5G网络环境下的通信协议安全性分析与改进

徐伟龙
日海恒联通信技术有限公司　河南　郑州　450000

摘　要：在5G网络环境下，通信协议开放性增强、架构复杂化，使其面临多维度安全威胁。本文针对通信协议层的主要风险进行系统分析，涵盖协议接口暴露、虚拟化架构漏洞、切片与边缘计算中的隔离缺失及应用层复合威胁。在评估现有物理、网络与应用层防护机制基础上，提出包括量子密钥分发、行为感知认证、切片级安全策略及AI入侵检测在内的改进路径，构建多层协同的安全防控体系。研究结果对提升5G协议通信链路的安全性和可信性具有现实指导意义。

关键词：5G通信协议；网络安全；动态密钥管理；智能检测

引言

5G技术以其高速率、低时延和大连接特性，成为新一代信息通信的基础支撑。然而，协议层结构的开放化、虚拟化与分布式架构设计显著拓展了攻击面，使通信协议成为潜在攻击的核心载体。面对API滥用、切片越权、行为伪装等新型威胁，传统静态安全机制已难以适配5G复杂多变的业务场景[1]。因此，系统分析其安全脆弱性，并从加密、认证、隔离与智能防御等维度提出可行改进策略，已成为保障5G网络稳定与可信运行的核心课题。

1 5G 通信协议面临的主要安全威胁分析

1.1 通信协议开放性带来的新型攻击面

随着5G网络架构向服务化、虚拟化演进，其通信协议接口日益趋于开放与标准化，尽管提升了互操作性和灵活性，却也扩大了潜在攻击面。特别是在跨域通信、异构网络接入等场景中，协议接口的暴露使得未经授权的数据探测、指令注入等风险显著增加。攻击者可以利用接口调用机制中的弱加密、弱鉴权等漏洞，通过构造恶意报文绕过认证流程，甚至获取系统控制权限。由于5G协议体系涉及多个层级和模块，传统的访问控制模型难以满足复杂场景下的细粒度权限管理需求，导致身份认证机制在高动态环境中难以持续保证实体可信性。这类基于协议层的攻击具备隐蔽性强、扩散快、危害深的特点，尤其在运营商核心网和行业专网中，其所引发的安全事件可能导致大规模服务中断和敏感信息泄露，严重威胁网络运行的稳定性与用户数据的安全性[2]。

1.2 多维虚拟化架构的安全漏洞

5G网络广泛采用网络功能虚拟化（NFV）与软件定义网络（SDN）架构以增强灵活性和资源调度效率，但其多层虚拟资源的抽象与重构也引入了新的协议层安全隐患[3]。在NFV环境中，虚拟网络功能（VNF）之间的协议通信路径往往缺乏明确的安全边界，攻击者一旦获取任一节点权限，极易实施横向协议劫持，窃取、篡改或重放网络信令数据。SDN控制层与转发层之间的南向接口若配置不当，也极易被利用进行控制命令篡改，诱导网络行为偏离预期路径，形成系统级的安全威胁。虚拟资源编排与调度过程中缺乏可信执行环境支撑，导致非法访问、权限漂移及虚拟机逃逸成为现实威胁。攻击者可通过操控调度协议接口获取高权限资源访问，从而绕开边界防护系统，实现对核心业务数据的渗透与操控。

1.3 网络切片与边缘计算中的协议隔离问题

5G网络切片和边缘计算（MEC）技术实现了业务定制化与时延优化，但其协议运行环境复杂，易形成隔离机制薄弱的“灰区”，成为跨片攻击与边缘节点入侵的重要突破口。在网络切片场景中，尽管理论上不同切片应具备严格的资源与协议隔离机制，然而实际部署中，为提高资源利用率，多个切片常共享底层硬件或中间件，导致攻击者可能借助同构协议栈的漏洞，在一处切片中注入恶意协议流，跨越虚拟边界攻击其他业务切片。MEC节点部署分散、能力异构，其安全验证机制多依赖集中式策略，一旦边缘节点安全认证流程存在缺陷，协议传输过程就极易被篡改、劫持甚至假冒源头信息进行伪装攻击，尤其在数据下沉、智能终端广泛接入的背景下，边缘协议在未经过完整链路审计与验证的情况下运行，其隐蔽性攻击更具破坏性。因此，必须针对切片与边缘协议架构设计更加精细的信任锚机制，强化边界校验与动态隔离能力。

1.4 应用层协议面临的复合威胁

5G网络引入了更多面向服务的开放API接口与敏捷开

作者简介：徐伟龙（1989.03-），男，汉族，籍贯：河南省新乡市，本科，工程师，研究方向：无线基站

发架构，尽管极大提升了应用生态的扩展性与灵活度，但也使得应用层协议暴露于多维度安全威胁之下。API滥用问题日益严峻，攻击者可以通过构造畸形请求、参数注入等方式调用敏感功能接口，绕过权限验证或进行信息探测，造成系统逻辑崩溃或业务数据泄露。身份伪造攻击愈发复杂，通过重放历史令牌或仿冒用户终端伪装合法访问主体，绕过认证流程，实现数据窃取或非法控制。在高速传输和低时延要求下，部分协议压缩安全审查流程，使数据传输过程中缺乏充分的加密与完整性校验，进一步加剧了协议被篡改、窃听或劫持的风险，特别是在边缘云、IoT设备广泛部署的背景下，协议攻击链条更加多样化、传染性更强。应对这类威胁需在协议设计之初引入“安全即默认”理念，辅以实时动态检测与零信任访问控制机制，方能实现应用层协议的全链路安全防护。

2 5G 通信协议现有防护机制评估

2.1 物理层与链路层的加密保护手段

5G通信协议在物理层主要通过信号扰码、频谱加扰和发射功率调制等方式[4]，提升对抗干扰与非法侦测的能力；终端与基站之间的数据链路普遍采用基于对称加密算法的加密传输技术，如128-NEA算法对用户数据进行加密，防止中间节点截取或篡改通信内容。在链路层，使用完整性保护机制（如128-NIA算法）以确保下行数据未被篡改，并结合链路标识符动态分配技术防止重放攻击和伪装行为。然而，这些保护手段多数依赖于预设密钥及物理设备的安全性，一旦密钥分发机制或设备认证流程遭到破坏，加密机制将形同虚设。因此，虽然物理与链路层的加密手段在防护通信基础安全方面起到一定作用，但其独立性与抗入侵能力仍有待提升。

2.2 网络层的认证与路由安全机制

网络层作为5G通信协议中的关键承载通道，其安全防护主要依赖身份认证机制与路由协议加固两方面[5]。当前，5G核心网采用基于公钥基础设施（PKI）的身份验证架构，通过设备唯一标识（如SUCI/SUPI）结合随机质询，实现双向认证流程，显著提升设备与网络之间的信任关系。引入访问管理功能（AMF）与安全功能（SEAF）的分离架构，增强了认证链的灵活性与扩展性。在路由层，部分部署了BGP-SEC、IPSec隧道与SDN控制平面加密等安全协议，防范路径操控、路由劫持及会话劫断等攻击行为。5G网络强调网络切片间路由隔离，以降低攻击扩散风险。然而，这些认证与路由安全机制普遍依赖中心化控制与静态策略配置，面对大规模移动设备接入、动态拓扑变换时，其响应速度与细粒度安全策略的部署能力仍显不足，难以支撑极端安全态势下的实时防护需求。

2.3 应用层的访问控制与数据完整性机制

5G应用层的通信协议保护机制主要围绕访问控制策略和数据完整性保障展开，主要有OAuth2.0、JWT等协议授权框架，能够实现对应用接口访问请求的分级授权、时间约束与作用域限制，从而避免未授权访问和功能滥用。数据在传输与存储过程中常结合使用AES、SHA-256等加密与哈希算法，确保数据未被非法篡改，支持服务端与客户端双向验证以增强完整性校验能力。部分系统还集成了Web应用防火墙（WAF）、API网关与行为分析模型，对高频访问、异常参数调用等操作实时拦截。然而，在物联网和边缘智能等典型5G场景中，由于终端异构性强、资源受限，导致安全控制策略部署能力受限，难以实现持续可信的访问管控，加之部分开发者在协议设计阶段未充分嵌入安全逻辑，导致应用层仍是攻击频发的高风险区域。

2.4 防护机制存在的技术局限与实施难点

尽管5G通信协议已集成多层次安全防护机制，但在实际应用中仍面临一系列技术局限与实施难点。首先，多协议协同背景下的安全策略分散，造成协议间上下层联动能力薄弱，难以在多域协商中实现快速响应与统一防控；其次，动态密钥更新、切片隔离等关键机制对基础设施依赖性高，增加了部署复杂性与运维负担，尤其是在边缘计算与大规模终端接入环境中，安全机制难以同步落地。此外，目前部分标准化协议仍未完全覆盖5G新兴业务场景，如工业控制、远程医疗等高可靠性需求领域，在安全建模与机制设计上存在明显滞后。同时，当前依赖静态策略与规则匹配的安全框架难以应对日益复杂的隐蔽攻击与零日漏洞，缺乏对异常行为的预测与联动响应能力。因此，如何实现跨层联防、弹性配置与智能感知，成为提升5G协议防护有效性的关键突破口。

3 5G 通信协议安全性改进方向

3.1 协议加密与动态密钥管理优化

量子密钥分发（QKD）机制基于量子态不可克隆与测量扰动原理，能够实现理论上不可窃听的密钥传输，极大增强了协议通信链路的抗窃听能力。与之配套的动态密钥更新机制亦需优化，从静态周期更新转向基于会话状态和风险等级的自适应密钥管理策略，实现密钥生命周期与通信行为动态耦合。部署端到端加密机制可确保通信数据即使在中继节点中被捕获亦无法解密，从而断绝链路监听的可行性。通过结合轻量级加密算法与分布式密钥管理框架，有望在保证计算资源高效利用的前

提下，构建一个高度弹性、可信度强的5G协议加密系统，全面提升通信链路在开放环境下的安全保障能力。

3.2 多因素认证机制与行为分析集成

通过集成生物识别（如指纹、人脸、虹膜）、位置验证、设备指纹识别等多种要素，构建出更为稳健的身份验证框架，可有效降低身份仿冒与会话劫持风险。结合协议行为建模与异常模式识别算法，建立基于用户行为偏移程度的动态风险评估体系，使认证策略具备场景适应性和风险响应能力。当系统检测到通信行为与历史模型显著偏离时，即可自动触发二次验证或限制访问权限，从而实现“最小信任”原则下的安全接入管理。

3.3 协议级切片安全策略设计

随着5G网络切片技术的广泛应用，基于协议层的细粒度安全隔离策略成为切实保障多业务并存环境中通信安全的关键。在切片内部，需通过协议栈虚拟化隔离与访问路径映射绑定机制，防止不同业务协议实体在同一物理资源上产生跨权访问，实现真正的协议空间隔离。对于跨切片交互场景，引入可信认证机制与链路审计功能，确保信令消息在多个切片之间传递过程中的完整性、身份合法性及链路溯源能力。通过构建切片间通信的信任根与密钥交换链，可有效防范伪造信令注入与非授权访问行为。动态权限管控机制应结合协议级角色授权与资源访问控制策略，实现按需授权与实时收回，提升安全策略对业务变化的响应力。

3.4 基于AI的协议入侵检测与响应系统

面向复杂多变的5G通信协议环境，传统基于规则的入侵检测系统（IDS）在识别新型或变异攻击方面存在明显滞后，亟需构建融合人工智能算法的智能入侵检测与响应系统。基于AI的协议入侵检测与响应系统基于深度学习或图神经网络技术，对协议流量进行语义级建模与行为特征提取，实现对加密流、非标准协议操作等异常行为的智能识别与高效分类。借助历史攻击样本与正常通信模式的对比分析，系统可自主学习潜在威胁特征并动态更新检测模型，有效提升未知攻击识别率。结合自动化响应机制，基于检测结果实时生成防护策略，如阻断恶意通信链路、调整访问权限、联动警报系统等，形成自适应闭环防护能力。

4 结语

综上，本文聚焦于5G网络通信协议在开放架构和高度虚拟化环境下的安全性挑战，系统梳理了协议层面主要的安全隐患及其机制不足。在此基础上，提出了从加密体系、身份认证、协议隔离到AI驱动检测响应的多维改进策略，旨在构建更为弹性、智能和可信的协议安全框架。研究成果为5G网络安全体系的构建与演进提供了理论依据和实践路径，也为未来面向6G通信环境的安全设计奠定基础。

参考文献

[1]梁能.面向5G需求响应的网络通信安全问题研究[J].电子元器件与信息技术,2023,7(3):208-210,214.

[2]梁爽,董丽红.5G网络安全:威胁、机制与实现[J].电脑知识与技术,2025,21(12):64-66.

[3]岳博石.5G新技术驱动下的网络安全痛点分析及需求和策略研究[J].网络安全技术与应用,2022(10):74-75.

[4]陆南昌,蔡厚恩,赖宇.基于5G无线通信技术的无线网络安全通信防御技术研究[J].通讯世界,2024,31(8):37-39.

[5]孙宁,吴信强,孙霈翀,等.基于5G承载网的IPRAN组网、优化与安全探讨[J].中国宽带,2024,20(4):13-15.