Secure Communications in NOMA System: Subcarrier Assignment and Power Allocation

Haijun Zhang, *Senior Member, IEEE*, Ning Yang, Keping Long, *Senior Member, IEEE*, Miao Pan, *Member, IEEE*, George K. Karagiannidis, *Fellow, IEEE*, and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*— Secure communication is a promising technology for wireless networks because it ensures secure transmission of information. In this paper, we investigate the joint subcarrier (SC) assignment and power allocation problem for non-orthogonal multiple access amplify-and-forward two-way relay wireless networks, in the presence of eavesdroppers. By exploiting cooperative jamming (CJ) to enhance the security of the communication link, we aim to maximize the achievable secrecy energy efficiency by jointly designing the SC assignment, user pair scheduling and power allocation. Assuming the perfect knowledge of the channel state information at the relay station, we propose a low-complexity subcarrier assignment scheme (SCAS-1), which is equivalent to many-to-many matching games, and then SCAS-2 is formulated as a secrecy energy efficiency maximization problem. The secure power allocation problem is modeled as a convex geometric programming problem, and then, solved by interior point methods. Simulation results demonstrate that the effectiveness of the proposed SSPA algorithms under scenarios of using and not using CJ, respectively.**

***Index Terms*— Cooperative jamming, non-orthogonal multiple access, physical layer security, energy efficiency.**

I. Introduction

RECENTLY, non-orthogonal multiple access (NOMA) has been considered as a promising solution to significantly improve energy efficiency for wireless communications [1]–[5]. The main advantage of NOMA is that it can simultaneously serves multiple users on the same subcarrier (SC) to increase the system throughput [1]. The concept of successive interference cancellation (SIC) at the receiver sides was applied in NOMA to address the inter-user interference. NOMA can utilize different resource allocation methods to achieve a good spectral efficiency and energy efficiency performance. In [6], the effective capacity with power control policy was introduced to guarantee delay quality of service (QoS) for downlink NOMA system. In [7], the power allocation techniques were studied to ensure fairness under instantaneous channel state information (CSI) and average CSI in NOMA system. In [8], user grouping based on user locations was applied to reduce interference and the power allocation scheme was employed to improve sum rate for visible light communication multi-cell networks.

Meanwhile, physical layer security has drawn much attention in wireless networks [9], [10]. Due to the broadcast nature of wireless communications, wireless transmissions are exposed to unauthorized users and vulnerable to both the jamming and eavesdropping attacks. Physical layer security is regarded as an important methodology to realize secrecy transmissions against eavesdropping attacks [11]. Specifically, secrecy capacity can be enhanced by exploiting multiple antennas additional spatial degrees of freedom in multiple-input-multiple-output (MIMO) wiretap channel [12], [13]. Furthermore, researchers applied robust beamforming transmission technique, artificial noise (AN), and Multi-antenna relay scheme to improve physical layer security [14]–[18]. Additionally, the physical layer security of cooperative communication in large-scale cognitive radio networks was investigated [19] by invoking a multiphase transmission scheme.

Cooperative jamming (CJ) is a special physical layer technique, which uses AN to confuse the eavesdropper. In [20], CJ nodes were studied and interfered untrusty relay nodes with splitted power. In [21], the distinct precoding vectors of node users and jamming signals were designed in two-way relaying wiretap systems. In [22], secure transmission schemes were designed for relay network by exploiting CJ and signal superposition methods in two typical communication scenarios. One scenario is to maintain a satisfactory transmission rate while minimizing message leakage. The other scenario is to improve the average throughput of the system. In addition, an uncoordinated cooperative jamming scheme was investigated and uncoordinated single-antenna users independently transmit jamming signal. The central control properly allocated the jamming power of each helper to optimize secrecy sum rate [23].

Manuscript received September 15, 2017; accepted December 30, 2017. Date of publication April 11, 2018; date of current version October 18, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61471025 and Grant 61771044, in part by the Young Elite Scientist Sponsorship Program by CAST under Grant 2016QNRC001, in part by the Research Foundation of the Ministry of Education of China and China Mobile under Grant MCM20170108, in part by the Beijing Natural Science Foundation under Grant L172025, in part by the Fundamental Research Funds for the Central Universities under Grant RC1631 and Grant FRF-GF-17-A6, and in part by the U.S. National Science Foundation under Grant US CNS-1343361, Grant CNS-1350230 (CAREER), Grant CNS-1646607, and Grant CNS-1702850. *(Corresponding authors: Haijun Zhang; Keping Long.)*

H. Zhang, N. Yang, and K. Long are with the Beijing Engineering and Technology Research Center for Convergence Networks and Ubiquitous Services, University of Science and Technology Beijing, Beijing 100083, China (e-mail: haijunzhang@ieee.org; s20150694@xs.ustb.edu.cn; longkeping@ustb.edu.cn).

M. Pan is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA (e-mail: mpan2@uh.edu).

G. K. Karagiannidis is with the Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece (e-mail: geokarag@auth.gr).

V. C. M. Leung is with the Department of Electrical and Computer Engineering, The 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/JSAC.2018.2825559

Resource allocation plays a crucial role in exploiting the potential performance gain for NOMA wireless networks. Several works have employed different optimization methods to improve the sum rate in several research works, such as the monotonic optimization [24], Lagrangian duality theory [25], and matching theory [26]. Besides the maximization of sum rate and resource allocation with security considerations for NOMA networks have also been addressed in the existing works. In [27], a robust resource allocation framework was investigated in half-duplex relay networks to improve the physical layer security. In [29], a secure cooperative communication was introduced in cognitive radio networks with users and eavesdroppers, where secondary users were allowed to access the spectrum of primary users in the presence of malicious eavesdroppers. In [30], the joint relay selection and subcarrier allocation scheme was employed in decode-and-forward relay assisted secure vehicle-to-vehicle communications. However, secure resource allocation has not been well studied for NOMA two-way relay wireless networks. These motivated our work. A preliminary work on this research problem was published in [28], and this paper extends [28] as follows: (1) the cooperative jamming is considered in secure energy efficient resource allocation in NOMA networks; (2) more simulation results are provided to verify the proposed methods with and without cooperative jamming.

In this paper, we consider secrecy energy efficiency maximization based amplify-and-forward (AF) two-way relay wireless networks under power constraints. To ensure the worst-case secrecy energy efficiency for each user is a positive rate, we assume that an upper-bound capacity can be achieved for each eavesdropper. The eavesdropper is regarded as a untrusted user and the user pair patterns are known to eavesdroppers. The secure resource allocation problem is complex due to the combinatorial aspect induced by SC assignment and user pair scheduling and power allocation. Our contributions and novelties can be summarized as follows.

1) We investigate secure communications for NOMA two-way relay wireless networks in the presence of eavesdroppers under scenarios of using and not using CJ at the relay station (RS). In this work, we consider perfect CSI for the secrecy subcarrier assignment and power allocation problem and formulate it as a mixed non-convex optimization problem. The constraints include the maximum system power, the minimum data rate for each user pair, the maximum number of users can be multiplexed on the same SC and the maximum number of SCs occupied by each user pair.
2) A matching algorithm SCAS-1 is proposed for SC assignment to improve the secrecy energy efficiency. In this scheme, the user pair scheduling is updated in each iteration. The system energy efficiency improves until it converges. To achieve high secrecy energy efficiency of the system, SCAS-2 scheme is proposed in the NOMA wireless network.
3) Based on the proposed SCAS schemes, a novel power allocation scheme is proposed for the NOMA wireless network and the power allocation for each SC is derived by utilizing interior methods. To tackle this NP-hard optimization problem, the proposed SSPA-2 scheme obtains global optimal. In addition, we proposed SSPA-2 scheme to strike a balance between system performance and computational complexity.
4) Simulation results verify the derived theoretical analytical results and demonstrate the performance superiority of the proposed SSPA schemes in terms of the average secrecy without and with CJ.

Organization: The rest of this paper is organized as follows. Section II provides the system model and problem formulation of secure resource allocation. In Section III, secrecy energy efficiency subcarrier assignment schemes for NOMA wireless network. In Section IV, secrecy energy efficiency power allocation scheme for NOMA wireless network. In Section V, performance of the proposed algorithms are evaluated by simulations. Finally, Section VI concludes the paper.

II. System Model

A. Secrecy NOMA Two-Way Relay Wireless Networks Without Cooperative Jamming

We consider a NOMA two-way relay wireless network composed of M preassigned user pairs, denoted by $\mathcal{M} = \{1, \ldots, M\}$. The NOMA channel composes of N SCs, denoted by $\mathcal{N} = \{1, \ldots, N\}$, and each has a bandwidth B. As shown in Fig. 1, two users (A_m and B_m), a RS, and an eavesdropper are presented. In the case of not using CJ, there is no artificial noise (AN). The bi-directional communications between users A_m and B_m are aided by the RS. Eavesdropper is passive and intercepts the information from A_m and B_m without alteration.

AF protocol is considered in this paper which is divided into two phases: the multiple access (MA) phase and the broadcast (BC) phase. All user pairs do simultaneous wireless messages and power transfer with the RS in the MA phase; the RS further amplifies and forwards the received signals to user pairs employing its transmit power in the BC phase. Based on the CSI for NOMA two-way relay wireless network, one SC can be allocated to multiple user pairs, and one user pair can receive from the RS through multiple SCs. Meanwhile, the RS assigns different power to user pairs over SCs. Block fading channel is assumed to be flat and consisted of distance-dependent path loss and Rayleigh fading on each of the SC. We assume a slow fading environment where all the SCs are invariable during a complete transmission cycle and cochannel interference among user pairs on each SC is considered.

In the MA phase, we assume that SC i is allocated to the K user pairs, where $\mathcal{K} = \{1, \ldots, K\}$. The mth user pair is composed of user A_m and user B_m, where $m \in \mathcal{K}$, $m \in \mathcal{M}$. The received signal on SC i at the RS is given by

$$y_{RS,i} = \sum_{m \in \mathcal{K}} (\sqrt{P_{A_m,i}} h_{A_m,R,i} s_{A_m,i} + \sqrt{P_{B_m,i}} h_{B_m,R,i} s_{B_m,i}) + n_{RS,i} \quad (1)$$

where $i \in \mathcal{N}$; $s_{A_m,i}$ and $s_{B_m,i}$ are the transmitted signals of users A_m and B_m on SC i, respectively, which are cyclic symmetric complex Gaussian (CSCG) random variables given by $s_{A_m,i} \sim \mathcal{CN}(0,1)$ and $s_{B_m,i} \sim \mathcal{CN}(0,1)$ separately;

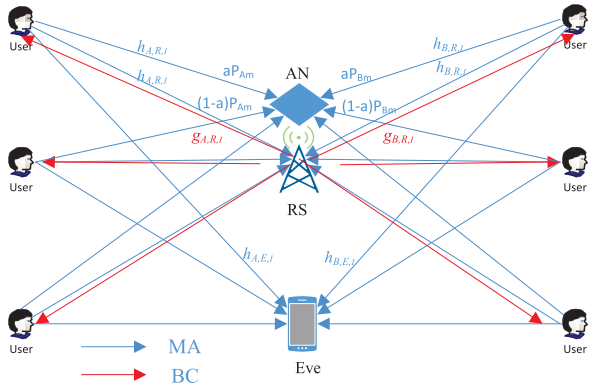

Fig. 1. System model of the security transmission in two-way relay wireless network.

$n_{RS,i} \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the RS on SC i. The total transmission power of users A_m and B_m are constrained by P_{A_m} and P_{B_m}, respectively; $h_{A_m,R,i}$ and $h_{B_m,R,i}$ are, respectively, the channel gains from A_m to RS and from B_m to RS on SC i.

The received signal at the eavesdropper on SC i can be expressed as

$$y_{E,i} = \sum_{m\in\mathcal{K}} (\sqrt{P_{A_m,i}} h_{A_m,E,i} s_{A_m,i} + \sqrt{P_{B_m,i}} h_{B_m,E,i} s_{B_m,i}) + n_{E,i} \quad (2)$$

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

In the BC phase, we assume that SC j is allocated to the mth user pair with transmitted power $P_{R,j}$. $\beta_i y_{RS,i}$ is the signal transmitted from the RS, and $\beta_i = \sqrt{P_{R,j}}/\alpha_i$ is the amplifying coefficient. α_i is a normalized factor denoted by $\alpha_i = \sqrt{\sum_{m\in\mathcal{K}} (P_{A_m,i}|h_{A_m,R,i}|^2 + P_{B_m,i}|h_{B_m,R,i}|^2) + \sigma^2}$. The total transmission power of RSs are constrained by $\sum_{j=1}^{N} P_{R,j} \le P_{\mathrm{R}}$. The received signal on SC j at A_m is that $y_{A_m,i,j} = \sqrt{P_{R,j}} g_{A_m,j} y_{RS,i}/\alpha_i + n_{A_m,j}$, which is further given by

$$y_{A_m,i,j} = \sum_{m\in\mathcal{K}} (\sqrt{P_{R,j}} g_{A_m,j} \sqrt{P_{A_m,i}} h_{A_m,R,i} s_{A_m,i}/\alpha_i + \sqrt{P_{R,j}} g_{A_m,j} \sqrt{P_{B_m,i}} h_{B_m,R,i} s_{B_m,i}/\alpha_i) + \sqrt{P_{R,j}} g_{A_m,j} n_{RS,i}/\alpha_i + n_{A_m,j}. \quad (3)$$

Similarly, the received signal on SC j at B_m is $y_{B_m,i,j} = \sqrt{P_{R,j}} g_{B_m,j} y_{RS,i}/\alpha_i + n_{B_m,j}$, which is further given by

$$y_{B_m,i,j} = \sum_{m\in\mathcal{K}} (\sqrt{P_{R,j}} g_{B_m,j} \sqrt{P_{A_m,i}} h_{A_m,R,i} s_{A_m,i}/\alpha_i + \sqrt{P_{R,j}} g_{B_m,j} \sqrt{P_{B_m,i}} h_{B_m,R,i} s_{B_m,i}/\alpha_i) + \sqrt{P_{R,j}} g_{B_m,j} n_{RS,i}/\alpha_i + n_{B_m,j} \quad (4)$$

where $g_{A_m,j}$ and $g_{B_m,j}$ are, respectively, the channel gains on SC j from the RS to the mth user pair A_m and B_m; and $n_{A_m,j}$ and $n_{B_m,j}$ are separately, AWGNs at A_m and B_m on SC j are denoted by $n_{A_m,j} \sim \mathcal{CN}(0,\sigma^2)$ and $n_{B_m,j} \sim \mathcal{CN}(0,\sigma^2)$. $G_{A_m,i} \triangleq |g_{A_m,R,i}|^2/\sigma^2$ and $G_{B_m,i} \triangleq |g_{B_m,R,i}|^2/\sigma^2$ denote the channel response normalized by noise (CRNN) of the user A_m and B_m separately.

The received signal at the eavesdropper on SC j in the BC phase can be expressed as

$$y_{E,i,j} = \sum_{m\in\mathcal{K}} (\sqrt{P_{R,j}} g_{E,j} \sqrt{P_{A_m,i}} h_{A_m,R,i} s_{A_m,i}/\alpha_i + \sqrt{P_{R,j}} g_{E,j} \sqrt{P_{B_m,i}} h_{B_m,R,i} s_{B_m,i}/\alpha_i) + \sqrt{P_{R,j}} g_{E,j} n_{RS,i}/\alpha_i + n_{E,j} \quad (5)$$

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

Assuming cochannel interference among user pairs on each SC is considered. The signal-to-interference-plus-noise ratios (SINRs) of users A_m and B_m, sharing SC i in the MA phase and SC j in the BC phase, which can be respectively given by

$$SNR_{A_m,i,j} = \frac{P_{R,j}|g_{A_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2}{I_{A_m} + (P_{R,j}|g_{A_m,j}|^2/\alpha_i^2 + 1)\sigma^2} \quad (6)$$

and

$$SNR_{B_m,i,j} = \frac{P_{R,j}|g_{B_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2}{I_{B_m} + (P_{R,j}|g_{B_m,j}|^2/\alpha_i^2 + 1)\sigma^2}. \quad (7)$$

$$\begin{aligned}
I_{A_m} &= \sum_{m\in\mathcal{K}} (P_{R,j}|g_{A_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{A_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\
&\quad -(P_{R,j}|g_{A_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{A_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\
I_{B_m} &= \sum_{m\in\mathcal{K}} (P_{R,j}|g_{B_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{B_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\
&\quad -(P_{R,j}|g_{B_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{B_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2). \quad (8) \\
ET &= \sum_{m\in\mathcal{K}} (P_{A_m,i}|h_{A_m,E,i}|^2 + P_{B_m,i}|h_{B_m,E,i}|^2) - (P_{A_m,i}|h_{A_m,E,i}|^2 + P_{B_m,i}|h_{B_m,E,i}|^2) + \sigma^2 \\
ER &= \sum_{m\in\mathcal{K}} (P_{R,j}|g_{E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{E,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\
&\quad -(P_{R,j}|g_{E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{E,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) + (P_{R,j}|g_{E,j}|^2/\alpha_{m,i}^2)\sigma^2. \quad (9)
\end{aligned}$$

where I_{A_m} and I_{B_m} are given by (8) at the bottom of the previous page.

Based on (2) and (5), the received signal in the two phases of the eavesdropper can be modeled as a 2-by-2 point-to-point MIMO channel expressed as

$$\boldsymbol{y}_E = \boldsymbol{H}_E \boldsymbol{s} + \boldsymbol{n}_E \tag{10}$$

where

$$\begin{aligned}
H_E &= \begin{bmatrix} h_{1,A_m} & h_{1,B_m} \\ h_{2,A_m} & h_{2,B_m} \end{bmatrix} \\
h_{1,A_m} &= \sqrt{P_{A_m,i}} h_{A_m,E,i} \\
h_{1,B_m} &= \sqrt{P_{B_m,i}} h_{B_m,E,i} \\
h_{2,A_m} &= \sqrt{P_{R,j}} g_{E,j} \sqrt{P_{A_m,i}} h_{A_m,R,i}/\alpha_i \\
h_{2,B_m} &= \sqrt{P_{R,j}} g_{E,j} \sqrt{P_{B_m,i}} h_{B_m,R,i}/\alpha_i
\end{aligned} \tag{11}$$

$$\begin{aligned}
s &= \begin{bmatrix} s_{A_m,i} & s_{B_m,i} \end{bmatrix}^T \\
n_E &= \begin{bmatrix} n_{A_m,i} & n_{B_m,i} \end{bmatrix}^T
\end{aligned} \tag{12}$$

$$\begin{aligned}
n_{A_m,i} &= \sum_{m \in \mathcal{K}} (h_{1,A_m} + h_{1,B_m}) + n_{E,i} - (h_{1,A_m} + h_{1,B_m}) \\
n_{B_m,i} &= \sum_{m \in \mathcal{K}} (h_{2,A_m} + h_{2,B_m}) + \sqrt{P_{R,j}} g_{E,j} n_{RS,i}/\alpha_i \\
&\quad + n_{E,j} - (h_{2,A_m} + h_{2,B_m}).
\end{aligned} \tag{13}$$

For users A_m and B_m, the instantaneous mutual information (IMI) rate are expressed as

$$R_{A_m,i,j} = \frac{1}{2} B \log(1 + SNR_{A_m,i,j}) \tag{14}$$

and

$$R_{B_m,i,j} = \frac{1}{2} B \log(1 + SNR_{B_m,i,j}) \tag{15}$$

respectively.

For the eavesdropper, due to (10) is equivalent to a 2-by-2 point-to-point MIMO system with the transmit signals $s = \begin{bmatrix} s_{A_1,i} & s_{B_1,i} & \dots & s_{A_m,i} & s_{B_m,i} \end{bmatrix}^T$, denoted by $\boldsymbol{s} \sim \mathcal{CN}(0, \boldsymbol{I})$. The maximum achievable received signal for the eavesdropper is defined as [31, Ch. 8]

$$R_{E,i,j} = \frac{1}{2} B \log\det(\boldsymbol{I} + \boldsymbol{H}_E \boldsymbol{H}_E^H \boldsymbol{Q}_E^{-1}) \tag{16}$$

where

$$Q_E = E\left[n_E n_E^H\right] = \begin{bmatrix} ET & 0 \\ 0 & ER \end{bmatrix} \tag{17}$$

ET and ER are given by (9) at the bottom of the previous page. The factor $\frac{1}{2}$ and $\mathbb{E}[\cdot]$ reflects the statistical average in (16) in a complete transmission slot accounts for the two phases. Hence, the worst-case secrecy sum rate for the mth users over the SC pair (i, j) is expressed as [32]

$$R_{\text{sec},m,i,j} = [R_{A_m,i,j} + R_{B_m,i,j} - R_{E,i,j}]^+ \tag{18}$$

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

B. Secrecy NOMA Two-Way Relay Wireless Networks With Cooperative Jamming

Base on the CSI for the RS, we investigate a similar problem which is described in Section II-A with CJ.

In the MA phase, $s'_{A_m,i}$ and $s'_{B_m,i}$ are, respectively, the incorporating jamming signals of the users A_m and B_m on SC i for the exchange messages. The portions of the transmission power of the AN are denoted by $\alpha_{1,i}$ and $\alpha_{2,i}$ at A_m and B_m on SC i separately. Accordingly, A_m splits its transmission power on SC i into $(1-\alpha_{1,i})P_{A_m,i}$ for exchange message $s_{A_m,i}$, and $\alpha_{1,i}P_{A_m,i}$ for AN, $s'_{A_m,i}$, respectively. Similar transmission scheme is used for B_m. The received signal on SC i at the RS can be expressed as

$$\begin{aligned}
y_{RS,i} = \sum_{m \in \mathcal{K}} (&\sqrt{(1-\alpha_{1,i})P_{A_m,i}} h_{A_m,R,i} s_{A_m,i} \\
&+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}} h_{B_m,R,i} s_{B_m,i} \\
&+ \sqrt{\alpha_{1,i}P_{A_m,i}} h_{A_m,R,i} s'_{A_m,i} \\
&+ \sqrt{\alpha_{2,i}P_{B_m,i}} h_{B_m,R,i} s'_{B_m,i}) + n_{RS,i}.
\end{aligned} \tag{19}$$

For the eavesdropper, the received signal on SC i is given by

$$\begin{aligned}
y_E^{(1)} = \sum_{m \in \mathcal{K}} (&\sqrt{(1-\alpha_{1,i})P_{A_m,i}} h_{A_m,E,i} s_{A_m,i} \\
&+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}} h_{B_m,E,i} s_{B_m,i} \\
&+ \sqrt{\alpha_{1,i}P_{A_m,i}} h_{A_m,E,i} s'_{A_m,i} \\
&+ \sqrt{\alpha_{2,i}P_{B_m,i}} h_{B_m,E,i} s'_{B_m,i}) + n_{E,i}.
\end{aligned} \tag{20}$$

Assuming AN signals $s'_{A_m,i}$ and $s'_{B_m,i}$, which are fully known by the RS before being transmitted over some higher-layer cryptographic protocols, so $\sqrt{\alpha_{1,i}P_{A_m,i}} h_{A_m,R,i} s'_{A_m,i}$ and $\sqrt{\alpha_{2,i}P_{B_m,i}} h_{B_m,R,i} s'_{B_m,i}$ in (19) can be canceled [33] [34] at the RS. As a result, only $s_{A_m,i}$ and $s_{B_m,i}$ are broadcasted on SC j in BC phase. Then, A_m and B_m can subtract s_{A_m} and subtract s_{B_m} to obtain desirable signal from the broadcast signal, respectively. However, eavesdropper suffers from large interference due to ANs are kept strictly confidential to the eavesdropper. After canceling $s'_{A_m,i}$ and $s'_{B_m,i}$, $y'_{RS,i}$, which transmits the remaining signal be expressed as

$$\begin{aligned}
y'_{RS,i} = \sum_{m \in \mathcal{K}} (&\sqrt{(1-\alpha_{1,i})P_{A_m,i}} h_{A_m,R,i} s_{A_m,i} \\
&+ \sqrt{(1-\alpha_{2,i})P_{B_m,i}} h_{B_m,R,i} s_{B_m,i}) + n_{RS,i}
\end{aligned} \tag{21}$$

the amplifying coefficient is denoted by $\beta_i = \sqrt{P_{R,j}}/\gamma_i$ where γ_i can be regarded as a normalized factor for the forwarded signal and it is shown in (22) at the top of the next page. The transmit power of the RS on SC j is denoted by $P_{R,j}$. Note that we can further simplify the received signal at the A_m by substituting β_i and $y'_{RS,i}$ due to A_m can successfully

$$\gamma_i = \sqrt{\sum_{m\in\mathcal{K}}((1-\alpha_{1,i})P_{A_m,i}|h_{A_m,R,i}|^2 + (1-\alpha_{2,i})P_{B_m,i}|h_{B_m,R,i}|^2) + \sigma^2}. \tag{22}$$

$$\begin{aligned}
ET' =& \sum_{m\in\mathcal{M}}(\alpha_{1,i}P_{A_m,i}|h_{A_m,R,i}|^2 + \alpha_{2,i}P_{B_m,i}|h_{B_m,R,i}|^2) - (\alpha_{1,i}P_{A_m,i}|h_{A_m,R,i}|^2 + \alpha_{2,i}P_{B_m,i}|h_{B_m,R,i}|^2) + \sigma^2 \\
&+ \sum_{m\in\mathcal{M}}((1-\alpha_{1,i})P_{A_m,i}|h_{A_m,R,i}|^2 + (1-\alpha_{2,i})P_{B_m,i}|h_{B_m,R,i}|^2) \\
ER' =& \sum_{m\in\mathcal{M}}(P_{R,j}|g_{R,E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\gamma_i^2 + P_{R,j}|g_{R,E,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\gamma_i^2) \\
&-(P_{R,j}|g_{R,E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\gamma_i^2 + P_{R,j}|g_{R,E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\gamma_i^2) + (P_{R,j}|g_{R,E,j}|^2/\gamma_i^2)\sigma^2.
\end{aligned} \tag{23}$$

$$\begin{aligned}
I'_{A_m} =& \sum_{m\in\mathcal{K}}((1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,A_m,j}|^2|h_{A_m,R,i}|^2/\gamma_i^2 + (1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,A_m,j}|^2|h_{B_m,R,i}|^2/\gamma_i^2) \\
&-((1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,A_m,j}|^2|h_{A_m,R,i}|^2/\gamma_i^2 + (1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,A_m,j}|^2|h_{B_m,R,i}|^2/\gamma_i^2) \\
I'_{B_m} =& \sum_{m\in\mathcal{K}}((1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,B_m,j}|^2|h_{A_m,R,i}|^2/\gamma_i^2 + (1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,B_m,j}|^2|h_{B_m,R,i}|^2/\gamma_i^2) \\
&-((1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,B_m,j}|^2|h_{A_m,R,i}|^2/\gamma_i^2 + (1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,B_m,j}|^2|h_{B_m,R,i}|^2/\gamma_i^2).
\end{aligned} \tag{24}$$

cancel its previously transmitted $s_{A_m,i}$ at its receiver. In the BC phase, the received signal at the A_m is given by

$$\begin{aligned}
y_{A_m,i,j} =& \sum_{m\in\mathcal{K}}(\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{A_m,R,i}s_{A_m,i}/\gamma_i \\
&+\sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{A_m,R,j}s_{B_m,i}/\gamma_i) \\
&+\sqrt{P_{R,j}}g_{A_m,R,j}n_{RS,i}/\gamma_i + n_{A_m,j}.
\end{aligned} \tag{25}$$

Similarly, the received signal at the B_m is defined as

$$\begin{aligned}
y_{B_m,i,j} =& \sum_{m\in\mathcal{K}}(\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{B_m,R,i}s_{A_m,i}/\gamma_i \\
&+\sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{B_m,R,j}s_{B_m,i}/\gamma_i) \\
&+\sqrt{P_{R,j}}g_{B_m,R,j}n_{RS,i}/\gamma_i + n_{B_m,j}.
\end{aligned} \tag{26}$$

For the eavesdropper, it receives a combined signal of $s_{A_m,i}$ and $s_{B_m,i}$ due to the transmission signals are unknown, which is expressed as

$$\begin{aligned}
y_E^{(2)} =& \sum_{m\in\mathcal{K}}(\sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{R,E,j}s_{A_m,i}/\gamma_i \\
&+\sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{R,E,j}s_{B_m,i}/\gamma_i) \\
&+\sqrt{P_{R,j}}g_{R,E,j}n_{RS,i}/\gamma_i + n_{E,j}.
\end{aligned} \tag{27}$$

Based on (20) and (27), the received signals at the eavesdropper during a transmit slot to the equivalent point-to-point 2-by-2 MIMO channel can be combined into

$$y_E = H_E{}'s + n_E{}' \tag{28}$$

The equivalent channel matrix between the user pairs and the eavesdropper over the SC pair (i,j) is defined as

$$\begin{aligned}
H_E =& \begin{bmatrix} h_{1,A_m}{}' & h_{1,B_m}{}' \\ h_{2,A_m}{}' & h_{2,B_m}{}' \end{bmatrix} \\
h'_{1,A_m} =& \sqrt{(1-\alpha_{1,i})P_{A_m,i}}h_{A_m,E,i} \\
h'_{1,B_m} =& \sqrt{(1-\alpha_{2,i})P_{B_m,i}}h_{B_m,E,i} \\
h'_{2,A_m} =& \sqrt{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}}h_{A_m,R,i}g_{R,E,j} \\
h'_{2,B_m} =& \sqrt{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}}h_{B_m,R,i}g_{R,E,j}
\end{aligned} \tag{29}$$

In the MA phase, $\tilde{n}_{A_1,i}$ indicates that the equivalent received noise at the eavesdropper treating with the generated AN by the user pair as noise, which is denoted by

$$n'_{A_m,i} = \sum_{m\in\mathcal{K}}(h'_{1,A_m} + h'_{1,B_m}) + n_{E,i} - (h'_{1,A_m} + h'_{1,B_m}). \tag{30}$$

In the BC phase, $\tilde{n}_2$ denotes the amplified noise and the additive noise, which is given by

$$\begin{aligned}
n'_{B_1,i} =& \sum_{m\in\mathcal{K}}(h'_{2,A_m} + h'_{2,B_m}) - (h'_{2,A_m} + h'_{2,B_m}) \\
&+\sqrt{P_{R,j}}g_{R,E,j}n_{RS,i}/\gamma_i + n_{E,j}.
\end{aligned} \tag{31}$$

For this equivalent noise the associated covariance matrix at the eavesdropper can be expressed as

$$\begin{aligned}
Q_E =& E\left[(n_{A_m,i}, n_{B_m,i})^H(n_{A_m,i}, n_{B_m,i})\right] \\
=& \begin{bmatrix} ET' & 0 \\ 0 & ER' \end{bmatrix}.
\end{aligned} \tag{32}$$

where ET' and ER' are given by (23) at the top of this page. From (25) and (26), the SINRs of users A_m and B_m, which

share SC i in the MA phase and SC j in the BC phase, can be respectively denoted as

$$SNR_{A_m,i,j}{}' = \frac{(1-\alpha_{2,i})P_{R,j}P_{B_m,i}|g_{R,A_m,j}|^2|h_{B_m,R,i}|^2/\gamma_i^2}{I'_{A_m}+(P_{R,j}|g_{R,A_m,j}|^2/\gamma_i^2+1)\sigma^2} \tag{33}$$

and

$$SNR_{B_m,i,j}{}' = \frac{(1-\alpha_{1,i})P_{R,j}P_{A_m,i}|g_{R,B_m,j}|^2|h_{A_m,R,i}|^2/\gamma_i^2}{I'_{B_m}+(P_{R,j}|g_{R,B_m,j}|^2/\gamma_i^2+1)\sigma^2}. \tag{34}$$

where I'_{A_m} and I'_{B_m} are given by (24) at the top of the previous page.

The IMI rate for the user A_m and B_m are expressed as

$$\tilde{R}_{A_m,i,j} = \frac{1}{2}B\log_2(1+SNR'_{A_m,i,j}) \tag{35}$$

and

$$\tilde{R}_{B_m,i,j} = \frac{1}{2}B\log_2(1+SNR'_{B_m,i,j}) \tag{36}$$

respectively.

For the eavesdropper, due to (28) is equivalent to a 2-by-2 point-to-point MIMO system with transmission signals $s = \left[\, s_{A_1,i}\ s_{B_1,i}\ \ldots\ s_{A_m,i}\ s_{B_m,i}\,\right]^T$, denoted by $\boldsymbol{s} \sim \mathcal{CN}(0,\boldsymbol{I})$. The maximum achievable received signal for the eavesdropper is defined as [31, Ch. 8]

$$\tilde{R}_{E,i,j} = \frac{1}{2}B\log_2\det\left(\boldsymbol{I}+\boldsymbol{H_E}\boldsymbol{H_E^H}\tilde{\boldsymbol{Q}}_{\boldsymbol{E}}^{-\mathbf{1}}\right). \tag{37}$$

Hence, the worst-case secrecy sum rate with CJ for the mth user pair over the SC pair (i,j) can be denoted by [32]

$$\tilde{R}_{\mathrm{sec},m,i,j} = [\tilde{R}_{A_m,i,j}+\tilde{R}_{B_m,i,j}-\tilde{R}_{E,i,j}]^+. \tag{38}$$

C. Problem Formulation

We introduce a $N \times M$ SC matrix in which the binary element $c_{m,i,j}$ denotes whether mth user pair is allocated to SC i in the MA phase and SC j in the BC phase. For energy efficient secure communication, our objective is to maximize the total secrecy sum rate of the system by setting the variables $\{c_{m,i,j}, p_{m,j}\}$. The energy efficiency of the system is formulated as

$$\eta_E(c_{m,i,j},p_{m,j}) = \frac{R_{\mathrm{sec},m,i,j}(c_{m,i,j},p_{m,j})}{P_s(c_{m,i,j},p_{m,j})} \tag{39}$$

where $P_s(c_{m,i,j},p_{m,j}) = P_c + P_T$, P_T and P_c are transmission power and the circuit power consumption, respectively. Accordingly, the energy efficiency maximization problem is defined as

$$\max_{c_{m,i,j},p_{m,j}} \sum_{m\in\mathcal{M}}\sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}} \eta_E(c_{m,i,j},p_{m,j}) \tag{40}$$

$$\begin{aligned}
\text{subject to}\ \ & C1: \sum_{m\in\mathcal{M}} c_{m,i,j} \le H, \quad \forall i\in\mathcal{N},\ \forall j\in\mathcal{N},\\
& C2: \sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}} c_{m,i,j} \le V, \quad \forall m\in\mathcal{M},\\
& C3: c_{m,i,j}\in\{0,1\},\ \forall m\in\mathcal{M},\ \forall i\in\mathcal{N},\ \forall j\in\mathcal{N},\\
& C4: R_{\mathrm{sec},m,i,j}(c_{m,i,j},p_{m,j}) \ge R_{\min},\\
& \forall m\in\mathcal{M}, \quad \forall i\in\mathcal{N},\forall j\in\mathcal{N},\\
& C5: \sum_{m\in\mathcal{M}}\sum_{j\in\mathcal{N}} p_{m,j} \le P_s,\ \forall m\in\mathcal{M},\ \forall j\in\mathcal{N},\\
& C6: p_{m,j}\ge 0, \quad \forall m\in\mathcal{M}, \quad \forall j\in\mathcal{N}.
\end{aligned} \tag{41}$$

Constraints (C1)-(C2) restrict that each SC pair can occupy at most H user pairs and each user pair can be assigned to at most V SC pairs, separately; Constraints C3 ensures user pair scheduling variables to be binary. Constraints C4 ensures the QoS for each user pair, which requests secure data rate for each user pair must be larger than the minimum user pair data rate $R_{\min}$; Constraints (C5)-(C6) constraint that power variables satisfy transmitting power of the RS; The optimization problem is a non-convex optimization problem and an NP-hard problem.

The achievable secrecy energy efficiency affected by power allocation in the BC phase. The power allocation for user A_m and on SC_j denoted as

$$p_{A_m,j} = p_n\frac{(G_{A_m,j})^{-\lambda}}{\sum_{m=1}^{M}(G_{m,j})^{-\lambda}} \tag{42}$$

where λ is a decay factor. When $\lambda = 0$, it corresponds to equal power allocation among the allocated users. When λ increases, it reflects more power is allocated to the user pair with poorer CRNN.

If we use constraint $\sum_{m\in\mathcal{M}} p_{m,j} \le P_s/N, \forall m\in\mathcal{M}, \forall j\in\mathcal{N}$ to replace constraints C2 and C5, then the optimization problem is transformed into a closed-form optimal problem, which is easy to handle. Energy efficiency problem can be rewritten as

$$\max_{c_{m,i,j},p_{m,j}} \sum_{m\in\mathcal{M}}\sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}} \eta_E(c_{m,i,j},p_{m,j}) \tag{43}$$

$$\begin{aligned}
\text{subject to}\ \ & C1: \sum_{m\in\mathcal{M}}\sum_{j\in\mathcal{N}} p_{m,j} = P_s,\\
& C2: p_{m,j}\ge 0, \quad \forall m\in\mathcal{M},\ \forall j\in\mathcal{N}\\
& C3: R_{\mathrm{sec},m,i,j}(c_{m,i,j},p_{m,j}) \ge R_{\min},\\
& \forall m\in\mathcal{M}, \quad \forall i\in\mathcal{N},\forall j\in\mathcal{N}.
\end{aligned} \tag{44}$$

III. Energy Efficient Subcarrier Matching Scheme for NOMA

A. Subcarrier Matching Problem Formulation

We first introduce the concepts of matching game, preferred matched pair, preferred matching. Considering the set of user pairs and the set of SCs as two disjoint sets of players aiming to maximize their own energy efficiency, formally presented as.

Definition 1 (Two-sided Matching [38]): Consider two disjoint sets, the user pairs $\mathcal{M} = \{1,\ldots,M\}$, the SCs $\mathcal{N} = \{1,\ldots,N\}$, a many-to-many mapping Φ, such that for every $m\in\mathcal{M}$ and $SC_i\in\mathcal{N}$.

$$\begin{aligned}
&1)\ \ \Phi(m)\subseteq\mathcal{N}, \Phi(SC_i)\subseteq\mathcal{M};\\
&2)\ \ |\Phi(SC_i)|\le H, |\Phi(m)|\le V;\\
&3)\ \ SC_i\in\Phi(m), m\in\Phi(SC_i).
\end{aligned} \tag{45}$$

Condition 1) implies that each user pair is matched with a set of SC pairs and each SC pair is matched with a set of user pairs. Condition 2) states that each SC pair can occupy at most H user pairs, and each user pair can be assigned to at most V SC pairs. To better describe the operation process of each player, Condition 3) means user m and SC_i are matched with each other.

Definition 2 (Preferred Match Pair): Given any two subcarriers $SC_i, SC_{i'} \in \mathcal{N}, i \neq i'$, any one user pair m and two matchings Φ, Φ', $SC_i \in \Phi(m), SC_{i'} \in \Phi(m)$, if $E_{m,i}(\Phi) > E_{m,i'}(\Phi')$ implies that user pair m prefers SC_i in Φ to $SC_{i'}$ in Φ'. Similarly, given any two user pairs $m, m' \in \mathcal{M}, m \neq m'$, and two matchings Φ, Φ', $m = \Phi(SC_i), m' = \Phi'(SC_i)$, if $E_{m,i}(\Phi) > E_{m',i}(\Phi')$ implies that SC_i prefers the user pairs m to m'.

Since many-to-many matching is hard to achieve stable matching, we introduce the notion of switch matching as below.

Definition 3 (Preferred Matching): Given a matching Φ with $SC_i \in \Phi(m), SC_j \in \Phi(n)$, and $SC_i \notin \Phi(n), SC_j \notin \Phi(m)$, if $E_i(m) > E_j(n)$, there exists $\Phi_{n,j}^{m,i}$;

$$SC_i \in \Phi_{n,j}^{m,i}(m), SC_j \in \Phi_{n,j}^{m,i}(n), \\ SC_i \notin \Phi_{n,j}^{m,i}(n), SC_j \notin \Phi_{n,j}^{m,i}(m) \tag{46}$$

$\Phi_{n,j}^{m,i}$ is called a preferred matching. Two user pairs in the same subset exchange their matches in the opposite subset while other matches remain unchanged. Note that if a preferred matching is approved, then at least one player's data rates will increase, and the achievable rates of any player involved will not decrease at the same time.

B. Subcarrier Assignment Algorithm for NOMA

We formulate two SC assignment algorithms (SCAS-1 and SCAS-2). In SCAS-1, we assume that a larger CRNN of the SC has a higher priority to select user pairs. The preferred matching phase in SCAS-2, the RS keeps searching for two user pairs to form a match pair, then executes the preferred matching and updates the current matching if satisfied conditions. The iterations stop until no user pairs can form a new match pair. SCAS-1 and SCAS-2 are described in detail in Algorithms 1 and 2.

Algorithm 1 Subcarrier Assignment Scheme (SCAS-1)

Based on the CSI of each SC, the RS allocates the transmission of power equally to each SC;
Initialize all of unmatched user pairs and unmatched SCs;
repeat
  if $|\Phi(SC_i)| \leq H$ **then**
    SC_i selects its most preferred unmatched user pair by using CRNNs;
  end if
  if $|\Phi(SC_i)| = H$ **then**
    Set the proportional factor of power for each user pair according to (42);
    For any two SCs SC_i and SC_j select any two user pairs m and n, respectively. $SC_i \in \Phi(m), SC_j \in \Phi(n), SC_i \notin \Phi(n), SC_j \notin \Phi(m)$;
    while $E_i(m) > E_j(n)$ **do**
      Execute preferred matching $SC_i \in \Phi(n), SC_j \in \Phi(m)$, $SC_i \notin \Phi(m), SC_j \notin \Phi(n)$;
      Update all user pairs' energy efficiency;
    end while
  end if
until Convergence

Algorithm 2 Subcarrier Assignment Scheme (SCAS-2)

Based on the CSI of each SC, the RS allocates the transmission of power equally to each SC;
Initialize all of unmatched user pairs and unmatched SCs;
repeat
  if $|\Phi(SC_i)| \leq H$ and $|\Phi(m)| \leq V$ **then**
    All of the SCs and user pairs are matched with each other arbitrarily;
  end if
  if $|\Phi(SC_i)| = H$ **then**
    Set $E_{\mathrm{sec,max}} = E_{\mathrm{sec},total}(\Phi)$;
    while $\ell < L_m$ **do**
      Two user pairs (m, n) and SCs (SC_i, SC_j) are selected with $SC_i \in \Phi(m), SC_j \in \Phi(n)$,$SC_i \notin \Phi(n), SC_j \notin \Phi(m)$;
      while $E_{\mathrm{sec},tatol}(\Phi_{n,j}^{m,i}) > E_{\mathrm{sec,max}}$ **do**
        Execute preferred matching $\Phi_{n,j}^{m,i}$;
        Set $E_{\mathrm{sec,max}} = E_{\mathrm{sec},tatol}(\Phi_{n,j}^{m,i})$;
        $\ell = \ell + 1$;
      end while
    end while
  end if
until Convergence

IV. Energy Efficient Power Allocation Scheme for NOMA

As mentioned in Section III, we investigate the SC assignment scheme in the two-way relay NOMA network. In order to further improve the system energy efficiency, we design user pairs' power allocation algorithm instead of equal power allocation. In this section, we introduce GP programming approach and discuss its effects of different power proportional factor on the energy efficiency of the system.

A. Energy Efficient Power Allocation Algorithm for NOMA

The objective function in (43) is non-convex. We introduce the parameter transformation to avoid high complexity of the solution. We assume that the proportion of the power is assigned on SC i in the MA phase and on SC j in the BC phase, denoted by $u_{i,j}$. We can formula the non-convex optimization problem as GP [35]. Therefore, the energy efficiency maximization for power allocation problem can rewrite as

$$u_E = \max \frac{R_{\mathrm{sec},m,i,j}(c_{m,i,j}, p_{m,j})}{P_s(c_{m,i,j}, p_{m,j})} \tag{47}$$

$$\min u_{i,j} P_s(c_{m,i,j}, p_{m,j}) - R_{\mathrm{sec},m,i,j}(c_{m,i,j}, p_{m,j}) \tag{48}$$

$$\text{subject to} \quad C1: \sum_{m\in\mathcal{M}}\sum_{j\in\mathcal{N}} p_{m,j} = P_s,$$
$$C2: p_{m,j} \geq 0, \quad \forall m \in \mathcal{M}, j \in \mathcal{N}$$
$$C3: R_{\text{sec},m,i,j}(c_{m,i,j}, p_{m,j}) \geq R_{\min},$$
$$\forall m \in \mathcal{M}, \quad \forall i \in \mathcal{N}, \forall j \in \mathcal{N}$$
$$C4: \sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}} u_{i,j} = 1. \tag{49}$$

In the following, an iterative resource allocation algorithm for power allocation can be proposed. Due to the objective function is linear and the constraints are convex, we can utilize interior point methods to solve the global-optimal problem [36] [37]. The secrecy energy efficiency significantly improves for each iteration in algorithm 3.

Algorithm 3 Power Allocation Algorithm

1: Based on the CSI of each SC, the RS allocates the transmission of power equally to each SC;
2: Initialize the maximum tolerance ε and the number of iterations ℓ and the maximum number of iterations L_m;
3: **while** $|R_{\text{sec},m,i,j} - u_E P_s| > \varepsilon$ or $\ell \leq L_m$ **do**
4: Update p by solving the formulated problem in (48) and (49) using the interior point methods;
5: $\ell = \ell + 1$;
6: **end while**

B. Stability, Convergence and Complexity

We give remarks on the stability, convergence and complexity for proposed SSPA schemes.

1) Stability: When no user pair $m \in \mathcal{M}$ can find another user pair $n \in \mathcal{M}$ to match with each other, we regard the proposed SSPA convergence as the best choice for current matching. There is any user pair cannot improve its utility by using to change its matches. Hence, the terminal matching Φ^* is two-sided exchange stable matching, which guarantees the proposed SSPA schemes to remain stable.

2) Convergence: Convergence of SSPA algorithms depend on preferred matching and power allocation by using interior point methods.

1) After a number of match operations for one time power allocation:

We assume that the preferred matching are (Am, Bm) and (An, Bn) with $\Phi_\ell = \Phi_{\ell-1}{}^{mi}_{nj}$. We ensure that the utility of SC_p and SC_q satisfies $E_{SC_p}(\Phi_\ell) \geq E_{SC_p}(\Phi_{\ell-1})$ and $E_{SC_q}(\Phi_\ell) \geq E_{SC_q}(\Phi_{\ell-1})$ after each preferred matching. Hence, the total secrecy energy efficiency increase after each match operation ℓ. There exists a preferred matching after which the total secrecy energy efficiency stops increasing for one time power allocation.

2) After power allocation for the SSPA algorithms:

The total energy efficiency will increase after a number of iterations. Due to the limited spectrum resource the total secrecy energy efficiency has an upper limit. Hence, the total secrecy energy efficiency will stop increasing after a limited number of iterations. Therefore, the proposed SSPA algorithms for secure resource allocation is guaranteed to converge.

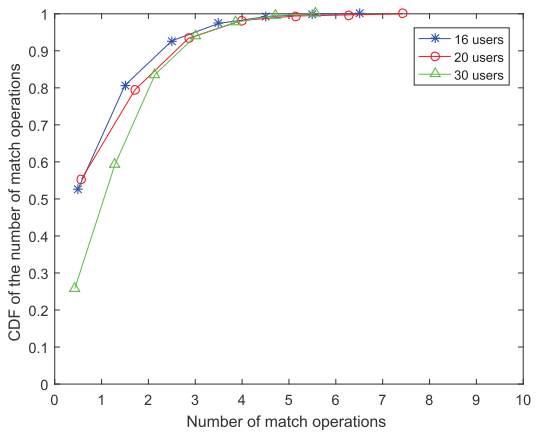

Fig. 2. Number of match operations vs. the number of users.

3) Complexity

The complexity of the proposed SSPA-1 algorithm is $O(PSMHV(N-V)M^2)$. When $|\Phi(SC_i)| \leq H$. The complexity mainly produces in the process of using the CRNN, which is O(M^2). For user pair m, there exist $V(N-V)$ possible combinations of SC_i and SC_j in $\Phi^{m,i}_{n,j}$ need to be considered. For the SC_i, the preferred matching $\Phi^{m,i}_{n,j}$ with m has $HV(N-V)$ possible combinations. There are $\frac{1}{2}MHV(N-V)$ preferred matchings need to be considered for M user pairs in each iteration. The number of total match iterations is S and power allocation iterations is P. The computational complexity of SSPA-1 can be presented by $O(PSMHV(N-V)M^2)$. Similar analysis can be performed for the proposed SSPA-2 algorithm and the complexity of which is $O(PSMHV(N-V)N^{H+1})$.

V. Simulation Results and Discussion

In this section, we evaluate the performance of the proposed SSPA schemes with both SCAS-1 and SCAS-2 applied, and compare its performance with a random allocation scheme (RA-NOMA). We assume that two adjacent users are considered as a user pair, which selects the same SC. Each SC can be assigned to at most $H = 3$ user pairs, and each user pair can occupy at most $V = 4$ SCs. In the RA-NOMA scheme, the SCs is randomly allocated to the user pairs satisfying $H \leq 3$ and $V \leq 4$. For the simulations, the total of RSs peak power Ps is 46dBm, system bandwidth is 4.5MHz and the transmit power for each user is $P_{A_m} = 300mW, P_{B_m} = 300mW$ on the uplink. We assume that noise power spectral density is -150 dBm/Hz, circuit power consumption $P_c =$ 1dB and eavesdropper is allocated at a distance of 500 m from the RS, if there is no special instructions. Pass loss functions can be obtained by hata urban propagation model [39]. The coverage radius of the RS is $r = 30$ m and user pairs are evenly distributed in a circle around the central RS. Considering the computational complexity, we assume that there are 10 SCs in the NOMA wireless network.

Fig. 2 shows the cumulative distribution function (C.D.F.) of the total number of iterations for the SCAS-1 to convergence. To evaluate the performance of the proposed SCAS-1 scheme, we adopt (42) power allocation scheme for each user. Note

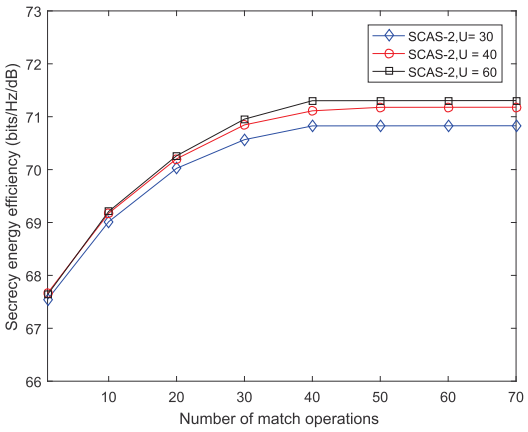

Fig. 3. C.D.F. of the number of match operations in SCAS-2.

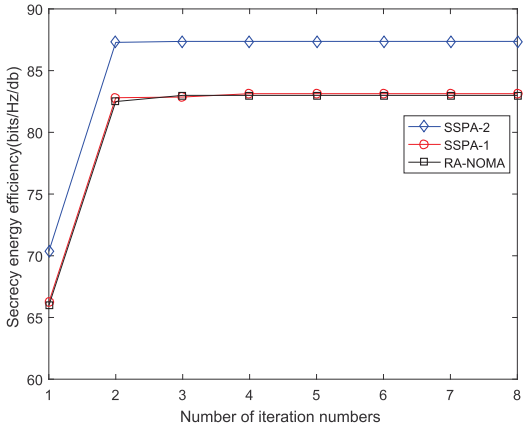

Fig. 4. Secrecy energy efficiency vs. number of iterations.

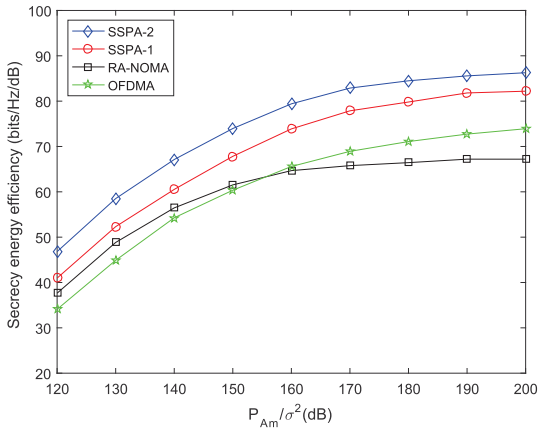

Fig. 5. Secrecy energy efficiency vs. P_{A_m}/σ^2.

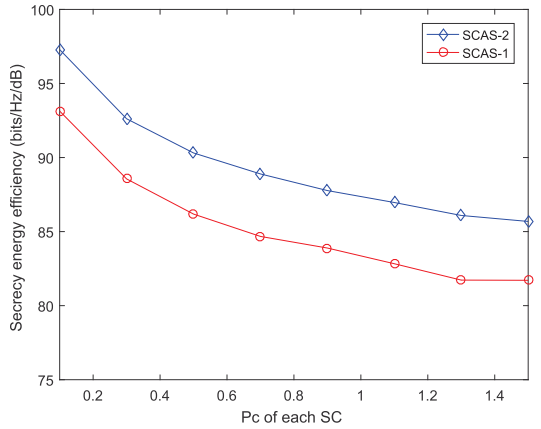

Fig. 6. Secrecy energy efficiency vs. Pc of each SC.

that the random variable $\mathcal{Y}$ is the total number of match numbers required for the SCAS-1. With the number of the user pairs increasing, the speed of convergence becomes slower. In addition, the proposed SCAS-1 converges within 2-10 match operations and further reflecting the relatively low computational complexity.

Fig. 3 shows secrecy energy efficiency performance vs. the number of match operations in the SCAS-2 scheme. When users become larger, the number of match operations become higher due to more user pairs have the opportunity to be serviced by the RS. From Fig. 3, we can see energy efficiency increases with the match operation number increasing within 40 match operations. The energy efficiency closes to a relatively stable level when match operation number over 40 match operations which implies the proposed SCAS-2 scheme also has a low complexity.

Fig. 4 illustrates the secrecy energy efficiency performance vs. the number of iterations for the proposed algorithm 3. We can see that the proposed SSPA algorithms based power allocation algorithm (Algorithm 3) takes at most 10 iterations to converge. The energy efficiency goes up sharply with 1 iteration, and then it closes to a relatively stable level when the number of iterations over 1 time. However, although the SSPA-2 scheme show a higher iteration than SSPA-1 scheme and RA-NOMA scheme, it provides a higher secrecy energy efficiency than the other schemes.

Fig. 5 illustrates the secrecy energy efficiency performance vs. P_{A_m}/σ^2 for the two SSPA proposed schemes and RA-NOMA scheme. As the P_{A_m}/σ^2 grows, the secrecy energy efficiency continues to increase, but the growth rate slows down. When P_{A_m}/σ^2 over 155 db, the cochannel interference seriously affected the performance of the system the RA-NOMA scheme is worse than the OFDMA scheme. From Fig. 5, we can also see that both SSPA-1 scheme and SSPA-2 scheme have better performance than RA-NOMA scheme, proving that SSPA schemes effectively improve the system's secrecy energy efficiency. Meanwhile, since SSPA-2 provides more freedom in the SC allocation than the randomly predefined user pairs in the SSPA-1, the SSPA-2 scheme thoroughly outperforms the SSPA-1 scheme.

Fig. 6 depicts the secrecy energy efficiency of the proposed SSPA schemes and RA-NOMA scheme vs. circuit power consumption of each SC. The circuit power consumption for each SC is set from 0.1 dB to 1.5 dB. As shown in this figure, we can be observed that the secrecy energy efficiency decreases with a grow of circuit power consumption. The main factor is that more energy is consumed by the circuit, the energy used for signal transmission will be greatly reduced. Thus, as expected, the circuit power consumption can degrade the secrecy energy efficiency performance.

Fig. 7 depicts the secrecy energy efficiency performance vs. σ^2 for the two SSPA proposed schemes and RA-NOMA

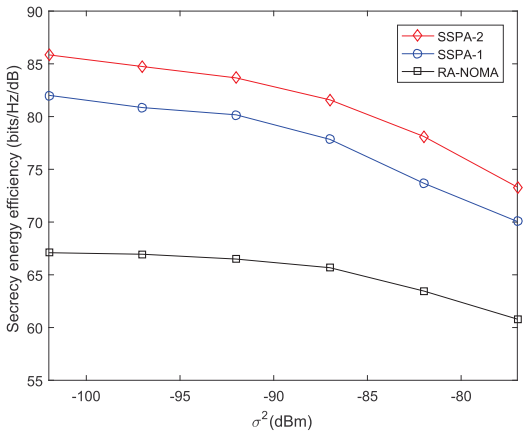

Fig. 7. Secrecy energy efficiency vs. σ^2.

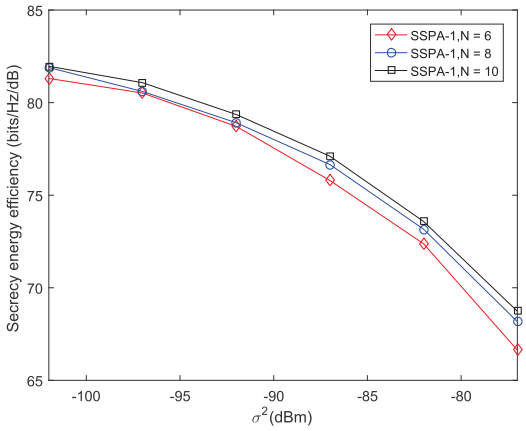

Fig. 8. Secrecy energy efficiency vs. σ^2.

scheme with CJ. Under the CJ scenario, we propose generating AN at the RS for further enhancing the secrecy performance. The performance of the proposed SSPA-2 scheme for the NOMA wireless network achieves higher energy efficiency than that of SSPA-1 scheme as well as RA-NOMA scheme. Fig. 7 demonstrates that the secrecy energy efficiency is remarkably deteriorated by the additive white Gaussian noise. Therefore, σ^2 increases, as a result, the secrecy energy efficiency decrease. The secrecy energy efficiency obtained from the proposed SSPA-1 scheme drops down fast for σ^2 over -90 dBm, and less so fast σ^2 within -90 dBm.

Fig. 8 shows the secrecy energy efficiency performance vs. σ^2 for $N = 6$, $N = 8$, $N = 10$ in SSPA-1 with CJ. As observed in Fig. 8, The energy efficiency decreases sharply with the σ^2 increases. Obviously, when secrecy energy efficiency increases with the number of SCs N grows, due to the more user pairs be allocated over SCs.

Fig. 9 shows the secrecy energy efficiency performance vs. σ^2 for different value of user pairs in SSPA-2 with CJ. Similar to Fig. 7 and Fig. 8 show that the secrecy energy efficiency in NOMA wireless network deceases when σ^2 increased. It can be observed from the figure, the more number of user pairs in the NOMA wireless network is, the better of the performance is obtained. The main reason is that, as the number of the total SC is fixed as N, with the

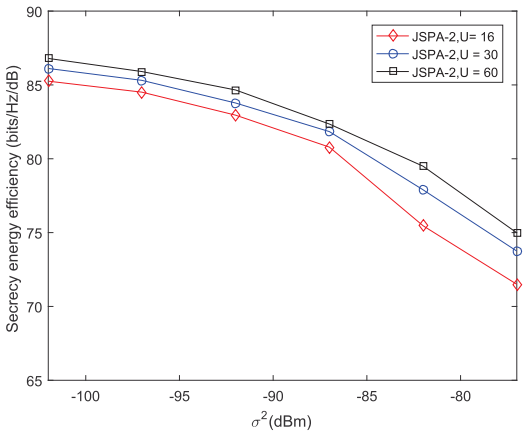

Fig. 9. Secrecy energy efficiency vs. σ^2.

increase of the number of user pairs, the more diversity gains over SCs.

VI. Conclusion

In this paper, we investigated the secure SC assignment and power allocation for the NOMA two-way relay wireless networks in the presence of an eavesdropper without and with CJ. The proposed SSPA algorithms with SCAS applied properly allocate resources to user pairs, and the performance of secrecy energy efficiency of the system can be significantly improved than the RA-NOMA scheme. Moreover, the SSPA-2 scheme thoroughly outperforms the SSPA-1 scheme.

References

[1] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[2] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[3] Y. Gao, B. Xia, K. Xiao, Z. Chen, X. Li, and S. Zhang, "Theoretical analysis of the dynamic decode ordering SIC receiver for uplink NOMA systems," *IEEE Commun. Lett.*, vol. 21, no. 10, pp. 2246–2249, Oct. 2017.

[4] B. Xu, Y. Chen, J. R. Carrión, and T. Zhang, "Resource allocation in energy-cooperation enabled two-tier NOMA HetNets toward green 5G," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2758–2770, Dec. 2017.

[5] S. Mumtaz, J. M. Jornet, J. Aulin, W. H. Gerstacker, X. Dong, and B. Ai, "Terahertz communication for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5617–5625, Jul. 2017.

[6] J. Choi, "Effective capacity of NOMA and a suboptimal power control policy with delay QoS," *IEEE Trans. Commun.*, vol. 65, no. 4, pp. 1849–1858, Apr. 2017.

[7] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.

[8] X. Zhang, Q. Gao, C. Gong, and Z. Xu, "User grouping and power allocation for NOMA visible light communication multi-cell networks," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 777–780, Apr. 2017.

[9] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3614–3628, Aug. 2017.

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

[11] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[13] Y. Wu, S. Jin, X. Gao, M. R. McKay, and C. Xiao, "Transmit designs for the MIMO broadcast channel with statistical CSI," *IEEE Trans. Signal Process.*, vol. 62, no. 17, pp. 4451–4466, Sep. 2014.
[14] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.
[15] Y. Wu, S. Jin, X. Gao, C. Xiao, and M. R. McKay, "MIMO multichannel beamforming in Rayleigh-product channels with arbitrary-power co-channel interference and noise," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3677–3691, Oct. 2012.
[16] L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming-aided secrecy enhancement in P2P communications with social interaction constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1144–1158, Feb. 2017.
[17] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, Dec. 2015.
[18] 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.
[19] P.-H. Lin, F. Gabry, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Multi-phase smart relaying and cooperative jamming in secure cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 1, pp. 38–52, Mar. 2016.
[20] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.
[21] H. Long, W. Xiang, and Y. Li, "Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1309–1318, Jun. 2017.
[22] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10732–10747, Dec. 2017.
[23] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4457–4462, May 2017.
[24] Y. Sun, D. W. K. Ng, Z. Ding, and R. Schober, "Optimal joint power and subcarrier allocation for full-duplex multicarrier non-orthogonal multiple access systems," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1077–1091, Mar. 2017.
[25] L. Lei, D. Yuan, C. K. Ho, and S. Sun, "Power and channel allocation for non-orthogonal multiple access in 5G systems: Tractability and computation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8580–8594, Dec. 2016.
[26] S. M. A. Kazmi *et al.*, "Mode selection and resource allocation in device-to-device communications: A matching game approach," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3126–3141, Nov. 2017.
[27] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 885–899, Feb. 2017.
[28] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis, and A. Nallanathan, "Energy efficient resource allocation for secure NOMA networks," in *Proc. VTC-Spring*, Porto, Portugal, 2018, pp. 1–6.
[29] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.
[30] D. Han, B. Bai, and W. Chen, "Secure V2V communications via relays: Resource allocation and performance analysis," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 342–345, Jun. 2017.
[31] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[32] 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.
[33] 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.
[34] 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.
[35] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optim. Eng.*, vol. 8, no. 1, pp. 67–127, 2007.
[36] S. Boydl, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[37] B. Di, L. Song, and Y. Li, "Sub-channel assignment, power allocation, and user scheduling for non-orthogonal multiple access networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7686–7698, Nov. 2016.
[38] A. E. Roth and M. A. O. Sotomayor, *Two-Sided Matching: A Study in Game-Theoretic Modeling and Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[39] *Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations, Release 12*, document 3GPP TR 25.996, Sep. 2014.
[40] G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi, *Complexity and Approximation: Combinatorial Optimization Problems and Their Approximability Properties*. New York, NY, USA: Springer, 2003.
[41] M. Sipser, *Introduction to the Theory of Computation*. Boston, MA, USA: Cengage Learning, 2012.

Haijun Zhang (M'13–SM'17) was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada. From 2011 to 2012, he visited the Centre for Telecommunications Research, King's College London, London, U.K., as a Visiting Research Associate. He is currently a Full Professor with the University of Science and Technology Beijing, China. He received the IEEE ComSoc Young Author Best Paper Award in 2017. He serves/served as a General Co-Chair for GameNets'16, and a Symposium Chair for Globecom'19, a TPC Co-Chair for the INFOCOM 2018 Workshop on Integrating Edge Computing, Caching, and Offloading in Next Generation Networks, a General Co-Chair for the ICC 2018 (ICC 2017, GLOBECOM 2017) Workshop on 5G Ultra Dense Networks, and a General Co-Chair for the GLOBECOM 2017 Workshop on LTE-U. He serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE 5G TECH FOCUS, and the *EURASIP Journal on Wireless Communications and Networking*, and serves/served as a Leading Guest Editor for *IEEE Communications Magazine* and the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING.

Ning Yang is currently pursuing the Ph.D. degree with the University of Science and Technology Beijing, China. Her research interests include resource allocation, power control, energy efficiency in wireless communications, software-defined wireless networks, fog wireless access networks, and slicing networks. She serves as a Reviewer for *IEEE Communications Magazine*.

Keping Long (SM'06) received the M.S. and Ph.D. degrees from the University of Electronic Science and Technology of China, Chengdu, in 1995 and 1998, respectively.

From 1998 to 2000, he was a Post-Doctoral Research Fellow at the National Laboratory of Switching Technology and Telecommunication Networks, Beijing University of Posts and Telecommunications, China, where he was an Associate Professor from 2000 to 2001. From 2001 to 2002, he was a Research Fellow with the ARC Special Research Centre for Ultra Broadband Information Networks, The University of Melbourne, Australia. He is currently a Professor and the Dean with the School of Computer and Communication Engineering, University of Science and Technology Beijing. He has published over 200 papers, 20 keynote speeches, and invited talks at international and local conferences. His research interests include optical Internet technology, new-generation network technology, wireless information networks, value-added services, and secure technology of networks.

Dr. Long received the National Science Fund for Distinguished Young Scholars of China in 2007 and selected as the Chang Jiang Scholars Program Professor of China in 2008. He has been a TPC or ISC Member of COIN 2003–2010, IEEE IWCN2010, ICON2004/2006, and APOC2004/06/08, a Co-Chair of the organization Committee for IWCMC2006, a TPC Chair of COIN 2005/08, and a TPC Co-Chair of COIN 2008/10. He is a member of the Editorial Committees of *Sciences in China Series F* and *China Communications*.

Miao Pan (S'07–M'12) received the B.Sc. degree in electrical engineering from the Dalian University of Technology, China, in 2004, the M.A.Sc. degree in electrical and computer engineering from the Beijing University of Posts and Telecommunications, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2012. He was an Assistant Professor in computer science with Texas Southern University from 2012 to 2015. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Houston. His research interests include cognitive radio networks, cyber-physical systems, and cybersecurity. He received the Best Paper Awards in GLOBECOM 2017 and GLOBECOM 2015, respectively. He is currently an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Greece. He received the University Diploma (5 years) and Ph.D. degrees in electrical and computer engineering from the University of Patras in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In 2004, he joined the Faculty of the Aristotle University of Thessaloniki, Greece, where he is currently a Professor with the Electrical and Computer Engineering Department and the Director of the Digital Telecommunications Systems and Networks Laboratory. He is also an Honorary Professor with Southwest Jiaotong University, Chengdu, China.

His research interests include digital communications systems and signal processing, with emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, molecular and nanoscale communications, stochastic processes in biology, and wireless security. He has authored or co-authored of over 450 technical papers published in scientific journals and presented at international conferences. He is also an author of the Greek edition of a book on telecommunications systems and a co-author of the book *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012).

Dr. Karagiannidis has been involved as a general chair, a technical program chair, and a member of Technical Program Committees in several IEEE and non-IEEE conferences. In the past, he was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, a Senior Editor of the IEEE COMMUNICATIONS LETTERS, an Editor of the *EURASIP Journal of Wireless Communications and Networks* and several times a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. From 2012 to 2015, he was the Editor-in-Chief of the IEEE COMMUNICATIONS LETTERS.

Dr. Karagiannidis is one of the highly cited authors across all areas of electrical engineering, recognized as the 2015, 2016, and 2017 Web-of-Science Highly Cited Researcher.

Victor C. M. Leung (S'75–M'89–SM'97–F'03) is currently a registered Professional Engineer in the Province of British Columbia, Canada. He is a fellow of the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He received the IEEE Vancouver Section Centennial Award and the 2011 UBC Killam Research Prize. He was a recipient of the 2017 Canadian Award for Telecommunications Research. He has co-authored papers that received the 2017 IEEE ComSoc Fred W. Ellersick Prize and the 2017 IEEE Systems Journal Best Paper Award. He has served on the Editorial Boards of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS–Wireless Communications Series and Series on Green Communications and Networking, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMPUTERS, and the *Journal of Communications and Networks*. He is serving on the Editorial Boards of the IEEE WIRELESS COMMUNICATIONS LETTERS, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the IEEE ACCESS, *Computer Communications*, and several other journals. He has guest-edited many journal special issues, and provided leadership to the organizing committees and technical program committees of numerous conferences and workshops.