

卫星互联网地面缺省场景下 用户设备的接入认证及重认证机制研究

卜秋雨¹, 曹进¹, 程利甫², 马如慧¹, 李晖¹

(1. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126;

2. 上海航天电子技术研究所, 上海 201109)

摘 要: 针对当前用户设备接入认证机制均需要地面参与带来较大的通信时延以及可扩展性差等问题, 提出一种卫星互联网地面缺省场景下的用户设备接入认证及重认证协议, 并进一步针对用户设备认证过程中可能发生断电重新连接和 AV 不同步等问题, 提出一种断电重连场景下的用户设备快速认证机制和 AV 快速安全同步机制, 确保用户可以安全地接入卫星网络并获取相关服务。在所提出的方案中, 利用初次接入认证中生成的 AV 向量来辅助重认证过程完成实体之间的身份认证, 无须网络控制中心的参与, 保障了通信系统的容灾性。形式化验证工具 Scyther 表明, 该协议可以抵抗常见的协议攻击, 保障通信过程中的机密性和完整性, 并且具有较小的计算、带宽以及存储开销, 适用于卫星互联网。

关键词: 卫星互联网; 地面缺省; 接入认证; 重认证

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2023017

Research on Access Authentication and Re-Authentication Mechanism of User Devices in Terrestrial Default Scenario in Satellite Internet

BU Qiuyu¹, CAO Jin¹, CHENG Lifu², MA Ruhui¹, LI Hui¹

1. School of Cyber Engineering, Xidian University, Xi'an 710126, China;

2. Shanghai Aerospace Electronic Technology Institute, Shanghai 201109, China

Abstract: For the current user device access authentication mechanism requires ground participation to bring about large communication delays and poor scalability, a user device access authentication and re-authentication protocol in the ground default scenario in the space-ground integrated network was proposed, and further for the user device authentication process may occur in the power outage reconnection and AV asynchronization and other problems, a user device fast authentication mechanism and AV fast security synchronization mechanism under power failure reconnection scenario were proposed to ensured that users could safely accessed the satellite network and obtain related services. In the proposed scheme, the AV vector generated in the initial access authentication was used to assisted the re-authentication process to completed the authentication between entities without the involvement of the network control center, which guaranteed the communication system resilience. The formal verification tool Scyther showed that the proposed protocol was resistant to common protocol attacks, guaranteed the confidentiality and integrity of the communication process, and had a small signaling, computational, and bandwidth overhead, made it suitable for the satellite internet.

Keywords: satellite internet, ground defaults, access authentication, re-authentication

收稿日期: 2023-01-31; 修回日期: 2023-05-10;

基金项目: 国家自然科学基金面上项目 (No. 61772404)

Foundation Item: The National Natural Science Foundation of China (No. 61772404)

0 引言

随着传统地面网络吞吐量的提高和传输时延的降低,人们对于随时随地进行通信的需求越来越迫切^[1]。将地面通信网络和卫星网络相融合的卫星互联网将发挥越来越大的技术优势,推进卫星互联网融合势在必行^[2]。

卫星互联网是由天基网络和地面网络组成的新型异构网络,以其庞大的卫星星座为主体、关口站节点为基础,互联了成熟的地面互联网和移动通信网,实现了信息资源的互联共享、高效协同^[3-4]。用户设备可以通过星地链路接入卫星天基信息网络来克服传统无线网络中地理限制的不足,使通信更加便捷。作为国家重要基础设施的卫星互联网,以其独特通信的优势,推动着我国科技领域、社会领域和经济领域的快速发展,产生了显著的综合效益。当前,我国卫星互联网采用多层次轨道卫星相结合的方式。其中,低地球轨道(Low Earth Orbit, LEO)卫星与其他轨道卫星相比,因其星地传输时延低、发射成本低等特点更适合提供数据通信和访问服务。

卫星互联网具有网络拓扑变化频繁、网络节点资源受限、星地传输时延大等特点。此外,由于网络中的节点处于高度暴露的环境之中,节点之间的信道属于公开信道,极易受到攻击者和敌方的攻击。这些特点使得传统地面通信协议如5G认证与密钥协商(Authentication and Key Agreement, AKA)在卫星网络环境下面临诸多挑战,如高度动态的网络拓扑可能导致协议中的密钥管理和分发变得复杂,网络节点资源受限可能导致5G AKA协议在处理能力和能耗方面难以满足卫星网络的需求。同时星地传输时延可能导致序列号(Sequence Number, SQN)同步问题,进一步影响协议的实时性和可靠性。此外,信道损耗和干扰可能导致数据包丢失,从而影响认证信令的正确性和消息认证码(MAC)校验。因此,传统地面通信协议如5G AKA难以直接应用到卫星网络下的用户设备接入场景中^[5]。为了构建安全高效的服务网络,首要问题就是解决卫星网络下的用户设备接入认证问题。其次,地面互联网基础设施易受自然灾害等的影响,导致通信服务中断和经济效益的巨大损失,需要设计在地面缺省条件下,即无须地面参与认证过程的用户设备重认证机制,保证用户可以稳定使用卫星网络提供的通信服务。并针对用户设备资源有限的特点,在认证过程中可能发生断电重新连接的情况,设计针对断电重连的快速认证机制。最后,在上述认证过程中,可能存在认证双方的AV向量不同步的情况,导致身份认证失

败,需要设计针对AV向量的快速安全同步机制,保障安全认证过程中所需安全参数的一致性。

随着卫星互联网的不断完善,用户设备-卫星接入点-地面控制中心常见的接入认证网络架构,根据使用的密码技术不同可以分为非对称密码体制、对称密码体制和轻量级密码体制^[6]。

在非对称密码体制中,参考文献[7]提出将非对称密码算法应用于卫星网络,实体之间的相关身份认证通过地面控制中心下发的数字证书来完成,然而该方案中大量的加解密操作,带来了较大的计算开销。参考文献[8]基于身份的非对称密码算法提出一种自我验证机制,实现用户设备和网络控制中心的双向认证,用户设备侧具有良好的性能开销。参考文献[9]提出一种利用证书的分布式管理模型,卫星层采用集中式证书管理,终端层和其他接入节点采用分布式管理,具有良好的扩展性。参考文献[10]提出一种基于椭圆曲线密码(Elliptic Curve Cryptography, ECC)体制的移动卫星网络认证方案,移动用户避免使用临时身份,降低了受到分布式拒绝服务(Distributed Denial of Service, DDoS)攻击的可能性,提高了认证系统抗干扰的能力。参考文献[11]提出一种基于ECC和轻量级哈希算法的接入认证机制,可以支持用户匿名性和不可追踪性,具有良好的用户体验。参考文献[12]提出一种安全高效的椭圆曲线多因素认证协议,实现了会话密钥的安全性。参考文献[13]提出一种基于ElGamal加密的卫星终端接入认证机制,减少了认证过程中的信令开销;除此以外,对于批量验证的支持使得在涉及大量用户时切换更加高效,然而在该方案中大量的点乘操作带来了较大的计算开销。参考文献[14]利用代理签名技术来确保授权的卫星节点可以从网关处获得权限,强调卫星节点具备认证功能,不需要网络控制中实时参与,降低了认证时延。参考文献[15]基于盲签名技术提出一种针对不同区域、不同类型的用户设备卫星网络接入认证方案,认证过程仅需要用户设备和卫星接入点两者的参与,减少了认证时延,但是该方案使用了大量的签名/验签操作,带来了较大的计算开销,不适用于卫星网络。参考文献[16]基于半聚合签名机制提出一种终端接入认证协议,具有前后向保密性,可以抵抗量子计算攻击,但是该方案使用了大量的矩阵向量点乘,带来较大的计算开销,不适用于卫星网络。

由于非对称密码算法可能会带来大量复杂的运算,针对对称密码算法的接入认证方案逐渐受到研究人员的密切关注。参考文献[17]首次基于对称密码提出一种移动用户设备接入认证方案,有效减少了用户设备接入卫星网络

过程中的计算开销,然而在认证过程中,使用当前会话密钥来加密新的会话密钥,密钥的后向安全性无法保证,带来了较大的安全隐患。参考文献[18]提出一种增强型的身份认证协议,提高了认证系统的抗干扰能力,但是用户的身份信息可能会被攻击者假冒从而带来严重的安全问题。参考文献[19]基于3GPP认证密钥协议提出一种认证机制,可以实现低轨卫星之间的快速组网、群组密钥的协商。参考文献[20]改进演进的分组交换系统认证与密钥协商(Evolved Packet System Based Authentication and Key Agreement, EPS-AKA),提出一种基于令牌的动态接入认证协议,用户可以接入低轨卫星网络,然而卫星节点的数据存储带来了巨大的压力。

参考文献[21]提出一种适用于移动卫星通信系统的增强密钥认证方案,不需要验证表来验证用户的身份和密码,降低了卫星的存储开销。参考文献[22]提出一种椭圆曲线密码体制和轻量级算法相结合的认证方案,实现了用户和网络控制中心之间的双向认证,具有完美的前向保密性。参考文献[23]指出参考文献[22]的方案并不能抵抗密码离线攻击和用户假冒攻击,因此提出一种改进的卫星移动的通信系统动态认证方案,实现了用户的匿名性,用户的隐私信息得以保护。参考文献[24]指出参考文献[23]的方案在认证阶段存在安全缺陷,用户与网络控制中心之间无法完成双向认证,进而无法建立安全的会话密钥,因此提出一种增强型移动卫星通信系统的认证方案,所提方案具有较低的信令开销和计算开销以及更强的安全性。

综上所述,本文提出一种地面缺省条件下的用户设备接入认证和重认证方案,其特点如下。

(1) 提出一种卫星互联网地面缺省条件下的用户设备接入认证和重认证机制,避免了因地面通信基础设施受到自然破坏或者军事打击等造成通信系统瘫痪的问题,实现用户和卫星网络节点之间的双向身份认证和会话密钥协商。

(2) 支持能耗不足的设备发生断电之后快速安全地重新接入卫星网络,保证用户可以稳定使用卫星网络提供的通信服务。

(3) 无地面网络参与的情况下需将一组认证向量 AV 发送给卫星节点来实现用户设备和卫星间的双向认证,但是由于卫星和用户设备的移动性,可能发生用户设备接入的卫星并不是拥有其认证向量的卫星,需要解决卫星节点间认证向量的快速共享和同步,提出一种认证向量 AV 快速安全同步机制,保障安全认证过程中所需安全参数的一致性。

(4) 采用安全分析和性能分析充分评估本文协议的安

全性,使用BAN逻辑和形式化验证工具Scyther证明其安全性。结合信令、计算、带宽以及存储开销对本文和其他类似方案进行对比,本文所提出的方案在满足所提安全性的前提下,减少了相关认证开销,达到了性能和安全性之间的平衡,更加适用于卫星互联网。

1 系统模型、安全需求和设计思路

1.1 系统模型

目前卫星互联网中的卫星网络具有一定的计算/存储能力,为更好地利用其资源,提高资源的利用率,设计了针对卫星互联网地面缺省条件下用户设备重认证的系统架构,如图1所示。其主要实体包括:用户设备(User Equipment, UE)、多层次天基信息网络以及网络控制中心(Network Control Center, NCC)。各实体功能如下所述。

(1) 用户设备是指具有卫星通信能力的各种类型用户终端,常见的用户设备分为手持设备、机载设备、车载设备、船载设备等。用户设备首先在网络控制中心注册获取相应的安全参数,通过星地链路接入多层次天基信息网络,访问相应的网络资源。

(2) 多层次天基信息网络由多层次卫星构成,其特点是具有不同轨道和倾角,可以承担一定的运算任务,主要通过卫星之间的协同工作支持星地链路的信息处理和数据传输^[25]。在LEO卫星网络中,每颗卫星运行在特定的轨道上,具有不同的倾角和高度,轨道高度范围通常在500~2 000 km。其特点是星地传输时延较小,一般作为用户设备接入卫星网络的接入点。LEO卫星可以通过之间的星间链路进行数据通信,具有灵活性高的特点,从而提供更高效的通信服务。MEO卫星网络由若干颗MEO卫星组成,相比LEO卫星,其轨道高度更高,覆盖范围更广,通信时延也 longer,但通信的可靠性更高。

(3) 网络控制中心是天基网络的主要管理者,主要负责相关安全参数的分发与管理、用户设备的注册与验证等,具有较好的计算/存储能力,可以执行大量复杂的计算。

1.2 安全需求

假设实体网络控制中心是完全可信的,除此以外,根据所述系统架构,用户设备在卫星互联网场景下进行重认证属于无线通信领域的场景。Dolev-Yao是无线通信领域中常见的威胁模型,攻击者将具有如监听、截获、篡改、重放信道消息的能力等。因此,用户设备的重认证机制安全需求如下。

(1) 双向认证:为了确保通信双方信息的有效性和完整性,LEO卫星需要验证UE身份的合法性,防止非法的

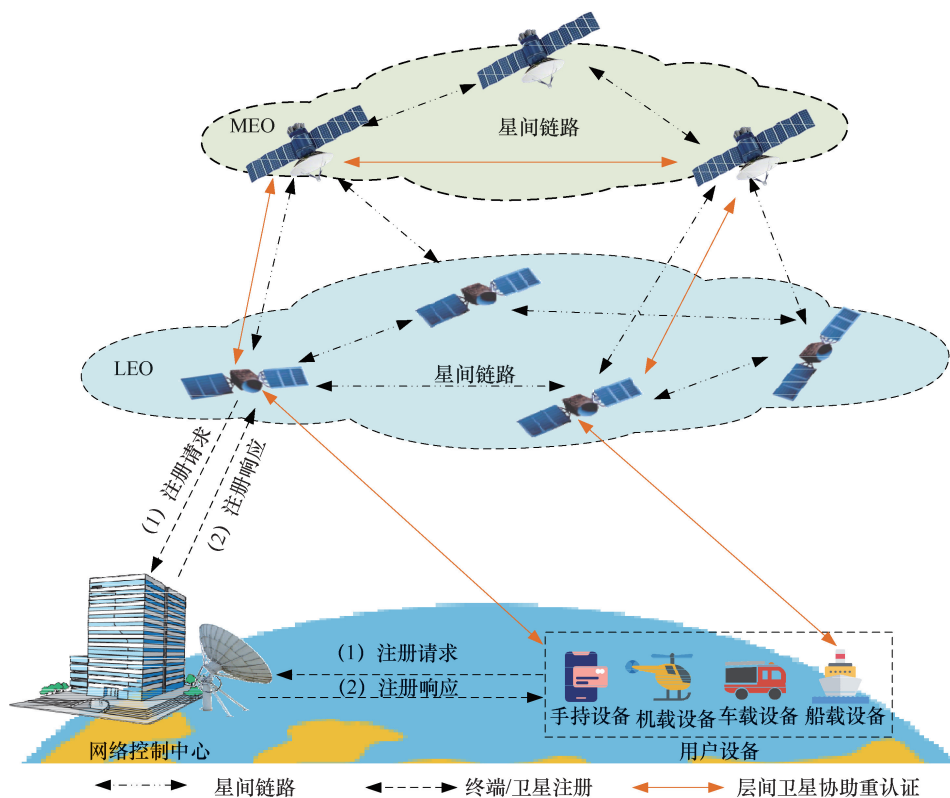


图1 系统架构

用户设备接入网络破坏其安全性或者获得相应的资源;UE需要验证LEO卫星的身份的可靠性,防止中间人攻击等,确保隐私信息不会被泄露。

(2) 会话密钥协商: 在用户设备初次接入认证之后,UE和接入卫星LEO卫星之间协商会话密钥,建立安全的通信信道,确保通信过程中消息的机密性不被破坏;当用户设备完成重认证之后,UE和拜访域卫星VLEO之间也应协商新的会话密钥,建立安全的通信信道。

(3) 条件隐私性: UE在认证过程中将使用NCC生成的临时身份标识进行通信。UE真实的身份标识只有NCC知道,网络中的其余实体不能获取其真实身份。NCC生成临时身份标识时应该具有独立性和随机性,防止网络中的攻击者以此追踪并进行相应的技术攻击。此外,对于UE的相关隐私信息,如位置信息,在传输时应进行加密保护来保障数据的安全性。

(4) 前后向安全性: 在认证过程中,要保证会话密钥的前向、后向安全性。虽然当前使用的会话密钥泄露,但是历史的或者未来的会话密钥不会被敌方计算或者推断出来,进而非法获取更多有关的用户信息,保障数据传输的安全性。

除上述所述攻击外,所设计的协议还应可以抵抗无线通信领域中常见的攻击,如中间人攻击、重放攻击等。

1.3 设计思路

本文的方案主要包括用户注册、初始接入、重认证、断电重连和AV同步5个阶段,设计思路如图2所示。

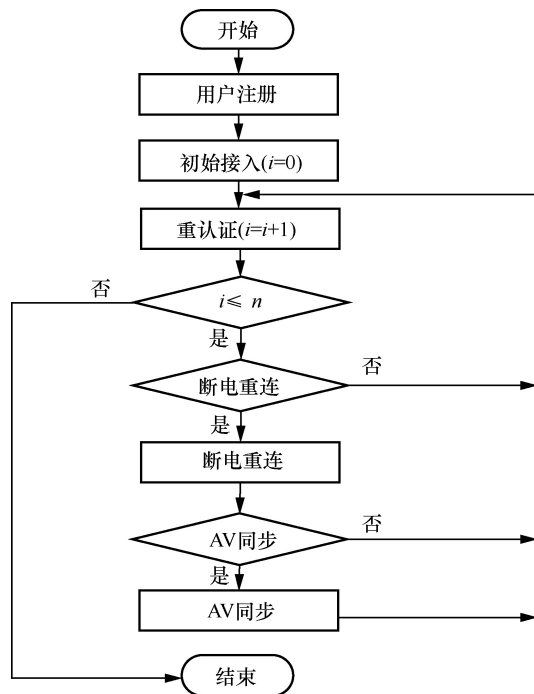


图2 设计思路

UE 首先在 NCC 处完成注册过程,包括临时身份标识的分发、预置长期共享密钥等。在初次接入认证阶段,UE 初次获得卫星网络的访问权限,主要通过轻量级哈希函数、异或操作、对称加密算法完成 UE 与 LEO 卫星之间的双向认证。通过用户设备的真实身份标识信息、随机数、位置信息生成会话密钥来保障数据传输的安全性。NCC 生成 AV 向量,发送至 LEO 卫星处。在重认证阶段,LEO 卫星与 VLEO 卫星可能因为物理因素、链路遮蔽等原因无法直接进行通信,需要通过所属的 MEO 卫星进行信息转发,此时,UE 与 VLEO 卫星之间将完成重认证。VLEO 卫星将通过所属的 VMEO 卫星与 LEO 卫星所属的 MEO 卫星之间获取 AV(i),UE 和 VLEO 卫星产生新的会话密钥,并确认 AV(i) 的有效性。在重认证过程中可能存在用户设备因为能耗不足而未完成重认证,继而需要进行断电重连的情况,需要利用申请的 AV(i) 完成双向身份认证和密钥协商,并确认 AV(i) 的有效性。在认证过程中,可能存在认证双方记录的随机数不同,从而造成认证失败的情况。因此需要进行 AV 快速同步过程,以最后一次使用的随机数为基准,双方实体之间进行 AV 同步,确保后续通信所需安全参数的一致性。

2 方案设计

2.1 用户设备初次接入认证过程

2.1.1 注册阶段

在用户设备注册阶段,UE 将离线进行注册过程,NCC 完成临时身份标识、预置密钥的安全参数分发,具体用户

注册过程如图 3 所示。

(1) UE 根据自身身份的标识信息 ID_u 向 NCC 发送注册请求。

(2) NCC 随机生成 UE 的接入认证所使用的临时身份标识 PID_u 、随机数 r_1 、 r_2 , 根据自身的基础密钥 K , 生成用户设备和网络控制中心的预置密钥 K_{UE-NCC} 、用户设备和卫星(不区分轨道高度)的预置密钥 K_{UE-SAT} 。NCC 保存 UE 的真实身份标识 ID_u 、临时身份标识 PID_u 、预置密钥 $K_{UE-NCC} = f(r_1 \| K)$ 、 $K_{UE-SAT} = f(r_2 \| K)$, 并将 UE 的临时身份标识 PID_u 连同预置密钥 $K_{UE-NCC} \| K_{UE-SAT}$ 一起分发至 UE。

(3) UE 将收到消息后,将预置密钥 K_{UE-NCC} 、 K_{UE-SAT} 写入密码模块,保存临时身份标识 PID_u 。

2.1.2 初始接入

本文针对卫星互联网链路高度开放、网络拓扑频繁变化等特点,设计一种安全高效的初始接入认证协议。协议中将对称密码体制和哈希函数相结合,实现 UE 和 LEO 卫星之间的双向身份认证和会话密钥协商,减少认证系统的计算开销,具体认证过程如图 4 所示。

(1) UE 获取当前的时间 T_u 、位置信息 L_u , 生成随机数 N_u , 结合自身的 ID_u 标识、预置密钥 K_{UE-NCC} , 计算加密密钥 $CK = KDF(K_{UE-NCC}, ID_u \| T_u)$ 、位置密钥 $AK = KDF(K_{UE-SAT}, PID_u \| N_u \oplus L_u)$ 、生成消息验证码 $MAC_u = h(AK, PID_u \| T_u \| N_u \oplus L_u)$, 将 $PID_u \| E_{CK}(N_u \| L_u) \| MAC_u \| T_u$ 发送至 LEO 处。

(2) LEO 卫星收到来自 UE 的消息后,检查时间戳 T_u 的有效性,生成随机数 N_{sl} , 在消息后附加其身份标识信

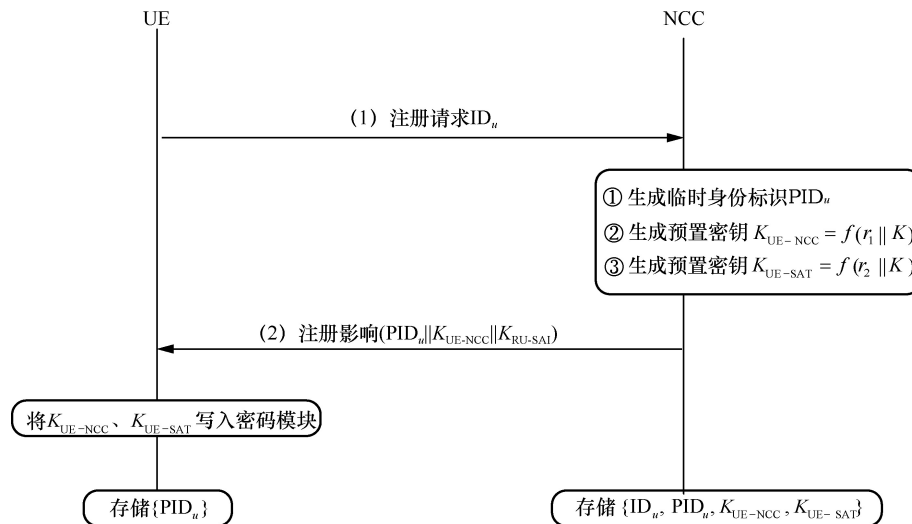


图3 用户注册过程

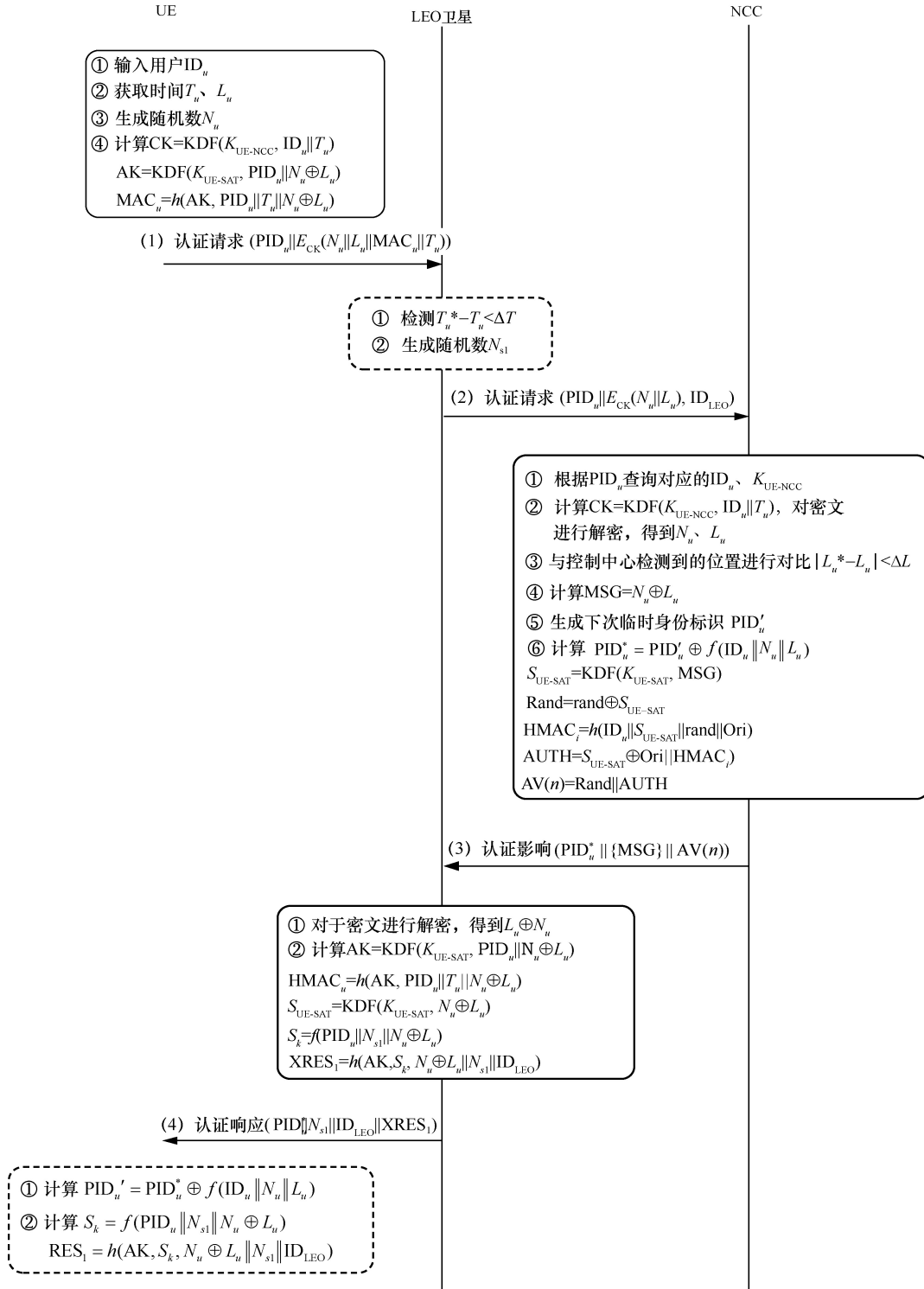


图4 初始接入认证过程

息标识 ID_{LEO} , 发送至 NCC 处。

(3) NCC 收到来自 LEO 卫星的消息后, 根据 PID_u 查找对应的真实用户标识符 ID_u, K_{UE-NCC} , 计算位置解密密钥 $CK = KDF(K_{UE-NCC}, ID_u || T_u)$, 对于 $E_{CK}(N_u || L_u)$ 进行解密,

获得 L_u, N_u , 与 NCC 检测到的位置进行对比, 看其是否满足 $|L_u^* - L_u| < \Delta L$, ΔL 为预先设定的位置容忍精度, 若满足则计算 $MSG = N_u \oplus L_u$, 生成下次临时身份标识 PID_u' , 计算临时身份保护序列 $PID_u^* = PID_u' \oplus f(ID_u || N_u || L_u)$, 秘密值

$S_{UE-SAT} = KDF(K_{UE-SAT}, MSG)$ 、随机数保护序列 $Rand = rand \oplus S_{UE-SAT}$ 、消息验证码 $HMAC_i = h(ID_u \parallel S_{UE-SAT} \parallel rand \parallel Ori)$ 、认证令牌 $AUTH = S_{UE-SAT} \oplus Ori \parallel HMAC_i$ 、认证向量 $AV(n) = Rand \parallel AUTH$ 。其中 $AV(1)$ 中的 Ori 、 $rand$ 是由 NCC 生成的两个随机数，之后认证向量 $AV(i)$ 中的 Ori 是由认证向量 $AV(i-1)$ 中的 Ori 和 $rand$ 进行相加后得到的。计算完成之后，将 $PID_u \parallel MSG \parallel AV(n)$ 发送给 LEO 卫星。

(4) LEO 收到来自 NCC 的信息后，获得 $L_u \oplus N_u$ ，位置密钥 $AK = KDF(K_{UE-SAT}, PID_u \parallel N_u \oplus L_u)$ ，比较消息认证码 $HMAC_u = h(AK, PID_u \parallel T_u \parallel N_u \oplus L_u)$ 是否与收到的 MAC_u 相等。若相等，计算 $S_k = f(PID_u \parallel N_{s1} \parallel N_u \oplus L_u)$ ，认证响应值 $XRES_1 = h(AK, S_k \parallel N_u \oplus L_u \parallel N_{s1} \parallel ID_{LEO})$ 。计算完成之后将 $PID_u \parallel N_{s1} \parallel ID_{LEO} \parallel XRES_1$ 发送至 UE 处。

(5) UE 收到来自 LEO 的信息后，计算下一次临时身份标识 $PID_u' = PID_u \oplus f(ID_u \parallel N_u \parallel L_u)$ ，计算 $S_k = f(PID_u \parallel N_{s1} \parallel N_u \oplus L_u)$ ，认证响应值 $RES_1 = h(AK, S_k \parallel N_u \oplus L_u \parallel N_{s1} \parallel ID_{LEO})$ 是否与收到的 $XRES_1$ 相等。若相等，则完成身份认证。

2.2 用户设备重认证过程

2.2.1 重认证

卫星网络通信往往作为地面通信网络的补充，在灾难救援等特殊场景下，地面通信基础设施容易受到摧毁和打击，可能导致无法避免的服务中断，因此本文基于椭圆曲线密码体制提出一种地面缺省条件下的用户设备重认证方案，实现 UE 和拜访域卫星 VLEO 的双向身份认证和新的会话密钥的协商。另外，针对 $AV(i)$ 向量进行认证确认操作，确保了每次通信中的认证向量都是不可重复使用的，提高了通信过程中的可靠性和安全性。具体过程如下。

2.2.1.1 星间卫星协助的重认证阶段

UE 发起重认证请求，如果通信轨道不遮挡可直接通信，拜访域卫星 VLEO 通过星间链路根据其 ID 寻找上一颗接入卫星 LEO，具体流程如图 5 所示。

(1) UE 获取当前时间戳 T_1 ，生成一个随机数 u ，并计算其 UE 侧的密钥片段 $KF_u = u * P$ 。其中， P 是有限域椭圆曲线上的一个生成元。将 $PID_u \parallel KF_u \parallel ID_{LEO} \parallel T_1$ 发送至卫星 VLEO 处。

(2) VLEO 卫星收到来自 UE 的信息后，将认证消息转发 $PID_u \parallel KF_u \parallel ID_{LEO}$ 至低轨卫星 LEO 处。

(3) LEO 卫星收到来自 VLEO 卫星的信息后，获得

KF_u 、选择 $AV(i)$ 向量将 $PID_u \parallel \{S_{UE-SAT}\} \parallel AV(i)$ 发送至低轨卫星 VLEO 处，其中 S_{UE-SAT} 通过 LEO 和 VLEO 的安全信道进行传输。

(4) VLEO 卫星收到来自 LEO 卫星的信息后，对于消息进行解密获得 S_{UE-SAT} ，生成随机数 b 、 N_{s2} ，计算新秘密值 $S_{UE-SAT}' = S_{UE-SAT} \oplus N_{s2}$ 、临时密钥 $TK = b * KF_u$ 、卫星侧的密钥片段 $KF_b = b * P$ ，消息 $MSG_{b2} = E_{TK}(N_{s2}) \parallel ID_{VLEO} \parallel KF_b$ ，将 $AV(i) \parallel MSG_{b2} \parallel ID_{VLEO} \parallel T_2$ 发送至 UE 处。

(5) UE 收到来自 VLEO 卫星的信息后，计算 $S_{UE-SAT} = KDF(K_{UE-SAT}, N_u \oplus L_u)$ ，计算临时密钥 $TK = u * KF_b$ ，解密其消息获得随机数 N_{s2} ，计算 $S_{UE-SAT}' = S_{UE-SAT} \oplus N_{s2}$ 、 $rand = Rand \oplus S_{UE-SAT}$ ；检查 Ori ，若相等，计算消息验证码 $MAC_i = f(ID_u \parallel S_{UE-SAT} \parallel rand \parallel Ori)$ 、新的会话密钥 $S_k' = f(PID_u \parallel rand \parallel Ori \parallel S_{UE-SAT}')$ 、用户设备侧认证响应值 $RES_2 = h(S_k, rand \parallel Ori \parallel S_{UE-SAT}' \parallel ID_{VLEO} \parallel KF_b)$ ，更新 Ori ，将 RES_2 发送至 VLEO 处。

(6) VLEO 卫星收到来自 UE 的信息后，计算 $rand = Rand \oplus S_{UE-SAT}$ ，新的会话密钥 $S_k' = f(PID_u \parallel rand \parallel Ori \parallel S_{UE-SAT}')$ ，认证响应值 $XRES_2 = h(S_k', rand \parallel Ori \parallel S_{UE-SAT}' \parallel ID_{VLEO} \parallel KF_b)$ ，比较自己的 $XRES_2$ 与收到的 RES_2 是否相等。计算 $THMAC_i = MAC_i \oplus f(PID_u \parallel S_{UE-SAT} \parallel rand \parallel Ori)$ ，将 $THMAC_i$ 发送至 LEO 处。

(7) LEO 收到来自 VLEO 卫星的信息后，计算 $TMAC_i = MAC_i \oplus f(PID_u \parallel S_{UE-SAT} \parallel rand \parallel Ori)$ ，比较自己的 $TMAC_i$ 与收到的 $THMAC_i$ 是否相等，更新 Ori 。

2.2.1.2 层间卫星协助的重认证阶段

在 LEO 星座的网络中，卫星运行在特定的轨道上以特定的方向运行，相邻的卫星轨道可能运行方向和速度完全不同，因此彼此之间由于存在物理因素并不能建立稳定的通信连接。此时重认证过程中，UE 发起重认证请求，由于通信连接的不稳定性，低轨卫星双方可通过所属的 MEO 卫星完成相关安全参数的传递，方便完成后续认证。具体流程如图 6 所示。

(1) UE 获取当前时间戳 T_1 ，计算密钥片段选择一个随机数 u 作为系统私钥，并计算密钥片段 $KF_u = u * p$ ， p 为椭圆曲线上的一个生成元， q 为一个大素数。将 $PID_u \parallel KF_u \parallel ID_{LEO} \parallel T_1$ 发送至卫星 VLEO 处。

(2) VLEO 卫星收到来自 UE 的信息后，进行认证消息转发 $PID_u \parallel ID_{LEO}$ 至所属中轨卫星 VME0 处。

(3) VME0 卫星收到来自 VLEO 卫星的信息后，进行广播认证消息转发 $PID_u \parallel ID_{LEO}$ 至 LEO 卫星所属的中轨卫

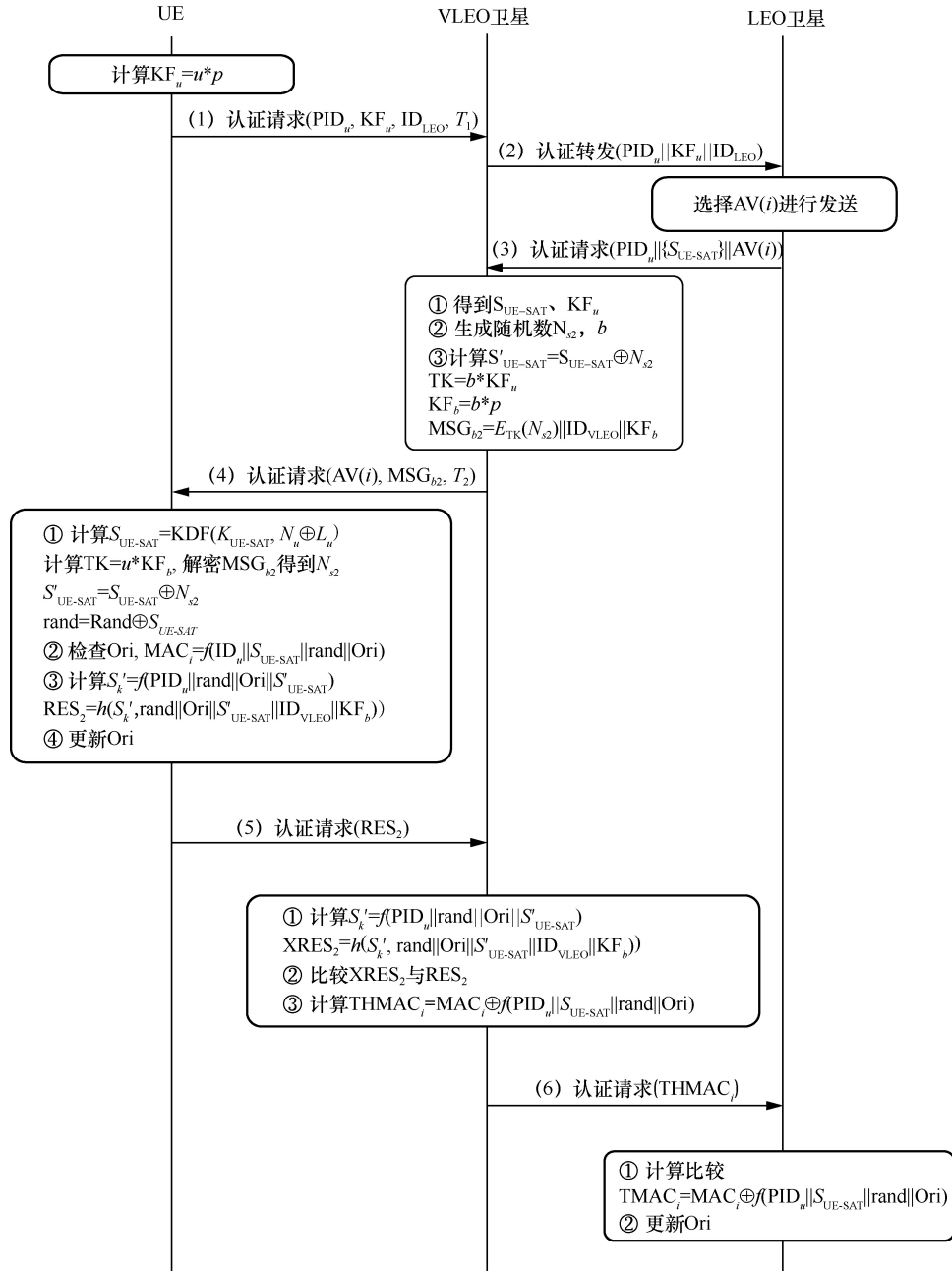


图 5 星间卫星协助的重认证

星 MEO 处。

(4) MEO 卫星收到来自 VLEO 卫星的信息后, 进行认证消息转发 PID_u 至低轨卫星 LEO 处。

(5) LEO 卫星收到来自 MEO 卫星的信息后, 计算 $MSG_{b1} = S_{UE-SAT} \parallel Irand$, 将认证消息请求 $PID_u \parallel \{MSG_{b1}\} \parallel AV(n)$ 发送至所属的中轨卫星 MEO 处。

(6) MEO 卫星收到来自 LEO 卫星的信息后, 存储 $AV(n)$, 解密 S_{UE-SAT} 、 $Irand$, 将 $PID_u \parallel \{S_{UE-SAT}\} \parallel AV(i) \parallel ID_{MEO}$ 发送至中轨卫星 VLEO 处。

(7) VLEO 卫星收到来自 MEO 卫星的信息后, 将认证消息转发 $PID_u \parallel \{S_{UE-SAT}\} \parallel AV(i) \parallel ID_{MEO}$ 至卫星 VLEO 处。

(8) 步骤 (8) ~ 步骤 (11) 同 2.2.1.1 小节中的步骤 (4) ~ 步骤 (7), 此外在用户设备侧更新存储认证向量 $AV(n)$ 的卫星标识。

2.2.2 断电重连

针对用户设备可能因为设备能耗不足发生断电重连的情况, 本文基于哈希函数和椭圆曲线密码体制设计一种

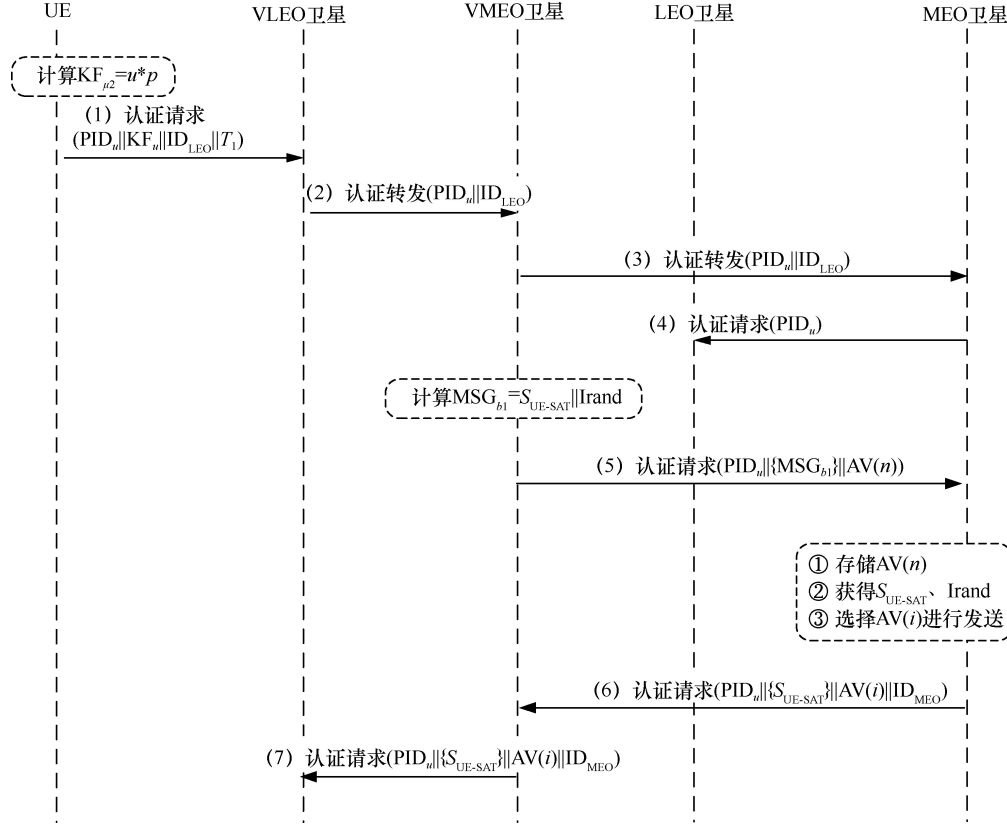


图6 层间卫星协助的重认证过程

断电重连场景下的用户设备快速认证方案，确保 UE 在实际应用场景中断电重连之后，可以继续接入卫星网络获得相应服务。如果 UE 在 2.2.1.1 小节重认证过程中步骤（1）之前断电重连，则需要重新进行重认证流程；如果在步骤（5）之前断电重连，则需要进行断电重连流程；如果在步骤（5）之后断电重连，则直接使用新的会话密钥进行通话，具体步骤如图 7 所示。

（1）UE 获取当前时间戳 T_3 ，计算密钥片段选择一个随机数 u_2 作为系统私钥，并计算密钥片段 $KF_{u2} = u_2^* p$ ， p 为椭圆曲线上的一个生成元， q 为一个大素数。将 $PID_u || KF_{u2} || T_3$ 发送至卫星 VLEO 处。

（2）VLEO 卫星收到来自 LEO 卫星的信息后，生成随机数 N_{s3} 、 b_2 ，计算新秘密值 $S'_{UE-SAT} = S_{UE-SAT} \oplus N_{s3}$ 、临时密钥 $TK_2 = b_2^* KF_{u2}$ 、密钥片段 $KF_{b2} = b_2^* p$ ，消息 $MSG_{b3} = E_{TK2}(N_{s3}) || ID_{VLEO} || KF_{b2}$ ，将 $AV(i) || MSG_{b3} || T_4$ 发送至 UE 处。

（3）UE 收到其消息后，计算 $S_{UE-SAT} = KDF(K_{UE-SAT}, N_u \oplus L_u)$ ，计算临时密钥 $TK_2 = u_2^* KF_{b2}$ ，解密其消息获得随机数 N_{s3} ，计算 $S'_{UE-SAT} = S_{UE-SAT} \oplus N_{s3}$ 、 $rand = Rand \oplus S_{UE-SAT}$ ，检查 Ori。若相等，计算消息验证码

$MAC_i = f(ID_u || S_{UE-SAT} || rand || Ori)$ 、新的会话密钥 $S'_k = f(PID_u || rand || Ori || S'_{UE-SAT})$ 、认证响应值 $RES_2 = h(S'_k, rand || Ori || S'_{UE-SAT} || ID_{VLEO} || KF_{b2})$ ，更新 Ori，将 RES_2 发送至 VLEO 卫星处。

（4）VLEO 卫星收到来自 UE 的信息后，计算 $rand = Rand \oplus S_{UE-SAT}$ ，新的会话密钥 $S'_k = f(PID_u || rand || Ori || S'_{UE-SAT})$ ，认证响应值 $XRES_2 = h(S'_k, rand || Ori || S'_{UE-SAT} || ID_{VLEO} || KF_{b2})$ ，比较自己的 $XRES_2$ 与收到的 RES_2 是否相等。计算 $THMAC_i = MAC_i \oplus f(PID_u || S_{UE-SAT} || rand || Ori)$ ，将 $THMAC_i$ 发送至 LEO 处。

（5）LEO 卫星收到来自 VLEO 卫星的信息后，计算 $TMAC_i = MAC_i \oplus f(PID_u || S_{UE-SAT} || rand || Ori)$ ，比较自己的 $TMAC_i$ 与收到的 $THMAC_i$ 是否相等，相等则完成身份认证。

2.2.3 AV 同步

卫星网络中链路高度开放，可能会造成认证双方认证所选取的随机数不一致，从而导致认证失败。本文提出一种基于哈希函数和异或操作的快速安全同步方案，保障实体双向认证时所需安全参数的一致性。当 UE 的随机数小

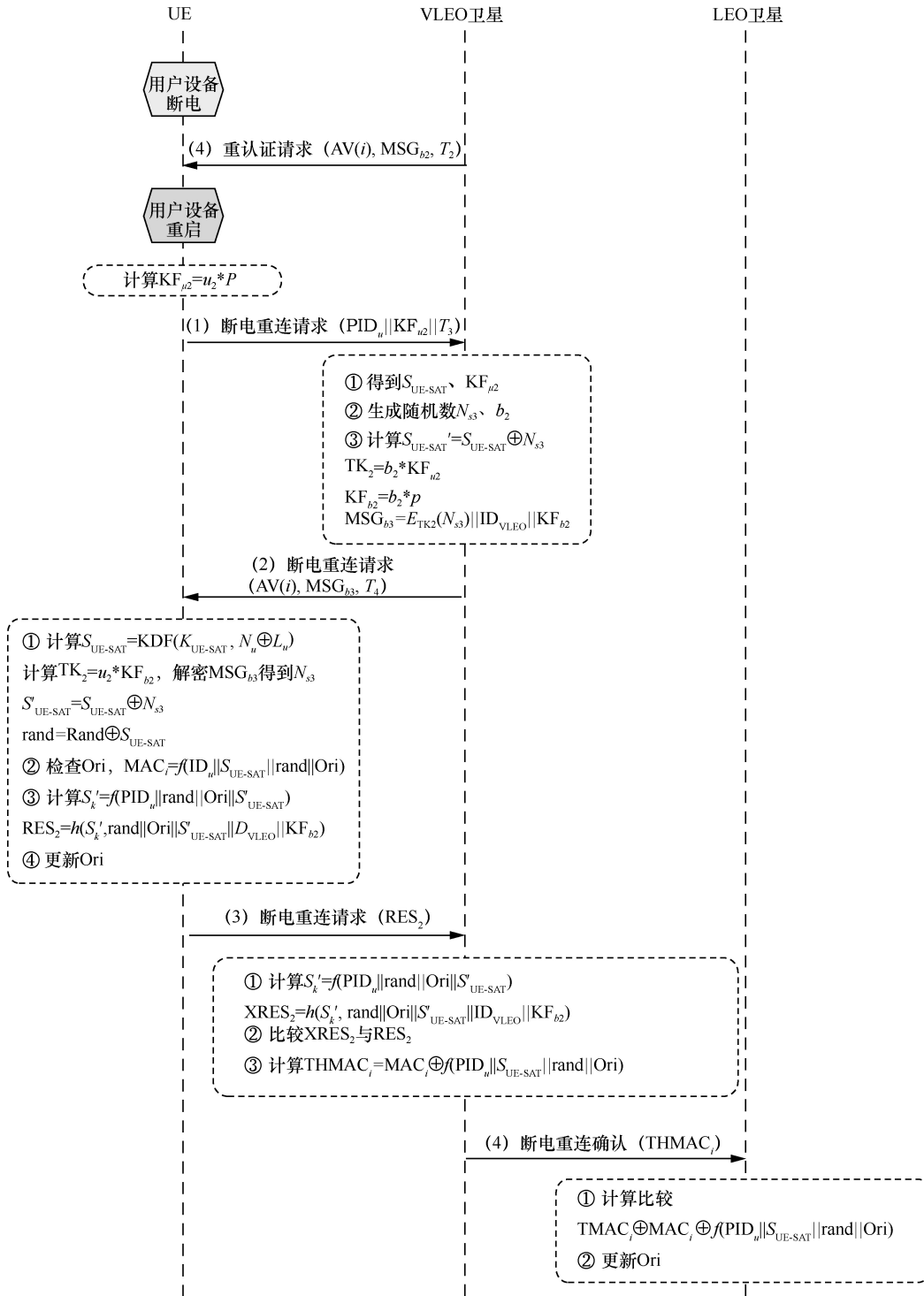


图 7 断电重连过程

于 LEO 卫星的随机数时, 需要申请新的 AV 向量完成认证; 当 UE 的随机数大于 LEO 卫星的随机数时, 进行 AV 同步操作, 具体步骤如图 8 所示。

(1) LEO 在规定的时间内没有收到消息回复, 发起同步请求将 PID_u 发送至 VLEO 卫星处。

(2) VLEO 卫星收到来自 LEO 卫星的信息后, 将 $THMAC_i$ 发送至 LEO 卫星; 若 VLEO 卫星没有计算 $THMAC_i$, 则发送同步请求 $PID_u \parallel T_5$ 至 UE 处。

(3) UE 收到其消息后, 计算同步凭证 $AUTS = Ori \oplus S_{UE-SAT} \parallel MAC_i$, 发送同步请求

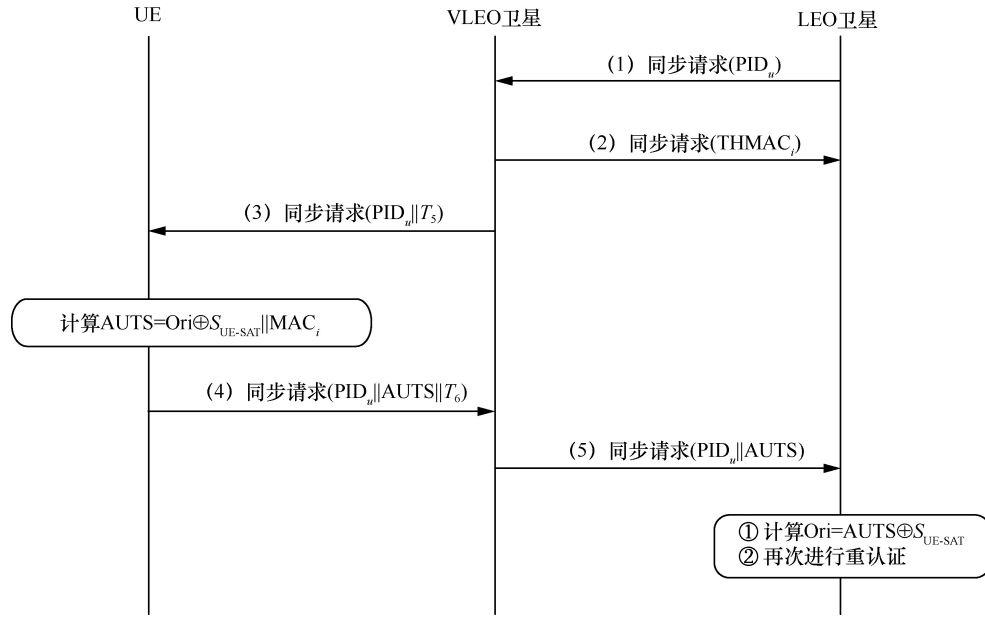


图8 AV同步过程

$PID_u || AUTS || T_6$ 至 VLEO 卫星处。

(4) VLEO 卫星收到来自 UE 的信息后, 进行同步消息转发 $PID_u || AUTS$ 至 LEO 卫星处。

(5) LEO 卫星收到来自 VLEO 卫星的信息后计算 $Ori = AUTS \oplus S_{UE-SAT}$, 选择 $Ori' = Ori + rand$ 进行重新认证。

3 安全性分析

下面将采用非形式化分析和形式化验证工具 Scyther 来验证本文提出的方案的安全性, 并讨论抵御各种攻击类型的能力。

3.1 非形式化安全分析

(1) 相互认证: 在 UE 初次接入卫星网络的过程中, UE 通过比较本地的认证响应值 RES_1 与收到的 $XRES_1$ 是否相等来确认 LEO 的身份并进行密钥确认操作; LEO 卫星通过比较本地的消息验证码 $HMAC_u$ 与收到的 MAC_u 是否相等来确认 UE 的身份, 实现了 UE 和 LEO 卫星之间双向身份认证。在重认证过程中, UE 通过比较本地的消息验证码 MAC_i 与收到的 $HMAC_i$ 是否相等来确认 VLEO 卫星的身份; VLEO 卫星通过比较本地的认证响应值 $XRES_2$ 与收到的 RES_2 是否相等来确认 VLEO 卫星的身份并进行密钥确认操作, 实现了 UE 和 VLEO 卫星之间的双向身份认证。

(2) 会话密钥协商: 在初次接入认证的过程中, 由用户设备的临时身份标识, 结合认证过程中生成的随机数 N_u 和 N_{s1} 以及位置信息 L_u 来计算会话密钥 S_k 。因此, UE 和 LEO 卫星之间可以安全协商会话密钥; 在重认证过程

中, UE 和 VLEO 卫星通过 AV 认证向量中包含的随机数 $rand$ 、 Ori 以及协商的秘密信息 S_{UE-SAT} 生成新的会话密钥 S_k' , 确保了后续通信信息的机密性。

(3) 条件隐私性: 本文用户设备的隐私信息包括用户真实身份标识信息和用户的位置信息。在认证过程中, UE 使用临时身份标识 PID_u 进行通信, 并由 NCC 随机生成下一次认证的临时身份标识 PID'_u ; PID'_u 在传输过程中通过临时身份保护序列进行保护, 保障了用户设备身份的匿名性。用户设备的位置信息级联随机数在传输过程进行对称加密, 只有 NCC 可以进行正确解密, 对于攻击者来说, 因为不持有 UE 的真实身份标识从而无法得到正确的解密密钥, 所以无法破解用户设备的位置信息。

(4) 不可链接性: 由于卫星网络的链路具有高度的开放性, 攻击者可以监听公开信道中传输的任何消息。UE 使用的临时身份标识每次由 NCC 随机生成, 每个临时身份表示之间不存在任何关联, 攻击者不可以从中链接到具体某个实体。

(5) 前后向安全性: 本文生成会话密钥的时候使用新的随机数来确保各会话密钥的独立性。即使当前的会话密钥泄露, 攻击者也不能推断出之前或者之后会话中使用到的会话密钥, 保证了通信消息的机密性。

(6) 抵御多种协议攻击: 在本文所提的初次接入认证方案中, UE 发送的认证请求如 $PID_u || E_{CK}(N_u || L_u) || MAC_u || T_u$ 加入了时间戳, 为公开信道中的信息增加实时信息, 保证了消息的可信性与及时性。重认证、断电重

连以及 AV 同步过程同理, 因此方案可以抵抗重放攻击。由于 UE 和 LEO 之间的相互认证和会话密钥协商已经实现, 且交互消息均基于密钥派生函数构造位置密钥 AK, 只有双方期望交互的接收方才能够生成位置密钥 AK, 因此攻击者无法伪装成合法的 UE 和 LEO 卫星, 向 UE 或 LEO 卫星发起中间人攻击。重认证、断电重连以及 AV 同步过程同理, 因此方案可以抵抗中间人攻击。在初次接入认证过程中, 只有 UE 和 LEO 卫星知晓用户选取的随机数和位置信息的异或值 $N_u \oplus L_u$, 攻击者无法获得 UE 选取的随机数和位置信息的异或值 $N_u \oplus L_u$ 。因此, 攻击者无法根据截获的消息解密 UE 和 LEO 卫星的会话内容, 也就无法假冒其中一方与另一方进行通信。重认证、断电重连以及 AV 同步过程同理, 因此方案可以抵抗假冒攻击。

(7) 地面缺省: 基于 UE 初次接入认证过程中生成的 AV 认证向量, 在重认证过程中卫星网络进行 AV 向量的传递完成实体之间的身份双向认证, 无须地面 NCC 的参与, 减少了星地传输次数, 避免了灾难救援等特殊场景下因地面通信基础设施受到破坏或者打击而造成通信系统瘫痪的问题, 保障了通信系统容灾性。

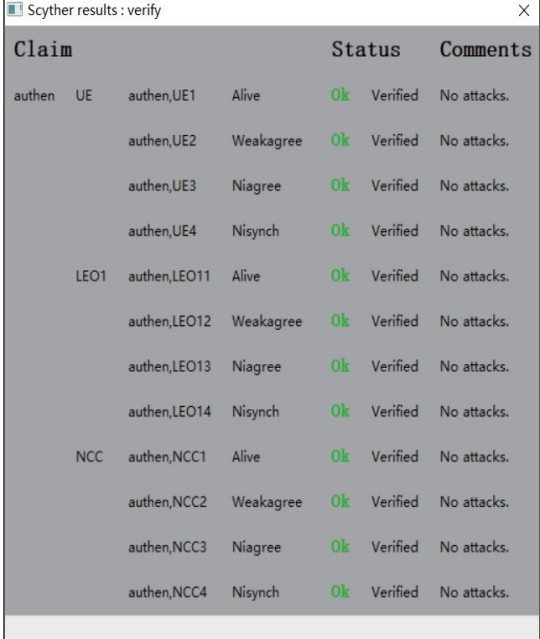
3.2 Scyther 形式化安全分析

本文涉及用户设备的注册、初次接入、重认证、断电重连和 AV 同步 5 个阶段。由于用户离线完成注册流程、断电重连阶段和重认证阶段过程基本一致, AV 同步阶段只是通过信道同步随机数, 故这 3 个阶段不进行形式化安全验证, 将对 UE 的初次接入认证过程以及重认证阶段进行形式化分析。

Scyther 是一种基于模式细化的算法, 允许证明协议对于无线轮数会话的正确性。Scyther 要将协议转换为安全协议描述语言 (Security Protocol Description Language, SPDL), 建模相关安全属性进行验证, 其验证结果可以提示在某个范围内是否存在攻击, 并且可以生成攻击图方便研究人员进行攻击类别查询^[22-23]。使用形式化验证工具 Scyther 对于本文中提出的协议进行验证, 首先声明相关算法如哈希函数、字符串等, 其次声明协议名称、角色名, 然后定义所需的相关安全参数、发送和接收相关认证消息、指定其拥有的安全属性, 最后进行工具验证。若安全属性得到满足, 输出结果为 **verified**, 否则输出结果为 **falsified**, Scyther 验证结果如图 9~10 所示。

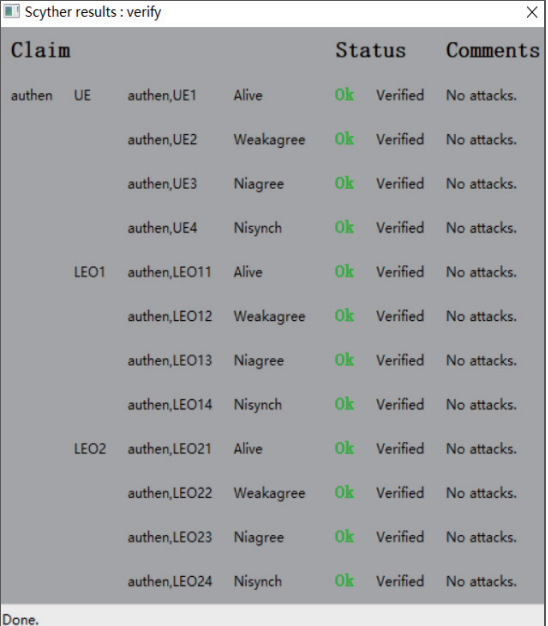
针对用户设备初次接入认证阶段, 涉及 3 个实体 UE、LEO 卫星和 NCC; 重认证阶段中, 涉及 3 个实体 UE、VLEO

卫星和 LEO 卫星。对于通信实体的安全属性 **Alive**、**Weakagree**、**Niagree** 以及 **Nisynch** 进行声明。在 Scyther 所声明的安全范围内进行建模均未发现任何攻击, 在初次接入认证过程及重认证过程中均实现了实体之间的双向身份认证和通信信息的机密传输并且可以抵抗常见的协议攻击。



Claim				Status	Comments
authen UE	authen,UE1	Alive	Ok	Verified	No attacks.
	authen,UE2	Weakagree	Ok	Verified	No attacks.
	authen,UE3	Niagree	Ok	Verified	No attacks.
	authen,UE4	Nisynch	Ok	Verified	No attacks.
LEO1	authen,LEO11	Alive	Ok	Verified	No attacks.
	authen,LEO12	Weakagree	Ok	Verified	No attacks.
	authen,LEO13	Niagree	Ok	Verified	No attacks.
	authen,LEO14	Nisynch	Ok	Verified	No attacks.
NCC	authen,NCC1	Alive	Ok	Verified	No attacks.
	authen,NCC2	Weakagree	Ok	Verified	No attacks.
	authen,NCC3	Niagree	Ok	Verified	No attacks.
	authen,NCC4	Nisynch	Ok	Verified	No attacks.

图 9 初始接入认证阶段 Scyther 仿真结果



Claim				Status	Comments
authen UE	authen,UE1	Alive	Ok	Verified	No attacks.
	authen,UE2	Weakagree	Ok	Verified	No attacks.
	authen,UE3	Niagree	Ok	Verified	No attacks.
	authen,UE4	Nisynch	Ok	Verified	No attacks.
LEO1	authen,LEO11	Alive	Ok	Verified	No attacks.
	authen,LEO12	Weakagree	Ok	Verified	No attacks.
	authen,LEO13	Niagree	Ok	Verified	No attacks.
	authen,LEO14	Nisynch	Ok	Verified	No attacks.
LEO2	authen,LEO21	Alive	Ok	Verified	No attacks.
	authen,LEO22	Weakagree	Ok	Verified	No attacks.
	authen,LEO23	Niagree	Ok	Verified	No attacks.
	authen,LEO24	Nisynch	Ok	Verified	No attacks.

Done.

图 10 重认证阶段 Scyther 仿真结果

4 性能分析

本节首先从协议安全性的角度将本文提出的协议和其他类似方案进行分析；然后从计算开销、带宽开销、存储开销3个方面对本文提出的协议和其他类似方案进行对比分析。

4.1 安全性对比

各协议安全性对比见表1。表1表明,参考文献[11]、[13]和[20]密钥的前后向安全性存在缺陷,攻击者可以通过当前的会话密钥破解出之前/之后的会话密钥,可能会破解信道中更多有用信息,带来严重的安全问题。因参考文献[23]采用签名/验签的方式,无须地面参与,其余文献均无法在地面缺省条件下完成双向身份认证。参考文献[13]和[20]在会话密钥生成之后,没有对会话密钥进行确认,可能存在双方会话密钥不一致的情况,影响后续通信的实时性。本文所提出的协议可以满足上述安全属性,在地面缺省条件下,通过在卫星网络中AV向量的传递完成UE和VLEO卫星之间的身份认证,保障了会话密钥的前后向安全性。

表1 各协议安全性对比

协议	双向认证	密钥确认	条件 隐私性	前后向 安全性	地面缺省
参考文献[11]	√	√	√	×	×
参考文献[13]	√	×	√	√	√
参考文献[20]	√	×	√	×	×
参考文献[23]	√	√	√	×	×
本文所提协议	√	√	√	√	√

4.2 计算开销

在身份认证过程中,涉及级联、异或、哈希运算 T_H 、对称加解密运算 T_s 、非对称加密运算 T_{enc} 、非对称解密运

算 T_{dec} 、签名运算 T_{sig} 、验签运算 T_{ver} 、密钥生成函数运算 T_{KDF} 、点乘运算 T_{mul} ,其中,级联和异或操作由于执行时间较短可忽略不计,通过构建一个仿真平台来测试以上密码学算法的开销。

选择两台性能不同的计算机,一台处理器为Intel(R)Core(TM)m3-6Y30 CPU@0.9 GHz,模拟计算资源、存储资源受限的用户设备/卫星;另一台处理器为Core(TM)i7-7500U CPU@2.70 GHz,模拟地面控制中心。所有密码算法基于openssl-1.0.2e^[28]实现,将每个密码学算法运行1000次,然后取平均运行时间作为该密码学算法的计算开销,具体见表2。表3中列出了其他类似方案和本文所提出方案的计算开销。

表2 每个密码学算法的平均运行时间

运算类型	UE/卫星的计算开销/ μ s	控制中心的计算开销/ μ s
T_H	2.39	1.21
T_s	2.26	1.05
T_{enc}	8.97	5.32
T_{dec}	0.08	0.03
T_{sig}	1.20×10^3	0.73×10^3
T_{ver}	0.81×10^3	0.44×10^3
T_{KDF}	2.42	1.23
T_{mul}	1.00×10^3	0.52×10^3

图11绘制了各个类似方案和本文所提出的方案在认证阶段计算开销随认证次数增加时的变化。可以看出,参考文献[11]、[13]和[23]在方案中进行了大量的点乘操作,带来了较大的计算开销;本文所提出的方案计算开销虽然高于参考文献[20],但是参考文献[20]不能保证会

表3 认证阶段计算开销对比

方案	终端设备的计算开销/ μ s	卫星的计算开销/ μ s	网络控制中心的计算开销/ μ s	总计算开销/ μ s
参考文献[11]	$4T_H + 3T_{mul} + T_s$	—	$5T_H + 3T_{mul} + T_s$	4 586.02
参考文献[13]	$2T_H + 3T_{mul} + T_{sig} + 2T_{ver}$	$T_H + 2T_{mul} + T_{sig} + 2T_{ver}$	T_{mul}	9 167.17
参考文献[20]	$4T_H$	T_s	$6T_H + T_s$	20.13
参考文献[23]	$10T_H + 3T_{mul}$	—	$7T_H + 3T_{mul}$	4 592.37
接入认证	$4T_H + 2T_{KDF} + 2T_s$	$3T_H + 2T_{KDF}$	$2T_H + 2T_{KDF}$	35.81
重认证	$3T_H + 2T_{mul} + 2T_s + T_{KDF}$	$4T_H + 2T_{mul}$	—	4 023.94

话密钥的前后向安全性，容易造成会话信息的泄露，带来严重的安全问题。

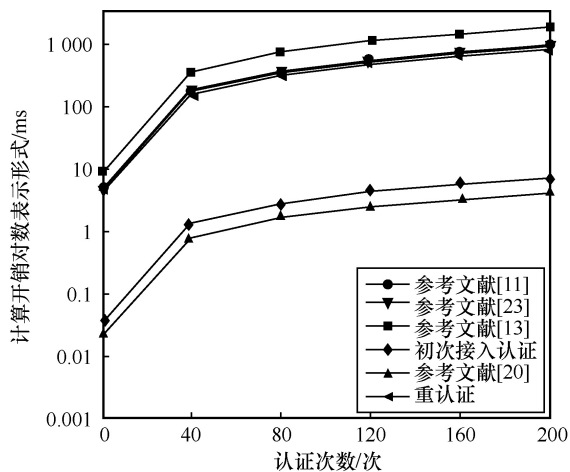


图 11 各协议计算开销随认证次数增加时的变化

4.3 带宽开销

为了保证协议带宽开销分析的公平性，设定安全级别为 AES-128 bit。其中对称密码体制采用 SM4 算法，密钥长度为 128 bit；非对称密码体制公钥长度为 3 072 bit，私钥长度为 256 bit；ECC 上的密钥长度为 320 bit；哈希、KDF 算法的输出长度为 128 bit；用户设备的真实身份标识、临时身份标识为 128 bit；卫星身份标识、时间戳长度为 32 bit；随机数的长度为 128 bit。表 4 列举了各协议认证阶段带宽开销对比。

表 4 认证阶段带宽开销对比

方案	终端设备的 带宽开销/bit	卫星的带 宽开销/bit	网络控制中心 的带宽开销/bit	总带宽 开销/bit
参考文献[11]	992	64	512	1 568
参考文献[13]	7 264	4 544	-	11 808
参考文献[20]	672	32	640	1 344
参考文献[23]	928	64	480	1 472
接入认证	416	320	640	1 376
重认证	640	672	-	1 312

图 12 绘制了各个类似方案和本文所提出的方案在认证阶段带宽开销随认证次数增加时的变化。参考文献[13]发送采用签名/验签操作所需的信息，产生了较大的带宽开销。参考文献[11]和[23]多次发送了点乘的运算结果，增加了所需的带宽开销。本文所提出的方案虽然略高于参考文献[20]，但是参考文献[20]的安全属性并不具备优势，将威胁到用户的隐私安全。

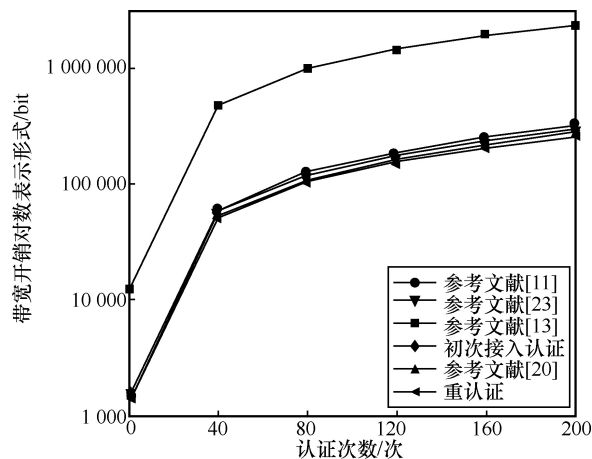


图 12 各协议带宽开销随认证次数增加时的变化

4.4 存储开销

为了公平起见，本节将各协议的存储开销进行统一的对比，采用 AES-128 bit 同等安全级别进行比较。其具体计算长度和 4.3 小节所述一致。表 5 列举了各协议的存储开销对比。

表 5 认证阶段各协议存储开销对比

方案	终端设备的 存储开销/bit	卫星的 存储开销/bit	网络控制中心 的存储开销/bit	总存储 开销/bit
参考文献[11]	896	32	512	1 440
参考文献[13]	6 848	3 328	-	10 176
参考文献[20]	384	800	416	1 600
参考文献[23]	960	32	416	1 408
接入认证	512	384	384	1 280
重认证	384	592	-	976

各协议存储开销随认证次数增加时的变化如图 13 所示。从图 13 可以看到，参考文献[13]的方案因为采用公钥密码算法，需要存储认证相关实体的私钥和公钥，产生了较大的存储开销。本文所提出的接入认证协议采用轻量级算法，在用户设备侧需要存储相关基础密钥、下一次临时身份标识和会话密钥；在卫星侧存储相关基础密钥、用户设备的临时身份标识以及会话密钥；在网络控制中心侧存储相关密钥、用户设备的真实身份标识、下一次临时身份标识。在重认证过程中，用户设备侧存储随机数、新的会话密钥以及下一次临时身份标识；在卫星侧存储随机数和认证向量。本文提出的协议的存储开销均低于其他类似方案，对节点资源进行了更合理的分配，适用于计算/存储能力有限的卫星互联网。

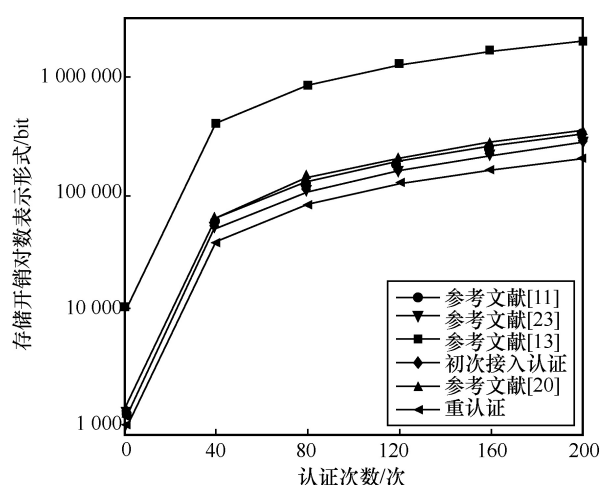


图 13 各协议存储开销随认证次数增加时的变化

参考文献：

- [1] ALSHARIF M H, KELECHI A H, ALBREEM M A, et al. Sixth generation (6G) wireless networks: vision, research activities, challenges and potential solutions[J]. Symmetry, 2020, 12(4): 676.
- [2] 吴巍. 天地一体化信息网络发展综述[J]. 天地一体化信息网络, 2020, 1(1): 1-16.
WU W. Survey on the development of space-integrated-ground information network[J]. Space-Integrated-Ground Information Networks, 2020, 1(1): 1-16.
- [3] SHENG M, ZHOU D, LIU R Z, et al. Resource mobility in space information networks: opportunities, challenges, and approaches[J]. IEEE Network, 2019, 33(1): 128-135.
- [4] 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.
- [5] 曾勇, 王驭, 徐文斌, 等. 无线链路安全防护技术探讨[J]. 信息安全与通信保密, 2020, 18(10): 100-106.
ZENG Y, WANG Y, XU W B, et al. Discussion on the wireless link security protection technology of the space-ground integrated information network[J]. Information Security and Communications Privacy, 2020, 18(10): 100-106.
- [6] 曹进, 陈李兰, 马如慧, 等. 面向多类型终端的天地一体化信息网络接入与切换认证机制研究[J]. 天地一体化信息网络, 2021(3): 2-14.
CAO J, CHEN L L, MA R H, et al. Research on access and handover authentication mechanism of space-integrated-ground information network for multi-type terminals[J]. Space-Integrated-Ground Information Networks, 2021(3): 2-14.
- [7] CRUICKSHANK H S. A security system for satellite networks[C]//Proceedings of Fifth International Conference on Satellite Systems for Mobile Communications and Navigation. London: IET, 2002: 187-190.
- [8] TZUNG-HER C, WEI-BIN L, HSING-BAI C. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers & Electrical Engineering, 2009, 35(1): 41-48.
- [9] 任方, 马建峰, 郝选文. 空间信息网基于证书的混合式公钥基础设施[J]. 吉林大学学报(工学版), 2012, 42(2): 440-445.
REN F, MA J F, HAO X W. Certificate-based hybrid public key infrastructure for space information networks[J]. Journal of Jilin University (Engineering and Technology Edition), 2012, 42(2): 440-445.
- [10] 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.
- [11] QI M P, CHEN J H, CHEN Y T. A secure authentication with key agreement scheme using ECC for satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2019, 37(3): 234-244.
- [12] SEROUSSI G. Elliptic curve cryptography[C]//Proceedings of 1999 Information Theory and Networking Workshop (Cat. No.99EX371). Piscataway: IEEE Press, 2002: 41.
- [13] 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.
- [14] 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 (MASS). Piscataway: IEEE Press, 2018: 237-244.
- [15] LIU Y, NI L Q, PENG M G. A secure and efficient authentication protocol for satellite-terrestrial networks[J]. IEEE Internet of Things Journal, 2023, 10(7): 5810-5822.
- [16] 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.
- [17] 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.
- [18] LASC I, DOJEN R, COFFEY T. Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications[J]. Computers & Electrical Engineering, 2011, 37(2): 160-168.
- [19] 张子剑, 周琪, 张川, 等. 新的低轨星座组网认证与群组密钥协商协议[J]. 通信学报, 2018, 39(6): 146-154.
ZHANG Z J, ZHOU Q, ZHANG C, et al. New low-earth orbit satellites authentication and group key agreement protocol[J]. Journal

on Communications, 2018, 39(6): 146-154.

- [20] 朱辉, 陈思宇, 李凤华, 等. 面向低轨卫星网络的用户随遇接入认证协议[J]. 清华大学学报(自然科学版), 2019, 59(1): 1-8.
ZHU H, CHEN S Y, LI F H, et al. User random access authentication protocol for low earth orbit satellite networks[J]. Journal of Tsinghua University (Science and Technology), 2019, 59(1): 1-8.
- [21] QI M P, CHEN J H. An enhanced authentication with key agreement scheme for satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2018, 36(3): 296-304.
- [22] ALTAF I, ARSLAN A M, MAHMOOD K, et al. A novel authentication and key-agreement scheme for satellite communication network[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(7): e3894.
- [23] CHEN Y L, CHEN J H. An enhanced dynamic authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2021, 39(3): 250-262.
- [24] KUMAR U, GARG M. A note on an enhanced dynamic authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2022, 40(5): 317-329.
- [25] CASONI M, GRAZIA C, KLAPEZ M, et al. Integration of satellite and LTE for disaster recovery[J]. IEEE Communications Magazine, 2015, 53(3): 47-53.
- [26] 韩旭, 陆思奇, 程庆丰. 形式化工具 Scyther 优化与实例分析[J]. 信息安全研究, 2016, 2(3): 272-279.
HAN X, LU S Q, CHENG Q F. The improvement and instance analysis of the formal verification tool scyther[J]. Journal of Information Security Research, 2016, 2(3): 272-279.
- [27] 陆思奇, 杨忠霖, 程庆丰. 形式化分析工具 Scyther 性能研究[C]//第十九届全国青年通信学术年会论文集. [出版地不详, 出版者不详], 2014: 217-224.
LU S Q, YANG Z L, CHENG Q F, et al. The research of formal verification tool scyther[C]//Proceedings of the 19th Annual National Youth Communication Academic Conference. [S.l:s.n], 2014: 217-224.
- [28] BERINGER L, PETCHER A, YE K Q, et al. Verified correctness and security of OpenSSL HMAC[C]//Proceedings of the 24th USENIX Conference on Security Symposium. New York: ACM, 2015: 207-221.

[作者简介]



卜秋雨 (1998-), 女, 西安电子科技大学网络与信息安全学院硕士生, 主要研究方向为 4G/5G 网络、卫星互联网安全认证机制研究等。



曹进 (1985-), 男, 博士, 西安电子科技大学网络与信息安全学院教授、博士生导师, 主要研究方向为 4G/5G 网络、卫星互联网安全性及认证协议设计与分析等。



程利甫 (1985-), 男, 上海航天电子技术研究所高级工程师, 主要研究方向为空间信息安全、高性能星载计算机等。



马如慧 (1991-), 女, 博士, 西安电子科技大学网络与信息安全学院讲师, 主要研究方向为 4G/5G 网络、卫星互联网安全认证机制研究等。



李晖 (1968-), 男, 博士, 西安电子科技大学网络与信息安全学院教授、博士生导师, 主要研究方向为密码学、无线网络安全、信息理论和网络编码等。