# Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming

Haijun Zhang, *Member, IEEE*, Hong Xing, *Student Member, IEEE*, Julian Cheng, *Senior Member, IEEE*, Arumugam Nallanathan, *Senior Member, IEEE*, and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*—We consider secure resource allocations for orthogonal frequency division multiple access (OFDMA) two-way relay wireless sensor networks (WSNs). The joint problem of subcarrier (SC) assignment, SC pairing and power allocations, is formulated under scenarios of using and not using cooperative jamming (CJ) to maximize the secrecy sum rate subject to limited power budget at the relay station (RS) and orthogonal SC allocation policies. The optimization problems are shown to be mixed integer programming and nonconvex. For the scenario without CJ, we propose an asymptotically optimal algorithm based on the dual decomposition method and a suboptimal algorithm with lower complexity. For the scenario with CJ, the resulting optimization problem is nonconvex, and we propose a heuristic algorithm based on alternating optimization. Finally, the proposed schemes are evaluated by simulations and compared with the existing schemes.**

***Index Terms*—Cooperative jamming (CJ), orthogonal frequency division multiple access (OFDMA), physical layer security, secure resource allocation, wireless sensor network (WSN).**

## I. Introduction

WIRELESS sensor networks (WSNs) play an important role in industrial monitoring and control [1], [2]. Relay node makes the WSN's transmission more reliable to satisfy the strict requirements in industrial applications [3]. In the case that data from two wireless sensors are forwarded in opposite directions, two-way relay networks, in which sources exchange information through one assisting relay based on the idea of network coding, can make the bidirectional transmission more efficient [4]. In orthogonal frequency division multiple access (OFDMA)-based two-way relay networks, channel gains of one subcarrier (SC) for one user[1] differ from the other user, and system capacity can be maximized by SC pairing, SC allocation and power allocation [5]. SC pairing means the pairing of SCs in the two phases of two-way relay network. SC assignment means the allocation of SC pairs to wireless sensor pairs. Power allocation means the power control of each SC pair.

In order to achieve the multiuser diversity, SC-pairing-based resource allocation has been investigated in two-way relay systems [6]–[8], which optimize resource allocation using the Lagrange dual decomposition method. In [6], both rate and power allocation with SC-user assignment were optimized based on the Lagrange dual decomposition method for a two-way relay network, while a multiuser system with a single relay was considered in [7]. SC-pairing-based power allocation, SC-pair assignment, and relay selection were jointly optimized in [8], where an asymptotically optimal algorithm was proposed based on a dual method.

Recently, physical layer security in terms of the secrecy capacity has drawn much attention due to the broadcast (BC) nature of wireless sensor communications [9], [10]. Compared to the traditional cryptography, physical layer security can strengthen secure transmission by taking full advantage of the additive nature of electromagnetic waves at low complexity [11]–[14].

Novel strategies have been explored to optimize secrecy capacity from either information-theoretic or signal processing approach. In [15], a resource allocation scheme was employed for OFDMA networks with coexistence of secure users and normal users, where the secure users have a minimum secrecy data rate requirement and the normal users are provided with best-effort services. Physical layer network coding (PNC) is an effective capacity boosting technique to improve throughput by embracing intrinsic interference in wireless channels [16]. In another popular scheme in the signal space of wiretap channel, cooperative jamming (CJ) was studied in [17] and [18].

Secure resource allocation and scheduling were investigated in half-duplex decode-and-forward (DF) relay assisted

Manuscript received April 11, 2015; revised August 05, 2015; accepted September 13, 2015. Date of publication October 12, 2015; date of current version October 31, 2016. This work was supported in part by the National Natural Science Foundation of China under Grant 61471025; in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2016D07, and in part by the Fundamental Research Funds for the Central Universities under Grant ZY1426. This paper was presented in part at the IEEE Global Communications Conference (Globecom 2012), Anaheim, CA, USA. Paper no. TII-15-0582.

H. Zhang is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: dr.haijun.zhang@ieee.org).

H. Xing and A. Nallanathan are with the Centre for Telecommunications, King's College London, London WC2R 2LS, U.K. (e-mail: hong.xing@kcl.ac.uk; nallanathan@ieee.org).

J. Cheng is with the School of Engineering, University of British Columbia, Kelowna, BC V1V 1V7, Canada (e-mail: julian.cheng@ubc.ca).

V. C. M. Leung is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: vleung@ece.ubc.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2015.2489610

[1]The terms "user" and "sensor" are used interchangeably in this paper.

OFDMA networks [19], with the objective of maximizing average secrecy outage capacity by using artificial noise (AN) to combat a passive eavesdropper. In [20], power allocation for secrecy capacity maximization was studied in DF relay systems with the presence of an eavesdropper. In [21], secure resource allocation was investigated in two-way relay network. However, to the best of the authors' knowledge, secure resource allocation jointly considering SC pairing, SC assignment and power allocation in two-way relay WSNs without and with CJ, has not been studied in the literature.

In this paper, we investigate the secure resource allocation problem for an OFDMA two-way relay WSN in the presence of an eavesdropper with and without CJ. For the scenario without CJ, the joint optimization of SC pairing, SC assignment and power allocation, at the relay node is formulated as a mixed integer programming problem, which is then solved using the dual method in an asymptotically optimal manner. To reduce the complexity of the proposed resource allocation algorithm, we also propose a suboptimal algorithm. For the scenario with CJ, the resulting optimization problem is nonconvex, and we propose a heuristic algorithm based on alternating optimization. Performance of the proposed schemes is verified by simulations.

This paper is organized as follows. Section II describes the system model without and with CJ. In Section III, the secure resource allocation scheme without jamming is proposed by jointly considering SC assignment, SC pairing and power allocation based on the dual decomposition method, and a new suboptimal low-complexity algorithm is proposed. In Section IV, we propose a suboptimal algorithm to solve the nonconvex optimization problem of secure resource allocation with CJ. In Section V evaluates performance of the proposed algorithms by simulations. Finally Section VI concludes this paper.

## II. System Model

### A. Secrecy Two-Way Relay WSNs Without CJ

We consider an OFDMA-based two-way relay WSN consisting of $M$ preassigned pairs of sensors, denoted by $\mathcal{M} = \{1, \ldots, M\}$. These sensors aim to exchange information through the assistance of a fixed relay station (RS) in the presence of an eavesdropper (Eve) over an OFDMA channel composed of $N$ SCs, denoted by $\mathcal{N} = \{1, \ldots, N\}$, each having a bandwidth $B$. As shown in Fig. 1, the system is composed of $M$ pairs of legitimate users. The only eavesdropper, denoted by $E$, is passive and attempts to overhear information from these wireless sensors. The RS operates in a half-duplex mode and relays the bidirectional traffic using the amplify-and-forward (AF) protocol, which is also known as analog network coding [22]. All wireless sensors, RS, and eavesdropper are assumed to be equipped with a single omni antenna.

The AF two-way relay wireless sensor transmission is divided into two phases: 1) the multiple access (MA) phase; and 2) the BC phase. In the MA phase, all wireless sensors transmit signals to the RS simultaneously; in the BC phase, the RS amplifies and broadcasts the received signals to wireless

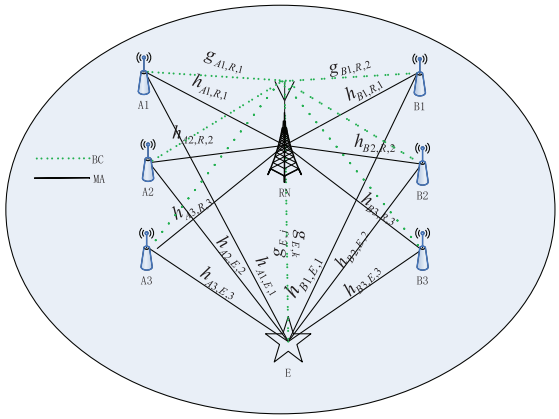


Fig. 1. System model of the security transmission in two-way relay sensor network.

sensors. In both phases, each SC is occupied by no more than one wireless sensor pair in order to avoid the cochannel interference, while each wireless sensor pair can occupy more than one SCs. The $m$th wireless sensor pair is composed of wireless sensor $A_m$ and wireless sensor $B_m$, where $m \in \mathcal{M}$.

We focus on the secure resource allocation including SC pairing, SC assignment together with power allocation in the two-way relay wireless sensor system under the assumption that global channel state information (CSI) is known [23], [15] at the cooperative helper, RS. The fading channel on each of the SCs is assumed to be flat and composed of distance-dependent path loss and small-scale fading. We consider a slow fading environment where all the channels are assumed to remain constant within the total transmission phase of our interest.

Assuming SC, $i$ is allocated to the $m$th wireless sensor pair in the MA phase, and the received signal at the RS on SC $i$ can be expressed as

$$y_{\mathrm{RS},i} = \sqrt{P_{A_m,i}} h_{A_m,R,i} s_{A_m,i} + \sqrt{P_{B_m,i}} h_{B_m,R,i} s_{B_m,i} + n_{\mathrm{RS},i} \tag{1}$$

where $i \in \mathcal{N}$; $s_{A_m,i}$ and $s_{B_m,i}$ are, respectively, the transmitted signals on SC $i$ from wireless sensors $A_m$ and $B_m$, and are assumed to be cyclic symmetric complex Gaussian (CSCG) random variables denoted by $s_{Am,i} \sim \mathcal{CN}(0,1)$ and $s_{Bm,i} \sim \mathcal{CN}(0,1)$, respectively; $P_{A_m}$ and $P_{B_m}$ are, respectively, the total transmit powers of $A_m$ and $B_m$ over all the available bandwidth; $h_{A_m,R,i}$ and $h_{B_m,R,i}$ are, respectively, the channel gains on SC $i$ from $A_m$ to RS and from $B_m$ to RS; and $n_{\mathrm{RS},i}$ is the additive white Gaussian noise (AWGN) with mean zero and variance $\sigma^2$ at the RS on SC $i$, and it is denoted by $n_{\mathrm{RS},i} \sim \mathcal{CN}(0, \sigma^2)$.

The received signal on SC $i$ at the eavesdropper is given by

$$y_{E,i} = \sqrt{P_{A_m,i}} h_{A_m,E,i} s_{A_m,i} + \sqrt{P_{B_m,i}} h_{B_m,E,i} s_{B_m,i} + n_{E,i} \tag{2}$$

where $h_{A_m,E,i}$ and $h_{B_m,E,i}$ are the channel gains on SC $i$ from $A_m$ to the eavesdropper and from $B_m$ to the eavesdropper, respectively; and $n_{E,i}$ is the AWGN at the eavesdropper on SC $i$, and it is denoted by $n_{E,i} \sim \mathcal{CN}(0, \sigma^2)$.

Assuming SC $j$ is allocated to the $m$th wireless sensor pair in the BC phase, the signal transmitted from the relay is

given by $\beta_{m,i}y_{\mathrm{RS},i}$ and it is transmitted with power $P_{R,j}$ on SC $j$, where $\beta_{m,i}$ is the amplifying coefficient, denoted by $\beta_{m,i}=\sqrt{P_{R,j}}/\alpha_{m,i}$, and where $\alpha_{m,i}$ is a normalized factor given by $\alpha_{m,i}=\sqrt{P_{A_m,i}|h_{A_m,R,i}|^2+P_{B_m,i}|h_{B_m,R,i}|^2+\sigma^2}$. We consider a total power constraint that limits the total transmit power at the RS over all SCs, i.e., $\sum_{j=1}^{N}P_{R,j}\le P_R$. The received signal at $A_m$ on SC $j$ in the BC phase is thus $y_{A_m,i,j}=\sqrt{P_{R,j}}g_{A_m,j}y_{\mathrm{RS},i}/\alpha_{m,i}+n_{A_m,j}$, which can be further expressed as

$$\begin{aligned}y_{A_m,i,j}=&\sqrt{P_{R,j}}g_{A_m,j}\sqrt{P_{A_m,i}}h_{A_m,R,i}s_{A_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{A_m,j}\sqrt{P_{B_m,i}}h_{B_m,R,i}s_{B_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{A_m,j}n_{\mathrm{RS},i}/\alpha_{m,i}+n_{A_m,j}.\end{aligned}\tag{3}$$

Similarly, the received signal at $B_m$ on SC $j$ is $y_{B_m,i,j}=\sqrt{P}_{R,j}g_{B_m,j}y_{\mathrm{RS},i}/\alpha_{m,i}+n_{B_m,j}$, which is further expressed as

$$\begin{aligned}y_{B_m,i,j}=&\sqrt{P_{R,j}}g_{B_m,j}\sqrt{P_{A_m,i}}h_{A_m,R,i}s_{A_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{B_m,j}\sqrt{P_{B_m,i}}h_{B_m,R,i}s_{B_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{B_m,j}n_{\mathrm{RS},i}/\alpha_{m,i}+n_{B_m,j}\end{aligned}\tag{4}$$

where $g_{A_m,j}$ and $g_{B_m,j}$ are the channel gains from the RS to the $m$th user pair $A_m$ and $B_m$ on SC $j$, respectively; and $n_{A_m,j}$ and $n_{B_m,j}$ are AWGNs on SC $j$ at $A_m$ and $B_m$, and they are denoted by $n_{A_m,j}\sim\mathcal{CN}(0,\sigma^2)$ and $n_{B_m,j}\sim\mathcal{CN}(0,\sigma^2)$, respectively.

The received signal on SC $j$ at the eavesdropper in the BC phase is given by

$$\begin{aligned}y_{E,i,j}=&\sqrt{P_{R,j}}g_{E,j}\sqrt{P_{A_m,i}}h_{A_m,R,i}s_{A_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{E,j}\sqrt{P_{B_m,i}}h_{B_m,R,i}s_{B_m,i}/\alpha_{m,i}\\&+\sqrt{P_{R,j}}g_{E,j}n_{\mathrm{RS},i}/\alpha_{m,i}+n_{E,j}\end{aligned}\tag{5}$$

where $g_{E,j}$ is the channel gain between the RS and the eavesdropper on SC $j$; and $n_{E,j}$ is the AWGN at the eavesdropper on SC $j$, and it is denoted by $n_{E,j}\sim\mathcal{CN}(0,\sigma^2)$.

The signal-to-noise ratios (SNRs) of wireless sensors $A_m$ and $B_m$, which share SC $i$ in the MA phase and SC $j$ in the BC phase, can be respectively written as

$$\mathrm{SNR}_{A_m,i,j}=\frac{P_{R,j}|g_{A_m,j}|^2P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_{m,i}^2}{(P_{R,j}|g_{A_m,j}|^2/\alpha_{m,i}^2+1)\sigma^2}\tag{6}$$

and

$$\mathrm{SNR}_{B_m,i,j}=\frac{P_{R,j}|g_{B_m,j}|^2P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_{m,i}^2}{(P_{R,j}|g_{B_m,j}|^2/\alpha_{m,i}^2+1)\sigma^2}.\tag{7}$$

Based on (2) and (5), the composite received signal over the two phases at the eavesdropper can be modeled as a 2-by-2 point-to-point multiple-input-multiple-output (MIMO) channel given by

$$\boldsymbol{y}_E=\boldsymbol{H}_E\boldsymbol{s}+\boldsymbol{n}_E\tag{8}$$

where

$$\boldsymbol{H}_E=\begin{bmatrix}\sqrt{P_{A_m,i}}h_{A_m,E,i} & \sqrt{P_{B_m,i}}h_{B_m,E,i}\\ \frac{\sqrt{P_{R,j}}g_{E,j}\sqrt{P_{A_m,i}}h_{A_m,R,i}}{\alpha_{m,i}} & \frac{\sqrt{P_{R,j}}g_{E,j}\sqrt{P_{B_m,i}}h_{B_m,R,i}}{\alpha_{m,i}}\end{bmatrix}\tag{9}$$

$$\boldsymbol{s}=\begin{bmatrix}s_{A_m,i}\\ s_{B_m,i}\end{bmatrix}\ \text{and}\ \boldsymbol{n}_E=\begin{bmatrix}n_{E,i}\\ \frac{\sqrt{P_{R,j}}g_{E,j}n_{\mathrm{RS},i}}{\alpha_{m,i}}+n_{E,j}\end{bmatrix}.\tag{10}$$

The instantaneous mutual information (IMI) rate for the wireless sensor $A_m$ and $B_m$ is given by

$$R_{A_m,i,j}=\frac{1}{2}B\log(1+\mathrm{SNR}_{A_m,i,j})\tag{11}$$

and

$$R_{B_m,i,j}=\frac{1}{2}B\log(1+\mathrm{SNR}_{B_m,i,j})\tag{12}$$

respectively.

For the eavesdropper, since (8) is equivalent to a 2-by-2 point-to-point MIMO system with transmit signals $\boldsymbol{s}=(s_{A_m,i},s_{B_m,i})^T$, which follows $\boldsymbol{s}\sim\mathcal{CN}(0,\boldsymbol{I})$, the maximum achievable rate between the source pairs $A_m$ and $B_m$, and the eavesdropper is given by [28, Chap.8]

$$R_{E,i,j}=\frac{1}{2}B\log\det\left(\boldsymbol{I}+\boldsymbol{H}_E\boldsymbol{H}_E^H\boldsymbol{Q}_E^{-1}\right)\tag{13}$$

where

$$\begin{aligned}\boldsymbol{Q}_E&=\mathbb{E}[\boldsymbol{n}_E\boldsymbol{n}_E^H]\\&=\sigma^2\begin{bmatrix}1 & 0\\ 0 & 1+P_{R,j}|g_{E,j}|^2/\alpha_{m,i}^2\end{bmatrix}.\end{aligned}\tag{14}$$

Note that $\mathbb{E}[\cdot]$ denotes the statistical average and the factor $\frac{1}{2}$ in (13) accounts for the two phases in a complete transmission slot. Since, $R_{E,i,j}$ is only achievable when the eavesdropper itself has full CSI of the legitimate users, i.e., $h_{A_m,R,i}$ and $h_{B_m,R,i}$. The achievable rate $R_{E,i,j}$ given in (13) is an upper-bound capacity for the eavesdropper. Accordingly, the worst-case secrecy sum rate for the $m$th wireless sensors over the SC pair $(i,j)$ is defined as [27]

$$R_{\mathrm{sec},m,i,j}=[R_{A_m,i,j}+R_{B_m,i,j}-R_{E,i,j}]^+\tag{15}$$

where $[x]^+=\max\{0,x\}$.

### B. Secrecy Two-Way Relay WSNs With CJ

We consider a similar problem to that described in Section II-A with CJ. CSIs related to wireless sensors and the RS as well as those of the eavesdropper are also assumed to be known at the RS.

In the MA phase, $A_m$ and $B_m$ transmit messages for exchange, i.e., $s_{A_m,i}$ and $s_{B_m,i}$ by simultaneously incorporating jamming signals denoted as $s'_{A_m,i}$ and $s'_{B_m,i}$, respectively. Specifically, $A_m$ splits its transmit power on SC $i$ into $(1-\alpha_{1,i})P_{A_m,i}$ for the exchange message $s_{A_m,i}$, and $\alpha_{1,i}P_{A_m,i}$ for

the jamming signal, i.e., AN, $s'_{A_m,i}$, respectively. $\alpha_{1,i}$ is the factor denoting the portion of the transmit power used for generating AN at $A_m$ on SC $i$. Similar transmission scheme is used for $B_m$, and the associated portion factor indicating the amount of power used for generating AN at $B_m$ on SC $i$ is denoted as $\alpha_{2,i}$. The received signal at the RS is thus given by

$$\begin{aligned} y_{\mathrm{RS},i} = &\sqrt{(1-\alpha_{1,i})P_{A_m,i}}h_{A_m,R,i}s_{A_m,i} \\ &+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}}h_{B_m,R,i}s_{B_m,i} \\ &+ \sqrt{\alpha_{1,i}P_{A_m,i}}h_{A_m,R,i}s'_{A_m,i} \\ &+ \sqrt{\alpha_{2,i}P_{B_m,i}}h_{B_m,R,i}s'_{B_m,i} + n_{\mathrm{RS},i}. \end{aligned} \tag{16}$$

For the eavesdropper, it receives a mixed signal on SC $i$ expressed as

$$\begin{aligned} y_E^{(1)} = &\sqrt{(1-\alpha_{1,i})P_{A_m,i}}h_{A_m,E,i}s_{A_m,i} \\ &+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}}h_{B_m,E,i}s_{B_m,i} \\ &+ \sqrt{\alpha_{1,i}P_{A_m,i}}h_{A_m,E,i}s'_{A_m,i} \\ &+ \sqrt{\alpha_{2,i}P_{B_m,i}}h_{B_m,E,i}s'_{B_m,i} + n_{E,i}. \end{aligned} \tag{17}$$

In this work, it is assumed that the AN signals $s'_{A_m,i}$ and $s'_{B_m,i}$ are perfectly known to the RS prior to transmission via certain higher layer cryptographic protocols, and as a result, at the RS, both $\sqrt{\alpha_{1,i}P_{A_m,i}}h_{A_m,R,i}s'_{A_m,i}$ and $\sqrt{\alpha_{2,i}P_{B_m,i}}h_{B_m,R,i}s'_{B_m,i}$ in (16) can be canceled [29], [30]. Thus, only $s_{A_m,i}$ and $s_{B_m,i}$ are broadcasted on SC $j$ in the successive BC phase. Then, by means of analog network coding, $A_m$ will be able to subtract $s_{A_m}$ from the BC signal and obtain $s_{B_m}$ as it desires, so will $B_m$. However, since ANs are kept strictly confidential to the eavesdropper, it suffers from large interference caused by ANs and/or analog network coded signals containing both $s_{A_m}$ and $s_{B_m}$. Assuming the RS works in AF mode, it transmits the remaining signal after canceling $s'_{A_m,i}$ and $s'_{B_m,i}$, i.e., $y'_{Rs,i}$, which is given by

$$\begin{aligned} y'_{\mathrm{RS},i} = &\sqrt{(1-\alpha_{1,i})P_{A_m,i}}h_{A_m,R,i}s_{A_m,i} \\ &+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}}h_{B_m,R,i}s_{B_m,i} + n_{\mathrm{RS},i} \end{aligned} \tag{18}$$

with an amplifying coefficient denoted by $\beta_{m,i} = \sqrt{P_{R,j}}/\gamma_{m,i}$ where

$$\gamma_{m,i} = \sqrt{(1-\alpha_{1,i})P_{A_m,i}|h_{A_m,R,i}|^2+(1-\alpha_{2,i})P_{Bm,i}|h_{B_m,R,i}|^2+\sigma^2}.$$

The parameter $\gamma_{m,i}$ can be seen as a normalized factor for the forwarded signal, and thus $P_{R,j}$ denotes the transmit power of the RS on SC $j$ in the BC phase. Hence, the received signal at the $A_m$ is given by

$$y_{A_m,i,j} = \beta_{m,i}g_{R,A_m,j}y'_{\mathrm{RS},i} + n_{A_m,j}. \tag{19}$$

Note that since $A_m$ can successfully cancel its previously transmitted $s_{A_m,i}$ at its receiver, we can further simplify the received signal at the $A_m$ by substituting $\beta_{m,i}$ and $y'_{\mathrm{RS},i}$ into (19)

$$\begin{aligned} y_{A_m,i,j} = &\sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{R,A_m,j}s_{B_m,i}/\gamma_{m,i} \\ &+ \sqrt{P_{R,j}}g_{R,A_m,j}n_{\mathrm{RS},i}/\gamma_{m,i} + n_{A_m,j}. \end{aligned} \tag{20}$$

Similarly, the received signal at the $B_m$ is given by

$$\begin{aligned} y_{B_m,i,j} = &\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{R,B_m,j}s_{A_m,i}/\gamma_{m,i} \\ &+ \sqrt{P_{R,j}}g_{R,B_m,j}n_{\mathrm{RS},i}/\gamma_{m,i} + n_{B_m,j}. \end{aligned} \tag{21}$$

For the eavesdropper, since it does not know either $s_{A_m,i}$ or $s_{B_m,i}$, it receives a combined signal of $s_{A_m,i}$ and $s_{B_m,i}$, which is expressed as

$$\begin{aligned} y_E^{(2)} = &\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{R,E,j}s_{A_m,i}/\gamma_{m,i} \\ &+ \sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{R,E,j}s_{B_m,i}/\gamma_{m,i} \\ &+ \sqrt{P_{R,j}}g_{R,E,j}n_{\mathrm{RS},i}/\gamma_{m,i} + n_{E,j}. \end{aligned} \tag{22}$$

From (17) and (22), we can combine the received signals at the eavesdropper during the two phases in one transmit slot into an equivalent point-to-point 2-by-2 MIMO channel as

$$\boldsymbol{y}_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix} = \begin{bmatrix} \tilde{h}_{11} & \tilde{h}_{12} \\ \tilde{h}_{21} & \tilde{h}_{22} \end{bmatrix} \begin{bmatrix} s_{A_m,i} \\ s_{B_m,i} \end{bmatrix} + \begin{bmatrix} \tilde{n}_1 \\ \tilde{n}_2 \end{bmatrix} \tag{23}$$

where $\tilde{h}_{11}=\sqrt{(1-\alpha_{1,i})P_{A_m,i}}h_{A_m,E,i}$, $\tilde{h}_{12}=\sqrt{(1-\alpha_{2,i})P_{B_m,i}}h_{B_m,E,i}$, $\tilde{h}_{21}=\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{R,E,j}$, and $\tilde{h}_{22}=\sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{R,E,j}$. For convenience, we denote the equivalent channel matrix from the wireless sensor pairs to the eavesdropper over the SC pair $(i,j)$

$$\tilde{\boldsymbol{H}}_{\boldsymbol{E,m,i,j}} = \begin{bmatrix} \tilde{h}_{11} & \tilde{h}_{12} \\ \tilde{h}_{21} & \tilde{h}_{22} \end{bmatrix}. \tag{24}$$

In (23), $\tilde{n}_1$ denotes the equivalent received noise at the eavesdropper treating the AN generated by the wireless sensor pair as noise in the MA phase, which is given by

$$\begin{aligned} \tilde{n}_1 = &\sqrt{\alpha_{1,i}P_{A_m,i}}h_{A_m,E,i}s'_{A_m,i} \\ &+ \sqrt{\alpha_{2,i}P_{B_m,i}}h_{B_m,E,i}s'_{B_m,i} + n_{E,i}. \end{aligned} \tag{25}$$

Similarly, $\tilde{n}_2$ denotes the amplified noise introduced by the RS as well as the additive noise received by the eavesdropper in BC phase, and it is given as

$$\tilde{n}_2 = \sqrt{P_{R,j}}g_{R,E,j}n_{\mathrm{RS},i}/\gamma_{m,i} + n_{E,j}. \tag{26}$$

The associated covariance matrix for this equivalent noise at the eavesdropper can thus be derived as

$$\begin{aligned} \tilde{\boldsymbol{Q}}_{\boldsymbol{E,m,i,j}} &= \mathbb{E}\left[(\tilde{n}_1\ \tilde{n}_2)^H(\tilde{n}_1\ \tilde{n}_2)\right] \\ &= \mathrm{diag}\left(\alpha_{1,i}P_{A_m,i}|h_{A_m,E,i}|^2\right. \\ &\quad + \alpha_{2,i}P_{B_m,i}|h_{B_m,E,i}|^2 \\ &\quad \left. + \sigma^2, \left(P_{R,j}|g_{R,E,j}|^2/\gamma_{m,i}^2+1\right)\sigma^2\right). \end{aligned} \tag{27}$$

Besides, according to the received signal at $A_m$ and $B_m$ given by (20) and (21), the SNRs of wireless sensors $A_m$ and $B_m$, which share SC $i$ in the MA phase and SC $j$ in the BC phase, can be respectively expressed as

$$\mathrm{SNR}'_{A_m,i,j} = \frac{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,A_m,j}|^2|h_{B_m,R,i}|^2/\gamma^2_{m,i}}{\left(P_{R,j}|g_{R,A_m,j}|^2/\gamma^2_{m,i}+1\right)\sigma^2} \tag{28}$$

and

$$\mathrm{SNR}'_{B_m,i,j} = \frac{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,B_m,j}|^2|h_{A_m,R,i}|^2/\gamma^2_{m,i}}{\left(P_{R,j}|g_{R,B_m,j}|^2/\gamma^2_{m,i}+1\right)\sigma^2}. \tag{29}$$

Similar to Section II-A without using CJ, the IMI rate for the wireless sensor $A_m$ and $B_m$ is given by

$$\tilde{R}_{A_m,i,j} = \frac{1}{2}B\log_2(1+\mathrm{SNR}'_{A_m,i,j}) \tag{30}$$

and

$$\tilde{R}_{B_m,i,j} = \frac{1}{2}B\log_2(1+\mathrm{SNR}'_{B_m,i,j}) \tag{31}$$

respectively.

For the eavesdropper, since (23) is equivalent to a 2-by-2 point-to-point MIMO system with white transmission covariance denoted by $\boldsymbol{s}\sim\mathcal{CN}(0,\boldsymbol{I})$, where $\boldsymbol{s}=(s_{A_m,i},s_{B_m,i})^T$, the maximum achievable rate at the Eve is thus given by [28, Chap. 8]

$$\tilde{R}_{E,i,j} = \frac{1}{2}B\log_2\det\left(\boldsymbol{I}+\tilde{\boldsymbol{H}}_{\boldsymbol{E},\boldsymbol{m},\boldsymbol{i},\boldsymbol{j}}\tilde{\boldsymbol{H}}^{\boldsymbol{H}}_{\boldsymbol{E},\boldsymbol{m},\boldsymbol{i},\boldsymbol{j}}\tilde{\boldsymbol{Q}}^{-\mathbf{1}}_{\boldsymbol{E},\boldsymbol{m},\boldsymbol{i},\boldsymbol{j}}\right). \tag{32}$$

Accordingly, the worst-case secrecy sum rate using the scheme of CJ for the $m$th wireless sensor pair over the SC pair $(i,j)$ can be expressed as [27]

$$\tilde{R}_{\mathrm{sec},m,i,j} = \left[\tilde{R}_{A_m,i,j}+\tilde{R}_{B_m,i,j}-\tilde{R}_{E,i,j}\right]^+. \tag{33}$$

## III. Secure Resource Allocation Without CJ

### A. Proposed Problem Without CJ

Our target is to maximize the total secrecy sum rate of the $M$ wireless sensor pairs by optimizing the SC pairing, SC assignment and power allocations, for the relay over different SCs. This optimization problem can thus be formulated as

$$(\mathrm{P1}): \underset{\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P}}{\text{maximize}} \sum_{m=1}^{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\pi_{(i,j)}\rho_{m,(i,j)}R_{\mathrm{sec},m,i,j} \tag{34}$$

$$\text{subject to } C1: \sum_{j=1}^{N}P_{R,j}\le P_R, \quad C2: P_{R,j}\ge 0 \quad \forall j$$

$$C3: \sum_{j=1}^{N}\pi_{(i,j)}\le 1 \quad \forall i, \quad C4: \sum_{i=1}^{N}\pi_{(i,j)}\le 1 \quad \forall j$$

$$C5: \sum_{m=1}^{M}\rho_{m,(i,j)}\le 1 \quad \forall (i,j)$$

$$C6: \pi_{(i,j)},\rho_{m,(i,j)}\in\{0,1\} \quad \forall m,i,j \tag{35}$$

where $\boldsymbol{\pi}=\{\pi_{(i,j)}\}$, $\boldsymbol{\rho}=\{\rho_{m,(i,j)}\}$, $\boldsymbol{P}=\{P_{R,j}\}$ for $m\in\mathcal{M}$, $i,j\in\mathcal{N}$. In order to ensure that each SC pair $(i,j)$ is assigned to no more than one wireless sensor pair, we define the indicator of SC allocation as $\rho_{m,(i,j)}\in\{0,1\}$, where $\rho_{m,(i,j)}=1$ if the $m$th wireless sensor pair occupies SC $i$ in the MA phase and SC $j$ in the BC phase; and $\rho_{m,(i,j)}=0$, otherwise. Denote $\pi_{(i,j)}$ as the SC pairing variable such that $\pi_{(i,j)}=1$ if SC $i$ in the MA phase is paired with SC $j$ in the BC phase, and $\pi_{(i,j)}=0$, otherwise. Constraint $C1$ limits the total transmit power of the RS over all SCs; $C2$ represents the non-negative power constraint on each SC; $C3$ and $C4$ guarantee that each SC is paired with no more than one other SC; $C5$ guarantees that each paired SCs can be assigned to at most one wireless sensor pair; and $C6$ indicates the integer property of $\pi_{(i,j)}$ and $\rho_{m,(i,j)}$.

The optimization problem defined in (34) under the constraints given in (35) is a nonconvex integer-mixed optimization problem. According to [24], the duality gap between the primal problem and the dual problem approaches zero when the number of SCs is sufficiently large. In this section, we propose both near optimal and suboptimal schemes to solve the joint SC pairing, SC assignment and power allocations problem for the secrecy transmission in the OFDMA two-way relay WSNs using the Lagrange dual decomposition method [25], [26].

### B. Near Optimal Algorithm to (P1)

The Lagrangian of (P1) is given by

$$L(\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P},\lambda) = \sum_{m=1}^{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\pi_{(i,j)}\rho_{m,(i,j)}R_{\mathrm{sec},m,i,j} + \lambda\left(P_R-\sum_{j=1}^{N}P_{R,j}\right)\Bigg|\sum_{j=1}^{N}\pi_{(i,j)}\le 1 \quad \forall i,$$
$$\sum_{i=1}^{N}\pi_{(i,j)}\le 1 \quad \forall j, \sum_{m=1}^{M}\rho_{m,(i,j)}\le 1 \quad \forall (i,j). \tag{36}$$

In (36), $\lambda$ is the Lagrange multiplier (also called the dual variable) for the constraints $C1$ in (35) under the boundary constraints of $C3\sim C6$ in (35). Accordingly, the Lagrange dual function is defined as

$$g(\lambda) = \underset{\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P}}{\text{maximize}}\, L(\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P},\lambda). \tag{37}$$

The dual problem can be expressed as

$$\underset{\lambda}{\text{minimize}}\ g(\lambda) \tag{38}$$

$$\text{subject to } \lambda\ge 0. \tag{39}$$

We decompose the Lagrangian of (P1) in (36) into one master problem and $N$ subproblems with each of them corresponding to a different SC $j$. Therefore, the Lagrangian in (36) is rewritten as

$$L(\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P},\lambda)=\sum_{j=1}^{N}L_j(P_{R,j},\pi_{(i,j)},\rho_{m,(i,j)},\lambda)+\lambda P_R\left|\sum_{j=1}^{N}\pi_{(i,j)}\le 1\quad\forall i,\sum_{i=1}^{N}\pi_{(i,j)}\le 1\quad\forall j,\sum_{m=1}^{M}\rho_{m,(i,j)}\le 1\quad\forall(i,j)\right. \tag{40}$$

and the associated subproblem can be formulated as

$$\begin{aligned}\underset{\pi(i,j),\rho_{m,(i,j)},P_{R,j}}{\text{maximize}}\ &\sum_{m=1}^{M}\sum_{i=1}^{N}\pi_{(i,j)}\rho_{m,(i,j)}R_{\text{sec},m,i,j}-\lambda P_{R,j}\\ \text{subject to}\ &\sum_{i=1}^{N}\pi_{(i,j)}\le 1,\quad\sum_{m=1}^{M}\rho_{m,(i,j)}\le 1,\\ &P_{R,j}\le P_R.\end{aligned} \tag{41}$$

Since $L_j(P_{R,j},\pi(i,j),\rho_{m,(i,j)},\lambda)$ is an integer-mixed function and nonconcave over $P_{R,j}$, it cannot be solved directly. In the remaining of this section, we propose to jointly optimize $P_{R,j}$, $\pi(i,j)$, and $\rho_{m,(i,j)}$ given $\lambda$.

First, providing that the SC-pairing indicator $\pi_{(i,j)}$ and the SC assignment indicator $\rho_{m,(i,j)}$ are given as $\check{\pi}_{(i,j)}$ and $\check{\rho}_{m,(i,j)}$, respectively, the objective is thus to maximize $L_j(p_{R,j},\check{\pi}(i,j),\check{\rho}_{m,(i,j)},\lambda)$ over $P_{R,j}$. Since, $L_j(p_{R,j},\check{\pi}(i,j),\check{\rho}_{m,(i,j)},\lambda)$ over $P_{R,j}$ is still not concave over $P_{R,j}$ but a continuous function over one single variable $P_{R,j}$. We deploy the function fmincon in MATLAB as $[P^*_{R,j},\text{fval},\text{exitflag},\text{output}]=\text{fmincon}(L_j,P^{(0)}_{R,j},[],[],[],[],0,P_R)$,[2] in which $P^*_{R,j}$ denotes the near optimal solution and fval the corresponding near optimal value, to solve the following problem:

$$\underset{P_{R,j}}{\text{maximize}}\ L_j(p_{R,j},\check{\pi}(i,j),\check{\rho}_{m,(i,j)},\lambda) \tag{42}$$

$$\text{subject to}\quad P_{R,j}\ge 0. \tag{43}$$

Next, we focus on finding the near optimal SC pairing for (41). The SC pairing problem can be equivalently transformed into an assignment problem and then solved by the classic Hungarian algorithm, where the assignment matrix consists of $N\times N$ elements, with their index corresponding to the SC pair occupied during the phase of MA and BC, respectively, and with each entry a cost function given by

$$c(\pi(i,j),\lambda)=R_{\text{sec},\check{m},i,j}-\lambda\check{P}_{R,j} \tag{44}$$

where $\check{P}_{R,j}$ is given by the solution to (42) providing that $\pi(i,j)=1$, $\rho_{\check{m},(i,j)}=1$, and $\check{m}=\arg\max_m R_{\text{sec},m,i,j}-\lambda\check{P}_{R,j}$. After filling in all entries, we denote the obtained near optimal SC pairing policies via the Hungarian algorithm as $\boldsymbol{\pi}^*$.

At last, given the near optimal SC paring policies $\boldsymbol{\pi}^*$, the optimum SC assignment for each pair of wireless sensors can be simultaneously given as

$$\check{\rho}_{m,(i,j)}=\begin{cases}1, & \text{for } m=\check{m}\quad\forall(i,j)\in\boldsymbol{\pi}^*\\ 0, & \text{otherwise.}\end{cases} \tag{45}$$

We denote the near optimal SC assignment as $\boldsymbol{\rho}^*$. Note that $P^*_{R,j}$ is already given when calculating (44).

Hence, given $\lambda$, we can solve the corresponding $P^*_{R,j}$, $\boldsymbol{\pi}^*$, and $\boldsymbol{\rho}^*$ jointly for all $j$. Problem (P1) is then iteratively solved by updating $\lambda$ via a bisection method [25] given in Algorithm 1. The required subgradient for updating $\lambda$ can be shown to be $P_R-\sum_{j=1}^{N}P^*_{R,j}$ [cf.,(36)].

**Algorithm 1.** Proposed Algorithm to Solve (P1)

1: Initialize $i=0$, $\lambda^{(i)}_{\text{low}}=\lambda_{\min}$, $\lambda^{(i)}_{\text{up}}=\lambda_{\max}$;
2: **repeat**
3: Update $\lambda^{(i+1)}=(\lambda^{(i)}_{\text{low}}+\lambda^{(i)}_{\text{up}})/2$;
4: $i=i+1$;
5: Given $\lambda^{(i)}$, update $\{P^{*(i)}_{R,j}\}$, $\{\boldsymbol{\pi}^{*(i)}\}$ and $\{\boldsymbol{\rho}^{*(i)}\}$ based on (44) and (45);
6: Calculate the required sub-gradient: $subg^{(i)}=P_{\text{R}}-\sum_{j=1}^{N}P^{*(i)}_{R,j}$;
- if $subg^{(i)}\ge 0$, $\lambda^{(i)}_{\text{up}}=\lambda^{(i)}$,
- otherwise, $\lambda^{(i)}_{\text{low}}=\lambda^{(i)}$;

7: **until** $|g(\lambda^{(i)})-g(\lambda^{(i-1)})|<\epsilon$, where $\epsilon$ is a small positive number that controls the algorithm accuracy.

### C. Suboptimal Algorithm to (P1)

Section III-B gives a near optimal resource allocation algorithm, the complexity of which may will still be high with large values of $M$ and $N$. In this section, we propose a suboptimal algorithm to reduce the computational complexity by decomposing the joint optimization into three subproblems.

1) *SC assignment for given power allocation and SC pairing*: We first allocate the power equally among all SCs, assuming the SC pairing as $\pi_{(i,i)}=1,\pi_{(i,j)}=0,\forall i\ne j$, i.e., the same SC is allocated to both MA and BC phases. Then, the SC pairing $\pi_{(i,i)}$ is allocated to wireless sensor $m$ according to

$$\hat{m}=\arg\max_m R_{\text{sec},m,i,i}\quad\forall i \tag{46}$$

i.e., $\rho_{\hat{m},(i,i)}=1$. Then, the SCs occupied by wireless sensor $\hat{m}$ are denoted by the set $\mathcal{S}_m=\{i|\rho_{m,(i,i)}=1\}$, $\forall m\in\mathcal{M}$.

2) The SC pairing schemes given equal power allocations over all SCs, and the obtained $\mathcal{S}_m$s are given by Algorithm 2. Since the SC pairing is not jointly optimized, it can be easily found that Algorithm 2 is suboptimal.

[2]Function "fmincon" is called in the syntax of: [x,fval,exitflag,output] = fmincon(fun,x0,A,b,Aeq,beq,lb,ub) (cf., doc "fmincon" in MATLAB R2011b).

**Algorithm 2.** Suboptimal SC Pairing Algorithm for (P1)

1: Initialize $k=0$, $j^{(k)}=\emptyset$;
2: $\forall m \in \mathcal{M}$, $\tilde{\mathcal{S}_m}=\mathcal{S}_m$,
3: **repeat**
4: **Set** $k=k+1$; if $\mathcal{S}_m \neq \emptyset$, randomly select an $\hat{i} \in \tilde{\mathcal{S}_m}$, and choose
- $\hat{j}^{(k)}=\arg\max_{j\in\mathcal{S}_m} R_{\text{sec},m,\hat{i},j}$;

5: $\tilde{\mathcal{S}_m}=\tilde{\mathcal{S}_m}\setminus\{\hat{i}\}$, $\mathcal{S}_m=\mathcal{S}_m\setminus\{\hat{j}^{(k)}\}$;
6: **until** $\mathcal{S}_m$ (or $\tilde{\mathcal{S}_m}$) $=\emptyset$.

3) Given the SC assignment and the SC pairing schemes as stated in 1) and 2), the optimal power allocations can be obtained via calling the function fmincon as described in Section III-B.

The problem (P1) is thus solved iteratively by the same updating subgradient as stated in Section III-B via the bisection method [25].

### D. Complexity Analysis

The total complexity of the proposed optimal algorithm is $O(Y(ZMN^2+N^3))$, where $Y=\log_2(\frac{\lambda_{\max}-\lambda_{\min}}{\varepsilon})$ is the number of iterations for implementing bisection method given in Algorithm 1; $Z$ is the complexity for the numerical solver called by fmincon; $ZMN^2$ is the number of arithmetic operations required to attain all the entries of the Hungarian assignment matrix, i.e., $\{c(\pi(i,j),\lambda)\}_{i,j}$ $\forall i\in\mathcal{N}$, $\forall j\in\mathcal{N}$; and $N^3$ is the complexity for the classical Hungarian algorithm with $N$ tasks and $N$ workers. The proposed optimal scheme thus has a much lower complexity than the exhaustive search, which has a complexity of $O(Y(2^N-1)^M N!Z)$.

Similar analysis can be performed for the proposed suboptimal algorithm, and the complexity of which is $O(Y(MN+\sum_{m=1}^{M}\frac{|\mathcal{S}_m|^2}{2}+Z))$, which is even lower than the proposed optimal algorithm.

## IV. Secure Resource Allocation With CJ

### A. Proposed Problem With CJ

For the same problem with CJ, the objective function and constraints of the proposed resource allocation optimization can be modified as

$$(\text{P1-general}):$$

$$\underset{\tilde{\boldsymbol{\pi}},\tilde{\boldsymbol{\rho}},\tilde{\boldsymbol{P}},\{\alpha_{1,i}\},\{\alpha_{2,i}\}}{\text{maximize}} \sum_{m=1}^{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\tilde{\pi}_{(i,j)}\tilde{\rho}_{m,(i,j)}\tilde{R}_{\text{sec},m,i,j} \tag{47}$$

$$\text{subject to } C1:\sum_{j=1}^{N}\tilde{P}_{R,j}\le P_{\text{R}},\quad C2:\tilde{P}_{R,j}\ge 0\quad\forall j$$

$$C3:\sum_{j=1}^{N}\tilde{\pi}_{(i,j)}\le 1\quad\forall i,\quad C4:\sum_{i=1}^{N}\tilde{\pi}_{(i,j)}\le 1\quad\forall j$$

$$C5:\sum_{m=1}^{M}\tilde{\rho}_{m,(i,j)}\le 1\quad\forall(i,j)$$

$$C6:\tilde{\pi}_{(i,j)},\tilde{\rho}_{m,(i,j)}\in\{0,1\}\quad\forall m,i,j$$

$$C7:0\le\alpha_{1,i}\le 1,\ 0\le\alpha_{2,i}\le 1\quad\forall i \tag{48}$$

where $\tilde{\boldsymbol{\pi}}=\{\tilde{\pi}_{(i,j)}\}$, $\tilde{\boldsymbol{\rho}}=\{\tilde{\rho}_{m,(i,j)}\}$, $\tilde{\boldsymbol{P}}=\{\tilde{P}_{R,j}\}$ for $m\in\mathcal{M}$, $i,j\in\mathcal{N}$ are of the same meaning as those for problem (P1) but with different notations to represent variables of SC and power allocations for the new problem with the scheme of CJ. Constraints $C3\sim C6$ have the same meaning as those of (35); $C7$ is the range constraint for variables denoting portions of the total transmit power allocated for AN at $A_m$ and $B_m$, respectively.

Similar to the secure resource allocation problem (P1) without CJ, the optimization problem (P1-general) is not a convex problem either since $\tilde{R}_{\text{sec},m,i,j}$ is not concave over $\alpha_{k,i}$ and/or $\tilde{P}_{R,j}$, $\forall i,j\in\mathcal{N}$ and $k\in\{1,2\}$. The relationship between (P1-general) and (P1) can be seen as follows. When $\alpha_{1,i}=0$, $\alpha_{2,i}=0$, problem (P1-general) reduces to problem (P1). It is easy to verify that, with $\alpha_{1,i}=0$, $\alpha_{2,i}=0$, $\text{SNR}'_{A_m,i,j}$ and $\text{SNR}'_{B_m,i,j}$ in (28) and (29) can be simplified into $\text{SNR}_{A_m,i,j}$ and $\text{SNR}_{B_m,i,j}$ in (6) and (7), respectively. In addition, (24) and (27) also reduce to (9) and (14), respectively. Therefore, problem (P1-general) with CJ is a general case of problem (P1).

### B. Proposed Suboptimal Algorithm to (P1-General)

Similar to (P1), (P1-general) can be decomposed into parallel subproblems for each SC. The subproblem for SC $j$ is

$$\underset{\pi(i,j),\rho_{m,(i,j)},\alpha_{1,i},\alpha_{2,i},P_{R,j}}{\text{maximize}} \sum_{m=1}^{M}\sum_{i=1}^{N}\tilde{\pi}_{(i,j)}\tilde{\rho}_{m,(i,j)}\tilde{R}_{\text{sec},m,i,j}-\lambda P_{R,j}$$

$$\text{subject to}\sum_{i=1}^{N}\pi_{(i,j)}\le 1,\ \sum_{m=1}^{M}\rho_{m,(i,j)}\le 1,$$

$$0\le\alpha_{1,i}\le 1,\ 0\le\alpha_{2,i}\le 1,$$

$$P_{R,j}\le P_{\text{R}}. \tag{49}$$

Since (49) is an integer-mixed function and nonconcave over $P_{R,j}$ and/or $\alpha_{k,i}$, $k\in\{1,2\}$, (P1-general) is challenging to solve in general, and thus we propose to solve it via alternating optimization over $\alpha_{k,i}$, $\forall k\in\{1,2\}$, $\forall i\in\mathcal{N}$. Substitute the optimal $\boldsymbol{\pi}^*$, $\boldsymbol{\rho}^*$, and $\boldsymbol{P}^*$ to problem (P1) into (P1-general). Then, for each $j$, since the corresponding $i$ is already given as $\hat{i}=\arg\pi^*(i,j)$, (49) can be simplified into

$$\underset{0\le\alpha_{1,\hat{i}}\le 1,0\le\alpha_{2,\hat{i}}\le 1}{\text{maximize}}\ \tilde{R}_{\text{sec},m,\hat{i},j}. \tag{50}$$

However, since (50) is still not a convex problem due to its nonconcavity over $\alpha_{1,\hat{i}}$ and/or $\alpha_{2,\hat{i}}$, we first fix $\alpha_{1,\hat{i}}=\bar{\alpha}_{1,\hat{i}}$ and optimize $\alpha_{2,\hat{i}}$ by solving the following problem:

$$(\text{P1}-\text{general}-\text{sub1}):\ \underset{0\le\alpha_{2,\hat{i}}\le 1}{\text{maximize}}\ \tilde{R}_{\text{sec},m,\hat{i},j}$$

$$\text{subject to } 0\le\alpha_{2,\hat{i}}\le 1.$$

Let the optimal solution to (P2-general-sub1) be denoted by $\bar{\alpha}_{2,\hat{i}}$, we optimize $\alpha_{1,\hat{i}}$, by fixing $\alpha_{2,\hat{i}} = \bar{\alpha}_{2,\hat{i}}$ and solve a symmetric problem as follows:

$$(\mathrm{P1-general-sub2}): \underset{0\le\alpha_{1,\hat{i}}\le 1}{\text{maximize}} \ \tilde{R}_{\mathrm{sec},m,\hat{i},j} \quad \text{subject to } 0 \le \alpha_{1,\hat{i}} \le 1.$$

Problem (P1-general-sub1), despite of nonconvexity, can be easily solved via a one-dimensional (1-D) search over $\alpha_{2,\hat{i}} \in [0,1]$. Similar method can be applied to solving (P1-general-sub2).

Since alternatively solving (P1-general-sub1) and (P2-general-sub2) guarantees that the secrecy sum rate $\tilde{R}_{\mathrm{sec},m,\hat{i},j}$ in (50) is nondecreasing after each iteration, it at least converges to a local optimum solution to (50). Together with $\pi^*(i,j)$, $\rho^*_{m,(i,j)}$, and $P^*_{R,j}$, we find a suboptimal solution to (50). Moreover, as $\alpha_{1,\hat{i}}$ and $\alpha_{2,\hat{i}}$ are independent over $i$s, problem (P1-general) can finally be solved state by state over all $j$s. (Note that $i$s and $j$s compose a one-to-one correspondence after implementing Algorithm 1 in Section III-B.) Next, denote the optimal power portion factors for generating AN given $\boldsymbol{\pi}^*$, $\boldsymbol{\rho}^*$, and $\boldsymbol{P}^*$ as $\alpha^*_{1,i}$s and $\alpha^*_{2,i}$s, we further optimize (P1-general) by fixing $\alpha^*_{1,i}$s and $\alpha^*_{2,i}$s as follows.

By decomposing (P1-general) into parallel subproblems, each for one SC $j$ $(j \in \mathcal{N})$, the modified subproblem for (P1-general) can be expressed as

$$\begin{aligned}\underset{\tilde{\pi}(i,j),\tilde{\rho}_{m,(i,j)},\tilde{P}_{R,j}}{\text{maximize}} & \sum_{m=1}^{M}\sum_{i=1}^{N} \tilde{\pi}_{(i,j)}\tilde{\rho}_{m,(i,j)}\tilde{R}_{\mathrm{sec},m,i,j} - \lambda\tilde{P}_{R,j} \\ \text{subject to} & \sum_{i=1}^{N}\tilde{\pi}_{(i,j)} \le 1, \quad \sum_{m=1}^{M}\tilde{\rho}_{m,(i,j)} \le 1, \\ & \tilde{P}_{R,j} \le P_{\mathrm{R}}. \end{aligned} \tag{51}$$

Then, similar procedure to that of problem (41) can be taken to solve (51). Therefore, given $\alpha^*_{1,i}$s and $\alpha^*_{2,i}$s, problem (P1-general) can also be approximately solved by the Lagrangian dual decomposition method due to the same reason as that for (P1). The overall suboptimal algorithm for solving (P1-general) is summarized in Algorithm 3.

**Algorithm 3.** Proposed Suboptimal Algorithm to Solve (P1-general)

1: Denote optimal solution to (P1) as $\boldsymbol{\pi}^*$, $\boldsymbol{\rho}^*$ and $\boldsymbol{P}^*$;
2: **Initialize** $\boldsymbol{\pi} = \boldsymbol{\pi}^*$, $\boldsymbol{\rho} = \boldsymbol{\rho}^*$, $\boldsymbol{P} = \boldsymbol{P}^*$, $j = 0$;
3: **repeat**
4: **Set** $j = j + 1$ and **Initialize** $k = 0$, $\alpha^{(k)}_{1,i} = 0.5$, where $i = \arg\pi^*(i,j)$;
a. **Set** $k = k + 1$;
b. with $\bar{\alpha}_{1,i} = \alpha^{(k-1)}_{1,i}$, obtain $\alpha^{(k)}_{2,i}$ by solving (P1-general-sub1);
c. with $\bar{\alpha}_{2,i} = \alpha^{(k)}_{2,i}$, obtain $\alpha^{(k)}_{1,i}$ by solving (P1-general-sub2);
d. **Update** $\tilde{R}^{(k)}_{\mathrm{sec},m,i,j}$;
e. **Until** $\left|\tilde{R}^{(k)}_{\mathrm{sec},m,i,j} - \tilde{R}^{(k-1)}_{\mathrm{sec},m,i,j}\right| \le \epsilon$, where $\epsilon$ is a small positive number that controls the algorithm accuracy.
f. **Denote** final $\alpha^{(k)}_{1,i}$'s and $\alpha^{(k)}_{2,i}$'s, as $\alpha^*_{1,i}$ and $\alpha^*_{2,i}$, respectively.
5: **until** $j = N$.
6: **Solve** (P1-general) given $\{\alpha^*_{1,i}\}$ and $\{\alpha^*_{2,i}\}$ based on Algorithm 1.

### C. Complexity Analysis

The complexity of the proposed suboptimal algorithm is $O(NX + Y(ZMN^2 + N^3))$, where $X$ is the number of arithmetic operations required for conducting alternating optimization including (P1-general-sub1) and (P1-general-sub2). Since (P1-general) contains three continuous variables, i.e., $\alpha_{1,i}$, $\alpha_{2,i}$, and $\tilde{P}_{R,j}$, which are coupled together besides integer variables, i.e., $\tilde{\pi}(i,j)$ and $\tilde{\rho}_{m,(i,j)}$ for SC allocations. It is computationally expensive for exhaustive search over the feasible region without complexity-friendly heuristic algorithms such as the one proposed in Algorithm 3.

## V. Simulation Results and Discussion

Simulation results are given in this section to evaluate the performance of the proposed resource allocation algorithms. Figs. 2–5 are the results of secure resource allocation without jamming, and Figs. 6–8 are the results of secure resource allocation with CJ. Legitimate users are distributed evenly along a circle around the central RS with a radius of 30 m. Except for the simulation in Fig. 2, the eavesdropper is assumed to be located at a distance of $d = 200$ m from the RS. The total transmit power for each wireless sensor is $P_{A_m}(P_{B_m}) = 300$ mW for Fig. 2, Fig. 3, and Fig. 5. The carrier frequency is 2 GHz and the noise power is $\sigma^2 = BN_0$, where $B = 150$ kHz is the bandwidth of each SC and $N_0 = 10^{-21}$ mW/Hz is the AWGN power spectral density.

Unless otherwise specified, there are $N = 32$ SCs assumed in the OFDMA two-way relay WSN. The path loss exponent is 3. The number of wireless sensor pairs is fixed at 3 if not specified otherwise. There exists only one eavesdropper. The multipath channel fading coefficients are modeled as independent and identically distributed (i.i.d.) Rayleigh distributed random variables.

Fig. 2 illustrates the secrecy sum rate of both near optimal and suboptimal algorithms of P1 for different numbers of legitimate wireless sensor pairs assuming that a potential eavesdropper may exist at a distance between 150 and 500 m from the RS. In Figs. 2–5, "near optimal" refers to the near optimal algorithm proposed for P1 in Section IV-A, and "suboptimal optimal" refers to the suboptimal algorithm proposed for P1 in Section IV-B. We can see that the secrecy sum rate increases when the eavesdropper moves further away from the RS, in particular, when the eavesdropper departs from the relay at a distance within 200 m, because pathloss is a major factor deteriorating the received signal of the eavesdropper. The secrecy sum rate approaches a relatively stable level when

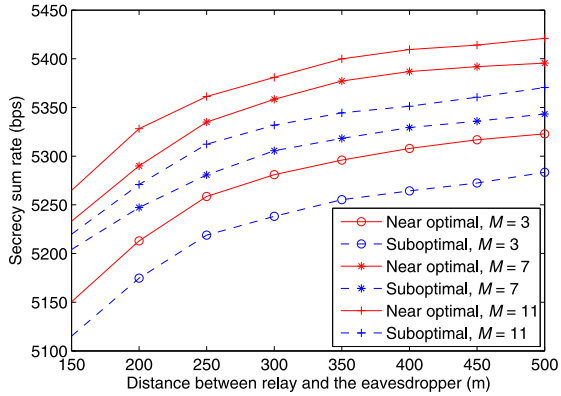


Fig. 2. Secrecy sum rate of the system versus $d$.

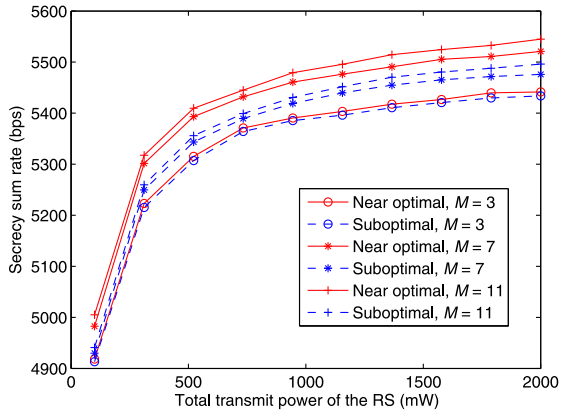


Fig. 3. Secrecy sum rate of the system versus $P_R$.

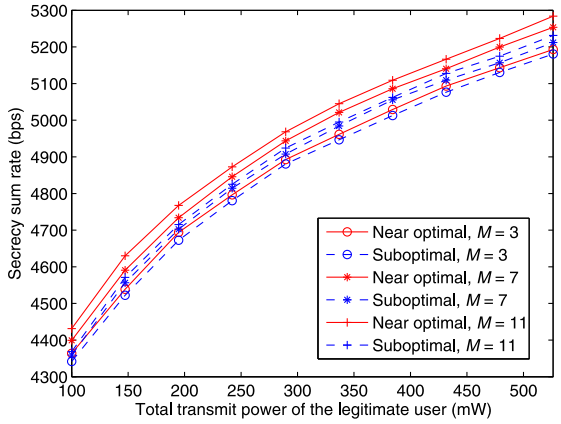


Fig. 4. Secrecy sum rate of the system versus $P_{A_m}(P_{B_m})$.

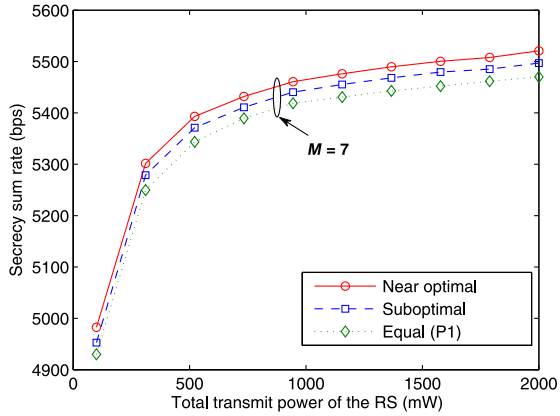


Fig. 5. Secrecy sum rate of the system versus $P_R$.

the eavesdropper is away from the RS for more than 500 m. Meanwhile, the suboptimal algorithm performs worse than the near optimal scheme.

Fig. 3 shows the secrecy sum rate of the first two proposed algorithms of P1 versus the total transmit power of the RS for 3, 7, and 11 pairs of legitimate wireless sensors. It can be observed that the secrecy sum rate grows with an increase of the transmit power of the RS. In our proposed power allocation algorithm, the transferred Lagrange dual problem is solved by Algorithm 1, which results in a $32 \times 1$ vector $\boldsymbol{P}$ containing optimal power in each SC. This solution to (33) demonstrates that in a specified $P_{\mathrm{R}}$, the sum of entries in the vector always equals $P_{\mathrm{R}}$. That means the secrecy sum rate converges to its optimal value when the total transmit power of the RS is thoroughly allocated. Therefore, higher secrecy sum rate will be obtained with more $P_{\mathrm{R}}$, owing to the considerably increased legitimate sum rate received by wireless sensors in the BC phase.

Fig. 4 depicts the secrecy sum rate versus the total transmit power of each legitimate user for $m = 3$, 7, and 11. We can find that the secrecy sum rate increases with the increased transmit power of each wireless sensor. The reason for this is that in our modeled system, the number of wireless sensors is much larger than that of the eavesdropper (only 1 is assumed). Thus, their increased transmit power leading to larger legitimate SNR will reasonably cause an increase in the secrecy sum rate. As expected, the near optimum algorithm of P1 outperforms the suboptimal algorithm of P1 and the disparity between them enlarges when $m$ gets larger. However, considering the lower complexity of the suboptimal algorithm for P1, there is a tradeoff between its complexity and secrecy performance.

Fig. 5 shows improved performance of the proposed near optimal and suboptimal algorithms for P1 in terms of the secrecy capacity versus $P_{\mathrm{R}}$, compared to the equal power allocation scheme, where $M = 7$ is set. In Fig. 5, the equal (P1) scheme is composed of SC pairing and assignment discussed in Part A of Section IV, and an equal power allocation across all SCs.

Fig. 6 plots the sum rate and the secrecy sum rate of the two-way relay wireless sensor system deploying optimal SC assignment and equal power allocation versus $P_{A_m}/\sigma^2$ for different values of $N$. The RS has a fixed total transmit power of 600 mW over all SCs. The system sum rate goes up sharply with an increase of the SNR of wireless sensor at each SC, while the secrecy sum rate increases at a relatively lower rate because of those information leaked to the eavesdropper. Fig. 6 demonstrates that in a secrecy sensitive two-way relay wireless sensor system, the secrecy sum rate is remarkably deteriorated due to the potential leaked data rate to an eavesdropper. Particularly, in a system with a higher SNR of legitimate wireless sensors, leaked rate to the eavesdropper gets larger as well, which can be seen from the difference between the two curves of the same $N$.

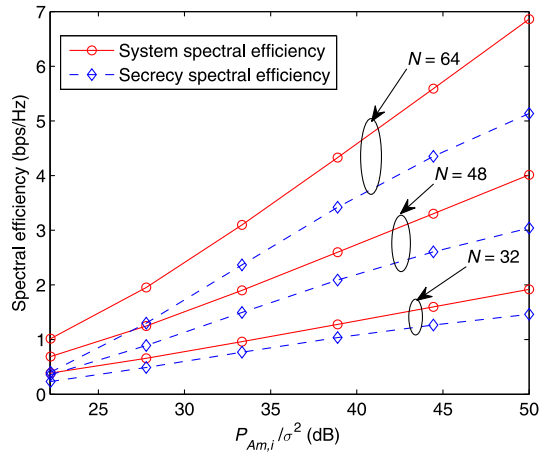


Fig. 6. Spectral efficiency/secrecy spectral efficiency of the system versus $P_{Am,i}/\sigma^2$.

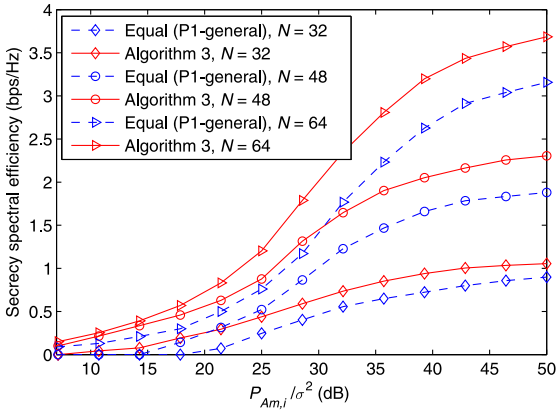


Fig. 7. Secrecy sum rate of the system versus $P_{Am,i}/\sigma^2$.

Obviously, when diversity gains in an OFDMA system increase with number of SCs $N$, the system leaked rate also enlarges.

Fig. 7 shows the optimized secrecy sum rate and equal power allocation-based secrecy sum rate of the two-way relay wireless sensor system versus the $P_{Am,i}/\sigma^2$ of the wireless sensor at SC $i$ for different $N$, where the RS has a fixed transmit power 100 mW. In Fig. 7, the equal (P1-general) scheme is Algorithm 3 with equal power allocation. The system secrecy sum rate obtained from the proposed suboptimal Algorithm 3 grows fast for $P_{Am,i}/\sigma^2$ between 20 and 35 dB, and less so fast after $P_{Am,i}/\sigma^2$ reaches 40 dB. The proposed Algorithm 3 thoroughly outperforms the equal (P1-general) scheme. However, under scenarios with less SCs, the difference between them is obviously smaller due to the less diversity gains over SCs. It shows that the proposed Algorithm 3 performs to its full advantage at a medium to high range of $P_{Am,i}/\sigma^2$ in OFDMA systems, which is reasonable in practical systems.

Fig. 8 shows the improved performance of the proposed Algorithm 3 versus $P_{R,j}/\sigma^2$ over each individual carrier $j$ ($k$), when compared to the equal (P1-general) scheme and the near optimal scheme in P1, for $N = 48$ and $N = 64$, where the transmit power of wireless sensors is fixed at 100 mW over all SCs. It can be observed that the secrecy sum rate in the system

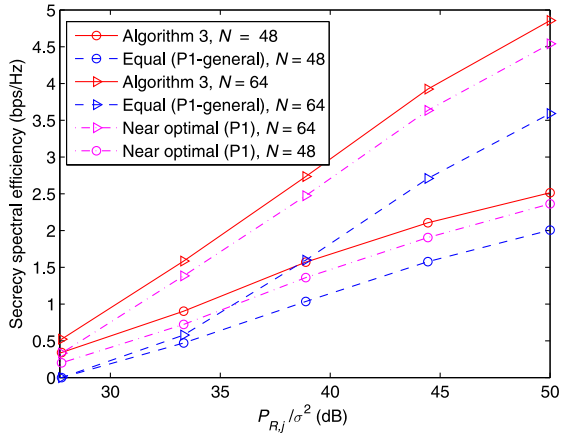


Fig. 8. Secrecy sum rate of the system versus $P_{R,j}/\sigma^2$.

deploying the proposed Algorithm 3 increases with the increasing of $P_{R,j}/\sigma^2$. The selected working mode of the RS, i.e., AF, can account for the fast growing secrecy sum rate of the two-way relay wireless sensor system, which closely depends on the transmit power at the RS in the BC phase. We can also find that when $N$ becomes larger, the proposed Algorithm 3 outperforms more significantly than the equal (P1-general) scheme. Compared to cases with increased $P_{Am,i}/\sigma^2$ of wireless sensor, increased $P_{R,j}/\sigma^2$ is shown to make more advantage of the proposed Algorithm 3. It also makes sense that in practical systems, larger $P_{R,j}/\sigma^2$ of the central RS is easier to be realized than larger $P_{Am,i}/\sigma^2$ of every distributed wireless sensors. As shown in Fig. 8, CJ enabled Algorithm 3 outperforms the near optimal scheme for P1 without CJ.

## VI. Conclusion

In this paper, we investigated the joint SC pairing, SC allocation and power allocation for secure two-way relay WSN in the presence of an eavesdropper without and with CJ. In the scenario without CJ, the proposed near optimal resource allocation algorithm properly allocates resources to wireless sensors, and the performance of secrecy sum rate of the system can be significantly improved. Moreover, a suboptimal algorithm was proposed to reduce the computational complexity. In the other scenario, a CJ scheme agreed by each pair of wireless sensors was proposed to confuse the eavesdropper while keeping the RS informed. Simulation results were presented to show the effectiveness of the proposed algorithms. In the future, we will extend this work to multieavesdropper and imperfect channel knowledge scenarios [31].

## References

[1] F. Dobslaw, T. Zhang, and M. Gidlund, "End-to-end reliability-aware scheduling for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 758–767, Apr. 2016.

[2] C. Jiang, N. He, Y. Ren, C. Chen, and J. Ma, "uSD: Universal sensor data entry card," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1450–1456, Aug. 2010.

[3] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter, "An experimental study of selective cooperative relaying in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1806–1816, Aug. 2014.

[4] J. Zhu, "Exploiting opportunistic network coding for improving wireless reliability against co-channel interference," *IEEE Trans. Ind. Informat.*, Jul. 2015, to be published.
[5] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X. Wen, and M. Tao, "Resource allocation in spectrum-sharing OFDMA femtocells with heterogeneous services," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2366–2377, Jul. 2014.
[6] K. Jitvanichphaibool, R. Zhang, and Y. Liang, "Optimal resource allocation for two-way relay-assisted OFDMA," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3311–3321, Sep. 2009.
[7] G. Sidhu, F. Gao, W. Chen, and A. Nallanathan, "A joint resource allocation scheme for multiuser two-way relay networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 2970–2975, Nov. 2011.
[8] H. Zhang, Y. Liu, and M. Tao, "Resource allocation with subcarrier pairing in OFDMA two-way relay networks," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 61–64, Apr. 2012.
[9] C. Jiang, X. Wang, J. Wang, H. Chen, and Y. Ren, "Security in space information networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 82–88, Aug. 2015.
[10] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[11] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[12] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.
[13] Y. Zou, X. Li, and Y. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.
[14] Y. Zou, B. Champagne, W. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.
[15] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.
[16] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *Proc. 12th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Los Angeles, CA, USA, Sep. 2006, pp. 514–519.
[17] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.
[18] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[19] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
[20] C. Jeong and I. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.
[21] H. Zhang, H. Xing, X. Chu, A. Nallanathan, W. Zheng, and X. Wen, "Secure resource allocation for OFDMA two-way relay networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM'12)*, Anaheim, CA, USA, Dec. 2012, pp. 3649–3654.
[22] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," in *Proc. ACM SIGCOMM'07*, Kyoto, Japan, Aug. 2007, pp. 397–408.
[23] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, USA, Mar. 2007, pp. 905–910.
[24] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.
[25] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ., 2004.
[26] W. Dang, M. Tao, H. Mu, and J. Huang, "Subcarrier-pair based resource allocation for cooperative multi-relay OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1640–1649, May 2010.
[27] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ., 2005.
[29] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[30] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.
[31] K. Cumanan, Z. Ding, B. Sharif, G. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

**Haijun Zhang** (M'13) received the Ph.D. degree in communications and information system from the Beijing University of Posts Telecommunications (BUPT), Beijing, China, in 2013.

He is a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, University of British Columbia (UBC), Vancouver, BC, Canada. From September 2011 to September 2012, he visited the Centre for Telecommunications Research, King's College London, London, U.K., as a Visiting Research Associate, supported by the China Scholarship Council. He has published more than 60 papers and authored two books. His research interests include 5G, resource allocation, heterogeneous small cell networks, and ultra-dense networks.

Dr. Zhang serves as an Editor of the *Journal of Network and Computer Applications*, *Wireless Networks*, and the *KSII Transactions on Internet and Information Systems*. He also serves as a Leading Guest Editor of Springer Mobile Networks and Applications (MONET) Special Issue on Game Theory for 5G Wireless Networks. He serves as General Chair of GameNets'16, and served as Symposium Chair of GameNets'14 and Track Chair of ScalCom'15.

**Hong Xing** (S'12) received the B.Eng. degree in electronic sciences and technologies, and the B.A. degree in English from Zhejiang University (ZJU), Hangzhou, China, in 2011. She is currently pursuing the Ph.D. degree in telecommunications at the Department of Informatics, King's College London, London, U.K.

From November 2012 to March 2014, she was a Visiting Ph.D. Student with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Her research interests include physical-layer security, wireless information and power transfer, cooperative communications, and applications of convex optimization in wireless communications.

**Julian Cheng** (S'96–M'04–SM'13) received the B.Eng. degree (first class) in electrical engineering from the University of Victoria, Victoria, BC, Canada, in 1995, the M.Sc. (Eng.) degree in mathematics and engineering from Queen's University, Kingston, ON, Canada, in 1997, and the Ph.D. degree in electrical engineering from the University of Alberta, Edmonton, AB, Canada, in 2003.

He is currently an Associate Professor with the School of Engineering, University of British Columbia, Vancouver, BC, Canada. His research interests include digital communications over fading channels, orthogonal frequency-division multiplexing, statistical signal processing for wireless applications, and optical wireless communications.

Dr. Cheng serves as an Editor for IEEE COMMUNICATIONS LETTERS and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

**Arumugam Nallanathan** (S'97–M'00–SM'05) received the Ph.D. degree in electrical engineering from the University of Hong Kong, Pokfulam, Hong Kong, in 2000.

He is a Professor of Wireless Communications with the Department of Informatics, King's College London (University of London), London, U.K. He served as the Head of Graduate Studies with the School of Natural and Mathematical Sciences, King's College London, in 2011/12. He was an Assistant Professor with the Department of Electrical and Computer Engineering, National

University of Singapore, Singapore, from August 2000 to December 2007. He has coauthored more than 250 papers. His research interests include 5G technologies, millimeter wave communications, and energy harvesting.

Mr. Nallanathan is a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS LETTERS, and IEEE SIGNAL PROCESSING LETTERS. He was the recipient of the IEEE Communications Society Signal Processing and Communications Electronics Outstanding Service Award in 2012 and the IEEE Communications Society Radio Communications Committee Outstanding Service Award in 2014.

**Victor C. M. Leung** (S'75–M'89–SM'97–F'03) received the Ph.D. degree in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 1982.

He is a Professor of Electrical and Computer Engineering and a TELUS Mobility Research Chair with UBC. He has coauthored more than 800 technical papers in archival journals and refereed conference proceedings. His research interests include wireless networks and mobile systems.

Dr. Leung is a Fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada. He is serving on the Editorial Boards of the Series on Green Communications and Networking of the IEEE JOURNAL ON SELECTED AREAS AND NETWORKING, IEEE WIRELESS COMMUNICATIONS LETTERS, and several other journals. He was the recipient of the 1977 Association of Professional Economists of British Columbia Gold Medal, the Natural Sciences and Engineering Research Council of Canada Postgraduate Scholarships from 1977 to 1981, the 2012 UBC Killam Research Prize, and the IEEE Vancouver Section Centennial Award.