基于区块链的无人机轻量化身份认证方案

李扬，陈浩男，胡全贵，于莉莉，赵光俊
国网思极位置服务有限公司，北京 102200

摘要
目前无人机身份认证存在流程繁琐低效、无人机资源限制等挑战，为应对这些挑战，设计分层区块链架构，差异化拆分去中心化身份（decentralized identifier， DID）标识与认证声明链上存储逻辑，提出一种基于国密算法的无人机身份认证方案，重构轻量化身份认证协议。方案采用轻量级且安全的分层区块链结构，实现快速身份验证；结合国密算法完成数字签名、会话密钥协商与数据加密，确保身份数据的合法性；基于去中心化身份在区块链全局信息更新链存储 DID 文档，身份信息更新链存储可验证声明，实现无人机身份的统一管理。在联盟链 Hyperledger Fabric 框架下进行实验并分析，方案具有较低的计算开销，并能够有效应对动态无人机群应用中的多种安全威胁。

关键词
区块链；无人机；国密算法；身份认证

中图分类号：TP309/V279 文献标志码：A

Lightweight identity authentication scheme for UAV based on blockchain

LI Yang, CHEN Haonan, HU Quangui, YU Lili, ZHAO Guangjun
State Grid Siji Location Service Co. , Ltd. , Beijing 102200, China

Abstract
At present, there are challenges in UAV identity authentication such as cumbersome and inefficient process and UAV resource limitation. In order to deal with these challenges, this paper proposes a lightweight identity authentication scheme for UAV based on hierarchical blockchain. The scheme adopted a lightweight and secure hierarchical blockchain structure to achieve fast authentication. Combined with the national secret algorithm, digital signature, session key agreement and data encryption were completed to ensure the legitimacy of identity data. Based on the Decentralized Identifier (DID), DID documents were stored in the global information update chain of the blockchain, and verifiable declarations were stored in the identity update chain, so as to realize the unified management of UAV identity. Experiments and analysis were carried out under the framework of the consortium blockchain Hyperledger Fabric. The results show that the scheme has low computational overhead and can effectively deal with various security threats in the application of dynamic UAV swarm.

Key words

blockchain, unmanned aerial vehicle, national secret algorithm, authentication

1 引言

近年来，无人机技术广泛应用于军事侦察、物流运输等诸多领域，无人机网络正朝着动态化、规模化、异构化的方向发展[1]。无人机网络安全是无人机系统可靠运行的保障，无人机身份认证是无人机安全通信的关键环节。

传统的身份认证机制大多依赖公钥基础设施等中心化信任模型[2]，对于资源受限无人机的动态网络仍存在一些挑战。中心化信任模型依赖可信第三方认证中心，且数字证书的签发和验证阶段流程繁琐，在无人机跨域认证场景中，中心化信任模型难以建立互信身份，存在隐私泄露的风险。

一些学者提出了基于区块链的无人机身份认证，Du等人[3]提出基于雾节点辅助区块链的无人机身份认证方案，利用智能合约实现无人机注册与认证。张楦杰等人[4]提出基于区块链的无人机跨域身份认证方案，通过身份标识匿名化抵御常见的网络攻击。高杉逸[5]基于椭圆曲线密码学构造一种溯源密钥体系，并将该体系应用于分布式身份模型，具有更全面的安全性表现。Qiao等人[6]利用私有链保证无人机的匿名性，无人机在进行跨域认证之前先相互认证，形成相互信任的的无人机群组。Zuo等人[7]提出了包含需求分析层、评估层和管理层的区块链无人机群节点信任管理模型，解决无人机群节点动态进出信任度评估精度低的问题。Kong等人[8]设计了基于区块链的路由协议，能够自适应配置区块链网络。Jiao等人[9]提出了将区块链与可聚合子向量承诺结合压缩身份状态，优化了批量身份验证的计算复杂度。在分布式身份DID的研究中，Peng等人[10]提出了基于DID的无人机群身份管理模型，避免集中式管理存在的单点故障，为本文研究提供一定参考。在密码算法方面，将国密算法应用在无人机领域已成为一种趋势。国密SM2公钥密码算法、SM3哈希算法和SM4分组密码算法在数字签名、消息完整性验证、密钥交换、加密解密等方面与国际标准具有相当的安全性，且更符合国内监管要求。已有研究者将国密算法与区块链结合，应用于数据共享[11]、身份认证[12]等场景，并验证了方案的安全性与可行性，但将SM2算法、SM3算法和SM4算法系统地应用在无人机身份认证领域的研究尚不充分，现有研究未充分考虑无人机资源受限特性，在计算与通信开销方面仍有优化空间；其次，较少研究者将分层区块链架构、国密算法与DID标准应用在无人机身份认证场景，同时满足高效、合规、身份自主管理的特点。

针对上述挑战，本文聚焦于资源受限的无人机动态身份认证场景，提出一种轻量化的分布式身份认证方案，主要贡献如下：

(1)提出双层区块链的轻量化身份认证架构。采用全局信息链和身份信息更新链双层区块链结构，全局信息更新链作为全局信任链，仅存储无人机的分布式身份标识、公钥和凭证哈希的轻量级身份数据；身份信息更新链作为业务链，存储身份认证信息并处理身份认证事务，实现身份验证的快速响应。

(2)设计基于国密SM2、SM3、SM4算法的身份认证协议。遵循国密算法，设计基于椭圆曲线的无人机身份认证协议，降低认证过程中的计算开销，包括无人机身

份注册、边缘节点注册、本域身份认证和跨域身份认证四个阶段。

(3)实现DID的分布式无人机身份认证模型。基于去中心化身份标准，为每架无人机生成唯一的分布式身份标识，构建无人机硬件标识与分布式数字身份的绑定、链上存证的无人机身份认证体系。

2 相关技术

2.1 无人机网络与安全威胁模型

无人机网络主要由无人机和地面控制站两类实体构成，地面控制站验证在本领域的无人机身份，授予无人机飞行权限[13]。然而，无人机网络开放性与动态性使得无线信号在广播时通信数据易被窃听、篡改或重放[14]，传统的公钥基础设施依赖于中心机构，存在单点故障风险[9]。

因此基于上述挑战并参考文献[15]，本文构建以下威胁模型：

(1)外部攻击者：能够被动窃听或拦截、篡改、重放无线信道的通信数据。

(2)内部恶意节点：已通过初始身份注册的合法无人机或地面节点可能被敌手俘获或仿冒，从而发起中间人攻击或者消息伪造攻击。

2.2 区块链技术

区块链是一种分布式账本技术，是工业4.0的关键推动因素之一，应用于医疗、物流、电力、制造业和电子商务等领域[16]。区块链因具有去中心化、不可篡改、可追溯等特点，契合本模型中的安全认证需求。然而公有链的高能耗共识机制和全量数据存储模式难以满足无人机网络的轻量化需求。因此，本文提出的分层区块链架构更有利于物联网环境，能够提升模型的可扩展性和处理效率[17]。

2.3 去中心化身份(DID)

去中心化身份(Decentralized Identifier, DID)是W3C推荐的一种数字身份标准，旨在让实体能够完全掌控自己的数字身份，而不依赖于任何中心化机构[18]，其核心组件包括：DID标识符、DID文档和可验证声明(Verifiable Claims, VP)。DID文档用来描述DID主体，包含DID标识符与其对应的公钥等信息，该文档存储在分布式账本或点对点网络中。可验证声明是由发行者签名的数字声明，持有者可以向验证者出示身份声明，以证明其身份属性。

2.4 国密算法

SM2[19]算法是我国自主设计的椭圆曲线公钥密码算法，支持椭圆曲线迪菲-赫尔曼密钥交换(elliptic curve Diffie - Hellman key exchange，ECDH)协议，包含数字签名、密钥交换和公钥加密三个模块，其安全性基于椭圆曲线离散对数困难问题，与RSA算法相比较，SM2的安全性更高，计算量更小。SM3算法可用于商业加密应用中的数字签名认证、随机数生成和消息认证码的生成，包含消息填充和解析、消息扩展和消息压缩三个阶段。SM4[20]算法是一种分组对称密码算法，分组长度和密钥长度均为128位，采用非平衡Feistel结构，经过32轮迭代运算，具有较高的安全性和实现效率。

3 系统模型

3.1 模型概述

区别于现有文献[4]依托区块链消除中心化CA单点故障的传统思路，本文提出双层区块链架构，对DID数据、可验证声明做分层存储，同时面向无人机资源受限场景，设计国密分层验签机制，形成适配无人机场景下的定制化方案。

本文提出的基于分层区块链和国密算法的轻量化无人机身份认证模型，包括全局信息更新链、身份信息更新链、边缘节点、KGC、无人机五个实体，区块链网络采用联盟链。本文方案模型如图1所示。

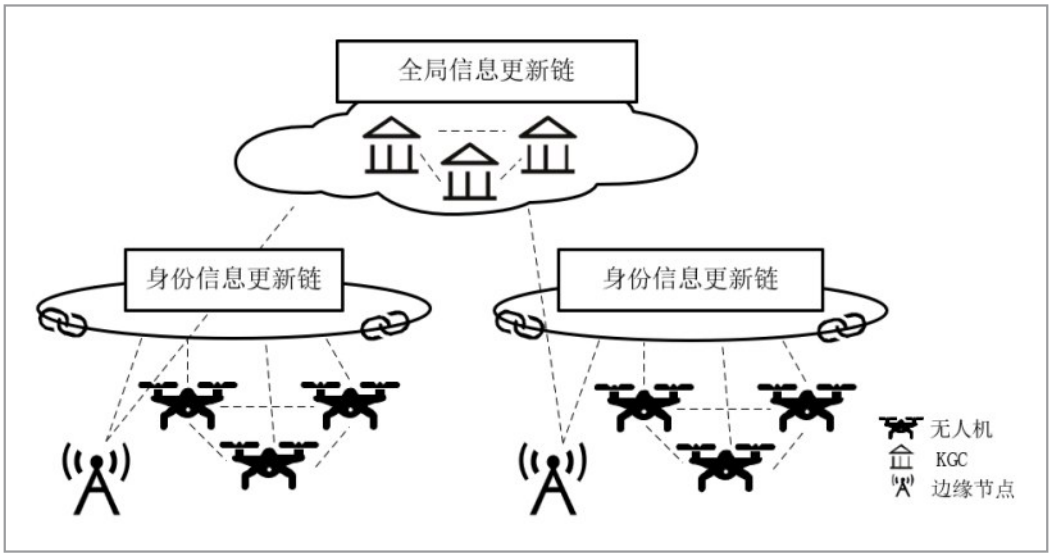

图1 系统模型图

全局信息更新链（global information update chain, GIUC）：是无人机身份认证模型的全局信任层，仅存储无人机DID、公钥和身份声明哈希，通过存储轻量级数据降低共识与存储开销。

身份信息更新链（identity information update chain, IIUC）：负责本域和跨域的无人机身份验证，存储可验证声明，与全局信息更新链进行DID标识符校验，提高认证效率。

无人机（unmanned aerial vehicle, UAV）：无人机具有发起本域或跨域身份认证请求的能力。各个域内的每架无人机都拥有唯一的DID标识符和用于身份验证的合法信息，无人机在访问域时必须经过身份认证。

边缘节点（edge node）：部署在无人机作业域的轻量化节点，对无人机进行身份认证，参与区块链共识。

密钥生成中心（key generation center, KGC）：可信第三方机构，KGC参与系统参数的生成。在实体注册阶段，为终端无人机、边缘节点生成公私钥对。

3.2 符号及描述

双层区块链的分布式无人机身份认证方案所用到的密码学符号如表1所示。

表1 密码学符号表

符号	含义描述	符号	含义描述
HASH	SM3算法	sk_{EN}	边缘节点私钥
sk_{KGC}	KGC私钥	pk_{EN}	边缘节点公钥
pk_{KGC}	KGC公钥	ID_{UAV}	无人机身份标识
sk_{UAV}	无人机私钥	ID_{EN}	边缘节点身份标识
pk_{UAV}	无人机公钥	$Sign$	SM2签名算法

3.3 模型关键流程设计

3.3.1 系统初始化

系统初始化阶段由KGC完成，KGC选择椭圆曲线E确定参数并公布，选择生成元P，秘密保存私钥sk_{KGC}，生成对应公钥$pk_{KGC}=sk_{KGC}\cdot P$。

3.3.2 实体注册

参与区块链网络的实体都需要进行注册，以获取唯一的去中心化身份标识符DID。实体注册包括边缘节点注册和无人机身份注册。

(1)边缘节点注册过程如下：

1)边缘节点将身份信息及时间戳(ID_{EN},T_{EN})传输至KGC。

2)KGC收到(ID_{EN},T_{EN})，随机选择随机数sk_{EN}作为边缘节点的私钥，计算其公钥$pk_{EN}=sk_{EN}\bullet P$，DID标识符$DID_{EN}=HASH(ID_{EN}\,//\,pk_{EN})$，其中$HASH$算法采用国密SM3算法。

3)KGC删除sk_{EN}，并将DID文档$\{DID_{EN},pk_{EN}\}$存储至全局信息更新链。

(2)无人机注册过程如下：

1)无人机通过安全信道发送身份信息唯一标（如出厂硬件序列）和时间戳(ID_{UAV},T_U)至KGC。

2)KGC收到(ID_{UAV},T_U)验证时间戳是否在允许范围内，若有效，则选择随机数作为其私钥sk_{UAV}，计算公钥$pk_{UAV}=sk_{UAV}\bullet P$，DID标识符$DID_{UAV}=HASH\left(ID_{UAV}\,//\,pk_{UAV}\right)$。

3)KGC删除sk_{UAV}，将$\{DID_{UAV},pk_{UAV}\}$传输至全局信息更新链。

4)无人机与边缘节点通过ECDH协商会话密钥key,，向边缘节点发送注册请求，消息包含(Sig_{UAV},C)，其中$Sig_{UAV}=Sign(sk_{UAV},T_{UAV}\,//\,HASH(VC))$，$C=E\_SM4(key,VC)$，可验证凭证(Verifiable Credential，VC)包含无人机的$VCID$、DID标识符、设备型号、域范围、任务类型等。

5)边缘节点收到(Sig_{UAV},C)后，查询全局信息更新链DID文档提取公钥pk_{UAV}，验证签名有效性，并解密C获取VC，检查时间戳T_{UAV}是否在有效时间范围，防止重放攻击。

6)边缘节点核验无人机硬件序列是否在预授权列表中，若存在，对无人机传输的身份数据签名，将可验证声明VP同步广播至身份信息更新链，可验证声明哈希$VPHash$同步至全局信息更新链，$VP=(VP_{ID},DID_{UAV},DID_{EN},Sign\left(sk_{EN},VC\right))$。签名算法采用SM2公钥密码算法。

3.3.3 本域身份认证

(1)认证请求：UAV_i向边缘节点EN_k发送认证请求，$UAV_i\rightarrow EN_k{:}AuthReq=\{DID_{UAV},Sig_{UAV_i},C\}$，$C=E\_SM4(key,M),Sig_{UAV_i}=Sign(sk_{UAV_i},M)$，$M=timestamp_1\,//\,VC_1$，其中$timestamp_1$为当前时间戳，$key$为双方协商的会话密钥。

(2)解密及验证：EN_k收到请求后，查询身份信息更新链是否存在UAV_i的可验证声明VP_2，如有则查询UAV_i的公钥pk_{UAV_i}和$VCHash$，验证签名有效性，解密得到M，并验证$HASH\left(VC_1\right)=VCHash$是否相等，若

相等且 $timestamp_1$ 有效，则允许无人机 UAV_i 与边缘节点 EN_k 通信。

3.3.4 跨域身份认证

(1)跨域请求：UAV_j 从作业域 $Domain_1$ 访问作业域 $Domain_2$，向 $Domain_2$ 的边缘节点 EN_m 发送凭证 VP 申请跨域访问，$UAV_j \rightarrow EN_m$:$CrossAuthReq = \{DID_{UAV_j}, VP_1, timestamp_2, Sig_{UAV_j}\}$，$Sig_{UAV_j} = Sign\left(sk_{UAV_j}, VP_1 \,//\, DID_{UAV_j} \,//\, timestamp_2,\right)$。

(2)验证身份：EN_m 验证签名及时间有效性，查询全局信息更新链 DID_{UAV_j} 对应的可验证声明哈希 $VPHash$，验证 $HASH\left(VP_1\right) = VPHash$ 是否一致，确认 $Domain_1$ 为可信域，解析 VP 中的设备型号、域范围、任务类型等信息。

(3)跨域认证上链：EN_m 核验无人机 UAV_j 是否在预授权列表中，若存在，对跨域认证凭证 VC_2 签名生成认证声明 VP_2，将其写入 $Domain_2$ 的身份信息更新链。其中 $VC_2 = \{VP_{ID}, DID_{UAV_j}, DID_{EN_m}, Domain_1, Domain_2, Sig_{EN_m}\}$，$Sign_{EN_m} = (sk_{EN_m}, VC_2)$ 并将 VP_2Hash 同步至全局信息更新链。

4 实验结果与分析

4.1 安全性分析

4.1.1 抗中间人攻击

对于中间人攻击，中间人必须假冒无人机或者边缘节点。在本方案中，无人机与边缘节点间通信采用SM2签名以及SM4加密算法传输信息，中间人无法获取无人机和边缘节点的私钥伪造合法签名。其次，全局信息更新链存储DID文档，中间人无法篡改无人机和边缘节点的身份。该方案能够抵抗抗中间人攻击。

4.1.2 抗消息篡改

无人机在进行身份认证时，认证请求包含时间戳，由无人机的私钥签名，若攻击者篡改认证请求中的任意值，边缘节点查询区块链提取无人机公钥，在签名验证时认定为无效请求。若攻击者重复发送截获的合法消息，因请求中的时间戳与当前时间差超过阈值而拒绝请求，有效抵御消息篡改与重放攻击。同时，无人机与边缘节点协商的会话密钥椭圆曲线点，会话密钥哈希值存储在区块链中，因此，攻击者无法获取并篡改正确会话密钥。

4.1.3 抗身份假冒

无人机和边缘节点的身份合法性依赖全局信息更新链的DID文档和SM2私钥签名技术。攻击者若要假冒合法无人机，需同时修改无人机的私钥与DID文档，而SM2私钥存储于无人机本地安全模块，KGC不保留私钥备份，攻击者无法获取私钥，DID文档存储在全局信息更新链，具有不可篡改性，攻击者无法伪造合法的DID文档。因此，本方案可有效抵御身份假冒攻击。

4.2 性能分析

在仿真环境中进行实验测试，实验使用的服务器CPU为Intel Xeon Silver 4309Y，内存为128G。为了进行有效测试，使用Docker技术来模拟无人机节点，使用Kubernets来自动化管理容器。区块链基于Hyperledger Fabric 2.4构建，采用PBFT共识算法，Python实现。DID文

档遵循 W3C 可验证凭证标准。国密 SM2、SM3、SM4 算法通过标准 GmSSL 密码库实现。

(1) 认证时延与吞吐量分析

经过仿真实验，得到在不同网络规模下，系统的平均认证时延和峰值吞吐量，结果如图 2 所示。

从图 2 可以看出，在 50 个节点以下的中等规模网络中，平均认证时延被控制在 200 毫秒以内，能够满足无人机协同任务对实时认证的需求。尽管随着身份信息更新链内共识消息的增加，当节点数增至 100，时延为 310 毫秒仍在可接受范围内。随着节点数增加，吞吐量缓慢下降，当节点数为 20 时，系统吞吐量约 87TPS，在 100 节点时约为 50TPS，所提出的分层区块链架构在吞吐量上仍具有明显的优势。

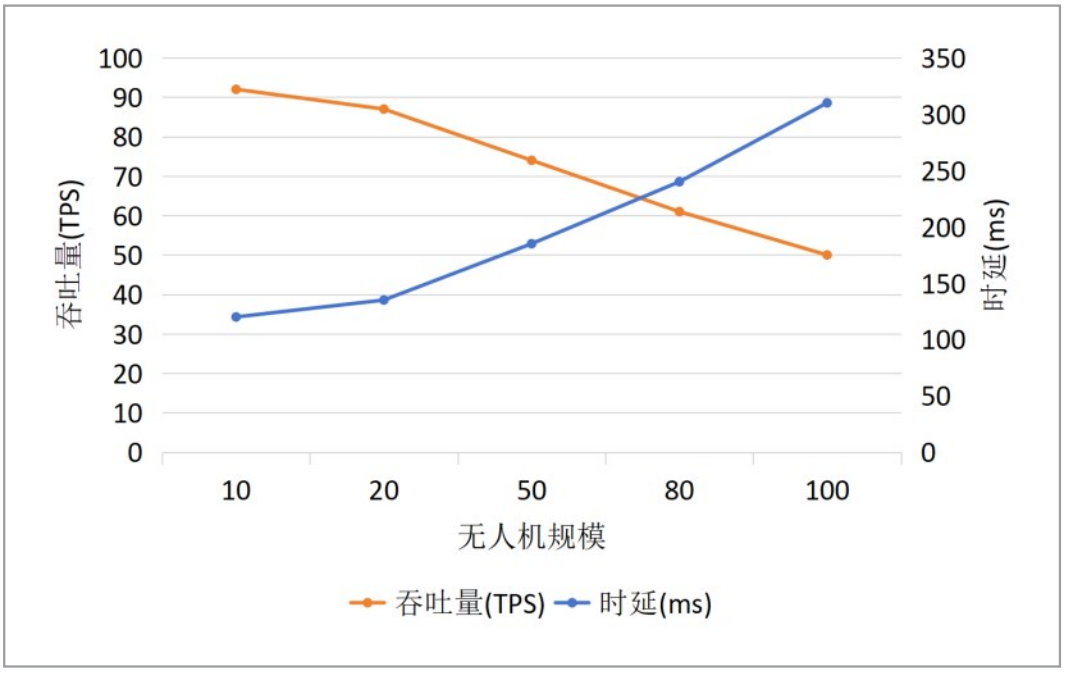

图 2 认证时延与吞吐量变化图

(2)计算开销分析

本文提出的无人机轻量化认证方案，从注册阶段和认证阶段两过程分析计算开销，其中注册阶段包括无人机注册和边缘节点注册，认证阶段分为本域认证和跨域认证。T_m 为椭圆曲线点乘运算，T_h 为哈希运算，T_e 加密运算，T_s 为签名运算，根据文献[4]，T_m=4.107ms，T_h=0.320ms，T_e=4.406ms，T_s=2.165ms。本文的计算开销对比实验如表 2 所示，在注册阶段，本文方案所用时为 8.854ms，文献[4]所需用时为 9.494ms；在认证阶段，本文本域认证所用时为 6.815ms，跨域认证所用时为 4.97ms，文献[4]没有进行本域认证，跨域认证所用时为 11.339ms，注册阶段和认证阶段本文方案均具有较小的计算开销。

(3)对比分析与讨论

本研究提出的方案与基于传统 PKI 的

表2 计算开销

方案	注册阶段	认证阶段	
		本域认证	跨域认证
本文	$2T_m+2T_h$	$T_e+T_s+T_h$	$2T_s+2T_h$
文献[4]	$2T_m+4T_h$	×	$2T_m+T_s+3T_h$

中心化认证方案[21]和基于单一公有链的认证方案[22]两种典型方案进行对比，对比结果如表3所示。传统方案采用证书验证通信开销大，认证时延长，且身份依赖于中心化机构，单一公有链方案受制于区块的确认，需要在终端同步大量交易数据，本文方案在认证时延、通信开销及隐私安全保护方面均具有优势。

本方案采用分层区块链架构，平衡去中心化与性能，通过全局信息更新链建立全局信任，同时利用身份信息更新链处理认证事务，与其他两种方案相比，本方案在时延和通信开销方面，具有较好的优势。

性能测试结果表明，在基于Docker与Kubernetes的仿真环境中，本文提出的方案在认证时延、系统吞吐量、计算开销等关键指标上均表现良好，能够满足无人机网络对身份认证的实时性、安全性与轻量化需求，具有实际应用潜力。

表3 方案对比分析表

评估维度	传统PKI方案	单一公有链方案	本方案
认证时延	证书验证	受制于区块确认	<200ms(50节点)
通信开销	需传输证书	需同步大量交易	签名验证
隐私保护	身份信息集中暴露	交易公开但伪匿名	DID与ID分离

5 结束语

本研究提出的基于分层区块链的无人机轻量化身份认证方案，通过双层区块链结构、去中心化标识以及国产密码算法，实现了快速本域认证和低时延跨域认证，并在仿真的Hyperledger Fabric环境下完成原型实现。实验表明，方案在计算开销、时延、吞吐量以及安全性等方面均具有优势，能够满足资源受限的无人机身份认证的作业需求。未来工作将进一步探索零知识证明与边缘计算的深度研究，以提升隐私保护与系统弹性。

参考文献：

[1] Tan Y, Wang J, Liu J, et al. Blockchain-assisted distributed and light-creditation service for industrial unmanned air vehicles[J]. IEEE Internet of Things Journal, 2022, 9(18): 16928-16940.

[2] Liu B, Yu K, Feng C, et al. Cross-domain authentication for 5G-enabled UAVs: A blockchain approach[C]//Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond. New York: Association for Computing Machinery, 2021: 25-30.

[3] Du X, Tao S, Yuan K, et al. A blockchain authentication scheme for UAV-aided

fog computing[J]. Complex & Intelligent Systems, 2024, 10(2): 1689-1702.

[4] 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(07):1959-1964.
Zhang X, Zhang M, Liu T, et al. Research on cross-domain Identity Authentication of UAV Network based on blockchain[J]. Application Research of Computers, 2024,41(07):1959-1964.

[5] 高杉逸.无人机集群跨域身份认证与访问控制技术研究[D].北京:北京邮电大学,2024.
Gao S, Research on Cross-Domain Identity Authentication and Access Control Technology for Drone Swarms[D]. Beijing: Beijing University of Posts and Telecommunications,2024.

[6] Qiao G, Zhuang Y, Ye T, et al. BCDAIoD: An efficient blockchain-based cross-domain authentication scheme for Internet of Drones[J]. Drones, 2023, 7(5): 302.

[7] Zuo J, Cao R, Qi J, et al. A hierarchical blockchain-based trust measurement method for drone cluster nodes[J]. Drones, 2023, 7(10): 627.]

[8] Kong L, Chen B, Hu F. Blockchain-assisted adaptive reconfiguration method for trusted UAV network[J]. Electronics, 2022, 11(16): 2549.

[9] Jiao J, Chen B, Hu F, et al. A Lightweight and Dynamic Authentication Scheme Based on Blockchain and aSVC for UAV Swarm[J]. Drones, 2025, 9 (9): 654.

[10] Han P, Sui A, Wu J. Identity management and authentication of a UAV swarm based on a blockchain[J]. Applied Sciences, 2022, 12(20): 10524.

[11] 向宴颉,宿雅萍,刘贺,等.基于区块链的飞行数据共享模型研究[J].无线互联科技,2025,22(05):67-70.
Xiang Y, Su Y, Liu H, et al. Research on flight data sharing model based on blockchain[J]. Wireless Internet Technology, 2025,22(05):67-70.

[12] 祁志荣,吕世民,郑乾坤.基于国密算法的ModbusTCP协议安全防护与研究[J].信息安全研究,2024,10(01):20-24.
Qi Z, Lv S, Zheng Q, et al. Security Protection and Research of ModbusTCP Protocol Based on National Secret Algorithm[J]. Journal of Information Security Research, 2024,10(01):20-24.

[13] Hafeez S, Cheng R, Mohjazi L, et al. Blockchain-enhanced uav networks for post-disaster communication: A decentralized flocking approach[J]. arXiv preprint arXiv:2403.04796, 2024.

[14] Xie M, Chang Z, Li H, et al. Basuv: A blockchain-enabled uav authentication scheme for internet of vehicles[J]. IEEE Transactions on Information Forensics and Security, 2024.

[15] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on information theory, 2003, 29(2): 198-208.

[16] 肖楚乔,刘竹森,倪雄,等.基于微服务架构的区块链体系与应用范式研究[J/OL].大数据,1-18[2026-05-21].
Xiao C, Liu Z, Ni X, et al. Research on Blockchain Systems and Application Paradigms Based on Microservice Architecture[J/OL]. Big Data Research, 1-18[2026-05-21].

[17] Zhang L. A Cross Network Identity Authentication Scheme for UAVs Based on Layered Blockchain Technology[C]//International Conference on Intelligent Networking and Collaborative Systems. Cham: Springer Nature Switzerland, Cham: Spring, 2024: 131-141.

[18] Dunphy P, Petitcolas F A P. A first look at identity management schemes on the blockchain[J]. IEEE security & privacy, 2018, 16(4): 20-29.

[19] 全国信息安全标准化技术委员会(SAC/TC 260).信息安全技术 SM2椭圆曲线公钥密码算法 第1部分:总则:GB/T 32918.1-2016[S].中国标准出版社,2016.
China National Information Technology Standardization Network(SAC/TC 260). Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves Part 1: General: GB/T 32918.1-2016[S]. Standards Press of China, 2016.

[20] 全国信息安全标准化技术委员会(SAC/TC 260).信息安全技术 SM4分组密码算法:GB/T 32907-2016[S].中国标准出版社,2016.
China National Information Technology Standardization Network(SAC/TC 260). Information security technology-SM4 block cipher algorithm: GB/T 32907-2016 [S]. Standards Press of China, 2016.

[21] 李铭堃,马利民,王佳慧,等.基于区块链和PKI的身份认证技术研究[J].信息安全研究,2024,10(2):148-155
Li M, Ma L, Wang J, et al. Research on Identity Authentication Technology Based on BlockChain and PKI [J]. Journal of Information Security Research, 2024,10(2):148-155.

[22] Chen C L, Yang J, Tsaur W J, et al. Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application[J]. Sensors, 2022, 22(3): 1146.

李扬(通讯作者)(1989–)，男，硕士，国网思极位置服务有限公司，高级工程师，研究方向：区块链，无人机飞行监管

陈浩男，男，博士，工程师，研究方向：地理信息系统、电力北斗

胡全贵，男，高级工程师，研究方向：电网数字化规划与顶层设计、中台技术和电网时空技术应用

于莉莉，女，硕士，中级工程师，研究方向：地理信息系统

赵光俊：男，本科，高级工程师，研究方向：3S（GIS GNSS RS）。

收稿日期: 2026-04-08
通信作者:
基金项目: 国网信息通信产业集团有限公司科技项目资助(546821230010000K0000000)
Foundation Items: