6G星地融合网络安全需求及关键技术

Security Requirements and Key Technologies for 6G Integrated Satellite and Terrestrial Network

梁亚从/LIANG Yacong[1,2]，徐晖/XU Hui[1]
（1. 大唐移动通信设备有限公司，中国 北京 100083；
2. 北京航空航天大学，中国 北京 100191）
(1. Datang Mobile Communication Equipment Co. Ltd., Beijing 100083, China;
2. Beihang University, Beijing 100191, China)

DOI：10.12142/ZTETJ.202503003
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20250610.1125.002.html
网络出版日期：2025-06-10
收稿日期：2025-04-12

摘要：6G星地融合网络的复杂异构性导致其面临多层面的安全威胁与挑战。基于现有移动通信网络的架构与特性，分析了6G星地融合网络的安全挑战，明确了安全需求并提出了相应的安全参考架构。重点研究了无线通信安全、用户接入认证及隐私保护等关键技术在星地融合网络中的应用。研究表明，构建适配星地融合网络特性的安全技术体系是保障6G网络安全的基础。

关键词：6G；星地融合网络；网络安全；用户接入认证

Abstract: The complex heterogeneity of the 6G integrated satellite and terrestrial network leads to multi-layered security threats and challenges. Based on the architecture and characteristics of existing mobile communication networks, this paper analyzes the security challenges of the 6G integrated satellite and terrestrial network, clarifies the security requirements, and proposes a corresponding security reference architecture. The study focuses on applying key technologies such as wireless communication security, user access authentication, and privacy protection in the 6G integrated satellite and terrestrial network. The research demonstrates that establishing a security technology system tailored to the unique features of satellite-terrestrial integrated networks is fundamental to ensuring 6G network security.

Keywords: 6G; integrated satellite and terrestrial network; network security; user access authentication

引用格式：梁亚从, 徐晖. 6G星地融合网络安全需求及关键技术 [J]. 中兴通讯技术, 2025, 31(3): 9-13. DOI: 10.12142/ZTETJ.202503003
Citation: LIANG Y C, XU H. Security requirements and key technologies for 6G integrated satellite and terrestrial network [J]. ZTE technology journal, 2025, 31(3): 9-13. DOI: 10.12142/ZTETJ.202503003

作为实现“万物智联”6G总体愿景的基础支撑，6G网络架构设计需遵循兼容创新的理念，构建具有多域融合特征的新型网络体系[1]。6G网络需同时支持天基、空基、地基多维接入方式，融合固定、移动、卫星等异构连接类型，以满足全域覆盖、万物智联的网络需求。当前星地融合网络发展采用“5G体制兼容，6G系统融合”的技术路径[2]，通过高、中、低轨卫星网络与地面移动通信网络的深度协同，构建立体化全域覆盖通信体系[3]。然而，卫星节点的移动性、网络环境和无线链路的开放性，以及星地异构组网特性，对现有移动通信安全体系提出了新的挑战。为此，亟需针对6G星地融合网络的特有属性和业务特征，开展安全架构及关键技术研究。本文基于地面移动通信系统安全框架，结合6G星地融合网络架构特性，系统分析该网络面临的安全威胁与防护需求，并提出相应的安全关键技术体系。

基金项目：国家重点研发计划项目（2022YFB2902203）

1 6G星地融合网络架构及研究现状

星地融合作为6G网络的核心特征，通过融合高、中、低轨卫星网络与地面移动通信网络，构建了一个全方位的立体覆盖通信系统。这一融合不仅涉及体制、协议、网络等多个层面，还实现了天基网络与地面移动通信网络的融合，满足地面及立体空间的全域、全天候覆盖需求，确保用户能随时随地按需接入网络。图1为6G星地融合网络示意图。

6G网络通过星地融合的多接入技术，可为用户提供服

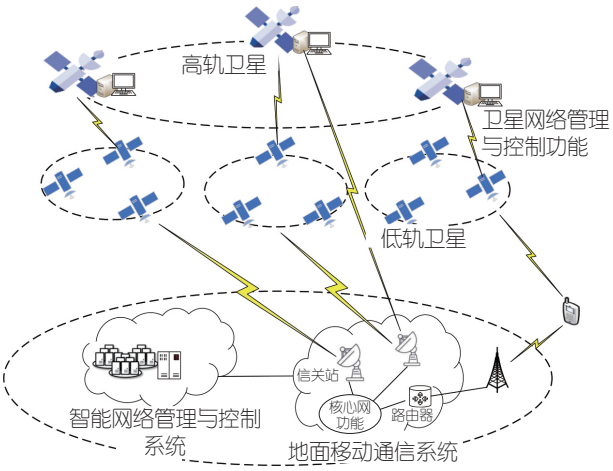

图1 6G星地融合网络示意图

务质量保障和高可靠性连接，确保通信服务的连续性与稳定性，从而显著提升用户体验。卫星通信网络的高动态性、卫星节点的快速变化以及星地网络的异构性，使得星地融合网络需考虑通信拓扑的动态性、复杂性和可扩展性，还需应对空间节点的高速移动性、有限存储与计算能力等挑战[4]。

6G星地融合网络采用服务化架构设计，可根据业务需求与组网场景灵活部署网络功能。具体而言，地面网络部署完整的移动通信核心网与接入网，而卫星端则基于组网需求与卫星能力，对网络功能进行动态分割与灵活部署，从而提供定制化网络服务并增强多场景适应能力。通过容器等虚拟化技术，可在卫星节点部署定制化网络功能。同时，采用轻量化设计与细粒度分割策略，结合组网形态、业务需求、网络资源状态及节点处理能力，在星地节点间实现网元功能的优化分配。该架构支持网络功能的按需定制与动态重构，显著提升系统灵活性与可扩展性。然而，星地间网络功能的动态定制与重构也引入了新的安全风险，包括星地/星星无线传输安全防护需求，以及轻量化认证机制的实施挑战。

第3代合作伙伴计划（3GPP）在Release 15的需求定义中已经明确将卫星接入列为5G多接入技术之一[5]，在Release 16和Release 17中，3GPP主要针对透明转发的组网场景开展研究和标准化工作；Release 18则重点研究卫星覆盖增强、网络验证终端位置等工作；Release 19开始研究卫星工作在再生模式即基站上星的架构，支持存储转发场景和用户设备（UE）–Satellite–UE的场景。同时3GPP也是从R19开始了星地融合网络安全相关的标准化研究，主要关注的是安全关键问题和潜在解决方案、5G新空口（NR）非地面网络（NTN）和物联网（IoT）NTN在存储转发模式下的安全关键问题和潜在解决方案，以及UE–Satellite–UE场景下的安全关键问题和潜在解决方案。

2 6G星地融合网络安全威胁

星地融合网络包括以卫星为主的卫星网络和地面移动通信系统网络，其中卫星网络主要由高轨卫星网络、中低轨卫星网络组成。在6G时代，星地融合网络将与其他网络协同形成全域无缝覆盖的立体通信架构，最终实现无盲区宽带移动通信的目标。然而，该网络固有的链路开放性、拓扑动态性及多跳传输等特性，为6G系统引入了新型安全威胁。

2.1 无线通信面临的安全威胁

相较于地面移动通信系统，星地融合网络的安全威胁维度显著扩展：除空口安全外，星间链路与馈电链路同样以无线传输方式存在，导致网络暴露面扩大，遭受攻击的风险加剧。如图2所示，用户通过卫星无线链路接入6G系统时，卫星可能承载基站或部分核心网功能[6]。在此架构下，用户上行数据及网络控制信令可能需经星间链路传输；若卫星判定需地面处理，则通过馈电链路将数据转发至地面信关站，最终抵达地面核心网。基于链路类型划分，其安全防护可分为3个维度：接入安全、星间安全及馈电安全。

1）接入安全

当前3GPP制定的NTN标准要求用户上报位置信息。由于卫星波束覆盖范围广且空间环境开放，存在恶意攻击者窃听或干扰空口消息的风险，攻击者可利用获取的用户位置信息发起针对性攻击。此外，现有移动通信系统中对UE的认证依赖核心网提供的认证结果。考虑到卫星的移动性，当星载基站无法及时连接地面网络获取认证结果时，系统易遭受拒绝服务（DoS）攻击。

2）星间安全

星间链路作为卫星间通信的无线传输通道，承担数据中继功能，可实现地面信关站与用户数据通过卫星网络的远距离传输。但该链路的高度开放性导致信道监听风险显著提升，可能面临重放攻击、数据篡改等安全威胁。

3）馈电安全

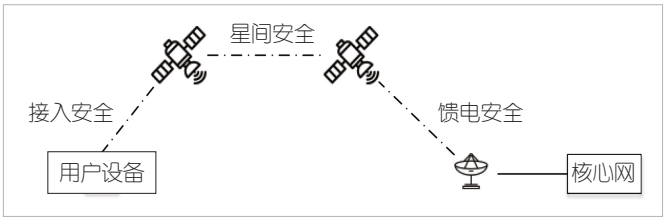

图2 6G星地融合网络无线链路安全威胁

馈电链路主要采用Ka或Q/V频段微波链路，为信关站与卫星之间提供无线数据传输通道，实现用户链路的回传功能。该链路面临以下安全威胁：恶意攻击者可通过干扰信关站破坏其对卫星的跟踪瞄准功能；攻击者可能通过身份伪装手段入侵星地融合系统，窃取敏感信息。此外，强干扰信号攻击可能导致卫星接收机饱和阻塞，造成服务中断[8]。

星地融合网络的安全威胁来源可分为3类：卫星网络固有安全威胁、地面网络固有安全威胁、星地融合组网架构引入的新型安全威胁。其中，架构威胁主要包括多跳长距离通信传输的安全风险、认证结果获取延迟引发的安全隐患。

2.2 认证面临的安全威胁

星地融合网络作为多层次异构网络融合系统，其网络覆盖范围显著扩大。由于具有传输路径长、接入设备多等特点，与单一网络明确的安全边界相比，融合网络需要建立更加完备的认证机制。按照认证交互对象划分，主要认证包括：UE与网络之间的认证、卫星与卫星之间的认证以及卫星与信关站之间的认证。若认证系统存在缺陷，任一节点遭受攻击都可能危及整个网络安全，导致严重后果。同时，星地融合网络需要支持全球范围内海量物联网设备的接入，但这些设备普遍存在能源受限、计算能力不足等问题，若缺乏轻量化的认证系统将严重影响其接入效率。

脆弱的认证机制易引发DoS攻击。以卫星通信系统为例，其对接入的UE数量存在严格限制。攻击者通过伪造UE身份发起大量接入请求时，由于卫星无法快速鉴别UE合法性，必须依赖与地面网络的交互来完成注册认证。该过程会消耗大量系统资源，使合法UE无法接入，形成DoS攻击。

2.3 用户隐私保护面临的安全威胁

在星地融合网络中，UE的位置信息和身份信息的泄露是两大重要的隐私安全问题。因低轨卫星的高速移动性，网络需要通过获取UE的位置信息来完成卫星接入，从而保障高质量的连续服务。此外，根据各国法律法规要求，UE需上报其位置信息以确定归属国家，并将服务移交至相应运营商，确保合规性。在此过程中，UE播发的辅助定位消息可能泄露其位置信息。若卫星与UE交互定位时未采取有效隐私保护措施，UE位置信息将面临泄露风险，不仅侵犯用户隐私权，还可能使用户面临潜在安全威胁。

6G星地融合网络仍存在传统UE身份信息泄露问题。在与卫星建立连接时，UE需提供标识信息以完成链路建立；连接建立后，还需与核心网交互完成接入认证与授权。在这些过程中，UE的标识信息存在泄露风险，不仅可能导致用户隐私暴露，还可能被恶意利用，例如实施身份伪造或非法接入。

3 6G星地融合网络安全需求

针对星地融合网络面临的安全威胁，构建系统安全需建立全面的安全需求框架。首先，基于网络固有特性，必须保障通信链路上的数据加密传输。针对脆弱认证机制引发的DoS攻击，需设计完善的认证方案。此外，由于星地融合网络业务特性与地面网络存在差异，需重新分析其安全需求，特别要引入针对UE位置信息的隐私保护机制。

3.1 无线通信安全需求

无线通信安全需求主要包含3个方面：1）接入安全，需保障用户接入时与卫星间通信安全，通过数据加密和完整性保护机制确保用户身份隐私，防止位置信息和小区标识泄露；2）星间链路安全，需实现数据传输的机密性和完整性保护，并具备抗重放攻击能力；3）切换安全，针对低轨卫星高速移动特性导致的频繁切换，需建立卫星间信任关系，并对传输的安全上下文等敏感信息实施机密性和完整性保护。馈电链路安全需确保数据传输的机密性和完整性，同时要求信关站与卫星间实施双向认证，防止伪终端接入。

基于上述分析，无线通信安全的技术需求可归纳为加密机制与完整性校验技术，以保障无线通信链路的端到端安全传输及数据隐私保护。

3.2 认证安全需求

星地融合网络需构建完善的密码认证体系，这包括3个层面：节点认证，支持UE–网络、卫星–卫星及卫星–信关站间的双向认证；安全防护，认证机制需具备抗DoS攻击能力，并增强多用户共享终端的认证能力；终端认证，需实现基于密码的卫星终端认证。建立覆盖用户、终端及信关站的认证系统，可以为星地融合网络提供安全可靠的通信保障。

3.3 用户隐私保护安全需求

在星地融合网络中，由于卫星小区覆盖范围明显大于地面网络，UE需主动上报地理位置信息以实现网络接入。这一特性使得位置信息与用户标识的保护面临严峻挑战。为此，网络需采用加密传输、数据匿名化及隐私保护协议等多重安全机制，确保UE敏感信息在传输与存储过程中的安全性，从而有效保障用户隐私并维护系统安全。

4 6G星地融合网络安全关键技术

为满足星地融合网络的安全需求，6G网络需部署以下核心安全技术：无线通信安全技术、用户接入认证技术以及

隐私保护技术。

4.1 无线通信安全技术

星地融合网络的无线通信安全涵盖3个层面：接入通信安全、星间链路安全和馈电链路安全。其中，接入通信安全涉及UE与基站的通信保护，而基站在该网络中可部署于卫星或地面。因此，现有移动通信的安全机制可适用于星地融合网络的接入通信安全防护。

在星间链路与星地馈电链路通信安全方面，基于卫星与陆地站之间可通过星历精确预测相对位置的特点，星地融合网络可采用预置密钥机制来实现两类链路的通信安全保护。

星间链路与馈电链路通信安全可采用IPSec或类似技术实现端到端保护，对所有传输数据进行加密。尽管IPSec具备架构简单的优势，但其仍存在数据重复加密问题：无须加密或已加密数据仍被二次处理，导致卫星资源浪费。鉴于卫星资源受限的特性，需对IPSec进行针对性优化以适应星地通信场景。针对IPSec在星上可能会存在的资源浪费问题，目前的研究主要提出了基于多层IPsec安全保护方案。该方案将数据包划分成几部分，并对不同部分实施不同的保护措施，并且互相隔离，在端到端的数据包传输过程中可以分区进行处理。这样能减少加密解密开销，提高网络性能[9-10]。

6G星地融合网络可以将接入通信、星间通信和馈电通信的安全统一考虑，通过将UE安全通信终结点从基站延伸至用户面功能（UPF），实现接入通信、星间链路及馈电链路的端到端安全保护。

4.2 用户接入认证技术

卫星终端认证技术是指核心网依据存储的UE签约信息，借助卫星链路完成对终端的身份核验，从而为其提供相应的卫星通信服务。卫星终端的标准认证可直接沿用3GPP定义的UE认证技术体系实现。

星地融合网络利用卫星物联网技术为偏远地区提供全天候广覆盖连接，弥补了传统网络的覆盖不足。针对物联网设备低功耗、低算力和窄带通信特性，网络需在支持标准3GPP UE注册功能的同时，提供轻量化认证与安全机制。现有认证架构在天地融合场景下存在效率瓶颈，多跳通信与复杂流程导致卫星终端注册时延过高。因此，需设计新型轻量化认证授权架构，通过流程优化提升认证效率，满足物联网等轻量化应用需求。

在UE与卫星的认证过程中存在以下关键问题：1）安全风险方面，UE可能接入伪卫星，导致位置信息和设备标识泄露；2）时效性约束，受限于卫星移动的窗口期，需采用轻量化认证机制实现快速双向认证；3）连接限制，在馈电链路不可用场景下，传统认证与密钥协商（AKA）认证需经历4个交互阶段（UE–卫星初次连接、卫星–信关站初次连接、UE–卫星二次连接、卫星–信关站二次连接）才能完成完整认证流程。在星间链路存在的情况下，完整认证仍需经历4次星地往返交互，具体如图3所示。这种认证机制将导致明显的路由时延，尤其对偏远地区物联网设备及移动终端而言，时延累积效应更为突出且难以精确预估。

因此，用户接入认证可采用两种方案：第一种是将存储用户签约数据及承担认证功能的网元部署至卫星端，具体包括将归属签约用户服务器（HSS）、鉴权中心（AuC）、统一数据管理功能（UDM）和接入及移动管理功能（AMF）上星，实现在星载系统内完成用户与网络间的双向认证；第二种方案采用UE主导的认证机制，由UE生成鉴权向量或鉴权响应并发送至卫星，卫星通过地面网络完成验证后返回结果。该方案仅需1次UE与卫星的连接即可完成认证。根据3GPP的研究[8]，可在第1阶段利用UE生成的鉴权向量保护传输数据，实现认证阶段即开始数据传输，从而提升认证效率。另外，也有解决方案提出，UE可以一次性存储多个核心网产生的鉴

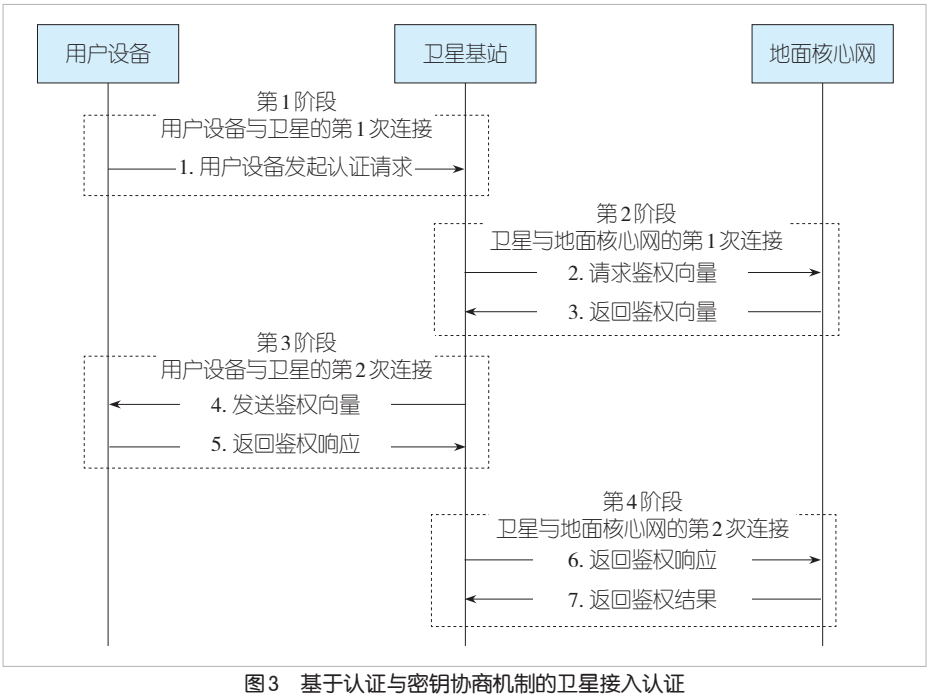

图3 基于认证与密钥协商机制的卫星接入认证

权向量。当UE需要注册认证时，基于存储的鉴权向量产生鉴权响应，随认证请求发送给接入的卫星，卫星连接地面核心网后，核心网验证鉴权响应，返回鉴权结果。

区块链技术是一种基于分布式账本的去中心化数据存储与验证机制，其凭借密码学算法、共识协议及链式数据结构等核心技术，实现多方协作环境下数据的不可篡改性与透明可追溯性，其分布式架构与融合网络的异构性、多方参与特性高度适配。针对当前认证体系存在的问题，已有研究提出基于区块链的跨域认证方案：通过构建卫星节点区块链网络，以分布式账本形式分散存储用户认证凭证，有效降低与第三方信任中心的交互时延；同时借助共识机制，使各卫星节点可直接采信链上其他节点的认证结果，进而实现用户身份的快速验证[11-13]。

4.3 隐私保护技术

在6G星地融合网络中，隐私保护的关键环节集中于数据空口传输与数据共享阶段。6G的诸多业务（如选网流程、切换流程等）均依赖终端位置信息，为此需在空口引入终端位置上报机制。然而，终端精确位置上报存在隐私泄露风险，可通过两类隐私保护技术应对：实现用户身份与位置信息的解耦，例如采用频繁更新用户标识的方式；对位置信息本身进行保护，具体包括利用数据加密技术，确保仅持有正确密钥的授权方能够获取位置数据，或通过位置信息模糊化处理，如扩大上报位置范围以替代精确坐标。

为保障数据使用过程中的隐私安全，可采用隐私计算技术与数据脱敏技术。隐私计算技术致力于在数据不对外泄露的前提下实现数据分析与计算，重点保护数据使用流程及计算结果的安全性。其中，差分隐私技术通过在数据查询或分析过程中引入可控噪声，依据应用场景设定合适的噪声强度，有效抵御攻击者基于外部查询推测内部数据的风险；同态加密技术则支持在密文状态下直接执行计算操作，且所得结果与明文计算结果完全一致，确保数据处理全程处于加密保护状态。

5 结束语

6G星地融合网络的安全技术发展需重点关注以下研究方向：首先，在认证技术方面，需深入研究星间认证及卫星组网认证机制，包括高低轨卫星间认证和同轨道卫星间认证，这些场景可能需采用差异化的认证方案。其次，在数据安全领域，针对云边端协同架构下多方参与的数据流转，需强化访问控制与隐私保护等关键技术。星地融合网络需持续迭代安全需求，深化新型安全技术的探索、研究与应用，以有效应对日趋复杂多元的安全挑战。

参考文献

[1] IMT-2030推进组. 6G总体愿景与潜在关键技术白皮书 [R]. 2023
[2] 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. DOI: 10.23919/JCC.2020.12.011
[3] 宋雅琴, 徐晖, 刘险峰, 等. 面向星地融合网络的统一编排架构和关键技术 [J]. 移动通信, 2024, 48(1): 19 - 24
[4] 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, 29(5): 9 - 15. DOI: 10.12142/ZTETJ.202305003
[5] 3GPP. Service requirements for the 5G system; stage 1(Release 18) [S]. 2024
[6] 宋雅琴, 徐晖, 刘险峰, 等. 星地融合网络的组网关键技术探讨 [J]. 天地一体化信息网络, 2024, 5(3): 68-77. DOI: 10.11959/j.issn.2096-8930.2024030
[7] IMT-2030推进组. 6G天地一体化网络安全技术研究报告 [R]. 2024
[8] 3GPP. Study on security aspects of 5G satellite access in the 5G architecture; phase 3 (release 19) [R]. 2023
[9] 黄飞, 许辉, 吴诗其. 基于PEP-IPSec实现卫星IP网的网络安全 [J]. 计算机应用研究, 2007, 24(8): 132-136. DOI:10.3969/j.issn.1001-3695.2007.08.040
[10] 罗晋. IPsec在卫星IP网络中的改进与应用 [D]. 成都: 电子科技大学, 2016
[11] WANG B Y, CHANG Z, LI S C, et al. An efficient and privacy-preserving blockchain-based authentication scheme for low earth orbit satellite-assisted Internet of Things [J]. IEEE transactions on aerospace and electronic systems, 2022, 58(6): 5153 - 5164. DOI: 10.1109/TAES.2022.3187389
[12] 魏松杰, 李帅, 莫冰, 等. 基于共识机制的LEO低轨卫星网络区域合作认证协议 [J]. 计算机研究与发展, 2018, 55(10): 2244-2255
[13] 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

作　者　简　介

梁亚从，大唐移动通信设备有限公司创新中心标准研究工程师，北京航空航天大学在读博士生；主要研究领域为移动通信安全、星地融合网络等。

徐晖，大唐移动通信设备有限公司创新中心技术总监；主要研究领域为移动通信网络、移动通信安全、星地融合网络等；先后主持和参加国家“863”计划项目、国家重大专项和国家重点研发计划项目近10项；已发表论文10余篇。