

# Secure Short-Packet Transmission with Aerial Relaying: Blocklength and Trajectory Co-Design

Milad Tatar Mamaghani\*, Xiangyun Zhou\*, Nan Yang\*, and A. Lee Swindlehurst†

\*School of Engineering, Australian National University, Canberra, ACT 2601, Australia

†Henry Samueli School of Engineering, University of California, Irvine, CA 92697, USA

Email: milad.tatarmamaghani@anu.edu.au, xiangyun.zhou@anu.edu.au, nan.yang@anu.edu.au, swindle@uci.edu

**Abstract**—In this paper, we propose a secure short-packet communication (SPC) system involving an unmanned aerial vehicle (UAV)-aided relay in the presence of a terrestrial passive eavesdropper. The considered system, which is applicable to various next-generation Internet-of-Things (IoT) networks, exploits a UAV as a mobile relay, facilitating the reliable and secure exchange of intermittent short packets between a pair of remote IoT devices with strict latency. Our objective is to improve the overall secrecy throughput performance of the system by carefully designing key parameters such as the coding blocklengths and the UAV trajectory. However, this inherently poses a challenging optimization problem that is difficult to solve optimally. To address the issue, we propose a low-complexity algorithm inspired by the block successive convex approximation approach, where we divide the original problem into two subproblems and solve them alternately until convergence. Numerical results demonstrate that the proposed design achieves significant performance improvements relative to other benchmarks, and offer valuable insights into determining appropriate coding blocklengths and UAV trajectory.

**Index Terms**—Beyond-5G networks, short-packet communication, unmanned aerial vehicle, aerial relaying, physical-layer security, trajectory and blocklength optimization.

## I. INTRODUCTION

Short-packet communication (SPC) is a critical component of emerging beyond-5G (B5G) wireless networks and Internet of Things (IoT) applications, where devices need to exchange short-packet data to fulfill low-latency and low-cost communication requirements. On the other hand, reduced channel coding gain associated with short-packet transmission poses a major hurdle to communication reliability in SPC. In addition, security issues such as eavesdropping in SPC-IoT networks are more pronounced due to confidential and sensitive SPC data that IoT networks frequently need to share in an open wireless environment, particularly for mission-critical scenarios [1]–[3]. Physical-layer security (PLS) technology is a promising candidate for safeguarding SPC. PLS techniques exploit the physical-layer characteristics of wireless channels or smart signaling for communication secrecy through wiretap coding, without suffering from the high complexity of resource-demanding key-based security methods [4].

This work was supported by the Australian Research Council’s Discovery Projects funding scheme (project number DP220101318).

Nevertheless, conventional PLS techniques adopt wiretap codes based on the assumption of infinite blocklengths. Substantial studies have thus far been conducted to secure different wireless networks working in the infinite blocklength regime (e.g., see [5], [6] and references therein). However, SPC generally involves the transmission of short packets on the order of tens of bytes as opposed to several kilobytes in conventional wireless systems. Consequently, PLS-based designs need to be meticulously revisited, as adopting the so-called *Secrecy Capacity*, i.e., a typical performance metric for conventional PLS systems [7], is no longer applicable for systems operating under SPC due to the finite blocklength assumption. In light of this, [8] fundamentally studied the attainable secrecy rate (SR) in a wiretap channel with specific reliability and secrecy requirements under the finite blocklength assumption. The authors in [9] and [10], developed PLS schemes for SPC assuming fading channels. The work in [11] holistically investigated the performance of secure SPC in a mission-critical IoT system with an external adversary. Nevertheless, these studies have only considered system designs that involve stationary communication nodes and adopted a fixed number of information bits per short-packet transmission. Consequently, the approaches developed in [9]–[11] may not work well in highly dynamic scenarios or when the number of information bits generated for transmission by IoT devices varies.

Unmanned aerial vehicles (UAVs), with their relatively rapid on-demand deployment, low-cost maintenance, and maneuverability, can potentially be used in a myriad of wireless applications ranging from serving as an aerial base station (BS) or mobile relay for remote sensing and real-time monitoring in IoT networks [12]. Accordingly, it has been anticipated that integrating UAV technology into forthcoming B5G IoT systems is a cost-effective promising solution with substantial benefits. Due to their operation at relatively high altitudes, UAVs are particularly helpful in improving coverage by reducing signal attenuation in wireless links caused by blockage or shadowing. As a result, UAV-empowered wireless IoT systems, if properly designed, would require less power for transmissions. This is specifically beneficial for energy-hungry IoT networks since it expands their operational lifetime. On the other hand, UAV-IoT scenarios are more susceptible to eavesdropping attacks due to line-of-sight (LoS)-dominant air-ground (AG) links [13]. Thus, securing such systems presents significant challenges, and of course, requires further research.

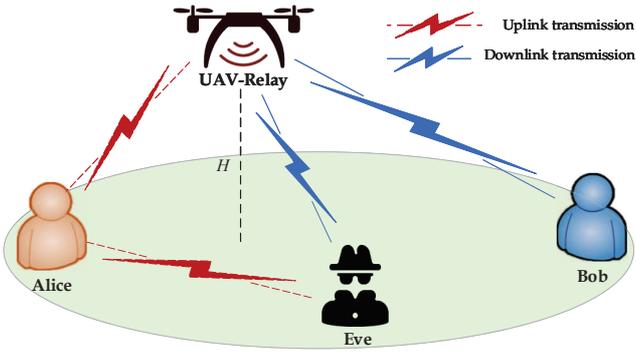


Fig. 1: System model for secure UAV-SPC relaying.

To address the above-mentioned challenges, in this work we propose a secure UAV-aided relaying scheme with SPC, where sensitive short packets need to be periodically transmitted from a remote IoT device to a designated receiver with a stringent latency requirement while combating passive eavesdropping. We formulate a new optimization problem for the considered UAV-aided SPC system under security, reliability, latency, and mobility constraints. The formulated problem is nonconvex, and hence challenging to solve optimally. To tackle the challenging nonconvex problem, we apply the block successive convex approximation (BSCA) approach to iteratively solve a sequence of convex subproblems: coding blocklength optimization and UAV trajectory design. We then propose a low-complexity algorithm combining these solutions to optimize the system performance. We conduct simulations to draw some useful insights into the performance of the proposed joint blocklength optimization and trajectory design, and highlight its secrecy performance advantage compared to other competitive benchmarks.

## II. SYSTEM MODEL AND ASSUMPTIONS

As illustrated in Fig. 1, we consider a UAV-aided IoT communication system with secure SPC, wherein a source (Alice) periodically sends short packets containing confidential information to a designated remote destination (Bob) via a mobile UAV-Relay (UR), while a passive eavesdropper (Eve) attempts to overhear the ongoing confidential transmissions. In practice, Alice periodically generates short-packet sensitive information from the environment and, if feasible, immediately transmits it to Bob with a stringent latency requirement. We assume that a packet is generated at the beginning of each *timeslot* and the period of each timeslot is  $\delta_t$ . We also assume that Alice generates and sends a varying amount of information bits during each timeslot to handle different tasks such as monitoring, controlling, or sensing.

In this work, we assume that the direct link between Alice and Bob is absent due to long distance or blockages, and hence a UAV-mounted relay is employed to facilitate the end-to-end SPC. Moreover, we assume that all the communication nodes are equipped with a single antenna, as commonly considered

for low-cost and resource-constrained IoT devices (see [14] and references therein). In addition, the mobile relaying strategy adopted by the UR is assumed to be the decode-and-forward (DF) protocol with time division duplexing (TDD), operating in a shared bandwidth  $W$  for both reception and transmission. We assume that the UR-aided DF relaying for SPC occurs at the beginning of each timeslot  $\delta_t$ , which consists of two phases. In the first phase (i.e., uplink transmission) in timeslot  $n$ , Alice generates a short packet, containing sensitive information, and transmits the packet with fixed power  $p_a$  to the UR over  $l_u[n]$  channel uses, where  $n = \{1, 2, \dots\}$  denotes the index of each timeslot, and then the UR decodes the received signal to obtain the transmitted confidential message. In the second phase (i.e., downlink transmission) in timeslot  $n$ , the UR encodes the obtained message from the first phase with a different codebook for security purposes, forwarding the result to Bob over  $l_d[n]$  channel uses with fixed relaying power  $p_r$  and Bob retrieves the original confidential information. While Eve wiretaps the ongoing transmissions in two phases to obtain confidential data, since the signals from both Alice and the UR are encoded with different codebooks, she cannot exploit a diversity combining strategy to improve her reception and pose stronger security threats. We also note that the end-to-end SPC generally occupies much less time than one timeslot. Since the time taken for one channel use is inversely proportional to the available bandwidth, we have  $\delta_i[n] = \frac{l_i[n]}{W} \forall n$ , where  $i \in \{u, d\}$ , and  $\delta_i[n]$  indicates the time needed for a finite blocklength SPC in either the uplink or downlink transmission.

The three-dimensional Cartesian coordinates of Alice, Bob, and Eve are denoted by  $\mathbf{q}_a = [x_a, y_a, 0]^T$ ,  $\mathbf{q}_b = [x_b, y_b, 0]^T$ , and  $\mathbf{q}_e = [x_e, y_e, 0]^T$ , respectively, where  $[\cdot]^T$  represents the transpose operator. Note that all the communication nodes are assumed to be a part of the same network; thus, the location of the communication nodes is perfectly known. Nonetheless, the information exchanged between Alice and Bob should be kept secret from Eve for confidentiality purposes. We assume that the UR's flight time horizon is set to  $T$ , and is split into  $N$  timeslots such that  $T = N\delta_t$ . Since the SPC duration is small, we assume that the UR's location over the transmission phase in each timeslot remains approximately unchanged, but varies from one timeslot to another. Furthermore, the altitude of the UR is fixed at  $H$ , which typically corresponds to the minimum flying altitude for being avoided by obstacles or mountainous areas, establishing LoS-dominant channel components [14]. Therefore, the UR's location in timeslot  $n$  can be denoted by  $\mathbf{q}_r[n] = [x[n], y[n], H]^T$ . As such, the UR's continuous trajectory can be approximated by  $(N + 1)$  waypoints, i.e.,  $\{\mathbf{q}_r[n]\}_{n=1}^N$ . Assuming that the UR's initial and final locations are denoted by  $\mathbf{q}_i = [x_i, y_i, H]^T$  and  $\mathbf{q}_f = [x_f, y_f, H]^T$ , respectively, the following mobility constraints are imposed on the UR trajectory:

$$\text{C1 : } \mathbf{q}_r[1] = \mathbf{q}_i, \mathbf{q}_r[N] = \mathbf{q}_f, \quad (1a)$$

$$\text{C2 : } \|\mathbf{q}_r[n+1] - \mathbf{q}_r[n]\| \leq v^{max} \delta_t, n = 1, \dots, N-1 \quad (1b)$$

where the constraint C2 limits the displacement of the UR for consecutive timeslots, and  $v^{max}$  indicates the maximum flight velocity of the UR.

The AG channels are assumed to be dominated by path-loss with negligible fading [6]. Thus, for the Alice-UR link, the UR-Eve link, and the UR-Bob link, denoted as  $h_{ra}[n]$ ,  $h_{re}[n]$ , and  $h_{rb}[n] \forall n$ , respectively, we express their LoS-dominant channel power gains as

$$h_{rj}[n] = \frac{\beta_0}{\|\mathbf{q}_r[n] - \mathbf{q}_j\|^2}, \forall n, j \in \{a, e, b\} \quad (2)$$

where  $\beta_0$  denotes the path-loss at a reference distance under omnidirectional propagation. Furthermore, since both Alice and Eve are terrestrial nodes, the channel model for the Alice-Eve link constitutes both distance-dependent attenuation and small-scale Rayleigh fading [5], the power gain of which can be represented as

$$h_{ae}[n] = \frac{\beta_0}{\|\mathbf{q}_a - \mathbf{q}_e\|^\alpha} \zeta[n], \forall n \quad (3)$$

where  $\zeta[n]$  is a unit-mean exponential random variable, and  $\alpha$  is the corresponding environmental path-loss exponent, with a typical range between  $2 < \alpha \leq 4$ .

Delay tolerance in SPC is crucial as the communication system must deliver sensitive information quickly to be effective. Thus, for the considered short-packet delay-sensitive system, the requirement on delay tolerance can be imposed by constraining the number of total blocklengths per transmission to be less than the maximum allowable end-to-end delay, expressed as

$$\text{C3: } \sum_i l_i[n] \leq L^{max}, l_i[n] \in \mathbb{Z}^{0+}, i \in \{u, d\}, \forall n \quad (4)$$

where  $L^{max}$  denotes the maximum latency tolerance and  $\mathbb{Z}^{0+}$  represents the set of nonnegative integers.

### III. PROBLEM FORMULATION

Let  $\varepsilon$  and  $\eta$  denote the network node's decoding error probability and information leakage, respectively. For simplicity, we also assume that the additive white Gaussian noise (AWGN) power at any node is equal for all timeslots and denoted by  $\sigma^2$ . Consequently, we express the achievable average SR in bits per channel use for the short-packet uplink transmission in timeslot  $n$ , according to [8], as

$$\begin{aligned} \tilde{R}_u^{sec}[n] &= \mathbb{E}_{\zeta[n]} \left\{ \log_2 \left( \frac{1 + \gamma_r[n]}{1 + \gamma_{ae}[n]} \right) - \sqrt{\frac{V(\gamma_r[n])}{l_u[n]}} Q^{-1}(\varepsilon) \right. \\ &\quad \left. - \sqrt{\frac{V(\gamma_{ae}[n])}{l_u[n]}} Q^{-1}(\eta) \right\}, \forall n \end{aligned} \quad (5)$$

$$\begin{aligned} &\stackrel{(a)}{\approx} \log_2 \left( \frac{1 + \gamma_r[n]}{1 + \bar{\gamma}_{ae}[n]} \right) - \sqrt{\frac{V(\gamma_r[n])}{l_u[n]}} Q^{-1}(\varepsilon) \\ &\quad - \sqrt{\frac{V(\bar{\gamma}_{ae}[n])}{l_u[n]}} Q^{-1}(\eta) \triangleq R_u^{sec}[n], \forall n \end{aligned} \quad (6)$$

where  $\mathbb{E}_x\{\cdot\}$  indicates expectation over the random variable  $x$ , and  $Q^{-1}(x)$  is the inverse of the complementary Gaussian cumulative distribution function  $Q(x)$ , defined as  $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{r^2}{2}} dr$ . Moreover,  $\gamma_r[n]$  and  $\gamma_{ae}[n]$ , denoting the received signal-to-noise ratios (SNRs) at the UR and Eve in timeslot  $n$ , are given respectively by

$$\gamma_r[n] = \frac{\rho_a}{\|\mathbf{q}_r[n] - \mathbf{q}_a\|^2}, \forall n \quad (7)$$

$$\gamma_{ae}[n] = \frac{\rho_a}{\|\mathbf{q}_a - \mathbf{q}_e\|^\alpha} \zeta[n], \forall n \quad (8)$$

Note that the approximation (a) in (6) follows from Jensen's inequality, and  $\bar{\gamma}_{ae}[n] = \frac{\rho_a}{\|\mathbf{q}_a - \mathbf{q}_e\|^\alpha}$ , where  $\rho_a = \frac{\beta_0 \beta_0}{\sigma^2}$ . Furthermore, the function  $V(\cdot)$  indicates channel dispersion, which can be mathematically expressed, according to [8], as

$$V(\gamma) = \log_2^2(\mathbf{e}) \left[ 1 - (1 + \gamma)^{-2} \right], \forall n \quad (9)$$

Note that  $V(\gamma)$  is a monotonically increasing function of the SNR  $\gamma$ .

Likewise, the achievable SR for short-packet downlink transmission in timeslot  $n$  is given by

$$\begin{aligned} R_d^{sec}[n] &= \log_2 \left( \frac{1 + \gamma_b[n]}{1 + \gamma_{re}[n]} \right) - \sqrt{\frac{V(\gamma_b[n])}{l_d[n]}} Q^{-1}(\varepsilon) \\ &\quad - \sqrt{\frac{V(\gamma_{re}[n])}{l_d[n]}} Q^{-1}(\eta), \forall n \end{aligned} \quad (10)$$

where  $\gamma_b[n]$  and  $\gamma_{re}[n]$  denote the received SNRs at Bob and Eve in timeslot  $n$ , given respectively by

$$\gamma_b[n] = \frac{\rho_r}{\|\mathbf{q}_r[n] - \mathbf{q}_b\|^2}, \forall n \quad (11)$$

$$\gamma_{re}[n] = \frac{\rho_r}{\|\mathbf{q}_r[n] - \mathbf{q}_e\|^2}, \forall n \quad (12)$$

with  $\rho_r = \frac{\beta_r \beta_0}{\sigma^2}$ . Now, considering that Alice and the UR securely encode the transmit short-packet data in timeslot  $n$  to maintain the desired reliability and security requirements of the considered system  $(\varepsilon, \eta)$ , we define the secrecy throughput metric as the rate of the effective number of securely transmitted information bits in bits per second (bps) as

$$\bar{B}_s[n] = \frac{1 - \varepsilon}{\delta_t} \left[ \min(R_u^{sec}[n] l_u[n], R_d^{sec}[n] l_d[n]) \right]_+, \forall n \quad (13)$$

where  $[x]_+ = \max(x, 0)$ .

Our objective is to optimize the secrecy performance of the proposed UAV-SPC relaying system by designing the transmission blocklengths  $\mathbf{L} = \{l_u[n], l_d[n], \forall n\}$ , and the UR trajectory  $\mathbf{Q} = \{\mathbf{q}[n], \forall n\}$ . The resulting optimization maximizes the Effective Average Secrecy Throughput (EAST) over the mission duration, which is formulated as

$$\begin{aligned} (\mathbf{P}) : \max_{\{\mathbf{L}, \mathbf{Q}\}} \text{EAST} &= \frac{1}{N} \sum_{n=1}^N \bar{B}_s[n] \\ \text{s.t.} \quad &\text{C1} - \text{C3}. \end{aligned} \quad (14)$$

Note that (P) is a nonconvex optimization problem due to the nonconvex objective function with nonsmooth operator

$[\cdot]_+$ , and highly coupled optimization variables. Thus, it is too challenging to be solved optimally. First, we note that the nonsmoothness of the objective function in **(P)** can be handled since at the optimal point,  $\bar{B}_s[n]$  should hold a nonnegative value. Otherwise, by setting  $l_u[n] = 0$  and/or  $l_d[n] = 0$  (i.e., no transmission) in the given timeslot, one obtains  $\bar{B}_s[n] = 0$ , which violates the optimality. In light of this, we remove the nonsmoothness operator from the objective function without impacting the optimal solution. Here, introducing a slack variable vector  $\boldsymbol{\tau} = \{\tau[n], \forall n\}$ , we convert **(P)** to a more tractable version, whose objective function is differentiable and serves as a lower bound on that of the original problem:

$$\begin{aligned} \text{(P1)} : \max_{\{\mathbf{L}, \mathbf{Q}, \boldsymbol{\tau}\}} & \frac{1-\varepsilon}{T} \sum_{n=1}^N \tau[n] \\ \text{s.t.} & \mathbf{C1} - \mathbf{C3}, \end{aligned} \quad (15a)$$

$$R_u^{sec}[n]l_u[n] \geq \tau[n], \quad \forall n \quad (15b)$$

$$R_d^{sec}[n]l_d[n] \geq \tau[n], \quad \forall n \quad (15c)$$

In the following, we propose a low-complexity iterative solution to solve **(P1)** based on the BSCA algorithm, wherein we optimize each block of variables while keeping others unchanged in an alternating manner. Such an algorithm generally approaches a locally optimal solution but with guaranteed convergence.

#### IV. PROPOSED SOLUTION

In this section, we divide **(P1)** into two subproblems: i) short-packet blocklength optimization, and ii) UR trajectory optimization. Thereafter, we propose an efficient overall iterative algorithm. Note that in the sequel, we omit the fixed multiplicative term  $\frac{1-\varepsilon}{T}$  from the objective function, which has no impact on the proposed solution.

##### A. Short-packet Blocklength Optimization

In this subsection, we optimize the blocklength vectors of both the uplink and downlink SPC, i.e.,  $\mathbf{L} = \{l_u[n], l_d[n], \forall n\}$ , while keeping other variables fixed. As such, the corresponding subproblem can be written as

$$\begin{aligned} \text{(P2)} : \max_{\mathbf{L}, \boldsymbol{\tau}} & \sum_{n=1}^N \tau[n] \\ \text{s.t.} & \mathbf{C3}, \text{ (15b)}, \text{ (15c)}. \end{aligned} \quad (16)$$

Note that **(P2)** is a nonlinear integer programming, which is in general a challenging NP-hard problem. Nevertheless, analyzing the objective function of **(P2)**, we see that it is non-decreasing with respect to  $\mathbf{L}$ , implying that the constraint **C3** should be satisfied with equality at the optimal point, i.e.,  $l_u[n] + l_d[n] = L^{max} \forall n$ ; otherwise, increasing the blocklength leads to an increase in the objective function, which violates the optimality. Hence, we can solve **(P2)** via a simple 1D

search over the discrete set  $\mathcal{L} = \{0, 1, 2, \dots, L^{max}\}$  to obtain the optimal blocklengths for the uplink transmissions:

$$l_u^{opt}[n] = \arg \max_{x \in \mathcal{L}} \bar{B}_s[n] \Big|_{l_u[n]=x, l_d[n]=L^{max}-x}, \quad \forall n \quad (17)$$

Then, the optimal blocklengths for the downlink transmissions can be determined by

$$l_d^{opt}[n] = L^{max} - l_u^{opt}[n] \quad \forall n.$$

##### B. UR Trajectory Optimization

This subsection explores the joint optimization of the UR's motion and altitude. In light of this, we recast **(P1)** to optimize **Q**, while keeping the other variables fixed, which gives

$$\begin{aligned} \text{(P3)} : \max_{\{\mathbf{q}_r, \boldsymbol{\tau}\}} & \sum_{n=1}^N \tau[n] \\ \text{s.t.} & \mathbf{C1} - \mathbf{C2}, \end{aligned} \quad (18a)$$

$$\begin{aligned} \log_2(1 + \gamma_r[n]) - b_0 \sqrt{1 - (1 + \gamma_r[n])^{-2}} \\ \geq b_2 \tau[n] + b_1, \quad \forall n \end{aligned} \quad (18b)$$

$$\begin{aligned} \log_2\left(\frac{1 + \gamma_b[n]}{1 + \gamma_{re}[n]}\right) - c_0 \sqrt{1 - (1 + \gamma_b[n])^{-2}} \\ - c_1 \sqrt{1 - (1 + \gamma_{re}[n])^{-2}} \geq c_2 \tau[n], \quad \forall n \end{aligned} \quad (18c)$$

where

$$b_0 = \frac{Q^{-1}(\varepsilon) \log_2 e}{\sqrt{l_u[n]}}, \quad b_2 = \frac{1}{l_u[n](1-\varepsilon)},$$

$$b_1 = \log_2(1 + \gamma_{ae}[n]) - \sqrt{\frac{V(\gamma_{ae}[n])}{l_u[n]}} Q^{-1}(\eta),$$

$$c_0 = \frac{Q^{-1}(\varepsilon) \log_2 e}{\sqrt{l_d[n]}}, \quad c_1 = \frac{Q^{-1}(\eta) \log_2 e}{\sqrt{l_d[n]}}, \quad c_2 = \frac{1}{l_d[n](1-\varepsilon)}.$$

We stress that **(P3)** is still a nonconvex optimization problem due to nonconvex constraints **(18b)** and **(18c)**. In the following, we focus on transforming these constraints into convex approximates to make the problem tractable.

1) *Convex reformulation of (18b)*: We equivalently write **(18b)** in a more tractable way by introducing nonnegative slack variables  $\boldsymbol{\lambda} = \{\lambda_1[n], \lambda_2[n], \forall n\}$  and  $\boldsymbol{\beta} = \{\beta_1[n], \forall n\}$ , as

$$\log_2(1 + \lambda_1[n]) - b_0 \beta_1[n] \geq b_2 \tau[n] + b_1, \quad \forall n \quad (19a)$$

$$\rho_a \lambda_2[n] \geq \|\mathbf{q}_r[n] - \mathbf{q}_a\|^2, \quad \forall n \quad (19b)$$

$$\lambda_1[n] \lambda_2[n] \leq 1, \quad \forall n \quad (19c)$$

$$\beta_1^2[n] \geq 1 - (1 + \lambda_1[n])^{-2}, \quad \forall n \quad (19d)$$

We note that the constraints **(19a)** and **(19b)** are convex, while the additional constraints **(19c)** and **(19d)**, introduced to ensure the smoothness of **(P3)**, are nonconvex. We stress that **(19b)**-**(19d)** should hold with equality at the optimal point. Before proceeding further, we present a lemma below.

**Lemma 1.** Let  $f(x, y) = \frac{1}{xy}$  with  $x, y > 0$ . At any given point  $(x_0, y_0)$  in the domain of  $f$ , the following function serves as a global lower bound on  $f(x, y)$  [15], i.e.,

$$f_{lb}(x, y; x_0, y_0) = -\frac{x y_0 + x_0 y - 3 x_0 y_0}{x_0^2 y_0^2} \leq f(x, y). \quad (20)$$

Thus, at a given point  $(\mathbf{q}_r^{lo}, \boldsymbol{\lambda}^{lo}, \boldsymbol{\beta}^{lo})$ , the convex approximations of the constraints (19c) and (19d) are

$$1 \leq f_{lb}(\lambda_1[n], \lambda_2[n]; \lambda_1^{lo}[n], \lambda_2^{lo}[n]), \quad \forall n \quad (21a)$$

$$\ln(\beta_1[n]) + \ln(1 + \lambda_1[n]) \geq g(\lambda_1[n]; \lambda_1^{lo}[n]), \quad \forall n \quad (21b)$$

where the convex function  $g(x; x_0)$  is defined as

$$g(x; x_0) = A_0(x_0) + A_1(x_0)(x - x_0),$$

with  $A_0(x)$  and  $A_1(x)$  being defined for  $x > 0$  as

$$A_0(x) = \frac{1}{2} \ln(x[2 + x])$$

and

$$A_1(x) = \frac{x + 1}{x(x + 2)},$$

respectively. Here, (21a) follows from Lemma 1 and (21b) follows from the concavity of the logarithm function.

2) *Convex reformulation of (18c):* Introducing the non-negative slack variables  $\boldsymbol{\omega} = \{\omega_1[n], \omega_2[n], \forall n\}$ ,  $\boldsymbol{\psi} = \{\psi_1[n], \forall n\}$ ,  $\mathbf{u} = \{u_1[n], \forall n\}$ , and  $\mathbf{v} = \{v_1[n], v_2[n], \forall n\}$ , we reformulate (18c) into approximate convex constraints, using Lemma 1 and [14, Lemma 3], as

$$\log_2(1 + \omega_1[n]) - \log_2(1 + u_1^{-1}[n]) \geq c_0 \psi_1[n] + c_1 v_1[n] + c_2 \tau[n], \quad \forall n \quad (22a)$$

$$1 \leq f_{lb}(\omega_1[n], \omega_2[n]; \omega_1^{lo}[n], \omega_2^{lo}[n]), \quad \forall n \quad (22b)$$

$$\rho_r \omega_2[n] \geq \|\mathbf{q}_r[n] - \mathbf{q}_b\|^2, \quad \forall n \quad (22c)$$

$$\ln(\psi_1[n]) + \ln(1 + \omega_1[n]) \geq g(\omega_1[n]; \omega_1^{lo}[n]), \quad \forall n \quad (22d)$$

$$\rho_r u_1[n] \leq 2(\mathbf{q}_r^{lo}[n] - \mathbf{q}_e)^T \mathbf{q}_r[n] + d_0^{lo}[n], \quad \forall n \quad (22e)$$

$$\ln(v_1[n]) + \ln(1 + v_2[n]) \geq g(v_2[n]; v_2^{lo}[n]), \quad \forall n \quad (22f)$$

$$u_1[n] \geq v_2^{-1}[n], \quad \forall n \quad (22g)$$

where  $d_0^{lo}[n] = \|\mathbf{q}_e\|^2 - \|\mathbf{q}_r^{lo}[n]\|^2$  and  $(\mathbf{q}_r^{lo}, \boldsymbol{\omega}^{lo}, \boldsymbol{\psi}^{lo}, \mathbf{v}^{lo}, \mathbf{u}^{lo})$  is the given local point. We now express the convex reformulation of subproblem (P3) as

$$\begin{aligned} (\text{P3.1}) : \quad & \max_{\{\mathbf{q}_r, \boldsymbol{\tau}, \boldsymbol{\lambda}, \boldsymbol{\beta}, \boldsymbol{\omega}, \boldsymbol{\psi}, \mathbf{u}, \mathbf{v}\}} \sum_{n=1}^N \tau[n] \\ & \text{s.t. C1 - C2, (19a), (19b), (21), (22)}. \end{aligned} \quad (23)$$

Since (P3.1) is convex, it can be efficiently solved by standard convex optimization tools such as CVX [16].

### C. Overall Iterative Algorithm

In this subsection, we propose an overall iterative algorithm based on the sequential block optimization summarized in Algorithm 1.

---

#### Algorithm 1: Overall EAST optimization algorithm.

---

- 1: **Initialize:** Iteration index  $i = 0$ , choose a feasible local point  $(\mathbf{L}^{(i)}, \mathbf{Q}^{(i)})$ ;
  - 2: **Repeat:**
    - 2.1: Calculate EAST<sup>(i)</sup>, update  $i \leftarrow i + 1$ ;
    - 2.2: Solve (P2) via (17), then update  $\mathbf{L}^{(i)} = \{l_u^{(i)}[n], l_d^{(i)}[n], \forall n\}$ ;
    - 2.3: Given  $\mathbf{L}^{(i)}$ , initialize slack variables  $(\boldsymbol{\lambda}^{lo}, \boldsymbol{\beta}^{lo}, \boldsymbol{\omega}^{lo}, \boldsymbol{\psi}^{lo}, \mathbf{u}^{lo}, \mathbf{v}^{lo})$ , and solve (P3.1), then update  $\mathbf{Q}^{(i)} = \{\mathbf{q}_r^{(i)}[n] = [x_r^{(i)}[n], y_r^{(i)}[n], H]^T, \forall n\}$ ;
    - 2.4: Calculate EAST<sup>(i)</sup> at the new point  $(\mathbf{L}^{(i)}, \mathbf{Q}^{(i)})$ ;
  - 3: **Until:**  $\|\text{EAST}^{(i)} - \text{EAST}^{(i-1)}\| \leq \epsilon$ ;
- 

It can be proved that the proposed algorithm is guaranteed to converge to a local optimum commencing from a feasible point. Moreover, the time complexity of Algorithm 1, based on the complexity of each convex subproblem and the convergence accuracy parameter  $\epsilon$ , can be approximately obtained as  $\mathcal{O}(N^{3.5} \log_2(\frac{1}{\epsilon}))$ , where  $\mathcal{O}(\cdot)$  represents big-O notation. The overall complexity order of Algorithm 1 is polynomial, and thus our proposed approach can be reasonably implemented for energy-limited UAV-IoT scenarios with SPC.

## V. NUMERICAL RESULTS AND DISCUSSION

In this section, we demonstrate the EAST enhancement achieved by our proposed optimization algorithm for the considered UAV-aided SPC-IoT scenario. To exhibit the effectiveness of our joint trajectory and blocklength design in Algorithm 1, labeled **JTBD**, we compare it with the following benchmark schemes:

- **Trajectory Design with Fixed Blocklength (TDFB):** With fixed coding blocklengths, only the UR trajectory is optimized using (P3.1) in a sequential manner.
- **Blocklength Design with Fixed Trajectory (BDFT):** Keeping the UR trajectory fixed, only the optimization of blocklengths is taken via solving (P2) using (17).

Table I lists the system parameters used in this section, unless otherwise stated. These parameters are mainly adopted in the literature such as in [2] and [14]. In addition, the initial feasible trajectory of the UR,  $\mathbf{Q}^{(0)}$ , is taken to be on a direct line with fixed speed from the initial location to the final location. The uplink and downlink transmission blocklengths per timeslot are initialized as  $l_u^{(0)}[n] = l_d^{(0)}[n] = \frac{L^{max}}{2} \forall n$ .

Fig. 2 depicts the EAST performance against the iteration index for all schemes to verify the quick convergence of Algorithm 1 and the validity of our analysis, as well as to demonstrate the performance advantage of our joint design. We observe from the figure that the EAST is non-decreasing

TABLE I: System parameters

Simulation parameter (notation)	Value
Transmit power ( $p_a$ )	20 dBm
Relaying power ( $p_r$ )	20 dBm
Reference channel power gain ( $\beta_0$ )	-70 dB
Terrestrial path-loss exponent ( $\alpha$ )	3
Channel noise power ( $\sigma^2$ )	-140 dBm
Transmission period ( $\delta_t$ )	1 s
Maximum latency tolerance ( $L^{max}$ )	400
Mission time ( $T$ )	100 s
UAV's altitude ( $H$ )	60 m
Maximum flying speed ( $v^{max}$ )	30 m/s
UAV's initial location ( $\mathbf{q}_i$ )	$[-500, -1000, 60]^T$ m
UAV's final location ( $\mathbf{q}_f$ )	$[1000, 500, 60]^T$ m
Alice's location ( $\mathbf{q}_a$ )	$[-700, 0, 0]^T$ m
Bob's location ( $\mathbf{q}_b$ )	$[700, 0, 0]^T$ m
Eve's location ( $\mathbf{q}_e$ )	$[-500, 900, 0]^T$ m
Decoding error probability ( $\varepsilon$ )	$10^{-3}$
Information leakage parameter ( $\eta$ )	$10^{-2}$
Convergence threshold ( $\epsilon$ )	$10^{-3}$

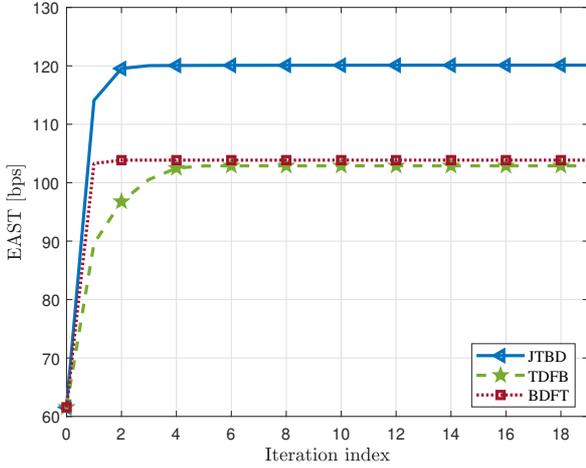
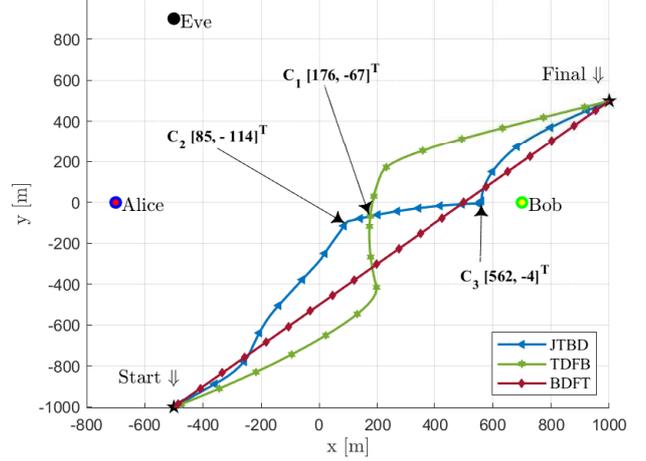


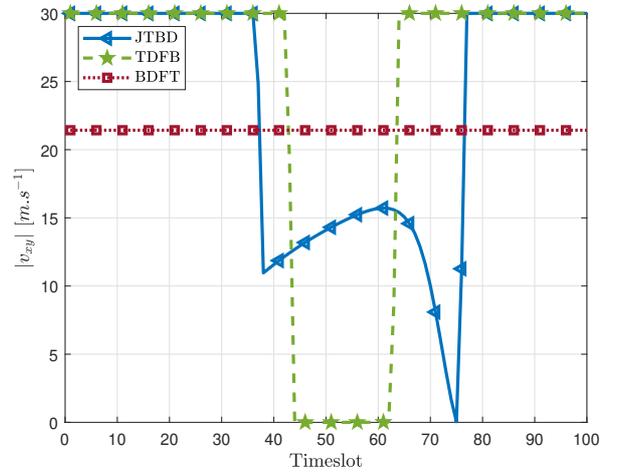
Fig. 2: EAST vs. iteration index.

over the iteration index for all algorithms, and that convergence occurs quickly in just a few iterations. Our proposed **JTBD** approach achieves the best EAST performance amongst all. For example, **JTBD** can reach up to 120 bps, approximately 14% more than both the **BDFT** and **TDFB** designs, and nearly twice the EAST of the initial feasible setting. Also, Fig. 2 shows that using the baseline trajectory and optimizing transmission blocklengths is more important for SPC than optimizing the trajectory with fixed blocklengths, while the joint design of both is clearly preferable concerning the EAST performance metric.

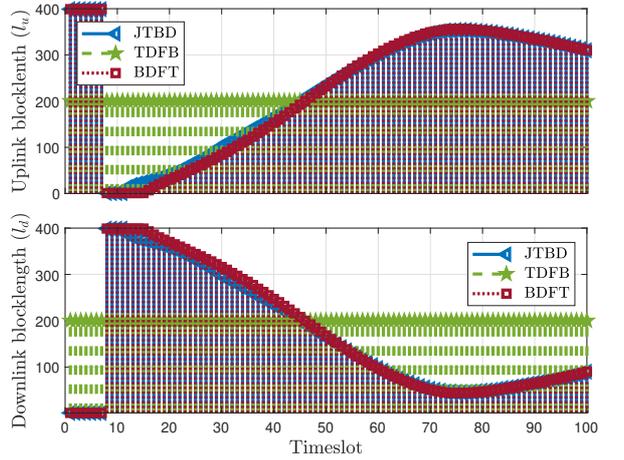
Fig. 3 illustrates the trajectory and velocity profiles of the UR, as well as both the uplink and downlink short-packet blocklengths for the specific realization of the user locations based on different design scenarios. We observe from Figs. 3(a) and 3(b) that in contrast to the other schemes, for



(a) UR's trajectory profile.



(b) UR's velocity vs. timeslot.



(c) Blocklengths vs. timeslot.

Fig. 3: Designed UR's trajectory and velocity profiles, and coding blocklengths according to different schemes.

**TDFB** the UR attempts to fly with the maximum velocity while heading towards a position between Alice and Bob located at the coordinate  $\mathbf{C}_1 = [176, -67, 60]^T$  m, and hovering at that point as long as possible, i.e., between  $T = 44$  s and  $T = 62$  s. This solution greatly improves the EAST compared with the initial direct-path trajectory with fixed velocity, but not as much as **BDFT** and our proposed **JTBD**. We also observe from Fig. 3(c) that when the UR is farther from Bob, larger downlink coding blocklengths are adopted, and they reduce in length as the UR approaches Bob. As the UR flies away from Alice, the proposed algorithm efficiently increases the uplink blocklength, which ultimately enhances the EAST. Interestingly, the blocklength designs of both **JTBD** and **BDFT** follow a very similar trend, even though their corresponding trajectories are different. Nevertheless, when both the trajectory design and blocklength optimization are taken into account as in the proposed **JTBD** design, the UR demonstrates effective navigation and ability to considerably enhance the EAST compared to other benchmarks. Specifically, the effective trajectory for the **JTBD** scheme requires the UR to fly with full speed from the initial location  $\mathbf{q}_i$  to the position marked as  $\mathbf{C}_2 = [85, -114, 60]^T$  m, according to the path illustrated in Fig. 3(a). Then, a sharp velocity drop occurs at  $T = 36$  s, enabling the UR to move with relatively low speed from the position  $\mathbf{C}_2$  to a location with the coordinate  $\mathbf{C}_3 = [562, -4, 60]^T$  m, for improving the overall EAST performance. Finally, the UR travels through an arc path tilted away from Bob while maximally increasing its velocity at timeslot  $T = 75$  s and maintaining this velocity so that the last part of the mission from  $\mathbf{C}_3$  to the final location  $\mathbf{q}_f$  could be accomplished by the end of the specified duration. Overall, this observation reinforces the significance of communication blocklength and trajectory co-design for the secrecy performance improvement of aerial relaying with SPC.

## VI. CONCLUSION

This work presented the design of a secure and reliable UAV-IoT relaying system with SPC. To optimize the EAST performance of the system, an effective joint design approach that incorporates the UAV trajectory and both uplink and downlink blocklengths was proposed, and was shown to achieve quick convergence with low complexity. The efficacy of the proposed approach was evaluated through numerical simulations, and the results demonstrated the superiority of our **JTBD** scheme in terms of EAST compared to benchmarks that only consider either trajectory design or blocklength optimization. Our results further indicated that both the uplink and downlink blocklengths should be adaptively adjusted according to the UAV location along the trajectory.

- [1] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sept. 2016.
- [2] C. Feng and H. M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 96–102, Sept. 2021.
- [3] M. Shirvanimoghaddam *et al.*, "Short block-length codes for ultra-reliable low latency communications," *IEEE Commun. Mag.*, vol. 57, pp. 130–137, Feb. 2019.
- [4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, pp. 20–27, Apr. 2015.
- [5] M. Tatar Mamaghani, A. Kuhestani, and K.-K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, vol. 67, pp. 8451–8465, Sept. 2018.
- [6] M. Tatar Mamaghani and Y. Hong, "Improving PHY-security of UAV-enabled transmission with wireless energy harvesting: Robust trajectory design and communications resource allocation," *IEEE Trans. Veh. Technol.*, vol. 69, pp. 8586–8600, Aug. 2020.
- [7] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Natl. Acad. Sci. U.S.A.*, vol. 114, no. 1, pp. 19–26, Jan. 2017.
- [8] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonsymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, pp. 4069–4093, July 2019.
- [9] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Physical-layer security in the finite blocklength regime over fading channels," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 5, pp. 3405–3420, May 2020.
- [10] C. Feng, H. M. Wang, and H. V. Poor, "Reliable and secure short-packet communications," *IEEE Trans. Wirel. Commun.*, vol. 21, pp. 1913–1926, Mar. 2022.
- [11] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wirel. Commun.*, vol. 18, pp. 2565–2578, May 2019.
- [12] Q. Wu *et al.*, "A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence," *IEEE J. Sel. Areas Commun.*, vol. 39, pp. 2912–2945, Oct. 2021.
- [13] H. M. Wang, X. Zhang, and J. C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 32–39, Oct. 2019.
- [14] M. Tatar Mamaghani and Y. Hong, "Joint trajectory and power allocation design for secure artificial noise aided UAV communications," *IEEE Trans. Veh. Technol.*, vol. 70, pp. 2850–2855, Mar. 2021.
- [15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [16] M. Grant and S. Boyd, "CVX: Matlab Software for Disciplined Convex Programming, Version 2.2," Jan. 2020. [Online]. Available: <http://cvxr.com/cvx>