面向天地一体化网络的终端可信接入认证与密钥协商协议

谢绒娜，周竞，张晨佳，史国振
（北京电子科技学院密码科学与技术系，北京 100070）

摘要：针对低轨卫星信道易受攻击、易中断及星上资源受限问题，提出了一种面向天地一体化网络的终端可信接入认证与密钥协商协议，实现终端用户与低轨卫星之间安全高效的双向认证与密钥协商。采用轻量级密码原语，由地面控制中心承担主要计算任务。通过设计伪身份和身份密码保护终端隐私性。基于初次接入生成的认证参数，协助断线后卫星对用户终端快速认证，提高断线重认证的效率。利用真实–随机（ROR）模型和Tamarin工具验证表明，协议具有更强的安全性和隐私保护性。性能分析表明，计算开销和通信效率优于现有方案，满足天地一体化网络的轻量级需求。

关键词：天地一体化网络；接入认证；断线重连；密钥协商；隐私保护
中图分类号：TP393
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260240

Trusted terminal access authentication and key agreement protocol for space-air-ground integrated networks

Xie Rongna, Zhou Jing, Zhang Chenjia, Shi Guozhen
Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: To address the vulnerabilities, interruptions, and limited onboard resources of low earth orbit (LEO) satellite channels, a trusted terminal access authentication and key agreement protocol for integrated space-ground networks was proposed, enabling secure and efficient two-way authentication and key exchange between end users and LEO satellites. The protocol employed lightweight cryptographic primitives, with the ground control center handling most of the computational tasks. Pseudonyms and identity encryption were designed to protect user privacy. Authentication parameters generated during initial access enable rapid re-authentication by the satellite after disconnection, improving the efficiency of reconnection. Security analysis using the real-or-random (ROR) model and the Tamarin tool demonstrates that the protocol offers stronger security and privacy protection. Performance evaluation shows that it outperforms existing schemes in terms of computational overhead and communication efficiency, meeting the lightweight requirements of integrated space-ground networks.

Key words: space-air-ground integrated network, access authentication, re-authentication, key agreement, privacy preservation

0 引言

天地一体化网络由空间段与地面段深度融合构成，是支撑未来广域覆盖、全球互联和多样化业务的新型信息基础设施[1]。其中，低轨（low earth orbit, LEO）卫星星座凭借低时延、高带宽和终端易小型化的独特优势，成为地面终端接入天地一体化网络的核心载体。然而，地面终端与低轨卫星接入点之间的通信链路高度动态、时延与抖动明显、信

收稿日期：2026–04–30；修回日期：2026–07–16
通信作者：史国振，1427980882@qq.com
基金项目：国家密码科学基金资助项目（No.2025NCSF02028）；中央高校基本科研业务费资金资助项目（No.3282023008）
Foundation Items：The National Cryptologic Science Fund of China (No.2025NCSF02028), The Fundamental Research Funds for the Central Universities (No.3282023008)

道开放易受窃听与篡改，同时星上计算与存储资源受限，使终端可信接入、链路中断后的快速恢复面临严峻的安全与性能挑战。近年来，学术界提出了一系列天地一体化场景下的终端接入认证方案[2-3]，但是大多没有考虑通信中断导致的频繁接入认证问题。本文围绕上述问题，研究如何设计适用于天地一体化网络的终端接入认证与密钥协商协议。本文的主要贡献如下。

（1）采用轻量级密码原语和零知识证明，提出了终端可信接入认证与密钥协商协议，实现地面终端与低轨卫星之间的安全高效认证。双方借助地面控制中心完成密钥协商过程，生成共享会话密钥，为后续双方安全会话提供保障。

（2）基于终端接入认证阶段构造快速认证参数，提出了轻量级断线重认证协议，实现不需要重新执行完整接入认证的快速重连，提高了会话的连续性与可靠性。

（3）利用真实–随机（real-or-random, ROR）模型证明本文协议的安全性，借助 Tamarin 工具验证了协议隐私保护的有效性和安全性。实验仿真与性能评估表明，本文协议具有较低的计算和通信开销，适用于资源受限的天地一体化网络环境。

1　相关工作

截至目前，学术界已经设计了大量针对天地一体化网络的认证方案，这些方案涉及多种密码体制和认证方式，为当前协议的设计、安全性提升和适用性增强提供了重要的借鉴。Zheng 等[4]针对卫星终端资源受限的特点，创新性地提出了仅依赖哈希函数与异或运算的轻量级认证方案，为低功耗卫星终端认证提供了可行思路。然而，Zhao 等[5]通过安全性分析指出，该方案在身份验证环节存在逻辑缺陷：攻击者可利用伪造的临时凭证绕过卫星中继的校验机制，实施假冒终端接入攻击，暴露了其抗伪造能力不足。为弥补这一漏洞，Altaf 等[6]提出了基于哈希链的改进方案，通过多轮哈希迭代增强身份凭证的时效性与不可伪造性。Xu 等[7]则转向公钥密码体系，利用非对称加密算法实现终端与地面网络的双向认证，试图通过数学难题提升安全性。但 Huang 等[8]与 Ostad-Sharif 等[9]后续研究表明，上述两种方案可能遭受暴力攻击。近年来，量子计算机的快速发展，使传统密码体系面临根本性挑战。在此背景下，Kumar 等[10]与 Dharminder 等[11]率先将后量子密码学引入卫星认证领域，并提出了基于环上带错误学习（learning with error over ring, Ring-LWE）问题的认证协议，其安全假设在量子计算模型下仍被证明是可靠的，且算法可通过多项式环结构实现高效计算，适配卫星终端的资源约束。尽管上述方案在安全性上逐步提升，但共同局限在于依赖卫星作为“透明中继”。随着卫星计算和存储能力的逐步提升，一些利用卫星直接认证终端的方案逐渐被提出。曹进等[12]首次提出了针对双层卫星网络的认证架构，省去了地面中心的参与环节，认证时延降低 60%。此后，Yi 等[13]与 Ma 等[14]进一步结合格密码技术，设计了全链路抗量子的直连认证方案，将单次认证的计算耗时压缩至微秒级。Guan 等[15]则另辟蹊径，引入区块链技术解决传统基于身份认证的密钥托管风险。该方案彻底摆脱了地面中心依赖，平均认证时延降至 100 ms 以内，但区块链的分布式共识机制带来额外的通信和计算开销，在 LEO 卫星星座的高动态拓扑下仍面临节点同步难题。

2　系统模型

2.1　系统框架

系统框架如图 1 所示，其中涉及 3 个实体：各类用户终端（user terminal, UT）、LEO 卫星和地面控制中心（ground control center, GCC）。由于天地一体化网络中星上计算资源紧张，处理能力受限，目前天地一体化网络中资源管理和安全防护都放在地面进行，卫星组网路由阶段大多经过 GCC[16-17]。此外，星地无线链路开放暴露，极易遭受窃听、篡改、伪造及中间人攻击，对协议的轻量性与抗攻击能力提出了双重要求。

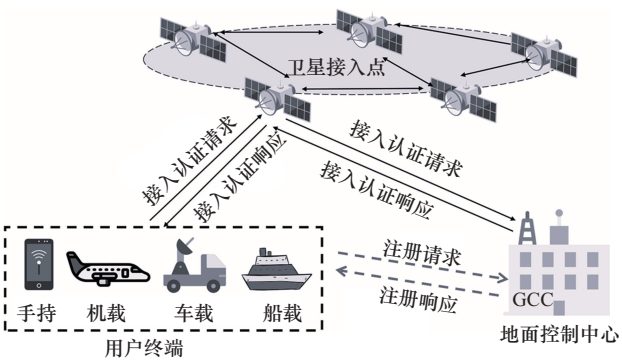

图 1　系统框架

因此，本文协议采用星地协同的设计思想，依托GCC完成核心密钥管理与可信支撑，有效规避星上资源瓶颈，同时适配动态接入场景。

2.2　安全目标

面向天地一体化网络的终端可信接入认证协议是保障星地异构网络可信互联的核心安全机制，旨在实现域内身份认证、资源协同及服务连续性[18]。本文协议应满足以下安全要求。

（1）双向认证。终端、卫星及网络控制中心三方身份互信，确保通信主体身份合法可信，并支持高动态拓扑下快速、安全的重认证。

（2）身份隐私与可审计性。在保护终端身份隐私、防止长期追踪的同时，实现身份的可控追溯与审计，兼顾匿名性与监管可追溯需求。

（3）端到端数据保护。保障端到端数据传输的机密性与完整性，抵御中间人攻击，实现安全、高效的数据通信保护。

3　方案设计

本节提出了一种天地一体化网络中的终端可信接入认证协议，该协议包括系统初始化、实体注册、初始接入认证与密钥协商和断线重认证与密钥协商4个阶段。本文中部分符号定义如表1所示。

表1　　符号定义

符号	说明
ID	真实身份
TID	伪身份
q,G	大素数/基点
s、P_{pub}	系统私钥/公钥
(sk,PK)	公私钥对
$K_{\text{U-L}}$,$K_{\text{L-U}}$	会话密钥
EXP_{time}	有效期
MAC	消息验证码
RE	认证返回值
Tag	快速认证标识
‖	连接运算
⊕	异或运算

3.1　系统初始化

系统初始化阶段由GCC完成系统安全参数的初始化配置，具体步骤如下。

步骤1　选定椭圆曲线群，该群的阶为素数q，生成元为G。

步骤2　生成随机数$s \in Z_q^*$作为系统主私钥，计算系统公钥$P_{\text{pub}} = sG$。

步骤3　选取抗碰撞的单向哈希函数H: $\{1,0\}^* \to Z_q^*$，向网络公开参数$\{q, G, H, P_{\text{pub}}\}$。

3.2　实体注册

在实体注册阶段，UT与LEO卫星需在GCC完成注册，整个注册流程通过安全信道执行，具体分为两个子阶段。

（1）用户终端注册阶段

步骤1　UT向GCC发送注册请求，包括真实身份标识ID_{U}。

步骤2　GCC接收到注册请求后，选择随机数$\text{sk}_{\text{U}} \in Z_q^*$作为用户私钥，计算对应的用户公钥$\text{PK}_{\text{U}} = \text{sk}_{\text{U}}G$，生成用户密码$\text{PW}_{\text{U}}$，向UT发送$\{(\text{sk}_{\text{U}}, \text{PK}_{\text{U}}), \text{PW}_{\text{U}}\}$。

步骤3　UT在本地安全存储$\{(\text{sk}_{\text{U}}, \text{PK}_{\text{U}}), \text{PW}_{\text{U}}\}$。

（2）LEO卫星接入点注册阶段

步骤1　LEO卫星向GCC发送注册请求，包括真实身份标识ID_{L}。

步骤2　GCC接收到注册请求后，选择随机数$\text{sk}_{\text{L}} \in Z_q^*$作为卫星私钥，计算对应的卫星公钥$\text{PK}_{\text{L}} = \text{sk}_{\text{L}}G$，生成卫星密码$\text{PW}_{\text{L}}$，向LEO卫星发送$\{(\text{sk}_{\text{L}}, \text{PK}_{\text{L}}), \text{PW}_{\text{L}}\}$。

步骤3　LEO卫星在本地安全存储$\{(\text{sk}_{\text{L}}, \text{PK}_{\text{L}}), \text{PW}_{\text{L}}\}$。

3.3　初始接入认证与密钥协商

初始接入认证与密钥协商阶段面向终端首次接入低轨卫星网络的场景，完整流程如图2所示，具体步骤如下。

步骤1　UT获取当前时间戳T_1，选择随机数$r_{\text{U}} \in Z_q^*$作为临时私钥，计算$R_{\text{U}} = r_{\text{U}}G$作为临时公钥。生成伪身份$\text{TID}_{\text{U}} = \text{ID}_{\text{U}} \oplus H(\text{sk}_{\text{U}} \| T_1)$，计算消息验证码$\text{MAC}_{\text{U}} = r_{\text{U}} + \text{sk}_{\text{U}} H(\text{TID}_{\text{U}} \| R_{\text{U}} \| \text{PW}_{\text{U}} \| T_1)$。向LEO卫星发送请求消息$M_1 = \{\text{TID}_{\text{U}}, R_{\text{U}}, T_1, \text{MAC}_{\text{U}}\}$。

步骤2　LEO卫星收到M_1后，检查时间戳T_1的新鲜度，检验通过后获取当前时间戳T_2，同时暂存UT的临时公钥R_{U}。选择随机数$r_{\text{L}} \in Z_q^*$作为临时私钥，计算$R_{\text{L}} = r_{\text{L}}G$作为临时公钥。生成伪身份$\text{TID}_{\text{U}} = \text{ID}_{\text{L}} \oplus H(\text{sk}_{\text{L}} \| T_2)$，计算消息验证码

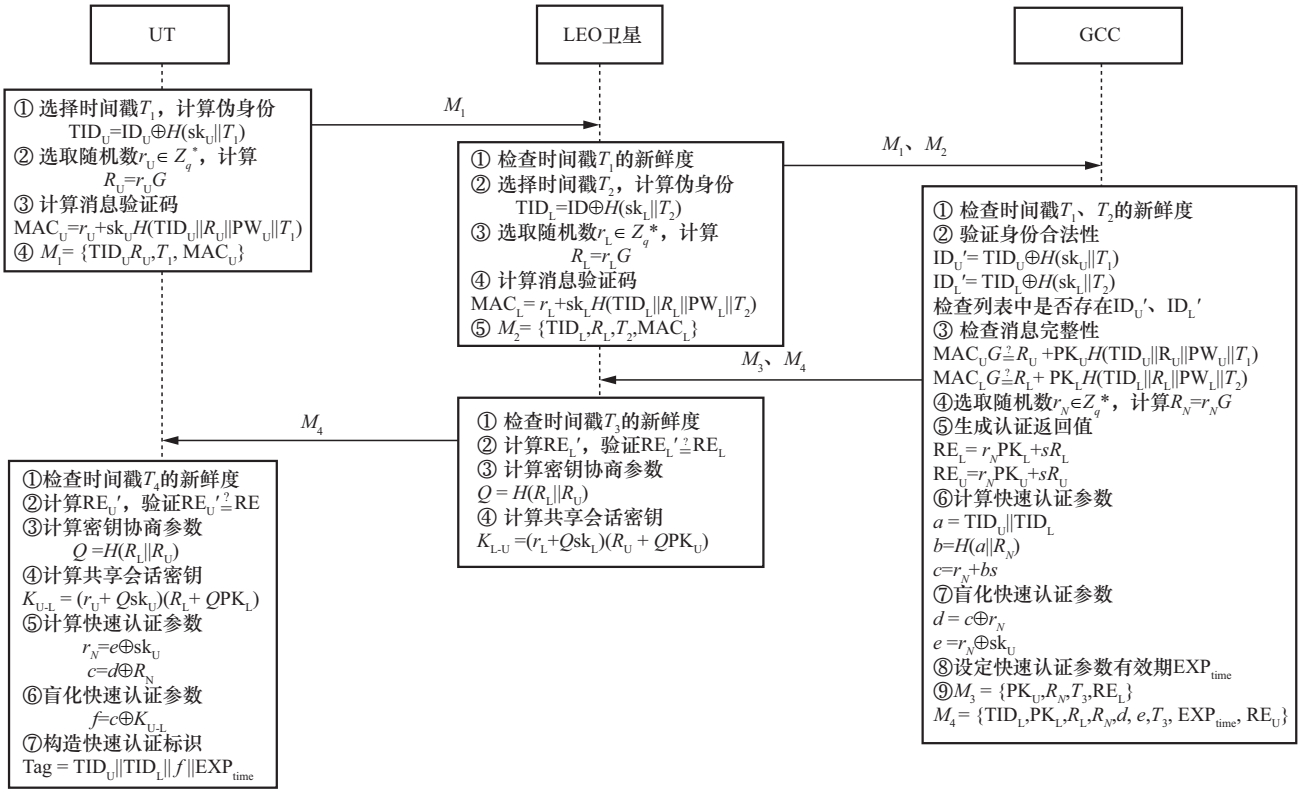

图2　初始接入认证与密钥协商

$MAC_L=r_L+sk_LH(TID_L||R_L||PW_L||T_2)$。将$\{M_1,M_2\}$转发至GCC，其中$M_2=\{TID_L,R_L,T_2,MAC_L\}$。

步骤3　GCC收到消息后，检查时间戳T_1、T_2的新鲜度，检验通过后获取当前时间戳T_3。计算$ID_U'=TID_U\oplus H(sk_U||T_1)$、$ID_L'=TID_L\oplus H(sk_L||T_2)$，通过将$ID_U'$和$ID_L'$与真实身份对比验证合法性。根据身份标识查找对应的密码PW_U和PW_L，计算$MAC_UG\stackrel{?}{=}R_U+PK_UH(TID_U||R_U||PW_U||T_1)$、$MAC_LG\stackrel{?}{=}R_L+PK_LH(TID_L||R_L||PW_L||T_2)$对消息完整性进行验证。身份认证后，GCC选择随机数$r_N\in Z_q^*$作为临时私钥，计算$R_N=r_NG$作为临时公钥，分别生成LEO卫星和UT的认证返回值$RE_L=r_NPK_L+sR_L$和$RE_U=r_NPK_U+sR_U$。

为提高用户断线后重连效率，初次接入认证时GCC同步生成快速认证参数。令$a=TID_U||TID_L$，计算$b=H(a||R_N)$、$c=r_N+bs$。GCC计算保护参数$d=c\oplus r_N$和中介参数$e=r_N\oplus sk_U$，设定EXP_{time}为快速认证参数的有效期。构造响应消息$M_3=\{PK_U,R_N,T_3,RE_L\}$、$M_4=\{TID_L,PK_L,R_L,R_N,d,e,T_3,EXP_{time},RE_U\}$并向LEO卫星发送。

步骤4　LEO卫星收到消息后，检查时间戳T_3的新鲜度，检验通过后获取当前时间戳T_4。计算认证返回值$RE_L'=r_LP_{pub}+sk_LR_N$，计算$RE_L'\stackrel{?}{=}RE_L$以验证GCC的身份。认证通过后LEO卫星计算会话参数$Q=H(R_L||R_U)$，得到共享会话密钥$K_{L\text{-}U}=(r_L+Qsk_L)(R_U+QPK_U)$。LEO卫星存储$\{TID_U,P_{pub}\}$，在参数有效期内暂存$\{K_{L\text{-}U},R_N\}$，并向UT转发$M_4$。

步骤5　UT收到M_4后，检查时间戳T_4的新鲜度，检验通过后计算认证返回值$RE_U'=r_UP_{pub}+sk_UR_N$，计算$RE_U'\stackrel{?}{=}RE_U$以验证GCC的身份。认证通过后UT计算会话参数$Q=H(R_L||R_U)$，得到共享会话密钥$K_{U\text{-}L}=(r_U+Qsk_U)(R_L+QPK_L)$。根据参数$d$、$e$计算快速认证参数$c$和保护参数$f=c\oplus K_{U\text{-}L}$。构造快速认证标识$Tag=TID_U||TID_L||f||EXP_{time}$用于后续断线重认证。

3.4　断线重认证与密钥协商

星地链路处于开放暴露状态，易遭受安全威胁。在链路发生异常中断后，星地双方依托预存储的快速认证参数，完成轻量级的身份认证与会话密钥协商，确保高动态断连场景下协议安全属性，提高协议的效率。完整流程如图3所示，具体步骤

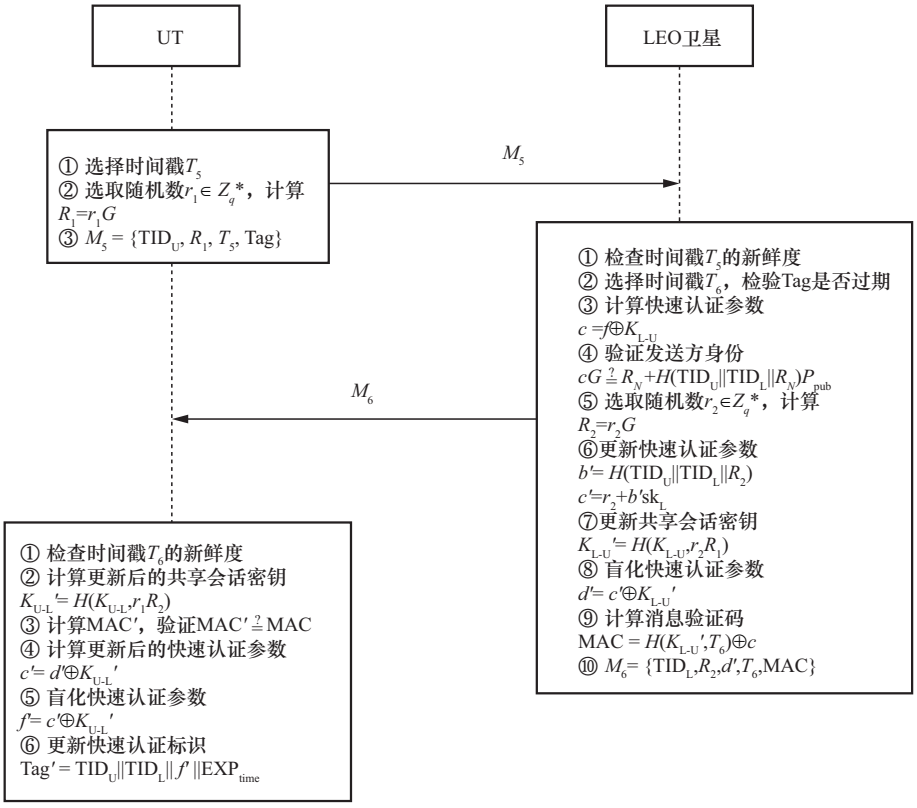

图3　断线重认证与密钥协商

如下。

步骤 1　UT 获取当前时间戳 T_5，生成随机数 $r_1 \in Z_q^*$ 作为重连会话的临时私钥，计算对应的临时公钥 $R_1 = r_1G$。向 LEO 卫星发送重连请求信息 $M_5 = \{\mathrm{TID_U}, R_1, T_5, \mathrm{Tag}\}$，触发重认证流程。

步骤 2　LEO 卫星收到 M_5 后，检查时间戳 T_5 的新鲜度，检验通过后获取当前时间戳 T_6。验证快速认证标识 Tag 中的有效期，检验通过后恢复快速认证参数 $c = f \oplus K_{\mathrm{L\text{-}U}}$，计算 $cG \stackrel{?}{=} R_N + H(\mathrm{TID_U}\|\mathrm{TID_L}\|R_N)P_{\mathrm{pub}}$ 以验证 UT 的身份。

生成随机数 $r_2 \in Z_q^*$ 作为临时私钥，计算对应的临时公钥 $R_2 = r_2G$。更新快速认证参数和共享会话密钥：计算 $b' = H(\mathrm{TID_U}\|\mathrm{TID_L}\|R_2)$，得到 $c' = r_2 + b'\mathrm{sk_L}$ 和 $K_{\mathrm{L\text{-}U}}' = H(K_{\mathrm{L\text{-}U}}, r_2R_1)$。计算保护参数 $d' = c' \oplus K_{\mathrm{L\text{-}U}}'$ 和消息验证码 $\mathrm{MAC} = H(K_{\mathrm{L\text{-}U}}', T_6) \oplus c$。构造响应消息 $M_6 = \{\mathrm{TID_L}, R_2, d', T_6, \mathrm{MAC}\}$ 并发送至 UT。

步骤 3　UT 收到 M_6 后，检查时间戳 T_6 的新鲜度，检验通过后计算更新后的共享会话密钥 $K_{\mathrm{U\text{-}L}}' = H(K_{\mathrm{U\text{-}L}}, r_1R_2)$。计算消息验证码 $\mathrm{MAC} \stackrel{?}{=} H(K_{\mathrm{U\text{-}L}}', T_6) \oplus c$ 验证消息的完整性。LEO 卫星恢复出更新后的快速认证参数 $c' = d' \oplus K_{\mathrm{U\text{-}L}}'$，同时计算保护参数 $f' = c' \oplus K_{\mathrm{U\text{-}L}}'$。更新快速认证标识 $\mathrm{Tag}' = \mathrm{TID_U}\|\mathrm{TID_L}\|f'\|\mathrm{EXP_{time}}$。并用新的快速认证参数 c'、d' 和 f' 替换原有的认证参数 c、d 和 f，新的快速认证标识 Tag' 替换原有的快速认证标识 Tag、新的共享会话密钥 $K_{\mathrm{U\text{-}L}}'$ 替换原有的共享会话密钥 $K_{\mathrm{U\text{-}L}}$。

每次断线重连都生成新的随机数 r_1 和 r_2，并更新认证参数和快速认证标识，以及用户和卫星之间的共享会话密钥 $K_{\mathrm{U\text{-}L}}$，提高了抵抗重放攻击的能力。

4　安全性分析

4.1　基于 ROR 的形式化证明

本节使用 ROR 模型来分析评估本文协议是可证明安全的。协议涉及 3 个参与实体：发起方终端 A、响应方卫星 B 和 GCC。使用 Π_U^i 表示参与者 U 的第 i 个协议实例，其中 $U \in S_{\mathrm{A}}, S_{\mathrm{B}}, \mathrm{GCC}$。每个实例在协议执行过程中维护自身的内部状态，攻击者 $\mathcal{A}$ 通过以下查询与协议交互。

$\mathrm{Execute}(\Pi_{\mathrm{A}}^i, \Pi_{\mathrm{AAS}}^k, \Pi_{\mathrm{B}}^j)$：$\mathcal{A}$ 窃听并记录该会话

在星地链路上传输的所有消息。

Send(Π_U^i,m)：$\mathcal{A}$向实例Π_{U}^i发送消息m并接收响应，以此模拟伪造、重放或篡改攻击。

Hash(m)：$\mathcal{A}$输入消息m，若列表中已有记录则返回对应哈希值，否则返回一个新的随机值。

Reveal(Π_U^i)：$\mathcal{A}$获得该实例当前已生成的会话密钥$\mathrm{SK_{AB}}$。

Corrupt(U)：模拟设备物理俘获或内部攻击，若$\mathcal{A}$执行此询问能窃取到U设备内存中所有的秘密参数。此查询不泄露当前未结束会话中的临时随机数。

Test(Π_U^i)：用于检验会话密钥的不可区分性。预言机抛掷一枚硬币$b\in\{0,1\}$。若$b=1$，返回真实的会话密钥$\mathrm{sk_{AB}}$；若$b=0$，返回与$\mathrm{sk_{AB}}$等长的随机字符串。

定理1 假设$\mathcal{A}$是在多项式时间t内攻击本文方案的敌手。那么，敌手$\mathcal{A}$在推导U^{α}和L^{β}之间的共享会话密钥$K_{\mathrm{U-L}}$和$K_{\mathrm{L-U}}$的优势可以估计为：

$$\mathrm{Adv}_P^{\mathrm{ake}}(A)\leqslant\frac{q_h^2}{2^{l_{\mathrm{hash}}}}+\frac{(q_{\mathrm{send}}+q_h)^2}{2^{l_{\mathrm{nonce}}}}\tag{1}$$

其中，l_{hash}为哈希输出长度，l_{nonce}为随机数长度，q_{send}和q_h分别为Send和Hash查询次数。

证明 本文方案将设计序列游戏Game_0~Game_5来模拟攻击过程。设Succ_i为攻击者$\mathcal{A}$在Game_i中赢得Test()查询的事件。

Game_0：ROR模型下的初始游戏，完全模拟攻击者在真实网络环境下的攻击行为。该游戏成功的概率与方案无法抵抗敌手$\mathcal{A}$攻击的概率是一致的。通过语义安全的定义得到：

$$\mathrm{Adv}_P^{\mathrm{ake}}(A)=\left|2\Pr[\mathrm{Succ}_0]-1\right|\tag{2}$$

Game_1：在此游戏中，$\mathcal{A}$执行Execute()查询以被动窃听信道上的所有消息。在UT、LEO卫星和GCC之间通信的消息如下。

Msg1. UT—>LEO：$\{\mathrm{TID_U},R_{\mathrm{U}},T_1,\mathrm{MAC_U}\}$

Msg2. LEO—>GCC：$\{M_2,\mathrm{TID_L},R_{\mathrm{L}},T_2,\mathrm{MAC_L}\}$

Msg3. GCC—>LEO：$\{\mathrm{PK_U},R_N,T_3,\mathrm{RE_L}\}$

Msg4. LEO—>UT：$\{\mathrm{TID_L},\mathrm{PK_L},R_{\mathrm{L}},R_N,d,e,T_3,\mathrm{EXP_{time}},\mathrm{RE_U}\}$

消息可以被敌手$\mathcal{A}$读取或拦截，$\mathcal{A}$执行Test()查询以检查输出是会话密钥还是随机值。由于$\mathcal{A}$未执行任何主动查询且不知晓任何主密钥，因此，$\mathcal{A}$从窃听中获得的信息不足以区分真实密钥与随机数，其获胜概率与Game_0相同。

$$\left|\Pr[\mathrm{Succ}_1]-\Pr[\mathrm{Succ}_0]\right|=0\tag{3}$$

Game_2：模拟Send()和Hash()查询，排除哈希碰撞和随机数碰撞对安全性的干扰。这轮游戏被视为主动攻击，其中敌手$\mathcal{A}$试图欺骗参与者相信已被篡改或伪造的消息。在本文方案中，消息{Msg1, Msg2, Msg3, Msg4}与当前时间戳、随机数和参与者身份相关联，因此它们是新鲜的。即使敌手使用篡改或伪造的消息连续执行Hash()查询，这些查询中的目标消息也不会发生冲突。因此，基于生日悖论，有如下关系。

$$\left|\Pr[\mathrm{Succ}_2]-\Pr[\mathrm{Succ}_1]\right|\leqslant\frac{q_h^2}{2^{l_{\mathrm{hash}}}}+\frac{(q_{\mathrm{send}}+q_h)^2}{2^{l_{\mathrm{nonce}}}}\tag{4}$$

Game_3：此游戏模拟设备物理俘获场景，假设敌手$\mathcal{A}$在目标会话结束后执行Corrupt(S_A)查询，那么在这轮游戏中，$\mathcal{A}$可以从UT获得所有秘密参数$\{r_{\mathrm{U}},\mathrm{sk_U},\mathrm{ID_U},c\}$。另外，如果$\mathcal{A}$可以从$\{R_{\mathrm{U}}=r_{\mathrm{U}}G,\mathrm{PK_U}=\mathrm{sk_U}G,\mathrm{TID_U}=\mathrm{ID_U}\oplus H(\mathrm{sk_U}\|T_1),c=r_N+bs\}$中猜测出用户的秘密参数，那么只有知道共享会话密钥$K_{\mathrm{U-L}}$和系统私钥$s$才能实现。而且$\mathcal{A}$可以试图使用物理俘获攻击从卫星接入点LEO中获取秘密参数$\{\mathrm{sk_L},r_{\mathrm{L}}\}$，但通过Send()查询从LEO卫星处的秘密参数恢复会话密钥在计算上是不可行的。这证明即使设备被俘获，历史会话密钥依然是安全的。

$$\left|\Pr[\mathrm{Succ}_3]-\Pr[\mathrm{Succ}_2]\right|\approx 0\tag{5}$$

Game_4：模拟地面站被攻破或内部恶意卫星的场景，假设$\mathcal{A}$执行Corrupt(NCC)，获得卫星接入点的长期密钥$\mathrm{sk_L}$，此时$\mathcal{A}$可以解密LEO卫星与GCC的消息并获得$\mathrm{ID_L}$。但若$\mathcal{A}$想计算最终双方的共享会话密钥，须获取星地链路上的随机数r_{L}。在消息M_2中，r_{L}可通过$R_{\mathrm{L}}G$或$\mathrm{MAC_L}=r_{\mathrm{L}}+\mathrm{sk_L}H(\mathrm{TID_L}\|R_{\mathrm{L}}\|\mathrm{PW_L}\|T_2)$获取，由于密码$\mathrm{PW_L}$是在注册阶段离线预置在卫星中的，$\mathcal{A}$无法获得此凭证，因此无法计算$K_{\mathrm{L-U}}$。实现对地面站信任的解耦。

$$\left|\Pr[\mathrm{Succ}_4]-\Pr[\mathrm{Succ}_3]\right|=0\tag{6}$$

Game_5：在排除上述所有攻击手段后，$\mathcal{A}$面对Test()查询时，由于始终缺少计算共享会话密钥的必要参数，故拥有的信息与随机数在统计上是不可

区分的。$\mathcal{A}$ 赢得游戏的概率为:

$$\Pr[\mathrm{Succ}_5]=\frac{1}{2} \tag{7}$$

综合式(1)~式(6),利用三角不等式 $|a\pm b|\leqslant|a|+|b|$ 累加各游戏的优势差,得到:

$$\mathrm{Adv}_P^{\mathrm{ake}}(A)\leqslant 2\left(\frac{q_h^2}{2^{l_{\mathrm{hash}}}}+\frac{(q_{\mathrm{send}}+q_h)^2}{2^{l_{\mathrm{nonce}}}}\right) \tag{8}$$

哈希长度 l_{hash} 和随机数长度 l_{nonce} 足够大,该优势是可忽略的。证毕。

4.2　基于 Tamarin 的安全证明

本文的实验平台为 Ubuntu22.04 操作系统,使用的是 Tamarin1.12.0 版本。Tamarin 通过 autoprove 自动证明安全引理,工具会搜索满足引理约束的执行轨迹,判断是否存在反例。若找到符合引理的轨迹,代表引理存在可行执行路径,在验证界面输出 SOLVED // trace found 并生成对应的证明脚本;若不存在满足条件的轨迹,则引理无法成立。图 4 为协议构建的 4 个安全引理的证明,包括身份隐私的保护、会话密钥的机密性、断线重连的前提等。下面展示协议中一个安全引理的关键建模过程。

当 UT 与 LEO 卫星完成初始接入认证后,应能协商出共享会话密钥,且若在某时刻建立了共享会话密钥,则在此前必然已发生对应的 UT_Completed (ID_U, ID_L),即完成认证是建立会话密钥的前提,示例如下。

lemma SessionKey_Established:

exists-trace

"Ex ID_U ID_L K #*i* #*j*.

SessionKey(ID_U, ID_L, K) @ #*i* &

UT_Completed(ID_U, ID_L) @ #*j* &

#*j* < #*i*"

结果证明,协议中的各参与实体能够正确解析消息、同步更新密钥、安全保存参数,不存在协议死锁或参数类型不匹配的问题。

4.3　非形式化安全证明

本节将从以下几方面进行安全性分析。

(1) 双向认证。以 LEO 卫星与 GCC 之间的认证为例,LEO 卫星利用私钥计算消息验证码 MAC,GCC 利用公钥计算其发送的 MAC 是否等于 $R_{\mathrm{L}}+\mathrm{PK}_{\mathrm{L}}H(\mathrm{TID}_{\mathrm{L}}\|R_{\mathrm{L}}\|\mathrm{PW}_{\mathrm{L}}\|T_2)$ 以判断身份合法性。而 GCC 发送认证返回值 RE_{L},LEO 卫星计算其是否等于 $r_{\mathrm{L}}P_{\mathrm{pub}}+\mathrm{sk}_{\mathrm{L}}R_N$ 以判断身份合法性,以此实现对 GCC 的认证。

(2) 前向后向安全性。UT 和 LEO 卫星通过 $(r_{\mathrm{L}}+Q\mathrm{sk}_{\mathrm{L}})(r_{\mathrm{U}}+Q\mathrm{sk}_{\mathrm{U}})G$ 建立会话密钥。由于每次建立会话密钥使用的随机数 r_{L} 和 r_{U} 都是独立生成,因此不同会话之间建立的会话密钥没有直接关联,实现了前向后向安全性。

(3) 抵抗中间人攻击。UT、LEO 卫星发送的消息 M_1 和 M_2 包含伪身份 $\mathrm{TID}_{\mathrm{U}}$、$\mathrm{TID}_{\mathrm{L}}$ 和消息验证码 $\mathrm{MAC}_{\mathrm{U}}$、$\mathrm{MAC}_{\mathrm{L}}$,以修改消息 $M_1=\{\mathrm{TID}_{\mathrm{U}},R_{\mathrm{U}},T_1,\mathrm{MAC}_{\mathrm{U}}\}$ 为例,敌手 $\mathcal{A}$ 伪造 UT 的临时私钥 r_{U}'、长期私钥 $\mathrm{sk}_{\mathrm{U}}'$ 和密码 $\mathrm{PW}_{\mathrm{U}}'$,计算 $\mathrm{MAC}_{\mathrm{U}}'=r_{\mathrm{U}}'+\mathrm{sk}_{\mathrm{U}}'H(\mathrm{TID}_{\mathrm{U}}\|R_{\mathrm{U}}\|\mathrm{PW}_{\mathrm{U}}'\|T_1)$。由于临时私钥为随机数,而长期私钥和密码基于注册阶段获得,敌手 $\mathcal{A}$ 无法获取,因此敌手 $\mathcal{A}$ 计算的 $\mathrm{MAC}_{\mathrm{U}}'\neq\mathrm{MAC}_{\mathrm{U}}$ 无

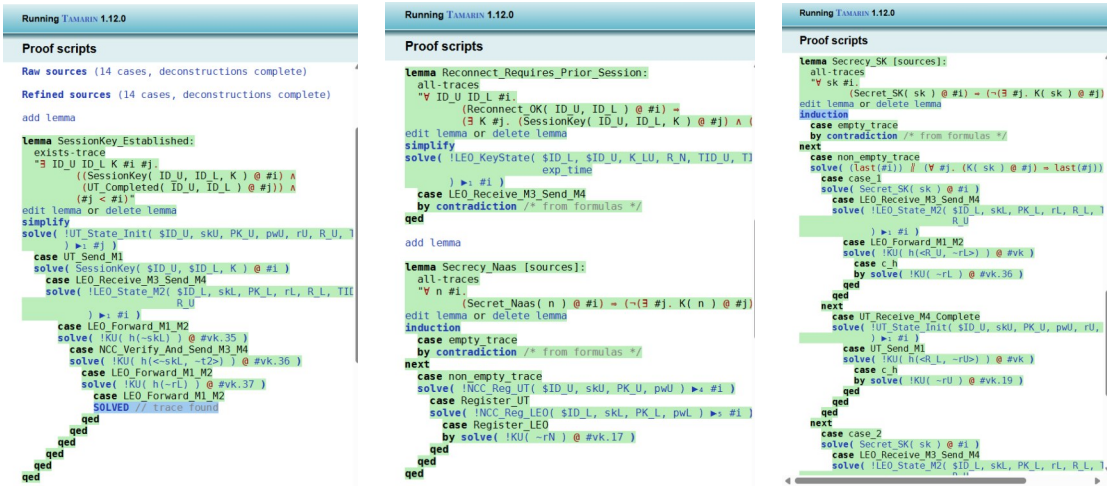

图 4　安全引理自动化验证结果

法通过GCC的认证，故本文协议可以抵抗中间人攻击。

（4）抵抗拒绝服务攻击

接收方需要通过消息中的消息验证码MAC或认证返回值RE计算哈希值并进行完整性和间接的身份认证，如GCC对MAC_U和MAC_L的验证、UT和LEO卫星对RE_U和RE_L的验证，使响应节点能够在协议执行过程中拒绝来自敌手$\mathcal{A}$的非法请求，从而有效抵御拒绝服务攻击。

5　性能分析

本节将本文协议与基于椭圆曲线密码学（elliptic curve cryptography, ECC）的协议[8]、基于哈希函数的协议[11]和基于对称密码体制的协议[12]进行安全特性、计算开销、通信开销和时延开销4个方面的性能对比分析。通过与同类协议的比较，证明本文协议适用于天地一体化网络中的终端接入认证。

5.1　安全特性

本节从双向认证等7个方面将本文协议中的初始接入认证和断线重连阶段与文献[8,11-12]进行对比，如表2和表3所示。

表2　初始接入认证安全性对比

安全特性	文献[8]	文献[11]	文献[12]	本文协议
双向认证	√	√	√	√
身份隐私保护	√	√	√	√
前向后向安全性	×	√	√	√
抵抗中间人攻击	×	×	√	√
抵抗假冒攻击	×	√	×	√
抵抗重放攻击	√	√	√	√
抵抗拒绝服务攻击	√	×	×	√

结果表明，文献[8,11-12]在初始接入认证阶段可以满足大部分安全特性，但不能完全抵抗所有攻击；在断线重连阶段则安全性较差，而本文协议在两个阶段均能够满足表中所述的安全特性要求或抵抗相应攻击，特别是在抵抗中间人攻击和拒绝服务攻击两个方面。

表3　断线重连安全性对比

安全特性	文献[8]	文献[11]	文献[12]	本文协议
双向认证	√	√	√	√
身份隐私保护	√	√	√	√
前向后向安全性	×	√	√	√
抵抗中间人攻击	×	×	√	√
抵抗假冒攻击	×	√	×	√
抵抗重放攻击	√	√	√	√
抵抗拒绝服务攻击	√	×	×	√

5.2　计算开销

本文实验环境操作系统为Ubuntu 18.04.6 64 bit，在VMware虚拟机运行，运行内存为4 GB。硬件环境为Intel(R) Core(TM) i5-10210U CPU@1.60 GHz。随机模拟1 000次不同密码运行操作进行分析，模拟得出协议中涉及的密码学运算耗时如表4所示（忽略异或运算和级联运算耗时）。

表4　密码学运算耗时

运算	开销/ms
T_h	0.002 3
T_{mul}	0.005 3
T_{sym}	0.004 6
T_{ecm}	2.226
T_{eca}	0.028 8

使用表4中的密码学操作执行时间计算本文提出的终端初始接入认证及断线重连与文献[8,11-12]中相同两个阶段的计算开销进行对比，结果如表5和图5所示。

表5　协议计算开销对比

协议	初始接入认证阶段			初始接入认证阶段/ms	断线重连阶段/ms
	UT/ms	LEO卫星/ms	GCC/ms		
文献[8]	$7T_h+4T_{ecm}$	$5T_h+T_{eca}+5T_{ecm}$	$10T_h+3T_{eca}+8T_{ecm}$	$22T_h+4T_{eca}+17T_{ecm}$=38.007 8	$4T_h+2T_{eca}+3T_{ecm}$=6.744 8
文献[11]	$6T_h+2T_{sym}+3T_{ecm}$	$4T_h+1T_{sym}+3T_{ecm}$	$9T_h+2T_{sym}+4T_{ecm}$	$19T_h+5T_{sym}+10T_{ecm}$=22.326 7	$4T_h+2T_{sym}+3T_{ecm}$=6.696 4
文献[12]	$2T_h+2T_{eca}+3T_{ecm}$	$2T_h+2T_{eca}+3T_{ecm}$	$5T_h+2T_c+3T_{ecm}$	$9T_h+4T_{eca}+2T_c+9T_{ecm}$=23.079 9	$2T_h+2T_{sym}+2T_{eca}+3T_{ecm}$=6.749 4
本文协议	$4T_h+4T_{eca}+2T_{ecm}$	$4T_h+2T_{eca}+2T_{ecm}$	$6T_h+4T_{eca}+6T_{ecm}$	$14T_h+10T_{eca}+10T_{ecm}$=22.580 2	$2T_h+2T_{eca}+2T_{ecm}$=4.514 2

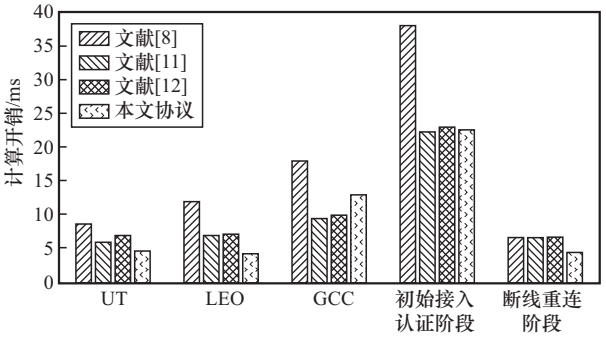

图5　协议计算开销对比

文献[8]在初始接入认证阶段所需开销较大，因其频繁使用复杂的双线性对运算，增加了计算量。而本文协议在初始接入认证阶段的计算开销略高于文献[11]，这是因为多花费了 1 次椭圆曲线标量乘法，计算了快速认证参数，能更安全便捷地实现后续断线重连过程。在断线重连阶段，本文协议利用快速认证参数完成双向认证，不需要 GCC 参与计算，因此计算开销比所有协议都更低。

5.3　通信开销

设定所有方案涉及的同类通信开销大小一致，使用的元数据长度如表 6 所示。

表 6　　元数据长度

元数据	长度/bit
L_{id}	32
L_h	160
L_t	32
L_p	512
L_n	512
L_c	480
L_{ecm}	320
L_{sym}	256

使用表 6 中的元数据长度，计算本文提出的终端初始接入认证阶段及断线重认证通信开销，并与文献[8,11-12]的通信开销进行对比，结果如表 7 和图 6 所示。本文协议在初始接入认证阶段总通信开销略高于文献[11]和文献[12]，相较于这二者而言，协议在初始接入认证阶段传递的消息中包含了快速认证参数的协商信息，该参数为后续安全快捷地实现断线重认证提供基础。在断线重连阶段，LEO 卫星只需要验证快速认证参数即可实现相互验证，该阶段的总通信开销远小于其他协议。

表 7　　协议通信开销对比

协议	消息数量/条		总通信开销/bit	
	初始接入认证	断线重连	初始接入认证	断线重连
文献[8]	5	3	$5L_{id}+5L_t+2L_{ecm}+8L_n$=5 568	$5L_{id}+2L_h+2L_{sym}+6L_t+4L_{ecm}$=2 464
文献[11]	4	3	$7L_{id}+6L_h+4L_t+8L_{ecm}$=4 256	$3L_{id}+4L_h+2L_{sym}+4L_t+2L_{ecm}$=2 016
文献[12]	4	3	$4L_{id}+8L_h+5L_t+2L_p+6L_{ecm}$=4 512	$4L_{id}+2L_h+4L_t+6L_{ecm}$=2 496
本文协议	4	2	$3L_{id}+7L_h+5L_t+10L_{ecm}$=4 576	$2L_{id}+2L_t+4L_{ecm}$=1 436

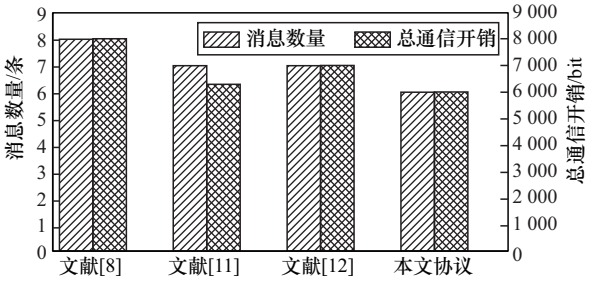

图6　协议通信开销对比

5.4　时延开销

在天地一体化网络实际场景中，星地无线传输存在传播时延、GCC 跨网转发引入额外排队时延，卫星切换产生状态同步开销。本节结合低轨卫星典型轨道参数、天地一体化组网工程实测参数，量化协议总时延为：

$$T_{total} = T_{calc} + NT_{prop} + T_{GCC} + T_{sync} \tag{9}$$

其中，T_{calc} 为星载处理器运算时延，T_{prop} 为星地传播时延，T_{GCC} 为 GCC 排队转发时延，T_{sync} 为参数同步时延，N 为交互轮次，T_{calc}' 为 5.2 节计算的桌面处理器计算开销，具体时延开销如表 8 所示。

表 8　　时延开销

时延	开销/ms
T_{calc}	$3.2T_{calc}'$
T_{prop}	3.66
T_{GCC}	5.5
T_{sync}	4

表 9 协议时延开销对比

协议	初始接入认证阶段/ms	断线重连阶段/ms	总认证时延/ms
文献[8]	$38.4T_h+7.2T_{eca}+27.8T_{ecm}+5T_{prop}+T_{GCC}$	$8.4T_h+2T_{eca}+17.4T_{ecm}+3T_{prop}+T_{NCC}+T_{sync}$	$46.8T_h+9.2T_{eca}+45.2T_{ecm}+8T_{prop}+2T_{GCC}+T_{sync}$=145.267 8
文献[11]	$41T_h+11.6T_{sym}+21.2T_{ecm}+4T_{prop}+T_{GCC}$	$8.4T_h+2T_{sym}+17.4T_{ecm}+3T_{prop}+T_{NCC}+T_{sync}$	$49.4T_h+13.6T_{sym}+38.6T_{ecm}+7T_{prop}+2T_{GCC}+T_{sync}$=126.719 8
文献[12]	$17.8T_h+12.8T_{eca}+2T_c+22.2T_{ecm}+4T_{prop}+T_{GCC}$	$2T_h+6.4T_{sym}+4.2T_{eca}+7.4T_{ecm}+3T_{prop}+T_{GCC}+T_{sync}$	$19.8T_h+6.4T_{sym}+17T_{eca}+29.6T_{ecm}+2T_c+7T_{prop}+2T_{GCC}+T_{sync}$=107.074 2
本文协议	$31.6T_h+23.2T_{eca}+22.2T_{ecm}+4T_{prop}+T_{GCC}$	$6.4T_h+6.4T_{eca}+3.2T_{ecm}+2T_{prop}+T_{sync}$	$38T_h+29.6T_{eca}+25.4T_{ecm}+6T_{prop}+T_{GCC}+T_{sync}$=88.935 1

根据式(9)和表 8 的数据，计算本文提出的终端初始接入认证及断线重认证总时延开销，并与文献[8,11-12]进行对比，结果如表 9 和图 7 所示。本文协议在认证时延上的优势主要体现在断线重连阶段，由于提前预置了快速认证参数，不需要 GCC 参与认证，减少了消息交互轮次，避免了 GCC 排队转发时延，降低了通信实体的运算量。

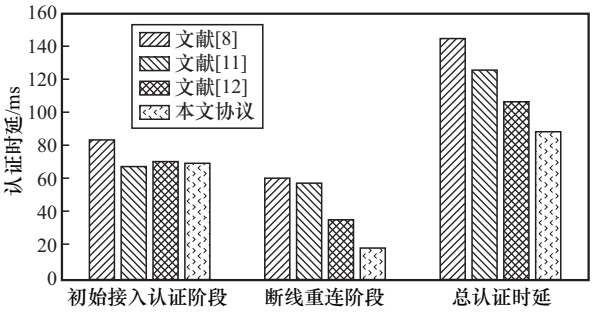

图 7 不同协议认证时延对比

根据 LEO 卫星轨道参数标准[19]，单星有效通信窗口约 764 s，本文协议时延开销远低于链路可用时长，可在链路失效前完成密钥协商。综合来看，天地一体化网络中终端断线重连为高频业务，本文协议在高频场景时延优势抵消初次接入认证微小开销，整体满足 LEO 卫星高动态、链路时变和资源受限的轻量化部署需求。

6 结束语

本文针对天地一体化网络中终端与卫星接入点的可信接入认证、断线重认证效率及通信与计算开销优化的问题，提出了一种终端可信接入认证与密钥协商协议。本文协议采用轻量级密码原语和零知识证明，实现了终端与卫星的双向身份认证、会话密钥协商，同时实现了用户身份隐私与通信数据的安全保护。GCC 作为半可信第三方，通过初始认证与密钥协商阶段完成终端与卫星的间接身份认证并生成快速认证参数，实现了断线场景下的快速重认证，有效降低了协议的整体通信与计算开销。通过 ROR 模型和 Tamarin 形式化验证工具，证明了协议在初次接入认证、会话密钥协商及断线重连场景下的安全性。实验与分析结果表明，本文协议在计算与通信上的综合开销较低，总认证时延较少，能够在保证高安全特性的同时显著降低系统开销，适配天地一体化网络的动态接入需求。

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] 李贺武, 吴茜, 徐恪, 等. 天地一体化网络研究进展与趋势[J]. 科技导报, 2016, 34(14): 95-106.
Li H W, Wu Q, Xu K, et al. Progress and tendency of space and earth integrated network[J]. Science & Technology Review, 2016, 34(14): 95-106.

[3] 谢绒娜, 谭莉, 武佳卉, 等. 面向天地一体化网络的认证与密钥协商协议[J]. 密码学报, 2023(5): 1035-1051.
Xie R N, Tan L, Wu J H, et al. Authentication and key agreement protocol for space-ground integrated network[J]. Journal of Cryptologic Research, 2023(5): 1035-1051.

[4] Zheng G, Ma H T, Cheng C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks[J]. IET Information Security, 2012, 6(1): 6-13.

[5] Zhao W W, Zhang A X, Li J H, et al. Analysis and design of an authentication protocol for space information network[C]//Proceedings of the MILCOM 2016 - 2016 IEEE Military Communications Conference. Piscataway: IEEE Press, 2016: 43-48.

[6] Altaf I, Saleem M A, Mahmood K, et al. A lightweight key agreement and authentication scheme for satellite-communication systems[J]. IEEE Access, 2020, 8: 46278-46287.

[7] Xu S S, Liu X D, Ma M M, et al. An improved mutual authentication protocol based on perfect forward secrecy for satellite communications[J]. International Journal of Satellite Communications and Networking, 2020, 38(1): 62-73.

[8] Huang H H, Miao X Y, Wu Z H, et al. An efficient ECC-based authentication scheme against clock asynchronous for spatial information network[J]. Mathematical Problems in Engineering, 2021, 2021: 8811970.

[9] Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications[J]. Computer Communications, 2019, 147: 85-97.

[10] Kumar U, Garg M. Learning with error-based key agreement and authentication scheme for satellite communication[J]. International Journal of Satellite Communications and Networking, 2022, 40(2): 83-95.

[11] Dharminder D, Dadsena P K, Gupta P, et al. A post quantum secure construction of an authentication protocol for satellite communication[J]. International Journal of Satellite Communications and Networking, 2023, 41(1): 14-28.

[12] 曹进, 石小平, 马如慧, 等. 融合双层卫星网络的星地和星间AKA协议[J]. 网络与信息安全学报, 2023, 9(1): 18-31.
Cao J, Shi X P, Ma R H, et al. Fusion of satellite-ground and inter-satellite AKA protocols for double-layer satellite networks[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 18-31.

[13] Yi Z, Du X H, Liao Y, et al. An access authentication algorithm based on a hierarchical identity-based signature over lattice for the space-ground integrated network[C]//Proceedings of the 2019 International Conference on Advanced Communication Technologies and Networking (CommNet). Piscataway: IEEE Press, 2019: 1-9.

[14] Ma R H, Cao J, Feng D G, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[J]. IEEE Internet of Things Journal, 2020, 7(4): 2791-2805.

[15] Guan J F, Wu Y N, Yao S, et al. BSLA: blockchain-assisted secure and lightweight authentication for SGIN[J]. Computer Communications, 2021, 176: 46-55.

[16] Cascudo I, Cozzo D, Giunta E. Verifiable secret sharing from symmetric key cryptography with improved optimistic complexity[C]//Advances in Cryptology-ASIACRYPT 2024. Singapore: Springer Nature Singapore, 2024: 100-128.

[17] Zia M, Obaidat M S, Mahmood K, et al. A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 1683-1690.

[18] Wang S B, Zhou X, Wen K, et al. Security analysis of a user authentication scheme for IoT-based healthcare[J]. IEEE Internet of Things Journal, 2023, 10(7): 6527-6530.

[19] Cakaj S. Practical horizon plane and communication duration for low earth orbiting (LEO) satellite ground stations[C]//Proceedings of the Wseas Transactions on Communications. New York: ACM Press, 2009: 373-383.

[作者简介]



谢绒娜（1976– ），女，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码理论与应用、数据安全与隐私保护。



周竞（2001– ），男，北京电子科技学院硕士生，主要研究方向为密钥管理、密钥协商。



张晨佳（2002– ），女，北京电子科技学院硕士生，主要研究方向为密钥管理、密钥协商。



史国振（1974– ），男，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码工程与应用、安全体系结构与系统安全。