 DOI: https://doi.org/10.12345/bdai.v7i2.37675

Research and Implementation of Network Intrusion Detection System Based on Machine Learning

Zhenglian Zhou

Ludong University, Zaozhuang, Shandong, 264025, China

Abstract

As cyberattack methods continue to evolve, traditional intrusion detection approaches based on feature matching have become inadequate for addressing complex cybersecurity challenges. This study systematically investigates the application of machine learning in intrusion detection, examining dimensions including data feature construction, model selection, training strategies, and system implementation. By analyzing multidimensional attributes of network traffic, we establish a feature system tailored for classification tasks. Through performance comparisons using supervised learning, ensemble learning, and deep learning models, we develop a detection solution adaptable to diverse scenarios. The proposed deployable intrusion detection system architecture integrates data collection, feature transformation, model inference, and alert management processes. Research demonstrates that machine learning models achieve high detection rates and low false alarm rates in high-dimensional, complex traffic environments, providing robust support and practical references for intelligent cybersecurity system development.

Keywords

Machine learning; Network security; Intrusion detection; Anomaly detection; System implementation

基于机器学习的网络入侵检测系统研究与实现

周政涟

鲁东大学，中国·山东 枣庄 264025

摘　要

随着网络攻击方式不断演化，传统基于特征匹配的入侵检测方法已难以满足复杂网络安全需求。本文围绕机器学习在入侵检测中的应用展开系统研究，从数据特征构建、模型选择、训练策略与系统实现等维度进行探讨。通过分析网络流量的多维属性，构建面向分类任务的特征体系，并基于监督学习、集成学习及深度学习等多类模型进行性能比较，形成适用于多场景的检测方案。文章设计了一个可部署的入侵检测系统架构，实现数据采集、特征转换、模型推理及警报管理的完整流程。研究结果显示，机器学习模型能够在高维、复杂的流量环境中取得较高检测率与较低误报率，为智能化网络安全系统构建提供了有效支撑与实践参考。

关键词

机器学习；网络安全；入侵检测；异常检测；系统实现

1 引言

信息化与数字化发展使网络系统成为关键基础设施，网络攻击的复杂性、隐蔽性日益增强。传统入侵检测系统依赖静态规则或特征签名，对未知威胁的识别能力有限，而攻击方式的多样化使规则更新滞后问题愈加突出。在此背景下，机器学习因其可从数据中提取模式、自动分类未知样本的特点，被广泛引入入侵检测领域。机器学习不仅能够提升检测系统的智能化程度，也使入侵识别从经验驱动过渡到数据驱动。然而，网络环境高维数据、多样协议与动态行为模式也给模型构建带来挑战，特别是在数据不平衡、特征冗余、实时性要求等方面，需要进行深入研究。本文围绕模型构建、系统设计与应用场景展开讨论，在理论分析与应用实现之间构建更加紧密的联系，以期为机器学习入侵检测系统提供可行方案。

2 机器学习在网络入侵检测中的应用基础

2.1 网络入侵行为特征的数据表示方法

入侵检测离不开有效的数据特征表达。网络流量包含时间、空间及协议多维信息，其特征通常来自数据包头字段、连接行为统计与内容特征分析等方面。高质量的特征不仅提升模型的识别精度，也决定检测系统对不同攻击类型的适应能力。常见入侵特征包括连接持续时间、数据包数量、协议类型、目的端口分布、流量方向比等，这些特征能够较好地反映网络行为状态。为减少冗余特征带来的模型过拟合

【作者简介】周政涟（2005—），男，中国山东省枣庄人，在读本科，从事计算机研究。

风险，需结合特征选择技术，通过相关性分析、主成分转换或基于模型的特征重要度评价，实现对高维数据的压缩。在实际应用中，特征表达还需兼顾可计算性与实时性，使模型适用于动态网络场景。

2.2 机器学习模型类型与算法特性分析

网络入侵检测中的机器学习模型主要包括监督学习、无监督学习与集成学习三类。监督学习模型如支持向量机、决策树、随机森林与神经网络，依赖标签数据进行分类，适用于攻击样本特征明确的场景。无监督模型如聚类分析、孤立森林等更适合未知威胁检测，可在无标签条件下识别偏离正常行为的异常流量。集成学习通过组合多个弱分类器提升泛化能力，在入侵检测中表现出较高稳定性。随着深度学习的发展，卷积神经网络、长短期记忆网络等能够自动学习流量特征，提高对复杂攻击模式的识别能力。不同模型的训练复杂度、解释能力与计算资源需求各不相同，需根据具体场景选择适宜算法。

2.3 数据质量与模型性能的关系研究

机器学习模型在入侵检测中的表现高度依赖训练数据的代表性与有效性。数据不平衡情况普遍存在，攻击样本数量远低于正常样本，导致模型偏向正常行为而忽视潜在威胁。为缓解此问题，可采用过采样、欠采样或基于生成模型的数据增强策略提升分类平衡性。此外，网络数据噪声多、来源复杂，需通过预处理保证数据的清洁性。

3 基于机器学习的网络入侵检测模型设计

3.1 特征工程的构建与优化策略

特征工程在入侵检测系统中具有基础性作用，其质量直接决定模型对复杂网络行为的刻画能力。为构建高效特征体系，需从协议结构、流量行为与内容负载三个维度进行综合提取。在协议层面，通过分析 TCP、UDP 等协议的连接频率、握手过程及报文字段异常，可揭示潜在攻击；在行为层面，统计流量大小、端口规律及连接持续时间，可有效描述扫描、暴力破解等宏观特征；在内容层面，分析数据包负载有助于识别溢出攻击与恶意代码。为提升模型稳定性，特征需经标准化处理以消除量纲影响。同时，可运用 PCA、自动编码器等降维技术构建紧凑特征空间，并借助互信息、卡方检验或嵌入式方法筛选最具区分度的特征，从而在增强模型泛化能力的同时降低计算开销。

3.2 模型训练策略与分类性能提升方法

网络入侵检测的训练数据往往存在类别不平衡问题，正常流量占比远高于攻击流量，导致模型容易忽略低频攻击样本。为此，可采用代价敏感学习策略，通过对高风险攻击行为设置更高的误分类代价，使模型在训练中增强对少数类样本的关注度。此外，可采用 SMOTE、ADASYN 等过采样方法重构训练集，使数据分布更加均衡。训练过程中，通过交叉验证评估不同的超参数配置，利用网格搜索、随机搜索或贝叶斯优化提升模型性能。为了降低过拟合风险，可引入 L1/L2 正则化、随机失活（Dropout）以及提前停止训练等策略。集成学习方法，如随机森林、梯度提升树以及模型投票机制，可综合多个模型的优势，提高入侵检测的稳健性与整体准确率。在复杂场景中，多模型融合往往表现出更高的泛化能力，有助于应对不断变化的攻击模式。

3.3 深度学习在入侵检测中的应用探索

深度学习技术因其具备自动特征提取能力，已成为入侵检测领域的重要研究方向。卷积神经网络（CNN）能够利用局部感受野与参数共享机制，从流量数据的空间结构中提取关键特征，适用于识别具有固定模式的攻击行为。循环神经网络（RNN）与长短期记忆网络（LSTM）在处理时间序列数据方面具有优势，可捕获流量序列中的依赖关系，从而识别多阶段攻击或具有持续特征的恶意行为。近年来，基于 Transformer 的注意力机制模型在入侵检测中展现出卓越表现，通过动态关注关键特征，能够在复杂环境下实现高精度识别。尽管深度模型提升了检测准确率，但其计算需求较高，尤其在实时场景中容易受限于硬件资源。因此，在实际部署中需在性能与开销之间做好权衡，可结合模型压缩与硬件加速技术实现高效运行。

4 网络入侵检测系统的架构设计与实现

4.1 系统整体架构的分层设计思路

基于机器学习的网络入侵检测系统在结构设计上通常采用分层式架构，以实现系统在复杂网络环境中的稳定运行与便捷维护。整个系统主要由数据采集层、特征处理层、模型推理层与告警响应层构成。数据采集层依托交换机镜像端口、网络流量监控设备或数据代理工具获取实时网络数据，确保流量来源的完整性与连续性。特征处理层对原始流量进行清洗、格式化、统计分析与特征转换，以降低噪声对模型的干扰并提升模型输入的有效性。模型推理层使用预训练的机器学习或深度学习模型对特征向量进行分类，识别正常行为与潜在攻击。告警响应层根据模型输出的风险等级触发告警机制，记录日志并生成报告，以便安全人员进行后续分析。分层架构使各模块具备独立性，可根据实际需求进行灵活替换与扩展，从而提升系统的可维护性与扩展能力。

4.2 模型部署与系统实时性优化策略

在实际网络环境中，大规模流量与高并发数据要求入侵检测系统具备较高的实时性与响应速度。因此，模型部署需要在性能、计算成本与准确率之间取得平衡。轻量化模型由于参数规模小、计算速度快，适合部署于边缘节点，实现近源检测，降低中心服务器压力；而复杂模型可部署在后端服务器中，通过批量推理处理高复杂度的攻击检测任务。为了提高实时性，系统可采用批处理策略，将连续数据合并后统一推理，减少模型调用频次；同时利用内存缓存机制降低数据读写延迟。在硬件方面，可采用 GPU 或 FPGA 加速推

理过程，提高深度模型的处理效率，使系统能够应对高带宽、高并发的网络环境。在此基础上，模型压缩与推理引擎优化技术也可进一步提升系统的整体运行速度。

4.3 告警机制与可视化分析平台构建

一套完善的告警机制对于提高网络安全响应效率具有重要意义。入侵检测系统需要根据攻击类型、威胁等级与流量特征的变化对告警进行分级处理，使安全管理人员能够快速判断事件的紧急程度与潜在影响。系统应提供规则化、可配置的告警策略，支持多种告警方式，如短信提醒、邮件推送与后台控制台提示等。在分析层面，构建可视化平台可显著提升系统的可读性与可操作性，通过图表、时间序列、风险分布等方式展示流量趋势与模型检测结果，使复杂数据更易于理解。结合日志归档与查询模块，系统能够对历史入侵事件实现复盘分析，帮助安全人员识别攻击模式、评估防护策略效果，并为模型更新提供依据。可视化与告警机制的结合不仅增强系统的实用性，也提升整体网络防御能力。

5 基于机器学习的入侵检测系统应用问题与改进方向

5.1 数据隐私与安全问题的挑战

在网络入侵检测系统的构建与应用过程中，数据采集与模型训练往往需要处理大量网络流量，这些流量中可能包含用户身份信息、访问记录、通信内容等敏感数据。若缺乏完善的隐私保护机制，可能导致数据滥用、非法泄露等安全风险，严重影响系统在实际环境中的可用性。因此，如何实现隐私保护与数据分析的兼容成为关键挑战。常见解决途径包括采用数据匿名化技术，将身份关联信息移除或模糊处理，从根源上降低隐私暴露风险；采用加密传输与加密计算技术，确保数据在存储与传输过程中不被窃取或篡改；利用联邦学习等分布式训练技术，使模型能够在各数据节点独立训练并共享参数，而无需直接集中原始数据，从而在不泄露数据的前提下提升模型性能。隐私保护机制的完善不仅关系到法律合规性，也直接影响系统在实际部署中的信任度和可推广性。

5.2 模型泛化能力不足与对新型攻击的适应问题

网络攻击手段更新速度极快，新型攻击在特征模式、攻击流程和隐蔽性方面表现出高度复杂性，使传统固定模型难以长期保持稳定的识别能力。模型在训练数据与真实流量之间存在分布差异，导致泛化能力不足，尤其是在面对零日攻击或变种攻击时容易出现误判或漏判。为解决此问题，可引入在线学习策略，使模型能够在系统运行过程中持续接收新的样本数据并更新参数，从而逐步适应网络环境的动态变化。此外，迁移学习技术也能有效提升模型在不同网络环境之间的适应性，通过共享基础特征学习能力，使模型在数据量较少的新场景中仍可保持较高性能。研究表明，结合异常检测方法、集成学习技术与行为模式分析，可进一步提升系统对未知威胁的识别能力，使入侵检测更加灵活、稳健。

5.3 系统部署成本与资源消耗的限制

机器学习特别是深度学习模型在入侵检测中的应用往往伴随较高的计算与存储成本，使其在资源受限的网络环境中难以大规模部署。深度模型的训练与推理需要大量算力，在高并发网络环境中可能影响检测实时性，甚至造成系统延迟。为提升适用性，可引入模型压缩、参数量化、剪枝技术等方法在保证精度的同时减少模型规模，使模型运行更加轻量化。

6 结语

机器学习为网络入侵检测带来了新的发展契机，使系统可以摆脱对人工经验与静态规则的依赖，通过学习历史数据模式识别复杂威胁。本文从特征工程、模型训练、系统架构与部署等方面对基于机器学习的入侵检测技术进行了全面讨论，并提出面向未来的优化方向。研究表明，机器学习在检测未知攻击、处理复杂流量与提升系统智能化水平方面具有显著优势，但仍需在隐私保护、模型泛化与部署资源等方面持续优化。未来入侵检测系统将更加依赖数据协同、跨领域模型集成与智能决策机制，实现从“检测”到“预测”的跨越，为网络安全保障提供更强支撑。

参考文献

[1] 孙贻刚.基于机器学习的网络入侵检测系统设计与实现[J].信息记录材料,2025,26(12):165-167.

[2] 方丽萍,刘腾飞,刘栋,等.基于机器学习的网络入侵检测系统端到端框架设计[J].电子设计工程,2025,33(21):26-31.

[3] 罗晓璐,陈鑫,卢微.机器学习在网络入侵检测系统中的应用与效能分析[J].网络安全技术与应用,2024,(12):10-12.

[4] 韩佩阳.基于机器学习的网络入侵检测与分类系统研究[J].电脑编程技巧与维护,2024,(06):104-107.

[5] 王壮.基于机器学习的网络入侵检测系统研究[D].电子科技大学,2023.