基于联盟链与门限签名的低空智联网跨域服务功能链接入机制

吴 遥,贾子晔,朱秋明,周福辉
(南京航空航天大学电子信息工程学院电磁频谱空间认知动态系统工信部重点实验室,江苏南京 211106)

摘 要: 随着低空智联网(Low-Altitude Intelligent Network,LAIN)在空天地一体化网络中的广泛应用,服务功能链(Service Function Chain,SFC)技术通过将虚拟化网络功能按需编排与串联,成为实现跨管理域资源协同与业务按需构建的关键支撑。然而,低空智联网具有的高动态拓扑导致认证会话频繁中断,管理域的异构性使得跨域身份映射与信任传递异常复杂,开放无线信道加剧了认证信息被窃取与篡改的风险。这些独特挑战使得基于固定基础设施或集中式管理的传统认证机制难以适应跨域SFC场景对安全性、实时性与可靠性的严苛需求。传统中心化方案存在单点故障与性能瓶颈,而去中心化方案又常面临效率低下、可扩展性不足等难题。针对上述问题,本文提出了一种基于联盟区块链与灵活门限签名(Flexible Threshold Signature Scheme,FlexiTSS)的跨域SFC安全接入与认证机制。该机制首先构建一个由多管理域边缘节点共同维护的联盟链,作为分布式的全局信任锚,实现身份与策略的统一存证与验证。然后,设计了一种支持动态成员管理的FlexiTSS算法,使得多个管理域可联合完成对关键操作的签名授权,显著提升签名效率。此外,本文提出了一种轻量级动态编排器选举算法,依据网络实时拓扑与业务负载自适应选择最优编排节点,有效实现了负载均衡,避免了单点失效。实验结果表明,与典型的中心化认证、基础区块链认证等方案相比,本文提出的方案在跨域认证时延、高动态环境下的任务成功率和控制面通信开销等方面均具有显著优势,能够在大规模节点与长服务链场景下保持稳定的性能,较好地解决了安全、效率与可扩展性之间的权衡问题,为低空智联网的跨域安全协同提供了切实可行的技术途径。

关键词: 低空智联网;服务功能链;跨域认证;联盟区块链;门限签名

基金项目: 国家自然科学基金(No.62231015,No.62301251);江苏省研究生科研与实践创新计划项目(No.SJCX25_0152)

中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112(XXXX)XX-0001-13

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20251175

A Cross-Domain Service Function Chain Access Mechanism Based on Consortium Blockchain and Threshold Signature in LAIN

WU Yao, JIA Ziye, ZHU Qiuming, ZHOU Fuhui
(*School of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Key Laboratory of Dynamic Cognitive System of Electromagnetic Spectrum Space, Ministry of Industry and Information Technology, Nanjing, Jiangsu* 211106, *China*)

Abstract: With the widespread application of the Low-Altitude Intelligent Network (LAIN) in the integrated space-air-ground network, Service Function Chain (SFC) technology has emerged as a key enabler for cross-domain resource coordination and on-demand service construction by orchestrating and chaining virtualized network functions as needed. However, the highly dynamic topology of LAIN leads to frequent interruptions of authentication sessions, while the heterogeneity of management domains complicates cross-domain identity mapping and trust propagation. Moreover, the open wireless channel heightens the risk of authentication information being stolen or tampered with. These unique challenges render traditional authentication mechanisms based on fixed infrastructure or centralized management inadequate to meet the stringent security, real-time, and reliability requirements of cross-domain SFC scenarios. Centralized solutions suffer from single points of failure and performance bottlenecks, whereas decentralized approaches often face inefficiency and scalability issues. To address these problems, this paper proposes a cross-domain SFC secure access and authentication mechanism based on consortium blockchain and a Flexible Threshold Signature Scheme (FlexiTSS). The mechanism first constructs a consortium blockchain maintained by edge nodes across multiple management domains, serving as a distributed global trust anchor to achieve unified storage and verification of identities and policies. Furthermore, a FlexiTSS algorithm supporting dynamic member management is designed, enabling multiple management domains to jointly authorize critical operations

收稿日期:2026-01-12;录用日期:2026-01-26;责任编辑:宋甲英

through signature, thereby significantly improving signature efficiency. Additionally, a lightweight dynamic orchestrator election algorithm is proposed, which adaptively selects the optimal orchestration node based on real-time network topology and service load, effectively achieving load balancing and avoiding single points of failure. Experimental results demonstrate that, compared to typical centralized authentication and basic blockchain authentication schemes, the proposed scheme exhibits significant advantages in cross-domain authentication latency, task success rate in highly dynamic environments, and control plane communication overhead. It maintains stable performance in large-scale node and long service chain scenarios, effectively resolving the trade-off between security, efficiency, and scalability, thereby providing a practical technical approach for cross-domain secure collaboration in LAIN.

Keywords: low-altitude intelligent network; service function chain; cross-domain authentication; consortium blockchain; threshold signature

Foundation Item(s): National Natural Science Foundation of China (No.62231015,No.62301251); Postgraduate Research & Practice Innovation Program of Jiangsu Province (No.SJCX25_0152)

0 引言

随着新一代通信技术与边缘计算的深度耦合,低空智联网正经历从孤立的传感节点向自主协同的空中计算平台演进[1]。在空天地一体化网络、战场态势感知及智慧城市治理等复杂场景下,服务功能链(Service Function Chain,SFC)技术作为网络功能虚拟化的核心载体,能够将分布在低空智联网中异构无人机节点上的虚拟网络功能按需编排,实现跨域资源的弹性整合与业务逻辑的高效构建[2-3]。然而,低空智联网天然具有的拓扑高动态性、通信信道开放性以及管理域异构性,使得SFC在跨域部署与执行过程中面临严峻的安全挑战[4-5]。

首先,多域并存所导致的信任边界异构性是跨域协作的首要障碍[6]。低空智联网往往由隶属于不同管理域的实体构成,缺乏统一的信任根,传统的边界防护模型难以应对跨域数据流转中的身份伪造与越权访问[7]。其次,高动态拓扑与弱连接环境加剧了认证机制的失效风险[8]。无人机节点的高速移动引发网络拓扑频繁剧变,基于静态证书链或中心化服务器的传统认证方案在链路拥塞或断裂时,极易因单点性能瓶颈导致服务器瘫痪[9]。最后,资源受限与实时性需求的矛盾难以调和。无人机节点受限于尺寸、重量与功耗,难以承载复杂的重型密码协议,而SFC业务通常对时延极其敏感,如何在有效时间窗口内完成高强度的跨域身份核验与密钥协商,是当前亟待突破的关键问题[10]。解决上述安全问题和效率问题的核心在于为动态、异构的无人机节点构建一个高效、可靠的跨域信任锚点[11-12]。然而,现有技术路径均存在局限:中心化认证方案虽效率较高,但存在单点故障和信任瓶颈隐患,难以适配多域并存的场景[13];而基于公有链的去中心化方案虽能实现分布式信任,却受制于共识效率与存储开销,难以满足高实时性与资源受限的边缘网络需求[14-15]。因此,探索一种融合联盟区块链治理优势与分布式密码学灵活特性的新型架构,打破安全性、高效性与可扩展性的三难困境,具有重要的理论意义与应用价值。本文针对低空智联网环境,提出了一种基于联盟区块链与门限签名的跨域SFC安全接入机制。本文的主要贡献包括如下三点。

(1)构建多域联合治理架构。利用联盟链维护全局信任视图,结合门限签名实现跨域身份的分布式管理与策略联合授权,消除单点故障并提供拜占庭容错能力。

(2)设计原子化预验证协议。提出基于区块链状态的批量预验证机制,签发包含时空约束的安全授权凭证,有效降低跨域切换认证开销。

(3)提出动态编排器选举算法。基于加权拓扑中心度与路径覆盖度实现SFC编排节点的自适应迁移,解决静态编排导致的负载失衡问题。

1 相关工作

低空智联网跨域SFC的安全接入是一个涵盖网络安全、分布式系统与密码学的交叉课题[16]。既往研究在身份认证、区块链信任管理及安全编排等方面已取得一定进展,但针对多域、高动态及长链路特性的综合解决方案仍较为缺乏[17]。

在身份认证与访问控制领域,早期研究主要沿用互联网公钥基础设施体系[18]。尽管通过精简证书字段可在一定程度上降低传输开销,但在高动态的低空智联网中,证书撤销列表的分发与在线状态查询引发的信令风暴不仅消耗宝贵的带宽资源,而且严重依赖在线证书颁发机构的可用性。为摆脱证书管理负担,基于身份的密码体制和无证书公钥密码体制被广泛引入,研究者通常利用设备标识生成公钥[19]。然而,此类方案普遍存在密钥托管隐患,一旦密钥生成中心被攻破或发动内部攻击,全网安全体系将面临崩溃。此外,现有的访问控制模型,如基于角色的访问控制与基于属性的访问控制等,多针对点对点通信设计,

缺乏对SFC链式结构的全局感知能力,导致数据包在经过每一跳服务节点时均需执行全量认证,这种重复开销严重推高了端到端的时延[20]。

为解决多域互信难题,区块链技术凭借其去中心化与不可篡改的特性成为研究热点。现有工作多利用联盟链构建无人机注册与飞行日志的分布式账本[21]。虽然区块链有效打破了信任孤岛,但在直接将其应用于对实时性要求极高的SFC网络时,会面临显著的性能与效率失衡问题。主流共识算法的确认延迟通常在秒级以上,无法满足SFC毫秒级的节点切换需求[22]。同时,要求资源受限的无人机维护完整账本或频繁进行链上交互,会带来不可承受的存储与计算负担[23]。现有研究往往侧重于利用区块链记录事后审计日志,而未能有效解决如何利用区块链实现实时的快速接入控制。

为了弥补中心化认证的脆弱性并提升效率,分布式密码学技术,特别是门限签名方案(Threshold Signature Scheme,TSS)逐渐受到关注。该技术允许多个参与者共同管理密钥,仅当集齐预设数量以上签名份额时方可生效,天然契合分布式网络的容错需求[24]。部分工作尝试将门限机制应用于移动自组网的密钥管理,或结合安全多方计算验证服务链的完整性[25]。然而,现有分布式方案在适配无人机特性方面仍有局限:一方面,大多数门限方案基于静态群组假设,缺乏支持节点频繁进出的动态成员变更机制,导致网络抖动时的重新密钥生成开销巨大;另一方面,现有安全编排算法多聚焦于虚拟网络功能(Virtual Network Function,VNF)的放置位置优化,忽视了安全认证与业务编排的深度耦合,导致安全机制往往是“外挂式”而非“内生式”的,难以有效防御针对服务链路径的劫持与篡改攻击[26-27]。

综上所述,现有方案难以同时满足低空智联网跨域SFC对高鲁棒性、低时延及动态适应性的多重需求。因此,急需一种融合联盟区块链治理优势与分布式密码学灵活特性的新型安全架构,以突破安全性、高效性与可扩展性之间的三难困境。

2　问题描述与系统建模

2.1　场景与问题描述

在跨域协同的低空智联网中,复杂任务需通过SFC的形式下发,即将若干VNF按顺序部署到不同无人机上,使得任务数据能够沿预定路径依次处理。由于通信依赖开放无线信道、网络拓扑高度动态且涉及多个自治管理域,SFC在跨域执行过程中易受到身份伪造、中间人攻击、重放攻击、跨域信任滥用等威胁[28-29]。传统方案通常依赖单一认证服务器或中心化控制平面进行身份认证与授权,难以在恶劣链路条件下同时保证安全性、低时延和高可用性。此外,静态的一次性认证与粗粒度授权,很难约束无人机在任务执行过程中的动态行为。因此,本文设计了一种结合区块链与分布式密码技术的跨域SFC安全认证框架,实现去中心化身份管理、多域联合授权以及细粒度的时空约束。

如图1所示,该系统由可信机构(Trusted Authority,TA)、联盟区块链(Consortium Blockchain,CB)、多个配备边缘服务器的管理域和大规模无人机实体构成。

(1)TA作为离线根信任源,负责生成全局密码参数与根密钥,并为各管理域签发域证书。系统采用基于secp256k1曲线的椭圆曲线群$\mathbb{G}$,生成元为g,群阶为素数p。TA设置哈希到曲线函数$H_{\text{map}}:\{0,1\}^*\to\mathbb{G}$与哈希函数$H:\{0,1\}^*\to\mathbb{Z}_p$,生成根密钥对$(\text{sk}_{\text{TA}},\text{pk}_{\text{TA}})$并构造根证书$\text{Cert}_{\text{TA}}$,随后通过智能合约将$\{\mathbb{G},g,p,H_{\text{map}},H,\text{Cert}_{\text{TA}}\}$发布到联盟区块链中。

(2)BC由各管理域的边缘服务器共同组成,只允许持有有效域证书的节点作为共识节点加入。BC用于存储域证书、无人机注册信息、SFC授权策略以及审计日志,依托共识机制保证数据的不可篡改与高可靠性。智能合约封装了参数发布、域注册、无人机注册与状态更新、授权绑定与撤销以及审计记录写入等操作,为跨域信任提供统一的状态视图。

(3)系统划分为多个自治管理域N_i。每个域内部署一台边缘服务器ES_i,负责本域无人机的注册与管理,并作为BC的共识节点参与区块生成与链上验证。边缘服务器ES_i为本域生成域级密钥对$(\text{sk}_{N_i},\text{pk}_{N_i})$,并向TA申请域证书$\text{Cert}_{N_i}$。获得证书后,$\text{ES}_i$将在证书链上注册,以便其他域通过BC验证其身份与公钥。

(4)无人机D_i是SFC的实际执行节点,具备全局唯一的设备标识u_i,并为自己生成长期公私钥对$(\text{sk}_{\text{D}_i},\text{pk}_{\text{D}_i})$,其中私钥存储在硬件安全模块中。无人机搭载轻量级VNF模块,可依据SFC编排执行数据过滤、加解密和转发等操作。无人机通过所属边缘服务器接入BC,在链上完成注册、状态更新和授权策略写入。

2.2　初始化与区块链配置

系统初始化阶段由TA主导。TA首先设定全局密码参数$(\mathbb{G},g,p,H_{\text{map}},H)$,生成根密钥对$(\text{sk}_{\text{TA}},\text{pk}_{\text{TA}})$与自签名根证书$\text{Cert}_{\text{TA}}$,并通过智能合约写入BC。此后,任何节点均可通过验证Cert_{TA}获得系统根公钥。

域初始化阶段由各边缘服务器执行。边缘服务器ES_i生成域私钥$\text{sk}_{N_i}\in_R[1,p-1]$(其中,$R$表示均匀随机

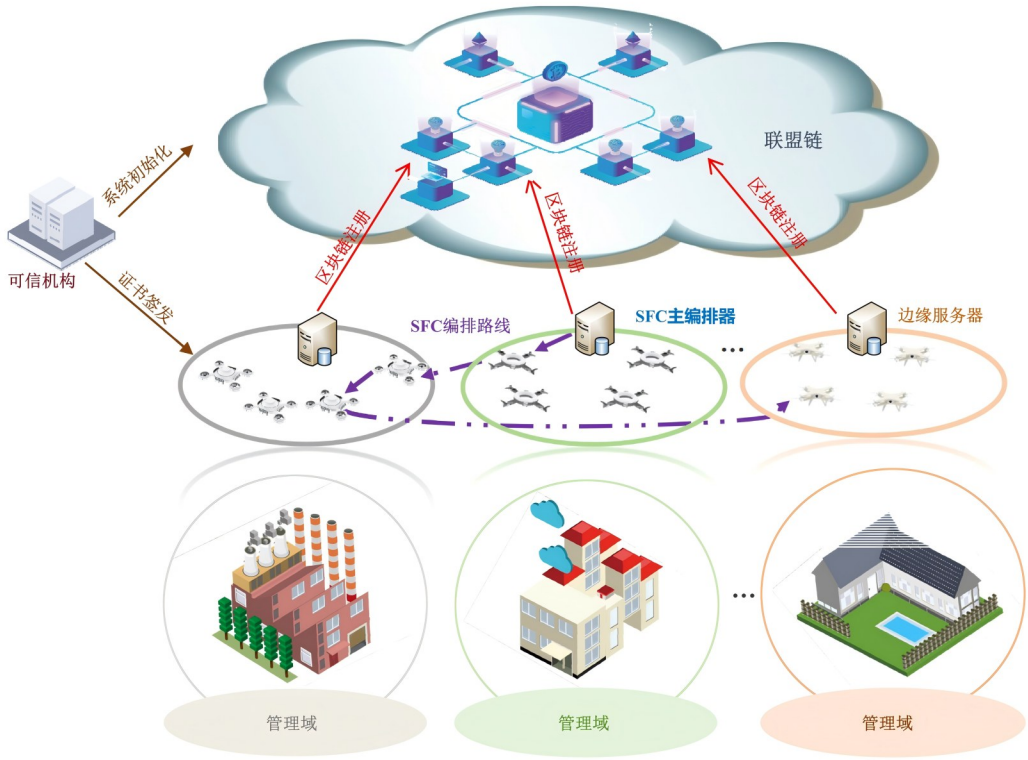

图1 低空智联网SFC安全框架系统模型图

Figure 1 System model of SFC security framework for low-altitude intelligent network

选取),并计算域公钥$\mathrm{pk}_{N_i}=g^{\mathrm{sk}_{N_i}}$,将$(\mathrm{pk}_{N_i},N_i)$及metadata提交TA。其中,metadata为描述证书属性的元数据,包括颁发者标识、有效期等信息。TA使用$\mathrm{sk}_{\mathrm{TA}}$对$H(\mathrm{pk}_{N_i}\|N_i\|\mathrm{metadata})$签名,生成域证书$\mathrm{Cert}_{N_i}$,由$\mathrm{ES}_i$通过交易写入BC,其中‖表示连接操作。至此,每个域都具备可公开验证的身份与公钥,为后续跨域认证与授权提供基础。

2.3 信任与威胁模型

为构建严密的安全分析基准,本文首先确立信任边界的核心要素。信任模型以完全可信的信任锚TA为根基,负责系统初始化参数的生成与根密钥的分发;联盟区块链网络的正确运行则依托于共识协议的鲁棒性,即在诚实共识节点占多数的前提下,分布式账本能够维持数据的一致性与不可篡改性。此外,边缘服务器与无人机节点的安全基础锚定于其搭载的安全硬件(如可信执行环境或安全元件)。系统认定这些硬件模块具备抗物理攻击能力,能够为长期私钥提供隔离保护,从而构成不可逾越的硬件信任根,防止密钥在软件层面被提取或泄露。

基于上述信任模型,本文定义了一个具备多项式时间计算能力的强敌手,它虽然无法攻破密码学原语或硬件防护,但具备全方位的内外部攻击能力。在网络层面,敌手不仅能够对无线信道实施被动监听以进行流量模式分析,还具备发起主动中间人攻击的能力,旨在对通信消息进行截获、篡改或重放。在节点层面,敌手可能渗透部分边缘节点,利用获取的合法凭证发起内部攻击,通过伪造SFC请求来实现越权访问与横向移动。针对系统可用性,模型考量了针对静态编排器或认证节点的拒绝服务攻击风险,此类攻击意在人为触发单点故障。尤为关键的是,在跨域协作场景下,该模型将恶意管理域纳入威胁范畴,此类敌手可能在本地伪造用户注册身份,并向区块链网络注入虚假的访问策略与交易记录,企图破坏跨域信任链的完整性。

3 算法设计

本章首先介绍基于区块链驱动的无人机身份管理算法,然后详细说明本文所提出的灵活阈值签名算法(Flexible Threshold Signature Scheme, FlexiTSS),继而给出跨域SFC安全认证协议的具体流程,最后描述轻量级动态编排器选举算法。这四部分共同构成从密钥材料分发、身份注册、策略授权、任务执行到审计闭环的完整技术链路。

3.1 区块链驱动的身份管理

3.1.1 域注册与证书发布

每个管理域N_i由边缘服务器ES_i负责注册,其步骤如下。

(1)密钥生成。ES_i随机选择域私钥$sk_{N_i} \in_R [1, p-1]$,并计算域公钥$pk_{N_i} = g^{sk_{N_i}}$。

(2)证书申请。ES_i将(pk_{N_i}, N_i)及元数据metadata提交TA。元数据可包含证书有效期、用途限制与算法标识等信息。

(3)证书签发。TA使用根私钥sk_{TA}对消息$H(pk_{N_i} \| N_i \| \text{metadata})$签名,得到

$$\sigma_{N_i} = \text{Sign}_{sk_{TA}}(H(pk_{N_i} \| N_i \| \text{metadata})) \tag{1}$$

其中,数字签名算法Sign(·)及其配套的验证算法Verify(·)采用基于椭圆曲线secp256k1的椭圆曲线数字签名算法。该算法通过椭圆曲线离散对数问题保障签名的不可伪造性。域证书表示为

$$\text{Cert}_{N_i} = (pk_{N_i}, N_i, \text{metadata}, \sigma_{N_i}) \tag{2}$$

(4)链上注册。ES_i通过智能合约提交包含Cert_{N_i}的域注册交易,交易确认后,域证书持久存储在BC中,其他节点可通过验证Cert_{TA}与σ_{N_i}确认N_i的合法性。

3.1.2　无人机注册与凭证发放

假设无人机D_i隶属于域N_A,其注册过程如下。

(1)本地检查与注册请求生成。无人机首先检查本地是否已有未过期的注册凭证。如无,则以设备标识u_i为输入计算身份哈希$h_i = H(u_i)$,生成时间戳t_i,并构造注册请求消息:

$$\text{REG\_request}_i = (h_i, t_i) \tag{3}$$

随后,使用域公钥pk_{N_A}加密该消息:

$$\text{register}_i = \text{Enc}_{pk_{N_A}}(\text{REG\_request}_i) \tag{4}$$

并将register_i发送给ES_A,加密函数Enc(·)采用椭圆曲线集成加密方案。该方案是一种混合加密机制,结合了椭圆曲线密码的高效性和对称加密的速度,可提供选择明文攻击下的语义安全性。

(2)解密与账户分配。ES_A使用域私钥sk_{N_A}解密register_i得到(h_i, t_i),检查t_i的新鲜性,并在BC中查询h_i的注册状态。如为新设备或既有凭证已失效,ES_A为D_i分配新的区块链账户地址Addr_i。

(3)注册凭证构造。为生成防伪注册凭证,ES_A随机选择掩码值$\alpha_i \in \mathbb{Z}_p^*$,计算

$$s_i = \alpha_i + h_i \bmod p \tag{5}$$

再使用域私钥生成签名

$$\sigma_i = \text{Sign}_{sk_{N_A}}(H(\text{Addr}_i \| s_i \| t_i)) \tag{6}$$

设凭证失效时间为T_i,注册凭证表示为

$$C_i = <pk_{N_A}, \text{Addr}_i, s_i, \sigma_i, t_i, T_i> \tag{7}$$

(4)链上存证与返回。ES_A构造注册交易$\text{Tx}_{\text{REG}}(h_i, \text{Addr}_i, C_i)$提交至BC。交易确认后,无人机注册状态与凭证被持久存储。随后,ES_A将C_i返回给D_i,可根据需要使用pk_{D_i}加密返回内容。

(5)凭证验证与使用。无人机在本地存储C_i,后续任意验证者可通过查询BC获取Cert_{N_A},利用其中的pk_{N_A}和签名σ_i验证D_i的注册状态与凭证的完整性。

在运行过程中,边缘服务器和编排器通过智能合约接口获取和更新身份状态。例如,编排器在SFC预验证阶段按Addr_i或h_i检索无人机的注册记录与授权SFC列表。各域在吊销或恢复无人机时,通过提交状态更新交易修改链上状态。对访问控制表更新等关键交易,系统要求附加门限签名,以保证跨域策略的一致性。

3.2　FlexiTSS阈值多重签名算法

参与FlexiTSS的边缘服务器集合记为$\mathcal{R} = \{ES_1, ES_2, \ldots, ES_n\}$,门限参数为$t$,满足$1 \leqslant t \leqslant n$。系统维护恶意节点集合$\mathcal{M}$,初始为空,用于记录在协议中被识别为异常的节点。各节点通过分布式密钥生成(Distributed Key Generation,DKG)获得联合私钥sk和公钥$pk = g^{sk}$,并分别持有私钥份额sk_i与公钥份额$pk_i = g^{sk_i}$。协调者由边缘服务器选举产生,负责组织密钥生成、预签名与在线签名流程。

3.2.1　分布式密钥生成

FlexiTSS采用可验证秘密分享生成联合密钥。每个节点ES_i随机选择次数为$t-1$的多项式

$$f_i(x) = \sum_{k=0}^{t-1} a_{ik} x^k \bmod p \tag{8}$$

其中,$a_{ik} \in \mathbb{Z}_p$。节点计算承诺向量

$$\boldsymbol{V}_i = (C_{i0}, C_{i1}, \ldots, C_{i(t-1)}) = (g^{a_{i0}}, g^{a_{i1}}, \ldots, g^{a_{i(t-1)}}) \tag{9}$$

并广播$\boldsymbol{V}_i$。随后,ES_i向每个ES_j通过私有信道发送份额:

$$s_{ij} = f_i(j) \bmod p \tag{10}$$

节点ES_j接收后,验证$g^{s_{ij}} \stackrel{?}{=} \prod_{k=0}^{t-1} C_{ik}^{j^k}$,符号$\stackrel{?}{=}$表示是否等于,以确保份额与承诺一致。所有份额验证通过后,定义全局多项式

$$f(x) = \sum_{i=1}^{n} f_i(x) \bmod p \tag{11}$$

联合私钥为

$$sk = f(0) = \sum_{i=1}^{n} a_{i0} \bmod p \tag{12}$$

联合公钥为$pk = g^{sk}$。每个节点ES_j计算本地私钥份额

$$sk_j = f(j) = \sum_{i=1}^{n} s_{ij} \bmod p \tag{13}$$

并得到对应的公钥份额$pk_j = g^{sk_j}$。各节点在DKG完

成后公开 pk_j，并保留 sk_j 及自身多项式系数 $\{a_{jk}\}$，以支持后续签名和新节点的加入。

3.2.2 离线预签名生成

为降低在线签名时延，FlexiTSS将部分计算预先执行。每个节点 ES_i 周期性随机选择 $(d_i, e_i) \in_R \mathbb{Z}_p^2$，计算承诺

$$A_i = g^{d_i}, \quad B_i = g^{e_i} \tag{14}$$

形成预签名承诺对 $\rho_i = (A_i, B_i)$，通过安全信道发送给协调者。协调者缓存各节点的预签名承诺，并在预签名资源即将耗尽时通知相关节点补充。

3.2.3 在线签名与验证

在线签名包括会话发起、局部签名份额生成与聚合三个步骤。

在会话发起阶段，协调者从集合 $\mathcal{R}\backslash\mathcal{M}$ 中选取子集 $\mathcal{S}$，满足 $|\mathcal{S}| \geqslant t$，为每个 $\mathrm{ES}_i \in \mathcal{S}$ 指定一对预签名承诺 (A_i, B_i)。协调者计算组承诺

$$A = \prod_{i \in \mathcal{S}} A_i, \quad B = \prod_{i \in \mathcal{S}} B_i \tag{15}$$

并基于联合公钥 pk、参与集合 $\mathcal{S}$、组承诺与待签消息 m 计算会话绑定因子

$$b = \mathcal{H}_0(\mathrm{pk}, \mathcal{S}, A, B, m) \tag{16}$$

随后，将 $(\mathcal{S}, A, B, m)$ 广播给 $\mathcal{S}$ 中的所有节点。

在局部份额生成阶段，每个 $\mathrm{ES}_i \in \mathcal{S}$ 计算临时公钥 $R_{\mathcal{S}} = A \cdot B^b$，并基于消息与 $R_{\mathcal{S}}$ 计算挑战值

$$c = \mathcal{H}_1(m, R_{\mathcal{S}}, \mathrm{pk}) \tag{17}$$

根据集合 $\mathcal{S}$ 中的节点编号，节点计算自身的拉格朗日系数

$$\lambda_i = \prod_{j \in \mathcal{S}, j \neq i} \frac{j}{j - i} \bmod p \tag{18}$$

然后，利用私钥份额 sk_i 计算签名份额

$$\sigma_i = d_i + e_i \cdot b + \lambda_i \cdot \mathrm{sk}_i \cdot c \bmod p \tag{19}$$

出于前向安全考虑，节点同时生成新的预签名对 $(d_{i'}, e_{i'})$ 及承诺 $(A_{i'}, B_{i'})$，并将 $<i, \sigma_i, (A_{i'}, B_{i'})>$ 返回给协调者。

在份额验证与聚合阶段，协调者对每个响应节点验证

$$g^{\sigma_i} \stackrel{?}{=} A_i \cdot B_i^b \cdot \mathrm{pk}_i^{c \cdot \lambda_i} \tag{20}$$

若验证失败，则将该节点加入 $\mathcal{M}$，并在新的参与集合上重新发起签名会话。对至少 t 个验证通过的份额，协调者计算聚合标量

$$z = \sum_{i \in \mathcal{S}} \sigma_i \bmod p \tag{21}$$

得到联合签名 $\sigma = (R_{\mathcal{S}}, z)$，同时，协调者更新成功节点的预签名池，将 $(A_{i'}, B_{i'})$ 纳入备用资源。任意验证者在获得 (m, σ, pk) 后，首先计算 $c = \mathcal{H}_1(m, R_{\mathcal{S}}, \mathrm{pk})$，再检查

$$g^z \stackrel{?}{=} R_{\mathcal{S}} \cdot \mathrm{pk}^c \tag{22}$$

若等式成立，则确认该签名由不少于 t 个合法节点联合生成。系统对访问控制表更新、新域加入与审计策略调整等交易要求附加 FlexiTSS 联合签名，以实现多域联合决策。

3.2.4 动态节点管理

为适应联盟规模与拓扑变化，FlexiTSS 支持新节点加入与旧节点移除。为支持新节点加入，假设现有节点在 DKG 完成后保留自身多项式 $f_i(x)$ 的系数，或等效的份额生成状态。当新边缘服务器 $\mathrm{ES}_{\mathrm{new}}$ 获得 TA 签发的域证书后，现有节点 ES_i 为其计算份额

$$s_{i,\mathrm{new}} = f_i(\mathrm{ID}_{\mathrm{new}}) \bmod p \tag{23}$$

通过安全信道发送给 $\mathrm{ES}_{\mathrm{new}}$。新节点聚合得到私钥份额

$$\mathrm{sk}_{\mathrm{new}} = \sum_{i=1}^{n} s_{i,\mathrm{new}} \bmod p \tag{24}$$

并计算公钥份额 $\mathrm{pk}_{\mathrm{new}} = g^{\mathrm{sk}_{\mathrm{new}}}$，随后生成预签名承诺提交协调者，加入集合 $\mathcal{R}$。当某节点 ES_k 因故障或恶意行为需被移除时，系统将其从 $\mathcal{R}$ 中删除，该节点本地擦除 sk_k 与预签名因子，协调者删除其预签名承诺。如该节点参与了正在进行的签名会话，协调者会终止该会话，并在新的参与集合上重新发起，以保证签名服务的连续性。

3.3 跨域SFC安全认证协议

本节在前述身份管理与门限签名机制基础上，给出跨域SFC安全认证协议的完整流程，包括任务预验证、首节点启动、逐跳会话密钥协商与交接凭证，以及任务完成后的链上审计。协议中的关键实体包括编排器 Orch、各域边缘服务器 ES_i、无人机 D_i，以及联盟区块链 BC。编排器由边缘服务器通过选举算法选出，负责 SFC 路径编排、批量预验证与安全认证凭证（Secure Authorization Credential，SAC）签发。边缘服务器维护本域无人机凭证与公钥，并提供链上查询服务。无人机持有长期密钥对 $(\mathrm{sk}_{\mathrm{D}_i}, \mathrm{pk}_{\mathrm{D}_i})$，执行 VNF 功能并参与会话密钥协商。BC 记录所有注册信息、授权策略与审计摘要。

3.3.1 SFC预验证与SAC签发

当发起 SFC 请求时，编排器 Orch 根据拓扑与策略计算路径

$$\mathrm{Path} = [\mathrm{D}_1@N_{a_1} \rightarrow \mathrm{D}_2@N_{a_2} \rightarrow \cdots \rightarrow \mathrm{D}_L@N_{a_L}] \tag{25}$$

并分配任务标识 SFC_ID。其中，符号@用于表示隶属关系，具体而言，$\mathrm{D}_1@N_{a_1}$ 表示无人机 D_1 隶属于管理域节点 N_{a_1} 或由其管控，该符号表明无人机与其所属管理域的对应关系。随后，Orch 调用智能合约对

路径中所有无人机执行一次预验证:对每个D_ℓ查询其注册地址和状态,确认其为激活;检查链上授权策略,验证(Drone_ID$_\ell$,SFC_ID)绑定存在且未过期;确认其所属域N_{a_ℓ}的域证书是否有效。若任一节点未通过验证,则Orch拒绝该SFC请求或重新选路。否则,Orch构造安全授权凭证

$$\mathrm{SAC}=\{\mathrm{SFC\_ID},T_{\mathrm{start}},T_{\mathrm{expire}},\mathrm{Nonce}_{\mathrm{SAC}},\mathrm{Enc\_Path},\mathrm{Sig}_{\mathrm{SAC}}\} \tag{26}$$

其中,$[T_{\mathrm{start}},T_{\mathrm{expire}}]$为任务允许执行时间窗,$\mathrm{Nonce}_{\mathrm{SAC}}$为随机数标识任务实例,$\mathrm{Enc_Path}=\mathrm{Enc}_{\mathrm{pk}_{\mathrm{D}_1}}(\mathrm{Path})$使用首节点公钥加密完整路径,$\mathrm{Sig}_{\mathrm{SAC}}=\mathrm{Sign}_{\mathrm{sk}_{\mathrm{Orch}}}(\mathrm{SAC_body})$为编排器对凭证主体的签名。Orch通过开放信道将SAC发送给首节点所在域的边缘服务器或直接发送给D_1。

3.3.2　首节点验证与启动

首节点D_1接收SAC后,首先从BC查询编排器公钥或证书,利用$\mathrm{Verify}_{\mathrm{pk}_{\mathrm{Orch}}}$验证$\mathrm{Sig}_{\mathrm{SAC}}$,确保SAC未被篡改或伪造。随后,$D_1$使用私钥$\mathrm{sk}_{\mathrm{D}_1}$解密Enc_Path获得明文路径Path,确认路径首元素为$D_1@N_{a_1}$。在时效性检查中,D_1读取当前时间Current_Time,验证

$$T_{\mathrm{start}}\leqslant\mathrm{Current\_Time}<T_{\mathrm{expire}} \tag{27}$$

并利用本地缓存检查$\mathrm{Nonce}_{\mathrm{SAC}}$是否为新随机数,防止旧SAC被重放。一旦通过这些检查,D_1就会启动本地VNF功能,对输入数据进行处理,并为下一跳D_2的安全交接做准备。

3.3.3　逐跳密钥协商与交接凭证

在从D_i向D_j转移数据与执行权前,两节点需完成会话密钥协商并构造交接凭证。

会话密钥协商过程如下。首先,D_i与D_j均通过BC验证对方公钥与注册状态。D_i随机选择$r_i\in_R\mathbb{Z}_p^*$,生成时间戳t_i与随机数nonce_i,构造$m_i=(r_i\|\,t_i\|\,\mathrm{nonce}_i)$,并计算

$$c_i=\mathrm{Enc}_{\mathrm{pk}_{\mathrm{D}_j}}(m_i),\quad \sigma_i=\mathrm{Sign}_{\mathrm{sk}_{\mathrm{D}_i}}(c_i\|\,t_i\|\,\mathrm{nonce}_i) \tag{28}$$

D_i将(c_i,σ_i)发送给D_j。D_j使用$\mathrm{sk}_{\mathrm{D}_j}$解密$c_i$得到$(r_i,t_i,\mathrm{nonce}_i)$,检查$t_i$新鲜性并验证$\sigma_i$。随后,$D_j$对称地选择$r_j\in_R\mathbb{Z}_p^*$,生成$t_j$与$\mathrm{nonce}_j$,构造$m_j=(r_j\|\,t_j\|\,\mathrm{nonce}_j)$,并得到

$$c_j=\mathrm{Enc}_{\mathrm{pk}_{\mathrm{D}_i}}(m_j),\quad \sigma_j=\mathrm{Sign}_{\mathrm{sk}_{\mathrm{D}_j}}(c_j\|\,t_j\|\,\mathrm{nonce}_j) \tag{29}$$

发送(c_j,σ_j)给D_i。D_i解密并验证后,双方调用会话密钥派生函数$\mathrm{KDF}:\{0,1\}^*\to\{0,1\}^\kappa$生成会话密钥

$$K_{\mathrm{sess}}=\mathrm{KDF}(r_i\|\,r_j\|\,\mathrm{nonce}_i\|\,\mathrm{nonce}_j\|\,t_i\|\,t_j\|\,\mathrm{ID}_i\|\,\mathrm{ID}_j) \tag{30}$$

其中,ID_i与ID_j为双方的逻辑身份标识(例如链上账户地址)。随后,D_i发送$\mathrm{MAC}_{K_{\mathrm{sess}}}(\mathrm{nonce}_i\,/\!/\,\mathrm{nonce}_j)$给$D_j$完成正向确认,$D_j$返回$\mathrm{MAC}_{K_{\mathrm{sess}}}(\mathrm{nonce}_j\,/\!/\,\mathrm{nonce}_i)$完成反向确认。双方验证成功后确认会话密钥一致并未被篡改。

交接凭证构造如下。当前节点D_i或ES_{a_i}为下一跳$D_j@N_{a_j}$生成

$$\mathrm{HC}_{ij}=\{\mathrm{SFC\_ID},\mathrm{D}_j@N_{a_j},T_{\mathrm{now}},\mathrm{Nonce}_{ij}\} \tag{31}$$

其中,T_{now}为当前时间戳,Nonce_{ij}为交接随机数。所属域使用私钥$\mathrm{sk}_{N_{a_i}}$生成域级签名

$$\mathrm{Sig}_{N_{a_i}}=\mathrm{Sign}_{\mathrm{sk}_{N_{a_i}}}(\mathrm{HC}_{ij}) \tag{32}$$

然后,使用$\mathrm{pk}_{\mathrm{D}_j}$加密交接内容$\mathrm{Enc_HC}_{ij}=\mathrm{Enc}_{\mathrm{pk}_{\mathrm{D}_j}}(\mathrm{HC}_{ij}\,/\!/\,\mathrm{Sig}_{\mathrm{N}_{a_i}})$,交接报文$\mathrm{HC_Packet}_{ij}=\mathrm{Enc_HC}_{ij}$通过开放信道发送至目标域。目标无人机$D_j$使用$\mathrm{sk}_{\mathrm{D}_j}$解密$\mathrm{Enc_HC}_{ij}$,恢复$\mathrm{HC}_{ij}$和$\mathrm{Sig}_{N_{a_i}}$,并从BC查询$\mathrm{pk}_{N_{a_i}}$验证域签名。验证通过后,$D_j$检查自身标识是否与交接凭证一致,确认SFC_ID与本地任务一致,并检查T_{now}的时效性。如上述检查均通过,D_j接受交接,启动对应VNF功能,并通过已建立的K_{sess}安全传输后续数据。该过程沿路径逐跳执行,直至末节点完成服务链部署。

3.3.4　链上审计

当末节点D_L完成任务后,向编排器或所属边缘服务器发送任务完成通知。各参与域可根据策略将关键交接行为的摘要写入BC。对一次跨域交接$N_{a_i}\to N_{a_j}$,可构造审计条目

$$\mathrm{Log\_entry}=(\mathrm{SFC\_ID},N_{a_i}\to N_{a_j},T_{\mathrm{now}},\mathrm{Digest}_{ij}) \tag{33}$$

其中,Digest_{ij}为HC_{ij}及相关元数据的哈希摘要。对于重要任务,审计交易可附加FlexiTSS联合签名,确保多域共同认可审计记录。审计智能合约在接收日志后检查路径跳数、时间顺序与SAC中的时空约束是否一致,从而在链上形成可验证的、不可篡改的SFC执行轨迹。

3.4　跨域SFC编排器的轻量级动态选举

为消除静态中心编排器的单点风险并改善负载分配,本节给出基于业务分布的轻量级动态编排器选举算法。该算法利用拓扑中心性和路径覆盖度两个指标,对候选边缘服务器进行综合评价。

3.4.1　评价指标

设当前SFC涉及的无人机集合为$\mathcal{U}_{\mathrm{SFC}}$,参与域集合为$\mathcal{D}_{\mathrm{SFC}}$,任务总规模为$N_{\mathrm{total}}=|\mathcal{U}_{\mathrm{SFC}}|$。候选编排器集合记为$\mathcal{E}_{\mathrm{cand}}$。

(1)拓扑中心度。对候选边缘服务器$e\in\mathcal{E}_{\mathrm{cand}}$,其加权拓扑中心度定义为

$$\mathrm{WTC}(e)=\sum_{d\in\mathcal{D}_{\mathrm{SFC}}}\left(\frac{n_d}{N_{\mathrm{total}}}\cdot\mathrm{dist}(e,e_d)\right) \tag{34}$$

其中，n_d为域d中参与本次SFC的无人机数量，e_d为域d的边缘服务器，$\mathrm{dist}(e,e_d)$为e到e_d的最短跳数。该指标反映候选节点在业务相关域之间的平均拓扑距离，值越小越优。

（2）路径覆盖度。对候选节点e，其路径覆盖度定义为

$$\mathrm{PC}(e)=\frac{|\mathcal{U}_e\cap\mathcal{U}_{\mathrm{SFC}}|}{N_{\mathrm{total}}} \tag{35}$$

其中，$\mathcal{U}_e$为由e管辖或可直接控制的无人机集合。$\mathrm{PC}(e)$刻画本次SFC任务中可在该节点本域内直接调度的无人机比例，值越大意味着跨域调度与认证的额外开销越小。

（3）综合得分。为同时兼顾时延与本地处理能力，引入综合得分函数

$$\mathrm{SCORE}(e)=\omega\cdot\frac{\mathrm{WTC}_{\min}}{\mathrm{WTC}(e)}+(1-\omega)\cdot\mathrm{PC}(e) \tag{36}$$

其中，$\mathrm{WTC}_{\min}=\min_{e'\in\mathcal{E}_{\mathrm{cand}}}\mathrm{WTC}(e')$，$\omega\in[0,1]$为权重参数。通过比值$\mathrm{WTC}_{\min}/\mathrm{WTC}(e)$将中心度归一化到$[0,1]$区间，并与$\mathrm{PC}(e)$线性融合。延迟敏感场景中可取较大$\omega$，强调拓扑中心性；资源受限或本地处理优先的场景中可降低ω，增强路径覆盖度的权重。

3.4.2 选举过程

选举过程在每次新的SFC任务触发时运行，包括候选筛选、得分计算与竞争决策三个阶段。

在候选筛选阶段，任务发起域的边缘服务器向全网广播任务描述报文，包含SFC_ID、$\mathcal{D}_{\mathrm{SFC}}$和$\mathcal{U}_{\mathrm{SFC}}$的摘要。各边缘服务器$e$接收后，根据自身管理的无人机集合$\mathcal{U}_e$判断是否与$\mathcal{U}_{\mathrm{SFC}}$存在交集。如无交集，则认为与本次任务无关，不加入$\mathcal{E}_{\mathrm{cand}}$；否则，将自身加入候选集合。

在分布式得分计算阶段，每个候选节点$e\in\mathcal{E}_{\mathrm{cand}}$基于本地拓扑信息计算自己到每个$e_d$的最短跳数，求得$\mathrm{WTC}(e)$；结合$\mathcal{U}_e$和$\mathcal{U}_{\mathrm{SFC}}$的交集计算$\mathrm{PC}(e)$。通过一轮轻量级广播，候选节点交换各自的$\mathrm{WTC}(e)$或直接交换当前最小值，从而获得$\mathrm{WTC}_{\min}$。随后，各候选节点本地计算$\mathrm{SCORE}(e)$，形成去中心化的评分结果。

在竞争决策阶段，系统为选举设置时间窗口$[T_0,T_0+\Delta T]$。每个候选节点在窗口内随机选择一个时刻广播自己的$\mathrm{SCORE}(e)$和身份标识，并在整个窗口期间监听其他候选的得分广播。在本地维护当前观测到的最高得分及其对应节点。当某节点在其发送时刻前未检测到比自身$\mathrm{SCORE}(e)$更高的节点时，可以广播声明消息，宣布自己是本次SFC的编排器；其他候选节点在接收到得分更高的声明后放弃竞选，将声明节点记为当前编排器。如果窗口结束时尚未形成一致结果，那么可按需重新发起选举或由参与节点通过FlexiTSS对多个候选进行裁决。该算法在不引入集中式控制的前提下，以较低开销实现了对动态业务与拓扑变化的自适应编排器选择。

4 实验与结果分析

4.1 实验设置与评价体系

为系统评估本文所提出的基于联盟链与FlexiTSS的跨域SFC认证机制（以下简称Proposed）在低空智联网下的综合性能表现，本研究设计了一个基于离散事件仿真的实验环境。该仿真模拟了多域边缘计算场景下的大规模无人机网络，其中节点在空间上随机分布，并可根据业务需求动态组建跨域SFC。实验区域被划分为若干个独立的管理域，每个域内设有边缘计算节点以提供本地认证与协调功能。跨域SFC由随机选择的在线无人机节点按序动态构成，以模拟真实环境中网络拓扑的动态性与业务链路的异构特征。在对比方案的选择上，本研究选取了四种具有代表性的认证架构作为基准参照。这些方案涵盖了从传统集中式到现代分布式、从全局协同到局部自治的主要技术范式，旨在通过多维度的对比，深入揭示不同设计理念对系统性能的影响机制。

（1）Centralized-Auth（完全中心化认证架构）。该方案采用单一可信中心处理所有跨域认证请求，其设计理念源于经典的集中式信任模型，代表了传统系统中以中心化权威为基础的安全管理范式，有助于审视中心化架构在可扩展性与单点依赖方面的固有特性。

（2）Simple-Blockchain（基础区块链认证架构）。在此方案中，每个SFC节点均独立触发链上查询与验证操作，不引入任何批量优化机制，体现了区块链技术在认证领域的原生应用形态，为分析底层链上操作的开销及其对整体性能的影响提供了基础参照。

（3）Static-Orchestrator（静态编排认证架构）。该方案具备一定程度的批量验证能力，但其编排节点是静态指定，缺乏根据网络状态动态调整的能力，反映了在固定拓扑假设下具有一定优化但适应性有限的认证管理策略。

（4）P2P-NoBlockchain（纯点对点认证架构）。该方案完全依赖节点间的局部认证机制，不引入全局信任锚点，体现了去中心化系统中基于对等关系的轻量级认证理念，为探索全局信任与局部自治之间的权衡提供了重要视角。

为全面考察各认证方案在可扩展性、鲁棒性及运行效率等方面的表现，本研究设计了覆盖多维度参数的实验环境。无人机节点规模从20逐步递增至160，

以模拟不同规模的网络负载;管理域数量由3扩展至11,用于考察多域协同机制的有效性;SFC长度覆盖3~15跳,以反映不同复杂度的服务链认证需求;节点离线率与恶意节点比例在0.02~0.30区间内变化,用以评估系统在动态不可靠环境下的容错能力。所有实验结果均基于100次独立重复试验取统计平均值,以确保数据的可靠性与结论的统计显著性。

4.2　系统规模与时延性能分析

图2展示了各方案总时延随UAV网络规模(20~160)的变化趋势。随着节点规模扩大,各方案时延均呈现增长趋势,主要受网络拥塞与处理队列延长的影响。其中,P2P-NoBlockchain方案因无需全局共识或中心化协调,时延最低,可作为理论下界参考。Proposed方案的时延曲线与P2P-NoBlockchain方案最为接近,且在所有规模下均显著优于另外三种基准方案。从机制上分析,这得益于Proposed方案所采用的批量验证机制,有效抑制了规模扩展带来的时延增长。相比之下,Centralized-Auth方案受限于中心节点的I/O瓶颈,排队时延快速增长;Simple-Blockchain方案则因频繁的链上交互而引入较高开销,二者可扩展性均较差。

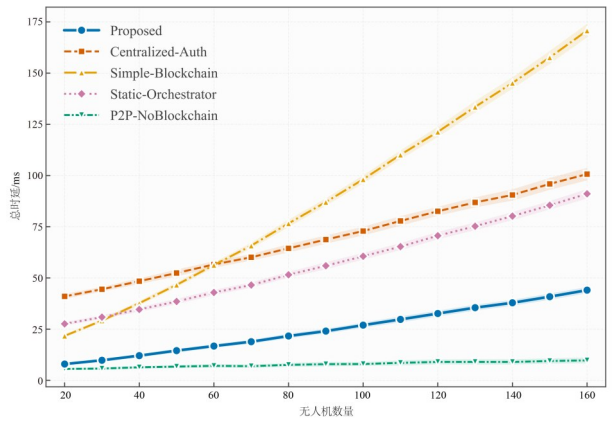

图2　系统总时延随UAV网络规模的变化曲线

Figure 2　System total delay curve with the change of UAV network scale

为深入分析时延构成,图3给出了不同SFC长度下的时延分解结果(柱状图中底部为认证时延,顶部为切换时延)。可以看出,随着SFC长度增加,各方案在数据平面的切换时延均近似线性增长,说明其在转发层面性能基本一致。然而,在控制平面的认证时延方面,Simple-Blockchain方案与Centralized-Auth方案均表现出明显的累积效应,反映出其逐跳验证或集中协调机制在长链路场景下的局限性。Proposed方案通过FlexiTSS门限签名对多跳认证请求进行聚合处理,使得认证时延对SFC长度变化不敏感,表明该方案在长链路、跨多域的复杂服务链中仍能保持较低的认证开销。

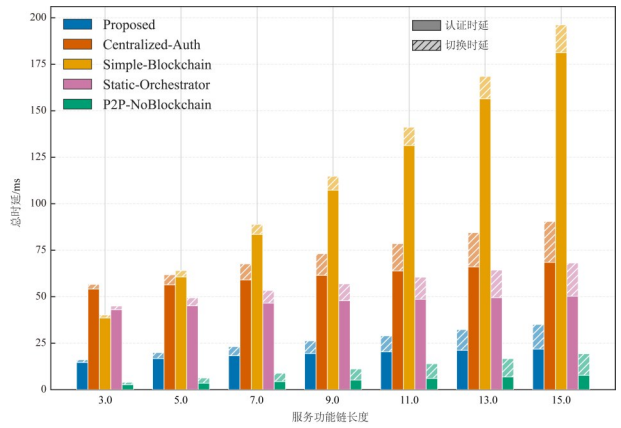

图3　不同SFC长度下的认证时延与切换时延分解

Figure 3　Decomposition of authentication delay and handover delay under different SFC lengths

4.3　复杂环境下的鲁棒性与安全性

为评估方案在动态不可靠环境下的表现,图4和图5分别从服务可用性和安全韧性两个维度进行分析。

图4反映了节点离线概率(0.02~0.30)对SFC任务成功率的影响。Proposed方案在整个区间内保持最高成功率,在高离线区域性能差距更明显。其优势源于结合联盟区块链的全局状态视图与多域协同机制,当部分节点离线时,系统可基于冗余的诚实域节点快速完成签名重构与路径恢复。Simple-Blockchain方案因缺乏批量优化机制,在高离线率环境下易出现路由失败,成功率下降明显。Centralized-Auth受单点故障影响,对节点动态性极为敏感。

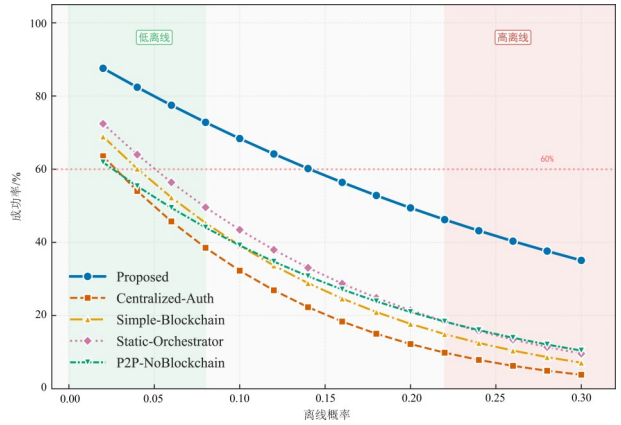

图4　节点离线概率对SFC任务成功率的影响

Figure 4　Impact of node offline probability on SFC task success rate

图5展示了系统在面对恶意节点攻击时的稳健性。随着恶意节点概率升高,P2P-NoBlockchain方案的成功率急剧下降,反映出其在无信任锚环境下对抗

中间人攻击或拒绝服务攻击的脆弱性。Proposed方案通过FlexiTSS的(t,n)门限机制实现拜占庭容错，只要合谋恶意域数量不超过阈值t，即可保证认证的正确性与服务连续性，因此在恶意比例达到0.30时仍能维持相对较高的可用性，展现出良好的安全韧性。

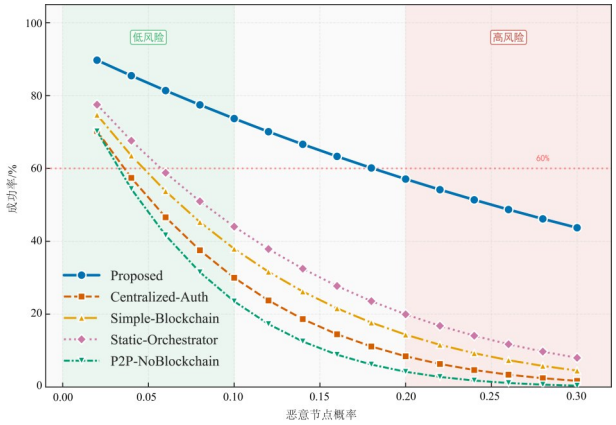

图5 恶意节点概率对SFC任务成功率的影响

Figure 5 Impact of malicious node probability on SFC task success rate

4.4 通信开销与域扩展性

图6对比了各方案在网络控制平面的通信开销。结果显示，Proposed方案通过聚合签名技术，大幅压缩了控制信令的体积，其开销仅略高于无安全防护的P2P-NoBlockchain方案。相比之下，Simple-Blockchain方案产生了巨量的链上交互数据，而Centralized-Auth方案则带来了沉重的回程信令负担，两者的网络资源消耗随SFC长度呈快速增长趋势，难以适应带宽受限的低空智联网环境。

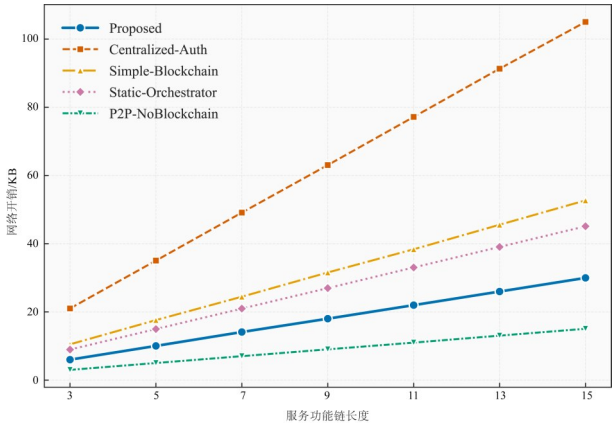

图6 各方案控制平面通信开销对比

Figure 6 Comparison of control plane communication overhead among various schemes

图7考察了管理域数量从3增至11对认证时延的影响。随着域数量增加，跨域认证协调复杂度上升，Centralized-Auth方案与Simple-Blockchain方案的认证时延增长显著，表明其架构难以适应大规模多域协同场景。Proposed方案通过动态编排与门限签名机制有效降低了域间协调开销，时延增长较为平缓，展现出较好的多域扩展性。P2P-NoBlockchain方案因不涉及域间共识，时延几乎不受域数影响，但其代价为全局安全机制的缺失。

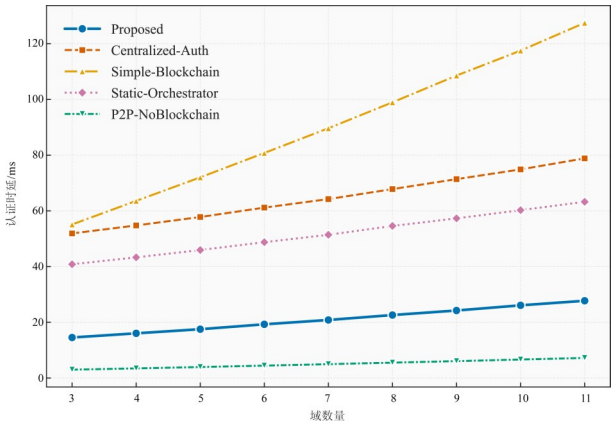

图7 管理域数量对跨域认证时延的影响

Figure 7 Impact of the number of management domains on cross-domain authentication delay

4.5 负载均衡与综合效能评估

图8通过最大服务器负载与Jain公平性指数(Jain's Fairness Index，JFI)评估系统负载均衡性能。Proposed方案依托动态编排器选举算法，能根据实时负载将认证任务合理分布至各域边缘节点，JFI接近1.0，最大负载保持较低水平，显示出良好的负载均衡效果。Centralized-Auth则呈现明显的负载集中现象，中心节点压力突出，JFI仅为0.2左右。Static-Orchestrator受限于静态编排策略，在高并发场景下仍存在一定程度的负载不均。

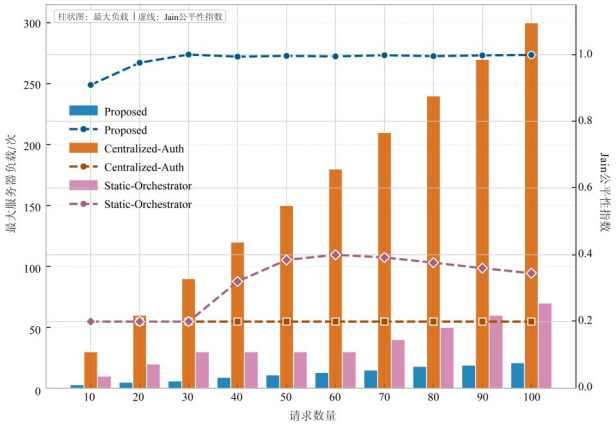

图8 各方案服务器负载均衡性能对比

Figure 8 Comparison of server load balancing performance among various schemes

图9采用雷达图从时延、吞吐量、可靠性、安全性和开销五个维度对各类方案进行综合对比。Proposed方案在各维度均表现良好,所形成的雷达图面积最大、形状均衡,说明其在保持高性能(低时延、低开销)的同时未牺牲安全性与可靠性,有效突破了传统认证方案中性能、安全性和可扩展性之间的权衡困境,适用于跨域低空智联网中的动态复杂环境。

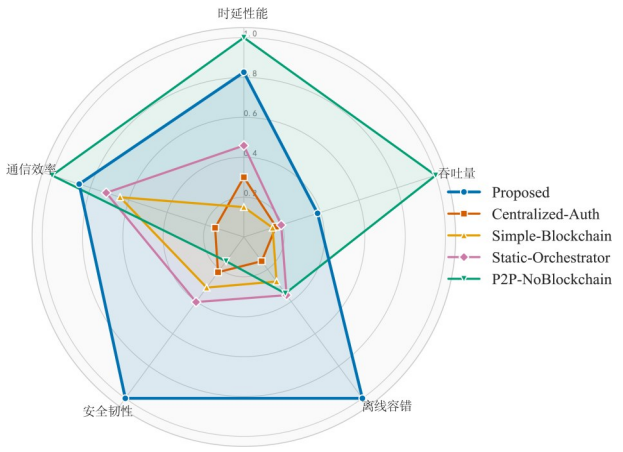

图9　各认证方案在多维性能指标上的综合对比雷达图

Figure 9　Radar chart of comprehensive comparison of various authentication schemes on multi-dimensional performance indicators

5　结论

本文针对跨域低空智联网中SFC面临的安全认证问题,提出了一种基于联盟区块链与门限签名的创新解决方案。研究重点解决了传统认证方案在跨域协同场景下存在的单点故障、效率低下和可扩展性不足等关键问题。该方案通过构建分布式信任管理体系,建立了可靠的跨域认证基础,在此基础上设计的FlexiTSS门限签名方案通过批量验证机制显著提升了认证效率。此外,进一步引入动态编排器选举算法,基于拓扑中心度和路径覆盖度实现了系统负载的智能均衡,最终通过完整的协议设计确保了服务链全生命周期的安全性。实验结果表明,相较于传统中心化认证与基础区块链等方案,本文所提方案在认证时延、系统吞吐量和环境鲁棒性等关键指标上均表现更优,尤其是在大规模网络拓扑和长服务功能链场景下展现出更强的稳定性。凭借这一性能优势,本文所提方案能够有效缓解现有方法在实际部署中长期存在的安全性、效率与可扩展性难以兼顾的矛盾。未来研究将进一步拓展其应用边界,包括探索分层共识机制支持更大规模部署、开发运动感知的自适应凭证管理策略应对高动态场景,以及设计轻量级密码学实现适配多样化边缘设备,从而为更广泛的低空智联网应用场景提供全面支持。

参考文献

[1] Harbi Y, Medani K, Gherbi C, et al. A systematic literature review of blockchain technology for Internet of drones security[J]. Arabian Journal for Science and Engineering, 2023, 48(2): 1053-1074.

[2] Jia Z Y, Sheng M, Li J D, et al. VNF-based service provision in software defined LEO satellite networks[J]. IEEE Transactions on Wireless Communications, 2021, 20(9): 6139-6153.

[3] Yazdinejad A, Parizi R M, Dehghantanha A, et al. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1120-1132.

[4] Yang W C, Wang S, Yin X F, et al. A review on security issues and solutions of the Internet of drones[J]. IEEE Open Journal of the Computer Society, 2022, 3: 96-110.

[5] 吴启晖, 董超, 贾子晔, 等. 低空智联网组网与控制理论方法[J]. 航空学报, 2024, 45(3): 028809.
Wu Qihui, Dong Chao, Jia Ziye, et al. Networking and control mechanism for low-altitude intelligent networks[J]. Acta Aeronautica et Astronautica Sinica, 2024, 45(3): 028809. (in Chinese)

[6] 张楦杰, 张敏, 刘韬, 等. 基于区块链的无人机网络跨域身份认证研究[J]. 计算机应用研究, 2024, 41(7): 1959-1964.
Zhang Xuanjie, Zhang Min, Liu Tao, et al. Research on cross-domain identity authentication of unmanned aerial vehicle network based on blockchain[J]. Application Research of Computers, 2024, 41(7): 1959-1964. (in Chinese)

[7] Xie M Y, Chang Z, Wang L, et al. Blockchain-assisted lightweight cross-domain authentication for multi-UAV wireless networks[J]. IEEE Transactions on Mobile Computing, 2025, 24(11): 11449-11464.

[8] 于静茹, 姚升悦, 陈喜群, 等. 面向网联自动驾驶部署的车—路—无人机跨域协同技术[J]. 中国图象图形学报, 2024, 29(11): 3293-3304.
Yu Jingru, Yao Shengyue, Chen Xiqun, et al. Cross-domain collaborative technology among vehicles, infrastructure, and drones for connected and autonomous driving deployment[J]. Journal of Image and Graphics, 2024, 29(11): 3293-3304. (in Chinese)

[9] Zhao J J, Xue S T, Cai K Q, et al. Near-field integrated sensing and communications for secure UAV networks[J]. IEEE Journal on Selected Areas in Communications, 2026, 44: 371-385.

[10] Wu Y, Jia Z Y, Wu Q H, et al. Adaptive QoE-aware SFC orchestration in UAV networks: A deep reinforcement learning approach[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(6): 6052-6065.

[11] Feng C S, Liu B, Guo Z, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones[J]. IEEE Internet of Things Journal, 2022, 9(8): 6224-6238.

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

[13] Huang K K, Hu H D, Lin C L. BAKAS-UAV: A secure blockchain-assisted authentication and key agreement scheme for unmanned aerial vehicles networks[J]. IEEE Internet of Things Journal, 2024, 11(22): 36858-36883.

[14] 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.

[15] Shahidinejad A, Abawajy J H. Anonymous blockchain-assisted authentication protocols for secure cross-domain IoD communications[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(3): 2661-2674.

[16] Feng C S, Liu B, Yu K P, et al. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3582-3592.

[17] Tong Z H, Wang J J, Hou X W, et al. Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks[J]. IEEE Internet of Things Journal, 2024, 11(21): 34270-34282.

[18] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报, 2021, 44(1): 55-83.
Xu Ke, Ling Sitong, Li Qi, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 55-83. (in Chinese)

[19] Chen Z G, Zhu C F, Zhang H W, et al. A lightweight UAV secure communication scheme integrating cross-domain group authentication and reputation awareness[J]. Internet of Things, 2025, 34: 101781.

[20] Yang Y, Wang B H, Guo R X, et al. Efficient and secure service function chain deployment method for delay optimization in air traffic information network[J]. Scientific Reports, 2024, 14: 25829.

[21] Wang W M, Zhang S M, Liu G J, et al. A blockchain-based cross-domain authentication scheme for unmanned aerial vehicle-assisted vehicular networks[J]. World Electric Vehicle Journal, 2025, 16(4): 2155-2166.

[22] Hossain M I, Tahtali M, Turhan U, et al. Blockchain integration in UAV networks: Performance metrics and analysis[J]. Sensors, 2024, 24(23): 7813.

[23] Xie H, Zheng J, Wei S J, et al. Blockchain-and-6G-based ubiquitous UAV task security management architecture [J]. Computer Communications, 2024, 217: 259-267.

[24] Chen J X, Wang Z X, Srivastava G, et al. Industrial blockchain threshold signatures in federated learning for unified space-air-ground-sea model training[J]. Journal of Industrial Information Integration, 2024, 39: 100593.

[25] He L, Gan Y, Yin Y F. Efficient threshold attribute-based signature scheme for unmanned aerial vehicle (UAV) networks[J]. Electronics, 2025, 14(2): 339.

[26] Wang S Y, Yang L X. Securing dynamic service function chain orchestration in EC-IoT using federated learning[J]. Sensors, 2022, 22(23): 9041.

[27] 曹怡璐, 贾子晔, 尤嘉豪, 等. 基于SDN和NFV的空天地一体化网络任务部署与恢复综述[J]. 电信科学, 2025, 41(5): 1-16.
Cao Yilu, Jia Ziye, You Jiahao, et al. A survey of task deployment and recovery in space-air-ground integrated networks based on SDN and NFV[J]. Telecommunications Science, 2025, 41(5): 1-16. (in Chinese)

[28] 习宁, 周晓琳, 孙聪, 等. 支持物理交互的无人机飞控系统安全测试方法[J]. 电子学报, 2025, 53(3): 765-781.
Xi Ning, Zhou Xiaolin, Sun Cong, et al. Security testing method for unmanned aerial vehicle flight control system supporting physical interaction[J]. Acta Electronica Sinica, 2025, 53(3): 765-781. (in Chinese)

[29] 徐勇军, 鲁承壮, 董燚恒, 等. 低轨卫星通信系统面向安全通信的鲁棒资源分配算法[J]. 电子学报, 2025, 53(5): 1482-1490.
Xu Yongjun, Lu Chengzhuang, Dong Yiheng, et al. Robust resource allocation algorithm for secure communication in LEO-based satellite communication systems[J]. Acta Electronica Sinica, 2025, 53(5): 1482-1490. (in Chinese)

作者简介

吴　遥　男,1994年1月出生于江西省南昌市。现为南京航空航天大学电子信息工程学院博士研究生。主要研究方向为信息安全、网络功能虚拟化。

E-mail: wu_yao@nuaa.edu.cn

贾子晔　女,1990年10月出生于山西省忻州市。现为南京航空航天大学电子信息工程学院副教授。主要研究方向为空天地一体化网络、低空智联网。

E-mail: jiaziye@nuaa.edu.cn

朱秋明　男,1979年8月出生于江苏省苏州市。现为南京航空航天大学电子信息工程学院教授。主要研究方向为无线信道测量建模与数字孪生、电磁频谱态势可视化测绘与认知。

E-mail: zhuqiuming@nuaa.edu.cn

周福辉　男,1988年7月出生于江西省抚州市。现为南京航空航天大学电子信息工程学院教授。主要研究方向为频谱智能管控和资源鲁棒优化、认知智能与知识图谱。

E-mail: zhoufuhui@nuaa.edu.cn