Multi-Objective Optimization for Secure UAV-Assisted Data Collection via Intermittent Jamming

Xiujuan Zhang[1], Yujiao Han[1], Shiyu Wang[2,3], Xin Fan[2,3], Jin Qian[4], Chuanwen Luo[2,3]
{xiujuanzhang@qfnu.edu.cn, Han20010503@qfnu.edu.cn, WSY2619@bjfu.edu.cn,
fanxin@bjfu.edu.cn, qianjin@tzu.edu.cn, chuanwenluo@bjfu.edu.cn}

[1]School of Computer Science, Qufu Normal University, Rizhao 276826, China
[2]School of Information Science and Technology, Beijing Forestry University, Beijing 100083, China
[3]Hebei Key Laboratory of Smart National Park, Beijing 100083, China
[4]College of Information Engineering, Taizhou University, Taizhou 225300, China

Abstract. Unmanned Aerial Vehicles (UAVs) have emerged as pivotal tools for Internet of Things (IoT) data collection by leveraging their superior mobility. However, the open nature of wireless channels renders UAV communications susceptible to malicious eavesdropping. Furthermore, the limited onboard energy of UAVs and the stringent requirements for Age of Information (AoI) freshness pose significant challenges to data collection operations. To address these issues, this paper proposes a dual-UAV cooperative secure data collection scheme based on an intermittent jamming strategy. We formulate a multi-objective optimization problem aimed at minimizing AoI and energy consumption while maximizing the eavesdropper's Bit Error Rate (BER) by jointly optimizing UAV trajectories, time scheduling, and jamming parameters. Given the non-convexity of the problem and the complex coupling between variables, we develop an efficient iterative algorithm based on Block Coordinate Descent (BCD) and Successive Convex Approximation (SCA). Simulation results demonstrate that the proposed scheme achieves an optimal trade-off among the metrics.

Keywords: UAV, Data Collection, Age of Information, Energy Consumption, Physical Layer Security, Intermittent Jamming

1 Introduction

In large-scale Internet of Things (IoT) networks, Unmanned Aerial Vehicles (UAVs) serve as mobile aggregators. By leveraging their high mobility and Line-of-Sight (LoS) transmission advantages, UAVs break through the coverage limitations of fixed base stations in complex terrains, significantly enhancing the flexibility and reliability of data collection [1]. With the evolution of wireless networks, ensuring low latency has become a critical objective for time-sensitive applications [2]. Consequently, Age of Information (Aol) has emerged as a crucial metric for timeliness.

IIKI 2025, December 18-21, Chengdu, People's Republic of China

DOI 10.4108/eai.18-12-2025.2365276

Meanwhile, Age of Information (AoI) has emerged as a crucial metric for timeliness. From the receiver's perspective, AoI characterizes the time elapsed since the generation of the latest successfully received status update. It directly reflects the freshness of status information and has replaced traditional throughput metrics as a core optimization objective for UAV trajectory planning and resource scheduling[3], [4].

However, due to size limitations, the onboard energy of UAVs is severely restricted, leading to increasing research on energy conservation[5]. Xiao *et al.* addressed the system energy efficiency maximization problem in UAV-assisted data collection by jointly optimizing UAV trajectory and communication resources, effectively reducing total energy consumption [6]. Li *et al.* utilized Orthogonal Frequency Division Multiple Access (OFDMA) technology to solve the data collection maximization problem under energy constraints by jointly optimizing the UAV's hovering locations and sojourn duration [7]. Bai *et al.* satisfied the data collection volume requirements while reducing energy consumption by jointly optimizing discrete functional module switches and continuous flight and transmission parameters [8]. Similarly, in the broader context of energy-constrained IoT, Huo *et al.* proposed a secure relay selection strategy to optimize security performance under energy harvesting constraints [9]. In [10], Zhao *et al.* considered the importance of both AoI and energy consumption, proposing a multi-objective optimization problem to minimize both metrics. Moreover, in energy-constrained networks, Xu *et al.* investigated secure transmission solutions, emphasizing the critical trade-off between energy availability and security performance [11].

Furthermore, in UAV-assisted IoT networks, the broadcast nature of UAVs and the openness of wireless channels induce severe eavesdropping risks. Indeed, physical layer security has garnered significant attention across various network architectures, such as NOMA-enabled cognitive radio networks, to mitigate such inherent vulnerabilities [12]. To address such security issues, Huo *et al.* investigated cooperative jamming schemes and jointly optimized power allocation to improve the secrecy rate [13]. Addressing collusive eavesdroppers, Fan *et al* enhanced security by designing a SINR-maximizing cooperative jamming scheme and deriving closed-form SOP expressions under worst-case signal aggregation [14]. From a theoretical perspective, Fan and Huo further analyzed the reliability of jamming-assisted transmission by deriving the analytical expressions for Secrecy Outage Probability (SOP) [15]. Regarding the implementation of jamming, Huang *et al.* explored the utilization of artificial noise to secure wireless connections without requiring perfect channel state information [16]. Complementing this, Fan et al. proposed a space power synthesis-based cooperative jamming scheme, which effectively synthesizes jamming signals to suppress eavesdropping even when channel state information is unknown [17]. Subsequently, Xiong *et al.* investigated secure data collection for UAVs. By constructing a novel 3D flight energy consumption model and jointly optimizing the flight trajectory and communication schedule, the authors successfully achieved data collection while satisfying security constraints [18]. Similarly, in [19], Zhang *et al.* considered not only security but also practical propulsion energy consumption to maximize the Secrecy Energy Efficiency (SEE) of UAV data collection.

1.1 Motivation and Contributions

Although existing research has made significant strides in addressing energy efficiency, AoI and physical layer security individually or in pairs, a unified framework that jointly optimizes these

three conflicting metrics remains underexplored. In practical UAV-assisted IoT networks, minimizing AoI necessitates frequent status updates and extended flight times, which inevitably conflicts with the goal of energy conservation. Meanwhile, ensuring high-level security typically demands substantial jamming power, further exacerbating the energy scarcity issue. Consequently, balancing these interconnected and competing objectives poses a significant challenge.

Furthermore, contrary to the energy-intensive continuous jamming strategies prevalent in prior literature—which indiscriminately transmit artificial noise regardless of channel conditions—we propose a flexible intermittent jamming strategy. By dynamically activating jamming only during critical time slots, this approach effectively reduces the burden on limited onboard batteries without compromising security.

Motivated by these theoretical and practical gaps, we present a novel cooperative secure data collection scheme. The main contributions of this paper are summarized as follows:

- We propose a multi-objective optimization framework for dual-UAV cooperative secure data collection. In this framework, one UAV (Bob) collects data while ensuring the AOI, and the other UAV (Jack) is responsible for jamming eavesdroppers. By jointly optimizing the UAV trajectories, time scheduling, and jamming parameters, we achieve an optimal trade-off among the eavesdropper's Bit Error Rate (BER), AoI, and energy consumption.
- To prolong the UAV's operational time and enhance system security, we propose an intermittent jamming strategy. This strategy effectively mitigates the excessive energy consumption caused by continuous jamming, thereby ensuring the security of data collection in a more energy-efficient manner.
- We decompose the non-convex problem into five subproblems and solve them via an iterative Successive Convex Approximation (SCA) and Block Coordinate Descent (BCD) based algorithm. Simulations verify its rapid convergence and the achieved optimal trade-off among the objectives.

2 System Model and Problem Formulation

2.1 System Model

As shown in Fig. 1 , we define a UAV-assisted IoT system consisting of two UAVs, M sensor nodes (INs), and a ground eavesdropper (Eve) with uncertain location information. The legitimate UAV (Bob) departs from the depot $\mathbf{q}_F$, collects all confidential information from M INs, and returns to the depot. To ensure security, another friendly UAV (Jack) departs from the base $\mathbf{q}_{J,F}$ simultaneously to intermittently transmit artificial noise to jam Eve, and then returns to the base.

We assume all devices are equipped with a single antenna. The set of INs is denoted by $\mathscr{M} = \{1,2,\ldots,M\}$. In our study, we adopt a quasi-static channel model and divide the total mission time into N time slots $\mathscr{N} = \{1,2,\ldots,N\}$, where the length of each slot is $T[n]$. To achieve lower AoI and allocate more precise collection time for each device, we assume that time slots are of unequal length, and the length of each slot cannot exceed a maximum value $T_{\max}$.

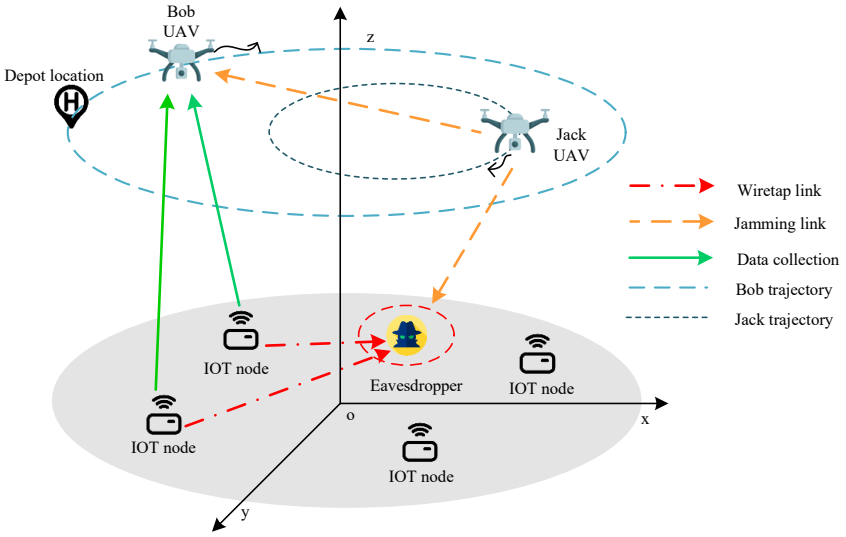

Fig. 1. System model of UAV-assisted IoT Secure data collection

We use a Cartesian coordinate system to describe the physical locations of all devices. The horizontal coordinates of the INs are denoted by $\mathbf{w}_m = [x_m, y_m]^T$. The eavesdropper's location is estimated to be within a circle, where $\mathbf{w}_E \in \mathbb{R}^{2\times 1}$ represents the center of the circle and r_E represents the radius. Thus, Eve's location satisfies $\|\mathbf{w}_E - \bar{\mathbf{w}}_E\| \leq r_E$. In experiments, it is generally assumed that r_E is usually smaller than the distance between Eve and the nodes, $\|\mathbf{w}_m - \mathbf{w}_E\| \geq r_E$. During the mission, both UAVs fly at a constant altitude H. Let $\mathbf{q}_B[n] = [x_B[n], y_B[n]]^T$ and $\mathbf{q}_J[n] = [x_J[n], y_J[n]]^T$ denote the horizontal coordinates of Bob and Jack in slot n, respectively. Defining their maximum speeds as v_{Bm} and v_{Jm}, the velocity constraints in the n-th slot are:

$$\mathbf{v}_B[n] = \frac{\mathbf{q}_B[n+1] - \mathbf{q}_B[n]}{T[n]} \leq v_{Bm}, \quad \forall n = 1, \ldots, N-1. \tag{1}$$

$$\mathbf{v}_J[n] = \frac{\mathbf{q}_J[n+1] - \mathbf{q}_J[n]}{T[n]} \leq v_{Jm}, \quad \forall n = 1, \ldots, N-1. \tag{2}$$

2.2 Communication and Data Collection Model

For ease of study, we assume the channel power gain between any two nodes follows the free-space path loss model $h = \rho_0/d^2$. Thus, in the n-th slot, the channel gain from an IoT node to the collection UAV is:

$$h_{mB}[n] = \frac{\rho_0}{d_{mB}^2[n]} = \frac{\rho_0}{\|\mathbf{q}_B[n] - \mathbf{w}_m\|^2 + H^2}, \tag{3}$$

where ρ_0 is the reference channel gain, and d is the Euclidean distance. Similarly, the channel gain from the friendly jammer to the collection UAV is $h_{JB}[n] = \frac{\rho_0}{d_{JB}^2[n]} = \frac{\rho_0}{\|\mathbf{q}_J[n]-\mathbf{q}_B[n]\|^2}$.

To ensure system robustness against Eve's location uncertainty, we consider the worst-case scenario. Specifically, to ensure a lower bound on security performance, we assume Eve is located closest to the INs and farthest from the jamming UAV. Thus, the channel gain from the eavesdropper to the IoT node is $h_{mE}[n] = \frac{\rho_0}{(\|\mathbf{w}_m-\mathbf{w}_E\|-r_E)^2}$, and from the friendly jammer to Eve is $h_{JE}[n] = \frac{\rho_0}{(\|\mathbf{q}_J[n]-\mathbf{w}_E\|+r_E)^2+H^2}$. Let $i \in \{B,E\}$ denote Bob and Eve, respectively.

Considering the proposed intermittent jamming scheme, the Signal-to-Interference-plus-Noise Ratio (SINR) at receiver i is:

$$\gamma_{mi}^c = \frac{p_m[n]h_{mi}[n]}{I_i^c[n]+\sigma^2}, \quad c \in \{j,a\}, i \in \{B,E\}, \tag{4}$$

where c represents the phase state. specifically, $c = j$ represents the jamming phase, where $I_i^j[n] = (P_J[n]/\beta[n])h_{Ji}[n]$, $c = a$ represents the non-jamming (silent) phase, where $I_i^a[n] = 0$. $P_m[n]$ denotes the transmit power of INs, and $\beta[n] \in (0,1]$ is the jamming duration ratio, representing the proportion of time in the n-th slot used for jamming. Thus, $P_J[n]/\beta[n]$ represents Jack's actual jamming power during the active phase.

The average achievable data transmission rate $R_m[n]$ of the m-th IN in the n-th slot is determined by the weighted sum of channel capacities in the jamming and non-jamming phases:

$$\begin{aligned} R_m[n] = {} & \beta[n]B\log_2(1+\gamma_{mB}^j) \\ & + (1-\beta[n])B\log_2(1+\gamma_{mB}^a). \end{aligned} \tag{5}$$

Let t_{mn} be the time Bob spends collecting data from the m-th IN in the n-th slot. The UAV acquires a set of INs via TDMA, and Bob collects data from at most one IN within each $t_m[n]$. The time resource allocation must satisfy:

$$T[n] \geq \sum_{m=1}^{M} t_m[n], \quad \forall n,m. \tag{6}$$

Defining the data task requirement for each IN as D_m, the cumulative data collected by Bob from each IN by the end of the mission must meet the total task requirement:

$$\sum_{n=1}^{N} R_m[n]t_m[n] \geq D_m, \quad \forall m. \tag{7}$$

2.3 BER Model

We define the Bit Error Rate (BER) at receiver i under BPSK modulation as the time-weighted sum of BERs in both phases:

$$\begin{aligned} f_{ei}^{\mathrm{BPSK}}[n] = {} & \beta[n]Q(\sqrt{2\gamma_{mi}^j}) \\ & + (1-\beta[n])Q(\sqrt{2\gamma_{mi}^a}), \quad i \in \{B,E\}, \end{aligned} \tag{8}$$

where $Q(\cdot)$ is the Gaussian Q-function.

2.4 AoI Model

To quantify the timeliness of sensed data, we adopt AoI as the performance metric. Considering the characteristics of the data collection task, we assume all IoT nodes generate status update data at $t = 0$, and the UAV offloads data uniformly only after completing all collection tasks and returning to the depot. Therefore, for the receiver, the maximum AoI of the data is determined by the UAV's total mission duration, defined as $\Delta_{\max}$:

$$\Delta_{\max} = \sum_{n=1}^{N} T[n]. \tag{9}$$

2.5 Energy Consumption Model

This paper stipulates that propulsion energy consumption is much greater than communication energy consumption. The system's total energy consumption consists mainly of the flight propulsion energy of both UAVs and the jamming energy of the jammer. Let the relationship between UAV flight propulsion power and velocity v be $P_{\text{prop}}(v)$ (see [20] for the specific power model). Thus, the total energy consumption includes propulsion energy E_{hover} (term used in source formula) and jamming energy E_J. Considering battery limits, the total energy consumption must satisfy the maximum energy budget $E_{\max}$:

$$\begin{aligned} E_{\text{total}} = \sum_{n=1}^{N} T[n](P_{\text{prop}}(\|\mathbf{v}_B[n]\|) + P_{\text{prop}}(\|\mathbf{v}_J[n]\|)) \\ + \sum_{n=1}^{N} T[n]\beta[n]P_J[n] \leq E_{\max}. \end{aligned} \tag{10}$$

2.6 Problem Formulation

We define the multi-objective joint optimization problem (P1) as follows:

$$
\begin{aligned}
(\mathrm{P1}) \min_{\mathscr{X}} \quad & \omega_1 \cdot \Delta_{\max} + \omega_2 \cdot E_{\text{total}} - \omega_3 \cdot f_{eE}^{\text{BPSK}} && \text{(11a)}\\
\text{s.t.} \quad & T[n] \le T_{\max}, && \text{(11b)}\\
& T[n] \ge \sum_{m=1}^{M} t_m[n], \quad \forall n, && \text{(11c)}\\
& \sum_{n=1}^{N} R_m[n] t_m[n] \ge D_m, \quad \forall m, && \text{(11d)}\\
& 0 < \beta[n] \le 1, && \text{(11e)}\\
& f_{eB}^{\text{BPSK}}[n] \le \theta_B, && \text{(11f)}\\
& E_{\text{total}} \le E_{\max}, && \text{(11g)}\\
& 0 \le P_J[n] \le P_{\max}^{J}, && \text{(11h)}\\
& \mathbf{q}_B[1] = \mathbf{q}_F, \mathbf{q}_B[N] = \mathbf{q}_F, && \text{(11i)}\\
& \mathbf{q}_J[1] = \mathbf{q}_{J,F}, \mathbf{q}_J[N] = \mathbf{q}_{J,F}, && \text{(11j)}\\
& \mathbf{q}_i[n+1] - \mathbf{q}_i[n] = \mathbf{v}_i[n] T[n], i \in \{B, J\}, && \text{(11k)}\\
& \|\mathbf{v}_i[n]\| \le v_{\max}, \quad \forall n, i \in \{B, J\}, && \text{(11l)}\\
& \|\mathbf{q}_B[n] - \mathbf{q}_J[n]\| \ge D_{\min}, \quad \forall n, && \text{(11m)}
\end{aligned}
$$

where $\mathscr{X} = \{\mathscr{Q}_B, \mathscr{Q}_J, \mathscr{T}, \tau, \mathscr{P}_J, \beta\}$ are the key optimization variables. Specifically, Bob's trajectory $\mathscr{Q}_B = \{\mathbf{q}_B[n], \forall n\}$, Jack's trajectory $\mathscr{Q}_J = \{\mathbf{q}_J[n], \forall n\}$, time slot duration $\mathscr{T} = \{T[n], \forall n\}$, collection time $\tau = \{t_m[n], \forall m, \forall n\}$, jamming power $\mathscr{P}_J = \{P_J[n], \forall n\}$, and jamming duration ratio $\beta = \{\beta[n], \forall n\}$. We adopt the Weighted Sum Method to transform the multi-objective optimization problem into a single-objective one. The objective function comprises three conflicting performance metrics: minimizing $\Delta_{\max}$ to guarantee data freshness, minimizing E_{total} to prolong the UAV network lifetime, and maximizing the eavesdropper's BER f_{eE}^{BPSK} to suppress eavesdropping. $\omega_1, \omega_2, \omega_3$ denote the weighting factors used to balance priorities under different application scenarios. Constraint (11b) ensures that the time slot does not exceed the specified maximum value; (11c) guarantees the resource allocation of TDMA; (11d) ensures that the data collection requirement D_m of each IoT node must be satisfied; (11e) defines the feasible region of the jamming duration; (11f) ensures the BER of the legitimate link is below the threshold θ_B; (11g) restricts the system's total energy consumption within the maximum budget; (11h) specifies the jamming power; (11i)–(11m) constrain the UAVs' mobility (start/end points, maximum speed) and the safe collision avoidance distance, respectively.

3 Algorithm Design

Since the objective function involves non-convexity and complex coupling, P1 is difficult to solve directly. We propose an iterative algorithm based on Block Coordinate Descent (BCD) and Successive Convex Approximation (SCA) to decompose the original problem into five tractable subproblems.

3.1 Subproblems(P2-P4): Optimization of Jamming and Time Resources

In this subsection, we first optimize the jamming resources $\{\mathscr{P}_J, \beta\}$ with fixed trajectories and time resources. For the non-convex term $P_J[n]\beta[n]$, we apply the first-order Taylor expansion at the k-th iteration point $(\beta^{(k)}[n], P_J^{(k)}[n])$ to obtain its global upper bound $z^k(\beta^{(k)}[n], P_J^{(k)}[n])$. Simultaneously, using the derivative of the composite function, we linearize the eavesdropper's BER as $f_{E,n}(P_J[n], \beta[n])$. Similarly, the legitimate receiver's BER is linearized as $f_{B,n}(P_J[n], \beta[n])$. Finally, we obtain the convex subproblem (P2)

$$
\begin{aligned}
(\mathrm{P2}) \min_{\mathscr{P}_J, \beta} \quad & \omega_2 \sum_{n=1}^{N} (T[n]E_{\text{hover}} + z^k(\beta^{(k)}[n], P_J^{(k)}[n])) \\
& - \omega_3 \frac{1}{N} \sum_{n=1}^{N} f_{E,n}(P_J[n], \beta[n]) && \text{(12a)} \\
\text{s.t.} \quad & (11\text{e}), && \text{(12b)} \\
& f_{B,n}(P_J[n], \beta[n]) \leq \theta_B, && \text{(12c)} \\
& \sum_{n=1}^{N} (T[n]E_{\text{hover}} + z^k(\beta^{(k)}[n], P_J^{(k)}[n])) \leq E_{\max}. && \text{(12d)}
\end{aligned}
$$

After obtaining the jamming strategy, we note that with fixed collection time, trajectories, and jamming resources, the objective function and constraints regarding $\mathscr{T}$ in the original problem are linear forms. Thus, this constitutes a standard Linear Programming (LP) problem. We can efficiently solve subproblem (P3) using the CVX toolkit. Similarly, by fixing the time slot length, trajectories, and jamming resources, we can optimize the collection time τ by directly solving subproblem (P4).

3.2 Subproblem(P5): Data Collection UAV Trajectory Optimization

In this subsection, we fix time resources, jamming resources, and Jack's trajectory to optimize Bob's trajectory $\mathscr{Q}_B$. The difficulty lies in the non-convex rate constraints and collision avoidance constraints. For the rate constraints, we introduce slack variables $\mathscr{O} = \{o_m[n]\}, \mathscr{S} = \{s_m[n]\}, \mathscr{L} = \{l[n]\}, \mathscr{U} = \{u[n]\}$ to rewrite the constraints(11d)

$$
\sum_{n=1}^{N} o_m[n] t_{mn} \geq D_m, \quad \forall m, \tag{13}
$$

where $o_m[n]$ satisfies $o_m[n] \leq \beta[n]B\log_2(1+\frac{1}{s_m[n]l[n]})+(1-\beta[n])B\log_2(1+\frac{1}{s_m[n]})$. The relaxations for the auxiliary variables are given by $s_m[n] \geq \frac{[\|W_m-\mathbf{q}_B[n]\|^2+H^2]\sigma^2}{P_m[n]\rho_0}$ and $l[n] \geq \frac{(P_J[n]/\beta[n])\rho_0(u[n]^{-1})}{\sigma^2}+1$. Furthermore, the relaxation for the relative distance is expressed as $u[n] \leq \|\mathbf{q}_J[n]-\mathbf{q}_B[n]\|^2, \forall n$.

For the key non-convex term $B\log_2(1+\frac{1}{s_m[n]l[n]})$, we apply first-order Taylor expansion at point $(s_m^{(k)}[n], l^{(k)}[n])$ to obtain the convex lower bound $f_1(s_m[n], l[n], s_m^{(k)}[n], l^{(k)}[n])$

$$\begin{aligned} B\log_2(1+\frac{1}{s_m[n]l[n]}) \geq B\Bigg[& \log_2(1+\frac{1}{s_m^{(k)}[n]l^{(k)}[n]}) \\ & -\frac{s_m[n]-s_m^{(k)}[n]}{\ln 2(s_m^{(k)}[n]+(s_m^{(k)}[n])^2 l[n])} \\ & -\frac{l[n]-l^{(k)}[n]}{\ln 2(l^{(k)}[n]+(l^{(k)}[n])^2 s_m^{(k)}[n])}\Bigg] \\ & \triangleq f_1(s_m[n], l[n], s_m^{(k)}[n], l^{(k)}[n]). \end{aligned} \tag{14}$$

Similarly, using first-order Taylor expansion to convexify $B\log_2(1+\frac{1}{s_m[n]})$, we obtain the convex lower bound $f_2(s_m[n], s_m^{(k)}[n])$. For the collision constraint, we perform a first-order Taylor expansion at the local point $\mathbf{q}_B^{(k)}[n]$ to obtain the lower bound of the squared norm function as $f_3(\mathbf{q}_B[n], \mathbf{q}_B^{(k)}[n])$.To facilitate the subsequent optimization process, we denote the aggregate set of optimization variables as $\mathbf{x_1} = \{\mathscr{Q}_B, \mathbf{v}, \mathbf{O}, \mathscr{S}, \mathscr{L}, \mathscr{U}\}$. With these definitions in place, the final convex subproblem (P5) is given by:

$$(\text{P5}) \min_{\mathbf{x_1}} \quad \omega_2 E_{\text{total}}(\mathbf{v}_B[n]) \tag{15a}$$

$$\text{s.t.} \quad (11\text{d}), (11\text{i}), (11\text{k})-(11\text{l}), (11\text{g}), \tag{15b}$$

$$o_m[n] \leq \beta[n]f_1 + (1-\beta[n])f_2, \tag{15c}$$

$$s_m[n] \geq \frac{\left[||W_m - q_B[n]||^2 + H^2\right]\sigma^2}{P_m[\text{n}]\rho_0}, \tag{15d}$$

$$l[n] \geq \frac{(P_J[n]/\beta[n])\rho_0(\text{u}[n]^{-1})}{\sigma^2}+1, \tag{15e}$$

$$u[n] \leq f_3(\mathbf{q}_B[n], \mathbf{q}_B^{(k)}[n]), \quad \forall n, \tag{15f}$$

$$f_3(\mathbf{q}_B[n], \mathbf{q}_B^{(k)}[n]) \geq D_{\min}^2, \quad \forall n. \tag{15g}$$

3.3 Subproblem(P6): Jamming UAV Trajectory Optimization

In this subsection, we fix time resources, jamming resources, and Bob's trajectory to optimize Jack's trajectory $\mathscr{Q}_J$. We introduce slack variables $A_E[n]$ such that $A_E[n] \geq [(\|\mathbf{q}_J[n]-\mathbf{W}_E\|+r_E)^2+$

$H^2]$. Let $g(A_E[n])$ be defined in the SINR form

$$g(A_E[n]) = \frac{a}{A_E[n]\sigma^2 + b}, \tag{16}$$

where a, b represent non-negative coefficients. Since $g(A_E[n])$ is a concave increasing function with respect to $A_E[n]$, and $Q(x)$ is a convex decreasing function, according to the properties of composite functions, $-Q(g(A_E[n])) = -h(A_E[n])$ is a decreasing concave function with respect to $A_E[n]$. We perform a first-order Taylor expansion at $A_E^{(k)}[n]$ to find its convex upper bound

$$\begin{aligned} -h(A_E[n]) \leq & -h(A_E^{(k)}[n]) \\ & + h'(A_E^{(k)}[n])(A_E[n] - A_E^{(k)}[n]). \end{aligned} \tag{17}$$

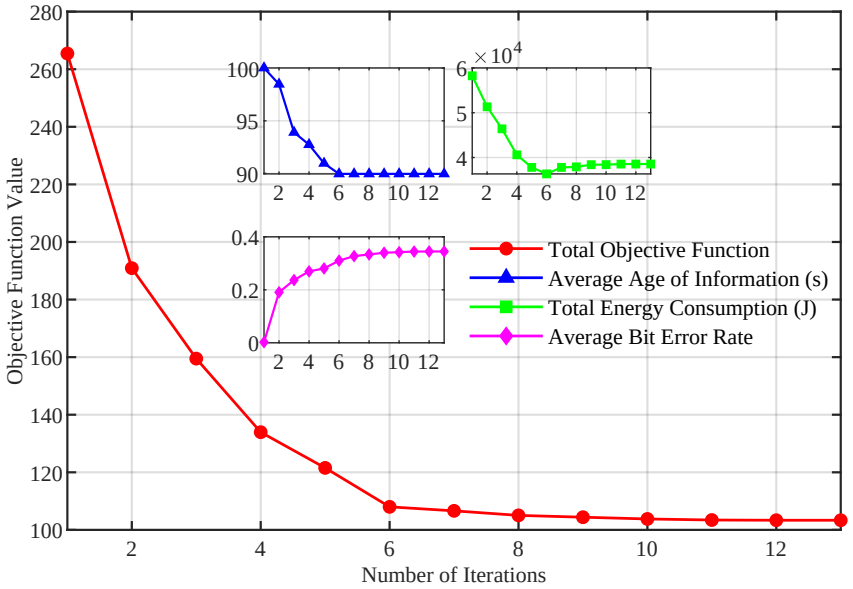

Fig. 2. Convergence performance of the algorithm.

Similarly to Subproblem 4, we linearize the collision constraint to $f_4(\mathbf{q}_J[n], \mathbf{q}_J^{(k)}[n])$. The final

convex subproblem P6 is:

$$
\begin{aligned}
(\mathrm{P6}) \min_{\mathcal{Q}_J,\mathbf{v},A_E} \quad & \omega_2 E_{\text{total}}(\mathbf{v}_J[n]) \\
& + \omega_3 \frac{1}{N} \sum_{n=1}^{N} \beta[n] \Big[-h(A_E^{(k)}[n]) \\
& - h'(A_E^{(k)}[n])(A_E[n] - A_E^{(k)}[n]) \Big] && \text{(18a)} \\
\text{s.t.} \quad & (11\text{j}) - (11\text{l}), (11\text{g}), && \text{(18b)} \\
& f_4(\mathbf{q}_J[n], \mathbf{q}_J^{(k)}[n]) \geq D_{\min}^2, \quad \forall n, && \text{(18c)} \\
& A_E[n] \geq [(\|\mathbf{q}_J[n] - \mathbf{W}_E\| + r_E)^2 + H^2]. && \text{(18d)}
\end{aligned}
$$

By alternately solving the above convex subproblems $\{\mathrm{P2}, \mathrm{P3}, \mathrm{P4}, \mathrm{P5}, \mathrm{P6}\}$, the objective function value is non-increasing monotonically, and the algorithm finally converges.

4 Simulation Results

In this section, we validate the effectiveness of the proposed algorithm through numerical simulations. The experimental scenario consists of two rotary-wing UAVs (Bob and Jack), 4 randomly distributed IoT nodes, and a mobile eavesdropper with uncertain location. We set up a 500×500 m^2 area for simulation. The flight altitude of the two UAVs is fixed at $H = 10$ m, and the minimum safety distance between them is set to $D_{\min} = 25$ m. The maximum speed limit for both Bob and Jack is 40 m/s. The total mission time is divided into $N = 60$ time slots, with the maximum duration of a single time slot set to $T_{\max} = 2$ s. The total data collection requirement is set to $D_M = 3 \times 10^7$ bits. The communication bandwidth is 1 MHz. The reference channel power gain at a distance of 1 meter is $\rho_0 = -50$ dB, and the Gaussian white noise power is $\sigma^2 = -100$ dBm. The transmit power of the INs is 20 mW.

The maximum jamming power of the jamming UAV is limited to $P_{\max}^J = 0.8$ W. Finally, the weighting factors for the optimization objectives are set to $\omega_1 = \omega_2 = \omega_3 = 1/3$. The relevant parameters for UAV propulsion energy consumption are set as follows: profile power $P_0 = 79.8$ W, induced power $P_i = 112.5$ W, tip speed $U_{\text{tip}} = 120$ m/s, fuselage drag ratio $d_0 = 0.6$, rotor solidity $s = 0.05$, air density $\rho = 1.225$ kg/m^3, mean rotor induced velocity $v_0 = 4.03$ m/s, and rotor disc area $A = 0.5$ m^2.

4.1 Convergence Analysis

Fig. 2 illustrates the convergence behavior of the proposed algorithm. As observed from the main red curve, the total objective function value rapidly converges to a stable point within 13 iterations, demonstrating the algorithm's computational efficiency in handling non-convex problems. The embedded subplots further elucidate the dynamics of individual metrics: both the Age of Information (AoI, blue curve with triangles) and total energy consumption (green curve with circles)

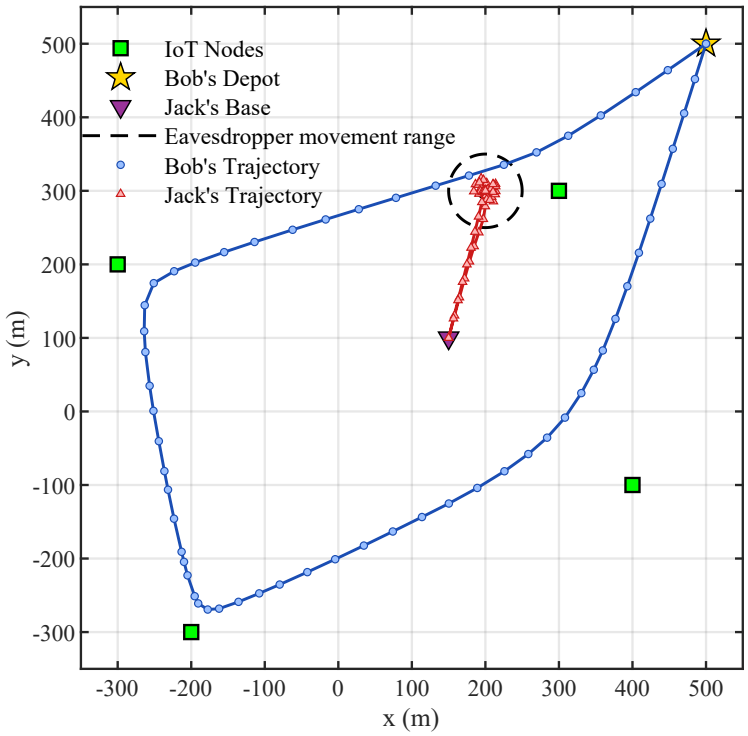

Fig. 3. The optimized trajectories of dual UAVs.

exhibit a monotonic decrease before stabilizing, which validates the effectiveness of the joint time-slot and trajectory optimization. Simultaneously, the eavesdropper's average Bit Error Rate (BER, pink curve with diamonds) ascends and stabilizes at approximately 0.35. This confirms that the optimized jamming strategy effectively degrades the wiretap channel, thereby achieving a superior trade-off among physical layer security, data freshness, and energy efficiency.

4.2 Trajectory Analysis

Fig. 3 displays the optimized horizontal flight trajectories of UAVs. The data collection UAV (Bob, blue trajectory) plans a cyclical path to sequentially approach the uniformly distributed ground IoT nodes. This maneuver allows Bob to obtain better Line-of-Sight (LoS) channel gains to meet data collection requirements. Conversely, the jamming UAV (Jack, red trajectory) flies directly towards and hovers above the potential area of the eavesdropper.

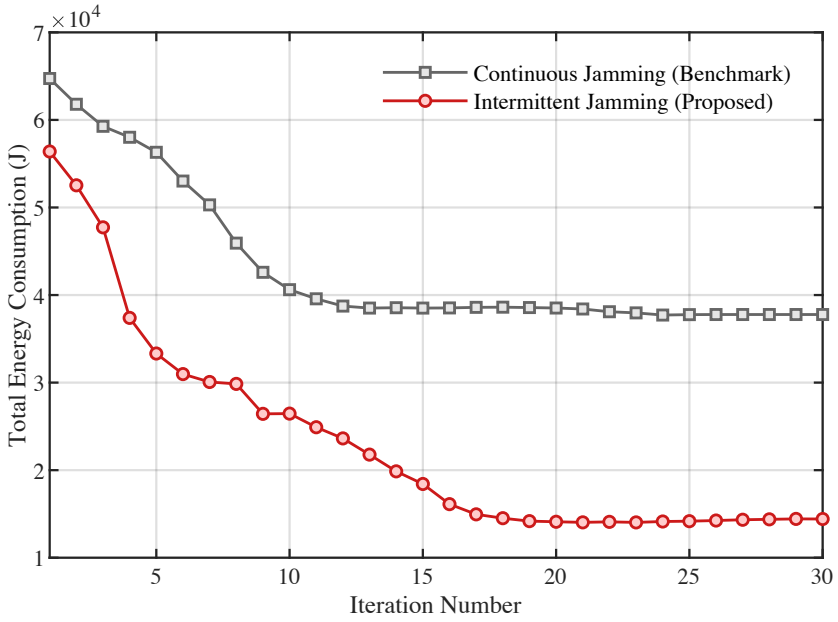

Fig. 4. Comparison of Energy Consumption Under Different Jamming Schemes.

By shortening the jamming distance, Jack maximizes the suppression of the eavesdropping link. This differentiated spatial scheduling strategy intuitively verifies the effectiveness of the algorithm in balancing information freshness and physical layer security.

4.3 Energy Efficiency Comparison

Fig. 4 compares the total system energy consumption of our proposed intermittent jamming scheme with the continuous jamming benchmark scheme. In the experiment, the total data collection requirement is set to 2×10^6bits. As shown in the figure, although the energy consumption of both schemes converges with iterations, the final energy consumption of the proposed scheme is significantly lower than that of the benchmark, achieving energy savings of more than 60%. This is mainly attributed to the proposed algorithm's ability to flexibly schedule the jamming duration ratio. It enables jamming with optimal power only in critical time slots that contribute most to security performance, thereby effectively avoiding the continuous high energy overhead caused by continuous jamming. This validates the superiority of the intermittent jamming scheme.

5 Conclusion

In this paper, we proposed an innovative dual-UAV cooperative communication scheme designed to ensure secure data collection against malicious eavesdroppers with highly uncertain locations. To effectively neutralize these location-incertitude threats without depleting limited power reserves, we introduced a novel intermittent jamming mechanism. However, integrating this mechanism resulted in a highly complex, non-convex optimization problem. To overcome this fundamental mathematical challenge, we developed an efficient iterative algorithm leveraging SCA and BCD techniques. This advanced algorithmic framework allowed us to jointly and dynamically optimize the UAV flight trajectories, the precise intermittent jamming parameters, and the overall time scheduling of the mission. Consequently, our comprehensive approach successfully strikes an optimal balance among three critical, yet often conflicting, system objectives: minimizing total energy consumption, reducing the AoI to ensure timeliness, and maximizing physical layer security. Extensive simulation results rigorously validate the rapid convergence properties of our proposed algorithm. Furthermore, the numerical evaluations conclusively demonstrate that our intermittent jamming strategy significantly outperforms traditional benchmark schemes across various scenarios. It achieves vastly superior energy efficiency while simultaneously enforcing a critically high BER at the eavesdropper, providing robust security and strictly guaranteeing data freshness.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Nos. 62502036, 62572058, U24A20244, and 62472251), the China Postdoctoral Science Foundation (No. 2024M750199), the Outstanding Youth Team of Central Universities (No. QNTD202504), the Young Elite Scientists Sponsorship Program by the China Association for Science and Technology (No. 2023QNRC001), the Taizhou Science and Technology Support Program (Social Development) (No. TSL202519), the General Project for Philosophy and Social Sciences Research in Jiangsu Universities (No. 2025SJYB1697), the Jiangsu Province's "Qinglan Project" (2025): The Program for Middle-aged and Young Academic Leaders,and the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 23KJB510033).

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Messaoudi K, Oubbati OS, Rachedi A, Lakas A, Bendouma T, Chaib N. A survey of UAV-based data collection: Challenges, solutions and future perspectives. Journal of Network and Computer Applications. 2023;216:103670.

[2] Fan X, Huo Y. An overview of low latency for wireless communications: an evolutionary perspective. arXiv preprint arXiv:210703484. 2021.

[3] Amodu OA, Bukar UA, Mahmood RAR, Jarray C, Othman M. Age of Information minimization in UAV-aided data collection for WSN and IoT applications: A systematic review. Journal of Network and Computer Applications. 2023;216:103652.

[4] Fu F, Wei X, Zhang Z, Yang LT, Cai L, Luo J, et al. Age of information minimization for UAV-assisted Internet of Things networks: A safe actor-critic with policy distillation approach. IEEE Transactions on Network Science and Engineering. 2023;11(1):1265-76.

[5] Eldeeb E, de Souza Sant'Ana JM, Pérez DE, Shehab M, Mahmood NH, Alves H. Multi-UAV path learning for age and power optimization in IoT with UAV battery recharge. IEEE Transactions on Vehicular Technology. 2022;72(4):5356-60.

[6] Xiao T, Wei W, Hongliang H, et al. Energy-efficient data collection for UAV-assisted IoT: Joint trajectory and resource optimization. Chinese Journal of Aeronautics. 2022;35(9):95-105.

[7] Li Y, Liang W, Xu W, Xu Z, Jia X, Xu Y, et al. Data collection maximization in IoT-sensor networks via an energy-constrained UAV. IEEE Transactions on Mobile Computing. 2021;22(1):159-74.

[8] Bai Z, Shi J, Li Z, Li M, Liao X. An MA-HPPO approach for multi-UAV data collection. IEEE Transactions on Wireless Communications. 2024. Early Access.

[9] Huo Y, Xu M, Fan X, Jing T. A novel secure relay selection strategy for energy-harvesting-enabled Internet of things. EURASIP Journal on Wireless Communications and Networking. 2018;2018(1):264.

[10] Zhao H, Lu Y, Hong Y, Luo C, Fan X, Chen Z. AoI-and-energy tradeoff scheduling for multi-UAV-enabled data acquisition in Wireless Sensor Networks. Ad Hoc Networks. 2025:103985.

[11] Xu M, Jing T, Fan X, Wen Y, Huo Y. Secure transmission solutions in energy harvesting enabled cooperative cognitive radio networks. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2018. p. 1-6.

[12] Wei L, Jing T, Fan X, Wen Y, Huo Y. The secrecy analysis over physical layer in NOMA-enabled cognitive radio networks. In: 2018 IEEE international conference on communications (ICC). IEEE; 2018. p. 1-6.

[13] Huo Y, Fan X, Ma L, Cheng X, Tian Z, Chen D. Secure communications in tiered 5G wireless networks with cooperative jamming. IEEE Transactions on Wireless Communications. 2019;18(6):3265-80.

[14] Fan X, Huo Y. Security analysis of cooperative jamming in internet of things with multiple eavesdroppers. In: 2019 IEEE Global Communications Conference (GLOBECOM). IEEE; 2019. p. 1-6.

[15] Fan X, Huo Y. Cooperative secure transmission against collusive eavesdroppers in internet of things. International Journal of Distributed Sensor Networks. 2020;16(6):1550147720933464.

[16] Huang L, Fan X, Huo Y, Hu C, Tian Y, Qian J. A novel cooperative jamming scheme for wireless social networks without known CSI. IEEE Access. 2017;5:26476-86.

[17] Fan X, Huang L, Huo Y, Hu C, Tian Y, Qian J. Space power synthesis-based cooperative jamming for unknown channel state information. In: International Conference on Wireless Algorithms, Systems, and Applications. Springer; 2017. p. 483-95.

[18] Xiong X, Sun C, Ni W, Wang X. Three-dimensional trajectory design for unmanned aerial vehicle-based secure and energy-efficient data collection. IEEE Transactions on Vehicular Technology. 2022;72(1):664-78.

[19] Zhang R, Pang X, Lu W, Zhao N, Chen Y, Niyato D. Dual-UAV enabled secure data collection with propulsion limitation. IEEE Transactions on Wireless Communications. 2021;20(11):7445-59.

[20] Zhu Y, Wang S. Efficient aerial data collection with cooperative trajectory planning for large-scale wireless sensor networks. IEEE Transactions on Communications. 2021;70(1):433-44.