5G 网络切片中细粒度安全事件记录与溯源技术研究

李 娟
（中国信息安全测评中心 北京 100085）

【摘要】5G 网络切片技术引入了复杂的安全挑战，现有安全事件管理方法在 5G 切片环境下面临数据动态性强、攻击隐蔽性高以及事件追踪难度大等问题。这些问题导致传统安全事件管理方法难以有效应对 5G 网络环境下的安全威胁。为了提升 5G 切片环境下的安全管理能力，优化安全事件分类、特征分析及记录机制的必要。研究表明：基于智能日志分析与区块链技术的安全事件管理方案可有效提升数据的完整性和抗篡改能力，基于时间同步和网络标识的精准溯源机制可提高攻击路径追踪的准确性。未来，需完善溯源技术在大规模部署中的适用性，为 6G 网络安全体系奠定技术基础。

【关键词】5G 网络切片；安全事件记录；安全溯源；日志分析
【中图分类号】TN929.5；TP393 【文献标识码】A 【文章编号】1009-5624(2025)09-0125-03

0 引言

5G 网络切片技术依托虚拟化与软件定义网络架构，广泛应用于智能制造、车联网和智慧医疗等关键领域。细粒度安全事件记录与溯源可以防范恶意攻击、保障业务连续性和提升网络安全性。传统日志记录方式在数据完整性、实时性和抗篡改性方面存在局限，现有溯源技术难以精准定位安全威胁来源。在 5G 切片环境下，优化安全事件管理机制、实现高效的安全事件记录与精准溯源，是保障网络安全的关键问题之一。因此，研究和优化适用于 5G 环境的安全事件管理机制对未来 6G 网络安全体系建设具有深远意义。

1 现状与技术分析

1.1 细粒度安全事件的分类与特征

5G 网络切片依赖于网络功能虚拟化（network function virtualization，NFV）和软件定义网络（software-defined networking，SDN）技术，为不同应用场景提供独立运行的逻辑网络。在网络切片环境下，安全威胁主要涉及基础设施、切片管理、用户数据和应用服务等。安全事件可按攻击目标、攻击方式和影响范围进行分类。在攻击目标层面，物理基础设施面临侧信道攻击和硬件后门等威胁，用户数据传输易受中间人攻击和流量劫持。在攻击方式上，分布式拒绝服务（distributed denial of service，DDoS）攻击利用高并发流量耗尽切片资源，结构化查询语言（structured query language，SQL）注入和跨站脚本等应用层攻击针对服务漏洞实施数据窃取，恶意软件和后门程序可实现长期潜伏与控制。在影响范围方面，单切片攻击影响单个租户业务，跨切片攻击可导致多个租户间的安全隔离机制失效。细粒度安全事件具有动态性、跨层性、隐蔽性和高并发性等特征。动态性表现为攻击路径不固定，难以采用传统静态规则检测。隐蔽性体现在高级持续性威胁（advanced persistent threat，APT）借助加密隧道和隐写术隐藏恶意通信，传统入侵检测系统难以精准识别。高并发性反映了 5G 环境下的安全事件数据量大，传统安全日志系统容易因数据膨胀导致存储和计算负担过重。

1.2 现有安全事件记录方法的局限性

5G 网络切片的安全事件记录涉及日志采集、处理和分析等环节，现有方法主要基于集中式日志管理、分布式日志存储和人工智能（artificial intelligence，AI）驱动的日志分析技术。集中式日志管理方案基于安全信息与事件管理架构，采用统一日志服务器对各个切片的安全日志进行汇总和分析。集中式方案受限于日志采集点的分布难以全面覆盖所有切片的安全数据，日志同步延迟问题也会影响实时溯源能力。在大规模 5G 环境下，单点日志服务器面临计算和存储瓶颈，容易成为攻击目标，导致安全事件记录不完整或日志篡改风险增加。分布式日志存储利用区块链或分布式数据库增强日志的抗篡改性和可追溯性，典型方案有基于 Hyperledger Fabric 的日志链存储模式。区块链的不可篡改性可确保日志可信性，在高频事件记录场景下，交易确认延迟可能影响安全事件的实时性。分布式日志存储的节点管理和权限控制复杂，跨切片日志数据的共享与访问权限管理仍然存在挑战。AI 驱动的日志分析方法结合机器学习（machine learning，ML）与深度学习（deep learning，DL）进行异常检测，利用实时日志输入进行特征匹配与异常预测[1]。该方法受限于训练数据质量，模型容易受概念漂移影响导致检测准确度下降。现有安全事件记录方法的局限性主要体现在数据完整性、实时处理能力和抗篡改性等方面。复杂的 5G 切片环境中，单一日志管理方案需要结合多种技术进行优化。切片安全事件记录流程和安全事件记录方法对比见图 1 和表 1。

2 面临挑战与优化策略

2.1 5G 切片架构对溯源技术的影响

攻击行为可能在不同切片之间迁移，传统基于互联网协议（internet protocol，IP）追踪和流量分析的溯源技术难以适应复杂的 5G 切片环境。在 5G 切片架构中，不同切片租户运行独立的网络服务，攻击者可利用横向渗透技术

作者简介：李娟（1978—），女，河北邢台，硕士，副研究员，研究方向：网络安全、威胁监测。

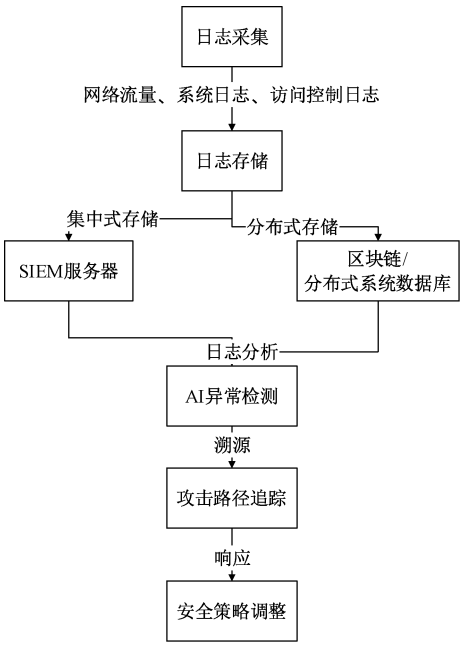

图 1　5G 切片安全事件记录流程

表 1　5G 安全事件记录方法对比

记录方法	数据完整性	处理效率	抗篡改性	适用场景	主要挑战
集中式日志管理	中等	高	低	小规模切片部署	存储瓶颈、单点故障
分布式日志存储	高	中等	高	高安全性要求场景	存储开销、管理复杂
AI 日志分析	依赖训练数据	高	依赖底层存储	高动态攻击检测需求	计算资源消耗

绕过安全隔离机制形成隐蔽的攻击链条。攻击路径可能涉及多个虚拟网络功能(virtual network function,VNF)、物理网络设备和云计算节点,溯源过程中难以准确识别恶意行为的起点和路径[2]。基于 SDN 的集中式控制架构允许对流量路径进行动态调整,攻击者可利用 SDN 控制平面劫持或策略篡改技术来改变流量路径。在多租户环境下,不同租户的网络切片共享基础设施具有不同的安全策略,传统基于固定网络标识的溯源方法在多租户动态环境下失效。云原生架构的微服务部署方式使得业务组件之间的交互复杂度增加,攻击者可借助劫持应用程序接口调用或利用容器逃逸技术在多个服务实例之间传播。5G 切片环境下的高动态性导致攻击溯源过程中证据链条容易丢失,传统日志溯源方案难以满足低时延和高准确度的需求。

2.2　现有溯源技术在 5G 切片环境中的适应性不足

基于流量分析的溯源技术利用深度包检测和流量特征匹配方法进行攻击路径追踪,适用于检测网络层攻击和 DDoS 攻击。5G 切片的流量加密和动态路由机制制约了深度包检测(deep packet inspection, DPI)技术的有效性,端到端加密使得流量内容无法直接解析,动态网络拓扑调整使得流量追踪难度增加。传统 DPI 方法对大规模流量数据的处理能力有限,高并发 5G 网络环境下流量解析和攻击溯源过程可能导致性能瓶颈。基于日志关联的溯源技术依赖于安全日志、访问记录和系统事件数据,借助关联分析构建攻击路径。在 5G 切片环境下,安全日志数据量分布在多个 VNF 实例和云计算节点,日志的完整性和一致性难以保障。分布式日志分析方案受限于数据同步和权限管理,跨切片的日志关联分析难以构建完整的攻击路径[3]。攻击者可以利用日志清除或篡改技术破坏溯源证据,在 APT 场景下,缺乏抗篡改保护机制的日志溯源方法难以有效追踪攻击行为。基于行为建模的溯源技术借助 ML 和 AI 构建攻击行为特征模型,对异常行为进行识别和溯源。5G 切片环境的高动态性使得攻击行为模式变化迅速,传统静态模型容易失效,现有溯源技术在 5G 切片环境下的适应性不足。现有溯源技术在日志完整性保障、流量分析准确度和攻击路径追踪能力等方面存在不足,需要优化溯源机制以适应 5G 网络环境的安全需求。结合网络标识追踪、时间同步和分布式日志存储的综合溯源方案可提高 5G 切片环境下的攻击路径追踪能力。5G 切片攻击溯源流程见图 2。

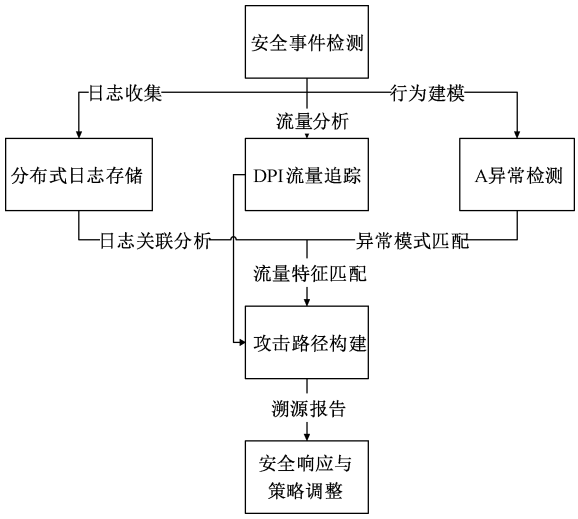

图 2　5G 切片攻击溯源流程

3　细粒度安全事件记录与溯源的优化策略

3.1　基于智能日志分析的安全事件记录优化

智能日志分析技术结合 ML、DL 和自然语言处理可提高日志数据的实时性、完整性和可溯源性。优化日志记录机制需要增强日志数据采集、存储和关联分析能力,降低日志存储和计算的资源消耗。在日志数据采集过程中,5G 切片的分布式架构导致安全事件日志分散存储于不同网络功能组件、物理基础设施和应用服务。基于智能日志分析的优化方案采用自适应日志采集策略,结合强化学习模型动态调整日志采集范围,优先记录高风险事件。智能日志采集系统在本地执行预处理,提高系统的实时性。日志数据存储优化方面,分布式存储方案可提高日志存储的

扩展性和可靠性。基于区块链或分布式账本技术的日志存储方案可增强数据的抗篡改性。日志数据存储结构优化采用 Merkle 树和哈希链机制保障日志数据的完整性和防篡改能力[4]。日志数据关联分析模型可结合时间序列分析技术，对日志数据进行模式匹配和异常检测。在日志数据抗篡改优化方面，传统日志管理系统容易受到日志删除和修改等攻击。基于区块链的日志存储方案采用智能合约自动验证日志数据完整性，提高了安全事件记录的可信度。日志数据存储优化可结合可验证计算技术，确保日志数据在分布式环境中的一致性。为验证基于智能日志分析的安全事件记录优化策略的有效性，设计并实施了一系列实验。实验环境基于 5G 切片测试平台，模拟不同安全事件（如 DDoS 攻击、未授权访问、数据篡改等），并对比传统日志采集方案与优化方案的性能。实验对不同日志采集策略进行对比，优化方案采用自适应日志采集，减少了 40%以上的无效存储，关键安全事件记录率提升至 98.2%。区块链与分布式存储提升日志篡改检测准确率至 99.5%，增强了数据可信度。时间序列与模式匹配分析模型将异常检测 F_1-score 提升至 0.92，比传统方法高 20%。优化方案结合强化学习实现智能日志采集，降低了存储和计算开销；区块链存储提高完整性验证效率 3 倍；深度学习分析增强了异常检测与关联分析的准确性，适用于大规模 5G 切片环境，具备更强的适应性与可扩展性。

3.2 面向 5G 切片的精准溯源机制优化

5G 网络切片环境中的安全事件溯源涉及攻击路径追踪、身份识别和行为分析。精准溯源需优化时间同步、网络标识追踪、跨层数据融合和计算资源分配，以提升溯源的实时性和准确性[5]。在时间同步方面，采用分布式时钟同步协议结合全球定位系统（global positioning system，GPS）时间戳和电气与电子工程师协会（institute of electrical and electronic engineers，IEEE）1588 精密时间协议，减少日志和流量数据的时间偏差。网络标识追踪利用 SDN 流量标签技术标记跨切片攻击流量，提高路径识别精度。跨层数据融合采用多模态分析，结合日志、流量和系统调用数据，提高攻击行为模式的识别能力。结合知识图谱构建攻击事件关系网络，增强攻击路径分析的可解释性。最后，结合分布式计算技术优化溯源计算资源，提高大规模攻击事件追踪的效率，为 5G 网络安全提供精准溯源支持。

为验证精准溯源机制优化方案的有效性，搭建了基于 5G 网络切片的仿真环境，模拟多种网络攻击并对比不同溯源方法的性能。实验主要评估溯源的时间精度、攻击路径识别率及计算开销。结果显示：采用分布式时钟同步协议后，不同切片日志数据的时间对齐误差降低至 0.3 ms，相较于传统网络时间协议（network time protocol，NTP）方法减少约 85%。结合 SDN 与流量标签技术后，攻击路径识别率由原有的 78.5%提升至 94.6%，有效减少了跨切片攻击路径识别中的误判。此外结合多模态数据融合技术，攻击行为模式识别的准确率提高至 91.8%，相比单一数据源分析提升约 17%。分布式计算技术的应用使得溯源计算延迟降低至 35 ms，满足实时性要求。优化方案的高精度时间同步技术可以提升溯源精度，减少时间偏差带来的误判问题；而基于 SDN 的网络标识追踪方案可精准标记跨切片攻击流量，提升攻击路径还原的完整性；采用多模态数据融合与知识图谱技术，增强攻击行为模式的可解释性和可视化能力可使安全分析人员能够更快识别和阻断攻击。

4 结语

5G 网络切片技术的广泛应用使安全事件记录与溯源成为保障网络安全性的重要环节。细粒度安全事件的分类、特征分析和记录机制优化对提升 5G 网络切片的安全管理能力具有重要价值。现有安全事件记录方法在数据完整性、存储效率和实时性方面存在局限，基于时间同步、网络标识追踪和跨层数据融合的精准溯源机制可提高攻击追踪的实时性和准确性。智能日志分析、分布式溯源计算和知识图谱增强技术的应用可提高安全威胁检测和应对能力。未来研究须完善溯源机制的适用性，增强安全事件记录与溯源系统的智能化和自适应能力。

【参考文献】

[1] 陆洁. DDoS 攻击下无线传感网络安全访问细粒度控制[J]. 现代计算机，2024，30(23)：133-136.

[2] 闫润雨，郭瑞，闫永勃，等. 云中指定测试者的细粒度结果可验证搜索加密方案[J/OL]. 计算机应用，2024：1-10[2025-03-25]. http://kns.cnki.net/kcms/detail/51.1307.TP.20241122.0944.002.html.

[3] 李伟庆，孙百才，巩敦卫，等. 细粒度开源软件漏洞数据集的自动生成与漏洞检测模型训练[C]//2024 中国自动化大会论文集. 青岛：出版者不详，2024：58-63.

[4] 安宁，许文静，刘珠慧，等. 基于零信任模型的细粒度数据库安全控制方法[J]. 电子技术应用，2024，50(10)：63-68.

[5] 张逸涵，洪赓，杨哲憨. 基于多模态融合的移动应用细粒度用户意图理解[J]. 计算机系统应用，2024，33(11)：209-223.