UAV-Enabled Secure Data Dissemination via Artificial Noise: Joint Trajectory and Communication Optimization

AN LI, (Senior Member, IEEE), WENJING ZHANG, AND SHAOTING DOU
Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
Corresponding author: An Li (lian@ncu.edu.cn)

This work was supported in part by the NSFC under Grant 41504026 and Grant 61362009, in part by the Foundation for Distinguished Young Talents Training Programme of Jiangxi under Grant 20171BCB23006, and in part by the Graduate Innovation Special Fund of Nanchang University under Grant CX2018143.

ABSTRACT This paper studies a single UAV-enabled secure data dissemination system, in which the UAV is employed as an aerial base station to secretly communicate with multiple ground users. To prevent confidential signal intended to scheduled users overhearing by unscheduled ones, artificial noise (AN) is introduced and the UAV transmits a mixture of intended signal and a priori known AN to scheduled user at each time slot. The trajectory and the power splitting factor of UAV as well as the user scheduling are jointly optimized to maximize the minimum average secrecy rate over a finite flight period. To address the non-convexity of the formulated problem, an efficient iterative algorithm is presented based on alternating optimization and successive convex optimization techniques, which can ensure convergence to at least a local optimal solution. Simulation results show significant secrecy gains of the proposed design over benchmark scheme with circular trajectory.

INDEX TERMS Physical layer security, UAV-enabled data dissemination, artificial noise, max-min secrecy rate, trajectory design.

I. INTRODUCTION
As forecasted by IHS Markti [1], the number of IoT-connected devices would rise up to approximately 80 billion worldwide by 2025. Such massive deployments in various areas such as smart home, wearables, and agricultural monitoring, etc., are poised to create profound change in the interaction between humans and machines and make the world smarter and more connected [2], [3]. One of the core pillars of IoT building our connected life is enhanced data dissemination through multi-hop routing from the fixed ground base station (BS) to the physical IoT nodes to efficiently manage data. Such static ground BS architecture faces the following two major challenges. First, the energy consumption of IoT nodes in different location is unbalanced. The closer a IoT node is to the static BS, the more quickly its energy is depleted because of the heavier load, thus resulting in energy hole and significantly shortening the entire lifetime of IoT system. Second, multi-hop routing makes the forwarded confidential information more vulnerable to eavesdropping by illegitimate ground nodes close to legitimate IoT nodes along relaying path, thus introducing significant computation and control overheads for resource constrained IoT nodes to safeguard multi-hop system.

Recently, unmanned aerial vehicles (UAVs) have emerged as a promising solution for providing reliable and cost-effective wireless communications [4], [5] owing to their inherent attributes such as controllable mobility, high flexibility, adaptive altitude, and line-of-sight (LoS) air-to-ground link. For instance, Google launched project Loon that deploys UAVs to enable ubiquitous Internet connectivity [6]. After authorized by FAA, Qualcomm and AT&T are trailing to employ UAVs to deliver wide-scale wireless access in the 5G networks [7]. Amazon Prime Air and Google’s Project Wing initiative is an exciting new user case for cellular-connected UAVs [8]. Meanwhile, many researchers from academia have devoted extensive efforts to using UAVs as enablers of multifarious substantial applications including UAV-aided ubiquitous coverage [9], [10], information dissemination or data collection [11]–[13], aerial cloud computing [14]–[16],
flying cellular-connected users [17], [18], and energy broadcasting [19], etc. In particular, employing UAVs as flying BSs to disseminate data for ground IoT nodes is able to overcome the aforementioned drawbacks facing the static ground BS. By properly designing UAV’s trajectory and ground IoT nodes’ communication scheduling, UAV is capable of sequentially visiting all IoT nodes and transferring data only in single-hop range instead of multi-hop transmission, thus maintaining the energy balance among all IoT nodes. However, the openness of UAV-to-ground wireless channels makes information transmission over LoS links more susceptible to terrestrial eavesdropping, which leads to a new and challenging security problem.

Pioneered by Wyner’s work [20], physical layer security has received growing attention to secure viable keyless wireless transmission by harnessing the intrinsic physical properties of wireless channels, such as thermal noise, interference, and fading [21], [22]. However, the feasibility of physical layer security is highly dependent on the superiority of the main channel between the source and the destination to the wiretap channel between the source and the eavesdropper. Various physical layer security techniques based on artificial noise (AN) or cooperation have been investigated in the literature to create the main channel quality advantage for traditional terrestrial wireless communication [23]. Furthermore, additional degree of freedom provided by the fully controllable UAV mobility brings new opportunity to guarantee the expected channel superiority and thus enhance secrecy performance [24], [25]. Reference [26] first investigated secure both downlink and uplink UAV communications against the ground eavesdropper with known position, where joint UAV trajectory and transmit power optimization algorithms are designed to maximize the average achievable secrecy rate. Reference [27] considered a more practical UAV-to-ground communication scenario where the eavesdroppers’ locations are not perfectly known but bounded within given circular regions. The average worst case secrecy rate is maximized by jointly optimizing the UAV trajectory and transmit power. Meanwhile, UAV-enabled friendly jamming scheme was first presented in [28], which is extended to dual UAV-enabled communications where one UAV serves as an aerial BS transmitting confidential messages and another acts as a mobile jammer sending AN to interfere ground eavesdroppers [29], [30]. It is shown that such UAV-enabled jamming schemes can further improve the secrecy rate by joint single/multiple-UAV trajectory optimization and resource allocation, but introducing extra resource loss for the exploitation of cooperative UAV jammer.

Motivated by the above studies, in this paper, we consider secure single UAV-enabled data dissemination where a UAV-BS wishes to covertly communicate with a group of ground users. Specifically, time-division multiple access (TDMA) protocol is adopted where at each time slot, the UAV transmits confidential information intended to one scheduled user. To keep it secret from unscheduled ones since they could be potential eavesdroppers, AN is introduced to further improve the security performance. Independent AN is added to the intended signal at UAV but only the scheduled user is able to cancel it before decoding the private information. Under given UAV transmit power, although increasing the transmit power to AN can boost degrading the eavesdropping channel, the main channel rate may reduce resulting from the decrease of allocated power to intended signal. Apparently, the coefficient of power splitting at UAV should be carefully designed to enhance the superiority of the main channel. As a result, to guarantee fairness among all ground users, our goal is to maximize the minimum average secrecy rate by jointly optimizing the UAV trajectory, transmit power splitting factor as well as user scheduling over a finite flight period. The formulated minimum secrecy rate maximization problem is a non-convex problem and difficult to be solved efficiently. To tackle this problem, we propose an efficient iterative algorithm by applying successive convex optimization and alternating optimization techniques to find a locally optimal solution. Numerical results manifest the proposed algorithm outperforms benchmark scheme with circular trajectory.

The rest of this paper is organized as follows. Section II introduces the system model and formulates the max-min secrecy rate problem of UAV-enabled secure data dissemination. A suboptimal solution and corresponding iterative algorithm are presented to jointly optimize the user scheduling, UAV’s power splitting factor and trajectory in Section III. Simulation results and conclusion are exhibited in Section IV and Section V respectively.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig.1, we consider a single UAV-enabled secure data dissemination system where a UAV is dispatched to deliver a confidential information to one of $K$ group users periodically with duration $T$ in second (s). Each period $T$ is divided into $N$ equally spaced time slots. Note that the number of time slots $N$ is appropriately chosen such that the movement change of UAV relative to the ground users within each slot can be ignored approximately. During any period to facilitate downlink multiple users transmission, the UAV serves all the $K$ users via TDMA-based protocol in which
the UAV transmits the intended data to at most one scheduled user at each time slot. To guarantee the security of data, AN, known a priori for the scheduled user, is introduced to prevent other unscheduled users from intercepting the transmitted data. Similar as in [31], [32], in each time slot the UAV splits the available power into two parts, one for sending the secret information to the scheduled user, another for creating artificial interference to the unscheduled users. Note that we assume the AN is shared between the UAV and the scheduled user, and all channel state knowledge are available, thus it will just confuse the unscheduled users’ listening but not cause any harm to the scheduled user since the scheduled user can completely eliminate it from the received signal. In practice, the secure sharing of AN can be implemented by the PHY-layer “key” distribution method in [33] with a small amount of overhead. Specifically, the same AN generator and seed tables are first pre-stored at both the UAV and the scheduled user (but not available at the unscheduled users). Next the index of one seed randomly selected from the seed table is shared between the UAV and the scheduled user before each transmission via a two-step phase-shift modulation-based method as follows. In the first step, the scheduled user sends a pilot signal for the UAV to estimate the channel phase from the UAV to the scheduled user. In the second step, the UAV randomly selects a seed index, and transmits it with phase modulation after pre-compensating the phase offset of the channel estimated in the previous step. Thus, the scheduled user can decode the seed index transmitted by the UAV from the phases of the received signal. Since the length of this seed index sharing procedure is very short and the channel phase of the received signal. Since the length of this seed index is secretly sent from the UAV to the scheduled user in such a short time period. Meanwhile, the UAV’s high mobility can be fully exploited to help the UAV move as close as possible to the scheduled user, thus obtaining a better secure communication link. It is worth noting that such proposed strategy provides a theoretical upper bound for the achievable secrecy rate of the UAV-enabled secure data dissemination system although it may not be optimal since certain common information a priori is assumed to be secretly shared between the UAV and the scheduled user. Meanwhile, such proposed strategy is also applicable to the worst case where the AN is the same as the additive noise and can not be cancelled at the scheduled user.

Without loss of generality, we consider a three-dimensional Cartesian coordinate system where the location of each ground user \( k \) is fixed at \( w_k = [x_k, y_k, 0]^T \), \( k \in K \triangleq \{1, \cdots, K\} \), which is known to the UAV. The coordinate of UAV at time slot \( n \) is denoted as \( q(n) = [x(n), y(n), H]^T \), \( n \in \mathcal{N} \triangleq \{1, \cdots, N\} \), where the UAV is assumed to fly at a constant altitude \( H \) in meter (m) above the ground level. In practice, \( H \) may be specified according to government regulations [34] for safety consideration without unnecessary energy consumption for frequent aircraft ascending or descending. Over period \( T \) with sufficiently large (small) \( N (T/N) \), all the line-segments connecting \( N \) discrete locations \( q(n), n \in \mathcal{N} \) approximately represents the UAV’s trajectory, which needs to satisfy the following mobility constraints

\[
q[1] = q[N], \quad (1a)
\]
\[
\|q[n+1] - q[n]\| \leq V_{\text{max}} \frac{T}{N}, \quad n \in \mathcal{N}, \quad (1b)
\]

where \( V_{\text{max}} \) is the maximum allowed speed of UAV. (1a) means that the UAV should return to its starting location after each period. Similar to [26], the channels of UAV-to-ground users adopt the simple LoS links where the channel gains only depend on the distance between the UAV and ground users, and the Doppler effect can be compensated by the scheduled user simultaneously. Therefore, the channel power gain from the UAV to user \( k \) at slot \( n \) can be given by

\[
h_k[n] = \rho_0 d_k^{-2}[n] = \frac{\rho_0}{\|q[n] - w_k\|^2 + H^2}, \quad k \in K, \quad n \in \mathcal{N},
\]

(2)

where \( d_k[n] \) is the distance from the UAV and the \( k \)-th ground user in slot \( n \), and \( \rho_0 \) denotes the channel power gain at a reference distance \( d_0 = 1 \) m.

For TDMA-based secure data-dissemination system, the UAV only sends information to at most one scheduled user among all \( K \) ground users each slot, while the information sent to the scheduled user should be kept secret from other unscheduled users. At any slot \( n \in \mathcal{N} \), we use a binary indicators \( g_k[n] \in \{0, 1\}, k \in K \) to denote the user communication scheduling in the system. In time slot \( n \), the UAV transmits its indented information to the user \( k \) if \( g_k[n] = 1 \); otherwise, \( g_k[n] = 0 \). Due to TDMA, the following constraints should be satisfied

\[
g_k[n] \in \{0, 1\}, k \in K, \quad \sum_{k \in K} g_k[n] \leq 1, \quad n \in \mathcal{N}. \quad (3)
\]

Let \( P_s[n] = P_s \) denote the UAV’s transmit power each slot. To degrade the UAV-unscheduled users’ channel, the transmitted signal of UAV is a mixture of the message signal and the AN. Let \( 0 \leq \alpha[n] \leq 1 \) represent the power splitting coefficient at UAV within slot \( n \), which is the ratio of power allocated for the intended signal to the total transmit power \( P_s \). The remaining fraction \((1 - \alpha[n])\) of \( P_s \) is used to generate the AN. Accordingly, when user \( k, k \in K \) is scheduled for communicating with the UAV in time slot \( n \), i.e. \( g_k[n] = 1 \), the achievable rate \( R_k[n] \) from the UAV to scheduled user \( k \) in bits/second/Hertz (bps/Hz) can be written as

\[
R_k[n] = \log_2 \left( 1 + \frac{h_k[n]\alpha[n]P_s}{\sigma^2} \right) = \log_2 \left( 1 + \frac{\gamma_0 \alpha[n]P_s}{\|q[n] - w_k\|^2 + H^2} \right), \tag{4}
\]

where \( \sigma^2 \) denotes the noise power at the receiver, and \( \gamma_0 = \frac{\rho_0}{\sigma^2} \) is the reference signal-to-noise ratio (SNR). Note that in reality, the cancelation of AN at the scheduled user can never be perfect, nevertheless the residue interference owing to
the imperfect cancelation of AN could be included in $\sigma^2$. Similarly, the achievable rate $R_j[n]$ from the UAV to unscheduled users $j, (j \in K, j \neq k)$ in bps/Hz is given as

$$R_j[n] = \log_2\left(1 + \frac{h_j[n]a[n]P_s}{\sigma^2 + h_j[n](1 - a[n])P_s}\right)$$

$$= \log_2\left(1 + \frac{\gamma_0a[n]P_s}{\|q[n] - w_j\|^2 + H^2 + \gamma_0(1 - a[n])P_s}\right).$$

(5)

With (4) and (5), the average achievable worst-case secrecy rate in bps/Hz for the scheduled user $k$ over period $T$ can be expressed as

$$R_{S,k} = \frac{1}{N} \sum_{n=1}^{N} g_k[n] \left[ R_k[n] - \max_{j \neq k} R_j[n] \right]^+,$$

(6)

where $[x]^+ = \max\{x, 0\}$.

Let the user scheduling $G = \{g_k[n], k \in K, n \in N\}$, the UAV’s transmit power splitting factor $A = \{a[n], n \in N\}$ and the UAV’s trajectory $Q = \{q[n], n \in N\}$. Taking into account the fairness among all ground users, our goal is to maximize the minimum average achievable worst-case secrecy rate of the system by jointly optimizing the user scheduling $G$, the transmit power splitting factor $A$ and trajectory $Q$ of UAV over all the time slots subject to UAV’s mobility constraints in (1). Let define $\eta(G, A, Q) = \min_{k \in K} R_{S,k}$, so that the optimization problem can be formulated as

\[\begin{align*}
\text{(P1)}: \quad & \max_{G,A,Q} \eta \\
\text{s.t.} & \quad \frac{1}{N} \sum_{n=1}^{N} g_k[n] \left[ R_k[n] - \max_{j \neq k} R_j[n] \right]^+ \geq \eta, \quad k \in K, \\
& \quad 0 \leq a[n] \leq 1, \quad n \in N, \\
& \quad (1), (3).
\end{align*}\]

It can be first observed that for problem (P1), the operation $[x]^+$ makes the minimum secrecy rate constraints non-smooth at the point 0. Second, the optimization scheduling parameters $G$ are binary, thus involving integer constraints (3). Third, the constraints (7b) and (1) are all non-convex with respect to UAV’s trajectory $Q$ and power splitting factor $A$. For these reasons, (P1) is challenging to be solved in general since it is a mixed-integer non-convex problem. To tackle the above difficulty, we propose an efficient iterative algorithm by leveraging successive convex optimization and alternating optimization techniques for approximately solving (P1), which is guaranteed to converge to at least a locally optimal solution.

**III. PROPOSED SOLUTION**

First, we tackle the non-smooth constraints on the basis of the following Lemma.

**Lemma 1:** Problem (P1) achieves the same optimum value as the following problem

\[\begin{align*}
\text{(P2)}: \quad & \max_{G,A,Q} \eta \\
\text{s.t.} & \quad \frac{1}{N} \sum_{n=1}^{N} g_k[n] \left( R_k[n] - \max_{j \neq k} R_j[n] \right) \geq \eta, \quad k \in K, \\
& \quad (1), (3).
\end{align*}\]

\[\begin{align*}
\text{(P3)}: \quad & \max_{\eta,G} \eta \\
\text{s.t.} & \quad \frac{1}{N} \sum_{n=1}^{N} g_k[n] \xi_k[n] \geq \eta, \quad k \in K, \\
& \quad g_k[n] \in \{0, 1\}, \\
& \quad \sum_{k \in K} g_k[n] \leq 1.
\end{align*}\]

Although problem (P3) is a binary integer programming, its closed-formed optimal solution can be attained as [30]

\[g_k^*[n] = \begin{cases} 
1, & \xi_k[n] > 0, \\
0, & \xi_k[n] \leq 0.
\end{cases}\]

**B. SUBPROBLEM 2: OPTIMIZING POWER SPLITTING FACTOR A**

Second, we determine the power splitting factor $A$ with any given user scheduling $G$ and UAV’s trajectory $Q$. 
Let $a_k, b_k = \frac{\gamma_0 P_s}{\|q[n] - w_k\|^2 + H^2}, c_k = \|q[n] - w_k\|^2 + H^2 + \gamma_0 P_s, c = -\gamma_0 P_s$, problem (P2) can be reformulated as

\begin{equation}
\begin{aligned}
\text{max}_{\theta, A} \quad & \eta \\
\text{s.t.} \quad & 1 \leq \sum_{n=1}^{N} g_k[n] \log_2 \left( 1 + a_k, n \alpha[n] \right) \\
& - \max_{j \neq k} \log_2 \left( 1 + \frac{-ca[n]}{b_j,n + ca[n]} \right) \geq \eta, k \in K, \\
& 0 \leq \alpha[n] \leq 1.
\end{aligned}
\end{equation}

To solve (P4), we introduce a slack variable $C = \{C_k[n] = k \in K \}$, and equivalently write (P4) as

\begin{equation}
\begin{aligned}
\text{max}_{\theta, A, C} \quad & \eta \lambda \\
\text{s.t.} \quad & 1 \leq \sum_{n=1}^{N} g_k[n] \log_2 \left( 1 + a_k, n \alpha[n] \right) \\
& - C_k[n] \geq \eta \lambda, k \in K, \\
& \log_2 \left( 1 + \frac{-ca[n]}{b_j,n + ca[n]} \right) \leq C_k[n], j \in K, j \neq k, \\
& 0 \leq \alpha[n] \leq 1.
\end{aligned}
\end{equation}

One can easily observe that (P5) is a strict convex optimization problem, which thus can be solved efficiently using standard convex optimization tools such as CVX [35].

**C. SUBPROBLEM 3: OPTIMIZING UAV'S TRAJECTORY Q**

Last but not the least, the UAV’s trajectory is optimized with fixed $G$ and $A$. We first introduce a new auxiliary variable $Z = \{z_k[n], k \in K, n \in N\}$, such that

\begin{equation}
\begin{aligned}
z_k[n] \geq \|q[n] - w_k\|^2 + H^2, k \in K, n \in N, \\
z_k[n] \leq \|q[n] - w_j\|^2 + H^2, j \in K, j \neq k, n \in N.
\end{aligned}
\end{equation}

Let $d_n = \alpha[n]P_s\gamma_0, e_n = (1 - \alpha[n])P_s\gamma_0$, then the problem to find the UAV’s trajectory can be expressed as

\begin{equation}
\begin{aligned}
\text{max}_{\eta, Q, Z, C} \quad & \eta \lambda \gamma \\
\text{s.t.} \quad & 1 \leq \sum_{n=1}^{N} g_k[n] \log_2 \left( 1 + d_n \right) \\
& - C_k[n] \geq \eta \lambda, k \in K, \\
& \log_2 \left( 1 + \frac{d_n}{z_j[n] + e_n} \right) \leq C_k[n], j \in K, j \neq k, \\
& (1), (13).
\end{aligned}
\end{equation}

Problem (P6) is equivalent to (P5) since the constraint (13) must hold with equality. This is because if the constraint in (13) is met with inequality, the objective value to (P6) can be improved by reducing (increasing) $C_k[n]/z_j[n]$ [zj[n]]. Note that (P6) is still non-convex due to the non-convex constraints in (13b) and (14b). To address the non-convexity of constraints (13b) and (14b), we adopt the successive convex optimization technique to successively approximate the primal problem (P6) into a convex one at a given initial point in each iteration. Specifically, denote $Q^{(r)} = \{q^{(r)}[n], n \in N\}$ as the given UAV trajectory at the $r$-th iteration. Since the term $\log_2 \left( 1 + \frac{d_n}{z_j[n]} \right)$ in (14b) is a convex function with respect to $z_k[n]$, we can obtain its globally concave lower bound by using the first-order Taylor expansion at the given point $q^{(r)}[n]$. Therefore, with given initial trajectory $Q^{(0)}$ at the $r$-th iteration, we can obtain the following lower bound, i.e.,

\begin{equation}
\begin{aligned}
\log_2 \left( 1 + \frac{d_n}{z_j[n]} \right) \geq A_k[n] + B_k[n](z_k[n] - z_k^{(r)}[n]) \\
= \tilde{R}_k[n], k \in K,
\end{aligned}
\end{equation}

where $A_k[n] = \log_2 \left( 1 + \frac{d_n}{z_j[n]} \right)$ and $B_k[n] = -\frac{1}{m z_k^{(r)}[n] + d_n}$. Similarly, since $\|q[n] - w_j\|^2$ is also a convex function with respect to $q[n]$, a concave lower bound of $\|q[n] - w_j\|^2$ in constraint (13b) can be attained by applying the first-order Taylor expansion as

\begin{equation}
\|q[n] - w_j\|^2 \geq -\|q^{(r)}[n]\|^2 + 2[q^{(r)}[n] - w_j]^T q[n] + \|w_j\|^2 = D_j[n], j \in K, j \neq k.
\end{equation}

With the lower bounds in (15) and (16), at the $r$-th iteration, a convex approximated problem for (P6) can be constructed as

\begin{equation}
\begin{aligned}
\text{max}_{\eta^{(r)}, Q, Z, C} \quad & \eta \lambda \gamma \\
\text{s.t.} \quad & 1 \leq \sum_{n=1}^{N} (\tilde{R}_k[n] - C_k[n]) \geq \eta \lambda \gamma, k \in K, \\
& \log_2 \left( 1 + \frac{d_n}{z_j[n] + e_n} \right) \leq C_k[n], j \in K, j \neq k, \\
& z_j[n] - H^2 \leq D_j[n],
\end{aligned}
\end{equation}

Obviously, (P7) is a convex optimization problem and thus can be efficiently solved by standard convex optimization tools such as CVX. Note that since the first-order Taylor expansions in (15) and (16) at the given point $q^{(r)}[n]$ give their global under-estimators, the objective function value of the approximate problem (P7) provides a lower bound of that of the primal problem (P6).

**D. OVERALL ALGORITHM**

To sum up, an efficient iterative algorithm for sub-optimally solving (P2) is summarized in Algorithm 1 by applying the alternating optimization method. Specifically, the user scheduling $G$, UAV’s power splitting factor $A$ and trajectory

\[\text{Algorithm 1: Iterative Algorithm for Sub-Optimal Solution} \]

1 It is shown in Section III-D that $Q^{(r)}$ is the obtained solution in the $(r-1)$-th iteration, and the initial trajectory $Q^{(0)}$ is given in Section IV.
Algorithm 1 Proposed Iterative Algorithm for Problem (P2)

1: Initialize $A^{(0)}, Q^{(0)}$ and slack variable $Z^{(0)}$. Let $r = 0$.
2: repeat
3: Obtain user scheduling $G^{(r+1)}$ using the closed-formed solution (10) with fixed $Q^{(r)}$ and $A^{(r)}$.
4: Solve problem (P5) to update UAV’s power splitting factor $A^{(r+1)}$ with given $G^{(r+1)}$ and $Q^{(r)}$.
5: Update UAV’s trajectory $Q^{(r+1)}$ and the slack variable $Z^{(r+1)}$ by solving problem (P7) with given $G^{(r+1)}$, $A^{(r+1)}$ and the slack variable $Z^{(r)}$.
6: Set $r = r + 1$.
7: until The fractional increase of the objective function value of (P2) is below a small threshold $\epsilon > 0$.

$Q$ are successively optimized via solving problem (P3), (P5) and (P7) respectively, while fixing the other variables. Then, the local solution obtained from each iteration is used as the input of the next one until convergence.

Next, we show the convergence analysis for the proposed Algorithm 1. Let define $\eta_Q^{(b,r)}(G^{(r)}, A^{(r)}, Q^{(r)}) = \eta_Q^{(r)}$ as the objective function values of (P7) at the $r$-th iteration. Since (P3) and (P5) are optimal solved, we have

$$
\eta(G^{(r)}, A^{(r)}, Q^{(r)}) \leq \eta(G^{(r+1)}, A^{(r+1)}, Q^{(r)}) \\
\leq \eta(A^{(r+1)}, A^{(r+1)}, Q^{(r)}) \\
\leq \eta(A^{(r+1)}, A^{(r+1)}, Q^{(r)}) \\
\leq \eta(Q^{(r+1)}, A^{(r+1)}, Q^{(r)}) ,
$$
(18)

where (a) and (b) holds since (P4) is equivalent to (P5). For the optimization of UAV’s trajectory, since the first-order Taylor expansions in (15) and (16) are tight at the given local point $Q^{(r)}$, it follows that

$$
\eta(G^{(r+1)}, A^{(r+1)}, Q^{(r+1)}) \leq \eta(G^{(r+1)}, A^{(r+1)}, Q^{(r+1)}) \\
\leq \eta(G^{(r+1)}, A^{(r+1)}, Q^{(r+1)}) \\
\leq \eta(Q^{(r+1)}, A^{(r+1)}, Q^{(r+1)}) ,
$$
(19)

where (c) holds since with given $G^{(r+1)}$ and $A^{(r+1)}$, (P7) is solved optimally, and (d) is true because the objective value of (P7) always provides a lower bound for that of (P6). Combining (18) and (19), we can obtain

$$
\eta(G^{(r)}, A^{(r)}, Q^{(r)}) \leq \eta(G^{(r+1)}, A^{(r+1)}, Q^{(r+1)}) ,
$$
(20)

which demonstrates that the objective function value of (P2) is non-decreasing over the iterations, thus the proposed Algorithm 1 is guaranteed to converge to a locally optimal solution.

IV. NUMERICAL RESULT
In this section, numerical results are provided to manifest the performance of the proposed joint optimization of the user scheduling and the UAV’s power splitting factor as well as the trajectory design (denoted by “Proposed optimization”). For comparison, we also consider a benchmark algorithm with circular trajectory (denoted by “Circular trajectory”). Specifically, the center of the circular trajectory locates at the geometric center of users $c_k = \frac{\sum_{k=1}^{K} w_k}{K}$. Denote the distance between $c_k$ and the $k$-th user as $r_k = \|c_k - u_k\|$. To balance the users’ number inside and outside the trajectory circle, the radius of circular trajectory is chosen as $r_u = \frac{1}{2}(\max(r_k) + \min(r_k))$. Note that under given finite UAV’s flight time $T$ and maximum speed $V_{\text{max}}$, $r_u$ may not be achievable if $2\pi r_u > V_{\text{max}} T$. In this case, the maximum allowed radius can be attained as $r_{\text{max}} = \frac{V_{\text{max}} T}{2\pi}$. Consequently, the trajectory circle radius is set as $r_{\text{trj}} = \min(r_{\text{max}}, r_u)$. Let $\theta_{\ell} = 2\pi \frac{n-1}{N}$, $n \in \mathcal{N}$, then the circle trajectory is obtained as:

$$
q_{\text{trj}}[n] = c_u + [r_{\text{trj}} \cos \theta_{\ell}, r_{\text{trj}} \sin \theta_{\ell}, H]^T, \quad n \in \mathcal{N}.
$$
(21)

Given this circular trajectory, the “Circular trajectory” algorithm optimizes the user scheduling and the UAV’s power splitting factor by solving (P3) and (P5). The initial feasible trajectory $Q^{(0)} = (q_{\text{trj}}[n], n \in \mathcal{N})$ for the proposed “Proposed optimization” is generated by the “Circular trajectory” algorithm, i.e., $q_{\text{trj}}[n] = q_{\text{trj}}[n], n \in \mathcal{N}$.

Considering $K = 4$ ground users which locations are uniformly distributed in a given square area of $1500 \times 1500\text{m}^2$. The following results are attained based on one realization of the random users’ locations as shown in Fig.2. The altitude of UAV is fixed at $H = 50\text{m}$. The UAV’s maximum speed and the transmit power are set to $V_{\text{max}} = 40\text{m/s}$ and $P_s = 20\text{dBm}$, respectively. The duration of each equal-length slot is $d = 1\text{s}$. The reference SNR at $d_0 = 1\text{m}$ is $y_0 = 80\text{dB}$. The threshold in Algorithm 1 is set as $\epsilon = 10^{-4}$.

Fig.2 exhibits the optimized UAV’s trajectory as well as the normalized UAV speed and the power splitting factor of different algorithms with different periods $T$. The locations of ground users are marked with $\bigcirc$, $\diamond$, $+$, and $\times$, respectively. It is first observed from Fig. 2 that with the increase of $T$, for the proposed “Proposed optimization”, the UAV fully exploits its mobility to dynamically adjust its trajectory to fly closer to each scheduled user for shorter LoS links since the AN can be completely cancelled at the scheduled user. When $T$ is sufficiently large, e.g., $T = 500\text{s}$, the UAV flies at the maximum speed in a straight line to sequentially serve all the ground users and remains stationary above each scheduled user as long as possible (i.e., with a zero speed). This is because this hovering is able to make the scheduled user enjoy the best LoS channel. While for “Circular trajectory”, the UAV’s trajectory is restricted to fly along a circle, and the radius of circle increases as $T$ gets larger until reaching $r_u$. Furthermore, it is observed from Fig. 2(b), (d) and (f) that $\alpha$ increases when the UAV moves closer to the scheduled user, and vice versa. In particular for the proposed “Proposed optimization”, when the UAV is hovering on the top of the scheduled user, the maximum power proportion is used for the confidential information transmission. This is because the better LoS links the scheduled user possesses, the more power
A. Li et al.: UAV-Enabled Secure Data Dissemination via AN: Joint Trajectory and Communication Optimization

the UAV allocates to transmit the confidential information to enhance the scheduled user’s data rate. On the other hand, when the UAV serves a scheduled user with a closer neighbor unscheduled user, e.g. the user ◊, the maximum allowed $\alpha$ is smaller than that for another one with a farther neighbor unscheduled user, e.g. the user ♦ in order to more effectively jam the closer unscheduled user. This indicates that the more power should be allocated to generate the AN to confuse the closer neighbor unscheduled user’s listening, thus $\alpha$ should be optimized to strike a balance between improving

FIGURE 2. Trajectories, normalized speed and $\alpha$ of different algorithms for various $T$. 
the scheduled user’s data rate and deceasing the unscheduled user’s data rate. It is also observed that for the proposed “Proposed optimization”, the UAV employs a binary speed, i.e., it remains stationary for a certain duration when it arrives the served scheduled user, and flies at the normalized speed 1 otherwise, while for “Circular trajectory”, the UAV keeps flying at a constant normalized speed $V = \frac{2\pi r_{u,v}}{T_{vax}}$.

Fig.3 shows the achievable average max-min secrecy rate as a function of period $T$ for different algorithms when $P_s = 25\text{dBm}$ and $20\text{dBm}$. It is first shown that the max-min secrecy rate increases with $T$ as expected. This is because a larger $T$ provides more time to move closer to the served user, especially for “Proposed optimization” scheme to hover longer above the scheduled user, thus improving the max-min secrecy rate. It is also observed that the “Proposed optimization” scheme significantly outperforms the “Circular trajectory” algorithm, especially the performance gap between the two schemes gets larger with $T$. This is because the circular trajectory constraint makes that the scheduled user which is not around the circle experiences worse channels, and more power is allocated to jam the unscheduled users, which both impose the bottleneck for the max-min secrecy rate. While for “Proposed optimization” scheme, the UAV is able to fully exploit its mobility to move closer to or even remain stationary on the top of the scheduled user for better LoS links, and then more power can be allocated to transmit the secret information. As a result, the achievable max-min secrecy rate is improved.

Fig.4 illustrates the convergence speed for the proposed iterative algorithm. It is observed that the proposed Algorithm 1 is very efficient and it converges after carrying out very few iterations for different periods $T$. Meanwhile, the secrecy performance gap between the converged max-min secrecy rate and the initial one further demonstrates secrecy rate gain brought by joint optimization of the trajectory and the power splitting factor of the UAV as well as the user scheduling.

V. CONCLUSION

In this paper, we have investigated a single UAV-enabled secure data dissemination system by introducing AN. The achievable average minimum secrecy rate has been maximized by jointly optimizing the user scheduling, the UAV’s power splitting factor and the trajectory. To tackle the non-convexity of the optimized problem, an efficient iterative algorithm has been proposed based on alternating optimization and successive convex optimization techniques, which is guaranteed to converge to at least a locally optimal point. Numerical results have validated that the proposed algorithm can significantly enhance the system secrecy rate as compared to the benchmark scheme. It is worth noting that it is interesting to extend this work to the other reconfiguring passive jammer (e.g. with intelligent reflecting surface fixed mobile [36]).

REFERENCES

[1] IHS Markit. The Top Technology Trends of 2019 [EB/OL]. Accessed: Jun. 19, 2019. [Online]. Available: https://news.ihs.markit.com/press-release/technology/ihs-markit-white-paper-top-technology-trends-2019
[2] N. Chen, T. Qiu, X. Zhou, K. Li, and M. Atiquzzaman, “An intelligent robust networking mechanism for the Internet of Things,” IEEE Commun. Mag., vol. 57, no. 11, pp. 91–95, Nov. 2019.
[3] T. Qiu, J. Liu, W. Si, and D. O. Wu, “Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 27, no. 3, pp. 1028–1042, Jun. 2019.
[4] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, “A tutorial on UAVs for wireless networks: Applications, challenges, and open problems,” IEEE Commun. Survveys Tuts., vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.
[5] Y. Zeng, R. Zhang, and T. J. Lim, “Wireless communications with unmanned aerial vehicles: Opportunities and challenges,” IEEE Commun. Mag., vol. 54, no. 5, pp. 36–42, May 2016.
[6] K. Kamnani and C. Suratkar, “A review paper on Google Loon technique,” Int. J. Res. Sci. Eng., vol. 1, no. 1, pp. 167–171, 2015.
[7] Paving the Path to 5G: Optimizing Commercial LTE Networks for Drone Communication. [Online]. Available: https://www.qualcomm.com/news/press-room/2016/09/06/paving-path-5g-optimizing-commercial-lte-networks-drone-communication
[8] J. Stewart, “Google tests drone deliveries in project wing trials,” BBC World Service Radio, London, U.K., Tech. Rep. 28964260, 2014.
[9] H. Wu, X. Tao, N. Zhang, and X. Shen, “Cooperative UAV cluster-assisted terrestrial cellular networks for ubiquitous coverage,” IEEE J. Sel. Areas Commun., vol. 36, no. 9, pp. 2045–2058, Sep. 2018.
[10] T. Li, K. Ota, T. Wang, X. Li, Z. Cai, and A. Liu, “Optimizing the coverage via the UAVs with lower costs for information-centric Internet of Things,” *IEEE Access*, vol. 7, pp. 15292–15309, 2019.

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

[12] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, “Mobile Internet of Things: Can UAVs provide an energy-efficient mobile architecture?” in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC USA, Dec. 2016, p. 1.

[13] C. Zhan and Y. Zeng, “Completion time minimization for multi-UAV-enabled data collection,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 10, pp. 4859–4872, Oct. 2019.

[14] F. Luo, C. Jiang, S. Yu, J. Wang, Y. Li, and Y. Ren, “Stability of cloud-based UAV systems supporting big data acquisition and processing,” *IEEE Trans. Cloud Comput.*, vol. 7, no. 3, pp. 866–877, Jul. 2019.

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

[16] W. Chen, B. Liu, H. Huang, S. Guo, and Z. Zheng, “When UAV swarm meets edge-cloud computing: The QoS perspective,” *IEEE Netw.*, vol. 33, no. 2, pp. 36–43, Mar. 2019.

[17] M. M. Azari, F. Rosas, and S. Pollin, “Cellular connectivity for UAVs: Network modeling, performance analysis, and design guidelines,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3366–3381, Jul. 2019.

[18] S. Zhang, Y. Zeng, and R. Zhang, “Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization perspective,” *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2580–2604, Mar. 2019.

[19] J. Baek, S. I. Han, and Y. Han, “Optimal UAV route in wireless charging sensor networks,” *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1327–1335, Feb. 2020.

[20] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[21] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[22] D. S. Karas, A.-A.-A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, “Physical layer security in the presence of interference,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.

[23] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[24] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, “Physical layer security in UAV systems: Challenges and opportunities,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[25] Q. Wu, W. Mei, and R. Zhang, “Safeguarding wireless network with UAVs: A physical layer security perspective,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[26] G. Zhang, Q. Wu, M. Cui, and R. Zhang, “Securing UAV communications via joint trajectory and power control,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

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

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

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

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

[31] L. Dong, H. Yousefi zadeh, and H. Jafarkhani, “Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[32] H. Xing, L. Liu, and R. Zhang, “Secrecy wireless information and power transfer in fading wiretap channel,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[33] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[34] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodrigurez, and J. Yuan, “Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[35] M. Grant and S. Boyd, CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1 [EB/OL]. Accessed: Mar. 2016. [Online]. Available: http://cvxr.com/cvx

[36] Q. Wu and R. Zhang, “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,” *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

WENJING ZHANG received the B.S. degree from Henan Normal University, in 2017. She is currently pursuing the master’s degree with the Department of Electronics Information Engineering, Nanchang University. Her current research interests include physical layer security and UAV communication.

SHAOTING DOU received the B.S. degree from Linyi University, in 2019. She is currently pursuing the master’s degree with the Department of Electronics Information Engineering, Nanchang University. Her research interest includes physical layer security.