计算机研究与发展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(1): 207−231, 2025

互联网服务场景下基于机器学习的 KPI 异常检测综述

尚书一[1,2] 李宏佳[1] 宋 晨[1] 卢至彤[1] 王利明[1] 徐 震[1]
[1](中国科学院信息工程研究所 北京 100093)
[2](中国科学院大学网络空间安全学院 北京 100049)
(shangshuyi@iie.ac.cn)

Survey of Machine Learning-Based KPI Anomaly Detection on Internet-Based Services

Shang Shuyi[1,2], Li Hongjia[1], Song Chen[1], Lu Zhitong[1], Wang Liming[1], and Xu Zhen[1]
[1](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093)
[2](*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract Key performance indicator (KPI) anomaly detection is a fundamental technology for artificial intelligence for IT operations (AIOps) of Internet-based services. To improve the efficiency and accuracy of KPI anomaly detection, machine learning-based KPI anomaly detection has become a hotspot in both academia and industry recently. Through synthetically analyzing prior arts in this field, we first provide a technical framework of KPI anomaly detection for Internet-based services. Then, from the perspective of mining KPI's dependency patterns in different domains (including time domain, metric domain and entity domain), we explore the motivation for model selection of KPI anomaly detection on three KPI types (including univariate KPI, multivariate KPIs and matrix-variate KPIs). Furthermore, guided by the detection performance objectives, we elaborate on KPI anomaly detection techniques from two perspectives: accuracy-centric anomaly detection techniques which focus on how to improve the accuracy of KPI anomaly detection models and multi-objective balancing-centric anomaly detection techniques which focus on how to balance theoretical performance with actual application objectives. Finally, we sort out five challenges on machine learning-based KPI anomaly detection, including KPI monitoring and KPI pre-processing, generality of the model, interpretability of the model, alarm management of anomalies, and limitations of KPI anomaly detection; and we also point out the corresponding potential research directions.

Key words Internet-based services; anomaly detection; key performance indicator (KPI); machine learning; artificial intelligence for IT operations (AIOps)

摘 要 关键性能指标(key performance indicator, KPI)异常检测技术是互联网服务智能运维的基础支撑技术. 为了提升 KPI 异常检测的效率与准确性, 基于机器学习的 KPI 异常检测技术成为近年来学术界与工业界的研究热点. 在综合分析相关研究的基础上, 给出了面向互联网服务的 KPI 异常检测技术框架. 然后, 分别针对单变量 KPI、多变量 KPI 和矩阵变量 KPI, 从挖掘 KPI 在不同维度域(时间域、度量域、实体域)的依赖模式的角度出发, 探讨了用于 KPI 异常检测的机器学习模型的选择动机. 进一步地, 以检测性能目标为导向, 详细介绍了以准确性目标为核心的 KPI 异常检测技术(关注如何提升 KPI 异常检测模型的准确性)和以多目标平衡为核心的 KPI 异常检测技术(关注如何平衡理论性能与实际应用目标间的

收稿日期: 2023-07-17; **修回日期**: 2024-03-14
基金项目: 5G 终端安全技术和管控技术研究项目(E3V1581)
This work was supported by the Project of Security Management and Control Technology on 5G Terminal (E3V1581).
通信作者: 李宏佳(lihongjia@iie.ac.cn)

关系). 最后, 梳理了基于机器学习的KPI异常检测技术在KPI监控及预处理、模型通用性、模型可解释性、异常告警管理以及KPI异常检测任务自身局限性5个方面的挑战, 同时指出了与之对应的潜在研究方向.

关键词 互联网服务; 异常检测; 关键性能指标; 机器学习; 智能运维

中图法分类号 TP274; TP181

DOI: 10.7544/issn1000-1239.202330577 **CSTR:** 32373.14.issn1000-1239.202330577

互联网服务[1-2]可概括为能够通过互联网访问的服务的总称. 传统互联网通常指消费互联网, 其服务一般面向个人用户, 如即时通信服务、电商服务、网络游戏服务以及搜索引擎服务等. 随着5G通信、云计算、物联网等技术的高速发展, 互联网的应用场景不断丰富, 并逐渐从消费领域扩展至生产领域, 衍生出面向企业生产管理的工业互联网, 并产生了满足工业领域需求的一系列服务, 包括智能制造、智能供应链等.

同时, 为了满足移动、高效、可扩展的服务需求, 相关领域学者通过对传统互联网体系结构的增量式修补, 提出了一系列改良方案[3-4], 如改善移动用户网络连接性问题的移动IP(mobile IP)协议、提高传输服务质量的内容分发网络(content distribution network, CDN)以及优化网络管理效率的软件定义网络(software defined network, SDN)等. 基于上述新型互联网体系结构的服务均属于本文描述的互联网服务范畴.

然而, 互联网服务中任何异常事件的发生都可能导致服务质量下降或服务中断, 从而影响用户体验, 给企业用户造成严重的经济损失. Gartner调查数据显示, 服务中断造成的平均损失高达每分钟5 600美元[5]. 互联网服务运维是保障互联网服务安全可靠运行的有效手段, 而异常检测技术则是运维的基础支撑技术.

传统互联网服务运维及其异常检测技术存在2个问题:

问题1. 数据是驱动运维技术发展的核心, 互联网服务中的运维数据一般采集自网络跟踪、系统日志以及其他监控系统, 并根据时效性分为历史数据和实时数据[6]. 互联网服务通常要求其运维系统能够离线分析海量历史数据, 并在线监测实时数据, 这无疑给运维系统的计算及存储增添了挑战. 另外, 传统异常检测技术往往针对非时序数据设计, 很难捕获与异常事件关联的全部时序信息, 以适应不同的互联网服务.

问题2. 传统的手工运维方式工作效率低, 运维人员需要掌握大量专业的业务及系统知识, 手动处理随时可能发生的异常事件, 不适用于大规模互联网服务的运维. 自动化运维方式的出现减轻了手工运维中部分重复性工作, 利用自动化工具形成基于规则的专家系统, 自动识别已知异常, 提高了运维效率. 然而, 简单的自动化运维仍然依赖人工生成规则, 面对规模庞大且模式复杂的互联网服务, 其可用性依旧不足.

针对问题1, 当前互联网服务运维系统一般选择从各类数据源中提取关键性能指标(key performance indicator, KPI)数据进行异常检测. KPI数据是经过专家筛选的能够高度反映当前服务软硬件及业务状态的关键指标, 其数据结构为数值型, 具备丰富的时序信息且易于存储. 研究表明, 有效收集KPI数据进行运维操作可以将存储和通信占用空间减少85%以上[7]. 因此, 针对KPI数据的异常检测技术得到广泛关注.

针对问题2, 当前互联网服务运维正向智能化方向推进. 智能运维(artificial intelligence for IT operations, AIOps)[8-9]旨在利用机器学习方法, 自动从海量数据中总结规则并执行决策, 无需专家干预, 从而突破自动化运维的瓶颈. 因此, 智能运维场景下的各项技术都在朝基于机器学习方法[10-29]的方向改进. 对于KPI异常检测任务而言, 机器学习方法能够更好地捕捉海量高维KPI中的依赖模式, 检测精度及效率更高. 因此, 基于机器学习的KPI异常检测技术逐渐占据主流地位.

本文首先就互联网服务场景下基于机器学习的KPI异常检测技术文献展开调研. 调研发现, 自AIOps的概念在2016年被Gartner[9]提出以来, 有关互联网服务的KPI异常检测技术的文献发表数量呈不断上升趋势, 并于近2年趋于稳定. 然而相关综述文章[30-32]较少, 未能深入探讨KPI异常检测的模型选择动机以及如何继续提升或优化KPI异常检测性能. 因此, 本文在全面梳理KPI异常检测技术相关理论的基础上, 总结了KPI异常检测技术框架, 探讨了用于KPI异常检测的机器学习模型的选择动机, 并以检测性能目标为导向, 详细介绍了KPI异常检测技术的相关文献工作. 最后, 针对现阶段运维环境的变化及当前解决方案的不足, 展望了关于KPI异常检测技术未来的研究方向.

1 基础概述

本节主要介绍 KPI 异常检测技术的理论基础，包括 KPI 数据的定义、特点及分类，KPI 异常的定义及分类，KPI 异常检测问题数学描述以及 KPI 异常检测常用数据集和评价指标.

1.1 KPI 数据的定义、特点及分类

1.1.1 KPI 定义

时间序列数据[33-34]是指具有时间维度的变量记录，并按照时间顺序进行排列，其记录值在特定时间段和某些定律下是连续的，且单条时间序列中的采样频率保持一致. 时间序列数据点可表示为由时间戳和记录值组成的元组.

KPI 数据[35]是一种根据 IT 领域知识量化出的特殊时间序列数据，可指示互联网服务在运行过程中随时间变化的状态.

KPI 的相关数学定义如下：

定义 1. KPI. KPI 定义为 n 个连续数据点的时间序列，即 $\boldsymbol{T}=(\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n)$，长度为 n，对于任意时间 t，$\boldsymbol{x}_t \in \mathbb{R}^{M\times E}$，$M \in \mathbb{N}_+$，$E \in \mathbb{N}$.

定义 2. KPI 子序列. KPI 子序列定义为对 $\boldsymbol{T}$ 的连续 m 个位置的采样，即 $\boldsymbol{C}=(\boldsymbol{x}_{t-m+1}, \boldsymbol{x}_{t-m+2}, \cdots, \boldsymbol{x}_t)$，长度为 m，其中 $m \leqslant t \leqslant n$.

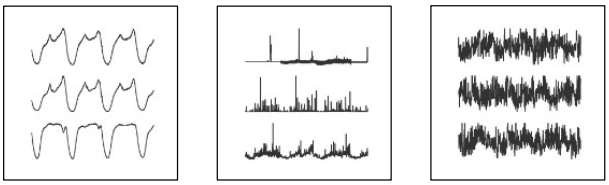
定义 3. KPI 滑动窗口. 给定长度为 n 的 $\boldsymbol{T}$ 以及用户定义的子序列长度 w，通过在 $\boldsymbol{T}$ 上按照一定步长滑动大小为 w 的窗口，提取所有可能的子序列，其中步长一般设置为 1.

1.1.2 KPI 特点

互联网服务中的 KPI 数据一般具备以下特点：

1）规模大. 随着云计算及 5G 时代的到来，互联网服务运行期间产生的 KPI 数据呈爆发式增长. 雅虎公司[36]及微软公司[37]表示，为更加全面地描述服务不同部分的属性状态，其运维系统自动监控数以百万计的 KPI 用于异常检测等任务. KPI 数据的规模不仅表现在度量域及实体域，还存在于时间域. 例如，文献 [38] 对某大型互联网公司数据中心的数十万台机器（实体域）中的数十个 KPI（度量域）进行实时细粒度监控，每台机器中的每个 KPI 每天产生 2 880 个时间点（时间域）.

2）多样化. 由于业务类型、服务运行环境、监控来源等多方因素影响，互联网服务产生的 KPI 在曲线形态上展现出多样化特点. 例如，在某全球顶级搜索引擎服务中[6]，页面浏览量指标受用户日常行为影响，常表现出规律的周期性；慢响应次数指标得益于强大的数据中心资源支撑，表现出稳定性；而平均搜索响应时间指标受随机噪声影响较大，表现出不稳定的波动性. 3 种 KPI 曲线类型如图 1 所示.



(a) 周期性 KPI　(b) 稳定性 KPI　(c) 波动性 KPI

Fig. 1 Types of KPI curve

图 1 KPI 曲线类型

3）动态波动. KPI 数据是一种实时动态到达的流式数据，可能会伴随“概念漂移”现象，即数据的分布随着时间变化朝着不可预测的方向发展[39]. 例如，图 2 中阴影处展示了某 KPI 突然的水平波动变化，这是一种典型的“概念漂移”.

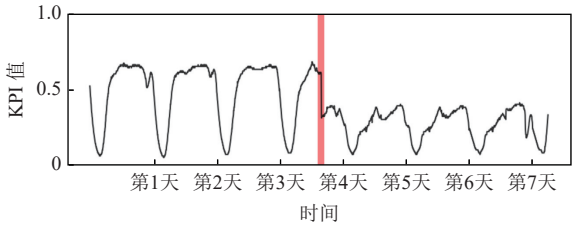


Fig. 2 An example of concept drift

图 2 概念漂移示例

4）正负样本不平衡. 由于服务在大部分时间处于正常运行状态，因此真实场景下收集到的 KPI 异常点非常少，正负样本的比例极不平衡. 在一些研究中，训练集中的正例样本（即异常）常常被忽略不计. 本文统计了 5 个互联网服务 KPI 异常检测公开数据集[36,40-43]中的正负样本比例，其中正例样本（异常点）占比最高为 4.16%，最低仅为 0.15%.

1.1.3 KPI 分类

KPI 数据存在多种不同的分类方式：按照 KPI 变量或维度域数目不同，可分为单变量 KPI（univariate KPI）、多变量 KPI（multivariate KPIs）和矩阵变量 KPI（matrix-variate KPIs）；按照 KPI 曲线形态特点不同，可分为周期性 KPI（seasonal KPI）和非周期性 KPI；按照 KPI 噪声分布不同，可分为平滑 KPI 和复杂 KPI；按照监控来源不同，可分为服务 KPI（service-level KPI）和机器 KPI（machine-level KPI）. 这 4 种分类方式在 KPI 异常检测中重叠使用，具体释义及举例表示如表 1 所示.

Table 1 Summary of KPI Data Types

表 1 KPI 数据类型总结

KPI 类型		释义	举例或表示
变量或维度域数目不同	单变量 KPI	每个时间点由单一元素表示的 KPI（该元素一般代表度量域中的单个度量值）	$\boldsymbol{X}=(x_1, x_2, \cdots, x_n), \forall X^{(t)}=x_t\in\mathbb{R}$
	多变量 KPI	每个时间点由含 M 个元素的向量表示的 KPI（该向量一般代表度量域中的多个度量值）	$\mathcal{X}=(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_M), \forall \mathcal{X}^{(t)}=\boldsymbol{X}_{1:M}^{(t)}\in\mathbb{R}^M, M\geqslant 1\in\mathbb{N}_+$
	矩阵变量 KPI	每个时间点由 $M\times E$ 的 2 维矩阵表示的 KPI（矩阵的行向量和列向量分别代表度量域和实体域）	$\bar{\mathcal{X}}=(\mathcal{X}_1, \mathcal{X}_2, \cdots, \mathcal{X}_E), \forall \bar{\mathcal{X}}^{(t)}=\mathcal{X}_{1:E}^{(t)}\in\mathbb{R}^{M\times E}, E\geqslant 1\in\mathbb{N}_+$
形态特点不同	周期性 KPI	呈现固定变化规律的 KPI	见图 1（a）
	非周期性 KPI	无固定变化规律的 KPI	见图 1（b）（c）
噪声分布不同	平滑 KPI	具有对角多元高斯噪声的 KPI	
	复杂 KPI	非高斯噪声分布的 KPI	
监控来源不同	服务 KPI	反映服务质量的业务级 KPI	页面浏览量、在线用户数及响应时间等
	机器 KPI	反映机器状态的实体级 KPI	CPU 利用率、内存利用率及吞吐量等

1.2 KPI 异常的定义及分类

1.2.1 KPI 异常定义

由于异常数据存在多样性、复杂性、随机性、稀缺性等多重特点，很难对其进行全方位的总结概括. 因此，异常通常被定义为数据中不符合定义良好的预期（正常）行为的模式[44]，并且假设系统在大部分时间处于正常运行状态. 按照上述原则，KPI 异常[38]被定义为在某时间点上与正常数据有显著差异的 KPI 向量.

1.2.2 KPI 异常分类

按照异常发生的维度域不同，我们将 KPI 异常分为 4 种类型：时序异常（temporal anomalies）、度量异常（intermetric anomalies）、时序-度量异常（temporal-intermetric anomalies）以及实体相关异常（entity-related anomalies）. 其中单变量 KPI 中仅存在时序异常，多变量 KPI 中可能存在时序异常、度量异常以及时序-度量异常，而矩阵变量 KPI 中存在与实体相关的任意异常类型.

1）时序异常[6]通常对应单变量 KPI，指某 KPI 序列中存在某个时间点出现不同于其他大部分时间点（正常时间点）的形态，如突然上升、下降或趋势变化. 图 3（a）中阴影处显示了 6 个不同 KPI 的部分时序异常.

2）度量异常[40]通常对应多变量 KPI，其中每个 KPI 作为单独个体时均遵循正常行为模式，但当多个 KPI 作为一个整体时，KPI 度量间的线性或非线性关系出现了偏离历史模式的形态. 例如，图 3（b）中阴影处显示 $\boldsymbol{X}_{12}$ 与 $\boldsymbol{X}_8$, $\boldsymbol{X}_9$, $\boldsymbol{X}_{10}$, $\boldsymbol{X}_{11}$ 发生度量异常，其相关性在标记时间段内发生改变，这可能是由于机器局部故障导致 $\boldsymbol{X}_{12}$ 的短暂波动.

3）时序-度量异常[40]表示上述 2 种异常情况均有发生，在实际工作中通常被首先识别为时序异常或度量异常.

4）实体相关异常[45]一般指发生在不同实体（如服务器、子服务、服务等）中不同形态的时序异常、度量异常或时序-度量异常. 例如，业务类型（如在线购物、社交网络、视频直播等）的差异导致服务中存在不同形态的时序-度量异常.

另外，实体依赖关系的变化还会引起实体异常（entity anomalies），即：在矩阵变量 KPI 中，各个实体变量间的线性或非线性关系出现了偏离历史模式的形态，图例可参照图 3（b）. 其他实体相关异常还包括时序-实体异常、度量-实体异常和时序-度量-实体异常，其中度量-实体异常表现在矩阵变量中，行向量和列向量（分别代表度量域和实体域）间的线性或非线性关系均发生变化.

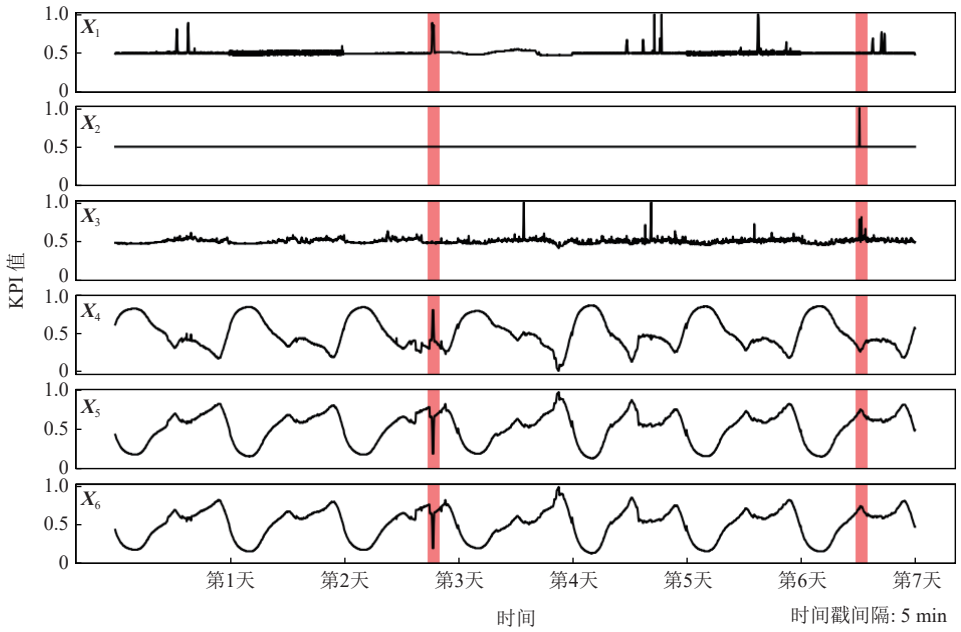
1.3 KPI 异常检测问题的数学描述

KPI 异常检测问题的数学定义分为 2 种：

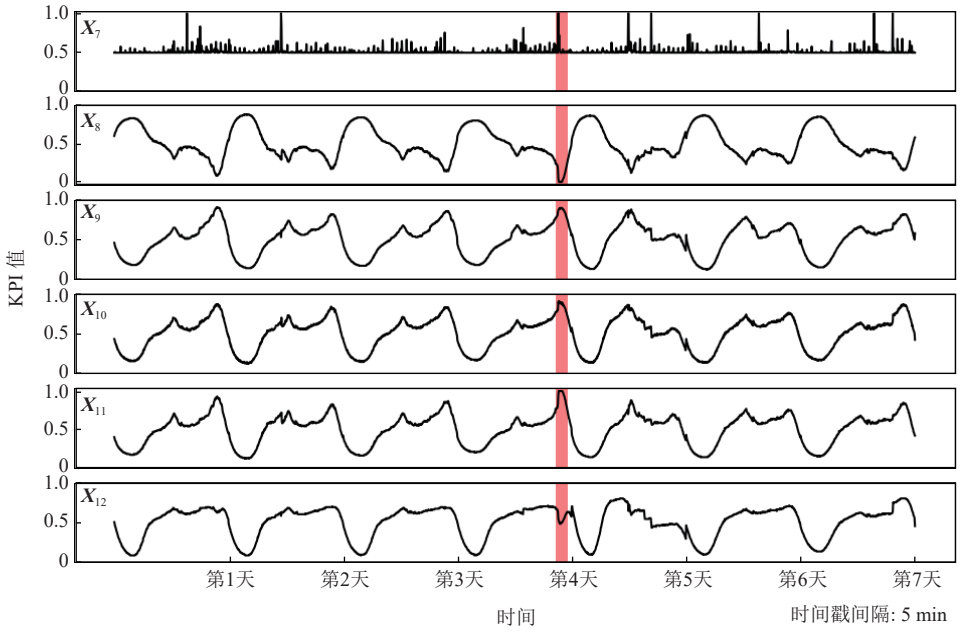
定义 4. 一般形式的 KPI 异常检测. 对于给定 $\boldsymbol{T}=(\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n)$，判断每个时间 $t(t\leqslant n)$是否发生异常. 异常点用$y_t=1$表示，输出为$\{y_1, y_2, \cdots, y_n\}$.

定义 5. 窗口形式的 KPI 异常检测. 定义窗口大小 w 并假设默认步长为 1，对于任意时间 $t(w\leqslant t\leqslant n)$，给定 $\boldsymbol{T}=(\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n)$中的一组历史观测 $(\boldsymbol{x}_{t-w+1}, \boldsymbol{x}_{t-w+2}, \cdots, \boldsymbol{x}_t)$，判断在时间 t 是否发生异常. 异常点用$y_t=1$表示，输出为$\{y_w, y_{w+1}, \cdots, y_n\}$.

为了有效地利用时间维度信息，窗口形式的 KPI 异常检测应用更加广泛[46]. 绝大多数研究采用滑动窗口表示定义 5 中的历史观测. 有研究在此基础上继续丰富窗口表示形式，文献 [47–48] 采用长短期双滑动窗



(a) 时序异常



(b) 度量异常

Fig. 3 Two basic types of KPI anomalies

图 3 KPI 的 2 种基本异常类型

口结构, 分别表达数据中关于长期和短期的时序特征, 提升了时间信息的利用率. 文献 [49] 采用滚动窗口和滑动窗口 2 种窗口策略. 滚动窗口是步长等于窗口大小的一种特殊滑动窗口, 其优势在于学习速度更快, 但对于跟踪 KPI 的快速变化, 滑动窗口效果更佳.

1.4 KPI 异常检测常用的数据集和评价指标

当前领域用于测试、评估 KPI 异常检测性能的数据集和评价指标越来越丰富, 本节主要介绍该领域常用数据集和评价指标.

1.4.1 常用数据集

KPI 异常检测领域数据集中的每列数据代表 1 条时间序列, 其中每个数据点一般具有 3 个记录值: 时间戳、值和异常标签. 按照数据集采集场景不同, 我们将常用数据集分为 2 类: 互联网服务 KPI 异常检测数据集和其他时间序列异常检测数据集.

1) 互联网服务 KPI 异常检测数据集

目前已公开的 5 个常用互联网服务 KPI 异常检测数据集具体细节如表 2 所示.

Table 2 Datasets for KPI Anomaly Detection on Internet-Based Services

表 2 互联网服务 KPI 异常检测数据集

数据集	KPI 变量数目（度量域×实体域）	KPI 数据点总数	异常点占比/%
Yahoo[36]	367×1	572 966	0.68
ASD[40]	19×12	154 171	4.16
SMD[41]	38×28	1 416 825	4.16
KPI[42]	58×1	5 922 913	2.26
NAB-Twitter[43]	9×1	142 765	0.15

KPI 变量数目(度量域×实体域)中的第 1 维表示度量域变量数目, 第 2 维表示实体域变量数目. 例如, SMD 数据集包含了在 28 台服务器实体中各自采集的 38 个 KPI.

Yahoo 数据集[36] 是由 Yahoo 实验室提供的时间序列异常检测公开数据集, 采样时间间隔为 1h. 该数据集分为 4 个子集: A_1, A_2, A_3, A_4. 其中, A_1 由从 Yahoo 真实 Web 服务中收集的 67 条时间序列数据组成; A_2, A_3, A_4 则由基于现实分布的自动化工具人工合成, 共计 300 条时间序列数据.

ASD 数据集[40] 是由文献 [40] 从某大型互联网公司的一组稳定运行服务中收集的机器实体级 KPI 异常检测数据集, 采集时间为期 45 d, 采样间隔为 5 min. 该数据集包含 19×12 个机器 KPI, 并为每个 KPI 数据点提供了额外的异常维度解释标签.

SMD 数据集[41] 与 ASD 数据集类似, 是由文献 [41] 从某大型互联网公司收集的机器实体级 KPI 异常检测数据集, 采集时间为期 5 周. 该数据集包含 38×28 个机器 KPI, 同样提供了额外的异常维度解释标签.

KPI 数据集[42] 是由 AIOps 挑战竞赛发布的关于互联网 Web 服务的 KPI 异常检测数据集, 来源包括阿里巴巴、腾讯、百度、eBay 等多家大型互联网公司的真实监控系统. 该数据集由多条已标注的服务 KPI 和机器 KPI 组成, 其采样时间间隔多为 1 min, 少部分时间间隔为 5 min.

NAB 数据集[43] 是由 Numenta 公司提供的关于评估实时应用程序性能的时间序列异常检测公开数据集. 该数据集来源于多个真实互联网服务场景以及人工合成场景, 如由亚马逊网络服务收集的服务器机器 KPI 数据集, 由大型工业工厂内部传感器收集的温度 KPI 数据集, 由 Twitter 等社交媒体中收集的关于谷歌、IBM 等大型上市公司被提及次数的时间序列数据集等.

2)其他时间序列异常检测数据集

研究者为了验证所提出的 KPI 异常检测算法在其他领域的通用性, 还会与针对其他场景的时间序列异常检测技术进行对比. 时间序列异常检测领域常用数据集包括: 某土壤湿度卫星遥测数据集 SMAP[50]、火星实验室的探测器数据集 MSL[50]、某水处理网络测试数据集 SWaT[51]、某水处理网络测试数据集 WADI[52]、多领域的时间序列公开数据集 UCR[53] 等.

1.4.2 常用评价指标

按照评价角度, 本文将 KPI 异常检测领域的常用评价指标分为 2 类: 准确性评价指标和应用性评价指标.

1)准确性评价指标

KPI 异常检测作为一个 2 分类问题, 在理论研究中通常采用基于混淆矩阵[54] 的评估方法计算各种衡量异常识别准确性的指标. 常用准确性指标包括: 准确率(accuracy, *ACC*)、精确率(precision, *P*)、召回率(recall, *TPR*)、特异度(specificity, *TNR*)、误报率(false positive rate, *FPR*)、漏报率(false negative rate, *FNR*)、*F*1 分数(*F* score)和 ROC 曲线下方面积(area under curve, *AUC*)[55] 等.

2)应用性评价指标

为满足不同服务的应用目标, KPI 异常检测的实际性能不仅取决于准确性指标, 还取决于其他应用性指标. 互联网服务场景下针对 KPI 异常检测任务所提出的应用目标有 3 种: 鲁棒性、实时性和可解释性. 为衡量这 3 个方面的性能, 相关研究采用了 4 类应用性评价指标:

① 时间指标[46]. 例如训练时间、检测时间、单步骤执行时间、通信时间等, 用于从时间方面反映模型的检测效率, 衡量检测实时性.

② 延迟指标[56]. 例如检测延迟(detection lag/detection delay)、告警延迟(alert delay)等, 用于直接反映模型检测或告警实时性. KPI 异常检测中的检测延迟定义为检测 1 个异常点或 1 个异常段所消耗的时间, 也可称为检测时间. 而告警延迟定义为异常段中第 1 个真实异常点与第 1 个检测异常点之间的时间戳距离. 许多研究将这 2 种指标视为等同.

③ 可解释性指标[40-41,46]. 可解释性指的是人对模型所做决策理解程度的一种能力, 目前 KPI 异常检测研究工作中还没有明确统一的可解释性评价指标. 表 3 概括了 KPI 异常检测研究工作中关于可解释性指标的不同计算公式, 主要思路是计算模型检测到的异常度量为真实异常度量的命中率.

Table 3 Interpretability Metrics of KPI Anomaly Detection

表 3 KPI 异常检测中的可解释性指标

典型工作	可解释性指标	释义
OmniAnomaly[41]	$HitRate@P\% = \dfrac{Hit@\lfloor P\% \times \lvert \boldsymbol{GT}_i \rvert \rfloor}{\lvert \boldsymbol{GT}_i \rvert}$	$\boldsymbol{GT}_i$表示真实异常度量的排序数组，P=100 或 150，$Hit@\lfloor P\% \times \lvert \boldsymbol{GT}_i \rvert \rfloor$表示模型在$\lfloor P\% \times \lvert \boldsymbol{GT}_i \rvert \rfloor$下的异常度量命中数量
DAEMON[46]	$RDCG@P\% = \sum_{i=1}^{\lvert G_u \rvert} \dfrac{v_i}{\mathrm{lb}(d_i+2)}$	在 $HitRate@P\%$ 基础上考虑不同异常度量的重要性，其中，v_i 表示第 i 个度量是否命中（$v_i=1$ 或 $v_i=0$），d_i 表示真实异常度量排序集合中 i 的位置索引与模型检测到的异常度量排序集合中 i 的位置索引间的距离
InterFusion[40]	$IPS = \sum_{a=1}^{A} \dfrac{w_a \lvert \boldsymbol{G}_{\phi_a} \cap \boldsymbol{I}_{\phi_a} \rvert}{\lvert \boldsymbol{G}_{\phi_a} \rvert}, w_a = \dfrac{N_{\phi_a}}{\sum_{a=1}^{A} N_{\phi_a}}$	在 $HitRate@P\%$ 基础上考虑异常段级的可解释性，其中，N_{ϕ_a} 表示异常段ϕ_a的长度，w_a用于衡量该异常段在所有异常段中的重要性

④ 鲁棒性指标. 鲁棒性指的是模型在数据不确定性的扰动下，保持性能稳定不变的能力. 鲁棒性越强，其抗干扰能力越强，模型工作越稳定. 各类模型的鲁棒性评估方法可参考文献 [57].

2 KPI 异常检测技术框架

在介绍互联网服务场景下基于机器学习的 KPI 异常检测技术框架前，首先再次明确互联网服务的定义. 引言中提到，本文所描述的互联网服务是基于互联网的服务，即用户可以通过互联网访问的各类服务，这些服务不仅可以构建在不同的互联网体系结构或网络协议之上（如基于 CDN 的服务[58-60]、基于移动互联网的服务[61-63]，以下分别简称为“CDN 服务”和“移动互联网服务”），也可以部署在不同的计算环境之中（如基于云的服务），还可以连接不同的服务对象（如基于物联网的服务[64-65]，以下简称为“物联网服务”）. 另外，服务间还存在交叉关系. 例如，许多移动互联网服务（尤其是流媒体服务，如视频点播、直播等）选择使用 CDN 作为其网络架构，以加强服务内容的传输效率与稳定性. 再例如，当前的物联网服务越来越倾向使用 5G, WiFi6 等移动网络连接各种智能终端，以满足低功耗、广域覆盖的需求.

按照工作流程顺序，面向互联网服务的 KPI 异常检测技术框架可概括为 3 个阶段：KPI 监控与预处理、异常检测模型构建与训练、在线检测与告警. 技术框架如图 4 所示. 除此之外，本节还讨论了多种互联网服务在该框架下的关键需求.

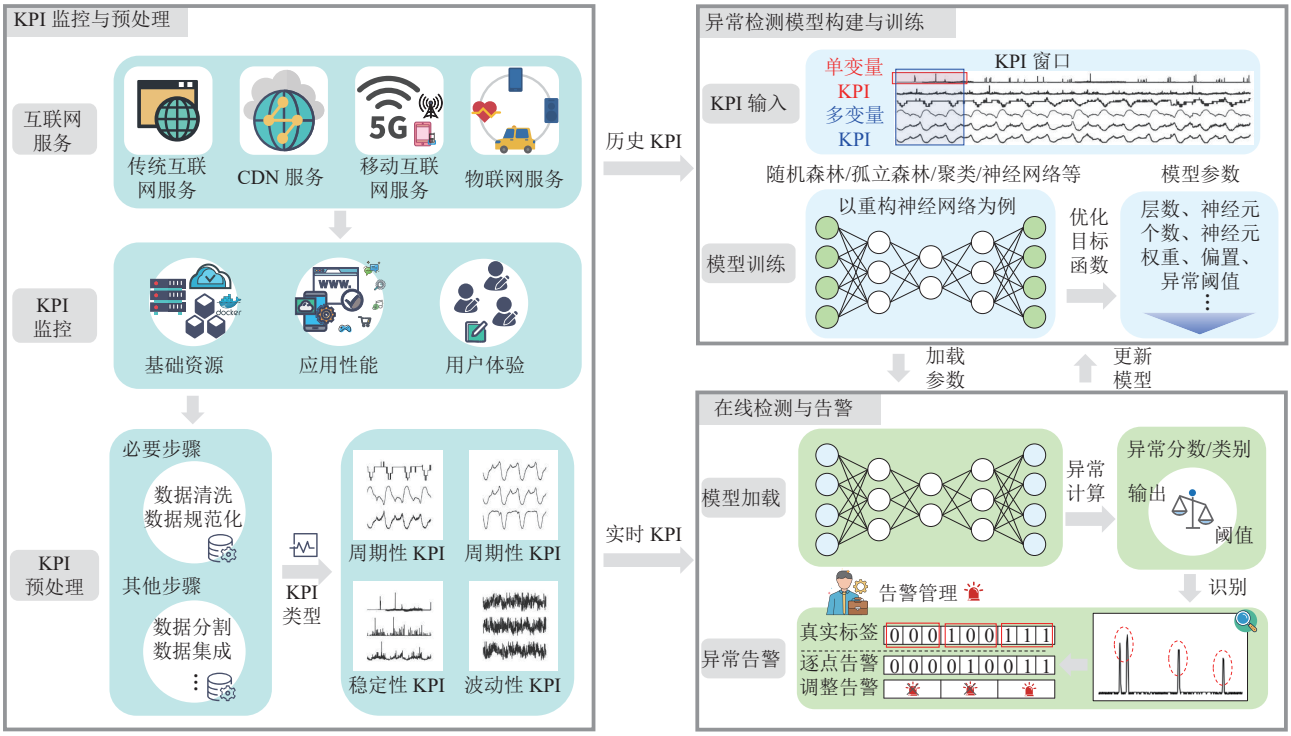


Fig. 4 Technical framework of KPI anomaly detection

图 4 KPI 异常检测技术框架

2.1 KPI 监控与预处理

首先，在不影响服务正常运行的原则下，对互联

网服务运行环境中各个层次的重要节点部署监控代理, 全方位收集 KPI 数据. 互联网服务 KPI 监控体系主要概括为 3 个层次: 基础资源、应用性能及用户体验, 其中以基础资源监控(通常将其 KPI 定义为机器 KPI)和应用性能监控(通常将其 KPI 定义为服务 KPI)在 KPI 监控中最为常见. 表 4 所示为各层次 KPI 监控范围介绍及举例. 常用基础资源监控工具包括 Zabbix 等, 常用应用性能监控工具包括 SkyWalking 等.

Table 4 KPI Monitoring System

表 4 KPI 监控体系

监控层次	监控范围	相关 KPI
基础资源	主要对服务中的硬件设备、虚拟机或容器集群等资源进行监控	CPU 利用率、网络接口流量、丢包数、吞吐量等
应用性能	主要对服务中的可用性状态、应用处理能力、业务运营状态等应用性能进行监控	页面浏览量、服务响应时间、交易量、在线用户数等
用户体验	主要对用户真实访问体验及反馈意见进行监控	首屏时间、下载速度、用户反馈文本中某些关键词组合出现的频率[47] 等

关于互联网服务中不同监控层面的责任归属问题, 本文不作讨论. 不同互联网服务提供商或运营商可结合自身业务需求或 IT 架构制定不同的 KPI 监控体系. CDN 服务[58] 更注重网络性能监控, 监控内容包括可以反映用户访问量、访问时延以及状态码相关的各项 KPI. 文献 [61] 指出用户体验质量(quality of experience, QoE)可以作为与服务质量(quality of service, QoS)互补的移动互联网服务性能评价标准, 因此移动互联网服务场景下[47] 还会收集与用户体验相关的 KPI.

其次, 需要对监控到的大量 KPI 数据进行预处理, 以确保后续模型训练的有效性. 基于机器学习的 KPI 异常检测技术一般包含数据清洗(如缺失值填补)和数据规范化(如零均值规范化)两项预处理步骤, 部分技术中也可能会涉及数据分割(如基于滑动窗口的时间序列)、数据集成(如多源 KPI 合并)及数据降维(如特征提取、特征选择)等其他预处理步骤. 处理后的 KPI 可根据不同角度进行分类(见 1.1.3 节).

2.2 异常检测模型构建与训练

首先, 根据历史 KPI 构建基于机器学习的异常检测模型, 即检测器(detector). 其次, 训练模型, 得到检测器全部参数, 包括结构参数、训练参数以及异常阈值参数等.

该阶段中, 异常检测模型构建一般又分为机器学习模型选择和机器学习模型优化设计 2 部分. 模型的选择主要取决于 KPI 中的依赖模式. 不同服务存在不同的依赖模式. 例如, CDN KPI[58-59] 之间表现出一定的实体依赖, 物联网服务场景下[64] 的 KPI 与空间呈强关联性, 异构无线网络环境导致移动互联网服务 KPI 表现出各种复杂的周期性模式和趋势等. 而模型的优化设计则更多考虑影响检测技术性能(包括准确性、鲁棒性、实时性、可解释性等)的多重因素, 如 KPI 噪声分布、模型计算复杂度等.

2.3 在线检测与告警

首先接收服务运行过程中传输的实时 KPI, 加载、部署异常检测模型. 然后将实时 KPI 输入模型, 并输出异常分数或直接获得异常分类结果. 异常分数计算方法与训练中的损失函数计算方法密切相关. 当异常得分超过模型设定阈值或直接被模型判定为异常时, 将依据相关告警策略向运维人员发出异常告警.

除此之外, 随着资源调整、软件升级等服务变化, 许多互联网服务还会在线动态调整异常检测模型, 实时更新模型相关参数, 以保持模型在实际应用中的鲁棒性.

该阶段中, 异常分数计算方法和阈值选择机制主要影响在线检测的准确性指标, 而模型部署位置、告警策略、模型动态调整方式等则会影响检测的应用性指标. 文献 [65] 指出物联网服务中的终端设备安全性较差, 容易遭受 DDoS 等网络攻击. 而 DDoS 攻击会引起大量异常信息过载, 若不调整告警策略, 将严重影响物联网服务中的检测实时性.

3 KPI 异常检测技术的模型选择动机及分类

模型选择是基于机器学习的 KPI 异常检测技术的重要基础. 我们发现, 大部分研究主要从如何挖掘 KPI 中的依赖模式这一动机出发, 选择具备相应能力的机器学习模型.

针对这一角度, 本节首先根据互联网服务的场景特点和应用需求, 将 KPI 异常检测任务分为针对单变量 KPI 的异常检测、针对多变量 KPI 的异常检测和针对矩阵变量 KPI 的异常检测. 其次, 分析 3 种 KPI 场景中所包含的依赖模式, 探讨不同场景下 KPI 异常检测技术的模型选择动机. 最后, 提出以检测性能目标为导向, 对 KPI 异常检测技术进一步分类.

3.1 KPI 依赖模式分析

KPI 中表现出的一般依赖模式可分为 3 种: 时序依赖(temporal dependency)、度量依赖(intermetric dependency)以及实体依赖(entity dependency). 按照依

赖模式是否随时间变化，又可细分为静态依赖（时不变性）和动态依赖（时变性）.

1）时序依赖. 即与时序有关的依赖模式，如短期或长期的趋势、周期性和波动性等.

2）度量依赖. 即与其他KPI度量有关的依赖模式，一般指KPI之间存在的线性或非线性关系，如网络吞吐量与CPU利用率呈正相关等.

3）实体依赖. 即与其他实体有关的依赖模式，一般指不同实体中某一KPI之间存在的线性或非线性关系. 这里的实体小到可以单指某一运行机器，大到可以表示单个子服务功能甚至单个服务.

KPI中表现出的其他依赖模式还包括频域模式、异常模式等. 频域是遵循特定规则的一个数学构造，在KPI异常检测的研究中，频域模式是对时序依赖模式的补充. 而由于异常模式通常具有稀缺、随机等特点，很少有研究单独分析KPI的异常模式. 因此，对于频域模式和异常模式，我们不作单独讨论.

3.2 单变量KPI异常检测的模型选择动机

单变量KPI中依赖模式较为单一，仅包含时序依赖. 单变量KPI异常检测技术假设各个KPI独立反映服务某方面的性能，采样粒度粗，KPI长度、数量相对较小. 因此，单变量KPI异常检测技术一般对每个或每类KPI进行单独训练，专注于挖掘时序依赖，以识别时序异常.

3.2.1 挖掘时序依赖

人工特征提取[6,35,47,66-76]是挖掘KPI时序依赖的常用方法之一. 首先，提取上下文信息特征，将单变量KPI中的每个数据点转换为普通的多维离散数据. 然后，将转换后的数据输入到传统机器学习模型（随机森林、孤立森林、聚类等）中，识别时序异常. 文献[35]认为当前KPI值偏离预测结果越大则越有可能是异常，于是采用6种经典时间序列预测模型提取了6个预测误差特征，挖掘单变量KPI中的短期或长期趋势. 文献[66]认为KPI出现剧烈变化时可能发生异常，因此根据2个连续窗口中KPI数据的变化提取了19个时序特征，挖掘单变量KPI中的长期时序依赖. 文献[67]计算了KPI窗口内的均值、方差、自相关等基本统计特征，可用于挖掘KPI中的短期时序信息. 文献[68]认为频域信息更有利于检测波动性时间序列上的异常，因此提取小波特征代替时序特征，挖掘超出时域范围的频域模式.

时间序列聚类[77]是挖掘KPI时序依赖的另一种常用方法. 首先，通过优化经典聚类模型中的相似性度量方法，使其成为适应序列数据的版本. 然后将原始KPI划分为不同的聚类簇，从而区分KPI中的动态时序依赖. 最后再结合其他KPI异常检测模型针对每个簇进行训练和检测. 时间序列聚类可以很好地挖掘单变量KPI在不同时间段的动态周期性. 例如，对于在线购物服务，工作日的页面浏览量指标通常高于休息日. 文献[77]采用DBSCAN聚类分割KPI数据，将每条KPI划分为工作日、休息日和春节3种周期模式类别.

除上述2种挖掘方式之外，近年流行的工作[37,78-84]一般是直接利用序列神经网络挖掘KPI时序依赖，实现时序依赖挖掘与异常检测训练步骤的深度融合，更好地胜任当前互联网服务场景下的智能运维要求.

循环神经网络（recurrent neural network, RNN）及其变体长短期记忆网络（long short-term memory, LSTM）和门控循环单元（gated recurrent unit, GRU）网络是专门用来提取时序特征的神经网络模型. RNN通过隐变量的循环连接，按时间顺序传递序列数据中的信息，从而表达其中的时序依赖. 然而，简单的RNN结构受短时记忆的限制，无法学习时间序列中的长期时序依赖. 文献[78–81]采用LSTM网络，利用“门”机制，使其具备保留信息或遗忘信息的功能，更好地挖掘KPI中的长期时序依赖.

另有研究表明，通过正确选择卷积核大小、步长及卷积层层数等相关参数，沿时间维度应用的1维卷积神经网络（convolutional neural network, CNN）[37,82-83]也可以捕获时间序列上的长期时序依赖，并且不受RNN等循环结构中梯度消失问题的困扰，训练速度更快. 文献[37]采用谱残差（spectral residual, SR）模型获取KPI中的频域信息，并将原始KPI序列转化为更易被CNN学习的模式，然后输入到1维CNN中，继续挖掘KPI中的时序依赖. 文献[82]同样考虑频域和时域2部分信息，将快速傅里叶变换（fast Fourier transform, FFT）获得的频域辅助分量与原始KPI序列串联，共同输入到基于CNN的序列预测模型中进行预测. 文献[85]提出了一种专门针对时间序列数据建模的时域卷积网络（temporal convolutional network, TCN），该网络采用因果卷积（causal convolution）或扩张卷积（dilated convolution）的方式，在获取更多时域信息的同时提高了计算速度. 文献[83]引入TCN与1维CNN结合，共同挖掘KPI时序依赖.

3.2.2 挖掘不同度量中的时序依赖

时间序列聚类[67,69-71,86-88]可以挖掘不同KPI度量中周期性模式的相似性. 该方式本质上是通过计算2条序列间的相似性，将具有相同周期性模式的KPI

聚类在一起, 并未涉及 KPI 度量依赖挖掘. 即通过聚类, 将多变量 KPI 切分为多类单变量 KPI, 然后再对每类 KPI 进行异常检测. 文献 [86] 提出了 ROCKA 聚类算法, 该算法是一种 DBSCAN 聚类的变体, 采用形状距离(shape-based distance, SBD)作为相似性度量的标准, 从数据本身推断真实的聚类个数(即周期性模式数量), 并自然地利用形状相似性的传递性扩展聚类, 非常适合挖掘不同 KPI 度量中的静态周期性.

3.3 多变量 KPI 异常检测的模型选择动机

多变量 KPI 中包含时序依赖、度量依赖及其混合模式. 多变量 KPI 异常检测技术假设各个 KPI 之间相互关联, 共同反映服务整体的健康状态, KPI 采样粒度细、KPI 规模更大且分布更复杂. 因此, 多变量 KPI 异常检测技术通常会将服务中采集的多变量 KPI 看作一个整体, 进行统一训练, 不仅要挖掘单个 KPI 度量内的时序依赖, 而且更重要的是挖掘多个 KPI 度量间复杂的度量依赖, 以识别时序异常、度量异常或时序-度量异常.

3.3.1 挖掘度量依赖

早期挖掘多变量 KPI 度量依赖的工作通常采用传统机器学习模型, 先是通过人工特征提取[72] 的方式提取相关性变化特征, 挖掘多变量 KPI 中的动态度量依赖, 然后再输入到机器学习模型中检测异常. 然而传统机器学习模型过度依赖于人工标签, 挖掘复杂度量依赖的能力有限.

随着深度学习的不断突破, 深度神经网络逐渐成为挖掘多变量 KPI 度量依赖的主流技术. 根据我们的调研, 序列神经网络一般仅适合挖掘时间序列数据中的时序依赖, 对于捕捉 KPI 之间复杂的度量依赖关系以及抗噪声的能力较弱. 与此同时, 基于重构神经网络的自动编码器(autoencoder, AE)[89-91] 或变分自动编码器(variational autoencoder, VAE)[56,87,92-94] 能够一定程度上避免多变量 KPI 中不确定性因素的影响, 成为挖掘多变量 KPI 度量依赖的主要方法. 文献 [89] 采用对抗式训练的 AE 模型, 提高对多变量 KPI 中正常模式的重构能力. 文献 [90] 采用一种异步实时信号处理技术, 纠正多变量 KPI 在真实场景下因异步观察导致的更加复杂的非线性度量依赖关系, 将异步多变量 KPI 转换为同步表示, 以提高后续 AE 模型的挖掘能力.

3.3.2 挖掘时序-度量依赖的混合模式

不仅如此, 深度神经网络还可以通过扩展网络层的深度及广度, 引入多种序列化结构, 实现针对多变量 KPI 度量依赖与时序依赖的混合模式挖掘[40-41,48,58,95-107].

文献 [41] 首先利用 GRU 层学习时间嵌入 $\boldsymbol{e}_t$, 然后采用随机连接技术, 将时间 $t-1$ 的 VAE 隐变量 $\boldsymbol{z}_{t-1}$ 与时间 t 的 GRU 隐变量 $\boldsymbol{e}_t$ 以串联的方式拼接在一起, 显式建模时间 t 的时序-度量嵌入, 实现了时序和度量依赖融合的混合模式挖掘. 文献 [40] 采用基于层次 VAE 的双视图嵌入方法, 分别利用 1 维 CNN 层和修改后的切片循环神经网络(modified sliced recurrent neural network, m-SRNN)层, 按层次顺序依次学习多变量 KPI 中的低维时间嵌入 $\boldsymbol{z}_2$ 和度量嵌入 $\boldsymbol{z}_1$, 使得模型在挖掘度量依赖的同时可以感知到时间信息, 同样实现了混合模式挖掘. 文献 [95] 采用 VAE 与 TCN 的混合模型, 也实现了对多变量 KPI 中局部度量依赖与长期时序依赖的并行建模.

近年来, 基于自注意力机制(self-attention)的 Transformer 模型[96-101,108] 在时间序列预测等领域取得了巨大进展. 相比于 RNN 等传统循环网络结构, Transformer 通过提取所有数据点沿时间维度的权重分布, 表达更丰富的时序依赖, 从根本上解决了时间序列的长期记忆难题. 另外, Transformer 利用位置编码在并行计算过程中实现对完整时间序列的顺序学习, 训练速度快、计算开销低, 更适合处理大规模多变量 KPI 数据. 文献 [96] 在 LSTM-VAE 架构的基础上引入基于多头注意力(multi-head attention)机制的 Transformer 层, 提升时序依赖的挖掘效果. Informer[102-103] 是基于 Transformer 模型的变体, 通过概率稀疏自注意力机制等改进, 进一步降低了 Transformer 模型的时间复杂度和空间复杂度. 文献 [102] 先采用图注意力网络捕捉多变量 KPI 间的度量依赖, 然后并行使用 Informer 层和 GRU 层, 联合捕捉 KPI 数据中的长期时序依赖.

除了随时间变化而呈现出的动态时序依赖, 文献 [58] 发现 CDN 场景中的多变量 KPI 表现出隐藏的时不变特征, 这些特征不受时间相关的随机输入的影响, 在不同的时间尺度上保持不变性. 在 AE 架构中采用双向 LSTM(bidirectional LSTM, BiLSTM)[109] 和循环 VAE 双层结构, 分别挖掘多变量 KPI 中的时不变性和时变性, 其中 BiLSTM 能够同时学习过去和未来 2 个方向上的时序依赖.

3.3.3 挖掘不同实体中的时序、度量依赖及其混合模式

深度神经网络[38,110] 还可以对不同实体的多变量 KPI 建模. 该方式并未涉及矩阵变量 KPI 中的实体依赖挖掘, 即通过聚类或直接划分的方式将矩阵变量

KPI 从实体域向量化(列向量化)，然后分别挖掘不同实体(实体类)中多变量 KPI 的时序、度量依赖及其混合模式.

考虑到不同实体中多变量 KPI 可能存在时序、度量依赖的差异，文献 [38] 利用基于 Wasserstein 距离的层次聚类方法，将所有机器实体中的多变量 KPI 分为多个聚类簇(每个机器实体对应 1 个多变量 KPI)，并单独微调每个簇的异常检测模型，以区分实体间的时序、度量依赖的混合模式. 文献 [110] 在 VRNN(variational RNN)基础上，通过切换高斯模型分别捕获不同网站(实体)中多变量 CDN KPI 的时序、度量依赖的混合模式. 研究表明，这种切换机制在仅使用 1 组训练参数的情况下，能够有效针对不同网站的 CDN 多变量 KPI 建模.

3.4 矩阵变量 KPI 异常检测的模型选择动机

根据矩阵变量时间序列的定义[33]，矩阵变量 KPI 包含时序依赖、度量依赖、实体依赖及其混合模式. 矩阵变量 KPI 异常检测技术假设矩阵变量 KPI 中的各个实体(列向量)间相互关联，存在实体依赖. 由于相关工作较少，当前矩阵变量 KPI 异常检测技术的建模思路一般是将矩阵变量 KPI 从度量域向量化(行向量化)，挖掘多变量 KPI 中的时序、实体依赖及其混合模式. 与 3.3 节中指代不同，本节描述的多变量指代实体变量，每个多变量 KPI 代表不同度量(度量类)在多个实体中的状态.

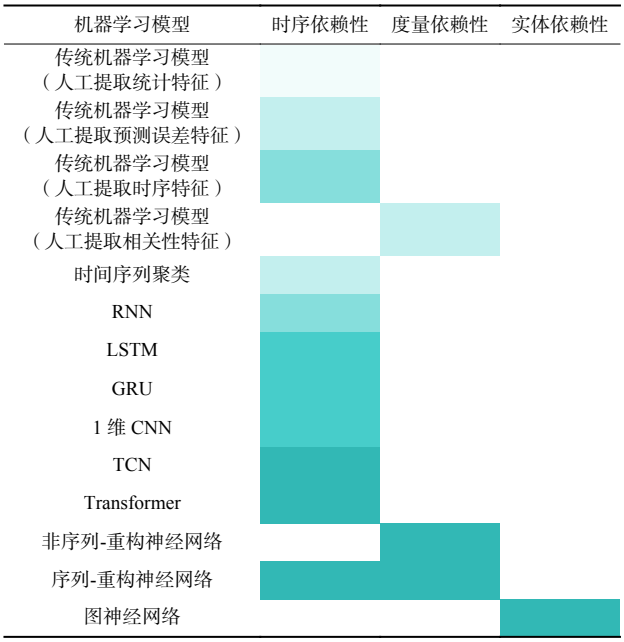
许多研究工作致力于研究因实体空间位置(如服务器部署位置、子服务在调用链结构中的位置等)差异导致的空间依赖(spatial dependency). 图卷积神经网络(graph convolutional neural network, GCN)是挖掘 KPI 中时序、空间依赖混合模式的主要方法，例如，文献 [111–112] 利用图卷积层分别学习 SDN 和大型云 IT 系统下 KPI 中的时空依赖.

文献 [45] 在线上到线下(online to offline, O2O)服务场景中提出了用于挖掘实体依赖的 KPI 异常检测方案，这里的实体表示不同零售商的 O2O 服务. 采用属性图注意力网络和时序-实体图注意力网络 2 层顺序结构，依次从 2 个角度向量化矩阵变量 KPI，分别挖掘不同实体中的度量依赖和时序、实体依赖的混合模式.

表 5 对比了主要机器学习模型的 KPI 依赖模式的挖掘能力，颜色越深表示挖掘能力越强. 表 6 总结了 KPI 异常检测技术的模型选择动机，具体内容包括 KPI 场景、机器学习模型、模型选择动机以及与之对应的代表性工作.

Table 5 Comparison of Mining Ability for KPI's Dependency Patterns

表 5 KPI 依赖模式挖掘能力对比



注：颜色越深表示该模型相应的挖掘能力越强.

3.5 以检测性能目标为导向的 KPI 异常检测技术分类框架

本文继续以检测性能目标为导向，将互联网服务场景下基于机器学习的 KPI 异常检测技术分为以准确性目标为核心的 KPI 异常检测技术和以多目标平衡为核心的 KPI 异常检测技术.

通过统计 36 篇 KPI 异常检测技术代表性工作的核心目标，我们发现，直至当前阶段，该领域绝大多数工作将 KPI 异常检测的研究重心放在提升检测准确性上，优化应用性指标常常作为辅助任务. 具体文献分类总结如图 5 韦恩图所示. 该分类方式将 KPI 异常检测中面临的实际问题与理论研究中的模型评价指标对应，更清晰地指出了各个问题所对应的研究方向及解决方案. 具体分类框架如图 6 所示.

1)以准确性目标为核心的 KPI 异常检测技术，其重点是对 KPI 异常检测模型选择后的进一步研究，从提升 KPI 异常检测准确性角度，研究不同模型的性能提升方式. 性能提升方式可分为 6 种，分别对应 KPI 异常检测技术框架中的不同阶段，详细介绍见第 4 节.

2)以多目标平衡为核心的 KPI 异常检测技术，着眼于实际互联网服务场景，以在工业界实现 KPI 异常检测技术的高可用性为原则，在保证甚至牺牲一部分检测准确性的基础上，讨论如何平衡其他应用性指标. 详细介绍见第 5 节.

Table 6 Motivation for Model Selection of KPI Anomaly Detection

表 6 KPI 异常检测的模型选择动机

KPI 场景	机器学习模型	模型选择动机 （主要动机是挖掘 KPI 依赖模式的能力）	代表性工作
单变量 KPI	传统机器学习模型（人工提取统计特征）	挖掘短期时序依赖	文献 [67–70,73–74]
	传统机器学习模型（人工提取预测误差特征）	挖掘趋势及偏离预测的异常模式	文献 [6,35,47,66–68,71]
	传统机器学习模型（人工特征提取时序特征）	挖掘长期时序依赖及剧烈变化的异常模式	文献 [66–67,69–70,75]
	传统机器学习模型（人工特征提取小波特征）	挖掘频域模式有利于检测波动性 KPI 异常	文献 [68]
	时间序列聚类（DBSCAN）+传统机器学习模型	挖掘周期性模式的相似性	文献 [66,69–71,77,86–88]
	序列神经网络（RNN）	挖掘短期时序依赖	
	序列神经网络（LSTM）	挖掘长期时序依赖	文献 [78–81]
	序列神经网络（GRU）	挖掘长期时序依赖	
	序列神经网络（1 维 CNN）	挖掘长期时序依赖，缓解梯度消失，训练快	文献 [37,82–83]
	序列神经网络（TCN）	挖掘长期时序依赖，扩大卷积核的感受野	文献 [83]
多变量 KPI	传统机器学习模型（人工提取相关性特征）	挖掘度量依赖	文献 [72]
	重构神经网络（AE）	挖掘度量依赖	文献 [89–91]
	重构神经网络（VAE）	挖掘度量依赖且缓解过拟合问题	文献 [56,87,92–94]
	序列-重构神经网络	挖掘时序、度量依赖的混合模式	文献 [38,40–41,48,58,95,104–107,110]
	Transformer 及其变体	挖掘时序、度量依赖的混合模式，训练快	文献 [96–103,108]
	聚类+重构神经网络	挖掘不同实体中时序、度量依赖的混合模式	文献 [38]
	切换高斯模型+重构神经网络	挖掘不同实体中时序、度量依赖的混合模式	文献 [110]
矩阵变量 KPI	图卷积网络	挖掘时序、实体（空间）依赖的混合模式	文献 [111–112]
	图注意力网络	挖掘时序、实体依赖的混合模式	文献 [45]

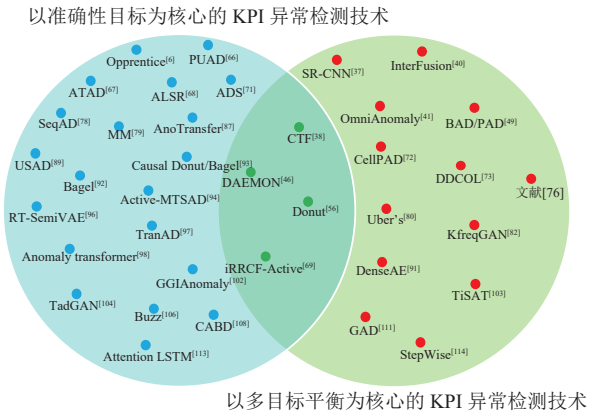


Fig. 5 Venn graph of the KPI anomaly detection techniques

图 5 KPI 异常检测技术韦恩图

4 以准确性目标为核心的 KPI 异常检测技术

随着云计算、5G 通信等技术的高速发展，互联网服务产生的 KPI 数据呈爆发式增长，即使是具备强大表征能力的机器学习模型，也需要不断优化、迭代，以适应场景或数据的变化，提升 KPI 异常检测准确性. 提升异常检测准确性的方法可以分别对应到 KPI 异常检测技术框架中的 3 个阶段：1)KPI 预处理阶段，主要方式是人工提取高质量特征；2)模型构建与训练阶段，主要方式包括完善模型结构、优化目标函数以及改进训练方式(主要指半监督学习)；3)在线检测阶段，包括改进异常分数计算方法以及调整阈值选择机制. 本节针对 KPI 异常检测技术中的 5 种常用机器学习模型(3 种传统机器学习模型和 2 种深度学习模型)，展开介绍以准确性目标为核心的 KPI 异常检测技术.

4.1 传统机器学习模型准确性提升

基于传统机器学习的异常检测技术是从专家系统异常检测技术到人工智能异常检测技术的过渡，其中特征提取和模型训练过程相互独立.

特征提取的好坏严重影响传统机器学习模型的准确性. 相关研究[66-67,69-70,72] 主要通过多角度、全方位的提取方式丰富特征信息. 例如，文献 [67] 提取了关于统计特征、预测误差特征和时序特征 3 种类型的特征共 37 个，用于基于聚类和随机森林混合模型的异常检测，大大提高了检测准确性.

对于模型训练和在线检测阶段中所采用的准确性提升方法，各个机器学习模型之间存在较大差异，本节将分开讨论. 随机森林、孤立森林(isolation forest,

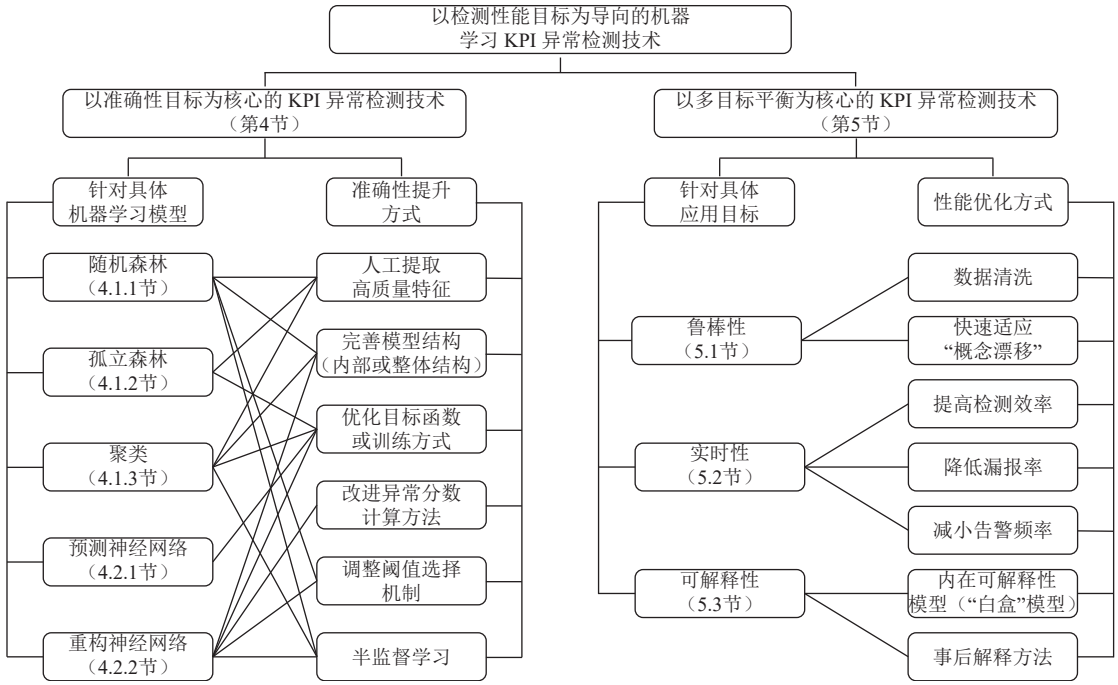


Fig. 6 Classification framework of KPI anomaly detection techniques

图 6 KPI 异常检测技术分类框架

IF）和聚类是最具代表性的 3 种传统机器学习模型.

4.1.1 随机森林

随机森林[6,66,68,72,115]作为一种基于 Bagging 算法的集成学习模型，引入了随机性，且参数少、推理速度快、准确率高，被证明是一种对噪声特征鲁棒的异常检测模型，在工业界中使用广泛. 调研发现，绝大多数基于随机森林的 KPI 异常检测技术围绕模型结构（主要是与其他模型结合）以及异常阈值选择方面的创新来提升检测性能，随机森林模型本身只是作为一个性能良好的分类器或回归器，运用于各个异常检测方案中.

基于分类的随机森林[6,68]可以作为 KPI 异常检测的二次分类器提升检测性能. 文献 [6] 借助 14 个基本异常检测器初步学习和提取特征，并采用随机森林建立异常检测的分类模型进行二次学习，进一步提高检测准确率. 文献 [68] 利用简单的前馈神经网络分别进行标签筛选和基础分类 2 次训练，再采用随机森林对前馈神经网络识别出的异常进行小范围重学习，排除少量误报.

基于回归的随机森林[72,115]可以作为 KPI 异常检测的预测器，通过集成学习方式提高预测准确率. 文献 [115] 将包含随机森林的集成学习模型的预测结果再次输入到 4 种分类器中进行异常检测，这种叠加方式进一步提升了异常检测性能.

此外，随机森林作为一种概率模型，异常阈值的选择会直接影响模型的分类结果. 传统异常检测技术为操作方便，直接将阈值设置为 0.5 的固定值，但是这种简单设置忽略了真实场景中 KPI 数据正异样本不平衡的问题，造成准确率虚高. 一些工作[6,66]通过在检测精确率与召回率之间权衡，优化了随机森林的阈值选择机制. 例如，文献 [6] 考虑运维人员不同程度的精确率及召回率偏好，将 $F1$ 分数指标替换为 PC 分数（preference-centric score）指标，并基于 EWMA（exponentially weighted moving average）预测方法根据观察结果动态调整阈值. PC 分数指标计算为

$$PC(r,p)=\begin{cases}\dfrac{2r\times p}{r+p}+1, & r\geqslant R, p\geqslant P,\\ \dfrac{2r\times p}{r+p}, & \text{其他},\end{cases} \tag{1}$$

其中 r, p 分别表示实验过程中真实 PR 曲线中的召回率与精确率，R, P 分别表示运维人员偏好的召回率与精确率.

4.1.2 孤立森林

孤立森林[35,69]是专门设计用于异常检测任务的无监督模型，由若干二叉树组成. 其原理类似于随机森林，但每次在进行分割时，随机选择样本、特征和分割点. 由于异常点占比少、分布稀疏且距离高密度区域的正常点较远，在孤立森林中，样本越靠近根节点，越可能是异常. 文献 [69] 提出了一种改进的随机孤立森林算法用于提升 KPI 异常检测性能，改进内

容包括: 在选择切割维度时考虑特征间的最大距离, 在选择切割阈值时采用最稀疏间隔, 在计算异常分数时同时考虑节点深度等.

4.1.3 聚 类

聚类是另一种常用的无监督异常检测模型, 在用作检测器时, 通常将不属于任何集群的样本视为异常. DBSCAN(density-based spatial clustering of applications with noise)密度聚类[73-74,86,104,116]是KPI异常检测领域最常用的聚类检测器.

文献[73]采用DBSCAN密度聚类识别聚类簇外的异常, 并提出了一种基于排序 K 距离图的参数自适应方法, 优化邻域半径参数 *Eps*, 进而提升KPI异常识别准确性.

实际上, 在KPI异常检测领域, 绝大多数工作[66-67,71,117]将聚类与随机森林模型结合, 建立混合模型, 采用半监督训练方式, 仅需少量人工标注即可显著提高检测质量. 文献[71]采用一种弹性的半监督学习框架CPLE(contrastive pessimistic likelihood estimation)[118], 将半监督学习应用于KPI异常检测领域. 先是利用ROCKA聚类[86]将历史KPI划分为几个聚类簇, 并为每条聚类质心KPI随机标注少量异常. 然后将已标注的质心KPI和新加入的、未标注的KPI在提取特征后共同送入随机森林分类器进行基于CPLE的半监督训练. CPLE训练思想基于“对比”和“悲观”2个原则, 通过最大化利用无标签数据提升检测性能. 文献[66, 117]在文献[71]基础上又融合主动学习思想, 利用主动学习方式继续标注足够多的最有可能为异常的样本, 进一步优化检测效果.

4.2 深度学习模型准确性提升

近年来, 深度学习方法通过不断加深神经网络层数、优化神经网络结构, 使其对KPI依赖模式的挖掘能力不断增强, 逐渐在异常检测领域崭露头角. 不同于传统机器学习方法将异常检测任务分模块完成, 深度学习提供了一种“端到端”的训练范式, KPI依赖模式挖掘(特征提取和学习)与异常检测同时进行, 对复杂KPI中存在的多种异常类型更具检测通用性.

多层感知机(multi-layer perception, MLP)、RNN、CNN、注意力机制、AE、VAE以及GAN是KPI异常检测领域常用的深度学习模型, 基于深度学习的KPI异常检测技术通常在模型结构、目标函数、训练方式、异常分数计算方法以及阈值选择方面进行创新, 提高异常检测的准确性.

4.2.1 预测神经网络

传统时间序列异常检测中, MLP、RNN、LSTM、1维CNN等序列神经网络常作为预测模型[37,45,79-83,102,113], 使用未来预期值和实际观测值之间的预测误差来判断异常. 文献[113]利用格兰杰因果关系, 收集与待预测KPI相关的全部KPI, 然后采用基于多头注意力机制的LSTM充分挖掘多变量KPI中的历史信息, 提高了预测的准确性. 然而互联网服务场景下的KPI数据分布复杂、采样频率高且存在不确定性, 序列预测模型很难在长期模式下保持对未来正常值的准确预测. 因此, 当前研究多集中在以AE, VAE为主的重构模型的性能优化上.

4.2.2 重构神经网络

AE[48,78-79,89-91,97-100,103-105,111]通过最小化编码器输入与解码器输出之间的重构损失训练模型参数. 文献[78]采用基于随机步长连接的RNN, 构建多个不同结构的顺序自编码器, 并采用静态损失相加原则, 以集成学习的方式进行训练, 有效缓解了单个AE模型在KPI异常检测中的过拟合问题. 在此基础上进一步优化, 提出了动态平衡损失函数[79], 根据每个AE在训练过程中的损失变化率来平衡其在集成学习中的权重, 取得了更加满意的效果.

不同于AE仅最小化重构损失, VAE[38,40-41,46,56,58,87,92-96,106-108,110]在此基础上引入随机采样噪声, 最小化重构损失与相似性损失之和, 并在求解目标函数时转化为最大化似然概率的形式. 通过该过程, VAE还学习了隐变量 $\boldsymbol{z}$ 的分布, 从而能够生成新的数据, 缓解了AE在KPI异常检测任务中容易出现的过拟合问题. 文献[56]发现在基于VAE的KPI异常检测工作中, 采用正常数据与少量异常数据共同训练比仅使用正常数据训练的效果更好. 于是提出了Donut算法, 对VAE目标函数推导出的证据下界(evidence lower bound, ELBO)公式进行权重修正, 修改为

$$\tilde{L}_{\text{Donut}}=E_{q_\phi(\boldsymbol{z}|\boldsymbol{x})}\left[\sum_{w=1}^{W}\alpha_w\log p_\theta(\boldsymbol{x}_w|\boldsymbol{z})+\beta\log p_\theta(\boldsymbol{z})-\log q_\phi(\boldsymbol{z}|\boldsymbol{x})\right], \tag{2}$$

其中异常数据与缺失点的权重 a_w=0. 该思想使得VAE可以在异常窗口内重建正常数据模式, 以获得更加准确的检测结果. 但是Donut的问题在于它所采用的VAE未使用序列结构, 在训练时会将KPI窗口的顺序打乱, 影响长期时序依赖挖掘, 进而限制了检测准确性的提升. 因此, 文献[92]在Donut基础上提出了Bagel, 一种基于条件VAE(conditional VAE, CVAE)[119]的KPI异常检测算法, 将时间信息作为外部条件输入到VAE中, 并通过额外的Dropout层, 避免在拟合

时间信息与KPI数据之间的关系时发生过拟合. 为了进一步修正训练过程中异常数据给VAE模型带来的偏差, 文献 [93] 提出了一种基于因果关系的异常去偏机制, 通过切断从异常标签到输入数据的因果路径, 在编码过程中即可消除异常数据影响. 该方案已成功应用于Donut和Bagel模型中, 将其$F1$分数提高了5%.

然而, 由于训练方式及神经网络表达能力的限制, 上述工作在KPI复杂经验分布上的训练性能仍然较低且不稳定. 为了解决此类问题, 一般考虑5种优化方式:

1)采用由粗到精(coarse to fine, CTF)的微调策略. 文献 [38] 首先采用VAE训练一个粗粒度的检测模型, 其中VAE的层结构由多层RNN与密集层组成. 其次, 利用层次聚类对粗训练后的数百万个机器KPI降维, 形成若干聚类簇. 随后, 再对每个簇的KPI采样, 以增量学习的方式微调每个簇的粗粒度模型, 并在微调时固定浅层RNN参数, 保持模型泛化. 实验证明, 这种由粗到精的微调策略实现了比单一模型(每台机器单独训练1个模型)或整体模型(所有机器共同训练1个模型)更好的可扩展性和准确性.

2)采用生成对抗网络(generative adversarial network, GAN)中的对抗式训练思想. 在KPI异常检测中, GAN模型通常与重构模型结合使用[46,104, 106,120], 以减轻模式崩溃现象对GAN生成器在模拟真实分布时的干扰, 同时提升重构检测模型在复杂KPI上的训练稳定性. 文献 [106] 将GAN与VAE结合, 提出了第一个针对复杂KPI建模的无监督异常检测算法Buzz. Buzz选择WGAN(Wasserstein GAN)[121]结构作为对抗式训练的主体, 并将其中的生成器替换为VAE, 用于生成重构的“假数据”. 再利用梯度惩罚技术[122]和贝叶斯正则项, 修改其目标函数, 以保证对抗训练的准确性及稳定性. 文献 [46, 104] 进一步强化对抗式训练在复杂KPI上的鲁棒性优势, 建立双层GAN结构, 将VAE或AE编码器输出的隐变量和解码器输出的重构数据作为不同的生成数据, 分别输入到2个判别器中.

除了直接使用GAN, 文献 [89] 则是借鉴GAN的思想, 通过构建共享单一编码器的2个AE结构, 形成二者对抗. 实验证明, 该网络结构能够学习如何放大包含异常输入的重构误差, 检测准确性更高且相较于普通GAN结构更加稳定. 文献 [97] 提出了类似的对抗式单编码器-双解码器结构, 同时引入Transformer在编码过程中提升学习性能.

3)采用图结构挖掘深层次度量依赖. 文献 [123] 将多变量KPI转换为图结构, 每个KPI代表图上的1个节点, 然后利用图注意力网络学习更深层次的度量依赖, 并成功应用于基于预测和重构的异常检测模型中, 提高了基线模型(如Donut[56])的$F1$分数.

4)采用正异模式可区分的关联差异思想. 基于单一重构模型的时间序列异常检测技术在建模时容易被正常数据主导, 从而忽略异常模式信息, 影响检测性能. 文献 [98] 观察到, 正常点通常与整个序列的所有数据点建立相对均匀的关联关系, 而异常点仅与邻域点相关. 于是, 引入基于双分支结构的Transformer, 分别利用高斯核和自注意力机制提取关注邻域区域的先验关联(prior-association)和原始序列关联(series-association), 然后将先验关联分布与序列关联分布之间的对称KL散度作为关联差异, 确保正常点的关联差异较大. 最后优化目标函数, 在最小化重构损失基础上, 尽可能放大关联差异, 使得异常的重构更加困难, 从而更容易被识别出来. 文献 [99] 在此基础上, 利用掩码机制(mask mechanism)继续放大正异模式间的差异, 与文献 [98] 相比, 识别出了更多的异常.

5)采用半监督修正策略. 文献 [96] 采用伪标签学习方式, 在Donut基础上引入一个半监督分类器对数据进行预测, 并将编码的隐变量与预测的伪标签一起输入到解码器中进行解码重构, 大大提升了无监督VAE对于异常识别的准确性, 且有效缓解了对原始标注数据的依赖. 文献 [94] 是将主动学习思想纳入VAE检测模型的工作, 首先采用基于多种集成查询策略(top-k采样、不确定性采样和间隔随机采样)的主动学习方法, 为VAE模型提供少量数据标签. 然后设计了3种基于标签信息的反馈策略(分母惩罚、负惩罚和基于伪标签的度量学习)优化检测模型, 并将VAE模型的目标函数修改为重构损失、相似性损失和度量损失之和. 其中, 分母惩罚和负惩罚策略显式利用标签信息, 使得异常样本具有较大的重构损失L_{recon}, 而基于伪标签的度量学习则通过控制样本在潜在空间上的类内和类间距离, 增加异常样本的度量损失L_{metric}.

在异常分数计算方面, 重构神经网络一般直接采用重构损失(包括重构误差形式和重构概率形式)作为异常分数. 为了优化异常分数计算方法, 进一步提升检测性能, 文献 [89, 97, 104] 设计了基于重构误差与对抗误差融合的计算方法 , 而文献 [98] 则设计了基于关联差异标准化的重构误差计算方法.

在异常阈值选择方面, 相关工作的常用做法大致可以分为 2 派: 1)实验派[40,56,58,89,91-93,95,105-106]. 选取小部分数据作为验证集, 枚举所有可能的阈值逐一实验, 然后计算与其对应的 $F1$ 分数指标, 并选择最佳 $F1$ 分数对应的阈值作为最终阈值. 2)算法派[38,41,78-79,87,97,110]. 一般采用时间序列异常检测领域常用的 POT(peaks-over-threshold)或 SPOT(streaming peaks-over-threshold)算法[124], 自动选择阈值.

表 7 总结了以准确性目标为核心的 KPI 异常检测主要研究工作, 内容包括代表性工作、主要模型以及准确性提升方式. 基于传统机器学习(如随机森林、孤立森林和聚类)的检测技术对异常结果的可解释性强, 但检测效率低, 检测精度严重依赖于特征提取的好坏. 基于深度学习的检测技术检测通用性强, 但可解释性差. 这 2 类方法在实际应用时均存在不足.

Table 7 Accuracy-Centric KPI Anomaly Detection Techniques

表 7 以准确性目标为核心的 KPI 异常检测技术

代表性工作	主要模型	准确性提升方式
文献 [6]	随机森林分类	利用随机森林分类进行二次学习, 设计动态阈值②④
文献 [68]	随机森林分类	利用随机森林分类进行二次学习②
文献 [115]	随机森林回归	集成学习②
文献 [69]	孤立森林	改进孤立森林中的切割算法③
文献 [66]	混合模型(聚类+随机森林)	利用主动学习修正错误结果②③④
文献 [67]	混合模型(聚类+随机森林)	提取多角度特征①②
文献 [71]	混合模型(聚类+随机森林)	引入半监督学习框架 CPLE②③
文献 [117]	混合模型(聚类+随机森林)	无监督聚类直接推导随机森林的决策规则, 利用主动学习修正错误结果②③
文献 [113]	预测神经网络	采用基于多头注意力机制的 LSTM③
文献 [78]	重构神经网络	集成学习②
文献 [56]	重构神经网络	通过修正异常数据权重去除异常偏差③
文献 [92]	重构神经网络	引入额外的时间信息输入至 VAE (CVAE)②
文献 [79]	重构神经网络	集成学习, 采用动态平衡损失函数②③④
文献 [93]	重构神经网络	通过切断异常标签到输入的因果路径去除异常偏差③
文献 [38]	混合模型(重构神经网络+聚类)	利用聚类实现检测模型由粗到精地微调②④
文献 [46]	对抗式重构神经网络	采用双层 GAN+VAE, 对目标函数进行显式地对抗正则化处理②③
文献 [106]	对抗式重构神经网络	采用 WGAN+VAE, 利用梯度惩罚以及贝叶斯正则项修改目标函数②③
文献 [89]	对抗式重构神经网络	采用基于对抗式训练思想的双层解码器 AE②③④
文献 [97]	对抗式重构神经网络	采用基于对抗式训练思想的双层解码器 AE, 引入 Transformer 层②③④
文献 [104]	对抗式重构神经网络	采用双层 GAN+AE②③④
文献 [123]	图注意力+重构神经网络	采用图结构挖掘深层次度量依赖②
文献 [98]	基于关联差异的重构神经网络	采用基于关联差异思想的 Transformer 变体③④
文献 [96]	半监督重构神经网络	伪标签学习③
文献 [94]	半监督重构神经网络	利用主动学习修正错误结果及目标函数②③

检测技术准确性提升方式可概括为 4 种: ①人工提取高质量特征; ②完善模型结构; ③优化目标函数或改进训练方式; ④调整异常计算方法或阈值选择机制.

5 以多目标平衡为核心的 KPI 异常检测技术

为实现 KPI 异常检测技术在真实场景中的高可用性, 仅仅专注于理论层面的研究不足以解决实际面临的应用问题. 因此, 越来越多的 KPI 异常检测技术从服务场景的应用目标出发, 确保检测准确性在可接受范围内的同时, 平衡其他应用性指标. 然而, 互联网服务是一个相当庞杂的概念, 根据网络架构、部署环境、服务对象、网络连接方式等诸多方面的不同可以划分出多种互联网服务, 不同服务甚至同一服务在不同时期或不同监控层面中的异常检测应用目标可能相差很大. 本节基于常见的互联网服务, 分别针对鲁棒性目标、实时性目标和可解释性目标 3 种典型应用目标介绍以多目标平衡为核心的 KPI 异常检测技术.

5.1 平衡准确性与鲁棒性

一般而言, 真实的服务运行环境远比实验环境更加复杂, 异常检测过程应当保持良好的鲁棒性, 以抵抗复杂环境的干扰. 除模型自身结构鲁棒外, 影响 KPI 异常检测技术鲁棒性的主要因素有 2 点: 1)数据采集中的错误及噪声数据; 2)时间序列的“概念漂移”现象. 因此, 本节分别从这 2 点展开介绍平衡准确性与鲁棒性的 KPI 异常检测技术.

5.1.1 数据清洗

数据采集通常是一个松散的控制过程[125], 常常导致数据存在噪声、缺失以及不可靠等情况. 例如, 物联网服务中恶劣的传感器部署环境经常造成数据丢失或读数错误, 这些未经筛选的数据会严重干扰正常的预测方向. KPI 异常检测工作中常采用缺失值填补的方式清洗错误数据, 具体填补方法参考表 8. 另外, 某些基于重构模型的工作[37,46] 为保证重构学习的准确性(即仅学习正常分布), 还会采用 SR 模型提前清洗掉数据集中的异常.

5.1.2 快速适应“概念漂移”现象

由于互联网服务产生的 KPI 数据都是动态到达的时间序列, 其统计属性常常随着时间推移朝某一方向变化, 从而可能引起数据标签的改变, 即“概念

Table 8 Common Imputation Methods for Missing Values

表 8 常用缺失值填补方法

代表性工作	缺失值填补方法
文献 [38]	采用前一个观测值填补缺失位置
文献 [40,56,106]	采用 MCMC（Markov chain Monte Carlo）插补法填补缺失位置
文献 [35,77–79,86–87]	采用线性插值法根据邻居点填补缺失位置
文献 [73]	采用缺失点所在滑动窗口的平均值填补缺失位置

漂移”现象. 然而，“概念漂移”对数据标签的影响在不同情况下有所不同. 例如，在某些软件服务中，服务器故障和软件变更均可能导致页面浏览量指标的显著变化，前者是一种意外的异常，数据标签发生改变，而后者则是预期事件下的正常表现，数据标签保持不变，这种预期事件所造成的“概念漂移”给异常检测工作带来了强烈的噪声干扰. 文献 [73] 通过提取差异特征代替基于原始特征分布的学习，天然地避免了“概念漂移”的影响. 文献 [70] 直接使用去趋势成分的KPI进行异常检测，避免错误地识别由趋势变化所引起的“概念漂移”. 文献 [114] 采用双重差分模型判断“概念漂移”的正确分类. 文献 [117] 提出了一种基于邻域的新概念，即逆最近邻，通过计算每个KPI数据点逆最近邻的统计属性分数，区分KPI数据中的正常、预期“概念漂移”与异常. 而文献 [91] 则通过在滑动窗口中采用一小段检测延迟换取对预期“概念漂移”的正确识别.

5.2 平衡准确性与实时性

一些大规模在线软件服务（尤其是移动互联网服务）或某些工业互联网服务场景（如智能电网等）非常注重服务实时性，通常要求其运维系统能够实时处理海量KPI数据中的异常，从而避免服务功能停滞.

KPI异常检测技术的实时性指在一定时效范围内发现异常的能力. 在不考虑运维成本的理想情况下，这种实时检测能力可以直接用检测效率或可接受延迟内的漏报率衡量，检测效率高且漏报率低，则实时性高. 然而，低漏报率意味着异常检测模型高度敏感，代价是产生大量误报. 由于真实场景下运维人力有限，频繁的告警容易引起告警消息阻塞，许多真正的异常隐匿其中而被忽略，反过来增加了发现异常的时间，甚至是升高了漏报率. 因此，告警频率是影响KPI异常检测技术实时性的间接因素. 为加强KPI异常检测的实时性，研究人员一般从提高检测效率、降低漏报率及减小告警频率3个方面入手.

5.2.1 提高检测效率

检测延迟是反映模型检测效率的直接指标，检测延迟越小表示检测效率越高. 文献 [6] 指出基于机器学习方法的检测延迟由特征提取时间和分类时间组成，其中分类时间远小于特征提取时间，我们将其统称为计算时间. 除此之外，在当前互联网服务普遍采用的分布式架构下，数据通信时间也成为检测延迟的另一重要组成部分. 因此，提升模型检测效率（即降低检测延迟）的主要方式有提高运算速度[35,49,73,82,86,111,117]、多节点并行计算[38,88,111]、减少通信量[76]等.

1）时间复杂度是描述模型计算量的时间度量，时间复杂度越低，运算速度越快，所消耗的计算时间越少. 文献 [111] 利用Chebyshev多项式递归计算GCN卷积核，减轻了GCN中对拉普拉斯矩阵进行特征分解的计算成本，将其时间复杂度从 $O(n^2)$ 降低到线性时间. 文献 [49] 提出了一种基于核密度估计（kernel density estimation, KDE）的自适应KPI异常检测算法，该方法通过树型结构KD-Trees实现密度估计，并将运算的时间复杂度从原始KDE方法的二次时间降低到 $O(n\log n)$. 文献 [73, 82] 分别通过子采样技术和调整KPI窗口大小来控制KPI的数量或长度，同样降低了KPI异常检测技术的时间复杂度. 文献 [73] 还认为，对于传统机器学习模型来说，过度提取特征会增加不必要的时间和内存消耗，于是仅提取一阶差分和二阶差分2个差异特征作为KPI数据的最终表示.

2）并行计算以“空间换时间”的折中策略缩短计算时间. 文献 [38] 采用了由粗到精的微调策略，在微调模型期间，利用6台CPU服务器并行计算，大大节省了计算时间. 文献 [111] 则是允许以并行方式对多变量KPI进行编码，同样节省了计算时间.

3）分布式场景下，将检测模型部署在某一中心服务器并以集中方式处理KPI数据，会使得各节点与中心节点间的数据通信时间急剧增加. 文献 [76] 为提高传感器网络中异常检测的实时性，将异常检测任务直接部署在边缘层设备，有效减少了与云服务器间的数据通信量，该思路同样可以应用于边缘网络场景下的KPI异常检测任务.

5.2.2 降低漏报率

文献 [56] 提出了一种可接受延迟内的性能计算调整方法. 可接受延迟一般是指可接受的告警延迟，当告警延迟在可接受范围内时，认定该异常段中所有异常点被检测到. 因此，该技术更关心连续异常段中的检测性能，设置可接受延迟能有效降低检测漏

报率. 实验证明, 该计算方式更能满足实际应用中的运维需求. 最后还比较了 VAE 模型 Donut[56] 和随机森林模型 Opprentice[6] 在 3 个真实 KPI 异常检测数据集上的平均告警延迟, 两者的延迟均在可接受范围内, 但 Donut 的召回率更高, 即漏报率低, 说明深度神经网络模型对 KPI 中的异常更加敏感.

5.2.3 减小告警频率

告警频率高可能导致异常检测实时性能下降. 引起告警频率高的主要因素在于重复告警或误报过多, 为了解决这 2 个问题, 相关研究工作分别采用了以下 2 种方法:

1)真实场景中, 异常通常以事件形式出现, 即连续异常, 一些网络抖动引起的瞬时异常一般无需处理. 因此, 对异常点逐一执行告警会生成大量重复或不必要的告警消息. 文献 [38] 设计了一种简单的告警策略, 即至少连续检测到 5 个异常点时触发警报, 减少了 KPI 异常检测中的重复告警情况.

2)文献 [80] 利用贝叶斯神经网络捕获预测的不确定性估计. 在 KPI 异常检测任务中, 预测区间构造为 $\left[\hat{y}^*-z_{\alpha/2}\eta,\hat{y}^*+z_{\alpha/2}\eta\right]$, 其中 $\alpha=0.05$, $z_{\alpha/2}$ 表示标准正态分布的 α 上分位数, η 表示预测的不确定性误差. 当观测值落在预测区间之外时触发警报. 实验证明, 这种对预测的不确定性估计仅增加了少量计算开销, 但有效减少了异常检测过程中产生的误报, 进而减小了告警频率.

另外, 文献 [103] 提出了一种可以同时衡量检测准确性与实时性的新指标, 称为序列精度延迟 (sequence precision delay, *SPD*). 类似于 *AUC*, *SPD* 量化了以归一化平均检测延迟为横坐标、以精确率为纵坐标的感受性曲线下方面积. *SPD* 越接近于 1, 表示告警越具有高精度和低延迟.

5.3 平衡准确性与可解释性

当前安全敏感型任务(如医疗诊断、自动驾驶、智能运维等)对于可解释性的需求越来越强烈. 可解释性是模型的一种固有属性, 包括对模型内部机制的理解以及对模型结果的解释. KPI 异常检测技术中的可解释性目标即帮助运维人员理解检测到的异常. KPI 异常检测模型按照模型自身是否可解释分为“白盒”检测模型和“黑盒”检测模型.

“白盒”模型是指具有良好内在可解释性的简单模型, 如线性模型、决策树模型等. 文献 [69] 利用基于孤立森林的“白盒”检测模型, 解释异常的生成原因, 并为后续的主动学习组件提供了每个样本的重要性.

深度学习模型是典型的“黑盒”模型[126], 其运作方式掩盖了学习中基本的逻辑及推理机制, 无法对决策结果进行合理解释. 因此, 越来越多的基于深度学习的 KPI 异常检测技术[40-41,46] 开始引入异常解释, 将平衡准确性与可解释性作为目标, 使其在检测异常的同时让运维人员理解并采纳其结论, 加快后续的故障排除速度并提高模型的迁移能力.

当前基于深度学习的 KPI 异常检测技术一般使用基于样本实例的局部解释方法, 在训练好的模型中提取逻辑规则, 帮助运维人员理解单个样本的异常结果. 基于重构模型的异常检测逻辑规则指的是: 通过计算多变量 KPI 中每个变量对整体重构损失的贡献, 将贡献高的 KPI 变量解释为异常发生的原因. 贡献计算方法如表 9 所示.

Table 9 Contribution Computing Methods of KPI Anomaly Interpretation

表 9 KPI 异常可解释性的贡献计算方法

代表性工作	贡献计算
InterFusion[40]	重构概率分量 $S_t^i=\frac{1}{L}\sum_{l=1}^{L}\left[\log p_\theta\left(x_t^i\middle\vert z_1^{(l)},z_2^{(l)}\right)\right]$
OmniAnomaly[41]	重构概率分量 $S_t^i=\log p_\theta\left(x_t^i\middle\vert z_{t-T:t}\right)$
DAEMON[46]	重构误差分量 $S_t^i=\left\Vert x_t^i-x_t^{i'}\right\Vert_1$

文献 [41] 提出了关于多变量 KPI 异常检测问题的可解释性方法. 对于每个被检测到的异常, 将每个度量变量在 VAE 中的重构概率分量作为其异常解释. 然而, 多变量 KPI 中各度量变量间相互依赖, 因此异常度量可能引起其他正常度量的重构偏差, 影响贡献计算. 于是文献 [40] 利用 MCMC 插补法在含有异常的多变量 KPI 中尽可能合理重建正常数据模式, 并根据修正后的重构概率解释异常. 具体可解释性评价指标参考表 3.

表 10 总结了以多目标平衡为核心的 KPI 异常检测主要研究工作, 内容包括代表性工作、主要应用目标以及性能优化方式.

6 挑战与展望

随着云计算的发展及云原生概念的提出, 互联网服务部署上云已经成为大势所趋. 真正的服务云化不仅表现在物理资源部署在云端, 更重要的是整个应用的开发及运维管理方式都要基于云的思路转变, 最终达成对云端资源的充分利用. 面对当前不断变化的云运维环境, KPI 异常检测技术中还存在许多

Table 10 Multi-Objective Balancing-Centric KPI Anomaly Detection Techniques

表 10 以多目标平衡为核心的KPI异常检测技术

代表性工作	主要应用目标	性能优化方式
文献 [37]	鲁棒性	SR模型清洗异常①
文献 [72]	鲁棒性	去除KPI中的趋势成分②
文献 [91]	鲁棒性	在滑动窗口中采用一小段检测延迟②
文献 [117]	鲁棒性	采用逆最近邻区分预期“概念漂移”与异常②
文献 [114]	鲁棒性	采用双重差分模型判断“概念漂移”正确分类②
文献 [30]	鲁棒性、实时性	缺失值填补，并行计算，连续检测到5个异常点触发告警①③⑤
文献 [56]	鲁棒性、实时性	缺失值填补，提出一种可接受延迟内的性能计算调整方法降低漏报率①④
文献 [73]	鲁棒性、实时性	缺失值填补，提取差异特征代替基于原始特征的学习，调整子采样技术以降低时间复杂度，仅提取一阶、二阶差分特征以减少不必要的时间和内存消耗①②③
文献 [103]	实时性	提出一种同时衡量检测延迟和精确率的新指标③
文献 [49]	实时性	采用基于KD-Trees的核密度估计降低时间复杂度③
文献 [82]	实时性	调整KPI窗口大小（控制样本长度）以降低时间复杂度③
文献 [111]	实时性	并行编码，利用Chebyshev多项式降低时间复杂度③
文献 [76]	实时性	将异常检测任务部署在边缘设备以减少通信量③
文献 [80]	实时性	利用贝叶斯网络捕获预测的不确定性估计以减少误报⑤
文献 [40]	鲁棒性、可解释性	缺失值填补，采用基于特征重要性的局部解释方法①⑦
文献 [46]	鲁棒性、可解释性	SR模型清洗异常，采用基于特征重要性的局部解释方法①⑦
文献 [41]	可解释性	采用基于特征重要性的局部解释方法⑦
文献 [69]	可解释性	采用基于孤立森林的“白盒”模型（实现内在可解释性）⑥

检测技术性能优化方式可细分为7种：①数据清洗；②快速适应“概念漂移”；③提高检测效率；④降低漏报率；⑤减小告警频率；⑥“白盒”检测模型；⑦事后解释方法.

问题值得进一步研究.本文总结出5项挑战并提出了未来研究方向.

1)KPI监控及预处理的难度增大

当前互联网企业倾向采用混合云及多云策略部署服务,以提升服务的可靠性、安全性、可扩展性等多元化需求.然而复杂异构的部署环境同时也在放大互联网服务运维中KPI监控及预处理的压力:①云环境下,企业获得的公共云信息有限,其服务运维很大程度依赖于云提供商,多云平台中各个云提供商的监控接口不统一,导致企业对其服务的监控能力降低,监控灵活性较差;②多云模式造成数据隔离问题,使得监控到的KPI在采样频率、形态特点等方面存在较大差异,增加了KPI预处理工作的难度.

因此,针对多源监控数据进行统一实时监控,一致且高效地定义和提取跨数据源的KPI,开发可靠的整体监控管理工具,仍然是当前领域亟待解决的问题.对于跨源的不规则KPI,当前所使用的归一化及对齐处理方法较为简单,针对不规则KPI的预处理技术将是未来重要的研究方向.

2)模型通用性有待提高

部署在云上的互联网服务场景模式多样,进而监控到的KPI具有多种形态,因此,KPI异常检测技术的通用性对于方案的实际推广具有重要意义.限制KPI异常检测技术通用性的主要原因在于:①当前绝大多数KPI异常检测工作采用私有数据集训练模型,数据采集范围有限导致KPI行为模式(特别是异常模式)涵盖不全;②大规模互联网服务动态运行过程中监控到的KPI通常表现出复杂的噪声,异常数据常常隐匿于噪声中不易被发现,尽管深度学习方法在KPI异常检测中表现出强大的学习能力,然而多数方法通过捕捉正常KPI模式,反向推导异常,从而忽略了异常模式的学习.

因此,当前该领域迫切需要构建大规模、多样化的KPI异常检测公开数据集.除此之外,通过主动学习、解耦学习等方式学习KPI中的异常模式,更加清晰地捕捉正常模式与异常模式之间的区别,将是未来KPI异常检测模型的一个主要设计思路.

3)模型可解释性的研究不全面

研究KPI异常检测技术的可解释性能够帮助运维人员理解技术难点并快速响应告警事件,这对于优化检测技术、维护服务的稳定性至关重要.5.3节中提到,当前已有部分KPI异常检测工作将模型可解释性作为一项重要研究目标.然而相关工作还处于初步研究阶段,当中存在2个关键问题:①目前KPI异常检测技术的可解释性研究仅采用简单的基于样本实例的局部解释方法,即对单个异常结果做出解释,分析最有可能导致该观测值被判定为异常的KPI变量,却并未在检测模型角度解释,KPI异常可能具备怎样的输入特征,其解释的完整性、稳定性及真实性有待验证;②目前KPI异常检测工作中还没有统一的可衡量模型可解释性效果的评价原则或指标.

采用更加可靠的事后解释模型(如线性代理模型等)或设计符合KPI异常检测任务的内在解释模型(如注意力机制网络等),并制定统一的评价指标,全面分析模型机制及异常结果的可解释性,将是完善KPI异常检测技术可解释性目标的主要方向.

4)异常告警管理机制过于简单

现有的KPI异常检测技术主要关注如何准确发

现更多的异常,而忽视了如何将发现的异常信息有效地转化为后续任务(如异常定位、根因分析等)的输入,这种转化工作可以通过优化告警管理机制实现.当前工作中采用简单且固定的告警管理机制,实用性差,主要原因在于:①服务运行环境的动态性以及运维人力的有限性要求我们设计更加弹性高效的告警管理机制;②目前云环境下普遍采用分布式架构或微服务架构,将单体应用分解成多个子服务独立部署、编译和运行,各级子服务间复杂的依赖关系使得告警关联困难.例如,不同子服务中的KPI可能呈现错峰异常,但根因实际指向同一目标,我们不能仅凭告警时间将异常信息关联在一起.

因此,针对不同异常告警进行动态分级以及实时调整告警规则等,是完善KPI异常检测技术中告警管理机制的主要方式,也是提升KPI异常检测技术实用性的关键.另外,如何选择合适的角度(如度量角度、KPI异常类型角度、微服务调用结构角度等)及方法对异常告警进行关联分析,未来还需进一步扩大研究.

5)KPI异常检测任务的局限性

面对大规模且日益复杂的互联网服务,监控KPI所获得的信息十分有限,在当前普遍采用的微服务架构中,某些KPI还会容易受到跟踪(trace)链差异的影响,进而干扰异常检测结果.例如,服务的响应时间指标可能受跟踪链长度或微服务调用结构的影响,在不同跟踪链中具有不同分布;又或是,在同一跟踪链中,微服务的响应时间指标可能由于调用该服务的父节点不同,同样存在不同分布.

因此,无论是在服务级还是微服务级层面,KPI均有可能受到跟踪链影响,造成检测误判.利用跟踪链数据辅助的KPI异常检测技术将得到广泛关注.

7 结束语

随着人工智能等技术的发展,互联网服务运维也在朝智能化方向转变.本文聚焦KPI异常检测这项互联网服务智能运维中的基础支撑技术,从机器学习模型选择动机及检测性能目标角度全面梳理了当前互联网服务场景下基于机器学习的KPI异常检测工作.我们发现,当前研究主要从KPI依赖模式挖掘的角度出发,选择合适的机器学习模型,然后通过多种方式进一步优化,提升检测准确性及其他应用性指标.通过分析当前技术及环境的发展变化,我们认为规范统一、通用、可解释、弹性告警管理以及利用跟踪链数据辅助的KPI异常检测技术将是该领域未来很长一段时间内的研究重点.

作者贡献声明: 尚书一负责论文调研、整理和撰写工作;李宏佳辅助论文设计,并提供了关于论文主题、框架和内容等方面的指导意见;宋晨、卢至彤、王利明、徐震对论文内容和结构进行了讨论,并提出了修改及指导意见.

参 考 文 献

[1] Han Yanbo, Zhao Zhuofeng. Aggregating, operating, sharing and utilizing Internet-based services with the VINCA approach[C]//Proc of the 12th Asia-Pacific Web Conf. Piscataway, NJ: IEEE, 2010: 398−398

[2] Ono E, Ikkatai Y. Internet-based services to obtain information on science and technology according to the degree of interest[C]//Proc of the 9th Int Congress on Advanced Applied Informatics (IIAI-AAI). Piscataway, NJ: IEEE, 2020: 328−331

[3] Wu Jianping, Lin Song, Xu Ke, et al. Advances in evolvable new generation Internet architecture[J]. Chinese Journal of Computers, 2012, 35(6): 1094−1108 (in Chinese)
(吴建平, 林嵩, 徐恪, 等. 可演进的新一代互联网体系结构研究进展[J]. 计算机学报, 2012, 35(6): 1094−1108)

[4] Xu Ke, Zhu Min, Lin Chuang. Internet architecture evaluation models, mechanisms and methods[J]. Chinese Journal of Computers, 2012, 35(10): 1985−2006 (in Chinese)
(徐恪, 朱敏, 林闯. 互联网体系结构评估模型、机制及方法研究综述[J]. 计算机学报, 2012, 35(10): 1985−2006)

[5] Gartner. The cost of downtime[EB/OL]. (2014-07-16)[2023-03-30]. https://www.loadbalancer.org/blog/how-to-calculate-the-cost-of-downtime-to-your-organization

[6] Liu Dapeng, Zhao Youjian, Xu Haowen, et al. Opprentice: Towards practical and automatic anomaly detection through machine learning[C]//Proc of the 2015 ACM/SIGCOMM Conf on Internet Measurement Conf. New York: ACM, 2015: 211−224

[7] Mekuria R, McGrath M J, Riccobene V, et al. Automated profiling of virtualized media processing functions using telemetry and machine learning[C]//Proc of the 9th ACM Multimedia Systems Conf. New York: ACM, 2018: 150−161

[8] Pei Dan, Zhang Shenglin, Pei Changhua. AIOps based on machine learning[J]. Communications of the CCF, 2017, 13(12): 67−73 (in Chinese)
(裴丹, 张圣林, 裴昶华. 基于机器学习的智能运维[J]. 中国计算机学会通讯, 2017, 13(12): 67−73)

[9] Gartner. AIOps (Artificial Intelligence for IT Operations)[EB/OL]. [2024-12-13]. https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations

[10] Ho T K. Random decision forests[C]//Proc of the 3rd Int Conf on

Document Analysis and Recognition. Piscataway, NJ: IEEE, 1995: 278−282

[11] Breiman L. Bagging predictors[J]. Machine Learning, 1996, 24(2): 123−140

[12] Ester M, Kriegel H P, Sander J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise[C]//Proc of the 2nd Int Conf on Knowledge Discovery and Data Mining. Palo Alto, CA: AAAI, 1996: 226−231

[13] Kriegel H P, Kröger P, Sander J, et al. Density - based clustering[J]. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2011, 1(3): 231−240

[14] LeCun Y, Bottou L, Bengio Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278−2324

[15] Elman J L. Finding structure in time[J]. Cognitive Science, 1990, 14(2): 179−211

[16] Le Q V, Jaitly N, Hinton G E. A simple way to initialize recurrent networks of rectified linear units[J]. arXiv preprint, arXiv:1504.00941, 2015

[17] Hochreiter S, Schmidhuber J. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735−1780

[18] Chung Junyoung, Gulcehre C, Cho K H, et al. Empirical evaluation of gated recurrent neural networks on sequence modeling[J]. arXiv preprint, arXiv:1412.3555, 2014

[19] Rumelhart D E, Hinton G E, Williams R J. Learning representations by back-propagating errors[J]. Nature, 1986, 323(6088): 533−536

[20] Kingma D P, Welling M. Auto-encoding variational bayes[J]. arXiv preprint, arXiv:1312.6114, 2014

[21] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative adversarial networks[J]. arXiv preprint, arXiv:1406.2661, 2014

[22] Mnih V, Heess N, Graves A. Recurrent models of visual attention[C]// Proc of the 28th Int Conf on Neural Information Processing Systems. Cambridge, MA: MIT, 2014: 2204−2212

[23] Bahdanau D, Cho K, Bengio Y. Neural machine translation by jointly learning to align and translate[J]. arXiv preprint, arXiv:1409.0473, 2015

[24] Parikh A P, Täckström O, Das D, et al. A decomposable attention model for natural language inference[C]//Proc of the 2016 Conf on Empirical Methods in Natural Language. Stroudsburg, PA: ACL, 2016: 2249−2255

[25] Cheng Jianpeng, Dong Li, Lapata M. Long short-term memory-networks for machine reading[C]//Proc of the 2016 Conf on Empirical Methods in Natural Language. Stroudsburg, PA: ACL, 2016: 551−561

[26] Lin Zhouhan, Feng Minwei, Santos C N, et al. A structured self-attentive sentence embedding[C/OL]//Proc of the 5th Int Conf on Learning Representations (Poster). New York: OpenReview. net, 2017[2024-01-24]. https://openreview.net/forum?id=BJC_jUqxe

[27] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]//Proc of the 31st Int Conf on Neural Information Processing Systems. Cambridge, MA: MIT, 2017: 5998−6008

[28] Zhou Haoyi, Zhang Shanghang, Peng Jieqi, et al. Informer: Beyond efficient transformer for long sequence time-series forecasting[C]// Proc of the 35th AAAI Conf on Artificial Intelligence. Palo Alto, CA: AAAI, 2021: 11106−11115

[29] Veličković P, Cucurull G, Casanova A, et al. Graph attention networks[J]. arXiv preprint, arXiv:1710.10903, 2017

[30] Qian Ji, Zeng Guangfu, Cai Zhiping, et al. A survey on anomaly detection techniques in large-scale KPI data[C]//Proc of the 9th Int Conf on Computer Engineering and Networks. Berlin: Springer, 2021: 767−776

[31] He Shiming, Yang Bo, Qiao Qi. Overview of key performance indicator anomaly detection[C/OL]//Proc of the 2021 IEEE Region 10 Symp (TENSYMP). Piscataway, NJ: IEEE, 2021[2024-03-09]. https://ieeexplore.ieee.org/abstract/document/9550989

[32] Wang Su, Lu Hua, Wang Shuo, et al. Research progress of KPI anomaly detection in intelligent operation and maintenance[J]. Telecommunications Science, 2021, 37(5): 42−51 (in Chinese)
(王速, 卢华, 汪硕, 等. 智能运维中KPI异常检测的研究进展[J]. 电信科学, 2021, 37(5): 42−51)

[33] Chen E Y, Tsay R S, Chen Rong. Constrained factor models for high-dimensional matrix-variate time series[J]. arXiv preprint, arXiv: 1710.06075, 2017

[34] Wu Husheng. A survey of research on anomaly detection for time series[C]//Proc of the 13th Int Computer Conf on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). Piscataway, NJ: IEEE, 2016: 426−431

[35] Zhao Nengwen, Zhu Jing, Liu Rong, et al. Label-less: A semi-automatic labelling tool for KPI anomalies[C]//Proc of the 38th IEEE Conf on Computer Communications (INFOCOM). Piscataway, NJ: IEEE, 2019: 1882−1890

[36] Laptev N, Amizadeh S, Flint I. Generic and scalable framework for automated time-series anomaly detection[C]//Proc of the 21st ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2015: 1939−1947

[37] Ren Hansheng, Xu Bixiong, Wang Yujing, et al. Time-series anomaly detection service at Microsoft[C]//Proc of the 25th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2019: 3009−3017

[38] Sun Ming, Su Ya, Zhang Shenglin, et al. CTF: Anomaly detection in high-dimensional time series with coarse-to-fine model transfer[C/OL]//Proc of the 40th IEEE Conf on Computer Communications (INFOCOM). Piscataway, NJ: IEEE, 2021[2024-03-09]. https://ieeexplore.ieee.org/document/9488755

[39] Gama J, Zliobaite I, Bifet I, et al. A survey on concept drift adaptation[J]. Computing Surveys, 2014, 46(4): 1−37

[40] Li Zhihan, Zhao Youjian, Han Jiaqi, et al. Multivariate time series anomaly detection and interpretation using hierarchical inter-metric and temporal embedding[C]//Proc of the 27th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2021: 3220−3230

[41] Su Ya, Zhao Youjian, Niu Chenhao, et al. Robust anomaly detection

for multivariate time series through stochastic recurrent neural network[C]//Proc of the 25th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2019: 2828−2837

[42] 2018AIOps. The AIOps dataset [EB/OL]. [2023-03-30]. https://github.com/NetManAIOps/KPI-Anomaly-Detection?tab=readme-ov-file

[43] Lavin A, Ahmad S. Evaluating real-time anomaly detection algorithms – The Numenta anomaly benchmark[C]//Proc of the 14th IEEE Int Conf on Machine Learning and Applications (ICMLA). Piscataway, NJ: IEEE, 2015: 38−44

[44] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey[J]. ACM Computing Surveys, 2009, 41(3): 1−58

[45] Chen Xu, Qiu Qiu, Li Changshan, et al. GraphAD: A graph neural network for entity-wise multivariate time-series anomaly detection[C]//Proc of the 45th Int ACM SIGIR Conf on Research and Development in Information Retrieval. New York: ACM, 2022: 2297−2302

[46] Chen Xuanhao, Deng Liwei, Huang Feiteng, et al. DAEMON: Unsupervised anomaly detection and interpretation for multivariate time series[C]//Proc of the 37th IEEE Int Conf on Data Engineering. Piscataway, NJ: IEEE, 2021: 2225−2230

[47] Zheng Wujie, Lu Haochuan, Zhou Yangfan, et al. iFeedback: Exploiting user feedback for real-time issue detection in large-scale online service systems[C]//Proc of the 34th IEEE/ACM Int Conf on Automated Software Engineering (ASE). Piscataway, NJ: IEEE, 2019: 352−363

[48] Zhang Shuo, Chen Xiaofei, Chen Jiayuan, et al. Anomaly detection of periodic multivariate time series under high acquisition frequency scene in IoT[C]//Proc of the 20th Int Conf on Data Mining Workshops. Piscataway, NJ: IEEE, 2020: 543−552

[49] Ibidunmoye O, Rezaie A R, Elmroth E. Adaptive anomaly detection in performance metric streams[J]. IEEE Transactions on Network and Service Management, 2017, 15(1): 217−231

[50] Hundman K, Constantinou V, Laporte C, et al. Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding[C]//Proc of the 24th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2018: 387−395

[51] Goh J, Adepu S, Junejo K N, et al. A dataset to support research in the design of secure water treatment systems[C]//Proc of the 11th Int Conf on Critical Information Infrastructures Security. Berlin: Springer, 2016: 88−99

[52] Ahmed C M, Palleti V R, Mathur A P. WADI: A water distribution testbed for research in the design of secure cyber physical systems[C]//Proc of the 3rd Int Workshop on Cyber-physical Systems for Smart Water Networks. New York: ACM, 2017: 25−28

[53] Dau H A, Bagnall A, Kamgar K, et al. The UCR time series archive[J]. IEEE/CAA Journal of Automatica Sinica, 2019, 6(6): 1293−1305

[54] Stehman S V. Selecting and interpreting measures of thematic classification accuracy[J]. Remote Sensing of Environment, 1997, 62(1): 77−89

[55] Faraggi D, Reiser B. Estimation of the area under the ROC curve[J]. Statistics in Medicine, 2002, 21(20): 3093−3106

[56] Xu Haowen, Chen Wenxiao, Zhao Nengwen, et al. Unsupervised anomaly detection via variational auto-encoder for seasonal KPIs in web applications[C]//Proc of the 27th Web Conf. New York: ACM, 2018: 187−196

[57] Ji Shouling, Du Tianyu, Deng Shuiguang, et al. Robustness certification research on deep learning models: A survey[J]. Chinese Journal of Computers, 2022, 45((1):): 190−206 (in Chinese)
(纪守领, 杜天宇, 邓水光, 等. 深度学习模型鲁棒性研究综述[J]. 计算机学报, 2022, 45(1): 190−206)

[58] Dai Liang, Lin Tao, Liu Chang, et al. SDFVAE: Static and dynamic factorized VAE for anomaly detection of multivariate CDN KPIs[C]//Proc of the 30th Web Conf. New York: ACM, 2021: 3076−3086

[59] Zolfaghari B, Srivastava G, Roy S, et al. Content delivery networks: State of the art, trends, and future roadmap[J]. ACM Computing Surveys, 2020, 53(2): 1−34

[60] Ghaznavi M, Jalalpour E, Salahuddin M A, et al. Content delivery network security: A survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2166−2190

[61] Wu Jiyi, Li Wenjuan, Huang Jianping, et al. Key techniques for mobile Internet: A survey[J]. SCIENTIA SINICA Informationis, 2015, 45(1): 45−69 (in Chinese)
(吴吉义, 李文娟, 黄剑平, 等. 移动互联网研究综述[J]. 中国科学: 信息科学, 2015, 45(1): 45−69)

[62] Hsieh M Y. SoLoMo technology: Exploring the most critical determinants of SoLoMo technology in the contemporary mobile communication technology era[J]. Journal of Ambient Intelligence and Humanized Computing, 2018, 9(2): 307−318

[63] Li Hui, Li Fenghua, Cao Jin, et al. Survey on security and privacy preserving for mobile Internet service[J]. Journal on Communications, 2014, 35(11): 1−11 (in Chinese)
(李晖, 李凤华, 曹进, 等. 移动互联服务与隐私保护的研究进展[J]. 通信学报, 2014, 35(11): 1−11)

[64] Wang Jiuchao, Zhao Zhuofeng. Entity-data-based modeling for Internet of things services[J]. Computer System & Applications, 2023, 32(6): 70−79 (in Chinese)
(王久超, 赵卓峰. 基于实体-数据的物联网服务建模[J]. 计算机系统应用, 2023, 32(6): 70−79)

[65] Sun Haili, Long Xiang, Han Lansheng, et al. Overview of anomaly detection techniques for industrial Internet of things[J]. Journal on Communications, 2022, 43(3): 196−210 (in Chinese)
(孙海丽, 龙翔, 韩兰胜, 等. 工业物联网异常检测技术综述[J]. 通信学报, 2022, 43(3): 196−210)

[66] Zhang Shenglin, Zhao Chenyu, Sui Yicheng, et al. Robust KPI anomaly detection for large-scale software services with partial labels[C]//Proc of the 32nd IEEE Int Symp on Software Reliability Engineering (ISSRE). Piscataway, NJ: IEEE, 2021: 103−114

[67] Zhang Xu, Lin Qingwei, Xu Yong, et al. Cross-dataset time series anomaly detection for cloud systems[C]//Proc of the 2019 USENIX Annual Technical Conf. Berkeley, CA: USENIX Association, 2019: 1063−1076

[68] Wang Jingyu, Jing Yuhan, Qi Qi, et al. ALSR: An adaptive label screening and relearning approach for interval-oriented anomaly detection[J]. Expert Systems with Applications, 2019, 136: 94−104

[69] Wang Yao, Wang Zhaowei, Xie Zejun, et al. Practical and white-box anomaly detection through unsupervised and active learning[C/OL]// Proc of the 29th Int Conf on Computer Communications and Networks (ICCCN). Piscataway, NJ: IEEE, 2020[2024-03-09]. https://ieeexplore.ieee.org/document/9209704

[70] Moysen J, Ahmed F, García-Lozano M, et al. Big data-driven automated anomaly detection and performance forecasting in mobile networks[C/OL]//Proc of the 2020 IEEE Global Communications Conf Workshops. Piscataway, NJ: IEEE, 2020[2024-03-09]. https://ieeexplore.ieee.org/document/9367579

[71] Bu Jiahao, Liu Ying, Zhang Shenglin, et al. Rapid deployment of anomaly detection models for large number of emerging KPI streams[C/OL]//Proc of the 37th IEEE Int Performance, Computing, and Communications Conf. Piscataway, NJ: IEEE, 2018[2024-03-09]. https://ieeexplore.ieee.org/document/8711315

[72] Wu Jun, Lee P P C, Li Qi, et al. CellPAD: Detecting performance anomalies in cellular networks via regression analysis[C/OL]//Proc of the 17th IFIP Networking Conf. Piscataway, NJ: IEEE, 2018 [2024-03-09]. https://ieeexplore.ieee.org/document/8697027

[73] Yu Guang, Cai Zhiping, Wang Siqi, et al. Unsupervised online anomaly detection with parameter adaptation for KPI abrupt changes[J]. IEEE Transactions on Network and Service Management, 2019, 17(3): 1294−1308

[74] Chen Haiwen, Yu Guang, Liu Fang, et al. Unsupervised anomaly detection via DBSCAN for KPIs jitters in network managements[J]. Computers, Materials & Continua, 2020, 62(2): 917−927

[75] Wang Zhichao, Singh S, Pereira A. Large scale time series analysis for infrastructure reliability[C]//Proc of the 7th IEEE Int Conf on Big Data. Piscataway, NJ: IEEE, 2019: 6240−6242

[76] Teh H Y, Kevin I, Wang K, et al. Expect the unexpected: Unsupervised feature selection for automated sensor anomaly detection[J]. IEEE Sensors Journal, 2021, 21(16): 18033−18046

[77] Zhao Nengwen, Zhu Jing, Wang Yao, et al. Automatic and generic periodicity adaptation for KPI anomaly detection[J]. IEEE Transactions on Network and Service Management, 2019, 16(3): 1170−1183

[78] Zhao Na, Han Biao, Cai Yang, et al. SeqAD: An unsupervised and sequential autoencoder ensembles based anomaly detection framework for KPI[C/OL]//Proc of the 29th IEEE/ACM Int Symp on Quality of Service (IWQoS). Piscataway, NJ: IEEE, 2021[2024-03-09]. https://ieeexplore.ieee.org/document/9521258

[79] Zhao Na, Han Biao, Li Ruidong, et al. A multivariate KPIs anomaly detection framework with dynamic balancing loss training[J]. IEEE Transactions on Network and Service Management, 2023, 20(2): 1418−1429

[80] Zhu Lingxue, Laptev N. Deep and confident prediction for time series at uber[C]//Proc of the 17th Int Conf on Data Mining Workshops. Piscataway, NJ: IEEE, 2017: 103−110

[81] Lee Mingchang, Lin Jiachun, Gan E G. ReRe: A lightweight real-time ready-to-go anomaly detection approach for time series[C]// Proc of the 44th IEEE Annual Computers, Software, and Applications Conf (COMPSAC). Piscataway, NJ: IEEE, 2020: 322−327

[82] Yao Yueyue, Ma Jianghong, Ye Yunming. KfreqGAN: Unsupervised detection of sequence anomaly with adversarial learning and frequency domain information[J]. Knowledge-Based Systems, 2022, 236: 107757

[83] Shang Zijing, Zhang Yingjun, Zhang Xiuguo, et al. Time series anomaly detection for KPIs based on correlation analysis and HMM[J]. Applied Sciences, 2021, 11(23): 11353

[84] Ahmad S, Lavin A, Purdy S, et al. Unsupervised real-time anomaly detection for streaming data[J]. Neurocomputing, 2017, 262: 134−147

[85] Lea C, Vidal R, Reiter A, et al. Temporal convolutional networks: A unified approach to action segmentation[C]//Proc of the 14th European Conf on Computer Vision Workshops. Berlin: Springer, 2016: 47−54

[86] Li Zhihan, Zhao Youjian, Liu Rong, et al. Robust and rapid clustering of KPIs for large-scale anomaly detection[C/OL]//Proc of the 26th IEEE/ACM Int Symp on Quality of Service (IWQoS). Piscataway, NJ: IEEE, 2018[2024-03-09]. https://ieeexplore.ieee.org/document/8624168

[87] Zhang Shenglin, Zhong Zhenyu, Li Dongwen, et al. Efficient KPI anomaly detection through transfer learning for large-scale web services[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(8): 2440−2455

[88] Huo Wunjun, Wang Wei, Li Wen. AnomalyDetect: An online distance-based anomaly detection algorithm[C]//Proc of the 16th IEEE Int Conf on Web Services. Piscataway, NJ: IEEE, 2019: 63−79

[89] Audibert J, Michiardi P, Guyard F, et al. USAD: Unsupervised anomaly detection on multivariate time series[C]//Proc of the 25th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2020: 3395−3404

[90] Abdulaal A, Lancewicki T. Real-time synchronization in neural networks for multivariate time series anomaly detection[C]//Proc of 2021 the IEEE Int Conf on Acoustics, Speech and Signal Processing (ICASSP). Piscataway, NJ: IEEE, 2021: 3570−3574

[91] Jensen L, Fosa J, Teitelbaum B, et al. How dense autoencoders can still achieve the state-of-the-art in time-series anomaly detection [C]//Proc of the 20th IEEE Int Conf on Machine Learning and Applications (ICMLA). Piscataway, NJ: IEEE, 2021: 1272−1277

[92] Li Zeyan, Chen Wenxiao, Pei Dan. Robust and unsupervised KPI anomaly detection based on conditional variational autoencoder [C/OL]//Proc of the 37th IEEE Int Performance, Computing, and Communications Conf. Piscataway, NJ: IEEE, 2018[2024-03-09].

https://ieeexplore.ieee.org/document/8710885

[93] Ji Jiemin, Guan Donghai, Deng Yuwen, et al. Model-agnostic causal principle for unbiased KPI anomaly detection[C/OL]//Proc of the 2022 Int Joint Conf on Neural Networks (IJCNN). Piscataway, NJ: IEEE, 2022[2024-03-09]. https://ieeexplore.ieee.org/document/9892664

[94] Wang Wenlu, Chen Pengfei, Xu Yibin, et al. Active-MTSAD: Multivariate time series anomaly detection with active learning[C]//Proc of the 52nd Annual IEEE/IFIP Int Conf on Dependable Systems and Networks (DSN). Piscataway, NJ: IEEE, 2022: 263−274

[95] Wu Bo, Xu Qian, Yao Zhenjie, et al. VAE-TCN hybrid model for KPI anomaly detection[C/OL]//Proc of the 23rd Asia-Pacific Network Operations and Management Symp (APNOMS). Piscataway, NJ: IEEE, 2022[2024-03-09]. https://ieeexplore.ieee.org/document/9919985

[96] Chen Ningjiang, Tu Huan, Duan Xiaoyan, et al. Semisupervised anomaly detection of multivariate time series based on a variational autoencoder[J]. Applied Intelligence, 2023, 53(5): 6074−6098

[97] Tuli S, Casale G, Jennings N R. TranAD: Deep transformer networks for anomaly detection in multivariate time series data[J]. Proceedings of the VLDB Endowment, 2022, 15(6): 1201−1214

[98] Xu Jiehui, Wu Haixu, Wang Jianmin, et al. Anomaly transformer: Time series anomaly detection with association discrepancy[C/OL]// Proc of the 10th Int Conf on Learning Representations. New York: OpenReview. net, 2022[2024-01-24]. https://openreview.net/forum?id=LzQQ89U1qm_

[99] Zhong Jie, Zuo Enguang, Chen Chen, et al. A masked attention network with query sparsity measurement for time series anomaly detection[C]//Proc of the 30th IEEE Int Conf on Multimedia and Expo (ICME). Piscataway, NJ: IEEE, 2023: 2741−2746

[100] Qin Shuxin, Zhu Jing, Wang Dan, et al. Decomposed transformer with frequency attention for multivariate time series anomaly detection[C]//Proc of the 10th IEEE Int Conf on Big Data. Piscataway, NJ: IEEE, 2022: 1090−1098

[101] Zhang Yu, Wang Tianbo. Applying value-based deep reinforcement learning on KPI time series anomaly detection[C]//Proc of the 15th IEEE Int Conf on Cloud Computing (CLOUD). Piscataway, NJ: IEEE, 2022: 197−202

[102] Shu Yanjun, Gao Tianrun, Zhang Zhan, et al. A general KPI anomaly detection using attention models[C]//Proc of the 19th IEEE Int Conf on Services Computing (SCC). Piscataway, NJ: IEEE, 2022: 114−119

[103] Doshi K, Abudalou S, Yilmaz Y. Reward once, penalize once: Rectifying time series anomaly detection[C/OL]//Proc of the 2022 Int Joint Conf on Neural Networks (IJCNN). Piscataway, NJ: IEEE, 2022[2024-03-09]. https://ieeexplore.ieee.org/document/9891913

[104] Geiger A, Liu Dongyu, Alnegheimish S, et al. TadGAN: Time series anomaly detection using generative adversarial networks[C]//Proc of the 8th IEEE Int Conf on Big Data. Piscataway, NJ: IEEE, 2020: 33−43

[105] Zhao Jiachen, Li Yongling, He Haibo, et al. One-step predictive encoder-gaussian segment model for time series anomaly detection[C/OL]//Proc of the 2020 Int Joint Conf on Neural Networks (IJCNN). Piscataway, NJ: IEEE, 2020[2024-03-09]. https://ieeexplore.ieee.org/document/9207569

[106] Chen Wenxiao, Xu Haowen, Li Zwyan, et al. Unsupervised anomaly detection for intricate KPIs via adversarial training of VAE[C]//Proc of the 38th IEEE Conf on Computer Communications (INFOCOM). Piscataway, NJ: IEEE, 2019: 1891−1899

[107] Zhao Yun, Zhang Xiuguo, Shang Zijing, et al. A novel hybrid method for KPI anomaly detection based on VAE and SVDD[J/OL]. Symmetry, 2021, 13(11): 2104

[108] He Zilong, Chen Pengfei, Huang Tao. Share or not share? Towards the practicability of deep models for unsupervised anomaly detection in modern online systems[C]//Proc of the 33rd IEEE Int Symp on Software Reliability Engineering (ISSRE). Piscataway, NJ: IEEE, 2022: 25−35

[109] Graves A, Schmidhuber J. Framewise phoneme classification with bidirectional LSTM and other neural network architectures[J]. Neural Networks, 2005, 18(5/6): 602−610

[110] Dai Liang, Chen Wenchao, Liu Yanwei, et al. Switching Gaussian mixture variational RNN for anomaly detection of diverse CDN websites[C]//Proc of the 41st IEEE Conf on Computer Communications (INFOCOM). Piscataway, NJ: IEEE, 2022: 300−309

[111] Qi Qi, Shen Runye, Wang Jingyu, et al. Spatial-temporal learning-based artificial intelligence for IT operations in the edge network[J]. IEEE Network, 2021, 35(1): 197−203

[112] Scheinert D, Acker A. TELESTO: A graph neural network model for anomaly classification in cloud services[C]//Proc of the 2020 Int Conf on Service-Oriented Computing Workshops. Berlin: Springer, 2020: 214−227

[113] Ji Suozhao, Wu Wenjun, Pu Yanjun. Multi-indicators prediction in microservice using Granger causality test and Attention LSTM[C]//Proc of the 2020 IEEE World Congress on Services (SERVICES). Piscataway, NJ: IEEE, 2020: 77−82

[114] Ma Minghua, Zhang Shenglin, Pei Dan, et al. Robust and rapid adaption for concept drift in software system anomaly detection[C]// Proc of the 29th IEEE Int Symp on Software Reliability Engineering (ISSRE). Piscataway, NJ: IEEE, 2018: 13−24

[115] Wang Jingwen, Liu Jingxin, Pu Juntao, et al. An anomaly prediction framework for financial IT systems using hybrid machine learning methods[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(11): 15277−15286

[116] Zhang Shupeng, Fung C, Huang Shaohan, et al. PSOM: Periodic self-organizing maps for unsupervised anomaly detection in periodic time series[C/OL]//Proc of the 25th IEEE/ACM Int Symp on Quality of Service (IWQoS). Piscataway, NJ: IEEE, 2017[2024-03-09]. https://ieeexplore.ieee.org/document/7969174

[117] Le K H, Papotti P. User-driven error detection for time series with events[C]//Proc of the 36th IEEE Int Conf on Data Engineering. Piscataway, NJ: IEEE, 2020: 745−757

[118] Loog M. Contrastive pessimistic likelihood estimation for semi-supervised classification[J]. IEEE Transactions on Pattern Analysis

and Machine Intelligence, 2015, 38(3): 462−475

[119] Sohn K, Lee H, Yan Xinchen. Learning structured output representation using deep conditional generative models[C]//Proc of the 29th Int Conf on Neural Information Processing Systems. Cambridge, MA: MIT, 2015: 3483−3491

[120] Chen Xuanhao, Deng Liwei, Zhao Yan, et al. Adversarial autoencoder for unsupervised time series anomaly detection and interpretation[C]//Proc of the 16th ACM Int Conf on Web Search and Data Mining. New York: ACM, 2023: 267−275

[121] Arjovsky M, Chintala S, Bottou L. Wasserstein generative adversarial networks[C]//Proc of the 34th Int Conf on Machine Learning. New York: ACM, 2017: 214−223

[122] Gulrajani I, Ahmed F, Arjovsky M, et al. Improved training of Wasserstein GANs[C]//Proc of the 31st Int Conf on Neural Information Processing Systems. Cambridge, MA: MIT, 2017: 5767−5777

[123] Zhu Haiqi, Rho S, Liu Shaohui, et al. Learning spatial graph structure for multivariate KPI anomaly detection in large-scale cyber-physical systems[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 1−16

[124] Siffer A, Fouque P A, Termier A, et al. Anomaly detection in streams with extreme value theory[C]//Proc of the 23rd ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2017: 1067−1075

[125] García S, Luengo J, Herrera F. Data Preprocessing in Data Mining[M]. Cham, Switzerland: Springer International Publishing, 2015

[126] Cheng Keyang, Wang Ning, Shi Wenxi, et al. Research advances in the interpretability of deep learning[J]. Journal of Computer Research and Development, 2020, 57(6): 1208−1217 (in Chinese)
(成科扬, 王宁, 师文喜, 等. 深度学习可解释性研究进展[J]. 计算机研究与发展, 2020, 57(6): 1208−1217)



Shang Shuyi, born in 1996. PhD candidate. Her main research interests include time series data mining, machine learning, and AIOps.

尚书一, 1996 年生. 博士研究生. 主要研究方向为时序数据挖掘、机器学习、智能运维.



Li Hongjia, born in 1981. PhD, associate professor. His main research interests include cyberspace security, 5G/6G network, and edge intelligence computing.

李宏佳, 1981 年生. 博士, 副研究员. 主要研究方向为网络空间安全、5G/6G 网络、边缘智能计算.



Song Chen, born in 1984. PhD, senior engineer. Her main research interest includes cyber security.

宋　晨, 1984 年生. 博士, 高级工程师. 主要研究方向为网络安全.



Lu Zhitong, born in 1993. Master, engineer. Her main research interests include image adversarial learning and information security.

卢至彤, 1993 年生. 硕士, 工程师. 主要研究方向为图像对抗学习、信息安全.



Wang Liming, born in 1978. PhD, professorate senior engineer. Member of CCF. His main research interests include cloud security, date security, and wireless security.

王利明, 1978 年生. 博士, 正高级工程师. CCF 会员. 主要研究方向为云安全、数据安全、无线安全.



Xu Zhen, born in 1976. PhD, professorate senior engineer. Member of CCF. His main research interests include trusted computing, cyber security, and system security.

徐　震, 1976 年生. 博士, 正高级工程师. CCF 会员. 主要研究方向为可信计算、网络安全、系统安全.