



Deposited via The University of York.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/199246/>

Version: Accepted Version

---

**Article:**

Wu, Lei, Wang, Wei, Ji, Zengshuan et al. (2023) UAV-Assisted Maritime Legitimate Surveillance: Joint Trajectory Design and Power Allocation. IEEE Transactions on Vehicular Technology. ISSN: 0018-9545

<https://doi.org/10.1109/TVT.2023.3276323>

---

**Reuse**

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.

# UAV-Assisted Maritime Legitimate Surveillance: Joint Trajectory Design and Power Allocation

Lei Wu, Wei Wang, *Member, IEEE*, Zengshuan Ji, Yongjie Yang, Kanapathippillai Cumanan, *Senior Member, IEEE*, Gaojie Chen, *Senior Member, IEEE*, Zhiguo Ding, *Fellow, IEEE*, and Octavia A. Dobre, *Fellow, IEEE*

**Abstract**—This paper investigates a novel maritime wireless surveillance scenario, where a legitimate monitor vessel moves around to eavesdrop the suspicious communication from a suspicious unmanned aerial vehicle (UAV) to a suspicious vessel with the help of a cooperative UAV. Specifically, the cooperative UAV can adjust its jamming power and trajectory to exactly control the transmission rate of the suspicious link, thus improving the monitor vessel’s surveillance performance. Furthermore, since the cooperative UAV cannot land or replenish energy on the sea surface, its jamming power allocation on the ocean should be carefully designed by the energy thresholds. Under such setup, we formulate a sum eavesdropping rate maximization problem, which jointly optimizes the jamming power and three-dimensional (3D) trajectory of the cooperative UAV, as well as the two-dimensional (2D) trajectory of the monitor vessel. To address this non-convex optimization problem, we decompose the design problem into three subproblems and propose an iterative algorithm to find its suboptimal solution. Numerical results show that the proposed jamming-assisted 3D joint design can significantly improve the eavesdropping rate and save the jamming power compared to the benchmark schemes.

**Index Terms**—Maritime legitimate surveillance, UAV cooperative jamming, power allocation, trajectory design.

## I. INTRODUCTION

Nowadays, wireless information surveillance is considered as a promising technique to deal with the increasing suspi-

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

Lei Wu, Wei Wang, Zengshuan Ji and Yongjie Yang are with the School of Information Science and Technology, Nantong University, Nantong 226019, China, and also with the Nantong Research Institute for Advanced Communication Technologies, Nantong 226019, China (e-mail: 2010310027@stmail.ntu.edu.cn, wwang2011@ntu.edu.cn, 2010310045@stmail.ntu.edu.cn, Yang.yj@ntu.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).

Gaojie Chen is with 5GIC & 6GIC, Institute for Communication Systems, University of Surrey, Guildford GU2 7XH, U.K. (e-mail: gaojie.chen@surrey.ac.uk).

Zhiguo Ding is with the Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, UAE, and with the Department of Electrical and Electronic Engineering, The University of Manchester, Manchester M13 9PL, U.K. (e-mail: zhiguo.ding@manchester.ac.uk).

Octavia A. Dobre is with the Faculty of Engineering and Applied Science, Memorial University, St. Johns, NL A1B 3X5, Canada (e-mail: odobre@mun.ca)

This work was supported in part by the Future Network Scientific Research Fund Project under Grant FNSRFP-2021-YB-42, in part by the Science and Technology Program of Nantong under Grant JC2021016 and in part by the Key Research and Development Program of Jiangsu Province under Grant BE2021013-1. (*Corresponding author: Wei Wang*)

cious communication [1]. Till now, one recognized wireless surveillance strategy is called proactive eavesdropping. For instance, in [2], the authors first proposed a full-duplex-assisted proactive eavesdropping scheme, where the monitor can simultaneously eavesdrop the suspicious links and purposely send jamming signals. However in practice, the self interference cancellation is challenging to achieve as perfect. Such jamming-assisted proactive eavesdropping was then extended to a half-duplex parallel fading channels in [3]. In [4], the multi-antenna techniques were applied at the monitor to achieve more efficient jamming. Moreover, in [5], the authors proposed a spoofing relay-assisted proactive eavesdropping strategy to overhear the suspicious link.

In contrast to the aforementioned works, e.g., [1]–[5], mainly focus on the ground surveillance scenarios, the unmanned aerial vehicles (UAVs)-assisted legitimate surveillance has recently drawn significant attentions due to the agile maneuverability [6]–[8]. In [9], the authors first investigated a wireless surveillance in a UAV-aided suspicious communication network. In [10], the authors considered a UAV-assisted proactive eavesdropping in a suspicious multi-relay system. This UAV-assisted proactive eavesdropping was then extended to multiple suspicious links in [11], where the sum eavesdropping rate was maximized by jointly designing the jamming power and UAV’s position. In [12], the authors studied a wireless surveillance of UAV communication system, where a legitimate UAV tried to eavesdrop the transmission of suspicious UAVs. Furthermore, in [13], the authors considered a multi-UAV-enabled wireless surveillance system, where there were three UAVs collaboratively eavesdropped on suspicious wireless transmitters on the ground.

Recently, UAVs have been extended to maritime communication scenarios [14]–[16], which makes maritime safety more vulnerable to threats, since these maritime UAVs may be misused by the illegal authorities to commit crimes. However, the works in [1]–[5], [9]–[13] only considered the terrestrial cases, which may not be applicable to UAV-assisted maritime surveillance scenarios. This is mainly due to the fact that the vessels on the ocean, unlike the users in the terrestrial case with random distributions and static patterns, often have unique characteristics in terms of both distribution and mobility. Furthermore, since the UAV cannot land or replenish energy on the sea surface, its power allocation on the ocean should be carefully designed by the energy thresholds. Motivated by the aforementioned facts, in this paper we

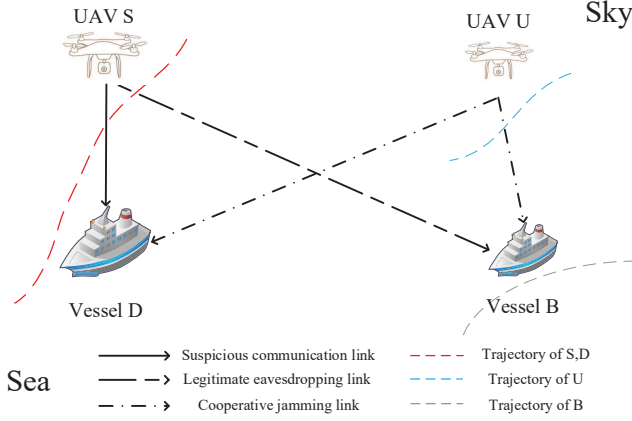


Fig. 1: Illustration of a UAV-assisted maritime surveillance scenario.

study a new maritime surveillance system, where a legitimate monitor vessel moves around to eavesdrop the suspicious communication from a suspicious UAV to a suspicious vessel with the help of an energy-constrained cooperative UAV. In particular, the mobility of both maritime vessels and UAVs are taken into account. Moreover, we adopt a practical UAV-vessel channel model that includes both large-scale and small-scale fading components. Our objective is to maximize the sum eavesdropping rate over all time slots by jointly optimizing the cooperative UAV three-dimensional (3D) trajectory and jamming power, and the monitor vessel two-dimensional (2D) trajectory under the mobility, security, and power-limited constraints. The main contributions are summarized as follows:

1) In the existing literature, this paper is the first attempt to investigate the proactive eavesdropping in the UAV-assisted maritime surveillance scenarios. Specifically, we consider a more practical UAV-vessel channel model and formulate an optimization problem by taking into account the mobility of both vessels and UAVs.

2) In each iteration, we derive closed-form expressions for the jamming power, UAV and vessel trajectories. Different from the terrestrial proactive eavesdropping scheme, the proposed maritime proactive jamming scheme cannot only covertly disturb the suspicious receivers with the channel qualities, but also effectively save the jamming power by the energy thresholds.

3) For the energy-constrained UAV-assisted maritime surveillance scenario, the proposed jamming-assisted 3D joint design can significantly improve the eavesdropping rate and save the jamming power compared to the benchmark schemes in the literature.

*Notations:* Non-boldface and boldface letters denote scalars and vectors, respectively.  $|\cdot|$ ,  $\|\cdot\|$  and  $\mathbb{E}(\cdot)$  denote the absolute value, Euclidean norm, and statistical expectation, respectively. The distribution of a circular symmetric complex Gaussian vector with mean vector  $\mathbf{x}$  and covariance matrix  $\Sigma$  is denoted by  $\mathcal{CN}(\mathbf{x}, \Sigma)$ .

## II. SYSTEM MODEL AND PROBLEM FORMULATION

A UAV-assisted maritime legitimate surveillance system is considered as shown in Fig. 1, where a monitor vessel  $B$  tries to overhear the suspicious communication from a suspicious UAV  $S$  to a suspicious vessel  $D$  with the help of a cooperative UAV  $U$ . In practice, the vessel  $D$  and UAV  $S$  on the ocean often follow a set of predefined sea lanes for safety [14]–[16]. Specifically, since the cooperative UAV  $U$  cannot land or replenish energy on the sea surface, its jamming power allocation on the ocean should be carefully designed among all time slots. We consider a particular UAV's flight time  $T$ , which is discretized into  $N$  time slots with equal duration  $d_t = T/N$ , where  $\mathcal{N} \triangleq \{1, 2, \dots, N\}$  denotes the set of slots. Furthermore, a 3D Cartesian coordinate system is considered, where the coordinates of the vessel  $B$  and UAV  $U$  can be denoted as  $(x_B[n], y_B[n], 0)$  and  $(x_U[n], y_U[n], z_U[n])$ , respectively. Additionally, the coordinates  $(x_D[n], y_D[n], 0)$  and  $(x_S[n], y_S[n], z_S[n])$  represent the location of the suspicious vessel  $D$  and UAV  $S$ , respectively. Under the above setting, the mobility constraints of the vessel  $B$  and UAV  $U$  can be formulated as

$$\|\mathbf{q}_B[n] - \mathbf{q}_B[n-1]\| \leq V_B d_t, \quad (1a)$$

$$\|\mathbf{q}_U[n] - \mathbf{q}_U[n-1]\| \leq V_{U,h} d_t, \quad (1b)$$

$$|z_U[n] - z_U[n-1]| \leq V_{U,v} d_t, \quad (1c)$$

$$z_{min} \leq z_U[n] \leq z_{max}, \forall n \in \mathcal{N}, \quad (1d)$$

where  $\mathbf{q}_B[n] = (x_B[n], y_B[n])$  and  $\mathbf{q}_U[n] = (x_U[n], y_U[n])$  represent the horizontal coordinate in time slot  $n$ , respectively. The symbols  $z_{min}$  and  $z_{max}$  denote the minimum and maximum flight altitudes of UAV  $U$ , respectively. The symbols  $V_B$ ,  $V_{U,h}$  and  $V_{U,v}$  represent the maximum horizontal and vertical speed of the vessel  $B$  and UAV  $U$ , respectively. Moreover, to ensure the secrecy of eavesdropping activities, we define the following security distance constraint:

$$\{d_{BS}[n], d_{BD}[n]\} \geq d_{Bmin}, \quad (2a)$$

$$\{d_{US}[n], d_{UD}[n]\} \geq d_{Umin}, \quad (2b)$$

where  $d_{ij}[n] = \sqrt{\|\mathbf{q}_i[n] - \mathbf{q}_j[n-1]\|^2 + |z_i[n] - z_j[n]|^2}$ ,  $i, j \in \{B, U, S, D\}$ , indicates the distance from  $i$  to  $j$  at slot  $n$ . The symbols  $d_{Bmin}$  and  $d_{Umin}$  are the minimum safe distance.

In addition, we consider a more practical UAV-vessel channel model [14]–[16], which can be defined by

$$\begin{aligned} h_{ij}[n] &= g_{ij}[n] \tilde{h}_{ij}[n] \\ &= \beta_0 d_{ij}^{-2}[n] \left( \sqrt{\frac{K[n]}{K[n]+1}} + \sqrt{\frac{1}{K[n]+1}} \phi_{ij} \right)^2, \end{aligned} \quad (3)$$

where  $g_{ij}$  and  $\tilde{h}_{ij}[n]$  represent the large-scale and small-scale fading coefficients, respectively. The symbol  $\phi_{ij} \in \mathcal{CN}(0, 1)$ , and  $\beta_0$  and  $K[n]$  denote the reference power gain and Rician factor, respectively. In general, the sea lanes of the vessels can be obtained from the Automatic Identification System (AIS) and thus the coefficients  $g_{ij}$  and  $K[n]$  are available [14]–[16].

Since the UAV  $U$  is powered by an energy-limited onboard battery and cannot replenish energy on the sea surface, the jamming power  $P_U[n]$  needs to meet the following constraints:

$$\sum_{n=1}^N P_U[n] \leq E, \quad (4a)$$

$$0 \leq P_U[n] \leq P_{Umax}, \quad (4b)$$

where  $E$  and  $P_{Umax}$  denote the total and the maximum jamming power, respectively. Based on the above setting, at time slot  $n \in \mathcal{N}$ , the achievable average rate of the eavesdropping link and the suspicious link can be derived respectively as

$$R_B[n] = \mathbb{E} \left\{ \log_2 \left( 1 + \frac{P_S[n]h_{SB}[n]}{N_0 + \lambda P_U[n]h_{UB}[n]} \right) \right\}, \quad (5a)$$

$$R_D[n] = \mathbb{E} \left\{ \log_2 \left( 1 + \frac{P_S[n]h_{SD}[n]}{N_0 + P_U[n]h_{UD}[n]} \right) \right\}, \quad (5b)$$

where  $P_S[n]$  denotes the transmit power of the UAV  $S$ . The symbols  $N_0$  denotes the noise power and  $\lambda$  represents the interference cancellation factor. Therefore, as defined in [9], [10], the effective eavesdropping rate can be expressed as

$$R_{BE}[n] = \begin{cases} R_D[n], & R_B[n] \geq R_D[n], \\ 0, & R_B[n] < R_D[n]. \end{cases} \quad (6)$$

Our objective is to maximize the sum eavesdropping rate over all time slots by jointly optimizing the jamming power and 3D trajectory of the UAV  $U$ , and the 2D trajectory of the vessel  $B$ , subject to the mobility, security, and power-limited constraints. This optimization problem is formulated as

$$\begin{aligned} & \max_{\mathbf{q}_B[n], \{\mathbf{q}_U[n], z_U[n]\}, P_U[n]} \sum_{n=1}^N R_{BE}[n] \\ & \text{s.t. (1), (2), (4).} \end{aligned} \quad (7)$$

Since the problem defined in (7) contains highly non-linear objective functions (both numerator and denominator of  $R_B[n]$  and  $R_D[n]$  depend on the optimization variables  $\{\mathbf{q}_B[n], \mathbf{q}_U[n], z_U[n]\}$ ); it is challenging to obtain the global optimal solution. In the following section, we propose an iterative algorithm to circumvent this non-convexity issue.

### III. PROPOSED ITERATIVE ALGORITHM

To efficiently solve problem (7), we first introduce an indicator function  $R[n]$ , which is defined as

$$R[n] = \begin{cases} 1, & R_B[n] \geq R_D[n], \\ 0, & R_B[n] < R_D[n]. \end{cases} \quad (8)$$

Then, problem (7) is equivalently reformulated as follows:

$$\begin{aligned} & \max_{\mathbf{q}_B[n], \{\mathbf{q}_U[n], z_U[n]\}, P_U[n]} \sum_{n=1}^N R[n]R_D[n] \\ & \text{s.t. } R[n] = \{0, 1\}, \\ & \quad (1), (2), (4). \end{aligned} \quad (9)$$

In the following, we propose an iterative algorithm to find an approximated optimal solution.

#### A. Optimization of the vessel $B$ trajectory $\mathbf{q}_B[n]$

For given UAV  $U$  trajectory  $\{\mathbf{q}_U[n], z_U[n]\}$  and transmit power  $P_U[n]$ , problem (9) is simplified as

$$\begin{aligned} & \max_{\mathbf{q}_B[n]} \sum_{n=1}^N R[n]R_D[n] \\ & \text{s.t. } R[n] = \{0, 1\}, \\ & \quad (1a), (2a). \end{aligned} \quad (10)$$

For the given  $R_D[n]$ , it is obvious that if we want the objective function in (10) to increase, the number of  $R[n] = 1$  slots increases, which needs more slots satisfy  $R_B[n] \geq R_D[n]$ . Thus, we rewrite problem (10) into the following form:

$$\begin{aligned} & \max_{\mathbf{q}_B[n]} \sum_{n=1}^N R_B[n] \\ & \text{s.t. (1a), (2a).} \end{aligned} \quad (11)$$

Problem (11) is challenging to be directly solved due to the small-scale fading  $\tilde{h}_{ij}[n]$  constraints in the numerator and denominator of  $R_B[n]$ . Thus, we first derive the lower bound of  $R_B[n]$  as follows:

$$\begin{aligned} R_B[n] &= \mathbb{E} \left\{ \log_2 \left( 1 + \frac{P_S[n]h_{SB}[n]}{N_0 + \lambda P_U[n]h_{UB}[n]} \right) \right\} \\ &\geq \log_2 \left( 1 + \frac{P_S[n]g_{SB}[n]}{N_0 + \lambda P_U[n]g_{UB}[n]\Gamma_{max}} \right) = R_B^{lb}[n], \end{aligned} \quad (12)$$

where  $\Gamma_{max}$  represents the upper bound of small-scale fading between UAV  $U$  and vessel  $B$ , and  $R_B^{lb}[n]$  denotes the lower bound of  $R_B[n]$ . Then, by introducing a slack variable  $r_n[n] = \frac{\beta_0 P_S[n]}{N_0 + \lambda P_U[n]g_{UB}[n]\Gamma_{max}}$ , we have the first-order Taylor series expansions of  $R_B^{lb}[n] = \log_2 \left( 1 + \frac{r_n[n]}{d_{SB}^2[n]} \right)$  as follows:

$$\begin{aligned} & \log_2 \left( 1 + \frac{r_n[n]}{d_{SB}^2[n]} \right) \\ & \geq \log_2 \left( 1 + \frac{r_n[n]}{d_{SB_{fea}}^2[n]} \right) - \frac{r_n[n](d_{SB}^2[n] - d_{SB_{fea}}^2[n])}{\ln 2 (d_{SB_{fea}}^4[n] + r_n[n]d_{SB_{fea}}^2[n])}, \end{aligned} \quad (13)$$

where  $d_{SB_{fea}}[n]$  is the feasible solution at the  $(l-1)$ th iteration. As a result, based on (12) and (13), problem (11) is approximately transformed into the following form:

$$\begin{aligned} & \max_{\mathbf{q}_B[n]} \sum_{n=1}^N \log_2 \left( 1 + \frac{r_n[n]}{d_{SB_{fea}}^2[n]} \right) - \frac{r_n[n](d_{SB}^2[n] - d_{SB_{fea}}^2[n])}{\ln 2 (d_{SB_{fea}}^4[n] + r_n[n]d_{SB_{fea}}^2[n])} \\ & \text{s.t. (1a), (2a).} \end{aligned} \quad (14)$$

Note that problem (14) is a convex optimization problem, which can be optimally solved by the interior-point method [14], [15].

### B. Optimization of the UAV $U$ trajectory $\{\mathbf{q}_U[n], z_U[n]\}$

For given  $\mathbf{q}_B[n]$  and  $P_U[n]$ , problem (9) is recast as

$$\begin{aligned} \max_{\{\mathbf{q}_U[n], z_U[n]\}} & \sum_{n=1}^N R[n]R_D[n] \\ \text{s.t.} & R[n] = \{0, 1\}, \\ & (1b) \sim (1d), (2b). \end{aligned} \quad (15)$$

Based on 5(a) and 5(b), to guarantee  $R_B[n] \geq R_D[n]$ , the UAV  $U$  should be close to the suspicious vessel  $D$  with the given  $\mathbf{q}_B[n]$  and  $P_U[n]$ , which implies that the achievable rate  $R_D[n]$  will decrease. Therefore, problem (15) is rewritten as follows:

$$\begin{aligned} \min_{\{\mathbf{q}_U[n], z_U[n]\}} & \sum_{n=1}^N R_D[n] \\ \text{s.t.} & (1b) \sim (1d), (2b). \end{aligned} \quad (16)$$

Similarly, we can derive the upper bound of  $R_D[n]$  as follows:

$$\begin{aligned} R_D[n] &= \mathbb{E} \left\{ \log_2 \left( 1 + \frac{P_S[n]h_{SD}[n]}{N_0 + P_U[n]h_{UD}[n]} \right) \right\} \\ &\leq \log_2 \left( 1 + \frac{P_S[n]g_{SD}[n]}{N_0 + P_U[n]g_{UD}[n]\Gamma_{min}} \right) = R_D^{up}[n], \end{aligned} \quad (17)$$

where  $\Gamma_{min}$  represents the lower bound of small-scale fading between UAV  $U$  and vessel  $D$ , and  $R_D^{up}[n]$  denotes the upper bound of  $R_D[n]$ . Then, by substituting (17) into (16), problem (16) reduces to an equivalent form as

$$\begin{aligned} \min_{\{\mathbf{q}_U[n], z_U[n]\}} & \sum_{n=1}^N \log_2 \left( 1 + \frac{P_S[n]g_{SD}[n]}{N_0 + P_U[n]g_{UD}[n]\Gamma_{min}} \right) \\ \text{s.t.} & (1b) \sim (1d), (2b). \end{aligned} \quad (18)$$

It is obvious that the problem in (18) can be solved by standard convex optimization technique, such as CVX [17].

### C. Optimization of the UAV $U$ transmit power $P_U[n]$

With the fixed variables  $\mathbf{q}_B[n]$  and  $\{\mathbf{q}_U[n], z_U[n]\}$ , problem (9) is expressed as

$$\begin{aligned} \max_{P_U[n]} & \sum_{n=1}^N R[n]R_D[n] \\ \text{s.t.} & R[n] = \{0, 1\}, \\ & (4a), (4b). \end{aligned} \quad (19)$$

To solve problem (19), we provide the following important theorem.

**THEOREM 1.** *The optimal transmit power  $P_U[n]$  of problem (19) can be derived as follows:*

$$P_U[n] = \begin{cases} P_U^*[n], & 0 \leq P_U^*[n] \leq P_{Umax}, \\ 0, & \text{otherwise,} \end{cases} \quad (20)$$

where  $P_U^*[n] = \frac{N_0(g_{SD}[n]-g_{SB}[n])}{g_{UD}[n]g_{SB}[n]\Gamma_{min}-\lambda g_{UB}[n]g_{SD}[n]\Gamma_{max}}$ .

---

### Algorithm 1 The Proposed Iterative Algorithm

---

**Input:**  $(x_B^0, y_B^0)$ ,  $(x_U^0, y_U^0, z_U^0)$ ,  $P_U^0$  and  $E$ ;  
1: **Set**  $l_{max} = 50$ ,  $l = 0$ ,  $\gamma = 10^{-5}$ ,  $R_0^l = 0$ , and  $R_f^l = 100$ ;  
2: **while**  $R_f^l > \gamma$  and  $l < l_{max}$  **do**  
3:   Let  $l = l + 1$   
4:   Calculate  $(x_B^l, y_B^l)$  of (14) for given  $(x_U^{l-1}, y_U^{l-1}, z_U^{l-1})$  and  $P_U^{l-1}$ ;  
5:   Calculate  $(x_U^l, y_U^l, z_U^l)$  of (18) based on  $(x_B^l, y_B^l)$  and  $P_U^{l-1}$ ;  
6:   Calculate  $P_U^l$  of (20) under given  $(x_B^l, y_B^l)$  and  $(x_U^l, y_U^l, z_U^l)$ ;  
7:   Determine  $R_{BE}^l = \sum_{n=1}^N R[n]R_D^{ub}[n]$  and  $R_f^l = |R_0^l - R_{BE}^l|$ ;  
8:   Update  $R_0^{l+1} = R_{BE}^l$ ;  
9: **end while**  
**Output:**  $(x_B^l, y_B^l)$ ,  $(x_U^l, y_U^l, z_U^l)$ ,  $P_U^l$  and  $R_{BE}^l$ .

---

*Proof:* When the total jamming power  $E$  is large enough, for given  $\mathbf{q}_B[n]$  and  $\{\mathbf{q}_U[n], z_U[n]\}$ , to guarantee  $R_B[n] \geq R_D[n]$ , i.e.,  $R_B^{lb}[n] \geq R_D^{up}[n]$ , the UAV  $U$  should send the jamming signal with the power  $P_U[n] \geq \frac{N_0(g_{SD}[n]-g_{SB}[n])}{g_{UD}[n]g_{SB}[n]\Gamma_{min}-\lambda g_{UB}[n]g_{SD}[n]\Gamma_{max}}$ . Due to the fact that  $R_D^{up}[n] = \log_2 \left( 1 + \frac{P_S[n]g_{SD}[n]}{N_0 + P_U[n]g_{UD}[n]\Gamma_{min}} \right)$ ,  $R_D^{up}[n]$  is strictly monotonically decreasing with respect to  $P_U[n]$ , and it can be observed that when  $P_U[n] = \frac{N_0(g_{SD}[n]-g_{SB}[n])}{g_{UD}[n]g_{SB}[n]\Gamma_{min}-\lambda g_{UB}[n]g_{SD}[n]\Gamma_{max}}$ ,  $R_D^{up}[n]$  can obtain maximum value. Hence, when  $R_B^{lb}[n] = R_D^{up}[n]$ , the optimal transmit power  $P_U[n]$  can be derived as in (20). Next, if  $E$  is limited, the UAV  $U$  cannot send the optimal jamming power at every time slot  $n$ , which leads to  $R_B[n] < R_D[n]$  in some time slots. Thus, in this case, the jamming signal will not be sent for saving power to obtain more effective eavesdropping rate, i.e., we have  $P_U[n] = 0$ .

### D. Overall algorithm

In this subsection, based on the results presented in the previous three subsections, we develop an iterative algorithm, which is summarized in Algorithm 1. In each iteration, the problems defined in (14), (18) and (19) are alternately solved by using the existing standard convex optimization techniques, and thus a suboptimal solution of problem (9) can be obtained by the proposed iterative algorithm in Algorithm 1; the relevant details can be found in [15]. Furthermore, the whole complexity of the proposed algorithm in Algorithm 1 is  $\mathcal{O}(N_{ite}(N)^{3.5})$ , where  $N_{ite}$  and  $N$  denote the number of required iterations and time slots, respectively.

## IV. SIMULATION RESULTS

The parameters are set as follow. The coordinates of the initial and final positions of UAV  $U$  and vessel  $B$  are set to  $(x_U[0], y_U[0], z_U[0]) = (400, 0, 70)$  m and  $(x_U[N], y_U[N], z_U[N]) = (400, 300, 70)$

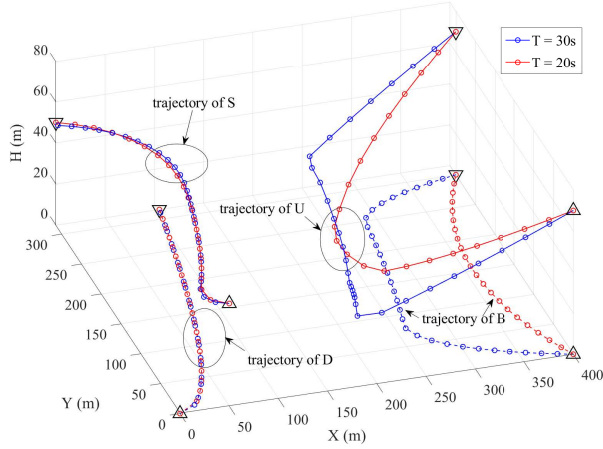


Fig. 2: Optimized UAV and vessel trajectories during different time durations  $T$ .

m, and  $(x_B[0], y_B[0], 0) = (400, 0, 0)$  m and  $(x_B[N], y_B[N], 0) = (400, 300, 0)$  m, respectively. Furthermore, unless otherwise specified, we set  $\beta_0 = -60$  dBm,  $N_0 = -110$  dBm [9]–[11],  $\Gamma_{max} = 1.35$ ,  $\Gamma_{min} = 0.65$  [14],  $P_S[n] = 25$  dBm,  $P_{U_{max}} = 25$  dBm,  $E = 400$  mW,  $V_B = 15$  m/s,  $V_{U,h} = 23$  m/s,  $V_{U,v} = 6$  m/s,  $z_{min} = 20$  m,  $z_{max} = 120$  m,  $d_{B_{min}} = 200$  m and  $d_{U_{min}} = 150$  m, respectively [15], [16].

Fig. 2 depicts the trajectories of the UAVs and vessels onto the 3D plane during different time durations  $T$ , respectively. The symbols  $\triangle$  and  $\nabla$  represent the initial and final positions of the UAVs and vessels, respectively. From the simulation results illustrated in Fig. 2, when  $T = 20$  s, both vessel  $B$  (dashed curves) and UAV  $U$  (solid curves) almost directly move (fly) to the final position. However, when  $T$  increases, the vessel  $B$  and UAV  $U$  first move quickly to the vessel  $D$ , then they follow the vessel  $D$  as long as possible. The reason is that the vessel  $B$  needs to follow the mobile vessel  $D$  to eavesdrop more information while UAV  $U$  moves closer to the vessel  $D$  to get the best position for jamming accordingly.

Fig. 3 illustrates the achievable eavesdropping rate versus different vessel speed  $V_B$  and time slots  $N$ , respectively. As shown in in Fig. 3, the achieved eavesdropping rate first increases and then decreases as the time slots  $N$  increases for all considered values of  $V_B$ . This is because the vessel  $B$  first comes closer to the vessel  $D$ , and then moves to the final location as the time slots  $N$  increases. Moreover, from Fig. 3, when the maximum vessel speed  $V_B$  is large, i.e.,  $V_B = 15$  m/s and  $V_B = 18$  m/s, the achieved maximum eavesdropping rate remains the same. This is because when  $V_B$  is large enough, the vessel  $B$  cannot fully use the maximum speed to approach the vessel  $D$  due to the fact that there is a minimum safe distance constraint.

Fig. 4 presents the jamming power of the UAV  $U$  versus different  $E$  thresholds and flight time  $N$ . As expected, the jamming power of the UAV  $U$  first decreases and then

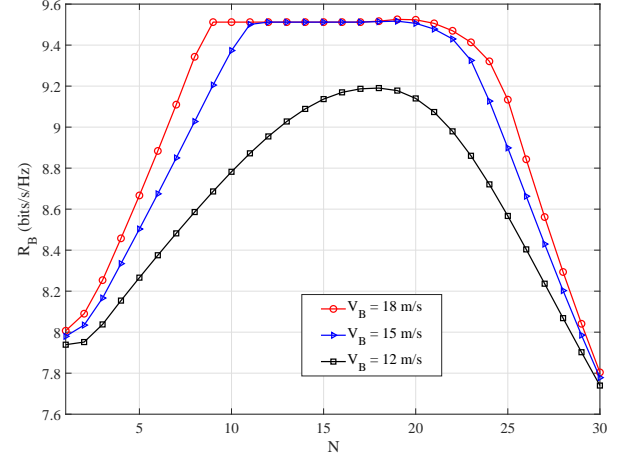


Fig. 3: Achieved eavesdropping rates at different vessel speed  $V_B$ .

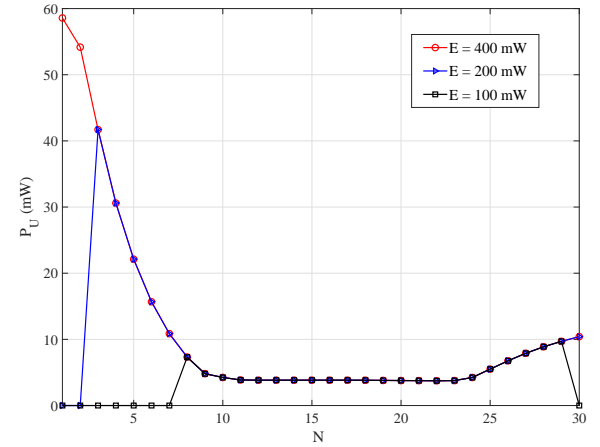


Fig. 4: Jamming power of the UAV  $U$  with different  $E$  thresholds.

increases as the flight time  $N$  increases, regardless of the total jamming power  $E$  value. This is because when  $N$  is small or large, the UAV  $U$  is far from the vessel  $D$ , and thus a larger jamming power  $P_U$  needs to be allocated to satisfy  $R_B[n] \geq R_D[n]$ . In addition, it is worth noting that when  $E$  is not large enough, i.e.,  $E = 200$  mW and  $E = 100$  mW, the UAV  $U$  reduces the jamming power  $P_U$  to zero for a certain period of time. This is because when  $E$  is limited, the UAV  $U$  cannot send the enough jamming power to satisfy  $R_B[n] \geq R_D[n]$  at every time slot  $n$ . Thus, for those time slots that far from the vessel  $D$ , the UAV  $U$  will not send jamming signal for saving power to obtain a more effective eavesdropping rate.

Fig. 5 compares the performance of our proposed jamming-assisted 3D joint design (denoted as Proposed scheme) with other three benchmark schemes with  $N = 30$ , namely: 1) The 2D joint design scheme (denoted as 2D scheme), i.e., the UAV  $U$  flight altitude  $z_U[n] = 70$  m [11]; 2) The time-slot

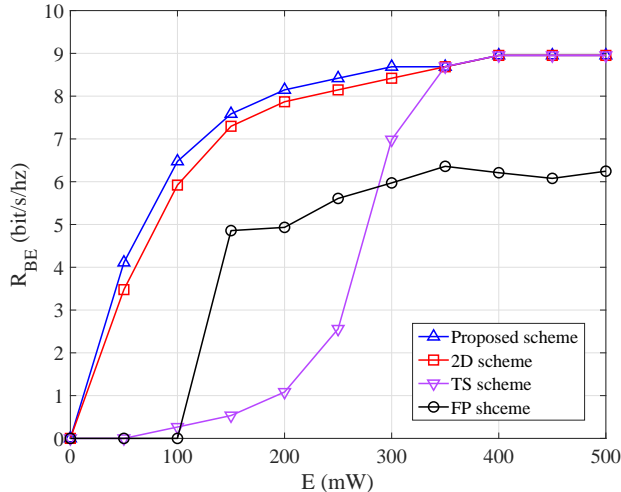


Fig. 5: Achieved effective eavesdropping rates of different algorithms versus  $E$ .

sequence allocation scheme (denoted as TS scheme), i.e., the UAV  $U$  jamming power allocation in time-slot sequence [5]; 3) The fixed power design scheme (FP scheme), i.e., the UAV  $U$  jamming power  $P_U[n] = \frac{E}{N}$  mW,  $\forall n \in \mathcal{N}$ . As shown in Fig. 5, when the total jamming power  $E$  is small, both TS and FP schemes cannot achieve the effective eavesdropping rate. This is because when  $E$  is limited, the UAV  $U$  still sends the jamming signal with the optimal power or the fixed power in some time slots that far from the vessel  $D$ , which leads to  $R_B[n] < R_D[n]$  on all time slots. Moreover, it is also observed that the Proposed scheme only requires less jamming power to achieve the same or better performance compared to the benchmark schemes. The reason is that the proposed algorithm can jointly optimize the jamming power and 3D trajectory of the UAV  $U$ , and thereby can save the jamming power based on the channel qualities.

## V. CONCLUSIONS

This paper has investigated the legitimate surveillance in a UAV-assisted maritime communication scenario. In the considered scheme, with the help of a cooperative UAV transmitting jamming noise, the jamming power and 3D trajectory of the cooperative UAV, as well as the 2D trajectory of the monitor vessel have been jointly optimized to maximize the sum eavesdropping rate under the mobility, security, and power-limited constraints. Simulation results have confirmed that the proposed jamming-assisted 3D joint design significantly improved the eavesdropping rate and saved the jamming power compared to the considered reference schemes.

## REFERENCES

[1] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152-159, Aug. 2017.

[2] 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.

[3] 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.

[4] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585-4599, Jul. 2017.

[5] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449-1461, Dec. 2016.

[6] W. Wu, F. Zhou, B. Wang, Q. Wu, C. Dong, and R. Q. Hu, "Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 78-85, Aug. 2022.

[7] 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.

[8] C. Wang et al., "Covert communication assisted by UAV-IRS," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 357-369, Jan. 2023.

[9] 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.

[10] G. Hu and Y. Cai, "UAVs-assisted proactive eavesdropping in AF multi-relay system," *IEEE Communications Letters*, vol. 24, no. 3, pp. 501-505, Mar. 2020.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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