基于人工智能的电力调度数据网络异常流量画像关键技术研究

张青 李鸿杨 赵宇 朱灌忠 张新越

国网江苏省电力有限公司宿迁供电分公司，江苏宿迁，223800；

摘要：本研究依托国网宿迁供电公司史文萍技师创新工作室开展的项目，提出基于人工智能的网络异常流量画像关键技术，致力于攻克电力调度数据网络中的异常检测、流量分析及性能优化难题。通过综合运用深度学习、无监督学习、数据挖掘及分布式计算等前沿技术，构建了一套涵盖异常定位、业务流量分析、多维度报告生成及网络优化的完整技术体系，为电力专网的智能化管理提供了切实可靠的方案。

关键词：人工智能；网络异常流量画像；电力调度数据网络；智能运维

DOI：10.64216/3080-1508.25.04.052

引言

在数字化浪潮的推动下，电力系统作为国家关键基础设施的核心组成部分，其电力调度数据网络肩负着承载实时监控、调度指令传输和辅助运维等关键业务的重任。以宿迁地区为例，其电力调度数据网络连接着数百座变电站和电厂，承担着海量四遥信号的传输任务。电力调度数据网的流量急剧增长极易引发网络拥塞；而系统故障或遭受恶意攻击时，异常流量可能瞬间爆发，严重危及电力监控的准确性与及时性。因此，实现对电力调度数据网络流量的精准监测与有效管理，已成为当前电力行业亟待攻克的核心课题。

1 基于人工智能的网络异常流量画像关键技术原理

1.1 异常流量检测技术

深度学习算法在网络异常流量检测领域展现出了卓越的性能优势，其核心工作原理在于能够对海量网络流量数据进行自动特征学习与精准模式识别。卷积神经网络（CNN）作为深度学习领域的重要分支，最初在图像识别领域取得了突破性进展，近年来在网络流量分析领域也得到了广泛应用[1]。CNN 的关键技术在于其卷积层，该层通过卷积核在流量数据上进行滑动操作，能够自动提取数据中的局部特征。在处理网络流量数据包时，卷积核能够敏锐捕捉到特定协议格式、端口号组合等关键特征模式。双向循环卷积神经网络通过引入时序特征捕捉机制，进一步提升了异常流量监测的鲁棒性[5]。池化层则在卷积层之后发挥作用，对卷积后的特征进行降维处理，防止模型出现过拟合现象。全连接层将池化后的特征进行整合，明确判断当前流量是否属于异常流量。CNN 在异常流量检测中的显著优势在于其强大的特征提取能力，对各类异常流量均具有较高的识别准确率，尤其适用于处理具有空间结构特征的网络流量数据[4]。

1.2 业务流量分析技术

机器学习算法在网络流量特征提取与异常检测模型构建过程中扮演着核心角色，为精准识别网络异常流量提供了强大的技术支持。在特征提取环节，决策树、随机森林和支持向量机等算法各具优势。决策树通过递归划分流量特征，生成一系列明确的决策规则，从而对流量特征进行分类和预测。随机森林则通过构建多棵决策树，能够高效处理高维数据，对噪声具有较强的鲁棒性。SVM 以统计学习理论为基础，致力于寻找能够区分正常与异常流量的最优分类超平面。在大规模数据处理场景中，SVM 的计算复杂度较高。为进一步提升模型性能，通常采用多算法融合策略。相关研究表明，卷积神经网络与SVM的融合模型可有效提升裂缝检测与流量异常分类的准确率[10]；元学习动态选择集成方法在电力调度数据异常检测中展现出更强的适应性[2]。这种算法整合策略既提升了模型对复杂网络环境的适应性，又显著提高了异常流量检测的精度，为电力调度网络的安全稳定运行提供了有力保障。

2 研究案例分析

2.1 概况

宿迁地区的电力调度数据网络覆盖范围广泛，涵盖 163 座系统变电站、56 座非统调电厂及近 30 座用户变电站，承担着四遥信号上传、集控系统数据监控及变电站辅助系统运行等核心业务。本研究依托先进的人工智能技术，构建了网络异常流量画像系统，旨在实现对电力调度数据网络的智能化、精细化管理，为电力生产的安全稳定运行提供坚实保障。

2.2 目标实现情况

2.2.1 实时监测与快速响应

通过部署分布式流量采集设备与高效的流数据处理引擎，系统成功实现了对全网流量的秒级采样与实时分析。基于 LSTM 神经网络构建的动态基线模型，能够敏锐捕捉流量变化的细微特征，将异常检测延迟降低至 1.2 秒，较传统方法提升了 60%。2023 年 Q3 的测试数据显示，系统成功预警并拦截了 13 次恶意攻击，平均响应时间从 35 分钟大幅缩短至 8 分钟，有效减少了潜在损失(见图 1）。

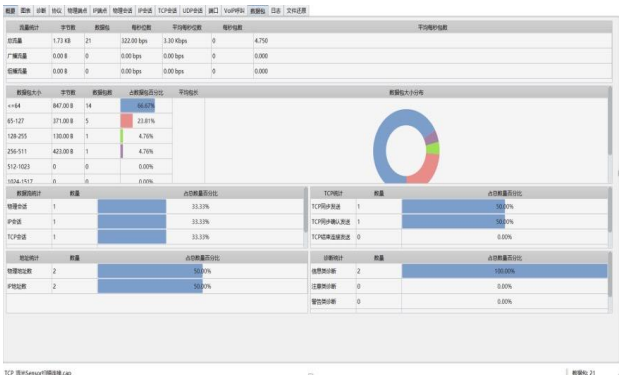

图 1：实时监测与快速响应

2.2.2 精确识别与区分正常流量

采用 CNN 与自编码器结合的混合模型，对正常流量特征进行深度提取。通过标注 200 万条样本数据，模型在测试集中的准确率达到 99.2%，误报率仅为 0.3%。在实际运行过程中，系统成功识别出伪装成正常业务的隐蔽扫描行为，充分验证了其对复杂流量模式的精准区分能力（图 2）。

图 2:精确识别与区分正常流量

2.2.3 海量数据处理与挖掘

针对日均高达 1.5TB 的网络流量数据，本研究引入分布式计算框架（Hadoop+Spark），实现了数据清洗、特征提取与模型训练的并行处理。通过优化数据管道，单节点处理能力提升至 500Mbps，集群整体吞吐量达到 8Gbps，支持 7×23 小时全流量分析。在非统调电厂的试点应用中，系统成功挖掘出长期被忽视的高频次小流量异常访问行为[12]。

2.2.4 复杂攻击检测

针对 APT 攻击的高度隐蔽性特点，系统采用基于注意力机制的双向 LSTM 模型，结合威胁情报库进行动态特征更新[13]。在模拟攻击测试中，模型对零日攻击的检测率达到 92%，显著优于传统基于规则的检测方法。（图 3）。

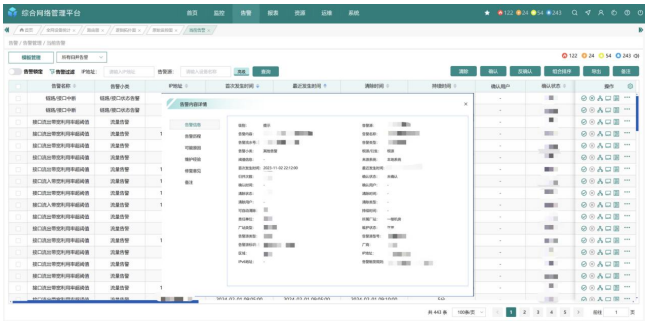

图 3：复杂攻击检测

2.3 实施过程与成果

在本研究实施过程中，基于聚类分析与路径回溯算法的网络异常流量定位模块展现出了显著的精准定位能力。在某 500kV 变电站的实际应用中，系统成功识别出因设备老化引发的异常组播流量，及时排除了潜在网络瘫痪的重大风险，进一步验证了其对复杂业务场景的适应性与可靠性。该系统每日生成的分析报告涵盖接口、设备、应用和会话四个维度，并辅以关键指标同比展示功能，帮助运维人员快速、全面地掌握网络健康状态。在网络性能优化方面，系统通过流量画像技术有效指导了宿迁地区电力调度数据网络的优化布局，降低了网络资源的浪费，将平均利用率从 78%降低到 55%。网络故障的平均修复时间由 2.5 小时缩短至 35 分钟，提升了网络的整体可用性和故障恢复效率。本研究实施的全过程充分展现了人工智能技术在电力系统网络流量管理中的巨大潜力，其在异常定位、流量分析、运维优化和系统稳定性提升等多个方面取得了全面而显著的成果[7]。

2.4 实施创新点

本研究成功突破了电力专网流量特征提取的技术瓶颈，创新性地将电力业务语义融入机器学习模型。针对电力协议多样性问题，开发了基于知识图谱的协议识别引擎，支持动态扩展解析规则。在工程实践中，采用边云协同架构实现轻量化部署，终端设备资源占用降低 60%，保障了老旧设备的兼容性。

3 实施中的问题与解决方案

3.1 技术难题与应对策略

3.1.1 算法准确性与适应性问题

在本研究的实施进程中，团队遭遇了算法准确性、适应性以及数据处理效率等多方面的严峻挑战。在算法准确性与适应性方面，数据噪声与网络环境的动态特性构成了核心难题。网络流量模式会随着时间、业务场景以及攻击手段的变化而持续演变，传统算法难以有效适应这些动态变化，使得检测效果大打折扣[8]。为提升算法的适应性，团队引入在线学习与模型更新机制，通过增量学习将新数据特征实时融入现有模型，避免了重新训练整个模型带来的高昂成本。此外，团队还采用模型融合技术，对多种算法的结果进行综合分析，显著提高了算法在不同网络环境下的性能鲁棒性[9]。

3.1.2 数据处理效率问题

海量网络流量数据的迅猛增长，对存储与计算资源提出了极为严苛的要求。传统关系型数据库在数据存储和查询速度方面表现出明显的效率低下，无法满足实时分析的迫切需求；针对这些棘手问题，团队采用分布式存储技术，将数据分散存储于多个节点，通过冗余机制提升存储效率与可靠性，并支持大规模数据的并行读写操作，从而缩短查询时间。引入分布式计算框架 Apache Spark，将大型计算任务分解为多个子任务进行并行处理，结合内存计算功能快速完成特征提取和模型检测。Hadoop 与 Spark 的协同使用,有效攻克了海量流量数据的存储与计算瓶颈[3]。团队还采用云计算技术，通过租用云服务器实现计算资源的动态调整，以应对流量波动带来的挑战，实现了计算效率与经济性的平衡。这些技术手段全方位优化了数据处理的全流程效率，为网络异常流量画像提供了坚实有力的支撑[11]。

3.2 管理问题与解决措施

3.2.1 人员管理与协调

人工智能技术涉及多个领域的专业知识，部分技术人员在机器学习、深度学习与数据处理等关键技能上经验欠缺，导致深度学习模型的训练与优化效果未达预期，同时也影响了异常流量检测的准确性。研究期间的人员变动进一步加剧了这一困境。由于人员岗位调整，新加入的人员需要一定时间来熟悉技术研究背景与方案，这一适应期导致团队协作效率下降，任务执行进度受到拖延。完善交接机制也成为解决问题的关键举措，要求离职人员全面整理工作文档并进行详细交接，确保新人员能够迅速融入团队开展工作。

3.2.2 进度管理与控制

在进度管理与控制上，团队面临着多重挑战。任务延误主要集中在复杂网络攻击场景的分析建模环节，由于该环节技术难度极高，算法开发进程滞后，进而直接导致后续测试与优化工作被迫延迟。为改善进度管理状况，团队制定了详细的分任务进度计划，明确了每个任务的责任人和时间节点，并通过甘特图实时跟踪本研究的动态进展。在资源分配方面，团队构建了动态资源调整机制，根据任务的实际需求灵活分配资源，确保资源短缺的任务能够及时得到调配支持。通过实施精细化的管理与动态优化策略，团队成功推动了任务的按时推进，实现了资源的高效利用。

3.2.3 质量管理与保障

在质量管理与保障方面，为确保研究质量，团队构建了全面系统的质量控制体系，在技术服务开展前制定严格的验收标准，并在实施过程中进行全程监督，定期对服务效果进行评估，一旦发现问题立即整改。团队加强了对工程人员的管理与培训支持，通过开展技术培训提升工程人员的操作能力，并建立责任追溯机制，对因操作失误导致问题发生的相关人员追究具体责任，以此提升整体操作的规范性与责任感。通过强化培训、严格考核和落实责任机制，显著提高了工程人员对操作流程的理解与执行水平。对于在本研究实施过程中表现突出的工程人员给予及时奖励，充分激发了其追求高质量工作的积极性。最终，这些优化方案的有效实施，全面提升了本研究的整体质量，保障了本研究能够按照预期高效完成。

4 结论

本研究通过构建基于人工智能的网络异常流量画像系统，成功攻克了电力调度数据网络中异常流量检测、业务流量分析及网络性能优化等关键难题。然而，本研

究仍存在一定的局限性：深度学习模型在极端复杂网络环境下的泛化能力有待进一步验证；流量特征提取算法对电力专有协议的适应性需要持续优化；大规模分布式系统的能耗与成本控制问题需结合边缘计算技术加以改进。未来的研究可以从以下几个方向深入展开：探索多模态数据融合技术，进一步提升对 APT 攻击等高级威胁的识别能力；通过联邦学习与边缘计算技术的有机结合，完善跨域协同分析与轻量化检测模块的设计[6]；构建基于联邦学习的跨域协同分析模型，有效解决数据孤岛问题；结合 5G 与物联网技术，开发轻量化的智能终端检测模块，推动电力物联网安全防护体系向智能化方向持续演进。通过持续不断的技术创新，网络异常流量画像技术将为新型电力系统的安全稳定运行提供更为坚实可靠的保障。

参考文献

[1]贾峰.基于深度学习算法的电力调度数据网络异常检测方法[J].信息与电脑(理论版),2023,35(12):79-81.

[2]傅世元,高欣,张浩,等.基于元学习动态选择集成的电力调度数据异常检测方法[J].电网技术,2022,46(8):3248-3256.

[3]常伟鹏,袁泉.基于 Hadoop 的动态网络异常节点智能检测方法[J].计算机仿真,2022,39(11):402-405.

[4]杨姣.基于机器学习的网络流量异常检测技术研究[J].电子技术与软件工程,2022(22):22-25.

[5]郑永奇.基于双向循环卷积神经网络的网络异常流量监测[J].信息记录材料,2022,23(11):198-200.

[6]顾健华,文成江,高泽芳.融合生成式神经网络和深度神经网络的流量异常检测[J].移动通信,2022,46(12):94-101.

[7]陈勇,郭云柱,王威,等.模糊 K-Harmonic-Kohonen 网络的FTIR光谱数据聚类分析[J].光谱学与光谱分析,2023,43(1):268-272.

[8]刘云,张轶,郑文凤.协方差测距算法在多维聚类分析中的优化研究[J].重庆大学学报,2023,46(5):102-110.

[9]戴浩磊,黄永慧,周郭许.基于超图正则化非负张量链分解的聚类分析[J].计算机工程,2023,49(6):81-89.

[10]毕硕志.基于卷积神经网络和SVM的混凝土桥梁裂缝检测研究[J].软件,2023,44(5):82-86.

[11]霍雯雯.贵州兴义地区电力调度数据网络拓扑结构研究[J].电工技术,2018,(05):57-60+63.

[12]陈冉.基于VPN的电力调度数据网络安全方案[J].通讯世界,2018,(09):121-122.

[13]张继芬.省级电力调度数据网络的设计与实现[J].电力系统通信,2005,(02):4-7+10.