Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5390771, 11 pages
https://doi.org/10.1155/2022/5390771

Research Article

A Secure Downlink Transmission Scheme for a UAV-Assisted Edge Network

Xinmei Gao,[1,2] Yan Huo,[1] Qinghe Gao,[1] Hongjun Zhao,[3] and Long Ma[4]

[1]*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China*
[2]*Hebei Key Laboratory of Power Internet of Things Technology, North China Electric Power University, Baoding, Hebei 071003, China*
[3]*Beijing Research Institute of Automation for Machinery Industry LTD., Beijing 100120, China*
[4]*Computer Science Department, Troy University, Troy, AL 36082, USA*

Correspondence should be addressed to Yan Huo; yhuo@bjtu.edu.cn

Received 26 January 2022; Revised 9 March 2022; Accepted 28 March 2022; Published 21 April 2022

Academic Editor: Yingjie Wang

As an extension of centralized cloud services in a space-air-ground integrated network, an unmanned aerial vehicle (UAV-)-enabled edge network brings computation as close ground terminals of need as possible. In this scenario, the UAV is considered a mobile base station (MBS) to achieve data forwarding and processing from cloud servers to terminals. Note that downlink signals from the MBS to ground terminals are vulnerable to passive wiretapping by a malicious node. We formulate an average secrecy rate maximization problem to tackle the wiretapping issue by simultaneously transmitting confidential information and artificial noise (AN). We decompose the problem into two subproblems, including the UAV transmit power allocation subproblem and the UAV trajectory subproblem. Then, we adopt the successive convex approximation scheme and the alternating optimization method to develop our iterative algorithm to achieve secure transmission. Simulation results demonstrate that the proposed scheme is significantly better than other benchmarks in UAV-enabled downlink communication secrecy performance.

1. Introduction

Data-intensive applications such as video streaming are experiencing an unprecedented surge as digital savvy generation rises. In conjunction with the rapid development of mobile computing and the Internet of Things (IoT), large volumes of data have been moving within edge networking [1]. As an extension of backbone networks, edge computing enables terminals with limited resources to upload computing-intensive tasks to edge servers for execution by deploying servers near edge users. It can greatly reduce computational load and communication costs of terminals and cloud servers [2]. However, complex environments may introduce high infrastructure deployment costs, especially for remote areas and emergency relief applications.

Unmanned aerial vehicles (UAVs-)-enabled wireless network is considered a promising paradigm to provide beyond line-of-sight (LOS) signal transmission. Due to high maneuverability, flexible deployment, low cost, and strong hover ability, it is expected to be one of the critical steps in a space-air-ground integrated network (SAGIN). Many works on UAVs-enabled communications include air-to-ground (A2G) channel modeling, optimal throughput-based deployment, and multi-UAV cooperative communication [3]. These technologies may be conveniently introduced into most scenarios and applications, e.g., surveillance missions, weather monitoring, emergency search, and recognition missions [4].

With the gradual maturity of UAV technology, UAVs with flexible operation, good scalability, and adaptability to

various harsh environments bring more possibilities for network construction, route inspection, and other scenarios. Combining UAVs with a mobile edge computing (MEC) network and assuming UAVs as MEC servers, we can realize rapid deployment and flexible unloading of computing tasks. At the same time, UAVs limited by endurance time and detection range need to plan resources and paths during application.

Note that data in UAV-enabled edge networks contain sensitive and private information [5]. The security of data transmission in the open wireless environment is of critical importance for the wide deployment and acceptance of edge services in the future [6, 7]. Traditional methods to address wireless communication security are based on cryptography. It may cause high key management costs and computational complexity. The idea of physical layer security is to use channel information to enhance transmission security, which is an effective supplement to the upper layer security. Some scholars devoted to UAV-aided secure cooperation research [8, 9]. They considered a UAV a mobile relay or a friendly jammer to achieve secure transmission. This scenario is similar to a relay network with cooperative jamming. Essentially, the more general model in UAV-enabled secure communication includes a UAV aerial base station (ABS) and numerous mobile users [10]. A UAV can actively send signals instead of just forwarding information. In this case, an enabled mobile base station leads to changeable channel states, which may complex cooperative jamming design. Thus, it is a crux to design a feasible cooperative jamming scheme for secure communication in a mobile UAV-ABS scenario.

For secure communication of UAV-ABS scenarios, several techniques have been introduced to achieve positive secrecy rates or low secrecy outage probability [11]. In [12], the authors intended to jointly optimize the UAV's trajectory, transmit power, and power allocation of jamming signals to achieve the maximum average secrecy rate (ASR) for a UAV-enabled communication system. For a multi-UAV scenario, the authors in [13] used the orthogonal frequency division multiple access (OFDMA) technology to assign idle UAVs to send artificial noise (AN) to achieve secure transmission.

Motivated by the existing works, we discuss secure downlink transmission for a multiantenna UAV-ABS in this paper. In addition, inspired by [14], our system model adopts a hybrid probability channel, including a LOS link and a non-line-of-sight (NLOS) link. In this scenario, we intend to find the ASR. The main contributions of the paper are summarized as follows.

(i) Considering a UAV-ABS edge network with the random subcarrier selection-orthogonal frequency division multiplexing-direction modulation (RSCS-OFDM-DM) technology, we propose an ASR maximization problem to jointly optimize a feasible three-dimensional (3D) trajectory and power allocation

(ii) We exploit the successive convex approximation (SCA) scheme and the alternating optimization (AO) method to design our iterative algorithm to solve the initial nonconvex problem

(iii) We provide numerous simulation results, including the optimal flight trajectory, ASR, and average transmit power to evaluate our secure transmission method

The rest of the paper is organized as follows. The related work is presented in the next section. Next, we provide the system model and problem formulation and following propose an efficient iteration algorithm to solve our average secrecy rate maximization problem. Finally, we discuss and evaluate the performance of our method and conclude the article in the last two sections.

2. Related Work

2.1. Secure Transmit for a UAV Network. Due to the flexibility of UAV-enabled networking, many scholars have studied secure data transmission methods as shown in Table 1. In [15], Wu et al. studied energy-saving secure communication for a downlink A2G link. They discussed the impact of a jitter UAV on secure performance and formulated a power minimization and allocation problem with security constraints. Then, they further used secrecy coverage probability (SCP) and ergodic secrecy capacity (ESC) to investigate how to exploit the UAV jitter feature to enhance secrecy in [16]. Considering various service requirements, the authors in [17] proposed an achievable minimum secrecy rate maximization problem and designed a joint optimization method based on user scheduling, power allocation, and trajectory. In addition, [18] considered UAVs networks with downlink millimeter-wave direction modulation simultaneous wireless information and power transfer under nonorthogonal multiple access (NOMA) and orthogonal multiple access schemes. The authors derived secure outage probability (SOP) and effective secure throughput (EST) to measure security and reliability. In [19], Shengnan et al. proposed a secure transmission scheme of UAVs relay-assisted cognitive radio network (CRN), which optimized UAV relay's flight trajectory and transmit power to maximize secrecy rate. In [20], the authors considered a scenario of GPS interference and Eve covert operation. They proposed a robust joint optimization problem of UAV jamming power and trajectory to maximize the average security rate without completed information of UAV receiver and Eve.

However, the above work does not discuss the misuse of friendly jamming signals due to variable flight altitudes and unreasonable jammer configurations. In [21, 22], the authors introduced a RSCS-OFDM-DM technology to efficiently utilize multiple antennas to reduce unnecessary resource deployment. The use of the technology can reduce the impact on system secrecy performance when the eavesdropper and the legitimate user are in the same beam direction and reduce the complexity of the receiver through fast Fourier transformation.

2.2. Optimization in MEC Networks. There are rich literatures on MEC resource management that aims at optimizing

Table 1: Secure transmission for a UAV-enabled network.

References	Metrics	Contributions
[15]	Secrecy rate	Design a joint optimization to transmit confidential signals and artificial noise to achieve secrecy requirements.
[16]	SCP and ESC	Propose a UAV-jitter-based method to enhanced secrecy performance for an A2G wiretapping scenario.
[17]	Secrecy rate	Use a UAV-ABS with the NOMA technology to develop a secure multiuser data transmit scheme.
[18]	SOP and EST	Design a direction modulation (DM) scheme for a mmWave UAV network with the simultaneous wireless information and power transfer (SWIPT) technical.
[19]	Secrecy rate	Propose a secure data transmission scheme for a UAV relay-assisted CRN to improve spectrum utilization and communication secrecy rate.
[20]	ASR	Use a block coordinate descent method to jointly optimize jamming power and trajectory to maximize ASR.

system latency [23, 24], energy consumption [25, 26], and overall cost of system latency and/or energy consumption [27, 28]. In [23], Ren et al. investigated the joint communication and computation resource allocation problem under the cooperation of cloud computing and edge computing to minimize system delay of all mobile devices. Park et al. in [24] proposed a Cloud-Ran architecture for cloud computing and local edge node collaborative computing. They intend to minimize end-to-end delay by jointly optimizing computing and communication resources. Zhang et al. [25] studied the problem of task unloading and resource allocation in dense network Cloud-Ran architecture to optimize network energy efficiency. Then, Zhou et al. designed a double deep Q network (DDQN-)-based method to joint optimize computation offloading and resource allocation in a dynamic multiuser MEC system in [26]. Their objective is to minimize the energy consumption of the entire MEC system by considering the delay constraint and the uncertain resource requirements of heterogeneous computation tasks. In [27], we studied the joint task unloading and resource allocation of MEC in NOMA-based HetNets. And Dai et al. designed an optimized computing offload and resource allocation strategy using DRL based on 5G beyond terminal edge cloud coordination network to minimize system energy consumption in [28].

Considering the flexible deployment of UAVs, some works introduced UAVs into MEC networks and discussed optimization issues for a UAV-enabled MEC network. In [29], the authors proposed a secure communication scheme for a dual UAV-MEC system. They optimized the resource and trajectories of UAV servers to maximize secure computing power. In [30], the authors studied a secure transmission problem for dual UAV-assisted MEC systems. One UAV is called to help ground terminals (GTs) calculate unloading tasks, and the other UAV acts as a jammer to suppress malicious eavesdroppers. By jointly optimizing the communication resources, computing resources, and UAV's trajectories, they discussed the maximization problem of the minimum secure capacity in time division multiple access and NOMA scenarios. In addition, [31] proposed an innovative UAV-MEC system that involved an interaction between IoT devices, UAVs, and edge clouds. UAVs and edge clouds in the system cooperate in providing MEC services for a group of IoT devices. By jointly optimizing UAV location, communication, computing resource allocation, and task segmentation decision, the weighted sum of service delay of IoT devices and UAV energy consumption is minimized.

Note that these studies assumed wired or dedicated wireless links with sufficient bandwidth among edge nodes deployed in a fixed paradigm. Yet, the assumption is not suitable for data secure transmit in the existing MEC, especially in massive edge users or sparse distribution of network facilities scenarios [32]. Accordingly, we intend to study secure data transmission during task offloading in a UAV-assisted edge network.

3. System Model

Considering flexibility and low-cost features of UAVs, they are very suitable as edge servers to provide signal coverage and information forward for edge terminals. In an UAV-ABS edge network, a UAV can be regarded as an edge server, and ground terminals are edge nodes, as shown in Figure 1. When communicating with a UAV, the edge node is vulnerable to wiretapping by an eavesdropper. This may cause private information disclosure and reduce the secure level of an edge network. In order to ensure secure data transmission, we intend to design a novel scheme to solve the security issue in this scenario.

3.1. A UAV-ABS Network Model. According to Figure 1, a typical UAV-ABS network model includes a UAV source with a N_T-element linear antenna array, a legitimate ground terminal (GT) with a single antenna, and a ground eavesdropper (Eve) with a single antenna. We assume that positions of GTs and the eavesdropper are known and static, which are defined as $\mathbf{U} = (x_U, y_U, 0)$ and $\mathbf{E} = (x_E, y_E, 0)$, respectively. To simplify the optimization problem, the UAV flight duration from the initial position to the final position is T time, and it can discretize into N time slots, where $T = N\delta_t$ and δ_t is the fixed length of a transmission time slot. Assuming δ_t is small enough, the flight in each time slot can be regarded as a uniform motion. Therefore, in time slot $n(n \triangleq 1, 2, \cdots, N)$, the coordinates of a UAV can be denoted as $\mathbf{L}[n] \triangleq (x[n], y[n], h[n])$. The UAV can exploit

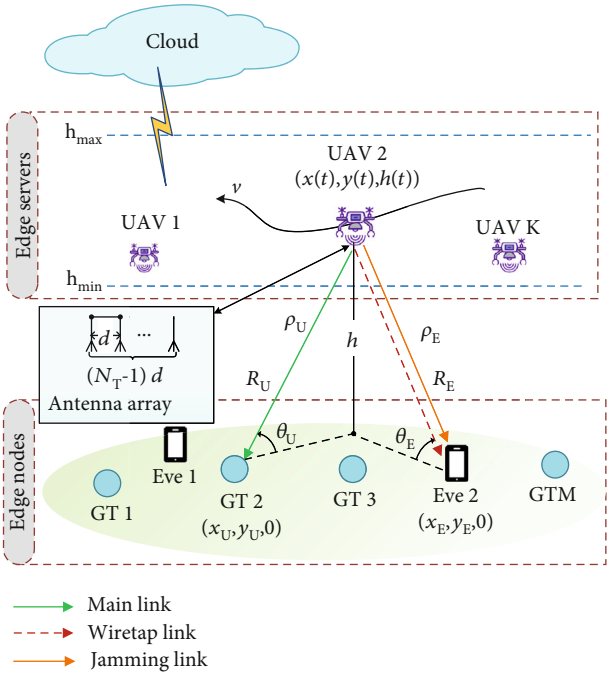

FIGURE 1: A downlink UAV-ABS model.

its multiple antennas to broadcast confidential signals and sends AN directly to the eavesdropper via the RSCS-OFDM-DM technology [21].

In the system, the UAV uses its linear antenna array to send OFDM symbols to the target GTs by randomly selecting multiple subcarriers from the subcarrier set. Supposing that there are N_s orthogonal subcarriers [21], the set is defined as follows:

$$S_s = \{f_m | f_m = f_c + m\Delta f\}, (m = 0,\cdots,N_s - 1)\}, \quad (1)$$

where m is the number of subcarriers and Δf is the bandwidth of a subchannel. In this paper, we assume that the total bandwidth of subcarriers is much less than the center carrier frequency, i.e., $N_s\Delta f \ll f_c$. The signals transmitted by the kth $(k = 1,\cdots,N_T)$ antenna at time slot n can be defined as follows:

$$S_k(n) = \sqrt{\alpha_1[n]P_s}xe^{j\phi_k} + \sqrt{\alpha_2[n]P_s}w_k, \quad (2)$$

where x is confidential signals with $\mathbb{E}\{x^*x\} = 1$, ϕ_k is the initial vector of the kth antenna, and w_k is the artificial noise. The transmit power at time slot n is P_s, and $\alpha_1[n]$ and $\alpha_2[n]$ are the distribution ratio of transmit power to confidential signals and AN, respectively.

The above signals with AN are emitted to the open wireless channel. We assume that the wireless channel experiences a small-scale Rayleigh fading and a large-scale path loss. This channel consists of a LOS link and a NLOS one, where $P_L + P_N = 1$. The probability of the LOS link is related to the elevation angle θ and that of time slot n is defined as follows:

$$P_L(\theta[n]) = \frac{1}{1 + a\exp\left[-b((180^\circ/\pi)\theta[n] - a)\right]}, \quad (3)$$

where a and b are two constants, depending only on the wireless environment, which are provided in work [33]. Similarly, the probability of the NLOS link is denoted as follows:

$$P_N(\theta[n]) = 1 - P_L(\theta[n]). \quad (4)$$

By combining these two links, the expected channel power gain can be computed as follows:

$$|\rho(\theta[n])|^2 = \frac{\beta_0\eta_L P_L(\theta[n])}{R[n]^{\alpha_L}} + \frac{\beta_0\eta_N P_N(\theta[n])}{R[n]^{\alpha_N}}, \quad (5)$$

where $\beta_0 \triangleq 20\log_{10}(C/4\pi d_0 f_c)$ is the path loss at a reference distance $d_0 = 1$ meter. $R[n]$ is the distance of the first antenna of the UAV and the target receiver in time slot n. α_L and α_N denote the pass loss exponents for the LOS and NLOS links. η_L and η_N are the excessive path loss coefficients for the LOS and NLOS links.

Considering $R[n]$, we further define the distance between the kth antenna of the UAV, and the receiver is $R_k[n] = R[n] - (k-1)d\cos(\theta[n])$, where $d = C/2f_c$ is the distance between the antennas. Thus, the reference phase of $R[n]$ is $\varphi_0(R[n]) = 2\pi f_c(R[n]/C)$, and the phase shifting of the kth antenna is computed as follows:

$$\psi_k(\theta[n], R_k[n]) = \frac{2\pi(f_c + k_n\Delta f)R_k[n]}{C} - \varphi_0(R[n]), \quad (6)$$

where k_n is the serial number of the randomly selected subcarrier, corresponding to m.

In Figure 1, we assume that the elevation angle of the legitimate GT and the distance between the first reference antenna of the UAV and the GT are $(\theta_U[n], R_U[n])$. Similarly, these parameters of eavesdropper are $(\theta_E[n], R_E[n])$. For the GT, the received signals synthesized by all array antennas can be expressed as follows:

$$\begin{aligned} y(\theta_U[n], R_U[n]) &= \rho(\theta_U[n])\sqrt{\alpha_1[n]P_s}x \\ &\quad + \rho(\theta_U[n])\sqrt{\alpha_2[n]P_s}\mathbf{h}^H\mathbf{w} + \sum_{k=1}^{N_T} n_0, \end{aligned} \quad (7)$$

where $\mathbf{h}$ is a channel vector from UAV to the GT; i.e.,

$$\mathbf{h} = \frac{1}{\sqrt{N_T}}\left[e^{j\psi_1(\theta_U[n],R_U[n])},\cdots,e^{j\psi_{N_T}(\theta_U[n],R_U[n])}\right]^T. \quad (8)$$

And $n_0 \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise. $\mathbf{w}$ is the artificial noise that is designed in the zero space of $\mathbf{h}$, i.e., $\mathbf{w} = (\mathbf{I}_{N_T} - \mathbf{h}\mathbf{h}^H)\mathbf{z}$.Here, $\mathbf{z}$ is a vector

1: Input
$\mathbf{P}^{(0)}$: the initial power allocation coefficients.
$\mathbf{Q}^{(0)}$: the initial UAV 3D trajectory.
ξ_U^0: a slack variable.
2: **Set:** iteration index $i = 1$, the maximum iteration step $L = 20$, and the threshold $\omega = 10^{-3}$
3: **repeat**
4: Compute the optimal P^i by solving (20) with Q^{i-1}.
5: Compute the optimal Q^i by solving (27) with P^i
6: Obtain the current optimal objective function R^i
7: Update iteration index $i = i + 1$
8: **until**$(R - R_{\text{old}})/R_{\text{old}} \le \omega$ or $i > L$
9: **Output** the objective value $R_{\text{old}} = R^i$

Algorithm 1: The proposed hybrid iteration algorithm.

Table 2: Simulation parameters.

Parameters	Values
Number of antennas, N_T	4
Carrier frequency, f_c	3 GHz [21]
Bandwidth of subchannel, Δf	50 kHz
Channel gain, β_0	−42 dB
Duration of each time slot, δ_t	0.5 s [29]
UAV maximum velocity, $v_{\max}$	20.6 m/s [17, 35]
UAV minimum flight altitude, $h_{\min}$	100 m
UAV maximum flight altitude, $h_{\max}$	200 m
UAV maximum average transmit power, P_s	30 dBM [29]
Noise power, σ^2	−110 dBm [29]
Channel environment coefficients, a, b	20, 0.2 [33]
LOS link excess path loss coefficient, η_{L}	−2.14 dB [15]
NLOS link excess path loss coefficient, η_{N}	−3.14 dB [15]
LOS link path loss exponent, α_{L}	2
NLOS link path loss exponent, α_{N}	3

composed of N_T independent and identically distributed (i.i.d.) circular symmetric complex Gaussian random variables with zero mean and unit variance. It satisfies the distribution of $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}_{N_T})$. Thus, $\mathbf{h}^H\mathbf{w} = 0$ holds. The received signals of the GT can be rewritten as follows:

$$y(\theta_U[n], R_U[n]) = \rho(\theta_U[n])\sqrt{\alpha_1[n]P_s}x + \sum_{k=1}^{N_T} n_0. \tag{9}$$

Similarly, the received signals of the eavesdropper is defined as follows:

$$\begin{aligned} y(\theta_E[n], R_E[n]) &= \rho(\theta_E[n])\sqrt{\alpha_1[n]P_s}x \\ &\quad + \rho(\theta_E[n])\sqrt{\alpha_2[n]P_s}\boldsymbol{h_E}^H\boldsymbol{w} + \sum_{k=1}^{N_T} n_0, \end{aligned} \tag{10}$$

where $\mathbf{h_E}$ is a channel steering vector from the UAV to the eavesdropper. Then, we can derive the signal to interference plus noise ratio of the GT and eavesdropper as follows:

$$\gamma_U[n] = \frac{|\rho(\theta_U[n])|^2\alpha_1[n]P_s}{N_T\sigma^2}, \tag{11}$$

$$\gamma_E[n] = \frac{|\rho(\theta_E[n])|^2\alpha_1[n]P_s}{|\rho(\theta_E[n])|^2\alpha_2[n]P_s\|\mathbf{h_E}^H\mathbf{w}\|^2 + N_T\sigma^2}. \tag{12}$$

3.2. UAV Models. In the system, we consider the mobile UAV can fly in 3D space. And the distance of the flight in the nth time slot, $\mathbf{D}[n]$, satisfies the following constraints:

$$\|\mathbf{D}[n]\| = \|\mathbf{L}[n] - \mathbf{L}[n-1]\| \le v_{\max}\delta_t, n = 1, \cdots, N, \tag{13}$$

where $v_{\max}$ is the maximum flying speed of a UAV and $\|\cdot\|$ denotes the Euclidean norm of a vector. In addition, to avoid collisions with buildings and ensure effective communication links during flight, the flying height of a UAV should meet a height constraint, i.e.,

$$h_{\min} \le h[n] \le h_{\max}, n = 1, \cdots, N, \tag{14}$$

where $h_{\min}$ and $h_{\max}$ are the lowest and the highest height of a UAV.

For the mobile UAV, we introduce an AN projection matrix to the null space of a channel steering vector of confidential signals. In this case, signals received by the eavesdropper will have a phase offset. Thus, the eavesdropping correctness will be decreased. During the flight, if the total power of a UAV is P_{tot}, the transmit power at time slot n is computed as follows:

$$P_s \triangleq P_{\text{tot}}/N. \tag{15}$$

And the power allocation of confidential signals and AN is as follows:

$$\alpha_1[n] + \alpha_2[n] = 1, \alpha_1[n], \alpha_2[n] \ge 0, \forall n \in N. \tag{16}$$

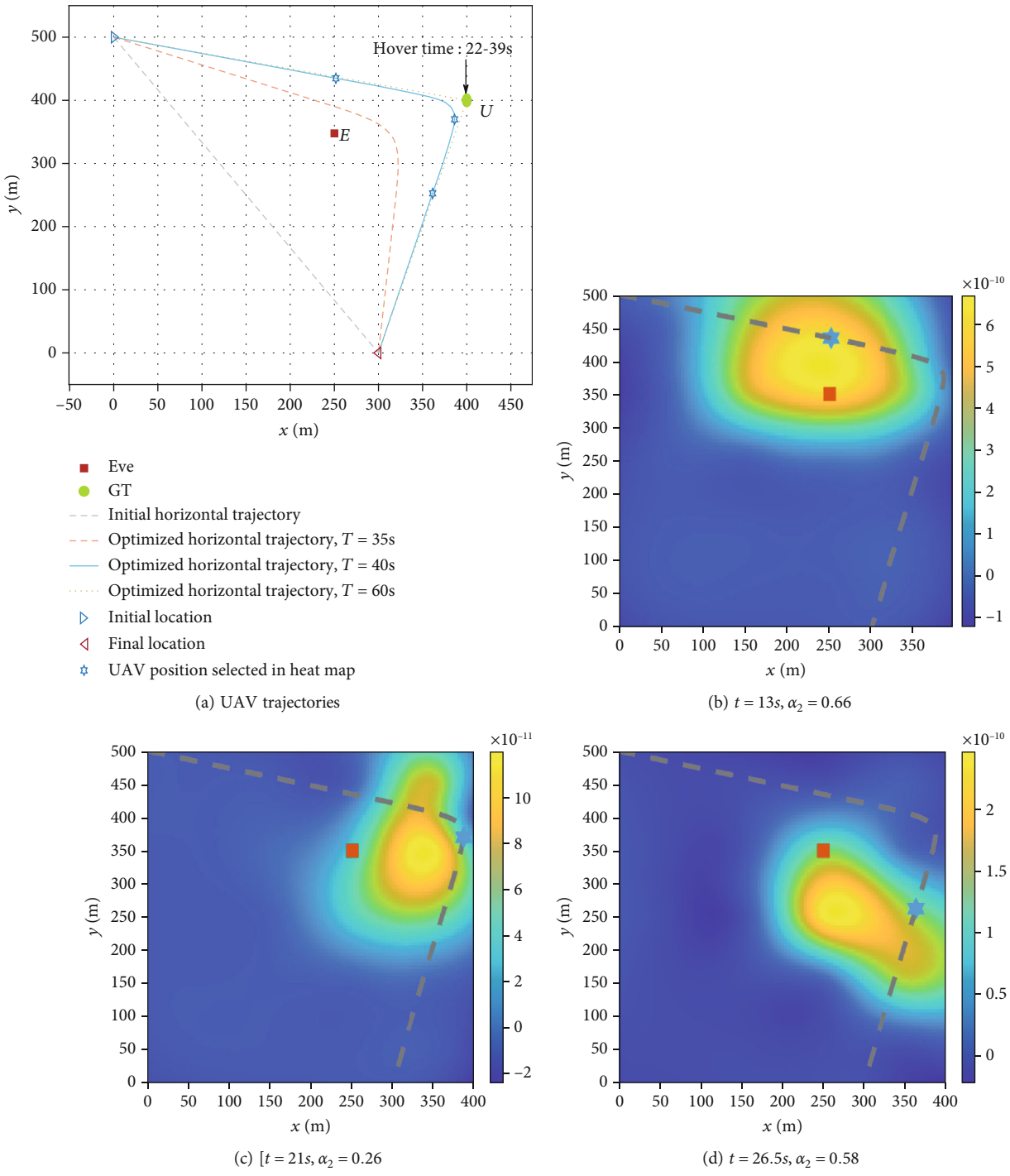

Figure 2: Horizontal trajectories analysis and jamming temperatures at different positions with $T = 40\,s$.

In the next section, we expect to find the optimal power distribution ratio by changing transmit power.

3.3. Problem Formulation. In order to realize secure communication of a UAV-ABS network, we exploit the RSCS-OFDM-DM technology to maximize the average secrecy rate by jointly optimizing UAV trajectory and the UAV power allocation ratio. The maximization problem is as follows:

$$\begin{aligned} \max_{\mathbf{Q},\mathbf{P}} \quad & SR \\ \text{s.t.} \quad & (13), (14), \text{and } (16), \end{aligned} \tag{17}$$

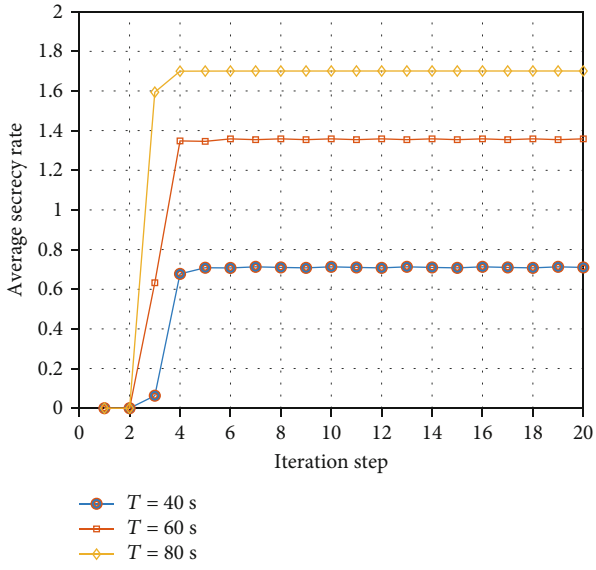

Figure 3: Convergence analysis.

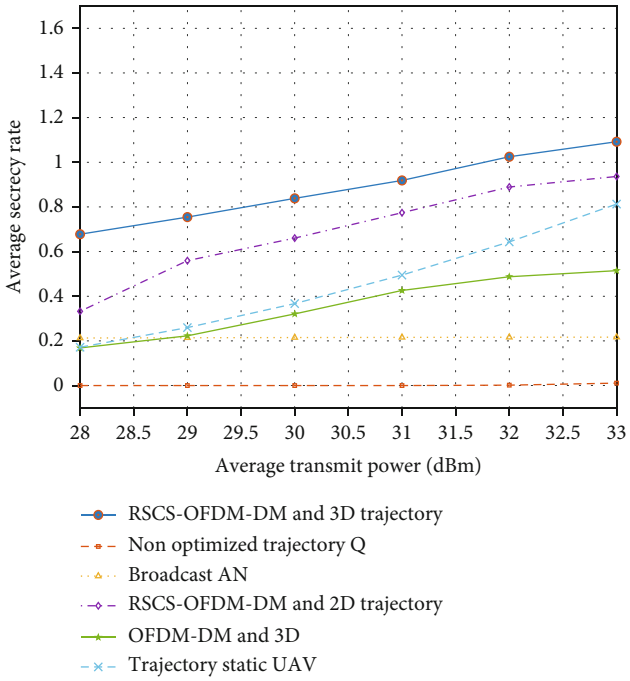

Figure 4: ASR *vs* transmit power.

where $\mathbf{Q} \triangleq \{\mathbf{L}[n] \in \mathbb{R}^{3\times 1} | \forall n\}$ represents the position set of a UAV, $\mathbf{P} \triangleq \{\alpha_i[n] \in \mathbb{R} | i \in \{1, 2\}, \forall n\}$ is the set of power allocation coefficients, and the objective function is defined as follows:

$$SR = \frac{1}{N}\sum_{n=1}^{N}\left[\log_2(1+\gamma_U[n]) - \log_2(1+\gamma_E[n])\right]^+, \tag{18}$$

where $[a]^+ = \max\{a, 0\}$; when the secrecy rates are favorable, UAVs and legitimate ground nodes can communicate normally.

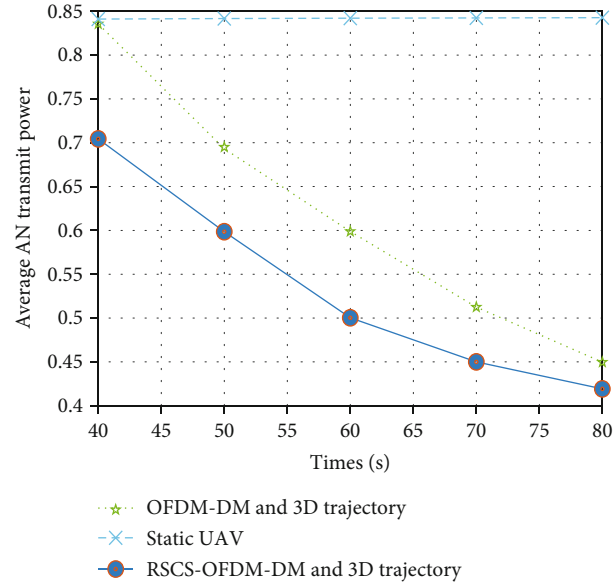

Figure 5: Average AN power.

4. Maximal ASR Scheme Design

Solving problem (17) directly is challenging due to its nonconvexity. We use AO and SCA methods to find the approximate optimal solution of (17). In particular, we study the optimization problem from two perspectives, i.e., UAV transmit power allocation and UAV 3D trajectory design during each flight time slot.

4.1. Power Allocation Subproblem. In this subproblem, we assume that the UAV source 3D trajectory is predefined. We introduce two slack variables, τ and $\mathbf{u}$, into (17). Then, the UAV transmit power allocation subproblem is formulated as follows:

$$\max_{\boldsymbol{P},\tau,\boldsymbol{u}} \tau \tag{19a}$$

$$\text{s.t.} \frac{1}{N}\sum_{n=1}^{N}\{\log_2(1+A_1[n]\alpha_1[n]) - \mu[n]\} \geq \tau, \tag{19b}$$

$$\log_2\left(1+\frac{A_2[n]\alpha_1[n]}{A_3[n](1-\alpha_1[n])+1}\right) \leq \mu[n], \tag{19c}$$

$$\text{and } (16),$$

where $\mathbf{u} \triangleq \{\mu[n] \in \mathbb{R} | n \in N\}$ is the upper boundary of eavesdropper's transmit rate, $A_1[n] = |\rho(\theta_U[n])|^2 P_s/N_T\sigma^2$, $A_2[n] = |\rho(\theta_E[n])|^2 P_s/N_T\sigma^2$, and $A_3[n] = |\rho(\theta_E[n])|^2 P_s \|\boldsymbol{h_E}^H \boldsymbol{w}\|^2/N_T\sigma^2$. Because the UAV trajectory is predefined, $A_1[n]$, $A_2[n]$, and $A_3[n]$ can be regarded as constants. Yet, the constraint (19c) is still nonconvex. Then, we further transform it based on the first-order Taylor approximation method; i.e., $g(x) = g(x^*) + g'(x^*)(x - x^*)$, where x^* is the result of

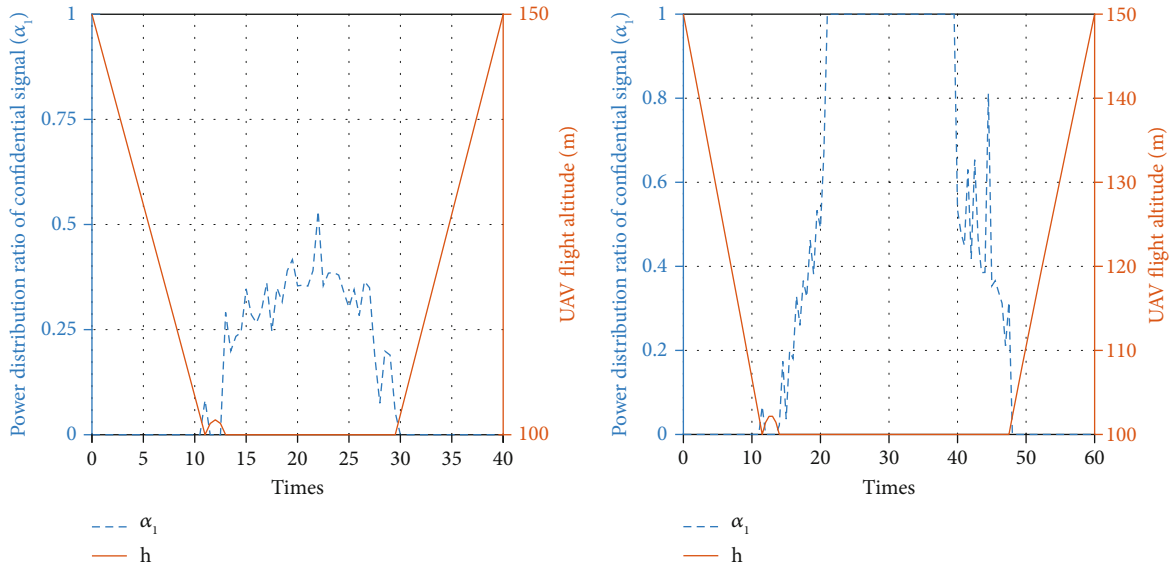

FIGURE 6: The altitude and power allocation coefficient.

the previous iteration x. Then, (19c) can be rewritten as follows:

$$\begin{aligned} \max_{\mathbf{P},\tau,\mathbf{u}} \quad & \tau \\ g(\alpha_1[n]) \le \mu[n], \quad & \\ \text{s.t.} \quad & (16) \text{ and } (19b). \end{aligned} \tag{20}$$

We can exploit CVX toolbox to solve the subproblem since it satisfies the convex optimization requirements.

4.2. UAV 3D Trajectory Subproblem. When the power allocation coefficients are known, we still introduce two slack variables, $\zeta_{\mathbf{U}}$ and $\zeta_{\mathbf{E}}$, to simplify the original problem to the UAV 3D trajectory subproblem as follows:

$$\max_{\mathbf{Q},\zeta_{\mathbf{U}},\zeta_{\mathbf{E}}} \frac{1}{N}\sum_{n=1}^{N} SR[n], \tag{21a}$$

$$\text{s.t.} \xi_U[n] \ge \|\boldsymbol{L}[n] - \boldsymbol{U}\|^2, \tag{21b}$$

$$\xi_E[n] \le \left\|\boldsymbol{L}[n] - \boldsymbol{E}^2\right\|, \tag{21c}$$

$$\xi_U[n] \ge h_{\min}^2, \tag{21d}$$

where $SR[n] = \log_2(1 + D_1[n]|\rho(\theta_U[n])|^2) - \log_2(1 + (D_1[n]|\rho(\theta_E[n])|^2/D_2[n]|\rho(\theta_E[n])|^2 + 1))$, $\zeta_{\mathbf{U}} \triangleq \{\xi_U[n]|\forall n\}$, $\zeta_{\mathbf{E}} \triangleq \{\xi_E[n]|\forall n\}$, $D_1[n] = \alpha_1[n]P_s/N_T\sigma^2$, and $D_2[n] = \alpha_2[n]P_s\|\boldsymbol{h_E}^H\boldsymbol{w}\|^2/N_T\sigma^2$. Because the flight time slot of the UAV is tiny, we assume that the elevation change before and after trajectory iteration is small. The channel power gains of the legitimate GT and the eavesdropper can be rewritten as follows:

$$|\rho_U[n]|^2 = \frac{\eta_{\mathrm{L}}P_{\mathrm{L}}(\theta_U^*[n])\beta_0}{\xi_U[n]^{\alpha_{\mathrm{L}}/2}} + \frac{\eta_{\mathrm{N}}P_{\mathrm{N}}(\theta_U^*[n])\beta_0}{\xi_U[n]^{\alpha_{\mathrm{N}}/2}}, \tag{22}$$

$$|\rho_E[n]|^2 = \frac{\eta_{\mathrm{L}}P_{\mathrm{L}}(\theta_E^*[n])\beta_0}{\xi_E[n]^{\alpha_{\mathrm{L}}/2}} + \frac{\eta_{\mathrm{N}}P_{\mathrm{N}}(\theta_E^*[n])\beta_0}{\xi_E[n]^{\alpha_{\mathrm{N}}/2}}. \tag{23}$$

Then, the objective function can be rewritten as follows:

$$\widetilde{SR}[n] = \log_2\left(1 + D_1[n]|\rho_U[n]|^2\right) - \log_2\left(1 + \frac{D_1[n]|\rho_E[n]|^2}{D_2[n]|\rho_E[n]|^2 + 1}\right). \tag{24}$$

Note that the constraint (21c) is still a nonconvex constraint on $\mathbf{L}[n]$, which causes the subproblem to be nonconvex. We use the SCA method to transform this nonconvex subproblem into a convex one. We assume that the coordinate of the previous iteration is $\mathbf{L}^*[n]$. Since the first-order Taylor expansion of a convex function at one point is its lower bound, the constraints (21c) and $\widetilde{SR}[n]$ can be approximates as follows:

$$\xi_E[n] \le 2(\mathbf{L}^*[n] - \mathbf{E})^T(\mathbf{L}[n] - \mathbf{L}^*[n]) + \|\mathbf{L}^*[n] - \mathbf{E}\|^2, \tag{25}$$

$$\widetilde{SR}[n] \ge \widehat{SR}^*[n] = g(\xi_U[n]) - \log_2\left(1 + \frac{D_1[n]|\rho_E[n]|^2}{D_2[n]|\rho_E[n]|^2 + 1}\right), \tag{26}$$

where $g(\xi_U[n])$ is also the first-order Taylor expansion of the first term in (24). Accordingly, the subproblem (21a) is approximately equivalent to the following convex problem:

$$\max_{\mathbf{Q},\zeta_U,\zeta_E} \quad \frac{1}{N}\sum_{n=1}^{N}\widehat{SR}^*[n] \tag{27}$$
$$\text{s.t.} \quad (13), (14), (21b), (21d), \text{and } (25).$$

4.3. Hybrid Iteration Algorithm. We design a hybrid iteration algorithm to solve the problem (17). In the ith iteration, we obtain the optimal transmit allocation ratio $\mathbf{P}^i$ with a given UAV 3D trajectory $\mathbf{Q}^{i-1}$ by solving subproblem (20). Next, the optimal UAV 3D trajectory is $\mathbf{Q}^i$ with a given transmit allocation ratio of $\mathbf{P}^i$ by solving the subproblem (27). The details of our algorithm are summarized in **Algorithm**1.

In each iteration of Algorithm 1, two convex subproblems (20) and (27) are solved by SCA algorithm. We define that the number of UAVs is K, the number of GTs is M, and the number of time slots is N. The number of optimization variables in (20) is only related to K and N. If the number of iterations is assumed to be L_1, the computational complexity of (20) can be calculated as $\mathcal{O}(L_1K^3N^3)$ [34]. Similarly, the number of optimization variables in (27) is related to K, M, and N. And the computational complexity of (27) is $\mathcal{O}(L_2K^3M^3N^3)$ when the number of iterations is L_2. Therefore, the computational complexity of **Algorithm1** is $\mathcal{O}(L(L_1K^3N^3 + L_2K^3M^3N^3))$, where L is the iteration number of Algorithm 1.

5. Simulation and Discussion

In this section, we evaluate the performance of our proposed scheme through numerical simulation. Unless otherwise specified, simulation parameters are shown in Table 2.

In Figure 2, we first discuss the optimal trajectory of the UAV and the corresponding interference temperature. According to Algorithm 1, we find the optimal horizontal trajectory of the UAV under flight time $T = 35$ s, 40 s, and 60 s, as shown in Figure 2(a) It is found that as flight time increased, the UAV preferred to stay closer to the GT and away from the eavesdropper to increase the ASR. In particular, the UAV will hover over the legitimate GT as long as possible to increase the ASR when $T = 60$ s. Figures 2(b)–2(d) demonstrate that the ground eavesdropper is subject to intense interference temperature at three different positions of UAV's flight trajectory. In Figure 2(c), $\alpha_2 = 0.26$, the transmitted AN is relatively small, so the order of magnitude of the interference temperature is smaller than Figures 2(b) and 2(d). Compared with Figure 2(d), the eavesdropper in Figures 2(c) and 2(d) is located at the edge of the interference temperature mass. The interference temperature is constrained by the AN power and the distance between the UAV and the ground eavesdropper. In addition, we find that the interference temperature radiates to the eavesdropper with the UAV as the center in Figure 2(b). Yet, the center of the interference temperature in Figures 2(c) and 2(d) Figure appears between the UAV and the eavesdropper's position with a slight offset. The reason is that AN signals sent by the UAV is affected by GT's positions.

In Figure 3, we discuss the convergence of the proposed algorithm at flight time $T = 40$ s, 60 s, and 80 s. The ASR of the first two iterations is almost zero because the trajectory optimization of the UAV at the beginning of the iteration is similar to the initial trajectory. Then, the ASR increases sharply as the increasing number of iterations and gradually converges to a fixed value after four or five iterations. It shows that the proposed algorithm can effectively converge to the optimal solution. Also, the longer the flight time, the higher ASR after convergence. The reason is that the hovering time of the UAV becomes longer as the flight time increases.

In order to verify the effectiveness of our iterative algorithm, we next compare the ASR performance of different schemes in Figure 4. In the figure, we know that the ASR performances of either two-dimensional (2D) or 3D trajectory optimization are greater than that of static UAV and nonoptimized trajectory schemes. This explains the impact of trajectory optimization on the system secrecy performance. The reason is that the UAV trajectory design can help to obtain a better channel between a UAV and a GT. In addition, the RSCS-OFDM-DM technology has a better jamming effect on an eavesdropper via comparing with OFDM-DM and broadcast AN schemes. Overall, the proposed algorithm can jointly optimize the 3D flight trajectory and transmit signal power to improve physical layer security of the UAV-enabled network. Then, we compare the average transmit AN power of different schemes in Figure 5. It shows that the scheme using both random subcarrier selection and mobile UAV has higher energy efficiency. In the case of the same total transmit power, our scheme can send the smallest average transmit AN power to achieve the same secrecy performance.

Figure 6 provides the impact of the UAV's flight altitude h on power distribution ratio of confidential signals when the flight durition is $T = 40$ s and $T = 60$ s, respectively. It can be seen that h is inversely proportional to α_1. When the UAV is closer to the eavesdropper and farther from the GT, $\alpha_1 = 0$. This means that all transmit power is used to emit artificial noise. As the UAV approaches the GT and the eavesdropper, α_1 increases, while the UAV's altitude decreases. It can improve the quality of the channel between the UAV and the legitimate ground node to ensure secure communication. For the $T = 60$ s case, the UAV hovers over the GT during the period of 22 s to 39 s. In this period, the quality of the legitimate channel is the best. All power is used to transmit confidential signals.

6. Conclusion

In this paper, we study how to improve security of data transmission for a UAV-enabled edge network by jointly optimizing the 3D flight trajectory and power allocation design. First, we formulate an optimization problem by

establishing a UAV communication system model based on the RSCS-OFDM-DM technology. Next, we divide the optimization problem into two subproblems for discussion, i.e., UAV transmit power allocation and UAV 3D trajectory design, and then present a hybrid iterative algorithm to find the optimal solution of the optimization problem. Finally, we compare the secrecy performance of the proposed scheme with other five schemes. Also, we verify that the mobile UAV and random subcarrier selection can improve the secrecy energy efficiency.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2019JBZ001, in part by the Beijing Natural Science Foundation, under Grant 4202054, in part by the National Natural Science Foundation of China, under Grant 61871023, in part by the Hangzhou Innovation Institute, Beihang University, under Grant 2020-Y5-A-022, and in part by the S&T Program of Hebei, under Grant SZX2020034.

References

[1] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.

[2] S. Han, X. Xiaodong, S. Fang et al., "Energy efficient secure computation offloading in NOMA-based mMTC networks for IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5674–5690, 2019.

[3] X. Sun, D. W. K. Ng, Z. Ding, X. Yanqing, and Z. Zhong, "Physical layer security in UAV systems: challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[4] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[5] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[6] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[7] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.

[8] W. Wang, J. Tang, N. Zhao et al., "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 5028–5040, 2020.

[9] Y. Huo, Y. Tian, H. Chunqiang, Q. Gao, and T. Jing, "Jamming strategies for physical layer security," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 1832051, 11 pages, 2017.

[10] S. Enayati, H. Saeedi, H. Pishro-Nik, and H. Yanikomeroglu, "Moving aerial base station networks: a stochastic geometry analysis and design perspective," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 2977–2988, 2019.

[11] Z. Cai, Z. Xiong, X. Honghui, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: a survey toward private and secure applications," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–38, 2021.

[12] M. T. Mamaghani and Y. Hong, "Joint trajectory and power allocation design for secure artificial noise aided UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2850–2855, 2021.

[13] R. Li, Z. Wei, L. Yang, D. W. K. Ng, J. Yuan, and J. An, "Resource allocation for secure multi-UAV communication systems with multi-eavesdropper," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4490–4506, 2020.

[14] J. Lyu and H.-M. Wang, "Secure UAV random networks with minimum safety distance," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2856–2861, 2021.

[15] W. Huici, Y. Wen, J. Zhang, Z. Wei, N. Zhang, and X. Tao, "Energy-efficient and secure air-to-ground communication with jittering UAV," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 3954–3967, 2020.

[16] W. Huici, H. Li, Z. Wei, N. Zhang, and X. Tao, "Secrecy performance analysis of air-to-ground communication with UAV jitter and multiple random walking eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 572–584, 2021.

[17] H.-M. Wang and X. Zhang, "UAV secure downlink NOMA transmissions: a secure users oriented perspective," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5732–5746, 2020.

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

[19] C. Shengnan, J. Xiangdong, G. Yixuan, and Z. Yuhua, "Physical layer security communication of cognitive UAV mobile relay network," in *2021 7th International Symposium on Mechatronics and Industrial Informatics (ISMII)*, pp. 267–271, Zhuhai, China, 2021.

[20] Y. Roh, S. Jung, and J. Kang, "Cooperative UAV jammer for enhancing physical layer security: robust design for jamming power and trajectory," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, pp. 464–469, Norfolk, VA, USA, 2019.

[21] T. Shen, S. Zhang, R. Chen et al., "Two practical random-subcarrier-selection methods for secure precise wireless transmissions," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9018–9028, 2019.

[22] F. Shu, W. Xiaomin, H. Jinsong, J. Li, R. Chen, and J. Wang, "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 890–904, 2018.

[23] J. Ren and Y. Guanding, "Collaborative cloud and edge computing for latency minimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 5031–5044, 2019.

[24] S.-H. Park, S. Jeong, J. Na, O. Simeone, and S. Shamai, "Collaborative cloud and edge mobile computing in C-RAN systems with minimal end-to-end latency," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 259–274, 2021.

[25] Q. Zhang, L. Gui, F. Hou, J. Chen, S. Zhu, and F. Tian, "Dynamic task offloading and resource allocation for mobile-edge computing in dense cloud RAN," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3282–3299, 2020.

[26] H. Zhou, K. Jiang, X. Liu, X. Li, and V. C. M. Leung, "Deep reinforcement learning for energy-efficient computation offloading in mobile-edge computing," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1517–1530, 2022.

[27] X. Chen, G. Zheng, and X. Zhao, "Energy-minimization task offloading and resource allocation for mobile edge computing in NOMA heterogeneous networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 16001–16016, 2020.

[28] Y. Dai, K. Zhang, S. Maharjan, and Y. Zhang, "Edge intelligence for energy-efficient computation offloading and resource allocation in 5G beyond," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12175–12186, 2020.

[29] L. Weidang, Y. Ding, S. H. Yuan Gao, W. Yuan, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2022.

[30] X. Yu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 573–588, 2021.

[31] Y. Zhe, Y. Gong, S. Gong, and Y. Guo, "Joint task offloading and resource allocation in UAV-enabled mobile edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3147–3159, 2020.

[32] T. Salam, W. U. Rehman, and X. Tao, "Data aggregation in massive machine type communication: challenges and solutions," *IEEE Access*, vol. 7, pp. 41921–41946, 2019.

[33] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569–572, 2014.

[34] C. Zhan and Y. Zeng, "Aerial–ground cost tradeoff for multi-UAV-enabled data collection in wireless sensor networks," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1937–1950, 2020.

[35] DJI, "DJI inspire 2 technical parameters," https://www.dji.com/inspire-2.