# User Pairing and Power Allocation in Untrusted Multiuser NOMA for Internet-of-Things

Chaoying Yuan, Wei Ni, Senior Member, IEEE, Kezhong Zhang, Jingpeng Bai, Jun Shen, and Abbas Jamalipour, Fellow, IEEE

Abstract-In the Internet-of-Things (IoT), massive sensitive and confidential information is transmitted wirelessly, making security a serious concern. This is particularly true when technologies, such as non-orthogonal multiple access (NOMA), are used, making it possible for users to access each other's data. This paper studies secure communications in multiuser NOMA downlink systems, where each user is potentially an eavesdropper. Resource allocation is formulated to achieve the maximum sum secrecy rate, meanwhile satisfying the users' data requirements and power constraint. We solve this non-trivial, mixed-integer non-linear programming problem by decomposing it into power allocation with a closed-form solution, and user pairing obtained effectively using linear programming relaxation and barrier algorithm. These subproblems are solved iteratively until convergence, with the convergence rate rigorously analyzed. Simulations demonstrate that our approach outperforms its existing alternatives significantly in the sum secrecy rate and computational complexity.

*Index Terms*—Internet-of-Things (IoT), non-orthogonal multiple access (NOMA), untrusted user, user pairing, power allocation.

#### I. INTRODUCTION

THE increasing number of Internet-of-Things (IoT) devices connected to wireless networks has made IoT the dominant communication paradigm for connecting the physical world to the Internet [1]. Ericsson predicted that around 5.9 billion cellular IoT devices will be deployed by 2026 [2]. These devices collect and process data, and make intelligent decisions, improving efficiency, productivity, and convenience. However, the rapid expansion of IoT has brought challenges, including wireless resource scarcity and security and privacy concerns. It is crucial to address these issues in order to ensure satisfactory wireless communication and protect the security and privacy of IoT devices.

In the IoT scenarios, the adoption of non-orthogonal multiple access (NOMA) could potentially improve the connectivity and efficiency of massive IoT devices [3]. In contrast to orthogonal multiple access (OMA) in the time, frequency, and code domains, a NOMA transmitter can allocate different transmit powers for different receivers within the same

W. Ni is with the Data61, CSIRO, Marsfield, NSW 2122, Australia (e-mail: wei.ni@data61.csiro.au).

resource block, according to the channel conditions of the receivers. Supposition coding (SC) is adopted at the transmitter. Successive interference cancellation (SIC) is deployed at the receivers. However, the broadcast nature of radio and the use of SIC at the receivers make NOMA susceptible to attacks launched by external and internal eavesdroppers [4].

To address these security concerns, physical layer security (PLS) techniques have been considered a promising approach [4]. PLS can be computationally effective compared to other forms of security, such as cryptography, because they rely on simple operations that can be performed at the physical layer, such as power allocation [5]. PLS is more appropriate for low-cost IoT devices that often have limited computing resources and energy constraints [6]. By using simple and efficient PLS techniques, IoT devices can achieve strong confidentiality of their communications without incurring high computational or energy costs [7]. Some other recent studies, e.g., [1], [8], [9], also attempted to improve the secrecy performance of NOMA-based IoT systems in the presence of external eavesdropping.

It is possible for some users to eavesdrop on the signals intended for other users by executing the SIC, since users in a NOMA system share the same resource block. Most studies have been under a two-user setting: Some assumed far users untrusted [10], [11], and others assumed near users untrusted [12], [13]. Several studies [14]–[16] considered both users were untrusted. Different from the two-user settings in [14]–[16], the authors of [17] proposed a decoding ordering criterion for untrusted multiuser NOMA with persistent power allocation. The authors considered all users share the same resource block, leading to fast growing interference and complexity at the receivers with the increase of users.

In this paper, we investigate multiuser NOMA systems for IoT applications in the presence of untrusted users. User pairing and power allocation are optimized jointly to maximize the sum secrecy rate of the systems. To the best of our knowledge, user pairing and power allocation, which are critical to multiuser NOMA, have never been jointly considered in untrusted multiuser NOMA systems in the literature.

The key contributions of this paper are:

- We study a new problem to maximize the sum secrecy rate of multiuser NOMA with untrusted IoT users, by jointly optimizing power allocation and user pairing.
- To effectively maximize the sum secrecy rate of all IoT devices, we adopt alternating optimization to circumvent the non-convexity of the new problem and decouple user pairing and power allocation.

C. Yuan is with the China Telecom Corporation Limited, Shanghai, China, 200122 (e-mail: yuancy3@chinatelecom.cn).

K. Zhang graduated from the Beijing University of Posts and Telecommunications (e-mail: zhangkz@foxmail.com).

J. Bai and J. Shen are with the China Telecom Corporation Limited, Guangzhou, China, 510630 (e-mail: baijp@chinatelecom.cn; shenjun6@chinatelecom.cn).

A. Jamalipour is with the School of Electrical and Information Engineering, The University of Sydney, NSW 2006, Australia (email: a.jamalipour@ieee.org).

- Given user pairing, we derive analytically the optimal power allocation in closed form. Then, we develop user pairing obtained effectively using linear programming relaxation and the barrier method.
- Rigorous analyses are conducted for the convergence rate and complexity of our algorithm, confirming the validity of the algorithm.

Our approach addresses the challenges of interference and implementation complexity in untrusted multiuser NOMA systems, and has the potential to improve the security and performance of these systems. Extensive simulations demonstrate that the approach has superior secrecy performance, compared to existing schemes, and that joint consideration of user pairing and power allocation is critical for achieving this performance.

The remainder of the paper is arranged in the following way. In Section II, the related works are reviewed. Section III defines the system setting. In Section IV, the problem statement is provided, and the solution is delivered. In Section V, simulation results are analyzed to show the merits of our solution. Finally, this article is concluded in Section VI.

*Notations:* Upper- and lower-case symbols stand for matrices and vectors, respectively;  $^{T}$  denotes transpose;  $\preccurlyeq$  stands for component-wise less than;  $\cup$  and  $\cap$  stand for the union and intersection operations, respectively;  $\nabla$  denotes gradient. Tab. I summarizes notations used in this paper.

# II. RELATED WORK

Most of the existing NOMA security studies have focused on external eavesdropping. Secure transmissions in a NOMAbased IoT system were investigated in [1]. The system offered the users different communication requirements. The authors of [8] studied the secrecy performance of cooperative NOMAassisted IoT and derived the security outage probability under either a single- or multi-antenna setting. The authors of [9] jointly designed beamforming vector, power and subcarrier allocation to improve the worst-case sum secrecy rate in a multicarrier NOMA-assisted IoT system.

Another potential security threat in a NOMA system comes from internal users. A simple two-user setting has been actively studied. ElHalawany et al. [10] studied the secrecy outage probability in a two-user NOMA system under the assumption that the far user was untrusted. In [11], two optimal relay selection schemes were designed, and closed-form expressions of the secrecy outage probability was derived. Zhang et al. [12] proposed an optimal decoding order of SIC and a jammer-aided cooperative jamming scheme for NOMA systems to defend against a stronger, near-user eavesdropper to improve the secrecy rate of the systems. In [13], a secure beamforming and power allocation strategy was designed to evaluate the secrecy outage probability of the systems in the presence of an untrusted near user. Unlike [10]-[13], the authors of [14]-[16] treated both far and near users as the untrusted users. Specifically, the authors of [14] proposed an optimal decoding order to maximize secrecy fairness of a NOMA system. Hota et al. [15] analyzed the ergodic rate and the ergodic secrecy rate of a two-user untrusted NOMA system with imperfect SIC. Amin et al. [16] studied the

TABLE I: Notation list

Notations	Descriptions
$\mathcal{D}$	The disc-shaped area centered at the BS
$s_k$	The data symbol designed for user $k$
s	Transmit signal
$p_k$	The transmit power assigned for user $k$
$g_k$	The Rayleigh fading channel coefficient of user $k$
$d_k$	The distance between user $k$ and the BS
$h_k$	The channel impulse response of user $k$
$\sigma$	The standard deviation of the AWGN
$\gamma_{m,n}$	The SNR of user $m$ decoded by user $n$
$w_k$	The AWGN at user $k$
$R_n^s$	The secrecy rate of user $n$
$R_{m,n}$	The achievable rate of user $m$ decoded by user $n$
	User pairing indicator; if user $m$ and $n$ share the same
$x_{m,n}$	resource block, $x_{m,n} = 1$ . Otherwise, $x_{m,n} = 0$
37	The matrix of user pairing of which the $(m, n)$ -th
Λ	element is $x_{m,n}$
	The vectorization of the elements above the main
x	diagonal of $\mathbf{X}$ in the row-major order
	The continuous relaxation of <b>X</b> with the $(m, n)$ -th element,
$\hat{\mathbf{X}}$	$\hat{x}_{m,n} \in [0,1]$ , indicating how likely user m and n are
	paired to share a resource block.
^	The vectorization of the elements above the main
x	diagonal of $\hat{\mathbf{X}}$ in row-major order
$p_{m,n}$	The transmit powers for paired users $m$ and $n$
D	The vectorization of $(p_m + p_n)$ in row-major order
1	A vector with all one entries
0	A vector with all zero entries
$\mathbf{w}$	The Lagrange variable
Ι	The identify matrix
А	$\mathbf{A} = [\mathbf{I}, -\mathbf{I}, \mathbf{p}]^T$
$\mathbf{K}(\mathbf{x}, \mathbf{w})$	The Karush-Kuhn-Tucker (KKT) matrix
S	The upper bound of $\ \mathbf{K}(\mathbf{x}, \mathbf{w})^{\dagger}\ $
~	The Lipschitz constant satisfying: $\forall (\mathbf{x}; \mathbf{w})$
L	$\  (\mathbf{x} \cdot \mathbf{w}_i) \  < \  (\mathbf{y}_i^{(0)} \cdot \mathbf{w}_i^{(0)}) \ $
N	$\ \langle \mathbf{A}_i, \mathbf{w}_i \rangle\ _F \leq \ \langle \mathbf{A}_i, \mathbf{w}_i \rangle \rangle\ _F$
Čπ	The control factors in backtracking line search
ς, γ	The error tolerance of user pairing
¢	The control factor of the step size for user pairing
s n	The tolerance level of the overall algorithm
δ	The indicator function on the feasible domain $\mathcal{F}$
~~	

secrecy rate maximization of the a trusted decode-and-forward relay-assisted NOMA system by optimizing power allocation. These designs provided secure communication by addressing the potential for internal eavesdropping in NOMA.

Compared with a two-user setting [14]–[16], the security of a multi-user untrusted scenario is a more realistic and challenging problem. The most relevant, existing study [17] proposed a decoding order strategy for multi-user untrusted NOMA with fixed power allocation. However, excessive devices sharing the same resource block may lead to severe co-channel interference. To this end, an adequate user pairing strategy, in coupling with effective power allocation, is critical. In [18] and [19], a Gale-Shapley algorithm-based and a Simplex method-based approaches were developed and dedicated to user pairing, respectively. Compared to the user pairing strategies developed in [18] and [19], our approach delivers effective user pairing solution using logarithmic barrier method in couple with closed-form optimal power allocation, hence achieving improved efficiency and accuracy.

#### **III. SYSTEM MODEL**

In this paper, we investigate a multiuser downlink NOMA system with a base station (BS) and 2K untrusted users. The

users are untrusted in the sense that each user in the system may act as a potential eavesdropper and may attempt to intercept the confidential messages transmitted by other users to its own advantage. The users are dispersed within a disc-shaped area  $\mathcal{D}$  centered at the BS. The BS and users are equipped with omnidirectional antennas. The direct link between the BS and each user experiences Rayleigh fading [20]. In order to reduce complexity, we divide the users into K pairs, with each pair occupying a different resource block. This allows us to consider the system in manageable chunks and design efficient resource allocation strategies.

At the BS, the transmit signal for the users at each pair is

$$s = \sqrt{p_m} s_m + \sqrt{p_n} s_n, \tag{1}$$

where  $s_k$  (k = m, n) is the data symbol destined for user k with unit energy  $\mathbb{E}[|s_k|^2] = 1$ , and  $p_k$  represents the corresponding transmit power assigned for user.

The received signal of user k is given by

$$y_k = h_k \left(\sqrt{p_m} s_m + \sqrt{p_n} s_n\right) + \omega_k, \tag{2}$$

where  $h_k = g_k d_k^{-\alpha}$  with  $g_k$  being the Rayleigh fading coefficient,  $d_k$  the distance of user k from the BS, and  $\alpha$  the path loss;  $w_k$  is the zero-mean additive white Gaussian noise (AWGN) with variance  $\sigma^2$ .

Assume the paired user with  $|h_m|^2 < |h_n|^2$ . By following the NOMA principle, user n with a higher channel gain first decodes the signal of user m, and then executes SIC to decode its own signal. User m with poor channel gain first decodes its own signal and then executes SIC to decode user n's signal. As such, we have

$$\gamma_{m,n} = \frac{p_m |h_n|^2}{p_n |h_n|^2 + \sigma^2}, \quad \gamma_{n,n} = \frac{p_n |h_n|^2}{\sigma^2}, \quad (3)$$

$$\gamma_{m,m} = \frac{p_m |h_m|^2}{p_n |h_m|^2 + \sigma^2}, \quad \gamma_{n,m} = \frac{p_n |h_m|^2}{\sigma^2}, \tag{4}$$

where  $\gamma_{m,n}$  is the signal-to-interference-plus-noise-ratio (SINR) of user *m* decoded by user *n*, and  $\gamma_{n,m}$  is the other way around.

Then, the achievable rates of the paired users are

$$R_{n,n} = \log_2\left(1 + \gamma_{n,n}\right); \tag{5}$$

$$R_{m,m} = \log_2 \left( 1 + \gamma_{m,m} \right). \tag{6}$$

The secrecy rate  $R_n^s$  of user n is defined as

$$R_n^s = \max\{R_{n,n} - R_{n,m}, 0\}.$$
 (7)

Here,  $R_{n,m} = \log_2 (1 + \gamma_{n,m})$  is the eavesdropping rate of user *m* on user *n*'s message. A positive secrecy rate can be awarded since  $|h_m|^2 < |h_n|^2$ .

#### IV. PROBLEM STATEMENT AND PROPOSED SOLUTION

In this section, power allocation and user pairing are optimized in an attempt to achieve the maximum sum secrecy rate under the data rate and transmit power constraints. Let  $x_{m,n} \in \{0,1\}$  denote the binary scheduling variables. If user m is served together with user n, we have  $x_{m,n} = 1$ . Otherwise,  $x_{m,n} = 0$ . The considered problem is cast as

$$\max_{x_{m,n}, p_n, p_m} \sum_{m=1}^{2K} \sum_{n=m+1}^{2K} x_{m,n} R_n^s$$
(8a)

s.t.  $R_{m,m} \ge x_{m,n} R_m$ , (8b)

$$R_{n,n} \geqslant x_{m,n} R_n, \tag{8c}$$

$$\sum_{m=1}^{2K} \sum_{n=m+1}^{2K} x_{m,n} \left( p_n + p_m \right) \leqslant P, \quad (8d)$$

$$x_{m,n} \in \{0,1\}, 1 \le m, n \le 2K,$$
 (8e)

$$x_{m,n} = x_{n,m}, 1 \leqslant m, n \leqslant 2K, \tag{8f}$$

$$\sum_{m=1}^{2K} x_{m,n} = 1, 1 \le n \le 2K,$$
(8g)

$$\sum_{n=1}^{2K} x_{m,n} = 1, 1 \leqslant m \leqslant 2K,$$
 (8h)

where P is the total transmit power of the BS;  $R_m$  and  $R_n$  are the achievable rates of user m and user n in an OMA system, respectively, and

$$R_m = \frac{1}{2} \log_2 \left( 1 + \frac{p_{m,n} |h_m|^2}{\sigma^2} \right); R_n = \frac{1}{2} \log_2 \left( 1 + \frac{p_{m,n} |h_n|^2}{\sigma^2} \right).$$

Here,  $p_{m,n}$  is the transmit power for each pair of users, i.e.  $p_{m,n} = p_m + p_n$ . The coefficient  $\frac{1}{2}$  is due to the fact that conventional OMA results in a multiplexing loss of  $\frac{1}{2}$ .

The problem presented in (8) is a mixed-integer nonlinear programming (MINLP) problem, which is typically NP-hard and intractable to solve the global optimal solution. The key difficultly in solving (8) arises from the binary scheduling variables, achievable data rate constraint, and objective function. To improve the tractability, in this paper, we decouple Problem (8) into the subproblem of power allocation and user pairing, and solve the subproblems separately in an alternating manner.

### A. Power Allocation Optimization

p

First, we optimize the transmit power of each user  $p_n$ and  $p_m$  for given user pairing  $x_{m,n}$ . The power allocation subproblem is given by

$$\max_{n,p_m} \sum_{m=1}^{2K} \sum_{n \in S_m} R_n^s$$
(9a)

s.t. 
$$R_{m,m} \ge R_m$$
, (9b)

$$R_{n,n} \geqslant R_n,\tag{9c}$$

$$\sum_{m=1}^{2K} \sum_{n \in S_m} \left( p_n + p_m \right) \leqslant P, \qquad (9d)$$

where  $S_m = \{n | x_{m,n} = 1\}$ . Despite the non-convexity of the subproblem, we can derive its closed-form solution, as follows. According to (9b), we have

$$p_n \leqslant \frac{\sigma^2}{|h_m|^2} \left( \sqrt{1 + \frac{p_{m,n}|h_m|^2}{\sigma^2}} - 1 \right).$$
 (10)

Similarly, according to (9c), we have

$$p_n \ge \frac{\sigma^2}{|h_n|^2} \left( \sqrt{1 + \frac{p_{m,n}|h_n|^2}{\sigma^2}} - 1 \right)$$
 (11)

The first-order partial derivative of  $R_n^s$  with respect to (w.r.t.)  $p_n$  is

$$\frac{\partial R_n^s}{\partial p_n} = \frac{1}{\ln 2} \frac{\left(|h_n|^2 \sigma^2 - |h_m|^2 \sigma^2\right)}{(p_n|h_n|^2 + \sigma^2)(p_n|h_m|^2 + \sigma^2)}, \quad (12)$$

which is always non-negative, given  $|h_m|^2 < |h_n|^2$ . As a result,  $R_n^s$  is an increasing function of  $p_n$ , and the optimal value of  $p_n$ , denoted by  $p_n^*$ , is given by

$$p_n^* = \frac{\sigma^2}{|h_m|^2} \left( \sqrt{1 + \frac{p_{m,n} |h_m|^2}{\sigma^2}} - 1 \right).$$
(13)

By substituting  $p_n^*$  into the objective function (9a), we obtain

$$R_{n}^{s} = \log_{2} \left( 1 + \frac{|h_{n}|^{2}}{|h_{m}|^{2}} \left( \sqrt{1 + \frac{p_{m,n}|h_{m}|^{2}}{\sigma^{2}}} - 1 \right) \right) - \frac{1}{2} \log_{2} \left( 1 + \frac{p_{m,n}|h_{m}|^{2}}{\sigma^{2}} \right).$$
(14)

Then, Problem (9) can be equivalently rewritten as

$$\max_{p_{m,n}} \sum_{m=1}^{2K} \sum_{\substack{n \in S_n \\ 2K}} R_n^s \tag{15a}$$

s.t. 
$$\sum_{m=1}^{2K} \sum_{n \in S_n} x_{m,n} p_{m,n} \leqslant P.$$
 (15b)

Taking the second-order derivative of  $R_n^s$  w.r.t.  $p_n$  yields

$$\frac{d^2 R_n^s}{d p_{m,n}^2} = -\frac{|h_m|_2 |h_n|_2 \ln 2}{4\sigma^4 \left(1 + \frac{|h_m|_2 p_{m,n}}{\sigma^2}\right)^{\frac{3}{2}}} < 0.$$
(16)

Therefore, we can drawn the conclusion that (15a) is concave in  $p_{m,n}$ . In turn, Problem (15) exhibits convexity and can be efficiently solved taking the Lagrange multiplier method. The Lagrange function of Problem (15) is

$$L(p_{m,n},v) = -\sum_{m=1}^{2K} \sum_{n \in S_n} \log_2 \left( 1 + \frac{|h_n|^2}{|h_m|^2} \left( \sqrt{1 + \frac{p_{m,n} |h_m|^2}{\sigma^2}} - 1 \right) \right) + \sum_{m=1}^{2K} \sum_{n \in S_n} \frac{1}{2} \log_2 \left( 1 + \frac{p_{m,n} |h_m|^2}{\sigma^2} \right) + v \sum_{m=1}^{2K} \sum_{n \in S_n} (p_{m,n} - P), \quad (17)$$

where v > 0 is the dual variable corresponding to (15b).

After taking the first-order partial derivative of (17) w.r.t.  $p_{m,n}$ , the KKT conditions of (15) are given by

$$\frac{\partial L(p_{m,n},\upsilon)}{\partial p_{m,n}} = \alpha^3 - \frac{|h_n|^2 - |h_m|^2}{|h_n|^2} \alpha^2 - \frac{|h_m|^2 (|h_n|^2 - |h_m|^2)}{2\ln 2\sigma^2 \upsilon |h_n|^2}$$

where  $\alpha = \sqrt{\frac{p_{m,n}|h_m|^2}{\sigma^2}} + 1 > 1$ . Since the optimal solution to Problem (15) satisfies  $\frac{\partial L(p_{m,n},v)}{\partial n} = 0$ , we define  $f(\alpha) : \mathbb{R}^+ \to \mathbb{R}$  as  $\partial p_{m,n}$ 

$$f(\alpha) = \alpha^3 - \frac{|h_n|^2 - |h_m|^2}{|h_n|^2} \alpha^2 - \frac{|h_m|^2 (|h_n|^2 - |h_m|^2)}{2 \ln 2\sigma^2 v |h_n|^2}$$

Note that  $f(\alpha) = 0$  holds at the optimal  $p_{m,n}$ . Taking the first-order derivative of  $f(\alpha)$  w.r.t.  $\alpha$ , we have

$$\frac{\mathrm{d}f(\alpha)}{\mathrm{d}\alpha} = 3\alpha \left[ \alpha - \frac{2}{3} \left( 1 - \frac{|h_m|^2}{|h_n|^2} \right) \right].$$
 (18)

Then, setting  $\frac{df(\alpha)}{d\alpha} = 0$  yields two roots:

$$\alpha_1 = 0, \ \alpha_2 = \frac{2}{3} \left( 1 - \frac{|h_m|^2}{|h_n|^2} \right) < \frac{2}{3}.$$
(19)

We can analyze the number of positive roots of  $f(\alpha) = 0$ based on the monotonicity of  $f(\alpha)$ . Since  $f(\alpha_1) < 0$ ,  $f(\alpha_2) < 0$ 0, and  $\alpha_1 < \alpha_2$ , according to the monotonicity of a cubic function, there is only one positive root of  $f(\alpha) = 0$ :

$$\alpha = \frac{\sqrt[3]{a_{m,n}}}{3 \cdot \sqrt[3]{4}} + \frac{\sqrt[3]{4} (|h_n|^2 - |h_m|^2)^2}{3\sqrt[3]{a_{m,n}} |h_n|^4} + \frac{|h_n|^2 - |h_m|^2}{3|h_n|^2},$$
(20)

where  $a_{m,n}$  is given by

$$a_{m,n} = 4 - \frac{4|h_m|^6}{|h_n|^6} + |h_m|^2 \left(\frac{27}{\ln 2\sigma^2 \upsilon} - \frac{12}{|h_n|^2}\right) + \frac{3|h_m|^4}{|h_n|^4} \left(4 - \frac{9|h_n|^2}{\ln 2\sigma^2 \upsilon}\right) + 3\sqrt{3} \frac{|h_m|\left(|h_n|^2 - |h_m|^2\right)}{|h_n|^4 \ln 2\sigma^2 \upsilon} \times \sqrt{8\ln 2\sigma^2 \upsilon \left(|h_n|^2 - |h_m|^2\right) + 27|h_n|^4 |h_m|^2}.$$
(21)

We solve (20) using Formula of Cardano [21] and choose the positive root. The Formula of Cardano is a widely-used approach for solving cubic equations.

When  $x_{m,n} = 1$ , by substituting  $\alpha = \sqrt{\frac{p_{m,n}|h_m|^2}{\sigma^2} + 1}$  into (20), the optimal power allocation, denoted by  $p_{m,n}^*$ , can be obtained in closed-form, as given by

$$p_{m,n}^{*} = \frac{\sigma^{2}}{|h_{m}|^{2}} \left[ \left( \frac{\sqrt[3]{a_{m,n}}}{\sqrt[3]{4}} + \frac{\sqrt[3]{4} \left( |h_{n}|^{2} - |h_{m}|^{2} \right)}{3\sqrt[3]{a_{m,n}} |h_{n}|^{4}} + \frac{|h_{n}|^{2} - |h_{m}|^{2}}{3|h_{n}|^{2}} \right) - 1 \right], \quad (22)$$

Moreover, according to (13) and (22), the optimal  $p_m$ , denoted by  $p_m^*$ , can be obtained since  $p_m^* = p_{m,n}^* - p_n^*$ . By adjusting the dual variable v until  $\sum_{k=1}^{2K} p_k^* = P, \forall k = 1, \dots, 2K$ , we obtain the optimal transmit power  $p_k^*, \forall k$ .

## B. User Pairing Optimization

Given the power allocation  $p_n^\ast$  and  $p_m^\ast,$  we can relax the binary variables  $x_{m,n} \in \{0,1\}$  into continuous variables  $\hat{x}_{m,n} \in \{0,1\}$ [0, 1]. Problem (8) can be recast as

$$\max_{x_{m,n}} \sum_{m=1}^{2K} \sum_{n=1}^{2K} \hat{x}_{m,n} R_n^s$$
(23a)

s.t. 
$$R_{m,m} \ge \hat{x}_{m,n} R_m$$
, (23b)

$$R_{n,n} \ge \hat{x}_{m,n} R_n, \tag{23c}$$

$$\sum_{m=1}^{2K} \sum_{n=m+1}^{2K} \hat{x}_{m,n} \left( p_n + p_m \right) \leqslant P, \quad (23d)$$

$$0 \leqslant \hat{x}_{m,n}, \leqslant 1, 1 \leqslant m, n \leqslant 2K, \tag{23e}$$

$$\hat{x}_{m,n} = 0, \tag{23f}$$

$$\sum_{\substack{m=1\\2K}}^{2K} \hat{x}_{m,n} = 1, 1 \leqslant n \leqslant 2K,$$
(23g)

$$\sum_{n=1}^{2K} \hat{x}_{m,n} = 1, 1 \le m \le 2K,$$
(23h)

Here,  $\hat{x}_{m,n} \in [0,1]$  can be interpreted as how likely users m and n are assigned to form a NOMA group and share the same resource block.

By vectorization, Problem (23) is rewritten as

$$\max_{\hat{\mathbf{x}}} \mathbf{r}_s^T \hat{\mathbf{x}}$$
(24a)

s.t. 
$$\hat{\mathbf{x}} \preccurlyeq \mathbf{b}$$
, (24b)

$$\mathbf{p}^T \, \hat{\mathbf{x}} \leqslant P, \tag{24c}$$

$$-\mathbf{x} \preccurlyeq \mathbf{0},$$
 (24d)

$$\mathbf{D}\mathbf{x} = \mathbf{1},\tag{24e}$$

where  $\hat{\mathbf{x}} \in \mathbb{R}^{K(2K-1)}$  and  $\mathbf{p} \in \mathbb{R}^{K(2K-1)}$  are the vectorization of the elements above the main diagonal of  $\hat{\mathbf{X}}$  and  $\{p_m + p_n\}$  in the row-major order, respectively. Then, the  $\left[\frac{1}{2}\left(4K - m\right)\left(m - 1\right) + n - m\right]$ -th elements of  $\hat{\mathbf{x}}$ ,  $\mathbf{p}$ ,  $\mathbf{r}_s \in \mathbb{R}^{K(2K-1)}$ , and  $\mathbf{b} \in \mathbb{R}^{K(2K-1)}$  are  $\hat{x}_{m,n}$ ,  $p_m + p_n$ ,  $R_n^s$  and min  $\left\{\frac{R_{m,m}}{R_m}, \frac{R_{n,n}}{R_n}, 1\right\}$ , respectively. Moreover, the *n*-th row of  $\mathbf{D} \in \mathbb{R}^{2K \times K(2K-1)}$ , denoted by  $\mathbf{d}_n^T$ , satisfies  $\mathbf{d}_n^T \hat{\mathbf{x}} = \sum_{m-1}^{2K} \hat{x}_{m,n}$ , according to constraints (23g) and (23h). By combining (24b), (24c), and (24d), Problem (24) can be

further rewritten as

$$\max_{\hat{s}} \mathbf{r}_{s}^{T} \hat{\mathbf{x}}$$
(25a)

a.t. 
$$A\hat{\mathbf{x}} \preccurlyeq \mathbf{u}$$
, (25b)

$$\mathbf{D}\hat{\mathbf{x}} = \mathbf{1},\tag{25c}$$

where  $\mathbf{A} = [\mathbf{I}, -\mathbf{I}, \mathbf{p}]^T \in \mathbb{R}^{[2K(2K-1)+1] \times K(2K-1)}$  and  $\mathbf{u} = [\mathbf{b}^T, \mathbf{0}^T, P]^T \in \mathbb{R}^{2K(2K-1)+1}$ .

The logarithmic barrier and Simplex methods [19] are widely adopted by various Linear Programming (LP) solvers, e.g., CVX Toolbox [22]–[24]. Since D is sparse, the barrier method is more effective than the Simplex method in solving sparse LP problems [25].

We utilize the logarithmic barrier method [26] to solve Problem (25). In the method, the optimization problem is modified by adding a logarithmic barrier function to the objective function. The barrier function penalizes the constraints, encouraging the optimization to move towards feasible solutions [26]. The barrier function is typically the sum of the negative logarithms of the variables that define the feasible region. The barrier function we choose is

$$\phi\left(\hat{\mathbf{x}}\right) = -\sum_{i=1}^{2K(2K-1)+1} \ln\left(u_i - \mathbf{a}_i^T \hat{\mathbf{x}}\right), \qquad (26)$$

where  $u_i \in \mathbb{R}$  and  $\mathbf{a}_i \in \mathbb{R}^{K(2K-1)}$  are the *i*-th rows of **u** and **A**, respectively.

Let t > 0 denote the parameter (or step size) of the logarithmic barrier method. Problem (25) is then rewritten as

$$\min_{\mathbf{x}} g\left(\hat{\mathbf{x}}\right) = -t\mathbf{r}_{s}^{T}\hat{\mathbf{x}} + \phi\left(\hat{\mathbf{x}}\right)$$
(27a)

s.t. 
$$\mathbf{D}\hat{\mathbf{x}} = \mathbf{1}$$
. (27b)

Let  $y_i = \frac{1}{u_i - \mathbf{a}_i^T \hat{\mathbf{x}}}$  be the *i*-th element of  $\mathbf{y} \in \mathbb{R}^{2K(2K-1)+1}$  and  $\mathbf{w} \in \mathbb{R}^{2K}$  be the Lagrange multiplier associated with (27b).

In each iteration of the logarithmic barrier method, we update *t* by  $t := \xi t$ , which regulates the accuracy of using (27) to approximate (25). Here,  $\xi > 1$  is a preconfigured coefficient. Given the fixed *t*, the infeasible start Newton method [27], [28] is adopted to solve (27) iteratively.

The infeasible start Newton method starts by evaluating the primal and dual Newton steps  $\Delta \mathbf{w} \in \mathbb{R}^{2K}$  and  $\Delta \hat{\mathbf{x}} \in \mathbb{R}^{K(2K-1)}$ . Given t, the primal and dual Newton steps of Problem (27) are given by

$$\mathbf{K}\left(\hat{\mathbf{x}},\mathbf{w}\right)\cdot\begin{bmatrix}\Delta\hat{\mathbf{x}}\\\mathbf{w}+\Delta\mathbf{w}\end{bmatrix} = -\begin{bmatrix}-t\mathbf{r}_{s}+\mathbf{A}\mathbf{y}\\\mathbf{D}\hat{\mathbf{x}}-\mathbf{1}\end{bmatrix},\qquad(28)$$

where  $\mathbf{K}(\hat{\mathbf{x}}, \mathbf{w})$  is the Karush-Kuhn-Tucker (KKT) matrix [29] and is given by

$$\mathbf{K}(\hat{\mathbf{x}}, \mathbf{w}) = \begin{bmatrix} \mathbf{A}^T \operatorname{diag}(\mathbf{y}) \ \mathbf{A} & \mathbf{D}^T \\ \mathbf{D} & \mathbf{0} \end{bmatrix}$$
(29)

We utilize the LU decomposition [30] to solve (28) for  $\Delta \hat{\mathbf{x}}$  and  $\Delta \mathbf{w}$ , so that we can avoid computationally expensive matrix inversions [31]. Let  $\mathbf{L}, \mathbf{U} \in \mathbb{R}^{K(2K+1) \times K(2K+1)}$  denote the lower and higher triangular matrices, respectively, and

$$\mathbf{LU} = \mathbf{K} \left( \hat{\mathbf{x}}, \mathbf{w} \right). \tag{30}$$

By using the forward and back substitution algorithms [32], we can derive  $\Delta \hat{\mathbf{x}}$  and  $\Delta \mathbf{w}$ .

Define  $\mathbf{J}: \mathbb{R}^{K(2K-1)} \times \mathbb{R}^{2K} \to \mathbb{R}^{K(2K-1)} \times \mathbb{R}^{2K}$  as

$$\mathbf{J}\left(\hat{\mathbf{x}},\mathbf{w}\right) = \left(\nabla g\left(\hat{\mathbf{x}}\right) + \mathbf{D}^{T}\mathbf{w},\mathbf{D}\hat{\mathbf{x}} - \mathbf{1}\right).$$
 (31)

The Frobenius norm of  $\mathbf{J}(\mathbf{\hat{x}}, \mathbf{w})$  is given by

$$\left\|\mathbf{J}\left(\hat{\mathbf{x}},\mathbf{w}\right)\right\|_{F} = \sqrt{\left\|\nabla g\left(\hat{\mathbf{x}}\right) + \mathbf{D}^{T}\mathbf{w}\right\|_{F}^{2} + \left\|\mathbf{D}\hat{\mathbf{x}} - \mathbf{1}\right\|_{F}^{2}}.$$
(32)

Next, we utilize backtracking line search to produce the step size by  $s := \tau s$  for updating  $\hat{\mathbf{x}}$  and  $\mathbf{w}$ , i.e.,

$$\hat{\mathbf{x}} := \hat{\mathbf{x}} + s\Delta\hat{\mathbf{x}}$$
 and  $\mathbf{w} := \mathbf{w} + s\Delta\mathbf{w}$  (33)

until 
$$\|\mathbf{J}(\hat{\mathbf{x}}+s\Delta\hat{\mathbf{x}},\mathbf{w}+s\Delta\mathbf{w})\|_{F} \leq (1-\zeta s) \|\mathbf{J}(\hat{\mathbf{x}},\mathbf{w})\|_{F}$$
. (34)

Here,  $\tau \in (0,1)$  and  $\zeta \in (0,\frac{1}{2})$  are preconfigured coefficients.

Upon the stopping criterion (34) is satisfied, the updated  $\hat{\mathbf{x}}$  and  $\mathbf{w}$  are substituted into (28) and (29) to update  $\Delta \hat{\mathbf{x}}$  and  $\Delta \mathbf{w}$ , followed by the updating of  $\hat{\mathbf{x}}$  and  $\mathbf{w}$  using (33). This repeats until  $\|\mathbf{J}(\hat{\mathbf{x}}, \mathbf{w})\|_{F}$  is smaller than a predefined, sufficiently small threshold, e.g.,  $\rho$ , and (27b) is satisfied.

Let L and S denote constants satisfying:  $\forall$  ( $\hat{\mathbf{x}}_i, \mathbf{w}_i$ ), i = 1, 2,

$$\begin{aligned} \left\| \mathbf{K}(\hat{\mathbf{x}}_{1},\mathbf{w}_{1}) - \mathbf{K}(\hat{\mathbf{x}}_{2},\mathbf{w}_{2}) \right\|_{F} \leq L \sqrt{\left\| \hat{\mathbf{x}}_{1} - \hat{\mathbf{x}}_{2} \right\|_{2}^{2} + \left\| \mathbf{w}_{1} - \mathbf{w}_{2} \right\|_{2}^{2}}; \end{aligned}$$
(35)  
$$S \geq \left\| \mathbf{K} \left( \hat{\mathbf{x}}, \mathbf{w} \right)^{\dagger} \right\|_{F}. \end{aligned}$$
(36)

The step size *s*, obtained by backtracking line search, satisfies s < 1 in the damped Newton phase if  $\|\mathbf{J}(\hat{\mathbf{x}}, \mathbf{w})\|_F > \frac{1}{S^2L}$  [26]. Hence,  $\|\mathbf{J}(\hat{\mathbf{x}}, \mathbf{w})\|$  is reduced in each iteration [33]. Once the damped Newton phase has reasonably converged,

i.e.,  $\|\mathbf{J}(\hat{\mathbf{x}}, \mathbf{w})\|_F \leq \frac{1}{S^2L}$ , the logarithmic barrier method enters the quadratically convergent phase, where the step size is s = 1 and the error converges quadratically to zero [34]. This allows the algorithm to find a high-precision solution in relatively few iterations.

When the infeasible start Newton method converges, t is updated by  $t := \xi t$  and then the infeasible start Newton method restarts. This repeats until  $\frac{1}{t}K(2K-1) < \epsilon$ , where  $\epsilon$  indicates the approximation accuracy of (27) with regards to (25). The output of the logarithmic barrier method is the continuous relaxation of user pairing, i.e.,  $\hat{\mathbf{X}}$ .

Finally, given the continuous  $\hat{\mathbf{X}}$ , we utilize a greedy method that iteratively chooses the most probable pairs. U is initialized to be empty, i.e.,  $\mathbf{U} = \emptyset$  initially. In each iteration, we choose and record the pair  $\{m, n\}$  with the largest  $\hat{x}_{m,n}$  from unrecorded pairs, i.e.,  $\mathbf{U} \cap \{m, n\} = \emptyset$ , since users m and n have the highest pairing probability among all users not recorded in U yet.

The algorithm of user pairing is summarized in Alg. 1, where  $\hat{\mathbf{x}}^*$  denotes the optimum of (25).

#### C. Algorithm Summary

The overall algorithm is illustrated in Alg. 2, which consists of two phases (i.e., power allocation and user pairing) operating in an alternating manner. In the power allocation phase, we utilize (13) and (22) to obtain the transmit power of each user with a given fixed user pairing strategy **X**. In the user pairing phase, Alg. 1 is executed to produce the user pairing strategy given the fixed transmit powers of all users. The user pairing strategy is then input to the power allocation to start the next iteration of the power allocation and user pairing phases. Let  $o_q$  and  $\eta$  denote the sum secrecy rate in the q-th iteration of Alg. 2 and the tolerance, respectively. If  $|o_q - o_{q-1}| < \eta$ , Alg. 2 returns the user pairing strategy **X** and transmit power of each user  $p_n$ ,  $n = 1, \dots, 2K$ .

# D. Convergence Analysis

1) Convergence of User Pairing: We analyze the convergence rate of the LP relaxation in Alg. 1. According to [26, eq. (11.13)], the LP in Alg. 1 requires  $N_{\rm LP}$  iterations to adjust the parameter t and guarantee the desired accuracy level of  $\epsilon$ :

$$N_{\rm LP} = \left\lceil \log \left( \frac{K \left( 2K - 1 \right)}{\epsilon t^{(0)}} \right) / \log \left( \xi \right) \right\rceil, \tag{37}$$

where  $t^{(0)}$  is the initial value of t.

In each of the LP iterations, backtracking line search is carried out to search for the step size s. According to [26], the backtracking line search in the damped Newton phase uses fewer than  $N_l = \left\lceil \log \left(S^2 L \kappa\right) / \log \left(\frac{1}{\tau}\right) \right\rceil$  iterations to choose the step size s. Here,  $\kappa = \left\| \mathbf{J} \left( \hat{\mathbf{x}}^{(0)}, \mathbf{w}^{(0)} \right) \right\|_F$ , where  $\hat{\mathbf{x}}^{(0)}$  and  $\mathbf{w}^{(0)}$  are the initial  $\hat{\mathbf{x}}$  and  $\mathbf{w}$ , respectively. According to [35], the damped Newton phase takes  $N_{\rm D} = \left\lceil S^2 L \kappa / \zeta \tau \right\rceil$  iterations to achieve  $\left\| \mathbf{J} \left( \hat{\mathbf{x}}, \mathbf{w} \right) \right\|_F \leqslant \frac{1}{S^2 L}$  before the commencement of the quadratically convergent phase. In the quadratically convergent phase, according to [33], it takes  $N_{\rm Q} = \left\lceil \log_2 \left(1 - \log_2 \left(S^2 L \rho\right) \right) \right\rceil$  iterations to obtain the

# Algorithm 1: User Pairing

**Data:** Initialize  $t = t^{(0)}, \xi > 1, \epsilon > 0, \rho > 0$ , control factors in backtracking line search  $\zeta \in (0, 0.5)$ ,  $\tau \in (0, 1)$ , pairing set  $\mathbf{U} = \emptyset$ ,  $\mathbf{X} = \mathbf{0}$ /\* logarithmic barrier-based approach to obtain the assignment \*/ 1 while  $\frac{1}{t}K(2K-1) < \epsilon$  do /\* Using infeasible start Newton method to compute (27) with the given t\*/ s := 12 while  $\mathbf{D}\mathbf{\hat{x}} = \mathbf{1} \&\& \|\mathbf{J}(\mathbf{\hat{x}}, \mathbf{w})\|_{F} \leq \rho \text{ do}$ 3 Calculate  $\Delta \hat{\mathbf{x}}$  and  $\Delta \mathbf{w}$  in (28) 4 /\* Backtracking line search to obtain step size s\*/ while  $\|\mathbf{J}(\hat{\mathbf{x}} + s\Delta\hat{\mathbf{x}}, \mathbf{w} + s\Delta\mathbf{w})\|_{F} >$ 5  $(1-\zeta s) \left\| \mathbf{J}\left(\mathbf{\hat{x}},\mathbf{w}\right) \right\|_{F} \mathbf{do}$  $s := \tau s$  $\hat{\mathbf{x}}^* := \hat{\mathbf{x}} + s\Delta\hat{\mathbf{x}}$  and  $\mathbf{w} := \mathbf{w} + s\Delta\mathbf{w}$ // update  $\mathbf{\hat{x}}$  and t $\mathbf{\hat{x}} := \hat{\mathbf{x}}^*$ 9  $t := \xi t$ 10 obtain the assignment  $\hat{\mathbf{x}}$ . /\* greedy-based approach to obtain the user pairing strategy \*/ 11 for  $m = 1, \cdots, 2K - 1$  do for  $n = m + 1, \dots, 2K$  do 12 if  $\mathbf{U} \cap \{m, n\} = \emptyset$  then 13 Choose the largest element  $\hat{x}_{m,n}$  and set 14  $x_{m,n} = 1$ 15  $\mathbf{U} = \mathbf{U} \cup \{m, n\}$ Set  $\hat{x}_{m,n_0} = \hat{x}_{m_0,n} = -\infty$  for  $n_0 = 1, \cdots, 2K$ , and  $m_0 = 1, \cdots, 2K$ 16 else 17 continue 18 19 return the user pairing strategy  $\mathbf{X} = \{x_{m,n}\}$ 

solution to Problem (27). Overall, the infeasible start Newton method takes  $N_{\rm N}$  iterations per LP iteration:

$$N_{\rm N} = N_l N_{\rm D} + N_{\rm Q} \\ = \left[ \frac{\log \left( S^2 L \kappa \right)}{\log \left( \frac{1}{\tau} \right)} \right] \left[ \frac{S^2 L \kappa}{\zeta \tau} \right] + \left[ \log_2 \left( 1 - \log_2 \left( S^2 L \rho \right) \right) \right].$$
(38)

Moreover, the greedy method used for the discretization of user pairing in Alg. 1 takes  $N_g$  iterations to obtain the discrete assignment strategy:

$$N_g = \sum_{m=1}^{2K-1} (2K - m) = K (2K - 1).$$
 (39)

2) Convergence of Overall Algorithm: We can interpret Alg. 1 as a mapping  $\tilde{Q}$  from  $\hat{\mathbf{X}}$  to  $\mathbf{X}$ , i.e.,  $\tilde{Q} : \mathbb{R}^{2K \times 2K} \to$ 

# Algorithm 2: Overall Algorithm

**Data:** Initial  $o_q = +\infty$ ,  $o_{q-1} = -\infty$ , counter q = 0, tolerance  $\eta > 0$ 1 while  $|o_q - o_{q-1}| < \eta$  do // record the previous sum secrecy rate  $o_q = \sum_{m=1}^{2K} \sum_{n=m+1}^{2K} x_{m,n} R_n^s$ 2 // power allocation phase Use (13) and (22) to obtain the optimal power 3 allocation  $p_{m,n}^*$ // user pairing phase Use Alg. 1 to obtain the pairing strategy 4  $\mathbf{X} = \{x_{m,n}\}$ // update the counter q := q + 15 // record the sum secrecy rate  $o_q = \sum_{m=1}^{2K} \sum_{n=m+1}^{2K} x_{m,n} R_n^s$ 

7 **return** the user pairing strategy  $\mathbf{X} = \{x_{m,n}\}$  and the power allocation  $\{p_n\}, m, n = 1, \dots, 2K$ 

 $\mathbb{R}^{2K \times 2K}$ . In this case, the problem solved by Alg. 2, i.e., Problem (8), can be rewritten as

$$\min_{\substack{x_{m,n}, \hat{x}_{m,n}, p_m, p_n}} -2^{\operatorname{tr}\left(\mathbf{R}_s^T \mathbf{X}\right)} = -2^{\operatorname{tr}\left(\mathbf{R}_s^T \tilde{Q}(\hat{\mathbf{X}})\right)}$$
(40a)

s.t. 
$$R_{m,m} \ge \hat{x}_{m,n} R_m$$
, (40b)

$$R_{n,n} \ge \hat{x}_{m,n} R_n, \tag{40c}$$

$$\sum_{m=1} \sum_{n=m+1} \hat{x}_{m,n} \left( p_n + p_m \right) \leqslant P, \tag{40d}$$

$$0 \leqslant \hat{x}_{m,n}, \leqslant 1, 1 \leqslant m, n \leqslant 2K, \tag{40e}$$

$$\hat{x}_{m,n} = 0, \tag{40f}$$

$$\sum_{\substack{m=1\\2K}}^{2K} \hat{x}_{m,n} = 1, 1 \leqslant n \leqslant 2K, \tag{40g}$$

$$\sum_{n=1}^{2K} \hat{x}_{m,n} = 1, 1 \leqslant m \leqslant 2K, \tag{40h}$$

where  $\mathbf{R}_s \in \mathbb{R}^{2K \times 2K}$  is the secrecy rate matrix whose (m, n)-th element is the secrecy rate of user n against the potential eavesdropping by user m.

We can further interpret Alg. 2 as a mapping  $Q : \mathbb{R}^{2K} \times \mathbb{R}^{2K \times 2K} \times \mathbb{R}^{2K \times 2K} \to \mathbb{R}$ , which maximizes the sum secrecy rate. Then,

$$Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right) = -2^{\operatorname{tr}\left(\mathbf{R}_{s}^{T} \tilde{Q}(\hat{\mathbf{X}})\right)} + \delta_{\mathcal{F}}\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$$
(41)

where  $\bar{\mathbf{p}} = \{p_n, \forall n\}$  is the vector of the transmit powers; and the indicator function  $\delta_{\mathcal{F}}(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X})$  is given by

$$\delta_{\mathcal{F}}\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right) = \begin{cases} 0, & \text{if } \left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right) \in \mathcal{F} \\ +\infty, & \text{otherwise.} \end{cases}$$
(42)

Here,  $\mathcal{F}$  is the feasible domain of (40) defined by (40b)–(40h).

As a result, Alg. 2 can be interpreted to solve (40) using the Block Coordinate Descent (BCD). In each iteration, the algorithm sequentially solves subproblems  $\min_{\bar{\mathbf{p}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ ,  $\min_{\hat{\mathbf{X}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ , and  $\min_{\mathbf{X}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ . The convergence of each of the subproblems has been confirmed, since Section IV-A shows the semi-closed solution  $\bar{\mathbf{p}}$  and Section IV-D1 analyzes the convergence of  $\hat{\mathbf{X}}$  and  $\mathbf{X}$ . The overall convergence rate of Alg. 2 is established in the following, starting with a few definitions.

**Definition 1** (Semi-algebraic set [36]–[38]). A subset of  $\mathbb{R}^n$ , denoted by  $\mathcal{D}$ , is called semi-algebraic if there exists finite  $U, V \in \mathbb{N}$ , such that

$$\mathcal{D} = \bigcup_{u=1}^{U} \cap_{v=1}^{V} \left\{ \mathbf{z} \in \mathbb{R}^{n} \middle| p_{u,v}\left(\mathbf{z}\right) = 0, q_{u,v}\left(\mathbf{z}\right) > 0 \right\}$$
(43)

where  $p_{u,v}(\mathbf{z})$  and  $q_{u,v}(\mathbf{z})$  are real polynomial functions for  $u = 1, \dots, U$  and  $v = 1, \dots, V$ .

**Definition 2** (Semi-algebraic function [39]–[41]). Let  $\mathcal{D} \in \mathbb{R}^n$ and  $\mathcal{E} \in \mathbb{R}^m$  be two semi-algebraic sets. A mapping  $F : \mathcal{D} \to \mathcal{E}$  is semi-algebraic if its graph

$$\{(\mathbf{z}, \mathbf{o}) \in \mathcal{D} \times \mathcal{E} \mid \mathbf{o} = F(\mathbf{z})\} \subset \mathbb{R}^n \times \mathbb{R}^m$$
(44)

is a semi-algebraic set.

**Lemma 1.** The function  $Q(\cdot)$  is semi-algebraic.

With the aid of Lemma 1, the convergence rate of Alg. 2 can be established:

**Theorem 1.** When S and L exists, there exist constants  $C, \rho, q_0 > 0$ , satisfying the following inequality

$$\eta \leqslant C q^{-\frac{1}{\varrho}} \tag{45}$$

after  $q > q_0$  iterations of the overall algorithm, where  $\eta > 0$  is the tolerance. In other words,  $q \sim \mathcal{O}\left(\frac{1}{n^{\varrho}}\right)$ .

#### E. Complexity Analysis

1) Power Allocation: Since (13) and (22) provide the closed-form power allocation strategy per user group, the complexity, denoted by  $T_{PA}$ , depends linearly on the number of user groups, K; i.e.,  $T_{PA} = O(K)$ .

2) User Pairing: We analyze the computational complexity of solving (25) using the logarithmic barrier method. As discussed in Sec. IV-D1, the desired accuracy  $\epsilon$  is achieved after  $N_{\rm LP}$  logarithmic barrier method iterations. In each of the iterations, the infeasible start Newton method is performed.

The infeasible start Newton method also iterates. In each iteration of the damped Newton phase of the infeasible start Newton method, computing (28) through the LU decomposition takes  $\mathcal{T}_{LU} = \frac{2}{3} [K (2K+1)]^3 + 2 [K (2K+1)]$  floating operator points (FLOPs) [30]. The complexity of the backtracking line search is  $\mathcal{T}_1 = \mathcal{O}(K^2)$  per step. As a result, the backtracking line search in the damped Newton phase is  $\mathcal{T}_s = N_l \mathcal{T}_1 = \mathcal{O}(\log (S^2 L \kappa) K^2 / \log (\frac{1}{\tau}))$ . Moreover, updating  $\hat{\mathbf{x}}$  and  $\mathbf{w}$  in Line 6 of Alg. 1 incurs  $\mathcal{T}_{\hat{\mathbf{x}}} = 2K(2K-1)$  and  $\mathcal{T}_{\mathbf{w}} = 4K$  FLOPs [42]. Hence, the complexity of the damped Newton phase is

$$\mathcal{T}_{\rm D} = N_{\rm D} \left( \mathcal{T}_{\rm LU} + \mathcal{T}_s + \mathcal{T}_{\hat{\mathbf{x}}} + \mathcal{T}_{\mathbf{w}} \right) = \mathcal{O} \left( \frac{S^2 L \kappa \log \left( S^2 L \kappa \right)}{\zeta \tau \log \left( \frac{1}{\tau} \right)} K^2 + \frac{16}{3} K^6 \right).$$
(46)

Likewise, the complexity of the quadratically convergent phase is given by

$$\mathcal{T}_{Q} = N_{Q} \left( \mathcal{T}_{LU} + \mathcal{T}_{\hat{\mathbf{x}}} + \mathcal{T}_{\mathbf{w}} \right)$$
$$= \mathcal{O} \left( \log \left( 1 - \log \left( S^{2} L \rho \right) \right) K^{2} + \frac{16}{3} K^{6} \right)$$
(47)

Thus, the complexity of the logarithmic barrier method is

$$\mathcal{T}_{LP} = N_{LP} \left( \mathcal{T}_{D} + \mathcal{T}_{Q} \right)$$
$$= \mathcal{O} \left( \frac{\log \left( \frac{K^{2}}{\epsilon t^{(0)}} \right)}{\log \left( \xi \right)} \left( \frac{S^{2} L \kappa \log \left( S^{2} L \kappa \right)}{\zeta \tau \log \left( \frac{1}{\tau} \right)} + \log \left( 1 - \log \left( S^{2} L \rho \right) \right) \right) K^{2} + \frac{32}{3} K^{6} \right)$$
(48)

The greedy method for discretization of the user pairing utilizes double loops to search for discrete user pairing strategies. Thus, the computational complexity is  $\mathcal{T}_g = \mathcal{O}(K^2)$ . The overall complexity of user pairing in Alg. 1 is  $\mathcal{T}_{UP} = \mathcal{T}_{LP} + \mathcal{T}_g$ .

3) Overall Complexity: According to Theorem 1, it takes  $q = \mathcal{O}\left(\frac{1}{\eta^{\varrho}}\right)$  iterations for Alg. 2 to converge. Therefore, the overall complexity is  $\mathcal{T} = (\mathcal{T}_{PA} + \mathcal{T}_{UP}) q$ .

# V. SIMULATION AND DISCUSSION

Extensive simulations are provided to gauge the proposed scheme, where the users are distributed in a circular area with radius l = 300 m and the BS is located at the center of the area. The path loss exponent is set to 3. The bandwidth of each resource block is 0.5 MHz. The receiver noise power spectral density is -174 dBm/Hz.

To assess the merits of the proposed algorithm, we compare the algorithm with the following alternative approaches:

- *Equal power allocation (EPA)*: This mechanism allocates the same transmit power for all users. The proposed user pairing is used. By comparing our algorithm with the EPA, we can assess the benefit of the proposed power allocation strategy.
- *Random pairing (RP):* This mechanism randomly selects user pairs. We use the optimal power allocation strategy proposed in this paper to determine the transmit power for each user.
- *Gale-Shapley algorithm-based alternative:* We take the Gale-Shapley algorithm [18] to pair users, without considering their channel conditions. The optimal power allocation strategy proposed in this paper is used to determine the transmit power for each user.
- *Simplex method-based alternative:* We take the Simplex method [19] to solve the LP problem in user pairing. The optimal power allocation strategy developed in this paper is adopted to specify the transmit power for each user.

By comparing the proposed algorithm with the RP-, Gale-Shapley algorithm- and Simplex method-based alternatives, we can evaluate the gain of the proposed user pairing algorithm.

Fig. 1 shows the evolution of the sum secrecy rate as the number of iterations increases. It is observed that the sum secrecy rate rises quickly and usually converges within 10



Fig. 1: Sum secrecy rate against number of iterations with 2K = 6, 8, 10, and P = 20 dBm.



Fig. 2: Sum secrecy rate against user number with P = 20 dBm.

iterations. It is also noticed that the user number has a nonnegligible impact on the sum secrecy rate, especially when there are many users. The reason is that more users lead to stronger interference, hence penalizing the sum secrecy rate. Our algorithm mitigates the interference by properly allocating the power and pairing the users. These observations highlight the importance of the proposed algorithm in multiuser NOMA systems with many users.

Fig. 2 plots the sum secrecy rate as users increase in the considered system. We notice that the sum secrecy rate increases with users under all five schemes. Our approach consistently outperforms the benchmark schemes, EPA and RP, indicating the algorithm can effectively allocate the powers and pair the users to promote the sum secrecy rate. In order to verify the user pairing algorithm delivered in this paper, we compare our algorithm with the Gale-Shapley and Simplex methods. We observe that the new user pairing is more effective than the Gale-Shapley and Simplex algorithms. Although the gap of



Fig. 3: Sum secrecy rate against transmit power with 2K = 8.



Fig. 4: Running time against user number with P = 20 dBm.

the sum secrecy rate is small between the proposed algorithm and the Simplex method, our algorithm is significantly more computationally efficient than the Simplex method, as will be discussed shortly.



Fig. 5: Sum secrecy rate against  $\epsilon$  with P = 20 dBm.

Fig. 3 shows that the sum secrecy rate increases with the transmit power of the BS. This is expected because more trans-

mit power means that the users can transmit their messages at higher levels, which improves the secrecy performance. We also observe that our algorithm consistently outperforms the benchmarks, EPA, RP, Gale-Shapley and Simplex based algorithm. In other words, the new algorithm can effectively allocate the power and pair the users, leading to improved sum secrecy rate compared to alternative methods. In addition, we see that the NOMA-based EPA outperforms the NOMA-based RP, suggesting that NOMA systems are more sensitive to user pairing than they are to power allocation. All this confirms the effectiveness of our algorithm and the criticality of user pairing in NOMA.

Fig. 4 demonstrates the relationship between the running time and user number in the considered system. As anticipated, the running time increases with users, since a larger number of users require more time for the system to decide on user pairing, extending considerably the running time. It is noticed that our algorithm has the lowest complexity and the Simplex method-based alternative has the highest, albeit they achieve similar sum secrecy rates.

Last but not least, Fig. 5 presents the effect of the parameter  $\epsilon$  on the sum secrecy rate for various numbers of users in Alg. 1. It is noticed that a larger  $\epsilon$  value can cause a faster decrease in the sum secrecy rate, as  $\epsilon$  represents the tolerance for errors in the proposed algorithm. However, a smaller  $\epsilon$  value can result in a higher computational complexity, requiring more iterations to reach a satisfactory solution. Here, we set  $\epsilon = 1 \times 10^8$  in order to balance the trade-off between sum secrecy rate and running time.

# VI. CONCLUSION

This paper studied a multiuser NOMA system with untrusted IoT devices, and drew up a joint power allocation and user pairing problem in an attempt to achieve the maximum sum secrecy rate of the system, subject to the data rate requirements of individual users and the transmit power of the BS. To effectively solve this MINLP problem, we decomposed the problem between two subproblems: power allocation with a closed-form solution, and user pairing solved using the logarithmic barrier method. Simulations showed that our algorithm offers superior secrecy performance to existing alternatives, indicating that the algorithm is effective in improving the secrecy of NOMA systems and that holistic consideration of both user pairing and power allocation is critical.

#### REFERENCES

- Y. Zhang, X. Zhao, Z. Zhou, P. Qin, S. Geng, C. Xu, Y. Wang, and L. Yang, "Robust resource allocation for lightweight secure transmission in multicarrier NOMA-assisted full duplex IoT networks," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6443–6457, 2022.
- [2] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, "Cellular, wide-area, and non-terrestrial IoT: a survey on 5G advances and the road toward 6G," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 1117–1174, 2022.
- [3] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. s. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 721–742, 2017.
- [4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1773–1828, 2019.

- [5] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1878–1911, 2019.
- [6] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physicallayer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, 2019.
- [7] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.
- [8] R. Ruby, Q. V. Pham, K. Wu, A. A. Heidari, H. Chen, and B. M. ElHalawany, "Enhancing secrecy performance of cooperative NOMA-based IoT networks via multiantenna-aided artificial noise," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5108–5127, 2022.
- [9] Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding, and Y. Song, "Secure transmission in a NOMA-assisted IoT network with diversified communication requirements," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11 157–11 169, 2020.
- [10] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *IEEE Global Telecommun. Conf.*, 2018, pp. 1–6.
- [11] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure NOMA systems under untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1942–1955, 2020.
- [12] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13005– 13017, 2020.
- [13] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2930– 2943, 2020.
- [14] S. Thapar, D. Mishra, and R. Saini, "Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13259–13272, 2020.
- [15] P. K. Hota, S. Thapar, D. Mishra, R. Saini, and A. Dubey, "Ergodic performance of downlink untrusted NOMA system with imperfect SIC," *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 23–26, 2022.
- [16] I. Amin, D. Mishra, R. Saini, and S. Aïssa, "QoS-aware secrecy rate maximization in untrusted NOMA with trusted relay," *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 31–34, 2022.
- [17] S. Thapar, D. Mishra, and R. Saini, "Decoding orders for securing untrusted NOMA," *IEEE Networking Lett.*, vol. 3, no. 1, pp. 27–30, 2021.
- [18] Z. Zhou, K. Ota, M. Dong, and C. Xu, "Energy-efficient matching for resource allocation in D2D enabled cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5256–5268, 2017.
- [19] F. A. Ficken, *The simplex method of linear programming*. NY, USA: Courier Dover Publications, 2015.
- [20] H. Wang, R. P. Liu, W. Ni, W. Chen, and I. B. Collings, "Vanet modeling and clustering design under practical traffic, channel and mobility conditions," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 870–881, 2015.
- [21] I. N. Bronshtein, K. A. Semendyayev, G. Musiol, and H. Mühlig, *Handbook of mathematics*, 6th ed. Berlin, Heidelberg, German: Springer, 2015.
- [22] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "Energyefficient cooperative relaying for unmanned aerial vehicles," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1377–1386, 2016.
- [23] X. Lyu, W. Ni, H. Tian, R. P. Liu, X. Wang, G. B. Giannakis, and A. Paulraj, "Optimal schedule of mobile edge computing for Internet of things using partial information," *IEEE J. Selected Areas Commun.*, vol. 35, no. 11, pp. 2606–2615, 2017.
- [24] —, "Distributed online optimization of fog computing for selfish devices with out-of-date information," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7704–7717, 2018.
- [25] X. Lyu, H. Tian, W. Ni, Y. Zhang, P. Zhang, and R. P. Liu, "Energyefficient admission of delay-sensitive tasks for mobile edge computing," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2603–2616, 2018.
- [26] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [27] X. Zhang, A matrix algebra approach to artificial intelligence. Singapore: Springer, 2020.
- [28] C. Weihs, O. Mersmann, and U. Ligges, Foundations of statistical algorithms: with references to R packages. Boca Raton, FL, USA: CRC Press, 2013.
- [29] R. J. Vanderbei, *Linear programming*, 5th ed., C. C. Price, J. Zhu, and F. S. Hillier, Eds. New York, NY, USA: Springer, 2020.

- [30] G. H. Golub and C. F. Van Loan, *Matrix computations*. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 2013.
- [31] M. T. Heath, Scientific computing: an introductory survey, 2nd ed. PA, USA: SIAM, 2018.
- [32] K. W. Cassel, Matrix, numerical, and optimization methods in science and engineering. Cambridge, U.K.: Cambridge Univ. Press, 2021.
- [33] N. Andrei, Modern numerical nonlinear optimization, P. M. Pardalos and M. T. Thai, Eds. Cham, Switzerland: Springer Nature, 2022, vol. 195.
- [34] C. Feller, Relaxed barrier function based model predictive control. Berlin, German: Logos Verlag Berlin, 2017.
- [35] J. H. Gallier and J. Quaintance, Linear algebra and optimization with applications to machine learning volume II: fundamentals of optimization theory with applications to machine learning. World Scientific, 2020.
- [36] J. B. Lasserre, An introduction to polynomial and semi-algebraic optimization. Cambridge, U.K.: Cambridge Univ. Press, Feb. 2015.
- [37] T. Sun, H. Jiang, L. Cheng, and W. Zhu, "Iteratively linearized reweighted alternating direction method of multipliers for a class of nonconvex problems," *IEEE Trans. Signal Process.*, vol. 66, no. 20, pp. 5380–5391, 2018.
- [38] J. Bolte, S. Sabach, and M. Teboulle, "Proximal alternating linearized minimization for nonconvex and nonsmooth problems," *Math. Program.*, vol. 146, no. 1, pp. 459–494, 2014.
- [39] G. M. Lee and T. Pham, "Stability and genericity for semi-algebraic compact programs," J. Optim. Theory Appl., vol. 169, no. 2, pp. 473– 495, 2016.
- [40] H. Attouch, J. Bolte, P. Redont, and A. Soubeyran, "Proximal alternating minimization and projection methods for nonconvex problems: An approach based on the Kurdyka-Łojasiewicz inequality," *Math. Operations Res.*, vol. 35, no. 2, pp. 438–457, 2010.
- [41] C. Bao, H. Ji, Y. Quan, and Z. Shen, "l<sub>0</sub> norm based dictionary learning by proximal methods with global convergence," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2014, pp. 3858–3865.
- [42] X. Zhang, Matrix analysis and applications. Cambridge, U.K.: Cambridge Univ. Press, 2017.
- [43] A. Neyman, "From Markov chains to stochastic games," in *Stochastic Games and Applications*, A. Neyman and S. Sorin, Eds. Dordrecht: Springer Netherlands, 2003, pp. 9–25.
- [44] M. Shiota, Geometry of subanalytic and semialgebraic sets. Boston, MA, USA: Birkhäuser, 1997.
- [45] M. Donatelli and S. Serra-Capizzano, Computational methods for inverse problems in imaging. Cham, Switzerland: Springer, 2019, vol. 3.
- [46] G. H. Givens and J. A. Hoeting, *Computational statistics*, 2nd ed. Hoboken, NJ, USA: Wiley, 2012.
- [47] J. Bolte, A. Daniilidis, and A. Lewis, "The Łojasiewicz inequality for nonsmooth subanalytic functions with applications to subgradient dynamical systems," *SIAM J. Optim.*, vol. 17, no. 4, pp. 1205–1223, 2007.
- [48] Y. Xu and W. Yin, "A block coordinate descent method for regularized multiconvex optimization with applications to nonnegative tensor factorization and completion," *SIAM J. Imag. Sci.*, vol. 6, no. 3, pp. 1758–1789, 2013.
- [49] A. A. Khan, E. Köbis, and C. Tammer, Variational analysis and set optimization: developments and applications in decision making. Boca Raton, FL, USA: CRC Press, 2019.

#### Appendix A

#### PROOF OF LEMMA 1

To prove Lemma 1, we first prove the mapping  $\tilde{Q}(\hat{\mathbf{X}}) = \mathbf{X}$  is semi-algebraic. To do this, we define  $\mathbf{U} = \{(m_1, n_1), \dots, (m_K, n_K)\}$  to collect the indices chosen by the greedy method in Alg. 1, and

$$x_{m_1,n_1} \geqslant \dots \geqslant x_{m_K,n_K}; \tag{49a}$$

$$x_{m_k,n_k} \geqslant x_{m',n'}, \forall (m_k,n_k), (m',n') \notin \mathbf{U}.$$
(49b)

Let  $\mathcal{U}$  be the set of all possible U. The graph of  $\tilde{Q}\left(\mathbf{\hat{X}}\right) = \mathbf{X}$  can be given by

graph 
$$\left(\tilde{Q}\right) = \bigcup_{\mathbf{U}\in\mathcal{U}} \left\{ \left(\hat{\mathbf{X}}, \mathbf{X}\right) \middle| x_{m,n} = 1, x_{m',n'} = 0, \right.$$

$$\forall (m,n) \in \mathbf{U}, (m',n') \notin \mathbf{U} \}$$
(50)  
$$= \bigcup_{\mathbf{U} \in \mathcal{U}} \left[ \left( \bigcap_{(m,n) \in \mathbf{U}} \left\{ \left( \hat{\mathbf{X}}, \mathbf{X} \right) \middle| x_{m,n} = 1 \right\} \right) \right]$$
$$\left( \bigcap_{(m',n') \notin \mathbf{U}} \left\{ \left( \hat{\mathbf{X}}, \mathbf{X} \right) \middle| x_{m',n'} = 0 \right\} \right) \right].$$

Since (50) is semi-algebraic,  $\tilde{Q}(\hat{\mathbf{X}}) = \mathbf{X}$  is semi-algebraic.

Next, we prove that the objective function of (40) is semialgebraic. The graph of (40a) is

$$\left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}, z \right) \middle| -2^{\operatorname{tr}(\mathbf{R}_{s}^{T} \hat{\mathbf{X}})} = z \right\}$$

$$= \bigcup_{\mathbf{U} \in \mathcal{U}} \left[ \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}, z \right) \middle| \prod_{(m,n) \in \mathbf{U}} \check{p}_{m,n} = \sigma^{2} z \prod_{(m,n) \in \mathbf{U}} \check{q}_{m,n} \right\}$$

$$\cap \left( \bigcap_{(m,n) \in \mathbf{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}, z \right) \middle| x_{m,n} = 1 \right\} \right)$$

$$\left( \int_{(m',n') \notin \mathbf{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}, z \right) \middle| x_{m',n'} = 0 \right\} \right)$$

$$\cap \left( \bigcap_{(m,n) \in \mathbf{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}, z \right) \middle| \check{p}_{m,n} - \sigma^{2} \check{q}_{m,n} \geqslant 0 \right\} \right) \right],$$

$$(51)$$

where  $\check{p}_{m,n}$  and  $\check{q}_{m,n}$  are given by

$$\check{p}_{m,n} = \left( |h_m|^2 p_n + \sigma^2 \right) \left( |h_n|^2 p_n + \sigma^2 \right);$$
 (52a)

$$\check{q}_{m,n} = |h_m|^2 (p_n + p_m) + \sigma^2.$$
 (52b)

According to [43, Corol. 4], the composition of semi-algebraic function is semi-algebraic. Since the mapping  $\tilde{Q}(\hat{\mathbf{X}}) = \mathbf{X}$  is semi-algebraic, both (51) and the objective function of (40) are semi-algebraic.

Further, we prove that the indicator function  $\delta_{\mathcal{F}}(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X})$  is semi-algebraic. Specifically, we prove that the feasible domain  $\mathcal{F}$  is semi-algebraic as follows. We first show that the feasible domain  $\mathcal{F}_1$  defined by (40b) is semi-algebraic. The set  $\mathcal{F}_1$  is given by

$$\mathcal{F}_{1} = \bigcup_{\mathbf{U}\in\mathcal{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X} \right) \middle| R_{m,m} \ge R_{m}, \hat{x}_{m,n} = 1, \hat{x}_{m',n'} = 0 \right\}$$
$$= \bigcup_{\mathbf{U}\in\mathcal{U}} \left[ \left( \bigcap_{(m,n)\in\mathbf{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X} \right) \middle| \hat{p}_{m,n} \leqslant 0, \hat{x}_{m,n} = 1 \right\} \right) \right]$$
$$\bigcap \left( \bigcap_{(m',n')\notin\mathbf{U}} \left\{ \left( \bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X} \right) \middle| \hat{p}_{m',n'} \leqslant 0, \hat{x}_{m',n'} = 0 \right\} \right) \right], \tag{53}$$

where  $\hat{p}_{m,n}$  is given by

$$\hat{p}_{m,n} = \left[ (p_m + p_n) + \frac{\sigma^2}{|h_m|^2} \right] \left[ p_n^2 - \frac{\sigma^2}{|h_m|^2} (p_m - p_n) \right].$$
(54)

We can find that (53) is semi-algebraic.

Similarly, the feasible domain  $\mathcal{F}_2$  defined by (40c) is

$$\mathcal{F}_{2} = \bigcup_{\mathbf{U}\in\mathcal{U}} \left\{ \left( \mathbf{\bar{p}}, \mathbf{\hat{X}}, \mathbf{X} \right) \middle| R_{n,n} \ge R_{n}, \hat{x}_{m,n} = 1, \hat{x}_{m'n'} = 0 \right\}$$
$$= \bigcup_{\mathbf{U}\in\mathcal{U}} \left[ \left( \bigcap_{(m,n)\in\mathbf{U}} \left\{ \left( \mathbf{\bar{p}}, \mathbf{\hat{X}}, \mathbf{X} \right) \middle| \tilde{p}_{m,n} \le 0, \hat{x}_{m,n} = 1 \right\} \right) \right]$$
$$\bigcap \left( \bigcap_{(m',n')\notin\mathbf{U}} \left\{ \left( \mathbf{\bar{p}}, \mathbf{\hat{X}}, \mathbf{X} \right) \middle| \tilde{p}_{m',n'} \le 0, \hat{x}_{m',n'} = 0 \right\} \right) \right], \tag{55}$$

where  $\tilde{p}_{m,n}$  is given by

$$\tilde{p}_{m,n} = -|h_n|^2 p_n^2 + (p_m - p_n) \sigma^2.$$
(56)

We can find that (55) is also semi-algebraic.

The feasible domain  $\mathcal{F}_3$  defined by (40d)–(40h) is also semialgebraic, since these constraints are polynomial.

According to [44, eq. I.2.9.1], the intersection of semialgebraic sets is also semi-algebraic. Therefore, the feasible domain of (40), which is given by

$$\mathcal{F} = \mathcal{F}_1 \cap \mathcal{F}_2 \cap \mathcal{F}_2, \tag{57}$$

is also semi-algebraic. As a result,  $\delta_{\mathcal{F}}\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$  is semialgebraic, since the indicator function of a semi-algebraic set is semi-algebraic [45].

As discussed above, both the objective function of (40) and indicator function of feasible domain are semi-algebraic. Since the finite sum of semi-algebraic functions is also semi-algebraic [46], the mapping of the overall algorithm, i.e., (41) is semi-algebraic. This proof is complete.

# APPENDIX B Proof of Theorem 1

According to Lemma 1, the mapping of the overall algorithm is semi-algebraic. Thus, Q has the KL property [47]. Let  $\bar{\mathbf{p}}^{(q)}$ ,  $\hat{\mathbf{X}}^{(q)}$  and  $\mathbf{X}^{(q)}$  denote the  $\bar{\mathbf{p}}$ ,  $\hat{\mathbf{X}}$  and  $\mathbf{X}$  generated in the q-th iteration, respectively. { $\bar{\mathbf{p}}^{(q)}$ } is bounded since  $|h_n|$ ,  $|h_m|$  and  $\sigma$  are bounded. Similarly, both L and s are bounded. Therefore, subproblems  $\min_{\bar{\mathbf{p}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ ,  $\min_{\hat{\mathbf{X}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ , and  $\min_{\mathbf{X}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$  converge in each iteration of the overall algorithm. On the other hand, it is easy to know that both  $\hat{\mathbf{X}}^{(q)}$  and  $\mathbf{X}^{(q)}$  are bounded. When the algorithm sequentially solves  $\min_{\bar{\mathbf{p}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ ,  $\min_{\hat{\mathbf{X}}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ , and  $\min_{\mathbf{X}} Q\left(\bar{\mathbf{p}}, \hat{\mathbf{X}}, \mathbf{X}\right)$ , the sequence  $\left(\bar{\mathbf{p}}^{(q)}, \hat{\mathbf{X}}^{(q)}, \mathbf{X}^{(q)}\right)$  generated by the algorithm is bounded. According to [48], as a bounded sequence generated by the function with KL property,  $\left(\bar{\mathbf{p}}^{(q)}, \hat{\mathbf{X}}^{(q)}, \mathbf{X}^{(q)}\right)$  converges to a stationary point of (40).

Furthermore, let  $o^*$  denote the optimum of the algorithm. When S and L exists, it was shown in [48], [49] that there exist constant C,  $\rho$ , and  $q_0 > 0$ , satisfying

$$|o_q - o^*| \leqslant \frac{C}{2} q^{-\frac{1}{\varrho}},\tag{58}$$

after  $q > q_0$  iterations. Hence, we have

$$|o_q - o_{q-1}| \leq |o_q - o^*| + |o_{q-1} - o^*| \leq Cq^{-\frac{1}{\varrho}}.$$
 (59)

We can choose  $\eta$  satisfying

$$|o_q - o_{q-1}| \leqslant C q^{-\frac{1}{\varrho}} \leqslant \eta.$$
(60)

Hence, we have

$$q \geqslant \left(\frac{C}{\eta}\right)^{\varrho}.\tag{61}$$

The number of iterations of the overall algorithm is given by

$$q \sim \mathcal{O}\left(\frac{1}{\eta^{\varrho}}\right),$$
 (62)

which concludes this proof.