telecom

MDPI

Article

Security Improvement for UAV-Assisted Integrated Sensing, Communication, and Jamming Networks

Lin Shi [1,†], Chuansheng Yan [2,†], Dingcheng Yang [1], Yu Xu [1,*], Fahui Wu [1] and Huabing Lu [1]

[1] The Information Engineering School and the Jiangxi Provincial Key Laboratory of Advanced Signal Processing and Intelligent Communications, Nanchang University, Nanchang 330031, China; sl@email.ncu.edu.cn (L.S.); yangdingcheng@ncu.edu.cn (D.Y.); wufahui@ncu.edu.cn (F.W.); luhuabing@ncu.edu.cn (H.L.)

[2] China Mobile (Jiangxi) Virtual Reality Technology Co., Ltd., Nanchang 330031, China; yanchuansheng@jx.chinamobile.com

* Correspondence: xuyu@ncu.edu.cn

† These authors contributed equally to this work.

Abstract

We propose a unmanned aerial vehicle (UAV)-assisted integrated sensing, communication, and jamming (U-ISJC) framework, in which a multifunctional UAV first detects the sensing target to obtain sensing information, and subsequently transmits the information to communication users via a unified beam in the presence of multiple eavesdroppers. To avoid functional conflicts, a time slot frame structure is designed for the UAV's multifunctional capabilities, enabling communication, sensing, and jamming tasks within each timeslot. The time slot allocation factor dynamically adjusts based on the UAV's flight trajectory for efficient UAV resource utilization. Additionally, to prevent security rate leakage caused by eavesdroppers, a jamming beam is added to serve both jamming and sensing functions. Our objective is to maximize the the worst-case total secure data transmission rate by jointly optimizing sub-time slot allocation, beamforming, and UAV trajectory. To address this problem, we propose a joint optimization algorithm that adopts the concave–convex procedure (CCCP) technique and semi-definite relaxation (SDR), under the block coordinate descent (BCD) framework. The simulation results show that compared with the baseline scheme, the proposed algorithm substantially improves the communication security rate while ensuring the quality of communication and sensing.

Keywords: beamforming; integrated sensing communication, and jamming; secure rate; trajectory; UAV

Check for updates

Academic Editor: George Tsoulos

Received: 15 January 2026
Revised: 6 February 2026
Accepted: 13 February 2026
Published: 3 March 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Under the 6G (sixth generation) communication standard, sensing and communication functions [1–3] will coexist and be integrated within the same system. Compared to traditional solutions that separate sensing and communication [4], integrated sensing and communication (ISAC) technology enables the sharing of the same time domain, frequency domain, and other wireless communication resources, thereby achieving mutual benefits [5]. ISAC offers two primary advantages: integration gain enables the efficient utilization of congested wireless/hardware resources, while coordination gain balances dual-function performance and achieves synergistic complementarity [6]. In the 6G era, sensing and communication functions will coexist and be deeply integrated within a single system [7], sharing temporal, and frequency and spatial domain resources alongside critical elements

such as waveforms, signal processing, and hardware. The integration of sensing and communication functions can be achieved at various levels, ranging from loose coupling to full integration. This encompasses spectrum sharing, hardware sharing, and even shared signal processing and protocol stacks, extending to cross-module and cross-layer information sharing to achieve mutual benefits.

Meanwhile, unmanned aerial vehicles (UAVs) are increasingly deployed within ISAC networks due to their high cost-effectiveness and operational flexibility [8]. Serving as economical aerial platforms [9], UAVs leverage their high cruising altitudes and three-dimensional maneuverability to deliver enhanced coverage and improved sensing and communication services. Traditional UAV-enabled wireless network research primarily focuses on designs separating sensing and communication functions, neglecting integrated waveform design for co-located sensing and communication. However, integrating UAV and ISAC technologies not only leverages UAVs' high mobility and airspace resource advantages but also conserves spectrum resources, enabling synchronous communication and sensing with users.

However, due to the inherent line of sight (LoS) channel characteristics of UAVs, they are more susceptible to eavesdropping and jamming attacks [10]. Therefore, protecting legitimate users from malicious attacks has emerged as a novel and challenging problem. Similarly, while ISAC networks enhance spectrum utilization, they also introduce new security vulnerabilities [11], posing numerous challenges to physical layer security. First, due to the deep integration of communication signals and perception, malicious attackers exploit the characteristics of spectrum resource sharing to target both perception and communication bands, disrupting normal system operation [12]. Second, ISAC networks integrate multiple functions and technologies, resulting in more complex network architectures. This complexity increases the number of potential security vulnerabilities within the network. This implies that as functionality diversifies and technologies converge, ISAC networks face heightened security risks alongside enhanced capabilities. Consequently, drone-supported ISAC secure communications have become a focal point of intense research debate [13].

Unlike research on physical layer security for traditional drone ISACs, integrated sensing, jamming, and communication (ISJC) networks not only provide synchronized sensing and communication services but also establish secure communication environments by integrating jamming capabilities [14,15]. Existing ISJC network studies primarily focus on deploying artificial noise (AN) or jamming beams to enhance secure communication rates. The primary methods include generating spoofed signals mimicking legitimate signals to interfere with malicious nodes' signal demodulation and decoding, and transmitting high-power noise or frequency-sweeping signals to degrade malicious nodes' signal-to-noise ratio below communication thresholds. Introducing artificial noise within communication ranges effectively thwarts eavesdropping attempts and prevents information leakage. Consequently, drone research incorporating ISJC technology has emerged as a hot topic in drone physical layer security.

1.1. Related Work

Numerous studies in the literature have explored UAV-assisted ISAC. Xu et al. [16] proposed a novel UAV-ISAC framework that involves a fundamental trade-off between computational power and perception beam gain. In [17], the authors investigated resource allocation for multi-UAV-assisted ISAC systems, aiming to maximize the weighted sum bit rate for all ground users. Leveraging the convergence of UAV and multi-antenna technologies, numerous studies have focused on key aspects of UAV-ISAC on beamforming techniques [18]. In [19], the authors propose a multi-antenna UAV ISAC system that jointly optimizes target scheduling, transmit beamforming, and UAV trajectories to maximize

the average beam gain of the radar receiver while satisfying specific communication performance constraints. In [20], Zhenyu Xiao et al. explored the potential of millimeter–wave–UAV communications, proposing two multi-beamforming schemes to increase the number of served users. Some works also combine the high mobility advantages of UAVs with beamforming techniques. Xian Zhang et al. proposed a novel RF signal sensing-assisted beamforming and trajectory design method for UAV networks in [21]. In [22], K. Meng et al. achieve overall reachable rate maximization by jointly optimizing beamforming, user association, sensing time selection, and UAV trajectories. Notably, most of these studies focus on resource allocation, beamforming, and trajectory optimization to enhance overall system efficiency or achieve reachable rate maximization.

Regarding drone safety, Heng Zhang et al. designed a novel optimal three-dimensional coordinate and power search method for mobile UAV base station scenarios [23], which includes enhancing UAV communication network performance by employing friendly jamming drones. Wei Wang et al. investigated robust joint design for secure drone communication systems under energy constraints with incomplete eavesdropper location information [24], incorporating the cooperative transmission of artificial noise signals to confuse malicious eavesdroppers. In [25], Gaurav K. Pandey et al. introduced a dual-UAV-assisted communication scheme enabling secure information transmission between IoT devices and base stations under multiple eavesdroppers. Xiangyun Meng et al. leveraged inter-user interference in uplink non-orthogonal multiple access [26] to enhance IoT node security. In [27], Runze Dong et al. investigated secure relay systems for secure transmission within drone swarms by optimizing beamforming vectors and bandwidth allocation coefficients to maximize achievable confidential rates. Thus, secure communication for UAVs remains a prominent research topic. Consequently, UAV-enabled ISAC secure communication has become a hotly debated subject among researchers [28–31]. Specifically, Ref. [28] proposes an extended Kalman filter-based approach to design secure ISAC systems by optimizing real-time UAV trajectories. Ref. [29] investigates a UAV-supported secure ISAC system where the UAV functions as an aerial base station simultaneously handling user communications and ground target detection, while a dual-function eavesdropper attempts to intercept sensing and communication signals. Zeyu Yang in [30] studies secure transmission in UAV-assisted ISAC systems under eavesdropper presence, where the UAV serves as an aerial dual-function access point. In [31], Chen Dai formulates a privacy-oriented joint optimization problem integrating UAV trajectory design, RIS phase shift configuration, beamforming, and decoupled uplink–downlink user association. Notably, most traditional UAV-ISAC security research focuses on filtering algorithms, beamforming design, trajectory planning, and resource allocation to maximize secure rates.

Many researchers have enhanced the security of UAV-ISAC communication systems by introducing AN. For instance, Ref. [32] proposed two intelligent reflecting surface (IRS)-UAV security schemes enabling ISAC to counter jamming and eavesdropping attacks. Additionally, aerial IRS can coordinate artificial noise to ensure target detection accuracy while suppressing eavesdropping. In addition, the paper [33] proposes a secure rate-partitioned multiple-access enhanced ISAC framework that simultaneously addresses both active and passive eavesdroppers, enhancing system security while maintaining perception performance. The paper [34] proposes a drone-assisted secure communication system for ISAC in multi-eavesdropper scenarios, guaranteeing the security of communication links between source drones and users despite multiple eavesdroppers. Furthermore, Ref. [35] proposes a novel ISJC framework and online resource allocation design to secure drone-supported downlink communications, advocating the use of artificial noise for the simultaneous detection and jamming of eavesdropping drones. Building upon this architecture, Ref. [36] proposed an integrated sensing, navigation, and communication

framework to protect UAV-enabled wireless networks against mobile eavesdropping UAVs, estimating the eavesdropping UAV's state and predicting eavesdropping channel characteristics. However, the aforementioned studies [32–36] all treat the perception target and jamming target as the same entity. They also neglect the gains in improving the system communication security rate achieved through dynamic resource allocation between perception and communication functions. Additionally, most of the aforementioned studies employ a single-antenna UAV design, disregarding the impact of deploying multi-antenna UAVs with beamforming techniques on enhancing the system's secure communication rate. Traditional ISAC-AN schemes involve significant trade-offs between communication and jamming targets. Most adopt passive jamming to counter eavesdropping, failing to fully leverage directional advantages. Their limited jamming methods prove ineffective in complex scenarios with energy constraints and large numbers of users. For convenience, the comparisons of our work with the state of the art schemes are summarized in Table 1.

Table 1. Comparison between state-of-the-art schemes and our work.

Reference	ISAC	UAV Trajectory	Resource Allocation	Beamforming	Multiple Targets	Target Separation	Artificial Noise	Secure Rate Maximization
[3]	✓							
[8]		✓						
[10]		✓				✓	✓	✓
[11]	✓							✓
[13]	✓	✓	✓					✓
[15]	✓			✓	✓			
[16]	✓	✓		✓				
[24]					✓		✓	✓
[27]			✓	✓				✓
[28]	✓	✓						✓
[31]	✓	✓		✓				✓
[32]	✓						✓	✓
[33]	✓		✓		✓	✓		✓
[34]	✓	✓	✓		✓	✓		✓
[35]	✓				✓		✓	
Our Work	✓	✓	✓	✓	✓	✓	✓	✓

✓indicates that the relevant literature review covers this technology, while a blank space indicates that it does not.

1.2. Motivations and Contributions

Existing research rarely addresses the gains in secure rate improvement from dynamic sub-time slot allocation and beamforming optimization. Furthermore, due to the diversity of UAV secure communication scenarios, the issue of separating sensing targets from jamming targets warrants in-depth investigation. The innovative significance of distinguishing between sensing and jamming targets lies in revealing the spatial, temporal, and power mismatches between sensing and jamming behaviors. This enables the independent optimization of these two functions, which significantly enhances the precision of jamming and improves system communication security. However, existing UAV-ISAC security research has not addressed this aspect. To address these gaps, this paper proposes a UAV-assisted integrated sensing, jamming, and communication (U-ISJC) architecture. A multifunctional UAV first acquires echo information by sensing ground sensing targets (STs). Subsequently,

it communicates with communication users (CUs) via a unified beam in an environment containing eavesdroppers (Eves). Simultaneously, to mitigate information leakage risks, the UAV synchronously transmits jamming signals through this unified beam.

The main contributions of this paper are summarized as follows:

- We propose a novel U-ISJC framework that aims maximize the secure rate by jointly optimizing the sub-time slot allocation, beamforming, and UAV trajectory, while satisfying communication and sensing thresholds, fairness requirements, and UAV mobility constraints.
- To solve this challenging non-convex problem, we first use an equivalence method to transform it into a tractable form. Then, we apply the block coordinate descent (BCD) structure, and invoke the concave–convex procedure (CCCP) and the semi-definite relaxation (SDR) to develop an iterative algorithm.
- Numerical results demonstrate the convergence performance of the proposed algorithm, and further show that it significantly improves the secure communication rate of the U-ISJC network compared to the benchmark schemes.

1.3. Organization and Notations

The paper is organized as follows: Section 2 briefly introduces the frame structure design, system model, channel model, and problem description of the U-ISCJ secure communication system. Section 3 elaborates on the joint optimization algorithm proposed in this paper, which primarily consists of three optimization subproblems: sub-time slot allocation optimization, beamforming optimization, and UAV trajectory optimization. Section 4 presents simulation analyses of the proposed method, covering algorithm convergence, UAV trajectory optimization results, UAV velocity optimization results, sub-time slot allocation factor optimization results, and the impact of antenna power, UAV flight altitude, and eavesdropper count on the worst-case security rate. Section 5 summarizes the conclusions of this study.

Notations: $||\cdot||$, $||\cdot||_2$, and $||\cdot||_*$ are used to denote Euclidean norm, spectral norm, and nuclear norm, respectively. $|\cdot|$ denotes the modulus, $\mathbf{x}^\dagger$ denotes the transpose of vector $\mathbf{x}$, and $\mathbf{X}^H$ denotes Hermitian transpose of matrix $\mathbf{X}$. $\mathbb{C}^{M\times N}$ denotes the complex matrix with space of $M \times N$, and use $\otimes$ to denote Kronecker product; $x \sim \mathcal{CN}(\mu, \sigma^2)$ means that x obeys μ-mean and σ^2-variance circularly symmetric complex Gaussian (CSCG) distribution. The main notations used in this paper are listed in Table 2.

Table 2. List of notations.

Notation	Definition	Parameter Value
K	Number of legitimate communication users	3
J	Number of illegal communication eavesdroppers	2
S	Number of ground sensing targets	2
M	Number of UAV antennas	4×4
$\mathbf{q}_I$	UAV flight starting point	$[-200, -200]$ m
$\mathbf{q}_F$	UAV flight endpoint	$[200, 200]$ m
q_z	UAV flight altitude	100 m
T	Total service time	30 s
V_{max}	Maximum flight speed	30 m/s
δ_t	Duration of the sub-time slot	0.5 s

Table 2. *Cont.*

Notation	Definition	Parameter Value
β_0	Average channel power gain at a distance of 1m	−30 dB
σ_k^2	Noise power received by authorized users	−80 dBm
σ_j^2	Illegal user receiver noise power	−80 dBm
σ_e^2	Perceived noise power at the target receiver	−150 dBm
P_{max}	Maximum antenna output power	1 W
$R_{\min}^k$	Communication quality threshold	0.25 bit/s/Hz
Γ_e	Sensing intensity threshold	10^{-12}
ε	Algorithm convergence accuracy	10^{-2}
I_{max}	Maximum iteration count for the algorithm	50

2. System Model and Problem Formulation

2.1. System Model

As shown in Figure 1, we consider a U-ISJC framework, where the UAV performs downlink communication to K CUs while simultaneously sensing E ground STs. There are J Eves attempting to intercept the communication between the UAV and CUs. The UAV is equipped with an $M = M_x \times M_y$ uniform planar array (UPA). Assuming the total flight time T is divided into N time slots, each with a duration of $\delta_t = T/N$, we deliberately adopt a quasi-static (or slowly time-varying) channel assumption within each time slot, disregarding Doppler effects induced by high mobility. In a three-dimensional Cartesian coordinate system, the horizontal positions of the UAV in time slot n is denoted by $\mathbf{q}[n] = [q_x[n], q_y[n]]^\dagger$. The position of CU k, Eve j, and ST e are presented by $\mathbf{u}_k$, $\mathbf{u}_j$, and $\mathbf{u}_e$, respectively. Furthermore, it is assumed that the UAV flies at a fixed altitude q_z.

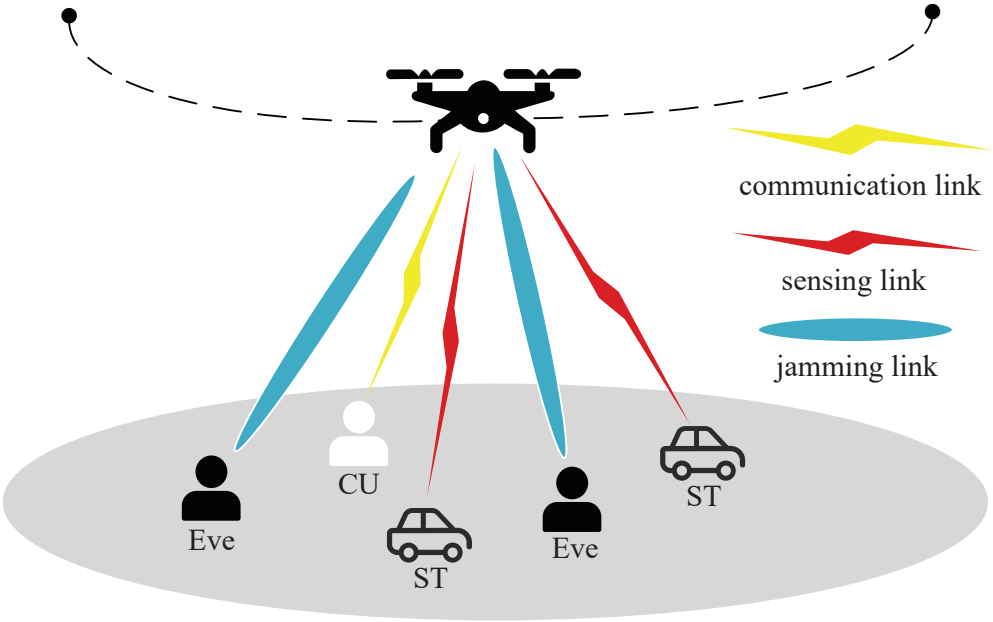

Figure 1. U-ISJC secure communication system.

Assuming that the UAV ground channels are dominated by LoS links and following the free space channel model, let $\mathbf{h}_k^H[n] \in \mathbb{C}^{M\times 1}$ and $\mathbf{h}_j^H[n] \in \mathbb{C}^{M\times 1}$ represent the channels from the UAV to the CU, and the UAV to the Eve, i.e., we have

$$\mathbf{h}_\epsilon^H[n] = \sqrt{\beta_0} d_\epsilon^{-1}[n] \mathbf{a}^H(\mathbf{q}[n], \mathbf{u}_\epsilon), \tag{1}$$

where $\epsilon = \{k, j, e\}$ denotes the channels between each element and the UAV and β_0 denotes the reference channel gain; where β_0 denotes the reference channel gain at 1 m, the response vector of the drone antenna array is as follows [13]:

$$\begin{aligned}\mathbf{a}^H(\mathbf{q}[n], \mathbf{u}_k) = [1, e^{j\frac{2\pi}{\lambda}d_x\Phi_k[n]}, \ldots, e^{j\frac{2\pi}{\lambda}(M_x-1)d_x\Phi_k[n]}] \otimes \\ [1, e^{j\frac{2\pi}{\lambda}d_y\Omega_k[n]}, \ldots, e^{j\frac{2\pi}{\lambda}(M_y-1)d_y\Omega_k[n]}],\end{aligned} \tag{2}$$

where $\Phi_k[n] = \frac{\mathbf{q}_x[n]-u_{kx}}{d_k[n]}$ and $\Omega_k[n] = \frac{\mathbf{q}_y[n]-u_{ky}}{d_k[n]}$ are dependent on the zenith angle of departure (AoD) of the signal from the UAV to CU k and the corresponding azimuth angle of AoD. Moreover, $d_\epsilon[n] = \sqrt{||\mathbf{q}[n] - \mathbf{u}_\epsilon||^2 + q_z^2}$ refers to the Euclidean distance; λ represents the wavelength; and d_x and d_y are the antenna spacing along x-axis and y-axis, respectively.

(1) U-ISJC Frame Structure: To coordinate the communication and sensing, we propose a U-ISJC time frame structure, as illustrated in Figure 2. Specifically, to coordinate the radar sensing and communication, each time slot is divided into two segments, i.e., $\alpha[n]\delta_t$ for radar sensing and $(1-\alpha[n])\delta_t$ for communication,with $\alpha[n] \in [0, 1]$. Within each time slot, the UAV first senses the STs, and then transmits the sensed signals to CUs with the unified beam. This factor $\alpha[n]$ directly governs the time allocation between perception and communication. Increasing the perception sub-time slot enhances the perception quality but compresses the communication time, thereby limiting the achievable communication rates; the reverse holds true. This trade-off is particularly critical in UAV-ISJC systems, as perception quality in turn influences the upper bound of communication rates through information causality constraints.

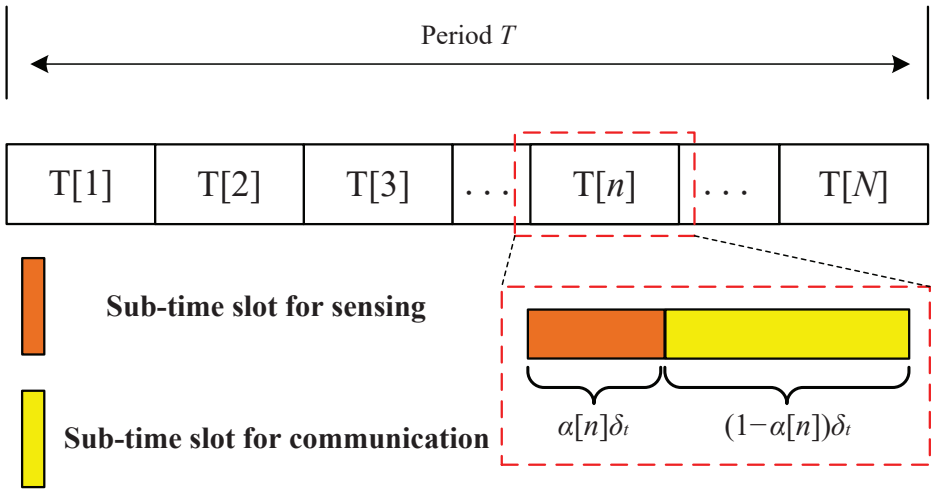

Figure 2. ISJC-UAV frame structure design.

(2) Communication Model: Let $\mathbf{s}_k[n]$ denote the transmit information signal to CU k, and $\mathbf{s}_j[n]$ denote the jamming signal to Eve j. $\mathbf{s}_k[n]$ and $\mathbf{s}_j[n]$ serve as indicators, marking the sections responsible for signal transmission. They are transmitted simultaneously with their corresponding beamformers $\mathbf{w}_k[n] \in \mathbb{C}^{M\times 1}$ and $\mathbf{v}_j[n] \in \mathbb{C}^{M\times 1}$. Thus, the transmitted signal in time slot n is given by $\mathbf{w}[n] = \mathbf{w}_k[n]\mathbf{s}_k[n] + \mathbf{v}_j[n]\mathbf{s}_j[n]$. In unified beam design, power is dynamically allocated among sensing, communication, and jamming functions. Increasing the jamming power helps suppress eavesdroppers but may degrade the sensing quality or communication–SNR ratio, necessitating fine-tuned optimization adjustments. Although sensing and jamming share the same unified beam in hardware implementation, their optimization targets are independent in the mathematical model. The beamforming

vector is optimized to balance these two independent objectives, rather than coupling them into a single target.

We assume that the interference signals in the paper are pre-designed using artificial noise similar to that in [14]. This interference signal can generate specific interference signals based on channel characteristics, thereby enhancing confidentiality capacity by reducing eavesdropping channel capacity without affecting legitimate channel capacity. Accordingly, the communication rate between the UAV and CU k in time slot n (in bit/s/Hz) is expressed as

$$R_k^{com}[n] = (1-\alpha[n])\log_2\left(1+\frac{\left|\mathbf{h}_k^H[n]\mathbf{w}_k[n]\right|^2}{\sum\limits_{i\neq k}\left|\mathbf{h}_k^H[n]\mathbf{w}_i[n]\right|^2+\sigma_k^2}\right). \tag{3}$$

Similarly, the intercepted rate at Eve j for CU k's signal can be denoted as

$$R_{j,k}^{com}[n] = (1-\alpha[n])\times \log_2\left(1+\frac{\left|\mathbf{h}_j^H[n]\mathbf{w}_k[n]\right|^2}{\sum\limits_{i\neq k}\left|\mathbf{h}_j^H[n]\mathbf{w}_i[n]\right|^2+\sum\limits_{s=1}^{J}\left|\mathbf{h}_j^H[n]\mathbf{v}_s[n]\right|^2+\sigma_j^2}\right). \tag{4}$$

The jamming performance is measured by the suppression of the Eve's intercept rate in (4). Since multiple Eves exist in the scenario, and multiple Eves simultaneously eavesdrop on legitimate CUs, we select the Eve causing the most severe leakage of legitimate information as the worst-case eavesdropping scenario. Therefore, for any CU k in time slot n, we can define its worst-case security rate as

$$R_k^{sec}[n] = R_k^{com}[n] - \max_{\forall j} R_{j,k}^{com}[n]. \tag{5}$$

(3) Sensing Model: Based on [22], the beam gain of the UAV in the direction of ST e in time slot n is given by

$$P_e[n] = \mathbf{a}^H(\mathbf{q}[n],\mathbf{u}_e)\times \left(\sum_{k=1}^{K}\mathbf{w}_k[n]{\mathbf{w}_k}^H[n]+\sum_{j=1}^{J}\mathbf{v}_j[n]{\mathbf{v}_j}^H[n]\right)\mathbf{a}(\mathbf{q}[n],\mathbf{u}_e). \tag{6}$$

The sensing performance is quantified by the beam gain (6). The UAV's radar estimation rate for ST e (in bit/s/Hz) in time slot n is expressed as [35]

$$R_e^{rad}[n] = \alpha[n]\log_2\left(1+\frac{\rho^{rad}P_e[n]}{d_e^2[n]}\right), \tag{7}$$

where $\rho^{rad}=\frac{\vartheta_e\beta_0}{16\pi^2\sigma_e^2}$, ϑ_e is the radar cross-section of target e. Since the UAV channel changes slowly and the ground targets are stationary, we neglected Doppler interference. For high-speed ground targets, the Doppler frequency shift can be compensated by the existing signal processing methods. OTFS waveforms [37] have excellent performance in terms of suppressing Doppler effects by transforming the time frequency selective channel into a flat channel in the Doppler delay domain.

Interference can be suppressed through established radar signal processing techniques such as pulse compression and constant false alarm detection. It assumes that the UAV receives interference-free echoes, containing only signals reflected from the target [38].

Adopting the sensing-free communication approach from [39], the portion of the sensing signal can be removed at the receiver by employing the successive interference cancellation (SIC) technique.

(4) Information causality constraint: In practical systems, sensing precedes communication, and communication must depend on the information acquired during the sensing phase. To maintain information consistency, we set an upper bound that ensures the communication rate does not exceed the sensing capabilities of the system. The constraints on information causality are as follows:

$$R_k^{com} \leq \sum_{e=1}^{E} R_e^{rad}[n], \forall k. \tag{8}$$

The core logic of this constraint (8) is based on the information source dependency in the U-ISJC framework. In our system, the communication data of the UAV is derived entirely from the sensing results of ground targets. The communication process is essentially the transmission of sensing information, so the communication rate cannot exceed the information generation rate of the sensing module.

This constraint ensures that, under worst-case conditions, the communication rate for each CU is limited by the actual sensing capability, thus securing the communication. This design is a central feature of the ISJC framework and prevents eavesdroppers from exploiting higher communication rates to access more illicit information.

2.2. Problem Formulation

In this paper, we aim to maximize the total worst-case secure rate of the network by jointly optimizing the communication beamforming, jamming beamforming, sub-time slot allocation, and UAV trajectory. The optimization problem is formulated as follows:

$$\text{(P1)}: \max_{\mathbf{w}_k[n], \mathbf{v}_j[n], \alpha[n], \mathbf{q}[n]} \sum_{n=1}^{N} \sum_{k=1}^{K} R_k^{sec}[n] \tag{9a}$$

$$\text{s.t. } 0 \leq \alpha[n] \leq 1, \forall n, \tag{9b}$$

$$\frac{1}{N} \sum_{n=1}^{N} R_k^{com}[n] \geqslant R_{\min}^k, \forall k, \tag{9c}$$

$$R_k^{com} \leq \sum_{e=1}^{E} R_e^{rad}[n], \forall k, \tag{9d}$$

$$\sum_{k=1}^{K} \|\mathbf{w}_k[n]\|^2 + \sum_{j=1}^{J} \|\mathbf{v}_j[n]\|^2 \leqslant P_{max}, \forall n, \tag{9e}$$

$$P_e[n] \geq d_e^2[n] \Gamma_e, \forall n, \tag{9f}$$

$$||\mathbf{q}[n+1] - \mathbf{q}[n]|| \leq V_{\max} \delta_t, \forall n, \tag{9g}$$

$$\mathbf{q}[1] = \mathbf{q}_I, \mathbf{q}[N] = \mathbf{q}_F, \tag{9h}$$

where (9b) denotes the sub-time slot allocation factor; (9c) guarantees minimum communication quality $R_{\min}^k$ for CUs; (9d) represents the information causality constraint, which ensures that the communication bits do not exceed the radar estimation bits; (9e) limits the UAV transmit power, where P_{max} is the maximum transmit power; (9f) ensures that the sensing signal-to-noise ratio (SNR) for target e must exceed the threshold Γ_e; and (9g) and (9h) indicate the UAV mobility constraints, where V_{max} is the maximum speed, and $\mathbf{q}_I$ and $\mathbf{q}_F$ denote the UAV's initial and final location, respectively. Due to the non-convexity introduced by (9c), (9d), and the objective function, solving problem (P1) is extremely challenging.

3. Proposed Solution

In this section, we propose a joint optimization algorithm to solve problem (9). For notational convenience, let $\mathbf{H}_k[n] = \mathbf{h}_k[n]\mathbf{h}_k^H[n]$, $\mathbf{H}_j[n] = \mathbf{h}_j[n]\mathbf{h}_j^H[n]$, $\mathbf{W}_k[n] = \mathbf{w}_k[n]\mathbf{w}_k^H[n]$, $\mathbf{V}_j[n] = \mathbf{v}_j[n]\mathbf{v}_j^H[n]$, $\tilde{\mathbf{H}}_k[n] = \mathbf{a}_k[n]\mathbf{a}_k^H[n]$, $\tilde{\mathbf{H}}_j[n] = \mathbf{a}_j[n]\mathbf{a}_j^H[n]$, and $\tilde{\mathbf{H}}_s[n] = \mathbf{a}_s[n]\mathbf{a}_s^H[n]$, with $\mathbf{W}_k[n] \succeq 0$ and $\text{rank}(\mathbf{W}_k[n]) = 1, \forall k, n$. As a result, we obtain $\mathbf{Q}[n] = \sum_{k=1}^{K} \mathbf{W}_k[n] + \sum_{j=1}^{J} \mathbf{V}_j[n]$, and $P[n] = \text{Tr}(\mathbf{Q}[n]\tilde{\mathbf{H}}_s[n])$.

Theorem 1. *Problems (P1) and (P2) are equivalent.*

Proof of Theorem 1. To prove the equivalence of problems (P1) and (P2), we just need to prove the equation $r_k[n] = R_k[n]$ at the optimal solution. For discussion purposes, let $\hat{R}_k[n]$ denote the right-hand side of the inequality in (10b). If $\hat{R}_k[n] \leq \sum_{e=1}^{E} R_e^{rad}[n]$, this indicates that $r_k[n]$ is dominated by (10b). In this case, both the inequations in (10b) and (10h) have to hold with equations at the optimal solution of problem (10). Otherwise, the objective value can be further enlarged by increasing the value of $r_k[n]$ and/or decreasing the value of $s_k[n]$. If $\hat{R}_k[n] > \sum_{e=1}^{E} R_e^{rad}[n]$, this indicates that $r_k[n]$ is dominated by (10h). Thus, there is $r_k[n] = R_k[n]$ at the optimal solution. The proof is completed. □

By defining $\gamma_0 = \beta_0/\sigma^2$ and introducing slack variables $r_k[n]$, $s_k[n]$ and $\beta_k[n]$, and also defining the optimization variables as $\Xi_A = \{\mathbf{w}_k[n], \mathbf{v}_j[n]\}$, problem (P1) is converted into the following tractable form [16]:

$$\text{(P2)}: \max_{\Xi_A} \sum_{n=1}^{N} \sum_{k=1}^{K} (r_k^{com}[n] - \beta_k[n]) \tag{10a}$$

$$\text{s.t. (9b), (9f), (9g), (9h),}$$

$$r_k[n] \leq (1 - \alpha[n]) \times \log_2 \left(1 + \frac{\gamma_0 \text{Tr}(\tilde{\mathbf{H}}_k[n]\mathbf{W}_k[n])}{\gamma_0 \sum_{j \neq k} \text{Tr}(\tilde{\mathbf{H}}_k[n]\mathbf{W}_j[n]) + s_k[n]}\right), \tag{10b}$$

$$\frac{1}{N} \sum_{n=1}^{N} r_k^{com}[n] \geqslant R_{\min}^k, \forall k, \tag{10c}$$

$$\sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k[n]) + \sum_{j=1}^{J} \text{Tr}(\mathbf{V}_j[n]) \leq P_{\max}, \forall n, \tag{10d}$$

$$s_k[n] \geq \left\| \mathbf{q}[n] - \mathbf{u}_k \right\|^2 + q_z^2, \forall k, n, \tag{10e}$$

$$\mathbf{W}_k[n] \succeq 0, \forall k, n, \tag{10f}$$

$$\text{rank}(\mathbf{W}_k[n]) = 1, \forall k, n, \tag{10g}$$

$$r_k^{com}[n] \leq \sum_{e=1}^{E} R_e^{rad}[n], \forall k, n, \tag{10h}$$

$$\beta_k[n] \geq R_{j,k}^{com}[n], \forall k, j, n. \tag{10i}$$

However, problem (P2) remains a non-convex semi-definite programming (SDP) problem due to the non-convex constraints (10b), (10c), (10h), and (10i) and the rank-one constraint. To overcome the complex coupling of optimization variables, we decompose the original optimization problem into three independent subproblems.

3.1. Sub-Time Slot Allocation Optimization

For given UAV trajectory $\mathbf{q}[n]$ and beamforming vectors $\mathbf{w}_k[n]$ and $\mathbf{v}_j[n]$, we can rewrite the sub-time slot allocation optimization as follows:

$$\begin{aligned}(\text{SP1}): \max_{\alpha[n]} \ & \sum_{n=1}^{N}\sum_{k=1}^{K}(R_k^{com}[n]-\beta_k[n]) \\ \text{s.t.} \ & (9b),(9f),(9g),(9h),\end{aligned} \tag{11}$$

which is a standard linear problem (LP) that can be solved using CVX toolbox [40].

3.2. Beamforming Optimization

For given UAV trajectory $\mathbf{q}[n]$ and allocation factor $\alpha[n]$, we rewrite the beamforming optimization problem as follows:

$$\begin{aligned}(\text{SP2}): \max_{r_k[n],\mathbf{w}_k[n],\mathbf{v}_j[n]} \ & \sum_{n=1}^{N}\sum_{k=1}^{K}(r_k^{com}[n]-\beta_k[n]) \\ \text{s.t.} \ & (10b)\text{–}(10d),(10f)\text{–}(10i).\end{aligned} \tag{12}$$

Due to the non-convexity of (10b), (10c), (10h) and (10i), solving problem (SP2) is quite intractable. By introducing $\xi_k[n]=\gamma_0\sum_{j\neq k}\mathrm{Tr}(\tilde{\mathbf{H}}_k[n]\mathbf{W}_j[n])$ and $\ell_k[n]=\gamma_0\mathrm{Tr}(\tilde{\mathbf{H}}_k[n]\mathbf{W}_k[n])$, constraint (10b) is turned into the difference-of-convex (DC) form,

$$r_k[n]\leq(1-\alpha[n])(\hat{R}_{1k}[n]-\hat{R}_{2k}[n]), \tag{13}$$

where $\hat{R}_{1k}[n]=\log_2(\ell_k[n]+\xi_k[n]+s_k[n])$ and $\hat{R}_{2k}[n]=\log_2(\xi_k[n]+s_k[n])$. Since $\hat{R}_{2k}[n]$ is convex, we adopt the first-order Taylor expansion (FOTE) to obtain its upper-bound function at the given point $\xi_k^{(l)}[n]$, expressed by

$$\hat{R}_{2k}^{ub}[n]=\frac{\hat{R}_{2k}^{(l)}[n]+(\xi_k[n]-\xi_k^{(l)}[n])}{\ln 2(\xi_k^{(l)}[n]+s_k[n])}, \tag{14}$$

where $\hat{R}_{2k}^{(l)}[n]=\log_2(\xi_k^{(l)}[n]+s_k[n])$. (13) can be converted into

$$r_k[n]\leq(1-\alpha[n])(\hat{R}_{1k}[n]-\hat{R}_{2k}^{ub}[n])\triangleq\tilde{r}_k^{B}[n]. \tag{15}$$

Let $\xi_j[n]=\gamma_0(\sum_{i\neq k}\mathrm{Tr}(\tilde{\mathbf{H}}_j[n]\mathbf{W}_i[n])+\sum_s^S\mathrm{Tr}(\tilde{\mathbf{H}}_j[n]\mathbf{V}_s[n])+\mathrm{Tr}(\tilde{\mathbf{H}}_j[n]\mathbf{W}_k[n]))$, $\ell_j[n]=\gamma_0\mathrm{Tr}(\tilde{\mathbf{H}}_j[n]\mathbf{W}_k[n])$, $\xi_e[n]=\rho^{rad}P[n]$, and $R_{j,k}^{com}[n]$ and $R_e^{rad}[n]$ can be transformed as follows:

$$R_{j,k}^{com}[n]=(1-\alpha[n])(R_{1j}[n]-R_{2j}[n]), \tag{16}$$

$$R_e^{rad}[n]=\alpha[n](\log_2(\xi_e[n]+d_e[n])-R_{2e}[n]), \tag{17}$$

where $R_{1j}[n]=\log_2(\xi_j[n]+d_j[n])$, $R_{2j}[n]=\log_2(\xi_j[n]-\ell_j[n]+d_j[n])$, $R_{1e}[n]=\log_2(\xi_e[n]+d_e[n]^2)$ and $R_{2e}[n]=\log_2(d_e[n]^2)$. Since the first part of the right-hand side in (16) and (17) is convex, we adopt the FOTE to obtain its lower-bound function at the given point $\xi_j^{(l)}[n]$, $\xi_e^{(l)}[n]$, expressed by

$$R_{1j}^{lb}[n]=\frac{R_{1j}^{(l)}[n]+(\xi_j[n]-\xi_j^{(l)}[n])}{\ln 2(\xi_j^{(l)}[n]+d_j[n])}, \tag{18}$$

$$R_{1e}^{lb}[n]=\frac{R_{1e}^{(l)}[n]+(\xi_e[n]-\xi_e^{(l)}[n])}{\ln 2(\xi_e^{(l)}[n]+d_e[n])}, \tag{19}$$

where $R_{1j}^{(l)}[n] = \log_2(\xi_j^{(l)}[n] + d_j[n])$ and $R_{1e}^{(l)}[n] = \log_2(\xi_e^{(l)}[n] + d_e[n])$. Thus, $\tilde{R}_{j,k}^{com}[n]$ and $\tilde{R}_s^{rad}[n]$ can be obtained to replace $R_{j,k}^{com}[n]$ and $R_e^{rad}[n]$ in problem (12) as follows:

$$\tilde{R}_{j,k}^{com}[n] = (1 - \alpha[n])(R_{1j}^{lb}[n] - R_{2j}[n]), \tag{20}$$

$$\tilde{R}_e^{rad}[n] = \alpha[n](R_{1e}^{lb}[n] - R_{2e}[n]). \tag{21}$$

Thus, by defining the optimization variables set $\Xi_B = \{\tilde{r}_k^B[n], \tilde{R}_{j,k}^{com}[n], \tilde{R}_s^{rad}[n], \mathbf{w}_k[n], \mathbf{v}_j[n], \xi_k[n], \xi_j[n], \xi_e[n], \ell_j[n]\}$, problem (SP2) is reformulated as

$$\text{(SP2-1)}: \max_{\Xi_B} \sum_{n=1}^{N} \sum_{k=1}^{K} (\tilde{r}_k^B[n] - \beta_k[n]) \tag{22a}$$

$$\text{s.t. (10d), (10f), (15),}$$

$$\frac{1}{N} \sum_{n=1}^{N} \tilde{r}_k^B[n] \geqslant R_{\min}^k, \forall k, \tag{22b}$$

$$\tilde{r}_k^B[n] \leq \sum_{e=1}^{E} \tilde{R}_e^{rad}[n], \forall k, n, \tag{22c}$$

$$\beta_k[n] \geq \tilde{R}_{j,k}^{com}[n], \forall k, j, n. \tag{22d}$$

Considering the rank-one constraint is intractable to handle in practice, we neglect the rank-one constraint of the problem. Then, the CVX solver can be employed to effectively solve this semi-definite relaxation (SDR) problem. In order to ensure that the obtained results satisfy the rank-one constraint, we employ a beam pre-inspection method similar to that in [16] prior to performing Gaussian randomization to resolve the rank-one problem and reduce the algorithmic complexity.

3.3. UAV Trajectory Optimization

For given allocation factor $\alpha[n]$ and beamforming vectors $\mathbf{w}_k[n]$ and $\mathbf{v}_j[n]$, we can rewrite the UAV trajectory optimization problem as follows:

$$\begin{aligned} \text{(SP3)}: &\max_{r_k[n], \beta_k[n], \mathbf{q}[n]} (r_k^{com}[n] - \beta_k[n]) \\ &\text{s.t. (9f)–(9h), (10b), (10c), (10e), (10h), (10i).} \end{aligned} \tag{23}$$

Due to the non-convexity of (10b), (10c), (10h) and (10i), solving problem (SP3) owing DC form (13). We regain the upper bound on the second part of the right-hand side of of the inequality in (13).

$$\log_2(\xi_k[n] + s_k[n]) \leq \hat{R}_{2k}^{\prime(l)}[n] + \frac{s_k[n] - s_k^{(l)}[n]}{\ln 2(\xi_k[n] + s_k^{(l)}[n])}, \tag{24}$$

where $\hat{R}_{2k}^{\prime(l)}[n] = \log_2(\xi_k[n] + s_k^{(l)}[n])$.

Then, we obtain

$$\begin{aligned} &r_k[n] \leq (1 - \alpha[n]) \\ &\left(\hat{R}_{1k}[n] - \hat{R}_{2k}^{(l)}[n] - \frac{s_k[n] - s_k^{(l)}[n]}{\ln 2(\xi_k[n] + s_k^{(l)}[n])} \right) \triangleq \tilde{r}_k^C[n]. \end{aligned} \tag{25}$$

We perform SCA on $\hat{R}_k[n]$ to address its non-convexity. To this end, we introduce slack variable $s_k[n]$, satisfying

$$\bar{s}_k[n] \leq \left\|\mathbf{q}[n] - \mathbf{u}_k\right\|^2 + q_z^2. \tag{26}$$

By applying the Taylor formula, we can obtain the lower bound of $\|\mathbf{q}[n] - \mathbf{u}_k\|^2$ in (26) as

$$\begin{aligned} &\|\mathbf{q}[n] - \mathbf{u}_k\|^2 \geq \left\|\mathbf{q}^{(l)}[n] - \mathbf{u}_k\right\|^2 + \\ &2(\mathbf{q}^{(l)}[n] - \mathbf{u}_k)^{\dagger}(\mathbf{q}[n] - \mathbf{u}_k) \triangleq \|\mathbf{q}[n] - \mathbf{u}_k\|_{lb}^2. \end{aligned} \tag{27}$$

Hence, we define $\overline{R}_k[n]$ as the lower bound of $\hat{R}_k[n]$, i.e.,

$$\overline{R}_k[n] \geq (1 - \alpha[n])(\overline{R}_{1k}^{ub}[n] - \overline{R}_{2k}[n]) \triangleq \bar{r}_k[n], \tag{28}$$

where $\overline{R}_{1k}^{ub}[n]$ is the upper-bound function for the first term in $\overline{R}_k[n]$, obtained by performing FOTE at the lth iteration for a given point $\bar{s}_k^{(l)}[n]$. Specifically, $\overline{R}_{1k}^{ub}[n]$ is defined as

$$\overline{R}_{1k}^{ub}[n] = \overline{R}_{1k}^{(l)}[n] + \frac{\bar{s}_k[n] - \bar{s}_k^{(l)}[n]}{\ln 2(\ell_k[n] + \xi_k[n] + \bar{s}_k^{(l)}[n])}, \tag{29}$$

where $\overline{R}_{1k}^{(l)}[n] = \log_2(\ell_k[n] + \xi_k[n] + \bar{s}_k^{(l)}[n])$.

Similarly, we can obtain the lower-bound function for the first term in (16) $R_{1j}^{'lb}[n]$ for a given point $d_j^{(l)}[n]$, defined as

$$R_{1j}^{'lb}[n] = \log_2(\xi_j[n] + d_j^{(l)}[n]) + \frac{d_j[n] - d_j^{'(l)}[n]}{\ln 2(\xi_j[n] + d_j^{'(l)}[n])}. \tag{30}$$

Thus, $\overline{R}_{j,k}^{com}$ can be obtained to replace $R_{j,k}^{com}$ in the original problem, i.e., $\overline{R}_{j,k}^{com}[n] = (1 - \alpha[n])(R_{1j}^{'lb}[n] - R_{2j}[n])$. We also can obtain the upper bound of $R_{2e}[n]$ in (17), for a given point $d_e^{(l)}[n]$, which is defined as

$$R_{2e}^{ub}[n] = 2\log_2(d_e^{(l)}[n]) + \frac{d_e[n]^2 - d_e^{(l)}[n]^2}{2\ln 2(d_e^{(l)}[n])}. \tag{31}$$

Define $\overline{R}_e^{rad}[n] = \alpha[n](R_{1e}[n] - R_{2e}^{ub}[n])$. Thus, let set $\Xi_C = \{\tilde{r}_k^C[n], \bar{r}_k[n], \overline{R}_{j,k}^{com}[n], \overline{R}_e^{rad}[n], \mathbf{q}[n], s_k[n], \bar{s}_k[n]\}$, so that problem (SP3) is reformulated as

$$\text{(SP3-1)}: \max_{\Xi_C} (\tilde{r}_k^C[n] - \beta_k[n]) \tag{32a}$$

$$\text{s.t. } (9f)\text{–}(9h), (10e),$$

$$\frac{1}{N}\sum_{n=1}^{N} \tilde{r}_k^C[n] \geqslant R_{\min}^k, \forall k, \tag{32b}$$

$$\bar{r}_k[n] \leq \sum_{e=1}^{E} \overline{R}_e^{rad}[n], \forall k, n, \tag{32c}$$

$$\beta_k[n] \geq \overline{R}_{j,k}^{com}[n], \forall k, j, n, \tag{32d}$$

$$\bar{s}_k[n] \leq \|\mathbf{q}[n] - \mathbf{u}_k\|_{lb}^2, \forall k, n. \tag{32e}$$

The CVX can be employed to effectively solve this subproblem. The alternating optimization algorithm to solve the primal problem (P1) is summarized in Algorithm 1.

Algorithm 1 Alternating optimization algorithm.

1: Initialize $\alpha^{(l)}[n]$, $\mathbf{w}_k^{(l)}[n]$, $\mathbf{v}_j^{(l)}[n]$ and $\mathbf{q}^{(l)}[n]$; set the iteration index $l = 0$ and the maximum number of iterations I_{max}; set accuracy ε;
2: **repeat**
3: Solve (SP1) with $\alpha^{(l)}[n]$ and $\mathbf{q}^{(l)}[n]$, and obtain $\mathbf{w}_k^{(l+1)}[n]$, $\mathbf{v}_j^{(l+1)}[n]$;
4: Solve (SP2-1) with $\alpha^{(l)}[n]$, $\mathbf{w}_k^{(l+1)}[n]$ and $\mathbf{v}_j^{(l+1)}[n]$, and obtain $\mathbf{q}^{(l+1)}[n]$;
5: Solve (SP3-1) with $\mathbf{w}_k^{(l+1)}[n]$, $\mathbf{v}_j^{(l+1)}[n]$ and $\mathbf{q}^{(l+1)}[n]$, and obtain $\alpha^{(l+1)}[n]$;
6: $l = l + 1$;
7: **until** the objective value converges within a specified threshold ε or the maximum number of iterations reaches.

3.4. Overall Algorithm and Analysis

The proposed algorithm is developed within the BCD framework, where the original optimization problem is decomposed into three independent subproblems corresponding to sub-time slot allocation, beamforming design, and UAV trajectory optimization. As a result, the overall computational complexity is determined by the cumulative complexity of these subproblems. Specifically, the sub-time slot allocation subproblem is formulated as a standard LP problem with variable dimension N, whose objective function depends on the number of communication users K, and sensing targets E; thus, when solved via an interior point method, its computational complexity is on the order of $\mathcal{O}(N(K+E))$. The beamforming optimization subproblem is addressed using SDR, leading to a semi-definite programming (SDP) formulation in which the variable dimension scales with the square of the number of antennas, i.e., M^2. Taking into account the number of users K and eavesdroppers J, and following classical SDP complexity analysis, the computational complexity of this subproblem is given by $\mathcal{O}(M^{3.5}(K+J)^2)$ [22]. In addition, the UAV trajectory optimization subproblem is a convex optimization problem involving the UAV position variables over N time slots, whose complexity using interior point methods scales as $\mathcal{O}(N^2)$. The overall algorithm adopts an alternating iterative procedure and converges within L iterations; therefore, the total computational complexity of the proposed algorithm can be expressed as $\mathcal{O}L(N(K+E) + M^{3.5}(K+J)^2 + N^2)$.

4. Numerical Results

In this section, we present simulation results to demonstrate the performance of the proposed algorithm. The specific notation meanings and parameter values are shown in Table 2. In this chapter, we analyze the simulation results, specifically discussing the impact of sub-time slot allocation factors, beamforming, and UAV trajectories on the worst-case secure communication rate. Additionally, we analyze the effects of real-time changes in UAV flight speed, variations in the number of Eves, and alterations in UAV altitude on the system's security performance.

Figure 3 compares the algorithmic iterative convergence performance and the converged secure rates of four different schemes. Both the static and straight flight (SF) schemes perform sub-time slot allocation factor and beamforming optimization, with the UAV trajectories in the stationary and straight flight states, respectively. Traveler scheme (TSP) refers to the UAV maintaining straight-line flight from the starting point $\mathbf{q}_I$ to the destination $\mathbf{q}_F$, with each CU fixed as an intermediate flight node. Consistent with the static scheme and SF scheme, it simultaneously performs sub-time slot allocation factor and beamforming optimization. The waveform and trajectory only (OnlyW&T) scheme fixes the sub-time slot allocation factor as $\alpha[n] = 0.5$, optimizing only the beamforming and trajectory. Based on the proposed algorithm, all four schemes converge around four iterations, demonstrating

the excellent convergence performance of the proposed algorithm. In terms of the secure rate after final convergence, the proposed scheme achieves a higher secure rate than the SF, static, and OnlyW&T schemes.

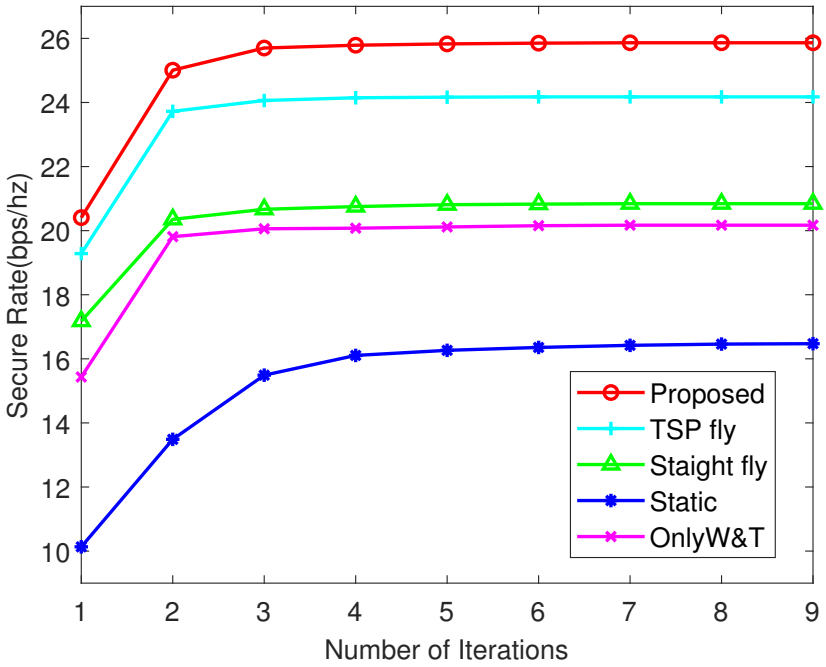

Figure 3. Convergence of the proposed algorithm.

Notably, although all schemes adopt beamforming optimization, the SF scheme outperforms the scheme without sub-time slot allocation factor optimization (i.e., OnlyW&T), indicating that optimizing the allocation factor can effectively improve system performance. When simultaneously optimizing sub-slot allocation factors, incorporating UAV trajectory optimization (i.e., the proposed scheme) significantly enhances the security rate compared to the SF scheme and partially improves it relative to the TSP scheme. Since the TSP scheme prioritizes CU proximity as its sole objective while disregarding eavesdropping links, it not only compromises perception quality but also partially reduces the security rate compared to the proposed scheme. The simulation results show that optimizing both the allocation factor and UAV trajectory under the premise of beamforming optimization can significantly enhance system performance. The proposed scheme achieves the maximum worst-case secure rate compared with other baseline schemes, verifying the superiority of the proposed scheme.

Figure 4 presents the trajectory optimization results and transmit beampatterns achieved by the proposed algorithm at different time slots. It should be noted that the UAV moves from the upper right corner to the lower left corner of the map, where $N = 6$ and $N = 42$ represent the positions of the UAV at the 6th and 42nd time slots in the optimized trajectory, respectively. Notably, compared with the initial SF trajectory, the optimized trajectory of the UAV tends to approach the CUs and STs while moving away from the Eves to maximize the worst-case communication secure rate. For instance, under the premise of satisfying the minimum communication and sensing threshold constraints, the UAV maintains a relatively safe distance from Eve 1 to avoid interference, while approaching CU 2 as closely as possible for secure communication, and consistently moves toward the CUs and STs during flight.

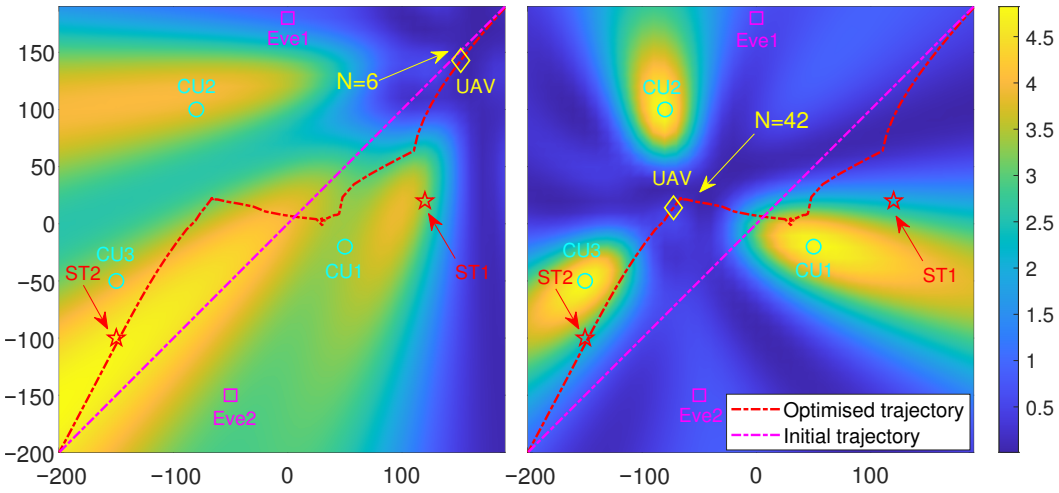

Figure 4. Beampattern at $N = 6$ and $N = 42$.

Regarding the beam focusing results, when the UAV starts to move (i.e., $N = 6$), the beampattern exhibits a wide-range focusing trend to meet the sensing threshold constraint of ST 2 and avoid interference from Eve 2 on the basis of focusing on the CUs. When the UAV moves to the middle position (i.e., $N = 42$), all communication and sensing constraints are satisfied, enabling the beam to focus more effectively on each CU. The discussion of simulation results reveals that the trajectory changes of the UAV generally follow this trend: while ensuring basic communication quality, it strives to approach ST to enhance perception quality and moves away from Eve to reduce eavesdropping link gain, aiming to maximize secure communication rate. The beam direction generally remains focused on CU and ST to maintain the fundamental power allocation for the ISAC primary task. Naturally, when the beam coverage includes the eavesdropper, information leakage is significantly reduced due to the presence of the interference beam. This is illustrated by the OnlyW&T scheme in Figure 3. Combining the two optimization results, it can be observed that the beam is dynamically adjusted as the UAV position changes continuously, which verifies the effectiveness of the proposed algorithm in trajectory optimization and beam design.

Figure 5 investigates the impact of different UAV antenna transmit powers on the total worst-case secure rates under various optimized schemes. It can be observed that as the antenna transmit power increases, the total worst-case secure rates of all schemes improve, indicating a positive correlation between the secure rate and antenna transmit power.

In addition, with the increase in antenna transmit power, the gap in secure rates between the static scheme and other flight schemes gradually narrows. This demonstrates that under the sub-time slot design conditions proposed in this paper, a good secure communication rate can be guaranteed even when the UAV is stationary, provided that sufficient power is supplied. Meanwhile, the proposed scheme consistently achieves a higher secure rate compared with the other four schemes, which further verifies that the proposed scheme maintains superior performance across different antenna transmit powers.

Figure 6 illustrates the real-time velocity variations of the UAV in the optimization results of the proposed scheme. It can be observed that the UAV's velocity is consistently constrained within the maximum speed limit of 30 m/s. Specifically, when the UAV initially departs, it is far from the CUs and close to the Eves, thus requiring full-speed operation to rapidly establish secure communication. The same velocity logic applies when approaching the destination. During the process of approaching the CUs and STs, the velocity continuously decreases. Meanwhile, due to the presence of multiple Eves in the

scenario, there are instances where the velocity increases to move away from the Eves. Once a sufficient safe distance from the Eves is achieved, the UAV reduces its velocity again to communicate with the CUs and sense the STs. Evidently, the optimized UAV velocity decreases when approaching the CUs and STs or moving away from the Eves, and increases when departing from the CUs and STs or approaching the Eves. This not only increases the time allocated to serving CUs and sensing STs but also reduces the time spent within the proximity of Eves. Consequently, the proposed flight plan can effectively improve the total worst-case secure rate between the UAV and the CUs.

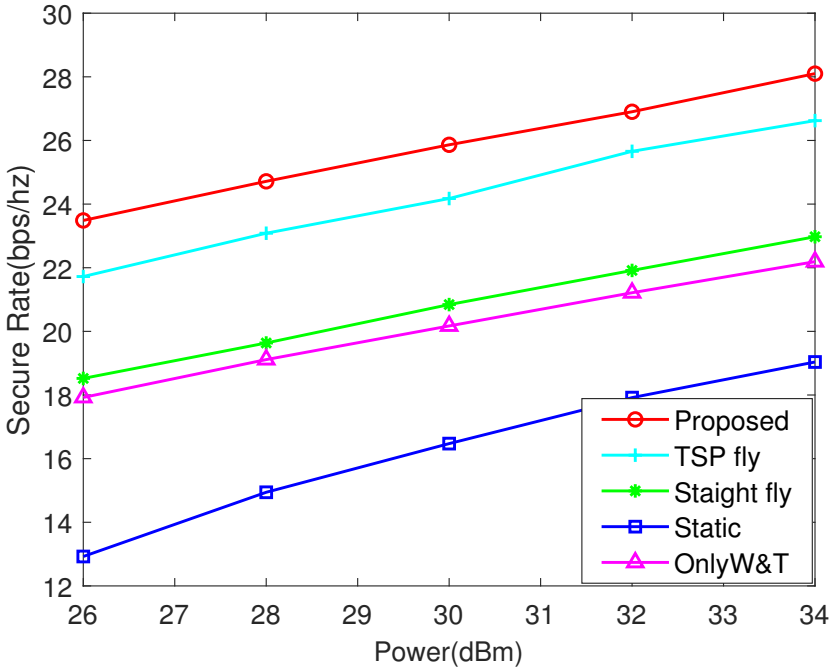

Figure 5. Comparison of secure rates with different transmit power.

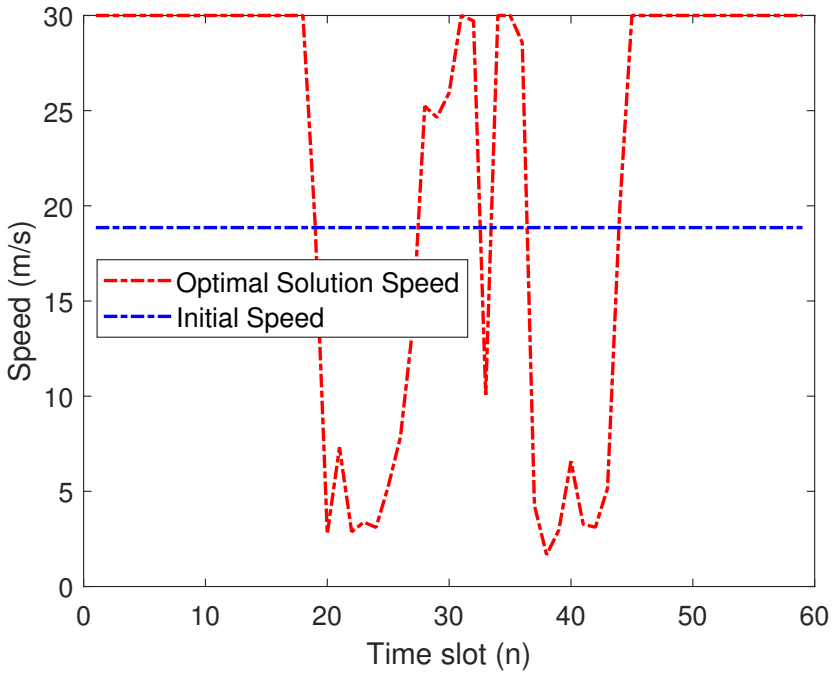

Figure 6. Speed of UAV.

Figure 7 presents the optimization results of the sub-time slot allocation factor in the proposed scheme. In conjunction with the trajectory optimization shown in Figure 4, it can be observed that, during the initial flight phase of the UAV, the sensing allocation factor maintains a relatively high value due to the prioritized requirement for sensing the STs. After satisfying the sensing threshold constraints, the proportion of resources allocated to sensing is gradually reduced to increase the communication–resource allocation ratio, aiming to establish reliable communication with the CUs. Once the UAV enters a stable flight region, the allocation ratio between sensing and communication remains basically stable with only slight fluctuations. Notably, the dynamic variation of the sub-time slot allocation factor exhibits strong correlation with the UAV's trajectory and target presence in the scene.

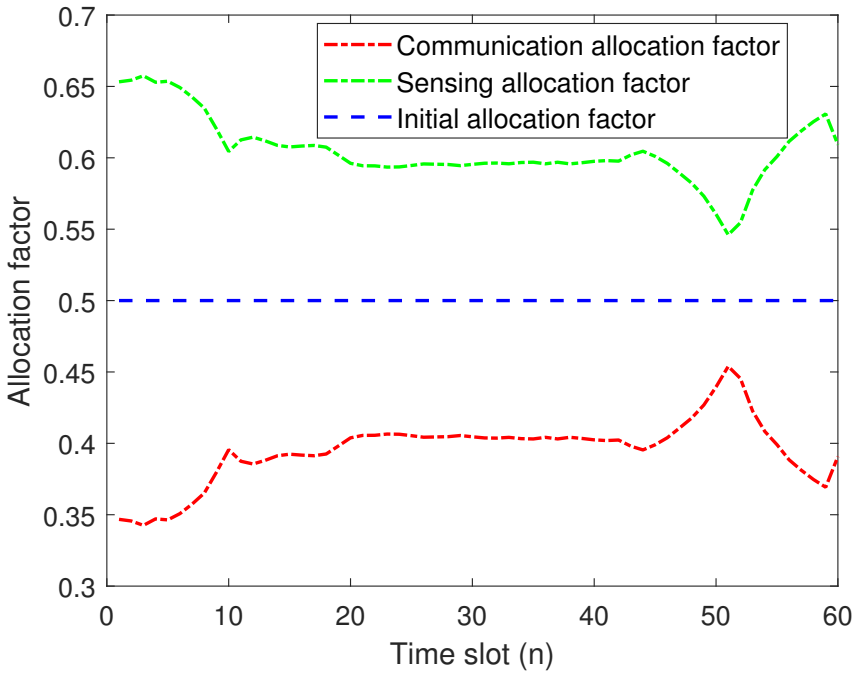

Figure 7. Allocation factor of UAV.

Specifically, as the UAV gradually approaches the vicinity of ST 2 and CU 3 (i.e., $N = 52$), its distance to ST 2 decreases while simultaneously reducing its distance to Eve 2. Consequently, the communication allocation factor gradually increases while the perception allocation factor gradually decreases, ensuring a higher secure communication rate. As the UAV moves away from this area, the demand for sensing gradually increases, leading to a slow upward trend in the sensing allocation factor. Thus, it can be concluded that the dynamic variation of the sub-time slot allocation factor exhibits a tendency to converge toward enhancing the overall worst-case safety rate.

Figure 8 compares the total worst-case secure rates under different numbers of Eves and UAV altitudes. It should be noted that "No jammer, q_z = 100 m" denotes the scenario where the proposed algorithm only removes the jamming beam, with two Eves present and the UAV operating at an altitude of 100 m. "Three Eves, q_z = 100 m" represents the scenario where the proposed algorithm includes the jamming beam, with three Eves present and the UAV flying at an altitude of 100 m, and other cases follow this analogy. It can be observed that both the increase in the number of Eves and the UAV altitude lead to decreases in the secure rate, but the impact of altitude variation is not significant. When the number of Eves exceeds two, due to the small scenario area, the increase in the number of Eves leads to a corresponding increase in eavesdropping density. Thus, constrained by the scenario, the magnitude of the secure rate decrease slightly intensifies. In addition, compared with

the no jammer scenario, the proposed algorithm significantly improves the secure rate in the presence of Eves by adding the jamming beam, which verifies the effectiveness of the jamming beam in enhancing the worst-case secure rate.

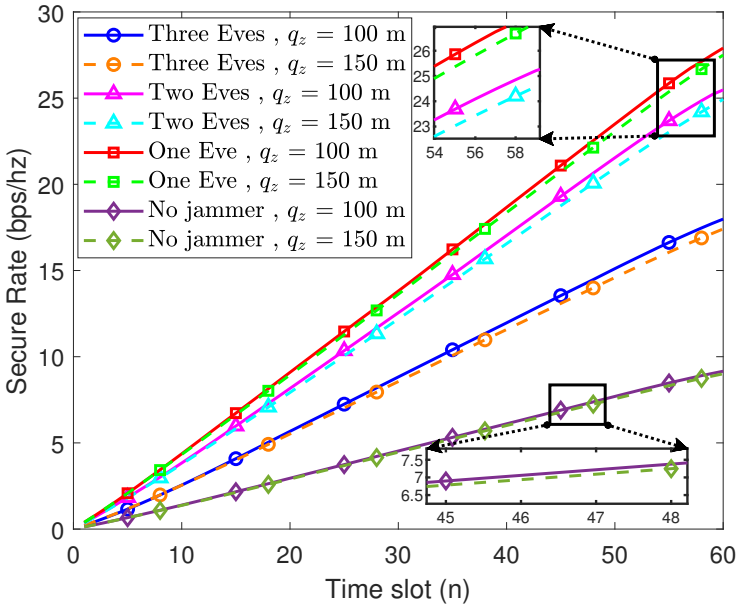

Figure 8. Comparison of total worst-case secure rate under different scenarios.

5. Conclusions

This paper investigated a novel U-ISJC framework that incorporates sub-time slot frame structure design and optimization, aiming to ensure both a secure communication environment and efficient resource utilization. The framework provides a fundamental approach for beamformers and UAV trajectory in U-ISJC framework. In order to maximize the secure rate, we proposed a joint optimization problem for sub-time slot allocation, beamforming and UAV trajectory. The numerical results validated the stable convergence of the proposed algorithm. The simulation results showed that the proposed scheme significantly improved the secure communication performance. This paper's simulation assumptions are conducted under ideal conditions. Future work may extend this approach to complex scenarios involving multipath interference, noise, and self-interference. Additionally, designing an energy-efficient ISJC that incorporates energy efficiency as an optimization objective presents a challenging research direction, particularly due to the introduction of new fractional non-convex structures.

Author Contributions: Conceptualization, L.S. and C.Y.; methodology, L.S. and Y.X.; validation, D.Y. and F.W.; investigation, C.Y. and H.L.; writing—original draft, L.S. and D.Y.; writing—review and editing, L.S. and C.Y.; and visualization, L.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant 62401241, Grant 62461040, and Grant 62261035, and partly by the Joint Funds of the Jiangxi Provincial Natural Science Foundation of China under Grant No 20244BAB28002, and partly by the Key Research and Development Project of Jiangxi Province under Grant No 20252BCE310050.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: Author Chuansheng Yan was employed by the company China Mobile (Jiangxi) Virtual Reality Technology Co., Ltd. The remaining authors declare that the research was conducted

in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

UAV	Unmanned aerial vehicle
6G	Six generation
ISJC	Integrated sensing, communication, and jamming
ISAC	Integrated sensing and communication
IRS	Intelligent reflecting surface
CCCP	Concave–convex procedure
SDR	Semi-definite relaxation
UPA	Uniform planar array
BCD	Block coordinate descent
LOS	Line of sight
CU	Communication user
Eve	Eavesdropper
ST	Sensing target
LP	Linear problem
DC	Difference-of-convex
FOTE	First-order Taylor expansion
SF	Straight Flight
OnlyW&T	Waveform and trajectory only

References

1. Liu, F.; Cui, Y.; Masouros, C.; Xu, J.; Han, T.X.; Eldar, Y.C.; Buzzi, S. Integrated sensing and communications: Toward dual functional wireless networks for 6G and beyond. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1728–1767. [CrossRef]
2. Zhang, J.A.; Dong, M.; Zhou, X.; Guo, H.; Zhang, J.; Ottersten, B.; Poor, H.V. An overview of signal processing techniques for joint communication and radar sensing. *IEEE J. Sel. Top. Signal Process.* **2021**, *15*, 1295–1315. [CrossRef]
3. Wu, Q.; Ding, G.; Wang, J.; Yao, Y.-D. Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: Two-dimensional sensing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 516–526. [CrossRef]
4. Li, B.; Petropulu, A.P.; Trappe, W. Optimum co-design for spectrum sharing between matrix completion based MIMO radars and a MIMO communication system. *IEEE Trans. Signal Process.* **2016**, *64*, 4562–4575. [CrossRef]
5. Hassanien, A.; Amin, M.G.; Zhang, Y.D.; Ahmad, F. Dual-function radar communication systems: A solution to the spectrum congestion problem. *IEEE Signal Process. Mag.* **2019**, *36*, 115–126. [CrossRef]
6. Kaushik, A.; Markakis, E.; Neokosmidis, I.; Chrysikos, T.; Anastasopoulou, M.P.; Trakadas, P.; Fernández-Caramés, T.M.; Monteiro, P.P. Integrated Sensing and Communications for IoT: Synergies with Key 6G Technology Enablers. *IEEE Internet Things Mag.* **2024**, *7*, 136–143. [CrossRef]
7. Demirhan, U.; Alkhateeb, A. Integrated Sensing and Communication for 6G: Ten Key Machine Learning Roles. *IEEE Commun. Mag.* **2023**, *61*, 113–119. [CrossRef]
8. Meng, K.; Wu, Q.; Chen, W.; Li, D.; Li, J.; Al-Dhahir, N.; Hanzo, L. UAV-Enabled Integrated Sensing and Communication: Opportunities and Challenges. *IEEE Wirel. Commun.* **2024**, *31*, 97–104. [CrossRef]
9. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1123–1152. [CrossRef]
10. Sun, X.; Ng, D.W.K.; Ding, Z.; Xu, Y.; Zhong, Z. Physical Layer Security in UAV Systems: Challenges and Opportunities. *IEEE Wirel. Commun.* **2019**, *26*, 40–47. [CrossRef]
11. Yang, Z.; Li, D.; Zhao, N.; Wu, Z.; Li, Y.; Niyato, D. Secure Precoding Optimization for NOMA-Aided Integrated Sensing and Communication. *IEEE Trans. Commun.* **2022**, *70*, 8370–8382. [CrossRef]
12. Chu, J.; Lu, Z.; Liu, R.; Li, M.; Liu, Q. Joint Beamforming and Reflection Design for Secure RIS-ISAC Systems. *lEEE Trans. Veh. Technol.* **2024**, *73*, 4471–4475. [CrossRef]
13. Yang, W.; Liu, X.; Liu, Z. Joint Trajectory and Resource Allocation Optimization for Mobile Vehicles in UAV Assisted Secure ISAC System. In *Proceedings of the 2024 IEEE 24th International Conference on Communication Technology (ICCT)*; IEEE: New York, NJ, USA, 2024; pp. 321–325.

14. Niu, H.; Xiao, Y.; Lei, X.; Chen, J.; Xiao, Z.; Li, M.; Yuen, C. A survey on artificial noise for physical layer security: Opportunities, technologies, guidelines, advances, and trends. *IEEE Commun. Surv. Tutor.* **2025**, *28*, 341–381. [CrossRef]
15. Shu, Y.; Qi, C.; Mao, S. Joint Transmit Waveform and Receive Filter Design for ISAC System With Jamming. *IEEE Trans. Veh. Technol.* **2025**, *74*, 13278–13283. [CrossRef]
16. Xu, Y.; Zhu, Y.; Han, K.; Zhu, Y.; Xiao, Z.; Xia, X.G. UAV-enabled integrated sensing, computing, and communication: A fundamental trade-off. *IEEE Wirel. Commun.* **2023**, *12*, 843–847. [CrossRef]
17. Zhang, R.; Zhang, Y.; Tang, R.; Zhao, H.; Xiao, Q.; Wang, C. A Joint UAV Trajectory, User Association, and Beamforming Design Strategy for Multi-UAV-Assisted ISAC Systems. *IEEE Internet Things* **2024**, *11*, 29360–29374. [CrossRef]
18. Van Veen, B.D.; Buckley, K.M. Beamforming: A versatile approach to spatial filtering. *IEEE ASSP Mag.* **1988**, *5*, 4–24. [CrossRef] [PubMed]
19. Wang, W.; Liu, X.; Liu, Z. Joint Beamforming and Trajectory Design for Multi-Antenna UAV-Enabled ISAC. *lEEE Trans. Veh. Technol.* **2025**, *75*, 3283–3287. [CrossRef]
20. Xiao, Z.; Zhu, L.; Xia, X.-G. UAV communications with millimeter-wave beamforming: Potentials, scenarios, and challenges. *China Commun.* **2020**, *17*, 147–166. [CrossRef]
21. Zhang, X.; Peng, M.; Liu, C. Sensing-Assisted Beamforming and Trajectory Design for UAV-Enabled Networks. *lEEE Trans. Veh. Technol.* **2024**, *73*, 3804–3819. [CrossRef]
22. Meng, K.; Liu, F.; Masouros, C.; Eldar, Y.C.; Nallanathan, A.; Hanzo, L. Throughput maximization for UAV-enabled integrated periodic sensing and communication. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 671–687. [CrossRef]
23. Zhang, H.; Sun, J.; Wang, X.; Gong, C. Achieving Physical Layer Security Against Location Unknown Eavesdroppers via Friendly Jammer. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 2038–2040. [CrossRef]
24. Wang, W.; Zhao, N.; Gao, H.; Gui, G.; Wang, G.; Niyato, D.; Adachi, F. Energy-Constrained UAV-Assisted Secure Communications With Position Optimization and Cooperative Jamming. *IEEE Trans. Commun.* **2020**, *68*, 4476–4489. [CrossRef]
25. Pandey, G.K.; Gurjar, D.S.; Yadav, S.; Prasad, G.; Gazda, J. Resource Allocation and Robust Trajectory Design for Dual UAV-Assisted Secure Communications. *lEEE Trans. Veh. Technol.* **2025**. [CrossRef]
26. Meng, X.; Wu, X.; Xie, Z.; Zhang, T.; Xu, T. Secure Resource Allocation and Trajectory Design for UAV-Assisted IoT With Double Cluster Head. *IEEE Trans. Green Commun. Netw.* **2024**, *8*, 1661–1675. [CrossRef]
27. Dong, R.; Wang, B.; Cao, K. Security enhancement of UAV swarm enabled relaying systems with joint beamforming and resource allocation. *China Commun.* **2021**, *18*, 71–87. [CrossRef]
28. Wu, J.; Yuan, W.; Hanzo, L. When UAVs meet ISAC: Real-time trajectory design for secure communications. *lEEE Trans. Veh. Technol.* **2023**, *72*, 16766–16771. [CrossRef]
29. Yao, J.; Yang, Z.; Yang, Z.; Xu, J.; Quek, T.Q.S. UAV-Enabled Secure ISAC Against Dual Eavesdropping Threats: Joint Beamforming and Trajectory Design. *IEEE Wirel. Commun.* **2025**, *14*, 3199–3203. [CrossRef]
30. Yang, Z. Enhanced Security-Aware Beamforming and Trajectory Design for UAV-Assisted Integrated Sensing and Communication. In *Proceedings of the 2025 5th International Conference on Sensors and Information Technology, Nanjing, China, 21–23 March 2025*; IEEE: New York, NJ, USA, 2025; pp. 710–714.
31. Dai, C.; Wang, Y.; Wu, T.; Gu, X.; Cao, H.; Sun, G. Robust Multi-Agent Reinforcement Learning for Physical Layer Security Communication in RIS-Assisted UAV-Enabled ISAC Networks. *IEEE Trans. Netw. Sci. Eng.* **2025**, *13*, 4969–4984. [CrossRef]
32. Xu, J.; Zhu, Y.; Ng, D.W.K.; Al-Dhahir, N.; Schober, R. IRS-UAV Assisted Secure Integrated Sensing and Communication. *IEEE Wirel. Commun.* **2024**, *31*, 61–67. [CrossRef]
33. Zhao, B.; Qiu, T.; Ge, Y. RSMA-Enhanced Secure Precoding for ISAC Systems with Both Active and Passive Eavesdroppers. *Comput. Netw.* **2025**, *275*, 111952. [CrossRef]
34. Liu, Y.; Xu, J.; Xiong, Z.; Kang, J.; Niyato, D.; Huang, C. Secure rate maximization for ISAC-UAV assisted communication amidst multiple eavesdroppers. *IEEE Trans. Veh. Technol.* **2024**, *73*, 15843–15847. [CrossRef]
35. Wei, Z.; Liu, F.; Ng, D.W.K.; Schober, R. Safeguarding UAV networks through integrated sensing, jamming, and communications. In *Proceedings of the ICASSP 2022—2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, 22–27 May 2022*; IEEE: New York, NJ, USA, 2022; pp. 8737–8741.
36. Wei, Z.; Liu, F.; Liu, C.; Yang, Z.; Ng, D.W.K.; Schober, R. Integrated sensing, navigation, and communication for secure UAV networks with a mobile eavesdropper. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 7060–7078. [CrossRef]
37. Kumar, A.S.; Shekhar, S.; Muthukrishnan, G.; Srinivasan, M.; Kalyani, S. Integrating OTFS in Airplane-Aided Next-Generation Networking. *arXiv* **2026**, arXiv:2601.15166.
38. Khalili, A.; Rezaei, A.; Xu, D.; Schober, R. Energy-Aware Resource Allocation and Trajectory Design for UAV-Enabled ISAC. In *Proceedings of the IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 4–8 December 2023*; IEEE: New York, NJ, USA, 2023; pp. 4193–4198.

39. An, J.; Li, H.; Ng, D.W.K.; Yuen, C. Fundamental Detection Probability vs. Achievable Rate Tradeoff in Integrated Sensing and Communication Systems. *IEEE Wirel. Commun.* **2023**, *22*, 9835–9853. [CrossRef]
40. CVX Research, Inc. CVX: Matlab Software for Disciplined Convex Programming. Available online: https://cvxr.com/cvx (accessed on 15 April 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.