引用格式：李雪晴, 邹德财. 基于区块链的GEO/LEO卫星网络安全认证技术研究[J]. 时间频率学报, 2024, 47(3): 219-228.

基于区块链的GEO/LEO卫星网络安全认证技术研究

李雪晴[1,2,3]，邹德财[1,2,4]

1. 中国科学院 国家授时中心，西安 710600；
2. 时间基准及应用重点实验室（中国科学院），西安 710600；
3. 中国科学院大学，北京 100049；
4. 中国科学院大学 天文与空间科学学院，北京 101408

摘要：由于卫星网络高暴露、高时延的特点，不同系统星座组网进行遥控指令发布及遥测信息回传时，容易受到其他卫星恶意接入导致信息泄露。卫星网络安全认证成为天基测控实现过程中必须解决的技术问题。面向高轨和低轨双层卫星网络场景下的安全组网需求，提出了一种基于区块链的星间组网认证技术，该技术包括基于区块链的卫星身份认证和星间消息认证。研究设计将卫星临时身份登记上区块链，通过比对链上信息完成卫星的身份认证。为进一步增强消息传输安全性，采用椭圆曲线数字签名算法对星间消息进行签名验证。通过仿真分析，验证了所提技术能够以较小的时间开销满足卫星在组网认证阶段的多种安全需求。

关键词：区块链；GEO/LEO卫星网络；身份认证；消息认证；椭圆曲线数字签名算法

DOI：10.13875/j.issn.1674-0637.2024-03-0219-10

Research on blockchain-based secure authentication technology for GEO/LEO satellite network

LI Xue-qing[1,2,3], ZOU De-cai[1,2,4]

1. National Time Service Center, Chinese Academy of Sciences, Xi'an 710600, China;
2. Key Laboratory of Time Reference and Applications, Chinese Academy of Sciences, Xi'an 710600, China;
3. University of Chinese Academy of Sciences, Beijing 100049, China;
4. School of Astronomy and Space Science, University of Chinese Academy of Sciences, Beijing 101408, China

Abstract: Since the high exposure and high latency of satellite network, the issuance of telecommand and the transmission of telemetry data by different satellite constellations during networking are vulnerable to information leakage caused by malicious satellite intrusion. Satellite network security authentication has become a technical issue that must be addressed in the process of space-based telemetry, tracking and command. This study proposes a blockchain-based inter-satellite networking authentication scheme for the security networking

收稿日期：2023-05-06；接受日期：2023-06-17
基金项目：军委科技委项目

needs in a double-layer satellite network scenario of geosynchronous earth orbit(GEO) and low earth orbit(LEO), which includes satellite identity authentication and inter-satellite message authentication based on blockchain technology. The research design will register the temporary identity of the satellite on the blockchain, and complete the identity authentication of the satellite by comparing the information on the blockchain. To further improve the security of message transmission, an elliptic curve digital signature algorithm is used to verify the signature of inter-satellite messages. Through simulation analysis, it is verified that the proposed scheme can satisfy the various security requirements of the satellite in the networking authentication stage with less time.

Key words: blockchain; GEO/LEO satellite network; identity authentication; message authentication; elliptic curve digital signature algorithm

随着空间信息技术的高速发展，世界各国对于卫星网络的研究愈发重视。卫星网络具有较好的连通性和覆盖性，其不受地理环境的限制，有效延伸了地面网络的应用范围[1]，成为天地一体化信息网络中至关重要的组成部分，不断拓展了定位导航授时 PNT（positioning，navigation，timing）体系的业务范围，在遥测遥控、导航定位和灾害预警等领域发挥着不可或缺的作用。

卫星网络的开放特性，致使通信很容易被攻击者拦截或恶意接入。一旦测控信令或网管信息被窃取、篡改和伪造，卫星极易遭受非法截获和干扰，造成遥测数据泄露[2−3]，甚至导致整个星网瘫痪，给用户及卫星本身带来了严重影响。确保卫星安全组网的需求极为迫切。

卫星身份认证是节点入网的必要条件，是保障卫星网络安全组网的重要前提。针对卫星网络的身份认证技术主要分为两类：一是采用公钥、证书等技术，二是采用对称加密算法。Cruickshank 等[4]于 1996 年提出了基于公钥体制的认证技术，首次解决了双向认证的问题，极大地提高了安全性，具有开创性意义。彭岩等[5]提出了一种轻量级快速安全认证策略，在可证明安全性的前提下减少频繁切换产生的时间开销。窦志斌等[6]依托于预共享密钥体制，提出了一种适用于卫星网络的星地轻量化认证鉴权架构。石小平等[7]针对低轨卫星网络链路断续连通的问题，提出了基于对称密码体制设计的接入认证、通信恢复和卫星切换认证技术。张帅领等[8]为解决 5G 卫星网络中海量终端的匿名接入认证问题，改进了 5G-AKA 认证与密钥协商协议，提出了一种安全高效的群组匿名认证协议。然而，这些传统认证技术存在依赖可信第三方、认证过程复杂、存在安全性隐患等问题，在应用上存在一定的局限性。

区块链作为一种融合了分布式数据存储、对等网络、分布式共识机制、数据加密等多项计算机技术的新型应用模式，可以在实现去中心化数据管理的同时保证数据可追溯、不可篡改等特性，为研究星间安全组网认证提供了全新的思路。Wei 等[9]结合基于身份的加密和区块链技术，提出了一种基于身份的加密（IBE，identity based encryption）密钥的低轨道卫星（LEO，low Earth orbit）星座区块链访问验证协议，分别研究了 IBE 和区块链两种不同的密钥管理方法，这进一步提高了 LEO 星座中认证的可靠性和效率。CLARK 等[10]最先对卫星中继网络进行基于区块链的信誉系统研究，利用区块链对卫星和地面站的已知信誉数据进行维护和更新。Deng 等[11]提出了一种在 LEO 卫星网络中使用加密货币技术的基于区块链的认证协议，改善了证书管理的困难。马煜[12]基于区块链技术设计了低轨卫星分布式数字化身份加密系统，实现了星间通信网络的安全加密。Razzaq 等[13]提出了一种区块链辅助保护遥感数据的方法，减少了对可信第三方认证机构的需求。Xiong 等[14]提出了一种基于区块链的保密认证技术，用于空地综合网络中的星座间协作，引入联盟区块链用于在合作卫星星座之间共享信息，提出了一种副本存储节点方法，利用资源充足的卫星缓存通过区块链共享的复制信息。李望[15]提出了一种采用区块链技术的卫星编队组网认证设计，通过对比各加密算法的时间开销，证明了使用椭圆加密算法进行批量消息认证可以有效减少计算时延。

2022 年 7 月 25 日，欧洲通信卫星公司 Eutelsat 与英国互联网卫星制造商 OneWeb 合并，准备将 Eutelsat 的 648 颗同步轨道卫星（geo-stationary Earth orbit，GEO）与 OneWeb 的 428 颗 LEO 结合起来，开发互补的 GEO/LEO 服务，包括通用平台、混合终端和完全互联的网络，为用户创建一站式解决方案[16]。我国也正加速部署抢占频率和轨道资源的 LEO 星座，加快空天地一体化网络的建设，实现全球覆盖的卫星组网。GEO/LEO 双层卫星网络与区块链相结合实现卫星组网的安全认证在未来具有很大的发展应用空间。

本文针对 GEO/LEO 双层卫星网络间的安全组网问题，设计了一种基于区块链的卫星组网认证技术。重点关注 GEO 和 LEO 卫星之间的安全认证过程。每颗卫星都拥有保护通信隐私的临时身份，并由卫星生成私钥避免密钥泄漏。采用非形式安全分析方法论证了提出身份认证方法的安全性。同时，选择使用椭圆曲线数字签名算法（elliptic curve digital signature algorithm，ECDSA）完成星间消息认证，与 RSA（Rivest-Shamir-Adleman）算法相比 ECDSA 算法在时间性能上具有更好的效果，有利于推广和应用。

1　卫星网络技术基础

1.1　GEO/LEO 双层卫星网络模型

由于卫星遥感测控地面站分布不均，卫星的遥测遥控指令收发、密钥更新等都需要在地面站可视范围内由地面控制中心（telluric control center，TCC）进行操作，相对受限的卫星控制方式给星间组网实时管控和遥测遥控数据传输等都带来了诸多不便。为实现 TCC 对海量在轨卫星的全天候管理，以数据中继技术和分级管理方式为特征的新型卫星网络受到了国内外的广泛关注[17]。一种典型的分布式星群组网模型是建设同时包含 GEO 和 LEO 的双层卫星网络，如图 1 所示。在该网络中，GEO 卫星作为骨干网主要负责接收 TCC 发出的遥控指令、转发遥控指令给 LEO 星座进行处理、接收遥测数据回传到 TCC，管理其覆盖范围内各 LEO 星座等任务。LEO 卫星承担遥测信息收集、传输与交换等任务。TCC 是卫星任务的核心组成部分，主要负责监控、控制和管理卫星的运行。星间安全组网认证主要考虑 GEO 和 LEO 卫星。

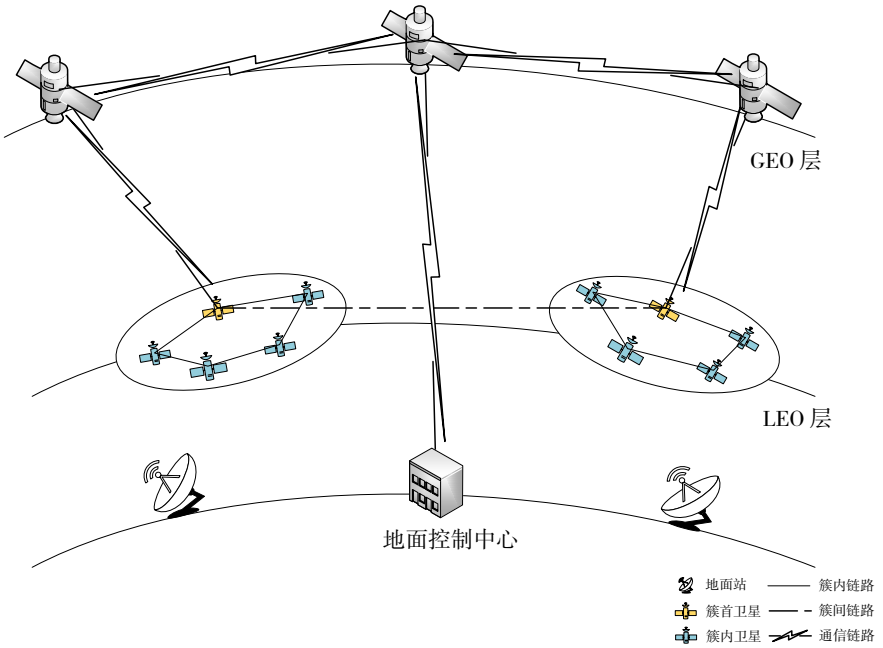


图 1　GEO/LEO 双层卫星网络架构

1.2　区块链

区块链是一个可被复制的公共数据库，能够提供可验证的、仅追加的链式数据结构来记录、存储和更新数据库。区块链的逻辑结构与数据结构如图

2 所示。在逻辑结构上，主要包含应用层、合约层、激励层、共识层、网络层和数据层[18]。在数据结构上，每个区块由区块头和区块体构成。区块头中，至少包含 5 个参数：时间戳，父区块哈希值，随机数 Nonce，目标哈希，以及 Merkle 根。其中，Merkle 根是包含所有交易记录区块体的一个哈希值。

参照图 2 框架，卫星网络安全认证主要集中在网络层和合约层，在网络层中考虑双层卫星网络结构和认证机制，在合约层利用智能合约代码处理 GEO 和 LEO 的认证。其中系统节点指卫星或地面站，分布式账本可以设计为临时身份账本、请求信息账本和注册账本等。

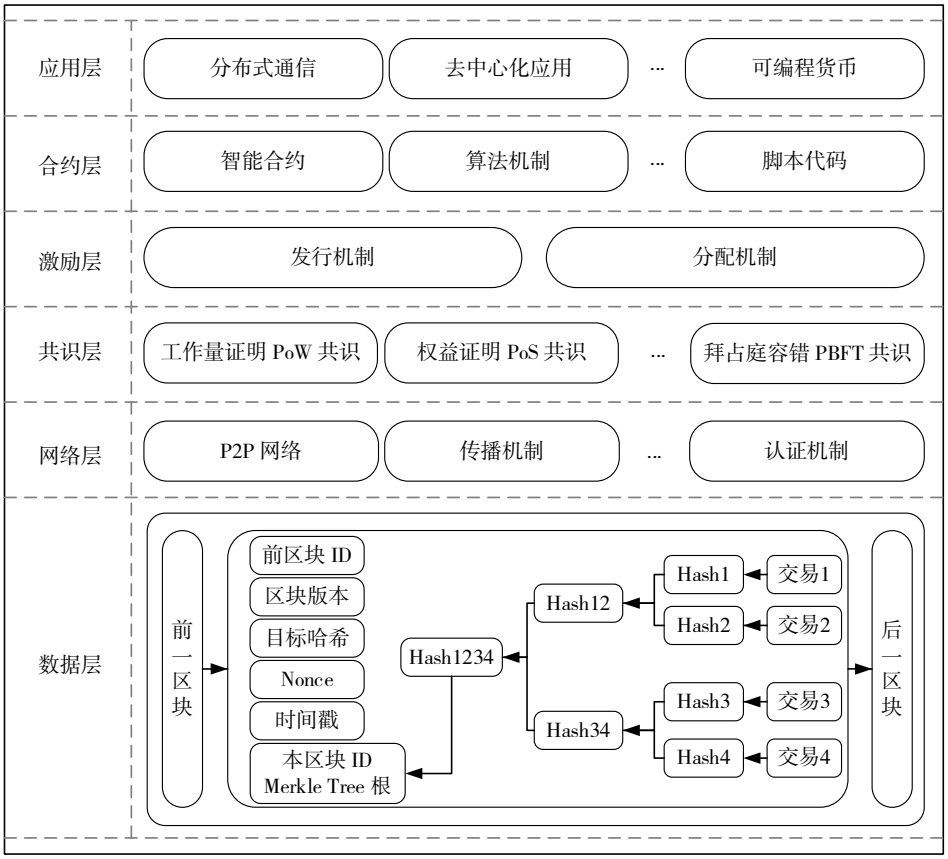


图 2 区块链的逻辑结构与数据结构

2 基于区块链的 GEO/LEO 双层卫星网络安全认证技术

为满足星间组网的安全需求，本节提出了一种基于区块链的 GEO/LEO 双层卫星网络安全认证技术，详细描述了加入区块链技术后 GEO 和 LEO 卫星间的身份认证过程，通过基于椭圆曲线数字签名算法实现了星间消息认证。

2.1 安全需求

随着卫星搭载星间链路，减少了 TCC 的参与，极大地提高了卫星组网的自主性。但由于其网络信道的高度开放，攻击者能够通过监听、重放等手段对卫星间组网进行干扰和破坏[19]。同时，卫星处理器计算能力与存储容量有限，无法负担高性能的加密和签名算法和认证协议，防护能力存在严重不足。为保证卫星通信网络的安全组网，对认证技术提出了以下安全需求。

① 匿名身份

除了地面控制中心能够知道卫星的真实身份标识外，组网过程中涉及到的卫星均无法获得卫星真实身份标识，防止攻击者通过流量分析等手段获取卫星真实身份信息，从而推断出卫星相关参数。

② 双向认证

保证进行组网连接的卫星均可相互检验对方身份，攻击者无法通过假冒卫星身份恶意接入卫星

网络[20]。

③ 抵抗重放

防止攻击者截获卫星通信网络中的消息、中断传输进程、篡改和伪造截获的消息进行重新发送攻击，干扰卫星组网认证的正常运行。认证技术需要具备检验认证消息完整性和时效性。

2.2 基于区块链的 GEO/LEO 卫星身份认证设计

在 GEO/LEO 卫星身份认证设计中，区块链上存储卫星节点的临时身份等信息，通过验证身份的合法性，证明卫星具有所声明的权限可以完成安全可信的组网。卫星身份认证过程包括 3 个阶段：系统初始化、卫星临时身份注册上链和星间安全认证。

2.2.1 系统初始化

在系统初始化阶段，建立区块链网络来保存身份认证数据，定义基本的卫星身份数据结构。TCC 在卫星发射准备阶段为每颗卫星注册真实身份（NORAD ID）、卫星通用名称（common name）、卫星来源（source）和卫星权限（authority）等信息。

2.2.2 卫星临时身份注册上链

LEO 卫星和 GEO 卫星利用自增生成隐藏真实身份的临时身份标识 TID(temporary identification)。通过 TCC 的确认，将 TID、时间戳等信息登记上区块链。区块链上的每个区块维护着所有可信卫星的身份标识。区块链系统会验证卫星身份证明的有效性，并根据卫星节点的权限来授权其执行相应的操作。

2.2.3 星间安全认证

当有卫星节点请求加入卫星网络时，合约层启动智能合约发起对卫星节点的身份认证，合约定义了卫星身份认证的规则、条件和过程。星间安全认证阶段主要包括 GEO 和 LEO 的双向认证流程，如图 3 所示。当 GEO 卫星发起组网请求，区块链验证其对应的临时身份，确认该卫星是否属于可信组网卫星。完成身份确认后区块链将该认证请求广播到卫星网络。接收方 LEO 卫星可以收到请求即认定该 GEO 卫星身份可信，通过解析该卫星的认证参数，生成当前时间戳和应答字符等传递给区块链。GEO 卫星收到认证结果完成组网认证。

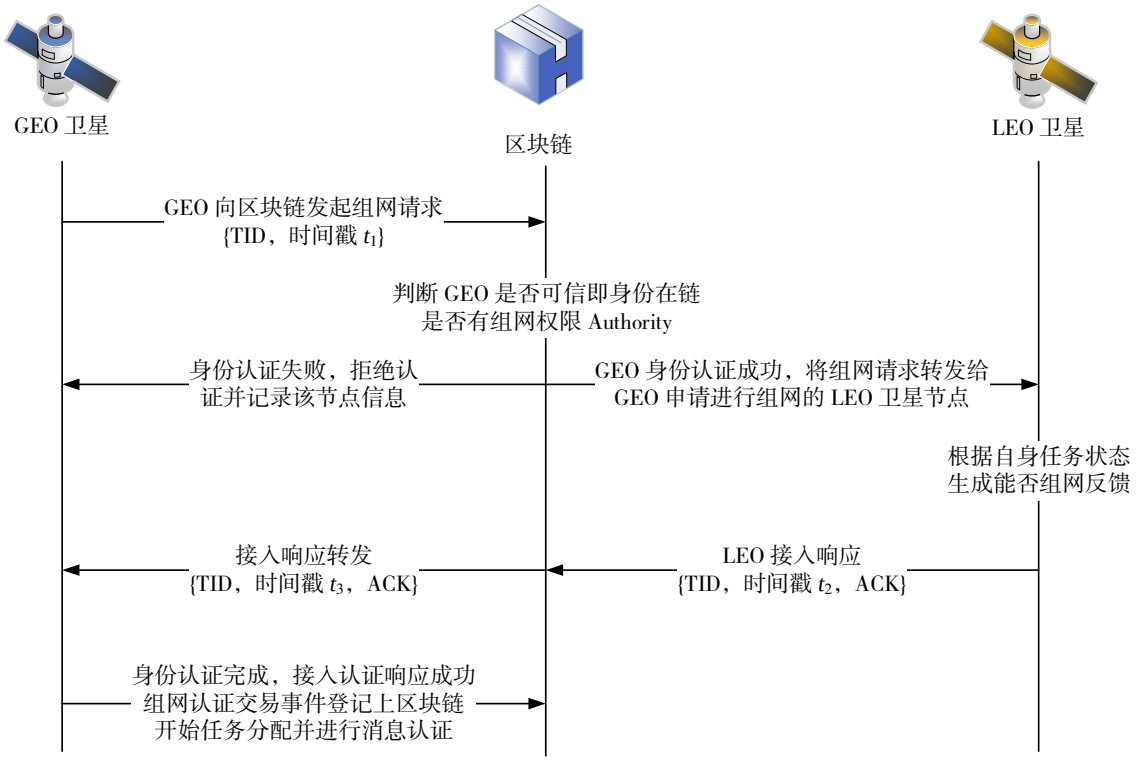


图 3　基于区块链的 GEO/LEO 双向认证流程

2.3 基于椭圆曲线数字签名算法的星间消息认证

Diffie 与 Hellman[21]在 1976 年首次提出公开密钥密码体制的概念，发明了非对称加密算法，奠定了公钥密码学的基础。与传统对称密码体制使用相同密钥进行加解密的方式不同，公钥密码体制将密钥分为对外界公开的公钥（public key）和只有所有者可知的私钥（private key）。当使用公钥对数据进行加密时，只能用对应的私钥才能进行解密。反之若用私钥对数据进行加密，则只能用对应的公钥才能解密。公钥密码体制给密钥管理带来了诸多便利，不仅可以用于加解密，还广泛应用在数字签名和身份认证等服务中。基于公钥密码的数字签名体制采用私钥生成签名，公钥验证签名。假定接收方已知发送方的公钥，发送方则可用私钥对消息的散列码进行加密产生数字签名，接收方用发送方公钥验证签名从而确认签名和消息的真实性，如图 4 所示。

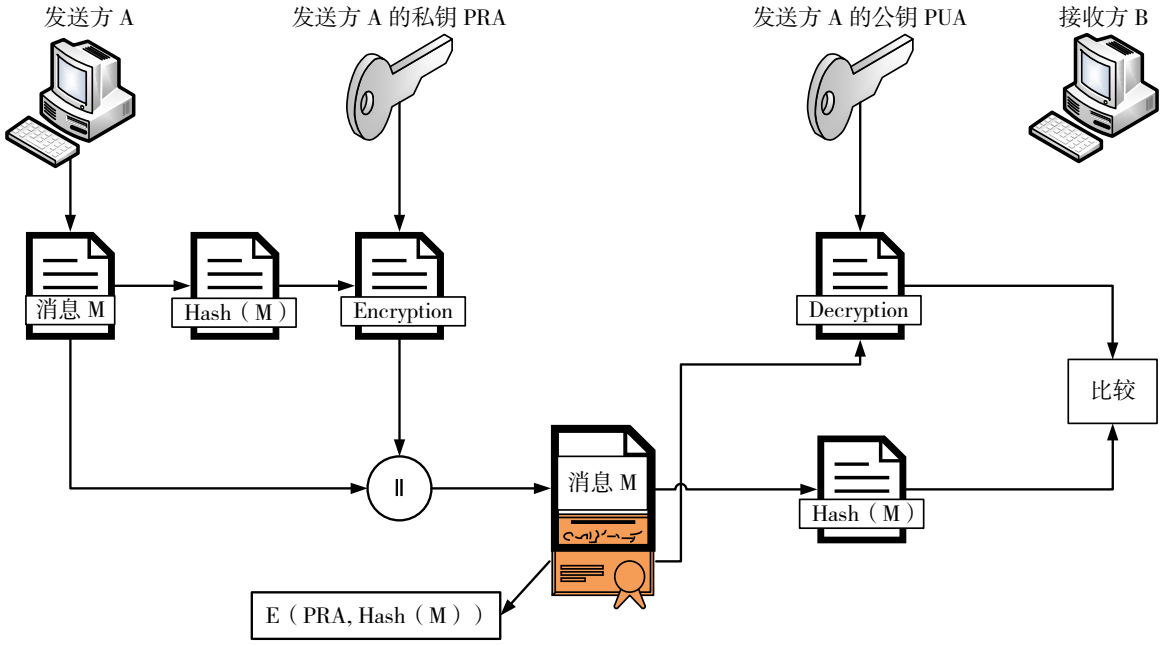


图 4 基于公钥密码体制的数字签名原理

1978 年，Rivest、Shamir 和 Adleman 3 位研究者共同发明了可用于数据加密和签名的公钥系统 RSA，首次开发出具备商业实用性的非对称 RSA 加密算法[22]。RSA 算法属于分组密码体制，其理论基础是大整数的素因子分解是困难问题。Koblitz[23]和 Mille[24]于 1985 年首次提出将椭圆曲线算法（elliptic curves cryptography，ECC）应用于密码学，并建立公钥加密的算法。ECDSA 算法的工作原理是依靠椭圆曲线上离散对数的复杂性问题。相对于 RSA 需要设置很长的密钥才能保证算法安全，ECDSA 使用的密钥长度更短，减少了计算开销和存储空间，提升了运算效率。比特币以及中国的二代身份证都使用了 256 比特的椭圆曲线密码算法。使用短密钥的优势在于加解密速度快、节省能源、节省带宽和存储空间，最重要的是适合星上处理能力有限的卫星网络环境[25]。

ECDSA 算法签名将所有通信方都使用相同的全局参数，用于定义椭圆曲线以及曲线上的基点。签名发送方首先生成一对公私钥，选择一个随机数或者伪随机数作为私钥，利用随机数和基点算出作为公钥另一点。然后对消息计算 Hash 值，用私钥、全局参数和 Hash 值生成签名。签名验证方用签名发送方的公钥、全局参数等验证。

椭圆曲线的曲线方程是以下形式的二元三次方程：

$$E: y^2 + axy + by = x^3 + cx^2 + dx + e \text{。} \qquad (1)$$

式（1）也称为 Weierstrass 方程式，它是由方程的

全体解 (x,y) 再加上一个无穷远点 O 构成的集合，其中 a，b，c，d，e 是实数，x 和 y 也在实数集上取值。但并非所有的椭圆曲线都适合加密，密码学中普遍采用有限域上的椭圆曲线。椭圆曲线密码主要将椭圆曲线定义为两类，一种是在 p 为奇素数的基础下定义的椭圆曲线，其方程表达式为式（2），也是 ECC 最常用的椭圆曲线方程。另一种为在 $\mathbb{F}_2$ 域的模定义下的椭圆曲线，其椭圆曲线又被称为非奇异椭圆曲线，其方程为式（3）。本文 ECDSA 算法选择基于 $\mathbb{F}_p$ 有限域上的 secp256k1 椭圆曲线，曲线方程为式（4）。

$$E: y^2 = x^3 + ax + b\,, \tag{2}$$

$$E: y^2 + xy = x^3 + ax^2 + b\,, \tag{3}$$

$$E: y^2 = x^3 + 7\,。 \tag{4}$$

仿真模拟 50 次签名算法，采用点对点的方式模拟星间发送，RSA 密钥选择 1 024 bit，计算分析 ECDSA 算法和 RSA 算法的时间开销。因仅做算法间比较，暂未考虑卫星传输时延。图 5 为 ECDSA 算法与 RSA 算法在生成密钥阶段消耗时间，ECDSA 算法明显优于 RSA 算法，时间稳定在 1 ms，RSA 算法生成密钥时间最高 319.56 ms。

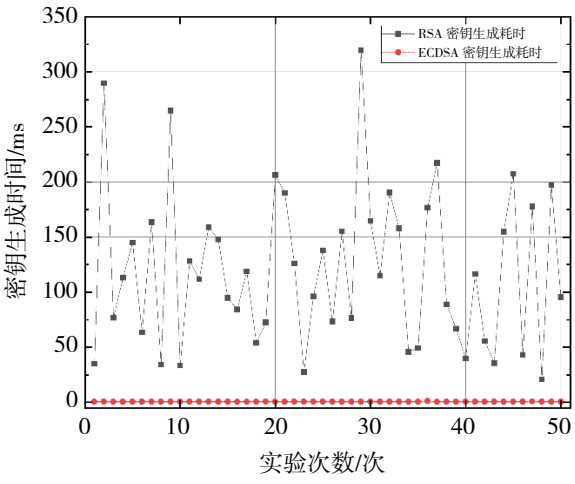
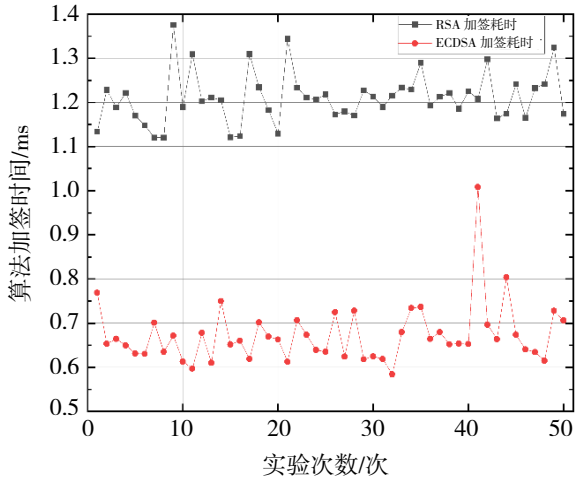
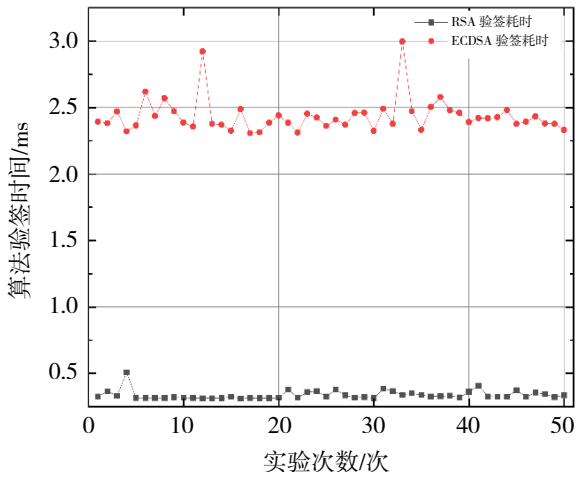


图 5　ECDSA 算法与 RSA 算法密钥生成时间

图 6 为 ECDSA 算法与 RSA 算法对同一段信息增加签名的时间和对信息进行验证签名的时间。在加签过程中，RSA 算法均高于 1 ms，但 ECDSA 算法维持在 1 ms 内完成认证消息的签名操作。在验签过程中，ECDSA 算法消耗时间在 2~3 ms 内波动，RSA 算法低于 0.5 ms。



（a）　ECDSA 算法



（b）　RSA 算法

图 6　ECDSA 算法与 RSA 算法加签与验签时间

经过上述实验综合分析 ECDSA 算法密钥规模小，速度快，适用于计算能力受限的应用领域。卫星测控通信系统中，需要在短时间内对卫星组网消息进行验证，因此可以考虑时间开销较低的 ECDSA 算法进行消息认证。设计基于 ECDSA 算法的星间消息认证如图 7 所示，当卫星 A 向卫星 B 发送消息，发送带有数字签名的消息，接收卫星 B 可以使用区块链上的卫星公钥对加密的摘要进行解密，从而核实卫星 A 对消息的签名，因为只有卫星 A 拥有私钥 A，才可以有效确认消息没有被调包和篡改。

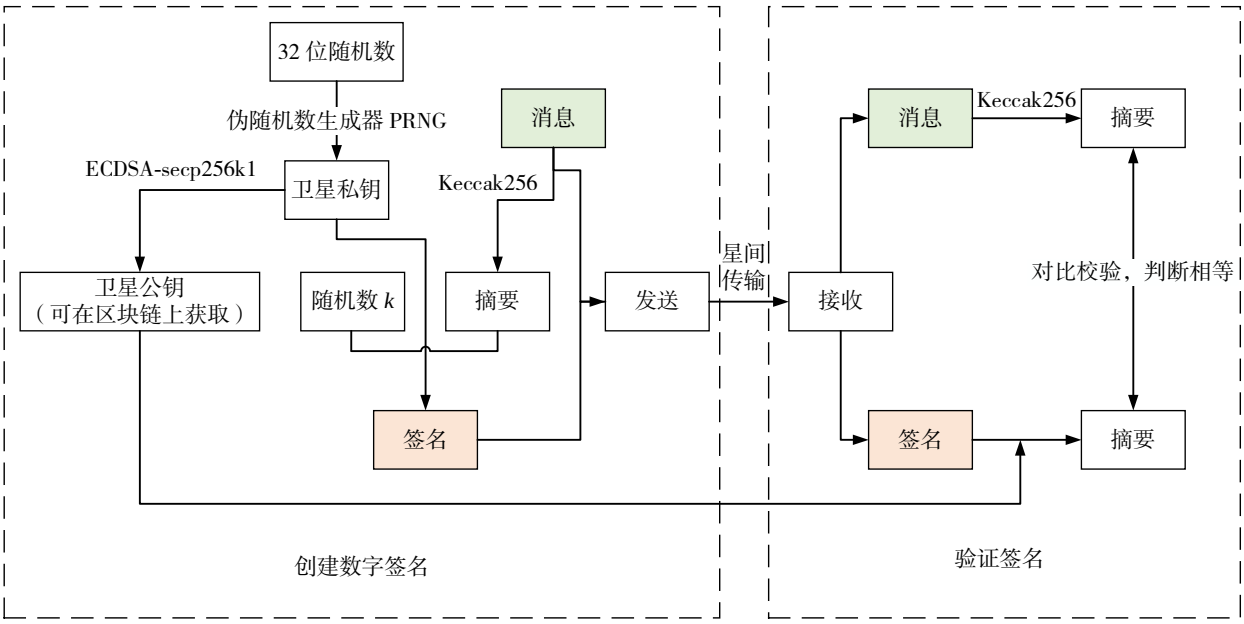


图 7 基于 ECDSA 算法的星间消息认证

3 技术分析

3.1 安全性分析

① 双向认证

本文所提技术能够实现 GEO 和 LEO 之间的双向认证。每颗卫星通过 32 位随机数生成私钥，并在区块链上注册并公开其公钥。在身份认证阶段，只有当两颗卫星均具有链上合法临时身份时，才能实现卫星之间的相互认证。当 GEO 想要向 LEO 发送加密信息并进行消息认证时，GEO 首先需要用自己的私钥对消息进行签名，并将签名值发送给 LEO。LEO 向区块链查询 GEO 的公钥，并使用该公钥进行验签。若验证成功，说明消息确实来自可信 GEO，LEO 向 GEO 发送一条加签的确认消息。GEO 收到确认消息和签名值后，使用 LEO 公钥进行验签，从而确定其来自 LEO。

② 身份隐私保护

卫星的真实身份是敏感的，卫星将临时身份上链。临时身份和永久身份之间没有相关性。因此，攻击者无法从传输的信息中获得卫星的真实身份，也就无法得到卫星的实际参数等信息。

③ 抗重放攻击

在认证过程中，由于每次对卫星临时身份进行确认会更新区块链上时间戳信息。如果攻击者将消息重放，接收方卫星可以通过时间戳判断该消息是否为重放消息，若时间戳不一致则拒绝其消息请求，有效防止认证中的重放攻击。时间戳的工作基础是哈希算法的有效性，哈希算法是在区块链中保证交易信息不可被篡改的一种单向的密码机制。例如，当卫星 B 发起对卫星 A 的组网认证请求消息：Hello satellite A，this is satellite B，requesting network authentication 2023-03-10T14:30:57，在 Keccak256 哈希算法下该消息哈希值为 656507271444336d9dfc423561656302ff55f759dada3b1eaa102361ca4da0d0。重放会改变消息生成的时间戳，如变更为 2023-03-10T14:30:58，仅增加 1 s，哈希值将变为 2855fb668acf6a46877463e9b21baa058f8e987c61f0d7a22e9ac7b5328b185e，造成的影响会产生雪崩效应，容易被识别出消息被更改从而拒绝认证。

3.2 时间性能分析

基于区块链的星间组网认证时间包括身份认证时间和消息认证时间，主要包括密钥生成 T_{KDF}、哈希运算 T_{hash}、椭圆曲线签名运算 T_{ECDSA}、区块链交易时间 T_{trans}、节点共识时间 T_{POX}，星间接入认证机制下计算时间开销 T_{SA} 有如下公式：

$$T_{\mathrm{SA}} = 2T_{\mathrm{KDF}} + T_{\mathrm{hash}} + T_{\mathrm{ECDSA}} + T_{\mathrm{trans}} + T_{\mathrm{POX}}。\quad (5)$$

仿真实现了基于以太坊区块链的星间身份认

证及消息认证。系统注册了单节点 3 个 GEO 账户和 66 个 LEO 账户，完成了将 69 个卫星账户生成临时身份上链。模拟 GEO1 与 LEO1-LEO6 完成身份认证并进行组网任务传输消息认证，当身份认证和消息认证成功时，系统返回认证时间，总时间为 471 ms，仿真界面结果如图 8 和图 9 所示。经实验分析，完成安全认证的时间稳定低于 1 s，能够在容忍时间内完成身份认证及消息认证。

图 8　卫星身份认证仿真界面

图 9　星间消息认证仿真界面

当身份认证或消息认证失败，如恶意卫星发出组网请求、消息被重放会话 ID 发生变化、消息传输用户非组网内卫星等，则返回认证失败错误信息。其中，当恶意节点发起组网申请时会识别卫星身份及权限，反馈认证失败的信息如图 10 所示。

图 10　恶意节点认证失败界面

4　结语

卫星网络的高速发展对安全、高效的互联互通提出了更高的要求，传统认证技术已经无法满足需求。本文通过充分结合 GEO/LEO 双层星座网络架构和区块链技术的特性，设计了基于区块链的星间组网认证技术。论证了身份证书、消息扩散和双向认证等主要功能在双层卫星网络应用背景下的安全性，分析了星间安全认证技术的时间开销。

未来工作将继续推进区块链技术在组网路由中的应用，建立覆盖可信认证与路由协议融合的安全组网模型。

参考文献：

[1] 毕梦格. 低轨卫星网络路由技术研究[D]. 西安: 西安电子科技大学, 2019.

[2] SAHA S S, RAHMAN S, AHMED M U, et al. Ensuring cybersecure telemetry and telecommand in small satellites: recent trends and empirical propositions[J]. IEEE Aerospace and Electronic Systems Magazine, 2019, 34(8): 34-49.

[3] 李凤华, 张林杰, 陆月明, 等. 天地网络安全保障技术研究[J]. 天地一体化信息网络, 2020, 1(1): 17-25.

[4] CRUICKSHANK H S. A security system for satellite networks[C] // Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, London: The Institution of Engineering and Technology, 1996: 187-190.

[5] 彭岩, 廖珊, 赵宝康. 一种面向软件定义卫星网络的轻量级快速安全认证策略[J]. 信息网络安全, 2017(8): 53-59.

[6] 窦志斌, 白鹤峰, 李文屏, 等. 一种卫星网络中的星地轻量化认证鉴权架构[J]. 无线电工程, 2020, 50(4):

262-268.

[7] 石小平, 马如慧, 曹进, 等. 面向卫星网络断续连通场景的接入和切换认证机制[J]. 天地一体化信息网络, 2021, 2(3): 24-34.

[8] 张帅领, 陈李兰, 曹进, 等. 一种适用于 5G 卫星网络的海量终端匿名群组认证协议[J]. 通信技术, 2021, 54(5): 1199-1213.

[9] WEI S J, LI S, LIU P, et al. BAVP: blockchain-based access verification protocol in LEO constellation using IBE keys[J]. Security and Communication Networks, 2018(4): 1-14.

[10] CLARK L, TUNG Y C, CLARK M, et al. A blockchain-based reputation system for small satellite relay networks[C] // 2020 IEEE Aerospace Conference, Big Sky: IEEE, 2020: 1-8.

[11] DENG X, SHAO J, CHANG L, et al. A blockchain-based authentication protocol using cryptocurrency technology in LEO satellite networks[J]. Electronics, 2021, 3151(10): 1-18.

[12] 马煜. 基于区块链的星间通信网络安全加密控制系统设计[J]. 计算机测量与控制, 2021, 29(3): 171-175.

[13] RAZZAQ A, MOHSAN S A H, GHAYYUR S A K, et al. Blockchain-enabled decentralized secure big data of remote sensing[J]. Electronics, 2022, 11(19): 3164.

[14] 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.

[15] 李望. 采用区块链技术的卫星编队组网安全认证设计[J]. 电讯技术, 2022, 62(7): 859-864.

[16] Oneeb. Eutelsat and OneWeb to combine: a leap forward in satellite connectivity[EB/OL]. (2022-07-25)[2023-03-08]. https://oneweb.net/resources/Eutelsat and oneweb combine leap forward satellite connectivity.

[17] 武衡. 卫星安全组网认证关键技术研究[D]. 西安: 西安电子科技大学, 2019.

[18] 朱睿, 张玉东, 魏雅婷, 等. 基于区块链的多层卫星互联网络安全管理技术[J]. 天地一体化信息网络, 2022, 3(1): 79-86.

[19] 朱辉, 武衡, 赵海强, 等. 适用于双层卫星网络的星间组网认证方案[J]. 通信学报, 2019, 40(3): 1-9.

[20] 赵玉清. 面向卫星网络的蜂群终端安全接入与切换认证[D]. 西安: 西安电子科技大学, 2020.

[21] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[22] RABIN M. Digitalized signatures and public-key functions as intractable as factorization[R] // Cambridge: Massachusettsc Institute of Technology, 1979.

[23] WRIGHT M A. The elliptic curve cryptosystem: a synopsis[J]. Network Security, 1998(10): 14-17.

[24] MILLER V S. Use of elliptic curves in cryptography[C] // Advances in Cryptology—CRYPTO' 85 Proceedings, Berlin, Heidelberg: Springer LNCS, 1985: 417-426.

[25] 吴旦. 椭圆曲线加密算法在卫星通信中的应用[J]. 数字通信世界, 2018(9): 160.