Robust Trajectory and Resource Allocation Design for Secure UAV-aided Communications

Xiaofang Sun†, Chao Shen‡, Derrick Wing Kwan Ng†, and Zhangdui Zhong‡

*State Key Lab of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
†Beijing Engineering Research Center of High-speed Railway Broadband Mobile Communications, Beijing, China
‡School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia

Email: {xiaofangsun, chaoshen, zhdzhong}@bjtu.edu.cn, w.k.ng@unsw.edu.au

Abstract—This paper aims to enhance the physical layer security against potential internal eavesdroppings by exploiting the maneuverability of an unmanned aerial vehicle (UAV). We consider a scenario where two receivers with different security clearance levels require to be served by a legitimate transmitter with the aid of the UAV. We jointly design the trajectory and resource allocation to maximize the accumulated system confidentiality data rate. The design is formulated as a mixed-integer non-convex optimization problem which takes into account the partial position information of a potential eavesdropper. To circumvent the problem non-convexity, a series of transformations and approximations are proposed which facilitates the design of a computationally efficient suboptimal solution. Simulation results are presented to provide important system design insights and demonstrate the advantages brought by the robust joint design for enhancing the physical layer security.

I. INTRODUCTION

Recently, unmanned aerial vehicle (UAV) has drawn significant interests in wireless communications, due to its high mobility, on-demand of deployment, line-of-sight (LoS) air-to-ground channel, and low cost [1]. Despite the special and unique advantages brought by UAVs, the open and strong LoS nature of air-to-ground channels lead to a high potential in information leakage. As such, security plays an important role in UAV networks. However, traditional encryption techniques require a large amount of energy consumption due to their high computational complexities [2]. As an alternative, physical layer security against potential eavesdroppings is an effective and energy efficient approach to address the security issues in UAV networks by exploiting the randomness of wireless channels from the information theoretic perspective. Consequently, physical layer security has been widely studied in the literature for safeguarding wireless communications, e.g., [3]. On the other hand, the high mobility and flexibility of UAVs can also be exploited to enhance the physical layer security. Hence, a thorough study on the role of UAVs in secure communication systems is necessary.

Recently, the physical layer security in UAV systems has gained increasing attentions in the literature. For example, UAV-aided jamming scheme was proposed to handle the security issues in [4]. Besides, joint trajectory and resource allocation design was investigated in [5]–[7] for improving the system secrecy rate with UAV-mounted base stations and UAV-aided relaying protocols, respectively. However, the previous works are all based on an assumption that accurate position information of eavesdroppers is available at UAVs which is over optimistic. In practice, obtaining such precise position information is challenging and expensive in terms of hardware cost and energy consumption. Then, based on the imperfect channel state information of an external eavesdropper, a robust trajectory design was proposed in [8] for providing secure communications to the UAV-mounted legitimate transmitter. Differently, in this work, we address the security issues caused by an internal eavesdropper with a lower security clearance level and only partial position information available, via exploiting a UAV as a mobile relay.

Inspired by the advantages and challenges brought by UAVs, in this work, we study a robust trajectory and resource allocation design for UAV-aided wireless communications to enhance the physical layer security against internal eavesdrop-pings. In the considered scenario, two ground receivers, named Bob and Eve, respectively, with different security clearance levels desire to be served by a remote transmitter (Alice) in the absence of direct communication links. Specifically, the receiver with a lower security clearance level (Eve) not only imposes a certain QoS requirement on its own messages, but also intends to intercept the messages with a higher security clearance level. To this end, a UAV is introduced as a mobile relay to meet the QoS requirements of different users and to guarantee secure communications simultaneously. In many practical scenarios, obtaining accurate position information of a potential eavesdropper is usually difficult if not impossible. As such, in this work, we exploit partial position information of the potential eavesdropper to facilitate the robust design by considering the worst-case. The joint design of the trajectory and resource allocation is formulated a non-convex optimization problem to maximize the accumulated confidential data rate while ensuring Eve is only able to decode its desired data. To facilitate the joint design, we propose a computationally efficient suboptimal iteration algorithm based on the successive convex approximation (SCA) approach [9]. Moreover, we numerically examine the performance of the proposed robust joint design.

Notation: $\| \cdot \|$ denotes the Euclidean norm. $[x]_a$ denotes the $a$th component of vector $x$. The distribution of a circularly symmetric complex Gaussian (CSCG) variable with mean $\mu$ and variance $\sigma^2$ is denoted by $CN(\mu, \sigma^2)$. $E(\cdot)$ denotes the statistical expectation. $(\cdot)^T$ denotes the transpose operation.
II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

In this paper, the considered secure UAV-aided communication system is modeled by a wiretap channel, as depicted in Fig. 1 where Alice is the legitimate ground transmitter serving two ground users, named Bob and Eve, respectively, with different security clearance levels. Without loss of generality, we assume that Bob has a higher security clearance level while Eve having a lower one. In the considered scenario, the direct communication links from Alice to Bob and to Eve are both assumed to be not available. To address this issue, a UAV is introduced to serve an intelligent relay providing the physical layer security against potential internal eavesdroppings via exploiting the UAV’s maneuverability. Moreover, we assume that the accurate locations of Alice and Bob are known by the UAV. In contrast, only the partial position information of Eve is available for the trajectory and resource allocation design.

We define the maximum flight duration of the UAV by $T$, which mainly depends on the battery capacity, the flight control system, and the flight condition. The three-dimensional (3D) location of the UAV at any certain time is denoted by $q(t) \in \mathbb{R}^3$. Notably, the continuous UAV trajectory leads to infinite many variables, which make the problem intractable. As a result, we adopt a commonly used approach in the literature to facilitate the system design. In particular, we discretize the maximum flight duration $T$ into $N$ time slots with equal time length $T_n$, i.e., $T = NT_n$. Notably, each time slot is sufficiently small such that the flying speed of the UAV within it can be assumed to be constant. Consequently, the UAV’s coordinate at time slot $n$ can be denoted by $q_n \in \mathbb{R}^3$ for $n \in \{1, \cdots, N\}$. The maximum speed of the UAV is denoted by $V_{\text{max}}$. Then, we have the following constraints imposed on UAV in terms of trajectory

$$
\|q_n - q_{n-1}\| \leq D, \quad q_0 = s_I, q_N = s_F, [q_n]_3 = H, \quad \forall n.
$$

We assume that frequency division duplex (FDD) protocol is adopted. Specifically, the uplink (UL) transmission (from Alice to UAV) and the downlink (DL) transmission (from UAV to Bob and Eve) are separated in two orthogonal frequency bands. In addition, the communication bandwidth can be dynamically optimized and allocated to improve the spectral efficiency. Denote the total bandwidth by $B$ Hz, which is adaptively divided into $b_{1,n}$ Hz and $b_{2,n}$ Hz for uplink and downlink transmissions, respectively, in time slot $n$. Hence, we have

$$
b_{1,n} \geq 0, \quad b_{2,n} \geq 0, \quad b_{1,n} + b_{2,n} \leq B, \quad \forall n.
$$

The UAV adopts the cache-aided decode-and-forward (DF) protocol for information relaying. Here, we assume that the cache equipped at the UAV is large enough such that there will be no packet overflow.

Denote the locations of Alice and Bob in a 3D Cartesian coordinate system by $s_a$ and $s_b$, respectively. Without loss of generality, the uncertain ground area of Eve is modeled by a disc with radius $d_e$ centered at $s_e$. According to the filed trial results in [10], the line-of-sight (LoS) component dominates air-to-ground channels in many practical scenarios, especially for rural areas or at moderately high UAV altitude. Hence, the air-to-ground channel between UAV and a ground node $k$ at each time slot can be accordingly modeled by

$$
h_{k,n} = \frac{\gamma_0}{\|q_n - s_k\|}, \quad k \in \{a, b\},
$$

where $\gamma_0$ is the channel power gain at a reference distance of 1 m. To guarantee the communication security, we focus on the worst-case scenario. In particular, the channel gain between the UAV and Eve is bounded by

$$
h_{e,n}^u = \frac{\gamma_0}{d_{e,n}^u} \quad \text{and} \quad h_{e,n}^w = \frac{\gamma_0}{d_{e,n}^w},
$$

which are the upper bound and lower bound, respectively, where

$$
d_{e,n}^u = \|q_n - s_e\|^2 + d_e^2 - 2d_e D_{G,n},
$$

$$
d_{e,n}^w = \|q_n - s_e\|^2 + d_e^2 + 2d_e D_{G,n},
$$

where $D_{G,n} = \sqrt{[\|q_n\| - |s_e|]^2 + [\|q_n\| - |s_e|]^2}$ is the projected distance on the ground.

B. Transmission Strategy

Denote the uplink signal in time slot $n$ from Alice to the UAV by $x_{a,n}$ which contains the messages intended to Bob and/or Eve. The average transmission power satisfies

$$
p_{a,n} \triangleq \mathbb{E}[|x_{a,n}|^2] \leq P_A, \quad n \in \{1, \cdots, N\}.
$$

The received signal at the UAV in time slot $n$ is given by

$$
y_{u,n} = \sqrt{p_{a,n}} x_{a,n} + z_{u,n},
$$

where $z_{u,n} \sim CN(0, \sigma^2)$ denotes the additive white Gaussian noise (AWGN). Without loss of generality, we assume that the received noise powers at all nodes are the same. Then, the uplink capacity from Alice to the UAV in time slot $n$ is

$$
C_{n}^{\text{UA}} = b_{1,n} \ln \left(1 + \frac{\gamma p_{a,n}}{b_{1,n} \|q_n - s_a\|^2}\right) \text{nat/s},
$$

where $\gamma = \gamma_0 / \sigma^2$ is the noise normalized channel power gain.

We denote $R_{u,n}^b$ and $R_{u,n}^e$ as the coding rates from Alice to the UAV for conveying messages to Bob and Eve, respectively.
Thus, \( R_{u,n}^b \) and \( R_{u,n}^e \) are constrained by the achievable uplink capacity, i.e.,

\[
R_{u,n}^b \geq 0, \quad R_{u,n}^e \geq 0, \quad R_{u,n}^b + R_{u,n}^e \leq C_n^{A \rightarrow U}, \quad \forall n.
\] (10)

At the UAV, the received data from Alice is cached in the buffer for forwarding to Bob and Eve separately in the following time slots. Recall that Bob and Eve are both desired to be served but with different secrecy clearance levels. To this end, the two types of signals are transmitted in orthogonal time slots. For the sake of clarity, we introduce a set of binary variables \( \rho_n \), where

\[
\rho_n = \begin{cases} 
1, & \text{the UAV only serves Bob,} \\
0, & \text{the UAV only serves Eve.} 
\end{cases}
\]

1) \( \rho_n = 1 \): The UAV transmits confidential signal \( x_{b,n} \) to Bob but has a potential of leakage to Eve. The transmission power is defined by \( p_{b,n} = \mathbb{E}[\|x_{b,n}\|^2] \). The coding rate of \( x_{b,n} \) is defined by \( R_{b,n} \) nat/s. Due to the open nature of wireless channels, the transmitted signal can be received at both Bob and Eve. Their received signal equations are given by

\[
y_{b,n} = \sqrt{h_{b,n}}x_{b,n} + z_{b,n}, \quad \forall n \in \{b, e\}.
\]

The corresponding channel capacity between the UAV and Bob is

\[
C_n^{U \rightarrow B} = \rho_nb_{2,n} \ln \left( 1 + \frac{\gamma_{b,n}}{b_{2,n}^2 \mathbb{E}[q_{b,n} - s_b^2]} \right) \text{nat/s}. \quad (11)
\]

The potential maximum wiretap channel capacity between the UAV and Eve is given by

\[
C_n^{U \rightarrow E} = \rho_nb_{2,n} \ln \left( 1 + \frac{\gamma_{b,n}}{b_{2,n}^2 d_{c,n}^2 \mathbb{E}[q_{c,n} - s_c^2]} \right) \text{nat/s}. \quad (12)
\]

To ensure the communication reliability at Bob, the coding rate \( R_{b,n} \) is constrained by \( R_{b,n} \leq C_n^{U \rightarrow B} \). Moreover, the corresponding minimum secrecy rate for \( x_{b,n} \) in time slot \( n \) is defined as

\[
R_n^s = [R_{b,n} - C_n^{U \rightarrow E}, R_{b,n}^+]. \quad (13)
\]

2) \( \rho_n = 0 \): The signal \( x_{c,n} \) is intended to Eve from UAV in time slot \( n \) with \( \rho_n = 0 \). Its allocated power and coding rate are defined by \( p_{c,n} = \mathbb{E}[\|x_{c,n}\|^2] \) and \( R_{c,n} \) nat/s, respectively. Likewise the received signal with \( \rho_n = 1 \), for guaranteeing reliable communications, we consider the potential minimum channel capacity of \( x_{c,n} \) at Eve, which is given by

\[
C_n^{U \rightarrow E} = (1 - \rho_n)b_{2,n} \ln \left( 1 + \frac{\gamma_{c,n}}{b_{2,n}^2 d_{c,n}^2 \mathbb{E}[q_{c,n} - s_c^2]} \right) \text{nat/s}. \quad (14)
\]

Similarly, to ensure communication reliability at Eve, the coding rate \( R_{c,n} \) is constrained by \( R_{e,n} \leq C_n^{U \rightarrow E} \).

Recall that the UAV acts as an aerial relay to cache and forward data from Alice to Bob and Eve. Hence, additional information causality constraints [6] in terms of signals to Bob and Eve are imposed on UAV, which are given by

\[
\sum_{i=1}^{n} R_{b,i} \leq \sum_{i=1}^{n} R_{u,i}^b \quad \text{and} \quad \sum_{i=1}^{n} R_{e,i} \leq \sum_{i=1}^{n} R_{u,i}^e, \quad \forall n, \quad (15)
\]

respectively.

We note that the allocated transmission powers \( p_{b,n} \) and \( p_{c,n} \) are limited by the maximum transmission powers of UAV, i.e.,

\[
0 \leq p_{b,n} \leq P_U, \quad 0 \leq p_{c,n} \leq P_U, \quad \forall n. \quad (16)
\]

C. Problem Formulation

In this section, we formulate the resource allocation and trajectory design as an optimization problem. In the considered system, the UAV assists Alice to deliver a certain amount of data to Eve for a given time duration \( T \). We aim to maximize the accumulated confidential data rate achieved at Bob while guaranteeing a minimum required data rate for Eve to decode its own messages. To this end, the resource allocation and trajectory of UAV are to be jointly optimized. Mathematically, the optimization problem is formulated as

\[
\begin{align}
\text{P1:} \quad & \text{maximize} \quad \Delta \sum_{n=1}^{N} R_{n}^b, \\
& \text{s.t.} \quad C_n^{U \rightarrow B} \geq R_{b,n}, \quad \forall n, \\
& \quad C_n^{U \rightarrow E} \geq R_{e,n}, \quad \forall n, \\
& \quad \sum_{n=1}^{N} R_{e,n} \geq R_E, \\
& \quad \rho_n \in \{0,1\}, \quad \forall n, \\
& \quad (1), (2), (7), (10), (15), (16),
\end{align}
\]

where \( \Delta = \{\Delta_1, \{b_{2,n}, p_{a,n}, p_{b,n}, p_{c,n}, \rho_n\}_{n=1}^{N}\} \) and \( \Delta_1 = \{b_{1,n}, q_{b,n}, R_{u,n}, R_{b,n}, R_{e,n}\}_{n=1}^{N} \) are the sets of optimization variables. \( R_E \) is the minimum required data rate for Eve to decode its own message. The considered optimization formulation is a generalization of existing ones in the literature. For example, external eavesdropping, e.g., [7], and complete position information of the eavesdropper, e.g., [5], are two special cases of this framework with \( R_E = 0 \) and \( d_e = 0 \), respectively.

III. Joint Trajectory and Resource Allocation Design Strategy

The considered optimization problem P1 is a mixed-integer programming which is NP-hard in general [11]. In particular, the optimization variables are coupled together resulting in an intractable problem. To tackle P1 in (17), we first provide some useful insights to simplify the problem at hand. Then, we propose a series of transformations and approximations to facilitate the design of a suboptimal solution.

A. Simplifications of the Optimization Problem P1

In particular, without loss of optimality, the uplink and downlink transmissions in each time slot fully occupy the total bandwidth, i.e., \( b_{1,n} + b_{2,n} = B, \forall n \). This is due to the fact that if the bandwidth allocation satisfies \( b_{1,n} + b_{2,n} < B \) with strict inequality in some time slots, the objective function may be further increased by allocating the available bandwidth to the uplink and/or downlink channels subject to the constraints.

Then, to further facilitate the joint design, in the following lemma, we discuss the optimal transmission strategy for secure communications adopted at the UAV.

Lemma 1: If the UAV locates closer to Bob than Eve, i.e., \( \|q_{a} - s_b\|^2 < \|q_{a} - s_e\|^2 + d_e^2 - 2d_e D_{C,n} \), the optimal strategy is to transmit confidential signal with \( \rho_n = 1 \). Otherwise, the UAV either caches data from the uplink channel or delivers data with a lower security clearance level to Eve.
By exploiting this lemma, the objective function given in (17a) can be simplified to:

\[ \sum_{n=1}^{N} R_{b,n} - C_{b,n}^{U\rightarrow E}. \]  

(18)

We note that \( \rho_n \) is a binary optimization variable in \( P_1 \) and additionally coupled with other variables. Now, by exploiting the binary property of \( \rho_n, C_{n}^{U\rightarrow B} \) in \( P_1 \) can be equivalently written as:

\[ C_{n}^{U\rightarrow B} = \rho_n b_{2,n} \ln \left( 1 + \frac{\gamma p_{b,n}}{\rho_n b_{2,n} \| q_n - s_b \|^2} \right). \]  

(19)

This can be proved directly when \( \rho_n = 1 \) and via the L’Hospital’s rule when \( \rho_n = 0 \).

Furthermore, we introduce two auxiliary optimization variables \( \eta_n \geq 0 \) and \( \tau_n \geq 0 \) to replace \( \rho_n b_{2,n} \) and \( (1 - \rho_n) b_{2,n} \), respectively. To this end, two types of constraints are imposed on the new variables, which are given by:

\[ \tau_n = B - b_{1,n} - \eta_n, \quad \rho_n \geq 0, \quad \eta_n \geq 0, \quad \forall n, \]  

(20a)

\[ \eta_n \tau_n \leq 0, \quad \forall n. \]  

(20b)

These constraints guarantee that the UAV serves Bob and Eve with orthogonal time slots. Notably, \( \eta_n \) and \( \tau_n \) are coupled in (20b) which is non-convex and to be addressed in the following sections.

**B. Transformation of the Optimization Problem \( P_1 \)**

We note that the optimization variables are still coupled in constraints (10), (17b), (17c), (18), (20b). In this section, we transform the optimization problem \( P_1 \) into its equivalent form to facilitate the computationally efficient resource allocation and trajectory design. To this end, we first introduce some auxiliary optimization variables \( \mu_{a,n}, \mu_{b,n}, \) and \( \mu_{e,n} \) to bound \( \| q_n - s_a \|^2, \| q_n - s_b \|^2, d_{e,n}^{\psi} \) from above, respectively. As a consequence, some additional constraints are imposed on the auxiliary variables, which are given by:

\[ \| q_n - s_a \|^2 \leq \mu_{a,n}, \quad \mu_{a,n} \geq 0, \quad \forall n, \]  

(21a)

\[ \| q_n - s_b \|^2 \leq \mu_{b,n}, \quad \mu_{b,n} \geq 0, \quad \forall n, \]  

(21b)

\[ d_{e,n}^{\psi} \leq \mu_{e,n}, \quad \mu_{e,n} \geq 0, \quad \forall n. \]  

(21c)

Inspired by the fact that a quadratic-over-linear function is convex with respect to its positive inputs, respectively [12], we introduce some new variables \( \alpha_{a,n} \geq 0, \alpha_{b,n} \geq 0, \) and \( \alpha_{e,n} \geq 0 \) to replace \( \sqrt{\mu_{a,n}}, \sqrt{\mu_{b,n}}, \) and \( \sqrt{\mu_{e,n}}, \) respectively.

We then introduce a set of auxiliary variables \( \theta_n \geq 0 \) to bound \( \frac{\alpha_{a,n}}{\alpha_{b,n}} \) from above. As such, the constraint imposed on the new variable is given by

\[ \frac{\alpha_{a,n}}{\alpha_{b,n}} + 2d_e D_{G,n} \leq \| q_n - s_e \|^2 + d_e^2, \quad \theta_n \geq 0, \quad \forall n. \]  

(22)

Based on the previous transformations, the optimization problem \( P_1 \) is transformed into its equivalent form, which is given by

\[ \begin{align*}
\max_{\Delta_2} & \sum_{n=1}^{N} R_{b,n} - \eta_n \ln \left( 1 + \frac{\gamma \alpha_{b,n}^{2}}{\eta_n} \right), \\
\text{s.t.} & R_{u,n}^b + R_{u,n}^e \leq b_{1,n} \ln \left( 1 + \frac{\gamma \alpha_{a,n}^{2}}{b_{1,n} \mu_{a,n}} \right), \quad \forall n, \\
& \tau_n \ln \left( 1 + \frac{\gamma \alpha_{e,n}^{2}}{\tau_n \mu_{e,n}} \right) \geq R_{e,n}, \quad \forall n, \\
& \alpha_{a,n}^2 \leq P_A, \quad \alpha_{b,n}^2 \leq P_U, \quad \alpha_{e,n}^2 \leq P_U, \quad \forall n, \\
& \eta_n \geq 0, \quad \tau_n \geq 0, \quad \forall n, \\
& \rho_n \in \{0, 1\}, \quad \forall n.
\end{align*} \]  

(23a)

where \( \Delta_2 := \{ \Delta_1 \}, \) is the new optimization variable set. However, the objective function (23a) and constraints (20b), (22), (23b), (23c), and (23d) are still non-convex, due to the coupling variables. In the following section, we focus on the approximations of these non-convex objective function and constraints.

**C. Approximations of the Optimization Problem \( P_2 \)**

In this section, we convexify the non-convex objective function and constraints via the SCA approach [13].

1) SCA Method Based on the First-Order Taylor Expansion: We note that the non-convex functions in the constraints (23b), (23c), and (23d) are desired to be approximated to concave functions. To this end, the SCA approach based on the first-order Taylor expansion is employed. In particular, \( \frac{\alpha_{k,n}^2}{\mu_{k,n}} \) is convex with respect to \( \alpha_{k,n} \) and \( \mu_{k,n} \), respectively, where \( k \in \{a, b, e\} \). Thus, for any fixed point in the \( n \)th iteration \( \alpha_{k,n}^* \geq 0 \) and \( \mu_{k,n}^* \geq 0 \), \( \alpha_{k,n}^2 \) can be bounded from below, i.e.,

\[ \frac{\alpha_{k,n}^2}{\mu_{k,n}^*} \geq R_{k,n} \triangleq \frac{2\alpha_{k,n}^*}{\mu_{k,n}^*} \alpha_{k,n}^* - \frac{(\alpha_{k,n}^* \mu_{k,n})^2}{(\mu_{k,n}^*)^2}, \]  

As a result, the constraints (23b), (23c), and (23d) are approximated to

\[ \begin{align*}
& b_{1,n} \ln \left( 1 + \frac{\gamma R_{a,n}}{b_{1,n}} \right) \geq R_{u,n}^b + R_{u,n}^e, \quad \forall n, \\
& \eta_n \ln \left( 1 + \frac{\gamma R_{b,n}}{\eta_n} \right) \geq R_{b,n}, \quad \forall n, \\
& \tau_n \ln \left( 1 + \frac{\gamma R_{e,n}}{\tau_n} \right) \geq R_{e,n}, \quad \forall n,
\end{align*} \]  

(24a)

(24b)

(24c)

respectively, which are convex, since perspective functions preserve convexity [12].
Moreover, the second term on the left-hand side of the objective function (23a) desires to be approximated to a convex function and the associated constraint (22) is to be approximated to a concave one. To this end, by employing the first-order Taylor expansion, the objective function (23a) and the constraint are approximated to

\[
\tilde{R}_n^a \triangleq R_{b,n} - \eta_n \ln \left(1 + \frac{\theta_n}{\eta_n} \right) - \frac{\alpha_{b,n}^2 + \theta_n}{\eta_n} \frac{\partial \alpha_{b,n}}{\partial \theta_n} + \theta_n, \]

\[
\frac{\alpha_{b,n}^2 + 2d_c D_{G,n} - d_c^2}{\theta_n} \leq \left\| q_n^a - s_n \right\|^2 + 2r(q_n - q_n^a), \forall n. \quad (25)
\]

where \( r \triangleq (q_n^a)^T - s_n^T, \theta_n, \eta_n, \) and \( q_n^a \) are fixed points in the \( r \)th iteration.

2) SCA Method Based on Arithmetic-Geometric Mean (AGM) Inequality: Notably, constraint (20b) is bilinear with respect to \( \tau_n \) and \( \psi_n \), respectively. For handling the bilinear function, we adopt the SCA approach based on AGM Inequality. As such, the non-convex bilinear function is sequentially upper bounded by a convex one, i.e., \( \eta_n \tau_n \leq \frac{1}{2} \left( \frac{\eta_n^2}{\psi_n^2} + (\tau_n \psi_n)^2 \right), \forall n \), where \( \psi_n \geq 0 \) is a fixed point for tightening the upper bound, which is updated by \( \psi_n^{r+1} = \sqrt{\frac{2\tau_n}{\eta_n}} \) in the \( r \)th iteration. Consequently, the non-convex constraint (20b) can be safely replaced by

\[
\frac{1}{2} \left( \frac{\eta_n^2}{\psi_n^2} + (\tau_n \psi_n)^2 \right) \leq 0, \forall n. \quad (26)
\]

Specifically, we find that the non-convex feasible set is approximated by a convex set which only contains one possibility, i.e., \( \eta_n = 0 \) and \( \tau_n = 0, \forall n \). However, this possible solution violates constraint (17d) for guaranteeing the QoS requirement of Eve. To address this issue, we augment (26) into the objective function via introducing a set of penalty factor \( \lambda_n \gg 0 \) to obtain an equivalent form.

Based on the previous approximations, the optimization problem \( P_2 \) in (25) has been approximated to a convex one, which is given by

\[
P_2: \maximize \Delta_2 \triangleq \sum_{n=1}^{N} \sum_{a=1}^{N} \lambda_n \left( \frac{\eta_n^2}{\psi_n^2} + (\tau_n \psi_n)^2 \right)
\]

s.t. (1), (2), (15), (17d), (20a), (21), (23a), (24), (25).

The above optimization problem \( P_2 \) is convex given the fixed points and can be solved efficiently by off-the-shelf convex solvers, e.g., CVX [14].

We note that \( \lambda_n \) is updated by adopting gradient descent method [15]. Specifically, at the \( r \)th iteration, \( \lambda_n^r \) is updated by \( \lambda_n^{r+1} = \lambda_n^r + \delta_n \left( \frac{\eta_n^2}{\psi_n^2} + (\tau_n \psi_n)^2 \right), \) where \( \delta_n \geq 0 \) is the \( r \)th step size.

Based on the concept of SCA [9], the fixed points are iteratively updated in the \( r \)th iteration as

\[
\alpha_{k,n}^r = \alpha_{k,n}, \mu_{k,n}^r = \mu_{k,n}, \forall n, k \in \{a, b, e\},
\]

\[
\theta_n^r = \theta_n, \eta_n^r = \eta_n, q_n = q_n^a, \forall n.
\]

Therefore, we obtain the SCA-based iterative algorithm for problem (27), as summarized in Algorithm 1 in which we define \( \Gamma_1 \) as

\[
\Gamma_1 \triangleq \{ (\alpha_{a,n}, \alpha_{b,n}^r, \alpha_{r,n}^r, \mu_{a,n}^r, \mu_{b,n}^r, \mu_{e,n}^r, \theta_{n}^r, \eta_n^r, q_n^a) \}_{n=1}^{N} \}.
\]

Based on the results in [16], the proposed SCA-based algorithm can converge to a stationary Karush-Kuhn-Tucker point. Hence, the algorithm is able to achieve a suboptimal solution of \( P_1 \) with polynomial-time computational complexity.

### IV. Numerical Results

In this section, we numerically examine the secure performance of the proposed transmission strategy. In the simulation, all nodes are located in a 3D Cartesian coordinate system. Without loss of generality, Alice and Bob are set to be located at \((0, 0, 0)\) and \((5 \text{ km}, 0, 0)\), respectively. The initial and final locations of the UAV are located at \((-2 \text{ km}, 1 \text{ km}, 0.1 \text{ km})\) and \((6 \text{ km}, 1 \text{ km}, 0.1 \text{ km})\), respectively. The reference channel power gain at distance one meter and the noise power are set as \( \gamma_0 = -50 \text{ dB} \) and \( \sigma^2 = -150 \text{ dBm/Hz} \), respectively. The communication bandwidth is set as \( B = 10 \text{ MHz} \). The maximum flight duration is set as \( T = 450 \text{ s} \). The maximum speed of the UAV and the time slot duration are set as \( V_{\text{max}} = 20 \text{ m/s} \) and \( T_s = 10 \text{ s} \), respectively. The maximum power budget at Alice and the UAV are set as \( P_A = 30 \text{ dBm} \) and \( P_U = 27 \text{ dBm} \), respectively.

![Fig. 2. Trajectory of the UAV with different targets data rate of Eve, i.e., \( R_E = 100 \text{ Mbps} \) and \( R_E = 50 \text{ Mbps} \) with \( s_e = (4 \text{ km}, 0.5 \text{ km}, 0) \), \( d_e = 0.3 \text{ km} \).](image-url)
In Fig. 2 we plot the optimized trajectory of the UAV against the potential internal eavesdropping. For the sake of observation, the projected ground locations of Alice, Bob, initial and final points of UAV are displayed with makers while the uncertain area of Eve is shaded. From this figure, we can observe that the UAV first tries to approach Alice for data caching as much as possible, and then flies towards Eve for completing data delivery mission. After that, UAV flies away Eve to Bob and hovers above Bob for secure communications with the best-effort. Finally, UAV flies back to its final location with its full speed. Moreover, we find that when the accumulated data rate requirement of Eve becomes more stringent, the UAV has to spend more time and power resources on serving Eve. For example, the UAV needs to hover above the central point of Eve’s uncertain area when the data requirement of Eve is high, e.g., $R_E = 100$ Mbps, while only flying close to Eve’s uncertain area with a relatively high speed when $R_E = 50$ Mbps. Finally, we find that the cruising duration significantly limited the performance of UAV, as UAV may not have enough time slots to hover above Alice and Bob for data caching and delivery, respectively.

In Fig. 3, we compare the performance of the proposed joint design strategy with two strategies which serve as benchmarks. In fixed bandwidth strategy, the total bandwidth allocated to uplink and downlink transmission is fixed and equally divided, i.e., $b_{1,n} = 0.5B$ and $b_{2,n} = 0.5B, \forall n$. In fixed time slot strategy, the total time slots are equally allocated to Bob and Eve separately. From this figure, we find that the proposed joint design strategy always outperforms the other two. This is due to the fact that the proposed joint design exploits more degrees of freedom by adaptively adjusting the optimization variables. For example, when the UAV approaches Alice for caching data, the proposed joint design tends to adaptively allocate more bandwidth resources to the uplink transmission. Moreover, when secure communication can be guaranteed by optimizing the trajectory, the proposed design would allocate more time slots and power resources for transmitting confidential data as much as possible. Furthermore, we find that the maximum accumulated confidential data rate achieved at Bob monotonically decreases with the increasing uncertainty of Eve’s position. The reasons are twofold. With the increasing uncertainty of Eve’s position, the UAV is forced to make a longer detour and reduce its transmit power for communicating with Bob, when it is close to the uncertain region leading to a smaller secrecy rate. On the other hand, the resource allocation also tends to allocate more time slots and power to convey the messages to Eve for meeting its QoS requirement, which leads to a further decreasing performance achieved at Bob.

V. Conclusion

In this work, we have investigated the robust physical layer security against internal eavesdropping in a UAV-aided wireless communications system. The optimization problem is formulated as a generalization of existing ones to improve the secrecy rate while guaranteeing a minimum required data rate for the internal eavesdropper by jointly designing UAV’s trajectory and resource allocation. To tackle the difficulties brought by the formulated non-convex NP-hard problem, we have exploited the properties of the problem to simplify the formulation. Then, a series of transformations and approximations have been proposed to facilitate the design of a computationally efficient suboptimal resource allocation algorithm. Numerical results have demonstrated the advantages brought by the joint design for enhancing the physical layer security in communication systems.

References

[1] 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,” *IEEE Trans. Commun.*, accepted to appear 2019.
[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.
[3] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, “A survey on multiple-antenna techniques for physical layer security,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.
[4] C. Zhong, J. Yao, and J. Xu, “Secure UAV communication with cooperative jamming and trajectory control,” *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.
[5] X. Sun, C. Shen, T.-H. Chang, and Z. Zhong, “Joint resource allocation and trajectory design for UAV-aided wireless physical layer security,” in *Proc. IEEE Globecom workshops*, Abu Dhabi, Dec. 2018.
[6] 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. 62 849–62 855, 2018.
[7] G. Zhang, Q. Wu, M. Cui, and R. Zhang, “Securing UAV communications via trajectory optimization,” in *Proc. IEEE Globecom*, Singapore, Dec. 2017, pp. 1–6.
[8] 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.
[9] X. Sun, N. Yang, S. Yan, Z. Ding, D. W. K. Ng, C. Shen, and Z. Zhong, “Joint beamforming and power allocation in downlink NOMA multiuser MIMO networks,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5367–5381, Aug. 2018.
[10] 3GPP, “Technical specification group radio access network: Study on enhanced LTE support for aerial vehicles,” 3rd Generation Partnership Project (3GPP), Technical Report (TR) 36.777, 2017, version 15.0.0.
[11] D. W. K. Ng, Y. Wu, and R. Schober, “Power efficient resource allocation for full-duplex radio distributed antenna networks,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2896–2911, Apr. 2016.
[12] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.
[13] S. Boyd, L. Xiao, A. Mutapic, and J. Mattingley, “Sequential convex programming, notes for EE364b Stanford University,” [Online]. Available: http://www.stanford.edu/class/EE364b/, 2007.
[14] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming, version 2.1.” http://cvxr.com/cvx Mar. 2014.
[15] S. Boyd, “Subgradient methods,” 2014. [Online]. Available: https://web.stanford.edu/class/ee364b/lectures/subgrad_method_notes.pdf
[16] M. Razaviyayn, M. Hong, and Z.-Q. Luo, “A unified convergence analysis of block successive minimization methods for nonsmooth optimization,” SIAM J. Optim., vol. 23, no. 2, pp. 1126–1153, 2013.