

RESEARCH

Open Access



UAV-assisted NOMA secure communications: joint transmit power and trajectory optimization

Ruibo Han¹, Yongjian Wang² and Yang Zhang^{2*} 

*Correspondence:
zhangyang.nju05@163.com

¹ Yantai Research Institute
of Harbin Engineering University,
Yantai 264000, China

² National Computer Network
Emergency Response Technical
Team/Coordination Center
of China, Beijing 100000, China

Abstract

With the inherent advantages of exceptional maneuverability, flexible deployment options and cost-effectiveness, unmanned aerial vehicles (UAVs) present themselves as a viable solution for providing aerial communication services to Internet of Things devices in high-traffic or remote areas. Nevertheless, the openness of the air-ground channel poses significant security challenges to UAV-based wireless systems. In this paper, a UAV-assisted secure communication system model is established based on non-orthogonal multiple access (NOMA) from the perspective of physical layer security, aiming to conceal the transmission behavior between UAVs and legitimate users (LUs). Specifically, a mobile UAV assumes the role of an aerial base station, leveraging NOMA technique to transmit data to LUs while evading detection from mobile eavesdropper situated on the ground. To fortify the security performance of the system, a hovering UAV acts as a friendly jammer and transmits interference signals to mobile eavesdropper (referred to as Eve). The objective of this scheme is to maximize the minimum average secure rate of all LUs by meticulously optimizing the trajectory and power allocation of the mobile UAV, subject to secrecy performance constraints. The highly interdependent and non-convex nature of this optimization problem renders direct solutions infeasible. Hence, this paper designs an efficient iterative algorithm that decouples the original problem into two subproblems, enabling an alternating optimization process for the trajectory and power allocation of the mobile UAV until the convergence of the objective function is achieved. Simulation results demonstrate that the proposed algorithm effectively improves the minimum average secure rate of all LUs compared with the benchmark scheme.

Keywords: Unmanned aerial vehicles, Non-orthogonal multiple access, Physical layer security, Power allocation

1 Introduction

With the exponential growth of Internet of Things (IoT) applications, it is estimated that the global number of IoT devices will reach a staggering 30 billion by 2030 [1–4]. However, in regions where ground communication infrastructure is absent or in emergency scenarios, IoT devices may face challenges in accessing reliable communication services [5–7]. Conversely, in geographically isolated areas, the deployment of unmanned aerial vehicles (UAVs) presents a compelling solution due to their exceptional maneuverability, adaptable deployment capabilities and cost-effectiveness [8–10]. By capitalizing on these

advantages, UAVs can swiftly establish emergency communication systems in areas deprived of ground infrastructure, ensuring steadfast channel connectivity with IoT devices [11–14]. This, in turn, guarantees uninterrupted and dependable transmission of information and seamless data collection for IoT devices, thereby significantly bolstering emergency communication capabilities in regions affected by disasters.

As a highly promising technology, UAV-assisted communication showcases three typical application scenarios [15–17]. Firstly, UAVs can be deployed as airborne base stations, enabling pervasive wireless coverage within their designated service areas [18–20]. Zhang et al. [18] introduced a communication system model that leverages multiple UAV base stations, aiming to minimize the required number of UAVs while optimizing their three-dimensional positions, user clustering and frequency band allocation to enhance coverage. Secondly, UAVs can function as aerial relays, establishing reliable wireless connections for remote users when direct communication is unfeasible [21, 22]. Ji et al. [22] delved into the security challenges of cache-enabled UAV relay networks featuring device-to-device (D2D) communication, considering the presence of eavesdroppers (Eves). They formulated an optimization problem that jointly optimized cache layout and UAV flight trajectory within a limited flying cycle, with the objective of maximizing the minimum secrecy rate among receivers. Lastly, UAVs can serve as airborne access points, facilitating mobile data collection and information dissemination to cater to diverse user demands [23]. Zeng et al. [23] proposed an innovative UAV-assisted wireless communication scheme utilizing cyclic multi-access and optimized transmission time allocation based on UAV positions to achieve maximum minimum throughput. By capitalizing on these remarkable advantages, UAVs have become an indispensable and complementary component of existing communication systems.

Nevertheless, wireless systems, including UAV communication, have long grappled with the limited availability of spectrum resources [24]. In light of this challenge, researchers have been actively exploring efficient strategies to transmit information within the constraints of restricted frequency bands. In contrast to orthogonal multiple access (OMA), non-orthogonal multiple access (NOMA) [25–28] enables multiple users to share the same spectrum by superimposing their signals in the power domain. To mitigate interference caused by overlapping signals, successive interference cancellation (SIC) techniques are employed at the receiver level. NOMA exhibits superior spectrum efficiency, reduced latency and enhanced connectivity when compared with OMA. In a particular study [29], a UAV was employed to serve multiple ground users using NOMA. The research focused on optimizing the layout and power allocation of the UAV to maximize overall throughput. Zhao et al. [30] proposed a NOMA-UAV system, where the UAV cooperates with a base station to provide services to ground users. By jointly optimizing the trajectory of the UAV and NOMA precoding techniques, the research aimed to maximize the transmission rate for ground users facilitated by the UAV. Furthermore, Wu et al. [31] introduced a UAV-based two-user broadcast channel, wherein the UAV independently transmitted information to two ground users. By considering constraints on the UAV's maximum speed and transmit power, a joint optimization approach was employed to determine the UAV's flight trajectory and power allocation. The objective was to effectively characterize the throughput of the broadcast channel within a given duration of UAV

flight. Additionally, Nasir et al. [32] investigated the problem of maximizing the minimum transmission rate under various constraints, including total transmit power, total bandwidth, UAV altitude and antenna beamwidth. To address this optimization challenge, they employed a trajectory optimization algorithm to obtain an efficient UAV-NOMA system with notable enhancements in transmission rates.

However, wireless systems, including UAV communication, are confronted with the pervasive risk of eavesdropping and malicious attacks, posing intricate challenges in delivering secure and dependable communication services for ground-based IoT devices [33–35]. In contrast to conventional encryption methods, recent research has extensively explored the realm of physical layer security (PLS), which capitalizes on the intrinsic characteristics of the wireless channel and employs (artificial) noise to accomplish secure information transmission [36, 37]. Yang et al. [38] and Jameel et al. [39] conducted investigations into the utilization of artificial noise (AN) emitted from ground terminals to deliberately degrade the eavesdropper's channel and curtail the capacity of the eavesdropping channel. This approach effectively enhances the system's secrecy capacity. Zhang et al. [40] underscored the advantages conferred by UAVs, such as their flexible deployment and mobility, in augmenting the security performance of the system. By orchestrating the optimization of UAV deployment or flight trajectories alongside wireless communication resources, the channel capacity of UAV-to-ground communication can be amplified, thereby fortifying the secrecy capacity. Moreover, Gao et al. [41] delved into a UAV-to-ground communication system, where a UAV is tasked with transmitting confidential information to authorized users while contending with the presence of eavesdroppers and adhering to no-fly zones. Through the joint optimization of the UAV's trajectory and transmission power, the research aimed to maximize the minimum secure rate experienced by users within the system. Additionally, Luo et al. [42] examined both the uplink and downlink scenarios in a UAV communication system, where confidential information is exchanged between a legitimate ground user and the UAV, while an active Eve seeks to intercept the information and introduces interference signals. To tackle this challenge, they proposed a resource allocation algorithm that maximizes the average secure rate within this configuration.

By the analysis of the aforementioned literature, two drawbacks can be identified in previous works on UAV physical layer secure communication. Firstly, existing research has not taken into account the impact of eavesdropper location uncertainty on secure communication. Secondly, most works have only considered a single ground LU, neglecting the interactive influence among multiple LUs. Therefore, a UAV-assisted secure communication system is proposed based on NOMA to achieve secure data transmission for legitimate users in this paper. NOMA and PLS are employed to enhance the spectrum efficiency of the system and ensure wireless transmission security, respectively. The contributions of this paper are summarized as follows:

- A UAV-assisted secure communication system model based on NOMA is established. Addressing the scenario with multiple legitimate users, a UAV is strategically deployed as an aerial base station, leveraging NOMA technique to dynami-

cally provide communication services through carefully planned periodic flight trajectories. Moreover, to safeguard the integrity of the system, a low-altitude UAV is ingeniously employed as a friendly jammer, effectively disrupting potential eavesdroppers. Eve is presumed to be mobile on the ground, following specific trajectories or directions.

- A coordinated design scheme for the trajectory and transmit power of a mobile UAV is proposed. In the IoT environment where mobile Eve exist, optimizing the transmit power of mobile UAV based on real-time tracking of the Eve's trajectory can improve the flexibility of resource allocation. Concurrently, by optimizing the UAV trajectory, network security is enhanced to a considerable extent. The objective of this scheme is to maximize the minimum average secure rate among all LUs by the joint optimization of the mobile UAV's trajectory and transmit power, while adhering to the constraints imposed by secrecy performance.
- A highly efficient optimization algorithm to enhance the performance of the UAV-assisted secure communication system is designed. To achieve this, an alternating iterative algorithm that optimizes both the trajectory and transmission power of the mobile UAV is proposed. Firstly, by fixing the UAV trajectory, relaxation variables is introduced to optimize power allocation. Then, with the power allocation fixed, we proceed to optimize the UAV trajectory and employ the CVX tool for trajectory calculation. Finally, by iteratively performing the aforementioned two steps, we achieve convergence of the optimization objective, thereby maximizing the minimum average secure rate of all LUs.

The content and organization of this paper are outlined as follows. In Sect. 2, the system model of the UAV-assisted secure communication system based on NOMA is introduced, along with the formulation of the corresponding optimization problem. Section 3 provides a comprehensive mathematical formulation of the optimization problem and presents a highly efficient iterative algorithm specifically designed for its solution. The simulation results are presented in Sect. 4, followed by the concluding remarks in Sect. 5.

2 System model and problem formulation

Considering the UAV-assisted secure communication network model based on NOMA depicted in Fig. 1, the network comprises two layers: a low-altitude layer consisting of a mobile UAV and a hovering friendly jammer, and a ground layer comprising K legitimate users and a mobile Eve. The set of LUs is denoted as $\mathcal{K} = \{1, 2, \dots, K\}$. In this model, the mobile UAV and hovering friendly jammer (Jammer) are assumed to be at heights H_U and H_J , respectively. The legitimate users are randomly distributed on the ground, while the mobile eavesdropper moves on the ground in a specified direction. The positions of LUs $k \in \mathcal{K}$ and the hovering friendly jammer in the three-dimensional Cartesian coordinate system are represented by coordinate vectors $\mathbf{w}_k = (x_k, y_k)^T$ and $\mathbf{q}_J = (x_J, y_J)^T$, respectively.

For the sake of analysis, the mission cycle T is discretized into N equal time slots, where each slot has a duration of $\delta = T/N$. The horizontal position coordinates of the mobile Eve and the mobile UAV can be represented as $\mathbf{W}_E = (x_E[n], y_E[n])^T, n \in \mathcal{N} = \{1, 2, \dots, N\}$ and $\mathbf{q}_U = (x_U[n], y_U[n])^T, n \in \mathcal{N} = \{1, 2, \dots, N\}$, respectively. When the mobile UAV

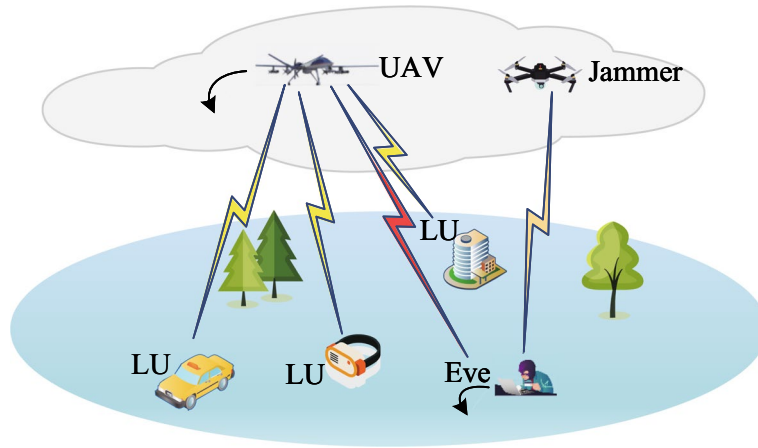


Fig. 1 System model

operates in a periodic manner, its endpoint position $\mathbf{q}_U[N]$ coincides with its starting point position $\mathbf{q}_U[1]$. It is assumed that the UAV maintains a constant speed throughout each time slot, and the maximum speed of the UAV is denoted as V_{\max} . Hence, the mobility constraint of the UAV can be formulated as follows:

$$[\mathbf{q}_U[1] = \mathbf{q}_U[N] \quad (1)$$

$$\|\mathbf{q}_U[n+1] - \mathbf{q}_U[n]\|^2 \leq \left(\frac{V_{\max}T}{N}\right)^2, n = 1, 2, \dots, N-1 \quad (2)$$

$$\|\mathbf{q}_U[n] - \mathbf{q}_J\|^2 \geq d_{\min}^2, \forall n \quad (3)$$

where d_{\min} denotes the minimum permissible distance ensuring safety between the mobile UAV and the hovering friendly jammer.

Throughout the mission cycle, the transmit power of the friendly jammer remains constant at P_J , while in the n th time slot, the mobile UAV's transmit power is represented as $P_U[n]$. Both entities adhere to the following constraints

$$0 \leq P_U[n] \leq P_{\max}, \forall n \quad (4)$$

$$P_J \geq 0 \quad (5)$$

where P_{\max} denotes the maximum transmit power of the mobile UAV in the n th time slot.

In the proposed network, the mobile UAV functions as a high-altitude base station, delivering services to LUs. The impact of terrain, obstacles and shadowing can be disregarded. Consequently, the communication channels between the mobile UAV and friendly jammer in the low-altitude layer, involving LUs and the mobile Eve on the ground, can be predominantly characterized as line-of-sight (LoS) links. Thus, during the n th time slot, the channel gain between the mobile UAV and a LUs conforms to the free-space path loss model and can be expressed as

$$h_{k,U}[n] = \frac{\beta_0}{d_{k,U}^2[n]}, \forall k \quad (6)$$

where β_0 represents the channel power gain at a reference distance of $d_0 = 1$ m. $d_{k,U}[n]$ stands for the distance between the k th LU and the mobile UAV during the n th time slot, and it can be expressed as

$$d_{k,U}[n] = \sqrt{H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_k\|^2}, \forall k \quad (7)$$

Similarly, the channel gain $h_{U,E}[n]$ between the mobile UAV and Eve during the n th time slot can be expressed as follows:

$$h_{U,E}[n] = \frac{\beta_0}{d_{U,E}^2[n]}, \forall n \quad (8)$$

where $d_{U,E}[n]$ denotes the distance between the mobile UAV and Eve during the n th time slot, and it can be formulated as

$$d_{U,E}[n] = \sqrt{H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_E[n]\|^2}, \forall n \quad (9)$$

During the n th time slot, the channel gain $h_{J,E}[n]$ between the friendly jammer and the mobile Eve can be expressed as follows:

$$h_{J,E}[n] = \frac{\beta_0}{d_{J,E}^2[n]}, \forall n \quad (10)$$

where $d_{J,E}[n]$ denotes the spatial separation between the friendly jammer and the mobile Eve during the n th time slot and can be mathematically expressed as

$$d_{J,E}[n] = \sqrt{H_J^2 + \|\mathbf{q}_J - \mathbf{W}_E[n]\|^2}, \forall n \quad (11)$$

Based on the system model, the achievable rate from the mobile UAV to LUs in the n th time slot can be defined as follows:

$$R_k[n] = \sum_{k=1}^K \log_2 \left(1 + \frac{P_U[n]h_{k,U}[n]}{\sum_{k=k+1}^K P_k[n]h_{k,U}[n] + N_0} \right), \forall k, n \quad (12)$$

where $\sum_{k=k+1}^K P_k[n]h_{k,U}[n]$ denotes the interference caused by the $(k+1)$ th to the K th legitimate users when the mobile UAV communicates with the k th legitimate user. The term N_0 represents the power spectral density of the additive white Gaussian noise (AWGN).

In the n th time slot, the intercepted achievable rate by the mobile Eve from the mobile UAV can be expressed as

$$R_E[n] = \log_2 \left(1 + \frac{P_U[n]h_{U,E}[n]}{N_0 + P_J h_{E,J}[n]} \right), \forall n \quad (13)$$

Hence, the average secure rate of LUs k across all time slots can be formulated as

$$R_{sk} = \frac{1}{N} \sum_{n=1}^N (R_k[n] - \max(R_E[n])), \forall k, n \quad (14)$$

where $\max(R_E[n])$ represents the maximum achievable rate at which the mobile eavesdropper can intercept the moving UAV across all time slots.

Define the variables $\mathcal{P} = \{P_U[n], \forall n\}$ and $\mathcal{Q} = \{\mathbf{q}_U[n], \forall n\}$ as follows. The objective of this paper is to maximize the minimum average secure rate of all LUs by simultaneously optimizing the trajectory \mathcal{Q} and power allocation \mathcal{P} of the mobile UAV, subject to the constraint of secrecy performance. In addition, a relaxation variable $\varphi = \min R_{sk}$ is introduced. Consequently, the optimization problem can be formulated as follows:

$$\max_{\varphi, \mathcal{P}, \mathcal{Q}} \varphi \quad (15a)$$

$$\text{s.t. } R_{sk} \geq \varphi, \forall k \quad (15b)$$

$$\|\mathbf{q}_U[n+1] - \mathbf{q}_U[n]\|^2 \leq \left(\frac{V_{\max} T}{N}\right)^2, n = 1, 2, \dots, N-1 \quad (15c)$$

$$\|\mathbf{q}_U[n] - \mathbf{q}_J\|^2 \geq d_{\min}^2, \forall n \quad (15d)$$

$$\mathbf{q}_U[1] = \mathbf{q}_U[N] \quad (15e)$$

$$0 \leq P_U[n] \leq P_{\max}, \forall n \quad (15f)$$

$$P_J \geq 0 \quad (15g)$$

Clearly, due to the intricate interdependence among the variables, solving Eq. (15) directly poses a significant challenge. This is mainly attributed to the fact that (15b) constitutes a complex non-convex fractional expression entailing the coupling of optimization variables. As a result, problem (15) constitutes a non-convex optimization problem that presents difficulties in direct solution.

3 Proposed solution

In this section, we address the challenging non-convex optimization problem (15) by decomposing it into two subproblems, specifically focusing on the trajectory \mathcal{Q} and power allocation \mathcal{P} of the mobile UAV. To handle the non-convexity, we utilize the relaxation variable method and employ the successive convex approximation (SCA) technique to transform the respective non-convex subproblems into convex ones. By alternating iterations, we iteratively solve these convex subproblems and aim to achieve convergence of the optimization objective.

3.1 Transmit power optimization

Given the predetermined trajectory of the mobile UAV, denoted as \mathcal{Q} , the optimization problem concerning power allocation, denoted as \mathcal{P} , can be described as follows:

$$\max_{\varphi, P} \quad \varphi \quad (16a)$$

$$\text{s.t.} \quad \frac{1}{N} \sum_{n=1}^N \left(\sum_{k=1}^K \log_2 \left(1 + \frac{P_U[n] h_{k,U}[n]}{\sum_{\tilde{k}=k+1}^K P_{\tilde{k}}[n] h_{\tilde{k},U}[n] + N_0} \right) \right) - \max(R_E[n]) \geq \varphi, \forall k, n \quad (16b)$$

$$0 \leq P_U[n] \leq P_{\max}, \forall n \quad (16c)$$

$$P_I \geq 0 \quad (16d)$$

Due to the non-convex nature of constraint (16b), the optimization problem (16) becomes a challenging non-convex problem to solve directly. To obtain an effective approximation solution for this problem, successive convex approximation is employed. By leveraging Lemma 1, the non-convex constraint (16b) is transformed into a convex constraint.

Lemma 1 *The non-convex constraint (16b) in Eq. (16) can be reformulated as a convex constraint utilizing the following transformation*

$$\frac{1}{N} \sum_{n=1}^N \left(\sum_{k=1}^K \log_2 \left(1 + \frac{P_U[n] h_{k,U}[n]}{\sum_{\tilde{k}=k+1}^K P_{\tilde{k}}[n] h_{\tilde{k},U}[n] + N_0} \right) - \gamma \right) \geq \varphi \quad (17)$$

$$A_U^l[n] + B_U^l[n](P_U[n] - P_U^l[n]) \leq \gamma \quad (18)$$

where

$$A_U^l[n] = \log_2 \left(1 + \frac{P_U^l[n] h_{U,E}[n]}{N_0 + P_I h_{E,J}[n]} \right) \quad (19)$$

$$B_U^l[n] = \frac{\log_2(e) h_{U,E}[n]}{N_0 + P_I h_{E,J}[n] + P_U^l[n] h_{U,E}[n]} \quad (20)$$

1 Proof

Firstly, by introducing a relaxation variable $\gamma = \max(\log_2(1 + \frac{P_U[n] h_{U,E}[n]}{N_0 + P_I h_{E,J}[n]}))$, the transformed formulation of the equation can be obtained as follows:

$$R_E[n] = \log_2 \left(1 + \frac{P_U[n] h_{U,E}[n]}{N_0 + P_I h_{E,J}[n]} \right) \leq \gamma \quad (21)$$

It is evident that Eq. (21) with respect to $P_U[n]$ is non-convex. To address this, a Taylor series expansion can be employed to derive an upper bound for $R_E[n]$. In each iteration, an approximate value $R_E^l[n]$ is substituted for $R_E[n]$, thereby transforming the constraint

(21) into a convex constraint. In the l th iteration, the first-order Taylor series expansion of $R_E[n]$ can be expressed as follows:

$$R_E[n] \leq A_U^l[n] + B_U^l[n](P_U[n] - P_U^l) \triangleq R_E^l[n] \quad (22)$$

where $A_U^l[n]$ and $B_U^l[n]$ are defined according to Eqs. (19) and (20), respectively. With this, the proof is concluded. \square

Hence, (16) can be reconfigured as

$$\max_{\varphi, P} \varphi \quad (23a)$$

$$\text{s.t. (17) - (20), (16c), (16d)} \quad (23b)$$

3.2 UAV trajectory optimization

The optimization problem statement pertaining to the trajectory \mathcal{Q} of the mobile UAV, leveraging the power allocation $P_U[n]$ derived via optimization, is described as follows:

$$\max_{\varphi, Q} \varphi \quad (24a)$$

$$\text{s.t. } \frac{1}{N} \sum_{n=1}^N \left(\sum_{k=1}^K \log_2 \left(1 + \frac{P_U[n] h_{k,U}[n]}{\sum_{k=k+1}^K P_k[n] h_{k,U}[n] + N_0} \right) \right) - \max(R_E[n]) \geq \varphi, \forall k, n \quad (24b)$$

$$\|\mathbf{q}_U[n+1] - \mathbf{q}_U[n]\|^2 \leq \left(\frac{V_{\max} T}{N} \right)^2, \quad n = 1, 2, \dots, N-1 \quad (24c)$$

$$\|\mathbf{q}_U[n] - \mathbf{q}_j\|^2 \geq d_{\min}^2, \quad \forall n \quad (24d)$$

$$\mathbf{q}_U[1] = \mathbf{q}_U[N] \quad (24e)$$

Lemma 2 The non-convex constraint (24b) present in optimization problem (24) can be effectively converted into a convex constraint

$$\frac{1}{N} \sum_{n=1}^N \left(\sum_{k=1}^K R_U^l[n] - \lambda \right) \geq \varphi, \forall k, n \quad (25)$$

$$\log_2 \left(1 + \frac{P_U[n] \beta_0}{(N_0 + P_j h_{E,j}[n]) (H_U^2 + \|\mathbf{q}_U[n] - \mathbf{w}_E[n]\|^2)} \right) \leq \lambda \quad (26)$$

$$R_U^l[n] = C_U^l[n] + D_U^l[n] (\|\mathbf{q}_U[n] - \mathbf{w}_k\|^2 - \|\mathbf{q}_U^l[n] - \mathbf{w}_k\|^2) \quad (27)$$

$$C_U^l[n] = \log_2 \left(1 + \frac{b_{k,U}[n]}{H_U^2 + \|\mathbf{q}_U^l[n] - \mathbf{W}_k\|^2} \right) \quad (28)$$

$$D_U^l[n] = \frac{-\log_2(e)b_{k,U}[n]}{\left(H_U^2 + \|\mathbf{q}_U^l[n] - \mathbf{W}_k\|^2 \right)^2 + b_{k,U}[n] \left(H_U^2 + \|\mathbf{q}_U^l[n] - \mathbf{W}_k\|^2 \right)} \quad (29)$$

$$b_{k,U}[n] = \frac{P_U[n]\beta_0}{\sum_{\tilde{k}=k+1}^K P_{\tilde{k}}[n]h_{\tilde{k},U}[n] + N_0} \quad (30)$$

1 Proof

Initially, introduce a slack variable, thereby facilitating the acquisition of an alternative formulation for the equation

$$R_E[n] = \log_2 \left(1 + \frac{P_U[n]\beta_0}{(N_0 + P_J h_{E,J}[n]) \left(H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_E[n]\|^2 \right)} \right) \leq \lambda \quad (31)$$

Note that constraint (31) exhibits convexity, whereas constraint (24b) persists as non-convex. Let us proceed with defining

$$b_{k,U}[n] = \frac{P_U[n]\beta_0}{\sum_{\tilde{k}=k+1}^K P_{\tilde{k}}[n]h_{\tilde{k},U}[n] + N_0} \quad (32)$$

Furthermore, (24b) can be further simplified as follows:

$$\frac{1}{N} \sum_{n=1}^N \left(\sum_{k=1}^K \log_2 \left(1 + \frac{b_{k,U}[n]}{H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_k\|^2} \right) - \lambda \right) \geq \varphi, \forall k, n \quad (33)$$

Evidently, by employing a first-order Taylor series expansion, a lower bound can be derived for the convexity of $\log_2 \left(1 + \frac{b_{k,U}[n]}{H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_k\|^2} \right)$ in terms of

$$\|\mathbf{q}_U[n] - \mathbf{W}_k\|^2.$$

Consequently, the expansion results in the following expression

$$\begin{aligned} & \log_2 \left(1 + \frac{b_{k,U}[n]}{H_U^2 + \|\mathbf{q}_U[n] - \mathbf{W}_k\|^2} \right) \\ & \geq C_U^l[n] + D_U^l[n] \left(\|\mathbf{q}_U[n] - \mathbf{W}_k\|^2 - \|\mathbf{q}_U^l[n] - \mathbf{W}_k\|^2 \right) = R_U^l[n] \end{aligned} \quad (34)$$

where $C_U^l[n]$ and $D_U^l[n]$ are given by (28) and (29), respectively.

The proof is complete. \square

Observe that the non-convex constraint (24b) undergoes a transformation into a convex constraint (25), it follows that for any given l th iteration of the mobile UAV trajectory $\mathbf{q}_U^l[n]$, the optimization problem (24) can be reasonably substituted with the optimization problem (35) during the subsequent $(l+1)$ th iteration, i.e.,

$$\max_{\varphi, Q} \varphi \quad (35a)$$

$$\text{s.t.} (25) - (30), (24c), (24d), (24e) \quad (35b)$$

3.3 Proposed algorithm

In order to address the original optimization problem (15) with minimal complexity, a highly efficient alternating iterative algorithm is introduced aimed at obtaining an approximate optimal solution in this section. Drawing insights from the discussions in Sects. 3.1 and 3.2, Eq. (15) is decomposed into two non-convex subproblems: optimizing, respectively, the power allocation and trajectory of mobile UAV. Subsequently, by an iterative process that alternates between solving these two subproblems, an approximate optimal solution for Eq. (15) is derived. The proposed iterative algorithm is depicted in Algorithm 1.

Algorithm 1 SCA Algorithm for Solving Problem (15)

- 1: **Initialize:** $P^{(0)}$, $Q^{(0)}$, and $\tilde{l} = 0$
 - 2: **Repeat:**
 - 3: Solve problem (23) with given $Q^{(\tilde{l})}$,
then denote the solution as $P^{(\tilde{l}+1)}$.
 - 4: Solve problem (35) with given $P^{(\tilde{l}+1)}$,
then denote the solution as $Q^{(\tilde{l}+1)}$.
 - 5: **Update** $\tilde{l} = \tilde{l} + 1$.
 - 6: **Until** convergence or a maximum number of iterations has been reached.
 - 7: **Output** $P^{(\tilde{l}+1)}$ and $Q^{(\tilde{l}+1)}$.
-

The overall time complexity of the proposed algorithm is $\mathcal{O}(L \times N \times K)$, where L , N and K represent the number of iterations, the total number of time slots and the number of LUs, respectively. The specific values of these variables will influence the runtime of the program code.

4 Numerical results and discussions

In this section, we begin by configuring the simulation parameters, followed by presenting the simulation results to substantiate the efficacy of the proposed algorithm. A sophisticated communication network is considered comprising a single mobile UAV, a friendly jammer, K LUs and a mobile Eve. The LUs are distributed randomly within a $1000 \times 1000 \text{ m}^2$. The mobile UAV operates at an altitude of $H_U = 100 \text{ m}$, with a flight period of $T = 100 \text{ s}$. Meanwhile, the friendly jammer remains stationary at an elevation of $H_J = 100 \text{ m}$, actively transmitting interference signals to impede the mobile Eve. To accommodate the time division multiple access scheme, the network is divided into $N = 50$ time slots, with each slot spanning $\delta = 2 \text{ s}$. The maximum speed achievable by the UAV is $V_{\max} = 40 \text{ m/s}$. Considerations for noise power spectral density and channel

power gain are given as $N_0 = -110$ dBm/Hz and $\beta_0 = -20$ dB, respectively. Within each time slot, the mobile UAV has a designated transmit power budget denoted as $P_{\max} = 0.3$ W while the friendly jammer possesses a separate transmit power allocation identified as $P_j = 0.4$ W.

To streamline the process, the initial movement trajectory is formulated as a circular path [20]. More precisely, the geometric center of all LUs abscissae $L_d = \sum_{k=1}^K \mathbf{W}_k / K = [L_x, L_y]^T$ is first computed and assigned as the central point of the initial trajectory. Subsequently, half the distance between and the farthest LU is regarded as $r_d = \max \|\mathbf{W}_k - L_d\|/2, \forall k$, which is duly selected as the radius. Consequently, the mobile UAV's position in time slot n can be determined as follows:

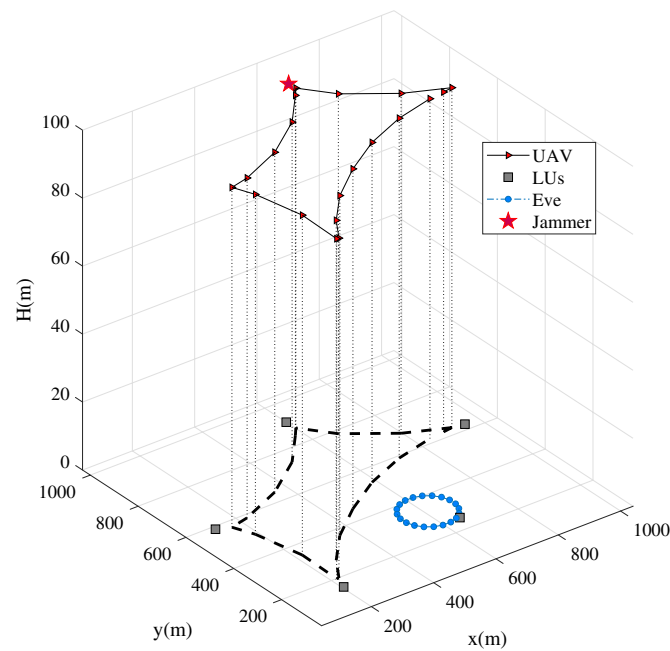
$$q_U^{(0)}[n] = \left[L_x + r_d \sin \frac{2\pi(n-1)}{N-1}, L_y + r_d \cos \frac{2\pi(n-1)}{N-1} \right]^T \quad (36)$$

Figure 2 illustrates the trajectory optimization of the mobile UAV in response to variations in the central position of the moving Eve. Two representative locations of the Eve's central point were selected to validate the efficacy of the proposed algorithm. As anticipated, the mobile UAV dynamically adjusts its trajectory to approach LUs with utmost proximity while maintaining a safe distance from the Eve. This strategic maneuver ensures the preservation of superior channel conditions, thereby augmenting the minimum average secure rate for LUs. Upon examining Fig. 2a and b, it becomes apparent that due to security constraints, the mobile UAV is unable to reach the LUs in closer proximity to the Eve. Instead, it prioritizes serving other LUs in order to achieve the optimization objective. In practice, the mobile UAV tends to allocate resources to LUs with more favorable channel conditions, thus optimizing the minimum average secure rate.

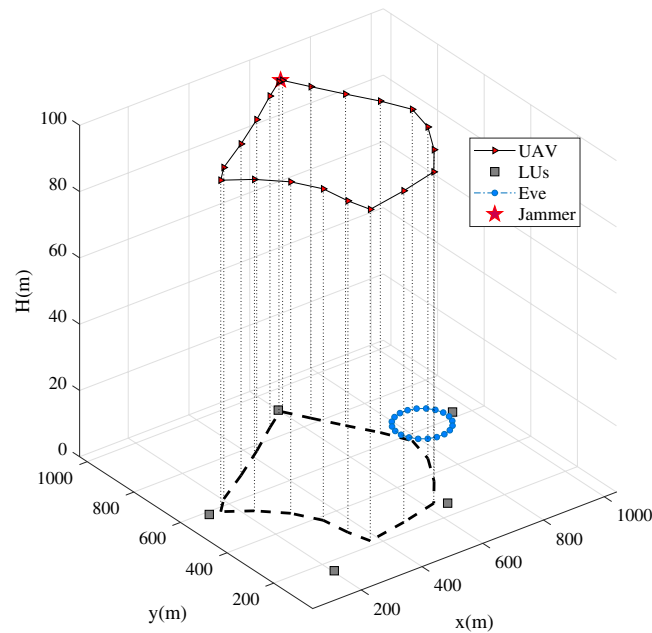
Figure 3 shows the speed profiles of distinct mobile eavesdroppers at different centroids. Notably, Fig. 3a illustrates that mobile UAV exhibit accelerated flight speeds during time slots 4–7, 13–16, 21–23 and 32–36. By juxtaposing Fig. 2a, it becomes apparent that UAV swiftly navigate toward subsequent lawful targets, aiming to accomplish confidential transmission tasks promptly within the mission cycle. Conversely, during time slots 2, 9, 18–19 and 25–26, the mobile UAV maintain reduced speed as they require a prolonged hover above designated LUs, facilitating the transmission of additional information. Figure 3b mirrors the speed variations observed in Fig. 3a.

Figure 4 illustrates the transmit power of UAV at different locations of mobile Eve's centers. Figure 4a shows that the mobile UAV exhibits reduced transmit power during time slots 29–37. By examining Figs. 2a and 3a in conjunction, it becomes apparent that the mobile UAV's proximity to the mobile Eve prompts a decrease in transmit power, ensuring secure information dissemination. During time slots 0–15, the transmit power of the mobile UAV gradually escalates as it moves farther away from the mobile Eve. With the relaxation of confidentiality constraints, UAV can amplify its transmit power to enhance the minimum average security rate for all LUs. The variation pattern of transmit power depicted in Fig. 4b closely resembles that observed in Fig. 4a.

Figure 5 illustrates the trajectories of UAV across varying maximum flight speed, with the center of the mobile Eve situated at point $[610, 330]^T$. At lower speeds $V_{\max} = 20$ m/s, the mobility of UAV falls short of efficiently reaching all LUs, limiting their ability to



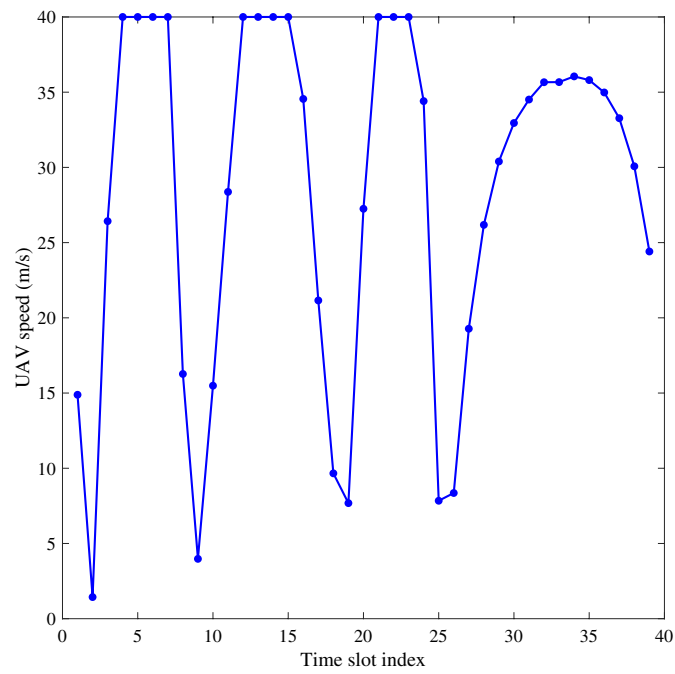
(a) The central position of the mobile Eve is located at $[610, 330]^T$.



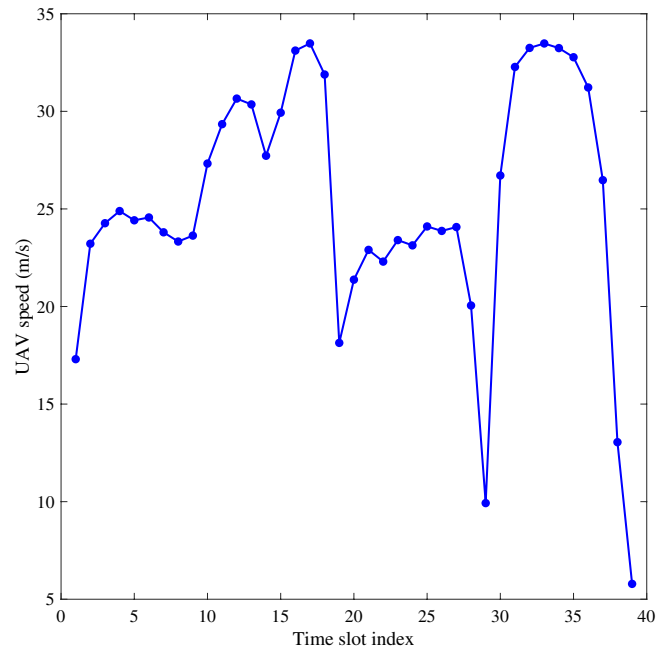
(b) The central position of the mobile Eve is located at $[855, 625]^T$.

Fig. 2 UAV trajectory at different center positions of mobile Eve

provide optimal service. However, as the speed escalates, the drones exhibit enhanced efficacy in reaching the LUs while maintaining a safe distance from the mobile Eve. Consequently, its trajectory progressively stabilize over time.

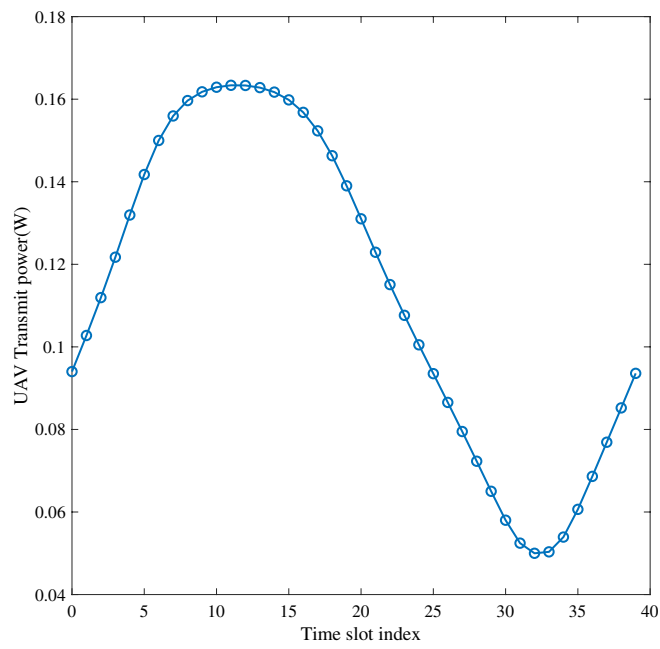


(a) The central position of the mobile Eve is located at $[610, 330]^T$.

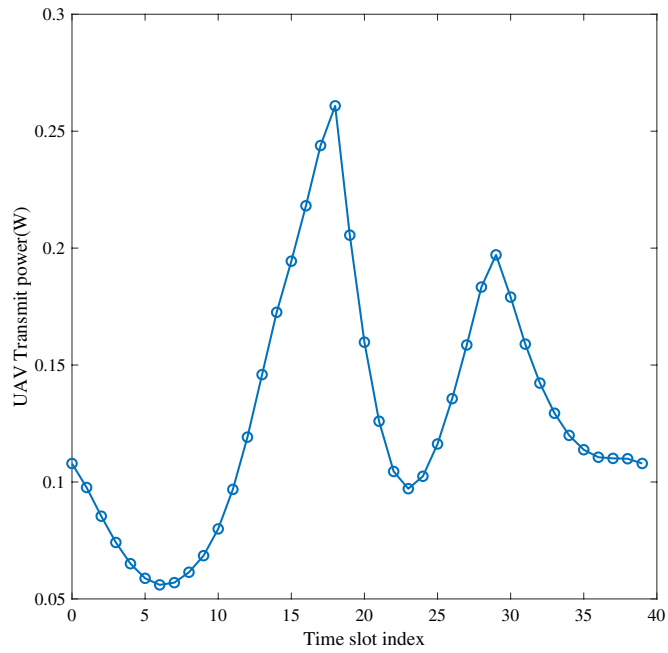


(b) The central position of the mobile Eve is located at $[855, 625]^T$.

Fig. 3 UAV speed at different center positions of mobile Eve



(a) The central position of the mobile Eve is located at $[610, 330]^T$.



(b) The central position of the mobile Eve is located at $[855, 625]^T$.

Fig. 4 UAV transmit power at different center positions of mobile Eve

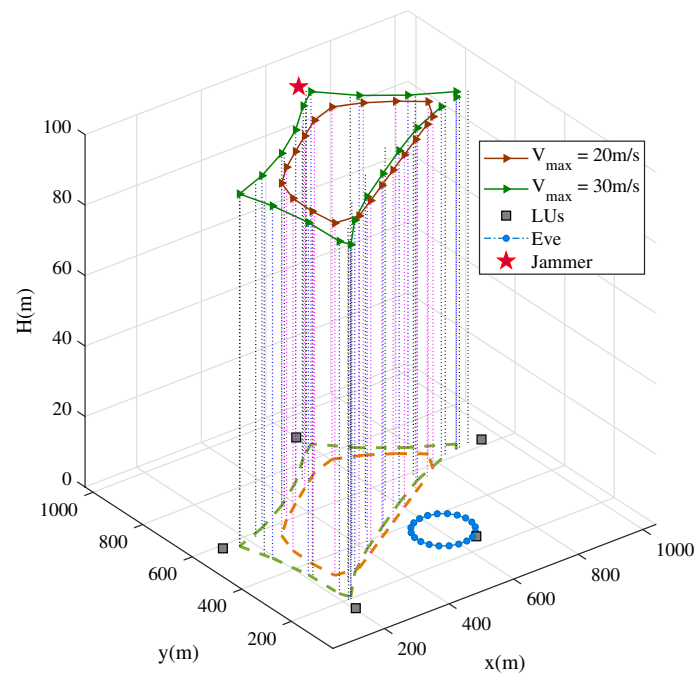


Fig. 5 Trajectories of UAV at different maximum flight speeds

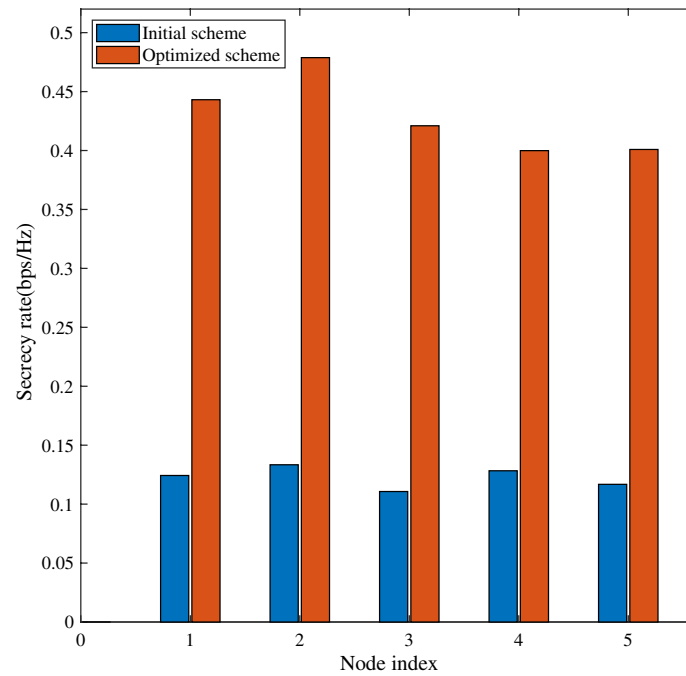


Fig. 6 Average secure rate of each LU

Figure 6 depicts the average secure rate attained by each LU when considering both the initial scheme and the proposed optimization scheme, with the mobile Eve positioned at point $[610, 330]^T$. The graphical representation reveals that the average secure rate for each LU is notably meager with respect to the initial scheme.

Nonetheless, following the application of joint optimization techniques, a substantial enhancement in the average secure rate of every LU becomes evident. This notable enhancement can be attributed to the efficacy of optimizing the trajectory and power allocation of UAV. By meticulous optimization of the UAV's trajectory and transmit power, it becomes possible to concurrently bolster communication quality while minimizing the Eve's capacity to intercept sensitive information. Consequently, each LU gains access to a heightened average secure rate, resulting in the overall fortification of system security and performance.

Figure 7 shows the dynamic evolution of the minimum average secure rate among all LUs as a function of iteration count. Evidently, with an increasing number of iterations, the minimum average secure rate for each LU demonstrates a corresponding improvement, denoting the algorithm's effectiveness in enhancing system security performance. Remarkably, at the 10th iteration, the minimum average secure rate reaches its pinnacle and maintains stability throughout subsequent iterations. This achievement serves as further validation for the algorithm's convergence and efficacy. These findings offer invaluable insights into the algorithm's performance and stability, providing valuable guidance for system design and optimization endeavors.

5 Conclusions

In addressing the challenge of ensuring reliable information exchange in scenarios involving multiple LUs, a UAV-assisted secure communication system model based on NOMA is proposed in this paper. Distinguishing itself from existing models, our proposed framework leverages NOMA to facilitate data transmission from the mobile UAV to LUs while simultaneously employing cooperative interference from the UAV to transmit jamming signals, effectively safeguarding LU's information security against potential

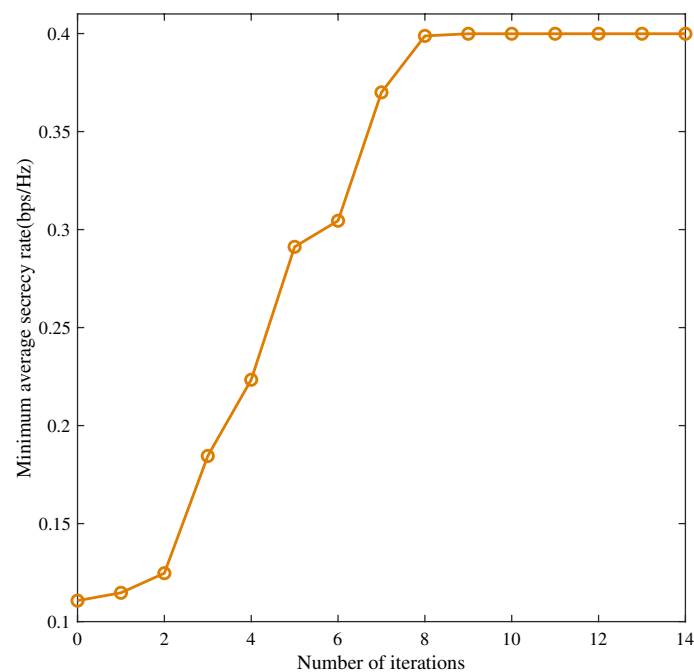


Fig. 7 Relationship between the minimum average secure rate and the number of iterations

eavesdroppers. To optimize the system, a joint optimization scheme that strategically plans the trajectory and power allocation of the mobile UAV is introduced, aiming to maximize the minimum average secure rate for all LUs. To tackle the inherent complexity, the original problem is intelligently decomposed into two non-convex subproblems, employing advanced techniques such as relaxed methods and SCA to optimize both the trajectory and transmit power of the mobile UAV. By an iterative solution process for these subproblems, we successfully attain a solution that meets predefined thresholds.

Simulation results substantiate the following conclusions. Firstly, compared with the baseline scheme, the proposed joint optimization scheme exhibits significant enhancements in the security of LU's information transmission. Secondly, the proposed algorithm demonstrates remarkable adaptability in adjusting the trajectory of the mobile UAV based on the position of the mobile Eve, showcasing the excellent convergence property.

Acknowledgements

We appreciate the editors and reviewers who processed and reviewed our manuscript to provide the detailed professional comments on the technical contributions, logical structure and content presentation of this paper.

Author contributions

RH was involved in conceptualization, data curation, validation and writing—original draft preparation. YW was responsible for methodology, software, visualization and writing—original draft preparation. YZ contributed to funding acquisition, resources, supervision and writing—reviewing and editing.

Funding

This work was supported by the National Natural Science Foundation of China under grant No. 61931019.

Availability of data and materials

Parts of the models, data and codes that support the study are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

All authors approved the final manuscript and the submission to this journal.

Competing interests

The authors declare that they have no competing interests.

Received: 31 July 2023 Accepted: 14 September 2023

Published online: 28 September 2023

References

1. A.M. El-Shorbagy, 5g technology and the future of architecture. *Procedia Comput. Sci.* **182**, 121–131 (2021)
2. X. Ma, Z. Na, B. Lin, L. Liu, Energy efficiency optimization of uav-assisted wireless powered systems for dependable data collections in internet of things. *IEEE Trans. Reliab.* **72**(2), 472–482 (2023)
3. S. Tang, L. Chen, K. He, J. Xia, L. Fan, A. Nallanathan, Computational intelligence and deep learning for next-generation edge-enabled industrial iot. *IEEE Trans. Netw. Sci. Eng.* **10**, 1–13 (2022)
4. L. Chen, X. Lei, Relay-assisted federated edge learning: Performance analysis and system optimization. *IEEE Trans. Commun.* **71**(6), 3387–3401 (2023)
5. Y. Guo, R. Zhao, S. Lai, L. Fan, X. Lei, G.K. Karagiannidis, Distributed machine learning for multiuser mobile edge computing systems. *IEEE J. Sel. Top. Signal Process.* **16**(3), 460–473 (2022)
6. L. Chen, L. Fan, X. Lei, T.Q. Duong, A. Nallanathan, G.K. Karagiannidis, Relay-assisted federated edge learning: performance analysis and system optimization. *IEEE Trans. Commun.* **71**(6), 3387–3401 (2023)
7. S. Zheng, C. Shen, X. Chen, Design and analysis of uplink and downlink communications for federated learning. *IEEE J. Sel. Areas Commun.* **39**(7), 2150–2167 (2021)
8. X. Lin, V. Jainanarayana, S.D. Muruganathan, S. Gao, H. Asplund, H.-L. Maattanen, M. Bergstrom, Y.-P. Sebastian Euler, E. Wang, The sky is not the limit: Lte for unmanned aerial vehicles. *IEEE Commun. Mag.* **56**(4), 204–210 (2018)
9. X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, J. Chen, Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Commun. Mag.* **56**(4), 68–74 (2018)
10. W. Zhou, X. Lei, Priority-aware resource scheduling for uav-mounted mobile edge computing networks. *IEEE Trans. Vehic. Tech.* **72**(99), 1–6 (2023)

11. Z. Na, J. Wang, C. Liu, M. Guan, Z. Gao, Joint trajectory optimization and communication design for uav-enabled ofdm networks. *Ad hoc Netw.* **98**, 102031.1-102031.10 (2020)
12. Z. Fang, J. Wang, C. Jiang, Q. Zhang, Y. Ren, Aoi-inspired collaborative information collection for auv-assisted internet of underwater things. *IEEE Internet Things J.* **8**(19), 14559–14571 (2021)
13. H. Su, Yu. Bin, C. Qian, Y. Xiao, Q. Xiong, C. Sun, Y. Gao, Nonorthogonal interleave-grid multiple access scheme for industrial internet of things in 5g network. *IEEE Trans. Industr. Inf.* **14**(12), 5436–5446 (2018)
14. X. Liu, Z. Liu, B. Lai, B. Peng, T.S. Durrani, Fair energy-efficient resource optimization for multi-uav enabled internet of things. *IEEE Trans. Veh. Technol.* **72**(3), 3962–3972 (2023)
15. Y. Zeng, R. Zhang, T.J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Commun. Mag.* **54**(5), 36–42 (2016)
16. B. Li, Z. Na, R. Liu, B. Lin, Energy consumption minimization of rotary-wing uavs for data distribution. *IEEE Commun. Lett.* **27**(7), 1819–1823 (2023)
17. X. Liu, B. Lai, B. Lin, V.C.M. Leung, Joint communication and trajectory optimization for multi-uav enabled mobile internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **23**(9), 15354–15366 (2022)
18. C. Zhang, L. Zhang, L. Zhu, T. Zhang, Z. Xiao, X.-G. Xia, 3d deployment of multiple uav-mounted base stations for uav communications. *IEEE Trans. Commun.* **69**(4), 2473–2488 (2021)
19. Z. Na, Y. Liu, J. Shi, C. Liu, Z. Gao, Uav-supported clustered noma for 6g-enabled internet of things: trajectory planning and resource allocation. *IEEE Internet Things J.* **8**(20), 15041–15048 (2021)
20. J. Wang, Z. Na, X. Liu, Collaborative design of multi-uav trajectory and resource scheduling for 6g-enabled internet of things. *IEEE Internet Things J.* **8**(20), 15096–15106 (2021)
21. B. Yu, X. Guan, Y. Cai, Joint blocklength and power optimization for half duplex unmanned aerial vehicle relay system with short packet communications. In *2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 981–986, 2020
22. J. Ji, K. Zhu, D. Niyato, R. Wang, Joint cache and trajectory optimization for secure uav-relaying with underlaid d2d communications. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020
23. J. Lyu, Y. Zeng, R. Zhang, Cyclical multiple access in uav-aided communications: a throughput-delay tradeoff. *IEEE Wirel. Commun. Lett.* **5**(6), 600–603 (2016)
24. Z. Na, B. Li, X. Liu, J. Wang, M. Zhang, Y. Liu, B. Mao, Uav-based wide-area internet of things: an integrated deployment architecture. *IEEE Netw.* **35**(5), 122–128 (2021)
25. A. Maatouk, E. Çalıřkan, M. Koca, M. Assaad, G. Gui, H. Sari, Frequency-domain noma with two sets of orthogonal signal waveforms. *IEEE Commun. Lett.* **22**(5), 906–909 (2018)
26. Y. Liu, Z. Qin, M. El Kashlan, Z. Ding, A. Nallanathan, L. Hanzo, Nonorthogonal multiple access for 5g and beyond. *Proc. IEEE* **105**(12), 2347–2381 (2017)
27. G. Gui, H. Sari, E. Biglieri, A new definition of fairness for non-orthogonal multiple access. *IEEE Commun. Lett.* **23**(7), 1267–1271 (2019)
28. X. Liu, H. Ding, H. Su, Uplink resource allocation for noma-based hybrid spectrum access in 6g-enabled cognitive internet of things. *IEEE Internet Things J.* **8**(20), 15049–15058 (2021)
29. X. Liu, J. Wang, N. Zhao, Y. Chen, S. Zhang, Z. Ding, F. Richard Yu, Placement and power allocation for noma-uav networks. *IEEE Wirel. Commun. Lett.* **8**(3), 965–968 (2019)
30. N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, M.-S. Alouini, Joint trajectory and precoding optimization for uav-assisted noma networks. *IEEE Trans. Commun.* **67**(5), 3723–3735 (2019)
31. W. Qingqing, X. Jie, R. Zhang, Capacity characterization of uav-enabled two-user broadcast channel. *IEEE J. Sel. Areas Commun.* **36**(9), 1955–1971 (2018)
32. A.A. Nasir, H.D. Tuan, T.Q. Duong, H. Vincent Poor, Uav-enabled communication using noma. *IEEE Trans. Commun.* **67**(7), 5126–5138 (2019)
33. Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends. *Proc. IEEE* **104**(9), 1727–1765 (2016)
34. J. Xia, L. Fan, X. Wei, X. Lei, X. Chen, G.K. Karagiannis, A. Nallanathan, Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers. *IEEE Trans. Commun.* **67**(11), 7672–7685 (2019)
35. N.L. Khoa, Performance analysis of secure communications over dual correlated rician fading channels. *IEEE Trans. Commun.* **66**(12), 6659–6673 (2018)
36. Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: theories, technologies, and challenges. *IEEE Commun. Surv. Tutor.* **19**(1), 347–376 (2017)
37. Z. Na, C. Ji, B. Lin, N. Zhang, Joint optimization of trajectory and resource allocation in secure uav relaying communications for internet of things. *IEEE Internet Things J.* **9**(17), 16284–16296 (2022)
38. N. Yang, L. Wang, G. Geraci, M. El Kashlan, J. Yuan, M. Di Renzo, Safeguarding 5g wireless communication networks using physical layer security. *IEEE Commun. Mag.* **53**(4), 20–27 (2015)
39. F. Jameel, S. Wyne, G. Kaddoum, T.Q. Duong, A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tutor.* **21**(3), 2734–2771 (2019)
40. G. Zhang, W. Qingqing, M. Cui, R. Zhang, Securing uav communications via joint trajectory and power control. *IEEE Trans. Wireless Commun.* **18**(2), 1376–1389 (2019)
41. Y. Gao, H. Tang, B. Li, X. Yuan, Joint trajectory and power design for uav-enabled secure communications with no-fly zone constraints. *IEEE Access* **7**, 44459–44470 (2019)
42. B. Duo, J. Luo, Y. Li, H. Hao, Z. Wang, Joint trajectory and power optimization for securing uav communications against active eavesdropping. *China Commun.* **18**(1), 88–99 (2021)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.