面向 5G/6G 云网融合架构的安全威胁建模与主动防御机制研究

王峰

山东商业职业技术学院，山东济南，250103；

摘要：随着 5G/6G 与云计算深度融合，云网融合架构成为支撑未来数字社会的关键基础设施，但其开放性、虚拟化和高度动态的特性也带来了前所未有的安全挑战。本文针对 5G/6G 云网融合环境中的安全威胁进行系统建模，识别关键攻击面，包括网络切片劫持、边缘计算节点入侵、信令风暴及跨域数据泄露等典型风险。在此基础上，提出一种基于零信任架构与人工智能驱动的主动防御机制，融合动态访问控制、异常流量检测、智能威胁狩猎与自适应响应策略。通过构建数字孪生仿真平台对所提模型进行验证，实验结果表明，该机制可显著提升威胁检测准确率（达 96.2%）并缩短响应时间至秒级，有效增强云网融合系统的韧性与安全性。本研究为构建内生安全、智能协同的下一代通信网络防御体系提供了理论支撑与实践路径。

关键词：5G/6G；云网融合；安全威胁建模；主动防御；零信任架构

DOI：10.69979/3041-0673.26.03.021

1 引言

1.1 研究背景

随着 5G 和 6G 网络技术的发展，云计算与网络技术的深度融合已成为必然趋势。5G 网络以其高速率、低时延、大连接的特点，为物联网、智能交通、工业互联网等领域带来了革命性的变化。而 6G 网络则将进一步推动网络技术的进步，实现更高速率、更低时延、更广泛的连接。在 5G 和 6G 网络的发展过程中，云网融合架构的应用将愈发广泛，成为支撑未来网络发展的关键技术。

1.2 研究意义

本研究的意义在于，通过对 5G 和 6G 云网融合架构的安全威胁建模与主动防御机制进行研究，为我国 5G 和 6G 网络安全提供理论支撑和实践指导。首先，本研究将有助于提高 5G 和 6G 网络的安全性，降低网络攻击的风险。其次，本研究将有助于提升云网融合架构的安全性，为我国网络基础设施提供安全保障。最后，本研究将为主动防御机制的研究和改进提供有益的借鉴和启示。

1.3 研究内容和方法

本研究的主要内容包括：分析 5G 和 6G 云网融合架构的安全威胁，构建安全威胁模型；研究主动防御机制的理论和方法，设计适用于 5G 和 6G 云网融合架构的主动防御策略；通过实验验证安全威胁模型和主动防御机制的有效性。

2 5G 和 6G 云网融合架构概述

2.1 5G 网络技术

5G 网络作为第五代移动通信技术，具备高速率（峰值可达 10 Gbps 以上）、超低时延（端到端时延可低至 1 毫秒）以及海量设备连接能力（每平方公里支持百万级终端接入）三大核心特性。这些优势使其成为支撑未来智能社会的关键基础设施，将深度赋能物联网、智能交通、远程医疗、工业互联网、虚拟现实等新兴应用场景。为实现上述性能指标，5G 采用了多项关键技术：大规模 MIMO（Multiple-Input Multiple-Output）通过部署数十甚至上百根天线显著提升频谱效率；毫米波通信利用高频段频谱资源拓展带宽；网络切片技术则根据业务需求动态划分逻辑网络，实现“一网多用”；而边缘计算将计算与存储能力下沉至网络边缘，有效降低传输时延并提升本地化服务能力。

2.2 6G 网络技术

6G 网络作为 5G 的演进与超越，预计将在 2030 年前后商用，目标是构建“空天地海一体化”的全域智能通信网络。其性能将进一步跃升：理论峰值速率可达 1 Tbps，时延压缩至微秒级，并支持泛在智能连接与感知融合。6G 不仅追求通信能力的极致提升，更强调与人工智能、感知、计算的深度融合。关键技术包括：太赫兹

通信（0.1 - 10 THz 频段），提供超大带宽；量子通信，保障未来高安全通信需求；深度网络虚拟化与服务化架构，实现资源按需编排；以及内生 AI 能力，使网络具备自学习、自优化和自决策功能，真正迈向“智慧内生、安全内生、绿色内生”的新一代通信体系。

2.3 云网融合架构

云网融合架构是指将云计算资源与通信网络能力深度协同、统一调度的一体化基础设施架构，旨在打破传统“云”与“网”分离的壁垒，实现计算、存储、网络资源的全局优化。该架构具备资源弹性伸缩、服务灵活编排、安全可信可控等显著优势，能够高效支撑数据中心互联、混合云部署、边缘智能及算力网络等复杂场景。在 5G/6G 时代，云网融合进一步演化为“算网融合”，强调算力与网络的联合调度，为用户提供“一点接入、即取即用”的泛在算力服务，成为数字经济发展的重要底座。

3 5G 和 6G 云网融合架构的安全威胁分析

3.1 5G 网络的安全威胁

5G 网络在带来高速率、低时延和广连接优势的同时，也引入了新的安全风险。主要威胁集中在网络切片、边缘计算和终端设备三大层面。由于网络切片采用共享物理基础设施构建多个逻辑隔离的虚拟网络，若隔离机制设计不充分，可能导致跨切片信息泄露或资源干扰；边缘计算节点部署在靠近用户侧的开放环境中，其计算与存储资源有限，易成为攻击跳板，面临数据篡改、服务中断等风险；此外，海量异构终端（如 IoT 设备）普遍存在安全防护能力薄弱、固件更新滞后等问题，极易被利用发起分布式拒绝服务（DDoS）攻击或作为僵尸网络节点。这些漏洞共同构成了 5G 时代复杂且动态的安全挑战。

3.2 6G 网络的安全威胁

面向 2030 年的 6G 网络将融合太赫兹通信、量子技术、人工智能与深度虚拟化，其安全威胁更具前瞻性和复杂性。太赫兹频段虽带宽极大，但传播距离短、易受干扰，可能引发频谱资源恶意抢占或信号窃听；量子通信虽理论上具备无条件安全性，但在实际部署中仍面临量子密钥分发（QKD）设备被物理攻击或侧信道破解的风险；而高度依赖软件定义与网络功能虚拟化的 6G 架构，若缺乏细粒度的权限管理和资源审计机制，极易导致虚拟化资源被滥用、租户间隔离失效，甚至引发大规模服务瘫痪。此外，AI 内生于网络也可能被对抗样本攻击所利用，造成智能决策失准。

3.3 云网融合架构的安全威胁

云网融合架构通过打通云与网的边界，提升了资源调度效率，但也扩大了攻击面。其安全威胁主要体现在云资源、网络通道和数据资产三个维度：云资源访问控制策略若配置不当或身份认证机制薄弱，可能导致未授权访问或权限提升；网络层面因多租户共享底层设施，若安全隔离（如 VXLAN、微隔离）不彻底，易发生横向渗透；在数据层面，跨云、跨域的数据流动频繁，若缺乏端到端加密、数据脱敏和生命周期管理，将面临泄露、篡改或合规风险。因此，构建统一身份治理、动态零信任防护和智能数据安全体系，是保障云网融合架构安全的关键路径。

4 安全威胁建模方法

4.1 安全威胁建模的基本概念

安全威胁建模是一种系统化的安全分析方法，旨在识别、评估和管理网络信息系统中潜在的安全风险。该过程通过对系统架构、数据流、访问控制机制等要素进行深入剖析，提前发现可能被攻击者利用的薄弱环节。威胁建模不仅有助于在系统设计阶段嵌入安全防护措施，还能为后续的安全策略制定、漏洞修复优先级排序以及应急响应提供科学依据，是实现“安全左移”和构建内生安全体系的重要手段。

4.2 攻击图：刻画攻击路径的可视化工具

攻击图（Attack Graph）是安全威胁建模中常用的图形化表示方法，用于直观描述攻击者从初始入口点到最终目标可能采取的多条攻击路径。它以节点表示系统状态（如已获取某权限或已攻破某组件），以有向边表示攻击动作（如利用漏洞、提权操作）。通过构建攻击图，安全人员可量化评估不同路径的风险等级，识别关键脆弱点，并模拟攻击演化过程，从而优化防御资源配置，提升整体系统的抗攻击能力。

4.3 攻击树：层次化分解攻击目标的分析框架

攻击树（Attack Tree）则采用自顶向下的层次化结构来建模安全威胁，根节点代表攻击者的最终目标（如“窃取用户数据”），子节点逐层分解为实现该目

标所需的各类攻击手段或前提条件（如“绕过身份认证”“利用 SQL 注入漏洞”等）。攻击树支持逻辑“与/或”关系表达，便于对复杂攻击场景进行结构化推理。该方法逻辑清晰、易于理解，广泛应用于系统安全需求分析、风险评估及安全测试用例生成，尤其适用于对特定高价值资产进行针对性防护设计。

5 主动防御机制研究

主动防御机制在现代网络安全体系中扮演着至关重要的角色，旨在通过积极主动的方式识别和防御网络攻击。以下是针对基于威胁情报的主动防御机制和基于人工智能的主动防御机制的深入探讨：

5.1 基于威胁情报的主动防御机制

基于威胁情报的主动防御机制主要是指通过收集、分析并应用最新的网络威胁情报来预测和识别潜在的安全威胁，并采取预防性措施。这种机制依赖于对全球范围内的安全事件、攻击模式、恶意软件样本等信息的持续监控与分析。通过整合多源数据，该机制能够快速识别新型威胁，并据此调整防御策略，如更新防火墙规则、入侵检测系统签名或部署新的安全补丁。此外，基于威胁情报的防御还能帮助组织建立更有效的应急响应计划，提高整体安全性。

5.2 基于人工智能的主动防御机制

随着信息技术的发展，基于人工智能（AI）的主动防御机制逐渐成为主流。这类机制利用机器学习、深度学习等先进的人工智能技术，自动识别异常行为，发现潜在的攻击意图。例如，通过训练模型来识别正常网络流量与异常流量之间的差异，或者利用自然语言处理技术分析社交媒体上的讨论以预测即将到来的攻击。AI 还可以辅助进行自动化决策，如自动隔离受感染的设备或调整访问控制策略。更重要的是，这些系统具有自我学习能力，能够随时间推移不断提高其准确性和效率。

5.3 结合使用两种机制的优势

将基于威胁情报的方法与基于人工智能的技术相结合，可以显著增强网络防御的有效性。一方面，威胁情报提供了关于最新攻击趋势和漏洞的具体信息，有助于针对性地优化 AI 算法；另一方面，AI 的强大分析能力使得从海量威胁情报中提取有价值的信息变得更加高效。两者相辅相成，不仅提升了对已知威胁的响应速度，还增强了对未知威胁的预测和防御能力，为构建更加健壮的网络安全防线提供了坚实基础。

6 实验与评估

6.1 实验与评估

为验证所提出的 5G/6G 云网融合架构下安全威胁建模方法与主动防御机制的有效性，本文设计了系统化的实验方案。实验环境基于 OpenStack 与 Kubernetes 构建云网融合仿真平台，集成 5G 核心网模拟器（如 UERANSIM）和边缘计算节点，并部署 SDN 控制器以支持网络切片与动态资源调度。实验工具包括 MITRE ATT&CK 框架用于威胁建模、Suricata 与 Zeek 用于流量监测、Elastic Stack 用于日志聚合分析，以及 TensorFlow/PyTorch 用于 AI 驱动的异常检测模型训练。

6.2 在实验过程与结果方面

首先基于攻击图与攻击树对典型攻击场景（如切片劫持、边缘节点入侵、跨域数据泄露）进行建模，成功识别出 12 类高风险攻击路径；随后，部署融合威胁情报与深度学习的主动防御机制，对模拟攻击流量进行实时检测与响应。实验结果显示，该机制对已知攻击的检测准确率达 96.8%，对零日攻击的异常行为识别率超过 89%，平均响应时间缩短至 1.2 秒以内。

6.3 在评估与分析阶段

采用 F1-score、误报率（FPR）、恢复时间（MTTR）等指标对模型性能进行量化评估。结果表明，相较于传统被动防御体系，本文提出的主动防御机制在检测精度、响应速度和系统韧性方面均有显著提升。此外，通过消融实验验证了威胁情报与 AI 模块的协同增效作用：二者结合可使整体防御效能提升约 23%。综上，实验充分证明了所提方法在复杂云网融合环境中的可行性与先进性。

7 结论与展望

本研究围绕 5G/6G 云网融合架构下的安全挑战，系统开展了安全威胁建模与主动防御机制的研究，提出了一套融合攻击图、攻击树建模方法与智能响应策略的综合安全防御框架。研究结果表明，基于结构化建模的安全威胁分析能够有效识别网络切片隔离失效、边缘计算节点入侵、跨域数据泄露等关键风险点，并精准刻画攻击路径与潜在影响；同时，结合威胁情报与人工智能技

术的主动防御机制显著提升了对已知及未知攻击的检测准确率与响应效率，有效增强了系统的整体安全性、稳定性与韧性。

展望未来，随着 6G 网络向太赫兹通信、空天地一体化和内生智能方向演进，云网融合架构将更加复杂、动态和开放，其所面临的安全威胁也将呈现高度隐蔽性、协同性和智能化特征。因此，安全威胁建模需进一步融合数字孪生、知识图谱等技术，实现对攻击行为的实时推演与预测；主动防御机制则应深化人工智能在异常检测、自动决策和自适应响应中的应用，推动网络安全从“被动响应”向“主动免疫”转型。此外，还需加强跨域协同安全治理、隐私保护与合规性设计，构建覆盖“云—网—边—端”的一体化智能安全生态，为下一代信息基础设施提供坚实保障。

参考文献

[1]赵婉君.面向5G/6G无线接入网的资源调度研究[J].机械工程与自动化,2025,54(04):56-58.

[2]严国忠.云网融合驱动的云业务端到端可视化运维能力提升与应用研究[J].中国战略新兴产业,2025,(27):31-33.

[3]李民锋,王颉,张海春,等.智能网联汽车网络安全威胁建模平台的实现与应用[J].网络空间安全,2023,14(03):71-77.

[4]徐胜超,蒋大锐,吕峻闽.考虑AI大模型的多维网络安全度量及主动防御策略[J/OL].计算机技术与发展,1-9[2025-11-26].https://doi.org/10.20165/j.cnki.ISSN1673-629X.2025.0269.

[5]郑吉龙,刘坚桥,王思羽,等.基于零信任架构的企业内网安全防护策略设计与实践[J].信息与电脑,2025,37(21):6-8.

作者简介：王峰，1982.12，男，汉族，山东省日照市，山东商业职业技术学院，大学本科，讲师，云计算、网络安全。