



EDHOC-NTN: 一种基于 CL-PKC 的轻量级认证及星地融合回传安全协议

陈美玲^{1*}, 曹进², 杨元元², 杜海涛¹, 孙玲玲¹, 黄晓婷¹, 粟粟¹

1. 中国移动通信有限公司研究院, 北京 100053

2. 西安电子科技大学网络与信息安全学院, 西安 710126

* 通信作者. E-mail: chenmeiling@chinamobile.com

收稿日期: 2025-11-01; 修回日期: 2026-01-16; 接受日期: 2026-02-24; 网络出版日期: 2026-03-06

摘要 6G 天地一体化是以基于第三代合作伙伴计划 (3rd Generation Partnership Project, 3GPP) 标准的非地面网络 (non-terrestrial network, NTN) 为具体实现路径, 它通过将卫星作为基站实现全域覆盖、低时延和多场景适配. 然而, 由于非地面网络的星地回传链路具有链路断续联通、传播时延高、网络拓扑动态变化等特征, 当前 3GPP 地面网络所采用的互联网协议安全 (Internet protocol security, IPSec) 方案由于交互轮数多、时延大、严重依赖 IP 地址进行身份认证等缺陷, 并不适合当前卫星高速移动的场景. 为此, 基于无证书公钥密码体制 (certificateless public key cryptography, CL-PKC) 与增强型密钥交换协议 (ephemeral Diffie-Hellman over COSE, EDHOC), 本文提出一种轻量级认证及星地融合回传安全协议 EDHOC-NTN, 所提出的协议在保障回传链路安全的基础上, 实现了低开销、低延迟与强安全性的统一. 基于启发式分析与形式化安全协议验证, 表明本协议具备抗重放、中间人、假冒攻击等安全性; 性能分析与仿真实验证明, 该方案较标准的 IPSec 协议能够节省 41.7% 的带宽开销和 26.4% 的计算开销, 更加适配资源受限的星地融合网络环境.

关键词 NTN, 回传安全, EDHOC, 安全认证, 基站上星

1 研究背景

空天地一体网络代表了下一代通信体系的演进范式, 其核心在于深度融合天基 (卫星)、空基 (如无人机、高空平台) 与地基网络, 以构建一个全域覆盖、无缝协同的立体化智能连接架构. 在这一体系架构的标准化进程中, 第三代合作伙伴计划 (3rd Generation Partnership Project, 3GPP) 扮演了核心角色: 早在 R15 阶段, 3GPP 就将 NTN (non-terrestrial network) 技术纳入第五代移动通信技术 (5G) 系统框架, 明确了其应用前景^[1]; 在 R17 阶段, 实现了里程碑式的突破, 制定了首个支持新空口 (new radio, NR) 卫星接入的 5G NTN 标准^[2]; 在 R18 阶段, 着重于性能强化, 特别是提升上行链路覆盖能力, 以保障更可靠的语音与消息服务^[3]; 正在进行的 R19 阶段则聚焦于架构创新与场景拓展, 重点研究再生卫星模式, 并为物联网 (Internet of Things, IoT) NTN 的存储转发机制和上行能力进行增强^[4].

在 NTN 的技术实现路径上, 主要衍生出两大分支: 基于窄带物联网 (narrow band Internet of Things, NB-IoT) 技术的 NTN NB-IoT, 和基于 NR 技术的 NTN-NR. 前者侧重以低复杂度、低成本的优势支持增强型机器

引用格式: 陈美玲, 曹进, 杨元元, 等. EDHOC-NTN: 一种基于 CL-PKC 的轻量级认证及星地融合回传安全协议. 中国科学: 信息科学, 2026, 56: 560–580, doi: 10.1360/SSI-2025-0464

Chen M L, Cao J, Yang Y Y, et al. EDHOC-NTN: a lightweight authentication and satellite-terrestrial integrated backhaul security protocol design based on CL-PKC. Sci Sin Inform, 2026, 56: 560–580, doi: 10.1360/SSI-2025-0464

类通信 (enhanced machine-type communication, eMTC) 和 NB-IoT 接入卫星网络; 后者则基于成熟的 5G NR 框架, 致力于为智能手机等终端提供直连卫星的数据与语音服务. 在网络架构层面, 3GPP 主要定义了透明转发和再生两种核心模式. 在透明转发模式下, 卫星主要作为中继节点, 负责在终端与地面信关站之间透明传输射频信号, 而所有基带协议处理均依赖于地面核心网完成. 由于其架构简单、星上处理需求低, 该模式尤其适用于对时延不敏感、但覆盖范围要求极高的场景, 例如利用地球静止轨道 (geostationary orbit, GEO) 卫星进行物联网数据回传. 相比之下, 再生模式赋予了卫星更强的星上处理能力, 使其能够完成信号的解调、解码乃至路由功能, 并可进一步通过星间链路实现空间网络的自组网. 这种架构显著降低了对地面设施的依赖, 并有效缩减了端到端传输时延, 因而在需要高速、低延迟通信的低地球轨道 (low Earth orbit, LEO) 卫星中展现出巨大潜力. 正因如此, 再生模式被 3GPP R19 阶段确立为重点推进的演进方向, 其核心特征在于将部分或完整的基站, 即 5G 新一代基站 (next generation nodeB, gNB) 功能乃至部分核心网用户面功能部署于星上, 从而在根本上提升传输效率与系统自主性.

然而, 当前 3GPP 标准的 NTN 回传链路的安全架构设计面临严峻挑战, 其根本原因在于传统地面网络的安全机制与 NTN 独特的物理及拓扑特性之间存在根本性不匹配. 尽管 3GPP 在 R17 和 R18 阶段建议采用 IPsec 协议并集成 5G 安全架构以增强防护^[2,3]. 但其在资源受限的卫星环境中存在显著矛盾. 具体而言, 传统认证与密钥协商协议 (如传输层安全协议 (transport layer security, TLS)/IPSec) 基于低时延、持久连接与静态拓扑的前提而设计, 使得其难以适用于传播时延较高、链路断续联通, 以及网络拓扑频繁变化的 NTN 网络. 传统的协议普遍依赖多次往返握手协议, 在 NTN 环境中将导致连接建立延迟急剧增加, 并在频繁的链路切换过程中造成严重的服务中断. 此外, 星上节点计算资源的有限性, 以及动态拓扑场景下静态安全配置的固有局限性, 进一步加剧了这一矛盾. 更进一步地, IPsec 的安全关联 (security association, SA) 严重依赖固定的互联网协议 (Internet protocol, IP) 地址进行身份认证^[5]. 在卫星节点高速移动的场景中, IP 变化将触发 SA 频繁重建, 严重损害通信效率. 因此, 为保障 NTN 回传链路安全并赋能空天地一体化网络, 亟需设计一种兼顾低开销、低时延与高安全性的轻量化认证与密钥协商方案, 以便保障 NTN 回传链路安全, 推动空天地一体化网络的平稳发展. 针对上述挑战, 本文提出了一种适用于 NTN 场景的轻量化认证与密钥协商方案. 该方案的设计思路是寻求两种关键技术优势互补: 一方面, 引入专为受限环境设计的轻量级密钥交换协议——EDHOC, 以取代不适应 NTN 长时延与断续链路特性的 IPSec 框架, 从而确保密钥协商过程本身的高效与鲁棒性; 另一方面, 采用 CL-PKC 作为 EDHOC 协议的身份认证根基, 可以规避传统公钥基础设施 (public key infrastructure, PKI) 带来的证书开销, 从而为整个安全协议建立极其轻量的信任根. 综上所述, 所提方案能够更加适应星地链路的特性, 降低信令交互的轮次、信令开销与计算负载, 达成安全与资源效率的统一.

本论文的主要贡献如下所述:

- (1) 本文所提出的方案以无证书公钥密码体制为安全基础, 设计并实现适配星上环境的 CL-PKC 密钥派生机制, 在提升安全强度的同时显著降低系统开销;
- (2) 本文对现有 EDHOC 协议进行轻量化优化与增强, 提出 EDHOC-NTN 密钥交换与认证协议: 采用 CL-PKC 生成的公私钥对作为 DH 静态密钥, 并引入可扩展认证协议框架旨在解决对 IP 协议的依赖问题, 从而更适配高时延、资源受限的星地通信环境;
- (3) 最后, 通过形式化安全分析与性能评估, 验证所提方案在信令开销、带宽消耗与计算负载方面的综合优势, 证实了所提方案具备良好的可靠性与可扩展性.

本文后续内容安排如下: 第 2 节综述相关的研究工作, 并分析现有方案不足; 第 3 节详细展开所提回传安全机制的设计细节; 第 4 和 5 节分别进行安全性分析与性能分析; 第 6 节分析了 NTN 环境特性对协议性能的理论影响分析; 第 7 节对全文进行总结并展望未来研究方向.

2 相关研究工作

2.1 传统的回传安全机制

在移动通信网络中,回传链路指基站(如 gNB/eNB)与核心网之间的传输通道,用于承载用户面数据和控制面信令,通常基于光纤或无线中继(如 IAB)实现连接.在 3GPP 标准框架下,回传链路的安全机制主要由以下 2 个协议规定. TS 33.210^[6]:该标准定义了网络域安全(network domain security, NDS)/IP,明确要求回传链路须采用 IPsec 协议保障数据传输的机密性与完整性. IPsec 通过加密与认证机制,保护基站与核心网之间的通信,构成回传链路的主要安全手段. TS 33.501^[7]:作为 5G 核心安全标准,该文件进一步扩展了安全要求,涵盖用户面与信令数据的保护.针对回传链路,标准要求采用传输层安全协议或 IPsec,以确保接口安全,防范中间人攻击及数据篡改.

在卫星通信网络中,并没有专门定义的回传链路概念,卫星通信协议体系多采用空间数据系统咨询委员会(CCSDS)或数字视频广播(DVB)标准:SCPS 安全协议(space communication protocol specification-security protocol, SCPS-SP)隶属于空间通信协议标准(SCPS)协议栈,旨在为空间通信提供无连接的端到端安全保护^[8].根据 DVB Document A155-1 与 ETSI TS 101 545-1^[9,10],DVB 体系在管理与控制平面采用传输保密技术降低安全风险.该技术包括链路层加密及其相关的密钥管理、身份认证和流量隐藏/混淆机制,并针对不同安全需求设定了消费级、企业级与政府级三级安全配置^[11].

2.2 星地融合网络认证机制

在星地融合网络安全领域,国内外学者提出了很多认证机制,根据采用的密码学技术的不同,这些机制主要分为以下 3 类.

(1) 基于对称密码机制:认证实体依赖双方共享的预置密钥,利用哈希函数或对称加密算法实现高效的身份验证.2019 年, Zhu 等人^[12]设计了一种基于预配置密钥的星间组网认证协议,并依据卫星轨道可预测原理设计了轻量级的 LEO 与 GEO 重认证机制.2023 年, Yang 等人^[13]借助卫星轨迹可预测特性,提出将身份信息绑定到位置密钥上,通过验证位置密钥确保身份合法性,实现星间轻量级双向认证和密钥协商.同年, Cao 等人^[14]基于层次化管理与区域划分思想,提出了覆盖 GEO 卫星、LEO 卫星与地面节点认证场景的 3 种组网认证机制,旨在降低对地面控制中心的依赖.

(2) 基于非对称密码机制:包括基于传统 PKI 的认证、基于椭圆曲线密码学(elliptic curve cryptography, ECC)的认证、基于身份密码体制(identity-based cryptography, IBC)的认证以及基于 CL-PKC 的认证方案.2020 年, Xue 等人^[15]针对空间信息网络(spatial information network, SIN)提出基于秘密共享的组密钥协商协议,并哈希函数、对称加密技术设计了组密钥切换认证方案.2021 年, Guo 等人^[16]针对无线信道易受攻击、卫星中继节点安全性不足及动态拓扑带来的切换问题,提出一种基于 ECC 的可证明安全的接入与切换认证协议.2022 年, Liu 等人^[17]针对用户设备频繁切换的问题,提出具有用户匿名可追溯性的接入认证协议与分层组密钥分配方案.2024 年, Gautam 等人^[18]针对卫星-地面融合网络易受未授权入侵的问题,提出基于 ECC 和卫星空间坐标的星间认证协议.同年, Ren 等人^[19]提出一种基于 ECC 的 LEO 与地面网络的安全认证方案,可扩展至物联网、中高轨卫星网络等多种场景,满足完美前向安全并能抵抗多种网络攻击.2025 年, Chang 等人^[20]提出了一种三方认证协议,通过批量认证和中国剩余定理实现了用户-卫星-地面站之间的相互认证.

(3) 基于混合密码体系与新兴技术的认证机制:该类研究融合多种技术实现实体认证与密钥协商.2022 年, Abdrabou 等人^[21]以多普勒频移和接收功率为特征,结合阈值假设检验与支持向量机(support vector machine, SVM)技术,提出一种 LEO 卫星物理层认证方案.2023 年, Soni 等人^[22]将区块链与聚合签名技术融合,提出面向 6G 异构网络的群组切换认证方案.2024 年, Chen 等人^[23]基于区块链技术构建了去中心化的卫星网络系统安全通信机制,通过分布式架构解决了传统集中式认证中存在的单点故障、性能瓶颈及节点安全性不足等问题.2025 年, Yan 等人^[24]提出基于多特征融合与 SVM 分类的 LEO 卫星物理层认证方案,但该方案难以抵御高资源对抗者或内部攻击.同年, Ramesh 等人^[25]提出基于信任评估的卫星物联网终端认证机制,结合哈希链和

SM2 数字签名技术设计了访问认证协议,实现了对不同信任级别终端的差异化服务.

然而,对称密码体制在动态组网下面临严峻的密钥分发与管理挑战;非对称密码体制虽简化了密钥管理,但高昂计算开销会加重星上资源的负担;区块链共识机制因固有的时延,无法满足星地链路实时性需求;物理层认证的稳定性会受信道快速变化影响,可靠性不足.因此,需要设计一种安全高效且扩展性良好的回传链路安全认证方案,以便提升星地融合网络安全性.

3 所提出的方案: EDHOC-NTN

3.1 安全威胁与安全目标

3.1.1 星地融合回传安全威胁

首先,LEO 卫星网络最显著的特征之一是其拓扑结构的高度动态性^[26].由于卫星在轨道上高速运行,卫星与地面站之间的链路频繁切换,星间链路也因卫星相对位置的持续变化而不断重构.这种动态性导致网络拓扑在短时间内发生多次变化,使得路由协议需频繁进行重计算与重收敛;同时,星载基站也因载体运动而需周期性地执行切换与更新.

其次,LEO 卫星的空口传输距离通常较远,星间链路的信号传播距离可达数百公里.长距离传输使信号更易受到宇宙射线、太阳粒子等带电粒子辐射的环境干扰.此外,卫星网络的开放性使攻击者能够利用此类干扰手段,例如通过大功率信号干扰卫星通信链路,造成服务中断^[27].长距离传输也增加了信号被窃听的风险,攻击者可更轻易地截获并破解通信内容.因此,与地面移动通信网络相比,星地回传链路面临更为严峻的空口安全威胁^[28].

再次,LEO 卫星网络的动态拓扑与长距离传输特性,为攻击者实施多种攻击创造了条件^[29],主要包括如下.
(1) 无线信号窃听与干扰:星地回传链路所使用的无线信号易被地面站或邻近飞行器截获与干扰.(2) 中间人攻击:攻击者插入基站与地面信关站之间,冒充通信双方进行欺骗.(3) 假冒攻击:攻击者伪装为合法基站或地面核心网网关,以获取访问权限或欺骗用户.(4) 重放攻击:攻击者截获并重复发送历史合法通信数据,以扰乱系统或非法获取权限.(5) 密钥破解与窃取:攻击者破解或窃取基站或核心网的私钥.(6) 资源耗尽攻击:通过发送大量无效请求,耗尽卫星平台的计算、带宽等资源,造成服务中断.

最后,卫星平台在计算能力、电源与带宽等方面资源受限,许多在地面网络中成熟的密码算法难以直接适用于星上环境.因此,星地融合网络的安全方案设计需在给定的计算、能源、带宽与成本约束下,寻求兼顾性能、安全与管理的最优解,构建一种轻量化的安全身份认证机制.

3.1.2 安全需求、攻击模型及安全目标

- 安全模型. NTN 回传链路既需保障数据机密性与完整性,适配无线链路高误码率、长时延及网络拓扑高动态性,也需要满足运营商对网络流量的可视性与可管理性要求;更关键的是,在“卫星归属卫星运营商、星上基站归属地面移动运营商”的星地异构归属架构下,安全机制需实现卫星平台与基站载荷(物理分离但逻辑一体)的联合身份认证.星地融合回传安全要求基站与地面核心网网关双向身份认证并协商会话密钥,以保障连接建立后的数据传输安全;卫星与信关站也需完成身份合法性核验,确保接入实体正确,安全模型如图 1 所示.

- 攻击模型. 基于上述安全模型,我们采用 Dolev-Yao 模型作为攻击模型.在此模型中,攻击者能够监视、篡改协议中传输的所有信息,并可以冒充合法参与者与其他方进行通信.具体地,我们假设攻击者拥有以下能力.

- (1) 完全控制通信信道:可窃听、拦截、伪造、重放或篡改用户与卫星之间、卫星与地面网络之间传输的任何消息.

- (2) 冒充合法实体:可伪装成合法的用户终端或卫星接入节点,发起会话或响应请求(但无法直接获取其长期私钥或生物特征等安全要素).

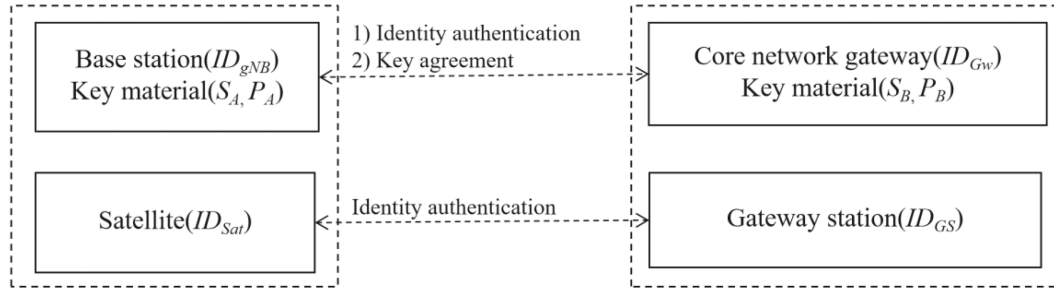


图 1 星地融合安全模型.

Figure 1 Satellite-ground integrated security model.

(3) 节点妥协能力: 考虑到卫星节点暴露于开放空间且可能资源受限, 攻击者可能通过物理攻击或侧信道分析, 临时获取部分卫星节点的会话状态或临时密钥, 但无法大规模获取长期根密钥.

● 安全目标. 我们结合 NTN 星地链路高度开放、卫星资源受限等特点, 其在协议层面易遭受信息窃听、数据篡改、中间人攻击等多种安全威胁, 确立了以下安全目标.

M1. 相互认证与密钥协商: 在协议执行结束后, 参与认证的实体之间必须相互确认对方身份的真实性, 并协商出一个仅双方知晓的会话密钥.

M2. 保障前向与后向安全性: 前向安全性指的是即使协议参与方的长期私钥在未来某时刻被泄露, 攻击者也无法恢复出在此之前协商的任何会话密钥. 后向安全性指的是即使攻击者已掌握某些旧的会话密钥, 也无法利用它们推算出当前或未来的会话密钥.

M3. 密钥确认: 在密钥协商完成后, 通信双方均能确信对方已正确计算出与自己相同的会话密钥.

M4. 可扩展性与灵活性: 确保协议能够适用于大规模、动态的 NTN 环境, 且允许安全地动态加入或移除网络节点.

M5. 抵御重放攻击: 攻击者无法通过记录并重新发送某个过往合法协议运行中的消息, 来欺骗通信是实体接受一个旧的会话.

M6. 抵御中间人攻击: 在攻击者完全控制通信信道 (可拦截、篡改、注入消息) 的情况下, 协议必须阻止攻击者冒充实体中的任何一方, 使得对等实体误以为正在与合法的实体进行通信.

M7. 抵御身份假冒攻击: 在没有合法实体的长期私钥或生物特征等安全要素的前提下, 攻击者无法成功伪装成一个合法的实体与另一方完成认证协议.

3.2 基于 CL-PKC 的密钥分发过程

为解决 NTN 星上设备资源受限、星地链路高动态及证书管理复杂问题, 本节设计基于 CL-PKC 的密钥材料分发方案. 该方案由地面密钥生成中心、星上基站与地面核心网网关参与, 具体的步骤为: (1) 系统初始化; (2) 部分私钥分发与验证; (3) 通信实体独立生成完整公私钥对.

3.2.1 系统初始化

该阶段由地面可信机构 – 密钥生成中心 (key generation center, KGC) 在离线状态下完成.

● 参数生成: 输入安全参数 k , KGC 运行双线性映射参数生成算法 $IG(k)$, 输出系统参数 $\langle G1, G2, e \rangle$, 其中 $G1, G2$ 是阶为素数 q 的加法循环群和乘法循环群, $e: G1 \times G1 \rightarrow G2$ 为一个双线性映射.

● 主密钥生成: KGC 随机选择一个主密钥 $s \in \mathbb{Z}_q^*$, 计算系统公钥 $P_{pub} = sP$, 其中 P 是 $G1$ 的一个生成元.

● 哈希函数选择: 选择密码学哈希函数 $H1: \{0, 1\}^* \rightarrow G1^*$, 用于将用户身份映射到群元素.

● 参数分发: KGC 公开系统参数 $params = \langle G1, G2, e, P, P_{pub}, H1 \rangle$, 并将其通过安全方式预配置至星上基站与地面核心网网关. 主密钥 s 由 KGC 绝密保存.

表 1 密码学符号/操作及其定义.

Table 1 Cryptographic symbols/operations and their definitions.

Cryptographic symbols/operations	Definition
Extract(salt, ikm)	Hash-based key derivation function (HKDF)-extract operation.
Expand(prk, info, len)	HKDF-expand operation.
G_{XY}	The shared secret computed by ECDH from the on-board base station's ephemeral private key (G_X) and the gateway's ephemeral public key (G_Y) (or vice versa).
G_{AY}	The shared secret computed by ECDH from the on-board base station's static private key (G_A) and the gateway's ephemeral public key (G_Y).
G_{BX}	The shared secret computed by ECDH from the gateway's static private key (G_B) and the on-board base station's ephemeral public key (G_X).
$TH_2 = H(\text{message}_1)$	The transmission hash of message ₂ .
$TH_3 = H(TH_2 \parallel \text{data}_2)$	The transmission hash of message ₃ .

3.2.2 部分私钥分发与验证

KGC 为每个网络实体生成与其身份绑定的部分私钥.

- 部分私钥生成: 对于身份为 ID_{gNB} 的星上基站, KGC 计算 $Q_{gNB} = H1(ID_{gNB})$ 作为其部分公钥, 进而计算其部分私钥 $D_{gNB} = sQ_{gNB}$. 同理, 为地面核心网网关 ID_{GW} 生成 Q_{GW} 和 $D_{GW} = sQ_{GW}$.
- 安全分发: 部分私钥通过安全上行链路 (如发射前预置或安全指令注入) 分发至对应实体.
- 实体端验证: 实体在收到部分私钥后, 需验证其有效性, 以抵御不诚实的 KGC 攻击. 星上基站验证等式 $D_{gNB} = sQ_{gNB}$ 是否成立. 若等式成立, 则证明部分私钥有效. 地面核心网网关执行相同的验证流程.

3.2.3 用户完整密钥对生成

各实体独立生成其秘密值, 并与部分私钥结合, 形成完整的非管型密钥对; 该过程因无需网络交互, 能良好适配 NTN 的断连环境.

- 秘密值生成: 星上基站随机选择 $x_{gNB} \in \mathbb{Z}_q^*$ 为其秘密值, 并安全存储于星载硬件安全模块中. 地面核心网网关同理生成 x_{GW} .
- 星上基站完整公私钥:

$$PK_{gNB} = \langle X_{gNB}, Y_{gNB} \rangle = \langle x_{gNB} \cdot P, x_{gNB} \cdot P_{pub} \rangle, \langle S_{gNB} = x_{gNB} \cdot D_{gNB} \rangle.$$

- 网关完整公私钥:

$$PK_{GW} = \langle X_{GW}, Y_{GW} \rangle = \langle x_{GW} \cdot P, x_{GW} \cdot P_{pub} \rangle, \langle S_{GW} = x_{GW} \cdot D_{GW} \rangle.$$

3.3 认证与轻量级密钥交换认证过程

为满足 NTN 回传链路对联合认证与轻量化密钥派生的需求, 本小节对标准 EDHOC 协议^[30]进行了扩展. 所提方案支持通信双方基于彼此的公钥进行临时 DH 共享密钥的协商, 并利用自身私钥对包含 EAD 身份信息的信息进行 COSE 签名与绑定操作; 方案进一步集成 EAP 框架的灵活性, 最终实现星上基站与“卫星-信关站-地面核心网网关”联合体的双向身份认证, 并派生出满足完美前向与后向保密性的会话密钥.

在所提协议中, 采用 EDHOC METHOD = 3 进行身份认证和密钥协商, 即通信双方均支持静态 DH 认证方式, 如图 2 所示. EDHOC 作为一种新的密钥交换方式, 在移植到移动通信网中需要借助现有的协议进行封装, 因此本协议采用 EAP 协议对 EDHOC 消息进行封装. 具体的认证与密钥交换协议流程如下所述: 为了方便书写和表达, 我们使用 P_A 和 P_B 来替代 P_{gNB} 和 P_{GW} . 所提协议中所采用的密码学符号/操作的定义如表 1 所示.

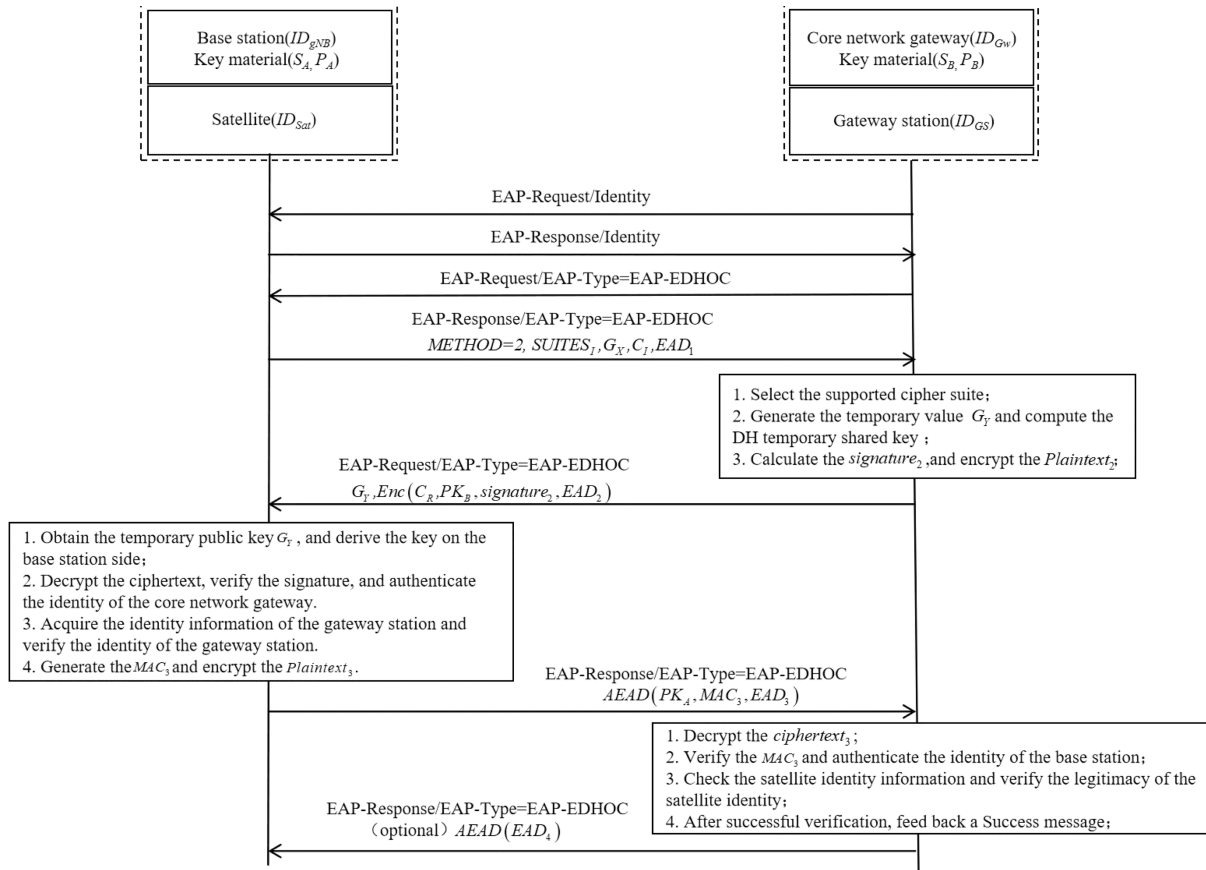


图 2 EDHOC-NTN 轻量级密钥交换协议.

Figure 2 EDHOC-NTN lightweight key exchange protocol.

步骤 0: 地面核心网网关发起 EAP 认证. 地面核心网网关作为认证方, 向星上基站发送一个 EAP-Request/EAP-Type = EAP-EDHOC 消息. 此消息作为一个触发器, 用于发起整个 EAP-EDHOC 认证流程. 其载荷可以为空, 或仅包含一个指示开始认证的标识符. 它的主要作用是通知星上基站应开始准备并发送 EDHOC 的第 1 个关键消息.

步骤 1: 星上基站响应并发送 EDHOC 初始消息.

(1) 消息构造. 基站生成一个 EDHOC 初始消息 $message_1$, 包含以下关键参数.

- METHOD: 设置为 3, 表明双方均使用静态 DH 密钥交换.
- SUITES_I: 基站支持的密码套件列表, 供网关选择.
- G_X : 基站生成的临时 DH 公钥.
- C_I : 基站的连接标识符.
- EAD₁: 外部授权数据.

(2) 封装与发送. 星上基站将 $message_1$ 进行简洁二进制对象表示 (concise binary object representation, CBOR) 编码, 并封装在 EAP-Response 数据包中, 其 EAP-Type 字段指定为 EAP-EDHOC, 随后发送给地面核心网网关.

步骤 2: 地面核心网网关处理消息并回复.

(1) 解码与校验. 地面核心网网关收到响应后

- 剥离 EAP 封装, 对载荷进行 CBOR 解码, 得到 $message_1$;
- 从 SUITES_I 中选择一个双方都支持的密码套件.

(2) 密钥计算与派生.

- 网关生成临时 DH 密钥对.

PRK _{2e} derivation—ephemeral session foundation
IF message ₁ exchange is completed THEN shared_secret_ephemeral := ECDH(x, G_Y) = ECDH(y, G_X) = G_{XY} ; PRK _{2e} := Extract(salt = NULL, ikm = G_{XY}); State_Key := PRK _{2e} ; END IF

- 加密密钥: 根据共享密钥, 采用附录 A 中的 EDHOC-NTN 派生方式产生 message₂ 的加密密钥.
- 密钥派生: 根据 EDHOC-NTN 的密钥衍生方式, 派生出 PRK_{3e2m}.
- 完整性校验: 地面核心网网关使用自身的临时私钥与星上基站的静态 DH 公钥计算共享密钥 G_{BX} , 进而生成消息认证码 MAC₂.

message ₂ encryption and authentication key derivation
IF State_Key == PRK _{2e} AND generate message ₂ THEN Keystream ₂ := Expand(PRK _{2e} , info = "EDHOC message ₂ encryption", len = len(Plaintext ₂)); Ciphertext ₂ := Plaintext ₂ $\oplus$ Keystream ₂ ; Salt _{3e2m} := Expand(PRK _{2e} , info = TH ₂ "salt for 3e2m", len = hash_len); shared_secret_static_ephemeral := ECDH(b, G_X) = G_{BX} ; PRK _{3e2m} := Extract(salt = Salt _{3e2m} , ikm = G_{BY}); MAC _{Key₂} := Expand(PRK _{3e2m} , info = "MAC ₂ Key", len = mac_key_len); MAC ₂ := MAC(MAC _{Key₂} , TH ₂ Ciphertext ₂ context ₂); State_Key := PRK _{3e2m} ; END IF

(3) 消息构造. 地面核心网网关准备响应数据, 具体包括如下.

- C_R : 地面核心网网关的连接标识符.
- PK_B : 地面核心网网关预置的公钥.
- MAC₂: 使用 EDHOC-NTN 衍生密钥对明文生成的消息验证码.
- EAD₂: 外部授权数据, 此处用于携带地面信关站的身份 ID_{GS}.
- 使用步骤 2 派生的加密密钥, 将上述数据加密, 生成密文 Ciphertext₂.

(4) 封装与发送. 将 Ciphertext₂ 与临时公钥 G_Y 拼接成 message₂, 进行 CBOR 编码后, 封装到 EAP-Response/EAP-Type=EAP-EDHOC 中, 发送回星上基站.

步骤 3: 星上基站验证地面核心网网关并回复.

(1) 解码与密钥计算. 星上基站收到消息后

- 对 message₂ 进行 CBOR 解码, 得到 G_Y 和 Ciphertext₂;
- 使用自己的临时私钥和网关的临时公钥 G_Y , 计算得到相同的共享密钥;
- 执行与网关相同的密钥派生流程, 得到解密密钥.

(2) 解密与身份验证.

- 使用临时 DH 派生出的密钥解密 Ciphertext₂, 还原出 C_R , P_B , MAC₂, ID_{GS} 等.
- 地面核心网网关身份验证. (i) 将 ID_{GS} 提供给卫星, 查询其是否在预置的合法信任列表中. 若不在, 立即终止流程. (ii) 使用地面核心网网关的临时 DH 公钥和自身的静态 DH 私钥, 计算出相同的临时 - 静态共享密

钥, 并据此验证 MAC_2 的有效性. 验证成功, 则完成对地面核心网网关的身份认证.

(3) 生成确认消息.

- 将自身的静态 DH 公钥、 MAC_3 和 EAD_3 (此处携带卫星的身份信息 ID_{sat}), 根据 EDHOC-NTN 密钥派生, 使用关联数据认证加密 (authenticated encryption with associated data, AEAD) 算法加密, 生成密文 $Ciphertext_3$.

- 使用地面核心网网关的临时 DH 公钥 (G_Y) 和星上基站自身的静态 DH 私钥, 通过 EDHOC-NTN 密钥派生流程计算生成 MAC_3 .

```

message3 encryption and authentication key derivation
IF State_Key == PRK3e2m AND generate message3 THEN
    Salt4e3m := Expand(PRK3e2m, info = TH3 || "salt for 4e3m", len = hash_len);
    shared_secret_ephemeral_static := ECDH(a, GY) = GAY;
    PRK4e3m := Extract(salt = Salt4e3m, ikm = GAY);
    K3_IV3 := Expand(PRK4e3m, info = "K3\IV3 derivation", len = key_len + iv_len);
    K3 := K3_IV3[0 : key_len];
    IV3 := K3_IV3[key_len : key_len + iv_len];
    Ciphertext3 := AEAD_Encrypt(K3, IV3, Plaintext3, associated_data = TH3);
    MAC_Key3 := Expand(PRK4e3m, info = "MAC3 Key", len = mac_key_len);
    MAC3 := MAC(MAC_Key3, TH3 || Ciphertext3 || context3);
    State_Key := PRK4e3m;
END IF

```

步骤 4: 地面核心网网关完成双向认证.

(1) 解密与验证. 地面核心网网关收到消息后

- 使用派生的相应密钥解密 $Ciphertext_3$, 得到星上基站的公钥 PK_A 和 MAC_3 ;
- 星上基站身份验证: 获取星上基站的公钥, 验证 MAC_3 . 验证成功, 则确认星上基站身份合法.

(2) 流程完成. 至此, 双向身份认证成功完成. 双方在流程中已衍生出相同的一套会话密钥, 可用于后续通信的加密和完整性保护.

```

Final session key derivation
IF State_Key == PRK4e3m AND mutual authentication is successful THEN
    Session_PRK := Expand(PRK3e2m, info = "Session Key derivation", len = session_key_len);
    APP_Key1 := Expand(Session_PRK, info = "Application Key 1", len = key_len);
    APP_Key2 := Expand(Session_PRK, info = "Application Key 2", len = key_len);
    State_Key := Session_Established;
END IF

```

4 安全性分析

4.1 启发式分析

在启发式分析方面, 我们将从以下 8 个方面对所提协议进行安全性分析.

(1) 相互认证和密钥协商. 本方案通过 DH 密钥协商在星上基站与地面核心网网关间生成临时共享密钥, 并衍生出后续会话所需密钥. 地面核心网网关使用其静态公钥与临时密钥生成 MAC, 并通过 DH 派生密钥加密消息; 星上基站利用相同临时密钥解密消息, 并以网关公钥验证消息来源. 同样, 网关通过基站公钥验证消息认证码, 实现双方相互认证.

表 2 协议的安全性对比.

Table 2 Comparison of the security of various protocols.

	Gautam et al. [18]	Chang et al. [20]	Liu et al. [17]	Guo et al. [16]	IPsec [5]	Our protocol
Mutual authentication and key agreement	Yes	Yes	Yes	Yes	Yes	Yes
Forward secrecy	Yes	Yes	Yes	Yes	Yes	Yes
Backward secrecy	Yes	Yes	Yes	Yes	Yes	Yes
Key confirmation	No	No	No	No	Yes	Yes
Scalability and flexibility	No	No	No	No	Yes	Yes
Resistance to replay attacks	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to man-in-the-middle attacks	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to impersonation attacks	Yes	Yes	Yes	Yes	Yes	Yes

(2) 前向安全. 本协议采用 ECDH 密钥交换机制, 会话密钥由双方临时公钥计算得到的共享秘密派生而来. 即便攻击者在未来获取星上基站或地面核心网网关的长期静态私钥, 也无法据此推导出此前会话使用的临时共享秘密, 进而无法解密任何历史通信内容, 有效实现完美前向安全.

(3) 后向安全. 本协议中, 每次会话均生成独立的临时 DH 密钥对 (G_X, G_Y) , 且各会话密钥在数学层面互不关联. 因此, 即便某一会话密钥泄露, 攻击者也无法据此推演未来会话的密钥, 保障协议具备完美后向安全特性.

(4) 密钥确认. 本协议中, 星上基站成功解密 message_2 并验证其 MAC 后, 不仅能完成对地面核心网网关的认证, 还可确认地面核心网网关已正确计算出共享密钥——只有持有正确密钥, 才能生成可通过验证的 MAC. 同理, 地面核心网网关对星上基站完成身份认证后, 也实现了对应的密钥确认.

(5) 可扩展性与灵活性. Suites_I 参数支持通信双方协商选用的密码算法, 使所提协议可适配不同安全需求与计算环境, 且在未来密码算法淘汰时便于升级; 此外, EAD_1 与 EAD_2 字段为协议提供了高灵活性, 支持在不改变核心密码逻辑的前提下, 携带额外应用层信息 (如卫星、信关站的身份), 助力协议更好地融入复杂星地融合架构.

(6) 抵抗重放攻击. 协议在每次认证过程中均采用新生成的临时公钥, 攻击者若重放旧公钥, 将导致共享秘密计算失败, 进而使密钥派生与解密过程失效; 同时, 协议通过连接标识符 (C_I, C_R) 绑定认证请求与响应, 任何重放的旧认证消息都会被识别为过期或重复并被拒绝. 此外, message_2 与 message_3 中的凭证及 MAC 均经过加密与完整性保护, 重放消息无法通过完整性验证, 进一步确保协议具备抗重放攻击能力.

(7) 抵抗中间人攻击. 协议采用 $\text{METHOD} = 3$ (静态 DH 模式), 通信双方通过长期静态密钥完成身份认证, 星上基站与地面核心网网关通过验证对方公钥确认身份真实性. 因攻击者不持有任一方的私钥, 既无法在密钥交换过程中计算出正确的共享秘密, 也无法伪造可通过验证的签名或 MAC, 故无法实施中间人攻击.

(8) 抵抗假冒攻击. 一方面, 攻击者因不掌握星上基站或地面核心网网关的静态私钥, 无法生成合法 MAC, 进而无法假冒任一实体身份; 另一方面, 协议将卫星与信关站的身份信息绑定至 EAD_1 与 EAD_2 字段, 且这些字段受完整性保护, 若攻击者篡改这两个字段, 会导致 EAD 内容与认证流程不一致, 最终被系统识别并拒绝.

从表 2 的安全性对比结果来看, 本文所提出的协议在安全属性的表现方面优于其他对比协议. 具体而言, 本协议不仅支持相互认证与密钥协商、前向安全、后向安全、抵抗重放攻击、中间人攻击及假冒攻击等基本安全功能, 还拥有 Gautam 等人、Chang 等人、Liu 等人、Guo 等人等协议所缺乏的“密钥确认”和“可扩展性与灵活性”. 因此, 本协议在综合安全性能上具有显著优势, 尤其在确保密钥交换的可信性与系统可扩展方面表现突出.

4.2 ROR 模型分析

ROR (real-or-random) 安全模型分析是密码学中用于验证对称加密、AEAD 等算法保密性的形式化证明框架, 其核心思路是通过挑战者向敌手交替发送真实算法生成的密文和等长的随机字符串, 并要求敌手区分两者. 若在多项式时间内, 敌手成功区分的优势是可忽略的 (趋近于 0), 则证明该算法满足 ROR 安全属性, 能够抵抗选择明文攻击等常见威胁^[31]. 本节使用 ROR 模型对 EDHOC-NTN 轻量级密钥交换协议进行形式化分析. 协议中涉及 4 类交互实体: 核心网网关实例 Π_{GW}^g (g 是网关实例编号)、星上基站实例 Π_{gNB}^b (b 是基站实例编号)、信关站实例 Π_{GS}^s (s 是信关站实例编号)、卫星实例 Π_{Sat}^t (t 是卫星实例编号). KGC 是可信的第三方, 仅承担系统初始化与密钥分发的职责, 不参与实例模拟过程.

接收状态定义. 当实例收到最终预期消息并通过全量验证, 且其收发的所有通信消息形成有序会话连接时, 进入接受状态.

- (1) Π_{gNB}^b : 接收 Π_{GW}^g 发送的 message_2 后, 解密 AEAD, 验证 MAC_2 , 检验 ID_{GS} 是否在信任列表中.
- (2) Π_{GW}^g : 接收 Π_{gNB}^b 发送的 message_3 后, 解密 AEAD, 验证 MAC_3 , 检验 ID_{Sat} 是否在信任列表中.
- (3) $\Pi_{\text{GS}}^s/\Pi_{\text{Sat}}^t$: 接收关联实例的身份检验请求, 并反馈合法确认信号.

配对定义. Π_{GW}^g 和 Π_{gNB}^b 互为伙伴需同时满足如下条件.

- (1) 双方均处于接受状态.
- (2) 完成双向身份认证: 网关通过基站公钥验证 MAC_3 , 基站通过网关公钥验证 MAC_2 , 并且实体身份, 即 ID_{GS} , ID_{Sat} 均在预置的可信列表 TrustList 内.
- (3) 双方协商的会话密钥完全一致, 且无其他实例与其中一方形成有效配对.

新鲜性定义.

- (1) 前向安全: 若 Π_{gNB}^b 和 Π_{GW}^g 建立的会话密钥未通过 Reveal 查询泄露, 即便双方长期私钥后续泄露, 该会话仍视为新鲜.
- (2) 后向安全: 若未来会话的临时密钥对未被捕获, 即便当前会话泄露, 未来会话仍视为新鲜.
- (3) 核心判定标准: 新鲜实例的会话密钥未泄露, 且关联的临时/长期密钥未被用于破解该会话.

攻击者能力定义. 基于 Dolev-Yao 威胁模型, 攻击者 $\mathcal{A}$ 具备以下能力.

- (1) $\text{Execute}(\Pi_{\text{GW}}^g, \Pi_{\text{gNB}}^b, \Pi_{\text{GS}}^s, \Pi_{\text{Sat}}^t)$: 窃听网络信道, 获取 message_1 , message_2 , message_3 的完整传输数据.
- (2) $\text{Send}(\Pi_X^x, m)$: 向目标实例发送伪造的消息 m , 并获取响应数据.
- (3) $\text{Reveal}(\Pi_{\text{GW}}^g, \Pi_{\text{gNB}}^b)$: 获取当前会话的会话密钥 SK .
- (4) $\text{RevealCurrent}(\Pi_{\text{GW}}^g, \Pi_{\text{gNB}}^b)$: 仅泄露当前会话 SK , 不涉及临时/长期密钥及未来会话数据.
- (5) $\text{Corrupt}_{\text{gNB}}(\Pi_{\text{gNB}}^b)$: 捕获基站, 获取其部分私钥 D_{gNB} 、秘密值 x_{gNB} 及系统参数.
- (6) $\text{Corrupt}_{\text{GW}}(\Pi_{\text{GW}}^g)$: 捕获网关, 获取其部分私钥 D_{GW} 、秘密值 x_{GW} 及系统参数.
- (7) $\text{Corrupt}_{\text{GS/Sat}}(\Pi_{\text{GS}}^s/\Pi_{\text{Sat}}^t)$: 获取信关站/卫星的身份标识及信任列表 TrustList .
- (8) $\text{Hash}(x)$: 向哈希预言机提交任意输入 x , 获取对应的哈希值 $\text{Hash}(x)$, 用于尝试寻找哈希碰撞或验证伪造消息的哈希有效性.
- (9) $\text{Test}(\Pi_{\text{GW}}^g, \Pi_{\text{gNB}}^b)$: 投掷公平硬币 b , 当 $b = 0$ 时返回与 SK 等长的随机字符串, 当 $b = 1$ 时返回真实 SK , 以此验证语义安全.

安全优势的定義. 攻击者 $\mathcal{A}$ 的核心目标是区分真实 SK 与随机字符串, 游戏结束时需提交猜测结果 b' . 协议 P 的安全优势定义为

$$\text{Adv}_P^{\text{AKA}} = |2\Pr[b' = b] - 1|. \quad (1)$$

若 $\text{Adv}_P^{\text{AKA}} \leq \epsilon$ (其中 ϵ 为可忽略小正数), 则表明协议在 ROR 模型下满足语义安全, 且同时具备前向安全与后向安全属性.

定理与证明过程.

定义1 设攻击者 $\mathcal{A}$ 在多项式时间 t 内运行, q_s 为 Send 查询次数, q_h 为 Hash 查询次数, $\text{Adv}_A^{\text{ECDH}}(t)$ 为 $\mathcal{A}$ 解决 ECDH 问题的优势, $|\text{Hash}|$ 为哈希函数值域, $\text{negl}(\lambda)$ 为安全参数 λ 的可忽略函数, 则协议的安全优势上限满足

$$\text{Adv}_P^{\text{AKA}}(t) \leq 2\text{Adv}_A^{\text{ECDH}}(t) + \frac{q_h^2}{|\text{Hash}|} + \frac{q_s}{|\text{TrustList}|} + \text{negl}(\lambda). \quad (2)$$

证明 定义 SUC_k 为 $\mathcal{A}$ 在 Game_k 中猜对 b 的事件, $\text{Pr}[\text{SUC}_k]$ 为该事件发生的概率, 通过逐步添加攻击者能力, 分析其对猜测概率的影响.

Game0: 真实攻击场景. $\mathcal{A}$ 不执行任何查询, 仅通过随机猜测区分 SK 与随机字符串. 由语义安全的定义可得

$$\text{Adv}_P^{\text{AKA}} = |2\text{Pr}[\text{SUC}_0] - 1|. \quad (3)$$

Game1: 添加 Execute 查询. $\mathcal{A}$ 通过窃听获取所有会话消息, 但 $\text{message}_{1/2/3}$ 中的核心数据 (如临时私钥、会话密钥派生值等) 均通过 AEAD 加密或 MAC 提供安全保护, 仅凭借窃听数据无法推导会话密钥 SK. 因此, 攻击者的猜测概率未发生变化

$$\text{Pr}[\text{SUC}_1] = \text{Pr}[\text{SUC}_0]. \quad (4)$$

Game2: 添加 Send 与 Hash 查询. $\mathcal{A}$ 发起主动伪造攻击, 并执行 Hash 查询尝试寻找哈希碰撞. 协议通过连接标识符 (C_I/C_R)、时间戳及 MAC 抵御重放攻击与数据篡改, 根据生日悖论, 哈希碰撞的概率上限为

$$|\text{Pr}[\text{SUC}_2] - \text{Pr}[\text{SUC}_1]| \leq \frac{q_h^2}{2|\text{Hash}|}. \quad (5)$$

Game3: 添加 $\text{Corrupt}_{\text{gNB}}$ 查询. $\mathcal{A}$ 捕获基站后, 可获取其长期私钥 ($D_{\text{gNB}}, x_{\text{gNB}}$), 但会话密钥 SK 由临时 DH 共享密钥 G_{XY} 派生而来, 攻击者需破解 ECDH 问题才能获取 G_{XY} , 进而推导 SK. 因此

$$|\text{Pr}[\text{SUC}_3] - \text{Pr}[\text{SUC}_2]| \leq \text{Adv}_A^{\text{ECDH}}(t). \quad (6)$$

此步骤验证了协议的前向安全, 即便基站长期私钥泄露, 攻击者仍无法破解历史会话的 SK.

Game4: 添加 $\text{Corrupt}_{\text{GW}}$ 查询. $\mathcal{A}$ 捕获网关并获取其长期私钥后, 仍需破解 ECDH 问题才能推导会话密钥 SK, 进一步强化了前向安全的约束

$$|\text{Pr}[\text{SUC}_4] - \text{Pr}[\text{SUC}_3]| \leq \text{Adv}_A^{\text{ECDH}}(t). \quad (7)$$

Game5: 添加 $\text{Corrupt}_{\text{GS/Sat}}$ 查询. $\mathcal{A}$ 获取 TrustList 后, 尝试伪造 $\text{ID}_{\text{GS}}/\text{ID}_{\text{Sat}}$ 参与认证, 其成功概率取决于伪造尝试次数与 TrustList 规模的比值, 即

$$|\text{Pr}[\text{SUC}_5] - \text{Pr}[\text{SUC}_4]| \leq \frac{q_s}{|\text{TrustList}|}. \quad (8)$$

Game6: 添加 RevealCurrent 查询. $\mathcal{A}$ 泄露当前会话的 SK, 但协议设计中每次会话均生成独立的临时 DH 密钥对 (G_X/G_Y), 未来会话的 SK 由新的临时密钥对派生, 与当前 SK 无任何数学关联. 攻击者无法通过当前 SK 推导未来会话的 G_{XY} 或临时私钥, 因此

$$|\text{Pr}[\text{SUC}_6] - \text{Pr}[\text{SUC}_5]| \leq \text{negl}(\lambda). \quad (9)$$

此步骤验证了协议的后向安全, 即当前会话密钥泄露不会影响未来会话的安全性.

在 **Game6** 中, $\mathcal{A}$ 已用尽所有可能的攻击能力 (窃听、伪造、捕获实体、泄露当前会话密钥), 无额外有效攻击路径, 其猜对 b 的概率仅为随机猜测的结果, 即 $\text{Pr}[\text{SUC}_6] = 1/2$.

根据三角不等式, 将各游戏间的概率差叠加可得

$$\begin{aligned} |\Pr[\text{SUC}_0] - 1/2| &\leq |\Pr[\text{SUC}_1] - \Pr[\text{SUC}_0]| + |\Pr[\text{SUC}_2] - \Pr[\text{SUC}_1]| \\ &\quad + |\Pr[\text{SUC}_3] - \Pr[\text{SUC}_2]| + |\Pr[\text{SUC}_4] - \Pr[\text{SUC}_3]| \\ &\quad + |\Pr[\text{SUC}_5] - \Pr[\text{SUC}_4]| + |\Pr[\text{SUC}_6] - \Pr[\text{SUC}_5]|. \end{aligned} \quad (10)$$

将式 (4)~(9) 的概率差上限代入式 (10), 并注意到 $\Pr[\text{SUC}_1] = \Pr[\text{SUC}_0]$, 可得

$$\left| \Pr[\text{SUC}_0] - \frac{1}{2} \right| \leq \frac{q_h^2}{2|\text{Hash}|} + 2\text{Adv}_A^{\text{ECDH}}(t) + \frac{q_a}{|\text{TrustList}|} + \text{negl}(\lambda).$$

由于 $\text{Adv}_P^{\text{AKA}} = |2\Pr[\text{SUC}_0] - 1| = 2\left|\Pr[\text{SUC}_0] - \frac{1}{2}\right|$, 因此

$$\text{Adv}_P^{\text{AKA}} \leq 2\text{Adv}_A^{\text{ECDH}}(t) + \frac{q_h^2}{|\text{Hash}|} + \frac{q_a}{|\text{TrustList}|} + 2\text{negl}(\lambda).$$

由于 $\text{negl}(\lambda)$ 为可忽略函数, $2\text{negl}(\lambda)$ 仍为可忽略函数, 可合并为 $\text{negl}(\lambda)$. 至此, 定理 1 得证.

EDHOC-NTN 协议的形式化安全分析表明, 其安全性可归结为 4 个相互关联的密码学基础: 协议的前向安全性依赖于 ECDH 问题在计算上的困难性; 其抗主动伪造能力由抗碰撞哈希函数保障; 实体身份的不可冒充性通过预置与动态核验的可信列表 (TrustList) 实现; 而后向安全性则由每次会话独立生成的临时密钥对确保. 基于 ROR 模型的形式化证明显示, 协议的整体安全优势上界 $\text{Adv}_P^{\text{AKA}}$ 由上述因素共同约束, 且每一项均为关于安全参数的可忽略函数. 因此, 本协议在 ROR 模型下被证明同时满足语义安全、前向安全与后向安全, 能够系统性地抵御窃听、消息重放与篡改、身份冒充、长期私钥泄露及会话密钥泄露等威胁, 适用于具有高动态拓扑与资源约束特征的星地融合回传链路安全场景.

4.3 形式化验证工具分析

Scyther 是一种基于形式化方法的安全协议验证工具, 核心作用是基于密码学假设, 自动检测认证协议中的安全漏洞, 并列举协议中可能存在的攻击路线^[32]. Scyther 的安全模型建立在经典的 Dolev-Yao 攻击模型之上, 默认攻击者能彻底掌控通信信道, 既能窃听、拦截消息, 也能篡改或伪造消息, 但是无法破坏密码学算法本身. 在 Scyther 工具中, 采用专属的安全协议描述语言 (security protocol description language, SPDL), 协议通过一组可交互的“角色”来描述, 每个角色对应一个协议参与者. 角色的行为由事件序列确定, 通过“发送”和“接收”两种操作明确消息交换的顺序和具体内容. 最终在每个角色内部声明形式化验证的目标, 其中有 4 类常见点安全属性: Secret, Alive, Weakagree, Niagree/Nisynch. Scyther 的安全性分析结果如图 3 所示, 所有角色内部的安全属性验证均显示 “No attacks”, 这意味着星上基站与地面核心网网关不仅实现了会话密钥的保密, 需要认证的实体也满足可用性要求, 还达成了协议参与方之间的强认证与消息同步, 能有效抵御假冒攻击、中间人攻击及重放攻击等威胁.

5 性能分析

本节将从信令开销、带宽开销、计算开销 3 个方面针对所提协议进行详细的性能分析, 并与其他协议进行对比分析. 在对比分析过程中, 本文假设认证实体的数量为 N , 即存在 N 个星上基站与地面核心网网关进行身份认证和密钥协商.

5.1 信令开销

各个协议的信令开销对比如表 3 所示. 从信令开销的数值对比可以看出, Chang 等人^[20]提出的方案 $(N+3)$ 显著低于其他协议, 关键在于其采用了批量认证机制, 能够对一组通信实体执行聚合式的认证与密钥协商, 从而大幅降低了按成员数量线性增长的信令负担. 相比之下, Guo 等人^[16]、IPsec^[5] 及本协议均采用实体之间的点



Claim	Status	Comments
zuwang BS zuwang,BS1 Secret KDF(KDF(G(x,y)))	Ok Verified	No attacks.
zuwang,BS2 Alive	Ok Verified	No attacks.
zuwang,BS3 Weakagree	Ok Verified	No attacks.
zuwang,BS4 Niagree	Ok Verified	No attacks.
zuwang,BS5 Nisynch	Ok Verified	No attacks.
GW zuwang,GW1 Secret KDF(KDF(G(x,y)))	Ok Verified	No attacks.
zuwang,GW2 Alive	Ok Verified	No attacks.
zuwang,GW3 Weakagree	Ok Verified	No attacks.
zuwang,GW4 Niagree	Ok Verified	No attacks.
zuwang,GW5 Nisynch	Ok Verified	No attacks.

Done.

图 3 (网络版彩图) Scyther 验证结果.

Figure 3 (Color online) Scyther verification results.

表 3 协议的信令开销对比.

Table 3 Comparison of signaling overhead of different protocols.

	Gautam et al. [18]	Chang et al. [20]	Liu et al. [17]	Guo et al. [16]	IPsec [5]	Our protocol
Signaling overhead	$2N$	$N + 3$	$2N$	$4N$	$4N$	$3N$

对点安全信令交互模式, 因此其开销随成员数 N 呈更高的线性增长, 分别为 $4N$, $4N$ 与 $3N$. Gautam 等人^[18]和 Liu 等人^[17]的方案中仅需 2 条信令实现身份认证. 但是这两个方案并没有实现密钥确认过程, 只有消息开始传输了才能确定是否协商成功, 可能造成星上基站资源耗尽、拒绝服务等问题. 本协议的信令开销处于中等水平, 由于采用了 EDHOC 认证框架, 通过轻量化的握手过程, 在控制信令负荷与提供必要的安全保证之间实现了平衡.

5.2 带宽开销

带宽开销为执行一次认证与密钥协商协议过程中, 所有信令中携带的总字节数. 为统一比较本文所提协议与其他相关方案的带宽开销, 本文根据 NIST 标准^[33]规定的 128 位的安全强度, 对协议中所涉及的各类参数长度作如下标准化假设: 身份标识的长度为 16 字节, 对称加密/解密的输出、外部授权数据 EAD 的长度均为 16 字节; 哈希函数的输出为 32 字节, 随机数、椭圆曲线点乘运算结果均为 32 字节; 时间戳、密码套件列表 SUITES 的长度均为 4 字节; 索引、连接标识符 C_I/C_R 的长度为 2 字节; 轨道参数长度为 40 字节. 所提协议与其他协议的带宽开销的对比如表 4 所示, 并且图 4 直观地展示了各个协议在认证实体数量递增情况下的带宽开销的变化趋势.

由于篇幅限制, 以本文所提出的协议为例进行介绍. 我们对 EDHOC-NTN 的 3 条主消息的有效载荷逐项进行累加计算 (忽略步骤 0 的触发消息开销): 消息 1 包含方法、密码套件、临时公钥、连接标识符和外部授权数据, 共计 55 字节; 消息 2 包含响应方临时公钥和加密载荷 (内含连接标识符、公钥、MAC 及外部授权数据), 共计 162 字节; 消息 3 包含加密载荷 (内含公钥、MAC 及外部授权数据), 共计 128 字节, 累计总开销为 $345N$ 字节 (假设认证实体的数量为 N). Chang 等人^[20]的方案采用卫星统一转发 N 个节点的接入认证信令至地面站, 其开销包含卫星与地面站之间的固定信令部分以及随 N 线性增长的部分; Guo 等人^[16]、Liu 等人^[17]所发送的消息中包含椭圆曲线公钥、对称加密等字节数较高的数据, 导致总带宽开销较大, 分别为 $468N$, $340N$. 而

表 4 协议的带宽开销对比.

Table 4 Comparison of bandwidth overhead of different protocols.

	Gautam et al. [18]	Chang et al. [20]	Liu et al. [17]	Guo et al. [16]	IPsec [5]	Our protocol
Bandwidth overhead	$248N$	$242N + 152$	$340N$	$468N$	$592N$	$345N$

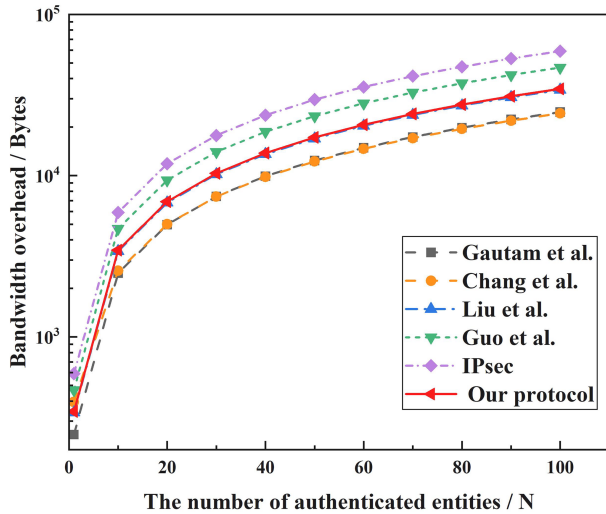


图 4 带宽开销随实体数量变化对比.

Figure 4 Comparison of bandwidth overhead with varying numbers of entities.

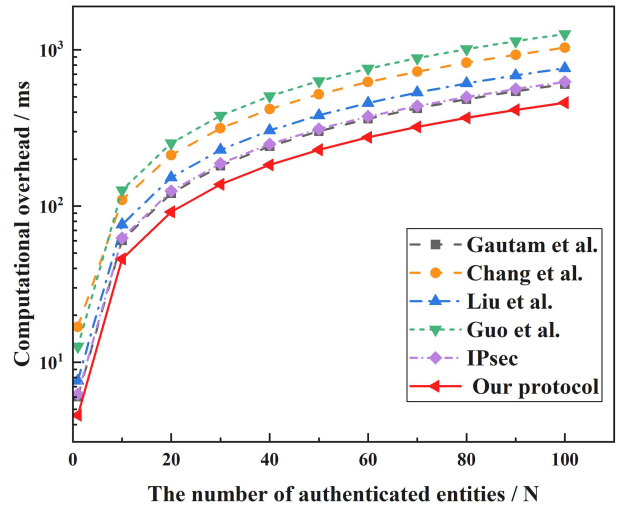


图 5 计算开销随实体数量变化对比.

Figure 5 Comparison of computational overhead with varying numbers of entities.

Gautam 等人^[18]的协议将动态的卫星实时位置压缩为固定长度的哈希值,在认证过程中仅传输此哈希值而非完整的椭圆曲线公钥或原始坐标数据,从而显著降低了每次认证交换中身份验证与密钥协商所需传输的数据量,总计 $248N$. IPsec^[5]作为通用互联网安全协议,其设计侧重于兼容性与灵活性,因此信令交互轮次多、消息内载荷种类复杂且头部冗余大,总开销高达 $592N$ 字节.本文提出的 EDHOC-NTN 采用紧凑的 CBOR 编码与精简的载荷结构,并将更多认证信息高效内嵌,从而大幅降低了协议自身的有效载荷开销.与 IPsec 相比,本协议能够减少约 41.7% 的带宽消耗.

5.3 计算开销

在 NTN 星地回传链路安全认证场景中,认证过程产生的计算开销主要包括哈希运算 T_{hash} 、椭圆曲线点乘和点加运算 T_{mul} , T_{add} 、对称加解密运算 T_{enc} , T_{dec} 、签名和验签运算 T_{sig} , T_{ver} 、密钥派生函数 T_{kdf} . 由于在当前的空间信息网络中,卫星和设备功耗及处理能力有限,通常只能部署一些安全性较低的轻量级算法.然而,随着卫星技术的发展,未来的卫星和设备可能具备更强的计算和处理能力,安全性将成为首要考虑因素.因此,为了更好地评估我们所提出的认证机制的适用性和有效性,我们已搭建了一个模拟真实空间信息网络的测试环境.具体而言,我们使用两台性能不同的计算机进行测试: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 作为资源受限卫星(基站),另一台处理器为 Core(TM) i7-7500U CPU @2.70 GHz 作为地面核心网网关,随后在这两台电脑上编译并运行 openssl-1.0.2e 库.在测试阶段,针对每个密码学算法独立执行 1000 次运算,记录每次运算的时间开销,最终取算术平均值作为对应密码学操作的计算开销.表 5 展示了各种密码学操作的计算开销.

表 5 系统对比了各个协议在计算开销方面的性能差异,图 5 进一步呈现了各认证协议在认证实体数量递增情况下的计算开销变化趋势.需要补充说明的是,表 5 所列各项基本密码学操作的单次执行耗时,单位为微秒.在评估完整协议的计算开销时,需对其中依次调用的各类密码学操作时间进行累计求和.由于各协议均包含多

表 5 各个密码学操作的计算开销 (μs).Table 5 Computational overhead (μs) of various cryptographic operations.

	T_{hash}	T_{mul}	T_{add}	T_{enc}	T_{dec}	T_{kdf}	T_{sig}	T_{ver}
Satellite (base station)	2.39	1.00×10^3	2.53	8.97	0.08	2.42	1.20×10^3	0.81×10^3
Core network gateway	1.21	0.52×10^3	1.39	5.32	0.03	1.23	0.73×10^3	0.44×10^3

次耗时较高的椭圆曲线点乘运算,使得协议级总开销自然累积至毫秒级.因此,在表5中,我们统一将协议总开销转换为秒为单位,该处理方式不影响协议间性能比较的公正性.

由于篇幅限制,我们以Gautam等人^[18]、Chang等人^[20]中的协议为例进行介绍:在文献[18]中, N 个卫星同时发起星间组网认证协议流程时,完成星间组网认证需进行 $15N$ 次哈希运算、 $6N$ 次椭圆曲线密钥乘法.在Chang等人^[20]协议中, N 个用户通过卫星完成与地面的认证与密钥协商时, N 个用户需进行 $5N$ 次椭圆曲线密钥乘法, $5N$ 次哈希运算和 4 次椭圆曲线密钥加法,卫星需进行 4 次椭圆曲线密钥乘法, 3 次哈希运算和 2 次椭圆曲线密钥加法,地面站需进行 $2N$ 次哈希运算, $3N$ 次椭圆曲线密钥乘法, $2N$ 次密钥派生, N 次加密运算和 N 次解密运算.本协议相比IPsec在计算开销上显著降低,总体计算开销从IPse的 $6.24N$ s减少至本协议的 $4.59N$ μs ,降低了26.4%的计算消耗.主要原因是在IPsec中,卫星侧需执行高开销的签名与验签操作,且星地负载对称,未区分节点性能差异;而本协议充分适配了NTN星地节点的性能异构特性,省去了卫星侧的签名与验签操作,仅在地面高性能侧适度增加一次密钥派生操作,从而避免卫星承载重负载,并利用地面算力分担开销,最终实现了计算开销的显著下降.

6 NTN环境特性对协议性能的理论影响分析

为更全面、深入地评估EDHOC-NTN协议在真实NTN环境中的适用性,本节建立理论分析模型,量化NTN的关键特征长传播时延与链路不稳定性对协议性能的影响.

6.1 模型与参数设置

(1) 轨道参数与传播时延:采用动态性较强的LEO卫星网络场景,轨道高度 $h = 600$ km,最小工作仰角 $\theta_{\min} = 10^\circ$.基于几何模型计算,星地通信的单程时延 τ 随仰角 θ 变化,如下所示:

$$\alpha = \arcsin\left(\frac{R}{R+h} \cos \theta\right), \quad \tau = \frac{\sqrt{R^2 + (R+h)^2 - 2R(R+h) \cos \alpha}}{c},$$

其中 $R = 6371$ km为地球半径, $c = 3 \times 10^8$ m/s为光速.取典型通信状态(仰角 30°)下的时延作为基准,计算可得 $\tau = 5.00$ ms.

(2) 计算开销 T_{proc} :参考表6中的统计结果,取 $N = 1$ 的值.

(3) 信令交互次数 M :参考表3中的统计结果,取 $N = 1$ 的值.

6.2 安全连接建立时延

安全连接建立总时延 T_{total} 包含协议中各种密码学操作的计算时间 T_{proc} 和传播时延 T_{prop} ,即 $T_{\text{total}} = T_{\text{proc}} + T_{\text{prop}}$.其中,传播时延 $T_{\text{prop}} = M \cdot \tau$.

各个协议的安全连接建立时延如表7所示.本协议的总握手时延为19.59 ms,仅高于Gautam等人^[18]和Liu等人^[20]的方案,显著低于Chang等人^[20]、Guo等人^[20]及IPsec协议.本协议总握手时延较低的原因是计算开销较低仅为4.59 ms,大幅减少了本地处理时间;同时,本协议的信令交互次数为3次,少于Chang等人^[20]、Guo等人^[20]及IPsec协议,降低了往返交互的时延,通过合理平衡交互次数与传播时延,实现了更优的总时延表现.

表 6 协议的计算开销对比.

Table 6 Comparison of computational overhead of various protocols.

Protocol	Satellite (base station)/user	Core network gateway/ ground control center	Total computational overhead (ms)
Gautam et al. [18]	$N(15T_{\text{hash}} + 6T_{\text{mul}})$	None	$6.04N$
Chang et al. [20]	$N(5T_{\text{mul}} + 5T_{\text{hash}} + 4T_{\text{add}}) + 4T_{\text{mul}}$ $3T_{\text{hash}} + 2T_{\text{add}}$	$(N+5)T_{\text{mul}} + (3N+3)T_{\text{hash}} + (N+3)T_{\text{add}}$	$10.67N + 6.62$
Liu et al. [17]	$N(3T_{\text{hash}} + 5T_{\text{mul}} + 2T_{\text{add}} + T_{\text{enc}})$	$N(3T_{\text{hash}} + 5T_{\text{mul}} + 2T_{\text{add}} + T_{\text{dec}})$	$7.63N$
Guo et al. [16]	$N(9T_{\text{hash}} + 10T_{\text{mul}} + 7T_{\text{add}})$	$N(4T_{\text{hash}} + 5T_{\text{mul}} + 3T_{\text{add}})$	$12.65N$
IPsec [5]	$N(2T_{\text{mul}} + T_{\text{kdf}} + T_{\text{enc}} + T_{\text{dec}}$ $+ T_{\text{sig}} + T_{\text{ver}})$	$N(2T_{\text{mul}} + T_{\text{kdf}} + T_{\text{enc}} + T_{\text{dec}} + T_{\text{sig}} + T_{\text{ver}})$	$6.24N$
Our protocol	$N(2T_{\text{hash}} + 3T_{\text{mul}} + T_{\text{kdf}} + T_{\text{enc}} + T_{\text{dec}})$	$N(2T_{\text{hash}} + 3T_{\text{mul}} + 2T_{\text{kdf}} + T_{\text{enc}} + T_{\text{dec}})$	$4.59N$

表 7 各个协议安全连接建立时延对比.

Table 7 Comparison of security connection setup delay of different protocols.

Protocol	T_{proc} (ms)	M	T_{prop} (ms)	T_{total} (ms)
Gautam et al. [18]	6.04	2	10.0	16.04
Chang et al. [20]	17.29	4	10.0	27.29
Liu et al. [17]	7.63	2	10.0	17.63
Guo et al. [16]	12.65	4	20.0	32.65
IPsec [5]	6.24	4	20.0	26.24
Our protocol	4.59	3	15.0	19.59

6.3 误码率与认证鲁棒性

采用二进制对称信道模型, 假设各比特错误独立同分布, 误码率记为 p . 在该信道下, 一条长度为 L 比特的消息完整无误接收的概率为 $P_{\text{msg}}(L) = (1-p)^L$. 对于信令交互次数为 M 的认证协议, 若各消息长度分别为 $L_1, L_2, \dots, L_M$, 则单次认证成功概率 P_{auth} 可表示为各消息成功概率的乘积

$$P_{\text{auth}} = \prod_{i=1}^M (1-p)^{L_i} = (1-p)^{\sum_{i=1}^M L_i} = (1-p)^{L_{\text{total}}},$$

其中 L_{total} 为认证交互的总比特长度.

由于星地链路受大气衰减、卫星高速运动及频繁切换影响, p 呈动态变化. 为评估各个协议在 NTN 场景下的认证鲁棒性, 设定以下典型的误码率场景.

- $p = 1 \times 10^{-6}$: 对应表面光纤/微波中继或 NTN 中高仰角晴空无雨衰的最佳链路状态.
- $p = 1 \times 10^{-5}$: 对应 NTN 中等仰角、轻度大气衰减场景.
- $p = 1 \times 10^{-4}$: 对应 NTN 典型中等恶化状态, 如低轨卫星中低仰角或轻度降雨衰减.
- $p = 5 \times 10^{-4}$: 对应 LEO 卫星低仰角或较强降雨衰减的恶劣链路状态.
- $p = 1 \times 10^{-3}$: 对应 NTN 极恶劣信道状态, 接近链路失联阈值.

在分析所有协议的成功概率时, 我们基于以下统一信道假设: 所有协议交互的所有消息, 无论实际传输路径为星地无线链路、星间无线链路或地面光纤链路, 均统一采用相同的星地无线链路误比特率. 在此统一假设下, 各协议的成功概率差异仅由其总传输长度 L_{total} 决定, 排除了信道类型差异的干扰. 表 8 对比了不同协议在多种误码率下的认证成功概率. 本协议总比特数为 2760, 远低于 Chang 等人、Guo 等人及 IPsec 的方案, 与 Liu 等人的方案相对接近. 在低误码率下, 各协议性能接近; 随着误码率上升, 本协议认证成功概率始终优于 Chang 等人、Guo 等人及 IPsec 协议, 与 Liu 等人的方案基本持平, 略低于 Gautam 等人的方案. 综合来看, 本协议以较低开销实现了良好的鲁棒性, 在资源受限场景下具有明显优势.

表 8 不同误码率下各协议的认证成功概率对比.

Table 8 Comparison of authentication success probability of different protocols under different bit error rates.

Protocol	L_{total} (bits)	$p = 1 \times 10^{-6}$	$p = 1 \times 10^{-5}$	$p = 1 \times 10^{-4}$	$p = 5 \times 10^{-4}$	$p = 1 \times 10^{-3}$
Gautam et al. [18]	1984	99.80%	98.04%	82.00%	37.08%	13.75%
Chang et al. [20]	3152	99.69%	96.90%	72.96%	20.68%	4.28%
Liu et al. [17]	2720	99.73%	97.32%	76.19%	25.67%	6.59%
Guo et al. [16]	3744	99.63%	96.33%	68.77%	15.38%	2.37%
IPsec [5]	4736	99.53%	95.37%	62.28%	9.37%	0.88%
Our protocol	2760	99.72%	97.28%	75.88%	25.16%	6.33%

6.4 链路丢包率与握手成功率

卫星网络链路不稳定性体现为数据包丢失的概率. 该参数由物理层误码率、链路层前向纠错能力、网络动态性 (如切换) 及拥塞等多种因素共同决定. 为了量化评估 NTN 链路不稳定性对安全协议连接建立可靠性的影响, 分析链路丢包率对协议的握手成功率的影响. 设参考消息长度为 L_{ref} (本文取 $L_{\text{ref}} = 100$ 字节), 其对应的链路丢包率为 P_{ref} . 假设信道为独立比特错误信道, 且每比特错误概率恒定, 则长度为 L 比特的消息在实际传输中的丢包率为

$$P_{\text{loss}}(L) = 1 - (1 - P_{\text{ref}})^{L/L_{\text{ref}}}.$$

基于无重传的理想模型进行分析, 若协议握手过程包含 M 次顺序依赖的消息交互, 且各消息长度近似相等 (取平均长度 L_{avg}), 则整体握手成功率为

$$P_{\text{handshake}} = [1 - P_{\text{loss}}(L_{\text{avg}})]^M = \left[(1 - P_{\text{ref}})^{L_{\text{avg}}/L_{\text{ref}}} \right]^M = (1 - P_{\text{ref}})^{M \cdot L_{\text{avg}}/L_{\text{ref}}}.$$

由于星地链路受大气衰减、卫星高速运动及频繁切换影响, P_{ref} 呈动态变化. 为评估各个协议的鲁棒性, 我们设定以下典型的 P_{ref} .

- 优质链路: $P_{\text{ref}} = 0.1\%$, 对应无遮挡、非切换期稳定连接.
- 常规链路: $P_{\text{ref}} = 1\%$, 对应轻度干扰或常规运动状态.
- 恶劣链路: $P_{\text{ref}} = 5\%$, 对应频繁切换准备或中度干扰.
- 极限链路: $P_{\text{ref}} = 10\%$, 对应深度衰落、切换期间或强干扰场景.

基于统一信道假设: 数据传输阶段所有协议面临的端到端丢包率相同, 使得吞吐量差异仅来源于协议处理时延和带宽开销的差异, 排除信道质量不一致 (星间链路、星地链路) 的干扰. 根据各个协议的星地交互次数 M , 计算不同丢包率下的握手成功率, 结果如表 9 所示. 随着链路丢包率从 0.1% 提升至 10%, 所有协议的握手成功率均呈显著下降趋势. 在低丢包率场景下, Gautam 等人的方案表现最优, 本协议与 Liu 等人的方案并列第二; 当丢包率提升至 1% 时, 本协议优于 Chang 等人、Guo 等人及 IPsec 协议; 在高丢包率场景下, 本协议的握手成功率接近 Liu 等人的方案, 显著优于 IPsec 等传统协议. 同时, 本协议还具备了密钥确认与良好的可扩展性, 最大化对抗链路不稳定的能力.

6.5 切换恢复时延

在 NTN 的高动态拓扑中, 卫星节点需要频繁地在不同地面信关站或星间链路之间切换, 以维持连续服务. 切换发生后, 安全上下文通常失效, 必须与新接入的节点重新建立认证与密钥协商. 因此, 切换恢复时延 T_{recovery} 是衡量协议适应动态网络能力的关键指标. 在最坏的情况下, 切换目标节点 (如一个新的地面信关站或协作卫星) 与当前节点之间没有预先共享的安全上下文. 因此, 切换恢复过程需要执行一次完整的、端到端的认证与密钥协商流程, 那么 T_{recovery} 在数值上等于安全连接建立时延 T_{total} : $T_{\text{recovery}} = T_{\text{total}}$. 因此, 本协议的切换恢复时延 (19.59 ms) 将显著低于 IPsec (26.24 ms), 这主要是因为其更少的交互轮次和更低的计算开销, 使得在必须重新认证的切换场景下, 能更快恢复安全连接, 减少服务中断时间.

表 9 不同链路丢包率下各协议的握手成功率对比.

Table 9 Comparison of handshake success rate of different protocols under different link packet loss rates.

Protocol	L_{avg} (bits)	$P_{\text{ref}} = 0.1\%$	$P_{\text{ref}} = 1\%$	$P_{\text{ref}} = 5\%$	$P_{\text{ref}} = 10\%$
Gautam et al. [18]	992	99.75%	97.54%	88.06%	77.00%
Chang et al. [20]	788	99.61%	96.12%	81.70%	66.02%
Liu et al. [17]	1360	99.66%	96.64%	84.00%	69.90%
Guo et al. [16]	936	99.53%	95.41%	78.66%	61.08%
IPsec [5]	1184	99.41%	94.22%	73.81%	53.61%
Our protocol	920	99.66%	96.59%	83.78%	69.54%

6.6 吞吐量

在建立安全连接后, 数据传输的稳态吞吐量 Throughput 由可靠传输协议主导, 其长期平均吞吐量可由经典的 Padhye 模型构建 [34]. 其中, 当 P_{ref} 较小且窗口受接收端限制时, 吞吐量可近似表示为

$$\text{Throughput} \approx \frac{\text{MSS} \cdot W_{\text{max}}}{\text{RTT} \cdot \sqrt{P_{\text{ref}}}}.$$

星地往返时延 RTT 主要包括物理传播时延 (2τ) 和单数据包的处理时延 (发送端与接收端的加密/解密、协议栈处理等). 通常情况下, 单包处理时延远小于 LEO 场景的传播时延. 因此, 单包处理时延可被忽略, RTT 近似为 $\text{RTT} \approx 2\tau = 10.00 \text{ ms}$. 此外, 取 $P_{\text{ref}} = 1\%$, 最大传输单元 $\text{MSS} = 1460 \text{ bytes}$, 最大拥塞窗口 $W_{\text{max}} = 10$, 计算可得理论吞吐量 Throughput 约为 2.29 Mbps . 此值为各协议在相同物理条件下的理论上限, 实际吞吐量会因协议额外开销、拥塞控制策略等有所差异.

虽然 NTN 的传播时延 τ 是限制吞吐量的根本瓶颈, 各协议在相同物理层条件下能达到的吞吐量上限相近. 与 IPsec 协议相比, 本协议通过两个方面间接提升有效吞吐量. (1) 更高的握手成功率: 如表 9 所示, 在丢包环境下更可靠的连接建立减少了因握手失败导致的重复尝试和等待时间. (2) 更低的协议开销: 表 4 展示了本协议的带宽开销比 IPsec 低 41.7%, 这意味着在传输相同应用数据时, 本协议消耗的链路容量更少, 从而为数据传输预留更多的带宽.

7 总结展望

本文针对基站上星场景, 分析了星地回传链路在拓扑动态变化、资源受限环境下面临的安全挑战, 并提出一种轻量级的认证与密钥协商方案. 相较于传统 IPsec 等依赖于固定网络假设与复杂证书管理的安全机制, 本方案基于无证书公钥密码体制, 避免了 PKI 的证书管理开销; 同时, 通过对 EDHOC 协议进行适应性优化, 实现了星载基站与地面核心网网关间的高效认证与密钥交换, 并依托 EAP 框架支持底层协议集成. 安全性方面, 通过启发式分析与形式化验证, 证明该方案可抵御多种攻击, 具备较高的安全强度; 性能方面, 从信令、带宽与计算开销 3 个维度评估, 表明其在效率与可扩展性之间取得了良好平衡. 因此, 本方案更能适应 NTN 回传链路高动态、资源受限的特点, 弥补了 IPsec 等传统协议在该场景下的不足. 未来工作将聚焦于 LEO 卫星高动态组网环境中, 针对 IP 地址频繁变更与星间链路切换导致的安全关联重建问题, 研究基于层次化密钥衍生的星间可持续安全机制.

参考文献

- 1 3GPP. Study on new radio (NR) to support non-terrestrial networks. TR 38.811, 2020
- 2 3GPP. Solutions for NR to support non-terrestrial networks (NTN). TR 38.821, 2023
- 3 3GPP. Solutions for NR to support non-terrestrial networks (NTN): non-terrestrial networks (NTN) related RF and coexistence aspects. TR 38.863 V18.0.0, 2023
- 4 3GPP. Study on satellite access Phase 3 (Release 19). TR 22.865 V19.1.0, 2023

- 5 Internet Engineering Task Force (IETF). Internet key exchange protocol version 2 (IKEv2). RFC 7296, 2014
- 6 3GPP. Aspects: network domain security (NDS): IP network layer security (Release 18). TS 33.210 V18.1.0, 2024
- 7 3GPP. Security architecture and procedures for 5G system (Release 19). TS 33.501 V19.0.0, 2024
- 8 Consultative Committee for Space Data Systems (CCSDS). Space communications protocol specification-security protocol (SCPS-SP). CCSDS 713.5-B-1, 2006
- 9 DVB. Second generation DVB interactive satellite system (DVB-RCS2): Part 1: overview and system level specification. DVB Document A155-1, 2019
- 10 ETSI. Digital video broadcasting (DVB); Second generation DVB interactive satellite system (DVB-RCS2); Part 1: overview and system level specification. ETSI TS 101 545-1, 2020
- 11 ETSI. Digital video broadcasting (DVB); Second generation DVB interactive satellite system (DVB-RCS2); Part 4: guidelines for implementation and use of EN 301 545-2. ETSI TR 101 545-4 V1.1.1, 2014
- 12 Zhu H, Wu H, Zhao H Q, et al. Inter-satellite networking authentication scheme for two-layer satellite networks. *J Commun*, 2019, 40: 1–9 [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. *通信学报*, 2019, 40: 1–9]
- 13 Yang Y, Cao J, Ren X, et al. LK-AKA: a lightweight location key-based authentication and key agreement protocol for S2S communication. *Comput Commun*, 2023, 197: 214–229
- 14 Cao J, Shi X P, Ma R H, et al. AKA protocols for satellite-to-ground and inter-satellite in integrated two-layer satellite networks. *Chinese J Netw Inform Secur*, 2023, 9: 18–31 [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. *网络与信息安全学报*, 2023, 9: 18–31]
- 15 Xue K, Meng W, Zhou H, et al. A lightweight and secure group key based handover authentication protocol for the software-defined space information network. *IEEE Trans Wireless Commun*, 2020, 19: 3673–3684
- 16 Guo J, Du Y, Zhang Y, et al. A provably secure ECC-based access and handover authentication protocol for space information networks. *J Netw Comput Appl*, 2021, 193: 103183
- 17 Liu Y, Ni L, Peng M. A secure and efficient authentication protocol for satellite-terrestrial networks. *IEEE Int Things J*, 2023, 10: 5810–5822
- 18 Gautam D, Kanwar S, Prajapat S, et al. A robust ECC based authentication protocol for satellite-to-satellite communication network. *Telecommun Syst*, 2024, 87: 541–559
- 19 Ren S, Liu J, Ji R, et al. A secure authentication scheme for satellite-terrestrial networks. *IEEE Trans Netw Sci Eng*, 2024, 11: 6470–6482
- 20 Guo J, Yao S, Song Y, et al. N3PA-STIN: a novel three-party authentication protocol for multiuser access in satellite terrestrial integrated networks. *IEEE Int Things J*, 2025, 12: 14952–14968
- 21 Abdrabou M, Gulliver T A. Authentication for satellite communication systems using physical characteristics. *IEEE Open J Veh Technol*, 2022, 4: 48–60
- 22 Soni M, Singh D K. Blockchain-based group authentication scheme for 6G communication network. *Phys Commun*, 2023, 57: 102005
- 23 Chen T M, Zhang J, Leng C, et al. Design and verification of security communication mechanism for satellite network system based on blockchain. *Aerospace Shanghai*, 2024, 41: 88–105 [陈韬鸣, 张健, 冷超, 等. 基于区块链的卫星网络系统安全通信机制设计与验证. *上海航天*, 2024, 41: 88–105]
- 24 Yan R, Jia F. A multi-feature fusion approach for physical layer authentication in LEO satellites. *Comput Commun*, 2025, 242: 108308
- 25 Ramesh J V N, Nimma D, Dasari R, et al. Satellite IoT terminal authentication mechanism for enhancing consumer security over cyber-physical systems. *IEEE Trans Consumer Electron*, 2025, 71: 4771–4779
- 26 Li J, Xue K, Liu J, et al. An ICN/SDN-based network architecture and efficient content retrieval for future satellite-terrestrial integrated networks. *IEEE Netw*, 2019, 34: 188–195
- 27 Jiang C, Wang X, Wang J, et al. Security in space information networks. *IEEE Commun Mag*, 2015, 53: 82–88
- 28 Bi Y, Han G, Xu S, et al. Software defined space-terrestrial integrated networks: architecture, challenges, and solutions. *IEEE Netw*, 2019, 33: 22–28
- 29 He D, Li X, Chan S, et al. Security analysis of a space-based wireless network. *IEEE Netw*, 2019, 33: 36–43
- 30 Selander G, Mattsson J P, Palombini F. EDHOC: ephemeral Diffie-Hellman over COSE. RFC 9528, 2024
- 31 Li G, Luan T H, Lai C, et al. DTHA: a digital twin-assisted handover authentication scheme for 5G and beyond. *IEEE Trans Dependable Secure Comput*, 2025, 22: 6422–6440
- 32 Cremers C J F. The Scyther tool: verification, falsification, and analysis of security protocols: tool paper. In: *Proceedings of the International Conference on Computer Aided Verification*, 2008. 414–418
- 33 Barker E. Recommendation for key management: Part 1—general. NIST SP 800-57 Part 1, 2020
- 34 Padhye J, Firoiu V, Towsley D, et al. Modeling TCP throughput: a simple model and its empirical validation. In: *Proceedings of the ACM SIGCOMM'98 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, 1998

附录 A

EDHOC-NTN 采用了以 CL-PKC 为密码基础、增强 EDHOC 协议, 实现 NTN 场景下的回传链路安全. 从 $message_2$ 开始对消息进行加密保护, 涉及到的输入、函数、输出可参考 RFC9528, 其中 (G_{BX}) 和 (G_{AY}) 是使用临时 DH 参数和静态公钥计算结果, 密钥衍生如图 A1 所示.

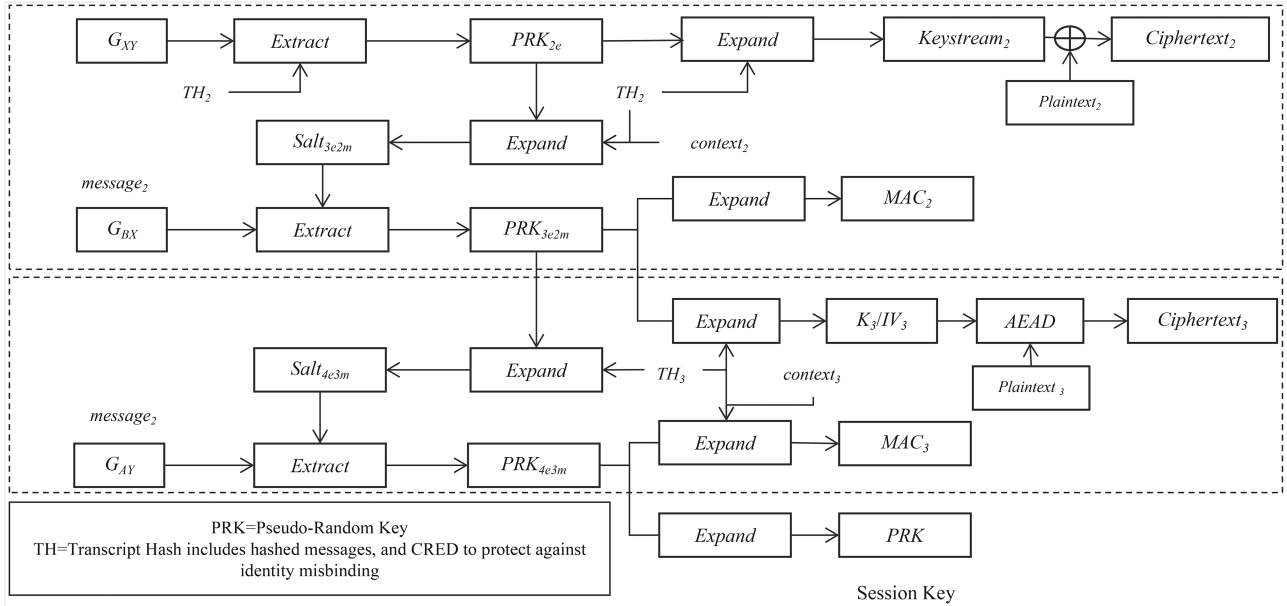


图 A1 密钥衍生流程图.

Figure A1 Key derivation flowchart.

EDHOC-NTN: a lightweight authentication and satellite-terrestrial integrated backhaul security protocol design based on CL-PKC

Meiling CHEN^{1*}, Jin CAO², Yuanyuan YANG², Haitao DU¹, Lingling SUN¹, Xiaoting HUANG¹ & Li SU¹

1. China Mobile Research Institute, Beijing 100053, China

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

* Corresponding author. E-mail: chenmeiling@chinamobile.com

Abstract The 3GPP-standardized non-terrestrial network (NTN) serves as a critical enabler for 6G integrated space-air-ground architectures, providing global coverage, low-latency connectivity, and multi-scenario adaptability through satellite-based base stations. However, due to the characteristics of intermittent connectivity, high propagation delay, and dynamic changes in network topology of the NTN satellite-ground backhaul links, the current Internet protocol security (IPSec) solution adopted by 3GPP terrestrial networks, which has defected such as multiple interaction rounds, high latency, and severe reliance on IP addresses for identity authentication, is not suitable for the current satellite high-speed mobile scenarios. To address this issue, this paper introduces EDHOC-NTN, a key exchange and authentication protocol that integrates certificateless public-key cryptography (CL-PKC) with the lightweight authenticated key agreement protocol EDHOC (ephemeral Diffie-Hellman over COSE). Our proposed protocol, while ensuring the security of the return link, achieves the integration of low overhead, low latency and strong security. Heuristic analysis and formal security verification confirm that the protocol resists replay, man-in-the-middle, and impersonation attacks. Performance evaluation and simulation results show that our proposed protocol can save 41.7% of the bandwidth consumption and 26.4% of the computing cost compared to the standard IPSec protocol, making it more suitable for resource-constrained satellite-ground integrated network environments.

Keywords NTN, backhaul security, EDHOC, security authentication, base station onboard satellite