electronics

MDPI

Article

A Robust Scheme for RIS-Assisted UAV Secure Communication in IoT

Pengzhi Qian [1], Yu Zhang [1], Xiaojuan Yan [2], Yong Chen [1,3,*] and Yifu Sun [1]

[1] The Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China; qianpengzhi16@nudt.edu.cn (P.Q.); zhyu63@nudt.edu.cn (Y.Z.); sunyifu.nudt@nudt.edu.cn (Y.S.)
[2] Guangxi Key Laboratory of Ocean Engineering Equipment and Technology, Qinzhou 535011, China; yxj9609@163.com
[3] College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
* Correspondence: chy63s@126.com

Abstract: Reconfigurable intelligent surface (RIS)-assisted unmanned aerial vehicles (UAV) have been extensively studied on the Internet of Things (IoT) systems to improve communication performance. In this paper, we aimed to counter simultaneous jamming and eavesdropping attacks by jointly designing an active beamforming vector at the base station (BS) and reflect phase shifts at the RIS. Specifically, considering imperfect angular channel state information (CSI), the sum secrecy rate maximization problem in the worst case could be formulated, which is NP-hard and non-convex. To address this problem, we improved the robust enhanced signal-to-leakage-and-noise ratio (E-SLNR) beamforming to reduce the computational complexity and mitigate the impact of interference, eavesdropping and jamming. Furthermore, a genetic algorithm with a tabu search (GA-TS) method was proposed to efficiently obtain an approximate optimal solution. The simulation results demonstrated that the proposed GA-TS method converged faster with better results than conventional GA, while the proposed robust scheme could achieve higher sum secrecy rates than the zero-forcing (ZF) and SLNR schemes.

Keywords: RIS; UAV; IoT; physical-layer security; E-SLNR; GA-TS

Citation: Qian, P.; Zhang, Y.; Yan, X.; Chen, Y.; Sun, Y. A Robust Scheme for RIS-Assisted UAV Secure Communication in IoT. *Electronics* **2023**, *12*, 2507. https://doi.org/10.3390/electronics12112507

Academic Editor: Dimitra I. Kaklamani

Received: 28 April 2023
Revised: 26 May 2023
Accepted: 31 May 2023
Published: 2 June 2023

1. Introduction

Recently, the Internet of Things (IoT) technology has been widely studied in fields such as smart homes, smart cities, smart grids, and autonomous vehicles due to its ability to connect a massive number of wireless devices [1]. According to a recent study by Ericsson, more than 25 billion IoT connections will be reached in 2025 [2]. Considering the limited spectral resources and energy constraints of IoT devices, fixed terrestrial base stations (BSs) face significant challenges in providing services to an increasing number of IoT devices and networks. Fortunately, unmanned aerial vehicles (UAVs) have been widely discussed for their ability to quickly deploy as air relays to boost the capacity and coverage of existing terrestrial networks and enhance the quality of wireless communication [3–5]. Due to the heterogeneity and geographical dispersion of IoT devices, several security issues have arisen. Particularly, sensitive information is generally sent as a type of plaintext by IoT devices, which is easily susceptible to eavesdropping attacks [6]. Furthermore, jamming is also a common attack on IoT to compromise data privacy, integrity and security [7,8]. However, the traditional UAV relay requires a large transmit power to forward signals and is vulnerable to counter eavesdropping and malicious jamming [9].

The reconfigurable intelligent surface (RIS) is a promising technology that can overcome these aforementioned shortcomings [10]. RIS is constituted of many passive low-cost reflectors whose phase and amplitude can be intelligently adjusted by a controller to reconfigure the wireless propagation environment [11]. It has been verified in [12] that RIS-assisted transmission can outperform the decode-and-forward (DF) relay protocol in

terms of energy efficiency (EE) for high-speed transmission. Thus, RIS has attracted a lot of interest in improving the security and performance of wireless communications while saving power consumption [10–15].

1.1. Related Works

Over the past few years, the UAV and RIS have been explored as assisting wireless communication in IoT. Many studies have introduced UAVs to increase the coverage and network capacity of wireless networks. For instance, in [16], a fast and efficient heuristic algorithm was proposed to address the UAV flight optimization problem, which aimed to provide an optimal throughput for a set of locations while considering the battery constraints of the UAVs and energy costs. In [17], the optimal 3D deployment problem of UAVs was solved to maximize the downlink coverage performance with a minimum transmit power. In [18], a 3D beamforming was designed to increase the coverage of the wireless communication system, in which UAVs were distributed at different heights and equipped with Multiple-Input-Multiple-Output (MIMO). In [19], a scenario of UAVs with imperfect beam alignment was considered, and an analytical framework was proposed to analyze the coverage probability of UAV-assisted networks under cluster users. In these aforementioned works, the position/trajectory and transmit power of UAVs were mainly studied to enhance wireless communication capabilities.

As an emerging technology, RIS adds a new dimension to the optimization of wireless communication performance and can effectively increase the performance of traditional UAV relay systems [9,20–22]. In [9], the RIS-UAV relaying communication system was proposed, and the system throughput was maximized by jointly optimizing the UAV trajectory, RIS passive beamforming and source power allocation for each time slot. In [21], the UAV-mounted RIS was utilized in the IoT network to enhance data collection, and an energy model was designed which took into account the weight of the UAV and RIS, as well as the environmental conditions and UAV's velocity. An air-to-ground downlink communication network with UAV-mounted RIS was proposed in [22] to improve the system's energy efficiency by jointly optimizing the trajectory of the UAV, phase shifts of RIS, and transmit power of BS. A block coordinate descent (BCD) method was used to solve the nonconvex inequality constraint, and the resource allocation problem of the BS transmit power was addressed by the Dinkelbach algorithm.

Furthermore, wireless communication scenarios with malicious nodes have also been discussed [23–26]. In [23], an aerial RIS was proposed against jamming attacks to enhance legitimate transmissions by jointly designing the deployment and passive beamforming of the aerial RIS through an alternating optimization algorithm with successive convex optimization. Reference [24] explored a communication scenario in which RIS was mounted on the UAV to resist malicious jamming attacks. A dueling double deep Q networks multi-step learning algorithm was proposed to jointly optimize the trajectory and passive beamforming. In [25], a RIS-assisted UAV secure communication scheme was proposed to counter eavesdropping and a maximum average secrecy rate was achieved through joint optimization of the BS's beamforming power, RIS's reflect phase shift, and UAV's trajectory. Additionally, the proposed non-convex optimization problem was decomposed into three sub-optimization problems, which could be solved efficiently. In [26], the distribution of eavesdroppers was modeled by the stochastic geometry theory, and novel expressions were proposed for a legitimate receiver and eavesdropper to analyze the impact of the number of reflecting units of RIS and the location of UAV on the secrecy outage probability performance. However, previous studies either did not consider malicious nodes or only considered eavesdropping or malicious jamming.

Moreover, it is noteworthy that these works concentrated on obtaining optimal solutions but inevitably resulted in high computational complexity and a heavy hardware burden. Recently, zero-forcing (ZF) beamforming and signal-to-leakage-plus-noise ratio (SLNR) beamforming have been proposed to reduce computational complexity and improve the security of communication [27,28]. ZF beamforming focus on nulling out the

inter-user interference with brute force [28]. Compared to ZF beamforming, SLNR beamforming can achieve higher secrecy rates [29,30]. Nevertheless, in order to implement these methods, the transmitter requires a perfect CSI. However, this is unrealistic considering the noncooperation between the transmitter and illegitimate nodes.

1.2. Contributions

Motivated by these aforementioned observations, this paper investigated the RIS-assisted UAV secure communication in the IoT network system to ensure the quality of wireless transmissions under eavesdropping and jamming attacks. Moreover, a robust optimization problem was proposed to maximize the sum secrecy rate by jointly optimizing the transmit beamforming of BS and the reflect phase shift of RIS. In order to efficiently solve the proposed optimization problem, many heuristic methods were proposed, such as Genetic Algorithms (GA) [31], Particle Swarm Optimization [32] and Tabu Search [33]. In this study, we introduced the TS algorithm into the traditional GA algorithm. The main contributions of this paper are summarized as follows:

(1) An RIS-assisted UAV secure communication in the IoT network system is proposed, in which UAV can be equipped with RIS to relay source signals and counter interference, eavesdropping and malicious jamming attacks simultaneously. Due to the imperfect angular channel state information of illegitimate nodes, we formulated a robust optimization problem to maximize the sum secrecy rate by jointly optimizing the active beamforming of BS and the reflection phase shift of RIS.

(2) We improved the robust E-SLNR beamforming of BS to counter interference, eavesdropping and malicious jamming simultaneously and reduced computational complexity and the impact of imperfect angular channel state information. For the nonconvex optimization problem, a GA-TS method was proposed to efficiently obtain an approximate optimal solution.

(3) The numerical results indicate that the proposed GA-TS method can converge faster than the conventional GA method, and the robustness of this proposed scheme was demonstrated. Compared to traditional ZF and SLNR beamforming, our improved E-SLNR beamforming provides better performance in security transmission. As a larger number of RIS units is set, the higher sum secrecy rate of the proposed scheme can be obtained.

The remainder of the paper is organized as follows. In Section 2, the system model of the RIS-assisted UAV secure communication in IoT and the optimization problem formulation is presented. Section 3 investigates the robust E-SLNR beamforming and the GA-TS method. Numerical results are shown in Section 4. Finally, we conclude this paper in Section 5.

2. System Model and Problem Formulation

2.1. System Model

As shown in Figure 1, we considered a multi-output single-input IoT communication network with a RIS-assisted UAV, which boosted information security. Meanwhile, there existed a jammer with $L = L_1 \times L_2$ antennas attempting to interrupt the legitimate transmissions and a single-antenna eavesdropper attempting to intercept the intended signals. Furthermore, it was assumed that BS equipped with $M = M_1 \times M_2$ antennas transmitted the desired data to K single-antenna users. In addition, uniform planar arrays (UPAs) with $N = N_1 \times N_2$ units were applied in the RIS. We considered UAV hovering in the air to provide a relay service, in other words, its position did not change. We let $\mathbf{G}_{BR} \in \mathbf{C}^{M\times N}$, $\mathbf{h}_{RU,k} \in \mathbf{C}^{N\times 1}$, $\mathbf{h}_{BU,k} \in \mathbf{C}^{M\times 1}$, $\mathbf{h}_{BE} \in \mathbf{C}^{M\times 1}$, $\mathbf{h}_{RE} \in \mathbf{C}^{N\times 1}$, $\mathbf{G}_{JR} \in \mathbf{C}^{L\times N}$, $\mathbf{h}_{JU,k} \in \mathbf{C}^{L\times 1}$ denote the channel coefficients between the BS and the RIS, between the RIS and the device k, between the BS and the device k, between the BS and the eavesdropper, between the RIS and the eavesdropper, between the jammer and the RIS, and between the jammer and the device k, respectively. Due to the limited transmit power, the transmit beamforming vector $\mathbf{w}_k \in \mathbf{C}^{M\times 1}$ satisfied $\sum_{k=1}^{K} \|\mathbf{w}_k\| \leq P_{Max}$, and the jamming beamforming vector

$\mathbf{w}_{J,k} \in \mathbf{C}^{L\times 1}$ satisfied $\sum_{k=1}^{K} \|\mathbf{w}_{J,k}\| \leq P_{J,Max}$, in which P_{Max}, $P_{J,Max}$ was the maximum of BS's transmitting power and the maximum jamming power, respectively. Thus, the desired signal sent by BS could be written as $\sum_{k=1}^{K} \mathbf{w}_k s_{T,k} \in \mathbf{C}^{M\times 1}$, and the jamming signal sent by the jammer could be represented as $\sum_{k=1}^{K} \mathbf{w}_{J,k} s_{J,k} \in \mathbf{C}^{L\times 1}$. In addition, due to hardware limitations, we considered the controllable number of RIS elements to be b. Specifically, we let $\mathbf{v} = (v_1, v_2, \cdots, v_N)^{\mathrm{T}}$ denote the reflect phase shift matrix of RIS, in which $v_i = e^{j\theta_i}$ and $\theta_i \in \left\{0, \frac{2\pi}{2^b}, \cdots, \frac{(2^b-1)2\pi}{2^b}\right\}$.

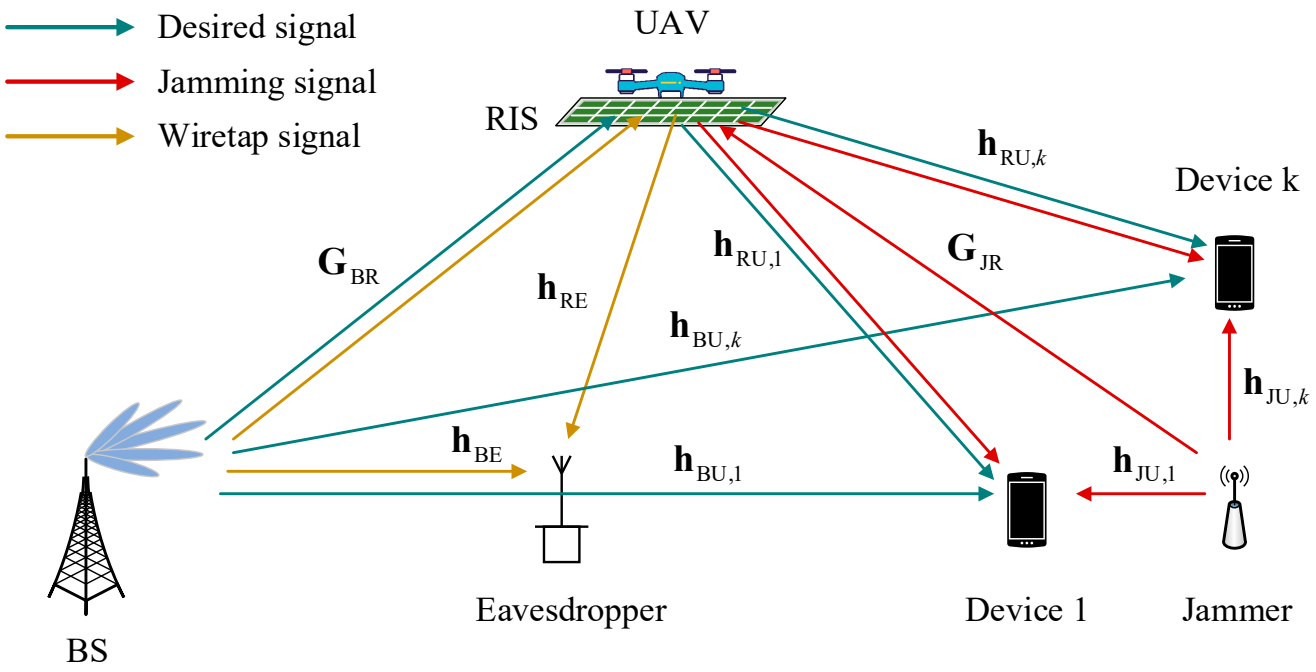

Figure 1. System model.

Due to the potential cooperation between the eavesdropper and jammer, it was assumed that the jammer signals received by the eavesdropper could be eliminated. Hence, the signals received at the device k from the BS could be given by:

$$y_{U,k} = \sum_{i=1}^{K} \mathbf{H}_{BU,k}^{\mathrm{T}} \mathbf{w}_i s_i + \sum_{i=1}^{K} \mathbf{H}_{JU,k}^{\mathrm{T}} \mathbf{w}_{J,i} s_{J,i} + n_{U,k} \tag{1}$$

and the signals received by the eavesdropper could be expressed as:

$$y_{\mathrm{E}} = \sum_{k=1}^{K} \mathbf{H}_{BE}^{\mathrm{T}} \mathbf{w}_k s_k + n_E \tag{2}$$

in which $\mathbf{H}_{BE} = \mathbf{h}_{BE} + \mathbf{G}_{BR}\mathbf{P}\mathbf{h}_{RE}$, $\mathbf{H}_{BU,k} = \mathbf{h}_{BU,k} + \mathbf{G}_{BR}\mathbf{P}\mathbf{h}_{RU,k}$, $\mathbf{H}_{JU,k} = \mathbf{h}_{JU,k} + \mathbf{G}_{JR}\mathbf{P}\mathbf{h}_{RU,k}$, $\mathbf{P} = diag(\mathbf{v})$. The symbol $n_{U,k} \sim CN(0, \sigma_{U,k}^2)$, $n_E \sim CN(0, \sigma_E^2)$ represented the thermal noise of the device k and eavesdropper, respectively, in which CN denoted the distribution of a circularly symmetric complex gaussian random vector. Hence, the desired signal rate of the device k and the wiretap signal rate at the eavesdropper for the device k were, respectively, given by:

$$R_{U,\,k} = \log_2\left(1 + \frac{\left|\mathbf{H}_{BU,\,k}^{\mathrm{T}}\mathbf{w}_k\right|^2}{\sum\limits_{i\neq k}^{K}\left|\mathbf{H}_{BU,\,k}^{\mathrm{T}}\mathbf{w}_i\right|^2 + \sum\limits_{i=1}^{K}\left|\mathbf{H}_{JU,\,k}^{\mathrm{T}}\mathbf{w}_{J,\,i}\right|^2 + \sigma_{U,\,k}^2}\right) \tag{3}$$

$$R_{E,\,k} = \log_2\left(1 + \frac{\left|\mathbf{H}_{\mathrm{BE},k}^{\mathrm{T}}\mathbf{w}_k\right|^2}{\sum\limits_{i\neq k}\left|\mathbf{H}_{\mathrm{BE}}^{\mathrm{T}}\mathbf{w}_i\right|^2 + \sigma_E^2}\right) \tag{4}$$

Regarding the definition in [34], the secrecy rate of the device k could be expressed as:

$$R_{S,\,k} = R_{U,\,k} - R_{E,\,k} \tag{5}$$

2.2. Channel Model

In the discussed system model, the channel that was considered consisted of two components: the line-of-sight (LoS) channel and the single-bounce non-LoS (NLoS) channel [35,36]. This was the same as that described in [35], where the channel vector could be modeled as:

$$\mathbf{G}/\mathbf{h} = g_0\mathbf{a}_P\left(\theta_0^{RX},\varphi_0^{RX}\right)\mathbf{a}_P^H\left(\theta_0^{TX},\varphi_0^{TX}\right) + \sqrt{\frac{1}{M_p}}\sum_{d=1}^{M_p} g_d\mathbf{a}_P\left(\theta_d^{RX},\varphi_d^{RX}\right)\mathbf{a}_P^H\left(\theta_d^{TX},\varphi_d^{TX}\right) \tag{6}$$

$$\mathbf{h} = g_0\mathbf{a}_P\left(\theta_0^{TX},\varphi_0^{TX}\right) + \sqrt{\frac{1}{M_P}}\sum_{d=1}^{M_p} g_d\mathbf{a}_P\left(\theta_d^{TX},\varphi_d^{TX}\right) \tag{7}$$

in which M_P denotes the number of multiple paths, $\theta^{TX}(\varphi^{TX})$ denotes the vertical (horizontal) Angle of Departure (AoD), and θ^{RX} (φ^{RX}) denotes the vertical (horizontal) Angle of Arrival (AoA), respectively. Moreover, g is the large-scale fading coefficients, in which we could assume that $g \sim CN(0, 10^{PL/10})$, $PL = -30.18 - 26\log_{10}(d_s)$, and d_s is the distance between the transmitter and receiver. Furthermore, $\mathbf{a}_P(\theta,\varphi)$ represents the steering vectors of UPA, which can be expressed by:

$$\mathbf{a}_P(\theta,\varphi) = \left[1, e^{j\frac{2\pi d_1}{\lambda}\sin\theta\cos\varphi}, \cdots, e^{j\frac{2\pi d_1(N_1-1)}{\lambda}\sin\theta\cos\varphi}\right]^T \otimes \left[1, e^{j\frac{2\pi d_2}{\lambda}\cos\theta}, \cdots, e^{j\frac{2\pi d_2(N_2-1)}{\lambda}\cos\theta}\right]^T \tag{8}$$

in which N_1, N_2 represents the number of array elements along the UPA side, respectively. d_1, d_2 is the inter-element spacing along the UPA side, respectively. In this paper, the inter-element spacing was set as the half-wavelength, i.e., $d_1 = d_2 = \lambda/2$.

As we know, the CSI of the RIS-assisted systems could be accurately obtained through several channel estimation techniques in recent works, e.g., [37]. Hence, it was assumed that the CSI of legitimate channels ($\mathbf{G}_{BR}$, $\mathbf{h}_{IU,\,k}$ and $\mathbf{h}_{BU,\,k}$) could be accurately obtained. However, the CSI of illegitimate channels ($\mathbf{h}_{BE}$, $\mathbf{h}_{RE}$, $\mathbf{G}_{JR}$, $\mathbf{h}_{JU,\,k}$) were unavailable for accurate estimation by BS due to its lack of cooperation with the illegitimate nodes. To account for this effect on the system, a given angle-based range was adopted to characterize the illegitimate CSI [38]. The coupled angular uncertainties were defined as $\{\Delta_E, \Delta_J\}$, which was modeled as:

$$\Delta_E = \left\{\mathbf{h}_i \middle| \theta_i^E \in \left[\theta_{i,L}^E, \theta_{i,U}^E\right], \varphi_i^E \in \left[\varphi_{i,L}^E, \varphi_{i,U}^E\right], \left|g_i^E\right| \in \left[\left|g_{i,L}^E\right|, \left|g_{i,U}^E\right|\right], i \in (RE, BE)\right\} \tag{9}$$

$$\Delta_{J,h} = \left\{ \mathbf{h}_{JU,k} \middle| \theta_k^J \in \left[\theta_{k,L}^J, \theta_{k,U}^J \right], \varphi_k^J \in \left[\varphi_{k,L}^J, \varphi_{k,U}^J \right], \left| g_k^J \right| \in \left[\left| g_{k,L}^J \right|, \left| g_{k,U}^J \right| \right], \forall k \right\} \tag{10}$$

$$\begin{aligned} \Delta_{J,G} = \Big\{ \mathbf{G}_{JR} \Big| \theta_G^{J,T} \in \left[\theta_{G,L}^{J,T}, \theta_{G,U}^{J,T} \right], \varphi_G^{J,T} \in \left[\varphi_{G,L}^{J,T}, \varphi_{G,U}^{J,T} \right], \theta_G^{J,R} \in \left[\theta_{G,L}^{J,R}, \theta_{G,U}^{J,R} \right], \\ \varphi_G^{J,R} \in \left[\varphi_{G,L}^{J,R}, \varphi_{G,U}^{J,R} \right], \left| g_G^J \right| \in \left[\left| g_{G,L}^J \right|, \left| g_{G,U}^J \right| \right], \forall k \Big\} \end{aligned} \tag{11}$$

in which $\Delta_J = \left\{ \Delta_{J,h}, \Delta_{J,G} \right\}$, θ_L and θ_U denote the lower and upper bounds of vertical AoA, respectively. φ_L and φ_U denote the lower and upper bounds of horizontal AoA, respectively. g_L and g_U denote the lower and upper bounds of the channel gain amplitude, respectively.

2.3. Problem Formulation

In order to ensure the security of IoT wireless communication, a sum secrecy rate maximization problem in the worst-case was formulated in this section. Namely, we aimed to maximize the sum achievable secrecy rate by jointly designing BS's active beamforming vector $\{\mathbf{w}_k\}_{k=1}^K$ and RIS's reflect phase shift matrix $\mathbf{v}$ to mitigate the impact of jamming and eavesdropping attacks, with the imperfect angular CSI Δ_E, Δ_J and no knowledge of the jamming beamforming. Furthermore, the BS's maximum transmits power constraint, and the RIS unit-modulus constraint (UMC) was considered. Hence, the optimization problem could be formulated as follows:

$$\begin{aligned} \max_{\mathbf{w},\mathbf{v}} \quad & \min_{\Delta_J, \Delta_E} \sum_k R_{S,\,k}(\mathbf{w}, \mathbf{v}) \\ s.t. \quad & \mathrm{C1}: \sum_k \|\mathbf{w}_k\|^2 \le P_{max} \\ & \mathrm{C2}: |v_i| = 1, \forall i \end{aligned} \tag{12}$$

in which $\mathbf{W} = \{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_K\}$ represents BS's active beamforming matrix. Obviously, the formulated optimization problem was non-convex and NP-hard, which was complex and challenging to be directly solved. Accordingly, robust E-SLNR beamforming was proposed to reduce the computational complexity and the impact of imperfect angular channel state information in the following section. Moreover, the GA-TS method was improved for handling the formulated complex optimization problem to design active beamforming and the reflect phase shift.

3. Robust Scheme

3.1. Robust Transmit Beamforming Design

Differing from the conventional SLNR beamforming, this paper proposes E- SLNR beamforming, which takes the malicious jamming power and the eavesdropped signal power into account. The specific expression for this is as follows:

$$\mathrm{E-SLNR}_k = \frac{\left| \mathbf{H}_{BU,\,k}^{\mathrm{T}} \mathbf{w}_k \right|^2}{\sum\limits_{i \ne k}^{K} \left| \mathbf{H}_{BU,\,i}^{\mathrm{T}} \mathbf{w}_k \right|^2 + |\mathbf{H}_{BE} \mathbf{w}_k|^2 + \sum\limits_{i=1}^{K} \left| \mathbf{H}_{JU,\,k}^{\mathrm{T}} \mathbf{w}_{J,\,i} \right|^2 + \sigma_k^2} \tag{13}$$

in which the numerator in Equation (13) represents the desired signal power received by the device k, the first term of the denominator in Equation (13) denotes the inter-user interference power, the second term of the denominator in Equation (13) represents the signal power received by the eavesdropper, the third term of the denominator in Equation (13) denotes the malicious jamming power, and the final term of the denominator in Equation (13) represents the thermal noise of the device k.

Based on fairness, it was assumed that the transmit power for each device was equal. When the reflect phase shift matrix **v** was given, according to the E-SLNR beamforming, the formulated optimization problem in (12) could approximately be relaxed into the following E-SLNR maximization problem:

$$\begin{aligned} \max_{\mathbf{w}} \min_{\Delta_J, \Delta_E} \mathrm{E-SLNR}_k &= \frac{\mathbf{w}_k^{\mathrm{H}} \mathbf{H}_{BU,k}^{*} \mathbf{H}_{BU,k}^{\mathrm{T}} \mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}} \left[\sum_{i \neq k}^{K} \mathbf{H}_{BU,i}^{*} \mathbf{H}_{BU,i}^{\mathrm{T}} + \mathbf{H}_{BE}^{*} \mathbf{H}_{BE}^{\mathrm{T}} + \left(D_{j,k} + \sigma_k^2\right)/P_k\right] \mathbf{w}_k} \\ s.t. \|\mathbf{w}_k\|^2 &= P_{\mathrm{k}} \end{aligned} \tag{14}$$

in which $D_{j,\,k} = \sum_{i=1}^{K} \left| \mathbf{H}_{JU,\,k}^{\mathrm{T}} \mathbf{w}_{J,\,i} \right|^2$ represents the jamming power received by device k and $P_{\mathrm{k}} = P_{\max}/M$ denotes the transmit power for device k. However, due to the imperfect CSI, $D_{j,k}$ and $\mathbf{H}_{BE}^{*}\mathbf{H}_{BE}^{\mathrm{T}}$ could not be obtained accurately. Hence, active beamforming could not be solved directly. The upper bound of $D_{j,k}$ could be obtained by the Cauchy–Schwarz inequality as:

$$D_{j,k} \leq \sum_{i=1}^{K} \hat{p}_{J,i} \mathbf{H}_{JU,k}^{\mathrm{T}} \mathbf{H}_{JU,k}^{*} \tag{15}$$

in which $\hat{p}_{J,i}$ represents the estimation of the jamming power for device i, which can be estimated by the rotational invariance techniques [39]. Furthermore, $\mathbf{H}_{JU,k}^{\mathrm{T}}\mathbf{H}_{JU,k}^{*}$ could be expanded as:

$$\begin{aligned} \mathbf{H}_{JU,k}^{\mathrm{T}} \mathbf{H}_{JU,k}^{*} &= \mathbf{h}_{JU,k}^{\mathrm{T}} \mathbf{h}_{JU,k}^{*} + 2\mathrm{Re}\left\{ \mathbf{h}_{RU,k}^{\mathrm{T}} \mathbf{P} \mathbf{G}_{JR}^{\mathrm{T}} \mathbf{h}_{JU,k}^{*} \right\} + \mathbf{h}_{RU,k}^{\mathrm{T}} \mathbf{P} \mathbf{G}_{JR}^{\mathrm{T}} \mathbf{G}_{JR}^{*} \mathbf{P}^{*} \mathbf{h}_{RU,k}^{*} \\ &= H_{JU,k} + 2\mathrm{Re}\left\{ \mathbf{h}_{RU,k}^{\mathrm{T}} \mathbf{P} \mathbf{G}_{RU,k} \right\} + \mathbf{h}_{RU,k}^{\mathrm{T}} \mathbf{P} \Phi_{JR} \mathbf{P}^{*} \mathbf{h}_{RU,k}^{*} \end{aligned} \tag{16}$$

in which $H_{JU,k} = \mathbf{h}_{JU,k}^{\mathrm{T}} \mathbf{h}_{JU,k}^{*}$, $\mathbf{G}_{RU,k} = \mathbf{G}_{JR}^{\mathrm{T}} \mathbf{h}_{JU,k}^{*}$, $\Phi_{JR} = \mathbf{G}_{JR}^{\mathrm{T}} \mathbf{G}_{JR}^{*}$. Moreover, the coupled angular uncertainties Δ_J could be rewritten as:

$$\Lambda_J = \left\{ H_{JU,k}, \mathbf{G}_{RU,k}, \Phi_{JR} \middle| \Delta_J \right\} \tag{17}$$

According to [40], any imperfect CSI in the angular uncertainty set could be expressed as the combination of discrete elements. Thus, when the uncertainty region based on angular information was known, we could uniformly sample the angles in a set of Λ_J as:

$$\begin{aligned} \theta^{(i_1)} &= \theta_L + (i_1 - 1)\Delta\theta, i_1 = 1, \cdots, Q_1 \\ \varphi^{(i_2)} &= \varphi_L + (i_2 - 1)\Delta\varphi, i_2 = 1, \cdots, Q_2 \end{aligned} \tag{18}$$

in which $Q_1 \geq M_1$ and $Q_2 \geq M_2$ represent the sample number of θ and φ, respectively. $\Delta\theta = (\theta_U - \theta_L)/(Q_1 - 1)$, and $\Delta\varphi = (\varphi_U - \varphi_L)/(Q_2 - 1)$.

As proved in [41], the robust form of $\widetilde{H}_{\mathrm{JU},k}$, $\widetilde{\mathbf{G}}_{RU,k}$, $\widetilde{\Phi}_{\mathrm{JR}}$ could be expressed as:

$$\widetilde{H}_{JU,k} = \sum_{i_1=1}^{L_1} \sum_{i_2=1}^{L_2} (1/L) \mathbf{h}_{JU,k}^{(i_1,i_2),\mathrm{T}} \mathbf{h}_{JU,k}^{(i_1,i_2),*} \tag{19}$$

$$\widetilde{\mathbf{G}}_{RU,k} = \sum_{i_1=1}^{L_1} \sum_{i_2=1}^{L_2} \sum_{i_3=1}^{N_1} \sum_{i_4=1}^{N_2} (1/LN) \mathbf{G}_{JR}^{(i_1,i_2,i_3,i_4),\mathrm{T}} \mathbf{h}_{JU,k}^{(i_1,i_2),*} \tag{20}$$

$$\widetilde{\Phi}_{JR} = \sum_{i_1=1}^{L_1} \sum_{i_2=1}^{L_2} \sum_{i_3=1}^{N_1} \sum_{i_4=1}^{N_2} (1/LN) \mathbf{G}_{JR}^{(i_1,i_2,i_3,i_4),\mathrm{T}} \mathbf{G}_{JR}^{(i_1,i_2,i_3,i_4),*} \tag{21}$$

Hence, the robust upper bound of $D_{j,k}$ could be obtained as:

$$\widetilde{D}_{j,k} = \sum_{i=1}^{K} \hat{p}_{J,i}\left(\widetilde{H}_{JU,k} + 2\mathrm{Re}\left\{\mathbf{h}_{RU,k}^{\mathrm{T}}\mathbf{P}\widetilde{\mathbf{G}}_{RU,k}\right\} + \mathbf{h}_{RU,k}^{\mathrm{T}}\mathbf{P}\widetilde{\Phi}_{JR}\mathbf{P}^{*}\mathbf{h}_{RU,k}^{*}\right) \tag{22}$$

Similarly, the robust form of $\mathbf{H}_{\mathrm{BE}}^{*}\mathbf{H}_{\mathrm{BE}}^{\mathrm{T}}$ could be expressed as:

$$\widetilde{\Psi} = \widetilde{\Phi}_{BE} + 2\mathrm{Re}\left\{\mathbf{G}_{BR}^{*}\mathbf{P}^{*}\widetilde{\mathbf{G}}_{RE}\right\} + \mathbf{G}_{BR}^{*}\mathbf{P}^{*}\widetilde{\Phi}_{RE}\mathbf{P}\mathbf{G}_{BR}^{\mathrm{T}} \tag{23}$$

in which:

$$\widetilde{\Phi}_{BE} = \sum_{i_1=1}^{M_1}\sum_{i_2=1}^{M_2}(1/L)\mathbf{h}_{BE}^{(i_1,i_2),*}\mathbf{h}_{BE}^{(i_1,i_2),\mathrm{T}} \tag{24}$$

$$\widetilde{\mathbf{G}}_{RE} = \sum_{i_3=1}^{N_1}\sum_{i_4=1}^{N_2}(1/N)\mathbf{h}_{RE}^{(i_3,i_4),*}\mathbf{h}_{BE}^{(i_1,i_2),\mathrm{T}} \tag{25}$$

$$\widetilde{\Phi}_{RE} = \sum_{i_3=1}^{N_1}\sum_{i_4=1}^{N_2}(1/N)\mathbf{h}_{RE}^{(i_3,i_4),*}\mathbf{h}_{RE}^{(i_3,i_4),\mathrm{T}} \tag{26}$$

Thus, by substituting $\widetilde{D}_{j,k}$ and $\widetilde{\Psi}$ into the optimization problem in (14), the worst-case E-SLNR maximization problem could be rewritten as:

$$\begin{aligned} \max_{\mathbf{w}} \mathrm{E-SLNR}_k &= \frac{\mathbf{w}_k^{\mathrm{H}}\mathbf{H}_{BU,k}^{*}\mathbf{H}_{BU,k}^{\mathrm{T}}\mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}}\left[\sum_{i\neq k}^{K}\mathbf{H}_{BU,i}^{*}\mathbf{H}_{BU,i}^{\mathrm{T}} + \widetilde{\Psi} + \left(\widetilde{D}_{j,k} + \sigma_k^2\right)/P_k\right]\mathbf{w}_k} \\ s.t. &\|\mathbf{w}_k\|^2 = P_{\mathrm{k}} \end{aligned} \tag{27}$$

According to [42], the problem could be resolved as:

$$\mathbf{w}_k = P_k \cdot \max.\mathrm{eigenvector}\left(\left[\sum_{i\neq k}^{K}\mathbf{H}_{BU,i}^{*}\mathbf{H}_{BU,i}^{\mathrm{T}} + \widetilde{\Psi} + \left(\widetilde{D}_{j,k} + \sigma_k^2\right)/P_k\right]^{-1}\mathbf{H}_{BU,k}^{*}\mathbf{H}_{BU,k}^{\mathrm{T}}\right) \tag{28}$$

in which the E-SLNR beamforming $\mathbf{w}_k$ is proportional to the eigenvector corresponding to the maximum eigenvalue of the matrix. This could be directly solved using tools in MATLAB, such as the function eigs [43].

3.2. GA-TS Method

In this section, the method for obtaining the reflect phase shift matrix **v** and the joint optimization algorithm is studied. According to (28), the close-form solution of **v** could not be obtained. Namely, when the E-SLNR beamforming **w** was given, the reflect phase shift matrix **v** could not be obtained directly. Due to the discreteness of the phase shifts, we propose utilizing the GA to solve this problem.

We took the discrete phase shifts of RIS as the individual gene of the population and the sum secrecy rate of the IoT system as the fitness. Through a continuous iterative crossover and mutation, we could obtain the fittest individual that maximized the sum secrecy rate. Compared to traditional GA [31], a tabu search (TS) was introduced to accelerate the convergence speed of the algorithm. In each generation, the fittest individual gene of the population was recorded in the tabu table if the gene had not been recorded yet. In other words, the tabu table recorded the local optimal solutions. With a continuous iteration, the fitness of the genes recorded in the tabu table became better and better. Furthermore, after the process of the crossover and mutation, the child genes could be mutated if the child genes already existed in the tabu table. Specifically, only a small portion of the child genes underwent mutations to explore better solutions. In addition, the length of the tabu table was fixed. Thus, when the tabu table was full, the initial value could be overwritten by the new value. Through the TS, the algorithm could avoid falling into local optima and converge faster. The specific process of the GA-TS is shown in Algorithm 1.

Algorithm 1: The Proposed GA-TS Algorithm

1: **Initialize the GA parameters**: Population size N_p, Crossover probability p_c, Mutation probability p_{mut}, Number of generations N_g, Number of elites N_f, Number of participants in tournament N_t;
2: Randomly generate the reflect phase shift matrix $\mathbf{v}$ as the individuals of the first generation;
3: Compute the robust beamforming $\mathbf{w}$ by (28);
4: Compute the achievable sum secrecy rate as fitness of each individual;
5: **repeat**
6: **Elitism**: Select the N_f fittest individual genes directly as the child genes;
7: **Tournament**: Randomly select the N_t individual to compare their fitness, use the fittest individual as a parent, and repeat until $N_p - N_f$ parents are selected;
8: **Crossover Operator**: Randomly match parents genes, and generate the child genes by crossing the selected parents with probability p_c;
9: **Mutation Operator**: Randomly select child genes for mutation with probability p_{mut};
10: **Tabu Search**: Compare the child genes on the tabu table. If the gene is found in the tabu table, mutate the gene;
11: Compute the $\mathbf{w}$ and the fitness of each individual;
12: Record the fittest $\mathbf{v}^*$ into the tabu table;
13: **until** the maximum number of generations is reached.
14: Return the fittest $\mathbf{w}^*$, $\mathbf{v}^*$.

4. Simulation Results

In this section, simulation results are provided to evaluate the performance of the improved GA-TS method and proposed robust scheme. We assumed that the BS served two users, namely K = 2, in which the antenna number of BS was set as $M = 8 \times 8$. Moreover, the antenna number of the jammer was set as $L = 4 \times 4$, and the reflect units' number of RIS was set as $N = 8 \times 8$. In addition, the position of BS was set as (0,0,0), the position of users was set as (20,15,0) and (25,5,0), the position of RIS was set as (20,0,30), while the position of eavesdropper was set as (60,−15,0) and the position of jammer was set as (300,0,0), respectively. As shown in [10], the carrier frequency was considered at 5.8 GHz, the noise power was set as $\sigma_{U,k}^2 = \sigma_E^2 = -80$ dBm. Furthermore, the transmitting power of BS was set as, $P_{Max} = 30$ dBm, and the jamming power of the jammer was set as $P_{J,Max} = 40$ dBm.

Figure 2 depicts the comparison of the proposed GA-TS and the conventional GA for convergence [31]. As shown, the population size was set as 30, 60 and 100, respectively. In addition, the crossover probability was set as $p_c = 0.6$, the mutation probability was set as $p_{mut} = 0.8$, the number of elites was set as $N_f = 2$, and the number of participants in the tournament was set as $N_t = 5$. As shown in Figure 2, under the same population size, the proposed GA-TS converged faster and achieved better fitness compared to the conventional method. Because of the introduction to TS, this population could escape from the local optimal solution faster and accelerate the convergence. Meanwhile, with the population size increasing, the convergence speed of the method was faster, and better fitness could be obtained. Furthermore, the increase in the population size corresponded to an increase in attempts to the optimal solution, which led to a decrease in the gain of TS.

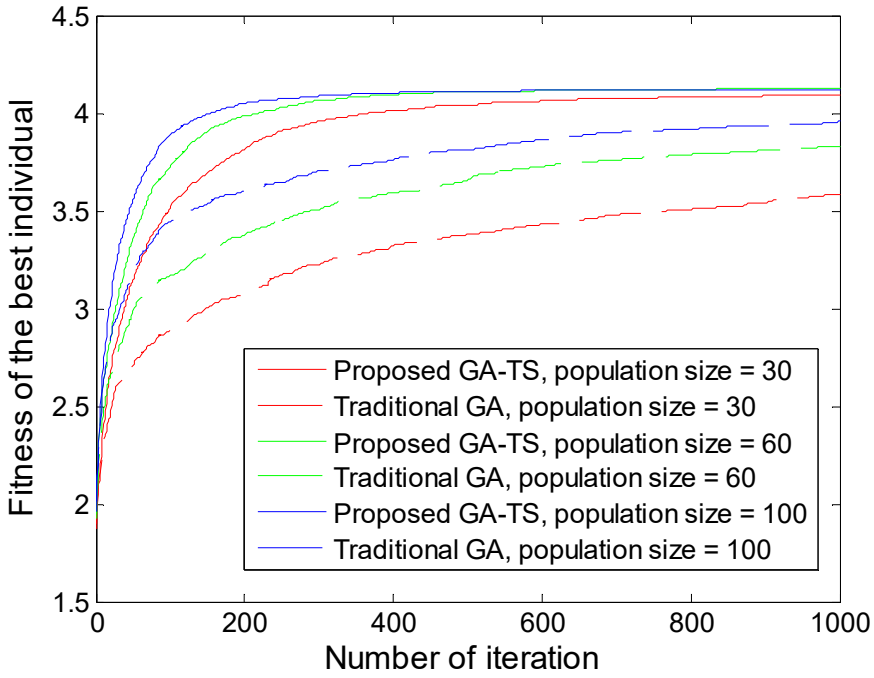

Figure 2. Convergence of the algorithms.

Figure 3 shows the comparison of the sum desired signal rate, sum wiretap signal rate and sum secrecy rate of the proposed E-SLNR, using the uncertainty angular region $\Delta_E = \Delta_J = 2°, 4°, 6°, 8°$. Due to the uncertainty angular region, the direction of the sum rate (i.e., sum desired signal rate, sum wiretap signal rate and sum secrecy rate) change was unknown. As shown, with the uncertainty angular region increasing, there was no significant change in the sum rate. Due to the adoption of the robust form, although the sum rate generally showed a downward trend when the uncertainty angular region increased, there was no sharp fluctuation. Namely, the robustness of the proposed scheme was demonstrated.

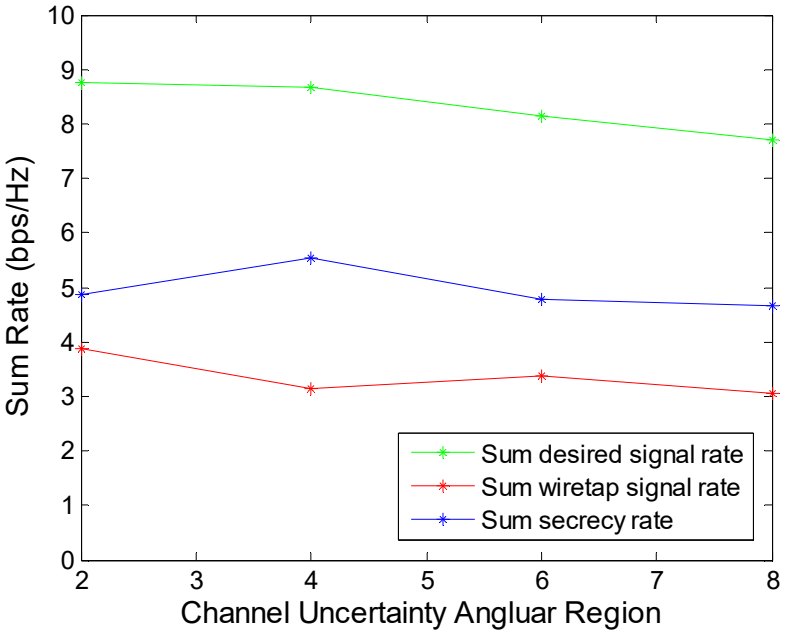

Figure 3. Sum achievable rate versus uncertainty angular region Δ.

Figure 4 shows the comparison of the sum secrecy rate versus the number of RIS units with a different scheme. The uncertainty angular region was set at 4°. We compare dthe performance of the proposed scheme with the following scheme: (1) ZF with RIS: under the assistance of RIS, BS was set as the ZF beamforming with an estimated illegitimate CS; (2) SLNR with RIS: under the assistance of RIS, BS was set as the traditional SLNR beamforming with an estimated illegitimate CS; (3) Ideal E-SLNR with RIS: under the assistance of RIS, BS was set as the proposed E-SLNR beamforming with an exact illegitimate CS; (4) E-SLNR with random RIS: BS was set as the proposed E-SLNR beamforming with a random reflect phase shift matrix of RIS and an estimated illegitimate CSI. As expected, the numerical results of the proposed robust scheme were better compared to the ZF with RIS and the SLNR with RIS. Because ZF beamforming requires accurate channel information to null out the wiretap rate, and traditional SLNR does not consider the impact of interference. As the larger number of RIS units was set, the higher sum secrecy rate of the proposed scheme could be obtained. This can be explained be the fact that more RIS units exploit more degrees of freedom to enhance the desired signal and reduce the impact of malicious nodes. Compared to the E-SLNR with random RIS, the validity of the optimization method of the proposed robust scheme was verified. Due to the impact of the random reflect phase shift matrix of RIS, which caused RIS not to enhance the desired signal, the sum secrecy rate of E-SLNR with random RIS could not be improved with the increase in the number of RIS units. Moreover, due to the fact that traditional SLNR did not consider jamming power, its sum secrecy rate was very low and was not affected by the number of RIS units.

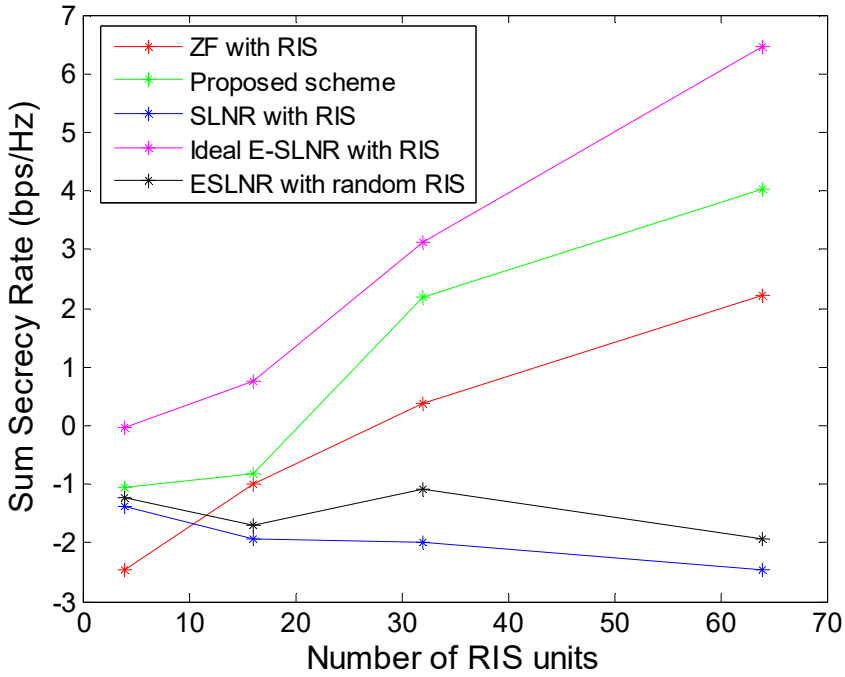

Figure 4. Sum secrecy rate versus the number of RIS units.

5. Conclusions

In this paper, to counter simultaneous jamming and eavesdropping attacks, we investigated a robust scheme for IoT's secure communication with support from UAV-assisted RIS. Specifically, considering the impact of imperfect angular CSI, a sum secrecy rate maximization problem in the worst case was formulated subject to the maximum transmission power constraint of BS and the UMC of RIS. Furthermore, we improved a robust E-SLNR beamforming for the reduction in the computation complexity and the impact of interference, eavesdropping and jamming simultaneously. Finally, a GA-TS method was proposed to jointly optimize the active beamforming of BS and the phase shift matrix of the RIS. The

numerical results suggested that the proposed GA-TS method had a better performance compared to the conventional GA method. Moreover, the robustness of the proposed scheme was demonstrated.

For future works, the IoT wireless communication network assisted by multiple UAVs with RISs was researched. In this system, a higher performance of anti-jamming and anti-eavesdropping could be obtained. However, the channel model became more complex, and computational complexity exponentially increased. Thus, traditional heuristic algorithms might not be able to provide results promptly, and artificial intelligence methods, such as neural networks, deep learning, reinforcement learning, etc., need to be introduced.

Author Contributions: Conceptualization, Y.C., Y.Z. and P.Q.; methodology, P.Q. and Y.S.; validation, P.Q., Y.S.; investigation, P.Q. and X.Y.; writing—original draft preparation, P.Q.; writing—review and editing Y.C., Y.Z., X.Y. and Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

Description of the parameters

Parameter	Definition
LM	Antenna numbers of jammer/BS
L_1/L_2	Antenna numbers of jammer along the X/Y axis
M_1/M_2	Antenna numbers of BS along the X/Y axis
N	Unit numbers of RIS
N_1/N_2	Unit number of array elements along the X/Y axis
$\mathbf{w}_k$	Transmit beamforming vector of the BS
$\mathbf{w}_{J,k}$	Jamming beamforming vector to k-th device
$\mathbf{v}$	Reflect phase shift matrix of RIS
$n_{U,\,k}/n_E$	Thermal noise of k-th device/eavesdropper
$\mathbf{G}_{BR}/\mathbf{h}_{BU,k}/\mathbf{h}_{BE}$	Channel vector between BS and RIS/k-th device/eavesdropper
$\mathbf{h}_{RU,k}/\mathbf{h}_{RE}$	Channel vector between RIS and k-th device/eavesdropper
$\mathbf{G}_{JR}/\mathbf{h}_{JU,k}$	Channel vector between jammer and RIS/k-th device

References

1. Tran, D.H.; Nguyen, V.D.; Chatzinotas, S.; Vu, T.X.; Ottersten, B. UAV Relay-Assisted Emergency Communications in IoT Networks: Resource Allocation and Trajectory Optimization. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1621–1637. [CrossRef]
2. Ericsson. *Ericsson Mobility Report: November 2019*; Ericsson: Stockholm, Sweden, 2019.
3. Wang, W.; Li, X.; Zhang, M.; Cumanan, K.; Ng, D.W.K.; Zhang, G.; Tang, J.; Dobre, O.A. Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming. *IEEE Trans. Commun.* **2020**, *68*, 4476–4489. [CrossRef]
4. Liao, N.; He, P.; Du, Y.; Zhang, Y.; Chen, Y.; Liang, T. Joint mission planning and spectrum resources optimization for multi-UAV reconnaissance. *IET Commun.* **2023**, *17*, 324–335. [CrossRef]
5. Wu, D.; Zhang, Y.; Chen, Y. Joint Optimization Method of Spectrum Resource for UAV Swarm Information Transmission. *Electronics* **2022**, *11*, 3372. [CrossRef]
6. Liu, G.; Quan, W.; Cheng, N.; Gao, D.; Lu, N.; Zhang, H.; Shen, X. Softwarized IoT Network Immunity Against Eavesdropping With Programmable Data Planes. *IEEE Internet Things J.* **2021**, *8*, 6578–6590. [CrossRef]
7. Gouissem, A.; Abualsaud, K.; Yaacoub, E.; Khattab, T.; Guizani, M. Accelerated IoT Anti-Jamming: A Game Theoretic Power Allocation Strategy. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 10607–10620. [CrossRef]
8. D'Andreagiovanni, F. Revisiting wireless network jamming by SIR-based considerations and multiband robust optimization. *Optim. Lett.* **2014**, *9*, 1495–1510. [CrossRef]
9. Liu, X.; Yu, Y.; Li, F.; Durrani, T.S. Throughput Maximization for RIS-UAV Relaying Communications. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 19569–19574. [CrossRef]
10. Sun, Y.; An, K.; Zheng, G.; Wong, K.K.; Chatzinotas, S.; Yin, H.; Liu, P. RIS-Assisted Robust Hybrid Beamforming Against Simultaneous Jamming and Eavesdropping Attacks. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 9212–9231. [CrossRef]

11. Mondal, A.; Junaedi, A.M.A.; Singh, K.; Biswas, S. Spectrum and Energy-Efficiency Maximization in RIS-Aided IoT Networks. *IEEE Access* **2022**, *10*, 103538–103551. [CrossRef]
12. Björnson, E.; Özdogan, O.; Larsson, E.G. Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying? *IEEE Wirel. Commun. Lett.* **2020**, *9*, 244–248. [CrossRef]
13. Sun, Y.; An, K.; Luo, J.; Zhu, Y.; Zheng, G.; Chatzinotas, S. Intelligent Reflecting Surface Enhanced Secure Transmission Against Both Jamming and Eavesdropping Attacks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 11017–11022. [CrossRef]
14. Niu, H.; Chu, Z.; Zhou, F.; Zhu, Z.; Zhen, L.; Wong, K.-K. Robust Design for Intelligent Reflecting Surface-Assisted Secrecy SWIPT Network. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 4133–4149. [CrossRef]
15. An, K.; Chatzinotas, S.; Hu, Y.; Lin, Z.; Niu, H.; Wang, Y.; Zheng, G. Refracting RIS Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724.
16. Chiaraviglio, L.; d'Andreagiovanni, F.; Choo, R.; Cuomo, F.; Colonnese, S. Joint Optimization of Area Throughput and Grid-Connected Microgeneration in UAV-Based Mobile Networks. *IEEE Access* **2019**, *7*, 69545–69558. [CrossRef]
17. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Efficient Deployment of Multiple Unmanned Aerial Vehicles for Optimal Wireless Coverage. *IEEE Commun. Lett.* **2016**, *20*, 1647–1650. [CrossRef]
18. Alkama, D.; Ouamri, M.A.; Alzaidi, M.S.; Shaw, R.N.; Azni, M.; Ghoneim, S.S.M. Downlink Performance Analysis in MIMO UAV-Cellular Communication With LOS/NLOS Propagation Under 3D Beamforming. *IEEE Access* **2022**, *10*, 6650–6659. [CrossRef]
19. Ouamri, M.A.; Alkanhel, R.; Gueguen, C.; Alohali, M.A.; Ghoneim, S.S.M. Modeling and analysis of uav-assisted mobile network with imperfect beam alignment. *Comput. Mater. Contin.* **2023**, *74*, 453–467. [CrossRef]
20. Pogaku, A.C.; Do, D.T.; Lee, B.M.; Nguyen, N.D. UAV-Assisted RIS for Future Wireless Communications: A Survey on Optimization and Performance Analysis. *IEEE Access* **2022**, *10*, 16320–16336. [CrossRef]
21. Taniya, S.; Hina, T.; Ekram, H. Optimization of Wireless Relaying With Flexible UAV-Borne Reflecting Surfaces. *IEEE Trans. Commun.* **2021**, *69*, 309–325.
22. Yao, Y.; Lv, K.; Huang, S.; Li, X.; Xiang, W. UAV Trajectory and Energy Efficiency Optimization in RIS-Assisted Multi-User Air-to-Ground Communications Networks. *Drones* **2023**, *7*, 272. [CrossRef]
23. Tang, X.; Wang, D.; Zhang, R.; Chu, Z.; Han, Z. Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6232–6237. [CrossRef]
24. Hou, Z.; Chen, J.; Huang, Y.; Luo, Y.; Wang, X.; Gu, J.; Xu, Y.; Yao, K. Joint Trajectory and Passive Beamforming Optimization in IRS-UAV Enhanced Anti-Jamming Communication Networks. *China Commun.* **2022**, *19*, 191–205. [CrossRef]
25. Wang, D.; Zhao, Y.; He, Y.; Tang, X.; Li, L.; Zhang, R.; Zhai, D. Passive Beamforming and Trajectory Optimization for Reconfigurable Intelligent Surface-Assisted UAV Secure Communication. *Remote Sens.* **2021**, *13*, 4286. [CrossRef]
26. Wang, W.; Tian, H.; Ni, W. Secrecy Performance Analysis of IRS-Aided UAV Relay System. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 2693–2697. [CrossRef]
27. Zheng, G.; Arapoglou, P.D.; Ottersten, B. Physical layer security in multibeam satellite systems. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 852–863. [CrossRef]
28. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2023**, *59*, 2085–2088. [CrossRef]
29. Piya, P.; Simon, A.; Angela, D. On the equivalence between SLNR and MMSE precoding schemes with single-antenna receivers. *IEEE Commun. Lett.* **2012**, *16*, 1034–1037.
30. Lee, D.; Jang, Y.; Jung, M.; Choi, S. SCLNR-based precoding scheme for multi-user MIMO SWIPT systems. *IEEE Trans. Veh. Technol.* **2019**, *68*, 12392–12395. [CrossRef]
31. Souto, V.D.P.; Souza, R.D.; Uchoa-Filho, B.; Li, Y. Intelligent Reflecting Surfaces Beamforming Optimization with Statistical Channel Knowledge. *Sensors* **2022**, *22*, 2390. [CrossRef]
32. Wu, Q.; Zhang, R. Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5394–5409. [CrossRef]
33. Khanduzi, R.; Sangaiah, A.K. Tabu search based on exact approach for protecting hubs against jamming attacks. *Comput. Electr. Eng.* **2019**, *79*, 106459. [CrossRef]
34. An, K.; Lin, M.; Ouyang, J.; Zhu, W. Secure Transmission in Cognitive Satellite Terrestrial Networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 3025–3037. [CrossRef]
35. Sun, Y.; An, K.; Zhu, Y.; Zheng, G.; Wong, K.-K.; Chatzinotas, S.; Ng, D.W.K.; Guan, D. Energy-efficient hybrid beamforming for multi-layer RIS-assisted secure integrated terrestrial-aerial networks. *IEEE Trans. Commun.* **2022**, *70*, 4189–4210. [CrossRef]
36. An, K.; Liang, T.; Zheng, G.; Yan, X.; Li, Y.; Chatzinotas, S. Performance Limits of Cognitive-Uplink FSS and Terrestrial FS for Ka-Band. *IEEE Trans. Aerosp. Electron. Syst.* **2019**, *55*, 2604–2611. [CrossRef]
37. Zhou, G.; Pan, C.; Ren, H.; Wang, K.; Di Renzo, M.; Nallanathan, A. Robust beamforming design for intelligent reflecting surface aided miso communication systems. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1658–1662. [CrossRef]
38. Sun, Y.; An, K.; Luo, J.; Zhu, Y.; Zheng, G.; Chatzinotas, S. Outage Constrained Robust Beamforming Optimization for Multiuser IRS-Assisted Anti-Jamming Communications With Incomplete Information. *IEEE Internet Things J.* **2022**, *9*, 13298–13314. [CrossRef]
39. Schmidt, R. Multiple emitter location and signal parameter estimation. *IEEE Trans. Antennas Propag.* **1986**, *34*, 276–280. [CrossRef]

40. Lin, Z.; Lin, M.; Huang, Y.; Cola, T.d.; Zhu, W.-P. Robust multi-objective beamforming for integrated satellite and high altitude platform network with imperfect channel state information. *IEEE Trans. Signal Process.* **2019**, *67*, 6384–6396. [CrossRef]
41. Shi, W.; Ritcey, J. Robust beamforming for MISO wiretap channel by optimizing the worst-case secrecy capacity. In Proceedings of the 2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 7–10 November 2010; pp. 300–304.
42. Sadek, M.; Tarighat, A.; Sayed, A.H. A leakage-based precoding scherne for downlink multi-user MIMO channels. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 1711–1721. [CrossRef]
43. Mathworks. Available online: https://www.mathworks.com/help/matlab/ref/eigs.html?s_tid=doc_ta (accessed on 20 February 2023).