中图分类号：TP393
学科分类号：081200
论文编号：1028716 23-S018

硕士学位论文

面向多跳无人机自组织网络的路由协议研究

研究生姓名　　翟文斌
学科、专业　　计算机科学与技术
研 究 方 向　　无人机网络路由技术
指 导 教 师　　王立松　教授

南京航空航天大学
研究生院　计算机科学与技术学院

二〇二三年三月

Nanjing University of Aeronautics and Astronautics
The Graduate School
College of Computer Science and Technology

Research on Routing Protocol for Multi-hop Unmanned Aerial Vehicle Ad-hoc Networks

A Thesis in

Computer Science and Technology

by

Wenbin Zhai

Advised by

Prof. Lisong Wang

Submitted in Partial Fulfillment

of the Requirements

for the Degree of

Master of Engineering

March, 2023

承诺书

本人声明所呈交的硕士学位论文是本人在导师指导下进行的研究工作及取得的研究成果。除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得南京航空航天大学或其他教育机构的学位或证书而使用过的材料。

本人授权南京航空航天大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本承诺书）

作者签名：翟文斌

日　　期：2023.3.31

摘　要

随着传感器、无线通信等技术的发展，多跳无人机自组织网络已经被广泛应用于军事和民用领域。路由技术是保障无人机网络数据通信、信息共享以及集群协作的基本前提，需要同时兼顾性能与安全。然而，无人机网络的众多独特特性，例如节点高速移动、网络拓扑动态变化、节点稀疏分布等，给路由协议的设计带来了严峻的挑战。本文基于整体跨层优化的思想，研究面向多跳无人机网络的路由技术，取得的主要研究成果如下：

(1) 现有无人机网络路由协议大多仅利用网络协议栈下三层的参数进行路由决策，未利用多维度跨层信息，提出一个面向多跳无人机网络的跨层路由优化框架 HOLO (A Holistic Cross-Layer Routing Optimization Framework for UAV Networks)，将物理、数据链路、网络、传输以及应用等协议层考虑在内，对各个协议层的路由参数、信息以及反馈进行整体的收集、分析和利用，从而达到整体的跨层交互和融合。同时，提出面向优化目标的高效路由决策机制以优化路由，从而达到更好的网络整体性能。

(2) 基于 HOLO 跨层路由优化框架，针对现有路由协议假设无人机的传输功率固定，未考虑联合功率调度和控制进行跨层路由优化的问题，提出一种功率感知的多跳无人机网络路由协议 PAR (A Power-Aware Routing Algorithm for UAV Networks)，综合物理层的功率感知、应用层的 QoS 需求以及预先规划的无人机轨迹信息，对路由决策进行联合跨层优化。PAR 对物理层的功率信息进行自适应调节，并利用预先规划的轨迹信息来计算不同功率级别下无人机之间的相遇情况。基于相遇信息，联合应用层的 QoS 需求，以延迟约束和能耗最小化为优化目标，构建功率感知相遇树，从而找到满足条件的高效传输路径。实验结果表明，与现有算法相比，PAR 能够在保持较高投递率、较低网络负载率的同时节约能耗。

(3) 针对现有无人机网络路由协议未考虑延时攻击的问题，提出一种抗延时攻击的多跳无人机网络安全路由协议。首先提出一个整体跨层的延时攻击检测框架 HOTD (A Holistic Cross-Layer Time-Delay Attack Detection Framework for UAV Networks)。通过对协议栈各层的延迟相关特征进行提取，采用监督学习建立选定特征和转发延迟的一致性模型，并基于训练建立的一致性模型计算出网络中各个节点的一致性程度。然后根据网络节点一致性程度，利用聚类方法来区分恶意节点和良性节点。最后在聚类分类结果的基础上对恶意节点进行路由隔离以保证路由安全。实验结果表明，HOTD 在检测准确率、假阳性率以及假阴性率等方面均优于现有经典的延时攻击检测方法，在引入不到 2.5% 的额外开销的情况下，实现了高于 85% 的检测准确率。另外，本文提出的抗延时攻击安全路由协议能够有效降低延时攻击对无人机网络路由协议性能的

影响。

关键词：无人机网络，路由协议，跨层设计，能耗高效，功率感知，延时攻击，恶意节点检测

ABSTRACT

With the development of technologies such as sensors and wireless communications, Unmanned Aerial Vehicle (UAV) ad-hoc networks have been widely used in military and civilian applications. Routing technology is the basic premise for data communication, information sharing, and cluster collaboration of UAV networks, which needs to take both performance and security into account. However, many unique characteristics of UAV networks, such as high-speed mobility of nodes, high dynamics of network topology, and sparse distribution of nodes, pose severe challenges to the design of routing protocols. In this paper, the routing technology for multi-hop UAV networks is studied from the perspective of holistic cross-layer optimization. The main contributions of this paper are given as follows:

(1) Most of the existing routing protocols for UAV networks only simply use the parameters at the lower three layers for routing decisions, without the utilization of multi-dimensional cross-layer information. Therefore, we propose a holistic cross-layer routing optimization (HOLO) framework for UAV networks, which takes physical, data link, network, transmission, and application layers into consideration. HOLO performs holistic collection, analysis, and utilization of routing parameters, information, and feedback of each protocol layer from a cross-layer perspective, thereby achieving a holistic cross-layer interaction and fusion. Meanwhile, an efficient routing decision-making mechanism is proposed to optimize routing based on the optimization goals, thus achieving better overall network performance.

(2) The existing routing protocols for UAV networks typically assume that the transmission power of UAVs is fixed, the cross-layer joint power scheduling and control are not taken into account for routing optimization. Therefore, based on the HOLO framework, we propose a Power-Aware Routing (PAR) algorithm for UAV networks. PAR combines the power-aware characteristic of the physical layer, the QoS requirements of the application layer, and the pre-planned trajectory information to jointly optimize the routing decision. PAR adaptively adjusts power information at the physical layer, and utilizes the pre-planned trajectory information of UAVs to calculate encounters at different power levels. Based on the encounter information, PAR combines the QoS requirements of the application layer, takes delay constraint and energy consumption minimization as optimization goals, and constructs a power-aware encounter tree to find an efficient transmission path. The experimental results show that compared with the existing algorithms, PAR significantly reduces the energy consumption with a higher delivery ratio and lower network overhead.

(3) The existing routing protocols for UAV networks ignore Time-Delay Attacks (TDAs); to overcome this issue, in this paper, we propose a secure routing protocol against TDAs for UAV networks. First, a holistic cross-layer time-delay attack detection framework (HOTD) is proposed, which performs a holistic extract of the delay-related features available at all layers, before adopting supervised learning to build a consistency model between these selected features and the forwarding delay to calculate the degree of consistency of each node. Then, the clustering method is used to distinguish malicious from benign nodes according to their degree of consistency. Finally, the routing isolation mechanism is performed on malicious nodes to ensure routing security. Experimental results show that the performance of HOTD is superior to that of state-of-the-art detection methods in terms of detection accuracy, false positive rate, and false negative rate, and it achieves a detection accuracy higher than 85% with less than 2.5% additional overhead. Meanwhile, the proposed secure routing protocol can greatly reduce the impact of TDAs on the performance of UAV networks.

Keywords: UAV networks, routing protocol, cross-layer design, energy-efficient, power-aware, time-delay attack, malicious node detection

目　录

图表清单

注释表

G	加权有向图	u_1, u_i, u_j, u_N	无人机
e, e_u, e_n, e_c	有向边（相遇点）	p_1, p_2, p_k, p_L	可调功率级别
T	延迟约束	t	时隙
$E_e(p_k)$	功率 p_k 下传输一跳的能耗	m	消息
e_i	功率 p_1 下的相遇点	c_i	功率 p_2 下的相遇点
pa_i	传输路径	pa_i'	pa_i 的传输子路径
s	源节点	d	目的节点
g_0	地面站	n, u	节点
c, C	孩子节点	$n.t$	n 与其父节点的相遇时间
$c.pa$	从 s 到 c 的传输路径	$E_t(c.pa)$	m 沿着 $c.pa$ 的传输总能耗
PET	功率感知相遇树	PQ	优先级队列
ECM	能耗指标	ET	相遇时间
$u(e_{m+1})$	u 第 $m+1$ 次被添加到 PET	P_{TDA}	节点实施延时攻击的概率
t_i^s	节点 $node_i$ 的消息发送时间	t_{i+1}^r	$node_{i+1}$ 的消息接收时间
t_{trans}	消息一跳的传输时间	τ	延时攻击的持续时间
$t_i^{s\prime}$	经过恶意延迟后 $node_i$ 的消息发送时间	$t_{i+1}^r{}'$	经过恶意延迟后 $node_{i+1}$ 的消息接收时间
$t_{dur(i,i+1)}$	$node_i$ 和 $node_{i+1}$ 相遇持续时间	$t_{ste(i,i+1)}$	$node_i$ 和 $node_{i+1}$ 相遇开始时间
M	传输消息的形式	D	消息 M 的原始有效载荷
Log_i	$node_i$ 的传输日志信息	$RT_i\ (ST_i)$	$node_i$ 接收（发送）M 的时间
$RD_i\ (SD_i)$	$node_i$ 与 $node_{i-1}\ (node_{i+1})$ 之间的距离	$RS_i\ (SS_i)$	$node_i$ 接收（发送）M 时的飞行速度向量
$RB_i\ (SB_i)$	$node_i$ 接收（发送）M 时的缓冲区占用	RL_i	M 被 $node_i$ 接收时的 TTL
		TP_i	$node_i$ 的传输功率
t_{sc}^i	$node_i$ 存储携带 m 的预计持续时间	LQ_i	$node_i$ 的链路质量
		t_{fd}^i	$node_i$ 相对于 m 的转发延迟
$bf_i\ (mf_i)$	$node_i$ 的良性（恶意）转发行为数量	C_i	$node_i$ 的一致性程度
		N	传输消息的数量
H_i	M_i 的总传输跳数	A_i	M_i 中每个节点附加信息大小

缩略词

缩略词	英文全称
UAV	Unmanned Aerial Vehicle
MAV	Manned Aerial Vehicle
UANETs	Unmanned Aerial Vehicle Ad-Hoc Networks
WSNs	Wireless Sensor Networks
MANETs	Mobile Ad-Hoc Networks
QoS	Quality of Service
LOS	Line-Of-Sight
HOLO	A Holistic Cross-Layer Routing Optimization Framework for UAV Networks
PAR	A Power-Aware Routing Algorithm
HOTD	A Holistic Cross-Layer Time-Delay Attack Detection Framework
OLSR	Optimized Link State Routing
RREQ	Route Request
RREP	Route Reply
DSR	Dynamic Source Routing
AODV	Ad hoc On-Demand Distance Vector Routing
MEC	Mobile Edge Computing
RL	Reinforcement Learning
ZRP	Zone Routing Protocol
TORA	Temporally Ordered Routing Algorithm
GPS	Global Positioning System
SCF	Store-Carry-Forward
DTN	Delay Tolerant Network
PSO	Particle Swarm Optimization
ACO	Ant Colony Optimization
GSO	Glowworm Swarm Optimization
KHA	Krill Herd Algorithm
SSO	Social Spider Optimization

MFO	Moth-Flame Optimization
SDN	Software-Defined Networking
MITM	Man-In-The-Middle Attacks
PUF	Physically Unclonable Function
ABE	Attribute-Based Encryption
BLS	Boneh-Lynn-Shacham
SVM	Support Vector Machine
RF	Random Forest
DT	Decision Tree
MLR	Multiple Linear Regression
GRU	Gated Recurrent Unit
DRL	Deep Reinforcement Learning
OSI	Open System Interconnection
RSSI	Received Signal Strength Indicator
SNR	Signal-to-Noise Ratio
SINR	Signal-to-Interference-plus-Noise Ratio
PER	Packet Error Rate
BER	Bit Error Rate
MAC	Media Access Control
LLC	Logical Link Control
ETX	Expected Transmission Count
IMUs	Inertial Measurement Units
PDR	Packet Delivery Ratio
MDP	Markov Decision-making Process
DNN	Deep Neural Network
PET	Power-aware Encounter Tree
ECM	Energy Consumption Metric
ET	Encounter Time
ONE	Opportunistic Network Environment
TDAs	Time-Delay Attacks
TTL	Time To Live

CPSs	Cyber Physical Systems
PTP	Precision Time Protocol
HLSTM	Hierarchical Long Short-Term Memory
TP	True Positive
TN	True Negative
FN	False Negative
FP	False Positive
FPR	False-Positive Rate
FNR	False-Negative Rate
ACC	Accuracy Rate
MLP	MultiLayer Perceptron
RNN	Recurrent Neural Network
AGNES	Agglomerative Nesting Hierarchical Clustering
GMM	Gaussian Mixed Model
EM	Expectation-Maximization

第一章　绪论

1.1　研究背景与意义

无人机，全称为无人驾驶飞行器 (Unmanned Aerial Vehicle, UAV)，是指机上没有任何人类飞行员，通过远程无线电遥控或者嵌入式自主计算程序进行控制和管理的飞行器。无人机的起源可以追溯到 19 世纪 20 年代第一次世界大战期间的“斯佩里空中鱼雷号”，并在之后的第二次世界大战、海湾战争、叙利亚内战、俄乌战争等军事活动中被频繁应用于执行各种任务。近年来，随着传感器、无线通信以及电池储能等技术的快速进步与发展，无人机已经作为空中机器人技术的一种新范式，引起了广泛的关注并被应用到各种军事和民用领域，例如军事侦察、情报收集、高空打击、边境巡逻、灾后搜救、农田监测、物流运输、影视拍摄等[1,2]。与载人飞行器 (Manned Aerial Vehicle, MAV) 相比，无人机，由于具有体积小、机动性高、部署灵活、操作自主、制造成本低、生存能力强、环境要求低等特点和优势[3]，具有巨大的商业价值和应用潜力。根据 Frost&Sullivan 报告，2021 年全球民用无人机市场规模超过 1600 亿人民币，相比于 2015 年的 214 亿人民币，年均复合增长率达到 39.84%，同时预计到 2025 年将突破 5000 亿人民币大关[4]。

传统的无人机系统由单架精密复杂、集成度较高的大型无人机和相关基础地面控制单元组成。这样的无人机可以通过先进的控制策略实现高精度的实时姿态控制，完成某些航行距离远、执行时间长的任务[5]，例如我国研发的翼龙系列无人机，最大航程为 10000 公里以上，最大续航为 40 小时，其既可以精准地完成军事侦查、打击任务，也可应用于各种民用及科学研究领域。民用版翼龙-2H 应急救灾型无人机在四川省地震、河南省特大暴雨等国家重大地质灾害期间对灾情地区执行探测勘查、提供应急通信保障。然而，单无人机系统也有着其固有缺陷：首先，单无人机系统的容错率较低，一旦无人机出现故障或者遭受攻击，任务将直接终止失败；其次，单无人机系统不适用于大规模、较复杂的应用场景，其任务完成效率较低；最后，单无人机系统的建造价格和维护成本很高。

近年来，随着传感器和无线通信技术的进步，以及嵌入式和分布式系统的兴起，多无人机系统引起了人们的关注，并逐渐成为了研究和应用的潮流。在多无人机系统中，大量的中小型无人机通过自组织的方式动态组网，相互协作配合，共同完成任务[6]。相比于由单架大型无人机构成的单无人机系统，由多架中小型无人机组成的多无人机系统具有更多的优势：首先，在多无人机系统执行任务期间，即便单架无人机出现故障被迫终止任务，多无人机系统也可以快速反应、及时调整，从而继续完成任务，故障容忍性和可靠性更高；其次，多架无人机可以并行地执行任务，并且可以相互配合，优势互补，作业效能更高；最后，中小型无人机的制造成

本更低，部署也更为灵活。由于上述优势，多无人机系统已经被广泛应用于各种实际任务场景，但是与单无人机系统相比，多无人机系统中任务的顺利执行和完成更加依赖于无人机集群之间的信息共享、协作与配合[7]。通信作为无人机之间信息共享的关键手段，是多无人机系统实现集群协作的基本前提，更是多无人机系统中的一项严峻挑战。与单无人机系统中无人机只需要与地面站进行通信不同，多无人机系统中无人机之间同样需要进行高效的信息通信，从而实现更高的任务效能。

为了保障无人机间高效可靠的通信，多无人机系统通常通过动态组网的方式构成一个空中多跳无人机自组织网络 (Unmanned Aerial Vehicle Ad-Hoc Networks, UANETs)，本文也简称为无人机网络 (UAV Networks)[8]。无人机网络继承自传统的无线传感器网络 (Wireless Sensor Networks, WSNs) 和移动自组织网络 (Mobile Ad-Hoc Networks, MANETs)，可以视作是两者的一种扩展和新范式。在无人机网络中，无人机作为网络节点，配备了相应的移动通信模块，在具备报文转发能力的同时兼顾了路由寻址功能。因此，无人机网络能够通过多跳无线中继的方式实现无人机之间的数据传输，具有动态性、自治性、临时性、异构性等特点。然而，与传统的无线传感器网络和移动自组织网络相比，无人机网络不仅具有多跳、自组织、无中心等共同特征，还具备其自身特点：

(1) 节点的高速移动性、网络拓扑的高度动态性和通信连接的间断性。这是无人机网络与传统无线传感器网络和移动自组织网络之间最为显著的区别。无人机的飞行速度可以达到 30 ~ 460 km/h，这种高速的移动性会造成网络拓扑的高度动态变化，从而对网络的连通性和通信链路的稳定性造成严重的影响。这给无人机网络中的通信和路由带来了严峻的挑战和独特的设计要求。

(2) 节点的稀疏性和网络的异构性。由于无人机网络覆盖范围较大且无人机移动性较强，无人机节点大多稀疏地分布在空域中，节点密度较低，这会对网络的连通性产生一定的影响。此外，由于不同无人机承载的任务不同，在网络中有着不同的职能定位，无人机之间的类型可能不同，配备着不同的资源。例如，搜寻无人机负责任务的执行，而摆渡无人机则主要负责帮助搜寻无人机之间的消息传递。

(3) 节点移动模型的特殊性。不同于传统的无线传感器网络和移动自组织网络中节点移动的随意性，无人机网络中节点的移动具有规律性和可预测性，可以通过任务规划或者路径规划预先设定，同时在任务执行过程中可以进行动态更新。

由于无人机网络的众多特性，传统的静态网络、无线传感器网络以及移动自组织网络中的路由协议直接应用于无人机网络将面临着诸如低投递率、高延迟、低吞吐量和高能耗等问题。许多国内外的研究学者对无人机网络进行了深入的研究，并提出了许多路由协议来优化无人机网络的性能。然而，当前的研究工作仍然存在着以下不足：

(1) 现有的无人机网络路由协议大多只是传统无线传感器网络和移动自组织网络路由协议

的衍生和变体，它们并没有针对无人机网络的特性进行自适应的调整和优化。与无线传感器网络和移动自组织网络相比，无人机网络的众多独特特性使得其路由协议的设计挑战变得更为严峻，而只是将其他网络的路由协议进行简单的变种就直接应用于无人机网络已经不能满足无人机网络的实际应用需求。目前尚无针对无人机网络特性进行全面优化的无人机网络路由协议。

(2) 现有为无人机网络设计的路由协议大多是基于非跨层的方式，即在路由决策时仅使用网络层或其相邻层中有限的路由参数，而无法利用其他层的路由信息。同时，无人机网络具有丰富的应用场景，有着不同的实际需求和优化目标，而非跨层的方法只适用于特定的应用，不具备一般性。因此，它们无法为高度动态的无人机网络提供足够的性能表现，更无法满足丰富且严格的无人机应用需求和目标。只有以跨层的形式让无人机网络充分贴近应用，同时联合各个协议层的信息进行路由优化，才能实现高效的网络性能。然而，目前的跨层无人机网络路由协议仅针对了协议栈下三层（即物理层、数据链路层和网络层）的跨层联合优化，而忽略了其他层的信息。此外，它们仅对路由信息进行了简单的利用，如加权和中和，其本质上只是一种简单的信息集成。目前尚无全面、深入地利用和融合各个协议层的信息来进行跨层优化设计的无人机网络路由协议。

(3) 除了高效的传输性能要求之外，无人机网络路由协议也有着较高的网络安全要求。近年来，随着无人机网络的广泛应用，其通信网络中的安全漏洞也在被不断地探索，例如外部的主动干扰攻击、内部的黑洞攻击等。除了继承自无线传感器网络和移动自组织网络的安全挑战外，无人机网络也存在着自身的安全挑战并且其特性使得这些安全挑战更为严峻和复杂，因此，需要一种有效的安全机制在尽量不影响路由性能的同时保证无人机网络的安全。

综上所述，传统的无人机网络路由协议缺乏对无人机网络特性的深入分析和优化、跨层设计的全面融合和利用、网络安全的考量和设计，使得本课题的研究具有重要的理论意义和应用价值。

1.2 无人机网络路由协议

1.2.1 无人机网络路由协议设计要求

由于无人机网络的独特特性，无人机网络路由协议的设计要求远远超出了传统的无线传感器网络和移动自组织网络。首先，无人机网络路由协议要能够适应高速移动的节点、频繁变化的网络拓扑以及间断连接的通信链路等特性。其次，无人机网络的路由协议设计需要考虑应用场景、数据流量及其相应的服务质量 (Quality of Service, QoS) 要求。例如，在高空打击、灾后搜救等实时场景中，路由协议必须满足低延迟、低带宽和中等抖动的要求；而在情报收集、地理测绘等延迟容忍场景中，存储转发的数据信息则具有较高延迟、抖动容忍以及高宽带要求的特点；此外，无人机之间以及地面控制站与无人机之间的命令和控制数据流量则必须以低延迟、低带宽、低抖动的方式进行传输。同时，无人机网络路由协议还需要考虑诸如无人机功率限制、

负载均衡、链路质量等因素，以进一步地提高无人机之间通信的可靠性。

除了在无人机之间寻找可靠和高效的路由路径之外，安全需求也是无人机网络路由协议设计需要考虑的重中之重，因为无人机网络传输传感、命令、控制以及路由协议流量等关键信息。目前，无人机网络已经被广泛应用到各种军用和民用领域，各种攻击引发的数据泄露可能会危及商业、公共乃至国家安全。无人机网络在继承了很多传统无线传感器网络和移动自组织网络的安全挑战的同时，也具备其自身独特的安全挑战，例如由于高视距 (Line-Of-Sight, LOS) 的链路属性，无人机网络更容易受到主动干扰攻击 (Active Interfering Attacks)。同时，其自身的独特特性以及设计约束也使得无人机网络安全路由协议的设计变得更有挑战性，例如，无人机网络中节点的高速移动性和稀疏分布性使得路由协议很难将由网络拓扑的高度变化和节点通信的间断连接导致的链路故障与由拜占庭节点的恶意活动引起的传输失败区分开。此外，由于在成本和部署效能上的考虑，无人机节点资源受限，因此很难将精密复杂和资源密集型的安全方案部署到无人机上，例如通信加密和身份验证机制。综上所述，无人机网络安全路由协议的设计与优化必须充分考虑无人机的移动特征、能量约束、计算能力以及延迟要求等特性。

1.2.2 无人机网络路由协议技术

现有面向多跳无人机自组织网络的路由协议技术根据优化目标的不同可分为无人机网络高效路由协议和无人机网络安全路由协议。高效是无人机网络路由协议的设计初衷和首要目标，同时随着安全漏洞和攻击平面不断地被探索，安全也是路由协议需要考虑的重中之重，因此本节分别从高效和安全两个角度对无人机网络路由协议技术进行介绍。

(1) 无人机网络高效路由协议

现有无人机网络高效路由协议根据路由策略的不同可分为基于网络拓扑的路由协议、基于地理位置的路由协议以及仿生路由协议。

基于网络拓扑的高效路由协议利用无人机网络当前的全局拓扑信息来指导数据传输，需要在数据传输之前获取到数据完整的路由路径，根据获取方式的不同可进一步划分为主动式的基于网络拓扑的高效路由协议[9–12]和反应式的基于网络拓扑的高效路由协议[13–16]。主动式的高效路由协议需要无人机网络中的节点各自维护一张路由表，其中存储着通往网络中其他所有节点的路由路径，在数据传输时只需对路由表进行查询，然后沿着路由表中的路由路径进行传输即可。同时，为了维护路由表中信息的可用性，节点需要周期性的进行控制交互以对其中的信息进行更新。由于无人机网络的高度动态性，主动式的高效路由协议会产生巨大的控制开销、导致较重的网络负载。而反应式的高效路由协议无需维护路由表，而是在消息传输之前执行路由发现过程，寻找数据相应的路由路径，这大大降低了网络的控制开销和额外负载，但同时也引入了不小的传输延迟。此外，由于无人机网络节点的高速移动性，即便是当前建立的通信链路也极有可能失效。

基于地理位置的路由协议[17–20]不再依赖于网络的全局拓扑信息，而是利用当前节点和邻居节点的位置信息进行路由决策，基本思想是选择离目的地最近的邻居节点进行路由转发。与基于网络拓扑的路由协议不同，基于地理位置的路由协议无需维护无人机网络的全局拓扑信息，控制开销较低，但是由于它采用贪婪转发的路由策略，在无人机网络的实际应用场景中仍然不可避免地会陷入局部最优。

仿生路由协议[21–24]利用基于生物群体智能的优化算法来解决无人机网络的路由性能优化问题，通过对鸟群、蜂群、蚁群等的研究、模拟和利用来优化路由决策，可以在投递率和延迟方面能达到较好的性能。但是仿生路由的任务空间过大导致协议初期收敛速度过慢，并且其适用于节点密度较高且分布均匀的无线网络，而高度动态和稀疏分布的无人机网络不利于发挥其全局探索和寻优能力，从而导致路由协议优化效率和性能表现的降低。

(2) 无人机网络安全路由协议

根据策略机制的不同，无人机网络安全路由协议可细分为基于身份验证和通信加密的安全路由协议以及基于信誉评估和恶意节点检测的安全路由协议。

基于身份验证和通信加密的安全路由协议[25–28]利用密码学知识对节点的身份进行验证，对节点之间的通信信道进行加密保护，以提供对数据的保密性、完整性和隐私性保护。但是此类协议需要消耗大量的计算、通信、能量以及存储资源，这对于资源受限的无人机网络来说是不可承受的代价。此外，它还存在着密钥被攻破的风险，一旦存在无人机被攻击者恶意物理捕获并攻破其密钥系统，攻击者将能够掌握网络中的所有数据传输，整个无人机网络将会集体失能和瘫痪。同时，此类协议属于被动防御，无法识别出网络中的恶意攻击，更无法对攻击者进行精确的定位。更甚的是，它无法抵御诸如延时攻击、重播攻击、泛洪攻击等无需对密码体制进行破译就可以实施的内部攻击。

基于信誉评估和恶意节点检测的安全路由协议[29–32]通过对网络运行状况以及节点行为的观察利用数学模型或机器学习模型计算出节点的信誉值，并以此为依据将节点区分为良性和恶意节点，然后在判别结果的基础上，实施诸如路由隔离等策略来保障无人机网络的路由安全。但是数学模型需要对问题的输入、输出以及两者之间的映射关系进行精确的定义，这对于高度复杂、动态和不确定的无人机网络来说是非常困难甚至是完全不可行的。并且，由于无人机网络的状态和解空间过大，数学模型无法对其中复杂的映射关系进行精确的拟合和求解。另一方面，现有的机器学习模型中特征选择多种多样且随意性较大，没有统一的架构和标准来对特征进行抉择，同时方法仅针对特定的应用场景，不具备一般性。

1.3 主要研究内容

本文在对无人机网络及其特性进行全面深入的分析研究之后，主要针对面向多跳无人机自组织网络的路由协议进行深入的研究，具体内容如下：

(1) 针对现有无人机网络路由协议或基于非跨层方式或仅简单跨层利用协议栈下三层参数进行路由设计而导致的性能不足和应用特异性等问题，提出了一个面向多跳无人机网络的整体跨层路由优化框架 HOLO (A Holistic Cross-Layer Routing Optimization Framework for UAV Networks)。针对无人机网络的特性，HOLO 从三维的角度对无人机网络的协议体系结构及其功能进行了深入的分析。同时，HOLO 采用跨层设计，对各个协议层的路由参数、信息以及反馈进行整体的收集、分析和利用，从而达到整体的跨层交互和融合。此外，根据优化目标的类型，HOLO 采用不同的高效路由决策机制来优化路由，从而达到更好的网络整体性能。

(2) 现有的无人机网络路由协议大多基于无人机功率固定的假设进行路由优化，而没有考虑无人机的功率感知特性，即无人机的功率是可调节的。此外，它们大多依赖于路由表的建立或大量拓扑消息的转发来感知网络拓扑，而没有考虑无人机网络中节点移动模型的特殊性，即无人机的轨迹通常是预先规划好的。因此，基于 HOLO 跨层路由优化框架，本文提出了一种高效的功率感知的多跳无人机网络路由协议 PAR (A Power-Aware Routing Algorithm for UAV Networks)。PAR 联合物理层的功率感知、应用层的 QoS 需求以及预先规划的无人机轨迹信息来对网络层的路由决策进行联合跨层优化。PAR 对物理层的功率信息进行跨层感知和调整，同时利用预先规划的轨迹信息来感知网络未来拓扑，并计算在不同功率下无人机之间的相遇情况。然后，基于应用层的 QoS 感知，以延迟约束和能耗最小化为优化目标，构建出功率感知相遇树，从而找到满足条件的高效传输路径。最后，本文对 PAR 的最优性进行了理论证明，同时仿真实验结果表明 PAR 在保证消息被及时成功投递的同时显著降低了传输能耗和网络负载。

(3) 针对无人机网络目前尚无检测和抵抗延时攻击研究的问题，提出了一个抗延时攻击的多跳无人机网络安全路由协议。延时攻击能够以极小的代价对无人机网络产生相当大的影响，而现有的延时攻击检测研究集中于静态网络。因此基于 HOLO 跨层路由优化框架，首先提出了一个整体的跨层延时攻击检测框架 HOTD (A Holistic Cross-Layer Time-Delay Attack Detection Framework for UAV Networks)。HOTD 从跨层的角度对无人机网络协议栈的所有层（即物理层、数据链路层、网络层和应用层）中可用的延迟相关的特征进行整体的选择。然后利用监督学习在这些选择的特征与相应的数据转发延迟之间构建一致性模型，并在此模型的基础上计算出网络中各个节点的一致性程度。接着，根据节点的一致性程度，采用聚类方法将节点区分为恶意节点和良性节点。最后，一个抗延时攻击的多跳无人机网络安全路由协议被提出，对恶意节点进行路由隔离，以保证网络路由的高效和安全。HOTD 能够在引入低于 2.5% 网络额外负载的同时达到高于 85% 的检测准确率，同时抗延时攻击的安全路由协议可以极大地降低延时攻击对无人机网络数据传输的投递率、延迟以及网络负载的影响。

1.4 论文组织结构

第一章论述面向多跳无人机自组织网络的路由协议研究的重要性和必要性，说明本课题的研究背景和意义，阐述多跳无人机网络路由协议技术及其设计要求，给出本文的主要研究内容和文章组织结构。

第二章对多跳无人机自组织网络环境下的高效路由协议和安全路由协议进行总结、分类和介绍，探讨现有工作已经取得的研究成果以及其不足之处。

第三章研究多跳无人机网络环境下跨层路由优化方法。在对无人机网络体系结构进行深入分析理解后，提出一个面向多跳无人机网络的整体跨层路由优化框架，分别给出路由信息收集的途径以及路由参数交互和信息融合的方式，并根据优化目标的类型采用不同的高效路由决策机制。

第四章研究功率感知的多跳无人机网络路由协议，该协议充分利用物理层的功率可调特性、应用层的 QoS 需求以及预先规划的轨迹信息来寻找高效的路由传输路径。首先给出网络模型并将问题形式化，然后构建功率感知相遇树并对其进行剪枝优化和最优性证明，最后通过实验分析验证算法的有效性。

第五章研究多跳无人机网络环境下延时攻击的检测方法和安全路由机制的设计。首先对网络模型和延时攻击模型等系统模型进行了建模，论证延时攻击在多跳无人机网络中的特异性和危害性。然后设计一个整体跨层的延时攻击检测框架，并详细介绍其工作流程。接着提出一种抗延时攻击的安全路由协议，构建安全路由机制。最后，分别设计实验验证检测框架和路由协议的有效性。

第六章对本文的主要工作成果和研究贡献进行总结，同时说明其不足之处并进一步探讨未来的研究方向。

第二章　相关工作

面向多跳无人机自组织网络的路由协议的研究目标主要集中于高效和安全两方面，根据优化目标的不同可分为无人机网络高效路由协议和无人机网络安全路由协议。高效是路由协议的设计初衷和首要目标；同时，随着无人机网络攻击平面的不断发展和披露，安全也是无人机网络路由协议需要考虑的重中之重。本章分别对无人机网络高效和安全路由协议进行介绍，并对相关技术进行分类和分析。

2.1　无人机网络高效路由协议

由于无人机网络的众多特性，传统的无线传感器网络和移动自组织网络路由协议并不适用于无人机网络，因此研究学者在对一些传统的路由协议进行改进的同时也提出了一些较新的专用于无人机网络的路由协议。本节根据路由策略的不同将现有的无人机网络高效路由协议分为四大类：基于网络拓扑的路由协议、基于地理位置的路由协议、混合路由协议（基于网络拓扑和地理位置的路由协议的结合）以及仿生路由协议；同时对每一类协议的原始作品、后续研究、最新进展以及它们的优缺点分别进行了探讨。

2.1.1　基于网络拓扑的路由协议

基于网络拓扑的路由协议依赖于对无人机网络全局拓扑信息的发现、维护和利用，在数据传输之前需要获取到数据完整的路由传输路径。根据路由发现和路由维护策略的不同，现有的基于网络拓扑的无人机网络高效路由协议可进一步细分为主动路由协议、反应式路由协议以及主动和反应式混合的路由协议。

2.1.1.1　主动路由协议

主动路由协议 (Proactive Routing Protocols) 也称为表驱动路由协议，在此类协议中，网络中的每个节点都需要维护一张路由表，其中存储着通往网络中其他所有节点的路由信息；同时节点之间定期交换消息以维护和更新路由表中的信息。节点根据本地存储的路由表中的信息提前获取路由路径，从而进行消息路由，无需其他操作。最有代表性的主动路由协议为 OLSR (Optimized Link State Routing) 路由协议[33]，通过定期广播控制消息与邻居节点交互拓扑信息，进而感知整个网络拓扑。为了进一步优化协议的性能，在 OLSR 协议的基础上已经提出了许多变种和优化的主动路由协议。

Zhang 等人[9] 提出了一种基于定向天线多波束扫描的新邻居发现机制，结合功率控制和多波束扫描避免了广播消息的泛洪、减小了邻居发现的时间；同时使用基于社交网络的中继选择

方案对 OLSR 协议进行了扩展，通过分析节点的重要性程度来帮助路由决策。Kadadha 等人[10]将区块链 (Blockchain) 技术与 OLSR 协议相结合，通过智能合约为节点的信誉提供了透明、可信的验证方式，以鼓励节点之间的相互合作；此外，一个改进的支持区块链的 Stackelberg 博弈模型被应用于选择合适稳定的中继节点，提高了路由协议的成本效益。Jain 等人[11] 在 OLSR 协议的基础上进一步考虑了 QoS 参数，在进行路由决策时综合考虑网络吞吐量、端到端延迟、数据包的能耗成本以及每个节点的剩余能量。Kanagasundaram 等人[12] 则是在选择中继节点时综合考虑了节点的缓冲区占用、剩余能量、功率级别、转发成功率等因素，以便以更低的能耗进行邻居发现、中继选择以及数据传输。

然而，无人机网络中节点的高速移动性以及网络拓扑的高度动态性会导致路由表中的路由信息快速的过时失效，而频繁的拓扑感知又会占用大量的能量和带宽资源，从而导致这类协议在无人机网络中效率低下甚至是不可用[34]。

2.1.1.2 反应式路由协议

反应式路由协议 (Reactive Routing Protocols) 无需维护路由表，而是在需要传输数据前执行路由发现过程，因此又称为按需路由协议。源节点和目的节点通过广播路由请求 (Route Request, RREQ) 和路由回复消息 (Route Reply, RREP) 的方式建立通信路由路径，从而执行消息路由与传输。最具代表性的反应式路由协议为 DSR (Dynamic Source Routing) 和 AODV (Ad hoc On-Demand Distance Vector Routing) 路由协议，其变体被应用于无人机网络中[35]。

Anamalamudi 等人[13] 利用定向天线来调节混合信道控制，同时基于同步认知协调、异步分布式协调以及定向的端到端的路由发现来优化认知 AODV 协议，从而减小传输能耗、增加网络吞吐量。Zhang 等人[14] 将移动边缘计算 (Mobile Edge Computing, MEC) 部署到无线网络中，基于聚类算法对节点进行分类并采用不同的通信模式；同时在综合考虑节点移动速度、能量消耗以及链路质量的基础上利用强化学习 (Reinforcement Learning, RL) 优化 AODV 协议及其中间节点的选择，减小了端到端延迟和拓扑控制开销。Gankhuyag 等人[15] 在 AODV 协议的基础上考虑了无人机网络的特性，在路由发现时考虑无人机节点的风险信息和效用函数并将其添加到数据包中，其中风险信息由无人机的大小、任务、操作要求、导航位置以及剩余能量等特定参数组成，效用函数则考虑了链路预期连接时间、节点故障概率以及跳数；同时采用动态角度调整技术以及定向天线优化传输范围和链路。Liang 等人[16] 在 DSR 协议的基础上引入了路径可靠性过滤和链路监控修复机制，在数据传输前计算每条传输路径的可靠性权重并选择可靠性较高的路径，在数据传输的过程中对链路状态进行监控并通过其邻居节点对断链进行及时修复。

与主动路由相比，反应式路由中节点无需更新和维护路由表，这降低了网络的控制开销和存储开销，但同时反应式路由协议的路由发现过程给消息传递引入了不小的延迟，此外，无人机网络的高度动态性会导致路由发现过程中的传输路径过时失效，从而频繁触发相应的路由维

护机制，这同样会消耗大量的带宽和能量资源。

2.1.1.3 混合路由协议

混合路由协议 (Hybrid Routing Protocols) 是主动路由和反应式路由的结合体，目的是希望通过对两者特性的融合和权衡以解决主动路由协议中控制消息的高开销和反应式路由协议中路由发现的高延迟问题。混合路由协议的基本思想是将无人机网络划分为多个簇群或者组别，簇内通信使用主动路由协议，簇间通信使用反应式路由协议。典型的混合路由协议为 ZRP (Zone Routing Protocol) 和 TORA (Temporally Ordered Routing Algorithm) 路由协议[36]。

针对 ZRP 路由协议中节点路由区域存在大量重叠，产生大量冗余和重复路由请求的问题，Zhang 等人[37] 设计了一种分层的 ZRP 路由协议，根据网络中节点的剩余能量、传输功率、剩余频带、转换频率对节点进行分层，层内使用主动路由，层间使用反应式路由，从而减小了控制开销。Kumar 等人[38] 不再对节点进行区域划分，网络中每个节点通过控制消息维护自身两跳以内的邻居节点，当目的地不在其邻居列表内时才启动路由请求机制执行路由发现。Malwe 等人[39] 在 ZRP 路由协议的基础上对路由发现机制进行了限制，提出了选择性的边界广播机制，根据节点的连通性和网络密度选择特定的边界节点进行路由请求；同时，利用目的地先前的位置信息来优化路由发现机制，减小控制开销。Li 等人[40] 在 AODV 路由协议的基础上引入了主动路由机制，结合节点位置信息、移动预测、链路质量以及安全性提出了一个链路稳定性度量；基于此度量，在路由发现的过程中维护多条不相交的较为稳健的传输路径，当链路断开时可以以较低的延迟切换到下一条较为可靠的路由路径。

2.1.2 基于地理位置的路由协议

基于网络拓扑的路由协议由于路由发现和邻居维护等机制的存在，在带宽、能量、存储以及可扩展性方面表现不佳；相反，基于地理位置的路由协议利用本地的位置信息而不是全局的拓扑信息来进行数据路由，从而有效缓解了额外开销的问题。此类路由协议基于无人机本地配备全球定位系统 (Global Positioning System, GPS)，能够实时掌握自身位置的基本假设，在进行路由决策时只需知道邻居节点和目的节点的位置信息即可；其最基本的思想是基于贪婪转发机制将数据包传递给距离目的节点最近的邻居节点，根据路由过程中是否采用存储-携带-转发 (Store-Carry-Forward, SCF) 机制，基于地理位置的路由协议可进一步地划分为 DTN (Delay Tolerant Network) 路由协议以及非 DTN 路由协议。

2.1.2.1 非 DTN 路由协议

基于地理位置的非 DTN 路由协议简单地采用贪婪转发机制进行消息路由，将消息直接转发给距离目的节点最近的邻居节点。Huang 等人[17] 基于地理位置、剩余能量以及能量消耗等信

息做出自适应的路由决策以降低路由能耗，同时动态建立两条不相交的路由路径以便更好地从路由空洞中执行路由恢复，并实现负载均衡。Choi 等人[18] 对节点的前进方向、移动速度、链路质量进行预测，并与位置信息相结合，采用贪婪转发机制来寻找下一跳邻居节点。Huang 等人[19] 根据节点的能耗和位置信息构建出了能量感知多播树来指导消息的多播传输，能够自适应地选择最接近能量最优中继位置的节点作为下一跳转发节点以实现数据传输的节能高效；同时采用无信标握手机制来降低开销，使用右手法则来绕过路由空洞。

但是基于地理位置的非 DTN 路由协议的贪婪转发机制在除了节点本身之外没有其他更为接近目的地的预期节点的情况下会失效；在节点稀疏分布和通信间歇连接的无人机网络中，这种情况非常常见，因此此类协议不足以应对高度动态的无人机网络。

2.1.2.2 DTN 路由协议

为了应对上述挑战与不足，DTN 路由协议采用存储-携带-转发机制来对路由协议进行优化：当节点当前的通信范围内不存在适合的数据转发节点时，允许节点在一个预定义的时间范围内存储携带该数据包，直到通信范围内出现满足条件的预期转发节点或者到达最大持有时间阈值。因此，此类协议相比于非 DTN 路由协议而言能够更好地适应节点稀疏分布和高速移动的无人机网络。

Liu 等人[20] 考虑了一个较为新颖的无人机应用场景，其中无人机网络覆盖区域可以被建模为由若干个矩形组成的带状区域，例如管道、河流、长城。传统的地理位置路由协议没有考虑传输方向，在此类场景下可能会完全失效，沿着相反方向传输，因此其在地理位置的基础上进一步考虑数据包的传输方向，对网络进行切分，提高网络的路由效率。Arafat 等人[41] 利用 Guess-Markov 模型来预测无人机网络中节点的未来位置，并且引入了摆渡无人机来辅助消息路由，节点转发首次执行贪婪转发机制，在第一次尝试失败后采用 DTN 机制进行容忍，并在第二次失败后将消息传输给距离最远的邻居节点。Fu 等人[42] 同时考虑了节点的发射和接收能量，并将时间离散化，通过对节点位置的预测，将最小能耗路由问题转换为组合优化问题，并将其建模为等效的有向斯坦纳树问题；对斯坦纳树问题的求解可以被再次映射回相应的传输方案。Rahimi 等人[43] 应用模糊逻辑 (Fuzzy Logic) 在综合考量邻居节点的数量、方向、速度以及到目的地的距离的基础上为每个邻居节点计算出一个机会值，在进行基于 DTN 机制的贪婪转发时选择机会值最大的节点，从而缓解局部最优问题。Asadpour 等人[44] 在无人机位置信息的基础上额外考虑了对无人机未来一段时间内位置和轨迹的预测以及无人机的负载情况，同时考虑了真实链路和预测链路的吞吐量和持续时间，以优化路由决策。

存储-携带-转发机制的引入使得基于地理位置的路由协议性能有所提升，但是由于无人机网络的高度动态性，此类协议在实际应用场景中仍然不可避免地会陷入局部最优。

2.1.3 混合路由协议

基于网络拓扑的路由协议需要在路由传输开始之前获取全部的路由信息及路径，这会引入额外的控制开销；而基于地理位置的路由协议采用贪婪转发机制，不需要额外负载的同时却容易陷入局部最优。因此，混合路由协议对两者的特性进行结合，力求能达到路由协议开销和性能的权衡。

Mahmood 等人[45] 针对传统基于地理位置的路由协议中的路由空洞问题，结合按需路由协议，提出了一种混合按需贪婪路由协议，采用简单的贪婪和回溯策略进行路由转发：在路由建立期间采用贪婪策略进行路由请求传播，同时在遇到路由空洞时使用简单的回溯方法来绕过空洞，避免了平面化网络图的构建，减小了控制开销和延迟。Almesaeed 等人[46] 结合了反应式路由和基于地理位置的路由协议，首先根据源节点和目的节点的位置将两者之间的区域划分为若干个扇形，然后在各个扇形内执行路由发现过程，只有在定向扇形区域内的节点才能参与路由发现，减少了消息的泛洪，最后根据节点的位置、剩余能量以及接收功率选择合适的中继节点进行数据转发。Arianmehr 等人[47] 基于节点的移动速度、链路持续时间、到目的节点的距离以及附近节点的密度为网络中的每个节点计算优先级，在消息转发时，如果邻居节点的优先级高于当前节点，则使用基于地理位置的路由策略，否则使用反应式路由协议。Yang 等人[48] 将无人机网络抽象为虚拟拓扑并通过异步事件驱动机制来进行拓扑维护，从而将无人机网络中的路由决策问题形式化为加权距离最小化问题，无人机域内通信采用虚拟拓扑转发与地理位置转发相结合的无环路由策略来提高通信效率，同时域间通信利用反应式路由执行路由发现过程。

现有混合路由协议对邻居节点的维护依旧依赖于控制消息的转发，对节点移动性的容忍性较差，在节点高速移动和拓扑高度变化的无人机网络中需要频繁地对邻居表进行维护，控制开销较大。

2.1.4 仿生路由协议

受鸟群、蜂群、蚁群、植物群等生物系统集体协作或遗传进化等过程启发的基于群体智能的优化算法，例如粒子群优化算法 (Particle Swarm Optimization, PSO)、蚁群算法 (Ant Colony Optimization, ACO) 等，由于其解决复杂优化问题的能力，已经被广泛应用于无人机网络中的路由优化，这类协议被统称为仿生路由协议 (Bio-Inspired Routing Protocols)。

Arafat 等人[21] 提出了一种基于 PSO 的无人机网络路由协议，基于对目标无人机节点位置的估计使用边界框和 PSO 方法对有限边界的参数空间进行搜索，同时基于节点适应度函数进行聚类，适应度函数由估计距离、能量消耗以及地理位置组成。Khan 等人[22] 结合了萤火虫群优化算法 (Glowworm Swarm Optimization, GSO) 和磷虾群算法 (Krill Herd Algorithm, KHA) 对路由协议进行优化，基于无人机的荧光素水平以及剩余能量使用 GSO 对无人机集群进行分簇，簇间

使用 KHA 进行集群管理，进一步减小能耗，提高通信效率。Azzoug 等人[23] 利用社交蜘蛛优化算法 (Social Spider Optimization, SSO) 来选择中继节点，根据通信模式的不同采用全局或局部搜索，其中全局搜索基于对节点的相遇概率、相遇时间、连通性等历史信息的分析，而局部搜索则依赖于节点的移动性、位置距离等状态参数。Khan 等人[24] 提出了一个基于飞蛾扑火优化算法 (Moth-Flame Optimization, MFO) 的路由协议，由簇头选择、簇群形成、簇群管理、簇群维护、簇头重新选择这五大步骤组成，在对簇群进行维护的同时对网络拓扑进行有效的管理，进而使用路由识别功能执行消息传输的路由选择。

仿生路由协议在投递率和延迟方面达到了较好的性能，但是却加重了无人机网络的能耗和网络负载。同时，仿生路由的全局任务空间很大，在高度动态复杂且不确定的无人机网络环境中，其求解决策速度过慢，且容易陷入到局部最优，降低了路由协议的优化效率和性能表现。此外，仿生路由依赖于生物群智能优化算法，适用于节点密度较高且分布均匀的无线网络，而高度动态和稀疏分布的无人机网络不利于发挥其全局探索和寻优能力。

2.2 无人机网络安全路由协议

对于多跳无人机网络而言，路由协议的设计初衷和首要目标是提高网络效率的同时减少不必要的能耗，从而提高网络中数据传输的性能。针对不同的应用需求，包括上述路由协议在内的高效路由协议不断地涌现，并且在效率和节能等方面都呈现出逐渐完善的趋势。但是，随着无人机网络的广泛应用，其在安全方面考虑不足的问题也逐渐暴露出来[49]。由于无人机网络的分布式、开放式特性，以及节点的移动性、环境的复杂性，使得无人机很容易受到敌方的捕获、拆解和修改，并且冒充成合法节点进行恶意的内部攻击，对网络产生巨大威胁[50]。相比于由未经许可的外部无人机实施的外部攻击相比，由内部恶意无人机发起的恶意网络攻击更加难以识别和检测，给无人机网络及其路由安全带来了巨大的隐患。

无人机网络中的路由安全一经提出就引起了学者的广泛关注；安全路由[51] 应运而生，其目的就是在保证无人机网络性能表现的同时对传输数据的安全性进行检查、维护和保证。然而，无人机网络中节点的计算、能量、通信以及存储等资源受限给安全路由的设计带来了严峻的挑战。如何在满足能量消耗尽可能小、运行成本尽可能低的前提下设计出能够保证网络安全运行的路由协议成为了无人机网络安全路由协议设计的一个严峻挑战和重要目标。

2.2.1 基于身份验证和通信加密的安全路由协议

基于身份验证和通信加密的无人机网络安全路由协议源自传统的计算机网络，因此，为了解决无人机网络的安全问题，针对无人机网络中的密钥管理以及数据的保密性、完整性和隐私性保护，首先提出了基于传统的密码学的方法，例如基于对称加密[52]、非对称加密[53]、身份加密[54] 等的安全方案。但是，无人机网络作为传统无线传感器网络和移动自组织网络的新范式，

在继承了来自两者的安全威胁的同时，也具备其自身特有的安全威胁。与传统的计算机具备强大的资源不同，无人机的计算、能量、存储和通信资源都十分受限，而数据的数字签名以及加密解密需要较为强大的计算能力并且会消耗大量的能量，同时加密后的数据尺寸会变大，需要更多的存储空间以及通信资源来对其进行传输，这对于无人机网络来说都是不可承受的代价。因此，研究学者对无人机网络中的身份验证和加密技术进行了深入的研究[55]，致力于轻量级和低成本的目标，同时结合一些新的技术来优化方案，例如软件定义网络 (Software-Defined Networking, SDN)[56]、区块链[57]、移动边缘计算[58]、雾计算 (Fog Computing)[59] 等。

2.2.1.1 身份验证

身份验证是对网络中的合法用户和设备进行识别并授权的过程，其禁止非法和非授权用户和设备进行任何越权访问和操作。身份验证可以减轻和防御无人机网络内部的一些网络攻击，例如中间人攻击 (Man-In-The-Middle Attacks, MITM)、女巫攻击 (Sybil Attacks)。就目前而言，身份验证是无人机网络安全中最受欢迎、最主流的方法。Wazid 等人[25] 提出了一种轻量级的用户身份验证和密钥协商方案，使用单项散列哈希函数和按位异或运算来减小计算开销，并且在用户验证阶段使用模糊提取器强化无人机身份验证。在此工作的基础上，Deebak 等人[60] 进一步优化了身份验证方案，利用切比雪夫混沌映射将无人机之间的相互验证规约到一个预定义的时间范围内，同时采用身份令牌技术提供有效的验证时间段以及持续的身份验证，并且通过密钥交换来降低对称加密和解密函数的计算成本，从而降低设备的能耗。Tian 等人[61] 利用移动边缘计算技术优化身份验证和隐私保护，无人机的数字签名由离线和在线两阶段组成，无人机自身控制密钥的生成和管理，不涉及任何密钥托管操作，同时基于移动边缘计算设计了快速的模块化算术运算，降低了数字签名生成、验证以及密钥生成、管理的成本。Srinivas 等人[62] 提出了一种基于临时时间凭证的匿名身份验证方案，临时时间凭证由无人机设备凭证、用户密码以及生物识别技术三部分组成，保障了数据的安全性和完整性。

上述方案均宣称实现了轻量级和低成本的优化目标，但是它们在无人机网络中仍然存在着固有缺陷，即密钥被攻破的风险：密钥存储在无人机本地，并且无人机网络共用同一套密钥系统。一旦存在无人机被攻击者恶意物理捕获并攻破其密钥系统，攻击者将能够掌握网络中的所有数据传输，整个无人机网络将会集体失能和瘫痪。为了解决上述方案，近年来提出了基于物理不可克隆函数 (Physically Unclonable Function, PUF) 芯片的身份验证方案[63]，其不依赖于密码学知识，而是采用硬件安全的方式。PUF 不在无人机的物理内存中存储任何密钥，而是基于质询-响应的方式根据身份验证的需求动态生成密钥，具有随机性和不可预测性，增加了无人机网络的安全性。Alladi 等人[26] 提出了一种基于 SDN 的无人机网络的两阶段相互验证协议，SDN 将无人机网络划分为三层，即地面站、领航无人机和集群无人机，在此基础上验证协议由领航无人机和地面站之间的相互验证以及集群无人机和领航无人机之间的身份验证组成，每一次身

份验证都会利用嵌入在无人机内部的 PUF 芯片生成唯一的会话密钥，同时无需将密钥存储在无人机的物理内存中。Bansal 等人[27] 使用 PUF 进行动态验证，并且使用基于生成树的遍历方法来支持无人机网络的动态拓扑和多跳通信，一次可以验证多个设备，从而实现了高可扩展性，显著降低了身份验证的通信成本。Tian 等人[64] 研究了跨域身份验证，即支持不同域中的无人机与多个地面站之间的相互验证和安全通信，在发起和完成身份验证时采用一次性的假名和掩码来保护无人机的真实身份，同时结合可重复使用的模糊提取器从嘈杂的 PUF 中提取出唯一的密钥。然而，上述方案大多基于无人机与 PUF 之间的通信是安全的以及 PUF 是不可篡改的这两个假设，而这在完全开放和动态的无人机网络中是无法保证的。同时，无人机网络中数据交互十分频繁，对每一次的通信都进行 PUF 验证会引入不小的延迟并且消耗一定的能量，这会导致路由协议性能的降低，与无人机网络路由协议的效率和节能的设计初衷相违背。

2.2.1.2 通信加密

除了身份验证之外，无人机网络还需要支持高效可靠的通信，在组内通信时应该对消息使用密钥加密后再进行传输，避免明文传输，防止窃听者侵入无人机网络，非法获取相关数据。目前无人机网络中加密机制的研究主要集中在资源受限无人机的轻量级和低成本加密上。He 等人[65] 聚焦于无人机网络的公共安全服务场景中的 Wi-Fi 攻击和 GPS 欺骗攻击 (GPS Spoofing Attacks)，为了支持细粒度的访问，使用基于属性的加密算法 (Attribute-Based Encryption, ABE) 进行密钥管理，同时使用同态加密 (Homomorphic Encryption) 进行数据聚合，在无需解密数据的前提下减少了数据传输所需的带宽和通信资源。García-Magariño 等人[66] 为了抵抗中间人攻击提出了一种基于区块链的方案来证实网络中各种来源的事件消息，同时基于可信机构签发的无人机预共享列表，使用非对称加密算法来完成无人机签名的验证以及消息的加解密。Ge 等人[67] 对区块链技术进行了改进，重新设计了其构成，并利用迪菲-赫尔曼密钥交换 (Diffie–Hellman Key Exchange) 算法进行共享密钥的生成和分发，在减小计算和存储开销的同时能够低抵御女巫攻击、DDos 攻击以及 GPS 欺骗攻击。Li 等人[68] 设计了一种基于 SM4 的轻量级对称加密算法以及相关的密钥协商和更新机制来保证无人机网络中通信内容的机密性，同时还引入了改进的聚合 BLS (Boneh-Lynn-Shacham) 签名方案和哈希树以保证消息在传输过程中的完整性和真实性。Xiao 等人[69] 提出了一个无人机集群监控系统，一方面使用可信计算和 RSA 非对称加密算法实现网络中的身份验证、密钥分发和数据传输；另一方面利用区块链技术对身份注册、任务分配、数据传输、资源访问和节点管理等各个环节进行验证，保证无人机网络的可用性。

但是，在实际的无人机网络应用中基于通信加密的方案仍然存在着以下不足：(1) 无法识别和定位恶意攻击者：基于密钥管理和通信加密的无人机网络安全路由协议属于被动防御机制，它无法识别出网络中是否存在恶意攻击者，更无法对恶意攻击者进行精确的定位。一旦发生了恶意行为，只能对无人机网络进行整体更换，灵活性和容忍性较差；(2) 无法抵御所有内部攻击：

无人机网络面临着各种各样的内部攻击，而基于通信加密的方法只能抵御诸如篡改攻击等部分内部攻击，而在面对延时攻击、重播攻击、泛洪攻击等无需对密码体制进行破译就可以实施的内部攻击时则完全失效。

2.2.2 基于信誉评估和恶意节点检测的安全路由协议

信誉评估和恶意节点检测是针对无人机网络中不断涌现的安全问题的一种较新的防御和检测方法。基于对网络运行状况及节点各种行为的观察，利用数学模型或者机器学习模型对网络中的节点进行动态评估，计算出节点的一个信誉值。评估的依据通常是节点的历史行为记录或者是来自其他节点的评价，然后从概率上得出节点的可信程度，并对节点的可信程度进行量化，作为其可信程度的评价结果，并以此为依据对节点进行区分判别，判断节点是否可信。然后，在判别结果的基础上实施诸如路由隔离等决策机制实现无人机网络的安全路由。这种基于信誉评估和恶意节点检测的管理机制能够准确地识别出内部的恶意节点，具有较好的预防和检测作用，并且具有较强的可扩展性，为整个无人机网络提供一个安全可靠的环境。

2.2.2.1 数学模型

数学模型具备坚实可靠完备的理论基础，并且易于实现、可解释性强，能够清晰明确地反映各个因素与目标之间的映射关系，同时无需大量数据的训练，它已经被广泛应用于无线网络恶意节点检测和安全路由的设计中。Pham 等人[70] 专注于合谋攻击 (Colluding Attacks)，攻击者合作实施黑洞攻击 (Blackhole Attacks) 和灰洞攻击 (Greyhole Attacks)，即故意丢弃全部或者部分接收到的数据包，并且恶意节点互相掩盖对方的不当行为和恶意记录，相互配合欺骗防御和检测系统。节点内部记录的相遇信息中虚假相遇记录的出现频率以及各个节点的消息转发率的异常模式被用于检测个体攻击和合谋攻击，从而进一步地确认网络中的恶意节点。Aneja 等人[71] 根据是否对虚假消息和正常消息进行泛洪，设计了三种不同的泛洪攻击 (Flooding Attacks)。通过对节点当前行为的评估，结合节点的历史信誉，计算节点的当前信誉，当节点信誉值高于一定程度时，则认为该节点是可信的；而当该节点信誉值低于一定阈值时，则该节点被认定为是恶意的，并对其进行路由隔离。Velusamy 等人[72] 研究一种由丢包攻击 (Dropping Attacks)、诽谤攻击 (Bad-mouthing Attacks) 以及女巫攻击组成的跨层路由攻击，并提出一种跨层信任评估的安全路由协议，基于数据包转发率计算节点的直接信誉；基于从可靠邻居收集到的证据推断节点的间接信誉；基于传输速率、缓冲区大小等跨层指标计算节点的置信度。将以上三者进行加权计算得到节点的信誉值，然后再结合跳数距离以及链路质量，使用模糊逻辑得到最终的路由决策。

然而，基于数学模型的方法完全依赖于学者对环境、事物以及问题的深入充分的理解和把握，需要对问题的输入、输出以及两者之间的映射关系进行精确的定义，而这在大规模复杂、高

度动态且不确定的无人机网络环境中是非常困难甚至是完全不可行的。同时，由于无人机网络的状态和解空间过大，数学模型无法对其中复杂的映射关系进行精确的拟合和求解，更无法根据实时的环境动态做出路由决策。

2.2.2.2 机器学习

由于其强大的学习能力和处理复杂关系的能力，机器学习算法已经被用于无线传感器网络和无人机网络中的恶意节点检测[73]。机器学习能够处理多维多样的数据，且能够自动从过去的经验和数据中进行学习和改进，同时无需明确的关系定义和过多的人工干预。

在有监督学习 (Supervised Learning) 中，训练数据包括相关的数据特征以及数据相应的标签，监督学习的目标是通过对训练数据的学习构建出一个由特征输入到标签输出的映射关系函数或模型，并基于此模型对给定的输入预测其归属的类别。Shams 等人[29] 对丢包攻击和延迟攻击进行检测和防御，数据包传输路径上的每一个节点都会对其下一跳节点的行为进行检查，以揭露恶意节点的不当行为迹象。基于对丢包率、数据包传输延迟以及数据包的转发间隔的收集，利用支持向量机 (Support Vector Machine, SVM) 对节点的信誉值进行评估，从而检测恶意节点，提高网络性能。Prathapchandran 等人[30] 对天坑攻击 (Sinkhole Attacks) 进行研究，在这种攻击中恶意节点向邻居广播虚假消息，宣称其拥有到达目的地的最短路径。当网络拥有足够的信息，即投递率、平均延迟、能耗以及通信成功率时，利用随机森林 (Random Forest, RF) 来计算节点的直接信誉值并以此为依据识别网络中的恶意节点；而当相关信息不足时，网络接收来自邻居节点的推荐，并使用主观逻辑 (Subjective Logic) 来推断节点的间接信任。Wan 等人[74] 对网络协议栈的通信特征进行了收集、提取和分析，并利用五种不同的监督学习方法对零日攻击 (Zero-day Attacks) 这一已知攻击进行检测，同时结合基于异常值的检测方案来发现未知攻击的异常可疑行为。Anthi 等人[75] 提出了一种轻量级的三层入侵检测系统，其中第一层负责根据设备类型对设备进行分类并对相应的数据包进行分流，第二层部署检测系统利用决策树 (Decision Tree, DT) 算法对设备行为进行识别，第三层则负责对具体的恶意行为种类进行区分。

与上述有监督学习模型相反，无监督学习 (Unsupervised Learning) 只需要数据的特征而不依赖于数据的标签，它通过寻找数据之间的相似性和异构型，从而发现隐藏的结构模式并对数据进行分组。Ma 等人[31] 考虑了一种混合攻击，其中攻击者可能同时发起丢包、篡改 (Tampering Attacks) 和重放攻击 (Replay Attacks)。节点之间的信息交换被用来评估节点信誉值，对可能实施恶意攻击的节点从多种维度进行信誉值惩罚，并且给予可信节点相应的信誉值奖励。基于信誉值，K-means 聚类算法被用来区分良性节点和恶意节点。Yang 等人[32] 研究了一种更为智能的选择性攻击，其中恶意节点只对发送给特定邻居节点的数据包实施攻击。所有节点和边的信誉模型被形式化为一个多元线性回归 (Multiple Linear Regression, MLR) 问题，基于对路径信誉的评估采用支持向量机计算出边的信誉矩阵，从而得到节点的信誉，最后利用 K-means 聚类确定

网络中的恶意节点。Liu 等人[76] 则考虑了另一种高级的选择性攻击，恶意节点只攻击满足某些特定条件的数据包。回归和聚类算法被用于评估节点的可信度，并将恶意节点与良性节点区分开。同时，优化了数据包的传输路由以收集更多的节点信息来增强路由安全。

为了更好地处理无人机网络复杂的结构，应对其众多的安全挑战，除了上述有监督和无监督学习方案外，一些其他的机器学习方法也被应用到检测无人机网络中的恶意节点并保障网络的路由安全之中。针对机器学习在无人机网络的不同环境中适应性和鲁棒性不佳的问题，Gao 等人[77] 提出了一个基于集成学习 (Ensemble Learning) 的环境自适应的恶意节点检测方案，预训练适应不同环境的弱检测模型的同时训练一个弱检测模型评估器，然后针对不同的环境基于评估器选择出性能表现较好的若干个弱检测模型，从而构建出一个适应环境的强集成检测模型。为了保护无线网络中数据的隐私性的同时提高各个节点之间的协作性，Nguyen 等人[78] 设计了一个基于联邦学习 (Federated Learning) 的异常检测系统，异常检测模型使用门控递归单元 (Gated Recurrent Unit, GRU) 并部署在本地网关负责对物联网设备进行检测，同时相关的模型参数而不是具体的网络数据被上传到云服务器执行模型的聚合和分发，以进一步地提高模型的训练精度。Zhang 等人[79] 为了抵抗无人机网络中的窃听攻击 (Eavesdropping Attacks)，提出了一种多智能体协作方法，采用集中式训练、分布式执行的模式，同时利用深度强化学习 (Deep Reinforcement Learning, DRL) 来联合优化无人机的轨迹、无人机发射器的发射功率以及无人机干扰器的干扰功率来保证无人机的安全路由。

上述机器学习方案均有其优势，并且适用于不同的无人机应用场景。但是，现有方案的无人机网络架构模型不统一，特征选择多种多样且随意性较大，没有统一的架构和标准来对特征进行抉择，同时方法仅针对特定的应用场景，不具备一般性。

2.3 本章小结

本章主要介绍和分析了与本文相关的研究工作，分别从高效和安全这两个角度对无人机网络路由协议进行了介绍和分析。无人机网络高效路由协议主要从基于拓扑、基于地理位置、混合、仿生这四种策略进行了介绍；而无人机网络安全路由协议则主要从基于身份验证和通信加密以及基于信誉评估和恶意节点检测的安全路由协议这两个层次进行了介绍和分析。

第三章　面向多跳无人机网络的跨层路由优化框架

3.1　引言

多跳路由在将数据信息从源节点投递到目的节点的过程中起着关键作用。然而，由于无人机网络具有拓扑高度动态、通信连接间断、网络资源受限以及通信链路不稳定等独特特点，无人机网络的多跳路由面临着投递率低、延迟高、吞吐量低、能耗高等诸多挑战。为了解决这些问题，许多无人机网络的多跳路由协议被提出以优化网络性能。但是，现有为无人机网络设计的大多数路由协议[80] 都是基于非跨层的方式，这些路由协议在进行路由决策时不使用其他层的路由信息和参数。此外，它们大多仅针对无人机网络的其中一个问题进行了特定的优化。因此，这些非跨层的路由协议无法在高度动态的无人机网络及其丰富的应用场景中提供足够高效的性能表现，并且无法满足严格的用户 QoS 要求。

上述问题的有效解决依赖于无人机网络协议栈中层与层之间的信息交互和融合，即通过不同层之间的联合优化，来获得更好的性能，这意味着需要使用跨层设计。跨层设计[81] 是一种很有前景的方法，有利于优化无人机网络在各类场景和各种应用中的性能表现。传统的分层网络模型，例如 TCP/IP 协议族、OSI 模型，在层与层之间提供了严格的信息封装，各层对各自独享的信息和设计细节进行隐藏，仅在相邻层次之间维持一个有限的接口，从而使得网络中的消息传输严格地按照同一标准进行处理。各层只能调用相邻层级提供的有限服务，这形成了分层网络模型一个非常重要的黑盒特性。一方面，层与层之间的抽象使得开发人员无需考虑过多的底层细节而能够轻易地实现上层应用；另一方面，对消息进行过分的封装也会导致一些副作用，例如 QoS 的下降、延迟的增加、额外的负载等等。

跨层路由优化打破了传统的各层信息被各层独享的封装，利用各个协议层之间的交互和依赖关系来实现可观的性能改进。跨层路由并不破坏传统网络模型的分层架构，只是提供了不相邻层之间的层间通信。此外，各个协议层之间互相公开和共享内部路由信息和参数，以实现对路由决策的联合优化。目前，有关无人机网络中跨层路由的研究设计已经吸引了国内外学者的广泛关注和极大兴趣。然而，现有的大多数跨层路由协议[82] 只能称之为部分跨层路由协议，即它们专注于利用较低三层的路由参数和信息，即物理层、数据链路层以及网络层，而忽略了无人机网络的其他协议层，它们没有对无人机网络中所有协议层可用的路由信息进行整体地收集、分析和利用。此外，它们对于较低三层中可用的路由参数信息也只是进行了简单的利用。不同层的路由参数被简单地进行加权和中和以形成路由度量，其本质上只是一种信息集成，没有对不同层的信息进行整体的融合来帮助优化路由决策。因此，为了实现无人机网络的高效通信，如何全面、深入地利用并融合各层的信息来设计跨层优化的无人机网络路由协议是一个富有开放

性和挑战性的问题。

通过对不同协议层的路由参数和信息进行整体的收集、分析、利用和融合，可以得到大量有用的信息，例如无人机的轨迹信息、任务信息、编队信息以及安全信息等，这些信息均可以被利用来进一步地提升无人机网络中数据传输的健壮性和稳定性。此外，无人机网络可以服务于具有不同优化目标的多样化应用，这些优化目标可以从应用层获取，并且应该在制定路由策略时被考虑在内。综合考虑和利用上述信息才可以制定出更高效的路由策略机制、做出更合适的路由决策，从而获得更好的网络整体性能。

本章对无人机网络的整体跨层路由优化进行了全面系统的研究，并提出了一个整体的跨层路由优化框架 (A Holistic Cross-Layer Routing Optimization Framework for UAV Networks, HOLO)。HOLO 的基本思想就是收集、分析、利用和融合来自不同协议层的反馈、参数和信息，以帮助做出更合适的路由决策。同时，本章回答了以下三个问题：

(1) 无人机网络中的哪些信息可以被收集并进一步用于跨层路由优化？

(2) 如何处理收集到的路由信息并将其融合到网络层以帮助优化路由决策？

(3) 如何根据跨层路由信息设计整体的跨层路由策略以做出高效的路由决策？

3.2 无人机网络协议体系结构

传统的计算机网络通信体系结构采用开放式系统互联 (Open Systems Interconnection, OSI) 模型，自下而上可划分为七个层级，分别为物理层、数据链路层、网络层、传输层、会话层、表示层以及应用层。但是，由于无人机网络众多的特性，其与传统的计算机网络在体系结构上存在着巨大的差异：首先，与传统计算机网络不同，无人机网络中节点之间的通信并不依赖于会话层和表示层，只需要其余五层即可完成无人机节点之间的数据处理和通信[83,84]。此外，除了这五层协议层之外，无人机网络还需要考虑众多的问题，例如节点的能量管理、移动控制、任务管理等。因此，如图 3.1 所示，除了从传统的分层网络通信协议这一维角度进行总结之外，本章还结合无人机网络的特点从三维的角度对无人机网络协议体系结构及功能进行深入分析。

(1) 物理层

物理层主要由无线发射器和接收器组成，其专注于物理设备及传输介质，并负责管理无人机网络所有的物理层操作，例如物理层需要对无线信号进行实时监测，并负责对物理传输信道进行选择，以便对数据进行调制和解调，从而实现节点之间的数据发送与接收。传输功率的调整、信道编码和调制方案的设计、移动性和传播效应的影响是物理层的重要设计因素。无线通信能力是无人机节点的必备功能之一，每架无人机的通信范围取决于可调的发射功率，该功率应大于接收阈值。同时，在路由过程中，无人机网络的无线信道特征通常可在物理层获得，例如接收信号强度指示 (Received Signal Strength Indicator, RSSI)、信噪比 (Signal-to-Noise Ratio, SNR)、信干噪比 (Signal-to-Interference-plus-Noise Ratio, SINR) 以及误包率 (Packet Error Rate, PER)。

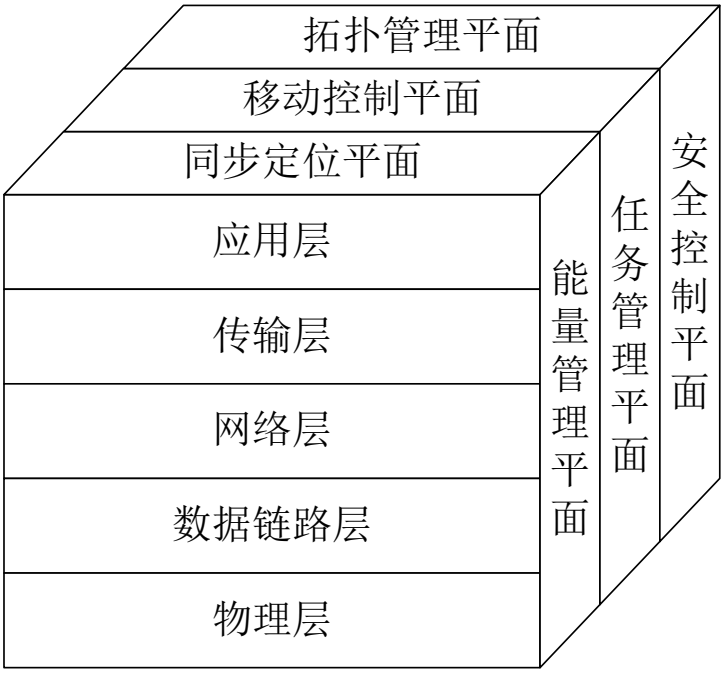


图 3.1　无人机网络协议体系结构

- 接收信号强度指示：它是对无人机网络中数据发送方和接收方之间无线传输的信号强度的度量。它已经被应用于指示接收方的功率水平，并且可以粗略估计通信双方的距离[72]，但是它忽略了无线传输中的噪声和干扰现象。
- 信噪比：它被定义为无线传输中有效信号功率与背景噪声功率的相对比值。信噪比在标识信号强度的同时进一步考虑了无线传输中的背景噪声，但它仍然忽略了干扰现象。
- 信干噪比：它被定义为无线传输中特定感兴趣的有用信号的功率除以来自其他所有干扰信息与电磁背景噪声的功率之和。在大多数情况下，相对于接收信号强度指示和信噪比来说，信干噪比是一个更好的物理层路由参数，因为它综合考虑了信号强度、干扰以及噪声。
- 误包率：误包率是基于误码率 (Bit Error Rate, BER) 的，在某些场景下可以通过信干噪比进行推断。无人机网络可以根据应用场景选择是否采取将包含误码的数据包丢弃的策略，并在此基础上计算出误码率或者误包率。

(2) 数据链路层

在无人机网络中，无人机节点之间共享通信信道，并通过竞争等方式来争夺通信信道的使用权以便进行数据传输。数据链路层则负责管理和协调无人机节点对网络通信信道以及传输介质的使用方式，尽量减少甚至避免节点之间数据传输的冲突，以提高无人机网络的带宽使用效

能和吞吐量。同时，数据链路层还负责数据差错控制、拥塞控制和队列管理。它由两个子层组成，即介质访问控制 (Media Access Control, MAC) 子层和逻辑链路控制 (Logical Link Control, LLC) 子层，其中 MAC 层规定了无人节点对网络公共通信信道以及传输介质的使用方式，而 LLC 层则负责对数据链路层的服务进行封装，并对网络层提供统一的服务接口。在无人机网络的路由决策中，可以从数据链路层获得与节点特性相关的参数，如缓存空间、重传次数。这些参数有助于在做出路由决策时最大限度地减小拥塞和数据包丢失。

- 排队信息：排队信息 (Queuing Information) 反映了无人机的流量负载情况，可以定义为数据包占用的队列大小与无人机缓冲区空间大小的比值。排队信息对于避免无人机网络中的传输碰撞和数据包丢失来说至关重要，因此它在无人机网络的各类应用场景中被广泛使用。
- 预期传输次数：预期传输次数 (Expected Transmission Count, ETX) 在一定程度上反映了链路质量，链路质量越差，预期传输次数越多。
- 到达间隔时间：到达间隔时间 (Inter-arrival Time) 是指队列中两个连续数据包到达同一个节点之间所经过的时间。
- 报文串大小：报文串大小 (Packet Train Size) 是指在单个传输周期内发送的数据包数量的平均值。通过数据包排序技术，无人机网络可以将多个数据包捆绑在一起，在一个竞争周期内传输，以减少竞争时间，提高网络带宽利用率。

(3) 网络层

网络层是无人机网络协议栈最复杂的层次之一，其最主要的功能是路由的发现、维护以及选择，指导无人机节点进行更高效的数据转发，从而使得数据包能够以无线中继的方式通过多跳到达目的节点，提高数据传输的效率。同时，网络层还负责邻居发现、数据融合和资源分配功能，用于辅助数据包的路由和传输。用于表征端到端传输路径的路由参数，例如跳数 (Hop Count)、往返时间 (Round-trip Time)、路径成本 (Path Cost) 等等，都可以从网络层获取，然后在进行路由决策时被依次使用以实现更高的网络性能。

(4) 传输层

无人机网络协议体系结构可支持传输层，也可将传输层的功能上移或下移，用于为无人机网络提供节点中具体进程之间的通信。传输层一方面联合物理层、数据链路层以及网络层对无人机网络协议的 QoS 进行保障，例如通过联合拥塞控制、流量控制以及重传机制等对数据的交付、时延和带宽的可靠性进行保证；另一方面它可以在下三层的基础上进一步地对网络的可靠性和安全性进行强化，例如采用密码机制对无人机网络中传递的消息进行加密。此外，传输层还负责对无人机网络中可用的频谱和带宽进行多路复用和多路分解。

(5) 应用层

应用层是无人机网络实际应用场景与网络协议栈交互的接口和媒介，为用户提供服务的同

时表征应用程序的客观实体：一方面将应用场景和应用程序的任务相关信息、QoS 需求等转换为具体的网络参数和套接字以供无人机网络协议栈进行针对性优化，从而达到更好的网络整体性能；另一方面无人机网络协议栈传输、处理后的数据最终都要汇聚到应用层，以供终端应用程序和用户作进一步的处理、分析和利用。

(6) 同步定位平面

由于无人机节点的高速移动性、分布的稀疏性，无人机节点除了利用通信协议栈满足正常数据通信需求之外，还需要配备一些辅助模块以保证无人机网络的正常运行。一方面，每个无人机节点都需要配备本地运行的内部时钟，以达到无人机网络的时钟同步。无人机节点进行本地感知、处理和通信及其相关事件都需要与本地时钟控制的时间戳信息相关联。节点需要具备对无人机网络中的事件进行正确排序的能力，以精确建立当前无人机网络的感知模型；同时，终端用户可能对来自多个无人机节点的协同信息感兴趣，这需要节点之间时钟的一致性，否则可能会返回不一致的错误信息，给用户造成困扰。

另一方面，除了时间同步之外，无人节点之间的交互同样需要相关的位置信息。现代无人机大多配备了 GPS 和 GLONASS 等双重全球导航卫星系统，作为其主要的位置、导航信息来源，最新的无人机可能配置了中国的北斗导航卫星系统。大多数的无人机应用场景都需要高精度的导航和定位，例如军事打击、地图测绘以及灾后搜救等。无人机的飞行控制器通过位置数据的交互来提供各自在特定时间点的位置坐标，以实现高效协作。

(7) 移动控制平面

无人机网络中节点的高速移动性和高度灵活性需要高可靠的移动控制平面。现代无人机都配备了陀螺仪、惯性测量单元 (Inertial Measurement Units, IMUs) 以及飞行控制器：其中陀螺仪为无人机提供保持平稳飞行及悬停的能力，同时还为中央飞行控制器提供相关的位置导航信息；惯性测量单元则为飞行控制器提供当前无人机的运动旋转状态信息，例如俯仰、滚动、偏航、抖动等；飞行控制器是无人机的中央大脑，它可以使用来自陀螺仪、惯性测量单元等功能模块的信息为无人机网络或地面控制单元提供必要的反馈信息。

同时，现代无人机网络依赖于无人机集群之间的相互协作配合，大多使用自主程序进行控制和管理，而不再完全由操作员进行远程无线电遥控，这对无人机的自主控制提出了更高的要求。例如，在大多数无人机网络的应用场景中，执行任务之前，无人机的飞行轨迹可以由地面控制单元通过任务规划或者路径规划算法进行预先设定；在执行任务时，无人机沿着各自预先规划好的轨迹飞行，从而实现高性能和高效率的相互协同配合。同时，如果某架无人机的轨迹需要动态调整，地面站会对其进行重新规划，然后将新的轨迹信息通过带外信道发送给相关无人机，以确保所有无人机拥有最新的全局轨迹信息，提高无人机网络的可靠性。

(8) 拓扑管理平面

无人机网络中节点分布稀疏、移动迅速、节点之间通信连接间歇，使得网络拓扑高度动态

变化，变得难以维护。现有的应用于静态网络的拓扑管理方案主要分为两类：一类通过节点之间定期地转发拓扑控制消息来对网络拓扑信息更新维护，然而拓扑控制消息的转发会占用大量的带宽和能量资源，这对于带宽资源紧缺、能量资源有限的无人机网络来说成本过高；另外一类通过路由发现和修复机制来维护网络拓扑，但是无人机网络高度动态的环境使得路由信息频繁快速的过时，导致路由效率低下。因此，需要高效的拓扑管理方案来保持无人机网络的连通性以及消息的可投递性。

(9) 能量管理平面

由于现有无人机尺寸和重量的限制，其机载能量有限，因此对于无人机网络数据通信而言，在无人机能量资源受限的情况下，能量消耗成为了无人机网络协议需要重点关注的问题。无人机网络需要根据自身的特性制定高效节能的路由策略，以提高能源消耗的效率、降低数据投递的能耗，从而延长无人机网络的生命周期；同时，网络中可能存在一些消耗能量但其实目前并不必需的进程，需要对它们进行识别和停止，从而提高无人机网络的性能表现。此外，对无人机网络中硬件和软件的组件配置进行联合优化，可以减少大部分低效甚至无效的活动。例如，大量不必要的能量都是由网络中的空闲进程或者通信子进程浪费的，通过软件配置的优化，可以减少节点对网络盲目的感知和侦听，减小能量消耗。另外，睡眠调度机制也是协调感知、通信以及能耗的一种动态调度方法。

(10) 任务管理平面

无人机网络被应用于各种现实应用场景，存在不同的关注和需求，因此，无人机网络不能像传统的静态网络或者互联网 (Internet) 一样使用统一的网络通信协议。根据不同的应用背景和系统要求，无人机网络的硬件系统、软件平台以及网络协议必然会有很大的差异，所追求的目标也是不同的。必须让无人机充分贴近应用需求，才能实现高效的目标，因此需要结合任务需求来对路由协议进行相应的设计和优化。

此外，无人机集群通常以编队的形式协作执行任务，而非是杂乱无序的一盘散沙。对应用需求和任务信息加以利用，能够对无人机编队的协同控制以及信息通信进行相应的设计优化，实现实时的队形调整、高效的组间通信，从而能够达到更好的无人机网络性能和任务效能。

(11) 安全控制平面

除了网络通信的性能之外，路由安全也是无人机网络协议必须考虑的重中之重。由于无人机网络的开放性以及分布式特性，它容易遭受到各种外部和内部网络攻击，例如主动干扰攻击、丢包攻击、篡改攻击、重放攻击等等。同时，无人机网络被广泛应用于各种关键任务场景，例如边境巡逻、战场监测、军事打击等任务，任何遭受攻击的无人机都可能向入侵者泄露重要信息，并可能影响整个无人机网络。

此外，无人机的有效载荷有限，其尺寸、功率和重量限制导致其自身并不具备充足的通信和计算能力。因此，传统的加密方案以及计算需求较大的安全机制并不适用于无人机网络，亟

须一个在计算、通信和存储方面均轻量级的安全路由协议来保证无人机通信的安全。

3.3 整体跨层路由优化框架总体架构

在对无人机网络协议体系结构进行全面深入地分析后，本节简要概述所提出的整体跨层路由优化框架 HOLO ，它主要利用无人机网络协议栈不同层的路由参数和信息之间的交互和融合，来优化路由决策并提高整体网络性能。如图 3.2 所示，HOLO 主要包括三个阶段，即路由信息收集阶段、整体跨层融合阶段和跨层路由决策阶段。首先，在路由信息收集阶段，信标消息 (Beacon Messages) 或路由发现 (Route Discovery) 可以被利用来收集各层的路由信息和参数，这些路由信息和参数可以反映无人机网络的状态，从而有助于优化路由决策。此外，在整体跨层融合阶段，通过不同层之间的信息融合，可以获得大量有用的信息，例如轨迹信息、任务信息、编队信息和安全信息。然后，这些融合出的信息以及不同层的参数将被融合到网络层中，以帮助做出更明智的路由决策。例如，轨迹信息可用于预测无人机的未来位置，从而获得无人机网络未来的拓扑结构，这有助于做出更合理的决策。最后，在跨层路由决策阶段，HOLO 利用跨层融合信息来优化决策，从而实现更为高效的路由决策机制。同时，根据无人机网络的应用场景以及优化目标的类型，采用不同的优化算法：对于单目标优化而言，进化算法 (Evolutionary Algorithms) 是一个不错的选择；而基于深度强化学习或者模糊逻辑的优化算法则更适合于多优化目标的应用场景。

3.4 路由信息收集

在无人机网络中，邻居发现和路由信息收集是路由协议的基本组成部分。本节将介绍 HOLO 的路由信息收集阶段的步骤和内容。

传统的自组织网络协议通过路由发现和路由维护来识别网络中所有可能的路由路径。网络中的节点各自维护一张路由表，用于存储到其他所有节点的路由路径。这种路由协议的优点是路由发现时间短，可以以较低的延迟对数据进行转发；然而，它的缺点是每个节点都必须维护一张路由表。如果网络中的节点数量变多，那么路由表就会变得很大，从而占用很大的内存空间。同时，路由建立之后，路由中断仍然会导致数据无法被成功投递到目的地，需要相应的路由维护和修复机制，但是路由表中的信息维护需要每个节点定期地向其他可用节点广播“Hello”数据包以对可用路由进行维护，这会大大增加网络的负载。因此，尽管这种类型的路由协议已经在无人机网络中实现，但是由于无人机网络高度动态的环境以及极度稀缺的带宽资源，它们的性能发生了显著的下降。无人机网络的高移动节点、间歇性连接以及不稳定链路等独特特性，使得路由表中的信息会频繁快速地过时，从而导致路由效率低下甚至是不可用。

上述问题的一个可能解决方案是利用信标消息来更新邻居节点之间的信息。与路由发现机制不同的是，节点不再维护无人机网络的全局拓扑及路由信息，而是只对可用邻居节点进行发

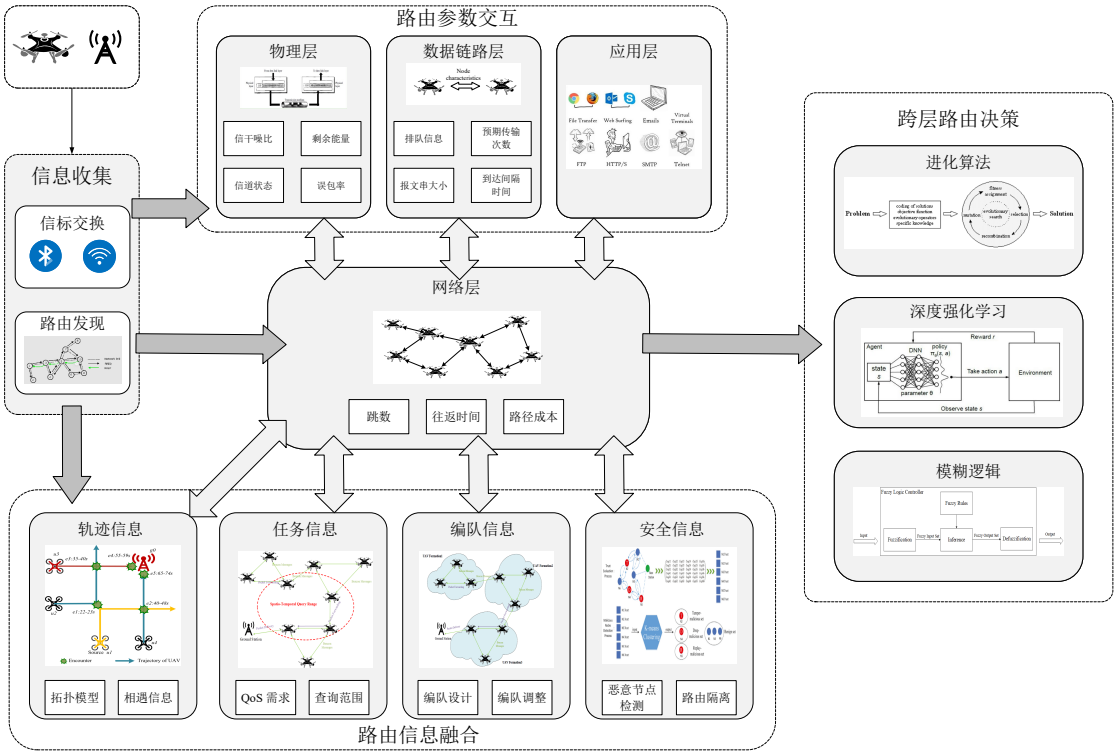


图 3.2　HOLO 总体架构图

现和维护，从而减小了网络的负载。因此，节点不必建立和维护路由表，只需对邻居节点及其相关信息进行发现、存储和维护。无人机在消息传输和转发之前通常使用这些消息用于在邻居节点之间定期交换信息，其中包含有助于优化路由决策的信息，例如节点定位信息以及链路质量信息。因此，节点在进行路由决策时已经知道其邻居的相关信息，从而可以选择出最合适的通往目的地的邻居节点。这种方式的代价在于数据包的投递延迟会出现一定程度的上升，这是因为节点在做出路由决策需要对邻居节点的信息进行更新以做出最佳选择。然而，相比于路由发现机制导致的无人机网络投递率低下、带宽负载重、存储需求大等问题，一定程度的延迟是可接受的。

因此，本章使用信标机制对邻居节点的信息进行收集，即每个无人机并没有网络的全局视图，其仅能跟踪与其邻居节点的连接。无人机在进行实际的数据传输之前，并没有执行路由发现，而是根据本地信息进行下一跳的路由选择。同时，为了有效地收集邻居节点的信息，无人机定期广播信标消息。根据无人机网络及其应用场景的需求，信标信息中可以包含诸如定位信息等可用于优化路由的信息，3.2节全面系统地总结了不同层中可用的路由参数和信息，不再赘述。

3.5 整体跨层融合

在对路由参数信息进行收集之后，本节将从两个角度，即路由参数交互和路由信息融合，来解释 HOLO 是如何分析、利用和融合不同层之间的信息的。路由参数交互是指 HOLO 利用不同层路由参数之间的交互，共同做出更合适的路由决策。此外，通过对不同层的路由参数和信息进行整体的收集、分析、利用和融合，HOLO 可以获得大量有益的信息，例如无人机的轨迹信息、任务信息、编队信息和安全信息，本章将其称之为路由信息融合，这些信息可用于促进更稳定高效的数据转发机制的发展进步。

3.5.1 路由参数交互

3.5.1.1 物理层交互

在路由决策时，物理层中路由参数的交互将使路由协议能够更加健壮地抵抗传输信道上的问题。例如，信干噪比通常在物理层可用，它在确定噪声和干扰方面始终起着至关重要的作用。同时，物理层的一些可用的信息可用于和其他层联合优化无人机网络中的路由，例如，利用物理层信息来调整数据链路层的拥塞控制机制，可以实现更高的吞吐量和能效增益。此外，在无人机网络的通信过程中，除了数据的发送和接收，数据链路层的载波监听也会消耗大量的能量，而通过对物理层的功率控制和剩余能量等信息的交互，可以自适应地调整载波监听的方式，在保证节点通信和减小传输能耗之间进行权衡，以达到更高的能量使用效率。同时，网络层可以利用物理层的信道状态、剩余能量、地理位置、发射功率等信息作为其路由决策的依据。

3.5.1.2 数据链路层交互

数据链路层能够较好地反映无人机网络当前总体的信道质量和拥塞状况。通过对数据链路层中的路由参数进行交互有助于其他协议层更好地针对当前的网络环境进行控制和调整，从而达到更高的吞吐量和带宽利用率。例如，数据链路层可以基于当前网络总体的信道质量和拥塞状况对节点的可调功率信息进行调整，同时调整差错控制机制，而物理层则可以基于这些信息进一步优化对物理无线信道的使用以及数据的传输，以减少传输错误、提高传输成功率。同时，链路质量较差或者网络较为拥塞可能会导致传输层的连接超时，此时，传输层可以通过联合数据链路层和物理层对重传机制进行优化。例如，传输层可以联合物理层对传输功率进行降低，联合数据链路层对当前数据帧的传输长度进行调整，从而优化传输层的性能，提高网络的吞吐量和带宽利用率。

3.5.2 路由信息融合

上文中介绍了各层可用的一些路由参数，并解释了它们是如何在不同层之间进行交互以及如何利用这些路由参数来优化路由的。尽管已经有一定量的无人机网络跨层路由协议，但它们中的大多数都没有对不同层可用的路由信息 进行整体地收集、分析和利用。此外，不同层之间的信息没有进行融合以帮助优化路由决策。然而，通过对不同层可用路由参数和信息的整体收集、分析、利用和融合，可以衍生出大量有用的信息，例如无人机的轨迹信息、任务信息、编队信息和安全信息，这些信息可用于促进稳定高效的数据转发机制的发展进步。

3.5.2.1 轨迹信息

在许多无人机网络的军事和民用应用场景中，无人机搭载 GPS 模块，可以实时获得其自身的位置信息。同时，为了获得更好的协作效能和任务效率，在执行任务前，大多由地面控制单元对各无人机的轨迹进行提前规划，无人机在执行任务时只需沿着预定义的轨迹飞行，相互配合完成任务[85]。此外，如果无人机的轨迹需要动态调整，需要由地面站进行规划，并将更新后的轨迹信息通过带外信道广播给相关无人机，以确保网络中所有无人机都拥有最新的全局轨迹信息[44]。因此，这种预先规划的轨迹信息可以被利用来优化无人机网络中的路由：基于无人机预先规划的轨迹信息，可以随时构建出无人机网络的全局拓扑模型，而无需冗余的信标交换。然后，可以预测出一些关于无人机网络中节点和路径的特征信息，例如无人机之间的相遇情况[86]。结合这些信息可以进一步地计算出数据包的高效传输路径而避免陷入局部最优以及数据包的冗余传输。

3.5.2.2 任务信息

无人机网络具有丰富的应用场景，同时在不同的应用场景中无人机网络执行多样化的任务，而任务信息则决定了用户的 QoS 需求以及路由协议的优化目标。对于不同类型的任务而言，通用的无人机网络路由协议往往无法达到令人满意的性能表现，需要结合任务信息对路由协议进行相应的设计改进和优化，以使路由协议达到更好的性能。例如，在无人机网络典型的覆盖查询类任务场景中，用户可能会根据需要进行时空范围查询，以收集特定时间段内无人机网络覆盖区域中特定区域的感知数据[87]。由于无人机网络的高度动态特性，当用户提交时空范围查询时，存储用户感兴趣的历史数据的无人机可能因为飞行移动已经不在查询的特定区域中。如果不对任务信息进行利用，无人机网络必须对网络中所有无人机存储的信息进行收集，这将导致巨大的网络开销以及极低的查询效率。在这种情况下，无人机网络收集的大多数数据并不是用户真正关心和需要的，而是冗余的数据传输。但是，通过联合任务信息和轨迹信息，则可以快速地查询存储相关历史信息的无人机，并通过多跳路由将满足时空约束的数据传输给用户，提高查询效率。

3.5.2.3 编队信息

多跳无人机网络可以同时服务于多个任务以及多种应用；通常将在同一个应用场景下执行相同任务的无人机集群编制成一个无人机编队，以便无人机之间更高效地相互协作、完成任务，同时一个无人机编队也可以根据具体子任务的不同进一步地划分为若干个子编队。因此，基于编队信息，可以将数据传输的路由问题根据源节点和目的节点是否在同一个编队中进行分类：当两者处于同一编队时可以直接应用现有的传统无人机网络路由协议；而当两者不在同一个编队时，虽然现有的传统无人机网络路由协议依然是可行的，但是利用无人机网络的编队信息可以进一步地优化数据路由和传输[88]。此时，无人机网络中的数据路由问题可以被划分为两个子问题：编队之间的数据传输以及编队内部的数据传输。编队之间数据传输的其中一个重要问题是边界无人机的选择，可以利用编队控制信息，例如编队设计、编队调整和编队重构来联合优化路由。

3.5.2.4 安全信息

随着无人机网络的广泛应用，其开放式和分布式的特性也使得自身容易遭受到各种各样的攻击、入侵和威胁。例如，攻击者可以实施内部攻击，对网络中的一些无人机实施物理捕获并进行非法入侵，然后利用这些被入侵的恶意无人机去攻击和破坏无人机网络的正常运行，例如篡改攻击、丢包攻击和重放攻击。近年来，无人机网络的攻击平面不断地被披露，作为传统无线传感器和移动自组织网络的变体，无人机网络除了继承自两者的安全挑战外，也存在着自身的安全挑战并且其自身的特性使得这些安全挑战变得更为严峻和复杂。因此，在设计路由协议、进行路由决策时需要兼顾路由性能和网络安全。联合无人机网络的安全信息，可以对网络中节点的身份进行验证、信誉进行评估，然后采用诸如路由隔离等机制来保障无人机网络的路由安全。

3.6 跨层路由决策

3.6.1 优化目标

无人机网络具有丰富的应用场景，不同的应用场景具有不同的优化目标。例如，军事打击、灾后搜救等实时应用场景对数据传输的延迟要求很高，数据必须以较低的延迟完成投递，而对带宽的要求则相对较低；但在地图测绘、影视拍摄等延迟容忍场景中，数据的传输需要满足高带宽的要求，而对延迟的要求则相对宽松。此外，数据传输的成功率以及所消耗的能量也是无人机网络路由协议需要关注的重点。因此，为了满足用户的 QoS 需求、实现高效的任务效能，在路由决策时需要充分考虑优化目标，一些有代表性的优化目标如下:

- 数据包投递率 (Packet Delivery Ratio, PDR)：数据包投递率被定义为成功投递到目的地的

数据包数量与网络中总生成的数据包数量的比值，它被用于衡量路由协议的可靠性和稳定性。

- 投递延迟 (Delivery Delay)：数据包的投递延迟是从数据包生成到它被成功投递到目的节点所经过的时间。更低的延迟意味着数据包能够被更快地投递到目的地。
- 跳数 (Hop Count)：在有线网络中，跳数是两个节点之间距离的粗略测量；而在无人机网络中，跳数是指数据包在被成功投递到目的节点时所经历的总传输次数，它在一定程度上指示了能耗，但与距离无关。
- 能耗 (Energy Consumption)：数据包的能耗指数据包从源节点到目的节点所经过的每一跳消耗能量的总和。
- 负载率 (Overhead Ratio)：负载率反映了无人机网络中数据传输路径的多样性，当多个数据包通过相同的路由路径或同一个节点进行传输时，无人机网络的负载率会上升。
- 吞吐量 (Throughput)：吞吐量是衡量无人机网络在单位时间内可以将多少个数据包传送到目的地的指标。它是衡量无人机带宽和网络高效性的一个度量。

鉴于不同层的信息融合以及多样化的优化目标，需要设计高效的路由决策机制来利用这些信息做出更合适的路由决策。本章提出面向优化目标的高效路由决策机制，根据优化目标类型的不同，采用不同的路由决策机制。

3.6.2 单目标优化

无人机网络的一些应用场景在进行路由决策时只需要考虑单一的优化目标。例如，在灾后搜救任务中，延迟是最重要的优化目标，一旦无人机发现幸存者等关键信息，需要以尽可能小的延迟进行消息传输，以便及时营救幸存者。

针对单目标优化，已经提出了许多的无人机网络路由协议，其中一部分基于路由发现和拓扑维护机制，在数据传输之前预先维护好路由路径，但这同时给无人机网络引入了极大的网络负载和不小的传输延迟；另外一部分使用基于度量的方法来为数据传输的下一跳选择合适的转发节点，然而这些路由协议在进行路由决策时基于贪婪转发的思想，只考虑当前节点和邻居节点的本地信息，而没有对网络的全局信息进行综合考虑和利用，在高度复杂动态的无人机网络中，这些路由协议很容易陷入局部最优。为了缓解甚至避免上述问题，本章采用进化算法[89] 来应对无人机网络的单目标路由优化。

进化算法通过对生物种群遗传和进化过程的模拟在问题空间中寻找最优解，它是一种相对比较成熟的全局优化算法，已经被广泛应用于无线网络的单目标路由优化[90]。一方面，与基于度量和穷举的优化方法不同，进化算法不直接优化某个具体的路由参数，而是在问题的整个搜索空间中进行联合优化。此外，基于度量和穷举的优化方法通常从一个初始点开始对问题进行求解，且只考虑当前的局部信息，这种基于有限视角的问题求解很容易陷入局部最优；而进化

算法则基于对生物种群遗传进化过程的模拟，从多个初始点开始并行地对问题空间进行搜索和求解，同时具有动态自适应性，在求解过程中能够根据环境的变化自适应地对参数进行调整，在多数情况下均能够找到全局最优解。另一方面，进化算法无需对传输路由和网络拓扑进行维护，不会为无人机网络引入额外的开销，具有较好的实用性和可扩展性；同时进化算法由于其自身特性，天生具有分布式、自组织以及自适应的特点，这与无人机网络高度契合，在无人机网络的各种单目标优化场景中，可以很好地对优化问题进行建模，对求解空间进行并行式搜索，有效找到问题的最优解，即最优的路由决策和全局传输路由。

3.6.3 多目标优化

单目标优化在无人机网络的实际应用场景中仍然占少数；在大多数情况下，无人机网络仍然需要根据用户和应用场景的 QoS 需求进行多目标联合优化，并且不同的应用场景和用户需求对 QoS 的要求是不同的，也就意味着路由协议的优化目标是不同的。进化算法能够为无人机网络的单目标优化场景提供较好的路由性能保障，但是由于多目标优化的全局任务空间过大，导致进化算法的搜索效率和收敛速度过慢，并且不能对全局最优解进行保证，容易陷入到局部最优，极大地降低了路由协议的优化效率和性能表现。同时，无人机网络高度复杂、动态和不确定，因此很难利用数学模型或者关系模型对无人机网络多目标优化之间的关系和映射进行精确定义、拟合和求解。

近年来，人工智能方法再次引起了研究学者的广泛关注和应用，由于其强大的学习能力和处理复杂关系的能力，它被认为是解决诸如无人机网络多目标路由优化等复杂动态且难以建模的问题的高效解决方法。人工智能方法无需明确的关系定义和过多的人工干预，能够自动从过去的经验和数据中进行学习和改进，从而实现更为高效、智能的路由决策优化机制。深度强化学习和模糊逻辑是其中两种具有巨大潜力的技术，并且已经被应用于无人机网络多目标路由优化中。

3.6.3.1 深度强化学习

无人机网络的多目标路由优化在大多数情况下都可以被归约和建模为马尔可夫决策过程 (Markov Decision-making Process, MDP)。虽然 MDP 理论上可以通过诸如动态规划 (Dynamic Programming)、进化算法以及强化学习技术来解决，但是，在高度动态复杂且不确定的无人机网络环境中，动态规划和进化算法等技术在求解速度过慢的同时很难找到最优解，因此并不适用；同时，传统的强化学习依赖于 Q 表中对环境状态和最佳路由决策之间的映射，而无人机网络的多目标优化场景中环境状态巨大且难以进行精确映射，会产生巨大的存储开销和决策偏差，因此并不可行。

为了克服上述这些问题，本章利用深度强化学习来对无人机网络的多目标路由优化进行求

解。深度强化学习不再依赖于 Q 表对状态和决策的枚举，而是在强化学习的基础上使用深度神经网络 (Deep Neural Network, DNN) 通过训练数据的学习构建出一个由特征输入到标签输出的映射关系函数或模型，能够适应大规模且复杂的无人机网络环境[91]。深度强化学习将深度学习和强化学习有机地结合起来，融合了两者的优点：一方面强化学习使得节点可以在学习过程中实时监控网络环境的变化、逐渐获取和建立无人机网络的环境知识，从而逐步学习最优路由决策；另一方面，基于深度学习，节点无需对无人机网络环境进行精准建模，可以在没有完整和准确的网络信息的情况下对路由决策进行优化，同时允许无人机根据相对实时的环境信息动态地做出路由决策。因此，深度学习和强化学习的有机结合大大提高了无人机网络路由协议的决策速度和优化性能。同时，深度强化学习也被广泛应用于解决无人机网络中的一些其他问题，例如路径规划、频谱管理。

3.6.3.2 模糊逻辑

除了深度强化学习之外，模糊逻辑也适用于环境复杂、模型不确定且非线性较强的无人机网络[92]。在无人机网络的多目标路由优化中，路由决策需要权衡各项优化目标，同时各个路由指标之间不仅会相互协调，也有可能会相互冲突，对同一路由决策可能会持有不同甚至完全相反的建议，而模糊逻辑能较好地处理这种不确定和不精确的情况。与精确的数学模型不同，模糊逻辑模拟人类的思维模式，根据不同的无人机网络环境和应用场景定义不同的模糊规则，并利用模糊隶属函数 (Fuzzy Membership Function) 进行模糊推断和判断，能够很好地适应各种不同且复杂的无人机网络环境。此外，它还可以通过改变规则和隶属函数进行调整，较为灵活地为高度分布式的无人机网络提供可靠的网络性能和路由保障。

3.7 本章小结

本章针对多跳无人机网络提出了一种整体的跨层路由优化框架 HOLO 。首先，结合无人机网络的特点以及传统的分层网络通信协议，从三维的角度对无人机网络协议体系结构及功能进行了深入分析。然后，对无人机网络中路由参数等信息的收集、整体交互以及跨层融合的方式和内容进行了介绍，通过从跨层的角度对所有层的反馈、参数和信息进行整体的收集、分析、利用和融合，得到了大量有益信息，可用于优化路由决策。最后，设计了面向优化目标的高效路由决策机制，根据优化目标类型的不同，分别提出了高效的路由决策机制，利用跨层融合信息做出最佳路由决策。

第四章　功率感知的多跳无人机网络路由协议

4.1　引言

在许多无人机网络的应用场景中，例如灾后搜索与救援任务，无人机需要长时间的工作以完成大规模、较复杂的任务。但是，由于现有无人机尺寸和重量的限制，其机载能量有限，因此，对于无人机网络数据通信而言，在无人机能量资源受限的情况下，提高能源消耗的效率、降低数据投递的能耗至关重要。能耗高效路由协议就是为给定的数据包找到一条通往目的地的总能耗最小的传输路径，从而有效节省带宽和能量等无人机网络中较为稀缺的网络资源，提高无人机网络性能的同时延长其生命周期[93]。

关于能耗高效路由协议，现有的研究主要针对传统的无线传感器网络和移动自组织网络，它们都依赖于稳定的网络拓扑[94]。但是，无人机网络中节点的高速移动，会导致其网络拓扑高度动态变化，同时对网络的连通性和通信链路的稳定性造成严重的影响，现有的研究不得不通过频繁地转发大量的拓扑控制消息来更新维护网络拓扑信息，这会导致大量的能量消耗，缩短无人机网络的生命周期。此外，现有的能耗高效路由协议都是基于非跨层的方法，即它们只利用了网络层及其相邻协议层的信息来进行路由优化[95]。实际上，无人机网络协议栈的各个层都会影响数据包传输的能耗，例如物理层的功率控制信息，通过联合分配、功率控制和链路调度可以减小能耗和增加单跳吞吐量[81]。

同时，无人机网络具有丰富的应用场景，不同应用场景下的优化目标是不同的。在对数据包的传输能耗进行优化的同时，必须充分考虑网络的应用场景及用户的 QoS 需求，这些可以从网络协议栈的应用层获取到。例如，在绝大多数应用场景中，除了能耗之外，数据包的投递延迟也应该被充分的考虑，这是另一个关键的性能指标，不同场景下的需求也不同。无人机网络对数据的投递延迟有着一定的要求[42]：实时应用场景，例如情报收集、军事打击等任务，要求消息的投递延迟相当小，以实现快速反应；而在其他的一些非实时应用场景中，例如地理测绘、影视拍摄等，网络延迟的要求则相对比较宽松。因此，在无人机网络进行消息传输的同时对消息添加相应的延迟约束是合理且有必要的，这意味着消息必须在 T 的时间长度内被成功交付。基于此，可以通过简单地动态调整延迟约束 T 的大小来很好地归约和表征上述所有情况。因此，需要寻求延时约束与其他网络性能，例如能量消耗，之间的权衡，以更好地发挥无人机网络的应用潜力。

此外，无人机网络中节点分布稀疏、通信连接间歇，节点之间并不存在持续稳定的即时端到端通信路径。传统的延迟容忍网络 (Delay-tolerant Networks, DTNs) 采用存储-携带-转发机制[96]进行消息的转发与投递：当持有消息的无人机当前的通信范围内不存在或找不到合适的转发节

点时，允许该无人机暂时存储携带该消息，直到其通信范围内出现满足条件的转发节点或目的节点。存储-携带-转发机制能够在一定程度上缓解网络间歇性连接带来的问题，然而，在高度动态的无人机网络中其仍然面临着很多的挑战，例如路由空洞[17]、乒乓效应[97] 等，这严重损坏了路由协议的性能。

为了有效解决上述问题，基于所提出的面向多跳无人机网络的整体跨层路由框架，本章提出了一种高效的功率感知的多跳无人机网络路由协议 (A Power-Aware Routing Algorithm for UAV Networks, PAR)。该路由协议利用存储-携带-转发机制进行消息的传输与投递，并且使用了跨层设计，联合物理层的功率感知、应用层的 QoS 需求以及预先规划的无人机轨迹信息来对无人机网络的路由决策进行联合优化。首先，该协议结合应用层的 QoS 需求，以延迟约束和能耗最小化为原则指导路由决策的优化。同时，该协议利用预先规划的轨迹信息以及存储-携带-转发机制来辅助路由优化，从而找到更优的传输路径。此外，该协议还对物理层的功率信息进行跨层感知和调整，在保证消息延迟约束的同时进一步地优化路径、降低能耗。

4.2 系统模型

4.2.1 网络模型

本章以无人机网络执行灾后搜救任务作为示例应用场景，这是一种具有代表性的覆盖任务应用场景，其中无人机网络由多架无人机以及单个固定的地面站组成。为了优化无人机网络的性能，根据任务类型的不同，可以进一步地将无人机细分为搜索无人机 (Searching UAV) 和摆渡无人机 (Ferrying UAV), 其中搜索无人机配备着摄影仪、热成像仪等传感器设备，其主要任务是在各自指定的区域内执行覆盖、拍摄、搜索、救援等任务，并根据需要将数据发送给地面站以做进一步的分析和处理；而摆渡无人机则主要负责协助搜索无人机进行数据和控制消息的传递，保证无人机网络连通性的同时进一步地提高无人机之间的协作效率以及无人机网络的任务效能。在无人机网络执行任务之前，地面站会根据任务规划或者路径规划算法预先计算出每架无人机的飞行轨迹[98]，以更高效地完成指定任务，例如搜索无人机可以采用“Z”字形的运动模式以高效地对区域进行覆盖、搜索，而摆渡无人机则可以在搜索无人机和地面站之间沿着预定的 (类似于直线) 的航路来回飞行，在协助搜索无人机执行任务的同时对搜索无人机之间可能存在的覆盖空洞进行进一步地搜索。此外，如果在执行任务中出现需要动态调整无人机飞行轨迹的需求，也需要由地面站进行统一调度并将调整过的最新轨迹信息同步给相关无人机[99]，以确保任务的继续执行。综上所述，本章中无人机网络具有以下特性：

(1) 混合通信模型：节点配备两种不同的无线电技术，使用两种独立的无线通信链路。一种是短距离、高吞吐量链路 (High-throughput Links)，该链路可以通过 Wi-Fi 技术 (IEEE Std. 802.11ax) 实现，可以在 2.4G/5G/6G 频段进行通信，最大吞吐量可达 600 ~ 9608 Mbit/s，可在 200 ~ 300 m 的通信范围内提供较为稳定的通信链路。在本章中，其被用于无人机之间、无人机与地面站之间传

输大规模、大尺寸的数据，例如图像数据。另一种是长距离、低吞吐量链路 (Long-range Links)，该链路可通过 XBee-PRO (IEEE Std. 802.15.4) 实现，它可以提供长达 1.5 km 但吞吐量低于 80 kbit/s 的通信链路，在无人机网络中这被用于控制命令、确认信息、位置信息、轨迹信息等轻量级数据的传输。XBee-PRO 在本章中充当带外信道 (Out-of-band Channel)，在 2.4G 频段运行，并将每架无人机连接到地面站。

(2) 功率的动态感知与调整：针对节点之间的短距离、高吞吐量链路，节点可以通过跨层优化设计，跨层感知网络协议栈的数据链路层以及物理层，动态进行功率调度与控制，并根据自身剩余能量、网络环境状况以及应用场景需求等信息自适应地调整发射功率水平[100]，在减小节点之间干扰、提高系统吞吐量的同时降低传输能耗，这可以通过 IEEE Std. 802.11h 实现，能够被集成到 Wi-Fi 技术当中。本章考虑分布式独立控制，网络中每个节点独立进行功率调度和控制，节点之间不相互影响各自的传输功率。

(3) 轨迹、位置、移动信息的可用性：在无人机网络执行任务之前，会根据任务规划或者路径规划对无人机的轨迹信息进行预先规划，同时每架无人机都会在本地存储所有无人机的轨迹信息。在任务执行期间，无人机沿着各自预先规划好的轨迹飞行。如果某架无人机的轨迹需要动态调整，地面站会对其进行重新规划，然后将新的轨迹信息通过带外信道发送给无人机，以确保所有无人机拥有最新的全局轨迹信息。此外，无人机都配备了 GPS 和惯性测量单元，可以实时获取自身的位置信息以及运动传感信息，并通过带外通信等方式将其同步给其他无人机。因此，每架无人机都可以获取到网络中所有无人机的轨迹、位置和移动信息，进而感知网络拓扑情况，用以辅助路由决策。

(4) 节点的稀疏分布：在大多数无人机网络应用场景中，无人机通常稀疏分布在任务区域中，节点密度较低、网络连通性较差。节点之间可能并不存在即时稳定的端到端路由路径，节点以存储-携带-转发的方式将消息逐跳投递给其他节点。一方面，部署密集型无人机网络成本过高，且远远超出完成任务所需的数量，这违背了多跳无人机网络的使用本意；另一方面，由于无人机节点的高速移动性，密集型部署可能会导致碰撞等问题。此外，节点之间的负载和干扰也会成为密集型网络中严峻的挑战，会导致无人机网络性能的降低。

除了以上特性之外，本章将无人机网络从三维空间抽象为欧几里得空间，忽略垂直空间[101]，并将其建模为一个加权有向图 $G = (V, E, P)$。有向图中的节点代表无人机或者地面站，记作 $V = \{u_1, u_2, \ldots, u_N\}$，表示无人机网络中共有 N 架无人机。无人机的功率感知特性被离散化为若干个功率级别，即每架无人机拥有 L 个可调功率级别，表示为 $P = \{p_1, p_2, \ldots, p_k, \ldots, p_L\}$。同时，时间被划分为离散的 T 个时隙 (Time Slot)，节点在一个时隙的时间内保持静态[42]。有向图中的边 $e = (u_i, u_j, t, p_k)$，其中 $1 \le i, j \le N$、$0 \le t \le T$、$1 \le k \le L$ 以及 $i \ne j$，表示节点 u_i 将会在时隙 t 与节点 u_j 相遇，并且节点 u_i 可以以功率级别 p_k 与节点 u_j 通信。边的集合记作 $E = \{e_1, e_2, \ldots, e_G\} \subseteq V \times V$。节点之间的通信是双工的，即无人机 u_i 和 u_j 在彼此的通信范围

内且建立通信链路之后可以互相传输消息。节点 u_i 以功率级别 p_k 向 u_j 传输一个数据包 m 所需要消耗的能量记为 $E_e(p_k)$。

4.2.2 问题形式化

给定一个无人机网络，每次源节点无人机生成实时消息 m 时，都会根据消息的紧急程度将其与一个延迟约束相关联。考虑到无人机的功率感知特性，本章的目标是以延迟约束和能耗最小化为原则，为消息 m 寻找一条满足延迟约束且能量消耗最小的高效传输路径。

4.3 功率感知的高效路由算法 PAR

4.3.1 基本思想

PAR 的基本思想就是联合无人机网络物理层的功率感知特性、应用层的 QoS 需求以及预先规划的轨迹信息来对无人机网络的路由决策进行优化，从而实现了物理层、网络层、应用层以及轨迹信息的跨层联合优化。首先，利用无人机预先规划的轨迹信息和物理层的功率感知特性计算出无人机在不同功率级别下的相遇情况。然后，基于无人机的相遇信息，结合应用层的 QoS 需求，以延时约束和能耗最小化为原则，设计并构造出功率感知相遇树，其中每个节点的功率可以根据各自的相遇情况进行自适应的调整，从而保证每个消息的及时投递以及能耗的最小化，提高网络的持久性。

如图 4.1 所示，无人机网络由五架无人机 u_1、u_2、u_3、u_4、u_5 以及一个地面站 g_0 组成。无人机沿着各自预先规划好的轨迹信息航行，如图中各箭头所示。为了方便表示，将无人机的功率离散化，并假设无人机存在两个不同的功率级别，即 p_1 和 p_2。图 4.1 中显示了无人机在不同功率级别下的相遇情况：无人机在功率级别 p_1 下的相遇表示为 e_i，在功率级别 p_2 下的相遇则表示为 c_i。为了便于区分，本章将无人机在功率级别 p_1 下的相遇 e_i 抽象为相遇点，即当两架无人机能够以功率级别 p_1 通信时，它们两者的飞行轨迹必然相交。例如，无人机 u_1 和 u_2 会在 10 s 的时候于位置 e_1 相遇，功率级别为 p_1。此外，当无人机能够以功率级别 p_2 相互通信时，它们的轨迹不必相交：无人机 u_2 和 u_3 会在 25 s 的时候于位置 c_1 相遇，功率级别为 p_2; 无人机 u_2 和 u_5 会在 25 s 的时候于位置 c_2 相遇，功率级别为 p_2; 无人机 u_5 和 u_2 会在 45 s 的时候于位置 c_3 相遇，功率级别为 p_2。

源节点 u_1 需要将消息 m 发送给地面站 g_0，消息的延迟约束为 T。本章使用文献[102] 中的亚线性能耗模型，即以功率级别 p_1 传输两次相同大小的消息所需的能耗大于以功率级别 p_2 传输一次消息的能耗，表示为 $2E_e(p_1) > E_e(p_2)$。值得注意的是，PAR 并不受特定能耗模型的限制。根据预先规划的轨迹信息和计算出的相遇情况，可以推断出至少存在四条传输路径：

(1) $pa_1 : u_1 \xrightarrow{e_2} u_3 \xrightarrow{e_4} g_0$。传输路径为 $(u_1, u_3, 5s, p_1), (u_3, g_0, 60s, p_1)$。消息 m 沿着此路径传输的投递时间为 60 s，且总能耗为 $2E_e(p_1)$。

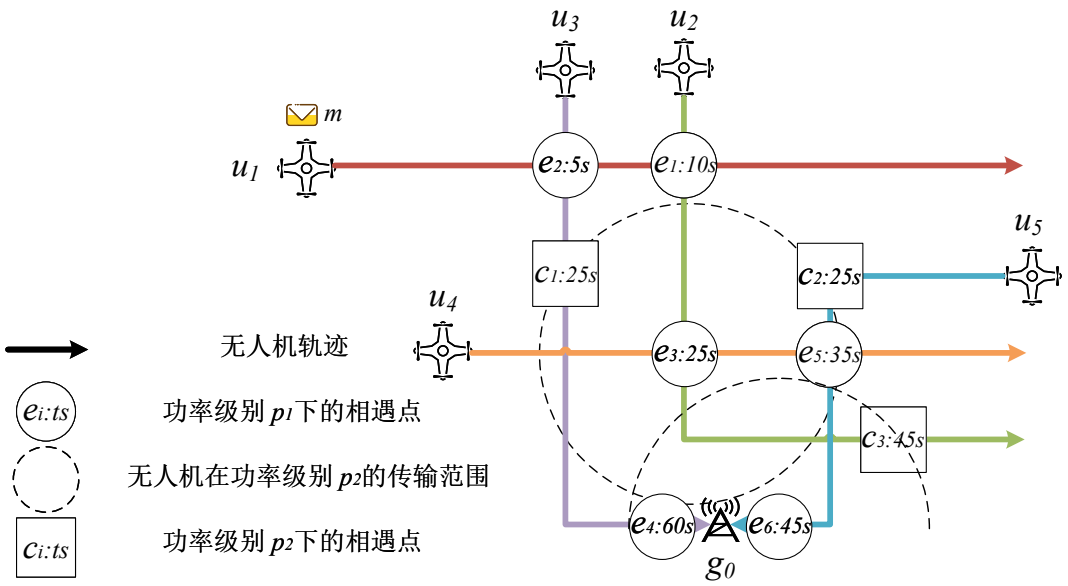


图 4.1　当无人机具有两个功率级别时无人机之间的相遇点示例图

(2) $pa_2 : u_1 \xrightarrow{e_1} u_2 \xrightarrow{c_1} u_3 \xrightarrow{e_4} g_0$。传输路径为 $(u_1, u_2, 10s, p_1), (u_2, u_3, 25s, p_2), (u_3, g_0, 60s, p_1)$。消息 m 沿着此路径传输的投递时间为 60 s，且所需要的总能量为 $2E_e(p_1) + E_e(p_2)$。

(3) $pa_3 : u_1 \xrightarrow{e_1} u_2 \xrightarrow{c_2} u_5 \xrightarrow{e_6} g_0$。传输路径为 $(u_1, u_2, 10s, p_1), (u_2, u_5, 25s, p_2), (u_5, g_0, 45s, p_1)$。消息 m 沿着此路径传输的投递时间为 45 s，且总能耗为 $2E_e(p_1) + E_e(p_2)$。

(4) $pa_4 : u_1 \xrightarrow{e_1} u_2 \xrightarrow{e_3} u_4 \xrightarrow{e_5} u_5 \xrightarrow{e_6} g_0$。相应的传输路径为 $(u_1, u_2, 10s, p_1)$, $(u_2, u_4, 25s, p_1)$, $(u_4, u_5, 35s, p_1), (u_5, g_0, 45s, p_1)$。消息 m 沿着此路径传输的投递时间为 45 s，且所需要的总能量为 $4E_e(p_1)$。

当延迟约束 $T \geq 60$ s 的时候，上述四条路径均能将消息 m 及时成功投递，但是与其他三条传输路径相比，第一条传输路径 pa_1 是最佳选择，因为它在保证消息及时投递的同时传输能耗最小。然而，当 45 s $\leq T <$ 60 s 时，第一条和第二条传输路径，即 pa_1 和 pa_2，不再能满足用户的 QoS 需求，因为沿着它们传输消息的投递时间为 60 s，超出了所规定的延迟约束。在这种情况下，如果不考虑无人机的功率可调特性，即无人机只能以功率级别 p_1 进行数据传输，那么最合适的传输路径为 pa_4，消息 m 沿着 pa_4 传输的投递时间为 45 s，满足时延要求，同时总能耗为 $4E_e(p_1)$。但是，如果将无人机的功率级别可调考虑在内的话，可以找到一条更优的传输路径，即 pa_3。尽管 pa_3 和 pa_4 都可以保证消息 m 的及时送达，但是沿着 pa_3 传输所需的能耗为 $2E_e(p_1) + E_e(p_2)$，小于沿着不考虑可调功率级别的 pa_4 传输所需的能耗。基于上述例子，可以发现通过对各个节点的功率进行自适应的调整可以在保证消息及时投递的同时进一步地减小能耗。后文将详细介绍如何找到一条满足延迟约束且能耗最小的最优传输路径。

4.3.2 功率感知相遇树构建

本章以延迟约束和能耗最小化为原则，利用无人机的预先规划的轨迹信息和功率可调特性来优化路由。为了在数据包 m 的延迟约束内找到一条能耗最小的高效传输路径，提出了一种功率感知相遇树 (Power-aware Encounter Tree, PET)，它是基于无人机在延迟约束内不同功率级别下的相遇信息构造的。在描述功率感知相遇树的构建过程之前，首先介绍一下功率感知相遇树的一些基本定义：

(1) 功率感知相遇树是一棵有向树，根节点为创建消息的源节点 s，它是消息传输的起始点，消息的目的节点为 d。

(2) 树中的每个节点 n 都代表着网络中的一个无人机或者地面站，无人机或者地面站的编号（例如 u_1、g_0）即为树节点的编号。由于节点的功率可调特性，节点具有多个功率级别，因此节点可以在树中重复出现。

(3) 树中节点之间的每条边 e 都是有向边，它代表了节点双方之间的相遇以及通信链路的建立。有向边的方向指示了消息的传输方向；有向边的起点即消息的发送方为父节点，有向边的终点即消息的接收方为子节点。相遇点的编号（例如 e_1、c_1）即为有向边的编号；与节点不同的是，相遇点具有唯一性，即每个相遇点只能在树中出现一次。

(4) 树中每个节点 n 的孩子节点是节点 n 在与其父节点相遇之后以及延迟约束之前，以不同功率级别能够相遇的其他节点。对于根节点而言，由于它没有父节点，因此它在消息的延迟约束之前以不同功率级别能够相遇的节点均为它的孩子节点。节点 n 的孩子节点可以被表示为：

$$n.C = \bigcup_{k=1}^{L} N(n, n.t, T, p_k), \tag{4.1}$$

其中 $n.t$ 表示节点 n 与其父节点的相遇时间，T 代表消息 m 的延迟约束，并且 $N(n, n.t, T, p_k)$ 表示节点 n 在与其父节点相遇之后、延迟约束之前（即在时间段 $n.t$ 到 T 之间），能够以 p_k 的功率级别相遇的节点集合。

(5) 对于节点 n 的每个孩子节点，将其记作 $c \in n.C$，则从源节点 s 到节点 c 的传输路径可以被递归地定义，即它由从源节点 s 到父节点 n 以及从父节点 n 到子节点 c 的两条传输路径组成，表示为 $c.pa = n.pa \rightarrow (n, c, c.t, p_k)$。

(6) 从源节点 s 沿着传输路径 $c.pa$ 将消息 m 传输到节点 c 的总能耗记为 $E_t(c.pa)$。根据上述传输路径的划分，它同样可以被递归地定义，且由两部分能耗组成：$E_t(c.pa) = E_t(n.pa) + E_e(p_k)$，其中 $E_e(p_k)$ 表示节点 n 以功率级别 p_k 将消息成功传输给其子节点 c 所需的能耗。

(7) 当功率感知相遇树初始化时，它仅包含源节点 s，同时对于源节点 s 而言，$s.t = 0$、$E_t(s.pa) = 0$。

接下来描述功率感知相遇树的构建过程，它是从源节点开始向功率感知相遇树中一个接着一个地插入新的节点和相遇点（即有向边）对，直到找到满足要求的传输路径的过程。每一对新

添加的节点 n 和有向边 e_n 都关联着一个能耗指标 (Energy Consumption Metric, ECM) 以及一个相遇时间 (Encounter Time, ET), 并且 $ECM = E_t(n.pa)$、$ET = n.t$。同时使用优先级队列 (Priority Queue) PQ 来辅助节点和有向边的插入。当每个节点被添加到 PQ 中时，它的父节点和相遇点（即关联的有向边）已经确定。节点和有向边对按照关联的 ECM 和 ET 进行排序，以确保 PQ 头部的节点具有最小的 ECM。同时，为了保证相遇点在功率感知相遇树中的唯一性，使用位图 V 来标记相遇点添加情况。如果 $V[e_n] = 1$，则代表相遇点 e_n 已经被作为边插入到功率感知相遇树中；如果 $V[e_n] = 0$，则代表相遇点 e_n 还未被插入功率感知相遇树。功率感知相遇树 PET 的主要构造过程如算法 4.1 所示，其流程解释如下：

(1) 将消息源节点插入到优先级队列 PQ 中，并将位图 V 中的所有元素都初始化为 0，这表示所有的相遇点都还没有被添加到功率感知相遇树中。

(2) 如果优先级队列 PQ 为空，则功率感知相遇树的构建过程完成；否则，从优先级队列 PQ 中取出头节点（记为节点 u），该节点是具有最小 ECM 的节点。如果节点 u 是源节点，则转到步骤 (4)；否则，获取节点 u 与其父节点之间的相遇点 e_u，然后执行步骤 (3)。

(3) 判断功率感知相遇树中是否已经存在相遇点 e_u。如果是，即 $V[e_u] = 1$，则将节点 u 丢弃并返回执行步骤 (2)；否则，转至步骤 (4)。

(4) 根据预先规划好的轨迹信息、位置信息和相遇信息，计算出节点 u 的子节点，即 $u.C$。节点 u 的孩子节点是节点 u 在与其父节点相遇之后、延迟约束之前（即在时间 $u.t$ 和 T 之间）以不同功率级别（即从功率 p_1 到功率 p_L）相遇的无人机。

(5) 对于节点 u 的每个子节点 c，即 $c \in u.C$，根据节点 u 和 c 之间的相遇点 e_c 计算节点 c 的 ECM 和 ET。如果功率感知相遇树中已经存在相遇点 e_c，则不做任何处理并将其丢弃；否则将节点 c 与相遇点 e_c 一同插入到优先级队列 PQ 中。优先级队列 PQ 对节点按照 ECM 进行排序，以保证头节点始终具有最小的 ECM。

(6) 如果节点 u 是源节点，那么它是功率感知相遇树的根节点；否则，将节点 u 添加到功率感知相遇树中，并将其作为子节点插入到其父节点相应的子列表中。它们之间的有向边 e_u 表示节点 u 与其父节点之间的相遇。同时，将对应的位图元素 $V[e_u]$ 设置为 1，表示相遇点 e_u 已经被插入到功率感知相遇树中。

(7) 判断目的节点 d 是否已经添加到功率感知相遇树中。如果是，则功率感知相遇树的构造过程结束并将其返回，表明已经找到了一条满足要求的传输路径；否则，跳转至步骤 (2)。

4.3.3 剪枝优化

如上一节中所述，PAR 通过将新的节点和有向边对逐个添加到功率感知相遇树中来完成对它的构建和扩展。根据构建出来的功率感知相遇树，能够为消息找到满足延迟约束的同时能耗最小的传输路径。但是，功率感知相遇树只保证了节点之间相遇点的唯一性，而节点则允许被重

算法 4.1 功率感知的高效路由算法 PAR

输入: 消息源节点 s、目的节点 d、延迟约束 T

输出: 功率感知相遇树 PET

1: PQ.push(s), initialize(V, 0) // 将源节点 s 插入到优先级队列 PQ 中，并将位图 V 中所有元素都初始化为 0
2: **while** !PQ.isEmpty() **do**
3: $u \Leftarrow PQ$.poll()
4: **if** $V[e_u] == 1$ **then**
5: continue // 相遇点 e_u 已被添加过，丢弃并返回
6: **end if**
7: Pruning(u, e_u) // 剪枝优化
8: $u.C \Leftarrow \bigcup_{k=1}^{L} N(u, u.t, T, p_k)$ // 找出节点 u 的所有孩子节点
9: **for** each $c \in u.C$ **do**
10: computeECM(c) // 计算每个子节点的能耗指标 ECM
11: computeET(c) // 计算每个子节点的相遇时间 ET
12: **if** $V[e_c] == 0$ **then**
13: PQ.push(c) // 相遇点 e_c 未被添加，将子节点 c 插入优先级队列 PQ
14: **end if**
15: **end for**
16: insertPET($u, u.parent, e_u$) // 将节点 u 插入到功率感知相遇树中，父节点为 $u.parent$，相遇点为 e_u
17: set $V[e_u] = 1$
18: **if** $u == d$ **then**
19: break // 目的节点 d 被添加到 PET 中，构造过程结束
20: **end if**
21: **end while**
22: **return** PET

复添加。并且，由于 PAR 考虑了无人机的功率可调特性，因此它需要将无人机节点在所有不同功率级别下的相遇情况都考虑进去。所有的相遇点都有可能会被添加到功率感知相遇树中，这会导致 PAR 的解空间过大，从而降低路由协议的性能和效率。

为了克服上述问题，本节进一步地对功率感知相遇树的构建过程进行深入的分析，然后提出相应的剪枝优化机制。如4.3.1节所述，在图 4.1 中，至少有四条传输路径可以将消息 m 从无人机 u_1 传输到地面站 g_0。消息沿着传输路径 pa_1 和 pa_2 的投递时间均为 60 s，但是 pa_2 的能量消耗 $2E_e(p_1)+E_e(p_2)$ 要高于 pa_1 的能量消耗 $2E_e(p_1)$，这意味着传输路径 pa_2 不如传输路径 pa_1，因为 pa_2 在没有缩短消息 m 投递时间的前提下额外增加了能耗。PAR 更倾向于选择 pa_1 而不是 pa_2 作为消息最终的传输路径。

追根究底，这是因为消息 m 沿着 pa_2 传递给 u_3 所需要的能耗和时间都比沿着 pa_1 传输给 u_3 所需的能耗和时间高：沿着 pa_2 传递 m 给 u_3 的路径为 $u_1 \xrightarrow{e_1} u_2 \xrightarrow{c_1} u_3$，记作 pa_2'，它的 $ECM=E_e(p_1)+E_e(p_2)$ 以及 $ET=25s$; 而沿着 pa_1 传递 m 给 u_3 的路径为 $u_1 \xrightarrow{e_2} u_3$，记作 pa_1'，它的 $ECM=E_e(p_1)$ 以及 $ET=5s$。因此，不应该将 pa_2' 添加到功率感知相遇树中，即不应该把相遇点 c_1 添加到 pa_2 中，因为 pa_2' 在无助于消息 m 更快投递的同时还额外增加了能耗。类似地，沿着 pa_3 将消息 m 传输到 u_5 的路径为 $u_1 \xrightarrow{e_1} u_2 \xrightarrow{c_2} u_5$，记为 pa_3'，它的 $ECM=E_e(p_1)+E_e(p_2)$ 以及 $ET=25s$；而沿着 pa_4 将消息 m 传输到 u_5 的路径为 $u_1 \xrightarrow{e_1} u_2 \xrightarrow{e_3} u_4 \xrightarrow{e_5} u_5$，记为 pa_4'，它的 $ECM=3E_e(p_1)$ 以及 $ET=35s$。沿着 pa_3' 传输所需的能耗和时间均低于沿着 pa_4' 传输所需的能耗和时间，因此，后者需要被剪枝，即相遇点 e_5 不应该被添加到 pa_4 中。

基于以上全面深入的分析，本节进一步地提出了 PAR 的剪枝优化机制。对于每个节点 u 来说，由于其他节点可能和节点 u 在不同功率级别下相遇，因此 u 可以被多次添加到功率感知相遇树中。但是，每个相遇点只能被添加到功率感知相遇树中一次。假设节点 u 已经被添加到功率感知相遇树中 m 次，表示为 $U=\{u(e_1),u(e_2),\ldots,u(e_i),\ldots,u(e_m)\}$。那么，当节点 u 第 $m+1$ 次即将被添加到功率感知相遇树中时，记为 $u(e_{m+1})$，如果在功率感知相遇树中存在一个相遇点 e_i，其中 $u(e_i)\in U$, 通过相遇点 e_i 将消息 m 投递给 u 所需要的能耗和时间均低于通过相遇点 e_{m+1} 传输所需的总能耗和时间，即 $E_t(u(e_i).pa)\le E_t(u(e_{m+1}).pa)$ 且 $u(e_i).t\le u(e_{m+1}).t$，则本次相遇点 e_{m+1} 需要被剪枝，不应该被添加到功率感知相遇树中，这是因为相遇点 e_{m+1} 的插入既不能降低消息传输的总能耗，也无益于消息的及时投递。算法 4.2 总结了 PAR 的剪枝优化机制。

4.3.4 最优性证明

在介绍完 PAR 的主要工作流程和剪枝优化机制之后，本小节对 PAR 传输路径选择的最优性进行理论证明。

定理 4.1：当目的节点 d 首次被加入到功率感知相遇树 PET 时，其关联的传输路径 $d.pa$ 是满足延迟约束条件下能耗最小的传输路径。

算法 4.2 剪枝优化机制 Pruning

输入: 当前节点 u、关联相遇点 e_u

输出: 无

1: **for** $k \Leftarrow 1$ to m **do**
2: **if** $E_t(u(e_i).pa) \leq E_t(u(e_u).pa)$ and $u(e_i).t \leq u(e_u).t$ **then**
3: continue
4: **end if**
5: **end for**

证明: 假设存在另一条传输路径 $d.pa_1$，它在同样满足延迟约束的情况下能耗比 $d.pa$ 更少，即 $E_t(d.pa_1) < E_t(d.pa)$，那么存在以下两种情况：

(1) $d.pa_1$ 已经被添加到功率感知相遇树 PET 中。这与目的节点 d 是第一次被加入到功率感知相遇树的条件相矛盾。

(2) $d.pa_1$ 的部分或者全部仍然在优先级队列 PQ 中，还未添加到功率感知相遇树 PET 中。假设优先级队列 PQ 中 $d.pa_1$ 的部分为 $u.pa_1'$，则根据假设，$E_t(u.pa_1') \leq E_t(d.pa_1) < E_t(d.pa)$。但是，根据 PAR 构建功率感知相遇树的规则，优先级队列 PQ 中头节点的 ECM 是最小的。因此，当目的节点 d 从优先级队列 PQ 中取出并加入到功率感知相遇树中时，其关联的传输路径 $d.pa$ 的 ECM 是最小的，即 $E_t(d.pa) < E_t(u.pa_1') \leq E_t(d.pa_1)$。这与上述假设相矛盾。

因此，除了 $d.pa$ 之外，不存在其他在满足延迟约束的情况下能量消耗更低的传输路径，即 $d.pa$ 是满足消息延迟约束条件下能量消耗最小的传输路径。 □

基于以上分析，可以证明，如果存在满足要求的最优传输路径， PAR 总能找到这条路径，这保证了 PAR 的正确性和最优性。

4.3.5 实例举证

本节将详细说明功率感知相遇树的构建过程。不失一般性地，使用文献[102] 中的亚线性能量模型，即 $2E_e(p_1) > E_e(p_2)$；同时为了简洁直观地进行说明，设置 $E_e(p_1) = 1$、$E_e(p_2) = 1.5$。如图 4.1 所示，无人机 u_1 向地面站 g_0 发送一个数据包 m，其延迟约束为 $T = 45$ s, 图 4.2 展示了为消息 m 构建功率感知相遇树的过程。

首先，如图 4.2(a) 所示，将源消息节点 u_1 插入到优先级队列 PQ 中。第二步，如图 4.2(b) 所示，从优先级队列 PQ 中取出头节点 u_1 并将其添加到功率感知相遇树，作为相遇树的根节点。由于节点 u_1 会在 5 s 的时候于位置 e_2 以功率级别 p_1 与节点 u_3 相遇，在 10 s 的时候于位置 e_1 以功率级别 p_1 与节点 u_2 相遇，因此节点 u_2 和 u_3 是节点 u_1 的孩子节点。将 $u_3(e_2)$ 以及 $u_2(e_1)$ 加入到队列 PQ 中，此时 PQ 中的顺序为 $u_3(e_2)$、$u_2(e_1)$。第三步，如图 4.2(c) 所示，头节

点 $u_3(e_2)$ 被取出，由于它此前并没有被插入到相遇树中，将 u_3 插入，并将其与其父节点 u_1 通过有向边 e_2 连接。因为节点 u_3 在与其父节点 u_1 相遇之后，会在 25 s 的时候与节点 u_2 相遇、功率级别为 p_2、相遇点为 c_1，因此节点 u_2 可以作为 u_3 的孩子节点，将 $u_2(c_1)$ 插入到优先级队列 PQ 中，并对其中所有的节点进行排序，此时顺序为 $u_2(e_1)$、$u_2(c_1)$。值得注意的是，尽管节点 u_3 在与其父节点 u_1 相遇之后同样会与节点 g_0 相遇，但是由于它们两者之间的相遇时间为 60 s，大于延迟约束所规定的 45 s，因此 $g_0(e_4)$ 不会被添加到队列 PQ 中。

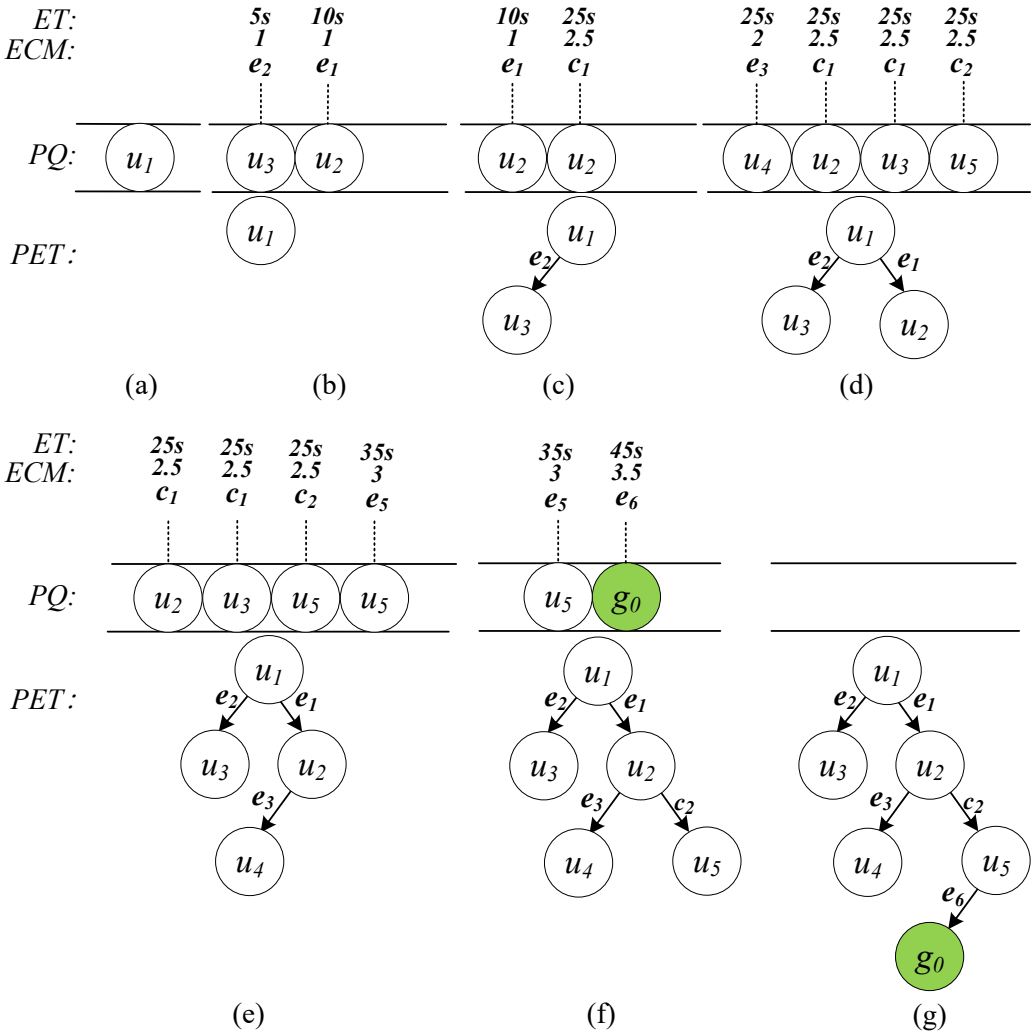


图 4.2　延迟约束 T = 45 s 时功率感知相遇树的构建过程

第四步，如图 4.2(d) 所示，头节点 $u_2(e_1)$ 被从优先级队列 PQ 中取出。由于相遇点 e_2 还未被添加，将 $u_2(e_1)$ 插入到到功率感知相遇树中，将节点 u_2 与其父节点 u_1 通过有向边 e_1 相连。在节点 u_2 与它的父节点 u_1 相遇之后，它将会在 25 s 与节点 u_4 相遇，相遇点为 e_3、功率级别

为 p_1。同时，它还会在 25 s 的时候以功率级别 p_2 分别与节点 u_3 和 u_5 相遇，相遇点分别为 c_1 和 c_2。因此，将 $u_4(e_3)$、$u_3(c_1)$、$u_5(c_2)$ 插入到队列 PQ 中。此时，优先级队列 PQ 中的顺序为 $u_4(e_3)$、$u_2(c_1)$、$u_3(c_1)$、$u_5(c_2)$。同理，如图 4.2(e) 所示，头节点 $u_4(e_3)$ 被从 PQ 取出并添加到功率感知相遇树中，其孩子节点 $u_5(e_5)$ 被添加到优先级队列 PQ 中，此时优先级队列 PQ 中的顺序为 $u_2(c_1)$、$u_3(c_1)$、$u_5(c_2)$、$u_5(e_5)$。

然后，从优先级队列 PQ 中取出头节点 $u_2(c_1)$，但是由于 $u_2(c_1)$ 的能耗和投递时间，即 $ECM = 2.5$、$ET = 25s$，均高于 $u_2(e_1)$，即 $ECM = 1$、$ET = 10s$，因此 $u_2(c_1)$ 不会被添加到功率感知相遇树中。接着，从优先级队列中取出下一个头节点 $u_3(c_1)$。同理，由于 $u_3(c_1)$ 的能耗和投递时间 ($ECM = 2.5$、$ET = 25s$) 都比 $u_3(e_2)$ 的能耗和时间 ($ECM = 1$、$ET = 5s$) 要高，因此 $u_3(c_1)$ 同样不会被加入到功率感知相遇树中。第五步，如图 4.2(f) 所示，头节点 $u_5(c_2)$ 从优先级队列 PQ 中取出并被加入到功率感知相遇树中。由于节点 u_5 将在 45 s 的时候与地面站 g_0 相遇，相遇点为 e_6，功率级别为 p_1，因此 $g_0(e_6)$ 是节点 u_5 的孩子节点，并被加入到优先级队列 PQ。同理，基于剪枝优化机制，$u_5(e_5)$ 也不会被添加到功率感知相遇树中。最终，如图 4.2(g) 所示，从优先级队列中取出头节点 $g_0(e_6)$ 并将其添加到功率感知相遇树中。此时，目的地节点 g_0 首次被添加到功率感知相遇树中，满足延迟约束且能耗最小的传输路径被找到：$u_1 \xrightarrow{e_1} u_2 \xrightarrow{c_2} u_5 \xrightarrow{e_6} g_0$，即 $(u_1, u_2, 10s, p_1), (u_2, u_5, 25s, p_2), (u_5, g_0, 45s, p_1)$。功率感知相遇树的构造过程结束。

上述实例展示了 PAR 的构造过程以及相应的剪枝优化机制，基于功率感知相遇树，PAR 可以找到一条延迟约束内到达目的地 g_0 的能耗最小的最优传输路径，该路径同时考虑了能量消耗和投递延迟，实现了高投递率和低能耗之间的双赢。

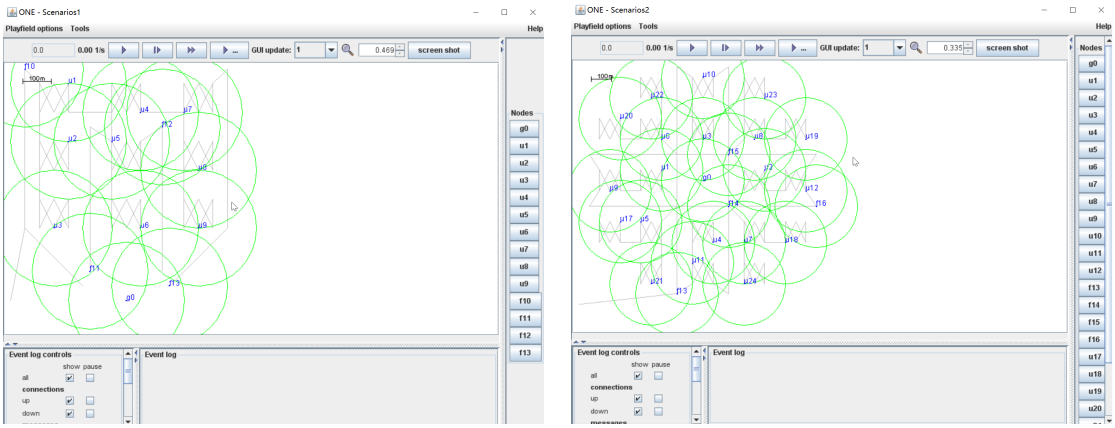
4.4 仿真实验与分析

本节使用机会网络模拟器 (Opportunistic Network Environment, ONE)[103,104] 通过仿真实验验证 PAR 路由性能，并对其进行扩展以支持无人机网络的多个功率级别。所有程序使用 Java 编写，运行在 Ubuntu 22.04.1 LTS 系统上，实验硬件平台为 Lenovo XiaoXin - 15ARE 2020 (AMD Ryzen 7 4800U with Radeon Graphics @ 1.80 GHz CPU，16 GB 内存，512 GB 固态硬盘)。

4.4.1 实验场景

参考文献[44] 中的实验场景，本节设计了两个具有不同网络规模的无人机灾后搜救任务场景。如图 4.3 所示，任务场景一由 9 架搜索无人机 ($u_1 \sim u_9$)、4 架摆渡无人机 ($f_{10} \sim f_{13}$) 以及 1 个固定的地面通信站 (g_0) 组成。每架搜索无人机负责一片选定的区域，大小为 200×200 m^2, 并且采用典型的“Z”字型运动模式，以高效地对任务区域进行覆盖搜索；而每架摆渡无人机则沿着类似于直线的航路来回飞行，以协助搜索无人机传输数据包、完成任务，同时它也可以执行搜索任务。任务场景二相对于任务场景一来说更为复杂，覆盖区域由 800×800 m^2 扩大到 1200

$\times 1200\ \mathrm{m}^2$，并且无人机网络由 20 架搜索无人机 ($u_1 \sim u_{12}$、$u_{17} \sim u_{24}$)、4 架摆渡无人机 ($f_{13} \sim f_{16}$) 以及 1 个固定的地面站 ($g_0$) 组成，其他实验设置与任务场景一相同。表 4.1 总结了详细的实验参数。



(a) 任务场景一　　(b) 任务场景二

图 4.3　两种任务场景仿真模拟图

4.4.2　评价指标

为了充分地验证 PAR 的路由性能，本章使用文献[44] 中的三种经典的路由算法作为对比协议：DTN_{geo}、DTN_{close} 以及 DTN_{load}，它们都是针对多跳无人机网络设计的路由协议，其中 DTN_{geo} 利用无人机的当前位置信息以及轨迹信息进行路由转发决策；DTN_{close} 则在 DTN_{geo} 的基础上对无人机的未来位置进行预测，从而进一步优化路由决策；而 DTN_{load} 则进一步考虑了无人机网络的负载，以此来优化路由协议的性能表现。为了全面地比较和验证不同协议的性能，本章采用以下性能指标：

(1) 数据包投递率 (Packet Delivery Ratio)：简称为投递率，它被定义为成功投递到目的地的数据包的数量除以网络中总生成的数据包的数量。此指标是路由协议可靠性的度量。

(2) 平均能耗 (Average Energy Consumption)：平均能耗是网络中将一个消息从源节点成功投递到目的地所需要的总能耗，它是消息经过的每一跳所发生的能耗的总和。

(3) 网络负载率 (Overhead Ratio)：在本章中，网络负载率的定义为：

$$Overhead = \frac{Sum_{relay} - Sum_{delivery}}{Sum_{delivery}} \tag{4.2}$$

其中 Sum_{relay} 是指所有消息在仿真实验期间被传输的次数，$Sum_{delivery}$ 则是指成功投递到目的地的消息的总个数。该指标主要用于评估路由协议的效率。

同时，为了避免单次实验引起的结果偏差，本章中所有实验都运行了 100 次，并计算平均

表 4.1　仿真实验参数设置

参数	任务场景一	任务场景二
仿真区域大小 (m^2)	800 × 800	1200 × 1200
无人机节点数量	13	24
仿真实验时间 (s)	480	
移动模型	MapRouteMovement	
无人机移动速度 (m/s)	4.5	
功率级别个数	4	
通信范围 (m)	200	
消息大小 (Byte)	1400	
链路吞吐量 (KB/s)	14	
每架无人机消息产生速率 (message/s)	6	
消息产生时间区间 (s)	0 ~ 400	
消息延迟约束 (s)	75	

值作为最终的实验结果。此外，由于 DTN_{geo}、DTN_{close} 以及 DTN_{load} 并没有考虑无人机的功率感知特性，因此对三者分别在每个固定功率级别上进行仿真实验，并选择最佳的仿真结果作为它们最终的实验结果。

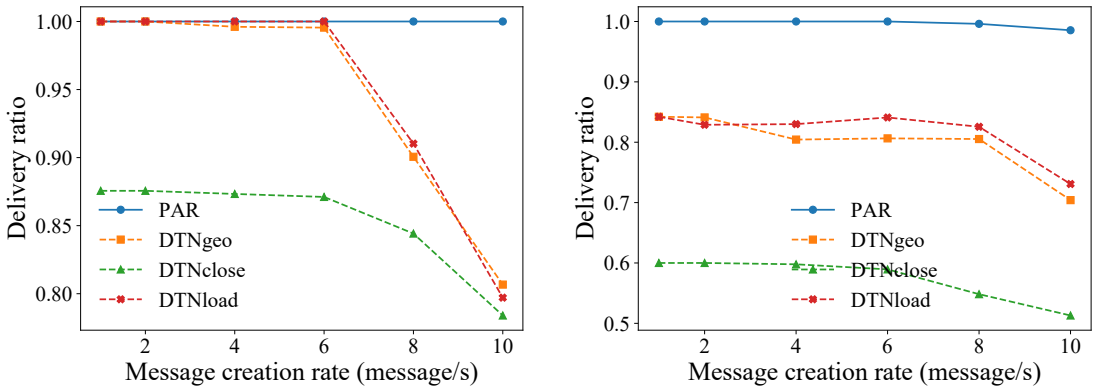
4.4.3　仿真实验结果分析

本节主要研究消息产生速率、无人机飞行速度以及消息延迟约束等变量对路由协议性能的影响。

4.4.3.1　消息产生速率对路由协议性能的影响

如图 4.4 所示，在两种任务场景下，PAR 均保持了最高的数据包投递率，尤其是当消息产生速率变得非常高时，PAR 明显优于另外三种路由协议；并且任务场景的扩大和复杂化使得对比路由协议的投递率均发生了显著的下降，而 PAR 则依旧能保持较高的投递率。这是因为 PAR 利用了无人机的功率感知特性和预先规划好的轨迹信息，提前为数据包计算出了传输路径，避免了局部最优，从而提高了数据投递率。

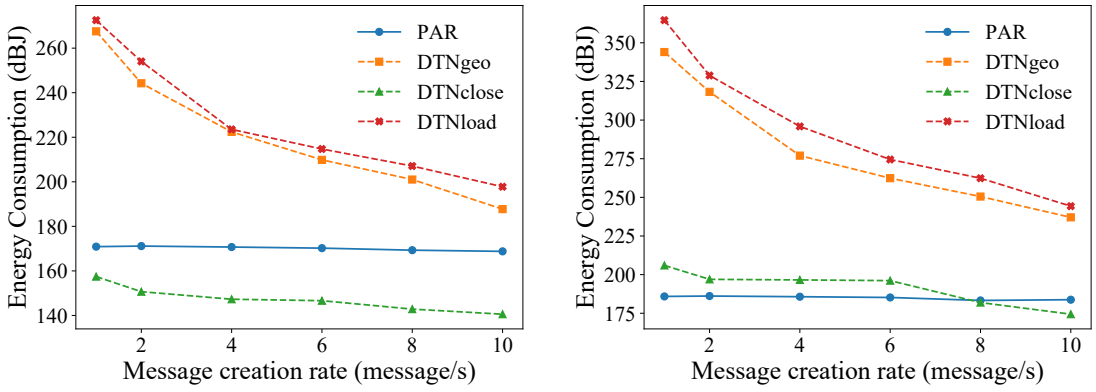
同时，如图 4.5 所示，PAR 的能耗远低于 DTN_{geo} 和 DTN_{load}，但在一些情况下要高于 DTN_{close}。但是值得注意的是，DTN_{close} 是以数据包投递率的牺牲作为代价的，如图 4.4 所示，DTN_{close} 的投递率在所有场景下均为最低；而 PAR 则是在尽量保证消息成功投递的前提下再



(a) 任务场景一　　(b) 任务场景二

图 4.4　消息产生速率对投递率的影响

考虑能耗的最小化。PAR 可以通过提高无人机的功率级别、增加能耗来保证消息的及时投递。如果消息不能被成功及时投递，那么所谓的能耗将毫无意义。此外，在两种任务场景中，四种路由算法的投递率和平均能耗都随着消息产生速率的增加而降低，这是因为消息产生速率的提升，一方面会快速消耗无人机网络的可用带宽资源，从而导致消息投递率的下降，另一方面也可以通过数据包排序技术将多个消息捆绑成报文串在一个竞争窗口期内统一进行传输，从而减小了单个数据包所需的能耗。

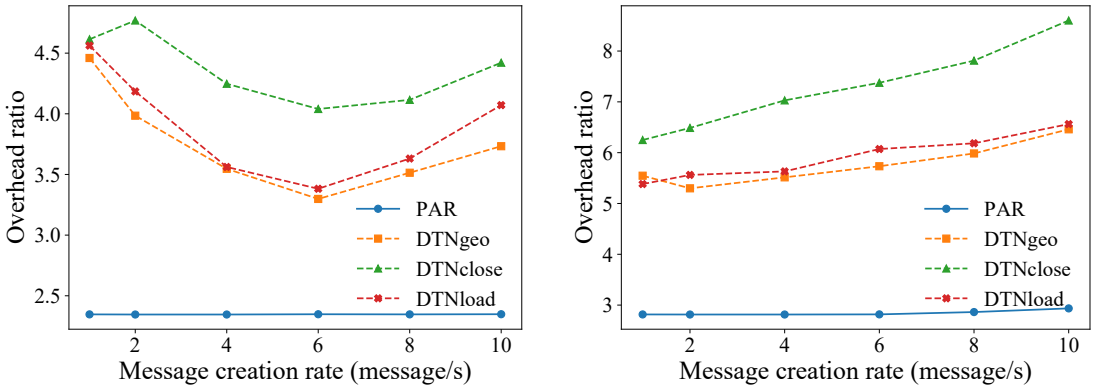


(a) 任务场景一　　(b) 任务场景二

图 4.5　消息产生速率对平均能耗的影响

对于网络负载率而言，如图 4.6 所示，PAR 达到了最小的网络负载，并且几乎不会随着消息产生速率发生波动。这是因为 PAR 预先计算了传输路径，然后根据这些计算出来的路径转发消息，没有进行冗余的转发，从而减少了消息转发的次数，降低了网络的负载。在任务场景一

中，三种对比算法的网络负载率均是先下降，在消息产生速率为 6 message/s 的时候达到最低，然后逐渐上升。这是因为三种算法的数据包投递率从消息产生速率为 6 message/s 的时候开始发生了显著下降，这导致了 $Sum_{delivery}$ 变小，因此 $Overhead$ 变大，如式 4.2 所示。而在任务场景二中，三种对比路由协议的网络负载率则呈现出逐渐上升的趋势，网络场景的复杂化、节点数量的增多以及单个节点消息产生速率的提升使得网络负载不断增大。



(a) 任务场景一　　(b) 任务场景二

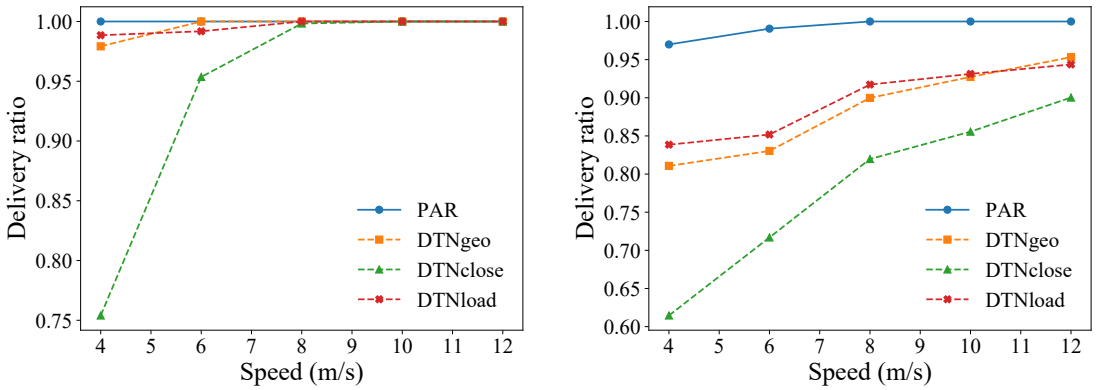
图 4.6　消息产生速率对网络负载率的影响

4.4.3.2　无人机飞行速度对路由协议性能的影响

如图 4.7 所示，四种算法的数据包投递率均随着无人机飞行速度的增加而增加。原因在于随着无人机飞行速度的增加，相同的时间窗口内无人机之间相遇的机会也会变多，因此消息的当前持有者在消息的延迟约束之内可以有更多和其他节点相遇的机会，从而有更多的机会选择合适的转发节点，同时，随着任务场景的扩大，三种对比路由协议的投递率均出现了不同程度的下降，但是可以看到 PAR 仍然保持着几乎完美的数据包投递率，这是因为当无人机飞行速度过低导致节点之间相遇机会过少时，PAR 动态调整无人机的功率以增加节点之间的相遇机会，从而提高数据包的投递率。

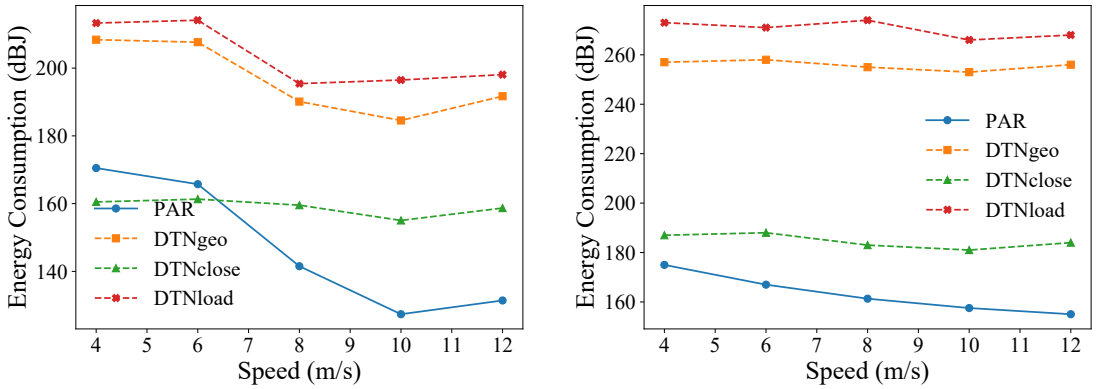
如图 4.8 所示，PAR 的能耗始终低于 DTN_{geo} 和 DTN_{load}，但是在任务场景一中，当无人机的飞行速度低于 8 m/s 时，PAR 的能耗要高于 DTN_{close}。这是因为 PAR 动态地调整无人机的功率级别以找到消息的高效传输路径；相反，DTN_{close} 并不能保证消息的及时投递。当 PAR 和 DTN_{close} 的数据包投递率相同时，可以发现 PAR 的能耗要远低于 DTN_{close}。此外，随着任务场景的扩大和复杂化，PAR 通过节点功率的动态调整在保持最高数据包投递率的同时达到了最低的传输能耗，展示了 PAR 性能的优越性。

对于网络负载率而言，如图 4.9 所示，PAR 始终保持着最低的网络负载，尤其是在任务场



(a) 任务场景一　　(b) 任务场景二

图 4.7　无人机飞行速度对投递率的影响



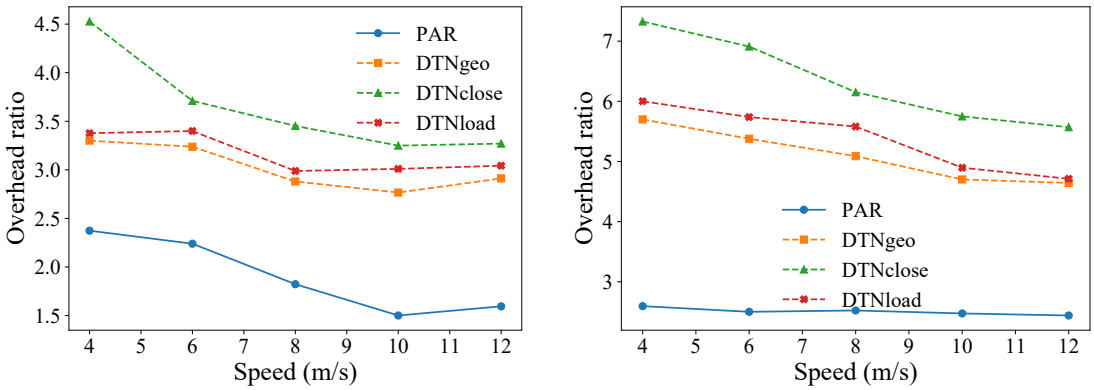
(a) 任务场景一　　(b) 任务场景二

图 4.8　无人机飞行速度对平均能耗的影响

景二中，PAR 的网络负载率甚至不到其他三种路由协议网络负载率的一半。同时所有算法的网络负载都随着无人机飞行速度的增加而减小。这是因为 $Sum_{delivery}$ 的增加以及 Sum_{relay} 的减小导致了 $Overhead$ 的降低，并且节点飞行速度的增加可以让消息以更短的延迟被成功投递到目的地，降低了网络的负载。

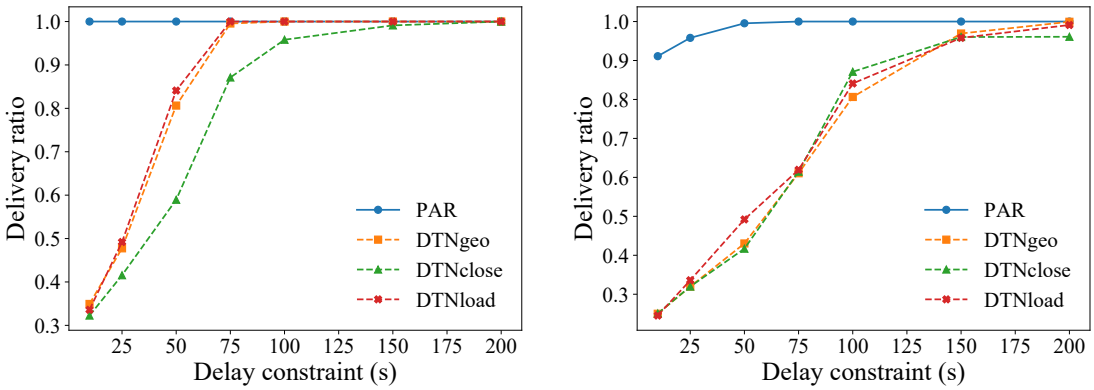
4.4.3.3　消息延迟约束对路由协议性能的影响

本小节探究消息延迟约束对路由协议性能的影响，消息的延迟约束从 10 s 逐渐增长到 200 s。如图 4.10 所示，在两种任务场景中，即使当延迟约束很小时，PAR 仍然能保持几乎完美的投递率，而三种对比路由协议的性能则出现了明显的波动，原因在于 PAR 可以通过增加无人机的功率级别来保证消息的及时投递。



(a) 任务场景一　　(b) 任务场景二

图 4.9　无人机飞行速度对网络负载率的影响

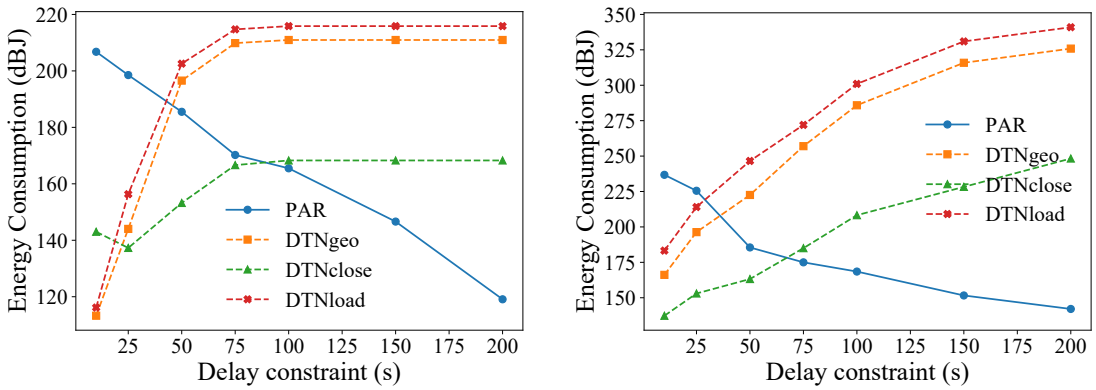


(a) 任务场景一　　(b) 任务场景二

图 4.10　消息延迟约束对投递率的影响

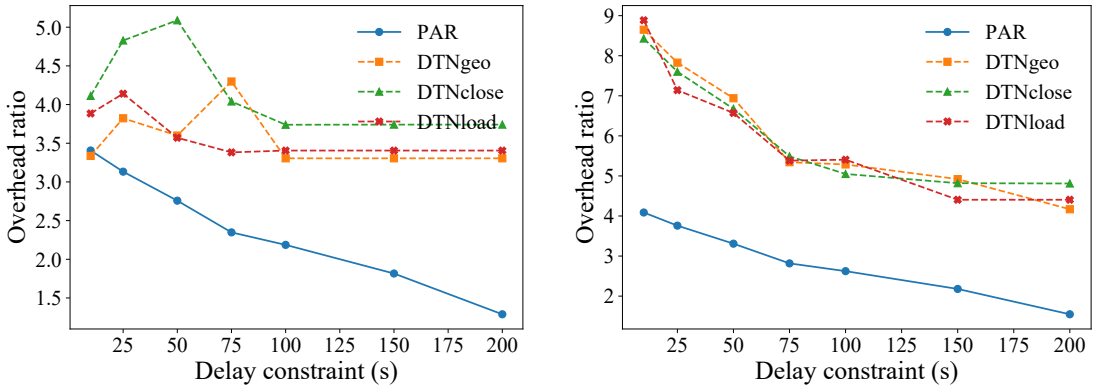
如图 4.11 所示，PAR 的能耗随着延迟约束的宽松逐渐降低，与其他三种对比路由协议的趋势完全相反。这是因为，当延迟约束很小时，PAR 为了保证消息的及时投递，不得不增加节点的传输功率，以增加能耗的方式尽量确保消息的及时投递。同时，随着消息延迟约束的逐渐宽松，PAR 逐步调整、降低无人机的功率级别来最小化能耗。任务场景一中，当 PAR 和其他三种路由协议的投递率相同时，PAR 的能耗明显小于三种对比算法；在任务场景二中，当延迟约束小于 75 s 时，PAR 以小幅度的能耗代价实现了投递率的大幅度领先，而当延迟约束大于 75 s 时，PAR 在保持更高投递率的同时达到了更低的能耗。

如图 4.12 所示，PAR 始终保持着最小的网络负载率，并且随着延迟约束的宽松逐步下降，这是因为 PAR 始终在满足延迟约束的前提下选择能耗最小的传输路径。同时，在任务场景一中，三种对比路由协议的网络负载随着延迟约束的宽松先上升后下降最后趋于稳定，这是因为当延



(a) 任务场景一　　(b) 任务场景二

图 4.11　消息延迟约束对平均能耗的影响



(a) 任务场景一　　(b) 任务场景二

图 4.12　消息延迟约束对网络负载率的影响

迟约束从 10 s 逐渐增加到 50 s 时，无人机之间的相遇机会大大增加，Sum_{relay} 急速增加，但延迟约束的苛刻使得消息的投递率并没有快速的提升，从而导致网络负载的提高；而随着延迟约束逐步从 50 s 增加到 100 s 时，数据包的投递率迅速增加，而此时无人机之间的相遇机会逐渐稳定，有效降低了网络的负载；最后投递率也趋于稳定，因此网络负载率几乎没有波动。在任务场景二中，三种对比路由协议的网络负载率随着延迟约束的宽松逐步下降，因为更大的延迟约束意味着路由协议有更多的投递时间，能够达到更高的数据包投递率，从而降低了网络负载。

4.5　本章小结

现有的无人机网络能耗高效路由协议大多基于非跨层的方式，仅利用网络层及其相邻协议层的信息来进行路由优化，导致网络性能不佳。本章提出了一种高效的功率感知的多跳无人机

网络路由协议 PAR 。首先，PAR 跨层联合物理层的功率感知特性以及预先规划的轨迹信息对无人机在不同可调功率级别下的相遇情况进行了计算。然后，结合应用层的 QoS 需求，以延迟约束和能耗最小化为原则，PAR 利用计算出的相遇信息构造功率感知相遇树 PET 。基于构造出的功率感知相遇树, PAR 找到最优传输路径，同时为传输路径上的每个转发节点选择合适的功率级别，以保证数据包及时投递的同时最小化传输能耗。实验结果表明，PAR 算法在多种任务场景下均能在保持较高数据投递率和较低网络负载的同时，节约大量的能量消耗。

第五章　抗延时攻击的多跳无人机网络安全路由协议

5.1　引言

无人机网络由于多跳、自组织、无中心等特点，使用方式非常灵活，然而，其分布式特性同时也使得它们容易受到各种安全威胁，包括外部攻击 (External Attacks) 和内部攻击 (Internal Attacks)[105]。网络内部恶意节点发起的内部攻击要比未经授权的外部无人机发起的外部攻击危害要大，例如攻击者可以入侵合法的无人机并出于特定的恶意目的进行各种类型的网络攻击，例如丢包攻击、泛洪攻击、重放攻击以及篡改攻击[106]。不幸的是，已经证明仅靠传统的通信加密和身份验证方案无法有效抵御内部攻击[107]。

延时攻击 (Time-Delay Attacks, TDAs) 是一种内部攻击，其中恶意节点在将接收到的数据包转发到目的地之前故意地延迟其传输。与其他类型的内部攻击相比，延时攻击的处理和解决更具挑战性，其对无人机网络的威胁也更大。延时攻击的特点是易于实施且难以检测：与需要破坏密码保护和篡改数据包的传统的基于数据驱动的攻击不同，延时攻击仅延迟数据包传输，而不会对数据包内容进行任何操纵和修改[108]。此外，与丢包、泛洪和重放等攻击不同，谨慎实施的延时攻击可能不会明显影响数据包的传输模式，引起数据包传输行为的显著改变[109]。

同时，延时攻击普遍存在于无人机网络的各种应用场景，并且可能造成重大的损害。无人机网络的许多时间敏感应用场景，例如森林监测[110]、交通监控[42]、视频会议[111]、灾难救援[112]、任务协调[6] 和战场网络[113]，涉及严格的对数据传输延迟的要求。数据必须被按时送达目的地；否则，它们的价值将大大降低甚至完全无效。例如，在森林火灾监测中，如果火灾报警信息被恶意延迟，可能会导致火势迅速蔓延，造成巨大的生命财产和生态资源损失[114]。此外，无人机网络的实时协作依赖于无人机之间定期交换编队控制和路由维护信息[115]。如果此类信息被恶意延迟，则可能导致编队控制混乱和失败（例如无人机碰撞）、路由路径过时和无效，甚至可能失去对无人机集群的控制[116]。

由于延时攻击的巨大威胁，必须开发有效的检测机制和安全路由机制，以保障无人机网络的任务效能和路由安全。然而，大多数现有工作都集中在丢包、泛洪、重放和篡改等攻击[70,71,117]的检测和防御上，对延时攻击的研究很少。此外，不幸的是，现有对延时攻击的少量研究也主要集中在有线网络和静态无线传感器网络[118–120]，而不是无人机网络。

与传统的无线传感器网络和移动自组织网络相比，无人机网络具有移动性强、分布稀疏、通信连接间断、链路质量不稳定等特点。这些特性可能导致无人机网络缺乏即时和稳定的端到端传输路径。因此，许多无人机网络基于存储-携带-转发机制来传递数据包[44,86,87]：当通信范围内没有合适的下一跳节点时，当前持有消息的无人机存储并携带该消息直到它遇到了合适的转发

无人机。上述这些特性使得现有的延时攻击检测方法不适用于高度动态的无人机网络。

据了解，目前还没有针对无人机网络中延时攻击检测的研究。在无人机网络中实现延时攻击检测的挑战是多方面的：(1) 由于拓扑高度动态和通信连接间歇，数据包的传输路径和投递延迟变化迅速、波动频繁、差距较大。因此，无法通过投递延迟的显著波动来检测恶意延时攻击。(2) 由于存储-携带-转发机制，攻击者注入的相对较短的恶意延迟很可能被误判为正常的无人机存储携带行为。(3) 由于复杂的网络环境及其高度动态性，许多因素都会影响数据包和节点的转发延迟，导致难以构建精确的数学或关系模型。

为了克服上述这些问题，本章首先构建了无人机网络中延时攻击的数学模型，据了解这是首次在无人机网络中研究和检测延时攻击。然后，本章提出了一个整体跨层的延时攻击检测框架 (A Holistic Cross-Layer Time-Delay Attack Detection Framework for UAV Networks, HOTD)，并基于此提出了一个抗延时攻击的多跳无人机网络安全路由协议 (A Secure Routing Protocol Against Time-Delay Attacks for UAV Networks)。为了实现高效准确的延时攻击检测，HOTD 对节点的转发延迟而不是消息的投递延迟进行评估。首先，由于转发延迟与无人机网络协议栈的每一层，即物理层、数据链路层、网络层和应用层，都息息相关，HOTD 对这些层可用的信息进行整体收集，然后从跨层的角度来选择延迟相关的特征。随后，监督学习被利用来在所选特征和相应转发延迟之间建立一致性模型以计算网络中每个节点的一致性程度。最后，根据节点的一致性程度使用聚类方法来区分恶意节点和良性节点。同时，基于上述评估结果，抗延时攻击的安全路由协议对相应的恶意节点采用路由隔离机制以确保无人机网络的路由安全。

5.2 系统模型

本节对系统模型进行形式化，首先对无人机网络模型进行描述，然后对无人机网络中延时攻击进行建模并对其特异性进行阐明。

5.2.1 网络模型

与第四章相似，本章同样以无人机网络执行灾后搜救任务为示例应用场景，同时将无人机网络从三维空间抽象为欧几里得空间[101]。无人机的飞行轨迹由地面控制单元在执行任务前预先规划；在执行任务期间如果某架无人机需要动态调整并重新规划轨迹，地面站可以提前获得其最新的轨迹信息，并通过带外信道将这些轨迹同步给相关无人机[85,99]。与第四章不同的是，为了便于针对无人机网络的延时攻击进行研究，本章不再考虑无人机的功率动态感知与调整，因此在本章中，无人机的传输功率固定。基于预先规划的轨迹信息，地面站可以计算出无人机之间的相遇情况[87]。同时为了便于表示，本章将无人机之间的通信抽象为一个相遇点 (Encounter Point)[86]。如图 5.1 所示，无人机网络由四架无人机 u_1、u_2、u_3、u_4 以及一个地面站 g_0 组成。每架无人机沿着各自预先规划的的轨迹飞行，如图中各箭头所示。同时，无人机之间会不定时地

相遇以及进行数据通信，例如，无人机 u_1 和 u_2 在 10 到 14 s 之间会在位置 e_1 相遇，这意味着无人机 u_1 和 u_2 可以在 10 到 14 s 之间互相通信；无人机 u_2 和 u_3 在 23 到 25 s 之间会在位置 e_2 相遇，以此类推。

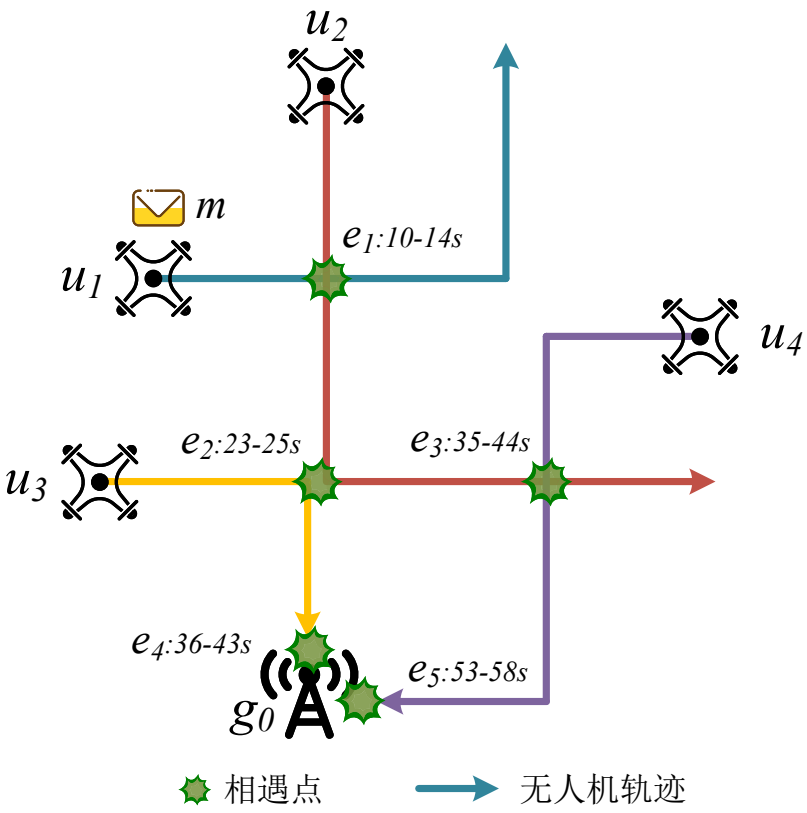


图 5.1　无人机网络示例

5.2.1.1　节点模型

本章假设网络中存在以一定概率执行延时攻击的恶意无人机，而地面站是从无人机收集数据包的可信机构[31]。为方便起见，本章中出现的“无人机”和“节点”均代表网络中的无人机。此外，一个节点可以被表示为：

$$Node =< id, P_{TDA} >, \tag{5.1}$$

其中 id 代表网络中各节点的编号，例如图 5.1 中的 u_1 和 u_2；P_{TDA} 则是节点发起延时攻击的概率：对于良性节点而言，$P_{TDA} = 0$；而对于恶意节点而言，$0 < P_{TDA} \leq 1$。

5.2.1.2 路径模型

无人机网络节点分布的稀疏性以及通信连接的间断性使得节点之间可能并不存在即时稳定的端到端路由路径，节点需要以存储-携带-转发的方式将数据包逐跳投递给其他节点。因此，本章将数据包 m 的传输路径形式化为：

$$\begin{aligned} Path = &\langle (node_1, node_2, t_1^s, t_2^r), (node_2, node_3, t_2^s, t_3^r), \ldots, \\ &(node_i, node_{i+1}, t_i^s, t_{i+1}^r), \ldots, (node_n, node_{n+1}, t_n^s, t_{n+1}^r) \rangle, \end{aligned} \tag{5.2}$$

其中 $node_1$ 和 $node_{n+1}$ 分别指代消息的源节点和目的节点；t_i^s 表示节点 $node_i$ 开始向节点 $node_{i+1}$ 发送消息 m 的时间；t_{i+1}^r 则表示节点 $node_{i+1}$ 成功从节点 $node_i$ 接收到消息 m 的时间；并且 $t_{i+1}^r - t_i^s = t_{trans}$，其中 t_{trans} 是将消息 m 从节点 $node_i$ 成功传输到节点 $node_{i+1}$ 所花费的时间。

例如，如图 5.1 所示，无人机 u_1 在开始时（即 0 s）生成消息 m 并希望将其发送给地面站 g_0。为方便起见，本章假设消息传输每一跳所需要的时间为 1 s，即 $t_{trans} = 1$ s。根据预先规划的轨迹信息，可以推断出存在一条传输路径，即 $\langle (u_1, u_2, 10, 11), (u_2, u_3, 23, 24), (u_3, g_0, 36, 37) \rangle$。无人机 u_1 在 10 到 11 s 之间于位置 e_1 遇到无人机 u_2，并将消息 m 传输给无人机 u_2。然后，无人机 u_2 存储并携带消息 m，直到其在 23 到 24 s 之间于位置 e_2 遇到无人机 u_3，然后将消息 m 传输给无人机 u_3。最后，无人机 u_3 在 36 到 37 s 之间于位置 e_4 遇到地面站 g_0，并将消息 m 传输给地面站 g_0。

5.2.2 延时攻击模型

与之前的研究类似[31,32,76,106,121]，本章假设攻击者具备相应的能力可以入侵无人机并利用它们发起延时攻击，恶意延迟数据包的传输，持续时间为 τ s。设 $t_i^{s\prime}$ 表示恶意节点 $node_i$ 实施延时攻击后开始向节点 $node_{i+1}$ 传输消息 m 的时间；$t_{i+1}^{r\prime}$ 表示经过恶意延迟后，$node_{i+1}$ 从 $node_i$ 成功接收 m 的时间。在传统的有线网络和静态无线传感器网络中，延时攻击的模型可以形式化为：

$$t_i^{s\prime} = t_i^s + \tau, \tag{5.3}$$

$$t_{i+1}^{r\prime} = t_{i+1}^r + \tau. \tag{5.4}$$

然而，由于存储-携带-转发机制，上述模型并不总是适用于无人机网络。为方便起见，假设每个无人机在持有消息 m 后总是将其传输给它所遇到的第一个无人机。因此，在无人机网络不存在恶意节点的情况下，消息 m 的传输路径为 $\langle (u_1, u_2, 10, 11), (u_2, u_3, 23, 24), (u_3, g_0, 36, 37) \rangle$。

然后，假设节点 u_2 是恶意节点并执行延时攻击。当 $\tau = 1$ s 时，传输路径变为 $\langle (u_1, u_2, 10, 11), (u_2, u_3, 24, 25), (u_3, g_0, 36, 37) \rangle$，与上述攻击模型一致。随后，当 $\tau = 3$ s 时，根据式 5.3，$t_2^{s\prime}$ 应该是 $23 + 3 = 26$ s。但是，如图 5.1 所示，在 26 s 的时候没有无人机可以与节点 u_2 通信，u_2 不得不

存储并携带消息 m 直到它在位置 e_3 遇到无人机 u_4，然后在另一次延时攻击之后将消息 m 传输给无人机 u_4。因此，消息 m 的传输路径变为 $\langle(u_1,u_2,10,11),(u_2,u_4,38,39),(u_4,g_0,53,54)\rangle$。此时，$t_2^{s\prime}=38\text{ s}\gg 26\text{ s}$。在这种情况下，延时攻击改变了数据包原来的传输路径。此外，尽管延时攻击的持续时间仅为 3 s，但是消息 m 的投递延迟增加了 $17\text{ s}\gg 3\text{ s}$。因此，无人机网络的独特特性以及存储-携带-转发机制使得延时攻击变得更具破坏性。

当 $\tau=10\text{ s}$ 时，没有传输路径可以将消息 m 从 u_1 传输到 g_0。在这种情况下，延时攻击对数据包投递所产生的不利影响相当于丢包攻击。然而，延时攻击仅延迟数据包的传输以阻止数据包的及时投递，而在丢包攻击中恶意中继节点则会随机丢弃接收到的数据包，这会造成数据传输通路的意外中断。此外，现有研究已经表明丢包攻击可以很容易地被检测和甄别[31,117]，而延时攻击则更加隐蔽、难以检测。

总而言之，与传统的有线网络和静态无线传感器网络不同，无人机网络中的延时攻击模型可以形式化为：

$$t_i^{s\prime}=\begin{cases}t_i^s+\tau, & \text{if } \tau+t_{trans}\le t_{dur(i,i+1)},\\ t_{ste(i,i+1)}{}'+\tau, & \text{otherwise,}\end{cases}\tag{5.5}$$

$$t_{i+1}^{r}{}'=t_i^{s\prime}+t_{trans},\tag{5.6}$$

其中 $t_{dur(i,i+1)}$ 表示节点 $node_i$ 和 $node_{i+1}$ 之间相遇的持续时间；$t_{ste(i,i+1)}{}'$ 代表节点 $node_i$ 和 $node_{i+1}{}'$ 相遇的开始时间，其中 $node_{i+1}{}'$ 为根据路由协议[44]选择出的最合适的下一跳节点，并且 $node_{i+1}{}'$ 需满足 $\tau+t_{trans}\le t_{dur(i,i+1)}{}'$。

5.3 整体跨层的延时攻击检测框架 HOTD

5.3.1 主要工作流程

图 5.2 显示了 HOTD 的主要工作流程，包括信息收集、特征选择、模型训练和恶意节点检测。

(1) 信息收集：传输的消息被利用来收集信息。无人机节点在对消息进行处理和转发的同时会附加一些日志信息，主要由自身的延迟相关信息构成。最终，所有中继转发节点的日志信息随着消息的投递一同被地面站接收，以作进一步的分析和处理。

(2) 特征选择：在地面站接收到消息之后，会对消息进行整体全面的分析，然后从跨层的角度选择每一层（即物理层、数据链路层、网络层和应用层）的延迟相关的特征。

(3) 模型训练：基于每一层的延迟相关特征，监督学习模型被利用来在这些选择的特征和相应的转发延迟之间构建一个一致性模型。

(4) 恶意节点检测：节点的每一次转发行为都基于训练好的一致性模型进行评估，据此可以获得每个节点的一致性程度。然后，聚类算法被利用来根据节点的一致性程度来区别恶意节点

和良性节点。

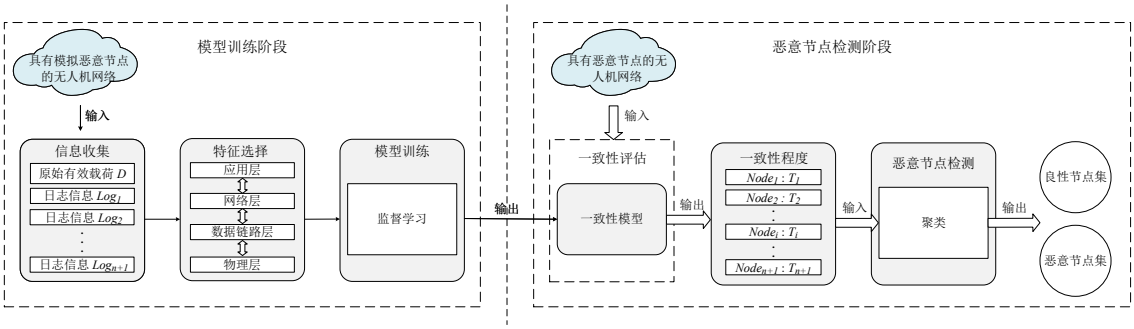


图 5.2　HOTD 的主要工作流程

5.3.2　信息收集

为了在无人机网络的每一层有效地收集延迟相关的信息，节点在转发消息的同时将它们的延迟相关信息附加到消息中。传输的消息可以形式化为：

$$M =< D, Log_1, Log_2, \ldots, Log_i, \ldots, Log_{n+1} >, \tag{5.7}$$

$$Log_i =< id, RT_i, RD_i, RS_i, RB_i, RL_i, TP_i, LQ_i, ST_i, SD_i, SS_i, SB_i >, \tag{5.8}$$

其中 D 是消息 M 的原始有效载荷；Log_i 表示节点 $node_i$ 附加到消息 M 中的传输日志信息，主要由节点 $node_i$ 的延迟相关信息构成；RT_i (ST_i) 为节点 $node_i$ 接收（发送）消息 M 的时间；RD_i (SD_i) 表示节点 $node_i$ 接收（发送）消息 M 时，节点 $node_i$ 与 $node_{i-1}$ ($node_{i+1}$) 之间的距离；RS_i (SS_i) 是表示节点 $node_i$ 接收（发送）消息 M 时的飞行速度的向量；RB_i (SB_i) 为节点 $node_i$ 接收（发送）消息 M 时的缓冲区占用；RL_i 表示当节点 $node_i$ 接收到消息 M 时，消息 M 的剩余存活时间 (Time To Live, TTL)；TP_i 和 LQ_i 则分别表示节点 $node_i$ 的传输功率和链路质量。

尽管信息收集方法在消息中附加了一些与延迟相关的信息，但是它在存储方面仍然是轻量级的。本节实现了一个消息原型来进一步地分析消息附加引入的额外开销。首先，本节使用 7 bits 对 id 进行编码，以便网络可以支持 2^7 架无人机。然后，假设无人机网络可执行长达 2 小时的任务[122]，因此 RT_i、RL_i 以及 ST_i（单位为秒）可以用 13 bits 进行编码。接下来，假设无人机有 7 个可调功率级别，因此 TP_i 由 3 bits 编码。最后，为了准确反映通信双方的相隔距离、飞行速度、缓冲区占用以及链路质量，RD_i、RS_i、RB_i、LQ_i、SD_i、SS_i 以及 SB_i 采用 8 bits 编码。因此，每个转发节点在报文中附加的传输日志信息总占用的大小为 $7 + 13 \times 3 + 3 + 8 \times 7 = 105$ bits ≈ 13 B。

同时，如5.5.8节所示，实验结果也证实了本章收集方法的轻量级特性。在任何情况下，信息附加所引入的额外开销都不超过 2.5%。此外，如果采用有效的存储优化方案或者数据压缩方

法[123]，可以进一步地降低存储和传输成本，例如除了源节点记录完整的时间戳之外，消息传输路径上的其他转发节点可以只记录相对时间戳，以减少额外的开销[124]。

5.3.3 特征选择

由于无人机网络复杂的环境架构以及众多独特的特性，必须对延迟相关的信息进行全面、系统的分析，探索可能揭示攻击者不当行为的措施和方案。但是，无人机网络拓扑高度动态、通信连接间歇，这导致数据包的传输路径和投递延迟变化迅速、波动频繁、差距较大，无法通过投递延迟的显著波动来检测恶意延时攻击。因此，为了准确有效地评估和识别网络中各个节点的行为，本章遍历接收到的每个消息的传输路径并提取所有两跳子路径，可以形式化为：

$$Path \Rightarrow \bigcup_{i=2}^{n} \langle (node_{i-1}, node_i, t_{i-1}^s, t_i^r), (node_i, node_{i+1}, t_i^s, t_{i+1}^r) \rangle. \tag{5.9}$$

例如，无人机 u_1 在 0 s 的时候生成消息 m 并希望将其发送给地面站 g_0，如图 5.1 所示。当网络中没有恶意节点时，消息 m 的传输路径为 $\langle (u_1, u_2, 10, 11), (u_2, u_3, 23, 24), (u_3, g_0, 36, 37) \rangle$。该路径可以被分为两个两跳子路径：$\langle (u_1, u_2, 10, 11), (u_2, u_3, 23, 24) \rangle$ 以及 $\langle (u_2, u_3, 23, 24), (u_3, g_0, 36, 37) \rangle$。然后，对于消息 m 的每个两跳子路径，表示为 $\langle (node_{i-1}, node_i, t_{i-1}^s, t_i^r), (node_i, node_{i+1}, t_i^s, t_{i+1}^r) \rangle$，本章从跨层的角度选择每一层的延迟相关特征来评估节点 $node_i$ 的行为和表现。

5.3.3.1 物理层

物理层主要负责为无人机网络中的数据传输提供物理无线通信信道。然而，由于拓扑结构的高度动态性以及通信连接的间歇性，无人机网络中数据包的传输缺乏即时的端到端路径，其依赖于节点之间的动态连接。此外，节点之间不稳定的链路质量会显著影响转发延迟，而物理层可用的无线信道参数则可以很好地反映链路质量。因此，物理层信息的利用有利于评估当前通信信道的状态，抵抗丢包和重传等因素对时延的影响。

本章选择信干噪比作为物理层信道参数的代表，因为它综合考虑了信号强度、传输干扰以及背景噪声。此外，利用通信双方的传输距离可以很好地估计数据传输所需的传播延迟，同时结合数据链路层的功率控制、差错控制以及拥塞控制可以进一步地对当前的信道状态进行评估，从而更准确地评估数据包的转发延迟。因此，如表 5.1 所示，最终选择的物理层特征为 $RxDist$、$SndDist$ 以及 LQ，可以表示为：

$$PFS = (RxDist, SndDist, LQ). \tag{5.10}$$

5.3.3.2 数据链路层

数据链路层主要负责数据错误控制和拥塞控制；在无人机网络中，可以从该层中获取与节点相关的信息。数据链路层中延迟相关信息的选择可以有效地抵抗拥塞对转发延迟的影响，从而准确地评估节点的行为。

数据链路层的信息可以在一定程度上反映转发延迟。例如，无人机的缓冲区占用率反映了它们当前的流量负载和消息排队延迟；而节点的发射功率在一定程度上决定了节点的链路质量和通信范围，这与消息的传播延迟有关。

此外，使用数据链路层中延迟相关信息可以评估节点的行为并帮助检测延时攻击。例如，恶意节点由于实施延时攻击，当它们持有数据包且与其他合适的转发节点相遇时，它们并不会立即对持有的数据包进行转发，而是会延迟数据包的传输。这种延时攻击行为往往会导致恶意节点比正常节点持有更多的数据，从而使得其缓冲区占用率高于正常节点，导致与正常转发延迟之间的不一致。

如表 5.1 所示，数据链路层最终选取的特征为 $RxBufOcc$、$SndBufOcc$、$BufSize$ 以及 $TxPwr$，可以表示为：

$$MFS = (RxBufOcc, SndBufOcc, BufSize, TxPwr). \tag{5.11}$$

5.3.3.3 网络层

网络层的目标是为节点提供稳定的数据通信，可以在该层获得用于表征消息和端到端传输路径的信息。提取网络层中与延迟相关的特征有助于评估转发延迟并识别恶意节点。例如，传输延迟（即消息的第一位和最后一位离开发送节点之间的时间）取决于数据包的大小；同时，消息 TTL 的利用有助于进一步地评估节点的转发延迟。

此外，选择消息的源节点、目的节点以及消息类型作为特征，能够更好地检测和识别一系列针对特定条件和功能的更为智能的延时攻击，例如针对特定源节点[76] 或者特定目的节点[32] 或者特定消息类型的选择性攻击。将这些特征与其他延迟相关的特征相结合，能够更加细粒度地对节点的行为进行检测、对延时攻击进行识别。

因此，如表 5.1 所示，HOTD 选取的网络层特征为 $MsgSize$、$RemTTL$、$MsgSrc$、$MsgDst$ 以及 $MsgType$, 可以表示为：

$$NFS = (MsgSize, RemTTL, MsgSrc, MsgDst, MsgType). \tag{5.12}$$

5.3.3.4 应用层

应用层为用户提供服务并表征应用程序的客观实体。在无人机网络中，该层基于数据管理和处理进行进一步地分析和利用。

对于消息 m 的每一个两跳子路径，表示为 $\langle (node_{i-1}, node_i, t^s_{i-1}, t^r_i), (node_i, node_{i+1}, t^s_i, t^r_{i+1}) \rangle$，则节点 $node_i$ 相对于消息 m 的转发延迟 t^i_{fd} 可以形式化为：

$$t^i_{fd} = t^r_{i+1} - t^s_{i-1}. \tag{5.13}$$

然而，由于无人机网络独特的存储-携带-转发机制，t_{fd}^{i} 不仅包括消息的传输延迟，还包含了无人机节点 $node_i$ 存储和携带此消息的时间。例如，对于两跳子路径 $\langle(u_1,u_2,10,11),(u_2,u_3,23,24)\rangle$ 而言，如图 5.1 所示，节点 u_2 是良性节点，它的转发延迟为 t_{fd}^{2} = 24 s −10 s = 14 s，其中包含 2 s 的传输延迟以及 12 s 的无人机存储携带时间（从 11 到 23 s）。

因此，如果直接使用转发延迟 t_{fd}^{i} 作为模型训练的输入，无人机存储和携带数据包的时间，记为 t_{sc}^{i}，会极大地影响训练后的一致性模型的性能。为了消除这一持续时间的不利影响，本章利用在应用层获得的预先规划的轨迹信息来对这一时间进行估计，然后将其作为一个特征来构建与转发延迟 t_{fd}^{i} 之间更好的一致性模型。t_{sc}^{i} 被用来评估无人机存储和携带数据包的持续时间，它被形式化为：

$$t_{sc}^{i} = t_{ste(i,i+1)} - t_{i-1}^{s}, \tag{5.14}$$

其中 $t_{ste(i,i+1)}$ 代表节点 $node_i$ 和 $node_{i+1}$ 之间相遇的开始时间。例如，如图 5.1 所示，节点 u_2 和 u_3 之间相遇的开始时间为 23 s。因此，t_{sc}^{2} = 23 s −10 s = 13 s。然后，假设 u_2 是一个恶意节点并实施延时攻击。当 τ = 1 s 时，相应的两跳子路径为 $\langle(u_1,u_2,10,11),(u_2,u_3,24,25)\rangle$，此时，$t_{fd}^{2}$ = 25 s −10 s = 15 s 以及 t_{sc}^{2} = 23 s −10 s = 13 s。此外，当 τ = 3 s 时，传输路径变为了 $\langle(u_1,u_2,10,11),(u_2,u_4,38,39),(u_4,g_0,53,54)\rangle$；相应的两跳子路径也发生了变化，变为 $\langle(u_1,u_2,10,11),(u_2,u_4,38,39)\rangle$，这和原始的传输路径不同。此时，$t_{fd}^{2}$ = 39 s −10 s = 29 s $\gg t_{sc}^{2}$ = 13 s。因此，如果节点 $node_i$ 是攻击者并实施了延时攻击，则 t_{fd}^{i} 和 t_{sc}^{i} 之间会出现不一致，尤其是当延时攻击更改了原始的传输路径的时候。

此外，将无人机的飞行速度和方向与其他层的延迟相关信息，例如物理层的传输功率，相结合，可以进一步地估计未来一段时间内节点之间的链路质量和通信范围[44]。

如表 5.1 所示，应用层最终选择的特征为 t_{sc}^{i}、$RxDir$、$RxSpd$、$SndDir$ 以及 $SndSpd$，可以表示为：

$$AFS = (t_{sc}^{i}, RxDir, RxSpd, SndDir, SndSpd). \tag{5.15}$$

同时，为了消除特征之间的维度影响并进一步提高一致性模型的性能表现，本章进行了特征归一化，即 Z-score 归一化 (Z-score Normalization)[125]：

$$\mathbf{x}' = \frac{\mathbf{x} - \bar{\mathbf{x}}}{\sigma}, \tag{5.16}$$

其中 $\mathbf{x}$ 是原始特征向量，$\bar{\mathbf{x}}$ 是平均特征向量，σ 是标准差。特征归一化有利于避免异常值，并增加样本之间的差异性和特征之间的区分度。

5.3.4 模型训练

本章利用监督学习来构建一致性模型以检测无人机网络中的延时攻击。为了获得足量有标签的良性样本和恶意样本来训练一致性模型，本章在模型训练之前将数据包注入到无人机网络

之中，同时驱动一些良性节点来模拟恶意节点的延时攻击行为，即以一定的概率实施延时攻击。地面站对这些注入的数据包进行收集、分析，从而获得相关的良性样本和恶意样本，这些带有标签的数据样本被用于一致性模型的训练和构建。

表 5.1　选定特征

特征	描述
t_{sc}^{i}	节点 $node_i$ 存储携带消息 m 的预计持续时间
$RxSpd$	节点 $node_i$ 从 $node_{i-1}$ 接收消息 m 时的速度
$RxDir$	节点 $node_i$ 从 $node_{i-1}$ 接收消息 m 时的方向
$SndSpd$	节点 $node_i$ 在将消息 m 发送给 $node_{i+1}$ 时的速度
$SndDir$	节点 $node_i$ 在将消息 m 发送给 $node_{i+1}$ 时的方向
$MsgSize$	消息 m 的数据包大小
$RemTTL$	当节点 $node_i$ 从 $node_{i-1}$ 接收到消息 m 时消息 m 的剩余 TTL
$MsgSrc$	消息 m 的源节点
$MsgDst$	消息 m 的目的节点
$MsgType$	m 的消息类型
$RxBufOcc$	节点 $node_i$ 从 $node_{i-1}$ 接收消息 m 时的缓冲区占用
$SndBufOcc$	节点 $node_i$ 在将消息 m 发送给 $node_{i+1}$ 时的缓冲区占用
$BufSize$	节点 $node_i$ 的缓冲区大小
$TxPwr$	节点 $node_i$ 的传输功率
$RxDist$	当节点 $node_i$ 从 $node_{i-1}$ 接收到消息 m 时 $node_i$ 和 $node_{i-1}$ 之间的距离
$SndDist$	当节点 $node_i$ 将消息 m 发送给 $node_{i+1}$ 时 $node_i$ 和 $node_{i+1}$ 之间的距离
LQ	当节点 $node_i$ 将消息 m 发送给 $node_{i+1}$ 时 $node_i$ 和 $node_{i+1}$ 之间的链路质量参数

具体来说，本章对所有注入数据包的传输路径进行遍历，并提取出所有的两跳子路径来研究和识别传输路径上各个节点的转发行为。对于每个两跳子路径来说，通过分析转发节点 $node_i$ 的延迟相关特征来获得训练样本 z，可以被表示为 $z=(\mathbf{x},y)$，其中 $\mathbf{x}=(PFS,MFS,NFS,AFS,t_{fd})$；$y$ 则表示 $\mathbf{x}$ 的分类标签：如果 $node_i$ 的转发行为是良性的，则标记 y 为 0；否则，$node_i$ 的转发行为是恶意的，y 被标记为 1。经过一段时间的数据采样后，获得了由良性和恶意样本组成的、有标记的训练数据集，这些样本与监督学习一起被用于训练本章的一致性模型。

5.3.5 恶意节点检测

在获得训练好的一致性模型后，一致性模型被用于识别恶意节点并检测延时攻击。对于网络中的每个节点，评估其所有转发行为从而计算并获得它们的一致性程度。节点 $node_i$ 的一致性程度可以表示为：

$$C_i = \frac{bf_i}{bf_i + mf_i}, \tag{5.17}$$

其中 bf_i 和 mf_i 分别表示 $node_i$ 的良性和恶意转发行为的数量；C_i 必须是 0 到 1 之间的实数，它最初被设置为 0.5，其中 $bf_i = mf_i = 1$，这表示本章假设在初始阶段对节点的行为和类型完全无知，持有中立态度。

恶意节点检测过程如下：首先，以与模型训练阶段相同的方式分析每个接收到的数据包以获取检测样本。但是，与训练阶段不同的是，此时获得的所有样本都是没有标签的。对于每个未标记的样本，使用训练好的一致性模型确定当前转发节点 $node_i$ 的延迟相关特征是否与其相应的转发延迟一致。如果此样本被标记为一致，则节点 $node_i$ 的本次转发行为被判定为是良性的，同时 bf_i 增加 1；否则，样本被判定为是不一致的且节点的行为是恶意的，因此 mf_i 增加 1。最后，获得了每个节点的一致性程度，并通过聚类方法以区分出恶意节点和良性节点。聚类算法的输出是良性和恶意节点集。

5.4 抗延时攻击的安全路由协议

如相关工作所示，无人机网络应用场景丰富、路由协议种类众多，需要根据具体的应用场景使用不同的路由协议。然而，延时攻击普遍存在于无人机网络的各种应用场景，并且可能对无人机网络产生巨大的威胁、造成严重的损害，仅设计一种特定的安全路由协议不能满足无人机网络的实际应用需求。

因此，本节在 HOLO 跨层路由优化框架的指导下，基于 HOTD 延时攻击检测框架，设计了一种通用的抗延时攻击的安全路由协议 (A Secure Routing Protocol Against Time-Delay Attacks for UAV Networks)，它可以和任意的无人机网络高效路由协议相结合，并且适用于不同的无人机应用场景。

无人机网络在进行数据包传输与投递的同时需要根据 HOTD 的要求向数据包中添加延迟相关的信息。地面站作为从无人机收集数据包的可信机构，具有丰富的计算、通信、存储等资源，同时部署着延时攻击检测模型，对收集到的数据包进行实时分析，并基于 HOTD 进行恶意节点的分类与确认。此外，对于每一个通信周期而言，地面站周期性地将恶意节点与良性节点的判定结果通过带外信道或泛洪机制对整个无人机网络进行广播，以确保所有无人机都成功接收到此分类消息。无人机在进行消息转发的路由决策时，首先根据分类结果对邻居节点进行筛选，以剔除被判定为恶意的邻居节点，然后基于所部署的高效路由协议的路由决策机制，选择出合

适的转发节点进行消息传输；如果良性邻居节点为空，且根据路由机制无遇到良性节点的机会或者其预期成本过高，则当前节点在不排除恶意节点的情况下直接根据路由策略选择最合适的转发节点，同时当前节点保留消息的副本，如果以后与良性节点相遇且此时该消息仍未被确认接收，则节点在满足路由策略的情况下对该消息的副本继续进行转发。无人机网络基于 HOTD 的抗延时攻击安全路由协议的路由过程如算法 5.1 所示。

5.5 仿真实验与分析

本章使用机会网络模拟器[103,104] 通过模拟实验来评估和分析 HOTD 以及安全路由协议的性能。路由协议使用 Java 编写，机器学习相关由 Python 实现，两者均运行在 Ubuntu 22.04.1 LTS 系统上，实验硬件平台为 Lenovo XiaoXin - 15ARE 2020 (AMD Ryzen 7 4800U with Radeon Graphics @ 1.80 GHz CPU，16 GB 内存，512 GB 固态硬盘)。

5.5.1 实验场景

与第四章相似，本章受森林监测任务和军事战斗网络[44,126] 的启发为无人机网络设计了两个模拟场景，具备不同的实验区域大小、无人机数量以及无人机的部署位置。每架无人机负责 200×200 m^2 的区域，使用典型的锯齿形运动模式并沿着预先规划的轨迹飞行来有效地覆盖区域。同时，地面站是一个可信机构，而网络中存在实施延时攻击的恶意节点。表 5.2 总结了默认的实验参数设置。

5.5.2 实验设置

为了深入评估 HOTD 以及安全路由协议的性能，本章在无人机网络中的四种经典路由协议上进行了广泛的实验：Epidemic[127]、SprayAndWait[128]、Prophet[129] 以及 MaxProp[130] 路由。由于缺乏对无人机网络中延时攻击检测的研究，本章将 HOTD 与网络物理系统 (Cyber Physical Systems, CPSs) 以及精确时间协议 (Precision Time Protocol, PTP) （即静态网络）中最先进的延时攻击检测方案进行了对比，以证明延时攻击在无人机网络中的独特性以及 HOTD 的高效性。同时，为了衡量安全路由协议的性能表现，本章对四种经典的路由协议在三种不同网络状态下的性能进行实验对比：(1) 正常运转：网络中不存在恶意节点和延时攻击 (Router-NonTDA)；(2) 网络中存在恶意节点实施延时攻击但没有部署相应的安全路由协议 (Router-TDA-None)；(3) 网络中存在恶意节点实施延时攻击且部署有相应的安全路由协议 (Router-TDA-HOTD)。

本章使用文献[109] 中先进的基于深度学习的方法来表征和检测 CPS 中的延时攻击。分层长短期记忆 (Hierarchical Long Short-Term Memory, HLSTM) 模型是一种数据驱动的方法，用于处理连续的数据流以及描述延时攻击的特征。随后，利用一个深度学习模型作为分类模块来检测延时攻击。由于该方法与攻击的位置无关，即不考虑攻击具体发生的位置，因此本章利用该方

算法 5.1 抗延时攻击的安全路由协议

输入: 地面站接收消息集 $Messages$、高效路由协议 ERP、当前传输消息 M

输出: 无

地面站 g:

BNS, MNS = HOTD ($Messages$) // 基于接收到的消息利用 HOTD 对节点分类

if $t == T$ **then**

  broadcast (BNS, MNS) // 周期性地广播良性和恶意节点集

  $t = 0$

end if

无人机 u:

$BNeighbor = Neighbor - MNS$ // 隔离恶意的邻居节点

if $BNeighbor \neq \emptyset$ **then**

  for each $m \in \{M\} \cup CCQ$ **do**

    SFN = ERP ($BNeighbor$, m) // 根据部署的高效路由协议进行路由决策选择合适的转发节点

    if $SFN \neq \emptyset$ **then**

      forward (m, SFN) // 执行消息转发

      delete (m) // 删除本地消息

    else

      storeAndCarry (u, m) // 转发失败，无人机存储携带消息

      CCQ.push(m) // 将消息添加到无人机的携带副本队列中

    end if

  end for

else if $BNeighbor == \emptyset$ && P (ERP, u, M) == 0 **then**

  SFN = ERP ($Neighbor$, M) // 良性邻居节点为空且根据 ERP 路由机制判定无遇到良性节点的机会, 则不执行恶意节点隔离

  forward (M, SFN)

  storeAndCarry (u, M) // 无人机存储携带消息的副本

  CCQ.push(M) // 将消息副本添加到无人机的携带副本队列中

else

  storeAndCarry (u, M)

  CCQ.push(M)

end if

表 5.2　默认仿真实验参数设置

	任务场景一	任务场景二
仿真区域大小 (m^2)	800 × 800	1200 × 1200
无人机节点数量	13	24
移动模型	MapRouteMovement	
通信范围 (m)	200	
无人机飞行速度 (m/s)	6	
消息大小 (Byte)	1400	
链路吞吐量 (KB/s)	14	
链路质量	1.0	
单架无人机的消息产生速率 (s)	5	
消息延迟约束 (s)	50	
延时攻击概率	0.3	
延时攻击时长 (s)	3	
恶意节点占比	0.3	
通信周期 (s)	240	

法分别对每个无人机节点进行单独识别。同时，由于该方法是一种在线检测方法，为确保公平性，本章将该方法的检测反应延迟设定为实验的结束时间，也就是说，该方法只需要在实验结束时识别出恶意节点。其他所有使用的参数都是文献[109]中的默认值。

基于先前的基础工作[119]，文献[131]对 PTP 中的延时攻击进行了全面的分析和总结，然后对延时攻击的影响进行了建模和量化。基于 PTP 中主时钟和副时钟之间通信路径的对称性假设，该方法准确地模拟了延迟特性，并通过观察和计算主时钟 (Primary Clocks) 和副时钟 (Secondary Clocks) 之间的偏移来检测延时攻击。本章使用该方法来描述和检测 PTP 中的延时攻击。

5.5.3　性能指标

为了衡量和比较检测性能，本章使用如表 5.3 所示的混淆矩阵，其中真阳性 (True Positive, TP) 和真阴性 (True Negative, TN) 代表延时攻击的正确检测；而假阴性 (False Negative, FN) 和假阳性 (False Positive, FP) 则是不正确的检测。检测方法的敏感性和特异性分别对应于假阳性率 (False-Positive Rate, FPR) 和假阴性率 (False-Negative Rate, FNR) 的避免。本章使用准确率 (Accuracy Rate, ACC)、假阳性率和假阴性率作为性能指标，并定义为 $ACC = (TP+TN)/(TP+FP+FN+TN)$、

$FPR = FP/(FP+TN)$ 以及 $FNR = FN/(FN+TP)$。

表 5.3　混淆矩阵

		预测情况	
		恶意	良性
真实情况	恶意	真阳性 (TP)	假阴性 (FN)
	良性	假阳性 (FP)	真阴性 (TN)

同时，为了进一步地评估安全路由协议的性能表现，本章使用数据包投递率 (Packet Delivery Ratio)、平均投递延迟 (Average Delay) 以及网络负载率 (Overhead Ratio) 作为性能指标，其中数据包投递率和网络负载率的定义和4.4.2节中所定义的一样，而平均投递延迟表示将数据包从源节点成功投递到目的地所需要的时间。此外，为了避免单次实验导致的结果偏差，本章中每个实验都运行了 100 轮，并计算平均值作为最终的实验结果。

5.5.4　算法组合对比

HOTD 的性能依赖于监督学习和聚类算法的组合，因此本节进行实验以研究 HOTD 下不同算法组合对无人机网络中延时攻击的检测准确率。本章选择了四种典型的监督学习算法：支持向量机[132]、多层感知机 (MultiLayer Perceptron, MLP)[133]、卷积神经网络 (Convolutional Neural Network, CNN)[134] 和循环神经网络 (Recurrent Neural Network, RNN)[135]；以及四种经典的聚类算法：K 均值聚类 (K-means Clustering)[136]、凝聚层次聚类 (Agglomerative Nesting Hierarchical Clustering, AGNES)[137]、高斯混合模型 (Gaussian Mixed Model, GMM)[138] 和谱聚类 (Spectral Clustering)[139]。

MLP 模型由一个输入层、一个全连接层（有 10 个隐藏神经元）和一个输出层组成。CNN 模型包括两个 1D-CNN（过滤器分别为 64 和 128、卷积核为 4）、一个扁平层、一个全连接层（有 256 个隐藏的神经元，激活函数为校正线性单元 ReLU）、一个随机失活层（失活率为 0.5）和一个全连接层（激活函数为 SoftMax）。RNN 模型由以下部分组成：一个门控递归单元 (Gated Recurrent Unit, GRU) 和一个全连接层。

实验结果如图 5.3 和 5.4 所示。可以发现 CNN + GMM 算法的性能优于其他算法组合。一方面，基于共享卷积核，CNN 可以很好地处理高度复杂的无人机网络数据，并且它已经被证明可以有效地检测 WSN 中的恶意节点[140,141]。CNN 的卷积层可以自动进行特征提取，这使得 CNN 适用于具有复杂结构以及众多延迟相关特征的无人机网络。此外，CNN 的全连接层缓解了过度拟合，同时减少了特征信息的损失。另一方面，GMM 聚类考虑了数据的均值和方差，并使用

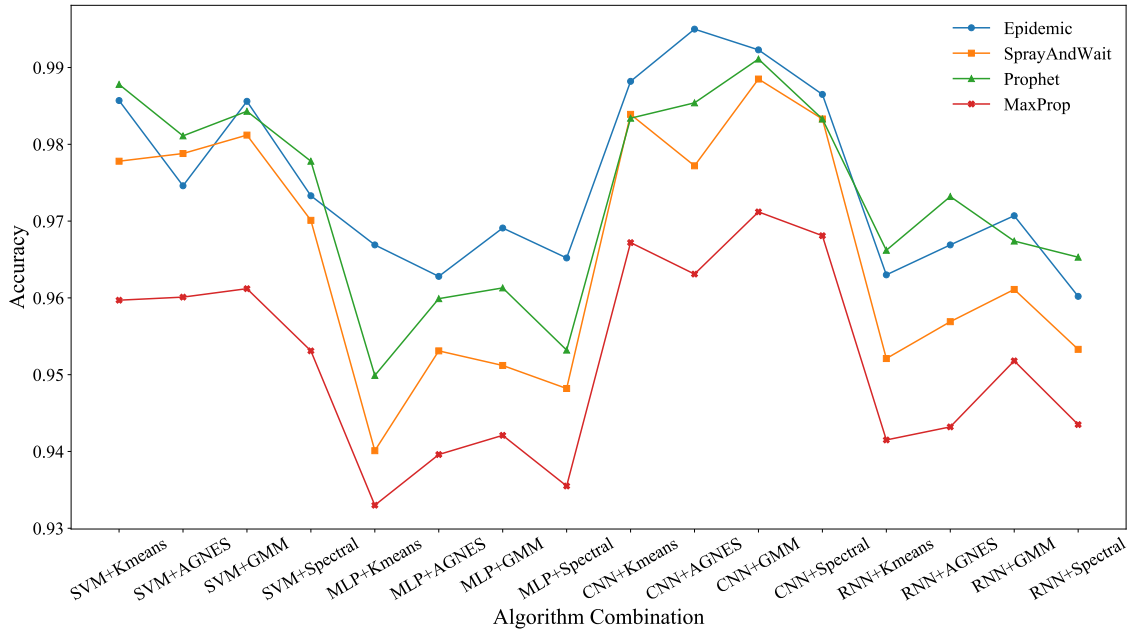


图 5.3　任务场景一中不同算法组合对检测准确率的影响

最大期望 (Expectation-Maximization, EM) 算法来迭代更新模型参数，从而达到更高的精度。此外，GMM 采用了概率模型，即软分类，从而比其他聚类方法提供了更多的灵活性。

值得注意的是，所有的算法组合在两个场景和四种路由协议中都取得了良好的检测性能（超过 90%），这表明 HOTD 的广泛适用性。由于本研究的篇幅限制，本章选择 CNN+GMM 算法来代表 HOTD 进行实验。

5.5.5　检测性能比较

本节将 HOTD 与目前 CPS[109] 和 PTP[131] 中的最先进的延时攻击检测方案进行对比，实验结果如表 5.4 所示。HOTD 始终可以在保持低 FPR 和低 FNR（均低于 10%）的同时取得良好的准确率（高于 95%）。在无人机网络的延时攻击场景中，HOTD 的性能要远远高于针对 CPS 和 PTP 中延时攻击的检测方法。其原因如下：首先，由于无人机网络结构复杂，HOTD 对无人机网络协议各层的信息进行了整体分析，然后从跨层的角度提取各层与延迟相关的特征，实现了对延时攻击全面准确的特征描述。其次，HOTD 在这些特征与相应的转发延迟之间构建了一个一致性模型，以有效评估网络中每个节点的转发行为。第三，网络中每个节点的一致性程度可以根据对各个节点的转发行为的评估来计算。然后，HOTD 利用聚类算法对节点进行分类，这减轻了单次的评估偏差对总体结果的影响。

如表 5.4 所示，CPS 中的方法[109] 在任务场景一中表现良好，但是在任务场景二中性能出现了急剧下降。这表明 CPS 中的延时攻击检测方法在高度动态且环境复杂的无人机网络中的可

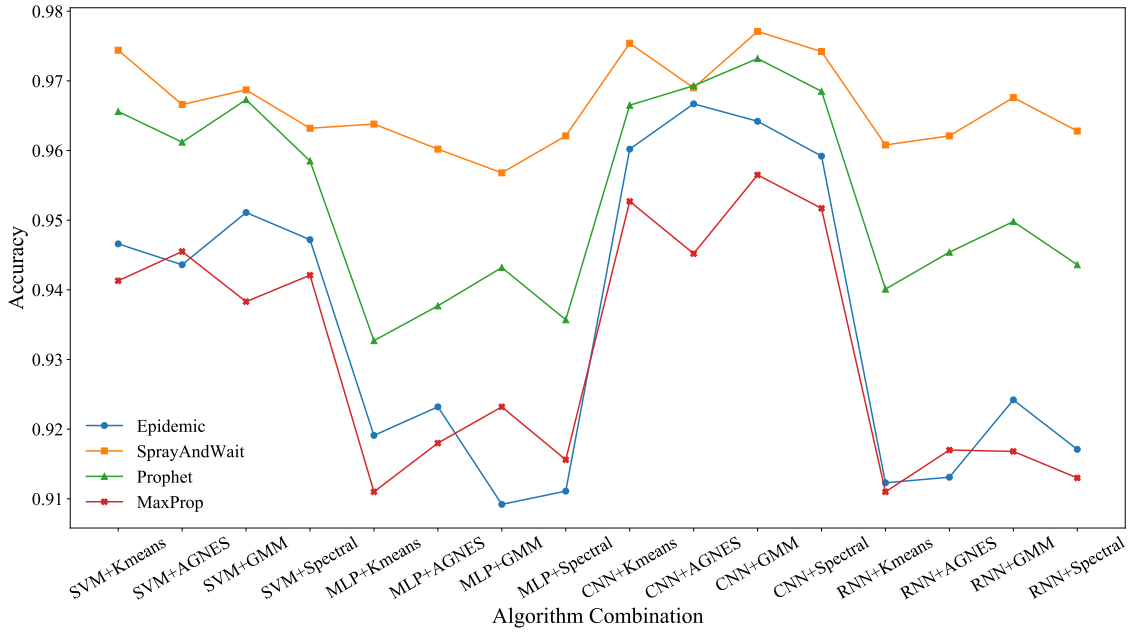


图 5.4　任务场景二中不同算法组合对检测准确率的影响

扩展性较差。因此，它们不能适应实际应用场景中规模逐渐扩大、环境日益复杂的无人机网络。同时，可以发现虽然该方法的 FNR 较低，但是其 FPR 非常高，这表明虽然该方法很少遗漏恶意节点，但它同时也将许多的良性节点误判为恶意节点，产生了大量的误报，在实际应用中这是非常令人困扰的。原因在于在 CPS 中，报文的传输路径是固定的，每个节点的数据包是序列、连续的。因此，该方法使用 LSTM，能够准确地捕获时间序列中的依赖关系和特征来检测延时攻击。然而，由于无人机网络的高度动态性，报文的传输路径也随之在不断变化。同时，对于单个节点而言，它所传输的数据包之间并没有绝对的密切相关性，相邻传输的数据包可能是毫无关联的，并且数据包之间也没有相应的时序依赖关系。因此，LSTM 无法学习识别无人机网络中恶意节点的有效行为模式。

表 5.4 的结果显示，PTP 中延时攻击的检测方法同样不适用于无人机网络。在两种任务场景的四种路由协议下，该方法[131] 的检测准确率约为 50%，同时在大多数情况下，其 FPR 和 FNR 高达 50%，这表明该方法完全不能区分和检测出无人机网络中的延时攻击。这是因为 PTP 假设主节点和次要节点之间的通信路径是对称的，同时现有针对 PTP 中延时攻击的检测方法均依赖于这一假设。但是由于无人机网络的拓扑高度动态，这一假设在无人机网络中并不成立。此外，由于 PTP 的结构相对简单，其只与时间特征有关，因此该检测方法只需要提取和处理与延迟相关的时间信息，而无需考虑其他因素。然而，由于无人机网络的环境架构极其复杂，许多因素都会影响节点和消息转发延迟，很难对这种复杂的关系进行准确地建模。

表 5.4　不同检测方案的实验结果

		任务场景一 (Router)				任务场景二 (Router)			
		Epidemic	*SprayAndWait*	*Prophet*	*MaxProp*	*Epidemic*	*SprayAndWait*	*Prophet*	*MaxProp*
HOTD (本章)	*ACC*	0.9923	0.9885	0.9911	0.9712	0.9642	0.9771	0.9732	0.9565
	FPR	0.0094	0.0211	0.0132	0.0277	0.0357	0.0206	0.0223	0.0613
	FNR	0.0076	0.0393	0.0178	0.0293	0.0368	0.0329	0.0532	0.0542
Ganesh 等人[109]	*ACC*	0.9724	0.9224	0.8149	0.8506	0.6616	0.7523	0.5457	0.6071
	FPR	0.0322	0.0557	0.1538	0.2442	0.5782	0.3596	0.6513	0.6663
	FNR	0.0193	0.1081	0.2746	0.0186	0.0751	0.0156	0.1398	0.0663
Moussa 等人[131]	*ACC*	0.5352	0.5035	0.5773	0.5100	0.5047	0.5651	0.5758	0.4994
	FPR	0.3857	0.4509	0.3150	0.4718	0.5139	0.3381	0.3111	0.5381
	FNR	0.6124	0.5654	0.6908	0.5181	0.4755	0.6563	0.6825	0.4602

5.5.6　路由协议性能分析

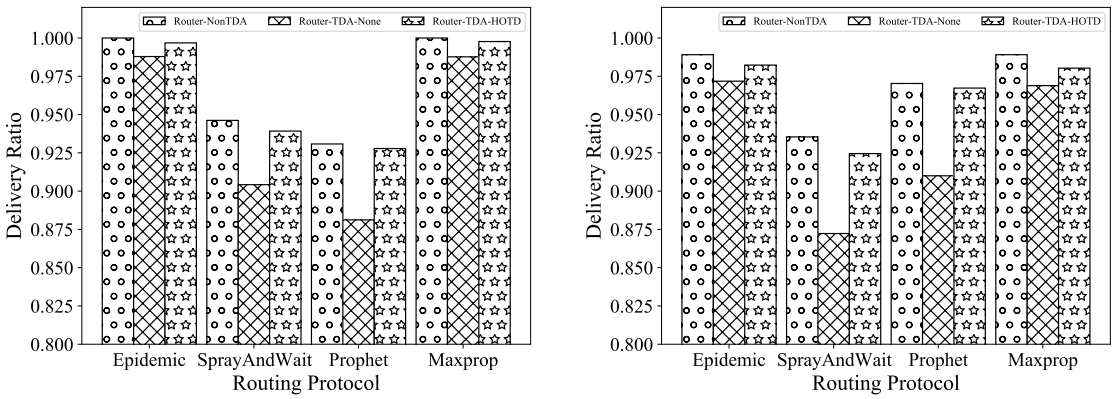
本节在两种任务场景及四种经典路由协议下对抗延时攻击的安全路由协议的性能进行分析, 实验结果如图 5.5、5.6 和 5.7 所示。

由于 Epidemic 和 MaxProp 路由协议都是基于泛洪机制的，即持有消息的无人机发送消息的副本给每一个与其相遇的无人机，因此这两种路由协议的投递率最高、平均延迟最低，但同时由于大量转发消息的副本导致两者的网络负载也是最高的。而延时攻击的存在则在降低数据包投递率以及增加数据包平均延迟的同时极大地增加了网络的负载。原因在于延时攻击使得恶意节点不再立即转发数据包，而是更倾向于延迟对消息的处理和转发，使得消息在网络中更大规模地泛洪，这导致网络中充斥着大量消息的副本，极大地增加了网络的负载。通过采用本章所提出的抗延时攻击的安全路由协议，可以发现能够在进一步减小延时攻击对数据包投递率和平均延迟的影响的同时，极大地降低无人机网络的负载，如图 5.7 所示。

SprayAndWait 路由协议是在 Epidemic 和 MaxProp 路由协议的基础上对网络中消息副本的最大数量进行限制。可以发现持续时间为 3 s 的延时攻击的存在使得两种任务场景下该路由协议的数据包投递率的下降高达 4% 和 6%，数据包的平均延迟增加了 4 s，同时网络负载也有所增加。这是因为在对消息副本的数量进行限制之后，由于无人机网络的特性，延时攻击对消息的延迟传输极大地影响了消息的按时投递。

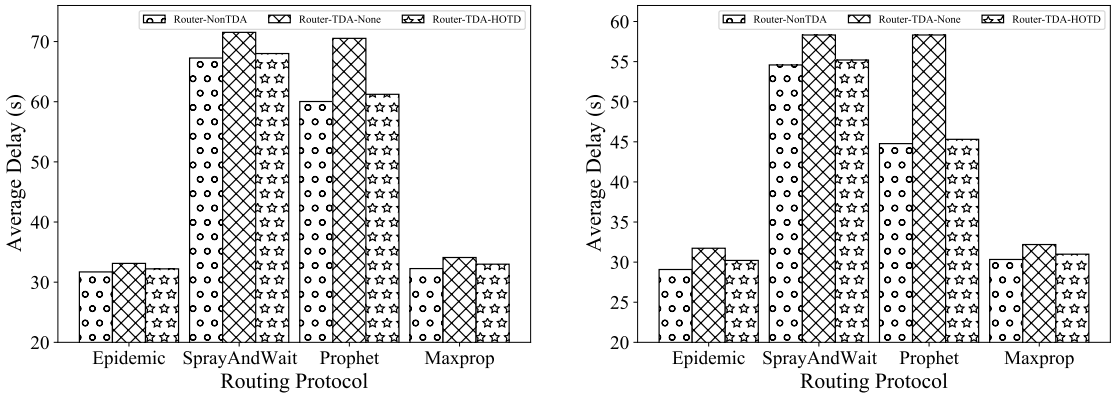
Prophet 路由协议基于节点的历史相遇信息进行路由决策，与上述三种路由协议不同的是，此时网络中仅存在消息的唯一副本，现有为无人机网络设计的路由协议的基本机制构造均与该路由协议相似。实验结果显示延时攻击在该路由协议上产生了巨大的危害，造成了投递率的下降、平均延迟的上升以及网络负载的增加。值得注意的是，无人机网络采用该路由协议时，网

络中 30% 的恶意节点实施的时长为 3 s 的延时攻击却造成数据包的平均延迟在两种任务场景下分别增加了约 10 s 和 14 s，同时数据包投递率的下降也高达 6%，体现出延时攻击对无人机网络的危害。通过在该路由协议上部署抗延时攻击的安全路由协议，可以极大地降低延时攻击对无人机网络的影响，如图 5.5、5.6 和 5.7 所示，抗延时攻击的安全路由协议通过采用路由隔离机制，极大地降低了延时攻击的影响：数据包投递率的下降从原本的 6% 减小到 1% 以内，同时平均延迟控制在 1 s 以内，此外对网络负载的影响也实现了大幅度的降低。



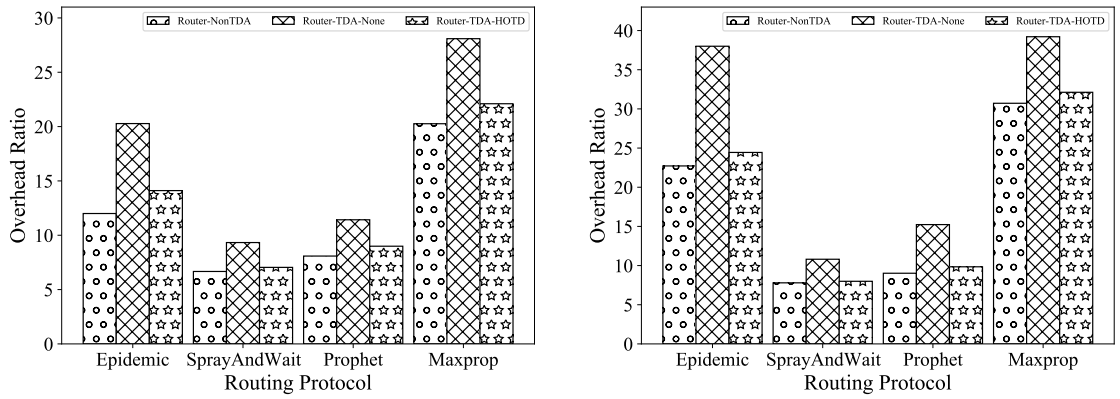
(a) 任务场景一　　(b) 任务场景二

图 5.5　延时攻击对路由协议投递率的影响



(a) 任务场景一　　(b) 任务场景二

图 5.6　延时攻击对路由协议平均延迟的影响



(a) 任务场景一　　(b) 任务场景二

图 5.7　延时攻击对路由协议负载率的影响

5.5.7　特征影响

本节研究了 HOTD 中不同特征对检测准确率的贡献和影响，并在两个场景、四种路由协议以及三种网络负载下进行了广泛的实验。由于空间限制，本节仅展示以下五种关键组合的准确率结果，如表 5.5 所示：

(1) 组合一：不同层的所有特征，如表 5.1 所示。

(2) 组合二：物理层、网络层和应用层的特征。

(3) 组合三：物理层、数据链路层和网络层的特征。

(4) 组合四：物理层和网络层的特征。

(5) 组合五：物理层的 LQ；数据链路层的 $RxBufOcc$、$SndBufOcc$ 和 $BufSize$；网络层的 $MsgSize$、$MsgSrc$、$MsgDst$ 和 $MsgType$；应用层的 t_{sc}^{i}。

5.5.7.1　协同互补

本小节关注不同特征对检测准确率的贡献，并选择组合 1 ~ 4 作为代表性结果。首先，物理层和网络层构成了无人机网络通信的基础，因此利用这两层的特征，即组合四，可以达到一定的检测准确率。同时，实验结果显示数据链路层和应用层的特征有利于检测不同环境中的延时攻击。数据链路层主要负责数据错误控制和拥塞控制，而应用层则执行进一步地数据处理和应用。因此，在物理层和网络层的基础上，利用数据链路层的特征，即组合三，可以更好地处理规模较大、负载较重的无人机网络。此外，本章利用可在应用层获得的预先规划的轨迹信息来估计无人机存储和携带数据包的持续时间并消除其不利影响。因此，当网络负载较轻时，可以更准确地分析和利用轨迹信息，即组合二，从而构建出更好的一致性模型，提高检测准确率。

最后，将所有层的特征都考虑进去，即组合一，在所有情况下都实现了最佳的检测准确率。

表 5.5　不同特征组合的准确率结果

路由	组合	任务场景一			任务场景二		
		轻	中等	重	轻	中等	重
Epidemic	*1*	0.9976	0.9795	0.9113	0.9697	0.9579	0.9166
	2	0.9943	0.9770	0.8188	0.9528	0.8963	0.8435
	3	0.9849	0.9013	0.8817	0.9499	0.9304	0.8877
	4	0.7626	0.8127	0.7721	0.8691	0.7554	0.6945
	5	0.9912	0.9768	0.8832	0.9554	0.9222	0.8782
SprayAndWait	*1*	0.9955	0.9810	0.9431	0.9828	0.9664	0.9487
	2	0.9898	0.9732	0.9106	0.9775	0.9594	0.8655
	3	0.8860	0.9051	0.9266	0.9013	0.9040	0.9440
	4	0.6748	0.8161	0.8456	0.8157	0.8204	0.8072
	5	0.9787	0.9676	0.9097	0.9754	0.9565	0.9305
Prophet	*1*	0.9912	0.9911	0.9245	0.9740	0.9732	0.9570
	2	0.9854	0.9830	0.8730	0.9705	0.9573	0.9077
	3	0.9374	0.9608	0.9116	0.9501	0.9293	0.9438
	4	0.7789	0.8314	0.8085	0.7881	0.6963	0.8518
	5	0.9864	0.9737	0.8886	0.9487	0.9627	0.9466
MaxProp	*1*	0.9920	0.9364	0.9059	0.9678	0.9565	0.9605
	2	0.9889	0.9011	0.8751	0.9286	0.8677	0.9091
	3	0.9472	0.9023	0.8885	0.9193	0.9257	0.9517
	4	0.7636	0.8215	0.7707	0.7602	0.7777	0.8949
	5	0.9889	0.9193	0.8703	0.9452	0.9007	0.9394

总而言之，不同层的特征均有自己的优缺点，并且都有助于提高检测准确率。通过从跨层的角度对所有层的信息进行整体的收集、选择、分析和利用，HOTD 实现了特征之间的互补和协同，从而能够在不同环境下均能检测和处理延时攻击。

5.5.7.2 开销性能权衡

HOTD 使用消息附加的方式进行信息收集，这不可避免地增加了网络的额外开销。因此，本小节探索额外开销和检测准确率之间的权衡，旨在牺牲少量检测准确率的同时最大限度地减小额外的开销。为此，本章进行了广泛的实验，但是由于空间限制，本小节只展示最终的实验结果。

如表 5.5 所示，与组合一相比，组合五在达到不错的检测准确率的同时大大减少了额外的开销。组合五引入的额外开销为 $7+13+13+8+8+8=57$ bits，仅仅是组合一 (105 bits) 的 54%；同时，组合五检测准确率的下降在 6% 以内。因此，HOTD 能够在额外开销和检测准确率之间有效地实现良好的权衡。

5.5.8 开销分析

在无人机网络中，节点的存储和计算资源相对比较充足；而通信资源则较为紧张[44]。因此，本小节进行实验来研究所需收集的信息的传输所引入的额外开销率 (Extra Overhead Ratio)，其被定义为：

$$EOR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{H_i} j \times A_i}{\sum_{i=1}^{N} D_i \times H_i}, \tag{5.18}$$

其中 N 是传输消息的数量，D_i 是消息 M_i 的原始有效载荷的大小，H_i 是将消息 M_i 投递到目的地所需的跳数，A_i 是每个转发节点附加到消息 M_i 中的信息的大小。如表 5.2 所示，本章设置 $A_i = 105$ bits 以及 $D_i = 1400$ B。表 5.6 列出了两种任务场景下四种路由协议的实验结果：在所有情况下，HOTD 引入的额外开销率都非常小，均小于 2.5%，这表明了 HOTD 的可行性和实用性。

表 5.6 额外开销率

	Epidemic Router	*SprayAndWait Router*	*Prophet Router*	*MaxProp Router*
任务场景一	2.28%	1.80%	1.86%	2.30%
任务场景二	2.21%	1.78%	1.82%	2.17%

5.5.9 不同变量对检测准确率的影响

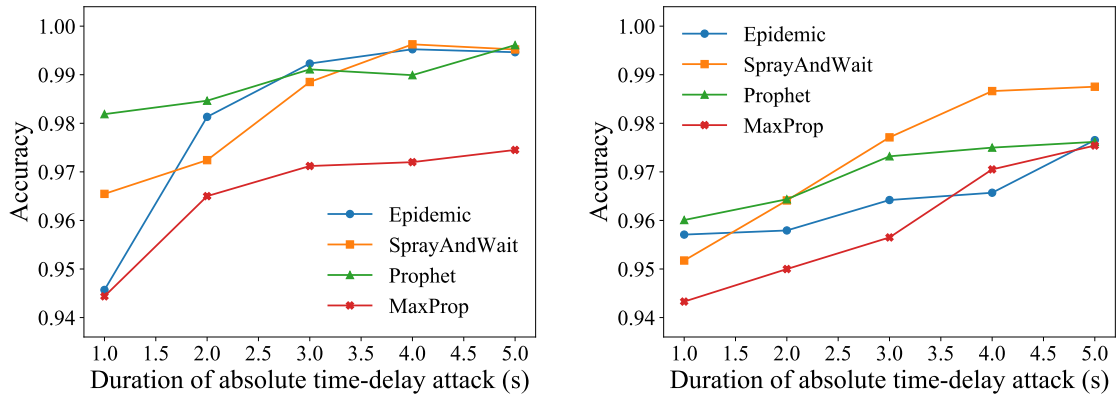
本小节主要研究不同变量对检测准确率的影响。

5.5.9.1 延时攻击时长对检测准确率的影响

本小节研究延时攻击时长对检测准确率的影响，为此本小节设计了两种不同的延时攻击，包括绝对延时攻击 (Absolute TDAs) 和相对延时攻击 (Relative TDAs)。在绝对延时攻击中，恶意节点实施固定时长的延时攻击，实验设置为 1 ~ 5 s；而相对延时攻击则根据数据包的传输时间延迟一定比例的时长，实验设置为传输时间的四分之一、一半、一倍、两倍和四倍。实验结果如图 5.8 和 5.9 所示。

首先，HOTD 检测准确率随着绝对延时攻击时长的增加而提高，这是因为延时攻击时长的增加会导致延迟相关的特征和基于训练出的一致性模型所得到的相应转发延迟之间出现明显的不一致，从而揭示出节点的恶意行为。同时，HOTD 的检测准确率在所有情况下均高于 94%。

此外，为了进一步地研究 HOTD 的性能，本节设计了一个更为隐蔽的相对延时攻击。相对延时攻击的持续时间取决于消息的传输时间，即四分之一、一半、一倍、两倍和四倍的时长。实验结果表明，在两种任务场景以及四种路由协议中，HOTD 的检测准确率均高于 91%，如图 5.9 所示。这是因为 HOTD 从跨层的角度对不同层的延迟相关信息进行整体的收集、提取和选择，训练好的一致性模型从而可以处理不同环境下的延时攻击。

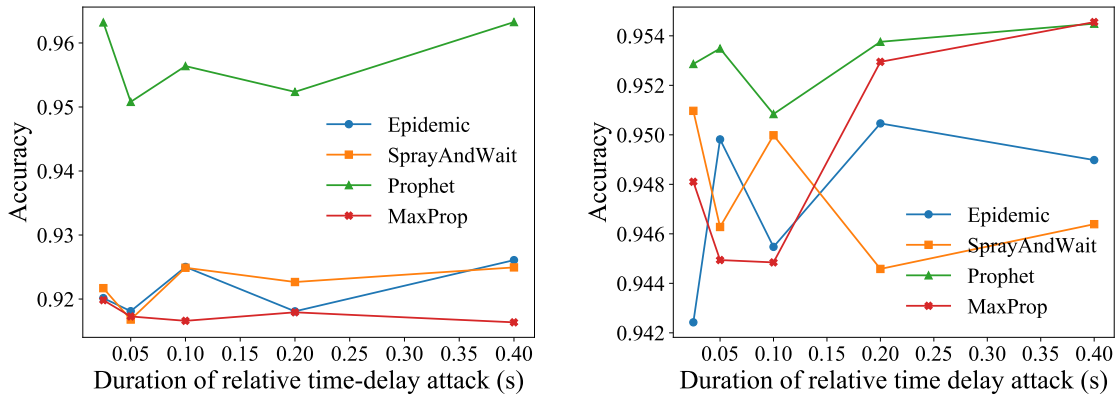


(a) 任务场景一　　(b) 任务场景二

图 5.8　绝对延时攻击时长对检测准确率的影响

5.5.9.2 延时攻击概率对检测准确率的影响

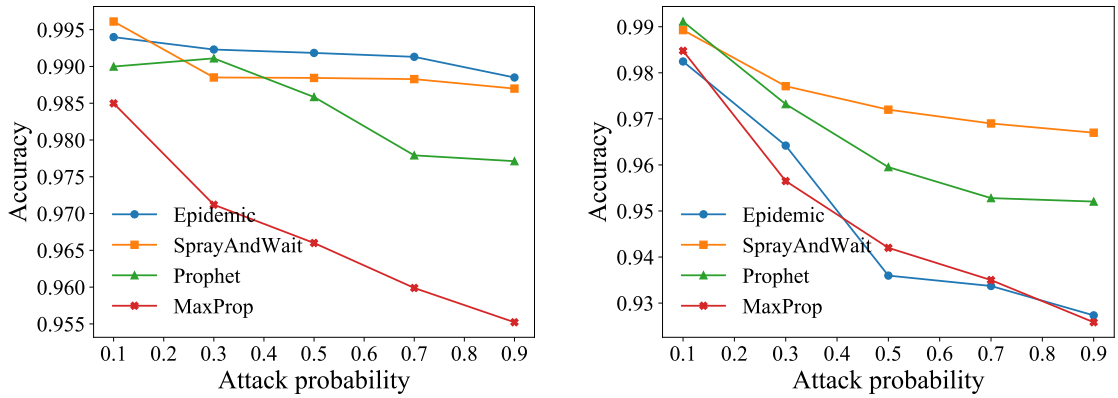
图 5.10 给出了不同延时攻击概率下 HOTD 的检测准确率。在所有的情况下，HOTD 的检测准确率都保持在 92% 以上。同时，随着恶意节点攻击概率的增加，检测准确率略有下降，这是因为网络中的延时攻击越多，无人机网络环境就越复杂，从而导致难以准确地提取出与延迟相关的信息。



(a) 任务场景一　　(b) 任务场景二

图 5.9　相对延时攻击时长对检测准确率的影响

此外，在大多数情况下，在 SprayAndWait 和 Prophet 路由上的检测准确率要优于在 Epidemic 和 MaxProp 路由的检测准确率。原因在于 Epidemic 和 MaxProp 路由协议的路由策略本质上都是基于传统的泛洪 (Flooding) 机制。当网络采用这种路由机制时，网络中所有节点的负载都会急剧上升，无论是恶意节点还是良性节点。这会导致 HOTD 中数据链路层的特征对检测准确率的贡献和影响降低，从而导致整体检测准确率的下降。



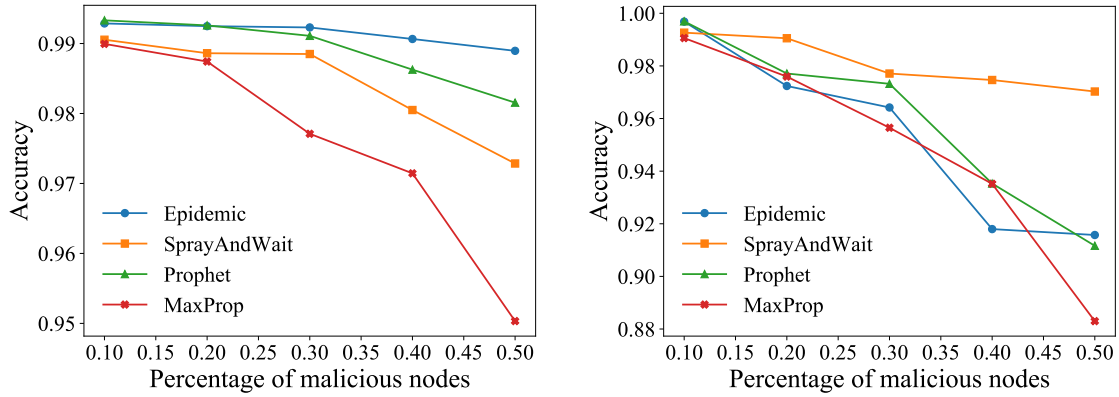
(a) 任务场景一　　(b) 任务场景二

图 5.10　延时攻击概率对检测准确率的影响

5.5.9.3　恶意节点占比对检测准确率的影响

本小节研究恶意节点占比对检测准确率的影响，实验设置恶意节点占比为 0.1 ~ 0.5，实验结果如图 5.11 所示。

在大多数情况下，HOTD 的检测准确率超过了 90%；同时，随着恶意节点占比的提高，检测准确率出现了下降。就总体趋势而言，实验结果与5.5.9.2节中延时攻击概率的结果相似；但是，恶意节点占比对检测准确率的影响要大于延时攻击概率对检测准确率的影响。原因在于相对于延时攻击概率的增加，恶意节点占比的提高能够更广泛、更快速地对相邻节点乃至整个网络产生不利影响，从而能够全面快速地降低网络的整体性能。这导致良性节点和恶意节点之间的区分度下降，造成检测准确率的降低。



(a) 任务场景一　　(b) 任务场景二

图 5.11　恶意节点占比对检测准确率的影响

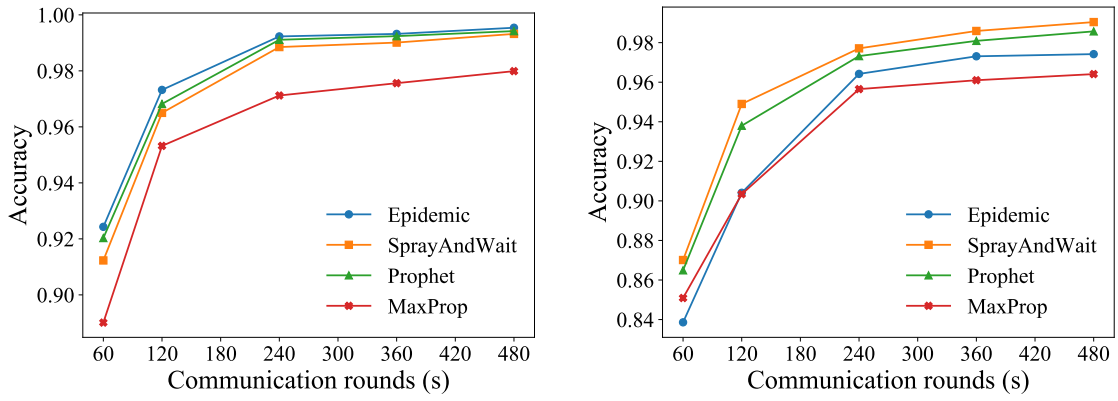
5.5.9.4　通信周期对检测准确率的影响

本小节研究通信周期对检测准确率的影响，实验分别设置通信周期为 60、120、240、360 和 480 s，实验结果如图 5.12 所示。

随着通信周期的增加，HOTD 的检测准确率也随之提高，这是因为每个通信周期中可用于评估的样本数量也随着增加，这可以很好地缓解样本数据分布和单一评估偏差对整体结果的影响，从而能够更为准确地计算出节点的一致性程度。具体来说，当通信周期只有 60 s 时，HOTD 的检测准确率在所有情况下仍高于 82%；而当通信周期从 60 s 逐步增长到 240 s 时，HOTD 的检测准确率迅速提升；随后，HOTD 的检测准确率逐渐趋于稳定，在通信周期为 480 s 时达到最高。

5.5.9.5　链路质量对检测准确率的影响

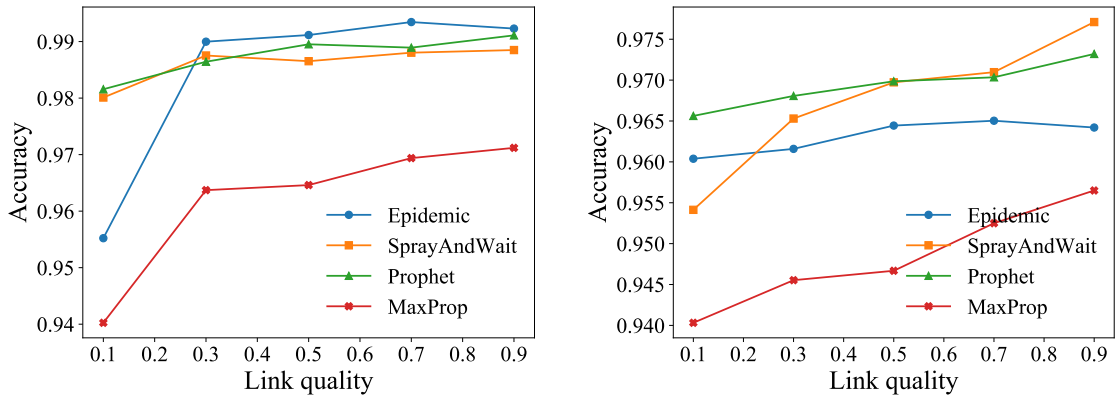
图 5.13 显示了链路质量对检测准确率的影响，可见，HOTD 的检测准确率通常会随着链路质量的提升而提高。原因在于当链路质量较差时，网络中会充斥着大量的数据包丢失和重传，这浪费了大量的数据包传输时间，并且导致了网络负载的增加。这种恶劣糟糕的网络环境会导致



(a) 任务场景一　　(b) 任务场景二

图 5.12　通信周期对检测准确率的影响

节点转发行为的异常以及消息延迟的异常波动，这无疑大大增加了延时攻击的检测难度。但是，即便如此，HOTD 在所有情形下的检测准确率都在 94% 以上。



(a) 任务场景一　　(b) 任务场景二

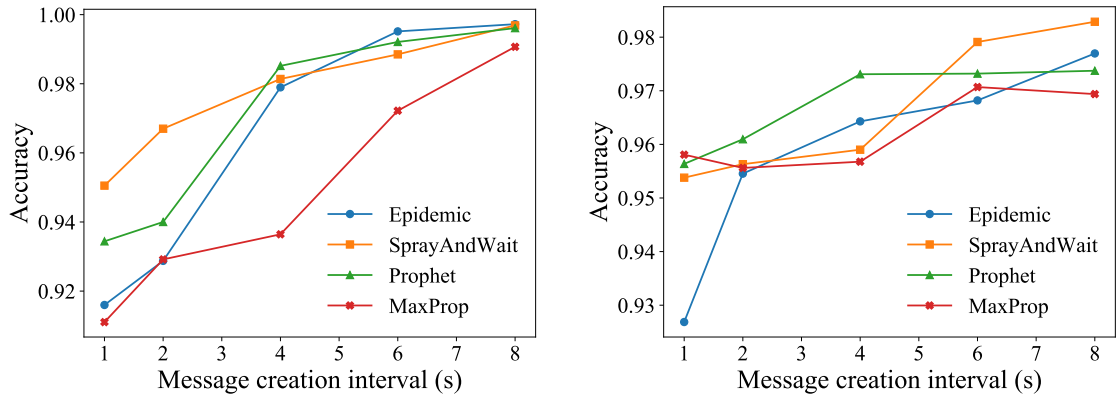
图 5.13　链路质量对检测准确率的影响

5.5.9.6　消息创建间隔对检测准确率的影响

本小节旨在研究消息创建间隔对检测准确率的影响，同时保证在不同消息创建间隔中注入的数据包的总数是相同的。HOTD 的实验结果如图 5.14 所示。

随着消息创建间隔的增加，HOTD 在两种任务场景以及四种路由协议下的检测准确率都在逐渐增加。原因在于消息创建间隔的增加使得无人机网络负载降低，这有利于降低复杂的无人机网络环境中各种因素对特征提取和攻击检测的影响，例如拥塞、排队、重传等等。所提取出

的延迟相关特征能够更加准确地对延时攻击进行检测和识别。同时，在所有情况下，HOTD 的检测准确率均高于 91%。



(a) 任务场景一　　(b) 任务场景二

图 5.14　消息创建间隔对检测准确率的影响

5.6　本章小结

本章针对无人机网络的延时攻击进行了全面深入的分析，设计了一个整体跨层的延时攻击检测框架 HOTD，并提出了一种抗延时攻击的安全路由协议。首先，HOTD 从跨层的角度对无人机网络协议栈中每一层的延迟相关特征进行了整体选择，然后采用监督学习在这些选定的特征和相应的转发延迟之间构建一致性模型，并在此基础上，计算出网络中每个节点的一致性程度。接着，根据一致性程度，HOTD 使用聚类方法来区分恶意节点和良性节点。最后，抗延时攻击的安全路由协议基于 HOTD 的分类结果对恶意节点进行路由隔离，保障路由安全。实验结果表明，HOTD 在无人机网络中的性能远优于静态网络中最先进的延时攻击检测方法。在各种无人机网络场景和路由协议中，HOTD 在额外开销不到 2.5% 的同时实现了高于 85% 的检测准确率。同时，抗延时攻击的安全路由协议在各种环境下都能够大幅度降低延时攻击对路由协议投递率、平均延迟以及网络负载率的影响。

第六章　总结与展望

6.1　论文工作总结

多跳无人机自组织网络具有部署灵活、使用方便、可扩展性好、建造成本低、生存能力强、环境要求低等优点，近年来已经被广泛应用于各种军事和民用领域。高效可靠的路由协议技术是保障无人机网络数据通信、信息共享、集群协作和任务执行的基本前提，但无人机网络的特性，例如节点的高速移动性、网络拓扑的高度动态性和通信连接的间断性，给路由协议技术的研究与设计带来了严峻的挑战。传统的无人机网络路由协议缺乏对无人机网络特性的深入分析和优化、跨层设计的整体融合和利用、网络安全的考量和设计；为了应对这些不足和挑战，本文从整体跨层的角度研究面向多跳无人机自组织网络的路由协议技术，研究成果主要包括以下几个方面：

(1) 现有为无人机网络设计的路由协议大多数都是基于非跨层的方式，这些路由协议在进行路由决策时不使用其他层的路由信息和参数。此外，它们大多仅针对无人机网络的其中一个问题进行了特定的优化，不能为无人机网络及其应用场景提供足够高效的性能表现。针对这些问题提出了一种整体的跨层路由优化框架 HOLO，综合考虑无人机网络的特点以及无人机网络协议体系结构，从跨层的角度对不同协议层的反馈、参数和信息进行整体的收集、分析、融合和利用，从而得到大量有益的跨层路由相关信息。基于跨层信息，提出了面向优化目标的高效路由决策机制，针对不同的优化目标类型，分别设计不同的路由决策机制。

(2) 基于整体跨层路由优化框架，本文进一步对无人机网络能耗高效路由协议进行研究。现有研究主要基于无人机传输功率固定的假设，没有考虑联合功率调度与控制来对路由协议进行优化。本文提出了一种高效的功率感知的多跳无人机网络路由协议 PAR，使用跨层设计，联合物理层的功率感知、应用层的 QoS 需求以及预先规划的无人机轨迹信息来对无人机网络的路由决策进行联合优化。PAR 联合物理层的功率感知以及预先规划的轨迹信息计算出无人机在不同可调功率级别下的相遇情况。基于计算出的相遇信息，PAR 结合应用层的 QoS 需求，以延迟约束和能耗最小化为优化目标，构建功率感知相遇树，从而选择最优的传输路径。与现有算法相比，该协议充分考虑传输能耗以及投递延迟，在达到较高消息投递率、较低网络负载率的同时节约了大量的能量资源。

(3) 延时攻击易于实施且难以检测，同时无人机网络的独特特征大大增加了此攻击的隐蔽性和破坏性。然而，目前尚无针对无人机网络中延时攻击检测和防御的研究。针对上述不足，本文对无人机网络中延时攻击进行分析与建模，提出了一个整体跨层的延时攻击检测框架 HOTD，并基于此提出了一个抗延时攻击的多跳无人机网络安全路由协议。HOTD 从跨层的角度全面

系统地选择、收集无人机网络协议栈每一层的延迟相关特征，然后利用监督学习构建选定特征与相应转发延迟之间的一致性模型。根据此模型，计算网络各个节点的一致性程度，并利用聚类算法将节点划分为良性节点和恶意节点。抗延时攻击的无人机网络安全路由协议根据分类结果采取路由隔离机制来保证网络安全。实验结果表明 HOTD 在引入低于 2.5% 的网络额外开销的同时达到高于 85% 的检测准确率，同时抗延时攻击的无人机网络安全路由协议能够极大地降低延时攻击对无人机网络路由协议性能的影响。

6.2 未来研究展望

本文对多跳无人机自组织网络的路由协议技术进行了研究，在对无人机网络协议体系结构及其功能全面深入分析的基础上提出了一个整体跨层路由优化框架，并基于此框架，分别从高效和安全两个角度对无人机网络路由协议进行了设计。但是，高效和安全是无人机网络路由协议的永恒追求，而本文仅做出一些初步探索和初期工作，尚有很大的研究空间。结合本文已有工作，进一步的研究工作包括：

(1) 在无人机网络的跨层路由协议研究中，选择协议栈各层中合适的路由参数和信息至关重要。不同的无人机网络应用场景有着不同的优化目标，不同的的路由参数在不同的优化目标中具备不等的作用，合理的路由参数选择有利于做出更优的路由决策。同时，路由参数之间不仅相互协同补充，也有可能会相互冲突，两个不同的路由参数可能对同一路由决策持有不同甚至完全相反的建议。进一步的研究将重点关注路由参数和信息的分析和选择，权衡它们之间的协同和冲突，以达到更好的网络性能。

(2) 在能耗高效的无人机网络路由协议中，本文只考虑了数据传输中发送方的能量消耗，而忽略了接收端的能量消耗；并且只针对单播路由协议进行研究，而多播环境下的能耗优化则更加复杂。进一步研究中需联合发送和接收能量进行综合优化，同时针对无人机网络的多播路由协议进行优化设计。

(3) 本文设计的抗延时攻击的无人机网络安全路由协议依赖于标签数据和地面站，是一种集中式的监督学习方式。尽管本文对信息收集方法的轻量级进行了证明，但它仍然不可避免地引入了通信开销；此外在无人机网络的实际应用场景中，对恶意标签数据的收集并不容易，需要良性节点进行模拟，而这可能会干扰无人机网络的正常运行。因此，需要进一步研究以分布式和无监督的方式对无人机网络的安全路由进行优化。

参考文献

[1] Mishra D, Natalizio E. A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements[J]. Computer Networks, 2020, 182:107451.

[2] Rovira-Sugranes A, Razi A, Afghah F, et al. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook[J]. Ad Hoc Networks, 2022, 130:102790.

[3] Wang H, Zhao H, Zhang J, et al. Survey on unmanned aerial vehicle networks: A cyber physical system perspective[J]. IEEE Communications Surveys & Tutorials, 2019, 22(2):1027–1070.

[4] Zhaoxuan L, Kaiquan C, Yanbo Z. Civil unmanned aircraft system operation in national airspace: A survey from Air Navigation Service Provider perspective[J]. Chinese Journal of Aeronautics, 2021, 34(3):200–224.

[5] Erat O, Isop W A, Kalkofen D, et al. Drone-augmented human vision: Exocentric control for drones exploring hidden areas[J]. IEEE transactions on visualization and computer graphics, 2018, 24(4):1437–1446.

[6] Yanmaz E, Yahyanejad S, Rinner B, et al. Drone networks: Communications, coordination, and sensing[J]. Ad Hoc Networks, 2018, 68:1–15.

[7] Alzahrani B, Oubbati O S, Barnawi A, et al. UAV assistance paradigm: State-of-the-art in applications and challenges[J]. Journal of Network and Computer Applications, 2020, 166:102706.

[8] Chriki A, Touati H, Snoussi H, et al. FANET: Communication, mobility models and security issues[J]. Computer Networks, 2019, 163:106877.

[9] Zhang L, Hu L, Hu F, et al. Enhanced OLSR routing for airborne networks with multi-beam directional antennas[J]. Ad Hoc Networks, 2020, 102:102116.

[10] Kadadha M, Otrok H. A blockchain-enabled relay selection for QoS-OLSR in urban VANET: A Stackelberg game model[J]. Ad Hoc Networks, 2021, 117:102502.

[11] Jain R, Kashyap I. An QoS aware link defined OLSR (LD-OLSR) routing protocol for MANETs[J]. Wireless Personal Communications, 2019, 108(3):1745–1758.

[12] Kanagasundaram H, Kathirvel A. EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network[J]. IET Communications, 2019, 13(5):553–559.

[13] Anamalamudi S, Sangi A R, Alkatheiri M, et al. AODV routing protocol for Cognitive radio access based Internet of Things (IoT)[J]. Future Generation Computer Systems, 2018, 83:228–238.

[14] Zhang D, Gong C, Zhang T, et al. A new algorithm of clustering AODV based on edge computing strategy in IOV[J]. Wireless Networks, 2021, 27(4):2891–2908.

[15] Gankhuyag G, Shrestha A P, Yoo S J. Robust and reliable predictive routing strategy for flying ad-hoc networks[J]. IEEE Access, 2017, 5:643–654.

[16] Liang Q, Lin T, Wu F, et al. A dynamic source routing protocol based on path reliability and link monitoring repair[J]. Plos one, 2021, 16(5):e0251548.

[17] Huang H, Yin H, Min G, et al. Energy-aware dual-path geographic routing to bypass routing holes in wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2017, 17(6):1339–

1352.

[18] Choi S C, Hussen H R, Park J H, et al. Geolocation-based routing protocol for flying ad hoc networks (FANETs)[C]. Proceedings of 2018 Tenth international conference on ubiquitous and future networks (ICUFN). IEEE, 2018. 50–52.

[19] Huang H, Zhang J, Zhang X, et al. EMGR: Energy-efficient multicast geographic routing in wireless sensor networks[J]. Computer Networks, 2017, 129:51–63.

[20] Liu C, Fang D, Hu Y, et al. EasyGo: Low-cost and robust geographic opportunistic sensing routing in a strip topology wireless sensor network[J]. Computer Networks, 2018, 143:191–205.

[21] Arafat M Y, Moh S. Localization and clustering based on swarm intelligence in UAV networks for emergency communications[J]. IEEE Internet of Things Journal, 2019, 6(5):8958–8976.

[22] Khan A, Aftab F, Zhang Z. BICSF: Bio-inspired clustering scheme for FANETs[J]. IEEE Access, 2019, 7:31446–31456.

[23] Azzoug Y, Boukra A. Enhanced UAV-aided vehicular delay tolerant network (VDTN) routing for urban environment using a bio-inspired approach[J]. Ad Hoc Networks, 2022. 102902.

[24] Khan A, Khan S, Fazal A S, et al. Intelligent cluster routing scheme for flying ad hoc networks[J]. Science China Information Sciences, 2021, 64(8):1–14.

[25] Wazid M, Das A K, Kumar N, et al. Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment[J]. IEEE Internet of Things Journal, 2018, 6(2):3572–3584.

[26] Alladi T, Chamola V, Kumar N, et al. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks[J]. Computer Communications, 2020, 160:81–90.

[27] Bansal G, Sikdar B. S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms[J]. IEEE Transactions on Vehicular Technology, 2021, 70(11):12088–12100.

[28] Fan K, Luo Q, Zhang K, et al. Cloud-based lightweight secure RFID mutual authentication protocol in IoT[J]. Information Sciences, 2020, 527:329–340.

[29] Shams E A, Rizaner A, Ulusoy A H. Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks[J]. Computers & Security, 2018, 78:245–254.

[30] Prathapchandran K, Janani T. A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST[J]. Computer Networks, 2021, 198:108413.

[31] Ma Z, Liu L, Meng W. Towards multiple-mix-attack detection via consensus-based trust management in IoT networks[J]. Computers & Security, 2020, 96:101898.

[32] Yang L, Liu L, Ma Z, et al. Detection of selective-edge packet attack based on edge reputation in IoT networks[J]. Computer Networks, 2021, 188:107842.

[33] Clausen T, Jacquet P. Optimized link state routing protocol (OLSR)[R]. Technical report, 2003.

[34] Nayyar A. Flying adhoc network (FANETs): simulation based performance comparison of routing protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP[C]. Proceedings of 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). IEEE, 2018. 1–9.

[35] Saini T K, Sharma S C. Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept[J]. Ad Hoc Networks, 2020, 103:102148.

[36] Walikar G A, Biradar R C. A survey on hybrid routing mechanisms in mobile ad hoc networks[J].

Journal of Network and Computer Applications, 2017, 77:48–63.

[37] Xijie Z, Chunxiu X, Jiaqi X. Hierarchical ZRP's performance vs ZRP's performance in MANET[C]. Proceedings of 2015 IEEE International Conference on Communication Software and Networks (ICCSN). IEEE, 2015. 423–426.

[38] Kumar K S, Tarun R, Sowparnika A, et al. Hybrid on demand multipath distance vector routing protocol[C]. Proceedings of 2015 International Conference on Developments of E-Systems Engineering (DeSE). IEEE, 2015. 65–70.

[39] Malwe S R, Rohilla S, Biswas G. Location and selective-bordercast based enhancement of zone routing protocol[C]. Proceedings of 2016 3rd International Conference on Recent Advances in Information Technology (RAIT). IEEE, 2016. 83–88.

[40] Li X, Yan J. LEPR: Link stability estimation-based preemptive routing protocol for flying ad hoc networks[C]. Proceedings of 2017 IEEE symposium on computers and communications (ISCC). IEEE, 2017. 1079–1084.

[41] Arafat M Y, Moh S. Location-aided delay tolerant routing protocol in UAV networks for post-disaster operation[J]. IEEE Access, 2018, 6:59891–59906.

[42] Fu L, Fu X, Zhang Z, et al. Joint optimization of multicast energy in delay-constrained mobile wireless networks[J]. IEEE/ACM Transactions on Networking, 2018, 26(1):633–646.

[43] Rahimi S, Jabraeil Jamali M A. A hybrid geographic-DTN routing protocol based on fuzzy logic in vehicular ad hoc networks[J]. Peer-to-Peer Networking and Applications, 2019, 12(1):88–101.

[44] Asadpour M, Hummel K A, Giustiniano D, et al. Route or carry: Motion-driven packet forwarding in micro aerial vehicle networks[J]. IEEE Transactions on Mobile Computing, 2016, 16(3):843–856.

[45] Mahmood B A, Manivanann D. Hybrid on-demand greedy routing protocol with backtracking for mobile ad-hoc networks[J]. International Journal of Pervasive Computing and Communications, 2020..

[46] Almesaeed R, Jedidi A. Dynamic directional routing for mobile wireless sensor networks[J]. Ad Hoc Networks, 2021, 110:102301.

[47] Arianmehr S, Jabraeil Jamali M A. HybTGR: a hybrid routing protocol based on topological and geographical information in vehicular ad hoc networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(4):1683–1695.

[48] Yang J, Sun K, He H, et al. Dynamic virtual topology aided networking and routing for aeronautical ad-hoc networks[J]. IEEE Transactions on Communications, 2022, 70(7):4702–4716.

[49] Tsao K Y, Girdler T, Vassilakis V G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks[J]. Ad Hoc Networks, 2022. 102894.

[50] Zhi Y, Fu Z, Sun X, et al. Security and privacy issues of UAV: a survey[J]. Mobile Networks and Applications, 2020, 25(1):95–101.

[51] Fatemidokht H, Rafsanjani M K, Gupta B B, et al. Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7):4757–4769.

[52] Bera B, Das A K, Sutrala A K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment[J]. Computer Communi-

cations, 2021, 166:91–109.

[53] Xu X, Zhao H, Yao H, et al. A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT[J]. IEEE Internet of Things Journal, 2020, 8(4):2431–2443.

[54] Wani A R, Gupta S K, Khanam Z, et al. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme[J]. IET Intelligent Transport Systems, 2022..

[55] Hassija V, Chamola V, Agrawal A, et al. Fast, reliable, and secure drone communication: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4):2802–2832.

[56] Al-Turjman F, Abujubbeh M, Malekloo A, et al. UAVs assessment in software-defined IoT networks: An overview[J]. Computer Communications, 2020, 150:519–536.

[57] Mehta P, Gupta R, Tanwar S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons[J]. Computer Communications, 2020, 151:518–538.

[58] Zhou Y, Pan C, Yeoh P L, et al. Secure communications for UAV-enabled mobile edge computing systems[J]. IEEE Transactions on Communications, 2019, 68(1):376–388.

[59] He D, Qiao Y, Chan S, et al. Flight security and safety of drones in airborne fog computing systems[J]. IEEE Communications Magazine, 2018, 56(5):66–71.

[60] Deebak B D, Al-Turjman F. A smart lightweight privacy preservation scheme for IoT-based UAV communication systems[J]. Computer Communications, 2020, 162:102–117.

[61] Tian Y, Yuan J, Song H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones[J]. Journal of Information Security and Applications, 2019, 48:102354.

[62] Srinivas J, Das A K, Kumar N, et al. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment[J]. IEEE Transactions on Vehicular Technology, 2019, 68(7):6903–6916.

[63] Mall P, Amin R, Obaidat M S, et al. CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN[J]. Computer Networks, 2021, 199:108476.

[64] Tian C, Jiang Q, Li T, et al. Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment[J]. Computer Networks, 2022, 218:109421.

[65] He D, Chan S, Guizani M. Drone-assisted public safety networks: The security aspect[J]. IEEE Communications Magazine, 2017, 55(8):218–223.

[66] García-Magariño I, Lacuesta R, Rajarajan M, et al. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain[J]. Ad Hoc Networks, 2019, 86:72–82.

[67] Ge C, Ma X, Liu Z. A semi-autonomous distributed blockchain-based framework for UAVs system[J]. Journal of Systems Architecture, 2020, 107:101728.

[68] Li T, Zhang J, Obaidat M S, et al. Energy-efficient and Secure Communication towards UAVs Networks[J]. IEEE Internet of Things Journal, 2021..

[69] Xiao W, Li M, Alzahrani B, et al. A blockchain-based secure crowd monitoring system using UAV swarm[J]. IEEE Network, 2021, 35(1):108–115.

[70] Pham T N D, Yeo C K. Detecting colluding blackhole and greyhole attacks in delay tolerant networks[J]. IEEE Transactions on Mobile Computing, 2015, 15(5):1116–1129.

[71] Aneja S, Nagrath P, Purohit G. Energy efficient reputation mechanism for defending different types of flooding attack[J]. Wireless Networks, 2019, 25(7):3933–3951.

[72] 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, 2019, 38(1):193–204.

[73] Farooq U, Tariq N, Asim M, et al. Machine learning and the Internet of Things security: Solutions and open challenges[J]. Journal of Parallel and Distributed Computing, 2022, 162:89–104.

[74] Wan Y, Xu K, Xue G, et al. Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes[C]. Proceedings of IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020. 874–883.

[75] Anthi E, Williams L, Słowińska M, et al. A supervised intrusion detection system for smart home IoT devices[J]. IEEE Internet of Things Journal, 2019, 6(5):9042–9053.

[76] Liu L, Xu X, Liu Y, et al. A detection framework against CPMA attack based on trust evaluation and machine learning in IoT network[J]. IEEE Internet of Things Journal, 2021..

[77] Gao B, Maekawa T, Amagata D, et al. Environment-adaptive malicious node detection in MANETs with ensemble learning[C]. Proceedings of 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018. 556–566.

[78] Nguyen T D, Marchal S, Miettinen M, et al. DÏoT: A federated self-learning anomaly detection system for IoT[C]. Proceedings of 2019 IEEE 39th International conference on distributed computing systems (ICDCS). IEEE, 2019. 756–767.

[79] Zhang Y, Mou Z, Gao F, et al. UAV-enabled secure communications by multi-agent deep reinforcement learning[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10):11599–11611.

[80] Jiang J, Han G. Routing protocols for unmanned aerial vehicles[J]. IEEE Communications Magazine, 2018, 56(1):58–63.

[81] Amponis G, Lagkas T, Sarigiannidis P, et al. A survey on FANET routing from a cross-layer design perspective[J]. Journal of Systems Architecture, 2021, 120:102281.

[82] Sah D K, Amgoth T. Parametric survey on cross-layer designs for wireless sensor networks[J]. Computer Science Review, 2018, 27:112–134.

[83] IEEE Draft Trial-Use Standard for Aerial Ad Hoc Networks[J]. IEEE P1920.1/D10, October 2022, 2022. 1–85.

[84] IEEE Standard for a Framework for Structuring Low-Altitude Airspace for Unmanned Aerial Vehicle (UAV) Operations[J]. IEEE Std 1939.1-2021, 2021. 1–94.

[85] Zhou Z, Feng J, Gu B, et al. When mobile crowd sensing meets UAV: Energy-efficient task assignment and route planning[J]. IEEE Transactions on Communications, 2018, 66(11):5526–5538.

[86] Peng J, Gao H, Liu L, et al. TBM: An Efficient Trajectory-Based Multicast Routing Protocol for Sparse UAV networks[C]. Proceedings of 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2020. 867–872.

[87] Li X, Liu L, Wang L, et al. Trajectory-aware spatio-temporal range query processing for unmanned aerial vehicle networks[J]. Computer Communications, 2021, 178:271–285.

[88] Arafat M Y, Moh S. A survey on cluster-based routing protocols for unmanned aerial vehicle

networks[J]. IEEE Access, 2018, 7:498–516.

[89] Slowik A, Kwasnicka H. Evolutionary algorithms and their applications to engineering problems[J]. Neural Computing and Applications, 2020, 32(16):12363–12379.

[90] Mousavi S, Afghah F, Ashdown J D, et al. Use of a quantum genetic algorithm for coalition formation in large-scale UAV networks[J]. Ad Hoc Networks, 2019, 87:26–36.

[91] Luong N C, Hoang D T, Gong S, et al. Applications of deep reinforcement learning in communications and networking: A survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4):3133–3174.

[92] Singh V, Sharma K P, Verma H K. ABNT: Adaptive beaconing and neighbor timeout for geographical routing in UAV networks[J]. Peer-to-Peer Networking and Applications, 2022, 15(4):2079–2100.

[93] Thangaramya K, Kulothungan K, Logambigai R, et al. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT[J]. Computer Networks, 2019, 151:211–223.

[94] Guleria K, Verma A K. Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks[J]. Wireless Networks, 2019, 25(3):1159–1183.

[95] Shafiq M, Ashraf H, Ullah A, et al. Systematic literature review on energy efficient routing schemes in WSN–A survey[J]. Mobile Networks and Applications, 2020, 25(3):882–895.

[96] Sakai K, Sun M T, Ku W S. Data-intensive routing in delay-tolerant networks[C]. Proceedings of IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019. 2440–2448.

[97] Naeem B, Ngah R, Hashim S Z M. Reduction in ping-pong effect in heterogeneous networks using fuzzy logic[J]. Soft Computing, 2019, 23(1):269–283.

[98] Hu M, Liu W, Lu J, et al. On the joint design of routing and scheduling for vehicle-assisted multi-UAV inspection[J]. Future Generation Computer Systems, 2019, 94:214–223.

[99] Jeong J P, Kim J, Hwang T, et al. TPD: travel prediction-based data forwarding for light-traffic vehicular networks[J]. Computer Networks, 2015, 93:166–182.

[100] Zhang G, Wu Q, Cui M, et al. Securing UAV communications via joint trajectory and power control[J]. IEEE Transactions on Wireless Communications, 2019, 18(2):1376–1389.

[101] Schneider K, Zhang B, Benmohamed L. Hop-by-hop multipath routing: Choosing the right nexthop set[C]. Proceedings of IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020. 2273–2282.

[102] Zamalloa M Z, Seada K, Krishnamachari B, et al. Efficient geographic routing over lossy links in wireless sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008, 4(3):1–33.

[103] Keranen A. Opportunistic network environment simulator[J]. Special Assignment report, Helsinki University of Technology, Department of Communications and Networking, 2008..

[104] Keränen A, Ott J, Kärkkäinen T. The ONE simulator for DTN protocol evaluation[C]. Proceedings of Proceedings of the 2nd international conference on simulation tools and techniques, 2009. 1–10.

[105] Liu X, Abdelhakim M, Krishnamurthy P, et al. Identifying malicious nodes in multihop iot networks using diversity and unsupervised learning[C]. Proceedings of 2018 IEEE International Conference on Communications (ICC). IEEE, 2018. 1–6.

[106] Sun S, Ma Z, Liu L, et al. Detection of malicious nodes in drone ad-hoc network based on supervised learning and clustering algorithms[C]. Proceedings of 2020 16th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2020. 145–152.

[107] Kaliyar P, Jaballah W B, Conti M, et al. LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks[J]. Computers & Security, 2020, 94:101849.

[108] Lou X, Tran C, Yau D K, et al. Learning-based time delay attack characterization for cyber-physical systems[C]. Proceedings of 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2019. 1–6.

[109] Ganesh P, Lou X, Chen Y, et al. Learning-based Simultaneous Detection and Characterization of Time Delay Attack in Cyber-Physical Systems[J]. IEEE Transactions on Smart Grid, 2021..

[110] Wu Q, Xu J, Zeng Y, et al. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence[J]. IEEE Journal on Selected Areas in Communications, 2021..

[111] Fu X, Xu Z, Peng Q, et al. ConMap: A novel framework for optimizing multicast energy in delay-constrained mobile wireless networks[C]. Proceedings of Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2017. 1–10.

[112] Meng K, Li D, He X, et al. Space Pruning Based Time Minimization in Delay Constrained Multi-Task UAV-Based Sensing[J]. IEEE Transactions on Vehicular Technology, 2021, 70(3):2836–2849.

[113] Xiong F, Li A, Wang H, et al. An SDN-MQTT based communication system for battlefield UAV swarms[J]. IEEE Communications Magazine, 2019, 57(8):41–47.

[114] Hu J, Zhang H, Song L, et al. Cooperative internet of UAVs: Distributed trajectory design by multi-agent deep reinforcement learning[J]. IEEE Transactions on Communications, 2020, 68(11):6807–6821.

[115] Dong X, Li Y, Lu C, et al. Time-varying formation tracking for UAV swarm systems with switching directed topologies[J]. IEEE transactions on neural networks and learning systems, 2018, 30(12):3674–3685.

[116] Zema N R, Quadri D, Martin S, et al. Formation control of a mono-operated UAV fleet through ad-hoc communications: a Q-learning approach[C]. Proceedings of 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2019. 1–6.

[117] Ma Z, Liu L, Meng W. DCONST: Detection of multiple-mix-attack malicious nodes using consensus-based trust in IoT networks[C]. Proceedings of Australasian Conference on Information Security and Privacy. Springer, 2020. 247–267.

[118] Xiahou K, Liu Y, Wu Q. Robust Load Frequency Control of Power Systems Against Random Time-Delay Attacks[J]. IEEE Transactions on Smart Grid, 2020, 12(1):909–911.

[119] Moussa B, Debbabi M, Assi C. A detection and mitigation model for PTP delay attack in an IEC 61850 substation[J]. IEEE Transactions on Smart Grid, 2016, 9(5):3954–3965.

[120] Lou X, Tran C, Tan R, et al. Assessing and mitigating impact of time delay attack: case studies for power grid controls[J]. IEEE Journal on Selected Areas in Communications, 2019, 38(1):141–155.

[121] Ma Z, Liu L, Meng W. ELD: Adaptive Detection of Malicious Nodes under Mix-Energy-

Depleting-Attacks Using Edge Learning in IoT Networks[C]. Proceedings of International Conference on Information Security. Springer, 2020. 255–273.

[122] Qin Y, Kishk M A, Alouini M S. Performance evaluation of UAV-enabled cellular networks with battery-limited drones[J]. IEEE Communications Letters, 2020, 24(12):2664–2668.

[123] Yu X, Peng Y, Li F, et al. Two-level data compression using machine learning in time series database[C]. Proceedings of 2020 IEEE 36th International Conference on Data Engineering (ICDE). IEEE, 2020. 1333–1344.

[124] Pelkonen T, Franklin S, Teller J, et al. Gorilla: A fast, scalable, in-memory time series database[J]. Proceedings of the VLDB Endowment, 2015, 8(12):1816–1827.

[125] Singh D, Singh B. Investigating the impact of data normalization on classification performance[J]. Applied Soft Computing, 2020, 97:105524.

[126] Peng J, Gao H, Liu L, et al. FNTAR: A Future Network Topology-aware Routing protocol in UAV networks[C]. Proceedings of 2020 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2020. 1–6.

[127] Vahdat A, Becker D, et al. Epidemic routing for partially connected ad hoc networks, 2000.

[128] Spyropoulos T, Psounis K, Raghavendra C S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks[C]. Proceedings of Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, 2005. 252–259.

[129] Lindgren A, Doria A, Schelén O. Probabilistic routing in intermittently connected networks[J]. ACM SIGMOBILE mobile computing and communications review, 2003, 7(3):19–20.

[130] Burgess J, Gallagher B, Jensen D D, et al. MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks[C]. Proceedings of Infocom, volume 6. Barcelona, Spain, 2006.

[131] Moussa B, Kassouf M, Hadjidj R, et al. An extension to the precision time protocol (PTP) to enable the detection of cyber attacks[J]. IEEE Transactions on Industrial Informatics, 2019, 16(1):18–27.

[132] Wang H, Gu J, Wang S. An effective intrusion detection framework based on SVM with feature augmentation[J]. Knowledge-Based Systems, 2017, 136:130–139.

[133] Almogren A S. Intrusion detection in Edge-of-Things computing[J]. Journal of Parallel and Distributed Computing, 2020, 137:259–265.

[134] Cui Z, Du L, Wang P, et al. Malicious code detection based on CNNs and multi-objective algorithm[J]. Journal of Parallel and Distributed Computing, 2019, 129:50–58.

[135] Rehman S, Khaliq M, Imtiaz S I, et al. Diddos: An approach for detection and identification of distributed denial of service (ddos) cyberattacks using gated recurrent units (gru)[J]. Future Generation Computer Systems, 2021, 118:453–466.

[136] Rose T, Kifayat K, Abbas S, et al. A hybrid anomaly-based intrusion detection system to improve time complexity in the Internet of Energy environment[J]. Journal of Parallel and Distributed Computing, 2020, 145:124–139.

[137] Sun Y, Wang S, Huang D, et al. A multiple hierarchical clustering ensemble algorithm to recognize clusters arbitrarily shaped[J]. Intelligent Data Analysis, 2022, 26(5):1211–1228.

[138] Zhao Y, Shrivastava A K, Tsui K L. Regularized Gaussian mixture model for high-dimensional clustering[J]. IEEE transactions on cybernetics, 2018, 49(10):3677–3688.

[139] Yang X, Deng C, Zheng F, et al. Deep spectral clustering using dual autoencoder network[C]. Pro-

ceedings of Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019. 4066–4075.

[140] Kwon D, Natarajan K, Suh S C, et al. An Empirical Study on Network Anomaly Detection Using Convolutional Neural Networks.[C]. Proceedings of ICDCS, 2018. 1595–1598.

[141] Van Wyk F, Wang Y, Khojandi A, et al. Real-time sensor anomaly detection and identification in automated vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 21(3):1264–1276.

致　　谢

本文是对我硕士两年多学习研究工作的一个总结，成文之际谨向多年来给予我指导、关心和帮助的各位老师、同学和家人们表示衷心的感谢！

首先我要感谢我的导师王立松教授，王老师对待工作认真负责，对待学生积极耐心，这让我十分尊敬。王老师的宽容豁达，让我看见了一位学者的风范和大度，也让我明白了为人处世的道理。非常感谢王老师给我提供了一个好的科研环境。

感谢南京中医药大学的丁有伟副教授，丁老师是我本科期间的导师，在丁老师身上，我感受到了一名科研工作者丰富的研究经验和扎实的理论基础。丁老师对学术科研的热情与追求潜移默化地影响着我，引领着我走上学术科研之路。同时，丁老师在日常生活方面也对我悉心关照，在我陷入焦虑和迷茫的时候给我指明方向，教会我在困境中依旧坚忍不拔、淡定从容。即便我已经本科毕业，丁老师依旧对我保持着十分的关爱、指导和照顾，感谢丁老师一直以来对我的关怀与帮助，对于我而言，丁老师将是我一辈子的良师益友！

感谢实验室的刘亮副教授。如果说丁老师使我产生了学术科研的萌芽，那么刘老师则是完全激发了我的科研兴趣。刘老师渊博的学识和严谨的治学态度深深地影响着我的科研工作。本文的研究工作便是在刘老师的悉心指导下完成的，一直以来刘老师就论文选题、研究思路、实验仿真以及论文撰写等方面都给予了我无微不至的指导和关心。同时，刘老师和我亦师亦友，在学习和生活方面都给予了我巨大的帮助，以他的人格魅力影响着我的为人处事。在刘老师的辛勤培育和关心帮助下，我收获的不仅仅是研究成果，更多的是研究方法和处世之道，这些将使我终身受益！

特别感谢山东大学的葛春鹏教授对我科研生涯的关心、指导和帮助！感谢 107 实验室的所有同学，谢谢你们带给我如同家人般的温暖！感谢马祖超师兄、彭剑飞师兄、李鑫师兄、孙姗姗师姐、徐翔宇师兄、陆艺仁、王枫、胡玲玲对我科研工作和日常生活的关心和帮助！

感谢我的父母对我学术生涯的理解和支持，从贫困和低保家庭将我养育至今，成人成才，谢谢你们二老一直以来对我无私的付出！感谢我的女朋友在心理和生活方面给我提供了诸多支撑，谢谢她一直以来对我的陪伴，因为她的出现我的生活变得更加精彩！

最后，向参加论文评审和答辩的各位老师致以最诚挚的谢意！

在学期间的研究成果及学术论文情况

攻读硕士学位期间发表（录用）论文情况

1. **Zhai W**, Sun S, Liu L, et al. HOTD: A Holistic Cross-Layer Time-Delay Attack Detection Framework for Unmanned Arial Networks[J]. Journal of Parallel and Distributed Computing, 2022.（CCF B 期刊，第一作者，已发表）
2. **Zhai W**, Liu L, Peng J, et al. PAR: A Power-Aware Routing Algorithm for UAV Networks[C]//International Conference on Wireless Algorithms, Systems, and Applications. Springer, Cham, 2022: 333-344.（CCF C 会议，第一作者，已发表）

攻读硕士学位期间投稿论文情况

1. **Zhai W**, Liu L, Ding Y, et al. ETD: An Efficient Time Delay Attack Detection Framework for UAV Networks[J]. IEEE Transactions on Information Forensics and Security, 2022. （CCF A 期刊，第一作者，小修已修回，终审中）
2. **Zhai W**, Liu L, Ding Y, et al. A Holistic Cross-Layer Routing Optimization Framework for UAV networks. （第一作者）
3. **Zhai W**, Wang F, Liu L, et al. Federated Semi-Supervised and Semi-Asynchronous Learning for Anomaly Detection in IoT Networks.（第一作者）

研究生期间参与的科研项目

1. 国家自然科学基金 (No.U20B2050, No. 82004499)
2. 国家重点研发计划 (No.2021YFB2700500, No.2021YFB2700502)
3. 面向信创产业基础软硬件供应链保障公共服务平台项目 (No.TC210804A)
4. 面向飞行区自主作业机器人的行为编程语言及其编译技术研究 (No.SATS202206)
5. 上海云曾科技有限公司，CDN 融合平台
6. 北京计算机技术及应用研究所，动态组网跨域认证及分布式无线密钥分发