Energy-Efficient Secure Offloading for NOMA-Enabled Machine-type Mobile-Edge Computing

Yuan Zhou
Electrical and Computer Engineering Department
Utah State University
Logan, UT, USA 84322
yuan.zhou@ieee.org

Haijian Sun
School of Electrical and Computer Engineering
University of Georgia
Athens, GA
hsun@uga.edu

Xiang Ma
Electrical and Computer Engineering Department
Utah State University
Logan, UT, USA 84322
xiang.ma@ieee.org

Rose Qingyang Hu
Electrical and Computer Engineering Department
Utah State University
Logan, UT, USA 84322
rose.hu@usu.edu

2023 IEEE International Conference on Industrial Technology (ICIT) | 979-8-3503-3650-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIT58465.2023.10143151

***Abstract*—Mobile edge computing (MEC) has emerged as a crucial paradigm for enhancing the capabilities in machine-type communication, which relies on sufficient spectrum resources to efficiently process the offloading tasks. However, the rise in the number of IoT devices and the expansion of machine-type communication traffic can cause spectrum shortages. Non-orthogonal multiple access (NOMA) allows multiple users to share the same bandwidth simultaneously, which can be applied to improve spectrum efficiency. Furthermore, the growing connectivity of devices and transmission of sensitive data in IoT networks give rise to significant concerns regarding both security threats and energy efficiency. In this paper, a NOMA-enabled MEC system is studied. In the presence of an eavesdropper, the secrecy rate is further adopted to measure the security performance of offloading. We aim to maximize secrecy computation efficiency in a NOMA-enabled MEC system. The simulation results demonstrate the improvement of secrecy computation efficiency by applying NOMA in mobile edge computing systems.**

I. Introduction

With the rise in the number of IoT devices and the expansion of machine-type communication traffic within the Internet of Things (IoT), supporting newly developed applications requires a high volume of network connections and low-latency transmission. To meet these requirements, two promising techniques have emerged: mobile edge computing (MEC) and non-orthogonal multiple access (NOMA). MEC involves moving the server closer to the source data from the cloud to the edge, which reduces transmission time from IoT devices to traditional cloud data centers. NOMA, unlike orthogonal multiple access (OMA) methods such as time-division multiple access (TDMA) or frequency-division multiple access (FDMA), allows multiple mobile devices to transmit signals simultaneously in the same channel. This increases spectrum efficiency and the number of network connections.

Advancements in the computation capacity of IoT devices have made it possible to perform computations either fully or partially on these devices. In cases where an IoT device has a large amount of data to process within a limited time frame, it can offload a portion/all of the data to the MEC server and compute the remainder locally. In general, the offloading task can be divided into two categories. One is binary offloading, which makes the user offload all data to the MEC server or compute everything locally. Another is partial offloading which dynamically partitions the data into two parts, with one offloading to the MEC server and the other processing locally. Here we consider partial offloading.

NOMA employs superposition coding at the transmitter and successive interference cancellation (SIC) at the receiver, which enables user multiplexing in the power domain [1]. Multiple users can transmit signals simultaneously without the need to wait for scheduled time slots as in TDMA, making low-latency transmission possible. The combination of MEC and NOMA has been extensively researched, including resource allocation in the NOMA-MEC system to minimize system energy consumption [2]-[3], with joint optimization of time and power. Another study [4] aimed to minimize offloading delay in NOMA-MEC networks, formulated as a minimax problem that aimed to minimize the maximum task completion time for different users.

While the MEC technique can protect against attacks from the backbone network, it remains vulnerable to privacy disclosure threats from eavesdroppers, particularly in wireless networks. A previous study in [5] considered physical layer security using secrecy encoding, but only focused on minimizing system energy consumption. Another study in [6] proposed using the cooperative interference between NOMA user pairs to enhance offloading security. This study uses secrecy outage

probability and secrecy computation probability as metrics to measure the security of user offloading tasks and overall computing tasks.

This study focuses on a secrecy computation efficiency offloading problem in the MEC system, where NOMA is employed for uplink transmission with enhanced security. The transmission rate is constrained by the secrecy rate when an eavesdropper is present. The main metric used in this study is computation efficiency, as opposed to energy consumption. Computation efficiency is defined as the ratio of total computation bits to total energy consumption, which strikes a balance between maximizing computation bits and minimizing energy consumption. To solve the non-convex problem, an iterative algorithm is proposed.

The paper is organized as follows. The system model is presented in Section II. In section III, a secrecy computation efficiency maximization problem is formulated. Then, our proposed method is presented. Section IV presents the simulation results. Finally, the paper is concluded in Section V.

II. System Model

As the model illustrated in Fig. 1, a typical MEC system with one server and K user equipments (UEs) with a single antenna is considered. UEs transmit their signal via power domain multiplexing, where the interference caused by non-orthogonal signals is addressed by SIC. A wireless access point (AP) has a single antenna to serve other devices. The system also includes a malicious eavesdropper (Eve), which is also a single antenna node. Due to limited local computation resources and power constraints, each user performs partial offloading to process computationally heavy tasks within a required time duration.

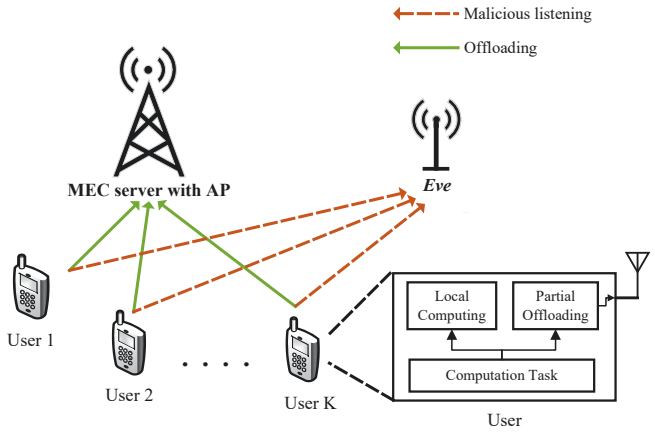

Fig. 1: System model

A. Secure Offloading

An active eavesdropper is considered in this work. It is assumed that the channels between UEs and Eve can be perfectly estimated by other users. Perfect channel state information (CSI) for the channels between UEs and the AP is also assumed available.

The channel coefficients between the AP and the kth UE and that between the Eve and the kth UE are denoted as h_k and g_k, respectively. It is assumed that the channel follows the block fading model, where the channel coefficients are assumed to be constants within a block time and be independent from one block to another. The received channel at the AP and Eve can be written as

$$y_k = h_k^H s_k + \sum_{j=1,(j\neq k)}^{K} h_j^H s_j + n_k, \forall k = 1, \ldots, K, \quad (1)$$

$$y_e^k = g_k^H s_k + \sum_{j=1,(j\neq k)}^{K} g_j^H s_j + n_e^k, \forall k = 1, \ldots, K. \quad (2)$$

Where $s_k \in \mathbb{C}$ is the transmit signal of the kth UE. In both equations, the first term at the right-hand side is the signal from the kth UE, and the second term is the interference from other UEs. The additive white Gaussian noise at the AP side and Eve side are denoted as $n_k \in \mathcal{CN}(0, \sigma_k^2)$ and $n_k \in \mathcal{CN}(0, \sigma_{ek}^2)$, respectively.

The secrecy rate, which is defined as the difference between transmission rates from UEs to the AP and that from UEs to the Eve, can be employed to enhance the security in the presence of Eve, given as,

$$R_{k,a}^{\text{sec}} = \big[\log(1 + \frac{p_k h_k^2}{\sum_{j=k+1}^{K} p_j h_j^2 + \sigma_k^2}) - \log\big(1 + \frac{p_k g_k^2}{\sum_{j=k+1}^{K} p_j g_j^2 + \sigma_{ek}^2}\big)\big]^+, \quad (3)$$

where $[a]^+ = \max(a, 0)$. A potential assumption is that the users are sorted according to their channel gains (i.e., $h_1^2 \geq h_2^2 \geq \cdots \geq h_K^2$, $g_1^2 \geq g_2^2 \geq \cdots \geq g_K^2$). It is also assumed that both the Eve and the AP apply SIC to decode received signals, which is a general assumption made in related works [9]. It is worth noting that the interference in the second term of the right-hand side in (3) can be utilized to enhance security. Owing to signals passing through the different channels before arriving at the AP and Eve, a trade-off can be exploited to reduce the SINR at the Eve side while maintaining an acceptable SINR at the AP side.

B. Local Computing

The limited computational capability of mobile devices makes it challenging to execute resource-intensive tasks locally. Therefore, task partitioning allows the mobile device to execute the part of the task that it can handle locally while offloading the computationally intensive part to the MEC server. As the local computing model used in [7], the computation rate of local computing depends on two parts: The number of cycles to finish the computation of a single bit of data by the kth UE and the clock speed of the kth UE, which are denoted as C_k and f_k, respectively. The energy consumption for local computing can be modeled as $E_k^{\text{comp}} = \epsilon_k f_k^3 T$, where ϵ_k is the CPU energy coefficient [10], [11].

C. Mobile Edge Computing

UEs compute the local part of tasks within the whole time duration T. Meanwhile, all UEs transmit the offloading part of tasks to the MEC server simultaneously, which takes $t \leq T$ to complete. Then, the offloading part will be executed by the MEC server. Finally, after processing the offloading computation task, UEs download the results from the MEC server. The time spent on MEC computing and result downloading is negligible because of the powerful computation capacity of the MEC server and the small size of computation results. This assumption has been widely used [12]-[13]. Fixed circuit consumption and transmission consumption are considered for offloading, the total power consumption can be given as

$$E_k^{\text{off}} = p_k t + p_r t. \tag{4}$$

III. Computation Efficiency with Eavesdropper in MEC Systems

A NOMA-enabled green MEC system is considered, where the objective is to maximize the secrecy computation efficiency. The optimization problem can be formulated as follows.

$$\mathbf{P}_1 \max_{\substack{\{t\},\{f_k\},\\ \{m_k\},\{p_k\}}} \sum_k w_k \frac{BR_{k,a}^{\text{sec}} t + \frac{Tf_k}{C_k}}{\epsilon_k f_k^3 T + p_k t + p_r t} \tag{5a}$$

$$\text{s.t. } C1 \quad : \quad t \leq T, \tag{5b}$$

$$C2 \quad : \quad BR_{k,a}^{\text{sec}} t \geq m_k, \forall k, \tag{5c}$$

$$C3 \quad : \quad L_k - \frac{Tf_k^{\max}}{C_k} \leq m_k \leq L_k, \forall k, \tag{5d}$$

$$C4 \quad : \quad \epsilon_k f_k^3 T + p_k t + p_r t \leq E_k^{th}, \forall k, \tag{5e}$$

$$C5 \quad : \quad 0 \leq f_k \leq f_k^{\max}, t \geq 0, p_k \geq 0, \ \forall k. \tag{5f}$$

In problem $\mathbf{P}_1$, L_k denotes the total number of bits to be computed for the kth UE, m_k is the number of bits that the kth UE offloads to the MEC securely, p_k is the transmit power of the kth UE, f_k is the CPU frequency of UE k, E_k is the maximum allowed energy consumption for the kth UE, and B is the bandwidth. The weighted summation of each UE's secrecy computation efficiency is maximized by optimizing the transmit power, offloading time, and CPU frequency. $C1$ requires the offloading ends before time T. $C2$ and $C3$ are the constraints of the minimum transmission rate and the requirement for the local computation rate. $C4$ guarantees that the energy consumption is less than the maximum allowed energy consumption of each UE. The CPU frequency, transmit power, and transmit time should be non-negative, which are guaranteed by $C5$.

In problem $\mathbf{P}_1$, the objective function is non-convex. In addition, a non-convex constraint $C2$ with coupling variables makes the problem more challenging.

A. Solving the Formulated Problem

Let $\tilde{p}_k = p_k t$. Then, (5c) can be transformed into equation sets as follows.

$$N_{r,k} \geq \frac{1}{\sigma_k^2} \sum_{j=k+1}^{K} \tilde{p}_j h_j^2, \tag{7a}$$

$$\tau_k \geq \frac{1}{\sigma_{ek}^2} \sum_{j=k}^{K} \tilde{p}_j g_j^2, \tag{7b}$$

$$\begin{aligned} &t\log\big(1+\frac{N_k}{t}\big) - t\log\big(1+\frac{N_{r,k}}{t}\big) \\ &-t\log\big(1+\frac{\tau_k}{t}\big) + t\log\big(1+\frac{\tau_{r,k}}{t}\big) \geq \frac{m_k}{B}, \end{aligned} \tag{7c}$$

$$\tau_{r,k} \leq \frac{1}{\sigma_{ek}^2} \sum_{j=k+1}^{K} \tilde{p}_j g_j^2, \tag{7d}$$

$$N_k \leq \frac{1}{\sigma_{ek}^2} \sum_{j=k}^{K} \tilde{p}_j h_j^2 \tag{7e}$$

Due to the sum-of-ratios structure and coupling variables, $\mathbf{P}_1$ is non-convex. We first address non-convex terms by successive convex approximation. Considering the non-convex term $tR_{k,a}^{\text{sec}}$, which can be written as

$$\begin{aligned} tR_{k,a}^{\text{sec}} =& t\log\big(1+\frac{N_k}{t}\big) - t\log\big(1+\frac{N_{r,k}}{t}\big) \\ &- t\log\big(1+\frac{\tau_k}{t}\big) + t\log\big(1+\frac{\tau_{r,k}}{t}\big) \end{aligned} \tag{8}$$

Let $v_k^{(i)} = \log\big(1+N_k^{(i)}/t^{(i)}\big) - \frac{N_k^{(i)}}{N_k^{(i)}+t^{(i)}}$, $v_{r,k}^{(i)} = \log\big(1+N_{r,k}^{(i)}/t^{(i)}\big) - \frac{N_{r,k}^{(i)}}{N_{r,k}^{(i)}+t^{(i)}}$, $\theta_k^{(i)} = \log\big(1+\tau_k^{(i)}/t^{(i)}\big) - \frac{\tau_k^{(i)}}{\tau_k^{(i)}+t^{(i)}}$, and $\theta_{r,k}^{(i)} = \log\big(1+\tau_{r,k}^{(i)}/t^{(i)}\big) - \frac{\tau_{r,k}^{(i)}}{\tau_{r,k}^{(i)}+t^{(i)}}$. By applying first-order Taylor series expansion on $tR_{k,a}^{\text{sec}}$ at $(N_k, N_{r,k}, \tau_k, \tau_{r,k}) = (N_k^{(i)}, N_{r,k}^{(i)}, \tau_k^{(i)}, \tau_{r,k}^{(i)})$, the approximation can be given as

$$\begin{aligned} &(v_k^{(i)} - v_{r,k}^{(i)} - \theta_k^{(i)} + \theta_{r,k}^{(i)})(t - t_k^{(i)}) \\ &+\frac{t_k^{(i)}}{t_k^{(i)}+N_k^{(i)}}(N_k - N_k^{(i)}) - \frac{t_k^{(i)}}{t_k^{(i)}+N_{r,k}^{(i)}}(N_{r,k} - N_{r,k}^{(i)}) \\ &-\frac{t_k^{(i)}}{t_k^{(i)}+\tau_k^{(i)}}(\tau_k - \tau_k^{(i)}) + \frac{t_k^{(i)}}{t_k^{(i)}+\tau_{r,k}^{(i)}}(\tau_{r,k} - \tau_{r,k}^{(i)}) + \varphi_k^{(i)}, \end{aligned} \tag{9}$$

where $\varphi_k^{(i)} = t_k^{(i)}\log\big(1+N_k^{(i)}/t^{(i)}\big) - t_i^{(i)}\log\big(1+N_{r,k}^{(i)}/t^{(i)}\big) - t_i^{(i)}\log\big(1+\tau_k^{(i)}/t^{(i)}\big) + t_i^{(i)}\log\big(1+\tau_{r,k}^{(i)}/t^{(i)}\big)$. Once the convex relaxation at the previous feasible solution is obtained, the approximated convex problem can be solved to obtain a new feasible solution.

Having addressed non-convex terms and coupling variables, a Dinkelbach-like method can be applied to transform $\mathbf{P}_1$ to

$$\max_{\substack{\{t\},\{f_k\},\{m_k\},\\ \{\tilde{p}_k\},\{\tau_k\},\{N_k\}}} \sum_k \quad \lambda_k w_k B\Big\{(v_k^{(i)} - v_{r,k}^{(i)} - \theta_k^{(i)} + \theta_{r,k}^{(i)})(t - t_k^{(i)}) + \frac{t_k^{(i)}}{t_k^{(i)} + N_k^{(i)}}(N_k - N_k^{(i)}) - \frac{t_k^{(i)}}{t_k^{(i)} + N_{r,k}^{(i)}}(N_{r,k} - N_{r,k}^{(i)}) \tag{6a}$$

$$-\frac{t_k^{(i)}}{t_k^{(i)} + \tau_k^{(i)}}(\tau_k - \tau_k^{(i)}) + \frac{t_k^{(i)}}{t_k^{(i)} + \tau_{r,k}^{(i)}}(\tau_{r,k} - \tau_{r,k}^{(i)})\Big\} + \sum_k \frac{\lambda_k w_k T f_k}{C_k} - \sum_k \lambda_k \beta_k \big(\epsilon_k f_k^3 T + \tilde{p}_k + p_r t\big)$$

$$\text{s.t.} \quad B\Big\{(v_k^{(i)} - v_{r,k}^{(i)} - \theta_k^{(i)} + \theta_{r,k}^{(i)})(t - t_k^{(i)}) + \frac{t_k^{(i)}}{t_k^{(i)} + N_k^{(i)}}(N_k - N_k^{(i)}) - \frac{t_k^{(i)}}{t_k^{(i)} + N_{r,k}^{(i)}}(N_{r,k} - N_{r,k}^{(i)}) \tag{6b}$$

$$-\frac{t_k^{(i)}}{t_k^{(i)} + \tau_k^{(i)}}(\tau_k - \tau_k^{(i)}) + \frac{t_k^{(i)}}{t_k^{(i)} + \tau_{r,k}^{(i)}}(\tau_{r,k} - \tau_{r,k}^{(i)}) + \varphi_k^{(i)}\Big\} + \frac{T f_k}{C_k} \geq L_k,$$

$$(10c) - (10g). \tag{6c}$$

be a convex optimization problem [14]. We first transform $\mathbf{P}_1$ to be

$$\mathbf{P}_2 \max_{\substack{\{t\},\{f_k\},\{m_k\},\{\tilde{p}_k\},\\ \{\beta_k\},\{\tau_k\},\{N_k\}}} \sum_k w_k \beta_k \tag{10a}$$

$$\text{s.t.} \quad C1: R_k \geq \beta_k E_k, \forall k, \tag{10b}$$

$$C2 \quad : \quad t \leq T, \tag{10c}$$

$$C3 \quad : \quad L_k - \frac{T f_k^{\max}}{C_k} \leq m_k \leq L_k, \forall k, \tag{10d}$$

$$C4 \quad : \quad \epsilon_k f_k^3 T + \tilde{p}_k + p_r t \leq E_k^{th}, \forall k, \tag{10e}$$

$$C5 \quad : \quad 0 \leq f_k \leq f_k^{\max}, t \geq 0, \tilde{p}_k \geq 0 \ \forall k, \tag{10f}$$

$$C6 \quad : \quad (7a) - (7e). \tag{10g}$$

where β_k is an auxiliary variable, $R_k = B R_k^{\text{sec}} t + \frac{T f_k}{C_k}$, and $E_k = \epsilon_k f_k^3 T + \tilde{p}_k + p_r t$.

Algorithm 1 Secure Computation Efficiency Maximization Algorithm

1: **Initialization:** the algorithm accuracy indicator u_1 and u_2, set $i = 0$, give initial values for $v_k^{(i)}, \theta_k^{(i)}, t^{(i)}, N_k^{(i)}$, $\tau_k^{(i)}$, $\lambda_k^{(i)}$ and $\beta_k^{(i)}$.
2: **while** $||\mathbf{T}(\lambda_k, \beta_k)|| > u_1$ **do**
3: **while** $|\alpha_k(j+1) - \alpha_k(j)| > u_2$ **do**
4: Solve $\mathbf{P}_3$ by CVX, obtain the optimal values $\{t\}, \{f_k\}, \{m_k\}, \{\tilde{p}_k\}, \{\tau_k\}$, and $\{N_k\}$.
5: Let $j = j + 1$.
6: **end while**
7: Let $i = i + 1$, update auxiliary variables $\lambda_k(i+1)$ and $\beta_k(i+1)$ from (13) and (14).
8: **end while**
9: Output the optimal secrecy computation efficiency.

Lemma 3.1: Let $(\{t^*\}, \{f_k^*\}, \{m_k^*\}, \{\tilde{p}_k^*\}, \{\beta_k^*\}, \{\tau_k^*\}, \{N_k^*\})$ be the optimal solution of $\mathbf{P}_2$ for $\forall k$, there exist $\{\lambda_k^*\}$ such that $(\{t^*\}, \{f_k^*\}, \{m_k^*\}, \{\tilde{p}_k^*\}, \{\tau_k^*\}, \{N_k^*\})$ satisfies the Karush-Kuhn-Tucker (KKT) condition of the following problem for $\lambda_k = \lambda_k^*$ and $\beta_k = \beta_k^*$.

$$\mathbf{P}_3: \quad \max_{\{t\},\{f_k\},\{P_k\}} \sum_k \lambda_k (w_k R_k - \beta_k E_k) \tag{11a}$$

$$\text{s.t.} \quad (10c) - (10g). \tag{11b}$$

Furthermore, $(\{t^*\}, \{f_k^*\}, \{m_k^*\}, \{\tilde{p}_k^*\}, \{\tau_k^*\}, \{N_k^*\})$ satisfies the following equations for $\lambda_k = \lambda_k^\star$ and $\beta_k = \beta_k^\star$:

$$\lambda_k = \frac{w_k}{E_k}, \ \beta_k = \frac{w_k R_k}{E_k}, \forall k. \tag{12}$$

The proof of the lemma can be found in [14], which provides an iterative solution for $\mathbf{P}_3$. As the formulas shown at the top of this page, the convex optimization problem can be solved with given auxiliary variables (λ_k, β_k). Then, the auxiliary variables will be updated as follows.

$$\lambda_k(i+1) = (1 - \alpha(i))\lambda_k(i) + \frac{\alpha(i)}{E_k(\tilde{p}_k^*, t^*, f_k^*)}, \tag{13}$$

$$\beta_k(i+1) = (1 - \alpha(i))\beta_k(i) + \alpha(i)\frac{w_k R_k(\tilde{p}_k^*, t^*, f_k^*)}{E_k(\tilde{p}_k^*, t^*, f_k^*)}, \tag{14}$$

where $\alpha(i)$ is the largest α that satisfies $||\mathbf{T}(\lambda_k(i) + \alpha^l \mathbf{q}_{K+1:2K}^i, \beta_k(i) + \alpha^l \mathbf{q}_{1:K}^i)|| \leq (1 - z\alpha^l)||T(\lambda_k(i), \beta_k(i)||$, where $T_j(\beta_j) = \beta_j E_k - w_k R_k$ and $T_{j+K}(\lambda_j) = \lambda_j E_k - 1$, $j \in \{1, 2, \ldots, K\}$, and $\mathbf{q}$ is the Jacobian matrix of $\mathbf{T}$, $l \in \{1, 2, \ldots\}$, $\alpha_l \in (0, 1)$, and $z \in (0, 1)$. The optimal solution for λ_k and β_k can be obtained by solving $\mathbf{T}(\lambda_k, \beta_k) = [T_1, T_2, \ldots, T_{2K}] = \mathbf{0}$. The detail of the algorithm is presented in **Algorithm 1**.

IV. Simulation and results

In this section, we provide a convergence analysis of the algorithm and compare it with traditional OMA methods. Additionally, the effectiveness of the proposed scheme is evaluated by comparing it with offloading-only and local computing schemes. The settings are given as follows. The number of users are assumed to be $K = 2$, both of which have the same weight $w_1 = w_2 = 1$. The transmission bandwidth is $B = 200$ *KHz*. The operation rounds for CPU to complete one bit computation is taken to be $C_k = 1000$. The scaling factor

for energy consumption is set as $\epsilon_k = 1 \times 10^{-24}$. The maximum frequency for local CPU is assumed as $f_k^{\max} = 1 \times 10^9$ Hz. The energy constraint for each user is $E_k = 1$ Joule. It is assumed that the noise to signal ratio (SNR) at AP is $h_k^2/\sigma_k^2 = H_k h_0$, where $H_1 = 7$, $H_2 = 5$. The SNR at Eve side is $g_k^2/\sigma_k^2 = G_k h_0$.

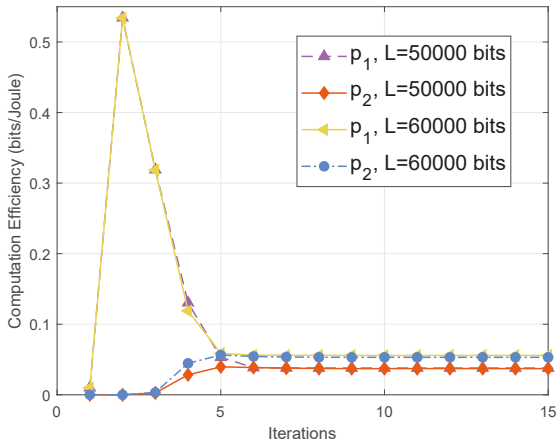

Fig. 2: Iterative Algorithm Convergence Analysis

Fig. 2 shows the convergence of the proposed iterative algorithm with different required computation bits, where $L_1 = L_2 = \{50000, 60000\}$, $G_1 = G_2 = 2$. It can be observed that p_1 and p_2 both increase with L_k. The reason for this is that users increase their transmit power to offload more computational bits to cope with the increasing size of the required computing data. In addition, the curves in both cases show good convergence. p_1 and p_2 take only 6 iterations to achieve convergence.

The computation efficiency versus required computation bits for different schemes are presented in Fig. 3, where $G_1 = G_2 = 1.5$. The curves for all schemes decrease as the required computation bits increase, suggesting that the increase of CPU frequency and transmit power will reduce the computation efficiency. Another observation is that the performance of the proposed scheme is close to that of local computing-only scheme when the required computing data size is small. The reason is that the local computing can achieve higher computation efficiency with the decrease of required computation bits. In contrast, offloading can achieve better performance when the number of required computation bits is great. It is worth noting that the proposed scheme outperforms other schemes for different required computation bit sizes.

Fig. 4 shows the comparison between the performance of the proposed NOMA-enabled MEC with that of the OMA-based MEC in [7]. The computation efficiency under different malicious listening channels are compared, where $G_1 = G_2 = \{3.0, 3.5\}$. The proposed NOMA-enabled system outperforms the OMA-based system in terms of computation efficiency. Because the users in NOMA-enabled scheme have higher bandwidth available to users in the NOMA-enabled scheme

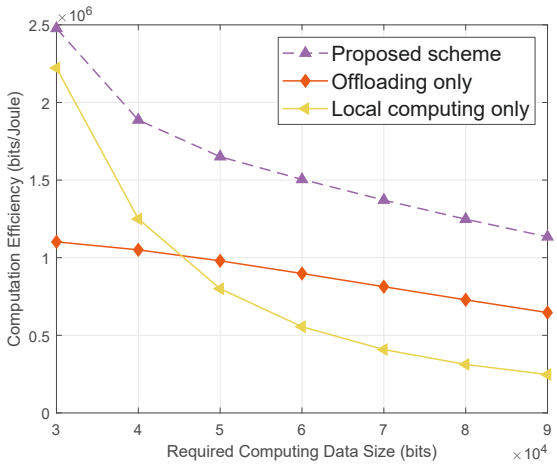

Fig. 3: Computation Efficiency v.s. Required Computation Bits under Different Computation Schemes

and the interference at the Eve side from user 2 when decoding the information from the first user. Furthermore, the gap between the two schemes increases as the required computation bits increase. The reason is that the computation efficiency are dominated by local computing when the required computation bits is small, where the communication scheme plays a minor role.

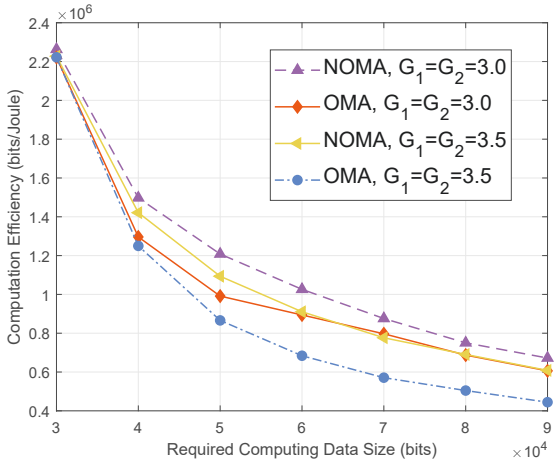

Fig. 4: Computation Efficiency v.s. Required Computation Bits under Different *Eve* Channels

V. Conclusions

In this paper, secrecy computation efficiency in a NOMA-enabled MEC system is maximized by jointly optimizing the transmit power, offloading time, and local computing frequency. A non-convex problem with a weighted sum-of-ratios structure is first formulated. By employing SCA and a Dinkelbach-like algorithm, the problem is transformed into a convex problem that can be effectively solved. The simulation results demonstrate the improvement of secrecy computation

efficiency by applying NOMA in mobile edge computing systems.

VI. Acknowledgement

This work was partially supported by the National Science Foundation under grants CNS-2007995 and ECCS-2139508.

References

[1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, K. Higuchi, "Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access," in *2013 IEEE VTC Spring*, Jun. 2013, pp. 1-5.

[2] Z. Ding, J. Xu, O. A. Dobre, H. V. Poor, "Joint Power and Time Allocation for NOMA–MEC Offloading," *IEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6207–6211, Mar. 2019.

[3] J. Zhu, J. Wang, Y. Huang, F. Fang, K. Navaie, Z. Ding, "Resource Allocation for Hybrid NOMA MEC Offloading," *IEEE Trans. Wireless Commun.*, vol. 19, no. 7, pp. 4964-4977, Apr. 2020.

[4] F. Fang, Y. Xu, Z. Ding, C. Shen, M. Peng, G. K. Karagiannidis, "Optimal Resource Allocation for Delay Minimization in NOMA-MEC Networks," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 6207-6211, Dec. 2020.

[5] W. Wu, F. Zhou, R. Q. Hu, B. Wang, "Energy-Efficient Resource Allocation for Secure NOMA-Enabled Mobile Edge Computing Networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 493-505, Oct. 2019.

[6] B. Li, W. Wu, W. Zhao, H. Zhang, "Security Enhancement With a Hybrid Cooperative NOMA Scheme for MEC System," *IEEE Trans. Veh. Technol.*, vol. 70, no.3, pp. 2635-2648, Mar. 2021.

[7] H. Sun, Q. Wang, X. Ma, Y. Xu and R. Q. Hu, "Towards Green Mobile Edge Computing Offloading Systems with Security Enhancement," in *2020 Intermountain Engineering, Technology and Computing (IETC)*, 2020, pp. 1-6.

[8] M. R. Zamani, M. Eslami, M. Khorramizadeh, H. Zamani and Z. Ding, "Optimizing Weighted-Sum Energy Efficiency in Downlink and Uplink NOMA Systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11112-11127, Jul. 2020.

[9] Y. Zhang, H. -M. Wang, Q. Yang and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," in *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930-933, Mar. 2016.

[10] Q. Wu, W. Chen, D. W. Kwan Ng, J. Li and R. Schober, "User-centric energy efficiency maximization for wireless powered communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6898-6912, Oct. 2016.

[11] Y. Wang, M. Sheng, X. Wang, L. Wang and J. Li, "Mobile-edge computing: partial computation offloading using dynamic voltage scaling," *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4268-4282, Oct. 2016.

[12] L. Yang, H. Zhang, M. Li, J. Guo and H. Ji, "Mobile edge computing empowered energy efficient task offloading in 5G," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6398-6409, Jan. 2018.

[13] F. Zhou and R. Q. Hu, "Computation efficiency maximization in wireless-powered mobile edge computing networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3170-3184, Feb. 2020.

[14] Y. Jong, "An efficient global optimization algorithm for nonlinear sum-of-ratios problem," May. 2012. [Online]. Available: http://www.optimization-online.org/DBFILE/2012/08/3586.pdf