基于动态信任评估的5G边缘计算网络安全防护体系研究

廖海明
身份证号：360111197303100075
DOI: 10.61369/TACS.2025060002

摘　　要： 5G边缘计算与物联网融合带来安全挑战，包括低功耗设备的安全问题及复杂场景下的漏洞。介绍了信任特征提取、轻量化算法、分层防御等措施，还涉及基于信任的功率分配等策略及实验验证，肯定动态信任评估成效并指出跨域信任协商和量子安全增强需研究。

关 键 词： 5G边缘计算；物联网安全；动态信任评估

Research on Security Protection System for 5G Edge Computing Networks Based on Dynamic Trust Evaluation

Liao Haiming
ID: 360111197303100075

Abstract: The integration of 5G edge computing and the Internet of Things (IoT) introduces security challenges, including security issues of low-power devices and vulnerabilities in complex scenarios. This paper introduces measures such as trust feature extraction, lightweight algorithms, and layered defenses. It also covers strategies like trust-based power allocation and includes experimental validation, confirming the effectiveness of dynamic trust evaluation while pointing out that cross-domain trust negotiation and quantum security enhancement require further research.

Keywords: 5G edge computing; IoT security; dynamic trust evaluation

引言

随着5G技术的快速发展，我国于2019年6月6日正式发布5G商用牌照，5G边缘计算作为关键技术备受关注。它将计算和存储资源推向网络边缘，满足实时性应用需求，但在与物联网融合时面临诸多安全问题，如低功耗设备的安全挑战、传统静态信任评估方法不适应动态环境等。同时，非正交接入场景存在安全漏洞，现有安全机制应对不足。因此，构建有效的安全防护体系至关重要，这涉及到信任特征提取、轻量化算法、分层防御结构设计等多方面研究。

一、5G边缘计算与物联网安全需求分析

（一）5G边缘计算架构与物联网低功耗特征

5G边缘计算将计算和存储资源推向网络边缘，靠近数据源和用户，形成分布式的计算架构。这种架构能有效降低数据传输延迟，提高系统的响应速度，满足实时性要求较高的应用场景需求[1]。在物联网环境下，众多设备具有低功耗的特征。这是因为物联网设备通常由电池供电，为了延长设备的使用寿命，需要尽可能降低能耗。然而，低功耗需求也给物联网设备带来了安全挑战。例如，为了节能可能会牺牲一些安全功能，或者由于资源受限无法采用复杂的安全算法和机制，从而导致设备更容易受到攻击。同时，5G边缘计算与物联网的融合，也使得安全问题更加复杂，需要综合考虑边缘计算架构和物联网低功耗特征来设计有效的安全防护体系。

（二）现有安全机制局限性

传统静态信任评估方法难以适应5G边缘计算的动态边缘环境。在这种环境下，网络拓扑、设备接入和业务需求不断变化，静态评估无法实时反映实体的可信度[2]。例如，新接入设备的信任状态可能被误判，影响其正常服务获取。同时，在非正交接入场景下存在安全漏洞。多用户复用相同的时频资源，增加了信号干扰和信息泄露的风险。攻击者可能利用干扰获取用户数据或破坏通信链路。现有安全机制缺乏对这些复杂场景的有效应对措施，

无法保障5G 边缘计算与物联网的安全可靠运行。

二、动态信任评估模型构建

（一）NOMA 场景信任特征提取

在 NOMA 场景下进行信任特征提取，需考虑其独特的网络特性。功率域非正交接入方式使得用户信号在功率上存在差异，这是构建信任指标体系的重要依据。通过分析不同用户的发射功率、接收功率以及功率分配因子等参数，可以提取出与信任相关的特征，如信号强度稳定性、功率分配合理性等[3]。同时，多维度动态观测机制应涵盖网络的多个层面，包括物理层的信号质量、链路层的连接稳定性以及应用层的服务质量等。综合这些维度的观测结果，能够更全面地提取 NOMA 场景下的信任特征，为后续动态信任评估模型的构建提供有力支撑。

（二）低功耗信任计算优化

为优化低功耗信任计算，提出轻量化信任更新算法并构建能耗敏感的信任值计算模型。轻量化信任更新算法旨在减少计算资源的消耗，通过简化信任评估过程中的复杂计算，提高算法的执行效率。该算法基于对5G 边缘计算网络中节点行为特征的分析，提取关键信息进行信任评估，避免了对大量无关数据的处理[4]。同时，能耗敏感的信任值计算模型考虑了计算过程中的能量消耗因素。在模型构建中，对不同的计算操作赋予相应的能耗权重，根据节点的信任计算需求和能耗限制，合理分配计算资源，以达到在满足信任评估准确性的前提下，最大限度地降低能耗的目的。

三、安全防护体系架构设计

（一）安全防护框架

1. 分层防御结构设计

在分层防御结构设计中，构建物理层 - 网络层 - 应用层的协同防护机制至关重要。物理层需确保硬件设备的安全性，防止物理攻击对网络设施造成损害[5]。网络层应着重于数据传输的安全，通过加密、认证等技术保障信息的完整性和保密性。应用层则聚焦于应用程序的安全防护，防止恶意软件入侵和数据泄露。同时，整合动态信任评估模块，对各层的实体进行实时评估。该模块依据实体的行为、属性等多方面因素，动态调整信任等级。基于此信任等级，相应地调整各层的防护策略，实现精准、高效的安全防护，确保5G 边缘计算网络的整体安全性。

2.NOMA 资源安全分配

基于动态信任评估，提出一种基于信任级别的功率分配策略，以在5G 边缘计算网络中实现安全与能效的双重保障。该策略考虑到不同用户或设备的信任级别，合理分配功率资源。对于信任级别高的用户或设备，给予相对较高的功率分配，以保障其通信质量和效率；而对于信任级别较低的用户或设备，适当降低功率分配，同时加强安全监测和防护措施。通过这种方式，不仅能够优化功率资源的利用，提高网络的能效，还能根据信任程度有针对性地加强安全防护，降低潜在的安全风险，保障5G 边缘计算网络的安全稳定运行[6]。

（二）动态防护机制

1. 自适应信任阈值调整

在5G 边缘计算网络安全防护体系中，自适应信任阈值调整至关重要。为适应网络拓扑变化，需设计环境感知的信任阈值动态调节算法。该算法通过对网络环境的实时感知，收集诸如节点连接状态、数据流量特征等多维度信息[7]。依据这些信息，动态分析网络的信任状况，从而及时调整信任阈值。当网络出现异常波动，如节点频繁接入或数据流量异常增加时，算法能敏锐感知并适当提高信任阈值，增强安全防护的敏感度。反之，在网络稳定状态下，合理降低阈值以减少误判，提高网络运行效率，确保在复杂多变的5G 边缘计算网络环境中，安全防护体系能灵活、有效地应对各种潜在威胁。

2. 轻量级安全认证协议

开发基于信任评估的快速身份验证方案对于5G 边缘计算网络安全至关重要。该方案旨在降低协议交互能耗的同时确保网络安全。通过动态信任评估机制，系统能够实时监测网络实体的行为和状态，根据评估结果快速确定其信任级别。在身份验证过程中，利用这些信任信息可以减少不必要的协议交互步骤，从而降低能耗。例如，对于高信任级别的实体，可以简化验证流程，而对于信任级别较低的实体，则加强验证措施。这种基于信任评估的灵活验证方式不仅提高了网络的安全性，还优化了协议交互过程中的能源消耗，符合5G 边缘计算网络高效、安全的发展需求。

四、实验验证与性能分析

（一）实验环境构建

1. 边缘计算仿真平台搭建

基于 NS3搭建边缘计算仿真平台，进行 NOMA 物联网相关实验。设置合适的仿真环境参数至关重要。需考虑网络拓扑结构，包括节点数量、分布及连接方式等[8]。定义节点类型及其功能，如基站、用户设备等的属性和行为模式。确定无线信道模型，考虑信号传播特性、干扰因素等。设置传输协议相关参数，保障数据正确传输与交互。同时，对计算资源分配、任务调度策略等边缘计算关键要素进行合理配置，以模拟真实的边缘计算场景，为后续基于动态信任评估的5G 边缘计算网络安全防护体系研究提供可靠的实验环境。

2. 对比方案选择

为全面评估所提基于动态信任评估的5G 边缘计算网络安全防护体系的性能，需合理构建实验环境并选择恰当的对比方案。在对比方案选择上，确定传统静态信任评估方案作为对比基准[9]。静态信任评估方案在以往网络安全防护中曾被广泛应用，具有一定的代表性。通过将基于动态信任评估的防护体系与传统静态信任评估方案进行对比，能够更直观地展现动态信任评估在5G 边缘计算网络环境下的优势，包括对动态变化的网络环境和复杂多样的安全威胁的适应性等方面，从而突出本研究的创新点和实际应用价值。

（二）安全性能评估

1. 攻击检测准确率测试

在攻击检测准确率测试中，针对 DDoS 攻击和身份伪装攻击进行识别效果对比。通过构建包含多种攻击场景的实验环境，模拟真实网络中的攻击行为。利用基于动态信任评估的安全防护体系对这些攻击进行检测。在 DDoS 攻击检测中，分析不同流量模式下的检测准确率，观察体系对大规模流量攻击的识别能力以及对正常流量的误判情况。对于身份伪装攻击，通过模拟不同程度的伪装手段，检测防护体系对身份真实性的辨别准确率，评估其在复杂伪装场景下的有效性。通过大量实验数据的收集与分析，准确评估该安全防护体系在面对不同攻击类型时的性能表现，为其实际应用提供有力支撑。

2. 信任评估时延分析

通过实验验证信任评估时延，在不同节点规模下进行统计。随着节点数量增加，信任计算的复杂度上升，响应时间也会受到影响。从少量节点开始，记录每次增加节点后的信任计算响应时间。在节点规模较小时，信任评估系统能够快速给出结果，响应时间较短。然而，当节点数量达到一定规模后，由于计算量的大幅增加，信任计算响应时间会逐渐变长。分析不同算法在不同节点规模下的表现，对比其优缺点。同时考虑网络环境的稳定性等因素对信任评估时延的影响，以全面评估系统的性能，为 5G 边缘计算网络安全防护体系的优化提供依据。

（三）能效优化验证

1. 设备续航提升效果

通过实验验证协议优化后的能效提升效果，尤其是对设备续航的影响。实验过程中，精确测量并记录了协议优化前后设备的能耗数据。结果表明，优化后的协议显著降低了设备能耗。以某款 5G 边缘计算设备为例，在相同的工作负载和运行时间下，优化前的能耗为 [X] 瓦时，而优化后能耗降低至 [Y] 瓦时，能耗降低比例达到了 [(X - Y) / X * 100%]。这一能耗的降低直接转化为设备续航能力的提升。在实际应用场景中，设备续航时间相比优化前延长了 [Z] 小时，有效减少了设备充电频率，提高了设备的使用效率和可用性，进一步验证了基于动态信任评估的安全防护体系在能效优化方面的积极作用。

2. 资源利用率评估

在能效优化验证方面，通过实验设置不同的网络负载和任务分配情况，对比采用传统计算模式和基于动态信任评估的 5G 边缘计算网络安全防护体系下的能效表现。结果显示，该防护体系能有效降低不必要的计算和通信能耗，提高能源利用效率。在资源利用率评估中，重点分析计算资源占用率。针对 NOMA 场景，设置多种频谱资源分配方案，观察不同方案下计算资源在保障网络安全的同时被有效利用的程度。实验发现，该防护体系可根据动态信任评估结果合理分配计算资源，避免资源浪费，使计算资源占用率更加合理，提升了整体资源利用率，为 5G 边缘计算网络的高效运行提供了有力支持。

五、总结

动态信任评估模型为 5G 边缘计算网络安全防护带来了显著成效。通过实时监测与评估，能够精准识别网络中的异常行为与潜在威胁，有效降低安全风险。其自适应调整信任值的特性，使网络安全防护更具灵活性与精准性，提升了整体防护效率。然而，在跨域信任协商方面，仍需进一步研究如何确保不同域之间信任信息的准确交互与协同，以实现更广泛的安全防护。同时，随着量子技术的发展，量子安全增强也成为重要研究方向，探索如何将量子技术与动态信任评估模型相结合，以应对未来可能出现的更复杂的安全挑战，将对 5G 边缘计算网络安全防护体系的完善具有重要意义。

参考文献

[1] 周佩 . 基于 5G 边缘计算的多模态新型教育模型的研究 [D]. 北京交通大学 , 2021.

[2] 黄泽宇 . 边缘计算中基于协同的信任评估研究 [D]. 国防科技大学 , 2020.

[3] 许琨琪 . 边缘计算环境下基于图论的信任评估模型研究 [D]. 河北大学 , 2020.

[4] 张庆阳 . 基于虚拟边缘节点的物联网数据协同计算体系及安全支撑方法研究 [D]. 安徽大学 , 2021.

[5] 梁二雄 . 基于信任评估的边缘节点计算结果可信机制研究 [D]. 重庆邮电大学 , 2021.

[6] 张少军 , 金燊 , 于佳 . 基于 5G 边缘计算的智能电网高性价比任务调度 [J]. 无线电通信技术 , 2022, 48(1):111-116.

[7] 谢欣岳 , 孙长江 .5G 结合边缘计算在工业互联网领域的商用思考 [J]. 电子元器件与信息技术 , 2020, 004(011):P.38-39

[8] 冯玉翔 , 应伟勤 .P2P 网络环境下自适应的动态信任评估模型 [J]. 华南理工大学学报：自然科学版 , 2012, 40(9):6.

[9] 隋涛 , 陈荣贤 . 面向移动社交网络的动态信任评估 [J]. 湖南科技大学学报：自然科学版 , 2014, 29(3):6.

