

面向全服务化网络的安全、隐私、可信及韧性综述

平子键¹, 王明君¹, 闫峥^{1,2}, 王海光³, 李铁岩³

(1. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126;

2. 空天地一体化综合业务网全国重点实验室, 陕西 西安 710071;

3. 华为技术有限公司谢尔德实验室, 广东 东莞 523808)

摘要: 服务化架构是5G核心网的重要创新, 其通过将传统紧耦合的网元拆分为松耦合、可重用、独立部署的网络功能, 并通过标准化服务接口灵活调用, 实现了网络的云原生、模块化、弹性扩展和开放性。然而, 服务化的开放性和灵活性扩大了移动网络安全和隐私的威胁面。近年来, 面向服务化移动网络的安全和隐私保护的研究和标准化工作方兴未艾。然而, 现有工作缺乏系统性梳理服务化移动网络安全相关学术进展和研究脉络的调研工作。为此, 面向全服务化移动网络, 对安全、隐私、可信及韧性开展了系统化调研。首先, 系统分析移动核心网、接入网以及用户终端所面临的安全与隐私风险, 并全面总结服务化网络的核心安全需求。在此基础上, 提出一个面向全服务化网络的四维可信服务化网络评价指标体系。应用该评价体系, 对现有研究和标准化工作进行全面系统的分析和对比, 揭示现有服务化网络存在的缺乏统一安全架构、安全策略易冲突以及AI安全保障缺失等严重的开放性问题, 并指出未来研究方向, 旨在为学术界和工业界提供有价值的理论和技术参考, 助力下一代移动通信网络的健康与安全发展。

关键词: 下一代移动通信网络; 服务化架构; 安全防护; 隐私保护; 信任管理; 系统韧性

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.AQ25304

Security, privacy, trust and resilience in the service-based mobile networks: a comprehensive survey

Ping Zijian¹, Wang Mingjun¹, Yan Zheng^{1,2}, Wang Haiguang³, Li Tieyan³

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

2. National Key Laboratory of Integrated Services Networks, Xi'an 710071, China

3. Trusted Technology Laboratory, Shield Lab, Huawei Technologies Co., Ltd., Dongguan, 523808

Abstract: The service-based architecture (SBA) represents a pivotal innovation of the 5G core networks. It decouples traditionally tightly coupled network elements into loosely coupled, reusable, and independently deployable network functions (NF), which can be flexibly invoked via standardized service-based interfaces (SBI). This paradigm enables cloud-native deployment, modular design, elastic scaling, and open interoperability of mobile networks. Nevertheless, the openness and flexibility introduced by SBA also expand the threat surface for network security and user privacy. Recently, research efforts and standardization activities concerning security and privacy

收稿日期: 2025-12-25; 修回日期: 2026-05-03

通信作者: 王明君, mjwang@xidian.edu.cn

基金项目: 国家自然科学基金资助项目 (No. U23A20300); 华为-西电技术合作项目 (No.HX01202011024, No.HX01202408049)

Foundation Items: The National Natural Science Foundation of China (No. U23A20300), Huawei-Xidian University Research Cooperation Project (No.HX01202011024, No.HX01202408049)

preservation for SBA mobile networks have been vigorously advanced. However, there still lacks a systematic survey that comprehensively sorts out the academic advances and research trajectories in this field. To fill this research gap, this paper conducts a systematic survey covering security, privacy, trustworthiness, and resilience issues in fully SBA networks. Firstly, we thoroughly analyzed the security and privacy risks faced by three main components of the mobile networks, i.e., the core network, the access network, and the user terminals, and summarized the key security and privacy requirements of the networks. Then, we proposed the four-dimensional trustworthiness evaluation criteria system (4DTECS), specifically designed for SBA network. By adopting 4DTECS, we performed a comprehensive analysis and investigation on existing academic research and standardization efforts. Furthermore, we identify several critical open challenges and outline some promising future research directions, aiming to provide valuable theoretical insights and technical references for academia and industry, and facilitate the sound and secure evolution of next-generation mobile communication networks.

Key words: next-generation mobile communication network, holistic service-based architecture, security protection, privacy preservation, trust management, resilience

0 引言

服务化架构 (service-based architecture, SBA) 是一种以软件服务为核心构建系统的方法, 其核心思想是将传统的、紧耦合的网络功能 (network function, NF) 拆分为一系列独立的、可复用的网络功能服务 (NF services)^[1]。每个服务通过基于 HTTP/2 等协议的标准化表述性状态传递应用程序接口 (RESTful API) 进行通信, 并能被动态发现和调用^[2]。该架构实现了网络功能的解耦与接口开放, 是 5G 核心网实现云原生化和灵活性的关键技术。

截至 2025 年年底, 基于服务化架构 (service based architecture, SBA) 的 5G 网络已成为全球 5G 独立组网 (standalone, SA) 的主流架构, 在技术演进和商业化部署方面取得显著进展。根据全球移动供应商协会 (global mobile suppliers association, GSA) 的最新报告^[3], 全球已有 163 家运营商在 65 个国家和地区投资 5G SA 网络, 其中 73 家运营商已在 40 个国家正式或软启动 5G SA 商用网络, 覆盖北美、欧洲、亚太、中东等地区。中国已经建成全球最大 5G SA 网络, 拥有 80% 的 5G SA 网络覆盖率。

当前, 全球通信产业正加速向 5G-Advanced (5.5G) 演进, 并全面启动 6G 技术研究。在网络架构层面, SBA 正朝着全服务化架构 (holistic service-based architecture, HSBA) 深化演进^[4]。HSBA 是对 5G SBA 的继承与发展, 其目标是构建一个支持智能内生、安全内生、跨域融合的更

加灵活和强大的网络基础。移动网络通过服务化设计, 支持功能的动态编排和快速组合, 显著提升了网络灵活性, 以高效响应多样化业务需求。HSBA 进一步增强了场景适应能力, 依托端到端云化和服务化架构, 能够精准匹配差异化、碎片化场景, 提供个性化、定制化的按需服务^[5-6]。在性能与效率方面, 6G 要求时延优化至微秒级, 以保障高可靠性与实时交互能力。HSBA 通过云化实现资源的动态共享与高效利用, 大幅提升资源利用率。此外, 服务化架构通过深度融合人工智能技术, 赋予网络自组织、自优化和智能决策能力, 推动通信网络向智能化、融合化的信息服务全面演进^[7-8]。

在标准化方面, 国际标准化组织 ITU 和 3GPP 均在其技术愿景和研究中强调了 SBA 持续增强的重要性^[9]。3GPP 已完成 Release 15 至 Release 19 的 SBA 演进, 目前正在开展 Release 20 和 Release 21 的标准化工作。其中, Release 18 进一步完善 SBA 安全机制, 并研究零信任、可信计算、区块链等新技术在 SBA 中的应用, 以构建多维可信评估体系服务化以及服务化的证书管理; Release 19 和 Release 20 在用户平面功能 (user plane function, UPF) 的服务化^[10]、安全最佳实践^[11]以及自动化证书管理环境 (automated certificate management environment, ACME) 的服务化方面^[12]正在开展相关研究。

此外, 国内外移动运营商以及设备提供商等也在积极推动 SBA 的发展和演进。《中国移动 5G 服务化架构 (SBA) 白皮书》^[13-14]中提出 “三体-

四层-五面”的6G总体架构，明确了HSBA的核心地位，旨在将服务化理念拓展到用户面、接入网以及用户端等多个网络结构，并进一步深化服务机制、优化服务设计、提升服务化接口效率，从而全方位提升服务化能力。华为在《广域网络服务化白皮书》^[15]中首次提出了广域网络服务化的概念，定义了广域网络服务化的设计理念和众多应用场景，使SBA从标准化的服务调用平台逐步转型为智能化和场景化的核心网络中枢。上述进展不仅验证了SBA作为全球统一架构的成熟度，也为6G的进一步演进奠定了坚实的技术基础。

全服务化架构在推动通信技术迈向新高度的同时，也面临着诸多新型安全风险^[16]。首先，SBA开放性与复杂性导致攻击面扩大。服务化架构高度依赖开放的应用程序编程接口（application programming interface, API）进行通信，这使得API本身成为首要攻击目标，易遭受注入、未授权访问等攻击；同时，NF被拆分为细粒度的微服务，微服务间频繁的交互显著增加了东西向通信被窃听或篡改的风险；此外，服务编排与动态调度引入了新的脆弱点，攻击者可能通过恶意操纵编排策略来破坏服务链的完整性。其次，身份管理、访问控制与控制层面的安全挑战加剧。在动态分布式环境中，NF的实例化、发现与认证过程变得异常复杂，如何确保NF与NF，NF

与服务通信代理（service communication proxy, SCP）之间的双向可信认证是关键挑战；此外，细粒度访问控制难度陡增，传统的粗粒度权限模型难以适应微服务间精细的授权需求，令牌滥用或权限提升风险突出；跨域服务调用时，统一的身份管理与信任传递机制若存在缺陷，极易导致安全策略失效。再次，SBA的内生安全与动态可信保障机制存在不足。服务链的端到端安全传输难以保障，在请求经过多个SCP转发时，机密性与完整性面临挑战；架构的可观测性与安全监控能力不足，在复杂调用链中难以快速实施故障定位、入侵检测与取证。最后，新技术融合引入叠加风险。例如，未来的SBA可能依赖AI实现智能运维与安全调度，但AI模型自身面临投毒、逃逸与推断攻击的威胁，其决策可靠性可能被破坏；若未来引入区块链技术用于服务交易与审计，其智能合约漏洞和性能瓶颈也可能成为新的攻击入口。综上所述，全服务化架构面临的安全风险已从传统的网络边界威胁，转向针对开放化接口、统一身份管理、访问控制、可信防护、新技术融合的新型威胁矩阵，其安全保障需贯穿于服务设计、部署、通信与管理的全生命周期。

当前，已有大量关于5G和6G网络以及服务化发展的国内外调研工作，服务化网络调研论文总结与对比见表1。Dogra^[17]、Quy^[18]、Jiang^[19]、

表1 服务化网络调研论文总结与对比

调研方向	服务化调研论文	主要调研内容
6G网络架构、服务化架构、O-RAN架构演进	文献[17-21]	调研从5G到6G的服务化架构演进、技术、应用场景及挑战，阐述如何通过服务化、虚拟化、智能化等手段实现网络的灵活部署、高效管理和多样化应用支持
	文献[22-25]	调研O-RAN架构中的网络切片服务化、AI/ML应用、可解释AI（XAI）以及智能化手段在无线网络资源管理和服务水平提升中的作用
	文献[26-28]	调研6G网络中集成地面和非地面网络的虚拟化技术，以及AI、ML、IoE在服务化架构中的深度集成与零接触网络自动化管理
服务化架构以及安全隐私	文献[29]	调研6G网络的架构、协议、安全和隐私问题，以及标准化途径，探讨了6G网络中的安全和隐私风险，并提出了相应的缓解策略
	文献[30]	调研6G网络中服务化架构的演变、安全和隐私需求、面临的挑战以及相关的防御策略
	文献[31]	调研6G网络中的服务化架构及其带来的安全性和隐私保护挑战
	文献[32]	调研6G网络中服务化架构的安全性和信任问题，详细分析了O-RAN在6G网络中的应用，以及如何利用区块链和零信任架构来增强O-RAN的安全性和韧性
	文献[33]	调研FL在5G和6G网络中的应用安全
全服务化网络、安全、隐私、可信、韧性	本文	全面分析全服务化网络面临的安全、隐私威胁，制定四维可信服务化网络评价指标体系，评估标准化工作和学术论文方案的安全、隐私、可信和韧性

Wang^[20]、Akgul^[21]等主要从服务化架构、虚拟化、智能化等角度探讨了从 5G 到 6G 的网络演进、灵活部署与高效管理。Yeh^[22]、Nguyen^[23]、Brik^[24]、Niknam 等^[25]聚焦开放无线接入网 (open radio access network, O-RAN) 架构中的网络切片、AI/机器学习 (ML) 应用、可解释 AI 及智能化资源管理。Ammar^[26]、Prasad^[27]、Coronado^[28]等主要调研了 6G 中 AI/ML、万物互联 (IoE) 的深度集成、虚拟化技术及零接触自动化管理。也有部分调研工作涉及服务化架构安全与隐私。例如, Yang 等^[29]系统调研了从 5G 到 6G 演进中的安全、隐私及标准化路径, 详细分析了 6G 网络架构、协议、安全隐私风险, 并提出了相应的缓解策略和标准化建议。Nguyen 等^[30]对 6G 网络中的安全隐私问题进行了全面调查, 详细分析了服务化架构的演变过程、安全需求、面临的挑战以及相关的防御策略。Farao 等^[31]深入研究了 6G 网络中的网络安全挑战和陷阱, 重点关注服务化架构带来的安全性和隐私保护问题。Abou El Houda 等^[32]研究了区块链技术与 O-RAN 的融合, 分析了 O-RAN 在 6G 网络中的应用, 提出基于区块链和零信任架构的安全韧性框架来解决服务化架构的安全信任问题。Blika 等^[33]全面综述了联邦学习在 5G 和 6G 网络中的应用与安全, 探讨了通过联邦学习 (federated learning, FL) 增强服务化架构的网络安全性和可信度。

虽然上述调研工作以及 3GPP 和 O-RAN 标准从不同角度探讨了服务化架构的技术实现、应用场景和安全挑战, 但是现有工作在系统性整合 5G/6G 网络全服务化架构的安全、隐私、可信与韧性 4 个维度方面仍存在明显不足。具体来说主要有: ① 3GPP 的安全标准主要围绕传统接入认证、核心网安全及用户隐私, 注重静态安全机制的设计与部署, 对动态可信评估、AI 内生安全等新兴需求覆盖不足; ② O-RAN 虽然在安全规范中借助开放化架构引入第三方应用安全、接口安全等机制, 但其安全设计更多聚焦于接入网开放化带来的新型攻击面, 在第三方动态评估、AI 模型自身安全及跨域协同方面仍存在明显缺口; ③ 6G 网络新增了对韧性的迫切需求, 上述现有标准与相关调研工作对系统韧性的考量严重不

足, 例如, 3GPP 安全标准仅零星涉及快速恢复机制, 缺乏对自适应能力、AI 鲁棒性、服务链可靠性等韧性指标的统一定义与评估方法; ④ O-RAN 安全规范虽在架构层面引入了弹性设计, 但尚未形成系统性的韧性保障框架。

因此, 本文面向移动网络向全服务化架构演进的技术发展趋势, 全面系统地分析全服务化架构下移动网络面临的安全漏洞和威胁, 为 6G 网络提供全面的安全和可信评估框架。本文的主要贡献如下。

(1) 提出了一个面向下一代全服务化网络的四维可信服务化网络评价指标体系。该体系从安全、隐私、可信和韧性 4 个维度系统性地构建了共计 32 项可综合评估的指标来评价网络的可信性, 该体系针对现有研究在服务化网络可信性综合评估方面的不足, 提供了系统的评估维度和量化参考示例, 为 6G 网络“智能内生、安全内生”愿景的实现提供了系统性的理论支撑和可落地的评估基准。

(2) 系统梳理了 3GPP、O-RAN 联盟及国内外运营商在服务化安全领域的标准化工作, 并采用四维可信服务化网络评价指标体系对各标准化中的安全、隐私、可信和韧性进行全面的梳理和分析。通过逐一评估各标准化工作在安全、隐私、可信、韧性 4 个维度上的覆盖情况, 揭示了现有标准的显著差异与共性不足, 例如: 3GPP 标准在安全与隐私方面较为完善, 但对韧性维度的系统性考量不足; O-RAN 规范在接口开放性与信任管理方面有创新, 但隐私保护机制仍有待深化等。这一系统性的对比分析, 为学术界理解标准演进脉络以及产业界识别标准化不足提供了清晰的指引。

(3) 采用四维可信服务化网络评价指标体系分别从网络安全架构、身份与证书管理、网络攻击检测、O-RAN 安全与冲突管理、终端设备安全以及应用场景安全 6 个角度对服务化研究工作进行深入的评价, 应用上述评价指标体系, 对每一项工作的安全防护能力、隐私保护水平、可信保障机制和系统韧性表现进行了细致的定性描述与指标覆盖度分析。更重要的是, 本文还设置了专门的对比分析段落, 从技术路线选择、设计理念侧重、应用场景约束、资源开销考量等方面,

解释了不同工作在指标覆盖上存在差异的根本原因，为后续研究工作提供指导。

(4) 基于可信指标体系的评估结果，总结出下一代全服务化网络在安全、隐私、可信和韧性等方面的五大核心开放问题，即：①统一安全架构缺失导致的碎片化风险；②网络态势感知滞后与动态策略冲突引发的安全盲区；③数据壁垒与隐私计算效率困境制约的跨域协同；④服务链端到端可靠性保障不足带来的级联故障隐患；⑤AI/ML模型自身安全脆弱性引发的智能系统信任危机。针对上述每一个开放问题，本文均结合具体研究案例和数据论证其严重性与紧迫性，并提出了与五大问题一一对应的5个未来研究方向，即：①构建覆盖四维需求的高可信网络安全架构；②研发动态可信管理与实时威胁感知技术；③突破多维度协同隐私计算体系；④构建自主可控、弹性可扩展的服务链可信执行体系；⑤攻克AI模型抗干扰、可解释、可验证等可信AI关键技术。这些研究方向旨在为学术界提供清晰的技术攻关路径，为产业界和标准化组织提供有价值的技术参考，最终推动6G网络“智能内生、安全内生”愿景的全面实现。

1 服务化标准工作与安全、隐私、可信和韧性需求分析

1.1 现有服务化标准工作

1.1.1 3GPP

截至2025年6月底，3GPP在5G服务化架构标准化方面已完成从Release 15到Release 19的完整演进。Release 15首次提出了5G核心网的服务化，奠定了基于NF间服务调用的基础安全模型。Release 16推进了SBA架构的安全性增强。新的NF用例基于现有SBA安全机制（如基于令牌的授权），无须改动，实现对整体安全架构的前向兼容。Release 17和Release 18在SBA网络中引入了SCP间接通信，增强了SBA的适用性。SCP成为实现从Release 15 SBA向Release 18及后续架构平滑过渡的关键使能器，并能提供安全隔离功能，适用于包含不同信任域的网络切片和NF的多信任域环境。然而，SCP的引入使得5G核心网的安全性过于依赖SCP的安全。相关研究

聚焦于如何通过SCP实现信令消息的端到端保护，以及NF消费者（NFc）对NF生产者（NFp）的认证机制。标准明确要求，间接通信的使用前提是SCP的绝对可信，以在保障安全的同时充分发挥SCP带来的优势。Release 19正在开展UPF服务化的标准化工作，旨在更好地将UPF集成到控制面中。例如，增强应用功能（application function, AF）与5GC之间的接口安全，以支持UPF对数据分组头的处理以及相关的报告/通知机制等。这可以看作SBA安全原则向用户面管理功能领域的延伸。当前，3GPP正推进Release 20和Release 21的工作，其中重点推动SBA在UPF的服务化演进^[10]、SBA架构安全最佳实践的探索^[11]以及ACME系统的服务化演进^[34]。

1.1.2 O-RAN联盟与AI-RAN联盟

O-RAN联盟是一个面向下一代无线接入网（radio access network, RAN）开放化、虚拟化和智能化演进的标准化组织。自成立以来，O-RAN联盟在服务化标准方面不断取得显著进展，通过持续制定和完善技术规范，已发布多版本规范涵盖服务管理和编排、RAN智能控制、开放式前传等架构各环节^[35]，例如，O-RAN联盟分别在2021年到2024年，分阶段开启了Release 1到Release 4版本规范的立项和迭代。同时，O-RAN也不断推进开源软件版本演进^[36]，O-RAN软件社区从2022年的第5版、第6版软件，到2025年计划推出的“Release H”版本软件，不断强化功能的集成与优化。在技术应用与创新上，O-RAN联盟于2024年在AI驱动的网络管理方面成果颇丰，2025年利用近实时无线接入网智能控制器（near-real-time RAN intelligent controller, near-RT RIC）中的Python和AI/ML算法开发节能方案^[37]。在测试与认证方面，开放测试与集成中心不断扩展，O-RAN联盟和开放测试与集成中心（OTIC）合作推行认证和徽章颁发计划，推动产品商业化和互操作性^[38]。此外，还积极与行业其他标准化组织达成合作，共同推动RAN开放和创新。2025年3月，O-RAN联盟与3GPP协同推进6G统一愿景^[39-40]，明确了双方在6G规范制定中的角色和协作方式，此前也与众多标准化组织达成合作共识，共同推

动全球 O-RAN 标准和产业生态的发展,致力于构建更加开放、智能和高效的无线网络架构^[41]。

AI-RAN 联盟于 2024 年在西班牙巴塞罗那世界移动通信大会 (MWC2024) 期间正式成立,由亚马逊云科技、ARM、爱立信、微软、诺基亚、英伟达、三星等 11 家科技企业与机构共同发起,旨在通过整合人工智能技术与蜂窝通信网络,提升无线接入网效率,推动下一代移动通信网络的智能化发展。AI-RAN 将重点在 3 个领域开展研究工作 (即 AI for RAN、AI and RAN、AI on RAN),以提升下一代无线接入网的性能、降低开销、激发新服务能力和提高网络智能水平^[42]。

1.1.3 国内外运营商

近年来,国内外电信运营商也在不断推动下一代网络的服务化进程。

截至 2025 年 6 月底,中国移动在 5G 服务化架构^[14]领域保持全球领先地位,不仅主导了 3GPP 中 5G SBA 标准的制定,还建成了全球最大的 5G SA 商用网络^[43],覆盖全国所有县级以上区域,5G 用户数突破 12 亿^[44]。在 5G-Advanced 阶段,中国移动重点推进无源物联网、RedCap 轻量化 5G 等创新技术^[45],实现终端成本降低 50%~65%,并在工业互联网、智慧矿山等领域落地典型应用。同时,中国移动积极布局 6G 全服务化架构研究^[46-47],参与 IMT-2030^[48]推进组工作,推动通感算智一体化发展,为下一代网络演进奠定基础。中国电信也在 5G SBA 领域取得突破性进展,已在 150 个重点城市规模部署 5G-A 网络^[49],建成约 7 万个基站,5G-A 用户突破 1 000 万。通过“智聚大上行”^[50]技术实现上行速率提升 15%、时延降低 30%,并完成全球首个全频段 RedCap 商用验证,模组成本降低 80%。在行业应用方面,重庆“万兆工厂”、京沪高铁 5G-A 网络^[51]和武汉光谷通感一体化^[52]等标杆项目成效显著。同时,中国电信积极参与 3GPP 标准制定,推动“超级上行”等技术创新^[53],并联合华为成立 5G-A 实验室,为 6G 全服务化架构演进奠定基础,持续巩固其在全球 5G 创新中的领先地位^[54]。

在国际方面,欧美主流运营商也在积极部署

5G SA 网络并探索新技术。英国运营商 EE 在 2025 年年底加速部署 5G 独立组网 (5G SA) 服务后,于 2026 年 4 月 28 日宣布其 5G+ 网络已覆盖英国 610 多个城镇的超 5 000 万用户,超额完成了原定 2026 年春季覆盖 4 100 万人的目标。EE 还推出了全球首家基于爱立信高级无线接入网协调 (advanced RAN coordination, ARC) 产品的站点间 5G 载波聚合,能够将多个独立基站的闲置容量整合,使下行数据传输性能平均提升 20%。沃达丰西班牙公司选择爱立信作为其主要技术合作伙伴,提供基于 5G Core 双模平台的 5G SA 核心网络,2025 年年底已覆盖 90% 的人口和 3 700 多个城市。西班牙电信 (Telefonica) 在 MWC2025 上宣称完成欧洲首例 5G SA 通话测试,采用诺基亚 Cloud RAN 解决方案并运行于亚马逊云科技 (AWS) 云端基础设施上,推动电信产业云端化网络转型。美国运营商中,AT&T 和 Verizon 均于 2025 年启动各自的 5G SA 网络。

全球运营商正致力于通过网络功能虚拟化 (network functions virtualization, NFV)、云原生架构和人工智能等技术提升网络灵活性和效率。例如,Verizon 与风河公司等合作,成功实现了全球首次端到端完全虚拟化 5G 数据会话,采用了基于容器且采用标准化接口的虚拟化架构。这些努力共同推动着电信网络向更加开放、智能和高效的方向演进,为 5G-A 和 6G 未来的发展奠定基础。

1.2 服务化标准中的安全、隐私、可信需求

本节将详细分析 3GPP、O-RAN 联盟、运营商等开展的服务化标准工作中涉及的安全、隐私、可信以及韧性的需求。

1.2.1 3GPP

3GPP 在 TS 33.501^[55]中详细制定了关于服务化网络的安全、隐私、可信以及韧性的需求,接下来分别从上述 4 个方面进行整理和总结。

(1) 安全需求

保密性 (S1): 通过多种加密机制保障信令和用户数据的安全。例如,TS 33.501 第 6.4.4 节规定了非接入层 (non-access stratum, NAS) 信令加密的算法,确保 NAS 信令的机密性。此外,第 5.2.2、5.3.2、5.5.1 节及第 6.5.2、6.6.3 节也涉

及用户设备（UE）/基站（gNB）/接入和移动性管理功能（AMF）对用户面和无线资源控制（RRC）的加密要求。

完整性（S2）：通过多种加密算法和机制保障信令和通信数据的完整性。例如，TS 33.501第6.4.3节规定了NAS完整性保护流程，完整性激活时同步激活重放保护。此外，第5.2.3、5.3.3、5.5.2节及第6.5.1、6.6.4节也涉及用户设备（UE）/基站（gNB）/接入和移动性管理功能（AMF）对用户面和无线资源控制（RRC）的完整性要求。

可用性（S3）：确保系统和数据在授权用户需要时能够正常访问和使用。例如，TS 33.501第5.9.3.2节要求安全边缘保护代理（security edge protection proxy, SEPP）实施速率限制功能，以防御过量信令攻击，保护自身及后续网络功能免受信令风暴影响；此外，第5.9.3.4节涉及从用户层面保障可用性，第6.8.1.1节涉及安全上下文的存储与恢复机制，确保UE在状态转换时的服务连续性。

双向认证（S4）：围绕双向认证机制和密钥协商协议确保用户设备与网络的合法身份相互验证。例如，TS 33.501第6.1节详细规定了5G认证与密钥协商（authenticated key agreement, AKA）和EAP-AKA'两种认证方法的完整流程，包括认证向量生成、挑战一响应机制、密钥派生及相互认证。此外，第5.1.2节也规定了订阅认证、服务网络认证等基础要求。

密钥管理（S5）：建立严格的密钥管理体系来保障密钥的安全存储以及密钥分离机制。例如，TS 33.501第6.2节定义了完整的密钥层级及派生规则，确保密钥分离与算法绑定。此外，第5.1.3、5.2.4、5.3.5、5.8.1节也涉及密钥长度、安全存储等要求。

安全的可见性与配置性（S6）：提供对安全状态的实时监控和灵活配置能力，便于安全运维。例如，TS 33.501第5.10.1节要求UE向应用层提供每协议数据单元（protocol data unit, PDU）会话粒度的安全信息，包括接入层（access stratum, AS）机密性（加密算法、承载信息）、AS完整性（完整性算法、承载信息）、NAS机密性（加密算法）、NAS完整性（完整性算法）以及服

务网络标识符；第5.10.2节允许用户配置全球用户识别卡（universal subscriber identity module, USIM）访问权限等基础设置；此外，第5.9.2.2节要求网络存储功能（network repository function, NRF）作为授权服务器，支持基于角色的策略配置，体现了配置性的部分实现。

端到端安全（S7）：通过全路径加密和切片安全隔离实现通信全链路保护。例如，TS 33.501第5.9.3节要求SEPP提供源和目的网络之间特定消息元素的端到端机密性和完整性保护。此外，第6.1.1.3节也涉及锚密钥绑定到服务网络的机制。

重放保护性（S8）：通过序列号、时间戳等机制确保接收方能够识别并拒绝重复或延迟的旧消息。例如，TS 33.501第6.4.3.2节规定完整性激活时同时激活重放保护，接收方只接受每个NAS COUNT值一次。此外，第5.3.3、5.5.2、5.9.2.1、5.9.3.1节也涉及用户面、NAS、服务发现、互联场景的重放保护。

虚拟化隔离（S9）：通过硬件级安全隔离和侧信道攻击防护确保虚拟化环境安全。例如，TS 33.501第5.3.8节定义了gNB中安全环境的逻辑边界，要求支持敏感数据的安全存储、敏感功能执行、安全启动、完整性保证和授权访问。此外，第5.2.4、5.8.1节也涉及UE和统一数据管理（UDM）的安全环境要求。

细粒度授权与访问控制（S10）：基于动态策略对网络功能或服务进行最小权限的精准授权管理。例如，TS 33.501第13.4节定义了基于OAuth 2.0框架的NF服务访问的授权流程，包括令牌请求、令牌验证、作用域管理等。此外，第5.9.2.1、5.9.2.3节也涉及NRF和网络开放功能（network exposure function, NEF）的授权要求。

空口安全（S12）：通过用户身份保护和强制完整性保护强化无线接口防护。例如，TS 33.501第6.12节详细规定了用户隐藏标识符（SUCI）的构造、5G-全局唯一临时标识符（GUTI）的分配与更新机制，保护用户身份在空口的机密性。此外，第5.2.2、5.2.3、5.3.2、5.3.3节也涉及空口加密和完整性算法要求。

(2) 隐私需求

用户身份隐私保护 (P1): 通过对真实身份进行加密和替代实现对用户身份的隐私保护。例如, TS 33.501 第 6.12 节详细规定了 SUCI 的生成方式、5G-GUTI 的分配与更新机制, 以及订阅标识符去隐藏功能 (SIDF) 对 SUPI 的解隐藏功能。此外, 第 5.2.5 节也规定了永久身份标识 (subscription permanent identifier, SUPI) 不应在空口明文传输等基础要求。

用户位置隐私保护 (P2): 通过对位置标识的加密和隐藏机制实现用户地理位置的隐私保护。例如, TS 33.501 第 5.9.3.3 节要求 N32 接口上传输时对位置数据强制加密, 无论数据类型的加密策略如何。此外, 第 5.9.2.1 节也涉及拓扑隐藏机制, 间接支持位置隐私。

用户行为隐私保护 (P3): 通过最小化元数据暴露原则实现对用户通信行为的隐私保护。例如, TS 33.501 第 5.9.2.3 节要求 NEF 不得将内部信息发送到 3GPP 运营商域外, SUPI 也不得由 NEF 发送到域外。这体现了对用户通信相关元数据的保护。

隐私保护的标准化与合规性 (P4): 通过隐私保护框架确保符合国际隐私法规要求。例如, TS 33.501 第 5.2.5 节规定 SUCI 加密策略可由运营商配置, 订阅隐私启用的控制权归属网络, 提供了可配置的隐私保护机制。此外, 第 6.12 节也提供了 SUCI/5G-GUTI 的技术实现基础。

(3) 可信需求

透明性 (T1): 通过向用户及上层应用公开必要的安全状态信息, 确保安全机制的可观测性。例如, TS 33.501 第 5.10.1 节要求 UE 向应用层提供每 PDU 会话粒度的安全信息, 包括 AS 机密性、AS 完整性、NAS 机密性、NAS 完整性以及服务网络标识符。

可验证性 (T2): 通过验证机制或审计机制确保所有实体的身份与行为可信。例如, TS 33.501 第 5.9.2.1 节要求每个 NF 验证所有入站消息, 不符合协议规范和网络状态的消息被拒绝或丢弃。此外, 第 13.3 节也涉及 NF 与 NRF 的认证和静态授权。

可审计性 (T3): 对系统操作和事件的完整

记录和追踪能力。3GPP TS 33.501 中未系统定义可审计性指标, 仅在 TS 33.501 第 5.9.3.2 节中要求 SEPP 记录错误事件和异常, 以及第 5.9.4 节规定了信令流量监控的安全要求, 为审计提供了基础。

基础信任设施管理 (T4): 确保公钥基础设施的可信及数字证书的全生命周期管理。例如, TS 33.501 第 13.1 节要求所有 NF 支持相互认证的传输层安全 (TLS) 协议, 使用 X.509v3 证书, 并支持服务器端和客户端证书。此外, 第 5.3.4、5.9.3.2 节也涉及 gNB 证书注册和 SEPP 信任锚管理。

供应链安全 (T5): 确保软硬件从开发到部署全流程的安全性。例如, TS 33.501 第 5.3.4 节要求 gNB 软件更新在安装前进行验证, 确保软件传输的机密性和完整性, 使用授权数据/软件。

合规性与标准化 (T7): 符合行业安全标准和法规要求。例如, TS 33.501 第 5.11 节规定了算法标识符的全局一致值, 避免私有实现导致的安全漏洞或兼容性问题, 确保跨厂商互操作性。

(4) 韧性需求

快速恢复能力 (R1): 通过智能切换机制确保网络服务的持续可用性。例如, TS 33.501 第 6.8.1.1 节规定了 UE 从注销状态向注册状态转换时, 如何从 USIM 或非易失性存储器中检索存储的 native 5G NAS 安全上下文并重新激活, 实现安全状态的快速恢复。此外, 第 6.8.1.1.1 节也涉及状态转换时安全上下文的存储与标记。

自适应能力 (R2): 通过智能检测与动态响应机制提升网络安全韧性。TS 33.501 第 5.9.3.2 节中要求 SEPP 实施速率限制功能以防御过量信令, 以及第 5.9.4 节规定了信令流量监控的安全要求。

容错能力 (R3): 通过冗余架构设计确保关键功能在组件故障时仍可运行。例如, TS 33.501 第 6.9.3 节描述了接入和移动性管理功能 (access and mobility management function, AMF) 间上下文转移机制, 当源 AMF 决定执行水平密钥派生时, 向目标 AMF 传递新的安全上下文和密钥派生指示, 支持关键功能在组件间迁移时的容错设计。此外, 第 6.8.1.1.1 节也涉及安全上下文冗余切换, 第 6.9.2.3 节涉及 N2 切换中的密钥派生

机制。

备份机制的有效性 (R4)：通过多层次冗余策略保障关键数据与服务可快速恢复。例如，TS 33.501 第 6.8.1.1.2 节规定当 UE 从注销状态向注册状态转换时，若无 5G NAS 安全上下文可用，移动设备 (ME) 应从 USIM 或非易失性存储器中检索存储的本地 5G NAS 安全上下文。此外，第 6.8.1.1.1 节也规定了安全上下文在状态转换时的持久化存储机制。

高可用性 (R6)：通过弹性架构设计实现服务的无缝接续。例如，TS 33.501 第 5.9.3.2 节要求 SEPP 实施速率限制功能以防御过量信令攻击，保护自身及后续 NF。此外，第 5.9.3.4 节也涉及 PLMN 间用户面安全 (IPUPS) 丢弃畸形包及非活跃会话数据包，第 5.9.4 节涉及信令流量监控接口的安全保护，这些机制隐含了高可用性设计。

1.2.2 O-RAN 联盟

O-RAN 联盟安全工作小组 WG 11 提出的技术规范 “Security Requirements and Controls Specifications 14.0”^[56] 制定了关于 O-RAN 系统安全、隐私、可信以及韧性的需求，整理和总结如下。

(1) 安全需求

保密性 (S1)：确保数据在传输、存储和处理过程中不被未授权者访问或泄露。例如，规范第 5.2.1 节要求采用 TLS 1.3 加密传输，确保接口数据的机密性。此外，第 5.2.2 节、第 5.2.3 节、第 5.2.5.6 节、第 5.3.8 节及第 5.1.8.6 节也涉及 O1/O2 接口、开放前传 MACsec、日志加密存储及硬件安全模块等保密要求。

完整性 (S2)：确保数据在传输、存储和处理过程中不被篡改或破坏。例如，规范第 5.3.2 节要求所有 rApp/xApp 应用包经数字签名验证并在部署时重新校验。此外，第 5.2.2 节、第 5.2.5.6 节及第 5.1.3 节也涉及 O1 接口 TLS/MACsec 完整性保护及近实时 RIC 对 A1/Y1 接口数据的值域和速率检查。

可用性 (S3)：确保系统和数据在授权用户需要时能够正常访问和使用。例如，规范第 5.1.1 节要求服务管理与编排 (SMO) 和近实时 RIC 组件支持分布式拒绝服务 (DDoS) 攻击检测与恢复。

此外，第 5.2.5.3 节也涉及 S 复平面 (S-Plane) 采用多主时钟冗余架构确保时间同步可靠性。

双向认证 (S4)：通信双方在建立连接前相互验证对方身份，防止身份伪造。例如，规范第 5.2.1 和 5.2.3 节，要求 A1 和 O2 接口采用双向传输层安全协议 (mTLS) 双向认证。此外，第 5.2.6 节及第 5.2.2 节也涉及 R1 接口使用 OAuth 2.0 令牌认证以及网络访问控制模型 (NACM) 限制 O1 接口的网络配置协议 (NETCONF) 操作权限。

密钥管理 (S5)：对密钥的生成、分发、存储、更新和销毁进行全生命周期安全管理。例如，规范第 5.3.9 节要求采用公钥基础设施 (PKI) 体系和证书管理协议版本 2 (CMPv2) 协议管理证书生命周期。此外，第 5.1.4 节、第 5.1.5 节及表 5-1 也涉及用户面与控制面密钥分离以及密钥按策略定期自动轮换。

安全的可见性与配置性 (S6)：提供对安全状态的实时监控和灵活配置能力，便于安全运维。例如，规范第 7.8 节要求通过安全仪表盘实时展示加密状态、认证结果及异常事件告警。此外，第 5.3.10 节也涉及支持基于角色的安全策略灵活配置。

重放保护性 (S8)：防止攻击者通过重复发送已截获的合法消息来欺骗系统。例如，规范第 4.2 节和第 4.9 节要求 TLS 和媒体访问控制层安全 (MACsec) 使用序列号机制防止消息重放攻击。此外，第 5.2.5.3 节及第 6.6 节也涉及关键精确时间协议 (precision time protocol, PTP) 报文时间戳验证以及 OAuth 2.0 使用一次性有效令牌。

虚拟化隔离 (S9)：确保不同虚拟机、容器或租户之间的资源、数据和网络相互隔离。例如，规范第 5.1.8.4 节要求虚拟机与容器间实施严格的资源隔离。此外，第 5.1.8.4.2 节也涉及通过 NetworkPolicy 等软件定义网络 (software defined network, SDN) 策略限制虚拟网络流量。

细粒度授权与访问控制 (S10)：基于最小权限原则，对资源访问进行精细化、动态化的权限管理。例如，规范第 5.3.8.11.5 节要求基于属性控制日志文件的访问。此外，第 5.1.8.4.3 节也涉及 O-Cloud 采用基于角色的按需授权并严格执行最小必要权限原则。

(2) 隐私需求

用户标识隐私保护 (P1): 保护用户的永久身份标识符不被泄露或关联。例如, 规范第 5.3.8.11.6 节提出了 REQ-SEC-POL-7, 该要求规定日志处理时必须移除或加密个人身份识别信息。此外, 参考 3GPP 规范也涉及采用 SUCI 加密 SUPI 保护空口用户标识以及定期更新 5G-GUTI 临时标识。

用户位置隐私保护 (P2): 保护用户的地理位置信息不被未授权获取或精确定位。例如, 规范第 5.3.8.11.5 节要求通过严格访问控制限制位置数据的访问权限。

用户行为隐私保护 (P3): 保护用户的使用习惯、业务偏好等行为模式不被分析或关联。例如, 规范第 5.3.12 节提出了 REQ-SEC-AIML-8 和 REQ-SEC-AIML-9, 该要求允许在 AI/ML 训练和推理中应用差分隐私技术。此外, 第 5.3.8.11.5 节还要求日志记录时过滤敏感操作参数, 并在业务关键性能指标 (key performance indicator, KPI) 统计时对数据进行去标识做处理, 确保统计结果不关联到个人用户。

隐私保护的可配置性与可见性 (P4): 支持运营商灵活配置隐私策略, 并向用户或监管方展示隐私处理情况。例如, 在规范第 5.3.8.11.6 节要求支持运营商按通用数据保护条例 (general data protection regulation, GDPR) 要求配置数据收集范围。

隐私保护的标准化与合规性 (P5): 遵循法律法规和行业标准, 确保隐私保护的合规性。例如, 规范第 5.3.8.11.6 节提出了 REQ-SEC-POL-7 和 REQ-SEC-POL-8, 这两项要求规定了数据最小化存储原则以及归档日志的机密性和完整性保护。

(3) 可信需求

透明性 (T1): 系统的安全策略、决策逻辑和操作行为应公开、可审查, 避免黑箱操作。例如, 规范第 5.3.12 节要求机器学习决策逻辑公开可查, 避免黑箱操作。此外, 第 8.4 节也涉及系统日志完整记录管理行为以及安全配置参数可视化展示。

可验证性 (T2): 系统的身份、软件完整性和运行环境可通过技术手段进行独立验证。例如, 规范第 5.3.2 节要求所有软件包强制进行数

字签名验证。此外, 第 5.1.8.7 节也涉及 O-Cloud 平台实施远程证明验证运行环境完整性以及通信实体采用证书链认证。

可审计性 (T3): 对系统操作和事件的完整记录和追踪能力。例如, 规范第 5.3.8.11 节要求所有关键操作日志强制记录, 支持事后审计。此外, 第 6.3 节也涉及应用包版本信息全程追踪以及安全事件时间戳精确到毫秒级。

基础信任设施管理 (T4): 对数字证书的颁发、更新、撤销进行自动化、全生命周期管理, 确保身份可信。例如, 规范第 5.3.9 节要求采用 CMPv2 协议自动进行证书颁发、更新和撤销。此外, 第 4.2.3 节也涉及证书吊销列表实时更新以及证书有效期强制策略管控。

软件供应链安全 (T5): 确保软件从开发、打包到部署的整个供应链中组件安全可信。例如, 规范第 6.3 节要求强制验证软件物料清单, 确保无已知漏洞组件。此外, 第 5.1.8.8 节也涉及对硬件加速器等设备实施供应商安全审计以及第三方代码安全扫描。

合规性与标准化 (T7): 遵循国际标准和行业规范, 通过安全认证确保系统合规。例如, 规范第 4 节要求严格遵循 O-RAN 安全协议规范。此外, 第 24.1 节也涉及定期进行 3GPP 安全保障规范 (SCAS) 等安全标准符合性认证。

(4) 韧性需求

快速恢复 (R1): 系统在遭受攻击或故障后, 能够快速自动恢复正常服务。例如, 规范第 5.1.1 节和第 5.1.3 节要求 SMO 和近实时 RIC 支持从 DDoS 攻击中自动恢复。此外, 第 5.1.8.5 节也涉及 O-Cloud 采用滚动升级策略实现无中断更新以及关键服务故障时秒级切换备用实例。

自适应能力 (R2): 系统能够根据实时威胁动态调整防护策略, 实现智能主动防御。例如, 规范第 5.1.3 节要求近实时 RIC 根据流量特征动态调整限速策略。此外, 第 5.3.12 节也涉及 AI/ML 模型持续监控网络行为并实时检测与阻断对抗样本攻击。

容错能力 (R3): 通过冗余设计, 防止单点故障导致系统失效。例如, 规范第 5.2.5.3 节要求 S-Plane 采用多主时钟冗余架构确保时间同步可

靠性。此外，第5.3.9节也涉及证书更新失败时的自动回滚机制。

备份机制的有效性（R4）：对关键数据和配置进行定期备份，并支持快速恢复。例如，规范第5.3.8.11.2节和第5.1.8.6节要求对日志和用户数据定期加密备份并存储于隔离环境。此外，第5.3.8.11.3节也涉及安全配置实施版本控制支持快速回滚以及备份数据完整性校验。

AI/ML鲁棒性（R5）：确保AI/ML模型能够抵御对抗样本、投毒攻击等，保持决策可靠性。例如，规范第5.3.12节要求采用对抗训练增强模型的抗干扰能力。此外，本节中的REQ-SEC-AIML-13也涉及对输入数据进行严格清洗过滤以防止投毒攻击，以及模型输出结果的多重校验。

1.2.3 国内外运营商与其他组织

中国移动在《6G安全愿景白皮书》^[57]和《2024年6G数字孪生网络安全技术白皮书（1.0）》^[58]中，中国联通在《6G分布式网络架构及关键技术白皮书》中，中国电信在《基于云网融合的6G关键技术白皮书》中以及三星公司在《AI原生应用与可持续通信》中分别讨论了下一代服务化网络中需要保障的安全、隐私、可信以及韧性需求，总结如下。

安全需求。保密性（S1）：通过数据加密和访问控制实现全生命周期数据保护。例如：采用高级加密标准（advanced encryption standard, AES）和量子加密算法保护数据传输；实施基于角色的访问控制（role-based access control, RBAC）策略限制敏感数据访问等。**完整性（S2）：**通过多重校验机制确保数据真实可靠。例如：使用数字签名验证软件包完整性；采用哈希算法校验数据一致性；关键操作日志通过区块链存证防篡改等。**可用性（S3）：**通过冗余架构和防护系统保障服务持续可用。例如：部署分布式云原生架构实现自动负载均衡；采用抗DDoS系统防御流量攻击；通过网络切片技术隔离关键业务保障服务质量等。**双向认证（S4）：**通过多维度验证实现动态安全授权。例如：结合指纹/虹膜等生物识别技术；实施多因素认证（multi-factor authentication, MFA）机制；基于零信任模型持续验证访问权限等。**密钥管理（S5）：**通过抗量子计算技

术强化密钥安全。例如：采用格基加密等量子抗性算法；密钥生成/存储使用认证的硬件安全模块；实施自动化密钥轮换策略等。**端到端安全（S7）：**通过全链路加密构建纵深防御体系。例如：空口通信采用5G-AKA双向认证；数据传输全程启用传输层安全性协议加密；关键路径部署量子密钥分发等。**虚拟化隔离（S9）：**通过硬件级隔离保障云环境安全。例如：采用单根输入输出虚拟化（SR-IOV）技术实现网络功能虚拟化；通过微隔离策略控制东西向流量；构建可信执行环境等。**安全共享（S11）：**通过隐私计算技术实现可信数据协作。例如：基于智能合约的跨域访问控制；采用同态加密处理敏感数据；联邦学习框架支持多方安全计算等。

隐私需求。用户标识保护（P1）：通过去中心化身份和匿名化技术保护用户身份信息。例如：采用去中心化标识符（decentralized ID, DID）实现分布式身份管理；应用匿名凭证，例如零知识证明等技术进行身份验证；临时标识定期轮换避免身份追踪等。**用户位置隐私保护（P2）：**通过隐私增强算法保护用户位置数据。例如：采用差分隐私技术添加噪声扰动位置信息；使用k-匿名算法确保轨迹数据不可关联特定用户以及地理围栏数据聚合处理降低定位精度等。**用户行为隐私保护（P3）：**通过分布式学习和数据处理技术保护用户行为数据。例如：采用联邦学习框架实现多方数据协同建模；对敏感行为数据实施脱敏处理（如泛化、抑制）；用户画像数据实施差分隐私保护等。**合规性与标准化（P5）：**通过隐私增强技术和自动化工具确保合规要求。例如：采用安全多方计算（secure multi-party computation, MPC）实现隐私数据协同分析；部署自动化合规审计系统实时监测GDPR合规状态；隐私影响评估（privacy impact assessment, PIA）工具自动生成合规报告等。

可信需求。透明性（T1）：通过可解释性技术和开放审计机制确保系统决策透明。例如：采用可解释AI（XAI）算法提供模型决策依据；关键组件开源代码接受第三方审计；安全策略配置参数可视化展示等。**可验证性（T2）：**通过密码学验证技术保障系统真实性。例如：基于区块链

存证关键操作日志；采用零知识证明验证身份凭证有效性；硬件级可信执行环境远程认证等。可审计性（T3）：通过不可篡改记录技术实现全链路追踪。例如：操作日志采用区块链存证防篡改；敏感数据嵌入数字水印追踪泄露源头；版本控制系统记录所有代码变更历史等。

韧性需求。快速恢复能力（R1）：通过智能修复和备份机制确保业务连续性。例如：采用AI驱动的自动化故障诊断与修复系统；实施分钟级备份快照技术实现数据快速回滚；关键业务组件预置热备实例等。自适应能力（R2）：通过智能网络技术实现动态防护。例如：部署意图驱动网络自动优化安全策略；采用强化学习算法实时调整防御参数；基于流量特征的自适应DDoS防护等。AI鲁棒性（R5）：通过多重验证机制保障AI系统安全。例如：采用对抗训练增强模型抗干扰能力；实施严格的模型输入输出验证；部署模型监控系统检测异常行为等。高可用性（R6）：通过分布式架构实现业务永续。例如：采用多活数据中心架构消除单点故障；实施服务等级协议（service-level agreement, SLA）实时监控与自动告警；基于微服务的弹性伸缩设计等。

2 6G全服务化架构网络安全、隐私风险分析与可信评价指标体系

本节将系统分析6G全服务化网络在安全与隐私方面面临的新型风险，并构建一套覆盖安全、隐私、可信与韧性4个维度的综合评价指标体系。首先从核心网、接入网与终端3个层面识别威胁与脆弱性，随后基于5G架构的不足，构建面向6G服务化环境的可信性评估框架，为后续研究梳理与对比工作提供理论依据与评估基准。

2.1 6G安全、隐私风险分析

针对6G全服务化网络架构，从核心网、接入网以及终端设备3个子系统全面分析系统在服务化过程中面临的安全和隐私威胁。6G全服务化网络安全和隐私风险如图1所示。

核心网由于网络的虚拟化、服务化和云原生，可能面临多维度的新型攻击模式。首先，针对虚拟化隔离不足导致的侧信道攻击风险，攻击者具备在共享物理主机上部署恶意虚拟机或容器的能力，通过利用CPU缓存、内存访问模式等共享资源残留信息，构建隐蔽信道或实施侧信道分析，其攻击路径从同驻虚拟化环境出发，逐步推断目标虚拟机的密钥或敏感数据，影响范围可

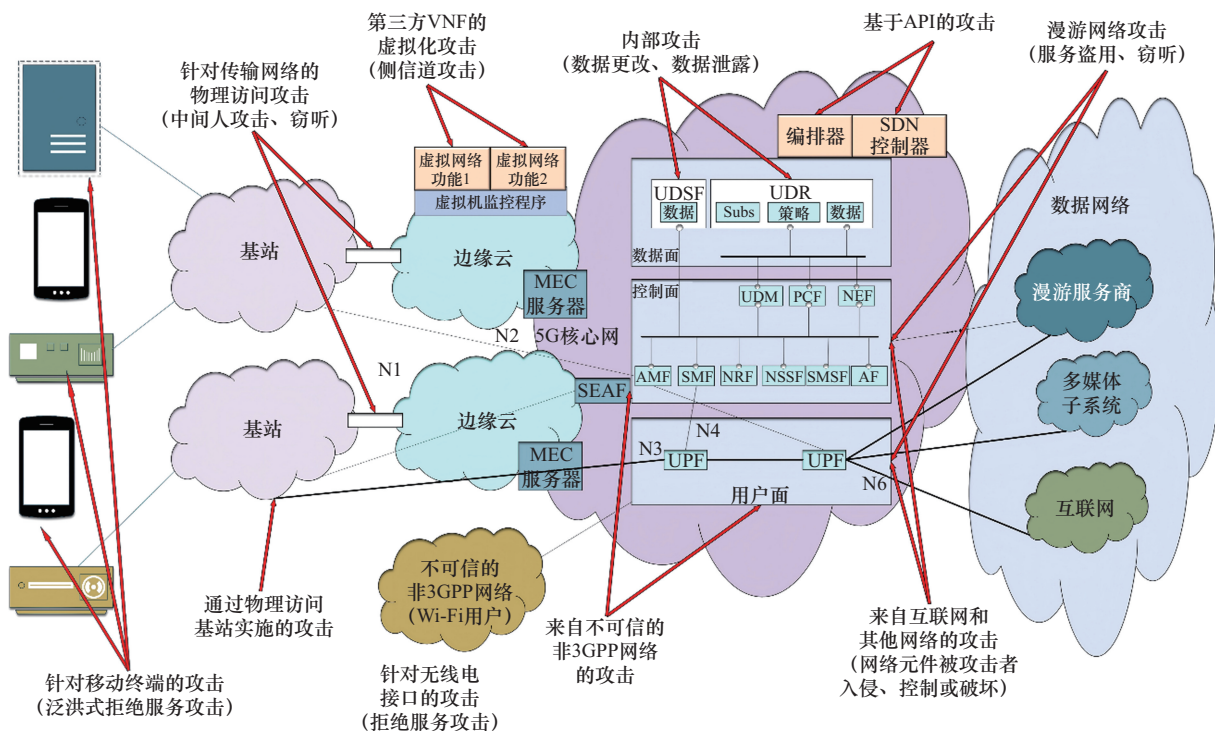


图1 6G全服务化网络安全和隐私风险

波及同宿主机上的多个网络功能或网络切片，最终可能导致系统级信息泄露和越权访问等严重后果^[59-60]。其次，针对服务接口开放化导致的API攻击风险，攻击者具备扫描和识别API端点脆弱性的能力，通过容器编排层或SDN控制器等控制实体的脆弱点构建API诱饵，注入恶意微服务或实施未授权访问，其攻击路径从外部网络渗透至服务编排层，进而影响云服务及核心网网络功能，可能导致服务中断、数据篡改或权限提升^[61-62]。此外，面对非3GPP接入引入的边界渗透风险，攻击者具备在非3GPP接入网络（如公共Wi-Fi、固网）中实施中间人攻击的能力，利用终端设备与5G网关非3GPP互通功能（N3IWF）之间的弱安全防护机制作为攻击入口，通过渗透进入核心网，其影响范围可扩展至整个核心网内部，可能使核心网直面来自非信任网络的各类后续攻击^[63]。最后，针对多代共存带来的遗留漏洞风险，攻击者具备利用4G网络已知漏洞的知识和能力，在4G与5G/6G互操作过程中发起降级攻击或伪造漫游信令，攻击路径从传统网络侧渗透至新一代核心网，影响范围涵盖跨代互操作接口及漫游网关，可能导致5G/6G网络的安全防护被绕过，引发用户数据泄露或服务中断^[64-65]。

O-RAN可能成为下一代移动通信网络的新型范式。相较于传统的接入网，O-RAN面临更为复杂的攻击面。首先，针对边缘云开放化导致的虚拟化攻击风险，攻击者具备利用第三方虚拟网络功能（virtual network function, VNF）实现漏洞的能力，通过在边缘云中部署恶意应用或利用现有漏洞发起虚拟化攻击和侧信道攻击，其攻击路径从第三方应用层面渗透至边缘云基础设施，影响范围可波及边缘云上运行的所有接入网服务，可能导致接入网信息泄露、服务失效或成为进一步攻击的跳板^[66]。其次，针对空口传输暴露导致的中间人攻击风险，攻击者具备在无线覆盖范围内捕获和处理空口信号的能力，通过在终端与基站之间实施中间人攻击或被动窃听，其攻击路径从无线信道延伸至接入网传输链路，影响范围覆盖基站覆盖区域内的所有终端设备，可能导致用户通信数据被截获、篡改或伪造^[67]。此外，针对协议兼容性引入的安全降级攻击风险，攻击者具备

部署伪基站的能力，通过诱导终端连接并强制其使用较弱的加密算法或回退至3G/4G网络，其攻击路径从伪基站渗透至终端与核心网的认证流程，影响范围涉及支持多代网络接入的终端设备，可能导致利用旧版协议的已知漏洞破坏网络安全性^[68]。最后，针对无线资源开放导致的拒绝服务攻击风险，攻击者具备伪造大量连接请求或异常信令的能力，通过耗尽基站的资源或无线带宽资源，其攻击路径从无线接口直接作用于基站调度器，可导致特定基站覆盖范围内的所有终端无法接入，可能造成合法用户服务中断^[69]。

针对更为多样化的异构移动终端设备，设备在各个层面都面临多种攻击威胁。首先，针对网络接入欺骗攻击风险，Hussain等^[70]指出攻击者具备部署伪基站并模拟合法网络身份的能力，通过诱导终端连接至非法网络，其攻击路径从空口信令交互渗透至终端身份认证过程，影响范围涉及伪基站覆盖范围内的所有终端，可能导致用户身份信息和通信内容被窃取。其次，针对资源耗尽型攻击风险，Javanmardi等^[71]指出攻击者具备向目标终端发送大量UDP数据包的能力，通过耗尽终端处理资源或网络带宽，其攻击路径从网络层渗透至终端操作系统，影响范围可针对特定终端或终端群组，可能导致合法服务不可用或终端死机。此外，针对信令层拒绝服务攻击风险，Ashaik等^[72]指出攻击者具备利用信令交互过程中状态机缺陷的能力，通过发送异常信令消息，其攻击路径从网络信令层渗透至终端协议栈，影响范围涵盖特定型号或协议实现的终端设备，可能导致终端陷入错误状态或频繁重启，造成服务中断。针对位置欺骗攻击风险，Gao等^[73]指出攻击者具备伪造定位参考信号（positioning reference signal, PRS）的能力，通过发射虚假定位信号诱导终端定位计算，其攻击路径从无线物理层渗透至终端定位服务模块，影响范围覆盖支持PRS定位的所有终端设备，可能导致位置隐私泄露或导航误导。最后，针对终端异构性导致的安全脆弱性风险，由于5G/6G网络中将接入更多种类的异构终端，如物联网设备、传感器、智能汽车等，攻击者具备利用低功耗设备计算能力不足、安全防护机制薄弱的特点，通过将其作为攻击跳板或

僵尸节点，其攻击路径从脆弱终端渗透至网络内部，影响范围可扩大至与这些终端互联的其他网络实体，可能导致大规模僵尸网络构建或连锁性网络攻击^[74]。

虽然 5G 网络已构建相对完善的安全体系，并在安全与隐私保护方面取得显著进展，但面向 6G 全服务化网络，现有架构仍存在明显局限。在安全与隐私方面，5G 现有机制难以全面应对 6G 新型场景中的复杂攻击。例如，针对服务化接口的 API 供应链攻击，攻击者可利用容器编排漏洞注入恶意微服务，绕过传统网络边界防护；此外，基于隐蔽信道的虚拟化侧信道攻击也暴露出 5G 在隔离机制与信息泄露防护方面的不足。因此，面向 6G 服务化网络的安全架构需要在安全与隐私等方面进一步加强。其次，5G 安全体系构建的是静态化的安全保障架构，对动态可信与系统韧性的覆盖缺失，使其无法保障系统在面对高级持续性威胁与系统级故障时的安全。例如，在缺乏持续信任评估机制的情况下，内部威胁与伪基站诱导的安全降级攻击难以被及时发现；同时，若未建立韧性感知的弹性恢复机制，一旦核心网元遭遇协同分布式拒绝服务攻击，将可能导致服务链级

联中断，影响全网可用性。所以急需构建一个覆盖安全、隐私、信任与韧性的全方位评价体系，以指导下一代网络的安全设计与实践。

2.2 四维可信服务化网络评价指标体系

通过对现有 5G/6G 安全标准和相关研究的系统梳理，基于前面对全服务化网络安全和隐私风险的全面分析，本文构建了一个四维可信服务化网络评价指标体系，如图 2 所示。该体系共计 4 个维度，即安全、隐私、可信和韧性，32 项综合评价指标，并面向移动通信系统全生命周期，从前置预防、实时监控、应急恢复 3 个阶段划分和分析相应指标，安全指标（S1~S14）主要覆盖前置预防（如保密性、认证、访问控制）和实时监控（如策略冲突检测、资源监控）；韧性指标（R1~R6）主要覆盖应急响应与恢复（如快速恢复、自适应能力）；隐私指标（P1~P5）贯穿数据全生命周期；可信指标（T1~T7）侧重于运行时验证与事后审计。该评价指标体系一方面弥补了现有 5G 安全标准（如 3GPP TS 33.501）在信任与韧性维度方面的考量不足，难以应对 6G 全服务化网络面临的动态可信评估与弹性恢复的迫切需求；另一方面针对多种新型风险，从更全面

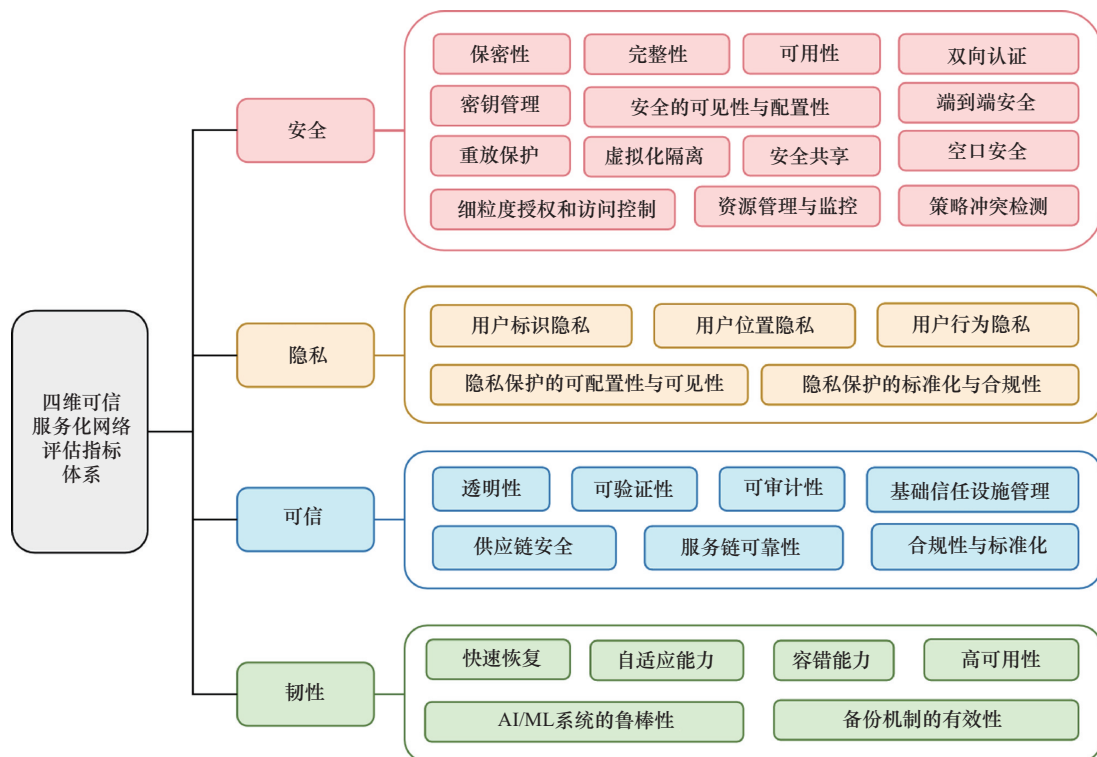


图2 四维可信服务化网络评价指标体系

的视角构建评估框架。

(1) 安全指标定义

保密性 (S1)：确保控制面信令、用户面消息和数据仅能被授权方访问，防止未授权信息泄露，有效防范窃听、数据泄露等安全风险。可使用包括数据加密、访问控制等技术手段实现。相关评估指标包括加密算法强度、密钥长度与更新周期、数据泄露风险评分等。

完整性 (S2)：保护信令、用户面消息和数据免受篡改或破坏，确保信息的准确性和一致性。常采用包括哈希校验、数字签名等技术手段实现，相关评估指标包括哈希算法类型与碰撞率、数字签名验证成功率、数据篡改检测响应时间等。

可用性 (S3)：保证合法用户对信息和资源的使用不会被不正当地拒绝，确保在需要时可以访问。该指标确保系统可有效抵御拒绝服务攻击或勒索攻击。相关的评估指标包括拒绝服务攻击 (DoS) 防护峰值处理能力等。

双向认证 (S4)：通信双方验证身份的真实性，防止仿冒攻击、中间人攻击等威胁。相关评估指标包括认证失败率、多因素认证覆盖率、认证时延等。

密钥管理 (S5)：对密钥的全生命周期进行安全管控，包括生成、分发、存储、轮换和销毁等环节，可有效抵御密钥泄露、密码分析攻击以及侧信道等攻击。相关评估指标包括密钥生命周期管理合规性、密钥泄露事件次数、密钥分发成功率等。

安全的可见性与配置性 (S6)：提供安全状态的可视化监控和灵活的安全策略配置能力。相关评估指标包括安全事件可视化覆盖率、策略配置平均时间、实时告警准确率等。

端到端安全 (S7)：保障设备到设备的通信链路安全，没有中继设备的安全中断，有效抵御窃听、篡改以及中间人等攻击。该指标与保密性 (S1)、完整性 (S2) 和双向认证 (S4) 指标相关，但更关注应用层端到端“安全管道”的建立。相关评估指标包括端到端加密协议支持率、终端认证一致性验证成功率等。

重放保护性 (S8)：防止攻击者截获并重复发送有效数据分组的安全机制，可采用时间戳、

序列号等安全措施有效抵御重放攻击、中间人等攻击。相关评估指标包括重放攻击检测率、时间戳/序列号同步精度等。

虚拟化隔离 (S9)：采用相关安全技术实现不同租户/服务间的虚拟资源隔离，有效抵御 VNF 虚拟化攻击，侧信道攻击等。相关评估指标包括虚拟资源隔离强度、侧信道攻击防护有效性评分等。

细粒度授权和访问控制 (S10)：基于角色、属性等多因素、多维度实现精确的授权和访问控制，可有效抵御权限滥用、越权访问等问题。相关评估指标包括策略规则数量与复杂度、权限滥用检测准确率、访问日志审计覆盖率等。

安全共享 (S11)：针对多安全域环境，保障数据、服务、算力等资源安全、可控的跨域分享和互操作，有效抵御数据泄露、越权访问等威胁。该指标及保密性 (S1) 与细粒度授权和访问控制 (S10) 相关，但该指标更关注跨域数据和资源共享的安全，而保密性 (S1) 关注的是数据本身的安全，细粒度授权和访问控制 (S10) 重点关注权限的分配和控制策略。相关评估指标包括跨域互操作成功率、共享资源安全审计覆盖率、动态策略更新时延等。

空口安全 (S12)：空口安全为针对无线通信的特殊安全保护机制，需有效防止伪基站、空口拒绝服务、无线窃听等攻击。该指标与多项安全性和隐私性指标相关，例如保密性 (S1)、完整性 (S2)、重放保护性 (S8)、用户标识隐私保护 (P1) 等，但空口安全更关注面向无线空口的整套安全保障机制，该指标的实现基于基础安全和隐私指标。相关评估指标包括伪基站识别率、空口加密协议支持情况、无线窃听防护强度评分等。

资源管理与监控 (S13)：对网络和服务资源的分配、使用情况进行实时监控和管理。可有效抵御拒绝服务攻击、控制器攻击等。相关评估指标包括资源使用率监控覆盖率、异常行为检测响应时间、资源调度策略合规性等。

策略冲突检测 (S14)：识别和解决不同安全策略之间的冲突问题，可有效抵御策略注入攻击、策略篡改攻击等。该指标关注系统安全和隐私等相关配置和管理策略。相关评估指标包括冲

突检测准确率、策略冲突解决平均时间、冲突预警覆盖率等。

(2) 隐私指标定义

用户标识隐私保护 (P1): 保护用户身份标识, 例如国际移动用户识别码 (IMSI)、SUPI 等, 不被泄露、跟踪及滥用。相关评估指标包括身份匿名化覆盖率、标识泄露事件次数、身份追踪抵抗强度评分等。

用户位置隐私保护 (P2): 防止用户位置信息被非法获取或追踪, 抵御用户跟踪和推理等攻击。相关评估指标包括位置模糊化精度、位置信息泄露频率、地理围栏隐私保护合规性等。

用户行为隐私保护 (P3): 保护用户通信行为、使用习惯等隐私数据, 抵御基于用户行为识别的多种攻击。相关评估指标包括行为数据脱敏率、行为模式识别抵抗能力评分、用户画像数据访问日志完整性等。

隐私保护的可配置性与可见性 (P4): 提供隐私设置的灵活配置和透明展示。相关评估指标包括隐私设置项数量与用户可调比例、隐私策略用户理解度评分、配置生效时延等。

隐私保护的标准化与合规性 (P5): 符合多项个人隐私信息保护法规和行业标准的要求。相关评估指标包括符合 GDPR、CCPA 等法规的条款覆盖率、隐私影响评估执行率、合规审计通过率等。

(3) 可信指标定义

透明性 (T1): 强调系统决策过程的可视化与可理解性。相关评估指标包括系统行为日志对外开放比例、决策可解释性评分、用户可见安全状态更新时间等。

可验证性 (T2): 系统决策和声明的可验证性, 如通过审计日志或可验证密码学工具等, 侧重于实体身份与声明的可信验证。相关评估指标包括审计日志完整性校验通过率、第三方验证接口支持情况、可信执行环境远程认证成功效率等。

可审计性 (T3): 对系统操作和事件的完整记录和追踪能力, 侧重于实体行为与系统事件的事后追溯。该指标与安全、隐私以及可信等多项指标有关, 但该指标强调的是对系统事件的完整记录和留存, 以及事后的审计和追溯能力。相关评估指标包括审计记录存储完整性、审计查询响

应时间、审计事件覆盖范围等。

基础信任设施管理 (T4): 确保基础信任设施, 例如公钥基础设施的安全可靠; 数字证书的签发、验证、更新和撤销等全生命周期管理等, 侧重于基础设施层的信任锚点与证书体系。相关评估指标包括证书颁发/撤销平均时间、PKI 系统可用性 SLA、信任链验证成功率等。

供应链安全 (T5): 确保软硬件从开发到部署全流程的安全性。可有效抵御供应链投毒、恶意依赖攻击等。该指标与基础信任设施管理 (T4) 有相关性, 但该指标重点关注系统软硬件来源和部署的可信性。相关评估指标包括软件物料清单覆盖率、第三方组件漏洞扫描频率、供应链攻击事件次数等。

服务链可靠性 (T6): 端到端服务交付的可靠性、一致性和可验证性保障, 可有效抵御服务链路径绕过、中间节点劫持、服务顺序篡改等攻击。该指标与供应链安全 (T5) 侧重点不同, 该指标关注系统服务编排与执行的可靠性, 而供应链安全 (T5) 更多关注系统软硬件组成的安全性。相关评估指标包括服务链端到端成功率、服务时延方差、故障传递阻断能力等。

合规性与标准化 (T7): 符合行业安全标准和法规要求。相关评估指标包括符合 3GPP/ITU-T 标准条款数、安全认证通过情况、国际互操作测试通过率等。

(4) 韧性指标定义

快速恢复 (R1): 在遭受攻击或故障后快速恢复正常服务的能力, 侧重于故障发生后的恢复速度与成功率。该指标与安全指标中的可用性 (S3) 相关, 但该指标更关注系统受攻击或故障后的恢复速度和成功率。相关评估指标包括平均修复时间、服务恢复成功率、灾难恢复演练频率等。

自适应能力 (R2): 根据环境变化自动调整安全、隐私、信任等策略的能力, 可有效抵御降级攻击、基于 API 的攻击等, 侧重于系统对动态环境的实时响应与策略调整能力。该指标与快速恢复 (R1) 相关, 但该指标更关注面对系统环境变化的系统自动调整能力。相关评估指标包括策略自适应调整响应时间、环境变化检测准确率、自适应学习模型更新频率等。

容错能力 (R3)：在系统部分组件失效时仍能维持基本功能的能力，侧重于组件失效条件下的服务持续能力。该指标与可用性 (S3) 和自适应能力 (R2) 相似，但该指标更关注系统部分组件和功能失效条件下的服务保障能力。相关评估指标包括单点故障影响范围、冗余资源覆盖率、故障隔离成功率等。

备份机制的有效性 (R4)：数据和服务备份的完整性、可用性和恢复效率，侧重于备份策略的完整性与恢复效率。相关评估指标包括备份数据完整性校验通过率、备份恢复时间目标、备份存储加密率等。

AI/ML 系统的鲁棒性 (R5)：AI/ML 系统抵抗对抗样本攻击等威胁的能力。可有效抵御基于 API 的攻击、SDN 控制器攻击等。相关评估指标包括对抗样本检测准确率、模型投毒攻击抵抗评分、AI 系统误判率等。

高可用性 (R6)：系统提供持续服务的能力，通常用 SLA 的可用性百分比衡量，侧重于系统在长期稳态运行下的高可靠持续服务能力。该指标与安全指标中的可用性 (S3) 不同，更关注提供高可靠持续服务的能力。相关评估指标包括系统可用性 SLA、服务降级策略执行成功率、负载均衡效率等。

上述4类32种指标共同构成了评估未来服务化6G网络安全的完整指标体系，每个指标都需要特定的技术手段和管理措施来实现和保障。在实际网络部署中，需要根据具体应用场景对这些指标进行权衡和优化。在本文的第2.2节中，3GPP和O-RAN已列出的需求主要集中于基础安全与接口安全层面，本文从指标覆盖范围对比了四维可信服务化网络评价指标体系与现有移动网络安全标准体系，即3GPP TS 33.501和O-RAN WG11安全规范，如图3所示。对比显示，安全



图3 四维可信服务化网络评价指标体系与现有移动网络安全标准体系对比

共享 (S11)、策略冲突检测 (S14)、服务链可靠性 (T6)、AI/ML 系统鲁棒性 (R5 的评估) 等面向 6G 全服务化网络的新型需求均未覆盖。本文所提四维可信服务化网络评价指标体系将韧性作为独立维度, 系统定义了 R1 至 R6 六大韧性指标, 并新增了 S11 (安全共享)、S14 (策略冲突检测)、T6 (服务链可靠性) 等指标, 有效填补了现有标准的缺口, 为 6G 全服务化网络的可信性评估提供了系统化的基准与方法论指引。

四维可信服务化网络评价指标体系与现有安全评价体系对比见表 2。对比显示, 在覆盖范围上, 四维可信服务化网络评价指标体系整合了安全、隐私、可信与韧性 4 个维度, 实现了全面覆盖; 在场景适配性上, 明确面向 6G 全域服务化网络, 突破了 5G 核心网与 O-RAN 接入网的局限; 在体系特点上, 既继承了标准化与开放化优势, 又形成了覆盖全面、体系完善的评估框架。需要指出的是, 本文提出的综合评价框架目前主要提供评估维度和评估指标, 尚缺乏大范围的实证验证。不同应用场景下指标权重和评分阈值的设定仍需结合具体需求进行校准, 框架的可复现性和通用性有待通过更多案例 (如工业物联网、卫星网络) 进一步检验。

3 服务化 5G/6G 网络安全、隐私、可信及韧性调研

为确保调研的系统性与可复现性, 本文遵循规范的调研方法。文献检索范围涵盖 IEEE Xplore、ACM Digital Library、SpringerLink、ScienceDirect 及中国知网 (CNKI) 等学术数据库, 以及 3GPP 官网、O-RAN 联盟官网等标准化文档源, 同时纳入了中国移动、中国电信、华为^[75]、爱立信、诺基亚等机构发布的产业白皮书。检索时间跨度为 2018 年 1 月至 2025 年 6 月,

以 3GPP Release 15 首次定义 5G 服务化架构为起点。关键词组合为: 英文 (“Service-Based Architecture” OR “SBA” OR “6G” OR “5G-Advanced”) AND (“security” OR “privacy” OR “trust” OR “resilience” OR “trustworthiness”); 中文 (“服务化架构” OR “SBA” OR “6G” OR “5G-Advanced”) AND (“安全” OR “隐私” OR “可信” OR “韧性”)。纳入标准为: 研究内容涉及服务化架构下的安全、隐私、可信或韧性, 研究对象为 5G/5G-Advanced/6G 移动网络, 文献类型为期刊论文、会议论文、标准化规范或产业白皮书; 排除标准为: 仅讨论物理层安全或非服务化架构, 或未涉及上述任一维度。经初筛获得 387 篇文献 (学术论文 276 篇、标准化文档 54 篇、白皮书 57 篇), 经标题、摘要筛选后保留 156 篇, 全文阅读后最终纳入核心文献 89 篇。按网络安全核心方向分为网络安全架构 (14 篇)、身份与证书管理 (12 篇)、网络攻击检测 (28 篇)、O-RAN 安全与冲突管理 (15 篇)、终端设备安全 (8 篇)、应用场景安全 (12 篇) 六大类。同时, 应用本文提出的四维可信服务化网络评价指标体系, 对每一项工作进行全面的评估。

3.1 网络安全架构

网络安全架构是保障网络系统及数据资产安全的安全体系框架, 通过整合安全策略、技术组件、管理流程、组织方式等, 构建分层的、一体化的整体结构。下一代全服务化网络与前几代移动通信网络在网络架构上有着较大的演进, 并且通过引入人工智能技术实现网络的智能化管控, 对现有 5G 安全架构产生了较大的影响。本节全面调研了面向下一代全服务化网络的网络安全架构的研究工作, 网络安全架构相关工作安全、隐私、可信及韧性比较与总结见表 3。

表 2 四维可信服务化网络评价指标体系与现有安全评价体系对比

安全体系	3GPP TS 33.501	O-RAN WG11 安全规范	四维可信服务化网络评价指标体系
范围	安全为主, 隐私为辅	安全、隐私、可信并重	安全、隐私、可信、韧性全覆盖
适配场景	5G 网络	接入网	6G 全域服务化网络
体系特点	标准化程度高	接口开放化、拓展性强	增强安全和隐私保障; 新增信任与韧性维度
体系不足	开放程度较低、智能化低	网络覆盖范围单一	尚未形成详细且可操作的量化评估体系, 有待通过更多场景案例检验复现

表 3 网络安全架构相关工作安全、隐私、可信及韧性比较与总结

指标	安全指标												隐私指标					可信指标						韧性指标								
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	P1	P2	P3	P4	P5	T1	T2	T3	T4	T5	T6	T7	R1	R2	R3	R4	R5	R6
3GPP	●	●	●	●	●	●	●	●	●	●	○	●	○	○	●	●	●	○	●	●	●	○	○	●	○	●	●	●	●	●	○	○
O-RAN	●	●	●	●	●	●	○	●	●	●	○	○	○	○	●	●	●	●	●	○	●	●	●	○	○	●	●	●	●	●	●	○
文献[76]	●	●	●	○	●	●	●	○	●	○	●	○	●	○	○	●	●	○	●	○	○	●	●	●	●	●	●	●	●	○	●	○
文献[77]	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
文献[78]	●	○	○	○	●	○	○	●	○	○	●	●	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	●	●	●	○	○
文献[79]	●	○	○	○	●	○	○	●	○	○	●	●	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	●	●	○	○	○
文献[80]	●	●	●	○	○	○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○
文献[33]	●	●	●	●	●	○	●	○	○	○	●	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○
文献 [81]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
文献[82]	●	○	●	○	○	●	●	○	●	○	●	○	●	○	●	●	●	●	●	●	●	●	○	○	●	●	●	●	●	●	●	●
文献[83]	●	●	●	●	○	●	●	○	●	●	●	○	●	●	●	●	●	●	●	●	●	●	○	○	●	●	●	●	●	●	○	●
文献[84]	●	○	●	○	○	●	○	●	○	○	○	○	●	○	●	○	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○
文献[85]	●	●	○	●	●	○	●	○	○	●	●	○	●	●	●	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Khorsandi 等^[76]探讨了 6G 网络的安全使能技术及其在构建整体安全架构时的作用和影响,分别从基础设施层、网络服务层、应用层以及管理与编织层讨论了保护安全、隐私和信任的需求以及使能技术。针对安全防护需求,指出了采用多种安全软硬件技术,例如密码加速器实现 6G 网络数据的安全高效传输;量子密钥分发技术实现安全的密钥管理。针对 6G 网络隐私需求,讨论了采用差分隐私、同态加密以及安全多方计算等技术实现在保护用户和商业隐私前提下的对用户数据的高效挖掘和利用。针对网络的可信需求,引入了信任等级指数,用以动态评估网络服务的可信性;同时,采用可信硬件以及远程验证等技术,构建了安全可信的网络基础设施。针对网络的韧性提升,指出了可通过多连接性实现架构的弹性,提高网络服务的可用性,还强调了架构的自动化和人工智能等关键架构使能器对网络韧性的影响。该研究是较早指出 6G 网络安全、隐私和可信研究重要性的工作,然而,其并未系统地提出安全、隐私以及可信的评价体系和需求,表 3 详细分析了该研究在四维可信服务化网络评价指标体系中的覆盖程度。

Rodriguez 等^[77]提出了一种面向 6G 无线与计算生态的安全服务管理架构 (HORSE),通过借助人工智能算法,实现 AI 驱动的端到端安全服务编排。在安全方面,架构集成了威胁检测与防护引擎、数字孪生和分布式可信 AI 引擎,实现预测性威胁识别与自动化响应。在隐私保护方面,通过策略与数据治理模块保障,支持数据匿名化、访问控制和加密传输。在可信保障方面,该架构通过对 AI 模型的解释性与合规性进行评估,确保决策过程透明可靠。在韧性方面,通过端到端主动安全连接管理器 (ePEM) 和跨域编排连接器,实现多域资源动态调度与故障恢复,提升系统在攻击下的持续服务能力。

Mahmoud 等^[78]和 Kelley 等^[79]分别提出将深度学习和物理层安全相结合的 6G 网络安全防护框架,旨在提升 6G 通信网络在面对多种物理层攻击时的安全性能。该框架通过设置多阶段检测机制,采用随机森林混合模型抽取网络特征,并采用

长短期记忆网络 (long short-term memory, LSTM) 模型进行序列学习,从而提高分类准确性,提升处理复杂数据模式的效率。该框架能够在多种攻击,例如,欺骗、干扰和窃听攻击中显著提升比特错误率 (bit error rate, BER) 和分类准确率,展现出在复杂通信环境中增强安全性的潜力。在隐私方面,强调通过物理层安全和 AI 驱动的检测机制保护分享数据的隐私性,防止未授权访问和数据泄露。特别地,该架构通过在 6G 服务化架构中引入“隐私平面”,以支持医疗、车联网等高敏感场景的安全通信。在可信性方面,虽未直接展开讨论,但指出为进一步提升网络的安全性和可信性,可以采用零信任机制与 AI 结合的方式,提升网络的整体安全。在韧性方面,通过模拟多种攻击场景并展示模型在攻击下的持续性能,体现了系统在面对干扰和异常时的恢复与适应能力。特别是在高噪声和复杂信道条件下,机器学习和混合模型仍能保持较低的 BER 和较高的准确率,显示出较强的通信韧性。

Baldoni 等^[80]提出了一个以数据为中心的全分布式边缘原生 6G 网络架构。该架构打破了 5G 及前代网络以主机为中心的集中式管理模式,基于以数据为中心的理念,采用数据流机制,将 6G 网络构建为一个动态服务链,有效增强网络的灵活性和资源的利用率。同时讨论了该架构下安全和韧性两方面的跨层设计理念:在服务层,提供基于内容的端到端安全和差错容忍的保障;在数据链路层,采用 TLS 或 mTLS 安全协议实现多跳安全;在原子功能层,采用传统认证和访问控制实现网络功能间的安全保障。

Blika 等^[33]系统调研了联邦学习在 5G/6G 安全生态中的角色。该调研工作覆盖智慧城市、工业物联网、卫星网络等多个应用场景,分析了联邦学习在 5G/6G 网络应用中可能面临的安全风险和威胁,例如投毒攻击、后门攻击、推理攻击等;讨论了多种保障联邦学习安全应用的使能技术,例如差分隐私、同态加密、安全多方计算等技术,并详细对比了这些技术的防御效果。在安全方面,详述了数据投毒、模型投毒、拜占庭等

攻击在6G大规模异构终端下采用联邦学习的安全威胁，提出了结合鲁棒聚合、安全多方计算与区块链审计等技术提升AI全局模型的完整性的研究思路。在隐私保护方面，指出联邦学习中上传的梯度数据仍可能泄露用户信息与属性，推荐使用本地/联邦差分隐私、梯度压缩或选择性掩码等隐私计算技术，实现数据不出域且模型可用的隐私保障。在可信性方面，讨论了AI的可信性，要求联邦学习在6G中具备可解释性、可验证性与公平性等可信要求，并建议通过联邦解释模型与零信任架构联动，持续评估节点信任值。在韧性方面，讨论了在非独立同分布、设备异构与频繁掉线等情况下对联邦学习模型收敛的影响，建议通过异步聚合、客户端选择及量子安全通信等手段增强系统在面对节点失效与恶意行为时的可靠性和韧性。

Abedi等^[81]分析了在未来移动网络中采用零信任架构增强服务架构网络安全性和韧性的可能性，分别讨论了直接通信场景、间接通信场景、API网关以及漫游场景下采用零信任架构保证认证、授权以及通信加密和数据完整性保护的方法。在直接通信场景中，NRF节点被定义为零信任网络中的策略决定节点进行访问请求的认证和授权；在间接通信中，SCP的中转削弱了点ToPoint安全通信的保障。因此，可以通过网络功能消费者授权SCP获取访问令牌的方式，保障访问的可信性和灵活性；在API网关场景中，NEF节点可以作为策略决定节点保障非3GPP网络功能与核心网网络功能直接相互认证和授权访问；在漫游场景中，由于5G网络引入了SEPP，因此，借助SEPP的位置和能力，可以实现本地网络与漫游网络间网络功能的安全访问。虽然该研究较为详细地讨论了现有SBA架构下实现零信任安全保障的拓展，然而，其并未对零信任架构下的隐私保护、可信保障以及网络韧性进行讨论，具有较大的局限性。

Liu等^[82]提出一个名为SOLIDS的6G移动网络架构，通过引入数据面、AI面、安全面、共享合作面四大逻辑平面，解决5G高成本、高功耗、运维复杂等问题，实现网络功能的自生成、自愈合、自进化。在安全方面，该架构包含一个

原生安全面，基于AI策略引擎动态编排安全功能，实现主动免疫与零接触运维，并支持安全能力的分享和共建。在隐私方面，数据面支持数据的本地清洗、脱敏订阅等功能，避免原始用户数据出域，以满足数据隐私保护的法规要求。在可信方面，该架构通过数字孪生面实时映射物理实体状态，结合区块链式共识形成“可信孪生体”，供多方验证并建立信任。在韧性方面，架构采用云原生微服务与数字孪生预演，可在孪生环境先行验证补丁或配置，再热迁移至实际网络，降低试错风险并实现网络级故障自愈。

Chatzieleftheriou等^[83]提出了一个名为ORIGAMI的6G移动网络架构。该架构通过引入3个新型组件——计算连续层（CCL）、全球服务化架构（GSBA）与零信任暴露层（ZTL），以及对应的3个新型智能控制回路，有效克服了现有5G网络架构面临的8项技术障碍，实现了6G网络的性能提升。在安全和可信方面，通过在零信任暴露层引入垂直和水平零信任支持能力，分别实现对外部服务提供商的零信任网络功能支持（垂直）和其他运营商及IP交换网络（IPX）提供商的统一安全管理，此外，通过采用去中心化身份与可验证凭证，使设备身份不再绑定单一运营商，实现身份即服务与动态可信协商。在韧性方面，计算连续层支持异构算力的动态资源匹配和调整，当某域资源故障时，可实现毫秒级重调度，保障业务不中断。

Groen等^[84]系统探讨了开放无线接入网络在5G及未来网络中的安全威胁与评估问题，重点分析了开放接口、AI原生智能控制与云平台三大核心组件所面临的安全威胁与防护策略。同时，分别针对上述三大组件，通过多项实验评估了IPsec加密对E2接口的时延、吞吐量与CPU负载的影响，采用基于AI的技术，例如自编码方式降低攻击威胁的影响，并提出了云计算平台安全风险的降低手段等。在安全方面，指出开放接口若无加密保护极易遭受中间人攻击、KPI伪造攻击与控制指令注入等攻击威胁，提出必须实施IPsec/TLS等加密、身份认证与完整性校验机制，实现接口的安全保护。在隐私方面，虽未深入讨

论用户数据或身份匿名化机制,但指出 AI 模型训练数据若被污染(如虚假 KPI 注入)将导致错误决策,隐含了对数据真实性与隐私完整性的关注。在可信方面,建议采用零信任架构保障 O-RAN 各种开放功能间的信任建模,并通过持续的动态风险和可信评估,实现对 O-RAN 乃至 6G 网络的安全保障。在韧性方面,实验表明即使在高吞吐量场景下,IPsec 引入的处理时延仍小于 50 μ s,且通过硬件加速或流量限制可进一步缓解 CPU 压力,显示出系统在面对安全增强带来的负载挑战时具备良好的弹性适应能力。

华为于 2025 年 ETSI 安全大会上首次提出了面向下一代智能服务化网络的“Max Trust”信任防护架构^[85]。该架构旨在解决传统零信任架构在性能、用户隐私、智能体支持能力以及多域网络环境中适配性不足等问题,重点围绕“多模态、多实体、智能化、异构性”四大网络特点,通过建立三大信任支柱,即多维信任(M-trust)、智能信任(A-trust)以及跨域信任(X-trust),构建多维度智能 AI 信任架构,以满足 AI 与通信深度融合场景下的信任需求,保障下一代服务化网络的安全和可信。在安全方面,该架构提出可采用多种新型加密技术和认证技术,实现对网络接入认证、安全通信、数据保密处理等多项安全需求的支持;在信任方面,该架构指出可采用多维信任根和区块链等技术,实现灵活的可信评估和信任关系建立;在隐私方面,可信执行环境(TEE)和联邦学习等技术的采用可实现对于用户数据的隐私保护。但是,该架构目前缺少具体的细节方案支撑,有待进一步完善。

由表 3 可知, Khorsandi 等^[76]较早地系统探讨了 6G 安全使能技术,因此在保密性、完整性、用户标识隐私保护等基础指标上覆盖较全,但在服务链可靠性、AI/ML 系统的鲁棒性等深层次可信与韧性指标上明显不足,反映出早期研究对系统性可信与韧性问题的关注有限。Rodriguez 等^[77]的 HORSE 架构与 Liu 等^[82]的 SOLIDS 架构均强调 AI 在安全策略动态编排中的作用,因此在自适应能力、透明性等指标上表现突出,但两者在用户行为隐私保护、隐私保护的可配置性与可见性方面覆盖较弱,表明智能编排中对用户隐

私策略的灵活支持尚不充分。Baldoni 等^[80]以数据流为核心构建服务链,在安全共享、容错能力等指标上具有优势,但在双向认证、基础信任设施管理等身份认证与信任基础设施方面存在明显缺口,体现了以数据为中心的设计对传统安全信任机制的挑战。Abedi 等^[81]尝试在 SBA 中应用零信任原则,在双向认证、细粒度授权和访问控制等指标上覆盖良好,但几乎未涉及快速恢复能力、容错能力等指标,说明零信任在移动网络中的韧性保障机制尚未成熟。Blika 等^[33]系统分析了联邦学习在 5G/6G 中的安全角色,在用户行为隐私保护、透明性等指标上表现突出,但较少涉及端到端安全、空口安全等方面,反映出联邦学习研究仍集中于数据与模型层,对底层通信安全的结合不足。Mahmoud 与 Kelley 等^[78-79]通过深度学习与物理层安全技术结合提升抗干扰与防窃听能力,在保密性、完整性等指标上有所贡献,但在用户隐私保护、可信机制方面覆盖较弱,表明物理层安全研究尚未与高层隐私可信机制深度融合。Chatzieleftheriou 等^[83]的 ORIGAMI 框架通过引入零信任暴露层与计算连续层增强 6G 网络安全,在双向认证、细粒度授权和访问控制、自适应能力等指标上表现良好,但在用户位置隐私保护、备份机制的有效性等指标上覆盖不足,反映出云原生架构在位置隐私与数据恢复方面的设计缺口。Groen 等^[84]通过实验评估 O-RAN 接口安全与 AI 威胁,在保密性、可用性、资源管理与监控等指标上表现突出,但在用户隐私保护、基础信任设施管理方面存在明显不足,凸显了开放架构中隐私与可信保障的薄弱环节。华为提出的 MAX Trust 架构围绕多维信任、智能信任与跨域信任构建,在基础信任设施管理、服务链可靠性、安全共享等指标上具有前瞻性,但在快速恢复能力、高可用性等韧性指标上覆盖较弱,表明工业界在概念创新与工程落地之间仍需平衡。

3.2 身份与证书管理

在用户身份管理领域,多项相关工作采用去中心化的架构对身份和证书进行管理,意图提升网络的整体安全性和可靠性。身份与证书管理相关工作安全、隐私、可信及韧性比较与总结见表 4。

表4 身份与证书管理相关工作安全、隐私、可信及韧性比较与总结

指标	安全指标														隐私指标					可信指标							韧性指标					
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	P1	P2	P3	P4	P5	T1	T2	T3	T4	T5	T6	T7	R1	R2	R3	R4	R5	R6
文献[86]	●	●	○	●	●	○	●	●	○	●	●	○	○	○	●	○	○	○	●	●	●	●	○	○	○	○	●	○	○	○	○	○
文献[87]	○	○	●	●	○	●	●	●	○	●	●	○	●	○	○	○	○	●	○	●	●	●	○	○	○	○	●	●	○	○	●	●
文献[88]	●	●	●	●	●	●	●	●	○	●	●	○	○	○	●	○	○	●	●	●	●	●	○	○	○	○	●	●	●	○	●	●
文献[89]	●	●	●	●	●	●	●	●	○	●	●	○	●	○	●	○	●	●	●	●	●	○	○	○	○	○	●	●	●	●	●	●
文献[90]	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Garzon 等^[86]提出了一种面向 6G 服务化架构的去中心化身份与访问控制机制。该方案采用 DID 与可验证凭证（verifiable credentials, VC）替代传统 X.509 证书与 OAuth2.0 令牌授权，解决多域网络中身份管理与授权的信任问题。在安全方面，该方案通过去除中心化证书机构，采用分布式架构，避免单点故障与跨域信任链断裂，提升整体系统的安全性；在隐私方面，通过采用可验证凭证实现身份与权限的可验证呈现，避免敏感身份信息的泄露，增强用户隐私保护能力；在可信方面，系统通过 DID 与 VC 建立自我主权身份模型，实现网络功能之间的可验证身份与权限交互，强化跨域通信的信任关系；在韧性方面，该方案虽未讨论所提出系统的韧性，但通过去中心化机制与可验证凭证的分布式管理，该方案可间接提升系统对节点失效或攻击的适应能力，提升网络韧性。

Garzon 等^[87-88]分析了 6G 多利益相关方环境下传统 PKI 的跨域信任瓶颈，提出采用 DID、自我主权身份（self-sovereign identity, SSI）管理技术以及分布式账本技术（distributed ledger technology, DLT）构建无证书颁发机构（certification authority, CA）的身份管理层，为漫游服务、网络切片与过顶业务（over-the-top, OTT）接入服务等提供灵活安全的接入和认证服务。在安全方面，通过 DLT 持久化 DID 文档内置公钥与验证方法，支持网络运营商之间以及网络功能之间的双向认证，消除单点失败。在隐私方面，用户数据以 VC 形式保存在终端钱包，链上仅存放非敏感 DID 文档，实现“数据可证而身份不可见”；此外，采用盲签名与选择性披露机制进一步隐藏用户属性。在可信方面，通过构建信任三角模型，

实现跨域信任的建立，任何通信方可凭链上公钥即时验证对方 DID 所有权，防止任何单方篡改身份状态，且无须中心背书。在韧性方面，分布式账本天然抗单点故障，凭证失效信息可秒级同步至所有节点。然而，该工作未对账本自身分叉或 DDoS 攻击的应对策略进行分析。

Mohamed 等^[89]和 Kiyemba 等^[90]分别针对移动核心网络 and 传统互联网，提出了基于联邦身份管理的分布式身份管理方案。Mohamed 等^[89]针对面向服务的架构（SOA）跨组织联邦身份管理面临的身份盗用、单点失效等威胁，提出了基于 PKI 的自适应安全架构。该架构通过加入智能安全引擎模块，采用双因子认证、交易令牌哈希与动态可信协商等机制，在保持单点认证方案兼容的同时提升抗攻击强度。在安全方面，以 PKI 为核心，通过数字签名与哈希链实现信令级别的安全保障，并测试了抵御 10 种主流攻击的量化结果。在隐私方面，强调了用户身份和属性数据的隐私保护需求，提出了身份联邦场景下的隐私威胁的扩大，然而，该研究并未给出详细的解决方案。在可信方面，该架构借助于传统的中心式 PKI 构建多个身份提供商（identity provider, IdP）之间的信任关系，然而，其无法有效避免 PKI 的单点故障问题。在韧性方面，采用分布式部署智能安全引擎的方式支持故障切换，即使某一 IdP 宕机，系统仍可通过链路服务将用户重定向至备用 IdP，从而保证联邦系统的高可用与业务连续性。Kiyemba 等^[90]针对 5G 网络中跨域身份管理的安全问题，提出一种适用于 5G 网络的联邦身份管理（federated identity management, FIdM）模型，通过引入身份提供者、服务提供者及身份代理等实体，实现跨运营商、跨服务域的单点登

录 (single sign on, SSO) 与统一认证授权, 解决多租户环境下的身份互操作问题。在安全方面, 采用 OAuth2 与 3GPP AKA 结合的二次认证机制, 确保用户在访问不同网络切片或外部服务时仍具备统一且可验证的安全上下文, 防止未授权访问。在隐私方面, 通过使用伪身份 (EID)、临时令牌与通用公共订阅标识符 (generic public subscription identifier, GPSI) 替代用户永久身份标识, 避免用户永久标识在跨域访问中暴露。在可信方面, 通过跨域 PKI 信任关系、身份映射协议以及 IdP 与服务提供者 (service provider, SP) 之间的联盟协定等机制, 建立起用户、网络与服务之间的可信交互框架, 确保身份断言可验证且不可伪造。在韧性方面, 模型引入 IdP 代理与 SP 代理作为中间代理, 支持跨平台身份转换与服务发现, 能在部分 IdP 失效或网络分区情况下维持认证流程, 但未深入讨论在联盟节点遭攻陷或证书失效时的自动撤销与恢复策略。

分析表 4 可知, Garzon 等^[86]的研究采用 DID 与可验证凭证替代传统证书, 在用户标识隐私保护、隐私保护的可配置性与可见性、基础信任设施管理等指标上表现突出, 但在密钥管理、容错能力等指标上覆盖不足, 表明去中心化身份方案在密钥安全生命周期与系统抗故障能力方面仍存在技术挑战。Garzon 等^[87-88]的另一项研究进一步探讨了 DID 与自我主权身份在 6G 多利益相关方环境中的应用, 在双向认证、基础信任设施管理等指标上有较好表现, 但在用户位置隐私保护、备份机制的有效性等方面尚未进行深入研究, 反映出分布式身份在动态环境下的隐私与韧性保障仍需加强。Mohamed 与 Kiyemba 等^[89-90]的研究基于 PKI 与联邦协议实现跨域身份管理, 在双向认证、端到端安全、合规性与标准化等指标上表现良好, 但在用户行为隐私保护、基础信任设施管理等指标上存在明显不足, 体现了传统联邦身份方案在隐私保护深度与信任去中心化方面的局限性。

3.3 网络攻击检测

网络攻击检测能力是实现网络内生安全、快速响应威胁、保障可靠网络服务的重要能力和手段。由于 5G 网络架构向虚拟化和服务化转变,

近年来, 涌现出诸多基于服务化架构的网络攻击检测研究工作。该类工作结合服务化架构的开放能力和人工智能的强大潜力, 为下一代移动网络的智能、实时、高效的网络攻击检测能力开拓了诸多可能性。基于 O-RAN 的攻击检测相关工作安全、隐私、可信及韧性比较与总结见表 5。

Chen 等^[91]提出了一种针对空天地一体化 6G 车联网的接入侧 DDoS 攻击防御架构。通过在接入侧部署分布式控制点, 联合本地控制器, 共同构建了一个快速、无缝且具有高隐私保护的车联网防护边界, 有效防护恶意流量的渗透。在安全方面, 强调将攻击检测能力下沉到接入侧, 采用基于博弈论的主动防御决策、多域协同检测和自优化分组采样策略, 实现对恶意流量的尽早检测并阻断, 避免威胁移动核心网以及消耗网络资源。在隐私保护方面, 通过采用区块链网络实现身份与信任值的安全管理, 用户身份信息和信任等级信息仅在控制平面处理, 避免上传至云端, 从而保护用户的隐私。在可信方面, 通过基于区块链的可信评估机制, 记录用户设备历史行为, 实时评估用户节点的信任值, 通过信任等级实现对通信实体的可信管理。该研究的韧性体现在架构支持跨域协同与应急防御切换, 能够快速响应 DDoS 攻击并维持服务连续性。

Sedjelmaci 等^[92]提出一个基于零信任架构的协同攻击检测框架, 旨在保护 6G 边缘计算网络免受网络攻击。该架构通过“云-边-端”3 级检测链与非合作博弈动态触发协同策略, 提高网络的健壮性并降低时延, 使得网络快速恢复、自适应和容错能力得到提升。在安全方面, 以“永不信任、持续验证”为原则, 采用签名规则、强化学习以及联邦学习的混合检测机制, 可识别 DDoS、Botnet、零日攻击等网络攻击。在隐私方面, 通过采用联邦学习技术, 实现仅交换模型梯度, 避免原始安全数据出域, 保护设备行为特征和数据的隐私。在可信方面, 通过博弈收益函数实时量化节点可信度, 通过对比误报及漏报成本与计算开销, 控制节点间协同合作, 防止恶意节点滥用协作。在韧性方面, 由于采用动态零信任架构, 可根据攻击强度自适应切换本地轻量化

表 5 基于 O-RAN 的攻击检测相关工作安全、隐私、可信及韧性比较与总结

指标		安全指标										隐私指标					可信指标						韧性指标										
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	P1	P2	P3	P4	P5	T1	T2	T3	T4	T5	T6	T7	R1	R2	R3	R4	R5	R6
文献[91]		○	●	●	●	○	●	○	○	○	●	○	●	○	○	●	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
文献[92]		●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	●	●	○	●	●	●	●	●	●	●	●
文献[93]		●	●	●	○	○	○	●	●	○	○	○	●	○	○	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○
文献[94]		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
文献[95]		○	●	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[96]		○	●	●	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[97]		●	●	●	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[98]		●	●	●	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[99]		●	○	●	●	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[100]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[101]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[102]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[103]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[104]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[105]		○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

检测与跨域协同检测模式, 可在 60% 的恶意流量场景下, 仍保持 90% 以上的检测率与低于 5% 的误报率, 且计算开销降低 30%。

Wen 等^[93]设计了一个基于 O-RAN 架构的攻击检测系统。该系统以面向安全协议审计为目标, 通过将用户端和网络功能节点的流量信息和事件信息整合为统一的 Mobiflow 数据类型, 再设置攻击检测规则, 实现对 20 多种针对接入网和核心网攻击的有效识别, 从而实现安全内生的设计。在隐私方面, 虽未具体讨论隐私保护策略, 但其中部分攻击涉及用户身份信息和用户位置信息泄露, 例如身份链接攻击、针对 LTE 的位置跟踪攻击等, 通过提出的防御机制, 可对用户身份信息和位置信息提供有效的保护。在可信方面, 多次提到 O-RAN 架构与核心网之间的信任关系, 并以零误报的实验结果建立 RAN 以及核心网对 xApp 输出的信任。在韧性方面, 该系统可在每秒 4 万包负载的高强度网络流量下, 维持低于 2% 的中央处理器占用率与 500 ms 时延, 实现高效的攻击检测效率和有效的资源利用率。

Amachaghi 等^[94]全面梳理基于 O-RAN 架构的入侵检测系统的安全挑战和对应策略, 涵盖了加密、身份验证和访问控制。该研究提出了技术—非技术双层威胁分类法, 对比了 5 种入侵检测系统并给出集中、分布、边缘、云化 4 种部署架构, 为后续 5G/6G 切片、人工智能、区块链增强的入侵检测系统研究提供路线图。在安全方面, 全面分析了 O-RAN 扩大的攻击面, 具体包括虚拟机管理程序漏洞、恶意 xApp、接口注入、供应链篡改等攻击, 主张在各开放接口布设入侵检测探针实现安全内生的设计。在隐私方面, 从位置隐私、身份隐私与元数据隐私等方面进行讨论, 提出可采用假名、盲签名、联邦学习等技术无线智能控制器层隐藏用户真实身份, 同时警告人工智能机器学习梯度交换可能泄露训练数据隐私。在可信方面, 提出了“零信任入侵检测系统”的概念, 对所有无线单元/分布式单元/集中式单元节点与 xApp/rApp 持续验证, 通过区块链互认、OAuth2.0 与相互传输层安全建立信任锚点, 实现网络的信任建立和维护。在韧性方面, 指出分布式入侵检测系统比集中式更具弹性, 可

在边缘无线智能控制器失效时由云端接管, 并引入自愈机制利用人工智能预测攻击并动态迁移虚拟网络功能, 实现分钟级业务恢复。

Kouchaki 等^[95]通过在 O-RAN 架构中集成入侵检测和安全切片 xApp, 实现了对接入网入侵检测的快速识别以及恶意用户的及时隔离功能。在安全方面, 入侵检测 xApp 通过订阅物理资源块、参考信号接收功率等指标, 对拒绝服务、伪基站等安全威胁实现快速检测, 随后, 入侵检测 xApp 向安全切片 xApp 发送威胁消息, 利用切片级调度将攻击者锁进隔离切片, 形成检测到响应的闭环。在韧性方面, 利用安全切片 xApp 对恶意用户进行动态切片资源重配, 实现对攻击的快速隔离和对系统的防护, 表现出较强的系统韧性。在隐私和可信方面, 该研究并未涉及。

Tsourdinis 等^[96]同样基于 O-RAN 架构, 采用了多个 AI/ML 算法, 提出异常流量检测器 xApp。该检测器采用随机森林对 UPF 镜像流量进行分类, 一旦判定拒绝服务立即触发无线资源控制连接释放并重分配物理资源块, 使合法用户吞吐量提升近 1 倍、往返时延从 3 s 降至 18 ms, 中央处理器占用降 15%。在安全方面, 异常流量检测器通过数据包操控工具深度解析通用无线分组封装隧道数据, 对安全相关特征实时推理, 识别恶意流量。在隐私方面, 强调仅提取包头统计特征, 不解析用户面内容, 且用户设备标识在异常流量检测器内部映射为临时哈希, 避免人工智能推理时的隐私泄露, 符合 GDPR 中对数据隐私保护的最小化原则。在韧性方面, UPF 可在持续高速 DoS 攻击下保持稳定, xApp 通过滑动窗与比例缩放算法自动调整资源分配, 展现出弹性的资源伸缩与自愈能力。

Hung 等^[97]针对 O-RAN 中近实时无线智能控制器面临的多种攻击, 提出一种异常流量检测模块。该模块通过内置状态机与协议一致性校验功能, 实时识别并阻断来自 E2 接口和 xApp 的恶意信令, 实现对不期望流量和 DoS 攻击的识别和阻断。在安全方面, 列举出了多种针对 E2 接口以及第三方 xApp 的注入攻击和 DoS 攻击, 检测模块通过验证信令合法性并采用协议一致性进行有

效阻断,实现对移动网络接入网的安全性增强。在隐私方面,并未提及用户身份隐私和位置隐私等隐私保护需求。在可信方面,借助状态机验证技术实现信任边界的建立,实现报文可信性检测。在韧性方面,模拟了针对E2接口的DoS攻击,在开启检测模块后,系统的时延从无限大缩短到100 ms,有效避免了系统E2接口的系统崩溃,提升了系统的韧性。

Xavier等^[98]提出一个基于人工智能的O-RAN跨层多源信息融合异常检测系统。该系统通过识别多层多源信息,例如物理层、MAC层以及网络层等重要特征,采用机器学习算法构造智能分类器,以xAPP的形式部署于近实时RIC,实现恶意流量早期识别。在安全方面,针对缺乏移动网络综合数据集的问题,通过构建开源测试平台和流量生成器,创建了带有标签的多源移动网络安全流量数据集,用于安全检测模型的训练和测试,实现对攻击源头检测的安全目标。然而,该研究并未对数据隐私、信任架构以及系统韧性进行讨论。

Soleymani等^[99]提出一个基于O-RAN架构的3层异常检测系统。该系统通过在RAN部署一个dApp和在nRT RIC部署2个智能xAPP,实现对异常行为的分层级检测。部署在RAN的dApp,由于靠近分布式单元(distributed unit, DU)和集中单元(centralized unit, CU)节点可以实现对恶意行为的快速检测;部署在nRT RIC的xApp-U,通过融合更多的数据,实现了对异常行为检测精度的提升;部署在nRT RIC的xApp-S,通过采用更深层的神经网络算法,并采集多层用户行为数据,可以实现对用户行为模式的精准识别,支持未知行为的检测。在安全方面,主要聚焦对DDoS攻击威胁的检测,通过集成防火墙和外部动态列表实现对威胁的主动安全防御,确保网络安全。在隐私方面,指出未授权用户行为可能造成对用户数据的未授权访问和隐私泄露,但并未给出详细的隐私保护方法,而是提出通过对未授权行为的发现和防御,避免隐私泄露。在韧性方面,通过精准的异常检测和及时的策略更新,保障RAN可以快速响应高强度DDoS攻击下的业务韧性。

Başaran等^[100]提出一种基于深度自编码器的用户侧射频异常检测算法。该算法通过在O-RAN近实时RIC中部署深度自编码器,识别用户设备侧的射频异常,从而为用户和设备提供无缝的切换服务。在安全方面,通过检测射频异常间接增强了系统对潜在无线层攻击的识别能力,但未明确归类为攻击类型或提出响应机制。在可信方面,强调使用预训练模型以保证推理输出的可靠性,体现出对模型一致性和系统稳定性的重视。在韧性方面,通过提升异常检测准确率增强系统对异常行为的适应能力,表现出一定的系统韧性提升。实验表明,相较于传统隔离森林算法,该研究所提算法在准确率上提升了10%,适用于高维数据场景并支持动态结构调整。

Ratti等^[101]探讨了如何利用O-RAN架构增强移动网络中定位、干扰检测以及攻击检测的能力。提出通过将人工智能算法以xApp形式部署于O-RAN,可以实现对干扰检测、用户定位与入侵检测系统(intrusion detection system, IDS)的性能的大幅度提升。在安全方面,系统分析了O-RAN面临的威胁并提出基于机器学习的检测与定位机制,显著增强了网络对恶意行为的识别与响应能力。在隐私方面,并未深入讨论用户身份或位置等信息的隐私保护问题。在可信方面,通过持续监测KPI等数据,间接体现出对数据可靠性和系统监控能力的信任构建。在韧性方面,通过实时检测与定位攻击源,系统具备快速响应与自我恢复能力,展现出较强的网络韧性。

Yao等^[102]和Chen^[103]提出一种结合可解释AI与统计学习的异常检测方法,基于O-RAN设备的运行数据(如RRC连接数)识别异常并触发自动重启机制,通过现场测试验证其在实际网络中的有效性,并强调模型的可解释性对运营商的重要性。在安全方面,通过异常检测机制提升了系统对设备故障或潜在攻击的识别能力,增强了网络运行的安全性。在隐私方面,未深入讨论用户数据保护或敏感信息处理机制。在可信方面,强调可解释AI的作用,使运营商能够理解模型决策过程,从而增强对系统判断的信任。在韧性方面,通过自动检测与响应机制,系统可在异常

发生时快速恢复运行, 体现出较强的系统韧性。

Rumesh 等^[104]提出了一种基于联邦学习的异常检测系统。该系统基于数字孪生网络 (digital twin network, NDT), 通过在分布式 E2 节点和近实时 RIC 上进行分层模型学习, 最终在非近实时 RIC 上进行模型聚合, 实现对 3 种 5G 业务切片的高精度识别与攻击检测。在安全方面, 该系统采用 LSTM 模型, 对各个 E2 节点和近实时 RIC 节点的上下行链路信息模式进行学习, 实现对 DDoS、僵尸网络以及干扰等攻击行为的检测, 显著提升了网络的安全防护能力。在隐私方面, 通过联邦学习实现本地训练与参数聚合, 避免原始数据上传, 有效保护了用户数据隐私。在可信方面, 通过分析 E2 节点、RIC 节点以及 NDT 平台的可信性, 构建起分布式学习和攻击检测的信任模型, 增强了系统对 AI 决策的信任。在韧性方面, 通过分布式检测与持续学习能力, 能够快速适应新型攻击并维持网络运行, 展现出极强的网络韧性。

Alves 等^[105]提出采用监督式机器学习模型, 例如多层感知机、决策树以及支持向量机等模型, 基于 3 个开源移动数据集, 通过 t-SNE 降维技术, 处理融合多 KPI 移动数据, 实现在多种数据不平衡场景下的检测准确率达 90% 以上。在安全方面, 重点关注信道相关信息变化, 如信令风暴、伪造流量或资源滥用等, 强调通过 AI 模型提前识别以防止服务降级与网络入侵等威胁。在隐私方面, 未深入讨论用户身份或位置信息的匿名化机制, 但指出 KPI 数据需脱敏处理以防泄露用户轨迹与网络拓扑信息, 体现对敏感数据保护的隐含关注。在可信方面, 模型通过对正常行为基线学习与维护, 以高置信度分类结果支撑可信网络状态判断, 从而增强运维人员对系统状态的信任。在韧性方面, 实验显示即使在异常样本占比极低的极端不平衡场景下, 模型仍保持高 F1 分数 (F1-score), 表现出对罕见攻击或未知异常的鲁棒识别与弹性响应能力。

分析表 5 可知, Chen 等^[91]的研究针对车联网接入侧 DDoS 攻击防御, 在快速恢复能力、安全共享等指标上表现突出, 但在用户位置隐私保护、用户行为隐私保护等指标上覆盖较弱, 反映出跨

域协同防御中对隐私保护机制的整合不足。在零信任协同检测框架方面, Sedjelmaci 等^[92]的研究采用“永不信任、持续验证”原则, 在双向认证、细粒度授权和访问控制、快速恢复能力等指标上覆盖全面, 但在隐私保护的配置性与可见性、软件供应链安全等指标上存在短板, 表明零信任框架在隐私策略灵活性与供应链可信保障方面有待深化。Wen^[93]的 5G-Spector 系统、Amachaghi^[94]的入侵检测综述、Kouchaki^[95]的集成检测与切片安全方案、Tsourdinis^[96]的 AI 驱动资源分配检测、Hung^[97]的 E2 接口异常检测、Xavier^[98]的跨域 AI 早期检测、Soleymani^[99]的 DDoS 攻击检测与缓解、Başaran^[100]的射频异常检测、Ratti^[101]的物理层攻击检测、Yao^[102]与 Chen^[103]的可解释异常检测、Alves^[105]的机器学习异常检测等研究均基于 O-RAN 开放接口与 xApp 部署检测功能, 在保密性、完整性、资源管理与监控等指标上普遍表现良好, 但在用户标识隐私保护、用户位置隐私保护等指标上普遍缺失, 凸显了 O-RAN 检测方案对用户隐私保护的集体忽视。在 AI/ML 异常流量检测方面, 上述多数研究利用机器学习识别恶意流量, 在资源管理与监控、自适应能力等指标上多有贡献, 但在透明性、AI/ML 系统的鲁棒性等指标上普遍薄弱, 说明现有 AI 检测模型在决策透明度与对抗攻击抵抗力方面存在共性缺陷。Rumesh 等^[104]的研究基于数字孪生与联邦学习实现分布式检测, 在用户行为隐私保护、可验证性等指标上表现突出, 但在端到端安全、高可用性等指标上覆盖不足, 反映了联邦学习在保障端到端通信安全与服务持续性方面的挑战。

3.4 O-RAN 安全与冲突管理

O-RAN 的开放性和可编辑性为智能化接入网和实现新的部署场景提供了可能性。然而, O-RAN 平台上的众多 RIC 应用 (xApp、rApp 等) 可能来自不同的服务商和运营商, 它们之间的配置和相互调用可能面临较大的配置和管理冲突, 从而产生隐性的安全漏洞, 被攻击者利用, 威胁接入网、用户以及整个网络的安全。本节重点调研现有面向 O-RAN 平台的安全和冲突检测以及管理方案, 评估方案对安全、隐私、可信等的影响和保障, 为 O-RAN 的冲突检测和缓解提供安

全建议。O-RAN 安全与冲突管理与用户设备安全相关工作安全、隐私、可信及韧性比较与总结见表6。

Sultana 等^[106]在开源 O-RAN 平台上实现了针对 RIC 中 xApp 间直接配置冲突检测的原型系统。在近实时 RIC 中进入一个中心控制代理，采集各 xApp 间的信息，进行分析和比对，实现对 xApp 配置和操作的冲突检测。在安全方面，将 xApp 间的冲突视为安全完整性风险，该类风险可引起恶意或失控 xApp 的关键参数覆盖，从而引发服务中断；而中心控制代理通过实时监控消息日志与签名时间戳为事后审计提供可追溯的安全证据。在隐私方面，并未讨论相关内容，但对 xApp 间消息的监控和采集，必然会对 xApp 的数据隐私造成威胁，因此，有必要采取相应的数据隐私保护方案进行保护。在可信方面，平台采用默认不可信的冲突控制方式，所有 E2 控制消息必须经中央控制代理仲裁，只有被标记为无冲突后才下发，从而在 RIC 内部建立对第三方 xApp 的信任边界。在韧性方面，可以保障 10 ms 级间隔信令冲突的快速检测、裁决与重配置，保持 RAN 资源状态一致，体现出控制环的弹性恢复能力。

Adamczyk 等^[107]提出了一个针对 O-RAN 近实时 RIC 中 xAPP 决策冲突的冲突缓解框架。该框架定义了一个冲突检测代理，通过记录 RAN 控制信令和监控 RAN 节点性能管理数据，按标准中制定的优先级裁决，实现对 3 种冲突的检测和有效缓解，从而提升网络的性能。仿真结果显示，该架构可有效降低切换失败率与呼叫阻塞率。在安全方面，将 xApp 决策冲突视为影响安

全的错误配置，通过预检测能力，避免指令冲突，从而保障控制面安全。在可信方面，强调标准化冲突缓解流程是迈向可信控制面的关键步骤，并指出可以借助 RIC 间的共享信息建立多厂商 xAPP 的互信和协同。在韧性方面，实验结果显示启用冲突检测架构后，多项指标（例如平均基站负载、用户满意度、呼叫阻塞以及切换数量）均有大幅度改善，表明框架可提升网络在 xApp 决策失配场景下的性能韧性。

D' Oro 等^[108]针对现有 O-RAN 标准中控制时延过大，无法支持高精度用例管理和控制的问题，提出了分布式 dApp 的概念。dApp 通过将智能控制功能容器化，并下沉部署至 CU 和 DU，从而实现 10 ms 内级别的实时推理和管控，有效支持时延敏感型用例，例如成波束管理与用户调度等下层功能。在安全和隐私方面，只讨论了移动用户相关数据的安全本地保护，指出跨层数据采集和处理的安全和隐私风险，用以支持 dApp 在底层 CU 和 DU 部署和推理的合理性。在可信方面，dApp 的引入使得 O-RAN 的可信管控更为复杂，xApp、rApp 以及 dApp 间的信任模型面临更大的挑战。因此，需要引入更为智能和可信的安全和差错管控机制，保障 O-RAN 的安全和可信运行。在韧性方面，实验显示 dApp 可有效降低 E2 接口的流量，并在信道条件快速变化下维持 4 ms 级别的超可靠超低时延通信（uRLLC）时延，体现出对高动态环境的强韧性。

Noe 等^[109]全面剖析了 O-RAN 演进过程中，多厂商、多接口与 AI/ML 自动化引入导致的配置错误以及可能引起的安全威胁等问题。分析指出，O-RAN 系统的错误配置，不仅可能导致网

表6 O-RAN 安全与冲突管理与用户设备安全相关工作安全、隐私、可信及韧性比较与总结

指标	安全指标														隐私指标					可信指标							韧性指标					
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	P1	P2	P3	P4	P5	T1	T2	T3	T4	T5	T6	T7	R1	R2	R3	R4	R5	R6
文献[106]	○	●	●	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	○	●	●	●	○	○	●	●	●	●	●	○	○	●
文献[107]	○	●	●	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	○	●	●	●	○	○	●	●	●	●	●	○	○	●
文献[108]	●	○	●	○	○	●	●	○	●	●	●	○	●	●	●	●	●	○	●	●	●	○	●	●	●	●	●	●	●	●	●	●
文献[109]	○	○	●	○	○	●	○	○	○	○	○	○	●	●	○	○	○	○	○	●	○	○	○	○	●	○	○	●	○	○	○	●
文献[110]	●	○	●	○	○	●	○	●	○	○	○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○	○	●	○	○	○	●
文献[111]	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
文献[112]	●	●	●	●	●	●	○	○	○	●	○	●	○	○	●	●	○	○	●	●	●	○	○	○	○	●	●	○	●	○	○	○

络性能劣化,而且可能使系统面临严重的安全漏洞。系统梳理了AI/ML自身在数据、模型与策略层面的配置风险。在安全方面,详细列举了错误配置可能导致的安全后果,如默认端口未关闭、认证协议未启用、xApp间策略冲突等,这些都可能被利用以发起各种攻击,例如中间人攻击、拒绝服务或恶意节点注入攻击等;建议可在O-RAN系统中采用零信任架构实现对各组件行为的持续可信评估和验证。在隐私方面,指出通过采用xApp或rApp引入AI模型进行错误配置的检测和缓解,需要大量的RAN数据进行训练,这将对UE的数据隐私造成较大的威胁。若未对UE身份进行匿名化或未加密训练数据,将直接泄露用户位置与行为轨迹,违反数据最小化原则。指出可以采用联邦学习等隐私计算方法支持智能的差错配置环节。在可信方面,讨论了因为AI的不可解释性而引起的缺失问题。在韧性方面,主张利用数字孪生、图神经网络与强化学习实现从被动修复到主动容错的配置管理闭环,提升网络在配置漂移或恶意利用场景下的弹性恢复能力。

Shami等^[110]提出了基于图卷积神经网络(graph convolutional network, GCN)的xApp冲突预测与分析系统GRAPHICA。该系统通过收集xApp间复杂且隐含的依赖关系、控制参数以及KPI,用于实时对xApp间可能的冲突进行预测,并分析定位冲突的根本原因。该系统可以检测识别直接、间接与隐性冲突,解决多厂商AI应用目标不一、参数耦合或策略重叠导致的性能抖动与安全隐患。在安全方面,指出xApp间的配置和调用冲突如果未被及时检测,则系统可能被恶意xApp利用发起DoS或资源占用等多种攻击,因此,快速识别冲突并定位潜在风险xApp是保障O-RAN安全的基础。在可信方面,通过图结构追溯多个xApp的冲突,并输出可信冲突报告,为运营商提供可审计、可问责的决策依据,增强对多厂商应用行为的信任。在韧性方面,通过正则化显著提升模型对稀有冲突样本的鲁棒性,并结合数字孪生实现闭环验证,确保网络在遭遇异常或攻击时仍能维持服务稳定性,显示出良好的弹性适应能力。

Armstrong等^[111]提出了一种面向O-RAN服

务管理与编排功能的冲突检测架构,旨在解决非近实时RIC中多个自主管理代理(rApp)在网络优化过程中可能引发的配置冲突问题。该架构通过聚类分析和时间序列相似性评估,预测配置变更对网络KPI的潜在负面影响,从而提前识别并避免性能退化。在安全方面,虽未直接讨论安全风险问题,但通过识别行为的非预期影响,有效增加了对系统安全配置变更可能带来风险的防范。在可信方面,强调通过预测机制确保配置变更的可控制性,从而保障对系统行为的可预期性,保障系统的可信性。在韧性方面,提出的预测与反馈机制可增强系统在面对多个rApp并行操作时的稳定性与容错能力,实质上提升了系统在网络动态变化下的韧性表现。

分析表6可知,Sultana与Adamczyk等^[106-107]的研究通过在RIC中引入控制代理或冲突缓解框架,在策略冲突检测、快速恢复能力等指标上表现良好,但在用户标识隐私保护、基础信任设施管理等指标上均未涉及,表明冲突管理研究普遍未将隐私与信任作为核心设计考量。在分布式dApp实时控制方面,D'Oro等^[108]的研究将智能功能下沉至CU/DU,在快速恢复能力、资源管理与监控等指标上具有优势,但在用户位置隐私保护、基础信任设施管理等指标上覆盖不足,说明分布式控制中隐私保护与信任链构建尚未同步实现。Noe等^[109]的研究系统梳理了O-RAN错误配置引发的安全威胁,在策略冲突检测、用户行为隐私保护等指标上均有覆盖,但在服务链可靠性、备份机制的有效性等指标上存在不足,体现了智能运维中可靠性保障与数据恢复的薄弱环节。Shami等^[110]的GRAPHICA系统利用GCN建模xApp间依赖关系,在策略冲突检测、透明性等指标上表现突出,但在用户位置隐私保护、容错能力等指标上覆盖较弱,表明基于图的预测系统在隐私感知与故障容忍方面有待加强。Armstrong等^[111]的研究聚焦非实时RIC中rApp的配置冲突预测,在资源管理与监控、策略冲突检测等指标上有所贡献,但几乎未涉及双向认证、可验证性等指标,反映出SMO层冲突检测对安全身份验证与行为审计的关注不足。

3.5 终端设备安全

Bitsikas 等^[112]开发了一个面向 5G 独立组网 (5G standalone, 5G SA) 架构用户设备安全测试框架。该架构严格遵循 5G SA 在 NAS 和 RRC 层的消息结构和参数, 通过模块化的设计, 分析用户设备在与 5G 基站通信时存在的安全漏洞。通过搭建基于 Open5GS 和 srsRAN 的开源测试平台, 并对该测试平台进行代码修改, 支持 82 个安全相关的测试用例, 并对用户设备的上下行链路信令进行持续监测, 实现对安全攻击的检测。在安全方面, 通过实验, 发现了多个 5G SA 架构存在的设计级漏洞, 可被用于 DoS、伪基站附着与降级攻击, 表明 5G SA 在实现层仍继承部分 4G 网络架构的缺陷。在隐私方面, 测试显示在支持 SUCI 功能被禁用时, 用户设备在注册阶段以明文方式泄露 SUPI 或在身份请求中回传国际移动设备识别码 (IMEI), 暴露用户身份与设备指纹, 存在被追踪风险。在韧性方面, 实验发现部分设备在遭受异常消息或拒绝服务后无法自动恢复连接, 需手动重启或重新注册, 表明其在面对恶意输入或协议状态错乱时缺乏自我恢复与容错能力, 框架本身也未提供自动恢复或异常隔离机制。

分析表6可知,Bitsikas等^[112]的研究通过构建开源测试平台与测试用例,在保密性、完整性、可用性、双向认证、用户标识隐私保护等基础安全与身份隐私指标上覆盖较全,但在快速恢复能力、容错能力、基础信任设施管理、服务链可靠性等指标上有明显不足。这表明当前终端安全测试仍主要关注协议一致性与已知漏洞检测,

缺乏对设备在攻击下的自我恢复能力、硬件信任根、软件供应链安全以及服务交付可靠性等系统性可信与韧性问题的评估，终端安全研究需从“合规检测”向“韧性增强”与“可信构建”拓展。

3.6 应用场景安全

未来移动网络将作为经济社会发展的重要基础设施融入各个行业和领域，例如医疗健康领域、自动驾驶、车联网（V2X）、卫星网络、无人机网络等，其网络安全、隐私、韧性需求也将随应用领域和融合深度变化。本节重点调研了5G/6G网络在医疗、卫星、车联网中面临的特殊安全需求以及现有的研究工作。应用场景安全相关工作安全、隐私、可信及韧性比较与总结见表7。

(1) 医疗健康领域

医疗健康场景的核心特点是数据的极端敏感性与业务的生命攸关性，这要求网络在传输患者体征、手术指令等数据时，必须同时满足极致低时延、超高可靠性和绝对完整性的三重保障，而海量异构医疗物联网设备则显著扩大了攻击面，这一特点催生了多维度的核心安全需求。在安全层面，强化的端到端安全与数据完整性是全链路防止数据篡改的底线；细粒度访问控制是实现基于医疗角色与情境的动态授权关键。在隐私与可信层面，严格的标识与行为隐私保护是法律与伦理红线；可验证性则是建立医患数字信任、确保AI辅助诊断等操作可审计的基石。尤为关键的是，数据安全与高可靠性之间存在着根本性的设计矛盾：确保数据机密性与完整性的高强度加密

表7 应用场景安全相关工作安全、隐私、可信及韧性比较与总结

指标	安全指标														隐私指标					可信指标							韧性指标							
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	P1	P2	P3	P4	P5	T1	T2	T3	T4	T5	T6	T7	R1	R2	R3	R4	R5	R6		
文献[113]	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
文献[114]	●	●	○	●	○	○	●	○	○	●	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	○	●	○	○	○	○	○	○	
文献[115]	●	●	○	●	●	○	●	○	○	●	○	○	○	○	●	○	○	○	●	○	○	○	●	○	○	●	○	○	○	○	○	○	○	
文献[116]	○	●	●	○	○	●	●	○	○	○	●	○	●	○	○	○	○	○	●	●	○	●	○	○	●	●	●	●	○	○	○	○	●	
文献[117]	○	○	●	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	○	○	○	○	○	●	○	●	●	●	○	●	○
文献[118]	●	●	●	●	●	○	●	●	○	●	○	○	○	○	●	●	○	●	●	●	●	○	●	○	●	●	○	●	●	○	○	○	●	
文献[119]	●	●	●	●	●	●	●	●	○	●	●	○	●	○	●	○	○	●	●	●	●	○	●	○	●	●	○	●	●	○	○	○	●	
文献[120]	●	●	○	○	●	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	

与认证机制会引入计算与通信时延,而保障高可靠性的冗余传输、前向纠错等策略则会增加带宽消耗与协议复杂性,两者共同作用,对极致的低时延与确定性传输构成严峻挑战。然而,现有研究在将这些需求转化为可行方案时存在显著不足。Arastouei 等^[113]虽然前瞻性地提出了一个结合 AI 与区块链的多层安全隐私框架,但其分析过于宏观,缺乏针对具体临床业务流程(如远程手术控制流)的端到端安全协议设计与性能量化评估,也未能在网络动态波动时,给出如何实时、自适应地权衡数据安全强度与传输可靠性以保障核心业务连续性的具体机制。更根本的挑战在于,当前方案普遍陷入安全、隐私与性能难以调和的三元困境。例如,基于区块链或高级密码学的隐私保护方案虽能提升安全性,但其引入的计算与通信开销往往难以满足远程手术等应用对微秒级时延和确定性的苛刻要求。尤为关键的是,现有研究严重忽视了 AI 模型自身的安全与可信问题,未能有效针对针对诊断或控制 AI 的投毒、逃逸等攻击,而这些攻击一旦得逞,将直接导致生命危险。因此,构建一个能同时满足强安全隐私、确定性能与 AI 可信,并能在安全机制与可靠性策略之间实现智能动态平衡的医疗网络架构,仍是有待突破的核心难题。

分析表 7 可知,Arastouei 等^[113]研究构建了覆盖物理层、网络层与应用层的多层安全隐私框架,体现出医疗场景对保密性、完整性、用户标识隐私保护、用户位置隐私保护、用户行为隐私保护等基础安全与隐私指标的全面重视。这源于医疗数据的高敏感性与法规(如 HIPAA、GDPR)的严格合规要求。该研究在物理层引入智能反射面与分子通信技术以提升物理层安全容量,在网络层结合 SDN/NFV 与 AI 实现灵活的安全策略部署,在应用层则关注全息影像与数字孪生技术带来的新型隐私风险。然而,在基础信任设施管理、服务链可靠性、AI/ML 系统的鲁棒性、高可用性等深层次可信与韧性指标上覆盖较弱。这反映出医疗场景研究目前仍侧重于静态数据保护与访问控制,对跨域医疗设备间动态可信建立、远程手术等服务链的实时可靠性保障、医疗 AI 模型对抗攻击的鲁棒性,以及系统在故障

或攻击下的持续服务能力等系统性问题的探索尚处于起步阶段。

(2) 车联网领域

车联网场景的核心特点是通信实体海量且匿名、安全要求与实时决策深度耦合。车辆既是信息的消费者也是生产者,其广播的刹车预警等消息的真实性直接关乎集体安全,而车辆的连续移动则使得传统的中心化安全管理模式失效,这一特点催生了多维度的核心安全需求:在安全层面,空口安全与消息完整性是防御伪基站攻击与消息伪造的生命线;在隐私层面,位置隐私保护必须防止车辆轨迹被长期追踪;在可信与韧性层面,可审计性为事故定责提供证据链,而自适应能力则是网络应对突发流量与局部故障的关键。尤为关键的是,隐私保护、实时响应与系统处理效率之间存在着根本性的设计矛盾:确保身份匿名与数据隐私的机制(如差分隐私、假名变换)会显著增加通信与计算开销,而保障消息实时可靠广播的低时延要求又与复杂的安全协议相冲突,这使得在高速动态环境中实现安全、隐私与性能的协同优化面临严峻挑战。现有研究在应对上述挑战时存在明显局限。Boulalouache 等^[114]采用联邦学习进行协同攻击检测,其价值在于保护了数据隐私,但其引入的差分隐私等保护机制会显著增加模型训练与聚合的时延,难以满足高速动态场景下实时碰撞预警的要求。这暴露了现有方案普遍陷入的隐私、实时性与效率难以调和的三元困境。Kohli 等^[115]虽系统梳理了认证方案,但缺乏能统一实现车辆身份匿名性与消息可验证的轻量级协议框架。更为严峻的是,现有研究极少涉及“跨域协同安全”,未能实现为跨境、跨运营商车辆建立无缝可信的身份与信任关系,这使得全球无缝车联网愿景面临基础性障碍。因此,构建一个能同时实现强隐私保护、低时延通信、高效处理并支持跨域信任的 V2X 安全架构,仍是有待突破的核心难题。

分析表 7 可知,Boulalouache 等^[114]针对 6G-V2X 跨域网络切片场景,提出了基于多进程联邦学习与堆叠泛化的协同攻击检测方案,在安全共享、用户标识隐私保护等指标上表现突出。该方案通过切片隔离与联邦学习实现跨运营商数据协同,

体现了车联网对跨域协同与数据隐私的强烈需求。Kohli等^[115]则系统梳理了6G车联网在工业5.0与IoE背景下的认证方案与安全挑战，强调了车辆与路边单元、车辆与车辆通信中面临的DDoS攻击、消息篡改、冒充等威胁。这两项研究均显示出车联网对实时、可靠通信的依赖，因此在安全共享、用户标识隐私保护指标上着力较多。然而，两者在端到端安全、自适应能力指标上存在明显不足。Boualouache^[114]的研究未深入探讨车辆到核心网、车辆到云端的全程安全通道保障；Kohli^[115]的研究虽提及多种认证机制，但缺乏对车辆在高速移动、网络拓扑剧变环境下动态调整安全策略的自适应机制分析。这表明现有车联网安全研究在保障“通信全链路安全”与“环境动态适应”方面仍需加强，以适应6G车联网超低时延与高可靠性的要求。

（3）卫星网络领域

卫星网络（空天地一体化）场景的核心特点是信道高度开放、传播时延高、节点高速移动且拓扑时变、星上资源严格受限、运维更新极困难。这些特点使得其既易受窃听与干扰，又难以部署复杂的地面安全机制，由此催生了极具特殊性的核心安全需求。在安全层面，强化的端到端安全需求迫切，但需克服高时延对传统握手协议的制约；动态的密钥管理必须适应卫星频繁进出地面站视野的拓扑变化。在可信与韧性层面，软件供应链安全是确保星载软件在发射前绝对可信的命门；容错与备份能力则是应对单粒子翻转等空间环境威胁、维持星座整体服务不中断的核心。尤为关键的是，强安全需求与资源受限、高动态环境之间存在着根本性矛盾：复杂的密码学保障与频繁的密钥更新会消耗稀缺的星上计算与通信资源，而高时延、断续的连接使得传统基于实时交互的安全协议效率低下。现有研究在应对上述挑战时存在不足。尽管Han等^[116]和Cui等^[117]指出了内生安全与韧性需求，但大多数方案仍停留在单点技术创新（如设计轻量级星间认证协议），缺乏从星座系统全局视角出发，统一规划安全、路由与资源调度的韧性架构。一个被长期忽视的风险是空间物理故障在网络层面的级联效应，例如单粒子翻转可能导致卫星数据错误并通

过星间链路扩散，引发区域性服务降级，而对此类风险的建模与缓解机制研究才刚刚起步。更为严峻的挑战在于，在星地网络深度融合的背景下，跨天基与地基网络的统一信任管理、安全策略协同与动态编排仍是尚未充分探索的深水区。因此，构建一个能在资源严格受限、环境高度不确定的太空中实现内生安全、全局韧性并可管理跨域信任的卫星网络架构，是6G空天地一体化网络面临的核心难题。

分析表7可知，Han等^[116]的研究从网络层视角梳理了卫星网络标准化进展与安全挑战，重点关注卫星高速移动、星间链路时变带来的路由与移动性管理问题，因此在资源管理与监控、自适应能力指标上有所涉及。Cui等^[117]则提出了天地一体化网络的内生安全需求，强调通过可信技术与动态安全编排实现主动防御。这两项研究均认识到卫星网络开放、广域覆盖的特性带来的新型攻击面（如星地信令伪造、星际链路窃听等），但在用户标识隐私保护、基础信任设施管理指标上存在显著短板。Han等^[116]的研究未对用户通过卫星接入时的身份匿名化与防追踪机制进行深入探讨；Cui等^[117]的研究虽提出内生安全理念，但未给出构建星地、星间统一信任根的具体方案。这凸显了卫星网络因全球覆盖、节点异构、管理域多元等特点，在实现用户身份隐私与跨域信任传递方面面临比地面网络更严峻的挑战，这也是未来研究的重点与难点。

（4）其他领域

除上述三大高价值场景外，无人机网络、工业物联网等同样是6G全服务化网络的关键应用领域。这些场景普遍具有设备异构、控制实时、网络拓扑动态的特点，并由此引发了对虚拟化隔离、细粒度访问控制、分布式身份可信与系统自愈韧性的共性安全需求。针对这些共性挑战的现有研究仍显分散且存在局限。在无人机网络方面，如Abdalla等^[118]所指出的，现有3GPP标准虽定义了无人机认证与位置验证的基础框架，但其方案高度中心化，难以应对无人机集群的快速组网与协同任务场景中所需要的分布式、轻量级信任建立问题。同时，该研究也承认，对于无人机在非授权空域或信号拒止环境中的安全通信，现

有标准尚存空白。在更广泛的工业物联网与边缘计算场景中, Ali 等^[119]提出的零信任框架虽然为动态环境下的细粒度访问控制提供了宝贵思路, 但其架构严重依赖于持续的策略决策与上下文收集, 在资源严格受限的工业设备或高实时性控制回路中可能引入不可接受的时延与开销。Seyed 等^[120]在无人机安全跟踪上的工作则揭示了另一个普遍困境: 其采用的强化学习算法虽提升了跟踪与入侵检测的智能化水平, 但模型本身的可解释性与对抗鲁棒性不足, 这在安全攸关的工业控制中构成了新的风险点。

综上所述, 现有研究大多针对特定场景的单一问题提出点状解决方案, 缺乏一个能贯通不同垂直行业、在架构层面统一纳管虚拟化隔离、动态可信、韧性恢复与 AI 可信等核心挑战的系统性框架。因此, 未来的关键研究方向在于超越场景差异, 构建一个可编程、可证明, 并能与网络智能深度融合的 6G 全服务化内生安全基础架构。

4 开放问题与未来研究方向

基于对国内外研究现状的调研分析和比较, 本节总结了下一代服务化网络在安全、隐私、可信和韧性方面的几个开放问题, 并指出解决这些问题以及提升 6G 全服务化网络整体安全性和隐私性等的重点研究方向。

4.1 开放问题

通过对比现有标准化工作和国内外文献, 在本文所构建的指标体系之下, 总结发现: 在安全方面, 缺乏一个面向未来全服务化智能网络的统一安全架构, 且资源管理监控以及策略冲突检测和安全共享方面的研究涉及较少, 尚存在诸多不足; 在可信方面, 服务链可靠性方面研究较少; 在韧性方面, AI/ML 系统的鲁棒性方面研究涉及较少。关于现有研究的几个开放问题的详细介绍如下。

1) 网络架构不清晰。根据第 3 节对现有工作的评估分析 (见表 3) 可知, 在网络安全架构研究中, 仅文献[77]和文献[82-83]提出了相对完整的架构, 但均未形成覆盖安全、隐私、可信、韧性四维指标的统一框架。其余文献中, 文献[76]虽较早探讨了 6G 安全使能技术, 但在 AI 鲁棒性 (R5) 上完全缺失; 文献[80]以数据为中心的架

构在双向认证 (S4)、基础信任设施管理 (T4) 上存在明显缺口。此外, 零信任、区块链等新型安全理念的应用仍停留在概念验证层面 (如文献[82]仅分析场景而未量化认证开销)。在高频微服务调用场景中, 频繁的令牌验证可能导致系统吞吐量下降超过 30%, 难以满足 6G 微秒级时延要求。在跨域信任建立方面, 基于去中心化标识符与可验证凭证的方案^[86-87]依赖区块链共识, 在跨国漫游等大规模场景下身份验证时延可达数百毫秒, 且与现有 3GPP 认证与密钥协商协议存在兼容性障碍。因此, 构建面向未来智能服务化网络的统一安全架构迫在眉睫。

2) 网络态势感知滞后与动态策略冲突。根据第 3 节对现有工作的评估分析 (见表 5~表 6) 可知, 在冲突管理研究中, 文献[106-107]和文献[110]在策略冲突检测 (S14) 上均有涉及, 但在资源管理与监控 (S13) 方面普遍不足, 且均未实现实时动态策略自适应调整。文献[108]指出, 当前管理框架对供应链漏洞 (如 CVE-2023-48761) 的可见性严重不足。在攻击检测研究中, 仅文献[92]、文献[94]和文献[104]实现了动态策略冲突的实时感知与自适应调整 (R2), 其余均未覆盖该指标。在 O-RAN 实践中, 第三方开源库漏洞 (如 libssh2 的 Terrapin 攻击) 可被利用入侵系统、篡改 xApp; 多厂商 xApp 间的策略冲突^[107]可能导致资源分配错误, 甚至被利用演变为新型 DoS 攻击向量。现有框架对此类风险的可见性与控制力明显不足。

3) 数据壁垒与隐私计算效率困境。根据第 3 节对现有工作的评估分析 (见表 7) 可知, 在应用场景研究中, 需要跨域协同的场景, 如车联网^[114]、医疗文献^[113]中, 安全共享 (S11) 指标覆盖率不足 30%。联邦学习安全调研^[33]指出, 全同态加密等强隐私保护技术的计算开销比明文处理小 3 个数量级 (约 1/1 000)。文献[83]中基于联邦学习的车联网协同攻击检测方案, 在采用差分隐私后, 跨运营商模型聚合时延仍达秒级, 难以满足高速车联网实时响应需求。全同态加密在跨域用户行为分析中的联合查询响应时间是明文处理的 1 000 倍以上, 无法应用于 6G 核心网实时决策。综上, 突破数据壁垒与隐私计算效率困境,

构建多维度协同的隐私计算体系，是6G亟待解决的关键问题。

4) 服务链端到端可靠性保障挑战。根据第3节对现有工作的评估分析（见表3~表4）可知，在架构研究中，仅文献[80]和文献[82]明确涉及服务链可靠性（T6），且均未提供量化保障机制。在身份与证书管理研究中，去中心化身份方案（如文献[86-87]）在服务链层面缺乏端到端可信执行验证机制。在UPF服务化^[10]背景下，对深度数据包检测等计算密集型功能采用TEE全程保护，数据包处理吞吐量可能下降至少40%。以文献[80]中数据流服务链为例，若预处理微服务崩溃，依赖其结果的AI推理微服务将收到错误数据，可能触发错误的安全策略，而当前架构缺乏对级联故障的快速感知与隔离机制。性能与安全的矛盾尚未得到有效解决。

5) AI/ML模型的安全脆弱性。根据第3节对现有工作的评估分析（见表3、表5~表6）可知，现有标准和文献对AI的安全性覆盖不足。例如，仅文献[92]和文献[94]涉及AI鲁棒性（R5），覆盖率不足10%，且均为定性讨论，未提供量化评估；仅文献[109]讨论了AI模型配置风险，未深入分析对抗脆弱性；文献[77]和文献[82]在透明性（T1）上仅提供了概念描述。此外，AI在6G中深度嵌入接入网、核心网和终端，但其自身面临对抗样本攻击，如随机森林被恶意流量绕过^[96]、梯度反推隐私泄露^[114]等，攻击者可使AI以高置信度分类恶意流量完全绕过检测。同时，若AI系统被破坏，所有依赖AI的安全机制将同步失效。因此，必须构建“AI增强安全、传统机制兜底”的双重保障体系：部署独立于AI的传统IDS作为最后防线；建立多源证据可信评估；在AI异常时自动切换至静态策略或人工授权模式。

4.2 未来研究方向

为应对上述全服务化网络演进过程中遇到的各种挑战，需要综合考虑用户端、接入网以及核心网的安全、隐私、可信以及韧性需求以及6G网络的系统性能指标，重点开展如下研究。

1) 针对网络架构不明确的问题，需要在面向下一代智能体网络和服务化互联的安全和可信需

求中，研究全面覆盖安全、隐私、可信和韧性需求的高可信网络安全架构。针对新型网络场景和架构演进，深入研究和融合多种新型安全技术，例如AI、区块链、隐私计算、可信计算等，广泛采纳多种新型安全防务理念，例如，零信任理念、Max Trust理念^[85]等可信理念，尽快构建下一代移动网络可信安全架构。

2) 针对网络态势感知滞后与动态策略冲突问题，为应对网络态势及时感知缺乏的挑战，需重点研究动态可信管理技术与实时威胁感知技术。例如，研究微秒级威胁检测架构和轻量级行为分析引擎^[121]，通过过滤器实现信令流量监控，将攻击检测时延从分钟级降至毫秒级；采用数字孪生辅助决策，构建网络状态的虚拟镜像，通过并行仿真预判攻击路径，提前触发防御策略。在动态可信评估模型方面，设计上下文感知的信任评分机制，综合UE移动轨迹、服务调用模式、设备指纹等多维度特征，计算实体可信度；引入服务网格技术，通过在网络服务中嵌入信任管控代理，实现基于会话的动态权限调整等方法。在供应链攻击免疫方面，研究基于区块链存证的供应链清单机制，要求所有网络组件，包括第三方xApp在部署前提交完整的依赖树，并通过智能合约验证哈希一致性；研究基于联邦学习的跨境威胁检查框架，使运营商能共享威胁特征而不暴露原始数据，协同检测跨域供应链攻击。

3) 为突破数据隐私保护所带来的数据孤岛与隐私计算困境，需构建多维度协同的隐私计算体系。在算法层研发轻量级安全多方计算协议和动态联邦学习框架，结合混合加密技术提升计算效率；在标准层建立统一的数据交互规范和分级共享机制；在安全层，采用可信计算硬件、区块链等技术构建可验证计算环境；在系统层开发专用加速芯片并优化计算卸载策略。通过安全架构的搭建和数据隐私计算的创新，最终实现“数据不动价值动”的新型基础设施，既保障各参与方数据主权，又释放数据要素价值，为6G智能应用提供安全高效的数据支撑，推动形成开放共赢的运营商协作新生态。这一系统性突破将从根本上解决隐私保护与数据共享的矛盾，成为6G网络可持续发展的关键使能技术。

4) 针对服务链端到端可靠性保障挑战, 未来应重点研究: 构建去中心化的服务管理和编排框架, 实现故障的智能隔离与快速自愈; 结合硬件安全模块及密码学算法的安全验证技术, 研究轻量级可信执行验证机制, 在保证数据隐私的同时降低验证开销; 设计跨域信任协商协议, 建立统一的可信评估指标体系; 探索 AI 驱动的动态安全策略优化算法, 实现服务链性能与安全性的智能平衡; 研发支持弹性伸缩的安全验证中间件, 确保新加入实例的快速可信认证。这些创新举措将推动形成自主可控、弹性可扩展的 6G 服务链可信执行体系。

5) 针对 AI 增强安全以及 AI 的安全脆弱性问题, 未来应重点开展以下研究。第一, 构建 AI 与传统安全协同的防御体系。例如, 研究 AI 检测与传统 IDS 的融合架构, 提升攻击检测的时效性以及准确性; 设计动态可信评估与智能安全编排机制, 实现自适应威胁响应与协同防御; 采用新型分布式 AI 范式, 例如, 联邦学习, 实现跨域协同的安全隐私保护。第二, 研发抗干扰、可解释的可信 AI 技术^[122-123], 包括集成对抗训练与鲁棒优化提升模型对抗样本的抵抗能力, 研究可解释 AI 方法使决策过程透明可审计, 建立覆盖数据、训练、推理全生命周期的 AI 安全评估标准以量化评估 AI 鲁棒性。上述研究方向将共同推动 6G 网络 AI 系统在复杂对抗环境中实现安全、可靠、可解释的运行, 并通过传统安全机制的兜底保障, 形成“AI 增强安全、传统机制兜底”的双重保障体系。

为突破上述关键挑战, 需要学术界、产业界以及标准化组织深度协作, 通过创新技术、仿真测试和实证验证加速 6G 服务化架构的标准化和可靠落地。

5 结束语

6G 网络的全服务化架构作为通信技术的重大革新, 旨在通过全域覆盖、智能内生、数字孪生三大愿景构建灵活、高效且安全的下一代通信网络。然而, 随着架构的演进, 安全、隐私、可信和韧性问题日益凸显, 成为影响 6G 发展的关键挑战。本文围绕这些问题展开系统性调研, 取得了一系列成果: 首先, 充分调研了标准化组

织、运营商以及设备提供商针对下一代全服务化网络的标准化工作以及研究工作, 并总结了服务化演进中所涉及的安全、隐私、可信以及韧性的需求; 其次, 较为全面地分析了 6G 服务化网络面临的安全隐私风险, 并构建了四维可信服务化网络评价指标体系, 针对现有对于网络服务化安全、隐私、可信以及韧性研究评价体系的不足, 提供了新的评估视角和参考框架; 最后, 采用四维可信服务化网络评价指标体系, 针对当下 3GPP、O-RAN 联盟、运营商以及学术文献方案, 从网络安全架构、身份与证书管理、网络攻击检测、O-RAN 安全与冲突管理、终端设备安全以及应用场景安全 6 个角度进行全面梳理和分析, 揭示了现有标准和研究工作在安全防护、隐私保护、可信管理以及韧性等方面的不足, 并重点探讨了网络态势及时感知能力不足、数据孤岛与隐私计算难题、服务链可靠性问题以及 AI/ML 系统的鲁棒性问题等四大开放问题。

展望未来, 6G 安全研究需要在动态安全机制、跨域协同计算、可信服务链管理以及智能安全领域开展重点攻关, 突破技术和应用瓶颈, 以推动 6G 网络的健康发展。6G 全服务化网络的安全研究是一项复杂的系统工程, 需要学术界、产业界和标准组织的通力协作。本文的研究成果不仅为构建安全、可靠的 6G 网络奠定了基础, 也为未来通信技术的发展提供了参考。随着技术的不断进步, 6G 网络必将实现其“智能内生、安全内生”的愿景, 为社会带来更加安全、高效的网络服务。

参考文献:

- [1] 3GPP. System architecture for the 5G System (5GS), Release 19: TS 23.501[S]. 2025.
- [2] 3GPP. 5G System; Technical Realization of Service Based Architecture; Stage 3, Release 19: TS 29.500[S]. 2025.
- [3] GSA. GSA-5G_Standalone_april_2025_summary[R]. 2025.
- [4] 5G Americas. 5G-Advanced overview[R]. Bellevue: 5G Americas, 2025.
- [5] Nokia 贝尔实验室. 6G 服务化架构演进研究报告[R]. 2023. Nokia Bell Labs. 6G Service-oriented architecture evolution research report[R]. 2023.
- [6] 中兴通讯股份有限公司. 6G 网络智能化技术白皮书[R]. 2023. ZTE Corporation. 6G network intelligence technology white paper[R].

- 2023.
- [7] 中国电信研究院. 6G网络云化技术研究报告[R]. 2024.
China Telecom Research Institute. Research report on 6G network cloudification technology [R]. 2024.
- [8] 爱立信中国. 6G微秒级时延保障技术白皮书[R]. 2023.
Ericsson China. 6G microsecond-level latency guarantee technology white paper [R]. 2023.
- [9] 陈雁, 朱佩英, 童文. ITU-R WP5D 完成了 IMT-2030(全球 6G 愿景)框架建议书[R]. 2023.
Chen Y, Zhu P Y, Tong W. ITU-R WP5D completes the framework recommendation for IMT-2030 (Global 6G Vision) [R]. 2023.
- [10] 3GPP. Study on UPF enhancement for Exposure and SBA; Phase 2, Release 19: TR 23.700[R]. 2025.
- [11] 3GPP. Study on best security practices for the Service-Based Architecture (SBA), Release 20: TR 33.755[R]. 2025.
- [12] Rudolph H C, Kunz A, Iacono L L, et al. Security challenges of the 3GPP 5G service based architecture[J]. IEEE Communications Standards Magazine, 2019, 3(1): 60-65.
- [13] Duan X D, Wang X Y, Lu L, et al. 6G architecture design: from overall, logical and networking perspective[J]. IEEE Communications Magazine, 2023, 61(7): 158-164.
- [14] 中国移动. 中国移动 5G 服务化架构(SBA)白皮书[R]. 2025.
China Mobile. China Mobile 5G service-based architecture (SBA) white paper [R]. 2025.
- [15] 华为. 广域网络服务化白皮书[R]. 2022.
Huawei. Wide area network service-based white paper [R]. 2022.
- [16] 3GPP. Study on enhanced security aspects of the 5G Service Based Architecture (SBA), Release 18: TR 33.875[R]. 2023.
- [17] Dogra A, Jha R K, Jain S. A survey on beyond 5G network with the advent of 6G: architecture and emerging technologies[J]. IEEE Access, 2021, 9: 67512-67547.
- [18] Quy V K, Chehri A, Quy N M, et al. Innovative trends in the 6G era: a comprehensive survey of architecture, applications, technologies, and challenges[J]. IEEE Access, 2023, 11: 39824-39844.
- [19] Jiang W, Han B, Habibi M A, et al. The road towards 6G: a comprehensive survey[J]. IEEE Open Journal of the Communications Society, 2021, 2: 334-366.
- [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.
- [21] Akgul O U, Ericson M, Burguera P G, et al. Discussion on 6G architecture evolution: challenges and emerging technology trends[C]// Proceedings of the 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2024:664-669.
- [22] Yeh S P, Bhattacharya S, Sharma R, et al. Deep learning for intelligent and automated network slicing in 5G open RAN (ORAN) deployment[J]. IEEE Open Journal of the Communications Society, 2024, 5: 64-70.
- [23] Nguyen C T, Saputra Y M, Van Huynh N, et al. Emerging technologies for 6G non-terrestrial-networks: from academia to industrial applications[J]. IEEE Open Journal of the Communications Society, 2024, 5: 3852-3885.
- [24] Brik B, Chergui H, Zanzi L, et al. Explainable AI in 6G O-RAN: a tutorial and survey on architecture, use cases, challenges, and future research[J]. IEEE Communications Surveys & Tutorials, 2025, 27(5): 2826-2859.
- [25] Niknam S, Roy A, Dhillon H S, et al. Intelligent O-RAN for beyond 5G and 6G wireless networks[C]//Proceedings of the 2022 IEEE Globecom Workshops (GC Wkshps). Piscataway: IEEE Press, 2022:215-220.
- [26] Ammar S, Pong Lau C, Shihada B. An in-depth survey on virtualization technologies in 6G integrated terrestrial and non-terrestrial networks[J]. IEEE Open Journal of the Communications Society, 2024, 5: 3690-3734.
- [27] Prasad T S, Chinthaginjala R, Pau G, et al. Toward 6G: an overview of the next generation of intelligent network connectivity[J]. IEEE Access, 2025, 13: 925-961.
- [28] Coronado E, Behraves R, Subramanya T, et al. Zero touch management: a survey of network automation solutions for 5G and 6G networks[J]. IEEE Communications Surveys & Tutorials, 2022, 24(4): 2535-2578.
- [29] Yang M M, Qu Y Y, Ranbaduge T, et al. From 5G to 6G: a survey on security, privacy, and standardization pathways[J]. ACM Computing Surveys, 2026, 58(8): 1-38.
- [30] 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.
- [31] Farao A, Bolgouras V, Zarras A, et al. Cybersecurity challenges and pitfalls in 6G networks[J]. 2025.
- [32] Abou El Houda Z, Moudoud H, Khoukhi L. Blockchain meets O-RAN: a decentralized zero-trust framework for secure and resilient O-RAN in 6G and beyond[C]//Proceedings of the IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs). Piscataway: IEEE Press, 2024.
- [33] Blika A, Palmos S, Doukas G, et al. Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: a comprehensive survey[J]. IEEE Open Journal of the Communications Society, 2025, 6: 3094-3130.
- [34] 3GPP. Study of automatic certificate management environment (ACME) for the service based architecture (SBA), Release 19: TR 33.776[R]. 2025.
- [35] O-RAN Alliance. O-RAN technical specifications release 003 (Version 03.00)[S]. 2022.
- [36] O-RAN Alliance. O-RAN software community release H: functional enhancements and AI integration [R]. 2025.
- [37] O-RAN SCF&RIC Subgroup. Near-real-time RIC energy efficiency solutions using Python and mL algorithms[R]. 2025.
- [38] O-RAN ALLIANCE. Overview of open testing and integration centre (OTIC) and O-RAN Certification and badging [EB]. 2023.
- [39] O-RAN Alliance & 3GPP. Joint statement on 6g standardization roles and collaboration framework [EB]. 2025.
- [40] Telecom Infra Project (TIP) & O-RAN Alliance. Open RAN ecosystem expansion: MemO-RANdum of understanding[Z]. 2024.
- [41] O-RAN Alliance. Annual report: global O-RAN standardization

- and ecosystem development (2022 – 2025)[R]. 2025.
- [42] AI-RAN ORG. AI-RAN alliance vision and mission white paper[R]. 2024.
- [43] 中国移动. 5G-Advanced 技术创新与应用报告[R]. 2025.
China Mobile. 5G-Advanced technology innovation and application report[R]. 2025.
- [44] 工业和信息化部. 2025 年通信业统计公报[R]. 2025
Ministry of Industry and Information Technology. 2025 Communication industry statistical bulletin[R]. 2025.
- [45] 中国移动研究院. 5G RedCap 轻量化终端技术白皮书[R]. 2024.
China Mobile Research Institute. 5G RedCap lightweight terminal technology white paper[R]. 2024.
- [46] 中国移动, 中兴通讯. 工业互联网 5G-A RedCap 应用案例集[Z]. 2025.
China Mobile, ZTE Corporation. Industrial Internet 5G-A RedCap application case collection[Z]. 2025.
- [47] 中国移动通信集团有限公司. 中国移动 6G 网络架构技术白皮书[R]. 2022-06.
China Mobile Communications Group Co., Ltd., China Mobile 6G network architecture technology white paper[R]. 2022-06.
- [48] 中国移动, IMT-2030 推进组. 6G 全服务化架构(HSBA)技术愿景[R]. 2025.
China Mobile, IMT-2030 Promotion Group. Technical vision for 6G full service-based architecture (HSBA) [R]. 2025.
- [49] 中国电信. 中国电信 5G-A 商用网络建设报告[R]. 2025.
China Telecom. China Telecom 5G-A commercial network construction report[R]. 2025.
- [50] 中国电信, 华为. 5G-A 超级上行技术白皮书[R]. 2024.
China Telecom, Huawei. 5G-A super uplink technology white paper [R]. 2024.
- [51] 安徽移动, 华为. 京沪高铁宿州北段 5G-A 网络建设报告[R]. 2025.
Anhui Mobile, Huawei. 5G-A network construction report for the Suzhou north section of the Beijing-Shanghai high-speed railway [R]. 2025.
- [52] 武汉东湖高新区. 光谷新能源智能网联汽车产业发展规划(2022-2030)[Z]. 2023.
Wuhan East Lake High-Tech Development Zone. Optics valley new energy intelligent connected vehicle industry development plan (2022-2030)[Z]. 2023.
- [53] 中国电信研究院. 6G 网络架构关键技术研究报告[R]. 2025.
China Telecom Research Institute. Research report on key technologies of 6G network architecture [R]. 2025.
- [54] 中国电信, 华为. 5G-A 联合创新实验室技术成果[Z]. 2025.
China Telecom, Huawei. Technical achievements of the 5G-A joint innovation laboratory[Z]. 2025.
- [55] 3GPP. Security architecture and procedures for 5G System (Release 15): TS 33.501 V15.0.0[R]. 2018.
- [56] O-RAN.WG11.TS.Security-requirements-specification[R].2025.
- [57] NAMN 联盟. 6G 安全愿景白皮书[R]. 2023.
NAMN Alliance. 6G Trastworthiness Considerations[R]. 2023.
- [58] 中国移动. 2024 年 6G 数字孪生网络安全技术白皮书(1.0) [R]. 2024.
China Mobile. 2024 6G digital twin network security technology white paper (1.0) [R]. 2024.
- [59] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62-72.
Chen X J, Fang B X, Tan Q F, et al. Research on internal attack intention inference algorithm based on probabilistic attack graph[J]. Chinese Journal of Computers, 2014, 37(1): 62-72.
- [60] Michalopoulos D S, Gajic B, Gallego-Nicasio Crespo B, et al. Network resilience in virtualized architectures[C]//Interactive Mobile Communication Technologies and Learning. Cham: Springer, 2018: 824-839.
- [61] Sun R H, Wang Q X, Guo L. Research towards key issues of API security[C]//Cyber Security. Singapore: Springer, 2022: 179-192.
- [62] 张越, 陈庆旺, 刘宝旭, 等. 面向云原生的 API 攻击诱捕技术研究[J]. 西安电子科技大学学报, 2023, 50(4): 237-248.
Zhang Y, Chen Q W, Liu B X, et al. Research on API attack trapping technology for cloud native[J]. Journal of Xidian University, 2023, 50(4): 237-248.
- [63] Lemes M T, Alberti A M, Both C B, et al. A tutorial on trusted and untrusted non-3GPP accesses in 5G systems: first steps toward a unified communications infrastructure[J]. IEEE Access, 2022, 10: 116662-116685.
- [64] Weedage L, Magalhães S R C, Stegehuis C, et al. On the resilience of cellular networks: how can national roaming help? [J]. IEEE Transactions on Network and Service Management, 2024, 21(2): 1702-1714.
- [65] Aslan Ö, Aktuğ S S, Ozkan-Okay M, et al. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions[J]. Electronics, 2023, 12(6): 1333.
- [66] A. S. M. Asadujjaman. Integrity verification for virtualized networks using side-channel[D]. Montreal: Concordia University, 2023.
- [67] Zhang X G, Yang G H, Wasly S. Man-in-the-middle attack against cyber-physical systems under random access protocol[J]. Information Sciences, 2021, 576: 708-724.
- [68] Wani M S, Rademacher M, Horstmann T, et al. Security vulnerabilities in 5G non-stand-alone networks: a systematic analysis and attack taxonomy[J]. Journal of Cybersecurity and Privacy, 2024, 4(1): 23-40.
- [69] Islam M N U, Fahmin A, Hossain M S, et al. Denial-of-service attacks on wireless sensor network and defense techniques[J]. Wireless Personal Communications, 2021, 116(3): 1993-2021.
- [70] Hussain S R, Echeverria M, Singla A, et al. Insecure connection bootstrapping in cellular networks: the root of all evil[C]//Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2019.
- [71] Javanmardi S, Ghahramani M, Shojafar M, et al. M-RL: a mobility and impersonation-aware IDS for DDos UDP flooding attacks in IoT-Fog networks[J]. Computers & Security, 2024, 140: 103778.
- [72] Shaik A, Borgaonkar R, Asokan N, et al. Practical attacks against privacy and availability in 4G/LTE mobile communication systems[C]//Proceedings 2016 Network and Distributed System Security Symposium. Internet Society, 2016.
- [73] Gao K X, Wang H Q, Lyu H W, et al. Your locations may be lies:

- selective-PRS-spoofing attacks and defence on 5G NR positioning systems[C]//Proceedings of the IEEE INFOCOM 2023 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2023:1-10.
- [74] 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. New York: ACM, 2019: 669 - 684.
- [75] 华为技术有限公司. 6G愿景与关键技术白皮书[R]. 2025-05. Huawei Technologies Co., Ltd., 6G vision and key technologies white paper [R]. 2025-05.
- [76] Khorsandi B M, Bassoli R, Bernini G, et al. 6G E2E architecture framework with sustainability and security considerations[C]//Proceedings of the 2022 IEEE Globecom Workshops (GC Wkshps). Piscataway: IEEE Press, 2022: 1-6.
- [77] Rodriguez E, Masip-Bruin X, Martrat J, et al. A security services management architecture toward resilient 6G wireless and computing ecosystems[J]. IEEE Access, 2024, 12: 98046-98058.
- [78] Mahmoud H, Ismail T, Baiyekusi T, et al. Advanced security framework for 6G networks: integrating deep learning and physical layer security[J]. Network, 2024, 4(4): 453-467.
- [79] Kelley B, Ara I. An intelligent and private 6G air interface using physical layer security[C]//Proceedings of the MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM). Piscataway: IEEE Press, 2022:968-973.
- [80] Baldoni G, Quevedo J, Guimarães C, et al. Data-centric service-based architecture for edge-native 6G network[J]. IEEE Communications Magazine, 2024, 62(4): 32-38.
- [81] Abedi K, Nguyen G T, Strufe T. Improving resilience of future mobile network generations implementing zero trust paradigm[C]//Proceedings of the NOMS 2024-2024 IEEE Network Operations and Management Symposium. Piscataway: IEEE Press, 2024:1-5.
- [82] Liu G Y, Li N, Deng J, et al. The SOLIDS 6G mobile network architecture: driving forces, features, and functional topology[J]. Engineering, 2022, 8: 42-59.
- [83] Chatzieleftheriou L E, Gramaglia M, Garcia-Saavedra A, et al. Towards 6G: architectural innovations and challenges in the ORIGAMI framework[C]//Proceedings of the 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2024:1139-1144.
- [84] GROEN J, et al. Implementing and evaluating security in O-RAN: Interfaces, intelligence, and platforms[PP]. arXiv Preprint, 2024, arXiv:2304.11125.
- [85] Huawei. When trust meets AI-agentic networks: how the next-generation communication network should be designed? [C]// ETSI Security Conference 2025, Oct. 8, 2025.
- [86] Garzon S R, Dinh-Tuan H, Martinez M M, et al. Beyond certificates: 6G-ready access control for the service-based architecture with decentralized identifiers and verifiable credentials[C]//Proceedings of the 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2024:830-835.
- [87] Garzon S R, Yildiz H, Kupper A. Decentralized identifiers and self-sovereign identity in 6G[J]. IEEE Network, 2022, 36(4): 142-148.
- [88] Garzon S R, Yildiz H, Kupper A. Towards decentralized identity management in multi-stakeholder 6G networks[C]//Proceedings of the 2022 1st International Conference on 6G Networking (6GNet). Piscataway: IEEE Press, 2022:1-8.
- [89] Beer Mohamed M I, Hassan M F, Safdar S, et al. Adaptive security architectural model for protecting identity federation in service oriented computing[J]. Journal of King Saud University - Computer and Information Sciences, 2021, 33(5): 580-592.
- [90] Kiyemba Edris E K, Aiash M, Loo J K. The case for federated identity management in 5G communications[C]//Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC). Piscataway: IEEE Press, 2020:120-127.
- [91] Chen X, Feng W, Chen Y F, et al. Access-side DDoS defense for space-air-ground integrated 6G V2X networks[J]. IEEE Open Journal of the Communications Society, 2024, 5: 2847-2868.
- [92] Sedjelmaci H, Ansari N. Zero trust architecture empowered attack detection framework to secure 6G edge computing[J]. IEEE Network, 2024, 38(1): 196-202.
- [93] Wen H H, Porras P, Yegneswaran V, et al. 5G-spector: an O-RAN compliant layer-3 cellular attack detection service[C]//Proceedings 2024 Network and Distributed System Security Symposium. Internet Society, 2024.
- [94] Amachaghi E N, Shojafar M, Foh C H, et al. A survey for intrusion detection systems in open RAN[J]. IEEE Access, 2024, 12: 88146-88173.
- [95] Kouchaki M, Moore J, Zhang M L, et al. Advancing O-RAN security: integrated intrusion detection and secure slicing xApps[C]//Proceedings of the IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2024:1-2.
- [96] Tsourdinis T, Makris N, Korakis T, et al. AI-driven network intrusion detection and resource allocation in real-world O-RAN 5G networks[C]//Proceedings of the 30th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2024: 1842-1849.
- [97] Hung C F, Tseng C H, Cheng S M. Anomaly detection for mitigating xApp and E2 interface threats in O-RAN near-RT RIC[J]. IEEE Open Journal of the Communications Society, 2025, 6: 1682-1694.
- [98] Xavier B M, Dzaferagic M, Vilà I, et al. Cross-domain AI for early attack detection and defense against malicious flows in O-RAN [PP]. arXiv Preprint, 2024, arXiv:2401.09204.
- [99] Ahmad Soleymani S, Eslamnejad M, Alimohammadi H, et al. DDoS detection and mitigation using d/xApp in O-RAN[C]//Proceedings of the 2024 IEEE Future Networks World Forum (FNWF). Piscataway: IEEE Press, 2024:283-290.
- [100] Başaran O T, Başaran M, Turan D, et al. Deep autoencoder design for RF anomaly detection in 5G O-RAN near-RT RIC via xApps[C]//Proceedings of the 2023 IEEE International Conference on Communications Workshops (ICC Workshops). Piscataway: IEEE Press, 2023: 549-555.

- [101] Ratti S A, Piccioni A, Marotta A, et al. Enhancing mobile network security through O-RAN: architectural solutions for physical layer attack detection[C]//Proceedings of the 2024 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Piscataway: IEEE Press, 2024:1-3.
- [102] Yao C H, Chen Y A. Explainable AI and statistical learning for enhanced abnormal detection in O-RAN networks[C]//Proceedings of the 2024 International Conference on Consumer Electronics - Taiwan). Piscataway: IEEE Press, 2024: 655-656.
- [103] Chen Y A. Explainable AI based statistical learning scheme for joint abnormal detection and power control in O-RAN architecture[C]//Proceedings of the 2024 International Conference on Consumer Electronics. Piscataway: IEEE Press, 2024:723-724.
- [104] Rumes Y, Attanayaka D, Porambage P, et al. Federated learning for anomaly detection in open RAN: security architecture within a digital twin[C]//Proceedings of the 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2024:877-882.
- [105] Alves P V A, Goldbarg M A S S, Barros W K P, et al. Machine learning applied to anomaly detection on 5G O-RAN architecture[J]. Procedia Computer Science, 2023, 222: 81-93.
- [106] Sultana A, Bashar F, Chowdhury M R, et al. A software-defined radio based O-RAN platform for xApp conflict detection and mitigation[C]//Proceedings of the MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM). Piscataway: IEEE Press, 2024:686-687.
- [107] Adamczyk C, Kliks A. Conflict mitigation framework and conflict detection in O-RAN near-RT RIC[J]. IEEE Communications Magazine, 2023, 61(12): 199-205.
- [108] D'Oro S, Polese M, Bonati L, et al. dApps: distributed applications for real-time inference and control in O-RAN[J]. IEEE Communications Magazine, 2022, 60(11): 52-58.
- [109] Yungaicela-Naula N M, Sharma V, Scott-Hayward S. Misconfiguration in O-RAN: analysis of the impact of AI/ML[J]. Computer Networks, 2024, 247: 110455.
- [110] Shami M A, Yan J, Fapi E T. O-RAN xApps conflict management using graph convolutional networks[PP]. arXiv Preprint, 2025, arXiv:2503.03523.
- [111] Armstrong J, Fallon E, Fallon S. Pre-emptive conflict detection architecture for O-RAN service management and orchestration[C]//Proceedings of the 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT). Piscataway: IEEE Press, 2024: 335-340.
- [112] Bitsikas E, Khandker S, Salous A, et al. UE security reloaded: developing a 5G standalone user-side security testing framework[C]//Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2023: 121-132.
- [113] Arastouei N, Khan M A. 6G technology in intelligent healthcare: smart health and its security and privacy perspectives[J]. IEEE Wireless Communications, 2025, 32(1): 116-121.
- [114] Boualouache A, Jolfaei A A, Engel T. Multi-process federated learning with stacking for securing 6G-V2X network slicing at cross-borders[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(9): 10941-10952.
- [115] Kohli P, Sharma S, Matta P. Secured authentication schemes of 6G driven vehicular communication network in industry 5.0 Internet-of-everything (IoE) applications: challenges and opportunities[C]//Proceedings of the 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). Piscataway: IEEE Press, 2022: 1-5.
- [116] Han L, Dong L J, Retana A, et al. Evolution to 6G for satellite NTN integration: from networking perspective[C]//Proceedings of the 2023 IEEE 31st International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2023:1-6.
- [117] Cui H X, Zhang J, Geng Y H, et al. Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges[J]. China Communications, 2022, 19(2): 90-108.
- [118] Abdalla A S, Marojevic V. Security threats and cellular network procedures for unmanned aircraft systems: challenges and opportunities[J]. IEEE Communications Standards Magazine, 2022, 6(4): 104-111.
- [119] Ali B, Hijjawi S, Campbell L H, et al. A maturity framework for zero-trust security in multiaccess edge computing[J]. Security and Communication Networks, 2022, 2022: 1-14.
- [120] Ahmad Soleymani S, Shojafar M, Foh C H, et al. Secure target-tracking by UAVs in O-RAN environment[C]//Proceedings of the 2024 IFIP Networking Conference (IFIP Networking). Piscataway: IEEE Press, 2024: 204-212.
- [121] 吴佩翔, 张志龙, 陈力波, 等. 针对 5G 核心网协议的自动化漏洞挖掘方法[J]. 网络与信息安全学报, 2024, 10(1): 156-168.
- Wu P X, Zhang Z L, Chen L B, et al. Automated vulnerability discovery method for 5G core network protocol[J]. Chinese Journal of Network and Information Security, 2024, 10(1): 156-168.
- [122] 武影影, 毛伯敏. 面向 6G 智能反射面辅助的联邦学习安全速率优化[J]. 网络与信息安全学报, 2025, 11(2): 115-124.
- Wu Y Y, Mao B M. Federated learning secrecy rate optimization for 6G intelligent reflecting surface assistance[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 115-124.
- [123] 魏宣宣, 刘万平, 卢玲. 基于多模态特征融合的对抗样本防御方法研究[J]. 网络与信息安全学报, 2025, 11(2): 175-188.
- Wei X X, Liu W P, Lu L. Research on adversarial examples defense method based on multi-modal feature fusion[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 175-188.

[作者简介]



平子键 (2003-), 男, 西安电子科技大学硕士生, 主要研究方向为无线网络攻击与防御等。



王明君（1987-），男，博士，西安电子科技大学网络与信息安全学院讲师，主要研究方向为下一代移动通信安全和隐私保护、应用密码学等。



王海光（1973-），男，博士，华为技术有限公司谢尔德实验室资深研究员，主要研究方向为可信网络、AI代理安全协议、公钥证书管理、电信网络身份管理、认证与授权技术等。



闫峥（1972-），女，博士，西安电子科技大学网络与信息安全学院教授、博士生导师，主要研究方向为信任管理、可信AI、网络安全、隐私保护、区块链等。



李铁岩（1971-），男，博士，华为技术有限公司谢尔德实验室科学家，主要研究方向为未来网络与数字可信、AI安全、移动网络安全等。