sensors

MDPI

Article

Energy Consumption Minimization in Unmanned Aerial Vehicle-Enabled Secure Wireless Sensor Networks

Xufei Ding, Wen Tian, Guangjie Liu and Xiaopeng Ji *

School of Electronics and Information Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China; xufeiding@163.com (X.D.); csusttianwen@163.com (W.T.); gjieliu@gmail.com (G.L.)
* Correspondence: jixiaopeng_nj@163.com

Abstract: In wireless sensor networks (WSNs), unmanned aerial vehicles (UAVs) are considered an effective data collection tool. In this paper, we investigate the energy-efficient data collection problem in a UAV-enabled secure WSN without knowing the instantaneous channel state information of the eavesdropper (Eve). Specifically, the UAV collected the information from all the wireless sensors at the scheduled time and forward it to the fusion center while Eve tries to eavesdrop on this confidential information from the UAV. To surmount this intractable and convoluted mixed-integer non-convex problem, we propose an efficient iterative optimization algorithm using the block coordinate descent (BCD) method to minimize the maximum energy consumption of the ground sensor nodes (GSNs) under the constraints of secrecy outage probability (SOP), connection outage probability (COP), minimum secure data, information causality, and UAV trajectory. Numerical results demonstrate the superiority of the algorithm we proposed in energy consumption and secrecy rate compared with other schemes.

Keywords: unmanned aerial vehicle (UAV); wireless sensor network (WSN); data collection; trajectory optimization; energy minimization

Citation: Ding, X.; Tian, W.; Liu, G.; Ji, X. Energy Consumption Minimization in Unmanned Aerial Vehicle-Enabled Secure Wireless Sensor Networks. *Sensors* **2023**, *23*, 9411. https://doi.org/10.3390/s23239411

Academic Editor: Changchuan Yin

Received: 7 October 2023
Revised: 1 November 2023
Accepted: 22 November 2023
Published: 26 November 2023

1. Introduction

Wireless sensor networks (WSNs), owing to their decentralized control and freeform arrangement, have become prevalent across various applications, including intelligent living, weather monitoring, and health tracking [1,2]. While in regions with sturdy network infrastructure, WSNs can effortlessly link up to the internet and transmit data to the collector [3], in far-flung and inconvenient areas like deserts and plateaus where base stations are not readily deployable, WSNs confront insurmountable hurdles in direct communication with the fusion center [4]. Against this backdrop, unmanned aerial vehicles (UAVs) are emerging as a feasible choice for mobile data collectors for WSNs. Thanks to their pliable deployment and user-friendly control, UAVs can effectively overcome the communication gap and provide a reliable mechanism for WSNs in remote locations [5]. In summary, wireless sensor networks, despite their many merits, are limited in their application in regions where network infrastructure is weak or nonexistent. Fortunately, the deployment of UAVs as mobile data collection tools for WSNs offers a solution to this challenge [6].

WSNs typically consist of a plethora of economical wireless ground sensor nodes (GSNs). In most research on secure sensor networks, there are few studies on the lifespan of UAV-assisted sensor networks. Most papers focus on the energy consumption or communication rate issues of UAVs. However, the energy consumption of these sensors poses a potential threat to the WSN's lifespan [7]. To combat this issue, researchers have proposed a flexible trajectory design of UAVs, which incorporates a sleep and wake-up mechanism to efficiently gather information and preserve GSNs' energy consumption [8]. To further elucidate, the sleep and wake-up mechanism in WSNs implies that when the GSN is not

engaged in any communication with the UAV, it goes into a state of dormancy to conserve energy. Conversely, when the UAV approaches the GSN, the GSN promptly awakens and begins transmitting information to the UAV. However, given the constant movement of the UAV, it is essential to consider the highly dynamic wireless channels between the UAV and the GSNs to avoid any unexpected packet loss [9]. Therefore, reasonable UAV trajectory planning is an indispensable factor that must be taken into account [10].

In addition, the advent of UAVs has made wireless communications a breeze, thanks to their superior information transmission rates [11] and reduced transmit delay [12]. However, their broadcast characteristics make them a susceptible target for illegal eavesdroppers (Eve) [13]. Fortunately, physical layer security, a promising secure communication technology that is extensively employed, plays a pivotal role in preventing the prying eyes of Eve [14]. But here is the catch: in practice, it is very ideal to assume that the channel state information (CSI) of Eve is completely known [15]. Therefore, it is meaningful to discuss UAV-assisted secure communication when the CSI of Eve is unknown.

Driven by the aforementioned facts and challenges, we discuss a UAV-assisted secure WSN to reduce energy consumption in sensor networks while considering the unknown CSI of Eve in secure communication. Considering that turning off the sensors when they are not working can save a lot of energy, we introduce the sleep and wake-up mechanism to reduce sensors' energy consumption through trajectory planning of the UAV. In this paper, we aim to minimize the maximum energy consumption of the GSNs when sending covert information by jointly optimizing the GSN scheduling and the trajectory of the UAV. Moreover, we take things a step further and elevate the discourse by acknowledging the harsh realities of practical scenarios, wherein the instantaneous CSI of Eve is far from perfectly known. The main contributions of this paper are summarized as follows.

1. The crux of our proposition involves an adaptive secrecy transmission policy, which is centered around the classic Wyner encoding scheme. Considering the instantaneous CSI of the Eve link is unknown, we derive an expression for confidentiality capacity under the connection outage probability (COP) and the secrecy outage probability (SOP) constraints.
2. We formulate the energy optimization problem of GSNs as a joint optimization problem that includes GSN scheduling and UAV trajectory. The optimization is subject to several constraints, including COP, SOP, minimum secure communication requirements, GSN scheduling, and UAV trajectory. By solving this problem, we aim to minimize energy consumption and maximize the secrecy rate as much as possible through trajectory optimization while satisfying the aforementioned constraints.
3. We put forward an iterative optimization algorithm based on the block coordinate descent (BCD) approach to transform the intractable optimization problem into two subproblems: GSN scheduling and the UAV trajectory. In the final stage, the optimization problem is solved by alternating iterative optimization of GSN scheduling and UAV trajectory. It is worth mentioning that our algorithm is ultimately convergent, a property that has been mathematically proven.

The rest of this paper is organized as follows. Section 2 introduces the related research about the UAV-enabled secure WSN. Section 3 has a detailed account of the system model. Sections 4 and 5 establish an optimization problem of energy consumption minimization and propose an iterative optimization algorithm to solve it. Furthermore, the effectiveness of the proposed algorithm is verified in Section 6. Finally, the conclusion of this paper is in Section 7.

2. Related Work

2.1. The Application of UAVs in Secure WSNs

UAVs have a wide application space in WSNs, which cannot directly communicate with the data center. Ref. [16] discuss a UAV-powered WSN, where the UAV transmits energy to the ground sensor through the antenna, and the sensor will send the collected information to the UAV after receiving it. The author minimizes the time required for the

UAV to collect information by jointly optimizing the height of the UAV and the antenna beamwidth. In [17], the authors proposed a task offloading mechanism learning algorithm, which can predict the queuing delay of all UAVs, reduce network overhead and increase user satisfaction. Ref. [18] considered a large-scale WSN where some GSN may not be able to upload information for a long time, resulting in insufficient storage capacity. The authors proposed a data collection strategy to minimize the data loss by jointly optimizing the sensor scheduling and the UAV's trajectory. Refs. [19,20] investigated the energy consumption problem of the UAV-assisted WSN. Zhu et al. [19] proposed a novel optimization algorithm based on a deep reinforcement learning technique that can effectively reduce the UAV's consumption. Beak et al. [20] model the UAV collecting ground sensor information as a non-convex problem, and optimize the trajectory by the Voronoi diagram to maximize the residual energy after the sensor transmits information.

2.2. Security Performance in UAV-Enabled WSNs

Since UAVs are more vulnerable to eavesdropping by illegal parties, some recent studies have considered the physical layer security of UAV-assisted WSNs. Ref. [21] investigate a UAV-assisted WSN with multiple eavesdroppers, and considered a downlink secure transmission scheme based on power splitting, where the transmission power of the UAV is divided into information transmission and noise generation. The authors proposed an optimization algorithm to maximize the minimum average secrecy rate. In [22], the authors considered how to improve the quality of service (QoS) of the wireless networks, joint optimization of the video levels selection, power allocation, and a UAV trajectory algorithm is proposed to maximize the ratio of power consumption to video quality. Refs. [23,24] discussed secrecy capacity maximum problem in cache-enabled UAV communications. Ref. [23] investigate a UAV-enabled network with D2D communications, where the UAV and D2D transmitter are equipped with caches that the users can directly obtain high-frequency communication requirements without communicating with the base station. In [24], the caching-equipped UAV is used to replace the small cell to communicate with the user, and the replaced cell is used as the interference source to send interference signals to Eve to improve the security performance of the system.

2.3. Secrecy Energy Efficiency in UAV-Enabled WSN

To realize the goal of energy-efficient communication while ensuring communication, secrecy energy efficiency (SEE) has increasingly become hot research in UAV-assisted WSNs. Li et al. [25] discuss two main challenges in a UAV-enabled WSN: the UAV's energy consumption and secure transmission. The authors proposed a low-complexity iterative algorithm to maximize the secrecy energy efficiency. In [26], the authors discussed a multi-carrier multi-UAV enabled WSN, where the UAVs use Cooperative Rate-Splitting (CRS) technique to protect the communication between UAVs and the ground sensors, and proposed a secure resource allocation alternating iterative algorithm to maximize the UAV's SEE by jointly optimizing the resource allocation and the ground sensors' association matrix. Refs. [27,28] both introduced the simultaneous wireless information and power transfer (SWIPT) technology when considering the maximization of Secrecy Energy Efficiency, among which Ref. [27] assumed that the users divide the received signal into two parts, which are used for energy collection and information decoding, respectively. Ref. [28] assumed that only known the channel distribution information (CDI) of Eves. In addition, the dual-layer PS receiver architecture is introduced to solve the problem of energy harvesting (EH) circuits' performance limitation.

3. System Model

As shown in Figure 1, we consider a UAV-enabled secure WSN where a UAV of FD model is employed as a covert collector to receive the confidential information sent by the ground sensors and transmit the information to the fusion center (FC). The information here can include local communication, logistics, weather, etc. To facilitate subsequent data

processing and without significant loss of generality, we assume that the whole model is based on a three-dimensional (3D) Cartesian coordinate system. We assume that there are M GSNs denoted by $M = \{1, 2, \ldots, m, \ldots M\}$ and all GSNs equipped with an antenna to send collected information to the UAV. We assumed that the UAV's fly altitude H is fixed, and V_{max} represents the maximum flight speed. In addition, the start and end locations, which are denoted as $q_u^0 = \{x_0, y_0, H\}$ and $q_u^N = \{x_N, y_N, H\}$, respectively, are also predetermined. The total time required for the UAV to perform the task is T. We decompose the time T into N parts, $N = \{1, 2, \ldots n, \ldots, N\}$, and the length of each time gap is θ, i.e., $T = \theta N$. The UAV's coordinate at the time slot n is $q_u[n] = \{x_u[n], y_u[n], H\}$, and the coordinates of the SNs, Eve and the FC are denoted as $q_m = \{x_m, y_m, 0\}$, $q_e = \{x_e, y_e, 0\}$ and $q_f = \{x_f, y_f, 0\}$, respectively. We have the UAV's trajectory and start/end location constraints:

$$\begin{aligned} \|q_u[n] - q_u[n-1]\| \leq V_{max}\theta, \forall n \geq 2 \\ q_u[1] = q_u^0, q_u[N] = q_u^N \end{aligned} \tag{1}$$

We tend to adopt the Line of Sight (LoS) channel model for the UAV to GSNs links during this paper. This is often a reasonable assumption, since some researchers have proved that when UAVs fly at a sufficiently high altitude, the LoS channel dominates the UAV-to-ground channel [29]. Thus, the channel power gain from GSNs to the UAV, the UAV to the FC, and Eve can be expressed as:

$$\begin{aligned} g_{u,m}[n] = \beta_0 d_{u,m}^{-\zeta}[n] = \frac{\beta_0}{\|q_u[n] - q_m\|^2 + H^2}, \forall m, \\ g_{u,f}[n] = \beta_0 d_{u,f}^{-\zeta}[n] = \frac{\beta_0}{\|q_u[n] - q_f\|^2 + H^2} \\ g_{u,e}[n] = \beta_0 d_{u,e}^{-\zeta}[n] = \frac{\beta_0}{\|q_u[n] - q_e\|^2 + H^2} \end{aligned} \tag{2}$$

where $\zeta = 2$ denotes the path-loss exponent and β_0 represents the reference channel gain at $l = 1m$.

In addition, the channel power gain from GSNs to Eve can also be expressed as consisting of small-scale fading and large-scale path loss and can be given by

$$g_{m,e} = \beta_0 \|q_m - q_e\|^{-\zeta} \varphi \tag{3}$$

where φ represents the Rayleigh fading obeying exponential distribution with unit mean.

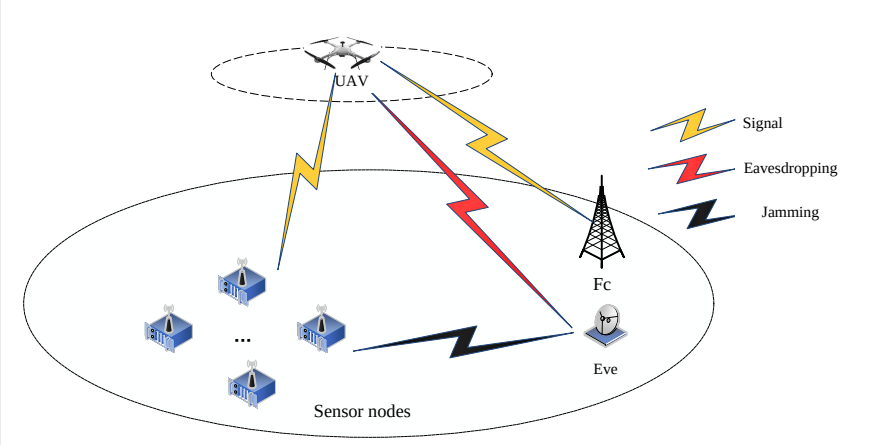

Figure 1. System model.

We assume that the wake-up and data-transmission policy is employed since the ground nodes' power is limited [30]. Specifically, the UAV can control whether the ground nodes wake up. Only when the UAV wakes up the GSNs can the information transmission

between them be carried out. At this time, other nodes are in the shutdown state. Moreover, the communication models between GSNs and the UAV are adopted the periodic time-division multiple access (TDMA) manner. In other words, the UAV can only transmit with one GSN at the same time slot. This can not only save energy consumption of GSNs but also avoid mutual interference between ground nodes during information transmission.

Define the binary wake-up scheduling variables $w_m[n] \in \{0,1\}$ at time slot n. When $w_m[n] = 1$ if the ground node sends data to the UAV; otherwise, $w_m[n] = 0$. Since only one device and the UAV have the communication link at time slot n, the user scheduling constraints can be expressed as follows:

$$\sum_{m=1}^{M} w_m[n] \leq 1, \forall n \in N, w_m[n] \in \{0,1\}. \tag{4}$$

Denoting the transmit power of the UAV and the GSNs as P_u and P_m. Due to the UAV's hardware limitations, although many self-interference (SI) cancellation technologies proposed, the UAV self-interference still exists. Let ω represent the level of SI cancellation. At the time slot n, when the GSNs are in the wake-up state for transmitting data to the UAV, i.e., $w_m[n] = 1$, the channel capacity between the UAV and GSNs can be expressed as:

$$C_{u,m}[n] = \log_2\left(1 + \frac{P_u g_{u,m}[n]}{P_u |g_{u,u}[n]|^2 + \sigma^2}\right), \forall m, \tag{5}$$

where the σ^2 denotes the noise power, and the UAV's self-interference $g_{u,u}$ follows $CN(0,\omega)$, ω is the UAV's self-interference level. Similarly, the channel capacity between the UAV and Eve at the time slot n can be expressed as

$$C_{u,e}[n] = \log_2\left(1 + \frac{P_u g_{u,e}[n]}{P_m g_{d,e} + \sigma^2}\right) \tag{6}$$

4. Problem Formulation

Since Eve's CSI is unknown, we introduce the classic Wyner's secrecy encoding scheme [31], where named two rates: the codeword rate $R_{u,m}[n]$ representing the size of the transmitted code word and the secrecy rate $R_{sec}[n]$. The information rate of Eve represents $R_{u,e}[n]$, and the secrecy rate can be expressed as:

$$R_{sec}[n] = [R_{u,f}[n] - R_{u,e}[n]]^+. \tag{7}$$

where $R_{u,f}[n]$ represent the FC's throughput.

Since there exists the inference channel, the codeword rate $R_{u,m}[n]$ between the UAV and the fusion center may be higher than the channel capacity $C_{u,m}[n]$, resulting the communication links to be interrupted. The COP denoted by $p_m^{cout}[n]$ represents the situation happening can be expressed as

$$\begin{aligned} p_m^{cout}[n] &= Pr(C_{u,m}[n] < R_{u,m}[n]) \\ &= \Pr\left(\log_2\left(1 + \frac{P_m g_{u,m}[n]}{P_u |g_{u,u}[n]|^2 + \sigma^2}\right) < R_{u,m}[n]\right) \\ &= \Pr\left(|g_{u,u}[n]|^2 > \frac{1}{P_u}\left(\frac{P_m g_{u,m}[n]}{2^{R_{u,m}[n]} - 1} - \sigma^2\right)\right) \\ &= 1 - \Pr\left(|g_{u,u}[n]|^2 \leq \frac{1}{P_u}\left(\frac{P_m g_{u,m}[n]}{2^{R_{u,m}[n]} - 1} - \sigma^2\right)\right) \end{aligned} \tag{8}$$

which the PDF of $|g_{uu}[n]|^2$ obeys an exponential distribution with parameter $1/\omega$. So, the $p_d^{cout}[n]$ can be expressed as

$$p_d^{cout}[n] = \exp\left(-\frac{1}{P_u\omega}\left(\frac{P_m g_{u,m}[n]}{2^{R_{u,m}[n]}-1} - \sigma^2\right)\right) \tag{9}$$

In addition, since the UAV cannot know the CSI of Eve, which means we do not have an ideal secure communication environment, and there may happen a secrecy outage incident. p_d^{sout} represent the probability of this situation happening and can be expressed as

$$\begin{aligned} p_d^{sout}[n] &= \Pr(C_{u,e}[n] > R_{u,e}[n]) \\ &= \Pr\left(\log_2\left(1 + \frac{P_u g_{u,e}[n]}{P_m g_{m,e} + \sigma^2}\right) > R_{u,e}[n]\right) \\ &= \Pr\left(g_{m,e} < \frac{1}{P_m}\left(\frac{P_u g_{u,e}[n]}{2^{R_{u,e}[n]}-1} - \sigma^2\right)\right) \end{aligned} \tag{10}$$

The PDF of $g_{m,e}$ obeys an exponential distribution function with parameter $1/(\beta_0 d_{m,e}^{-\zeta})$ in (3), so the SOP can be given by

$$p_d^{sout}[n] = 1 - \exp\left(-\frac{1}{P_m\beta_0 d_{m,e}^{-\zeta}}\left(\frac{P_u g_{u,e}[n]}{2^{R_{u,e}[n]}-1} - \sigma^2\right)\right). \tag{11}$$

Whether the connection outage events or the secrecy outage events, it is something we do not want to happen. Assume the maximum terminal COP and SOP that we can tolerate are ϕ_{cout} and ϕ_{sout}, respectively. So, we have the following constraints:

$$\sum_{m=1}^{M} w_m[n] P_m^{cout}[n] \le \phi_{cout}, \forall n, \sum_{m=1}^{M} w_m[n] P_m^{sout}[n] \le \phi_{sout}, \forall n \tag{12}$$

Let $W = \{w_m[n]\}, \forall d, n$, and $Q = \{q_u[n]\}, \forall n$. Our goal is to minimize the maximum energy consumption of the GSNs when the UAV transmits covert signals. Mathematically, the energy-efficient data collection problem can be formulated as follows:

$$\min_{\{W,Q\}} E_{max} \tag{13a}$$

$$s.t. \sum_{n=1}^{N} w_m[n] E_m \le E_{min}, \forall m, \tag{13b}$$

$$\sum_{m=1}^{M} w_m[n] P_m^{cout}[n] \le \phi_{cout}, \forall n, \tag{13c}$$

$$\sum_{m=1}^{M} w_m[n] P_m^{sout}[n] \le \phi_{sout}, \forall n, \tag{13d}$$

$$\sum_{n=1}^{N} w_m[n](R_{u,f}[n] - R_{u,e}[n]) \ge \xi, \forall m, \tag{13e}$$

$$\sum_{n=1}^{N} w_m[n] R_{u,m}[n] \le \sum_{n=1}^{N} w_m[n] R_{u,f}[n], \forall m, \tag{13f}$$

$$\sum_{m=1}^{M} w_m[n] \le 1, \forall n, w_m[n] \in \{0,1\}, \tag{13g}$$

$$\|q_u[n] - q_u[n-1]\| \le V_{max}\theta, \forall n \ge 2, \tag{13h}$$

$$q_u[1] = q_u^0, q_u[N] = q_u^N. \tag{13i}$$

where $E_m = P_m\theta$ is the energy consumption of the GSN in a one-time slot. Equations (13b) and (13d) are the COP and SOP constraint. B is the system bandwidth. ζ is the minimum confidential capacity we can receive. Equation (13f) is the information causality constraint which means the UAV cannot transmit the information that has not been received. Thus, the UAV's throughput $R_{u,m}[n]$ should no more than the FC's throughput $R_{u,f}[n] = \log_2(1 + P_u g_{u,f}[n]/\sigma^2)$. Since we want the UAV can collect covert information as much as possible, there must have lower bounds of the COP and SOP. Equation (13f) is the GSN scheduling constraint. Equations (13h) and (13i) are the UAV's mobile constraints. Obviously, the problem (13) is nonconvex, because of the complex constraints. Particularly, the constraints (13d) and (13e) are expressed in the form of probability, which makes it difficult for us to deal with this optimization problem.

Note that $p_m^{cout}[n]$ and $p_d^{sout}[n]$ are non-decreasing functions of $R_{u,d}[n]$ and $R_{u,e}[n]$, and it can be seen from (7) that when $R_{u,d}[n]$ increases, the security capacity of the UAV also increases. On the contrary, when $R_{u,e}[n]$ decreases, the security capacity also decreases. So, if we want to maximize the UAV's secrecy rate, the outage probability must be minimum, and the constraint (12) should become equation form, i.e., $\sum_{m=1}^{M} w_m[n]P_m^{cout}[n] = \phi_{cout}, \forall n; \sum_{m=1}^{M} w_m[n]P_m^{sout}[n] = \phi_{sout}, \forall n$. In addition, since the UAV can only have communication with one ground node at one time slot, we can also have $P_m^{cout} = \phi_{cout}$ and $P_m^{sout} = \phi_{sout}$. Combing (8) and (10) and the above analysis, the throughput of the FC and Eve can be expressed as

$$\begin{aligned} &R_{u,m}[n] \\ &= \log_2\left(1 + \frac{P_m g_{u,m}[n]}{-P_u \omega ln(\phi_{cout}) + \sigma^2}\right) \\ &R_{u,e}[n] \\ &= \log_2\left(1 + \frac{P_u g_{u,e}[n]}{-P_m \beta_0 d_{d,e}^{-\zeta} \ln(1 - \phi_{sout}) + \sigma^2}\right) \end{aligned} \tag{14}$$

In the sequel, after the above analysis and transformation, we can substitute Formula (14) into the problem (13) and remove the COP and SOP constraints, i.e., Equations (13b) and (13d). The optimization problem (13) can be simplified as follows:

$$\begin{aligned} &\min_{\{W,Q\}} \ E_{max} \\ &\text{s.t. (13b), (13e), (13f),(13g), (13h), (13i).} \end{aligned} \tag{15}$$

Although we simplify the original optimization problem and remove the complex constraints of probability representation, problem (15) is still non-convex because of the existence of $R_{sec}[n]$. In addition, since the ground nodes' scheduling variables are binary, the optimization problem (15) is nonconvex mixed-integer programming which is hard to cope with directly. In the sequel, we develop an iteration algorithm based on the block coordinate descent (BCD) method and the successive convex approximation (SCA) method to solve it.

5. Problem Solution

In this section, we split the original problem into two sub-problems based on the BCD method. In subproblem 1, with the given trajectory, we use the relaxation method to optimize the GSN schedulings. Subproblem 2 of optimizing the UAV's trajectory with given GSN schedulings is solved by the SCA method.

5.1. The Optimization of GSN Scheduling

First, we optimize the ground nodes' schedulings with the given UAV's trajectory. To this end, by relaxing the binary constraints in problem (15), the standard linear program (LP) can be reformulated as:

$$\begin{aligned} &\min_{\{W,Q\}} E_{max} \\ &\text{s.t. (13b), (13c),(13f), (13h), (13i).} \end{aligned} \tag{16}$$

where $R_{u,d}[n]$ and $R_{u,e}[n]$ can be obtained from (14). It is clear that (16) is an integer programming problem, which can be solved optimally with existing convex optimization techniques.

Notably, the optimization problem (16)'s optimal solution W is continuous. To convert the optimization results into the binary results we need, the rounding method in [32] is employed to cope with it. According to [32], this method not only does not affect the optimality, but can also effectively obtain the binary results we need through reconstructing the continuous results.

5.2. UAV Trajectory Optimization

Then, with the given scheduling W, the original optimization problem has been transformed into a problem of how to optimize the UAV's trajectory to maximize the minimum secrecy capacity of all the SNs, so that we can not only minimize the energy consumption of the GSNs but also maximize the secrecy capacity as much as possible. Introducing the slack variable ϖ and $Q_e[n]$, the UAV's trajectory optimization problem can be expressed as:

$$\max_{\{Q,Q_e,\varpi\}} \varpi \tag{17a}$$

$$s.t. \sum_{n=1}^{N} w_m[n](R_{u,f}[n] - R_{u,e}[n]) \geq \varpi, \forall m, \tag{17b}$$

$$\varpi \leq \sum_{n=1}^{N} R_{u,m}[n] \forall m, \tag{17c}$$

$$\|q_u[n] - q_u[n-1]\| \leq V_{max}\theta, \forall n \geq 2, \tag{17d}$$

$$q_u[1] = q_u^0, q_u[N] = q_u^N. \tag{17e}$$

$$Q_e[n] \leq \|q_u[n] - q_e\|^2, \tag{17f}$$

$$\tag{17g}$$

where

$$\begin{aligned} R_{u,m}[n] &= \log_2\left(1 + \frac{h}{H^2 + \|q_u[n] - q_m\|^2}\right) \\ R_{u,e}[n] &= \log_2\left(1 + \frac{P_u\beta_0}{gQ_e[n]}\right), \\ R_{u,f}[n] &= \log_2\left(1 + \frac{P_m\beta_0}{\sigma^2(H^2 + \|q_u[n] - q_f\|^2)}\right), \end{aligned} \tag{18}$$

where $h = \dfrac{P_u\beta_0}{-P_u\omega\ln(\phi_{cout}) + \sigma^2}$, $g = -P_m\beta_0 d_{m,e}^{-\zeta}\ln\phi_{sout} + \sigma^2$. Then, we introduce the following Lemma to deal with the nonconvex constraints (17b).

Lemma 1. *The constraint (17b) can be rewritten by the following convex constraints.*

$$\sum_{n=1}^{N} w_m[n](R_{u,f}^{lb}[n] - R_{u,e}[n]) \geq \varpi, \forall m, \tag{19}$$

where

$$\begin{aligned}
&R_{u,f}^{lb}[n] = \\
&\Phi^l[n] - \Theta^l[n]\left(\|q_u[n] - q_f\|^2 - \|q_u^l[n] - q_f\|^2\right), \\
&\Theta^l[n] = \\
&\frac{P_m\beta_0}{\ln 2(\sigma^2(H^2 + \|q_u^l[n] - q_f\|^2) + P_m\beta_0)} \\
&\times \frac{1}{\sigma^2(H^2 + \|q_u^l[n] - q_f\|^2)}, \\
&\Phi^l[n] = \log_2\left(1 + \frac{P_m\beta_0}{\sigma^2(H^2 + \|q_u^l[n] - q_f\|^2)}\right),
\end{aligned} \tag{20}$$

Proof. Obviously, $R_{u,f}[n]$ is not a convex function about $q_u[n]$, but we can see that $R_{u,f}[n]$ is a convex function about $\|q_u[n] - q_f\|^2$. It is well known that the lower bound of any convex function at its feasible point can be obtained by its first-order Taylor transformation. Assuming that $Q^l[n] = \{q_u^l[n], \forall n\}$ represents the UAV's trajectory optimization results at the l-th iteration, then at the feasible point $q_u^l[n]$, we can obtain the next iteration of $R_{u,f}[n]$:

$$\begin{aligned}
&R_{u,f}[n] \geq \\
&\Phi^l[n] - \Theta^l[n]\left(\|q_u[n] - q_f\|^2 - \|q_u^l[n] - q_f\|^2\right) \\
&\triangleq R_{u,f}^{lb}[n]
\end{aligned} \tag{21}$$

Similarly, we define $\Gamma_e[n] = (x_u[n] - x_e)^2 + (y_u[n] - y_e)^2 + H^2$, $\Gamma_m[n] = (x_u[n] - x_m)^2 + (y_u[n] - y_m)^2 + H^2$. By introducing the first-order Taylor transformation of $\Gamma[n]$, we have the lower bounds of $\Gamma_e[n]$, $\Gamma_m[n]$ and $R_{u,m}[n]$:

$$\begin{aligned}
&\Gamma[n]_e \geq \Gamma_e^l[n] + 2(x_u^l[n] - x_e)(x_u[n] - x_u^l[n]) \\
&+ 2(y_u^l[n] - y_e)(y_u[n] - y_u^l[n]) \triangleq \Gamma_e^{lb}[n], \\
&R_{u,m}[n] \geq R_{u,m}^{lb}[n] = \log_2\left(1 + \frac{h}{H^2 + \|q_u^l[n] - q_m\|^2}\right) \\
&- \frac{h\left(\|q_u[n] - q_m\|^2 - \|q_u^l[n] - q_m\|^2\right)\log_2 e}{(h + H^2 + \|q_u^l[n] - q_m\|^2)(H^2 + \|q_u^l[n] - q_m\|^2)}
\end{aligned} \tag{22}$$

where $(x_u^l[n], y_u^l[n])$ represents the l-th iteration results of UAV's trajectory.

As such, based on the above-mentioned results, the optimization problem can be approximated into the following convex problem:

$$\begin{aligned}
&\max_{\{Q, Q_e, \varpi\}} \ \varpi \\
&s.t. \sum_{n=1}^{N} w_m[n]\left(R_{u,f}^{lb}[n] - \log_2\left(1 + \frac{P_u\beta_0}{gQ_e[n]}\right)\right) \\
&\geq \varpi, \forall d, \\
&\varpi \leq \sum_{n}^{N} R_{u,m}^{lb}[n], Q_e[n] \leq \Gamma_e^{lb}[n], \forall n, m, \\
&\text{(13h), (13i).}
\end{aligned} \tag{23}$$

Observing that problem (23) is a convex problem, we can use the existing software tools such as CVX 2.2 to solve it efficiently. Thus, the optimization problem (17) can be solved by solving optimization problem (23) and constantly updating the feasible points $(x_u^l[n], y_u^l[n])$. The details of the UAV's trajectory optimization are shown in Algorithm 1.

In addition, Algorithm 1's objective values are non-decreasing and bounded during the iteration process, so Algorithm 1 is convergent. In the sequel, we introduce the overall algorithm to tackle the integer-relaxed problem (13).

Algorithm 1 Successive convex optimization algorithm for Problem (23)

1: Initialize iterations $l = 0$ and trajectory of the UAV as $\{x[i], y[i]\}^0$;
2: **Repeat**
3: Optimizing the problem (23) with given $Q^l[n]$ and $w_m[n]$, and obtain the optimal selection $\{x_u[n], y_u[n]\}^*$
4: Update $Q^{l+1}[n] = \{x_u[n], y_u[n]\}^*$
5: **Until** meeting the terminal condition
6: **Return** the optimal trajectory $\{x_u[n], y_u[n]\}^*$=$Q^l[n]$

□

5.3. Overall Iterative Algorithm and Convergence Analysis

According to the previous analysis, we first employ the BCD method to decompose the original optimization problem that is difficult to be solved directly into two sub-problems, then solve them separately, and finally jointly optimize the problem through the iterative algorithm. The iterative algorithm for the problem (15) is summarized in Algorithm 2.

Algorithm 2 Overall alternating iterative algorithm

1: Initialize iterations $l = 0$, $w_m[n]^0$ and $\{x[n], y[n]\}^0$;
2: **Repeat**
3: Optimizing the problem (16) with given $Q^l[n]$, and obtain the optimal selection $w_m^l[n]$.
4: Optimizing the problem (23) with given $Q^l[n]$ and $w_m^l[n]$, and obtain the optimal selection $Q^{l+1}[n]$.
5: Update $l = l + 1$
6: **Until** meeting the terminal condition.

Then, we analyze the convergence of the algorithm. As presented, the Algorithm enables the satisfaction of constraints (13e) with equality, which is evident after step 4. Subsequently, due to the maximization of the weighted minimum throughput in (17), it is possible to relax constraints (13e) after step 4. This relaxation leads to an expanded optimization space that can be utilized for the reduction of E_{max} in (16). Consequently, with Algorithm 2, the cost values obtained from (16) exhibit a non-increasing behavior across iterations. It is essential to note that the objective value of (16) can be lower-bounded by a finite value, thereby ensuring Algorithm 2's convergence. Moreover, the computational complexity of Algorithm 2 mainly comes from steps 3 and 4, i.e., the optimization of the GSN schedulings and UAV's trajectory. The proposed algorithm's computational complexity is given by $\mathcal{O}(IN^{(2)})$, where N is the number of time slots, and I is the number of iterations of Algorithm 2. As a result, the algorithm may be calculated in polynomial time, making it simple to implement in WSNs with limited resources.

6. Simulation Results

In this section, we verify the performance of the algorithm proposed through numerical simulations. The numerical results obtained by Matlab (2022b). The configuration of the computer is INTEL Core I9 13900KS and NVIDIA GeForce RTX 4090. The start/end locations of the UAV and the FC are all presented as $(800, 0, 0)$. There are 4 GSNs located at $(0, 1000, 0)$ m, $(0, -1000, 0)$ m, $(1000, 0, 0)$ m, and $(-1000, 0, 0)$ m, respectively. The detailed parameters are given in Table 1.

Table 1. Simulation parameters.

Parameters	Values
The altitude of the UAV [32], H	100 m
The reference channel power gain [32], β_0	-60 dB
The level of the UAV's self-inference [15], ω	-120 dB
The noise power [26] , σ^2	-110 dB
The maximum speed of the UAV [32], V_{max}	50 m/s
The length of each time slot [26], θ	0.5 s
The minimum tolerable data received [23], ξ,	100 Kbit
The power of the UAV and ground nodes [33], P_u, P_m,	10 dBm
The maximum SOP\COP constraint [34], $\phi_{sout}\backslash\phi_{cout}$,	0.05

The optimal UAV trajectories achieved by the proposed algorithm under different time T are shown in Figure 2, and Figure 3 shows the optimal UAV trajectories under case 1: $q_e = (500, 0, 0)$ m, case 2: $q_e = (0, 0, 0)$ m, and case 3: $q_e = (0, 500, 0)$ m with $T = 100$ s. According to the results, when the time is enough, the UAV will always be as close to each ground GSN as possible in different cases to obtain a better channel state. At the same time, when approaching the Eve gradually, the UAV will stay away from the Eve while approaching the SN to obtain more secrecy capacity. Figure 4 shows the scheduling optimization results of SNs in case 2. It can be seen from the figure that the GSN is always in the closed state when it is not communicating with UAV, and only when the UAV is fully closed can it be in the communication state. This avoids interference with other SNs and fully saves energy when transmitting confidential information.

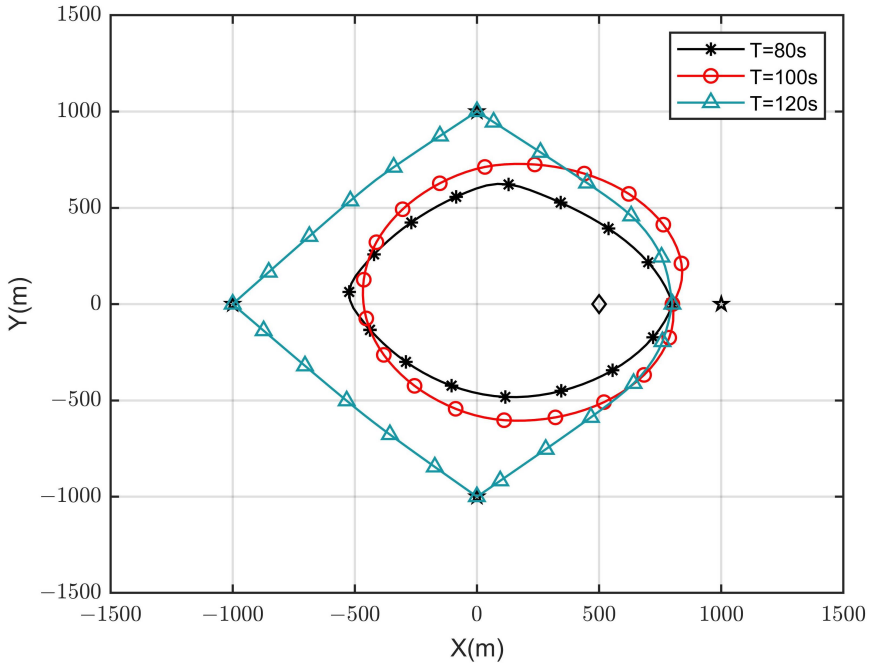

Figure 2. Optimized UAV trajectory in different values of T.

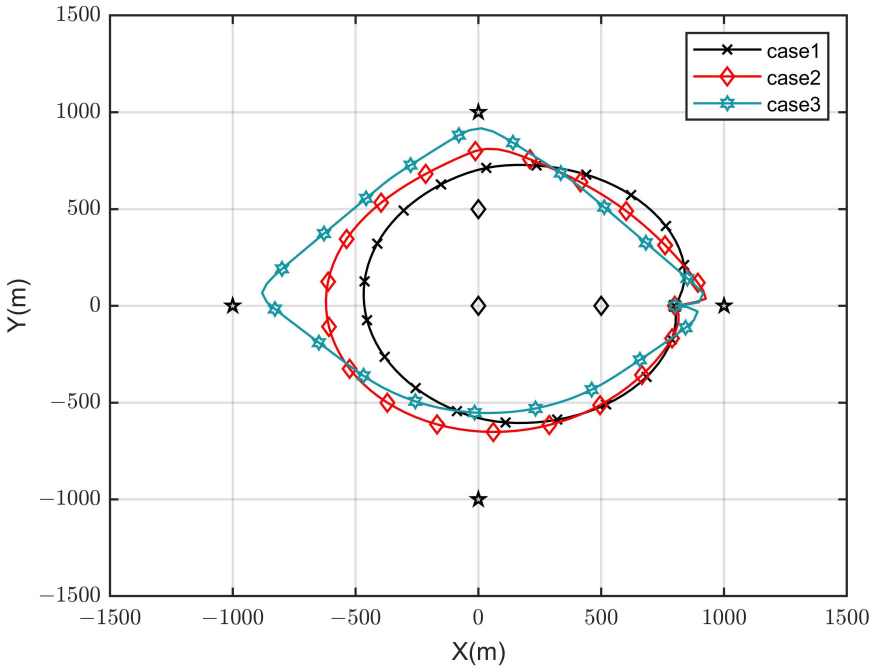

Figure 3. Optimized UAV trajectory under different cases.

Figure 5 shows the convergence of the proposed iterative algorithm under different levels of UAV self-interference. It can be seen that with the increasing number of iterations, the secrecy rate of the UAV is non-decreasing, which is consistent with the convergence analysis results above. In addition, with the increasing degree of self-interference, the secrecy rate will also decrease. This is because with the increase in self-interference, the interference of the signal received by the UAV will be greater and the safety rate will be reduced.

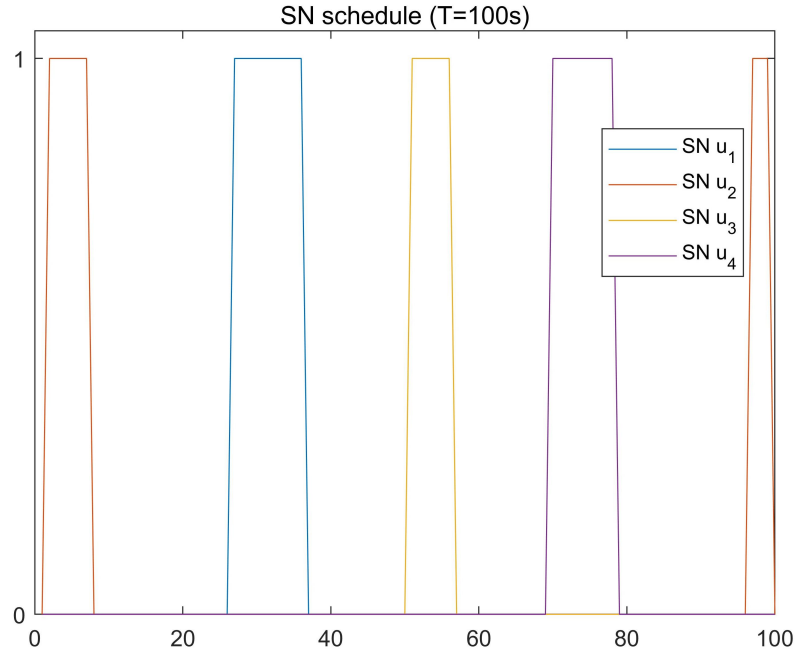

Figure 4. Optimized GSN scheduling.

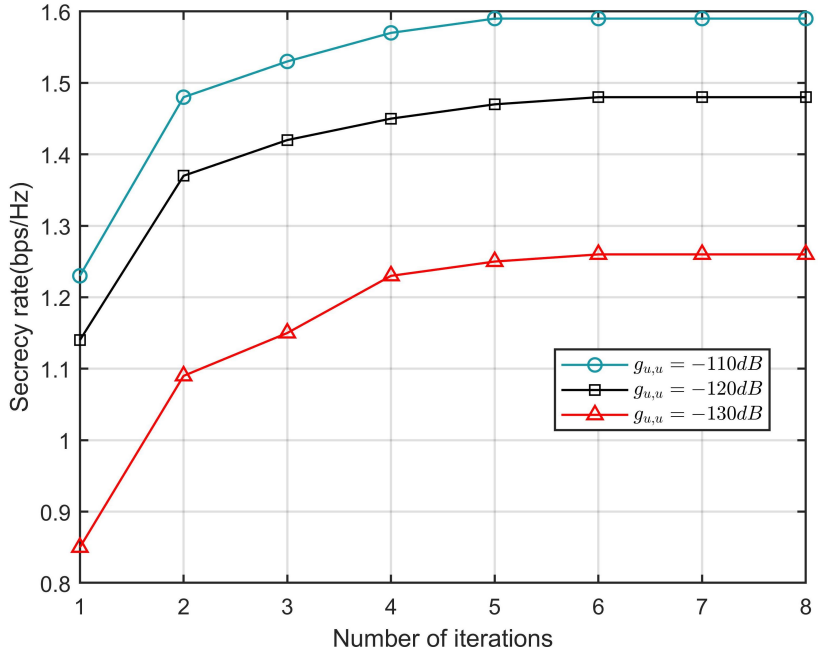

Figure 5. The convergence of the algorithm under different values of g_{uu}.

To better observe the effectiveness of the proposed algorithm, three benchmark schemes are considered for comparison: 1. Elliptic trajectory design with transmission power control. 2. Elliptic trajectory design with fixed transmission power. 3. UAV flies on a circular path with a radius of 500 centered on $(0, 0)$. 4. The UAV operating in TDD mode. Figure 6 shows the comparison of secrecy rate between our joint design scheme and other benchmark schemes at different times T, where Eve is at $(0, 500, 0)$ m. It can be seen that with the increase in time T, the secrecy rate of the UAV is also increasing, because, with the increase in time, the UAV can stay more time at the ground SNs to obtain better channel status and collect more information. In addition, the performance of the scheme with trajectory optimization is always better than that without trajectory optimization, which indicates that trajectory optimization is important to improving the secrecy rate.

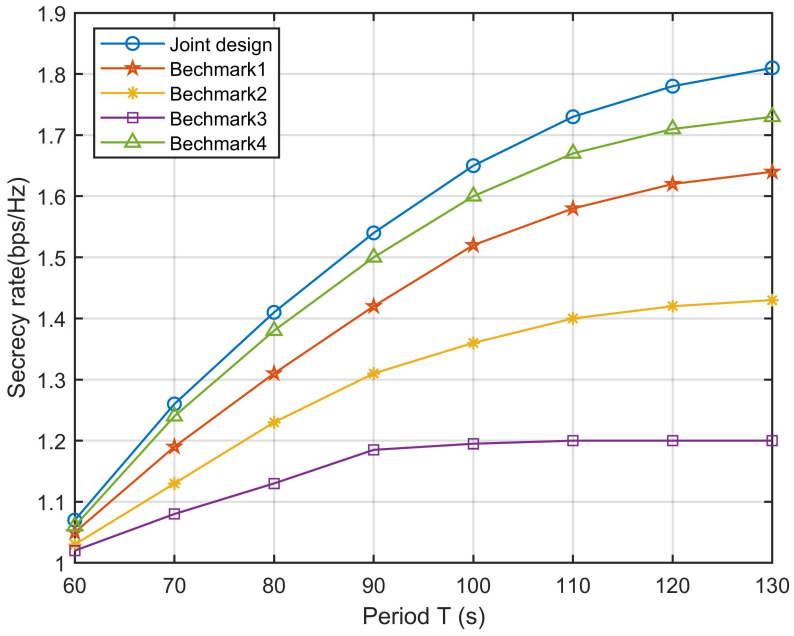

Figure 6. Secrecy rate comparison for different schemes and different values of T.

Figure 7 shows the energy consumption level of the proposed algorithm compared with the JAB algorithm [16], JDCSP algorithm [35], and other schemes under different SOP values. The *SC* and *CF* represent the static collecting scheme and the circular flight scheme [36], respectively. In Figure 7, it is evident that the proposed algorithm uses the least amount of energy, which indicates the importance of joint consideration of GSN scheduling and UAV trajectory. In addition, as SOP increases, the minimum energy consumption will as well, which is because the more stringent SOP requirements will cause the limited communication resources to be unable to support and make the energy consumption higher.

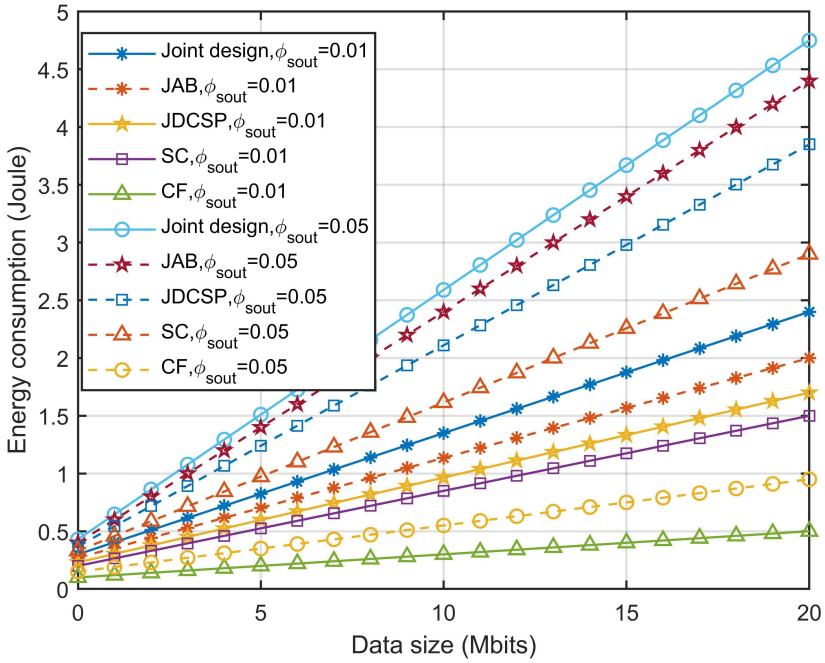

Figure 7. Energy consumption comparison for different schemes and different values of ϕ_{scout}.

7. Conclusions

This paper studies an energy-efficient data collection scheme in a UAV-assisted secure WSN that employs a wake-up mechanism to effectively preserve the energy of SNs. To minimize the energy consumption of sensors while ensuring communication requirements, we proposed a joint optimization algorithm that first decomposes the original problem into two sub-problems based on the BCD method and iteratively tackle each sub-problem to achieve the overall optimization objective. The simulation results demonstrate the effectiveness of our proposed algorithm. Under the premise of meeting communication requirements, the reasonable trajectory planning of the UAV and the wake-up mechanism effectively reduce the transmission energy consumption of sensors. In future work, more channel models and communication technologies will be studied, such as the small-scale fading and the intelligent reflecting surface technology. In addition, better optimization methods that can reduce the algorithm complexity are expected.

Author Contributions: X.D. and W.T.: writing—simulation, review and editing—original draft preparation. G.L. and X.J.: theoretical and writing guidance, funding sponsorship. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key R&D Program of China (Grants No.2021QY 0700) and the National Natural Science Foundation of China (Grants No.U21B2003,62072250), Jiangsu Province Natural Science Foundation (Grants No.BK20230415) and Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grants No.23KJB120007).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Amrallah, A.; Mohamed, E.M.; Tran, G.K.; Sakaguchi, K. Optimization of UAV 3D Trajectory in a Post-disaster Area Using Dual Energy-Aware Bandits. *IEICE Commun. Express* **2023**, *12*, 403–408. [CrossRef]
2. Bao, T.; Yang, H.C.; Hasna, M.O. Secrecy Performance Analysis of UAV-Assisted Relaying Communication Systems. *IEEE Trans. Veh. Technol.* **2020**, *69*, 1122–1126. [CrossRef]
3. Ye, J.; Zhang, C.; Lei, H.; Pan, G.; Ding, Z. Secure UAV-to-UAV Systems With Spatially Random UAVs. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 564–567. [CrossRef]
4. Ouyang, J.; Pan, Y.; Xu, B.; Lin, M.; Zhu, W.P. Achieving Secrecy Energy Efficiency Fairness in UAV-Enabled Multi-User Communication Systems. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 918–922. [CrossRef]
5. Yao, J.; Xu, J. Secrecy Transmission in Large-Scale UAV-Enabled Wireless Networks. *IEEE Trans. Commun.* **2019**, *67*, 7656–7671. [CrossRef]
6. Wang, W.; Tian, H.; Ni, W. Secrecy Performance Analysis of IRS-Aided UAV Relay System. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 2693–2697. [CrossRef]
7. Wang, Y.; Chen, M.; Pan, C.; Wang, K.; Pan, Y. Joint Optimization of UAV Trajectory and Sensor Uploading Powers for UAV-Assisted Data Collection in Wireless Sensor Networks. *IEEE Internet Things J.* **2022**, *9*, 11214–11226. [CrossRef]
8. Wang, Y.; Hu, Z.; Wen, X.; Lu, Z.; Miao, J. Minimizing Data Collection Time With Collaborative UAVs in Wireless Sensor Networks. *IEEE Access.* **2020**, *8*, 98659–98669. [CrossRef]
9. Ebrahimi, D.; Sharafeddine, S.; Ho, P.H.; Assi, C. UAV-Aided Projection-Based Compressive Data Gathering in Wireless Sensor Networks. *IEEE Internet Things J.* **2019**, *6*, 1893–1905. [CrossRef]
10. Wei, Z.; Zhu, M.; Zhang, N.; Wang, L.; Zou, Y.; Meng, Z.; Wu, H.; Feng, Z. UAV-Assisted Data Collection for Internet of Things: A Survey. *IEEE Internet Things J.* **2022**, *9*, 15460–15483. [CrossRef]
11. Abughalwa, M.; Hasna, M.O. A Secrecy Study of UAV Based Networks With Fountain Codes and FD Jamming. *IEEE Commun. Lett.* **2021**, *25*, 1796–1800. [CrossRef]
12. Wu, H.; Li, H.; Wei, Z.; Zhang, N.; Tao, X. Secrecy Performance Analysis of Air-to-Ground Communication With UAV Jitter and Multiple Random Walking Eavesdroppers. *IEEE Trans. Veh. Technol.* **2021**, *70*, 572–584. [CrossRef]
13. Pang, X.; Zhao, N.; Tang, J.; Wu, C.; Niyato, D.; Wong, K.K. IRS-Assisted Secure UAV Transmission via Joint Trajectory and Beamforming Design. *IEEE Trans. Commun.* **2022**, *70*, 1140–1152. [CrossRef]
14. Sun, G.; Tao, X.; Li, N.; Xu, J. Intelligent Reflecting Surface and UAV Assisted Secrecy Communication in Millimeter-Wave Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 11949–11961. [CrossRef]
15. Zhou, Y.; Pan, C.; Yeoh, P.L.; Wang, K.; Elkashlan, M.; Vucetic, B.; Li, Y. Secure Communications for UAV-Enabled Mobile Edge Computing Systems. *IEEE Trans. Commun.* **2020**, *68*, 376–388. [CrossRef]
16. Choi, H.H.; Lee, J.R. Joint Optimization of Altitude and Beamwidth for UAV-Powered Wireless Sensor Networks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 1279–1284. [CrossRef]
17. Al-Share, R.; Shurman, M.; Alma'aitah, A. A Collaborative Learning-Based Algorithm for Task Offloading in UAV-Aided Wireless Sensor Networks. *Comput. J.* **2021**, *64*, 1575–1583. [CrossRef]
18. Wang, X.; Liu, X.; Cheng, C.T.; Deng, L.; Chen, X.; Xiao, F. A Joint User Scheduling and Trajectory Planning Data Collection Strategy for the UAV-Assisted WSN. *IEEE Commun. Lett.* **2021**, *25*, 2333–2337. [CrossRef]
19. Zhu, B.; Bedeer, E.; Nguyen, H.H.; Barton, R.; Henry, J. UAV Trajectory Planning in Wireless Sensor Networks for Energy Consumption Minimization by Deep Reinforcement Learning. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9540–9554. [CrossRef]
20. Baek, J.; Han, S.I.; Han, Y. Energy-Efficient UAV Routing for Wireless Sensor Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 1741–1750. [CrossRef]
21. Fu, H.; Sheng, Z.; Nasir, A.A.; Muqaibel, A.H.; Hanzo, L. Securing the UAV-Aided Non-Orthogonal Downlink in the Face of Colluding Eavesdroppers. *IEEE Trans. Veh. Technol.* **2022**, *71*, 6837–6842. [CrossRef]
22. Zhang, Z.; Zhang, Q.; Miao, J.; Yu, F.R.; Fu, F.; Du, J.; Wu, T. Energy-Efficient Secure Video Streaming in UAV-Enabled Wireless Networks: A Safe-DQN Approach. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1892–1905. [CrossRef]
23. Ji, J.; Zhu, K.; Niyato, D.; Wang, R. Joint Trajectory Design and Resource Allocation for Secure Transmission in Cache-Enabled UAV-Relaying Networks With D2D Communications. *IEEE Internet Things J.* **2021**, *8*, 1557–1571. [CrossRef]
24. Zhao, N.; Cheng, F.; Yu, F.R.; Tang, J.; Chen, Y.; Gui, G.; Sari, H. Caching UAV Assisted Secure Transmission in Hyper-Dense Networks Based on Interference Alignment. *IEEE Trans. Commun.* **2018**, *66*, 2281–2294. [CrossRef]
25. Li, M.; Tao, X.; Li, N.; Wu, H.; Xu, J. Secrecy Energy Efficiency Maximization in UAV-Enabled Wireless Sensor Networks Without Eavesdropper's CSI. *IEEE Internet Things J.* **2022**, *9*, 3346–3358. [CrossRef]
26. Bastami, H.; Moradikia, M.; Abdelhadi, A.; Behroozi, H.; Clerckx, B.; Hanzo, L. Maximizing the Secrecy Energy Efficiency of the Cooperative Rate-Splitting Aided Downlink in Multi-Carrier UAV Networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 11803–11819. [CrossRef]

27. Yu, H.; Guo, S.; Yang, Y.; Ji, L.; Yang, Y. Secrecy Energy Efficiency Optimization for Downlink Two-User OFDMA Networks with SWIPT. *IEEE Syst. J.* **2019**, *13*, 324–335. [CrossRef]
28. Lu, Y.; Xiong, K.; Fan, P.; Ding, Z.; Zhong, Z.; Letaief, K.B. Secrecy Energy Efficiency in Multi-Antenna SWIPT Networks with Dual-Layer PS Receivers. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4290–4306. [CrossRef]
29. Lin, X.; Yajnanarayana, V.; Muruganathan, S.D.; Gao, S.; Asplund, H.; Maattanen, H.L.; Bergstrom, M.; Euler, S.; Wang, Y.P.E. The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles. *IEEE Commun. Mag.* **2018**, *56*, 204–210. [CrossRef]
30. You, C.; Zhang, R. Hybrid Offline-Online Design for UAV-Enabled Data Harvesting in Probabilistic LoS Channels. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3753–3768. [CrossRef]
31. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
32. Wu, Q.; Zeng, Y.; Zhang, R. Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2109–2121. [CrossRef]
33. Fazel, F.; Abouei, J.; Jaseemuddin, M.; Anpalagan, A.; Plataniotis, K.N. Secure Throughput Optimization for Cache-Enabled Multi-UAVs Networks. *IEEE Internet Things J.* **2022**, *9*, 7783–7801. [CrossRef]
34. Zhou, X.; Yan, S.; Shu, F.; Chen, R.; Li, J. UAV-Enabled Covert Wireless Data Collection. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3348–3362. [CrossRef]
35. Zhu, M.; Wei, Z.; Qiu, C.; Jiang, W.; Wu, H.; Feng, Z. Joint Data Collection and Sensor Positioning in Multi-UAV-Assisted Wireless Sensor Network. *IEEE Sens. J.* **2023**, *23*, 23664–23675. [CrossRef]
36. Xiao, L.; Xu, Y.; Yang, D.; Zeng, Y. Secrecy Energy Efficiency Maximization for UAV-Enabled Mobile Relaying. *IEEE Trans. Green Commun. Netw.* **2020**, *4*, 180–193. [CrossRef]