EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Secrecy Offloading Analysis of NOMA-based UAV-aided MEC in IoT Networks with Imperfect CSI and SIC

Anh-Nhat Nguyen[1,*], Tung-Son Ngo[1], Ngoc-Anh Bui[1], Phuong-Chi Le[1], and Manh-Duc Hoang[1]

[1] ICT Department, FPT University, Hanoi 10000, Vietnam

Abstract

Nonorthogonal multiple access (NOMA) increases spectrum efficacy by permitting multiple devices to share link resources. It can be used to provide convenient offloading computing services for edge devices (EDs) in unmanned aerial vehicle (UAV) and mobile-edge computing (MEC) networks. However, due to the Line-of-Sight (LoS) of UAV transmission, NOMA-based UAV-MEC systems are susceptible to information eavesdropping. In this paper, we investigate a secure offloading model for a NOMA-based UAV-aided MEC in Internet of Things (IoT) network concerning an aerial eavesdropper (EAV) that considers imperfect channel state information (ipCSI) and imperfect successive interference cancellation (ipSIC). We derive the expression of secrecy successful computation probability (SSCP) across the entire system to analyze EAV's impact on the performance of the NOMA-based UAV-aided MEC in IoT networks. In addition, we present a formulation of an optimization problem that optimizes the SSCP through the optimization of the UAV's altitude and location, as well as the offloading ratio. To address this issue, a genetic algorithm (GA)-based approach was implemented. The results of our study were corroborated by the Monte Carlo simulations, which assessed system performance by considering multiple system parameters including the UAV's location, altitude, average transmit signal-to-noise ratio (SNR), and offloading ratio.

Received on 02 02 2024 accepted on 10 06 2024; published on 23 07 2024

Keywords: nonorthogonal multiple access, unmanned aerial vehicle, mobile-edge computing, physical-layer security, Internet of Things

doi:10.4108/eetsis.4664

1. Introduction

The demand for computation capacity increases due to the exponential growth of Internet of Things (IoT) devices and their associated applications, including autonomous driving, augmented reality, virtual reality, and agriculture monitoring [1–3]. In response to this need, researchers and professionals from both academic and industrial sectors examined a novel computational methodology called mobile-edge computing (MEC). In this case, the edge device (ED) can delegate their responsibilities to the MEC servers, which are typically located at the network's edge. Furthermore, it facilitates energy consumption and reduces latency by enabling EDs to communicate with MEC servers over short distances [4–6].

Unmanned aerial vehicle (UAV) with great mobility and low cost can immediately provide an efficient emergency and auxiliary means for UAV deployment in remote locations [7, 8]. UAV equipped with MEC servers can dynamically improve wireless link quality and provide effective offloading compute service for ED [9–11]. Liu *et al.* investigated the resource management and cooperative offloading calculation scheme in the UAV-aided MEC architecture under the requirements of EDs and variable channels [9]. Hu *et al.* provided an effective technique for obtaining the UAV-MEC system's optimum solution [10]. To improve computational efficiency in the multiple UAV-aided MEC system, Zhang *et al.* developed an optimal approach [11].

*Corresponding author. Email: nhatna3@fe.edu.vn

On the other hand, nonorthogonal multiple access (NOMA) allows many EDs to share link resources, and successive interference cancellation (SIC) can be utilized to decode signals in NOMA transmission. As a result, NOMA transmission can achieve better spectrum use and throughput. Because of these benefits, NOMA is commonly used in UAV-aided MEC networks to provide flexible and convenient compute offloading services for large-scale access EDs [12–14]. Na *et al.* presented a collaborative optimization approach that employs clustered NOMA to reduce inter-channel interference while increasing the overall uplink rate [12]. Zhang *et al.* hypothesized that the UAV-aided MEC framework with NOMA can reduce offloading energy consumption and overcome device computing energy limitations [13]. Budhiraja *et al.* presented a NOMA-based uplink transmission technique that not only supports large-scale access but also improves the transmission quality of the UAV-aided MEC system [14].

It can be demonstrated that NOMA transmission can provide EDs in UAV-aided MEC networks with flexible and convenient calculation services. However, malevolent users can readily eavesdrop on offloading information, posing serious security vulnerabilities to NOMA-basedUAV-aided MEC networks. Physical-layer security (PLS) ensures high-quality, secure communication by employing wireless channels and transmission mechanisms effectively [15–18]. The protected zone technique was examined by Rupasinghe *et al.* to improve the PLS of UAV-based communication networks [15]. Cao *et al.* presented an anti-eavesdropping approach in NOMA networks using beamforming [16]. Sun *et al.* demonstrated that NOMA's UAV communication not only increases coverage but also enhances security [17]. To prevent eavesdroppers from collecting useful offloading information, Xu *et al.* investigated the security optimization strategy in the UAV-aided MEC networks [18]. UAV eavesdroppers will have significantly better channel conditions due to Line-of-Sight (LoS) transmission than ground eavesdroppers, which are positioned at fixed sites in existing works. As a result, flying UAVs can readily eavesdrop on the information.

This study investigates the performance of secrecy offloading in IoT networks that utilize NOMA-based UAV-aided MEC across Nakagami-m fading channels. Furthermore, we take into account the likelihood of LoS and non-LoS (NLoS) scenarios in wireless channels between UAV and ground devices. In addition, we examine the performance of the system in terms of secrecy offloading, taking into account the presence of imperfect channel state information (ipCSI) and imperfect successive interference cancellation (ipSIC) between the UAV and the EDs. Finally, we propose an optimization problem to enhance the secrecy performance of the system. The following are our paper's main contributions:

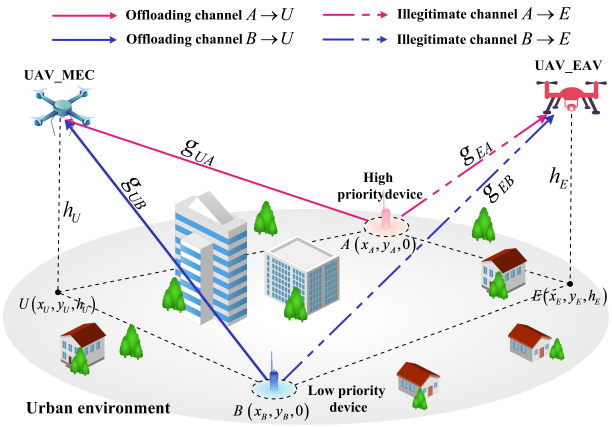

Figure 1. System model for a NOMA-based UAV-aided MEC in IoT network.

- We investigate a NOMA-based UAV-aided MEC in IoT networks in the presence of a passive flying eavesdropper. In addition, we take into account the use of ipCSI and ipSIC to ensure precise assessments of the system's secrecy offloading performance in real-work scenarios. Accordingly, we propose a system protocol to ensure effective secrecy offloading performance.
- We derive closed-form expressions of secrecy successful computation probability (SSCP) for the entire system. In addition, we formulated a problem for maximizing SSCP by optimizing the location and altitude of UAV and also offloading ratio. The problem was solved using a genetic algorithm (GA).
- To confirm the efficacy of our system, numerical results such as average transmit signal-to-noise ratio (SNR), location and altitude of UAV; and offloading ratio of ED are used to evaluate the system's secrecy offloading performance.

The remainder of this paper is organized as follows. In Section 2, the system model, the communication protocol are introduced. In Section 3, the SSCP and optimization problem are analyzed. In Section 4, numerical results are presented and discussed. Finally, conclusions are presented in Section 5.

2. System Model and Communication Protocol

2.1. System and channel model

We investigate a NOMA-based UAV-aided MEC in an IoT network with two EDs denoted by A and B, where A is a high-priority device and B is a low-priority device, as illustrated in Fig. 1. Due to their limited resources,

these two devices attempt to transfer confidential duties to the UAV-equipped MEC server, denoted by U_M, in the presence of a passive flying eavesdropper, denoted by U_E. Note that we assume that the position of U_E has been determined; all devices with a single antenna operate in half-duplex mode and are located in an urban environment.

Without loss of generality, we utilized a 3D Cartesian coordinate system, we use $U_M\left(x_{U_M}, y_{U_M}, h_{U_M}\right)$, where $h_{U_M} > 0$; $A\left(x_A, y_A, 0\right)$; $B\left(x_B, y_B, 0\right)$; and $U_E\left(x_{U_E}, y_{U_E}, h_{U_E}\right)$, where $h_{U_E} > 0$. The likelihood of LoS/NLoS is affected by the elevation angles of UAVs. The straight-line distance and angle of elevation between EDs and UAVs can be calculated following

$$\begin{cases} d_{ab} = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2 + (h_b - h_a)^2}, \\ \theta_{ab} = (180/\pi)\arcsin\left(h_b/d_{ab}\right), \end{cases} \tag{1}$$

where $a \in (A, B)$, $b \in (U_M, U_E)$. Then the probability of LoS/NLoS path between a and b is

$$\begin{cases} \mathcal{P}_{ab}^{LoS} = \frac{1}{1+\omega e^{-\varpi(\theta_{ab}-\omega)}}, \\ \mathcal{P}_{ab}^{NLoS} = 1 - \mathcal{P}_{ab}^{LoS}, \end{cases} \tag{2}$$

where ϖ and ω are constant values that vary according to the surrounding environment [19]. Thus the path loss in each case is given as [4]

$$\mathcal{L}_{ab}^{\xi} = \kappa_{\xi}(4\pi f_c d_{ab}/c)^{\sigma}, \tag{3}$$

where $\xi \in (LoS, NLoS)$, f_c is the carrier frequency, c is the speed of light, κ_{ξ} is the excessive path losses of the LoS/NLoS propagation, and σ is the path-loss exponent. The average path loss of LoS/NLoS is calculated as follows [5]:

$$\bar{\mathcal{L}}_{ab} = \mathcal{P}_{ab}^{LoS}\mathcal{L}_{ab}^{LoS} + \mathcal{P}_{ab}^{NLoS}\mathcal{L}_{ab}^{NLoS}. \tag{4}$$

The channel from the $a \to b$ is denoted by g_{ab}. Obtaining perfect CSI (pCSI) in wireless systems is difficult due to mistakes in channel estimation and response delay. Hence, the channel coefficient is expressed as follows:

$$g_{ab} = \hat{g}_{ab} + e_{ab}, \tag{5}$$

where $\hat{g}_{ab}$ is the estimated channel coefficient and $e_{ab} \sim \mathcal{CN}\left(0, \delta_{ab}\right)$ denotes the channel estimation error, which can be approximated as a Gaussian distribution, where the parameter δ_{ab} indicates the quality of channel estimation. In this paper, it is assumed that the channel estimation error variance δ_{ab} is constant [20]. We assume that all channels are modeled as Nakagami-m fading channels and that the channel coefficients are random variables (RVs) distributed following the Nakagami-m model [3]. Thus the cumulative distribution function (CDF) and probability density function (PDF) of channel are respectively expressed as:

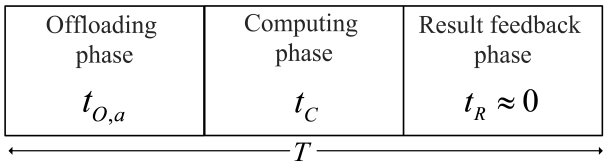

Figure 2. Time flowchart of the considered NOMA-based UAV-aided MEC in IoT networks.

$$F_{|\hat{g}_{ab}|^2}(y) = 1 - e^{-\frac{my}{\lambda_{ab}}}\sum_{s=0}^{m-1}\frac{1}{s!}\left(\frac{my}{\lambda_{ab}}\right)^s, \tag{6}$$

$$f_{|\hat{g}_{ab}|^2}(y) = \frac{m^m y^{m-1}}{\lambda_{ab}^m (m-1)!}e^{-\frac{my}{\lambda_{ab}}}, \tag{7}$$

where $|\hat{g}_{ab}|^2$ is the channel power gain and λ_{ab} denoted is an average channel gain. Assume that all EDs execute the same task of length L (bits) and are classified [5]. The capacity offload of A and B can thus be written as follows:

$$C_a = \beta_a L, \tag{8}$$

where β_a is the offloading ratio, $0 \le \beta_a \le 1$.

2.2. Communication protocol

In this subsection, we describe the proposed system's communication protocol. Fig 2 depicts the protocol's time flowchart and is described as follows.

- In the first phase, t_O: a based on uplink NOMA to offload L bits to U_M. Thus, the received signal at U_M is as follows:

$$y_{U_M} = \sqrt{\frac{\rho_A P}{\bar{\mathcal{L}}_{AU_M}}}\left(\hat{g}_{AU_M} + e_{AU_M}\right)x_A + \sqrt{\frac{\rho_B P}{\bar{\mathcal{L}}_{BU_M}}}\left(\hat{g}_{BU_M} + e_{BU_M}\right)x_B + n_{U_M}, \tag{9}$$

  where x_A and x_B are the offloaded signal to A and B, respectively; P is the transmit power of EDs; ρ_A and ρ_B are the power allocation coefficient, $\rho_A > \rho_B, \rho_A + \rho_B = 1$; $n_{U_M} \sim \mathcal{CN}\left(0, N_0\right)$ is additive white Gaussian noise (AWGN). U_M decodes x_A based on SIC [21]. Therefore, the received signal-to-interference-plus-noise ratios (SINRs) at U_M for detecting x_A is expressed as follows:

$$\gamma_{AU_M} = \frac{\gamma_1\left|\hat{g}_{AU_M}\right|^2}{\gamma_2\left|\hat{g}_{BU_M}\right|^2 + \gamma_3}, \tag{10}$$

where $\gamma_I = \frac{P}{N_0}$, $\gamma_1 = \frac{\rho_A \gamma_I}{\bar{\mathcal{L}}_{BU_M}}$, $\gamma_2 = \frac{\rho_A \gamma_I}{\bar{\mathcal{L}}_{BU_M}}$, $\gamma_3 = \gamma_1 \delta_{BU_M} + \gamma_2 \delta_{BU_M} + 1$. Considering the effect of ipSIC, the residual x_A from A is considered interfering information, then the received SINRs at U_M for detecting x_B can be represented as

$$\gamma_{BU_M} = \frac{\gamma_2 \left|\hat{g}_{BU_M}\right|^2}{\zeta \gamma_1 \left|\hat{g}_{AU_M}\right|^2 + \gamma_4}, \tag{11}$$

where $\zeta, 0 \le \zeta \le 1$ denotes the level of residual signal from A ($\zeta = 0$ corresponds to perfect SIC (pSIC)). Then, the instantaneous legitimate channel capacity $a \to U_M$ link is formulated as follows:

$$C_{aU_M} = W \log_2 \left(1 + \gamma_{aU_M}\right), \quad a \in (A, B), \tag{12}$$

where W is the bandwidth. Hence, the time offloading from a^* to U_M is given by

$$t_{O,a} = \frac{C_a}{C_{aU_M}}. \tag{13}$$

Similarly, the expression of signal received at U_E is as follows:

$$y_{U_E} = \sqrt{\frac{\rho_A P_E}{\bar{\mathcal{L}}_{AU_E}}} \left(\hat{g}_{AU_E} + e_{AU_E}\right) x_A + \sqrt{\frac{\rho_B P_E}{\bar{\mathcal{L}}_{BU_E}}} \left(\hat{g}_{BU_E} + e_{BU_E}\right) x_B + n_{U_E}, \tag{14}$$

where $n_{U_E} \sim \mathcal{CN}(0, N_E)$ is AWGN at U_E. We have assumed that the eavesdropper U_E is able to successfully decode the signals from the two EDs [22]. Therefore, the SINR to detect x_A and x_B at U_E is given by

$$\gamma_{AU_E} = \frac{\gamma_5 \left|\hat{g}_{AU_E}\right|^2}{\gamma_6 \left|\hat{g}_{BU_E}\right|^2 + \gamma_7}, \tag{15}$$

$$\gamma_{BU_E} = \frac{\gamma_6 \left|\hat{g}_{BU_E}\right|^2}{\gamma_8}, \tag{16}$$

where $\gamma_E = \frac{P_E}{N_E}$, $\gamma_5 = \frac{\rho_A \gamma_E}{\bar{\mathcal{L}}_{AU_E}}$, $\gamma_6 = \frac{\rho_B \gamma_E}{\bar{\mathcal{L}}_{BU_E}}$, $\gamma_7 = \gamma_5 \delta_{AU_E} + \gamma_6 \delta_{BU_E} + 1; \gamma_8 = \gamma_6 \delta_{BU_E} + 1$. Thus, the instantaneous illegal channel capacity $a \to U_E$ link is formulated as follows:

$$C_{aU_E} = W \log_2 \left(1 + \gamma_{aU_E}\right), \tag{17}$$

- In the second phase, t_C: U_M computes the tasks that have been offloaded. The time necessary to complete the computation for the number of task bits at U_M is as follows:

$$t_C = \frac{(C_A + C_B)\,\tau}{f_{U_M}^{MEC}}, \tag{18}$$

where τ is the number of CPU cycles required to run the computation for one input bit and $f_{U_M}^{MEC}$ is the MEC operating frequency at U_M.

- In the third phase, t_R: U_M send the resulting computation data to the a. Latencies for returning results from U_M to a are overlooked because the returned results are much smaller than the offloaded data [23].

3. Performance Analysis

3.1. Secrecy successful computation probability (SSCP)

In this subsection, we presents the secrecy and offloading performance of the system under consideration in terms of SSCP [24], denoted by S. The S is defined as the probability that all offloading tasks are completed within the maximum permissible system latency T_{th} and the corresponding secrecy capacity is greater than a predefined data rate threshold R_a. Thus, the S of the entire system is calculated as follows:

$$S = \Pr\left(t_{O,A} < T_{th}, t_{O,B} < T_{th}, C_A^{Sec} > R_A, C_B^{Sec} > R_B\right), \tag{19}$$

where $T_{th} = T - t_C$ and $R_a = \frac{C_a}{T_{th}}$ [5]; and the instantaneous secrecy capacity of a wireless transmission from a to U_M in the presence of a passive flying Eav is defined as [2]

$$C_a^S = \left[C_{aU_M} - C_{aU_E}\right]^+ = \begin{cases} W \log_2 \left(\frac{1+\gamma_{aU_M}}{1+\gamma_{aU_E}}\right), & \gamma_{aU_M} > \gamma_{aU_E} \\ 0, & \gamma_{aU_M} \le \gamma_{aU_E} \end{cases}, \tag{20}$$

Theorem 1. The closed-form expression for the SSCP of the entire system for UAV-aided NOMA-MEC under quasi-static Nakagami-m fading is as follows:

$$S = \Phi_1 \sum_{q=1}^{Q} \sum_{o=1}^{O} \Phi_2^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)} \Phi_3^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)} \left[1 - \Phi_4^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)} \Phi_7^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)} \left(1 - \Phi_8^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)}\right)\right], \tag{21}$$

where O and Q are the complexity versus accuracy trade-off coefficient [25]; Φ_1, $\Phi_2^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)}$, $\Phi_3^{\left(\varphi_q, \omega_o^{(\varphi_q)}\right)}$,

$\Phi_4^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$, Φ_5, $\Phi_6^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$, $\Phi_7^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$, $\Phi_8^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$ are defined as follows:

$$\Phi_1 = \frac{\pi^2}{4QO(m-1)^2!}\left(\frac{m}{\lambda_{BU_M}}\right)^m\left(\frac{m}{\lambda_{AU_M}}\right)^m, \tag{22}$$

$$\Phi_2^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \sqrt{1-\zeta_q{}^2}\sqrt{1-\zeta_o{}^2}\left(\varphi_q\omega_o^{(\varphi_q)}\right)^{m-1}, \tag{23}$$

$$\Phi_3^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = e^{-\frac{m\omega_o^{(\varphi_q)}}{\lambda_{AU_M}}}\omega_q{}^{\frac{m(\varphi_q)^2}{\lambda_{BU_M}}}\frac{\left(\Xi_2^{(\varphi_q)}-\Xi_1^{(\varphi_q)}\right)}{\omega_q\ln^2\left(\omega_q\right)}, \tag{24}$$

$$\Phi_4^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = e^{-\frac{m\Xi_5^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}}{\lambda_{BU_E}}}\sum_{i_1=0}^{m-1}\frac{1}{i_1!}\left(\frac{m\Xi_5^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}}{\lambda_{BU_E}}\right)^{i_1}, \tag{25}$$

$$\Phi_5 = \frac{1}{(m-1)!}\left(\frac{m}{\lambda_{BU_E}}\right)^m, \tag{26}$$

$$\Phi_6^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \frac{(m+i_2-1)!}{i_2!\,(s-i_2)!}\left(\frac{\gamma_7}{\gamma_6}\right)^{s-i_2}\left(\frac{m}{\lambda_{AU_E}}\Xi_3^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}\right)^s, \tag{27}$$

$$\Phi_7^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \left(\Psi_1^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}\right)^{-(m+i_2)}e^{-\frac{m\Xi_4^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}}{\lambda_{AU_E}}}, \tag{28}$$

$$\Phi_8^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = e^{-\Psi_2^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}}\sum_{i_3=0}^{m+i_2-1}\frac{1}{i_3!}\left(\Psi_2^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}\right)^{i_3} \tag{29}$$

where $\theta_A = 2^{\frac{C_A}{WT_{th}}}-1$, $\theta_B = 2^{\frac{C_B}{WT_{th}}}-1$, $\varphi_A = 2^{\frac{R_A}{W}}$, $\varphi_B = 2^{\frac{R_B}{W}}$; $\Xi_1^{(\varphi_q)}$, $\Xi_2^{(\varphi_q)}$, $\Xi_3^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$, $\Xi_4^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$, and $\Xi_5^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}$ are defined as follows:

$$\Xi_1^{(\varphi_q)} = \frac{\theta_A\left(\gamma_2\varphi_q+\gamma_3\right)}{\gamma_1}, \tag{30}$$

$$\Xi_2^{(\varphi_q)} = \frac{\gamma_2\varphi_q-\theta_B\gamma_4}{\theta_B\zeta\gamma_1}, \tag{31}$$

$$\Xi_3^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \left(\frac{\gamma_1\omega_o^{(\varphi_q)}}{\gamma_2\varphi_q+\gamma_3}+1-\varphi_A\right)\frac{\gamma_6}{\varphi_A\gamma_5}, \tag{32}$$

$$\Xi_4^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \left(\frac{\gamma_1\omega_o^{(\varphi_q)}}{\gamma_2\varphi_q+\gamma_3}+1-\varphi_A\right)\frac{\gamma_7}{\varphi_A\gamma_5}, \tag{33}$$

$$\Xi_5^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \left(\frac{\gamma_2\varphi_q}{\zeta\gamma_1\omega_o^{(\varphi_q)}+\gamma_4}+1-\varphi_B\right)\frac{\gamma_8}{\varphi_B\gamma_6}, \tag{34}$$

$$\Psi_1^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \frac{m\Xi_3^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}}{\lambda_{AU_E}}+\frac{m}{\lambda_{BU_E}}, \tag{35}$$

$$\Psi_2^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)} = \Psi_1^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}\Xi_5^{\left(\varphi_q,\omega_o^{(\varphi_q)}\right)}, \tag{36}$$

where $\zeta_q = \cos\left(\frac{\pi(2q-1)}{2Q}\right)$, $\omega_q = \frac{(\zeta_q+1)}{2}$, $\varphi_q = -\ln^{-1}\left(\omega_q\right)$, $\zeta_o = \cos\left(\frac{\pi(2o-1)}{2O}\right)$, and $\omega_o^{(\varphi_q)} = \frac{(\zeta_o+1)\left[\Xi_2^{(\varphi_q)}-\Xi_1^{(\varphi_q)}\right]}{2}+\Xi_1^{(\varphi_q)}$.

Proof. The proof is given in F. □

3.2. Optimization

To improve system performance, we optimize parameters such as UAV location, height, and offloading ratio of two clusters of EDs to maximize secrecy and successful computation. To accomplish this, we define and solve the SSCP maximization problem using an algorithm that is based on GA.

SSCP maximization problem:

$$\begin{aligned}(\text{P1}):\ &\underset{x_U,y_U,h_U,\beta}{\text{maximize}} && S\\ &\text{subject to} && 0\le x_U\le x_U^{\max}, && (37a)\\ &&& 0\le y_U\le y_U^{\max}, && (37b)\\ &&& 0\le h_U\le h_U^{\max}, && (37c)\\ &&& 0\le\beta\le 1, && (37d)\end{aligned}$$

where constraints (37a) and (37b) represent conditions on the UAV's projected location on the ground, constraint (37c) imposes conditions on the altitude of the UAV and constraint (37d) offloading ratio of the ED.

To solve the problem (37) with multiple constraints, we propose the GA [26]. The GA stands out as a widely used optimization approach owing to its adaptability and straightforward implementation. It draws inspiration from the principles of natural evolution, wherein individuals with the highest fitness are chosen to produce the next generation's offspring. The descendants are likely to enhance their attributes and increase their chances of survival if their parents exhibit superior fitness compared to others in the same generation. This iterative reproductive cycle continues until the most optimal individuals are identified. The process is as follows:

- Initialize Population: Generate a population of $\mathcal{N}$ individuals, where each individual represents

a potential solution, $\mathcal{E}_i\left(x_{U_M}, y_{U_M}, h_{U_M}, \beta\right), i \in (1, \mathcal{N})$.

- Fitness Function: Evaluate the fitness of each individual in the population. The fitness function measures how well an individual satisfies the optimization criteria, $\mathcal{F} = 1 - S\left(\mathcal{E}_i\right)$.
- Selection: Select individuals from the population based on their fitness. Using the roulette wheel selection method should increase the likelihood of selecting people with higher fitness values.
- Crossover: Combine genetic material from selected parents to create offspring. This emulates the crossover or recombination process in biological reproduction.
- Mutation: Introduce random changes to the genetic material of some individuals. This maintains genetic diversity and introduces new traits.
- Convergence: The algorithm iterates until the fitness value does not change. This means the algorithm generates kids that are identical to their parents, finding the best solution. The algorithm finishes after a certain period or number of generations.

Algorithm 1 presents the overall SSCP maximization based on GA (SSCPMax-GA) algorithm used for our proposed system model. The complexity of SSCPMax-GA typically depends on the population size $\mathcal{N}$, the number of generations $\mathcal{I}$, and the computational cost of evaluating fitness functions $\mathcal{F}$. Thus, the worst-case complexity of the SSCPMax-GA was given by $O(\mathcal{I}\mathcal{N}\mathcal{F})$.

4. Numerical result

In this section, we describe the numerical results used to validate the analytical expression of the SSCP described in Section 3 for the NOMA-based UAV-aided MEC in IoT network. Specifically, we consider the following system parameters in all simulations, shown in Table 1 [4, 5].

The impact of the average SNR, γ_I, the channel estimation error δ, and the level of residual signal, ζ on the SSCP of the entire system is depicted in Fig. 3. We can observe that the Monte Carlo simulation and our analysis have a powerful match, confirming the accuracy of our proposed model. In this figure, we compare SSCP for two different scenarios: $(\delta, \zeta) = (0, 0)$ i.e. pCSI-pSIC; and $(\delta, \zeta) = ([0.1, 0.3, 0.5], [0.1, 0.3, 0.5])$ i.e. ipCSI-ipSIC. As we can see, the case $(\delta, \zeta) = (0, 0)$ corresponds to the best system performance because this is the ideal case that the system wants to achieve. However, in practice, it may be difficult to achieve this ideal situation due to the limitations

Algorithm 1 SSCPMax-GA

Require: $\mathcal{N}, \mathcal{I}, S$, and constraint conditions
Ensure: x_U^*, y_U^*, h_U^* and β^*

function SSCPMAX
  $j = 1, \mathcal{I}$
  Initialize the population: $\mathcal{E}_i\left(x_{U_M}, y_{U_M}, h_{U_M}, \beta\right)$
  Check and modify the initial population
  while $i <= \mathcal{I}$ **do**
    Calculate the fitness value: $\mathcal{F} = 1 - S\left(\mathcal{E}_i\right)$.
    Store the individual with the highest fitness value
    Select the parents for next generation by roulette wheel selection methodology
    for all pairs of parents in the poll **do**
      Generate offspring through crossover operator
      for all generated offsprings **do**
        if mutation probability holds **then**
        end if
      end for
    end for
    Check and modify the next generation
    Calculate the fitness and leave the best individuals
    $i++$
  end while
  Get $x_{U_M}^*, y_{U_M}^*, h_{U_M}^*, \beta^*$
end function

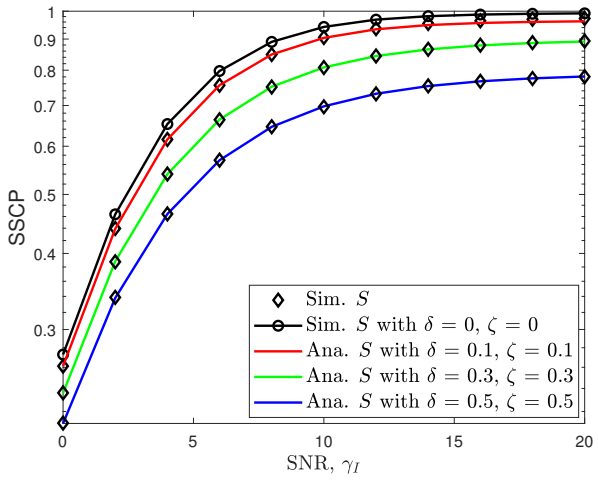

Figure 3. Impact of average transmit SNR, (γ_I) on SSCP of the entire system with different δ and ζ.

of wireless communication. Therefore, for the system under investigation, we are more interested in the ipCSI-ipSIC case. As the value of δ and ζ increases, it is clearly the case that ipCSI-ipSIC is detrimental to

Table 1. Simulation parameter.

Para.	Val.	Para.	Val.	Para.	Val.	Para.	Val.
(x_A, y_A)	(40, 0) (m)	P	[0, ..., 20] (dB)	ω	0.1581	$f_{U_M}^{MEC}$	10^4 (Hz)
(x_B, y_B)	(0, 50) (m)	P_E	10 (dB)	ω	9.6177	τ	1
$\left(x_{U_E}, y_{U_E}, h_{U_E}\right)$	(100, 100, 80) (m)	T	0.5 (s)	κ_{LoS}	1	$Q = O$	10^3
x_{U_M}	[0, ..., 80] (m)	W	10^5 (bps)	κ_{NLoS}	20	L	10^3 (bit)
y_{U_M}	[0, ..., 80] (m)	ρ_A	0.75	c	3.10^8 (m/s)	$\mathcal{N}$	150
h_{U_M}	[0, ..., 200] (m)	σ	2	f_c	10^4 (Hz)	$\mathcal{I}$	100

Table 2. Result of Algorithm 1.

P (dB)	x_U^* (m)	y_U^*(m)	h_U^* (m)	β^*
0	36.000069746984790	35.000521950444465	55.000017199247615	0.799999155070419
5	34.000369721641450	35.615000973341694	55.000929218186556	0.799432628372572
10	34.000010952722680	37.035463582606230	55.000003243601704	0.799996550616451
15	36.000022332516990	35.857151485044724	53.000003178133156	0.899999378299348
20	36.001831141447080	35.862911997892350	53.000505834925136	0.899974865333359

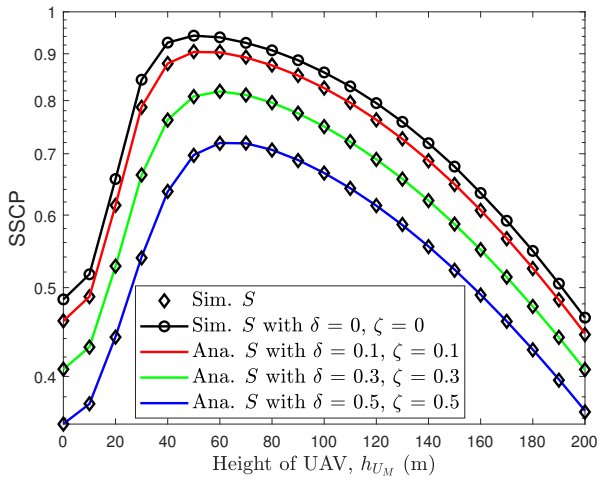

Figure 4. Impact of altitude of UAV, (h_U) on SSCP of the entire system with different number of ED in two clusters.

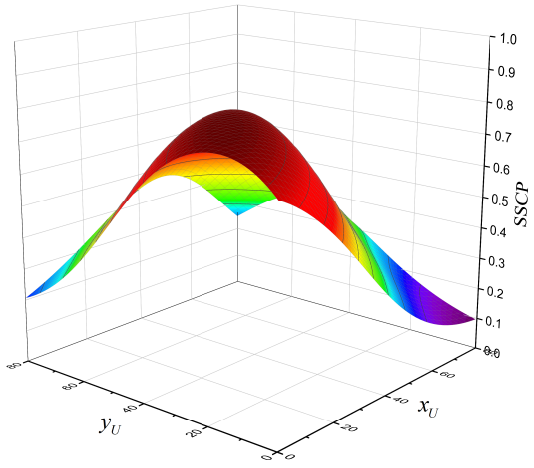

Figure 5. Impact of the location of UAV, (x_{U_M}, y_{U_M}) on SSCP of the entire system.

SSCP. In addition, we can see that as we increase the generation power at ED, the SSCP increases accordingly. This can be explained by the fact that when the ED's transmit power increases, the ED will have more energy for offloading tasks onto the UAV, which also increases the legal capacity, making it difficult for eavesdroppers to eavesdrop on information.

Fig. 4 depicts of the altitude of UAV, h_U on the SSCP of the entire system. We can also observe that the UAV will have an altitude to enhance secrecy offloading performance; this could explain why the UAV's altitude is low, the probability of encountering NLoS is greater than the probability of encountering LoS owing to urban obstructions. The increased altitude of the UAV enhances performance since the likelihood of encountering a LoS between the UAV and the ED is larger than the likelihood of encountering an NLoS. Nonetheless, as altitude grows, so does the communication distance between the UAV and the ED, increasing the pass loss of the UAV-ED links and, as a result, decreasing performance. As a result, there will be an altitude that maximizes the effectiveness of secrecy offloading.

Fig. 5 shows the impact of the location of UAV, (x_{U_M}, y_{U_M}) on the SSCP of the entire system. Beyond addressing the altitude concern of the UAV, it's crucial to factor in the UAV's position for improved communication with the ED. We identify optimal coordinates, denoted as $x_{U_M}^*$ and $y_{U_M}^*$, where system performance is optimized. This implies that the UAV strategically

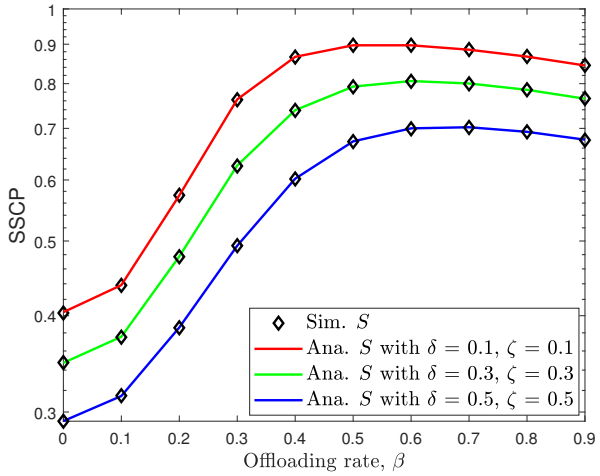

Figure 6. Impact of the task offloading ratio of ED, β on SSCP of the entire system.

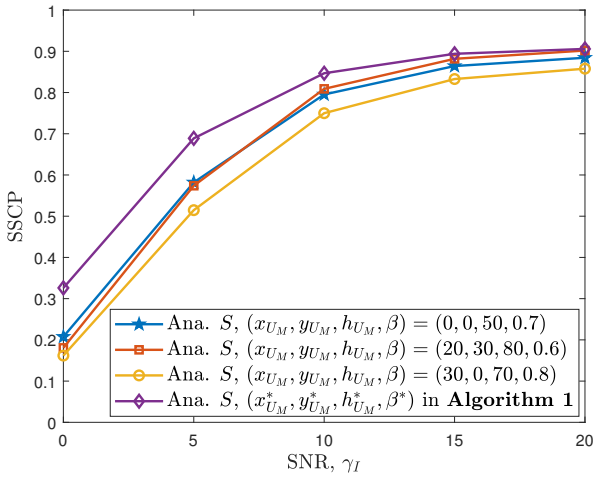

Figure 7. Compare security offloading performance of system with and without using optimization algorithms.

selects a location to enhance communication with the EDs, thereby maximizing the SSCP. This represents a notable capability of UAV.

Fig. 6 depicts of the task offloading ratio of ED, β on the SSCP of the entire system. As we have shown EDs all perform the same task of length L (bits). Therefore, there will be a ratio β that divides these L bits among the two EDs performing offloading. We can easily see that there is an optimal task offloading ratio that maximizes SSCP. This can be explained that the two EDs will self-allocate the most suitable task offloading ratio to offload their tasks onto the UAV. This also demonstrates fairness among EDs.

Fig. 7 depicts the impact of UAV location and altitude; and the task offloading ratio of ED, $\left(x_{U_M}, y_{U_M}, h_{U_M}, \beta\right)$ to the SSCP of the entire system. In this result, we substitute the optimal values found from solving the optimization problem proposed above **Algorithm 1**. We compare SSCP$\left(x^*_{U_M}, y^*_{U_M}, h^*_{U_M}, \beta^*\right)$ with fixed-value SSCP$\left(x_{U_M}, y_{U_M}, h_{U_M}, \beta\right)$, where the values of $\left(x^*_{U_M}, y^*_{U_M}, h^*_{U_M}, \beta^*\right)$ are taken from the results of Algorithm 1 comparing with the cases of fixed location and height for the UAV as well as the ED task offload ratio, note that these fixed values are qualitative in nature. In this paper, we consider changing the transmission power of ED to find the optimal $x^*_{U_M}$, $y^*_{U_M}$, $h^*_{U_M}$, and β^* that maximize SSCP. The results show that, by applying the SSCPMax-GA algorithm to give the optimal value, the secret offload performance is best compared to if we manually fixed these parameters for the system, the results are shown in Table 2.

5. Conclusion

In this paper, we studied the secret offloading performance of NOMA based on UAV supported MEC in IoT over Nakagami-m fading channel. We propose a three-phase system operation protocol, focusing on NOMA-MEC techniques to increase secrecy offloading performance. To evaluate the system performance, we obtain the closed-form expressions of SSCP of the entire system under the influence of ipCSI and ipSIC Additionally, we proposed an algorithm based on GA to determine the position and altitude of UAV and the task offload ratio of ED to maximize SSCP. We have provided numerical results to verify the covert offloading performance of the proposed system.

F. Proof of Theorem 1

By substituting (13) and (20) into (19), we can rewrite the S of system as

$$\begin{aligned} S = \Pr\Big\{\mathcal{X} > 0, \Xi_2^{(\mathcal{X})} > \mathcal{Y} > \Xi_1^{(\mathcal{X})}, \\ \mathcal{S} < \Xi_3^{(\mathcal{X},\mathcal{Y})}\mathcal{Z} + \Xi_4^{(\mathcal{X},\mathcal{Y})}, \mathcal{X} < \Xi_5^{(\mathcal{X},\mathcal{Y})}\Big\}, \\ = \int_0^{\infty}\int_{\Xi_1^{(\mathcal{X})}}^{\Xi_2^{(\mathcal{X})}}\int_0^{\Xi_5^{(\mathcal{X},\mathcal{Y})}} F_{\mathcal{S}}\left(\Xi_3^{(\mathcal{X},\mathcal{Y})}\mathcal{Z} + \Xi_4^{(\mathcal{X},\mathcal{Y})}\right) \\ \times f_{\mathcal{Z}}(z) f_{\mathcal{Y}}(y) f_{\mathcal{X}}(x)\, dz dy dx, \end{aligned} \tag{F.1}$$

where $\mathcal{X} = \left|\hat{g}_{BU_M}\right|^2$, $\mathcal{Y} = \left|\hat{g}_{AU_M}\right|^2$, $\mathcal{Z} = \left|\hat{g}_{BU_E}\right|^2$, $\mathcal{S} = \left|\hat{g}_{AU_E}\right|^2$, $\Xi_1^{(\mathcal{X})} = \frac{\theta_A(\gamma_2\mathcal{X}+\gamma_3)}{\gamma_1}$, $\Xi_2^{(\mathcal{X})} = \frac{\gamma_2\mathcal{X}-\theta_B\gamma_4}{\theta_B\zeta\gamma_1}$, $\Xi_3^{(\mathcal{X},\mathcal{Y})} = \left(\frac{\gamma_1\mathcal{Y}}{\gamma_2\mathcal{X}+\gamma_3} + 1 - \varphi_A\right)\frac{\gamma_6}{\varphi_A\gamma_5}$, $\Xi_4^{(\mathcal{X},\mathcal{Y})} = \left(\frac{\gamma_1\mathcal{Y}}{\gamma_2\mathcal{X}+\gamma_3} + 1 - \varphi_A\right)\frac{\gamma_7}{\varphi_A\gamma_5}$, $\Xi_5^{(\mathcal{X},\mathcal{Y})} =$

$\left(\frac{\gamma_2 \mathcal{X}}{\zeta \gamma_1 \mathcal{Y} + \gamma_4} + 1 - \varphi_B\right) \frac{\gamma_8}{\varphi_B \gamma_6}$. There are three integrals here, so we do the integration one by one from (F.1).

First, we solve the 1st integral, denoted by I_1. By combining the CDF in (6) and the PDF in (7) into I_1. Through a few mathematical transformation steps, we solve the integral of I_1 shown in (F.2).

$$I_1 = \int_0^{\Xi_5^{(\mathcal{X},\mathcal{Y})}} F_{\mathcal{S}}\left(\Xi_3^{(\mathcal{X},\mathcal{Y})} \mathcal{Z} + \Xi_4^{(\mathcal{X},\mathcal{Y})}\right) f_{\mathcal{Z}}(z)\, dz,$$
$$= 1 - \Phi_4^{(\mathcal{X},\mathcal{Y})} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{(\mathcal{X},\mathcal{Y})} \Phi_7^{(\mathcal{X},\mathcal{Y})} \left(1 - \Phi_8^{(\mathcal{X},\mathcal{Y})}\right), \tag{F.2}$$

where $\Phi_4^{(\mathcal{X},\mathcal{Y})} = e^{-\frac{m\Xi_5^{(\mathcal{X},\mathcal{Y})}}{\lambda_{BU_E}}} \sum_{i_1=0}^{m-1} \frac{1}{i_1!}\left(\frac{m}{\lambda_{BU_E}} \Xi_5^{(\mathcal{X},\mathcal{Y})}\right)^{i_1}$, $\Phi_5 = \frac{1}{(m-1)!}\left(\frac{m}{\lambda_{BU_E}}\right)^m$, $\Phi_6^{(\mathcal{X},\mathcal{Y})} = \frac{(m+i_2-1)!}{i_2!(s-i_2)!}\left(\frac{\gamma_7}{\gamma_6}\right)^{s-i_2}\left(\frac{m}{\lambda_{AU_E}} \Xi_3^{(\mathcal{X},\mathcal{Y})}\right)^s$, $\Phi_7^{(\mathcal{X},\mathcal{Y})} = \left(\Psi_1^{(\mathcal{X},\mathcal{Y})}\right)^{-(m+i_2)} e^{-\frac{m\Xi_4^{(\mathcal{X},\mathcal{Y})}}{\lambda_{AU_E}}}$, $\Phi_8^{(\mathcal{X},\mathcal{Y})} = e^{-\Psi_2^{(\mathcal{X},\mathcal{Y})}} \sum_{i_3=0}^{m+i_2-1} \frac{1}{i_3!}\left(\Psi_2^{(\mathcal{X},\mathcal{Y})}\right)^{i_3}$, $\Psi_1^{(\mathcal{X},\mathcal{Y})} = \frac{m\Xi_3^{(\mathcal{X},\mathcal{Y})}}{\lambda_{AU_E}} + \frac{m}{\lambda_{BU_E}}$, $\Psi_2^{(\mathcal{X},\mathcal{Y})} = \Psi_1^{(\mathcal{X},\mathcal{Y})} \Xi_5^{(\mathcal{X},\mathcal{Y})}$.

Next, we substitute I_1 in (F.2) and the PDF in (7) into the 2nd integral, denoted by I_2, then I_2 solved by applying the Gaussian-Chebyshev quadrature method [25] is shown by (F.3) at the top of the next page, where $\zeta_o = \cos\left(\frac{\pi(2o-1)}{2O}\right)$, $\omega_o^{(\mathcal{X})} = \frac{(\zeta_o+1)\left[\Xi_2^{(\mathcal{X})} - \Xi_1^{(\mathcal{X})}\right]}{2} + \Xi_1^{(\mathcal{X})}$, and O is the complexity versus accuracy trade-off coefficient.

Finally, we combining (F.3) and the PDF in (7) into the last integral in (F.1). Then S is solved as shown in (F.4) at the top of the next page, where $\zeta_q = \cos\left(\frac{\pi(2q-1)}{2Q}\right)$, $\omega_q = \frac{(\zeta_q+1)e^{-\nu_1}}{2}$, and $\theta_q = -\ln\left(\omega_q\right)$ with Q is the complexity versus accuracy trade-off coefficient. The closed-form expression for the SSCP of the entire system is obtained as given in **Theorem 1**.

References

[1] Farha, Y.A. and Ismail, M.H. (2022) Design and optimization of a UAV-enabled non-orthogonal multiple access edge computing IoT system. *IEEE Access* **10**: 117385–117398.

[2] Nguyen, A.N., Nhan Vo, V., So-In, C., Ha, D.B., Sanguanpong, S. and Baig, Z.A. (2019) On secure wireless sensor networks with cooperative energy harvesting relaying. *IEEE Access* **7**: 139212–139225.

[3] Nguyen, A.N., Vo, V.N., So-In, C. and Ha, D.B. (2021) System performance analysis for an energy harvesting iot system using a DF/AF UAV-enabled relay with downlink NOMA under nakagami-m fading. *Sensors* **21**(1).

[4] Nguyen, A.N., Ha, D.B., Vo, V.N., Truong, V.T., Do, D.T. and So-In, C. (2022) Performance analysis and optimization for iot mobile edge computing networks with RF energy harvesting and UAV relaying. *IEEE Access* **10**: 21526–21540.

[5] Nguyen, A.N., Ha, D.B., Truong, T.V., Vo, V.N., Sanguanpong, S. and So-In, C. (2023) Secrecy performance analysis and optimization for UAV-relay-enabled WPT and cooperative NOMA MEC in IoT networks. *IEEE Access* **11**: 127800–127816.

[6] Nguyen, A.N. and Bui, N.A. (2023) Performance analysis of IoT mobile edge computing networks using a DF/AF UAV-enabled relay with downlink noma. In *Proc. IEEE Symposium on Industrial Electronics and Applications (ISIEA)*: 1–6.

[7] Lu, W., Si, P., Gao, Y., Han, H., Liu, Z., Wu, Y. and Gong, Y. (2021) Trajectory and resource optimization in ofdm-based UAV-powered iot network. *IEEE Trans. Green Commun. Netw.* **5**(3): 1259–1270.

[8] Liu, Z., Qi, J., Shen, Y., Ma, K. and Guan, X. (2023) Maximizing energy efficiency in UAV-assisted NOMA–MEC networks. *IEEE Internet Things J.* **10**(24): 22208–22222.

[9] Liu, Y., Xie, S. and Zhang, Y. (2020) Cooperative offloading and resource management for UAV-enabled mobile edge computing in power IoT system. *IEEE Trans. Veh. Technol.* **69**(10): 12229–12239.

[10] Hu, Q., Cai, Y., Yu, G., Qin, Z., Zhao, M. and Li, G.Y. (2019) Joint offloading and trajectory design for UAV-enabled mobile edge computing systems. *IEEE Internet Things J.* **6**(2): 1879–1892.

[11] Zhang, J., Zhou, L., Zhou, F., Seet, B.C., Zhang, H., Cai, Z. and Wei, J. (2020) Computation-efficient offloading and trajectory scheduling for multi-UAV assisted mobile edge computing. *IEEE Trans. Veh. Technol.* **69**(2): 2114–2125.

[12] Na, Z., Liu, Y., Shi, J., Liu, C. and Gao, Z. (2021) Uav-supported clustered NOMA for 6G-enabled internet of things: Trajectory planning and resource allocation. *IEEE Internet Things J.* **8**(20): 15041–15048.

[13] Zhang, X., Zhang, J., Xiong, J., Zhou, L. and Wei, J. (2020) Energy-efficient multi-UAV-enabled multiaccess edge computing incorporating NOMA. *IEEE Internet Things J.* **7**(6): 5613–5627.

[14] Budhiraja, I., Kumar, N., Tyagi, S. and Tanwar, S. (2021) Energy consumption minimization scheme for NOMA-based mobile edge computation networks underlaying UAV. *IEEE Syst. J.* **15**(4): 5724–5733.

[15] Rupasinghe, N., Yapici, Y., Guvenc, I., Dai, H. and Bhuyan, A. (2018) Enhancing physical layer security for NOMA transmission in mmwave drone networks. In *Proc. 52nd Asilomar Conf. Signals, Syst., Comput.*: 729–733.

[16] Cao, Y., Zhao, N., Chen, Y., Jin, M., Ding, Z., Li, Y. and Yu, F.R. (2020) Secure transmission via beamforming optimization for NOMA networks. *IEEE Wireless Commun.* **27**(1): 193–199.

[17] Sun, X., Yang, W. and Cai, Y. (2020) Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks. *IEEE Internet Things J.* **7**(3): 1884–1897.

$$I_2 = \int_{\Xi_1^{(\mathcal{X})}}^{\Xi_2^{(\mathcal{X})}} \left[1 - \Phi_4^{(\mathcal{X},\mathcal{Y})} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{(\mathcal{X},\mathcal{Y})} \Phi_7^{(\mathcal{X},\mathcal{Y})} \left(1 - \Phi_8^{(\mathcal{X},\mathcal{Y})}\right)\right] f_{\mathcal{Y}}(y)\, dy,$$
$$= \frac{\pi \left(\Xi_2^{(\mathcal{X})} - \Xi_1^{(\mathcal{X})}\right)}{2O(m-1)!} \left(\frac{m}{\lambda_{AU_M}}\right)^m \sum_{o=1}^{O} \sqrt{1-\zeta_o{}^2} \left(\omega_o^{(\mathcal{X})}\right)^{m-1} e^{-\frac{m\omega_o^{(\mathcal{X})}}{\lambda_{AU_M}}} \left[1 - \Phi_4^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} \Phi_7^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} \left(1 - \Phi_8^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)}\right)\right], \quad \text{(F.3)}$$

$$S = \frac{\pi}{2O(m-1)!} \left(\frac{m}{\lambda_{AU_M}}\right)^m \sum_{o=1}^{O} \sqrt{1-\zeta_o{}^2} \int_0^{\infty} \left(\Xi_2^{(\mathcal{X})} - \Xi_1^{(\mathcal{X})}\right) \left(\omega_o^{(\mathcal{X})}\right)^{m-1} e^{-\frac{m\omega_o^{(\mathcal{X})}}{\lambda_{AU_M}}}$$
$$\times \left[1 - \Phi_4^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} \Phi_7^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)} \left(1 - \Phi_8^{\left(\mathcal{X},\omega_o^{(\mathcal{X})}\right)}\right)\right] f_{\mathcal{X}}(x)\, dx,$$
$$= \Phi_1 \sum_{o=1}^{O} \sqrt{1-\zeta_o{}^2} \int_0^1 \left(\omega_o^{(\mathcal{X})}\right)^{m-1} \left(-\ln^{-1}(u)\right)^{m-1} \Phi_3^{\left(-\ln^{-1}(u),\omega_o^{\left(-\ln^{-1}(u)\right)}\right)}$$
$$\times \left[1 - \Phi_4^{\left(-\ln^{-1}(u),\omega_o^{\left(-\ln^{-1}(u)\right)}\right)} - \Phi_5 \sum_{s=0}^{m-1} \sum_{i_2=0}^{s} \Phi_6^{\left(-\ln^{-1}(u),\omega_o^{\left(-\ln^{-1}(u)\right)}\right)} \Phi_7^{\left(-\ln^{-1}(u),\omega_o^{\left(-\ln^{-1}(u)\right)}\right)} \left(1 - \Phi_8^{\left(-\ln^{-1}(u),\omega_o^{\left(-\ln^{-1}(u)\right)}\right)}\right)\right] du, \quad \text{(F.4)}$$

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

[19] Al-Hourani, A., Kandeepan, S. and Lardner, S. (2014) Optimal lap altitude for maximum coverage. *IEEE Wireless Commun. Lett.* **3**(6): 569–572.

[20] Yang, Z., Ding, Z., Fan, P. and Karagiannidis, G.K. (2016) On the performance of non-orthogonal multiple access systems with partial channel information. *IEEE Trans. Commun.* **64**(2): 654–667.

[21] Nguyen, A.N., Ha, D.B., Truong, V.T., So-In, C., Aimtongkham, P., Sakunrasrisuay, C. and Punriboon, C. (2022) On secrecy analysis of UAV-enabled relaying NOMA systems with RF energy harvesting. In *Proc. Industrial Networks and Intelligent Systems*: 267–281.

[22] Rauniyar, A., Osterbo, O.N., Hakegard, J.E. and Engelstad, P.E. (2022) Secrecy performance analysis of cooperative nonorthogonal multiple access in iot networks. *IEEE Sensors J.* **22**(19): 19030–19045.

[23] Zhang, T., Xu, Y., Loo, J., Yang, D. and Xiao, L. (2020) Joint computation and communication design for uav-assisted mobile edge computing in iot. *IEEE Trans. Ind. Informat.* **16**(8): 5505–5516.

[24] Truong, V.T. and Ha, D.B. (2022) A novel secrecy offloading in NOMA heterogeneous mobile edge computing network. In *Proc. Advanced Engineering – Theory and Applications*: 468–477.

[25] Judd, K.L. (2012) Quadrature methods. In *Proc. Initiative Comput. Econ., Chicago*: 1–29.

[26] Wen, X., Ruan, Y., Li, Y., Xia, H., Zhang, R., Wang, C., Liu, W. *et al.* (2022) Improved genetic algorithm based 3-D deployment of UAVs. *Journal of Communications and Networks* **24**(2): 223–231.