Article:
Wang, Wei, Hao, Xu, Wu, Lei et al. (2026) UAV-Mounted RIS-Assisted Legitimate Surveillance Over Maritime Low-Altitude Communication Networks. IEEE Transactions on Network Science and Engineering. pp. 6944-6957. ISSN: 2327-4697

https://doi.org/10.1109/TNSE.2026.3665466

UAV-Mounted RIS-Assisted Legitimate Surveillance Over Maritime Low-Altitude Communication Networks

Wei Wang, *Member, IEEE*, Xu Hao, Lei Wu, Feng Zeng, Nan Zhao, *Senior Member, IEEE*, Kanapathippillai Cumanan, *Senior Member, IEEE*, and Emil Björnson, *Fellow, IEEE*

***Abstract*—This paper considers a challenging maritime low-altitude surveillance issue, in which, a legitimate monitor UAV intends to overhear a suspicious UAV-vessel link with the help of a jammer UAV. Both the suspicious receiver has the jamming detection ability and the jammer UAV is energy-constrained. To address these challenges, we propose a novel UAV-mounted reconfigurable intelligent surface (RIS) assisted approach, where the RIS is deployed on the jammer UAV to create an additional surveillance channel towards the legitimate UAV. Furthermore, the jammer UAV can also intelligently adjust its power allocation and flight trajectory to covertly disturb the suspicious transmission with the detection thresholds and the energy budgets. In such a setup, we consider a sum eavesdropping rate maximization problem of the legitimate UAV during all time slots. This formulated problem is solved by jointly optimizing the three-dimensional (3D) trajectory of the legitimate UAV, the reflecting phase shifts of the RIS, as well as the 3D trajectory and jamming power of the jammer UAV under the mobility, covertness, and power limitation constraints. We decompose the non-convex design problem into three subproblems and propose an iterative algorithm to find its approximated optimal solution by using the block coordinate descent method. In each iteration, we utilize the successive convex approximation and phase alignment techniques to handle these subproblems. Numerical simulation results are provided to validate the effectiveness and tremendous potential of UAV-mounted RIS in the maritime low-altitude surveillance.**

***Index Terms*—Maritime low-altitude surveillance, UAV-mounted RIS, energy-constrained power allocation, cooperative jamming, trajectory design.**

I. Introduction

Nowadays, the rapid development of unmanned aerial vehicles (UAVs) has given rise to the new concept low-altitude economy (LAE) [1]–[4], which could support a wide variety of important applications, such as emergency rescue [5], [6], data collection [7], [8], communication coverage [9], [10], and integrated sensing and communications (ISAC) [11]–[13]. Although there have been many discussions on utilizing UAVs in LAE networks, most only focus on the terrestrial scenarios. Recently, with the surge in marine activities [14]–[17], UAVs have been introduced to assist various maritime low-altitude communication networks due to their on-demand deployment and flexible dispatch [18]–[22]. Despite the significant advantages and potential benefits brought by the maritime low-altitude UAVs, once they are maliciously used by criminals or terrorists, it will bring substantial risks to the maritime public safety. Hence, effective surveillance of the low-altitude UAV-enabled maritime communication networks is of paramount importance and a challenging issue.

A. Related Works

To date, as one of important methods of wireless surveillance, jamming-assisted proactive eavesdropping has been already widely applied to various suspicious communication scenarios [23]–[29]. Nevertheless, the aforementioned works mainly consider the static distributions of the legitimate monitor and the suspicious transmitter/receiver, which may not be suitable for dynamic maritime surveillance scenarios. Recently, UAV-assisted legitimate surveillance has been recognized as an effective approach for improving eavesdropping capabilities in highly dynamic environments. This is due to the fact that the UAV can flexibly adjust its flight trajectory to approach the suspicious transmitter or receiver. For example, in [30], the authors considered an intelligent eavesdropping scheme based on reinforcement learning, which can find the optimal monitoring location by learning during the movement. In [31], the authors studied a UAV-aided suspicious communication scenario, where the jamming power was optimized to enhance the eavesdropping efficiency. In [32], a UAV-aided proactive eavesdropping system was investigated, where the sum eavesdropping rate was maximized by jointly designing the UAVs position and power allocation. Moreover, a UAV-assisted relay surveillance system was studied in [33], where the UAV can simultaneously wiretap the suspicious information from the source and the relay. In [34], the authors employed a spoofing relay and a UAV eavesdropper to collaboratively eavesdrop on multiple suspicious links. In [35], a full-duplex (FD) UAV-enabled legitimate monitoring system

Wei Wang, Xu Hao and Feng Zeng are with the School of Information Science and Technology, Nantong University, Nantong 226019, China (e-mail:wwang2011@ntu.edu.cn, 2330310012@stmail.ntu.edu.cn, zengfeng@ntu.edu.cn).

Lei Wu is with the Electronic Information School, Wuhan University, Wuhan 430072, China (e-mail: 2024102120054@whu.edu.cn).

Nan Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: zhaonan@dlut.edu.cn).

Kanapathippillai Cumanan is with the School of Physics, Engineering and Technology, University of York, York YO10 5DD, U.K. (e-mail: kanapathippillai.cumanan@york.ac.uk).

Emil Björnson is with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm 16440, Sweden (e-mail: emilbjo@kth.se).

The work of X. Hao was supported by the Postgraduate Research & Practice Innovation Program of School of Information Science and Technology, Nantong University under Grant NTUSISTPR24_02. The work of K. Cumanan was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/X01309X/1. The work of E. Björnson was supported by the Vinnova through the SweWIN center under Grant 2023-00572. *(Corresponding author: Feng Zeng.)*

was considered, where the UAV can simultaneously transmit jamming signals and receive suspicious information. Later on, this FD UAV-aided surveillance scheme was extended to a multiple links scenario in [36], where the goal was to enhance the eavesdropping success probability by jointly designing the UAVs deployment and power allocations. In contrast to the above works only focused on the static scenarios, the authors in [37], [38] studied a mobile surveillance system, where a monitor UAV intended to intercept the suspicious communications from an UAV pair. In addition, multiple UAV-assisted legitimate surveillance scheme was investigated in [39], [40], where the surveillance performance was optimized by jointly designing the jamming power levels and the cooperative UAVs trajectories. However, when the legitimate UAVs move closer to the suspicious transmitter or receiver to improve eavesdropping performance, which may be easily detected by the malicious users, and thereby deteriorate the surveillance performance. To deal with this issue, the authors in [41]–[44] developed a covert surveillance scheme to overhear the suspicious stationary or moving targets, where the trajectories of UAVs were designed to disguise the purpose of surveillance. However, if the legitimate UAVs need to keep the large distance from the malicious users to remain undetected, which may not achieve a effective eavesdropping performance due to long-distance path loss.

To overcome this difficulty, reconfigurable intelligent surfaces (RIS), also referred to as intelligent reflecting surfaces (IRS), have been applied to improve the eavesdropping performance by reconfiguring the propagation environment [45]–[49]. For example, an RIS-assisted legitimate monitoring problem was first investigated in [50], where the RIS is mounted on the monitor to constructively/destructively forward signals. In [51], the authors considered an RIS-aided proactive eavesdropping system, where a deep reinforcement learning scheme was developed to derive the optimal reflective beamforming strategy. Further, a robust RIS-assisted wireless surveillance system was considered in [52], in which a joint design of the RIS phase shifts and the legitimate receiver beamformer was proposed. In [53], a double-RIS enabled proactive eavesdropping problem was investigated, where the surveillance performance was optimized by jointly designing the double-RIS reflective phase shifts. In addition, different from the prior passive RIS, an active RIS was introduced to assist legitimate surveillance in [54]. This is because the active RIS can simultaneously adjust the reflective phase and amplify the signal amplitude. However, the works in [50]–[54] only considered silent eavesdroppers without jamming assistance. To achieve more efficient eavesdropping, the authors in [55] proposed an RIS-enabled proactive eavesdropping scheme, where the RIS was employed to collaboratively reflect the jamming signals. In [56], the authors considered an RIS-assisted proactive eavesdropping system, where the active jamming and passive reflection beamforming were jointly optimized to minimize the jamming power. In [57], an RIS-aided wireless surveillance network was investigated, in which a joint design of the RIS deployment strategy, the receive and jamming beamforming vectors was proposed. Moreover, in [58], the authors studied a hybrid reflecting-backscatter intelligent surface enabled legitimate surveillance system, where some elements of RIS are used to reflect the suspicious information while the remaining send jamming signals through backscatter techniques. Later on, this hybrid reflecting-backscatter surveillance scheme was extended to a double-RIS-assisted proactive eavesdropping scenario in [59], where the goal was to enhance the effective eavesdropping rate by jointly optimizing the reflection coefficients at two RISs. In addition, the authors in [60]–[63] considered a simultaneously transmitting and reflecting RIS (STAR-RIS)-aided proactive eavesdropping over the suspicious onehop or multihop links, where the STAR-RIS can adjust its functions to balance the channel gains of the suspicious and eavesdropping link. However, the authors in [50]–[63] only considered the static scenarios, i.e., the locations of monitor, RIS and suspicious transmitter/receiver are fixed. Additionally, the above works all assumed that the eavesdropper cannot be discovered by the suspicious users, which is not a realistic assumption. Therefore, in [64], an RIS-aided UAV-enabled eavesdropping scheme with a safety distance constraint was proposed, where the surveillance performance was optimized by jointly designing the the UAV trajectory and RIS configuration.

However, the aforementioned works, e.g., [50]–[64], only assumed that the RIS is used as a fixed anchor, which may not achieve a better eavesdropping performance in the mobile surveillance environments. More importantly, it is challenging to deploy the RIS at the appropriate location in oceans due to the geographically limited sites. Besides, the works in [30]–[44], [50]–[64] all assumed that the malicious users do not react to the eavesdropping attack from the monitor ([41], [42], [64] only considered the safety distance constraint), which is an impractical assumption and may result in significant degradation of eavesdropping performance. This is because if the suspicious users detect the eavesdropping attack, they will inform each other and terminate the transmission, and thereby degrade the surveillance performance. To address this issue, the authors in [65] proposed a machine learning algorithm for the detection of active eavesdropping attacks at the suspicious transmitter. In [66], the authors considered a jamming-assisted suspicious communications system, where the jammer can send jamming signals to protect the suspicious transmission. Moreover, in [67], a covert proactive surveillance scheme was proposed to improve eavesdropping performance, where the suspicious users have the detection ability of the artificial noise. However, the authors in [65]–[67] only considered static surveillance scenarios. In addition, the above mentioned works mainly focused on terrestrial scenarios [30]–[44], [50]–[67], which differ substantially from maritime wireless surveillance environments. This is because the suspicious users in the maritime scenario, unlike them in the terrestrial settings with static deployments and random distributions, are typically clustered on vessels, which are sparsely distributed and move

TABLE I
COMPARISON OF THIS PAPER WITH OTHER REPRESENTATIVE WORKS

References	Main idea	Limitations vs. our work
[39], [40]	Multiple UAVs cooperative eavesdropping; joint UAVs trajectories and jamming powers optimization.	It is easily detected by the malicious users; not suitable for jamming detection scenarios.
[41]–[44]	Multi-UAVs covert surveillance; optimize UAVs trajectories to disguise the purpose of surveillance.	Relying on the covert distance constraints; difficult to improve eavesdropping performance.
[64]	RIS-assisted UAV-enabled proactive eavesdropping; joint UAV+RIS collaborative design.	Only considering the safety distance constraints and the static suspicious transmission.
[67]	The suspicious receiver is capable of detecting artificial noise; covert surveillance under channel uncertainty.	Assumes the static distributions of the legitimate monitor and the suspicious transmitter/receiver.
[68]	Joint UAV and USV-aided maritime cooperative surveillance; suitable for maritime scenarios.	Low efficiency; only considering the safety distance constraint and USV's trajectory optimization.
[69]	Energy-constrained UAV jamming power allocation; joint UAV+vessel trajectories design.	Not involving the suspicious users with the jamming detection ability.
Our work	UAV-mounted RIS-assisted maritime low-altitude surveillance; UAVs 3D trajectories, RIS phase shifts and jamming power allocation co-design.	Suitable for jamming detection and energy-constrained scenarios; covertly disturb the suspicious transmission, and simultaneously enhance the eavesdropping efficiency as well as save the jamming power.

along predefined sailing routes. Furthermore, in contrast to the terrestrial jammer, it is difficult for the maritime jammer (e.g. UAV) to replenish energy on the ocean, its jamming power allocation need be carefully designed to improve the eavesdropping efficiency. Recently, some initial works (e.g., [68], [69]) have investigated the effective surveillance of UAV-enabled maritime suspicious communications. The authors proposed a jammer UAV-assisted maritime cooperative surveillance scheme for suspicious vessels links in [68], where the goal was to improve monitoring efficiency by optimizing the USV's trajectory. Moreover, in [69], the authors considered a maritime legitimate surveillance system, where the legitimate monitor vessel tried to overhear a suspicious UAV-vessel communication link with the help of a jammer UAV. Yet, these works all assumed that the jamming attack cannot be detected by the suspicious users, and thus, the results will not be suitable in practical surveillance environments with the jamming detection ability. To differentiate this work from existing works in the research area, a comparative analysis of various representative works is summarized in Table I.

B. Motivations and Contributions

Motivated by these challenges, this paper studies a new maritime low-altitude surveillance system, in which, a legitimate monitor UAV intends to eavesdrop a suspicious UAV-vessel communication link with the help of a jammer UAV. In particular, we consider a practical scenario where the suspicious receiver has the jamming detection ability and the jammer UAV is energy-constrained. To tackle these challenges, we propose a jammer UAV-mounted RIS enabled approach, where the jammer UAV can covertly send the jamming signals to the suspicious receiver while the deployed RIS also can potentially create a surveillance channel towards the legitimate UAV. Our objective is to jointly design the jammer UAV three-dimensional (3D) trajectory and power allocation, the legitimate UAV 3D trajectory, and the RIS's reflecting phase shifts for maximizing the sum eavesdropping rate over all time slots. The main contributions are summarized as follows:

$(\mathbf{1})$ We consider a novel maritime legitimate surveillance system, where a monitor UAV eavesdrops a suspicious UAV-vessel pair with the help of a jammer UAV. Different from the previous works, we assume that the suspicious receiver has the jamming detection ability and the jammer UAV is energy-constrained. Specifically, we propose a UAV-mounted RIS enabled approach, where the RIS is deployed on the jammer UAV to create a surveillance channel towards the legitimate UAV by configuring the radio environments. Meanwhile, the jammer UAV also can intelligently adjust its power allocation to disturb the suspicious transmission with the detection thresholds and the energy budgets.

$(\mathbf{2})$ We formulate an optimization problem that jointly designs the 3D trajectory of the legitimate UAV, the reflecting phase shifts of RIS, as well as the 3D trajectory and power allocation of the jammer UAV under the detection thresholds and the energy budgets constraints. Compared to the existing works on UAV-enabled legitimate surveillance [39], [64], [68], [69], the proposed UAV-mounted RIS scheme cannot only covertly confuse the malicious users, but also can simultaneously enhance the eavesdropping efficiency and save the jamming power, which is more suitable for practical maritime surveillance environments.

$(\mathbf{3})$ We decompose the non-convex formulated problem into three subproblems and then transform them into more tractable forms by using successive convex approximation and phase alignment methods, respectively. Next, we propose an iterative algorithm that alternately solve these equivalently subproblems by utilizing the block coordinate descent (BCD) technique. In each iteration, we derive closed-form solutions of the reflecting phase shifts, the jamming power and 3D flight trajectories. Additionally, we develop a novel optimal power allocation algorithm for the energy-constrained cases to improve the energy efficiency.

$(\mathbf{4})$ We discuss the convergence and the complexity of the proposed joint design, and verify the system performance based on the simulation results. Moreover, we demonstrate that for the surveillance scenario with the artificial noise detec-

TABLE II
LIST OF SYMBOLS.

Symbol	Description
M	RIS Reflecting Elements
T	Flight period of UAVs
d_t	Length of each time slot
$\mathbf{q}_a[n]$	Horizontal location of node a
$z_a[n]$	Vertical location of node a
$d_{ab}[n]$	Distance between a and b
d_{min}	Minimum security distance of UAVs
$p_J[n]$	Jamming power from J
$p_S[n]$	Transmit power from S
p_{total}	Total jamming power
p_{peak}	Peak jamming power
σ^2_{cov}	Artificial noise detection threshold
$d_{\{Smin,Dmin\}}$	Minimum safety distance from the suspicious users
$\mathrm{g}_{ab}[n]$	Large-scale channel coefficient between a and b
$\tilde{\mathrm{h}}_{ab}[n]$	Small-scale fading coefficient between a and b
$k[n]$	Rician factor
β_0	Channel power gain at a reference distance
$\mathbf{\Phi}[n]$	Phase shift matrix of the RIS
$\sigma^2_{\{D,E\}}$	Variance of the additive white Gaussian noise
$R_{\{D,E\}}[n]$	Achievable rate at the D and E
$R_{EE}[n]$	Effective eavesdropping rate
$\phi_{SJ}[n]$	Cosine of the angle of arrival from S to J
$\phi_{JE}[n]$	Cosine of the angle of departure from J to E
$\Gamma_{\{SE,JE,SJ,JD\}}$	Lower bound of small-scale fading
Γ_{SD}	Upper bound of small-scale fading
$R^{lb}_E[n]$	Lower bound of $R_E[n]$
$R^{ub}_D[n]$	Upper bound of $R_D[n]$

tion ability, the proposed UAV-mounted RIS enabled approach can simultaneously enhance the eavesdropping performance and save the power consumption compared to the existing works in the literature. In addition, when the energy budget is limited, we observe that the proposed optimal jamming policy can obtain the higher energy efficiency over the conventional power allocation scheme.

The rest of this paper is organized as follows. Section II provides the system model and problem formulation. The original optimization problem is decomposed into three subproblems and proposes an iterative algorithm in Section III to yield an approximated optimal solution. In Section IV, simulation results are presented and discussed, and finally, the work is concluded in Section V.

Notations: Boldface lowercase and uppercase letters denote vectors and matrices, respectively. $(\cdot)^H$, $||\cdot||$, $|\cdot|$ and $\mathbb{E}(\cdot)$ represent the conjugate transpose, Euclidean norm, absolute value and statistical expectation, respectively. Moreover, $\mathcal{CN}(0,\sigma^2)$ indicates the complex Gaussian distribution with zero mean and σ^2 variance. A list of symbols used in this paper is presented in Table II.

II. System Model and Problem Formulation

As shown in Fig. 1, we consider a maritime low-altitude surveillance system assisted by the UAV-mounted RIS, where an eavesdropper UAV E intends to overhear the suspicious transmission from a UAV-vessel link (S-D) with the help of a jammer UAV J. Specifically, the RIS is deployed on the UAV J to create an additional surveillance channel towards the UAV E by configuring the radio environments. Moreover, we consider a practical scenario where the suspicious receiver

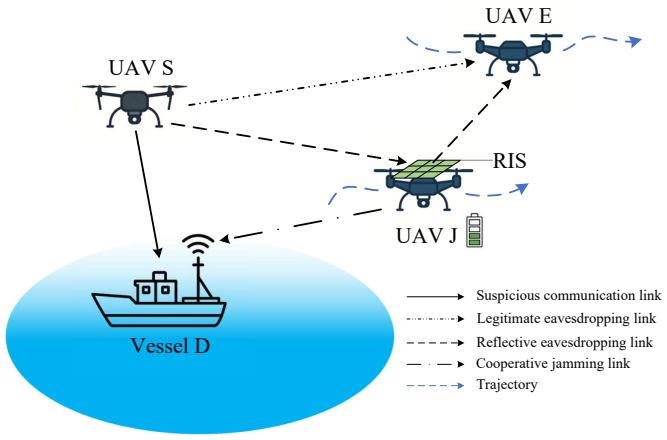


Fig. 1. Energy-constrained UAV-mounted RIS enabled maritime legitimate surveillance system.

D has the artificial noise detection ability and the jammer UAV J is energy-constrained, thus the jamming power allocation of the UAV J on the ocean need be carefully designed to improve the eavesdropping efficiency. In this surveillance system, it is assumed that both the UAVs and vessel are mounted with a single antenna, while the RIS consists of M reflecting elements. Furthermore, the ships in the maritime often move along predefined lanes and large-scale channel state information (CSI) is available.[1] For ease of exposition, we discretize the UAVs flying duration T into N time slots with equal length $d_t = T/N$, where $\mathcal{N} \triangleq \{1, 2, \cdots, N\}$. Moreover, let the coordinates $(\mathbf{q}_S[n], z_S[n])$, $\mathbf{q}_S[n] = (x_S[n], y_S[n])$, and $(\mathbf{q}_D[n], 0)$, $\mathbf{q}_D[n] = (x_D[n], y_D[n])$ represent the locations of the UAV S and vessel D, respectively. In addition, we denote the UAV E and J coordinates as $(\mathbf{q}_E[n], z_E[n])$ and $(\mathbf{q}_J[n], z_J[n])$, respectively, where $\mathbf{q}_E[n] = (x_E[n], y_E[n])$ and $\mathbf{q}_J[n] = (x_J[n], y_J[n])$. Accordingly, for any $n \in \mathcal{N}$, the low-altitude UAV obeys the following mobility constraints:

$$||\mathbf{q}_i[n+1] - \mathbf{q}_i[n]|| \leq v_{ih} d_t, \tag{1a}$$

$$|z_i[n+1] - z_i[n]| \leq v_{iv} d_t, \tag{1b}$$

$$z_{min} \leq z_i[n] \leq z_{max}, \tag{1c}$$

where v_{ih} and v_{iv} represent the maximum horizontal and vertical speed, $i \in \{E, J\}$, and z_{max} and z_{min} indicate the maximum and minimum flight altitude of UAVs, respectively. Furthermore, since the RIS was mounted on top of the UAV J to create an additional surveillance channel towards the UAV E, their flight altitudes also need to satisfy the following set of constraints:

$$\min\{z_S[n], z_E[n]\} \geq z_J[n] + z_{mhd}, \forall n, \tag{2}$$

where z_{mhd} represents the minimum height difference. Moreover, to prevent potential collisions between UAV E and

[1]This is typical for ocean scenarios [19]–[21], [69]–[71], where the positions of mobile ships can be obtained via the maritime Automatic Identification System (AIS) and be used as the prior information.

UAV J, the following minimum flight distance constraint is imposed:

$$d_{EJ}[n] \geq d_{min}, \forall n \in \mathcal{N} \tag{3}$$

where $d_{ij}[n] = \sqrt{||\mathbf{q}_i[n] - \mathbf{q}_j[n]||^2 + |z_i[n] - z_j[n]|^2}$ denotes the distance from i to j, and d_{min} indicates the minimum anti-collision distance.

Since the UAVs have difficulty to replenish energy on the ocean, the jamming power $p_J[n]$ of the UAV J should obey the following constraints:

$$\sum_{n=1}^{N} p_J[n] \leq p_{total}, \tag{4a}$$

$$0 \leq p_J[n] \leq p_{peak}, \tag{4b}$$

where p_{total} and p_{peak} indicate the total and the peak jamming power, respectively. Furthermore, if the legitimate UAVs move close to the suspicious users, they may be easily detected and resulting in failed surveillance missions. Therefore, we impose the following minimum distance constraints:

$$d_{iS}[n] \geq d_{Smin}, \tag{5a}$$

$$d_{iD}[n] \geq d_{Dmin}, \tag{5b}$$

where $i \in \{E, J\}$, and d_{Smin} and d_{Dmin} denote the minimum safety distance from the suspicious users, respectively. Moreover, different from the previous works, we also assume that the suspicious users have the jamming detection ability, i.e., if the vessel D detects the artificial noise power beyond the threshold, it will inform the UAV S to stop transmitting. Hence, for any $n \in \mathcal{N}$, the transmit power $p_J[n]$ of the UAV J should also obey the following covertness constraints:

$$0 \leq p_J[n] \leq p_{cov}[n], \tag{6}$$

where $p_{cov}[n] = \frac{\sigma_{cov}^2 - \sigma_D^2}{|h_{JD}[n]|^2}$, $h_{JD}[n]$ denotes the channel coefficients between the UAV J and the vessel D, and σ_{cov}^2 and σ_D^2 represent the artificial noise detection threshold and the receiver noise power at D, respectively. Thus, the constraint (4b) can be further expressed as

$$0 \leq p_J[n] \leq \min\{p_{cov}[n], p_{peak}\}, \forall n. \tag{7}$$

In addition to these constraints, due to the sea wave movement and the ocean scattering, a practical maritime channel model including both line-of-sight (LoS) and non-line-of-sight (NLoS) effects is employed [19]–[21], [69]. Accordingly, the channel coefficients at time n are defined as

$$\begin{aligned} h_{ij}[n] &= g_{ij}[n] \cdot \widetilde{h}_{ij}[n] \\ &= \sqrt{\frac{\beta_0}{d_{ij}^2[n]}} \cdot \left(\sqrt{\frac{k[n]}{1+k[n]}} + \sqrt{\frac{1}{1+k[n]}} \kappa_{ij} \right), \end{aligned} \tag{8}$$

where $g_{ij}[n]$ and $\widetilde{h}_{ij}[n]$ denote the large-scale and small-scale fading coefficients, respectively, $i, j \in \{S, D, E, J\}$. The symbol $\kappa_{ij} \in \mathcal{CN}(0, 1)$, β_0 represents the channel power gain at a reference distance of 1 m, and $k[n]$ denotes the Rician factor[2]. Based on this channel model, since the RIS and the emitting antenna were mounted on the top and bottom of the UAV J, the received signal at the UAV E and the vessel D can be expressed respectively as[3]

$$y_E[n] = x_S[n] h_{SE}[n] + x_S[n] \boldsymbol{h}_{JE}^H[n] \boldsymbol{\Phi}[n] \boldsymbol{h}_{SJ}[n] + n_E[n], \tag{9}$$

and

$$y_D[n] = x_S[n] h_{SD}[n] + x_J[n] h_{JD}[n] + n_D[n], \tag{10}$$

where $x_S[n]$ and $x_J[n]$ indicate the transmit signal from S and J, and $n_E[n] \sim \mathcal{CN}(0, \sigma_E^2)$ and $n_D[n] \sim \mathcal{CN}(0, \sigma_D^2)$ represent the receiver noise at the E and D, respectively. The symbol $\boldsymbol{\Phi}[n] = \mathrm{diag}(e^{j\theta_1[n]}, e^{j\theta_2[n]}, \cdots, e^{j\theta_M[n]})$, $\theta_m[n] \in [0, 2\pi]$, is the phase shift matrix of the RIS. Therefore, at time slot $n \in \mathcal{N}$, the achievable rate at the E and D can be derived respectively as

$$R_E[n] = \log_2 \left(1 + \frac{p_S[n] |h_{SE}[n] + \boldsymbol{h}_{JE}^H[n] \boldsymbol{\Phi}[n] \boldsymbol{h}_{SJ}[n]|^2}{\sigma_E^2} \right), \tag{11}$$

and

$$R_D[n] = \log_2 \left(1 + \frac{p_S[n] h_{SD}^2[n]}{\sigma_D^2 + p_J[n] h_{JD}^2[n]} \right), \tag{12}$$

where $p_S = \mathbb{E}(|x_S|^2)$ and $p_J = \mathbb{E}(|x_J|^2)$.

In practice, if and only if $R_E[n] \geq R_D[n]$, the UAV E can decode the suspicious information without distortion [23]–[29]. Thus, the effective eavesdropping rate can be defined as

$$R_{EE}[n] = \begin{cases} R_D[n], & R_E[n] \geq R_D[n], \\ 0, & R_E[n] < R_D[n]. \end{cases} \tag{13}$$

Under the above setting, we consider a maritime low-altitude eavesdropping system assisted by the energy-constrained UAV-mounted RIS, where the sum eavesdropping rate is maximized by jointly designing the 3D trajectory of the legitimate UAV, the reflecting phase shifts of the RIS, as well as the 3D trajectory and jamming power of the jammer

[2]The $k[n]$ is the ratio between the LoS power and the scattering power, which can be determined from the historical data of AIS [19]–[21], [69].

[3]This is because the RIS only reflect the signal from its front half-space, meanwhile, the jamming signal is known to the legitimate eavesdropper, which can be eliminated at the E [20], [69].

UAV. This optimization problem can be formulated as

$$\begin{aligned}\max_{\substack{\{\mathbf{q}_E[n],z_E[n]\},\mathbf{\Phi}[n],\\ p_J[n],\{\mathbf{q}_J[n],z_J[n]\}}} & \sum_{n=1}^{N} R_{EE}[n]\\ \text{s.t. } C1:\ & ||\mathbf{q}_i[n+1]-\mathbf{q}_i[n]|| \le v_{ih}d_t, i\in\{E,J\},\forall n,\\ C2:\ & |z_i[n+1]-z_i[n]| \le v_{iv}d_t, i\in\{E,J\},\forall n,\\ C3:\ & z_{min}\le z_i[n]\le z_{max}, i\in\{E,J\},\forall n,\\ C4:\ & \min\{z_S[n],z_E[n]\} > z_J[n]+z_{mhd},\forall n,\\ C5:\ & d_{EJ}[n]\ge d_{min},\forall n,\\ C6:\ & d_{iS}[n]\ge d_{Smin}, i\in\{E,J\},\forall n,\\ C7:\ & d_{iD}[n]\ge d_{Dmin}, i\in\{E,J\},\forall n,\\ C8:\ & \sum_{n=1}^{N} p_J[n]\le p_{total},\forall n,\\ C9:\ & 0\le p_J[n]\le \min\{p_{cov}[n],p_{peak}\},\forall n,\\ C10:\ & 0\le\theta_m[n]\le 2\pi,\forall m,n,\end{aligned} \tag{14}$$

where C1−C3 are the mobility constraints of UAVs and C4 is the mounting height constraint of the RIS. The constraint C5 is the anti-collision constraint between the UAV E and UAV J, the constraints C6 and C7 represent the safety distance constraint from the suspicious users, respectively. Moreover, the constraints C8 and C9 denote the power-limited and covert jamming constraint of the UAV J, respectively. The constraint C10 is the RIS phase shifts constraint.

Since the variables $\{\mathbf{q}_E[n], z_E[n], \mathbf{\Phi}[n], p_J[n], \mathbf{q}_J[n], z_J[n]\}$ are coupled in the objective function and constraints, it is highly complicated to determine the global optimal solution for problem (14). Thus, to circumvent this non-convexity issue, a computationally efficient iterative algorithm is proposed to yield a feasible solution for problem (14).

III. Proposed Iterative Algorithm

To efficiently solve the non-convex problem (14), in this section, we first decompose the original problem into three subproblems and then resort to the BCD technique to obtain an approximated optimal solution, i.e., alternately optimizing the variables $\{\mathbf{\Phi}[n], \mathbf{q}_J[n], z_J[n]\}$, $\{\mathbf{q}_E[n], z_E[n]\}$ and $p_J[n]$ while the remaining ones are fixed.

A. Joint optimization of the UAV J trajectory $\{\mathbf{q}_J[n], z_J[n]\}$ and RIS phase shifts $\mathbf{\Phi}[n]$

With any given UAV E trajectory $\{\mathbf{q}_E[n], z_E[n]\}$ and jamming power $p_J[n]$, the original non-convex problem (14) reduces to the following form :

$$\begin{aligned}\max_{\mathbf{\Phi}[n],\{\mathbf{q}_J[n],z_J[n]\}} & \sum_{n=1}^{N} R_{EE}[n]\\ \text{s.t. } C1:\ & ||\mathbf{q}_J[n+1]-\mathbf{q}_J[n]|| \le v_{Jh}d_t,\forall n,\\ C2:\ & |z_J[n+1]-z_J[n]| \le v_{Jv}d_t,\forall n,\\ C3:\ & z_{min}\le z_J[n]\le z_{max},\forall n,\\ C4:\ & \min\{z_S[n],z_E[n]\} > z_J[n]+z_{mhd},\forall n,\\ C5:\ & d_{EJ}[n]\ge d_{min},\forall n,\\ C6:\ & d_{JS}[n]\ge d_{Smin},\forall n,\\ C7:\ & d_{JD}[n]\ge d_{Dmin},\forall n,\\ C8:\ & 0\le\theta_m[n]\le 2\pi,\forall m,n.\end{aligned} \tag{15}$$

Since the RIS was mounted on top of the UAV J to enhance the received signal at the UAV E, for any $\{\mathbf{q}_J[n], z_J[n]\}$ in (15), we only have to align the phases to the UAV E to guarantee $R_E[n] \ge R_D[n]$ at more time slots. Hence, to maximize the objective function in (15), we first set

$$\begin{aligned}\theta_1[n] =& \theta_2[n] + \frac{2\pi d}{\lambda}(\phi_{JE}[n]-\phi_{SJ}[n])\\ &\vdots\\ =& \theta_M[n] + \frac{2\pi(M-1)d}{\lambda}(\phi_{JE}[n]-\phi_{SJ}[n])\\ =& \omega,\end{aligned} \tag{16}$$

where $\phi_{SJ}[n] = \frac{x_J[n]-x_S[n]}{d_{SJ}[n]}$ and $\phi_{JE}[n] = \frac{x_E[n]-x_J[n]}{d_{JE}[n]}$ denote the cosine of the angle of arrival and departure of the signal from S to J and J to E, respectively. The symbol ω represents an arbitrary phase shift with $\omega \in [0, 2\pi]$. Accordingly, the optimal phase shift of the m-th element in time slot n can be derived as follow:

$$\theta_m^*[n] = \omega + \frac{2\pi(m-1)d}{\lambda}(\phi_{JE}[n]-\phi_{SJ}[n]), \tag{17}$$

Then, according to the optimal values $\theta_m^*[n]$ in (17), problem (15) is recast as

$$\begin{aligned}\max_{\{\mathbf{q}_J[n],z_J[n]\}} & \sum_{n=1}^{N} R_{EE}[n]\\ \text{s.t. } & C1-C7.\end{aligned} \tag{18}$$

However, problem (18) is challenging to directly solve due to the coupled variables $\{\mathbf{q}_J[n], z_J[n]\}$ in both numerator and denominator of $R_E[n]$ and $R_D[n]$. Moreover, it is obvious that the optimization of the UAV J trajectory $\{\mathbf{q}_J[n], z_J[n]\}$ will simultaneously affect the eavesdropping rate $R_E[n]$ and the suspicious rate $R_D[n]$. Therefore, to maximize the objective function in (18), i.e., it is required to satisfy $R_E[n] \ge R_D[n]$ at more time slots n, problem (18) can be equivalently reformulated as

$$\begin{aligned}\max_{\{\mathbf{q}_J[n],z_J[n]\}} & \sum_{n=1}^{N} R_E[n]-R_D[n]\\ \text{s.t. } & C1-C7.\end{aligned} \tag{19}$$

To solve problem (19), by substituting (17) into (11), the eavesdropping rate $R_E[n]$ can be rewritten as

$$\begin{aligned} R_E[n]&=\mathbb{E}\left\{\log_2\left(1+\frac{p_S[n]|h_{SE}[n]+h_{JE}[n]h_{SJ}[n]Me^{jw}|^2}{\sigma_E^2}\right)\right\} \\ &\geq \log_2\left(A_1[n]+\frac{A_2[n]}{d_{SJ}^2[n]d_{JE}^2[n]}+\frac{A_3[n]}{d_{SJ}[n]d_{JE}[n]}\right)=R_E^{lb}[n], \end{aligned} \tag{20}$$

where $A_1[n]=1+\frac{p_S[n]\beta_0\Gamma_{SE}}{\sigma_E^2 d_{SE}^2[n]}$, $A_2[n]=\frac{p_S[n]\beta_0^2\Gamma_{JE}\Gamma_{SJ}M^2}{\sigma_E^2}$, $A_3[n]=\frac{2p_S[n]\beta_0^{\frac{3}{2}}\Gamma_{SE}\Gamma_{JE}\Gamma_{SJ}M}{\sigma_E^2 d_{SE}[n]}$. The symbols Γ_{SE}, Γ_{JE} and Γ_{SJ} denote the lower bound on the corresponding small-scale fading, respectively [19]–[21], [69], and $R_E^{lb}[n]$ indicates the lower bound of $R_E[n]$. Similarly, we can derive the upper bound on the suspicious communication rate R_D as follows:

$$\begin{aligned} R_D[n]&=\mathbb{E}\left\{\log_2\left(1+\frac{p_S[n]h_{SD}^2[n]}{\sigma_D^2+p_J[n]h_{JD}^2[n]}\right)\right\}, \\ &\leq \log_2\left(1+\frac{B_1[n]}{\sigma_D^2+\frac{B_2}{d_{JD}^2[n]}}\right)=R_D^{ub}[n], \end{aligned} \tag{21}$$

where $B_1[n]=\frac{p_S[n]\beta_0\Gamma_{SD}}{d_{SD}^2[n]}$, $B_2[n]=p_J[n]\beta_0\Gamma_{JD}$. The symbols Γ_{SD} and Γ_{JD} represent the upper and lower bound on the corresponding small-scale fading, respectively, and $R_D^{ub}[n]$ denotes the upper bound of $R_D[n]$. Then, based on (20) and (21), by defining the slack variables $r[n]$ and $s[n]$, problem (19) is equivalently transformed into the following form:

$$\begin{aligned} \max_{\{\mathbf{q}_J[n],z_J[n]\}} &\sum_{n=1}^{N}\log_2\left(A_1[n]+\frac{A_2[n]}{r[n]s[n]}+\frac{A_3[n]}{(r[n]s[n])^{\frac{1}{2}}}\right) \\ &-\log_2\left(1+\frac{B_1[n]}{\sigma_D^2+\frac{B_2}{d_{JD}^2[n]}}\right), \\ \text{s.t. } & r[n]\geq d_{SJ}^2[n],\forall n, \\ & s[n]\geq d_{JE}^2[n],\forall n, \\ & C1-C7. \end{aligned} \tag{22}$$

To efficiently solve problem (22), we provide the following proposition.

Proposition 1: Function $\log_2\left(A_1[n]+\frac{A_2[n]}{r[n]s[n]}+\frac{A_3[n]}{(r[n]s[n])^{\frac{1}{2}}}\right)$ is convex with respect to $r[n]$ and $s[n]$.

Proof: Please refer to Appendix A. ■

From Proposition 1, by the first-order Taylor series expansions, we have

$$\begin{aligned} &\log_2\left(A_1[n]+\frac{A_2[n]}{r[n]s[n]}+\frac{A_3[n]}{(r[n]s[n])^{\frac{1}{2}}}\right) \\ &\geq \log_2 A_4[n]-\left(\frac{A_2[n]}{\widetilde{r}^2[n]\widetilde{s}[n]}+\frac{\frac{1}{2}A_3[n]}{\widetilde{r}^{\frac{3}{2}}[n]\widetilde{s}^{\frac{1}{2}}[n]}\right)\frac{r[n]-\widetilde{r}[n]}{\ln 2\ A_4[n]} \\ &\quad-\left(\frac{A_2[n]}{\widetilde{r}[n]\widetilde{s}^2[n]}+\frac{\frac{1}{2}A_3[n]}{\widetilde{r}^{\frac{1}{2}}[n]\widetilde{s}^{\frac{3}{2}}[n]}\right)\frac{s[n]-\widetilde{s}[n]}{\ln 2\ A_4[n]}, \end{aligned} \tag{23}$$

where $A_4[n]=A_1[n]+\frac{A_2[n]}{\widetilde{r}[n]\widetilde{s}[n]}+\frac{A_3[n]}{\widetilde{r}^{\frac{1}{2}}[n]\widetilde{s}^{\frac{1}{2}[n]}}$, and $\widetilde{r}[n]$ and $\widetilde{s}[n]$ represent the l-th feasible solutions. As a result, substituting (23) into (22) yields

$$\begin{aligned} \max_{\{\mathbf{q}_J[n],z_J[n]\}} &\sum_{n=1}^{N}-\left(\frac{A_2[n]}{\widetilde{r}^2[n]\widetilde{s}[n]}+\frac{\frac{1}{2}A_3[n]}{\widetilde{r}^{\frac{3}{2}}[n]\widetilde{s}^{\frac{1}{2}}[n]}\right)\frac{r[n]-\widetilde{r}[n]}{\ln 2\ A_4[n]} \\ &-\left(\frac{A_2[n]}{\widetilde{r}[n]\widetilde{s}^2[n]}+\frac{\frac{1}{2}A_3[n]}{\widetilde{r}^{\frac{1}{2}}[n]\widetilde{s}^{\frac{3}{2}}[n]}\right)\frac{s[n]-\widetilde{s}[n]}{\ln 2\ A_4[n]} \\ &-\log_2\left(1+\frac{B_1[n]}{\sigma_D^2+\frac{B_2}{||\mathbf{q}_J[n]-\mathbf{q}_D[n]||^2+|z_J[n]-z_D[n]|^2}}\right), \\ \text{s.t. } & r[n]\geq ||\mathbf{q}_J[n]-\mathbf{q}_S[n]||^2+|z_J[n]-z_S[n]|^2,\forall n, \\ & s[n]\geq ||\mathbf{q}_J[n]-\mathbf{q}_E[n]||^2+|z_J[n]-z_E[n]|^2,\forall n, \\ & C1-C7. \end{aligned} \tag{24}$$

The problem (24) is convex and can be efficiently tackled by the interior-point method [20], [21], [69], [72].

B. Optimization of the UAV E trajectory $\{\mathbf{q}_E[n], z_E[n]\}$

For given $\mathbf{\Phi}[n]$, $\{\mathbf{q}_J[n], z_J[n]\}$ and $p_J[n]$, the problem defined in (14) can be rewritten as

$$\begin{aligned} \max_{\{\mathbf{q}_E[n],z_E[n]\}} &\sum_{n=1}^{N}R_{EE}[n] \\ \text{s.t. } & C1: ||\mathbf{q}_E[n+1]-\mathbf{q}_E[n]||\leq v_{Eh}d_t,\forall n, \\ & C2: |z_E[n+1]-z_E[n]|\leq v_{Ev}d_t,\forall n, \\ & C3: z_{min}\leq z_E[n]\leq z_{max},\forall n, \\ & C4: \min\{z_S[n],z_E[n]\}>z_J[n]+z_{mhd},\forall n, \\ & C5: d_{EJ}[n]\geq d_{min},\forall n, \\ & C6: d_{ES}[n]\geq d_{Smin},\forall n, \\ & C7: d_{ED}[n]\geq d_{Dmin},\forall n. \end{aligned} \tag{25}$$

Based on the definition of the effective eavesdropping rate in (13), for each time n in (25), optimizing the UAV E trajectory will not change the suspicious communication rate $R_D[n]$. Thus, if we want the objective function in (25) to increase, the UAV E will need to guarantee $R_E[n]\geq R_D[n]$ at more time slots n. Accordingly, problem (25) is equivalently converted as

$$\begin{aligned} \max_{\{\mathbf{q}_E[n],z_E[n]\}} &\sum_{n=1}^{N}R_E[n] \\ \text{s.t. } & C1-C7. \end{aligned} \tag{26}$$

To make problem (26) more tractable, we first derive a lower bound of $R_E[n]$ as follows:

$$\begin{aligned} R_E[n]&=\mathbb{E}\left\{\log_2\left(1+\frac{p_S[n]|h_{SE}[n]+h_{JE}[n]h_{SJ}[n]Me^{jw}|^2}{\sigma_E^2}\right)\right\} \\ &\geq \log_2\left(1+\frac{D_1[n]}{d_{SE}^2[n]}+\frac{D_2[n]}{d_{JE}^2[n]}+\frac{D_3[n]}{d_{SE}[n]d_{JE}[n]}\right), \end{aligned} \tag{27}$$

where $D_1[n] = \frac{p_S[n]\beta_0\Gamma_{SE}}{\sigma_E^2}$, $D_2[n] = \frac{p_S[n]\beta_0^2\Gamma_{JE}\Gamma_{SJ}M^2}{\sigma_E^2 d_{SJ}^2[n]}$, $D_3[n] = \frac{2p_S[n]\beta_0^{\frac{3}{2}}\Gamma_{SE}\Gamma_{JE}\Gamma_{SJ}M}{\sigma_E^2 d_{SJ}[n]}$. Then, by substituting (27) into (26) and introducing the slack variables $u[n]$ and $v[n]$, problem (26) reduces to an equivalent form as

$$\begin{aligned}\max_{\{\mathbf{q}_E[n],z_E[n]\}} &\sum_{n=1}^{N}\log_2\left(1+\frac{D_1[n]}{u^2[n]}+\frac{D_2[n]}{v^2[n]}+\frac{D_3[n]}{u[n]v[n]}\right)\\ \text{s.t. } & u[n]\geq d_{SE}^2[n],\forall n,\\ & v[n]\geq d_{JE}^2[n],\forall n,\\ & C1-C7.\end{aligned} \tag{28}$$

Similarly, by the first-order Taylor approximation, the objective function in problem (28) can be rewritten as

$$\begin{aligned}&\log_2\left(1+\frac{D_1[n]}{u^2[n]}+\frac{D_2[n]}{v^2[n]}+\frac{D_3[n]}{u[n]v[n]}\right)\\ &\geq \log_2 D_4[n]-\left(\frac{D_1[n]}{\widetilde{u}^2[n]}+\frac{\frac{1}{2}D_3[n]}{\widetilde{u}^{\frac{3}{2}}[n]\widetilde{v}^{\frac{1}{2}}[n]}\right)\frac{u[n]-\widetilde{u}[n]}{\ln 2\ D_4[n]}\\ &\quad-\left(\frac{D_2[n]}{\widetilde{v}^2[n]}+\frac{\frac{1}{2}D_3[n]}{\widetilde{u}^{\frac{1}{2}}[n]\widetilde{v}^{\frac{3}{2}}[n]}\right)\frac{v[n]-\widetilde{v}[n]}{\ln 2D_4[n]},\end{aligned} \tag{29}$$

where $D_4[n]=1+\frac{D_1[n]}{\widetilde{u}[n]}+\frac{D_2[n]}{\widetilde{v}[n]}+\frac{D_3[n]}{\widetilde{u}^{\frac{1}{2}}[n]\widetilde{v}^{\frac{1}{2}}[n]}$, and $\widetilde{u}[n]$ and $\widetilde{v}[n]$ denote the l-th feasible solutions, respectively. Accordingly, by substituting (29) into (28), we rewrite the problem in (28) into an equivalent form as

$$\begin{aligned}\max_{\{\mathbf{q}_E[n],z_E[n]\}} &\sum_{n=1}^{N}-\left(\frac{D_1[n]}{\widetilde{u}^2[n]}+\frac{\frac{1}{2}D_3[n]}{\widetilde{u}^{\frac{3}{2}}[n]\widetilde{v}^{\frac{1}{2}}[n]}\right)\frac{u[n]-\widetilde{u}[n]}{\ln 2\ D_4[n]}\\ &-\left(\frac{D_2[n]}{\widetilde{v}^2[n]}+\frac{\frac{1}{2}D_3[n]}{\widetilde{u}^{\frac{1}{2}}[n]\widetilde{v}^{\frac{3}{2}}[n]}\right)\frac{v[n]-\widetilde{v}[n]}{\ln 2D_4[n]},\\ \text{s.t. } & u[n]\geq ||\mathbf{q}_E[n]-\mathbf{q}_S[n]||^2+|z_E[n]-z_S[n]|^2,\forall n,\\ & v[n]\geq ||\mathbf{q}_E[n]-\mathbf{q}_J[n]||^2+|z_E[n]-z_J[n]|^2,\forall n,\\ & C1-C7.\end{aligned} \tag{30}$$

Note that problem (30) is a convex optimization problem, which can be solved efficiently by CVX [73]–[75].

C. Optimization of the UAV J jamming power $p_J[n]$

In this subsection, we fix the variables $\mathbf{\Phi}[n]$, $\{\mathbf{q}_E[n], z_E[n]\}$ and $\{\mathbf{q}_J[n], z_J[n]\}$ while optimizing the jamming power $p_J[n]$ of the UAV J. Then the problem defined in (14) is equivalently recast as

$$\begin{aligned}\max_{\mathrm{p_J[n]}} &\sum_{n=1}^{N}R_{EE}[n]\\ \text{s.t. } & C1:\sum_{n=1}^{N}p_J[n]\leq p_{total},\forall n,\\ & C2: 0\leq p_J[n]\leq \min\{p_{cov}[n],p_{peak}\},\forall n.\end{aligned} \tag{31}$$

For given $\mathbf{\Phi}[n]$, $\{\mathbf{q}_E[n], z_E[n]\}$ and $\{\mathbf{q}_J[n], z_J[n]\}$, it is noted that the optimization of the jamming power $p_J[n]$ of the UAV J will only change the suspicious communication rate $R_D[n]$. Thus, according to (13), to maximize the objective function in (31), we can determine the optimal power $p_J[n]$ when $R_E[n] = R_D[n]$ for any $n \in \mathcal{N}$. Based on this discussion, we provide the following theorem.

Algorithm 1 The optimal jamming power allocation policy.

Set $p^+ = 0$, $r = 1$.
Calculate the energy efficiency $\eta[n] = \frac{R_{EE}[n]}{p_J^*[n]}, n \in \mathcal{N}$, by substituting (32) into (31).
Rearrange the sequence $p_J^*[n]$ according to the value of $\eta[n]$, from large to small.
repeat
  $p^+ = p^+ + p_J^*[r]$
  $r = r + 1$
until $p^+ > p_{total}$
Restore the sequence $p_J^*[n]$ from the $p_J^*[r]$ in order of original time slots n.

THEOREM 1. *The optimal jamming power of problem* (31)*, denoted as* $p_J^*[n]$*,* $n \in \mathcal{N}$*, is*

$$p_J^*[n]=\begin{cases}\widetilde{p}_J[n], & 0\leq \widetilde{p}_J[n]\leq \min\left\{p_{peak},\widetilde{p}_{cov}[n]\right\},\\ 0, & \textit{otherwise},\end{cases} \tag{32}$$

where $\widetilde{p}_J[n] = \frac{d_{JD}^2[n]}{\beta_0}\left(\frac{\beta_0\Gamma_{SD}\sigma_E^2}{d_{SD}^2[n]F[n]}-\sigma_D^2\right)$, $F[n] = \frac{\beta_0\Gamma_{SE}}{d_{SE}^2[n]}+\frac{\beta_0^2\Gamma_{JE}\Gamma_{SJ}M^2}{d_{SJ}^2[n]d_{JE}^2[n]}+\frac{2\beta_0^{\frac{3}{2}}\Gamma_{SE}\Gamma_{JE}\Gamma_{SJ}M}{d_{SE}[n]d_{JE}[n]d_{SJ}[n]}$ and $\widetilde{p}_{cov}[n] = \frac{(\sigma_{cov}^2-\sigma_D^2)d_{JD}^2[n]}{\beta_0\Gamma_{JD}}$.

Proof: Please refer to Appendix B. ■

Since the UAVs have difficulty to replenish energy on the ocean, when the jamming power of the UAV J is limited, i.e., $p_{total} < \sum_{n=1}^{N} p_J^*[n]$, $n \in \mathcal{N}$, we develop an optimal jamming power allocation policy for this energy-constrained case to improve the energy efficiency, which is summarized in Algorithm 1.

Remark: From Algorithm 1, when the energy budget of the UAV J is limited, it cannot send the optimal jamming power at every time slot n. Thus, for this energy-constrained case, the system prefers to assign more jamming power on some time slots with larger value of $\eta[n]$, which will obtain a higher energy efficiency over the conventional power allocation scheme.

D. Overall Algorithm

We propose an iterative algorithm for solving problem (14) by using the BCD technique, the algorithm details are shown in Algorithm 2. Since the variables $\{\mathbf{\Phi}[n], \mathbf{q}_J[n], z_J[n]\}$, $\{\mathbf{q}_E[n], z_E[n]\}$ and $p_J[n]$ are updated alternately, Algorithm 2 is nondecreasing over iterations and converges to a stationary point; the relevant details are given in [20], [69], [74], [75]. Furthermore, in each iteration, the complexity of solving (24), (30) and (32) are $\mathcal{O}[(3N)^{3.5}]$, $\mathcal{O}[(3N)^{3.5}]$, and $\mathcal{O}[N + N\log(N)]$, respectively. Thus, the total complexity of

Algorithm 2 Proposed iterative algorithm for problem (14).

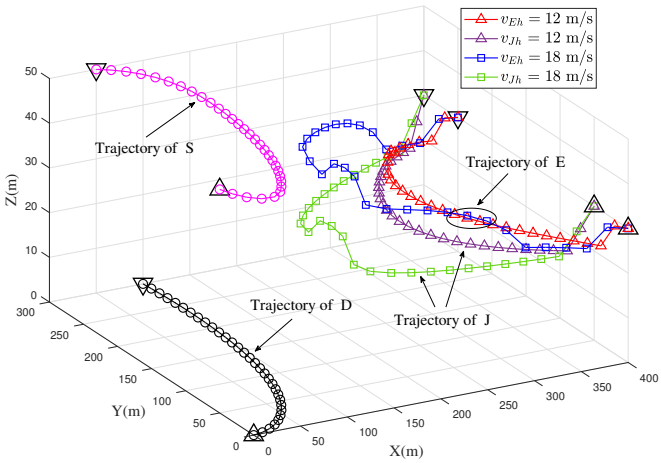
Set $l = 0$, $\gamma = 10^{-5}$, $R_0^l = 0$, and $R_f^l = 100$
Initialize $(\mathbf{q}_E^0, z_E^0)$, $(\mathbf{q}_J^0, z_J^0)$, (p_J^0) and $\mathbf{\Phi}^0$.
repeat
Let $l = l + 1$,
Obtain $\mathbf{\Phi}^l$ and $(\mathbf{q}_J^l, z_J^l)$ by using (17) and (24) for any given $(\mathbf{q}_E^{l-1}, z_E^{l-1})$ and $p_J^{(l-1)}$;
Calculate $(\mathbf{q}_E^l, z_E^l)$ of (30) based on $\mathbf{\Phi}^l$, (q_J^l, z_J^l) and $p_J^{(l-1)}$;
Update p_J^l based on (32) and Algorithm 1 under given $\mathbf{\Phi}^l$, $(\mathbf{q}_E^l, z_E^l)$ and $(\mathbf{q}_J^l, z_J^l)$;
Determine R_{EE}^l and $R_f^l = |R_0^l - R_{EE}^l|$.
Update $R_0^{l+1} = R_{EE}^l$;
until $R_f^l \leq \gamma$
Output $(\mathbf{q}_E^l, z_E^l)$, $(\mathbf{q}_J^l, z_J^l)$, p_J^l and $\mathbf{\Phi}^l$.

overall algorithm in Algorithm 2 is $\mathcal{O}[N_{ite}(3N)^{3.5}]$, where N_{ite} and N denote the numbers of required iterations and time slots, respectively.

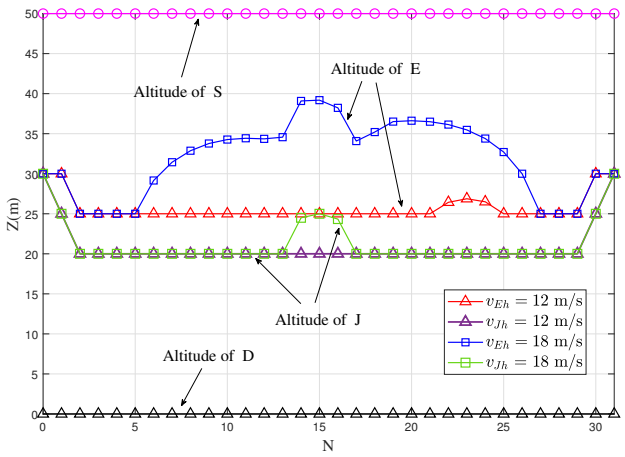
IV. Simulation Results

In this section, we evaluate and analyze the eavesdropping performance of the proposed UAV-mounted RIS-aided joint design scheme. The simulation parameters are set as follow. The initial and final coordinates of the UAV E and J are located at $\{x_E[0], y_E[0], z_E[0]\} = \{400, 0, 30\}$ m and $\{x_E[N], y_E[N], z_E[N]\} = \{400, 250, 30\}$ m, and $\{x_J[0], y_J[0], z_J[0]\} = \{400, 50, 30\}$ m and $\{x_J[N], y_J[N], z_J[N]\} = \{400, 300, 30\}$ m, respectively. The maximum and minimum flight altitudes of the UAVs are set to $z_{max} = 80$ m and $z_{min} = 20$ m, and the maximum horizontal and vertical speed are set to v_{ih}=18 m/s and $v_{iv} = 5$ m/s, $i \in \{E, J\}$, respectively [76], [77]. Furthermore, $\beta_0 = -20$ dBm is the channel power gain, $k[n] = 31.3$ is the Rician factor [19], and $\Gamma_{SE} = \Gamma_{SJ} = \Gamma_{JE} = \Gamma_{JD} = \Gamma_{min} = 0.65$ and $\Gamma_{SD} = \Gamma_{max} = 1.35$ are the lower and upper bounds on the corresponding small-scale fading, respectively [20], [69]. Moreover, unless stated otherwise, $\sigma_D^2 = \sigma_E^2 = -70$ dBm are the noise variances [78], $\sigma_{cov}^2 = -50$ dBm is the artificial noise detection threshold, $p_S = 25$ dBm is the transmission power of the UAV S, $p_{peak} = 25$ dBm and $p_{total} = 500$ mW are the peak and total jamming power of the UAV J, respectively [69], [79]. In addition, $N = 30$ is the numbers of time slots [80], $M = 64$ is the reflecting elements of RIS, $z_{mhd} = 5$ m is the minimum height difference, $d_{min} = 20$ m is the minimum anti-collision distance between the UAV E and J, and $d_{Smin} = d_{Dmin} = 100$ m are the minimum safety distance from the suspicious users, respectively.

Fig. 2(a) and Fig. 2(b) depict the trajectories of the UAVs onto the 3D and vertical plane with different horizontal speed v_{ih}, $i \in \{E, J\}$, respectively. The initial and final positions of the UAVs and vessels are set as $\triangle$ and $\bigtriangledown$, respectively. As show in the Fig. 2(a), when $v_{Eh} = v_{Jh} = 12$ m/s, we



(a)



(b)

Fig. 2. Optimized UAVs trajectories with different horizontal speeds v_{ih}: (a) 3D plane; (b) Vertical plane.

notice that both UAV E and UAV J almost directly fly to the final position due to the minimum flight time N constraint. However, when v_{ih} increases, both UAV E and UAV J first fly quickly to the suspicious users, then they follow the suspicious users for as long as possible. The reason is that the eavesdropper UAV E needs to follow the suspicious UAV S to overhear more information while the jammer UAV J moves closer to the suspicious receiver D to save the jamming powers. Furthermore, due to the noise detection threshold and the minimum safety distance constraints, both UAV E and UAV J need to keep a certain distance from the suspicious S and D to remain undetected. Moreover, from Fig. 2(b), when $v_{Eh} = v_{Jh} = 18$ m/s, both UAV J and UAV E first fly to a lower altitude, then they climb the altitude in a certain period of time, and subsequently reduces the altitude before reaching the final location. This is because when far from the suspicious users, the UAV J needs to reduce the

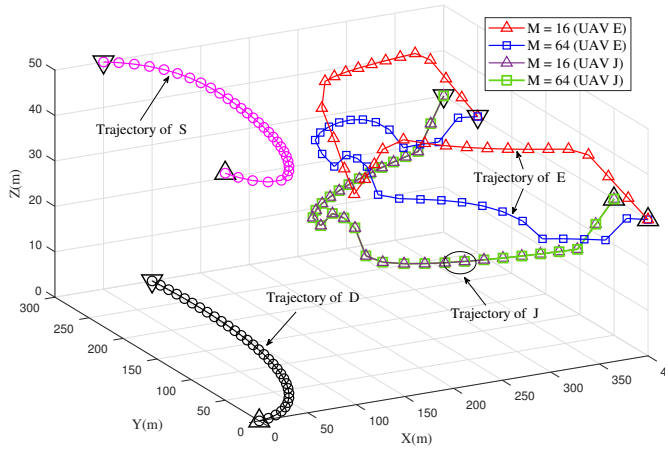


Fig. 3. Optimized UAVs trajectories with different RIS reflection elements M.

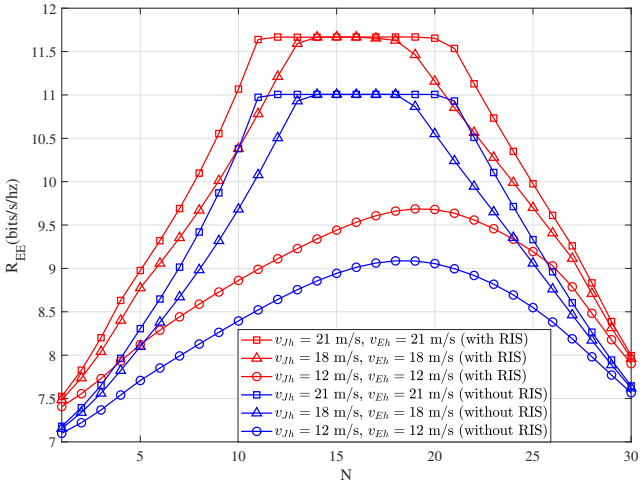


Fig. 4. Achieved eavesdropping rate with different UAVs speeds and RIS deployments.

flight altitude to get the better position for jamming while the UAV E moves closer to the UAV J to enhance the reflected signal from RIS. In addition, when the legitimate UAVs come closer to the suspicious users as N increases, the UAV J must ascend to a higher flight altitude to evade detection by the suspicious receiver D while the UAV E climbs the flight height to eavesdrop more information from the suspicious UAV S.

Fig. 3 plots the 3D trajectories of both UAV E and UAV J versus different numbers of reflection elements M. From the Fig. 3, for all given values of M, both UAV E and UAV J first move quickly to the suspicious users, then they follow the UAV S and vessel D as long as possible, respectively. However, when M is small, i.e., $M = 16$, the UAV E first flies to a higher altitude, then it reduces the altitude in a certain period of time, and subsequently climbs up before reaching the final location. This is because the reflected signal power from RIS decreases as M decreases, the UAV E needs to move closer to the suspicious S to eavesdrop more information. Furthermore, due to the minimum safety distance constraint, the UAV E reduces the altitude in some time slots to simultaneously move away from/closer to the UAV S/J to improve the eavesdropping performance. Moreover, for all considered values of M, the flight trajectory of the UAV J remains the same. The reason is that the UAV J needs to always keep the optimal routes to get the best position for jamming purpose.

Fig. 4 presents the achievable eavesdropping rate versus different UAVs speed v_{ih} and RIS deployment scenarios, respectively. As can be seen in Fig. 4, the achieved eavesdropping rate first increases and then decreases as N increases for all considered values of v_{ih}, $i \in \{E, J\}$. This is because both UAV E and UAV J first approache to the suspicious S and D, and gradually keeps away from them as N increases. However, when the maximum UAVs speed v_{ih} is large enough, i.e., v_{Jh} =v_{Eh}= 18 m/s and v_{Jh} =v_{Eh}= 21 m/s, the achieved maximum eavesdropping rate remains the same. The reason

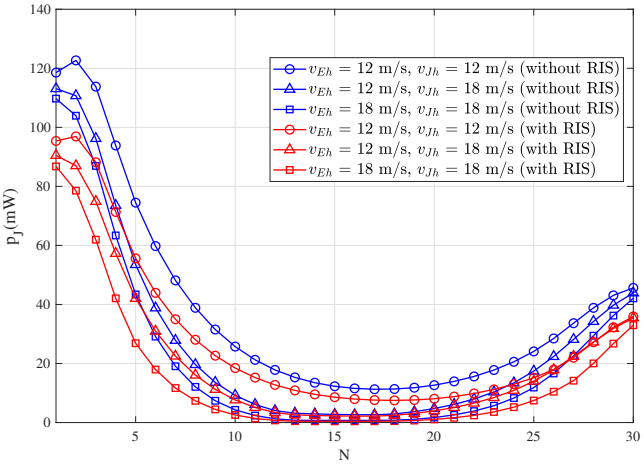


Fig. 5. Transmission power of the UAV J with different speeds v_{ih} and RIS deployments.

is that when v_{ih} is sufficiently enough, both UAV E and UAV J cannot fully utilize the maximum speed to approach the suspicious users due to the fact that there are the noise detection threshold and the minimum safety distance constraints. Moreover, as expected, the proposed UAV-mounted RIS enabled approach achieves a superior performance when compared with the baseline scheme without RIS. The reason is that the RIS can create an additional surveillance channel towards the UAV E by configuring the radio environments, and thereby enhances the effective eavesdropping rate.

Fig. 5 illustrates the transmission power of the UAV J versus different speed v_{ih} and RIS schemes, respectively. As presented in Fig. 5, for all considered UAVs speeds and RIS schemes, the transmission power of the UAV J first decreases and then increases as N increases. The reason is that when the UAV J is far away from the suspicious users, it needs to send a larger jamming power p_J to guarantee $R_E[n] \geq R_D[n]$.

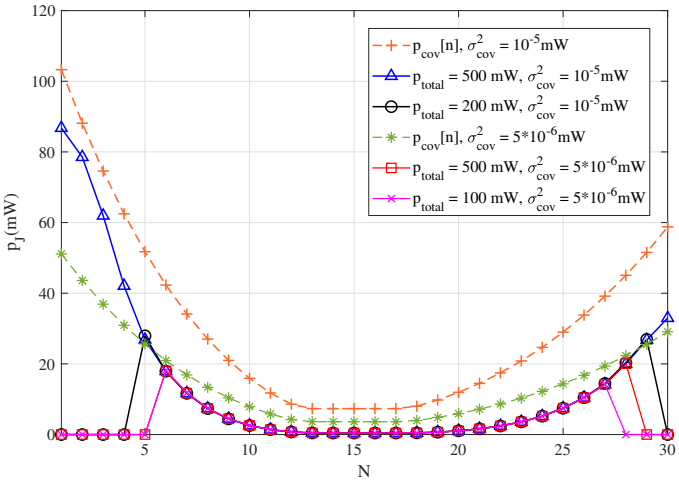


Fig. 6. Optimal jamming power of the UAV J with different noise detection thresholds σ_{cov}^2 and total power constraints p_{total}.

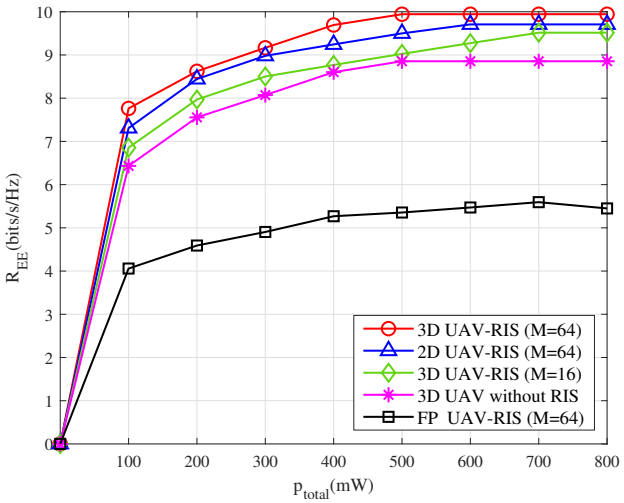


Fig. 7. Achieved average eavesdropping rates with different algorithms versus p_{total}.

Moreover, from the results in Fig. 5, the transmission power of the UAV J decreases as v_{Jh} or v_{Eh} increases. This is because when v_{Jh} or v_{Eh} is large enough, the UAV J or E can quickly approach to the suspicious D or S, and thus only need a small jamming power to guarantee $R_E[n] \geq R_D[n]$. In addition, compared with the scheme without RIS, the proposed UAV-mounted RIS scheme significantly reduces the transmission power of the UAV J, which has been previously explained in detail.

Fig. 6 shows the optimal jamming power $p_J[n]$ versus different artificial noise detection thresholds σ_{cov}^2 at the suspicious receiver D and total power constraints p_{total} at the jammer UAV J, respectively. For given detection thresholds $\sigma_{cov}^2 = 10^{-5}$ mW and $\sigma_{cov}^2 = 5 * 10^{-6}$ mW, the upper bound of the covert jamming power $p_{cov}[n]$ can be derived as red $+$ and green $*$, respectively. From the Fig. 6, when both σ_{cov}^2 and p_{total} are sufficiently enough, i.e., $\sigma_{cov}^2 = 10^{-5}$ mW and $p_{total} = 500$ mW, the optimal jamming power $p_J[n]$ can be allocated at every time slot n. However, when the energy budget of the jamming power is limited, i.e., $p_{total} = 200$ mW, the UAV J reduces the transmission power to zero in some time slots. The reason is that the system prefers to assign more jamming power on those time slots with larger value of $\eta[n]$, the relevant details can be found in Algorithm 1, which will obtain a higher energy efficiency over the conventional power allocation scheme. Moreover, when σ_{cov}^2 is small, even if the total power budget p_{total} is sufficiently enough, the UAV J also will not send jamming signal in a certain period of time to evade detection by the suspicious receiver D. In addition, if the p_{total} is also limited, i.e., $p_{total} = 100$ mW, the UAV J needs to assign the jamming power based on both the upper bound of $p_{cov}[n]$ and the energy efficiency $\eta[n]$.

Fig. 7 compares the average eavesdropping rates of the proposed UAV-mounted RIS scheme (denoted as 3D UAV-RIS) with the following benchmark approaches: (1) The fixed UAVs flight altitude scheme (denoted as 2D UAV-RIS), where the flight altitudes $z_E = 50$ m and $z_J = 20$ m; (2) The proposed 3D joint optimization scheme in [69] (denoted as 3D UAV without RIS), where the scheme without the assistance of the RIS; (3) The proposed fixed power allocation scheme in [68] (denoted as FP UAV-RIS), where the jamming power $P_J[n] = \frac{p_{total}}{N}$ mW, $\forall n \in \mathcal{N}$. As can be seen in Fig. 7, the achieved average eavesdropping rates of all algorithms first increases and then saturates as the total power budgets p_{total} increases. This is because when p_{total} is large enough, the UAV J cannot fully utilize the maximum jamming power to disturb the suspicious receiver D due to the fact that there is a minimum artificial noise detection threshold. Moreover, compared with the 2D and without RIS schemes, the proposed scheme significantly improves the average eavesdropping rates since it can simultaneously adjust UAVs 3D flight trajectories and create an additional surveillance channel. In addition, from the Fig. 7, the fixed power allocation scheme achieves a worse performance when compared with the other four schemes. This is because when the detection threshold σ_{cov}^2 is not sufficiently enough, the equal allocation scheme will result in the artificial noise power of the suspicious receiver D beyond the detection threshold at some time slots, and thereby degrade the eavesdropping performance.

V. Conclusions

In this paper, we have introduced UAV-mounted RIS into maritime low-altitude surveillance systems to enhance the eavesdropping performance by creating an additional surveillance channel towards the legitimate UAV, and meanwhile reduce the power consumption and improve the energy efficiency by adjusting the power allocation and flight trajectory of the jammer UAV. In the proposed scheme, the 3D trajectory of the legitimate UAV, the reflecting phase shifts of the RIS, as well as the 3D trajectory and the jamming power of the

jammer UAV have been jointly designed to maximize the sum eavesdropping rate under the UAVs mobility, the detection thresholds and the energy budgets constraints. To address the non-convexity issue, we have first decomposed the design problem into three subproblems and then converted them into more tractable forms. Finally, we have proposed an iterative algorithm to determine an approximated optimal solution of the designed problem. Moreover, we have evaluated and discussed the system performance and the impact of different parameters of the proposed scheme. The simulation results have demonstrated that the effectiveness and showed the capability of the proposed UAV-mounted RIS scheme in the maritime surveillance scenarios with the jamming detection ability. On the one hand, the harsh maritime environments may affect UAV flight stability. On the other hand, the typical hardware impairments will cause RIS phase-shift errors. As a result, in the future work, we will further consider these effects in the problem design to improve anti-interference capability and surveillance robustness.

Appendix A
Proof of Proposition 1

First, let us define $f(r[n], s[n])$ as the first term in the objective function of problem (22), then we derive the second-order partial of $f(r[n], s[n])$ with respect to $r[n]$ and $s[n]$, respectively:

$$\begin{aligned}\frac{\partial^2 f}{\partial r^2[n]} = &-\frac{1}{z^2 \ln 2}\left(\frac{A_2}{r^2[n]s[n]} + \frac{A_3}{2r^{3/2}[n]s^{1/2}[n]}\right)^2 \\ &+ \frac{1}{z \ln 2}\left(\frac{2A_2}{r^3[n]s[n]} + \frac{3A_3}{4r^{5/2}[n]s^{1/2}[n]}\right),\end{aligned} \tag{33}$$

$$\begin{aligned}\frac{\partial^2 f}{\partial s^2[n]} = &-\frac{1}{z^2 \ln 2}\left(\frac{A_2}{r[n]s^2[n]} + \frac{A_3}{2r^{1/2}[n]s[n]^{3/2}}\right)^2 \\ &+ \frac{1}{z \ln 2}\left(\frac{2A_2}{r[n]s^3[n]} + \frac{3A_3}{4r^{1/2}[n]s^{5/2}[n]}\right),\end{aligned} \tag{34}$$

and

$$\begin{aligned}\frac{\partial^2 f}{\partial s[n]\partial r[n]} = \frac{\partial^2 f}{\partial r[n]\partial s[n]} = &-\frac{1}{z^2 \ln 2} \cdot \\ &\left[\left(\frac{A_2}{r^2[n]s[n]} + \frac{A_3}{2r^{3/2}[n]s^{1/2}[n]}\right)\left(\frac{A_2}{r[n]s^2[n]} + \frac{A_3}{2r^{1/2}[n]s^{3/2}[n]}\right)\right] \\ &+ \frac{1}{z \ln 2}\left(\frac{A_2}{r^2[n]s^2[n]} + \frac{A_3}{4r^{3/2}[n]s^{3/2}[n]}\right),\end{aligned} \tag{35}$$

where $z(r[n], s[n]) = A_1 + \frac{A_2}{r[n]s[n]} + \frac{A_3}{\sqrt{r[n]s[n]}}$.

Based on (33)-(35), the Hessian matrix of $f(r[n], s[n])$ is

$$\nabla^2 f = \begin{bmatrix} \frac{\partial^2 f}{\partial r^2[n]} & \frac{\partial^2 f}{\partial r[n]\partial s[n]} \\ \frac{\partial^2 f}{\partial s[n]\partial r[n]} & \frac{\partial^2 f}{\partial s^2[n]} \end{bmatrix}. \tag{36}$$

As a result, according to the objective function $f(u[n], v[n])$ defined in (22), we can easily obtain $\frac{\partial^2 f}{\partial r^2[n]}\frac{\partial^2 f}{\partial s^2[n]} - \frac{\partial^2 f}{\partial r[n]\partial s[n]}\frac{\partial^2 f}{\partial s[n]\partial r[n]} > 0$ due to $\{r[n], s[n], A_1, A_2, A_3\} > 0$. Thus, the matrix $\nabla^2 f$ is positive definite and the function $f(r[n], s[n])$ is convex with respect to $r[n]$ and $s[n]$. This completes the proof.

Appendix B
Proof of Theorem 1

Suppose problem (31) is feasible and let $p_J^*[n]$ denotes its optimal solution. First, for given $\mathbf{\Phi}[n]$, $\{\mathbf{q}_E[n], z_E[n]\}$ and $\{\mathbf{q}_J[n], z_J[n]\}$, to guarantee $R_E[n] \geq R_D[n]$, we have the jamming power $\widetilde{p}_J[n] \geq \frac{d_{JD}^2[n]}{\beta_0}\left(\frac{\beta_0 \Gamma_{SD}\sigma_E^2}{d_{SD}^2[n]F[n]} - \sigma_D^2\right)$ based on (11) and (12), where $F[n] = \frac{\beta_0 \Gamma_{SE}}{d_{SE}^2[n]} + \frac{\beta_0^2 \Gamma_{JE}\Gamma_{SJ}M^2}{d_{SJ}^2[n]d_{JE}^2[n]} + \frac{2\beta_0^{\frac{3}{2}}\Gamma_{SE}\Gamma_{JE}\Gamma_{SJ}M}{d_{SE}[n]d_{JE}[n]d_{SJ}[n]}$. However, since the suspicious communication rate $R_D[n]$ is strictly monotonically decreasing with respect to $\widetilde{p}_J[n]$, we can determine the optimal jamming power when $R_E[n] = R_D[n]$ by (13), i.e., $\widetilde{p}_J[n] = \frac{d_{JD}^2[n]}{\beta_0}\left(\frac{\beta_0 \Gamma_{SD}\sigma_E^2}{d_{SD}^2[n]F[n]} - \sigma_D^2\right)$. If the feasible solution $\widetilde{p}_J[n]$ can satisfy both the peak and covert power constraints, i.e., $0 \leq \widetilde{p}_J[n] \leq \min\{p_{peak}, \widetilde{p}_{cov}[n]\}$, we can obtain the optimal solution $p_J^*[n] = \widetilde{p}_J[n] = \frac{d_{JD}^2[n]}{\beta_0}\left(\frac{\beta_0 \Gamma_{SD}\sigma_E^2}{d_{SD}^2[n]F[n]} - \sigma_D^2\right)$. Next, if the jamming power $\widetilde{p}_J[n] = \frac{d_{JD}^2[n]}{\beta_0}\left(\frac{\beta_0 \Gamma_{SD}\sigma_E^2}{d_{SD}^2[n]F[n]} - \sigma_D^2\right) < 0$, there must exist the relationship $R_E[n] > R_D[n]$, which shows that the UAV J doesn't need to send any jamming power to disturb the suspicious transmission, i.e, $p_J^*[n] = 0$. Moreover, if $\widetilde{p}_J[n] > p_{peak}$ or $\widetilde{p}_J[n] > \widetilde{p}_{cov}[n]$, due to the peak power and detection threshold constraints, the UAV J will not send the jamming signal in some time slots for saving power, i.e., we have $p_J^*[n] = 0$. Combining three parts above, the optimal solution $p_J^*[n]$ of problem (31) can be derived as (32). This completes the proof.

References

[1] Y. Wang *et al.*, "Toward realization of low-altitude economy networks: Core architecture, integrated technologies, and future directions," *IEEE Trans. Cogn. Commun. Netw.* vol. 11, no. 5, pp. 2788-2820, Oct. 2025.

[2] M. Song *et al.*, "Trustworthy intelligent networks for low-altitude economy," *IEEE Commun. Mag.*, vol. 63, no. 7, pp. 72-79, Jul. 2025.

[3] D. He, W. Yuan, J. Wu, and R. Liu, "Ubiquitous UAV communication enabled low-altitude economy: Applications, techniques, and 3GPPs efforts," *IEEE Network*, doi: 10.1109/MNET.2025.3574922.

[4] M. Ahmed *et al.*, "Toward a sustainable low-altitude economy: A survey of energy-efficient RIS-UAV networks," *IEEE Internet Things J.*, doi: 10.1109/JIOT.2025.3618483.

[5] X. Tang *et al.*, "Task assignment and exploration optimization for low altitude UAV rescue via generative AI enhanced multi-agent reinforcement learning," *IEEE Trans. Mobile Comput.*, doi: 10.1109/TMC.2025.3594188.

[6] R. Khalid *et al.*, "Computational efficiency maximization for UAV-assisted MEC networks with energy harvesting in disaster scenarios," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 9004-9018, Mar. 2024.

[7] Y. Wang, J. Huang, F. Shan, Y. Gao, R. Xiong, and J. Luo, "Optimizing joint speed and altitude schedule for UAV data collection in low-altitude airspace," *IEEE Trans. Mobile Comput.*, doi: 10.1109/TMC.2025.3591698.

[8] W. Zhang *et al.*, "Energy transfer and data collection from batteryless sensors in low-altitude wireless networks," *arXiv preprint arXiv:2507.07481*, 2025.

[9] Y. Li, W. Wang, C. Zhang, Y. Huang, and D. Niyato, "Joint UAV deployment and space-time-frequency resource allocation for low-altitude economy," *IEEE Wireless Commun. Lett.*, vol. 14, no. 9, pp. 2808-2812, Sep. 2025.

[10] W. Xie *et al.*, "Joint optimization of UAV-carried IRS for urban low altitude mmWave communications with deep reinforcement learning," *IEEE Trans. Mobile Comput.*, doi: 10.1109/TMC.2025.3600682.

[11] G. Cheng, X. Song, Z. Lyu, and J. Xu, "Networked ISAC for low-altitude economy: coordinated transmit beamforming and UAV trajectory design," *IEEE Trans. Commun.*, vol. 73, no. 8, pp. 5832-5847, Aug. 2025.

[12] C. Zhao, Y. Feng, H. Luo, F. Gao, F. Liu and S. Jin, "Networked ISAC based UAV tracking and handover towards low-altitude economy," *IEEE Trans. Wireless Commun.*, vol. 24, no. 9, pp. 7670-7685, Sep. 2025.

[13] X. Ye, Y. Mao, X. Yu, S. Sun, L. Fu, and J. Xu, "Integrated sensing and communications for low-altitude economy: A deep reinforcement learning approach," *IEEE Trans. Wireless Commun.*, doi: 10.1109/TWC.2025.3583950.

[14] M. M. Wang, J. Zhang, and X. You, "Machine-type communication for maritime Internet of Things: A design," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2550-2585, Fourth quarter 2020.

[15] S. Guan, J. Wang, C. Jiang, R. Duan, Y. Ren and T. Q. S. Quek, "MagicNet: The maritime giant cellular network," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 117-123, Mar. 2021.

[16] T. Wei, W. Feng, Y. Chen, C. -X. Wang, N. Ge and J. Lu, "Hybrid satellite-terrestrial communication networks for the maritime internet of things: Key technologies, opportunities, and challenges," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8910-8934, Jun. 2021.

[17] F. S. Alqurashi, A. Trichili, N. Saeed, B. S. Ooi and M. S. Alouini, "Maritime communications: A survey on enabling technologies, opportunities, and challenges," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3525-3547, Feb. 2023.

[18] N. Nomikos, P. K. Gkonis, P. S. Bithas, and P. Trakadas, "A survey on UAV-aided maritime communications: Deployment considerations, applications, and future challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 56-78, Jan. 2023.

[19] X. Li, W. Feng, Y. Chen, C. X. Wang and N. Ge, "Maritime coverage enhancement using UAVs coordinated with hybrid satellite-terrestrial networks," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2355-2369, Apr. 2020.

[20] W. Wang *et al.*, "Robust 3D-trajectory and time switching optimization for dual-UAV-enabled secure communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3334-3347, Nov. 2021.

[21] J. Liu, F. Zeng, W. Wang, Z. Sheng, X. Wei, and K. Cumanan, "Trajectory design for UAV-enabled maritime secure communications: A reinforcement learning approach," *China Communications*, vol. 19, no. 9, pp. 26-36, Sep. 2022.

[22] L. Liu, C. Shen, F. Shu, F. Wang, S. Li and T. Q. S. Quek, "HAP-UAV-assisted maritime IoT communication network," *IEEE Trans. Mobile Comput.*, doi: 10.1109/TMC.2025.3596169.

[23] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80-83, Feb. 2016.

[24] J. Xu, L. Duan and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790-2806, May 2017.

[25] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6707-6719, Oct. 2018.

[26] Y. Han, L. Duan, and R. Zhang, "Jamming-assisted eavesdropping over parallel fading channels," *IEEE Trans. Inf. Forensics and Security*, vol. 14, no. 9, pp. 2486-2499, Sep. 2019.

[27] G. Hu, J. Ouyang, Y. Cai, and Y. Cai, "Proactive eavesdropping in two-way amplify-and-forward relay networks," *IEEE Sys. J.*, vol. 15, no. 3, pp. 3415-3426, Sep. 2021.

[28] D. Guo, H. Ding, L. Tang, X. Zhang, L. Yang, and Y. C. Liang, "A proactive eavesdropping game in MIMO systems based on multiagent deep reinforcement learning," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 8889-8904, Nov. 2022.

[29] D. Xu and H. Zhu, "Proactive eavesdropping via jamming over short packet suspicious communications with finite blocklength," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7505-7519, Nov. 2022.

[30] J. Wang, P. Zhang, L. Tang, Y. Bai and L. Yang, "Intelligent passive eavesdropping in massive MIMO-OFDM systems via reinforcemen Learning," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1248-1252, June 2022.

[31] H. Lu, H. Zhang, H. Dai, W. Wu and B. Wang, "Proactive eavesdropping in UAV-aided suspicious communication systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1993-1997, Feb. 2019.

[32] G. Hu, Y. Cai, and Y. Cai, "Joint optimization of position and jamming power for UAV-aided proactive eavesdropping over multiple suspicious communication Links," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2093-2097, Dec. 2020.

[33] Q. Dan, H. Lei, K. H. Park, W. Lei and G. Pan, "Proactive eavesdropping in relay systems via trajectory and power optimization," *IEEE Internet Things J.*, vol. 11, no. 20, pp. 33744-33757, Oct. 2024.

[34] D. Guo, H. Ding, L. Tang, X. Zhang and Y. C. Liang, "Wireless surveillance in a MIMO System with spoofing relay and UAV-enabled eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15792-15797, Oct. 2024.

[35] S. Hu, Q. Wu and X. Wang, "Energy management and trajectory optimization for UAV-enabled legitimate monitoring systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 142-155, Jan. 2021.

[36] G. Hu *et al.*, "Maxmin fairness for UAV-enabled proactive eavesdropping with jamming over distributed transmit beamforming-based suspicious communications," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1595-1614, Mar. 2023.

[37] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni and E. Tovar, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2283-2293, Mar. 2019.

[38] X. Wang *et al.*, "Eavesdropping and jamming selection policy for suspicious UAVs based on low power consumption over fading channels," *Sensors*, vol. 19, no. 1126, 2019.

[39] D. Guo, L. Tang, X. Zhang and Y. C. Liang, "Joint optimization of trajectory and jamming power for multiple UAV-aided proactive eavesdropping," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 5770-5785, May 2024.

[40] D. He and H. Hou, "UAV-assisted legitimate wireless surveillance: performance analysis and optimization," in *Proc. IEEE Int. Conf. Unmanned Syst. (ICUS)*, Nanjing, China, 2024, pp. 1975-1979.

[41] H. Huang, A. V. Savkin and W. Ni, "Navigation of a UAV team for collaborative eavesdropping on multiple ground transmitters," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10450-10460, Oct. 2021.

[42] H. Huang, A. V. Savkin, and W. Ni, "Decentralized navigation of a UAV team for collaborative covert eavesdropping on a group of mobile ground nodes," *IEEE Trans. Automat. Sci. Eng.*, vol. 19, no. 4, pp. 3932-3941, Oct. 2022.

[43] S. Hu, W. Ni, X. Wang, A. Jamalipour and D. Ta, "Joint optimization of trajectory, propulsion, and thrust powers for covert UAV-on-UAV video tracking and surveillance," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1959-1972, 2021.

[44] J. Zhang, "A covert surveillance strategy for a solar-powered UAV over suspicious mobile target," in *Proc. 14th Int. Conf. Comput. Autom. Eng. (ICCAE)*, Brisbane, Australia, 2022, pp. 8-12.

[45] Y. Liu *et al.*, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546-1577, 3rd Quart., 2021.

[46] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106-112, Jan. 2020.

[47] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313-3351, May 2021.

[48] H. Jiang *et al.*, "Aerial IRS-enabled secure mobile communications: Joint 3D trajectory and beamforming design," *IEEE Wireless Commun. Lett.*, vol. 13, no. 3, pp. 647-651, Mar. 2024.

[49] J. Zhang *et al.*, "Intelligent integrated sensing and communication: A survey," *Sci. China Inf. Sci.*, vol. 68, no. 3, pp. 131301:42, Mar. 2025.

[50] J. Yao, T. Wu, Q. Zhang, and J. Qin, "Proactive monitoring via passive reflection using intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 24, no. 9, pp. 1909-1913, Sep. 2020.

[51] B. Li and K. Cui, "IRS-assisted proactive eavesdropping over fading channels based on deep reinforcement learning," *IEEE Commun. Lett.*, vol. 26, no. 8, pp. 1730-1734, Aug. 2022.

[52] T. Ji, M. Hua, C. Li, Y. Huang, and L. Yang, "A robust IRS-aided wireless information surveillance design with bounded channel errors," *IEEE Wirel. Commun. Lett.*, vol. 11, no. 10, pp. 2210-2214, Oct. 2022.

[53] Y. Cao, L. Duan, M. Jin, and N. Zhao, "Cooperative double-IRS aided proactive eavesdropping," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6228-6240, Sep. 2022.

[54] X. Hu, Y. Yi, K. Li, H. Zhang, and C. Kai, "Active reconfigurable intelligent surface aided surveillance scheme," *IEEE Wirel. Commun. Lett.*, vol. 12, no. 2, pp. 356-360, Feb. 2023.

[55] G. Hu, J. Si, Y. Cai, and N. Al-Dhahir, "Intelligent reflecting surface-assisted proactive eavesdropping over suspicious broadcasting communication with statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4483-4488, Apr. 2022.

[56] J. Yang, K. Huang, X. Sun and Y. Wang, "Joint active and passive beamforming optimization for intelligent reflecting surface assisted proactive eavesdropping," *IET Commun.*, vol. 38, no. 8, pp. 1735-1748, 2021.

[57] M. M. Zhao, Y. Cai, and R. Zhang, "Intelligent reflecting surface aided wireless information surveillance," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 2, pp. 1219-1234, Feb. 2023.

[58] Y. Cao, S. Xu, and J. Liu, "Proactive eavesdropping strategies using hybrid reflecting-backscatter intelligent surface," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5441-5446, Apr. 2023.

[59] Y. Cao, J. Wang and J. Liu, "Double-IRS assisted proactive eavesdropping with cooperative reflecting and backscatter," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Rome, Italy, 2023, pp. 1917-1921.

[60] G. Hu *et al.*, "Analysis and optimization of STAR-RIS-assisted proactive eavesdropping with statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 6850-6855, May 2023.

[61] G. Hu *et al.*, "STAR-RIS-assisted information surveillance over suspicious multihop communications," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 5344-5365, May 2024.

[62] F. Jafarian, M. Ardebilipour, M. Mohammadi and M. Matthaiou, "Wireless information surveillance via STAR-RIS," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Dubai, United Arab Emirates, 2024, pp. 1-6.

[63] S. Lin *et al.*, "STAR-RIS-empowered monitoring over two-way suspicious communications," *IEEE Trans. Veh. Technol.*, doi: 10.1109/TVT.2025.3595754.

[64] X. Yuan, S. Hu, W. Ni, X. Wang and A. Jamalipour, "Deep reinforcement learning-driven reconfigurable intelligent surface-assisted radio surveillance with a fixed-wing UAV," *IEEE Trans. Inf. Forensics and Security*, vol. 18, pp. 4546-4560, 2023.

[65] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," *IEEE Access*, vol. 9, pp. 31595–31607, 2021.

[66] D. Xu, "Proactive eavesdropping of jamming-assisted suspicious communications in fading channels: A stackelberg game approach," *IEEE Trans. Commun.*, vol. 72, no. 5, pp. 2913-2928, May 2024.

[67] Z. Cheng *et al.*, "Covert surveillance via proactive eavesdropping under channel uncertainty," *IEEE Trans. Commun.*. 69, no. 6, pp. 4024-4037, Jun. 2021.

[68] Z. Hu and Q. Xu, "USV trajectory optimization based legitimate maritime wireless surveillance," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Shanghai, China, 2025, pp. 1-6.

[69] L. Wu *et al.*, "UAV-assisted maritime legitimate surveillance: Joint trajectory design and power allocation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13701-13705, Oct. 2023.

[70] T. Wei, W. Feng, J. Wang, N. Ge, and J. Lu, "Exploiting the shipping lane information for energy-efficient maritime communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7204-7208, Jul. 2019.

[71] X. Li, W. Feng, J. Wang, Y. Chen, N. Ge, and C. -X. Wang, "Enabling 5G on the ocean: A hybrid satellite-UAV-terrestrial network solution," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 116-121, Dec. 2020.

[72] C. Zhan, H. Hu, Z. Liu, J. Wang, N. Cheng, and S. Mao, "Aerial video streaming over 3D cellular networks: An environment and channel knowledge map approach," *IEEE Trans. Wireless Commun.*, vol. 23, no. 2, pp. 1432-1446, Feb. 2024.

[73] M. Grant and S. Boyd, *CVX: Matlab Software for Disciplined Convex Programming*, Jul. 2010 [Online]. Available: http://cvxr.com/cvx.

[74] C. You and R. Zhang, "3D trajectory optimization in rician fading for UAV-enabled data harvesting," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3192-3207, Jun. 2019.

[75] W. Wang *et al.*, "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476-4489, Jul. 2020.

[76] N. V. Cuong, Y. W. P. Hong, and J. P. Sheu, "UAV trajectory optimization for joint relay communication and image surveillance," *IEEE Trans. Wireless Commun.*, vol. 21, no. 12, pp. 10177-10192, Dec. 2022.

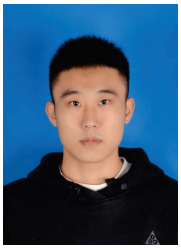
[77] Y. Pan *et al.*, "Joint optimization of trajectory and resource allocation for time-constrained UAV-enabled cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5576-5580, May 2022.

[78] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K. -K. Wong, "IRS-assisted secure UAV transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140-1152, Feb. 2022.

[79] H. Lu, Y. Zeng, S. Jin, and R. Zhang, "Aerial intelligent reflecting surface: Joint placement and passive beamforming design with 3D beam flattening," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4128-4143, Jul. 2021.

[80] X. Hao, H. Ma, W. Wang, F. Zeng, K. Cumanan, and E. Bjrnson, "UAV-mounted RIS enabled maritime secure sensing with joint beamforming and trajectory design," *IEEE Trans. Veh. Technol.*, vol. 74, no. 9, pp. 14833-14837, Sep. 2025.

Wei Wang (Member, IEEE) received the Ph.D. degree in communication and information system from Shanghai University, Shanghai, China, in 2011. Since 2011, he has been with Nantong University, China, where he is currently a Professor with the School of Information Science and Technology. From February 2016 to August 2016, he was a Visiting Scholar in the Department of Electrical and Computer Engineering at the Boise State University, ID, USA. From February 2019 to August 2019, he was an Academic Visitor in the Department of Electronic Engineering at the University of York, York, UK. His current research interests include unmanned aerial vehicle communications, maritime communications, and integrated sensing and communications.



Xu Hao received the B.S. degree in communication engineering from Dalian Minzu University, China, in 2023. He is currently pursuing the M.S. degree in information and communication engineering from Nantong University, China. His research interests include unmanned aerial vehicle communications, reconfigurable intelligent surfaces(RIS), and wireless information surveillance.

Lei Wu received the B.S. degree in Communication Engineering from Anhui Jianzhu University, China, in 2019, and the M.S. degree in Information and Communication Engineering from Nantong University, China, in 2023. He is currently pursuing the Ph.D. degree at the School of Electronic Information, Wuhan University, Wuhan, China. His research interests include Unmanned Aerial Vehicle communication and wireless communication coverage.

Feng Zeng received the B.S. degree in electronic and information engineering from China West Normal University, China, in 2005, and the M.S. degree in optical engineering from the Zhejiang University of Technology, China, in 2010. Since 2011, she has been with Nantong University, Nantong, China, where she is currently an Experimenter with the School of Information Science and Technology. Her research interests include Unmanned Aerial Vehicle communication and maritime communications.

Nan Zhao (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. He is currently a Professor at Dalian University of Technology, China.

Dr. Zhao is serving on the editorial boards of IEEE Wireless Communications and IEEE Wireless Communications Letters. He won the best paper awards in IEEE VTC 2017 Spring, ICNC 2018, WCSP 2018 and WCSP 2019. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.

Kanapathippillai Cumanan (Senior Member, IEEE) received the BSc degree with first class honors in electrical and electronic engineering from the University of Peradeniya, Sri Lanka in 2006 and the PhD degree in signal processing for wireless communications from Loughborough University, Loughborough, UK, in 2009.

He is currently a Professor of Wireless Communications at the School of Physics, Engineering and Technology, University of York, UK. His research interests include non-orthogonal multiple access (NOMA), cell-free massive MIMO, physical layer security, cognitive radio networks, convex optimization techniques and resource allocation techniques. He has published more than 100 journal articles and conference papers which have collectively received more than 5000 Google scholar citations.

Emil Björnson (Fellow, IEEE) received the M.S. degree in engineering mathematics from Lund University, Sweden, in 2007, and the Ph.D. degree in telecommunications from the KTH Royal Institute of Technology, Sweden, in 2011.

He is currently a Professor of wireless communication with the KTH Royal Institute of Technology. He has a podcast and YouTube channel called Wireless Future. His research focuses on multi-antenna communications, reconfigurable intelligent surfaces, radio resource allocation, and machine learning for communications. He has authored four textbooks and published much simulation code. He is a Digital Futures Fellow, a Wallenberg Academy Fellow, and a Clarivate Highly Cited Researcher. He received the 2018 and 2022 IEEE Marconi Prize Paper Awards in Wireless Communications, the 2019 EURASIP Early Career Award, the 2019 IEEE Communications Society Fred W. Ellersick Prize, the 2019 IEEE Signal Processing Magazine Best Column Award, the 2020 Pierre-Simon Laplace Early Career Technical Achievement Award, the 2020 CTTC Early Achievement Award, the 2021 IEEE ComSoc RCC Early Achievement Award, the 2023 IEEE ComSoc Outstanding Paper Award, and the 2024 IEEE Stephen O. Rice Prize.