面向 5G 网络的信息安全威胁与防御机制研究

包新军

中国铁塔股份有限公司丽水市分公司　浙江　丽水　323000

摘　要：本文系统梳理了 5G 网络相较于 4G 在架构上的关键变革，并在此基础上深入剖析了 5G 网络面临的主要信息安全威胁，包括来自网络切片、虚拟化与云原生环境、服务化架构（SBA）、终端设备以及供应链等多个维度的风险。针对这些威胁，本文进一步探讨了当前主流的防御机制，如零信任安全模型、基于人工智能的威胁检测、端到端加密与隐私增强技术、以及安全编排与自动化响应（SOAR）等。最后，文章对 5G 安全的未来发展趋势进行了展望，并提出了构建纵深防御体系、强化标准与法规协同、以及推动安全内生设计等综合性建议，以期为 5G 网络的安全、稳定、可靠运行提供理论参考与实践指导。

关键词：5G 网络；信息安全；网络切片；服务化架构；零信任

引言

在数字化浪潮汹涌澎湃的当下，物联网、工业互联网等新兴应用蓬勃发展。这些新兴应用对数据传输的带宽、时延以及连接密度提出了前所未有的高要求，使得 4G 技术在应对时逐渐力不从心，其局限性日益凸显。在此背景下，5G 应运而生，它以追求极致通信性能为目标，峰值速率高达 20 Gbps，端到端时延低至 1 毫秒，每平方公里更是能支持百万级设备连接。不仅如此，5G 还致力于构建通用、灵活且智能的网络平台，为千行百业的数字化转型提供强大动力。然而，5G 网络技术的革新犹如一把双刃剑。其核心网演进为开放式服务化架构，虽极大提升了网络的敏捷性与可扩展性，但也导致攻击面从物理边界扩展至逻辑层面，传统安全范式已难以适应。同时，5G 所支撑的关键业务场景，如智能交通、远程医疗等，对网络可靠性与安全性要求近乎苛刻，一旦发生安全事件，极有可能造成灾难性后果。因此，深入剖析 5G 信息安全威胁，构建主动、智能的防御机制，已成为保障国家数字经济稳健发展、维护社会稳定和公共安全的当务之急。

1 5G 网络架构及其安全特性

1.1 服务化架构（SBA）

5G 核心网（5GC）采用服务化架构（SBA），摒弃 4G 僵化的点对点接口。在 SBA 中，接入和移动性管理功能（AMF）等网络功能（NFs）被设计为独立、可重用的微服务，通过统一服务通信总线（如基于 HTTP/2 的 RESTful API）交互，由网络存储功能（NRF）负责服务注册、发现与授权。但 SBA 的开放性和灵活性带来巨大安全挑战：大量标准化 API 接口若认证、授权和输入验证机制不健全，易遭 API 滥用、注入或拒绝服务（DoS）攻击；微服务间动态调用关系使攻击路径复杂难追踪，传统防火墙和入侵检测系统（IDS）难以有效监控东西向流量。

1.2 网络切片

网络切片是 5G 实现“一网多能”的关键技术。它允许在同一套物理基础设施上，通过逻辑隔离的方式，创建多个端到端的、具有不同性能和服务等级协议（SLA）的虚拟网络。例如，可以为 eMBB（增强移动宽带）业务、uRLLC（超高可靠低时延通信）业务和 mMTC（海量机器类通信）业务分别创建独立的切片[1]。安全影响为：网络切片在带来资源高效利用的同时，也引入了切片间的安全隔离风险。如果隔离机制存在漏洞，攻击者可能通过一个安全性较弱的切片（如用于普通 IoT 设备的切片）作为跳板，横向渗透到承载关键业务（如电力控制）的高安全切片中，造成“跨切片攻击”。此外，切片的生命周期管理（创建、修改、删除）过程本身也可能成为攻击目标。

1.3 虚拟化与云原生

5G 核心网全面拥抱云计算技术，采用 NFV 将网络功能从专用硬件中解耦，并部署在通用的云基础设施上。同时，容器化（如 Docker）和编排系统（如 Kubernetes）等云原生技术被广泛应用于微服务的部署与管理。安全影响为：这导致了安全边界的模糊化。攻击面从单一的网络设备扩展到了整个云平台，包括虚拟机（VM）、容器、宿主机操作系统、Hypervisor/容器运行时以及底层硬

件。任何一个环节的漏洞都可能导致整个网络功能的瘫痪或数据泄露。特别是容器共享宿主机内核的特性，使得容器逃逸（Container Escape）成为一种高危威胁。

1.4 分布式用户面与边缘计算（MEC）

为了满足 uRLLC 等场景对超低时延的需求，5G 将用户面功能（UPF）下沉到网络边缘，靠近数据源和终端用户。这催生了多接入边缘计算（Multi-access Edge Computing, MEC）的发展，使得计算、存储和网络能力可以在网络边缘就近提供。安全影响为：边缘节点通常部署在物理安全防护较弱的环境中（如基站机房），更容易遭受物理篡改或侧信道攻击。同时，海量的边缘设备和应用增加了安全管理的复杂性，如何确保边缘应用的可信性和数据在边缘处理过程中的安全性，成为新的难题。

2 5G 网络面临的主要信息安全威胁

2.1 针对服务化架构（SBA）的威胁

（1）API 安全威胁：这是 SBA 面临的最直接威胁。攻击者可以利用未授权的 API 调用窃取用户位置、订阅信息等敏感数据；通过发送畸形请求或大量合法请求，对 NFs 发起 DoS/DDoS 攻击，耗尽其计算或网络资源。（2）服务发现与注册劫持：如果 NRF 的安全机制不足，攻击者可能伪造恶意 NF 向 NRF 注册，诱使其他合法 NF 与其通信，从而实施中间人（MitM）攻击或数据窃听。（3）信令风暴：利用 5G 信令流程的复杂性，攻击者可以发起大量虚假的注册、切换或会话建立请求，淹没核心网信令面，导致网络拥塞甚至瘫痪。

2.2 针对网络切片的威胁

（1）跨切片攻击：如前所述，这是网络切片安全的核心问题。攻击者一旦突破一个切片的防线，便可能利用共享的物理资源或管理平面漏洞，对其他切片发起攻击。（2）切片资源耗尽：攻击者可以针对某个特定切片发起资源消耗型攻击，使其无法为合法用户提供服务，破坏其 SLA 承诺[2]。（3）切片配置错误：由于切片的创建和管理高度依赖自动化，配置脚本或模板中的微小错误都可能导致严重的安全策略失效，例如错误地开放了不应公开的网络端口。

2.3 针对虚拟化与云原生环境的威胁

（1）虚拟机/容器逃逸：攻击者利用虚拟化层（Hypervisor）或容器运行时（如 runc）的漏洞，从被攻陷的虚拟机或容器中逃逸到宿主机，进而控制整个物理服务器，威胁其上运行的所有网络功能。（2）镜像供应链污染：微服务通常以容器镜像的形式分发。如果镜像仓库或 CI/CD 流水线被攻破，恶意代码可能被植入到官方镜像中，一旦部署，将形成大规模的后门。（3）云平台内部威胁：拥有云平台高级权限的内部人员或被其凭证的外部攻击者，可以任意查看、修改或删除网络功能实例，造成巨大破坏。

2.4 终端与接入安全威胁

（1）伪基站（IMSI Catcher）升级：5G 虽然增强了对用户身份（SUPI）的保护（通过 SUCI 加密），但攻击者仍可能利用降级攻击，诱使 5G 终端回落到不安全的 2G/3G/4G 网络，从而实施 IMSI 捕获和位置跟踪。（2）海量 IoT 设备的安全隐患：5G 连接的数十亿 IoT 设备，很多计算能力和安全防护能力极其有限，极易被僵尸网络（Botnet）控制，用作发起 DDoS 攻击的源头。（3）SIM 卡相关攻击：针对 eSIM（嵌入式 SIM）的远程配置管理接口，可能存在被滥用的风险，导致用户身份被非法克隆或服务被恶意取消。

2.5 供应链与后量子安全威胁

（1）供应链攻击：5G 网络设备和软件来自全球众多供应商，任何一个环节被植入后门或存在未披露的漏洞，都将对整个网络构成系统性风险。（2）后量子密码学（PQC）威胁：当前 5G 使用的公钥密码算法（如 RSA, ECC）在未来量子计算机面前将不堪一击。虽然短期内量子计算尚不成熟，但“先存储，后解密”（Harvest Now, Decrypt Later）的攻击模式意味着今天传输的加密数据，未来可能被解密。因此，向抗量子密码算法的迁移已成为一项紧迫的长期任务。

3 5G 网络安全防御机制

3.1 零信任安全架构（Zero Trust Architecture, ZTA）

零信任模型的核心思想是“永不信任，始终验证”。它摒弃了传统的“城堡与护城河”式的边界安全模型，假设网络内外都充满威胁。在 5G SBA 中，ZTA 要求对每一次服务调用都进行严格的身份认证、设备健康度检查和细粒度的访问授权。实现方式是：通过引入安全策略决策点（PDP）和策略执行点（PEP），结合身份提供商（IdP）和设备状态评估服务，对每个 API 请求进行实时的风险评估和授权决策。微隔离（Microsegmentation）技术可用于限制微服务之间的通信，即使某个服务被攻陷，也能有效遏制攻击的横向移动。

3.2 基于人工智能（AI）与机器学习（ML）的威胁检测

5G 网络产生的海量日志和流量数据，为人工作业分析带来了巨大挑战，却为 AI/ML 提供了绝佳的应用

场景。（1）异常检测：通过无监督学习算法（如聚类、孤立森林）建立网络正常行为的基线模型，能够自动识别出偏离基线的异常流量或信令模式，从而发现未知的0day 攻击或内部威胁。（2）恶意软件与入侵检测：利用深度学习模型（如 CNN, RNN）分析网络流量载荷或系统调用序列，可以高精度地识别恶意软件通信或入侵行为[3]。（3）自动化响应：AI 不仅可以用于检测，还可以与 SOAR 平台集成，根据预设的剧本（Playbook）自动执行隔离受感染主机、阻断恶意 IP、调整防火墙规则等响应动作，大大缩短响应时间（MTTR）。

3.3 端到端加密与隐私增强技术

保护用户数据的机密性和完整性是 5G 安全的基石。（1）增强的用户身份保护：5G 已采用公钥加密来保护永久用户标识（SUPI），生成临时的 SUCI，有效防止了 IMSI 捕获。（2）同态加密与安全多方计算：对于在 MEC 边缘处理的敏感数据，可以采用隐私计算技术。同态加密允许在密文上直接进行计算，结果解密后与明文计算一致；安全多方计算允许多方在不泄露各自私有数据的前提下，共同完成一个计算任务。这些技术能在保证数据可用性的同时，最大限度地保护用户隐私。（3）后量子密码迁移：标准化组织（如 NIST）正在积极推进 PQC 算法的标准化工作。5G 网络需要提前规划，设计支持密码算法敏捷替换的架构，以便在未来平滑过渡到抗量子安全时代。

3.4 安全编排、自动化与响应（SOAR）

SOAR 平台通过整合安全信息与事件管理（SIEM）、威胁情报（TI）和自动化工作流，为 5G 安全运营中心（SOC）提供强大的支撑。（1）集中化态势感知：SOAR 能够聚合来自 5G 核心网、无线接入网、MEC 节点、云平台等各个层面的安全日志和告警，提供全局的、可视化的安全态势图[4]。（2）自动化工作流：将安全专家的经验固化为可执行的剧本，实现从威胁发现、分析、调查到响应的全流程自动化，极大提升安全运营效率，缓解人才短缺的压力。

3.5 可信计算与硬件根信任

从硬件层面构建信任链，是抵御底层攻击的根本之道。（1）可信平台模块（TPM）/可信执行环境（TEE）：在服务器和边缘设备中集成 TPM 芯片，或利用 CPU 提供的 TEE（如 Intel SGX, ARM TrustZone）技术，可以为关键的网络功能（如密钥管理、认证服务）提供一个隔离的、防篡改的执行环境，确保其代码和数据的完整性。

4 结语

5G 网络作为数字经济底座，其安全性关乎国计民生。本文系统剖析了 5G 因架构革新产生的新型安全威胁，探讨了以零信任等为核心的综合防御机制，指出 5G 安全是复杂系统工程，无法单靠单一技术或产品解决。展望未来，5G 安全将呈现内生安全、AI 与安全深度融合、跨域协同防御等趋势。为此，建议构建纵深防御体系，结合多层次防护形成协同联动格局；强化标准与法规协同，完善技术标准与法律法规，明确各方责任；加强国际合作与人才培养，应对全球性挑战并培育复合型人才。只有多管齐下，才能充分释放 5G 潜能，构建安全、可信、繁荣的数字未来。

参考文献

[1] 崔世杰, 王云龙.5G 网络环境下通信工程数字化信息安全防护策略研究 [C]//江西省工程师联合会. 工程技术与新能源经济学术研讨会论文集. 中捷通信有限公司; 周口市文化馆;,2025:45-48.

[2] 周春梅.5G 通信时代计算机网络信息安全问题浅析 [J]. 网络安全和信息化,2024,(09):142-144.

[3] 张曾油.5G 时代网络信息安全问题与展望探析 [J]. 电子元器件与信息技术,2023,7(01):233-235+240.

[4] 裴宜春.5G 时代网络信息安全问题及对策研究 [J]. 无线互联科技,2022,19(05):9-10.