自动化学报
ACTA AUTOMATICA SINICA

面向复杂无人机群的TPT-Former关键节点脆弱性与攻击策略研究

董萍 田恩刚

TPT-Former-based Study of Critical Node Vulnerability and Attack Strategies in Complex UAV Swarms

DONG Ping, TIAN En-Gang

在线阅读 View online: https://doi.org/10.16383/j.aas.c260061

您可能感兴趣的其他文章

基于异构图神经网络的可解释兵棋态势预测方法

An Interpretable Wargame Situation Prediction Method Based on Heterogeneous Graph Neural Networks

自动化学报. 2025, 51(6): 1248−1260 https://doi.org/10.16383/j.aas.c240468

融合知识的多视图属性网络异常检测模型

Multi-view Outlier Detection for Attributed Network Based on Knowledge Fusion

自动化学报. 2023, 49(8): 1732−1744 https://doi.org/10.16383/j.aas.c220629

基于时序图推理的设备剩余使用寿命预测

Remaining Useful Life Estimation of Facilities Based on Reasoning Over Temporal Graphs

自动化学报. 2024, 50(1): 76−88 https://doi.org/10.16383/j.aas.c230014

基于小样本学习的图像分类技术综述

Survey on Image Classification Technology Based on Small Sample Learning

自动化学报. 2021, 47(2): 297−315 https://doi.org/10.16383/j.aas.c190720

基于不同故障传播路径差异化的故障诊断方法

Fault Propagation Path-aware Network: A Fault Diagnosis Method

自动化学报. 2025, 51(1): 161−173 https://doi.org/10.16383/j.aas.c240151

基于模体增强对比学习的图神经网络后门防御方法

Motif-augmented Contrastive Learning-based Defense Against Backdoor Attack on Graph Neural Networks

自动化学报. 2026, 52(4): 765−779 https://doi.org/10.16383/j.aas.c240767

面向复杂无人机群的 TPT-Former 关键节点脆弱性与攻击策略研究

董 萍 [1] 田恩刚 [1]

摘 要 针对复杂无人机群易受通信干扰与节点摧毁影响的问题, 研究资源受限条件下的关键节点识别与攻击策略. 首先构建无人机群图模型, 模拟覆盖多种拓扑与运行状态的数据集, 并基于连通性与任务性能变化形成任务退化导向标注; 其次在拓扑先验与任务状态增强 Transformer 框架下融合拓扑先验与任务状态信息, 提出关键节点评估模型, 并采用加权回归损失提升预测精度; 最后在攻击节点数量与总攻击成本双约束下, 设计基于学习型关键性评分的贪心攻击策略, 并与度中心性、介数中心性及传统图注意力网络策略进行对比. 结果表明, 所提方法在关键性预测与单位资源破坏效能方面优于对比方法, 可为无人机群抗毁性评估与拓扑加固提供参考.

关键词 复杂无人机群; 关键节点; 图神经网络; TPT-Former; 资源受限攻击

引用格式 董萍, 田恩刚. 面向复杂无人机群的 TPT-Former 关键节点脆弱性与攻击策略研究. 自动化学报, 2026, **52**(10): 2341−2352

DOI 10.16383/j.aas.c260061 **CSTR** 32138.14.j.aas.c260061

TPT-Former-based Study of Critical Node Vulnerability and Attack Strategies in Complex UAV Swarms

DONG Ping[1] TIAN En-Gang[1]

Abstract To address the susceptibility of complex unmanned aerial vehicle (UAV) swarms to communication interference and node destruction, this study investigates critical node identification and attack strategies under resource constraints. First, we develop a graph model of UAV swarms and generate a dataset via simulation spanning diverse topologies and operational states where task-degradation-oriented labels are assigned according to changes in network connectivity and mission performance. Second, within the proposed topology-prior and task-state enhanced Transformer (TPT-Former) framework, we fuse topological priors with task-state information to build a critical node evaluation model, and employ a weighted regression loss to improve the accuracy of criticality prediction. Finally, under joint constraints on the number of attacked nodes and the total attack cost, we design a greedy attack strategy guided by learned criticality scores and compare it with degree centrality, betweenness centrality, and conventional graph attention network strategies. The results show that the proposed approach outperforms the baselines in both criticality prediction and damage efficiency per unit resource, providing a reference for UAV swarm survivability assessment and topology reinforcement.

Keywords complex UAV swarms; critical node; graph neural network; TPT-Former; resource-constrained attack

Citation Dong Ping, Tian En-Gang. TPT-Former-based study of critical node vulnerability and attack strategies in complex UAV swarms. *Acta Automatica Sinica*, 2026, **52**(10): 2341−2352

随着人工智能与机器人技术的快速发展, 多无人机系统在灾害搜救、区域巡检与编队巡航等任务中展现出显著优势. 相关研究已围绕无人机群的深度强化学习控制、安全编队、任务分配与协同吊挂控制等问题展开[1−4]. 在安全约束控制、人工势场导航、分布式编队机动和神经网络模型预测控制方面的研究, 为复杂无人机群的安全协同提供了方法基础[5−8].

多无人机系统的协同能力依赖通信网络实现状态共享与分布式决策, 因而可抽象为网络化多智能体系统 (networked multi-agent system, NMAS). 在对抗环境下, 节点入侵、物理摧毁与通信干扰等攻击会破坏信息交互结构, 并通过闭环协同过程放大到编队误差、收敛速度与任务完成率等系统层面

收稿日期 2026-01-27 录用日期 2026-05-07
Manuscript received January 27, 2026; accepted May 7, 2026
国家自然科学基金 (62173231, 62503331) 资助
Supported by National Natural Science Foundation of China (62173231, 62503331)
本文责任编委 温广辉
Recommended by Associate Editor WEN Guang-Hui
1. 上海理工大学光电信息与计算机工程学院 上海 200093
1. School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093

指标, 进而造成任务性能退化甚至任务失败. 面向资源受限对抗, 重要数据与关键指标驱动的攻击资源分配和韧性估计研究, 为“攻击选择–性能退化”关系提供更具针对性的刻画工具[9−10]. 网络化控制系统中的攻击检测、安全估计与安全控制研究进一步揭示了攻击对闭环性能的破坏机理及风险边界[11−12]. 此外, 动态事件触发滤波、有限时间故障检测和隐私一致性控制等工作表明, 在开放网络中同时考虑故障、隐私与韧性具有重要意义[13−15].

现有关键节点分析方法多基于度中心性、介数中心性等静态图论指标, 侧重刻画结构重要性, 但难以覆盖协同任务中的“结构–状态–性能”耦合关系. 从控制与系统视角看, 节点关键性不应仅由拓扑位置决定, 还与任务过程中的状态分布及闭环演化密切相关. 例如, 连通性下降往往会降低一致性或编队误差的收敛速度并扩大扰动影响, 使攻击效应呈现显著的动态与场景依赖性. 因而, 若仅用静态中心性替代“攻击导致的闭环性能退化敏感度”, 容易出现结构指标与任务退化的不一致, 限制抗毁性评估与攻击/防御决策的针对性.

近年来, 图神经网络 (graph neural network, GNN) 为从数据中学习复杂网络的高阶依赖关系提供了有效工具, 典型模型包括图卷积网络 (graph convolutional network, GCN) 与图注意力网络 (graph attention network, GAT). 相关研究系统总结了 GNN 的模型谱系, 并通过注意力与解耦建模提升图节点表示能力[16−17]. 神经网络自适应一致性、固定时间一致性跟踪与策略梯度最优一致性控制等研究, 也为学习方法与多智能体闭环性能的结合提供了基础[18−20]. 然而, 面向无人机群协同任务的关键节点研究仍存在不足: 1) 缺少以闭环任务性能退化为依据的标注体系与可复现数据支撑, 导致“关键性”难以与系统指标严格对齐; 2) 现有模型往往侧重局部聚合, 对全局拓扑模式与任务状态差异的融合不足, 难以刻画任务退化机理; 3) 攻击决策层面常忽略攻击次数与成本等资源约束, 缺少在预算限制下对攻击集合选择与破坏效能的系统化评估.

针对上述问题, 本文面向敌对环境下无人机群抗毁性评估与资源受限攻击决策, 提出“任务退化导向关键性评估–成本约束攻击选点”的统一框架. 本文的主要贡献如下:

1) 模拟合成面向协同任务过程的无人机群时变图数据集, 并以攻击导致的闭环任务性能退化为依据, 建立关键性标注体系, 使节点关键性与系统指标严格对齐;

2) 提出拓扑先验与任务状态增强 Transformer (topology-prior and task-state enhanced Transformer, TPT-Former) 模型, 通过在注意力机制中显式注入结构位置信息与状态差异信息, 学习预测节点对任务退化的敏感度评分;

3) 在攻击次数与攻击成本双约束下, 基于关键性评分设计成本感知的贪心攻击策略, 并通过仿真对比验证其在单位资源破坏效能与任务退化效果上的优势.

本文结构安排如下: 第 1 节给出问题定义与资源受限攻击建模; 第 2 节介绍模拟数据集与任务退化导向标注体系; 第 3 节提出 TPT-Former 关键节点评估模型; 第 4 节给出资源受限攻击策略与仿真实验分析; 第 5 节总结全文并讨论后续工作.

1 问题定义

1.1 无人机群协同过程与图表示

考虑由 N 架无人机组成的 NMAS, 在离散时刻 k, 通信与状态可表示为时变图

$$G(k)=\big(V,\ E(k),\ \boldsymbol{X}(k)\big),\ V=\{1,\cdots,N\} \tag{1}$$

其中 $E(k)$ 为时刻 k 的链路集合, $\boldsymbol{X}(k)=[\boldsymbol{x}_1(k),\cdots,\boldsymbol{x}_N(k)]^{\mathrm{T}}$ 为节点特征矩阵. 记邻接矩阵为 $\boldsymbol{A}(k)=[a_{ij}(k)]$, $a_{ij}(k)\in\{0,1\}$ 表示时刻 k 是否存在边 (i,j). 本文将无人机群通信网络建模为无向时变图. 具体而言, 若在时刻 k, 节点 i 与节点 j 之间的链路可用, 则记无向边 $(i,j)\in E(k)$, 并令 $a_{ij}(k)=a_{ji}(k)\in\{0,1\}$, 因此邻接矩阵满足 $\boldsymbol{A}(k)=\boldsymbol{A}^{\mathrm{T}}(k)$. 相应地, 拉普拉斯矩阵 $\boldsymbol{L}(k)$ 为实对称矩阵, 其第二小特征值 $\lambda_2(\boldsymbol{L}(k))$ 按标准代数连通度定义, 用于刻画时刻 k 的网络连通性强弱. 令度矩阵 $\boldsymbol{D}(k)=\mathrm{diag}\{d_1(k),\cdots,d_N(k)\}$, 其中 $d_i(k)=\sum_{j=1}^{N}a_{ij}(k)$, 则拉普拉斯矩阵为

$$\boldsymbol{L}(k)=\boldsymbol{D}(k)-\boldsymbol{A}(k) \tag{2}$$

由于本文考虑时变拓扑, $\lambda_2(\boldsymbol{L}(k))$ 亦随时间变化, 因此后续实验中所绘制的 $\lambda_2(\boldsymbol{L}(k))$ 曲线均表示在每个离散时刻基于当前拓扑实时计算得到的代数连通度演化结果. 本文在第 4 节的时域演化实验中直接统计 $\lambda_2(\boldsymbol{L}(k))$ 随时间的变化, 并与编队误差演化共同用于解释攻击导致的闭环性能退化.

1.2 闭环任务过程与性能指标

本文关注抗毁性评估与攻击机理, 不以提出新控制器为目标. 因此, 假设无人机群在无攻击条件下采用既定分布式协同控制完成任务, 攻击通过使部分节点失效改变信息交互结构, 从而影响闭环演化. 以离散运动学为例, 记第 i 架无人机的位置为 $\boldsymbol{p}_i(k)\in\mathbf{R}^3$, 控制输入为 $\boldsymbol{u}_i(k)$, 采样周期为 Δt, 则

$$\boldsymbol{p}_i(k+1)=\boldsymbol{p}_i(k)+\Delta t\boldsymbol{u}_i(k) \tag{3}$$

为建立本文“拓扑变化 $\rightarrow$ 闭环性能退化”的分析主线, 给出一个与通信邻接关系直接耦合的典型编队. 需要强调的是, 本文不以控制律设计为目标, 而是将其作为生成任务性能指标与评估退化程度的仿真执行模型. 攻击通过改变邻接关系 $a_{ij}(k)$ 影响信息交互, 进而影响误差演化与任务结果:

$$\boldsymbol{u}_i(k)=-\sum_{j\in\mathcal{N}_i(k)}a_{ij}(k)\Big(\boldsymbol{p}_i(k)-\boldsymbol{p}_j(k)-(\boldsymbol{p}_i^{\mathrm{ref}}(k)-\boldsymbol{p}_j^{\mathrm{ref}}(k))\Big) \tag{4}$$

其中 $\mathcal{N}_i(k)=\{j\mid a_{ij}(k)=1\}$ 为邻居集合, $\boldsymbol{p}_i^{\mathrm{ref}}(k)\in\mathbf{R}^3$ 为期望编队轨迹.

定义 1 (编队误差). 给定期望编队轨迹 $\boldsymbol{p}_i^{\mathrm{ref}}(k)\in\mathbf{R}^3$, 定义时刻 k 的编队误差为

$$E_{\mathrm{form}}(k)=\frac{1}{N}\sum_{i=1}^{N}\big\|\boldsymbol{p}_i(k)-\boldsymbol{p}_i^{\mathrm{ref}}(k)\big\|_2^2 \tag{5}$$

其中 $\boldsymbol{p}_i(k)\in\mathbf{R}^3$ 为节点位置, N 为节点总数, $\|\cdot\|_2$ 表示欧氏二范数.

定义 2 (任务成功指示). 设任务终止时刻为 k_T, 给定任务完成判定阈值 $\varepsilon_{\mathrm{form}}>0$, 定义任务成功指标为

$$\eta_{\mathrm{task}}=I\big(E_{\mathrm{form}}(k_T)\le\varepsilon_{\mathrm{form}}\big) \tag{6}$$

其中 $I(\cdot)$ 为指示函数.

为实现可复现的“结构–状态–性能”联合评价, 本文采用“连通性 + 误差 + 任务失败惩罚”的综合性能代价描述闭环任务性能:

$$J(G,\,S)=w_1\overline{E}_{\mathrm{form}}+w_2\,\overline{\phi(\lambda_2(\boldsymbol{L}))}+w_3(1-\eta_{\mathrm{task}}) \tag{7}$$

其中 $S\subseteq V$ 为攻击 (失效) 节点集合 (下文简称为攻击集合); G 为对应的图样本; 连通性代价的时间平均为 $\overline{\phi(\lambda_2(\boldsymbol{L}))}=(1/T_w)\sum_{k=k_0}^{k_0+T_w-1}\phi\left(\lambda_2(\boldsymbol{L}(k))\right)$, k_0 为任务窗口的起始时刻. 设任务窗口长度为 T_w, 则时间平均编队误差定义为 $\overline{E}_{\mathrm{form}}^{\mathrm{raw}}=(1/T_w)\sum_{k=k_0}^{k_0+T_w-1}\times E_{\mathrm{form}}(k)$. 为消除量纲影响, 实现中采用无攻击基线窗口均值进行归一化: $\overline{E}_{\mathrm{form}}=\overline{E}_{\mathrm{form}}^{\mathrm{raw}}/(\overline{E}_{\mathrm{form}}^{(0)}+\epsilon_E)$, 其中 $\overline{E}_{\mathrm{form}}^{(0)}$ 为无攻击 ($S=\emptyset$) 时的窗口均值, $\epsilon_E>0$ 为避免分母为零的常数. $\phi(\cdot)$ 为连通性映射, 该映射单调递减, 使连通性越弱代价越大, 本文固定取 $\phi(\lambda_2)=1/(\lambda_2+\epsilon_\lambda)$, 其中 $\epsilon_\lambda>0$ 为避免分母为零的常数. w_1, w_2, $w_3>0$ 为权重系数, 在全部实验中固定取同一组数值 (见第 4 节实验设置), 并对所有对比方法保持一致.

定义攻击集合 S 导致的综合性能退化量为

$$\Delta J(G,\,S)=J(G,\,S)-J(G,\,\emptyset) \tag{8}$$

其中 $J(G,\,\emptyset)$ 为无攻击基线代价. 式 (7) ~ (8) 给出了本文贯穿数据标注 (第 2 节) 与攻击评估 (第 4 节) 的统一性能度量.

1.3　资源受限攻击问题

本文考虑节点失效型攻击: 攻击在预设时刻 k_a 生效后, 被攻击节点及其关联边从图中永久移除, 剩余节点构成的通信拓扑仍按原有时变规则继续演化; 本文所称“不进行控制律重构”, 仅指攻击后控制协议形式保持不变, 并不意味着拓扑冻结. 该设定用于刻画攻击发生后有限评估窗口内的保守退化情形, 可视为重构时延大于评估窗口的最坏情况近似. 在攻击次数与攻击成本双约束下, 资源受限最优攻击可表述为

$$\begin{aligned}&S^\star=\arg\max_{S\subseteq V}\ \Delta J(G,\,S)\\&\text{s.t. }|S|\le B,\ \sum_{i\in S}c_i\le C_{\max}\end{aligned} \tag{9}$$

其中 B 为最大攻击节点数; $C_{\max}$ 为总攻击预算; $c_i>0$ 为节点攻击成本 (例如骨干中继节点的成本更高), 用于刻画攻击者对不同类型节点实施破坏所需资源的差异. 本文将节点抽象为两类: 骨干中继节点和普通节点. 前者承担跨簇中继、多跳回传和数据汇聚等高负载通信功能, 在通信重要性、替代难度及防护强度上通常高于普通节点, 因此设置为较高成本 $c_i=2$; 后者主要承担常规感知与任务执行功能, 设置为 $c_i=1$. 该二值成本设定旨在以简洁形式刻画“高价值/高防护”与“常规/低防护”两类典型攻击对象. 实验中取 $B\in\{1,\,2,\,3,\,5\}$, $C_{\max}\in\{3,\,5,\,8\}$ 分别对应低、中、高三类典型资源水平: 低预算主要覆盖普通节点主导的攻击情形, 中等预算覆盖普通节点与骨干中继节点混合攻击情形, 较高预算可覆盖多个骨干中继节点或较大规模混合攻击情形. 因而, 该设置能够较好反映资源受限攻击中“节点数量受限”与“总体资源受限”并存的典型场景. 式 (9) 一般为组合优化问题. 为构造可计算策略, 先定义单点关键性标签

$$r_i=\Delta J\big(G,\,\{i\}\big) \tag{10}$$

并在第 2.3 节通过无攻击与单点失效仿真生成关键性标签, 归一化后作为监督信号. 单点标签用于近似刻画节点的边际退化贡献, 以显著降低组合标注的计算开销, 其在预算选点中的有效性将通过第 4 节的小规模最优对照实验进行验证. 第 3 节学习映射 $f_\Theta: G\mapsto\{s_i\}$ 以预测归一化单点关键性标签 $\hat{r}_i$,

第 4 节在预算约束下基于关键性评分 s_i 设计成本感知的贪心攻击策略.

2 无人机群图数据集与关键性标注体系

2.1 任务场景与时变拓扑生成

本文构建“城市灾后巡检与编队巡航”仿真场景数据集, 共生成 $M_{\mathrm{scn}}=120$ 个场景, 每个场景包含 $N\in[20,\ 40]$ 架无人机. 其中少量节点为骨干中继节点, 承担多跳回传与数据汇聚功能, 多数为普通节点. 场景示意如图 1 所示.

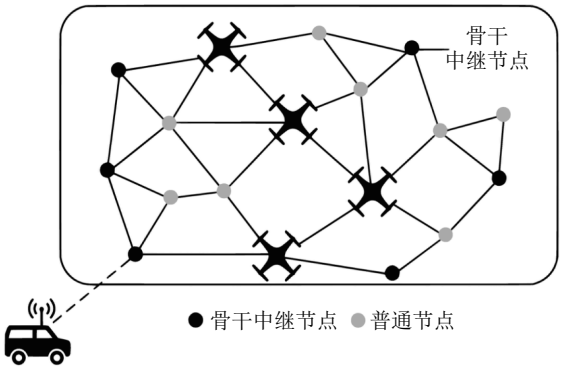


图 1 城市灾后巡检场景下复杂无人机群任务示意图

Fig. 1 Illustration of a complex UAV swarm mission in an urban post-disaster inspection scenario

考虑视距通信, 记第 i 架无人机在离散时刻 k 的位置为

$$\boldsymbol{p}_i(k)=\big[x_i(k),\ y_i(k),\ z_i(k)\big]^{\mathrm{T}}\in\mathbf{R}^3 \tag{11}$$

设通信半径为 R_c, 并用距离相关链路可用性刻画遮挡与衰落. 对边 $(i,\ j)$ 引入伯努利变量 $\xi_{ij}(k)\in\{0,\ 1\}$, 其中 $P(\xi_{ij}(k)=1)=1-p_{\mathrm{loss}}(d_{ij}(k))$, $P(\cdot)$ 为概率算子; $d_{ij}(k)=\|\boldsymbol{p}_i(k)-\boldsymbol{p}_j(k)\|_2$ 表示时刻 k 无人机 i 与无人机 j 之间的欧氏距离; $p_{\mathrm{loss}}(\cdot)$ 为距离相关的丢包概率函数, 其具体形式见第 4.1 节. 则邻接矩阵元素定义为

$$a_{ij}(k)=\begin{cases}1, & d_{ij}(k)\le R_c \text{ 且 } \xi_{ij}(k)=1\\ 0, & \text{其他}\end{cases} \tag{12}$$

为更贴近实际, 在编队结构诱导的规则拓扑 $\boldsymbol{A}_{\mathrm{form}}(k)$ 上叠加随机扰动拓扑 $\boldsymbol{A}_{\mathrm{rand}}(k)$, 得到

$$\boldsymbol{A}(k)=\boldsymbol{A}_{\mathrm{form}}(k)\vee\boldsymbol{A}_{\mathrm{rand}}(k) \tag{13}$$

其中“$\vee$”表示按元素逻辑或.

为控制数据规模并保留拓扑时变性, 设单个场景的仿真长度为 T, 并从每个场景任务窗口中抽取 K_{sample} 个代表性时间片构造图样本. 采用等间隔采样, 采样索引集合记为

$$\begin{cases}\mathcal{K}_{\mathrm{sample}}=\left\{k_s=\left\lfloor\dfrac{s(T-1)}{K_{\mathrm{sample}}-1}\right\rfloor\right\}_{s=0}^{K_{\mathrm{sample}}-1}\\ K_{\mathrm{sample}}=10\end{cases} \tag{14}$$

从而每个场景产生 K_{sample} 张图, 总图样本数为 $M=M_{\mathrm{scn}}K_{\mathrm{sample}}=1\,200$.

2.2 特征与任务状态构建

对每个图样本 $G(k)=(V,\ E(k),\ \boldsymbol{X}(k))$, 为节点 i 构造特征向量

$$\boldsymbol{x}_i(k)=\big[\boldsymbol{f}_i^{\mathrm{topo}}(k),\ \boldsymbol{f}_i^{\mathrm{task}}(k)\big]\in\mathbf{R}^{d_x} \tag{15}$$

其中 d_x 为节点特征维度, $\boldsymbol{f}_i^{\mathrm{topo}}(k)$ 与 $\boldsymbol{f}_i^{\mathrm{task}}(k)$ 分别为节点 i 的拓扑特征与任务状态特征, $[\cdot,\ \cdot]$ 表示拼接.

拓扑特征向量定义为

$$\boldsymbol{f}_i^{\mathrm{topo}}(k)=\big[d_i(k),\ \tilde{d}_i(k),\ \gamma_i(k),\ h_i\big] \tag{16}$$

其中 $d_i(k)$ 为节点 i 的拓扑特征选取度 (由邻接关系统计得到), $\tilde{d}_i(k)=d_i(k)/(N-1)$ 为归一化度, $\gamma_i(k)$ 用于表示局部聚类系数, $h_i\in\{0,\ 1\}$ 为节点角色标记 (1 表示骨干中继节点, 0 表示普通节点).

任务状态特征取局部编队误差与几何位置关系:

$$\begin{cases}e_i^{\mathrm{form}}(k)=\big\|\boldsymbol{p}_i(k)-\boldsymbol{p}_i^{\mathrm{ref}}(k)\big\|_2\\ d_i^{\mathrm{cen}}(k)=\big\|\boldsymbol{p}_i(k)-\boldsymbol{p}_c(k)\big\|_2\end{cases} \tag{17}$$

其中 e_i^{form} 表示节点 i 在时刻 k 的局部编队位置误差, d_i^{cen} 表示节点 i 在时刻 k 到编队质心的欧氏距离, $\boldsymbol{p}_c(k)$ 为编队质心 (如 $\boldsymbol{p}_c(k)=(1/N)\sum_{i=1}^{N}\boldsymbol{p}_i(k)$).

$$\boldsymbol{f}_i^{\mathrm{task}}(k)=\big[e_i^{\mathrm{form}}(k),\ d_i^{\mathrm{cen}}(k),\ l_i\big] \tag{18}$$

其中连续特征采用训练集统计量作 z-score 标准化, 离散标记保持 0/1 或小整数编码, 以保证跨场景的一致尺度. l_i 表示任务负载/角色离散标记. 在本文仿真中, 该标记由任务规划/调度模块直接给定; 在实际系统中, 可由任务分配结果、调度器状态、任务队列积压水平或链路层负载指示等运行时信息直接获得或在线统计得到. 因此, l_i 属于当前时刻可观测的任务状态描述, 而非由退化标签或攻击结果反推得到. 模型实现时, 离散标记 l_i 不单独作嵌入映射, 而是与连续特征直接拼接形成节点输入向量, 再统一通过输入层线性映射投影到隐藏空间. 考虑到本文中离散标记取值范围较小且语义明确, 该处理方式已足以表达其类别信息, 并可减少额外参数引入.

2.3 任务退化导向标注与数据划分

依据第 1 节给出的综合性能代价 $J(G,\ S)$ 与

综合性能退化量 $\Delta J(G,\,S)$, 对每个图样本 $G^{(m)}(k)$ 的节点进行“任务退化导向”标注. 先在无攻击条件下仿真得到

$$J_{\text{base}}^{(m)}(k)=J\big(G^{(m)}(k),\,\emptyset\big) \tag{19}$$

其中 m 为场景编号, $G^{(m)}(k)$ 为第 m 个场景在时刻 k 的图样本. $S=\emptyset$ 表示无攻击集合. 随后对每个节点 $i\in V^{(m)}$, $V^{(m)}$ 为第 m 个场景的节点集合, 在预设攻击时刻 k_a 将其置为失效, 并重新仿真至任务结束, 得到

$$\begin{cases} J_i^{(m)}(k)=J\big(G^{(m)}(k),\,\{i\}\big) \\ r_i^{(m)}(k)=J_i^{(m)}(k)-J_{\text{base}}^{(m)}(k) \end{cases} \tag{20}$$

其中 $\{i\}$ 表示单点攻击集合, $r_i^{(m)}(k)$ 为节点 i 的单点退化标签. 为便于训练, 对连续标签作 min-max 归一化:

$$\hat{r}_i^{(m)}(k)=\frac{r_i^{(m)}(k)-r_{\min}}{r_{\max}-r_{\min}} \tag{21}$$

其中 $r_{\min}$, $r_{\max}$ 分别为训练集标签的最小值与最大值. 数据划分采用“场景级”策略: 将 $M_{\text{scn}}=120$ 个场景按 6 : 2 : 2 划分为训练/验证/测试集, 并将同一场景下所有采样时间片整体划入同一子集, 以避免跨集合信息泄露. 单点标注需对每个图样本执行一次无攻击仿真及 N_m 次单点失效重仿真, 总仿真次数约为 $M(1+\bar{N})$, 其中 $\bar{N}$ 为平均节点数. 实现中按场景并行 (多进程) 生成标签, 在 16 核中央处理器 (central processing unit, CPU) 工作站上生成全部 $M=1\,200$ 张图样本的单点退化标签耗时约 6 h.

3　融合拓扑先验与任务状态的 Transformer 关键节点评估模型

3.1　总体框架

为学习图样本到节点关键性标签的映射, 本文采用 TPT-Former, 输入为第 2 节构造的图 $G(k)=(V,\,E(k),\,\boldsymbol{X}(k))$, 输出为节点级关键性评分 $\{s_i\}_{i=1}^{N}$, 用于近似归一化标签 $\{\hat{r}_i\}$. 模型结构如图 2 所示, 由输入层、TPT-Former 编码器和节点回归输出头组成. f_Θ 表示从图样本到节点关键性评分的学习映射, Θ 为模型参数.

3.2　拓扑先验与任务状态增强的图注意力

1) 输入与位置编码. 对节点 i 的原始特征 $\boldsymbol{x}_i\in\mathbf{R}^{d_x}$ 进行线性映射得到初始表示

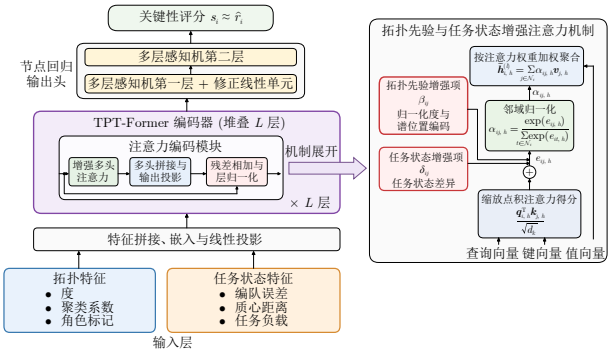


图 2　TPT-Former 关键节点评估模型结构示意图

Fig. 2　Architecture diagram of the proposed TPT-Former model for critical node evaluation

$$\boldsymbol{h}_i^{(0)}=\boldsymbol{W}_{\text{in}}\boldsymbol{x}_i+\boldsymbol{b}_{\text{in}} \tag{22}$$

其中 $\boldsymbol{h}_i^{(0)}$ 为初始隐表示; $\boldsymbol{W}_{\text{in}}$, $\boldsymbol{b}_{\text{in}}$ 为可学习参数. 为显式注入结构位置信息, 本文采用归一化拉普拉斯矩阵的前 d_{pe} 个非平凡特征向量作为谱位置编码, 实现时仅进行部分谱分解, 而非全量特征分解. 令归一化图拉普拉斯矩阵为

$$\boldsymbol{L}_{\text{n}}=\boldsymbol{I}-\boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{A}\boldsymbol{D}^{-\frac{1}{2}} \tag{23}$$

其中 $\boldsymbol{A}$ 为邻接矩阵, $\boldsymbol{D}$ 为度矩阵, $\boldsymbol{I}$ 为单位矩阵. 取 $\boldsymbol{L}_{\text{n}}$ 的前 d_{pe} 个非平凡特征向量组成 $\boldsymbol{P}_{\text{E}}\in\mathbf{R}^{N\times d_{\text{pe}}}$, d_{pe} 为谱编码维度, 第 i 行 $\boldsymbol{p}_{\text{E},\,i}$ 为节点 i 的位置编码. 由于谱特征向量存在符号不确定性, 训练时对 $\boldsymbol{P}_{\text{E}}$ 的每一列特征向量以 0.5 的概率乘以 -1, 进行符号翻转数据增强.

2) 增强注意力打分. 在第 l 层多头注意力中, 对每个头 $h\in\{1,\,\cdots,\,H\}$, 定义

$$\begin{cases} \boldsymbol{q}_{i,\,h}=\boldsymbol{W}_{q,\,h}^{(l)}\boldsymbol{h}_i^{(l-1)} \\ \boldsymbol{k}_{j,\,h}=\boldsymbol{W}_{k,\,h}^{(l)}\boldsymbol{h}_j^{(l-1)} \\ \boldsymbol{v}_{j,\,h}=\boldsymbol{W}_{v,\,h}^{(l)}\boldsymbol{h}_j^{(l-1)} \end{cases} \tag{24}$$

其中 $\boldsymbol{h}_i^{(l-1)}$ 为上一层节点表示; $\boldsymbol{q}_{i,\,h}$, $\boldsymbol{k}_{j,\,h}$, $\boldsymbol{v}_{j,\,h}$ 分别为第 h 个头的查询向量、键向量、值向量; $\boldsymbol{W}_{q,\,h}^{(l)}$, $\boldsymbol{W}_{k,\,h}^{(l)}$, $\boldsymbol{W}_{v,\,h}^{(l)}$ 为可学习矩阵. 对边 $(i,\,j)\in E$, 基础打分采用缩放点积形式, 并叠加两类增强项:

$$e_{ij,\,h}=\frac{\boldsymbol{q}_{i,\,h}^{\text{T}}\boldsymbol{k}_{j,\,h}}{\sqrt{d_k}}+\beta_{ij}+\delta_{ij} \tag{25}$$

其中 $e_{ij,\,h}$ 为第 h 个头的注意力打分, β_{ij} 为拓扑先验增强项, δ_{ij} 为任务状态增强项, d_k 为每个头的键向量维度. 为避免增强项尺度不一致, β_{ij} 与 δ_{ij} 均引入可学习缩放系数:

$$\beta_{ij}=w_d\big(\tilde{d}_i+\tilde{d}_j\big)+w_p\cdot\big(\boldsymbol{p}_{\text{E},\,i}^{\text{T}}\boldsymbol{p}_{\text{E},\,j}\big) \tag{26}$$

$$\delta_{ij} = -w_s \left\| \boldsymbol{f}_i^{\text{task}} - \boldsymbol{f}_j^{\text{task}} \right\|_2^2 \tag{27}$$

其中 w_d, w_p, w_s 为可学习标量 (在同一层内共享于各头); $\tilde{d}_i$, $\tilde{d}_j$ 为归一化度; $\boldsymbol{p}_{\text{E},\,i}^{\text{T}} \boldsymbol{p}_{\text{E},\,j}$ 为谱位置编码相似度; $\boldsymbol{f}_i^{\text{task}}$, $\boldsymbol{f}_j^{\text{task}}$ 为任务状态子特征. 注意力权重与聚合为

$$\alpha_{ij,\,h} = \frac{\exp(e_{ij,\,h})}{\sum\limits_{t \in \mathcal{N}_i} \exp(e_{it,\,h})}, \quad \tilde{\boldsymbol{h}}_{i,\,h}^{(l)} = \sum_{j \in \mathcal{N}_i} \alpha_{ij,\,h} \boldsymbol{v}_{j,\,h} \tag{28}$$

其中 $\alpha_{ij,\,h}$ 为第 h 个头的注意力权重, $\mathcal{N}_i$ 为节点 i 的邻居集合, $\tilde{\boldsymbol{h}}_{i,\,h}^{(l)}$ 为第 l 层第 h 个头的聚合结果. 多头输出拼接后经线性变换, 并采用残差与层归一化稳定训练:

$$\boldsymbol{h}_i^{(l)} = \text{LN}\left(\boldsymbol{h}_i^{(l-1)} + \boldsymbol{W}_o \big(\mathop{\Big\|}_{h=1}^{H} \tilde{\boldsymbol{h}}_{i,\,h}^{(l)} \big) \right) \tag{29}$$

其中 H 为注意力头数, $\boldsymbol{W}_o$ 为输出投影矩阵, LN$(\cdot)$ 为层归一化 (layer normalization, LN) 算子, $\|$ 表示拼接.

3.3 节点回归头与训练目标

编码器输出 $\boldsymbol{h}_i^{(L)}$ 经轻量多层感知机 (multilayer perceptron, MLP) 回归头得到关键性评分 s_i:

$$s_i = \boldsymbol{W}_2 \boldsymbol{z}_i + \boldsymbol{b}_2, \ \boldsymbol{z}_i = \text{ReLU}(\boldsymbol{W}_1 \boldsymbol{h}_i^{(L)} + \boldsymbol{b}_1) \tag{30}$$

其中 ReLU$(\cdot)$ 为修正线性单元 (rectified linear unit, ReLU) 激活函数; L 为编码器层数; $\boldsymbol{z}_i$ 为回归头中间表示; $\boldsymbol{W}_1$, $\boldsymbol{W}_2$, $\boldsymbol{b}_1$, $\boldsymbol{b}_2$ 为可学习参数. 为提高对高关键节点的拟合与排序敏感性, 采用标签加权均方误差:

$$\mathcal{L} = \frac{1}{M} \sum_{m=1}^{M} \frac{1}{N_m} \sum_{i=1}^{N_m} w_i^{(m)} \left(s_i^{(m)} - \hat{r}_i^{(m)} \right)^2 + \lambda \|\Theta\|_2^2 \tag{31}$$

其中 w_i 为样本权重, 定义为 $w_i = 1 + \lambda_{\text{imp}} \hat{r}_i$, λ_{imp} 为加权系数; $\mathcal{L}$ 为训练损失; M 为训练图样本数; N_m 为第 m 个图的节点数; λ 为二范数平方正则化系数.

4 资源受限攻击策略与仿真实验

4.1 场景可视化、攻击建模与实验设置

为直观呈现“选点差异 → 拓扑断裂 → 队形退化”的链式关系, 本节首先说明资源受限选点机制与实现流程, 随后给出代表性场景下攻击前后队形与通信拓扑快照以及关键性评分的空间分布与 Top-B 命中对比, 以展示不同选点导致的拓扑断裂形态与编队退化差异.

在攻击次数与攻击成本双约束下, 资源受限最优攻击问题可统一表述为第 1 节的式 (9). 为获得可计算的近似策略, 本文以第 3 节的关键性评分 s_i 作为归一化单点关键性标签 $\hat{r}_i$ 的预测值, 构造单位成本攻击价值

$$\rho_i = \frac{s_i}{c_i} \tag{32}$$

随后按 ρ_i 递减排序并采用贪心过程生成攻击集合, 其流程如图 3 所示. 为保证对比公平, 各基线方法均采用相同的“评分/指标 → 排序 → 贪心选点 → 仿真评估”流程, 仅替换排序依据 (度中心性、介数中心性或关键性评分), 并保持相同的 $(B,\ C_{\max})$ 与攻击时刻 k_a.

为增强“选点–拓扑断裂–队形退化”的可审查性, 本文设置在同一代表性场景、相同资源约束与相同攻击时刻下, 对比基线介数中心性选点 (betweenness) 与本文方法 (TPT-Former) 选点的可视化结果. 如图 4(a) 所示, 节点形状表征攻击成本 (灰色圆点为普通节点, $c_i = 1$; 蓝色方块为骨干中继节点, $c_i = 2$), 红色圈/框及编号标记表示在给定 $(B,\ C_{\max})$ 约束下经排序并贪心选中的攻击目标集合. 本文代表性场景的仿真长度为 $T = 150$, 因而 $k_a = \lfloor 0.3T \rfloor = 45$. 攻击生效后, 相关节点从通信图

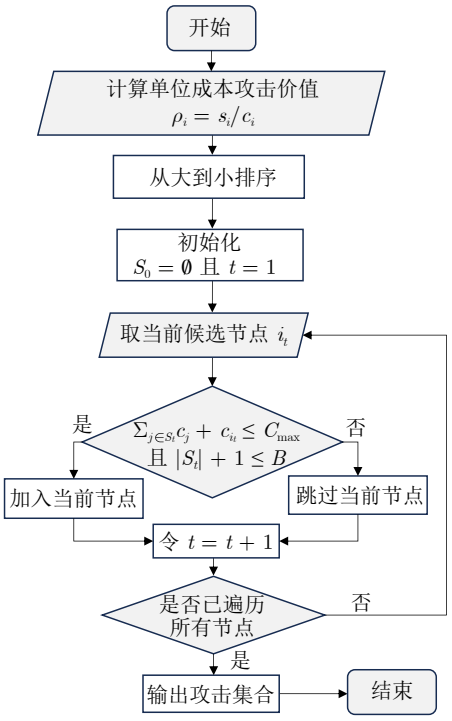
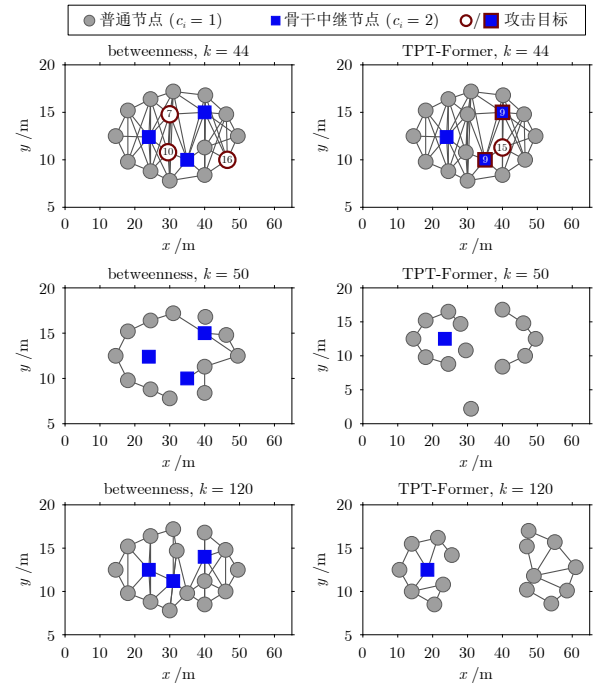
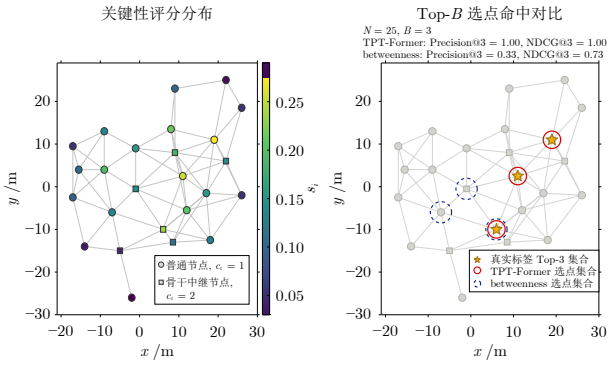


图 3 基于单位成本攻击价值的贪心选点过程示意图

Fig. 3 Schematic diagram of the greedy node-selection procedure based on attack value per unit cost



(a) 攻击前后队形与通信拓扑快照
(a) Formation and communication-topology snapshots before and after attacks



(b) 关键性评分空间分布与 Top-B 命中对比
(b) Spatial distribution of criticality scores and Top-B matching comparison

图 4　代表性场景下选点差异的可视化结果

Fig. 4　Visualization results of node selection differences in a representative scene

中删除, 剩余拓扑仍按第 1.3 节所述规则继续演化. 相比基线, 本文方法更倾向于命中承担跨簇信息转发的关键节点, 从而在相同预算下更易诱发连通性削弱与子图分裂, 并与后续时域连通性指标 $\lambda_2(\boldsymbol{L}(k))$ 的下降及编队误差 $E_{\mathrm{form}}(k)$ 的放大相一致. 图 4(b) 进一步给出学习到的关键性评分空间分布与 Top-B 命中示例, 可见高分区域更集中于桥接位置且区分度更强.

本文在“城市灾后巡检与编队巡航”仿真环境下生成时变无人机群图样本并开展对比实验. 每个任务场景的无人机数量取 $N \in [20, 40]$, 仿真长度为 $T = 100 \sim 150$ 个离散步长, 采样周期 $\Delta t = 0.1$ s. 为保留拓扑时变性并控制数据规模, 每个场景选取 $K_{\mathrm{sample}} = 10$ 个代表性时间片构造图样本, 并按“场景级”划分为训练/验证/测试集 (比例为 6 : 2 : 2), 避免同一场景跨集合导致信息泄露. 通信半径设为 $R_c = 30$ m, 链路可用性由距离相关随机变量 $\xi_{ij}(k)$ 决定. 丢包概率采用分段线性模型

$$p_{\mathrm{loss}}(d) = \begin{cases} 0, & d \le 0.7R_c \\ 0.3 \cdot \dfrac{d - 0.7R_c}{0.3R_c}, & 0.7R_c < d < R_c \\ 1, & d \ge R_c \end{cases} \tag{33}$$

其中, d 表示链路两端无人机之间的欧氏距离.

为增强拓扑时变性, 在规则拓扑上叠加随机删边与加边扰动, 删边概率 $p_{\mathrm{fail}} = 0.05$, 加边概率 $p_{\mathrm{add}} = 0.02$. 资源受限攻击评估中, 取 $B \in \{1, 2, 3, 5\}$、$C_{\max} \in \{3, 5, 8\}$, 节点成本由角色决定 (骨干中继节点 $c_i = 2$, 普通节点 $c_i = 1$). 其中, 上述预算分别覆盖以普通节点为主的低预算攻击、普通节点与骨干中继节点混合的中等预算攻击以及可攻击多个骨干中继节点或较大规模混合集合的较高预算攻击. 攻击时刻统一设置为 $k_a = \lfloor 0.3T \rfloor$, 以避免在初始瞬态阶段过早施加攻击, 并保证攻击后仍保留足够长的评估窗口用于统计连通性、编队误差与任务完成率的持续变化. 任务完成率与退化曲线采用 100 次蒙特卡洛 (Monte Carlo, MC) 重复仿真统计均值与标准差; 各学习模型重复训练 3 次并报告均值. 综合性能代价 (7) 中窗口长度取 $T_w = T$; 任务完成判定阈值取 $\varepsilon_{\mathrm{form}} = 1.0$, 并固定 $(w_1, w_2, w_3) = (1, 1, 5)$; 连通性映射取 $\phi(\lambda_2) = 1/(\lambda_2 + \epsilon_\lambda)$ 且 $\epsilon_\lambda = 10^{-3}$; 误差项归一化采用无攻击基线窗口均值并取 $\epsilon_E = 10^{-6}$ 以避免分母为零. 模型结构与训练超参数设置见表 1. 为验证综合代价函数中固定权重设定的合理性, 本文在测试集上进一步统计三项代价分量对总成本的窗口平均贡献占比. 如表 2 所示, 三项代价分量在测试集上的平均贡献占比分别为计算误差项、连通性项和任务失败惩罚项在总成本中的相对占比, 并以均值 ± 标准差形式报告. 统计结果表明, 三项分量在测试集上的平均贡献分别为 31.2% ± 6.8%、22.7% ± 5.4% 和 46.1% ± 7.3%, 均保持非退化贡献, 且未出现某一项长期单边主导总成本的现象, 这说明本文采用的固定权重 $(w_1, w_2, w_3) = (1, 1, 5)$ 具有基本的稳健性与可解释性.

此外, 为评估方法的计算代价, 本文在 $N = 20$, 30, 40 三种节点规模下统计了谱编码预处理、模型训练与推理耗时, 结果见表 3. 结果表明, 谱编码开销随节点规模增加而上升, 但在本文考虑的节点范

表 1 模型与训练超参数设置
Table 1 Model and training hyperparameter settings

超参数	取值
编码器层数 L /头数 H	4 / 4
隐藏维度 d /谱维度 d_{pe}	128 / 8
丢弃率 Dropout	0.1
优化器	AdamW
初始学习率/权重衰减	1×10^{-3} / 1×10^{-4}
批大小/最大训练轮数	16 / 200
早停耐心值	20
λ_{imp} / λ	2.0 / 1×10^{-4}

表 2 测试集上综合代价三项分量的窗口平均贡献占比 (%)
Table 2 Window-averaged contribution ratios of the three composite-cost components on the test set (%)

代价分量	平均贡献占比	标准差
$w_1 E_{\text{form}}$	31.2	6.8
$w_2\phi(\lambda_2(\boldsymbol{L}))$	22.7	5.4
$w_3(1-\eta_{\text{task}})$	46.1	7.3

围内, 其耗时仍处于可接受水平, 说明所提方法在中等规模复杂无人机群场景中具备实际可运行性.

4.2 关键性预测性能评估

在测试集上评估节点关键性预测的回归精度与排序一致性. 图 5 给出部分节点真实关键性标签与模型预测关键性评分的对应关系, 可见模型能够较好地跟踪关键性变化趋势. 在测试集上先对每个图样本分别计算均方误差 (mean squared error, MSE)、平均绝对误差 (mean absolute error, MAE) 与 Spearman 秩相关系数, 再对图样本取平均, 得到 MSE_{test}、MAE_{test} 与 ρ_{Spearman}.

表 4 汇总测试集指标: 相比于图注意力网络, 本文方法的 MSE_{test} 由 0.028 降至 0.021 (降低 25.0%), MAE_{test} 由 0.112 降至 0.096 (降低 14.3%), Spearman 秩相关系数由 0.819 提升至 0.887 (提升 0.068). 两种结构消融模型 (去除拓扑先验与去除任务状态) 在三项指标上均出现退化, 说明拓扑先验与任务状态对关键性建模具有实质贡献, 且预测排

表 3 不同节点规模下的谱编码与模型运行耗时
Table 3 Spectral-encoding and model runtimes for different numbers of nodes

节点数 N	谱编码 (ms)	训练 (s/轮)	推理 (ms/图)
20	1.8487	2.4139	0.7408
30	3.2514	3.6795	1.0823
40	5.1305	5.1458	1.4674

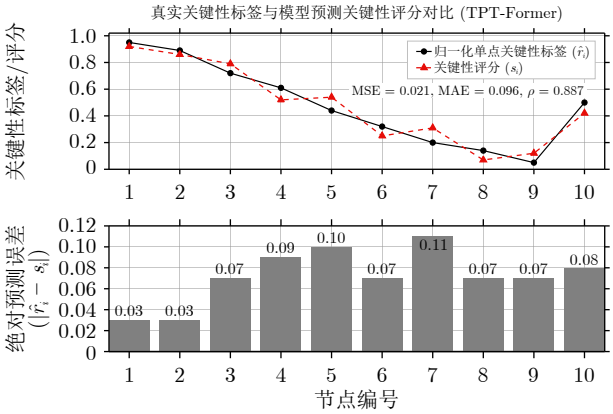


图 5 真实关键性标签与模型预测关键性评分对比及绝对预测误差
Fig. 5 Comparison of ground-truth criticality labels and model-predicted criticality scores with absolute prediction errors

表 4 不同模型在测试集关键性预测任务上的性能对比
Table 4 Performance comparison of different models for criticality prediction tasks on the test set

模型	MSE_{test}	MAE_{test}	ρ_{Spearman}
GCN	0.032	0.123	0.781
GAT	0.028	0.112	0.819
TPT-Former	0.021	0.096	0.887
去除拓扑先验	0.024	0.103	0.864
去除任务状态	0.025	0.107	0.856
去除 h_i	0.026	0.109	0.842
去除 $(h_i,\ l_i)$	0.029	0.114	0.828

序的稳定性能够支撑预算受限的 Top-B 选点. 为排除模型过度依赖角色标记 h_i 与任务负载/角色离散标记 l_i 带来的潜在信息泄露或“读答案”效应, 本文进一步移除 h_i, 同时移除 $(h_i,\ l_i)$ 进行消融. 由表 4 可见, 去除先验标记后性能有所下降 (如去除 h_i 的 ρ_{Spearman} 由 0.887 降至 0.842, 去除$(h_i,\ l_i)$ 降至 0.828), 但整体仍保持较强的排序一致性, 表明模型并非仅依赖角色/负载信息, 而是能够从拓扑与任务状态中学习到与退化敏感度相关的关键性表征.

为避免仅展示单一场景带来的偶然性, 本文在测试集上进一步统计 Top-B 命中性能 (均值 ± 标准差), 统计结果见表 5. 其中, 真实标签 (ground truth) 集合 $S_B^{\star}$ 由真实单点关键性标签 $r_i=\Delta J(G,\{i\})$ 排序后取前 B 个节点得到, 预测集合记为 $\hat{S}_B$; 准确率 Precision@B 定义为 $|S_B^{\star}\cap\hat{S}_B|/B$, 用于衡量预测前 B 个节点对真实高退化单点集合的命中率; 归一化折损累计增益 (normalized discounted cumulative gain, NDCG) NDCG@B 采用 r_i 作为

表 5　测试集 Top-B 命中性能统计

Table 5　Top-B matching performance statistics on the test set

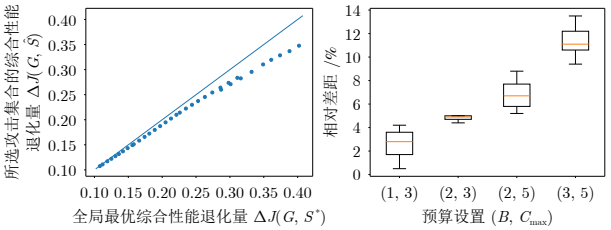
指标	$B=1$	$B=2$	$B=3$
Precision@B	0.66 ± 0.08	0.60 ± 0.07	0.55 ± 0.06
NDCG@B	0.78 ± 0.06	0.76 ± 0.05	0.74 ± 0.04

相关性得分, 用于衡量模型对高退化节点的优先排序能力. 需要说明的是, Top-B 命中统计主要用于佐证模型对高退化单点的排序稳定性, 其本身并不直接等价于双约束组合攻击问题式 (9) 的最优性证明; 预算约束下攻击集合对式 (9) 最优解的逼近能力, 通过下文的小规模最优对照实验进一步验证. 两者共同构成“单点标签近似预算选点”的互补证据链.

为进一步验证“单点标签近似预算选点”在组合层面的有效性, 本文在节点数较少、可精确求解的小规模图上补充了最优对照实验. 具体而言, 对满足预算约束 $(B,\ C_{\max})$ 的候选攻击集合进行穷举评估, 并以式 (9) 中的真实综合性能退化量 $\Delta J(G,\ S)$ 作为目标, 得到全局最优攻击集合 $S^{\star}$. 与此同时, 本文方法仍严格按照第 4.1 节所述流程, 先由模型输出节点关键性评分, 再在预算约束下采用贪心策略生成预测攻击集合 $\hat{S}$. 这样便可在相同预算条件下, 直接比较“本文方法得到的组合攻击效果”与“全局最优组合攻击效果”之间的差距, 从而把验证层次从单点排序推进到组合决策.

图 6(a) 表明, 大多数样本点均紧邻参考对角线分布, 这说明在多数小规模样本上, 本文方法得到的预算攻击集合所造成的真实综合退化量较接近全局最优值. 换言之, 虽然本文方法并不是直接对式 (9) 做组合求解, 而是通过“单点评分 + 预算贪心”的方式构造攻击集合, 但其最终得到的组合攻击效果在多数样本上仍能够较好地逼近最优结果. 同时也可以观察到, 当最优退化量逐渐增大时, 部分样本点与参考线之间出现了轻微偏离, 这表明在退化更强、组合效应更明显的场景下, 基于单点评分的预算贪心策略仍可能与全局最优之间存在一定差距, 但这种差距整体上仍处于可接受范围内.

进一步地, 图 6(b) 从分布角度给出了不同预算设置下本文方法相对于全局最优攻击集合的差距情况, 其中相对差距定义为 $\text{Gap} = (\Delta J(G,\ S^{\star}) - \Delta J(G,\ \hat{S}))/\Delta J(G,\ S^{\star}) \times 100\%$. 从图中可以看出, 在较紧预算设置下, 如 $(B,\ C_{\max}) = (1,\ 3)$ 和 $(2,\ 3)$, 差距的中位数较低且分布较集中, 说明当可选节点数量较少、资源约束较强时, 本文方法更容易逼近组合最优. 随着预算逐渐放宽至 $(2,\ 5)$ 和 $(3,\ 5)$, 差距的整体分布有所上升, 尤其在 $(3,\ 5)$ 条件下离散



(a) 所选攻击集合与全局最优攻击集合的综合性能退化量散点对比 (a) Scatter comparison of the performance degradation caused by the selected attack set and the globally optimal attack set

(b) 不同预算设置下相对于全局最优的相对差距分布 (b) Relative gap distributions to the global optimum under different budget settings

图 6　小规模最优对照实验结果

Fig. 6　Experimental results of the small-scale optimality benchmark

程度更为明显. 这一现象与问题本身的组合复杂性是一致的: 当预算变宽、可行攻击组合显著增多时, 不同节点之间的冗余关系和非加性交互效应会更加突出, 因此仅依赖单点评分构造的贪心选点不可避免地会产生一定近似误差. 但从整体趋势看, 这种误差并未破坏本文方法对组合最优的逼近能力, 而是反映了“单点标签 $\rightarrow$ 预算组合决策”这一近似链条在更复杂预算区域下的自然误差积累. 因而, Top-B 命中统计主要提供排序层面的稳定性证据, 而小规模最优对照实验则进一步给出了预算双约束组合攻击近优性的补充证据, 二者共同构成本文“单点标签近似预算选点”的验证链条.

4.3　资源受限攻击效果对比与退化机理分析

在相同资源约束 $(B,\ C_{\max})$ 下比较不同攻击策略对闭环任务的实际破坏效果. 对测试集所有场景取平均, 定义平均退化指标

$$\overline{\Delta J}(B,\ C_{\max}) = \frac{1}{M_{\text{test}}} \sum_{m=1}^{M_{\text{test}}} \Delta J^{(m)}\big(G^{(m)},\ S^{(m)}(B,\ C_{\max})\big) \tag{34}$$

其中, M_{test} 表示参与攻击效果评估的测试场景总数.

图 7 给出了任务完成率 η_{task} 随最大攻击节点数 B 的变化 (均值 ± 标准差, 100 次 MC). 在各预算条件下, 本文方法的任务完成率均低于介数中心性攻击 (betweenness), 说明其在相同资源约束下能够造成更强的任务破坏效果. 在 $B=2$ 时, 本文方法将任务完成率降至 0.736 ± 0.041, 相比介数中心性攻击的 0.802 ± 0.034 下降 0.066; 当 $B=3$ 时, 本文方法为 0.541 ± 0.042, 相比介数中心性攻击的 0.663 ± 0.038 下降 0.122; 当 $B=5$ 时, 本文方法为

0.413 ± 0.053, 相比介数中心性攻击的 0.477 ± 0.046 下降 0.064. 该结果表明, 在相同攻击次数约束下, 学习型选点更易命中对任务完成最敏感的节点集合, 且优势在中等预算区域更为明显.

图 8 进一步给出典型预算 $(B,\ C_{\max}) = (3,\ 5)$ 下 $\overline{\Delta J}$ 的收敛曲线. 在典型预算 $(B,\ C_{\max}) = (3,\ 5)$ 下, 本文方法的 $\overline{\Delta J}$ 高于介数中心性攻击、度中心性攻击 (degree) 以及 GAT 基线, 其中与本文方法最接近的对比对象为介数中心性攻击. 在 100 次仿真统计末端, 本文方法达到 $\overline{\Delta J} = 0.372$, 高于介数中心性攻击的 0.312, 高于度中心性攻击的 0.285, 且明显高于 GCN 基线与 GAT 基线 (分别为 0.258 与 0.283).

为验证成本感知建模在双约束条件下对资源利用效率的影响, 图 9 给出了策略消融结果, 其中 $C_{\max} = 5$, $k_a = \lfloor 0.3T \rfloor$, 结果为 100 次独立 MC 运行的均值 ± 标准差, 并在相同预算约束下对 rho-based (TPT-Former) $(\rho_i = s_i/c_i)$、score-only、cost-only、random 与 betweenness 进行对比. 结果显示, rho-based (TPT-Former) 在各预算区间均导致更低的 η_{task} 与更高的 $\overline{\Delta J}$, 且相较 betweenness 的 η_{task} 下降 0.188、$\overline{\Delta J}$ 增加约 0.060 (当最大攻击节点数 $B = 3$ 时), 表明式 (32) 可提升单位资源破坏效能.

进一步从动态过程层面分析退化机理. 图 10 绘制了代表性场景中攻击前后代数连通度 $\lambda_2(\boldsymbol{L}(k))$ 与编队误差 $E_{\text{form}}(k)$ 的时域演化. 攻击发生前, 各方法的 $\lambda_2(\boldsymbol{L}(k))$ 维持在较高水平且 $E_{\text{form}}(k)$ 收敛至低误差区间; 攻击发生后, 学习型选点导致 $\lambda_2(\boldsymbol{L}(k))$ 显著下降, 同时 $E_{\text{form}}(k)$ 出现更大幅度的瞬时放大并维持更高的稳态误差.

最后, 图 11 给出了攻击时刻 k_a、通信半径 R_c 与成本分布的单因素敏感性分析结果. 数据为 100 次独立 MC 运行的均值 ± 标准差, 每个子图仅改变一个因素且其余保持不变. 对比方法为 rho-based (TPT-Former) (基于 $\rho_i = s_i/c_i$ 的贪心选择) 与 betweenness (criticality-based baseline). 在不同参数配置导致的可通信性与资源异质性变化下, 学习

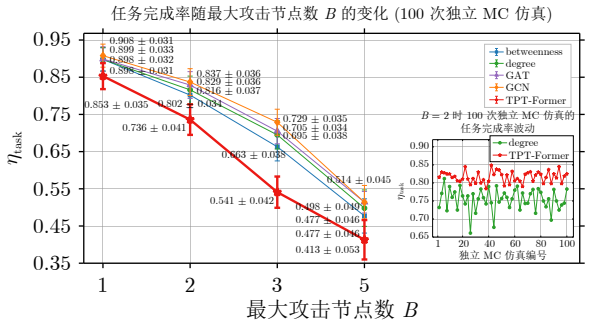


图 7 不同攻击策略下任务完成率随最大攻击节点数 B 变化曲线

Fig. 7 Variation curves of task success rate with the maximum number of attack nodes B under different strategies

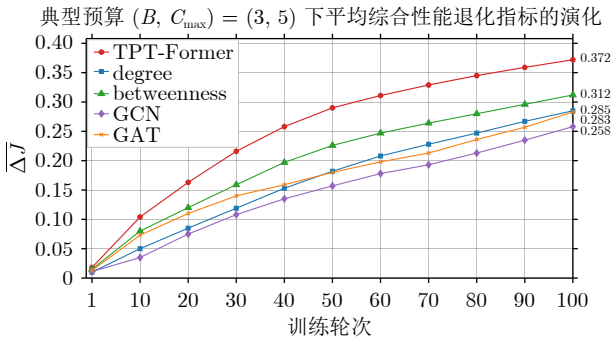
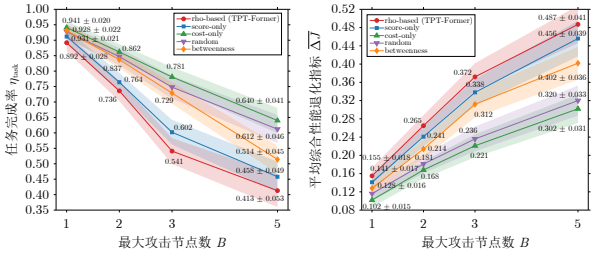


图 8 典型预算 $(B,\ C_{\max}) = (3,\ 5)$ 下综合性能退化量的收敛曲线

Fig. 8 Convergence curves of comprehensive performance degradation under the typical budget $(B,\ C_{\max}) = (3,\ 5)$



(a) 任务完成率随最大攻击节点数 B 的变化

(a) Task success rate versus maximum number of attack nodes B

(b) 平均性能退化量随最大攻击节点数 B 的变化

(b) Average performance degradation versus maximum number of attack nodes B

图 9 策略消融结果: η_{task} 与 $\overline{\Delta J}$

Fig. 9 Strategy ablation results for η_{task} and $\overline{\Delta J}$

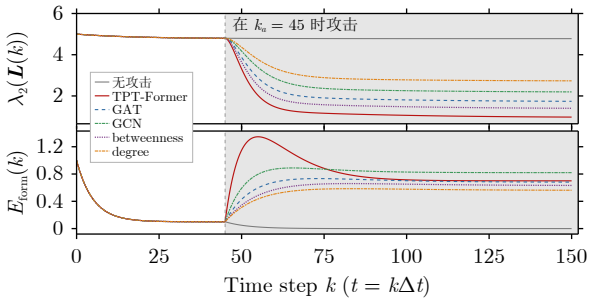
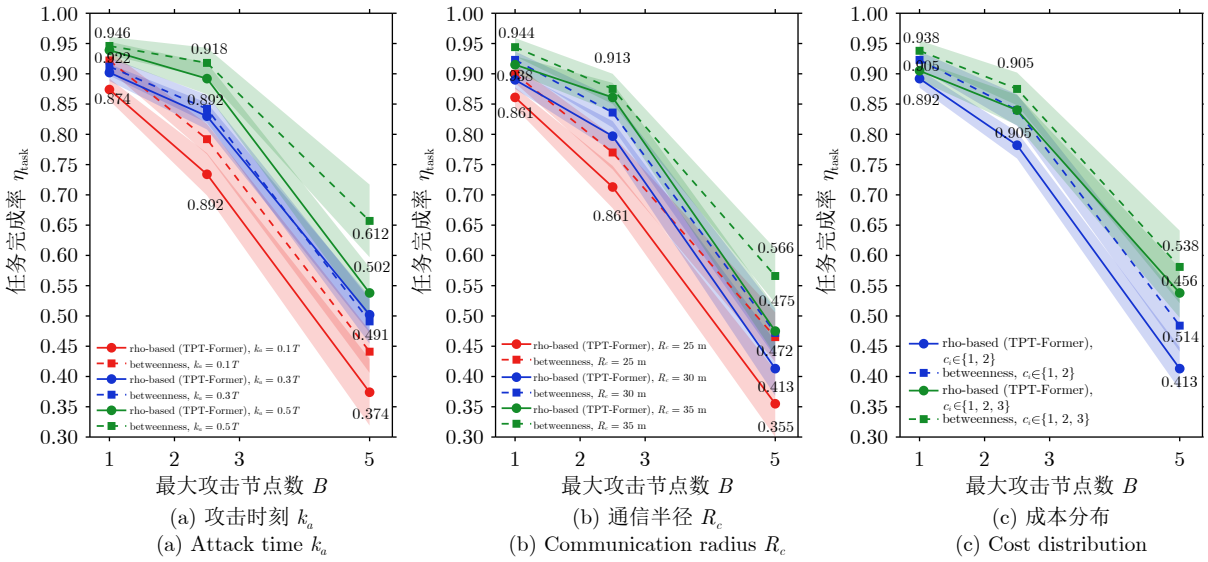


图 10 攻击后代数连通度与编队误差的时域演化 $(k_a = 45)$

Fig. 10 Time-domain evolution of algebraic connectivity and formation error after attacks $(k_a = 45)$



(a) 攻击时刻 k_a
(a) Attack time k_a

(b) 通信半径 R_c
(b) Communication radius R_c

(c) 成本分布
(c) Cost distribution

图 11　攻击时刻、通信半径与成本分布的敏感性分析

Fig. 11　Sensitivity analysis of attack time, communication radius, and cost distribution

型成本感知选点仍保持稳定优势, 表明所提方法具有良好的跨条件鲁棒性. 敏感性分析结果表明, 当攻击时刻在 $0.2T \sim 0.4T$ 范围内变化时, 本文方法相较 betweenness 基线的优势保持稳定: 任务完成率平均降低 $0.084 \sim 0.127$, 综合性能退化量 ΔJ 平均提高 $0.041 \sim 0.058$. 当 k_a 过早 (约 $0.1T$) 时, 系统尚未充分进入稳定协同阶段, 不同方法的退化差异有所减弱; 当 k_a 过晚 ($\geq 0.5T$) 时, 由于攻击后评估窗口缩短, 部分指标的区分度下降.

5　结束语

本文面向复杂无人机群在通信扰动与节点失效条件下的抗毁性评估需求, 构建了无人机群图建模与任务退化导向标注体系, 提出融合拓扑先验与任务状态增强的 Transformer 关键节点评估模型, 并在攻击节点数量与总攻击成本双约束下设计了基于关键性评分的资源受限选点策略. 仿真结果表明, 所提方法在关键性预测一致性与单位资源退化效能方面优于中心性指标与 GAT 等基线, 可为无人机群关键节点识别与加固决策提供参考. 后续将进一步考虑攻击后的在线拓扑重构与防御协同机制, 并在更大规模和异构通信条件下验证所提方法的泛化能力与实时性.

参考文献

1　Wang Yao-Nan, Hua He-An, Zhang Hui, Zhong Hang, Fan Ye-Xin, Liang Hong-Tao, et al. Performance function-guided deep reinforcement learning control for UAV swarm. *Acta Automatica Sinica*, 2025, **51**(5): 905−916
(王耀南, 华和安, 张辉, 钟杭, 樊叶心, 梁鸿涛, 等. 性能函数引导的无人机集群深度强化学习控制方法. 自动化学报, 2025, **51**(5): 905−916)

2　Fang Hao, Zhao Xin-Yue, Chen Jie. Autonomous control of unmanned aerial vehicle swarms: Prescribed performance driven safety formation control. *Acta Automatica Sinica*, 2025, **51**(5): 931−941
(方浩, 赵欣悦, 陈杰. 无人飞行器集群自主控制: 预设性能驱动的安全编队控制. 自动化学报, 2025, **51**(5): 931−941)

3　Jiang Bin, Ma Ya-Jie, Xue Shu-Xin. Autonomous control of unmanned aerial vehicle swarms: Task allocation based on coalition formation game. *Acta Automatica Sinica*, 2025, **51**(5): 942−959
(姜斌, 马亚杰, 薛舒心. 无人飞行器集群自主控制: 基于联盟形成博弈的任务分配. 自动化学报, 2025, **51**(5): 942−959)

4　Chen Mou, Liu Wei, Zhang Peng. Distributed collision avoidance tracking control for quadrotor cooperative suspension system under performance constraints. *Acta Automatica Sinica*, 2024, **50**(12): 2392−2406
(陈谋, 刘伟, 张鹏. 性能约束下的四旋翼无人机协同吊挂系统分布式避碰跟踪控制. 自动化学报, 2024, **50**(12): 2392−2406)

5　Ames A D, Xu X R, Grizzle J W, Tabuada P. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 2017, **62**(8): 3861−3876

6　Rimon E, Koditschek D E. Exact robot navigation using artificial potential functions. *IEEE Transactions on Robotics and Automation*, 1992, **8**(5): 501−518

7　Liu Y Y, Montenbruck J M, Zelazo D, Odelga M, Rajappa S, Bülthoff H H, et al. A distributed control approach to formation balancing and maneuvering of multiple multirotor UAVs. *IEEE Transactions on Robotics*, 2018, **34**(4): 870−882

8　Salzmann T, Kaufmann E, Arrizabalaga J, Pavone M, Scaramuzza D, Ryll M. Real-time neural MPC: Deep learning model predictive control for quadrotors and agile robotic platforms. *IEEE Robotics and Automation Letters*, 2023, **8**(4): 2397−2404

9　Tian E G, Fan M G, Ma L F, Yue D. Stochastic important-data-based attack power allocation against remote state estimation in sensor networks. *IEEE Transactions on Automatic Control*, 2025, **70**(3): 2012−2019

10　Liu G, Tian E, Xie X. Critical-metrics-based attack strategy and

resilient H_∞ state estimator design for multi-area power systems. *IEEE Transactions on Smart Grid*, 2025, **16**(2): 1619−1628

11 Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2013, **58**(11): 2715−2729

12 Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 2014, **59**(6): 1454−1467

13 Hu J, Li J X, Yan H C, Liu H J. Optimized distributed filtering for saturated systems with amplify-and-forward relays over sensor networks: A dynamic event-triggered approach. *IEEE Transactions on Neural Networks and Learning Systems*, 2024, **35**(12): 17742−17753

14 Hu J, Chen W L, Wu Z H, Chen D Y, Yi X J. Design of protocol-based finite-time memory fault detection scheme with circuit system application. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2024, **54**(5): 3110−3123

15 Hu X Y, Ye D. Event-based privacy-consensus control for multiagent systems: An enhanced framework for fault-tolerance and protection against eavesdropping. *Applied Mathematics and Computation*, 2025, **500**: Article No. 129446

16 Wu Z H, Pan S R, Chen F W, Long G D, Zhang C Q, Yu P S. A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2021, **32**(1): 4−24

17 Chen J, Chen S Z, Bai M Y, Pu J, Zhang J P, Gao J B. Graph decoupling attention Markov networks for semisupervised graph node classification. *IEEE Transactions on Neural Networks and Learning Systems*, 2023, **34**(12): 9859−9873

18 Qin J H, Zhang G S, Zheng W X, Kang Y. Neural network-based adaptive consensus control for a class of nonaffine nonlinear multiagent systems with actuator faults. *IEEE Transactions on Neural Networks and Learning Systems*, 2019, **30**(12): 3633−3644

19 Liu Y, Yang G H. Neural learning-based fixed-time consensus tracking control for nonlinear multiagent systems with directed communication networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2021, **32**(2): 639−652

20 Yang X D, Zhang H, Wang Z P. Data-based optimal consensus control for multiagent systems with policy gradient reinforcement learning. *IEEE Transactions on Neural Networks and Learning Systems*, 2022, **33**(8): 3872−3883



董 萍 上海理工大学光电信息与计算机工程学院硕士研究生. 主要研究方向为复杂无人机群关键节点识别与资源受限攻击策略, 网络化控制系统, 非线性随机控制与滤波.
E-mail: dongdp95@gmail.com
(**DONG Ping** Master student at the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology. Her research interests include critical node identification and resource-constrained attack strategies for complex UAV swarms, networked control systems, nonlinear stochastic control and filtering.)



田恩刚 上海理工大学光电信息与计算机工程学院教授. 2002 年获得山东师范大学数学专业学士学位, 2005 年获得南京师范大学运筹学与控制论专业硕士学位, 2008 年获得东华大学控制理论与控制工程专业博士学位. 主要研究方向为网络化控制系统, 非线性随机控制与滤波. 本文通信作者.
E-mail: tianengang@163.com
(**TIAN En-Gang** Professor at the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology. He received his bachelor degree in mathematics from Shandong Normal University in 2002, his master degree in operations research and cybernetics from Nanjing Normal University in 2005, and his Ph.D. degree in control theory and control engineering from Donghua University in 2008. His research interests include networked control systems, nonlinear stochastic control and filtering. Corresponding author of this paper.)