Energy Efficient Resource Allocation for Secure NOMA Networks

Ning Yang[†], Haijun Zhang[†], Keping Long[†], Miao Pan[‡], George K. Karagiannidis[§], Arumugam Nallanathan[¶]

[†]Beijing Engineering and Technology Research Center for Convergence Networks and Ubiquitous Services,
University of Science and Technology Beijing, Beijing, China

[‡] University of Houston, Houston, TX, USA

[§] Aristotle University of Thessaloniki, Thessaloniki, Greece

[¶] Queen Mary University of London, London, U.K.

***Abstract*—In this paper, we investigate the joint subcarrier (SC) assignment and power allocation problem for non-orthogonal multiple access (NOMA) amplify-and-forward two-way relay wireless networks. 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 (CSI) 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 (GP) problem, and then solved by interior point methods. Simulation results demonstrate that the effectiveness of the proposed SSPA algorithms.**

I. Introduction

Recently, non-orthogonal multiple access (NOMA) has been considered as a promising solution to significantly improve energy efficiency for wireless communications [1]. The main advantage of NOMA is that it simultaneously serves multiple users over the same subcarrier (SC) to increase the system throughput. 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 scheduling straegies to achieve a good spectral efficiency and energy efficiency performance [2].

Meanwhile, physical layer security has drawn much attention in wireless networks. 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[3]. Specifically, secrecy capacity can be enhanced by exploiting multiple antennas additional spatial degrees of freedom in multiple-input-multiple-output (MIMO) wiretap channel [4]. Furthermore, researchers applied robust beamforming transmission technique, artificial noise (AN), and Multi-antenna relay scheme to improve physical layer security [5–7].

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 [8], Lagrangian duality theory [9], and matching theory [10]. Besides the maximization of sum rate, resource allocation with security considerations for NOMA networks have also been addressed in the existing works. However, secure resource allocation has not been well studied for NOMA two-way relay wireless networks. These motivated our work.

In this paper, we consider secrecy energy efficiency maximization based amplify-and-forward (AF) two-way relay wireless networks. A matching algorithm SCAS-1 is proposed for SC assignment to improve the secrecy energy efficiency. To achieve high secrecy energy efficiency of the system, SCAS-2 scheme is proposed. Additional, a novel power allocation scheme is put forward for the power allocation 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. Simulation results verify the derived theoretical analytical results and demonstrate the performance superiority of the proposed SSPA schemes in terms of the average secrecy.

The rest of this paper is organized as follows. Section II provides the system model of secure resource allocation. In Section III, secrecy energy efficiency for NOMA wireless network. In Section IV, performance of the proposed algorithms are evaluated by simulations. Finally, Section VI concludes the paper.

II. System Model

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. AF protocol is considered in this study which is divided into two phases: the multiple access (MA) phase and the broadcast (BC) phase. All user pairs do simultaneous wireless information 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. Block fading channel is assumed to be flat and composed of distance-dependent path

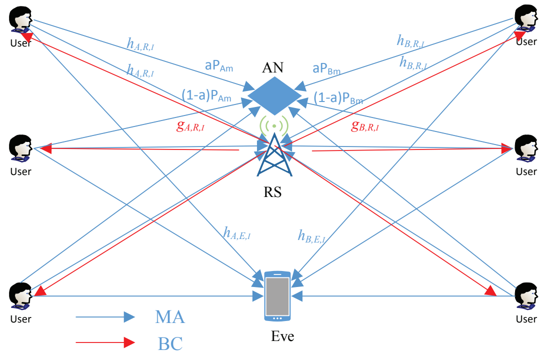

Fig. 1. System model of the security transmission in two-way relay wireless network.

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 at the RS on SC i is given by

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

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 assumed to be cyclic symmetric complex Gaussian (CSCG) random variables denoted by $s_{A_m,i}\sim\mathcal{CN}(0,1)$ and $s_{B_m,i}\sim\mathcal{CN}(0,1)$ separately; $n_{RS,i}\sim\mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the RS on SC i. The total transmit powers 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 on SC i at the eavesdropper can be expressed as

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

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 at the eavesdropper on SC i.

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 given by $\alpha_i=\sqrt{\sum\limits_{m\in\mathcal{K}}(P_{A_m,i}|h_{A_m,R,i}|^2+P_{B_m,i}|h_{B_m,R,i}|^2)+\sigma^2}$. The total transmit powers of RSs are constrained by $\sum\limits_{j=1}^{N}P_{R,j}\le P_{\mathrm{R}}$. The received signal on SC j at A_m is thus $y_{A_m,i,j}=\sqrt{P_{R,j}}g_{A_m,j}y_{RS,i}/\alpha_i+n_{A_m,j}$, which can be further given by

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

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

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

where $g_{A_m,j}$ and $g_{B_m,j}$ are the channel gains from the RS to the mth user pair A_m and B_m on SC j, respectively; and $n_{A_m,j}$ and $n_{B_m,j}$ are separately, AWGNs on SC j at A_m and B_m 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 on SC j at the eavesdropper in the BC phase can be expressed as

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

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, which share SC i in the MA phase and SC j in the BC phase, can be respectively given by

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

and

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

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

Based on (2) and (5), the received signal over the two phases at 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

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

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

$$\begin{array}{l} I_{A_m} = \sum\limits_{m \in \mathcal{K}} (P_{R,j}|g_{A_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{A_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\ -(P_{R,j}|g_{A_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{A_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\ I_{B_m} = \sum\limits_{m \in \mathcal{K}} (P_{R,j}|g_{B_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{B_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\ -(P_{R,j}|g_{B_m,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{B_m,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \end{array}. \tag{8}$$

$$\begin{array}{l} ET = \sum\limits_{m \in \mathcal{K}} (P_{A_m,i}|h_{A_m,E,i}|^2 + P_{B_m,i}|h_{B_m,E,i}|^2) - (P_{A_m,i}|h_{A_m,E,i}|^2 + P_{B_m,i}|h_{B_m,E,i}|^2) + \sigma^2 \\ ER = \sum\limits_{m \in \mathcal{K}} (P_{R,j}|g_{E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{E,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) \\ -(P_{R,j}|g_{E,j}|^2 P_{A_m,i}|h_{A_m,R,i}|^2/\alpha_i^2 + P_{R,j}|g_{E,j}|^2 P_{B_m,i}|h_{B_m,R,i}|^2/\alpha_i^2) + (P_{R,j}|g_{E,j}|^2/\alpha_{m,i}^2)\sigma^2 \end{array}. \tag{9}$$

$$\begin{array}{l} n_E = \left[\begin{array}{cc} n_{A_m,i} & n_{B_m,i} \end{array} \right]^T \\ n_{A_m,i} = \sum\limits_{m \in \mathcal{K}} (h_{1,A_m} + h_{1,B_m}) + n_{E,i} - (h_{1,A_m} + h_{1,B_m}) \\ n_{B_m,i} = \sum\limits_{m \in \mathcal{K}} (h_{2,A_m} + h_{2,B_m}) + \sqrt{P_{R,j}} g_{E,j} n_{RS,i}/\alpha_i \\ + n_{E,j} - (h_{2,A_m} + h_{2,B_m}) \end{array}. \tag{13}$$

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, since (10) is equivalent to a 2-by-2 point-to-point MIMO system with transmit signals $s = \left[\begin{array}{ccccc} s_{A_1,i} & s_{B_1,i} & \ldots & s_{A_m,i} & s_{B_m,i} \end{array} \right]^T$, denoted by $\boldsymbol{s} \sim \mathcal{CN}(0, \boldsymbol{I})$. The maximum achievable received signal for the eavesdropper is defined as [11, Chap. 8]

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

where

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

ET and ER are given by (9) at the top of this page. Note that $\mathbb{E}[\cdot]$ denotes the statistical average and the factor $\frac{1}{2}$ in (16) accounts for the two phases in a complete transmission slot. The achievable rate $R_{E,i,j}$ given in (16) is an upper-bound capacity for the eavesdropper when it has full CSI of the legitimate users, i.e., $h_{A_m,R,i}$ and $h_{B_m,R,i}$. Hence, the worst-case secrecy sum rate for the mth users over the SC pair (i,j) is expressed as

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

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

A. 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

$$\eta_E(c_{m,i,j}, p_{m,j}) = \frac{R_{\sec,m,i,j}(c_{m,i,j}, p_{m,j})}{P_s(c_{m,i,j}, p_{m,j})} \tag{19}$$

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

$$\max_{c_{m,i,j}, p_{m,j}} \sum_{m \in \mathcal{M}} \sum_{i \in \mathcal{N}} \sum_{j \in \mathcal{N}} \eta_E(c_{m,i,j}, p_{m,j}) \tag{20}$$

$$\begin{array}{ll} \text{subject to} & C1: \sum\limits_{m \in \mathcal{M}} c_{m,i,j} \le H, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}, \\ & C2: \sum\limits_{i \in \mathcal{N}} \sum\limits_{j \in \mathcal{N}} c_{m,i,j} \le V, \forall m \in \mathcal{M}, \\ & C3: c_{m,i,j} \in \{0,1\}, \forall m \in \mathcal{M}, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}, \\ & C4: R_{\sec,m,i,j}(c_{m,i,j}, p_{m,j}) \ge R_{\min}, \\ & \forall m \in \mathcal{M}, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}, \\ & C5: \sum\limits_{m \in \mathcal{M}} \sum\limits_{j \in \mathcal{N}} p_{m,j} \le P_s, \forall m \in \mathcal{M}, \forall j \in \mathcal{N}, \\ & C6: p_{m,j} \ge 0, \forall m \in \mathcal{M}, \forall j \in \mathcal{N}. \end{array} \tag{21}$$

Constraints (C1)-(C2) restrict that each SC pair can only be assigned to at most H user pairs and each user pair can only occupy 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 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 BC phase. The power allocation for user A_m and on SC_j denoted by

$$p_{A_m,j} = p_n \frac{(G_{A_m,j})^{-\lambda}}{\sum\limits_{m=1}^{M} (G_{m,j})^{-\lambda}} \tag{22}$$

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 $\sum_{m\in\mathcal{M}} p_{m,j} \leq P_s/N, \forall m \in \mathcal{M}, \forall j \in \mathcal{N}$ 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

$$\max_{c_{m,i,j},p_{m,j}} \sum_{m\in\mathcal{M}} \sum_{i\in\mathcal{N}} \sum_{j\in\mathcal{N}} \eta_E(c_{m,i,j}, p_{m,j}) \tag{23}$$

$$\begin{aligned} \text{subject to} \quad & C1: \sum_{m\in\mathcal{M}} \sum_{j\in\mathcal{N}} p_{m,j} = P_s, \\ & C2: p_{m,j} \geq 0, \forall m \in \mathcal{M}, \forall j \in \mathcal{N} \\ & C3: R_{\text{sec},m,i,j}(c_{m,i,j}, p_{m,j}) \geq R_{\min}, \\ & \forall m \in \mathcal{M}, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}, \end{aligned} \tag{24}$$

.

III. Secure Energy Efficient For NOMA

A. Subcarrier Matching For NOMA

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) 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 $SC_i \in \mathcal{N}$.

$$\begin{aligned} &1) \Phi(m) \subseteq \mathcal{N}, \Phi(SC_i) \subseteq \mathcal{M}; \\ &2) |\Phi(SC_i)| \leq H, |\Phi(m)| \leq V; \\ &3) SC_i \in \Phi(m), m \in \Phi(SC_i). \end{aligned} \tag{25}$$

Condition 1) implies that each user pair is matched with a subset of SC pairs and each SC pair is matched with a subset of user pairs. Condition 2) states that each SC pair can only be assigned to at most H user pairs, and each user pair can only occupy 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, if there exist $SC_i \in \Phi(m), SC_j \in \Phi(n)$, and $SC_i \notin \Phi(n), SC_j \notin \Phi(m)$ such that:

$$\begin{aligned} &1) \Phi_{n,j}^{m,i} = \Phi \backslash \{(m, SC_i), (n, SC_j)\} \cup \{(n, SC_i),; \\ &(m, SC_j)\} \\ &2) SC_i \in \Phi_{n,j}^{m,i}(m), SC_j \in \Phi_{n,j}^{m,i}(n), \\ &SC_i \notin \Phi_{n,j}^{m,i}(n), SC_j \notin \Phi_{n,j}^{m,i}(m) \end{aligned} \tag{26}$$

$\Phi_{n,j}^{m,i}$ is called a preferred matching. Two user pairs in the same set exchange their matches in the opposite set 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. The algorithms are described in detail in Table I and Table II as follow.

Algorithm 1 Subcarrier Assignment Scheme (SCAS-1)

```
Based on the CSI of each SC, the RS allocates the transmitted power equally to each SC;
Initialize the set of unmatched user pairs and the set of unmatched SCs;
repeat
  if |Φ(SC_i)| ≤ H then
    SC_i matches with its most preferred subset of user pair which is not fully matched according to CRNNs;
  end if
  if |Φ(SC_i)| = H then
    Set power proportional factor for each user pair by using (22);
    For any two SCs SC_i and SC_j select any two user pairs m and n, respectively. SC_i ∈ Φ(m), SC_j ∈ Φ(n), SC_i ∉ Φ(n), SC_j ∉ Φ(m);
    while E_i(m) > E_j(n) do
      Execute preferred matching SC_i ∈ Φ(n), SC_j ∈ Φ(m), SC_i ∉ Φ(m), SC_j ∉ Φ(n);
      Update all user pairs' energy efficiency;
    end while
  end if
until Convergence
```

B. Energy Efficient Power Allocation Scheme For NOMA

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 can formula the non-convex optimization problem as GP. Therefore, the energy efficiency maximization for power allocation problem can rewrite as

$$u_E = \max \frac{R_{\text{sec},m,i,j}(c_{m,i,j}, p_{m,j})}{P_s(c_{m,i,j}, p_{m,j})} \tag{27}$$

Algorithm 2 Subcarrier Assignment Scheme (SCAS-2)

Based on the CSI of each SC, the RS allocates the transmitted power equally to each SC;
Initialize the set of unmatched user pairs and the set of unmatched SCs;
repeat
  User pairs and SCs are randomly matched with each other subject to $|\Phi(SC_i)| \leq H$ and $|\Phi(m)| \leq V$;
  Set $E_{\sec,\max} = E_{\sec,total}(\Phi)$;
  while $\ell < L_m$ **do**
    Randomly select two user pairs (m,n) and SCs (SC_i, SC_j) such that $SC_i \in \Phi(m), SC_j \in \Phi(n)$,$SC_i \notin \Phi(n), SC_j \notin \Phi(m)$;
    while $E_{\sec,tatol}(\Phi_{n,j}^{m,i}) > E_{\sec,\max}$ **do**
      Execute preferred matching $\Phi_{n,j}^{m,i}$;
      Set $E_{\sec,\max} = E_{\sec,tatol}(\Phi_{n,j}^{m,i})$;
      $\ell = \ell + 1$;
    end while
  end while
until Convergence

$$\min u_{i,j} P_s(c_{m,i,j}, p_{m,j}) - R_{\sec,m,i,j}(c_{m,i,j}, p_{m,j}) \tag{28}$$

$$\begin{aligned} \text{subject to} \quad & C1: \sum_{m\in\mathcal{M}} \sum_{j\in\mathcal{N}} p_{m,j} = P_s, \\ & C2: p_{m,j} \geq 0, \forall m \in \mathcal{M}, j \in \mathcal{N} \\ & C3: R_{\sec,m,i,j}(c_{m,i,j}, p_{m,j}) \geq R_{\min}, \\ & \forall m \in \mathcal{M}, \forall i \in \mathcal{N}, \forall j \in \mathcal{N} \\ & C4: \sum_{i\in\mathcal{N}} \sum_{j\in\mathcal{N}} u_{i,j} = 1. \end{aligned} \tag{29}$$

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. The secrecy energy efficiency significantly improves for each iteration in algorithm 3.

Algorithm 3 A Novel Power Allocation Algorithm

Based on the CSI of each SC, the RS allocates the transmitted power equally to each SC;
Initialize the maximum tolerance ε and iteration numbers ℓ and the maximum number of iterations L_m;
while $|R_{\sec,m,i,j} - u_E P_s| > \varepsilon$ or $\ell \leq L_m$ **do**
  Update p by solving GP formulated in (28) and (29) using the interior point methods;
  $\ell = \ell + 1$;
end while

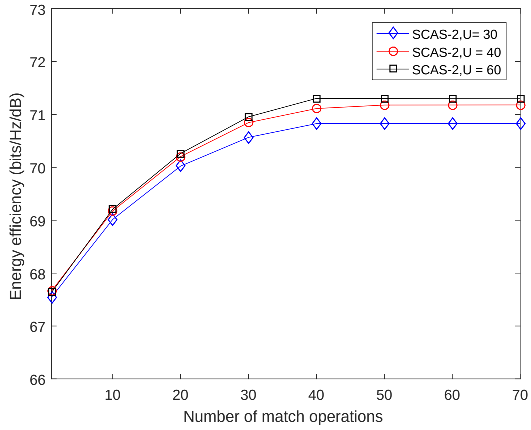

Fig. 2. C.D.F. of the number of match operations in SCAS-2.

IV. Simulation Results and Discussions

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). 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 set of 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 $P_c = 1$dB and eavesdropper is allocated at a distance of 500 m from the RS, if there is no special instructions. 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 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 served 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 approaches 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. 3 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 rate of growth becomes slower. 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. 3, 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

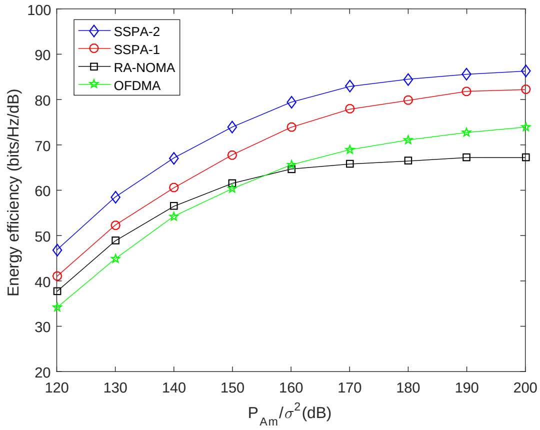

Fig. 3. Secrecy energy efficiency vs. P_{A_m}/σ^2.

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.

V. 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. 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.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (61471025, 61771044), the Young Elite Scientist Sponsorship Program by CAST (2016QNRC001), the Research Foundation of Ministry of Education of China & China Mobile (MCM20170108), Beijing Natural Science Foundation (L172025), and the Fundamental Research Funds for the Central Universities (FRF-GF-17-A6, RC1631). (Yang Ning and Haijun Zhang contributed equally to this work.) The corresponding authors: Haijun Zhang, Keping Long (e-mail: haijunzhang@ieee.org; longkeping@ustb.edu.cn).

References

[1] 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. PP, no. 99, pp. 1-1.

[2] J. Tang, D. K. C. So, A. Shojaeifard, K. Wong and J. Wen "Joint antenna selection and spatial switching for energy efficient MIMO SWIPT system," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4754-4769, July 2017.

[3] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. PP, no. 99, pp. 1-1, 2017.

[4] 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.

[5] 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.

[6] L. Wang, H. Wu, and G. L. Stuber, "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.

[7] 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.

[8] 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.

[9] 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.

[10] S. M. A. Kazmi, N. H. Tran, W. Saad, Z. Han, T. M. Ho, T. Z. Oo, and C. S. Hong, "Mode selection and resource allocation in device-to-device communications: A matching game approach," *IEEE Trans. Mobile Computing*, vol. PP, no. 99, pp. 1-1, 2017.

[11] D. Tse, and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.