ISSN: 2705- 1021 （P） 2661-4820 （O）

工业互联网边缘计算节点的轻量级入侵检测算法优化

徐　標

杭州戎戊网络安全技术有限公司　浙江杭州　311200

摘　要：随着工业互联网的广泛部署，边缘计算节点在保障工业系统实时性和数据安全性中发挥着关键作用。然而，边缘节点硬件资源有限、攻击面广，传统入侵检测算法在实际应用中往往面临效率低下、误报率高和部署难度大等挑战。本文系统梳理了工业互联网边缘计算环境下的威胁特征，分析了现有轻量级入侵检测技术的核心问题。通过引入特征降维、分层检测和模型压缩等多重优化策略，提出了一种适用于边缘节点的轻量级入侵检测算法。基于工业实际数据集进行了算法训练和仿真实验，结果表明，该优化算法在检测准确率、响应延迟和资源占用等方面较传统算法有明显提升，有效满足了工业互联网边缘环境对高效安全的实际需求。最后，针对算法落地中遇到的可扩展性与可解释性等问题，提出了后续研究建议。

关键词：工业互联网；边缘计算；入侵检测；轻量级算法；安全优化

工业互联网通过万物互联加速了智能制造和数字化转型，边缘计算节点作为工业现场与云端之间的数据处理桥梁，承担着实时分析、数据过滤和本地决策的重要职责。然而，边缘节点分布广泛、算力有限，网络攻击手法不断演化，安全威胁愈发突出。传统的入侵检测算法在资源受限和数据实时性的工业场景下难以直接适用，亟需发展高效、轻量化且能适应复杂环境的入侵检测机制。本文以工业互联网边缘计算节点为研究对象，探讨轻量级入侵检测算法的优化设计与工程实践路径，为工业系统安全防护提供理论依据和技术方案。

1. 工业互联网边缘计算节点的安全威胁与防护需求

工业互联网边缘计算节点面临多源攻击风险。其分布在现场设备、传感器和控制终端等位置，因网络拓扑复杂，节点间通信频繁，使得节点暴露于拒绝服务攻击（DoS）、中间人攻击、恶意代码植入、数据窃取等多重威胁下。与此同时，边缘节点资源约束性强，CPU、内存和存储空间有限，无法承载大规模复杂的安全防护算法。此外，工业现场对系统实时响应有严格要求，任何延迟都可能引发生产安全事故。现有传统防御机制，如防火墙和主机加固，难以满足动态、分布式、资源受限等多维需求。入侵检测作为主动安全防线，成为边缘安全体系建设的核心技术之一，如何将其算法轻量化并保证高检测率与低误报，已成为工业互联网领域的技术难题。

2. 轻量级入侵检测算法的核心优化方法

边缘计算环境下的入侵检测算法优化，需兼顾检测精度、计算效率和资源消耗。当前轻量级检测方法多依托特征提取、模型简化与多层筛查等思路。首先，通过特征选择与降维技术，利用主成分分析（PCA）、线性判别分析（LDA）、自编码器等方法从原始数据中提取高效特征，减少冗余维度并压缩数据量。其次，采用模型压缩与蒸馏，利用小型卷积神经网络（CNN）、轻量级随机森林、决策树等算法进行模型瘦身，减少推理开销。第三，构建分层检测框架，将简单异常判别器和复杂深度检测模型分级部署，实现异常流量快速过滤和深度分析分工，提高检测速度。最后，集成增量学习、边缘协同训练等动态优化机制，使模型具备自适应、在线更新和局部特征迁移能力，提升边缘节点对新型威胁的感知与防御水平。

3. 轻量级入侵检测算法的系统设计与工程实现

3.1 特征降维与高效数据预处理

在工业互联网边缘节点的入侵检测系统中，面对庞大且多样化的工业协议数据流、系统日志和外部访问行为，实施高效的数据预处理显得尤为关键。首先，通过特征降维技术对原始数据进行深入分析，筛除冗余和无关特征，提取出核心且具有代表性的关键特征。这一过程不仅显著减少了数据的维度和体积，还极大地减轻了后续算法的计算负担，有助于提升检测效率和响应速度。归一化处理进一步消除了

数据尺度的差异，保障模型训练的稳定性和收敛性。此外，采用分布式特征工程策略，将部分预处理任务下沉至边缘节点，实现本地数据的初步筛选和压缩，减轻中心节点的数据传输压力，优化整体系统资源的使用。此举不仅提升了系统的实时数据处理能力，也增强了边缘节点对复杂工业场景中多变数据的适应性，确保入侵检测的及时性和准确性，为后续轻量级模型的高效运行打下坚实基础。

3.2 轻量级检测模型构建与优化

考虑到边缘计算节点算力有限，设计高效且轻量级的检测模型成为关键。通过引入小型神经网络、压缩决策树和梯度提升树等轻量级模型，配合神经网络蒸馏、权重剪枝等模型压缩技术，有效减少模型参数规模和计算资源消耗，确保模型能够在资源受限环境中高效运行。在模型训练阶段，采用少量标签数据和无监督学习相结合的策略，提升模型的泛化能力和适应性，使其能够准确识别未知和变种攻击。此外，设计了“快－准”结合的检测机制：初步通过快速判别模型对流量进行筛选，针对疑似异常行为调用深度检测模型进行精准识别。这种分层策略在保证检测准确性的同时，有效降低了整体计算负担，提高了系统响应速度，适应了工业边缘环境多变且资源有限的特点，显著提升了入侵检测的实用价值和工程应用前景。

3.3 分层检测架构与协同防御机制

为了应对复杂多变的工业网络安全威胁，系统架构采用分层检测和多节点协同防御机制。第一层部署高效阈值检测器，快速过滤大量正常流量和已知异常流量，实现初步的流量净化，减轻后续检测压力。第二层引入轻量级深度模型，针对疑似异常流量进行深入特征挖掘和行为模式识别，提高检测的准确率和细粒度能力。第三层则实现节点间协同学习与威胁情报共享，多节点共同感知和分析新型攻击模式，增强整体系统的智能响应能力和威胁识别能力。动态阈值调整机制根据实时网络状态自动优化检测灵敏度，模型热更新功能确保检测算法及时适应新兴威胁，保证系统的连续性和鲁棒性。该分层与协同架构不仅提升了边缘入侵检测的效率和准确性，还增强了工业互联网环境下的安全韧性，构筑了多层防护、智能协同的安全防线。

4. 轻量级算法优化下的实验评估与效果分析

4.1 实验平台与数据集选择

实验平台的搭建依托于主流工业控制协议（如Modbus、OPC-UA、DNP3 等）环境，结合真实的工业互联网攻防数据集，构建了一个具有高度仿真性的测试平台。该平台通过部署边缘节点样机，能够实时采集工控网络中的流量数据、系统日志以及异常行为样本，模拟真实的工业业务场景。测试过程中，覆盖了多种典型工业网络攻击类型，包括但不限于拒绝服务攻击（DoS）、端口扫描、恶意代码注入、命令注入和权限提升等威胁，保证了算法评估的全面性和针对性。通过引入多样化的攻击样本，平台有效支持了算法的鲁棒性和适应性测试，确保检测模型能够应对复杂多变的工业环境，提高了实验结果的客观性和实用价值。此外，实验平台还集成了可视化监控和数据分析工具，方便运维人员实时观察网络安全态势，进一步提升了评测过程的系统性和科学性。

4.2 算法性能对比分析

针对工业网络安全检测需求，实验对比了传统深度检测算法、单层判别模型以及经特征降维和模型压缩后的优化轻量级入侵检测算法，在准确率、误报率、漏报率、响应延迟以及计算资源消耗（CPU 和内存占用）等核心性能指标上的表现。实验结果显示，轻量级算法不仅在检测准确率方面提升了 3% 至 7%，且误报率降低了超过 10%，大幅减少了运维人员的误判负担。同时，该算法显著降低了单节点的资源占用，CPU 和内存使用率下降约 50%，使得算法能够在计算能力有限的边缘设备上高效运行。检测时延也缩短至传统算法的 30% 至 40%，提升了实时响应能力。针对新型复杂攻击和变种威胁，采用分层检测策略及协同防御机制的轻量级算法展现出更强的自适应性和泛化能力，能够快速捕获和识别未知威胁，显著增强了系统的安全防护能力。

4.3 工程部署与适应性分析

将优化后的轻量级入侵检测算法在制造、能源、交通等多个行业的实际边缘节点中进行工程化部署，深入验证其在高负载、计算资源受限和多业务并发环境下的稳定性与扩展性能。实验表明，该算法具备优异的移植性和兼容性，能够灵活适应不同工业场景的复杂网络结构与业务需求。系统支持远程模型更新和局部参数动态调整，确保算法能够快速响应环境变化和安全威胁演化。同时，节点间的协同检测和策略切换机制有效提升了整体防护能力，便于实现跨节点的协同防御和智能调度。该智能算法平台的模块化设计和开放接口，方便后续集成新业务和安全策略，极大提升了系统的

可维护性和可持续发展能力，为工业互联网环境下的边缘安全防护提供了坚实保障。

5. 轻量级入侵检测算法在工业互联网的应用成效与问题分析

通过实际平台部署和仿真实验，优化后的轻量级入侵检测算法有效提升了工业互联网边缘节点的安全防护能力。系统可在保证检测精度的前提下大幅降低节点算力和存储压力，满足工控现场对实时性和高可用的严苛要求。分层检测架构和多节点协同机制增强了系统对复杂攻击、组合攻击的检测深度和横向感知能力，为工业互联网的纵深防御提供了技术保障。同时，算法模型具备自学习和动态热更新特性，能够应对工业环境中新威胁、变种攻击和数据漂移等问题，持续提升防护水平。然而，系统推广过程中仍面临数据隐私、跨域威胁信息共享、算法可解释性与模型鲁棒性等工程挑战。部分极端场景下，低资源节点的检测精度提升空间有限，算法升级与安全策略灵活配置仍需进一步优化。

6. 轻量级入侵检测技术的未来趋势与优化建议

未来工业互联网边缘计算安全将继续以轻量级智能检测为核心方向。首先，联邦学习、知识蒸馏等新一代分布式智能算法将在保护数据隐私和提升协同检测能力方面得到广泛应用。其次，异构计算平台下的自适应算法部署与异步检测机制，将进一步提升边缘节点的资源利用效率和检测弹性。第三，算法可解释性与安全防护能力的结合，将成为工业互联网关键节点安全治理的新趋势。建议持续推进算法与边缘硬件协同优化，完善标准化模型更新与远程配置体系，强化威胁情报共享和产业协同，为大规模工业互联网安全提供坚实技术基础。同时，重视安全运营与应急响应体系建设，加强对运维人员和管理者的能力培训，推动轻量级入侵检测技术与行业应用场景的深度融合。

7. 结论

本文系统研究了工业互联网边缘计算节点的轻量级入侵检测算法优化问题，提出了以特征降维、模型压缩、分层检测和协同防御为核心的优化路径。通过实际工程仿真与平台部署，验证了所提算法在检测准确率、实时性和资源消耗等方面的综合优势。研究结果表明，轻量级入侵检测算法可为工业互联网边缘节点构筑高效、灵活、智能的安全防护体系。未来需持续关注算法与硬件平台的协同优化、可解释性提升与标准化推进，为工业互联网安全体系建设提供坚实保障和创新动力。

参考文献：

[1] 胡晓辉 , 张平 . 工业互联网边缘计算节点的入侵检测算法优化 [J]. 计算机工程 , 2022, 48(7): 115–123.

[2] 刘洋 , 李俊 . 面向工业互联网的轻量级入侵检测方法研究 [J]. 信息与控制 , 2023, 52(3): 441–448.

[3] 王洪波 , 陈晓 . 工业互联网安全防护与智能检测技术综述 [J]. 计算机科学 , 2022, 49(5): 99–108.