基于双链区块链的空天地融合车载网络安全认证方案

朱思峰[1]，李卓[1]，张青华[2]，张宗辉[1]，郝志鹏[1]，鲍磊[1]，乔蕊[3]，陈国强[4]，许蒙蒙[5]，朱海[5]
（1.天津城建大学计算机与信息工程学院，天津 300384；2.天津城建大学图书馆，天津 300384；
3.周口师范学院计算机学院，河南 周口 466001；4.河南大学计算机与信息工程学院，河南 开封 475000；
5.河南工程学院计算机学院，河南 郑州 451191）

摘　要：针对空天地融合车载网络面临动态拓扑变化、信任传递困难与隐私泄露等多重挑战，提出了一种基于双链区块链的无证书跨域认证机制，构建了空间认证链与地面认证链的异构解耦模型。针对车辆节点的高移动性，采用椭圆曲线无证书签名实现了匿名可追溯，为无人机群组集成了PUF硬件绑定的轻量群认证。面向卫星周期性拓扑引入门限秘密共享算法构建了分布式认证框架，降低了跨域通信时延。实验分析表明，所提方案在计算时延和通信消耗方面较其他方案表现出显著优势，可满足实际应用需求。

关键词：空天地融合车载网络；车联网；无证书认证；双链协同
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025151

Secure authentication scheme for space-air-ground integrated vehicular networks based on dual-chain blockchain

ZHU Sifeng[1], LI Zhuo[1], ZHANG Qinghua[2], ZHANG Zonghui[1], HAO Zhipeng[1], BAO Lei[1], QIAO Rui[3], CHEN Guoqiang[4], XU Mengmeng[5], ZHU Hai[5]
1. School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China
2. Library, Tianjin Chengjian University, Tianjin 300384, China
3. School of Computer, Zhoukou Normal University, Zhoukou 466001, China
4. School of Computer and Information Engineering, Henan University, Kaifeng 475000, China
5. School of Computer, Henan University of Engineering, Zhengzhou 451191, China

Abstract: Aiming at multiple challenges such as dynamic topology changes, difficulties in trust transmission, and privacy leakage faced by the space-air-ground integrated vehicular network, a certificate-free cross-domain authentication mechanism based on a dual-chain blockchain was proposed, establishing a heterogeneous decoupling model of the spatial chain and terrestrial chain. For the high mobility of vehicle nodes, elliptic curve-based certificate-free signatures were employed to achieve anonymity and traceability, a lightweight group authentication for UAV groups was integrated with PUF hardware binding. For the periodic topology of satellites, a threshold secret sharing algorithm was introduced to construct a distributed authentication framework, reducing cross-domain communication latency. Experimental analysis shows that the proposed scheme exhibits significant advantages in computational delay and communication consumption compared to other schemes, and meets the practical application requirements.

Keywords: space-air-ground integrated vehicular network, IoV, certificateless authentication, double-chain collaboration

收稿日期：2025–06–17；**修回日期：**2025–08–13
通信作者：郝志鹏，hzpqina@163.com
基金项目：国家自然科学基金资助项目（No.62172457）；天津市自然科学基金重点资助项目（No.22JCZDJC00600）；河南省高校科技创新人才支持计划基金资助项目（No.23HASTIT029）；河南省科技攻关基金资助项目（No.242102210027）
Foundation Items: The National Natural Science Foundation of China (No.62172457), Tianjin Natural Science Foundation Project (No.22JCZDJC00600), Henan Science and Technology Innovation Talent Project (No.23HASTIT029), The Key Science and Technology Program of Henan Province (No.242102210027)

0　引言

近年来，空天地一体化网络（SAGIN, space-air-ground integrated network）作为一种融合卫星节点（SN, satellite node）、无人机（UAV, unmanned aerial vehicle）和车载单元（OBU, on-board unit）的异构通信架构，已成为车联网（IoV, Internet of vehicles）、边缘计算及灾害应急通信等多个关键应用的重要基础设施[1]。空天地融合车载网络（SAGVN, space-air-ground integrated vehicular network）是针对IoV的特殊应用场景而设计的网络架构，它在SAGIN的基础上进一步优化，以满足OBU对低时延、高可靠性和动态资源调度的需求。通过协同空、天、地通信节点，SAGVN在高速移动环境中实现无缝覆盖和高效通信，可为未来的智能交通系统提供可靠的网络支撑。伴随5G-V2X技术的突破与星地融合技术的发展，车载网络的覆盖范围与数据传输速率实现显著提升[2]。然而，空天地融合场景中的安全认证体系面临前所未有的挑战。

首先，在SAGVN多信任域协同的跨域认证环境中，OBU在高速移动过程中，需从地面通信域（由路侧单元（RSU, roadside unit）提供服务）无缝切换至空中或空间通信域（由UAV或SN提供服务），这是实现广域连续覆盖的必然需求。其核心挑战在于如何在不同信任域间高效传递信任，并避免认证时延对系统性能造成负面影响。具体而言，地面、空中与空间域通常由不同管理实体运营，彼此间缺乏直接信任锚点，导致传统的中心化公钥基础设施（PKI, public key infrastructure）难以适用。由于各个域的管理和认证机制存在差异，跨域认证的复杂度进一步提升。此外，现有研究多聚焦单一网络层安全，缺乏跨域异构节点（如SN、OBU和UAV）身份互认的全局设计，由此引发信任孤岛、隐私泄露及共识机制低效等问题[3]。这种局限性使现有方案无法满足车联网毫秒级实时性的要求，尤其是在大规模节点快速切换和高频次认证的场景下，认证时延成为制约系统性能的关键因素。因此，设计兼具跨域信任传递安全性与实时性的低时延认证机制，是该场景的核心技术难题。

其次，在多层级节点的异构验证场景中，SAGVN认证系统需应对计算能力差异显著的实体。对于无人机群组，当UAV编队需集体接入网络时，传统“一机一证”的认证模式将产生巨额开销，且UAV易被物理捕获，其存储密钥存在泄露风险。对于卫星节点，单颗SN无法作为绝对信任锚，需依赖分布式共识，但星间链路的高时延与拓扑的周期性变化，使传统共识机制效率低下。对于OBU节点，在高速移动过程中与多个RSU进行快速切换时，频繁执行完整认证流程将引发严重服务中断。这些特性对身份认证机制的安全性、实时性与可扩展性提出了严苛要求[4]。

OBU位置信息的泄露风险可导致高精度轨迹重构，而恶意UAV攻击又需快速溯源追责。SAGVN的广域覆盖特性加剧了此类问题，攻击者可通过关联不同域的认证记录，长期追踪车辆轨迹。在隐私敏感环境下的匿名认证场景中，现有动态假名机制在开放卫星信道中易受证书伪造攻击，传统群签名方案则因计算复杂度难以满足空天地融合环境下对实时性和高效性的迫切需求[5]。因此，需要构建一种跨域凭证生命周期管理机制，以消除重复签发造成的身份关联风险，从而在高动态拓扑与异构信任边界条件下，达成隐私保障与可追责性的协同一致。

应急通信中的快速认证是SAGVN面临的又一重大挑战。在突发灾难或紧急情况下，系统需在极短的时间内完成节点的身份认证，并建立可靠的通信链路。由于应急环境下的资源有限、网络拓扑变化迅速等特点，认证系统必须具备快速部署、快速认证和自适应调整的能力。此外，高动态拓扑和资源受限的环境对认证系统的要求更加苛刻，现有方案在动态拓扑、资源受限的应急环境下，难以兼顾认证速度与安全性。因此，如何在资源受限和高动态拓扑的应急环境下快速完成身份认证，并确保认证信息的安全性和可靠性，成为应急通信认证方案中的关键问题。

面对上述SAGVN中多域协同、隐私敏感、异构验证与应急响应等复杂场景带来的系统性挑战，现有研究虽在特定方向取得进展，但其架构设计仍难以全面适配SAGVN的融合特性与安全需求。其中，针对异构网络环境中的身份认证问题，已有多项研究在理论和技术层面取得了重要进展。Ren等[6]提出的星地认证方案虽通过XOR操作实现了会话密钥动态更新，但其依赖单一信任实体的中心化架构在多信任域环境下需要额外的跨域身份映射表同步过程，导致认证消息交互轮次增加，且无法支

持卫星域、地面车载域与无人机域的并行认证需求。此外，Xiong等[7]设计的基于联盟区块链的跨星座认证方案虽通过双身份机制保护卫星隐私，但无法适配OBU高速移动与UAV群组动态变化特性，缺乏节点差异化认证机制，难以满足车联网时延约束。在进一步探索身份认证机制时，Guo等[8]针对卫星–地面集成网络的多用户接入认证问题提出了N3PA-STIN三方互认证协议，通过批量验证机制降低计算开销，并采用基于中国余数定理的域密钥更新机制支持动态节点管理。但集中式架构未适配卫星拓扑周期性变化，导致跨域时延增加。并且缺乏OBU动态假名更新机制，密钥更新策略在高频跨域场景下易引发身份关联风险，难以平衡车联网隐私保护与可追溯性需求。Zhang等[9]结合匿名凭证与区块链提出了双链分阶段认证协议，通过选择性属性聚合实现了用户身份的匿名认证。然而，在SAGVN高频跨域切换时，未考虑OBU移动性导致的信任域频繁变更特性，其重认证机制仍需执行完整的双线性对验证操作，造成认证时延显著增加。Yang等[10]提出了终端分组管理与切换前认证机制，基于中国余数定理预配置认证信息。该机制依赖静态拓扑假设，在SAGVN高动态拓扑变化场景下，预配置认证信息无法及时更新，可能导致跨域信任链断裂。

区块链技术作为去中心化的分布式账本技术，凭借不可篡改、可追溯及智能合约等特性，在构建可信安全机制方面潜力巨大[11]。自2008年比特币诞生以来，区块链技术从加密货币领域拓展至多领域，其去中心化结构规避了传统认证体系的单点故障，智能合约为身份认证提供技术支撑[12]。本质上，区块链通过去中心化信任机构，实现了信任的分布式验证和自动执行[13]。针对IoV认证中的区块链应用，已有学者展开相关研究。Singh等[14]提出了基于区块链的轻量级认证协议，利用去中心化特性提高节点间的安全性和传输效率，但其时间戳验证机制未考虑星地链路高时延特性，在卫星轨道切换过程中易产生时间同步失效导致的认证失败。Ma等[15]针对IoV依赖大量RSU导致的同步难题，采用优化实用拜占庭容错（PBFT, practical Byzantine fault tolerance）算法将认证信息上链，提升传输效率并减少时延，但该模型未区分OBU、UAV与SN等多层级异构节点的安全需求，难以在保障隐私的同时满足不同实体的差异化认证要求。Xie等[16]通过优化智能合约操作来减少认证过程中的计算和通信成本。但在SAGVN环境中缺乏跨信任域凭证协调能力，难以有效处理卫星节点周期性拓扑变动引发的状态同步问题。Feng等[17]利用哈希与异或操作简化OBU与RSU认证，无法适应SN与UAV节点高时延通信和拓扑频繁变化导致的跨域认证时延累积问题。He等[18]针对IoV中节点动态变化的问题，采用权益授权证明（DPoS, delegated proof of stake）共识机制提升了交易确认速度。然而在密钥分发阶段强制要求2轮认证和密钥交换协议，显著增加了通信开销，难以满足SAGVN中高移动性节点在应急通信场景下的毫秒级认证时延要求。针对无证书签名机制也有许多研究[19-20]，然而它们都存在时延较大的问题。推动区块链技术与SAGVN的深度融合，是实现IoV安全高效发展的必然趋势。

综上所述，现有认证方案难以有效应对SAGVN在多信任域协同、隐私敏感环境、多层级节点异构及应急通信场景中的系统性挑战。因此选用空间认证链（SC, spatial chain）与地面认证链（TC, terrestrial chain）的双链架构，可以有效优化不同层次节点的认证过程。本文基于双链驱动的无证书跨域认证架构，提出了卫星链–车际链异构解耦模型，通过SC实现SN的门限秘密共享分布式认证，依托TC完成OBU无证书匿名签名与哈希绑定的身份锚定，同时为UAV群组设计物理不可克隆功能（PUF, physical unclonable function）集成的动态群组认证机制。该机制通过双链协同实现星地认证凭证的可信分发与跨域验证，构建了面向空天地3层实体的分层异构认证体系，有效解决了动态拓扑下跨域信任传递与资源受限设备的高效认证难题。通过这一系列创新性的认证机制，本文构建了一个高效、可扩展且兼具安全性的SAGVN认证方案。

本文的主要贡献总结如下。

1) 设计了一种基于卫星链和车际链的异构解耦双链认证架构，通过将SAGVN中的卫星网络与地面车载网络独立解耦，实现了星地协同身份锚定。该架构适配SAGVN动态拓扑特性，提升异构实体认证效率，可灵活应对节点频繁变化等挑战，尤其在OBU、UAV与SN协同认证中，显著增强认证的可扩展性与实时性，满足空天地融合网络的复杂认证需求。

2) 针对不同实体的特点，分别为OBU、UAV和SN设计了定制化的认证方案。OBU采用了无证书加密技术降低认证时延；UAV通过群组认证与PUF硬件绑定增强动态环境下的效率与安全性；SN利用门限秘密共享提升隐私保护。此外，多因素认证机制能够有效增强系统安全性，保障身份不可否认性、抗重放攻击能力和前向/后向安全。

3) 引入区块链令牌机制实现跨域认证高效管理，利用其不可篡改性与分布式存储保障令牌安全完整，为跨域认证奠定可靠基础。通过TC存储OBU/UAV的区块链证书哈希值，SC记录SN阈值签名令牌，依托分布式账本实现凭证防篡改托管与全网可验证。经过形式化博弈论规约证明、非形式化分析以及实验验证，充分证明了本文方案在满足SAGVN的安全需求方面的有效性，同时具有较低的计算和通信开销，进一步提升了方案的可行性与高效性。

1　系统模型与安全需求

1.1　系统模型

在SAGVN中，异构节点的动态接入与跨域协同对安全认证机制的可信性、隐私性及可扩展性提出了严格的技术要求。本文提出的SAGVN系统认证模型如图1所示。

SAGVN系统认证模型包含6类核心实体。首先是可信机构（TA, trusted authority），由密钥生成中心（KGC, key generation center）和追踪机构（TRA, trace authority）组成。其次是地面基站（GBS, ground base station）、RSU、OBU、SN和UAV节点。

1) TA。作为系统最高信任实体，TA主要负责为系统提供全局可信性。TA包含2个核心模块：KGC和TRA。KGC生成并安全分发私钥至OBU、UAV和SN，确保私钥安全；TRA则通过多因素认证机制为OBU节点分配匿名身份标识符，确保身份的隐私保护。TA的角色确保了空天地网络中各类节点的高效认证与安全性，同时其全局密钥管理功能也增强了系统的抗攻击能力。

2) RSU。作为半可信实体，RSU主要负责地面OBU和空中UAV与网络的认证交互。RSU部署于IoV关键位置，负责与附近OBU进行身份验证，并提供认证凭证。每个RSU节点可与TC进行交

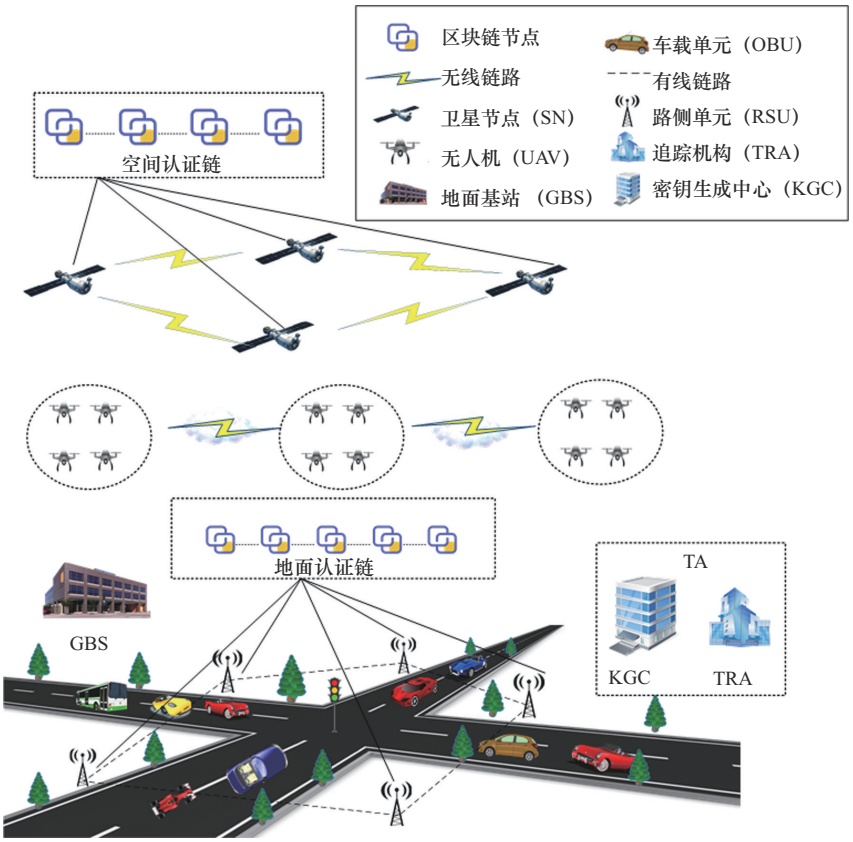

图1　SAGVN系统认证模型

互，处理区域OBU的身份验证请求。

3) GBS。作为UAV认证的完全可信实体，专门为UAV提供认证与密钥管理服务。GBS确保UAV节点在空天地融合网络中的身份认证和数据传输的安全性。GBS的主要职责是为UAV生成并管理长期私钥，同时支持与其他网络节点的跨域认证。

4) OBU。作为车载核心认证单元，主要职责在于处理车辆与地面网络以及RSU间的认证交互。OBU通过KGC下发的私钥，与其他实体进行安全的身份认证。OBU节点在身份认证过程中通过匿名身份标识符参与认证，并将其行为数据通过哈希上链至TC，从而保证了车辆身份的隐私安全及认证过程的高效性。

5) SN。SN主要构成空天地网络中的SC。特指低轨卫星（LEO, low earth orbit satellite）节点，这些SN通过专门的认证机制参与空天地融合网络的跨域认证。SN的主要功能是为地面节点（如OBU和UAV）提供跨域认证支持，确保认证过程的一致性与可靠性。由于SN轨道高度较高，星地链路传播时延显著增加，本文方案通过改进的认证机制，确保了星地协同认证的高效性。

6) UAV。UAV是空天地融合网络中的关键动态节点，负责与地面节点（如OBU和RSU）以及其他UAV的认证交互。UAV节点采用群组认证机制，通过动态身份绑定应对编队拓扑变化。群组认证机制能够有效减少频繁的密钥协商，提升认证效率。为降低能耗，UAV采用轻量级椭圆曲线Diffie-Hellman（ECDH）密钥协商协议生成会话密钥，从而确保了在高动态环境下的高效性与安全性。

在双链架构中，SC和TC各自承担不同的任务，确保SAGVN认证过程的高效性、安全性与可靠性。其中，SC负责卫星域认证事务，其数据结构采用轻量级默克尔前缀树，用于存储256位固定长度的跨域令牌哈希值，叶子节点为Leaf (BCert$_{\text{hash}}\|T_{\text{expire}}$)，其中$T_{\text{expire}}$为令牌有效期。并通过哈希链式连接确保数据的不可篡改性。每个区块均包含区块头（含时间戳、前哈希指针和共识签名）、交易列表和状态根。TC则服务于地面与空中动态节点，采用动态可扩展键值库作为数据结构，存储< PubK, Bert$_{\text{hash}}$, T_{Bert} >三元组，其中PubK是节点公钥，Bert$_{\text{hash}}$是跨域令牌哈希值，T_{Bert}是令牌有效期。数据类型是对称交互模式，支持高频双向读写，处理令牌验证与撤销事务。SC和TC均采用PBFT共识机制适配星载与车载设备的资源约束。PBFT可容忍最多$\frac{1}{3}$的恶意或失效节点，适用于对安全性要求较高的SAGVN认证场景。

此外，在SN与UAV节点稀疏、网络时延较高的场景中，PBFT的性能可能受到制约：其多阶段消息传递机制会因高时延加剧共识耗时、因节点动态变化降低适应性并影响消息可靠性。因此，可采用基于链式投票机制的HotStuff共识算法。HotStuff采用线性链式结构与连续共识机制，有效增强了在节点稀疏及拓扑动态变化场景下的适应性与可扩展性。相较于PBFT，HotStuff不仅能提供相同水平的安全性和容错能力，还能减少消息轮次和优化带宽消耗，显著提升了系统在高时延、不稳定环境下的性能表现。

1.2 安全需求

为确保SAGVN的通信安全，认证机制必须满足多个关键的安全属性，以确保通信的安全性、隐私性和可靠性。因此，本文方案需要满足以下关键安全性目标，从而确保系统整体的安全与可靠运行。

1) 签名不可链接性。要求攻击者无法通过分析不同时间点或上下文中的多个签名关联同一实体的真实身份。SAGVN环境需确保每次认证生成的签名与节点真实身份无直接关联，采用匿名身份标识符和临时密钥，使每次签名独立且无法通过后续行为关联至同一节点，从而保证节点在频繁跨域通信中的身份隐私不被泄露，避免攻击者通过签名轨迹追踪其运动路径或行为模式。

2) 密钥托管弹性。在SAGVN系统中，当私钥或密钥管理中心（如KGC）遭遇攻击时，能够保证密钥的安全性，并防止对系统安全造成严重影响。采取分散式的密钥生成和管理方式，不依赖单一的密钥托管中心。通过混合型密钥生成机制（如结合用户本地密钥和中心化生成的密钥）来确保即使中心密钥泄露，用户的密钥信息也能得到保护。

3) 抵抗恶意节点联盟攻击。要求系统能够抵御多个恶意节点的协同攻击，确保即使存在恶意节点的联合攻击行为，系统仍能保证认证机制的安全性。在SAGVN环境中，由于SN分布范围广且跨域协作频繁，单一节点的可信度易受复杂环境干

扰，采用门限签名构造认证令牌，确保认证过程的决策不依赖单一节点。即使多个节点联合进行攻击，只有在达到一定的门限条件时，认证才会通过，从而有效防止恶意节点联盟攻击对认证系统的破坏。

4) 认证状态的一致性。要求系统中所有节点对某一节点的认证状态保持一致，以防止出现认证状态不一致导致的安全漏洞。SAGVN 中节点在空、天、地三域切换时，其认证状态全局实时同步且无冲突。区块链技术确保所有节点在认证过程中获取到的认证凭证一致。通过共识机制，确保节点间的信息同步，避免某些节点因认证状态不一致而发生潜在的安全问题。

5) 身份隐私保护。要求节点的真实身份在认证过程中不被泄露，从而防止节点的位置信息、行为模式等敏感数据被泄露或滥用。在 SAGVN 中，网络覆盖空天地多域且节点移动性强，身份信息一旦暴露易导致轨迹追踪、行为预测等安全风险，需通过融合匿名身份标识符与加密技术，确保节点身份信息在传输与认证环节均不被公开或泄露。

除关键安全性目标外，SAGVN 认证系统需满足基础安全属性以实现全面防护。其中，需抵御的常见攻击包括重放攻击（重复发送已截获的有效消息以伪造通信）、篡改攻击（非法修改传输消息的内容或参数）、克隆攻击（复制合法节点身份信息以冒充参与通信）等。同时，消息认证需确保接收方能够验证消息发送者的身份合法性及消息原始性，防止伪造身份发送虚假信息。可追溯性要求在安全事件发生时，能通过审计机制追踪恶意行为的发起主体。数据完整性需保证传输或存储的认证消息被未授权篡改，确保接收内容与发送内容的一致性。上述需求确保系统在面临各种安全威胁时的稳定性与高效性，提供了应对 SAGVN 环境变化的强大安全能力。

2　认证方案流程

针对 SAGVN 中的安全认证需求，本文方案包含 4 个关键阶段，分别为系统初始化阶段、注册验证阶段、接入认证阶段和动态切换阶段。

在系统初始化阶段，系统安全参数将由可信方配置和初始化，以确保后续各阶段能够顺利进行。注册验证阶段确保各节点（如 OBU、UAV 和 SN）身份的真实性与隐私安全，为后续的安全认证和信息交换奠定基础。接入认证阶段通过首次认证确保节点与网络的安全连接，并生成跨域认证令牌，保证后续网络切换的无缝衔接。最后，在动态切换阶段，通过有效的密钥协商和认证令牌管理，确保网络切换过程的安全性和高效性。本文方案涉及的符号参数及其含义如表 1 所示。

表 1　　符号参数及其含义

符号参数	含义	符号参数	含义
σ	消息签名	RID_*	真实身份
s_*	系统私钥	PID_*	匿名身份
P_{pub}	系统公钥	PubK_*	实体公钥
$H(*)$	碰撞函数	PriK_*	实体私钥
T_*	时间戳	BCert_*	令牌凭证

2.1　系统初始化阶段

在系统安全参数配置中，本文方案采用 CL-PKC 无证书签名机制，并基于 BN（Barreto-Naehrig）曲线族实现椭圆曲线密码体制。通过密钥分离机制，即由可信机构生成部分私钥，同时用户自主选择秘密值，有效平衡了 SAGVN 系统的动态性、安全性与效率需求：一方面规避传统 PKI 的证书管理瓶颈，避免机构遭受攻击的单点故障问题；另一方面消除 ID-based 模型的密钥托管风险，适应卫星节点分布式认证场景。BN 曲线族提供 256 位等效安全强度，能在有效支持大规模节点认证和快速密钥生成过程的同时，显著优化资源受限设备的计算效率。

系统输入安全参数 λ，由信任方 TA 生成 BN 曲线族参数：生成一个素数 q，设 F_p 是 P 上的有限域，其中，$P = 36t^4 + 36t^3 + 24t^2 + 6t + 1$，$t = 2^{62} + 2^{55} + 1$。$P$ 表示有限域的大小，q 表示循环群的素数阶，且满足 $q = P + 1 - t$，t 为曲线迹。首先定义椭圆曲线 G：$y^2 = x^3 + m$，m 为曲线参数。选定基点 $(a,b) \in F_p$，Z_q^* 是 q 阶整数群。然后选择一个随机数 $s_{\mathrm{KGC}} \in Z_q^*$ 作为 KGC 的私钥。并计算 $P_{\mathrm{pub}}^{\mathrm{KGC}} = Ps_{\mathrm{KGC}}$ 作为 KGC 的公钥。选取随机数 $\alpha \in Z_q^*$ 为 TRA 的私钥，计算 TRA 对应公钥 $P_{\mathrm{pub}}^{\mathrm{TAR}} = \alpha P$。GBS 选择 $s_{\mathrm{GBS}} \in Z_q^*$ 为其私钥，计算 $P_{\mathrm{pub}}^{\mathrm{GBS}} = Ps_{\mathrm{GBS}}$ 为 GBS 对应公钥。同时 TA 定义碰撞哈希函数 H_0: $G \to Z_q^*$，H_1: $\{0,1\}^* \times G \to Z_q^*$，$H_2$: $\{0,1\}^* \times G \times G \times$

$\{0,1\}^* \to Z_q^*$，H_3: $\{0,1\}^* \to Z_q^*$。因此，系统公共参数为 $\mathrm{sp} = \left\{q, G, P, P_{\mathrm{pub}}^{\mathrm{KGC}}, P_{\mathrm{pub}}^{\mathrm{TAR}}, P_{\mathrm{pub}}^{\mathrm{GBS}}, H^*(\cdot)\right\}$，将公共参数通过安全信道分发至各实体层中预存，系统本地秘密保存私钥 $\mathrm{sk} = \left\{s_{\mathrm{KGC}}, \alpha, s_{\mathrm{GBS}}\right\}$。

2.2 注册验证阶段

在注册验证阶段，RSU、OBU、UAV 和 SN 等实体节点需提前通过可信机构获取匿名身份，同时完成身份注册。该过程确保节点的身份真实性与隐私安全，为后续的安全认证和信息交换奠定基础。

1) RSU 注册。RSU 向 TA 注册时提供必要的注册信息，包括真实身份标识 $\mathrm{RID}_{\mathrm{RSU}}$ 和其他相关信息，TA 接收验证后，TRA 存储 RSU 真实身份 $\left\{\mathrm{RID}_{\mathrm{RSU}} \| \text{其他}\right\}$，其中 ‖ 表示连接符号。KGC 随机选择 $\mathrm{PriK}_{\mathrm{RSU}}$ 作为 RSU 的私钥，并计算 $\mathrm{PubK}_{\mathrm{RSU}} = P\mathrm{PriK}_{\mathrm{RSU}}$ 作为 RSU 的公钥。TA 将公共参数 sp 发送到 RSU 中预存，同时 RSU 将 $\mathrm{PubK}_{\mathrm{RSU}}$ 上传至 TC 中保存。

2) OBU 注册。当 OBU 首次进入空地信号域时，需完成身份信息注册，用户输入身份标识信息 uid，车载装置同步采集用户的指纹信息 fp 与语音信息 vp，共同构成 OBU 的真实身份信息集合 $\mathrm{RID}_{\mathrm{OBU}} = \left\{\mathrm{uid}, \mathrm{fp}, \mathrm{vp}\right\}$。随后，OBU 选取随机数 κ，根据式(1)完成 OBU 的匿名身份计算。

$$\begin{aligned} \mathrm{PID}_1 &= \kappa P \\ \mathrm{PID}_2 &= \mathrm{RID}_{\mathrm{OBU}} \oplus H_0(\kappa P_{\mathrm{pub}}^{\mathrm{TAR}} \| \mathrm{VT}) \end{aligned} \tag{1}$$

其中，VT 为 OBU 匿名身份的有效期，由此，OBU 的假名表示为 $\mathrm{PID} = \left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{VT}\right)$，该假名有效期为单次使用，且需在指定时段后及时更新，以保障身份匿名性与安全性。

匿名身份获取后生成局部私钥。KGC 接收 TRA 提交的匿名身份 PID，选取随机数 $\alpha \in Z_q^*$，根据式(2)计算 OBU 的部分私钥。

$$\begin{aligned} A &= \alpha P \\ B &= H_3(A \| \mathrm{PID}) \\ \mathrm{PriK}_{\mathrm{OBU}}^1 &= (\alpha + Bs_{\mathrm{KGC}}) \bmod q \end{aligned} \tag{2}$$

KGC 将 $\left\{\mathrm{PID}, \mathrm{PriK}_{\mathrm{OBU}}^1, A\right\}$ 通过安全传输信道发送给 OBU，OBU 接收后，通过式(3)检查 $\mathrm{PriK}_{\mathrm{OBU}}^1 P = A + BP_{\mathrm{pub}}^{\mathrm{KGC}}$ 是否成立验证局部私钥的有效性。若式(3)成立，则将 $\left\{\mathrm{PID}, \mathrm{PriK}_{\mathrm{OBU}}^1, A\right\}$ 存储在 OBU 中；否则返回错误信息，终止注册流程。

$$\begin{aligned} \mathrm{PriK}_{\mathrm{OBU}}^1 P &= P(Bs_{\mathrm{KGC}} + \alpha) \\ \mathrm{PriK}_{\mathrm{OBU}}^1 P &= BPs_{\mathrm{KGC}} + \alpha P \\ \mathrm{PriK}_{\mathrm{OBU}}^1 P &= A + BP_{\mathrm{pub}}^{\mathrm{KGC}} \end{aligned} \tag{3}$$

获取局部私钥后，OBU 选取随机秘密值 $x \in Z_q^*$，并根据式(4)计算其完整私钥和公钥。

$$\begin{aligned} \mathrm{PriK}_{\mathrm{OBU}}^2 &= x\mathrm{PriK}_{\mathrm{OBU}}^1 \\ \mathrm{PubK}_{\mathrm{OBU}}^1 &= xG \\ \mathrm{PubK}_{\mathrm{OBU}}^2 &= \mathrm{PriK}_{\mathrm{OBU}}^2 P \end{aligned} \tag{4}$$

经上述流程，OBU 的公钥对最终确定为 $< \mathrm{PubK}_{\mathrm{OBU}}^1, \mathrm{PubK}_{\mathrm{OBU}}^2 >$，私钥对最终确定为 $< \mathrm{PriK}_{\mathrm{OBU}}^1, \mathrm{PriK}_{\mathrm{OBU}}^2 >$，完成密钥对的构建。

3) UAV 注册。当 UAV 发起注册时，首先选定自身唯一身份标识 $\mathrm{RID}_{\mathrm{UAV}}$，并向 GBS 发送注册请求。GBS 作为注册流程的核心处理节点，首先计算 UAV 的匿名身份，即 $\mathrm{PID}_{\mathrm{UAV}} = H_1\left(\mathrm{RID}_{\mathrm{UAV}} \| T_U\right)$（其中 T_U 表示匿名身份的有效期，用于保障身份新鲜性）。完成匿名身份生成后，GBS 对 UAV 身份合法性进行校验，校验通过后为 UAV 生成长期私钥 $\mathrm{PriK}_{\mathrm{UAV}}$，并基于椭圆曲线密码体制计算关联公钥 $\mathrm{PubK}_{\mathrm{UAV}} = \mathrm{PriK}_{\mathrm{UAV}} P$。为增强通信的安全性与灵活性，GBS 选取随机数 $x \in Z_q^*$ 作为 UAV 临时私钥并同步计算 $X = xP$ 为临时公钥。GBS 计算 $y = x + s_{\mathrm{GBS}} H_3(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}})$ 作为 UAV 的注册凭证。完成上述计算后，GBS 记录当前时间戳 T，并将注册响应包 $\left\{y, \mathrm{PriK}_{\mathrm{UAV}}, \mathrm{PubK}_{\mathrm{UAV}}, X, T\right\}$ 通过安全传输信道发送至 UAV。在 UAV 收到信息后，需执行合法性校验以确保数据完整性与来源可靠性。具体而言，UAV 首先根据式(5)验证 $yP = X + P_{\mathrm{pub}}^{\mathrm{GBS}} H_3(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}})$ 是否成立，若验证失败，UAV 丢弃接收信息以规避安全风险；若验证通过，则保留有效数据，进入后续安全协商流程。

$$\begin{aligned} yP &= P(x + s_{\mathrm{GBS}} H_3(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}})) \\ yP &= xP + Ps_{\mathrm{GBS}} H_3(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}}) \\ yP &= X + P_{\mathrm{pub}}^{\mathrm{GBS}} H_3(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}}) \end{aligned} \tag{5}$$

为了增强 UAV 动态群组环境下的认证效率和安全性，本文方案选择环形振荡器（RO, ring oscillator）型 PUF 作为 UAV 生成响应值的机制。RO 型 PUF 基于环形振荡器的物理特性，通过测量其启动时制造过程微小差异导致的随机时延生成唯一响应值，即使同型号设备，启动时延也存在差异。相较于静态随机存取存储器型（SRAM, static random access memory）PUF，其在 UAV 群组认证中优势

显著：一方面，稳定性更高，响应值与RO启动时延紧密相关，受环境变化影响较小，能为高动态UAV群组提供稳定可靠的响应，而SRAM型PUF因依赖SRAM单元启动状态，易受环境干扰导致响应不稳定；另一方面，硬件成本更低且易于集成，其设计简单可直接利用现有硬件资源，不需要复杂SRAM模块及额外存储单元，更适配UAV等资源受限设备，同时能增强认证可靠性以适应设备老化与环境变化。

在UAV节点启动时，首先加载其唯一身份序列号，RO型PUF响应值由UAV的内部环形振荡器自动激活生成并在本地存储。为防止环境干扰，生成的RO型PUF响应值与随机种子seed结合使用。seed在UAV节点内部生成并存储，并在每次认证时与UAV生成的PUF响应值进行组合。此时，UAV生成挑战值 C_{UAV}，并借助PUF计算响应值 $R_{\mathrm{UAV}} = \mathrm{PUF}(C_{\mathrm{UAV}}) \oplus \mathrm{seed}$。在每次认证时，UAV内部将当前生成的响应值 R^{*}_{UAV} 与存储的上一轮响应值 R_{UAV} 进行本地比对，使认证过程更加简洁和高效。同时，通过保存多个响应值并与最新值比对的冗余设计，可在部分响应值因环境或硬件问题失效时，借助备份值完成认证，从而提升可靠性。上述响应机制及认证过程如图2所示。然后UAV再通过哈希与异或运算构造隐私保护参数 $t_{\mathrm{UAV}} = H_3(R_{\mathrm{UAV}}) \oplus \mathrm{PriK}_{\mathrm{UAV}}$。最终，UAV本地存储关键注册参数 $\{\mathrm{PriK}_{\mathrm{UAV}}, t_{\mathrm{UAV}}, y, X, R_{\mathrm{UAV}}\}$，完成注册流程，为后续接入网络和参与通信建立安全基础。

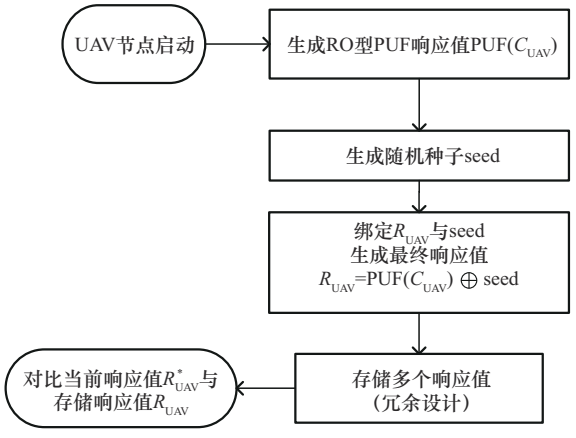

图2　RO型PUF响应机制及认证过程

4) SN注册。当SN启动注册流程时，先选择随机数 $d \in Z_q^{*}$，计算 $D = dP_{\mathrm{pub}}^{\mathrm{TAR}}$，并生成匿名信息 $\mathrm{AID}_{\mathrm{SN}} = \mathrm{RID}_{\mathrm{SN}} \oplus H_3(dP_{\mathrm{pub}}^{\mathrm{TAR}})$，其中 $\mathrm{RID}_{\mathrm{SN}}$ 和 $\mathrm{AID}_{\mathrm{SN}}$ 分别是SN的真实身份标识和匿名化处理后的身份标识。完成身份预处理后，SN发送 $\{\mathrm{AID}_{\mathrm{SN}}, D\}$ 给TRA，TRA收到后恢复SN的真实身份 $\mathrm{RID}_{\mathrm{SN}} = H_3(D) \oplus \mathrm{AID}_{\mathrm{SN}}$，并在本地建立“真实身份–匿名身份”映射关系，用于后续身份溯源与管理。

身份映射关系建立后，KGC介入私钥生成流程。KGC选择随机数 $r \in Z_q^{*}$ 并计算 $R = rP$，生成SN对应的私钥 $\mathrm{PriK}_{\mathrm{SN}} = r + s_{\mathrm{KGC}} H_1(\mathrm{AID}_{\mathrm{SN}}, R)$。为保障私钥传输安全性，KGC对私钥进行隐私保护处理，计算 $\mathrm{tmp} = \mathrm{PriK}_{\mathrm{SN}} \oplus \mathrm{RID}_{\mathrm{SN}}$，随后将加密后的私钥参数 $\{\mathrm{tmp}, R\}$ 回传至SN。

SN接收KGC响应后，执行私钥解密与验证操作。首先计算 $\mathrm{PriK}_{\mathrm{SN}} = \mathrm{tmp} \oplus \mathrm{RID}_{\mathrm{SN}}$ 得到私钥并保存，SN可以通过式(6)校验 $\mathrm{PriK}_{\mathrm{SN}}P = R + P_{\mathrm{pub}}^{\mathrm{KGC}} H_1(\mathrm{AID}, R)$ 是否成立验证私钥的正确性。

$$\begin{aligned} \mathrm{PriK}_{\mathrm{SN}}P &= P\left(r + s_{\mathrm{KGC}} H_1(\mathrm{AID}_{\mathrm{SN}}, R)\right) \\ \mathrm{PriK}_{\mathrm{SN}}P &= rP + P\left(s_{\mathrm{KGC}} H_1(\mathrm{AID}_{\mathrm{SN}}, R)\right) \\ \mathrm{PriK}_{\mathrm{SN}}P &= R + H_1(\mathrm{AID}_{\mathrm{SN}}, R)\left(s_{\mathrm{KGC}} P\right) \\ \mathrm{PriK}_{\mathrm{SN}}P &= R + P_{\mathrm{pub}}^{\mathrm{KGC}} H_1(\mathrm{AID}_{\mathrm{SN}}, R) \end{aligned} \tag{6}$$

若式(6)成立，表明私钥生成与传输过程未出现篡改或错误，SN完成私钥存储；反之，需重新发起注册流程。

2.3　接入认证阶段

在接入认证阶段，OBU通过与空地网络及天基网络的首次交互认证，完成身份验证并生成认证令牌。该认证令牌将用于后续的跨域换网认证，确保系统在不同网络域间的安全性和无缝衔接。

1) OBU和RSU双向认证。当用户请求访问空地信息网络资源时，首先需要与邻近区域内的RSU完成双向认证。认证通过后，RSU为OBU生成并上传凭证至TC，该凭证可支撑后续跨域及跨异构网络认证场景，构建全域可信认证基础。

当OBU发起签名认证请求 M_{req} 时，基于匿名身份PID记录当前时间戳 T，然后依据式(7)计算。

$$\begin{aligned} h &= H_2(M_{\mathrm{req}} || \mathrm{PID} || \mathrm{PriK}_{\mathrm{OBU}}^{2} || T) \\ \Gamma &= (\mathrm{PriK}_{\mathrm{OBU}}^{1} + h\mathrm{PriK}_{\mathrm{OBU}}^{2}) \bmod q \end{aligned} \tag{7}$$

以 Γ 作为签名值，OBU将消息元组 $\{A, M_{\mathrm{req}}, \mathrm{PID}, \mathrm{PubK}_{\mathrm{OBU}}^{2}, T, \Gamma\}$ 发送至邻近RSU或其他OBU。

邻近RSU接收到OBU消息后，首先通过记录当前时间戳 T_N 来验证消息的新鲜性，若 $T - T_N >$

ΔT（ΔT为系统允许的最大传输时延），则判定消息超时并返回时延告警；反之，执行深度验证：计算 $B = H_3(A \| \mathrm{PID})$ 和 $h = H_2(M_{\mathrm{req}} || \mathrm{PID} || \mathrm{PriK}^2_{\mathrm{OBU}} || \Gamma)$，由式(8)验证 $\Gamma P = A + BP^{\mathrm{KGC}}_{\mathrm{pub}} + h\mathrm{PubK}^2_{\mathrm{OBU}}$ 是否成立。若成立，RSU接收该认证消息；否则，返回错误信息，终止本次入网接入流程。

$$\begin{aligned} \Gamma P &= P(\mathrm{PriK}^1_{\mathrm{OBU}} + h\mathrm{PriK}^2_{\mathrm{OBU}}) \\ \Gamma P &= (\alpha + Bs_{\mathrm{KGC}})P + Ph\mathrm{PriK}^2_{\mathrm{OBU}} \\ \Gamma P &= A + BP^{\mathrm{KGC}}_{\mathrm{pub}} + h\mathrm{PubK}^2_{\mathrm{OBU}} \end{aligned} \tag{8}$$

RSU完成对OBU的入网认证后，首先为其生成区块链证书$\mathrm{BCert}_{\mathrm{OBU}}$，计算$m_{\mathrm{OBU}} = H_3(\mathrm{BCert}_{\mathrm{OBU}})$上传至TC保存，该证书涵盖OBU完整认证信息。然后RSU生成随机数$r \in Z_q^*$，记录当前时间戳T_{RSU}，依次执行如下计算：$R = rP$，$h = H_2(\mathrm{PubK}_{\mathrm{RSU}}, R, m_{\mathrm{OBU}}, T_{\mathrm{RSU}})$，$C_1 = R \oplus P$，$C_2 = m_{\mathrm{OBU}} \oplus P$，并通过私钥运算构造签名$\sigma = r^{-1}(\mathrm{PriK}_{\mathrm{RSU}} + h)$。最终，RSU将消息包$\{C_1, C_2, \sigma, T_{\mathrm{RSU}}\}$发送至OBU。

OBU接收到RSU的认证消息后，记录当前时间T_{OBU}，若$T_{\mathrm{OBU}} - T > \Delta T$，则判定认证消息超时并返回超时告警；如果成立则接受此认证消息。若新鲜性校验通过，OBU执行反向运算，使用P分别计算$R = C_1 \oplus P$，$m_{\mathrm{OBU}} = C_2 \oplus P$获得$R$和$m_{\mathrm{OBU}}$，然后根据式(9)验证$\sigma R = \mathrm{PubK}_{\mathrm{RSU}} + hP$是否成立，若成立，OBU判定RSU可信任，存储认证令牌哈希值m_{OBU}；反之，拒绝该认证消息。

$$\begin{aligned} \sigma R &= \sigma rP \\ \sigma R &= P\left(\mathrm{PriK}_{\mathrm{RSU}} + h\right) \\ \sigma R &= \mathrm{PubK}_{\mathrm{RSU}} + hP \end{aligned} \tag{9}$$

至此，OBU和RSU完成首次双向认证，OBU获得入网许可。OBU经RSU认证后，其匿名身份信息与认证令牌同步存储于TC，为后续跨域交互提供信任凭据。当TC完成令牌合法性校验后，区块链节点将未上链的合法令牌作为交易，生成新的区块并广播至TC网络。网络节点通过PBFT共识机制达成共识后，用户成功接入空地网络，具备访问该区域内RSU资源及UAV群组资源、开展任务交互的权限。

2) UAV和RSU双向认证。UAV具备轻量化计算与存储能力，当UAV群组进入新信任域并准备与域内实体通信时，需先与范围内RSU完成认证，获取令牌区块链证书。认证通过后，UAV可凭借该令牌与域内其他实体建立安全通信，并提供服务。UAV进入认证流程前首先计算$R^*_{\mathrm{UAV}} = \mathrm{PUF}(C_{\mathrm{UAV}})$，然后与本地存储的$R_{\mathrm{UAV}}$对比是否一致，不一致则认证失败；然后恢复私钥$\mathrm{PriK}_{\mathrm{UAV}} = H_3(\mathrm{R}_{\mathrm{UAV}}) \oplus t_{\mathrm{UAV}}$。随后，UAV选取随机数$r \in Z_q^*$，生成时间戳$T_{\mathrm{UAV}}$，依次计算$R = rP$和$\alpha_{\mathrm{UAV}} = H_2(R || \mathrm{PID}_{\mathrm{UAV}} || T_{\mathrm{UAV}} || \mathrm{PubK}_{\mathrm{UAV}})$，并结合私钥与证书参数生成签名$\sigma = r + \alpha_{\mathrm{UAV}}(\mathrm{PriK}_{\mathrm{UAV}} + y)$。最终，UAV将认证消息$M_{\mathrm{UAV}} = \{\sigma, T_{\mathrm{UAV}}, R, X\}$发送给协调者UAV，协调者UAV收集范围内其他UAV的请求消息后发送给边缘服务器RSU。

一段时间后，RSU收到UAV集群发送的认证请求后，首先校验时间戳T_{UAV}的新鲜性，通过$\sum_{i=1}^{n} T_{\mathrm{RSU}} - T_{\mathrm{UAV}} < \sum_{i=1}^{n} \Delta T$判定消息新鲜性。若新鲜性校验通过，RSU计算$\sum_{i=1}^{n} \alpha = \sum_{i=1}^{n} H_3(R || \mathrm{PID}_{\mathrm{UAV}} || T_{\mathrm{UAV}} || \mathrm{PubK}_{\mathrm{UAV}})$，依据式(10)验证等式是否成立。若成立，RSU接受该范围内的UAV认证请求；反之，拒绝认证，保障域内通信安全基线。

$$\begin{aligned} & P\sum_{i=1}^{n}\sigma = P\sum_{i=1}^{n}(r + \alpha_{\mathrm{UAV}}(\mathrm{PriK}_{\mathrm{UAV}} + y)) = \\ & \sum_{i=1}^{n} R + \alpha_u \sum_{i=1}^{n} \mathrm{PubK}_{\mathrm{UAV}} + \\ & \alpha_{\mathrm{UAV}} P \sum_{i=1}^{n}(x + s_{\mathrm{GBS}} h_1(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}})) = \\ & \sum_{i=1}^{n} R + \sum_{i=1}^{n}(\mathrm{PubK}_{\mathrm{UAV}} + X + \\ & P^{\mathrm{GBS}}_{\mathrm{pub}} h\alpha_{\mathrm{UAV}}(\mathrm{PID}_{\mathrm{UAV}} \| X \| \mathrm{PubK}_{\mathrm{UAV}})) \end{aligned} \tag{10}$$

当UAV首次通过RSU认证后，RSU对UAV匿名身份进行背书，将群组序列化身份列表纳入TC。并为UAV机群生成本次认证请求的组级认证令牌$\mathrm{BCert}_{\mathrm{UAV}}$，该令牌包含群组成员列表、认证时间、数字签名等字段。通过哈希运算获得$m_{\mathrm{UAV}} = H_3(\mathrm{BCert}_{\mathrm{UAV}})$，RSU选取随机数$k \in Z_q^*$，构造双重签名消息$\sigma^{(1)}_{\mathrm{RSU}} = k\mathrm{PubK}_{\mathrm{RSU}}$，$\sigma^{(2)}_{\mathrm{RSU}} = kH_3\left(m_{\mathrm{UAV}} \| T_{\mathrm{RSU}}\right)$，其中$T_{\mathrm{RSU}}$为当前时间戳。完成签名构造后，RSU发送广播消息包$\left\{m_{\mathrm{UAV}}, \sigma^{(1)}_{\mathrm{RSU}}, \sigma^{(2)}_{\mathrm{RSU}}, T_{\mathrm{RSU}}\right\}$至UAV机群。

为了增强系统的可靠性和适应性，防止因单个

节点故障而导致整个群组认证失败，本文方案中UAV群组采用扁平化拓扑结构，且未设立固定的组长节点。在此结构下，所有UAV地位平等，均可发起或参与认证流程。同时，为进一步提升认证效率，设计临时协调者机制：当某空域内的UAV节点检测到RSU发送的广播消息包后，可主动承担协调角色。并且该协调角色仅在当前认证周期内有效，认证完成后即释放权限，以此确保系统的去中心化特性不受破坏。

当协调者UAV收到消息时，根据式(11)验证$\sigma_{\mathrm{RSU}}^{(2)}\mathrm{PubK}_{\mathrm{RSU}}=\sigma_{\mathrm{RSU}}^{(1)}H_3\left(m_{\mathrm{UAV}}\|T_{\mathrm{RSU}}\right)$是否成立。若成立，则存储令牌哈希值$m_{\mathrm{UAV}}$；反之，丢弃消息，终止认证流程。随后，协调者UAV通过轻量级组播协议NORM将m_{UAV}下发至所有群组成员。整个过程采用组签名的方式，既降低了计算和通信负载，又保证了UAV个体身份的匿名性。这种组播分发机制显著降低了认证过程中的通信开销和时延，尤其适用于高速移动和资源受限的UAV应用场景。

$$\begin{aligned}&\sigma_{\mathrm{RSU}}^{(2)}\mathrm{PubK}_{\mathrm{RSU}}=k\mathrm{PubK}_{\mathrm{RSU}}H_3\left(m_{\mathrm{UAV}}\|T_{\mathrm{RSU}}\right)\\&\sigma_{\mathrm{RSU}}^{(2)}\mathrm{PubK}_{\mathrm{RSU}}=k\mathrm{PubK}_{\mathrm{RSU}}H_3\left(m_{\mathrm{UAV}}\|T_{\mathrm{RSU}}\right)\\&\sigma_{\mathrm{RSU}}^{(2)}\mathrm{PubK}_{\mathrm{RSU}}=k\mathrm{PubK}_{\mathrm{RSU}}H_3\left(m\|T_m\right)\\&\sigma_{\mathrm{RSU}}^{(2)}\mathrm{PubK}_{\mathrm{RSU}}=\sigma_{\mathrm{RSU}}^{(1)}H_3\left(m\|T_m\right)\end{aligned}\tag{11}$$

至此，UAV与RSU完成首次双向认证。UAV经RSU认证后，其匿名身份信息与认证令牌哈希值同步存储于TC，为跨域交互提供信任支撑。此时，UAV机群成功接入空基网络，具备为范围内OBU提供服务的能力，实现空–地异构网络的协同服务拓展。

3) UAV、OBU与SN认证。在SAGVN架构中，OBU与UAV的行动轨迹具备较强随机性与不可预测性，而SN因遵循严格轨道运行，其拓扑变化呈现周期性与可预测特征。基于此特性，当地面节点接入天基网络时，切换行为具备显著规律性。为实现UAV或OBU与天基网络的高效、安全对接，引入阈值签名技术，生成卫星网络通用认证令牌，为后续跨卫星网络切换提供可信凭证支撑。

SC采用阈值签名机制发行认证令牌，设定阈值为t，初始时SC执行$\mathrm{KeyGen}\left(1^{\lambda},t,n\right)$算法，生成阈值公钥mpk及各SN的链上私钥$\mathrm{PriK}_t=\left(\mathrm{PriK}_{t1},\cdots,\mathrm{PriK}_{tn}\right)$。当OBU或UAV需接入天基网络时，向网络覆盖范围内的SN发起认证请求。SN接收请求后，按预定义流程验证节点身份。验证通过后生成BCert，包括接入该天基网络的通用令牌cred和对证书的完整性签名。随后，SN将BCert广播至SC，并触发区块链共识机制。通过PBFT共识算法链上的其他SN收到广播后，调用区块链存储的SN公钥验证cred的完整性，若认可令牌签发，以自身链上私钥PriK_{tj}对cred进行签名，生成部分签名$\{\mathrm{cred},(\mathrm{cred})_{\mathrm{PriK}_{tj}}\}$后将其发送给SN。当发起广播的SN收集到的有效签名数量$\mathrm{Number}_{\mathrm{cerd}}\geqslant t$时，使用阈值聚合算法将多节点部分签名组合为最终可验证令牌BCert，确保令牌生成过程满足门限安全要求。

完成令牌聚合后，SN选取随机数$k\in Z_q^*$计算$K=kP$，对令牌BCert签名得$\sigma=k+\mathrm{PriK}_{\mathrm{SN}}H_2\left(\mathrm{BCert},K,\mathrm{AID}_{\mathrm{SN}},T_{\mathrm{SN}}\right)$，随后发送消息$\{\mathrm{BCert},K,R,\mathrm{AID}_{\mathrm{SN}},\sigma,T_{\mathrm{SN}}\}$给申请节点。

当OBU或UAV收到消息后，首先验证时间戳T_{SN}的有效性，然后依次计算$\alpha=H_1\left(\mathrm{AID}_{\mathrm{SN}},R\right)$和$\beta=H_2\left(\mathrm{BCert},K,\mathrm{AID}_{\mathrm{SN}},T_{\mathrm{SN}}\right)$，根据式(12)判定$\sigma P=K+\beta R+\alpha\beta P_{\mathrm{pub}}^{\mathrm{KGC}}$是否成立。若成立，则判定接入认证通过，申请节点存储BCert作为天基网络访问凭证；反之，拒绝接入请求。

$$\begin{aligned}&\sigma P=P\left(k+\beta\mathrm{PriK}_{\mathrm{SN}}\right)\\&\sigma P=K+\beta rP+\alpha\beta\left(Ps_{\mathrm{KGC}}\right)\\&\sigma P=K+\beta R+\alpha\beta P_{\mathrm{pub}}^{\mathrm{KGC}}\end{aligned}\tag{12}$$

通过上述流程，天基网络与地基网络（OBU、UAV所在网络）完成安全对接，实现跨域异构网络的可信互联。经过上述认证流程，SAGVN完成入网认证。SAGVN的认证交互流程如图3所示。接入该网络覆盖范围的OBU，可依托已建立的安全信任机制，申请调用SAGVN网络资源，实现多域异构网络环境下的互联互通，为后续IoV跨域业务协同与数据交互奠定安全可信基础。

2.4　动态切换阶段

在SAGVN场景中，当OBU节点执行跨域操作或进行网络切换以访问空天地融合网络资源时，可借助入网阶段获取的身份令牌，高效实现网络连接的快速切换，达成低时延的切换效果，契合IoV对高实时性的需求。本节详细阐述了切换阶段的密钥协商机制，旨在保障跨域场景下网络协同的安全性与可靠性，为多域异构网络的平滑过渡提供支撑。

在空地网络切换阶段，当OBU需跨域使用地基网络或切换空基网络时，由于OBU首次认证阶段的匿名身份与认证信息已存储于TC，二次认证

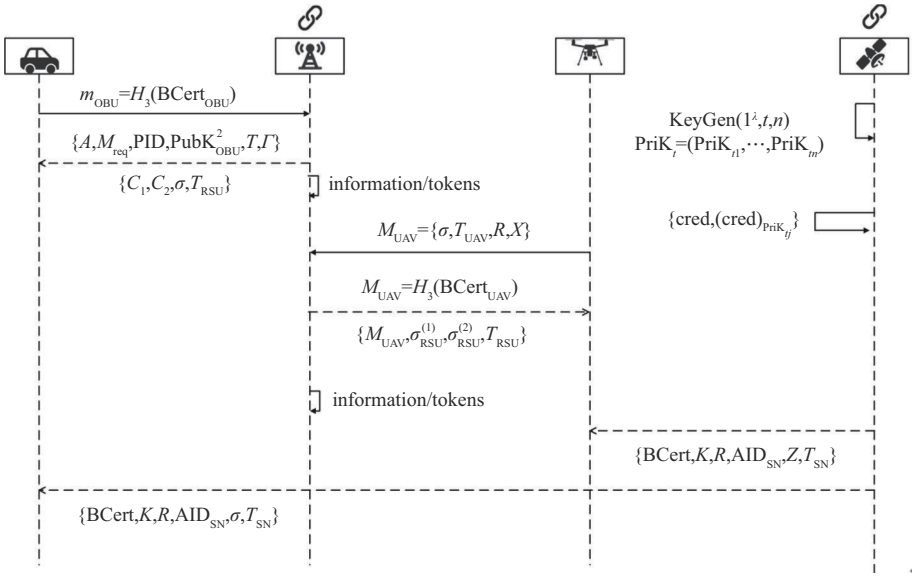

图3　SAGVN的认证交互流程

可通过轻量化交互完成。当OBU提交跨域认证请求后，RSU接受并向OBU发送随机数R_1，随后OBU对R_1生成签名$\mathrm{Sign}(R_1)$，将消息包$\{H_3(\mathrm{BCert}_{\mathrm{OBU}}),R_1,\mathrm{Sign}(R_1)\}$发送给RSU节点。

RSU收到消息后检查R_1的时效性与合法性，再通过TC查询令牌哈希值$H_3(\mathrm{BCert}_{\mathrm{OBU}})$，若查询无结果，判定认证失败并返回失败响应；若查询成功，OBU完成空地网络切换，进入会话密钥协商阶段。

在密钥协商流程中，接入空地网络的RSU按周期生成会话群提议，向范围内OBU与UAV广播会话请求并设置参与时间窗T。认证通过后，RSU生成会话密钥Ks，并用会话密钥加密随机数R_2，计算$R=\mathrm{Ks}\oplus R_2$，用OBU和UAV的公钥分别加密Ks和RSU的公钥$\mathrm{PubK}_{\mathrm{RSU}}$，然后将它们发送给范围内的OBU和UAV。

UAV和OBU收到消息后各自使用自己私钥解密获得Ks和$\mathrm{PubK}_{\mathrm{RSU}}$，同步校验$R_2$的有效性，完成对RSU的反向认证。认证通过后，OBU和UAV将获得群组会话密钥。RSU通过设置Ks的有效期，驱动域内节点周期性更新密钥，保障通信安全性与新鲜性。至此，OBU完成空地网络信号域切换，具备跨域交互能力，实现OBU-UAV跨域场景下的安全通信与资源协同。

在天基网络切换场景中，当OBU需执行SN更换操作时，OBU调用自身私钥对已获取的天基网络令牌BCert进行签名，构造认证消息M并发送至目标切换的SN。SN接收消息后，遵循天基网络认证逻辑，首先在区块链系统中查询该令牌对应的哈希值，通过哈希校验与签名验证，确认令牌的合法性与有效性。若验证通过，SN向OBU授予天基网络接入权限，完成跨域切换；若验证失败，终止切换流程并返回错误响应。

3　安全性分析

本节从形式化与非形式化2个维度对本文方案进行安全性分析，旨在验证其在抵御各类潜在攻击方面的能力，从而为构建安全可靠的SAGVN认证机制提供理论支撑与实践保障。

3.1　形式化安全性分析

本节在随机预言机模型下证明本文方案对类型I和II敌手在自适应选择消息攻击下的不可伪造性。在随机预言机模型中，哈希函数视为随机预言机，敌手仅能通过询问挑战者获取输出。其中涉及的关键符号参数及其含义如表2所示。

表2　符号参数及其含义

符号参数	含义	符号参数	含义
$\mathcal{A}_*$	敌手	$\mathcal{C}$	挑战者
H_i	哈希询问	λ	安全参数
q_i	哈希询问最大次数	$\perp$	逻辑空值
q_z	签名询问最大次数	P,Q	曲线基点
c	分支控制变量	ε	敌手优势
x	待计算私钥	L_*	查询列表

首先分析在OBU与RSU认证阶段的方案安全性。

定理1　在基于ECDLP假设和随机预言机模型下，若敌手$\mathcal{A}_1$能在概率多项式时间内，以不可忽略的优势$\varepsilon \geqslant \frac{10}{2^k}(q_z+1)(q_z+q_i)$赢得游戏1，则存在一个挑战者$\mathcal{C}$，能在概率多项式时间内，以极小的常数优势解决ECDLP困难问题。

证明　假设挑战者$\mathcal{C}$想解决ECDLP困难问题，其输入是$(P,Q{:}Q=P\mathrm{sk})$，若能计算出sk作为该问题的解，则挑战者$\mathcal{C}$可以解决ECDLP困难问题。

1) 系统初始化阶段。挑战者$\mathcal{C}$输入安全参数λ运行系统初始化算法，选取随机数$s\in Z_q^*$，计算$P_{\mathrm{pub}}=sP$。令$P_{\mathrm{pub}}\leftarrow Q$，产生系统参数$(q,G_1,P,P_{\mathrm{pub}},P_{\mathrm{pub}}^{\mathrm{TAR}},H^*(\cdot))$，其中，$q$为群$G_1$的素数阶，$P_{\mathrm{pub}},P_{\mathrm{pub}}^{\mathrm{TAR}}$为系统公钥，$H^*(\cdot)$为哈希计算。挑战者$\mathcal{C}$发送系统参数给敌手$\mathcal{A}_1$，将其中的哈希函数看成随机预言机模型。

询问阶段。$\mathcal{A}_1$可以重复进行如下询问。

2) H_2询问。挑战者$\mathcal{C}$维护列表L_{H2}，列表结构为$\{M_{\mathrm{req}},\mathrm{PID},T,h\}$且初始化为空，其中$M_{\mathrm{req}}$为认证消息请求，$T$为签名值，$h$为哈希询问值。当敌手$\mathcal{A}_1$使用元组$\langle M_{\mathrm{req}},\mathrm{PID},T\rangle$调用$H_2$询问时，如果该元组已经在列表$L_{\mathrm{H2}}$中，则挑战者$\mathcal{C}$返回$h$；否则，挑战者$\mathcal{C}$选取一个随机值$h\in Z_q^*$加入列表$\{M_{\mathrm{req}},\mathrm{PID},T,h\}$，并返回$h$给敌手$\mathcal{A}_1$。

3) 用户公钥询问。挑战者$\mathcal{C}$维护列表L_{PK}，列表结构为$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$且初始化为空。敌手$\mathcal{A}_1$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$进行询问，其中$i\in[1,q_c]$，如果该元组已经在列表$L_{\mathrm{PK}}$中，则挑战者$\mathcal{C}$返回公钥值$Y$；否则，挑战者$\mathcal{C}$随机选取随机数$a,b,c\in Z_q^*$，设置$A=aP_{\mathrm{pub}}+bP$，$B=-a \bmod q$，$\mathrm{PriK}_{\mathrm{OBU}}^2=b$，$\mathrm{PriK}_{\mathrm{OBU}}^1=bc$，$Y=cP$。验证$\mathrm{PriK}_{\mathrm{OBU}}^2P=A+BP_{\mathrm{pub}}$是否成立，如果成立则将$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$加入列表并返回$Y$给敌手$\mathcal{A}_1$。

4) 用户局部私钥询问。当敌手$\mathcal{A}_1$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$调用关于PID的局部私钥查询时，如果该元组已经在列表L_{PK}中，则挑战者$\mathcal{C}$返回局部私钥$\mathrm{PriK}_{\mathrm{OBU}}^1$给敌手$\mathcal{A}_1$。否则，挑战者$\mathcal{C}$回应⊥给敌手$\mathcal{A}_1$。

5) 用户局部私钥询问。当敌手$\mathcal{A}_1$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$调用关于PID的局部私钥查询时，如果该元组已经在列表L_{PK}中，则挑战者$\mathcal{C}$返回局部私钥$\mathrm{PriK}_{\mathrm{OBU}}^2$给敌手$\mathcal{A}_1$。否则，挑战者$\mathcal{C}$回应⊥给敌手$\mathcal{A}_1$。

6) 公钥替换询问。当敌手$\mathcal{A}_1$请求关于用户PID的公钥替换询问时，如果元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$已经在列表$L_{\mathrm{PK}}$中，则挑战者$\mathcal{C}$将公钥值$Y$替换成$Y'$，列表替换为$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^2,\mathrm{PriK}_{\mathrm{OBU}}^1,Y'\}$。

7) 签名询问。当敌手$\mathcal{A}_1$请求关于用户PID的签名询问时，挑战者$\mathcal{C}$依据式(13)抛掷偏心硬币，当$c=1$时，令$T=\perp$，返回T_i给敌手$\mathcal{A}_1$。当$c=0$时，挑战者$\mathcal{C}$随机选取$B,h,T\in Z_q^*$，计算$A=TP-BP_{\mathrm{pub}}-hY$，由此可推测出$TP=A+BP_{\mathrm{pub}}+hY$成立，则返回签名值$T$给敌手$\mathcal{A}_1$。

$$c\in\{0,1\}\left(\Pr[c=1]=\frac{1}{q_1+1},\Pr[c=0]=\frac{q_1}{q_1+1}\right) \tag{13}$$

8) 挑战阶段。进行上述询问后，敌手$\mathcal{A}_1$输出元组$\{A,M_{\mathrm{req}},\mathrm{PID},Y,T\}$，可以得到式(14)成立。

$$TP=A+BP_{\mathrm{pub}}+hY \tag{14}$$

根据分叉引理，敌手$\mathcal{A}_1$能够在多项式时间内以同样的方式伪造另一个有效元组$\{A,M_{\mathrm{req}},\mathrm{PID},Y,T^*\}$，可以得到式(15)成立。

$$T^*P=A+B^*P_{\mathrm{pub}}+hY \tag{15}$$

最后，由式(14)和式(15)得到算术推导式(16)。

$$\begin{aligned}&P(T-T^*)=TP-T^*P\\&P(T-T^*)=(BP_{\mathrm{pub}}-B^*P_{\mathrm{pub}})\\&P(T-T^*)=sP(B-B^*)\end{aligned} \tag{16}$$

计算$(T-T^*)=s(B-B^*)\bmod q$，最后挑战者$\mathcal{C}$得到参数$s=(B-B^*)^{-1}(T-T^*)$，挑战成功。

综上所述，挑战者$\mathcal{C}$可以借助敌手的能力计算出参数s的值作为ECDLP困难问题的解，利用预言机重放技术产生2个或以上密文时失败的概率可忽略，因此，挑战者$\mathcal{C}$解决ECDLP困难问题的优势为

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}(A_1)\geqslant\frac{1}{9}q_1^2q_2 \tag{17}$$

因此，在随机预言机模型和ECDLP假设下，在第一类敌手$\mathcal{A}_1$的适应性选择消息攻击、选择身份攻击以及公钥替换攻击下是不可伪造的、安全的。证毕。

定理2　在基于ECDLP假设和随机预言机模型

下，若敌手$\mathcal{A}_2$能在概率多项式时间内，以不可忽略的优势$\varepsilon \geqslant \frac{10}{2^k}(q_z+1)(q_z+q_i)$赢得游戏2，则存在一个挑战者$\mathcal{C}$，能在概率多项式时间内，以极小的常数优势解决ECDLP困难问题。

证明 假设挑战者$\mathcal{C}$想解决ECDLP困难问题，其输入是$(P,Q{:}Q=P\mathrm{sk})$，若能计算出sk作为该问题的解，则挑战者$\mathcal{C}$可以解决ECDLP困难问题。

1) 系统初始化阶段。挑战者$\mathcal{C}$输入安全参数λ运行系统初始化算法，随机选取$s\in Z_q^*$，计算$P_{\mathrm{pub}}=sP$。产生系统公共参数$(q,G_1,P,P_{\mathrm{pub}},P_{\mathrm{pub}}^{\mathrm{TAR}},H^*(\cdot))$。挑战者$\mathcal{C}$发送参数$s$和系统公共参数给敌手$\mathcal{A}_2$，将其中的哈希函数看成随机预言机模型。

2) 用户公钥询问。挑战者$\mathcal{C}$维护列表L_{PK}，列表结构为$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$且初始化为空。敌手$\mathcal{A}_2$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$进行询问，其中$i\in[1,q_c]$，如果该元组已经在列表$L_{\mathrm{PK}}$中，则挑战者$\mathcal{C}$返回$Y$，否则，挑战者$\mathcal{C}$随机选取随机数$\alpha,x^*\in Z_q^*$，设置参数$A=\alpha P$，$Q=H_1(A||\mathrm{PID})$，$\mathrm{PriK}_{\mathrm{OBU}}^1=(\alpha+Bs)\bmod q$，$\mathrm{PriK}_{\mathrm{OBU}}^2=\perp$，$Y=x^*P_{\mathrm{pub}}$。验证$\mathrm{PriK}_{\mathrm{OBU}}^2P=A+BP_{\mathrm{pub}}$成立后，将$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$加入列表并返回$Y$给敌手$\mathcal{A}_2$。

3) 用户局部私钥询问。当敌手$\mathcal{A}_2$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$调用关于PID的局部私钥查询时，如果该元组已经在列表L_{PK}中，则挑战者$\mathcal{C}$返回局部私钥$\mathrm{PriK}_{\mathrm{OBU}}^1$给敌手$\mathcal{A}_2$。否则，挑战者$\mathcal{C}$回应$\perp$给敌手$\mathcal{A}_2$。

4) 用户局部私钥询问。当敌手$\mathcal{A}_2$使用元组$\{\mathrm{PID},\mathrm{PriK}_{\mathrm{OBU}}^1,\mathrm{PriK}_{\mathrm{OBU}}^2,Y\}$调用关于PID的局部私钥查询时，如果该元组已经在列表L_{PK}中，则挑战者$\mathcal{C}$返回局部私钥$\mathrm{PriK}_{\mathrm{OBU}}^2$给敌手$\mathcal{A}_2$。否则，挑战者$\mathcal{C}$回应$\perp$给敌手$\mathcal{A}_2$。

5) 签名询问。当敌手$\mathcal{A}_2$请求关于用户PID的签名询问时，此时，挑战者$\mathcal{C}$根据式(13)抛掷偏心硬币，当$c=1$时，令签名值$T=\perp$，返回T给敌手$\mathcal{A}_2$。当$c=0$时，挑战者$\mathcal{C}$随机选取$B,h,T\in Z_q^*$，计算$A=TP-BP_{\mathrm{pub}}-hY$，由此可推测出$TP=A+BP_{\mathrm{pub}}+hY$成立，则返回签名$T$给敌手$\mathcal{A}_2$。

6) 挑战阶段。进行上述询问后敌手$\mathcal{A}_2$输出元组$\{A,M_{\mathrm{req}},\mathrm{PID},Y,T\}$并得到式(18)成立。

$$TP=A+BP_{\mathrm{pub}}+hY \tag{18}$$

根据分叉引理，敌手$\mathcal{A}_2$能够在多项式时间内以同样的方式伪造另一个有效元组$\{A,M_{\mathrm{req}},\mathrm{PID},Y,T^*\}$，可以得到式(19)成立。

$$T^*P=A+B^*P_{\mathrm{pub}}+hY \tag{19}$$

最后合并得到式(20)。

$$\begin{aligned}P(T-T^*)&=TP-T^*P\\P(T-T^*)&=(hY-h^*Y)\\P(T-T^*)&=x^*xP(h-h^*)\end{aligned} \tag{20}$$

最后挑战者$\mathcal{C}$根据式(20)得到参数$x=(x^*(h-h^*))^{-1}(T-T^*)$，挑战成功。综上所述，挑战者$\mathcal{C}$可以借助敌手$\mathcal{A}_2$的能力计算出参数$x$的值作为ECDLP困难问题的解，利用预言机重放技术产生2个或以上密文时失败的概率可忽略，因此，挑战者$\mathcal{C}$解决ECDLP困难问题的优势为式(17)。因此，在随机预言机模型和ECDLP假设下，在第二类敌手$\mathcal{A}_2$的适应性选择消息攻击、选择身份攻击以及公钥替换攻击下是不可伪造的，该过程是安全的。证毕。

其次，分析UAV与RSU认证阶段方案的安全性。

定理3 在基于ECDLP假设和随机预言机模型下，若敌手$\mathcal{A}_3$能在概率多项式时间内，以不可忽略的优势$\varepsilon \geqslant \frac{10}{2^k}(q_z+1)(q_z+q_i)$赢得游戏1，则存在一个挑战者$\mathcal{C}$，能在概率多项式时间内，以极小的常数优势解决ECDLP困难问题。

证明 假设挑战者$\mathcal{C}$想解决ECDLP困难问题，其输入是$(P,Q{:}Q=P\mathrm{sk})$，若能计算出sk作为该问题的解，则挑战者$\mathcal{C}$可以解决ECDLP困难问题。

1) 系统初始化阶段。挑战者$\mathcal{C}$输入安全参数λ运行系统初始化算法，随机选取$s\in Z_q^*$，计算$\mathrm{PubK}_{\mathrm{UAV}}=Q=xP$，产生系统参数$(q,G_1,P,s_{\mathrm{GBS}},H^*(\cdot))$。挑战者$\mathcal{C}$发送系统参数给敌手$\mathcal{A}_3$，将其中的哈希函数看成随机预言机模型。

2) H_3询问。挑战者$\mathcal{C}$维护列表L_{H3}，列表结构为$\{R,\mathrm{PID}_{\mathrm{UAV}},\mathrm{PubK}_{\mathrm{UAV}},\alpha\}$且初始化为空。当敌手$\mathcal{A}_3$使用元组$\{R,\mathrm{PID}_{\mathrm{UAV}},\mathrm{PubK}_{\mathrm{UAV}},\alpha\}$调用$H_3$询问时，如果该元组已经在列表$L_{\mathrm{H3}}$中，则挑战者$\mathcal{C}$返回$\alpha$，否则，挑战者$\mathcal{C}$选取一个随机值$\alpha\in Z_q^*$加入列表$\{R,\mathrm{PID}_{\mathrm{UAV}},\mathrm{PubK}_{\mathrm{UAV}},\alpha\}$，并返回$\alpha$给敌手$\mathcal{A}_3$。

3) 用户公钥询问。挑战者$\mathcal{C}$维护列表L_{PK}，列表结构为$\{\mathrm{PID}_{\mathrm{UAV}},\mathrm{PriK}_{\mathrm{UAV}},\mathrm{PubK}_{\mathrm{UAV}}\}$且初始化为空，其中$\mathrm{PriK}_{\mathrm{UAV}}$表示用户私钥，$\mathrm{PubK}_{\mathrm{UAV}}$表示用

户公钥。敌手 $\mathcal{A}_3$ 使用元组 $\{\mathrm{PID_{UAV}}, \mathrm{PriK_{UAV}}, \mathrm{PubK_{UAV}}\}$ 进行询问，如果该元组已经在列表 L_{PK} 中，则挑战者 $\mathcal{C}$ 返回 $\mathrm{PubK_{UAV}}$，否则，挑战者 $\mathcal{C}$ 随机选取随机数 $r \in Z_q^*$，令 $R = rP$，计算 $y = r + s_{\mathrm{GBS}} H_3(\mathrm{PID_{UAV}} \| R \| \mathrm{PubK_{UAV}})$，验证 $yP = R + P_{\mathrm{pub}}^{\mathrm{GBS}} H_3(\mathrm{PID_{UAV}} \| R \| \mathrm{PubK_{UAV}})$ 是否成立。如果成立，则将 $\{\mathrm{PID_{UAV}}, \mathrm{PriK_{UAV}}, \mathrm{PubK_{UAV}}\}$ 加入列表并返回 $\mathrm{PubK_{UAV}}$ 给敌手 $\mathcal{A}_3$。

4) 用户私钥询问。当敌手 $\mathcal{A}_3$ 使用元组 $\{\mathrm{PID_{UAV}}, \mathrm{PriK_{UAV}}, \mathrm{PubK_{UAV}}\}$ 调用关于 $\mathrm{PID_{UAV}}$ 的局部私钥查询时，如果该元组已经在列表 L_{PK} 中，则挑战者 $\mathcal{C}$ 返回 $\mathrm{PriK_{UAV}}$ 给敌手 $\mathcal{A}_3$。否则，挑战者 $\mathcal{C}$ 回应 $\perp$ 给敌手 $\mathcal{A}_3$。

5) 公钥替换查询。当敌手 $\mathcal{A}_3$ 请求关于用户 $\mathrm{PID_{UAV}}$ 的公钥替换询问时，如果元组 $\{\mathrm{PID_{UAV}}, \mathrm{PriK_{UAV}}, \mathrm{PubK_{UAV}}\}$ 已经在列表 L_{PK} 中，则挑战者 $\mathcal{C}$ 将 $\mathrm{PubK_{UAV}}$ 替换成 $\mathrm{PubK'_{UAV}}$，列表替换为 $\{\mathrm{PID_{UAV}}, \mathrm{PriK_{UAV}}, \mathrm{PubK'_{UAV}}\}$。

6) 签名询问。当敌手 $\mathcal{A}_3$ 请求关于用户 $\mathrm{PID_{UAV}}$ 的签名询问时，挑战者 $\mathcal{C}$ 根据式(13)抛掷偏心硬币，当 $c = 1$ 时，令签名值 $\sigma = \perp$。当 $c = 0$ 时，挑战者 $\mathcal{C}$ 随机选取 $\alpha \in Z_q^*$，如果满足 $\sigma = r + \alpha(\mathrm{PriK_{UAV}} + y)$，则返回签名值 σ 给敌手 $\mathcal{A}_3$。

7) 挑战阶段。进行上述询问后挑战者 $\mathcal{C}$ 输出元组 $\{\sigma', T', R', y'\}$，根据分叉引理重复上述询问后伪造另一个有效签名 σ''，使式(21)成立。

$$\begin{aligned} \sigma' P &= R + \alpha' P(\mathrm{PriK'_{UAV}} + y') \\ \sigma'' P &= R + \alpha' P(\mathrm{PriK'_{UAV}} + y') \end{aligned} \tag{21}$$

最后合并得到式(22)。

$$P(\sigma' - \sigma'') = \alpha' P(\mathrm{PriK'_{UAV}} - \mathrm{PriK''_{UAV}}) \tag{22}$$

由于 $\mathrm{PriK'_{UAV}} \neq \mathrm{PriK''_{UAV}}$，挑战者 $\mathcal{C}$ 可以通过求解式(22)提取 $\mathrm{PriK'_{UAV}}$，进而求解 ECDLP 难题，挑战成功。因此，在随机预言机模型和 ECDLP 假设下，在敌手 $\mathcal{A}_3$ 实施适应性选择消息攻击、选择身份攻击及公钥替换攻击的场景下，具备不可伪造性，可保障安全。证毕。

OBU 和 UAV 与 SN 认证过程证明与上述证明过程类似。

3.2　非形式化安全性分析

本节将从理论角度详细分析本文方案如何满足 SAGVN 的安全需求，具体涵盖消息认证、身份隐私保护、抗攻击能力、可追溯性、不可否认性、不可链接性等安全属性，以及防御重放攻击、篡改和伪造等常见安全威胁。

1) 签名不可链接性。在 OBU 与 RSU、UAV 与 RSU、TC 与 SC 的认证过程中，本文方案引入了时间戳、一次性哈希链和动态生成的临时身份标识等机制，以确保签名值的不可预测性和非确定性。例如，在 OBU 与 RSU 认证阶段 OBU 通过匿名身份生成签名 $\Gamma = (\mathrm{PriK_{OBU}^1} + h\mathrm{PriK_{OBU}^2}) \bmod q$，在 UAV 认证阶段使用随机秘密值和临时证书生成签名 $\sigma = r + \alpha_{\mathrm{UAV}}(\mathrm{PriK_{UAV}} + y)$，SN 接入阶段则采用随机组合 $\sigma = k + \mathrm{PriK_{SN}} H_2(\mathrm{BCert}, K, \mathrm{AID_{SN}}, T_{\mathrm{SN}})$。即便同一实体对相同消息多次签名，所生成的签名值也因密钥的不同而展现出高度随机性。因此，攻击者无法通过观察签名来判断其来源，满足了异构融合网络中签名不可链接性的基本要求。

2) 前向安全性。本文方案确保各终端节点的认证消息不会因后续认证信息的泄露而受到影响，从而保障各认证阶段的独立性。例如，在 OBU 与 RSU 的认证过程中，RSU 利用随机数生成 $R = rP$，然后组合 $h = H_2(\mathrm{PubK_{RSU}}, R, m_{\mathrm{OBU}}, T_{\mathrm{RSU}})$ 生成签名 σ，虽然涉及长期私钥但每个阶段在后续跨域通信的会话密钥 K 由 RSU 随机独立生成，即使私钥被泄露，攻击者也无法推导出之前通信过程中的会话密钥。

3) 抗重放攻击。本文方案通过引入时间戳 T 来防止攻击者截获并重放历史消息进行非法访问。在每个双向认证阶段，节点接收到认证请求后，首先验证时间戳的有效性。如果时间差超过系统设定的最大可容忍时延，则返回超时信息。例如，在 UAV 接入阶段还引入不同的临时密钥和随机数 $L = \{T, B, X, \sigma\}$，SN 生成签名时还依赖于一次性椭圆线点，进一步提升了系统的抗重放攻击能力。

4) 抵御中间人或假冒攻击。攻击者虚拟出一个中间节点，插入通信双方之间，使通信双方误认为彼此在直接通信，借此实现对通信内容的窃取、篡改或伪造。本文方案在各个阶段所构建的认证基础是基于 ECDLP 问题的困难性，确保了签名的安全性和不可伪造性。即便攻击者截获了认证消息，也无法从中推导出用户的真实私钥或伪造新的有效签名，从而无法实施中间人攻击或假冒攻击。

5) 密钥托管弹性。为了防止系统中的可信机

构（如KGC、TRA）遭受恶意控制或攻击，本文方案采用混合型私钥结构，以确保终端节点的私钥信息不会被恶意机构完全获取。在本文方案中，OBU的私钥一部分由KGC生成$\mathrm{PriK}_{\mathrm{OBU}}^{1}$，另一部分本地随机选取秘密值$\mathrm{PriK}_{\mathrm{OBU}}^{2}$。即便KGC试图伪造签名，也无法获取完整的私钥成分。UAV的私钥通过PUF机制恢复，而且还引入临时私钥w。因此，各个阶段均采用了混合型私钥结构，即由可信机构生成的部分私钥与用户本地随机选取的秘密值共同构成完整的私钥。这种设计使得即使KGC掌握系统主密钥，也无法获取用户的完整私钥信息，从而无法伪造签名或冒充合法实体。

6) 消息认证。包含2个核心要素：消息完整性验证和发送者身份合法性验证。通过将认证内容嵌入哈希函数并结合基于ECDLP的签名机制实现发送者身份合法性验证。所有通信均基于之前建立的身份认证关系，会话密钥的分发也嵌入了发送方的签名信息，接收方可通过验证签名机制判断消息来源是否合法，进一步保障了消息认证属性。

7) 身份隐私保护。本文方案中各个实体节点均通过匿名身份生成机制、本地随机选取的密钥材料以及基于哈希函数的身份映射策略，实现了对用户真实身份的有效隐藏。OBU使用PID替代$\mathrm{RID}_{\mathrm{OBU}}$参与认证；UAV使用$\mathrm{PID}_{\mathrm{UAV}}$替代$\mathrm{RID}_{\mathrm{UAV}}$进行通信；SN使用$\mathrm{AID}_{\mathrm{SN}}$替代$\mathrm{RID}_{\mathrm{SN}}$接入天基网络。所有真实身份信息均未在网络中传输，仅在本地或可信机构（如TRA）内部保存。同时，系统支持匿名身份的周期性更新机制，使攻击者即便获得了某个阶段的匿名身份，也无法将其与后续阶段的身份信息相关联，从而有效防止了长期身份追踪问题。

8) 可追溯性。认证过程要确保系统中的可信管理实体能够在必要时识别并追踪到匿名通信实体的真实身份，同时又不能损害用户在正常通信过程中的身份隐私。例如，在需要追溯的情况下，TRA可通过$\mathrm{RID}_{\mathrm{OBU}}=\mathrm{PID}_2\oplus H_0(\kappa P_{\mathrm{pub}}^{\mathrm{TAR}}\|\mathrm{VT})$恢复OBU的真实身份，通过$\mathrm{RID}_{\mathrm{SN}}=\mathrm{AID}_{\mathrm{SN}}\oplus h(d)$恢复SN的身份。GBS可以通过查询本地数据库找到UAV的映射，通过引入基于随机数的匿名身份生成机制与中心化验证结构，本文方案在各认证阶段均实现了匿名性与可追溯性的平衡设计。

9) 抵抗克隆和物理攻击。该属性确保即使攻击者对通信终端进行物理接触、逆向工程或尝试复制设备信息，也无法成功伪造合法身份或获取关键安全参数，从而防止非法接入和系统入侵。在OBU注册过程中，其真实身份PID由车载装置通过生物特征（如指纹fp和语音vp）生成，并结合本地随机数κ构造匿名身份$\mathrm{PID}_1=\kappa P$和$\mathrm{PID}_2=\mathrm{RID}_{\mathrm{OBU}}\oplus H_0(\kappa P_{\mathrm{pub}}^{\mathrm{TAR}}\|\mathrm{VT})$。UAV通过引入$R_{\mathrm{UAV}}=\mathrm{PUF}(C_{\mathrm{UAV}})$，$R_{\mathrm{UAV}}$依赖于PUF的物理特性，具有唯一性和不可预测性。由于PUF响应无法被复制或模拟，攻击者即使拥有相同型号的UAV硬件，也无法获得相同的R_{UAV}。因此，本文方案在OBU、UAV及SN终端的注册、认证与密钥协商等各阶段均实现了强健的抵抗克隆和物理攻击能力。

10) 认证状态的一致性。在SAGVN环境中，所有节点对某个用户是否已认证的状态保持一致视图，防止因局部认证失败或伪造而引发的安全漏洞。例如，在SN认证阶段，SC采用阈值签名机制，只有当超过设定数量的SN对认证结果达成一致后，才允许该认证信息被写入区块链。这一机制有效防止了个别恶意节点伪造认证状态，从而保证了全网范围内认证状态的一致性与可信性。

11) 抵抗恶意节点联盟攻击。在SAGVN架构中，本文方案基于t-Threshold秘密共享算法的阈值签名机制生成认证令牌$\mathrm{BCert}=S_1\oplus S_2\oplus\cdots\oplus S_T$，其中$S_i$表示第$i$个SN生成的部分签名，$\oplus$表示对部分签名的组合操作，BCert表示完整认证令牌。恶意少数SN联盟因缺乏足够可信节点参与，无法伪造有效令牌：即使恶意联盟包含$T-1$个节点并生成相应部分签名，仍无法合成有效签名，而有效签名需至少T个节点参与以满足阈值要求。区块链共识机制进一步增强了系统安全性与抗篡改性，各节点的签名及认证令牌均记录于分布式账本且不可篡改。伪造或篡改行为会被其他节点通过共识机制识别并抵制（如令牌广播后经公开验证可发现异常）。有效抵御单节点及联盟发起的串通攻击，提升认证系统的抗攻击性与身份验证安全性。

4　仿真与性能对比分析

计算与通信开销是评估身份认证机制性能的核心指标。本节将从这2个维度与近年来发表的高安全性接入认证方案进行对比，以阐释本文方案的高效性。

4.1　基本功能对比

为了有效分析本文方案的性能，本节对本文方案与 5 篇 IoV 领域的认证文献进行了基本功能对比，对比项目如表 3 所示。文献[21]在注册阶段的计算开销较低；文献[22]在跨域通信中的时延性能表现较为优异；文献[23]在签名阶段的计算开销较小；文献[24]在验证阶段的时延较为优越；文献[25]在总开销方面表现尚可。然而，本文方案在综合性能和多维度优化方面展现出了更为均衡的优势。

表 3 展示了各个方案在不同安全属性方面的实现功能对比，其中，√表示方案满足相应安全属性，×表示方案未能满足该安全属性。文献[21]虽可覆盖多数常规安全属性，但在用户 ID 自由变更及不可链接性等功能支持上存在缺失。文献[22]在抵御重放攻击与生成会话密钥方面表现优良，却未能实现条件隐私保护，不具备有效身份追溯能力。文献[23]尽管在前向/后向安全性方面表现突出，却缺乏可追溯性、不可链接性及条件隐私保护。文献[24]虽在安全性上具备保障，但仍未涵盖用户 ID 自由变更和不可链接性等安全属性。文献[25]总体上在安全性层面取得一定突破，却未能满足用户 ID 自由变更需求。显然，本文方案在满足更多安全属性的基础上，有效弥补了上述方案的不足，可提供更为全面的安全保障。

4.2　计算开销对比分析

在 SAGVN 这一特定场景下，相较于传统物联网，因其对实时性交互、安全驾驶保障等应用的严格需求，对时延的要求更为苛刻。所以本节将把本文方案的计算开销分别与上述文献进行对比。定义 T_h 表示执行单次的哈希运算时间、T_e 表示执行加密算法时间、T_d 表示执行解密算法时间、T_s 表示签名验证算法时间、T_a 表示椭圆曲线执行点加运算时间、T_m 表示椭圆曲线执行点乘运算时间、T_{tp} 表示双线性对操作时间、T_g 表示指数运算时间。本文方案使用配置为 Windows11 操作系统，处理器采用 Intel® Core™ i9-13900K CPU @ 3.00 GHz，内存为 32 GB 的个人计算机进行。借助 Python 的密码学相关库 cryptography，对方案中的各类密码学操作进行实现。通过测试脚本对每个操作重复执行 10^6 次，精确记录相应操作的平均执行时间如表 4 所示。由于异或运算、整数加法运算和整数乘法运算消耗时间相对较短，因此本文不再考虑。

表 4　　密码学操作时间

密码学操作	运算时间/ms
T_h	0.006
T_e	0.462
T_d	1.650
T_s	1.724
T_a	1.308
T_m	2.539
T_{tp}	0.400
T_g	0.006

表 3　　功能对比

安全属性	文献[21]	文献[22]	文献[23]	文献[24]	文献[25]	本文方案
用户匿名性	√	√	√	×	√	√
双向认证	√	√	√	√	√	√
抵御重放攻击	√	√	√	√	√	√
抵御中间人攻击	√	√	√	√	√	√
抵御假冒攻击	√	√	√	√	√	√
抵御篡改攻击	√	√	√	√	√	√
抵御重放攻击	√	√	√	√	√	√
生成会话密钥	√	√	√	√	√	√
前向/后向安全性	√	√	√	×	×	√
可追溯性	√	√	×	×	√	√
用户 ID 自由变更	×	×	×	×	×	√
不可链接性	×	√	×	×	√	√
条件隐私保护	√	×	×	×	√	√

对各方案的注册阶段平均计算开销进行可视化分析，结果如图4所示。

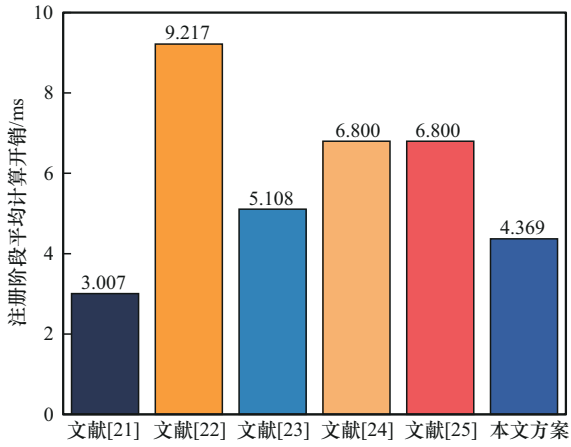

图4　注册阶段平均计算开销

相较于文献[21-25]，在注册阶段，本文方案的计算开销分别节约或多消耗（“–”表示节约，“+”表示多消耗）了+45.3%、–52.6%、–14.5%、–35.8%和–35.8%。综合来看，本文方案在注册阶段平均计算开销方面，相较于部分文献虽有增加，但对比高计算开销文献具备显著优势，整体性能表现良好。

对各方案的签名阶段平均计算开销进行可视化分析，结果如图5所示。相较于文献[21-25]，在签名阶段，本文方案的计算开销分别节约或多消耗了–51.4%、–66.6%、+5.5%、–36.7%和–58%。

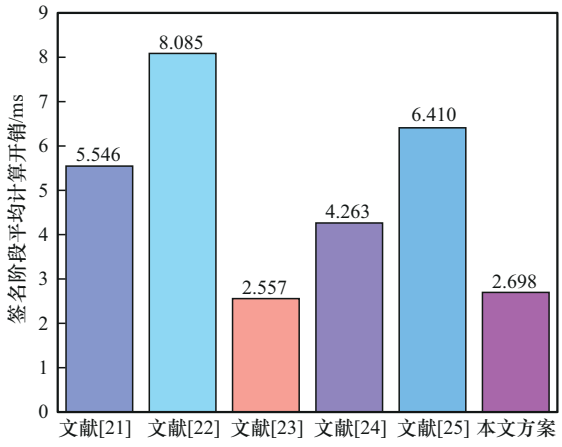

图5　签名阶段平均计算开销

综合而言，本文方案在签名阶段平均计算开销上，除对比文献[23]稍高外，相较于其他文献均展现出明显的计算开销优势，有效降低了签名过程的计算资源消耗。

对各方案的验证阶段平均计算开销进行可视化分析，结果如图6所示。相较于文献[21-25]，在验证阶段，本文方案的计算开销分别节约了–34.3%、–61.2%、–56.9%、–19.3%和–30.3%。

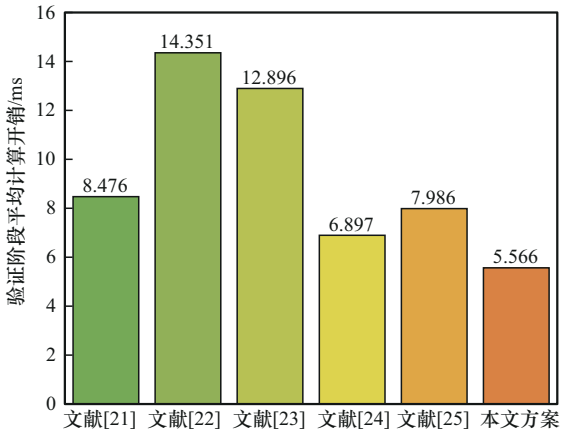

图6　验证阶段平均计算开销

整体来看，本文方案在验证阶段的计算开销显著低于多数对比文献，有效优化了验证过程的计算资源占用，能够在保障认证安全性的同时，提升系统验证效率。

对各方案跨域阶段平均计算开销进行可视化分析，结果如图7所示。相较于文献[21-25]，在跨域阶段，本文方案的计算开销分别节约了–53.3%、–55.4%、–48.8%、–38.0%和–53.6%。在跨域阶段平均计算开销上表现出显著的优化，这一优势源于区块链技术在跨域认证机制中的合理应用及对流程的优化。

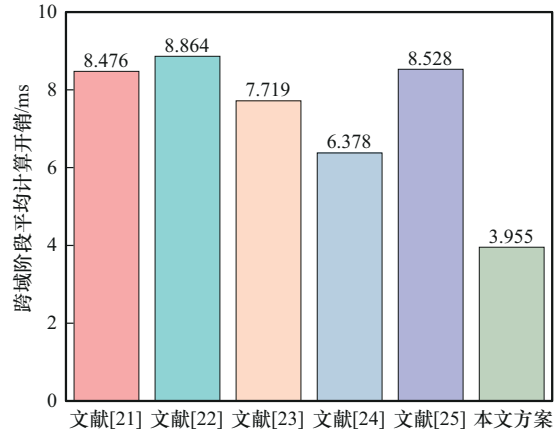

图7　跨域阶段平均计算开销

通过区块链令牌机制，结合分布式账本的不可篡改性与共识机制，本文方案实现了跨域数据的可

信交互与自主验证。相比传统中心化架构下需要多级转发和冗余校验的过程，区块链技术显著简化了跨域认证流程，减少了计算资源消耗。尤其在SAGVN的高频跨域切换场景中，区块链技术的应用有效地缩短了切换时延，提升了网络的运行效率，符合该场景对低时延和高可靠性的技术需求。

4.3　通信开销对比分析

本节分析本文方案与对比方案的通信开销。在认证密钥协商过程中，协议传输的数据量与通信开销呈正相关。为衡量不同协议的通信效率，本文对各文献在此过程中的数据传输量进行比较。对相关参数进行如下设定：协议中的时间戳$|T|$设为4 B，椭圆曲线上的点对$|G|$设置为128 B，大素数$\left|Z_q^*\right|$设置为32 B，单向散列函数$\left|H(*)\right|$设为32 B，签名长度$|\mathrm{Sig}|$设为96 B，加密密文$|\mathrm{ED}|$设为100 B。在此条件下，对本文方案中SAGVN在认证密钥协商过程中的表现展开研究。

在本文方案中，认证过程主要包括OBU与RSU的双向认证、UAV与RSU的认证以及TC与SC的跨层级认证3个核心阶段。在OBU与RSU认证阶段，双方共进行2次消息交互，涉及签名生成与验证、公钥传输及时间戳校验等操作，通信开销约为440 B（$|G|+2|\mathrm{Sig}|+2|H|+2|Z_q|+2|\mathrm{ID}|+6|T|$）。在UAV与RSU认证阶段，UAV发送认证请求，RSU返回认证响应，完成挑战–响应验证和区块链证书下发，通信开销约为208 B（$|G|+2|\mathrm{Sig}|+|H|+2|Z_q|+2|T|$）。在OBU/UAV与SN的认证过程中，地面节点向TC发起认证请求，SN通过阈值签名机制生成认证令牌并回传，完成天基网络接入，通信开销约为144 B（$|G|+2|\mathrm{Sig}|+|H|+2|T|$）。

综上，整个认证过程在SAGVN环境下，通过轻量级密码运算与区块链协同验证机制，实现了高效、安全的身份认证。不考虑注册和跨域阶段的情况下，平均端到端切换开销为264 B，平均接入认证开销为322 B，整体平均通信开销总计为966 B。在保障多层级互信与动态接入的同时，展现出较低的通信开销和良好的系统效率。

对各方案的平均接入认证开销进行可视化分析，结果如图8所示。相较于文献[21-25]，在接入阶段，本文方案的通信开销分别节约了–30.0%、–32.9%、–3.3%、–24.1%和–33.5%。综合来看，本文方案在平均接入认证开销方面，相较于对比文献展现出明显的优化效果，有效降低了接入认证过程中的数据传输量。

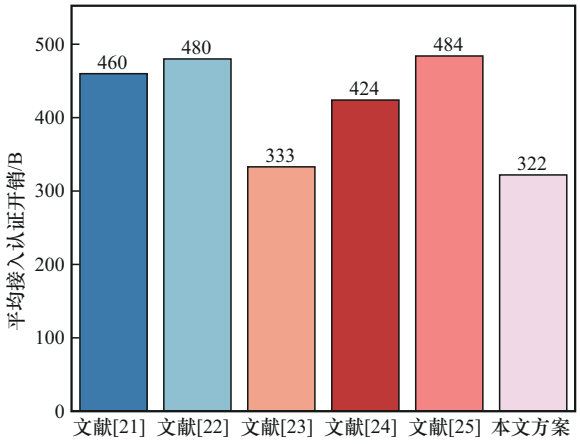

图8　平均接入认证开销

对各方案的平均切换认证开销进行可视化分析，结果如图9所示。

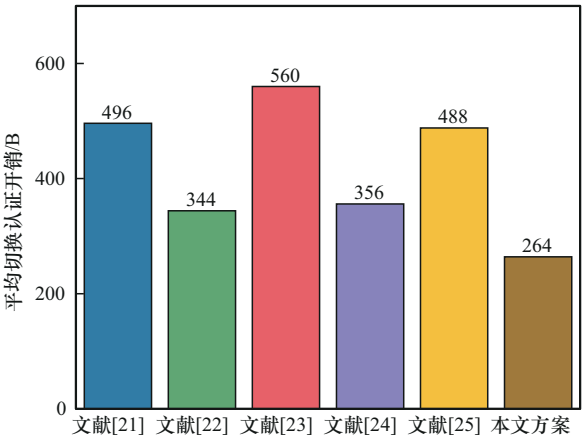

图9　平均切换认证开销

相较于文献[21-25]，在切换阶段，本文方案的通信开销分别节约了–46.8%、–23.3%、–52.9%、–25.8%和–45.9%。整体而言，本文方案在平均切换认证开销上显著优于所有对比文献，大幅降低了切换认证过程中的数据负载。采用双链结构和去中心化认证，使认证令牌可以直接由相关节点生成和验证，从而减少了不必要的数据传输和验证环节，显著减少了切换认证过程中的通信开销。

对各方案的平均总开销进行可视化分析，结果如图10所示。相较于文献[21-25]，在平均总开销方面，本文方案的平均总开销分别节约了–4.2%、–15.5%、–19.9%、–14.9%和–1.0%。综合来看，本文方案在平均总开销层面，相较于对比文献呈现

出一定的优化优势，有效控制了整个认证及交互流程的数据资源消耗。

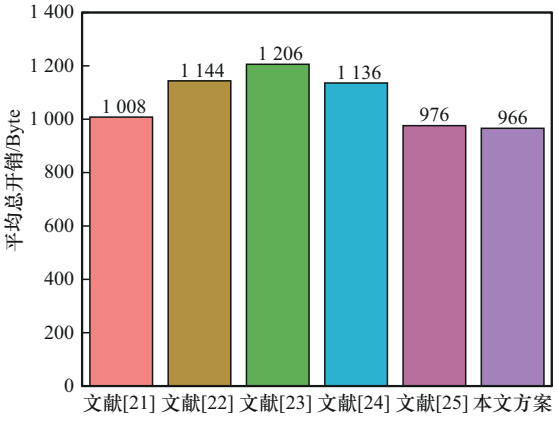

图10　平均总开销

5　结束语

本文提出了一种基于双链架构的跨域认证方案，针对SAGVN中的身份认证效率和系统鲁棒性等关键问题，创新性地设计了双链异构解耦模型，显著提升了认证效率和系统安全性。未来研究将探索区块链机制在SAGVN复杂动态环境中的创新优化方法，重点围绕共识算法与认证方案的协同改进展开。针对传统PBFT类算法在高时延、低连接度场景下的收敛效率受限与通信开销过大问题，拟引入HotStuff等具备线性通信复杂度与异步适应性的新型拜占庭容错机制，以提升稀疏或不稳定网络中的系统可用性与容错能力。同时，深化认证方案在低时延、高安全性约束下的协同设计，为SAGVN应用场景的广度拓展与深度延伸提供持续技术支撑。

参考文献：

[1] LIU J J, SHI Y P, FADLULLAH Z M, et al. Space-air-ground integrated network: a survey[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 2714-2741.

[2] CUI H X, ZHANG J, GENG Y H, et al. Space-air-ground integrated network (SAGIN) for 6G: requirements, architecture and challenges[J]. China Communications, 2022, 19(2): 90-108.

[3] ALALWANY E, MAHGOUB I. Security and trust management in the Internet of vehicles (IoV): challenges and machine learning solutions[J]. Sensors, 2024, 24(2): 368.

[4] WANG Y T, SU Z, NI J B, et al. Blockchain-empowered space-air-ground integrated networks: opportunities, challenges, and solutions[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 160-209.

[5] RANI P, SHARMA R. Intelligent transportation system performance analysis of indoor and outdoor Internet of vehicle (IoV) applications towards 5G[J]. Tsinghua Science and Technology, 2024, 29(6): 1785-1795.

[6] REN S Y, LIU J W, JI R H, et al. A secure authentication scheme for satellite-terrestrial networks[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(6): 6470-6482.

[7] XIONG T, ZHANG R, LIU J, et al. A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in space-ground integrated networks[J]. Computer Networks, 2022, 206: 108793.

[8] GUO J Y, YAO S, SONG Y, et al. N3PA-STIN: a novel three-party authentication protocol for multiuser access in satellite terrestrial integrated networks[J]. IEEE Internet of Things Journal, 2025, 12(10): 14952-14968.

[9] ZHANG Y S, ZHOU X Y, KONG J Y, et al. An anonymous credential-based efficient staged dual-chain authentication protocol for satellite-earth links[J]. Journal of King Saud University Computer and Information Sciences, 2025, 37(3): 30.

[10] YANG Y Y, CAO J, MA R H, et al. FHAP: fast handover authentication protocol for high-speed mobile terminals in 5G satellite-terrestrial-integrated networks[J]. IEEE Internet of Things Journal, 2023, 10(15): 13959-13973.

[11] BELOTTI M, BOŽIĆ N, PUJOLLE G, et al. A vademecum on blockchain technologies: when, which, and how[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3796-3838.

[12] SIBAHEE M A A, ABDULJABBAR Z A, NGUEILBAYE A, et al. Blockchain-based authentication schemes in smart environments: a systematic literature review[J]. IEEE Internet of Things Journal, 2024, 11(21): 34774-34796.

[13] CUI J, ZHU Y H, ZHONG H, et al. Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT[J]. IEEE Internet of Things Journal, 2024, 11(9): 16325-16338.

[14] SINGH A, RANI P, RAMESH J V N, et al. Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of vehicles communication[J]. IEEE Transactions on Consumer Electronics, 2024, 70(2): 4898-4907.

[15] MA Z F, JIANG J, WEI H, et al. A blockchain-based secure distributed authentication scheme for Internet of vehicles[J]. IEEE Access, 2024, 12: 81471-81482.

[16] XIE M Y, CHANG Z, LI H W, et al. BASUV: a blockchain-enabled UAV authentication scheme for Internet of vehicles[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 9055-9069.

[17] FENG X, CUI K P, WANG L M, et al. PBAG: a privacy-preserving blockchain-based authentication protocol with global-updated commitment in IoVs[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(10): 13524-13545.

[18] HE B J, LI Y. Blockchain-based key management and security decisions in Internet of vehicles[J]. IEEE Internet of Things Journal, 2025, 12(11): 17456-17472.

[19] LIN H T, JHUANG W L. Blockchain-based lightweight certificateless authenticated key agreement protocol for V2V communications in IoV[J]. IEEE Internet of Things Journal, 2024, 11(16): 27744-27759.

[20] MA M M, CHEN B W, TANG D H, et al. Certificateless searchable public key encryption with trapdoor indistinguishability for IoV[J]. IEEE Transactions on Vehicular Technology, 2025, 74(3): 5085-5096.

[21] LI L, FAN X J, ZHI B Y, et al. Highly secure authentication and key agreement protocol for the Internet of vehicles[J]. Telecommunication Systems, 2024, 87(1): 73-88.

[22] XI N, LI W H, JING L, et al. ZAMA: a ZKP-based anonymous mutual

authentication scheme for the IoV[J]. IEEE Internet of Things Journal, 2022, 9(22): 22903-22913.

[23] CHEN C M, LI Z, DAS A K, et al. Provably secure authentication scheme for fog computing-enabled intelligent social Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2024, 73(9): 13600-13610.

[24] SIBAHEE M A A, NYANGARESI V O, ABDULJABBAR Z A, et al. Two-factor privacy-preserving protocol for efficient authentication in Internet of vehicles networks[J]. IEEE Internet of Things Journal, 2024, 11(8): 14253-14266.

[25] TAN H W, ZHENG W Y, VIJAYAKUMAR P. Secure and efficient authenticated key management scheme for UAV-assisted infrastructureless IoVs[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(6): 6389-6400.

[作者简介]

朱思峰（1975– ），男，河南周口人，博士，天津城建大学教授，主要研究方向为空天地一体化网络、车联网安全、网络资源优化、多目标优化算法等。

李卓（2001– ），男，山西太原人，天津城建大学硕士生，主要研究方向为移动边缘计算、车联网安全、深度强化学习、区块链等。

张青华（1976– ），女，河南周口人，天津城建大学图书馆员，主要研究方向为图书信息处理。

张宗辉（1982– ），男，河北邢台人，天津城建大学实验师，主要研究方向为车联网、移动边缘计算、多目标优化算法等。

郝志鹏（1982– ），男，天津人，天津城建大学讲师，主要研究方向为区块链、车联网安全等。

鲍磊（1976– ），男，安徽巢湖人，天津城建大学讲师，主要研究方向为嵌入式系统、物联网、智能自动化等。

乔蕊（1982– ），女，河南周口人，博士，周口师范学院教授，主要研究方向为物联网安全、区块链、移动边缘计算。

陈国强（1977– ），男，河南开封人，博士，河南大学副教授，主要研究方向为网络优化、智能算法等。

许蒙蒙（1986– ），男，河南南阳人，博士，河南工程学院讲师，主要研究方向为车联网、资源分配、路由协议等。

朱海（1978– ），男，河南南阳人，博士，河南工程学院教授，主要研究方向为网络优化、智能算法等。