Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Energy- and Latency-Efficient Offloading for Secure Cooperative UAV-NOMA-Enabled Mobile Edge Computing Networks

Kaiwei Jiang

kwjiang@bjtu.edu.cn

Taizhou Vocational and Technical College

Article

Keywords:

Posted Date: November 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11176890/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Energy- and Latency-Efficient Offloading for Secure Cooperative UAV-NOMA-Enabled Mobile Edge Computing Networks

Kaiwei Jiang[1,2*]

[1*]School of Mechanical and Electrical Engineering, Taizhou Vocational and Technical College, Xueyuan Road, Taizhou, 318000, Zhejiang, China.

[2]School of Electronics and Information Engineering, Beijing Jiaotong University, Shangyuancun, Haidian, 100044, Beijing, Country.

Corresponding author(s). E-mail(s): kwjiang@bjtu.edu.cn;

Abstract

This work investigates energy- and latency-efficient computation offloading for secure cooperative UAV-NOMA-enabled MEC networks in the presence of an eavesdropper. A subset of UAVs serves as jammers to mitigate eavesdropping, while the rest perform partial offloading. Given the passive eavesdropper assumption, secrecy outage probability is adopted as the secrecy metric, and its closed-form expression is derived by analyzing SINR statistics at the ground access point and the eavesdropper. Three non-convex optimization problems are formulated: minimizing individual UAV energy consumption, minimizing total energy of offloading and jamming UAVs, and minimizing task latency under an energy budget. Suboptimal solutions are obtained via constraint simplification, multi-to-single-variable transformation, and numerical methods. Results demonstrate that partial offloading balances energy and latency, with optimal offloading bits and jamming power; larger latency deadlines, secrecy outage probability thresholds, or energy budgets enhance performance.

Keywords: Unmanned aerial vehicle (UAV), multi-access edge computing (MEC), energy-efficient, latency-efficient, cooperative jamming, non-orthogonal multiple access (NOMA), successive interference cancellation (SIC)

1 Introduction

1.1 Background

With the rapid proliferation of the internet of things (IoT) and the advent of latency-sensitive, computation-intensive applications, such as augmented reality (AR), ultra-high definition (UHD) video streaming, and tactile Internet, traditional cloud computing architectures face insurmountable challenges in meeting stringent quality-of-service (QoS) requirements [1, 2]. The centralized nature of cloud computing leads to excessive end-to-end latency due to long-distance data transmission, while the resource constraints of IoT devices (e.g., limited battery capacity, weak computational power) further hinder local execution of complex tasks [3]. To address these limitations, mobile edge computing (MEC) has emerged as a transformative paradigm, deploying computing and storage resources at the network edge (e.g., base stations (BSs), road-side units (RSUs)) to reduce latency and alleviate core network congestion [2, 4]. By enabling task offloading from resource-constrained IoT devices to nearby MEC servers, MEC significantly enhances the efficiency of real-time applications and extends the battery life of IoT terminals [5, 6].

However, the performance of MEC-enabled networks is inherently constrained by wireless communication bottlenecks, especially in dense IoT deployments where multiple devices compete for limited spectral resources. Conventional orthogonal multiple access (OMA) techniques, which allocate exclusive time/frequency resources to each user, struggle to meet the massive connectivity demands of next-generation IoT networks [7]. In this context, non-orthogonal multiple access (NOMA) has been adopted, allowing multiple users to share the same frequency-time resource via power-domain multiplexing [7, 8]. By exploiting successive interference cancellation (SIC) at the receiver, NOMA achieves higher spectral efficiency, lower access latency, and improved user fairness compared to OMA, making it an ideal candidate for MEC-enabled scenarios with diverse user requirements [9, 10].

The integration of unmanned aerial vehicles (UAVs) further expands the capabilities of MEC-NOMA networks. UAVs, with their flexible deployment, 3-D mobility, and line-of-sight (LoS) communication advantages, can act as aerial MEC servers, relays, or data collectors to enhance coverage in remote areas, disaster-stricken regions, or crowded hotspots [11, 12]. For instance, UAV-aided MEC systems can dynamically offload tasks from ground IoT devices in areas with damaged terrestrial infrastructure [13], or assist in load balancing during traffic bursts at large events [14]. Nevertheless, UAVs inherently suffer from resource limitations, including finite battery life, constrained computational power, and limited memory, which pose challenges to their role as reliable edge nodes [15]. Moreover, the open nature of wireless channels and the high mobility of UAVs expose MEC-NOMA networks to severe security threats, such as eavesdropping, jamming, and spoofing [16, 17]. These threats not only compromise data confidentiality and integrity but also degrade the efficiency of task offloading and resource allocation.

To mitigate security risks in UAV-aided MEC-NOMA systems, physical-layer security (PLS) has gained significant attention as a lightweight and efficient solution. Unlike upper-layer cryptography, which relies on complex mathematical algorithms

and may be infeasible for resource-constrained UAVs and IoT devices, PLS leverages the intrinsic randomness of wireless channels (e.g., fading, interference) to ensure information-theoretic security [17, 18]. Key PLS metrics, such as secrecy rate, secrecy capacity, and secrecy outage probability, quantify the ability to protect legitimate communications from eavesdroppers [3]. For example, UAVs can transmit artificial noise to jam eavesdroppers [18], or optimize their trajectories to enhance the LoS link with legitimate users while weakening the eavesdropper's channel [19]. When combined with NOMA, PLS can further improve security by exploiting power-domain differences between users to isolate malicious nodes [8, 9].

Despite these advancements, three critical challenges remain unresolved in the design of energy- and latency-efficient secure MEC-NOMA networks:

- Energy Efficiency Trade-offs: UAVs and IoT devices operate on limited energy, yet secure offloading (e.g., PLS-enabled transmission, artificial noise generation) and NOMA interference cancellation increase energy consumption [20, 21]. Balancing security requirements with energy efficiency, especially for UAVs with strict flight endurance constraints, remains a major hurdle.
- Latency Optimization Under Security Constraints: Task offloading in MEC-NOMA systems involves joint optimization of communication (e.g., power allocation, SIC decoding) and computation (e.g., offloading ratio, resource scheduling) resources. Security constraints (e.g., minimum secrecy rate) further complicate this optimization, as they may introduce additional latency overhead [10, 22].
- Dynamic Network Adaptation: The mobility of UAVs and IoT devices, coupled with time-varying wireless channels, leads to dynamic network topologies. Traditional static resource allocation and security schemes fail to adapt to these changes, resulting in suboptimal performance [23].

1.2 Motivation and Contributions

1.2.1 Motivation

The integration of UAVs, MEC, and NOMA has become a core paradigm for supporting latency-sensitive, computation-intensive IoT applications (e.g., disaster response, precision agriculture, crowd monitoring), thanks to UAVs' flexible deployment, MEC's low-latency edge computing, and NOMA's high spectral efficiency [4, 7, 8]. However, three critical gaps hinder its practical deployment, driving the need for targeted research:

First, security-constrained resource conflicts remain unaddressed. UAVs' finite battery and constrained computing power clash with the dual demands of secure offloading and efficient NOMA operation: PLS mechanisms (e.g., cooperative jamming) and SIC increase energy consumption, while strict flight endurance and latency deadlines leave no room for redundant resource allocation [15, 20]. This conflict often forces trade-offs that sacrifice either security or efficiency.

Second, static schemes fail in dynamic environments. UAV mobility and time-varying channels lead to rapidly changing network topologies. Traditional static

strategies (e.g., fixed offloading ratios, constant jamming power) cannot adapt, resulting in either excessive secrecy outage probability or unnecessary energy expenditure [23].

Third, unified optimization of security, energy, and latency is lacking. Existing works either prioritize energy/latency optimization without rigorous security guarantees [5, 6], or focus on PLS without accounting for UAV-MEC-NOMA-specific constraints (e.g., SIC decoding order, jamming UAV coordination). Few studies address all three objectives in a joint framework, especially for partial offloading, which is critical for balancing UAV resource limits and application demands.

Emerging technologies like federated learning (FL) and blockchain show promise for adaptive optimization and decentralized trust [24, 25]. For example, double deep Q-networks (DDQNs) optimize latency/energy in secure MEC-NOMA systems [26], and FL preserves privacy during collaborative resource allocation [27–29]; blockchain provides tamper-proof records for offloading transactions [30]. However, their integration with PLS and NOMA is still in its infancy, especially in energy- and latency-constrained UAV scenarios. There is an urgent need for lightweight, numerically tractable solutions that balance these competing objectives.

In summary, designing energy- and latency-efficient offloading mechanisms for secure cooperative UAV-NOMA-enabled MEC networks is critical to unlocking UAV applications' full potential. This work addresses these challenges by leveraging PLS, NOMA, and adaptive optimization, with a focus on balancing security, energy efficiency, and latency in UAV-enabled MEC environments.

1.2.2 Contributions

To fill the aforementioned gaps, this paper makes four key contributions:

- Novel Secure Partial Offloading System Model with Cooperative Jamming: We propose a cooperative UAV-NOMA-enabled MEC network where a subset of UAVs acts as jammers, while the rest perform partial task offloading. The model integrates dynamic voltage and frequency scaling (DVFS) for UAV local computing, capturing the trade-off between energy, latency, and secrecy more realistically than full/zero offloading models [Section 3].
- Closed-Form Derivation of Secrecy Outage Probability (SOP): By analyzing the statistical characteristics of signal-to-interference-plus-noise ratios (SINRs) at the multi-antenna ground access point (AP) and the passive eavesdropper, we derive a closed-form SOP expression. This expression quantifies the probability of secrecy rate falling below a target threshold, providing a rigorous, tractable security metric for optimization [Section 3.3].
- Non-Convex Optimization and Suboptimal Solution Framework: We formulate three core optimization problems:
  - **P1**: Minimize individual energy consumption of each offloading UAV (under latency and SOP constraints).
  - **P2**: Minimize total energy consumption of offloading and jamming UAVs.
  - **P3**: Minimize task latency for each UAV (under an energy budget and SOP constraint).

To tackle non-convexity (arising from SOP and NOMA interference), we propose a three-step framework: (1) simplify constraints via lemmas (e.g., binding CPU frequency to latency deadlines, Lemma 2); (2) transform multi-variable problems into single-variable counterparts); (3) solve via numerical methods [Section 5].

- Computational Complexity Analysis and Numerical Validation: We analyze the computational complexity of the proposed algorithms: $\mathrm{O}(m^3)$ for **P1**, $\mathrm{O}(m^5)$ for **P2**, and $\mathrm{O}(m^4)$ for **P3** (where m is SOP computation complexity). Extensive simulations validate that:
  - Partial offloading outperforms full/zero offloading, with each UAV achieving minimum energy at an optimal offloading bit ratio;
  - Optimal jamming power exists to balance jamming energy and offloading security;
  - Larger latency deadlines, SOP thresholds, or energy budgets significantly improve performance, especially for UAVs with weaker channel conditions [Section 6].

This work provides a practical, theoretically grounded framework for secure, energy- and latency-efficient offloading in UAV-NOMA-enabled MEC networks, bridging gaps between security modeling, resource optimization, and real-world deployment constraints.

1.3 Organization

The remainder of this paper is organized as follows. Section 2 give a brief introduction of the methodology used in this work. Section 3 presents and characterizes the system model for secure cooperative UAV-NOMA-enabled MEC networks, detailing the network topology, node roles, and key signal/channel models. Section 4 formulates the core optimization problems, including energy-efficient and latency-efficient objectives, with constraints on SOP, task deadlines, and resource limits. Suboptimal solutions for these non-convex problems are provided in Section 5, along with corresponding algorithm designs and computational complexity analysis. Section 6 validates the proposed strategies through simulations, presenting numerical results on energy consumption, latency, and the impacts of key parameters. Section 7 discusses the limitations of the study, and proposes the key directions for future research. Finally, Section 8 highlights key findings and concludes the work.

Notation: Vectors and matrices are denoted using a bold font. Let $\mathbf{I}_m$ represent the $m \times m$ identity matrix, and let $\|\cdot\|$ denote the Euclidean norm operator. Sets are indicated by a script font: $\mathcal{A}\backslash\mathcal{B}$ denotes the set difference (set $\mathcal{A}$ minus set $\mathcal{B}$), and $|\cdot|$ denotes the cardinality of a set. Distributions are specified as follows: $\mathcal{CN}$ for the circular symmetric complex Gaussian distribution, Exp for the exponential distribution, and χ^2_m for the chi-squared distribution with m degrees of freedom. The operator $[\cdot]^+ = max(\cdot, 0)$ denotes the non-negative part of a scalar. The logarithm log is base-2, and $Pr(\cdot)$ denotes the probability of an event.

2 Methods

We present an energy- and latency-efficient computation offloading method for secure cooperative UAV-NOMA-enabled MEC networks in the presence of an eavesdropper,

where a subset of UAVs acts as jammers for eavesdropping mitigation and the rest perform partial task offloading. This method is based on the statistical characteristics of SINR at the legitimate ground access point (AP) and the passive eavesdropper, and the trade-off between local computation and secure offloading of UAVs. Firstly, the system model of the cooperative UAV-NOMA-MEC network is constructed, including the definitions of local computation and secure partial offloading processes, and the SINR models at the AP and eavesdropper are established. Secondly, the closed-form expression of SOP is derived by analyzing the probability distribution of SINR, which serves as the core security metric for the subsequent optimization. Thirdly, three non-convex optimization problems are formulated according to different optimization objectives (minimizing individual UAV energy consumption, minimizing total energy of offloading and jamming UAVs, minimizing task latency under energy budget), with constraints of SOP, task latency deadline, UAV hardware performance and offloading bit range. Finally, suboptimal solutions for the non-convex problems are obtained through constraint simplification, multi-to-single-variable transformation and numerical methods, and the computational complexity of the corresponding solving algorithms is analyzed.

In our proposed research work, the experiments are conducted in a simulated environment with a 5-UAV scenario (3 offloading UAVs and 2 jamming UAVs). Various performance metrics are monitored and collected, including individual energy consumption versus offloading bits, minimum energy consumption versus latency deadline/SOP threshold/jamming power, task latency versus offloading bits, and minimum latency versus energy budget. Test metrics are critical for evaluating the performance advantages of the proposed offloading method under different network parameters and constraints.

3 System Model

We consider a secure cooperative UAV-NOMA-enabled MEC network. As illustrated in Fig. 1, a set of K hovering UAVs (denoted as $\mathcal{K}$) can offload their computation-intensive tasks (their own or collected from ground IoTs) to an edge computing server through a ground AP using the NOMA technique, while facing the threat of eavesdropping from a malicious eavesdropper (Eve). To enhance the secure offloading performance, the hovering UAVs operate in a cooperative mode: a specific subset of them (denoted as set $\mathcal{J}$) are designated as jammers, which emit artificial noise to interfere with Eve's interception, thereby improving the secure offloading rates for the remaining UAVs.

We assume that the ground AP is equipped with N antennas where $N \geq K$, whereas all other nodes, including the hovering UAVs and the eavesdropper (Eve), are configured with a single antenna each. The wireless channels between the UAVs and the AP, as well as those between the UAVs and Eve, are independent and subject to quasi-static Rayleigh fading. During the task offloading phase, the AP has perfect knowledge of each UAV's channel state information (CSI) and is capable of suppressing the pseudo-random artificial noise signals transmitted by the jammer UAVs. The symbols used in subsequent sections are defined in Table 1.

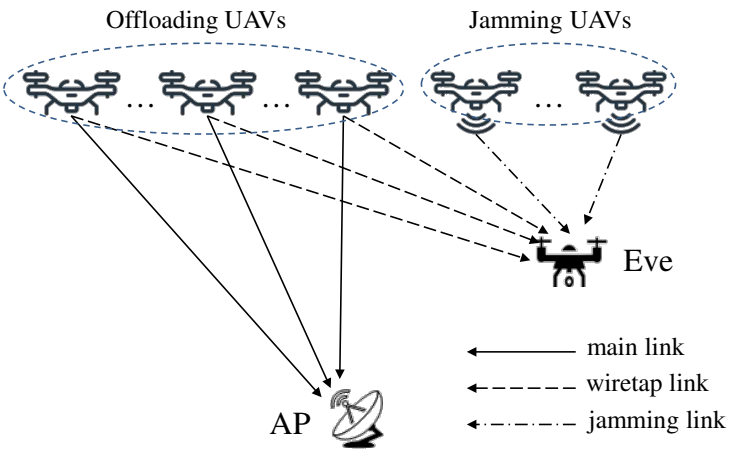


Fig. 1 A secure cooperative UAV-NOMA-enabled MEC network in the presence of an eavesdropper, where a subset of UAVs serves as jammers to mitigate eavesdropping, while the rest perform partial offloading.

Table 1 Symbol description.

Symbol	Description
x_k	Complex information symbol from UAV U_k
p_k	Offloading power from UAV U_k
$\mathbf{h}_k$	Channel gain vector from UAV U_k to AP
g_k	Channel gain from UAV U_k to Eve
$\mathbf{w}_a$	Complex Gaussian noise vector at AP
w_e	Complex Gaussian noise at Eve

After applying SIC, the aggregate received signals remaining at the ground AP and Eve before decoding UAV U_k can be characterized as follows:

$$\mathbf{y}_k^{(\Im)} = \mathbf{h}_k x_k + \sum_{i \in \Im} \mathbf{h}_i x_i + \mathbf{w}_a, \tag{1}$$

$$z_k^{(\mathcal{J})} = g_k x_k + \sum_{i \in \mathcal{J}} g_i x_i + w_e, \tag{2}$$

where $\Im \subseteq \mathcal{K} \backslash \mathcal{J} \backslash \{k\}$ denotes the set of co-channel interferer indices.

A conservative assumption is adopted: all co-channel interference in NOMA is canceled out, with only artificial noise remaining at Eve. The channel and noise parameters follow the following distributions: $\mathbf{h}_k \sim \mathcal{CN}(0, \delta_k^2 \mathbf{I}_N)$, $\mathbf{w}_a \sim \mathcal{CN}(0, N_a \mathbf{I}_N)$, $g_k \sim \mathcal{CN}(0, \sigma_k^2)$, $w_e \sim \mathcal{CN}(0, N_e)$.

3.1 Local Computation

We consider a more generalized scenario wherein each UAV's computation task can be partitioned into two components at an arbitrary ratio: one allocated for task offloading and the other for local computing. For UAV U_k, let L_k denote the total number of bits to be processed, l_k the number of bits processed remotely (i.e., $L_k - l_k$ bits locally), and X_k the computation intensity measured in CPU cycles per local bit. To regulate energy consumption, the DVFS technique is employed. As reported in [31], the energy consumption per CPU cycle can be modeled as $\kappa_k f_k^2$, where κ_k is a hardware-dependent constant associated with U_k's architecture, and f_k represents the CPU frequency of U_k. Consequently, the energy consumption for the local computation of $L_k - l_k$ bits is formulated as follows:

$$E_k^{loc} = \kappa_k (L_k - l_k) X_k f_k^2. \tag{3}$$

The corresponding computation time is given by:

$$t_k^{loc} = \frac{(L_k - l_k) X_k}{f_k}. \tag{4}$$

3.2 Secure Partial Offloading

Denote $R_{s,k}$ to be the secrecy rate that satisfies the targeted secure QoS at the offloading power of p_k for U_k. For simplicity, we assume the secrecy rate is constant during offloading. Therefore, the offloading duration is

$$t_k^{off} = \frac{l_k}{B R_{s,k}}, \tag{5}$$

where B is the channel's bandwidth.

The energy consumption of offloading is given by

$$E_k^{off} = p_k \frac{l_k}{B R_{s,k}}, \tag{6}$$

As the eavesdropper is always passive, and its CSI can not be mastered by the legal nodes in the MEC network. To this end, we adopt the secrecy outage probability for quantifying the QoS of secure offloading.

3.3 Secrecy Outage Probability

Prior to deriving the closed-form expression of the SOP, we first need to derive the statistical characteristics of the SINRs at both the AP and Eve.

Consistent with the approach in [32], we employ zero forcing (ZF). Based on this, the instantaneous main capacity for UAV U_k is given by

$$C_{b,k}^{(\Im)} = \log\left(1+\gamma_k^{(\Im)}\right) = \log\left(1+\frac{p_k\|\mathbf{Q}_k^{(\Im)}\mathbf{h}_k\|^2}{N_a}\right), \tag{7}$$

where $\mathbf{Q}_k^{(\Im)}$ is a $N-|\Im|$ by N matrix and $\mathbf{Q}_k^{(\Im)}\mathbf{Q}_k^{(\Im)H} = \mathbf{I}_{N-|\Im|}$.

From [32], we can conclude that $\gamma_k^{(\Im)}$ follows a chi-squared distribution with $2\times(N-|\Im|)$ degrees of freedom, and its distribution depends only on the cardinality of set $\Im$, rather than the specific UAVs contained within $\Im$. The closed-form expression of the probability distribution function (PDF) is given as follows [33],

$$f_{\gamma_k^{(n)}}(\gamma_k) = \frac{\lambda_k^{N-n}}{(N-n-1)!}\gamma_k^{N-n-1}e^{-\lambda_k\gamma_k},\ \gamma_k>0, \tag{8}$$

where $\lambda_k = \frac{N_a}{p_k\delta_k^2}$, $\forall k\in\mathcal{K}$.

Here, we replace the cardinality $|\Im|$ with n, and rewrite $\gamma_k^{(\Im)}$ by $\gamma_k^{(n)}$.

The instantaneous eavesdropper's capacity for U_k is

$$C_{e,k}^{(\mathcal{J})} = \log\left(1+\eta_k^{(\mathcal{J})}\right) = \log\left(1+\frac{\xi_k}{1+\sum_{i\in\mathcal{J}}\xi_i}\right), \tag{9}$$

where $\xi_i = \frac{|g_i|^2 p_i}{N_e}$,$\forall i\in\mathcal{K}$.

Obviously, all ξ_i ($\forall i\in\mathcal{K}$) in $\eta_k^{(\mathcal{J})}$ are mutually independent and exponentially distributed, i.e., $\xi_i\sim\text{Exp}(\mu_i)$, where $\mu_i = \frac{N_e}{p_i\sigma_i^2}$, $\forall i\in\mathcal{K}$. The cumulative distribution function (CDF) of $\eta_k^{(\mathcal{J})}$ can be derived as

$$F_{\eta_k^{(\mathcal{J})}}(\eta_k) = 1-\frac{e^{-\mu_k\eta_k}}{\prod_{i\in\mathcal{J}}\left(1+\frac{\mu_k}{\mu_i}\eta_k\right)}, \eta_k\geq 0. \tag{10}$$

Proof See Appendix A. □

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

Theorem 1 *The secrecy outage probability of an individual UAV U_k, with cooperative jamming from UAVs in the set $\mathcal{J}$ and in the presence of n co-channel interferers, can be expressed as*

$$P_{so,k}^{(\mathcal{J})}(n,R_s) = \frac{\boldsymbol{\gamma}(N-n,\lambda_k(2^{R_s}-1))}{(N-n-1)!} + \frac{\lambda_k^{N-n}e^{\lambda_k(1-2^{R_s})}}{(N-n-1)!}\sum_{i\in\mathcal{J}}a_i\Theta(\mu_i) \tag{11}$$

where

$$\Theta(\mu_i) = \frac{\mu_i}{\mu_k} 2^{R_s} e^{\mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k})} \sum_{m=0}^{N-n-1} \binom{N-n-1}{m} \times (-2^{R_s}(\frac{\mu_i}{\mu_k}-1)-1)^{N-n-m-1} \frac{\Gamma(m, \mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k}))}{(2^{-R_s}\mu_k+\lambda_k)^m}, \tag{12}$$

and

$$a_i = \frac{1}{\prod_{j\in\mathcal{J}, j\neq i}\left(1-\frac{\mu_i}{\mu_j}\right)}, i \in \mathcal{J}. \tag{13}$$

$\boldsymbol{\gamma}(a,x)$ and $\Gamma(a,x)$ denote the lower incomplete gamma function and the upper (complementary) incomplete gamma function, respectively, with the relationship $\boldsymbol{\gamma}(a,x) + \Gamma(a,x) = \Gamma(a)$ (where $\Gamma(a)$ is the complete gamma function).

Proof See Appendix B. □

4 Problem Formulation

This section concentrates on formulating the energy- and latency-aware resource allocation problem for the secure cooperative UAV-NOMA-enabled MEC network. The optimization variables encompass the offloading transmit power p_k, the number of offloaded bits l_k, the secrecy offloading rate $R_{s,k}$, and the local CPU operating frequency f_k, all of which are subject to the task constraint $A_k(L_k, T, X_k)$ of each UAV U_k.

By convention, our investigation exclusively focuses on the energy efficiency of the UAVs themselves (i.e., UAV-side energy consumption). We neglect two latency components: the data processing latency at the MEC server and the downlink transmission latency from the AP to the UAVs. This simplification is valid because MEC servers are typically equipped with high-performance computing capabilities (resulting in negligible processing delay) and the volume of processed result data returned to UAVs is significantly smaller than that of the offloaded task data (leading to minimal downlink latency).

Without loss of generality, we assume that UAVs U_1, U_2, ..., $U_{|\mathcal{J}|}$ are assigned to act as jammers, while the remaining UAVs $U_{|\mathcal{J}|+1}, U_{|\mathcal{J}|+2}, ..., U_K$ are dedicated to task offloading. We further specify that the AP decodes the offloaded signals of the latter group using successive interference cancellation in the order $U_{|\mathcal{J}|+1} \rightarrow U_{|\mathcal{J}|+2} \rightarrow ... \rightarrow U_K$. Under this SIC decoding order, the number of co-channel interferers encountered by UAV U_k (where $|\mathcal{J}|+1 \leq k \leq K$) is given by $n = K-k$.

4.1 Energy-Efficient Problem Formulation

4.1.1 Problem 1: Individual

Mathematically, under the constraint of a fixed jamming transmit power for the jammer UAVs (set $\mathcal{J}$), the individual energy consumption minimization problem for the

offloading UAV U_k (where $|\mathcal{J}|+1 \leq k \leq K$) can be formulated as follows:

$$\mathbf{P1}: \min_{f_k, l_k, p_k, R_{s,k}} \kappa_k (L_k - l_k) X_k f_k^2 + p_k \frac{l_k}{BR_{s,k}} \tag{14a}$$

$$s.t. \ \frac{(L_k - l_k) X_k}{f_k} \leq T, \tag{14b}$$

$$\frac{l_k}{BR_{s,k}} \leq T, \tag{14c}$$

$$P_{so,k}^{(\mathcal{J})}(K-k, R_{s,k}) \leq \epsilon, \tag{14d}$$

$$0 \leq l_k \leq L_k, \tag{14e}$$

$$f_k \leq f_k^{max}, \tag{14f}$$

where T represents the task completion deadline (i.e., the maximum allowable latency to finish the entire computation task), and f_k^{max} denotes the maximum CPU frequency constraint (upper bound) of UAV U_k.

4.1.2 Problem 2: Overall

Accordingly, the overall energy consumption minimization problem, which integrates the energy consumption of all offloading UAVs and the jamming energy consumption of jammer UAVs, can be formulated as follows:

$$\mathbf{P2}: \min_{\mathbf{f}, \mathbf{l}, \mathbf{p}, \mathbf{R}_s} \sum_{k=|\mathcal{J}|+1}^{K} \left(\kappa_k (L_k - l_k) X_k f_k^2 + p_k \frac{l_k}{BR_{s,k}} \right) + \sum_{j=1}^{|\mathcal{J}|} p_j \max_k \frac{l_k}{BR_{s,k}} \tag{15a}$$

$$s.t. \ \frac{(L_k - l_k) X_k}{f_k} \leq T, \ \ \forall k \in \mathcal{K}/\mathcal{J}, \tag{15b}$$

$$\frac{l_k}{BR_{s,k}} \leq T, \ \ \forall k \in \mathcal{K}/\mathcal{J}, \tag{15c}$$

$$P_{so,k}^{(\mathcal{J})}(K-k, R_{s,k}) \leq \epsilon, \ \ \forall k \in \mathcal{K}/\mathcal{J}, \tag{15d}$$

$$0 \leq l_k \leq L_k, \ \ \forall k \in \mathcal{K}/\mathcal{J}, \tag{15e}$$

$$f_k \leq f_k^{max} \ \ \forall k \in \mathcal{K}/\mathcal{J}, \tag{15f}$$

where $\mathbf{f} = [f_{|\mathcal{J}|+1}, ..., f_K]$, $\mathbf{l} = [l_{|\mathcal{J}|+1}, ..., l_K]$, $\mathbf{R}_s = [R_{s,|\mathcal{J}|+1}, ..., R_{s,K}]$ and $\mathbf{p} = [p_1, p_2, ..., p_K]$ denote the CPU frequency vector, offloading bit vector, secrecy offloading rate vector (all for offloading UAVs), and transmit power vector (for all UAVs), respectively.

The first term in (15a) denotes the total energy consumption of the offloading UAVs, while the second term represents that of the jamming UAVs.

4.2 Latency-Efficient Problem Formulation

We next formulate the task computation latency problem for UAV U_k over the offloading power p_k, offloading bits l_k, secrecy offloading rate $R_{s,k}$, and CPU frequency f_k under the constraint of a specific energy budget.

The problem is formulated as follows

$$\mathbf{P3}: \min_{f_k, l_k, R_{s,k}, p_k} \max\left(t_k^{loc}, t_k^{off}\right) \tag{16a}$$

$$s.t.\ \ \kappa_k(L_k - l_k)X_k f_k^2 + p_k \frac{l_k}{BR_{s,k}} \leq E_k^{bu}, \tag{16b}$$

$$P_{so,k}^{(\mathcal{J})}(K-k, R_{s,k}) \leq \epsilon, \tag{16c}$$

$$0 \leq l_k \leq L_k, \tag{16d}$$

$$f_k \leq f_k^{max} \tag{16e}$$

where $t_k^{loc} = (L_k - l_k)X_k/f_k$ and $t_k^{off} = l_k/(BR_{s,k})$ according to the definitions in Section 3, and E_k^{bu} refers to the energy budget of UAV U_k for its task.

4.3 Special Cases

4.3.1 Zero Offloading Mode

Zero offloading mode implies the computation are done locally. In this case, the energy consumption and computing duration for UAV U_k are $\kappa_k X_k^3 L_k^3/T^2$ and $L_k X_k/f_k$ by setting $l_k = 0$, respectively. However, the zero offloading mode is not always achievable unless $f_k^{max} \geq L_k X_k/T$ and $T \geq (\kappa_k X_k^3 L_k^3/E_k^{bu})^{1/2}$ are satisfied.

4.3.2 Full Offloading Mode

Similarly, the full offloading mode is not always feasible. This is because, given the SOP requirement, each UAV U_k has a corresponding asymptotic ϵ-outage secrecy capacity, which is explained by the following lemma

Lemma 1 *Given the SOP of ϵ, the limited value of secrecy rate $R_{s,k}$, i.e., asymptotic ϵ-outage secrecy capacity, for UAV U_k in the presence of n co-channel interferers satisfies*

$$\frac{\beta_k^{N-n}}{(N-n-1)!} \sum_{i \in \mathcal{J}} a_i \Phi(\mu_i, \beta_k, R_s) = \epsilon \tag{17}$$

where $\lambda_k/\mu_k = \beta_k$ and

$$\Phi(\mu_i, \beta_k, R_s) = e^{\mu_i(1+2^{R_s}\beta_k)} \sum_{m=0}^{N-n-1} \binom{N-n-1}{m} (-1)^{N-n-m-1} (2^{R_s})^{N-n} (\mu_i)^{N-n-m} \frac{\Gamma(m, \mu_i(1+2^{R_s}\beta_k))}{(1+2^{R_s}\beta_k)^m}. \tag{18}$$

Proof The asymptotic ϵ-outage secrecy capacity is achieved when the offloading power approaches to infinity, i.e., $\lim_{p_k\to\infty} P_{so,k}^{(\mathcal{J})}(n, C_{s,k}^{(\mathcal{J})}(\epsilon)) = \epsilon$.

According to the definitions of λ_k and μ_k in Section 3, we have $\lambda_k \to 0$ and $\mu_k \to 0$ when $P_k \to \infty$, while the ratio β_k is fixed.

As $\lambda_k \to 0$, $\boldsymbol{\gamma}(N-n, \lambda_k(2^{R_s}-1)) \to 0$ and $e^{\lambda_k(1-2^{R_s})} \to 1$ are satisfied. The asymptotic secrecy outage probability is reduced to

$$\lim_{p_k\to\infty} P_{so,k}^{(\mathcal{J})}(n, R_s) = \frac{\lambda_k^{N-n}}{(N-n-1)!} \sum_{i\in\mathcal{J}} a_i \Theta(\mu_i) \tag{19}$$

Since λ_k^{N-n} has the power of $N-n$, the items containing $1/\mu_k^{N-n}$ in $\Theta(\mu_i)$ less than $(N-n)$th power are eliminated, obtaining

$$\lim_{p_k\to\infty} \lambda_k^{N-n}\Theta(\mu_i) = (\frac{\lambda_k}{\mu_k})^{N-n} e^{\mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k})} \sum_{m=0}^{N-n-1} \binom{N-n-1}{m} (-1)^{N-n-m-1} (2^{R_s})^{N-n} (\mu_i)^{N-n-m} \times \frac{\Gamma(m, \mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k}))}{(1+2^{R_s}\frac{\lambda_k}{\mu_k})^m}. \tag{20}$$

After replacing λ_k/μ_k with β_k and substituting (20) into (19), we have

$$\lim_{p_k\to\infty} P_{so,k}^{(\mathcal{J})}(n, R_s) = \frac{\beta_k^{N-n}}{(N-n-1)!} \sum_{i\in\mathcal{J}} a_i \Phi(\mu_i, \beta_k, R_s) \tag{21}$$

The proof is done. □

5 Suboptimal Solutions

The problems outlined in Section 4 are both complex and non-convex, with their non-convexity attributed to the inherent non-convexity of the associated constraints. Given that closed-form expressions for the optimal solutions cannot be derived, we obtain suboptimal solutions through a numerical procedure consisting of the following steps: 1) simplifying the constraints to mitigate problem intractability; 2) relaxing and transforming the multi-variable optimization problems into solvable single-variable counterparts; 3) computing the required solutions using numerical methods.

5.1 Solution To Problem P1

We first simplify the constraints of the problem by the following lemma.

Lemma 2 *The constraint (14b) and (14d) are strictly binding for the optimal solution to Problem* **P1**, *i.e.,*

$$f_k = \frac{(L_k - l_k)X_k}{T}, \tag{22}$$

$$P_{so,k}^{(\mathcal{J})}\left(K-k, R_{s,k}\right) = \epsilon. \tag{23}$$

Proof Observing the first term in (14a), 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, $P_{so,k}^{(\mathcal{J})}\left(n, R_{s,k}\right)$ is an increasing function of $R_{s,k}$. The maximum $R_{s,k}$ that satisfies (14d) is the ϵ-outage secrecy capacity $C_{s,k}^{(\mathcal{J})}(\epsilon)$ which makes $P_{so,k}^{(\mathcal{J})}\left(n, C_{s,k}^{(\mathcal{J})}(\epsilon)\right) = \epsilon$ hold. This completes the proof. □

The problem **P1** is still complex and non-convex. We continue to transform the problem by relaxing offloading duration with T, i.e.,

$$\mathbf{P1.1}: \min_{l_k, p_k, R_{s,k}} \left(\frac{\kappa_k X_k^3 (L_k - l_k)^3}{T^2} + p_k T\right) \tag{24a}$$

$$s.t. \;\; R_{s,k} \geq \frac{l_k}{BT}, \tag{24b}$$

$$P_{so,k}^{(\mathcal{J})}\left(K-k, R_{s,k}\right) = \epsilon, \tag{24c}$$

$$\left[L_k - \frac{T f_k^{max}}{X_k}\right]^+ \leq l_k \leq L_k, \tag{24d}$$

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

Since the offloading 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 (24c). As such, we can further transform the problem into the one only having a single variable.

$$\mathbf{P1.2}: \min_{l_k} \left(\frac{\kappa_k X_k^3 (L_k - l_k)^3}{T^2} + P_k(K-k, p_1, ..., p_{|\mathcal{J}|}, \frac{l_k}{BT})T\right) \tag{25a}$$

$$s.t. \;\; \left[L_k - \frac{T f_k^{max}}{X_k}\right]^+ \leq l_k \leq L_k, \tag{25b}$$

where $P_k(n, ..., R_{s,k})$ is the expression of the function of the number of interferers, the jamming power, and the secrecy rate, for p_k, derived from $P_{so,k}^{(\mathcal{J})}\left(n, R_{s,k}\right) = \epsilon$.

Although we cannot get a closed-form solution to this problem, the suboptimal 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 UAV over offloading bit l_k independently. We will demonstrate it numerically in detail in Section 6.

5.2 Solution To Problem P2

Similar to the solution to problem **P1**, by applying Lemma 2 and relaxing the offloading and jamming durations with T, the problem **P2** is transformed into the following

Algorithm 1 Numerical solution to problem **P1**

setting: T, B, ϵ, N, K, M, α, N_a, N_e;
setting: f_k^{max}, κ_k, X_k, L_k, $d_{a,k}$;
initialization: δ_k^2;
repeat
    setting: $d_{e,j}$, p_j;
    initialization: σ_j^2, μ_j;
until $j = |\mathcal{J}|$
initialization: l_k;
repeat
    repeat
        Search p_k with certain l_k via constraint of (24c);
    until SOP converges to ϵ within a prescribed accuracy;
    Calculate $E_k^{loc} + E_k^{off}$;
until $l_k = L_k$
Search l_k^* to make $E_k^{loc} + E_k^{off}$ the least;
Calculate f_k^*, $R_{s,k}^*$, p_k^*;
output: l_k^*, f_k^*, $R_{s,k}^*$, p_k^*;

one,

$$\mathbf{P2.1}: \min_{\mathbf{l},\mathbf{p}} \sum_{k=|\mathcal{J}|+1}^{K} \frac{\kappa_k X_k^3 (L_k - l_k)^3}{T^2} + \sum_{k=|\mathcal{J}|+1}^{K} P_k(K-k, p_1, ..., p_{|\mathcal{J}|}, \frac{l_k}{BT})T + \sum_{j=1}^{|\mathcal{J}|} p_j T \tag{26a}$$

$$s.t. \quad \left[L_k - \frac{T f_k^{max}}{X_k}\right]^+ \leq l_k \leq L_k, \quad \forall k \in \mathcal{K}/\mathcal{J}, \tag{26b}$$

where $\mathbf{l} = [l_{|\mathcal{J}|+1}, ..., l_K]$ and $\mathbf{p} = [p_1, ..., p_{|\mathcal{J}|}]$, and the definition of $P_k(n, ..., R_{s,k})$ is the same as above, derived from $P_{so,k}^{(\mathcal{J})}(n, R_{s,k}) = \epsilon$.

By fixing the jamming power $p_1, p_2, ..., p_{|\mathcal{J}|}$, problem **P2.1** is transformed into the one with a single variable. As such, we can obtain the optimal solution for certain jamming power numerically. Finally, we can use the exhaustive search method for all possible $p_1, p_2, ..., p_{|\mathcal{J}|}$ to figure out the ultimate optimal solution. The numerical solution to problem **P2.1** is shown in Algorithm 2.

5.3 Solution To Problem P3

Before solving problem **P3** numerically, we need to simplify the problem via the following lemma.

Lemma 3 *The optimal solution of the variables f_k, l_k, $R_{s,k}$ and p_k should make $t_k^{loc} = t_k^{off}$.*

Algorithm 2 Numerical solution to problem **P2**

setting: T, B, ϵ, N, K, α, N_a, N_e;
repeat
  setting: $d_{e,j}$;
  initialization: σ_j^2;
until $j = |\mathcal{J}|$
repeat
  initialization: p_1, p_2,..., $p_{|\mathcal{J}|}$;
  repeat
    setting: f_k^{max}, κ_k, X_k, L_k, $d_{a,k}$;
    initialization: δ_k^2, l_k;
    repeat
      repeat
        Search p_k with certain l_k via constraint of (24c);
      until SOP converges to ϵ within a prescribed accuracy;
      Calculate $E_k^{loc} + E_k^{off}$;
    until $l_k = L_k$
  until $k = K$
until p_1, p_2,..., $p_{|\mathcal{J}|}$ exhaustively searched
Find out p_1^*, p_2^*,..., $p_{|\mathcal{J}|}^*$, and $l_{|\mathcal{J}|+1}^*$,..., l_K^* to make the sum energy consumption the least
repeat
  Calculate f_k^*, $R_{s,k}^*$, p_k^*;
  output: l_k^*, f_k^*, $R_{s,k}^*$, p_k^*;
until $k = K$

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 $\left\{f_k^*, l_k^{'}, R_{s,k}^*, p_k^*\right\}$, where $l_k^{'} = l_k^* - \tau_k$ and τ_k is a small positive value, making $(L_k - l_k^{'})X_k/f_k^* \leq l_k^{'}/(BR_{s,k}^*)$. Similarly, if $(L_k - l_k^*)X_k/f_k^* > l_k^*/(BR_{s,k}^*)$ is supposed, there exists another $\left\{f_k^*, l_k^{''}, R_{s,k}^*, p_k^*\right\}$ that makes $(L_k - l_k^{''})X_k/f_k^* \geq l_k^{''}/(BR_{s,k}^*)$ hold, where $l_k^{''} = l_k^* + \tau_k$. We complete the proof. □

Combined with Lemma 2 and Lemma 3, we transform the problem **P3** into the following form.

$$\mathbf{P3.1}: \min_{l_k} \ T_k \tag{27a}$$

$$s.t. \ \frac{\kappa_k X_k^3 (L_k - l_k)^3}{T_k^2} + P_k(K\text{–}k, p_1, ..., p_{|\mathcal{J}|}, \frac{l_k}{BT})T_k \leq E_k^{bu}, \tag{27b}$$

$$\left[L_k - \frac{T_k f_k^{max}}{X_k}\right]^+ \leq l_k \leq L_k, \tag{27c}$$

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 3.

Algorithm 3 Numerical solution to problem **P3**

setting: B, ϵ, N, K, α, N_a, N_e;
setting: f_k^{max}, κ_k, X_k, L_k, $d_{a,k}$, E_k^{bu};
initialization: δ_k^2;
repeat
    setting: $d_{e,j}$, p_j;
    initialization: σ_j^2, μ_j;
until $j = |\mathcal{J}|$
initialization: l_k, T_k;
repeat
    repeat
        repeat
            Search p_k with certain l_k and T_k via constraint of (16c);
        until SOP converges to ϵ within a prescribed accuracy;
        Calculate $E_k^{loc} + E_k^{off}$;
    until T_k satisfies the condition in (27b)
until $l_k = L_k$
Search l_k^* to make T_k the least;
Calculate f_k^*, $R_{s,k}^*$, p_k^*;
output: l_k^*, f_k^*, $R_{s,k}^*$, p_k^*;

5.4 Computational Complexity

Observing Algorithm 1, there roughly exist thress 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 offloading power and search optimal offloading power with certain l_k; 3) Calculate individual energy consumption and search for the optimal l_k to achieve minimum individual energy consumption. Therefore, the computational complexity is $O(m^3)$.[1]

Different from Algorithm 1, Algorithm 2 has two more nesting steps in the process of numerical-finding: 1) Loop from $U_{|\mathcal{J}|+1}$ to U_K; 2) Exhaustively search with variable jamming power. Therefore, the computational complexity of Algorithm 2 is $O(m^5)$.

While Algorithm 3 has only one more nesting step, compared with Algorithm 1, by including: Search for the minimum T_k for the fixed l_k, which makes its computational complexity be $O(m^4)$.

[1] Here m refers to the computational complexity of the SOP.

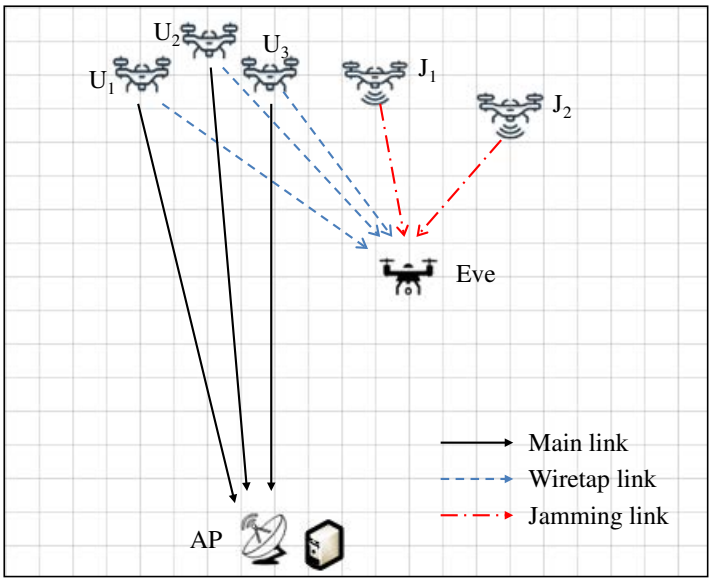


Fig. 2 A 5-UAV scenario of secure cooperative UAV-NOMA-enabled MEC network.

6 Results

In this section, we evaluate the performance of the proposed energy- and latency-efficient computation offloading strategies for this secure cooperative UAV-NOMA-enabled MEC network.

A 5-UAV scenario is adopted as an example, where 3 UAVs perform offloading tasks and 2 UAVs act as jammers. For clarity, all nodes are mapped onto a two-dimensional plane, as depicted in Fig. 2. Each grid in the plane represents 50 meters; based on this layout, the distance from U_1 to the AP is approximately 667 meters, and its distance to Eve is 500 meters. Using this method, all distances between UAVs and the AP, as well as between UAVs and Eve, are calculated and summarized in Tab. 2. According to the relative distances (i.e., the distance between each UAV and the AP versus the distance between the same UAV and Eve), the SIC order is set as $U_1 \to U_2 \to U_3$.

We further make the following assumptions: 1) the AP is equipped with 10 antennas, i.e., $N = 10$; 2) the bandwidth for each link is 100 MHz, i.e., $B = 100$; 3) the path loss in dB is given by $PL = 10\alpha \lg(d) + 43.5$, where the path loss exponent α is set to 2.1 in accordance with 3GPP line-of-sight path loss model; 4) the AP and Eve have the same the AWGN power spectral density , i.e., $N_0 = -160$ dBm/Hz, leading to $N_a = N_e = -80$ dBm; 5) all UAVs have identical performance and process the same task: the computation intensity is $X_1 = X_2 = X_3 = 10$ cycles/bit, the maximum CPU frequency is 2 GHz, the effective capacitance coefficient is set as $\kappa_1 = \kappa_2 = \kappa_3 = 10^{-28}$, and the total number of task bits for each UAV is $L_1 = L_2 = L_3 = 25$ Mbits.

Table 2 Distances between each UAV and AP as well as Eve.

Distance (meters)	U_1	U_2	U_3	J_1	J_2
AP	667	701.78	651.92	-	-
Eve	500	460.98	324.04	304.14	291.55

6.1 Energy-Efficient Computation

6.1.1 Individual Energy Consumption Minimization

Fig. 3 presents the individual energy consumption of each UAV against offloading bits (in Mbits), Each curve starts from the same initial value and exhibits a trend of first decreasing and then increasing as the offloading bits increase. In addition to the assumptions specified in the previous subsection, the following parameters are assumed herein: a latency deadline $T = 0.25$ s, a secrecy outage probability $\epsilon = 0.2$, and a jamming power $P_j = 10$ mW (per jamming UAV).

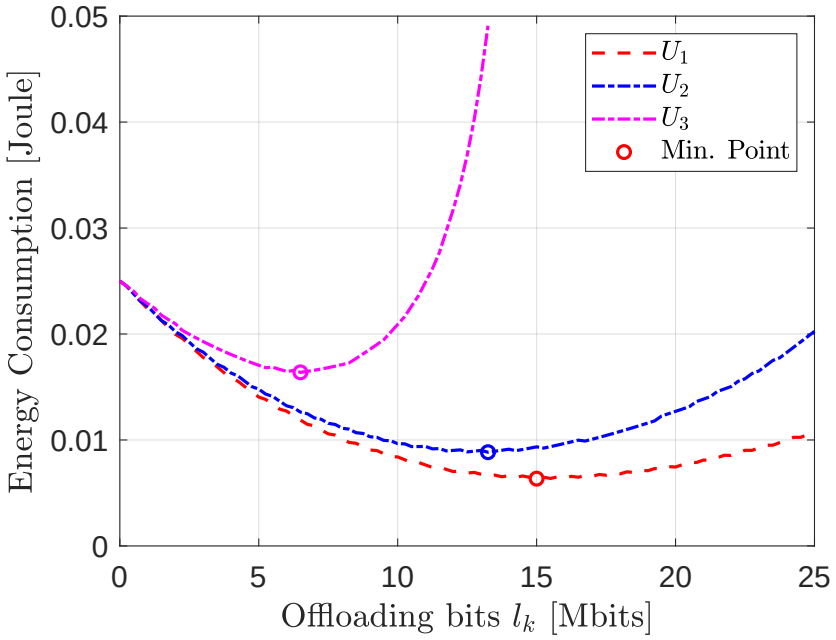


Fig. 3 Energy consumption versus offloading bits for individual at the assumption of $T = 0.25$ s, $\epsilon = 0.2$, and $P_j = 10$ mW each.

Note that $l_k = 0$ and $l_k = 25$ Mbits correspond to zero-offloading mode and full-offloading mode, respectively. At $l_k = 0$, each UAV has the same local computing energy consumption of 0.025 Joule, which is attributed to the assumption of identical UAV performance. However, only U_1 and U_2 can operate in the full-offloading mode; U_3 cannot do so because its ϵ-secrecy outage capacity is insufficient to complete the

transmission of 25 Mbits of data within the latency deadline $T = 0.25$ s. The asymptotic ϵ-secrecy outage capacities are $C_{s,1}^{(0)}(\epsilon = 0.2) = 2.22$ bps/Hz, $C_{s,2}^{(1)}(\epsilon = 0.2) = 1.66$ bps/Hz, $C_{s,3}^{(2)}(\epsilon = 0.2) = 0.63$ bps/Hz. The corresponding asymptotic offloading bits within $T = 0.25$ s are 55.5 Mbits, 41.5 Mbits, and 15.75 Mbits, respectively, which verifies full offloading mode is not available for U_3.

U_1, U_2, and U_3 achieve their minimum energy consumptions of 0.0064 Joule, 0.0088 Joule, and 0.0164 Joule, in the partial offloading mode, with the offloading bits of 15 Mbits, 13.25 Mbits, and 6.5 Mbits, i.e., $l_1^* = 15$ Mbits, $l_2^* = 13.25$ Mbits, $l_3^* = 6.5$ Mbits, respectively. In turn, we have $f_1^* = 400$ MHz, $f_2^* = 470$ MHz, $f_3^* = 740$ MHz; $R_{s,1}^* = 0.6$ bps/Hz, $R_{s,2}^* = 0.53$ bps/Hz, $R_{s,3}^* = 0.26$ bps/Hz; $p_1^* = 19$ mW, $p_2^* = 25$ mW, $p_3^* = 25$ mW. Here, the resolution of offloading bits and offloading power are 0.25 Mbits and 1 mW, respectively.

6.1.2 Impacts of T and ϵ

In this part, we demonstrate how the latency T and the secrecy outage probability ϵ impact on the individual and overall energy consumptions.

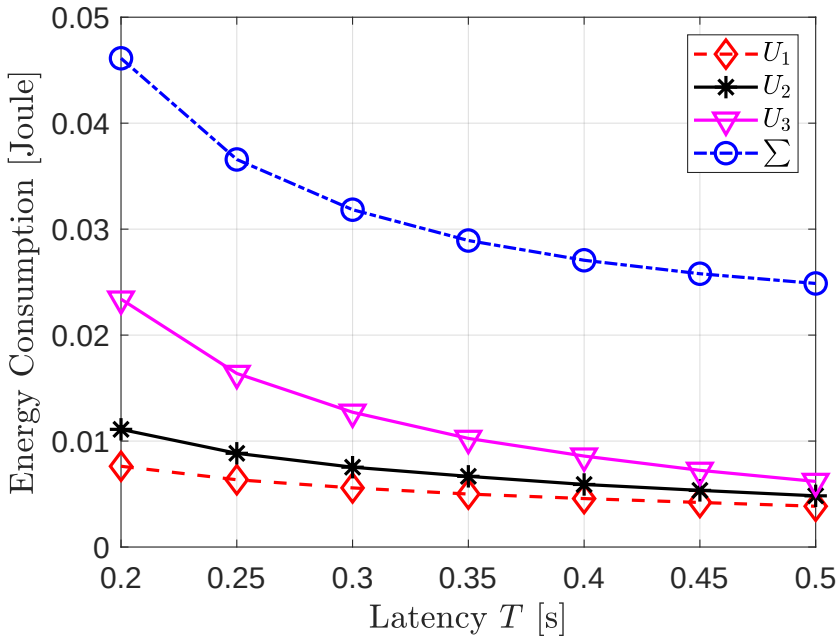


Fig. 4 Minimum energy consumption versus latency for individual and overall from $T = 0.2$ s to $T = 0.5$ s.

The minimum energy consumptions versus latency from $T = 0.2$ s to $T = 0.5$ s for each UAV are shown in Fig. 4. Here, the secrecy outage probability $\epsilon = 0.2$, and jamming power (from each jamming UAV) $P_j = 10$ mW are still assumed. We note the minimum energy consumption for individual and overall decreases by increasing

T. At $T = 0.2$ s, the minimum energy consumptions for U_1, U_2, U_3, and overall are 0.0.0076 Joule, 0.0111 Joule, 0.0234 Joule, and 0.0461 Joule, respectively, while they are reduced to 0.0039 Joule, 0.0048 Joule, 0.0062 Joule, ad 0.0249 Joule at $T = 0.5$ s. The minimum values for U_1, U_2 and U_3 at $T = 0.25$ s are 0.0064 Joule, 0.0088 Joule, and 0.0164 Joule, respectively, the same as those achieved in Fig. 3, which also confirms the reliability of the numerical results in Fig. 4. As expected, U_1 has the least energy consumptions for the same T, while U_3 needs more energy consumption than other two UAVs, to complete the similar task, just as in Fig. 3.

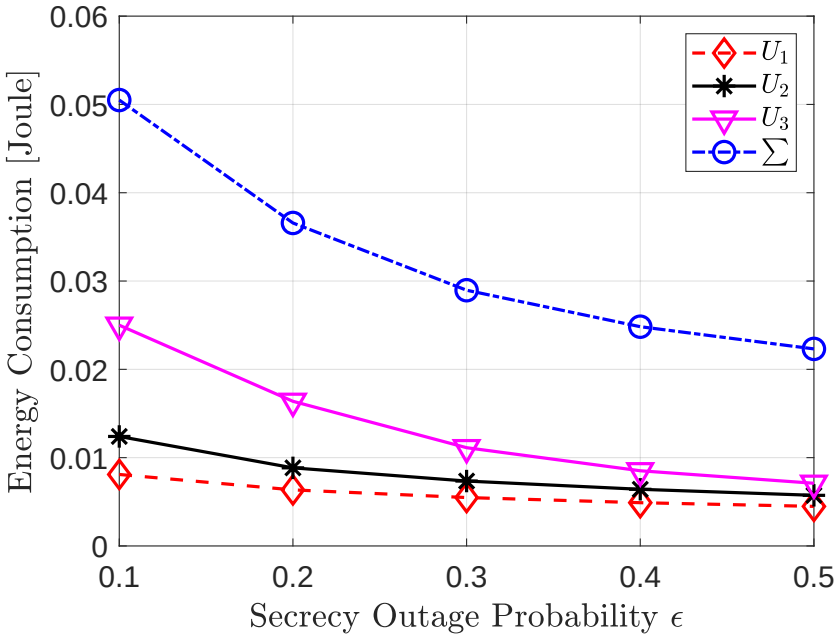


Fig. 5 Minimum energy consumption versus secrecy outage probability for each UAV and their sum from $\epsilon = 0.1$ to $\epsilon = 0.5$.

Fig. 5 shows the relationship between minimum energy consumptions and secrecy outage probability for each UAV and overall from $\epsilon = 0.1$ to $\epsilon = 0.5$, at the jamming power of 10 mW each. The minimum energy consumptions decline with the increase in secrecy outage probability, from 0.0081 Joule, 0.0124 Joule, 0.0250 Joule, 0.0505 Joule at $\epsilon = 0.1$ to 0.0055 Joule, 0.0074 Joule, 0.0111 Joule, 0.0290 Joule at $\epsilon = 0.3$ to 0.045 Joule, 0.0057 Joule, 0.0071 Joule, 0.0223 Joule at $\epsilon = 0.5$. We can also verify the reliability of the numerical results in Fig. 5 by observing the values at $\epsilon = 0.2$ which is the same as that in Fig. 3. We note the minimum energy consumption for U_3 at $\epsilon = 0.1$ is 0.025, which is just local computing only energy consumption. It implies zero offloading mode is much better to achieve minimum energy consumption.

6.1.3 Overall Energy Consumption Minimization

In the above, we focus on how to minimize individual energy consumption as well as the impacts from latency and secrecy outage probability. We next shift to study the impact of jamming power on the overall energy consumption.

Fig. 6 shows the minimum values of overall energy consumption versus jamming power for different requirements of latency, where the curves are convex and have the extreme values, similar to the above. At the requirement of $T = 0.2$ s, the jamming power of 25 mW each achieves the least overall energy consumption of 0.041 Joule at the side of UAVs (including jammers) for this NOMA MEC network. For the requirements of $T = 0.25$ and $T = 0.3$, the optimal points of jamming power are 15 mW and 10 mW, achieving the least overall energy consumptions of 0.036 Joule and 0.032 Joule, respectively. Here, the resolution of jamming power is 0.5 mW, and $\epsilon = 0.2$ is still supposed. As expected, the overall energy consumptions as well as their least values decrease with T increasing. We also note the impact of T are narrowed with the increase of jamming power. At the jamming power of $P_j = 30$ mW, the minimum values of overall energy consumption for $T = 0.25$ s and $T = 0.3$ s are very close to each other.

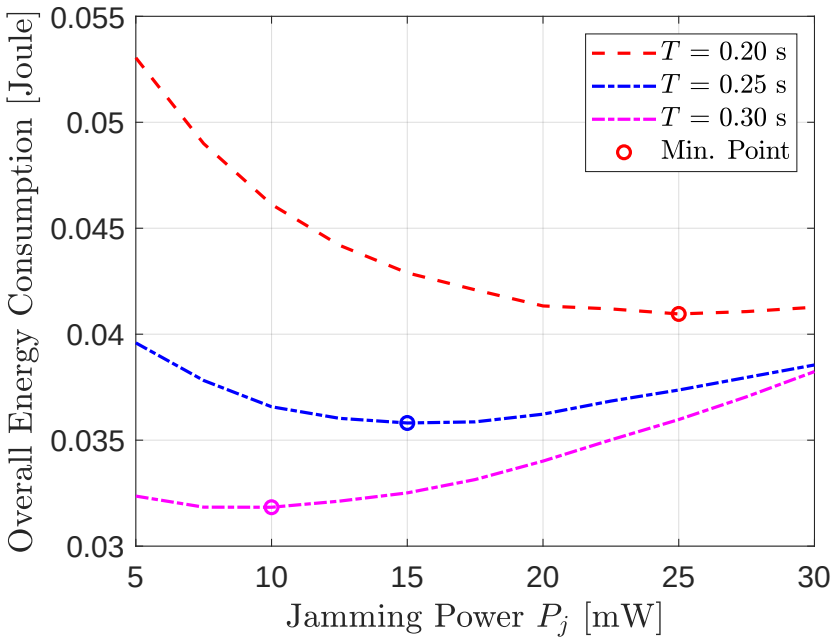


Fig. 6 Minimum values of overall energy consumption versus jamming power for different T at $\epsilon = 0.2$.

6.2 Latency-Efficient Computation

6.2.1 Latency Minimization

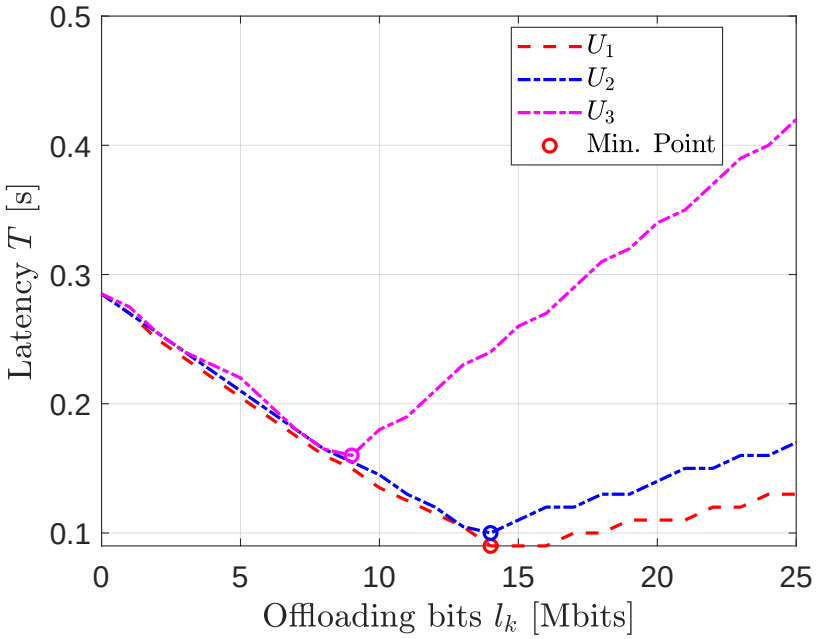


Fig. 7 Latency versus offloading bits for each UAV at the assumption of $E^{bu} = 0.025$ Joule and $\epsilon = 0.2$.

Fig. 7 illustrates the latency of the three UAVs against offloading bits, under the constraints of an energy budget $E^{bu} = 0.025$ Joule (encompassing energy consumption from jammers), with the assumptions that the secrecy outage probability is 0.2 and each jammer has a jamming power of 10 mW. The resolutions for latency T and offloading bits l_k are 5 ms and 1 Mbits, respectively. Each curve first decreases and then increases with the rise in offloading bits, allowing the minimum latency values to be derived. Specifically, the optimal offloading bits for U_1, U_2, and U_3 are 14 Mbits, 14 Mbits, and 9 Mbits, corresponding to minimum latencies of 90 ms, 100 ms, and 160 ms, respectively. With these optimal offloading bits ($l_1^* = 14$ Mbits, $l_2^* = 14$ Mbits, $l_3^* = 9$ Mbits) and minimum latencies ($T_1^* = 90$ ms, $T_2^* = 100$ ms, $T_3^* = 160$ ms), we further obtain the optimal solutions to the problem: $f_1^* = 1222.2$ MHz, $f_2^* = 1100$ MHz, $f_3^* = 1000$ MHz; $R_{s,1}^* = 1.56$ bps/Hz, $R_{s,2}^* = 1.4$ bps/Hz, $R_{s,3}^* = 0.56$ bps/Hz; and $p_1^* = 123$ mW, $p_2^* = 284$ mW, $p_3^* = 291$ mW.

6.2.2 Impact of Energy Budget

In Fig. 8, we present the curves depicting the relationship between minimum latency and energy budget (ranging from 0.02 Joule to 0.1 Joule) for each UAV. It is observed

that as the energy budget increases, the minimum latency of all UAVs decreases. Notably, this decreasing trend is more pronounced for U_3 compared to the other two UAVs: when the energy budget rises from 0.02 Joule to 0.06 Joule, the minimum latency of U_3 drops significantly from 165 ms to 110 ms. When the energy budget is further increased from 0.06 Joule to 0.1 Joule, the minimum latency of U_1 and U_2 exhibits little variation, whereas that of U_3 continues to decrease, falling from 110 ms to 90 ms.

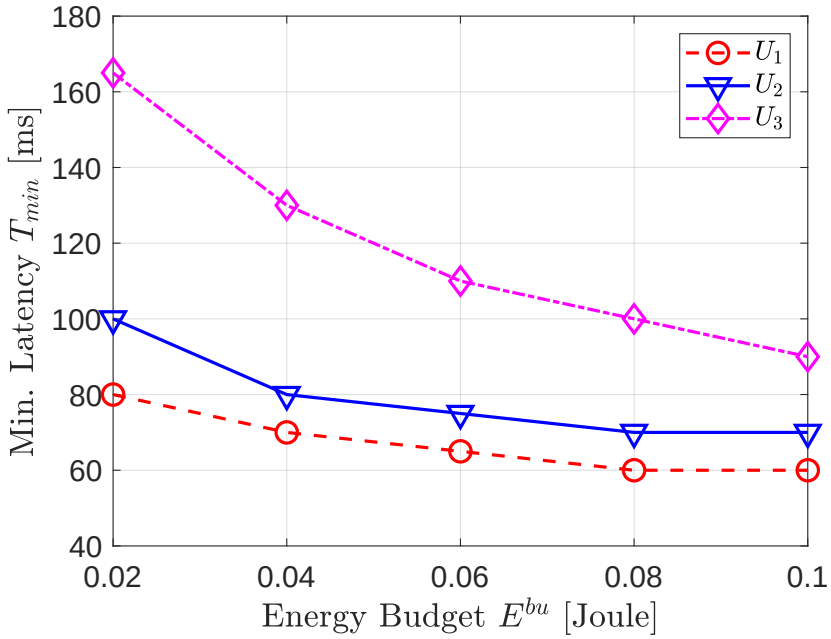


Fig. 8 Minimum latency versus energy budget for each UAV from $E^{bu} = 0.02$ Joule to $E^{bu} = 0.1$ Joule.

Up to this point, all the numerical results and observations presented in this section are consistent with our expectations.

7 Discussion

We admit the study has the following limitations:

- Static Network Assumption: This study assumes that UAVs are in hovering state (fixed 3D position) during task offloading, and the wireless channel is subject to quasi-static Rayleigh fading. In practical scenarios, UAVs often need to move dynamically to adapt to changing network topologies, and dynamic mobility will lead to time-varying channel conditions and NOMA interference, which may make the fixed offloading bit ratio and jamming power derived in this study suboptimal.

- Simplification of Latency and Energy Components: The study neglects two key latency components: MEC server data processing latency and downlink transmission latency from AP to UAVs. Although this simplification is reasonable under the assumption of high-performance MEC servers and small result data volume, in some dense IoT deployments, MEC servers face massive task offloading requests, and their processing latency will increase significantly.
- Fixed SIC Decoding Order and Jammer Assignment: The study sets a fixed SIC decoding order for offloading UAVs based on their relative distances to the AP and eavesdropper, and a fixed subset of UAVs is designated as jammers. In some scenarios, the optimal SIC decoding order of NOMA is closely related to UAV channel conditions and offloading power, and dynamic adjustment of the decoding order can further improve spectral efficiency and energy efficiency.
- Single Eavesdropper Scenario: The study only considers a single passive eavesdropper in the network, while practical UAV-NOMA-MEC networks may face multiple eavesdroppers with different positions and channel conditions.

Based on the above limitations, the key directions for future research are proposed as follows:

- Dynamic UAV mobility and trajectory optimization: Integrate UAV flight energy consumption and dynamic channel conditions into the optimization model, and jointly optimize UAV trajectory, offloading strategy, and jamming power to adapt to time-varying network topologies.
- Full network energy/latency optimization: Extend the optimization objective from UAV-side energy consumption to the total energy consumption of the entire network (including AP and MEC server), and consider MEC server processing latency and downlink transmission latency to build a more comprehensive latency model.
- Adaptive SIC decoding and jammer selection: Design dynamic SIC decoding order adjustment algorithms based on real-time channel conditions and offloading power, and develop adaptive jammer selection schemes for multiple eavesdropper scenarios to improve the flexibility and security of the network.
- Multi-eavesdropper and active attack defense: Extend the single passive eavesdropper model to multiple eavesdropper scenarios, and consider active jamming attacks from malicious nodes; design joint anti-eavesdropping and anti-jamming strategies by combining cooperative jamming with beamforming or trajectory optimization.
- Integration with emerging intelligent technologies: Combine the proposed offloading strategy with federated learning, reinforcement learning, and blockchain to design adaptive and secure resource allocation algorithms for UAV-NOMA-MEC networks, and explore the application of these technologies in energy- and latency-constrained UAV scenarios.

Despite the above limitations, this study provides important practical engineering implications for the deployment of secure UAV-NOMA-MEC networks:

- Partial offloading as a default strategy: For UAVs with strict energy and latency constraints, partial offloading with an optimal offloading bit ratio should be adopted instead of full/zero offloading, and the optimal offloading ratio can be pre-calculated

according to UAV channel conditions and task requirements (e.g., latency deadline, SOP threshold) using the numerical method proposed in this study.

- Optimal jamming power configuration: In cooperative jamming UAV networks, the jamming power should be configured according to the latency requirement of the task—higher latency deadlines allow lower jamming power, and vice versa—avoiding over-jamming or under-jamming to achieve energy-saving and secure offloading.
- Parameter tuning for performance improvement: For UAVs with weaker channel conditions, appropriately relaxing the SOP threshold (within the security requirements of the application) or increasing the energy budget can significantly improve their offloading performance; expanding the latency deadline is also an effective way to reduce energy consumption for non-latency-critical applications.
- Lightweight optimization for real-time deployment: The proposed suboptimal solution framework with low computational complexity is suitable for real-time resource allocation of resource-constrained UAVs, and can be implemented on UAV on-board computers with simple numerical calculation modules, without the need for complex intelligent algorithm training.

In summary, this study establishes a theoretical and methodological foundation for energy- and latency-efficient secure offloading in UAV-NOMA-MEC networks, and its findings and limitations provide clear guidance for the follow-up research and practical deployment of this emerging network paradigm.

8 Conclusion

We have investigated energy- and latency-efficient computational offloading for this secure cooperative UAV-NOMA-enabled MEC network in the presence of an eavesdropper, where a cluster of UAVs act as jammers to assist in achieving secure offloading for the remaining UAVs. The system is modeled with partial offloading, incorporating the secrecy metric of secrecy outage probability. First, the closed-form expression for the individual secrecy outage probability under jamming conditions is derived. Subsequently, we formulate two optimization problems focused on energy-efficient and latency-efficient computational offloading, respectively; these problems are non-trivial due to the non-convexity of their constraints. To address this, the original optimization problems are converted into suboptimal counterparts through three steps: 1) simplifying and relaxing the constraints; 2) transforming multiple variables into a single variable; 3) providing numerical solutions. In turn, the algorithms for solving these suboptimal problems, along with their computational complexities, are presented and elaborated. Finally, we validate the suboptimal solutions to these problems via a suitable numerical case.

List of Abbreviations

- UAV: Unmanned Aerial Vehicle
- MEC: Multi-access Edge Computing
- NOMA: Non-Orthogonal Multiple Access
- SIC: Successive Interference Cancellation

- IoT: Internet of Thing
- AR: Augmented Reality
- UHD: Ultra-High Definition
- QoS: Quality of Service
- BS: Base Station
- RSU: Road-Side Unit
- OMA: Orthogonal Multiple Access
- LoS: Line-of-Sight
- PLS: Physical-Layer Security
- FL: Federated Learning
- DDQN: Double Deep Q-Network
- DVFS: Dynamic Voltage and Frequency Scaling
- SOP: Secrecy Outage Probability
- AP: Access Point
- SINR: Signal-to-Interference-plus-Noise Ratio
- CSI: Channel State Information
- CPU: Central Process Unit
- ZF: Zero Forcing
- PDF: Probability Distribution Function
- CDF: Cumulative Distribution Function

Declarations

- Funding
  This work was supported in part by the Natural Science Foundation of Zhejiang Province (Grant No. Y202147949), in part by the Higher Vocational Education Teaching Reform Projects of Zhejiang Province (Grant No. jg20240246).
- Competing interests
  The author declares no conflict of interest.
- Data availability:
  The data used to support the findings of this work are available from the corresponding author upon request.
- Materials availability:
  The materials used to support the findings of this work are available from the corresponding author upon request.
- Code availability:
  The code used to support the findings of this work is available from the corresponding author upon request.
- Author contribution:
  Kaiwei Jiang conceived the idea of system model, designed the proposed schemes, performed simulation of the proposed schemes, and finished the work all by himself.
- Acknowledgements:
  We sincerely thank the Reviewers and the Editor for their valuable suggestions.
- Author Information:

Kaiwei Jiang was born in Linhai, Zhejiang Province, China in 1981. He received the B.S. degree from Northeast University, China, in 2004 and the M.S. degree from Beijing Jiaotong University, in 2007. From 2007 to 2011, he worked as a Software Engineer with Mediatek. He has been a faculty Member with the school of Mechanical and Electrical Engineering, Taizhou Vocational and Technical College, since 2011. He received the Ph.D. degree in 2018 with Shu Hua Wireless Network and Information Perception Center, Beijing Jiaotong University. His research interests are cognitive radio networks, wireless sensor networks and physical layer security.

Appendix A

Consider independent exponential random variables $\xi_0, \xi_1, \xi_2, ..., \xi_n$ with $\xi_i \sim \text{Exp}(\mu_i)$ for $i = 0, ..., n$ and distinct parameters $(\mu_i \neq \mu_j, \forall i \neq j)$. Define $Y_n = \sum_{i=1}^{n} \xi_i$, where ξ_0 and Y_n are independent.

The CDF of the random variable $Z_n = \frac{\xi_0}{1+Y_n}$ is then given by

$$\begin{aligned} F_{Z_n}(z) &= \int_0^\infty \int_0^{zy+z} f_{Y_n}(y) f_{\xi_0}(\xi) d\xi dy \\ &= \int_0^\infty f_{Y_n}(y) F_{\xi_0}(zy+z) dy \\ &= 1 - \underbrace{\int_0^\infty f_{Y_n}(y) e^{-\mu_0(zy+z)} dy}_{L_1}, \end{aligned} \tag{A1}$$

where,

$$F_{\xi_0}(\xi) = 1 - e^{-\mu_0 \xi}, \xi \geq 0 \tag{A2}$$

The PDF of the Y_n is derived in [34],

$$f_{Y_n}(y) = f_1(y) \prod_{i=1}^{n} \mu_i, y > 0 \tag{A3}$$

where

$$f_1(y) = \frac{\exp(-\mu_1 y)}{\prod_{i=2}^{n}(\mu_i - \mu_1)} + \cdots + \frac{(-1)^{k-1} \exp(-\mu_k y)}{\prod_{i=k+1}^{n}(\mu_i - \mu_k) \prod_{j=1}^{k-1}(\mu_k - \mu_j)} + \cdots + (-1)^{n-1} \frac{\exp(-\mu_n y)}{\prod_{j=1}^{n-1}(\mu_n - \mu_j)}. \tag{A4}$$

Substitute (A4) into L_1, and obtain,

$$L_1 = \left(\prod_{i=1}^{n} \mu_i \right) \int_0^\infty f_1(y) \exp(\mu_0 (zy + z)) dy$$

$$= \exp\left(-\mu_0 z\right) \frac{\prod_{i=1}^{n} \mu_i}{\prod_{i=1}^{n} \pi_i} \underbrace{\int_0^{\infty} \overbrace{f_2\left(y\right) \prod_{i=1}^{n} \pi_i}^{L_2} dy}_{L_3}, \tag{A5}$$

where $\pi_i = \mu_i + \mu_0 z$, $i = 1, ..., n$, and,

$$f_2\left(y\right) = \frac{\exp\left(-\pi_1 y\right)}{\prod_{i=2}^{n}\left(\pi_i - \pi_1\right)} + \cdots + \frac{\left(-1\right)^{k-1} \exp\left(-\pi_k y\right)}{\prod_{i=k+1}^{n}\left(\pi_i - \pi_k\right) \prod_{j=1}^{k-1}\left(\pi_k - \pi_j\right)} + \cdots + \left(-1\right)^{n-1} \frac{\exp\left(-\pi_n y\right)}{\prod_{j=1}^{n-1}\left(\pi_n - \pi_j\right)}. \tag{A6}$$

A direct comparison of $f_2\left(y\right)$ and $f_1\left(y\right)$ reveals they have an identical structure. This implies L_2 is also a PDF. With $L_3 = 1$, substituting these conditions into (A5) gives

$$L_1 = \frac{\prod_{i=1}^{n} \mu_i}{\prod_{i=1}^{n}\left(\mu_i + \mu_0 z\right)} e^{-\mu_0 z}, \tag{A7}$$

Furthermore, substitute (A7) into (A1), achieving,

$$F_{Z_n}\left(z\right) = 1 - \frac{\prod_{i=1}^{n} \mu_i}{\prod_{i=1}^{n}\left(\mu_i + \mu_0 z\right)} e^{-\mu_0 z}, z \geq 0 \tag{A8}$$

Finally, substituting specific parameters into (A8) obtains (10).
The proof is completed.

Appendix B

We first make a transformation of (10) for easy derivation next, by changing multiplication into addition, yielding

$$F_{\eta_k^{(\mathcal{J})}}(\eta_k) = 1 - \sum_{i \in \mathcal{J}} \frac{a_i e^{-\mu_k \eta_k}}{\left(1 + \frac{\mu_k}{\mu_i} \eta_k\right)}, \eta_k \geq 0 \tag{B9}$$

where a_i is defined in (13).

The process of the derivation for the secrecy outage probability of U_k is shown as follows,

$$P_{so,k}^{(\mathcal{J})}\left(n, R_s\right) = Pr\left(\frac{1 + \gamma_k^{(n)}}{1 + \eta_k^{(\mathcal{J})}} < 2^{R_s}\right)$$
$$= 1 - \int_{2^{R_s}-1}^{\infty} d\gamma_k \int_0^{2^{-R_s}\gamma_k + 2^{-R_s} - 1} f_{\gamma_k^n}\left(\gamma_k\right) f_{\eta_k^{(\mathcal{J})}}\left(\eta_k\right) d\eta_k$$

$$= 1 - \int_{2^{R_s}-1}^{\infty} f_{\gamma_k^n}(\gamma_k) F_{\eta_k^{(\mathcal{J})}}\left(2^{-R_s}\gamma_k + 2^{-R_s} - 1\right) d\gamma_k$$

$$= \underbrace{1 - \frac{\lambda_k^{N-n}}{(N-n-1)!} \int_{2^{R_s}-1}^{\infty} \gamma_k^{N-n-1} e^{-\lambda_k \gamma_k} d\gamma_k}_{L_1} + \underbrace{\int_{2^{R_s}-1}^{\infty} \frac{\lambda_k^{N-n} e^{\mu_k(1-\frac{1}{2^{R_s}})}}{(N-n-1)!} \sum_{i\in\mathcal{J}} \frac{a_i \gamma_k^{N-n-1} e^{-(\frac{\mu_k}{2^{R_s}}+\lambda_k)\gamma_k}}{1+\frac{\mu_k}{\mu_i}(\frac{\gamma_k}{2^{R_s}}+\frac{1}{2^{R_s}}-1)} d\gamma_k}_{L_2} \tag{B10}$$

By applying the following integral result [35, Eq.(3.381.9)],

$$\int_u^{\infty} x^m e^{-\beta x} dx = \frac{\Gamma(m+1, \beta u)}{\beta^{m+1}}, \tag{B11}$$

we obtain,

$$L_1 = 1 - \frac{\mathbf{\Gamma}(N-n, \lambda_k(2^{R_s}-1))}{(N-n-1)!} \tag{B12}$$

Since $\mathbf{\Gamma}(N-n, \lambda_k(2^{R_s}-1)) + \boldsymbol{\gamma}(N-n, \lambda_k(2^{R_s}-1)) = \mathbf{\Gamma}(N-n) = (N-n-1)!$, we further reduce to

$$L_1 = \frac{\boldsymbol{\gamma}(N-n, \lambda_k(2^{R_s}-1))}{(N-n-1)!} \tag{B13}$$

We continue the process of derivation by

$$L_2 = \frac{\lambda_k^{N-n} e^{\mu_k(1-2^{-R_s})}}{(N-n-1)!} \sum_{i\in\mathcal{J}} a_i \frac{\mu_i}{\mu_k} 2^{R_s} \int_{2^{R_s}-1}^{\infty} \frac{\gamma_k^{N-n-1} e^{-(2^{-R_s}\mu_k+\lambda_k)\gamma_k}}{\gamma_k + 2^{R_s}(\frac{\mu_i}{\mu_k}-1)+1} d\gamma_k. \tag{B14}$$

Let $\gamma_k = x - 2^{R_s}(\frac{\mu_i}{\mu_k}-1) - 1$, yielding

$$L_2 = \frac{\lambda_k^{N-n} e^{\lambda_k(1-2^{R_s})}}{(N-n-1)!} \sum_{i\in\mathcal{J}} \frac{a_i \frac{\mu_i}{\mu_k} 2^{R_s}}{e^{-\mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k})}} \overbrace{\int_{2^{R_s}\frac{\mu_i}{\mu_k}}^{\infty} \frac{(x - 2^{R_s}(\frac{\mu_i}{\mu_k}-1)-1)^{N-n-1}}{x e^{(2^{-R_s}\mu_k+\lambda_k)x}} dx}^{L_3} \tag{B15}$$

and

$$L_3 = \sum_{m=0}^{N-n-1} \binom{N-n-1}{m} (-2^{R_s}(\frac{\mu_i}{\mu_k}-1)-1)^{N-n-m-1} \underbrace{\int_{2^{R_s}\frac{\mu_i}{\mu_k}}^{\infty} \frac{x^{m-1}}{e^{(2^{-R_s}\mu_k+\lambda_k)x}} dx}_{L_4}. \tag{B16}$$

Similarly, apply the integral result in (B11), obtaining

$$L_4 = \frac{\Gamma(m, \mu_i(1 + 2^{R_s}\frac{\lambda_k}{\mu_k}))}{(2^{-R_s}\mu_k + \lambda_k)^m}. \tag{B17}$$

Finally, the closed-form expression of the secrecy outage probability is given by

$$P_{so,k}^{(\mathcal{J})}(n, R_s) = \frac{\boldsymbol{\gamma}(N-n, \lambda(2^{R_s}-1))}{(N-n-1)!} + \frac{\lambda_k^{N-n} e^{\lambda_k(1-2^{R_s})}}{(N-n-1)!} \sum_{i\in\mathcal{J}} a_i \frac{\mu_i}{\mu_k} 2^{R_s} e^{\mu_i(1+2^{R_s}\frac{\lambda_k}{\mu_k})} \sum_{m=0}^{N-n-1} \binom{N-n-1}{m} \times$$
$$(-2^{R_s}(\frac{\mu_i}{\mu_k} - 1) - 1)^{N-n-m-1} \frac{\Gamma(m, \mu_i(1 + 2^{R_s}\frac{\lambda_k}{\mu_k}))}{(2^{-R_s}\mu_k + \lambda_k)^m}. \tag{B18}$$

The proof is completed.

References

[1] Nomikos, A.N., Michailidis, B.E.T., Trakadas, C.P.: A uav-based moving 5g ran for massive connectivity of mobile users and iot devices. Veh. Commun. (Oct.), 25 (2020)

[2] Sabella, D., Vaillant, A., Kuure, P., Rauschenbach, U., Giust, F.: Mobile-edge computing architecture: The role of mec in the internet of things. IEEE Consum. Electron. Mag. **5**(4), 84–91 (2016)

[3] Liu, Y., Peng, M., Shou, G., Chen, Y., Chen, S.: Toward edge intelligence: Multiaccess edge computing for 5g and internet of things. IEEE Internet Things J. **7**(8), 6722–6747 (2020)

[4] Zhang, P., Wang, C., Jiang, C., Benslimane, A.: Uav-assisted multi-access edge computing: Technologies and challenges. IEEE Internet Things Mag. **4**(4), 12–17 (2021)

[5] Lin, W., Huang, T., Li, X., Shi, F., Wang, X., Hsu, C.-H.: Energy-efficient computation offloading for uav-assisted mec: A two-stage optimization scheme. ACM Trans. Internet Technol. **22**(1), 1–23 (2021)

[6] Zhang, L., Ansari, N.: Latency-aware iot service provisioning in uav-aided mobile-edge computing networks. IEEE Internet Things J. **7**(10), 10573–10580 (2020)

[7] Feng, W., Tang, J., Zhao, N., Zhang, X., Wang, X., Wong, K.-K., Chambers, J.A.: Hybrid beamforming design and resource allocation for uav-aided wireless-powered mobile edge computing networks with noma. IEEE J. Sel. Areas Commun. **39**(11), 3271–3286 (2021)

[8] Xu, Y., Zhang, T., Yang, D., Liu, Y., Tao, M.: Joint resource and trajectory optimization for security in uav-assisted mec systems. IEEE Trans. Commun. **69**(1), 573–588 (2021)

[9] Lu, W., Ding, Y., Gao, Y., Chen, Y., Zhao, N., Ding, Z., Nallanathan, A.: Secure noma-based uav-mec network towards a flying eavesdropper. IEEE Trans. Commun. **70**(5), 3364–3376 (2022)

[10] Wang, T., Li, Y., Wu, Y.: Energy-efficient uav assisted secure relay transmission via cooperative computation offloading. IEEE Trans. Green Commun. Netw. **5**(4), 1669–1683 (2021)

[11] Yu, Z., Zhang, Z., Zeadally, S., Shen, B., Pei, X.: Energy-efficient computing offloading with trajectory optimization and resource allocation in uavs aided industrial iot. IEEE Internet Things J. **12**(17), 34780–34792 (2025)

[12] Bui, T.T., Do, T.Q., Huynh, D.V., Duy, T.D., Nguyen, L.D., Cao, T.-V., Sharma, V., Duong, T.Q.: Task offloading optimization for uav-aided noma networks with coexistence of near-field and far-field communications. IEEE Trans. Green Commun. Netw. **9**(1), 327–337 (2025)

[13] Panda, K.G., Das, S., Sen, D., Arif, W.: Design and deployment of uav-aided post-disaster emergency network. IEEE Access **7**, 102985–102999 (2019)

[14] Zhao, Z., Cumino, P., Esposito, C., Xiao, M., Braun, T., Cerqueira, E., Sargento, S.: Smart unmanned aerial vehicles as base stations placement to improve the mobile network operations. Computer Commun. **181**, 45–57 (2022)

[15] Shafique, A., Mehmood, A., Elhadef, M.: Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access **9**, 46927–46948 (2021)

[16] He, D., Chan, S., Guizani, M.: Security in the internet of things supported by mobile edge computing. IEEE Commun. Mag. **56**(8), 56–61 (2018)

[17] Sun, X., Ng, D.W.K., Ding, Z., Xu, Y., Zhong, Z.: Physical layer security in uav systems: Challenges and opportunities. IEEE Wireless Commun. **26**(5), 40–47 (2019)

[18] Amos, P., Li, P., Wu, W., Wang, B.: Computation efficiency maximization for secure uav-enabled mobile edge computing networks. Physical Commun. **46**(5), 101284 (2021)

[19] Lu, W., Ding, Y., Gao, Y., Hu, S., Wu, Y., Zhao, N., Gong, Y.: Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems. IEEE Trans. Ind. Informat. **18**(4), 2704–2713 (2022)

[20] Bai, T., Wang, J., Ren, Y., Hanzo, L.: Energy-efficient computation offloading for secure uav-edge-computing systems. IEEE Trans. Veh. Technol. **68**(6), 6074–6087 (2019)

[21] Gu, X., Zhang, G., Wang, M., Duan, W., Wen, M., Ho, P.-H.: Uav-aided energy-efficient edge computing networks: Security offloading optimization. IEEE Internet Things J. **9**(6), 4245–4258 (2022)

[22] Zhou, Y., Pan, C., Yeoh, P.L., Wang, K., Elkashlan, M., Vucetic, B., Li, Y.: Secure communications for uav-enabled mobile edge computing systems. IEEE Trans. Commun. **68**(1), 376–388 (2020)

[23] Zhao, R., Xia, J., Zhao, Z., Lai, S., Fan, L., Li, D.: Green mec networks design under uav attack: A deep reinforcement learning approach. IEEE Trans. Green Commun. Netw. **5**(3), 1248–1258 (2021)

[24] Zhu, C., Zhu, X., Ren, J., Qin, T.: Blockchain-enabled federated learning for uav edge computing network: Issues and solutions. IEEE Access **10**, 56591–56610 (2022)

[25] Qin, P., Fu, M., Fu, Y., Wang, J.: Cooperative uav trajectory design and resource allocation in blockchain-enabled secure aerial edge computing network. IEEE Trans. Wireless Commun., 1–1 (2025)

[26] Ding, Y., Han, H., Lu, W., Wang, Y., Zhao, N., Wang, X., Yang, X.: Ddqn-based trajectory and resource optimization for uav-aided mec secure communications. IEEE Trans. Veh. Technol. **73**(4), 6006–6011 (2024)

[27] Consul, P., Budhiraja, I., Garg, D., Kumar, N., Singh, R., Almogren, A.S.: A hybrid task offloading and resource allocation approach for digital twin-empowered uav-assisted mec network using federated reinforcement learning for future wireless network. IEEE Trans. Consum. Electron. **70**(1), 3120–3130 (2024)

[28] Wang, P., Yang, H., Han, G., Yu, R., Yang, L., Sun, G., Qi, H., Wei, X., Zhang, Q.: Decentralized navigation with heterogeneous federated reinforcement learning for uav-enabled mobile edge computing. IEEE Trans. Mobile Comput. **23**(12), 13621–13638 (2024)

[29] Liaq, M., Ejaz, W.: Minimizing delay in uav-aided federated learning for iot applications with straggling devices. IEEE Open J. Commun. Soc. **5**, 7653–7667 (2024)

[30] Xu, Y., Xu, H., Chen, X., Zhang, H., Chen, B., Han, Z.: Blockchain-based ar offloading in uav-enabled mec networks: A trade-off between energy consumption and rendering latency. IEEE Trans. Veh. Technol., 1–16 (2025)

[31] Mao, Y., You, C., Zhang, J., Huang, K., Letaief, K.B.: A survey on mobile

edge computing: The communication perspective. IEEE Commun. Surveys Tuts. **19**(4), 2322–2358 (2017)

[32] Jiang, K., Jing, T., Zhang, F., Huo, Y., Li, Z.: Zf-sic based individual secrecy in simo multiple access wiretap channel. IEEE Access **5**, 7244–7253 (2017)

[33] Proakis, J.G.: Digital Communications, 4th edn. McGraw-Hill Companies, Inc., New York (2001)

[34] Shulong, S.: On distribution of sums of n independent random variables subject to exponential distribution. Journal of Liaoning Normal University **13**(4), 51–58 (1990)

[35] Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series and Products, 7th edn. Academic Press, San Diego, CA (2007)