基于机器学习的互联网网络异常流量检测研究

王 浩[1] 毛 倩[2]

1.中国电信股份有限公司孝感分公司 湖北 孝感 432100

2.中国电信股份有限公司武汉分公司 湖北 武汉 430000

【摘 要】：机器学习以数据驱动为核心，具备自主特征学习、复杂模式识别、动态迭代优化与泛化推理能力，成为构建新一代互联网异常流量检测体系的关键技术。本文围绕互联网网络流量异常检测全流程，系统研究机器学习在数据治理、特征工程、模型构建、系统部署中的应用机制，设计面向网络环境的轻量化高精度检测方案，通过多维度特征提取、混合模型融合、注意力机制增强与半监督学习优化，有效缓解样本不平衡、检测时延高、漏报与误报等关键问题。研究表明，基于机器学习的检测方法检测精度高、实时性强、泛化性好，可稳定支撑高并发场景下的异常识别与安全防御，为互联网智能安全防护提供了有效技术方案。

【关键词】：机器学习；互联网技术；网络流量；异常检测

DOI:10.12417/2705-0998.26.06.054

互联网作为数字社会的关键信息基础设施，承载着海量业务交互与数据传输，其安全稳定运行直接关系到网络服务质量与用户信息安全。当前，网络流量向高带宽、高并发、强加密、多协议方向发展，分布式拒绝服务（DDoS）攻击、恶意扫描、僵尸网络通信、非法入侵与数据窃取等威胁持续升级，攻击行为呈现智能化、隐蔽化、多态化特征，而机器学习能够从大规模多源流量数据中自动学习正常行为基线与异常分布模式，实现对已知与未知异常的精准识别与实时预警，显著提升了检测系统的自适应能力与防御效能。本文立足互联网技术应用实际，以机器学习为主线，构建从数据预处理、特征提取、模型训练到系统部署的一体化检测框架，重点突出算法模型在流量特征挖掘、异常分类识别与实时推理中的核心作用，为运营商网络安全防护升级提供理论依据与实践方案。

1 网络异常流量特征与机器学习检测机理

1.1 网络异常流量定义与分类

网络异常流量是指在数据包结构、时序分布、访问频率、协议行为、连接关系等维度显著偏离正常业务模型的网络传输行为，通常由网络攻击、恶意程序、设备故障或配置错误引发，按照流量成因与行为特征可划分为攻击类、恶意程序类、业务异常类与系统故障类四类，各类异常在流量统计与时序特征上存在可量化差异，为机器学习模型提供了可学习的区分依据：攻击类异常以资源耗尽与权限获取为目标，表现为流量突增、连接请求密集、报文特征高度重复；恶意程序类流量以远程控制与数据回传为特征，常伴随周期性心跳包、非常规端口通信与隐蔽隧道建立；业务行为异常多体现为非典型协议交互、高频短连接、单向数据流与异常大包传输；设备故障类流量则表现为流量环路、广播风暴、会话异常中断等规律性畸变。

1.2 机器学习检测核心优势

机器学习在互联网网络异常流量检测中具备不可替代的核心优势，它以数据驱动替代规则驱动，能够自主完成特征提取、模式学习、分类判决与模型迭代，突破人工特征设计的主观性与局限性，同时支持在线增量学习与动态更新，可快速适配流量变化与新型攻击手段。机器学习能够对高维、异构、时序流量数据进行端到端处理，自动挖掘人工难以定义的隐性特征，在小样本、不平衡、高噪声场景下仍保持稳定判别能力；深度学习模型进一步通过多层非线性变换，实现从底层报文特征到高层行为语义的逐级抽象，对加密流量、变异攻击与复合型攻击的识别能力显著优于传统方法。

1.3 典型算法性能对比

为直观体现机器学习算法在异常检测任务中的差异，采用主流公开数据集进行指标测试，结果如表 1 所示。

表 1 典型机器学习算法异常检测性能对比

算法类型	准确率	精确率	召回率	F1 分数	AUC	训练效率
支持向量机（SVM）	92.52%	91.18%	93.37%	92.26%	0.951	较低
随机森林（RF）	90.27%	89.46%	91.05%	90.25%	0.932	中等
轻量级梯度提升机（LightGBM）	95.14%	94.32%	95.68%	95.00%	0.975	高
卷积神经网络+注意力（CNN+注意力）	97.86%	97.24%	98.01%	97.62%	0.991	中等
双向长短期记忆网络+卷积神经网络（BiLSTM+CNN）	98.33%	97.95%	98.47%	98.21%	0.994	中等

2 基于机器学习的流量数据预处理与特征工程

2.1 数据预处理

数据预处理是保障机器学习模型性能的基础环节，原始互联网流量数据包含噪声、缺失值、冗余字段与量纲差异，直接影响模型收敛速度与检测精度，必须遵循标准化流程完成治理。研究以机器学习数据工程规范为指导，依次执行数据清洗、缺失值处理、归一化与数据均衡操作，通过过滤错误报文、去重、修正标签偏差降低噪声干扰，采用均值填充与规则填充保证数据完整性，使用最小-最大（Min-Max）缩放与标准化（Z-score）标准化统一特征尺度，避免量纲差异导致模型权重失衡。针对异常样本稀缺导致的类别不平衡问题，综合采用过采样、欠采样、合成少数类采样（SMOTE）样本生成与半监督学习策略，在不引入额外分布偏差的前提下提升模型对少数类异常的学习能力。预处理流程以流式处理架构为支撑，可对实时到达的流量数据进行逐批次清洗与转换，保证模型输入的时效性与一致性，为高精度、高鲁棒性检测奠定数据基础。

2.2 多维度特征提取与筛选

特征工程直接决定机器学习模型的上限，面向互联网流量场景，本研究从统计特征、时序特征、协议特征、行为关系特征四个维度完成特征提取，覆盖包长分布、流量速率、连接时长、会话时序、传输控制协议（TCP）标志位、端口规律、IP 访问关系等关键指标，全面刻画流量行为模式。统计特征聚焦单条流与滑动窗口内的宏观分布，时序特征重点捕捉请求间隔、波动趋势与周期性变化，协议特征深入解析报文头部字段与应用层载荷规律，行为关系特征构建 IP、端口、会话之间的关联图谱，形成多尺度、多层次特征空间。在此基础上，采用基于信息增益、方差分析与卡方检验的混合特征选择算法，自动剔除冗余特征、低区分度特征与高噪声特征，筛选贡献度高、相关性弱、泛化性强的核心特征集合，显著降低特征维度与计算开销，提升模型训练效率与推理速度。通过自动化特征工程与机器学习算法的深度耦合，实现从原始流量数据到高维可训练向量的高效转化，为高精度异常检测提供可靠特征支撑。

3 机器学习检测模型构建与优化

3.1 混合模型架构设计

采用传统机器学习+深度学习的混合检测架构，以适配互联网场景高精度与低时延双重需求：传统机器学习方面，选用轻量级梯度提升机（LightGBM）作为轻量级基线模型，基于梯度提升与直方图优化思想，在训练速度、资源占用与推理效率上具备显著优势，适用于边缘节点、接入网设备等高并发实时推理场景，能够在保证检测精度的同时满足大规模部署的性能要求；深度学习方面，构建卷积神经网络-双向长短期记忆网络（CNN-BiLSTM）融合模型，利用卷积神经网络（CNN）的局部感受野自动提取报文载荷与统一资源定位符（URL）文本特征，通过双向长短期记忆网络（BiLSTM）对长时序流量序列进行编码，精准捕捉时序依赖与渐变式异常，并引入通道注意力机制动态加权关键特征通道，强化对隐蔽异常与微小变异攻击的感知能力，使模型在复杂流量环境中仍能聚焦关键判别信息。针对日志文本与统一资源定位符（URL）恶意检测场景，分别采用文本卷积神经网络（CNN-Text）与空间注意力卷积神经网络（SA-CNN）模型，通过卷积、池化与注意力机制的组合，实现对关键字符串、异常路径与恶意代码片段的精准定位，大幅降低误报率。混合架构可根据场景动态切换模型组合，在骨干网核心节点启用高精度深度学习模型，在边缘接入点启用轻量化模型，实现精度与性能的全局最优，兼顾核心区域高检测质量与全网范围内低时延响应。

3.2 模型训练与评估体系

模型训练过程严格遵循机器学习工程实践，采用分层 K 折交叉验证、网格搜索与贝叶斯优化进行超参数调优，使用焦点损失函数（Focal Loss）与类别权重均衡解决样本不平衡问题，通过早停策略与正则化抑制过拟合，确保模型在开放网络环境下稳定收敛与泛化。模型评估摒弃单一准确率指标，构建以精确率、召回率、F1 分数、受试者工作特征曲线下面积（AUC）为核心，以推理时延、吞吐量、模型体积为辅助的多维度综合评价体系，重点关注漏报率与误报率，保证模型在真实网络环境中的可靠性与实用性。训练过程支持增量学习与迁移学习，可利用历史数据预训练、现网数据微调，快速适配不同地域、不同业务类型的流量分布特征，大幅降低模型部署成本。通过训练流程标准化、评估体系科学化与迭代机制自动化，实现模型性能最优、泛化能力最强、工程落地性最好的目标，让检测模型能够持续适应互联网流量动态变化与攻击手段持续升级的现实需求。

4 基于机器学习的互联网异常检测系统设计

4.1 系统总体架构

面向运营商互联网环境，构建以机器学习为核心的五层分布式异常检测系统，实现流量采集、数据处理、模型推理、异常决策、防御响应全流程智能化。系统采用微服务与分布式计算架构，通过分布式消息队列（Kafka）流式消息队列实现数据解耦与削峰填谷，依托容器编排平台（Kubernetes）完成容器编排与弹性扩缩容，支持高并发、大带宽流量处理，可满足骨干网与城域网多级部署需求。流量采集层通过端口镜像、网络数据流输出/网际协议流信息输出（NetFlow/IPFIX）与硬件探针完成全量数据采集，保证低侵入、高兼容、无业务影响；数据处理层基于分布式流式计算框架（Spark Streaming）实现流式清洗、特征计算与标准化，支持秒级特征输出；模型引擎层采用模型仓库与推理服务分离设计，支持多模型并行加载、热更新与灰度发布；异常决策层通过置信度分级、多源关联分

析、告警压缩与降噪算法，减少无效告警；防御响应层与防火墙、路由器、软件定义网络（SDN）控制器联动，实现自动限流、IP 封堵、路由调整与会话切断，形成完整安全闭环，确保异常流量可快速发现、精准定位、及时处置。

4.2 核心模块与性能指标

系统以机器学习推理引擎为核心中枢，包含数据预处理、特征工程、模型管理、实时检测、响应处置五大模块，支持模型在线迭代与增量学习，可根据业务流量动态调整检测策略与资源分配。模型管理模块提供版本控制、效果监控、自动回滚与周期重训练能力，保障模型长期稳定运行；实时检测模块支持批量推理与流式推理双模式，可根据流量负载动态调整并发数；异常决策模块引入上下文关联分析，结合黑白名单、威胁情报与历史行为，进一步提升判定准确性。系统关键性能指标如表 2 所示，在高并发与复杂攻击场景下仍保持低时延、高准确率与高防御成功率，满足互联网业务安全与运营商级可靠性要求，能够支撑电信级网络 7×24 小时稳定运行。

表 2 异常检测系统关键性能指标

测试场景	吞吐量	端到端时延	检测准确率	防御成功率
常规流量	1Gbps	5ms	98.62%	95.18%
高并发流量	500Mbps	8ms	95.37%	92.79%
复杂攻击	500Mbps	12ms	94.28%	91.46%

5 结语

机器学习为互联网网络异常流量检测提供了数据驱动、自主学习、实时推理、动态迭代的全新技术路径，从根本上解决了传统规则检测在复杂网络威胁下泛化能力弱、误报漏报高、响应滞后等核心问题，显著提升了互联网安全防护的智能化水平与防御效能。本文构建覆盖数据治理、特征工程、模型构建、系统部署的全流程机器学习检测体系，立足运营商实际场景，突出算法模型在特征提取、异常识别与实时推理中的核心作用，通过混合架构、注意力机制与半监督学习实现性能优化，具备较强的理论价值与工程落地能力。随着互联网技术持续演进与网络威胁不断复杂化，未来可进一步结合联邦学习、图神经网络、加密流量明文无关检测等前沿机器学习方向，提升跨域协同防御、隐蔽攻击识别与隐私保护能力，推动互联网安全防护向更智能、更高效、更可信的方向持续升级。

参考文献：

[1] 郑雯,孟晓青.基于机器学习的网络流量异常检测研究[J].信息系统工程,2025(06):87-89.

[2] 赵东明.基于机器学习的网络流量异常行为检测与入侵防御系统研究[J].信息与电脑(理论版),2025,37(12):84-86.

[3] 沈德松.基于机器学习的网络异常流量检测[J].安徽科技学院学报,2024,38(01):111-116.