IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 1, 2018, accepted March 12, 2018, date of publication March 19, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2817264

Artificial Noise-Based Physical-Layer Security in Interference Alignment Multipair Two-Way Relaying Networks

DEEB TUBAIL[1], MOHAMMED EL-ABSI[1,2], SALAMA S. IKKI[3], WESSAM MESBAH[4], (Member, IEEE), AND THOMAS KAISER[2], (Senior Member, IEEE)

[1]Palestinian Technology Research Center, Gaza, Palestine
[2]University of Duisburg-Essen, 47057 Duisburg, Germany
[3]Lakehead University, Thunder Bay, ON P7B 5E1, Canada
[4]King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding author: Deeb Tubail (dtubail@gmail.com)

This work was supported by the Deanship of Scientific Research, King Fahd University of Petroleum and Minerals, under Grant RG1416.

ABSTRACT This paper introduces two novel physical-layer security algorithms for interference alignment (IA)-based multipair communication systems with a single half-duplex relay and a single eavesdropper. According to these proposed physical-layer security algorithms, users mix their information signals with jamming signals, and broadcast them at the multiple access phase, while the relay forwards the mixed signals at the broadcast phase. Moreover, the relay and users' precoding and decoding matrices are designed in a way which enables the legitimate receivers to eliminate the jamming signals while the hidden eavesdropper is unable to eliminate these jamming streams. In this context, the proposed algorithms are designed to transmit the information streams with minimum power, preserving the user received signal to noise ratio above a pre-determined threshold and utilizing the remaining power for the jamming signals. Therefore, the user and relay power budgets allocation is formulated as a joint optimization problem that can be solved using an iterative optimization algorithm and semi-definite programming. In such fashion, four transmission models are proposed to manage the artificial noise transmission among the different users to achieve a tradeoff between the users sum-rate and secrecy rate. Extensive simulation results are provided to show the efficiency of the proposed algorithms and the transmission models in achieving the transmission security for IA-based multiuser relaying networks.

INDEX TERMS Interference alignment, two-way relaying, physical layer security, secrecy sum-rate.

I. INTRODUCTION

Security is a sensitive and critical issue in wireless communication networks for both the users and service providers due to the broadcast nature of such systems, making these wireless networks particularly vulnerable to eavesdropping and jamming. Researchers predict that physical layer security is a promising way to overcome security threats, since the physical layer security approach establishes a secure communication without the need to computational resources from the upper layers as in conventional security solutions [2], [3]. The theory behind physical layer security is to utilize the inherent randomness of noise and communication channels to limit the information rate that can be attained by the unauthorized users, where no limitations are assumed for the eavesdropper in terms of computational resources or network parameter knowledge.

Wireless networks that implement interference alignment (IA) and relaying concepts are considered as promising candidates for the future wireless communication systems. IA achieves the optimal sum-rate at the high signal-to-noise ratio (SNR) regime [4]–[6], while relaying extends the coverage area and provides diversity at the receivers [7]. In this context, relay aided IA is largely investigated in literature [8]. IA is a cooperative interference management technique that reduces the dimensionality of the interference subspace aiming at maximizing the degrees-of freedom (DoF) of wireless systems [4]. This concept can be achieved by designing linear precoders and decoders in a smart way in order to align the interference signals in half of the spatial subspaces at the receivers. Accordingly, IA is utilized to mitigate inter-pair interference in multipair two-way relaying, where multiple pairs of users simultaneously establish a communication link with the aid of a single shared relay [9], [10]. In half-duplex two way relaying protocol, the communication is established through two phases. In the first phase, called multiple access phase (MAC phase), the users transmit their signals to the relay, and the relay broadcasts the signals to the destinations in the second phase, called broadcast phase (BC phase) [11].

Physical layer security in different wireless systems is widely considered in the literature [2], [12]–[27]. In [2], the concept of secrecy-rate of degraded wiretap channel is studied, where the authors define the secrecy capacity as the highest information rate that can be achieved at the destination while the eavesdropper is unable to recover the transmitted signals. Bloch *et al.* [12] and Gopala *et al.* [13] consider the security in communications over fading channels. Increasing the secrecy in relay networks is investigated in [15] and [16], where the relays cooperate in security by generating jamming noise. In [17] and [18], several relay selection criteria are proposed and examined to secure multiple amplify-and-forward (AF) relay networks. The secure communication for multiuser relay network is analyzed in [19], where the authors propose an algorithm, for a system composed of two users and multiple relays, that allows the relays to transmit jamming signals along with the legitimate users. Sakran *et al.* [20] consider the sum secrecy-rate maximization in a full duplex two-way relaying systems. The works [21]–[23] study the security performance in the existence of untrusted relay. The achievable secrecy rate is analyzed for the general untrusted relay channel in [22], while an iterative algorithm for the jointly design of user and relay beamformers with an untrusted relay and for an AF MIMO untrusted relay system is proposed in [23]. Additionally, the impact of correlated fading on secure communication of multiple AF relaying networks is studied in [24]. Karas *et al.* [25] study the effect of fading and multiple interferers on the physical-layer security where they conclude that the impact of interference should be seriously taken into account in the design and deployment of a wireless system with physical-layer security. Moreover, the impact of co-channel interference on the security performance of multiple AF relaying networks is investigated in [18]. A novel frequency diverse array beamforming approach is designed in [26] to achieve physical layer security. In [27], the outage probability for secrecy rate in MIMO wireless systems in the presence of eavesdroppers and jammers for cyber physical system devices is analyzed.

Very recent works consider the physical layer security in IA based K-users interference channel systems, where anti-jamming and anti-eavesdropping algorithms are proposed [28]–[30]. The work in [29] analyzes the performance and feasibility conditions of the external eavesdropper and proposes an anti-eavesdropping algorithm for conventional IA systems. Two anti-jamming algorithms are proposed in [30] for the conventional IA networks, where the jamming and interference signals are aligned into the same subspace at each receiver in the first algorithm, whereas the received signal-to-interference plus-noise ratio (SINR) is maximized in the second algorithm. Afterwards, the work in [31] proves the secure DoF of the multi-way relay wiretap system, where the IA is implemented in two models. In the first model, called broadcast wiretap channel (BWC), the authors assume that the eavesdropper can only wiretap the signals in the second phase of the half duplex relaying network. In the second model, called multiple-access BWC (MBWC), the eavesdropper can wiretap the signals from both MAC and BC phases using full duplex relay, where the relay broadcasts jamming noise at both phases. Accordingly, MBWC algorithm adds hardware complexity to the system without capacity benefits.

In this work, we propose two secure transmission algorithms for IA based half-duplex two-way relaying system, where the two algorithms are effective in MAC and BC phases with lower complexity compared to [31]. In the proposed algorithms, the users and relay utilize parts of their power budget to transmit artificial noise signals mixed with the information signals. Accordingly, the proposed methods are performed via two steps. In the first step, the conventional IA matrices are redesigned to enable the legitimate users to eliminate the artificial jamming streams, while the hidden eavesdropper cannot distinguish the information signals from the jamming signals. In the second step, the relay and users divide the available power budget aiming at transmitting the artificial jamming streams with the maximum available power after guaranteeing the quality-of-service (QoS) of the users.

The main contributions of this paper are summarized as follows.

- Two secure transmission algorithms are proposed, that are effective in both of the two-way relaying phases without converting the half-duplex relay to full-duplex as in [31] and with lower number of antennas compared to [1].
- IA matrices are redesigned to enable the legitimate users to consequently eliminate the artificial jamming streams, while the hidden eavesdropper cannot distinguish the information streams from the jamming streams.
- Power allocation is performed between the information streams and the artificial jamming streams aiming at transmitting the artificial jamming streams with the maximum power after guaranteeing the QoS of the users.
- The proposed algorithms are manipulated in four transmission models. Such models manage the way and the criterion of artificial noise transmission in the MAC phase in order to achieve the required trade-off between the sum-rate and secrecy rate.

The paper is organized as follows. Section II describes the system model, and Section III introduces the anti-eavesdropping physical layer security algorithms. In Section IV, the optimization problem is formulated, and four transmission schemes are presented in Section V. Finally section VI presents the simulation results followed by conclusions in section VII.

Notations: a scalar is denoted by lower-case letter, boldface lower-case letters are used for vectors, and boldface upper-case letters are used for matrices. For any general matrix $\mathbf{A}$, $\mathbf{A}^{\mathrm{T}}$, $\mathbf{A}^{\mathrm{H}}$, and $\mathbf{A}^{-1}$ denote the transpose, conjugate transpose and inverse respectively. The symbol ($\bullet$) in the expression $\mathbf{A} \bullet \mathbf{B}$ means multiplication of each element in $\mathbf{A}(i, j)$ by the corresponding one $\mathbf{B}(i, j)$.

II. SYSTEM MODEL

Consider $2K$ users (transceivers), each with M antennas, who employ IA in exchanging their d data streams securely via a relay node with R antennas in a half-duplex two-way relay network [10]. A hidden external eavesdropper with R_{E} antennas tries to tap these legitimate data streams as seen in Fig. 1. Due to the nature of the half-duplex two-way relaying protocol, the eavesdropper has a chance to collect two copies of the legitimate data streams. The first copy is collected when the transmitters send their streams to the relay in the MAC phase; while the other copy is collected in BC phase when the relay broadcasts the signals to their destinations (transceivers). In order to reduce the amount of the eavesdropped information, users broadcast $\hat{d}$ artificial jamming streams mixed with their actual data streams, where the hidden eavesdropper is unable to distinguish the jamming streams from the received signal to eliminate, while such streams can easily be distinguished and eliminated by legitimate users.

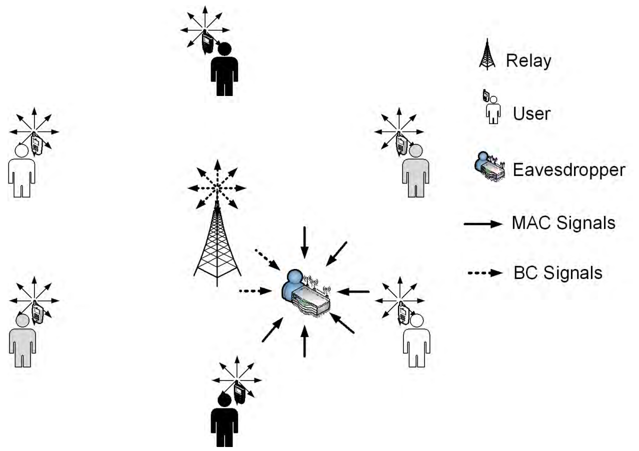

FIGURE 1. IA relaying system in the existence of an eavesdropper.

In the MAC phase, the k^{th} node, that has power matrix $\mathbf{P}_k$, exchanges d data streams with its partner, the j^{th} node, that has power matrix $\mathbf{P}_j$, where

$$j = \begin{cases} k+K & \text{if } k \leq K \\ k-K & \text{if } k > K. \end{cases}$$

Therefore, the k^{th} user mixes its d information streams with $\hat{d}$ artificial noise streams. Consequently, the k^{th} user's transmitted signal $\mathbf{s}_k$ is

$$\mathbf{s}_k = \mathbf{V}_k \mathbf{x}_k + \hat{\mathbf{V}}_k \hat{\mathbf{x}}_k, \tag{1}$$

where $\mathbf{x}_k \in \mathbb{C}^{d\times 1}$ and $\hat{\mathbf{x}}_k \in \mathbb{C}^{\hat{d}\times 1}$ are the transmitted data streams and artificial streams from the k^{th} user, respectively. $\mathbf{V}_k \in \mathbb{C}^{M\times d}$ and $\hat{\mathbf{V}}_k \in \mathbb{C}^{M\times \hat{d}}$ are the pre-coding matrices of the information streams and the artificial noise of the k^{th} node, respectively.

At this phase, the received signal at the relay is given by

$$\mathbf{y}_{\mathrm{R}} = \underbrace{\sum_{k=1}^{2K} \mathbf{H}_{\mathrm{r}k} \mathbf{V}_k \mathbf{x}_k}_{\text{useful signal}} + \underbrace{\sum_{k=1}^{2K} \mathbf{H}_{\mathrm{r}k} \hat{\mathbf{V}}_k \hat{\mathbf{x}}_k}_{\text{artificial noise}} + \mathbf{n}_{\mathrm{R}}, \tag{2}$$

where $\mathbf{H}_{\mathrm{r}k} \in \mathbb{C}^{R\times M}$ is the channel response between the k^{th} user and the relay, while the received signal at the eavesdropper is given by

$$\mathbf{e}^{(1)} = \underbrace{\sum_{k=1}^{2K} \mathbf{F}_k \mathbf{V}_k \mathbf{x}_k}_{\text{useful signal}} + \underbrace{\sum_{k=1}^{2K} \mathbf{F}_k \hat{\mathbf{V}}_k \hat{\mathbf{x}}_k}_{\text{artificial noise}} + \mathbf{n}_{\mathrm{E}}^{(1)}, \tag{3}$$

where the superscript 1 denotes the first phase (MAC phase), $\mathbf{F}_k \in \mathbb{C}^{R_{\mathrm{E}}\times M}$ is the channel response between the k^{th} user and the eavesdropper, $\mathbf{n}_{\mathrm{R}} \in \mathbb{C}^{R\times 1}$ is the independent and identically distributed (i.i.d) additive white Gaussian noise (AWGN) vector at the relay with zero mean and unit variance and $\mathbf{n}_{\mathrm{E}} \in \mathbb{C}^{R_{\mathrm{E}}\times 1}$ is i.i.d AWGN with zero mean and unit variance at the eavesdropper.

At the BC phase, the relay amplifies the received signals by multiplying them by the processing matrix $\mathbf{G} \in \mathbb{C}^{R\times R}$ then forwards them to their destinations (amplify and forward relaying protocol). Thus, the transmitted signal from the relay is

$$\mathbf{s} = \mathbf{G}\mathbf{y}_{\mathrm{R}}, \tag{4}$$

where the relay has a transmission power budget P_{r}.

The k^{th} node receives its signal at the second phase where the post-processing received signal is

$$\begin{aligned} \mathbf{y}_k &= \mathbf{U}_k^{\mathrm{H}} \left[\mathbf{H}_{k\mathrm{r}} \mathbf{G} \mathbf{y}_{\mathrm{R}} + \mathbf{n}_k\right] \\ &= \mathbf{U}_k^{\mathrm{H}} \mathbf{H}_{k\mathrm{r}} \mathbf{G} \Bigg[\underbrace{\mathbf{H}_{\mathrm{r}k} \mathbf{V}_k \mathbf{x}_k}_{\text{self-interference}} + \underbrace{\mathbf{H}_{\mathrm{r}j} \mathbf{V}_j \mathbf{x}_j}_{\text{useful data}} \\ &\quad + \underbrace{\sum_{l=1, l\neq k, l\neq j}^{2K} \mathbf{H}_{\mathrm{r}l} \mathbf{V}_l \mathbf{x}_l}_{\text{pairs interference}} + \underbrace{\sum_{k=1}^{2K} \mathbf{H}_{\mathrm{r}k} \hat{\mathbf{V}}_k \hat{\mathbf{x}}_k}_{\text{artificial noise}} + \mathbf{n}_{\mathrm{R}} \Bigg] + \mathbf{U}_k^{\mathrm{H}} \mathbf{n}_k, \end{aligned} \tag{5}$$

where $\mathbf{H}_{k\mathrm{r}} \in \mathbb{C}^{M\times R}$ is the channel response between the relay and the k^{th} user, $\mathbf{U}_k \in \mathbb{C}^{M\times d}$ is interference suppression matrix applied at the k^{th} user, and $\mathbf{n}_k \in \mathbb{C}^{M\times 1}$ is i.i.d AWGN with zero mean and unit variance at the k^{th} user.

According to (5), the post-processing received signal at the k^{th} node is composed of the useful signal, the self-interference signal, the interference from other pairs, and the artificial noise signals.

According to [32], the self-interference and pairs interference can be perfectly canceled at the receiver. The artificial noise signals can also be discarded perfectly as will be shown in section (III). Hence, the received signal at the k^{th} node is given by

$$\mathbf{y}_k = \mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}\Big[\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{x}_j + \mathbf{n}_{\mathrm{R}}\Big] + \mathbf{U}_k^{\mathrm{H}}\mathbf{n}_k, \tag{6}$$

while the received signal at the hidden eavesdropper at the second phase is given by

$$\begin{aligned}\mathbf{e}^{(2)} &= \mathbf{F}_{\mathrm{r}}\mathbf{G}\mathbf{y}_{\mathrm{R}} + \mathbf{n}_{\mathrm{E}}^{(2)}\\ &= \mathbf{F}_{\mathrm{r}}\mathbf{G}\Bigg[\underbrace{\sum_{k=1}^{2K}\mathbf{H}_{\mathrm{r}k}\mathbf{V}_k\mathbf{x}_k}_{\text{useful signal}} + \underbrace{\sum_{k=1}^{2K}\mathbf{H}_{\mathrm{r}k}\hat{\mathbf{V}}_k\hat{\mathbf{x}}_k}_{\text{artificial noise}} + \mathbf{n}_{\mathrm{R}}\Bigg] + \mathbf{n}_{\mathrm{E}}^{(2)},\end{aligned} \tag{7}$$

where $\mathbf{F}_{\mathrm{r}} \in \mathbb{C}^{R_{\mathrm{E}}\times R}$ is the channel frequency response between the eavesdropper and the relay.

According to the definition of the term "secrecy sum-rate" [29], the security performance of wireless systems is measured by the amount of un-tapped mutual information. Hence, the "secrecy sum-rate" term is expressed as

$$R_{\mathrm{s}} = \left(\left(\sum_{k=1}^{2K} R_k\right) - 0.5(R_{\mathrm{E}}^{(1)} + R_{\mathrm{E}}^{(2)})\right)^{+}. \tag{8}$$

Based on (6), the achievable data-rate at the k^{th} user from its partner is

$$\begin{aligned}R_k = \frac{1}{2}\log_2\Bigg|\mathbf{I} + \left(\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)\\ \times\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)^{-1}\Bigg|,\end{aligned} \tag{9}$$

where $\mathbf{Q}_{\mathrm{n}k}$ and $\mathbf{Q}_{\mathrm{Rn}}$ are the covariance matrices of $\mathbf{n}_k$ and $\mathbf{n}_{\mathrm{R}}$, respectively.

Under the assumption that the eavesdropper has a sufficient number of antennas, and is able to decode all the received signals, it can not distinguish the real signals from the jamming signals [29]. Consequently, the data-rate of the eavesdropper at the first phase based on (3) is

$$R_{\mathrm{E}}^{(1)} = \frac{1}{2}\log_2\left|\mathbf{I}_R + \left(\mathbf{Q}_{\mathrm{nE}}^{(1)} + \mathbf{Q}_{\mathrm{AN}}^{(1)}\right)^{-1}\left(\sum_{k=1}^{2K}\mathbf{F}_k\mathbf{V}_k\mathbf{P}_k\mathbf{V}_k^{\mathrm{H}}\mathbf{F}_k^{\mathrm{H}}\right)\right|, \tag{10}$$

where

$$\mathbf{Q}_{\mathrm{AN}}^{(1)} = \sum_{k=1}^{2K}\mathbf{F}_k\hat{\mathbf{V}}_k\hat{\mathbf{P}}_k\hat{\mathbf{V}}_k^{\mathrm{H}}\mathbf{F}_k^{\mathrm{H}}, \tag{11}$$

and the data-rate at the second phase based on (7) is

$$\begin{aligned}R_{\mathrm{E}}^{(2)} = \frac{1}{2}\log_2\Bigg|\mathbf{I}_R + \left(\mathbf{Q}_{\mathrm{nE}}^{(2)} + \mathbf{Q}_{\mathrm{AN}}^{(2)} + \mathbf{F}_{\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{F}_{\mathrm{r}}^{\mathrm{H}}\right)^{-1}\\ \times\left(\sum_{k=1}^{2K}\mathbf{F}_{\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}k}\mathbf{V}_k\mathbf{P}_k\mathbf{V}_k^{\mathrm{H}}\mathbf{H}_{\mathrm{r}k}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{F}_{\mathrm{r}}^{\mathrm{H}}\right)\Bigg|,\end{aligned} \tag{12}$$

where $\mathbf{Q}_{\mathrm{nE}}^{(1)}$, $\mathbf{Q}_{\mathrm{nE}}^{(2)}$ and $\mathbf{Q}_{\mathrm{Rn}}$ are the covariance matrices of $\mathbf{n}_{\mathrm{E}}^{(1)}$, $\mathbf{n}_{\mathrm{E}}^{(2)}$ and $\mathbf{n}_{\mathrm{R}}$, respectively and

$$\mathbf{Q}_{\mathrm{AN}}^{(2)} = \sum_{k=1}^{2K}\mathbf{F}_{\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}k}\hat{\mathbf{V}}_k\hat{\mathbf{P}}_k\hat{\mathbf{V}}_k^{\mathrm{H}}\mathbf{H}_{\mathrm{r}k}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{F}_{\mathrm{r}}^{\mathrm{H}}. \tag{13}$$

III. ANTI-EAVESDROPPING PHYSICAL LAYER SECURITY ALGORITHMS

In this section, two physical layer security algorithms are proposed for IA relay networks, where both depend on the transmission of jamming streams accompanied with the information streams from legitimate users in the MAC phase and from the relay in the BC phase. As a result, any hidden eavesdropper cannot eliminate these jamming streams and, consequentially, the actual data cannot be detected [29]. At the other side, the design of the precoding and decoding matrices of the users and the relay enables the legitimate users to eliminate these jamming streams in order to collect their desired streams.

In the first algorithm, $K\hat{d}$ dimensions are allocated at the relay for collecting the jamming streams, while lower dimension is occupied in the second algorithm, only $\hat{d}$ dimensions. Moreover, the desired data streams occupy Kd dimensions in both algorithms. Therefore, the pre-coding matrices and interference suppression matrices design should satisfy the following conditions

$$\operatorname{rank}\left(\mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\right) = d \quad \forall k, j. \tag{14}$$

$$\mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}l}\mathbf{V}_l = 0 \quad \forall l \neq j. \tag{15}$$

$$\mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}l}\hat{\mathbf{V}}_l = 0 \quad \forall k, l. \tag{16}$$

A. THE FIRST PROPOSED ALGORITHM

1) PRECODING AND DECODING MATRICES DESIGN

According to the first proposed algorithm *(Algorithm 1)*, the useful data streams are separated in Kd dimensions at the relay while the artificial streams are collected in $K\hat{d}$ dimensions. Therefore, the d columns of the precoding matrices $\mathbf{V}_k$ and $\mathbf{V}_j$ are chosen from the intersection subspace between the subspaces corresponding to $\mathbf{H}_{\mathrm{r}k}$ and $\mathbf{H}_{\mathrm{r}j}$, and can be found from

$$\operatorname{null}\left(\begin{bmatrix}\mathbf{H}_{\mathrm{r}k} & -\mathbf{H}_{\mathrm{r}j}\end{bmatrix}\right), \tag{17}$$

which achieves

$$\operatorname{span}\{\mathbf{H}_{\mathrm{r}k}\mathbf{V}_k\} = \operatorname{span}\{\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\} \qquad \forall k = 1, 2, \ldots, K, \tag{18}$$

where null(.) denotes the null space of the matrix within the brackets.

The $\hat{d}$ columns of the precoding matrices $\hat{\mathbf{V}}_k$ and $\hat{\mathbf{V}}_j$ are chosen from the previous intersection subspace that achieves

$$\operatorname{span}\{\mathbf{H}_{\mathrm{r}k}\hat{\mathbf{V}}_k\} = \operatorname{span}\{\mathbf{H}_{\mathrm{r}j}\hat{\mathbf{V}}_j\} \qquad \forall k = 1, 2, \ldots, K. \tag{19}$$

The d columns of the interference suppression matrices $\mathbf{U}_k$ and $\mathbf{U}_j$ are obtained from the intersection subspace between

Algorithm 1 Sub-Optimal Solution for SDP

```
Form the matrix in (40)
while $a_k < 0 \; \forall k$ do
    Let $j = \min(-\mathbf{a}_s^{T})$
    if $\mathbf{z}_j \leqslant 0$ then
        No Optimal Solution
    else
        for $m = 1 : 2K$ do
            if $z_{j,m} \geqslant 0$ then
                $R_m = \frac{d_{o,m}}{z_{j,m}}$
            end if
        end for
        Let $n = \min(R_m)$
    end if
    while $(z_{j,n} \neq 1)$ & $(z_{j,m} \neq 0 \; \forall m \neq n)$ do
        Use elementary row equation
    end while
end while
```

the subspaces $\mathbf{H}_{k\mathrm{r}}$ and $\mathbf{H}_{j\mathrm{r}}$ which is found from

$$\mathrm{null}\left(\begin{bmatrix} \mathbf{H}_{k\mathrm{r}} \\ -\mathbf{H}_{j\mathrm{r}} \end{bmatrix}\right), \tag{20}$$

aiming at accomplishing the following condition

$$\mathrm{span}\left\{\mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\right\} = \mathrm{span}\left\{\mathbf{U}_j^{\mathrm{H}}\mathbf{H}_{j\mathrm{r}}\right\} \quad \forall k = 1, 2, \ldots, K. \tag{21}$$

Let's define $\hat{\mathbf{U}}_k$ and $\hat{\mathbf{U}}_j$ as the matrices that achieves the following condition

$$\mathrm{span}\left\{\hat{\mathbf{U}}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\right\} = \mathrm{span}\left\{\hat{\mathbf{U}}_j^{\mathrm{H}}\mathbf{H}_{j\mathrm{r}}\right\} \quad \forall k = 1, 2, \ldots, K, \tag{22}$$

where their $\hat{d}$ columns are chosen from the same intersection in (20).

The perfect IA is done by the help of the relay that performs signal alignment using the receive zero-forcing matrix $\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}$ at MAC phase and the transmit zero-forcing matrix $\mathbf{G}_{\mathrm{tx}}$ at the BC phase. $\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}$ spatially separates the Kd effective data streams from other artificial streams, while $\mathbf{G}_{\mathrm{tx}}$ performs the channel alignment at BC phase to transmit the spatially orthogonalized signal through the Kd effective channels [32]. The relay processing matrix $\mathbf{G}$ is defined as $\mathbf{G} = \mathbf{G}_{\mathrm{tx}}\mathbf{G}_{\mathrm{p}}\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}$, where $\mathbf{G}_{\mathrm{p}}$ is the diagonal power matrix.

According to this algorithm, $\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}$ and $\mathbf{G}_{\mathrm{tx}}$ are defined as

$$\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}} = \begin{bmatrix} \mathbf{H}_{\mathrm{r}1}\mathbf{V}_1 & \cdots & \mathbf{H}_{\mathrm{r}k}\mathbf{V}_k & \mathbf{H}_{\mathrm{r}1}\hat{\mathbf{V}}_1 & \cdots & \mathbf{H}_{\mathrm{r}k}\hat{\mathbf{V}}_k \end{bmatrix}^{-1}, \tag{23}$$

and

$$\mathbf{G}_{\mathrm{tx}} = \begin{bmatrix} \mathbf{U}_1^{\mathrm{H}}\mathbf{H}_{1\mathrm{r}} \\ \vdots \\ \mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}} \\ \hat{\mathbf{U}}_1^{\mathrm{H}}\mathbf{H}_{1\mathrm{r}} \\ \vdots \\ \hat{\mathbf{U}}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}} \end{bmatrix}^{-1}, \tag{24}$$

2) FEASIBILITY CONDITIONS

In order to achieve the proposed design for precoding and decoding matrices, the network should be equipped with a sufficient number of antennas that can satisfy IA conditions. Next, we drive the feasibility conditions for *Algorithm 1*.

Since the relay subspace is divided into two subspaces, one with Kd dimensions for information streams and the other with $K\hat{d}$ dimensions for the artificial streams, the number of relay antennas should satisfy

$$R = Kd + K\hat{d} = K(d + \hat{d}).$$

According to [32] and [33], the number of variables of the information precoding matrix $\mathbf{V}$ of size Md can be reduced to $Md - d^2$ variable. Therefore, the total number of variables for $2K$ users is $2K(M - d)d$. In the same context, the total number of the relay variables for the information streams is $K(Kd - d)d$. Therefore, the total number of variables related to the information streams is

$$\zeta_{\mathrm{v}} = 2K(M - d)d + K(Kd - d)d.$$

According to [32], the total number of constraints for d information streams transmitted from the $2K$ nodes is given by

$$\zeta_{\mathrm{c}} = 2K(Kd - d)d.$$

The system is proper when the number of variables is equal or greater than the number of constraints and thus

$$\zeta_{\mathrm{v}} \geq \zeta_{\mathrm{c}}.$$

At each user, the number of antennas used to transmit the information streams is

$$\bar{M} \geq 0.5(K + 1)d.$$

In the same way, when a legitimate user adds $\hat{d}$ jamming streams for security purposes, the number of the additional antennas is

$$\hat{M} \geq 0.5(K + 1)\hat{d}.$$

Therefore, the system is proper and the conditions in (14)-(16) are satisfied when the number of variables is greater than the number of equations. Ultimately, the number of the antennas at the relay is

$$R = Kd + K\hat{d} = K(d + \hat{d}),$$

while the number of antennas equipped at each user is

$$M \geq 0.5(K + 1)(d + \hat{d}). \tag{25}$$

Algorithm 2 An Iterative Optimization Algorithm for Joint Optimization Problem

```
1: Initialize $\mathbf{P}_j = \frac{P_{\max}}{d}\mathbf{I}_{\mathrm{R}}$
2: Repeat
3: Solve Problem $P2$ and get $\mathbf{G}_{\mathrm{P}}$ when $\mathbf{P}_j$ is fixed.
4: Solve Problem $P7$ and get $\mathbf{P}_j$ using the previous $\mathbf{G}_{\mathrm{P}}$.
5: Until Problem $P1$ converges.
```

B. THE SECOND PROPOSED ALGORITHM

1) PRECODING AND DECODING MATRICES DESIGN

In the second proposed algorithm *(Algorithm 2)*, all jamming streams are collected only in $\hat{d}$ dimensions at the relay, whereas Kd dimensions are kept for the useful data streams. The d columns of the information precoding matrices $\mathbf{V}_k$ and $\mathbf{V}_j$ are chosen in the same way as in *Algorithm 1*, while the $\hat{d}$ columns forming the artificial streams precoding matrices $\hat{\mathbf{V}}_1$ and $\hat{\mathbf{V}}_{1+K}$ are chosen from the columns of the intersection between the subspaces corresponding to $\mathbf{H}_{\mathrm{r}1}$ and $\mathbf{H}_{\mathrm{r}(1+K)}$ that is found from

$$\mathrm{null}\Big(\big[\mathbf{H}_{\mathrm{r}1} \quad -\mathbf{H}_{\mathrm{r}(1+K)}\big]\Big), \tag{26}$$

which achieves

$$\mathrm{span}\{\mathbf{H}_{\mathrm{r}1}\hat{\mathbf{V}}_1\} = \mathrm{span}\{\mathbf{H}_{\mathrm{r}(1+K)}\hat{\mathbf{V}}_{(1+K)}\}.$$

After that, $\hat{\mathbf{V}}_k$ for other users should satisfy

$$\mathrm{span}\{\mathbf{H}_{\mathrm{r}k}\hat{\mathbf{V}}_k\} = \mathrm{span}\{\mathbf{H}_{\mathrm{r}1}\hat{\mathbf{V}}_1\} \quad \forall k \neq 1, 1+K, \tag{27}$$

which introduces the following equation

$$\hat{\mathbf{V}}_k = \mathbf{H}_{\mathrm{r}k}^{-1}\mathbf{H}_{\mathrm{r}1}\hat{\mathbf{V}}_1 \qquad \forall k \neq 1, 1+K. \tag{28}$$

The d columns of the interference suppression matrices $\mathbf{U}_k$ and $\mathbf{U}_j$ are also obtained from the intersection subspace between the subspaces $\mathbf{H}_{k\mathrm{r}}$ and $\mathbf{H}_{j\mathrm{r}}$ as in *Algorithm 1*, while the $\hat{d}$ columns of $\hat{\mathbf{U}}_1$ are chosen from the intersection

$$\mathrm{null}\left(\begin{bmatrix}\mathbf{H}_{1\mathrm{r}} \\ -\mathbf{H}_{(1+K)\mathrm{r}}\end{bmatrix}\right), \tag{29}$$

where $\hat{\mathbf{U}}_1$ is the matrix that achieves the following condition

$$\mathrm{span}\left\{\hat{\mathbf{U}}_1^{\mathrm{H}}\mathbf{H}_{1\mathrm{r}}\right\} = \mathrm{span}\left\{\hat{\mathbf{U}}_{1+K}^{\mathrm{H}}\mathbf{H}_{(1+K)\mathrm{r}}\right\}. \tag{30}$$

In this algorithm, the receive zero-forcing matrix $\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}$ is defined as

$$\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}} = \left[\mathbf{H}_{\mathrm{r}1}\mathbf{V}_1 \cdots \mathbf{H}_{\mathrm{r}k}\mathbf{V}_k \ \mathbf{H}_{\mathrm{r}1}\hat{\mathbf{V}}_1\right]^{-1}, \tag{31}$$

and the transmit zero-forcing matrix $\mathbf{G}_{\mathrm{tx}}$ is defined as

$$\mathbf{G}_{\mathrm{tx}} = \begin{bmatrix}\mathbf{U}_1^{\mathrm{H}}\mathbf{H}_{1\mathrm{r}} \\ \vdots \\ \mathbf{U}_k^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}} \\ \hat{\mathbf{U}}_1^{\mathrm{H}}\mathbf{H}_{1\mathrm{r}}\end{bmatrix}^{-1}. \tag{32}$$

2) FEASIBILITY CONDITIONS

According to *Algorithm 2*, the information streams for each paired users are separated in their own d dimensions at the relay, while all artificial data streams occupy only $\hat{d}$ dimensions at the relay. Therefore, the relay subspace dimension must be

$$R = Kd + \hat{d}.$$

From (28), $\hat{\mathbf{V}}$ is feasible when the channels between the nodes and the relay $\mathbf{H}_{\mathrm{r}k}$ are square and invertible which implies that the users should be equipped with the same number of antennas as the relay, i.e. $M = R$.

IV. PROBLEM FORMULATION

In the previous section, the precoding and decoding matrices are designed. However, the transmission of the jamming streams requires parts of the power budget of the users and the relay. Therefore, in this section, we formulate an optimization problem that that aims at enhancing the security performance of the systems by maximizing the transmitted power of the artificial streams while the users QoS are preserved. Accordingly, the objective of the optimization problem is to minimize the power allocated for the information streams at the users and the relay subject to the minimum SNR of the users that achieves the required QoS. Hence, the remaining power is utilized for the jamming streams. This problem is formulated as a joint optimization problem as follows

$$P1: \min_{\mathbf{G},\mathbf{P}_j} \mathrm{trace}\Big(\mathbf{G}\mathbf{y}_{\mathrm{R}}\mathbf{y}_{\mathrm{R}}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\Big) + \mathrm{trace}\Big(\sum_{j=1}^{2K}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\Big) \tag{33a}$$

$$\mathrm{s.t.}: \frac{\mathrm{trace}\left(\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)}{\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)} \geq \gamma_k \quad \forall k \tag{33b}$$

$$\mathbf{G} \succeq 0 \tag{33c}$$

$$\mathbf{P}_j \succeq 0 \quad \forall j. \tag{33d}$$

The cost function in (33a) has two terms: the first term is the relay power and the second is the user power. This objective aims at allocating the minimum relay and users power that is needed for information transmission. The constraints in (33b) guarantee that the SNR of the received signal at the destinations to be above a predetermined threshold, γ_k for the k^{th} destination. Moreover, the other two constraints in (33c) and (33d) keep non-negative power values for the relay and the users.

The iterative optimization algorithm in [34] is used to solve the joint optimization problem where an optimization variable is fixed to solve the optimization problem with respect to the other optimization variable.

According to the iterative algorithm, when the users' power matrices are fixed, the second term of the cost function of Problem $P1$ is dropped and Problem $P1$ becomes as shown in Problem $P2$, while fixing the relay power matrix $\mathbf{G}$ drops the first term of the cost function and converts Problem $P1$ to be as expressed as will be shown in Problem $P7$.

A. RELAY POWER ALLOCATION

The relay power allocation is more applicable when the users' power matrices are fixed and their term is dropped from Problem $P1$ according to the iterative algorithm. Dropping the users' power term from Problem $P1$ produces the optimization Problem $P2$ where the relay transmission power is minimized and the users QoS is guaranteed. The mathematical expression of the optimization problem is

$$P2: \min_{\mathbf{G}} \ \mathrm{trace}\left(\mathbf{G}\mathbf{y}_{\mathrm{R}}\mathbf{y}_{\mathrm{R}}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\right) \tag{34a}$$

$$\text{s.t.}: \ \frac{\mathrm{trace}\left(\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)}{\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)} \geq \gamma_k \quad \forall k \tag{34b}$$

$$\mathbf{G} \succeq 0. \tag{34c}$$

To allocate relay power, optimization Problem $P2$ is rewritten as a function of $\mathbf{G}_{\mathrm{p}}$ which converts the optimization in Problem $P2$ to be as

$$P3: \min_{\mathbf{G}_{\mathrm{p}}} \ \mathrm{trace}\left(\mathbf{G}_{\mathrm{tx}}\mathbf{G}_{\mathrm{p}}\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{y}_{\mathrm{R}}\mathbf{y}_{\mathrm{R}}^{\mathrm{H}}\mathbf{G}_{\mathrm{rx}}\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{G}_{\mathrm{tx}}^{\mathrm{H}}\right) \tag{35a}$$

$$\text{s.t.}: \ \mathrm{trace}\left(\mathbf{H}_{k\mathrm{r}}\mathbf{G}_{\mathrm{tx}}\mathbf{G}_{\mathrm{p}}\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}_{\mathrm{rx}}\mathbf{G}_{\mathrm{p}}^{\mathrm{H}} \mathbf{G}_{\mathrm{tx}}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right) \geq \gamma_k\left[\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}_{\mathrm{tx}}\mathbf{G}_{\mathrm{p}}\mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}_{\mathrm{rx}}\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{G}_{\mathrm{tx}}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)\right] \quad \forall k$$

$$\mathbf{G}_{\mathrm{p}} \ \text{Diagonal} \tag{35b}$$

$$\mathbf{G}_{\mathrm{p}} \succeq 0. \tag{35c}$$

By defining the following parameters

$$\begin{aligned}
\mathbf{D}_{\mathrm{o}} &= \mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{y}_{\mathrm{R}}\mathbf{y}_{\mathrm{R}}^{\mathrm{H}}\mathbf{G}_{\mathrm{rx}} \\
\mathbf{D}_k &= \mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}_{\mathrm{rx}} \\
\mathbf{J}_0 &= \mathbf{G}_{\mathrm{tx}}^{\mathrm{H}}\mathbf{G}_{\mathrm{tx}} \\
\mathbf{J}_k &= \mathbf{G}_{\mathrm{tx}}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}_{\mathrm{tx}} \\
\mathbf{D}_{\mathrm{n}} &= \mathbf{G}_{\mathrm{rx}}^{\mathrm{H}}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}_{\mathrm{rx}},
\end{aligned}$$

and after some mathematical manipulation, the optimization Problem $P3$ is converted to the optimization Problem $P4$, where

$$P4: \min_{\mathbf{G}_{\mathrm{p}}} \ \mathrm{trace}\left(\mathbf{G}_{\mathrm{p}}\mathbf{D}_{\mathrm{o}}\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{J}_0\right) \tag{36a}$$

$$\text{s.t.}: \ \mathrm{trace}\left(\mathbf{G}_{\mathrm{p}}\left(\mathbf{D}_k - \gamma_k\mathbf{D}_{\mathrm{n}}\right)\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{J}_k\right) \geq \gamma_k\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k}\right) \quad \forall k \tag{36b}$$

$$\mathbf{G}_{\mathrm{p}} \ \text{Diagonal} \tag{36c}$$

$$\mathbf{G}_{\mathrm{p}} \succeq 0. \tag{36d}$$

By defining the column vector $\hat{\mathbf{g}}_{\mathrm{p}} = \mathrm{diag}\left(\mathbf{G}_{\mathrm{p}}\right)$ and $\hat{\mathbf{G}}_{\mathrm{p}} = \hat{\mathbf{g}}_{\mathrm{p}}\hat{\mathbf{g}}_{\mathrm{p}}^{\mathrm{H}}$, the following two equalities hold

$$\mathrm{trace}\left(\mathbf{G}_{\mathrm{p}}\mathbf{D}_{\mathrm{o}}\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{J}_0\right) = \mathrm{trace}\left(\hat{\mathbf{G}}_{\mathrm{p}}\left(\mathbf{D}_0^{\mathrm{T}} \bullet \mathbf{J}_0\right)\right)$$

and

$$\mathrm{trace}\left(\mathbf{G}_{\mathrm{p}}\left(\mathbf{D}_k - \gamma_k\mathbf{D}_{\mathrm{n}}\right)\mathbf{G}_{\mathrm{p}}^{\mathrm{H}}\mathbf{J}_k\right) = \mathrm{trace}\left(\hat{\mathbf{G}}_{\mathrm{p}}\left(\left(\mathbf{D}_k - \gamma_k\mathbf{D}_{\mathrm{n}}\right)^{\mathrm{T}} \bullet \mathbf{J}_k\right)\right).$$

Consequentially, Problem $P4$ is rewritten as

$$P5: \min_{\hat{\mathbf{G}}_{\mathrm{p}}} \ \mathrm{trace}\left(\hat{\mathbf{G}}_{\mathrm{p}}\hat{\mathbf{J}}_0\right) \tag{37a}$$

$$\text{s.t.}: \ \mathrm{trace}\left(\hat{\mathbf{G}}_{\mathrm{p}}\hat{\mathbf{J}}_k\right) \geq \gamma_k\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k}\right) \quad \forall k \tag{37b}$$

$$\hat{\mathbf{G}}_{\mathrm{p}} \succeq 0, \tag{37c}$$

where $\hat{\mathbf{J}}_{\mathrm{o}} = \left(\mathbf{D}_{\mathrm{o}}^{\mathrm{T}} \bullet \mathbf{J}_{\mathrm{o}}\right)$ and $\hat{\mathbf{J}}_k = \left(\left(\mathbf{D}_k - \gamma_k\mathbf{D}_{\mathrm{n}}\right)^{\mathrm{T}} \bullet \mathbf{J}_k\right)$.

It is clear that Problem $P5$ can be solved efficiently using semi-definite programming (SDP). However, this optimal solution suffers from high computational complexity, where SDP problems are usually solved via interior point method and needs complexity of $O((K(2+d))^7)$ [19].

By defining the following vectors:

$$\mathbf{w}_{\mathrm{p}} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{\mathrm{R}} \end{bmatrix}$$

where $\mathbf{c}_i$ is the i^{th} column of $\hat{\mathbf{G}}_{\mathrm{p}}$, and

$$\mathbf{z}_{\mathrm{k}} = \begin{bmatrix} \mathbf{r}_1 & \mathbf{r}_2 & \ldots & \mathbf{r}_{\mathrm{R}} \end{bmatrix},$$

where $\mathbf{r}_i$ is the i^{th} row of $\hat{\mathbf{J}}_k$. Let

$$a_k = \gamma_k\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k}\right). \tag{38}$$

Accordingly, Problem $P5$ can be rewritten as

$$P6: \min_{\mathbf{w}_{\mathrm{p}}} \ \mathbf{z}_{\mathrm{o}}\mathbf{w}_{\mathrm{p}} \tag{39a}$$

$$\text{s.t.}: \ \mathbf{z}_{\mathrm{k}}\mathbf{w}_{\mathrm{p}} \geqslant a_k \ \ \forall k, \tag{39b}$$

$$\mathbf{w}_{\mathrm{p}} \succeq 0. \tag{39c}$$

The diagonal matrix constraint is avoided to be used in Problem $P6$, which can be solved using simplex algorithm. Accordingly, the solution of Problem $P6$ is reduced to $O((2K)^{\lfloor \frac{K*d}{2} \rfloor})$ as a worst case.

Simplex algorithm is defined in [35] where the initial simplex tableau matrix is defined as

$$\begin{bmatrix} \mathbf{z}_1 & \mathbf{z}_2 & \ldots & \mathbf{z}_{2\mathrm{K}} & \vdots & \mathbf{I}_R & \mathbf{z}_{\mathrm{o}} \\ \ldots & \ldots & \ldots & \ldots & \vdots & \ldots & \ldots \\ & & -\mathbf{a}_{\mathrm{s}}^{\mathrm{T}} & & \vdots & \mathbf{0}_{(R+1)\times 1} & \end{bmatrix}, \tag{40}$$

where $\mathbf{a}_{\mathrm{s}}$ is the column vector that contains the SINR constraints for all users, a_k. Subsequently, most negative entry in the bottom row in the matrix in (40) is located to detect the entering column. After that, the ratios of the entries in the $\mathbf{z}_{\mathrm{o}}$ to their corresponding positive entries in the entering column are formed where the raw corresponded to the smallest nonnegative is the departing row.

As seen in [35], the entries in the departing row and the entering column are called the pivot which is set to 1 using the elementary row operations while all other entries in the entering column are set to 0. This process continues until all the entries in the bottom row are non negative elements where the optimal solution is given by the entries in the lower raw of the tableau matrix, which is the diagonal elements of the matrix $\mathbf{G}_{\mathrm{P}}^{\mathrm{H}}\mathbf{G}_{\mathrm{P}}$. The proposed algorithm is concluded in Algorithm 1.

B. USERS POWER ALLOCATION

In this part, we solve for the users' power by fixing the relay processing matrix $\mathbf{G}$, where Problem $P1$ becomes

$$P7: \min_{\mathbf{P}_j} \ \mathrm{trace}\Big(\sum_{j=1}^{2K} \mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\Big) \tag{41a}$$

$$\text{s.t.}: \ \frac{\mathrm{trace}\left(\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)}{\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)} \geq \gamma_k \quad \forall k \tag{41b}$$

$$\mathbf{P}_j \succeq 0 \quad \forall j. \tag{41c}$$

According to *trace* properties, Problem $P7$ is written as in the following problem

$$P8: \min_{\mathbf{P}_j} \ \mathrm{trace}\Big(\sum_{j=1}^{2K} \mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{V}_j\Big) \tag{42a}$$

$$\text{s.t.}: \ \frac{\mathrm{trace}\left(\mathbf{P}_j\mathbf{V}_j^{\mathrm{H}}\mathbf{H}_{\mathrm{r}j}^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{H}_{\mathrm{r}j}\mathbf{V}_j\right)}{\mathrm{trace}\left(\mathbf{Q}_{\mathrm{n}k} + \mathbf{H}_{k\mathrm{r}}\mathbf{G}\mathbf{Q}_{\mathrm{Rn}}\mathbf{G}^{\mathrm{H}}\mathbf{H}_{k\mathrm{r}}^{\mathrm{H}}\right)} \geq \gamma_k \quad \forall k \tag{42b}$$

$$\mathbf{P}_j \succeq 0 \quad \forall j, \tag{42c}$$

where Problem $P8$ can be solved efficiently using SDP.

The iterative optimization algorithm used for solving the joint optimization Problem $P1$ is presented in Algorithm 2.

According to [19], the complexity of step (3) in Algorithm 2 is given by $O((K(2+d))^7)$, while step (4) in Algorithm 2 has complexity of $2K \times O((1+M)^7)$. Hence, the total complexity of Algorithm 2 is given by

$$O(I((K(2+d))^7 + 2K \times (1+M)^7)),$$

where I is the number of the iteration at which optimization Problem $P1$ converges. Since $(K(2+d))^7 \geq 0$ and $(2K+M)^7 \geq 0$ and using big-O sum and product rules, the complexity of Algorithm 2 is

$$O(I(((2K)^{\lfloor \frac{K*d}{2} \rfloor}) + 2K)).$$

V. PROPOSED TRANSMISSION MODELS

In this section, we propose four transmission models, where these models determine the way of transmitting the jamming streams in the MAC phase. The purpose of such models to achieve the required tradeoff between the users sum-rate and the secrecy sum-rate. The models are presented as follows.

1) ALL-JAMM Model

Each pair mixes the information streams and the jamming signals, and then transmits the combination using *Algorithm 1* or *Algorithm 2*. This model is denoted next by *All-Jamm* model where the information streams are transmitted using the minimum power that achieves the required QoS to save the remaining power for the jamming signals. In this model, the jamming signal power is high since all users contribute to it. However, the disadvantage of this model is that the users jam the eavesdropper only when the their QoS have been achieved.

2) MAXSNR-JAMM Model

In this model, that is denoted next by *MaxSNR-Jamm* model, the pair with best averaged received SNR is chosen to transmit the artificial noise using *Algorithm 1* or *Algorithm 2*. This selected pair transmits its information stream by minimum power that achieves its QoS, then it utilizes the remaining power in the transmission of the artificial noise. The other pairs utilize their full power budget to send only their information streams, which enhances the exchanged data-rate in the network. The argue of this model is that the user with maximum SNR achieves its QoS with lower power compared to the other pairs, where larger amount of power is utilized for the artificial noise.

3) MINSNR-JAMM Model

In this model, the transmission of the artificial noise is performed only from the pair with the worst received SNR using *Algorithm 1* or *Algorithm 2*, while the other pairs fully utilize their power budget to send their information streams without jamming signals. This model has two cases. In the first case, the pair who has lowest SNR is not able to achieve its QoS; this indicated pair uses its power budget to broadcast the artificial noise, while the other pairs utilize their power budget only to send their information streams. In the second case, when the power budget of the pair with lowest SNR can achieve the predetermined QoS, its power is optimized to achieve the QoS with minimum power in order to save power for the jamming signal. The advantage of this model is empowering the system to jam the eavesdropper all the time, especially at low power budgets.

4) ALL-MINSNR-JAMM Model

This model is a combination from *All-Jamm* Model and *MinSNR-Jamm* Model, where all pairs transmit artificial streams when all of them achieve their QoS. Otherwise, the pair with the worst receiving SNR transmits artificial streams with its full power budget while the other pairs transmit only their real streams without the artificial noise. *Algorithm 1* or *Algorithm 2* is used for artificial noise transmission. This model gains the advantages of *All-Jamm* Model and *MinSNR-Jamm* Model, where it enables the system to jam the eavesdropper all the time.

VI. NUMERICAL SIMULATION

In this section, the performance of the proposed anti-eavesdropping physical layer algorithms including the four transmission models are evaluated, where a hidden eavesdropper taps three pairs with $M = 4$ antennas. In such fashion, each pair wants to exchange $d = 1$ data stream using the IA concept in a multi-user two-way relay network. Accordingly, $R = 6$ is needed to achieve the feasibility conditions of *Algorithm 1*, while $R = 4$ is needed for *Algorithm 2*. All results of the proposed algorithms with different transmission models are compared with the conventional IA multi-user two-way relay network, in which neither users nor relay send artificial streams. For simulation environment, MatLab toolbox "CVX" in [36] is used to solve the SDP optimization problems, where 1000 channels are generated randomly and independently as Gaussian with zero mean and unit variance.

Fig.2 and Fig.3 present the security performance of the proposed algorithms in terms of secrecy sum-rate. The security sum-rate starts to be improved earlier in *MinSNR-Jamm* and *All-MinSNR-Jamm* models because those models transmit artificial noise at any power budget range. On the other side, *All-Jamm* and *MaxSNR-Jamm* models enhance the secrecy sum-rate starting from 12 dB users' power budget, since no artificial noise is broadcasted before achieving the QoS of the users. Moreover, *All-Jamm* and *All-MinSNR-Jamm* models achieve better security sum-rate performance at high power budget regime, since all users contribute in the transmission of artificial noise after achieving their QoS. On the other side, *MaxSNR-Jamm* and *MinSNR-Jamm* models have lower security capacity than the other models at high power budget regime because only one pair transmits the artificial noise. Accordingly, *All-MinSNR-Jamm* scheme is the most efficient at all power budgets compared to the other schemes.

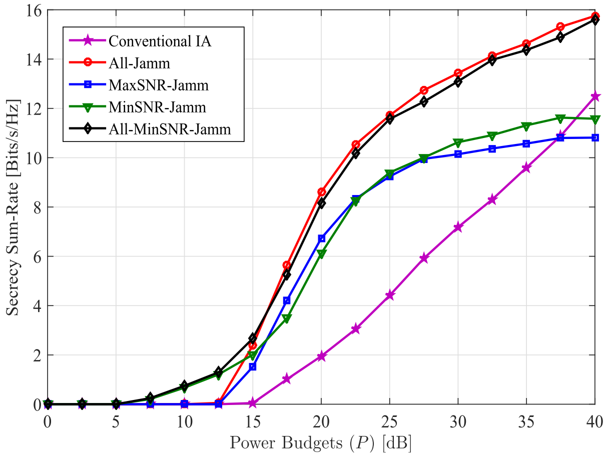

FIGURE 2. Algorithm 1: Secrecy Sum-Rate when $P_k = P_r = P$, $M = 4$ and $R = 6$.

Fig.4 and Fig.5 present the eavesdropper data-rates of the proposed transmission models using *Algorithm 1* and *Algorithm 2*, respectively. It is clearly noted that the eavesdropper data-rates associated to transmission models are significantly lower than the eavesdropper data-rate associated to conventional IA because of the transmission of artificial noise. In conventional IA, increasing the power budget will increase the eavesdropped data. This is not the

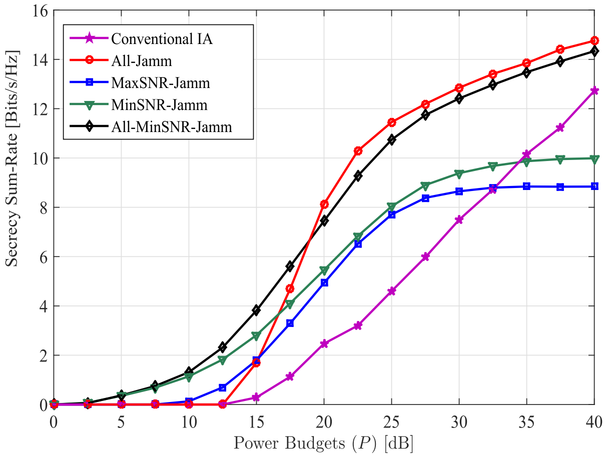

FIGURE 3. Algorithm 2: Secrecy Sum-Rate when $P_k = P_r = P$, $M = 4$ and $R = 4$.

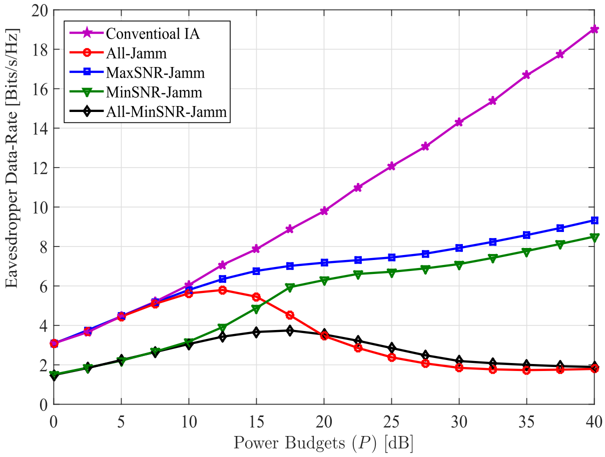

FIGURE 4. Algorithm 1: An eavesdropper data-are when $P_k = P_r = P$, $M = 4$ and $R = 6$.

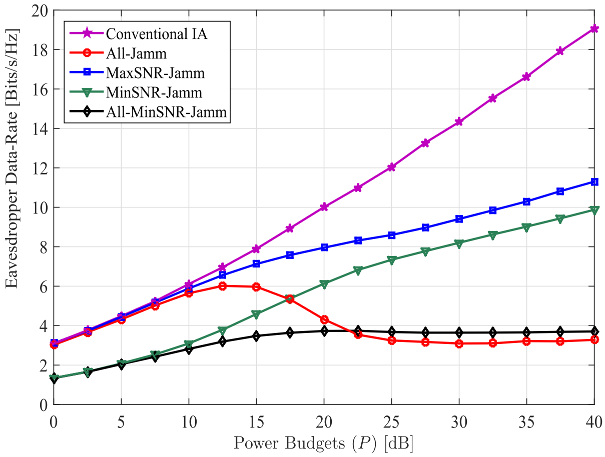

FIGURE 5. Algorithm 2: An eavesdropper data-rate when $P_k = P_r = P$, $M = 4$ and $R = 4$.

case for the proposed schemes, where all schemes succuss to degrade the eavesdropper data-rate. *MinSNR-Jamm* is efficient at low SNR regime because of the pair with the worst SNR broadcasts artificial noise even its QoS is not achieved. Such strategy has a minimal effect on the sum-rate of the users as will be discussed in Fig.6 and Fig.7. The model of *All-Jamm* is proficient at high SNR regime; this occurs when all pairs achieve their QoS and are able to jam the eavesdropper with the remaining power. Consequently, *All-MinSNR-Jamm* model is the best model since it collect the advantages of *All-Jamm* and *MinSNR-Jamm* models. Even *MaxSNR-Jamm* model attains less jamming, but it has better users sum-rates.

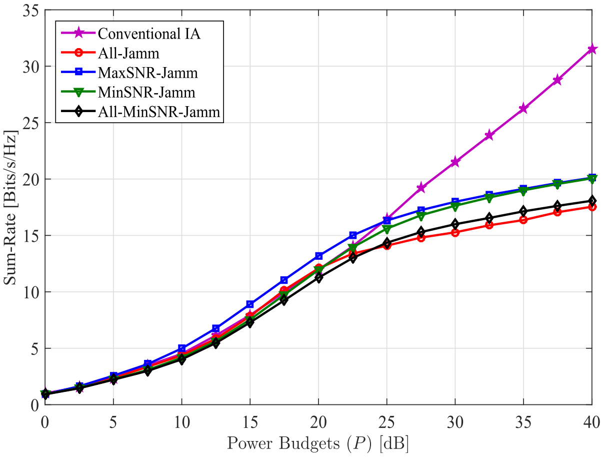

FIGURE 6. Algorithm 1: User sum-rate when $P_k = P_r = P$, $M = 4$ and $R = 6$.

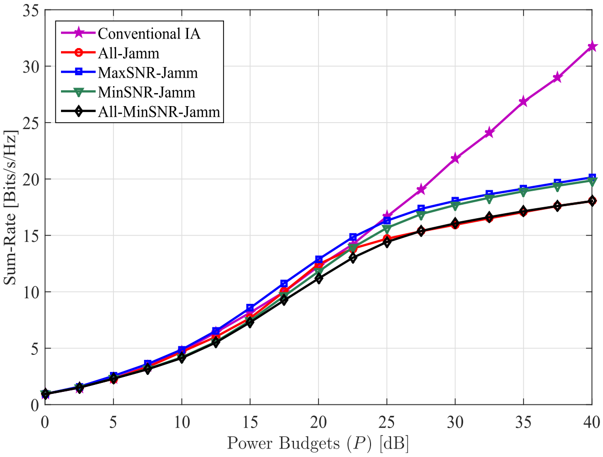

FIGURE 7. Algorithm 2: User sum-rate when $P_k = P_r = P$, $M = 4$ and $R = 4$.

Fig.6 and Fig.7 compare the users sum-rate of the proposed transmission models using *Algorithm 1* and *Algorithm 2* with conventional IA, respectively. Increasing the power budget in conventional IA increases the user sum-rate linearly because the power budgets are used totally for information streams. On the other side, the proposed transmission models present very close performance to the conventional IA until 20 dB. After that the sum-rate starts to saturate because the users at this regime achieve their QoS with the minimum required power, where the remaining power is utilized for the transmission of jamming streams. It is worth highlighting that even *MinSNR-Jamm* model utilizes the pair with the lowest SNR to only transmit the artificial noise; the user sum-rate has been minimally affected due to the worse channel the pair has. Moreover, it is noticed that the behavior of the sum-rates of the proposed transmission models are very similar since all the transmission models try to minimize the power of the information streams to maximize the power of jamming streams. Furthermore, it is noticed that the user sum-rates above 20 dB regime are the same for *All-Jamm* model and *All-MinSNR-Jamm* model because all users in this regime achieve their QoS and transmit artificial streams with the remaining power. In this SNR regime, *MaxSNR-Jamm* and *MinSNR-Jamm* models have the same behavior and better than the other two models, since one pair transmits artificial streams and the other pairs send their streams with their power budgets.

Fig.8 examines the convergence behavior of the proposed algorithms, where the cost function values of the optimization problems $P1$ and $P2$ are plotted versus the number of iterations. Algorithm 1 converges sufficiently at the second iteration, and just five iterations at maximum are needed for algorithm 2 to mostly converge.

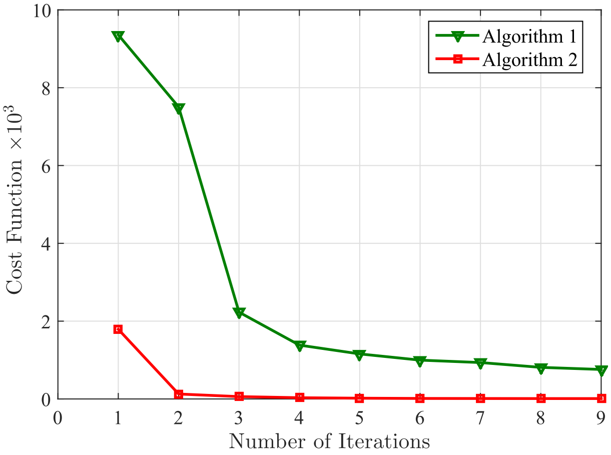

FIGURE 8. Convergence and local minimum of the optimization algorithms.

Fig.9 presents the performance of the simplified algorithm compared to the SDP solution, where the simplified algorithm can solve the optimization problems with lower complexity than SDP solution. This simplified algorithm successes to achieve exactly the same performance as the SDP solution with lower hardware complexity.

Since the behavior of *Algorithm 1* and *Algorithm 2* are identical, it is preferred to use the algorithm that can achieve lower hardware complexity. According to the feasibility conditions of the proposed algorithms, the relay in the *Algorithm 1* has more antennas than that in *Algorithm 2*. For the case of the users, there are main differences in their hard-

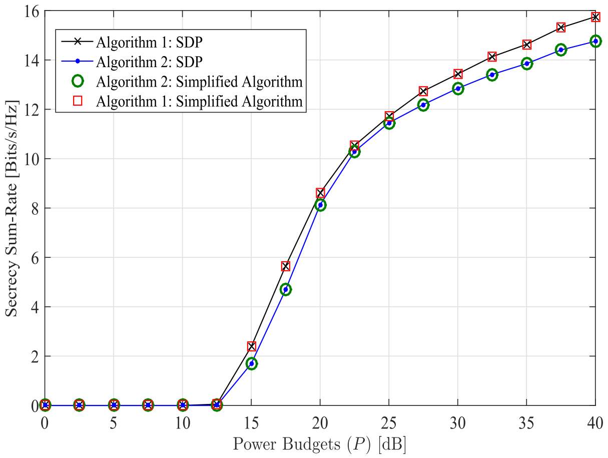

FIGURE 9. **Secrecy Sum-Rate when $P_k = P_r = P$.**

ware complexity according to the used algorithm, where the hardware complexity is a function of the differences between the number of legitimate data streams of the users d and the number of artificial noise streams $\hat{d}$. This relationship implies that

- When $d < \hat{d}$, each user should be employed greater number of antennas when using *Algorithm 1* compared to *Algorithm 2*.
- When $d = \hat{d}$, the users have the same number of antennas in both schemes.
- When $d > \hat{d}$, each user should be employed lower number of antennas when using *Algorithm 1* compared to *Algorithm 2*.

VII. CONCLUSION

In this paper, efficient physical layer security algorithms against eavesdropping for IA multiuser relay networks are proposed. The legitimate users confuse any hidden eavesdropper by mixing jamming streams with their information streams then transmitting them to the relay, which forwards these signals to their destinations. The precoding and decoding matrices of the users and relay are designed to enable legitimate users from canceling the jamming streams, while the eavesdropper cannot distinguish the jamming streams from the real streams in MAC and BC phases.

The proposed algorithms suggest transmitting the information streams from users and the relay with the minimum power budget that guarantees the user QoS constraints to maximize the remaining power and use it for the transmission of the artificial streams. This idea is formulated mathematically as a joint optimization problem, which is solved using an iterative optimization algorithm and semi-definite programming SDP, where the SDP solution is simplified to be solved using linear programming.

We investigate four transmission models to exchange the desired data between users in a secure wireless environment with minimum hardware complexity aiming at achieving the required trade-off between sum-rate and secrecy rate. The simulation results show that *All-MinSNR-Jamm* Model has the best performance, since it enhances the secrecy sum-rate in all power ranges efficiently. These results are also indicative of the fact that both the two proposed algorithms enhance the security performance of the system efficiently with different hardware complexities. The second algorithm always has a lower number of antennas at the relay but the complexity (number of antennas) at the users in both algorithms is determined according to the number of information streams and the number of jamming streams.

ACKNOWLEDGMENT

This paper was presented in part at the IEEE GLOBECOM 2017 [1].

REFERENCES

[1] D. Tubail, M. El-Absi, S. Ikki, W. Mesbah, and T. Kaiser, "Secure interference alignment based multiuser relay system using artificial noise," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

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

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

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

[5] M. El-Absi, M. Shaat, F. Bader, and T. Kaiser, "Interference alignment with frequency-clustering for efficient resource allocation in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7070–7082, Dec. 2015.

[6] M. El-Absi, S. Galih, M. Hoffmann, M. El-Hadidy, and T. Kaiser, "Antenna selection for reliable MIMO-OFDM interference alignment systems: Measurement-based evaluation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 2965–2977, May 2016.

[7] W. Deng and X. Gao, "Cooperative diversity with partially cooperative relays," in *Proc. 5th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCom)*, Oct. 2009, pp. 1–4.

[8] B. Nourani, S. A. Motahari, and A. K. Khandani, "Relay-aided interference alignment for the quasi-static interference channel," in *Proc. IEEE Int. Symp. Inf. Theory Process. (ISIT)*, Jun. 2010, pp. 405–409.

[9] H. Al-Shatri and T. Weber, "Interference alignment aided by non-regenerative relays for multiuser wireless networks," in *Proc. 8th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Nov. 2011, pp. 271–275.

[10] R. S. Ganesan, H. Al-Shatri, A. Kuehne, T. Weber, and A. Klein, "Pair-aware interference alignment in multi-user two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 3662–3671, Aug. 2013.

[11] B. Rankov and A. Wittneben, "Spectral efficient signaling for half-duplex relay channels," in *Proc. Conf. Rec. 39th Asilomar Conf. Signals, Syst. Comput.*, Nagoya, Japan, Oct. 2005, pp. 1066–1071.

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

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[14] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proc. Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 2183–2187.

[15] 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.

[16] 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.

[17] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sep. 2014.

[18] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[19] M. Obeed and W. Mesbah, "An efficient physical layer security algorithm for two-way relay systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Doha, Qatar, Apr. 2016, pp. 1–6.

[20] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[21] S. Zhang, L. Fan, M. Peng, and H. V. Poor, "Near-optimal modulo-and-forward scheme for the untrusted relay channel," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2545–2556, May 2016.

[22] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[23] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

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

[25] D. S. Karas, A.-A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, "Physical layer security in the presence of interference," *IEEE Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.

[26] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 671–684, Mar. 2018.

[27] D. B. Rawat, T. White, S. Parwez, C. Bajracharya, and M. Song, "Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1987–1993, Dec. 2017.

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

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

[30] N. Zhao, J. Guo, F. R. Yu, M. Li, and V. C. M. Leung, "Antijamming schemes for interference-alignment-based wireless networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1271–1283, Feb. 2016.

[31] Y. Fan, X. Liao, and A. V. Vasilakos, "Physical layer security based on interference alignment in K-user MIMO Y wiretap channels," *IEEE Access*, vol. 5, pp. 5747–5759, Apr. 2017.

[32] R. S. Ganesan, T. Weber, and A. Klein, "Interference alignment in multi-user two way relay networks," in *Proc. IEEE Veh. Technol. Conf.*, Yokohama, Japan, May 2011, pp. 1–5.

[33] 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, Sep. 2010.

[34] R. Zhang, C. C. Chai, and Y. C. Liang, "Joint beamforming and power control for multiantenna relay broadcast channel with QoS constraints," *IEEE Trans. Signal Process.*, vol. 57, no. 2, pp. 726–737, Feb. 2009.

[35] A. Schrijver, *Theory of Linear and Integer Programming* (Discrete Mathematics and Optimization). Chichester, U.K.: Wiley, 1986.

[36] M. Grant and S. Boyd. (Mar. 2014). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: http://cvxr.com/cvx

DEEB TUBAIL received the B.S. degree (Hons.) in electrical engineering and the M.Sc. degree (Hons.) in telecommunication from the Islamic University of Gaza, Palestine, in 2009 and 2014, respectively. His research interests include two main fields in communication (microwave and wireless communication). In microwave field, he is interested in coupled resonators circuits and microwave devices areas. While in wireless communication, he is interested in the areas of physical-layer security, interference alignment, multiuser MIMO systems, and optimization.

MOHAMMED EL-ABSI received the B.E. degree in electrical engineering from the Islamic university of Gaza, Gaza, Palestine, in 2005, the M.S. degree in electrical engineering from the Jordan University of Science and Technology in 2008, and the Ph.D. degree *(summa cum laude)* in electrical engineering from the University of Duisburg-Essen, Duisburg, Germany, in 2015. He is currently a Mercator Fellow with the Digital Signal Processing Institute, University of Duisburg-Essen. His research interests include communication and signal processing. In the context of wireless communication, his interests include interference mitigation techniques in wireless networks, cooperative communications, MIMO systems, multicarrier communications, and cognitive radio. He received the German Academic Exchange Service Fellowship in 2006 and 2011.

SALAMA S. IKKI received the B.S. degree from Al-Isra University, Amman, Jordan, in 1996, the M.Sc. degree from the Arab Academy for Science and Technology and Maritime Transport, Alexandria, Egypt, in 2002, and the Ph.D. degree from the Memorial University of Newfoundland, St. Johns, in 2009, all in electrical engineering.

He was a Research Assistant with INRS, University of Quebec, Montreal, from 2010 to 2012, and a Post-Doctoral Fellow with the University of Waterloo, Waterloo, ON, Canada, from 2009 to 2010. He is currently an Associate Professor in wireless communications with the Department of Electrical Engineering, Lakehead University. He has been carrying out research in communications and signal processing for over 10 years. He is widely recognized as an expert in wireless communications. He has authored or co-authored over 100 papers in peer-reviewed IEEE international journals and conferences with over 3100 citations and has a current h-index of 28. He was a recipient of the Best Paper Award published in the *EURASIP Journal on Advances in Signal Processing* and the IEEE COMMUNICATION LETTERS, the IEEE WIRELESS COMMUNICATION LETTERS Exemplary Reviewer Certificate in 2012, and the Top Reviewer Certificate from the IEEE TRANSACTION ON VEHICULAR TECHNOLOGY in 2015. His Ph.D. student received the second place for Best Poster from the School of Electrical and Electronic Engineering, Newcastle University, U.K., Annual Research Conference, in 2014. He serves on the Editorial Board of the IEEE COMMUNICATION LETTERS and the *IET Communications Proceeding*.

WESSAM MESBAH (S'08–M'09) received the M.Sc. and B.Sc. degrees (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2003 and 2000, respectively, and the Ph.D. degree from McMaster University, Hamilton, ON, Canada, in 2008. From 2009 to 2010, he was a Post-Doctoral Fellow with Texas A&M University, Doha, Qatar. He joined the Electrical Engineering Department, King Fahd University of Petroleum and Minerals, in 2010, where he is currently an Associate Professor. His research interests include cooperative communications and relay channels, layered multimedia transmission, wireless sensor networks, multiuser MIMO/OFDM systems, cognitive radio, optimization, game theory, and smart grids.

THOMAS KAISER (M'98–SM'04) received the Diploma degree in electrical engineering from Ruhr-University Bochum, Bochum, Germany, in 1991, and the Ph.D. (Hons.) and German Habilitation degrees in electrical engineering from Gerhard Mercator University, Duisburg, Germany in 1995 and 2000, respectively. From 1995 to 1996, he spent a research leave with the University of Southern California, Los Angeles, which was grant-aided by the German Academic Exchange Service. From 2000 to 2001, he was the Head of the Department of Communication Systems, Gerhard Mercator University, and from 2001 to 2002, he was the Head of the Department of Wireless Chips and Systems, Fraunhofer Institute of Microelectronic Circuits and Systems, Duisburg. From 2002 to 2006, he was a Co-Leader of the Smart Antenna Research Team, University of Duisburg-Essen, Duisburg. He joined the Smart Antenna Research Group, Stanford University, Stanford, CA, USA, in 2005, and the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA, in 2007, as a Visiting Professor. From 2006 to 2011, he headed the Institute of Communication Technology, Leibniz University of Hannover, Germany. He is currently the Head of the Institute of Digital Signal Processing, University of Duisburg-Essen, and he is also the Founder and the CEO of ID4us GmbH, an RFID Centric Company. He is the author and co-author of over 300 papers in international journals and conference proceedings and two books *Ultra Wideband Systems with MIMO* (Wiley, 2010) and *Digital Signal Processing for RFID* (Wiley, 2015). He is the speaker of the Collaborative Research Center Mobile Material Characterization and Localization by Electromagnetic Sensing. He was the General Chair of the IEEE International Conference on UltraWideBand in 2008, the International Conference on Cognitive Radio Oriented Wireless Networks and Communications in 2009, the IEEE Workshop on Cellular Cognitive Systems in 2014, and the IEEE Workshop on Mobile THz Systems in 2018. He was the Founding Editor-in-Chief of the e-letter of the IEEE Signal Processing Society.