doi:10.3969/j.issn.1001-4616.2025.05.010

基于混合神经网络的电力通信系统数据异常检测方法

王春迎[1],安致媛[1],赵　斌[2],李　宁[2]

(1.国网河南省电力公司信息通信分公司,河南 郑州 450000)
(2.南京师范大学计算机与电子信息学院/人工智能学院,江苏 南京 210000)

[**摘要**]　电力通信系统中的数据异常检测面临诸多严峻的挑战. 一方面,系统的数据维护日志通常包含大量专业术语,且格式复杂多样,传统的通用日志解析方法难以精准理解其深层语义信息. 另一方面,系统运行产生的日志数据具有显著的时序关联性与空间依赖性,现有方法对时空特征的协同建模能力不足,难以识别复杂的异常模式. 此外,若数据异常未能被及时发现和处理,可能对电力通信网络的稳定性和服务质量造成不利影响,危及电力系统的稳定运行. 因此,开发一种准确且高效的日志异常检测方法对于保障电力通信系统的运行安全具有重要意义. 本文提出了一种基于混合神经网络的日志异常检测方法,采用改进的 Drain3 算法进行日志解析,结合 BERT 模型与 IDF 加权机制进行特征表示,使用 Mogrifier LSTM 与 CNN 的混合模型进行异常检测. 实验结果表明,该方法在真实电力通信系统数据集上取得了优异的性能表现,对于日志异常检测的理论研究与工程实践具有一定的参考价值.

[**关键词**]　电力通信系统,日志异常检测,Mogrifier LSTM,CNN
[**中图分类号**]TM912　[**文献标志码**]A　[**文章编号**]1001-4616(2025)05-0085-08

Anomaly Detection Method for Power Communication System Data Based on a Hybrid Neural Network

Wang Chunying[1],An Zhiyuan[1],Zhao Bin[2],Li Ning[2]

(1.State Grid Henan Electric Power Company Information & Communication Branch,Zhengzhou 450000,China)
(2.School of Computer and Electronic Information/School of Artificial Intelligence,Nanjing Normal University,Nanjing 210000,China)

Abstract:Anomaly detection in power communication systems poses significant and unique challenges. On one hand,the maintenance logs of the system often contain numerous domain-specific terms and exhibit complex,heterogeneous formats,making it difficult for traditional log parsing methods to accurately capture their underlying semantic information. On the other hand,the log data generated during system operation is characterized by pronounced temporal correlations and spatial dependencies,yet existing approaches struggle to effectively model these spatiotemporal features,limiting their ability to identify complex anomaly patterns. Moreover,failure to promptly detect and address data anomalies may adversely affect the stability and service quality of the power communication network,thereby compromising the stable operation of the power system. Consequently,developing an accurate and efficient log anomaly detection method is critical to ensuring the operational security of power communication systems. This paper proposes a log anomaly detection method based on a hybrid neural network. The method employs an enhanced Drain3 algorithm for log parsing,integrates the BERT model with an IDF weighting mechanism for feature representation,and utilizes a hybrid model combining Mogrifier LSTM and CNN for anomaly detection. Experimental results demonstrate that the proposed method achieves superior performance on a real-world power communication system dataset,offering valuable insights for both the theoretical advancement and practical implementation of log anomaly detection in power communication systems.

Key words:electric power communication system,log anomaly detection,mogrifier LSTM,convolutional neural network

收稿日期:2025-06-30.
基金项目:国家自然科学基金资助项目(41971343,62406145).
通讯作者:赵斌,博士,副教授,研究方向:人工智能、大数据分析与挖掘、云计算. E-mail:zhaobin@njnu.edu.cn

国家电网公司新一代通信管理系统(以下简称 SG-TMS2.0)完成了通信实时监视、资源管理、运行管理三大类六项基础功能应用建设. 然而,在大量新能源厂站接入的背景下,电网及其通信网的复杂性和规模剧增,传统的人工数据维护方式易产生误录且难以校核,不仅为电力通信网络的稳定运行埋下安全隐患,还严重阻碍了电力通信系统智能化转型[1]. 因此,突破数据维护日志智能化分析技术实现异常数据检测已成为电力行业及通信专业发展的迫切需求[2].

在日志异常检测领域,学术界已开展了广泛的研究探索[3-4]. 在日志解析方面,传统方法主要包含三类:基于规则的方法能够有效处理已知格式的日志,但适应性较差;基于聚类的方法(如 IPLoM[5] 和 LKE[6])具备一定的自适应能力,但难以准确理解专业术语的语义;基于模板生成的方法(如 Drain[7] 和 Spell[8])通过自动识别日志模式生成模板,具有较强的灵活性. 在异常检测方面,早期研究主要集中在统计分析和传统机器学习两类方法:前者依赖规则分类和静态特征分析,后者则需先进行人工特征提取,再结合监督学习算法进行建模[9-10]. 近年来,随着深度学习技术的发展,研究者开始使用循环神经网络(RNN)、长短期记忆网络(LSTM)[11] 和卷积神经网络(CNN)等模型进行异常检测,取得了准确率的显著提升. 典型工作如 DeepLog[12] 采用双层 LSTM 实现了对日志模板序列和参数变量的异常检测,nLSALOG[13] 引入自注意力机制,增强了模型对序列依赖关系的捕捉能力,LogAnomaly[14] 创新性地运用词嵌入技术,提升了模型对未知异常的泛化能力. 然而,在电力通信系统这一特殊场景下,现有方法仍存在专业术语理解不足、时空特征表征能力有限等问题,难以满足日益增长的智能化需求[15].

电力通信系统中的日志异常检测面临独特且严峻的挑战. 一方面,系统日志通常包含大量专业术语,且格式复杂多样,传统的通用日志解析方法难以精准理解其深层语义信息. 另一方面,系统运行产生的日志数据具有显著的时序关联性与空间依赖性,现有方法对时空特征的协同建模能力不足,难以识别复杂的异常模式. 此外,若日志异常未能被及时发现和处理,可能对电力通信网络的稳定性和服务质量造成不利影响,危及电力系统的稳定运行. 因此,需要研究开发更加精准高效的日志异常检测方法.

为了应对上述挑战,本文提出了一种基于混合神经网络的日志异常检测方法,其核心贡献如下:(1)提出了一种面向电力通信系统的日志解析方案,采用改进的 Drain3 算法显著提升了对专业术语的理解能力和解析精度;(2)构建了一个结合 BERT 模型与 IDF 加权机制的特征表示体系,解决了传统方法在语义理解上的浅层化问题,增强了模型对电力通信系统日志中复杂语义信息的捕捉能力;(3)设计了一种 Mogrifier LSTM 与 CNN 相结合的网络架构,实现了对日志序列中复杂时空特征的有效建模. 该方法在真实电力通信数据集上进行实验,精确率和召回率分别达到 95.13%和 92.86%,显著优于其他方法. 实验结果表明,本文方法能够为电力通信网络的智能化运维提供有力支撑.

1 基于混合神经网络的日志异常检测方法

图 1 展示了某电力通信系统中两位操作员的日志异常检测示例. 该示例截取自 2024 年 4 月 15 日的系统运行日志,清晰呈现了两种典型的异常操作模式. 本文以两种典型案例作为验证,后续通过进一步数据标注可实现全类型日志异常检测. 通过案例实证,不仅验证了本研究提出的异常检测方法的有效性,也凸显了电力通信系统日志异常检测在保障系统安全运行方面的重要作用.

本研究提出的日志异常检测方法共包含以下 4 个核心步骤:

(1)日志采集:从 SG-TMS2.0 获取运行期间生成的日志数据.

(2)日志解析:引入基于 Drain3 算法的日志解析方法,将收集到的原始日志数据被转换为结构化格式.

(3)特征表示:构建结合 BERT 模型与 IDF 加权机制的特征表示体系,将解析后的日志数据转换为可用于日志异常检测的特征向量.

(4)异常判别:设计 Mogrifier LSTM 与 CNN 相结合的网络架构,对日志数据进行时空建模,以检测异常的日志事件,从而揭示潜在的系统问题或故障.

1.1 日志采集

本研究选取 SG-TMS2.0 在某省的实际运行日志作为研究对象,所采用的数据集包含 76 275 条日志记录,时间跨度覆盖完整的 12 个月运行周期,涵盖了系统在不同季节、不同负载条件下的运行状态. 该数据

日志异常类型示例

异常类型	异常描述
A	新增的站点没有关联光缆或光缆段
B	新增的光缆段没有关联的光缆
C	新增光路没有关联的配线链接
D	采集到新增通道链路，但无法找到对应方式单
E	新采集设备机框未关联机柜
F	同一条线路应该有至少2条以上保护业务，3条以上保护通道
G	光路删除后对应的配线连接未清楚
H	光缆段纤芯未关联光缆或一个纤芯属于多个光缆
…	…

日志异常操作示例

时间	操作日志	状态
9:07	简称属性由"01"值更改为"02"值	正常
9:08	光缆新增	正常
9:10	光缆段新增	异常B
9:11	光缆新增	正常
9:13	光缆段新增	正常

日志异常操作示例

时间	操作日志	状态
17:25	描述属性由"a1"值更改为"b1"值	正常
17:26	通道链路新增	异常D
17:29	添加与通道链路关联：通道链路【001】	正常
17:34	使用状态属性由"预占"值更改为"可用"值	正常

图 1　日志异常示例图

Fig. 1　Log anomaly illustration

集具有以下特点：

(1)数据来源权威:作为国家电网公司核心业务系统之一,SG-TMS2.0 的运行日志具有较高的参考价值和典型性;

(2)样本规模合理:76 275 条日志记录的规模确保了研究结果的统计显著性,为模型的训练和测试提供了充分的数据支撑;

(3)时间跨度完整:全年度的数据采集周期涵盖了系统在不同时间维度(日、周、月、季)的运行特征,保证了研究结果的时效性和普适性.

本研究建立在真实、可靠的数据基础之上,研究成果具有直接的工程应用价值,可为电力通信系统的运维管理提供有效的技术支撑.

1.2　日志解析

日志解析的主要目标是将原始日志消息分离为正则消息部分和特征消息部分,为异常检测提供结构化的输入数据. 解析的准确性对后续的检测性能具有重大影响. 研究表明,在数据解析过程中即使只有4%的误差,也可能导致异常检测阶段的性能显著下降,降幅可达 10 倍之多[16]. 因此,如何有效解析日志文件成为一个关键问题.

在电力通信系统中,日志解析面临着一系列独特的挑战. 首先,电力通信系统的日志通常包含复杂的中英文混合内容,增加了理解和解析的难度;其次,相较于普通日志,电力通信系统的日志还存在着格式复杂、术语众多等特点. 这要求解析方法必须具备高度的专业性和适应性,传统的日志解析方法难以直接应用. 例如,常见的基于正则表达式的日志解析方法在处理多语言混合和非结构化内容时,往往面临规则泛化能力弱、匹配准确率低等问题. 而基于聚类的日志模板生成方法虽具备一定的自适应能力,但在面对电力通信日志高度专业化、语义复杂性强的特点时,易产生模板误聚类现象,进而影响后续异常检测的准确性与稳定性.

针对电力通信系统日志专业术语密集、格式异构及流式数据处理需求,本文引入改进的 Drain3 算法,实现自适应日志解析. Drain3 是对经典 Drain 算法的扩展,其核心机制包括层次化聚类和动态模板更新,使其能够实时适应新出现的日志模式. 通过高效的数据结构和异步处理能力,Drain3 在保证内存效率的同时,显著提高了解析速度和精度. Drain3 的核心思想与 Drain 相似,均基于一个基本假设:由同一日志模板生成的日志在分词后的词数量是相同的. 在这一假设下,Drain3 构建了一棵解析树(Parse Tree),该树由

日志长度、前缀单词和日志模板组成. 其中第一层是根节点(Root Node);第二层代表分词后的词数,即日志的长度(Length);从第三层开始的各层,存储日志模板中的前缀单词;最底层的日志组(Log Group)由具有相同前缀单词的日志模板组成.

针对电力通信系统日志中普遍存在的中英文混杂问题,本文通过预先配置一些正则表达式,将匹配到的字符串替换为特定符号,从而提高日志解析的一致性和准确性. 以预处理好的数据为例,“操作员 A for 起始纤芯属性由 028 值更改为 029 值;终止纤芯属性由 028 值更改为 029 值”可以替换为“操作员 * for 起始纤芯属性由 * 值更改为 * 值;终止纤芯属性由 * 值更改为 * 值”,后者是一个修改完成的正则表达式.

在 Drain3 的解析树中,每个叶子节点可能关联多个日志组(Log Group). 每当有新日志到来时,需要从这些日志组中选择一个最合适的作为模板. 假设新日志分词后的序列为 $seq1$,而某个日志组中的日志事件分词后的序列为 $seq2$,可以计算 $seq1$ 和 $seq2$ 的相似度 $simSeq$.

$$simSeq=\frac{\sum_{i=1}^{n} equ(seq_1(i),seq_2(i))}{n}, \tag{1}$$

$$equ(t_1,t_2)=\begin{cases}1 & \text{if } t_1=t_2\\ 0 & \text{otherwise}\end{cases}. \tag{2}$$

在上述公式(1)中,n 表示 $seq1$ 中单词的数量. 由于 $seq1$ 和 $seq2$ 的单词数量相同,可以比较相同索引位置的单词 t_1 和 t_2 是否相同. 如果相同,则 $equ(t_1,t_2)$ 的值为 1,否则为 0. 从多个 $simSeq$ 值中选择最大的一个,如果该值不小于阈值 sim_th,则将其对应的日志组(Log Group)视为与新日志最匹配的日志模板.

1.3 特征表示

针对电力系统日志中专业术语密集以及关键事件低频高敏的特性,本文采用 MLog[17] 中基于语义的特征表示方法进行分析,主要包括以下两个方面:

(1)基于预训练的 BERT[18] 模型的语义表示:电力通信系统日志通常包含大量专业术语和特定设备名称,使用 BERT 可以更好地理解这些专业词汇的语义,特别是在处理未见过的新设备或事件时表现出良好的泛化能力.

(2)事件 IDF 加权机制:在电力通信系统中,某些事件(如设备故障、电网波动)虽然发生频率较低,但往往具有重要的业务意义和安全影响. 利用 IDF 加权机制可以提升这些低频高敏事件在特征表示中的权重,从而增强模型对异常事件的识别与响应能力.

对于事件 e_i,根据公式(3)计算其 IDF 权重:

$$w_{idf}(e_i)=\log\left(\frac{\sum_{i=1}^{n} count(e_i)}{count(e_i)}\right), \tag{3}$$

其中,$count(e_i)$ 表示聚合日志中事件 e_i 的出现次数. 该机制通过权重计算赋予低频高敏事件更高的权重,符合电力通信系统日志中低频高风险事件主导运维安全的领域特性. 为了避免 IDF 权重范围过大对最终语义向量计算的影响,使用最大最小归一化方法对 IDF 权值进行归一化,如公式(4)所示.

$$w_{nor-idf}(e_i)=\mu(max-min)+min, \tag{4}$$

其中,归一化参数 μ 由公式(5)给出:

$$\mu=\frac{w_{idf}(e_i)-IDF_{\min}}{IDF_{\max}-IDF_{\min}}. \tag{5}$$

其中,$IDF_{\min}$ 和 $IDF_{\max}$ 分别为 IDF 权重的最小值和最大值,max 和 min 分别为预定义区间的上限和下限.

1.4 异常判别

针对电力通信系统日志强时序关联性(如跨设备告警链式触发)与空间拓扑依赖性(如区域站点配置耦合)的核心特征,本文引入了一种基于日志模板语义信息和混合神经网络的日志异常检测方法 MLog. 该方法通过构建基于 Mogrifier LSTM 与卷积神经网络(CNN)的混合神经网络架构,实现了对电力系统日志序列中时空特征的协同建模,有效提升了异常检测的准确性与鲁棒性.

Mogrifier LSTM 是一种改进的长短期记忆网络,在传统 LSTM 的基础上引入了状态交互机制,使得输

入信息能够在隐藏状态与细胞状态之间反复交换,从而增强模型对长期依赖关系的建模能力. 对于电力通信系统的日志数据而言,其存在大量跨设备、跨时间点的告警传播现象,而 Mogrifier LSTM 能够更准确地刻画此类链式触发行为的时序演变过程,从而提高对潜在异常事件的预测与识别能力.

首先,使用 Mogrifier LSTM 对电力系统日志序列进行时序建模,在 Mogrifier LSTM 提取到全局时序特征后,进一步将隐藏层输出矩阵 H 输入到 CNN 层,利用其滑动窗口机制对时序向量进行局部特征提取. CNN 可以自动识别日志中重复出现的异常模式片段,尤其适用于捕捉电力通信系统中由于区域站点配置耦合导致的局部异常聚集现象. CNN 的输出经过全连接层映射到二维空间,如公式(6)所示:

$$\text{output}_T^Z = W * n_T^h + b, \tag{6}$$

最终,通过 softmax 函数生成概率分布,作为异常检测结果,如公式(7)所示:

$$pre = \text{softmax}(\text{output}_T^Z). \tag{7}$$

综上所述,Mogrifier LSTM 与 CNN 的混合建模策略充分考虑了电力通信系统日志的典型特征:Mogrifier LSTM 能够有效建模日志序列中的时序依赖关系,特别适用于跨设备之间的告警传播与连锁反应;CNN 则能够挖掘日志中的局部共现模式,有助于识别因站点间配置耦合或资源共享引起的区域性异常聚集现象;两者的结合不仅增强了模型对复杂日志行为的理解能力,还提升了其在面对低频高敏事件时的泛化性能,为电力通信系统的安全运行和故障预警提供了重要支持.

2 实验与结果分析

2.1 数据集与评价指标

本研究以 SG-TMS2.0 的日志数据作为分析对象. 数据集包含 76 275 条日志记录,覆盖 12 个月的时间跨度,具有较强的代表性和普适性. 实验在以下硬件环境下进行:CPU 为 Intel(R) Core i7-13700KF,GPU 为 RTX 4080S.

本研究采用精确率(Precision)、召回率(Recall)和 F1-score 作为评价指标:精确率衡量的是在所有被判定为异常的结果中,正确判定的比例. 低精确率意味着模型的误检率较高,可能导致大量系统误警. 召回率则表示在所有实际异常的结果中,正确判定的比例. 低召回率意味着模型的漏检率较高,系统可能无法有效识别日志异常. F1-score 是精确率和召回率的调和平均数,综合考虑了这两者对模型整体检测效果的影响. 虽然少数文献使用准确率(Accuracy)作为评价指标,它表示所有正确判定的结果占总结果数的比例,但在正常和异常样本比例严重失衡的日志异常检测任务中,正常日志占比大,对准确率的影响更显著,因此准确率通常不能很好地反映模型的性能. 本文使用的评价指标计算公式如下:

$$Precision = \frac{TP}{TP+FP}, \tag{8}$$

$$Recall = \frac{TP}{TP+FN}, \tag{9}$$

$$F1\text{-}score = 2\times\frac{Precision\times Recall}{Precision+Recall}, \tag{10}$$

其中,TP(True Positive)表示实际为真(异常日志)且被正确判定为真的样本数;FP(False Positive)表示实际为假(正常日志)但被错误判定为真的样本数;TN(True Negative)表示实际为假且正确判定为假的样本数;FN(False Negative)表示实际为真但被错误判定为假的样本数.

2.2 实例分析

本研究选取了 2024 年 1 月 14 日的连续日志记录作为样本案例进行分析. 该时间段内的日志数据涵盖了典型的电力通信系统操作场景. 所有涉及敏感信息的数据均经过严格脱敏处理,以保障数据安全.

其中 A1 和 B2 代表了两个操作员. 以不同的操作员为 block,15 min 为界限划分,可以得到两个序列,如表 2 和表 3 所示.

分析 A1 操作员的日志序列,根据提取的模板,该序列可以定义为{15,8,8,8,24,8}. 最后因为新增的光缆段没有关联的光缆,加上标签 1 表示异常.

分析 B2 操作员的日志序列,根据提取的模板,该序列可以定义为{29,15}. 最后加上标签 0 表示正常.

表 1　电力通信数据集示例

Table 1　Example of the power communication dataset

操作员	时间	操作内容
A1	8:59:47	退运日期属性由"c1"值更改为"c2"值
B2	8:59:47	运行状态属性由"在役"值更改为"停役"值
A1	9:00:08	光缆新增
A1	9:00:10	光缆新增
A1	9:01:42	光缆段新增
A1	9:01:43	重要等级属性由"c3"值更改为"c4"值
B2	9:01:55	退运日期属性由"c5"值更改为"c6"值;运行状态属性由"200"值更改为"800"值
A1	9:02:48	光缆新增

表 2　操作员 A1 操作示例

Table 2　Example of operator A1's operations

操作员	时间	操作内容
A1	8:59:47	退运日期属性由"c7"值更改为"c8"值
A1	9:00:08	光缆新增
A1	9:00:10	光缆新增
A1	9:01:42	光缆段新增
A1	9:01:43	重要等级属性由"c9"值更改为"c10"值
A1	9:02:48	光缆新增

表 3　操作员 B2 操作示例

Table 3　Example of operator B2's operations

操作员	时间	操作内容
B2	8:59:47	运行状态属性由"在役"值更改为"停役"值
B2	9:01:55	退运日期属性由"c11"值更改为"c12"值;运行状态属性由"200"值更改为"800"值

2.3　实验结果与分析

为了验证所提方法在电力通信系统日志异常检测中的有效性,本研究共对 76 275 条真实的电力系统日志记录进行了 20 次重复实验,并将另外两个最先进的基准模型应用于相同任务进行对比实验,结果如表 4 所示.

可以看出,本文方法取得了 95.13% 的精确率、92.86% 的召回率以及 93.98%的 F1 分数,相较于其他方法具有显著的性能提升. 实验结果表明,本文方法具有优异的电力通信日志异常检测性能.

此外,为进一步验证本文方法的泛化能力和适应性,在两个公开数据集 HDFS 和 BGL 上进行实验,结果如表 5 所示.

表 4　不同模型在电力通信数据集上的性能对比

Table 4　Performance comparison of different models on the power communication dataset

评估指标	模型		
	Deeplog	LogRobust	Mlog
准确率	87.56	91.17	95.13
召回率	88.13	89.11	92.86
F1 分数	89.71	93.76	93.98

表 5　Mlog 在 3 个数据集上的性能对比

Table 5　Performance comparison of Mlog on three datasets

评估指标	数据集		
	电力通信数据集	HDFS	BGL
准确率	95.13	97.92	98.41
召回率	92.86	99.93	98.92
F1 分数	93.98	98.91	98.66

可以看出,本文方法在公开日志数据集上也展现出卓越的性能. 然而,本研究所采用的电力通信系统

日志数据集(共 76 275 条记录)在规模上仍远小于主流公开数据集,如 HDFS 数据集(约 11 175 629 条记录),后者约为前者的 146 倍. 这种数据量级的差距可能限制模型训练的充分性与稳定性,也凸显出构建更大规模的电力通信系统日志数据集的必要性.

为了进一步验证本研究中改进的 Drain3 日志解析与 BERT+IDF 特征表示这两个核心模块对最终检测效果的具体贡献,我们设计了消融实验. 实验以“标准 Drain3 解析+传统 TF-IDF 表示”为基线,通过替换不同模块来衡量性能变化,实验在电力通信数据集上进行,结果如表 6 所示.

表 6　不同模块对检测性能的贡献分析

Table 6　Example of operator B2's operationsAnalysis of the contribution of different modules to detection performance

技术方案	准确率	召回率	F1 分数
标准 Drain3+TF-IDF	84.25	81.12	82.66
改进 Drain3+TF-IDF	88.76	89.21	88.98
标准 Drain3+BERT+IDF	89.48	84.34	86.84
改进 Drain3+BERT+IDF	95.13	92.86	93.98

3　结论

本文针对电力通信系统数据异常检测中专业术语理解不足、时空特征建模割裂等挑战,提出了一种基于混合神经网络的电力通信系统数据异常检测方法,通过改进的日志解析技术、高效的特征表示方法以及创新的混合神经网络模型,实现了对电力通信系统日志异常的高精度检测. 研究结果表明,该方法在处理复杂的电力通信系统日志时展现出了显著的优势,不仅具有卓越的异常检测性能,还具备良好的可扩展性和适应性. 本文方法已在某省电力通信网实际部署运行,成功实现了资产关联异常(如站点与光缆关联缺失、设备与机柜挂接错误)、配置完整性异常(如光路配线不完整、保护通道冗余度不足)、数据一致性异常(如设备容量参数不一致、调管单位信息不匹配)以及运行状态异常(如光功率异常、设备缺陷频发)等多维度数据异常的实时检测,以数据驱动的方式有效解决了传统人工规则构建及维护困难的实际问题.

尽管本研究取得了一定成果,但仍面临一些挑战,如高质量标注数据的获取、模型解释性的提升、实时监控场景下的计算效率优化,以及对未知异常的检测能力等. 这些挑战也为未来的研究指明了方向. 后续工作将重点关注以下几个方面:(1)探索半监督和无监督学习方法,减少对大量标注数据的依赖;(2)引入可解释 AI 技术,提高模型决策的透明度和可信度;(3)优化模型结构和算法,以适应实时监控的需求;(4)研究迁移学习和元学习等技术,增强模型对新型异常的泛化能力.

综上所述,本研究为电力通信系统数据异常检测领域提供了新的思路和方法,为提高电力通信系统的安全性、可靠性和智能化水平做出了积极贡献. 通过在实际生产环境中的成功应用,验证了该方法的实用价值和推广潜力. 随着相关技术的不断发展和完善,我们相信基于深度学习的日志异常检测方法将在电力通信系统运维中发挥越来越重要的作用,为电力行业的数字化转型提供有力支撑.

[参考文献]

[1] YUAN Y,ADHATARAO S S,LIN M,et al. Ada:Adaptive deep log anomaly detector[C]//IEEE Conference on Computer Communications. Virtual Conference,2020:2449-2458.

[2] 彭小圣,邓迪元,程时杰,等. 面向智能电网应用的电力大数据关键技术[J]. 中国电机工程学报,2015,35(3):503-511.

[3] ZHAO X,MIAO W,YUAN G,et al. Abnormal traffic detection system based on feature fusion and sparse transformer[J]. Mathematics,2024,12(11):1643.

[4] ZHANG X,ZHENG C,WU X,et al. Anomaly detection method for interactive data of third-party load aggregation platform based on multidimensional feature information fusion[C]//2022 IEEE 22nd International Conference on Communication Technology(ICCT). Nanjing,China,IEEE,2022:1893-1897.

[5] MAKANJU A,ZINCIR-HEYWOOD A N,MILIOS E E. A lightweight algorithm for message type extraction in system application logs[J]. IEEE transactions on knowledge and data engineering,2011,24(11):1921-1936.

[6] FU Q,LOU J G,WANG Y,et al. Execution anomaly detection in distributed systems through unstructured log analysis[C]//

IEEE International Conference on Data Mining. Miami, Florida, USA, 2009: 149-158.

[7] HE P, ZHU J, ZHENG Z, et al. Drain: An online log parsing approach with fixed depth tree[C]//IEEE International Conference on Web Services, Honolulu, Hawaii, USA, 2017: 33-40.

[8] DU M, LI F. Spell: Online streaming parsing of large unstructured system logs[J]. IEEE transactions on knowledge and data engineering, 2018, 31(11): 2213-2227.

[9] ASTEKIN M, ÖZCAN S, SÖZER H. Incremental analysis of large-scale system logs for anomaly detection[C]//IEEE International Conference on Big Data, Los Angeles, CA, USA, 2019: 2119-2127.

[10] CHEN R, ZHANG S, LI D, et al. Logtransfer: Cross-system log anomaly detection for software systems with transfer learning [C]//IEEE International Symposium on Software Reliability Engineering, Virtual Conference, 2020: 37-47.

[11] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Neural computation, 1997, 9(8): 1735-1780.

[12] DU M, LI F, ZHENG G, et al. Deeplog: Anomaly detection and diagnosis from system logs through deep learning[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, Texas, USA, 2017: 1285-1298.

[13] YANG R, QU D, GAO Y, et al. NLSALog: An anomaly detection framework for log sequence in security management[J]. IEEE Access, 2019, 7: 181152-181164.

[14] MENG W, LIU Y, ZHU Y, et al. Loganomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs[C]//International Joint Conference on Artificial Intelligence. Macao, China, 2019, 19(7): 4739-4745.

[15] 闫力, 夏伟. 基于机器学习的日志异常检测综述[J]. 计算机系统应用, 2022, 31(09): 57-69.

[16] HE P, ZHU J, HE S, et al. An evaluation study on log parsing and its use in log mining[C]//IEEE/IFIP International Conference on Dependable Systems and Networks. Toulouse, France, 2016: 654-661.

[17] FU Y, LIANG K, XU J. MLog: Mogrifier LSTM-based log anomaly detection approach using semantic representation[J]. IEEE transactions on services computing, 2023, 16(5): 3537-3549.

[18] DEVLIN J. Bert: Pre-training of deep bidirectional transformers for language understanding[J]. arXiv Preprint arXiv: 1810.04805, 2018.

[责任编辑: 陆炳新]