Robust Secure UAV Communications with the Aid of Reconfigurable Intelligent Surfaces
Sixian Li, Bin Duo, Marco Di Renzo, Meixia Tao, Xiaojun Yuan

To cite this version:
Sixian Li, Bin Duo, Marco Di Renzo, Meixia Tao, Xiaojun Yuan. Robust Secure UAV Communications with the Aid of Reconfigurable Intelligent Surfaces. IEEE Transactions on Wireless Communications, 2022, 20 (10), pp.6402 - 6417. 10.1109/TWC.2021.3073746 . hal-03838705

HAL Id: hal-03838705
https://hal.science/hal-03838705
Submitted on 3 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Robust Secure UAV Communications with the Aid of Reconfigurable Intelligent Surfaces

Sixian Li, Bin Duo, Member, IEEE, Marco Di Renzo, Fellow, IEEE, Meixia Tao, Fellow, IEEE, and Xiaojun Yuan, Senior Member, IEEE

Abstract—This paper investigates a novel unmanned aerial vehicles (UAVs) secure communication system with the assistance of reconfigurable intelligent surfaces (RISs), where a UAV and a ground user communicate with each other, while an eavesdropper tends to wiretap their information. Due to the limited capacity of UAVs, an RIS is applied to further improve the quality of the secure communication. The time division multiple access (TDMA) protocol is applied for the communications between the UAV and the ground user, namely, the downlink (DL) and the uplink (UL) communications. In particular, the channel state information (CSI) of the eavesdropping channels is assumed to be imperfect. We aim to maximize the average worst-case secrecy rate by the robust joint design of the UAV’s trajectory, RIS’s passive beamforming, and transmit power of the legitimate transmitters. However, it is challenging to solve the joint UL/DL optimization problem due to its non-convexity. Therefore, we develop an efficient algorithm based on the alternating optimization (AO) technique. Specifically, the formulated problem is divided into three sub-problems, and the successive convex approximation (SCA), S-Procedure, and semidefinite relaxation (SDR) are applied to tackle these non-convex sub-problems. Numerical results demonstrate that the proposed algorithm can considerably improve the average secrecy rate compared with the benchmark algorithms, and also confirm the robustness of the proposed algorithm.

Index Terms—UAV secure communication, reconfigurable intelligent surface, robust trajectory design, robust passive beamforming, robust power control.

I. INTRODUCTION

With the rapid growth of the number of network devices, it is expected that the overall mobile data traffic will reach astoundingly up to 77 exabytes per month by 2022 [1], which undoubtedly poses a tremendous challenge for current mobile communication networks. To meet these explosive demands, innovative wireless transmission technologies have been investigated in the past few years, such as unmanned aerial vehicles (UAVs) [2]–[4], reconfigurable intelligent surfaces (RISs) [5]–[9] and so on. Due to UAVs’ high mobility, they can be flexibly deployed to enhance the communication quality, while conventional terrestrial base stations (BSs) only serve the ground users in a fixed area. In addition, UAVs usually fly at a high altitude compared with the terrestrial infrastructure, which makes the transmission links between the UAV and the ground devices line-of-sight (LoS) dominated [10]. Thanks to these advantages, UAVs are expected to play a key role in beyond fifth generation (5G) and sixth generation (6G) networks [11], [12]. In the majority of research on UAV communications, secrecy is one of the key research areas, in which authors focus on enhancing the secure communication quality via the joint optimization of the UAV trajectory and communication resource allocation. For instance, the authors of [4] considered a simplified secure UAV communication system and maximized the average secrecy rate of the system via joint trajectory and power control design. The authors of [13] used a UAV as a jammer to transmit interfering signals to an eavesdropper, so as to improve the secrecy rate performance. A novel UAV-enabled secure communication system with cooperative jamming has been studied in [14]–[17], where one UAV acts as the legitimate transmitter and sends confidential data to the users, while another UAV acts as the jammer that delivers artificial noise (AN) to the eavesdroppers to weaken the quality of the eavesdropping channels. In particular, in [15]–[17], the scenario with multiple users and eavesdroppers was investigated, where the authors aimed at 7 maximizing the minimum secrecy rate among the legitimate users by jointly optimizing the UAV trajectory and corresponding communication resource allocation. In addition, the robust trajectory and transmit power design were studied in [18], and the S-Procedure method was used to efficiently solve the location uncertainty of the eavesdropper.

Benefiting from improving the propagation environment and enhancing the signal strength, RISs have been widely investigated as the technology enabler for realizing smart radio environments in the near future [19]–[22]. In general, an RIS is comprised of energy-efficient and cost-effective reconfigurable passive elements. Each element of the RIS can induce a phase shift on the incident signal by using a smart controller. Hence, with the aid of an RIS, the signals from different communication links can be added coherently at the desired receiver to enhance the received signal energy or can be added destructively at undesired receivers to avoid the information leakage [23]. This is also called passive beamforming. Due to the peculiar property of modifying the wireless propagation environment, RIS-assisted secure communication systems have attracted much attention [24]–[28]. In [24], the authors investigated a simplified RIS-aided secure
Although a passive eavesdropper always stays silent, it may send signals assumed that the channel state information (CSI) of the eavesdropping channels was not perfectly known at the BS. Hence, a joint and robust design of the beamforming (including active beamforming at the BS and passive beamforming at the RISs) and the AN covariance matrix was proposed to maximize the system sum-rate under a given information leakage threshold.

From the above discussion, UAVs can provide LoS dominant transmission links with the ground users, thanks to their high mobility, while RISs can achieve passive beamforming by adjusting their reflecting elements smartly. Recently, the design of RIS-assisted UAV communication systems has attracted increasing attention. In [29], an RIS was utilized to assist the UAV relay system, and the simulation results demonstrated that deploying RISs could significantly improve the coverage and reliability of UAV communication systems. In [30], a UAV was used as the mobile BS to serve the ground user with the assistance of an RIS. The authors aimed at maximizing the average achievable rate by the joint optimization of the UAV trajectory and RIS’s passive beamforming, and derived a closed-form solution of the RIS’s phase-shift matrix for any given UAV trajectory. In [31], an RIS was placed on the UAV to assist the users whose LoS path is blocked. Then, an efficient algorithm based on the reinforcement learning technique was proposed to solve the DL transmission capacity maximization problem. Similarly, in [32], a UAV equipped with an RIS was leveraged to achieve uplink secure communications. Based on the reinforcement learning method, the authors of [33] proposed a deep Q-network (DQN)-based algorithm to design the UAV’s trajectory and RIS’s passive beamforming to maximize the weighted fairness and data rate among all users. Additionally, the authors of [34] accounted for multiple RISs and a multi-antenna UAV, and maximized the received power by jointly optimizing passive beamforming, active beamforming, and the UAV’s trajectory. The authors of [35] studied a UAV-assisted RIS symbiotic radio system, where the UAV helped multiple RISs for their own information transmission. Based on statistical CSI, the problems of maximizing the minimum average rate and the weight sum rate over all RISs were solved, respectively, by the joint design of the UAV trajectory, RISs’ passive beamforming, and RISs’ scheduling.

It is observed that among the current works on RIS-aided UAV communications, there exists very limited research on the design of secure communication systems. Furthermore, in the existing RIS-aided UAV secure communication systems, it is assumed that the perfect CSI of the eavesdropping channels is known. This assumption may not be easy to be met in practice since the eavesdroppers always avoid being detected by the legitimate transmitters, so as to intercept the legitimate information transmission successfully. Motivated by this, in this paper, we investigate a novel RIS-aided UAV secure communication system as shown in Fig. 1 where the UAV flies over a given flight period to serve the ground user, and the ground user also uploads some messages to the UAV, while a potential eavesdropper intends to wiretap their communications. However, in complex urban environment, the quality of the secure information transmission may be poor. Thus, an RIS is leveraged to enhance the communication quality of the legitimate links and weaken that of the eavesdropping links. Specifically, the entire flight duration is divided into time slots. We assume that the time division multiple access (TDMA) protocol is applied. As a result, we divide each time slot into two parts, i.e., one for the downlink (DL) transmission and the other for the uplink (UL) transmission, where the UAV and the ground user are the legitimate transmitter (receiver) and receiver (transmitter), respectively. Since the eavesdropper always avoids to be detected as possible as it can, accurate estimates of the CSI of the eavesdropping links are usually not available. Hence, we assume imperfect CSI acquisition of the eavesdropping channel, and use a deterministic model to describe the CSI uncertainty. Under these assumptions, a robust joint design of the UAV’s trajectory, RIS’s passive beamforming, and the transmit power control of the legitimate transmitter is formulated as a non-convex joint UL/DL optimization problem for maximizing the average worst-case secrecy rate. The considered problem is difficult to solve due to its non-convexity. We first address its non-smooth objective function and transform the formulated problem into an equivalent problem based on the results in [4]. For the reformulated problem, however the corresponding optimization variables are coupled, which leads to a non-convex optimization problem. To tackle this difficulty, we propose an efficient algorithm based on the alternating optimization (AO) technique. More precisely, the reformulated problem is divided into three sub-problems: 1) transmit power control design for a given UAV trajectory and passive beamforming design; 2) passive beamforming design for a given UAV trajectory and transmit power control design; 3) UAV trajectory design for a given passive beamforming and transmit power control design. For sub-problem 1, we compute the optimal transmit

1In our paper, we assume that before the UAV starts moving, the ground user has achieved the uplink timing synchronization and has been allocated the corresponding radio resources by using random access (RA) schemes generally used in the long term evolution (LTE) and LTE advanced (LTE-A).

2Although a passive eavesdropper always stays silent, it may send signals to its dedicated wireless system. In this case, the signal leakage from the eavesdropper to the legitimate transmitter can be used for channel estimation. Furthermore, it is demonstrated that the eavesdropper’s location can be practically detected via a UAV-mounted camera or radar.
power control design according to the special structure of the objective function. Then, for sub-problem 2, we utilize the S-Procedure and successive convex approximation (SCA) techniques to handle the CSI uncertainty and the non-concave objective function, respectively. Finally, it is challenging to account for the CSI uncertainty and the small-scale fading component of the channel between the UAV and RIS. To cope with these challenges, we use the UAV trajectory of the previous iteration to estimate the current small-scale fading component of the channel between the UAV and RIS and the worst-case setup of the eavesdropping links. Then, the SCA method is applied to solve the optimization sub-problem efficiently. Simulation results demonstrate that our proposed algorithm can significantly increase the average secrecy rate, as compared to benchmark algorithms.

The remainder of this paper is organized as follows. In Section II, we present the system model and problem formulation. In Section III, we propose efficient algorithms based on the AO technique to solve the formulated joint UL/DL optimization problem. Simulation results are illustrated in Section IV. Finally, we conclude the paper in Section V.

Fig. 1. A RIS-assisted UAV secure communication system.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

As shown in Fig. 1, we consider a UAV-enabled communication system where a rotary-wing UAV and a ground user communicate with each other, while an eavesdropper attempts to intercept their legitimate communications. Due to the limited capacity of the UAV, the performance of such secure communication may be low. Thus, we use a building-mounted RIS to assist the secure data transmission. It is assumed that control and non-payload communications (CNPC) link\(^3\) are constructed between the UAV, the RIS and the ground user for the transmission of the control signals.

Without loss of generality, we assume that all communication nodes are placed in the three dimensional (3D) Cartesian coordinate system. The ground user’s and the eavesdropper’s horizontal coordinates are denoted by \(w_G = [x_G, y_G]^T\) and \(w_E = [x_E, y_E]^T\), respectively. The UAV is assumed to fly at a constant altitude denoted by \(z_U\) for a given flight period denoted by \(T\). For tractability, \(T\) is discretized into \(N\) time slots, namely, \(T = N \delta_t\), where \(\delta_t\) is the time slot length. Therefore, the UAV’s time-varying horizontal trajectory is denoted as the sequence \(q[n] = [x[n], y[n]]^T, n \in \mathbb{N} \triangleq \{1, \ldots, N\}\), which should meet the following mobility constraints:

\[
||q[n+1] - q[n]||^2 \leq D^2, n = 1, \ldots, N - 1,
\]

\[
||q[N] - q_F||^2 \leq D^2, q[1] = q_0,
\]

where \(q_0\) and \(q_F\) are the predetermined initial and final horizontal locations of the UAV, respectively, \(D = v_{\text{max}} \delta_t\) is the maximum horizontal distance that the UAV can fly in \(\delta_t\), and \(v_{\text{max}}\) is the maximum speed of the UAV. We assume that the UAV, the ground user, and the eavesdropper are equipped with a single-antenna. The RIS is equipped with \(M = M_x \times M_z\) reflecting elements, forming an \(M_x \times M_z\) uniform rectangular array (URA), and a controller that can intelligently adjust the phase shift of each element. The RIS is located in the \(x-z\) plane, and its altitude and horizontal coordinates are denoted by \(z_R\) and \(w_R = [x_R, y_R]^T\), respectively. \(\text{diag}(\bm{x})\) denotes a diagonal matrix in which each diagonal element is the corresponding element in \(\bm{x}\). The diagonal phase-shift matrix for the RIS in the time slot \(n\) is denoted by \(\Theta[n] = \text{diag}(e^{j\theta_1[n]}, e^{j\theta_2[n]}, \ldots, e^{j\theta_M[n]})\), where \(\theta_i[n] \in [0, 2\pi), i \in \mathcal{M} \triangleq \{1, \ldots, M\}\), is the phase shift of the \(i\)th reflecting element within a single time slot.

To ensure the mutual communication between the UAV and the ground user, we assume that the TDMA protocol is applied for them. Specifically, we utilize a weighted factor \(w \in [0, 1]\) to divide a single flight time slot into two parts: \(w\delta_t\) for the DL transmission in which the UAV serves the ground user, and \((1-w)\delta_t\) for the UL transmission in which the ground user uploads data that the UAV intends to harvest. The details are specified as follows.

1) DL Transmission: In this case, the UAV and the ground node serve as the legitimate transmitter and receiver, respectively. Let \(p[n]\) denote the transmit power of the UAV in time slot \(n\). In practice, \(p[n]\) is usually subject to both average and peak limits over time, denoted by \(\bar{P}\) and \(P_{\text{peak}}\), respectively. Thus, the transmit power constraints are expressed as

\[
\frac{1}{N} \sum_{n=1}^{N} p[n] \leq \bar{P},
\]

\[
0 \leq p[n] \leq P_{\text{peak}}, \forall n.
\]

We assume the Rician fading channel model for all communication links. Hence, the small-scale fading component of the link from the UAV to the RIS (U-R link) in the \(n\)th time slot, denoted by \(h_{UR}[n] \in \mathbb{C}^{M \times 1}\), can be expressed as

\[
h_{UR}[n] = \sqrt{\frac{\beta_{UR}}{1 + \beta_{UR}}} h^{\text{LoS}}_{UR}[n] + \sqrt{\frac{1}{1 + \beta_{UR}}} h^{\text{NLoS}}_{UR},
\]
where $\beta_{UR}$ is the Rician factor of the U-R link, $h_{UR}^{\text{LoS}}[n]$ is the deterministic LoS component, and $h_{UR}^{\text{NLoS}}[n]$ is the non-LoS (NLoS) component which is modeled by the circularly symmetric complex Gaussian (CSCG) distribution with zero mean and unit variance. In particular, $h_{UR}^{\text{LoS}}[n]$ depends on the UAV trajectory at time slot $n$, and it can be expressed as $[41]$.

$$h_{UR}^{\text{LoS}}[n] = a_y[n] \otimes a_x[n], \quad (4)$$

where

$$a_x[n] = \left[1, e^{-\frac{j2\pi d}{\lambda} \cos \phi_{UR}[n] \sin \varphi_{UR}[n]} \right]^T,$$

$$a_y[n] = \left[1, e^{-\frac{j2\pi d}{\lambda} \sin \phi_{UR}[n] \sin \varphi_{UR}[n]} \right]^T,$$

$$\sin \phi_{UR}[n] \sin \varphi_{UR}[n] = \frac{z_U - z_R}{d_{UR}[n]},$$

$$\cos \phi_{UR}[n] \sin \varphi_{UR}[n] = \frac{x_R - x[n]}{d_{UR}[n]},$$

$$d_{UR}[n] = \sqrt{(z_U - z_R)^2 + ||q[n] - w_R||^2}$$

denotes the distance between the UAV and the RIS in the $n$th time slot, $\phi_{UR}[n]$ and $\varphi_{UR}[n]$ represent the azimuth and elevation angles of the LoS component in time slot $n$, respectively, $d$ is the antenna separation, and $\lambda$ is the carrier wavelength. The small-scale fading components of the links from the RIS to the ground user (R-G link), the RIS to the eavesdropper (R-E link), the UAV to the ground user (U-G link), and the UAV to the eavesdropper (U-E link) can be generated with a similar procedure, and they are denoted as $h_{RG}^H \in \mathbb{C}^{1 \times M}$, $h_{RE}^H \in \mathbb{C}^{1 \times M}$, $h_{UG} \in \mathbb{C}$, and $h_{UE} \in \mathbb{C}$, respectively. We use the distance-dependent path loss model in $[43, 44]$ for the reflected links, i.e., the links from the UAV to the ground user via the RIS (U-R-G link) and the UAV to the eavesdropper via the RIS (U-R-E link), which can be expressed as

$$L_{URG}[n] = \frac{\rho (d_{UR}[n]d_{RG})^{-\alpha}},$$

$$L_{URE}[n] = \frac{\rho (d_{UR}[n]d_{RE})^{-\alpha}}, \quad (5, 6)$$

where

$$d_{RG} = \sqrt{z_R^2 + ||w_R - w_G||^2},$$

$$d_{RE} = \sqrt{z_R^2 + ||w_R - w_E||^2},$$

$\rho$ is the path loss at the reference distance $D_0 = 1$ m, and $\alpha$ is the path loss exponent for the U-R-G and the U-R-E links. For the direct links, namely, the U-G and the U-E links, the corresponding distance-dependent path loss models are given by

$$L_{UG}[n] = \frac{\rho (z_U^2 + ||q[n] - w_G||^2)^{-\frac{\alpha}{2}}},$$

$$L_{UE}[n] = \frac{\rho (z_U^2 + ||q[n] - w_E||^2)^{-\frac{\alpha}{2}}}, \quad (7, 8)$$

where $\kappa$ is the path loss exponent for the U-G and the U-E links.

With the above channel models, the received signal-to-noise ratios (SNRs) of the ground user and the eavesdropper in the $n$th time slot can be respectively expressed as

$$\gamma_{UG}[n] = \frac{p[n]|L_{UG}[n]h_{UG} + L_{URG}[n]h_{RG}^H \Theta_u[n]h_{UR}[n]|^2}{\sigma^2},$$

$$\gamma_{UE}[n] = \frac{p[n]|L_{UE}[n]h_{UE} + L_{URE}[n]h_{RE}^H \Theta_u[n]h_{UR}[n]|^2}{\sigma^2}, \quad (9, 10)$$

where $\Theta_u[n] = \text{diag}(e^{j\theta_1[n]}, e^{j\theta_2[n]}, \ldots, e^{j\theta_{M}[n]})$ is the phase-shift matrix of the DL transmission in the time slot $n$ and $\sigma^2$ is the noise variance. Thus, the achievable rates in bits/second/Hertz (bps/Hz) at the ground user and the eavesdropper in time slot $n$ are respectively given by

$$R_{UG}[n] = \log_2(1 + \gamma_{UG}[n]), \quad (11a)$$

$$R_{UE}[n] = \log_2(1 + \gamma_{UE}[n]). \quad (11b)$$

2) **UL Transmission:** In this case, the ground user and the UAV serve as the legitimate transmitter and receiver, respectively. Denote by $g[n]$ the transmit power of the ground user in time slot $n$. Similarly, $g[n]$ is constrained by an average power limit $G$ and a peak power limit $G_{\text{peak}}$, i.e.,

$$\frac{1}{N} \sum_{n=1}^{N} g[n] \leq G, \quad (12a)$$

$$0 \leq g[n] \leq G_{\text{peak}}, \forall n. \quad (12b)$$

Since the ground user and the eavesdropper are both on the ground, we assume that the eavesdropping channel between the ground user and the eavesdropper (G-E link) is modeled as a Rayleigh fading channel. Thus, the small-scale fading component of the G-E link, denoted by $h_{GE}$, is assumed to be a zero-mean and unit-variance CSCG random variable. The distance-dependent path loss of the G-E link is given by

$$L_{GE} = \sqrt{\rho (||w_G - w_E||^2)^{-\frac{\alpha}{2}}}, \quad (13)$$

where $\varsigma$ is the path loss exponent related to the G-E link. Similar to the DL transmission, the other channels in the UL transmission are assumed to be Rician distributed, and thus, we omit their specific structures for brevity. The small-scale fading components of the links from the RIS to the UAV, the ground user to the RIS, and the ground user to the UAV are denoted as $h_{RUG}[n] \in \mathbb{C}^{1 \times M}$, $h_{GRE} \in \mathbb{C}^{M \times 1}$, and $h_{GUG} \in \mathbb{C}$, respectively. We still use $L_{UG}[n]$ and $L_{URG}[n]$ to express the distance-dependent path loss models of the user-RIS-UAV (G-R-U) link and user-UAV (G-U) link, respectively. Therefore, the received SNRs of the UAV and the eavesdropper in the $n$th time slot can be respectively written as

$$\gamma_{GU}[n] = \frac{g[n]|L_{UG}[n]h_{GU} + L_{URG}[n]h_{RG}^H \Theta_u[n]h_{UR}[n]|^2}{\sigma^2},$$

$$\gamma_{GE}[n] = \frac{g[n]|L_{GE}h_{GE} + L_{GRE}h_{RE}^H \Theta_u[n]h_{UR}[n]|^2}{\sigma^2}, \quad (14, 15)$$
where

\[ L_{\text{GRE}} = \sqrt{p \left[ (z_R^2 + ||w_R - w_G||^2) (z_R^2 + ||w_R - w_E||^2) \right]^{-\frac{1}{2}}} \]

is the large-scale fading component of the user-RIS-eavesdropper (G-R-E) link, and \( \Theta_u[n] = \text{diag} \left( e^{j\theta_{u1}[n]}, e^{j\theta_{u2}[n]}, \cdots, e^{j\theta_{us}[n]} \right) \) is the phase-shift matrix of the uplink transmission in the time slot \( n \). Hence, the achievable rates in bps/Hz from the ground user to the UAV and the eavesdropper in time slot \( n \) are respectively given by

\[
R_{GU}[n] = \log_2 (1 + \gamma_{GU}[n]), \quad \text{and} \quad R_{GE}[n] = \log_2 (1 + \gamma_{GE}[n]).
\]

(16a) (16b)

B. CSI Assumption

In general, the legitimate transmitter is able to periodically update and refine the CSI of the legitimate receiver based on uplink pilots. In addition, some channel estimation techniques have been proposed for CSI acquisition in the presence of RISs recently. Based on these considerations, we assume that the CSI of the legitimate links is perfectly available in a central controller. However, the eavesdropper usually avoids being detected and tracked by the legitimate transmitter in order to intercept the legitimate communications. Hence, the estimated CSI of the eavesdropping channels are usually not accurate at the central controller. For this reason, we first rewrite \( \gamma_{UE} \) and \( \gamma_{GE} \) as

\[
\gamma_{UE}[n] = \frac{p[n]}{\sigma^2} \left| \bar{h}_{E1} [n]^H \bar{H}_{UE} \right|^2, \quad \text{(17)}
\]

\[
\gamma_{GE}[n] = \frac{g[n]}{\sigma^2} \left| \bar{h}_{E2} [n]^H \bar{H}_{GE} \right|^2, \quad \text{(18)}
\]

where

\[
\bar{H}_{UE} = \text{diag} \left( \left[ L_{\text{URE}}[n] h_{UER} \right] \right), \quad \bar{H}_{GE} = \text{diag} \left( \left[ L_{\text{GRE}} \bar{h}_{GE} \right] \right),
\]

\[
h_{E1}[n] = \bar{h}_{E1} + \Delta h_{E1}[n], \quad \Omega_1 \equiv \{ \Delta h_{E1}[n] \in \mathbb{C}^{M+1} : ||\Delta h_{E1}[n]|| \leq \epsilon_1, \forall n \},
\]

\[
h_{E2}[n] = \bar{h}_{E2} + \Delta h_{E2}[n], \quad \Omega_2 \equiv \{ \Delta h_{E2}[n] \in \mathbb{C}^{M+1} : ||\Delta h_{E2}[n]|| \leq \epsilon_2, \forall n \},
\]

where \( \bar{h}_{E1} = \left[ \bar{h}_{E1}^H, \bar{h}_{UE} \right]^H \) and \( \bar{h}_{E2} = \left[ \bar{h}_{E2}^H, \bar{h}_{GE} \right]^H \) are the estimated CSI, and \( \Delta h_{E1}[n] \) and \( \Delta h_{E2}[n] \) represent the estimated errors for \( \bar{h}_{E1} \) and \( \bar{h}_{E2} \), respectively. The continuous sets \( \Omega_1 \) and \( \Omega_2 \) contain all possible CSI uncertainties with norms bounded by the uncertainty radii \( \epsilon_1 \) and \( \epsilon_2 \), respectively.

C. Problem Formulation

Based on (11) and (16), the worst-case secrecy rates in time slot \( n \) in the DL and UL transmissions can be respectively expressed as

\[
R_{\text{sec}}[n] = \left[ R_{GU}[n] - \max_{\Delta h_{E1}[n] \in \Omega_1} R_{UE}[n] \right]^+, \quad \text{(20a)}
\]

\[
R_{\text{sec}}[n] = \left[ R_{GU}[n] - \max_{\Delta h_{E2}[n] \in \Omega_2} R_{GE}[n] \right]^+, \quad \text{(20b)}
\]

where \([x]^+ \equiv \max(x, 0)\). Hence, the average worst-case secrecy rate of the joint UL/DL RIS-assisted UAV secure communication system is given by

\[
R_{\text{sec}} = \frac{1}{N} \sum_{n=1}^{N} \left( w R_{\text{sec}}^\text{down}[n] + (1-w) R_{\text{sec}}^\text{up}[n] \right). \quad \text{(21)}
\]

Our objective is to maximize \( R_{\text{sec}} \) by jointly optimizing the UAV’s trajectory \( Q \equiv \{ q[n], n \in N \} \), the phase-shift matrices \( \Phi_d \equiv \{ \Theta_d[n], n \in N \} \) and \( \Phi_u \equiv \{ \Theta_u[n], n \in N \} \) of the RIS, the UAV’s transmit power \( p \equiv \{ p[n], n \in N \} \), and the transmit power \( g \equiv \{ g[n], n \in N \} \) of the ground user. Therefore, the problem can be formulated as

\[
\max_{Q, \Phi_d, \Phi_u, p, g} R_{\text{sec}} \quad \text{s.t.} \quad 0 \leq \theta^u_i[n] < 2\pi, \forall n, i, \quad 0 \leq \theta^d_i[n] < 2\pi, \forall n, i, \quad (22b) \quad (22c)
\]

It is observed that the constraints of problem (22) are all convex. However, it is still difficult to solve problem (22) since the objective function of problem (22) is highly non-concave with respect to \( Q, \Phi_d, \Phi_u, p, \) and \( g \). In the next section, we develop an efficient algorithm to solve problem (22).

III. PROPOSED SOLUTION FOR JOINT UL/DL OPTIMIZATION

In this section, we focus on solving the joint UL/DL optimization problem (22). Based on Lemma 1 in [4], it is known that the transmit power control design can guarantee

\[
R_{\text{UE}}[n] - \max_{\Delta h_{E1}[n] \in \Omega_1} R_{UE}[n] \geq 0 \quad \text{and} \quad R_{GU}[n] - \max_{\Delta h_{E2}[n] \in \Omega_2} R_{GE}[n] \geq 0,
\]

since the optimal transmit power of the UAV and the ground user in time slot \( n \), denoted as \( p^* [n] \) and \( g^* [n] \), respectively, are zero once the quality of the eavesdropping channels is better than that of the legitimate channels in time slot \( n \). Therefore, we reformulate problem (22) as

\[
\max_{Q, \Phi_d, \Phi_u, p, g} \frac{1}{N} \sum_{n=1}^{N} \left( w R_{\text{sec}}^\text{down}[n] + (1-w) R_{\text{sec}}^\text{up}[n] \right) \quad \text{s.t.} \quad (1), (2), (12), (22b), (22c)
\]

where

\[
R_{\text{sec}}[n] = \left[ R_{GU}[n] - \max_{\Delta h_{E1}[n] \in \Omega_1} R_{UE}[n] \right]^+.
\]
As a result, the non-smoothness of problem (22) is addressed, and there exists no performance loss in this step. However, problem (23) is still difficult to solve due to the coupled optimization variables $Q, \Phi_d, \Phi_u, p$, and $g$ in the objective function. To cope with this difficulty, we propose an efficient algorithm based on the AO method. Specifically, we divide problem (23) into three sub-problems:

1) The optimization of the transmit power $p$ and $g$ under the given UAV trajectory $Q$ and phase-shift matrices $\Phi_d$ and $\Phi_u$ (referred to as sub-problem 1);
2) The optimization of the phase-shift matrices $\Phi_d$ and $\Phi_u$ under the given UAV trajectory $Q$ and transmit power $p$ and $g$ (referred to as sub-problem 2);
3) The optimization of the UAV trajectory $Q$ under the given phase-shift matrices $\Phi_d$ and $\Phi_u$ and transmit power $p$ and $g$ (referred to as sub-problem 3).

The details are presented in the next three subsections, and subsequently the overall algorithm is summarized.

A. Solution to Sub-Problem 1

For any given $Q, \Phi_d,$ and $\Phi_u$, we have

$$h_{G1}^H[n]v[n] = L_{URC}[n]h_{URC} + L_{URG}[n]h_{URG}[n]h_{UR}[n],$$

$$h_{G2}^H[n]v[n] = L_{URG}[n]h_{GR} + L_{URC}[n]h_{FRG}[n]h_{GR}[n],$$

where

$$h_{G1}[n] = \text{diag} \left( \left[ \frac{L_{URG}[n]h_{UR}[n]}{L_{UR}[n]} \right] \right),$$

$$h_{G2}[n] = \text{diag} \left( \left[ \frac{L_{URG}[n]h_{GR}[n]}{L_{UR}[n]} \right] \right),$$

$$h_{G1} = \left[ h_{FRG}^H, h_{URC}^H \right]^H,$$

and

$h_{G2}[n] = \left[ h_{FRG}^H, h_{URC}^H \right].$ Then, sub-problem 1 can be expressed as

$$\max_{p, g} \frac{1}{N} \sum_{n=1}^{N} \left[ w R_{down}^p[n] + (1 - w) R_{up}^p[n] \right]$$

s.t. (22), (23),

where

$$R_{down}^p[n] = \log_2 \left( 1 + \frac{p[n]}{\sigma^2} \right),$$

and

$$R_{up}^p[n] = \log_2 \left( 1 + \frac{g[n]}{\sigma^2} \right).$$

Infinitely many possible CSI uncertainties in $\Omega_1$ and $\Omega_2$ make problem (24) intractable. However, the special structure of $h_{E1}^H[n]H_{E1}[n]v[n]$ and $h_{E2}^H[n]H_{E2}[n]v[n]$ can be utilized to address this problem. Let $\arg(x)$ denote the phase angle vector of $x$, in which each element is the phase angle of the corresponding element in $x$. We first have the following inequality:

$$|h_{E1}^H[n]H_{E1}[n]v[n]|^2 \leq |h_{E1}^H[n]H_{E1}[n]v[n]|^2 + |\Delta h_{E1}[n]H_{E1}[n]v[n]|^2,$$

where the equality holds if and only if

$$\arg \left( h_{E1}^H[n]H_{E1}[n]v[n] \right) = \arg \left( \Delta h_{E1}[n]H_{E1}[n]v[n] \right).$$

Thus, $\max_{h_{E1}[n] \in \Omega_1} \left| \Delta h_{E1}[n]H_{E1}[n]v[n] \right|^2 / \sigma^2$ can be transformed into

$$\max_{h_{E1}[n] \in \Omega_1} \left| \Delta h_{E1}[n]H_{E1}[n]v[n] \right|^2$$

s.t. \( \| \Delta h_{E1}[n] \| \leq \epsilon_1, \)

$$\| \Delta h_{E1}[n] \| = \arg \left( \Delta h_{E1}[n]H_{E1}[n]v[n] \right).$$

To facilitate the subsequent derivations, $\Delta h_{E1}[n]$ can be expressed as

$$\Delta h_{E1}[n] = \left[ \Delta h_{E1,1}[n] e^{j\tau_1[n]}, \Delta h_{E1,2}[n] e^{j\tau_2[n]}, \ldots, \right.$$  

$$\left. \Delta h_{E1,M+1}[n] e^{j\tau_{M+1}[n]} \right],$$

where $\Delta h_{E1,k}[n]$ and $\tau_k[n]$ are the magnitude and phase angle of the $k$th element of $\Delta h_{E1}[n]$ in time slot $n$, respectively, and $k \in K = \{1, \ldots, M+1\}$. Let $c[n] = H_{E1}[n]v[n]$. Similarly, $c[n]$ can be expressed as

$$c[n] = \left[ e_{c1,n} e^{j\psi_1[n]}, e_{c2,n} e^{j\psi_2[n]}, \ldots, e_{cM+1,n} e^{j\psi_{M+1}[n]} \right],$$

where $e_{c1}[n]$ and $\psi_k[n]$ are the magnitude and phase angle of the $k$th element of $c[n]$ in time slot $n$, respectively. Hence, $\Delta h_{E1}[n]H_{E1}[n]v[n]$ can be given by

$$\Delta h_{E1}[n]H_{E1}[n]v[n] = \Delta h_{E1}[n]c[n] = \Delta h_{E1,1}[n] e^{j\psi_1[n]} - \tau_1[n] + \ldots + \Delta h_{E1,M+1}[n] e^{j\psi_{M+1}[n]} - \tau_{M+1}[n].$$

It is known that the maximum of $\left| \Delta h_{E1}[n]H_{E1}[n]v[n] \right|^2$ can be obtained when all the items in the last step of (28) can be coherently added. Hence, we have $\psi_1[n] - \tau_1[n] = \psi_2[n] - \tau_2[n] = \cdots = \psi_{M+1} - \tau_{M+1}[n]$. Then, based on the constraints in (25), it is not difficult to show that the optimal $\tau_k[n]$, denoted as $\tau_k^{op}[n]$, is given by

$$\tau_k^{op}[n] = \psi_k[n] - \arg \left( h_{E1}^H[n]H_{E1}[n]v[n] \right).$$

As such, problem (25) can be transformed into

$$\max_{m_1[n]} \left| m_1[n] m_2[n] \right|^2$$

s.t. \( \| m_1[n] \| \leq \epsilon_1, \)

where

$$m_1[n] = \left[ \Delta h_{E1,1}[n], \Delta h_{E1,2}[n], \ldots, \Delta h_{E1,M+1}[n] \right]^T,$$

and

$$m_2[n] = \left[ e_{c1,n}, e_{c2,n}, \ldots, e_{cM+1,n} \right].$$
It is not difficult to show that the optimal $m_1[n]$, denoted as $m_1^{op}[n]$ is given by
\[ m_1^{op}[n] = \frac{e_1}{\|m_2[n]\|} m_2[n]. \tag{31} \]
Therefore, the optimal $\Delta h_{E1}[n]$, denoted as $\Delta h_{E1}^{op}[n]$, is
\[ \Delta h_{E1}^{op}[n] = \text{diag} \left( \left[ e^{j\pi m_1^{op}[n]}, e^{j\pi m_2^{op}[n]}, \ldots, e^{j\pi m_{N+1}^{op}[n]} \right] \right) m_1^{op}[n]. \tag{32} \]
\( \Delta h_{E2}^{op}[n] \) can also be obtained by using the above solution. With $\Delta h_{E1}^{op}[n]$ and $\Delta h_{E2}^{op}[n]$, problem (2) can be rewritten as
\[ \max \frac{1}{N} \sum_{n=1}^{N} \left[ w_1 \hat{R}_{\text{down}}[n] + (1-w) \hat{R}_{\text{up}}[n] \right] \tag{33} \]
\text{s.t. } (2), (12).
where
\[ \hat{R}_{\text{down}}[n] = \log_2 \left( 1 + p[n] a_1[n] \right) - \log_2 \left( 1 + p[n] b_1[n] \right), \]
\[ \hat{R}_{\text{up}}[n] = \log_2 \left( 1 + q[n] a_1[n] \right) - \log_2 \left( 1 + q[n] b_2[n] \right), \]
\[ a_1[n] = \frac{|h_{G1}^{H} H_{E1}[n] v^d[n]|^2}{\sigma^2}, \]
\[ b_1[n] = \frac{|h_{G1}^{H} H_{E2}[n] v^d[n]|^2}{\sigma^2}, \]
\[ a_2[n] = \frac{|h_{G2}^{H} H_{E1}[n] v^u[n]|^2}{\sigma^2}, \]
\[ b_2[n] = \frac{|h_{G2}^{H} H_{E2}[n] v^u[n]|^2}{\sigma^2}, \]
\[ h_{E1}^{op}[n] = \hat{h}_{E1} + \Delta h_{E1}^{op}[n], \text{ and } h_{E2}^{op}[n] = \hat{h}_{E2} + \Delta h_{E2}^{op}[n]. \]
Similar to sub-problem 1 in (4), the optimal solution of (33) is given by
\[ p^{op}[n] = \begin{cases} \left[ \tilde{p}[n]^+, \bar{P}_{\text{peak}} \right], & a_1[n] > b_1[n], \\ 0, & a_1[n] \leq b_1[n], \end{cases} \tag{34a} \]
\[ g^{op}[n] = \begin{cases} \left[ \tilde{g}[n]^+, \bar{G}_{\text{peak}} \right], & a_2[n] > b_2[n], \\ 0, & a_2[n] \leq b_2[n], \end{cases} \tag{34b} \]
where
\[ \tilde{p}[n] = \sqrt{\frac{1}{2b_1[n]} - \frac{1}{2a_1[n]}}^2 + \frac{1}{\omega_1 \ln 2} \left( \frac{1}{b_1[n]} - \frac{1}{a_1[n]} \right) \]
\[ - \frac{1}{2b_1[n]} - \frac{1}{2a_1[n]}, \tag{35a} \]
\[ \tilde{g}[n] = \sqrt{\frac{1}{2b_2[n]} - \frac{1}{2a_2[n]}}^2 + \frac{1}{\omega_2 \ln 2} \left( \frac{1}{b_2[n]} - \frac{1}{a_2[n]} \right) \]
\[ - \frac{1}{2b_2[n]} - \frac{1}{2a_2[n]} \tag{35b} \]
\( \Delta h_{E1}[n] \) and $\Delta h_{E2}[n]$ can be solved by the following lemma.

**Lemma 1 (S-Procedure [39].)** Let a function $f_m(x), m \in \{1, 2\}, x \in \mathbb{C}^{N \times 1}$, be defined as
\[ f_m(x) = x^H B_m x + 2 \text{Re} \{ b_m^H x \} + b_m, \tag{38} \]
where $B_m \in \mathbb{H}^N$, $b_m \in \mathbb{C}^{N \times 1}$, and $b_m \in \mathbb{R}^{1 \times 1}$. Then, the implication $f_1(x) \leq 0 \Rightarrow f_2(x) \leq 0$ hold if and only if there exists a $\delta \geq 0$ such that
\[ \delta \left[ B_1 b_1 \right] - \delta \left[ B_2 b_2 \right] \succeq 0, \tag{39} \]
provided that there exists a point $\hat{x}$ such that $f_m(\hat{x}) < 0$. 

**B. Solution to Sub-Problem 2**

For any given $p$, $g$, and $Q$, with the aid of the slack variables $\xi_1 = \{ \xi_1[n] \}_{n=1}^{N}$ and $\xi_2 = \{ \xi_2[n] \}_{n=1}^{N}$, sub-problem 2 can be expressed as
\[ \max \frac{1}{N} \sum_{n=1}^{N} \left[ w \hat{R}_{\text{down}}[n] + (1-w) \hat{R}_{\text{up}}[n] \right] \tag{36a} \]
\[ \text{s.t. } \max_{\Delta h_{E1}[n] \in \Omega_1} \frac{p[n]}{\sigma^2} |h_{G1}^{H} H_{E1}[n] v^d[n]|^2 \leq \xi_1[n], \forall n, \tag{36b} \]
\[ \max_{\Delta h_{E2}[n] \in \Omega_1} \frac{q[n]}{\sigma^2} |h_{G2}^{H} H_{E2}[n] v^u[n]|^2 \leq \xi_2[n], \forall n, \tag{36c} \]
\[ |v_i^d[n],| v_i^u[n] | = 1, \forall n, \tag{36d} \]
where
\[ \hat{R}_{\text{down}}[n] = \log_2 \left( 1 + \frac{p[n]}{\sigma^2} |h_{G1}^{H} H_{E1}[n] v^d[n]|^2 \right) \]
and
\[ \hat{R}_{\text{up}}[n] = \log_2 \left( 1 + \frac{q[n]}{\sigma^2} |h_{G2}^{H} H_{E2}[n] v^u[n]|^2 \right) \]
It is difficult to solve problem (36), since the constraints in (36b) and (36c) involve infinitely many inequality constraints. To overcome this difficulty, we first substitute (19a) and (19b) into (36b) and (36c), respectively, and obtain
\[ \Delta h_{E1}^{op}[n] \leq \xi_1[n] \leq 0, \forall n \tag{37a} \]
\[ \Delta h_{E2}^{op}[n] \leq \xi_2[n] \leq 0, \forall n \tag{37b} \]
\[ \frac{p[n]}{\sigma^2} |h_{G1}^{H} H_{E1}[n] v^d[n]|^2 \leq \xi_1[n] \leq 0, \forall n, \tag{37c} \]
\[ \frac{q[n]}{\sigma^2} |h_{G2}^{H} H_{E2}[n] v^u[n]|^2 \leq \xi_2[n] \leq 0, \forall n, \tag{37d} \]
where $V^d[n] = v^d[n] v^d[n]^H$ and $V^u[n] = v^u[n] v^u[n]^H$. The ranks of $V^d[n]$ and $V^u[n]$ are one. Then, we transform the constraints in (36b) and (36c) into linear matrix inequalities (LMIs) by using the following lemma.
\[ U_2[n] = \frac{p[n]}{\sigma^2} \begin{bmatrix} H_{E_1}[n] V^d[n] H_{E_1}^H[n] & H_{E_1}[n] V^d[n] H_{E_1}^H[n] h_{E_1} \\ h_{E_1}^H[n] H_{E_1}[n] V^d[n] H_{E_1}^H[n] & h_{E_1}^H[n] H_{E_1}[n] V^d[n] H_{E_1}^H[n] h_{E_1} \end{bmatrix} \]

\[ U_3[n] = \frac{g[n]}{\sigma^2} \begin{bmatrix} H_{E_2}[n] V^u[n] H_{E_2}^H[n] & H_{E_2}[n] V^u[n] H_{E_2}^H[n] h_{E_2} \\ h_{E_2}^H[n] H_{E_2}[n] V^u[n] H_{E_2}^H[n] & h_{E_2}^H[n] H_{E_2}[n] V^u[n] h_{E_2} \end{bmatrix} \]

Using Lemma 1, the following implications can be obtained: \( \eta_1 \Rightarrow \eta_2 \) and \( \eta_2 \Rightarrow \eta_3 \) holds if and only if there exist \( \eta_1[n] \geq 0 \) and \( \eta_2[n] \geq 0 \) such that

\[ U_1[n] - U_2[n] \geq 0, \quad U_3[n] - U_4[n] \geq 0, \]

where

\[ U_1[n] = \begin{bmatrix} \eta_1[n] I_{M+1} & 0 \\ 0 & -\eta_1[n] \xi_1 + \xi_1[n] \end{bmatrix}, \]

\[ U_3[n] = \begin{bmatrix} \eta_2[n] I_{M+1} & 0 \\ 0 & -\eta_2[n] \xi_2 + \xi_2[n] \end{bmatrix}. \]

\( I_{M+1} \) denotes the \((M+1) \times (M+1)\) identity matrix, and \( U_2[n] \) and \( U_4[n] \) are given in (43) and (44), respectively. Since the unit-modulus constraints in (46d) are non-convex, we apply the SDR method to relax the constraints.

\[ |h_{G_1}^H[n] h_{G_1}[n] v^d[n]|^2 = h_{G_1}^H[n] h_{G_1}[n] V^d[n] H_{G_1}^H[n] h_{G_1} = \text{Tr} \left( V^d[n] A_1[n] \right) \]

\[ |h_{G_2}^H[n] h_{G_2}[n] v^u[n]|^2 = h_{G_2}^H[n] h_{G_2}[n] V^u[n] H_{G_2}^H[n] h_{G_2} = \text{Tr} \left( V^u[n] A_2[n] \right), \]

where

\[ A_1[n] = H_{G_1}^H[n] h_{G_1}[n] h_{G_1}^H[n] H_{G_1}[n], \]

\[ A_2[n] = H_{G_2}^H[n] h_{G_2}[n] h_{G_2}^H[n] H_{G_2}[n], \]

and \( \text{Tr} \left( X \right) \) denotes the trace of \( X \). Thus, problem (45) can be reformulated as

\[ \max_{v^d[n], v^u[n], \xi_1[n], \xi_2[n]} \frac{1}{N} \sum_{n=1}^{N} \left[ w \tilde{R}_{down}^{phi}[n] + (1 - w) \tilde{R}_{up}^{phi}[n] \right] \]

s.t. \( \eta_1[n], \eta_2[n] \geq 0, \forall n, \)

\[ V^d[n], V^u[n] \geq 0, \forall n, \]

\[ V_{r,r}^d[n], V_{r,r}^u[n] = 1, r = 1, \cdots, M + 1, \forall n, \]

where

\[ \tilde{R}_{down}^{phi}[n] = \log_2 \left( 1 + \frac{p[n]}{\sigma^2} \text{Tr} \left( V^d[n] A_1[n] \right) \right) \]

\[ - \log_2 \left( 1 + \xi_1[n] \right), \]

\[ \tilde{R}_{up}^{phi}[n] = \log_2 \left( 1 + \frac{g[n]}{\sigma^2} \text{Tr} \left( V^u[n] A_2[n] \right) \right) \]

\[ - \log_2 \left( 1 + \xi_2[n] \right), \]

and \( V_{r,r}^d[n] \) and \( V_{r,r}^u[n] \) denote the \((r, r)\)th element of \( V^d[n] \) and \( V^u[n] \), respectively. It is still difficult to obtain the optimal solution of problem (45), since \( - \log_2 \left( 1 + \xi_1[n] \right) \) and \( - \log_2 \left( 1 + \xi_2[n] \right) \) are not concave with respect to \( \xi_1[n] \) and \( \xi_2[n] \), respectively. Nevertheless, it is known that the first-order Taylor expansion of a concave function is its global over-estimator and that of a convex function is its global under-estimator. Therefore, we apply the SCA method to solve problem (45). The first-order Taylor expansions of \( \log_2 \left( 1 + \xi_1[n] \right) \) and \( \log_2 \left( 1 + \xi_2[n] \right) \) at the given points \( \xi_{1,0} = \{\xi_{1,0}[n]\}_{n=1}^{N} \) and \( \xi_{2,0} = \{\xi_{2,0}[n]\}_{n=1}^{N} \) can be respectively expressed as

\[ \log_2 \left( 1 + \xi_1[n] \right) \leq \log_2 \left( 1 + \xi_{1,0}[n] \right) + \frac{1}{\ln 2} \left( \xi_1[n] - \xi_{1,0}[n] \right), \]

\[ \log_2 \left( 1 + \xi_2[n] \right) \leq \log_2 \left( 1 + \xi_{2,0}[n] \right) + \frac{1}{\ln 2} \left( \xi_2[n] - \xi_{2,0}[n] \right). \]

Then, problem (45) can be approximated as

\[ \max_{v^d[n], v^u[n], \xi_1[n], \xi_2[n]} \frac{1}{N} \sum_{n=1}^{N} \left[ w \tilde{R}_{down}^{phi}[n] + (1 - w) \tilde{R}_{up}^{phi}[n] \right] \]

s.t. \( 40, 45b, 45c, 45d \),

where

\[ \tilde{R}_{down}^{phi}[n] = \log_2 \left( 1 + \frac{p[n]}{\sigma^2} \text{Tr} \left( V^d[n] A_1[n] \right) \right) \]

\[ - \frac{\xi_1[n]}{\ln 2} \left( 1 + \xi_{1,0}[n] \right), \]

\[ \tilde{R}_{up}^{phi}[n] = \log_2 \left( 1 + \frac{g[n]}{\sigma^2} \text{Tr} \left( V^u[n] A_2[n] \right) \right) \]

\[ - \frac{\xi_2[n]}{\ln 2} \left( 1 + \xi_{2,0}[n] \right). \]

It is observed that problem (48) is a convex optimization problem, and thus can be solved efficiently by using standard solvers, such as the CVX. However, we emphasize that a rank-one solution may not be obtained. Hence, we use the Gaussian randomization method to recover \( v^d[n] \) and \( v^u[n] \) from \( V^d[n] \) and \( V^u[n] \), respectively, which is similar to that in [23] and thus omitted here for brevity.

C. Solution to Sub-Problem 3

For any given \( \Phi_{d}, \Phi_{u}, p, \) and \( g \), we can express sub-problem 3 as

\[ \max_{Q} \frac{1}{N} \sum_{n=1}^{N} \left[ (1 - w) \log_2 \left( 1 + \frac{g[n]}{\sigma^2} |h_{G_2}^H[n] H_{G_2}[n] v^u[n]|^2 \right) \right] \]

\[ + w R_{down}^{tra}[n] \]

s.t. 1,
However, from the structure of channels iteration to calculate the worst case setup for the wiretap given. Hence, we utilize the UAV trajectory of the UA V is worth noting that not only trajectory of the design intractable. To handle such difficulty, we use the UA V trajectory of the \( h_{\text{LoS}} \) is not a convex problem due to the non-concave objective function with respect to the UAV trajectory variables, which makes the UAV trajectory design intractable. To handle such difficulty, we use the UAV trajectory of the (j-1)th iteration to obtain an approximate \( h_{\text{UR}} \) in the jth iteration. Similarly, the LoS component of \( h_{\text{UR}} \) in the jth iteration is also designed by using the UAV trajectory of the (j-1)th iteration. Then, we can rewritten problem 49 as

\[
\max_Q \frac{1}{N} \sum_{n=1}^{N} \left[ (1-w) \log_2 \left( 1 + \rho_{\gamma_1}[n] h_{\text{LoS}}[n] h_{\text{ue}}[n] \right) + w R_{\text{down}}^{\text{tra}}[n] \right]
\]

s.t. (1),

where

\[
R_{\text{down}}^{\text{tra}}[n] = \log_2 \left( 1 + \frac{p[n]}{\sigma^2} | h_{G1}^H H_{C1}[n] v[\nu[n]] |^2 \right)
\]

\[
- \log_2 \left( 1 + \max_{\Delta h_{E1} \in \mathbb{H}_n} \frac{p[n]}{\sigma^2} | h_{E1}^H H_{E1}[n] v[\nu[n]] |^2 \right).
\]

In particular, \( R_{\text{UE}}[n] \) is not relevant to the UAV trajectory, and so we omit it in problem 49. It is challenging to cope with the infinitely many \( \Delta h_{E1} \). However, we note that the worst case of the objective function is obtained when the UAV trajectory is given, and the UAV trajectory can be optimized when the worst case of the wiretap channels, i.e., \( h_{\text{LoS}}[n] \), is given. Hence, we utilize the UAV trajectory of the \( (j-1) \)th iteration to calculate the worst case setup for the wiretap channels \( h_{\text{LoS}}[n] \) in the jth iteration, and this is obtained by using a procedure similar to (32). Besides, from (4)-(8), it is worth noting that not only \( L_{\text{UE}}[n], L_{\text{UE}}[n], L_{\text{URG}}[n], \) and \( L_{\text{UE}}[n] \) but also \( h_{\text{LoS}}[n] \) is relevant to the UAV trajectory. However, from the structure of \( h_{\text{LoS}}[n] \) in (4), it is observed that \( h_{\text{LoS}}[n] \) is complex and non-linear with respect to the UAV trajectory variables, which makes the UAV trajectory design intractable. To handle such difficulty, we use the UAV trajectory of the (j-1)th iteration to obtain an approximate \( h_{\text{LoS}}[n] \) in the jth iteration. Similarly, the LoS component of \( h_{\text{LoS}}[n] \) in the jth iteration is also designed by using the UAV trajectory of the (j-1)th iteration. Then, we can rewritten problem 50 as follows,

\[
\max_Q \frac{1}{N} \sum_{n=1}^{N} \left[ (1-w) \log_2 \left( 1 + \rho_{\gamma_1}[n] h_{\text{LoS}}[n] h_{\text{ue}}[n] \right) + w R_{\text{down}}^{\text{tra}}[n] \right]
\]

s.t. (1),

where

\[
R_{\text{down}}^{\text{tra}}[n] = \log_2 \left( 1 + \rho_{\gamma_0}[n] h_{\text{LoS}}[n] H_{Q}[n] h_{\text{ue}}[n] \right)
\]

\[
- \log_2 \left( 1 + \rho_{\gamma_0}[n] h_{\text{LoS}}^T[n] H_{Q}[n] h_{\text{ue}}[n] \right).
\]

It is observed that the constraints \( 58a-58d \) are non-convex feasible regions, and \( - \log_2 (1 + \zeta[n]) \) is non-concave with respect to \( \zeta[n] \). We use the SCA technique to address the non-convexity of these constraints. The first-order Taylor expansions of \( -x^2[n] \), \( -y^2[n] \), \( (u[n])^\frac{1}{2} \), \( (e[n])^\frac{1}{2} \), \( \log_2 (1 + \zeta[n]) \), \( h_{\text{ue}}[n] H_{Q}[n] h_{\text{ue}}[n] \), and \( h_{\text{ue}}^T[n] H_{Q}[n] h_{\text{ue}}[n] \) at the given feasible points \( x_0 = \{ x[n] \}_{n=1}^{N}, y_0 = \{ y[n] \}_{n=1}^{N}, \) \( u_0 = \{ u[n] \}_{n=1}^{N}, e_0 = \{ e[n] \}_{n=1}^{N}, \zeta_0 = \{ \zeta[n] \}_{n=1}^{N}, \) and \( H_{ue,0} = \)
10

\[ H_{QG}[n] = \left[ h_{IG}^H, \sqrt{(d_{RG})^{-\alpha}}(h_{UR}^{(j-1)}[n])^H \Theta_d^H [n] h_{RG} \right]^H \left[ h_{IG}^H, \sqrt{(d_{RG})^{-\alpha}}(h_{ER}^{(j-1)}[n])^H \Theta_d^H [n] h_{RG} \right] \]

(54)

\[ H_{GQ}[n] = \left[ h_{IG}^H, \sqrt{(d_{RG})^{-\alpha}}h_{GR}^H \Theta_u [n] h_{HU}^{-1} \right]^H \left[ h_{IG}^H, \sqrt{(d_{RG})^{-\alpha}}h_{GR}^H \Theta_u [n] h_{HU}^{-1} \right] \]

(55)

\[ H_{QE}[n] = \left[ \frac{h_{UE}^H[n]}{\sqrt{(d_{RE})^{-\alpha}}} \right]^H \left[ \frac{h_{UE}^H[n]}{\sqrt{(d_{RE})^{-\alpha}}} \right] \]

(56)

**Algorithm 1 Proposed algorithm for solving problem (4)**

1. **Initialization:**
   - Set the initial feasible points \( \Xi_0 = \{ Q^{(0)}, \Phi_d^{(0)}, \Phi_u^{(0)}, p^{(0)}, g^{(0)}, u_0, e_0, \xi_1,0, \xi_2,0, \xi_0 \} \). Set iteration index \( j = 0 \) and \( R_{sec}^{(0)} \).

2. **repeat**
   3. Set \( j \leftarrow j + 1 \);  
   4. With given \( \Phi_d^{(j-1)}, \Phi_u^{(j-1)}, g^{(j-1)}, u_0, e_0, \) and \( \xi_0 \), update \( Q^{(j)}, u^{(j)}, e^{(j)}, \) and \( \xi^{(j)} \) by solving problem (60);  
   5. Set \( u_0 = u^{(j)}, e_0 = e^{(j)}, \) and \( \xi_0 = \xi^{(j)} \);  
   6. With given \( Q^{(j)}, \Phi_d^{(j-1)}, \Phi_u^{(j-1)}, e^{(j)}, \) and \( \xi^{(j)} \), update \( \Phi_d^{(j)}, \Phi_u^{(j)}, \Phi_e^{(j)}, \Phi_r^{(j)}, \) and \( \xi^{(j)} \) by solving problem (59);  
   7. With given \( \Phi_d^{(j)}, \Phi_u^{(j)}, \Phi_e^{(j)}, \) update \( p^{(j)} \) and \( g^{(j)} \) by using (53);  
   8. With given \( Q^{(j)}, \Phi_d^{(j)}, \Phi_u^{(j)}, p^{(j)}, \) and \( g^{(j)} \), compute \( R_{sec}^{(j)} \);  
   9. until: \( R_{sec}^{(j)} - R_{sec}^{(j-1)} \leq \epsilon_c \) or \( j > j_{max} \).

The \( \tilde{h}_{ue,0}[n] \) are given by

\[ \tilde{h}_{ue,0}[n] = -\tilde{h}_{ue,0}^T[n] H_{QG}[n] H_{ue}[n] \]

(59a)

\[ + 2 R - \tilde{h}_{ue,0}^T[n] H_{QG}[n] H_{ue,0}[n] \]

\[ + 2 R - \tilde{h}_{ue,0}^T[n] H_{GQ}[n] H_{ue,0}[n] \]

(59b)

\[ \log_2 (1 + \tilde{\zeta}[n]) \leq \log_2 (1 + \zeta_0[n]) \]

\[ + \frac{1}{\ln 2 (1 + \zeta_0[n])} (\zeta_0[n] - \zeta_0[n]), \]

(59c)

\[ (u[n])^{-\frac{4}{\kappa}} \geq (u_0[n])^{-\frac{4}{\kappa}} - \frac{4}{\kappa} (u_0[n])^{-\frac{4}{\kappa}} - (u[n] - u_0[n]), \]

(59d)

\[ (e[n])^{-\frac{4}{\alpha}} \geq (e_0[n])^{-\frac{4}{\alpha}} - \frac{4}{\alpha} (e_0[n])^{-\frac{4}{\alpha}} - (e[n] - e_0[n]), \]

(59e)

\[ - x^2[n] \leq x_0^2[n] - 2 x_0[n] x[n], \]

(59f)

\[ - y^2[n] \leq y_0^2[n] - 2 y_0[n] y[n], \]

(59g)

Accordingly, problem (57) can be approximately trans-
In Fig. 4, we show the UA V speed during flight periods with different channel realizations. From Fig. 3, it is observed that, for all the algorithms, the UAV first flies to a certain location at $V_{\text{max}}$, then keeps static, and finally flies to the final location at $V_{\text{max}}$. However, as for the JO/NPB algorithm, the UAV first flies directly to a certain location where the UAV is close to the ground user and away from the eavesdropper as possible as it can, then hovers as long as possible, and finally flies along a relatively direct path to the final location in order to avoid being eavesdropped. By contrast, for the JO and JO/NR algorithms, the UAV tends to fly along an arc path to a certain location between the ground user and the RIS, then it hovers as long as possible, and finally flies along a relatively direct path to the final location in order to achieve the best communication quality. Besides, since the JO algorithm takes the CSI uncertainty into account, the UAV trajectories of the JO algorithm under different channel realizations are more decentralized than those of the JO/NR algorithm under different channel realizations.

In Fig. 5, we show the average worst-case secrecy rates for different algorithms versus $T$ with $w = 0.5$, $\delta_a^2 = 0.5$, and $P = \hat{G} = 20$ dBm. At the hovering location, the trade-off between enhancing the quality of the legitimate links and weakening the quality of the eavesdropping links is achieved for the UAV. Therefore, the maximum secrecy rate is achieved at the hovering location and the longer the UAV remains static at the hovering location, the larger the average worst-case secrecy rate is. This is the reason why the average worst-case secrecy rates of all the algorithms increase with $T$. In particular, our proposed algorithm exceeds all the benchmark schemes. This shows that, with the aid of the proposed robust joint design of the UAV trajectory, RIS’s passive beamforming, and joint transmit power and beamforming, respectively. Hence, the overall complexity of solving problem (22) is $O_{\text{sub2}} + O_{\text{sub3}}$. Furthermore, as shown in Fig. 2, we observe that the proposed algorithm can quickly converge.

IV. SIMULATION RESULTS

In this section, we present simulation results to verify the validity of the proposed algorithm (denoted as JO) for the joint UL/DL optimization. The following benchmark algorithms are used for comparison:

- Robust design of the UAV trajectory and transmit power without passive beamforming (denoted as JO/NPB).
- Robust design of the heuristic trajectory, transmit power, and passive beamforming (denoted as JO/HT).
- Non-robust design of the UAV trajectory, passive beamforming, and transmit power (denoted as JO/NR).

Specifically, “heuristic trajectory” refers to a preset trajectory where the UAV first flies directly to the ground user at the maximum speed, then hovers above the user as long as possible, and finally flies to the final location at its maximum speed for the rest of the flight time. Also, for the considered JO/NR algorithm, the estimated CSI of the eavesdropping channels is the exact CSI. Hence, it is a special case of our proposed algorithm that is obtained by setting $\epsilon_1 = \epsilon_2 = 0$. From the definitions of the uncertainty radii $\epsilon_1$ and $\epsilon_2$, the maximum normalized estimation error of the eavesdropping links is defined as $\delta_t = \epsilon_l / \|h_{EU}\|$, where $l \in \{1, 2\}$. Since the UAV usually flies higher than the RIS, the ground user and the eavesdropper in the DL transmission, the Rician factors for the U-G and U-E links are set to $\beta_{UG} = \beta_{UE} = 10$ dB, while the Rician factors for the R-G, R-E, and U-R links are set to $\beta_{UR} = \beta_{RG} = \beta_{RE} = 3$ dB. The corresponding Rician factors in the UL transmission are similar to the DL transmission, i.e., $\beta_{GU} = 10$ dB and $\beta_{RU} = \beta_{GR} = \beta_{GE} = 3$ dB. The initial feasible solutions of our proposed JO algorithm is given by the JO/HT algorithm. The remaining parameters are as follows: $q_0 = [-500, 20]^T$ m, $q_F = [500, 20]^T$ m, $w_G = [0, 120]^T$ m, $w_E = [200, 150]^T$ m, $w_R = [0, 0]^T$ m, $z_U = 100$ m, $z_R = 40$ m, $v_{\text{max}} = 30$ m/s, $\delta_t = 0.4$ s, $M = M_z \times M_y = 6 \times 5$, $\sigma^2 = -80$ dBm, $d = 5$, $\alpha = 2.2$, $\kappa = 3.3$, $\zeta = 3.4$, $\rho = -30$ dB, $\epsilon_c = 10^{-3}$, $J_{\text{max}} = 40$, $P_{\text{peak}} = 4\hat{P}$, and $G_{\text{peak}} = 4\hat{G}$.

In particular, we assume that all wiretap channels have the same maximum normalized estimation error variance, namely, $\delta_1 = \delta_2 = \delta_a$.

Fig. 2 plots the average worst-case secrecy rate of the proposed algorithm versus the number of iterations under different flight periods with $w = 0.5$, $\delta_a^2 = 0.5$ and $P = \hat{G} = 20$ dBm. It is observed that our proposed algorithm can quickly converge after around 10 iterations, and the average worst-case secrecy rate increases by increasing the flight time $T$.

In Fig. 3, we illustrate the UAV trajectories for different algorithms by setting $T = 124$ s, $\delta_a^2 = 0.5$, $P = \hat{G} = 20$ dBm, and $w = 0.5$. Fig. 3(a), Fig. 3(b), and Fig. 3(c) show more than 100 UAV trajectories by using the JO, JO/NPB and JO/NR algorithms, respectively, when $T$ is sufficiently large (e.g., $T = 124$ s). From Fig. 3 and Fig. 4, it is observed that, for all the algorithms, the UAV first flies to a certain location at $V_{\text{max}}$, then keeps static, and finally flies to the final location at $V_{\text{max}}$. However, as for the JO/NPB algorithm, the UAV first flies directly to a certain location where the UAV is close to the ground user and away from the eavesdropper as possible as it can, then hovers as long as possible, and finally flies along a relatively direct path to the final location in order to avoid being eavesdropped. By contrast, for the JO and JO/NR algorithms, the UAV tends to fly along an arc path to a certain location between the ground user and the RIS, then it hovers as long as possible, and finally reaches the final location. This is because the JO and JO/NR algorithms balance the channel gains between the direct links (i.e., the U-G, U-E, G-U, and G-E links) and reflecting links (i.e., the U-R-G, U-R-E, G-R-U, and G-R-E links) in each time slot in order to choose a trajectory, so as to achieve the best communication quality. Besides, since the JO algorithm takes the CSI uncertainty into account, the UAV trajectories of the JO algorithm under different channel realizations are more decentralized than those of the JO/NR algorithm under different channel realizations.

In Fig. 5, we show the average worst-case secrecy rates for different algorithms versus $T$ with $w = 0.5$, $\delta_a^2 = 0.5$, and $P = \hat{G} = 20$ dBm. At the hovering location, the trade-off between enhancing the quality of the legitimate links and weakening the quality of the eavesdropping links is achieved for the UAV. Therefore, the maximum secrecy rate is achieved at the hovering location and the longer the UAV remains static at the hovering location, the larger the average worst-case secrecy rate is. This is the reason why the average worst-case secrecy rates of all the algorithms increase with $T$. In particular, our proposed algorithm exceeds all the benchmark schemes. This shows that, with the aid of the proposed robust joint design of the UAV trajectory, RIS’s passive beamforming, and $\delta_a^2 = 0.5$, and $P = \hat{G} = 20$ dBm. At the hovering location, the trade-off between enhancing the quality of the legitimate links and weakening the quality of the eavesdropping links is achieved for the UAV. Therefore, the maximum secrecy rate is achieved at the hovering location and the longer the UAV remains static at the hovering location, the larger the average worst-case secrecy rate is. This is the reason why the average worst-case secrecy rates of all the algorithms increase with $T$. In particular, our proposed algorithm exceeds all the benchmark schemes. This shows that, with the aid of the proposed robust joint design of the UAV trajectory, RIS’s passive beamforming,
and transmit power control, the secrecy rate performance can be effectively improved. Furthermore, it is worth noting that the JO/NR algorithm outperforms the other benchmark algorithms. This demonstrates that even though the CSI uncertainty of the eavesdropping channels is not taken into account, which leads to inaccurate optimization, the joint design of the UAV trajectory, passive beamforming, and transmit power can still achieve a considerable gain, as compared with the counterpart schemes.

In Fig. 6 we investigate the average worst-case secrecy rates for different algorithms versus $\delta^2_a$ with $w = 0.5$, $T = 124$ s, and $\bar{P} = \bar{G} = 20$ dBm. We observe that the average
Hence, the JO algorithm not only considers how to increase the legitimate rates between the UAV and the ground user, but also considers how to decrease the wiretap rate from the UAV to the eavesdropper. This is also the reason why the first half paths, i.e., the paths from the initial location to the hovering location, when \( w = 0.9 \) are more decentralized than those when \( w = 0.1 \). Besides, in the second half paths, i.e., the paths from the hovering location to the final location, the UAV is closer to the eavesdroper than in the first half paths. Thus, when \( w \) is sufficiently large (e.g., \( w = 0.9 \)), the UAV is inclined to fly along relatively direct paths to the final location, so as to avoid the information leakage and increase the secrecy rate.

V. Conclusion

In this paper, as a supplement of the higher-layer encryption techniques, we studied a novel RIS-assisted UAV physical-layer secure communication, aiming at integrating RIS and UAV technologies for improving the system secrecy rate. In particular, a single flight time slot is allocated to the DL and UL transmissions between the UAV and the ground user, while the legitimate channels are wiretapped by an eavesdropper. Since the eavesdroppers always avoid being detected by the legitimate transmitter, the acquisition of the CSI of the eavesdropping channel is usually imperfect. Thus, we focused our attention on the joint and CSI-robust design of the UAV’s trajectory, RIS’s passive beamforming, and transmit power of the legitimate transmitter in order to maximize the average worst-case secrecy rate of the considered communication system. Although the formulated problem is intractable due to its non-convexity, we proposed an efficient algorithm to approximately solve it by applying the AO, SCA, S-Procedure, and SDR techniques. Simulation results demonstrated that the assistance of an RIS is beneficial to substantially improve the secrecy rate performance, and the joint design of UAV trajectory, RIS’s passive beamforming, transmit power of the legitimate transmitter can achieve a substantial gain. In addition, the robustness of our proposed algorithm was confirmed with respect to inaccurate estimates of the CSI of the wiretap channels.

The findings of this paper can be used as a reference for the study of the multi-user scenario. We now briefly discuss the extension of our proposed scheme to the multi-user scenario. Clearly, if an orthogonal multiple access protocol is employed, our proposed single-user scheme can be directly applied, except that an effective user scheduling strategy should be developed to schedule the data transmission of multiple users. If a non-orthogonal multiple access protocol is considered, then our proposed scheme cannot be directly applied and an effective interference cancellation algorithm is required to suppress the interference between multiple users. However, a detailed discussion of this issue is beyond the scope of this paper, and we leave this as future work.

REFERENCES

Fig. 7. UAV trajectories of the JO algorithm by different $w$ with $T = 124$ s, $\delta_a = 0.5$, $\bar{P} = \bar{G} = 20$ dBm


