基于深度学习的恶意流量检测与防御技术研究

林 英

中国石化销售股份有限公司云南德宏分公司 云南德宏

【摘要】随着网络攻击手段的不断演进，传统的恶意流量检测方法已难以满足复杂环境下的安全需求。基于深度学习的恶意流量检测技术，通过自动提取数据特征和多层次模式识别，显著提升了检测的准确性与实时性。本文围绕深度学习模型在恶意流量识别中的应用，探讨了多种主流网络攻击场景下的检测策略及其防御机制。研究表明，结合深度神经网络的智能分析方法不仅能有效识别复杂攻击，还能动态调整防御策略，实现对恶意流量的高效防护，推动网络安全防御技术向智能化发展迈进。

【关键词】深度学习；恶意流量检测；网络安全；智能防御；异常检测

【收稿日期】2025 年 5 月 12 日 【出刊日期】2025 年 6 月 4 日 【DOI】10.12208/j.jer.20250247

Research on malicious traffic detection and defense technology based on deep learning

Ying Lin

Sinopec Yunnan Dehong Branch, Dehong, Yunnan

【**Abstract**】As cyber attack methods continue to evolve, traditional malicious traffic detection techniques have become inadequate for the security requirements in complex environments. Deep learning-based malicious traffic detection technology significantly enhances accuracy and real-time performance through automatic data feature extraction and multi-level pattern recognition. This paper focuses on the application of deep learning models in malicious traffic identification, exploring detection strategies and defense mechanisms under various mainstream network attack scenarios. The study shows that intelligent analysis methods combining deep neural networks can not only effectively identify complex attacks but also dynamically adjust defense strategies, achieving efficient protection against malicious traffic and advancing cybersecurity defense technology towards smarter development.

【**Keywords**】Deep learning; Malicious traffic detection; Network security; Intelligent defense; Anomaly detection

引言

网络空间的安全威胁日益严峻，恶意流量作为攻击的核心载体，给信息系统带来了巨大风险。传统基于规则或特征匹配的检测技术在面对新型复杂攻击时表现出明显不足，难以实现高效、准确的识别[1]。深度学习技术凭借其强大的特征自动提取和模式识别能力，为恶意流量检测提供了全新的解决方案。通过构建多层神经网络模型，能够深入挖掘流量中的隐含特征，实现对多样化攻击行为的精准捕获与防御，有效提升了网络防护的智能化水平，满足了现代网络环境的安全需求。

1 恶意流量检测面临的挑战与问题分析

恶意流量的检测是保障网络安全的核心环节之一，然而随着网络攻击技术的不断升级，传统的检测方法面临诸多严峻挑战。网络流量的复杂性和多样性显著增加，攻击者通过伪装正常流量、变换攻击模式以及利用加密技术，使得恶意流量与合法流量的边界变得模糊[2]。这种高隐蔽性使得基于规则和特征匹配的传统检测机制难以有效识别，导致误报和漏报率显著上升，严重影响了网络安全防护的可靠性和实效性。随着物联网、云计算等技术的普及，网络环境日益开放，恶意流量传播的路径更加广泛且复杂，传统检测系统难以实现对大规模、高速数据流的实时监控和处理，网络安全防御的压力倍增。

另一个亟需解决的问题在于恶意流量的多样化表现。网络攻击类型涵盖分布式拒绝服务攻击（DDoS）、网络钓鱼、恶意软件传播、数据窃取等多种形式，每种攻击行为在流量表现、协议特征及传输模式上存在显著差异。传统检测技术往往依赖专家经验制定固定规则，难以覆盖所有攻击场景和变异手法，缺乏对未知攻

击的识别能力。特别是在面对零日攻击和高级持续威胁（APT）时，现有方法表现出明显不足，无法实现对新型恶意流量的有效防控。此外，流量数据的高维度和非结构化特点进一步增加了检测的难度，如何从海量流量中提取有效特征成为技术瓶颈。

网络环境的动态性也对恶意流量检测提出了更高要求。网络拓扑结构、应用服务以及用户行为不断变化，导致流量特征时刻处于变动状态。静态的检测模型缺乏自适应能力，难以快速响应新的威胁形态和攻击策略。对检测系统的实时性和准确性提出了更严苛的考验[3]。网络防御系统需要具备动态更新和学习能力，能够适应复杂多变的网络环境，并实现对攻击行为的快速识别和响应。由此可见，恶意流量检测面临的挑战不仅体现在技术层面，也体现在实际应用的多样性和复杂性上，亟需引入更为智能化的分析手段来提升检测的深度和广度，推动网络安全防御技术向更高水平发展。

2 深度学习技术在恶意流量识别中的关键方法

深度学习技术因其卓越的自动特征提取能力和复杂模式识别优势，逐渐成为恶意流量识别领域的关键突破口。相较于传统机器学习依赖人工设计特征的方法，深度神经网络能够从海量原始流量数据中自主学习高维度、非线性特征，有效捕捉恶意流量中隐蔽且复杂的攻击模式[4]。卷积神经网络（CNN）通过对流量数据进行局部空间特征提取，能够识别流量中潜在的异常分布和攻击痕迹，而循环神经网络（RNN）则擅长处理时间序列流量数据，捕捉攻击行为的动态演变规律。这种基于深度学习的多模态特征融合方法显著提升了恶意流量识别的准确率和鲁棒性。

除了常见的深度神经网络模型，近年来生成对抗网络（GAN）和自编码器（Autoencoder）等无监督学习技术也被引入恶意流量检测。生成对抗网络通过生成器和判别器的对抗训练，能够有效模拟正常流量与恶意流量的分布差异，从而强化检测模型对未知攻击的识别能力。自编码器则通过数据压缩与重构机制，自动发现流量的异常特征，适用于异常检测场景，能够在缺乏标注数据时实现高效识别。这些方法不仅丰富了深度学习在恶意流量识别中的技术手段，也为面对不断变化的网络威胁提供了灵活的应对策略。

深度学习模型的训练与优化同样是提升恶意流量识别性能的重要环节。大规模数据集的构建与标注成为技术实现的基础，如何平衡模型的复杂度与计算资源，避免过拟合和欠拟合，直接影响检测效果[5]。多任务学习和迁移学习技术被广泛应用，增强模型的泛化能力和适应性，使其能够在不同网络环境和攻击场景中保持高效表现。实时性方面，结合边缘计算和分布式训练技术，推动深度学习模型在实际网络环境中的部署与应用。整体来看，深度学习技术不仅改变了恶意流量识别的范式，更推动了网络安全防御向智能化、自动化的方向发展。

3 基于深度学习的恶意流量防御体系构建

基于深度学习的恶意流量防御体系的构建，是实现网络安全智能化的重要路径。该体系以深度神经网络为核心，通过对网络流量的实时分析和多层次特征提取，实现对恶意行为的精准识别与快速响应[6]。防御体系通常包括数据采集模块、深度学习检测模块和防御决策模块，形成闭环的安全防护机制。数据采集模块负责对网络流量进行全面监控，涵盖多协议、多层级的流量数据，保障信息的完整性和时效性。检测模块基于训练完善的深度学习模型，能够动态识别多样化的攻击模式，包括分布式拒绝服务攻击、入侵尝试以及隐蔽的高级持续威胁。防御决策模块则根据检测结果，自动调整网络访问控制策略、流量过滤规则，甚至触发流量隔离和流量重定向等应急措施，最大限度降低攻击对网络系统的影响。

防御体系的设计强调多层协同与动态适应能力。通过融合多种深度学习算法，构建集成模型，以提高检测的准确率和召回率。在流量数据的预处理阶段，采用特征选择和降维技术，优化模型训练效率，提升检测性能。系统引入在线学习机制，使模型能够不断更新，适应新的威胁形态，防止因环境变化导致的性能下降。深度强化学习方法被引入防御策略优化，通过智能代理不断调整防御动作，实现自适应防御能力。此外，结合边缘计算和云计算资源，实现对网络边界和核心区域的协同防护，提升系统的响应速度和扩展能力，确保在大规模网络环境下依然保持高效稳定的防御水平。

在实际应用中，基于深度学习的恶意流量防御体系展现出良好的实用价值。系统不仅能够识别已知攻击，还能通过异常检测发现未知威胁，增强了网络防护的前瞻性和主动性。多维度数据融合和多模型协同提升了检测的鲁棒性，降低了误报率，有效避免了安全运维的负担[7]。防御策略的智能化自动调整则提升了系统的灵活性和抗干扰能力，保障网络服务的连续性和稳定性。综合来看，深度学习驱动的防御体系为应对复杂多变的网络安全威胁提供了强有力的技术支撑，促进了网络安全防护从被动响应向主动防御的转变，推动

了整体防御架构的智能升级。

4 深度学习模型在恶意流量检测中的性能评估与应用效果

深度学习模型在恶意流量检测中的性能评估，是衡量其实际应用价值和技术成熟度的重要指标。评估过程通常涵盖准确率、召回率、F1 分数以及误报率等多项指标，通过多维度数据分析确保模型的综合性能。准确率反映了模型对恶意流量和正常流量区分的整体能力，召回率则重点体现对真实攻击流量的识别能力。F1 分数作为准确率与召回率的调和平均值，能够全面反映模型在平衡检测精度与覆盖范围方面的表现。误报率的控制对于保障正常业务的连续性至关重要，过高的误报不仅增加运维负担，还可能导致安全事件的忽视[8]。因而，深度学习模型需要在提升检测效果的同时，保持低误报率，实现检测系统的实用性与高效性兼顾。

应用效果方面，基于深度学习的恶意流量检测模型在多种实际网络环境中展现出优异的表现。模型通过对海量流量数据的训练和测试，成功识别了包括 DDoS 攻击、恶意扫描、数据窃取等多样化攻击行为，表现出较强的泛化能力和适应性。结合实时流量监控平台，深度学习模型能够实现对异常流量的快速定位和预警，极大提升了网络安全事件的响应速度。此外，模型的在线更新能力使其能够动态适应新出现的威胁，保障检测效果的持续稳定。多个实际案例表明，深度学习驱动的检测技术有效减少了安全漏洞的利用窗口，增强了防御体系的整体安全防护能力。

模型性能的提升离不开优化算法和硬件支持的协同发展。高性能计算平台与分布式训练架构为深度学习模型提供了强大算力保障，缩短了训练时间并支持大规模数据处理。针对网络流量的高维特征和时序特性，采用多层神经网络结构和注意力机制，显著提升了模型对复杂流量模式的识别能力。同时，模型轻量化与加速推理技术促进了在边缘设备和资源受限环境中的应用，实现了恶意流量检测的实时性和部署灵活性。整体来看，深度学习模型在恶意流量检测中的性能评估与应用效果不仅验证了其技术优势，也为网络安全防御提供了坚实的技术基础，推动了智能化检测技术的普及与深化。

5 结语

基于深度学习的恶意流量检测与防御技术，通过自动化特征提取和智能化模式识别，有效提升了网络安全防护的精准性与响应速度。面对日益复杂多变的网络攻击环境，深度学习模型展现出强大的适应能力和识别能力，为构建高效、动态的防御体系奠定了坚实基础。未来，结合先进的计算资源和优化算法，深度学习技术将在恶意流量检测领域发挥更大作用，推动网络安全向智能化、自动化方向不断迈进。

参考文献

[1] 王甜甜,鲍丽,刘圆圆,等.基于三维卷积神经网络的肺结核活动性分级 CT 辅助诊断模型的构建[J/OL].分子影像学杂志,1-7[2025-05-19].

[2] 王恩慈,卓力,李艳萍,等.基于关系网络的中医舌色苔色协同分类方法[J/OL].世界科学技术-中医药现代化,1-11[2025-05-19].

[3] 邱涛,吴倩,张艳艳.基于时谱域融合与时序自注意力增强的无监督遥感云层遮挡图像修复[J/OL].计算机系统应用,1-13[2025-05-19].

[4] 韩秀花,李辉.人工智能适应性攻击博弈与量子纠错优化模型研究[J].中国宽带,2025,21(05):154-156. DOI:10.20167/j.cnki.ISSN1673-7911.2025.05.52.

[5] 姚驰.基于人工智能的网络安全威胁检测与防御策略研究[J].中国宽带,2025,21(05):52-54.

[6] 张浩和,韩刚,杨甜甜,等.工业互联网中融入域适应的混合神经网络加密恶意流量检测[J].信息安全研究,2025,11(05):457-464.

[7] 杨春雨,吴奉燃,温涵,等.加密恶意流量检测系统[J].网络安全技术与应用,2025,(04):53-56.

[8] 田睿,张雅勤,董伟,等.机器学习在恶意加密流量检测中的应用及研究[J].电子技术应用,2025,51(04):1-11.