面向6G的天地一体化网络安全技术

Network Security Technology for Space-Ground Integrated Networks Towards 6G

陆海涛/LU Haitao[1,2]，周强/ZHOU Qiang[1]，
代九龙/DAI Jiulong[1,2]，卢帆/LU Fan[1]，李锐/LI Rui[1,2]
（1. 中兴通讯股份有限公司，中国 深圳 518057；
2. 深圳市5G接入网安全技术研究及应用重点实验室，中国 深圳 518055）
(1. ZTE Corporation, Shenzhen 518057, China;
2. Shenzhen Key Laboratory of 5G RAN Security Technology Research and Application, Shenzhen 518055, China)

DOI：10.12142/ZTETJ.202506011
网络出版地址：https://link.cnki.net/urlid/34.1228.TN.20240912.1755.002
网络出版日期：2024-09-13
收稿日期：2024-03-25

摘要：天地一体化是6G的基本组网架构，现有网络安全技术已不再适用新的安全风险与场景要求。分析了天地一体化网络广覆盖、海量接入、低时延、大带宽通信场景的安全需求。针对天地一体化网络面临的网络拓扑动态变化和卫星平台资源受限的挑战，重点分析了接入认证、星地回传安全传输、星间链路安全传输、轻量化的无线物理层安全、抗量子密码，以及量子保密通信和基于区块链的星地可信联盟等网络安全技术。认为未来有必要研究轻量化的接入认证、星地可信联盟等新技术，以解决当前天地一体化网络的安全与资源矛盾。

关键词：星载基站；星地协同；动态拓扑；轻量化；量子通信

Abstract: The Space-Ground Integrated Network is the fundamental networking architecture for 6G, and existing cybersecurity technologies are no longer adequate to address the new security risks and meet the scenario requirements. This paper analyzes the security requirements for the wide coverage, massive access, low latency, and large bandwidth communication scenarios of the Space-Ground Integrated Networks, and focuses on network security technologies such as access authentication, satellite-ground backhaul security transmission, inter-satellite link security transmission, lightweight wireless physical layer security, quantum-resistant cryptography and quantum secure communication, and blockchain-based satellite-ground trusted alliance. It is believed that future research should prioritize the development of new technologies like lightweight access authentication and satellite-ground trusted alliances to resolve the conflict between security and resource constraints in the Space-Ground Integrated Networks.

Keywords: satellite base station; satellite-ground collaboration; dynamic topology; lightweight; quantum communication

引用格式：陆海涛，周强，代九龙，等．面向6G的天地一体化网络安全技术 [J]. 中兴通讯技术，2025, 31(6): 75-83. DOI: 10.12142/ZTETJ.202506011
Citation：LU H T, ZHOU Q, DAI J L, et al. Network security technology for space-ground integrated networks towards 6G [J]. ZTE technology journal, 2025, 31(6): 75-83. DOI: 10.12142/ZTETJ.202506011

经过“十三五”以来的建设，中国已建成全球最大规模5G网络。截至2024年6月30日，中国累计建成5G基站383.7万座，占全球比例超过60%，下一步将统筹推进并加快信息通信业的高质量发展。“十四五”规划和2035年远景目标提出要建设高速泛在、天地一体、集成互联和安全高效的信息基础设施。天地一体是指将卫星通信网络作为地面通信网络的重要补充与延伸，通过深度融合天基与地基网络资源，构建一个覆盖全球、无处不在、高速智能和安全可靠的通信网络[1-4]。非地面网络（NTN）是天地融合通信的主流技术，第3代合作伙伴计划（3GPP）最早从R15阶段就开展了NTN技术研究和标准化工作，定义了NTN部署场景和相关网络架构；在R16阶段开展了NTN系统性解决方案的技术研究；在R17阶段基于NTN透明载荷的网络架构，针对卫星通信场景的多普勒频偏较大、通信端到端时延较大以及长距离传输带来的信号大幅度衰减等问题，设计了空口增

基金项目：广东省重点领域研发计划项目（2020B0101120003）

强协议，引入了多种增强技术；在R18阶段以针对NR NTN的增强功能、进一步完善5G卫星组网能力为目标，主要包括支持10 GHz以上频段部署、覆盖增强、移动性和服务连续性增强，以及星上本地数据交换技术[5]。2023年12月开始的R19阶段进一步增强NTN卫星通信网络能力，重点支持全基站上星的再生架构，扩展应用场景，开展下行覆盖增强、上行容量/吞吐量增强研究；R20及后续阶段将结合5G NTN遗留问题，针对多频段管理、高低轨卫星协同、核心网能力增强以及星地频谱共享等方面开展进一步研究。

3GPP R20已于2025年启动，将重点推进6G及其架构的初步研究。R21预计在2026年启动，将成为首个全球6G标准规范。与5G相比，6G网络需要应对超高速率、超低时延、超大规模连接等场景带来的新安全挑战。尤其是天地一体化网络引入的新安全风险与场景要求，现有网络安全技术不完全适用，这将极大影响6G网络研究与标准进程。因此，开展天地一体化网络安全技术研究十分必要。

本文首先介绍天地一体化网络架构的透明转发和可再生两种模式，然后分析天地一体化网络的广覆盖、海量接入、低时延、大带宽通信场景的安全需求，最后针对天地一体化网络面临的网络拓扑动态变化和卫星平台资源受限的挑战，分析接入认证、星地回传安全传输、星间链路安全传输、轻量化无线物理层安全、抗量子密码，以及量子保密通信和基于区块链的星地可信联盟等网络安全技术。

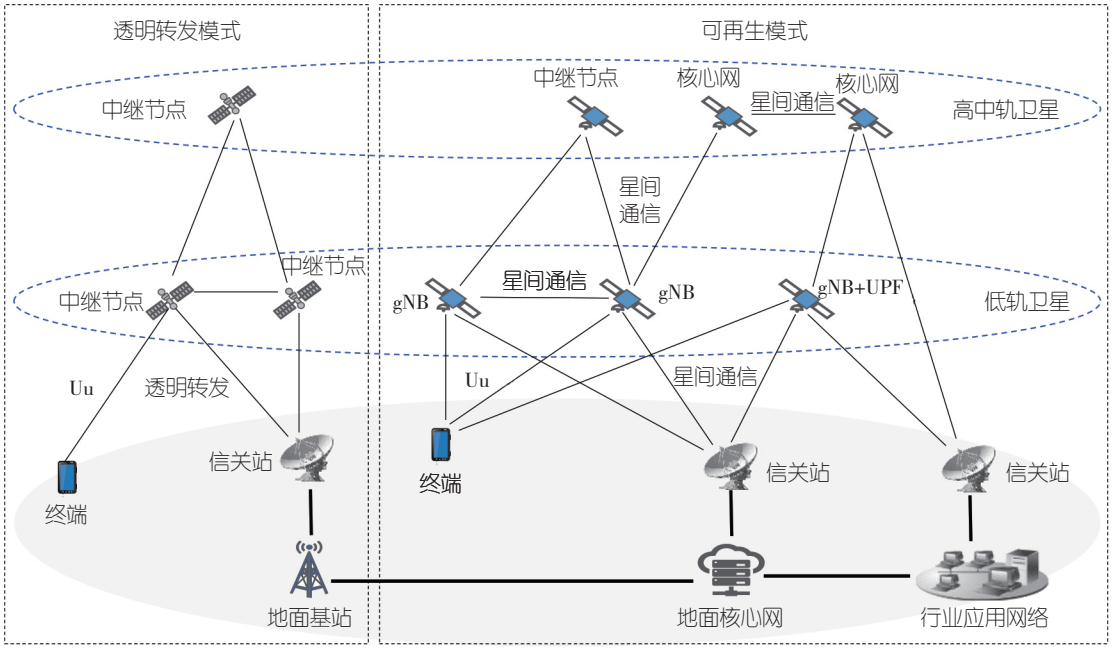
1 天地一体化网络架构

天地一体化是指天基和地基网络单元能无缝协同工作，为用户提供连续覆盖和无感知的超高速、超低时延和超大规模连接性能。天地一体化网络由用户段、地面段和空间段组成。其中，用户段包括手机、车载和船载传感器、无人机通信模块、物联网终端等设备；地面段由地面基站和核心网组成，可实现地面网络通信；空间段由高中低轨卫星组成，根据承载设备类型可分为中继卫星、星载基站和星载核心网，构成天基网络，与地面网络协同工作，实现天地一体化通信。

天地一体化网络根据工作模式可分为透明转发模式和可再生模式，如图1所示。

透明转发模式：卫星被作为中继节点，透明转发终端和地面基站之间的射频信号，适用于海洋、沙漠、山地等地面网络难以覆盖的场景，可作为地面网络的覆盖补盲，提供通信连接和连续业务服务。其缺点是空口时延较大，难以支持高速率业务，且覆盖范围高度依赖于地面信关站的部署，不利于实现全球广域覆盖。

可再生模式：将地面网络的部分或全部网元部署于卫星上，相当于实现地面通信网的立体化，形成星地协同与高中低轨协同的天地一体化网络架构。根据星载网元的部署方



gNB：新一代网络的基站节点　UPF：用户面功能　Uu：用户空口

图1　天地一体化组网架构

式，可再生网络主要可分为3种组网形式。

1）星载基站+地面核心网：基站上星部署，卫星提供接入网功能。星载基站通过3GPP用户空口（Uu）连接地面终端，同时星地回传通过卫星馈线链路连接地面信关站和地面核心网，支持3GPP下一代接口（NG）。星载基站部署在低轨卫星，离地高度一般为150～2 000 km，绕地球一圈只需1.5～2 h。因此，星载基站的切换一直在持续进行。除了星载基站与终端之间的切换外，星载基站与地面信关站和核心网的网络拓扑也一直在动态变化。此外，星载基站是多颗部署，星载基站之间星间链路通过激光通信承载3GPP基站互联接口（Xn）来进行互联。如果星载基站的轨道高度相同，则星载基站之间的相对位置无变化，网络拓扑可以保持相对稳定；如果星载基站的轨道高度不同，则星载基站之间的相对位置将持续变化，网络拓扑也会一直变化。

2）星载基站+用户面功能（UPF）+地面核心网：除了基站上星部署，核心网的数据处理单元UPF也可以下沉并和基站一起部署在卫星上，以减少传输时延，实现低时延和大带宽的数据处理，支持本地数据分流，缓解核心网的数据传输压力。

3）星载基站+星载核心网：基站与核心网同时上星部署，并且分布在不同轨道的卫星上。星载基站部署在低轨卫星，支持低时延和大带宽数据处理。星载核心网部署在高轨卫星，最大价值是实现全球覆盖的应急网络，其卫星轨道高度约36 000 km，保持与地面相对静止。理论上，3个星载核心网即可实现全球覆盖，这对于中国“一带一路”的通信保障具有非常重要的意义。星载基站与星载核心网之间的星间链路通过激光通信承载3GPP NG接口来进行互联。由于星载基站的相对位置在不断变化，星载基站与星载核心网的网络拓扑也一直在动态变化。此外，星载基站和星载核心网通过地面信关站与地面核心网和应用网络连接，支持星地协同，实现天地一体化的统一网络。

上述是可再生网络的几个基本组网形式，未来天地一体化网络的实际部署可能更复杂。例如，星载基站可划分为分布式单元（DU）和集中单元（CU），二者分别部署在不同的卫星上，甚至不同的轨道平面中。其中，星载DU支持更高效的数据处理，星载CU支持云化的卫星互联网。而星载核心网包含接入和移动管理功能（AMF）、会话管理功能（SMF）、策略控制功能（PCF）、统一数据管理功能（UDM）、认证服务器功能（AUSF）、UPF和边缘计算云平台（MEC）等网络功能，需要考虑哪些网络功能上星，哪些保持在地面。

可再生模式是6G天地一体化网络的主要网络架构，具有低时延、高带宽、广覆盖和灵活组网的特点。但相比于地面网络，网络安全面临的主要挑战有两点：一是网络拓扑一直在动态变化，需要持续地对终端和网元进行身份认证和连接控制；二是卫星平台资源受限，星载基站和星载核心网难以部署与地面网络相同的全面功能，部分功能需要进行裁剪，传统的安全技术和协议可能不适用于星上部署，因此需要考虑轻量化的安全技术和协议。对于天地一体化网络面临的安全挑战，接下来将分析具体的安全需求和安全技术。

2 天地一体化网络安全需求分析

天地一体化网络透明转发模式的网络结构比较单一，其更多是作为一种过渡性方案。未来6G天地一体化网络将以可再生模式为主，因此接下来的安全分析将基于该模式开展，将主要结合天地一体化网络的特征和场景进行安全需求分析。

天地一体化广覆盖场景安全需求：6G将融合地面基站、地面核心网、地面信关站、高中低轨星载基站、星载核心网及中继卫星等各类网络节点与设施，实现天地网络融合及全球无缝覆盖。由于卫星网络节点位置在不断变化，因此网络拓扑结构也在持续动态变化，需要保障网络拓扑变化过程中网络节点的身份认证，以及终端接入网络时的身份认证，同时，在多运营商融合组网场景下，还需要满足多方身份互信的需求。

天地一体化海量接入场景安全需求：6G天地一体化网络覆盖广，连接终端数量多，尤其是卫星物联网场景的海量终端接入，需要考虑星载基站和核心网设备对认证消息的处理能力，以支撑轻量化的认证技术。这包括简化认证流程、支持分组认证，同时需要研究支持无线物理层认证等新认证技术。在保证安全性的基础上，这些技术既可以满足海量接入认证需求，又可以降低资源占用与成本开销。在智能家居、智慧城市等领域，天地一体化网络需要连接大量的设备和传感器。这些设备和传感器需要进行身份验证和授权管理，以确保它们只能访问其被授权的数据和服务。

天地一体化低时延、大带宽通信场景安全需求：6G天地一体化网络受卫星轨道高度、频谱资源等因素的限制，难以提供低时延的服务，需要考虑简化接入协议来降低通信时延，包括采用多用户共享接入（MUSA）技术。因此，身份认证需要支撑简化接入信令交互流程时的认证机制，满足单条信令即可实现的用户认证鉴权需求。例如，在金融交易、实时通信等领域，快速的身份验证和授权管理是必不可少的。此外，6G通过采用更大规模天线、更大带宽等新空口技术，大幅提升了空口传输速率。而传统基于计算复杂度的数据加解密技术可能存在性能瓶颈，需要引入轻量化的数据加解密技术，基于安全和通信的深度融合，在保障安全性的

同时，提高系统的传输性能，满足6G网络高效的数据安全传输和高安全服务需求。

此外，天地一体化网络是多层次、立体化的网络架构，终端与网络之间的距离长且都处于开放的天空，更容易受到信号干扰、数据窃听和数据篡改攻击，因此需要研究星地空口安全保护方案，保障数据的机密性和和信令的完整性，抵御星地空口分布式拒绝服务（DDoS）攻击和信号干扰攻击。天地一体化网络是全球覆盖的网络，由于外太空间全球开放，不同国家和不同运营商都可以部署星载通信节点，因此也面临着对星载设备的干扰、窃听与篡改威胁，需要探索伪星载基站探测和防御安全方案，研究抵御UE降级攻击、Xn切换降级攻击、射频干扰攻击、指纹分析攻击及位置追踪攻击等网络安全技术。

3 天地一体化网络的安全技术分析

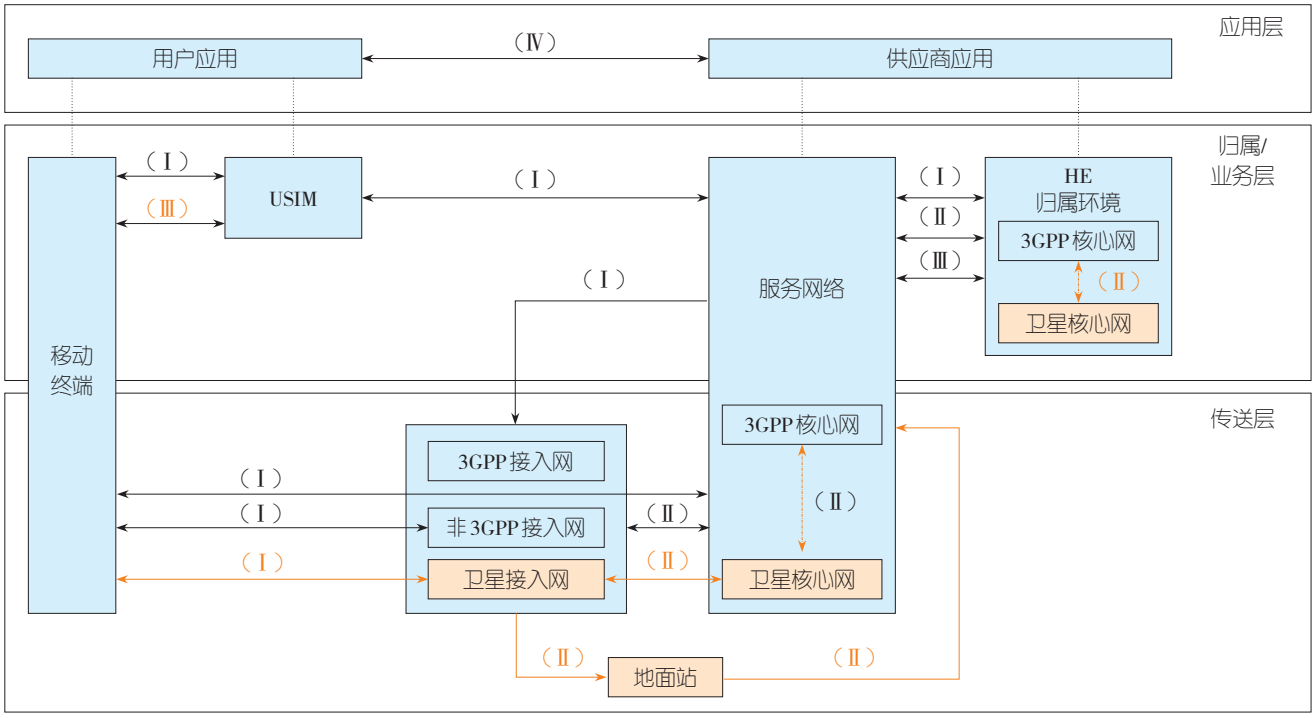
目前业界对6G网络安全技术已有不少分析，普遍共识是传统“外挂式”“补丁式”的安全机制将向6G内生安全方向演进。IMT-2030（6G）推进组把内生安全列为6G潜在的十大关键技术之一，同时定义了内生安全的主动免疫、弹性自治、虚拟共生和泛在协同四大特征[6]。文献[7]指出，轻量化也是6G内生安全的主要特征之一，传统的接入安全技术无法满足海量设备连接和实时传输需求，需要引入轻量化的安全机制。针对6G天地一体化网络面临的网络拓扑动态变化和卫星平台资源受限的挑战，本文将重点分析以下网络安全技术。

文献[8]基于3GPP 5G安全域模型[9]，将6G网络的安全新需求融入，尤其是天地一体化网络的安全需求，并提出6G网络的安全域模型，如图2所示。

相比于5G，6G网络安全域模型的最大特征是融入了卫星网络，新增了卫星接入网、卫星核心网和地面站等网元，在接入域、网络域和用户域进行安全增强。这主要涉及接入认证、星地回传安全传输、星间链路安全传输、轻量化物理层安全、抗量子密码迁移和区块链应用等网络安全技术。

1） 接入认证技术

天地一体化网络的星载通信节点位置在持续动态变化，并且处于开放的长距离空间环境中，更容易面临仿冒和劫持攻击风险，对此，系统首先需提供双向认证机制，基于共享秘钥以及多层级密钥推演机制，保证终端接入网络的身份合法，以及被接入的网络的合法性。其次，对于行业专网应用，提供对接入企业专网的终端进行二次认证——该认证基于3GPP标准定义的二次认证，同时提供更细粒度终端访问控制



3GPP：第3代合作伙伴计划　HE：归属环境　USIM：全球用户识别卡

图2　6G网络的安全域模型

（包括根据终端位置、机卡一致性、终端属性等多因素进行安全认证），以满足垂直行业业务对安全保密的更高要求。另外，对于快速移动的星载基站引起的切换场景，需提供安全的移动性管理；涉及密钥变更等过程时，要保持安全上下文和承载上下文的连续性。同时，为保证天地一体化网络的高可用性，建议提供星载基站的孤站自治功能：如果与天基核心网或地面核心网的链路断开，星载基站将启动断链保持模式，确保存量终端的正常业务和认证不受影响，同时支持新用户的接入认证，最终实现业务不中断、安全不失效。

由于天地一体化网络覆盖广且通信距离长，网络中存在海量终端的随机接入，因此面临着并发认证数多和认证链路长的风险。而星载通信节点受限于硬件资源条件，相比于地面网元更容易引起认证阻塞，因此需要研究提供轻量化的认证技术。具体包括两个方面：一是支持分组认证来降低并发认证数量，例如将同一区域或相同用户的物联网感应器标识为一终端群组，进行统一接入认证；当终端群组的一个用户通过接入认证，则该群组的所有用户都默认获得接入许可；反之，若一个用户被取消了接入许可，则该群组的所有用户都被禁止接入网络[10]。二是简化认证协议流程以缩短认证链路长度，通过一条信令即可完成接入和认证。例如，对第一条接入消息直接进行安全保护，这种方式可以保护海量终端的空口接入消息，防止攻击者窃听和篡改消息；同时用户标识（ID）也进行加密随消息发送，使得网络可以认证终端的合法性，防止非法终端连接网络[10]。

此外，数字身份技术基于身份与访问控制、生物特征识别、机器学习模型等技术，来增强访问安全和数据隐私，在未来天地一体化网络接入场景中，能够使用户和服务提供者之间建立起更加可靠的数字信任关系。具体方式包括：扩展现有手机用户识别卡（SIM）作为数字身份的认证基础，逐步增加安全芯片、数字证书、国家算法等能力，完善认证/核验平台、卡端接入平台及业务合作平台，集成面向个人、企业、政府的多场景应用，搭建并完善可信数字身份体系[11]。在天地一体化网络应用场景中，需要处理大量的设备和传感器。这些设备和传感器使用数字身份技术进行身份验证和授权管理，通过为每个设备分配一个唯一的数字身份，实现设备的权限和访问级别的管理与控制。

2） 星地回传安全传输技术

星地协同是6G天地一体化网络的一个主要特征，它使用统一的网络架构和标准体制，一体化的无线接入、传输和网络技术，以及一体化的星地协同无线资源分配与业务管理机制，为用户提供全域覆盖，满足用户随时随地的通信需求[12]。星地回传技术是星地协同的关键技术，它能够使星载基站的数据通过馈线链路传输至地面信关站，再由信关站转发至地面核心网和网管系统。星地回传具有4个突出特点：一是星载基站与地面信关站之间进行单点通信；二是通信数据量大，满足基站与核心网间NG接口的回传数据带宽要求；三是通信距离远、高速移动；四是要根据卫星运动轨迹，保证回传链路在不同信关站间的实时切换。

星地回传主要用于实现星载基站与地面核心网的NG接口连接。与地面NG接口有线传输相比，星地回传增加了星地馈线链路的无线传输。现有地面NG接口使用互联网安全协议（IPSec）来保护NG接口安全，因此星地回传的安全传输也以IPSec协议为主，具体分为基站IPSec和信关站IPSec两种方式。

基站IPSec是指星载基站从信关站动态获得公网IP，并与地面核心网安全网关建立IPSec隧道的安全传输方式，如图3所示。由于星载基站在持续高速移动，需根据其运动轨迹来切换信关站，此时星载基站需要重新获取公网IP并建立IPSec隧道。

信关站IPSec是指地面多个信关站通过公网与运营商核心网连接，并建立多条IPSec隧道，以此屏蔽信关站之间的差异，如图4所示。星载基站分配运营商内网IP，通过卫星平台提供的馈线链路通道连接信关站，然后信关站通过IPSec隧道转发星载基站数据。同时，馈线链路作为空间无线

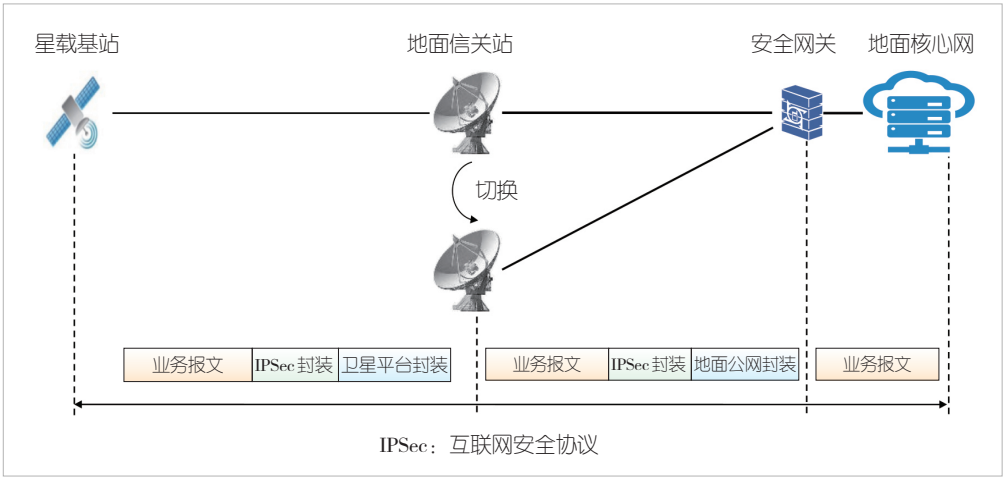


图3 基站IPSec星地回传安全传输

链路，增强了空口安全防护机制，以抵御空口干扰、窃听、伪造劫持等攻击。

3）星间链路安全传输技术

天地一体化网络中的星间链路是星载基站、星载核心网、中高轨中继卫星之间的通信链路。它将多颗卫星互联，实现卫星间高速传输和交换，形成一个以卫星为交换节点的空间通信网络，并支持3GPP NG/Xn接口连接。星间链路的引入，使低轨卫星移动通信系统能够更少地依赖地面网络，更为灵活地进行路由选择和网络管理，从而有助于减少地面信关站数量，降低部署复杂度和成本。

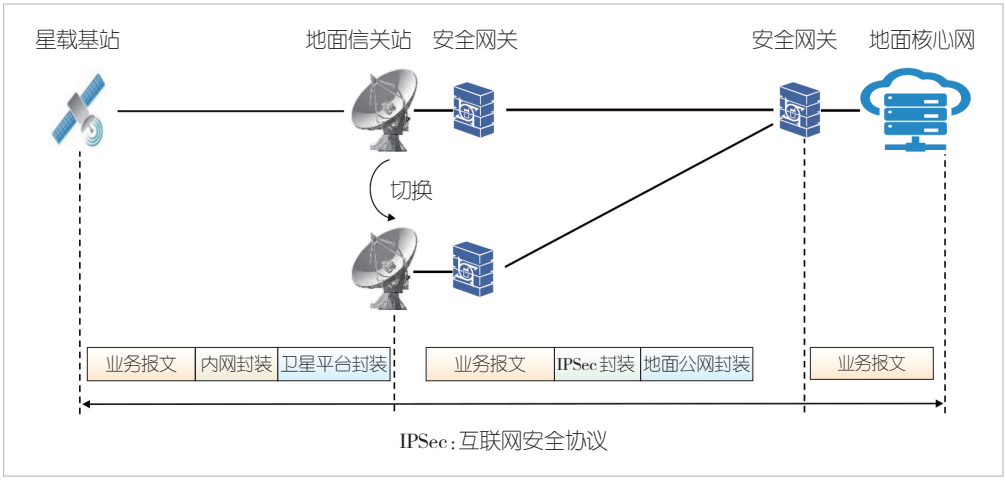


图4 信关站IPSec星地回传安全传输

激光通信技术应用于星间链路传输，相比微波通信有很大优势：首先是通信速率高，可不受无线频谱限制，传输速率可达到100 Gbit/s以上；同时还有抗干扰能力强、保密性好、设备轻量化及功耗低的优点。其缺点是异轨激光通信相对同轨通信，存在卫星相对移动速度快、对准难度高的问题。因此需要提供同轨与异轨场景下的高效连接管理机制，针对高轨核心网与低轨基站的NG接口连接，以及分布在低轨不同层次的星载基站之间的Xn口连接，支持根据网络拓扑变化实时调整激光对准精度。

此外，网元还可能部署在同一颗卫星或不同卫星上。例如，星载基站采用CU/DU分离部署、UPF下沉星载基站部署等。当这些网元位于不同卫星时，需为网元之间提供安全保障，包括网元间的信任关系建立和通信安全防护。

4）轻量化无线物理层安全技术

在天地一体化网络中，由于庞大的星载基站处于持续高速移动状态，空口信道特征呈现高度动态变化，具有较强的随机性和时变性。这为以信道特征为基础的无线物理层安全（PLS）技术提供了应用优势。PLS技术以信道状态、信号强度、功率谱密度、信道冲激响应和方向角等信道属性为内生安全因子，形成信道指纹，是一种利用合法通信双方的信道的唯一性和互易性实现安全保护的内生安全机制；而传统安全机制则基于高层密钥协商和计算复杂度加解密算法实现。由于无线物理层安全机制大幅减少甚至没有高层信令交互，因此可降低信令处理时延和计算复杂度，支持更多用户终端和接入，并降低系统计算资源消耗，是比较理想的轻量化安全技术。此外，基于信道指纹的时变性可以实现接近“一次一密”的安全效果，理论上是最安全的密码技术，有望成为抵抗量子攻击的候选关键技术。

除信道指纹外，无线物理层安全技术还可以辅助利用3类内生安全属性以进一步增强安全机制：一是基于发射机部件容差和工艺条件差异等形成的唯一射频指纹；二是基于天线制造公差产生的波束图形中不同的波束指纹；三是基于智能超表面（RIS）反射系数矩阵控制多径信号相移与幅度产生的相移指纹。

在天地一体化网络场景中，可以使用信道指纹和射频指纹进行轻量化无线物理层接入的身份检测和认证。网络侧利用信道互易性核对终端信道指纹后，即可判定终端的合法性，无需传统的交互认证协议。文献[13]提出了一种基于信道指纹的身份欺骗攻击检测方案，将波束域特性作为一种信道指纹，并将欺骗攻击中的身份检测问题建模成对其信道指纹的二分类问题，同时选用基于监督学习的支持向量机（SVM）算法。这种方案具有较高的认证准确率，对于不同频率、天线数量、移动速度（低速）的具有较好的鲁棒性。仿真结果表明，即使终端移动速度仅为5 m/s，所提方案仍可以保持95%的认证准确率[13]。

无线物理层安全技术也可以对抗空口信号窃听，实现无密钥安全防护。物理层安全预编码利用信道特征设计预编码矩阵，包括波束成形、人工噪声以及天线子集选择等。波束成形通过设计预编码矩阵调节发射天线阵列或其子阵列，将发送信号的能量集中到合法用户方向，以提高合法用户的信道条件，从而增强接收信号质量。人工噪声利用无线信道以及噪声内在的随机性，使得合法用户的信道质量优于窃听者信道，以保证合法用户的信噪比高于窃听者，从而达到安全传输的目的。天线子集选择在保证合法用户正常接收信号的同时，扰乱窃听者星座图，使窃听者无法准确解调信号[14]。

5） 抗量子密码及量子保密通信技术

随着量子技术的飞速发展，传统基于计算复杂度的密码算法及系统的安全性面临被量子计算破解的威胁。虽然对称密码可以通过增加密钥长度来抵抗量子攻击，但非对称密码如RSA（Rivest–Shamir–Adleman）、椭圆曲线密码（ECC）算法基于大数分解和离散对数的数学问题，正面临着量子计算的本质威胁。1994年SHOR等提出了分解大整数和求解离散对数的量子算法[15]，使得RSA、ECC密码算法可能被破解。未来，如果量子计算获得成功，则目前广泛使用的基于RSA、ECC密码的公钥体系可能不再安全，因此抗量子密码技术也是6G网络安全研究的关键技术。美国国家标准与技术研究所（NIST）在2023年8月发布了抗量子密码学的初始公开标准草案，包括基于有结构格的公钥加密/密钥封装算法Crystals–Kyber[16]、基于有结构化格的公钥签名算法Crystals–Dilithium[17]和基于哈希的公钥签名SPHINCS+[18]。此外，在NIST抗量子密码标准化项目中，中国学者主导并参与提交了多个后量子密码算法。其中，由中科院信息工程研究所路献辉教授团队设计的基于格的加解密（LAC）算法进入了第二轮[19]。

一直以来，中国在量子保密通信领域领跑世界。2023年8月工业和信息化部发布了《基于IPSec协议的量子保密通信应用设备技术规范》[20]等3项量子保密通信相关的通信行业标准，对量子保密通信产品设计和安全测评提供了权威指导，推动了有关设备产品的安全应用。

本文提出一种应用于天地一体化网络的量子保密通信技术方案，如图5所示。该方案通过量子加解密密钥与IPSec协议融合，提供天地一体化网络加解密安全服务。在星载基站与地面核心网NG接口处IPSec加解密通道的基础上，引入量子密钥后，星载基站和地面安全网关分别连接量子密钥系统，获得定期稳定的量子密钥，并通过“量子卫星+量子站”链路的密钥分发系统与量子密钥保持同步。该方案同时可以对IPSec协议进行改造，在密钥协商第一阶段增加量子加密服务协商通知载荷，实现量子加密服务的协商、密钥属性的交换和密钥获取结果的通知；在第二阶段改造使用量子密钥对原始会话密钥进行摘要或异或运算，生成最终的会话密钥。这种方案对IPSec协议改动较少，遵循标准规范，有利于商用推广，但缺点是量子密钥只作为密钥参数，不能直接使用量子密钥作为加密密钥。另一种方案是不启用IPSec密钥协商流程，而是直接使用量子密钥作为IPSec的加密密钥。该方式极大简化了IPSec协议流程，有利于实现轻量化的安全协议，提高系统性能和并发能力，但缺点是对IPSec协议改造很大，还未实现标准化，商用推广比较困难。

6） 星地可信联盟的区块链技术

天地一体化网络提供空、天、地、海全域泛在覆盖和海量用户连接，实现全球服务、应急服务和通导遥一体化服务，是中国“一带一路”的战略性基础设施。星地可信联盟网络满足全球卫星星座统一运营和各国地面运营商自治运营的需求，提供适配各国家政策法规和卫星/地面行业生态圈的安全可信与经济适用的泛在连接基础设施，由星载通信网的空间段和各国家地面通信网的地面段组成，如图6所示。

星地可信联盟是星载通信网和各国家地面通信网（基站+核心网）共同建立的联盟网络。这种网络通过星地馈线链路建立联盟连接，基于区块链分布式账本构建的共建式共识信任安全和交易框架，将空间星载通信网和各国家地面网共同纳入联盟安全可信体系，满足多方身份互信、各种资源

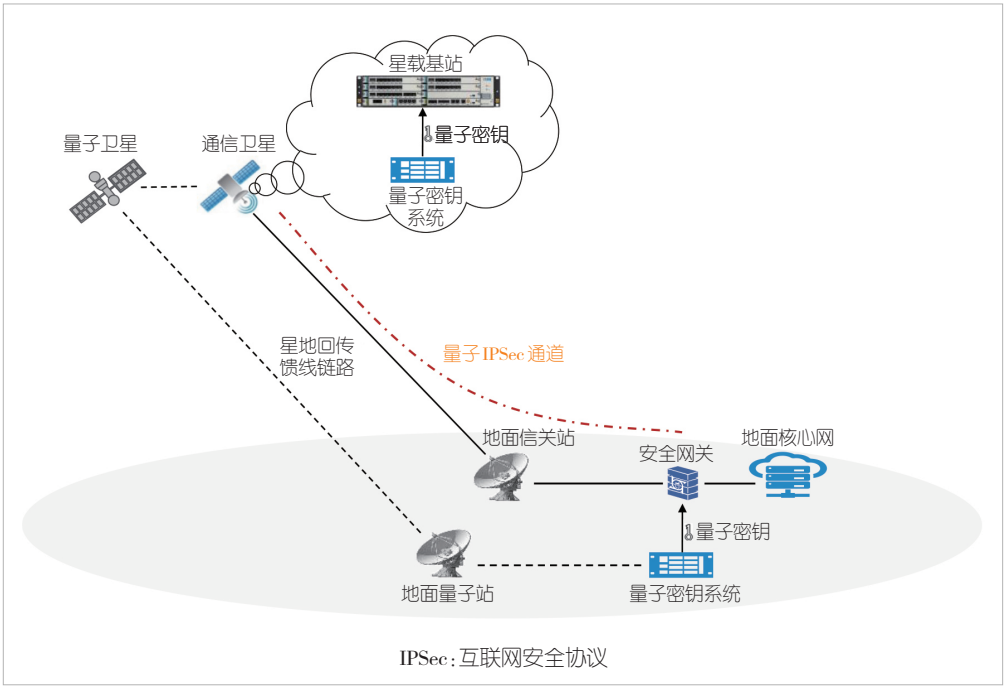


图5 天地一体化网络的量子保密通信技术方案

上链服务和价值兑现的需求，激活用户、行业和区域的参与度，打造商业模式创新平台。

区块链技术的一个突出特点是去中心化，即没有单一的实体可以控制联盟网络，联盟链上的每个节点都可以自主地维护自身的数据，能够有效避免中心化的安全漏洞。同时，所有传输数据都被加密并被添加到对应的区块中。每个区块都包含前一个区块的哈希值，形成了一个链式结构，其中每个节点都可以查看和验证数据。由于每个区块都依赖前一个区块的数据，因此要想篡改其中一个区块，就需要同时修改所有后续区块，这样可有效防止数据篡改和欺诈行为。区块链技术使用加密算法来保护数据的安全，只有授权用户才能解密和查看数据，防止数据窃取和篡改。

区块链的智能合约用于执行预定义的规则和条件，并在满足特定条件时自动执行，可以有效减少人为因素对网络的影响，提高网络的安全性和可靠性。例如，当有新的卫星节点请求加入联盟网络时，智能合约会发起共识请求对卫星节点身份进行认证，联盟网络中所有节点达成共识后，会更新数据层区块链的链上数据，最后才允许新节点加入联盟网络。当地面站请求与联盟网络建立连接时，首先需要对区块链中的数据进行检索，以查看是否有该地面站的认证信息。如果已经通过认证，则允许建立连接；否则，需要经过节点共识才允许接入。

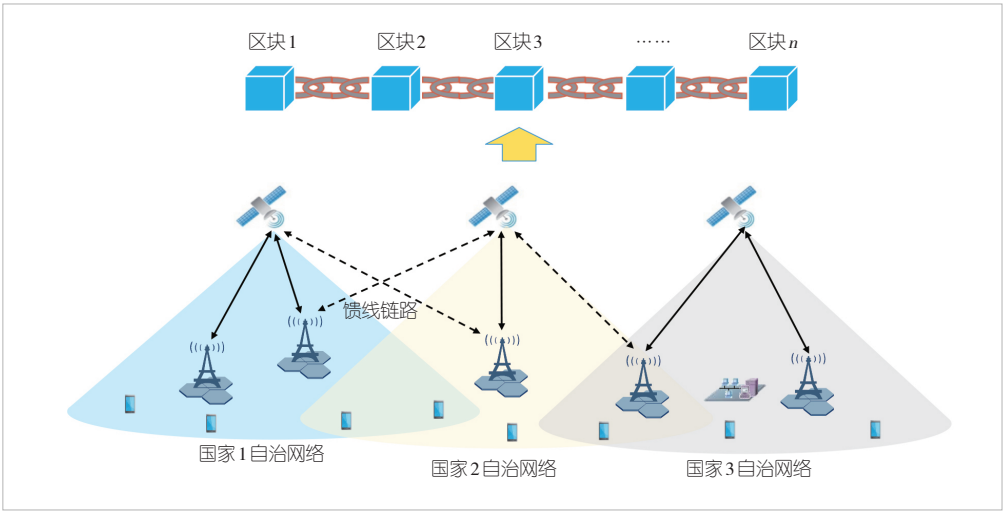


图6 天地一体化星地可信联盟

4 结束语

相比于5G，6G网络需要应对超高速、超低时延、超大规模连接场景带来的新的安全挑战。天地一体网络作为6G的基本组网架构，同样将面临新的安全风险，传统的网络安全技术也将难以适配。天地一体化网络面临的网络拓扑动态变化和卫星平台资源受限的安全挑战，将会极大影响6G网络研究和标准进程。因此，轻量化的接入认证、协议简化、轻量化的加解密和星地可信联盟等新技术研究是十分必要的。本文分析了接入认证、星地回传安全传输、星间链路安全传输、轻量化的无线物理层安全、抗量子密码及量子保密通信和基于区块链的星地可信联盟等网络安全技术，希望为后续6G天地一体化网络安全技术研究提供参考。

参考文献

[1] 刁兆坤, 杨丽, 王振章. 6G空天地一体化网络架构及其构建 [J]. 通信世界, 2024(4): 36-39
[2] 陈新宇, 张强, 陆光辉. 天地一体网络场景下的数字孪生关键技术 [J]. 中兴通讯技术, 2023, 27(2): 51-58. DOI: 10.12142/ZTETJ.202303010
[3] 缪德山, 邓凌越, 孙建成, 等. 6G星地融合无线网络及关键技术 [J]. 中兴通讯技术, 2024, 30(4): 42-49. DOI: 10.12142/ZTETJ.202404007
[4] 杨帅斌, 张昱, 卢为党. 面向6G的卫星通信感知一体化网络及关键技术 [J]. 中兴通讯技术, 2024, 30(5): 16-23. DOI: 10.12142/ZTETJ.202405004
[5] 夏旭. 面向5G/6G卫星: NTN标准发展、关键技术与未来思考 [J]. 广播电视网络, 2024(5): 60-65
[6] IMT-2030(6G)推进组. 6G网络安全愿景技术研究报告 [R]. 2021
[7] 陆海涛, 陈一喆, 娄笃仕. 5G/5G-Advanced/6G接入网安全技术演进及内生安全 [J]. 中兴通讯技术, 2022, 28(6): 85-94. DOI: 10.12142/ZTETJ.202206014
[8] 中国联通研究院. 6G网络安全需求及架构白皮书 [R]. 2024
[9] 3GPP. Security architecture and procedures for 5G system (Release 15): 3GPP TS 33.501 [S]. 2019
[10] LU H T, YAN X C, ZHOU Q, et al. Key intrinsic security technologies in 6G networks [J]. ZTE communications, 2022, 20(4): 22-31. DOI: 10.12142/ZTECOM. 202204004
[11] 中国移动通信研究院. 构建可信数字身份体系筑牢数字文明基石白皮书 [R]. 2024
[12] 徐晖, 陈山枝, 艾明. 面向6G的星地融合网络架构 [J]. 中兴通讯技术, 2023, 27(2): 9-15. DOI:10.12142/ZTETJ.202305003
[13] 杨立君, 李明航. 基于信道指纹的毫米波MIMO系统身份欺骗攻击检测方案 [J]. 电子与信息学报, 2023(12): 4228-4234
[14] 倪云云, 陈伯庆, 李刚. 5G毫米波通信中的物理层安全预编码 [J]. 中兴通讯技术, 2021(4): 53-59. DOI: 10.12142/ZTETJ.202104011
[15] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring [C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE, 1994: 124-134. DOI: 10.1109/SFCS.1994.365700
[16] NIST. Module-lattice-based key-encapsulation mechanism standard: 203 (draft) [EB/OL]. [2024-10-15].https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
[17] NIST. Module-lattice-based digital signature standard[EB/OL]. (2024-08-13) [2024-10-15]. https://nvlpubs. nist. gov/nistpubs/FIPS/NIST.FIPS.204.pdf
[18] NIST. Stateless hash-based digital signature standard [EB/OL].

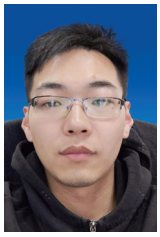
(2024-08-13) [2024-10-15]. https://nvlpubs. nist. gov/nistpubs/fips/nist.fips.205.pdf
[19] 西安电子科技大学广州研究院. 后量子密码迁移白皮书 [R]. 2024
[20] 中国通信标准化协会. 基于IPSec协议的量子保密通信应用设备技术规范: YD/T 4303-2023 [S]. 2023

作 者 简 介

陆海涛，中兴通讯股份有限公司资深系统架构师，正高级工程师，CISSP；主要从事无线网络架构、无线产品安全、大规模天线、动态频谱共享等技术研究；牵头承担10余项国家科技重大专项、“863”计划课题，获广东省科技进步奖；发表论文8篇，申请发明专利60余项。

周强（通信作者），中兴通讯股份有限公司5G ToB研发副总工，高级工程师；主要从事3G/4G/5G等无线通信技术研究；拥有丰富的无线系统产品设计和研发经验，牵头和参与多项国家科技重大专项课题；申请发明专利15项。

代九龙，中兴通讯股份有限公司RAN产品安全规划资深专家；主要从事无线网络协议栈、无线网络安全架构、无线产品安全、无线网络产品行业应用等技术研究；申请专利8项。



卢帆，中兴通讯股份有限公司RAN中心产品安全总监，CISSP；主要从事5G/6G网络安全、天地一体化网络、量子通信等无线通信技术研究；申请发明专利12项。

李锐，中兴通讯股份有限公司无线软件架构高级工程师；主要从事无线网络架构、网络安全、网络传输、软件架构等技术研究和开发；申请发明专利30余项。