UAV-Enabled Secure Communications: Joint Trajectory and Transmit Power Optimization

Xiaobo Zhou, Qingqing Wu, *Member, IEEE*, Shihao Yan, *Member, IEEE*, Feng Shu, *Member, IEEE*, and Jun Li, *Senior Member, IEEE*

***Abstract*—This paper studies the physical layer security of an unmanned aerial vehicle (UAV) network, where a UAV base station (UAV-B) transmits confidential information to multiple information receivers (IRs) with the aid of a UAV jammer (UAV-J) in the presence of multiple eavesdroppers. We formulate an optimization problem to jointly design the trajectories and transmit power of UAV-B and UAV-J in order to maximize the minimum average secrecy rate over all IRs. The optimization problem is non-convex and the optimization variables are coupled, which leads to the optimization problem being mathematically intractable. As such, we decompose the optimization problem into two subproblems and then solve it by employing an alternating iterative algorithm and the successive convex approximation technique. Our results show that the average secrecy rate performance of the proposed scheme provides about 20% and 150% performance gains over the joint trajectory and transmit power optimization without UAV-J scheme and the transmit power optimization with fixed trajectory scheme at flight period $T = 150$ s, respectively.**

***Index Terms*—UAV networks, physical layer security, artificial noise, trajectory optimization, transmit power optimization.**

I. Introduction

Unmanned aerial vehicle (UAV) networks are of great practical significance due to their tremendous application scenarios, particularly for the information technological community [1]–[6]. Although an increasing amount of research effort has been devoted to UAV networks, the security issue of UAV networks has not been fully addressed, while these issues are critical in UAV networks and secure communications over UAV networks are of an ever-increasing demand. This is mainly due to the fact that information can be easily intercepted by unauthorized receivers in wireless communications due to the inherent broadcast nature of the wireless medium. The traditional encryption technique can be used to partially address the security issues of UAV networks. However, the security of a cryptographic approach would be significantly limited, if an efficient method of solving its underlying hard mathematical problem was found. Against this background, physical layer security becomes a desirable candidate to address the security issues in UAV networks, since it does not require encryption keys and the security is fundamentally achieved by transmission design (e.g., [7]–[9]).

To exploit the potential of UAVs, a joint user scheduling and association, power control, and trajectory optimization framework was proposed in [10] for a general multi-UAV network. Then, three fundamentals tradeoffs in the communication and UAV trajectory design were proposed in [1]. However, the physical layer security is completely ignored in [1], [10]. Until now, there are only few works on this topic in the literature. For example, the authors of [11] considered improving physical layer security using UAV-enabled mobile relaying, in which a UAV serves as a mobile relay and adaptively adjusts its location in order to enhance the focused wireless communication security. In [12], the authors showed that a UAV as a mobile base station (BS) can improve the achieved secrecy rate by optimizing its flight trajectory to enhance the quality of the channel from the UAV to an information receiver (IR) and to deteriorate the quality of the eavesdropping channel. Using a UAV as a mobile jammer to transmit artificial noise (AN) signals to prevent an eavesdropper from eavesdropping on the confidential information was considered in [13], where a source, a destination, and the eavesdropper (Eve) are located on the ground, and the secrecy rate is improved by jointly optimizing the mobile jammer's trajectory and transmit power. A similar system model as [13] was also considered in [14], in which the authors focused on the secrecy outage probability and jamming coverage to demonstrate the effectiveness of using a UAV as a mobile jammer in enhancing physical layer security.

The aforementioned works only considered the scenarios where a UAV is solely used as a mobile BS/jammer [10], [12], [13], in which a high-level physical layer security may not be achievable. For example, when there are multiple IRs and multiple Eves on the ground, if we only optimize the trajectory and transmit power of a UAV BS (UAV-B), a non-trivial secrecy rate may not be guaranteed. This is because it is generally difficult for the UAV-B to keep far from all the Eves when it transmits confidential information to each IR. For this scenario, a UAV jammer (UAV-J) is highly appealing for more secured transmission. Motivated by this, we consider the physical layer security of a UAV network, where a UAV-B transmits confidential information to multiple IRs with the aid of a UAV-J in the presence of multiple Eves. We jointly optimize the trajectories and the transmit power of the UAV-B and UAV-J to enhance the considered physical layer security, subject to the mobility and power constraints. The resultant optimization problem is non-convex and difficult to tackle directly. Thus, we decompose it into two subproblems and then solve it by employing an alternating iterative algorithm and the successive convex approximation (SCA) technique. Our simulation results show that introducing UAV-J allows UAV-B to fly closer to the Eves, which enables UAV-B to have high flexibility to choose the trajectory and enjoy better air-to-ground channel conditions, thus achieving an improved average secrecy rate.

II. System Model

A. Considered Scenario and Adopted Assumptions

As shown in Fig. 1, we consider a physical layer security system in the UAV-aided networks, where M IRs and K Eves are located

Manuscript received December 1, 2018; accepted February 2, 2019. Date of publication February 18, 2019; date of current version April 16, 2019. This work was supported by National Natural Science Foundation of China under Grants 61727802, 61771244, and 61872184. The review of this paper was coordinated by Dr. M. Elkashlan. *(Corresponding author: Feng Shu.)*

X. Zhou is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China, and also with the School of Fuyang Normal University, Fuyang 236037, China (e-mail: zxb@njust.edu.cn).

Q. Wu is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: elewuqq@nus.edu.sg).

S. Yan is with the School of Engineering, Macquarie University, Sydney, NSW 2109, Australia (e-mail: shihao.yan@mq.edu.au).

F. Shu and J. Li are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: shufeng0101@163.com; jun.li@njust.edu.cn).

Digital Object Identifier 10.1109/TVT.2019.2900157

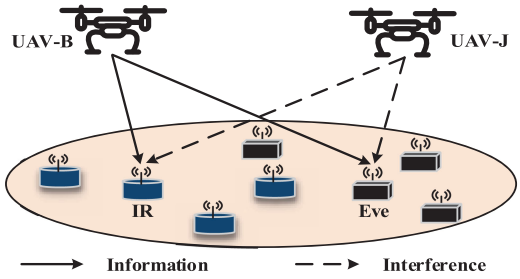


Fig. 1. An illustration of UAV-aided physical layer security system.

on the ground, a UAV-B (B) is employed to transmit the confidential messages to M IRs, and a UAV-J (J) generates AN to interfere with K Eves to prevent them from intercepting confidential messages that the UAV-B sends to IRs. To enable UAV-B to serve multiple ground IRs simultaneously, frequency division multiple access (FDMA) is considered. We assume that each IR is allocated with equal bandwidth, and it is normalized to 1. The proposed algorithm can be readily extended to the case of time division multiple access (TDMA). To ensure the security of the downlink communications, we consider the worst case, i.e., each Eve can wiretap all IRs. Therefore, UAV-J needs to have the ability to interfere with each IR's operating frequency band. For convenience, we define $m \in \mathcal{M} \triangleq \{1, 2, \ldots, M\}$, $k \in \mathcal{K} \triangleq \{1, 2, \ldots, K\}$, $s \in \mathcal{S} \triangleq \{B, J\}$, and $u \in \mathcal{U} \triangleq \{I_1, \ldots, I_M, E_1, \ldots, E_K\}$, where I_m and E_k denote m-th IR and k-th Eve, respectively. Without loss of generality, we consider a three-dimensional Cartesian coordinate system, where the horizontal coordinates of m-th IR and the k-th Eve are $\mathbf{q}_{I_m} = [x_{I_m}, y_{I_m}]^T$ and $\mathbf{q}_{E_k} = [x_{E_k}, y_{E_k}]^T$, respectively.

At time instant t, the horizontal coordinate of UAV s is denoted by $\mathbf{q}_s(t) \triangleq [x_s(t), y_s(t)]^T$. We note that the continuous time t implies an infinite number of speed constraints, which makes the trajectory design of the UAV s very difficult to tackle. As such, in this work, we set the flight period of UAV s to T seconds and divide it into N sufficiently small and equal-length time slots ($\delta_t = \frac{T}{N}$) such that the location of UAV s is considered to be approximately unchanged within each time slot. Consequently, the trajectory of UAV s over the period T can be approximated by the N-point sequences $\mathbf{q}_s[n] = [x_s[n], y_s[n]]^T$, $n \in \mathcal{N} \triangleq \{1, \ldots, N\}$. In addition, the UAV s is assumed to fly at a fixed altitude H, which can be considered as the minimum altitude to avoid collision with ground obstacles. Let $V_{\max}$ denote the maximum flying speed of UAV s, then its maximum flying distance is $L = V_{\max}\delta_t$ in each time slot. In addition, the UAV s should return to the initial location at the last time slot [10]. According to the above description, we express the mobility constraints of UAV s as

$$\|\mathbf{q}_s[n+1] - \mathbf{q}_s[n]\|^2 \le L^2, \forall s, n \in \mathcal{N} \setminus \{N\}, \tag{1a}$$

$$\mathbf{q}_s[1] = \mathbf{q}_s[N], \forall s. \tag{1b}$$

To avoid collision between the UAV-B and UAV-J, we impose the following minimum security distance constraint:

$$\|\mathbf{q}_B[n] - \mathbf{q}_J[n]\|^2 \ge d_{\min}^2, \forall n, \tag{2}$$

where $d_{\min}$ denotes the minimum distance between UAV-B and UAV-J. It is assumed that the channels from UAV s to the ground nodes are all dominated by line-of-sight (LoS) links [10]. At time slot n, the channel power gain from UAV s to ground node u follows the free-space path loss model, which is given by

$$h_{su}[n] = \beta_0 d_{su}^{-2}[n] = \frac{\beta_0}{\|\mathbf{q}_s[n] - \mathbf{q}_u\|^2 + H^2}, \forall s, u, n, \tag{3}$$

where β_0 denotes the channel power gain at the reference distance $d_0 = 1\,\mathrm{m}$, d_{su} denotes the distance from UAV s to ground node u. Compared with the fading channels on the ground, the channel power gain between UAV-J and Eves is easier to obtain because it only depends on the distance between them, and the Eve's location can be detected by a camera or radar mounted on the UAV-J.

Let $P_B^m[n]$ denote the transmit power corresponding to the confidential messages sent by the UAV-B to the m-th IR at the n-th time slot, and $P_J[n]$ denote the transmit power of the UAV-J at the n-th time slot, which satisfy the following peak power constraints:

$$P_B^m[n] \ge 0, \sum_{m=1}^{M} P_B^m[n] \le P_{B,\max}, 0 \le P_J[n] \le P_{J,\max}, \tag{4}$$

for $\forall m, n$, where $P_{B,\max}$ and $P_{J,\max}$ denote the peak transmit power of the UAV-B and UAV-J, respectively.

B. Performance Metric

The achievable rate of m-th IR in bits/second/Hertz (bps/Hz) at time slot n is given by

$$R_{I_m}[n] = \log_2\left(1 + \frac{P_B^m[n]\hat{h}_{BI_m}[n]}{\hat{P}_J[n]\hat{h}_{JI_m}[n] + 1}\right), \forall m, n, \tag{5}$$

and the achievable rate of k-th Eve wiretapping the m-th IR in bps/Hz at time slot n is given by

$$R_{E_k}^m[n] = \log_2\left(1 + \frac{P_B^m[n]\hat{h}_{BE_k}[n]}{\hat{P}_J[n]\hat{h}_{JE_k}[n] + 1}\right), \forall k, m, n, \tag{6}$$

where $\hat{h}_{su}[n] = \frac{\gamma_0}{\|\mathbf{q}_s[n] - \mathbf{q}_u\|^2 + H^2}, \forall s, u, n$, $\gamma_0 = \frac{\beta_0}{\sigma^2}$, $\hat{P}_J[n] = \frac{P_J[n]}{M}$, and σ^2 denotes the power of the additive white Gaussian noise (AWGN) at the m-th IR and k-th Eve. The average secrecy rate for m-th IR in bps/Hz over N time slots can be expressed as

$$R_{sec}^m = \frac{1}{N}\sum_{n=1}^{N}\left[R_{I_m}[n] - \max_k R_{E_k}^m[n]\right]^+, \forall k, m, \tag{7}$$

where $[x]^+ \triangleq \max(x, 0)$.

III. Optimization Problem Formulation

For ease of presentation, we define $\mathbf{Q}_s = \{\mathbf{q}_s[n], \forall s, n\}$ and $\mathbf{P}_s = \{P_B^m[n], P_J[n], \forall m, n\}$. Our objective is to maximize the minimum average secrecy rate among M IRs by jointly designing the UAV trajectory and the transmit power subject to the mobility constraints and power constraints of UAV s. The optimization problem can be formulated as

$$(\mathrm{P1}): \max_{\mathbf{Q}_s, \mathbf{P}_s} \min_m \sum_{n=1}^{N}\left[R_{I_m}[n] - \max_k R_{E_k}^m[n]\right] \tag{8a}$$

$$\text{s.t. } (1), (2), (4), \tag{8b}$$

where $\frac{1}{N}$ is omitted in (8a). In addition, we omit the operation $[\cdot]^+$ in (8a), because if the n-th summation term in the objective function is less than 0, we can set $P_B^m[n] = 0$. We observe that both the numerator and the denominator of the fractions in $R_{I_m}[n]$ and $R_{E_k}^m[n]$ have trajectory and transmit power optimization variables, while optimization variables in [12] or [13] exist only in the numerator or denominator of the fraction in the logarithmic function, which makes our problem (P1) more difficult to tackle. Moreover, we consider multiple IRs and

multiple Eves, while [12], [13] only consider one IR and one Eve, which are essentially special cases of our proposed general optimization framework. As such, problem (P1) is significantly different from the problems in [12], [13].

The optimization problem (P1) has a non-concave objective function in (8a) and a non-convex constraint in (8b), thus (P1) is difficult to solve directly. To facilitate solving this problem, we introduce slack variables η, $x_m[n]$, $y_m[n]$, $z_k^m[n]$, $v_k[n]$, $w_m[n]$, and then transform it into a more tractable form, i.e.,

$$(\text{P2}): \max_{\eta,\mathbf{P}_s,\mathbf{Q}_s,\mathbf{W}_m,\mathbf{X}_m,\mathbf{Y}_m,\mathbf{Z}_k^m,\mathbf{V}_k} \eta \tag{9a}$$

$$\text{s.t.} \sum_{n=1}^{N}\left[\frac{1}{\ln 2}(x_m[n]-y_m[n])-w_m[n]\right]\geq \eta, \forall m, \tag{9b}$$

$$z_k^m[n]-v_k[n]\leq w_m[n]\ln 2, \forall m,k,n, \tag{9c}$$

$$P_B^m[n]\hat{h}_{BI_m}[n]+\hat{P}_J[n]\hat{h}_{JI_m}[n]+1\geq e^{x_m[n]}, \forall m,n, \tag{9d}$$

$$\hat{P}_J[n]\hat{h}_{JI_m}[n]+1\leq e^{y_m[n]}, \forall m,n, \tag{9e}$$

$$P_B^m[n]\hat{h}_{BE_k}[n]+\hat{P}_J[n]\hat{h}_{JE_k}[n]+1\leq e^{z_k^m[n]}, \forall k,n, \tag{9f}$$

$$\hat{P}_J[n]\hat{h}_{JE_k}[n]+1\geq e^{v_k[n]}, \forall k,n, \tag{9g}$$

$$(1),(2),(4), \tag{9h}$$

where $\mathbf{X}_m=\{x_m[n],\forall m,n\}$, $\mathbf{Y}_m=\{y_m[n],\forall m,n\}$, $\mathbf{Z}_k^m=\{z_k^m[n],\forall m,k,n\}$, and $\mathbf{V}_k=\{v_k[n],\forall k,n\}$, $\mathbf{W}_m=\{w_m[n],\forall m,n\}$. Note that (P2) is still a non-convex optimization problem. In Section IV, we propose an efficient algorithm for solving problem (P2).

IV. Transmit Power and Trajectory Optimization

In this section, we decompose the problem (P2) into two subproblems, and then solve the two subproblems alternately until the algorithm converges.

A. Subproblem 1: Transmit Power Optimization

First, we optimize the transmit power $\mathbf{P}_s$ of UAV s by fixing the trajectory variable $\mathbf{Q}_s$. Given $\mathbf{Q}_s$, (P2) can be equivalently rewritten as

$$(\text{P3}): \max_{\eta,\mathbf{P}_s,\mathbf{W}_m,\mathbf{X}_m,\mathbf{Y}_m,\mathbf{Z}_k^m,\mathbf{V}_k} \eta$$
$$\text{s.t. (9b), (9c), (9d), (9e), (9f), (9g), (4).} \tag{10}$$

Note that although (9e) and (9f) are still non-convex constraints, they are both in the forms of the difference of two convex functions, which allows us to employ the SCA technique for solving the problem (P3). To this end, the first-order Taylor approximation is applied to construct the lower bounder of $e^{y_m[n]}$ and $e^{z_k^m[n]}$. Therefore, for a given feasible point $(\tilde{y}_m[n],\tilde{z}_k^m[n])$, (9e) and (9f) can be transformed to

$$\hat{P}_J[n]\hat{h}_{JI_m}[n]+1\leq e^{\tilde{y}_m[n]}(y_m[n]-\tilde{y}_m[n]+1), \tag{11}$$

for $\forall m,n$, and

$$P_B^m[n]\hat{h}_{BE_k}[n]+\hat{P}_J[n]\hat{h}_{JE_k}[n]+1\leq e^{\tilde{z}_k^m[n]}\times(z_k^m[n]-\tilde{z}_k^m[n]+1), \forall m,k,n, \tag{12}$$

respectively. The optimization problem that approximates the original optimization problem (P3) can be formulated as

$$(\text{P4}): \max_{\eta,\mathbf{P}_s,\mathbf{W}_m,\mathbf{X}_m,\mathbf{Y}_m,\mathbf{Z}_k^m,\mathbf{V}_k} \eta$$
$$\text{s.t. (9b), (9c), (9d), (11), (12), (9g), (4).} \tag{13}$$

For given $(\tilde{y}_m[n],\tilde{z}_k^m[n])$, (P4) is a convex optimization problem, which can be efficiently solved by convex optimization tools such as CVX [15]. The original problem (P3) can be solved by solving (P4) iteratively. At each iteration, the current optimal solution gradually approaches the optimal solution to (P3). Furthermore, the iteration will eventually converges to a point that satisfies the Karush-Kuhn-Tucker (KKT) optimality conditions of the original problem (P3) [16].

B. Subproblem 2: Trajectory Optimization

Second, we optimize the trajectory $\mathbf{Q}_s$ of UAV s by fixing the transmit power $\mathbf{P}_s$. Given $\mathbf{P}_s$, (P2) can be equivalently rewritten as

$$(\text{P5}): \max_{\eta,\mathbf{W}_m,\mathbf{Q}_s,\mathbf{X}_m,\mathbf{Y}_m,\mathbf{Z}_k^m,\mathbf{V}_k} \eta$$
$$\text{s.t. (9b), (9c), (9d), (9e), (9f), (9g), (1), (2).} \tag{14}$$

Problem (P5) is a non-convex optimization problem due to the non-convex constraints (9d), (9e), (9f), (9g), and (2).

To transform the non-convex constraints into convex constraints, we define $f_{A,B,\mathbf{a}}(\mathbf{x})\triangleq\frac{A}{\|\mathbf{x}-\mathbf{a}\|^2+B^2}$. It can be seen that $f_{A,B,\mathbf{a}}(\mathbf{x})$ is convex with respect to $\|\mathbf{x}-\mathbf{a}\|^2$. Thus, the first-order Taylor expansion of $f_{A,B,\mathbf{a}}(\mathbf{x})$ at point $\tilde{\mathbf{x}}$ is given by $f_{A,B,\mathbf{a}}(\mathbf{x})\geq\mathcal{F}_{A,B,\mathbf{a}}(\mathbf{x},\tilde{\mathbf{x}})=\frac{2A}{\|\tilde{\mathbf{x}}-\mathbf{a}\|^2+B^2}-\frac{A(\|\mathbf{x}-\mathbf{a}\|^2+B^2)}{(\|\tilde{\mathbf{x}}-\mathbf{a}\|^2+B^2)^2}$, where the inequality is due to the convexity of the function $f_{A,B,\mathbf{a}}(\mathbf{x})$ (convex with respect to $\|\mathbf{x}-\mathbf{a}\|^2$). Note that $\mathcal{F}_{A,B,\mathbf{a}}(\mathbf{x},\tilde{\mathbf{x}})$ is a concave function with respect to $\mathbf{x}$. Therefore, the constraints (9d) and (9g) can be transformed to

$$\gamma_0\mathcal{F}_{P_B^m[n],H,\mathbf{q}_{I_m}}(\mathbf{q}_B[n],\tilde{\mathbf{q}}_B[n])+$$
$$\gamma_0\mathcal{F}_{\hat{P}_J[n],H,\mathbf{q}_{I_m}}(\mathbf{q}_J[n],\tilde{\mathbf{q}}_J[n])+1\geq e^{x_m[n]}, \forall m,n, \tag{15a}$$

$$\gamma_0\mathcal{F}_{\hat{P}_J[n],H,\mathbf{q}_{E_k}}(\mathbf{q}_J[n],\tilde{\mathbf{q}}_J[n])+1\geq e^{v_k[n]}, \forall k,n, \tag{15b}$$

which are convex with respect to the optimization variables. To facilitate processing the non-convex constraints (9e) and (9f), we introduce slack variables $a_m[n]$, $b_k[n]$ and $c_k[n]$, and then rewrite (9e) and (9f) as

$$\frac{\gamma_0\hat{P}_J[n]}{a_m[n]}+1\leq e^{y_m[n]}, \forall m,n, \tag{16a}$$

$$\|\mathbf{q}_J[n]-\mathbf{q}_{I_m}\|^2+H^2\geq a_m[n], \tag{16b}$$

and

$$\frac{\gamma_0P_B^m[n]}{b_k[n]}+\frac{\gamma_0\hat{P}_J[n]}{c_k[n]}+1\leq e^{z_k^m[n]}, \forall m,k,n, \tag{17a}$$

$$\|\mathbf{q}_B[n]-\mathbf{q}_{E_k}\|^2+H^2\geq b_k[n], \forall k,n, \tag{17b}$$

$$\|\mathbf{q}_J[n]-\mathbf{q}_{E_k}\|^2+H^2\geq c_k[n], \forall k,n, \tag{17c}$$

respectively. It can be observed that (16a) and (17a) are in the forms of the difference of two convex functions, which can be transformed into

the following inequalities

$$\frac{\gamma_0 \hat{P}_J[n]}{a_m[n]} + 1 \le e^{\tilde{y}_m[n]}(y_m[n] - \tilde{y}_m[n] + 1), \forall m, n, \tag{18a}$$

$$\frac{\gamma_0 P_B^m[n]}{b_k[n]} + \frac{\gamma_0 \hat{P}_J[n]}{c_k[n]} + 1 \le e^{\tilde{z}_k^m[n]} \times (z_k^m[n] - \tilde{z}_k^m[n] + 1), \forall m, k, n. \tag{18b}$$

For the non-convex constraints (16b), (17b), (17c), and the minimum security distance constraint (2), we can find that they are all in the forms of the superlevel set of convex quadratic functions. Thus, we can obtian the following inequalities by performing the first-order Taylor expansion at $\tilde{\mathbf{q}}_B[n]$ and $\tilde{\mathbf{q}}_J[n]$,

$$\|\mathbf{q}_J[n] - \mathbf{q}_{I_m}\|^2 \ge \|\tilde{\mathbf{q}}_J[n] - \mathbf{q}_{I_m}\|^2 + 2(\tilde{\mathbf{q}}_J[n] - \mathbf{q}_I)^T(\mathbf{q}_J[n] - \tilde{\mathbf{q}}_J[n]) \triangleq \rho_m[n], \forall m, n, \tag{19a}$$

$$\|\mathbf{q}_B[n] - \mathbf{q}_{E_k}\|^2 \ge \|\tilde{\mathbf{q}}_B[n] - \mathbf{q}_{E_k}\|^2 + 2(\tilde{\mathbf{q}}_B[n] - \mathbf{q}_{E_k})^T(\mathbf{q}_B[n] - \tilde{\mathbf{q}}_B[n]) \triangleq \lambda_k[n], \forall k, n, \tag{19b}$$

$$\|\mathbf{q}_J[n] - \mathbf{q}_{E_k}\|^2 \ge \|\tilde{\mathbf{q}}_J[n] - \mathbf{q}_{E_k}\|^2 + 2(\tilde{\mathbf{q}}_J[n] - \mathbf{q}_{E_k})^T(\mathbf{q}_J[n] - \tilde{\mathbf{q}}_J[n]) \triangleq \tau_k[n], \forall k, n, \tag{19c}$$

$$\|\mathbf{q}_B[n] - \mathbf{q}_J[n]\|^2 \ge -\|\tilde{\mathbf{q}}_B[n] - \tilde{\mathbf{q}}_J[n]\|^2 + 2(\tilde{\mathbf{q}}_B[n] - \tilde{\mathbf{q}}_J[n])^T(\mathbf{q}_B[n] - \mathbf{q}_J[n]) \triangleq \varrho[n], \forall n. \tag{19d}$$

According to the above transformation, the original problem (P5) can be approximated as

$$(\text{P6}): \max_{\eta, \mathbf{Q}_s, \mathbf{W}_m, \mathbf{X}_m, \mathbf{Y}_m, \mathbf{Z}_k^m, \mathbf{V}_k, \mathbf{A}_m, \mathbf{B}_k, \mathbf{C}_k} \eta$$

$$\text{s.t. } (9b), (9c), (15), (18), (1)$$

$$\rho_m[n] + H^2 \ge a_m[n], \lambda_k[n] + H^2 \ge b_k[n],$$

$$\tau_k[n] + H^2 \ge c_k[n], \varrho[n] \ge d_{\min}^2, \forall m, k, n, \tag{20}$$

where $\mathbf{A}_m = \{a_m[n], \forall n\}$, $\mathbf{B}_k = \{b_k[n], \forall n\}$, and $\mathbf{C}_k = \{c_k[n], \forall n\}$. Note that problem (P6) is a convex optimization problem, which can be efficiently solved by convex optimization solvers such as CVX [15]. Similar to Section IV-A, the original problem (P5) can be solved by iteratively optimizing (P6) until achieving the convergence.

C. Overall Algorithm

Based on the results in the previous two subsections, we apply an alternating optimization algorithm to solve the original optimization problem (P2), for which the details are summarized in Algorithm 1. The convergence of Algorithm 1 has been proved in [10] and thus it is omitted here for brevity.

Algorithm 1: Alternating Optimization Algorithm for (P2).

Initialize: $(\mathbf{Q}_B^0, \mathbf{Q}_J^0, \{\mathbf{Z}_k^m\}^0, \mathbf{Y}_m^0)$; $i = 0$.

repeat

1. Given feasible solution $(\mathbf{Q}_B^i, \mathbf{Q}_J^i, \{\mathbf{Z}_k^m\}^i, \mathbf{Y}_m^i)$, solve problem (P4) and obtain the current optimal solution $(\mathbf{P}_B^{i+1}, \mathbf{P}_J^{i+1}, \{\mathbf{Z}_k^m\}^{i+1}, \mathbf{Y}_m^{i+1})$.
2. Update $(\{\mathbf{Z}_k^m\}^i, \mathbf{Y}_m^i) = (\{\mathbf{Z}_k^m\}^{i+1}, \mathbf{Y}_m^{i+1})$
3. Given $(\mathbf{P}_B^{i+1}, \mathbf{P}_J^{i+1}, \{\mathbf{Z}_k^m\}^i, \mathbf{Y}_m^i)$, solve problem (P6) and obtain $(\mathbf{Q}_B^{i+1}, \mathbf{Q}_J^{i+1}, \{\mathbf{Z}_k^m\}^{i+1}, \mathbf{Y}_m^{i+1})$; $i = i + 1$.

until Converges to a prescribed accuracy.

V. Numerical Results

In this section, we present numerical results to demonstrate the secrecy performance improvement achieved by our joint trajectory and transmit power optimization algorithm. The required system parameters are set as follows: $M = 4$, $K = 4$, $V_{\max} = 40$ m/s, $P_{B,\max} = 4$ W, $P_{J,\max} = 4$ W, $\gamma_0 = 10^6$, $H = 50$ m, and $d_{\min} = 5$ m. To demonstrate the effectiveness of the proposed algorithm, we consider the following two benchmark schemes:

- **BMS1**-Joint trajectory and transmit power optimization without UAV-J: In the absence of UAV-J, we jointly optimize the trajectory and transmit power of UAV-B.

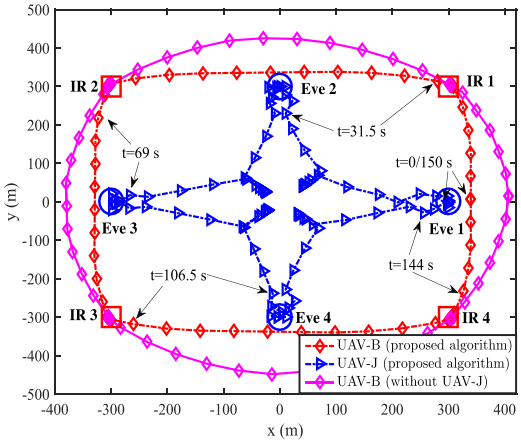
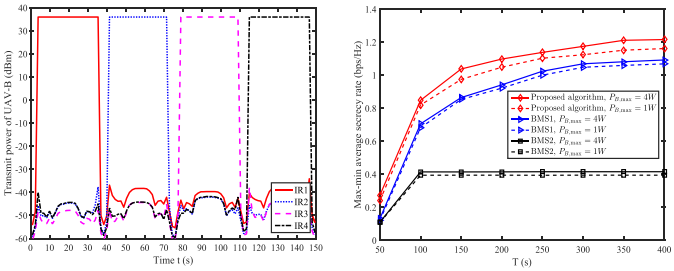


Fig. 2. The trajectories of UAV-B and UAV-J for $T = 150\,s$.

- **BMS2**-Circular trajectory with optimized transmit power: UAV-B and UAV-J are flying on their circular trajectories, respectively. The detailed procedures for obtaining the circular trajectories of UAV-B and UAV-J are given in [10].

In Fig. 2, we plot the trajectories of UAV-B and UAV-J achieved by our proposed algorithm and the benchmark scheme BMS1.[1] The IRs and Eves are marked with squares and circles, respectively. Each trajectory is sampled every 1.5 s. Based on the trajectories generated by the proposed algorithm, we observe that UAV-B hovers around each IR for a period of time to ensure a certain max-min secrecy rate. UAV-J attempts to fly far from the active IRs to reduce the co-channel interference, but UAV-J tends to fly as close as possible to the Eves that are near the active IRs so as to prevent it from intercepting the confidential information. For example, when UAV-B is hovering over IR 1, UAV-J locates itself in the middle of Eve 1 and Eve 2 to create interference. This is due to the fact that Eve 1 and Eve 2 are geometrically symmetric with respect to IR 1, and they can eavesdrop on the confidential information to IR 1 at the same rate. In addition, it is observed that when UAV-B is between two adjacent IRs, it flies at its maximum speed and selects the shortest path such that it has more time to stay above each IR, in order to guarantee wireless communication security. This observation is confirmed by the fact (found in our simulation) the speed of UAV-B is very small when it is located in the vicinity of each IR, while this speed is $V_{\max}$ when it is between two IRs. In Fig. 2, we further observe that, when UAV-B is located between two IRs, UAV-J hovers in the vicinity of the Eve that is closest to UAV-B, in order to create strong interference to this Eve. For the benchmark scheme BMS1, i.e.,

[1] Due to space limitation, the simple circular trajectories are omitted in Fig. 2, while the corresponding secrecy rate is shown later in Fig. 3(b).



(a) The transmit power of UAV-B (b) Average secrecy rate versus T

Fig. 3. Transmit power of UAV-B and max-min average secrecy rate.

the scheme without UAV-J, UAV-B chooses a trajectory as far from Eves as possible to prevent the confidential information from being intercepted, leading to a larger travel distance. However, this is also at the cost of sacrificing the direct favourable channel conditions to IRs. In contrast, the proposed algorithm with a mobile UAV jammer allows UAV-B to fly closer to the Eves, which enables UAV-B to have more freedom to choose the trajectory and enjoy better air-to-ground channel conditions. As such, UAV-B has more time to serve each IR and thus the average secrecy rate of the considered UAV network should be improved by our proposed algorithm, which will be confirmed by Fig. 3(b).

In Fig. 3(a), we plot the transmit power of UAV-B achieved by our proposed algorithm for each IR versus time. First, it is observed that the UAV-B always chooses to serve the IR when the best channel quality is created by hovering above it and then allocates all of its transmit power to this IR. In addition, one can observe that the transmit power of UAV-B is very small for a period of time when it is between two adjacent IRs. This can further enhance the security of its wireless transmissions. By comparing Fig. 2 and Fig. 3(a), we observe that UAV-B serves each IR for the same period in each T, due to the consideration of the max-min average secrecy rate in our optimization problem so as to achieve the fairness among these IRs.

In Fig. 3(b), we plot the max-min average secrecy rate versus flight duration T for different flight duration T. First, we observe that the proposed algorithm significantly outperforms the two benchmark schemes, which demonstrates the benefits of the joint optimization of the trajectories and transmit power of the UAV-B and UAV-J. In particular, by comparing to BMS1, the performance improvement is attributed by employing the mobile UAV jammer. We also observe that the max-min average secrecy rates increase as $P_{B,\max}$ increases for all schemes. This is due to the fact that the UAV-B hovers around each IR for a period of time and transmits confidential messages at the maximum transmit power. Furthermore, it is observed that the max-min average secrecy rate of BMS2 approaches an upper bound as T increases, while those of the other two schemes continuously increase with T. This demonstrates the necessity of the trajectory optimization in UAV-enabled secure communication.

VI. Conclusion

In this work, we jointly optimized the trajectories and transmit power of UAV-B and UAV-J in order to maximize the minimum average secrecy rate over all IRs. We proposed an alternating iterative algorithm and utilized the SCA technique to solve the associated optimization problem. Our examination shows that the physical layer security of the considered UAV network can be significantly enhanced by the proposed solution relative to two benchmark schemes. In the future work, we will consider dynamic bandwidth allocation among different IRs to further improve the security performance of the system. In addition, more practical scenarios where the locations of Eves are not perfectly available and/or IRs require delay-sensitive services are worth pursuing.

References

[1] Q. Wu, L. Liu, and R. Zhang, "Fundamental tradeoffs in communication and trajectory design for UAV-enabled wireless network," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 36–44, Feb. 2019.

[2] L. Xiao, X. Lu, D. Xu, Y. Tang, L. Wang, and W. Zhuang, "UAV relay in vanets against smart jamming with reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4087–4097, May 2018.

[3] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 5, pp. 1143–1153, May 2017.

[4] L. Xiao, C. Xie, M. Min, and W. Zhuang, "User-centric view of unmanned aerial vehicle transmission against smart attacks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3420–3430, Apr. 2018.

[5] Q. Wu and R. Zhang, "Common throughput maximization in UAV-enabled OFDMA systems with delay consideration," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6614–6627, Dec. 2018.

[6] Z. Kaleem and M. H. Rehmani, "Amateur drone monitoring: State-of-the-art architectures, key enabling technologies, and future research directions," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 150–159, Apr. 2018.

[7] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[8] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[9] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three artificial-noise-aided secure transmission schemes in wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3669–3673, Apr. 2018.

[10] 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.

[11] 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.

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

[13] L. An, 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, Feb. 2019.

[14] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, W. Hardjawana, and B. Vucetic, "Secrecy outage probability and jamming coverage of UAV-enabled friendly jammer," in *Proc. 11th Int. Conf. Signal Process. Commun. Syst.*, Dec. 2017, pp. 1–6.

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

[16] A. Zappone, E. Bjornson, L. Sanguinetti, and E. Jorswieck, "Globally optimal energy-efficient power control and receiver design in wireless networks," *IEEE Trans. Signal Process.*, vol. 65, no. 11, pp. 2844–2859, Jun. 2017.