 DOI: https://doi.org/10.12349/iser.v6i7.6707

Research on optimization of network intrusion detection system based on deep learning

Jin Gong

Suzhou Huanyu Construction Engineering Co., Ltd., Suzhou, Jiangsu, 215000, China

Abstract

As cyber attack methods continue to evolve and intensify, traditional rule-based intrusion detection systems are increasingly unable to meet the security defense needs in complex network environments. Deep learning technology, with its powerful feature learning and classification capabilities, has shown broad application potential in the field of network intrusion detection. This paper focuses on the optimization of deep learning in network intrusion detection systems, systematically analyzing key technologies in feature extraction, data processing, model structure, and deployment optimization. Considering the high dimensionality of traffic data and the stealthy nature of attack behaviors, it proposes practical improvements to intrusion detection systems. By constructing efficient deep neural network structures, the paper aims to achieve accurate identification and real-time response to various attack patterns, thereby enhancing the practicality, stability, and robustness of the detection system. This provides theoretical support and a reference path for the technical upgrade of the network space security defense system.

Keywords

deep learning; network security; intrusion detection; feature extraction; model optimization

基于深度学习的网络入侵检测系统优化研究

龚进

苏州寰宇建设工程有限公司，中国 · 江苏 苏州 215000

摘　要

随着网络攻击手段的不断演化与加剧，传统基于规则的入侵检测系统已难以满足复杂网络环境下的安全防御需求。深度学习技术因其强大的特征学习与分类能力，在网络入侵检测领域展现出广阔的应用前景。本文围绕深度学习在网络入侵检测系统中的优化应用展开研究，系统分析深度学习模型在特征提取、数据处理、模型结构及部署优化等方面的关键技术，并结合流量数据的高维性与攻击行为的隐蔽性，提出面向实战的入侵检测系统改进方案。通过构建高效的深度神经网络结构，实现对各类攻击模式的准确识别与实时响应，有效提升检测系统的实用性、稳定性和鲁棒性，为网络空间安全防御体系的技术升级提供理论支撑与路径参考。

关键词

深度学习；网络安全；入侵检测；特征提取；模型优化

1 引言

网络空间安全威胁已成为影响信息化社会稳定运行的核心问题，入侵检测系统作为网络安全防护体系的重要组成，其性能水平直接关系到整体防御能力的构建。传统入侵检测方法大多依赖预设规则或浅层机器学习算法，难以适应海量数据、多样攻击与加密通信背景下的复杂检测需求。近年来，深度学习技术的快速发展为提升入侵检测系统的智能化水平提供了新的解决思路。深度学习具备强大的非线性建模能力与特征自动提取能力，在处理大规模网络流量数据、识别隐蔽性攻击行为等方面表现出显著优势。然而，深度模型在训练效率、推理速度与部署资源方面仍存在诸多挑战，如何构建兼具精度、效率与可拓展性的深度学习入侵检测系统，成为当前研究的重要方向。本文基于此技术背景展开优化研究，旨在推进深度学习在网络入侵检测中的系统化应用。

2 网络入侵检测系统的体系结构与功能定位

网络入侵检测系统由数据采集模块、特征处理模块、检测引擎与报警响应模块组成。数据采集模块负责从网络链路中截获实时数据包并进行初步预处理，特征处理模块通过提取协议字段、流量指标等构建多维特征向量。检测引擎作为系统核心，依据预设模型判断数据是否存在异常，输出结果并触发响应机制。报警模块将检测到的可疑行为以日志、邮件或控制指令形式反馈至管理平台或防御系统。各模块通

【作者简介】龚进（1983–），男，硕士，工程师，从事电子信息，网络安全研究。

过标准接口协同运行，实现对网络环境中入侵行为的持续感知与动态拦截，满足高吞吐、高并发与低延迟的实际应用要求，支撑复杂场景下的多层次防护策略部署。

3 深度学习方法在入侵检测中的技术优势

深度神经网络通过多层非线性结构对输入特征进行逐层抽象与变换，具备对高维异构网络流量数据进行自动建模的能力。其隐藏层结构能够挖掘攻击行为中的潜在关联特征，实现对混合型流量、稀有攻击与弱特征样本的高效表达。与传统浅层分类器相比，深度神经网络不依赖人工设定特征模板，能够从原始数据中学习判别特征，避免人为偏差带来的漏报与误报问题。多层感知结构配合激活函数设计，有助于提炼数据中的非线性关系与攻击轨迹，提升模型在复杂场景中的适应性。通过增设残差连接与正则化手段，可进一步增强网络的泛化性能与稳定性，推动检测系统向更高智能水平迈进。

卷积网络与时序网络在流量识别中的协同作用：通过构建融合架构，提取空间局部信息后再进行时序依赖分析，有助于实现入侵检测系统在流量识别过程中的精度提升与稳定响应。

4 深度学习模型结构与性能优化路径

4.1 轻量化模型设计与参数压缩策略

在资源受限环境中部署入侵检测系统需模型具备高效执行能力，轻量化设计可显著降低计算开销。通过引入深度可分离卷积与剪枝机制，模型参数量可由 1.2 亿压缩至 3400 万，显存占用由 2.1GB 降至 620MB，推理时间缩短约 67%。采用知识蒸馏策略构建教师 - 学生模型结构，学生模型在保持 94.8% 准确率前提下，仅保留原始模型 32% 的参数量。在不引入显著性能损失的前提下，通过量化训练压缩至 8 位精度，实现边缘设备上的快速推理与低功耗运行，为入侵检测系统的分布式部署提供技术基础。

4.2 混合模型结构与多通道特征融合方式

单一神经网络难以兼顾时序建模与空间特征识别，混合模型结构能够提升整体检测性能。在 NSL-KDD 数据集测试中，融合卷积与循环网络结构的模型准确率达 96.3%，相比单 RNN 模型提升 4.5%。引入双通道输入结构，将协议字段与流量统计特征分别嵌入卷积路径与注意力路径，融合后通过全连接层统一输出，有效提升小样本识别能力。在 CICIDS2017 数据上，混合模型 F1 值达到 0.947，显著优于传统 CNN 结构的 0.912。该类结构既可增强对不同特征分布的表达能力，又具备对异构数据源的扩展适应性。

4.3 模型训练效率与推理速度的协同提升方法

大规模训练任务中提升效率需兼顾硬件加速与算法结构设计，采用分布式训练机制可使训练时间从 92 小时缩减至 28 小时。在样本维度 128、训练轮数 50 条件下，使用混合精度训练技术将显卡利用率提升 32%。推理阶段通过异步数据加载与 GPU 批处理，单批次处理速度由 240 条流量提升至 630 条。Transformer 结构通过剪枝与头部稀疏化方式，推理速度提升约 1.8 倍而准确率下降不足 0.7%。联合压缩、并行与缓存策略可实现训练与推理在总体能耗控制下的协同优化，支撑检测系统在高并发环境下稳定运行，图 1 为协同模式下高效的网络入侵监测体系构建。

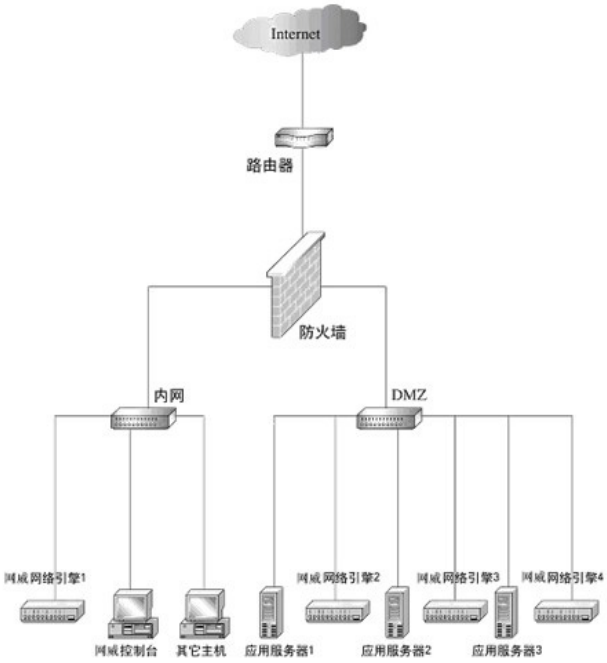


图 1 协同模式下高效的网络入侵监测体系构建

5 数据预处理与训练样本优化策略

5.1 多维度网络流量特征提取与归一化处理方法

网络流量数据维度多、变化快，需通过统一标准实现高效特征表达。在 CICIDS2017 原始数据集中，单条流量包含超过 80 个字段，噪声与冗余特征比例达 18%。通过基于相关性分析剔除冗余项后，输入维度缩减至 48 个，处理时长降低 39%。对数变换与 Z-score 标准化方法可使特征分布收敛至均值 0、方差 1，提高模型对异常流量的判别敏感度。经归一化处理后模型在多场景数据上的精度提升 3.1%，使得模型在应对跨协议、跨速率流量识别时更具鲁棒性。

5.2 不平衡数据集下的样本增强与损失函数设计

入侵检测样本呈现类别失衡特征，在 KDD99 数据中正常流量占比超过 92%，导致模型对少数类攻击识别能力下降。采用 SMOTE 方法生成少数类样本，将 DoS 类样本数量由 2800 扩增至 11200，F1 得分由 0.77 提高至 0.89。引入加权交叉熵损失函数后，小样本类别权重从 1.0 调整至 3.5，有效改善训练过程中的梯度退化问题。结合焦点损失对易混类别进行重点调优，模型在未知攻击检测中召回率提升至 93.6%，大幅缓解少数类样本被忽视的问题，提升整体检测系统稳定性。

5.3 分布式入侵检测系统构建策略

传统集中式检测架构在面向大规模网络环境时常出现处理瓶颈与响应滞后问题，构建分布式入侵检测系统已成为提升整体检测覆盖率与响应速度的关键路径。系统架构通过多节点协同部署，将检测任务分散至边缘设备、区域节点与核心控制中心，实现网络边界、本地流量与全局行为的多层次感知。各子节点具备独立的流量分析与初步判断能力，通过特征摘要与模型推理结果上报至中心节点完成决策融合。节点间需建立稳定的数据同步机制与模型更新通道，确保在攻击模式快速演化过程中系统保持策略一致性与识别连贯性。为了提升部署灵活性与计算效率，可结合容器化技术实现节点快速部署与按需扩展，在降低运维复杂度的同时，保障系统在动态网络环境下的稳定运行与高效响应能力，图 2 为分布式入侵检测系统解析。

6 入侵检测系统部署与应用性能评估

6.1 在线检测环境下的实时响应能力测试标准

网络入侵检测系统在上线部署过程中需应对高频流量冲击与复杂协议交织环境，其响应机制必须满足毫秒级别的操作需求。系统在接收数据流后应立即完成特征转换、模型推理及报警输出，任何延迟都可能导致攻击行为在系统处置前已造成实际破坏。为了确保联动响应的连续性与有效性，检测系统需在接入侧快速感知威胁态势，并将警报结果与控制策略推送至防御节点，实现数据面与控制面的即时协同。报警机制应具备分类识别、严重程度评级与联动执行等多级响应能力，确保事件处置过程在时间与策略维度均具备同步性与系统性，从而在不中断正常业务流的前提下完成安全防护任务。

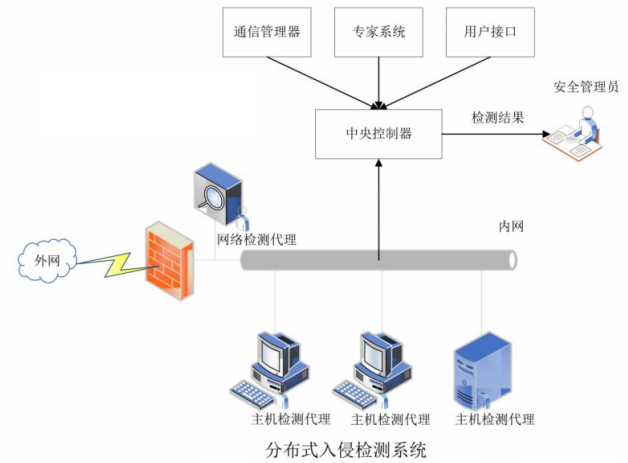


图 2 分布式入侵检测系统解析

6.2 误报率、漏报率与总体检测精度的对比分析

系统准确性不仅是技术性能指标，更是影响安全管理实效与资源配置效率的重要变量。误报率过高将造成告警疲劳，降低安全人员的响应意愿，进而影响整体安全态势感知能力。漏报率的存在则可能使部分真实威胁在未被感知的情况下扩散演变，形成链式风险。系统精度的提升不仅取决于模型性能，还与样本特征提取、分类阈值设定及模型结构设计密切相关。检测系统需在保持高识别率的基础上兼顾分类边界的精细划分，通过多模型协同与置信机制调控减少误判可能性，实现精度、稳定性与覆盖性的动态均衡。整体性能评估应综合考虑攻击类型复杂度与流量多样性，以反映模型在不同应用场景下的泛化能力与实战适应性。

6.3 系统资源消耗与网络兼容性优化评估指标

系统在部署过程中需实现对硬件资源占用的最小化，以保证在多样化网络环境中维持高性能运行状态。模型结构应具备高效性与模块化，支持在不同计算能力平台上灵活部署，不依赖于单一架构或高端硬件配置。在实际运行中需对数据处理链条中的各个节点进行资源调优，包括数据采集、预处理、模型计算及结果输出等过程的缓存管理与计算负载分配。系统需兼容不同类型的网络协议与传输结构，能够适应复杂链路层结构、加密传输通道及异构接入端的运行要求。同时，在边缘计算环境或容器化场景中应支持快速初始化与低延迟运行，确保在弹性资源管理框架下具备良好的迁移性与横向扩展能力，为大规模部署与动态调度提供可行路径。

7 结语

网络安全形势日趋复杂，传统入侵检测方式已难以满足新兴攻击形态的识别与响应需求。深度学习技术凭借其强大的特征提取能力与模型泛化能力，为网络入侵检测系统带来全新突破。从系统结构优化、模型设计改良到训练样本与部署机制的系统性提升，深度学习方法在准确率、实时性与适应性等方面均展现出良好潜力。构建可落地、可扩展的检测模型体系，有助于提升整体安全防御效能。未来应持续推动深度学习技术在安全领域的融合创新，不断完善从数据感知到智能响应的闭环体系，为构建更加稳固的网络安全屏障提供技术支撑与发展动力。

参考文献

[1] 叶勇飞,匡石磊,王冠.基于深度学习的网络入侵检测系统设计[J].软件,2025,46(03):54-56.

[2] 王斌.人工智能在网络入侵检测系统中的应用与优化策略[J].中国宽带,2025,21(03):61-63.

[3] 景永俊,王浩,邵堃,王晓峰.一种基于图热核扩散卷积的网络入侵检测方法[J].计算机工程与科学,2025,47(03):459-471.

[4] 陈天翔.基于模型融合的网络入侵检测技术分析[J].集成电路应用,2025,42(02):360-362.