天地一体化网络无缝切换和跨域漫游场景下的安全认证增强方案

薛开平，周焕城，孟薇，李少华
（中国科学技术大学信息科学技术学院，安徽 合肥 230026）

摘 要：由多种异构网络融合而成的天地一体化网络受到了研究者的广泛关注，但是其由于拓扑复杂、用户规模庞大而面临诸多安全威胁，容易出现链路切换和用户跨域漫游的情况。针对天地一体化网络的特点，提出了一种适用于天地一体化网络无缝切换和跨域漫游场景下的安全认证增强方案，基于安全凭证（Token）与散列链的结合，实现了用户与拜访域的双向快速认证，同时支持用户在拜访域中的合理计费。此外，针对天地一体化网络中卫星接入点频繁切换问题，提出了 2 种无缝切换机制以确保用户通信的连续性。安全性分析结果表明，所提方案不仅满足跨域漫游所必备的安全特性，还能够实现用户在拜访域的合理计费。

关键词：天地一体化网络；漫游；无缝切换；安全认证；计费
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019128

Secure authentication enhancement scheme for seamless handover and roaming in space information network

XUE Kaiping, ZHOU Huancheng, MENG Wei, LI Shaohua
School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China

Abstract: Space information network composed of a variety of heterogeneous networks is widely concerned. However, the space information network is facing more security threats and more likely to roam due to its complex topology and large user scale. Considering the characteristics of space information network, a secure authentication enhancement scheme for seamless handover and roaming in space information network was presented. The fast mutual authentication and reasonable accounting between the user and the visiting domain based on the combination of Token and Hash chain was achieved. In addition, two seamless handover mechanisms were proposed to ensure the continuity of user communication. Finally, security analysis indicates that the scheme can not only provide essential security properties, but also achieve reasonable accounting.

Key words: space information network, roaming, seamless handover, secure authentication, accounting

1 引言

近年来，随着航天和卫星通信技术的不断进步，卫星网络迅速发展。同时，国家安全、用户通信等需求的不断提高促使卫星网络进一步发展，由卫星网络、地面网络等多种网络融合而形成的天地一体化网络得到学术界和工业界的广泛关注。该网络具有覆盖范围广、拓扑动态变化、受地理条件限制小等特点，因战略性、基础性、带动性和不可替代性，成为了保障国民经济和国家安全的重大基础设施。为了接入天地一体化网络，终端必须利用卫星接入节点作为转发中继，而卫星接入节点包括地

收稿日期：2018−10−09；**修回日期**：2019−03−17
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800301）；国家自然科学基金面上项目资助项目（No.61379129）；中国科学院青年创新促进会会员基金资助项目（No.2016394）
Foundation Items: The National Key Research and Development Plan of China (No.2016YFB0800301), The National Natural Science Foundation of China (No.61379129), Youth Innovation Promotion Association of Chinese Academy of Sciences (No. 2016394)

球同步（GEO, geostationary earth orbit）卫星、中轨（MEO, medium earth orbit）卫星和低轨（LEO, low earth orbit）卫星。相比地球同步卫星，低轨卫星距离地球更近，在通信延时、通信质量等方面更具优势，更适合作为卫星接入点来为用户提供卫星通信服务。

然而，由于天地一体化网络的成分复杂且用户规模庞大，会产生许多安全需求。一方面，由于天地一体化网络具有链路高度开放的特点，更容易面临信息被窃取和干扰的威胁。另一方面，天地一体化网络是一个多种制式的卫星网络，是不同接入方式有机结合的异构网络，这样的网络不可能由一家运营商进行运营和管理，大规模用户往往属于不同的信任域。这些信任域彼此之间并不会完全信任对方，当用户从一个信任域管理的接入网关，接入到另外一个信任域管理的接入网关时，就涉及漫游。此时，为了保证位于外地信任域的合法用户仍然能够正常接入天地一体化网络，需要设计安全有效的漫游接入协议。因此，漫游问题无论对于目前传统网络还是未来网络都是一个需要重点考虑的问题。在为用户提供漫游服务时，如何确保用户通信服务的安全性、连续性及合理计费对于一个漫游协议来说是不可忽略的。因此，本文将从用户匿名性、网络可用性、合理计费等角度设计安全高效的漫游接入协议。

近来，针对天地一体化网络的特性，有许多研究提出了各种接入认证方案和安全切换方案。文献[1]从安全接入、安全路由、安全切换、安全传输、密钥管理等功能角度将这些方案进行了综述与评价。但是，至今尚未有适用于天地一体化网络的安全漫游方案。而传统无线网络中的漫游方案[2-3]虽然可以提供用户身份匿名从而保护用户的隐私，但是这些漫游方案并没有考虑计费问题。

基于以上考虑，本文提出了一种适用于天地一体化网络无缝切换和跨域漫游场景的安全认证增强方案。该方案可以实现安全漫游认证及用户在外地信任域中的合理计费。此外，由于卫星接入节点和一些终端的高速移动特性，本文还提出了无缝安全切换方案以保证用户的通信连续性。通过安全性与性能分析，证明了本文方案不仅能够实现用户在天地一体化网络中的安全漫游接入认证，而且可以保证用户在漫游过程中的合理计费。

2　相关工作

近年来，天地一体化网络（国外称为卫星网络）得到了国内外越来越多的关注，大量针对天地一体化网络安全的协议被提出。早在 1996 年，Cruickshank[4]首先提出了一个适用于卫星网络的认证系统，该系统利用公钥体系完成了用户与服务器之间的双向认证，然而认证效率不高，同时也会暴露用户的身份信息。2003 年，Hwang 等[5]提出了一种基于私钥密码系统的、适用于卫星网络的、改进版的认证方案。该方案与 Cruickshank[4]的方案相比计算开销小了许多。然而在 2005 年，Chang 等[6]发现了 Hwang 等[5]的方案并没有满足前向安全性，同时会受到密码猜测攻击，因此提出了一种基于散列链为认证手段的改进方案，使用 DH（Diffie-Hellman）密钥交换保证了前向安全性。

以上方案的目的都是解决卫星网络中的安全接入问题，但是都没有考虑卫星网络中的安全漫游问题。传统网络的漫游接入认证协议得到了学术界的广泛研究。2004 年，Zhu 等[7]提出了一种新的高效认证方案，声称可以为无线环境提供匿名性。随后 Lee 等[2]发现了 Zhu 等[7]的方案存在许多安全缺陷，并提出了改进方案。2008 年，Wu 等[8]提出了 Lee 等[2]的方案并不能保证用户匿名性。然而 Zeng 等[9]发现了 Wu 等[8]的方案也不能保护用户匿名性，更进一步地，Mun 等 [3]发现了 Wu 等[8]的方案存在更多问题，包括用户密码泄露、不满足密钥前向安全性等。

在以上漫游方案中，用户的漫游认证都需要用户归属域服务器参与验证，这不仅增加了认证时延，而且增大了用户归属域服务器的计算开销与通信负担，同时容易使用户归属域服务器成为漫游系统的性能瓶颈。因此在 2010 年，Yang 等 [10]提出了一种适用于无线匿名网络中的通用认证方案，该方案使用了组签名，每个移动用户都可以利用归属域服务器颁发的组私钥进行消息签名，拜访域只需要利用用户归属域服务器的公钥即可认证漫游用户的合法性。该方案保证了用户匿名性，但是由于复杂的签名算法带来较大的计算开销，因此可用性受到了限制。2012 年，He 等[11]提出了一种基于双线性映射的安全高效的切换认证方案，该方案通过使用用户归属域服务器颁发的假名实现用户匿名，同时利用了批量认证的手段减少认证开销。然而，该方案在认证过程中涉及大量的双线性映射操作，因

此计算开销比较大，并且该方案不能提供前向安全性。基于以上考虑，Li 等[12]提出了一种轻量级的漫游认证方案，该方案能够保证用户匿名性的同时降低计算开销。然而该方案没有考虑计费问题，另外，用户撤销问题也没有得到解决，即使用户身份在归属域服务器被撤销，在外地也仍然能够继续使用。而且该方案的认证流程存在漏洞，攻击者可以利用用户的公开信息临时通过认证步骤，虽然并不能获取认证成功之后的会话密钥，但是攻击者仍然能占用一条合法的链路，因此容易引发拒绝服务（DoS, denial of service）攻击。

2014 年，Yan 等[13]提出了一种基于全球认证中心的安全漫游方案，该方案中全球认证中心管理所有国家的服务器的认证信息，用户接入网络时，卫星会向全球认证中心请求用户注册域服务器的认证信息，并对用户进行认证。该方案解决了天地一体化网络中信任域众多难以管理的问题，但是引入了新实体——全球认证中心，在现实中不太合理，因此实用性欠佳。2016 年，Jiang 等[14]提出了一种基于 HMAC（Hash-based message authentication code）的 VANET（vehicular Ad Hoc network）高效匿名批量认证方案，然而该方案需要使用公钥基础设施（PKI, public key infrastructure)来完成对用户的接入认证。在天地一体化网络中，证书的管理十分复杂，此外，天地一体化网络通信带宽不大，链路质量也不佳，使用证书会引入大量的通信开销，进一步放大了天地一体化网络的难点问题。Bao 等[15]提出了一种基于身份的身份验证和无线漫游密钥协商协议，该协议的特点是使用了椭圆曲线密码与双线性映射，因此，可以实现快速认证且密钥短小，大大加快了认证速度，减少了存储开销。然而在天地一体化网络中，许多终端的计算能力都比较弱，这些终端可能无法运行双线性映射算法，因此，该方案的实用性也不高。

由于网络环境存在极大的差异，其他无线网络中的漫游方案很难适用于天地一体化网络，因此，针对天地一体化网络的节点移动和链路特性设计相应的漫游方案是研究天地一体化网络的重要问题之一。

3 网络和安全模型

3.1 系统模型

本文主要研究天地一体化网络中的安全漫游问题，这一过程中主要考虑以下实体：用户终端 A、归属域服务器 H（home server）、接入卫星 SAR（satellite access point）、归属域地面站 G（gateway）、拜访域地面站 FG（foreign gateway）与拜访域服务器 F（foreign server）组成。系统架构如图 1 所示。

用户终端 A。在其归属域服务器 H 上注册，希望通过接入卫星 SAR 使用拜访域网络。

归属域服务器 H。有用户的注册信息，同时为用户提供到特定拜访域的漫游凭证。

接入卫星 SAR。是用户终端 A 与地面站之间的中继节点，负责转发认证信息与会话数据。

归属域地面站 G。属于归属域服务器 H，为用户终端 A 提供网络服务，归属域地面站 G 与归属域服务器 H 之间有安全通道。

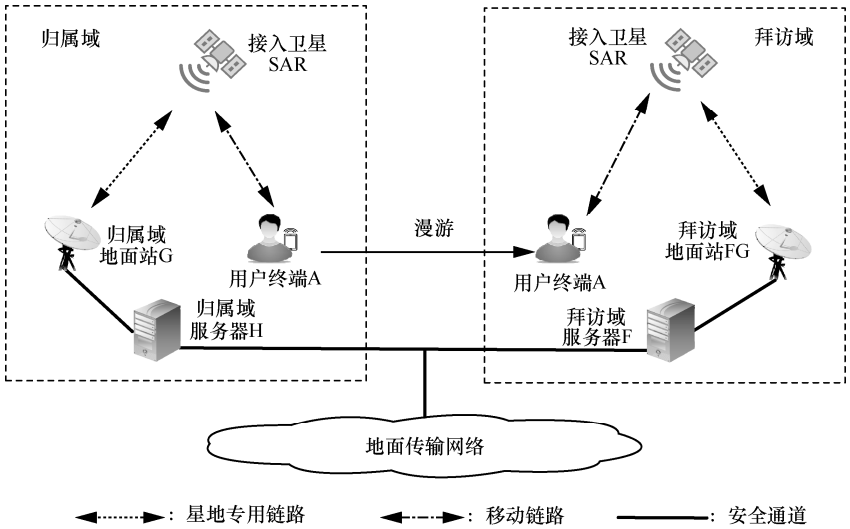


图 1 天地一体化网络中安全漫游架构

拜访域地面站 FG。属于拜访域服务器 F，为用户终端 A 提供网络服务，拜访域地面站 FG 与拜访域服务器 F 之间有安全通道。

拜访域服务器 F。用户终端 A 要漫游到的拜访域中的服务器，与用户归属域服务器 H 共享会话密钥，可以验证用户出示的漫游凭证。

3.2　安全假设

本文方案主要是基于以下的安全假设。

1) 接入卫星与地面站已建立安全通道，地面站与其归属的信任域服务器已建立安全通道，每个信任域服务器之间已建立安全通道。

2) 拜访域中的服务器、地面站及接入卫星对于用户的身份是好奇的，它们希望获得用户的真实身份，同时最大化自己的利益，因此可能会寻找机会多收取用户的费用。

3) 用户与归属域服务器希望最大化自己的利益，用户可能希望不出示或少出示计费凭证，从而减少自己的费用。如果有机会的话，归属域服务器会拒绝承认拜访域服务器出示的计费凭证。

4) 攻击者可以窃听用户接入拜访域网络时发出的认证信息，也有能力对内容进行篡改，并试图破坏用户正常接入网络、伪装成用户接入网络或窃听用户接入网络后发送的数据信息。

3.3　安全需求

基于以上安全模型，一种安全的漫游接入认证方案必须满足以下几个安全需求。

1) 双向认证。用户必须认证接入的地面站身份的合法性，防止接入假冒地面站。同时地面站必须认证用户的身份，确认用户拥有在本信任域的漫游资格。

2) 用户匿名性。用户在拜访域中使用网络，但是拜访域不能获取用户的真实身份。同时用户多次访问网络出示的多个临时身份之间应没有联系，即临时身份必须满足不可链接性。

3) 计费合理性。方案必须保证用户使用网络时按规定付费，拜访域服务器可以向用户归属域服务器正常收取费用，不能多收。归属域服务器不能不付或少付费用。

4) 用户身份动态撤销。当用户进行不合法行为，或者用户真实身份泄露时，需要对用户身份进行动态撤销，取消用户在拜访域中对应的漫游身份。

4　漫游认证方案

当用户漫游到拜访域中，希望使用拜访域网络时，为了实现安全漫游必须使用漫游认证方案。方案包括了 5 个阶段：漫游业务注册阶段、接入认证阶段、无缝安全切换阶段、计费阶段与撤销阶段。漫游认证方案中涉及的参数及其定义如表 1 所示，模型如图 2 所示。

表 1　　漫游方案中参数及其含义

符号	定义
p	一个 k bit 的素数
Z_p	一个素数群
$E_p(a,b)$	一个在素数域上的椭圆曲线
P	椭圆曲线上的生成元
pk_H	用户归属域服务器的公钥
sk_H	用户归属域服务器的私钥
pk_F	拜访域服务器的公钥
sk_F	拜访域服务器的私钥
pk_i	实体 i 的公钥
sk_i	实体 i 的私钥
ID_i	实体 i 的身份标识
TID_i	实体 i 的临时身份标识
$x_{i-\mathrm{F}}$	实体 i 在拜访域 F 中的计费链头部
$y_{i-\mathrm{F}}$	实体 i 在拜访域 F 中的计费链尾部
$f(x,y)$	对 $x\|y$ 进行散列操作
K_{i-j}	实体 i 与 j 共享的对称密钥
T_end	临时身份的有效截止日期

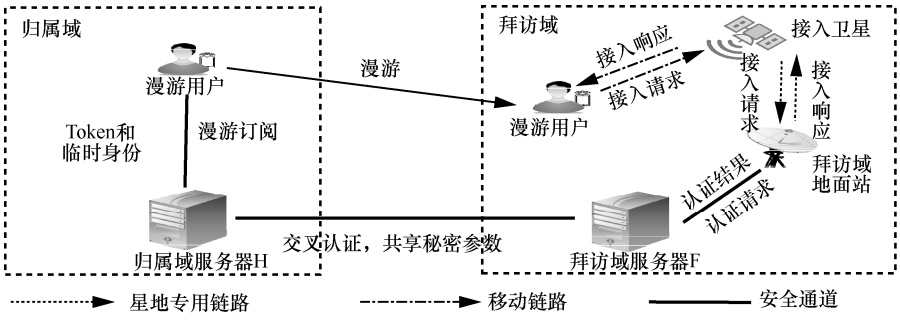


图 2　安全漫游方案模型

4.1 漫游业务注册阶段

当用户 A 希望获取漫游业务之前，需要向归属域服务器订阅对应的拜访域的漫游服务。首先定义一个函数 $f(x,y)=h(x||y)$，其中 $h()$函数是散列函数，并且定义 $f^i(x,y)=f\left(f^{i-1}(x,y),y\right),2<i\leqslant n$。

初始注册阶段流程如图 3 所示，具体步骤如下。

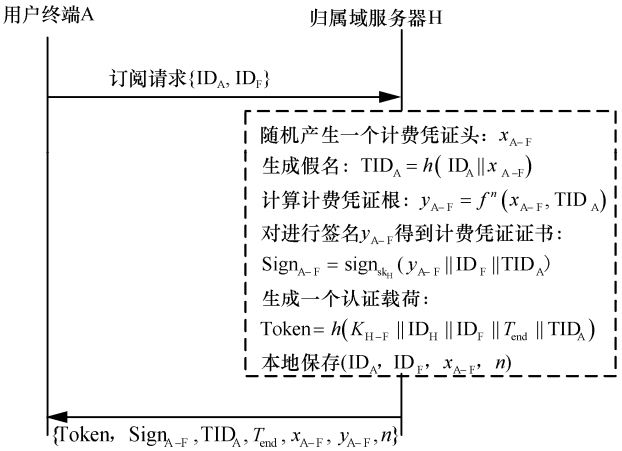


图 3 初始注册阶段流程

步骤 1 用户 A 首先向归属域服务器 H 发送漫游订阅请求$\{\mathrm{ID_A},\ \mathrm{ID_F}\}$，其中 $\mathrm{ID_F}$ 是拜访域服务器 F 的身份标识。

步骤 2 归属域服务器 H 为用户 A 随机产生一个计费凭证头 $x_{\text{A-F}}$，同时为用户 A 生成假名 $\mathrm{TID_A}=h\left(\mathrm{ID_A}||x_{\text{A-F}}\right)$。之后利用 $f(x,y)$函数对 $x_{\text{A-F}}$ 和 $\mathrm{TID_A}$ 进行 n 次计算，获得计费凭证根 $y_{\text{A-F}}=f^n\left(x_{\text{A-F}},\ \mathrm{TID_A}\right)$。并用私钥对 $y_{\text{A-F}}$ 进行签名得到计费凭证证书 $\mathrm{Sign_{A-F}}$。

$$\mathrm{Sign_{A-F}}=\mathrm{sign_{sk_H}}(y_{\text{A-F}}\,\|\,\mathrm{ID_F}\|\mathrm{TID_A})$$

为了让拜访域服务器 F 认证用户 A 的身份，归属域服务器 H 为用户 A 生成一个认证载荷 Token。

$$\mathrm{Token}=h\left(K_{\text{H-F}}\,\|\,\mathrm{ID_H}\,\|\,\mathrm{ID_F}\,\|\,T_{\text{end}}\,\|\,\mathrm{TID_A}\right)$$

其中，$K_{\text{H-F}}$ 是归属域服务器 H 与拜访域服务器 F 共享的对称密钥；T_{end} 是该载荷的有效期限，过期作废。

步骤 3 归属域服务器 H 将$\{\mathrm{Token},\mathrm{Sign_{A\text{-}F}},\mathrm{TID_A},T_{\text{end}},x_{\text{A-F}},y_{\text{A-F}},n\}$通过安全通道发送给用户 A，并在本地存储$\{\mathrm{ID_A},\ \mathrm{ID_F},\ x_{\text{A-F}},\ n\}$表项作为后续审计使用。

4.2 接入认证阶段

认证阶段如图 4 所示，具体步骤如下。

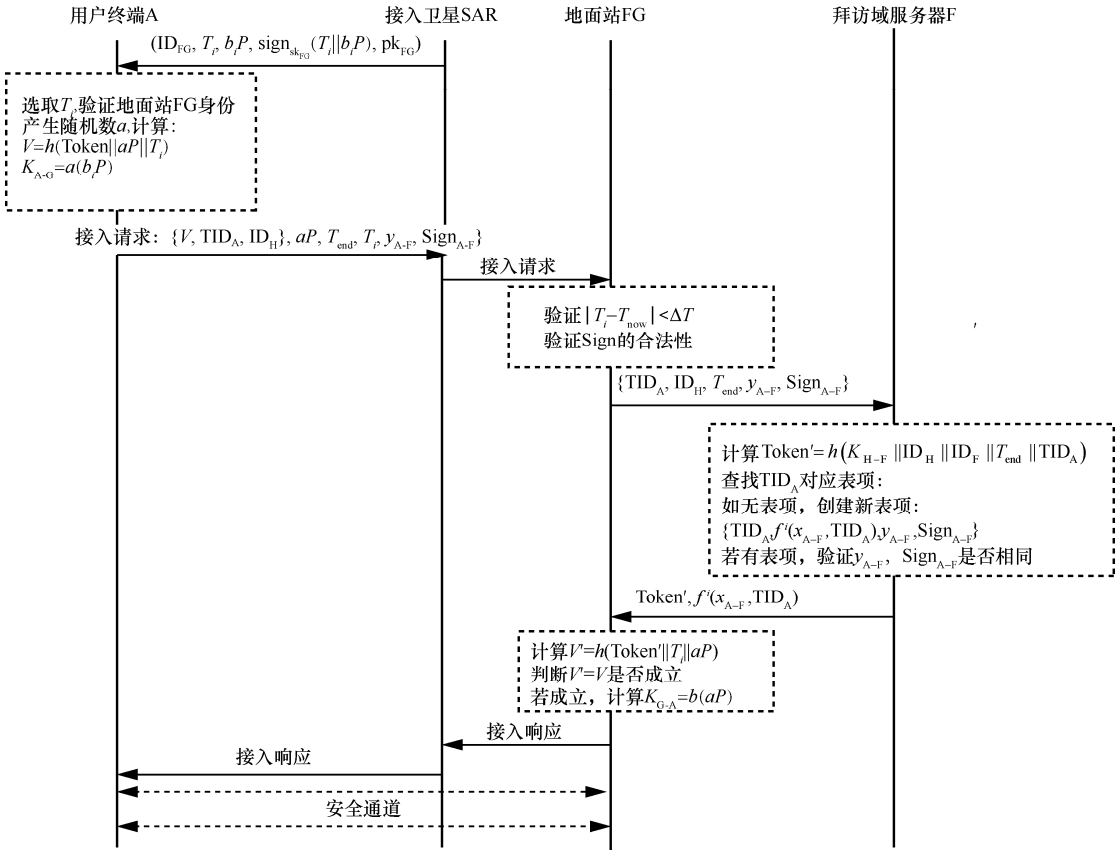


图 4 安全漫游认证流程

步骤 1　拜访域服务器 F 下属的地面站 FG 通过其连接的卫星接入点 SAR 不断向用户广播消息 $\{\mathrm{ID}_{\mathrm{FG}}, T_i, b_iP, \mathrm{sign}_{\mathrm{sk}_{\mathrm{FG}}}(T_i \| b_iP), \mathrm{pk}_{\mathrm{FG}}\}$，每个时间段 T_i 对应不同的 b_iP。

步骤 2　当用户 A 进入拜访域服务器的服务范围时，用户希望发起漫游业务请求。用户首先挑选一个时间点 T_i，并使用地面站 FG 的公钥 $\mathrm{pk}_{\mathrm{FG}}$ 验证其签名。若验证通过，则用户 A 生成随机数 a，并计算

$$K_{\mathrm{A-FG}}=a(b_iP)$$

$$V=h(\mathrm{Token}\|T_i\|aP)$$

向卫星 SAR 发送接入请求：$\{V, \mathrm{TID}_{\mathrm{A}}, \mathrm{ID}_{\mathrm{H}}, aP, T_{\mathrm{end}}, T_i, y_{\mathrm{A-F}}, \mathrm{Sign}_{\mathrm{A-F}}\}$。

步骤 3　卫星 SAR 收到用户 A 的接入请求后转发至地面站 FG。

步骤 4　地面站 FG 收到用户的接入请求后，首先验证式(1)是否成立，以防止重放攻击。

$$\left|T_i - T_{\mathrm{now}}\right| < \Delta T \tag{1}$$

通过验证后再验证签名 $\mathrm{Sign}_{\mathrm{A\text{-}FG}}$ 的合法性，若不合法，直接拒绝用户 A 的接入请求；否则地面站 FG 会向拜访域服务器 F 转发消息 $\{\mathrm{TID}_{\mathrm{A}}, \mathrm{ID}_{\mathrm{H}}, T_{\mathrm{end}}, y_{\mathrm{A-F}}, \mathrm{Sign}_{\mathrm{A-F}}\}$。

步骤 5　拜访域服务器 F 计算 Token'，并根据 $\mathrm{TID}_{\mathrm{A}}$ 查询本地表中是否有对应表项。

$$\mathrm{Token}'=h(K_{\mathrm{H-F}} \| \mathrm{ID}_{\mathrm{H}} \| \mathrm{ID}_{\mathrm{F}} \| T_{\mathrm{end}} \| \mathrm{TID}_{\mathrm{A}})$$

若查询不到表项，则拜访域服务器会为用户 A 创建新表项：$\{\mathrm{TID}_{\mathrm{A}}, f^i(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}), y_{\mathrm{A-F}}, \mathrm{Sign}_{\mathrm{A-F}}\}$，其中，$i=n$，即 $f^i\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)=y_{\mathrm{A-F}}$。若已有表项，则对比地面站 FG 发送的 $y_{\mathrm{A-F}}$、$\mathrm{Sign}_{\mathrm{A-F}}$ 与本地的 $y_{\mathrm{A-F}}$、$\mathrm{Sign}_{\mathrm{A-F}}$ 是否相同，若不相同则向地面站 FG 发送错误信息。最后拜访域服务器将 Token'与 $f^i\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)$ 一同返回给地面站。

步骤 6　地面站 FG 收到 Token'之后计算 V'。

$$V'=h(\mathrm{Token}'\|T_i\|aP)$$

判断 $V'=V$ 是否成立，若不成立，则用户 A 认证失败；否则地面站 FG 认可用户的身份，并且返回认证成功消息，然后计算与用户之间共享的会话密钥 $K_{\mathrm{FG-A}}=b_i(aP)$，同时记录下 $f^i\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)$，等待用户发送 $f^{i-1}\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)$，作为计费凭据。

步骤 7　卫星接入点 SAR 收到认证响应消息后转发给用户 A。

步骤 8　用户 A 收到认证成功消息后即可利用与地面站 FG 共享的对称密钥 $K_{\mathrm{A-FG}}$ 使用拜访域中的网络。同时用户 A 在使用网络时，地面站 FG 会按时间间隔或流量消耗情况，持续向用户 A 索取 $f^{i-1}\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right), f^{i-2}\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right), \cdots, x_{\mathrm{A-F}}$ 进行收费，否则将用户连接切断。

4.3　无缝安全切换阶段

在用户使用卫星网络时，由于卫星高速移动或者用户终端高速移动，可能会发生连接中断。为了保证用户的业务连续性，需要安全高效的网络切换机制。针对不同情况下引起的链路切换，本文提出了 2 种切换方案。

4.3.1　切换卫星接入点

在天地一体化网络中，由于卫星相对地面高速移动，用户大约每 10 min 就需要切换一个卫星接入点。为了便于讨论，本文假设新接入的卫星已经事先与地面站建立了信任关系，因此只需要让新接入卫星 NSAR 和用户 A 建立信任关系。具体做法如下。

步骤 1　当旧卫星 OSAR 离开用户时，用户向新卫星 NSAR 发起连接请求，同时附上 $f^{i-1}\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)$。

步骤 2　新卫星 NSAR 事先从地面站 FG 处获得了最新的 $f^i\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right)$，新卫星 NSAR 会验证式(2)。

$$f\left(f^{i-1}(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}), \mathrm{TID}_{\mathrm{A}}\right)=f^i\left(x_{\mathrm{A-F}}, \mathrm{TID}_{\mathrm{A}}\right) \tag{2}$$

若式(2)成立，则认为用户是曾经通过接入认证的合法用户，同意建立新的连接。

4.3.2　切换地面站

由于地面站的覆盖范围是有限的，而天地一体化网络中某些终端（如战斗机等）移动速度很快，在使用漫游业务的过程中可能会离开原地面站的覆盖范围，此时终端为了继续使用网络需要接入新的地面站。本文假设终端可以根据自己的轨迹预测出下一个要接入的地面站，并且新地面站（NFG, new foreign gateway）和旧地面站（OFG, old foreign gateway）之间彼此信任且具有安全通道。

步骤 1　用户 A 预先通过 OFG 为中继节点，向 NFG 发送 DH 密钥协商参数 $a'P$。

步骤 2　NFG 接收到用户 A 的密钥协商参数 $a'P$，生成随机数 b'，计算会话密钥 $K_{\mathrm{NFG'-A}}$。

$$K_{\mathrm{NFG'-A}}=b'(a'P)$$

并通过 OFG 向用户 A 发送 DH 密钥协商参数 b_iP。

步骤 3 用户 A 收到 NFG 的密钥协商参数 $b'P$，计算会话密钥 $K_{\text{A-NFG'}}$。

$$K_{\text{A-NFG'}} = a'(b'P)$$

用户 A 离开 OFG 的覆盖范围之前，会通知 OFG，并向 NFG 发送建立连接的请求，由于之前已经成功协商了会话密钥，因此这个过程耗时非常少。同时用户 A 发送 $f^{i-1}(x_{\text{A-F}},\text{TID}_\text{A})$，NFG 验证式(3)是否成立。

$$f(f^{i-1}(x_{\text{A-F}},\ \text{TID}_\text{A}),\ \text{TID}_\text{A}) \stackrel{?}{=} f^{i}(x_{\text{A-F}},\ \text{TID}_\text{A}) \quad (3)$$

其中，$f^{i}(x_{\text{A-F}},\text{TID}_\text{A})$ 是 OFG 发送给 NFG 的散列链节点。新连接完成后，用户 A 与 OFG 的连接会被销毁，切换过程也顺利完成。

4.4 计费阶段

在漫游过程中，由于用户的真实身份不能暴露给拜访域服务器 F，计费成为一个难点。在本方案中，利用散列链的特性顺利完成了漫游过程中的计费难题。具体分析计费阶段过程如下。

当用户 A 初始接入拜访域网络时，拜访域服务器 F 并没有用户 A 的信息。此时拜访域服务器 F 需要记录用户 A 的临时身份 TID_A、计费凭据根 $y_{\text{A-F}}$、最新凭据 $f^{i}(x_{\text{A-F}},\text{TID}_\text{A})$，用户归属域服务器 H 对凭据根 $y_{\text{A-F}}$ 的签名 $\text{Sign}_{\text{A-F}}$。之后用户 A 会持续发送 $f^{i-1}(x_{\text{A-F}},\text{TID}_\text{A}),f^{i-2}(x_{\text{A-F}},\text{TID}_A),\cdots,x_{\text{A-F}}$，给地面站 FG，当用户 A 离开网络时，地面站 FG 会将最新的 $f^{j}(x_{\text{A-F}},\text{TID}_\text{A})$ 发送给服务器 F。

当用户 A 再次接入拜访域网络时，拜访域服务器 F 会查到用户上次最新的凭据 $f^{i}(x_{\text{A-F}},\text{TID}_\text{A})$，并发送给用户 A 连接的地面站 FG（如 4.2 节步骤 5 所描述）。地面站 FG 会判断用户 A 是否接着上次的凭据 $f^{i}(x_{\text{A-F}},\text{TID}_\text{A})$ 继续发送 $f^{i-1}(x_{\text{A-F}},\text{TID}_\text{A})$，若验证通过则同意用户 A 接入网络。

拜访域服务器 F 结算费用时，可以利用最新的凭据 $f^{i}(x_{\text{A-F}},\text{TID}_\text{A})$、计费凭据根 $y_{\text{A-F}}$、$\text{Sign}_{\text{A-F}}$ 向用户归属域服务器 H 收费。归属域服务器 H 根据 $n-i$ 算出应付给拜访域服务器 F 的费用。

当用户 A 出示完 n 次计费凭据 $f^{n-1}(x_{\text{A-F}},\text{TID}_\text{A}),f^{n-2}(x_{\text{A-F}},\text{TID}_\text{A}),\cdots,x_{\text{A-F}}$，之后就暴露了 $x_{\text{A-F}}$，就无法再利用 TID_A 享受漫游业务了。用户 A 可以提前向归属域服务器 H 购买新的漫游凭据，获得新的 TID'_A 及新的计费凭据，利用新的临时身份和计费凭据继续享受漫游业务。

4.5 撤销阶段

有时归属域服务器 H 因为某些原因（比如用户 A 存在不合法行为、不小心泄露了身份等）希望撤销用户的漫游身份。由于用户 A 的漫游身份 $\text{TID}_{\text{A-F}}$ 是只在对应的拜访域生效的，因此归属域服务器 H 可以进行细粒度的动态撤销。当归属域服务器 H 希望撤销用户 A 在拜访域中的身份时，只需要查询本地表项，获得用户 A 申请在拜访域中的身份 $\text{TID}^1_{\text{A-F}},\text{TID}^2_{\text{A-F}},\cdots$，将这些身份添加至身份撤销列表中，发送给拜访域即可。拜访域服务器 F 收到用户的漫游业务请求时，会查询该用户的临时身份是否在撤销列表中，若是，则拒绝为其提供服务。这样就可以实现撤销用户在特定拜访域中的漫游身份，而不影响用户在其他拜访域中的正当漫游身份。同时由于每个漫游身份都有生存周期，当撤销列表中的漫游身份过期时，即可将这些过期身份从撤销列表中删除，可以进一步减少服务器的存储负担和传输撤销列表时占用的带宽。

5 安全性与性能分析

5.1 安全性分析

安全性分析基于以下前提条件。

前提 1 攻击者可能是不合法的用户，也可能是具有合法身份的用户。

前提 2 对于任何 x、y，若存在一者是未知的，则 $h(x||y)$是未知的。

前提 3 对于攻击者来说，归属域服务器 H 的私密信息、拜访域服务器 F 的私密信息及归属域服务器 H 与拜访域服务器 F 之间的共享秘密信息都是未知的。

前提 4 对于攻击者来说，其他合法用户的私密信息、其他合法用户与服务器之间共享的秘密信息都是未知的。

5.1.1 双向认证

1) 防恶意假冒地面站

对地面站的认证首先利用证书验证地面站的公钥，再利用公钥认证相应消息的签名。该过程所体现的架构与 PKI 体系是等同的，因此，对于仿冒攻击的抵御也完全等同于 PKI 的安全性：如果存在某攻击者有能力在这个过程中欺骗用户，并在用户不可察觉的情况下完成了与用户之间的认证流程，

则等价于该攻击者攻破 PKI 体系。因此，本方案能实现对地面站的合法性验证。

2) 防恶意用户接入

攻击目标。攻击者要以任意合法 $\mathrm{TID_A}$ 为身份，任意未来的时间 T_a 为时间产生的 V，以使地面站 FG 能检测到 V=V'，其中 V'来自两步的散列计算式如下

$$V' = h(\mathrm{Token}' \| T_i \| aP)$$

$$\mathrm{Token}' = h(K_{\mathrm{H-F}} \| \mathrm{ID_H} \| \mathrm{ID_F} \| T_{\mathrm{end}} \| \mathrm{TID_A})$$

攻击资源。攻击者能拿到多个过去时间 T_i 对应的通信信息，每个 T_i 对应一个 bP 与多个 $\{V, aP, \mathrm{ID_H}, \mathrm{ID_F}, T_{\mathrm{end}}, \mathrm{TID_A}\}$ 元组，其中 V 满足

$$V = h(\mathrm{Token} \| T_i \| aP)$$

$$\mathrm{Token} = h(K_{\mathrm{H-F}} \| \mathrm{ID_H} \| \mathrm{ID_F} \| T_{\mathrm{end}} \| \mathrm{TID_A})$$

地面站认证用户主要凭借的是 4.2 节步骤 6 中的 V=V'是否成立来对用户身份合法性进行判断。因此，对于该问题的攻击可形式化为生成六元组 $\{V, aP, \mathrm{ID_H}, T_{\mathrm{end}}, \mathrm{TID_A}, T_a\}$，其中，$T_a$ 为待攻击的未来某时间，V 是攻击者为了通过认证产生的认证信息，其他信息 aP、$\mathrm{ID_H}$、T_{end}、$\mathrm{TID_A}$ 对于攻击者来说都是已知且可以修改的。

由于 V'的计算式是事先确定的，攻击者只能修改计算 V'的输入参数 $\{aP, \mathrm{ID_H}, T_{\mathrm{end}}, \mathrm{TID_A}, T_a\}$，但是由前提 3 可知，$K_{\mathrm{H-F}}$ 对于攻击者来说是未知的。由前提 2 可知，由于 $K_{\mathrm{H-F}}$ 是未知的，Token′ 对于攻击者来说都是未知的。进一步由前提 2 推导出，V'对于攻击者来说是未知的。换句话说，攻击者可以修改 V'的值，但仍旧无法获得 V'的值，因此攻击者无法产生正确的 V，使得地面站验证 V=V'等式通过。

综上所述，攻击者无法通过地面站的验证过程，因此本方案可以实现地面站认证合法用户的功能。

5.1.2 防重放攻击

攻击目标。攻击者要以过去的时间 T_o 时合法用户产生的 V_o 作为认证载荷，使得地面站 FG 检测得到 V_o=V_o'。

攻击资源。攻击者能拿到多个过去时间 $T_{o\text{-}i}$ 对应的通信信息，每个 $T_{o\text{-}i}$ 对应一个 $b_{o\text{-}i}P$ 与多个 $\{V_{o-i}, a_{o-i}P, I\mathrm{D_H}, \mathrm{ID_F}, T_{\mathrm{endo}-i}, \mathrm{TID_{A}}_{o-i}\}$ 元组，其中 $V_{o\text{-}i}$ 满足

$$V_{o-i} = h(\mathrm{Token}_{o-i} \| T_{o-i} \| a_{o-i}P)$$

$$\mathrm{Token}_{o-i} = h(K_{\mathrm{H-F}} \| |\mathrm{ID_H} \| \mathrm{ID_F} \| T_{\mathrm{endo}-i} \| \mathrm{TID_{A}}_{o-i})$$

在 4.2 节步骤 4 中，地面站收到卫星转发的用户接入请求时，会验证时间 T_o 与当前时间 T_{now} 的差距是否大于阈值 ΔT，若差距过大，则会拒绝用户的接入请求，并不会进行接下来的认证步骤。因此当攻击者希望利用过去截获的合法用户认证信息通过认证时，地面站会及时发现并抵抗该攻击。因此，本方案可以抵抗重放攻击。

5.1.3 用户匿名性与身份不可链接性

由于用户 A 在接入拜访域网络时出示的是临时身份 $\mathrm{TID_A}$，真实身份 $\mathrm{ID_A}$ 从未暴露在拜访域网络中。而临时身份 $\mathrm{TID_A}$ 与真实身份 $\mathrm{ID_A}$ 的对应关系只有用户 A 和归属域服务器 H 知道，由前提 3 与前提 4 可知，攻击者无法获得临时身份 $\mathrm{TID_A}$ 与真实身份 $\mathrm{ID_A}$ 的对应关系，即无法通过用户 A 的临时身份 $\mathrm{TID_A}$ 推导出用户的真实身份 $\mathrm{ID_A}$，因此用户匿名性可以得到保证。

同时用户 A 每个临时身份 $\mathrm{TID_A^1}$，$\mathrm{TID_A^2}$，…，都是由用户归属域服务器 H 独立随机生成的，每个临时身份彼此没有联系，只有用户归属域服务器 H 知道这些临时身份对应同一个用户。由前提 3 可知，攻击者获得用户的多个临时身份，也无法将它们链接到一起，猜测出这多个临时身份是来自于同一个用户。因此本方案可以满足身份不可链接性。

5.1.4 抗中间人攻击

当攻击者希望在用户 A 与地面站 FG 进行中间人攻击时，必须使用户 A 相信其是一个合法的地面站 FG，同时使地面站 FG 相信其是用户 A。根据 5.1.1 节分析的双向认证特性，攻击者无法伪装成一个合法地面站，同时也无法仿冒用户 A 的身份，因此中间人攻击不会成功。而方案的安全性使中间人攻击只能将用户/卫星之间的认证数据和之后的通信数据进行不修改的转发，无法从中获得任何利益（如获得通信内容、伪造身份等）。

5.1.5 会话机密性

本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 $K_{\mathrm{A-FG}}$=abP。在本方案中，用户 A 和地面站 FG 分别随机产生 DH 密钥协商参数 aP 和 bP，攻击者只能获得 aP 和 bP，且无法篡改它们，因为一旦篡改密钥协商参数 aP 或 bP，那么 V 或 V'的值就会发生变化，则认证

会失败。所以任何除了用户 A 和地面站 FG 的实体都无法计算出会话密钥，包括卫星 FLEO。

5.1.6 计费与撤销

根据 4.4 节中对计费过程的分析和 4.5 节中对撤销过程的分析，可以知道本文方案能够完成合理的计费和细粒度的动态撤销功能。简要来说，用户必须出示计费凭证才能连续地享受漫游服务；同时基于散列链的单向性，拜访域服务器 F 无法通过已有的计费凭证推断出更多的计费凭证，因此拜访域服务器 F 无法多收取费用；而归属域服务器 H 用自身的私钥对计费凭证进行了签名，因此它无法对计费凭证抵赖，从而保证了拜访域服务器能够顺利向归属域服务器收取漫游费用。

5.2 性能分析

本文通过基于 Token 的安全认证机制，保证了安全漫游协议中用户与拜访域网络完成双向认证；通过基于散列链的计费凭证，达到实时计费的功能。表 2 是本文方案与文献[3]方案和文献[12]方案的性能对比结果。选取文献[3]方案和文献[12]方案的原因是文献[3]方案安全性能比较优秀，而文献[12]方案通信负担比较低。

假设用户 A 与 LEO、LEO 与 FG、FG 与服务器 F、服务器 F 与服务器 H 之间的通信时延分别为 $T_{\text{A-LEO}}$、$T_{\text{LEO-FG}}$、$T_{\text{FG-F}}$、$T_{\text{F-H}}$。由于低轨卫星和地面相距 500~2 000 km，一般通信时延为 10~30 ms，且经过实际测试，实验室主机到云端服务器单跳时延约为 10 ms。本文假定 $T_{\text{A-LEO}}$= $T_{\text{LEO-FG}}$=20 ms，$T_{\text{FG-F}}$ = $T_{\text{F-H}}$ =10 ms。另外，在 P-IV 3 GHz 处理器上利用 OPENSSL 库测得一些密码学计算的计算耗时，其中一次椭圆曲线点乘 T_{Mul}=0.376 ms，一次非对称加密 T_{Asym}=0.201 ms，一次对称加密 T_{Sym}=0.000 1 ms。由于散列操作和异或操作相对而言耗时极小，因此可以忽略它们带来的计算耗时。

从表 2 可以看到，相比文献[3]方案和文献[12]方案，本文方案安全性更强，性能上的表现也更佳。例如，本文方案支持实时计费与动态撤销，同时支持双向认证，这是文献[12]方案所欠缺的。从计算耗时上看，本文方案相比于文献[12]方案具有更低的计算开销。最为重要的是，本文方案考虑到天地一体化网络中通信时延较长的特点，大大简化了交互流程，因此通信时延相对较低。结合计算开销与通信时延，最终在整体的认证时延上本文方案比文献[3]方案和文献[12]方案耗时更短，性能表现更优。

6 结束语

本文针对天地一体化网络的特点，提出了一种安全漫游方案。该方案利用 Token 及散列链实现了用户在外地域中的安全漫游与合理计费；此外，考虑到卫星接入节点的高速移动性，提出了 2 种无缝安全切换方案以保证用户通信连续性。最后的安全性分析表明，本文方案能够实现用户在天地一体化网络中的安全漫游接入认证，同时通过合理的计费手段保证了各个实体的正当权益。

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] LEE C C, HWANG M S, LIAO I E. Security enhancement on a new authentication scheme with anonymity for wireless environments[J]. IEEE Transactions on Industrial Electronics, 2006, 53(5): 1683-1687.

[3] MUN H, HAN K, LEE Y S, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks[J]. Mathematical and Computer Modelling, 2012, 55(1): 214-222.

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

[5] 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.

表 2 与文献[3]方案、文献[12]方案的性能分析与对比

	用户匿名	双向认证	动态撤销	实时计费	计算开销	通信时延	认证时延/ms
文献[3]方案	有	有	有	无	T_{Asym}	$3T_{\text{A-LEO}}+3T_{\text{LEO-FG}}+2T_{\text{FG-F}}+2T_{\text{F-H}}$	160.201
文献[12]方案	有	弱	无	无	$4T_{\text{Mul}}+T_{\text{sym}}$	$3T_{\text{A-LEO}}+3T_{\text{LEO-FG}}+3T_{\text{FG-F}}$	151.504
本文方案	有	有	有	有	T_{Asym}	$2T_{\text{A-LEO}}+2T_{\text{LEO-FG}}+2T_{\text{FG-F}}$	100.201

[6] 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.

[7] ZHU J, MA J. A new authentication scheme with anonymity for wireless environments[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 231-235.

[8] WU C C, LEE W B, TSAUR W J. A secure authentication scheme with anonymity for wireless communications[J]. IEEE Communications Letters, 2008, 12(10):722-723.

[9] ZENG P, CAO Z, CHOO K K R, et al. On the anonymity of some authentication schemes for wireless communications[J]. IEEE Communications Letters, 2009, 13(3): 170-171.

[10] YANG G, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications[J]. IEEE Transactions on Wireless Communications, 2010, 9(1):168-174.

[11] HE D, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53.

[12] LI X, ZHANG Y, LIU X, et al. A lightweight roaming authentication protocol for anonymous wireless communication[C]//Global Communications Conference . IEEE, 2012: 1029-1034.

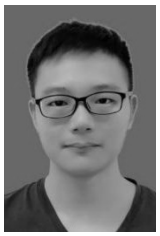
[13] YAN J, LU Y, LIU Y, et al. Research on Beidou-based inter-domain identity authentication for mobile object[C]//Advanced Research and Technology in Industry Applications. IEEE , 2014: 923-926.

[14] JIANG S, ZHU X, WANG L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.

[15] BAO Q, HOU M, CHOO K K R. A one-pass identity-based authentication and key agreement protocol for wireless roaming[C]//The Sixth International Conference on Information Science and Technology. IEEE, 2016: 443-447.

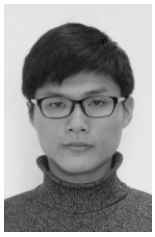
[作者简介]

薛开平（1980− ），男，江苏东台人，博士，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。



周焕城（1994− ），男，广东汕头人，中国科学技术大学硕士生，主要研究方向为网络安全与密码学。

孟薇（1993− ），女，安徽阜阳人，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。



李少华（1994− ），男，安徽蚌埠人，中国科学技术大学硕士生，主要研究方向为信息与系统安全。