

融合双层卫星网络的星地和星间 AKA 协议

曹进, 石小平, 马如慧, 李晖

(西安电子科技大学网络与信息安全学院, 陕西 西安 710126)

摘要: 天地一体化网络以其大时空、天网地网和星地融合的特性备受关注, 卫星不仅可以作为应急通信补充, 还可以充当空中中继站, 扩大地面网络覆盖范围, 在军用和民用场景都占据着重要地位。实体身份认证和密钥协商机制可以防止假冒实体加入天地一体化网络, 窃取用户隐私行为的发生, 保障网络信息安全。针对天地一体化网络星地传输时延较大、链路高度暴露、星上处理能力有限以及星间拓扑结构动态时变等特点, 提出一种轻量级的双层卫星网络的星间和星地组网实体身份认证 (AKA, authenticated key agreement) 协议, 以实现安全的卫星组网架构, 后续基于协商的会话密钥保护数据传输。所提协议基于对称密码体制, 采用轻量级密码算法, 引入群密钥和分层管理机制, 针对双层卫星网络的不同场景特点, 将认证协议分为高轨卫星星地和星间认证、层间和同轨道低轨卫星间认证以及相邻轨道低轨卫星间认证 3 部分。群密钥和分层管理机制提高了群组间信息的传递效率, 减轻了地面控制中心的认证压力, 且在三方认证协议中实现了双重验证, 提高了认证安全强度。不同于以往的单场景认证, 部分认证协议采取复用认证参数的形式, 在一次认证转发过程中可实现双场景的认证需求。通过协议形式化安全仿真工具 Scyther 分析结果表明, 所提协议均实现了安全接入认证。与现有协议相比, 所提协议提高了认证安全性, 降低了通信和计算开销。

关键词: 卫星通信; 双层卫星网络; 认证; 对称加密

中图分类号: TP302

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023004

Fusion of satellite-ground and inter-satellite AKA protocols for double-layer satellite networks

CAO Jin, SHI Xiaoping, MA Ruhui, LI Hui

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

Abstract: With the characteristics of large space-time and satellite-ground network integration, the space integrated ground network has attracted much attention. Satellites can not only be used as emergency communication supplements, but also serve as air stations to expand the coverage of terrestrial networks, occupying an important

收稿日期: 2022-05-12; 修回日期: 2022-11-02

通信作者: 曹进, jcao@xidian.edu.cn

基金项目: 国家重点研发计划 (2022YFB2902200); 国家自然科学基金 (62172317); 陕西省重点研发计划 (2020ZDLGY08-08)

Foundation Items: The National Key R&D Program of China (2022YFB2902200), The National Natural Science Foundation of China (62172317), The Key R&D Program of Shaanxi (2020ZDLGY08-08)

引用格式: 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.

Citation Format: 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.

position in both military and civilian scenarios. The entity authentication and key negotiation mechanism can prevent the malicious entities from joining the integrated network to steal users' privacy, and guarantee network information security. In view of the characteristics of the high satellite-ground transmission delays, exposed links, limited processing capability and dynamic topology of the integrated network, a lightweight authentication scheme between satellites and ground suitable for double-layer satellite network was proposed to achieve a secure satellite networking architecture with session keys to protect data transmission. The scheme was based on symmetric cryptographic system, using lightweight cryptographic algorithms and introducing group key and hierarchical management mechanisms. The proposed scheme included three parts: inter-satellite authentication for geostationary earth orbit satellites, layer and inter-satellite authentication for same low earth orbit, and inter-satellite authentication for adjacent low earth orbit satellites. The group key and hierarchical management mechanism improved the efficiency of inter-group information transfer, reduced the authentication pressure on the ground control center, and enhanced the authentication security strength by realizing double verification in the three-entities authentication protocol. Different from the previous single scene authentication, the proposed authentication protocol took the form of multiplexing authentication parameters, which can realize the authentication requirements of dual scenes in one process. The results of Scyther, a protocol formal security simulation tool, show that the proposed scheme achieves secure access authentication. Compared with existing protocols, the proposed scheme improves authentication security and reduces communication and computational overhead.

Keywords: satellite communications, double-layer satellite network, authentication, symmetric encryption

0 引言

随着科技信息技术的快速发展,移动通信技术从单一的语音文本业务逐渐转变为场景互联、智能融合发展,深刻影响着人类社会的进程。5G 主要应用于以下场景:增强型移动宽带(eMBB)、超可靠低时延通信(URLLC)和海量机器类通信(mMTC)。上述应用场景要求网络通信需要提供低时延、高可靠、大容量的通信业务,同时逐步实现通信场景覆盖至海洋、荒漠以及偏远地区,单纯的地面通信难以满足发展要求。因此,具有大时空特点的卫星网络受到各国的重视^[1-4]。

卫星网络具有高可靠性、灵活性和全覆盖性,可以作为地面移动互联网络的补充和储备,特别是可以满足紧急情况下的通信需求。首先,卫星网络可以通过增加卫星数量来提高网络容量,从而在全球范围内提供高速容量,缓解地理差异导致的用户请求超载进而造成地面链路拥挤的难题;其次,卫星能够为海上或空中移动平台、飞机、船只、导弹等提供海上或空中连接技术;另外,卫星可以作为物联网信息和其他内容的高速中继站,使用以信息为中心的网络跨多个站点实

现快速组播和广播通信,为设备和用户提供高效丰富的多媒体和其他数据内容。与此同时,卫星网络存在链路开放、星间拓扑网络动态时变以及星上存储和计算资源有限等特点,容易遭受各种被动攻击和主动攻击,如干扰、窃听、拒绝服务(DoS, denial of service)攻击、数据伪造或篡改、实体假冒等^[5-6]。如何解决动态开放链路环境下的星间安全组网认证问题,一直是国内外学者研究的重点。

为满足卫星通信过程中终端随遇切换、卫星动态组网的需求,通常采用不同轨道高度的卫星构成的双层或多层卫星网络来构建天地一体化信息网络。地球同步轨道(GEO)又称高轨卫星,轨道高度约为 35 786 km,单颗卫星的覆盖范围大,运行轨道是呈圆形的赤道轨道,运行周期与地球自转周期一致^[7]。高轨卫星间位置相对固定,大多为单星工作,少数进行组网。例如,海事卫星通信系统——Inmarsat,利用高轨卫星,为除两极之外的全球区域提供服务^[8]。但是,其星地传输时延较大,发射成本较高,且一旦损坏难以维护和补替,单一依靠 GEO 卫星网络会给通信带来较大的风险。中地球轨道(MEO)卫星轨道高度为 5 000~20 000 km,切换较少,星地

传输时延约为 100 ms ^[9]。低地球轨道 (LEO) 卫星轨道高度为 $500\sim 2\,000\text{ km}$, 星地传输时延最小^[10], 能够实现信息的快速转发, 是各国卫星网络发展的重点。低轨卫星的运行周期较短, 低轨卫星与地面站通信保持约几分钟, 为提供稳定的通信服务, 需要多颗低轨卫星构成卫星星座来实现全球覆盖。目前全球覆盖的中低轨卫星系统包括铱星系统和全球星系统。铱星系统采用极地轨道设计, 分为 6 个轨道面, 每个轨道面包含 11 颗在轨卫星和 1 颗伴随星, 具有星上处理和星上分组转发的能力, 可以利用轨道内和轨道间链路与前后左右卫星相连; 全球星系统采用 8 个倾斜的圆形轨道, 包含 48 颗卫星, 构成 Walker 星座^[8]。

随着商用 5G 业务的大规模快速发展, 6G 标准也提上议程。未来 6G 将在 5G 的基础上继续推进场景智能融合、移动互联网和天地空海一体化网络深度和广度发展。其中, 卫星间安全组网是保障用户安全接入卫星网络、获得可靠网络服务的第一步, 因此研究卫星网络安全组网是推进天地空海一体化网络发展的基础。

近年来, 对卫星组网认证的研究已经卓有成效, 可以划分为两部分: 基于公钥密码体系和基于对称密码体系。在基于公钥密码体系认证方面, 2007 年, 徐志博等^[11]提出了基于网络密钥交换 (IKE) 协议的端到端认证协议, 延长参数有效期, 降低第三方参与带来的时延, 实现了离线认证。Zhong 等^[12]提出了一种基于身份密码学的密钥交换协议, 通过哈希运算和可计算的 DH (CDH, computational Diffie-Hellman) 密钥协商机制, 以抵抗卫星分析和主动攻击, 提高认证效率。针对卫星资源盗用问题, 高婧等^[13]基于 ELGamal 数字签名机制提出了一种卫星网络安全认证方法, 需要密钥分配中心辅助, 认证过程简单, 开销较小, 并且减轻了卫星干扰的影响。2012 年, 任万等^[14]针对分层式空间卫星网络提出一种分布式和集中式证书授权 (CA) 混合认证模型, 增强卫星接入复杂卫星网络的认证能力。2022 年, Liu 等^[15]提出了一种分级组密钥分发和身份验证协议, 实现基于群组的接入点间的跨域切换认证, 从而有效地避免了再次认证。然而, 上述协议基于公钥密

码体系, 耗费了较多计算和带宽开销, 对星载资源受限的卫星网络提出较高的要求。

对称密码较公钥密码体制计算量小, 受到国内外学者的青睐。2009 年, Roy 等^[16]提出了一种基于定时高效流丢失容忍身份验证 (TESLA) 证书的轻量级对称密钥证书的组网通信认证协议, 该协议将卫星作为证书颁发机构, 与数字签名相比, 该协议在节点处的通信开销较小。2018 年, 针对低轨卫星网络, 张子剑等^[17]提出一种组网认证协议, 由于采用对称加密和单向哈希算法, 协议的计算开销较小, 但星间密钥协商过程完全依靠地面站, 增加了地面站压力。同年, 徐畅等^[18]提出了高轨卫星网络的组网认证协议, 设想了卫星失效情况下的密钥更新。紧接着, 徐畅等^[19]又提出了适用于低轨卫星间的轻量级组网认证协议, 该协议能抵抗拒绝服务攻击和时延较大下的重放攻击。针对低轨卫星网络临近轨道卫星间的认证, 2019 年武衡^[20]提出了星间身份认证与密钥协商 (L2L-AKA) 协议, 减少第三方参与, 提高卫星组网灵活性; 还提出了适用于双层卫星层间组网认证的层间身份认证与密钥协商 (G2L-AKA) 方案, 不需要可信第三方, 通过预计算认证材料提高认证效率。2020 年, Xue 等^[21]提出了一个轻量级的基于密钥的切换认证流程, 在群密钥协商部分定义了低轨卫星基于 (t, n) 秘密共享的软件定义空间信息网络 (SD-SIN) 协议。高轨卫星只进行信令转发, 不涉及层间卫星会话密钥的协商。随着信息技术的发展, 新的需求和新的技术层出不穷, 需要更加完整和成体系的安全组网机制, 并期望达到更优的性能。

本文针对星地、星间和层间场景提出一套适用于双层卫星网络的安全高效的认证协议, 具体贡献如下。

1) 提出高轨卫星星地和星间 AKA 协议, 高、低轨卫星的层间认证和同轨道低轨卫星的星间认证协议 (简称为层间和同轨道低轨卫星间认证) 以及相邻轨道低轨卫星间认证 3 种协议, 保障了通信信息的安全可靠传输, 灵活适应双层卫星网络安全认证的场景, 满足认证通信实体身份以及协商会话密钥的安全需求。

2) 所提协议采用对称密码体系, 在层间和星

间使用群密钥,提高了信息传输效率,对请求认证信息进行保护,如卫星身份标识、增强协议安全。

3) 所提协议针对双层卫星网络进行层次化管理,细化了认证管理体系,减轻了地面控制中心的认证压力。

4) 对所提协议的安全性采用非形式化分析和基于 Scyther 仿真工具的形式化分析,并在通信和计算开销方面进行性能比较。安全和性能对比结果显示,所提协议能以较小的认证开销满足安全认证需求。

1 系统模型和设计思路

1.1 系统模型

目前卫星数量呈海量化趋势发展,为了减轻地面站的压力,本文协议的地面站仅参与高轨卫星认证,同时采用网状组网方式^[22],卫星具有一定的星上处理和转发能力,归同一颗高轨卫星管辖的低轨卫星,由高轨卫星辅助完成认证;如果低轨卫星归不同高轨卫星管辖,则通过星间链路和星上路由选择辅助完成认证。图1为卫星系统模型。

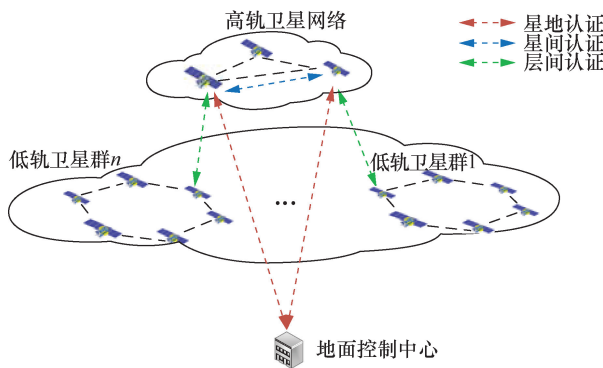


图1 卫星系统模型
Figure 1 Satellite system model

地面控制中心 (TCC, telluric control center), 存储高轨卫星认证所需要的身份、预共享密钥、轨道参数等信息,生成高轨卫星认证验证码、星地或星间会话密钥,完成目标卫星返回认证响应的校验。

高轨卫星,在星地认证过程中,完成认证验证码的校验,生成星地会话密钥、地面认证中心的认证响应;在星间认证过程中,存储低轨卫星认证所需的身份、预共享密钥、轨道参数等信息,

转发认证信息,生成或存储星间会话密钥,完成卫星返回的认证响应的校验。

低轨卫星,生成星间会话密钥,完成消息验证码或认证响应值的校验。

1.2 设计思路

针对双层卫星网络的场景需求,本文协议主要包括以下4个过程:注册阶段、高轨卫星星地和星间认证阶段、层间和同轨道低轨卫星间认证阶段以及相邻轨道低轨卫星间认证阶段,基本认证流程如图2所示。

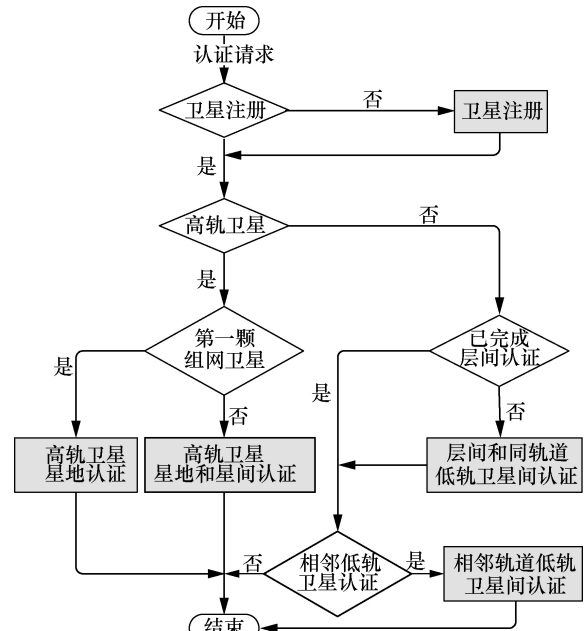


图2 整体认证流程
Figure 2 Overall certification process

发射高、低轨卫星前需要先在 TCC 完成卫星注册,赋予卫星身份标识符、预置采用的认证协议、轨道参数、密钥参数等,以便进行卫星实体认证、协商会话密钥,保证通信安全。其中,高轨卫星和 TCC 间共享一个长期密钥,低轨卫星与管理层高轨卫星间共享一个长期密钥。注册后,高轨卫星与 TCC 两两共享一对长期密钥,高轨卫星与 TCC 基于此长期共享密钥完成高轨卫星的星地和星间认证,大体过程如下。逐一发射高轨卫星,第一颗高轨卫星与 TCC 完成高轨卫星星地认证过程,其余的高轨卫星完成高轨卫星星地和星间认证。高轨卫星星地和星间认证过程完成后,高轨卫星通过星地链路获得与低轨卫星间的长期共享密钥,低轨卫星在注册阶段预置此长期共享

密钥。低轨卫星按照层间和同轨道低轨卫星间认证进行身份认证。其中，层间认证基于高轨卫星和低轨卫星间长期共享密钥生成认证材料和层间会话密钥；低轨卫星的星间认证过程中，发起方卫星基于刚刚协商出的层间会话密钥生成身份认证材料和星间会话密钥，接收方卫星的身份认证材料和星间会话密钥则由管理它的高轨卫星通过安全信道传递。层间和同轨道低轨卫星间认证过程完成后，相邻轨道的两颗低轨卫星，便可以利用高轨卫星完成相邻轨道低轨卫星间认证。

2 协议设计

2.1 卫星注册

在发射卫星之前，需要给卫星分配身份标识信息和预置长期密钥等。参数定义如表 1 所示。

表 1 参数定义
Table 1 Parameter definition

参数名称	定义
MsgKey_{gl}	群密钥
$\text{MainKey}_{\text{sec},A} / \text{MainKey}_{Ai}$	预共享密钥
$K_{\text{sec},A} / K_{AB} / K_{Ai} / K_{ij}$	会话密钥
SSID	卫星的广播身份标识
T_{msg}	时间戳
AK	时间戳的保护序列
MAC	消息验证码
RES	认证响应值
AV	认证向量
Token	认证凭证
$\text{Enc}_K(\cdot)$	基于密钥 K 的分组加密运算
$\text{KDF}(\cdot)$	基于密钥 K 的密钥生成函数
$\text{Dec}_K(\cdot)$	使用密钥 K 的解密运算
f_1	消息验证码生成函数
f_2	认证响应值生成函数
$I_1 \oplus I_2$	表示 I_1 异或 I_2 运算
$I_1 \parallel I_2$	表示 I_1 、 I_2 字符串连接运算

图 3 为高轨卫星注册流程，具体过程如下。

1) 卫星向注册域申请身份注册。

2) 注册域按照批次等信息生成卫星身份标识 ID，然后获取时间戳 T_s ，根据注册域私钥 m ，分别生成 TCC 与高轨卫星 G_A 的主密钥

$\text{MainKey}_{\text{sec},A} = \text{KDF}(m, \text{ID}_A, T_s)$ 、高轨卫星 G_A 与低轨卫星 L_i 间主密钥 $\text{MainKey}_{Ai} = \text{KDF}(m, \text{ID}_A, \text{ID}_i, T_s)$ 。

3) 注册域将 $(\text{ID}_A, \text{MainKey}_{\text{sec},A}, \text{MsgKey}_{g0})$ 、 $(\text{ID}_i, \text{MainKey}_{Ai}, \text{MsgKey}_{gl})$ 分别写入对应的高轨卫星或低轨卫星，并在本地对应存储 $(\text{ID}_A, \text{MainKey}_{\text{sec},A}, \text{MsgKey}_{g0})$ 、 $(\text{ID}_i, \text{MainKey}_{Ai})$ 用于身份认证。 MsgKey_{g0} 表示 TCC 与高轨卫星群间的群密钥， MsgKey_{gl} 表示高、低轨卫星群 l 中共享的群密钥。

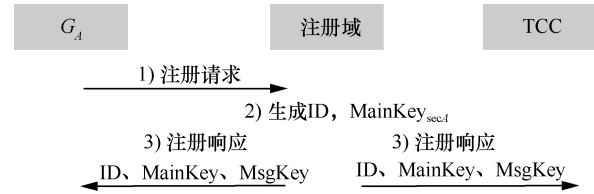


图 3 高轨卫星注册流程
Figure 3 Registration process of GEO

2.2 高轨卫星星地和星间认证协议

为了建立安全的星地和星间链路，最先部署的高轨卫星需要与 TCC 完成星地认证，其余高轨卫星需完成高轨卫星星地和星间认证接入卫星网络。此过程可概述为：首先，发起方认证请求中，添加目标卫星的身份标识符，以进行后续高轨卫星间认证；其次，TCC 基于星地长期共享密钥，查验发起方卫星身份，查验成功后，将高轨卫星间的响应值和会话密钥发送给目标卫星；然后，目标卫星获取星间会话密钥，并将认证响应值发送给发起方卫星；最后，发起方完成星地双向认证，回复星间认证响应值给目标卫星，完成星间双向认证和密钥协商。本节分别对星地认证和高轨卫星星地和星间认证进行介绍。

2.2.1 高轨卫星星地认证

针对高轨卫星星地时延较大的问题，此过程仅采用两次必要交互即可完成双向认证的安全需求，且通过时间戳避免了传统移动互联网认证过程中序列号同步造成的信令开销，高轨卫星星地认证流程如图 4 所示。

1) 高轨卫星 G_A 生成随机数 r ，获取时间戳 T_{MAC} ，生成消息验证码 $\text{MAC} = f_1(\text{MainKey}_{\text{sec},A}, \text{ID}_A, T_{\text{MAC}}, r)$ 、预期的认证响应值 $\text{XRES} = f_2(\text{MainKey}_{\text{sec},A}, \text{ID}_A, r)$ 、星地会话密钥 $K_{\text{sec},A} = \text{KDF}(\text{MainKey}_{\text{sec},A}, \text{ID}_A, T_{\text{MAC}})$ ；然后，存储

认证向量 $\mathbf{AV} = \text{XRES} \| K_{\text{sec},A} \| \text{Token}$ ，其中， $\text{Token} = r \| \text{MAC}$ ；最后，添加时间戳 T_{msg} ，向 TCC 发送认证请求 $\text{Token} \| \text{Enc}_{\text{MsgKey}_{g0}}(\text{ID}_A, T_{\text{MAC}}, T_{\text{msg}})$ 。

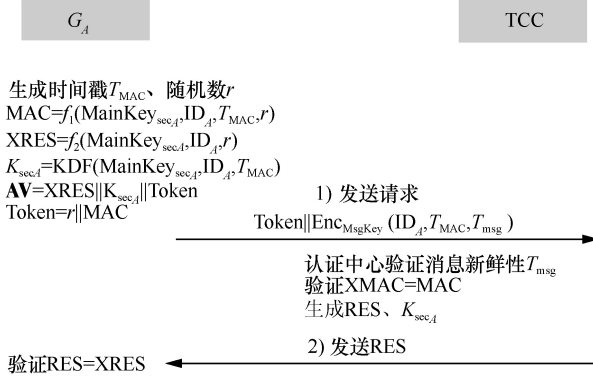


图 4 高轨卫星星地认证流程
 Figure 4 Satellite-to-ground certification process of GEO

2) TCC 的认证中心解密收到的请求，获取身份信息和时间戳。首先，检测 ID_A 的合法性以及 T_{msg} 的有效性，即需满足 $T_{\text{msg}} - T_0 \leq \Delta T_{\text{msg}}$ （当前时间 T_0 ，星地传输时延 ΔT_{msg} ）。当满足条件时，将信息传递给数据中心。数据中心根据 ID_A 查找卫星信息。如果未查找到密钥信息，判定为非法

卫星，认证终止；否则，导出长期共享密钥 $\text{MainKey}_{\text{sec},A}$ ，并从收到的消息中提取 r' 、 T'_{MAC} ，计算 $\text{XMAC} = f_1(\text{MainKey}_{\text{sec},A}, \text{ID}'_A, T'_{\text{MAC}}, r')$ ，验证 $\text{XMAC} = \text{MAC}$ 是否成立，如果成立，TCC 完成对高轨卫星 G_A 的身份认证。

随后，按照生成 XRES 和 $K_{\text{sec},A}$ 的方法计算响应值 RES 和星地会话密钥 $K_{\text{sec},A}$ ，将 RES 发送给高轨卫星 G_A 。

3) 高轨卫星 G_A 验证 $\text{RES} = \text{XRES}$ 是否成立。如果成立，则完成高轨卫星 G_A 与 TCC 的相互认证和会话密钥协商。随后，高轨卫星 G_A 与 TCC 采用会话密钥 $K_{\text{sec},A}$ 保护星地通信安全。

2.2.2 高轨卫星星地和星间认证

为实现安全的天网地网模式，在首颗高轨卫星认证完成星地认证之后，其余高轨卫星需进行高轨卫星星地和星间认证。此过程借助已认证的高轨卫星，一方面避免了待接入高轨卫星无法直接与 TCC 通信的问题，另一方面通过 4 次交互即可完成星地和星间初始接入认证，如图 5 所示。为了便于描述，假设高轨卫星 G_A 已建立安全的星地链路，高轨卫星 G_B 需接入卫星网络。

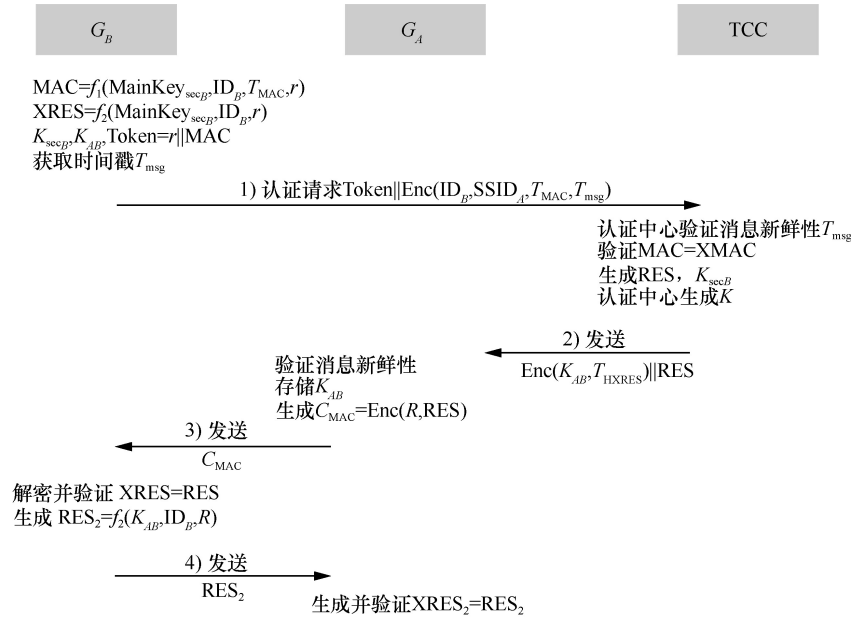


图 5 高轨卫星星地和星间认证流程
 Figure 5 Satellite-to-ground and inter-satellites certification process of GEO

1) 高轨卫星 G_B 生成随机数 r ，获取时间戳 T_{MAC} ，生成 $\text{MAC} = f_1(\text{MainKey}_{\text{sec},B}, \text{ID}_B, T_{\text{MAC}}, r)$ 、 $\text{XRES} = f_2(\text{MainKey}_{\text{sec},B}, \text{ID}_B, r)$ 、星地会话密钥

$K_{\text{sec},B} = \text{KDF}(\text{MainKey}_{\text{sec},B}, \text{ID}_B, T_{\text{MAC}})$ 和星间会话密钥 $K_{AB} = \text{KDF}(K_{\text{sec},B}, \text{ID}_A)$ 。然后，存储认证向量 $\mathbf{AV} = \text{XRES} \| K_{\text{sec},B} \| K_{AB} \| \text{Token}$ ， $\text{Token} = r \| \text{MAC}$ 。

高轨卫星 G_B 发送认证请求 $\text{Token} \parallel \text{Enc}_{\text{MsgKey}_{g_0}}(\text{ID}_B, \text{SSID}_A, T_{\text{mac}}, T_{\text{msg}})$ 给 TCC, SSID_A 为高轨卫星 G_A 的广播标识, T_{msg} 为时间戳。

2) TCC 解密收到的消息, 判断 ID_B 、 SSID_A 是否有效, T_{msg} 是否满足 $T_{\text{msg}} - T_0 \leq \Delta T_{\text{msg}}$ 。数据中心根据 ID_B 查询身份信息。若卫星没有注册, 认证终止; 否则, 导出密钥 $\text{MainKey}_{\text{sec } B}$, 生成消息验证码 $\text{XMAC} = f_1(\text{MainKey}_{\text{sec } B}, \text{ID}_B, T_{\text{mac}}, r)$, 验证 $\text{XMAC} = \text{MAC}$ 是否成立。如果成立, 计算响应值 $\text{RES} = f_2(\text{MainKey}_{\text{sec } B}, \text{ID}_B, r)$ 和星地会话密钥 $K_{\text{sec } B} = \text{KDF}(\text{MainKey}_{\text{sec } B}, \text{ID}_B, T_{\text{mac}})$, 随后将 RES 传递给认证中心。

认证中心根据 SSID_A 查找目标卫星的身份 ID_A 和星地会话密钥 $K_{\text{sec } A}$, 生成高轨卫星间会话密钥 $K_{AB} = \text{KDF}(K_{\text{sec } B}, \text{ID}_A)$, 添加时间戳合并成新的认证向量 $\text{AV}' = \text{Enc}_{K_{\text{sec } A}}(K_{AB}, T_{\text{HXRES}}) \parallel \text{RES}$, 将 AV' 发送给高轨卫星 G_A 。

3) 高轨卫星 G_A 利用 $K_{\text{sec } A}$ 解密得到 T_{HXRES} , 判断是否满足 $T_{\text{HXRES}} - T_0 \leq \Delta T_{\text{HXRES}}$ 。然后, 高轨卫星 G_A 生成随机数 R , 计算 $C_{\text{MAC}} = \text{Enc}_{K_{AB}}(R, \text{RES})$, 将 C_{MAC} 发送给高轨卫星 G_B 。

4) 高轨卫星 G_B 利用 K_{AB} 解密得到 R 和 RES, 验证 $\text{XRES} = \text{RES}$ 是否成立。如果验证成功, 高轨卫星 G_B 完成对高轨卫星 G_A 和 TCC 的身份认证。然后, 生成 $\text{RES}_2 = f_2(K_{AB}, \text{ID}_B, R)$ 发送给高轨卫星 G_A 。

5) 高轨卫星 G_A 收到消息后, 计算 $\text{XRES}_2 = f_2(K_{AB}, \text{ID}_B, R)$ 。如果 $\text{XRES}_2 = \text{RES}_2$, 高轨卫星 G_A 完成对高轨卫星 G_B 的身份认证, 整体认证和密钥协商完成。

2.3 层间和同轨道低轨卫星间认证协议

完成高轨卫星星地和星间认证后, TCC 利用认证过程协商出的星地会话密钥, 安全地传递高轨卫星与低轨卫星认证需要的信息, 包括低轨卫星的身份 ID_i 、长期共享密钥 MainKey_{Ai} 以及群组密钥 MsgKey_{gl} , 并将对应的身份信息和长期共享密钥存储在高轨卫星的数据中心。随后, 高轨卫星辅助低轨卫星执行层间和同轨道低轨卫星认证过程如下。

首先, 低轨卫星 L_i 需要先与高轨卫星 G_A 完成层间认证; 其次, 由高轨卫星 G_A 分发星间认证材料给已完成层间认证的低轨卫星 L_j ; 随后 L_i 和 L_j 利用认证材料完成同轨道低轨卫星间认证, 流程如图 6 所示。假设高轨卫星 G_A 与低轨卫

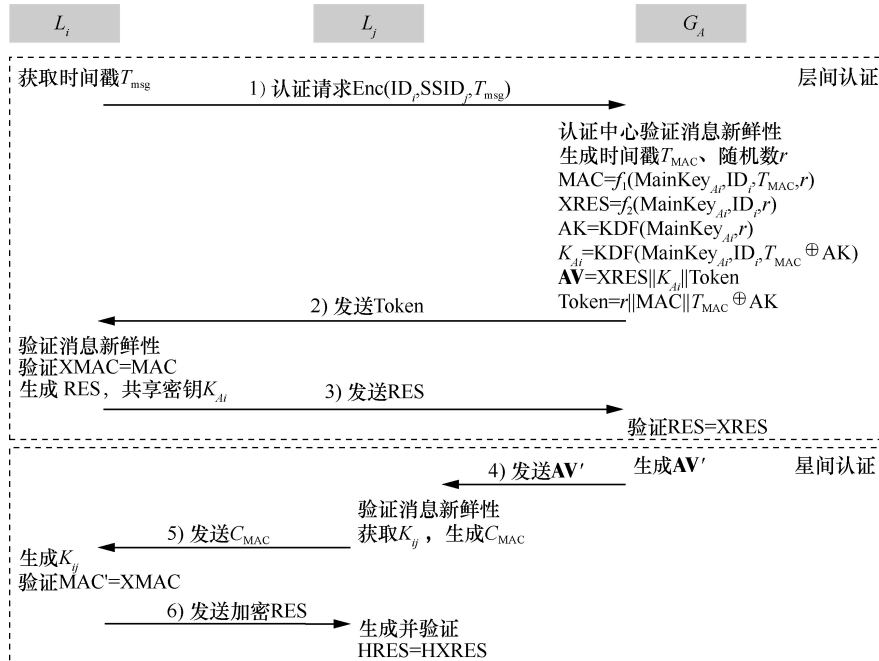


图 6 层间和同轨道低轨卫星间认证流程
Figure 6 Layer and inter-orbital certification phases of LEO

星 L_j 已经完成层间认证，并共享会话密钥 K_{Aj} ，过程如下。

1) 低轨卫星 L_i 获取时间戳 T_{msg} ，向高轨卫星 G_A 发送认证请求 $\text{Enc}_{\text{MsgKey}_{g1}}(\text{ID}_i, \text{SSID}_j, T_{\text{msg}})$ ， SSID_j 为低轨卫星 L_j 的广播标识。

2) 高轨卫星 G_A 利用 MsgKey_{g1} 解密认证请求，判断 ID_i 、 SSID_j 是否有效，且 $T_{\text{msg}} - T_0 \leq \Delta T_{\text{msg}}$ ，传递 ID_i 给高轨卫星 G_A 的数据中心。

数据中心根据 ID_i 在数据库中查询 G_A 与 L_i 的长期密钥，未查询到，认证终止；否则，导出密钥 MainKey_{Ai} ，生成随机数 r ，获取时间戳 T_{MAC} ，生成 $\text{MAC} = f_1(\text{MainKey}_{Ai}, \text{ID}_i, T_{\text{MAC}}, r)$ 、 $\text{XRES} = f_2(\text{MainKey}_{Ai}, \text{ID}_i, r)$ 、时间戳保护序列 $\text{AK} = \text{KDF}(\text{MainKey}_{Ai}, r)$ 、层间共享密钥 $K_{Ai} = \text{KDF}(\text{MainKey}_{Ai}, \text{ID}_i, T_{\text{MAC}} \oplus \text{AK})$ 。然后，合并成认证向量 $\text{AV} = \text{XRES} \parallel K_{Ai} \parallel \text{Token}$ ，其中， $\text{Token} = r \parallel \text{MAC} \parallel T_{\text{MAC}} \oplus \text{AK}$ 。高轨卫星 G_A 发送 Token 给低轨卫星 L_i 。

3) 低轨卫星 L_i 从 Token 中提取 r ，计算 AK ，验证是否满足 $T_{\text{MAC}} - T_0 \leq \Delta T_{\text{MAC}}$ 。不满足，终止认证；否则，计算消息验证码 $\text{XMAC} = f_1(\text{MainKey}_{Ai}, \text{ID}_i, T_{\text{MAC}}, r)$ ，验证 $\text{XMAC} = \text{MAC}$ 成立。生成认证响应值 $\text{RES} = f_2(\text{MainKey}_{Ai}, \text{ID}_i, r)$ 、层间共享密钥 $K_{Ai} = \text{KDF}(\text{MainKey}_{Ai}, \text{ID}_i, T_{\text{MAC}} \oplus \text{AK})$ ，将 RES 发送给高轨卫星 G_A 。

4) 高轨卫星 G_A 验证 $\text{RES} = \text{XRES}$ ，至此，高轨卫星 G_A 和低轨卫星 L_i 层间认证完成。

根据 SSID_j ，高轨卫星 G_A 查找对应的身份信息 ID_j 和会话密钥 K_{Aj} ，获取时间戳 T_{HXRES} ，生成低轨卫星 L_j 预期的认证响应 $\text{HXRES} = \text{KDF}(K_{Aj}, \text{XRES})$ 、低轨星间共享密钥 $K_{ij} = \text{KDF}(K_{Ai}, \text{ID}_j)$ ，合成认证向量 $\text{AV}' = \text{Enc}_{K_{Aj}}(K_{ij}, \text{HXRES}, T_{\text{HXRES}}, \text{MAC})$ ，将 AV' 发送给低轨卫星 L_j 。

5) 低轨卫星 L_j ，利用 K_{Aj} 解密得到 T_{HXRES} ， $T_0 \leq \Delta T_{\text{HXRES}}$ ，判断是否满足 $T_{\text{HXRES}} - T_0 \leq \Delta T_{\text{HXRES}}$ 。如果满足，低轨卫星 L_j 利用共享密钥 K_{ij} ，生成 $C_{\text{MAC}} = \text{Enc}_{K_{ij}}(\text{MAC})$ ，然后将 C_{MAC} 发送给低轨卫星 L_i 。

(6) 低轨卫星 L_i 收到 C_{MAC} 后，按照相同的方法生成低轨星间共享密钥 K_{ij} 。由生成的 K_{ij} 解密 C_{MAC} ，如果解密得到的 $\text{MAC}' = C_{\text{MAC}}$ ，则完成对低轨卫星 L_j 的认证，并认为低轨卫星 L_i 、 L_j 拥有共同的密钥 K_{ij} 。随后，计算并发送 $\text{Enc}_{K_{ij}}(\text{RES})$ 给低轨卫星 L_j 。

7) 低轨卫星 L_j 解密得到 RES ，计算 $\text{HRES} = \text{KDF}_{K_{Aj}}(\text{RES})$ ，如果 $\text{HRES} = \text{HXRES}$ ，认证成功。认证成功后，低轨卫星 L_i 与高轨卫星 G_A 利用 K_{Ai} 衍生密钥保护层间通信安全，低轨卫星 L_i 、 L_j 基于 K_{ij} 衍生密钥保护同轨道低轨卫星间通信安全。

2.4 相邻轨道低轨卫星间认证阶段

为了提高星间链路的灵活性，当相邻轨道上的两颗卫星运行到视距范围之内时，可以通过执行相邻轨道低轨卫星间认证以建立安全的通信链路。由于不同的轨道面可能由同一个或不同高轨卫星控制，相邻轨道低轨卫星间认证则借助于已完成层间认证的高轨卫星完成相互认证与密钥协商。

如图7所示，假设低轨卫星 L_i 、 L_k 分别属于高轨卫星 G_A 、 G_B ，首先低轨卫星需要按照层间认证过程完成实体身份认证和密钥协商；其次，发起方卫星 L_i 发起认证请求给高轨卫星 G_A ，此高轨卫星生成相邻轨道低轨卫星间的会话密钥；然后，高轨卫星 G_A 通过高轨卫星间的链路转发给高轨卫星 G_B ，高轨卫星 G_B 通过层间链路转发给卫星 L_k ；最后，低轨卫星 L_i 、 L_k 基于高轨卫星 G_A 生成的会话密钥完成相互认证。步骤如下。

1) 低轨卫星 L_i 获取时间戳 T_{msg} ，向高轨卫星 G_A 发送认证请求 $\text{Enc}_{\text{MsgKey}_{g1}}(\text{ID}_i, \text{SSID}_k, T_{\text{msg}})$ ， SSID_k 为低轨卫星 L_k 的广播标识。

2) 高轨卫星 G_A 利用 MsgKey_{g1} 解密认证请求，判断 ID_i 、 SSID_k 是否有效， T_{msg} 是否满足 $T_{\text{msg}} - T_0 \leq \Delta T_{\text{msg}}$ 。高轨卫星 G_A 根据 ID_i ，认证中心找到已经协商过的会话密钥 K_{Ai} ，然后根据 SSID_k 查找对应的 ID_k ，生成低轨卫星间共享密钥 $K_{ik} = \text{KDF}(K_{Ai}, \text{ID}_k, T_{\text{msg}})$ 。然后，高轨卫星 G_A 获取时间戳 $T_{\text{msg}'}$ ，利用高轨卫星 G_A 、 G_B 间的会话密

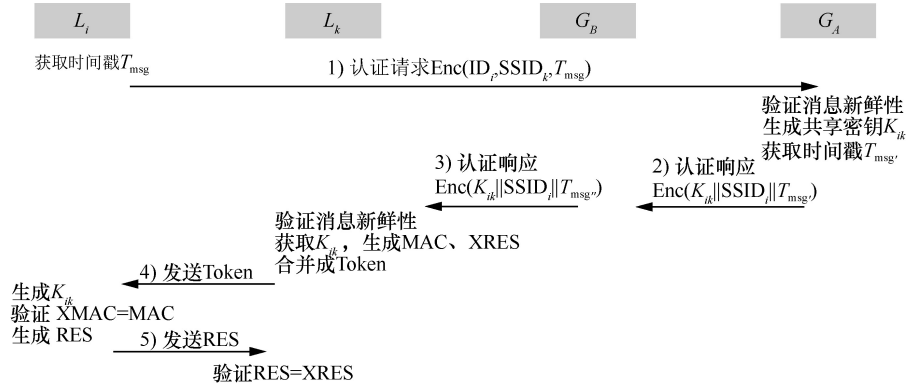


图 7 相邻轨道低轨卫星间认证流程
Figure 7 Adjacent orbital certification phases of LE

钥 K_{AB} 将 $\text{Enc}_{K_{ik}}(K_{ik}, \text{SSID}_i, T_{\text{msg}'})$ 传递给高轨卫星 G_B 。

3) 高轨卫星 G_B 解密后, 由 $T_{\text{msg}''}$ 判断消息新鲜性。然后, 获取时间戳 $T_{\text{msg}''}$, 利用层间会话密钥 K_{Bk} 给低轨卫星 L_k 发送消息 $\text{Enc}_{K_{Bk}}(K_{ik}, \text{SSID}_i, T_{\text{msg}''})$ 。

4) 低轨卫星 L_k 解密消息, 判断 $T_{\text{msg}''}$ 是否满足 $T_{\text{msg}'} - T_0 \leq \Delta T_{\text{msg}''}$ 。符合条件后, 根据 SSID_i 找到对应的 ID_i 。认证中心生成随机数 r , 生成 $\text{MAC} = f_1(K_{ik}, \text{ID}_i, r)$ 、 $\text{XRES} = f_2(K_{ik}, \text{ID}_k, r)$, 合并成 $\text{Token} = r || \text{MAC}$, 然后发送 Token 给 L_i 。

5) 计算低轨卫星 L_i 、 L_k 共享密钥 $K_{ik} = \text{KDF}(K_{Ai}, \text{ID}_k, T_{\text{msg}})$, 根据此密钥和 Token 中提取的 r 计算 $\text{XMAC} = f_1(K_{ik}, \text{ID}_i, r)$, 验证 $\text{XMAC} = \text{MAC}$ 是否成立。如果成立, 则计算响应值 $\text{RES} = f_2(K_{ik}, \text{ID}_k, r)$ 。

6) 卫星 L_i 回复 RES 给卫星 L_k , 卫星 L_k 验证 $\text{XRES} = \text{RES}$ 是否成立。若成立则完成低轨卫星间的相互认证和密钥协商。

另外, 当相邻轨道的两颗低轨卫星属于同一个高轨卫星管控, 可以直接利用层间会话密钥传输 $K_{ik} || \text{SSID}_i || T_{\text{msg}'}$ 。随后, L_i 和 L_k 可采用会话密钥 K_{ik} 保护通信数据的安全性。

3 安全性分析

3.1 非形式化安全性分析

(1) 双向认证

以高轨卫星星地和星间认证为例, 高轨卫星 G_B 与 TCC 的双向身份验证分别通过

$\text{XMAC} = \text{MAC}$ 、 $\text{XRES} = \text{RES}$ 完成, 因为只有拥有长期共享密钥 $\text{MainKey}_{\text{sec}B}$ 才能生成材料, 且时间戳和随机数都正确的条件下才能完成双向身份认证, 因此可以抵抗伪造和篡改攻击。高轨卫星 G_A 通过解密 C_{MAC} 获得由星间会话密钥加密的 $\text{RES} = \text{XRES}$ 验证高轨卫星 G_B 的身份, 只有拥有 K_{AB} 的卫星才能生成和获得 C_{MAC} ; 高轨卫星 G_B 通过验证 $\text{RES}_2 = \text{XRES}_2$ 来检验通信双方拥有相同密钥 K_{AB} 完成双向身份认证。

(2) 抗重放攻击

采用在消息中附加时间戳的方法来抵御消息重放攻击。以高轨卫星星地和星间认证为例, 高轨卫星 G_B 在认证请求中添加 T_{msg} , TCC 可以以此来甄别新鲜的请求, 进行响应。卫星 G_A 、 G_B 分别通过 TCC 附加的时间参数 T_{HXRES} 、 T_{MAC} 来检验消息是否在有效期内。

(3) 抗 DoS 攻击

通过在发送认证请求中添加 T_{msg} 来保证消息的新鲜性, 且对请求认证的卫星身份一起使用群密钥 MsgKey_{gi} 加密, 使得真正的卫星身份只能被网络内的卫星获得, 进行认证的卫星可以通过这两点快速剔除非认证请求, 以抵抗 DoS 攻击。

(4) 密钥独特性

以高轨卫星星地和星间认证为例, 地面认证中心和高轨卫星 G_B 的密钥 $K_{\text{sec}B} = \text{KDF}(\text{MainKey}_{\text{sec}B}, \text{ID}_B, T_{\text{MAC}})$ 基于共享主密钥各自生成, 基于 T_{MAC} 保证密钥新鲜且不可预测。对于高轨卫星 G_A 和高轨卫星 G_B 的共享密钥 $K_{AB} = \text{KDF}(K_{\text{sec}B}, \text{ID}_A)$, G_A 通过星地链路传输得到密钥, G_B 则通过 $K_{\text{sec}B}$ 生

成, 因为密钥 K_{secB} 、 K_{AB} 更新是同步的, 所以每次更新都会生成不同的密钥。

3.2 形式化安全性分析

本文使用形式化仿真工具 Scyther 来仿真和辅助分析协议的安全性^[23]。Scyther 是在完美密码学假设 (即除非攻击者知道加密密钥, 否则无法获取消息内容) 的前提下, 进行协议形式化分析的仿真工具。Scyther 基于 Dolev-Yao/强安全模型, 不存在状态空间爆炸, 适用于分析使用第三方加密算法且参与角色较少的协议。Scyther 使用 SPDL 标准协议描述语言描述协议, 按照参与角色来模拟消息传递过程, 从基本的协议形式化模型的安全属性角度, 验证认证协议中消息是否可达且被接受, 能否保证消息同步, 能否在一定程度上抵御消息篡改和伪造、身份假冒、中间人攻击等安全攻击。其结果只存在安全或攻击两种可能, 如果存在攻击, 则以攻击图的形式呈现在界面上。Scyther 仿真输出结果中 “characterize” 表示消息可达性, 即安全属性 Reachable 的验证结果, 而 “verify” 表示对安全属性的验证, 图标 “ok” 表示安全属性可满足。

本文涉及注册、高轨卫星星地和星间认证、层间和同轨道低轨卫星间认证、相邻轨道低轨卫星间认证协议, Scyther 中内置哈希函数, 通过 “hashfunction” 定义, 各协议按照角色集执行消息收发和安全属性验证。各协议 Scyther 验证结果如图 8 所示。

验证结果显示在共享长期密钥不被泄露的情况下, 消息能够有效传递, 可以满足 T_{MAC} 的机密性, 完成密钥协商; 满足时间戳参数的机密性, 即可以抵抗重放攻击; 认证实体身份不可否认, 可以完成双向认证。各协议成功验证所列出的 Scyther 安全要求, 并且在 Scyther 工具的测试下未发现任何攻击, 可满足所列出的安全属性, 包括双向认证、密钥协商、抗重放攻击和弱协商。

4 性能分析

通信开销和计算开销可以用来衡量卫星认证协议是否高效可行。本节选取部分已有组网认证协议进行比较, 其中, 文献[12]使用公钥密码学算法实现了卫星节点间的双向认证, 文献[24]基

于对称密钥学算法, 分别针对高、低轨卫星实现了层间认证和卫星节点间的双向认证, 文献[27]基于 ECDSA 实现了星地双向认证。特别说明, 文献[24]提出了认证双方基于共享密钥的认证和需要通过可信第三方传递密钥两种方式。本文提出的协议融合星地和星间协议, 即当高轨卫星星地和星间认证、层间和同轨道低轨卫星间认证两个协议执行一次时, 可以完成两次不同实体间的身份认证, 与以往单场景认证协议有所不同, 所以在对比过程中展示最终完成 N 次认证所需要的信令、带宽和计算开销。

4.1 通信开销

在卫星认证过程中, 信令需要在卫星网络和地面服务网络间进行路由转发, 本节只讨论无线链路中最短数据链路传输, 不考虑实体内部数据传递过程。由于涉及星地、层间和星间 3 种认证场景, 为了清晰直观地对比协议间的信令开销, 不对星地链路、层间链路和星间链路通信做细致区分。各协议的信令开销如表 2 第 2 列所示。

在达到与 AES-128 同等安全的条件下, 假设基于有限域密码体制的公钥长度为 3 072 bit、私钥长度为 256 bit, 椭圆曲线上的点长度为 320 bit。对于 Hash 算法以及生成 MAC、RES 的 $f1$ 、 $f2$ 算法, 采用 SM3-256 生成, 分别取运算后数据长度的前 128 bit 和后 128 bit 为 MAC 和 RES 值; 密钥派生函数 KDF 采用 SM3-HMAC-256 算法输出数据长度的前 128 bit 为密钥大小; 加密算法采用输出数据长度为 128 bit 的 SM4 算法。定义随机数的长度为 128 bit, 序列号、AMF 标识的长度为 48 bit, 时间戳、身份标识的长度为 32 bit。表 2 第 3 列列出了各协议的带宽开销。

为了更直观地展示对比结果, 图 9 以直方图的形式列出表 2 各协议的带宽开销情况。根据图 9 所示, 文献[12,27]提出的公钥协议的带宽开销较大, 文献[24,26]提出的协议中的相邻轨道低轨卫星认证实体间没有预共享密钥, 所以相对其他对称密钥协议增加了部分带宽用于身份信息请求和共享密钥传递。文献[25]提出的协议以及本文高轨卫星星地和星间认证的带宽开销较小。另外, 本文提出的 3 种协议在初次消息中使用了群密钥保障

Scyther results : verify					
Claim			Status		Comments
geo2tcc	I	geo2tcc,I2	Secret Tmsg	OK	Verified No attacks.
		geo2tcc,I3	Secret Tmac	OK	Verified No attacks.
		geo2tcc,I4	Secret k(R,I)	OK	Verified No attacks.
		geo2tcc,I5	Alive	OK	Verified No attacks.
		geo2tcc,I6	Weakagree	OK	Verified No attacks.
		geo2tcc,I7	Commit R,Tmsg,Tmac	OK	Verified No attacks.
		geo2tcc,I8	Niagree	OK	Verified No attacks.
		geo2tcc,I9	Nisynch	OK	Verified No attacks.
	R	geo2tcc,R2	Secret Tmsg	OK	Verified No attacks.
		geo2tcc,R3	Secret Tmac	OK	Verified No attacks.
		geo2tcc,R4	Secret k(R,I)	OK	Verified No attacks.
		geo2tcc,R5	Alive	OK	Verified No attacks.
		geo2tcc,R6	Weakagree	OK	Verified No attacks.
		geo2tcc,R7	Commit I,Tmsg,Tmac	OK	Verified No attacks.
		geo2tcc,R8	Niagree	OK	Verified No attacks.
		geo2tcc,R9	Nisynch	OK	Verified No attacks.

(a) 高轨卫星星地认证 verify 测试

Scyther results : verify					
Claim			Status		Comments
DoubleGeo	I	DoubleGeo,I1	Secret Tmsg	OK	No attacks within bounds.
		DoubleGeo,I2	Secret Tmac	OK	No attacks within bounds.
		DoubleGeo,I3	Alive	OK	Verified No attacks.
		DoubleGeo,I4	Weakagree	OK	No attacks within bounds.
	R	DoubleGeo,R1	Secret Tmsg	OK	No attacks within bounds.
		DoubleGeo,R2	Secret Tmac	OK	No attacks within bounds.
		DoubleGeo,R3	Secret Thres	OK	No attacks within bounds.
		DoubleGeo,R4	Alive	OK	No attacks within bounds.
		DoubleGeo,R5	Weakagree	OK	No attacks within bounds.
	S	DoubleGeo,S1	Secret Tmsg	OK	No attacks within bounds.
		DoubleGeo,S2	Secret Tmac	OK	No attacks within bounds.
		DoubleGeo,S3	Secret Thres	OK	No attacks within bounds.
		DoubleGeo,S4	Alive	OK	Verified No attacks.
		DoubleGeo,S5	Weakagree	OK	Verified No attacks.

(b) 高轨卫星星地和星间认证 verify 测试

Scyther results : verify					
Claim			Status		Comments
DoubleLeo1	I	DoubleLeo1,I1	Secret Tmsg	OK	Verified No attacks.
		DoubleLeo1,I2	Secret Tmac	OK	Verified No attacks.
		DoubleLeo1,I3	Alive	OK	Verified No attacks.
		DoubleLeo1,I4	Weakagree	OK	Verified No attacks.
	S	DoubleLeo1,S1	Secret Tmsg	OK	No attacks.
		DoubleLeo1,S2	Secret Tmac	OK	No attacks.
		DoubleLeo1,S3	Secret Thres	OK	Verified No attacks.
	J	DoubleLeo1,J1	Secret Tmac	OK	No attacks within bounds.
		DoubleLeo1,J2	Secret Thres	OK	No attacks within bounds.
		DoubleLeo1,J3	Alive	OK	Verified No attacks.
		DoubleLeo1,J4	Weakagree	OK	Verified No attacks.

(c) 层间和同轨道低轨卫星间认证 verify 测试

Scyther results : verify					
Claim			Status		Comments
DoubleLeo2	I	DoubleLeo2,I1	Secret Tmsg	OK	No attacks within bounds.
	S	DoubleLeo2,S1	Secret Tmsg	OK	Verified No attacks.
		DoubleLeo2,S2	Secret T1	OK	Verified No attacks.
	B	DoubleLeo2,B1	Secret Tmsg	OK	No attacks within bounds.
		DoubleLeo2,B2	Secret T1	OK	No attacks within bounds.
		DoubleLeo2,B3	Secret T2	OK	No attacks within bounds.
	J	DoubleLeo2,J1	Secret Tmsg	OK	No attacks within bounds.
		DoubleLeo2,J2	Secret T2	OK	No attacks within bounds.

(d) 相邻轨道低轨卫星间认证 verify 测试

图 8 协议 Scyther 验证结果
Figure 8 Protocol Scyther verification results

表 2 各协议开销
Table 2 Overhead of each protocol

协议	信令开销/次	带宽开销/byte	计算开销/ μ s
文献[12]	$2N$	$144N$	$(4T_H + 3T_{ME}) \cdot N = 4.1552 \times 10^3 \cdot N$
文献[24]-1	$2N$	$88N$	$(4T_H + 8T_{KDF}) \cdot N = 0.0157932 \times 10^3 \cdot N$
文献[24]-2	$2N$	$128N$	$(4T_H + 1T_{KDF} + 2T_{E/D}) \cdot N = 8.4735 \cdot N$
文献[25]	$3N$	$72N$	$(4T_H + 6T_{KDF} + 1T_{E/D}) \cdot N = 0.0143832 \times 10^3 \cdot N$
文献[26]	$5N$	$164N$	$(4T_H + 6T_{KDF} + 3T_{E/D}) \cdot N = 0.01714986 \times 10^3 \cdot N$
文献[27]	N	$120N$	$(1T_{sign} + 1T_{ver} + 1T_{ME}) \cdot N = 1.7 \times 10^3 \cdot N$
协议 1	$2N$	$64N$	$(4T_H + 2T_{KDF} + 1T_{E/D}) \cdot N = 9.4632 \cdot N$
协议 2	$4N / 2$	$144N / 2$	$(6T_H + 4T_{KDF} + 3T_{E/D}) \cdot N / 2 = 8.846145 \cdot N$
协议 3	$6N / 2$	$164N / 2$	$(4T_H + 7T_{KDF} + 3T_{E/D}) \cdot N / 2 = 9.22068 \cdot N$
协议 4	$5N$	$112N$	$(4T_H + 2T_{KDF} + 2T_{E/D}) \cdot N = 0.01093386 \times 10^3 \cdot N$

注：文献[24]-1：文献[24]中认证双方基于预共享密钥的认证过程；文献[24]-2：文献[24]中认证双方在可信第三方协助下的认证过程；
协议 1：星地认证；协议 2：高轨卫星星地和星间认证；协议 3：层间和同轨道低轨卫星间认证；协议 4：相邻轨道低轨卫星间认证。

卫星身份信息等不被非法卫星获取，增加了部分带宽开销，但增强了认证安全。

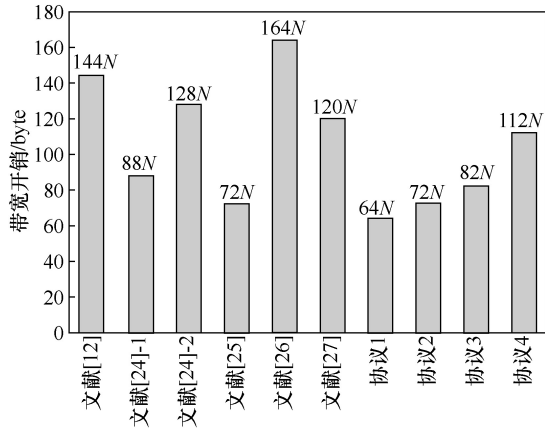


图9 带宽开销
Figure 9 Bandwidth overhead

4.2 计算开销

认证过程中的计算开销涉及异或运算、级联、单向哈希运算 T_H 、模幂运算 T_{ME} 、对称加解密运算 $T_{E/D}$ 、密钥派生函数 T_{ME} ，其中，异或和级联需要的计算时间较短，因此在计算开销中忽略这两类密码运算。本文参考文献[28]中的测试环境，各种密码运算的计算开销如表3所示。图10为各协议计算开销对比。由于采用计算量较小的单向哈希算法和对称密钥加解密算法，本文协议计算开销较文献[12,27]提出的协议小。相比文献[24-26]提出的协议，本文提出的3种协议计算开销较小，次于文献[24]提出的协议。

表3 密码运算的计算开销
Table 3 Computational cost of cryptographic calculations

密码运算	计算时间/ μs
T_{ME}	0.53×10^3
T_{sign}	0.73×10^3
T_{ver}	0.44×10^3
T_H	1.21
$T_{E/D}$	1.05
T_{KDF}	1.23

综上所述，表4给出了各协议性能对比，可以看出，本文提出的协议具有更小的计算开销，且与其他协议相比在带宽上开销较小。其中，由于相邻轨道低轨卫星间认证基于高轨卫星密钥传

递，并使用传递的低轨卫星间密钥进行了密钥确认，因此，带宽和信令开销增大，但安全性得到提升。另外，本文提出的协议对卫星的真实身份使用了群密钥加密，避免了卫星身份追踪的分析和攻击。

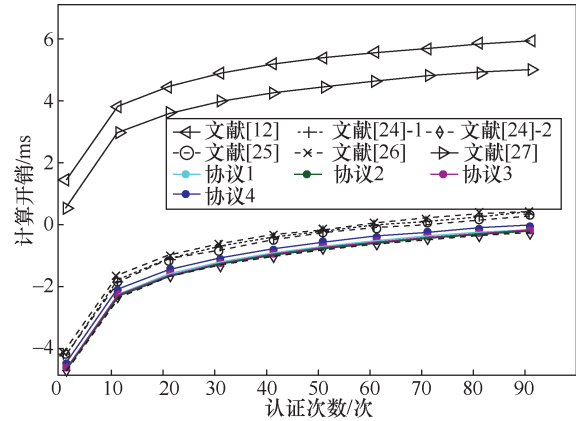


图10 计算开销对比
Figure 10 Computation overhead Comparison

表4 各协议性能对比
Table 4 Performance comparison of each protocol

协议	信令开销	带宽开销	计算开销
文献[12]	L	H	H
文献[24]-1	L	L	M
文献[24]-2	L	H	L
文献[25]	M	L	M
文献[26]	H	H	M
文献[27]	L	M	H
协议1	L	L	L
协议2	L	L	L
协议3	M	L	L
协议4	H	M	L

注：L 指开销低；H 指开销高；M 指开销中等。

5 结束语

本文根据高、低轨卫星构成的双层卫星网络模型，分析了高轨卫星的星地和星间认证、层间认证、低轨卫星的星间认证场景，以及在此场景下卫星需要完成的星地和星间组网认证要求和安全需求。

不同于以往只针对单一卫星组网场景的认证协议，根据 5G AKA 协议中服务网络和认证中心对用户进行两次身份验证的思路，本文提出双场

景认证,将高轨卫星的星地和星间认证协议融合,高、低轨卫星层间和低轨卫星间认证协议融合,满足一次认证过程中完成两对实体身份和密钥协商的认证需求,并且借助分层管理思想,减轻星上计算压力。本文协议基于对称密码,相比基于公钥体制的卫星组网认证协议,计算量较小;本文协议使用时间戳来抵抗重放攻击,减少随机数的生成、存储和计算资源的消耗,也不需要进行序列号同步过程;本文协议对认证请求中的身份信息进行一定程度的安全保护,并通过时间戳来筛选出合适的认证请求,在一定程度上可以抵御拒绝服务攻击。

本文对提出的协议完成安全验证,可以保证数据机密性和完整性,敌手无法伪造和假冒合法实体身份,能够完成卫星的双向认证和密钥协商。通过性能分析,本文协议实现了计算开销、带宽开销和信令开销的有效平衡,认证效率较高。

参考文献:

- [1] CHEN S Z, SUN S H, KANG S L. System integration of terrestrial mobile communication and satellite communication—the trends, challenges and key technologies in B5G and 6G[J]. *China Communications*, 2020, 17(12): 156-171.
- [2] LIN M, HUANG Q Q, COLA T D, et al. Integrated 5G-satellite networks: A perspective on physical layer reliability and security[J]. *IEEE Wireless Communications*, 2020, 27(6): 52-159.
- [3] CHIHA A, WEE M V, GORATTI L, et al. Techno-economic analysis of inflight connectivity using an integrated satellite-5G network[J]. *International Journal of Satellite Communications and Networking*, 2020, 39(4): 322-338.
- [4] VLK F, SCHWARZ R T, LORENZ M, et al. Emergency 5G communication on - the - move: Concept and field trial of a mobile satellite backhaul for public protection and disaster relief[J]. *International Journal of Satellite Communications and Networking*, 2020, 39(4): 417-430.
- [5] HE D J, LI X R, CHAN S, et al. Security analysis of a space-based wireless network[J]. *IEEE Network*, 2019, 33(1): 36-43.
- [6] 张桐. 天地一体化网络中攻击检测的研究与实现[D]. 北京: 北京邮电大学, 2020.
ZHANG T. The research and realization of attack detection in the space ground integrated network[D]. Beijing: Beijing University of Posts and Telecommunications, 2020.
- [7] SAEED N, ALMORAD H, DAHROUJ H, et al. Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges[J]. *IEEE Open Journal of the Communications Society*, 2021, 2: 1505-1525.
- [8] 易克初, 李怡, 孙晨华, 等. 卫星通信的近期发展与前景展望[J]. *通信学报*, 2015, 36(6): 157-172.
- YI K C, LI Y, SUN C H, et al. Recent development and its prospect of satellite communications[J]. *Journal on Communications*, 2015, 36(6): 157-172.
- [9] 王璇. 低轨卫星网络高效安全组网研究[D]. 西安: 西安电子科技大学, 2019.
WANG X. Research on efficient and secure networking in LEO satellite networks[D]. Xi'an: Xidian University, 2019.
- [10] 朱晓攀. 大规模低轨宽带卫星网络路由关键技术研究[D]. 北京: 中国科学院大学, 2020.
ZHU X P. Research on key routing technologies of large-scale low earth orbit broadband satellite network[D]. Beijing: University of Chinese Academy of Sciences, 2020.
- [11] 徐志博, 马恒太. 一种用于卫星网络安全认证的协议设计与仿真[J]. *计算机工程与应用*, 2007, 43(17): 130-132.
XU Z B, MA H T. Design and simulation of security authentication protocol for satellite network[J]. *Computer Engineering and Applications*, 2007, 43(17): 130-132.
- [12] ZHONG Y T, MA J F. A highly secure identity-based authenticated key-exchange protocol for satellite communication[J]. *Journal of Communications and Networks*, 2012, 12(6): 592-599.
- [13] 高婧, 黄望宗. 基于 ELGamal 数字签名的卫星网络认证方案[J]. *计算机工程与设计*, 2011, 32(12): 3980-3982.
GAO J, HUANG W Z. Satellite network authentication scheme based on ELGamal digital signature[J]. *Computer Engineering and Design*. 2011, 32(12): 3980-3982.
- [14] 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 Edition)*, 2012, 42(2): 440-445.
- [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*, 2022.
- [16] ROY C A, BARAS J S. A lightweight certificate-based source authentication protocol for group communications in hybrid wireless/satellite networks[C]//*IEEE Global Telecommunications Conference*, 2009.
- [17] 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): 150-158.
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): 146-158.
- [18] 徐畅, 陈雨馨, 黄聪裕, 等. 一种高轨卫星组网认证及可信保持协议[P]. CN107979408A, 2018.
XU C, CHEN Y X, HUANG C Y, et al. A high-orbit satellite network authentication and credibility retention protocol[P]. CN107979408A, 2018.
- [19] 徐畅, 童逍瑶, 周琪, 等. 一种轻量级低轨星座组网认证与群组密钥协商协议[P]. CN108055663A, 2018.
XU C, TONG X Y, ZHOU Q, et al. A lightweight low-orbit constellation network authentication and group key agreement protocol[P]. CN108055663A, 2018.
- [20] 武衡. 卫星安全组网认证关键技术研究[D]. 西安: 西安电子科技大学, 2019.

- WU H. Research on key technology of satellite network security authentication[D]. Xi'an: Xidian University, 2019.
- [21] XUE K P, MENG W, ZHOU H C, et al. A lightweight and secure group key based handover authentication protocol for the software-defined space information network[J]. IEEE Transactions on Wireless Communications, 2020, 19(6): 3673-3684.
- [22] 刘渊, 张浩, 叶海洋, 等. 面向天地一体化信息网络的卫星链路仿真研究[J]. 通信学报, 2018, 39(4): 56-67.
- LIU Y, ZHANG H, YE H Y, et al. Research on satellite link emulation for space-ground integration information network[J]. Journal on Communications, 2018, 39(4): 56-67.
- [23] 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, CHEN Q F. The improvement and instance analysis of the formal verification tool Scyther[J]. Journal of Information Security Research, 2016, 2(3): 272-279.
- [24] HUANG C Y, ZHU L H, LI C L, et al. A new satellite constellation networking certification and reliable maintenance protocol(DISA)[C]// Proceedings of 30th International Conference on Software Engineering and Knowledge Engineering, 2018.
- [25] 朱辉, 武衡, 赵海强, 等. 适用于双层卫星网络的星间组网认证方案[J]. 通信学报, 2019, 40(3): 1-9.
- ZHU H, WU H, ZHAO H Q, et al. Efficient authentication scheme for double-layer satellite network[J]. Journal on Communications, 2019, 40(3): 1-9.
- [26] 朱辉, 武衡, 张林杰, 等. 适用于低轨卫星网络的星间组网认证系统及方法[P]. CN109547213A, 2019.
- ZHU H, WU H, ZHANG L J, et al. Inter-satellite networking authentication system and method suitable for low-orbit satellite network[P]. CN109547213A, 2019.
- [27] YANG Q Y, XUE K P, XU J, et al. AnFRA: anonymous and fast roaming authentication for space information network[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 486-497.
- [28] 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.

[作者简介]



曹进 (1985-), 男, 陕西西安人, 西安电子科技大学教授、博士生导师, 主要研究方向为 4G/5G 网络、天地一体化网络安全性及认证协议设计与分析。



石小平 (1997-), 女, 山东潍坊人, 西安电子科技大学硕士生, 主要研究方向为 4G/5G 网络、天地一体化网络安全认证机制。



马如慧 (1991-), 女, 陕西榆林人, 西安电子科技大学讲师, 主要研究方向为 4G/5G 网络、天地一体化网络安全认证机制。



李晖 (1968-), 男, 陕西西安人, 西安电子科技大学教授、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。