

UANET 中基于任务感知的区块链共识与存储协同优化研究

姜来为^{1,2}, 廖江亨¹, 刘鑫³, 那振宇⁴

(1. 中国民航大学安全科学与工程学院, 天津 300300; 2. 中国民航大学计算机与人工智能学院, 天津 300300;
3. 大连理工大学信息与通信工程学院, 辽宁 大连 116024; 4. 大连海事大学信息科学技术学院, 辽宁 大连 116026)

摘要: 针对无人机自组织网络 (UANET) 中区块链共识协议通信复杂度高和节点存储资源受限的问题, 提出了 UANET 中面向任务的自适应动态共识协议 (ADAPT-BFT) 和协同任务存储优化策略 (TASK-Store)。ADAPT-BFT 通过任务感知检查器和自适应累加器等可信组件, 根据协同任务紧急程度和网络状态动态选择正常、追赶、协同 3 种共识模式; TASK-Store 基于任务分解依赖关系、协同热点访问模式和时效约束生命周期, 实现存储资源的精细化分配。仿真实验表明, 相比传统实用拜占庭容错 (PBFT) 协议, ADAPT-BFT 平均减少 69% 的共识时延; 相比全节点存储方案, TASK-Store 平均节省 63% 的存储开销, 在 UANET 不同网络规模和故障环境下均保持良好的可扩展性和容错能力。

关键词: 无人机自组织网络; 区块链; 共识协议; 存储优化; 协同任务

中图分类号: TP393.0; TP309.2

文献标志码: A

DOI: 10.11959/j.issn.1000-436x.2026004

Task-aware collaborative optimization of blockchain consensus and storage in UANET

Jiang Laiwei^{1,2}, Liao Jiangheng¹, Liu Xin³, Na Zhenyu⁴

1. School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China
2. School of Computer Science and Artificial Intelligence, Civil Aviation University of China, Tianjin 300300, China
3. School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China
4. School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

Abstract: Aiming at the problems of high communication complexity of blockchain consensus protocols and limited storage resources of UAV nodes in unmanned aerial vehicle ad-hoc network (UANET), an adaptive dynamic consensus protocol ADAPT-BFT for task-oriented scenarios and a collaborative task storage optimization strategy TASK-Store were proposed. The ADAPT-BFT was designed to dynamically select among normal, catch-up, and collaborative consensus modes based on task urgency and network conditions through trusted components including mission-aware checker and adaptive accumulator. The TASK-Store was developed to achieve fine-grained storage resource allocation based on task decomposition dependencies, collaborative hotspot identification, and time-constrained lifecycle management. Simulation experiments demonstrate that the ADAPT-BFT reduces consensus latency by 69% on average compared with the traditional practical Byzantine fault tolerance protocol (PBFT), while the TASK-Store saves 63% storage overhead on average compared with full-node storage schemes, maintaining good scalability and fault tolerance under different UANET network scales and fault environments.

Keywords: UANET, blockchain, consensus protocol, storage optimization, collaborative task

收稿日期: 2025-11-12; 修回日期: 2025-12-30

通信作者: 那振宇, nazhenyu@dlmu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.U2433205); 中央高校基本科研业务费专项资金资助项目 (No.3122018C022); 研究生科研创新资助项目 (No.2024YJSKC05002)

Foundation Items: The National Natural Science Foundation of China (No.U2433205), The Fundamental Research Funds for the Central University (No.3122018C022), Postgraduate Research and Innovation Project (No.2024YJSKC05002)

0 引言

无人机协同作业系统在现代军事侦察、灾害救援、环境监测、边界巡逻等关键应用中发挥着越来越重要的作用^[1]。为了高效地实现协同任务的执行,无人机群需构建具有动态组网特性的无人机自组织网络(unmanned aircraft vehicle ad-hoc network, UANET)。在此类分布式架构中,无人机节点与地面控制站(ground control station, GCS)共同构成协同作业网络,以实现任务数据的实时交互和协同任务的执行。

UANET在支撑协同任务执行方面面临严峻的安全挑战。相较于传统移动自组织网络^[2],UANET呈现出更为复杂的动态特性:无人机节点需要根据任务需求频繁调整位置,导致网络拓扑持续变化,节点间连接关系和通信质量不稳定;协同作业中的态势感知、目标识别等关键信息具有严格的时效性要求,过期信息不仅失去价值,还可能影响协同任务处理^[3]。与此同时,开放的通信环境使UANET易受数据窃听、会话劫持、虚假信息注入等多重攻击威胁^[4],恶意节点还可通过拒绝服务攻击快速耗尽无人机节点的电池电量。传统的中心化安全防护方案易产生单点故障,加上无人机节点在计算能力、存储容量和能源储备等方面均受到严格限制,使得直接部署现有的分布式安全解决方案变得极为困难^[5]。

区块链技术为构建UANET协同作业的安全防御体系提供了新思路^[6]。其分布式架构和不可篡改特性能够在不需要可信第三方的情况下实现多无人机间的安全协作和一致性决策。然而,传统区块链技术在UANET协同作业环境中的直接应用面临两个核心挑战,一是现有拜占庭容错共识协议的高通信复杂度与UANET动态网络特性之间的不匹配问题,固定的共识模式难以适应协同任务的多样化需求和网络环境的变化^[7];二是区块链数据的持续增长与无人机存储容量限制之间的矛盾,协同任务产生的大量交互数据使得无人机的存储压力大大增加^[8]。深入分析UANET中协同任务的执行特征可以发现,复杂任务往往需要分解为具有明确依赖关系的子任务序列,多无人机需要通过频繁的信息交互实现协同感知和决策,且许多应用场景对任务完成的时效性有严格要求^[9]。这些特征在区块链中表现为交易间复杂的引用依赖网络、以协同信息为中

心的热点区块访问模式,以及具有明确生命周期的时效敏感数据,为共识和存储优化提供了具体的设计依据。

综上所述,本文提出了面向UANET协同任务的区块链双重优化方案。该方案包含面向任务的自适应动态共识协议(ADAPT-BFT)和协同任务存储优化策略(TASK-Store)。本文主要的研究工作如下。

1) 提出了ADAPT-BFT,该协议突破了传统拜占庭容错共识协议固定执行模式的局限,创新性地引入任务感知检查器和自适应累加器等可信组件,能够根据协同任务的紧急程度和网络状态动态选择正常、追赶、协同3种共识模式。相比传统流水线化共识的固定三阶段执行,在网络稳定且前序任务已完成的情况下,正常共识模式仅需一个核心通信阶段即可完成共识。这种任务感知的模式切换机制使得协议能够在保证安全性的前提下,根据实际运行状况自动选择最优的共识模式,为UANET环境下的高效灵活共识提供了新的解决方案。

2) 设计了TASK-Store,该策略针对UANET协同任务的结构化特征,创新性地从任务分解依赖关系、协同热点访问模式和时效约束生命周期3个维度构建协同优化机制。与传统基于时间或简单引用计数的存储方案不同,TASK-Store通过分析任务分解依赖关系识别数据重要性,通过捕获协同热点访问模式优化缓存策略,通过时效约束生命周期实现精准的数据管理,3个维度的协同工作让TASK-Store建立了从任务语义到存储决策的映射关系,使得存储管理不再是对区块数据的盲目处理,而是基于任务执行逻辑的智能决策,保证了UANET中数据完整性和任务可靠性的有机统一。

3) 构建了无人机共识与存储协同优化的完整解决方案,共识协议的动态模式选择降低了UANET的通信开销和共识时延,为存储策略的高效执行创造了条件;存储策略通过精准的数据裁剪和压缩减轻了节点的存储负担,使得更多的存储资源可用于支持共识的完成,两者相互促进、协同优化。这种双重优化方案从通信效率和存储效率两个维度全面提升了UANET区块链系统的性能,为资源受限环境下的区块链应用提供了切实可行的技术路径。

1 相关工作

1.1 面向无人机协同任务的共识机制研究

区块链中的分布式共识为参与协同任务的多无人机建立了信任基础,然而传统共识协议在设计时主要考虑通用的网络环境,未充分考虑无人机场景下协同任务共识时的特殊需求。

以工作量证明 (proof of work, PoW) 为代表的能耗密集型共识机制不适用于能源受限的无人机网络。PoW 机制虽然提供了极大的安全性,但无人机有限的电池容量无法承担 PoW 中高能耗的算力需求^[3]。针对资源受限环境的优化研究中, Bahri 等^[10]提出的信任证明机制虽然降低了能耗,但要求所有节点达到相同信任度量,在协同任务中不同角色的无人机具有不同信任级别的情况下难以适用。Liu 等^[11]提出的多重协同证明机制虽然考虑了协作因素,但仍基于 PoW 框架,未能根本解决能耗问题。

实用拜占庭容错协议 (practical Byzantine fault tolerance protocol, PBFT) 在无人机网络规模扩大时面临通信复杂度瓶颈。PBFT 及其改进版本在联盟链中得到广泛应用,但传统 PBFT 的通信复杂度 $O(n^2)$ 限制了其在大规模无人机协同任务中的应用^[12]。现有 PBFT 优化方案在无人机协同任务场景下存在明显不足:文献[13]主要优化领导者的选取,未考虑协同任务中不同阶段对领导者能力的差异化要求;文献[14]虽然支持动态节点管理,但复杂的链排序算法增加了计算负担;文献[5]虽然结合信誉机制提升了共识的安全性,但该方案仅适用于稀疏型 UANET。

近年来出现的流水线化协议在无人机协同任务的紧急响应场景中仍有改进空间。文献[15]通过线性通信复杂度显著改善了可扩展性,但其固定的三阶段执行流程无法根据协同任务的紧急程度进行动态调整。文献[16]虽然引入可信执行环境技术减少了通信阶段,但该工作主要关注通用的网络环境,缺乏对无人机协同任务中任务优先级、任务依赖关系和时效约束等特征的深度优化。

1.2 面向无人机协同任务的存储优化研究

传统区块链的全节点存储模式在 UANET 环境中面临严重挑战,无人机节点的有限载荷难以存储不断增多的区块数据^[17]。

现有轻量级客户端^[18]只存储最近一段时间内

生成的区块,但难以保证任务数据查询的效率。文献[19]将轻量级块头存储在无人机节点,查询概率高的块体存储在雾节点中,而其他块体则卸载到云存储中。但该方法需要额外的区块调度算法进行维持,在网络分割时存在安全隐患。Xu 等^[20]提出的批量编码和基于高度的编码方法提供了基于纠删码的分布式存储优化思路,但 UANET 难以应对高昂的编解码计算开销和恶意节点传输错误编码块的问题。现有存储优化方案主要基于通用规则,未充分利用无人机协同任务的结构化特征。文献[21]通过过期区块消除和引用计数管理机制实现了存储优化,但其策略仍主要基于通用的时间和引用规则,未充分利用协同任务的结构化特征。然而, UANET 中协同任务数据具有明显的关联特征,为存储优化提供了清晰的设计思路,但现有研究在协同任务的特征利用方面仍存在不足。

综合分析可以发现,现有研究缺乏对无人机协同任务特征的系统化利用。在共识方面,现有方案要么沿用固定的多阶段执行流程,要么仅关注领导者选举等局部环节的改进,缺乏对协同任务动态特性的感知能力;在存储方面,现有方案主要依赖基于固定时间窗口的过期清理或基于全局引用计数的垃圾回收等通用机制,未能针对协同任务的结构化特征进行精细化管理。这些不足为基于任务分解依赖关系、多无人机协同热点访问模式、时效约束下生命周期3个维度设计任务感知的共识协议和存储策略提供了明确的优化方向。

2 系统模型

2.1 网络模型

本文考虑由 N 架无人机和一个 GCS 组成的 UANET 区块链系统,如图1所示。该模型包含3个核心要素,首先是节点角色与功能的对应,不同类型节点在区块链系统中承担不同的职责;其次是拜占庭容错能力,系统需要在存在恶意节点的情况下保证共识的正确性;最后是动态拓扑特性,高速移动的无人机会导致网络连接关系持续变化。基于上述考虑,系统采用分层架构设计,网络拓扑可表示为有向图 $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, 其中 $\mathcal{V} = \mathcal{U} \cup \{\text{GCS}\}$ 表示节点集合, \mathcal{E} 表示通信链路集合。

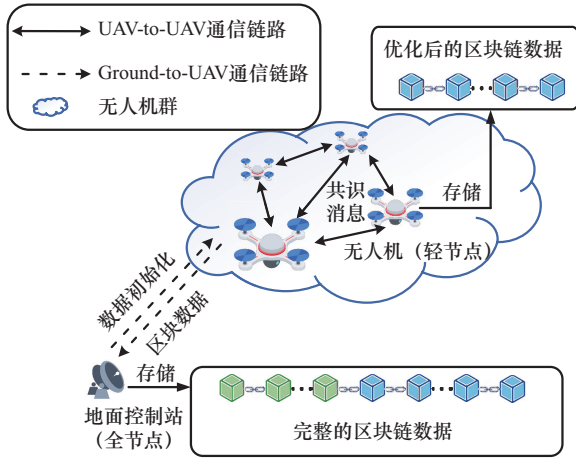


图1 UANET区块链系统模型

系统节点集合包含两类实体。

1) 无人机节点集合 $\mathcal{U} = \{u_1, u_2, \dots, u_N\}$, 其中 $|\mathcal{U}| = N$, N 为无人机总数。

2) GCS, 为单一的 GCS 节点, 具有强大的计算和存储能力。

总节点集合 $\mathcal{V} = \mathcal{U} \cup \{\text{GCS}\}$, 系统总节点数为 $N + 1$ 。根据功能和资源特性的差异, GCS 作为唯一的全节点存储完整的区块链数据 $\mathcal{B}_{\text{full}} = \{B_1, B_2, \dots, B_h\}$, 但不参与共识过程, 其中, B_i 表示第 i 个区块, h 为当前区块高度; 所有无人机节点 $u_i \in \mathcal{U}$ 均作为轻节点存储优化后的区块链数据 $\mathcal{B}_{\text{light}}^i \in \mathcal{B}_{\text{full}}$, 且积极参与共识过程。在开放的无人机网络环境中, 部分节点可能因硬件故障、软件漏洞或恶意攻击而表现出异常行为。为了评估系统的容错能力, 假设 f 为系统中最多可容忍的拜占庭故障节点数量, 则系统需满足 $N \geq 2f + 1$ 。其中, 诚实节点集合表示按照协议正确执行的无人机节点, 拜占庭节点集合表示可能表现出任意恶意行为的故障节点, 且节点集合满足互斥性和完整性。

无人机的移动特性使得网络拓扑呈现显著的动态性。在时刻 t , 无人机 u_i 与 u_j 的直接通信取决于它们的空间距离, 定义邻接矩阵元素 $A_{ij}(t)$ 为

$$A_{ij}(t) = \begin{cases} 1, & d_{ij}(t) \leq R_{\text{comm}} \\ 0, & d_{ij}(t) > R_{\text{comm}} \end{cases} \quad (1)$$

其中, $d_{ij}(t) = \|p_i(t) - p_j(t)\|_2$ 表示无人机 u_i 和 u_j 之间的欧氏距离, $p_i(t) = (x_i(t), y_i(t), z_i(t))$ 为无人机 u_i 在时刻 t 的三维坐标位置, R_{comm} 为无人机的通信

半径。基于邻接关系, 可进一步度量网络在时刻 t 的整体连通性。

$$C(t) = \frac{\sum_{i=1}^N \sum_{j=1}^N A_{ij}(t)}{N(N-1)} \quad (2)$$

其中, $C(t) \in [0, 1]$ 表示网络连通密度。当 $C(t) \geq C_{\text{min}}$ 时, 网络满足共识协议的基本连通性要求, C_{min} 为预设的最小连通度阈值。

2.2 通信模型

UANET 区块链系统支持两种主要的通信链路以满足不同的通信需求。UAV-to-UAV 通信链路实现无人机间的直接通信, 支持协同任务执行过程中的实时数据交换和共识消息传递。该链路采用无线自组织网络技术, 数据传输速率根据信道条件和距离动态调整。Ground-to-UAV 通信链路连接 GCS 与无人机, 主要用于系统初始化、证书分发和历史数据同步。GCS 具有更强的发射功率和更大的通信范围, 能够覆盖整个任务区域内的所有无人机。

无人机间通信采用自由空间传播模型, 信道增益随距离增加而衰减。在实际部署中, 通信链路质量会因无人机移动、环境障碍物和电磁干扰而动态变化, 因此协议设计需要具备适应性和鲁棒性。网络时延模型采用部分同步假设, 即存在未知的全局稳定时间 t_{GST} 和已知的消息传输时延上界 Δ , 在 t_{GST} 之后发送的所有消息都能在 Δ 时间内到达目的地。为保证消息的真实性和完整性, 系统采用椭圆曲线数字签名算法保证消息的真实性和完整性, 包含密钥生成 $(\text{sk}_i, \text{pk}_i) \leftarrow \text{KeyGen}(1^\kappa)$ 、签名生成 $\sigma \leftarrow \text{Sign}(\text{sk}_i, m)$ 和签名验证 $(0, 1) \leftarrow \text{Verify}(\text{pk}_i, m, \sigma)$ 3 个核心函数。其中, κ 为 256 bit 的安全参数, sk_i 和 pk_i 分别为节点 i 的私钥和公钥, m 为待签名消息, σ 为生成的数字签名。所有网络消息 m 都必须包含发送者的数字签名, 消息格式为 $(m, \sigma, \text{pk}_{\text{sender}})$, 接收者只有在验证 $\text{Verify}(\text{pk}_{\text{sender}}, m, \sigma)$ 成功后才处理消息。

2.3 任务模型

在 UANET 实际应用中, 复杂任务通常需要分解为多个子任务并分配给不同的 UAV 节点执行。这种任务分解机制不仅影响协同任务的执行效率, 更在区块链数据层面形成了特殊的引用模式和依赖结构。为利用这些 UANET 特征, 本节将从任务分解、协同依赖和时效约束 3 个维度建立任务模型,

为后续存储优化策略的设计奠定基础。

设主任务 M_0 被分解为 k 个子任务 $\sigma\{m_0, m_1, \dots, m_k\}$ 时, 每个子任务对应区块链中的一笔交易。子任务间的执行顺序和输入输出关系在区块链中表现为交易间的引用依赖网络。为量化这种依赖强度, 定义基于任务分解的引用频率为

$$\psi_{\text{decomp}} = \prod_{T_i \in \mathcal{T}} I\left(\exists M_j \in M: T_i \in \text{SubTasks}(M_j) \wedge |\text{SubTask}(M_j)| > 1\right) \quad (3)$$

其中, \mathcal{T} 表示系统中所有交易的集合, T_i 为第 i 笔交易, M_j 为第 j 个主任务。对于每笔交易 T_i , 指示函数 $I(\cdot)$ 判断是否存在某个主任务 M_j 要满足两个条件: 一是交易 T_i 属于该主任务的子任务集合 $\text{SubTasks}(M_j)$; 二是该主任务包含多个子任务, 即 $|\text{SubTasks}(M_j)| > 1$ 。当条件 $I(\cdot)$ 成立时返回1, 否则返回0。 ψ_{decomp} 值越大, 表明UANET中具有任务分解依赖关系的交易比例越高, 这类交易在协同任务执行中被频繁引用的可能性越大, 应在存储优化中优先保留。

多UAV协同作业场景要求节点间进行密切的信息交互, 协同任务的执行结果往往成为后续任务的输入依据。考虑UAV节点间的动态协同关系, 协同引用频率定义为

$$\psi_{\text{coop}}(t) = \frac{\sum_{ij} w_{ij}(t) \cdot \text{CoopMatrix}_{ij}}{\sum_{ij} w_{ij}(t)} \quad (4)$$

其中, 协同权重函数综合考虑空间邻近性和节点可信度。

$$w_{ij}(t) = \frac{1}{d_{ij}(t) + 1} \cdot \text{Rep}_i(t) \cdot \text{Rep}_j(t) \quad (5)$$

其中, $w_{ij}(t)$ 为时刻 t 节点 i 和 j 之间的协同权重, $d_{ij}(t)$ 为 t 时刻节点间通信距离, $\text{Rep}_i(t)$ 为节点 i 在时刻 t 的声誉值, 范围为 $[0, 1]$ 。

$$\text{Rep}_i(t) = \alpha_1 \cdot \text{Rep}_i(t - \Delta t) \cdot e^{-\lambda_1 \cdot \Delta t} + \alpha_2 \cdot \text{Perif}_i(t) \quad (6)$$

其中, $\text{Rep}_i(t - \Delta t)$ 表示节点 i 在上一时刻的声誉值, 通过时间衰减因子 $e^{-\lambda_1 \cdot \Delta t}$ 进行调整。 $\lambda_1 \in (0, 1]$ 为时间衰减系数, 取值越小表示历史声誉衰减越快。 Δt 为时间间隔, 权重系数 α_1 、 α_2 满足 $\alpha_1 + \alpha_2 = 1$ 且 $\alpha_1, \alpha_2 \in [0, 1]$, 分别控制历史声誉和当前节点状态对综合声誉的影响程度。 $\text{Perif}_i(t)$ 为节点 i 在时刻 t 的性能指标, 综合反映节点的任务完成质量和及时性。

$$\text{Perif}_i(t) = \omega_1 \cdot \frac{N_i^{\text{succ}}(t)}{N_i^{\text{total}}(t)} + \omega_2 \cdot \left(1 - \frac{D_i(t)}{D_{\text{max}}}\right) \quad (7)$$

其中, $N_i^{\text{succ}}(t)$ 表示节点 i 在时间窗口内成功完成的任务数, $N_i^{\text{total}}(t)$ 表示分配给节点 i 的总任务数, $D_i(t)$ 为节点 i 的平均任务时延, D_{max} 为系统允许的最大时延阈值, 权重系数 ω_1 、 ω_2 满足 $\omega_1 + \omega_2 = 1$ 且 $\omega_1 + \omega_2 \in [0, 1]$, 分别控制任务完成率和任务时延对节点性能的影响程度。协同矩阵 $\text{CoopMatrix} \in \mathbb{R}^{n \times n}$ 为对称矩阵, 元素 $\text{CoopMatrix}_{ij} \in [0, 1]$ 量化节点 i 与 j 之间的历史协同强度, 定义为

$$\text{CoopMatrix}_{ij} = \frac{\text{CoCount}(ij)}{\max(\text{CoCount}) \cdot \text{SucRate}(ij)} \quad (8)$$

其中, $\text{CoCount}(ij)$ 表示节点 i 和 j 在固定共识轮次内的协同任务次数, $\max(\text{CoCount})$ 为所有节点对中最大协同次数, $\text{SucRate}(ij)$ 为节点 i 和 j 协同任务的成功率。 $\text{CoopMatrix}_{ij} = 0$ 表示两节点从未协同, $\text{CoopMatrix}_{ij} = 1$ 表示两节点具有最高协同强度。

UANET中许多协同应用场景对任务完成的时效性有严格要求。针对具有时间约束的任务, 时效性引用频率定义为

$$\psi_{\text{time}}(T_i, t) = \begin{cases} \gamma \cdot e^{-\lambda_2(t - t_{\text{creat}}^i)}, & t - t_{\text{creat}}^i < \Delta T_{\text{expire}}^i \\ 0, & t - t_{\text{creat}}^i \geq \Delta T_{\text{expire}}^i \end{cases} \quad (9)$$

其中, t 为当前时刻, t_{creat}^i 为交易 T_i 的创建时间, $\Delta T_{\text{expire}}^i$ 为交易 T_i 对应任务的有效时间窗口, $\gamma \in (0, 1]$ 为基础引用强度参数, $\lambda_2 \in (0, 1]$ 为时间衰减系数控制引用价值的衰减速度。

综合上述任务分解、协同依赖和时效性约束3个维度, 系统的综合引用频率为

$$\psi(t) = \beta_1 \psi_{\text{decomp}} + \beta_2 \psi_{\text{coop}}(t) + \beta_3 \text{E}[\psi_{\text{time}}(T, t)] \quad (10)$$

其中, β_1 、 β_2 、 β_3 为权重系数满足 $\beta_1 + \beta_2 + \beta_3 = 1$ 且 $\beta_i \geq 0$, 分别控制任务分解依赖、协同热点和时效约束的权重; $\text{E}[\psi_{\text{time}}(T, t)]$ 为时效性引用频率在所有交易上的期望值。权重系数反映不同任务特征在具体应用场景中的相对重要性, 可根据任务类型动态调整。

3 方法设计

本文针对UANET协同任务的特点, 提出了共识与存储双重优化方案。图2为UANET协同任务处理流程, 具体展示了多无人机协同任务处理时的

三阶段过程。协同任务从 GCS 产生，由 GCS 分解子任务生成对应交易数据后按合理的发送速率发送给领导节点，领导节点通过交易数据构造的任务池对协同任务的处理进行 UANET 整体共识，采用 3 种共识模式应对不同的共识场景，共识过程中结合节点状态和任务优先级进行子任务的分配，最终通过共识结果实现协同任务的执行。共识结束后进入存储优化和数据恢复阶段，保证下一轮共识过程中节点存储状态和任务数据引用的执行效率。

3.1 ADAPT-BFT设计

ADAPT-BFT 旨在解决传统共识在 UANET 环境中面临的高通信复杂度和固定执行模式等问题。首先，本节通过可信执行环境构建任务感知检查器 (mission-aware checker, MAC) 和自适应累加器 (adaptive accumulator, AAC) 两个核心可信组件，为协议提供基本的安全保证；其次，定义核心消息类型，确保协议各阶段的准确执行；然后，根据新视图消息的完整性和任务状态信息，设计正常、追赶、协同 3 种动态共识模式，使协议能够根据协同任务的紧急程度和网络状态自动选择最优的共识模式；最后，通过证明确保该共识协议的安全性和活性。

3.1.1 可信执行环境组件

ADAPT-BFT 采用混合信任架构，结合密码学安全保证和可信执行环境的硬件支持。协议设计了 MAC 和 AAC 两个核心的可信组件，这两个组件协同工作作为协议提供关键的安全保证和效率提升。MAC 是每个无人机节点都配备的基础可信组件，其状态由 3 个部分组成：机密私钥和其他组件的公钥、单调递增的 (view, phase) 对以及最新准备区块的视图编号。MAC 提供 3 个核心功能，TEE_prepare 用于领导者提议新区块，保证每个视图最多只能提议一次；TEE_vote 用于对区块进行投票；TEE_store 用于存储最新提议的区块并生成存储证书。AAC 是仅由视图领导者运行的高级可信组件，其核心功能是聚合和验证来自其他节点的消息，以及根据当前情况选择最优的共识模式。AAC 接收来自其他节点的新视图消息，分析其中包含的任务信息和网络状态，然后决定采用正常共识、追赶共识还是协同共识等不同的共识模式。

3.1.2 协议消息定义

为了确保协议各阶段的准确执行，ADAPT-BFT 定义了一套精简而完备的消息类型体系。这些消息不仅装载了共识过程中的关键信息，更通过可信组件生成的证书保证消息的可验证性和不可伪造性。

共识协议的核心消息首先是任务提议消息 $\tau_p = \langle \text{task}_{\text{data}}, \varphi_{\text{mp}}, \text{ctx} \rangle$ ，其中， $\text{task}_{\text{data}}$ 表示具体的协同任务数据， φ_{mp} 为 MAC 生成的提议证书， ctx 为任务上下文信息，指在无人机协同任务执行过

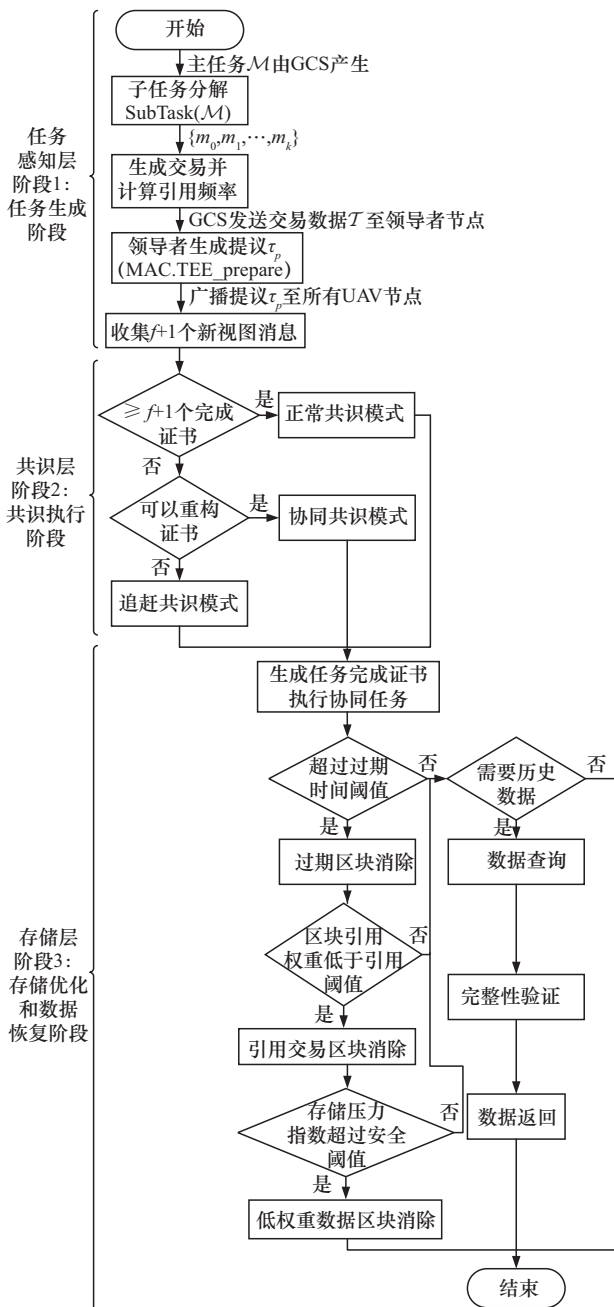


图2 UANET 协同任务处理流程

程中,为了保证任务的正确执行和协同配合而需要维护和传递的相关状态信息集合,包括任务依赖关系、执行进度、资源分配等关键要素。提议消息由视图领导者通过调用MAC的TEE_prepare函数生成,该函数的单调性约束保证每个视图最多只能进行一次提议,从而避免了领导者的双重提议攻击。

当节点接收并验证任务提议消息后,会调用TEE_store函数生成存储证书 $\varphi_{mp} = \langle \text{view}_s, \text{hash}_t, \text{view}_p, \sigma_i \rangle$,表示节点*i*在视图 view_s 中存储了在视图 view_p 中提议的哈希值为 hash_t 的任务数据。其中, view_s 表示节点存储该任务数据时编号为*s*的视图, hash_t 表示任务数据的哈希值, view_p 表示该任务数据最初被提议时编号为*p*的视图, σ_i 表示节点*i*的数字签名。

当领导者收集到足够多的存储证书后,将其聚合形成任务完成证书 $\varphi_{comp} = \langle \text{view}_c, \text{hash}_t, \text{view}_p, \sigma^{f+1} \rangle$,其中, view_c 任务数据达成共识时编号为*c*的视图, σ^{f+1} 表示聚合了*f*+1个节点的数字签名,证明在视图 view_c 中存储了在视图 view_p 中提议的哈希值为 hash_t 的任务数据已被足够多的节点确认。任务完成证书是共识达成的标志,其聚合签名机制既保证了安全性又减少了消息量。

在视图切换过程中,节点向新领导者发送新视图消息 $\varphi_{comp} = \langle \text{view}_c, \text{hash}_t, \text{view}_p, \sigma^{f+1} \rangle, \mu_{nv} = \langle \tau_p, \varphi_{store}, \varphi_{comp} \rangle$,包含节点已知的最新任务提议消息 τ_p 、相应的存储证书 φ_{store} 和任务完成证书 φ_{comp} 。新视图消息为领导者提供了当前UANET的状态,使其能够做出准确的模式选择决策。这些消息类型共同构成了ADAPT-BFT的通信基础,为动态共识模式的灵活切换提供了有力支撑。

3.1.3 动态共识模式设计

ADAPT-BFT采用信誉机制来增强系统安全性,通过维护黑名单 \mathcal{L} 识别和隔离频繁超时、发送无效消息等异常行为节点,并将其排除在领导者选择之外。ADAPT-BFT根据新视图消息的完整性和任务状态信息进行模式选择,不同共识模式通过调整各阶段的具体实现进行差异化处理。协议采用四阶段执行框架。

新视图阶段:所有节点向新领导者发送包含最新任务 τ_p 、存储证书 φ_{store} 和任务完成证书 φ_{comp} 的新视图消息 μ_{nv} ,领导者收集至少*f*+1个新视图消

息后构成消息集合 $\mathcal{M}_{nv} = \{\mu_{nv}^1, \mu_{nv}^2, \dots, \mu_{nv}^{f+1}\}$,为后续的模式选择提供决策依据。

准备阶段:领导者基于新视图消息集合 \mathcal{M}_{nv} 的分析结果选择共识模式,构造并广播任务提议消息 τ_p ,节点验证合法性后返回存储证书 φ_{store} 。

决定阶段:领导者聚合至少*f*+1个存储证书生成任务完成证书 φ_{comp} 并广播,节点验证后执行协同任务并更新本地状态。

任务执行阶段:节点根据任务类型和优先级执行协同操作,更新任务上下文ctx,并维护任务依赖关系。

本文利用2.1节定义的网络连通密度 $C(t)$ 和2.2节的部分同步假设参数 Δ 和 t_v 作为模式切换的量化依据,设计了3种动态共识模式。

1) 正常共识模式

该模式适用于网络状态良好且前一视图已完成共识的理想情况,仅需一个核心通信阶段即可完成。进入条件为:至少*f*+1个新视图消息 μ_{nv} 包含完整的任务完成证书 φ_{comp} ;这些任务完成证书指向同一个已确认的任务数据;网络连通度满足 $C(t) \geq C_{min}$,且新视图消息的收集时间未超过时延上界 Δ 。

正常共识模式的执行流程如图3所示。由于前一视图已成功完成共识,多数诚实节点持有相同的 φ_{comp} ,领导者据此直接构造扩展前序任务的新提议 τ_p 。各节点验证任务合法性和依赖关系后生成存储证书,领导者聚合后广播任务完成证书,节点执行协同操作并记录结果至ctx。

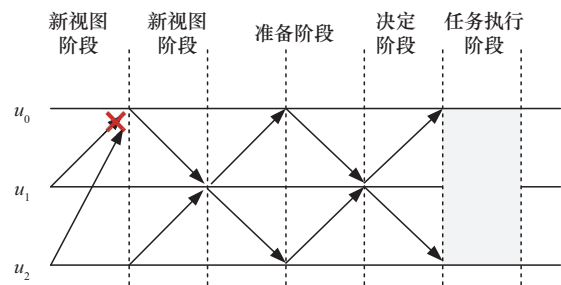


图3 正常共识模式的执行流程

2) 追赶共识模式

该模式处理存在共识任务未完成的复杂情况,通过额外的数据传递机制完成中断的共识过程。进入条件为:新视图消息中少于*f*+1个完整任务完

成证书；无法从现有的存储证书中重构出 $f+1$ 个聚合证书；存在未完成共识的任务数据，即收集到的存储证书数量满足 $1 \leq |\varphi_{\text{store}}| \leq f+1$ ；前一视图因响应时间超过 t_v 而触发超时切换或网络连通度 $C(t) < C_{\text{min}}$ 。

追赶共识模式的执行流程如图 4 所示。领导者分析不完整的证书信息后，识别出需追赶的最高优先级未完成的任务，调用 AAC 的 TEE_accum 函数生成累加器证书 acc 并广播。节点验证后调用 TEE_vote 生成投票证书 φ_{vote} 。领导者聚合至少 $f+1$ 个投票证书后构造新提议，后续流程与正常模式类似。本轮共识实际完成两个任务确认：被追赶的前序任务和当前新提议任务，节点需按依赖顺序执行以保证协同作业的连续性。

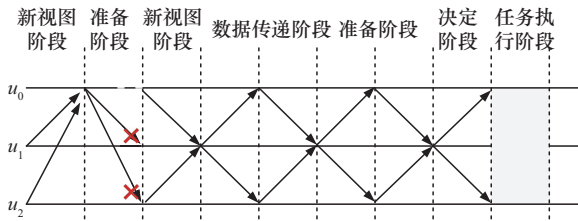


图 4 追赶共识模式的执行流程

3) 协同共识模式

该模式是针对 UANET 协同任务特征设计，当能够从新视图消息中重构出有效的法定人数证书时，可将前序任务的确认信息携带在新提议中实现批量确认。进入条件为：新视图消息中少于 $f+1$ 个任务完成证书，但收集到足够的存储证书 φ_{store} ；这些存储证书都指向同一个任务数据，且数量达到 $f+1$ 个；能够通过聚合这些存储证书重构出有效的任务完成证书；网络连通度 $C(t) \geq C_{\text{min}}$ 且当前消息响应时间不超过时延上界 Δ 。

协同共识模式的执行流程如图 5 所示。领导者从新视图消息中提取并验证存储证书的一致性，聚合重构出任务完成证书 $\varphi_{\text{comp}}^{\text{rc}}$ 。在广播扩展前序任务的新提议时，同时携带 $\varphi_{\text{comp}}^{\text{rc}}$ ，实现双重确认，明确前序任务完成状态的同时提议新任务。节点首先验证重构证书的有效性，再验证新提议与前序任务的依赖关系，通过后生成存储证书。任务执行时，节点优先处理尚未执行的前序任务，再执行当前新任务。

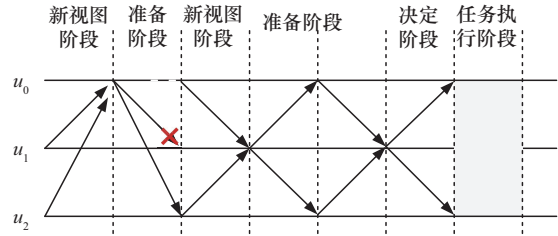


图 5 协同共识模式的执行流程

3.1.4 协议安全性与活性保证

ADAPT-BFT 通过多层验证机制保证安全性，包括可信组件的单调性约束、数字签名验证和严格的任务依赖性检查。活性通过超时机制和视图切换保证，确保系统在异常情况下能够自动恢复。

定理 1 安全性。当存在最多 f 个拜占庭节点且 $N \geq 2f+1$ 的条件下，ADAPT-BFT 保证不会有冲突的任务数据被诚实节点执行。

证明 根据 3.1.3 节协议流程可知，任务数据被执行的充要条件是诚实节点接收到有效的任务完成证书 φ_{comp} 。证毕。

引理 1 存储证书的唯一性。对于同一视图，诚实节点 u_i 至多为一个任务数据生成存储证书。

根据 3.1.1 节，存储证书由 MAC 组件的 TEE_store 函数生成。MAC 的状态包含单调递增的 (view, phase)，保证每个视图中的每个阶段最多执行一次。因此诚实节点在视图的准备阶段至多调用一次 TEE_store，只能为一个任务数据生成存储证书。

引理 2 诚实节点的确定性。在 $N \geq 2f+1$ 的系统中，任意两个包含 $f+1$ 个节点的集合必然至少包含一个诚实节点。

设诚实节点集合 \mathcal{H} 满足 $\mathcal{H} \geq f+1$ 。考虑两个大小为 $f+1$ 的节点集合 \mathcal{S}_1 和 \mathcal{S}_2 。若 $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ ，则 $|\mathcal{S}_1 \cap \mathcal{S}_2| = 2f+2$ 。但系统总节点数 $N \geq 2f+1$ ，当 $N = 2f+1$ 时， $\mathcal{S}_1 \cup \mathcal{S}_2$ 需要 $2f+2 > N$ 个节点，矛盾。因此 $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \emptyset$ ，且由于拜占庭节点最多 f 个，交集中心必包含至少一个诚实节点。

假设存在两个冲突的任务提议消息数据 τ_1 和 τ_2 在同一视图中都被诚实节点执行，则存在任务完成证书 $\varphi_{\text{comp}}^1 = \langle \text{view}_c^1, \text{hash}_t^1, \text{view}_p^1, \sigma_1^{f+1} \rangle$ 对应 τ_1 ，任务完成证书 $\varphi_{\text{comp}}^2 = \langle \text{view}_c^2, \text{hash}_t^2, \text{view}_p^2, \sigma_2^{f+1} \rangle$ 对应 τ_2 。

根据引理 2，签名集合 σ_1^{f+1} 和 σ_2^{f+1} 对应的节点

集合必有交集, 且交集中至少包含一个诚实节点 u_h 。这意味着诚实节点 u_h 在同一视图中为两个不同的任务数据 τ_1 和 τ_2 都生成了存储证书, 这与引理 1 矛盾。

因此假设不成立, 不会有两个冲突的任务数据在同一视图被诚实节点执行。对于不同视图的情况, 结合 3.1.3 节的新视图阶段设计, 后续视图必须基于前序视图的任务完成证书进行扩展, 保证了跨视图的一致性。证毕。

定理 2 活性。在网络最终同步且存在足够多诚实节点领导的视图条件下, ADAPT-BFT 保证诚实节点最终会执行新的任务数据。

证明 由 2.2 节可知, 存在未知的全局稳定时间 t_{GST} 和已知的消息传输时延上界 Δ , 在 t_{GST} 之后发送的所有消息都能在 Δ 时间内到达。

引理 1 表明, 当视图的领导者是诚实节点 u_L 且网络处于同步状态时, 该视图能够在有限时间内完成共识。

考虑诚实领导者 u_L 在视图中的执行过程。

1) 新视图阶段: u_L 收集至少 $f+1$ 个新视图消息 μ_{nv} 。由于网络同步, 所有诚实节点的消息能在 Δ 时间内到达。

2) 准备阶段: u_L 通过 MAC 的 TEE_prepare 生成任务提议消息 τ_p 并广播。由于 u_L 是诚实节点, 其提议合法有效。所有诚实节点在 Δ 时间内收到提议, 验证通过后调用 TEE_store 生成存储证书 ϕ_{store} 并返回给 u_L 。

3) 决定阶段: u_L 在至多 Δ 时间内收集到至少 $f+1$ 个存储证书, 聚合生成任务完成证书 ϕ_{comp} 并广播。所有诚实节点在 Δ 时间内收到 ϕ_{comp} , 验证通过后执行任务。

总时间复杂度为 $O(\Delta)$, 因此, 在 t_{GST} 之后发送的所有消息都能在 Δ 时间内到达。

引理 2 表明, 在网络同步状态下, 系统最终会进入由诚实节点领导的视图。

根据 3.1.3 节, 当视图超时未达成共识时, 触发视图切换。考虑领导者选择机制, 拜占庭节点被加入黑名单 \mathcal{L} 并排除在领导者候选之外, 按轮询方式 $u_L(\text{view}) = (v \bmod |\mathcal{U} \setminus \mathcal{L}|)$ 从诚实节点中选出领导者节点。由于诚实节点至少有 $f+1$ 个, 在至多 N 个视图内必定选中诚实领导者。结合引理 1, 该视图能够完成共识。

给定初始状态, 系统从视图 view_0 开始。若视图 view_0 的领导者是诚实节点, 由引理 1, 在 t_{GST} 后的时刻 $t \geq t_{\text{GST}} + O(\Delta)$, 诚实节点执行新的任务数据。假设到视图 view_k 尚未完成共识。考虑以下两种情况。

1) view_k 的领导者是拜占庭节点或网络未同步。经过视图超时 t_v 后, 触发视图切换到 view_{k+1} 。

2) 重复视图切换, 由引理 2, 至多 N 步必定进入由诚实节点领导且网络同步的视图 view_m 。

在视图 view_m 中, 由引理 1, 系统在有限时间内完成共识, 所有诚实节点执行新的任务数据。结合上述分析, 在 t_{GST} 之后的时刻 $t \geq t_{\text{GST}} + N \cdot t_v + O(\Delta)$, 诚实节点最终执行新的任务数据, 保证协议的活性。特别地, 3.1.3 节设计的 3 种共识模式都遵循相同的安全性和活性保证, 只是在执行效率上有所优化。证毕。

3.2 TASK-Store

本文提出的 TASK-Store 的核心设计理念是融合 UANET 中协同任务执行的结构化特征, 通过过期区块消除机制、引用交易区块消除机制和存储空间的动态管理实现比传统时间驱动或简单引用计数方法更加高效的存储管理方式。该策略的核心依据是, UANET 中的区块链数据并非均质的存储对象, 而是承载着不同任务语义和重要性级别的结构化信息载体。通过识别和利用任务分解依赖关系、协同热点访问模式以及时效约束生命周期, TASK-Store 能够在保证数据一致性和系统功能完整性的前提下, 显著降低无人机节点的存储开销。

3.2.1 过期区块消除机制

任务分解结构为存储优化提供了丰富的语义信息和清理依据。在 UANET 中, 复杂任务的分解通常遵循一定的逻辑结构, 子任务之间存在明确的执行顺序、条件依赖或并行关系。TASK-Store 通过构建任务分解图来刻画这种引用依赖关系。任务分解图是一个有向无环图 $\mathcal{G}_{\text{task}} = (\mathcal{V}_{\text{task}}, \mathcal{E}_{\text{task}})$, 其中节点 $v_i \in \mathcal{V}_{\text{task}}$ 代表子任务对应的区块链交易, 边 $e_{ij} \in \mathcal{E}_{\text{task}}$ 代表任务间的依赖关系。

对于交易 T_i , 系统根据其所属主任务的执行状态来判定任务完成状态。当交易 T_i 属于某个正在运行的主任务 M_i 时, 其状态标记为活跃状态; 当交易 T_i 所属的所有主任务都已完成时, 其状态标记为完成状态; 否则标记为过期状态。

当区块 B_k 中包含的所有交易都处于过期状态, 且 B_k 的创建时间与当前时间的差值超过基于任务特征动态确定的过期时间阈值 $T_{\text{expire}}^{\text{task}}$ 时, 则区块 B_k 成为过期区块。

基于任务分解的过期区块消除过程中, 系统首先遍历区块链 $\mathcal{B}^{\text{full}}$ 中的所有区块, 检查每个区块是否满足过期判定条件。对于满足条件的区块, 系统进一步验证其在任务分解图 $\mathcal{G}_{\text{task}}$ 中是否存在活跃的依赖关系。只有当确认区块的移除不会破坏任务依赖链的完整性时, 系统才会执行实际的清理操作。

3.2.2 引用交易区块消除机制

TASK-Store 中的引用交易区块消除机制综合考虑任务分解引用、协同依赖引用和时效性引用 3 个维度, 对区块中的交易数据进行生命周期管理。当交易数据完成对应的协同任务后, 相应的区块即可被安全清理, 从而释放宝贵的存储空间。

在 UANET 协同任务执行过程中, 后续任务通常需要引用前置任务的执行结果作为输入条件。对于交易 T_i , 首先定义引用该交易的后续交易集合为 \mathcal{R}_i , 已完成执行的引用交易集合为 \mathcal{C}_i , 则交易 T_i 的引用完成度表示为

$$RC_i = \frac{|\mathcal{C}_i|}{|\mathcal{R}_i|} \quad (11)$$

其中, \mathcal{R}_i 表示所有引用 T_i 的后续交易集合, $\mathcal{C}_i = \{T_j \in \mathcal{R}_i \mid \text{Status}(T_j) = 1\}$ 表示 \mathcal{R}_i 中已完成的交易子集。Status(T_j) 表示 T_j 的执行状态, Status(T_j) = 1 表示交易 T_j 已完成; Status(T_j) = 0 表示交易 T_j 未完成。当 $RC_i = 1$ 时, 表示所有引用交易 T_i 的后续任务都已完成执行, 该交易可以考虑进行存储优化; 当 $RC_i = 0$ 时, 表示仍有后续任务需要该交易的数据支持。

基于交易级别的引用完成度, 可进一步评估整个区块的引用权重。区块 B_k 的引用权重定义为

$$BW_k(t) = \sum_{T_i \in B_k.\text{txList}} [\psi(t) \cdot (1 - RC_i) \cdot \text{Pri}_i] \quad (12)$$

其中, Pri_i 表示交易 T_i 对应任务的优先级权重, $B_k.\text{txList}$ 表示 B_k 中包含的交易列表, $(1 - RC_i)$ 表示交易 T_i 的剩余引用需求强度。引用完成度越低的交易具有更高的保留权重, 而引用完成度高的交易则更适合进行存储优化。

基于引用频率的交易区块消除策略采用渐进式

清理方法。系统定期计算每个区块的引用权重 $BW_k(t)$, 当区块的引用权重低于动态设定的阈值 $\psi_{\text{threshold}}$ 时, 进一步验证区块中所有交易的引用完成情况。对于满足 $RC_i = 1$ 的交易, 系统执行区块压缩操作, 移除区块体但保留区块头用于完整性验证。当区块 B_k 被压缩后, 原本指向该区块交易的引用指针 $\{B_k.\text{index}, T_i.\text{index}\}$ 将重定向到引用了该交易且仍活跃的后续交易 $\{B_j.\text{index}, T_j.\text{index}\}$, 其中 $B_j.\text{index}$ 和 $T_j.\text{index}$ 分别表示目标区块和交易的索引。这种重定向机制通过引用链传递确保了数据依赖关系的完整性, 使得即使原始交易数据被压缩, 其语义信息仍能通过引用链追溯。

3.2.3 存储空间动态管理

TASK-Store 实现了基于存储压力和任务优先级的动态存储管理机制。该机制根据当前存储使用情况和协同任务的紧急程度, 动态调整存储策略的激进程度。在存储充足时保留更多历史数据, 在存储紧张时优先保证当前活跃任务的数据需求。

为精确评估节点的存储压力状况, 节点 u_i 的存储压力指数 SP_i 反映了存储资源的紧张程度和任务执行的紧迫性。

$$SP_i = \frac{S_{\text{used}}^i}{S_{\text{total}}^i} \cdot (1 + U_{\text{avg}}^i) \quad (13)$$

其中, S_{used}^i 表示节点 u_i 已使用的存储空间, S_{total}^i 表示节点 u_i 的总存储容量, U_{avg}^i 表示节点 u_i 当前活跃任务的平均紧急程度。引用频率阈值采用自适应调整策略。

$$\psi_{\text{threshold}}^i = \psi_{\text{base}} \cdot (1 - SP_i) + \psi_{\text{min}} \quad (14)$$

其中, $\psi_{\text{base}} \in (0, 1)$ 为系统预设存储清理的基准阈值, $\psi_{\text{min}} \in (0, \psi_{\text{base}})$ 为最小保护阈值, 为防止过度清理的保护下限, $\psi_{\text{threshold}}^i(t)$ 为节点 u_i 在时刻 t 的动态阈值。当存储压力 SP_i 增大时, 阈值 $\psi_{\text{threshold}}^i(t)$ 降低, 存储策略变得更加激进; 当存储压力较小时, 阈值提高, 保护更多的历史数据。节点 i 的引用阈值 $\psi_{\text{threshold}}^i(t)$ 决定了固定轮次共识结束后触发引用交易区块消除的判定条件, 2.3 节的综合引用频率 ψ 通过任务分解依赖、协同热点和时效约束来影响交易的引用依赖链长度和引用频率, 进而影响整个区块的引用权重 $BW_k(t)$, 间接决定了区块的存储生命周期。当 $BW_k(t) < \psi_{\text{threshold}}^i(t)$ 时, 触发引用交

易区块消除机制。

TASK-Store 综合存储管理采用三阶段清理策略。第一阶段执行基于任务分解的过期区块消除,清理明确过期且无依赖关系的任务数据;第二阶段基于引用频率进行精细化管理,压缩已完全引用的区块;第三阶段在存储压力超过安全阈值 θ_{safe} 时进行紧急清理,优先清理权重最低的数据块。该分层机制根据存储压力动态调整清理激进程度,在保证数据完整性前提下最大化存储效率。

通过任务分解依赖关系分析、协同热点访问模式识别和时效约束生命周期管理三维协同优化,TASK-Store 实现了任务感知的精准存储决策,在保证协同任务数据完整性的前提下显著减少无人机节点的存储负担,为资源受限的 UANET 环境提供了切实可行的存储优化解决方案。

4 实验与性能分析

4.1 实验设置

为了验证本文提出的 ADAPT-BFT 和 TASK-Store 在 UANET 环境下的有效性,本文采用 Intel (R) Xeon(R) Silver 4210R CPU,主频为 2.40 GHz,配备 32.0 GB RAM 的硬件配置和 Block Emulator 仿真器进行实验评估。为了获得更贴近实际应用的仿真结果,实验基于 DJI Matrice 100 飞行数据集的统计分析,配置了贴近真实 UANET 环境的仿真参数,如表 1 所示。无人机飞行模式采用数据集中验证的三角形巡航路径,能够有效覆盖目标区域并保

持网络连通性。

为了全面评估本文方法的性能优势,选择以下几种具有代表性的共识协议作为对比基准。

1) 文献[12]作为经典的实用拜占庭容错协议,采用传统的 $3f + 1$ 节点容错模型,在小规模网络中表现稳定但通信复杂度较高。

2) 文献[15]作为流水线化拜占庭容错协议(Byzantine fault tolerance Protocol, BFT) 的典型代表,具有线性通信复杂度特性,在可扩展性方面有所改进。

3) 文献[16]是基于可信执行环境的混合共识协议,采用 $2f + 1$ 节点容错模型并使用两个通信阶段达成共识。

4) 文献[21]是专门面向无人机网络设计的轻量级区块链方案,在存储和通信方面进行了针对性优化。

4.2 引用阈值对存储负载的影响实验

为了具体验证 TASK-Store 在不同引用密度环境下的存储优化效果,本文设计了引用阈值变化对无人机节点存储负载影响的对比实验。该实验通过调整区块间的引用频率参数,模拟从稀疏引用到密集引用的不同应用场景,在 1 000 轮共识过程中持续监测各节点的存储空间占用情况。

图 6 的实验结果清晰地展现了 TASK-Store 的显著优势。与传统的全节点存储方案相比,采用 TASK-Store 的轻节点在整个实验过程中始终保持相对稳定且较低的存储开销。在传统的全节点存储方案中,由于全节点需要存储所有完整的区块链数

表 1 系统参数

参数	含义	参数值	参数	含义	参数值
N	无人机节点数量/个	10~190	λ_1	信誉时间衰减系数	0.95
v_u	无人机飞行速度/(m·s ⁻¹)	10	α_1, α_2	声誉更新权重系数	0.6、0.4
s_u	无人机飞行区域范围/km	3.5 × 3.5	ω_1, ω_2	性能权重系数	0.5、0.5
h_u	无人机飞行高度范围/m	200~1000	θ_{safe}	安全存储阈值	0.8
R_{comm}	通信半径/m	300	γ	基础引用强度	1.0
W	带宽/(bit·s ⁻¹)	1 × 10 ⁸	λ_2	任务引用时间衰减系数	0.1
C_{min}	网络连通度阈值	0.6	$\beta_1, \beta_2, \beta_3$	综合引用频率权重系数	0.4、0.35、0.25
Δ	通信时延上界/ms	100	t_v	视图超时时间/s	1
T_{size}	交易大小/B	1 000	T_{co}	协同强度矩阵更新间隔/轮	20
B_{size}	区块大小/tx	3 500	ψ	引用阈值	0.1~0.6
T_{rate}	交易注入率/(tx·s ⁻¹)	5 500	ψ_{base}	基准引用阈值	0.4
B_{inter}	区块间隔/s	15	ψ_{min}	最小保护阈值	0.1
D_{max}	最大时延阈值/ms	500	T_{expire}^{task}	过期时间阈值/s	30
f	故障节点数/个	1~30			

据,没有任何优化策略,存储开销持续累积呈线性增长态势。随着交易引用阈值 ψ 的变化,TASK-Store呈现出不同的性能特征。当 $\psi = 0.4$ 时表现最优,这是因为更高的 ψ 值意味着更频繁的交易引用,使TASK-Store能有效地删除被引用完的无用区块,实现存储空间的动态释放。然而,当交易引用阈值继续增加时,系统开始出现性能劣化效应,存储负担反而增大。这是因为当交易引用阈值增大后,每个交易需要存储更多的引用指针来实现交易的引用机制,存储负担也会随之增加。

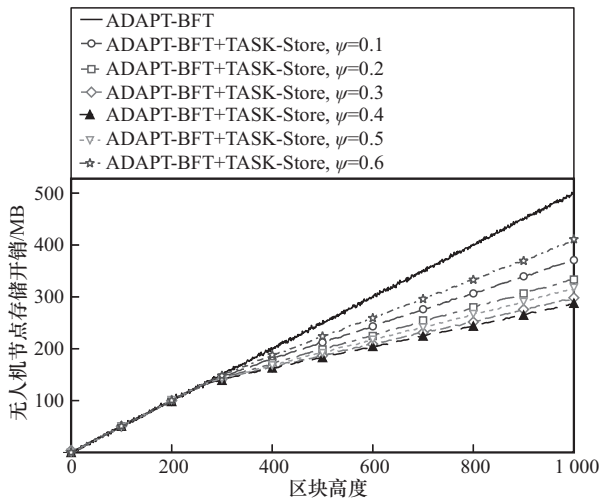


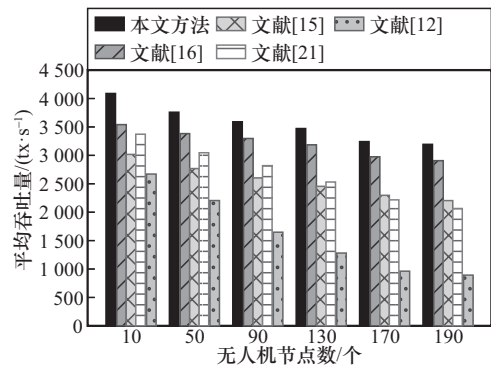
图6 引用阈值对无人机节点存储开销的影响

4.3 节点规模对共识吞吐量与时延的影响实验

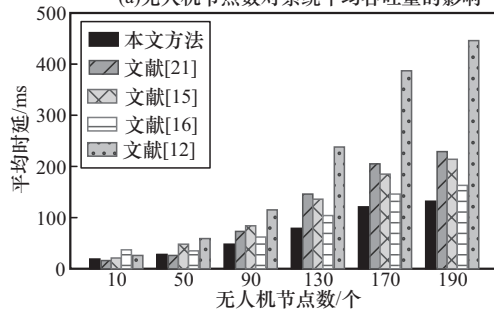
为了评估ADAPT-BFT在不同网络规模下的可扩展性表现,本文设计了无人机节点数对系统平均吞吐量的影响,如图7(a)所示。ADAPT-BFT在整个节点范围内始终保持最高吞吐量。在10个节点的小规模网络中,ADAPT-BFT相比文献[12]提升53.1%,相比文献[16]提升15.5%。随着节点数增加到190个,ADAPT-BFT的吞吐量性能保持率为78.1%,文献[12]性能保持率仅为33.4%,文献[16]性能保持率为82.1%。这主要得益于ADAPT-BFT在正常共识模式下的高效性,以及TASK-Store对通信开销的有效控制。ADAPT-BFT的自适应执行模式设计使其能够根据网络状态动态选择最优的共识模式,在网络条件良好时采用正常共识模式以最大化效率,在网络出现异常时切换到多阶段的协同共识模式或追赶共识模式以保证可靠性。

无人机节点数对系统平均时延的影响如图7(b)所示,本文方法也表现出了更为突出的优势。在

10个节点时,本文方法的平均时延为19ms,高于文献[21]的16ms,但优于其他方法。随着网络规模的扩展,本文方法的时延增长曲线保持相对平缓。在190个节点的大规模场景下,本文方法的时延相比文献[12]降低70.4%,相比文献[21]降低42.4%,相比文献[15]降低38.3%,相比文献[16]降低19.0%。这一性能优势在中等规模网络中表现尤其突出。从ADAPT-BFT的设计理念上看,首先,ADAPT-BFT通过TEE组件的支持减少了通信阶段的数量,将正常情况下的共识过程简化为一个核心通信阶段;其次,TASK-Store通过裁剪区块进一步减少了不必要的数据传输和存储操作。两者的结合使得在保证拜占庭容错能力的前提下,显著降低了共识过程的时间复杂度。



(a)无人机节点数对系统平均吞吐量的影响



(b)无人机节点数对系统平均时延的影响

图7 节点规模对共识性能的影响

4.4 拜占庭故障环境下的容错性能评估实验

为了验证ADAPT-BFT在存在拜占庭节点的动态环境下的鲁棒性和恢复能力,本文设计了定故障阈值下的运行时吞吐量波动监测实验。该实验设置无人机节点数为30,故障阈值为9,在较长的运行时间内持续监测各共识方法的瞬时吞吐量变化,重点观察各方法在面对节点故障和网络异常时的响应机制和恢复速度。

图8为 $N=30, f=9$ 下的运行时吞吐量波动监测。

从图 8 可以看出, 包括本文方法在内的流水线化共识方法都会出现瞬时吞吐量降为零的情况, 这一现象的根本原因在于领导者轮询机制检测到超时无响应时触发的非决定性视图切换过程。相比之下, 非流水线化的 BFT 类共识中, 文献[12]和文献[21]虽然在普通节点故障时会引起性能下降, 但没有出现吞吐量骤降的情况, 在安全的敌手模型范围内表现相对稳定。在视图切换前, 本文方法的稳定吞吐量保持在 3 600 tx/s 左右, 相比文献[16]和文献[15]具有显著优势。虽然本文方法也会经历这种瞬时性能波动, 但其恢复速度和整体稳定性明显优于其他流水线化协议, 这得益于 ADAPT-BFT 中集成的信誉机制和共识模式切换能力, 使得系统能够更快地识别和切换到可靠的领导者节点。

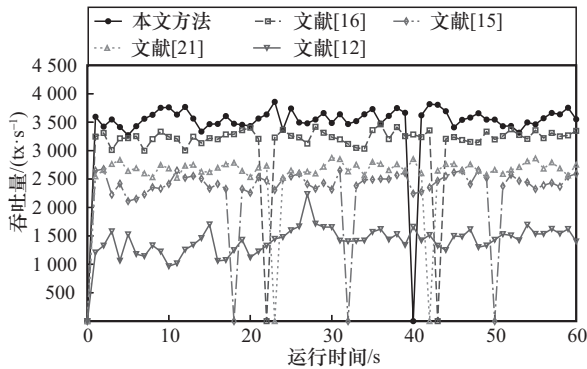


图 8 $N=30, f=9$ 下的运行时吞吐量波动监测

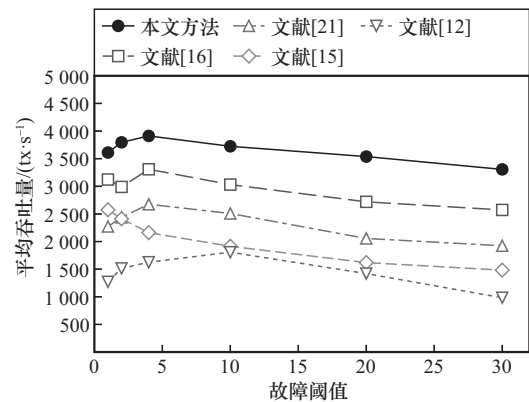
为了全面评估不同方法在不同拜占庭环境下的容错能力和性能稳定性, 本文还设计了多故障阈值下的时延和吞吐量对比实验。该实验涵盖了从轻度故障到重度故障的多个场景, 每个场景下都测量了相应的网络规模和性能指标, 以评估各方法的可扩展性和容错边界。表 2 根据不同方案的敌手模型在固定故障阈值条件下设定对应的节点数量。

表 2 固定故障阈值条件下不同方案的节点数量

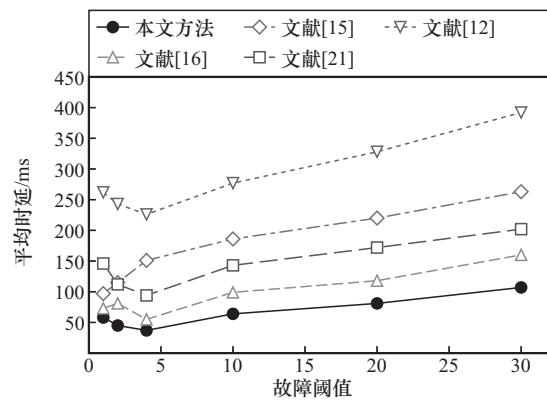
共识方法 故障阈值	本文 方法/个	文献[15] /个	文献[16] /个	文献[12] /个	文献[21] /个
1	3	3	3	4	4
2	5	5	5	7	7
4	9	9	9	13	13
10	21	21	21	31	31
20	41	41	41	61	61
30	61	61	61	91	91

从不同故障阈值下的性能表现来看, 本文方法展现出了良好的可扩展性和容错能力。

图 9(a)为故障阈值对系统平均吞吐量的影响。由图 9(a)可知, 在低故障环境下, 本文方法的平均吞吐量相比文献[16]高 15.7%, 相比文献[15]高 40.3%, 相比文献[21]高 58.9%, 相比文献[12]高 184.2%。随着故障阈值增加到 $f=4$ 时, 本文方法的吞吐量提升至峰值, 这表明本文方法在中等故障环境下具有更强的适应能力。同时, 随着故障阈值 f 的增加, 该方法的平均吞吐量下降幅度相对较小, 这体现了流水线化 BFT 类共识中 $2f+1$ 个节点要求相比传统 $3f+1$ 个节点的效率优势。更重要的是, TASK-Store 在高故障阈值环境下发挥了关键作用, 通过消除过期区块和压缩已引用区块的方式, 有效减轻了资源受限节点的存储负担, 从而在无人机网络规模扩大时仍能维持较好的性能水平。



(a) 故障阈值对系统平均吞吐量的影响



(b) 故障阈值对系统平均时延的影响

图 9 故障阈值对系统性能的影响

图 9(b)为故障阈值对系统平均时延的影响。由图 9(b)可知, 低故障环境下本文方法平均时延相比文献[16]低 20.5%, 相比文献[15]低 40.2%, 相比文

献[21]低 60.3%，相比文献[12]低 77.9%。当 $f=4$ 时，本文方法达到时延最低点，表明本文方法在中等故障环境下实现了时延与吞吐量的双重优化。对比相同敌手模型的文献[16]方法，本文方法在各故障阈值下均保持时延优势，特别是在 $f=30$ 时低 33.1%。这一差距主要体现在两个方面：一是 ADAPT-BFT 的动态模式选择相比文献[16]的固定两阶段流程具有更强的环境适应性，能够在不同故障率下选择最优执行路径；二是本文方法通过分析协同任务的紧急程度和依赖关系优化共识顺序，减少了不必要的等待时间。

4.5 组件拆分消融实验

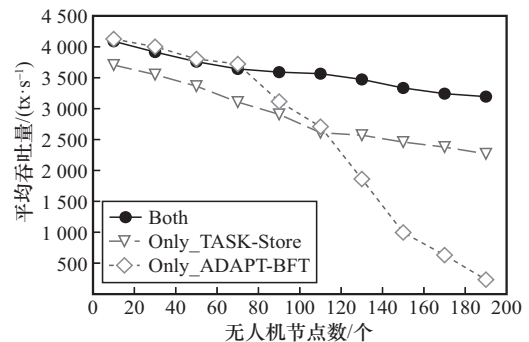
为评估本文方法中 ADAPT-BFT 和 TASK-Store 各自的贡献度，本文设计了组件拆分消融实验。实验设置 3 组对照：仅采用 ADAPT-BFT 共识优化 (Only_ADAPT-BFT)、仅采用 TASK-Store 存储优化 (Only_TASK-Store) 以及二者协同的完整方案 (Both)。

图 10(a)为不同方案在平均吞吐量方面的性能对比。在小规模网络中，Only_ADAPT-BFT 表现出与 Both 一致的性能优势。这表明在节点数量较少时，共识协议优化能够充分发挥其低通信复杂度的优势。然而，随着网络规模扩大，Only_ADAPT-BFT 的性能急剧下降，在 70~90 个节点出现明显转折，190 节点时性能保持率仅为 5.7%。相比之下，Only_TASK-Store 虽然初始吞吐量较低，但其性能衰减相对平缓，190 个节点时性能保持率达 61.2%。Both 在全规模范围内表现最为稳健，190 个节点时性能保持率高达 78.1%，相比 Only_ADAPT-BFT 提升约 12.7 倍，相比 Only_TASK-Store 提升约 27.6%。

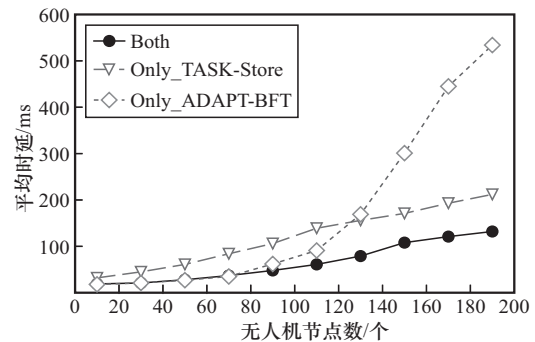
图 10(b)为不同方案在平均时延方面的性能对比。在小规模网络中，Only_ADAPT-BFT 也表现出与 Both 一致的性能优势，但随着节点增加，该方案因缺乏存储优化支持而导致时延急剧攀升，190 个节点时时延增长达 29.7 倍。Only_TASK-Store 时延增长相对线性，增长倍数为 6.6 倍，但由于缺乏共识优化，其时延始终高于 Both。Both 在大规模网络中展现出显著优势，190 个节点时相比 Only_ADAPT-BFT 时延降低 75.3%，相比 Only_TASK-Store 降低 37.7%，时延增长仅为 6.9 倍。

综合所有实验结果，TASK-Store 和 ADAPT-BFT 在无人机网络环境下展现出了良好的综合性能

表现。TASK-Store 有效解决了资源受限环境下的存储瓶颈问题，相比传统全节点存储方案平均节省了 63% 的存储开销，同时保持了数据完整性和可验证性。ADAPT-BFT 在保证安全性的前提下显著提升了共识效率，相比文献[12]平均减少了 69% 的共识时延，在大规模网络环境下优势更加明显。实验结果表明，本文方法在节点规模扩展和拜占庭故障环境下均表现出良好的鲁棒性，两者的结合为无人机区块链系统的应用提供了可行的技术方案，充分验证了本文方法的有效性和实用性。



(a) 不同方案在吞吐量方面的性能对比



(b) 不同方案在时延方面的性能对比

图 10 不同方案的拆分消融实验对比

5 结束语

本文针对无人机网络协同任务中区块链技术面临的通信复杂度高和存储资源受限等关键问题，提出了 ADAPT-BFT 和 TASK-Store 的双重优化方案。ADAPT-BFT 通过任务感知检查器和自适应累加器等可信组件，根据协同任务的紧急程度和网络状态动态选择正常、追赶、协同 3 种共识模式；TASK-Store 基于任务分解依赖关系、协同热点访问模式和时效约束生命周期 3 个维度，实现了存储资源的精细化分配和动态管理。

实验结果验证了本文方法的有效性，相比文

献[12], ADAPT-BFT在不同网络规模下平均减少69%的共识时延;相比全节点存储方案, TASK-Store平均节省63%的存储开销。在多故障阈值实验中,本文方法在 $f=30$ 的高故障场景下,吞吐量性能保持率达91.6%,时延仅为107 ms,充分验证了本文方法的容错能力和可扩展性。与现有方法相比,本文方法的创新之处在于深度融合了UANET协同任务的语义特征。在共识层面,通过任务感知的动态适配机制突破了传统拜占庭容错协议固定执行模式的局限;在存储层面,通过任务分解依赖关系分析、协同热点访问模式识别和时效约束生命周期管理三维协同优化,实现了更精准的数据生命周期管理。两者协同工作,从通信效率和存储效率两个维度全面提升了系统性能。

未来的研究工作将聚焦于以下几个方向。首先,在真实无人机飞行环境中部署测试,评估方案的鲁棒性和实用性。其次,研究轻量化可信组件的设计方案,降低对TEE硬件的依赖程度。再次,探索跨链协作机制,实现多无人机群组间的安全数据共享。最后,结合联邦学习等隐私保护技术,在保证数据隐私的前提下实现分布式模型训练和知识共享。

参考文献:

- [1] Xu X B, Zhao H, Yao H P, et al. A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT[J]. *IEEE Internet of Things Journal*, 2021, 8(4): 2431-2443.
- [2] 尹浩,魏急波,赵海涛,等.面向有人/无人协同的智能通信与组网关键技术:现状与趋势[J]. *通信学报*, 2024, 45(1): 1-17.
Yin H, Wei J B, Zhao H T, et al. Intelligent communication and networking key technologies for manned/unmanned cooperation: states-of-the-art and trends[J]. *Journal on Communications*, 2024, 45(1): 1-17.
- [3] 姜来为,陈正,杨宏宇.高动态复杂场景下航空自组网路由协议研究[J]. *西安电子科技大学学报(自然科学版)*, 2024, 51(1): 72-85.
Jiang L W, Chen Z, Yang H Y. Research on aviation ad hoc network routing protocols in highly dynamic and complex scenarios[J]. *Journal of Xidian University (Natural Science)*, 2024, 51(1): 72-85.
- [4] Alsamhi S H, Shvetsov A V, Shvetsova S V, et al. Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration[J]. *IEEE Transactions on Green Communications and Networking*, 2023, 7(1): 328-338.
- [5] Wang Y T, Su Z, Xu Q C, et al. Lifesaving with RescueChain: energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue[C]//*Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. Piscataway: IEEE Press, 2021: 1-10.
- [6] Xie H, Zheng J, He T, et al. B-UAVM: a blockchain-supported secure multi-UAV task management scheme[J]. *IEEE Internet of Things Journal*, 2023, 10(24): 21240-21253.
- [7] 白露,孙铭然,黄子蔚,等.面向应急通信的多无人机协同信道建模研究[J]. *通信学报*, 2023, 44(7): 38-50.
Bai L, Sun M R, Huang Z W, et al. Multi-UAV cooperative channel model for emergency communication[J]. *Journal on Communications*, 2023, 44(7): 38-50.
- [8] Wang Y T, Su Z, Xu Q C, et al. A secure and intelligent data sharing scheme for UAV-assisted disaster rescue[J]. *IEEE/ACM Transactions on Networking*, 2023, 31(6): 2422-2438.
- [9] Jing J F, Yang Y Z, Zhou X K, et al. Multi-UAV cooperative task offloading in blockchain-enabled MEC for consumer electronics[J]. *IEEE Transactions on Consumer Electronics*, 2025, 71(1): 2271-2284.
- [10] Bahri L, Girdzijauskas S. When trust saves energy: a reference framework for proof of trust (PoT) blockchains[C]//*Proceedings of the Companion of the The Web Conference 2018 on The Web Conference 2018 - WWW '18*. New York: ACM Press, 2018: 1165-1169.
- [11] Liu Y Q, Wang K, Lin Y, et al. LightChain: a lightweight blockchain system for industrial Internet of things[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(6): 3571-3581.
- [12] Castro M, Liskov B. Practical byzantine fault tolerance[C]//*Proceedings of the Third Symposium on Operating Systems Design and Implementation*. Berkeley: USENIX Association, 1999: 173-186.
- [13] Nahom Abishu H, Sun G L, Habtamu Yacob Y, et al. Multiagent DRL-based consensus mechanism for blockchain-based collaborative computing in UAV-assisted 6G networks[J]. *IEEE Internet of Things Journal*, 2025, 12(4): 4331-4348.
- [14] Wang J J, Wang J X, Tong Z H, et al. ACBFT: adaptive chained Byzantine fault-tolerant consensus protocol for UAV ad hoc networks[J]. *IEEE Transactions on Vehicular Technology*, 2025, 74(7): 11324-11336.
- [15] Yin M F, Malkhi D, Reiter M K, et al. HotStuff: BFT consensus with linearity and responsiveness[C]//*Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*. New York: ACM Press, 2019: 347-356.
- [16] Decouchant J, Kozhaya D, Rahli V, et al. DAMYSUS: streamlined BFT consensus leveraging trusted components[C]//*Proceedings of the Seventeenth European Conference on Computer Systems*. New York: ACM Press, 2022: 1-16.
- [17] Decouchant J, Kozhaya D, Rahli V, et al. OneShot: view-adapting streamlined BFT protocols with trusted execution environments[C]//*Proceedings of the 2024 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*. Piscataway: IEEE Press, 2024: 1022-1033.
- [18] Hu W J, Yu Y, Zong Y, et al. Cost-effective multi-type data scheduling for blockchain in massive Internet of UAVs[J]. *IEEE Internet of*

Things Journal, 2024, 11(12): 21092-21102.

- [19] Van D H L, Choo K R, Le-Khac N A. Process memory investigation of the Bitcoin clients electrum and Bitcoin core[J]. IEEE Access, 2017, 5: 22385-22398.
- [20] Xu M H, Guo H C, Cheng Y, et al. EC-chain: cost-effective storage solution for permissionless blockchains[C]//Proceedings of the IEEE INFOCOM 2025 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2025: 1-10.
- [21] Wang Z J, Xiong R Q, Jin J H, et al. AirBC: a lightweight reputation-based blockchain scheme for resource-constrained UANET[C]//Proceedings of the 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE Press, 2022: 1378-1383.

[作者简介]



姜来为 (1986-), 女, 黑龙江哈尔滨人, 博士, 中国民航大学讲师、硕士生导师, 主要研究方向为空天地一体化网络、无线自组网和网络资源优化、网络空间安全等。



廖江亨 (2000-), 男, 江西赣州人, 中国民航大学硕士生, 主要研究方向为无人机网络、区块链技术等。



刘鑫 (1984-), 男, 黑龙江哈尔滨人, 博士, 大连理工大学副教授、博士生导师, 主要研究方向为空天地一体化网络、无人机通信、无线资源优化。



那振宇 (1981-), 男, 黑龙江哈尔滨人, 博士, 大连海事大学教授、博士生导师, 主要研究方向为空天地一体化网络、无人机通信、卫星通信、无线自组网和网络资源优化等。