Resource Allocation for Enhancing Offloading Security in NOMA-Enabled MEC Networks

Wei Wu, *Member, IEEE,* Xinxin Wang, Fuhui Zhou, *Member, IEEE,* Kai-Kit Wong, *Fellow, IEEE,* Chunguo Li, *Senior Member, IEEE,* and Baoyun Wang, *Member, IEEE*

***Abstract*—This letter studies an uplink non-orthogonal multiple access (NOMA) enabled mobile-edge computing (MEC) network. Specifically, we focus on the practical design of secure offloading without knowing the eavesdropper's channel state information. The aim is to maximize the minimum anti-eavesdropping ability (AEA) for uplink NOMA users subject to the worst-case secrecy rate requirements and limited transmission power budgets. The formulated problem is non-convex and difficult to be solved directly. In order to tackle this issue, we propose an efficient iterative algorithm by jointly designing the secrecy rate, local computing bits and power allocation. The local computing bits and the power allocation are derived in closed form. Numerical results are provided to demonstrate the efficiency of our proposed scheme in terms of AEA.**

***Index Terms*—Non-orthogonal multiple access, mobile edge computing, anti-eavesdropping ability, physical layer security, resource allocation.**

I. Introduction

Recently, the demand of mobile data traffic has explosively grown in Internet of Things (IoT). However, the energy-constrained low-computing capability mobile terminal is not able to support an increasing number of applications which require sustainable and high-intensive computations, e.g., virtual/augmented reality (VR/AR), remote surgery and autonomous driving [1].

In order to overcome these challenges, mobile edge computing (MEC) and non-orthogonal multiple access (NOMA) have been proposed and recognized as two promising techniques for IoT networks [2]. The main idea of MEC is to exploit the surrounding available computing resources to facilitate the computation of mobile terminals, while NOMA is to allow multiple mobile terminals communicate through the same time/frequency resource block in the power domain. The essential feature of NOMA is that it requires superposition coding at the transmitting end and successive interference cancellation at the receiving end [3]. In regard to MEC, generally, it has two kinds of computation offloading modes, namely, partial offloading [4] and binary offloading [5]. Recently, many research work pays attention to the collaboration of NOMA and MEC techniques. The authors in [2] revealed that introducing NOMA into MEC networks can dramatically reduce latency and energy consumption. In the NOMA-based MEC networks, literature [6] further investigated energy consumption minimization problem, and the weighted sum energy consumption was minimized under multi-antenna configuration and both computation offloading modes.

Although MEC technique has the advantages in security, the computation task offloading can still be susceptible to be eavesdropped since the offloading wireless channel has open nature. For the purpose of improving security, physical layer security, as an alternative solution for encryption, has been considered a promising paradigm. In [7], the authors considered the secure transmission design by exploiting the secrecy channel encoding and the signaling under the practical assumption that the eavesdropper's channel state information (CSI) is unknown. Literature [8] was the first work introducing physical layer security into the task offloading secrecy issue, in which a latency-constrained weighted sum-energy minimization problem was studied. In [9], the authors first studied the secure offloading issue in an uplink NOMA-assisted MEC system with a malicious eavesdropper, the secrecy outage probability was used to evaluate the security of uplink offloading under the practical passive eavesdropping scenario with the known probability density function of the eavesdropping channel. However, the more practical secure offloading issues without knowing the eavesdropper's CSI in MEC networks have not yet been studied, which is the motivation of our work.

To the best of authors' knowledge, this is the first work that studies resource allocation problem for maximizing the minimum anti-eavesdropping ability in an uplink NOMA-enabled MEC network in the presence of an external malicious eavesdropper. Under the practical consideration that the eavesdropper's CSI is not known, we propose an efficient iterative algorithm and obtain the closed-form expressions at each iteration.

II. System Model and Problem Formulation

We consider a MEC network with one AP, two uplink users and a malicious eavesdropper. The AP is equipped with MEC server. Each node is configured with a single antenna.

W. Wu, X. Wang and B. Wang are with the College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China. (e-mail: weiwu@njupt.edu.cn, 1017010512@njupt.edu.cn, bywang@njupt.edu.cn)

F. Zhou is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, 211101, China. (e-mail: zhoufuhui@ieee.org)

K. K. Wong is with the Department of Electronic and Electrical Engineering, University College London, United Kingdom, WC1E 6BT. (email: kai-kit.wong@ucl.ac.uk)

C. Li is with the National Mobile Communications Research Laboratory, School of Information Science and Engineering, Southeast University, Nanjing 210096, China. (e-mail: chunguoli@seu.edu.cn)

This work was supported by the National Natural Science Foundation of China (61901231). (Corresponding author: Fuhui Zhou.)

Similar to [5]-[9], we adopt the frequency non-selective quasi-static block fading model, where the wireless channels remain unchanged during the focused finite transmission time period T. Each user has a computation task with $L_{\rm k} > 0$ input bits that need to be calculated within T time block. By exploiting the NOMA technique, both users are able to offload tasks simultaneously over the same time and frequency resource. Viewing the input task bit as an independent sub-task, we introduce the data partition task model to partial offloading. In this case, the kth user ($k \in \{1, 2\}$) can divide the tasks into two parts with ℓ_k bits executed locally and $(L_k - \ell_k)$ bits executed at the edge server.

Then, the signals received at the AP and the eavesdropper can be respectively expressed as $y_{AP} = \sum\limits_{k=1,2} \sqrt{p_k} h_{AP,k} s_k + n_{AP}$ and $y_e = \sum\limits_{k=1,2} \sqrt{p_k} h_{e,k} s_k + n_e$, where $h_{AP,k}$ is the channel coefficient between user k and the AP, $h_{e,k}$ is the channel coefficient between user k and the eavesdropper, $s_k \in \mathbb{C}$ is the task-bearing signal for offloading by user k with statistical expectation $\mathrm{E}\left[|s_k|^2\right]=1$, and $p_k > 0$ is the transmission power of user k, n_{AP} is the additive white Gaussian noise (AWGN) at the AP with zero mean and variance σ_{AP}^2, while n_e is the AWGN at the eavesdropper with zero mean and variance σ_e^2.

Without loss of generality, we assume that the channel gains of two users is ordered as $|h_{AP,1}|^2 < |h_{AP,2}|^2$. Then, similar to [2], [9], the AP performs successive interference cancellation to decode the received signal y_{AP}, and the receiving SINRs for s_1 and s_2 can be respectively given as $\Gamma_{AP,1} = \gamma_{AP,1} p_1$ and $\Gamma_{AP,2} = \frac{\gamma_{AP,2} p_2}{1+\gamma_{AP,1} p_1}$, where $\gamma_{AP,1} = |h_{AP,1}|^2 \big/ \sigma_{AP}^2$ and $\gamma_{AP,2} = |h_{AP,2}|^2 \big/ \sigma_{AP}^2$.

The lower bound of the achievable secure offloading rate is obtained under the assumption that the eavesdropper is able remove the uplink interference before decoding the message of interest [9]. Therefore, the receiving SINR at the eavesdropper of message s_k can be written as $\Gamma_{e,k} = \gamma_{e,k} p_k,\ k \in \{1, 2\}$, where $\gamma_{e,k} = |h_{e,k}|^2 \big/ \sigma_e^2$.

By adopting the Wyner's secrecy encoding scheme [11], for message s_k, its rate of the entire codeword $R_{t,k}$ includes two parts, the redundant information rate $R_{e,k}$ and the confidential information rate $R_{s,k}$, i.e., $R_{t,k} = R_{s,k} + R_{e,k}, k \in \{1, 2\}$. Denote the channel capacities of the AP and eavesdropper as $C_{AP,k} = \log_2(1 + \Gamma_{AP,k})$ and $C_{e,k} = \log_2(1 + \Gamma_{e,k})$, respectively. Then, it has two cases in which the outage occurs. One is, if $\Gamma_{AP,k}$ is less than $\beta_{t,k} = 2^{R_{t,k}} - 1$, then AP cannot recover the encoded information and a communication outage occurs. The other one is, if $\Gamma_{e,k}$ exceeds $\beta_{e,k} = 2^{R_{e,k}} - 1$, the confidential information may be wiretapped and a secrecy outage event happens. Similar to literatures [7] and [9], an adaptive secure transmission scheme is considered by fully exploiting the fading status of channel $h_{AP,k}$. In this case, user k can set the codeword rate $R_{t,k}$ to the channel capacity of legitimate channel $C_{AP,k}$, i.e., $\beta_{t,k} = \Gamma_{AP,k}, k \in \{1, 2\}$. It guarantees the reliable link from user k to AP and avoids the communication outage.

To avoid secrecy outage, the inequality $\beta_{e,k} > \Gamma_{e,k}$ must be hold. Then, the secrecy outage probability (SOP) [9] can be defined as $\mathrm{P}_{so,k} = \Pr\{\Gamma_{e,k} > \beta_{e,k}\} = \Pr\left\{\frac{p_k |h_{e,k}|^2}{\sigma_e^2} > \beta_{e,k}\right\}, k \in \{1, 2\}$, which is minimized in the following optimization problem. Since the wiretap channel $h_{e,k}$ is typically unknown to user k, we cannot access the exact SOP. However, by reformulating it as $\mathrm{P}_{so,k} = \Pr\left\{|h_{e,k}|^2 > \frac{\beta_{e,k}\sigma_e^2}{p_k}\right\}$, it can be find that the minimization of SOP is equivalent to the maximization of following metric

$$\Omega_k \triangleq \frac{\beta_{e,k}\sigma_e^2}{p_k}, k \in \{1, 2\}. \tag{1}$$

The Ω_k in (1) owns a specific physical significance. It quantizes user k's intrinsic ability in anti-eavesdropping, which is referred as the anti-eavesdropping ability (AEA). Under the metric of AEA, *we can explain the SOP as the probability that the power gain of the coded signal at the eavesdropper over the AEA. This relationship between SOP and AEA provides the reason why, for the sake of offloading security, we maximizing the AEA instead of the SOP when the eavesdropper's CSI is unknown.*

Since the secrecy encoding where $R_{e,k} = R_{t,k} - R_{s,k}$, we have $\beta_{e,k} = (\beta_{t,k} - \beta_{s,k})/(1 + \beta_{s,k})$. Thus, the AEA in (1) can be re-expressed as $\Omega_k = \frac{(\beta_{t,k} - \beta_{s,k})\sigma_e^2}{(1+\beta_{s,k})p_k}, k \in \{1, 2\}$.

To proceed, our aim is to maximize the minimum AEA of the uplink NOMA users under the constraints of the computation task execution offloading security and the transmission power budgets. Mathematically, the optimization problem is formulated as

$$\max_{\boldsymbol{\ell}, \mathbf{p}, \boldsymbol{\beta_s}} \min \left\{ \frac{(\beta_{t,1} - \beta_{s,1})\,\sigma_e^2}{(1 + \beta_{s,1})\,p_1}, \frac{(\beta_{t,2} - \beta_{s,2})\,\sigma_e^2}{(1 + \beta_{s,2})\,p_2} \right\} \tag{2a}$$

$$s.t. \quad 2^{\frac{L_k - \ell_k}{T}} - 1 \le \beta_{s,k} \le \beta_{t,k}, k \in \{1, 2\}, \tag{2b}$$

$$0 \le p_k \le p_k^{\max}, k \in \{1, 2\}, \tag{2c}$$

$$0 \le \ell_k \le \ell_k^{\max}, k \in \{1, 2\}, \tag{2d}$$

$$p_k T + \frac{\xi_k C_k^3 \ell_k^3}{T^2} \le E_k, k \in \{1, 2\}, \tag{2e}$$

where $\boldsymbol{\ell} = [\ell_1,\ \ell_2]$ is the task partition vector, $\mathbf{p} = [p_1,\ p_2]$ represents the power allocation vector, $\boldsymbol{\beta_s} = [\beta_{s,1}, \beta_{s,2}]$ is the confidential data vector. The constraints in (2b) ensure that the secrecy rate for each user k must be no smaller than the offloading rate, such that the task-input bits can be offloaded securely. In addition, the secrecy rate must also be no larger than the channel capacity of each user k. Constraints in (2e) denote that the energy consumed on local computing and edge offloading must be no more than the budget for each user k.

In the next section, we will propose an effective algorithm to tackle the difficult multi-variable coupled fractional programming fairness problem in (2).

III. Optimal Solution

A. Feasibility Analysis

There exists a minimum value of energy budget, that is once $E_k < E_k^{\min}$, then problem (2) will be unfeasible. At this time, the energy budget cannot support neither local computing nor

computation task offloading. The minimum value of energy budget can be gained from the following problem

$$\min_{\mathbf{p},\boldsymbol{\ell}} \quad p_k T + \frac{\xi_k C_k^3 \ell_k^3}{T^2}, \quad s.t. \ \ (2b)-(2d). \tag{3}$$

The optimal solution of problem (3) should satisfy $2^{\frac{L_k-\ell_k}{T}} - 1 = \beta_{t,k}, k \in \{1,2\}$. Thus, it has $p_k = (2^{\frac{L_k-\ell_k}{T}} - 1)\sigma_{AP}^2/|h_{AP,1}|^2$. By substituting p_k into (3), problem (3) is simplified to a convex optimization problem, which can be solved by CVX.

By checking the problem in (3) and setting $E_k \geq E_k^{\min}$, the feasibility of problem (2) can be guaranteed.

B. Optimal Solution

In this subsection, we lay emphasis on deriving the optimal solutions of the decision variables $\boldsymbol{\ell}$, $\mathbf{p}$ and $\boldsymbol{\beta_s}$. By substituting $\beta_{t,k} = \Gamma_{AP,k}$, $k \in \{1,2\}$ into problem (2), we have

$$\max_{\boldsymbol{\ell},\mathbf{p},\boldsymbol{\beta_s}} \min \left\{ \frac{\left(\gamma_{AP,1}p_1 - \beta_{s,1}\right)\sigma_e^2}{\left(1+\beta_{s,1}\right)p_1}, \frac{\left(\frac{\gamma_{AP,2}p_2}{1+\gamma_{AP,1}p_1} - \beta_{s,2}\right)\sigma_e^2}{\left(1+\beta_{s,2}\right)p_2} \right\} \tag{4a}$$

$$s.t. \ \ 2^{\frac{L_1-\ell_1}{T}} - 1 \leq \beta_{s,1} \leq \gamma_{AP,1}p_1, \tag{4b}$$

$$2^{\frac{L_2-\ell_2}{T}} - 1 \leq \beta_{s,2} \leq \frac{\gamma_{AP,2}p_2}{1+\gamma_{AP,1}p_1}, \tag{4c}$$

$$(2c)-(2e). \tag{4d}$$

Theorem 1: For a given transmission power $\mathbf{p}$, the optimal solutions of the decision variables $\boldsymbol{\ell}$ and $\boldsymbol{\beta_s}$ are respectively given by

$$\ell_k^* = \min\left\{ \ell_k^{\max}, \sqrt[3]{\frac{T^2(E_k - p_k T)}{\xi_k C_k^3}} \right\}, k \in \{1,2\}, \tag{5a}$$

$$\beta_{s,k}^* = 2^{\frac{L_k-\ell_k^*}{T}} - 1, k \in \{1,2\}. \tag{5b}$$

Proof: The objective value in (4a) increases as $\beta_{s,k}$ decreases. Then, from (4b) and (4c), we conclude that Ω_k can be maximized at $\beta_{s,k}^* = 2^{\frac{L_k-\ell_k}{T}} - 1$. Moreover, we note that $\beta_{s,k}^*$ decreases as ℓ_k increases. It implies that Ω_k increases with ℓ_k. Hence, to obtain the maximum objective value, from (2d) and (2e), the optimal ℓ_k can be obtained as $\ell_k^* = \min\left\{ \ell_k^{\max}, \sqrt[3]{\frac{T^2(E_k-p_kT)}{\xi_k C_k^3}} \right\}, k \in \{1,2\}$. Consequently, the optimal $\beta_{s,k}$ is $\beta_{s,k}^* = 2^{\frac{L_k-\ell_k}{T}} - 1, k \in \{1,2\}$. This complete the proof. ∎

Lemma 1: For the objective function in (4a), it has that $\Omega_1 = \Omega_2$ holds at the optimal solutions.

Proof: This lemma can be proved via contradiction. The monotonic relation between Ω_k and p_k can be exploited to verify the relationship between Ω_1 and Ω_2. Due to space limitation, the detailed proof is omitted here. ∎

From *Lemma 1*, we further obtain the function relationship of p_1 and p_2, which can be described as

$$p_2 = f(p_1) = \frac{p_1\beta_{s,2}}{\frac{p_1\gamma_{AP,2}}{(1+\gamma_{AP,1}p_1)} - \frac{(1+\beta_{s,2})}{(1+\beta_{s,1})}\left(\gamma_{AP,m}p_1 - \beta_{s,1}\right)}. \tag{6}$$

To proceed, the problem (4) is then simplified as

$$\max_{\mathbf{p}} \quad \Omega_1 \ or \ \Omega_2 \tag{7a}$$

$$s.t. \quad \frac{\beta_{s,1}}{\gamma_{AP,1}} \leq p_1 \leq A_1, \tag{7b}$$

$$\frac{\beta_{s,2}(1+\gamma_{AP,1}p_1)}{\gamma_{AP,2}} \leq f(p_1) \leq A_2, \tag{7c}$$

where $A_1 \triangleq \min\left\{ p_1^{\max}, \frac{E_1}{T} - \frac{\xi_1 C_1^3 \ell_1^3}{T^3} \right\}$ and $A_2 \triangleq \min\left\{ p_2^{\max}, \frac{E_2}{T} - \frac{\xi_2 C_2^3 \ell_2^3}{T^3} \right\}$.

Theorem 2: The optimal transmission power p_1 and p_2 of problem (7) are respectively given as

$$p_1^* = \min\{A_1, p_{14}\} \ \text{and} \ p_2^* = f(p_1^*), \tag{8}$$

where $p_{14} = \frac{-b_2+\sqrt{b_2^2-4a_2c_2}}{2a_2}$ with $a_2 = [\gamma_{AP,1}\beta_{s,2}(1+\beta_{s,1}) + A_2(1+\beta_{s,2})\gamma_{AP,1}^2]$, $b_2 = (1+\beta_{s,1})(\beta_{s,2} - A_2\gamma_{AP,2}) + A_2\gamma_{AP,1}(1+\beta_{s,2})(1-\beta_{s,1})$ and $c_2 = -A_2\beta_{s,1}(1+\beta_{s,2})$.

Proof: Firstly, $f(p_1) \geq \frac{\beta_{s,2}(1+\gamma_{AP,1}p_1)}{\gamma_{AP,2}}$ can be equivalently rewritten as

$$a_1 p_1^2 + b_1 p_1 + c_1 \geq 0, \tag{9}$$

where $a_1 = (1+\beta_{s,2})\gamma_{AP,1}^2$, $b_1 = \gamma_{AP,2}(\beta_{s,1} - \beta_{s,2}) + \gamma_{AP,1}(1-\beta_{s,1})(1+\beta_{s,2})$ and $c_1 = -\beta_{s,1}(1+\beta_{s,2})$. The range of variable p_1 for inequality (9) is $[-\infty, p_{11}] \cup [p_{12}, +\infty]$, where $p_{11} = \frac{-b_1-\sqrt{b_1^2-4a_1c_1}}{2a_1}$ and $p_{12} = \frac{-b_1+\sqrt{b_1^2-4a_1c_1}}{2a_1}$. It is easy to verify that $a_1 > 0$ and $c_1 < 0$, hence, $p_{11} < 0$ holds.

Secondly, $f(p_1) \leq A_2$ can be re-expressed as

$$a_2 p_1^2 + b_2 p_1 + c_2 \leq 0. \tag{10}$$

The range of variable p_1 for inequality (10) can be expressed as $[p_{13}, p_{14}]$, where $p_{13} = \frac{-b_2-\sqrt{b_2^2-4a_2c_2}}{2a_2}$. Note that it has $a_2 > 0$ and $c_2 < 0$ hold. Thus, we have $p_{13} < 0$.

By exploiting the inequalities (9), (10) and constraint (7b), $p_{12} \leq \min\{A_1, p_{14}\}$ is obtained consequently. Since the objective value of (7a) increases with p_1, we further have $p_1^* = \min\{A_1, p_{14}\}$. Then, by substituting p_1^* into (6), the optimal p_2 can be obtained and given as $p_2^* = f(p_1^*)$. ∎

Remark 1: From the obtained solutions, some useful insights on secure offloading design can be provided for practical uplink NOMA-enabled MEC network.

1) For the sake of anti-eavesdropping, Theorem 1 indicates that both users tend to perform task computation locally. However, due to the limitation of energy budget, they have to offload part of the task to the AP. To strike the balance between two users, Theorem 2 shows that user 1 should select its transmission power carefully among the maximum permissible power, the total energy budget and the interference with user 2. Then the transmission power of user 2 determined based on that of user 1.

2) From the AEAs in (4a), we observe that the AEA of each user increases as $\beta_{s,k}$ decreases. This means that the demand of low transmission latency and high offloading security cannot be satisfied simultaneously with given transmission power. In other words, the strengthening of offloading security is at the cost of increasing the transmission latency, since more redundant information is needed to resist eavesdropping.

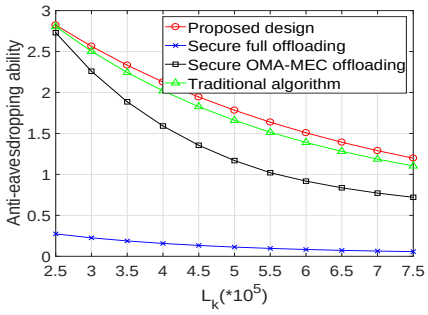

Fig. 1. The AEA versus the number of computation input bits L_k.

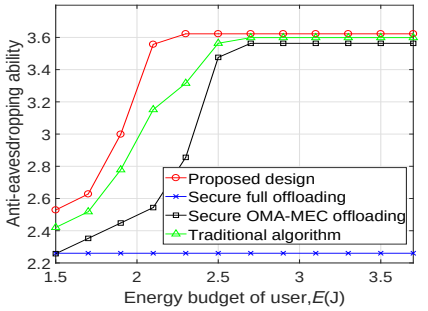

Fig. 2. The AEA versus the energy budget E of each user.

IV. Numerical Results

In this section, we evaluate the performance of our proposed resource allocation scheme through simulation. The simulation parameters are set as follows. The communication bandwidth per link is 1MHz, the transmission power budget is $p_1^{\max} = p_2^{\max} = 4.7$ dBw, the energy budget is $E_1 = E_2 = E = 1.5$ Joule, the time duration is $T = 0.1$ sec, the noise variance is $\sigma_{AP}^2 = \sigma_e^2 = -70$ dBm, the CPU cycle is $C_1 = C_2 = 10^3$ cycles/bit, the effective capacitance coefficient is $\xi_1 = \xi_2 = 10^{-28}$, the maximum number of locally computed bits $\ell_k^{\max} = 9 \times 10^5$ bits, $\forall k \in \{1, 2\}$.

The AEA versus the number of computation input bits L_k is shown in Fig. 1. The 'Secure full offloading' is the scheme that both users choose to offload all the task input bits to the AP for computing, the 'Secure OMA-MEC offloading' is the scheme that both users employ the TDMA protocol for partial offloading, the total time T is divided equally between two users, the 'Traditional algorithm' denotes the algorithm combining Dinkelbach method [5] with the iteration method to solve problem in (2). From Fig. 1, we note that the AEA decreases as the computation input bits L_k increases. This is owing to the fact that a larger L_k leads to a larger $\beta_{s,k}$ accordingly decreasing the AEA. In addition, comparison results show that partial offloading is better than full offloading in terms of secure offloading with limited energy budget, it tells us how to allocate task input bits to achieve the best security. Compared with OMA-MEC scheme, NOMA achieves the higher AEA at a cost of added computing complexity at the AP for successive interference cancellation. Our proposed design achieves nearly the same AEA performance as the traditional algorithm. However, it is obvious that the algorithm complexity of the proposed design is much lower than the traditional algorithm, since the proposed design obtained closed-form solutions and omitted the Dinkelbach based parameter search process.

In Fig. 2, we evaluate the AEA versus the energy budget E of each user with $L_k = 10^6$ bits. The AEA of proposed design increases with the energy budget. When the user's energy budget is large enough, it can insert enough redundant information into confidential information to fight eavesdropping. Hence, the transmission power p_k increases synchronously with β_k under given maximum offloading data bits. In this case, the AEA is close to saturation gradually. Simulation results show that the proposed design has a better performance than the existing schemes.

V. Conclusions

In this paper, we investigated the max-min AEA problem for an uplink NOMA-enabled MEC networks in the presence of an eavesdropper. The closed-form solutions for all the decision variables were derived and the corresponding design insights were given. Simulation results demonstrated that the proposed algorithm has a better AEA performance than the existing schemes. It is worth mentioning that the similar analysis skill behind the proposed design can be used to deal with other fractional programming problems with max-min fairness. For future work, it will be interesting to extend this work for UAV-enabled uplink NOMA MEC systems, optimizing the AEA in the presence of malicious eavesdropping.

References

[1] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy and Y. Zhang, "Mobile Edge Cloud System: Architectures, Challenges, and Approaches," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2495-2508, Sept. 2018.

[2] Z. Ding, P. Fan, and H. V. Poor, "Impact of non-orthogonal multiple access on the offloading of mobile edge computing," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 375-390, Jan. 2019.

[3] F. Zhou, Y. Wu, Y. Liang, Z. Li, Y. Wang, and K.-K. Wong, "State of the Art, Taxonomy, and Open Issues on NOMA in Cognitive Radio Networks," *IEEE Wirel. Commun.*, vol. 25, no. 2, pp. 100-108, 2018.

[4] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: the communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322-2358, Fourthquarter 2017.

[5] F. Zhou, Y. Wu, R. Q. Hu and Y. Qian, "Computation rate maximization in UAV-enabled wireless-powered mobile-edge computing systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1927-1941, Sep. 2018.

[6] F. Wang, J. Xu, and Z. Ding, "Multi-antenna NOMA for computation offloading in multiuser mobile edge computing systems," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2450-2463, Mar. 2019.

[7] T. Zheng, H. Wang, and H. Deng, "Improving anti-eavesdropping ability without eavesdropper's CSI: a practical secure transmission design perspective," *IEEE Commun. Lett.*, vol. 7. no. 6, pp. 946-949, Dec. 2018.

[8] J. Xu, and J. Yao, "Exploiting physical-layer security for multiuser multicarrier computation offloading," *IEEE Commun. Lett.*, vol. 8. no. 1, pp. 9-12, Feb. 2019.

[9] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-Efficient Resource Allocation for Secure NOMA-Enabled Mobile Edge Computing Networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 493-505, Jan. 2020.

[10] R. Chai, J. Lin, M. Chen and Q. Chen, "Task Execution Cost Minimization-Based Joint Computation Offloading and Resource Allocation for Cellular D2D MEC Systems," *IEEE Syst. J.*, vol. 13, no. 4, pp. 4110-4121, Dec. 2019.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.