人工智能技术在通信传输网络异常检测中的应用

张志敏
杭州赋信科技有限公司　浙江　杭州　310015

摘　要：随着通信传输网络规模扩大与复杂度提升，带宽异常、链路故障等问题频发，传统检测方法难以满足需求。本文分析了通信传输网络核心架构（骨干网、接入网、协议层）与异常诱因（攻击、老化等），再阐述监督、无监督、深度学习、强化学习在异常检测中的核心技术原理，最后落地四类技术的具体应用（如基线构建、轻量化部署）。研究表明，AI技术可提升检测精度与实时性，为通信网络稳定运行提供技术支撑。

关键词：人工智能技术；通信传输；网络异常检测；应用

引言：通信传输网络是数字经济的基础设施，其骨干网、接入网与协议层的协同运行保障数据高效传输。但网络攻击、设备老化等因素导致带宽占用异常、数据丢包等问题频发，传统阈值法、规则法存在误报率高、难测未知异常的缺陷。当前，AI技术凭借数据处理与自适应能力，成为突破检测瓶颈的关键。

1 通信传输网络概述与异常类型

1.1 通信传输网络的核心架构

通信传输网络的核心架构包含三个关键层级：（1）骨干网作为网络核心承载层，承担跨区域、大容量的数据传输任务，是网络整体连通性的基础；（2）接入网作为用户接入通道，负责将终端设备与骨干网衔接，实现用户数据的接入与分发；（3）传输协议层作为逻辑保障层，通过统一的通信规则，规范数据在不同设备、层级间的传输格式与流程，确保数据传输的有序性与兼容性，三者协同构成完整的传输网络功能体系。

1.2 通信传输网络常见异常类型

通信传输网络常见异常可分为四类：（1）带宽异常占用表现为网络带宽资源被非预期占用，导致正常业务带宽不足；（2）链路故障指网络传输通路出现中断或性能劣化，影响数据传输的连续性；（3）数据丢包是数据在传输过程中出现部分数据包丢失，导致接收端数据不完整；（4）协议异常则是网络设备在执行通信协议时出现偏差，破坏数据传输的规则性，四类异常均会影响网络正常运行。

1.3 异常产生的关键诱因

异常产生的关键诱因包括四类因素：网络攻击是外部恶意行为对网络的干扰，破坏网络安全与稳定性；设备老化是网络硬件设备长期运行后性能下降，导致传输能力减弱或故障；流量波动是网络业务流量出现非预期的激增或骤降，造成网络负载不均衡；配置错误是人为对网络设备参数设置不当，违背网络运行规则，四类诱因分别从外部攻击、硬件状态、业务负载、人为操作层面引发网络异常[1]。

2 人工智能技术在异常检测中的核心技术原理

2.1 监督学习技术及其异常检测适配性

监督学习以标注样本为核心驱动力，通过学习正常与异常数据的特征映射关系实现检测。逻辑回归基于线性回归框架引入sigmoid函数，将特征组合转化为异常概率值，适配数据分布近似线性、需快速输出检测结果的场景，但其对非线性特征的捕捉能力有限。支持向量机通过核函数将低维数据映射至高维空间，构建最优分离超平面区分异常与正常样本，在高维稀疏数据场景中适配性较强，可通过核函数选择平衡线性与非线性检测需求。决策树基于信息增益或基尼系数递归划分特征空间，形成可解释性强的检测规则，能直接输出特征重要性排序，适配需明确异常判定依据的场景。随机森林集成多棵决策树，通过袋外数据验证降低过拟合风险，提升对复杂数据模式的拟合能力，在噪声数据较多的场景中适配性更优，且能通过投票机制降低单一模型的误判率。

2.2 无监督学习技术的异常识别逻辑

无监督学习依托数据内在分布规律实现异常识别，无需依赖标注样本。K-均值聚类通过迭代优化簇中心，将数据划分为多个密集簇，将偏离所有簇中心的样本判定为异常，核心逻辑是基于“异常数据属于稀疏分布”的假设，但其检测效果受簇数量预设与初始中心选择影响。孤立森林通过随机划分特征构建多棵孤立树，异常样本因特征特殊会更快被孤立到叶子节点，通过路径长度量化异常程度，核心逻辑是利用异常数据的“易孤立性”，适配高维数据且检测效率较高。DBSCAN基于密度定义核心对象、可达关系与连通区域，将低密度区域的样本识别为异常，核心逻辑是“正常数据构成密集簇，异常数据处于低密度

区”，可自动识别任意形状的簇结构，无需预设簇数量。自组织映射通过二维网格拓扑映射高维数据，将相似数据映射至邻近节点，异常数据因缺乏相似样本会映射至网格边缘或孤立节点，核心逻辑是基于数据的拓扑相似性，兼具降维与异常识别能力。

2.3 深度学习技术的特征提取与检测机制

深度学习通过多层神经网络自动提取数据深层特征，实现端到端异常检测。卷积神经网络（CNN）通过卷积层的局部感受野与权值共享提取局部空间特征，池化层实现特征降维与鲁棒性增强，在处理含空间结构的数据时，可自动捕捉层次化特征，检测机制是通过比对特征分布差异识别异常，无需人工设计特征。长短期记忆网络（LSTM）通过输入门、遗忘门、输出门的门控机制，选择性保留与更新时序信息，解决传统循环网络的梯度消失问题，可捕捉长周期时序依赖特征，检测机制是基于正常时序模式的预测误差判定异常，适配时序性强的数据场景。自编码器（AutoEncoder）由编码器与解码器构成，编码器将高维数据压缩至低维潜在空间，解码器重构原始数据，核心机制是利用异常数据的重构误差显著高于正常数据的特性实现检测，通过调整网络深度与宽度平衡重构精度与检测效率，适配高维数据场景。

2.4 强化学习在动态网络异常自适应检测中的应用原理

强化学习通过智能体与环境的持续交互优化检测策略，适配动态网络环境。其核心框架包含状态空间、动作空间与奖励函数三大要素：状态空间将网络运行参数量化为可感知的向量，通过增量更新机制实时反映网络动态变化；动作空间定义智能体的检测行为（如调整检测阈值、切换检测模式），实现检测策略的灵活调整。奖励函数基于检测目标设计，对正确识别异常、降低误报率、缩短检测延迟等行为赋予正向奖励，对漏检、误判等行为赋予负向惩罚，引导智能体学习最优策略。通过经验回放机制存储历史交互数据并随机采样训练，避免短期数据波动导致的策略震荡；采用探索-利用策略在稳定检测与新模式探索间平衡，使智能体能自适应网络拓扑变化、流量波动等动态场景，持续优化检测性能[2]。

3 人工智能技术在通信传输网络异常检测中的具体应用

3.1 监督学习在通信传输网络异常检测中的具体应用

（1）标注样本的构建与维护：通过流量探针、设备日志采集器等工具，定向获取带宽占用、链路状态、协议交互等正常与异常场景的网络数据；依据带宽超阈值、链路中断信号、协议字段异常取值等预设规则，结合人工复核与机器辅助标注完成样本标注；建立动态维护机制，定期纳入新场景异常数据、剔除过时样本，确保样本库与当前网络环境匹配。（2）特征工程的实际落地：从时域提取数据均值、方差、波动周期，从协议维度提取字段取值分布、交互频次、报文长度等特征；采用相关性分析、方差分析筛选特征，剔除设备标识等冗余信息；对筛选后特征进行标准化处理，将值映射至[0,1]等统一区间，消除量纲差异，形成模型输入的标准化特征集。（3）模型的部署与适配：按场景实时性需求选模型，离线异常回溯用随机森林、梯度提升树等精度优先模型，实时带宽监控用逻辑回归、轻量级支持向量机等速度优先模型；通过模型封装转化为可调用接口，与网络监控系统对接，实现“数据输入-模型推理-结果输出”闭环；针对区域网络拓扑差异，微调支持向量机核函数等参数，适配局部网络特性。（4）检测结果的后处理：用规则过滤机制二次校验结果，剔除短期瞬时带宽波动等误判；按异常影响严重程度建立分级机制；将分级结果同步至运维平台，触发对应响应。

3.2 无监督学习在通信传输网络异常检测中的具体应用

（1）正常行为基线的构建：无标注样本场景下，采集连续72小时无异常的流量、设备状态等历史数据；用统计分析（计算均值、标准差、概率分布）或K-均值、DBSCAN等聚类算法建模，确定正常行为特征范围与分布规律，形成基线；每周更新基线，结合近期正常数据调整参数，适配流量波动、设备配置微调等变化。（2）未知异常的检测执行：实时数据与正常基线比对，计算欧氏距离、余弦相似度等偏离度；基于历史正常数据设定偏离度阈值，超阈值则判定为异常；通过聚类分析确定异常聚集特征，区分单个设备临时故障的“孤立异常点”与区域链路批量异常的“集群异常”，为排查提供方向。（3）多源异构数据的适配处理：针对设备日志文本、流量监测数值、协议报文二进制等异构数据，将文本转词向量、二进制解析为字段特征，实现特征对齐；用拼接融合、加权融合整合多源特征为统一向量输入模型；训练时采用加权损失函数，赋予设备状态数据等核心数据源更高权重，提升模型关注度。（4）检测阈值的动态优化：建立阈值调整反馈机制，定期统计误报、漏报比例；误报率高则提高阈值减少轻微偏离判定，漏报率高则降低阈值增强敏感度；结合业务高峰期流量增长等变化临时调阈值，避免业务波动导致误判[3]。

3.3 深度学习在通信传输网络异常检测中的具体应用

（1）时序网络数据的异常检测：用LSTM、GRU等

时序模型处理流量、延迟、丢包率等数据；将连续时序划分为5分钟/窗口等固定长度样本，输入模型学习正常时序规律；检测时模型预测实时数据，计算预测值与实际值误差，超阈值则判定为异常，识别流量突增、延迟骤升等时序异常。（2）高维网络特征的异常识别：用AutoEncoder、VAE等模型处理多协议层、多设备的高维特征；编码器将高维数据压缩至低维空间，解码器重构数据，以“重构误差”为判定依据；训练时以最小化重构误差学习正常特征，检测时若实时数据重构误差远超正常范围，判定为异常，识别协议字段细微异常组合等隐藏问题。（3）多协议层协同检测：采用多输入CNN-LSTM等多分支模型，针对物理层、数据链路层、网络层、传输层分别设置特征提取分支，提取信号强度、端口交互等关键特征；特征融合层整合分支特征输入分类/回归模块；检测时同步分析各层数据，既识别单一协议层异常，也捕捉物理层信号干扰导致传输层丢包等跨层异常，实现多维度覆盖。（4）模型的轻量化部署：针对基站、接入交换机等边缘节点计算限制，用模型剪枝剔除权重绝对值小于阈值的冗余神经元与连接，量化将32位浮点数参数转8位整数，降低存储与计算开销；轻量化模型部署至边缘节点实现本地检测，减少核心节点带宽消耗；建立边缘-核心节点同步机制，核心节点定期下发优化参数，保障边缘模型检测能力。

3.4 强化学习在通信传输网络异常检测中的具体应用

（1）动态网络环境的适配检测：网络拓扑变化、业务流量波动场景下，构建强化学习智能检测体（Agent）；定义链路数量、带宽利用率、设备负载等为状态空间，“继续监测”“判定异常”“调整参数”为动作空间；Agent通过与环境交互学习最优动作，以正确检测正向奖励、误判负向惩罚的奖励函数优化策略，实现动态适配。（2）多目标检测的优化平衡：用多目标强化学习模型满足“高准确率”“低误报率”“快实时性”需求；设计多维度奖励函数，对准确检测、减少误报、缩短延迟分别设奖励项，按运维优先级赋权（如核心链路检测中“低误报率”权重高于“实时性”）；Agent权衡奖励项调整策略（核心链路增二次校验降误报，普通链路简化步骤提速度），实现多目标平衡。（3）异常检测策略的自更新：建立在线学习机制，Agent实时接收误报、漏报等检测反馈并更新策略；用经验回放存储历史交互数据，随机采样训练避免短期数据导致策略震荡；设置连续3次误报、拓扑重大调整等触发条件，触发后Agent重新学习最优策略，确保适配当前网络，减少人工干预。（4）与网络运维的协同联动：将强化学习模型与网络运维系统对接，智能体在判定异常后，不仅输出异常结果，还能根据异常类型与严重程度，生成初步的运维建议；运维人员对建议的执行结果反馈至智能体，作为奖励函数的补充依据；通过这种协同机制，智能体逐步学习运维经验，优化异常判定与建议生成的准确性，形成“检测-运维-反馈-优化”的闭环[4]。

结束语：本文围绕通信传输网络异常检测需求，完整呈现了AI技术的应用体系：从网络架构与异常诱因的基础分析，到四类AI技术关键技术的拆解，再到各技术在样本处理、基线构建、时序检测等场景的落地实践，形成了“理论-技术-应用”的闭环。相关技术已在边缘节点部署、多协议层协同检测中验证有效性，可降低误报率并提升实时性。

参考文献

[1]王爱兵.人工智能技术在通信传输网络异常检测中的应用[J].信息记录材料,2025,26(8):86-88.

[2]邓松君,欧炳强.人工智能技术在通信网络故障诊断中的应用[J].移动信息,2025,47(6):25-26+35.

[3]卢艳飞.基于人工智能的云计算通信网络安全传输控制技术研究[J].新潮电子,2025(20):184-186.

[4]何鲤军.基于人工智能的云计算通信网络安全传输控制技术[J].通信电源技术,2024,41(18):161-163.