Non-orthogonal Multiple Access Enabled Power Allocation for Cooperative Jamming in Wireless Networks

Yuan Wu[1], Weicong Wu[2], Daohang Wang[2], Kejie Ni[2], Li Ping Qian[2,3(✉)], Weidang Lu[2], and Limin Meng[2]

[1] State Key Laboratory of Internet of Things for Smart City and Department of Computer and Information Science, University of Macau, Zhuhai, Macau SAR
[2] College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China
lpqian@zjut.edu.cn
[3] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Abstract. In this work, we investigate the non-orthogonal multiple access (NOMA) enabled power allocation for cooperative jamming under a two-user downlink scenario. In particular, we consider that there exists a malicious eavesdropper overhearing the data transmission of the mobile user (MU) with a stronger channel power gain. Meanwhile, exploiting the simultaneous transmission in NOMA, we consider that the other MU with a weak channel power gain provides cooperative jamming to the eavesdropper for enhancing the secure throughput of the stronger MU. In particular, we formulate a power allocation problem to maximize the secure throughput of the strong MU while satisfying the throughput requirement of the weak MU. Despite the non-convexity of the formulated problem, we provide an efficient algorithm to compute the optimal solution (i.e., the power allocations for the two users). Numerical results are provided to validate the effectiveness of our proposed algorithm and the performance of our optimal power allocation scheme.

Keywords: Non-orthogonal multiple access · Cooperative jamming · Power allocation

1 Introduction

Non-orthogonal multiple access (NOMA), which allows mobile users (MUs) to simultaneously use a same frequency channel for data transmission and further adopts the principle of successive interference cancellation (SIC) to mitigate the MUs' co-channel interference, has been considered as one of the enabling technologies for the fifth generation (5G) cellular systems [1,2]. Compared with the conventional orthogonal multiple access (OMA), NOMA has been expected

S. Han et al. (Eds.): AICON 2019, LNICST 286, pp. 79–93, 2019.
https://doi.org/10.1007/978-3-030-22968-9_8

to significantly improve the spectrum efficiency and the system throughput, and thus has attracted lots of research efforts. Many studies have been devoted to analyzing the potential performance advantage of NOMA [3,4], and NOMA has been exploited for many potential applications, e.g., heterogeneous cellular systems and mobile data offloading [5,6]. In particular, the proper radio resource allocation plays a critical role to reap the benefits of NOMA, and thus has attracted lost of interests for different network paradigms [7–11].

In addition to the improvement on spectrum efficiency and throughput, the simultaneous data transmissions of different MUs over a same frequency channel can also yield an important benefit, namely, the cooperative jamming to encounter the overhearing of some potential eavesdropper. Specifically, let us consider that a downlink NOMA scenario in which the base station (BS) uses NOMA to simultaneously transmit to a group of MUs. There exists a malicious eavesdropper who intentionally overhears the transmission of a targeted MU. Thanks to NOMA, the BS's transmissions to other MUs provide the cooperative jamming to the eavesdropper, which thus improves the secrecy level of the targeted MU. In this work, we thus investigate this cooperative jamming provided by NOMA via proper power allocation. Our detailed contributions in this work can be summarized as follows.

- We consider a representative scenario in which the BS uses NOMA to send data to two different MUs, i.e., one MU with a strong channel power gain and the other with a weak channel power gain, and there exists a malicious eavesdropper who intentionally overhears the strong MU's data. Thanks to NOMA, the BS's transmission to the weak MU provides a cooperative jamming to the eavesdropper and thus helps enhance the secure throughput for the strong MU. To analytically study this problem, we formulate an optimal power allocation problem that aims at maximizing the strong MU's secure throughput while satisfying the throughput requirement of the weak MU and the total power capacity of the BS.
- We use the secrecy-outage probability based on the physical layer security [12,13] to quantify how secure it is for the strong MU's transmission. Despite the non-convexity of the formulated power allocation problem, we identify the monotonic property via a vertical decomposition and thus propose an efficient layered-algorithm to compute the optimal solution. To further reduce the complexity, we exploit the hidden unimodal property with the respective to the secrecy-outage level and propose a low-complexity to compute the solution.
- We provide extensive numerical results to validate the effectiveness of our proposed algorithm and the performance advantage of the optimal cooperative jamming in enhancing the user's secure throughput.

The remainder of this paper is organized as follows. In Sect. 2, we present the system model and problem formulation. We focus on analyzing the most general case of the formulated problem in Sect. 3 and propose an efficient algorithm to compute the optimal solution. Numerical results are provided in Sect. 4, and conclusions are given in Sect. 5.

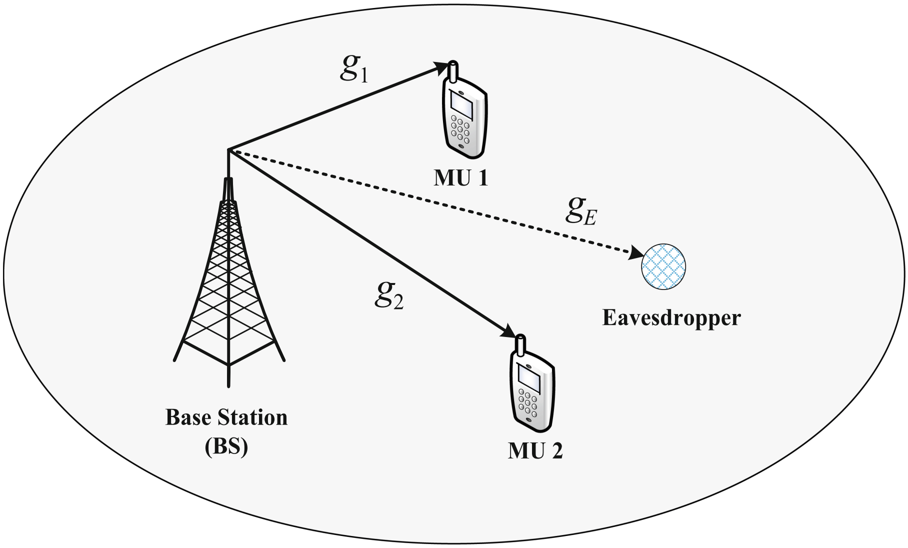


Fig. 1. System model

2 System Model and Problem Formulation

2.1 System Model and Formulation

We consider a two-user downlink NOMA scenario as shown in Fig. 1, in which the BS uses NOMA to simultaneously send data to two MUs. We use g_1, g_2, and g_{E} to denote the channel power gains from the BS to MU 1, MU 2, and the eavesdropper, respectively. For the sake of easy presentation, we assume that $g_1 \geq g_2$, meaning that MU 1 has a stronger downlink channel power gain than MU 2. Meanwhile, there exists a malicious eavesdropper who intentionally overhears the BS's data transmission to MU 1 (i.e., the strong user). Exploiting NOMA, the transmission to MU 2 provides a cooperative jamming to the eavesdropper for enhancing the security of MU 1's transmission. Let p_1 and p_2 denote the BS's transmit-powers to MU 1 and MU 2, respectively. Thus, based on the physical layer security [12,13], the secure throughput from the BS to MU 1 can be given as

$$R_1^{\mathrm{sec}} = \left[W \log_2(1 + \frac{p_1 g_1}{n_1}) - W \log_2(1 + \frac{p_1 g_E}{n_E + p_2 g_E}) \right]^+, \tag{1}$$

in which W denotes the channel bandwidth, n_1 and n_E denote the power of the background noise, respectively. Here, function $[x]^+$ denotes $\max(x, 0)$. In particular, the accurate value of g_{E} may not be available, since the eavesdropper may intentionally hide its location information. Thus, similar to [13], we assume that g_{E} follows an exponential distribution with the mean equal θ. Taking into account the randomness in g_E, we can express the probability that MU 1's data cannot be overheard by the eavesdropper as follows

$$\mathrm{P}_{\text{secure}}(x_1, p_1, p_2) = \Pr\big\{R_1^{\text{sec}} \geq x_1 | R_1^{\text{sec}} \geq 0\big\}, \tag{2}$$

where variable x_1 denotes the assigned throughput x_1 for MU 1. Correspondingly, the outage probability, i.e., the probability that MU 1's data is overheard by the eavesdropper is

$$\mathrm{P}_{\text{outage}}(x_1, p_1, p_2) = 1 - \mathrm{P}_{\text{secure}}(x_1, p_1, p_2). \tag{3}$$

With (3) we formulate the following secure throughput maximization (STM) as follows.

$$\begin{aligned}
\text{(STM)} \quad & \max x_1\big(1 - \mathrm{P}_{\text{outage}}(x_1, p_1, p_2)\big) \\
\text{subject to:} \quad & \mathrm{P}_{\text{outage}}(x_1, p_1, p_2) \leq \epsilon^{\max}, && (4) \\
& p_1 + p_2 \leq P_{\mathrm{B}}^{\text{tot}}, && (5) \\
& W \log_2\big(1 + \frac{p_2 g_2}{p_1 g_2 + n_2}\big) \geq R_2^{\text{req}}, && (6) \\
\text{variables:} \quad & x_1, p_1, \text{ and } p_2.
\end{aligned}$$

In Problem (STM), the objective function denotes MU 1's secure throughput. Constraint (4) limits the secure-outage probability for MU 1's transmission no greater than the required secrecy-requirement $\epsilon^{\max}$. Constraint (5) means that the BS's total power consumption for both MUs cannot exceed the budget of $P_{\mathrm{B}}^{\text{tot}}$, and finally, constraint (6) means that MU 2 can reach its throughput requirement R_2^{req}.

2.2 Analysis of the Secrecy-Outage Probability

To solve Problem (STM), we firstly derive the analytical expression of $\mathrm{P}_{\text{outage}}(x_1, p_1, p_2)$ as follows.

Proposition 1. *The analytical expression of the outage probability $P_{outage}(x_1, p_1, p_2)$ can be given in the following four cases:*

– *(Case-I) when $x_1 > W \log_2(1 + \frac{p_1 g_1}{n_1})$, then we have*

$$P_{outage}(x_1, p_1, p_2) = 1. \tag{7}$$

– *(Case-II) when $W \log_2(1 + \frac{p_1 g_1}{n_1}) \geq x_1 \geq W \log_2(1 + \frac{p_1 g_1}{n_1}) - W \log_2(1 + \frac{p_1}{p_2})$ and $p_2 \geq \frac{n_1}{g_1}$, then we have*

$$P_{outage}(x_1, p_1, p_2) = e^{-\frac{1}{\theta} M}, \tag{8}$$

where parameter M is given by:

$$M = \frac{n_E}{p_1} \frac{1}{\frac{1}{(1+\frac{p_1 g_1}{n_1})2^{-\frac{x_1}{W}} - 1} - \frac{p_2}{p_1}}. \tag{9}$$

– *(Case-III) when* $W\log_2(1+\frac{p_1g_1}{n_1}) - W\log_2(1+\frac{p_1}{p_2}) \geq x_1$ *and* $p_2 \geq \frac{n_1}{g_1}$*, we have*

$$P_{outage}(x_1, p_1, p_2) = 0. \tag{10}$$

– *(Case-IV) when* $W\log_2(1+\frac{p_1g_1}{n_1}) \geq x_1 \geq W\log_2(1+\frac{p_1g_1}{n_1}) - W\log_2(1+\frac{p_1}{p_2})$ *and* $p_2 < \frac{n_1}{g_1}$*, then we have*

$$P_{outage}(x_1, p_1, p_2) = \frac{e^{-\frac{1}{\theta}M} - e^{-\frac{1}{\theta}\frac{g_1n_E}{n_1-g_1p_2}}}{1-e^{-\frac{1}{\theta}\frac{g_1n_E}{n_1-g_1p_2}}}, \tag{11}$$

with parameter M *given in (9) before.*

Proof. Based on (2), we have

$$\mathrm{P}_{\mathrm{secure}}(x_1, p_1, p_2) = \frac{\Pr\{R_1^{\mathrm{sec}} \geq x_1\}}{\Pr\{R_1^{\mathrm{sec}} \geq 0\}}. \tag{12}$$

In particular, based on (1), we can derive $\Pr\{R_1^{\mathrm{sec}} \geq 0\}$ as

$$\Pr\{R_1^{\mathrm{sec}} \geq 0\} = \begin{cases} 1, & \text{when } p_2 \geq \frac{n_1}{g_1} \\ 1-e^{-\frac{1}{\theta}\frac{g_1n_E}{n_1-g_1p_2}}, & \text{when } p_2 < \frac{n_1}{g_1} \end{cases} \tag{13}$$

In particular, (13) is consistent with the intuition, namely, R_1^{sec} is always positive when p_2 is sufficiently large (i.e., MU 2 provides a sufficiently large jamming to the eavesdropper).

To derive $\Pr\{R_1^{\mathrm{sec}} \geq x_1\}$ (with $x_1 \geq 0$), we consider:

$$\begin{aligned} & W\log_2(1+\frac{p_1g_1}{n_1}) - W\log_2(1+\frac{p_1g_E}{n_E+p_2g_E}) \geq x_1 \\ \Longleftrightarrow\ & \frac{n_1+p_1g_1}{n_1}2^{-\frac{x_1}{W}} - 1 \geq \frac{p_1g_E}{n_E+p_2g_E} \quad (14) \\ \Longleftrightarrow\ & \frac{n_E}{p_1g_E} \geq \frac{1}{(1+\frac{p_1g_1}{n_1})2^{-\frac{x_1}{W}}-1} - \frac{p_2}{p_1} \quad (15) \end{aligned}$$

Notice that the equivalence between (14) and (15) requires $x_1 \leq W\log_2(1+\frac{p_1g_1}{n_1})$. Otherwise (i.e., $x_1 > W\log_2(1+\frac{p_1g_1}{n_1})$), there always exists $\Pr\{R_1^{\mathrm{sec}} \geq x_1\} = 0$ according to (1), which leads to Case-I in Proposition 1.

In the next, we consider $x_1 \leq W\log_2(1+\frac{p_1g_1}{n_1})$ for Case-II, Case-III, and Case-IV.

In particular, let us first consider the case that $p_2 \geq \frac{n_1}{g_1}$ (i.e., the case of $\Pr\{R_1^{\mathrm{sec}} \geq 0\} = 1$ in Eq. (13)). Then, we have

$$\begin{aligned} & \Pr\{R_1^{\mathrm{sec}} \geq x_1\} = 1 \text{ when } p_2 \geq \frac{n_1}{g_1} \text{ and} \\ & x_1 \leq W\log_2(1+\frac{p_1g_1}{n_1}) - W\log_2(1+\frac{p_1}{p_2}). \end{aligned} \tag{16}$$

As a result, we have $\mathrm{P}_{\text{outage}}(x_1, p_1, p_2) = 0$, which corresponds to Case-III in Proposition 1.

In addition, we have

$$\Pr\{R_1^{\text{sec}} \geq x_1\} = \Pr\{g_E \leq M\} \text{ when } p_2 \geq \frac{n_1}{g_1},$$

and

$$W \log_2(1 + \frac{p_1 g_1}{n_1}) \geq x_1 \geq W \log_2(1 + \frac{p_1 g_1}{n_1}) - W \log_2(1 + \frac{p_1}{p_2}),$$

where parameter M is given in Eq. (9) (notice that M can be derived from (15)). As a result, we have

$$\mathrm{P}_{\text{outage}}(x_1, p_1, p_2) = e^{-\frac{1}{\theta}M}, \tag{17}$$

which corresponds to Case-II in Proposition 1.

Finally, when $p_2 < \frac{n_1}{g_1}$, i.e., the case of $\Pr\{R_1^{\text{sec}} \geq 0\} = 1 - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}$ in Eq. (13), then we again have

$$\Pr\{R_1^{\text{sec}} \geq x_1\} = \Pr\{g_E \leq M\} \text{ when } p_2 < \frac{n_1}{g_1},$$

and

$$W \log_2(1 + \frac{p_1 g_1}{n_1}) \geq x_1 \geq W \log_2(1 + \frac{p_1 g_1}{n_1}) - W \log_2(1 + \frac{p_1}{p_2}).$$

As a result, we have

$$\mathrm{P}_{\text{outage}}(x_1, p_1, p_2) = \frac{e^{-\frac{1}{\theta}M} - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}}{1 - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}} \tag{18}$$

which corresponds to Case-IV in Proposition 1. Notice that based on (9), there always exists $M < \frac{g_1 n_E}{n_1 - g_1 p_2}$.

We thus finish the proof of Proposition 1.

To solve Problem (STM), we need to consider the above four cases given in Proposition 1, and the maximum secure throughput V^* of Problem (STM) can be given as:

$$V^* = \max\{V^{\text{I}*}, V^{\text{II}*}, V^{\text{III}*}, V^{\text{IV}*}\}, \tag{19}$$

where $V^{\text{I}*}, V^{\text{II}*}, V^{\text{III}*}$, and $V^{\text{IV}*}$ denote MU 1's maximum secure throughput under Case-I, Case-II, Case-III, and Case-IV, respectively. It is noticed that Case-I is a trivial case since $V^{\text{I}*} = 0$. In the following, due to the limited space in the paper, we focus on solving Problem (STM) under the most difficult case, i.e., Case-IV. The other two cases, i.e., Case-II and Case-III, can solved in a similar manner.

3 Optimization Problem Under Case IV

In this section, we focus on solving Problem (STM) under Case-IV. We introduce an auxiliary variable ϵ which denotes the secrecy-outage probability of MU 1, i.e.,

$$\epsilon = \frac{e^{-\frac{1}{\theta}M} - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}}{1 - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}} \tag{20}$$

according to (11).

Thus, based on (20), we can derive the following secrecy-based throughput for MU 1:

$$\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2) = W\log_2(1 + \frac{p_1 g_1}{n_1}) - W\log_2(1 + \frac{p_1 z_{(\epsilon,p_2)}}{n_E + p_2 z_{(\epsilon,p_2)}}), \tag{21}$$

where parameter $z_{(\epsilon,p_2)}$ is given by:

$$z_{(\epsilon,p_2)} = -\theta \ln\left(\epsilon + (1-\epsilon)e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}\right). \tag{22}$$

Notice that $z_{(\epsilon,p_2)}$ is always positive, since $p_2 \leq \frac{n_1}{g_1}$ holds in Case-IV. The secrecy-based throughput $\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2)$ can be treated as the maximum throughput of MU 1, under the given transmit-powers (p_1, p_2) as well as the given level of the secrecy-outage ϵ.

An observation on $\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2)$ is as follows.

Lemma 1. *There always exists*

$$\hat{x}_1^{IV}(\epsilon, p_1, p_2) > W\log_2(1 + \frac{p_1 g_1}{n_1}) - W\log_2(1 + \frac{p_1}{p_2}),$$

meaning that $\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2)$ is compatible with the conditions of Case- IV in Proposition 1.

Proof. Based on (21), we can analytically express $\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2)$ as follows:

$$\begin{aligned}\hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2) &= W\log_2(1 + \frac{p_1 g_1}{n_1}) - W\log_2(1 + \frac{p_1 z_{(\epsilon,p_2)}}{n_E + p_2 z_{(\epsilon,p_2)}}) \\ &> W\log_2(1 + \frac{p_1 g_1}{n_1}) - W\log_2(1 + \frac{p_1}{p_2}).\end{aligned}$$

We thus finish the proof of Lemma 1.

Based on Lemma 1, we can obtain the equivalent form of Problem (STM) under Case-IV as follows:

$$\begin{aligned}\text{(STM-E-IV):}\quad & \max \hat{x}_1^{\mathrm{IV}}(\epsilon, p_1, p_2)(1-\epsilon) \\ \text{subject to:}\quad & p_2 \leq \frac{n_1}{g_1}, & (23)\\ & 0 \leq \epsilon \leq \epsilon^{\max}, & (24)\\ & \text{constraints (5), (6), and (21).} \\ \text{variables:}\quad & p_1, p_2, \text{ and } \epsilon.\end{aligned}$$

Notice that constraint (23) comes from the condition of Case-IV. However, directly solving Problem (STM-E-IV) is still difficult since Problem (STM-E-IV) is a non-convex optimization problem [14].

To tackle with this difficulty, we exploit a vertical decomposition as follows. Suppose that the values of (p_2, ϵ) are given in advance. We firstly aim at finding the corresponding optimal p_1 (as a response to (p_2, ϵ)), which corresponds to solving the following optimization problem:

$$\text{(STM-E-IV-Sub)}\ V_{(p_2,\epsilon)}^{\text{IV-Sub}} = \max \frac{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_1 g_1(n_E + p_2 z_{(\epsilon,p_2)})}{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_1 n_1 z_{(\epsilon,p_2)}}$$

$$\text{variable: } 0 \le p_1 \le \min\left\{p_2(2^{\frac{R_2^{\text{req}}}{W}} - 1)^{-1} - \frac{n_2}{g_2}, P_B^{\text{tot}} - p_2\right\}. \tag{25}$$

In particular, we can analytically solve Problem (STM-E-IV-Sub) based on the following result.

Proposition 2. *Given (p_2, ϵ), the optimal solution of Problem (STM-E-IV-Sub) can be analytically given by:*

$$p_{1,(p_2)}^{IV*} = \begin{cases} p_2(2^{\frac{R_2^{req}}{W}} - 1)^{-1} - \frac{n_2}{g_2}, & \text{if } p_2 \le p_2^{IV,Tr} \\ P_B^{tot} - p_2, & \text{else} \end{cases} \tag{26}$$

where $p_2^{IV,Tr} = \frac{2^{\frac{R_2^{req}}{W}} - 1}{2^{\frac{R_2^{req}}{W}}}(P_B^{tot} + \frac{n_2}{g_2})$*, if the following condition holds:*

$$\frac{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_{1,(p_2)}^{IV*} g_1(n_E + p_2 z_{(\epsilon,p_2)})}{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_{1,(p_2)}^{IV*} n_1 z_{(\epsilon,p_2)}} > 1. \tag{27}$$

Otherwise (namely, (27) does not hold), then Problem (STM-E-IV-Sub) is infeasible.

Proof. The key of the proof is to show that the first order derivative of the objective function of Problem (STM-E-IV-Sub) is increasing in p_1. Therefore, for the sake of clear presentation, we introduce the following three auxiliary parameters:

$$A = n_1(n_E + p_2 z_{(\epsilon,p_2)}), \tag{28}$$

$$B = g_1(n_E + p_2 z_{(\epsilon,p_2)}), \tag{29}$$

$$C = n_1 z_{(\epsilon,p_2)}. \tag{30}$$

With the above defined A, B, and C, we can derive

$$\frac{d}{dp_1}\left(\frac{A + Bp_1}{A + Cp_1}\right) = \frac{A(B - C)}{(A + Cp_1)^2}. \tag{31}$$

We next focus on proving that $B > C$, namely, $g_1(n_E + p_2 z_{(\epsilon,p_2)}) > n_1 z_{(\epsilon,p_2)}$ always holds. The details are as follows. Based on (22) and $p_2 < \frac{n_1}{g_1}$, we can make the following derivations:

$$
\begin{aligned}
& g_1(n_E + p_2 z_{(\epsilon,p_2)}) > n_1 z_{(\epsilon,p_2)} \\
\Longleftrightarrow\ & \frac{g_1 n_E}{n_1 - g_1 p_2} \geq z_{(\epsilon,p_2)} = -\theta \ln\left(\epsilon + (1-\epsilon) e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}}\right) \\
\Longleftrightarrow\ & e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}} \leq \epsilon + (1-\epsilon) e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}} \\
\Longleftrightarrow\ & e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}} \leq e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}} + (1 - e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}})\epsilon.
\end{aligned}
$$

With $p_2 < \frac{n_1}{g_1}$, we have $e^{-\frac{1}{\theta}\frac{g_1 n_E}{n_1 - g_1 p_2}} < 1$, meaning that the above inequality always holds. As a result, $B > C$ always holds, which finishes the proof. Since the objective function of Problem (STM-E-IV-Sub) is increasing in p_1, it gives us the optimal solution in (26). Meanwhile, condition 27 is used to guarantee that $\hat{x}_1^{\mathrm{IV}}(\epsilon, p_{1,(p_2)}^{\mathrm{IV}*}, p_2) \geq 0$.

As a result, we can analytically express $V_{(p_2,\epsilon)}^{\text{IV-Sub}}$ as follows:

$$
V_{(p_2,\epsilon)}^{\text{IV-Sub}} = \frac{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_{1,(p_2)}^{\mathrm{IV}*} g_1 (n_E + p_2 z_{(\epsilon,p_2)})}{n_1(n_E + p_2 z_{(\epsilon,p_2)}) + p_{1,(p_2)}^{\mathrm{IV}*} n_1 z_{(\epsilon,p_2)}}. \tag{32}
$$

3.1 Proposed Algorithm to Find the Optimal (p_2, ϵ)

Based on (32), we then continue to find the optimal (p_2, ϵ), which corresponds to solving the following problem:

$$
\begin{aligned}
\text{(STM-E-IV-Top):} \quad & \max (1-\epsilon) W \log_2 \left(V_{(p_2,\epsilon)}^{\text{IV-Sub}}\right) \\
\text{subject to:} \quad & 0 \leq p_2 \leq \min\{P_B^{\text{tot}}, \tfrac{n_1}{g_1}\}, \\
& \text{constraints: (32) and (24)}, \\
\text{variables:} \quad & (p_2, \epsilon).
\end{aligned}
$$

An important observation of Problem (STM-E-IV-Top) is that p_2 falls within a fixed interval $p_2 \in [0, \min\{P_B^{\text{tot}}, \frac{n_1}{g_1}\}]$, and ϵ falls within a fixed interval $\epsilon \in [0, \epsilon^{\max}]$. Therefore, to solve Problem (STM-E-IV-Top), we can perform a two-dimensional linear-search (2DLS) on (p_2, ϵ) within $[0, \min\{P_B^{\text{tot}}, \frac{n_1}{g_1}\}] \times [0, \epsilon^{\max}]$ (with small step-sizes Δ_ϵ and Δ_p). The details are shown in the following 2DLS-Algorithm. Notice that the overall complexity in solving Problem (STM) under Case-IV is just $\frac{\epsilon^{\max}}{\Delta_\epsilon}\frac{\min\{P_B^{\text{tot}}, \frac{n_1}{g_1}\}}{\Delta_p}$.

Let $(p_2^{\mathrm{IV}*}, \epsilon^{\mathrm{IV}*})$ denote the output of our 2DLS-Algorithm. Then, we have $p_1^{\mathrm{IV}*} = p_{1,(p_2^{\mathrm{IV}*})}^{\mathrm{IV}*}$ (according to (26)), and $x_1^{\mathrm{IV}*} = \hat{x}_1^{\mathrm{IV}}(\epsilon^{\mathrm{IV}*}, p_1^{\mathrm{IV}*}, p_2^{\mathrm{IV}*})$ (according to (21)). Thus, the maximum secure throughput of MU 1 under Case-IV is $V^{\mathrm{IV}*} = x_1^{\mathrm{IV}*}(1 - \epsilon^{\mathrm{IV}*})$.

Sub-Algorithm: to solve top-problem (STM-E-IV-Sub) and find $(V^{\textbf{IV-Sub}}_{(p_2^{\textbf{cur}},\epsilon^{\textbf{cur}})})$

Input: p_2^{cur} and ϵ^{cur}.
Set $p^{\mathrm{IV}*}_{1,(p_2^{\mathrm{cur}})}$ according to (26).
if constraint(27) holds **then**
  Set $V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}$ according to (32).
else
  Set $V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})} = 1$.
end if
Output: $V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}$ and $(1-\epsilon^{\mathrm{cur}})W\log_2\big(V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}\big)$.

2DLS-Algorithm: to solve top-problem (STM-E-IV-Top) and output $V^{\textbf{IV}*}$ and the corresponding $(p_2^{\textbf{IV}*},\epsilon^{\textbf{IV}*})$

Initialization: Set step-size Δ_ϵ and Δ_p as a small number. Set CBV $=0$ and CBS $=\emptyset$.
Set $p_2^{\mathrm{cur}} = \Delta_p$, $\epsilon^{\mathrm{cur}} = \Delta_\epsilon$.
while $p_2^{\mathrm{cur}} \leq \min\{P_B^{\mathrm{tot}}, \frac{n_1}{g_1}\}$ **do**
  while $\epsilon^{\mathrm{cur}} \leq \epsilon^{\max}$ **do**
    Use Sub-Algorithm to compute $V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}$.
    if $(1-\epsilon^{\mathrm{cur}})W\log_2\big(V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}\big) > \mathrm{CBV}$ **then**
      Set CBV $= (1-\epsilon^{\mathrm{cur}})W\log_2\big(V^{\mathrm{IV\text{-}Sub}}_{(p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})}\big)$.
      Set CBS $= (p_2^{\mathrm{cur}},\epsilon^{\mathrm{cur}})$.
    end if
    Update $\epsilon^{\mathrm{cur}} = \epsilon^{\mathrm{cur}} + \Delta_\epsilon$.
  end while
  Update $p_2^{\mathrm{cur}} = p_2^{\mathrm{cur}} + \Delta_p$.
end while
Output: $V^{\mathrm{IV}*} = \mathrm{CBV}$ and $(p_2^{\mathrm{IV}*},\epsilon^{\mathrm{IV}*}) = \mathrm{CBS}$.

3.2 A Low-Complexity Algorithm Based on the Brent's Method

To further reduce the complexity of 2DLS-Algorithm, we identify the following property. Specifically, support that the value of p_2 is given in advance, we enumerate $\epsilon \in [0,\epsilon^{\max}]$ with a small step-size Δ_ϵ. The corresponding results are shown in Fig. 2 below. Notice that for each given (p_2,ϵ), we can use (26) to compute $p^{\mathrm{IV}*}_{1,(p_2)}$ and obtain the corresponding secure throughput $(1-\epsilon)W\log_2\big(V^{\mathrm{IV\text{-}Sub}}_{(p_2,\epsilon)}\big)$. Specifically, the left subplot shows the case when $p^{\mathrm{IV}*}_{1,(p_2)} = p_2(2^{\frac{R_2^{\mathrm{req}}}{W}}-1)^{-1} - \frac{n_2}{g_2}$, and the right subplot shows the case when $p^{\mathrm{IV}*}_{1,(p_2)} = P_B^{\mathrm{tot}} - p_2$.

As shown in both subplots, with the respectively given p_2, the secure throughput is always unimodal in ϵ. Such a phenomenon is consistent with the intuition, namely, neither a too large ϵ nor a too small ϵ will be beneficial to the secure throughput. A too large ϵ (meaning a too weak secrecy-level) will directly reduce the secure throughput. In comparison, a too small ϵ (meaning a too strict secrecy-level) will require larger a larger power consumption, which consequently limits the secure throughput due to (5). Thanks to this hidden unimodal property, we can use the Brent's method [15] to find ϵ^* under given p_2. The Brent's method is a numerical algorithm that jointly exploits the golden-section search and the parabolic interpolation, with the objective of efficiently finding the optimum of a single-variable function. In particular, for the unimodal function [15], the Brent's method is guaranteed to find its global optimum within a given interval. Due to the limited space in this paper, we skip the detailed operations of the Brent's method here. Interested readers can refer to [15] for the details. In particular, we emphasize within each round of the iteration in this Brent's method, we need to Sub-Algorithm to compute the value of $V^{\text{IV-Sub}}_{(p_2^{\text{cur}},\epsilon)}$ under the given ϵ (which is being currently evaluated in the Brent's method) as well as the given p_2^{cur}. Therefore, based on the output of the Brent's, we can further execute a linear-search of $p_2 \in [0, \min\{P_B^{\text{tot}}, \frac{n_1}{g_1}\}]$, which leads to the proposed LSBM-Algorithm. Here, "LSBM" means linear-search and the Brent's method.

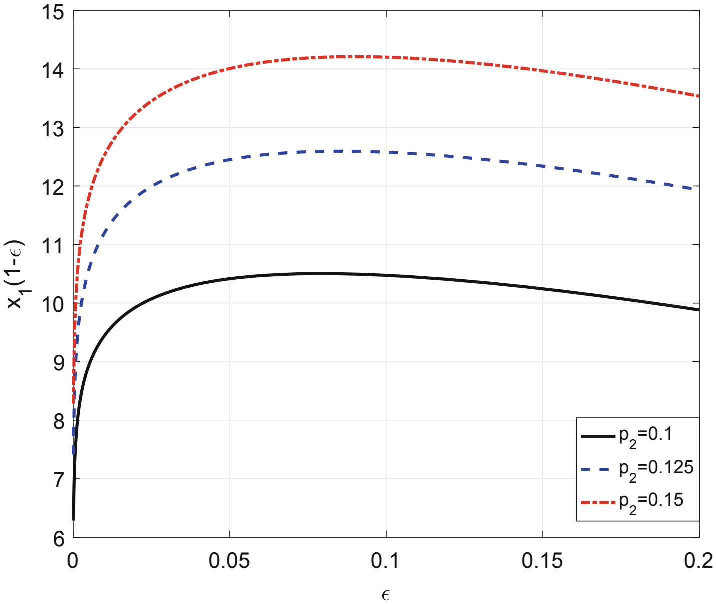
Although it is technically challenging to prove the unimodal property of the secure throughput of MU 1 with respect to ϵ, our following numerical results in Tables 1 and 2 show that our proposed LSBM-Algorithm can achieve the result almost same (with a negligible relative error) as our 2DLS-Algorithm. In the meantime, thanks to exploiting the Brent's method, LSBM-Algorithm can significantly reduce the computational time compared with 2DLS-Algorithm.

LSBM-Algorithm: to solve top-problem (STM-E-IV-Top) and find $(p_2^{\mathbf{IV}*}, \epsilon^{\mathbf{IV}*})$

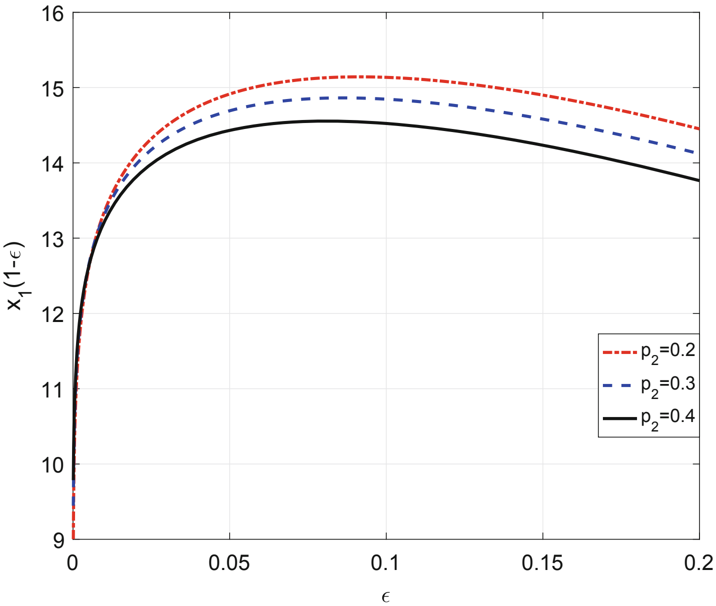
1: **Initialization:** Set step-size Δ_p as a small number. Set CBV $= 0$.
2: Set $p_2^{\text{cur}} = \Delta_p$.
3: **while** $p_2^{\text{cur}} \leq \min\{P_B^{\text{tot}}, \frac{n_1}{g_1}\}$ **do**
4: Use the Brent's method to compute $V^{\text{IV-Sub}}_{(p_2^{\text{cur}},\epsilon^{\text{cur}})}$ and ϵ^{cur}.
5: **if** $(1-\epsilon^{\text{cur}})W\log_2\left(V^{\text{IV-Sub}}_{(p_2^{\text{cur}},\epsilon^{\text{cur}})}\right) > \text{CBV}$ **then**
6: Set CBV $= (1-\epsilon^{\text{cur}})W\log_2\left(V^{\text{IV-Sub}}_{(p_2^{\text{cur}},\epsilon^{\text{cur}})}\right)$ and $(p_2^*, \epsilon^*) = (p_2^{\text{cur}}, \epsilon^{\text{cur}})$.
7: **end if**
8: Update $p_2^{\text{cur}} = p_2^{\text{cur}} + \Delta_p$.
9: **end while**
10: **Output**: $V^{\text{IV}*} = \text{CBV}$ and $(p_2^{\text{IV}*}, \epsilon^{\text{IV}*})$.

4 Numerical Results

We present the numerical results in this section. Figure 2 validates the unimodal property of the secure throughput in ϵ under the given p_2. Specifically, the left subplot shows the case when $p_2 \leq p_2^{\text{IV,Tr}}$, which leads to $p^{\text{IV}*}_{1,(p_2)} = p_2(2^{\frac{R_2^{\text{req}}}{W}} - 1)^{-1} - \frac{n_2}{g_2}$, The right subplot shows the case when $p_2 > p_2^{\text{IV,Tr}}$, which



(a) When $p^{\mathrm{IV}*}_{1,(p_2)} = p_2(2^{\frac{R_2^{\mathrm{req}}}{W}} - 1)^{-1} - \frac{n_2}{g_2}$



(b) When $p^{\mathrm{IV}*}_{1,(p_2)} = P_B^{\mathrm{tot}} - p_2$

Fig. 2. Illustration of hidden unimodal property of the secure throughput in ϵ under the given p_2. We set $W = 10$MHz, $P_B^{\mathrm{tot}} = 2$W, $R_2^{\mathrm{req}} = 1$Mbits, $n_1 = 1*10^{-6}$, $n_2 = 1*10^{-6}$, $n_E = 1*10^{-6}$, $\theta = 1*10^{-7}$, and $\epsilon^{\max} = 0.2$. In addition, the randomly generated channel power gains from the BS to the two MUs are $\{g_i\} = \{1.9330 * 10^{-6}, 1.9047 * 10^{-6}\}$.

thus leads to $p_{1,(p_2)}^{\mathrm{IV}*} = P_B^{\mathrm{tot}} - p_2$. As explained before in Sect. 3.2, when we enumerate ϵ, the corresponding MU 1's secure throughput (under different given p_2) always increases firstly and then gradually decreases, i.e., showing the unimodal property.

Tables 1 and 2 show the performance comparison between our proposed 2DLS-Algorithm and LSBM-Algorithm. In particular, the results show that LSBM-Algorithm can achieve approximately the same result as 2DLS-Algorithm($\Delta_p = 0.001$,$\Delta_\epsilon = 0.001$), while consuming a significantly less computation time. Such an advantage essentially stems from that we exploit the unimodal property of the secure throughput with respect to ϵ, which thus saves the operation of the linear-search in ϵ.

Table 1. 2-MU Scenario: We fix $W_i = 10$ MHz, and $\epsilon^{\max} = 0.2$

With $\theta = 1 * 10^{-7}$	$P_B^{\mathrm{tot}} = 1$ W	$P_B^{\mathrm{tot}} = 3$ W	$P_B^{\mathrm{tot}} = 5$ W	$P_B^{\mathrm{tot}} = 7$ W	$P_B^{\mathrm{tot}} = 9$ W	Ave. error
2DLS-Algorithm	10.7024, 2.6259 s	17.8531, 2.3464 s	20.9709, 2.1135 s	22.8431, 2.1369 s	22.9778, 2.0802 s	0.0023%
LSBM-Algorithm	10.7026, 0.1833 s	17.8535, 0.1717 s	20.9711, 0.1585 s	22.8436, 0.2006 s	22.9788, 0.2287 s	
With $\theta = 2 * 10^{-7}$	$P_B^{\mathrm{tot}} = 1$ W	$P_B^{\mathrm{tot}} = 3$ W	$P_B^{\mathrm{tot}} = 5$ W	$P_B^{\mathrm{tot}} = 7$ W	$P_B^{\mathrm{tot}} = 9$ W	Ave. error
2DLS-Algorithm	8.8601, 2.4043 s	14.4397, 2.4194 s	16.9766, 2.4750 s	18.2725, 2.3883 s	18.3641, 2.4481 s	0.0021%
LSBM-Algorithm	8.8603, 0.2390 s	14.4404, 0.2243 s	16.9768, 0.2878 s	18.2727, 0.2250 s	18.3643, 0.2086 s	

Table 2. 2-MU Scenario: We fix $W_i = 16$ MHz, and $\epsilon^{\max} = 0.2$

With $\theta = 1 * 10^{-7}$	$P_B^{\mathrm{tot}} = 1$ W	$P_B^{\mathrm{tot}} = 3$ W	$P_B^{\mathrm{tot}} = 5$ W	$P_B^{\mathrm{tot}} = 7$ W	$P_B^{\mathrm{tot}} = 9$ W	Ave. error
2DLS-Algorithm	17.4824, 1.9048 s	28.7146, 2.0574 s	33.5533, 1.9295 s	36.5498, 2.1404 s	38.4497, 2.2434 s	0.0017%
LSBM-Algorithm	17.4827, 0.1969 s	28.7152, 0.1781 s	33.5538, 0.1757 s	36.5503, 0.1983 s	38.4501, 0.2026 s	
With $\theta = 2 * 10^{-7}$	$P_B^{\mathrm{tot}} = 1$ W	$P_B^{\mathrm{tot}} = 3$ W	$P_B^{\mathrm{tot}} = 5$ W	$P_B^{\mathrm{tot}} = 7$ W	$P_B^{\mathrm{tot}} = 9$ W	Ave. error
2DLS-Algorithm	14.4187, 2.3016 s	23.1039, 2.4512 s	27.1639, 2.5397 s	29.2377, 2.5824 s	30.5101, 2.5057 s	0.0014%
LSBM-Algorithm	14.4191, 0.2444 s	23.1046, 0.2471 s	27.1640, 0.2482 s	29.2380, 0.2811 s	30.5101, 0.2683 s	

Figure 3 shows the impact of MU 2's throughput requirement R_2^{req}. We set $W = 10$MHz, $n_1 = 1{*}10^{-6}$, $n_2 = 1{*}10^{-6}$, $n_E = 1{*}10^{-6}$, $\theta = 1{*}10^{-7}$, and $\epsilon^{\max} = 0.2$. In addition, the randomly generated channel power gains from the BS to the two MUs are $\{g_i\} = \{1.9330 * 10^{-6}, 1.9047 * 10^{-6}\}$. As shown in Fig. 3, the MU 1's maximum secure throughput gradually decreases when R_2^{req} increases, which is consistent with the intuition. Corresponding, the corresponding ϵ^* gradually decreases, meaning that a stronger secrecy-level is provided to avoid a significant loss in the secure throughput.

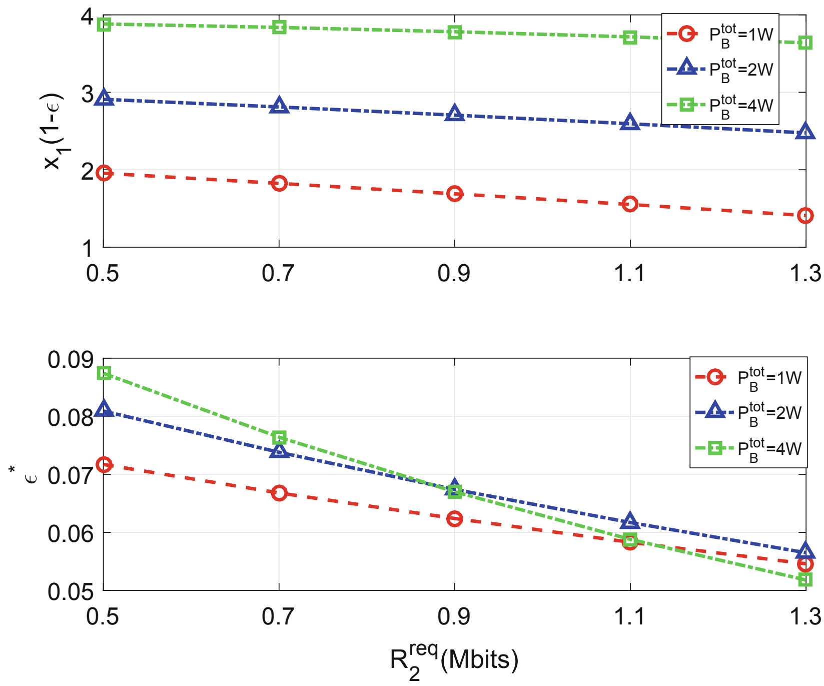


Fig. 3. Impact of MU 2's throughput requirement R_2^{req}.

5 Conclusion

In this paper, we have investigated the optimal power allocation for cooperative jamming in NOMA systems under a two-user downlink scenario. Specifically, exploiting the two MUs' simultaneous transmissions in NOMA, we use the BS's transmission to MU 2 (i.e., the MU with a weak channel power gain) to provide a jamming to the eavesdropper who intentionally overhears the BS's transmission to MU 1 (i.e., the MU with a strong channel power gain). To study this cooperative jamming, we have formulated a power allocation problem to maximize the secure throughput of MU 1 while satisfying the throughput requirement of MU 2. Despite the non-convexity of the above formulated problem, we have provided two efficient algorithms to compute the optimal solution. In addition, Numerical results have been provided to validate the effectiveness of our proposed algorithms and the performance of our proposed cooperative jamming scheme in NOMA.

Acknowledgement. This work was supported in part by the National Natural Science Foundation of China under Grant 61572440, in part by the Zhejiang Provincial Natural Science Foundation of China under Grants LR17F010002 and LR16F010003, and in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2019D11).

References

1. Liu, Y., Qin, Z., Elkashlan, M., Ding, Z., Nallanathan, A., Hanzo, L.: Non-orthogonal multiple access for 5G and beyond. Proc. IEEE **105**(12), 2347–2381 (2017)
2. Dai, L., et al.: Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. IEEE Commun. Mag. **53**(9), 74–81 (2015)
3. Zhang, Z., Sun, H., Hu, R.Q.: Downlink and uplink nonorthogonal multiple access in a dense wireless network. IEEE J. Sel. Areas Commun. **35**(17), 2771–2784 (2017)
4. Ding, Z., Fan, P., Poor, H.V.: Impact of user pairing on 5G nonorthogonal multiple access. IEEE Trans. Veh. Technol. **65**(8), 6010–6023 (2016)
5. Ding, Z., et al.: Application of non-orthogonal multiple access in LTE and 5G networks. IEEE Commun. Mag. **55**(2), 185–191 (2017)
6. Wu, Y., Chen, J., Qian, L., Huang, J., Shen, X.: Energy-aware cooperative traffic offloading via device-to-device cooperations: an analytical approach. IEEE Trans. Mob. Comput. **16**(1), 97–114 (2017)
7. Zhang, Y., Wang, H., Zheng, T., Yang, Q.: Energy-efficient transmission design in non-orthogonal multiple access. IEEE Trans. Veh. Technol. **66**(3), 2852–2857 (2017)
8. Zhang, S., Di, B., Song, L., Li, Y.: Sub-channel and power allocation for non-orthogonal multiple access relay networks with amplify-and-forward protocol. IEEE Trans. Wirel. Commun. **16**(4), 2249–2261 (2017)
9. Qian, L., Wu, Y., Zhou, H., Shen, X.: Joint uplink base station association and power control for small-cell networks with non-orthogonal multiple access. IEEE Trans. Wirel. Commun. **16**(9), 5567–5582 (2017)
10. Wu, Y., Qian, L., Mao, H., Yang, X., Shen, X.: Optimal power allocation and scheduling for non-orthogonal multiple access relay-assisted networks. IEEE Trans. Mob. Comput. **17**(11), 2591–2606 (2018)
11. Wu, Y., Ni, K., Zhang, C., Qian, L., Tsang, D.H.K.: NOMA assisted multi-access mobile edge computing: a joint optimization of computation offloading and time allocation. IEEE Trans. Veh. Technol. **67**(12), 12244–12258 (2018)
12. Zhang, N., Cheng, N., Lu, N., Zhang, X., Mark, J.W., Shen, X.: Partner selection and incentive mechanism for physical layer security. IEEE Trans. Wirel. Commun. **14**(8), 4265–4276 (2015)
13. Yue, J., Ma, C., Yu, H., Zhou, W.: Secrecy-based access control for device-to-device communication underlaying cellular networks. IEEE Commun. Lett. **17**(11), 2068–2071 (2013)
14. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, England (2004)
15. Brent, R.P.: Chapters 3–4 in Algorithms for Minimization Without Derivatives. Prentice-Hall, Englewood Cliffs (1973)