IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 14, 2019, accepted June 28, 2019, date of publication July 4, 2019, date of current version July 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2926741

Cooperative Jamming for Secure UAV Communications With Partial Eavesdropper Information

YUPENG LI[1,2], RONGQING ZHANG[3], (Member, IEEE), JIANHUA ZHANG[4], (Senior Member, IEEE), SHIJIAN GAO[2], AND LIUQING YANG[2], (Fellow, IEEE)

[1]Key Laboratory of Universal Wireless Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Department of Electrical and Computer Engineering, Colorado State University, Fort Collins, CO 80523-1373, USA
[3]School of Software Engineering, Tongji University, Shanghai 201804, China
[4]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Jianhua Zhang (jhzhang@bupt.edu.cn)

This work was supported in part by the National Science and Technology Major Program of the Ministry of Science and Technology under Grant 2018ZX03001031, in part by the Key Program of Beijing Municipal Natural Science Foundation under Grant L172030, in part by the Beijing Municipal Science & Technology Commission Project under Grant Z171100005217001, in part by the Key Project of State Key Laboratory of Networking and Switching Technology under Grant NST20170205, in part by the National Key Technology Research and Development Program of the Ministry of Science and Technology of China under Grant 2012BAF14B01, in part by the National Key Research and Development Project under Grant 2017YFE0119300, and in part by the China Scholarship Council (CSC) under Grant 201806470003.

ABSTRACT The broadcast nature of air-to-ground line-of-sight (LoS) wireless channel imposes a great challenge in secure unmanned aerial vehicle (UAV) communications. To address this issue, this paper investigates UAV-ground communications from the physical-layer security perspective. Specifically, the investigated scenario includes a UAV serving as the base station (BS) that transmits confidential signals to a legitimate ground user, and there are multiple eavesdroppers on the ground with unknown position information. To further enhance the secrecy performance of the UAV-ground communications, an idle UAV can be employed to serve as a friendly jammer, which can transmit jamming signals to confuse the eavesdroppers. In our proposed strategy, the flying trajectory and the transmit power for both the UAVs are jointly optimized by maximizing the worst-case secrecy rate (WCSR) of the system. Considering the intractability of the formulated non-convex problem, we further provide a block coordinate descent-based iterative optimization method. Simulations verify that our proposed algorithm can significantly improve the average WCSR in comparison with the existing works.

INDEX TERMS Worst case secrecy rate, physical layer security, UAV communications.

I. INTRODUCTION

Thanks to the low cost and high flexibility, unmanned aerial vehicles (UAVs) have gained increasing interests in the areas of emergency services, intelligent transportation, etc. Recently, UAVs have also been applied in wireless communications [1]–[3]. As the UAV-to-ground channels usually exhibit line-of-sight (LoS) links, UAV is regarded as an attractive candidate wireless service provider [4]. Hence, some information technology giants, such as Facebook [5] and Google [6], have launched pilot projects for providing ubiquitous access by using UAVs. Meanwhile, great efforts in academia have also been devoted to exploit various applications of UAVs [7] like the aerial base stations [8]–[10], the flying computing cloudlets [11], the mobile relays [12], the solar-powered UAV communication platform [13], and so on. However, the broadcast nature of wireless communications imposes great threat on the information secrecy for UAV. Besides, the UAV-to-ground channel usually exhibits an LoS link, which makes UAV communications more susceptible for interceptions by ground eavesdroppers. These impose a severe security challenge on UAV communications.

To address the secrecy issue in UAV communications, extensive information secrecy related techniques have been

The associate editor coordinating the review of this manuscript and approving it for publication was Anandakumar Haldorai.

proposed at different protocol layers. For example, cryptographic methods are deployed at the higher protocol layer usually with high computational complexity. As a more computationally efficient and resource-saving alternative [14], physical layer security (PLS) techniques [15]–[18] utilize the characteristics of wireless channels and the quality gap between the legitimate and wiretap channels to guarantee perfect information-theoretic secrecy. Therefore, PLS emerges as a promising concept in wireless communication systems.

Recently, several works have focused on how to guarantee a secure UAV communication by PLS-enhanced techniques [19], [20]. For example, UAV-enabled relaying technique was introduced to enhance the secrecy capacity of wireless communication systems [21], [22]. Besides, UAV could also serve as a friendly jammer to improve the secrecy performance [23]–[25]. In [26], a joint UAV trajectory and power allocation design strategy was studied, where the secrecy rate was maximized by enhancing the legitimate link and deteriorating the wiretap link. To strengthen the practicability of the scenario, a robust joint UAV trajectory and power allocation strategy was developed in [27], where more than one eavesdroppers exist on the ground with their exact locations unknown. However, since there are multiple eavesdroppers and their exact locations are unknown, it is difficult for the UAV to serve as source (termed as source UAV hereafter) keep far from all the eavesdroppers (Eves). Thus, it is very likely that the UAV-to-destination channel is worse than the UAV-to-eavesdropper channel during most of its flight. In such a scenario, the UAV-to-destination link cannot exchange any confidential information since the secrecy capacity is zero.

Motivated by the fact that once the main channel is noisier than the wiretap channel, the secrecy capacity will be zero, we employ an idle UAV which serves as a cooperative jammer to enhance the secrecy capacity of the UAV communications. To be specific, UAV serving as the cooperative jammer (termed as jammer UAV hereafter) can schedule its flying trajectory as close as possible to the ground eavesdroppers, and then transmits jamming signals to the eavesdroppers to compromise the wiretap channel [15], [16], [28], [29]. With the help of the jammer, it can be guaranteed that, during most of the flight, the UAV-to-destination link has a greater chance to be better than the UAV-to-eavesdropper link. Hence, in such a scenario, and with inexact eavesdropper location information, it is a meaningful and challenging issue to jointly optimize the trajectory and transmit power of both UAVs. To the best of our knowledge, this issue has yet not been addressed.

In this paper, we investigate the PLS issue in UAV communications with multiple location-unknown eavesdroppers. In the investigated scenario, a source UAV transmits confidential signals to a ground destination, where multiple on-ground eavesdroppers are present, with their specific locations unknown to the source UAV. Meanwhile, an idle UAV is employed to serve as a friendly jammer and transmit jamming signals to suppress the wiretap channel. Then, we propose to jointly optimize the transmit power and flying trajectories for both UAVs (i.e., source UAV and jammer UAV), in order to maximize the average worst-case secrecy rate (WCSR). The main contributions of our work are as follows:

- In this paper, we employ an idle UAV as a cooperative jammer who transmits jamming signals to confuse the eavesdroppers. Besides, this work also takes into account multiple eavesdroppers with inexact location information, which is more reasonable for practical applications. To the best of our knowledge, this is the first work that considers such a scenario.
- In our strategy, the flying trajectories and the transmit power for both UAVs are jointly optimized by maximizing the system WCSR. Considering the formulated optimization problem is an NP-hard one, we propose a block coordinate descent and successive convex optimization method, which optimizes the power of UAVs, the trajectory of source UAV, and the trajectory of jammer UAV in an iterative manner.
- Our proposed strategy possesses strong robustness against the uncertainty of the multiple eavesdroppers, which is verified by conducted simulations.

The remainder of the paper is organized as follows. In Section II, the system model and the problem formulation are described. In Section III, the problem solution to our formulated non-convex problem is described. Simulations are presented to verify the efficiency in enhancing the system secrecy of our proposed strategy in Section IV. Followed by the conclusions in Section V.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

We consider a UAV-ground wireless communication system. A source UAV (S) above the ground transmits confidential information to a legitimate ground destination (D), with K ground Eves (E) trying to wiretap the legitimate communication from S to D. In this paper, a jammer UAV (J) is employed to transmit jamming signals to confuse the Eves. Thanks to the mobility of UAVs, the source UAV is inclined to move close to the destination to enhance the legitimate channel and achieve higher transmit rate, while the jammer UAV tends to hover above the Eves to obtain better jamming performance. In the study, we assume that each node has a single antenna. The scenario is shown in Fig. 1.

Without loss of generality, we assume that D locates at $(0, 0, 0)$, which is exactly known by S. In practice, the rough location information of Eves can be estimated by an camera or synthetic aperture radar [27], [30]. While the Eves may try to hide their existences, and thus the location estimation may suffer from errors. Therefore, we express the relationship between the real and the estimated location of Eve k in the x-y coordinate as follows

$$x_k = x_{E_k} + \Delta x_k, \quad y_k = y_{E_k} + \Delta y_k \tag{1}$$

where $(x_{E_k}, y_{E_k}, 0)$ is the estimated location of Eve k, $k \in \{1, 2, \ldots, K\}$, $(x_k, y_k, 0)$ is the exact location of Eve k, Δx_k and Δy_k are the estimation errors for x_k and y_k

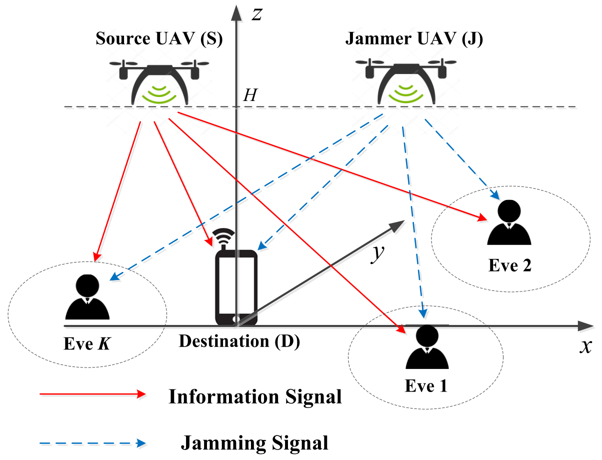


FIGURE 1. Cooperative jammer aided UAV communications with *K* potential eves on the ground.

respectively, i.e.,

$$(\Delta x_k, \Delta y_k) \in \varepsilon_k \triangleq \{(\Delta x_k, \Delta y_k) | \Delta x_k^2 + \Delta y_k^2 \leq Q_k^2\}. \quad (2)$$

And ε_k represents the possible error set. Then, we can regard that Eve k locates in a circular region with center $(x_{E_k}, y_{E_k}, 0)$ and radius Q_k.

It is assumed that UAVs fly at a constant altitude H, which is specified for the safety consideration such as building avoidance [26]. In practice, the constant altitude can help reduce the energy consumption in ascending or descending. Besides, the derived results in this paper can be easily extended to the case with the altitude considered. Thus, S's coordinate over time is expressed as $(x_S(t), y_S(t), H)$, $0 \leq t \leq T$, where T is its flight duration. To simplify the trajectory design, we quantize the flight duration T into N small time slots with equal length d_t. Since d_t is small enough, S can be regarded as static in each time slot. Thus, S's coordinate over the duration T can be expressed as a sequence $\{(x_S[n], y_S[n], H)\}_{n=1}^{N}$. S's initial and final locations are represented as $(x_S[0], y_S[0], H)$ and $(x_S[N+1], y_S[N+1], H)$, respectively. Then the mobility constraints of S can be expressed as

$$(x_S[n+1] - x_S[n])^2 + (y_S[n+1] - y_S[n])^2 \leq (v_{max} \cdot d_t)^2, \quad \forall n, \quad (3)$$

where v_{max} is the maximum speed for both UAVs.

Similarly, J's trajectory over the duration T can be expressed as a sequence $\{(x_J[n], y_J[n], H)\}_{n=1}^{N}$. J's initial and final locations are expressed as $(x_J[0], y_J[0], H)$ and $(x_J[N+1], y_J[N+1], H)$, respectively. Also, the mobility constraints of J is

$$(x_J[n+1] - x_J[n])^2 + (y_J[n+1] - y_J[n])^2 \leq (v_{max} \cdot d_t)^2, \quad \forall n. \quad (4)$$

The UAV-ground channels are mainly LoS links demonstrated in [26], [27]. As a result, we assume that the channel power gain mainly depends on the distance between transmitter UAV and the ground receiver. Thus, the channel gain between the UAV $p \in \{S, J\}$ and ground receiver $q \in \{D, E\}$ at slot n follows the free-space path loss model as follows,

$$\begin{aligned} h_{pq}[n] &= \beta_0 d_{pq}^{-2}[n] \\ &= \frac{\beta_0}{(x_p[n] - x_q[n])^2 + (y_p[n] - y_q[n])^2 + H^2}, \end{aligned} \quad (5)$$

where β_0 is the power gain within reference distance $d_0 = 1$, and d_{pq} is the distance between the UAV p and the ground node q at time n.

As we primarily concern about the system secrecy rate of the system and assume that the energy of the UAV is sufficient within the mission period. Therefore, we focus on the information transmit power of the UAV. Assume $P_p[n]$ is the transmit power in time slot n, P_{pmax} is the allowable peak transmit power of UAV p. Then, the power constraints of UAVs are

$$0 \leq P_S[n] \leq P_{S_{max}}, \quad (6a)$$

$$0 \leq P_J[n] \leq P_{J_{max}}. \quad (6b)$$

To guarantee a secure transmission under indeterministic eavesdropper channel state information (CSI), we adopt the WCSR as the performance matric. Concretely, the WCSR is defined as the minimum secrecy rate for any error of the uncertainty region,

$$R_{sec} = \frac{1}{N}\sum_{n=1}^{N} [\log_2 R_D[n] - \max_{k \in K} \max_{(\Delta x_k, \Delta y_k) \in \varepsilon_k} \log_2 R_{E_k}[n]]^+ \quad (7)$$

where

$$R_D[n] = 1 + \frac{P_S[n] h_{SD}[n]}{P_J[n] h_{JD}[n] + \sigma^2}, \quad (8)$$

$$R_{E_k}[n] = 1 + \frac{P_S[n] h_{SE_k}[n]}{P_J[n] h_{JE_k}[n] + \sigma^2}, \quad (9)$$

where $[x]^+ \triangleq \max(x, 0)$, σ^2 denotes Gaussian noise power. Then, $\log_2 R_D[n]$ and $\log_2 R_{E_k}[n]$ represent the achievable rate of D and Eve k at time slot n, respectively.

B. PROBLEM FORMULATION

For the secrecy communication from S to D, we jointly optimize the trajectory and transmit power for both source UAV and jammer UAV to maximize the average WCSR subject to their mobility and power constraints. The optimization variables include the flying trajectory and transmit power of both UAVs, which are $\boldsymbol{x_S} \triangleq [x_S[1], \ldots, [x_S[N]]\dagger$, $\boldsymbol{y_S} \triangleq [y_S[1], \ldots, [y_S[N]]\dagger$, $\boldsymbol{x_J} \triangleq [x_J[1], \ldots, [x_J[N]]\dagger$, $\boldsymbol{y_J} \triangleq [y_J[1], \ldots, [y_J[N]]\dagger$, $\boldsymbol{P_S} \triangleq [P_S[1], \ldots, [P_S[N]]\dagger$, and $\boldsymbol{P_J} \triangleq [P_J[1], \ldots, [P_J[N]]\dagger$, where $\dagger$ is the transpose operation. Then, the WCSR can be formulated as follows, where constant term $1/N$ is omitted,

$$\text{(P0)}: \max_{\substack{\boldsymbol{x_S}, \boldsymbol{y_S} \\ \boldsymbol{x_J}, \boldsymbol{y_J} \\ \boldsymbol{P_S}, \boldsymbol{P_J}}} \sum_{n=1}^{N} [\log_2 R_D[n] - \max_{k \in K} \max_{(\Delta x_k, \Delta y_k) \in \varepsilon_k} \log_2 R_{E_k}[n]]^+$$

$$\text{s.t.} \quad (3), (4), (6a), (6b),$$

(P0) is difficult to solve due to the following reasons: 1) the operator $[\cdot]^+$ is non-smoothness for the objective function; 2) the objective function is not concave even without the $[\cdot]^+$ operation; 3) the infinite number of possible (x_k, y_k) make (P0) an intractable optimization problem. Thus, in the following section, we propose an efficient iterative algorithm to solve (P0) approximately.

III. PROPOSED SOLUTION FOR (P0)

Through setting $P_S[n] = 0$, we can guarantee each item in the summation be non-negative. Thus, we can omit the operation $[\cdot]^+$, and the formula of (P0) can be derived as follows,

$$\text{(P1)}: \max_{\substack{\boldsymbol{x}_S,\boldsymbol{y}_S\\ \boldsymbol{x}_J\,\boldsymbol{y}_J,\\ \boldsymbol{P}_S,\boldsymbol{P}_J}} \sum_{n=1}^{N}\left\{\log_2 R_D[n] - \max_{k\in K}\max_{(\Delta x_k,\Delta y_k)\in\varepsilon_k}\log_2 R_{E_k}[n]\right\}$$
$$\text{s.t.}\quad (3),\ (4),\ (6a),\ (6b).$$

Although (P1) is more tractable, it is still a non-convex optimization problem. Fortunately, we observe it can be divided into two components, i.e., the trajectory and transmit power, which facilitates the problem optimization via the block coordinate descent method [31]. To be specific, we solve (P1) by solving the following three sub-problems iteratively:

- Optimize S's trajectory $(\boldsymbol{x}_S, \boldsymbol{y}_S)$ under given $\boldsymbol{P}_S$, $\boldsymbol{P}_J$ and $(\boldsymbol{x}_J, \boldsymbol{y}_J)$;
- Optimizie J's trajectory $(\boldsymbol{x}_J, \boldsymbol{y}_J)$ knowing $\boldsymbol{P}_S$, $\boldsymbol{P}_J$ and $(\boldsymbol{x}_S, \boldsymbol{y}_S)$;
- Jointly optimize the two UAVs' power $\boldsymbol{P}_S$ and $\boldsymbol{P}_J$ under certain UAVs' trajectories.

Then, the sub-optimization procedure experiences an iterative manner until the algorithm converges.

A. OPTIMIZING SOURCE UAV'S TRAJECTORY $(\boldsymbol{x}_S, \boldsymbol{y}_S)$

Knowing the $\boldsymbol{P}_S$, $\boldsymbol{P}_J$ and J's trajectory, (P1) can be expressed as

$$\text{(P2)}: \max_{\boldsymbol{x}_S,\boldsymbol{y}_S} \sum_{n=1}^{N}\left\{\log_2\left(1+\frac{P_S[n]h_{SD}[n]}{P_J[n]h_{JD}[n]+\sigma^2}\right)\right.$$
$$\left. -\log_2\left(1+\frac{P_S[n]\max\limits_{k\in K}\max\limits_{(\Delta x_k,\Delta y_k)\in\varepsilon_k} h_{SE_k}[n]}{P_J[n]h_{JE}[n]+\sigma^2}\right)\right\}$$
$$\text{s.t.}\quad (3). \tag{10}$$

By introducing $\boldsymbol{u} \triangleq [u[1], u[2], \ldots, u[N]]^\dagger$ and $\boldsymbol{t} \triangleq [t[1], t[2], \ldots, t[N]]^\dagger$ as the slack variables, and letting $g_n = P_S[n]/(P_J[n]h_{JD}[n]+\sigma^2)$, $p_n = P_S[n]/(P_J[n]h_{JE}[n]+\sigma^2)$, the optimization problem of S's trajectory can be derived as

$$\text{(P3)}: \max_{\substack{\boldsymbol{x}_S,\boldsymbol{y}_S,\\ \boldsymbol{u},\boldsymbol{t}}} \sum_{n=1}^{N}\log_2\left(1+\frac{g_n}{u[n]}\right)-\log_2\left(1+\frac{p_n}{t[n]}\right) \tag{11a}$$
$$\text{s.t.}\quad \min_{k\in K}\ \min_{(\Delta x,\Delta y)\in\varepsilon_k}\ (x_S[n]-x_k)^2$$
$$+(y_S[n]-y_k)^2+H^2 \geq t[n], \quad \forall n \tag{11b}$$
$$x_S^2[n]+y_S^2[n]+H^2-u[n]\leq 0, \quad \forall n \tag{11c}$$
$$t[n]\geq H^2, \quad \forall n, \tag{11d}$$
$$(3).$$

(P2) and (P3) are equivalent in terms of $(\boldsymbol{x}_S, \boldsymbol{y}_S)$, as the constraints (11b) and (11c) must hold with equalities at the optimal solution to (P3). Since if constraints (11b) and (11c) are not tight, the objective value of (11a) can be improved by increasing $t[n]$ or decreasing $u[n]$. Therefore, we can solve (P3) instead. However, (P3) is still difficult to solve, because of the infinite number of $(\Delta x_k, \Delta y_k)$ in constraint (11b). Now, we substitute (1) and (2) into (11b) as follows

$$\Delta x_k^2+\Delta y_k^2-Q_k^2\leq 0, \quad \forall k, \tag{12a}$$
$$-(x_S[n]-x_{E_k}-\Delta x_k)^2-(y_S[n]-y_{E_k}-\Delta y_k)^2$$
$$-H^2+t[n]\leq 0, \quad \forall k. \tag{12b}$$

According to S-procedure [27], which gives conditions under which a particular quadratic inequality is a consequence of another quadratic inequality, the implication (12a)⇒(12b) holds if and only if there is $\xi_k[n]\geq 0$ so that

$$\boldsymbol{\Phi}(x_S[n], y_S[n], t[n], \xi_k[n]) \succeq 0, \quad \forall k, n, \tag{13}$$

where

$$\boldsymbol{\Phi}(x_S[n], y_S[n], t[n], \xi_k[n])$$
$$=\begin{bmatrix} \xi_k[n]+1 & 0 & x_{E_k}-x_S[n] \\ 0 & \xi_k[n]+1 & y_{E_k}-y_S[n] \\ x_{E_k}-x_S[n] & y_{E_k}-y_S[n] & -Q_k^2\xi_k[n]+c_k[n] \end{bmatrix},$$

and

$$c_k[n]=x_S^2[n]-2x_{E_k}x_S[n]+x_{E_k}^2+y_S^2[n]-2y_{E_k}y_S[n]$$
$$+y_{E_k}^2+H^2-t[n]. \tag{14}$$

Then, the optimization problem can be rewritten as follows,

$$\text{(P4)}: \max_{\substack{\boldsymbol{x}_S,\boldsymbol{y}_S,\\ \boldsymbol{u},\boldsymbol{t},\boldsymbol{\Xi}}} \sum_{n=1}^{N}\log_2\left(1+\frac{g_n}{u[n]}\right)-\log_2\left(1+\frac{p_n}{t[n]}\right) \tag{15a}$$
$$\text{s.t.}\quad \boldsymbol{\Phi}(x_S[n], y_S[n], t[n], \xi_k[n])\succeq 0, \quad \forall k, n, \tag{15b}$$
$$\xi_k[n]\geq 0, \quad \forall k, n, \tag{15c}$$
$$(3),\ (11c),\ (11d),$$

where $\boldsymbol{\Xi} \triangleq [\xi_1, \ldots, \xi_K]$ and $\boldsymbol{\xi}_k \triangleq [\xi_k[1], \ldots, \xi_k[N]]^\dagger$.

Nevertheless, the objective function (P4) is still non-concave, due to the non-concavity of $\log_2(1+g_n/u[n])$ with respect to $u[n]$. Besides, the terms $x_S^2[n]$ and $y_S^2[n]$ in $c_k[n]$ are non-linear, leading to the non-convexity of constraint (15b). Thus, (P4) is still difficult to be solved. Therefore, we propose an iterative algorithm to obtain an approximate solution of (P4). First, we assume that

$$\boldsymbol{u}_{fea} \triangleq [u_{fea}[1], u_{fea}[2], \ldots, u_{fea}[N]]^\dagger,$$
$$\boldsymbol{x}_{Sfea} \triangleq [x_{Sfea}[1], x_{Sfea}[2], \ldots, x_{Sfea}[N]]^\dagger,$$
$$\boldsymbol{y}_{Sfea} \triangleq [y_{Sfea}[1], y_{Sfea}[2], \ldots, y_{Sfea}[N]]^\dagger,$$

are feasible solutions to (P4). With the first-order Taylor expansion of $x_S^2[n], y_S^2[n]$ and $log_2\left(1+\frac{g_n}{u[n]}\right)$ at their separate feasible points,

$$x_S^2[n] \geq -x_{Sfea}^2[n] + 2x_{Sfea}[n]x_S[n], \quad (16)$$

$$y_S^2[n] \geq -y_{Sfea}^2[n] + 2y_{Sfea}[n]y_S[n], \quad (17)$$

$$\log_2\left(1+\frac{g_n}{u[n]}\right) \geq log_2\left(1+\frac{g_n}{u_{fea}[n]}\right) - \frac{g_n(u[n]-u_{fea}[n])}{\ln 2(u_{fea}^2[n]+g_n u_{fea}[n])}, \quad (18)$$

(P4) is reformulated as follows,

$$\begin{aligned}
(\text{P5}):\ \max_{\substack{x_S,y_S,\\ u,t,\Xi}} \sum_{n=1}^{N} \Bigg\{ & -\frac{g_n u[n]}{\ln 2(u_{fea}^2[n]+g_n u_{fea}[n])} \\
& -\log_2\left(1+\frac{p_n}{t[n]}\right)\Bigg\} && (19a)\\
\text{s.t.}\ & \tilde{\mathbf{\Phi}}(x_S[n], y_S[n], t[n], \xi_k[n]) \succeq 0, \quad \forall k,n, && (19b)\\
& \xi_k[n] \geq 0, \quad \forall k,n, && (19c)\\
& (3), (11c), (11d),
\end{aligned}$$

where

$$\tilde{\mathbf{\Phi}}(x_S[n], y_S[n], t[n], \xi_k[n]) = \begin{bmatrix} \xi_k[n]+1 & 0 & x_{E_k}-x_S[n] \\ 0 & \xi_k[n]+1 & y_{E_k}-y_S[n] \\ x_{E_k}-x_S[n] & y_{E_k}-y_S[n] & -Q_k^2\xi_k[n]+\tilde{c}_k[n] \end{bmatrix},$$

and

$$\begin{aligned}
\tilde{c}_k[n] = & -x_{Sfea}^2[n] + 2x_{Sfea}[n]x_S[n] - 2x_{E_k}x_S[n] + x_{E_k}^2 \\
& + y_{Sfea}^2[n] + 2y_{Sfea}[n]y_S[n] - 2y_{E_k}y_S[n] + y_{E_k}^2 \\
& + H^2 - t[n].
\end{aligned}$$

After the above approximation, (19a) is concave and the constraints are convex. As a result, the (P5) is a semi-definite programming which can be simply solved with the interior-point method [31].

B. OPTIMIZING JAMMER UAV'S TRAJECTORY (x_J, y_J)

Given the $\boldsymbol{P}_S$, $\boldsymbol{P}_J$ and S's trajectory, (P1) can be expressed as

$$\begin{aligned}
\max_{x_J,y_J} \sum_{n=1}^{N} \Bigg\{ & \log_2\left(1+\frac{P_S[n]h_{SD}[n]}{P_J[n]h_{JD}[n]+\sigma^2}\right) \\
& -\log_2\left(1+\frac{P_S[n]h_{SE}[n]}{P_J[n]\min\limits_{k\in K}\min\limits_{(\Delta x_k,\Delta y_k)\in\varepsilon_k} h_{JE_k}[n]+\sigma^2}\right)\Bigg\} \\
\text{s.t.}\ & (4). && (20)
\end{aligned}$$

After introducing $\boldsymbol{l} \triangleq [l[1], l[2], \ldots, l[N]]^\dagger$, $\boldsymbol{m} \triangleq [m[1], m[2], \ldots, m[N]]^\dagger$ as the slack variables, and then letting $c_n = P_S[n]h_{SD}[n]/\sigma^2$, $e_n = P_S[n]h_{SE}[n]/\sigma^2$, the optimization problem of jammer's trajectory can be derived as

$$\begin{aligned}
(\text{P6}):\ \max_{\substack{x_J,y_J\\ \boldsymbol{l},\boldsymbol{m}}} \sum_{n=1}^{N} & \log_2\left(1+\frac{c_n}{\frac{P_J[n]\gamma_0}{l[n]}+1}\right) \\
& -\log_2\left(1+\frac{e_n}{\frac{P_J[n]\gamma_0}{m[n]}+1}\right) && (21a)\\
\text{s.t.}\ & l[n]-x_J^2[n]-y_J^2[n]-H^2 \leq 0, \quad \forall n, && (21b)\\
& \max_{k\in K}\max_{(\Delta x,\Delta y)\in\varepsilon_k} (x_J[n]-x_k)^2+(y_J[n]-y_k)^2 \\
& +H^2-m[n] \leq 0, \quad \forall k,n && (21c)\\
& l[n] \geq H^2, \quad \forall n, && (21d)\\
& (4),
\end{aligned}$$

where $\gamma_0 = \beta_0/\sigma^2$.

To solve (P6), firstly we simplify the constraint of (21c). We solve the eavesdropper k's location to maximize

$$h_k = \max_{(\Delta x,\Delta y)\in\varepsilon_k} (x_J[n]-x_k)^2+(y_J[n]-y_k)^2+H^2, \quad \forall n. \quad (22)$$

Assuming jammer's trajectory in the $(l-1)$th iteration is $(\boldsymbol{x}_J^{(l-1)}, \boldsymbol{y}_J^{(l-1)})$, we use the J' location in the $(l-1)$th iteration to approximately achieve the maximization of

$$h_k = \max_{(\Delta x,\Delta y)\in\varepsilon_k} (x_J{}^{(l-1)}[n]-x_k)^2+(y_J{}^{(l-1)}[n]-y_k)^2 + H^2, \quad \forall n. \quad (23)$$

Then, based on the geometrical theory, the location of Eve k can be obtained by maximizing h_k at the lth iteration, as follows

$$x_k^{(l)}[n] = x_{E_k} - Q_k\frac{(x_J^{(l-1)}[n]-x_{E_k})}{\sqrt{(x_J^{(l-1)}[n]-x_{E_k})^2+(y_J^{(l-1)}[n]-y_{E_k})^2}} \quad (24)$$

$$y_k^{(l)}[n] = y_{E_k} - Q_k\frac{(y_J^{(l-1)}[n]-y_{E_k})}{\sqrt{(x_J^{(l-1)}[n]-x_{E_k})^2+(y_J^{(l-1)}[n]-y_{E_k})^2}} \quad (25)$$

Therefore, constraint (21c) can be further rewritten as

$$\max_{k\in K} h_k = \max_{k\in K}(x_J[n]-x_k^{(l)}[n])^2+(y_J[n]-y_k^{(l)}[n])^2 + H^2 - m[n] \leq 0, \quad \forall n. \quad (26)$$

Besides, the objective function (21a) is non-concave. Hence, we approximate the term $\log_2\left(1+\frac{e_n}{\frac{P_J[n]\gamma_0}{m[n]}+1}\right)$ with its upper bound as follows,

$$\log_2\left(1+\frac{e_n}{\frac{P_J[n]\gamma_0}{m[n]}+1}\right) \leq (m[n]-m^{(l-1)}[n])C^k[n] + \log_2\left(1+\frac{e_n m^{(l-1)}[n]}{m^{(l-1)}[n]+\gamma_0 P_J[n]}\right), \quad (27)$$

where, $m^{(l-1)}$ is the solution of m in the $(l-1)$th iteration, and $C_k[n] = \frac{e_n\gamma_0 P_J[n]}{\ln 2(m^{(l-1)}[n]+\gamma_0 P_J[n])((e_n+1)m^{(l-1)}[n]+\gamma_0 P_J[n])}$.

Moreover, the terms $x_J^2[n]$ and $y_J^2[n]$ are non-linear, leading to the non-concavity of constraint (21b). Based on

$$x_J^2[n] \geq -(x_J^{(l-1)}[n])^2 + 2x_J^{(l-1)}[n]x_J[n]$$

and

$$y_J^2[n] \geq -(y_J^{(l-1)}[n])^2 + 2y_J^{(l-1)}[n]y_J[n]$$

constraint (21b) can be recast as

$$\begin{aligned} l[n] + x_J^{(l-1)}[n]^2 - 2x_J^{(l-1)}[n]x_J[n] + y_J^{(l-1)}[n]^2 \\ -2y_J^{(l-1)}[n]y_J[n] - H^2 \leq 0, \quad \forall k, n. \end{aligned} \tag{28}$$

Accordingly, (P6) can be approximately reformulated as

$$\begin{aligned} \text{(P7)}: \; \max_{\substack{\boldsymbol{x}_J, \boldsymbol{y}_J \\ \boldsymbol{l}, \boldsymbol{m}}} \sum_{n=1}^{N} \Bigg\{ \log_2 \Bigg(1 + \frac{c_n}{\frac{P_J[n]\gamma_0}{l[n]} + 1} \Bigg) \\ +(m(n) - m^{(l-1)}[n])C^k[n] \Bigg\}, \\ \text{s.t.} \;\; (4), \; (21\text{d}), \; (26), \; (28). \end{aligned} \tag{29}$$

It is worth noting that (P7) is a convex optimization problem, which can be solved efficiently by convex optimization such as CVX [31].

C. JOINTLY OPTIMIZING BOTH UAVs' TRANSMIT POWER P_S AND P_J

Knowing the trajectories of both UAVs, (P1) can be rewritten as

$$\text{(P8)}: \max_{\boldsymbol{P}_S, \boldsymbol{P}_J} \sum_{n=1}^{N} \Big\{ \log_2 R_D[n] - \max_{k \in K} \max_{(\Delta x_k, \Delta y_k) \in \varepsilon_k} \log_2 R_{E_k}[n] \Big\} \tag{30a}$$

$$\text{s.t.} \;\; 0 \leq P_S[n] \leq P_{S_{max}} \tag{30b}$$

$$0 \leq P_J[n] \leq P_{J_{max}} \quad . \tag{30c}$$

First, we optimize $(\Delta x_k, \Delta y_k)$ to obtain the maximization of $\log_2 R_{E_k}[n]$ as follows,

$$\max_{(\Delta x_k, \Delta y_k) \in \varepsilon_k} \log_2 \left(1 + \frac{P_S[n]h_{SE_k}[n]}{P_J[n]h_{JE_k}[n] + \sigma^2} \right). \tag{31}$$

As the value of $P_J[n]h_{JE_k}[n]$ is much greater than the noise power on the receiver side, we can approximately optimize the function as follows,

$$f_k = \max_{(\Delta x_k, \Delta y_k) \in \varepsilon_k} \log_2 \left(1 + \frac{P_S[n]h_{SE_k}[n]}{P_J[n]h_{JE_k}[n]} \right), \tag{32}$$

where the value of $h_{SE_k}[n]$ and $h_{JE_k}[n]$ can be solved based on (5). For eavesdropper k, we can obtain the solution of $(x_k[n], y_k[n])$ by mathematical manipulation as follows,

$$(x_k[n], y_k[n]) = \begin{cases} (x_S[n], y_S[n]), \quad d_{SE_k}[n] \leq Q_k \\ (x_{E_k} + Q_k \dfrac{(x_S[n] - x_{E_k})}{d_{SE_k}[n]}, \\ \quad y_{E_k} + Q_k \dfrac{(y_S[n] - y_{E_k})}{d_{SE_k}[n]}), \quad d_{SE_k}[n] > Q_k \end{cases} \tag{33}$$

where $(x_k[n], y_k[n])$ is the coordinate of Eve k in time slot n, $d_{SE_k}[n] = \sqrt{(x_S[n] - x_{E_k}[n])^2 + (y_S[n] - y_{E_k}[n])^2}$ is the distance between the S and Eve k. By (5), we can obtain $h_{SE_k}[n]$ and $h_{JE_k}[n]$ as follows

$$h_{SE_k}[n] = \begin{cases} \dfrac{\beta_0}{H^2}, \quad d_{SE_k}[n] \leq Q_k \\ \dfrac{\beta_0}{\left(\sqrt{(x_S[n] - x_k)^2 + (y_S[n] - y_k)^2} - Q_k\right)^2 + H^2}, \\ \quad d_{SE_k}[n] > Q_k \end{cases} \tag{34}$$

$$h_{JE_k}[n] = \begin{cases} \dfrac{\beta_0}{(x_J[n] - x_S[n])^2 + (y_J[n] - y_S[n])^2 + H^2}, \\ \quad d_{SE_k}[n] \leq Q_k \\ \dfrac{\beta_0}{(x_J[n] - x_k[n])^2 + (y_J[n] - y_k[n])^2 + H^2}, \\ \quad d_{SE_k}[n] > Q_k \end{cases} \tag{35}$$

Similarly, we can also obtain $h_{SD}[n]$ and $h_{JD}[n]$.

Then, we can obtain $\max\limits_{k \in K} f_k$ among the k eavesdroppers. Assuming $k = k^*$, $\log_2(1 + \frac{P_S[n]h_{SE_k}[n]}{P_J[n]h_{JE_k}[n] + \sigma^2})$ reaches its maximization. In this case, the corresponding coordinate of Eve is $(x_k^*[n], y_k^*[n])$, and the corresponding channel gains are $h_{SE}^*[n]$ and $h_{JE}^*[n]$, respectively.

As a result, (P8) is reformulated as follows,

$$\max_{\boldsymbol{P}_S, \boldsymbol{P}_J} \sum_{n=1}^{N} \left\{ \log_2 R_D[n] - \log_2 \left(1 + \frac{P_S[n]h_{SE}^*[n]}{P_J[n]h_{JE}^*[n] + \sigma^2} \right) \right\} \tag{36a}$$

$$\text{s.t.} \; 0 \leq P_S[n] \leq P_{S_{max}}, \tag{36b}$$

$$0 \leq P_J[n] \leq P_{J_{max}}. \tag{36c}$$

Constraints (36b) and (36c) constitute a closed plane, thus the continuous objective function can achieve its maximum value either on the boundary or Fermat point. Via simple mathematical manipulation, we can obtain the Fermat point of (36a) as follows,

$$P_J[n] = \frac{h_{SE}^*[n] - h_{SD}[n]}{h_{SD}[n]h_{JE}^*[n] - h_{SE}^*[n]h_{JD}[n]} \sigma^2, \tag{37}$$

$$P_S[n] = \frac{a_1[n]^2 a_3[n] - a_2[n]^2 a_4[n]}{a_2[n]a_4[n]h_{SD}[n] - a_1[n]a_3[n]h_{SE}^*[n]}, \tag{38}$$

where

$$\begin{aligned} a_1[n] &\triangleq P_J[n]h_{JE}^*[n] + \sigma^2, \\ a_2[n] &\triangleq P_J[n]h_{JD}[n] + \sigma^2, \\ a_3[n] &\triangleq h_{SD}[n]H_{JD}[n], \\ a_4[n] &\triangleq h_{SE}^*[n]H_{JE}^*[n]. \end{aligned}$$

On the other side, we can obtain the optimal values among boundary points by simple mathematical manipulation. Hence, we can obtain the maximum of (36a) among the Fermat point and the boundary optimal point. Finally, the optimal solution is achieved denoted as $(P_{S_{opt}}[n], P_{J_{opt}}[n])$.

Algorithm 1 Proposed Iterative Algorithm for (P1)

```
Initialization: source UAV's transmit power $\boldsymbol{P}_S^{(0)}$, jammer UAV's transmit power $\boldsymbol{P}_J^{(0)}$, source UAV's trajectory $(\boldsymbol{x}_S^{(0)}, \boldsymbol{y}_S^{(0)})$, jammer UAV's trajectory $(\boldsymbol{x}_J^{(0)}, \boldsymbol{y}_J^{(0)})$, $m^{(0)}$, $u^{(0)}$, and $l = 0$.
repeat
    Set $l = l + 1$.
    Set $\boldsymbol{x}_{Sfea} = \boldsymbol{x}_S^{(l-1)}, \boldsymbol{y}_{Sfea} = \boldsymbol{y}_S^{(l-1)}$, and $\boldsymbol{u}_{fea} = \boldsymbol{u}^{(l-1)}$. Solve (P5) under given $\boldsymbol{P}_S^{(l-1)}, \boldsymbol{P}_J^{(l-1)}, (\boldsymbol{x}_J^{(l-1)}, \boldsymbol{y}_J^{(l-1)})$, then we can get $(\boldsymbol{x}_S^{(l)}, \boldsymbol{y}_S^{(l)})$.
    Solve eavesdropper $k$'s location $(\boldsymbol{x}_k^{(l)}, \boldsymbol{y}_k^{(l)})$ with formula (24) and (25); Then, solve (P7) under given $\boldsymbol{P}_S^{(l-1)}, \boldsymbol{P}_J^{(l-1)}, (\boldsymbol{x}_k^{(l)}, \boldsymbol{y}_k^{(l)}), (\boldsymbol{x}_J^{(l-1)}, \boldsymbol{y}_J^{(l-1)})$, and $(\boldsymbol{x}_S^{(l)}, \boldsymbol{y}_S^{(l)})$. We can get $(\boldsymbol{x}_J^{(l)}, \boldsymbol{y}_J^{(l)})$.
    Solve the inner Fermat point $\boldsymbol{P}_S, \boldsymbol{P}_J$ with (37) and (38); Obtain the optimal value among boundary points; Select the point, who makes (36a) reach its maximum value, among the Fermat point and the boundary optimal point.
until The increase of the objective value is smaller than a threshold $\varepsilon$.
```

In summary, the entire solution to (P1) is obtained by iteratively and alternately employing block coordinate descent and successive convex approximation method, i.e. optimizing S's trajectory, optimizing J's trajectory, and jointly optimizing both UAVs' transmit power alternately and iteratively. The complexity of the proposed algorithm is $\mathcal{O}[L \cdot N^{3.5}]$ [31], where L is the number of iterations. Details of the proposed solution to (P1) are shown in Algorithm 1.

IV. SIMULATIONS

In this section, we carry out simulations to evaluate the performance of our proposed joint trajectory and transmit power design for both source and jammer UAVs with inexact eavesdropper location information, which we call as "partial CSI with jamming (P-CSI/&J)" scheme hereafter. We compare the proposed algorithm with the following two benchmark schemes: 1) joint trajectory and transmit power design without jammer, which we call as "partial CSI without jamming (P-CSI/NJ)" scheme hereafter. There is no jammer UAV in this scheme, the other configuration is the same as our proposed algorithm. 2) joint trajectory and transmit power design for both source and jammer UAVs with exact eavesdropper location information, that is the same problem as our proposed algorithm except for knowing exact eavesdropper location information. We call it "exact CSI with jamming (E-CSI/&J)" scheme hereafter. The E-CSI/&J scheme will give us a reference of the gap between our proposed solution and the ideal solution. In the simulation, we set the number of eavesdroppers to 2. The initial feasible points are designed as follows: the source UAV flies to the point above destination at the maximum speed, then hovers there, and finally flies at the maximum speed to reach its final location; the jammer UAV flies to the point above the geometric center of the eavesdroppers at the maximum speed, then hovers at that point, and finally flies at the maximum speed to reach its final location. If UAVs do not have sufficient time to reach their hovering points, they will turn midway and fly to the final locations at the maximum speed. The flight height (H) of UAV is 100 m, $v_{max} = 10\,\text{m/s}$, $d_t = 0.5\,\text{s}$, $\gamma_0 = 80\,\text{dB}$, $P_{Smax} = P_{Jmax}$. Two cases are considered, where UAVs have different initial and final locations. In case 1, we set $(x_S[0], y_S[0]) = (x_J[0], y_J[0]) = (100, 200)$ m and $(x_S[N+1], y_S[N+1]) = (x_J[N+1], y_J[N+1]) = (100, -200)$ m as shown in Fig. 2. The estimated circle centers of eavesdroppers are $(-40, 20)$ m and $(-40, -20)$ m, the corresponding radiuses are 15 m and 20 m. The precise Eve locations are $(-43, 24)$ m and $(-43, -25)$ m. In case 2, we set $(x_S[0], y_S[0]) = (x_J[0], y_J[0]) = (0, 200)$ m and $(x_S[N+1], y_S[N+1]) = (x_J[N+1], y_J[N+1]) = (0, -200)$ m as shown in Fig. 3. The estimated circle centers of eavesdroppers are $(-40, 0)$ m and $(-50, -50)$ m, the corresponding radiuses are 15 m and 20 m. The precise Eve locations are $(-42, -5)$ m and $(-55, -48)$ m.

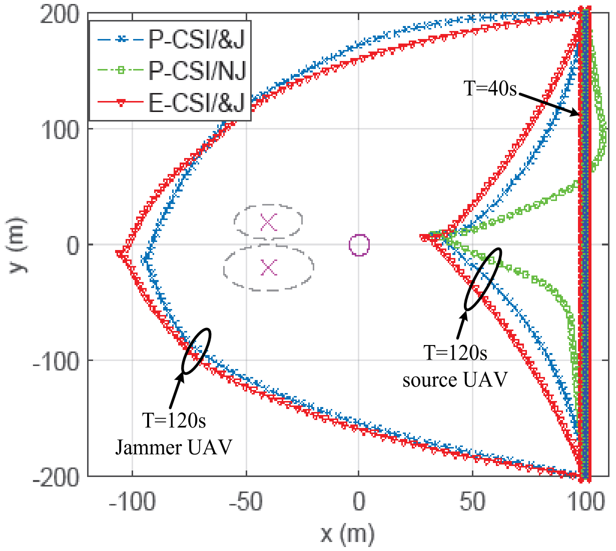


FIGURE 2. Trajectory comparisons of the proposed algorithm and the benchmark algorithms in case 1.

A. TRAJECTORIES OF UAVs FOR THE THREE ALGORITHMS

For case 1, Fig. 2 shows the trajectories of both UAVs for different schemes in different period T. The D and Eves are marked with ∘ and ×, respectively. The gray dotted circles represent the eavesdropper uncertain region. It is observed that when $T = 40$ s, the UAVs in different algorithms will obtain very similar trajectories, as $T = 40$ s is the minimum time for UAV flying from the initial location to the final location at the maximum speed. Then, we will analyze the situation when sufficient time is given, i.e. $T = 120$ s. We can split

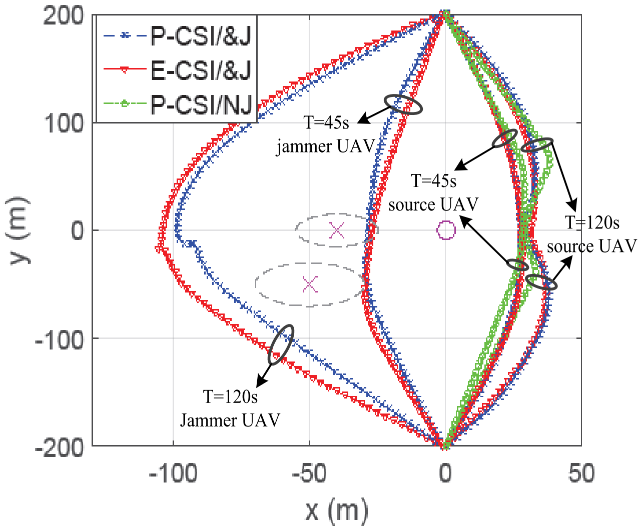
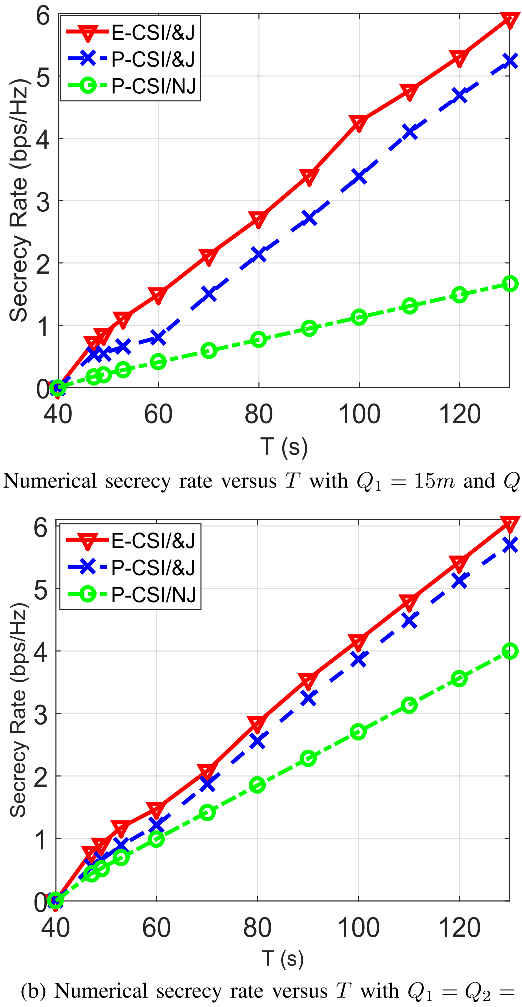


FIGURE 3. Trajectory comparisons of the proposed algorithm and the benchmark algorithms in case 2.



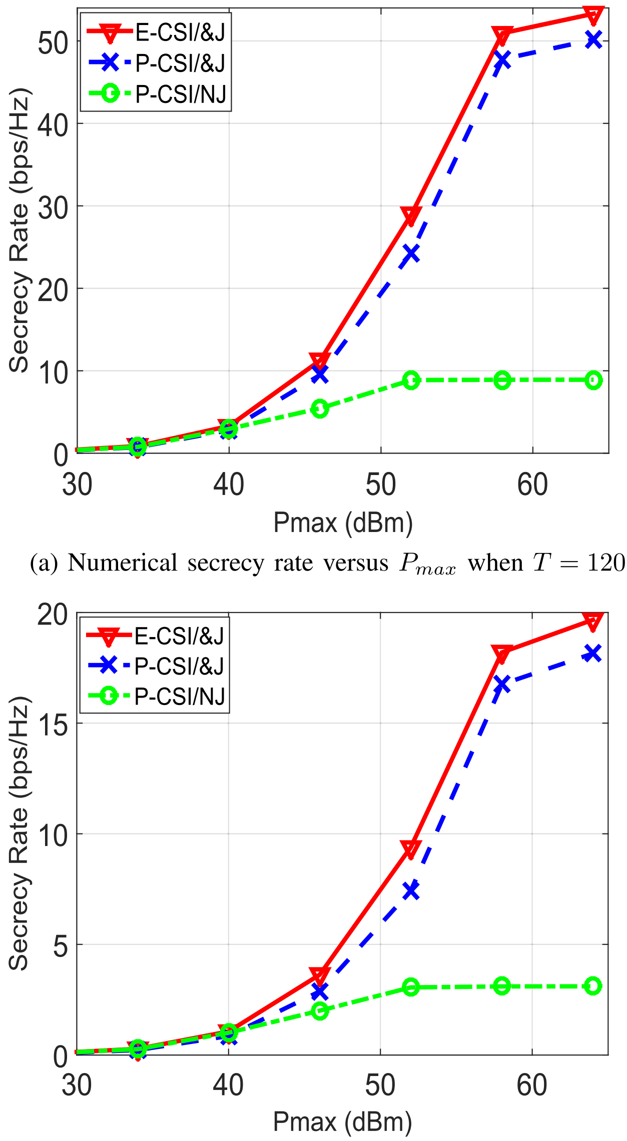
(a) Numerical secrecy rate versus T with $Q_1 = 15m$ and $Q_2 = 20m$.

(b) Numerical secrecy rate versus T with $Q_1 = Q_2 = 5m$.

FIGURE 4. Numerical secrecy rate performance versus T.

the flying into three stages. In the first stage, for all the three algorithms, the source UAVs fly in an arc path to a certain point near the destination at their maximum speed. In the second stage, they hover at this point as long as possible. The hovering point strikes an optimal balance between the information transmission and avoiding being eavesdropped by the Eves. Finally, in the third stage, they fly towards the final location in an arc path and reach there at the last time. For the E-CSI/&J and P-CSI/&J schemes, the jammer UAVs fly towards a certain point near the eavesdroppers and keep away from the destination in the first stage. Then, they hover at this point as long as possible, in the second stage. The hovering point strikes an optimal balance between the jamming service and not causing strong inference to the destination. Finally, they fly towards the final location and reach there at the last time. For both E-CSI/&J and P-CSI/&J schemes, in the first two stages, with the help of jammer, the trajectories of the source UAVs are more closed to the destination in comparison with P-CSI/NJ scheme. A smaller distance between the destination and the source UAV benefits the information confidential transmission between them. Besides, a shorter flying arc path in the first stage enables that the source UAV has more time to hover in the second stage, which also benefits the improvement of the achievable secrecy rate. The estimated circle centers of the Eves are symmetrical with respect to the x-axis, and Q_2 is bigger than Q_1. So all the stable points of source UAVs are above the x-axis to avoid wiretapping, and the stable point of the UAV friendly jammers are below the x-axis to suppress the Eves' channel more effectively.

For case 2, Fig. 3 shows the trajectories of both UAVs for different schemes in different period T. The D and Eves are marked with $\circ$ and $\times$, respectively. The gray dotted circles represent the eavesdropper uncertain region. When the flying time T is larger than the minimum flying time ($T = 40$ s) and not sufficient for UAVs to fly to the stable point, i.e. $T = 45$ s, both source UAV and jammer UAV fly in a compromise arc path to the final location non-stop. When given sufficient time, i.e. $T = 120$ s, the stable point will appear for both source UAV and jammer UAV. In the first stage, in both E-CSI/&J and P-CSI/&J schemes, the trajectories of source UAVs are more closed to the destination in comparison with the P-CSI/NJ scheme. A closer trajectory to the destination can obtain a better legitimate channel and achieve a higher rate for the destination. While, in the third stage, the opposite situation occurs. It is because that P-CSI/NJ turns off its power ($\boldsymbol{P}_S = 0$) most of the third stage. Note that once the distance of J-to-E is greater than that of J-to-D, the jamming signal will compromise the main channel more. Therefore, the jammer UAV keeps silent during the first few time slots. With the decrease of the J-to-E, the jammer UAV gradually increases its transmit power. The jammer UAV transmits jamming signals with the full power at the hovering point near the eavesdroppers. When the jammer UAV flies towards its final location, it turns off its transmit power gradually. With the help of jammer, our proposed P-CSI/&J scheme can



(a) Numerical secrecy rate versus P_{max} when $T = 120s$.

(b) Numerical secrecy rate versus P_{max} when $T = 60s$.

FIGURE 5. Numerical secrecy rate performance versus P_{max}.

enhance the average secrecy rate of the system in a large degree in comparison with P-CSI/NJ scheme. In the next section, we will verify the secrecy rate performance on the quantitative aspect.

B. SECRECY RATE PERFORMANCE FOR THE THREE SCHEMES

In this section, we verify the secrecy rate performances for the three schemes. The configuration is the same as case 2 except for a variational flying period T and a UAV maximum output power P_{max} in this section. Fig. 4 demonstrates the average secrecy rate versus the different flight duration T for different schemes. In the figure, it can be observed that the secrecy rates of all schemes increase with T. There is a relatively stable performance gap between E-CSI/&J and P-CSI/&J. The performance gap between them represents the gap between our proposed solution and the real solution. The P-CSI/&J scheme significantly outperforms the significantly outperformP-CSI/NJ scheme. From Fig. 4 (b) we can also see that, with the decrease of the eavesdropper uncertain region, the secrecy rate performances of both the P-CSI/&J scheme and P-CSI/NJ scheme increase, and the secrecy rate gap between the E-CSI/&J scheme and the P-CSI/&J scheme becomes smaller. It is because when the uncertainty of the eavesdropper reduces, the jammer "knows" more precise location information of the eavesdroppers. On the contrary, the E-CSI/&J scheme exhibits very similar performance under the two circumstances, as it knows the accurate locations of the Eves.

Fig. 5 demonstrates the average secrecy rate performance versus different maximum power P_{max} for different schemes. With the help of UAV friendly jammer, P-CSI/&J scheme significantly outperforms the P-CSI/NJ scheme. As we set a relatively small eavesdropper uncertain region, there exists a relative small performance gap between the E-CSI/&J scheme and the P-CSI/&J scheme, which has been demonstrated in Fig. 4. The above results demonstrate that, with the help of UAV friendly jammer, our proposed P-CSI/&J scheme can bring great performance gain to the achievable WCSR in comparison with P-CSI/NJ scheme.

V. CONCLUSIONS

In this paper, we have investigated the PLS issue in UAV networks with multiple location-unknown eavesdroppers. Specifically, the flying trajectories and transmit power for both UAVs have been jointly optimized by maximizing the WCSR of the system. To solve the formulated non-convex optimization problem, a block coordinate descent based iterative optimization method has been proposed. Simulation results demonstrate that, with the help of jammer UAV, our proposed scheme exhibits more preferable flying trajectories for both UAVs, and can significantly improve the average WCSR of the system, in comparison with the strategy without a jammer UAV.

ACKNOWLEDGMENT

This paper was presented at the IEEE Global Communications Conference in 2019.

REFERENCES

[1] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[2] J.-J. Wang, C.-X. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 73–82, Sep. 2017.

[3] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3949–3963, Jun. 2016.

[4] X. Lin, V. Yajnanarayana, S. D. Muruganathan, S. Gao, H. Asplund, H.-L. Maattanen, M. Bergstrom, S. Euler, and Y.-P. E. Wang, "The sky is not the limit: LTE for unmanned aerial vehicles," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 204–210, Apr. 2018.

[5] *Facebook Takes Flight*. Accessed: Apr. 10, 2017. [Online]. Available: http://www.theverge.com/a/mark-zuckerberg-future-of-facebook/aquiladrone-internet

[6] T. A. Johansen, A. Zolich, T. Hansen, and A. J. Sørensen, "Unmanned aerial vehicle as communication relay for autonomous underwater vehicle—Field tests," in *Proc. IEEE Global Workshops*, Austin, TX, USA, Dec. 2014, pp. 1469–1474.

[7] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[8] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Efficient deployment of multiple unmanned aerial vehicles for optimal wireless coverage," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1647–1650, Aug. 2016.

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

[10] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Energy-efficient resource allocation for secure UAV communication systems," 2019, *arXiv:1901.09308*. [Online]. Available: https://arxiv.org/abs/1901.09308

[11] S. Jeong, O. Simeone, and J. Kang, "Mobile edge computing via a UAV-mounted cloudlet: Optimization of bit allocation and path planning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2049–2063, Mar. 2018.

[12] P. Zhan, K. Yu, and A. L. Swindlehurst, "Wireless relay communications with unmanned aerial vehicles: Performance and optimization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 3, pp. 2068–2085, Jul. 2011.

[13] Y. Sun, D. Xu, D. W. K. Ng, L. Dai, and R. Schober, "Optimal 3D-trajectory design and resource allocation for solar-powered UAV communication systems," 2018, *arXiv:1808.00101*. [Online]. Available: https://arxiv.org/abs/1808.00101

[14] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[15] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[16] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[17] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[18] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[19] N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2281–2294, May 2018.

[20] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmWave networks using Matérn hardcore point processes," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[21] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[22] Q. Wang, Z. Chen, H. Li, and S. Li, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," *IEEE Access*, vol. 6, pp. 62849–62855, 2018.

[23] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280–11284, Nov. 2018.

[24] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Commun.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.

[25] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Jan. 2019.

[26] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–6.

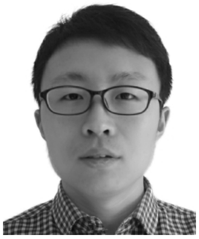
[27] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Sep. 2018.

[28] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[29] Z. Zhu, Z. Chu, N. Wang, S. Huang, Z. Wang, and I. Lee, "Beamforming and power splitting designs for AN-aided secure multi-user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[30] C. J. Li and H. Ling, "Synthetic aperture radar imaging using a small consumer drone," in *Proc. IEEE Int. Symp. Antennas Propag. USNC/URSI Nat. Radio Sci. Meeting*, Vancouver, BC, Canada, Jul. 2015, pp. 685–686.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



YUPENG LI received the B.S. degree from the Hebei University of Science and Technology in 2013 and the M.S. degree (Hons.) from Harbin Engineering University in 2016. He is currently pursuing the Ph.D. degree in information and communication engineering with the Beijing University of Posts and Telecommunications. From 2018 to 2019, he was a Visiting Ph.D. Student with Colorado State University, Fort Collins, CO, USA. His current research interests include machine learning, signal processing, physical layer security, and mobile communication.

RONGQING ZHANG (S'11–M'15) received the B.S. and Ph.D. degrees (Hons.) from Peking University, Beijing, China, in 2009 and 2014, respectively.

From 2014 to 2018, he was a Postdoctoral Research Fellow with Colorado State University, CO, USA. Since 2019, he has been an Associate Professor with Tongji University, Shanghai, China. He has authored or coauthored two books, two book chapters, and over 80 papers in refereed journals and conference proceedings. His current research interests include physical-layer security, vehicular communications and networking, UAV communications, and autonomous driving. He was a recipient of the Academic Award for Excellent Doctoral Students, Ministry of Education of China, was a co-recipient of the First-Class Natural Science Award, Ministry of Education of China, and received the Best Paper Awards at the IEEE ITST'12, ICC'16, and GLOBECOM'18, and ICC'19. He was also awarded as an International Presidential Fellow of Colorado State University, in 2017. He is currently serving as an Associate Editor for the *IET Communications* and Hindawi *Complexity*.

JIANHUA ZHANG received the Ph.D. degree in circuit and system from the Beijing University of Posts and Telecommunications (BUPT), in 2003, where she is currently a Professor of BUPT. She was the Drafting Group (DG) Chairwoman of the ITU-R IMT-2020 channel model. She has published more than 100 articles in refereed journals and conferences and holds 40 patents. Her current research interests include 5G, artificial intelligence, and data mining, especially in 3D MIMO and channel modeling. She received the 2008 Best Paper Award from the *Journal of Communication and Network*. In 2007 and 2013, she received two national novelty awards for her contribution to the research and development of Beyond 3G TDD demo system with 100Mbps@20MHz and 1Gbps@100MHz, respectively. In 2009, she received the Second Prize for Science Novelty from the Chinese Communication Standards Association for her contributions to ITU-R 4G (ITU-T M.2135) and 3GPP Relay channel model (3GPP 36.814). From 2012 to 2014, she did the 3D channel modeling work and contributed to 3GPP 36.873 and is also a member of 3GPP 5G channel model for bands up to 100 GHz.

SHIJIAN GAO received the B.Sc. degree in electrical engineering from Nankai University, in 2014, and the M.Sc. degree in electrical engineering from Peking University, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Colorado State University, Fort Collins, CO, USA. His research interests include wireless communications and related fields.

LIUQING YANG (S'02–M'04–SM'06–F'15) received the Ph.D. degree from the University of Minnesota, Minneapolis, MN, USA, in 2004. Her current research interests include communications and signal processing. She was a recipient of the Office of Naval Research Young Investigator Program Award, in 2007, the National Science Foundation Career Award, in 2009, the IEEE GLOBECOM Outstanding Service Award, in 2010, the George T. Abell Outstanding Mid-Career Faculty Award, the Art Corey Outstanding International Contributions Award at CSU, in 2012 and 2016, respectively, and the Best Paper Award of the IEEE ICUWB06, ICCC13, ITSC14, GLOBECOM14, ICC16, WCSP16, and GLOBECOM18. She has been actively serving within the technical community, including the organization of many IEEE international conferences, and on the Editorial Boards of a number of journals, including the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING.