Secure NOMA-Based UAV-MEC Network Towards a Flying Eavesdropper

Weidang Lu, *Senior Member, IEEE*, Yu Ding, Yuan Gao, *Member, IEEE*, Yunfei Chen, *Senior Member, IEEE*, Nan Zhao, *Senior Member, IEEE*, Zhiguo Ding, *Fellow, IEEE*, and Arumugam Nallanathan, *Fellow, IEEE*

***Abstract*—Non-orthogonal multiple access (NOMA) allows multiple users to share link resource for higher spectrum efficiency. It can be applied to unmanned aerial vehicle (UAV) and mobile edge computing (MEC) networks to provide convenient offloading computing service for ground users (GUs) with large-scale access. However, due to the line-of-sight (LoS) of UAV transmission, the information can be easily eavesdropped in NOMA-based UAV-MEC networks. In this paper, we propose a secure communication scheme for the NOMA-based UAV-MEC system towards a flying eavesdropper. In the proposed scheme, the average security computation capacity of the system is maximized while guaranteeing a minimum security computation requirement for each GU. Due to the uncertainty of the eavesdropper's position, the coupling of multi-variables and the non-convexity of the problem, we first study the worst security situation through mathematical derivation. Then, the problem is solved by utilizing successive convex approximation (SCA) and block coordinate descent (BCD) methods with respect to channel coefficient, transmit power, central processing unit (CPU) computation frequency, local computation and UAV trajectory. Simulation results show that the proposed scheme is superior to the benchmarks in terms of the system security computation performance.**

***Index Terms*—MEC, NOMA, resource and trajectory optimization, secure communication, UAV communication.**

I. Introduction

With the evolution of wireless communications, we have gradually entered the fifth generation (5G). High frequency spectrum utilization and massive device connections have become necessary for 5G networks [1]. Intelligent applications, such as face recognition, interactive games and autonomous driving, have increased dramatically our demand for wireless devices and data traffic, which are often computationally intensive and have higher requirement on the computation capabilities of the devices. Simultaneously, the Internet of Everything also requires a wide range of wireless coverage, to provide wireless services everywhere [2].

Mobile edge computing (MEC), which can alleviate the network congestion and hightlight the computation efficiency, is widely used in various 5G applications [3]. Pham *et al.* illustrated that the computation cost of the system can be reduced and the computation capacity can be improved by dividing the backhaul bandwidth and allocating the computing resource to MEC networks [4]. Unmanned aerial vehicle (UAV) with high mobility and low cost can quickly provide an efficient emergency and auxiliary means for internet-of-thing (IoT) deployment in the remote areas [5]-[6]. Mozaffari *et al.* proposed a novel framework to maximize the average number of bits transmitted to the users by finding the optimal cell partitions associated to the UAVs under a fair resource allocation policy with given the maximum possible flight time of UAVs [6]. UAV with MEC server can flexibly enhance the quality of wireless links and provide effective offloading computation service for ground users (GUs) [7]-[14]. Specifically, Yu *et al.* showed that UAV serving as a aerial base station (BS) can solve the problem of shadow fading or signal congestion in the ground coverage area between the traditional IoT devices and ground BS [7]. Zhou *et al.* studied a scheme to highlight the computation capability in the UAV-MEC system under the energy and mobility constraints [8]. Du *et al.* proposed a UAV-MEC system that uses time division multiple access (TDMA) to strengthen the system's performance via optimizing the UAV and computation resource [9]. Wang *et al.* studied a two-layer optimal scheme to provide better service for redundant mobile GUs by rationally deploying multiple UAVs and allocating system resource [10]. Liu *et al.* studied the resource management and cooperative offloading calculation scheme under the requirements of GUs and varying channels in the UAV-aided MEC architecture [11]. Hu *et al.* proposed a useful strategy to obtain the optimized solution of the UAV-MEC system [12]. Zhang *et al.* proposed an optimal scheme in the multiple UAV-aided MEC system to strengthen the computational efficiency [13]. Liu *et al.* proposed a distributed two-stage source allocation algorithm for the energy-efficient and secure offloading problem in air-to-ground MEC networks [14].

On the other hand, non-orthogonal multiple access (NOMA) allows multiple GUs to share link resource, and successive-interference-cancellation (SIC) can be used in NOMA transmission to decode signals. Thus, NOMA transmission can achieve efficient utilization of spectrum and throughput improvement [15]-[18]. Abushattal *et al.* pointed out that NO-

Weidang Lu and Yu Ding are with College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: luweid@zjut.edu.cn, 2112003309@zjut.edu.cn).

Yuan Gao is with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: yuangao08@tsinghua.edu.cn).

Yunfei Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

Nan Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China (e-mail: zhaonan@dlut.edu.cn).

Zhiguo Ding is s with the School of Electrical and Electronic Engineering, the University of Manchester, Manchester M13 9PL, U.K. (e-mail: zhiguo.ding@manchester.ac.uk).

Arumugam Nallanathan is with School of Electronic Engineering and Computer Science, Queen Mary University of London, E1 4NS, U.K. (e-mail: a.nallanathan@qmul.ac.uk).

MA transmission can highlight the performance of wireless communication system with low bandwidth requirement [18]. Driven by these advantages, NOMA is widely applied in UAV-MEC networks to provide flexible and convenient computation offloading service for large-scale access GUs [19]-[25]. Cui *et al.* proposed to utilize orthogonal multiple access (OMA) and NOMA in the communication link between the BS and UAV to increase the system rate [19]. Na *et al.* proposed a collaborative optimization algorithm, which uses clustered-NOMA to reduce the inter-channel interference and increase the total uplink rate [20]. Li *et al.* pointed out that NOMA-MEC can further reduce the offloading and caching pressure for large data [21]. Wu *et al.* proposed an optimal strategy to offload more information to the MEC server when the NOMA transmission has co-channel interference [22]. Guo *et al.* proposed a strategy related to computing and offloading in the UAV-aided MEC framework by introducing NOMA to improve the resource utilization [23]. Zhang *et al.* proposed that the UAV-enabled MEC framework with NOMA can reduce the energy consumption of offloading and overcome the limitation of device computing energy [24]. Budhiraja *et al.* proposed an uplink transmission scheme with NOMA, which can not only support large-scale access, but also enhance the transmission quality of the UAV-aided MEC system [25].

It can be seen that NOMA transmission can provide flexible and convenient computation service for GUs in large-scale UAV-MEC networks. However, the offloading information can be easily eavesdropped by the malicious users, which brings severe security risk to NOMA-based UAV-MEC networks. Physical layer security provides high-quality secure communication by intelligently utilizing wireless channels and transmission methods [26]-[35]. Rupasinghe *et al.* investigated the protected zone approach to enhance the physical layer security of UAV-based communication network [26]. Mu *et al.* studied the security efficiency maximization by considering computing UAVs and jamming UAVs [27]. Sheng *et al.* improved the security throughput of the worst users by allocating the time slots to send confidential information or artificial noise [30]. Cao *et al.* proposed an anti-eavesdropping scheme through beamforming in NOMA networks [31]. Sun *et al.* showed that the UAV communication performed by NOMA not only expands the coverage but also improves the security [32]. Duo *et al.* proposed a security optimization strategy in the presence of mobile eavesdroppers to ensure that the confidential information between UAV and GUs is not leaked [33]. Xu *et al.* studied the security optimization scheme in UAV-MEC system to prevent eavesdroppers from stealing useful offloading information [34]. Li *et al.* studied the rate improving design in case of imperfect eavesdropping channels [35]. Since UAV has the unique advantages of high mobility and easy concealment, it can be easily explored by malicious users to eavesdrop the legitimate signals [36]-[37]. Zhou *et al.* proposed a security computation offloading scheme in a traditional communication mode with UAV acting as an eavesdropper, and the signals from other users are treated as interference during the transmission [36]. Lu *et al.* proposed a scheme to enhance the Dual-UAV-MEC system's security performance via optimizing the UAV server trajectory and system resource with TDMA [37]. Comparing with the ground eavesdroppers, which are deployed at the fixed locations in the existing works, UAV eavesdroppers will have much better channel condition due to the LoS transmission. Thus, the information can be easily eavesdropped by flying UAVs. The major challenges for considering UAV eavesdroppers are to consider the uncertainty of UAV_E position and anti-collision constraint between UAVs, which were not considered for ground eavesdroppers.

Motivated by the above-mentioned reasons, security computation capacity optimization for NOMA-based UAV-MEC system with a flying eavesdropper is studied in this paper. To our best knowledge, this is the first work that considers UAV eavesdropping on GUs' offloading information in the NOMA-based UAV-MEC network. Specifically, a secure communication scheme is proposed for the NOMA-based UAV-MEC system towards a flying eavesdropper, where a UAV eavesdropper (UAV_E) intercepts the tasks information of GUs offloaded to a UAV Server (UAV_S). We maximize the average security computation capacity via optimizing the varying channel relationship coefficient allocation between UAV_S and GUs, CPU computation frequency, transmit power, local computation and UAV_S trajectory. The key advantage of the proposed scheme is that the security computation performance is greatly improved with the similar complexity by comparing with the existing works. The main contributions of this paper are summarized as follows.

- We propose a NOMA-based UAV-MEC system with a flying eavesdropper, which includes UAV_S and UAV_E, K GUs and one ground jammer (GJ). UAV_S carries the MEC server to assist K GUs to compute the offloading tasks information. The potential mobile UAV_E eavesdrops the tasks information from GUs offloading to UAV_S. In order to enhance the system's security computation performance, GJ sends the artificial jamming signal to disturb the eavesdropping of UAV_E. Compared with [30]-[37], our novelty is that we consider UAV eavesdropping on GUs' offloading information for the NOMA-based UAV-MEC system towards a flying eavesdropper. We formulate an optimization problem to maximize the average security computation capacity of the system.
- Under considering the constraints of the system energy, GUs and UAV_S computation capability, UAV flight movement, collision prevention between UAVs and the minimum security computation requirements of GUs, we formulate an optimization problem to maximize the average security computation capacity via optimizing the varying channel relationship coefficient allocation between UAV_S and GUs, CPU computation frequency, transmit power, local computation and UAV_S trajectory. Due to the uncertainty of UAV_E position, binary constraint, coupling of multi-variables and non-convexity of the problem, we propose an effective scheme to solve it.
- We study the worst security situation to solve the uncertainty of UAV_E position through mathematical derivation. Based on successive convex approximation (SCA),

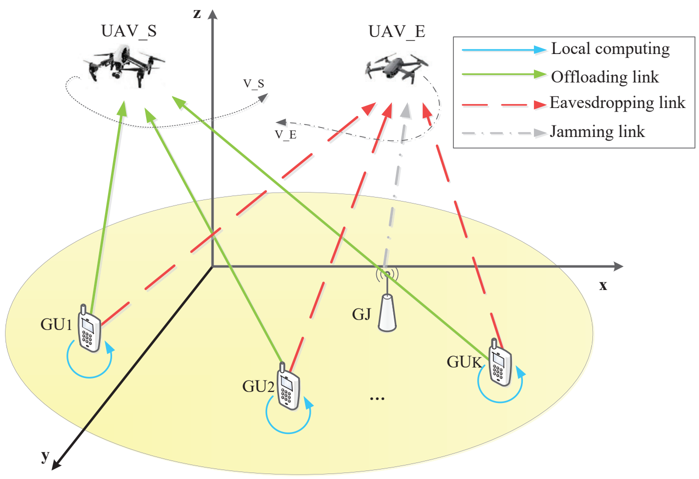


Fig. 1. The NOMA-based UAV-MEC system with a flying eavesdropper.

block coordinate descent (BCD), and alternating approximation, we obtain a high-quality solution for our joint optimization problem. We maximize the average security computation capacity of the system by optimizing the block structure of the variables in two steps, where the problems are approximately transformed to convex forms. Then, the variables are optimized by updating in an alternating manner.

The rest of this paper is organized as follows. Section II introduces the system of NOMA-based UAV-MEC. The problem of maximizing average security computation capacity is formulated in Section III. Optimization for maximizing average security computation capacity is studied in Section IV. Section V presents simulation results and discussion. Section VI concludes this paper.

II. System Model

Fig. 1 shows the proposed secure NOMA-based UAV-MEC system, in which the legitimate UAV_S carries the MEC server to serve K GUs, denoted by $\kappa = \{1, 2, ..., K\}$. UAV_S computes offloaded information of tasks from GUs, while the potential mobile UAV_E eavesdrops the offloaded tasks information. In order to enhance the security performance of the system, a GJ is set on the ground to disturb UAV_E's eavesdropping by sending artificial jamming signals to disrupt the eavesdropping. We assume that UAV_S has prior knowledge of the jamming signal sent by GJ because UAV_S and GJ belong to the legitimate network, the jamming signal sent by GJ are friendly to UAV_S. Thus, UAV_S will not be affected by the artificial jamming signals. However, UAV_E is unaware of GJ's presence because UAV_E is a mobile eavesdropper and it does not belong to the legitimate network. It treats all signals eavesdropped during flight as GUs' signals. Thus, the jamming signal sent by GJ will interfere UAV_E. All of GJ, GUs and UAVs in the system have a single antenna.

We consider a three-dimensional Cartesian coordinate system [34], the coordinates of GJ and GU$_k, k \in \kappa$, are represented as $w_j = (x_j, y_j, 0)^T, w_k = (x_k, y_k, 0)^T$, respectively. Assuming UAV_S and UAV_E fly at a certain altitude of H_s and H_e, respectively. The total flight time of UAVs is denoted as T. The positions of UAV_S and UAV_E are denoted as $q_s(t) = (x_s(t), y_s(t), H_s)$, $q_e(t) = (x_e(t), y_e(t), H_e), t \in [0, T]$, respectively. For convenience, we adopt discrete trajectory. The total flight time T is divided evenly into N time slots, e.g., $\delta_t = T/N$. The position UAV_S and UAV_E are denoted as $q_s[n] = (x_s[n], y_s[n], H_s)$, $q_e[n] = (x_e[n], y_e[n], H_e), n \in [1, 2, ..., N]$, respectively. The position of UAV_S is related to the origin of the three-dimensional Cartesian coordinate system. The position information can be get by GPS positioning or other methods [34], [36]-[37]. We assume that UAV_S has known the position of all GUs and GJ, and the channel state information of the corresponding links in advance by means of synthetic aperture radar, etc [34], [37]. We consider passive eavesdropping, in which UAV_E disguises itself as a normal UAV flying in the sky to hide itself, which makes it difficult for the legitimate network to accurately detect and track [35]-[36]. Thus, the position of UAV_E is imperfectly known at UAV_S. We consider a bounded eavesdropper location error model given by $||q_e[n] - \tilde{q}_e[n]|| \leq r_e$, where $\tilde{q}_e[n]$ is the estimated position of UAV_E, r_e is the maximum estimation error of the position of UAV_E. In practice, the maximum estimation error of the position of UAV_E will not exceed the distance between UAV_E and GU, i.e., $r_e \leq ||\tilde{q}_e[n] - w_k||$.

Denote q_s^I and q_s^F as UAV_S flight start point and end point, respectively. Denote q_e^I and q_e^F as UAV_E flight start point and end point, respectively. UAV_S flies from q_s^I to q_s^F within T to assist computing offloading. UAV_E flies from q_e^I to q_e^F within T to carry out its eavesdropping flight mission. Denote UAV_S maximum flight speed as $V_s^{\max}$. Then, UAV_S trajectory should satisfy

$$||q_s[n+1] - q_s[n]|| \leq V_s^{\max}\delta_t, \forall n = 1, 2, ..., N-1, \quad (1)$$

$$q_s[1] = q_s^I, \quad (2)$$

$$q_s[N] = q_s^F. \quad (3)$$

Define the minimum secure distance between UAVs to avoid collision as $d_{\min}$, which needs to satisfy

$$d_{\min}^2 \leq ||q_s[n] - q_e[n]||^2, \forall n = 1, 2, ..., N. \quad (4)$$

The distance between GU$_k$ and UAV_S, GJ and UAV_E, GU$_k$ and UAV_E in slot n are denoted as

$$d_{k,s}[n] = \sqrt{H_s^2 + ||w_k - q_s[n]||^2}, \quad (5)$$

$$d_{j,e}[n] = \sqrt{H_e^2 + ||w_j - q_e[n]||^2}, \quad (6)$$

$$d_{k,e}[n] = \sqrt{H_e^2 + ||w_k - q_e[n]||^2}. \quad (7)$$

As stated by 3GPP in [38], nearly 100% LoS probability can be achieved between UAV and ground user when the UAV is above 40m in the rural macro scenario or 100m in the urban macro scenario. In this work, the GU$_k$ to UAV_S channels, GJ to UAV_E channel and GU$_k$ to UAV_E channels are assumed to be well modeled by the quasi-static block fading LoS links and follow the distance-dependent path loss model. [1] Thus,

[1] This work can be easily extend to the cases with probabilistic LoS/NLoS channel model.

the channel gain between GU_k and UAV_S, GJ and UAV_E, GU_k and UAV_E in slot n are denoted as

$$h_{k,s}[n] = \sqrt{\frac{\beta_0}{d_{k,s}^2[n]}}, \tag{8}$$

$$h_{j,e}[n] = \sqrt{\frac{\beta_0}{d_{j,e}^2[n]}}, \tag{9}$$

$$h_{k,e}[n] = \sqrt{\frac{\beta_0}{d_{k,e}^2[n]}}, \tag{10}$$

where β_0 represents the path loss at the reference distance of $d = 1m$.

Define $p_k[n]$ as the transmit power of GU_k, which is not larger than the peak power of GU_k,

$$0 \leq p_k[n] \leq P_{\max}, \forall k, n. \tag{11}$$

III. Problem Formulation

In the NOMA-based UAV-MEC system, GUs utilize NOMA transmission for information offloading, in which GUs can simultaneously access to UAV_S by sharing the same time and bandwidth. UAV_S performs SIC to decode signals in descending order of channel gain, i.e., the signals of GUs far from UAV_S with lower channel gains are regarded as the interference to those signals that are closer to UAV_S with higher channel gains [15].

Assume that binary variable $\lambda_{k,l}[n]$ is used to represent the varying channel relationship coefficient between the channel of GU_k and UAV_S and the channel of GU_l and UAV_S in slot n. Since the unit channel power gain is the same, we use the relationship between the distance of GU_k and UAV_S and the distance of GU_l and UAV_S to denote $\lambda_{k,l}[n]$, which can be written as

$$\lambda_{k,l}[n] = \left\{ \begin{array}{l} 1, if d_{k,s}[n] \leq d_{l,s}[n], \\ 0, if d_{k,s}[n] > d_{l,s}[n], \end{array} \right. \tag{12a}$$

$$\lambda_{k,l}[n] \in \{0, 1\}, \tag{12b}$$

$$\lambda_{k,l}[n] + \lambda_{l,k}[n] = 1, \forall k, l, n, \tag{12c}$$

where $d_{l,s}[n]$ represents the distance between UAV_S and GU_l in slot n. As can be seen from (12a), if $d_{k,s}[n] \leq d_{l,s}[n]$, we have $h_{k,s}[n] \geq h_{l,s}[n]$. Thus, $\lambda_{k,l}[n] = 1$, which denotes that the channel condition of GU_k is better than GU_l and the task information of GU_l interferes with GU_k, otherwise $\lambda_{k,l}[n] = 0$. In order to avoid the interference in the SIC decoding process, we have (12b) to restrain it, which indicates that when the signal of GU_l interferes with the signal offloading of GU_k, the signal of GU_k will no longer interfere with the signal offloading of GU_l due to the SIC decoding.

A. Communication Model

As mentioned above, UAV_E is unaware of GJ's presence. Therefore, the jamming signals sent by GJ incurs a random effect on UAV_E. UAV_S has prior knowledge of the jamming signal sent by GJ. It will not be affected by the artificially disturbed signals. Thus, the signal-to-interference-plus-noise-ratio received at UAV_S and UAV_E are denoted as

$$r_{k,s}[n] = \frac{|h_{k,s}[n]|^2 p_k[n]}{\sum\limits_{l \neq k, l \in \kappa} \lambda_{k,l}[n] |h_{l,s}[n]|^2 p_l[n] + \delta_s^2}, \forall k, n, \tag{13}$$

$$r_{k,e}[n] = \frac{|h_{k,e}[n]|^2 p_k[n]}{|h_{j,e}[n]|^2 P_j + \sum\limits_{z \in K_k} |h_{z,e}[n]|^2 p_z[n] + \delta_e^2}, \forall k, n, \tag{14}$$

where $h_{z,e}[n]$ denotes the channel gain between GU_z and UAV_E, $K_k = \{z | z \in \kappa, |h_{z,e}| \leq |h_{k,e}|\}$ denotes the group of GUs whose channel gain to UAV_E is worse than that of GU_k to UAV_E, P_j denotes GJ transmit power, δ_s^2 and δ_e^2 denote power of Gaussian noise received at the UAV_S and the UAV_E, respectively.

Therefore, the achievable information offloading rate from UAV_S to GU_k and the achievable information eavesdropping rate from UAV_E to GU_k are denoted as

$$R_{k,s}[n] = \log_2 (1 + r_{k,s}[n]), \tag{15}$$

$$R_{k,e}[n] = \log_2 (1 + r_{k,e}[n]). \tag{16}$$

The security information offloading rate can be obtained as

$$R_{k,\sec}[n] = (R_{k,s}[n] - R_{k,e}[n])^+, \forall k, n. \tag{17}$$

B. Computation Model

In the NOMA-based UAV-MEC system, GU_k adopts partial offloading computation strategy, in which some tasks information of GU_k are calculated locally, and the remaining information tasks are offloaded to UAV_S for computation. Denote $l_{loc,k}[n]$ as the number of bits GU_k computes locally in slot n. Denote c_s and c_k as the required CPU computation cycles for computing a bit of information at UAV_S and GU_k, respectively. Denote $F_s^{\max}$ and $F_k^{\max}$ as UAV_S and GU_k maximum CPU frequency, respectively. Since GU_k cannot compute more than its maximum local computation capacity, it should satisfy

$$c_k l_{loc,k}[n] \leq F_k^{\max} \delta_t, \forall k, n. \tag{18}$$

Denote $f_k[n]$ as the CPU computation frequency allocated to GU_k at UAV_S to compute the offloaded information of tasks, which needs to satisfy

$$\sum_{k=1}^{K} f_k[n] \leq F_s^{\max}, \forall n, \tag{19a}$$

$$0 \leq f_k[n] \leq F_s^{\max}, \forall k, n. \tag{19b}$$

Similarly, the number of security computation bits offloaded from GU_k to UAV_S are limited to the computation capacity allocated by UAV_S to GU_k. Thus, the security offloading computation from GU_k to UAV_S has the following constraints

$$c_s B R_{k,\sec}[n] \delta_t \leq f_k[n] \delta_t, \forall k, n, \tag{20}$$

where B denotes channel bandwidth.

To guarantee the minimum security computation requirements for all the GUs, the amount of GU_k local computation and offloading computation assisted by UAV_S should be larger than the minimum security computation requirement, it should satisfy

$$l_{loc,k}[n] + B\delta_t R_{k,\sec}[n] \geq Q_m, \forall k, n, \tag{21}$$

where Q_m denotes the minimum security computation requirements for GUs.

Denote k_k as the effective capacitance coefficient of GU$_k$. Then, the energy consumption of GU$_k$ in local computation can be written as $\frac{k_k (c_k l_{loc,k}[n])^3}{\delta_t^2}$.

The energy consumption of GU$_k$ in computing the information of tasks locally and transmitting offloading task information to UAV_S over time T cannot be larger than the average energy budget of GU$_k$, it should satisfy

$$\sum_{n=1}^{N}\left(p_k[n]\delta_t + \frac{k_k (c_k l_{loc,k}[n])^3}{\delta_t^2}\right) \leq P_{ave}^k T, \forall k, n, \tag{22}$$

where P_{ave}^k denotes GU$_k$ average power budget.

The average security computation capacity of the NOMA-based UAV-MEC system in time T is obtained as

$$\overline{R}_{\sec} = \frac{1}{KT}\sum_{k=1}^{K}\left(\sum_{n=1}^{N} l_{loc,k}[n] + B\sum_{n=1}^{N} R_{k,\sec}[n]\delta_t\right), \tag{23}$$

which denotes the average of the total security computation capacity in all the time slots.

C. Problem Formulation

To maximize the average security computation capacity of the system, with respect to varying channel relationship coefficient $\lambda_{k,l}[n]$, transmit power $p_k[n]$, CPU computation frequency $f_k[n]$, local computation $l_{loc,k}[n]$ and UAV_S trajectory $q_s[n]$ are optimized, the optimization problem is formulated as

$$\begin{aligned}&(\mathrm{P1}): \max_{\{\lambda_{k,l}[n], f_k[n], p_k[n], l_{loc,k}[n], q_s[n]\}} \overline{R}_{\sec} \qquad (24)\\ &s.t. (1), (2), (3), (4), (11), (12), (18), (19), (20), (21), (22).\end{aligned}$$

The original problem (P1) is non-convex.

Proof: Due to the uncertainty of UAV_E position, coupling of multi-variables, binary constraint and the non-convexity of constraints (4), (20) and (21), the original problem (P1) is non-convex. Specifically, the right side of the constraint (4) is concave. Thus, (4) is non-convex. Constraints (20) and (21) are related to $R_{k,sec}[n]$. $R_{k,sec}[n]$ is composed of multiple optimization variables, e.g., $\lambda_{k,l}[n]$, $p_k[n]$ and $q_s[n]$, which makes (20) and (21) are multi-variables coupled and non-convex. Moreover, the objective function $\overline{R}_{\sec}$ is related to $R_{k,sec}[n]$, which is also non-convex. Therefore, the problem (P1) is non-convex. ■

IV. Optimization for Maximizing Average Security Computation Capacity

To simplify the original problem (P1), we introduce auxiliary variables $\hat{s}$, $\hat{s}_{1,k}[n]$, $\hat{s}_{2,k}[n]$ [34]. Then, the original problem (P1) can be equivalently rewritten as

$$(\mathrm{P1.1}): \max_{\hat{z}} \hat{s} \tag{25a}$$

$$s.t. (1), (2), (3), (4), (11), (12), (18), (19), (22)$$

$$KT\hat{s} \leq \sum_{k=1}^{K}\sum_{n=1}^{N}\left(l_{loc,k}[n] + B\delta_t\left(\hat{s}_{1,k}[n] - \hat{s}_{2,k}[n]\right)\right), \forall n, \tag{25b}$$

$$\hat{s}_{1,k}[n] \leq R_{k,s}[n], \forall k, n, \tag{25c}$$

$$\hat{s}_{2,k}[n] \geq R_{k,e}[n], \forall k, n, \tag{25d}$$

$$c_k B\left(\hat{s}_{1,k}[n] - \hat{s}_{2,k}[n]\right) \leq f_k[n], \forall k, n, \tag{25e}$$

$$B\delta_t\left(\hat{s}_{1,k}[n] - \hat{s}_{2,k}[n]\right) + l_{loc,k}[n] \geq Q_m, \forall k, n, \tag{25f}$$

where, $\hat{z}$ denotes the variables we need to optimize, $\hat{z} = \{\lambda_{k,l}[n], f_k[n], p_k[n], l_{loc,k}[n], q_s[n], \hat{s}, \hat{s}_{1,k}[n], \hat{s}_{2,k}[n]\}$. $\hat{s}$ represents the lower bound of the average security computation capacity $\overline{R}_{\sec}$, and $\hat{s}_{1,k}[n]$ represents the lower bound of the instantaneous tasks information offloading rate $R_{k,s}[n]$, which can be represented by (25b) and (25c). $\hat{s}_{2,k}[n]$ represents the upper bound of the instantaneous tasks information eavesdropping rate $R_{k,e}[n]$, which can be represented by (25d). $\hat{s}$ needs to satisfy the equality constraint in (25b), otherwise its value will tend to infinity. Thus, the optimization target can be represented by (25a). Constraints (20) and (21) are rewritten as (25e) and (25f), respectively.

Due to the uncertainty of UAV_E position, $R_{k,e}[n]$ in the objective function is implicit. In order to facilitate the derivation, we maximize the average security computation capacity of all GUs in the worst case in the NOMA-based UAV-MEC system. In Lemma 1, we obtain the upper bound of $R_{k,e}[n]$ and approximate it to the achievable information eavesdropping rate from UAV_E to GU$_k$.

Lemma 1: The upper bound of $R_{k,e}[n]$ is expressed as

$$\begin{aligned}R_{k,e}^{ub}[n] &= \log_2\left(1 + r_{k,e}^{ub}[n]\right)\\ &= \log_2\left(1 + \frac{p_k[n]|\hat{h}_{k,e}[n]|^2}{|\hat{h}_{j,e}[n]|^2 P_j + \sum\limits_{z=1, z\in K_k} p_z[n]|\hat{h}_{z,e}[n]|^2 + \delta_e^2}\right),\end{aligned} \tag{26}$$

where

$$|\hat{h}_{k,e}[n]|^2 = \frac{\beta_0}{H_e^2 + (||q_e[n] - w_k|| - r_e)^2}, \tag{27}$$

$$|\hat{h}_{z,e}[n]|^2 = \frac{\beta_0}{H_e^2 + (||q_e[n] - w_z|| + r_e)^2}, \tag{28}$$

$$|\hat{h}_{j,e}[n]|^2 = \frac{\beta_0}{H_e^2 + (||q_e[n] - w_j|| + r_e)^2}, \tag{29}$$

indicate the maximum estimation value of $|h_{k,e}[n]|^2$, the minimum estimation value of $|h_{z,e}[n]|^2$ and the minimum estimation value of $|h_{j,e}[n]|^2$.

Proof: According to the maximum estimate error previously proposed, $||q_e[n] - \tilde{q}_e[n]|| \leq r_e$, we can apply triangle inequality and anti-triangle inequality to solve the uncertainty of UAV_E position, as follows,

$$\begin{aligned}|q_e[n]-w_k|| &\geq ||q_e[n]-w_k||-||q_e[n]-\tilde{q}_e[n]|| \\ &\geq ||q_e[n]-w_k||-r_e,\end{aligned} \tag{30a}$$

$$\begin{aligned}||q_e[n]-w_z|| &\leq ||q_e[n]-w_z||+||q_e[n]-\tilde{q}_e[n]|| \\ &\leq ||q_e[n]-w_z||+r_e,\end{aligned} \tag{30b}$$

$$\begin{aligned}||q_e[n]-w_j|| &\leq ||q_e[n]-w_j||+||q_e[n]-\tilde{q}_e[n]|| \\ &\leq ||q_e[n]-w_j||+r_e.\end{aligned} \tag{30c}$$

Thus, the upper bound of $R_{k,e}[n]$ is expressed as (26). ■

Due to the multi-variables coupling constraints and binary constraints, problem (P1.1) is non-convex. We solve (P1.1) by optimizing the block structure of the variables in two steps. In Step 1, we optimize the block of variables $\{\hat{z}\backslash q_s[n]\}$ with fixed UAV_S trajectory $\{q_s[n]\}$. In Step 2, we optimize UAV_S trajectory $\{q_s[n]\}$ with fixed $\{\hat{z}\backslash q_s[n]\}$.

A. Step 1: Optimizing $\{\hat{z}\backslash q_s[n]\}$ with fixed $q_s[n]$.

With fixed UAV_S trajectory $q_s[n]$, problem (P1.1) is reformulated as

$$\begin{aligned}&(\mathrm{P2}): \max_{\hat{z}\backslash\{q_s[n]\}} \ \hat{s} \\ &s.t.(11),(12),(18),(19),(22),(25\mathrm{b})-(25\mathrm{f}).\end{aligned} \tag{31}$$

Problem (P2) is difficult to obtain the solution for two reasons. First, constraint (18) is a binary constraint, which is not continuous. Second, constraint (25c) and (25d) are both non-convex.

We use SCA and BCD technique to solve (P2), in which varying channel relationship coefficient optimization $A = \lambda_{k,l}[n]$, transmit power allocation $B = p_k[n]$, CPU computation frequency allocation $C = f_k[n]$ and local computation allocation $D = l_{loc,k}[n]$ can be obtained by updating in an iterative way by considering the others fixed [39].

1) Varying channel relationship coefficient optimization: For fixed transmit power allocation B, CPU computation frequency allocation C and local computation allocation D, we formulate the varying channel relationship coefficient optimization problem as

$$\begin{aligned}&(\mathrm{P2.1}): \max_{\{A\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \ \hat{s} \\ &s.t.(12),(25\mathrm{b})-(25\mathrm{f}).\end{aligned} \tag{32}$$

Introducing $\tilde{\lambda}_{k,l}[n]$ into binary constraint (12), it can be equivalently converted as

$$\lambda_{k,l}[n]=\tilde{\lambda}_{k,l}[n], \forall k,l,n, \tag{33a}$$

$$\lambda_{k,l}[n]\left(1-\tilde{\lambda}_{k,l}[n]\right)=0, \tag{33b}$$

$$\lambda_{k,l}[n]d_{k,s}[n] \leq d_{l,s}[n], \forall k,n. \tag{33c}$$

It can be seen that (33a) and (33b) are exactly equivalent to (12b) and (12c). From (33c), if $d_{l,s}[n] > d_{k,s}[n]$, $\lambda_{k,l}[n]$ could be 1 or 0, and if $d_{l,s}[n] < d_{k,s}[n]$, we have $\lambda_{k,l}[n] = 0$. However, $\lambda_{k,l}[n]$ and $\lambda_{l,k}[n]$ are constrained by (12c), if $\lambda_{k,l}[n]$ or $\lambda_{l,k}[n]$ is 1, the other one must be 0, then (33c) is equivalent to (12a). Thus, $\tilde{\lambda}_{k,l}[n]$ can effectively solve the binary constraint of (P2.1).

Then, problem (P2.1) is converted as

$$\begin{aligned}&(\mathrm{P2.1.1}): \max_{\{A,\tilde{\lambda}_{k,l}[n]\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \ \hat{s} \\ &s.t.(25\mathrm{b})-(25\mathrm{f}),(33).\end{aligned} \tag{34}$$

Problem (P2.1.1) can be solved by standard optimization techniques, e.g., CVX, since it is a typical linear problem [40].

2) Transmit power allocation: For fixed varying channel relationship coefficient optimization A, CPU computation frequency allocation C and local computation allocation D, we formulate the transmit power allocation problem (P2.2) as

$$\begin{aligned}&(\mathrm{P2.2}): \max_{\{B\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \ \hat{s} \\ &s.t.(11),(22),(25\mathrm{b})-(25\mathrm{f}).\end{aligned} \tag{35}$$

Note that problem (P2.2) is non-convex due to the non-convexity of (25c) and (25d), which is hard to solve. We can apply SCA technique to approximate the problem (P2.2) as a convex problem in each iteration [39], which can obtain the transmit power allocation solution by updating it iteratively.

Substituting (13) into (15) and (25c), we can obtain

$$\begin{aligned}&\hat{s}_{1,k}[n] \leq F_{1,k}[n] \\ &-\log_2\left(\sum_{l\neq k,l\in\kappa}\lambda_{k,l}[n]p_l[n]|h_{l,s}[n]|^2+\delta_s^2\right), \forall k,n,\end{aligned} \tag{36}$$

where

$$\begin{aligned}&F_{1,k}[n]= \\ &\log_2\left(\sum_{l\neq k,l\in\kappa}\lambda_{k,l}[n]p_l[n]|h_{l,s}[n]|^2+p_k[n]|h_{k,s}[n]|^2+\delta_s^2\right).\end{aligned} \tag{37}$$

Note that the convex function can be obtained by the global lower bound with the first-order Taylor expansion [5]. In Lemma 2, the lower bound of $\hat{s}_{1,k}[n]$ is approximately obtained.

Lemma 2: (36) is approximately transformed as

$$\begin{aligned}&\hat{s}_{1,k}[n] \leq F_{1,k}[n] \\ &-\log_2\left(\sum_{l\neq k,l\in\kappa}\lambda_{k,l}[n]|h_{l,s}[n]|^2p_l^r[n]+\delta_s^2\right) \\ &-\frac{1}{\ln2}\frac{\sum\limits_{l\neq k,l\in\kappa}\lambda_{k,l}[n]|h_{l,s}[n]|^2\left(p_l[n]-p_l^r[n]\right)}{\sum\limits_{l\neq k,l\in\kappa}\lambda_{k,l}[n]|h_{l,s}[n]|^2p_l^r[n]+\delta_s^2}, \forall k,n,\end{aligned} \tag{38}$$

where $p_l^r[n]$ denotes the transmit power acquired by GU_l in r_{th} iteration.

Proof: Define $f(x) = \log(1+ax)$, where a represents a constant. Giving a feasible point x_0, we can use first-order Taylor expansion to approximately transform $f(x)$ as

$$f(x) \approx \log(1+ax_0)+\frac{a(x-x_0)}{1+ax_0}. \tag{39}$$

Based on Lemma 2, (36) can be transformed as (38). ■

Similarly, substituting (14) into (16) and (25d), (25d) is equivalent as

$$\begin{aligned}&\hat{s}_{2,k}[n] \geq F_{2,k}[n]+ \\ &\log_2\left(\sum_{z\in K_k}|h_{z,e}[n]|^2p_z[n]+A_1[n]+|h_{k,e}[n]|^2p_k[n]\right), \forall k,n.\end{aligned} \tag{40}$$

where $A_1[n] = |h_{j,e}[n]|^2 P_j + \delta_e^2$, and

$$F_{2,k}[n] = \\ -\log_2\left(|h_{j,e}[n]|^2 P_j + \sum_{z\in K_k} |h_{z,e}[n]|^2 p_z[n] + \delta_e^2\right). \tag{41}$$

Then, (40) can be approximately transformed as (42), shown at the top of the next page, where $p_z^r[n]$ and $p_k^r[n]$ represent the transmit power acquired by GU$_z$ and GU$_k$ in r_{th} iteration, respectively.

Thus, the problem (P2.2) is transformed as

$$\begin{aligned}(\text{P2.2.1}):&\max_{\{B\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \quad \hat{s} \\ &s.t.(11),(22),(25\text{b}),(25\text{e}),(25\text{f}),(38),(42).\end{aligned} \tag{43}$$

Problem (P2.2.1) is a typical convex problem since all of its constraints are convex, e.g., constraint (11), (25b), (25e) and (25f) are linear and constraint (22), (28) and (42) are convex. The solution of (P2.2.1) can be obtained by using CVX.

3) CPU computation frequency allocation: For fixed varying channel relationship coefficient optimization A, transmit power allocation B and local computation allocation D, we formulate the CPU computation frequency allocation problem (P2.3) as

$$\begin{aligned}(\text{P2.3}):&\max_{\{C\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \quad \hat{s} \\ &s.t.(19),(25\text{b})-(25\text{f}).\end{aligned} \tag{44}$$

Problem (P2.3) is convex since all of its constraints are linear, e.g., constraint (19), (25b)-(25f) are linear, which can be solved by using CVX.

4) Local computation allocation: For fixed varying channel relationship coefficient optimization A, transmit power allocation B and CPU computation frequency allocation C, the local computation allocation problem (P2.4) is formulated as

$$\begin{aligned}(\text{P2.4}):&\max_{\{D\},\{\hat{s},\hat{s}_{1.k}[n],\hat{s}_{2,k}[n]\}} \quad \hat{s} \\ &s.t.(22),(25\text{b})-(25\text{f}).\end{aligned} \tag{45}$$

Problem (P2.4) is convex since all of its constraints are linear, e.g., constraint (22), (25b), (25e) and (25f) are linear, which can be solved by using CVX.

B. Step 2: Optimizing $q_s[n]$ with fixed $\{\hat{z}\backslash q_s[n]\}$.

For fixed varying channel relationship coefficient optimization A, transmit power allocation B, CPU computation frequency allocation C and local computation allocation D, the UAV_S trajectory optimization problem (P3) is re-transformed as

$$\begin{aligned}(\text{P3}):&\max_{\hat{z}\backslash\{q_s[n]\}} \quad \hat{s} \\ &s.t.(1),(2),(3),(4),(25\text{b})-(25\text{f}).\end{aligned} \tag{46}$$

Problem (P3) is hard to handle since constraints (4) and (25c) are non-convex. We can approximately handle it by SCA technique, in which UAV_S trajectory optimization solution can be obtained by updating it in iterations [39].

Assume $q_s^r[n]$ represents UAV_S trajectory after r_{th} iteration. We can approximately transform (4) into

$$\begin{aligned}d_{\min}^2 \le 2||q_s^r[n] - q_e[n]||||q_s[n] - |q_s^r[n]||+ \\ ||q_s^r[n] - q_e[n]||^2, \forall n.\end{aligned} \tag{47}$$

The right side of (25c) is equivalent to

$$\begin{aligned}&\pi_{1,k}[n] = \\ &\log_2\left(\frac{\beta_0 p_k[n]}{H_s^2+||q_s[n]-w_k||^2}+\sum_{l\neq k,l\in\kappa}\frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s[n]-w_l||^2}+\delta_s^2\right) \\ &-\log_2\left(\sum_{l\neq k,l\in\kappa}\frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s[n]-w_l||^2}+\delta_s^2\right).\end{aligned} \tag{48}$$

For the first and second item of $\pi_{1,k}[n]$ can be approximately converted as (49) and (50), shown at the top of the next page.

Thus, (25c) is approximated as

$$\hat{s}_{1,k}[n] \le t_{1,k}[n] - t_{2,k}[n]. \tag{51}$$

Problem (P3) is reformulated as

$$\begin{aligned}(\text{P3.1}):&\max_{\hat{z}\backslash\{q_s[n]\}} \quad \hat{s} \\ &s.t.(1),(2),(3),(25\text{b}),(25\text{d})-(25\text{f}),(47),(51).\end{aligned} \tag{52}$$

Problem (P3.1) is convex as all its constraints are convex, e.g., constraint (1), (2), (3), (25b) and (25d)-(25f) are linear and constraint (47) and (51) are convex. Then, we can solve it by using CVX in an iterative manner.

C. Algorithm for Problem (P1)

In conclusion, we can solve the problem (P2.1.1), (P2.2.1), (P2.3) and (P2.4) alternatively to obtain the solution of the problem (P2), and we can obtain the solution of the problem (P3) via solving the problem (P3.1). Then, we can solve the problems (P2) and (P3) iteratively to ensure that the objective function of the optimization problem (P1) is non-subtractive when the values of all variables are updated. The final problem (P1) can be solved in detail as shown in Algorithm 1.

The convergence of Algorithm 1 for problem (P1) is proved as follows.

Proposition 1: Algorithm 1 is convergent.

Proof: Since (P2.1.1) is a typical linear problem, the varying channel relationship coefficient optimization solution of (P2.1.1) at $(r+1)_{th}$ iteration is not less than the solution at r_{th} iteration, we have

$$\hat{s}^r \le \hat{s}^{r+1}. \tag{53}$$

Thus, the objective function of (P2.1.1) is non-subtractive when the values of all variables are updated. Similarly, the solution of problem (P2.2.1), (P2.3), (P2.4) and (P3.1) at $(r+1)_{th}$ iteration is also not less than the solution at r_{th} iteration, respectively. Therefore, the objective function of the original problem (P1) is non-subtractive. When the target value increment is lower than convergence accuracy ε, the upper bound of the maximum average security computation capacity is a finite value. Thus, Algorithm 1 is convergent. ■

$$\hat{s}_{2,k}[n] \geq F_{2,k}[n] + \log_2\left(\sum_{z\in K_k} |h_{z,e}[n]|^2 p_z^r[n] + A_1[n] + |h_{k,e}[n]|^2 p_k^r[n]\right) + \frac{\sum\limits_{z\in K_k} |h_{z,e}[n]|^2 \left(p_z[n]-p_z^r[n]\right) + |h_{k,e}[n]|^2 \left(p_k[n]-p_k^r[n]\right)}{\ln 2 \sum\limits_{z\in K_k} |h_{z,e}[n]|^2 p_z^r[n] + A_1[n] + |h_{k,e}[n]|^2 p_k^r[n]}. \tag{42}$$

$$t_{1,k}[n] = \log_2\left(\frac{\beta_0 p_k[n]}{H_s^2+||q_s^r[n]-w_k||^2} + \sum_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s^r[n]-w_l||^2} + \delta_s^2\right) - \frac{\frac{\beta_0 p_k[n]\left(||q_s[n]-w_k||^2-||q_s^r[n]-w_k||^2\right)}{\left(H_s^2+||q_s^r[n]-w_k||^2\right)^2}}{\ln 2\left(\frac{\beta_0 p_k[n]}{H_s^2+||q_s^r[n]-w_k||^2} + \sum\limits_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s^r[n]-w_l||^2} + \delta_s^2\right)} - \frac{\sum\limits_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]\left(||q_s[n]-w_l||^2-||q_s^r[n]-w_l||^2\right)}{\left(H_s^2+||q_s^r[n]-w_l||^2\right)^2}}{\ln 2\left(\frac{\beta_0 p_k[n]}{H_s^2+||q_s^r[n]-w_k||^2} + \sum\limits_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s^r[n]-w_l||^2} + \delta_s^2\right)}. \tag{49}$$

$$t_{2,k}[n] = \log_2\left(\sum_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s^r[n]-w_l||^2} + \delta_s^2\right) - \frac{2\sum\limits_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]\left(||q_s^r[n]-w_l||\right)\left(||q_s[n]-q_s^r[n]||\right)}{\left(H_s^2+||q_s^r[n]-w_l||^2\right)^2}}{\ln 2\left(\sum\limits_{l\neq k, l\in\kappa} \frac{\lambda_{k,l}[n]\beta_0 p_l[n]}{H_s^2+||q_s^r[n]-w_l||^2} + \delta_s^2\right)}. \tag{50}$$

Algorithm 1 Proposed optimization algorithm

```
Initialize Given $\{\lambda^r_{k,l}[n], p^r_k[n], f^r_k[n], l^r_{loc,k}[n], q^r_s[n]\}$, set initial iteration $r = 0$ and the convergence accuracy $\varepsilon$, $\varepsilon > 0$.
repeat
    Solve (P2.1.1) with fixed $\{p^r_k[n], f^r_k[n], l^r_{loc,k}[n], q^r_s[n]\}$, and obtain varying channel relationship coefficient optimization $\lambda_{k,l}[n]$. Update $\lambda^r_{k,l}[n] = \lambda_{k,l}[n]$.
    Solve (P2.2.1) with fixed $\{\lambda^r_{k,l}[n], f^r_k[n], l^r_{loc,k}[n], q^r_s[n]\}$, and obtain transmit power allocation $p_k[n]$. Update $p^r_k[n] = p_k[n]$.
    Solve (P2.3) with fixed $\{\lambda^r_{k,l}[n], p^r_k[n], l^r_{loc,k}[n], q^r_s[n]\}$, and obtain CPU computation frequency allocation $f_k[n]$. Update $f^r_k[n] = f_k[n]$.
    Solve (P2.4) with fixed $\{\lambda^r_{k,l}[n], f^r_{loc,k}[n], p^r_k[n], q^r_s[n]\}$, and obtain local computation allocation $l_{loc,k}[n]$. Update $l^r_{loc,k}[n] = l_{loc,k}[n]$.
    Solve (P3.1) with fixed $\{\lambda^r_{k,l}[n], p^r_k[n], f^r_k[n], l^r_{loc,k}[n]\}$, and obtain UAV_S optimized trajectory $q_s[n]$. Update $q^r_s[n] = q_s[n]$
    Update $r = r + 1$.
Until The target value increment is lower than convergence accuracy $\varepsilon$ or $r$ increases to the setting maximum iterations.
Output $\hat{s}, \hat{s}_{1,k}[n], \hat{s}_{2,k}[n], \lambda_k[n], p_k[n], f_k[n], l_{loc,k}[n]$ and $q_s[n]$.
```

D. Complexity of Proposed Algorithm

The complexity of Algorithm 1 is mainly determined by the total number of all variables we optimize. Algorithm 1 involves K GUs and N time slots. There are $N + 4KN$ variables that need to be optimized. Thus, the complexity of Algorithm 1 is $I_1 \log_2(\frac{1}{\varepsilon})O(N + 4KN)^{3.5}$, where I_1 indicates the iteration number of Algorithm 1, and ε indicates the convergence accuracy, which has the similar complexity of the scheme proposed in [37].

V. Simulation Results And Discussion

In this section, we present simulation results to validate the security computation performance of the proposed scheme. In our scenario, five GUs and one GJ are randomly distributed in $400 \times 400m^2$ area. UAV_S takes an optimized trajectory from $q_s^I = [-200, -10, 100]^T$ to $q_s^F = [200, -10, 100]^T$ and UAV_E takes a straight line from $q_e^I = [-200, 50, 100]^T$ to $q_e^F = [200, -60, 100]^T$. We set the reference channel power gain $\beta_0 = -60dB$, Gaussian noise power $\sigma_s^2 = \sigma_e^2 = -110dBm$, GJ transmit power $P_j = 0.1W$, GU$_k$ peak power $P_{\max} = 0.1W$, GU$_k$ average power budget $P_{ave}^k = 2W$, the required number of CPU computation cycles for computing one bit information at UAV_S and GU$_k$, $c_s = c_k = 10^3 cycles/bit$, GU$_k$ and UAV_S maximum CPU frequency $F_k^{\max} = 1GHz, F_s^{\max} = 20GHz$ [34], GU$_k$ effective capacitance coefficient $\kappa_k = 10^{-27}$, the maximum flight speed of UAV_S $V_s^{\max} = 50m/s$, the channel bandwidth

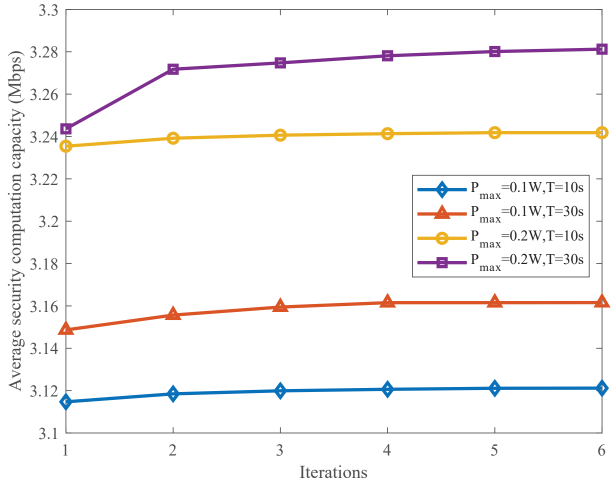


Fig. 2. Average security computation capacity convergence with different T and P_{max}.

$B = 1MHz$ and minimum security computation requirement of each GU $Q_m = 0.5Mbits$.

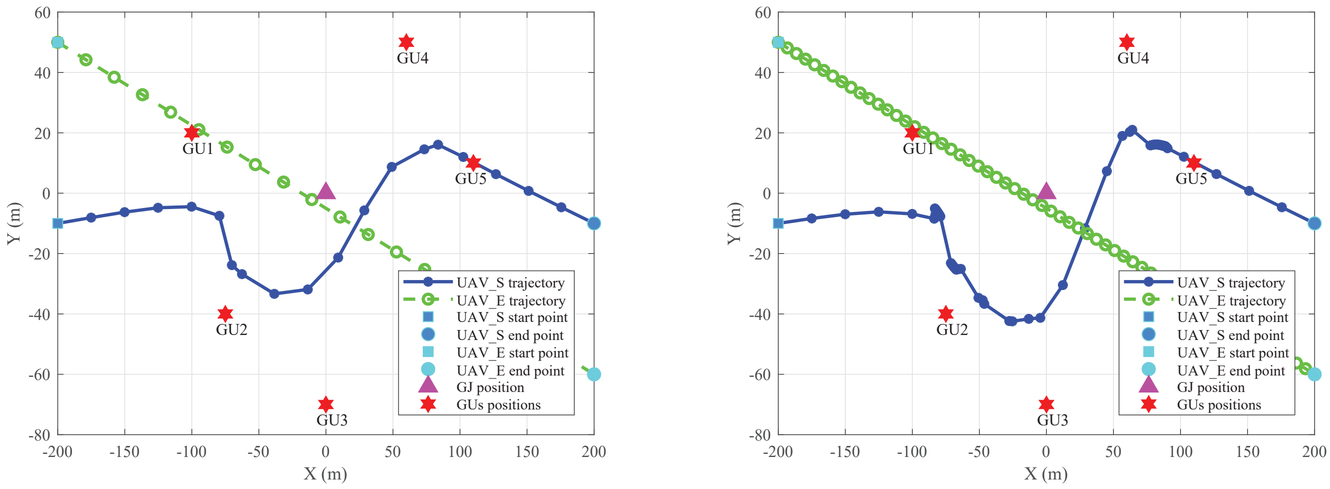
Fig. 2 shows the convergence of the average security computation capacity for different flight time T and different GUs transmit peak power P_{max}. We can observe that the proposed scheme has good convergence performance. When T and P_{max} increase, the average security computation capacity of the NOMA-based UAV-MEC system increases.

Fig. 3 shows the comparison of the optimized UAV_S trajectory and the pre-determined UAV_E trajectory with different flight time T. Fig. 3a shows the trajectories of UAV_S and UAV_E for NOMA transmission when $T = 10s$. We can observe that UAV_S adjusts its flight trajectory to try to approach GU. However, it cannot hover in the air because T is short and UAV_S needs to reach the end point on time. As shown in Fig. 3b, when T becomes large, UAV_S will have enough time to reach the end point. UAV_S will hover in some positions to increase the average security computation capacity of the system.

Fig. 4 shows the comparison of the optimized flight speed of UAV_S and the constant flight speed of UAV_E with different T. Since UAV_E flies from q_e^I to q_e^F with a fixed trajectory at a constant speed during the flight, its speed will not change when T is fixed. In Fig. 4a and Fig. 4b, the UAV_E flight speed are different, because UAV_E flies the same flight distance with different T. The trajectory of UAV_S is optimized to maximize the average security computation capacity. Thus, the flight speed of UAV_S changes accordingly in different time. When the flight time T is short, as shown in Fig. 4a, UAV_S flies almost at the maximum flight speed, $V_s^{\max}$, in order to reach the end point on time. When the flight time becomes large, as shown in Fig. 4b, UAV_S has relatively sufficient time to provide offloading computation service for GUs. Then, the flight speed of UAV_S drops to sufficiently utilize the best channel condition in maximizing the average security computation capacity.

In order to show the information computation of each GU during the UAVs flight, we compare the security computation capacity of each GU in each slot n for different T in Fig. 5. We can observe that the security computation capacity of all the GUs are larger than $0.5Mbits$, since the basic security computation needs for each GU Q_m is $0.5Mbits$. UAV_S flies from $[-200, -10, 100]^T$ to $[200, -10, 100]^T$, passing through GU1, GU2, GU3, GU4 and GU5 in turn. When UAV_S approaches GU$_k$, the communication resources and computation resources will be relatively inclined to GU$_k$ to enhance the system's average security computation performance. since GU$_k$ has the best channel condition to UAV_S, the security computation capacity of GU$_k$ is much larger than the other GUs.

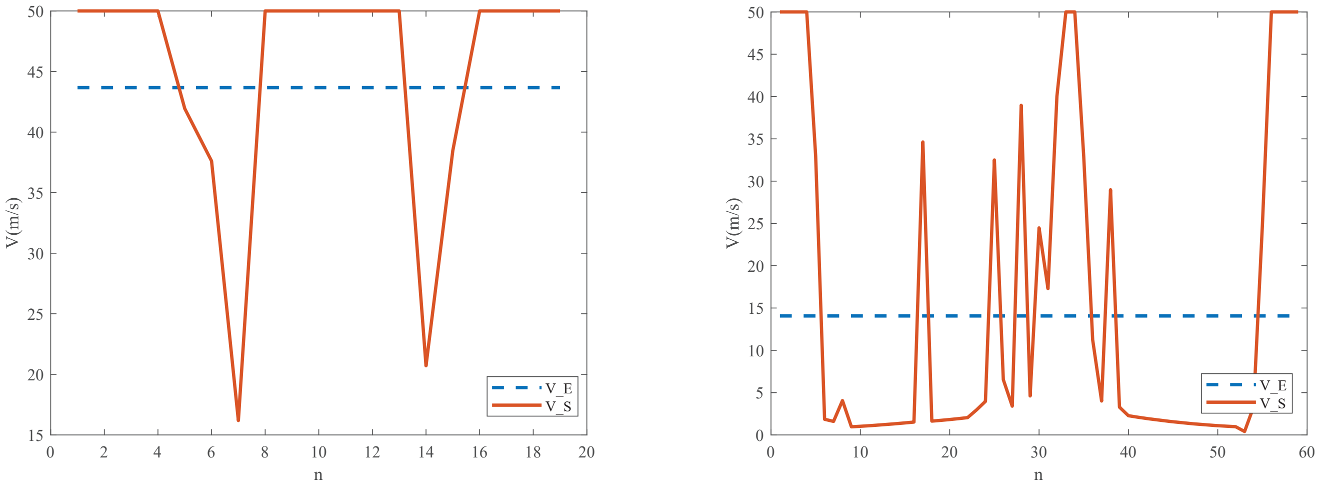
Fig. 6 shows the average security computation capacity of NOMA-based UAV-MEC system versus the peak power P_{max} with different flight time T. We can observe from Fig. 6 that when P_{max} increases, the average security computation capacity of the system will also increase, because GUs can



(a) UAV_S and UAV_E trajectory with $P_{max} = 0.1W$, $T = 10s$.

(b) UAV_S and UAV_E trajectory with $P_{max} = 0.1W$, $T = 30s$.

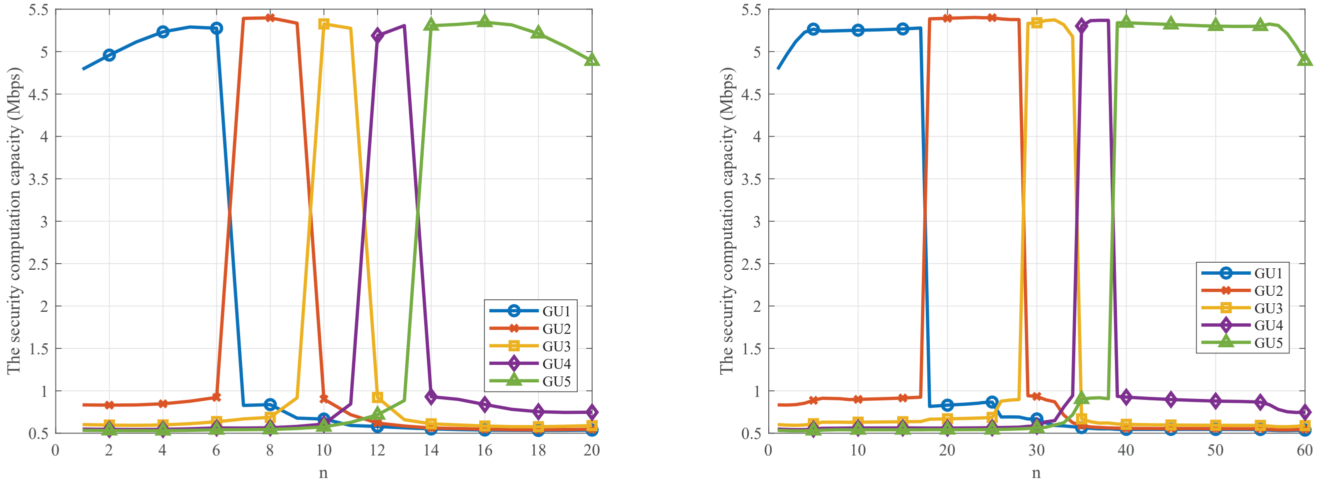
Fig. 3. Comparison of UAV_S and UAV_E trajectory with different T.



(a) UAV_S and UAV_E flight speed with $P_{max} = 0.1W$, $T = 10s$.

(b) UAV_S and UAV_E flight speed with $P_{max} = 0.1W$, $T = 30s$.

Fig. 4. Comparison of UAV_S and UAV_E flight speed with different T.



(a) The security computation of each GU in slot n with $P_{max} = 0.1W$, $T = 10s$.

(b) The security computation of each GU in slot n with $P_{max} = 0.1W$, $T = 30s$.

Fig. 5. Comparison of the security computation capacity of each GU in slot n with different T.

obtain more energy to support the transmission of offloading task information with larger P_{max}.

Fig. 7 shows the average security computation capacity versus T with different peak power P_{max}. We can observe from Fig. 7 that the average security computation capacity of the system increases with the UAV flight time T, because when T increases, UAV_S has more time to carry out information offloading transmission and calculate the offloading task information of GUs at a better position.

Fig. 8 shows the average security computation capacity of the system with different value of the required CPU computation cycles for computing a bit of information at UAV_S and GU_k, c_s and c_k. We can observe from Fig. 8 that when c_s decreases, the average security computation capacity of the system increases. This is because when c_s decreases, the computation speed by UAV_S becomes faster, which increases the security offloading computation capacity to the UAV_S. Similarly, when c_k decreases, the average security computation capacity of the system also increases accordingly. It is because that when c_k decreases, GU_k local computing speed becomes faster, which increases the local computation capacity.

To prove the superior security computation performance of the proposed scheme, we compare the security calculation performance with the following benchmark schemes in Fig. 9 and Fig. 10.

Scheme 1: The average security computation capacity of the system are maximized by optimizing GU_k local computation, GU_k transmit power, time allocating factor and UAV_S trajectory in TDMA based Dual-UAV-MEC system [37].

Scheme 2: UAV_S flies with straight trajectory, while the varying channel relationship coefficient, GU_k transmit power, GU_k CPU computation frequency, GU_k transmit power and

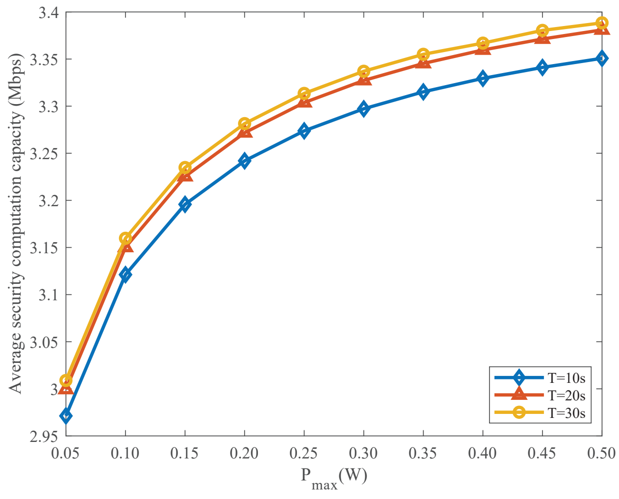


Fig. 6. Average security computation capacity variation versus P_{max} with different T.

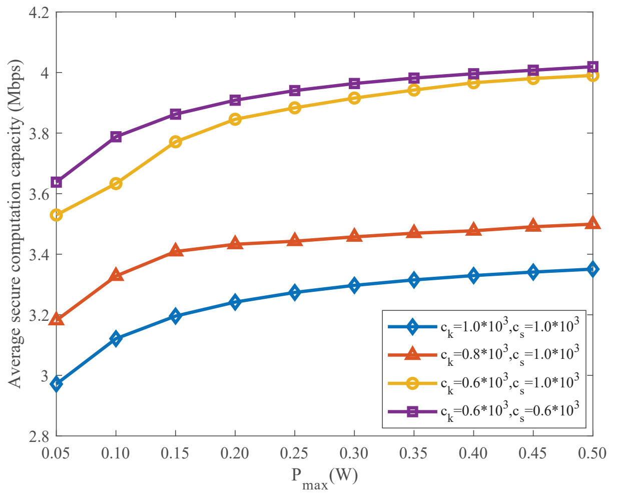


Fig. 8. Average security computation capacity variation with different c_s and c_k.

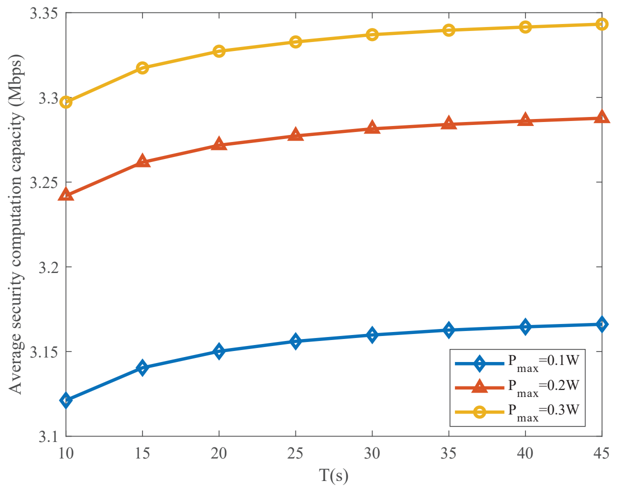


Fig. 7. Average security computation capacity variation versus T with different P_{max}.

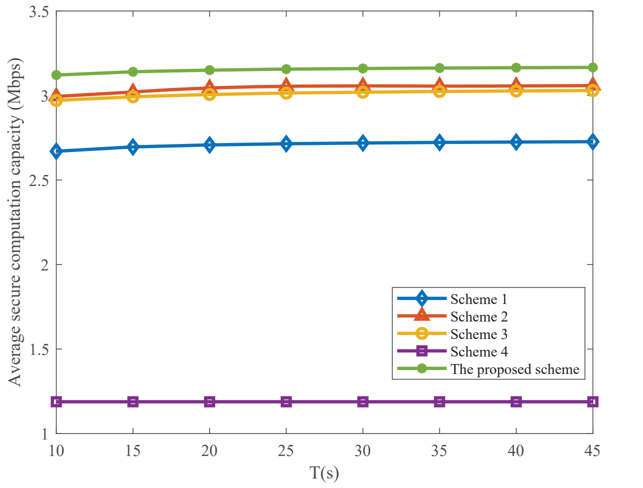


Fig. 9. The security computation performance comparison with different schemes versus T.

GU$_k$ local computation are optimized to maximize the average security computation capacity of the system.

Scheme 3: The transmit power of GUs are fixed, while the varying channel relationship coefficient, GU$_k$ CPU computation frequency, GU$_k$ local computation and UAV_S trajectory are optimized to maximize the average security computation capacity of the system.

Scheme 4: The security computation capacity of the system is maximized by optimizing UAV_S location, transmit power of GUs, jamming power, offloading ratio, UAV computing capacity and user association [36], in which UAV_S sends jamming signals to enhance security.

In Fig. 9, we can find that the security computation performance of the proposed scheme is much better than three benchmark schemes versus T. Compared with scheme 1, the proposed scheme has taken the advantages of NOMA transmission, which permits multi-users to share the same resource. Compared with scheme 2, the proposed scheme also optimizes the trajectory of UAV_S, indicating the importance of trajectory optimization in improving the security computation performance. Compared with scheme 3, the proposed scheme also optimizes the transmit power of GUs, indicating the importance of transmit power allocation in improving the security computation performance. Compared with scheme 4, the proposed scheme has optimized UAV_S trajectory, and UAV_S can fly to assist GUs in computing offloading tasks. Due to the UAVs location are fixed in scheme 4, the average security computation capacity will not change with the change of T.

Fig. 10 shows that the proposed scheme is superior to the benchmark schemes versus P_{max} in terms of the system average security computation performance. Compared with scheme 4, the proposed scheme has taken the advantage of NOMA transmission and optimizes the UAV trajectory, indicating the importance of UAV mobile trajectory optimization and NOMA transmission in improving the security computation

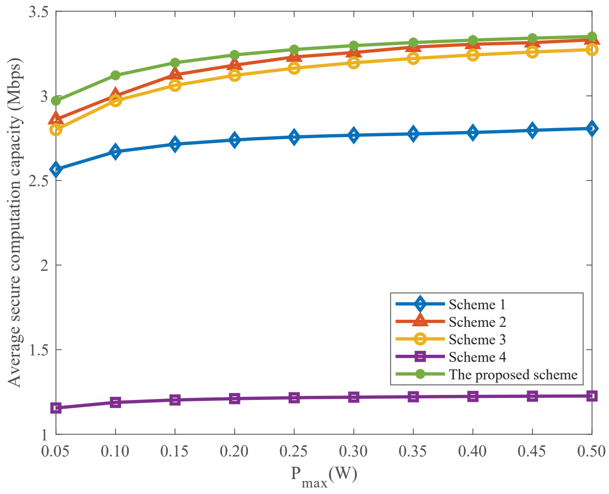


Fig. 10. The security computation performance comparison with different schemes versus P_{max}.

performance. Fig. 10 also proves that the proposed scheme is more advanced and effective than the other schemes.

VI. Conclusion

In this paper, we propose a secure communication scheme for NOMA-based UAV-MEC system towards a flying eavesdropper. Under the condition of minimum security computation requirements of each GU, we first study the worst security situation through mathematical derivation. Then, we maximize the average security computation capacity of the system via optimizing the varying channel relationship coefficient between the UAV_S and GUs, CPU computation frequency, transmit power, local computation and UAV_S trajectory. We utilize SCA and BCD methods to solve the proposed optimization problem in an iterative manner. The simulation results show that the proposed scheme performs better than the benchmark schemes in terms of the system security computation performance. In the future work, we will extend our work to more general system model by considering the hovering effects of the UAV, the statistical behavior of the channels and active eavesdropping behavior of UAV_E.

References

[1] A. Kiani and N. Ansari, "Edge computing aware NOMA for 5G networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1299-1306, Apr. 2018.

[2] R. Su, D. Zhang, R. Venkatesan, Z. Gong, C. Li, F. Ding, F. Jiang and Z. Zhu, "Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models," *IEEE Netw.*, vol. 33, no. 6, pp. 172-179, Nov.-Dec. 2019.

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

[4] Q. Pham, L. B. Le, S. Chung and W. Hwang, "Mobile edge computing with wireless backhaul: Joint task offloading and resource allocation," *IEEE Access*, vol. 7, pp. 16444-16459, 2019.

[5] W. Lu, P. Si, Y. Gao, H. Han, Z. Liu, Y. Wu and Y. Gong, "Trajectory and resource optimization in OFDM based UAV-powered IoT network," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1259-1270, Sep. 2021.

[6] M. Mozaffari, W. Saad, M. Bennis and M. Debbah, "Performance optimization for UAV-enabled wireless communications under flight time constraints," *GLOBECOM 2017 - 2017 IEEE Global Commun. Conf.*, 2017, pp. 1-6.

[7] Z. Yu, Y. Gong, S. Gong and Y. Guo, "Joint task offloading and resource allocation in UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3147-3159, Apr. 2020.

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

[9] Y. Du, K. Yang, K. Wang, G. Zhang, Y. Zhao and D. Chen, "Joint resources and workflow scheduling in UAV-enabled wirelessly-powered MEC for IoT systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10187-10200, Oct. 2019.

[10] Y. Wang, Z. -Y. Ru, K. Wang and P. -Q. Huang, "Joint deployment and task scheduling optimization for large-scale mobile users in multi-UAV-enabled mobile edge computing," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3984-3997, Sep. 2020.

[11] Y. Liu, S. Xie and Y. Zhang, "Cooperative offloading and resource management for UAV-enabled mobile edge computing in power IoT system," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12229-12239, Oct. 2020.

[12] Q. Hu, Y. Cai, G. Yu, Z. Qin, M. Zhao and G. Y. Li, "Joint offloading and trajectory design for UAV-enabled mobile edge computing systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1879-1892, Apr. 2019.

[13] J. Zhang, L. Zhou, F. Zhou, B. Seet, H. Zhang, Z. Cai and J. Wei, "Computation-efficient offloading and trajectory scheduling for multi-UAV assisted mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2114-2125, Feb. 2020.

[14] W. Liu, Y. Xu, D. Wu, H. Wang, X. Zheng and X. Chen, "Distributed energy-efficient and secure offloading in air-to-ground MEC networks," *EURASIP J. Adv. Signal Process.*, 2021.

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

[16] H. Lei, C. Zhu, K. -H. Park, W. Lei, I. S. Ansari and T. A. Tsiftsis, "On secure NOMA-based terrestrial and aerial IoT systems," *IEEE Internet Things J.*, doi: 10.1109/JIOT.2021.

[17] H. Lei, R. Gao, K. -H. Park, I. S. Ansari, K. J. Kim and M. -S. Alouini, "On secure downlink NOMA systems with outage constraint," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7824-7836, Dec. 2020.

[18] A. Abushattal, S. Althunibat, M. Qaraqe and H. Arslan, "A secure downlink NOMA scheme against unknown internal eavesdroppers," *IEEE Wireless Commun. Letters*, vol. 10, no. 6, pp. 1281-1285, June 2021.

[19] F. Cui, Y. Cai, Z. Qin, M. Zhao, and G. Y. Li, "Multiple access for mobile-UAV enabled networks: Joint trajectory design and resource allocation," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4980C4994, Jul. 2019.

[20] Z. Na, Y. Liu, J. Shi, C. Liu and Z. Gao, "UAV-supported clustered NOMA for 6G-enabled Internet of things: Trajectory planning and resource allocation," *IEEE Internet Things J.*, 2020.

[21] S. Li, B. Li and W. Zhao, "Joint optimization of caching and computation in multi-server NOMA-MEC system via reinforcement learning," *IEEE Access*, vol. 8, pp. 112762-112771, 2020.

[22] Y. Wu, K. Ni, C. Zhang, L. P. Qian and D. H. K. Tsang, "NOMA-assisted multi-access mobile edge computing: A joint optimization of computation offloading and time allocation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12244-12258, Dec. 2018.

[23] F. Guo, H. Zhang, H. Ji, X. Li and V. C. M. Leung, "Joint trajectory and computation offloading optimization for UAV-assisted MEC with NOMA," *IEEE INFOCOM 2019 - IEEE Conf. Computer Commun. Workshops (INFOCOM WKSHPS)*, 2019, pp. 1-6.

[24] X. Zhang, J. Zhang, J. Xiong, L. Zhou and J. Wei, "Energy-efficient Multi-UAV-enabled multiaccess edge computing incorporating NOMA," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5613-5627, Jun. 2020.

[25] I. Budhiraja, N. Kumar, S. Tyagi and S. Tanwar, "Energy consumption minimization scheme for NOMA-based mobile edge computation networks Underlaying UAV," *IEEE Systems J.*, 2021.

[26] N. Rupasinghe, Y. Yapici, I. Gvenc, H. Dai and A. Bhuyan, "Enhancing physical layer security for NOMA transmission in mmWave drone networks," *2018 52nd Asilomar Conf. Signals, Systems, and Computers.*, 2018, pp. 729-733.

[27] G. Mu, "Security efficiency maximization for multi-UAVCaided network with mobile edge computing," *Front. Comput. Sci.*, 3:691854. doi: 10.3389/fcomp.2021.

[28] A. Singh, M. R. Bhatnagar and R. K. Mallik, "Physical layer security of a multiantenna-based CR network with single and multiple primary

users," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11011-11022, Dec. 2017.

[29] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photonics J.*, vol. 11, no. 1, pp. 1-14, Feb. 2019.

[30] Z. Sheng, H. D. Tuan, A. A. Nasir, T. Q. Duong and H. V. Poor, "Secure UAV-enabled communication ssing HanCKobayashi signaling," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 2905-2919, May 2020.

[31] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li and F. R. Yu, "Secure transmission via beamforming optimization for NOMA networks," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 193-199, Feb. 2020.

[32] X. Sun, W. Yang and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1884-1897, Mar. 2020.

[33] B. Duo, J. Luo, Y. Li, H. Hu and Z. Wang, "Joint trajectory and power optimization for securing UAV communications against active eavesdropping," *China Commun.*, vol. 18, no. 1, pp. 88-99, Jan. 2021.

[34] Y. Xu, T. Zhang, D. Yang, Y. Liu and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 573-588, Jan. 2021.

[35] S. Li, B. Duo, M. D. Renzo, M. Tao and X. Yuan, "Robust secure UAV communications with the aid of reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402-6417, Oct. 2021.

[36] Y. Zhou, C. Pan, P. Yeoh, K. Wang, M. Elkashlan, B. Vucetic and Y. Li, "Secure communications for UAV-enabled mobile edge computing systems," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 376-388, Jan. 2020.

[37] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao and Y. Gong, "Resource and trajectory optimization for secure communications in Dual-UAV-MEC systems," vol. 18, no. 4, pp. 2704-2713, April, 2022.

[38] *Enhanced LTE support for aerial vehicles.* Accessed: Jul. 16, 2017. [Online]. Available:ftp://www.3gpp.org/specs/archive/36_series/36.777

[39] B. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Operations Research*, vol. 26, no. 4, pp. 681–683, 1978.

[40] S. Boyd and L. V andenberghe, Convex optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.