天地一体化网络中基于令牌的安全高效漫游认证方案

薛开平，马永金，洪佳楠，许婕，杨青友
（中国科学技术大学电子工程与信息科学系，安徽 合肥 230026）

摘 要：针对天地一体化网络中卫星和地面实体通信链路时延长、不稳定的问题，提出一种基于令牌的两方漫游认证方案。该方案利用网络中卫星节点具有一定计算能力的特性，将用户认证过程从网络控制中心（NCC）提前到接入卫星，由卫星直接检验 NCC 颁发的令牌来验证用户的身份；同时，基于单向累加器的令牌机制，实现了用户的动态加入、轻量级的用户自主业务定制和计费；并通过 Bloom Filter 的引入实现有效的用户撤销和恶意接入控制。和已有的方案相比，该方案在保证漫游认证的安全性同时，显著减少了认证和密钥协商过程的计算和通信开销。

关键词：天地一体化；漫游认证；令牌；单向累加器
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018076

Secure and efficient token based roaming authentication scheme for space-earth integration network

XUE Kaiping, MA Yongjin, HONG Jia’nan, XU Jie, YANG Qingyou
Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China

Abstract: Aiming at the problem of prolongation and instability of satellite and terrestrial physical communication links in the space-earth integration network, a two-way token based roaming authentication scheme was proposed. The scheme used the characteristics of the computing capability of the satellite nodes in the network to advance the user authentication process from the network control center (NCC) to the access satellite. The satellite directly verified the token issued by the NCC to verify the user's identity. At the same time, the token mechanism based on the one-way accumulator achieved the user's dynamic join, lightweight user self-service customization and billing,and the introduction of Bloom Filter enabled effective user revocation and malicious access management. Compared with the existing scheme, the scheme can guarantee the security of roaming authentication and significantly reduce the calculation and communication overhead of the authentication and key negotiation process.

Key words: space-earth integration, roaming authentication, token, one-way accumulator

1 引言

随着航天技术、卫星通信技术的高速发展，以及用户对网络全球化的迫切需求，卫星网络与地面网络融合组建天地一体化网络已经成为学术界和工业界的重要方向[1]。该网络以卫星网络为骨干，以地面网络为基础，实现空、天、地、海等多维网络的融合。相比传统无线网络，如蜂窝网络，它具有广域覆盖、不受地理限制、抗毁、应急能力强的优点。作为传统地面网络的扩充，边远地区、灾区、航海等场景下用户对接入天地一体化网络存在迫切的需求。

漫游业务是天地一体化网络中必须实现的服

收稿日期：2017-11-08；**修回日期**：2018-03-22
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800301）；国家自然科学基金资助项目（No.61379129）
Foundation Items: The National Key Research and Development Plan of China (No.2016YFB0800301), The National Natural Science Foundation of China (No.61379129)

务之一，因为这种异构、融合的网络中用户的漫游不可避免，如从传统的无线网络漫游到卫星网络，或在不同域天地一体化网络漫游。然而，由于卫星网络固有的特点，实现安全高效的漫游认证方案面临着许多挑战。一方面，无线信道的开放性使恶意用户可以通过监听信道窃取用户隐私或通过伪造、重放、中间人攻击破坏漫游协议，损害合法用户的权益[1]。另一方面，卫星和地面实体的高传播时延会给设计低延时的漫游方案带来严重的挑战。此外，卫星链路的高度动态性和不稳定性也使高时延消耗的漫游机制难以在天地一体化网络中实施。

现有的卫星网络无漫游认证协议而只有接入认证协议，主要有文献[2~4]。它们能提供用户和网络的双向认证，并进行密钥协商等，但不适合多域的漫游场景，且这些认证协议需要到网络控制中心或地面站认证用户的身份，认证时延大。另外，传统无线网络中的漫游认证协议，如文献[5,6]，尽管能保障漫游安全，包括漫游认证、匿名性、密钥协商等。但是这些漫游协议应用到天地一体化场景中会带来巨大的认证时延。因为在传统的卫星网络场景下，卫星只负责转发认证消息，认证过程由网络控制中心或地面站完成。因此，本文将针对天地一体化网络的特点，提出一种安全高效的漫游认证方案。

本文基于低轨卫星作为网络接入点的场景，立足于卫星具有一定计算能力的前提，设计了一种基于令牌的双方漫游认证方案。在本文的系统中，令牌是代表固定服务量（通话时长，流量）的入网凭据。用户根据自己的需求向网络控制中心（NCC，network control center）申请一定数目的令牌。本文将认证功能由 NCC 提前到卫星上，认证过程由携带令牌的漫游用户和卫星直接完成，大大减少了传播时延，且基于单向累加器生成的令牌，不仅初始化简单，一次模指数计算的认证过程还使认证过程计算开销小，进一步缩短认证时延。本文基于单向累加器的单向性设计令牌的计费方式。这种计费方式可以做到漫游域网络根据提供的总服务量向归属域网络收费；归属域网络也根据用户使用过的令牌数目向用户收费；用户多申请但没有使用的令牌不额外收费。另外，本文通过修改单向累加器密码学算法使令牌机制支持用户动态加入和自主业务定制，并通过引入 Bloom Filter 使漫游用户的身份可以随时撤销，同时防止恶意用户的接入。

2　相关工作

近年来，随着卫星网络的高速发展，许多卫星认证协议被提出。在 1996 年，Cruickshank[7]首先提出了卫星网络的认证模型，并提出了基于公钥密码体制的认证方案。但是该方案计算开销大，而且存在重放攻击，只能实现卫星对用户的单向认证。Hwang 等[8]提出了基于预共享密钥的认证方案。在此方案中，用户和 NCC 利用预共享密钥加密随机数实现双向认证。每次认证完后，NCC 会向用户发送新的预共享密钥和随机数实现密钥的更新，防止重放攻击。该方案相比文献[7]更高效，然而密钥存储开销大。Chang 等[9]的方案和 Hwang 类似，前者把后者中的加密函数换为高效的散列函数来提高认证效率，并且通过 DH (Diffie-Hellman)交换和反向散列链实现密钥更新。Chen 等[10]结合公钥密码体制和预共享密钥提出了一种新的认证方案，该方案既能实现双向认证，还能具有较低的认证开销和密钥更新开销。Chen 等[2]和 Zhao 等[3]根据现有方案的安全漏洞，提出了更安全的认证方案。他们的方案能防止恶意用户攻击，保护用户隐私。然而，由于天体一体化网络的多域漫游特征以及天地网络实体的高传播时延，这些方案不能直接应用到漫游场景中。

传统无线网络的漫游认证协议也不断被完善。Jiang 等[11]提出了一种基于秘密分割的匿名漫游协议，该方案具备匿名性，但是不具备不可追踪性。而且认证服务器两两之间需要共享会话密钥，这使系统难以管理，可扩展性差。公钥密码体制随即广泛用于实现无线网络中的漫游认证，用来克服对称密钥体制中的缺点。Yang 等[12]结合了无线漫游中的安全需求，提出了匿名无线漫游协议的整体框架结构。之后，Yang 等[13]在此结构框架基础上，进一步提出一种基于 DH 交换和公钥证书的无线漫游协议，并给出了详细的安全性分析。虽然相对于对称密钥体制而言，该方案更具备一定的灵活性以及很强的可扩展性。但是，由于 PKI 系统需要对证书进行大量处理，尤其是认证时需要在无线信道上传递证书并在终端进行证书的验证，严重增加了网络负载及移动终端的计算量。为了避免这类弊端，提出了不同的基于身份的认证协议。He 等[5]利用群签名机制实现了具有用户匿名性的漫游方案，然而该方案需要不断更新和检查用户撤销列表，用户撤销开

销大。针对此，Liu 等[6]提出了一种不需要用户撤销列表的群签名漫游方案。它将生存时间写入到用户的私钥中，过期的用户将会被漫游域 NCC 检测出而自动失效，大大节约了因用户撤销而造成的开销。尽管上述传统网络的漫游认证方案能提供安全性保障，但是在传统的卫星网络场景下，卫星和地面站的高传播时延将会导致无法忍受的高认证时延。

因此，这些方案无法直接应用到天地一体化漫游场景中。本文基于天地一体化网络的特异性，提出了一种基于令牌的双方漫游认证协议，不仅保证了安全性，还极大减少了认证时延。

3 预备知识

3.1 单向累加器

单向累加器的概念最早由 Benaloh 和 Mare 提出[14]，用于验证某个元素是否在一个指定的集合中。安全的单向累加器函数族是一个有限的函数 $f: X \times Y \to X$ 的集合且满足 3 个属性。

1) 计算有效性（computing availability）：存在一个多项式 P，对每个给定的整数 k，对所有的 $x \in X$ 以及所有的 $y \in Y$， $f(x,y)$ 是在 $P(k)$ 时间内可计算的。

2) 单向性(unidirection)：不存在多项式 P，使存在一个概率多项式时间算法 A_k，对任意给定的足够大的 k，随机给定 $(x,y) \in (X,Y)$， $y' \in Y$， A_k 找到 $x' \in X$，$(x,y) \neq (x',y')$，使等式 $f(x,y) = f(x',y')$ 成立的概率小于 $\frac{1}{P(k)}$。

3) 拟交换性（quasi-commutativity）：对所有的 $x \in X$， $y_1, y_2 \in Y$ 满足

$$f(f(x,y_1),y_2) = f(f(x,\ y_2),y_1) \tag{1}$$

单向累加器常用于成员验证（membership testing）[14]，定义集合 $Y' = \{y_1, y_2, \cdots, y_m\}$ 的累加值为 $f(f(\cdots f(f(x,y_1),y_2)\cdots, y_{m-1}), y_m)$。假设有 m 个元素，则 z 为集合 $Y = \{y_1, y_2, \cdots, y_m\}$ 的累加值，z_i 为集合 $Y_i = \{y_1, y_2, \cdots y_{i-1}, y_{i+1}, \cdots, y_{m-1}, y_m\}$ 的累加值。当单向累加器被用来验证群组成员时，系统公布 z，并颁发令牌 (z_i, y_i) 给成员。成员向验证者提供令牌，验证者计算 $f(z_i, y_i)$ 是否和 z 相等，若相等，则成员属于群组。f 的准交换性保证了一组数据按不同的顺序进行累加，所得的结果是相同的，也保证了上述等式的准确性。f 的安全性体现在它的单向性，即给定 $x \in X, y \in Y$，对 $y' \in Y$，找到满足 $f(x,y) = f(x',y')$ 是困难的。

Benaloh 和 Mare 在文献[14]中证明该单向累加器在强 RSA 假设的前提下是安全的，定义 $f(x,y) = e_n(x,y) = x^y \bmod n$；$e_n : QR_n \times Z_N^* \to QR_n$。$p,q$ 为 2 个大素数，且满足 $\frac{p-1}{2}$ 和 $\frac{q-1}{2}$ 均为大素数，$n = pq$。在本文方案中，令 $f(x,y) = x^y \bmod n$。

3.2 Bloom Filter

Bloom Filter[15]是一种高效的数据结构。它利用精简的比特数组来代表一个数据集。初始时候长度为 m 的比特数组置为全 0。在 Bloom Filter 的构建过程中，利用数据集中的每一个字符串作为 k 个散列函数的输入，输出 k 个 $[0, m-1]$ 的值。对每一个输出值，将数组相应位置置 1。如果相应位置已经是 1，就不再处理。在数据查询阶段，对查询的字符串也做同样的 k 次散列运算。检查比特数组相应 k 个位置的值是否全为 1，若有一位为 0，则表示该字符串一定不在这个数据集。若全为 1，则以一定的误判率判定该字符串属于该数据集。文献[15]通过数学分析得到的误判率为

$$f = (1 - \mathrm{e}^{-\frac{nk}{m}})^k \tag{2}$$

其中，n 为数据集的元素个数。由求导计算得当 $k = \left(\frac{m}{n}\right)\ln 2$ 时，误判率最低。

本文方案利用 Bloom Filter 来存储已使用过的或已撤销的令牌，实现失效令牌在卫星网络上的轻量级传输，能有效防止失效令牌的使用，进一步实现了漫游用户的管理和计费。

4 系统和安全模型

4.1 系统模型

系统模型如图 1 所示。在天地一体化网络的漫游场景下，用户离开归属域网络进入到漫游域网络。漫游域网络根据与归属域网络的协议对漫游用户进行认证，并提供网络接入服务。在本文方案中，系统模型主要包括以下几个实体：漫游用户（U）、低轨卫星（LEO）、地面站（GS）、网络控制中心（NCC）。下面是主要实体的具体描述。

1) 漫游用户（U）

在漫游场景下，U 作为移动实体，离开归属域网络进入到漫游域网络，并获得网络接入服务。在

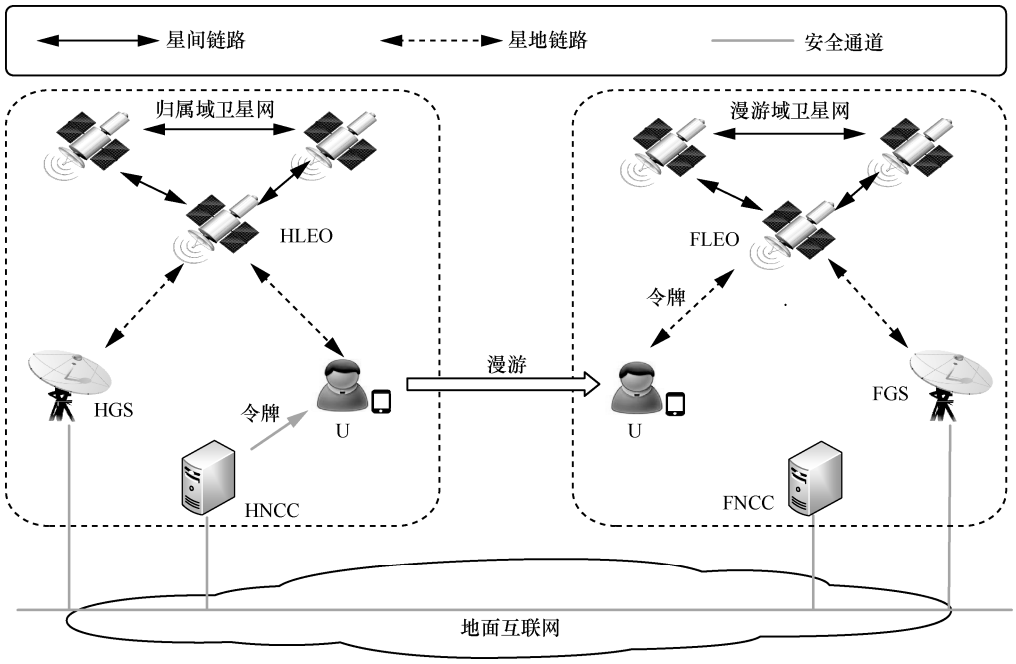


图 1　天地一体化网络漫游认证架构

本文方案中，U 向归属域 NCC（HNCC）申请漫游服务，HNCC 给 U 颁发漫游凭据令牌。漫游域网络认证 U 的令牌，并提供固定的网络服务。

2) 低轨卫星（LEO）

LEO 作为天地一体化网络的接入点，连接用户和地面站，具有一定的计算和存储能力[16]。在本文方案中，漫游域 LEO(FLEO)参与漫游认证过程，进一步减少认证时延。

3) 地面站（GS）

GS 连接卫星网络和地面互联网。用户可通过 GS 连入地面互联网。卫星也可通过 GS 与 NCC 进行通信。漫游时，U 通过漫游域 GS(FGS)连入地面互联网中。

4) 网络管理中心（NCC）

NCC 是所在域网络的管理中心。根据所在域不同，又可分为归属域 NCC（HNCC）和漫游域 NCC(FNCC)。在本文方案中，HNCC 与 FNCC 签署了漫游协议。HNCC 给 U 颁发令牌。漫游域网络对令牌进行认证。FNCC 收集 U 使用过的令牌向 HNCC 收取费用。

4.2　安全模型及安全需求

由于天地一体化网络信道的暴露性，任何用户均可通过监听信道获得通信数据。因此，攻击者可以通过窃听来获取合法用户的传输信息。另外，攻击者可以利用窃听到的数据进行篡改、重放或中间人攻击，假扮合法用户，从而欺骗系统，非法接入网络。

在漫游认证过程中，用户固定的身份信息会暴露用户的隐私，因为攻击者可以利用身份信息锁定用户的地理位置。这种危害在军事行动中尤为突出，敌方可以通过监听信道掌握我方的动向。完全的匿名性伴随的是不可审计性，这不利于漫游的计费以及对非法用户的追责。因此，用户的身份既要对其他用户匿名性，又要保证可追踪性，这种看似矛盾的要求是天地一体化网络的挑战。鉴于上述提出的天地一体化网络中的安全挑战，本文提出下列安全需求。

1) 双向认证：漫游域网络要对 U 进行认证，防止非法用户使用网络资源。同时，U 也要认证 FLEO，防止伪 FLEO 获取用户隐私并进行一系列恶意攻击。

2) 密钥协商：在相互认证完毕后，U 要和 FGS 协商出会话密钥，用于后续数据的认证和加密，防止攻击者伪造数据以及通过公开信道窃听数据。

3) 匿名性：U 的身份对其他用户匿名，但是 HNCC 能够揭露 U 的真实身份。

4.3　安全假设

基于上述安全模型和安全，本文做出下列安全假设。

1) HNCC 完全可信。它向 U 颁发令牌用于漫游服务，不可能被任何敌手攻破。

2) 漫游域网络实体半可信。它们遵循与归属域

的漫游协议，向合法 U 提供网络服务，但是为了谋取更多利益，漫游域网络实体可能伪造令牌用于向 HNCC 收取额外的费用。

3) 其他用户不可信。他们尝试破解本文提出的漫游认证方案。例如，试图破解合法 U 的隐私或伪造合法 U 的身份。

4) 不失一般性，本文假设用户与 HNCC、地面站与 HNCC、卫星与地面站之间存在安全通道。

5 漫游认证方案

本文先简要地介绍提出的漫游认证方案；然后详细描述方案细节，包括系统初始化及用户注册、预协商、漫游认证及密钥协商、用户动态加入及令牌动态补充、令牌失效及用户动态撤销、令牌计费。

为了描述方便，表 1 列举了方案中涉及的相关实体的符号定义。

表 1 实体符号定义

符号	定义
U (roaming user)	漫游用户
LEO (low earth orbit satellite)	低轨卫星
FLEO (foreign LEO)	漫游域低轨卫星
NCC (network control center)	网络控制中心
HNCC (home NCC)	归属域网络控制中心
FNCC (foreign NCC)	漫游域网络控制中心
GS (ground station)	地面站
FGS (foreign GS)	漫游域地面站

5.1 方案概述

漫游认证方案如图 2 所示。在系统初始化阶段，HNCC 通过 FNCC 向漫游域低轨卫星广播已撤销的令牌标识 y_i，卫星存入到 Bloom Filter 中。HNCC 给 U 颁发令牌。FGS 通过预协商将密钥协商参数 bP 和 FNCC 传来的用户暂时身份标识组 TMSI 发送给 FLEO。其中，P 为椭圆曲线的生成元，是系统公布参数，b 为 FGS 生成的随机数。待 U 进入漫游域时，他向 FLEO 出示令牌并发送密钥协商参数 aP。FLEO 验证令牌的合法性后，将从 TMSI 中随机抽取的标识 TMSI_i 和 bP 一起发送给 U。TMSI_i 用于后续对 U 提供定量的网络服务，并进行域内的管理和监督；bP 用于密钥协商。与此同时，FLEO 将 aP 和 y_i 发送给 FGS。aP 用于密钥协商；y_i 发送给 FNCC 用于向 HNCC 收取费用。最后 FLEO 将已认证过的 y_i 广播给其余卫星，防止令牌重用。由于 FLEO 直接验证用户的合法性，避免了地面站或 NCC 的直接参与，大大减少传播时延，且令牌也基于单向累加器产生，相比于其他认证方案，验证高效，大大减少了计算时延。

5.2 系统初始化及用户注册

NCC 利用单向累加器为每个卫星颁发身份验证凭据 (z_i', y_i')，将卫星公共参数 z' 通过安全通道广播给与它签订漫游协议的 NCC。其中 z'、z_i' 定义为

$$z' = f(\cdots f(x', y_1')\cdots, y_l') \tag{3}$$

$$z_i' = f(\cdots f(f(\cdots f(x', y_1')\cdots, y_{i-1}'), y_{i+1}')\cdots, y_l') \tag{4}$$

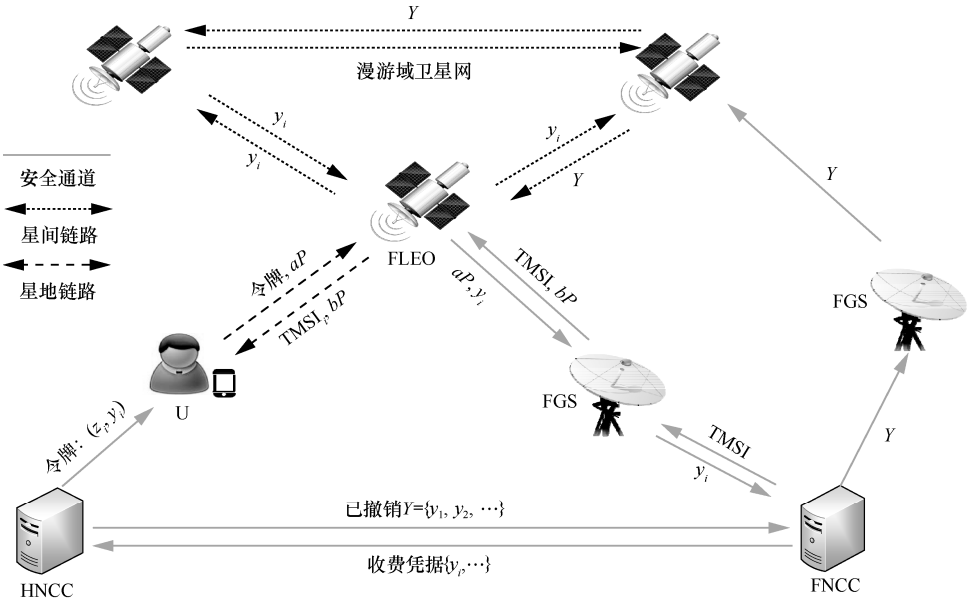


图 2 漫游认证方案

其中，y_i'为满足等式的自然数，l 为卫星数目。

在本文方案中，一个令牌代表一定的服务量（通话时长，流量），U 根据自己的需求向 HNCC 申请一定数目的令牌。HNCC 利用用户公共参数 z 为 U 分配令牌。z 有固定的有效期，以一个月为例。HNCC 在不同的月份用不同的 z 生成令牌。HNCC 将 12 个月份的 z 发送给与它签订漫游协议的 FNCC。FNCC 广播给域内所有低轨卫星。低轨卫星在不同的月份用相应的 z 验证令牌的合法性。令牌为 (z_i, y_i)，y_i 为满足等式的自然数，m 为令牌总数目，其他参数定义为

$$z = f(\cdots f(x, y_1)\cdots, y_m) \tag{5}$$

$$z_i = f(\cdots f(f(\cdots f(x, y_1)\cdots, y_{i-1}), y_{i+1})\cdots, y_m) \tag{6}$$

用户注册时，HNCC 将用户申请的令牌以及漫游域卫星公共参数 z' 通过安全通道发送给用户。每个卫星维护一个由系统撤销或已使用过的令牌标识 y_i 构建的 Bloom Filter。初始时候，HNCC 通过安全通道向 FNCC 传输当月已撤销的 y_i。FNCC 再通过安全通道向所在域所有低轨卫星广播这些 y_i。卫星将这些 y_i 添加到 Bloom Filter 中。

5.3　预协商

预认证过程如图 3 所示。FNCC 将域内暂时身份标识组 TMSI 通过安全通道传输给 FGS，且给不同的 FGS 传输不同的 TMSI 从而防止身份重用。FGS 生成密钥协商参数 bP，FGS 将 TMSI 和 bP 通过安全通道发送给 FLEO。

5.4　漫游认证及密钥协商

这个阶段发生在 U 移动到漫游域网络，并且向网络发起接入请求。U 首先和 FLEO 进行双向认证，接着通过 FLEO 和 FGS 协商出会话密钥。认证过程如图 3 所示，下面描述具体细节。

第一步，U 产生随机数 a，计算 aP，并结合当前的时间戳 ts_{U} 计算出散列值 $s_1 = h(aP \| ts_{\mathrm{U}})$。再通过 s_1 和令牌中的 z_i 产生认证载荷 $R_1 = f(z_i, s_1)$。最后 U 将密钥协商参数 aP、y_i、R_1，归属域标识 NETID，ts_{U} 一起发给 FLEO。

第二步，当 FLEO 收到 U 发来的接入请求载荷后，它首先验证传播时延 $t_{\mathrm{now}} - ts_{\mathrm{U}}$ 是否在可接受的阈值 Δt 以内。如果超出阈值，则认为此为重放分组，拒绝 U 的接入。如果未超出阈值，FLEO 将 y_i 作为查询元素，通过 Bloom Filter 检查令牌是否失效。若令牌失效，则 FLEO 拒绝 U 的接入。若令牌未失效，FLEO 通过 aP 和 ts_{U} 生成 s_1，并根据域 NETID 颁发的 z 验证等式 $f(R_1, y_i) = f(z, s_1)$ 是否成立。若不成立，同样拒绝用户接入。若成立，则认为 U 合法，继续执行下列步骤。FLEO 结合当前的时间戳 ts_{SAP} 和 FGS 发来的 bP 计算散列值 $s_2 = h(bP \| ts_{\mathrm{SAP}})$，接着利用 HNCC 颁发的身份验证

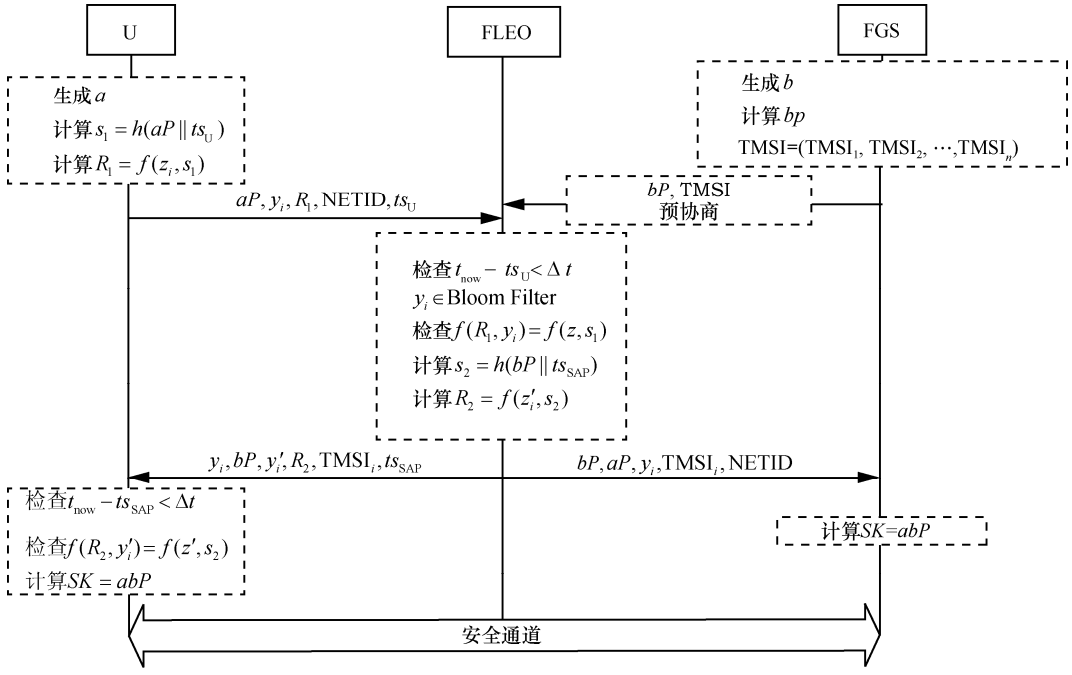


图 3　漫游认证及密钥协商

凭据产生认证载荷 $R_2 = f(z_i', s_2)$，然后随机从 TMSI 中选择一个 TMSI_i，将接入应答 $\{y_i, bP, y_i', R_2, \text{TMSI}_i, ts_{\text{SAP}}\}$ 发送给 U 同时将 $\{bP, aP, y_i, \text{TMSI}_i, \text{NETID}\}$ 通过安全通道发送给 FGS。最后，FLEO 将 y_i 插入到 Bloom Filter 中，并向所在域其他低轨卫星广播 y_i。其他卫星收到 y_i 后做同样操作。

第三步，U 收到 FLEO 发来的接入应答后，它首先验证传播时延 $t_{\text{now}} - ts_{\text{SAP}}$ 是否在可接受的阈值 Δt 以内。如果超出阈值，则认为是重放分组，忽略 FLEO 的应答。如果未超出阈值，U 通过 bP 和 ts_{SAP} 生成 s_2，并验证等式 $f(R_2, y_i') = f(z', s_2)$ 是否成立。若不成立，则认为 FLEO 非法，同样忽略 FLEO 的应答。若成立，计算会话密钥 $SK = abP$。FGS 收到卫星的应答分组后，也计算出和 U 共享的会话密钥 $SK = abP$，并将 y_i 和 NETID 发送给 FNCC，用于后续的计费。

至此，U 和 FGS 协商出共享的会话密钥，从而建立了安全通道。认证结束后，U 获得漫游域网络的暂时身份标识 TMSI_i，相当于漫游域的其他合法用户。漫游域网络根据本域规则对 U 进行管理和监督，并提供令牌包含的定量网络服务。

5.5 用户动态加入和令牌动态补充

在实际网络运营过程中，用户可能随时向 HNCC 申请新的令牌，包括新漫游用户因为需要漫游而申请令牌或老漫游用户因为令牌数目不足而申请新的令牌。所以，合理的方案必须要满足即使在系统初始化和用户注册完毕后，用户仍能申请令牌，即能实现令牌的动态加入。令牌动态加入过程如下：假设当月的用户公共参数为 z，HNCC 产生一个随机数 y_k，y_k 满足和 $(p-1)(q-1)$ 互素且未被使用过，HNCC 生成 z_k，z_k 满足

$$z_k = z^{y_k^{-1} \bmod (p-1)(q-1)} \bmod n \tag{7}$$

其中，$y_k^{-1} \bmod (p-1)(q-1)$ 表示 y_k 关于 $(p-1)(q-1)$ 的逆，用户新申请的令牌为 (z_k, y_k)，由式(7)可知新的令牌仍然满足 $f(z_k, y_k)=z$，即新的令牌有效且不改变原有的令牌。

5.6 令牌失效及用户动态撤销

当令牌被漫游域网络认证后，为了防止令牌重用，FLEO 将 y_i 插入到所维护的 Bloom Filter 中，同时向所在域其他低轨卫星广播已认证的 y_i，其他卫星收到 y_i 后做同样操作。当令牌被认证后，U 会被分配 TMSI_i。后续归属域网络利用 TMSI_i，根据所在域网络规则向 U 提供定量的网络服务。考虑到漫游高峰期可能存在过多漫游用户同时接入网络，FLEO 广播 y_i 开销大，此时，FLEO 可以将这一时间段的 y_i 聚合后再广播给其余低轨卫星。

由于令牌的验证依赖于用户公共参数 z，而 z 有特定的生存周期，卫星在不同月份用相应的 z 认证令牌，所以令牌也有特定的生存周期，它只在对应的月份有效。卫星在新的月份来临的时候清空 Bloom Filter，防止 Filter 无限增大。

由于一些 U 可能非法使用令牌或想申请退出漫游服务，系统需要主动撤销这些 U 的所有令牌来撤销用户。本文设计一套机制来支持用户的动态撤销。HNCC 将撤销用户有效期为当月的令牌 y_i 通过安全通道发送给 FNCC。FNCC 收到消息后，将这些 y_i 通过安全通道广播给所在域的所有低轨卫星。低轨卫星将这些值存入到 Bloom Filter 中。若用户还有剩余令牌没有撤销，则在令牌生效的月初执行撤销操作。

5.7 令牌计费

当 U 认证完毕后，FLEO 将 y_i 通过 FGS 发送给 FNCC。FNCC 利用收集的 y_i 向 HNCC 收取费用。HNCC 也根据用户使用的令牌数目向其收取费用。这样的计费方式有以下优点。

1) 用户享受多少服务就收取多少费用，极大维护用户的权益。

2) 用户即使多申请了额外的令牌也不用主动撤销，因为不使用的令牌不会被计费。

3) 漫游域根据提供的服务量向归属域收取费用，收费公平。

FNCC 可能试图伪造 y_i 向 HNCC 收取额外费用，下面本文证明这种行为不可能发生。令牌 (z_i, y_i) 由 HNCC 通过安全通道发送给 U，其他网络实体包括 FNCC 无法得知未使用过的 y_i。FNCC 可能猜测 y_i，然而由于单向累加器的单向性，以及 y_i 的随机性，猜测的 y_i 不一定准确，HNCC 针对错误的 y_i 给予严厉的惩罚措施可以制止这种行为。

6 安全分析

6.1 双向认证

1) FLEO 认证合法 U

在漫游接入阶段，U 向 FLEO 发送接入请求 $\{aP, y_i, R_1, \text{NETID}, ts_{\text{U}}\}$。由于用户公共参数 z 提前通过安全通道发送给 FLEO，所以 FLEO 可以通过

等式 $f(R_1,y_i)=f(z,s_1)$ 验证令牌的合法性从而验证 U 的身份。等式成立依据为

$$f(R_1,y_i)=f(f(z_i,s_1),y_i)=f(f(z_i,y_i),s_1)=f(z,s_1) \tag{8}$$

考虑攻击者伪造合法 U 身份恶意接入网络。

攻击目标：攻击者构造接入请求分组 $\{aP,y_i,R_1,\mathrm{NETID},ts_U\}$，以使 FLEO 能够检测到 $f(R_1,y_i)=f(z,s_1)$。其中，s_1 和 R_1 满足

$$s_1=h(aP\|ts_U) \tag{9}$$

$$R_1=f(z_i,s_1) \tag{10}$$

攻击资源：攻击者能够获得用户公共参数 z，并且能够获得过去时间内 U 发送的接入请求五元组 $\{aP,y_i,R_1,\mathrm{NETID},ts_U\}$。

攻击者的攻击可形式化为生成新的接入请求五元组 $\{aP,y_i,R_1',\mathrm{NETID},ts_U'\}$。根据攻击方式不同，$y_i$ 可以是伪造的令牌标识或是截获的已知令牌标识。R_1' 为构造的认证载荷，ts_U' 为待攻击的时间点，其他信息 aP 和 NETID 都是已知且可修改的。

若攻击者虚构 U 身份，则 y_i 由攻击者生成。由于 R_1' 由 z_i 和 s_1 经单向累加器函数生成，且 s_1 由已知信息 aP 和 ts_U' 散列生成，所以攻击可进一步归约为构造令牌 (z_i,y_i)。由单向累加器函数的单向性可知，已知 $z=f(z_i,y_i)$，构造 (z_i,y_i) 满足等式在计算上是不可行的。所以攻击者无法虚构 U 身份。

若攻击者截获用户发送的接入请求分组，并且假冒 U 身份，则 y_i 已知。且 R_1' 由 z_i 和 s_1 经单向累加器函数生成，s_1 由已知信息 aP 和 ts_U' 散列生成，所以攻击可进一步归约为构造已知 y_i 的令牌 (z_i,y_i)。已知

$$f(z_i,y_i)=z_i^{y_i}\ \bmod n=z \tag{11}$$

$$f(z_i,s_1)=z_i^{s_1}\ \bmod n=R_1 \tag{12}$$

攻击者可以从已知的 z 和 y_i 或 R_1 和 s_1 的关系中求解出 z_i，且这 2 种方式求解难度相同。在已知 z、y_i 和 n，但 n 的素因子 p 和 q 未知的情况下，求解 z_i 的难度等价于大数分解难题，这在计算上是不可行的。同理，已知 R_1 和 s_1，求解 z_i 在计算上也是不可行的。所以攻击者无法假冒 U 的身份。

综上所述，攻击者无法伪造接入请求分组以通过 FLEO 的验证，因此本方案可以实现 FLEO 认证合法 U 的功能。

2) U 认证合法 FLEO

在漫游应答阶段，FLEO 向 U 发送接入应答 $\{y_i,bP,y_i',R_2,\mathrm{TMSI}_i,ts_{\mathrm{SAP}}\}$。由于卫星公共参数 z' 提前通过安全通道发送给 U，所以 U 可以通过等式 $f(R_2,y_i')=f(z',s_2)$ 验证 FLEO 身份的合法性。等式成立依据为

$$f(R_2,y_i')=f(f(z_i',s_2),y_i')=f(f(z_i',y_i'),s_2)=f(z',s_2) \tag{13}$$

考虑攻击者伪造 FLEO 身份。

攻击目标：攻击者构造接入应答分组 $\{y_i,bP,y_i',R_2,\mathrm{TMSI}_i,ts_{\mathrm{SAP}}\}$，以使 U 能够检测到 $f(R_2,y_i')=f(z',s_2)$。其中，s_2 和 R_2 满足

$$s_2=h(bP\|ts_{\mathrm{SAP}}) \tag{14}$$

$$R_2=f(z_i',s_2) \tag{15}$$

攻击资源：攻击者能够获得卫星公共参数 z'，并且能够获得过去时间内 FLEO 对 U 发送的接入应答六元组 $\{y_i,bP,y_i',R_2,\mathrm{TMSI}_i,ts_{\mathrm{SAP}}\}$。

攻击者的攻击可形式化为生成接入应答六元组 $\{y_i,bP,y_i',R_2',\mathrm{TMSI}_i,ts_{\mathrm{SAP}}'\}$。其中，$y_i$ 为发起接入请求 U 的令牌标识，根据攻击方式不同，y_i' 可以是伪造的卫星身份验证凭据标识或是已知的 FLEO 身份验证凭据标识。R_2' 为构造的认证载荷，ts_{SAP}' 为待攻击的未来时间，其他信息 bP，TMSI_i 都是已知并且可修改的。

若攻击者虚构 FLEO 身份，则 y_i' 由攻击者生成。且 R_2' 由 z_i' 和 s_2 经单向累加器函数生成，s_2 由已知信息 bP 和 ts_{SAP}' 散列生成，所以攻击可进一步归约为构造卫星身份验证凭据 (z_i',y_i')。由单向累加器函数的单向性可知，已知 $z'=f(z_i',y_i')$，构造 (z_i',y_i') 满足等式在计算上是不可行的。所以攻击者也无法虚构 FLEO 的身份。

若攻击者假冒已知 FLEO 身份，则 y_i' 是已知的。且 R_2' 由 z_i' 和 s_2 经单向累加器函数生成，s_2 由已知信息 bP 和 ts_{SAP}' 散列生成，所以攻击可进一步归约为构造已知 y_i' 的卫星身份验证凭据 (z_i',y_i')。已知

$$f(z_i',y_i')=(z_i')^{y_i'}\bmod n=z' \tag{16}$$

$$f(z_i',s_2)=(z_i')^{s_2}\ \bmod n=R_2 \tag{17}$$

攻击者可以从已知的 z' 和 y_i' 或 R_2 和 s_2 的关系中求解出 z_i'，且这 2 种方式求解难度相同。已知 z'、y_i' 和 n，但是 n 的素因子 p 和 q 未知的情况下，求解 z_i' 的难度等价于大数分解难题，这在计算上是不可行

的。同理，已知 R_2 和 s_2，求解 z_i' 在计算上也是不可行的。所以攻击者无法构造已知 y_i' 的卫星身份验证凭据 (z_i', y_i')，即无法假冒已知 FLEO 的身份。

综上所述，攻击者无法伪造接入应答分组以通过 U 的验证，因此，本文方案可以实现 U 认证合法 FLEO 的功能。

6.2 抵抗中间人攻击

攻击目标：在漫游接入阶段，攻击者截获 U 发送的接入请求分组，修改密钥协商参数等信息，伪造新的接入请求分组以被 FLEO 验证通过。在漫游应答阶段，攻击者截获 FLEO 发送的接入应答分组，修改密钥协商参数等信息，伪造新的接入应答分组以被 U 验证通过。

攻击资源：用户公共参数 z，卫星公共参数 z'，U 发送给 FLEO 的接入请求五元组 $\{aP, y_i, R_1, \mathrm{NETID}, ts_{\mathrm{U}}\}$，FLEO 发送给 U 的接入应答六元组 $\{y_i, bP, y_i', R_2, \mathrm{TMSI}_i, ts_{\mathrm{SAP}}\}$。

由 6.1 节所分析的双向认证特性可知，攻击者在截获了 U 发送给卫星的接入请求分组后无法伪造新的接入请求分组以被 FLEO 验证通过，同时攻击者在截获了 FLEO 发送给用户的接入应答分组后也无法伪造新的接入应答分组以被 U 验证通过，即中间人攻击不会成功，因此，本文方案可以有效地抵抗中间人攻击。

6.3 抵抗重放攻击

攻击目标：攻击者重放在过去时间 ts_{U}' 合法 U 的漫游接入请求分组 $\{aP, y_i, R_1, \mathrm{NETID}, ts_{\mathrm{U}}'\}$，以使 FLEO 能够检测到 $f(R_1, y_i) = f(z, s_1)$。或攻击者重放在过去时间 ts_{SAP}' 合法 FLEO 的漫游接入应答分组 $\{y_i, bP, y_i', R_2, \mathrm{TMSI}_i, ts_{\mathrm{SAP}}'\}$，以使 U 能够检测到 $f(R_2, y_i') = f(z', s_2)$。

攻击资源：攻击者能够获得过去时间内 U 发送给 FLEO 的接入请求五元组 $\{aP, y_i, R_1, \mathrm{NETID}, ts_{\mathrm{U}}\}$，以及 FLEO 发送给 U 的接入应答六元组 $\{y_i, bP, y_i', R_2, \mathrm{TMSI}_i, ts_{\mathrm{SAP}}\}$。

漫游认证过程中，FLEO 在收到 U 的漫游接入请求分组后，会首先验证传播时延 $t_{\mathrm{now}} - ts_{\mathrm{U}}$ 是否在可接受的阈值 Δt 以内。若超出阈值，则认为接入请求超时，拒绝 U 的接入，所以能抵抗攻击者重放接入请求分组。U 在收到 FLEO 的漫游应答分组后，也会首先验证传播时延 $t_{\mathrm{now}} - ts_{\mathrm{SAP}}$ 是否在可接受的阈值 Δt 以内。如果超出阈值，则认为接入应答超时，终止认证操作，所以能抵抗攻击者重放接入应答分组。综上所述，本文方案可以抵抗重放攻击。

6.4 密钥协商

本文方案的密钥协商过程是基于椭圆曲线的 DH 密钥交换算法。基于 DH 困难假设，任何攻击者在仅知道 P、aP 和 bP 的情况下无法计算出 abP。在本文方案中，U 和 FGS 分别产生 DH 密钥协商参数 aP 和 bP，然后协商出会话密钥 $SK = abP$。鉴于上文所证明的安全性，攻击者只能获得 aP 和 bP，并且无法篡改他们，因为一旦篡改他们，认证将不通过，所以任何除了 U 和 FGS 的实体都无法计算出会话密钥，包括 FLEO。

6.5 身份隐私保护

U 根据自己的服务量向 HNCC 申请多个令牌。不同令牌之间不具有任何相关性，相当于多个假名。其他用户甚至 FNCC 都无法确定不同令牌是否属于同一个用户，只有 HNCC 能根据 y_i 或 z_i 查询令牌表确定 U 的真实身份。在 U 认证完毕后，FLEO 随机挑选一个 TMSI_i 发送给 U。TMSI_i 的随机性使 U 的身份对其他用户具有一定的匿名性。

7 性能分析

本文通过分析认证时延评估本方案的性能。认证时延是用户执行一次认证流程所耗费的总时间，包括各个认证实体执行密码学操作造成的计算时延以及实体间交互造成的通信时延，即认证时延=计算时延+通信时延。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。为了方便分析，本文分别将 U 到 FLEO，FLEO 到 FGS，FGS 到 FNCC，FNCC 到 HNCC 的传播时延表示为 $T_{\text{U-FLEO}}$、$T_{\text{FLEO-FGS}}$、$T_{\text{FGS-FNCC}}$、$T_{\text{FNCC-HNCC}}$。由于低轨卫星和地面相距 500~2 000 km[17]且实测实验室主机至云端服务器（百度服务器、阿里服务器等）来回时延 10~30 ms，所以本文设定 $T_{\text{U-FLEO}} = T_{\text{FLEO-FGS}} = 10\ \text{ms}$，$T_{\text{FGS-FNCC}} = 5\ \text{ms}$，$T_{\text{FNCC-HNCC}} = 5\ \text{ms}$。文献[18]以 Intel P-IV 3 GHz 处理器利用 OPENSSL 库测得一些密码学算法的计算耗时。其中，一次双线性映射、一次椭圆曲线的点乘、一次模指数运算分别耗时 $T_{\text{pair}} = 11.903\ \text{ms}$，$T_{\text{mul}} = 0.376\ \text{ms}$，$T_{\text{exp}} = 0.387\ \text{ms}$。由于散列运算和对称加密相对于别的密码学算法耗时可忽略不计，本文在方案比较过程中忽略散列运算带来的时延。另外，本文所提方案在认证过程中需要查询 Bloom Filter 表，而查表过程的复杂度

相当于做有限次散列运算，所以我们忽略查表带来的时延。

本文选取具有代表性的文献[2, 3, 5, 11]的漫游相关方案和本文方案进行比较。需要注意的是，由于卫星网络关于漫游的研究匮乏，所以选取的这些方案并非专门针对天地一体化网络漫游场景。文献[2, 3]的方案是卫星网络下的认证方案，选取它们作为比较对象是因为这 2 种方案和本文方案均针对天地一体化网络环境，且均提供了较为高效的认证方案。文献[5,11]的方案是无线网络环境下的漫游方案，选取它们作为比较对象是因为这 2 种方案和本文方案同处于漫游场景且也较为高效。鉴于这些方案和本文方案场景的差异性，本文根据天地一体化网络特点对被比较方案做了适应性修改。文献[2, 3]的方案的身份验证者原为所在域 NCC，本文将其的移动至 HNCC，既保证了方案的自然迁移也保障了安全性。文献[5,11]的方案的身份验证者原本即分别为 HNCC 和 FNCC，本文不做修改。

表 2 展示了相关方案性能对比的情况。从表 2 可以看出，本文方案在计算上需执行 6 次模指数运算，2 次椭圆曲线点乘运算。而文献[2]的方案需执行 3 次模指数运算，文献[5]的方案需执行 3 次双向线性映射计算和 16 次椭圆曲线点乘运算，文献[3]和文献[11]的方案由于涉及的密码学算法为散列计算或者对称加密，相比其他密码学算法计算时延可忽略不计。所以本文方案在计算时延上虽高于文献[2, 3, 11]的方案，但是差距不大，且明显低于文献[5]方案。本文方案将认证功能由 HNCC 提前至 FLEO，且漫游认证过程只需一次星地交互，显著减少通信时延。从表 2 可以看出，本文方案相比其他方案至少减少了一半通信时延。考虑到天地一体化网络特殊的环境，其认证时延瓶颈在于星地链路的高时延，所以本文方案在认证时延上具有不可比拟的优越性。通过模拟计算得出本文方案认证时延约为 23.074 ms，是整体耗时最少的，且几乎是其他耗时最少的 $\frac{1}{3}$。此外，本文方案相比其他方案同样具有匿名性，用户身份也支持动态撤销，另外，还考虑了用户、漫游域和归属域三方根据服务量计费的问题。即本文方案在功能完备性上具有一定的优越性。

8　结束语

本文针对天地一体化网络的漫游场景，提出了一种基于令牌的双方漫游认证方案。该方案将漫游认证功能从地面提前到接入卫星，很好地减少了传播时延。另外，基于单向累加器生成的令牌，不仅使认证过程高效，还支持灵活的加入和撤销。基于令牌的收费机制，既能防止 FNCC 向 HNCC 收取额外的费用，还能保证用户只为使用过的令牌支付费用，极大维护了用户和 HNCC 的权益。本文的安全分析表明：本文方案能够提供双向认证，抵抗中间人和重放攻击，还具有一定的匿名性。本文的性能分析表明：本文方案大大减少了漫游认证时延，具有显著的优越性。

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] CHEN C L, CHENG K W, CHEN Y L, et al. An improvement on the self-verification authentication mechanism for a mobile satellite communication system[J]. Applied Mathematics & Information Sciences, 2014, 8(1L): 97-106.

[3] ZHAO W, ZHANG A, LI J, et al. Analysis and design of an authentication protocol for space information network[C]// IEEE Military Communications Conference on MILCOM. IEEE, 2016: 43-48.

[4] LIU Y, ZHANG A, LI J, et al. An anonymous distributed key management system based on CL-PKC for space information network[C]// IEEE International Conference on Communications (ICC). 2016: 1-7.

[5] HE D, BU J, CHAN S, et al. Privacy-preserving universal authentication protocol for wireless communications[J]. IEEE Transactions on Wireless Communications, 2011, 10(2): 431-436.

表 2　　**相关方案性能对比**

方案	匿名性	动态撤销	计费	计算时延	通信时延	认证时延/ms
文献[2]方案	支持	支持	不支持	$3T_{\text{exp}}$	$2T_{\text{U-FLEO}}+2T_{\text{FLEO-FGS}}+2T_{\text{FGS-FNCC}}+2T_{\text{FNCC-HNCC}}$	61.161
文献[3]方案	支持	支持	不支持	/	$2T_{\text{U-FLEO}}+2T_{\text{FLEO-FGS}}+2T_{\text{FGS-FNCC}}+2T_{\text{FNCC-HNCC}}$	60
文献[5]方案	支持	支持	不支持	$3T_{\text{pair}}+16T_{\text{mul}}$	$2T_{\text{U-FLEO}}+2T_{\text{FLEO-FGS}}+2T_{\text{FGS-FNCC}}$	91.725
文献[11]方案	支持	支持	不支持	/	$3T_{\text{U-FLEO}}+3T_{\text{FLEO-FGS}}+2T_{\text{FGS-FNCC}}+2T_{\text{FNCC-HNCC}}$	80.0
本文方案	支持	支持	支持	$6T_{\text{exp}}+2T_{\text{mul}}$	$2T_{\text{U-FLEO}}$	23.074

[6] LIU J K, CHU C K, CHOW S S M, et al. Time-bound anonymous authentication for roaming networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(1): 178-189.

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

[8] 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.

[9] 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.

[10] CHEN T H, LEE W B, CHEN H B. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers & Electrical Engineering, 2009, 35(1): 41-48.

[11] JIANG Y, LIN C, SHEN X, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577.

[12] YANG G, WONG D S, DENG X. Anonymous and authenticated key exchange for roaming networks[J]. IEEE Transactions on Wireless Communications, 2007, 6(9):3461-3472.

[13] YANG G, WONG D S, DENG X. Formal security definition and efficient construction for roaming with a privacy-preserving extension[J]. Journal of Universal Computer Science, 2008, 14(3): 441-462.

[14] BENALOH J C, MARE M D. One-way accumulators: a decentralized alternative to digital signatures[C]//Workshop on the Theory and Application of of Cryptographic Techniques. 1993: 274-285.

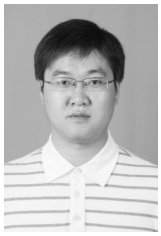
[15] BLOOM B H. Space/time trade-offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422-426.

[16] MUKHERJEE J, RAMAMURTHY B. Communication technologies and architectures for space network and interplanetary internet[J]. IEEE Communications Surveys & Tutorials, 2013, 15(2): 881-897.

[17] AKYILDIZ I F, UZUNALIOĞLU H, BENDER M D. Handover management in low earth orbit (LEO) satellite networks[J]. Mobile Networks and Applications, 1999, 4(4): 301-310.

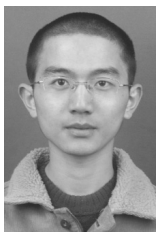
[18] HE D, BU J, CHAN S, et al. Handauth: efficient handover authentication with conditional privacy for wireless networks[J]. IEEE Transactions on Computers, 2013, 62(3): 616-622.

[作者简介]



薛开平（1980-），男，江苏东台人，中国科学技术大学副教授，主要研究方向为下一代网络体系结构与网络安全。

马永金（1994-），男，福建龙岩人，中国科学技术大学硕士生，主要研究方向为系统与网络安全。



洪佳楠（1989-），男，浙江宁波人，中国科学技术大学博士生，主要研究方向为网络安全协议设计与分析。

许婕（1995-），女，安徽六安人，中国科学技术大学硕士生，主要研究方向为网络安全协议设计与分析。

杨青友（1993-），男，海南万宁人，中国科学技术大学硕士生，主要研究方向为网络安全协议设计与分析。