空间信息网络中基于动态撤销机制的安全高效批量认证方案

张应辉[1,2,3]，胡凌云[1,3]，李艺昕[1,3]，宁建廷[2,4]，郑东[1,3,5]

（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；2. 福建师范大学福建省网络安全与密码技术重点实验室，福建 福州 350007；
3. 西安邮电大学无线网络安全技术国家工程实验室，陕西 西安 710121；
4. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；5. 卫士通摩石实验室，北京 100070）

摘 要： 针对空间信息网络中大量移动用户跨域认证问题，提出了一种基于动态撤销机制的安全高效的批量认证方案。所提方案通过对卫星行动轨迹的预测以及实时更新会话密钥，达到提前完成密钥协商的作用。同时，还设计了可供单个以及大量移动终端进行签名并验证的算法，有效减轻了卫星的计算负担，结合布谷鸟过滤器实现了移动终端动态撤销和恶意接入控制的功能。最后，在 Diffie-Hellman 假设下，基于随机预言机模型和自动化验证工具证明了所提方案可以抵抗重放以及中间人等攻击；方案实现了可追踪性、可撤销性等安全目标，与现有最优方案相比，传输和计算效率分别提高了 80%和 20%以上。

关键词：空间信息网络；密钥协商；动态撤销；批量认证；自动化验证工具

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022063

Secure and efficient batch authentication scheme based on dynamic revocation mechanism in space information network

ZHANG Yinghui[1,2,3], HU Lingyun[1,3], LI Yixin[1,3], NING Jianting[2,4], ZHENG Dong[1,3,5]

1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China
3. National Engineering Laboratory for Wireless Security , Xi'an University of Posts and Telecommunications, Xi'an 710121, China
4. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
5. Westone Cryptologic Research Center, Beijing 100070, China

Abstract: A secure and efficient batch authentication scheme based on dynamic revocation mechanism was proposed for the problem of cross-domain authentication of a large number of mobile users in space information networks. Early key negotiation was achieved by predicting the satellite trajectory and updating the session key in real time. Algorithms were designed for a single as well as a large number of mobile terminals to perform signing and verification, which effectively reduce the computational burden of satellites. Cuckoo filters were adopted by the new scheme to achieve dynamic revocation and malicious access control of mobile terminals. Finally, under the Diffie-Hellman assumption, the proposed scheme was proved to be resistant to replay and man-in-the-middle attacks based on a random oracle model and automated validation of internet security protocols and applications. Security goals such as traceability and revocability were achieved by the scheme, thus improving the efficiency of transmission and computation by more than 80% and 20%, respectively, compared with the existing optimal scheme.

Keywords: space information network, key agreement, dynamic revocation, batch authentication, AVISPA

收稿日期：2021−10−16；**修回日期：**2022−01−19

基金项目：国家自然科学基金资助项目（No.62072369, No.62072371, No.61972094）；陕西省创新能力支撑计划基金资助项目（No.2020KJXX-052）；陕西省特支计划青年拔尖人才支持计划基金资助项目；陕西省重点研发计划基金资助项目（No.2021ZDLGY06-02, No.2020ZDLGY08-04）

Foundation Items: The National Natural Science Foundation of China (No.62072369, No.62072371, No.61972094), The Innovation Capability Support Program of Shaanxi Province (No.2020KJXX-052), The Shaanxi Special Support Program Youth Top-notch Talent Program, The Key Research and Development Program of Shaanxi Province(No.2021ZDLGY06-02, No.2020ZDLGY08-04)

0　引言

随着航天技术和卫星通信技术的高速发展以及用户随时随地通信需求的日益迫切，将卫星通信融合到地面网络中已经成为必然的趋势和亟待解决的难题。空间信息网络（SIN, space information network）是由多颗不同轨道上、不同种类、不同性能的卫星形成星座覆盖全球，通过星间和星地链路，将地面、海上、空中和深空中的用户、航空器和各种通信平台紧密结合起来，采用互联网之间的通信协议（IP, Internet protocol）作为信息承载方式，采用智能高速星上处理、交换和路由技术，以光、红外多谱段信息为导向，遵循信息资源的最大化、有效综合利用原则，对信息进行准确获取、快速处理和高效传输的一体化高速宽带大容量信息网络[1] 。与传统的无线网络相比，空间信息网络具有更大的覆盖优势，这使一些地面上的无人区、海上和空中的用户更愿意访问空间信息网络，尤其是在某些极端情况下，如在海洋、沙漠或地震灾区等地区，没有分配的网关供用户去访问传统的无线网络，SIN 提供漫游等服务成为必要条件[2]。

同时，由于空间信息网络本身的特点，例如动态拓扑、有限的计算能力和无线广播的性质，它所面临的安全风险也越来越严重。一方面，卫星节点的计算能力受限、星际链路的不稳定性和高轨道卫星以及地球同步卫星通信时延相对较高等因素，使移动节点和卫星节点在漫游切换过程中需要反复接入认证，随之带来高通信时延；另一方面，与传统的无线网络一样，SIN 中的链路也是高度开放的，这一结构特性使系统容易受到拦截、篡改、重放和模拟攻击等传统恶意攻击[3-6]。即使外域网络实体也可能是潜在的攻击者，他们可以根据用户的身份信息泄露用户的隐私。此外，随着全球化进程的普遍性，大量的用户会选择访问该信息网络，这使卫星可能在同一时段需要进行大量的认证服务，从而要求所提出的方案支持批量身份验证，这是本文关注的焦点。

在空间信息网络中，卫星的轨迹是可以预测的，也就是说地面节点与新卫星节点之间的切换认证是可以提前完成的[7-8]。除了卫星的移动轨迹可以预测之外，位置相邻的用户在发生切换时也具有很多相似的特点，即相同的卫星接入节点、相同的目的卫星接入节点以及相同的切换时间，而以聚合消息的方式进行切换，可以节省通信开销以及卫星的计算开销。近年来，研究者已经提出了几种访问认证方案[9-11]，以提供安全可靠的 SIN 通信系统。然而，这些方案不能直接应用于 SIN 中的漫游场景，并且它们都没有考虑到 SIN 的长传播时延。这些方案在移动用户与地面设施，如网关和网络控制中（NCC, network control center）之间实现认证，卫星仅转发认证信令，而不参与实际的认证会话。因此，认证方案在地面与卫星之间（至少在用户/卫星与 NCC/卫星之间来回传输）需要至少 4 倍的信令传输时延，用户无法忍受这么长的访问时延。此外，作为 SIN 系统的接入节点，卫星应负责禁止未经授权的用户访问 SIN。然而，这些方案直到信令被转发到地面设施才能够识别非法接入请求。同访问用户及接入域卫星的身份验证相比，安全漫游也同样重要，但这一问题尚未引起足够的重视。如何确保安全高效的切换无疑是提高 SIN 通信质量的关键。事实上，随着卫星硬件技术的发展，卫星将具有更大的计算能力，并能够与用户进行认证交互。因此，让卫星代替地面设施执行访问控制成为一种有前途的方法，从而减少网络访问时延。

针对上述问题，本文主要做出了以下贡献。

1) 提出了基于动态撤销机制的安全高效批量认证方案，该方案不需要复杂且耗时的配对操作，从而提高了系统的计算效率。进行批量认证时，用户先从附近其他用户接收到所有签名信息，然后将其聚合为一个签名，这样卫星只需确认已注册移动终端签署的相应请求，从而减少总签名的大小和批量验证的开销。

2) 为了保证所提方案适用于漫游场景，要考虑计费的问题，因此所提方案加入了动态撤销机制。该机制通过引入布谷鸟过滤器，支持查询、插入和删除功能，进而可以随时动态地撤销用户，从源头上保护合法用户，达到实时更新保护的作用，利用其删除功能解决了卫星有限存储的问题。

3) 在安全性方面，采用随机预言机和形式化验证工具 AVISPA（automated validation of Internet security protocols and applications）对所提方案进行了严格的分析。结果表明，所提方案可以抵抗重放、篡改等传统攻击的同时，也兼顾了用户匿名以及可追踪等特性。尽管用户端在聚合时会额外产生一定的计算开销，但是由于所提方案不需要耗时的双线性对运算，因此在考虑用户端总的计算开销时，相

较于现有方案而言，所提方案在兼顾用户隐私数据完整性等安全需求的同时，传输和计算开销依然是最低的。

1 相关工作

由于空间信息网络很早就已经被使用，许多研究人员对其相应的通信安全认证方案进行了探索与改进。1996 年，Cruickshank[12]首先提出了一种使用公共密钥密码系统的身份验证方案，以实现移动用户与 NCC 之间的双向身份验证。但是，该方案需要复杂的加密和解密操作，并且用户的身份信息会被暴露，认证效率不高。2003 年，Hwang 等[13]在 Cruickshank 方案的基础上为了减少计算开销，提出了一种适用于空间信息网络的轻量级认证，其中涉及的计算操作都是一些简单的散列函数、异或操作等。与以前的基于公钥的身份验证方案相比，他们的方案具有较低的计算成本，但是在 2005 年，Chang 等[14]发现 Hwang 等的方案的安全性和效率仍然存在不足的地方，缺乏完善的前向保密性，因此提出了一种基于哈希链的身份验证方案，以提高效率和安全性，同时用 Diffie-Hellman 密钥交换来生成新的会话密钥生成，但是在 Chang 等的方案中，当有大量移动用户同时使用漫游服务时，归属域网络控制中心将会成为安全通信的瓶颈，因为它必须参与每个移动用户的身份验证会话。此外，Chang 等方案可能会遭受假冒攻击，并且用户的隐私保密也没有解决。公钥基础设施在解决隐私保护方面有一定的作用，并且公钥基础结构已在传统网络中广泛使用。然而，它需要复杂而耗时的证书管理。文献[15]针对重要信息的明文传输问题引入公钥加密算法，并采用中国剩余定理解决卫星快速切换问题。但是，这 2 种算法依赖于受信任的第三方，该第三方可能是单个瓶颈点，会受到攻击。文献[16]考虑了 5G 网络场景，在半可信第三方环境下结合区块链技术实现了不同网络之间的无缝切换，虽然该方案解决了第三方的瓶颈难题，但是并没有考虑卫星组网的场景。文献[17]采用群组管理的方法，使卫星切换效率得到了提高，但是方案没有实现用户的匿名保护。因此，这些方案在安全性方面的问题没有得到解决。

访问认证方案除了能在空间信息网络中应用外，还应满足漫游服务这个场景，空间信息网络与传统无线网络一样都是开放的链路，传统无线网络的安全漫游认证方案在不断改进。文献[18]分析了传统的匿名漫游认证方案，指出了其匿名性和通信时延的缺点。远程网络认证服务器基于一轮消息交互验证移动终端的身份合法性；另外，当移动终端发生恶意操作时，家庭网络认证服务器可协助远程网络认证服务器撤销移动终端的身份匿名性。然而，该方案未考虑计费问题，且要在列表中查找合法用户，加大了认证时延。对于通信量大等问题，文献[19]提出了一种基于无证书聚合签名的无线漫游方案，但该方案对于安全模型中的敌手均是可伪造的。针对这一安全问题，文献[20]给出了新的无证书聚合签名方案，该方案不使用双线性对操作，大大提高了效率，但是存在暴露用户身份隐私的问题。而在漫游环境中，确保用户的安全和有效访问一直是一个巨大的挑战。为了解决用户实时安全高效访问的问题，文献[21]提出了一种基于双线性对和聚合签名的组认证协议，节点密钥由密钥生成中心（KGC, key generation center）和节点同时生成以抵抗伪装攻击，并且由于离散对数问题引起了会话密钥，大大改善了身份验证过程中的计算复杂性。但是，该协议涉及大量的双线性对操作，即使卫星的计算能力已经改善了，还是会有通信时延增加的问题。在传统的空间信息网络方案中，由于卫星存储空间有限，会引发拒绝服务攻击，如文献[22-24]中虽然通过代理签名等算法对该问题进行了改进，但是改进后的效率大大降低。文献[25]对上述部分安全问题提出了解决方案，采用基于生物特性的三因子认证技术，实现了用户与外域网络的双向安全切换认证，但是该方案缺少具体的漫游计费叙述，适用性不高。上述文献为无线网络的漫游认证提供了安全性，但是在传统的空间信息网络场景下，卫星和网关之间的传播时延很高，导致移动用户承受高认证时延。因此，这些方案在空间信息网络漫游场景中实用性不高。

2 预备知识

本节主要对方案中所使用的算法定义进行概括。

2.1 Schnorr 签名

该签名算法主要分为初始化阶段、签名生成阶段和签名验证阶段。

1) 初始化阶段。首先选择一个大素数 p，使其在 Z_p 中求解离散对数困难；然后选择一个生成元

$g \in Z_p^*$，$g^q \equiv 1 (\mathrm{mod}\ p)$；最后选取随机数$1 < x < q$，计算$y \equiv g^x \bmod p$，则公钥为$(p,q,g,y)$，私钥为$x$。

2) 签名生成阶段。签名者已知以下条件：G是椭圆曲线$E_p(a,b)$的基点，H是哈希函数，m是待签名消息，x是私钥。签名者选择一个随机数k,令$K = kG$，对消息m进行如下计算：$r \equiv g^k \bmod p$，$e = H(r,m)$，$s \equiv xe + k \bmod q$，得到签名值(e,s)即Schnorr签名。

3) 签名验证阶段。验证者已知以下条件：G是椭圆曲线$E_p(a,b)$的基点，H是哈希函数，m是待签名消息，P是公钥，(R,s)是Schnorr签名。验证者在收到消息m和签名值(e,s)后，计算$r_1 \equiv g^s y^{-e} \bmod p$和$H(r_1,m)$，验证等式$H(r_1,m) = e$是否成立，若等式成立，则签名合法。

2.2　布谷鸟过滤器

当存在大量数据时，如何快速搜寻并确定数据的位置？对于这一问题，研究者以前会选择撤销算法或者使用布隆过滤器，但是布隆过滤器不支持反向删除元素，一旦数组元素被赋值，就无法删除。而布谷鸟过滤器是用于集合成员身份测试的新数据结构，与传统的布隆过滤器相比，它具有更低的误报率、更低的空间开销和更好的性能。布谷鸟过滤器支持在实现高性能的同时动态地添加和删除项目。布谷鸟过滤器本质上是一个由一组存储桶组成的哈希表，每个存储桶都包含固定数量的指纹（具有较少输出位的哈希函数）。

布谷鸟过滤器算法包括3个功能，即查询、插入和删除。查询函数首先计算查询项的指纹，并根据该指纹获取查询项在对应哈希表中的位置，如果找到该位置则查询成功。插入函数首先计算插入项的指纹，然后根据指纹获取插入项在相应哈希表中的位置，如果该位置已被占用，则从该位置移除元素，插入要插入的项目，再将移除的项目插入一个空位置。删除函数首先查询哈希表，如果查询成功，无论查询到存储桶中的指纹数量是否满足要求，仅删除一个指纹即可。布谷鸟过滤器源于布谷鸟哈希算法，布谷鸟哈希表有两张，分别是2个哈希函数，当有新的数据插入的时候，它会计算出这个数据在两张表中对应的2个位置，这个数据一定会被存储在这2个位置之一。一旦发现其中一张表的位置被占，就将该位置原来的数据踢出，被踢出的数据就去另一张表找对应的位置。通过不断地踢出数据，最终所有数据都可找到自己的位置[26]。

3　系统模型和安全需求

3.1　系统模型

本文主要研究的是空间信息网络中漫游场景下，多用户离开归属域网络进入漫游域网络认证通信过程，参与这一过程的主要有以下实体：移动用户（MU, mobile user）、归属域网络控制中心（HNCC, home network control center）、归属域网关（HG, home gateway）、归属域低轨道地球卫星（HLEO, home low earth orbit satellite）、拜访域网络控制中心（FNCC, foreign network control center）、拜访域网关（FG, foreign gateway）、拜访域低轨道地球卫星（FLEO, foreign low earth orbit satellite）。系统模型结构如图1所示，具体说明如下。

1) MU在其HNCC上注册，希望通过FLEO使用拜访域网络。

2) HNCC与FNCC为用户提供到特定拜访域的漫游凭证以及后续认证需要用到的信息。

3) FLEO和HLEO是MU与网关之间的中继节点，负责转发认证信息与会话协商参数。

4) HG和FG连接卫星网络和地面服务器。移动用户可通过网关接入地面互联网，卫星也可以通过网关与网络控制中心进行通信。漫游时，移动用户通过FG连入拜访域的网络中。

3.2　安全需求

本文方案基于Dolev-Yao攻击者模型[27]，该模型的描述如下。

1) 确定攻击者所掌握的信息集合。

2) 随机拦截网络中的任意一条消息，使用分解规则分解该条消息，并更新信息集合。

3) 随机使用合成规则来构造一个消息，将其发送到网络中，其中需要的信息从已有的信息集合中随机选取。

在该模型中，攻击者几乎是无所不能的，因此设计的方案如果抵抗了该模型的攻击，那就证明该方案是安全的。

本文方案中的各域网络控制中心是完全可信的。网络控制中心根据用户的注册信息来诚实地分发一些参数以及分发一些LEO的公私钥对。空间信息网络的卫星接入节点是不同区域的，接入节点在为用户提供接入服务的同时，为扩大自己的利益，对合法用户的身份及地理位置信息会感兴趣，

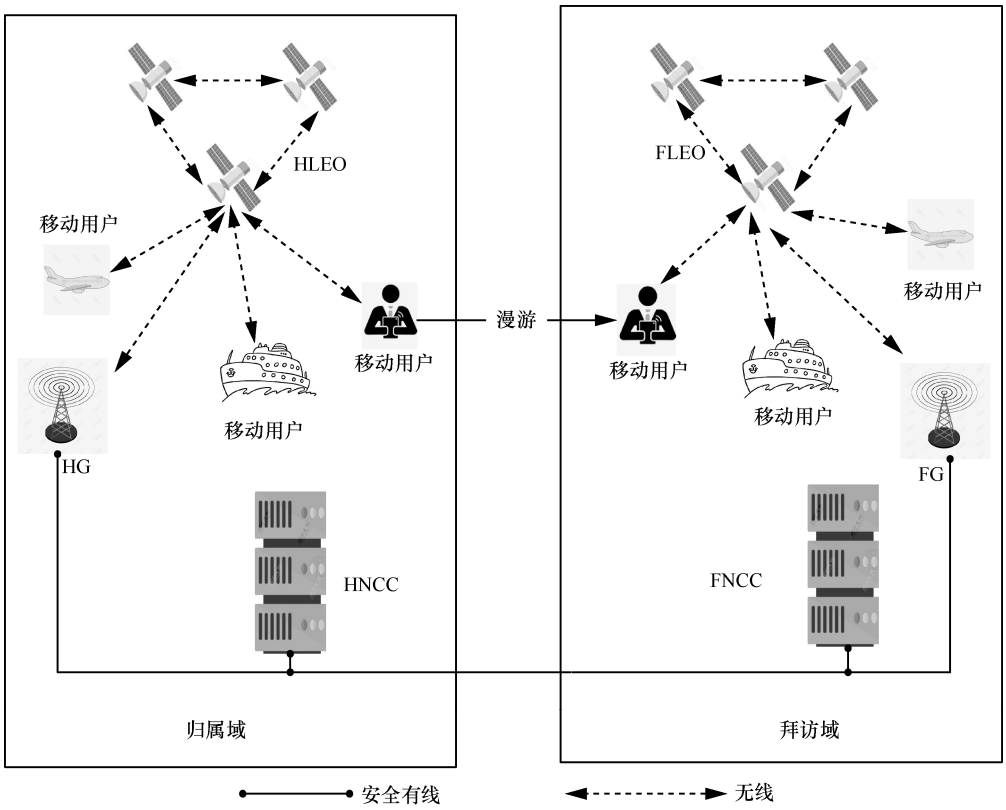

图 1 系统模型结构

所以外域接入节点对用户来说也会是恶意实体，而各域内的网关和 LEO 之间假设建立了可信关联。非授权移动用户被认为是系统模型中的恶意实体，他们会尝试采取各种非法手段来获得可以接入网络的权限，从而窃取合法用户的隐私信息以及非法访问网络服务。一般完全的匿名性伴随着不可审计性，这会让非法用户逃脱追责，且漫游服务的计费问题不易解决。因此，用户的身份既要是匿名的，又要保证是条件可追踪的，这 2 个特性看似矛盾，实则是对该网络的挑战。从以上的角度来看，本文方案应主要关注以下安全需求。

1) 双向认证。移动用户与 LEO 之间的相互认证是漫游服务的基本需求。验证 LEO 是为了保护用户的身份信息，绿化网络环境。验证移动用户是为了让合法用户访问网络，确保网络的权限。

2) 会话密钥协商。由于开放的通信环境，通信内容会被窃听，因此方案应该确保双方之间的通信是使用共享会话密钥进行加密的，从而保证通信过程的保密性。

3) 动态撤销及防止非法接入。当用户想要撤销时，一些用户可能非法使用票据或申请退出漫游服务，系统需要主动撤销这些用户的票据来撤销用户；一些非法用户使用已经过期的票据来进行漫游服务时，系统要能够查询并找出该非法用户。

4) 可追踪性。为了保护移动用户的隐私，本文方案应实现匿名性。然而，如果当用户实施非法行为时，该方案应该确定非法用户的真实信息并取消用户漫游身份。

5) 抗重放攻击。鉴于该网络中通信链路开放的特点，攻击者能更容易地窃取用户的传输信息，因此本文方案需要考虑验证消息的即时性以抵抗重放攻击。

6) 抗拒绝服务（DoS, denial of service）攻击。由于卫星的存储资源有限，应在快速有效地验证合法用法用户的身份同时拒绝非法请求，以避免 DoS 攻击。

4 漫游认证方案

本节主要描述了本文方案，包括系统初始化及用户注册、预协商、用户认证及密钥协商、批量验证、用户计费及动态撤销等阶段。为了描述方便，表 1 列举了涉及的相关符号及其定义。

表 1　　相关符号及其定义

符号	定义
G	椭圆曲线 E_p 的基点
n	基点 G 的阶
H_1, H_2, H_3	映射到椭圆曲线 E_p 上的哈希函数

4.1　系统初始化及用户注册阶段

1) 用户获取漫游服务前，需要向 HNCC 订阅对应拜访域的漫游服务。用户首先向 HNCC 发送漫游订阅请求 $\{\mathrm{ID}_i, \mathrm{ID}_{\mathrm{FNCC}}\}$，其中 $\mathrm{ID}_{\mathrm{FNCC}}$ 是拜访域网络控制中心的身份标识。

2) HNCC 生成一个随机数 d_i 作为其私钥，并将其私钥保密，相应的公钥为 $D_i = d_i G$。

3) HNCC 为用户随机生成一个计费凭证 x_i，通过计费凭证生成用户的伪身份 $\mathrm{TID}_i = H_1(\mathrm{ID}_i \| x_i)$，以及凭证相应的有效票据 T_{END}（过期作废）。

4) 在系统初始化阶段，每个 NCC 都可以看作密钥分发中心，当用户注册时，为用户分发公私钥 $\mathrm{sk}_i = H_1(\mathrm{ID}_i \| k_i) d_i$（其中 k_i 为随机数），其对应的公钥为 $P_i = \mathrm{sk}_i G$。

5) 各归属域内的卫星已经认证，网络控制中心为低轨道地球卫星（LEO, low earth orbit satellite）计算公、私钥对，分别为 $\mathrm{sk}_{\mathrm{LEO}} = H_1(\mathrm{ID}_{\mathrm{LEO}} \| l) d_i$（其中 l 为随机数），$\mathrm{pk}_{\mathrm{LEO}} = \mathrm{sk}_{\mathrm{LEO}} G$；然后把私钥通过安全通道发送给卫星，并公布公钥。

6) HNCC 把 $\{x_i, \mathrm{TID}_i, T_{\mathrm{END}}, \mathrm{sk}_i, \mathrm{pk}_{\mathrm{FLEO}}\}$ 通过安全通道发送给用户，然后本地存储 $\{\mathrm{ID}_i, \mathrm{ID}_{\mathrm{FNCC}}, x_i\}$ 作为后续计费审计用，并公布一些公共参数 $\{G, n, H_1, H_2, H_3, P_i, \mathrm{pk}_{\mathrm{LEO}}\}$。

用户注册阶段的信息交换如图 2 所示。

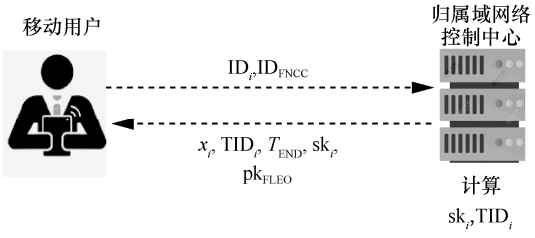

图 2　用户注册阶段的信息交换

4.2　预协商阶段

为了简单起见，本文假设接入卫星与网关已经完成了相互认证，并建立了信任关系。在此阶段，网关通过安全通道不断向本域内的卫星发送预协商消息 $\{\mathrm{ID}_G, T_{G\mathrm{new}}, R_G\}$。预协商消息包含网关的身份标识、时间戳和密钥协商参数，计算为 $R_G = r_G G$，其中，r_G 是网关选择的随机数，用于用户认证及密钥协商阶段生成会话密钥。卫星收到消息后，首先检查时间戳以防止重放攻击，然后检查网关的身份信息，最后存储此预协商消息。每个时间戳对应不同的协商参数，且每个时间对应不同的时间戳 $T_{G\mathrm{new}}$。预协商阶段的信息交换如图 3 所示。

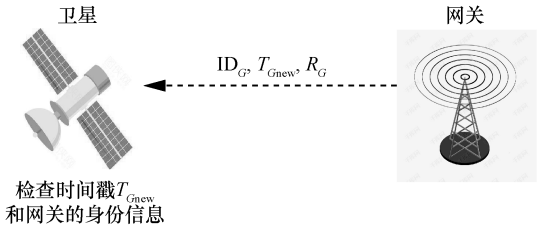

图 3　预协商阶段的信息交换

4.3　用户认证及密钥协商阶段

用户认证及密钥协商阶段发生在 MU 移动到漫游区域的网络，并且向网络发起请求时。由于同一时间段，计费凭证的有效期限相同，漫游到同一区域的用户很多，且卫星的运动轨迹可预测以及卫星的计算、存储能力有限。因此，以分组方式为这些用户执行漫游服务是合理的。如图 4 所示，当用户请求访问空间信息网络中的漫游资源时，将进行身份认证，具体步骤如下。

1) $\mathrm{MU}_i \rightarrow \mathrm{FLEO}: \{\mathrm{msg}_i, R_i, S_i, T_{\mathrm{END}}, T_i^1\}$。单个用户进行漫游认证时，$\mathrm{MU}_i$ 可以计算 $a_i = H_2(T_i^1 \| P_i)$，用户生成一个随机数 r_i 和时间戳 T_i^1，其中随机数 r_i 作为后续会话密钥协商阶段的参数，然后计算 $R_i = r_i G$，$Z = H_3(P_i \| R_i \| \mathrm{msg}_i)$，$S_i = (r_i + Z a_i \mathrm{sk}_i) \bmod n$，把 (R_i, S_i) 作为对消息 msg_i 的签名，其中 $\mathrm{msg}_i = \{\mathrm{TID}_{\mathrm{MU}_i}, \mathrm{ID}_{\mathrm{FLEO}}, \mathrm{ID}_{\mathrm{HNCC}}\}$，用户把消息和其响应的签名一并发送给接入卫星。

2) $\mathrm{FLEO} \rightarrow \mathrm{MU}_i: \{\mathrm{msg}_{\mathrm{FLEO}}, R_{\mathrm{FLEO}}, S_{\mathrm{FLEO}}, T_{\mathrm{FLEO}}^2\}$。对于收到的访问请求，FLEO 通过验证消息并生成访问响应消息。首先，验证传播时延 $T_{\mathrm{now}} - T_i^1$ 是否在可接受的阈值 Δt 内。如果超出阈值，FLEO 则认为该请求为重放分组，拒绝用户的请求；如果未超出阈值，则将 T_{END} 作为查询元素，通过布谷过滤器查询是否失效，若失效，则拒绝该请求；若未失效，当 FLEO 收到消息及签名后，计算 $a_i = H_2(T_i^1 \| P_i)$，$Z = H_3(P_i \| R_i \| \mathrm{msg}_i)$，并验证等式 $S_i G = Z P_i + R_i$ 是

否成立；若不成立，同样拒绝用户的访问请求，若成立，则该组用户合法。FLEO 读取在预协商阶段已缓存的密钥参数，并生成访问响应消息，然后选择一个随机数 r_{FLEO} 并计算 $R_{\mathrm{FLEO}}=r_{\mathrm{FLEO}}G$，$a_{\mathrm{FLEO}}=H_2(T^2_{\mathrm{FLEO}}\|\mathrm{pk}_{\mathrm{FLEO}})$，$Z=H_3(\mathrm{pk}_{\mathrm{FLEO}}\|R_{\mathrm{FLEO}}\|\mathrm{msg}_{\mathrm{FLEO}})$，$S_{\mathrm{FLEO}}=(r_{\mathrm{FLEO}}+Za_{\mathrm{FLEO}}\mathrm{sk}_{\mathrm{FLEO}})\bmod n$。最后，FLEO 将具有相应签名的访问响应消息 $\mathrm{msg}_{\mathrm{FLEO}}=\{\mathrm{TID}_{\mathrm{MU}},\ \mathrm{ID}_{\mathrm{FG}},\mathrm{ID}_{\mathrm{FLEO}},R_{\mathrm{FG}},R_i\}$，同时发送给漫游用户和 FG。

3) 验证后计算会话密钥。移动用户收到接入卫星发来的消息后，首先检查时间戳的有效性，即 $\Delta T=T_{\mathrm{now}}-T^2_{\mathrm{FLEO}}$，如果超出阈值范围，则丢弃该消息并中止方案；否则对等式 $S_{\mathrm{FLEO}}G=Z\mathrm{pk}_{\mathrm{FLEO}}+R_{\mathrm{FLEO}}$ 进行验证。如果验证通过，则计算会话密钥 $\mathrm{SK}=r_iR_G$；否则判定该接入卫星是不合法的并中止方案。网关收到响应消息后，先验证时间戳是否在阈值内，若在，则计算会话密钥 $\mathrm{SK}=r_GR_i$；若不在阈值内，则终止方案。

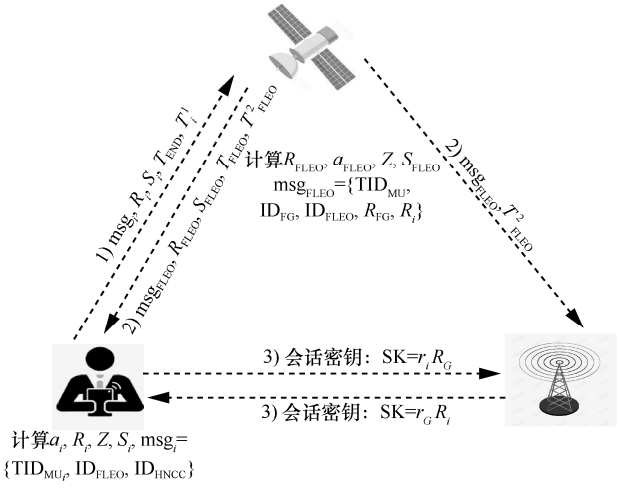

图 4 用户认证及密钥协商阶段

4.4 批量验证阶段

1) 同一时间段有相同的移动用户要访问同一区域的网络时，可以对移动用户进行分组。设该组成员有 m 个，其需要先把公钥和 R_j 值发送给组管理员，再进行各自的签名。设 $L=\{P_1,P_2,\cdots,P_m\}$ 表示用户公钥的集合，用户计算 $a_i=H_2(T^1_i\|L\|P_i)$，组管理员聚合公钥 $P=a_1P_1+a_2P_2+\cdots+a_mP_m$，用户随机选择一个整数 r_i 作为后续密钥协商阶段的参数，并计算 $R_i=r_iG$，$Z=H_3(P\|R\|\mathrm{msg}_i)$，$S_i=(r_i+Za_i\mathrm{sk}_i)\bmod n$，用户通过提前交互 S_i 和 R_j，再将其聚合 $R=R_1+R_2+\cdots+R_m$，$S=(S_1+S_2+\cdots+S_m)\bmod n$，把漫游用户的聚合签名设置为 (R,S)，最后用户把访问请求 $\{\mathrm{msg}_i,R,S,L,T_{\mathrm{END}},T^1_i\}$ 及其相应的签名 (R,S) 发送给卫星。

2) 当 FLEO 收到组用户发送的访问消息及其签名后，首先验证传播时延 $T_{\mathrm{now}}-T^1_i$ 是否在可接受的阈值 Δt 以内。若不在阈值内则认为其为重放分组，拒绝用户的请求。若在阈值内，FLEO 则使用 T_{END} 作为查询元素，通过布谷过滤器查询是否过期，若过期，则拒绝该请求；否则计算 $a_i=H_2(T^1_i\|L\|P_i)$，$P=a_1P_1+a_2P_2+\cdots+a_mP_m$，并验证等式 $sG=ZP+R$ 是否成立，若不成立，则拒绝该请求，否则 FLEO 计算 $a_{\mathrm{FLEO}}=H_2(T^2_{\mathrm{FLEO}}\|\mathrm{pk}_{\mathrm{FLEO}})$，$Z=H_3\cdot(\mathrm{pk}_{\mathrm{FLEO}}\|R_{\mathrm{FLEO}}\|\mathrm{msg}_{\mathrm{FLEO}})$，$S_{\mathrm{FLEO}}=(r_{\mathrm{FLEO}}+Za_{\mathrm{FLEO}}\mathrm{sk}_{\mathrm{FLEO}})\bmod n$，读取在预协商阶段缓存的会话参数并生成访问响应消息 $\mathrm{msg}_{\mathrm{FLEO}}=\{\mathrm{TID}_{\mathrm{MU}},\ \mathrm{ID}_{\mathrm{FG}},\mathrm{ID}_{\mathrm{FLEO}},R_{\mathrm{FG}}\}$ 及其签名 $(R_{\mathrm{FLEO}},S_{\mathrm{FLEO}})$ 发送给组用户。后续密钥会话步骤与用户认证及密钥协商阶段中的验证后计算会话密钥步骤相同。

4.5 用户计费及动态撤销阶段

HNCC 通过 FNCC 向 FLEO 发送当月有效票据，当用户被漫游区域的网络认证后，为防止有效票据被重复使用，FLEO 将认证之后的有效票据插入所维护的布谷过滤器的正过滤器中，过期的票据插入负过滤器中。为防止过滤器无限增大，每个月月初都会清空过滤器。当移动用户量增大时，卫星广播量增大，一种有效的解决方案是将过滤器切成薄片并将切片分配到附近的 LEO，详细步骤如下。首先，FLEO 将正滤波器和负滤波器分别切为切片集 $\{\mathrm{PF}_1,\mathrm{PF}_2,\cdots,\mathrm{PF}_m\}$ 和 $\{\mathrm{NF}_1,\mathrm{NF}_2,\cdots,\mathrm{NF}_m\}$。然后，FLEO 使用 ECDSA 签名算法计算 $\sigma_{\mathrm{FLEO}}=\mathrm{Sign}_{\mathrm{sk}_{\mathrm{FLEO}}}(\mathrm{PF}_1,\mathrm{PF}_2,\cdots,\mathrm{PF}_m,\mathrm{NF}_1,\mathrm{NF}_2,\cdots,\mathrm{NF}_m)$，并将签名广播到所在归属域的其他 LEO 上，其他 LEO 可以用该卫星的公钥去验证真实性。当用户想撤销时，由于一些用户可能非法使用票据或想要申请退出漫游服务，系统需要主动撤销这些用户的票据来撤销用户。HNCC 将撤销用户有效期的票据通过安全通道发送给 FNCC。FNCC 收到消息后，将这些票据通过 FG 的安全通道广播给所在域的所有 LEO，LEO 将这些值存入负过滤器中。同时，LEO 也可以通过验证发现非法用户，同样也会把非法用户对应的票据存入负过滤器中，并广播给 FG，FG 再反馈给 HNCC。

若用户还有剩余票据没有撤销，则在凭证生效的月初执行撤销操作。当用户认证完毕后，FLEO 把 x_i 通过 FG 发送给 FNCC。FNCC 利用收集的有效票据向 HNCC 收取费用，HNCC 再根据用户使用的凭证数目向其收取费用。用户计费及动态撤销如图 5 所示。

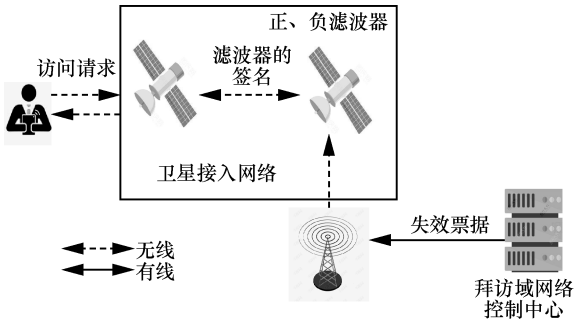

图 5　用户计费及动态撤销

5　安全评估

本节首先使用随机预言机模型（ROM, random oracle model）证明本文方案实施期间协商的会话密钥是安全的；然后，基于自动化验证工具 AVISPA[28] 来证明本文方案能抵抗重放和中间人等攻击；最后，非形式化分析说明了本文方案的安全属性和抵抗其他攻击的能力。

5.1　基于随机预言机模型的安全性分析

本节将使用 ROM 对本文方案进行安全性分析。

5.1.1　安全模型

假设存在一个多项式时间攻击者 A，其可以访问通信双方之间传输的所有消息，也知道所有公共参数。符号 $\prod_i^k$ 表示参与方 i 的第 k 个会话实例，每个会话实例也称为预言机。每个预言机有 3 种状态，即接受、拒绝、无效。如果预言机收到正确的消息，则状态为接受；如果预言机收到错误的消息，则状态为拒绝；如果预言机没有收到消息，则状态为无效。攻击者 A 可以使用模拟器进行以下询问以破坏提议方案的安全性。

5.1.2　询问模型

攻击者 A 的攻击能力用以下几个询问模型来模拟。

1) Extract ($\mathrm{ID_{MU}}$)。在这个询问模型中，攻击者 A 可以得到用户身份 $\mathrm{ID_{MU}}$ 对应的公钥/私钥对。

2) Send ($\prod_i^k$, m)。攻击者 A 通过访问这个询问对 $\prod_i^k$ 发起主动攻击。在这个询问模型中，攻击者 A 可以向预言机 $\prod_i^k$ 发送消息 m。当接收到 m 时，$\prod_i^k$ 根据方案进行计算并将相应的反馈返回给 A。

3) Reveal ($\prod_i^k$)。如果预言机接受这个询问，则返回一个会话密钥给攻击者 A；否则，将无效标识返回给 A。

4) Corrupt ($\prod_i^k$)。在这个询问模型中，攻击者 A 可以请求参与方 i 的私钥并获取其私钥。

5) Test ($\prod_i^k$)。Test 询问用于衡量会话密钥的语义安全强度。攻击者 A 可以向预言机 $\prod_i^k$ 发送单个测试询问。收到询问后，预言机开始抛硬币 $c\in\{0,1\}$，如果结果是 1，则返回给攻击者 A 真正的会话密钥；如果结果是 0，则返回给攻击者一个随机位串。

语义安全性。作为实验的一部分，攻击者 A 需要区分会话实例中的密钥是新会话密钥还是随机密钥。允许 A 对实例 MU 或 FLEO 实例执行多次测试询问。攻击者在游戏结束后，必须输出一个猜测结果。如果 A 猜中了正确的结果，则认为攻击者 A 获得了方案 D 的语义安全性的成功并把这个成功定义为 Succ，则攻击者 A 进行本次攻击的优势定义为

$$\mathrm{Adv}_D(A)=\left|2\Pr[\mathrm{Succ}]-1\right|$$

一般地，如果 $\mathrm{Adv}_D(A)$ 可以忽略不计（即对于任何足够小的 $\varepsilon>0$，有 $\mathrm{Adv}_D(A)<\varepsilon$），则称方案在随机预言机下是安全的。

5.1.3　安全性证明

定义 1　如果满足以下条件，则认为方案是安全的。在 $\prod_{\mathrm{MU}}^s$ 和 $\prod_{\mathrm{FLEO}}^t$ 上存在良性敌手的情况下，2 个预言机总是协商同一个会话密钥，并且这个密钥随机均匀分布。对于任何多项式敌手，成功的概率 $\mathrm{Adv}_D(A)$ 可以忽略不计。

引理 1　假设 ECDH 问题是困难的，那么在随机预言机模型中，攻击者对该方案的优势可以忽略不计。

证明　假设有一个敌手 A，他可以在多项式时间 t 内以不可忽略的概率 $\lambda(k)$ 破坏所提方案的认证密钥协商语义安全性，则可以从敌手 A 构造另一个算法 φ，以另一个不可忽略的概率求解 ECDH 问题。φ 在解决 ECDH 问题上的优势是 $\mathrm{Adv}^{\mathrm{ECDH}}(\varphi)$。

1) 算法 φ 被赋予系统参数 $(F_p,\frac{E}{F_p},G,h_1,h_2,h_3)$ 和 ECDHP 的一个实例 $(G,\alpha G,\beta G)$，它

的任务是计算 $\alpha\beta G$。φ 随机选择 $X\in[1,n_x]$, $Y\in[1,n_y]$, $Z\in[1,n_z]$。φ 选择一个随机数 $\mathrm{sk}_{\mathrm{NCC}}\in_R Z_q^*$ 并计算相应的公钥 $\mathrm{pk}_{\mathrm{NCC}}=\mathrm{sk}_{\mathrm{NCC}}G$。然后 φ 设置系统参数 $\mathrm{Para}=\{F_p, \frac{E}{F_p}, G, h_1, h_2, h_3, \mathrm{pk}_{\mathrm{NCC}}\}$ 并将其发送给攻击者 A。φ 回答 A 的询问如下。

2) Extract-Query。φ 维护一个元组组成形式为 $(\mathrm{ID}_x,\mathrm{TID}_x,d_x,\mathrm{sk}_x,\mathrm{pk}_x)$ 的空列表 LE_x。当攻击者 A 用 $(\mathrm{ID}_x,\mathrm{TID}_x)$ 询问预言机时，φ 通过索引 $(\mathrm{ID}_x,\mathrm{TID}_x)$ 搜索列表 LE_x。如果 $x=X$，则 φ 以 $(\mathrm{ID}_X,\mathrm{TID}_X,d_X,\mathrm{sk}_X,\mathrm{pk}_X)$ 响应；如果 $x\neq X$，则 φ 选择随机数 $h_{1,x},\mathrm{sk}_x\in_R z_q^*$，并计算对应的公钥 $\mathrm{pk}_x=\mathrm{sk}_xG$。最后，$\varphi$ 将元组 $(\mathrm{ID}_x,\mathrm{pk}_x,\mathrm{TID}_x,\mathrm{sk}_x,d_x)$ 插入列表 LE_x。

3) Corrupt-Query。收到这个询问后，如果 $x=X$，则 φ 中止当前会话。如果 $x\neq X$，则 φ 在列表 LE_x 中搜索 ID_x，如果 ID_x 在 LE_x 中，φ 用 sk_x^k 响应；否则，φ 询问 Extract-Query，并计算 sk_x^k 和 pk_x^k。

4) Send-Query。敌手 A 进行 Send $(\prod_x^z, m)$ 询问时，φ 首先验证时间戳是否新鲜。如果在时间域内，φ 退出当前会话；否则，φ 选择均匀随机数 $a_y,h_2^y\in Z_q^*$，并计算 $r_y=a_yG, R_y=h_2(\mathrm{pk}_y\|m\|r_y)$。$\varphi$ 将元组 $(\prod_x^z,T_y,\mathrm{pk}_y,R_y,a_y)$ 插入列表 LE_y 中，然后返回 $(\prod_x^z,T_y,\mathrm{pk}_y,R_y,a_y)$。

5) Reveal-Query。该询问中 φ 维护一个元组组成形式为 $(\prod_{x,y}^z,\mathrm{ID}_x,\mathrm{ID}_y,R_x,R_y,R_z,\mathrm{SK}_{x,y}^z)$ 的空列表 LS_y，其中符号 $\prod_{x,y}^z$ 表示实体 x 和 y 之间的第 z 个会话。当收到这个询问时，φ 回答如下。

① 如果 $z=Z\wedge x=X\wedge y=Y$，φ 退出游戏。

② 如果 $x=X$，φ 通过列表 LE_y 中的索引 (R_x,R_y,R_z) 查找列表 LE_y 以获得会话 (U_x^z,U_y^z)。然后 φ 检查 $e(R_x,R_z)=e(G,U_x^z)$ 或 $e(R_y,R_z)=e(G,U_y^z)$，φ 选择 U_x^z 或 U_y^z 作为会话密钥 $\mathrm{SK}_{x,y}^z$，并返回。

6) Test-Query。如果 φ 没有选择预言机 $\prod_{X,Y}^Z$ 之一来询问测试询问，则 φ 退出游戏；否则，φ 简单地输出一个随机值 $\eta\in\{0,1\}^k$。

分析 如果 φ 没有被中止，则 φ 选择 $\prod_{X,Y}^Z$ 作为测试询问预言机的概率为 $\left[\frac{1}{n_xn_yn_z}\right]$。如果 φ 能在这样的游戏中获胜，那么 φ 肯定分别进行了形式为 (T_x,R_x,h_2,U_x^z) 和 (T_y,R_y,h_3,U_y^z,U_y) 相应的询问。因此 φ 可以在询问中以概率 $\left[\frac{1}{n_{h_1}n_{h_2}}\right]$ 找到对应的项目，并输出 U_x^z 或 U_y^z 作为 ECDHP 的解。φ 求解 ECDHP 的概率为 $\mathrm{Adv}^{\mathrm{ECDH}}(\varphi)\geqslant\frac{\lambda(k)}{n_xn_yn_zn_{h_1}n_{h_2}}$。证毕。

5.2 基于 AVISPA 的安全性分析

本节首先介绍自动化验证工具 AVISPA；其次对本文方案用 AVISPA 的 OFMC（on-the-fly model-checker）分析终端进行分析，模拟攻击路径；最后根据攻击，证明本文方案的安全性。

1) 为了对本文方案的安全性进行形式化分析，本节使用工具对方案进行了建模和安全性证明，用高级协议规范语言（HLPSL, high level protocols specification language）实现了会话、目标和环境的角色说明。在 AVISPA 中，采用了 HLPSL 的模块化，通过表达形式语言来指定协议并验证协议的安全性。AVISPA 工具一共有 4 种终端分析技术，分别为 OFMC 终端、CL_AtSe（constraint-logic-based attack searcher）终端、SATMC（SAT-based model-checker）终端和 TA4SP（tree automata based on automatic approximations for the analysis of security protocols）终端。这 4 种终端分析技术基于 2 个假设，一个是完美的密码安全，一个是协议运行中存在的攻击者模型满足 Dolev-Yao 攻击者模型。本文用 HLPSL 对用户和卫星角色进行了描述，分析过程包括初始状态、角色转换状态、终止状态。具体以用户角色描述为例，如图 6 所示。

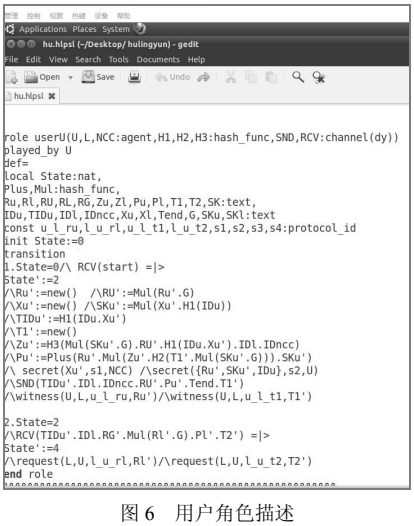

图 6 用户角色描述

2) 该模型的用户和卫星角色过程包含全局的常量和一个或者多个会话的混合角色过程，其中，方案的主体是卫星和用户产生并传送共享会话密钥，在发送的同时要确保共享会话密钥的机密性；用户和卫星之间可以有效分辨双方真实性。同时，入侵者可能伪装成合法用户，运行某些角色进行会话。

3) 以 OFMC 模块为例给出具体的分析，检测结果表明方案是安全的（SUMMARY:SAFE），结果中的统计量还包含运行搜索的时间开销为 0.05 s，访问的节点总数为 4 个，深度为 2，采用的入侵检测模型表明该方案中攻击者无突破口。

5.3 进一步安全性分析

1) 双向认证。在本文设计的接入认证方案中，用户和接入卫星之间能够实现双向认证。其中，卫星通过验证等式 $s_iG=[(r_i+Za_i\mathrm{sk}_i)\bmod n]G=R_i+ZP_i$ 是否成立来验证用户的合法性。基于椭圆曲线离散对数问题和哈希函数单向性的特点，攻击者在无法获得用户私钥的情况下仿造一个合法有效的接入请求消息是困难的。因此，只有在注册阶段获得合法有效的认证信息元组的用户才能产生有效的接入请求消息，从而成功被接入卫星认证。相似地，用户可以通过验证等式 $s_{\mathrm{FLEO}}G=[(r_{\mathrm{FLEO}}+Za_{\mathrm{FLEO}}\mathrm{sk}_{\mathrm{FLEO}})\bmod n]G=Z\mathrm{pk}_{\mathrm{FLEO}}+R_{\mathrm{FLEO}}$ 是否成立来认证该接入卫星的合法性，同样地，只有已注册的合法卫星才能够产生有效的接入响应消息 $\{\mathrm{msg}_{\mathrm{FLEO}}, R_{\mathrm{FG}}, R_{\mathrm{FLEO}}, S_{\mathrm{FLEO}}\}$。因此，本文方案能够实现用户与接入卫星之间的双向认证。

2) 会话密钥协商。本文方案采取椭圆曲线上的密钥交换技术，使用户与网关之间共同协商出会话密钥 $\mathrm{SK}=r_iR_G$ 和 $\mathrm{SK}=r_GR_i$，其中 r_G 和 r_i 是随机数。攻击者要想得到该会话密钥，需要从截获的消息中推导出 r_i 或者 r_G，这相当于求解椭圆曲线离散对数问题的难度，这种攻击方式在计算上是不可行的。因此，本文方案提出的认证方案可以实现安全的会话密钥协商。

3) 防止非法接入。当有用户想要在票据失效后或者已注销的用户想要再次连接该网络时，FNCC 通过查阅 FG 和 HNCC 发送的数据可找出失效或非法的用户，FNCC 再通过安全信道把名单发送给 HNCC，HNCC 根据其真实信息针对错误给出惩罚措施。

4) 条件匿名性及可追踪性。本文方案中，用户在可信网络控制中心上注册时，网络控制中心会为其生成临时伪身份，且传输的访问消息 $\{\mathrm{msg}_i, R_i, S_i, T_{\mathrm{END}}, T_i^1\}$ 中包含的也是临时伪身份。由于哈希函数单向性的特点，攻击者和其他参与认证的网络实体（接入卫星、网关）无法通过伪造的身份来冒充合法用户。然而用户的身份信息并不是完全可匿的，当用户在漫游期间做出非法的行为时，归属域网络控制中心可以通过 x_i 来计算出用户的真实身份，这样就实现了漫游方案的可追踪性。

5) 抗重放攻击。访问请求以及响应消息、预协商消息都包含时间戳。且对消息的签名中也对时间戳进行了哈希处理，攻击者无法篡改接入请求消息中的时间戳。一旦时间戳被修改，等式不再成立，接入卫星将拒绝接受该接入请求消息，同时通过检查时间戳和等式 $a=H_2(T\|\mathrm{pk})$ 可以找到重放消息。因此，所提方案能够抵抗重播攻击。

6) 抗 DoS 攻击。本文方案中，用户使用 T_{END} 来实现基本认证，而 T_{END} 是基于用户的身份生成的，是有时效性的，过期作废，因此 HNCC 不需要存储海量与用户的验证信息，且本文方案中设计的动态撤销机制可以删除过期的身份信息，通过简单的查询就可以验证用户的合法性，消耗极少的资源，因此无法实施 DoS 攻击。

为了显现所提方案的安全性，本文进一步将其与卫星网络中现有的其他认证方案进行了比较，具体如表 2 所示。

表 2　　安全性对比

方案	双向认证	匿名性	可追踪性	抗重放攻击	抗 DoS 攻击
文献[15]方案	√	×	√	√	×
文献[22]方案	√	√	√	√	×
文献[25]方案	√	√	×	√	√
本文方案	√	√	√	√	√

6 性能分析

本节基于安全目标对本文方案的计算开销、通信开销以及算法实现效率方面与现有方案进行比较。此外，本节分析了本文方案批量身份验证的优势，并给出了仿真结果。因为用户只在 HNCC 上注册一次，所以不考虑注册阶段的计算开销。

6.1 计算开销

对于漫游身份验证时延，本文将其定义为整个

身份验证过程的总时间成本，包括计算和传播时延的时间成本，即各个认证实体执行密码学操作所需的计算时延以及各个实体间交互造成的通信时延，计算式如下。

认证时延=计算时延+传输时延

其中，通信时延取决于实体之间信号的传播时延以及交互次数。因为验证过程主要由点乘法、点加法和哈希运算这几个操作来完成，为了方便评估计算成本，本文在方案比较过程中忽略哈希运算带来的时延，使用 Intel(R)Core(TM) 2.20 GHz 处理器上的 JPBC[29]代码仿真了密码术操作的时间成本分别为点乘法 T_{m} = 0.082 ms 和点加法 T_{a} = 0.073 ms。用户与卫星、卫星与网关、网关与服务器之间的信号传播时间成本分别表示为 T_{u-l}、T_{l-g}、T_{g-n}。由于卫星与地面距离为 500～2 000 km，因此设置 T_{u-l} = T_{l-g} = 10 ms。进行了大量实验并参考网上示例后，本文将移动用户连接到网络控制中心所需的时间设置为 20 ms。为便于比较认证时延，本文假设网关与网络控制中心之间的传播时延 T_{g-n} 为 10 ms。

本文方案需要执行 7 次椭圆双曲线点乘算法、2 次椭圆双曲线点加算法，而文献[22-24]方案则分别需要执行椭圆双曲线点乘算法 9 次、10 次、11 次，以及椭圆双曲线点加算法 4 次。批量认证时延数值分析如图 7 所示。从图 7 可以看出，本文方案在执行身份验证阶段所需的总时间（即本文方案成功进行切换身份验证所需的总时间）比文献[22-24]方案少得多。这是因为本文方案采用高效的操作，并且操作成本比其他方法低得多。因此，本文方案更适合于 SIN 为移动终端提供更好的接入服务。

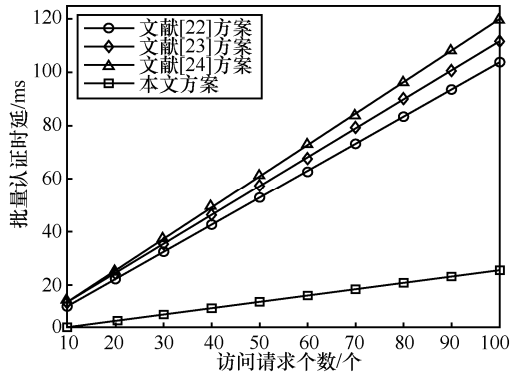

图 7 批量认证时延数值分析

6.2 批验证的评估

当卫星同时接收到来自多个用户的大量访问请求时，可以执行批量身份验证以显著减少卫星的计算开销。处理单个身份验证、n 个没有批处理验证的身份验证、文献[22]中 n 个有批处理验证以及本文方案中 n 个有批处理验证的系统验证开销数值分析如图 8 所示。结果表明，当 n 个用户同时转发其访问认证请求时，卫星通过本文方案的批量验证的操作可以显著降低计算成本。

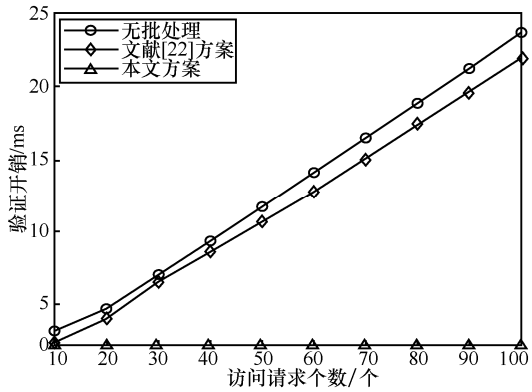

图 8 系统验证开销数值分析

7 结束语

本文针对空间信息网络漫游服务中存在的通信质量以及安全问题，引入了一种新型批量认证方案来提高身份验证的效率。本文方案考虑到卫星的运行轨迹可预测的特点，通过用户提前自主聚合公钥及签名来减轻卫星的验证负担，大大减少了冗余的身份验证，保障了空间信息网络的通信质量，而且专门为漫游方案设计了撤销机制以支持用户动态撤销。安全性分析表明，本文方案可以抵抗重放等传统攻击。性能分析结果表明，本文方案在满足可追踪性、匿名性、可撤销性等安全要求的同时效率优于其他方案。

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.

[2] KHALILI H, KHODASHENAS P S, SIDDIQUI S. On the orchestration of integrated satellite components in 5G networks and beyond[C]//Proceedings of 2020 22nd International Conference on Transparent Optical Networks (ICTON). Piscataway: IEEE Press, 2020: 1-4.

[3] ZHANG J X, ZHANG X, WANG P, et al. Double-edge intelligent

integrated satellite terrestrial networks[J]. China Communications, 2020, 17(9): 128-146.

[4] 薛开平, 马永金, 洪佳楠, 等. 天地一体化网络中基于令牌的安全高效漫游认证方案[J]. 通信学报, 2018, 39(5): 48-58.
XUE K P, MA Y J, HONG J N, et al. Secure and efficient token based roaming authentication scheme for space-earth integration network[J]. Journal on Communications, 2018, 39(5): 48-58.

[5] LARCOM J A, LIU H. Modeling and characterization of GPS spoofing[C]//Proceedings of 2013 IEEE International Conference on Technologies for Homeland Security. Piscataway: IEEE Press, 2013: 729-734.

[6] SHENG J, CAI X Q, LI Q Y, et al. Space-air-ground integrated network development and applications in high-speed railways: a survey[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, PP(99): 1-20.

[7] SCHRAML M G, SCHWARZ R T, KNOPP A. Multiuser MIMO concept for physical layer security in multibeam satellite systems[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1670-1680.

[8] KALANTARI A, ZHENG G, GAO Z, et al. Secrecy analysis on network coding in bidirectional multibeam satellite communications[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1862-1874.

[9] 徐国愚, 陈性元, 杜学绘. 一种新的基于上下文传递的临近空间安全切换机制[J]. 计算机科学, 2013, 40(4): 160-163.
XU G Y, CHEN X Y, DU X H. New near space security handoff scheme based on context transfer[J]. Computer Science, 2013, 40(4): 160-163.

[10] SU K, DONG Q Z, ZHU W Q. Space information security and cyberspace defense technology[C]//Proceedings of 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. Piscataway: IEEE Press, 2013: 1509-1511.

[11] DING X H, ZHANG Z L, LIU D P. Low-delay secure handover for space-air-ground integrated networks[C]//Proceedings of 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications. Piscataway: IEEE Press, 2020: 1-6.

[12] CRUICKSHANK H S. A security system for satellite networks[C]//Proceedings of the Fifth International Conference on Satellite Systems for the Mobile Communications and Navigation. London: IET, 1996: 187-190.

[13] HWANG M S, YANG C C, SHIU C Y. An authentication scheme for mobile satellite communication systems[J]. ACM SIGOPS Operating Systems Review, 2003, 37(4): 42-47.

[14] CHANG Y F, CHANG C C. An efficient authentication protocol for mobile satellite communication systems[J]. ACM SIGOPS Operating Systems Review, 2005, 39(1): 70-84.

[15] WANG Y, ZHANG W F, WANG X M. A lightweight and secure authentication protocol for space-ground integrated network of railway[C]//Proceedings of 2021 International Conference on Communications, Information System and Computer Engineering (CISCE). Piscataway: IEEE Press, 2021: 30-35.

[16] ZHANG Y H, DENG R H, BERTINO E, et al. Robust and universal seamless handover authentication in 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 858-874.

[17] XUE K P, MENG W, ZHOU H C, et al. A lightweight and secure group key based handover authentication protocol for the software-defined space information network[J]. IEEE Transactions on Wireless Communications, 2020, 19(6): 3673-3684.

[18] 周彦伟, 杨波, 张文政. 异构无线网络可控匿名漫游认证协议[J]. 电子学报, 2016, 44(5): 1117-1123.
ZHOU Y W, YANG B, ZHANG W Z. Controllable and anonymous roaming protocol for heterogeneous wireless network[J]. Acta Electronica Sinica, 2016, 44(5): 1117-1123.

[19] 刘丹, 石润华, 张顺, 等. 无线网络中基于无证书聚合签名的高效匿名漫游认证方案[J]. 通信学报, 2016, 37(7): 182-192.
LIU D, SHI R H, ZHANG S, et al. Efficient anonymous roaming authentication scheme using certificateless aggregate signature in wireless network[J]. Journal on Communications, 2016, 37(7): 182-192.

[20] 许芷岩, 吴黎兵, 李莉, 等. 无线漫游认证中可证安全的无证书聚合签名方案[J]. 通信学报, 2017, 38(7): 123-130.
XU Z Y, WU L B, LI L, et al. Provably secure certificateless aggregate signature scheme in wireless roaming authentication[J]. Journal on Communications, 2017, 38(7): 123-130.

[21] WANG L, ZHANG X J, ZHANG A Q, et al. EGIP: an efficient group identification protocol in roaming network[C]//Proceedings of 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). Piscataway: IEEE Press, 2017: 1280-1284.

[22] XUE K P, MENG W, LI S H, et al. A secure and efficient access and handover authentication protocol for Internet of things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.

[23] MENG W, XUE K P, XU J, et al. Low-latency authentication against satellite compromising for space information network[C]//Proceedings of 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems. Piscataway: IEEE Press, 2018: 237-244.

[24] IBRAHIM M H, KUMARI S, DAS A K, et al. Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks[J]. Security and Communication Networks, 2016, 9(18): 5563-5580.

[25] GUO J Y, DU Y. A secure three-factor anonymous roaming authentication protocol using ECC for space information networks[J]. Peer-to-Peer Networking and Applications, 2021, 14(2): 898-916.

[26] FAN B, ANDERSEN D G, KAMINSKY M, et al. Cuckoo filter: practically better than bloom[C]//Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies. New York: ACM Press, 2014: 75-88.

[27] 唐郑熠, 李祥. Dolev-Yao 攻击者模型的形式化描述[J]. 计算机工程与科学, 2010, 32(8): 36-38, 45.
TANG Z Y, LI X. The formalization description of the Dolev-Yao intruder model[J]. Computer Engineering & Science, 2010, 32(8): 36-38, 45.

[28] BLANCO V, GONZÁLEZ P, CABALEIRO J C, et al. AVISPA: visualizing the performance prediction of parallel iterative solvers[J]. Future Generation Computer Systems, 2003, 19(5): 721-733.

[29] DE C A, IOVINO V. jPBC: Java pairing based cryptography[C]// Proceedings of 2011 IEEE Symposium on Computers and Communications. Piscataway: IEEE Press, 2011: 850-855.

[作者简介]

张应辉（1985− ），男，陕西西安人，博士，西安邮电大学教授，主要研究方向为公钥密码学、云安全和无线网络安全。

胡凌云（1998− ），女，安徽马鞍山人，西安邮电大学硕士生，主要研究方向为无线网络安全和通信协议安全。

李艺昕（1996− ），女，陕西西安人，西安邮电大学硕士生，主要研究方向为云安全和无线网络安全。

宁建廷（1988− ），男，浙江衢州人，博士，中国科学院教授，主要研究方向为公钥密码学和云安全。

郑东（1964− ），男，山西临汾人，博士，西安邮电大学教授，主要研究方向为编码密码学和网络安全。