6G网络安全的架构与关键技术

Architecture and Key Technologies of 6G Network Security

罗涵一/LUO Hanyi，崔宝江/CUI Baojiang，仝鑫/TONG Xin
（北京邮电大学，中国 北京 100867）
(Beijing University of Posts and Telecommunications, Beijing 100867, China)

DOI：10.12142/ZTETJ.202503009
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20250522.1348.001.html
网络出版日期：2025-05-22
收稿日期：2025-04-05

摘要： 6G网络安全面临严峻挑战，尤其需应对5G固有的安全缺陷以及异构环境与量子计算带来的新型威胁。通过详细阐述6G网络安全需求及关键技术，系统性地梳理并分析了可信内生安全三层架构理念及其融合区块链、量子密钥分发与人工智能（AI）智能编排等关键技术的应用，为构建面向未来的安全、可信的6G网络提供理论参考。

关键词： 6G网络；安全架构；量子通信；区块链

Abstract: 6G network security faces significant challenges, particularly in addressing inherent security vulnerabilities of 5G and novel threats arising from heterogeneous environments and quantum computing. By thoroughly elaborating on 6G network security requirements and key enabling technologies, this paper systematically organizes and analyzes the concept of a trusted endogenous security three-layer architecture and its application in integrating key technologies such as blockchain-based distributed trust management, quantum key distribution, and AI-driven intelligent orchestration. This work aims to provide theoretical references for the construction of secure and trustworthy future 6G networks.

Keywords: 6G network; security architecture; quantum communication; blockchain

引用格式： 罗涵一, 崔宝江, 仝鑫. 6G网络安全的架构与关键技术 [J]. 中兴通讯技术, 2025, 31(3): 50-55. DOI: 10.12142/ZTETJ.202503009
Citation: LUO H Y, CUI B J, TONG X. Architecture and key technologies of 6G network security [J]. ZTE technology journal, 2025, 31(3): 50-55. DOI: 10.12142/ZTETJ.202503009

1 6G网络安全概述

1.1 研究背景

6G网络作为下一代通信技术的前沿代表，凭借其高速率、低时延和海量连接等特性，将在未来通信领域引发深刻变革。它不仅是智能交通、远程医疗、工业互联网等领域创新发展的重要驱动力，更是推动社会智能化、数字化发展的关键力量。然而，网络安全问题仍是严峻挑战，成为制约6G网络大规模发展的瓶颈。量子计算技术的兴起对传统加密算法构成威胁；海量物联网设备的接入增加了身份认证与管理的难度；空天地一体化网络的融合模糊了网络边界，增加了安全防护的复杂性[1]。深入研究6G网络安全架构，对保障网络稳定运行、数据安全等具有重要战略意义。

1.2 研究现状

欧盟和美国的科研机构及企业正积极推进6G网络安全研究。欧盟通过“Horizon 2020”计划资助了多个6G安全项目，重点研究量子加密、信任模型构建等前沿技术[2]。V. L. NGUYEN 等[3]对6G安全与隐私问题进行了系统综述，指出6G在延续前代通信技术安全风险的同时，还面临新型通信技术带来的威胁，例如针对太赫兹波段超大规模多输入多输出（MIMO）系统的无线电攻击等。美国科技企业正积极推进6G网络基础设施建设。SpaceX和AST SpaceMobile在卫星通信领域取得重大突破，其技术可视为6G网络的前期探索。SpaceX通过Starlink计划已部署大规模低轨高通量卫星群，显著提升了全球网络通信能力。AST SpaceMobile则利用BlueWalker 3卫星实现了技术突破，首次完成卫星与未修改的智能手机的直接语音通话连接[4]。

中国的各大通信运营商、科研院所也高度重视6G网络安全。中国移动牵头发布《6G可信内生安全架构研究报告》[5]，深入分析6G安全需求，提出涵盖基础资源层、网络基础设施层和管理及服务层的安全架构，构建6G可信内生安全架构。中国联通发布《6G网络安全需求与架构白皮书》[6]，提出融合“信任+安全”的设计理念。紫金山实验室开展内生安全试验场建设，基于拟态防御理论验证6G网络安全架构的可靠性，为6G网络安全技术的落地应用提供实践支撑[7]。

当前6G网络安全研究虽取得进展，但仍存在明显不足。

首先，针对新兴技术融合的安全风险研究尚不充分，特别是量子通信与传统通信技术结合产生的安全兼容性问题。其次，现有研究未能充分解决安全架构与行业特定需求的深度整合问题，安全与业务协同发展机制仍需完善[5]。

2 6G网络安全需求分析

2.1 1G—5G安全演进

移动通信技术从1G到5G的演进过程中，网络架构与安全防护机制持续升级。1G、2G时代主要依赖基础加密算法保护语音通信，但随着技术发展，这些算法的安全局限性逐渐显现。3G、4G阶段引入了更先进的加密体系和完善的认证机制，显著提升了系统安全性。5G时代网络架构革新催生了新的安全需求，包括网络切片隔离、服务化架构防护等创新安全方案[8-10]。网络安全信任模型经历了从边界防护到动态评估的转变。5G网络通过构建用户行为画像，实现基于身份和行为的动态信任评估，当检测到异常行为时可实时触发安全审查与风险预警机制。

2.2 5G安全缺陷

5G网络在安全机制方面虽取得重要突破，但仍存在若干安全隐患。其信令面与用户面分离的架构在提升网络灵活性和可扩展性的同时，使信令面成为潜在攻击目标，可能引发大规模通信中断。网络切片技术虽支持业务定制化服务，但切片间隔离存在安全缺陷，攻击者可能利用此漏洞实现跨切片渗透[11-13]。此外，移动边缘计算（MEC）技术将计算存储资源下沉至网络边缘，在降低时延的同时也增加了边缘节点的安全风险，使其易受物理和网络攻击威胁，导致数据泄露和服务中断。图1展示了1G—5G网络演进过程及现存安全威胁。

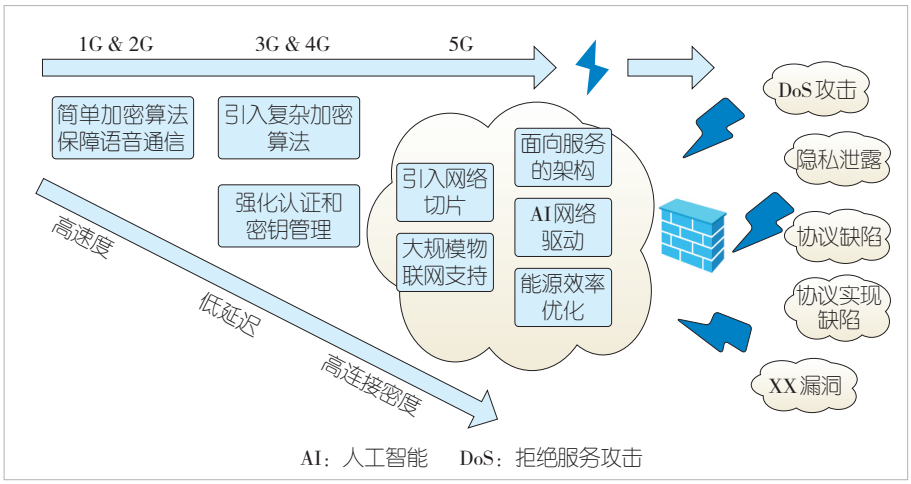


图1　1G—5G网络演进及现存安全威胁

2.3 6G安全设计理念

为应对6G网络的复杂安全挑战，业界提出了融合“信任+安全”的可信内生安全新体系。该体系整合并扩展了传统通信技术与信息技术安全理念[6]。6G可信内生安全架构基于信任构建、安全防护和协同防御的原则，通过信任机制建立可靠网络生态，结合安全检测技术实现风险防控。该架构实现了四大转变：从外挂式防护到内生安全、从被动响应到主动防御、从静态策略到动态调整、从孤立防护到协同联动[14]。这种主动、智能、弹性的安全体系将为6G异构网络环境和多样化业务场景提供保障。

3 6G网络安全架构设计

中国移动的粟栗等[15]提出的6G网络内生安全架构采用分层设计理念，构建了包含安全能力层、控制层和决策层的体系结构。该架构创新性地整合了协同信任共识机制、智能编排功能及人工智能技术，形成具备主动免疫特性、信任共识能力和协同弹性的安全运行机制，其架构如图2所示。

3.1 安全能力层

安全能力层作为基础支撑层，主要实现物理安全资源的整合与封装，其架构由信任使能单元和安全使能单元构成核心组件。该层通过接收上层控制系统的统一调度指令，动态协调各安全功能模块的协同运作。通过与网络资源调度系统的融合，该层能基于实时安全需求，智能实现安全能力的拓

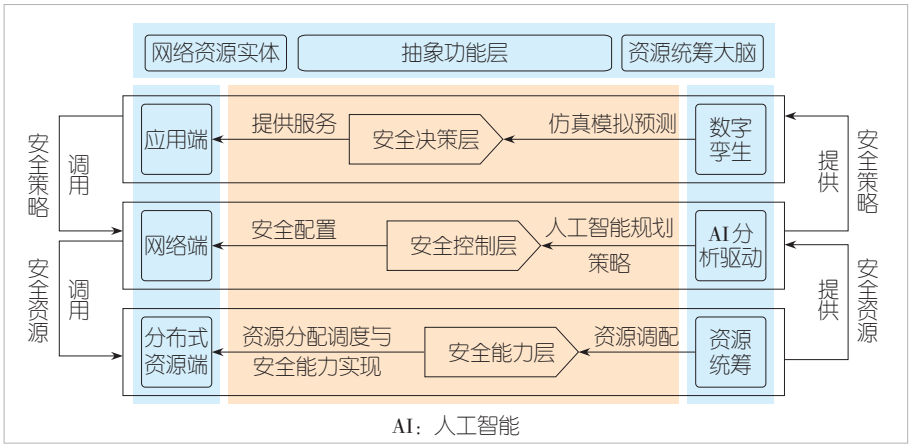


图2　6G网络安全架构

AI：人工智能

扑部署、弹性伸缩和动态调整，形成自适应安全防护体系。

3.1.1 信任使能单元

区块链技术凭借其去中心化与不可篡改性，在6G网络信任管理中展现出优势。基于区块链构建的分布式信任账本能可靠记录用户/设备身份信息、行为数据等，确保数据真实可信[16]。在身份认证环节，通过智能合约实现自动化验证与授权，提升认证效率和安全性。当用户接入6G网络服务时，智能合约自动核验身份信息并与信任账本比对，在确保认证过程不可篡改且可追溯的前提下，实现高效身份认证。

分布式公钥基础设施（DPKI）技术因其分布式特性，可有效适配6G网络的大规模、分布式需求。该技术通过分布式密钥管理与认证机制，确保用户身份安全认证及密钥可靠分发。在6G物联网场景中，DPKI能为海量接入设备提供唯一身份标识与密钥，保障设备间安全通信与认证[17]。然而，该技术在大规模部署时面临挑战：构建分布式信任账本及实施DPKI认证将消耗大量计算资源与能耗。这不仅对终端设备计算能力提出更高要求，其能源消耗问题也与绿色6G理念存在冲突。因此，6G网络架构设计需在安全可溯源计算与能耗效率之间寻求优化平衡。

3.1.2 安全使能单元

空天地一体化作为6G网络的典型特征，其安全接入面临新的技术挑战。针对该问题，需设计新型安全接入协议，集成多因子认证与加密隧道等技术，确保异构网络间的安全切换与数据传输。具体而言，在星地切换场景中，采用融合生物特征、密码等多因子的认证机制，保障切换过程的安全可信；同时部署动态加密隧道技术，实现传输数据的端到端保护，有效防范切换过程中的数据窃取与篡改风险[17]。

量子通信技术利用量子态的不可克隆性和量子纠缠特性，实现绝对安全的通信密钥分发，为6G网络的安全通信奠定了坚实的基础。通过量子密钥分发，能够保障通信数据的机密性，抵御量子计算攻击和传统的网络窃听攻击。在6G网络架构中，量子通信技术特别适用于核心数据传输场景，能够确保数据在传输过程中的安全性。

3.2 安全控制层

安全控制层作为安全体系的中枢管理单元，统筹安全能力层的调度部署、信任与安全协同及策略控制，依托人工智能技术构建网络功能层与安全能力层的联动机制。该层基于人工智能技术，构建了网络功能层与安全能力层的智能协同机制。通过解析上层策略指令并整合资源编排功能，实现对安全模块的动态部署。其核心创新在于通过跨层协同机制，达成安全策略的智能适配与防御资源的弹性调配，推动安全防护能力随网络态势动态演进。

3.2.1 安全能力调度

网元安全功能弹性组装技术通过将网络安全功能模块化，根据不同的业务需求和安全策略，动态地组装和部署安全功能模块。以视频业务为例，该技术能够依据内容敏感度和用户安全等级，智能配置加密强度、数字版权管理等差异化安全模块。这种基于业务需求的安全能力动态编排机制，实现了防护资源的精准调度与优化配置，显著提升了安全防护的针对性和运行效率。

3.2.2 信任与安全协同

信任传递机制采用信任链架构，实现从终端设备、网络基础设施到应用服务的逐级信任验证与传递。在风险控制层面，通过融合信任评估与威胁分析结果，实施分级防护策略：对高信任度对象采用轻量化安全策略以提升业务效率；对低信任度或高风险对象则增强安全监控强度。基于人工智能的协同度量系统通过分析网络信任数据与安全数据，构建双模评估体系（信任模型+安全模型），实现网络安全态势的实时评估与动态调控。当检测到风险超限时，系统可自动触发策略调整机制。然而，受限于AI模型部署成本及硬件设备维护费用，该技术在当前阶段难以实现6G网络的全域覆盖。

人工智能信任管理模型的高计算资源需求给网络基础设施带来压力，影响整体网络性能与用户体验。建议采用分阶段部署策略：初期优先在关键网络节点和敏感业务节点实施，待技术优化和资源条件成熟后，再向网络边缘扩展。

3.3 安全决策层

安全决策层是6G可信内生安全框架的核心，融合人工智能分析能力，具备多方面功能：进行集中化、智能化的安全数据分析，输出安全态势、威胁情报和安全策略；与数字孪生网络联动，开展安全运维分析与调优；作为安全能力和服务的对外输出接口，整合并输出安全服务能力。

3.3.1 智能分析

基于联邦学习的网络安全攻击检测技术通过多数据源协同学习，能够全面识别网络攻击模式。该技术允许参与方在不共享原始数据的前提下共同训练模型，有效保护数据隐私。结合深度学习算法，可对网络流量、用户行为等数据进行实时分析，检测异常行为与潜在安全攻击，实现网络安全威胁的智能预警与快速响应[18]。当系统检测到网络流量异常激增或用户行为异常时，将自动触发预警机制，通知安全管理人

员及时处置，并利用智能算法进行攻击溯源分析，定位攻击源与攻击路径，为后续防御提供依据。目前，异常流量监测系统已在运营商试点部署并取得良好效果。未来在6G网络中，此类系统具有广阔的发展前景，但仍面临诸多挑战。

在6G网络中，海量下沉物联网设备产生的巨量流量对异常检测模型提出了更高要求。同时，模型需针对未来可能出现的6G新型攻击进行适应性扩展，而非简单沿用现有方案。此外，6G网络的异常流量监测系统还需与入侵检测系统（IDS）、入侵防御系统（IPS）等安全体系深度融合，构建全方位、多层次的网络安全防护架构。

3.3.2 安全推演

通过构建与实际网络完全匹配的数字孪生模型，可在虚拟环境中模拟各类网络攻击场景，预先分析潜在影响与损失，并制定针对性防御策略。数字孪生网络支持对新型安全技术与策略的验证优化，评估其有效性与可行性，为实际网络安全防护提供依据。

3.3.3 安全能力开放

基于零信任架构，对所有网络访问实施身份认证与权限验证，突破传统网络边界信任模式。通过基于属性的密钥管理架构（ABKMA）协议等安全能力开放技术，实现安全能力的对外共享。第三方应用可借助标准化接口调用网络安全能力，既保障业务安全防护，又推动6G网络安全生态发展。

4 6G 网络安全关键技术

4.1 安全基础理论

4.1.1 可信计算

可信计算技术通过嵌入可信芯片构建可信计算环境，确保6G算网基础设施的安全性。可信芯片存储设备的唯一身份标识与密钥，在启动阶段对系统软件及应用程序进行完整性验证，防止非法篡改。该技术利用加密与签名机制保障数据处理过程中的机密性与完整性。在云环境中，可信计算可实现虚拟机安全隔离与数据安全存储，有效防范虚拟机逃逸及数据泄露。当用户在6G云平台处理敏感数据时，该技术确保仅授权用户及程序可访问数据，从而提供安全保障。

4.1.2 量子通信

量子通信基于量子力学原理实现量子密钥分发与加密传输。量子密钥分发利用量子态的不可克隆性和测量坍缩特性确保密钥安全生成与分发。

以BB84协议为例，其通过偏振态编码和基矢比对实现密钥的安全分发。发送端Alice在单光子的偏振维度上，选用两组非正交基矢以及每组基矢下两个正交偏振态。根据随机生成的0和1经典二进制比特随机序列，Alice将光源编码成相应偏振的单光子量子态——H偏振态（水平）及–45°偏振态代表经典比特信息0，V偏振态（垂直）及+45°偏振态代表经典比特信息1，并进行传输。接收端Bob随机选择直角基矢或斜角基矢之一进行测量并记录结果。

一段时间后，Alice和Bob通过认证的公共信道交换基矢选择信息，保留相同基矢对应的测量结果形成筛后密钥。双方从筛后密钥中随机选取部分数据进行误码率检测，若误码率超过预设阈值则判定通信不安全并重新建立连接；当误码率满足安全要求时，即完成密钥分发过程。

任何窃听者在对未知单量子态进行测量时，由于量子测不准原理的制约，必然导致量子态坍缩并产生随机测量结果。这种干扰将提高通信双方的误码率，使其无法通过安全筛选。该机制使得通信双方能够通过量子信道生成随机密钥，并实时监测潜在的窃听行为，确保密钥的绝对安全性。量子隐形传态技术通过实现量子态的瞬时传输，为构建未来超远距离、超高速的安全通信系统提供了理论基础。

当前量子密钥生成速率与传输距离仍存在明显限制。以A. E. HAJOMER团队[19]研发的连续变量量子密码系统（CV-QKD）为例，其实现了0.7 Gbit/s的密钥生成速率和85 km的安全传输距离。针对该技术瓶颈，6G网络可采用混合安全架构：量子通信技术专用于保障核心敏感数据的短距安全传输，通过量子密钥分发确保关键信息在传输过程中的保密性与完整性；而边缘数据则采用传统密码算法实施加密保护。

4.2 安全基础设施

4.2.1 区块链

区块链是一种基于分布式账本技术的去中心化系统，其核心特征包括数据不可篡改性。主要技术架构包含以下要素：采用工作量证明（PoW）、权益证明（PoS）等共识机制确保全网节点数据一致性；通过智能合约的预定义代码实现交易逻辑自动化执行；运用非对称加密算法保障数据隐私安全与身份认证；依托点对点网络（P2P）架构实现节点间直接通信，消除中心化中介；利用哈希算法（如SHA-256）生成数据唯一指纹，构建防篡改的链式数据结构。

在6G网络身份管理中，区块链技术可构建去中心化认证系统，用户身份信息经加密后存储于区块链，通过智能合约实现身份验证与授权。该技术能完整记录网络安全事件及

处理流程，实现安全信息共享与溯源。当遭受网络攻击时，可基于区块链快速追踪攻击源与路径，为安全响应提供决策依据。区块链可建立激励机制，对安全设备提供商、安全服务商等进行奖励。在6G安全防护中，节点发现威胁后可通过区块链实现信息全网共享，形成协同防御机制，并对积极参与防护的节点实施奖励，提升整体防护积极性。

华为2023年技术白皮书显示，其MPBFT-v2算法在50节点集群测试中实现了平均9.8 ms的共识延迟。华为6G白皮书提出通过将高频交易分流至边缘链处理，并采用侧链与主链异步同步的技术方案，可使系统吞吐量提升至12万TPS（每秒事务处理量）。这些区块链技术的突破为6G网络中下沉边缘节点构建去中心化身份认证系统提供了技术支撑。

4.2.2 PKI/DPKI

公钥基础设施（PKI）基于非对称加密技术构建信任体系，通过公钥加密和数字证书机制建立信任域。针对6G网络特性，DPKI展现出更优的适应性。DPKI采用分布式证书颁发机构和密钥管理中心，实现证书的分布式管理与验证。在跨域通信场景中，DPKI通过建立信任锚和证书链，有效解决不同信任域间的证书互信问题[20]。在6G网络中，当不同运营商网络需互联通信时，可依托DPKI技术实现安全的跨域身份认证与密钥交换，从而保障通信过程的安全性和可靠性。

4.3 安全功能

4.3.1 身份认证

针对6G网络中多样化业务终端的接入需求，需采用多模态身份认证技术，该技术融合生物特征识别、密码学技术以及行为特征分析，实现对用户及设备的精准身份认证。在物联网设备接入场景中，面对海量设备、有限资源及复杂环境等挑战，多模态身份认证技术能显著提升认证准确性与安全性，有效阻止非法设备接入，保障物联网系统稳定运行。通过分析物联网设备行为特征，结合设备指纹识别与数字证书认证，可确保仅合法设备接入6G网络，防止物联网设备遭受攻击与控制。

4.3.2 空天地一体化接入安全

空天地一体化网络通过融合卫星通信、高空平台通信和地面移动通信，实现全球无缝覆盖，同时面临多重安全挑战，其网络架构如图3所示。由于不同接入方式的网络特性差异显著，安全协议难以实现统一标准化。卫星通信链路存在易受干扰和窃听的风险，且卫星节点受限于计算和存储资源，难以支持复杂安全算法的部署。高空平台通信则面临平台移动性和定位精度问题，可能影响通信稳定性与安全性。

针对这些挑战，需构建统一的安全接入架构，开发适用于各类接入方式的轻量级安全协议。通过软件定义网络（SDN）和网络功能虚拟化（NFV）技术，实现对网络的集中化安全管理和动态资源调度。SDN控制器可实时监测网络流量与安全状态，根据接入需求和安全风险动态调整安全策略与资源分配，从而保障网络的安全稳定运行。

4.3.3 安全连接

在6G网络中，安全连接是实现数据可靠传输的核心保障。基于机器学习的智能路由协议通过实时分析网络拓扑、流量负载、链路质量和安全风险等多维度数据，动态优化路

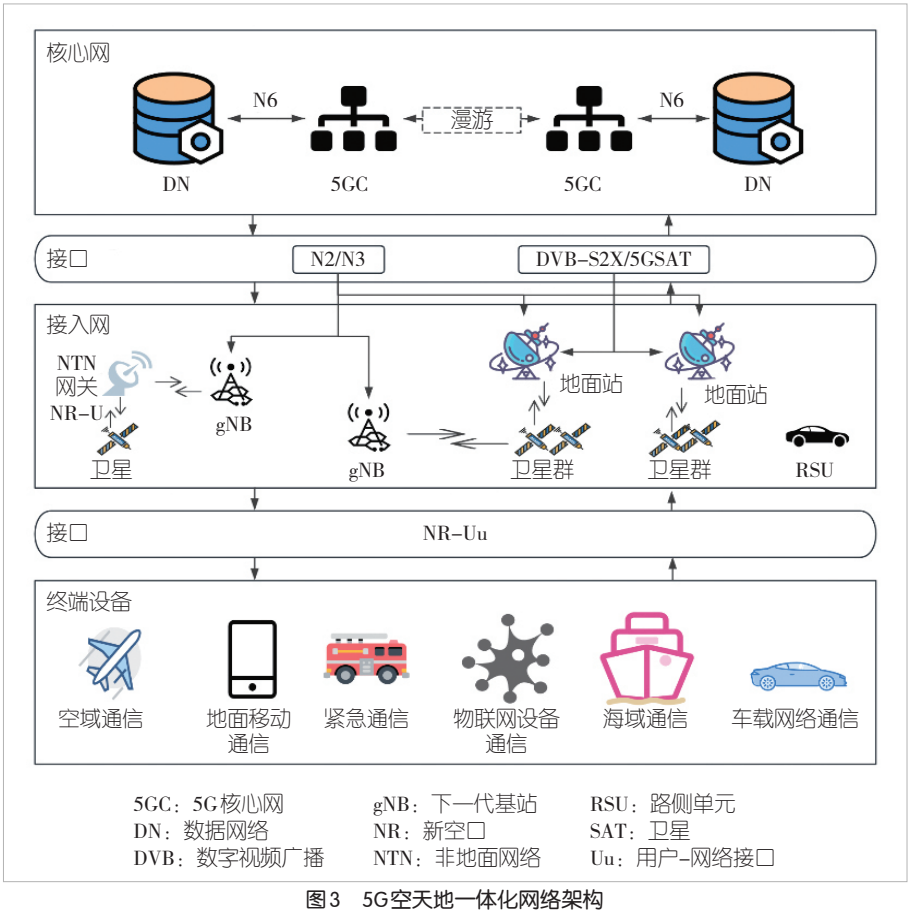


图3 5G空天地一体化网络架构

由策略，智能规避拥塞链路和安全威胁区域，确保数据传输的高效性与安全性。当检测到链路异常或遭受攻击时，该协议可快速切换至备用路径，维持数据传输连续性。

基于IPv6的段路由（SRv6）作为新型网络层协议，利用IPv6报头中的段列表实现灵活的源路由控制。在6G网络中，SRv6通过与安全策略深度集成，对段列表实施加密和验证，确保传输路径的安全可溯[21]。该协议还支持网络切片的安全隔离，通过差异化段列表路由各切片流量，有效阻断切片间安全风险传播，保障业务系统的独立安全运行。

5 结束语

当前6G网络安全研究虽取得阶段性成果，但仍面临诸多挑战。未来研究需重点关注以下方向：首先，需深入探究量子通信与人工智能等新兴技术融合引发的复合型安全风险；其次，应加强6G安全架构与垂直行业个性化需求的适配性研究，针对金融、医疗、工业等领域特有的安全需求开发定制化解决方案；最后，面对持续演进的网络攻击手段，需通过持续的技术创新提升6G网络动态防御能力，推动安全技术体系的迭代升级。

参考文献

[1] AKYILDIZ I F, KAK A, NIE S. 6G and beyond: the future of wireless communications systems [J]. IEEE access, 2020, 8: 133995–134030. DOI:10.1109/ACCESS.2020.3010896

[2] European Commission. Horizon 2020: work programme 2018—2020 [R]. 2018

[3] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges [J]. IEEE communications surveys & tutorials, 2021, 23(4): 2384–2428. DOI: 10.1109/COMST.2021.3108618

[4] KIM J, LEE J, KO H, et al. Space mobile networks: satellite as core and access networks for B5G [J]. IEEE communications magazine, 2022, 60(4): 58–64. DOI: 10.1109/MCOM.001.2100770

[5] IMT–2030(6G)推进组. 6G可信内生安全架构研究报告 [R]. 2022

[6] IMT–2030(6G)推进组. 6G网络架构愿景与关键技术展望白皮书 [R]. 2022

[7] 季新生. 6G内生安全可信技术白皮书 [R]. 网络通信与安全紫金山实验室, 2023

[8] 武巧荣. GSM系统中主要安全威胁防范机制的分析与设计 [D]. 北京: 北京邮电大学, 2011

[9] 安华萍, 贾宗璞. 3G移动网络的安全问题 [J]. 科学技术与工程, 2005, 5(6): 375–377, 381. DOI: 10.3969/j. issn. 1671–1815.2005.06.013

[10] 胡鑫鑫. 5G网络认证协议和非接入层协议安全性研究 [D]. 郑州: 战略支援部队信息工程大学, 2020. DOI: 10.27188/d. cnki. gzjxu.2020.000006

[11] BASIN D, DREIER J, HIRSCHI L, et al. A formal analysis of 5G authentication [C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018: 1383–1396. DOI: 10.1145/3243734.3243846

[12] HUSSAIN S R, ECHEVERRIA M, KARIM I, et al. 5G Reasoner: a property–directed security and privacy analysis framework for 5G cellular network protocol [C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2019: 669–684. DOI: 10.1145/3319535.3354263

[13] GSMA. Mobile security research acknowledgements [EB/OL]. [2025–03–25]. https://www. gsma. com/security/gsma mobile–security–research–acknowledgements/

[14] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges [J]. IEEE communications surveys & tutorials, 2021, 23(4): 2384–2428. DOI: 10.1109/COMST.2021.3108618

[15] 粟栗, 庄小君, 杜海涛, 等. 6G网络内生安全架构研究 [J]. 中国科学: 信息科学, 2022, 52(2): 205–216

[16] XU H, KLAINE P V, ONIRETI O, et al. Blockchain–enabled resource management and sharing for 6G communications [J]. Digital communications and networks, 2020, 6(3): 261–269. DOI: 10.1016/j.dcan.2020.06.002

[17] YLIANTTILA M, KANTOLA R, GURTOV A, et al. 6G white paper: research challenges for trust, security and privacy [EB/OL]. [2025–03–22]. https://arxiv.org/abs/2004.11665v2

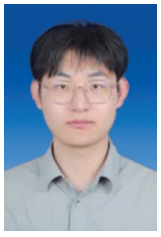
[18] LETAIEF K B, SHI Y M, LU J M, et al. Edge artificial intelligence for 6G: vision, enabling technologies, and applications [J]. IEEE journal on selected areas in communications, 2022, 40(1): 5–36. DOI:10.1109/JSAC.2021.3126076

[19] HAJOMER A A E, BRUYNSTEEN C, DERKACH I, et al. Continuous–variable quantum key distribution at 10 GBaud using an integrated photonic–electronic receiver [J]. Optica, 2024, 11(9): 1197. DOI: 10.1364/optica.530080

[20] WANG C X, YOU X H, GAO X Q, et al. On the road to 6G: visions, requirements, key technologies, and testbeds [J]. IEEE communications surveys & tutorials, 2023, 25(2): 905–974. DOI: 10.1109/COMST.2023.3249835

[21] FILSFILS C, CAMARILLO P, LEDDY J, et al. Segment routing over IPv6 (SRv6) network programming [EB/OL]. [2025–03–22]. https://www.rfc–editor.org/info/rfc8986

作　者　简　介



罗涵一，北京邮电大学计算机学院在读硕士生；主要研究方向为移动蜂窝网络安全。

崔宝江，北京邮电大学网络空间安全学院教授，博士生导师；主要研究方向为软件缺陷测试分析、智能信息检测、异常行为大数据分析、移动通信网和卫星互联网技术等；作为项目负责人承担国家重点研发计划等项目10余项；发表论文257篇，获授权专利64项。

仝鑫，北京邮电大学网络空间安全学院在读博士研究生；主要研究方向为人工智能、隐私保护等；发表论文2篇，获授权专利1项。