Received: 3 June 2021 | Revised: 21 November 2021 | Accepted: 18 December 2021

IET Communications

DOI: 10.1049/cmu2.12326

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Joint trajectory design and power allocation for unmanned aerial vehicles aided secure transmission in the presence of no-fly zone

Guoxiao Yin[1,2] | Xiaotian Zhou[1,2] | Piming Ma[2,3] | Fang Fang[4] | Peng Zhao[2,3]

[1] School of Control Science and Engineering, Shandong University, China

[2] Shandong Key Laboratory of Wireless Communication Technologies, Shandong University, China

[3] School of Information Science and Engineering, Shandong University, China

[4] Department of Engineering, Durham University, UK

Correspondence
Xiaotian Zhou, School of CSE, Shandong University, 17923 Jingshi Road, Jinan 250061, P. R. China.
Email: xtzhou@sdu.edu.cn;
Piming Ma, School of CSE, Shandong University, 17923 Jingshi Road, Jinan 250061, P. R. China.
Email: mapiming@sdu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61860206005, 61971270; Natural Science Foundation of Shandong Province, Grant/Award Number: ZR2019QF016; The Major Scientific and Technological Innovation Project of Shandong Province, Grant/Award Numbers: 2019JZZY010111, 2020CXGC010108

Abstract

Unmanned aerial vehicles (UAVs) are widely considered as key enablers for future wireless networks due to their advantages, such as high mobility and flexible deployment. In this paper, the UAV assisted secure communication system is investigated, where the UAV is deployed as the mobile jammer to prevent the eavesdropper from overhearing the confidential message. With the objective of maximizing the secrecy rate, a joint optimization problem involving the trajectory and transmit power of UAV, as well as the transmit power of source node is formulated. Moreover, the effects of Non-Fly Zone (NFZ) and imperfect estimation on the location of eavesdropper are also taken into consideration. As the original problem is hardly trackable, the worst case secrecy rate (WCSR) assumption is first employed to bypass the uncertainty brought by the estimation error. Then a block coordinate descent (BCD) based algorithm is proposed to decompose the problem into three sub-ones, where the trajectory of UAV, the transmit power of UAV and the transmit power of source can be obtained in an iterative manner. Simulation results reveal that the proposed algorithm can improve the secrecy performance significantly. In addition, the robustness of the proposed algorithm under the estimation error can also be verified.

1 | INTRODUCTION

The broadcasting nature of electromagnetic waves brings huge challenges to the privacy and information security of wireless communications. The traditional encryption techniques, which rely on the robustness of upper layer encryption algorithms, would consume a large amount of processing energy and hence reduce the lifespan of user equipment. Moreover, it is difficult to guarantee the information security once the malicious node has prior information or enough computation power to perform the decryption [1]. As an alternative, physical layer security was proposed as a promising approach to combat against the eavesdropping effectively [2]. The concept of physical layer secrecy was originally illustrated by Shannon [3] and then developed by Wyner [4] in terms of information theoretical security, where the secrecy rate was defined as a key metric to determine the quality of privacy. The secrecy rate suggests the exact amount of confidential information that can be reliably delivered in the presence of adversaries. To achieve the maximum security rate, numerous physical layer techniques were reported, such as beamforming [5, 6], artificial noise jamming [7], resource allocation [8, 9] etc.

On the other hand, the unmanned aerial vehicle (UAV) enabled wireless communications have been extensively studied recently as one potential technique for future wireless networks [10, 11]. Owing to the attractive features such as high mobility, flexibility and on-demand deployment, UAV can act as the aerial base station (BS) or relay node to help expand the coverage area and enhance the capacity of the network [12–16]. Moreover, recent research also reveals its potential in secure transmission [17–25]. For instance, [17] considered maximizing

the average security rate of the UAV based network by properly adjusting the transmit power and trajectory of UAV. An iterative algorithm is proposed in [18] to improve the security of the UAV based mobile relay system by optimizing the transmit powers of both relay and source node as well as the trajectory of UAV. The authors in [19] maximize the secrecy rate by optimizing the source/relay transmission power in UAV-enabled relaying system, where the formulated non-convex problem is solved by introducing difference-of-concave (DC) programming and a closed-form solution is derived for reducing the complexity of the proposed algorithm under a special case. In [20], a suboptimal algorithm with respect to the UAV trajectory planning is proposed, where the secure throughput per propulsion energy cost is maximized.

Another approach to improve the system security is to employ UAV as a jammer to transmit the interfering signals to the eavesdroppers [21]. Due to the high mobility of UAV, it can approach closer to the eavesdropper to deliver a better jamming effect while at the same time maintain low interference to the legitimate user. In such a context, [22] investigated the impact of the jamming power and spatial deployment of UAV on the security performance of the system, where a low complexity algorithm was proposed to maximize the defined intercept probability security region. [23] developed a novel secure transmission scheme through deploying two UAVs, with one transmitting the confidential messages to the users and the other jamming the eavesdropper. The minimum average secrecy rate is greatly improved through jointly optimizing the trajectories and transmitting power of the two UAVs. To combat eavesdropping of adversaries and maximize the secrecy rate of the system, a cooperative jamming strategy with two UAVs is proposed in [24]. In [25], the multiple UAVs enabled cooperative secure transmission scheme with multiple potential eavesdroppers was investigated. With the objective of maximizing the secure energy efficiency of the system, an iterative algorithm is proposed to deal with the power allocation and trajectory design in a successive manner.

Though numerous works have confirmed the promising performance of UAV assisted secure transmission, there are still challenges when implementing such an idea in practical scenario. For instance, the no-fly zones (NFZs), which caused by the geographic or policies restrictions, would impact the trajectory of UAV and consequently the secure performance of the system [26, 27]. On the other hand, the imperfect channel state information due to the uncertain location of the passive eavesdropper and complex air-terrestrial environment, should also be taken into consideration. Note that in some special cases, the eavesdropper might also be the legitimate user but without the authority to some certain message. As a result, the perfect CSI of the eavesdropper is still available to the system [28, 29]. However, for most scenarios, the perfect CSI between the transmitter and eavesdropper is hardly obtained as the malicious users are usually passive eavesdroppers. In such a case, only partial CSI is available, based on the rough location of eavesdropper captured via the friendly UAV equipped with camera or synthetic aperture radar [30].

Motivated by above-mentioned challenges, in this paper, we investigate a typical secure transmission system with one source node transmitting confidential information to the destination node. To prevent the eavesdropper from overhearing the message, one friendly UAV is deployed to send the interfering signals to the eavesdropper. Different from existing work, we consider both the imperfect location information of eavesdropper and the NFZs of UAV in the proposed scenario. With the objective of maximizing the secrecy rate of the system, a joint optimization problem, which considers the trajectory and jamming power of UAV, as well as the transmit power of source node is formulated. To bypass the uncertainty induced by the imperfect location information of eavesdroppers, the worst-case secrecy rate (WCSR) method is employed to convert the original problem into a more tractable one [31, 32]. As the converted problem is still non-convex, we opt to the block coordinate descent method (BCD) and propose an iterative algorithm to optimize the trajectory and jamming power of UAV, and the transmit power of source node in a successive manner. Simulations confirm the efficiency and robustness of the proposed algorithm.

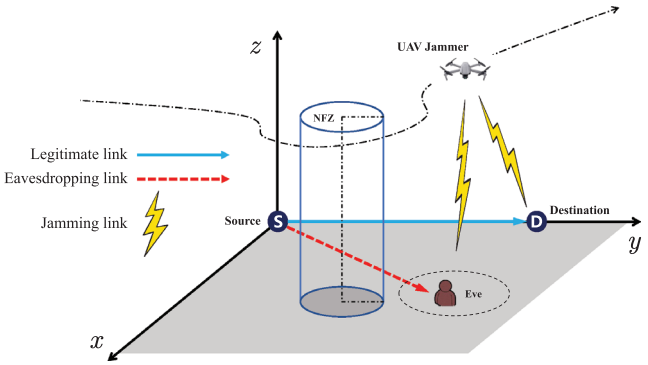

FIGURE 1 The three-terminal terrestrial communication system with a jamming UAV

The rest of the paper is organized as follows. Section 2 introduces the system model. In Section 3, the secrecy rate maximization problem is formulated. The proposed iterative algorithm is illustrated in Section 4, where the discussion on its complexity is also included. Section 5 provides numerical results to verify the performance of the proposed scheme and Section 6 concludes the paper.

2 | SYSTEM MODEL

As depicted in Figure 1, we consider a typical point to point wireless communication system with one source node S transmitting confidential information to the destination node D. There also exists an eavesdropper E who tries to overhear the message. To prevent it, a friendly UAV is deployed to broadcast the interfering signal to the eavesdropper. Taking advantage of high mobility, the UAV tends to fly close to E to get a better jamming effect. However, the limited energy supply restricts its flight range and also the power of the jamming signal it sent. Consequently, the trajectory and power control policy of UAV would impact the jamming effect greatly, which should be

carefully designed. To do so, the location information of these terrestrial nodes is required by the UAV.

We assume that the locations of the two legitimate terrestrial nodes S and D, denoted by their horizontal coordinates as $\mathbf{w}_S = (x_S, y_S)^\dagger$ and $\mathbf{w}_D = (x_D, y_D)^\dagger$, are fixed and known by the friendly UAV, where the superscript † stands for transpose. As for the eavesdropper, though the precise location $\mathbf{w}_E = (x_E, y_E)^\dagger$ is hardly obtained, its rough version $\mathbf{w}_e = (x_e, y_e)^\dagger$ can be estimated [32]. Assuming that $\mathbf{w}_E$ is placed somewhere within a circle with $\mathbf{w}_e$ as the center and r_E as the radius, the relationship between them can be expressed as:

$$\mathbf{w}_E = \mathbf{w}_e + \Delta\mathbf{w}, \tag{1}$$

where $\Delta\mathbf{w}$ is the estimation error, written as:

$$\Delta\mathbf{w} \in \varepsilon_E = \left\{(\Delta x_E, \Delta y_E)^\dagger | \Delta x_E^2 + \Delta y_E^2 \le r_E^2\right\}. \tag{2}$$

On the other hand, the UAV hovers at an altitude of H and can fly from the initial location $\mathbf{q}_0$ to the destination $\mathbf{q}_F$ during time frame T. To track its trajectory in a convenient way, we divide T into N successive time slots with equal length δ. Note that δ is chosen sufficiently small so the instantaneous location of UAV in the same time slot can be regarded unchanged, from the viewpoint of the ground node. Then the horizontal trajectory of UAV over the flight time T can be modeled by a discrete sequence $\tilde{\boldsymbol{q}} = \{\mathbf{q}[n], n \in \mathcal{N}\} = \{(x[n], y[n])^\dagger, n \in \mathcal{N}\}$, where $\mathcal{N} = \{1, \ldots, N\}$. The mobility constraints of UAV is therefore expressed as:

$$\|\mathbf{q}[n+1] - \mathbf{q}[n]\|^2 \le L^2, \quad n = 0, 1, 2, \ldots N-1, \tag{3}$$

where $L = \delta V_{max}$ is the maximum horizontal distance that the UAV can fly within a time slot, and V_{max} is the maximum horizontal speed of UAV. $\mathbf{q}[0] = \mathbf{q}_0$ denotes the starting point and $\mathbf{q}[N] = \mathbf{q}_F$ represents the final destination.

Furthermore, recall that NFZs are also considered in the scenario, where the UAV is banned from flying over. We assume that there are J NFZs in the system, each of which is modeled as a cylindrical region with a horizontal center at $\mathbf{w}_j^{NF} = (x_j^{NF}, y_j^{NF})^\dagger$ and a radius of $r_j, j \in \mathcal{J} = \{1, 2, \ldots, J\}$. Note that the heights of these NFZs are assumed to be large enough so that the UAV can never leap them. Then the corresponding constraints on the trajectory of UAV, owning to the NFZs can be expressed as

$$\|\mathbf{q}[n] - \mathbf{w}_j^{NF}\|^2 \ge r_j^2, \quad \forall j, n = 1, 2, \ldots, N-1. \tag{4}$$

With the preliminaries above, we then focus on the achievable secrecy rate of the proposed system, which can be calculated as the difference between the achievable rate of D and the eavesdropping rate of E. Note that though the purpose of deploying UAV is to jam the eavesdropper E, it also interferes D due to the broadcasting nature of electromagnetic waves. Denoting $P_S[n]$ and $P_U[n]$ the transmit power of S and the UAV during time slot n, respectively, the corresponding ergodic achievable rate of D can be expressed as:

$$R_D[n] = \mathbb{E}\left[\log_2\left(1 + \frac{P_S[n] g_{SD}}{P_U[n] h_{UD}[n] + \sigma^2}\right)\right], \tag{5}$$

where $\mathbb{E}[\cdot]$ is the expectation operator and σ^2 is the power of additive white Gaussian noise. $h_{UD}[n]$ and g_{SD} represents the channel gain from the UAV to D and S to D, respectively. The former is dominated by the LoS channel, which depends mainly on the path loss of the link as [34]:

$$h_{UD}[n] = \frac{\rho_0}{\|\mathbf{q}[n] - \mathbf{w}_D\|^2 + H^2}, \tag{6}$$

where ρ_0 denotes the reference channel power gain at distance of 1 meter. Note that $h_{UD}[n]$ varies with different n since the relative distance between D and UAV changes among different time slots.

On the other hand, the link from S to D, as the ground-to-ground one, is assumed to be the independent Rayleigh fading channel. Hence, g_{SD} is given by

$$g_{SD} = \rho_0 d_{SD}^{-\varphi} \xi_D = \frac{\rho_0 \xi_D}{\|\mathbf{w}_D - \mathbf{w}_S\|^\varphi}, \tag{7}$$

where $d_{SD} = \|\mathbf{w}_D - \mathbf{w}_S\|$ is the distance from S to D and φ is the path loss exponent. ξ_D is exponentially distributed random variable with unit mean.

Similar to the above process, one can also derive the ergodic eavesdropping rate at E as:

$$R_E[n] = \mathbb{E}\left[\log_2\left(1 + \frac{P_S[n] g_{SE}}{P_U[n] h_{UE}[n] + \sigma^2}\right)\right], \tag{8}$$

where $h_{UE}[n]$ and g_{SE} is the channel gain from the UAV to E and S to E, respectively. Similar to that in (6) and (7), they can further be written as:

$$\begin{aligned} h_{UE}[n] &= \frac{\rho_0}{\|\mathbf{q}[n] - \mathbf{w}_E\|^2 + H^2} \\ &= \frac{\rho_0}{\|\mathbf{q}[n] - (\mathbf{w}_e + \Delta\mathbf{w})\|^2 + H^2}, \end{aligned} \tag{9}$$

$$g_{SE} = \rho_0 d_{SE}^{-\varphi} \xi_E = \frac{\rho_0 \xi_E}{\|\mathbf{w}_e + \Delta\mathbf{w} - \mathbf{w}_S\|^\varphi}, \tag{10}$$

where $d_{SE} = \|\mathbf{w}_E - \mathbf{w}_S\| = \|\mathbf{w}_e + \Delta\mathbf{w} - \mathbf{w}_S\|$ is the distance from S to E. ξ_E is exponentially distributed random variable with unit mean.

Apparently, the exact value of $R_E[n]$ is difficult to get due to the uncertainty in $\Delta\mathbf{w}$, which is caused by the imperfect estimation on the location of the eavesdropper. Consequently, the exact value of the ergodic secrecy rate, which is the difference between $R_D[n]$ and $R_E[n]$, is also hardly calculated. To bypass this and also guarantee the secrecy performance of the system, we opt to the WCSR, which is the minimum secrecy rate under

arbitrary $\Delta\mathbf{w} \in \varepsilon_E$ [31]. That is:

$$R_{sec}[n] = \left(R_D[n] - \max_{\Delta\mathbf{w}\in\varepsilon_E} R_E[n] \right)^+. \tag{11}$$

Consequently, the average WCSR over the entire transmission period can be written as:

$$R_{sec}^{w} = \frac{1}{N}\sum_{n=1}^{N} R_{sec}[n] = \frac{1}{N}\sum_{n=1}^{N} \left(R_D[n] - \max_{\Delta\mathbf{w}\in\varepsilon_E} R_E[n] \right)^+. \tag{12}$$

3 | PROBLEM FORMULATION

To guarantee the secrecy performance of the system, we aim at maximizing the WCSR of system by properly optimizing the transmitter power and trajectory of UAV, as well as the transmit power of S. Defining $\mathbf{Q} = \{\mathbf{q}[n], n \in \mathcal{N}\}$, $\mathbf{P}_S = \{P_S[n], n \in \mathcal{N}\}$, and $\mathbf{P}_U = \{P_U[n], n \in \mathcal{N}\}$, the formulated optimization problem is given by:

P1 :

$$\max_{\{\mathbf{Q},\mathbf{P}_S,\mathbf{P}_U\}} \frac{1}{N}\sum_{n=1}^{N} \left(R_D[n] - \max_{\Delta\mathbf{w}\in\varepsilon_E} R_E[n] \right) \tag{13a}$$

$$s.t.: \quad \|\mathbf{q}[n+1] - \mathbf{q}[n]\|^2 \le L^2, \ n = 0, 1, \ldots, N-1, \tag{13b}$$

$$\|\mathbf{q}[n] - \mathbf{w}_j^{NF}\|^2 \ge r_j^2, \ \forall j, n = 0, 1, \ldots, N-1, \tag{13c}$$

$$\sum_{n=1}^{N} P_S[n] \le N\overline{P}_S, \ 0 \le P_S[n] \le P_S^{max}, n \in \mathcal{N}, \tag{13d}$$

$$\sum_{n=1}^{N} P_U[n] \le \overline{N}P_U, \ 0 \le P_U[n] \le P_U^{max}, n \in \mathcal{N}, \tag{13e}$$

where (13b) and (13c) represent constraints on trajectory of UAV with respect to the speed and NFZs, respectively. The remaining are the power constraints of UAV and S. For instance, (13d) reveals that the total power of S as well as that per each slot, should be both no larger than the give thresholds $N\overline{P}_S$ and P_S^{max}, respectively. Moreover, also note that the operator $(x)^+$ is omitted in the objective function. Intuitively speaking, the objective is to search the maximum of (12), which targets to at least a non-negative value on the secrecy rate per each time slot. Even at some tricky situation that $R_{sec}[n] < 0$, one can directly set $P_S[n] = 0$ to avoid the loss. Hence, the omission of $(x)^+$ will not affect the search of the optimal solution to R_{sec}^{w} [21, 32].

Nevertheless, **P1** is still difficult to solve. The reason lies in three aspects. First, owing to the ergodic rate terms inherited in the objective function, the complicated expectation calculation on the random variables ξ_D and ξ_E are required. Second, there are an infinite number of possible $\mathbf{w}_E$, which makes **P1** difficult to track. Third, the objective function itself is non-convexity.

To make **P1** tractable, we first employ the method proposed in [21] to replace $R_D[n]$ and $R_E[n]$ by their lower and upper bound, respectively. To be specific, by taking advantage of the convexity of $\ln(1 + e^x)$, we have

$$R_D[n] = \frac{1}{\ln 2}\mathbb{E}\left[\ln(1 + X_n)\right] \ge \frac{1}{\ln 2}\ln\left(1 + e^{\mathbb{E}[\ln X_n]}\right), \tag{14}$$

where

$$X_n = \frac{P_S[n]g_{SD}}{P_U[n]h_{UD}[n] + \sigma^2} = \frac{P_S[n]\rho_0 d_{SD}^{-\varphi}}{P_U[n]h_{UD}[n] + \sigma^2}\xi_D = \frac{1}{\lambda_n}\xi_D \tag{15}$$

is the exponential distributed random process with λ_n. Hence,

$$\mathbb{E}[\ln X_n] = \int_0^{\infty} \ln x \lambda_n e^{-\lambda_n x} dx = -\ln\lambda_n - \kappa, \tag{16}$$

where κ is the Euler constant. Substituting (16) into (14), the lower bound of $R_D[n]$ can be expressed as:

$$R_D^{low}[n] \triangleq \log_2\left(1 + \frac{P_S[n]e^{-\kappa}\rho_0 d_{SD}^{-\varphi}}{P_U[n]h_{UD}[n] + \sigma^2}\right). \tag{17}$$

On the other hand, by exploring the inequality $\mathbb{E}[\log(1 + x)] \le \log(1 + \mathbb{E}[x])$ one can also write the upper bound of (8) as:

$$R_E^{up}[n] \triangleq \frac{1}{\ln 2}\ln\left(1 + \frac{P_S[n]\rho_0 d_{SE}^{-\varphi}\mathbb{E}[\xi_E]}{P_U[n]h_{UE}[n] + \sigma^2}\right) = \frac{1}{\ln 2}\ln\left(1 + \frac{P_S[n]\rho_0 d_{SE}^{-\varphi}}{P_U[n]h_{UE}[n] + \sigma^2}\right), \tag{18}$$

Substituting (17) and (18) into the objective function, **P1** can be finally transformed into:

P2 :

$$\max_{\{\mathbf{Q},\mathbf{P}_S,\mathbf{P}_U\}} \sum_{n=1}^{N} \left(R_D^{low}[n] - \max_{\Delta\mathbf{w}\in\varepsilon_E} R_E^{up}[n] \right) \tag{19a}$$

$$s.t.: \quad (13b), (13c), (13d), (13e).$$

4 | THE PROPOSED ITERATIVE ALGORITHM

In this section, we focus on solving **P2**. As aforementioned, though the expectation operations are avoided, **P2** is still

difficult to deal with owing to the non-convexity of objective function as well as the infinite number of $\mathbf{w}_E$ it inherited. To handle the problem, we propose the block coordinate descent (BCD) approach to search the optimal power allocation and trajectory design in an iterative manner. To be specific, we decompose **P2** into three subproblems, where each of $\mathbf{Q}$, $\mathbf{P}_S$, and $\mathbf{P}_U$ is independently solved with the other two counterparts fixed. Then $\mathbf{Q}$, $\mathbf{P}_S$, and $\mathbf{P}_U$ are updated through the iteration among these subproblems. The optimal solution would be gradually approached as the whole algorithm converges.

4.1 | Optimize the UAV trajectory Q given $\mathbf{P}_S$ and $\mathbf{P}_U$

Once $\mathbf{P}_S$ and $\mathbf{P}_U$ are both fixed, **P2** solely depends on the trajectory of UAV $\mathbf{Q}$. However, there are still obstacles, for instance, the non-convexity of the objective function and also the uncertainty of $\Delta\mathbf{w}$. To deal with the former, we propose to employ the successive convex approximation (SCA) technique to obtain the approximated solution iteratively [37]. While dealing with the latter, we convert the original semi-infinite programming problem into a semidefinite programming (SDP) one by applying the $\mathcal{S}$-procedure method [32, 38].

By introducing $\boldsymbol{l} \triangleq [l[1], \dots, l[n]]^\dagger$, $\boldsymbol{m} \triangleq [m[1], \dots, m[n]]^\dagger$ and o as the slack variables, **P2** during the v^{th} iteration can be further expressed as:

SubP1 :%

$$\max_{\mathbf{Q},\boldsymbol{l},\boldsymbol{m},o} \sum_{n=1}^{N} \left[\log_2\left(1 + \frac{P_S[n]e^{-\kappa}\gamma_0 d_{SD}^{-\varphi}}{\frac{P_U[n]\gamma_0}{l[n]} + 1}\right) - \log_2\left(1 + \frac{\gamma_0 P_S[n] o^{-1}}{\frac{P_U[n]\gamma_0}{m[n]} + 1}\right)\right] \tag{20a}$$

$$s.t.: \ (13b), (13c),$$

$$l[n] - \|\mathbf{q}[n] - \mathbf{w}_D\|^2 - H^2 \le 0, \ \forall n, \tag{20b}$$

$$o - \|\mathbf{w}_E - \mathbf{w}_S\|^{\varphi} \le 0, \ \Delta\mathbf{w} \in \varepsilon_E, \tag{20c}$$

$$\|\mathbf{q}[n] - \mathbf{w}_E\|^2 + H^2 - m[n] \le 0, \ \forall n, \Delta\mathbf{w} \in \varepsilon_E, \tag{20d}$$

$$l[n] \ge H^2, \ \forall n, \tag{20e}$$

$$o \ge 0, \tag{20f}$$

where $\gamma_0 = \rho_0/\sigma^2$. It can be observed that there are an infinite number of inequalities in (20c) and (20d) due to the existence of $\Delta\mathbf{w} = (\Delta x_E, \Delta y_E)^\dagger$. As a result, **SubP1** is a semi-infinite programming problem which is difficult to solve. To deal with it, we substitute (1) and (2) into (20c) and (20d) to get

$$\Delta x_E^2 + \Delta y_E^2 \le r_E^2, \tag{21}$$

$$o^{\frac{2}{\varphi}} \le (x_e + \Delta x_E - x_S)^2 + (y_e + \Delta y_E - y_S)^2, \tag{22}$$

$$m[n] \ge (x[n] - x_e - \Delta x_E)^2 + (y[n] - y_e - \Delta y_E)^2 + H^2, \ \forall n. \tag{23}$$

Then the $\mathcal{S}$-procedure method is employed for further processing. To be specific, since there exists a strictly feasible point $(\Delta\hat{x}_E, \Delta\hat{y}_E)^\dagger = (0,0)^\dagger$ guarantees $\Delta\hat{x}_E^2 + \Delta\hat{y}_E^2 - r_E^2 < 0$, the implications (21)⇒(22) and (21)⇒(23) hold if and only if there exist $\theta \ge 0$ and $\chi[n] \ge 0$ such that

$$\Phi_1(o,\theta) = \begin{bmatrix} 1+\theta & 0 & x_e - x_S \\ 0 & 1+\theta & y_e - y_S \\ x_e - x_S & y_e - y_S & \psi_1 - \theta r_E^2 \end{bmatrix} \succeq 0, \tag{24a}$$

$$\Phi_2(x[n], y[n], m[n], \chi[n]) = \begin{bmatrix} \chi[n]-1 & 0 & x[n] - x_e \\ 0 & \chi[n]-1 & y[n] - y_e \\ x[n] - x_e & y[n] - y_e & \psi_2[n] - \chi[n] r_E^2 \end{bmatrix} \succeq 0, \ \forall n, \tag{24b}$$

where

$$\psi_1 = (x_e - x_S)^2 + (y_e - y_S)^2 - o^{\frac{2}{\varphi}}, \tag{25}$$

$$\psi_2[n] = -(x[n] - x_e)^2 - (y[n] - y_e)^2 - H^2 + m[n]. \tag{26}$$

With (24a) and (24b) in hand, **SubP1** can be converted to:

SubP1′ :%

$$\max_{\mathbf{Q},\boldsymbol{l},\boldsymbol{m},o} \sum_{n=1}^{N} \left[\log_2\left(1 + \frac{P_S[n]e^{-\kappa}\gamma_0 d_{SD}^{-\varphi}}{\frac{P_U[n]\gamma_0}{l[n]} + 1}\right) - \log_2\left(1 + \frac{\gamma_0 P_S[n] o^{-1}}{\frac{P_U[n]\gamma_0}{m[n]} + 1}\right)\right] \tag{27a}$$

$$s.t.: \ (13b), (13c),$$

$$l[n] - \|\mathbf{q}[n] - \mathbf{w}_D\|^2 - H^2 \le 0, \ \forall n, \tag{27b}$$

$$\Phi_1(o,\theta) \succeq 0, \tag{27c}$$

$$\Phi_2(x[n], y[n], m[n], \chi[n]) \succeq 0, \ \forall n, \tag{27d}$$

$$l[n] \geq H^2, \quad \forall n, \tag{27e}$$

$$o \geq 0, \tag{27f}$$

$$\theta \geq 0, \tag{27g}$$

$$\chi[n] \geq 0 \ \ \forall n. \tag{27h}$$

Note that the objective function in **SubP1′** is still non-convex due to the non-concavity of the second term with respect to $m[n]$ and o. To bypass this, we replace it with its first-order Taylor expansion at feasible points $m^{(v-1)}[n] = (\|\mathbf{q}^{(v-1)}[n] - \mathbf{w}_e\| + r_E)^2$ and $o^{(v-1)}$, that is:

$$\begin{aligned}
&\log_2\left(1 + \frac{\gamma_0 P_S[n] o^{-1}}{\frac{P_U[n]\gamma_0}{m[n]} + 1}\right) \\
&= \log_2(\gamma_0 P_U[n] o + \gamma_0 P_S[n] m[n] + m[n] o) \\
&\quad - \log_2(m[n] o) - \log_2\left(1 + \frac{\gamma_0 P_U[n]}{m[n]}\right) \\
&\leq \frac{\left(\gamma_0 P_U[n] + m^{(v-1)}[n]\right)(o - o^{(v-1)})}{\ln 2 \cdot C^{(v)}[n]} + \log_2(C^{(v)}[n]) \\
&\quad + \frac{\left(\gamma_0 P_S[n] + o^{(v-1)}\right)(m[n] - m^{(v-1)}[n])}{\ln 2 \cdot C^{(v)}[n]} \\
&\quad + \frac{\gamma_0 P_U[n](m[n] - m^{(v-1)}[n])}{\ln 2 \cdot (\gamma_0 P_U[n] m^{(v-1)}[n] + m^{(v-1)}[n]^2)} \\
&\quad - \log_2\left(1 + \frac{\gamma_0 P_U[n]}{m^{(v-1)}[n]}\right) - \log_2(m[n] o) \\
&\triangleq F^{(v)}[n],
\end{aligned} \tag{28}$$

where

$$\begin{aligned}
C^{(v)}[n] =& \gamma_0 P_U[n] o^{(v-1)} \\
&+ \gamma_0 P_S[n] m^{(v-1)}[n] + m^{(v-1)}[n] o^{(v-1)}.
\end{aligned} \tag{29}$$

We then focus on the properties of constraints listed in **SubP1′**. As for (13c), $\|\mathbf{q}[n] - \mathbf{w}_j^{NF}\|^2$ is convex with respect to $\mathbf{q}[n]$. Thus, its global over-estimator with respect to $\mathbf{q}^{(v-1)}[n]$ in previous iteration can be written as follows:

$$\begin{aligned}
\|\mathbf{q}[n] - \mathbf{w}_j^{NF}\|^2 \geq& \|\mathbf{q}[n]^{(v-1)} - \mathbf{w}_j^{NF}\|^2 \\
&+ 2(\mathbf{q}[n]^{(v-1)} - \mathbf{w}_j^{NF})^\dagger \times (\mathbf{q}[n] - \mathbf{q}[n]^{(v-1)}) \\
&\triangleq D_j^{(v)}[n], \quad \forall n, j.
\end{aligned} \tag{30}$$

Following the similar approach, we can also obtain the lower bound of $\|\mathbf{q}[n] - \mathbf{w}_D\|^2$ with respect to $\mathbf{q}^{(v-1)}[n]$ in (27b) as:

$$\begin{aligned}
\|\mathbf{q}[n] - \mathbf{w}_D\|^2 \geq& \|\mathbf{q}[n]^{(v-1)} - \mathbf{w}_D\|^2 \\
&+ 2(\mathbf{q}[n]^{(v-1)} - \mathbf{w}_D)^\dagger \times (\mathbf{q}[n] - \mathbf{q}[n]^{(v-1)}) \\
&\triangleq D_E^{(v)}[n], \quad \forall n.
\end{aligned} \tag{31}$$

We then focus on constraint (27d), which is non-convex due to the non-linearity of $o^{\frac{2}{\varphi}}$ and $x^2[n]$, $y^2[n]$ in ψ_1 and $\psi_2[n]$. To overcome this, we again utilize the corresponding first-order Taylor expansion at point $o^{(v-1)}$ and $\mathbf{q}[n]^{(v-1)} = (x^{(v-1)}[n], y^{(v-1)}[n])^\dagger$ to obtain the convex constraints as follows:

$$o^{\frac{2}{\varphi}} \geq (o^{(v-1)})^{\frac{2}{\varphi}} + \frac{2}{\varphi}(o^{(v-1)})^{\frac{2}{\varphi}-1}(o - o^{(v-1)}), \tag{32a}$$

$$\begin{aligned}
x^2[n] \geq& (x^{(v-1)}[n])^2 \\
&+ 2x^{(v-1)}[n](x[n] - x^{(v-1)}[n]),
\end{aligned} \tag{32b}$$

$$\begin{aligned}
y^2[n] \geq& (y^{(v-1)}[n])^2 \\
&+ 2y^{(v-1)}[n](y[n] - y^{(v-1)}[n]).
\end{aligned} \tag{32c}$$

Then ψ_1 and $\psi_2[n]$ can be transformed to:

$$\begin{aligned}
\widetilde{\psi}_1 =& (x_e - x_S)^2 + (y_e - y_S)^2 - (o^{(v-1)})^{\frac{2}{\varphi}} \\
&- \frac{2}{\varphi}(o^{(v-1)})^{\frac{2}{\varphi}-1}(o - o^{(v-1)}),
\end{aligned} \tag{33a}$$

$$\begin{aligned}
\widetilde{\psi}_2[n] =& \left(x^{(v-1)}[n]\right)^2 - x_e^2 + 2x[n]\left(x_e - x^{(v-1)}[n]\right) \\
&+ \left(y^{(v-1)}[n]\right)^2 - y_e^2 + 2y[n]\left(y_e - y^{(v-1)}[n]\right) \\
&- H^2 + m[n].
\end{aligned} \tag{33b}$$

By replacing (13c) and (27b) with their corresponding over estimators derived in (30) and (31), and also substituting (28) and (33) into **SubP1′**, the problem can be further approximated as:

SubP1″ :

$$\max_{\mathbf{Q}, l, m, o} \ \sum_{n=1}^{N}\left[\log_2\left(1 + \frac{P_S[n] e^{-\kappa}\gamma_0 d_{SD}^{-\varphi}}{\frac{P_U[n]\gamma_0}{l[n]} + 1}\right) - F^{(v)}[n]\right]$$

$$s.t. : \quad (13b), (27e), (27f), (27g), (27h)$$

$$l[n] - H^2 \leq D_E^{(v)}[n], \quad \forall n, \tag{34a}$$

$$r_j^2 \le D_j^{(v)}[n], \quad \forall n, j, \tag{34b}$$

$$\widetilde{\Phi}_1(\theta, o) \succeq 0, \tag{34c}$$

$$\widetilde{\Phi}_2(x[n], y[n], m[n], \chi[n]) \succeq 0, \quad \forall n, \tag{34d}$$

where

$$\widetilde{\Phi}_1(o, \theta) = \begin{bmatrix} 1+\theta & 0 & x_e - x_S \\ 0 & 1+\theta & y_e - y_S \\ x_e - x_S & y_e - y_S & \widetilde{\psi}_1 - \theta r_E^2 \end{bmatrix}, \tag{35a}$$

$$\widetilde{\Phi}_2(x[n], y[n], m[n], \chi[n]) = \begin{bmatrix} \chi[n]-1 & 0 & x[n]-x_e \\ 0 & \chi[n]-1 & y[n]-y_e \\ x[n]-x_e & y[n]-y_e & \widetilde{\psi}_2[n] - \chi[n] r_E^2 \end{bmatrix}. \tag{35b}$$

Now the obfjective function is concave with the feasible region been convex. As a result, the converted problem can be easily solved through standard convex optimization method, utilizing the solver such as CVX [39].

4.2 | Subproblem 2: Optimize the transmit power of source $\mathbf{P}_S$ given $\mathbf{P}_U$ and $\mathbf{Q}$

We then focus on the second subproblem of searching for the optimal $\mathbf{P}_S$ with both $\mathbf{Q}$ and $\mathbf{P}_U$ in hand, which can be expressed as:

SubP2 :

$$\max_{\mathbf{P}_S} \quad \sum_{n=1}^{N} \left[\log_2(1+\alpha_n P_S[n]) - \log_2(1+\beta_n P_S[n])\right]$$

$$s.t. : \quad (13d)$$

where

$$\alpha_n = \frac{e^{-\kappa}\rho_0 d_{SD}^{-\varphi}}{P_U[n] h_{UD}[n] + \sigma^2}, \tag{36a}$$

$$\beta_n = \max_{\Delta \mathbf{w} \in \varepsilon_E} \frac{\gamma_0 / d_{SE}^{\varphi}}{\frac{\gamma_0 P_U[n]}{\|\mathbf{q}[n] - \mathbf{w}_E\|^2 + H^2}} + 1. \tag{36b}$$

Apparently, α_n is now a constant as $\mathbf{P}_U$ and $\mathbf{Q}$ are both determined. However, it is still difficult to determine β_n due to the existence of $\Delta\mathbf{w}$. To deal with the infinite error set, we again consider the worst case when the wiretapping capacity reaches maximum. In such a scenario, the eavesdropper E is located nearest to the source node S. Assuming that the distance between $\mathbf{w}_S$ and $\mathbf{w}_e$ is lager than r_E, the coordinate of eavesdropper $\mathbf{w}_E = (x_E, y_E)^\dagger$ can be written as:

$$x_E = x_e + r_E \frac{x_S - x_E}{\|\mathbf{w}_S - \mathbf{w}_e\|}, \tag{37a}$$

$$y_E = y_e + r_E \frac{y_S - y_E}{\|\mathbf{w}_S - \mathbf{w}_e\|}. \tag{37b}$$

Consequently, β_n can be further expressed as:

$$\beta_n = \frac{\gamma_0 / (\|\mathbf{w}_e - \mathbf{w}_S\| - r_E)^{\varphi}}{\frac{\gamma_0 P_U[n]}{\|\mathbf{q}[n] - \mathbf{w}_E\|^2 + H^2}} + 1. \tag{38}$$

By substituting (38) into the objective function, **SubP2** can now be solved through the Lagrangian maximization approach [35, 38], where the corresponding Lagrangian function can be written as:

$$\mathcal{L}(\mathbf{P}_S, \lambda) = \sum_{n=1}^{N} \left[\log_2(1+\alpha_n P_S[n]) - \log_2(1+\beta_n P_S[n])\right] + \lambda\left(\sum_{n=1}^{N} P_S[n] - N\overline{P}_S\right), \tag{39}$$

By solving $\frac{\partial \mathcal{L}(\mathbf{P}_S, \lambda)}{\partial P_S[n]} = 0$ and $\frac{\partial \mathcal{L}(\mathbf{P}_S, \lambda)}{\partial \lambda} = 0$, the optimal solution can be obtained as:

$$P_S^*[n] = \begin{cases} \min\left(\left[\hat{P}_S[n]\right]^+, P_S^{max}\right) & \alpha_n > \beta_n, \\ 0 & \alpha_n < \beta_n, \end{cases} \tag{40}$$

where

$$\hat{P}_S[n] = \sqrt{\left(\frac{1}{2\beta_n} - \frac{1}{2\alpha_n}\right)^2 + \frac{1}{\lambda \ln 2}\left(\frac{1}{\beta_n} - \frac{1}{\alpha_n}\right)} - \frac{1}{2\beta_n} - \frac{1}{2\alpha_n}, \tag{41}$$

λ is a non-negative multiplier that associated with (13d), which can be founded by bisection search. The detailed procedure is concluded in Algorithm 1.

ALGORITHM 1 Bisection search of λ

1: Given the upper bound λ_{up} and the lower bound $\lambda_{low} = 0$ of multiplier, iteration number $i = 1$ and the threshold ζ.
2: **repeat**
3: Set $\lambda^i = (\lambda_{up} + \lambda_{low})/2$.
4: Compute $\hat{P}_S[n]$ according (40)(41). If $\sum_{n=1}^{N} P_S[n] > N\overline{P}_S$ then $\lambda_{low} = \lambda^i$, else $\lambda_{up} = \lambda^i$.
5: **until** $\lambda_{up} - \lambda_{low} < \zeta$

4.3 | Subproblem 3: Optimize The Jamming Power of UAV $\mathbf{P}_U$ Given $\mathbf{P}_S$ and $\mathbf{Q}$

We then focus on the optimization of $\mathbf{P}_U$ with fixed $\mathbf{P}_S$ and $\mathbf{Q}$, leaving (13e) the only constraint. Similar to the strategy applied in former subproblem, we adopt the worst case assumption to bypass $\Delta\mathbf{w}$ in the objective function, except that now we pay attention to the relative distance between the UAV jammer and eavesdropper. In the worst case, the eavesdropper would be located farthest from the UAV jammer. Hence, $\mathbf{w}_E[n] = (x_E[n], y_E[n])^\dagger$ can be calculated as:

$$x_E[n] = x_e + r_E \frac{x_e - x[n]}{\|\mathbf{q}[n] - \mathbf{w}_e\|}, \tag{42a}$$

$$y_E[n] = y_e + r_E \frac{y_e - y[n]}{\|\mathbf{q}[n] - \mathbf{w}_e\|}. \tag{42b}$$

Thus, by substituting (42) into the objective function of **P2**, **SubP3** can be formulated as:

SubP3 :

$$\max_{\mathbf{P}_U} \sum_{n=1}^{N} \left[\log_2\left(1 + \frac{a_n}{1 + b_n P_U[n]}\right) - \log_2\left(1 + \frac{c_n}{1 + d_n P_U[n]}\right)\right]$$

$$s.t.: \quad (13e),$$

where $a_n = P_S[n] e^{-\kappa} \gamma_0 d_{SD}^{-\varphi}$, $b_n = \frac{\gamma_0}{\|\mathbf{q}[n] - \mathbf{w}_D\|^2 + H^2}$, $c_n = \frac{P_S[n]\gamma_0}{\|\mathbf{w}_S - \mathbf{w}_E[n]\|^\varphi}$ and $d_n = \frac{\gamma_0}{(\|\mathbf{q}[n] - \mathbf{w}_e\| + r_E)^2 + H^2}$ are all constant since $\mathbf{P}_S$ and $\mathbf{Q}$ are both determined. Then by applying the Lagrangian dual method, the corresponding Lagrangian function with respect to **SubP3** can be written as:

$$\begin{aligned}\mathcal{L}(\mathbf{P}_U, \mu) = \mu\left(\sum_{n=1}^{N} P_U[n] - N\overline{P}_U\right) \\ + \sum_{n=1}^{N}\left[\log_2\left(1 + \frac{a_n}{1 + b_n P_U[n]}\right)\right. \\ \left. - \log_2\left(1 + \frac{c_n}{1 + d_n P_U[n]}\right)\right],\end{aligned} \tag{43}$$

where $\mu \geq 0$ is the Lagrange multiplier variable related to the constraint (13e). Note that (43) holds when N is sufficiently large [21]. With such assumption the duality gap between the primal and dual problem is negligible, according to the time-sharing condition [36]. Then the optimal solution can be found by solving the following equation:

$$\begin{aligned}\frac{\partial \mathcal{L}(\mathbf{P}_U, \mu)}{\partial P_U[n]} = & \mathcal{A}_n P_U^4[n] + B_n P_U^3[n] + C_n P_U[n]^2 \\ & + D_n P_U[n] + E_n = 0,\end{aligned} \tag{44}$$

ALGORITHM 2 BCD-Based Iterative Algorithm for Solving **P2**

1: Given the initial point: the power variables $\mathbf{P}_S^{(0)}$, $\mathbf{P}_U^{(0)}$, and the UAV's trajectory $\mathbf{Q}^{(0)}$. Initialize the iterative number $v = 0$ and set the threshold η.
2: **repeat**
3: Set $v = v + 1$.
4: Knowing the $\mathbf{P}_S^{(v-1)}$ and $\mathbf{P}_U^{(v-1)}$, and update the Taylor expansion point $m^{(v-1)}[n]$ and $\delta^{(v-1)}$ according to $\mathbf{Q}^{(v-1)}$. Then solve (34) we can obtain $\mathbf{Q}^{(v)}$.
5: Set the $\mathbf{P}_U^{(v-1)}$, $\mathbf{Q}^{(v)}$ as the given point. Solve **SubP2** then we can get $\mathbf{P}_S^{(v)}$.
6: Set the $\mathbf{P}_S^{(v)}$, $\mathbf{Q}^{(v)}$ as the given point. Solve **SubP3** then we can get $\mathbf{P}_U^{(v)}$.
7: **until** The improvement of the WCSR is smaller than η

where

$$\begin{aligned}\mathcal{A}_n &= \mu b_n^2 d_n^2, \\ B_n &= \mu b_n^2 d_n (c_n + 2) + \mu d_n^2 b_n (a_n + 2), \\ C_n &= \mu b_n^2 (c_n + 1) + \mu b_n d_n (a_n + 2)(c_n + 2) \\ &\quad + \mu d_n^2 (a_n + 1) + b_n d_n (a_n d_n - c_n b_n), \\ D_n &= \mu b_n (a_n + 2)(c_n + 1) + \mu d_n (c_n + 2)(a_n + 1) \\ &\quad + 2 b_n d_n (a_n - c_n), \\ E_n &= \mu (a_n + 1)(c_n + 1) + a_n b_n (c_n + 1) \\ &\quad - c_n d_n (a_n + 1).\end{aligned}$$

According to the complementary slackness of KKT condition [38], the constraint (13e) is inactive when $\mu = 0$. Consequently, the optimal solution is the Fermat point within the feasible region, which can be obtained by solving the following equation:

$$\begin{aligned}b_n d_n (a_n d_n - b_n c_n) P_U^2[n] + 2 b_n d_n (a_n - c_n) P_U[n] \\ + a_n b_n (c_n + 1) - c_n d_n (a_n + 1) = 0.\end{aligned} \tag{45}$$

Otherwise, when $\mu > 0$, the maximum value is achieved on the boundary of the feasible region, which can be found by bisection search.

Thus, the optimal solution of **SubP3** is:

$$P_U^*[n] = \min\left(\left[\hat{P}_U[n]\right]^+, P_U^{max}\right), \tag{46}$$

where $\hat{P}_U[n]$ is the non-negative real solution from (44) or (45), depending on which achieves the maximum value.

The above-mentioned three subproblems would be solved iteratively until converges. The detailed procedure of such a BCD based approach is concluded in Algorithm 2. Note that as working in an iterative manner, the complexity of the

TABLE 1 Simulation Parameters

Parameters	Description	Value
$\mathbf{w}_S$	The horizontal coordinate of S	$(0,0)^\dagger$
$\mathbf{w}_D$	The horizontal coordinate of D	$(300,0)^\dagger$
$\mathbf{w}_E$	The actual coordinate of E	$(190,210)^\dagger$
$\mathbf{w}_e$	The estimated circle center of E	$(200,200)^\dagger$
r_E	The estimated circle radius of E	20, 30, 40
$\mathbf{q}_0$	The initial horizontal coordinates of UAV	$(-100,100)^\dagger$
$\mathbf{q}_F$	The final horizontal coordinates of UAV	$(500,100)^\dagger$
V	The speed of UAV	10 m/s
δ	The time slot	0.5 s
$\gamma_0 = \rho_0/\sigma^2$	The ratio between the channel gain and noise power	80 dB
φ	The path loss exponent	3

proposed algorithm relies on that of solving the three subproblems it contains. Recall that N and J denotes the number of time slots and NFZs, respectively. The complexity of solving **SubP1** is $\mathcal{O}[N^{3.5}J^{1.5}]$ due to the interior point method employed [12]. As for **SubP2** and **SubP3**, both solutions can be obtained in an analytical way hence the complexity of these two subproblems is linear per time slot. Let K_1 and K_2 denotes the bisection search times of **SubP2** and **SubP3**, respectively. The total complexity of solving **SubP2** and **SubP3** writes $\mathcal{O}[(K_1+K_2)N]$. Finally, let K denotes the number of iterations for Algorithm 2 to converge, the total computational complexity of the proposed algorithm is on the order of $\mathcal{O}[K((K_1+K_2)N+N^{3.5}J^{1.5})]$.

5 | SIMULATION RESULTS

In this section, we carry out simulations to validate the effectiveness of the proposed algorithm. The simulation parameters are concluded in Table 1 unless otherwise noted. The times for Monte Carlo simulation is set to be 10^5 when calculate the secrecy rate. Denoting the proposed algorithm as **TP**, we compare it with the following benchmark schemes:

- **Scheme-PNT:** In the scheme, only the transmit power of source and UAV are optimized by alternatively solving **SubP2** and **SubP3**. While the trajectory of UAV is planned independently, with the objective of being closest to the eavesdropper under the maximum speed constraint, that is:

$$\min_{\mathbf{Q}} \sum_{n=1}^{N} \|\mathbf{q}[n]-\mathbf{w}_e\|$$
$$s.t.: \quad (3)$$

- **Scheme-TNP**: The trajectory of UAV is solely optimized without considering the power allocation of source and UAV. In such a case, the transmit power of S and UAV in each slot n is set as their corresponding average power.

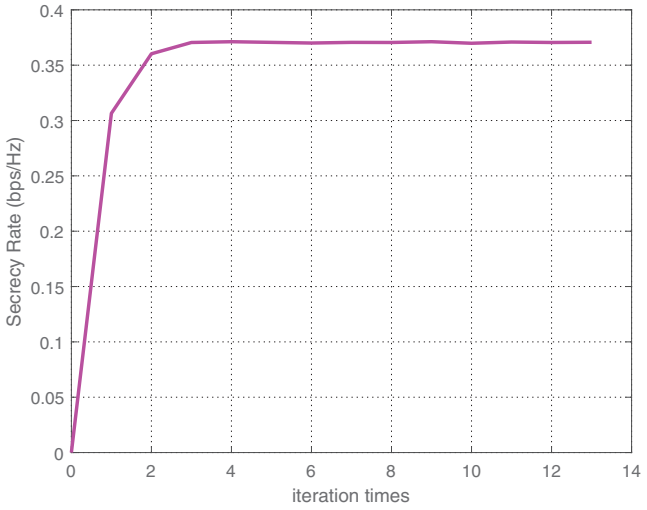

FIGURE 2 Convergence behavior of proposed scheme **TP** ($\overline{P}_S = 30$dBm, $\overline{P}_U = 10$ dBm, $r_E = 20$ m and $T = 80$ s).

- **Scheme-TP-E**: we consider the algorithm proposed in [21] as the benchmark scheme who optimize both the transmit power of S and UAV, as well as the trajectory of UAV. However, the perfect location information of the eavesdropper is available when performing the joint optimization.

To evaluate the efficiency of the proposed algorithm, we first numerically demonstrate its convergence behavior in Figure 2. The transmit power of the source node and UAV are set as $\overline{P}_S = 30$ dBm and $\overline{P}_U = 10$ dBm, respectively, $r_E = 20$m and $T = 80$s. It can be observed that the secrecy rate increases dramatically during the first several iterations, which reveals the effectiveness of the proposed algorithm. Moreover, the algorithm can converge with only 4 iterations, which shows the efficiency of the proposed algorithm.

Then we evaluate the performance of the proposed scheme in the case when NFZ is absent. Figure 3 illustrates the achievable secrecy rate of various schemes versus the allowed flight period T. The transmit power of S and the UAV is $P_S^{\max} = 4\overline{P}_S = 36$ dBm and $P_U^{\max} = 4\overline{P}_U = 16$ dBm, respectively. Note that the different location estimation errors of eavesdropper with $r_E = \{20, 30, 40\}$ m, are also considered here. It can be observed that the secrecy rate of all schemes increases when T gets larger. It is reasonable since the UAV would have a greater chance to fly close to the eavesdropper, and even hover there for a certain duration once T is sufficiently large. On the other hand, the performance of all schemes get worse when encountering larger estimation error. However, it is found that the proposed scheme always outperforms the other candidates, even when it experiences larger estimation error than the others. For instance, the performance of **TP** with $r_E = 40$ m is even better than other candidates with $r_E = 20$ m. In addition, the performance of the proposed scheme with $r_E = 20$ m is close to that of **TP-E**. While the latter is treated as the ideal benchmark one since there is no estimation error involved. To get a better insight of the superior performance of the proposed

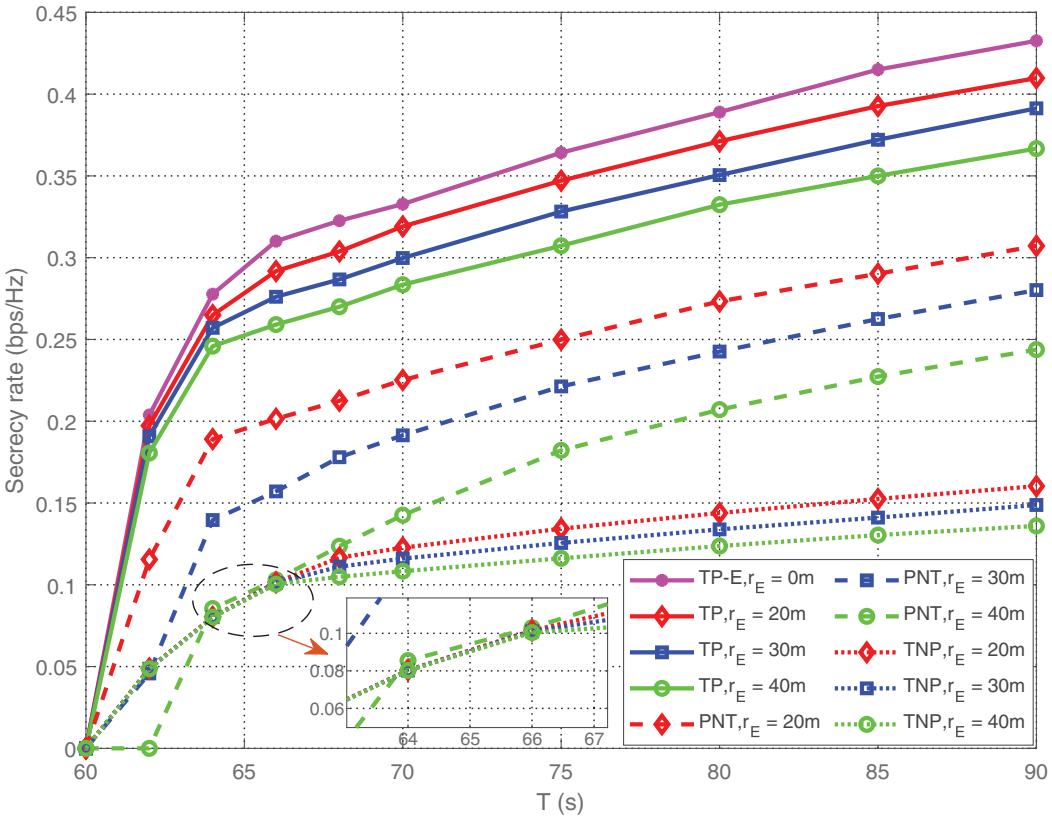

FIGURE 3 Average secrecy rate versus T and r_E

scheme, we further illustrate the trajectory it obtained in Figure 4, together with those from the other benchmark schemes. The corresponding flight speed of UAV per time slot is shown in Figure 5 for better understanding. It can be observed that when the flight time T is relatively short, the trajectories given by all schemes are mainly constrained by the maximum flight speed, and hence tend to choose the shortest path from the initial point to the final point. In the most stringent situation, that is, $T = 60$ s, the trajectories given by all schemes become a straight line between the initial and final point. While as T increases, for instance, when $T = 62$ s, there is more time for UAV to stay in air so that all schemes try to force UAV to fly close to the eavesdropper with maximum speed to get a better jamming effect. When the flight time is sufficient large, that is, $T = 80$ s, there is chance for UAV to fly by the eavesdropper. In such a case, the proposed scheme **TP** would force the UAV to first fly in an arc path to a certain point around $\mathbf{w}_e$, that is, the 'guessed' location of eavesdropper, at its maximum speed. Then it hovers there as long as possible. Finally, it flies away at its maximum speed to reach at the destination on time in an arc path. It reveals that the proposed scheme strikes an optimal balance between the jamming effect to the eavesdropper and the interference to the receiver D. Note that the scheme **TP-E** provides a similar trajectory to that of the proposed scheme except for a closer hover point to the actual location of eavesdropper, due to the more precise location information. While scheme **TNP** gives an outermost trajectory for UAV. Since only average power allocation can be adopted, it has to keep far away from D to guarantee the minimum overhearing rate. For scheme **PNT**, as aforementioned, the trajectory is fixed to be the shortest path. Hence, the UAV first flies directly to $\mathbf{w}_e$ at maximum speed. Then it will hover there for a while and finally move to the final point at the maximum speed along a straight line.

We then focus on the resulted power allocation with respect to the proposed algorithm, where the curves of P_S and P_U per time slot are given in Figures 6 and 7, respectively. We can observe that both P_S and P_U are impacted by the trajectory of UAV, that is, the per time slot changes on the relative distance of the links between UAV-S, UAV-E, and UAV-D. The only exception is **TNP** scheme who has no way to adjust the transmit power. To be specific, at the very beginning stage the UAV is too far away from the eavesdropper. The SINR of legitimate link is worse than the illegitimate one even if the source transmitted with the maximum power. In such a case, the best choice for the source node is to keep silence without sending the confidential information. On the other hand, the UAV also keeps silence when it is far away from the eavesdropper but too close to the source. Once the UAV flies closer to the eavesdropper and may have positive impacts on jamming the wiretapping channel, both P_S and P_U raises dramatically to improve the secrecy rate and would remain stable for a while when UAV reaches the hover point. After that, P_S gradually descend to 0 and the UAV turns off its jamming power during its flight towards the final point.

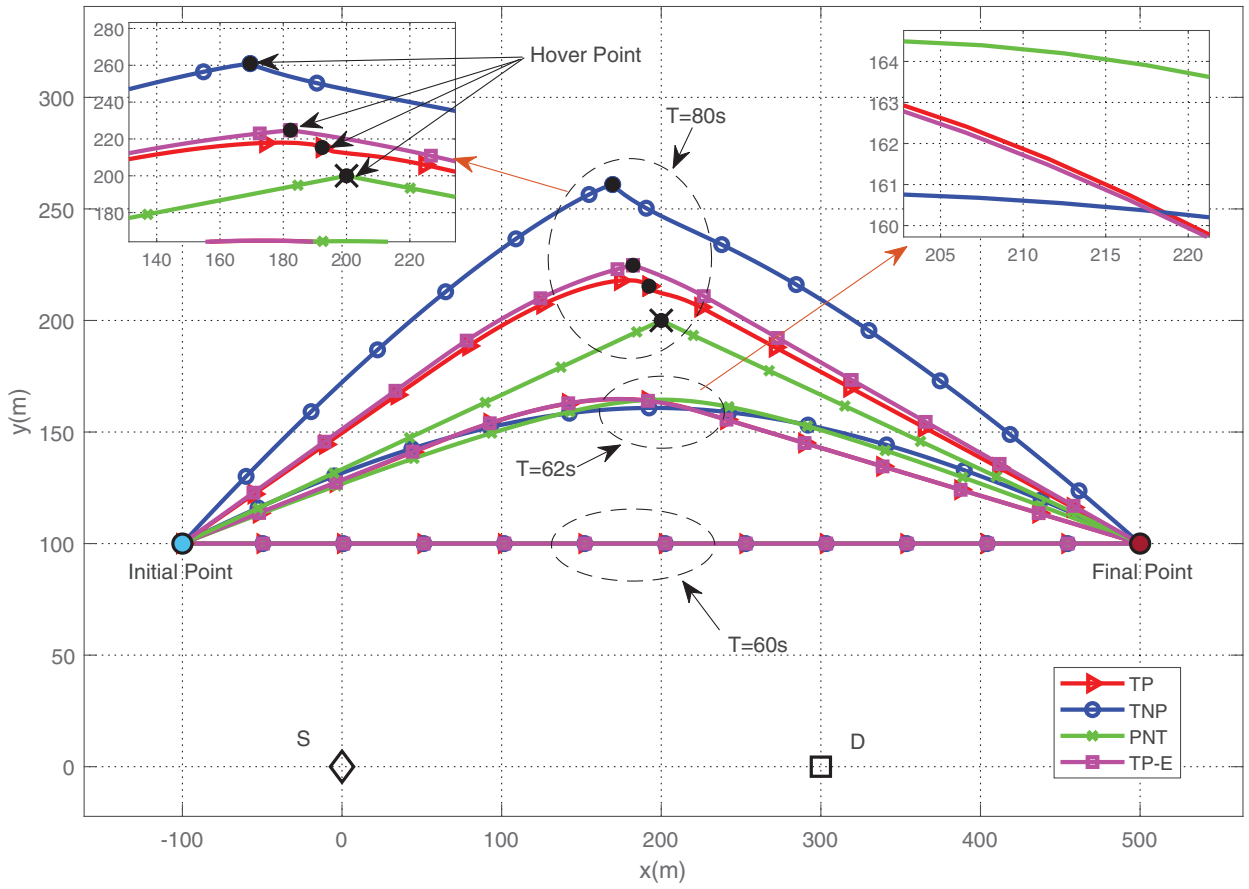

FIGURE 4 UAV trajectory comparisons of the proposed algorithm and the benchmark algorithms per time slot with different flight period T. $\overline{P}_S = 30$ dBm, $\overline{P}_U = 10$ dBm and $r_E = 20$ m

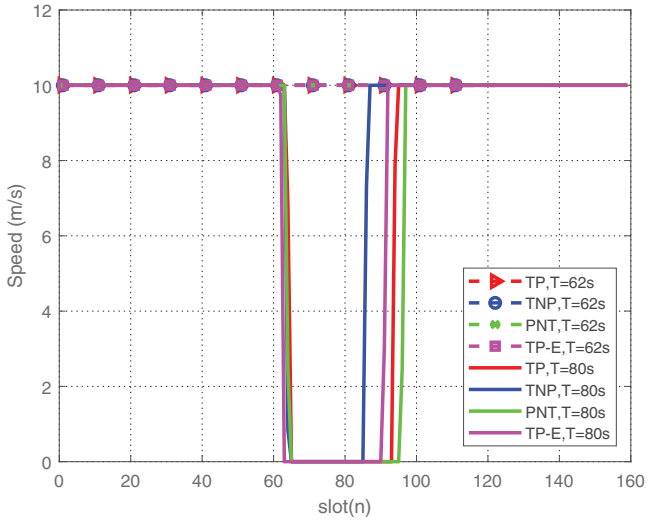

FIGURE 5 UAV flight speed comparisons of the proposed algorithm and the benchmark algorithms with different flight period T. $\overline{P}_S = 30$ dBm, $\overline{P}_U = 10$ dBm and $r_E = 20$ m

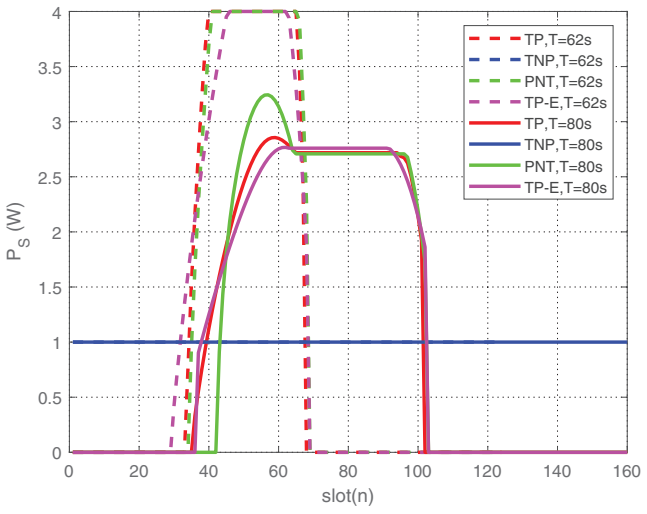

FIGURE 6 The transmit power of source node per time slot

To further demonstrate the impacts of joint trajectory design and power optimization on the performance of the system, Figures 8 and 9 provide the achievable secrecy rate per time slot from various schemes with $T = 62$ s and $T = 80$ s, respectively. It can be observed that in both scenarios, the achievable rate of all schemes first increases along with time and then gradually decreases. Such variation conveys with the dynamics of the UAV trajectory as well as P_U and P_S reported in previous simulations. Note that the secrecy rate of **TNP** turns

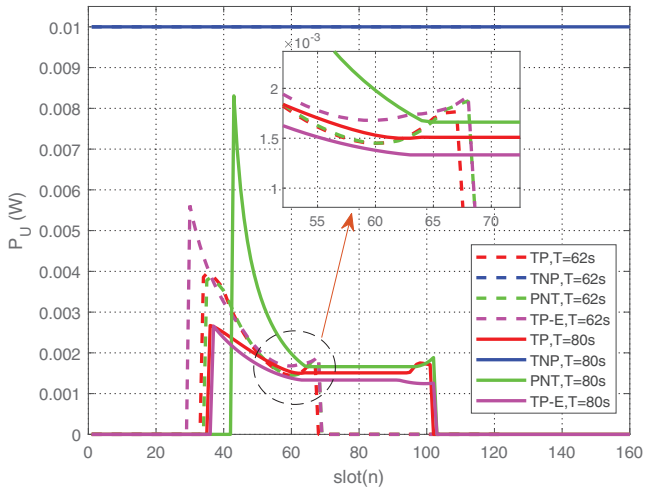

FIGURE 7 The transmit power of UAV per time slot

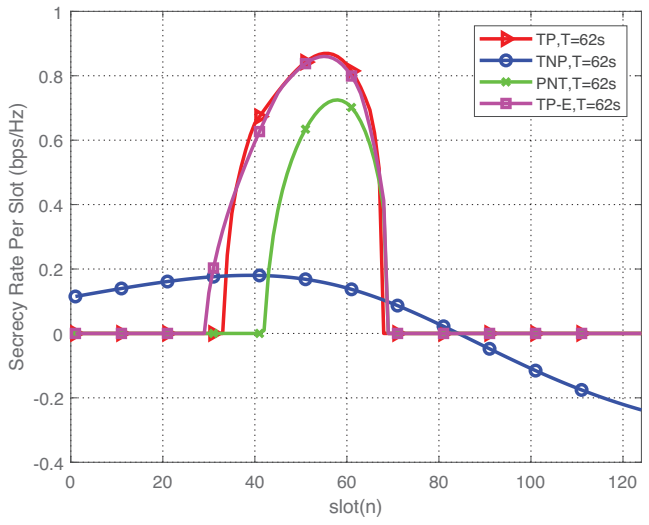

FIGURE 8 The achievable secrecy rate per time slot with $T = 62$ s

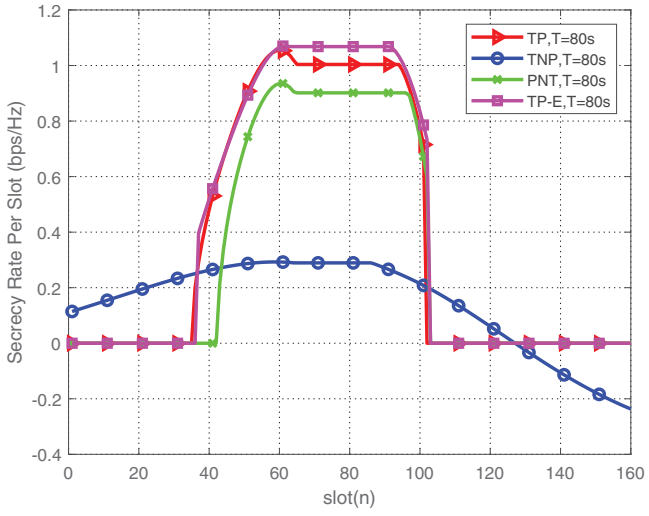

FIGURE 9 The achievable secrecy rate per time slot with $T = 80$ s

out to be negative during the final phase of flight since both P_U and P_S are set as their corresponding average power, which results in inevitable information leakage.

We then evaluate the effectiveness of the proposed scheme when encountering the NFZs. To do so we add a number of 4 NFZs to the coverage area, where NFZ-1 is co-located with $\mathbf{w}_e$ at $(200, 200)^\dagger$ with radius $r_1 = 15$ m. The remaining three NFZs, namely, NFZ-2, NFZ-3, and NFZ-4, are centered at $(0, 150)^\dagger$, $(300, 170)^\dagger$ and $(150, 150)^\dagger$ with radius $r_2 = 10$ m, $r_3 = 20$ m and $r_4 = 20$ m, respectively. The height of all NFZs $H = 100$ m and the flight time is set to be $T = 80$ s. The resulted trajectory when taken these NFZs into consideration is shown in Figure 10. To compare, we also illustrate the optimal trajectory when the NFZs are absent. It can be found that the UAV can bypass the NFZ successfully with the proposed scheme, which confirms its effectiveness. In addition, the trajectory is close to the optimal one, indicating that the proposed scheme tends to minimize the negative impact of the NFZ and approach the optimal solution.

Such inference can be further verified in Figure 11, where the achievable secrecy rates with various NFZ setups are illustrated. To be specific, besides the one with all 4 NFZs as illustrated in Figure 10, we also consider three other cases. They are the case with NFZ-4 only, the one with NFZ-1 only, as well as the one with both NFZ-2 and NFZ-3. Note that different cases would lead to different trajectories of UAV. The ideal case without NFZ is also included as the benchmark. It can be observed that not only the size and number of NFZs, but also their placement impacts the performance. For instance, the existence of NFZ-4 does not adversely affect performance as it stands outside the optimal trajectory of UAV. Their performance is therefore identical. While comparing the case with NFZ-1 and that have both NFZ-2 and NFZ-3, we can find that even the former owns fewer NFZs with smaller size, the performance is worse than the latter. That is mainly due to the placement of NFZ-1, which just stands around the eavesdropper. The UAV can only hover outside NFZ-1, leaving a longer distance to the eavesdropper compared to the latter case. The jamming effect is therefore effected. It should be noted that the one with all 4 NFZs performs similar to, and even slightly better than that with NFZ-1 only at some T. It is intuitively due to the fact that the trajectory of UAV is planned according to the 'guessed' location of eavesdropper. Though more NFZs exists, a better trajectory may be accidentally found when bypassing these NFZs, which provides chance to the UAV to fly closer to the actual location of eavesdropper.

6 | CONCLUSION

In this paper, we have studied the UAV assisted secure communication system in the presence of NFZs and imperfect estimation on the location of the eavesdropper. The secrecy rate maximization problem was formulated to jointly design the trajectory of UAV and adjust the transmit power of BS and UAV. To solve the problem, we first adopted WCSR to bypass the

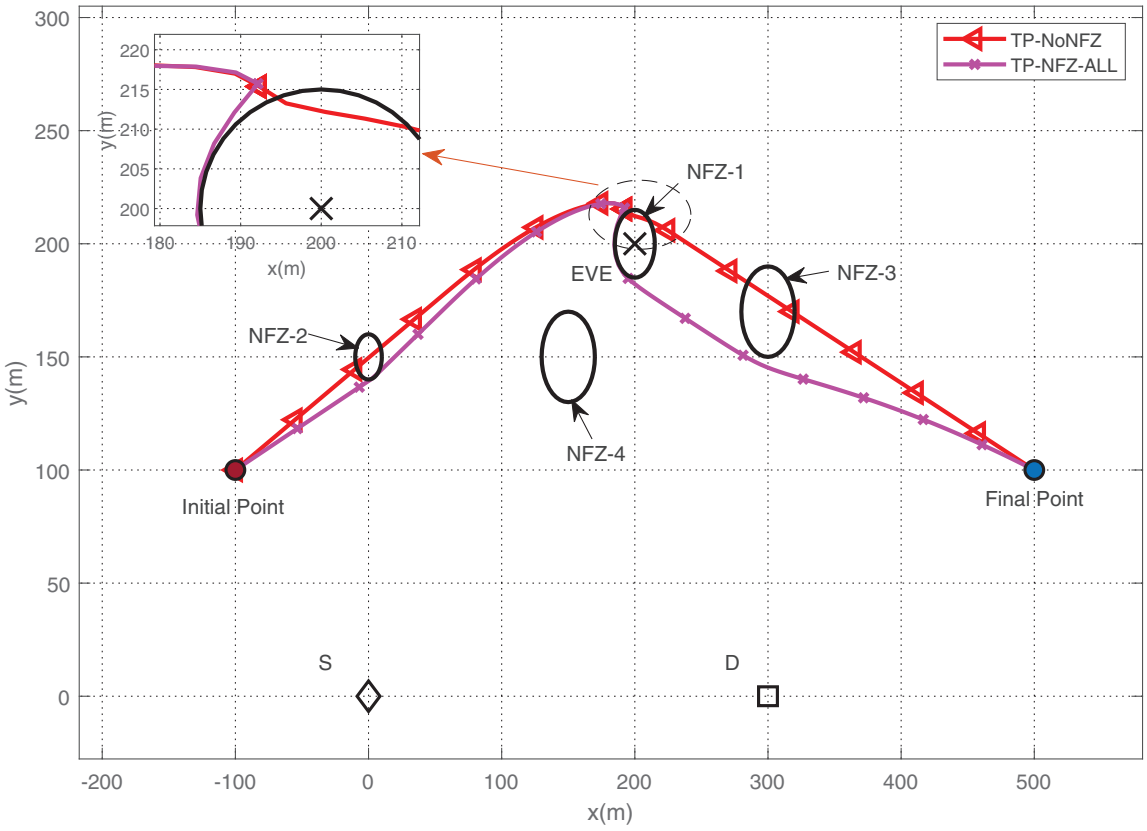

FIGURE 10 The impact of NFZs on UAV trajectory when $T = 80$ s

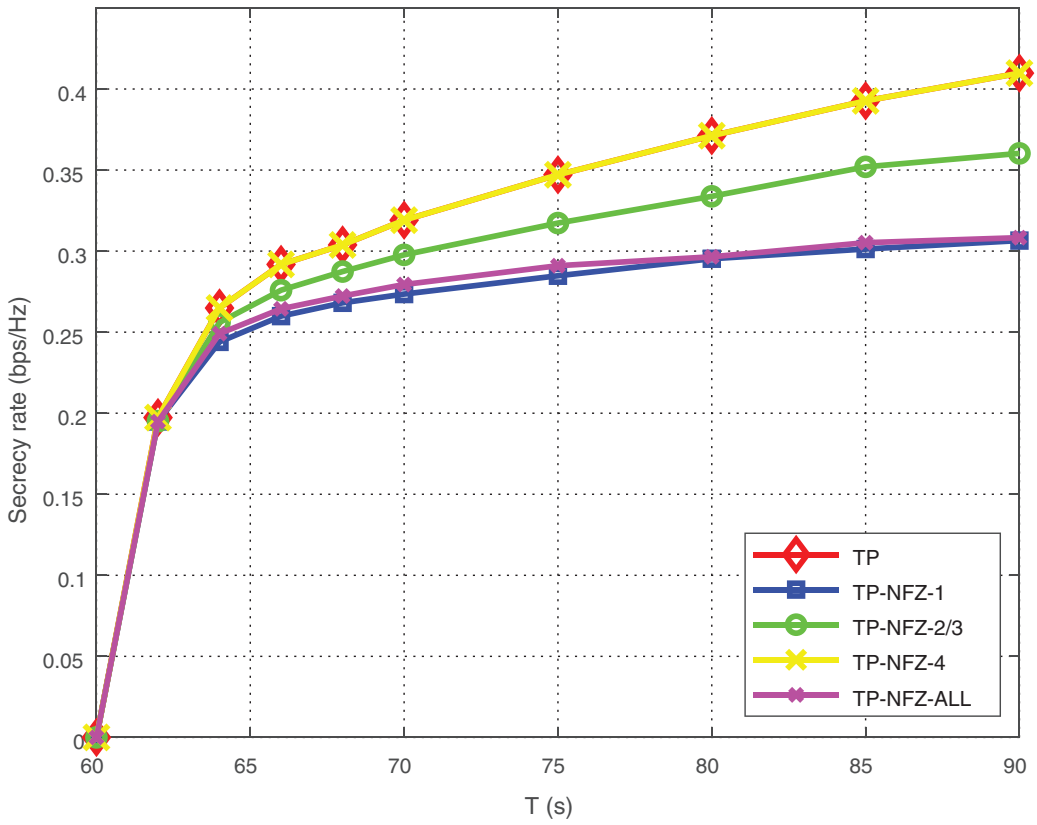

FIGURE 11 The secrecy rate comparison when UAV encounter with different NFZs

infinite set brought by the estimation error. A BCD based algorithm was then proposed to find the suboptimal solution iteratively. Simulation results confirmed the effectiveness of the proposed algorithm in the presence of NFZs and demonstrated its superior performance compared with other benchmark schemes. It also verified that the proposed algorithm is robust to the estimation error, with tolerable performance loss compared with that with perfect location information.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None

DATA AVAILABILITY STATEMENT

Research data are not shared.

ORCID

Xiaotian Zhou https://orcid.org/0000-0002-3237-5347

REFERENCES

1. Driessen, B., Hund, R., Willems, C., Paar, C., Holz, T.: Don't trust satellite phones: a security analysis of two satphone standards. In: 2012 IEEE Symposium on Security and Privacy, pp. 128–142. IEEE, Piscataway (2012)
2. Mukherjee, A., Fakoorian, S.A.A., Huang, J., Swindlehurst, A.L.: Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutorials 16(3), 1550–1573 (2014)
3. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. 28, 656–715 (1949)
4. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54, 1355–1387 (1975)
5. Choi, J.: A robust beamforming approach to guarantee instantaneous secrecy rate. IEEE Trans. Wireless Commun. 15(2), 1076–1085 (2016)
6. Qiao, J., Zhang, H., Zhou, X., Yuan, D.: Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems. IEEE Trans. Veh. Technol. 67(1), 567–579 (2018)
7. Deng, Y., Wang, L., Zaidi, S.A.R., Yuan, J., Elkashlan, M.: Artificial-noise aided secure transmission in large scale spectrum sharing networks. IEEE Trans. Commun. 64(5), 2116–2129 (2016)
8. Bai, Z., Liang, S., Ma, P., Dong, Y., Zhang, H., Ma, Y.: QoS driven power allocation in secure multicarrier full-duplex relay systems. IEEE Trans. Wireless Commun. 19(2), 929–941 (2020)
9. Bai, Z., Ma, L., Dong, Y., Ma, P., Ma, Y.: Energy-efficient resource allocation for secure cognitive radio network with delay QoS guarantee. IEEE Syst. J. 13(3), 2795–2805 (2019)
10. Zeng, Y., Zhang, R., Lim, T.J.: Wireless communications with unmanned aerial vehicles: opportunities and challenges. IEEE Commun. Mag. 54(5), 36–42 (2016)
11. Gupta, L., Jain, R., Vaszkun, G.: Survey of important issues in UAV communication networks. IEEE Commun. Surv. Tutorials 18(2), 1123–1152 (2016)
12. Wu, Q., Zhang, R.: Common throughput maximization in UAV-enabled OFDMA systems with delay consideration. IEEE Trans. Commun. 66(12), 6614–6627 (2018)
13. Xie, L., Xu, J., Zhang, R.: Throughput maximization for UAV-enabled wireless powered communication networks - Invited Paper. 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, 2018, pp. 1–7
14. Lamine, A., Mguis, F., Snoussi, H., Ghedira, K.: Coverage optimization using multiple unmanned aerial vehicles with connectivity constraint. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 1361–1366. IEEE, Piscataway (2019)
15. Lyu, J., Zeng, Y., Zhang, R., Lim, T.J.: Placement optimization of UAV-mounted mobile base stations. IEEE Commun. Lett. 21(3), 604–607 (2017)
16. Jiao, S., Fang, F., Zhou, X., Zhang, H.: Joint beamforming and phase shift design in downlink UAV networks with irs-assisted NOMA. J. Commun. Information Networks 5(2), 138–149 (June 2020)
17. Zhang, G., Wu, Q., Cui, M., Zhang, R.: Securing UAV communications via joint trajectory and power control. IEEE Trans. Wireless Commun. 18(2), 1376–1389 (2019)
18. Wang, Q., Chen, Z., Li, H., Li, S.: Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system. IEEE Access 6, 62849–62855 (2018)
19. Sun, G., Li, N., Tao, X., Wu, H.: Power Allocation in UAV-enabled relaying systems for secure communications. IEEE Access 7, 119009–119017 (2019)
20. Wang, Q., Chen, Z., Li, H.: Energy-efficient trajectory planning for UAV-aided secure communication. China Commun. 15(5), 51–60 (2018)
21. Li, A., Wu, Q., Zhang, R.: UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. IEEE Wireless Commun. Lett. 8(1), 181–184 (2019)
22. Y. Zhou,et al.: Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location. IEEE Trans. Veh. Technol. 67(11), 11280–11284 (2018)
23. Zhou, X., Wu, Q., Yan, S., Shu, F., Li, J.: UAV-enabled secure communications: joint trajectory and transmit power optimization. IEEE Trans. Veh. Technol. 68(4), 4069–4073 (2019)
24. Li, Y., Zhang, R., Zhang, J., Yang, L.: Cooperative jamming via spectrum sharing for secure UAV communications. IEEE Wireless Commun. Lett. 9(3), 326–330 (2020)
25. Hua, M., Wang, Y., Wu, Q., Dai, H., Huang, Y., Yang, L.: Energy-efficient cooperative secure transmission in multi-UAV-enabled wireless networks. IEEE Trans. Veh. Technol. 68(8), 7761–7775 (2019)
26. Shen, L., Zhu, J.: On-line avoidance strategy with multiple no-fly zones. In: 2018 IEEE CSAA Guidance, Navigation and Control Conference (CGNCC), pp. 1–6. IEEE, Piscataway (2018)
27. Gao, Y., Tang, H., Li, B., Yuan, X.: Joint trajectory and power design for UAV-enabled secure communications with no-fly zone constraints. IEEE Access 7, 44459–44470 (2019)
28. Jeong, C., Kim, I.: Optimal power allocation for secure multi-carrier relay systems. 2011 8th International Workshop on Multi-Carrier Systems & Solutions, Herrsching, 2011, pp. 1–4
29. Wang, Q., Chen, Z., Mei, W., Fang, J.: Improving physical layer security using UAV-enabled mobile relaying. IEEE Wireless Commun. Lett. 6(3), 310–313 (2017)
30. Li, C.J., Ling, H.: Synthetic aperture radar imaging using a small consumer drone. 2015 IEEE International Symposium on Antennas and Propagation USNC/URSI National Radio Science Meeting, pp. 685–686
31. Pei, Y., Liang, Y., Teh, K.C., Li, K.H.: Secure communication in multi-antenna cognitive radio networks with imperfect channel state information. IEEE Trans. Signal Process. 59(4), 1683–1693 (2011)
32. Li, Y., Zhang, R., Zhang, J., Gao, S., Yang, L.: Cooperative jamming for secure UAV communications with partial eavesdropper information. IEEE Access 7, 94593–94603 (2019)
33. Roh, Y., Jung, S., Kang, J.: 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. IEEE, Piscataway (2019)
34. 'Enhanced LTE support for aerial vehicles,' 3GPP, Sophia Antipolis, France, Rep. TR 36.777. https://www.3gpp.org/ftp/Specs/archive/36_series/36.777. Accessed 11 November 2021
35. Gopala, P.K., Lai, L., El Gamal, H.: On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory 54(10), 4687–4698 (Oct. 2008)
36. Yu, W., Lui, R.: Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans. Commun. 54(7), 1310–1322 (July 2006)

37. Wang, T., Vandendorpe, L.: Successive convex approximation based methods for dynamic spectrum management. In: 2012 IEEE International Conference on Communications (ICC), pp. 4061–4065. IEEE, Piscataway (2012)
38. Boyd, S., Vandenberghe, L.: Convex optimization. Cambridge University Press, Cambridge (2004)
39. CVX Research, Inc.: CVX: Matlab software for disciplined convex programming, version 2.0. http://cvxr.com/cvx. Accessed April 2011

How to cite this article: Yin G, Zhou X, Ma P, Fang F, Zhao P.: Joint trajectory design and power allocation for unmanned aerial vehicles aided secure transmission in the presence of no-fly zone. IET Commun. 16, 172–186 (2022). https://doi.org/10.1049/cmu2.12326