Joint Trajectory and Power Optimization for Securing UAV Communications Against Active Eavesdropping

Bin Duo[1], **Junsong Luo**[1,*], **Yilian Li**[1], **Hao Hu**[1], **Zibin Wang**[2]

[1] College of Information Science and Technology, Chengdu University of Technology, Chengdu 610059, China
[2] National Key Laboratory of Science and Technology on Information System Security, Beijing 100093, China
[*] The corresponding author, email: junsong_luo@163.com

Abstract: Due to both of jamming and eavesdropping, active eavesdroppers can induce more serious security threats to unmanned aerial vehicle (UAV)-enabled communications. This paper considers a secure UAV communication system including both the downlink (DL) and uplink (UL) transmissions, where the confidential information is transmitted between a UAV and a ground node in the presence of an active eavesdropper. We aim to maximize the average secrecy rates of the DL and UL communications, respectively, by jointly optimizing the UAV trajectory and the UAV/ground node's transmit power control over a given flight period. Due to the non-convexity of the formulated problems, it is difficult to obtain globally optimal solutions. However, we propose efficient iterative algorithms to obtain high-quality suboptimal solutions by applying the block coordinate descent and successive convex optimization methods. Simulation results show that the joint optimization algorithms can effectively improve the secrecy rate performance for both the DL and UL communications, as compared with other baseline schemes. The proposed schemes can be considered as special cases of UAV-assisted non-orthogonal multiple access (NOMA) networks.

Keywords: UAV communications; active eavesdropping; physical-layer security; secrecy rate maximization; power control; trajectory design

Received: Jun. 28, 2020
Revised: Aug. 6, 2020
Editor: Wei Duan

I. INTRODUCTION

With the advantages of low cost, high mobility, rapid deployment and wide coverage, unmanned aerial vehicles (UAVs) play an important role in many practical scenes, such as wireless sensor networks [1], disaster rescue [2] and aerial photography [3]. In particular, in wireless communication systems, the application of UAVs can effectively improve the throughput [4], enhance the security performance [5] and expand the communication distances [6], etc. However, although the line-of-sight (LoS) dominant transmission provides better communication quality in UAV communications, it is also extremely vulnerable to serious security threats such as eavesdropping, jamming and truncation caused by illegal communication nodes on the ground. This leads to the confidential information leakage and communication quality degradation. Therefore, how to ensure the security of information transmission in UAV communication systems has become a challenging issue.

By taking advantage of their flexible flying trajectory, UAVs can establish favorable transmission conditions for legitimate communications over malicious ground nodes. Therefore, the UAV trajectory design combined with physical-layer security technique can effectively improve the secrecy rates in UAV communications [7, 8]. A three-node secure UAV-enabled communication system was first considered in [9], where the joint optimization of the UAV trajectory and power control was proposed to improve the secrecy rates. The authors in [10] proposed an aerial cooperative jamming scheme for improving the secrecy performance of the ground wiretap channel, with the UAV being a friendly jammer to interfere with the potential eavesdropper. Based on the idea of the aerial cooperative jamming, a novel dual-UAVs communication system was proposed in [11], where one UAV transmits private information to ground nodes while the other UAV helps to interfere with eavesdroppers for enhancing the secrecy rates. To provide communication services for ground nodes with long distances, a UAV-aided relaying wireless network with caching was proposed in [12], where the UAV trajectory and time scheduling are jointly optimized to enhance the secrecy rate performance. Non-orthogonal multiple access (NOMA) as a promising technique can effectively enhance the spectral efficiency for wireless communication systems [13, 14]. Therefore, the UAV-aided NOMA networks were studied in [15] and a corresponding joint precoding optimization scheme was proposed to maximize the throughput of ground users while guaranteeing the system security via artificial jamming. In [16], a secure downlink UAV communication scheme enabled by NOMA was proposed to maximize the minimum achievable secrecy rate by the joint optimization of the user scheduling, power allocation and trajectory design.

However, with the rise of full-duplex technology, active eavesdropping brings more serious security threats to UAV communication systems. It cannot only send jamming signals to legitimate nodes for hindering them from obtaining valid and reliable information, but also wiretap the confidential information from UAV communications. Therefore, it is more practical to study the secure UAV communication in the presence of active eavesdroppers. The works in [17, 18] proposed artificial noise (AN) methods for safeguarding the UAV communications against full-duplex active eavesdroppers, where the power allocations of the AN and transmit signals as well as the UAV altitude are jointly optimized to improve the rate performance. Note that the above works do not fully take advantage of the UAV trajectory flexibility to mitigate active eavesdropping. Therefore, it motivates us to investigate whether anti-active eavesdropping trajectory design can further improve the secrecy rate performance of UAV-enabled communications.

In this paper, we consider both the uplink (UL) and downlink (DL) transmissions of the UAV-enabled communication system, where a ground node and a UAV form a legal communication link while an active eavesdropper intends to interfere and intercept the confidential information. Due to the existence of the active eavesdropper, the UAV trajectory should be adjusted to approach the ground user while keeping away from the active eavesdropper for establishing favorable transmission conditions. To safeguard both the UL and DL communications, we aim to maximize the worst-case average secrecy rates with a given UAV flying duration, by jointly designing the transmit power allocation and UAV trajectory optimization algorithms. The optimization problems are subject to the UAV mobility and transmit power constraints. Due to the non-convexity of the formulated problems, it is challenging to obtain globally optimal solutions with feasible complexity. To tackle such difficulties, we first transform the objective functions into achievable lower bound expressions. Then, we propose efficient iterative algorithms to solve the corresponding problems approximately by applying block coordinate descent (BCD) method. In this way, the optimization variables can be divided into two blocks, i.e., the UAV trajectory and the ground node/UAV transmit power control variables, which are alternately optimized over iterations. However, even with the given transmit power, the subproblems of UAV trajectory optimization are still intractable due to its non-convexity. We thus introduce slack variables and apply the successive convex approximation (SCA) technique to solve them approximately. The numerical results show that the proposed algorithms can significantly improve the secrecy rate performance, comparing with other benchmark schemes, which demonstrates the importance of the joint power control and trajectory design against active eavesdropping in both the DL and UL transmissions in UAV-enabled communications.

The rest of this paper is organized as follows. Section II represents the system model and problem formulation. In Section III and IV, we propose iterative algorithms for DL and UL transmissions, respectively. The numerical results are provided to validate the effectiveness of the proposed algorithms in Section V. Finally, Section VI concludes the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

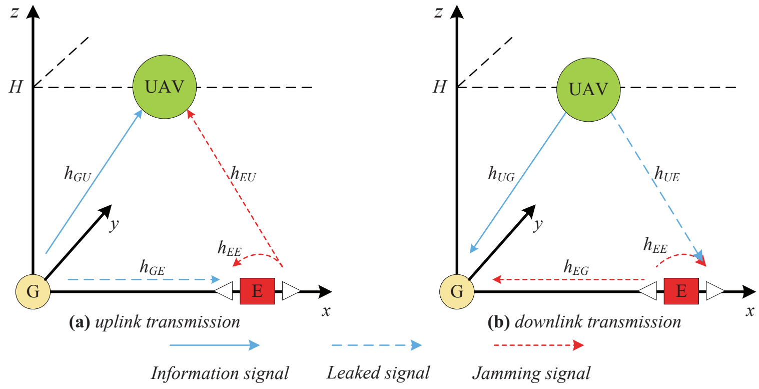

Figure 1. *Secure UAV communication systems subjected to an active eavesdropper.*

2.1 System Model

As shown in Figure 1, we consider two secure transmission schemes for UAV-aided communications: the UL transmission where a ground node (G) transmits to a legitimate UAV as well as the DL transmission where a UAV transmits to a legitimate G. Both schemes face severe security issues caused by a full-duplex active eavesdropper (E). The active eavesdropper wiretaps the secrecy information between G and the UAV, meanwhile sending jamming signals to degrade the legitimate transmissions. We establish the three-dimensional (3D) Cartesian coordinate system, where the horizontal coordinates of G and E are denoted by $\mathbf{w}_G = (0, 0)$ and $\mathbf{w}_E = (A, 0)$, respectively, with their locations being known to the UAV[1]

Within a given finite flight period T, the UAV flies horizontally from the pre-determined initial location to the final location, which are denoted by $\mathbf{q}_0 = (x_0, y_0)$ and $\mathbf{q}_F = (x_F, y_F)$, respectively, with a fixed altitude H. To make it more manageable, T is divided into N equal-length slots, i.e., $T = \delta_t N$, where δ_t is the length of a time slot. As such, the UAV trajectory can be denoted as $\mathbf{q}[n] = \{x[n], y[n]\}_{n=1}^{N}$. Denote by $V_{\max}$ the maximum flying speed of the UAV, and thus $D = V_{\max}\delta_t$ represents the maximum UAV horizontal flying distance in time slot n. Practically, the UAV should satisfy the mobility constraints as follows:

$$||\mathbf{q}[n+1] - \mathbf{q}[n]||^2 \le D^2, n = 1, \cdots, N-1, \quad (1)$$

$$\mathbf{q}_0 = \mathbf{q}[0], \quad (2)$$

$$\mathbf{q}_F = \mathbf{q}[N]. \quad (3)$$

2.1.1 Channel Model of Downlink Transmission

For the transmissions from the UAV to G (UG) and the UAV to E (UE) at time slot n, we assume that the channel power gain follows the free-space path loss model [9–12], which is given by[2]

$$h_{ij}[n] = \rho_0 d_{ij}^{-\alpha}[n], ij \in \{UG, UE\}, \quad (4)$$

where $d_{UG}[n] = \sqrt{H^2 + ||\mathbf{q}[n] - \mathbf{w}_G||^2}$, $d_{UE}[n] = \sqrt{H^2 + ||\mathbf{q}[n] - \mathbf{w}_E||^2}$, α is the path loss exponent and ρ_0 denotes the channel power gain at the reference distance $d_0 = 1$ m. For the ground transmission between E and G (EG), we adopt the Rayleigh fading channel model. As such, the channel power gain is expressed by

$$h_{EG} = \rho_0 A^{-\kappa}\zeta_{EG}, \quad (5)$$

where κ is the path loss exponent and ζ_{EG} is a random variable with unit mean exponential distribution to characterize small-scale Rayleigh fading.

Let $p_U[n], \bar{P}_U$ and $\tilde{P}_U$ denote the UAV's transmit power in time slot n, average and peak powers, respectively. In practice, they should satisfy the following constraints,

$$\frac{1}{N}\sum_{n=1}^{N} p_U[n] \le \bar{P}_U, 0 \le p_U[n] \le \tilde{P}_U, \quad (6)$$

where we assume $\bar{P}_U \le \tilde{P}_U$ to make the constraint non-trivial. Thus, the average achievable secrecy rate in bits/second/Hertz (bps/Hz) over N time slots is given by [19, 20]

$$R_{\text{sec}}^{DT} = \frac{1}{N}\sum_{n=1}^{N}\left[R_G[n] - R_E[n]\right]^{+}, \tag{7}$$

where $[x]^{+} = \max(x, 0)$. Let h_{EE} represents the self-interference from E's transmitting antenna to its receiving antenna and p_E is the maximum transmit power of E. The achievable rates at G and at E in time slot n can be expressed as

$$R_G[n] = \mathbb{E}\left[\log_2\left(1 + \frac{p_U[n]h_{UG}[n]}{p_E h_{EG} + \sigma^2}\right)\right], \tag{8}$$

$$R_E[n] = \log_2\left(1 + \frac{p_U[n]h_{UE}[n]}{p_E h_{EE} + \sigma^2}\right). \tag{9}$$

where $\mathbb{E}[\cdot]$ is the expectation operator with respect to ζ_{EG} and σ^2 is the additive white Gaussian noise (AWGN) power at G or E. Since $R_G[n]$ in (8) is convex with respect to its random variable ζ_{EG} [21], we can derive its lower bound based on Jensen's inequality, i.e.,

$$\begin{aligned} R_G[n] &= \mathbb{E}\left[\log_2\left(1 + \frac{p_U[n]h_{UG}[n]}{p_E h_{EG} + \sigma^2}\right)\right] \\ &\geq \log_2\left(1 + \frac{p_U[n]h_{UG}[n]}{p_E\rho_0 A^{-\kappa}\mathbb{E}[\zeta_{EG}] + \sigma^2}\right) \\ &= \log_2\left(1 + \frac{p_U[n]h_{UG}[n]}{p_E\rho_0 A^{-\kappa} + \sigma^2}\right). \end{aligned} \tag{10}$$

Note that we consider the worst-case secrecy rate performance by assuming that the active eavesdropper transmits with its maximum power over the whole period and it can perfectly cancel its self-interference h_{EE}. As such, $R_E[n]$ in (9) can be upper-bounded by

$$\begin{aligned} R_E[n] &= \log_2\left(1 + \frac{p_U[n]h_{UE}[n]}{p_E h_{EE} + \sigma^2}\right) \\ &\leq \log_2\left(1 + \frac{p_U[n]h_{UE}[n]}{\sigma^2}\right). \end{aligned} \tag{11}$$

2.1.2 Channel Model of Uplink Transmission

Similarly, for the ground-to-air links between G and the UAV (GU), and E and the UAV (EU) at time slot n, the channel power gain is given by

$$h_{ij}[n] = \rho_0 d_{ij}^{-\alpha}[n], ij \in \{GU, EU\}, \tag{12}$$

where $d_{GU}[n] = \sqrt{H^2 + ||\mathbf{q}[n] - \mathbf{w}_G||^2}$ and $d_{EU}[n] = \sqrt{H^2 + ||\mathbf{q}[n] - \mathbf{w}_E||^2}$. Correspondingly, the channel between G to E (GE) is given by

$$h_{GE} = \rho_0 A^{-\kappa}\zeta_{GE}, \tag{13}$$

where ζ_{GE} is an exponentially distributed random variable.

Denote by $p_G[n]$ the transmit power of G in time slot n. Similar to the DL transmission, $p_G[n]$ is constrained by average and peak power limits denoted by $\bar{P}_G$ and $\tilde{P}_G$, respectively, i.e.,

$$\frac{1}{N}\sum_{n=1}^{N} p_G[n] \leq \bar{P}_G, 0 \leq p_G[n] \leq \tilde{P}_G, \tag{14}$$

where $\bar{P}_G \leq \tilde{P}_G$ is assumed. Therefore, the average achievable secrecy rate over N time slots is given by

$$R_{\text{sec}}^{UT} = \frac{1}{N}\sum_{n=1}^{N}\left[R_U[n] - R_E[n]\right]^{+}, \tag{15}$$

where

$$R_U[n] = \log_2\left(1 + \frac{p_G[n]h_{GU}[n]}{p_E h_{EU}[n] + \sigma^2}\right), \tag{16}$$

$$\begin{aligned} R_E[n] &= \mathbb{E}\left[\log_2\left(1 + \frac{p_G[n]h_{GE}}{p_E h_{EE} + \sigma^2}\right)\right] \\ &\leq \log_2\left(1 + \frac{p_G[n]\rho_0 A^{-\kappa}}{p_E h_{EE} + \sigma^2}\mathbb{E}[\zeta_{GE}]\right) \\ &\leq \log_2\left(1 + \frac{p_G[n]\rho_0 A^{-\kappa}}{\sigma^2}\right). \end{aligned} \tag{17}$$

Eq. (17) holds due to the concavity of $R_E[n]$ with respect to ζ_{GE} [21] and the application of Jensen's inequality, as well as the assumption of perfect cancellation of h_{EE}.

2.2 Problem Formulation

For DL transmission, we aim to maximize the secrecy rate in (7) over N time slots by jointly optimizing the

UAV transmit power $\mathbf{p}_U \triangleq \{p_U[n], n \in \mathcal{N}\}$ and the UAV trajectory $\mathbf{q} \triangleq \{\mathbf{q}[n], n \in \mathcal{N}\}$. Since the secrecy rate is non-negative in practice, R_{sec}^{UT} is at least zero when adaptively setting $p_U[n] = 0$ under the power constraint (6). As such, the operation $[]^+$ can be dropped and thus the maximization problem is formulated as below

$$\max_{\mathbf{p}_U,\mathbf{q}} \sum_{n=1}^{N} \left(\log_2 \left(1 + \frac{p_U[n] h_{UG}[n]}{p_E \rho_0 A^{-\kappa} + \sigma^2} \right) - \log_2 \left(1 + \frac{p_U[n] h_{UE}[n]}{\sigma^2} \right) \right) \tag{18}$$

$$\text{s.t. } (1)\text{-}(3), (6).$$

Similarly, for UL transmission, our goal is to maximize the secrecy rate in (15) by jointly optimizing the G's transmit power $\mathbf{p}_G \triangleq \{p_G[n], n \in \mathcal{N}\}$ and the UAV trajectory $\mathbf{q} \triangleq \{\mathbf{q}[n], n \in \mathcal{N}\}$. As such, the maximization problem for the UL case is given by

$$\max_{\mathbf{p}_G,\mathbf{q}} \sum_{n=1}^{N} \left(\log_2 \left(1 + \frac{p_G[n] h_{GU}[n]}{p_E h_{EU}[n] + \sigma^2} \right) - \log_2 \left(1 + \frac{p_G[n] \rho_0 A^{-\kappa}}{\sigma^2} \right) \right) \tag{19}$$

$$\text{s.t. } (1)\text{-}(3), (14).$$

In general, solving problems (18) and (19) optimally with feasible complexity are both challenging since their objective functions are not concave with respect to their respective optimization variables. In Section III and IV, we propose efficient iterative algorithms based on BCD and SCA methods to obtain suboptimal solutions to problems (18) and (19), respectively.

III. PROPOSED ALGORITHM FOR SOLVING PROBLEM (18)

In this section, we first consider problem (18) for DL transmission. Specifically, we cope with problem (18) by solving two subproblems iteratively, i.e., the alternate optimization of the UAV transmit power $\mathbf{p}_U$ and the UAV trajectory $\mathbf{q}$.

3.1 Transmit Power Optimization Of the UAV

For given $\mathbf{q}$, problem (18) can be rewritten as

$$\max_{\mathbf{p}_U} \sum_{n=1}^{N} \left[\log_2 \left(1 + a_n p_U[n] \right) - \log_2 \left(1 + b_n p_U[n] \right) \right] \tag{20}$$

$$\text{s.t. } (6).$$

where $a_n = \frac{\gamma_0}{(H^2 + ||\mathbf{q}[n]||^2)^{\frac{\alpha}{2}} (p_E \gamma_0 A^{-\kappa} + 1)}$, $b_n = \frac{\gamma_0}{(H^2 + ||\mathbf{q}[n] - \mathbf{w}_E||^2)^{\frac{\alpha}{2}}}$ and $\gamma_0 = \rho_0 / \sigma^2$ is the reference signal-to-noise ratio (SNR). We can derive the close-form optimal solution based on [9], i.e.,

$$p_U^*[n] = \begin{cases} \min([\hat{p}_U[n]]^+, \tilde{P}_U), & a_n > b_n, \\ 0, & a_n \leq b_n, \end{cases} \tag{21}$$

where $\hat{p}_U[n] = \sqrt{\left(\frac{1}{2b_n} - \frac{1}{2a_n} \right)^2 + \frac{1}{\mu \ln 2} \left(\frac{1}{b_n} - \frac{1}{a_n} \right)} - \frac{1}{2a_n} - \frac{1}{2b_n}$, and $\mu \geq 0$ is a constant that guarantees the satisfaction of constraint (6), which can be obtain efficiently via the bisection search [21].

3.2 UAV Trajectory Optimization

With given $\mathbf{p}_U$, by letting $\mathbf{l} = \{l[n], n \in \mathcal{N}\}$ and $\mathbf{m} = \{m[n], n \in \mathcal{N}\}$ as the introduced slack variables, we can express problem (18) as

$$\max_{\mathbf{q},\mathbf{l},\mathbf{m}} \sum_{n=1}^{N} \left[\log_2 \left(1 + \frac{c_n}{l[n]} \right) - \log_2 \left(1 + \frac{d_n}{m[n]} \right) \right] \tag{22}$$

$$\text{s.t. } (H^2 + ||\mathbf{q}[n]||^2)^{\frac{\alpha}{2}} - l[n] \leq 0, \tag{23}$$

$$(H^2 + ||\mathbf{q}[n] - \mathbf{w}_E||^2)^{\frac{\alpha}{2}} - m[n] \geq 0, \tag{24}$$

$$m[n] \geq H^{\alpha}, \tag{25}$$

$$(1)\text{-}(3).$$

where $c_n = \gamma_0 p_U[n] / (p_E \gamma_0 A^{-\kappa} + 1)$ and $d_n = \gamma_0 p_U[n]$.

Note that the constraints (23) and (24) must hold with equalities in order to obtain the optimal solution, otherwise $l[n](m[n])$ can be increased (decreased) to decrease the objective value of problem (18). Therefore, problem (22) has the same optimal solution of $\mathbf{q}$ as that of problem (18).

Despite the introduction of slack variables, problem (22) is still non-convex due to its non-convex objective function and constraints. However, we observe that $\log_2 \left(1 + \frac{c_n}{l[n]} \right)$ in (22) is convex with respect to $l[n]$. As such, the SCA technique can be applied to solve problem (22) approximately. By using the first-order Taylor expansion at given local points denoted as $\mathbf{l}^k = \left\{l^k[n], n \in \mathcal{N}\right\}$ in the k-th iteration, $\log_2\left(1+\frac{c_n}{l[n]}\right)$ can be lower-bounded by

$$\log_2\left(1+\frac{c_n}{l[n]}\right) \geq \log_2\left(1+\frac{c_n}{l^k[n]}\right) - \frac{c_n(l[n]-l^k[n])}{\ln 2(l^k[n]+c_n)l^k[n]}. \tag{26}$$

According to the conditions on guaranteeing the convexity or concavity of composition functions in [21], $\left(H^2+\|\mathbf{q}[n]-\mathbf{w}_E\|^2\right)^{\frac{\alpha}{2}}$ is convex with respect to $\mathbf{q}[n]$. Similarly, by using the first-order Taylor expansion at the given local points denoted as $\mathbf{q}^k = \left\{\mathbf{q}^k[n], n \in \mathcal{N}\right\}$ in the k-th iteration, we have

$$\left(H^2+\|\mathbf{q}[n]-\mathbf{w}_E\|^2\right)^{\frac{\alpha}{2}} \leq Q^k[n], \tag{27}$$

where $Q^k[n] = \left(H^2+\left\|\mathbf{q}^k[n]-\mathbf{w}_E\right\|^2\right)^{\frac{\alpha}{2}} + \alpha\left(H^2+\left\|\mathbf{q}^k[n]-\mathbf{w}_E\right\|^2\right)^{\frac{\alpha}{2}-1}\left(\mathbf{q}^k[n]-\mathbf{w}_E\right)^T(\mathbf{q}[n] -\mathbf{q}^k[n])$.

Hence, with (26) and (27), problem (22) can be lower-bounded by

$$\max_{\mathbf{q},\mathbf{l},\mathbf{m}} \sum_{n=1}^{N}\left[-\frac{c_n l[n]}{\ln 2(l^k[n]+c_n)l^k[n]} - \log_2\left(1+\frac{d_n}{m[n]}\right)\right] \tag{28}$$

$$\text{s.t. } m[n] \leq Q^k[n], \tag{29}$$

$$(1)\text{-}(3), (23), (25).$$

We can see that the objective function of problem (28) is concave with all convex constraints now. Thus, it can be efficiently solved by the commonly used CVX solver [22].

3.3 Overall Algorithm and Computational Complexity

To sum up, the overall algorithm can achieve a suboptimal solution to problem (18) by alternately optimizing variables $\mathbf{p}_U$ and $\mathbf{q}$ in an iterative way. The detailed process for solving problem (18) is summarized in Algorithm 1.

Algorithm 1. *Proposed algorithm for solving problem* (18)

```
Initial $\mathbf{p}_U$, $\mathbf{q}$, $\mathbf{l}$ and $\mathbf{m}$. Let $k = 0$.
repeat
    Solve problem (20) with given $\mathbf{q}^k$
      and denote by $\mathbf{p}_U^{k+1}$ the optimal solution.
    Solve problem (28) with given $\mathbf{p}_U^k$
      and denote by $\mathbf{q}^{k+1}$ the obtained optimal solution.
    Update $k = k + 1$.
until Converge to a given threshold $\epsilon > 0$.
```

Based on the analysis in [9], Algorithm 1 ensures that the obtained objective value of problem (18) is non-decreasing over the iterations. The total complexity of Algorithm 1 is given by $O(KN^{3.5})$, where K presents the iteration number.

IV. PROPOSED ALGORITHM FOR SOLVING PROBLEM (19)

In this section, we consider the UL case. Similar to (18), we can also apply the BCD method to solve problem (19) by coping with two subproblems iteratively, i.e., the alternate optimization of the G's transmit power $\mathbf{p}_G$ under the given UAV trajectory $\mathbf{q}$ as well as the UAV trajectory $\mathbf{q}$ under the given G's transmit power $\mathbf{p}_G$, until the algorithm converges.

4.1 Transmit Power Optimization Of G

For given UAV trajectory $\mathbf{q}$, problem (19) can be rewritten as

$$\max_{\mathbf{p}_G} \sum_{n=1}^{N}\left[\log_2\left(1+a_n p_G[n]\right) - \log_2\left(1+b p_G[n]\right)\right] \tag{30}$$

$$\text{s.t. } (14),$$

where $a_n = \frac{\gamma_0}{(H^2+||\mathbf{q}[n]||^2)^{\frac{\alpha}{2}}} / \left(\frac{\gamma_0 p_E}{(H^2+||\mathbf{q}[n]-\mathbf{w}_E||^2)^{\frac{\alpha}{2}}}+1\right)$, $b = \gamma_0 A^{-\kappa}$. Problem (30) can be similarly solved by using (21), with b_n in (21) being replaced with b in (30).

4.2 UAV Trajectory Optimization

With given $\mathbf{p}_G$, let $e_n = \gamma_0 p_G[n]$ and $f = \gamma_0 p_E$ for notation simplicity. Similarly, we introduce slack variables $\mathbf{l} = \{l[n], n \in \mathcal{N}\}$ and $\mathbf{m} = \{m[n], n \in \mathcal{N}\}$. Then, problem (19) can be reformulated as

$$\begin{aligned} \max_{\mathbf{q},\mathbf{l},\mathbf{m}} \sum_{n=1}^{N} \Bigg[&\log_2 \left(1 + \frac{f}{m[n]} + \frac{e_n}{l[n]}\right) \\ &- \log_2 \left(1 + \frac{f}{m[n]}\right) \Bigg] \qquad (31) \\ \text{s.t. } &(1)\text{-}(3), (23)\text{-}(25). \end{aligned}$$

Despite the reformulation of problem (19), the objective function of problem (31) is still non-concave with its optimization variables. However, the function $\log_2 \left(1 + \frac{f}{m[n]} + \frac{e_n}{l[n]}\right)$ is jointly convex with respect to $m[n]$ and $l[n]$. As such, by using Taylor expansion of a convex function $g(x, y)$ in a neighborhood of $(x, y) = (x_0, y_0)$, i.e., $g(x, y) \approx g(x_0, y_0) + g_x(x_0, y_0)(x - x_0) + g_y(x_0, y_0)(y - y_0)$. The term $\log_2 \left(1 + \frac{f}{m[n]} + \frac{e_n}{l[n]}\right)$ in problem (31) at given local points denoted by $\mathbf{l}^k = \{l^k[n], n \in \mathcal{N}\}$ and $\mathbf{m}^k = \{m^k[n], n \in \mathcal{N}\}$, in the k-th iteration, can be given by

$$\begin{aligned} \log_2 \left(1 + \frac{f}{m[n]} + \frac{e_n}{l[n]}\right) &\geq \log_2 B^k[n] \\ &- \frac{f\left(m^k[n]\right)^{-2}\left(m[n] - m^k[n]\right)}{B^k[n] \ln 2} \\ &- \frac{e_n\left(l^k[n]\right)^{-2}\left(l[n] - l^k[n]\right)}{B^k[n] \ln 2}, \qquad (32) \end{aligned}$$

where $B^k[n] = 1 + \frac{f}{m^k[n]} + \frac{e_n}{l^k[n]}$.

For the non-convex constraint (24), it can be handled similarly as (27) to obtain constraint (29). Therefore, problem (31) can be lower-bounded by

$$\begin{aligned} \max_{\mathbf{q},\mathbf{l},\mathbf{m}} \sum_{n=1}^{N} \Bigg[&- \frac{f\left(m^k[n]\right)^{-2} m[n]}{B^k[n] \ln 2} - \frac{e_n\left(l^k[n]\right)^{-2} l[n]}{B^k[n] \ln 2} \\ &- \log_2 \left(1 + \frac{f}{m[n]}\right) \Bigg] \qquad (33) \\ \text{s.t. } &(1)\text{-}(3), (23), (25), \ (29). \end{aligned}$$

It is observed that problem (33) is convex with all convex constraints. As such, the CVX solver can also be used to efficiently solve this problem. Due to the similar algorithm with that for solving problem (18), we omit the details of the overall algorithm for UL transmission for brevity. Moreover, the complexity of the proposed algorithm is also in the order of $O(KN^{3.5})$, which means that the suboptimal solution is computed in polynomial time, and thus can be efficiently applied in practical systems.

V. NUMERICAL RESULTS

In this section, we show simulation results to verify the effectiveness of the proposed joint transmit power control and UAV trajectory optimization (denoted as T&P) algorithm for improving the secrecy rate performance. For comparison, two benchmark schemes are also considered in the following: 1) UAV trajectory optimization without power control (denoted as T/NP); and 2) Heuristic UAV trajectory with power control (denoted as HT/P). Specifically, the UAV trajectories in T/NP are obtained by solving problems (28) and (33) iteratively until the corresponding algorithms converge, respectively, with equal transmit power allocation over the whole duration T, i.e., $p_G[n] = \bar{P}_G$ and $p_U[n] = \bar{P}_U$. For the HT/P scheme, the UAV first flies directly to the location right above G at its maximum speed $V_{\max}$, then stays hovering as long as it can. By the end of T, it returns to its final location at $V_{\max}$. Given the fixed trajectories in HT/P, the transmit powers $p_U[n]$ and $p_G[n]$ for DL and UL transmissions can be obtained by solving problem (20) and (30), respectively. The simulation parameters are elaborated in Table 1.

5.1 Downlink Transmission

We first testify the convergence of the proposed Algorithm 1 for the DL case in Figure 2. It can be observed that the average secrecy rate increases with the number of iterations and rapidly converges after about 8 iterations for different T. Moreover, with the increase of T, the rate performance improved significantly. Note that no rate improvement can be observed for $T = 140s$. The reason is that without sufficient flying time for the UAV to complete its mission, the UAV cannot enjoy the benefits of the flexible trajectory design.

Figure 3 illustrates different UAV trajectories by different schemes for DL transmission with different

Table 1. *Simulation parameters.*

Notation	Physical Meaning	Simulation parameters
$\mathbf{w}_G$	Horizontal location of G	(0,0) m
$\mathbf{w}_E$	Horizontal location of E	(200,0)m
$\mathbf{q}_0$	UAV's initial location	(-700,-250)m
$\mathbf{q}_F$	UAV's final location	(700,-250)m
H	Altitude of UAV	100 m
$V_{\max}$	Maximum speed of the UAV	10 m/s
p_E	Jamming power of E in DL/UL transmission	10/7 dBm
δ_t	Time slot length	1s
ρ_0	Channel power gain at the reference distance	-60 dB
σ^2	AWGN power	-110 dBm
α and κ	Path loss exponent	2.2 and 3
$\bar{P}_U$ and $\tilde{P}_U$	Average and peak power of the UAV	10 dBm and 16 dBm
$\bar{P}_G$ and $\tilde{P}_G$	Average and peak power of the ground user	10 dBm and 16 dBm
ϵ	Threshold	10^{-4}

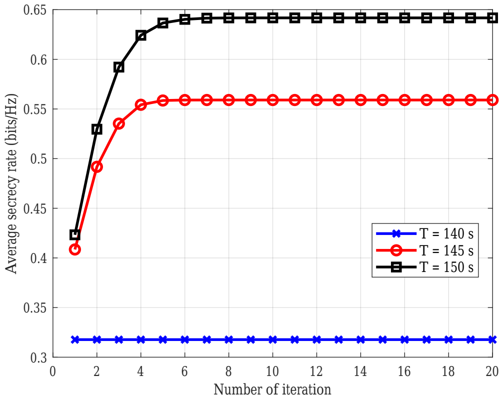

Figure 2. *Average secrecy rate versus iteration number.*

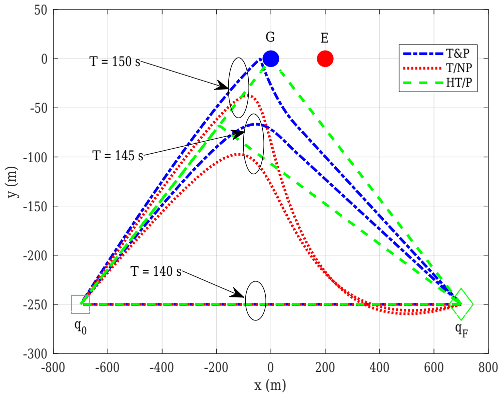

Figure 3. *UAV trajectories by different schemes for DL transmission.*

flight period T. Since $T = 140$s is the shortest time for the UAV to fly from the initial location to the final location, the trajectories of all schemes are the same as a straight line. When $T = 145$s, because the flight period is not enough for the UAV to reach G at its maximum speed, the UAV flies as close as possible to G and then arrives at the final location by the end of the limited duration. However, when T is sufficiently large, e.g., $T = 150$s, it is observed that the UAV in T&P first flies to the left of G along an approximate straight line, compared with that in HT/P which flies directly towards G. This is because at its hovering location, the UAV in T&P can achieve an optimal balance between the information leakage to E and jamming from E minimization as well as the achievable rate maximization. During the return trip, it is expected that the UAV trajectory in T&P is farther away from E compared to that in HT/P due to the optimized trajectory that degrades the channel quality of the leaked UAV-to-E transmission. However, the UAV trajectory in T/NP flies along a larger curved path to complete its mission, which differs much compared with that of other schemes. The reason is that since there is no power control, the UAV has to adjust its trajectory to fly father away from E to prevent it from leaking more information to E.

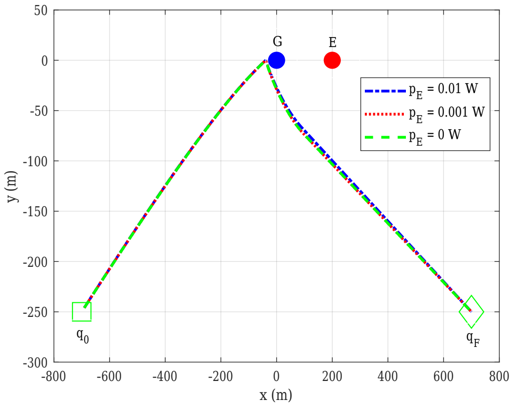

Figure 4. *UAV Trajectories by T&P under different jamming powers for DL transmission.*

Figure 4 shows different trajectories by T&P versus jamming power p_E for DL transmission. As expected, all UAV trajectories are identical. This is because the interference generated by the active eavesdropper mainly affects G, but has no impact on the UAV. Therefore, in the case of DL transmission, different jamming powers induced by E do not lead to the change of the resulting UAV trajectory.

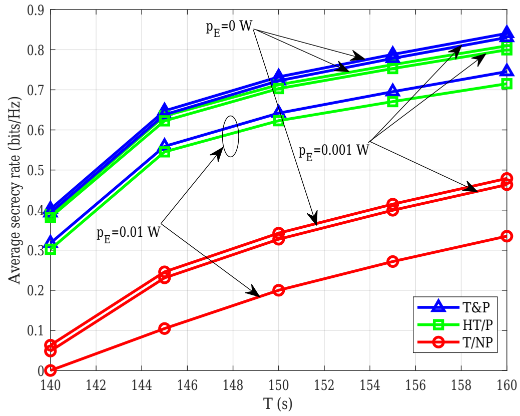

Figure 5. *Average secrecy rate versus T for DL transmission.*

Figure 5 illustrates the average secrecy rate versus T by different schemes with different p_E. It is shown that the average secrecy rates of all schemes increase with T. The reason is that the UAV can stay longer at its hovering location with the optimal trade-off when T is sufficiently large, thus leading to the larger secrecy rates. By comparing with all schemes, we can see that the proposed T&P scheme has the best secrecy rate performance while the T/NP scheme achieves worst. Although the secrecy rates of all schemes reduce with the increase of the jamming power p_E, as expected, their gaps become larger with T, which demonstrates the importance of the proposed joint trajectory and power control design against active eavesdropping. Particularly, by comparing the gains between T&P and T/NP, the results indicate that the transmit power control of the UAV is more effective for improving the secrecy rate performance in DL transmission.

5.2 Uplink Transmission

Figure 6 describes the UAV trajectories by different schemes in UL transmission with different flight period T. It is shown that the UAV trajectories in T&P and T/NP are similar from $\mathbf{q}_0$ to G but different in return trip with different T. Particularly, when T is sufficiently large, i.e., $T = 160$s, we can see that the UAV in T&P and T/NP flies to the left location of G at its maximum speed. At its hovering location, the UAV can arrive at an optimal trade-off to maximize the secrecy rate. However, when returning to its final location, the UAV in T/NP flies with a larger arc, compared to that in T&P. This is because without power control, the UAV in T/NP can only improve its secrecy rate via adjusting its trajectory to prevent it from the serious interference caused by E.

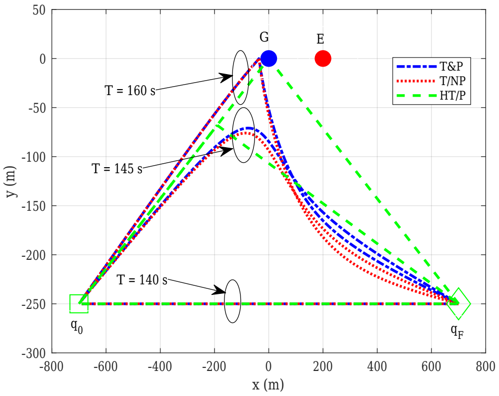

Figure 6. *UAV trajectories by different schemes for UL transmission.*

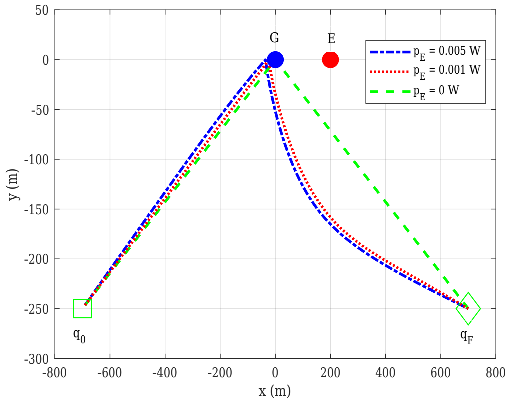

Figure 7. *UAV Trajectories by T&P under different jamming powers for UL transmission.*

Figure 7 illustrates the UAV trajectories by different jamming powers in UL transmission when $T = 160$s. It is observed that the hovering location of the UAV is farther from G when E transmits with higher jamming power. This is because in the UL case, jamming is more dominant in degrading the system performance. As such, the UAV needs to adjust its trajectory to strike a balance between maximizing the data collection rate while minimizing the malicious interference caused by E. Moreover, when the UAV returns to its final location, the UAV subjected to higher jamming power flies with a much larger arc. This indicates that the proposed scheme can effectively utilize the flexible UAV trajectory to prevent the active eavesdropping from the jamming and eavesdropping. Note that the UAV trajectory is same as that in the HT/P scheme when $p_E = 0$W. The reason is that in this case, E only wiretaps the confidential information from G, without sending jamming signals to the UAV. As such, both the jamming and eavesdropping of E have no impact on the UAV trajectory.

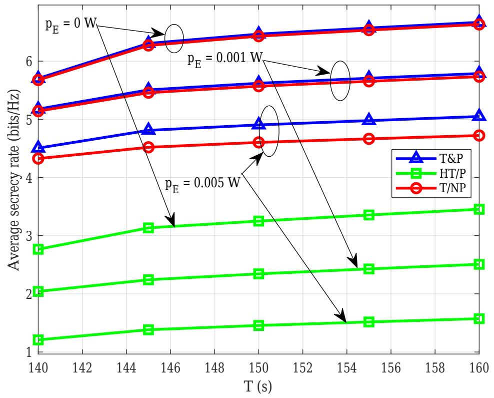

Figure 8. *Average secrecy rate versus T for UL transmission.*

Figure 8 shows the average secrecy rate versus T by different schemes with different p_E. It is observed that the average secrecy rate of the proposed T&P scheme outperforms other benchmark schemes, due to the joint optimization of the UAV trajectory and power control. Moreover, the secrecy rate gaps among all schemes become larger with the increase of p_E, which indicates the dominant role of the anti-active eavesdropping trajectory design. In particular, the larger gaps between T&P and HT/P for higher jamming power demonstrate that in the UL case, the UAV trajectory is more effective in improving secrecy rate performance, compared to the DL case.

VI. CONCLUSION

To tackle the new security challenges from active eavesdropping, in this paper, we studied secure UAV communication issues for both the UL and DL transmissions. We aimed to maximize the average achievable secrecy rates by jointly optimizing the G/UAV's transmit power control and UAV trajectory. To efficiently solve the non-convex optimization problems, we proposed iterative algorithms to cope with them based on BCD and SCA methods. Simulation results demonstrate that the proposed algorithms can improve the secrecy rate performance for both the DL and UL communications, by comparing with other benchmark schemes. Besides, it is shown that power control is more significant in improving the secrecy rate performance for DL transmission while the anti-active eavesdropping UAV trajectory design is more dominant for UL transmission.

Although we focus on securing UAV communications against active eavesdropping, the problem of secure transmission in UAV-assisted NOMA networks can also be solved by following a similar joint trajectory and power control optimization algorithm. In addition, it is interesting to pursue the application of the proposed scheme in urban areas. In this case, the angle-dependent Rician fading channel [23] or the probabilistic LoS channel [24] models can be adopted to design 3D UAV trajectory with both horizontal and altitude location optimization.

ACKNOWLEDGEMENT

This work was partially supported by the National Natural Science Foundation of China (No.61802034), National Key Research and Development Program of China (No. 2019YFC1509602) and Chongqing Natural Science Foundation (cstc2019jcyj-msxmX0264).

NOTES

[1] Since we target for the offline UAV trajectory design, and E also transmits jamming signals besides passive eavesdropping, it can be located by jammer detection methods with high accuracy such as those in [25, 26]. Furthermore, even if E does not send jamming signals, but only passively eavesdrops, its location can be practically detected via a UAV-mounted camera or radar [27, 28].

[2] Since field experiments demonstrate that the LoS probability of the UAV-to-ground channel approaches

to 1 at high altitudes [29–31], we consider LoS channel model for practicality.

References

[1] S. Liu, Z. Wei, *et al.*, "Performance analysis of UAVs assisted data collection in wireless sensor network," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. Porto, Portugal: IEEE, 2018, pp. 1–5.

[2] K. Miyano, R. Shinkuma, *et al.*, "Utility based scheduling for multi-UAV search systems in disaster-hit areas," *IEEE Access*, vol. 7, 2019, pp. 26 810–26 820.

[3] W.-Y. Chen and J.-K. Hu, "Research on drone's aerial photography aided learning system based on deep learning," in *2019 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. Taiwan, China: IEEE, 2019, pp. 1–2.

[4] Y. Wu, W. Fan, *et al.*, "Robust trajectory and communication design for multi-UAV enabled wireless networks in the presence of jammers," *IEEE Access*, vol. 8, 2019, pp. 2893–2905.

[5] Z. Li, M. Chen, *et al.*, "Joint trajectory and communication design for secure UAV networks," *IEEE Communications Letters*, vol. 23, no. 4, 2019, pp. 636–639.

[6] Q. Wang, Z. Chen, *et al.*, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," *IEEE Access*, vol. 6, 2018, pp. 62 849–62 855.

[7] C. Zhong, J. Yao, *et al.*, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Communications Letters*, vol. 23, no. 2, 2018, pp. 286–289.

[8] B. Duo, Q. Wu, *et al.*, "Energy efficiency maximization for full-duplex UAV secrecy communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, 2020, pp. 4590–4595.

[9] G. Zhang, Q. Wu, *et al.*, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, 2019, pp. 1376–1389.

[10] A. Li, Q. Wu, *et al.*, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Communications Letters*, vol. 8, no. 1, 2019, pp. 181–184.

[11] A. Li and W. Zhang, "Mobile jammer-aided secure UAV communications via trajectory design and power control," *China Communications*, vol. 15, no. 8, 2018, pp. 141–151.

[12] F. Cheng, G. Gui, *et al.*, "UAV-relaying-assisted secure transmission with caching," *IEEE Transactions on Communications*, vol. 67, no. 5, 2019, pp. 3140–3153.

[13] W. Duan, J. Ju, *et al.*, "Effective resource utilization schemes for decode-and-forward relay networks with NOMA," *IEEE Access*, vol. 7, 2019, pp. 51 466–51 474.

[14] W. Duan, X.-Q. Jiang, *et al.*, "Two-stage superposed transmission for cooperative NOMA systems," *IEEE Access*, vol. 6, 2018, pp. 3920–3931.

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

[16] H.-M. Wang and X. Zhang, "UAV Secure downlink NOMA transmissions: a secure users oriented perspective," *arXiv preprint arXiv:2006.05202*, 2020.

[17] C. Liu, J. Lee, *et al.*, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, 2019, pp. 2919–2931.

[18] C. Liu, T. Q. Quek, *et al.*, "Secure UAV communication in the presence of active eavesdropper," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*. Nanjing, China: IEEE, 2017, pp. 1–6.

[19] P. K. Gopala, L. Lai, *et al.*, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, 2008, pp. 4687–4698.

[20] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. UK: Cambridge University Press, 2011.

[21] S. Boyd, S. P. Boyd, *et al.*, *Convex optimization*. UK: Cambridge university press, 2004.

[22] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, Version 2.2," http://cvxr.com/cvx, Jan. 2020.

[23] C. You and R. Zhang, "3D trajectory optimization in Rician fading for UAV-enabled data harvesting," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, 2019, pp. 3192–3207.

[24] C. You and R. Zhang, "Hybrid offline-online design for UAV-enabled data harvesting in probabilistic LoS channel," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, 2020, pp. 3753–3768.

[25] M. Hasanzade, O. Herekoglu, *et al.*, "Localization and tracking of RF emitting targets with multiple unmanned aerial vehicles in large scale environments with uncertain transmitter power," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*. Miami, FL, USA: IEEE, 2017, pp. 1058–1065.

[26] S. Bhamidipati and G. X. Gao, "Locating multiple GPS jammers using networked UAVs," *IEEE Internet of Things Journal*, vol. 6, no. 2, 2019, pp. 1816–1828.

[27] S. Minaeian, J. Liu, *et al.*, "Vision-based target detection and localization via a team of cooperative UAV and UGVs," *IEEE Transactions on systems, man, and cybernetics: systems*, vol. 46, no. 7, 2015, pp. 1005–1016.

[28] S. Sohn, B. Lee, *et al.*, "Vision-based real-time target localization for single-antenna GPS-guided UAV," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 44, no. 4, 2008, pp. 1391–1401.

[29] X. Lin, V. Yajnanarayana, *et al.*, "The sky is not the limit: LTE for unmanned aerial vehicles," *IEEE Communications Magazine*, vol. 56, no. 4, 2018, pp. 204–210.

[30] I. Qualcomm Technologies, "LTE unmanned aircraft systems trial report," https://www.qualcomm.com/documents/lte-unmanned-aircraft-systems-trial-report.

[31] D. W. Matolak and R. Sun, "Air–ground channel characterization for unmanned aircraft systems—Part III: The suburban and near-urban environments," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, 2017, pp. 6607–6618.

Biographies

Bin Duo received his Ph.D. degrees in information and communication engineering from Harbin Institute of Technology, China in 2014 and from the University of Sydney, Australia, in 2016. He is currently an Associated Professor of College of Information Science & Technology, Chengdu University of Technology, China. His research interests include modern optimization theory, UAV communications and physical-layer security.

Junsong Luo received the M.S. degree in Applied Mathematics from the Chengdu University of Technology, Chengdu, China, in 2003. He is currently an Associated Professor of the College of Information Science and Technology, Chengdu University of Technology, China. His research interests include signal and information processing, communications and deep learning.

Yilian Li received the B.S. degree in Electrical Information engineering from Chengdu University, Chengdu, China, in 2019. She is currently pursuing the M.S. degree with Information and Communication Engineering, Chengdu University of Technology, China. Her research interests include optimization theory, UAV communications and physical-layer security.

Hao Hu received his B.S. degree from Chengdu Technological University, Chengdu, China, in 2019. He is currently pursuing his M.S. degree at the Chengdu University of Technology. His research interests include convex and non-convex optimization, physical-layer security and UAV communications.

Zibin Wang received his Ph.D. degree in information and communication engineering from National University of Defense Technology, China, in 2012. He is currently a researcher of National Key Laboratory of Science and Technology on Information System Security, Beijing, China. His research interests include wireless networks, satellite communications and physical-layer security.