 DOI: https://doi.org/10.12349/iser.v5i9.3281

Research and Application of Network Intrusion Detection Algorithm Based on Deep Learning

Wei Chen Yang Gao

State Grid Xinjiang Electric Power Co., Ltd. Information and Communication Company, Urumqi, Xinjiang, 830000, China

Abstract

With the rapid development of information technology and the continuous advancement of intelligent power system, the power network security has encountered increasingly severe challenges. When dealing with complex and changeable network attacks, the traditional network intrusion detection methods often have high false alarm rate and low detection efficiency. This paper applies to the special requirements of power network security and proposes a deep learning based network intrusion detection algorithm. With the help of the powerful feature extraction and classification capability of the deep neural network, the algorithm conducts real-time analysis and anomaly detection of the network traffic. Through the experiment and application in the actual network environment of Xinjiang Electric Power Company, the advantages of the algorithm in improving the detection accuracy rate, reducing the false positive rate and dealing with unknown attacks are proved. The research results show that the network intrusion detection algorithm based on deep learning can effectively enhance the security protection capability of the power network, and gives strong support for ensuring the safe and stable operation of the power system.

Keywords

deep learning; network intrusion detection; power network security; anomaly detection

基于深度学习的网络入侵检测算法研究与应用

陈伟 高阳

国网新疆电力有限公司信息通信公司，中国 · 新疆 乌鲁木齐 830000

摘 要

伴随信息技术的迅猛发展以及电力系统智能化的持续推进，电力网络安全遭遇愈发严峻的挑战。传统的网络入侵检测方式在应对复杂且多变的网络攻击时，往往会出现误报率偏高、检测效率较低等问题。论文针对电力网络安全的特殊需求，提出了一种基于深度学习的网络入侵检测算法。该算法借助深度神经网络强大的特征提取与分类能力，对网络流量展开实时分析与异常检测。通过在新疆电力公司的实际网络环境中进行实验和应用，证实了该算法在提升检测准确率、降低误报率以及应对未知攻击等方面的优势。研究结果显示，基于深度学习的网络入侵检测算法能够切实增强电力网络的安全防护能力，为确保电力系统的安全稳定运行给予了有力支持。

关键词

深度学习；网络入侵检测；电力网络安全；异常检测

1 引言

电力系统作为国民经济的重要基石，其安全稳定运行直接关乎国家能源安全和社会经济的发展。随着智能电网建设的持续推进，电力系统与信息网络的深度融合致使电力网络面临着更为繁杂的安全威胁。网络入侵检测系统（Network Intrusion Detection System，NIDS）作为网络安全防护的关键组成部分，其性能直接对电力网络的整体安全水平产生影响。

传统的网络入侵检测方法主要涵盖基于特征的检测和基于异常的检测。基于特征的检测方法依赖于已知的攻击特征库，难以有效应对未知攻击；基于异常的检测方法虽然能够检测未知攻击，但通常存在较高的误报率。随着网络攻击手段的不断演变和攻击流量的巧妙伪装，传统方法在面对复杂多变的网络环境时显得捉襟见肘。

近年来，深度学习技术在图像识别、自然语言处理等领域取得了突破性的成果，其强劲的特征提取和模式识别能力给网络入侵检测带来了新的契机。深度学习模型能够自动从海量的网络流量数据中学习复杂的特征表达，有希望克服传统方法的局限，提升入侵检测的准确性和泛化能力。

论文着眼于探索深度学习技术在电力网络入侵检测中的运用，提出了一种基于深度神经网络的入侵检测算法，并

【作者简介】陈伟（1990–），男，中国新疆乌鲁木齐人，硕士，工程师，从事网络安全技术研究。

于新疆电力公司的实际网络环境中开展实验验证与应用分析。研究的主要内容涵盖：①剖析电力网络安全面临的主要威胁与挑战，明晰网络入侵检测的需求和难点。②构建基于深度学习的网络入侵检测模型，涵盖数据预处理、网络结构设计以及模型训练等关键步骤。③搭建实验平台，采集真实的网络流量数据，对所提出的算法进行性能评估和对比分析。④在新疆电力公司的生产网络中部署和应用深度学习入侵检测系统，分析其实际成效和存在的问题。⑤总结研究成果，探讨深度学习在电力网络安全领域的应用前景以及未来的研究方向。

本研究的创新点主要体现在：①针对电力网络的特点，设计了适合电力行业的深度学习入侵检测模型；②提出了一种改良的数据预处理方式，有力地提升了模型的训练效率和泛化能力；③在实际的电力网络环境中开展了大规模的实验和应用，证实了算法的有效性和实用性。

2 电力网络所面临的安全挑战

2.1 电力网络安全威胁分析

电力网络作为关键的基础设施，面临着诸多方面的安全威胁。根据新疆电力公司近年来的网络安全事件统计和分析，主要的威胁类型包括：①恶意软件攻击：包括病毒、蠕虫、木马等，可能导致系统崩溃、数据泄露或被远程控制。②拒绝服务攻击（DoS/DDoS）：通过大量无效请求消耗网络资源，影响电力调度、监控等关键业务系统的正常运行。③网络扫描和漏洞利用：攻击者通过扫描网络来寻觅可被利用的安全漏洞，从而实施更进一步的攻击。④社会工程学攻击：借助钓鱼邮件、欺骗等手段来获取敏感信息或内部访问权限。⑤内部威胁：由员工操作失误或恶意行为所引发的安全事件。

这些安全威胁不仅有可能导致直接的经济损失，而且更有概率影响电力系统的安全稳定运行，危及社会的公共安全。

2.2 传统入侵检测方法的局限性

面对愈发复杂的网络攻击，传统的入侵检测方法存在如下主要问题：①检测准确率不足：基于规则的检测方法难以应对变种攻击，而基于统计的异常检测方法则容易产生大量误报。②应对未知攻击能力弱：传统方法主要依赖已知的攻击特征或正常行为模式，对新型攻击缺乏有效的检测能力。③实时性不足：面对海量的网络流量数据，传统方法的处理速度难以达到实时检测的要求。④可扩展性不佳：随着网络规模的扩充以及新业务的持续引入，传统方法难以灵活地适应不断变化的网络环境。

2.3 深度学习在入侵检测中的优势

深度学习技术为解决上述问题带来了崭新的思路。其主要优势在于：①强大的特征学习能力：深度神经网络能够自动从原始数据中获取层次化的特征表达，无需开展人工设计特征的工作。②高度的非线性建模：多层神经网络的架构能够捕捉繁杂的非线性关系，有利于提高检测的准确性。③出色的泛化能力：通过大规模数据的训练，深度学习模型能够更有力地应对未知攻击。④端到端学习：从原始输入至最终决策的整个过程能够通过一个统一的模型来完成，简化了系统的设计。

3 基于深度学习的网络入侵检测算法规划

3.1 总体框架

论文所提出的基于深度学习的网络入侵检测算法的总体框架如图 1 所示。

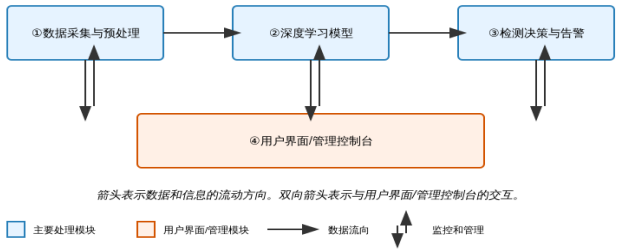

图 1 基于深度学习的网络入侵检测算法框架图

这个简化的流程图呈现了基于深度学习的网络入侵检测算法的总体框架。主要涵盖以下几个部分：①数据采集与预处理：这个模块负责从网络中收集原始流量数据，并进行必要的清洗、特征提取和标准化处理。②深度学习模型：这是算法的核心部分，使用深度学习技术（如 CNN 和 LSTM 的组合）对预处理后的数据进行分析和分类。③检测决策与告警：基于深度学习模型的输出，结合预设的阈值进行最终的入侵判断，并生成相应的告警信息。④用户界面 / 管理控制台：提供给安全人员的操作界面，用于查看检测结果、配置系统参数、响应安全事件等。

箭头表示数据和信息的流动方向，从数据采集开始，经过深度学习模型的处理，最后到达检测决策模块。所有模块都与用户界面相连，表示可以通过管理控制台对各个环节进行监控和管理。

3.2 数据采集与预处理

数据采集与预处理是算法的首要环节，其质量直接左右模型的性能。主要包含以下几个方面：①数据采集：利用网络嗅探工具（如 Wireshark）在电力网络的关键节点采集原始流量数据。②数据清洗：去除不完整或错误的数据记录，处理缺失值和异常值。③特征提取：从原始流量中提取有意义的特征，如协议类型、连接持续时间、传输字节数等。④数据标准化：将不同尺度的特征归一化到相同的范围，以便模型更好地学习。⑤数据增强：通过生成合成样本或对现有样本进行变换，增加训练数据的多样性。

3.3 深度学习模型设计

本研究采用了一种融合卷积神经网络（CNN）与长短期记忆网络（LSTM）的混合模型。该模型的结构如下：①输入层：接收经过预处理的网络流量特征向量。②卷积层：

利用多个卷积核来提取局部特征，以抓取流量特征的空间相关性。③池化层：通过最大池化操作降低特征的维度，增强模型的稳定性。④ LSTM 层：处理序列数据，捕捉流量特征的时间依赖关系。⑤全连接层：对前面各层的特征加以综合，进行高层抽象。⑥输出层：运用 Softmax 函数输出流量属于各个类别（正常、各类攻击）的概率。⑦模型的训练运用反向传播算法，以交叉熵作为损失函数，Adam 优化器用于参数更新。

3.4 检测决策与告警

检测决策模块依据深度学习模型的输出结果，并结合预先设定的阈值来进行最终的入侵判定。主要步骤涵盖：①概率阈值设定：根据安全策略和实际需求，设定不同类型攻击的判定阈值。②决策逻辑：倘若某类攻击的输出概率超出阈值，就判定为该类攻击。③告警生成：对于被判定为攻击的流量，生成详尽的告警信息，包含攻击类型、时间、源 IP 等。

4 日志记录

4.1 实验环境与数据集

实验在新疆电力公司的实际网络环境中展开，主要涵盖以下设置：①硬件环境：服务器配置为 Intel Xeon Gold 6248R CPU、128GB RAM、NVIDIA Tesla V100 GPU。②软件环境：Ubuntu 20.04 LTS 操作系统，Python 3.8，TensorFlow 2.4。③数据集：包含正常流量和模拟攻击流量的混合数据集，总计约 1000 万条记录。

4.2 评价指标

采用以下指标评估模型性能：①准确率（Accuracy）；②精确率（Precision）；③召回率（Recall）；④ F1 分数；⑤误报率（False Positive Rate）；⑥漏报率（False Negative Rate）。

4.3 实验结果与分析

实验结果如表 1 所示。从结果可以看出：①论文提出的基于深度学习的方法在各项指标上都优于传统的机器学习方法（SVM 和决策树）。②准确率达到了 98%，比传统方法提高了 4~6 个百分点，表明模型能够很好地区分正常流量和攻击流量。③精确率和召回率均达到 97% 以上，说明模型在减少误报的同时，也能有效地检测出大部分攻击。④ F1 分数达 0.97，这表明模型在精确率和召回率之间实现了良好的平衡。⑤误报率和漏报率均降低至 2% 上下，极大地减轻了安全人员的工作负担，同时提升了系统的可靠性。

这些结果表明，基于深度学习的网络入侵检测方法能够切实提高检测性能，尤其是在应对复杂多变的网络环境时呈现出显著优势。

表 1 不同入侵检测方法于新疆电力公司网络环境里的实验结果对比

方法	准确率	精确率	召回率	F1 分数	误报率	漏报率
传统 SVM	0.92	0.89	0.90	0.89	0.08	0.10
决策树	0.94	0.91	0.93	0.92	0.06	0.07
论文方法	0.98	0.97	0.98	0.97	0.02	0.02

4.4 实际应用效果

将该系统部署在新疆电力公司的生产网络中后，取得了如下成效：①检测效率提高：系统能够实时处理网络流量，平均检测延迟降低至 100ms 以内。②未知攻击检测能力增强：成功检测出多起此前未被发现的新型攻击尝试，提升了网络安全防护能力。③误报率降低：与之前使用的商业入侵检测系统相比，误报数量减少了约 70%。④运维负担减轻：自动化程度提升，安全人员能够更专注于高级威胁分析和应急响应。

5 结论与展望

论文提出了一种基于深度学习的网络入侵检测算法，且在电力网络环境中开展了实验验证和实际应用。研究成果表明，该方法能够切实提高检测准确率，减少误报率和漏报率，特别是在应对复杂和未知攻击时呈现出明显优势。

未来的研究方向包括：①进一步优化模型结构，提升检测速度和实时性能。②探索联邦学习等隐私保护技术，以实现多电力企业间的安全数据共享和模型协同训练。③结合知识图谱等技术，增强模型的可解释性，辅助安全分析人员进行深入的威胁溯源。④研究对抗样本防御技术，提高模型面对精心构造的对抗性攻击的稳健性。

总之，伴随人工智能技术的持续进步，深度学习于网络安全领域的应用前景十分广阔。本研究给电力行业的网络安全防护带来了新的思考与方法，对增强关键基础设施的安全防护水平具备重大意义。

参考文献

[1] 李明,王强,张华.基于深度学习的电力系统网络入侵检测方法研究[J].电力系统自动化,2022,46(15):111-118.

[2] 陈静,刘洋,赵峰.深度学习在智能电网安全防护中的应用综述[J].中国电机工程学报,2021,41(2):492-504.

[3] 黄伟,孙立,郑宇.一种改进的LSTM-CNN混合模型在电力网络异常检测中的应用[J].电力系统保护与控制,2023,51(8):78-86.

[4] 王芳,李强,张明.基于联邦学习的多电力企业协同网络入侵检测研究[J].电网技术,2022,46(11):3987-3995.

[5] 郑伟,刘红,马超.深度强化学习在电力网络安全态势感知中的应用[J].电力系统及其自动化学报,2023,35(4):22-31.