Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5230594, 11 pages
https://doi.org/10.1155/2022/5230594

WILEY | Hindawi

Research Article

Energy-Efficient Computational Offloading for Secure NOMA-Enabled Mobile Edge Computing Networks

Haiping Wang

School of Mechatronics and Mould Engineering, Taizhou Vocational College of Science and Technology, Zhejiang 318020, China

Correspondence should be addressed to Haiping Wang; 39552529@qq.com

Received 23 February 2022; Revised 27 March 2022; Accepted 7 April 2022; Published 27 April 2022

Academic Editor: Yan Huo

Computational offloading and nonorthogonal multiple access (NOMA) are two promising technologies for alleviating the problems of limited battery capacity, insufficient computational capability, and massive deployment of terminal equipment in the Internet of Things (IoT) era. However, offloading data may be threatened by malicious eavesdroppers, which leads to more energy consumptions to avoid being eavesdropped. In this work, we study the energy-efficient way of computational offloading under the condition of certain security requirement in a secure NOMA-enabled mobile-edge computing (MEC) networks, where K end users are intended to offload their data to the N-antenna access point (AP) through the same resource block under the threat of an eavesdropper. We first address energy-efficient local resource allocation by minimizing sum-energy consumption of end users, subject to CPU frequencies, offloading bits, secrecy offloading rate, and transmit power. We then optimize the local resources to obtain the minimum computation latency of task for each end user, with the constraint of certain energy budget. The solutions to the above two optimization problems are given and demonstrated numerically by a 3-user scenario.

1. Introduction

Research shows that the contradiction between the limited resources of mobile terminal equipment and its explosive development of business and application requirements has become the most challenging tasks in the field of mobile Internet and Internet of Things (IoT) [1]. The resources of the terminal equipment are mainly reflected in the computational capability of the processor and the battery capacity. According to the theory of integrated circuits, the power consumption of the CPU is proportional to the cube of its frequency [2]. The stronger computing power, the shorter battery life.

The newly developed mobile-edge computing (MEC) [3] technology helps to resolve the above contradiction. It allows terminal devices to migrate data to the MEC server for computing-computational offloading [4]. Although MEC effectively solves the contradictions faced by the terminal and improves the service experience, there are still problems of security and high energy consumption [5].

In recent years, most of the research on MEC computational offloading focuses on the optimization of energy consumption or/and time delay without considering the security threat. Some [6–9] investigated how to save energy, some [10–14] studied from the perspective of improving real-time performance, and [15] took into account both energy consumption and computation latency. Although many achievements have been received in the optimization of computational offloading performance under the condition of no security threat, in practical applications, data offloading often needs to consider information security issues. Whether it is IoT data, Internet of Vehicles (IoV) data, video streaming analysis data, or other data with high computational intensity [16], data leakage needs to be avoided. After security processing, such as encrypting and decrypting data in the terminal and MEC server, the computational offloading process inevitably increases energy consumption and computation latency, resulting in distortion of the existing performance optimization research results. To this end, security should be considered when studying the performance of computational offloading in practical applications.

The research on the security of the computational offloading process can mainly be divided into two categories:

one is based on the traditional cryptography; the other is based on the physical layer security. [17, 18] studied the energy efficiency of computational offloading based on cryptographic encryption, taking into account the delay and energy consumption caused by encryption, making energy efficiency evaluation closer to practical applications. [17] compared the energy consumption results of computational offloading with encryption and without encryption. As expected the energy consumption with encryption is greater than that without encryption. In turn, the authors further considered compressing the data to reduce the total amount of data, shorten the transmission delay and energy consumption, and achieve desired results.

Compared with traditional cryptography, computational offloading based on physical layer security is more attractive to researchers. The physical layer security is keyless, which avoids the network vulnerability problem caused by key distribution and management [19]; on the other hand, the physical layer security has been proved to be reliable from the perspective of information theory [20]. In addition, the physical layer security and traditional cryptography technology belong to different layers in the network system, and there is no replacement relationship between them, and the existing traditional security system can still be retained. Presently, the research combining physical layer security with MEC computational offloading energy efficiency is still in its infancy, and there are not many related studies. Most of them focus on secrecy offloading rate improvement and secrecy offloading resource allocation.

The most effective way to improve the energy efficiency of the terminal side is to increase the secrecy offloading rate without increasing the transmit power, shorten the data offloading time, and then reduce the offloading energy consumption of the terminal. Therefore, the related secrecy capacity enhancement techniques in the physical layer security can be applied, such as improving the main channel through relays; or deteriorating the eavesdropper's channel through artificial noise; or enhancing the main capacity through nonorthogonal multiple access technology. [21] studies the use of relay to improve the offloading rate. Since the relay is untrustworthy, the MEC server needs to interfere with it accordingly. [22] uses full-duplex artificial noise to deteriorate the eavesdropper's channel, that is, the MEC server sends out interference signals, which does not interfere with the legitimate receiver, but can influence the eavesdropper. Cooperative jamming assisted scheme via cooperative NOMA transmission was studied in [23]. A novel jamming signal scheme was designed to multiuser multiserver MEC-enabled IoT in [15, 24] adopts nonorthogonal multiple access technology to improve the terminal's antieavesdropping capability. [25–27] takes unmanned aerial vehicle (UAV) as the target of MEC data offloading and improves the secrecy capacity of end users by adjusting the position and power of UAV.

As for secure offloading resource allocation, there are two sides: terminal side and MEC side. The terminalside resources include CPU frequency, transmit power, transmission rate, and for the data "partial offloading" mode, also include the data partition ratio. MEC side resources include server CPU frequency, channel resources, and the like. [28] optimizes energy consumption by taking the proportion of data offloading and transmit power as resource allocation objects, that is, minimizing the energy consumption of the terminal by reasonably adjusting the data ratio of local computing and offloading computing and offloading power. The scenario is extended from single user to multiuser [29, 30], and the weighted total power is minimized by rationally distributing the data offloading ratio and transmit power of each user. Since the state-of-the-art CPU architecture used by most terminal devices adopts dynamic frequency and voltage scaling (DVFS) technique, the energy consumption can be controlled by flexibly adjusting the frequency or voltage of the CPU, so the local CPU frequency can be further included in the resource optimization object. [31–33] include channel resources (such as time slots and frequencies) into optimization objects while considering local resources. In addition, [34, 35] also studied dividing the data into several parts and offloading them to different MEC servers for computation.

In this work, we further investigate terminal-side resource allocation for multiterminal energy efficiency of a secure MEC system enabled with NOMA, which is of high spectral efficiency and can accommodate massive devices. Zero-forcing (ZF) combined with successive interference cancelation (ZF-SIC) is adopted on the side of AP. Different from MMSE, ZF is less complex and more energy-efficient. We consider "partial offloading" mode and take more practical secrecy performance metric of secrecy outage probability (SOP) during offloading. Although [30] has studied energy-efficient resource allocation in secure NOMA-enabled mobile MEC networks, the authors only addressed the scenario of two user NOMA and one single antenna at the AP associated with the MEC server for simplicity. In this paper, we generalize the model of secure NOMA-enabled MEC with multiple users and multiple antennas at AP and tackle the efficient problem of energy and latency via local resource allocation. The major challenges of this work are (1) modeling wiretap channel and partial offloading mode and giving the closed-form expressions; (2) formulating sum-energy consumption minimization problem and computation latency minimization problem; (3) transforming minimization problems with multiple variables into a single variable one and giving the optimal solutions.

We adopt SOP as the secure QoS metric rather than secrecy capacity or ergodic secrecy capacity based on the following considerations: (1) more favorable main channel than eavesdropper channel is not always available; (2) the eavesdropper is always passive, which implies the CSI of eavesdropper channel is not available; (3) ergodic secrecy capacity needs to encode over a long period of time over all channel realizations, which incurs long delay and is suitable only for delay-tolerant applications; (4) secrecy outage is suitable for encoding confidential message over a single coherence interval or channel block.

The main contributions of the paper are summarized as follows:

(1) We generalize the model of NOMA-enabled MEC networks against an external eavesdropper by K

users and N antennas at AP associated with MEC server. A novel design framework is introduced by adopting zero forcing plus successive interference cancelation at the AP, jointly optimizing the number of offloading bits, local CPU frequency, and transmit power, targeting at end users' energy and latency

(2) Aiming at energy-efficient design, we characterize the optimization problem of sum energy of end users under certain SOP and latency requirement in the secure NOMA-enabled MEC networks, subject to CPU frequency, offloading bits, secrecy offloading rate, and transmit power of each user. We transform the complex and nonconvex problem into a single-variable one and give solution by numerical-finding

(3) Aiming at latency-efficient design, we investigate the problem of minimizing the computation latency of each user's task under certain SOP and energy budget requirement, with the constraint of CPU frequency, offloading bits, secrecy offloading rate, and transmit power. Similarly, the algorithm of the solution is given by transforming the original complex problem into a single-variable one

The rest of the paper is organized as follows. In the following section, we model the multiuser secure NOMA-enabled mobile MEC system and derive the closed-form expression of the secrecy outage probability of an individual user. In the third section, the optimization problem of sum-energy consumption of end users under certain SOP and latency requirement is characterized, and the algorithm of the solution is given. The problem of minimizing the computation latency of each user's task under certain SOP and energy budget requirement is addressed and solved in the fourth section. Numerical results are presented in the section of "Numerical Results" to confirm the efficient design done in the previous sections. Finally, a conclusion is drawn in the last section.

2. System Model

As depicted in Figure 1, we consider a secure uplink NOMA-enabled MEC networks, where K single-antenna users are intended to offload their computation-intensive tasks to the N-antenna access point (AP) (with an MEC server integrated) by sharing the same radio resource (such as frequency and/or time) at the presence of an eavesdropper (Eve) which is equipped with a single antenna. Here, $N \geq K$ is assumed.

All the channels are experiencing quasistatic Rayleigh fading. To user $k(k \in \mathcal{K} \triangleq \{1, \cdots, K\})$, the symbols used hereinafter are listed in Table 1.

Therefore, the instantaneous composite signals received at the AP and Eve are given by

$$y_a = \sum_{k=1}^{K} \sqrt{p_k} h_{a,k} s_k + w_a, \tag{1}$$

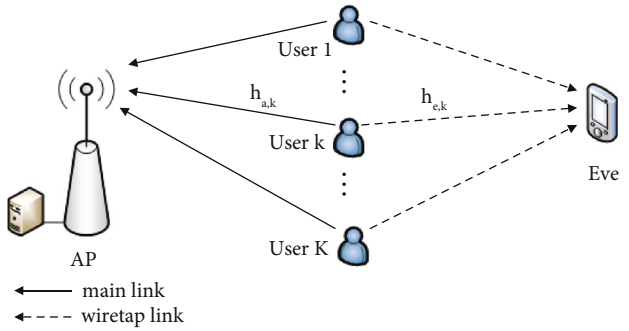

Figure 1: A model of secure uplink NOMA-enabled MEC networks with K users, one eavesdropper, and one N-antenna AP.

Table 1: Symbol description.

Symbol	Description
s_k	Complex information symbol from user k
p_k	Transmit power from user k
$h_{a,k}$	Channel gain vector from user k to AP
$h_{e,k}$	Channel gain from user k to Eve
w_a	Complex Gaussian noise vector at AP
w_e	Complex Gaussian noise at Eve
$d_{a,k}$	Distance from user k to AP
$d_{e,k}$	Distance from user k to Eve
α	Path-loss exponent
$g_{a,k}$	$g_{a,k} \sim \mathcal{CN}(0, I_N)$
$g_{e,k}$	$g_{e,k} \sim \mathcal{CN}(0, 1)$

$$y_e = \sum_{k=1}^{K} \sqrt{p_k} h_{e,k} s_k + w_e, \tag{2}$$

where $h_{a,k} = d_{a,k}^{-\alpha/2} g_{a,k}$ and $h_{e,k} = d_{e,k}^{-\alpha/2} g_{e,k}$; $\mathbb{E}[|s_k|^2] = 1$; $w_a \sim \mathcal{CN}(0, N_a I_N)$ and $w_e \sim \mathcal{CN}(0, N_e)$.

2.1. Wiretap Channel Model. Similar to [36], successive interference cancelation (SIC) combined with zero forcing (ZF) is employed at the AP, without loss of generality, to a specific user k, its aggregate signal left before decoding can be expressed as

$$y_{a,k}^{(\mathfrak{I})} = \sqrt{p_k} h_{a,k} s_k + \sum_{i \in \mathfrak{I}} \sqrt{p_i} h_{a,i} s_i + w_a, \tag{3}$$

where $\mathfrak{I} \subseteq \mathcal{K} \setminus \{k\}$, indicating U_k is decoded just before these users in set $\mathfrak{I}$ (index) during an SIC process.

After applying zero-forcing, the SINR of user k at the AP is given by

$$\gamma_k^{(\mathfrak{I})} = \frac{p_k \left\| Q_k^{(\mathfrak{I})} h_{a,k} \right\|^2}{N_a}, \tag{4}$$

where $Q_k^{(\mathfrak{I})}$ is a $N - |\mathfrak{I}|$ by N matrix whose rows are the orthonormal basis of the null space of the subspace spanned by the vector set $\{h_{a,i}|\forall i \in \mathfrak{I}\}$.

According to [37], $\gamma_k^{(\mathfrak{I})}$ obeys a chi-squared distribution with $2 \times (N - |\mathfrak{I}|)$ degrees of freedom and has nothing to do with the specific users in set $\mathfrak{I}$ but its cardinality $|\mathfrak{I}|$. Specifically, $\lambda_k \gamma_k^{(\mathfrak{I})} \sim \chi^2_{2(N-|\mathfrak{I}|)}$, where $\lambda_k = N_a d_{a,k}^{\alpha}/p_k$. For the ease of presentation, we denote the cardinality of $\mathfrak{I}$ by n and rewrite $\gamma_k^{(\mathfrak{I})}$ by $\gamma_k^{(n)}$, whose probability density function (pdf) is given by

$$f_{\gamma_k^{(n)}}(\gamma_k) = \frac{\lambda_k^{N-n}}{\Gamma(N-n)} \gamma_k^{N-n-1} e^{-\lambda_k \gamma_k}, \gamma_k \geq 0. \tag{5}$$

As for the SINR of user k (denoted as ξ_k) at eve, we adopt the conservative assumption that all user interference can be canceled out by Eve. Therefore, $\xi_k = |h_{e,k}|^2 p_k / N_e$ obeys an exponential distribution with parameter $\mu_k = N_e d_{e,k}^{\alpha}/p_k$, i.e., $\xi_k \sim \mathbf{Exp}(\mu_k)$, whose cumulative distribution function (CDF) is given by

$$F_{\xi_k}(\xi_k) = 1 - e^{-\mu_k \xi_k}, \xi_k > 0. \tag{6}$$

2.2. Partial Offloading Model. We assume the task for each user can be partitioned into two parts with an arbitrary ratio. Let L_k and l_k be the total number of bits to be processed and the number of bits to be offloaded to the AP.

We consider a more practical scenario that the eavesdropper is passive and the AP only has the statistical characteristics of eavesdropper's channels. To this end, we adopt the secrecy outage probability (SOP) for quantifying the quality-of-service (QoS) of secure transmissions.

Suppose $R_{s,k}$ is the secrecy rate for transmit power p_k that satisfies the targeted secure QoS for user k. Therefore, the energy consumption of offloading can be formulated as

$$E_k^{\text{off}} = p_k t_k^{\text{off}} = p_k \frac{l_k}{BR_{s,k}}, \tag{7}$$

where t_k^{off} and B refer to offloading duration and the bandwidth of the channel, respectively.

We present the closed-form expression of SOP in form of theorem as follows.

Theorem 1. *The secrecy outage probability of user k for the required secrecy rate $R_{s,k}$ at the presence of n-user interference can be expressed as*

$$\begin{aligned} P_{so,k}(n, R_{s,k}) = {} & \frac{\boldsymbol{\gamma}\left(N-n, \lambda_k\left(2^{R_{s,k}}-1\right)\right)}{\boldsymbol{\Gamma}(N-n)} \\ & + \left(\frac{\lambda_k}{\lambda_k + \mu_k 2^{-R_{s,k}}}\right)^{N-n} e^{\mu_k\left(1-2^{-R_{s,k}}\right)} \\ & \times \frac{\boldsymbol{\Gamma}\left(N-n, \left(\lambda_k + \mu_k 2^{-R_{s,k}}\right)\left(2^{R_{s,k}}-1\right)\right)}{\boldsymbol{\Gamma}(N-n)}, \end{aligned} \tag{8}$$

where

$$\boldsymbol{\gamma}(v, z) = \int_0^z u^{v-1} e^{-u} du, \tag{9}$$

and

$$\boldsymbol{\Gamma}(v, z) = \int_z^{\infty} u^{v-1} e^{-u} du = \boldsymbol{\Gamma}(v) - \boldsymbol{\gamma}(v, z), \tag{10}$$

are the incomplete Gamma function and its complement, respectively.

Proof. See Appendix. □

2.3. Local Computation Model. Let X_k be the computation intensity in CPU cycles per bit for user k. The total number of cycles for computing local part of task is $(L_k - l_k)X_k$. Each user adopts the advanced dynamic frequency and voltage scaling (DVFS) technique to control the energy consumption. According to [1], the energy consumption of a CPU cycle is given by $\kappa_k f_k^2$, where κ_k is a constant associated with the hardware architecture, and f_k is the CPU frequency for user k. For the local computation task of $(L_k - l_k)X_k$ cycles, the energy consumption can be derived:

$$E_k^{\text{loc}} = \kappa_k (L_k - l_k) X_k f_k^2. \tag{11}$$

The corresponding computation time for user k can be given by

$$t_k^{\text{loc}} = \frac{(L_k - l_k)X_k}{f_k}. \tag{12}$$

3. Sum-Energy Consumption Minimization

3.1. Problem Formulation. In this section, we focus on the problem of the sum-energy consumption minimization over transmit power p_k, offloading bits l_k, secrecy offloading rate $R_{s,k}$, and CPU frequency f_k, subject to the task $A_k(L_k, T, X_k)$ for each user.

By convention, we ignore the time of the data processing at the MEC as well as that of downlink transmission, due to the fact that the MEC processing speed is very fast and the processed result usually has fewer bits. Without loss of generality, the AP decodes the users' signals in the SIC order of user 1, user 2, ..., user K. As such, the number of user interferers for user k is $n = K - k$.

Mathematically, the minimization problem of sum-energy consumption can be formulated as

$$(P1): \ \min_{f,l,p,R_s} \sum_{k=1}^{K} \left(\kappa_k (L_k - l_k) X_k f_k^2 + p_k \frac{l_k}{BR_{s,k}}\right), \tag{13a}$$

$$\text{s.t.} \ \frac{(L_k - l_k)X_k}{f_k} \leq T, \forall k \in \mathcal{K}, \tag{13b}$$

$$\frac{l_k}{BR_{s,k}} \le T, \forall k \in \mathcal{K}, \tag{13c}$$

$$P_{so,k}(K-k, R_{s,k}) \le \epsilon, \forall k \in \mathcal{K}, \tag{13d}$$

$$0 \le l_k \le L_k, \forall k \in \mathcal{K}, \tag{13e}$$

$$f_k \le f_k^{\max} \forall k \in \mathcal{K}, \tag{13f}$$

where $f = [f_1, f_2, \cdots, f_K]$, $l = [l_1, l_2, \cdots, l_K]$, $p = [p_1, p_2, \cdots, p_K]$, and $R_s = [R_{s,1}, R_{s,2}, \cdots, R_{s,K}]$ refer to the CPU frequency vector, the offloading bit vector, the transmit power vector, and secrecy offloading rate vector, respectively; T is the computation latency, and $f_k^{\max}$ denotes the upper bound of CPU frequency for user k.

3.2. Solution to Problem (P1). The problem ($P1$) is complicated and nonconvex due to the nonconvex nature of constraints (13d). Although the closed-form expression of the optimal solution is not available, we can obtain a suboptimal solution numerically by (1) simplifying constraints, (2) relaxing and transforming the multivariable problem into a single variable problem, and (3) giving the solution numerically.

We first simplify the constraints by the following lemma.

Lemma 2. *The constraint (13b) and (13d) are strictly binding for the optimal solution of problem (P1), i.e.,*

$$f_k = \frac{(L_k - l_k)X_k}{T}, \forall k \in \mathcal{K}, \tag{14}$$

$$P_{so,k}(K-k, R_{s,k}) = \epsilon, \forall k \in \mathcal{K}. \tag{15}$$

Proof. Observing the first term in (13a), the local computation energy consumption is an increasing function of f_k. Obviously, the lowest CPU frequency that satisfies the condition achieves the minimum energy consumption.

According to the property of the SOP, $P_{so,k}(n, R_{s,k})$ is an increasing function of $R_{s,k}$. The maximum $R_{s,k}$ that satisfies (13d) is the ϵ-outage secrecy capacity $C_{s,k}^{(n)}(\epsilon)$ which makes $P_{so,k}(n, C_{s,k}^{(n)}(\epsilon)) = \epsilon$ hold. This completes the proof. □

The problem ($P1$) in (13a) is still complex and nonconvex. We continue to transform the problem by relaxing offloading duration with T, i.e.,

$$(P1.1): \ \min_{l,p,R_s} \sum_{k=1}^{K} \left(\frac{\kappa_k X_k^3 (L_k - l_k)^3}{T^2} + p_k T \right), \tag{16a}$$

$$\text{s.t.} R_{s,k} \ge \frac{l_k}{BT}, \forall k \in \mathcal{K}, \tag{16b}$$

$$P_{so,k}(K-k, R_{s,k}) = \epsilon, \forall k \in \mathcal{K}, \tag{16c}$$

$$\left[L_k - \frac{T f_k^{\max}}{X_k} \right]^+ \le l_k \le L_k, \forall k \in \mathcal{K}, \tag{16d}$$

where $[\cdot]^+ = \max(\cdot, 0)$.

Since the transmit power p_k increases with $R_{s,k}$, $R_{s,k} = l_k / BT$ achieves the minimum energy consumption for fixing other parameters. Moreover, p_k can be expressed as a function of $R_{s,k}$ from (16c). As such, we can further transform the problem into the one only having a single variable.

$$(P1.2): \ \min_l \sum_{k=1}^{K} \left(\frac{\kappa_k X_k^3 (L_k - l_k)^3}{T^2} + P_k\left(K-k, \frac{l_k}{BT}\right) T \right), \tag{17a}$$

$$\text{s.t.} \left[L_k - \frac{T f_k^{\max}}{X_k} \right]^+ \le l_k \le L_k, \forall k \in \mathcal{K}, \tag{17b}$$

where $P_k(n, R_{s,k})$ is the expression of the function for p_k derived from $P_{so,k}(n, R_{s,k}) = \epsilon$.

Although we cannot get a closed-form solution to this problem, the optimal solution can be found numerically. The numerical solution to problem $(P1.2)$ is shown in Algorithm 1. Obviously, the solution to problem $(P1.2)$ is equivalent to minimize the energy consumption of each user over offloading bit l_k independently. We will demonstrate it numerically in detail in Section.

3.3. Discussion

3.3.1. Local Computation Only Mode. The energy consumption of local computation only mode for user k is $\kappa_k X_k^3 L_k^3 / T^2$ by setting $l_k = 0$. However, the local computation only mode is not always available unless $f_k^{\max} \ge L_k X_k / T$ is satisfied.

3.3.2. Full Offloading Mode. Similarly, the full offloading mode is not always achievable as given the SOP requirement each user k has its asymptotic secrecy rate, which is explained by the following theorem.

Theorem 3. *Given the SOP of ϵ, the limited value of secrecy rate $R_{s,k}$ for user k at the presence of n-user interference is* $\log \mu_k / \lambda_k + 1/N - n \log \epsilon - \log(1 - \sqrt[N-n]{\epsilon})$.

Proof. $p_x \longrightarrow \infty$ makes μ_k and λ approach to 0 while their ratio keep as a limited value. Then, the asymptotic secrecy outage probability for (8) can be formulated as

$$P_{so,k}(n, R_{s,k}) \xrightarrow[p_x]{a.s.} \left(\frac{1}{1 + (\mu_k / \lambda_k) 2^{-R_{s,k}}} \right)^{N-n}. \tag{18}$$

In turn, the asymptotic -outage secrecy capacity is

$$C_{s,k}^{(n)}(\epsilon) \xrightarrow[p_x]{a.s.} \log \frac{\mu_k}{\lambda_k} + \frac{1}{N-n} \log \epsilon - \log\left(1 - \sqrt[N-n]{\epsilon}\right). \tag{19}$$

This completes the proof. □

1: **Setting**: T, B, ϵ, N, K, α, N_a, N_e;
2: **Repeat**
3: **Setting**: $f_k^{\max}$, κ_k, X_k, L_k, $d_{a,k}$, $d_{e,k}$;
4: **Initialization**: l_k;
5: **Repeat**
6: **Repeat**
7: Search p_k with certain l_k via constraint of (13d);
8: **Until** SOP converges to ϵ within a prescribed accuracy;
9: Calculate $E_k^{loc} + E_k^{off}$;
10: **Until** $l_k = L_k$
11: Search l_k^* to make $E_k^{loc} + E_k^{off}$ the least;
12: Calculate f_k^*, $R_{s,k}^*$, p_k^*;
13: **Output**: l_k^*, f_k^*, $R_{s,k}^*$, p_k^*;
14: **Until** $k = K$

Algorithm 1: Optimal solution to problem ($P1$).

If $N_a = N_e$, the asymptotic-outage secrecy capacity can be further expressed as

$$C_{s,k}^{(n)}(\epsilon) \xrightarrow[p_x]{a.s.} \alpha \log \frac{d_{e,k}}{d_{a,k}} + \frac{1}{N-n} \log \epsilon - \log\left(1 - \sqrt[N-n]{\epsilon}\right). \tag{20}$$

To achieve full offloading mode, the following inequality must be satisfied.

$$L_k < BT\left(\alpha \log \frac{d_{e,k}}{d_{a,k}} + \frac{1}{N-K+k} \log \frac{\epsilon}{1 - \sqrt[N-K+k]{\epsilon}}\right). \tag{21}$$

3.3.3. Computational Complexity. Observing Algorithm 1, there roughly exist five nesting steps in the process of numerical-finding: (1) calculate SOP with variable $R_{s,k}$ and find the ϵ-outage secrecy capacity; (2) calculate ϵ-outage secrecy capacity with variable transmit power and search optimal transmit power with certain l_k; (3) calculate total energy consumption and search for the optimal l_k to achieve minimum total energy consumption; (4) loop from user 1 to user K. Therefore, the computational complexity is $O(Km^3)$ (here, m refers to the computational complexity of SOP.).

4. Computation Latency Minimization

4.1. Problem Formulation. We continue to study the optimization problem of task computation latency over transmit power p_k, offloading bits l_k, secrecy offloading rate $R_{s,k}$, and CPU frequency f_k for user k with the constraint of certain energy budget in this section.

All the assumptions and notations are the same as in section. We form the problem as follows

$$(P2):\ \min_{f_k, l_k, R_{s,k}, p_k} \max\left(t_k^{\text{loc}}, t_k^{\text{off}}\right). \tag{22a}$$

$$\text{s.t.} \kappa_k (L_k - l_k) X_k f_k^2 + p_k \frac{l_k}{BR_{s,k}} \le E_k^{bu}, \tag{22b}$$

$$P_{so,k}(K-k, R_{s,k}) \le \epsilon, \tag{22c}$$

$$0 \le l_k \le L_k, \tag{22d}$$

$$f_k \le f_k^{\max}, \tag{22e}$$

where $t_k^{\text{loc}} = (L_k - l_k)X_k/f_k$ and $t_k^{\text{off}} = l_k/(BR_{s,k})$ according to the definitions in section, and E_k^{bu} refers to the energy budget of user k for its task.

4.2. Solution to Problem (P2). Before solving problem ($P2$) numerically, we need to simplify the problem via the following lemma.

Lemma 4. *The optimal solution of the variables f_k, l_k, $R_{s,k}$, and p_k should make $t_k^{loc} = t_k^{off}$.*

Proof. We prove this lemma via contradiction. Let f_k^*, l_k^*, $R_{s,k}^*$, and p_k^* be the jointly optimal values of f_k, l_k, $R_{s,k}$, and p_k. We assume $(L_k - l_k^*)X_k/f_k^* < l_k^*/(BR_{s,k}^*)$. One can find by keeping p_k and $R_{s,k}$ fixed, reducing l_k makes t_k^{off} and E_k^{off} decline. Although E_k^{loc} increases with l_k decreasing (f_k fixed), the increase in E_k^{loc} can be compensated by the decrease in E_k^{off}. Therefore, there exists another $\{f_k^*, l_k', R_{s,k}^*, p_k^*\}$, where $l_k' = l_k^* - \tau_k$ and τ_k is a small positive value, making $(L_k - l_k')X_k/f_k^* \le l_k'/(BR_{s,k}^*)$. Similarly, if $(L_k - l_k^*)X_k/f_k^* > l_k^*/(BR_{s,k}^*)$ is supposed, there exists another $\{f_k^*, l_k'', R_{s,k}^*, p_k^*\}$ that makes $(L_k - l_k'')X_k/f_k^* \ge l_k''/(BR_{s,k}^*)$ hold, where $l_k'' = l_k^* + \tau_k$.

We complete the proof. □

Combined with Lemma 2 and Lemma 4, we transform the problem ($P2$) into the following form.

$$(\text{P2.1}):\ \min_{l_k} T_k, \tag{23a}$$

$$\text{s.t.} \frac{\kappa_k X_k^3 (L_k - l_k)^3}{T_k^2} + P_k\left(K-k, \frac{l_k}{BT_k}\right) T_k \le E_k^{bu}, \tag{23b}$$

1: **Setting**: B, ϵ, N, K, α, N_a, N_e;
2: **Repeat**
3: **Setting**: $f_k^{\max}$, κ_k, X_k, L_k, $d_{a,k}$, $d_{e,k}$, E_k^{bu};
4: **Initialization**: l_k, T_k;
5: **Repeat**
6: **Repeat**
7: **Repeat**
8: Search p_k with certain l_k and T_k via constraint of (22c);
9: **Until** SOP converges to ϵ within a prescribed accuracy;
10: Calculate $E_k^{loc} + E_k^{off}$;
11: **Until** T_k satisfies the condition in (23b)
12: **Until** $l_k = L_k$
13: Search l_k^* to make T_k the least;
14: Calculate f_k^*, $R_{s,k}^*$, p_k^*;
15: **Output**: l_k^*, f_k^*, $R_{s,k}^*$, p_k^*;
16: **Until** $k = K$

Algorithm 2: Optimal solution to problem ($P2$).

$$\left[L_k - \frac{T_k f_k^{\max}}{X_k}\right]^+ \le l_k \le L_k, \tag{23c}$$

The problem is changed into the form with a single variable, and we can find the optimal solution numerically, the algorithm of which is shown in Algorithm 2.

Different from Algorithm 1, Algorithm 2 has one more nesting step in the process of numerical-finding: Search for the minimum T_k for the fixed l_k, which makes its computational complexity be $O(Km^4)$.

5. Numerical Results

In this section, numerical results are presented to further validate the previous research results of the energy-efficient computational offloading design in this secure uplink NOMA-enabled MEC networks.

To demonstrate the numerical results more clearly, we take a 3-user scenario for instance, the layout of which is shown in Figure 2. The distances (grid) between each user and the AP as well as eve are listed in Table 2. Each grid is supposed to be 20 meters, thus, the distance from user 1 to the AP is 80 meters and about 152.3 meters to eve.

We assume the number of antennas equipped at the AP is 10, i.e., $N = 10$, the path loss in dB is expressed as $PL = 10\alpha \lg(d) + 43.5$, where the path loss exponent α is set to 3.76 according to 3GPP urban path loss model. The bandwidth $B = 10$ MHz and the equal AWGN power of the AP and eve are supposed, i.e., $N_a = N_e = N_0 B$, where $N_0 = -160$ dBm/Hz is the AWGN power spectral density.

For simplicity, we assume each end user has the same performance and tasks to process. The total bits of task for each user is $L_1 = L_2 = L_3 = 3$ Mbits. The computation intensity is $X_1 = X_2 = X_3 = 50$ cycles/bit. The maximum CPU frequency is 2 GHz. The effective capacitance coefficient is set as $\kappa_1 = \kappa_2 = \kappa_3 = 10^{-28}$. Without loss of generality, the SIC order is from user 1 to user 2 to user 3.

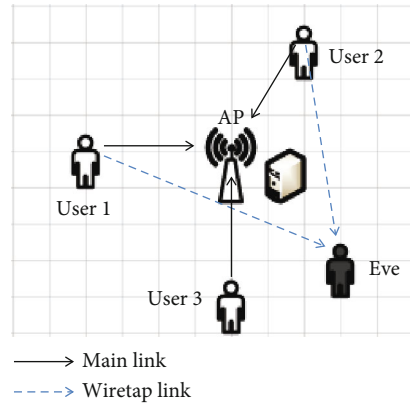

Figure 2: A 3-user scenario of secure uplink NOMA MEC system.

Table 2: Distances between each user and AP as well as eve.

Distance (grid)	User 1	User 2	User 3
AP	4	$\sqrt{13}$	4
Eve	$\sqrt{58}$	$\sqrt{37}$	$\sqrt{10}$.

5.1. Energy Consumption Minimization. Based on the above assumptions, the curves of the energy consumption versus offloading bits (Mbits) for each end user are shown in Figure 3, where the computation latency $T = 0.15$ s and the secrecy outage probability $\epsilon = 0.2$.

We note each curve starts from the same value (0.015 Joule) due to the similar parameter assumption for each user, goes down until the minimum energy consumption, then rises up, with the increase of offloading bits. $l_k = 0$ means local computation only mode, and $l_k = 3$ Mbits specifies full offloading mode. In this case, both modes cannot obtain the minimum energy consumption. The minimum energy consumptions for user 1, user 2, and user 3 are 0.0096 Joule, 0.0071 Joule, and 0.012 Joule, respectively. The corresponding offloading bits are $l_1 = 1$ Mbits, $l_2 = 1.3$

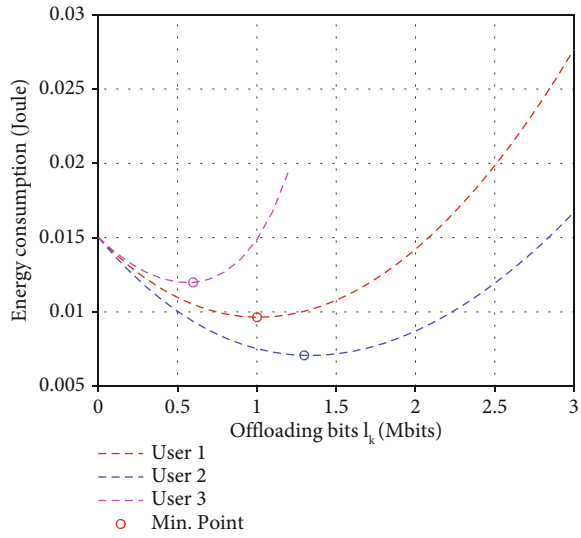

Figure 3: Energy consumption versus offloading bits for each user at the assumption of $T = 0.15$ s and $\epsilon = 0.2$

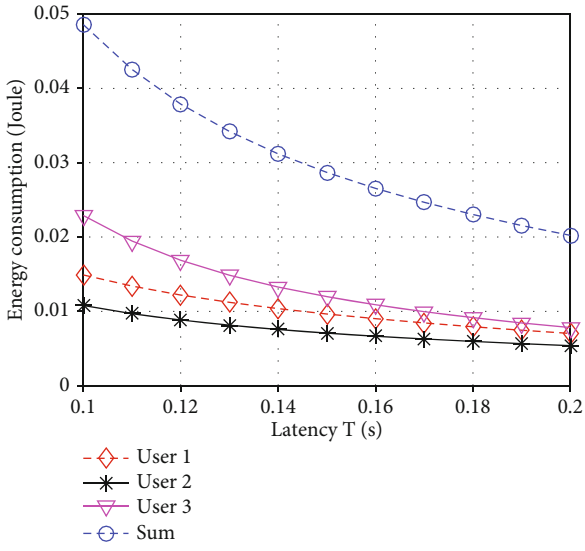

Figure 4: Minimum energy consumption versus latency for each user and their sum from 0.1 s to 0.2 s.

Mbits, and $l_3 = 0.6$ Mbits. Here, the resolution of offloading bits is 0.1 Mbits.

Although user 1 and user 3 have the same distances to the AP, due to the different distances to eve and the different SIC order, which result in the different secrecy outage capacities, user 1 has less energy consumption than user 3. Specifically, user 3 needs 0.0024 Joule more energy to overcome the distance difference of eve. Yet, user 2 has the least energy consumption even if it is not SIC decoded at last.

By the way, each user has an asymptotic ϵ-secrecy outage capacity. They are $C_{s,1}^{(2)}(\epsilon = 0.2) = 5.6589$ bps/Hz, $C_{s,2}^{(1)}(\epsilon = 0.2) = 5.1894$ bps/Hz, and $C_{s,3}^{(0)}(\epsilon = 0.2) = 1.2429$ bps/Hz. The asymptotic offloading bits for user 3 is about 1.86 Mbits, which indicates user 3 cannot conduct full offloading mode as the total bits of the task are 3 Mbits.

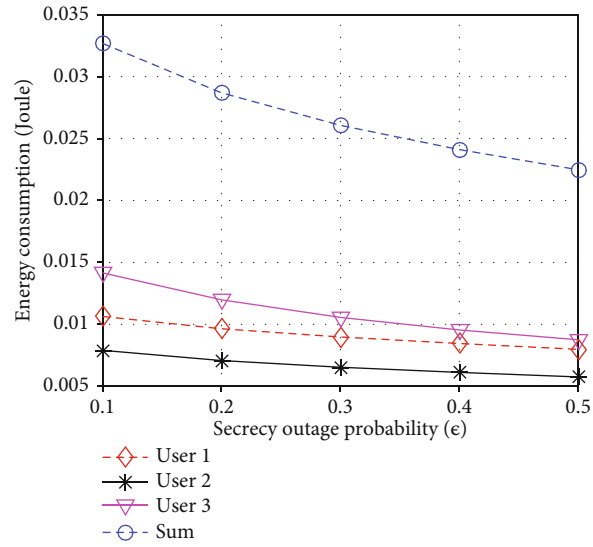

Figure 5: Minimum energy consumption versus secrecy outage probability for each user and their sum from $\epsilon = 0.1$ to $\epsilon = 0.5$.

We continue to study the impacts of the latency T and the secrecy outage probability ϵ on the minimum energy consumptions for each user and their sum.

We first illustrate the curves of the minimum energy consumption versus latency from $T = 0.1$ s to $T = 0.2$ s in Figure 4. For each user, the minimum energy consumption decreases with the increase of T. When $T = 0.1$ s, the minimum energy consumptions for user 1, user 2, user 3, and their sum are 0.015 Joule, 0.011 Joule, 0.023 Joule, and 0.049 Joule, respectively, while they are reduced to 0.007 Joule, 0.0054 Joule, 0.0078 Joule, and 0.0202 Joule when $T = 0.2$ s. The values for $T = 0.15$ s are the same as those achieved in Figure 3, which also confirms the reliability of the numerical results in Figure 4. As expected, user 2 has the least energy consumptions for the same T, while user 3 needs more energy consumption than user 1, just as in Figure 3.

Figure 5 depicts the curves of the minimum energy consumptions versus secrecy outage probability for each user and their sum from $\epsilon = 0.1$ to $\epsilon = 0.5$. It is easy to confirm the reliability of the numerical results in Figure 5 by observing the values for $\epsilon = 0.2$. Similar to the impact of latency T, the minimum energy consumptions decline with the secrecy outage probability increasing from 0.0106 Joule, 0.0079 Joule, 0.0142 Joule, 0.0327 Joule for $\epsilon = 0.1$ to 0.008 Joule, 0.0058 Joule, 0.0087 Joule, and 0.0225 Joule for $\epsilon = 0.5$. We note the minimum energy consumption for user 3 at $\epsilon = 0.1$ (0.0142 Joule) is very close to that of local computation only mode (0.015 Joule), which points out offloading is not always necessary especially when the eavesdropper's channel is much better than the legal channel.

5.2. Latency Minimization. Figure 6 shows the latency of the three end users versus offloading bits. The curves are generated on the assumption of the secrecy outage probability $\epsilon = 0.2$ and the energy budget $E^{bu} = 0.03$ Joule. The resolutions of the latency and offloading bits are 0.005 s and 0.05 Mbits, respectively. One can note each curve

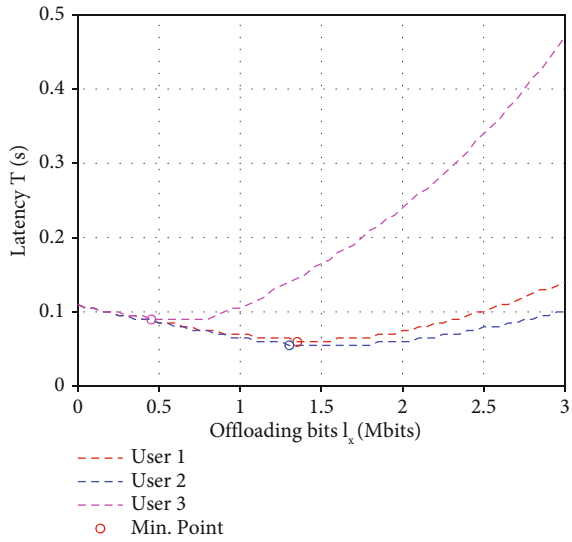

Figure 6: Latency versus offloading bits for each user at the assumption of $E^{bu} = 0.03$ Joule and $\epsilon = 0.2$.

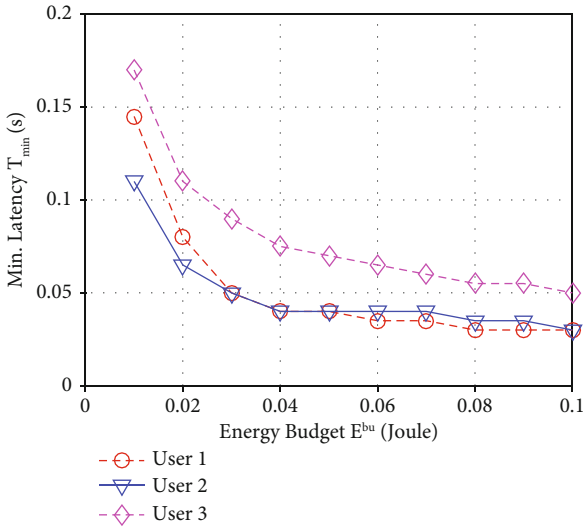

Figure 7: Minimum latency versus energy budget for each user from $E^{bu} = 0.01$ Joule to $E^{bu} = 0.1$ Joule.

declines first and then climbs up, which indicates there exists an optimal value. In this case, the minimum values of the latency for user 1, user 2, and user 3 are 0.06 s, 0.055 s, and 0.09 s, respectively, which are achieved by setting offloading bit $l_1^* = 1.35$ Mbits, $l_2^* = 1.30$ Mbits, and $l_3^* = 0.45$ Mbits, respectively. As such, $f_1^* = 1375$ MHz, $f_2^* = 1545.45$ MHz, $f_3^* = 1416.67$ MHz; $R_{s,1}^* = 2.25$ bps/Hz, $R_{s,2}^* = 2.36$ bps/Hz, $R_{s,3}^* = 0.5$ bps/Hz; and $p_1^* = 234.4$ mW, $p_2^* = 158.8$ mW, $p_3^* = 40.6$ mW.

Figure 7 shows the minimum latency versus the energy budget from $E^{bu} = 0.01$ Joule to $E^{bu} = 0.1$ Joule. As expected, the minimum latency decreases with the energy budget increasing. However, the decrease is significant from $E^{bu} = 0.01$ Joule to $E^{bu} = 0.04$ Joule, where the minimum latency for user 1 is reduced from 0.145 s to 0.05 s. For user 3 whose channel condition is not good enough, the reduction is still effective when E^{bu} is greater than 0.04 Joule. Meanwhile, the curves of user 1 and user 2 evert such that the minimum latency of user 2 is greater than that of user 1 from $E^{bu} = 0.05$.

Here so far, all these numeric results and observations in this section are consistent with the expectations.

6. Conclusion

In this work, we investigated a secure uplink NOMA-enabled MEC network under the threat of an eavesdropper, where K end users simultaneously offload their partial computation-intensive tasks to the MEC server in the same resource block and ZF-SIC is adopted at the multiantenna AP associated with MEC server. We first derived the closed-form expression of individual SOP for an arbitrary SIC order. We then characterize the optimization problem of sum-energy consumption subject to offloading bits, secrecy offloading rate, local CPU frequency, and transmit power and gave the solution. We further studied the problem of minimizing computation latency under condition of certain SOP requirement and energy budget through proving the equality of local computing time and offloading duration and transforming it into a single-variable problem. All the solutions are demonstrated and validated numerically by a 3-user case of a secure NOMA-enabled MEC network.

Appendix

Proof of Theorem 1

Given (5) and (6), jointly with the independence of $\gamma_k^{(n)}$ and ξ_k, the process of the derivation for the secrecy outage probability of user k is shown as follows,

$$
\begin{aligned}
P_{so,k}(n, R_s) &= \Pr\left(\frac{1+\gamma_k^{(n)}}{1+\xi_k} < 2^{R_s}\right) \\
&= 1 - \int_{2^{R_s}-1}^{\infty} d\gamma_k \int_0^{2^{-R_s}\gamma_k + 2^{-R_s} - 1} f_{\gamma_k^n}(\gamma_k) f_{\xi_k}(\xi_k) d\xi_k \\
&= 1 - \int_{2^{R_s}-1}^{\infty} f_{\gamma_k^n}(\gamma_k) F_{\xi_k}\left(2^{-R_s}\gamma_k + 2^{-R_s} - 1\right) d\gamma_k \\
&= 1 - \int_{2^{R_s}-1}^{\infty} \frac{\lambda_k^{N-n}\gamma_k^{N-n-1}}{\Gamma(N-n)e^{\lambda_k\gamma_k}} \left(1 - e^{-\mu_k\left(2^{-R_s}\gamma_k + 2^{-R_s} - 1\right)}\right) \\
&\quad \cdot d\gamma_k = 1 - \frac{\lambda_k^{N-n}}{\Gamma(N-n)} \int_{2^{R_s}-1}^{\infty} \gamma_k^{N-n-1} e^{-\lambda_k\gamma_k} d\gamma_k \\
&\quad + \frac{\lambda_k^{N-n} e^{\mu_k\left(1-2^{-R_s}\right)}}{\Gamma(N-n)} \int_{2^{R_s}-1}^{\infty} \gamma_k^{N-n-1} e^{-\left(\lambda_k + \mu_k 2^{-R_s}\right)\gamma_k} d\gamma_k \\
&= 1 - \frac{\Gamma\left(N-n, \lambda_k\left(2^{R_s}-1\right)\right)}{\Gamma(N-n)} \\
&\quad + \frac{\lambda_k^{N-n} e^{\mu_k\left(1-2^{-R_s}\right)}}{\left(\lambda_k + \mu_k 2^{-R_s}\right)^{N-n}} \frac{\Gamma\left(N-n, \left(\lambda_k + \mu_k 2^{-R_s}\right)\left(2^{R_s}-1\right)\right)}{\Gamma(N-n)} \\
&= \frac{\gamma\left(N-n, \lambda_k\left(2^{R_s}-1\right)\right)}{\Gamma(N-n)} \\
&\quad + \frac{\lambda_k^{N-n} e^{\mu_k\left(1-2^{-R_s}\right)}}{\left(\lambda_k + \mu_k 2^{-R_s}\right)^{N-n}} \frac{\Gamma\left(N-n, \left(\lambda_k + \mu_k 2^{-R_s}\right)\left(2^{R_s}-1\right)\right)}{\Gamma(N-n)}.
\end{aligned}
\tag{A.1}
$$

The following integral result is applied [[38], Eq. (3.381.9)] during the above derivation,

$$\int_u^{\infty} x^m e^{-\beta x} dx = \frac{\Gamma(m+1, \beta u)}{\beta^{m+1}}. \tag{A.2}$$

The proof is completed.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the General Scientific Research Projects of Zhejiang Education Department (Grant no. Y202147949).

References

[1] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: the communication perspective," *IEEE communications surveys & tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[2] T. D. Burd and R. W. Brodersen, "Processor design for portable systems," *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 13, no. 2-3, pp. 203–221, 1996.

[3] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[4] K. Guo, R. Gao, W. Xia, and T. Q. S. Quek, "Online learning based computation offloading in mec systems with communication and computation dynamics," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1147–1162, 2021.

[5] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: review and analysis of mobile edge computing and fog from a security and resilience perspective," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2586–2595, 2017.

[6] Y. Zhang, J. He, and S. Guo, "Energy-efficient dynamic task offloading for energy harvesting mobile cloud computing," in *2018 IEEE Int. Conf. Netw., Architecture and Storage (NAS)*, pp. 1–4, Chongqing, China, 2018.

[7] S. Chouhan, "Energy optimal partial computation offloading framework for mobile devices in multi-access edge computing," in *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, Split, Croatia, 2019.

[8] C. He, R. Wang, and Z. Tan, "Energy-aware collaborative computation offloading over mobile edge computation empowered fiber-wireless access networks," *IEEE Access*, vol. 8, pp. 24662–24674, 2020.

[9] X. Li, Y. Dang, M. Aazam, X. Peng, T. Chen, and C. Chen, "Energy-efficient computation offloading in vehicular edge cloud computing," *IEEE Access*, vol. 8, pp. 37632–37644, 2020.

[10] R. M. Shukla and A. Munir, "A computation offloading scheme leveraging parameter tuning for real-time iot devices," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, pp. 208-209, Gwalior, India, 2016.

[11] R. M. Shukla and A. Munir, "An efficient computation offloading architecture for the internet of things (iot) devices," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 728–731, Las Vegas, NV, USA, 2017.

[12] F. Zhou, Y. Wu, R. Q. Hu, and Y. Qian, "Computation rate maximization in uav-enabled wireless-powered mobile-edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1927–1941, 2018.

[13] Y. Shuai and R. Langar, "Collaborative computation offloading for multi-access edge computing," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 689–694, Arlington, VA, USA, 2019.

[14] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7944–7956, 2019.

[15] J. Xu, P. Zhu, J. Li, and X. You, "Secure computation offloading for multi-user multi-server mec-enabled iot," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, Montreal, QC, Canada, 2021.

[16] L. Tang and Q. Li, "Energy and time optimization for wireless computation offloading," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, Nanjing, China, 2015.

[17] I. A. Elgendy, W.-Z. Zhang, Y. Zeng, H. He, Y.-C. Tian, and Y. Yang, "Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile iot networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2410–2422, 2020.

[18] U. A. Khan, W. Khalid, and S. Saifullah, "Energy efficient resource allocation and computation offloading strategy in a uav-enabled secure edge-cloud computing system," in *2020 IEEE Int. Conf. Smart Internet of Things (SmartIoT)*, pp. 58–63, Beijing, China, 2020.

[19] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998.

[20] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[21] P. Zhao, W. Zhao, H. Bao, and B. Li, "Security energy efficiency maximization for untrusted relay assisted Noma-mec network with wpt," *IEEE Access*, vol. 8, pp. 147387–147398, 2020.

[22] X. He, R. Jin, and H. Dai, "Physical-layer assisted secure offloading in mobile-edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4054–4066, 2020.

[23] L. Qian, W. Wu, W. Lu, Y. Wu, B. Lin, and T. Q. Quek, "Secrecy-based energy-efficient mobile edge computing via cooperative non-orthogonal multiple access transmission," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4659–4677, 2021.

[24] W. Wu, X. Wang, F. Zhou, K. K. Wong, C. Li, and B. Wang, "Resource allocation for enhancing offloading security in Noma-enabled mec networks," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3789–3792, 2021.

[25] D. Han and T. Shi, "Secrecy capacity maximization for a uav-assisted mec system," *China Communications*, vol. 17, no. 10, pp. 64–81, 2020.

[26] Y. Li, Y. Fang, and L. Qiu, "Joint computation offloading and communication design for secure uav-enabled mec systems," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Nanjing, China, 2021.

[27] X. Gu, G. Zhang, M. Wang, W. Duan, M. Wen, and P. H. Ho, "UAV-aided energy-efficient edge computing networks: security offloading optimization," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4245–4258, 2022.

[28] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient computation offloading for secure uav-edge-computing systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 6074–6087, 2019.

[29] W. Zhao, B. Wang, H. Bao, and B. Li, "Secure energy-saving resource allocation on massive mimo-mec system," *IEEE Access*, vol. 8, pp. 137244–137253, 2020.

[30] W. Wei and F. Zhou, "Energy-efficient resource allocation for secure Noma-enabled mobile edge computing networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 493–505, 2020.

[31] H. Lin, Y. Cao, Y. Zhong, and P. Liu, "Secure computation efficiency maximization in Noma-enabled mobile edge computing networks," *IEEE Access*, vol. 7, pp. 87504–87512, 2019.

[32] J.-B. Wang, H. Yang, M. Cheng, J.-Y. Wang, M. Lin, and J. Wang, "Joint optimization of offloading and resources allocation in secure mobile edge computing systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8843–8854, 2020.

[33] S. Han, X. Xu, S. Fang et al., "Energy efficient secure computation offloading in Noma-based mmtc networks for iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5674–5690, 2019.

[34] F. Fang, K. Wang, and Z. Ding, "Optimal task assignment and power allocation for downlink Noma mec networks," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[35] M. Zhao, H. Bao, L. Yin, J. Yao, and T. Q. S. Quek, "Secrecy offloading rate maximization for multi-access mobile edge computing networks," *IEEE Communications Letters*, vol. 25, no. 12, pp. 3800–3804, 2021.

[36] K. Jiang, T. Jing, Z. Li, Y. Huo, and F. Zhang, "Analysis of secrecy performance in fading multiple access wiretap channel with sic receiver," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.

[37] K. Jiang, T. Jing, F. Zhang, Y. Huo, and Z. Li, "ZF-SIC based individual secrecy in simo multiple access wiretap channel," *IEEE Access*, vol. 5, pp. 7244–7253, 2017.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, 7th edition, 2007.