# 大语言模型增强的抗灰洞攻击海域无人机路由算法

李杰铃,肖 亮*,王鹏程,雷 妍,陈乔鑫,王成耀
(厦门大学信息学院,福建厦门 361102)

**摘 要:** 无人机路由实现图像、音频和位置等多模态数据至部署大语言模型的船载目的节点的高效传输,支撑目标搜索等推断任务,适用于环境监测和搜索救援等海域业务.然而,在恶劣海域信道条件下,无人机网络拓扑快速变化,路由稳定性显著下降.同时,灰洞攻击选择性丢弃数据包,导致感知数据传输的丢包概率和时延大幅增加,甚至引发推断失败.为此,本文提出大语言模型增强的抗灰洞攻击海域无人机路由算法,根据大语言模型所推断出的环境特征以及相邻无人机成功转发的数据包数,建立路由信任体系,采用强化学习优化下一跳无人机和发射功率.面向海域业务服务质量需求,结合相邻无人机信任度,设计路由策略分布函数,适配无人机群的网络拓扑和信道变化,快速恢复中断路由.针对海上节点分布稀疏及信道快速变化导致的反馈丢失问题,在路由经验回放中引入反馈恢复机制,提升路由稳定性.搭建海域无人机路由系统,在船载目的节点部署参数量为70亿的大模型LLaVA-1.5,以图像和相邻无人机位置等信息为输入,识别环境特征并将结果反馈给无人机,增强路由策略优化.基于厦门欧厝海域实测信道数据,构建30架无人机防御具有不同丢包概率灰洞攻击的结果表明,所提算法可提升72.8%的数据包到达率,降低75.1%的端到端时延和64.7%的能耗,支撑海域大语言模型任务.

**关键词:** 大语言模型;海域无人机路由;灰洞攻击;强化学习;多模态数据

**基金项目:** 国家自然科学基金(No.U21A20444);中央高校基本科研业务费专项资金(No.20720250036);国家重点研发计划(No.2023YFB3107603)

**中图分类号:** TP393 **文献标识码:** A **文章编号:** 0372-2112(2025)12-4474-11

**电子学报URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250878

# LLM-Enhanced Maritime UAV Routing Algorithm Against Gray-Hole Attacks

LI Jie-ling, XIAO Liang*, WANG Peng-cheng, LEI Yan, CHEN Qiao-xin, WANG Cheng-yao
(*School of Infomatics*, *Xiamen University*, *Xiamen*, *Fujian* 361102, *China*)

**Abstract:** Unmanned aerial vehicle (UAV) routing enables the efficient transmission of multimodal data such as images, audio and location to the shipborne destination node equipped with a large language model (LLM) to support inference tasks including target search, which are applicable to maritime applications such as environmental monitoring and search and rescue. However, UAV network topologies change rapidly under harsh maritime channel conditions, resulting in significant degradation of routing stability. Meanwhile, gray-hole attacks selectively discard packets, leading to substantial increases in packet loss rate and transmission latency, and even causing inference failures. To address these challenges, this paper proposes an LLM-enhanced maritime UAV routing algorithm against gray-hole attacks that exploits the environment feature inferred by the LLM and the number of packets successfully forwarded by neighboring UAVs to construct a routing trust framework and applies reinforcement learning to jointly optimize the next hop UAV and the transmit power. The routing policy distribution function is formulated based on the quality-of-service requirements and the trust levels of the neighboring UAV, enabling rapid self-healing in response to dynamic network topologies and channel variations. To address feedback loss caused by sparse node distribution and rapidly varying channels in maritime environments, a feedback recovery mechanism is incorporated into routing experience replay to enhance routing stability. We develop a maritime UAV routing system, with the shipborne as the destination hosting a 7-billion-parameter LLaVA-1.5 model. Taking the captured images and one-hop neighbor information such as location as input, this model infers environment features and feeds the results

收稿日期:2025-11-25;录用日期:2025-12-18;责任编辑:宋甲英
*通讯作者:肖亮

back to UAVs to enhance the routing policy optimization. Based on measured channel data from the Oucuo sea area in Xiamen, a simulation scenario is constructed with 30 UAVs under gray-hole attacks with different packet loss probabilities. The results show that the proposed algorithm improves 72.8% packet delivery ratio, reduces 75.1% end-to-end latency and 64.7% energy consumption, and effectively supports LLM-driven maritime applications.

Key words: large language model; maritime unmanned aerial vehicle routing; gray-hole attacks; reinforcement learning; multimodal data

Foundation Item(s): National Natural Science Foundation of China (No.U21A20444); Fundamental Research Funds for the Central Universities (No.20720250036); National Key Research and Development Program of China (No.2023YFB3107603)

## 1　引言

海域无人机路由选择下一跳传输图像、音频、目标船只位置和温湿度等多模海洋数据至目的节点,支撑基于大语言模型的目标搜索和场景理解,适用于海上应急通信、海洋资源勘探及环境监测等海域业务[1,2]. 但是,海域立体通信系统受到复杂气象条件和突发性波浪等因素影响,由海面反射造成复杂快变的恶劣信道环境,导致路由稳定性低. 此外,由于海域网络覆盖范围广阔且节点间连通性复杂,其安全性极易受到路由攻击的威胁. 其中,灰洞攻击者伪造路由信息,宣称拥有到达目的节点的最优路径,诱导数据经过自身节点并选择性丢弃接收到的数据包,可在短时间内破坏路由连通性且隐蔽性强,导致海上监测数据缺失、搜救指令延迟甚至应急通信中断.

基于强化学习的路由技术无需依赖全局网络拓扑和攻击模型等信息,令各无人机根据位置和信道状态等环境观测信息持续优化路由策略,降低端到端时延和路由能耗,并提升数据包到达率[3~6]. 文献[5]提出基于深度强化学习的无人机路由算法,根据目的地位置以及与相邻无人机的距离,采用多智能体行动者-评论家算法优化下一跳,提升网络吞吐量. 文献[6]进一步提出跨层路由算法,根据信道状态以及与相邻无人机和目的无人机的距离等信息,联合优化下一跳和中继功率,提升路径连接概率. 但是,由于无人机网络具有分布式拓扑特性,其路由过程易受到恶意节点攻击. 文献[7]提出基于信任的安全路由算法,根据数据包到达率和路径正确性评估无人机信任值,并进一步基于无人机位置、业务负载和信任值等信息构建强化学习状态,优化路由选择,抵御恶意节点攻击. 然而,当存在具有不同丢包概率的攻击行为时,难以将其与由海域恶劣信道等环境因素导致的丢包区分开来,导致策略优化不准确,使路由性能明显下降.

为此,本文提出大语言模型增强的抗灰洞攻击海域无人机路由算法,基于推断的环境特征,如当前网络环境的恶劣程度,以及信道状态、路由跳数、无人机电池电量、节点信任度、风速和湿度等信息,采用强化学习持续优化路由选择和发射功率,适配海域恶劣信道变化,抵御灰洞攻击. 其中,部署大语言模型的船载目的节点根据无人机所发送的俯视视角图像以及相邻无人机位置和速度等信息,推断海域环境特征并反馈至无人机,构建强化学习状态以指示未来的信道增益和环境变化等信息,增强路由策略优化. 基于相邻无人机成功转发的数据包数量与大语言模型反馈的环境特征联合评估节点信任度,通过假设检验与历史路由经验进行对比,实现对灰洞攻击的准确检测与中断路由的快速恢复.

根据所选下一跳无人机的平均节点信任度,评估路由策略的安全性,避免选中因丢弃数据包而导致路由失败的灰洞节点. 进一步,基于端到端时延和数据包到达率构建风险函数,评估海域无人机业务的服务质量需求和路由性能的差异,提升路由策略的鲁棒性,降低因信任评估误差带来的策略风险,并适配无人机群的网络拓扑和信道变化. 此外,针对海上节点分布稀疏及信道快速变化所导致的反馈丢失问题,在路由经验回放中引入反馈恢复机制,提升路由稳定性.

基于搭载树莓派和摄像头的无人机搭建海域路由系统,发送图片和无人机位置等多模态数据至部署参数量为70亿的LLaVA-1.5-7B的船载目的节点,支撑基于大语言模型的目标搜索和场景理解,适用于环境监测等海域业务. 基于厦门欧厝海域实测信道数据,构建30架无人机抵御具有不同丢包概率的灰洞攻击的仿真场景. 结果表明,所提算法可提升72.8%的数据包到达率,并降低75.1%的端到端时延和64.7%的路由能耗. 此外,随着无人机数量的增加,所提海域无人机路由算法均优于基准算法.

## 2　相关工作

无人机路由基于位置信息和链路质量等信息,采用主动路由、洪泛和强化学习等技术优化路由策略,提高数据包到达率,降低端到端传输时延和路由开销[8~15]. 文献[10]提出了改进型的主动路由算法,将无人机位置信息与改进的估计传输计数度量方法结合,优化下一跳,从而提高了数据包到达率并降低端到端延迟和路由开销. 文献[11]提出了一种增强型洪泛的路由算法,采用随机网络编码和聚类技术,无需依赖路

由路径和网络拓扑信息，实现了高效路由并减少路由跳数和时延. 文献[12]则融合主机中心和内容中心思想，提出了一种高效可扩展的路由算法，通过主机中心模式复用稳定路径的路由信息，减少路径探索的泛洪开销，同时借助内容中心模式进行路由故障检测以适配网络变化. 文献[13]提出了一种基于强化学习的路由算法，基于无人机水平位置和电量优化信道与下一跳节点选择，并提出了基于一种动态学习率的迭代算法以加速收敛，适用于大规模灾区的应急通信. 文献[14]提出了一种基于强化学习的快速路由算法，利用无人机群的信道状态和相邻无人机的路由参数等信息，建立基于时延约束和经验共享的强化学习模型，优化转发决策和传输功率，降低能耗和时延. 以上无人机路由算法未考虑路由过程中可能存在的恶意节点行为，路由攻击会破坏数据转发过程并导致路径选择失效，显著降低数据包到达率.

为了应对来自内部恶意节点和外部窃听等多种安全路由威胁，基于协作检测、风险规避、统计检验方法和动态信誉值等多种安全路由机制被提出，旨在确保网络链路高效传输的同时，抵御恶意节点攻击，保障数据传输的安全性[16~21]. 文献[17]提出基于信任的进化式自协作路由算法，将自我检测和协作检测相结合，动态评估网络节点行为的信任度，从而有效防御路由网络中的灰洞攻击. 文献[18]提出基于强化学习的无人机抗干扰路由算法，基于路径可用历史、信道状态和接收的信号强度等信息优化发射功率和路由发现间隔，以提升路径质量评估的准确性. 文献[19]提出了基于统计分析的检测技术，利用柯尔莫哥洛夫-斯米尔诺夫双样本检验技术，识别路由中的恶意节点，以应对合谋劫持攻击，提升对恶意节点的定位精度和响应速度. 文献[20]提出了基于多路径的风险规避路由算法，利用将原始消息通过异或编码分割成多个无法单独破解的数据片，沿着一组攻击者不相交的多路径进行传输，确保在恶劣环境下，依然能通过分散风险有效防止路由信息被窃听，保障路由安全. 文献[21]提出一种基于动态信誉的安全路由算法，利用动态信誉机制技术识别路由网络中的恶意节点，有效降低丢包概率并提高网络吞吐量.

基于数据理论评估、行为验证方法及强化学习算法提出了多种可信路由机制，旨在通过信任评估优化可信节点的选择，从而有效防范恶意节点攻击并提升数据包传输可靠性和效率[22~26]. 文献[23]提出了一种基于模糊逻辑的可信路由算法，采用贝叶斯理论、证据理论、层次分析法及跨层度量，分别评估直接信任、间接信任、节点信任度及链路信任度，提升在Sybil攻击下的数据包到达率. 文献[24]提出了一种信任感知的路由算法，通过行为验证和一致性验证方法，评估原始及中继数据包的信任度，提高对恶意节点的检测准确率和精度. 已有研究将环境特征用于辅助路由选择，文献[25]提出了一种基于信任的水下机会路由算法，根据链路可靠性和能量可用性进行信任评估，并基于节点分布和环境特征等状态信息，采用强化学习算法优化路由选择，提升数据包到达率并降低时延. 文献[26]提出了一种上下文感知的可信水下路由算法，结合环境感知模块和信任评估管理，采用深度确定性策略梯度算法和经验优先回放机制，优化路径选择，有效区分因环境变化引起的波动与节点的恶意行为. 然而，这些路由方案仅将环境特征和节点信任度作为强化学习的输入特征，本文所提无人机路由算法进一步在信任度评估中引入了大模型反馈的环境特征，并基于服务质量需求与节点信任度联合构建路由策略分布函数，有效降低了选择高丢包概率及不满足服务质量需求的路由策略的概率. 此外，针对海上节点分布稀疏和复杂气象条件导致的反馈丢失问题，在路由经验回放中引入反馈恢复机制，提升路由稳定性和路径优化效率.

## 3 系统模型

本节介绍大语言模型增强的抗灰洞攻击海域无人机路由的网络模型、信道模型和攻击模型.

### 3.1 网络模型

如图1所示，$M$架海上无人机发送图像和文本等多模态数据至船载目的节点，用于执行目标搜索和场景理解等大语言模型推断任务[27]，适用于海上应急通信、环境监测和搜索救援等海域业务. 例如，在海上灾后应急救援场景中，每时隙源无人机$\kappa_s$卸载包含监控图像的$X$个数据包至部署大语言模型LLaVA-1.5-7B的目的节点，以识别受灾船只和搜索受困人员的位置.

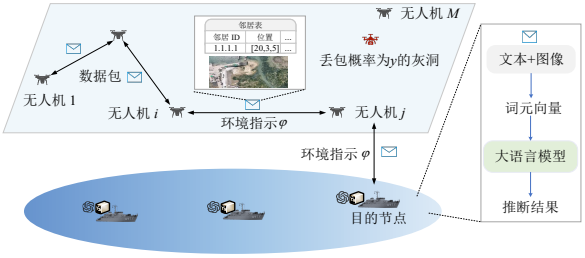



图1 大语言模型增强的抗灰洞攻击无人机路由

在第$k$个时隙，无人机$i$周期性广播包含自身位置$\boldsymbol{L}_i^{(k)}$、移动速度$v_i^{(k)}$和时间戳信息$t_i^{(k)}$的HELLO消息，以实现邻居发现和路由状态维护. 相邻无人机接收到广播信息后将位置等信息存储并更新于本地邻居表$\boldsymbol{T}^{(k)}$中. 每架无人机采用多模传感器采集图像信息$\boldsymbol{G}^{(k)}$，测量湿度$\chi^{(k)}$和风速$\tilde{v}^{(k)}$，估计与$N$个相邻无人机之间的信

道增益 $\boldsymbol{h}^{(k)}$ 和信任度 $\boldsymbol{f}^{(k)}$. 在此基础上,选择下一跳无人机 $a_1^{(k)}\in\{1,2,\cdots,N\}$,并以 $a_2^{(k)}\in[\bar{P},\underline{P}]$ 的发射功率将采集的图像数据 $\boldsymbol{G}^{(k)}$、邻居表信息 $\boldsymbol{T}^{(k)}$ 和接收到的上一跳图像数据 $\tilde{\boldsymbol{G}}^{(k)}$ 转发至所选下一跳.

部署大语言模型的船载目的节点接收到多模态数据,采用视觉编码器和分词器等模块,将多模态数据转化为词元向量,并根据路由业务需求生成相应的推断结果. 其中,大语言模型基于图像数据 $\boldsymbol{G}^{(k)}$ 和邻居表信息 $\boldsymbol{T}^{(k)}$ 推断环境指示 $\varphi^{(k)}$,以刻画当前无人机所处网络环境的恶劣程度并预测未来信道增益. 同时,船载目的节点统计端到端时延 $\tau^{(k)}$ 和数据包到达率 $\rho^{(k)}$,构建反馈信息 $\{\varphi^{(k)},\tau^{(k)},\rho^{(k)}\}$,并通过控制信道将该消息反馈给路由路径上的无人机.

### 3.2　信道模型

假设无人机 $i$ 和无人机 $j$ 之间的距离为 $d$,信道状态 $h_{i,j}$ 由路径损耗模型[28]决定,即

$$\mathrm{PL}(d)=\varsigma 10\log_{10}d+\mathrm{PL}_0,d\geqslant 1\ \mathrm{m} \tag{1}$$

其中,$\varsigma$ 为路径损耗指数,$\mathrm{PL}_0$ 为参考距离 1 m 的路径损耗. 根据文献[29,30]的海域路径损耗模型,无人机到船载节点的信道状态 $\tilde{h}$ 取决于海浪高度 $z$、频率参数 $c$ 以及无人机到船载节点的距离 $\tilde{d}$,即

$$\mathrm{PL}(\tilde{d})=10\left(z\left(\beta_1\log_{10}c+\beta_2\right)+2\right)\log_{10}\tilde{d}+\mathrm{PL}_0 \tag{2}$$

其中,$\beta_1$ 和 $\beta_2$ 分别表示海浪高度对路径损耗的影响参数和基础偏置. 特别地,有效波高 $\bar{z}$ 反映海浪高度 $z$ 的统计特性,可以表示为风速 $\tilde{v}$ 的函数[29],即 $\bar{z}=0.21\tilde{v}^2/\xi$,其中 $\xi$ 为重力加速度.

### 3.3　攻击模型

灰洞攻击者通过伪造或操纵路由控制信息,在路由建立初期伪装为可信节点,积极响应路由请求并宣称其为达到目的地的最短路径节点,从而参与数据转发过程. 一旦灰洞攻击者被选为中继无人机,将选择性丢弃部分数据包. 例如,灰洞攻击者转发路由包过程中,根据既定攻击策略以 $y\in(0,1]$ 的概率丢弃数据包,仅以 $1-y$ 概率转发数据包[31]. 此外,间歇性丢包攻击干扰了检测机制的判断,导致无人机难以准确识别数据包到达率下降是由海域网络环境恶化还是由灰洞攻击引起. 重要的符号如表1所示. 在不引起混淆的情况下,以下章节将省略上标 $k$.

**表1　重要符号列表**

| 符号 | 含义 |
|---|---|
| $M$ | 无人机数量 |
| $N$ | 相邻无人机数量 |
| $X$ | 转发的数据包数量 |
| $a_1^{(k)}$ | 下一跳无人机 |
| $a_2^{(k)}$ | 无人机发射功率 |
| $y^{(k)}$ | 灰洞攻击丢包概率 |
| $\boldsymbol{L}^{(k)}$ | 无人机位置 |
| $v^{(k)}$ | 无人机移动速度 |
| $b^{(k)}$ | 无人机电池电量 |
| $h_{i,j}^{(k)}$ | 无人机 $i$ 到无人机 $j$ 的信道增益 |
| $f_i^{(k)}$ | 相邻无人机 $i$ 的信任度 |
| $\tau^{(k)}$ | 端到端时延 |
| $\varpi^{(k)}$ | 路由能耗 |
| $\rho^{(k)}$ | 数据包到达率 |
| $\varphi^{(k)}$ | 大语言模型推断的环境指示 |

## 4　基于强化学习的抗灰洞攻击海域无人机路由算法

针对复杂快变海域环境的灰洞攻击,提出一种基于强化学习的可信无人机路由算法,简称RLTUR,传输多模态数据至船载目的节点,提升数据包到达率并降低路由时延和能耗,抵御灰洞攻击. 根据部署于船载目的节点的大语言模型所推断出的环境指示,结合相邻无人机成功转发的数据包数,建立无人机路由信任体系. 基于信道增益、无人机电池电量、湿度、风速,以及相邻无人机共享的信任度等信息,优化下一跳无人机选择与发射功率,算法运行流程如算法1所示.

**算法1　基于强化学习的可信无人机路由算法**

1. 初始化 $M,N,\boldsymbol{\theta}^{\mathrm{Q}},\boldsymbol{\theta}^{\mathrm{T}},\boldsymbol{\theta}^{\mathrm{R}},\varpi,\rho,\tau,\mathcal{D},\gamma$ 和 $J$
2. FOR $k=1,2,\cdots,K$ DO
3. 　接收 $X$ 个数据包
4. 　获取相邻无人机的位置信息 $\boldsymbol{L}^{(k)}$、移动速度 $\boldsymbol{v}^{(k)}$ 和信任度 $\boldsymbol{f}^{(k)}$
5. 　测量风速 $\tilde{v}$ 和湿度 $\chi$
6. 　估计与相邻无人机之间的信道增益 $\boldsymbol{h}$
7. 　根据式(3)构建 $\boldsymbol{s}^{(k)}$
8. 　输入 $\boldsymbol{s}^{(k)}$ 至 $\mathcal{Q},\mathcal{T}$ 和 $\mathcal{R}$ 获取 $\boldsymbol{Q},\boldsymbol{T}$ 和 $\boldsymbol{R}$
9. 　根据式(4)构建 $\boldsymbol{\pi}$
10. 　以 $a_2$ 的发射功率向下一跳节点 $a_1$ 发送 $X$ 个数据包
11. 　接收大模型推断的环境指示 $\varphi$,以及船载目的节点统计的数据包到达率 $\rho$ 和端到端时延 $\tau$
12. 　根据式(5)、(6)和(7)计算 $u^{(k)}$、$f^{(k)}$ 和 $r^{(k)}$
13. 　构建经验 $\left\{\boldsymbol{s}^{(k)},\boldsymbol{a}^{(k)},u^{(k)},r^{(k)},\boldsymbol{s}^{(k+1)},\boldsymbol{f}^{(k)}\right\}$ 并存入 $\mathcal{D}$
14. 　IF $|\mathcal{D}|\geqslant J$ do
15. 　　均匀随机采样 $J$ 条经验的样本
16. 　　根据式(8)、(9)和(10)更新 $\boldsymbol{\theta}^{\mathrm{Q}},\boldsymbol{\theta}^{\mathrm{T}}$ 和 $\boldsymbol{\theta}^{\mathrm{R}}$
17. 　END IF
18. END FOR

面向各种海域无人机业务的服务质量要求,基于路由时延和数据包到达率构建风险函数,并结合相邻无人机信任度,设计基于玻尔兹曼分布的路由策略函数,适配网络拓扑和海域恶劣信道变化,抵御不同丢包

概率的灰洞攻击. 此外,在路由经验池中引入了无人机信任度和策略风险值,并针对海上节点分布稀疏和复杂气象条件以及无人机移动速度各异导致的反馈丢失问题,在路由经验回放中引入反馈恢复机制,提升路由稳定性和路径优化效率.

具体而言,在第$k$个时隙,无人机从邻居表$\boldsymbol{T}$中获取当前相邻无人机数量$n$,以及所对应的位置$\boldsymbol{L}$和移动速度$v$,估计与相邻无人机的信道增益$\boldsymbol{h}$,测量自身电池电量$b$. 此外,通过搭载的传感器观测影响信号传播的湿度$\chi$和风速$\tilde{v}$,以预测未来信道增益的变化. 同时,无人机接收部署大语言模型的船载目的节点的反馈信息,提取推断的环境指示$\varphi$,以及统计的性能指标如路由时延$\tau$和数据包到达率$\rho$,其中,大语言模型基于提示词、邻居表信息和无人机所获取的俯视视角图像推断出环境指示. 基于相邻无人机成功转发的数据包数量和大语言模型推断的环境指示联合评估无人机信任度,避免因环境因素导致的丢包而将非恶意无人机误判为灰洞节点. 根据至多$N$个相邻无人机的位置$\boldsymbol{L}$、移动速度$\boldsymbol{v}$、信道增益$\boldsymbol{h}$、电池电量$\boldsymbol{b}$和信任度$\boldsymbol{f}$,以及环境指示$\varphi$、风速$\tilde{v}$和湿度$\chi$,构建状态$\boldsymbol{s}^{(k)}$为

$$\boldsymbol{s}^{(k)}=[n,\varphi,\boldsymbol{L},\boldsymbol{v},\boldsymbol{h},\boldsymbol{b},\boldsymbol{f},\chi,\tilde{v},\tau,\rho] \tag{3}$$

基于给定的网络状态和环境特征,优化包括下一跳无人机选择$a_1^{(k)}\in\{1,2,\cdots,N\}$和发射功率$a_2^{(k)}\in\left\{j\bar{P}/L|1\leqslant j\leqslant L\right\}$的路由策略$\boldsymbol{a}^{(k)}=\left[a_1^{(k)},a_2^{(k)}\right]$,则可选策略空间的大小为$F=NL$. 设计由两层全连接层组成的策略网络$\mathcal{Q}$、信任网络$\mathcal{T}$和风险网络$\mathcal{R}$,以状态$\boldsymbol{s}^{(k)}$作为输入,估计长期效益值$\boldsymbol{Q}=\left\{Q_i\right\}_{1\leqslant i\leqslant F}$、信任值$\boldsymbol{T}=\left\{T_i\right\}_{1\leqslant i\leqslant F}$和风险值$\boldsymbol{R}=\left\{R_i\right\}_{1\leqslant i\leqslant F}$,采用修正玻尔兹曼分布构建概率分布如式(4)所示:

$$\pi=\frac{\exp\left(T_iQ_i-R_i\right)}{\sum_{l=1}^{F}\exp\left(T_lQ_l-R_l\right)} \tag{4}$$

该分布倾向于选择具有更高信任值和长期效益值且更低风险值的路由策略,有效降低了选择具有较高丢包概率的下一跳节点概率,满足海域无人机业务的服务质量需求. 因此,无人机以$a_2^{(k)}$的发射功率向下一跳无人机$a_1^{(k)}$发送$X$个多模海洋数据包.

船载目的节点接收到数据包,通过本地部署的大语言模型推断环境指示$\varphi$,并统计路由性能指标如数据包到达率$\rho$和端到端时延$\tau$,通过反馈信道将其沿着路由路径发送给无人机. 此外,根据发射功率和持续时间,评估由转发引起的路由能耗$\varpi$. 由此,可根据数据包到达率$\rho$、端到端时延$\tau$和路由能耗$\varpi$评估无人机效益$u^{(k)}$,即

$$u^{(k)}=\rho-c_1\tau-c_2\varpi \tag{5}$$

基于相邻无人机成功转发的数据包数量$X'$以及接收到大模型反馈的环境指示$\varphi$,评估无人机信任度,以更好地区分由环境因素和攻击行为引起的丢包差异. 具体来说,构建检验统计量$X'/X$,其中$X$为相邻无人机接收到的数据包数量,并与检验阈值$\delta$进行比较,如果$X'/X\leqslant\delta$,无人机信任度减少$L_1$,若当前环境指示$\varphi>1$,即当前网络环境良好,则加速降低信任度,选择的下一跳无人机被视为灰洞的概率增大;若当前环境指示$\varphi\leqslant1$,即当前网络环境恶劣,信任度缓慢下降. 同理,如果$X'/X>\delta$,无人机信任度增加$L_2$,若当前网络环境良好,加速提升信任度. 因此,无人机信任度$f^{(k)}$更新如式(6)所示:

$$f^{(k)}=\begin{cases}\alpha f^{(k-1)}-(1-\alpha)L_1\varphi^{d_1}, & \dfrac{X'}{X}\leqslant\delta\\ \alpha f^{(k-1)}+(1-\alpha)L_2\log\left(1+d_2\varphi\right), & \text{o.w.}\end{cases} \tag{6}$$

特别地,在$\delta\in[0.6,0.9]$,$L_1\in[0.1,0.9]$,$L_2\in[0.1,0.9]$的区间进行初步实验调优,以分析参数变化对算法收敛速度与路由性能的影响. 此外,构建策略风险函数,分别将数据包到达率$\rho$和端到端时延$\tau$量化为$C_1$和$C_2$个级别的风险值,其对应可容忍的最小数据包到达率$\hat{\rho}_l$和最大端到端时延$\hat{\tau}_l$的惩罚因子分别为$c_{l,1}$和$c_{l,2}$,评估导致路由性能下降的风险程度,以满足海域无人机业务的服务质量需求[32],即

$$r^{(k)}=\sum_{l}^{C_1}c_{l,1}\frac{1}{1+\mathrm{e}^{\hat{\tau}_l-\tau}}+\sum_{l}^{C_2}c_{l,2}\frac{1}{1+\mathrm{e}^{\rho-\hat{\rho}_l}} \tag{7}$$

无人机接收到船载目的节点反馈的性能,构建经验$\left\{\boldsymbol{s}^{(k)},\boldsymbol{a}^{(k)},u^{(k)},r^{(k)},\boldsymbol{s}^{(k+1)},\boldsymbol{f}^{(k)}\right\}$,并存入完整经验池$\mathcal{D}$. 基于路由经验回放的反馈恢复机制利用不完整与完整的经验池,恢复由于海域信道恶劣导致的反馈丢失. 具体而言,对于不完整经验,若在未来最多$K$个时隙成功接收到反馈,则利用其效益值$u^{(k)}$和风险值$r^{(k)}$替换相应的缺失信息,并将该经验移动至完整经验池$\mathcal{D}$. 无人机每时隙从经验池$\mathcal{D}$中随机采样$J$条路由经验样本,通过最小化估计路由和目标路由之间的损失函数更新策略网络$\mathcal{Q}$的权重$\boldsymbol{\theta}^{\mathrm{Q}}$,即

$$\begin{aligned}\boldsymbol{\theta}^{\mathrm{Q}}=\arg\min_{\boldsymbol{\varphi}}\frac{1}{J}\sum_{l=1}^{J}\Big(&u^{(l)}-Q\left(\boldsymbol{s}^{(l)},\boldsymbol{a}^{(l)};\boldsymbol{\varphi}\right)\\&+\gamma Q\left(\boldsymbol{s}^{(l+1)},\arg\max_{\boldsymbol{a}'\in\mathbf{A}}Q\left(\boldsymbol{s}^{(l)},\boldsymbol{a}';\boldsymbol{\theta}^{\mathrm{Q}}\right);\boldsymbol{\theta}^{\mathrm{Q}}\right)\Big)\end{aligned} \tag{8}$$

其中,折扣率$\gamma$用于评估当前效益和未来效益的重要性. 此外,信任网络$\mathcal{T}$的权重$\boldsymbol{\theta}^{\mathrm{T}}$依据相邻无人机的共享信任度及其对应的策略信任值估计结果进行更新,以检测灰洞攻击,即

$$\boldsymbol{\theta}^{\mathrm{T}}=\arg\min_{\boldsymbol{\varphi}}\frac{1}{J}\sum_{l=1}^{J}\left(\frac{\sum_{j=1}^{N}f_j}{N+1}-T(\boldsymbol{s}^{(l)},\boldsymbol{a}^{(l)};\boldsymbol{\varphi})\right) \tag{9}$$

风险网络 $\mathcal{R}$ 输出所选路由策略的风险值,表示在海域业务中未能满足最小数据包到达率和最大时延要求的概率. 通过最小化估计风险值和目标风险值之间的损失函数更新权重 $\boldsymbol{\theta}^{\mathrm{R}}$,即

$$\begin{aligned}\boldsymbol{\theta}^{\mathrm{R}}=\arg\min_{\boldsymbol{\varphi}}\frac{1}{J}\sum_{l=1}^{J}\Big(&r^{(l)}-R\left(\boldsymbol{s}^{(l)},\boldsymbol{a}^{(l)};\ \boldsymbol{\varphi}\right)\\&+\gamma R\left(\boldsymbol{s}^{(l+1)},\arg\min_{\boldsymbol{a}'\in\mathbf{A}}R\left(\boldsymbol{s}^{(l)},\boldsymbol{a}';\ \boldsymbol{\theta}^{\mathrm{R}}\right);\ \boldsymbol{\theta}^{\mathrm{R}}\right)\Big)\end{aligned}\tag{10}$$

所提基于强化学习的可信无人机路由算法 RLTUR 的计算复杂度 $\Gamma$ 主要由前向传播和反向传播两部分构成,前者用于完成下一跳选择与发射功率的决策,后者用于更新神经网络的权重参数. 策略网络、信任网络和风险网络采用相同的网络结构,输入大小取决于状态维度 $5N+6$,两个隐藏层的神经元节点数为 $g_1$ 和 $g_2$,输出大小取决于动作维度 $NL$,其中 $N$ 为相邻无人机的最大数量,$L$ 为量化功率水平. 策略网络执行前向传播,选择下一跳无人机和发射功率,其运算涉及 $o_1$ 次乘法运算,即

$$o_1=(5N+6)Jg_1+J(g_1+1)g_2+J(g_2+1)NL\tag{11}$$

在反向传播过程中更新权重时需要进行 $o_2$ 次乘法运算,即

$$o_2=2(5N+6)Jg_1+2J(g_1+1)g_2+3J(g_2+1)NL\tag{12}$$

同样地,与策略网络结构相同的信任网络和风险网络在前向传播和反向传播分别进行 $o_1$ 次和 $o_2$ 次乘法运算,用于评估所选路由策略的安全性与可靠性. 根据文献[33],隐藏层的神经元节点数取决于输出大小 $NL$ 和学习样本数量 $K$,第一隐藏层的神经元节点数的计算公式如下:

$$g_1=\sqrt{K(NL+2)}+2\sqrt{\frac{K}{NL+2}}\tag{13}$$

第二隐藏层的神经元节点数为

$$g_2=NL\sqrt{\frac{K}{NL+2}}\tag{14}$$

因此,计算复杂度 $\Gamma$ 为

$$\Gamma=O\left(3o_1+3o_2\right)\tag{15a}$$

$$=O\left(J(5N+6)g_1+J\left(g_1+1\right)g_2+J\left(g_2+1\right)NL\right)\tag{15b}$$

$$=O\left(J(5N+6)\sqrt{KNL}+JKNL+J\sqrt{KNL}+JNL\sqrt{KNL}+JNL\right)\tag{15c}$$

$$=O(KJNL)\tag{15d}$$

其中,式(15b)由式(11)和式(12)所得,式(15c)由式(13)和式(14)所得,式(15d)由 $K\gg NL$ 所得. 因此,所提路由算法 RLTUR 的计算复杂度为 $O(KJNL)$,其随着相邻无人机数量 $N$、量化功率水平 $L$、学习样本数量 $K$ 和采样的路由经验样本大小 $J$ 的增加而增加.

## 5　系统部署

无人机搭载树莓派 5,遵循 IEEE 802.11ax 通信标准,以 5 阶量化最高 100 mW 的发射功率,将拍摄到的目标感知区域图像和相应的推断业务提示语发送到船载目的节点,执行场景理解和事件推断等无人机业务. 其中,船载目的节点配备两块 24 GB 显存的 RTX 4090 GPU,部署参数量为 70 亿且量化精度为 FP16 的 LLaVA-1.5-7B 大语言模型,模型结构由 32 层 Transformer 组成. 通过 JPEG 等格式处理 224 × 224 像素的图像数据,并对最大词元向量长度为 1 500 的业务提示语进行 UTF-8 编码.

如图 2 所示,船载目的节点将接收到图片和文本数据分别采用视觉编码器和分词器转化为词元向量,推断环境指示. 具体来说,针对图像数据,采用视觉编码器提取视觉特征,通过线性投影映射为初始词元向量,进一步将初始词元向量输入 Transformer 架构编码生成图像的嵌入表示,再通过线性投影层生成词元向量 $\boldsymbol{\psi}_1$. 针对相邻无人机位置和速度等信息,以及预设的提示词等文本数据,采用分词器根据字节对编码技术将单词拆分为子词单元,根据字符序列匹配技术将该文本转换词元向量 $\boldsymbol{\psi}_2$. 最后,通过向量拼接构建多模态数据的词元向量 $[\boldsymbol{\psi}_1,\boldsymbol{\psi}_2]$,输入预训练的大语言模型,输出环境指示 $\varphi$. 此外,提示词的设计通过明确描述无人机拍摄的周围环境图像及其相邻无人机信息,引导模型进行环境特征推断. 同时,通过预设诸如良好和恶劣等环境指示等级,使模型能够基于多模态数据与上下文信息生成可量化的环境指示.

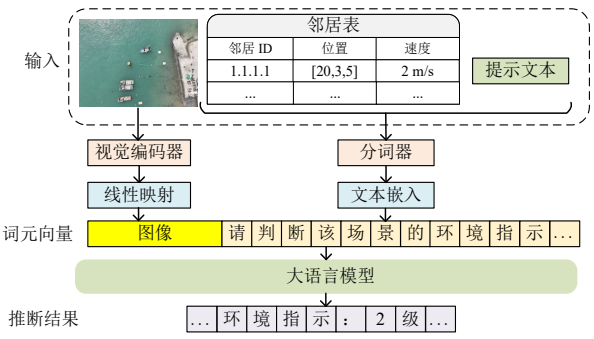



图 2　大语言模型推断示意图

无人机搭载的树莓派 5 配备主频 2.4 GHz 的 Arm Cortex-A76 处理器和 8 GB 内存,运行 Debian 12 操作系统,并连接两块网卡和 BME280 湿度传感器等多种传感器. 如图 3 所示,内置网卡通过用户数据报协议套接字,将经 Base64 编码的图像传输至船载目的节点. 数据包头部采用 JSON 编码,包含下一跳无人机 ID、源 ID、目的 ID、时间戳、电池电量、路由跳数及遍历路径等路由信息. 外接网卡通过传输控制协议套接字接收来自

船载目的节点的反馈信息，包括大语言模型推断的环境指示，以及统计得到的端到端时延和数据包到达率等性能指标．特别地，预先为大语言模型提供环境指示，并划分为两个等级：1级表示恶劣网络环境，2级表示良好网络环境．此外，无人机与船载目的节点采用时钟同步功能，以准确测量时延．


图3　系统部署方案示意图

在无人机上部署基于强化学习的可信路由优化算法，采用ad-hoc模式进行自组网，绑定无人机ID和媒体访问控制地址以选择下一跳 $a_1$，并通过执行“iwconfig txpower [value]”命令调整发射功率 $a_2$．此外，执行“iwconfig”命令读取内置网卡中的“Signal level”中的数值，估计信道增益．无人机部署两层全连接层的神经网络，包括输入输出层以及两个隐藏层，每个隐藏层有128个神经元．其中，神经网络权重更新过程中的折扣率 $\gamma$ 为0.5，经验池 $\mathcal{D}$ 的容量大小为512，随机采样 $J$=64条路由经验．基于假设检验的相邻无人机信任度更新阈值 $\delta$ 为0.7，信任度更新参数 $L_1$= $L_2$=0.5，能够容忍的最小数据包到达率和最大端到端时延的分别为80%和250 ms，成功接收到反馈的最大容忍时隙 $K$ 为10．

## 6　结果分析

如图4所示，基于厦门欧厝海域实测信道数据和大语言模型LLaVA-1.5-7B的推断结果构建仿真场景，包括30架无人机和一个船载目的节点．其中，实测的海域信道数据受到风速和湿度等因素的影响，海域传播环境总体表现为更高的路径损耗指数，信号衰落严重且具有强烈的时变性．根据海域实测数据，无人机到船载节点的信道参数 $\beta_1=0.496$，$\beta_2=0.802$，无人机之间的路径损耗指数 $\varsigma=2.832$．

此外，30架无人机的初始拓扑如图5所示，无人机间距为200 m，无人机的高度为16 m或8 m，与最近的相邻无人机保持至少10 m的安全距离．无人机以最高5 m/s的速度围绕预设点位，跟随逻辑中心执行确定性循环，并进行独立随机运动，以模拟无人机完成搜索救援等任务．无人机以发射功率 $a_2\in\{20,40,60,80,100\}$ mW向下一跳无人机 $a_1$ 传输由60个2 KB数据包组成的120 KB图像，直至船载目的节点，用于海域大语言模型推断．灰洞攻击者以 $\gamma$=0.9概率选择性地丢弃其截获的数据包．


图4　海域无人机信道数据测量

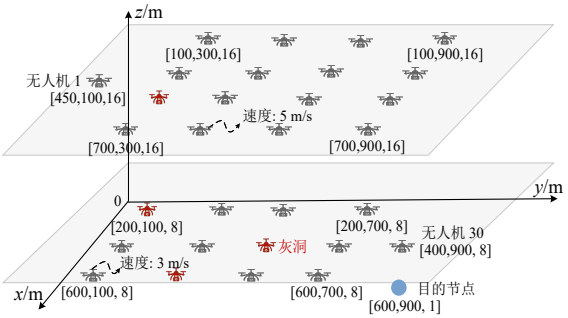
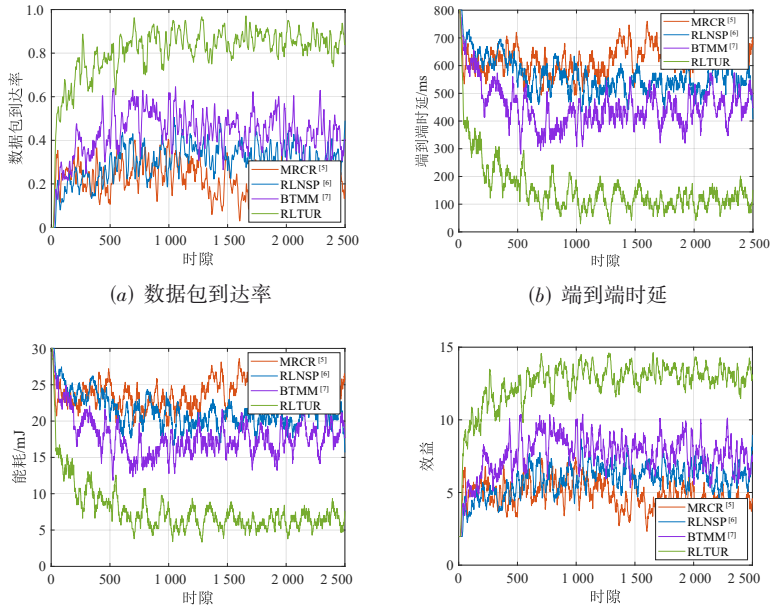



图5　仿真拓扑设置

如图6所示，基于30轮重复仿真给出抗灰洞攻击海域无人机路由算法的数据包到达率、端到端时延和路由能耗等性能表现．例如，所提路由算法RLTUR与基准算法MRCR[5]相比，在1 000时隙之后，将数据包到达率从25.3%提升至86.6%，同时将端到端时延降低了83.3%，路由能耗降低了72.4%．原因在于所提算法快速调整发射功率，适配海域恶劣快变信道．相比基准算法RLNSP[6]，所提路由算法将数据包到达率从36.5%提升至86.6%，降低了79.9%的端到端时延和69.5%的路由能耗．原因在于所提算法在路由策略分布中设计信任值评估路径安全性以对抗灰洞攻击，可以有效规避选择具有高丢包概率的路由策略．此外，相比安全路由

机制 BTMM[7],所提路由算法提升了 72.8% 的数据包到达率,降低了 75.1% 的端到端时延和 64.7% 的路由能耗. 这是由于大语言模型在推断任务中生成的环境指示能够有效区分数据包丢失是由灰洞攻击还是由恶劣信道条件引起,从而避免将非恶意节点误判为攻击节点,并减少不必要的路由能耗.




(a) 数据包到达率　(b) 端到端时延

(c) 路由能耗　(d) 效益

图 6　路由性能

图 7 开展消融分析,讨论所提路由算法中环境指示、信任评估和风险评估所带来的增益. 其中,与基于强化学习的无人机基础路由 RLUR 相比,在 1 000 时隙之后,环境指示与信任评估的结合分别提高了 84.2% 和 67.1% 的效益. 原因在于,大语言模型推断的环境指示结果可映射当前无人机所处网络环境的恶劣程度,辅助预测信道增益,而在路由策略分布中引入信任评估,使无人机倾向于选择具有高信任度的下一跳,降低了选择具有较高丢包率的下一跳无人机的概率. 此外,在路由策略分布中引入风险评估机制,有效规避选择易引发不满足服务质量需求的路由策略,从而加快路由优化速度,与无人机基础路由 RLUR 相比可提升 46.3% 的效益.

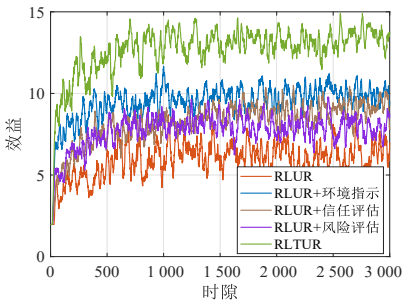
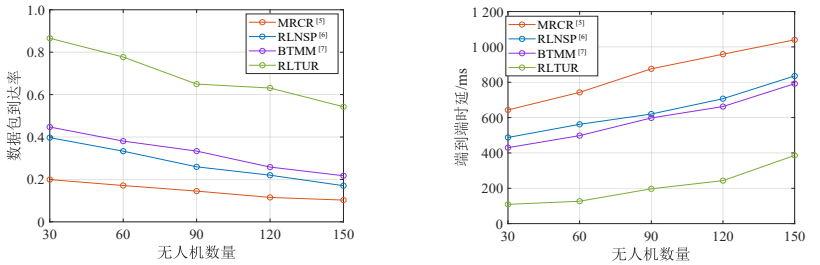



图 7　消融分析

如图 8 所示,所提海域无人机路由算法在不同无人机数量下均优于基准算法. 例如,当无人机数量为 90 时,与 RLNSP[6] 相比,所提算法将数据包达到率从 27.5% 提升到 65.1%,降低了 67.2% 的端到端时延,节省了 65.1% 的路由能耗. 这是因为基于策略网络、信任网络和风险网络的架构加速了大规模无人机群下的路由策略选择,且路由经验中的反馈恢复机制,降低路由策略决策的误差. 相比安全路由机制 BTMM[7],当无人机数量为 90 时,所提路由算法将数据包到达率从 32.5% 提升到 65.1%,降低了 66.6% 的端到端时延和 60.9% 的路由能耗.

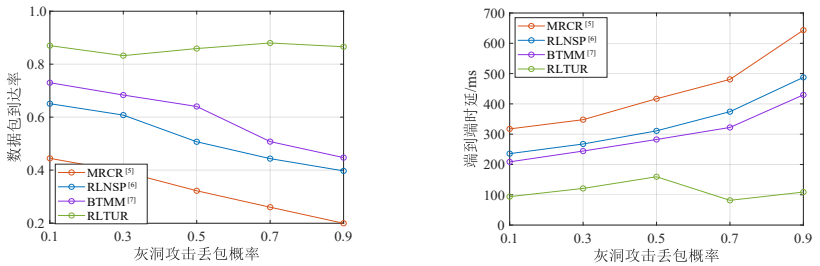
如图 9 所示,所提海域无人机路由算法在不同灰洞攻击丢包概率下均优于基准算法. 例如,当攻击丢包概率为 0.5 时,与 RLNSP[6] 相比,所提算法平均提升了 70.1% 的数据包达到率,降低了 44.2% 的端到端时延,节省了 48.8% 的路由能耗. 这是因为引入的信任网络可以有效评估相邻无人机信任度,防御不同丢包概率的灰洞攻击,快速恢复中断路由. 此外,与 BTMM[7] 相比,所提算法平均提升了 34.3% 的数据包达到率,降低了 41.4% 的端到端时延,节省了 45.5% 的路由能耗. 这是因为在信任评估机制中结合了大模型反馈的环境特征和相邻无人机成功转发的数据包数,实现对灰洞攻击的准确检测.




(a) 数据包到达率　(b) 端到端时延

(c) 路由能耗　(d) 效益

图8　不同无人机网络规模的路由性能




(a) 数据包到达率　(b) 端到端时延

(c) 路由能耗　(d) 效益

图9　不同灰洞攻击丢包概率的路由性能

## 7　结论

本文提出抗灰洞攻击海域无人机路由算法，基于大语言模型推断的环境指示以及测量的湿度风速等海域环境特征，采用强化学习持续优化路由选择和发射功率，抵御灰洞攻击，适配海域恶劣信道变化．结合策略风险评估和无人机路由信任体系，在满足多种海域业务服务质量要求的同时，规避因丢弃数据包而导致路由失败的灰洞节点，实现对中断路由的快速恢复．基于厦门欧厝海域实测信道数据和LLaVA-1.5-7B大语言模型的仿真结果表明，所提算法相比于基准安全路由算法，可提升72.8%的数据包达到率，降低75.1%的端到端时延和64.7%路由能耗，可有效支撑海域大语言模型任务．

### 参考文献

[1] LIU B C, ZHANG W K, CHEN W H, et al. Online computation offloading and traffic routing for UAV swarms in edge-cloud computing[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8777-8791.

[2] YANG T T, JIANG Z, SUN R J, et al. Maritime search

and rescue based on group mobile computing for unmanned aerial vehicles and unmanned surface vehicles[J]. IEEE Transactions on Industrial Informatics, 2020, 16(12): 7700-7708.

[3] 文鹏, 叶苗, 王勇, 等. SDWN中基于多智能体图强化学习的多对多通信路由方法[J]. 电子学报, 2025, 53(6): 1885-1905.
WEN P, YE M, WANG Y, et al. A multi-agent graph reinforcement learning method for many-to-many communication routing in SDWN[J]. Acta Electronica Sinica, 2025, 53(6): 1885-1905. (in Chinese)

[4] 孙鹏浩, 兰巨龙, 申涓, 等. 一种基于深度增强学习的智能路由技术[J]. 电子学报, 2020, 48(11): 2170-2177.
SUN P H, LAN J L, SHEN J, et al. An intelligent routing technology based on deep reinforcement learning[J]. Acta Electronica Sinica, 2020, 48(11): 2170-2177. (in Chinese)

[5] WANG Z L, YAO H P, MAI T L, et al. Learning to routing in UAV swarm network: A multi-agent reinforcement learning approach[J]. IEEE Transactions on Vehicular Technology, 2023, 72(5): 6611-6624.

[6] ZHANG X C, ZHAO H T, XIONG J, et al. Decentralized routing and radio resource allocation in wireless ad hoc networks via graph reinforcement learning[J]. IEEE Transactions on Cognitive Communications and Networking, 2024, 10(3): 1146-1159.

[7] JIA Z Y, HE S J, ZHU Q M, et al. Trusted routing for blockchain-empowered UAV networks via multi-agent deep reinforcement learning[J]. IEEE Transactions on Communications, 2025, 73(12): 14227-14242.

[8] 张雅楠, 仇洪冰. 基于深度强化学习的无人机可信地理位置路由协议[J]. 电子与信息学报, 2022, 44(12): 4211-4217.
ZHANG Y N, QIU H B. Trusted geographic routing protocol based on deep reinforcement learning for unmanned aerial vehicle network[J]. Journal of Electronics & Information Technology, 2022, 44(12): 4211-4217. (in Chinese)

[9] 孟超, 周倩, 郭林, 等. 基于相关性传输模型的无线链路质量估计方法及路由优化算法[J]. 电子学报, 2022, 50(10): 2409-2424.
MENG C, ZHOU Q, GUO L, et al. Estimation method of wireless link quality and routing optimization algorithm based on correlation transmission model[J]. Acta Electronica Sinica, 2022, 50(10): 2409-2424. (in Chinese)

[10] GANGOPADHYAY S, JAIN V K. A position-based modified OLSR routing protocol for flying ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2023, 72(9): 12087-12098.

[11] SONG H, LIU L J, SHANG B D, et al. Enhanced flooding-based routing protocol for swarm UAV networks: Random network coding meets clustering[C]//IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2021: 1-10.

[12] QIU X H, ZHANG S, WANG Z Y, et al. Integrated host- and content-centric routing for efficient and scalable networking of UAV swarm[J]. IEEE Transactions on Mobile Computing, 2024, 23(4): 2927-2942.

[13] ZHANG L, MA X Z, ZHUANG Z R, et al. Q-learning aided intelligent routing with maximum utility in cognitive UAV swarm for emergency communications[J]. IEEE Transactions on Vehicular Technology, 2023, 72(3): 3707-3723.

[14] LI J L, XIAO L, QI X C, et al. Reinforcement learning based energy-efficient fast routing for FANETs[J]. IEEE Transactions on Communications, 2024, 72(11): 7063-7076.

[15] 颜志, 易正伦, 欧阳博, 等. 无人机集群联合拓扑控制的智能路由规划方法[J]. 通信学报, 2024, 45(2): 137-149.
YAN Z, YI Z L, OUYANG B, et al. Intelligent route planning method with jointing topology control of UAV swarm[J]. Journal on Communications, 2024, 45(2): 137-149. (in Chinese)

[16] 惠鏸, 张晓静. 无线自组织网络的联合安全路由选择和功率优化算法[J]. 电子与信息学报, 2020, 42(12): 2923-2930.
HUI H, ZHANG X J. Joint secure routing and power optimization algorithm for wireless ad hoc networks[J]. Journal of Electronics & Information Technology, 2020, 42(12): 2923-2930. (in Chinese)

[17] CAI R J, LI X J, CHONG P H J. An evolutionary self-cooperative trust scheme against routing disruptions in MANETs[J]. IEEE Transactions on Mobile Computing, 2019, 18(1): 42-55.

[18] LI J L, XIAO L, WANG C X, et al. Learning-based energy-efficient anti-jamming FANET routing with QoS guarantee[J]. IEEE Transactions on Communications, 2025, 73(11): 11418-11431.

[19] ALTAWEEL A, STOLERU R, GU G F, et al. On detecting route hijacking attack in opportunistic mobile networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(3): 2516-2532.

[20] SAKAI K, SUN M T, KU W S, et al. Secure data communications in wireless networks using multi-path avoidance routing[J]. IEEE Transactions on Wireless Communications, 2019, 18(10): 4753-4767.

[21] 杨宏宇, 韩越. 基于动态信誉的无线Mesh网络安全路由机制[J]. 通信学报, 2019, 40(4): 195-201.
YANG H Y, HAN Y. Wireless Mesh network secure routing mechanism based on dynamic reputation[J]. Journal on Communications, 2019, 40(4): 195-201. (in Chinese)

[22] 李峰, 司亚利, 陈真, 等. 基于信任机制的机会网络安全路由决策方法[J]. 软件学报, 2018, 29(9): 2829-2843.

LI F, SI Y L, CHEN Z, et al. Trust-based security routing decision method for opportunistic networks[J]. Journal of Software, 2018, 29(9): 2829-2843. (in Chinese)

[23] VELUSAMY D, PUGALENDHI G, RAMASAMY K. A cross-layer trust evaluation protocol for secured routing in communication network of smart grid[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(1): 193-204.

[24] MIRZADEH I, SAYAD HAGHIGHI M, JOLFAEI A. Filtering malicious messages by trust-aware cognitive routing in vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(1): 1134-1143.

[25] HE Y, HAN G J, HOU Y, et al. Environment-tolerant trust opportunity routing based on reinforcement learning for Internet of underwater things[J]. IEEE Transactions on Mobile Computing, 2025, 24(7): 6348-6360.

[26] HE Y, HAN G J, JIANG J F, et al. CADTR: Context-aware trust routing algorithm based on priority sampling DDPG for UASNs[J]. IEEE Transactions on Mobile Computing, 2025, 24(11): 11688-11702.

[27] HE Y, FANG J C, YU F R, et al. Large language models (LLMs) inference offloading and resource allocation in cloud-edge computing: An active inference approach[J]. IEEE Transactions on Mobile Computing, 2024, 23(12): 11253-11264.

[28] CHEN Y F, ZHAO N, DING Z G, et al. Multiple UAVs as relays: Multi-hop single link versus multiple dual-hop links[J]. IEEE Transactions on Wireless Communications, 2018, 17(9): 6348-6359.

[29] TIMMINS I J, O´ YOUNG S. Marine communications channel modeling using the finite-difference time domain method[J]. IEEE Transactions on Vehicular Technology, 2009, 58(6): 2626-2637.

[30] WANG Z Y, DU J, JIANG C X, et al. UAV-assisted target tracking and computation offloading in USV-based MEC networks[J]. IEEE Transactions on Mobile Computing, 2024, 23(12): 11389-11405.

[31] SCHWEITZER N, STULMAN A, MARGALIT R D, et al. Contradiction based gray-hole attack minimization for ad-hoc networks[J]. IEEE Transactions on Mobile Computing, 2017, 16(8): 2174-2183.

[32] 段洁, 闫子豪, 刘亮, 等. 基于多元时变图的天地一体化网络组播路由算法[J]. 电子学报, 2025, 53(5): 1469-1481.
DUAN J, YAN Z H, LIU L, et al. Multicast routing algorithm for space-air-ground integrated networks based on multi-dimensional time-varying graphs[J]. Acta Electronica Sinica, 2025, 53(5): 1469-1481. (in Chinese)

[33] HUANG G B. Learning capability and storage capacity of two-hidden-layer feedforward networks[J]. IEEE Transactions on Neural Networks, 2003, 14(2): 274-281.

## 作者简介

**李杰铃** 男,1995年1月出生于福建省泉州市. 现为厦门大学信息学院博士研究生. 主要研究方向为网络安全、无人机组网等.
E-mail: 18759923858@163.com

**雷 妍** 女,2001年5月出生于广东省深圳市. 现为厦门大学信息学院博士研究生. 主要研究方向为无人机组网、网络安全等.
E-mail: 23320250157879@stu.xmu.edu.cn

**肖 亮** 女,1980年3月出生于河北省石家庄市. 现为厦门大学信息学院教授、博士研究生导师. 主要研究方向为无线通信、网络安全等.
E-mail: lxiao@xmu.edu.cn

**陈乔鑫** 男,1998年7月出生于福建省泉州市. 现为厦门大学信息学院博士研究生. 主要研究方向为无线安全、智能安全检测等.
E-mail: fjqiaoxin_chen@163.com

**王鹏程** 男,2002年8月出生于江苏省苏州市. 现为厦门大学信息学院硕士研究生. 主要研究方向为无人机组网、无线安全认证.
E-mail: amat_wpc@163.com

**王成耀** 男,2002年7月出生于广东省揭阳市. 现为厦门大学信息学院硕士研究生. 主要研究方向为无人机组网、无线抗干扰等.
E-mail: 19876818080@163.com