改进自适应模型池的在线异常检测算法

项秋艳,訾玲玲*,丛 鑫
(重庆师范大学计算机与信息科学学院,重庆 401331)

摘 要: 精确的在线异常检测方法是物联网行业发展的核心,其中,以复杂和动态数据流为对象的在线异常识别是研究热点. 现有在线异常检测方法存在处理复杂性负载过重问题,离线深度异常检测方法则存在因数据分布变化导致概念漂移问题. 针对上述问题,本文提出了改进自适应模型池的在线异常检测框架,该框架可以与基于自动编码器的异常检测方法协作实现在线异常检测. 首先,利用基于自动编码器的异常检测模型进行基本异常识别;其次,以自适应模型池为基础,融合概念漂移检测算法准确识别概念漂移,适应动态变化的数据流,解决概念漂移现象;最后,优化自适应模型池的模型合并方法,提升在线异常识别能力. 实验结果表明,相比自动编码器模型的流变体和原自适应模型池算法,提出的算法在异常检测精度指标上分别提升了20.2%和5.83%,同时,最佳精度指标高于现有在线异常检测算法约16.7%.

关键词: 无监督学习;自动编码器;概念漂移;异常检测;自适应模型池;数据流
基金项目: 重庆市教育科学规划重点课题(No.K22YE205098)
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112(2024)07-2503-12
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230731

Improved Adaptive Model Pools for Online Anomaly Detection Algorithms

XIANG Qiu-yan, ZI Ling-ling*, CONG Xin
(*College of Computer and Information Science*, *Chongqing Normal University*, *Chongqing* 401331, *China*)

Abstract: Accurate online anomaly detection methods are at the core of the development of IoT-related industries, in which online anomaly identification targeting complex and dynamic data streams is one of the important research hotspots. Existing online anomaly detection methods suffer from the problem of processing complexity overload, while offline deep anomaly detection methods suffer from the problem of concept drift due to the change of data distribution. To address the above problems, this paper proposes an online anomaly detection framework with improved adaptive model pooling, which can collaborate with autoencoder-based anomaly detection methods to achieve online anomaly detection. Firstly, the basic anomaly identification is carried out using the autoencoder-based anomaly detection model. Secondly, based on the adaptive model pool, the concept drift detection algorithm is integrated to accurately identify concept drift, adapt to the dynamically changing data flow, and solve the concept drift phenomenon. Finally, the model merging method of the optimised adaptive model pool is optimised, which enhances the capability of online anomaly identification. The experimental results show that compared with the flow variant of autoencoder model and the original adaptive model pool algorithm, the proposed algorithm improves the anomaly detection accuracy indexes by 20.2% and 5.83% respectively, and meanwhile is higher than the existing online anomaly detection algorithms in the best accuracy indexes by about 16.7%.

Key words: unsupervised learning; autoencoder; concept drift; anomaly detection; adaptive model pool; data stream
Foundation Item(s): Key Project of Chongqing Municipal Education Science Planning (No.K22YE205098)

1 引言

异常检测是目前机器学习应用中的重要分支,在众多领域都是研究热点,比如,金融行业的反欺诈、入侵检测、机器故障等[1~3]. 准确的在线异常检测能帮助相关人员及时察觉风险,处理异常,保障各行业稳定. 但由于来自物联网的数据流往往具有数据量巨大且结构多样化等特点[4~6],如何在数据流较为复杂的情况下在线准确识别异常是一大挑战. 传统在线异常检测算

收稿日期:2023-08-03;修回日期:2024-05-14;责任编辑:梅志强
*通讯作者:訾玲玲

法很多,例如高斯拟合等,但在面对复杂数据集时存在一定局限性[7]. 得益于深度学习的广泛研究和应用,学者开始探讨将深度学习应用于异常识别任务. 基于深度学习的异常检测技术具有强大复杂数据的处理能力,因此,在异常检测方面取得一定进展[8]. 特别是基于自动编码器(AutoEncoder,AE)的异常检测方法,AE模型因无监督的性质和处理高维数据的能力被广泛使用. 相对于监督学习而言,无监督学习能有效避免对海量数据标签的需求,有可能挖掘出新的异常类型[9,10]. 不过目前基于自动编码器的异常检测方法大多是离线设置.

离线异常检测往往会忽视数据流动态变化,即数据项的分布会随着时间变化而改变. 随着数据流不断发展,即使研究人员经过大量预处理和模型训练,但仍存在模型过时,导致模型异常检测不准确,出现概念漂移现象[11,12]. 这种复杂和不断发展的数据流在各种现实情况下被观察到[13,14]. 例如,气体传感器价值流,用于监测不同气体浓度的气体泄漏. 针对概念漂移,在现有基于深度学习的数据流异常检测中常见方法是建立初始模型,对模型进行增量更新[15,16]. 然而,相关研究表明这种增量方法模型只适应最新数据点,但不管数据流如何演变[17]. 对于数据流中的任意概念漂移,增量方法可能无效,因为它需要一些时间来完全适应新概念. 同时,增量更新的效率也比较低下,因为它很快就会忘记将来可能再次出现的概念. 比如,有一些基于递归神经网络(Recurrent Neural Network,RNN)的方法被提出用于时间序列异常检测[18,19],它们更侧重于学习局部序列内部的时间关系和增量更新单个模型. 如何能在复杂数据流中,随着数据变化去维护模型,更新模型,做到准确识别异常是目前具有挑战的问题. 本文提出一种改进后的自适应模型池算法(Optimize Adaptive framework foR online deep anomaly deteCtion Under a complex evolving data Stream,Optimize-ARCUS)能有效处理数据流的复杂性和演化性,做到在线准确识别异常. Optimize-ARCUS算法核心是利用AE模型进行基础异常检测,降低人工成本和解决数据流的复杂度,再利用概念漂移自适应方法解决演化问题.

本文的主要贡献如下:

(1)提出一种改进自适应模型池的在线异常检测框架Optimize-ARCUS,该框架可与基于AE的异常检测方法相结合,在复杂且不断演变的数据流中进行在线异常检测.

(2)通过融入概念漂移检测算法和优化模型的合并方式改进原有自适应模型池算法. 经消融实验证明,这2种方法都能有效提升异常检测精度.

(3)使用3种先进的AE模型对Optimize-ARCUS框架进行综合实验. 在6个高维概念漂移数据集上,Optimize-ARCUS的异常检测精度比AE模型的流变体、原自适应模型池算法分别提高20.2%和5.83%,比现有在线异常检测算法的最佳精度高出16.7%.

2 相关工作

2.1 基于深度学习的异常检测算法

异常检测,又称离群点检测或新颖性检测,是各界活跃的研究领域[8]. 异常可以被识别为与大多数其他数据点具有不同特征的数据点,它是新的观测、某种故障或意外的噪声等[20]. 传统的异常检测方法可分为:基于统计的方法、基于距离的方法、基于偏差的方法、基于密度的方法[21]. 例如,基于可扩展核密度的流数据异常检测方法(scalable Kernel density Estimation-based Local Outlier detection over large data Streams,KELOS)[22]主要利用抽象内核中心的密度评估模型有效检测数据中的局部离群值,通过分层区域跳跃进行局部异常值检测(local outlier detection by STAtionary REgion skipping,STARE)[23],采用平稳区域跳跃更新密度和异常分数. 其次,基于距离的异常检测方法(NET-effect-based Stream outlier detection,NETS)[24]和基于局部离群因子的异常检测方法(Memory efficient Incremental Local Outlier Factor detection,MILOF)[25]. 其中,NETS主要通过基于集合的方法来检测异常值,相似位置的数据点会被分为一组,在组级别上进行异常检测. 传统的方法有一些局限性,例如,传统方法在医学图像和序列数据集上的异常检测性能都较差,不能捕获数据中的复杂结构. 尤其在时间序列数据中,异常行为和正常行为之间往往是很难精确定义,且存在不断演变现象. 传统方法缺乏定义良好的代表性正态边界,高维数据的计算量大,也需要大量人工成本. 因此,本文提出了基于深度学习的方法. 深度异常检测能够从时间序列数据中学习层次识别特征,更容易准确识别异常[2,26].

最近深度神经网络的快速发展导致产生许多具有不同类型方法的深度异常检测方法(例如,AE,RNN)[7]. 其中,自编码器由于其无监督但有效去除输入中的噪声或异常信息的能力而得到广泛研究,取得先进性能[27]. 比如,用于无监督异常检测的深度自编码高斯混合模型(Deep Autoencoding Gaussian Mixture Model,DAGMM)[28]主要是通过AE来为每个输入数据点生成低维表示和重建误差,并利用高斯混合隶属度来检测异常. 基于空间恢复层的无监督自动编码器检测方法(Robust Subspace Recovery layer for unsupervised AutoEncoder detection,RSRAE)[29]则是在AE结构中增加RSR层来学习非线性嵌入数据点的隐线性结构,再

根据原始位置和映射位置之间的距离来检测异常. 基于投影路径重构的新颖性检测(novelty detection with Reconstruction Along the Projection Pathway, RAPP)[30]主要是通过在输入空间和隐藏空间中计算比较重构误差来检测异常,并利用AE获得隐藏空间的激活值以验证编码和解码过程是否存在信息丢失. 另外,一些基于深度学习的异常检测算法,也表现出不错的检测效果,不过,这些方法更加侧重于学习局部序列内部的时间关系和增量更新. 比如,基于LSTM的多传感器异常检测编解码器方法(LSTM-based AutoEncoder for multi-sensor anomaly detection, LSTM-AE)[19]和基于深度结构的无监督序列异常检测方法(Unsupervised sequential Outlier detection with Deep Architectures, UODA)[31]等. LSTM-AE是基于具有长短期记忆的编码器-解码器网络,主要是学习重构"正常"时间序列行为,使用重构错误来检测异常. UODA使用自编码器模型来捕捉异常值和正常实例之间的内在差异,并将差异集成到循环神经网络中检测异常.

2.2　概念漂移自适应方法

概念漂移主要指的是随着时间推移,数据并不稳定,数据分布与输入变量和输出目标变量之间的关系会发生变化. 概念漂移本质上是底层数据流分布变化[32]. 通常概念漂移可根据不同概念之间的转化形式分为:"突变""增量""渐近"和"重现"的漂移[33,34]. 如图1所示,其中,C_1和C_2分别代表2种不同概念. 如何能够一次性处理这4种类型也一直是目前概念漂移自适应领域的主要挑战. 本文主要介绍基于AE的概念漂移自适应方法.

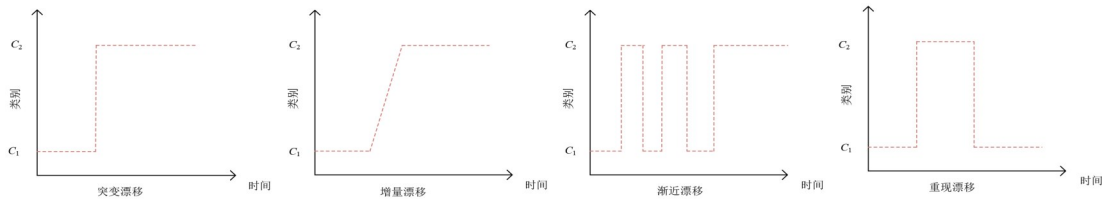


图1　概念漂移类型

AE主要由编码器和解码器组成[35],它与概念漂移自适应方法结合,主要用于一些高维数据的异常检测. 典型算法包括:无监督统计概念漂移检测(Unsupervised Statistical Concept Drift Detection based AutoEncoder, USCDD-AE)[36]、深度进化去噪自动编码器(Deep EvolVing Denoising AutoeNcoder, DEVDAN)[37]和基于内存的流异常检测(Memory-based Streaming anomaly detection, MemStream)[38]、在线深度异常检测自适应框架(Adaptive framework foR online deep anomaly deteCtion Under a complex evolving data Stream, ARCUS)[17]. USCDD-AE使用变分自编码器识别老年人行为异常,基于家庭数据和Kullback-Leibler Divergence的活动概率图检测概念漂移. DEVDAN主要使用网络显著性(Network Significance, NS)公式来评估模型的预测能力. 一旦捕获公式中的值上升,就会调整模型中的隐藏节点适应概念漂移. MemStream使用去噪自编码器提取特征,当新样本到达时,重新计算异常评分,更新AE的权重因子. 如果异常值超过用户设置的阈值,则重新训练模型来适应概念漂移. ARCUS包含概念驱动推理和漂移感知模型池更新2个模块,其中,概念驱动推理侧重于评估模型的可靠性,当可靠性低于阈值0.95时,更新模型池来适应概念漂移.

自适应模型池算法主要是利用AE模型进行异常检测,有效处理复杂和不断变化的数据流. 但自适应模型池算法仍存在概念漂移后新模型训练数据不够,概念漂移判断不准确,模型合并方式有待优化等问题,本文评估异常情况时,加入概念漂移检测技术,并利用概念漂移警告提前存储可能发生漂移的数据. 在模型池自适应过程中增加基于联邦合并中可靠性较高的模型参数占比,优化合并后的模型性能.

3　Optimize-ARCUS框架

3.1　基于Optimize-ARCUS的异常检测算法设计

3.1.1　问题设置

给定一个数据点序$<\boldsymbol{X}_{t-1}, \boldsymbol{X}, \boldsymbol{X}_{t+1}>$,代表实时数据流,基于AE的异常检测模型$M$,参数为$\theta_M$. 其中,AE模型由编码器$E$和解码器$D$组成,通过编码和解码尽可能重构输入,即$\min_{E,D}\left\| \boldsymbol{X}-D(\boldsymbol{Z})\right\|^2$,$\boldsymbol{Z}=E(\boldsymbol{X})$是输入$\boldsymbol{X}$的潜在表示. AE模型通常将给定输入的重建误差用作$\boldsymbol{X}$的异常分数. 将数据流分成同等大小批次,异常检测模型M无监督在线计算各个数据点的异常分数$<M(\boldsymbol{X}_{t-1};\theta_M), M(\boldsymbol{X}_t;\theta_M), M(\boldsymbol{X}_{t+1};\theta_M)>$,并判断是否为异常. 最后,根据环境的变化来更新参数θ_M或创建新模型,以此维护模型和自适应概念漂移. 在这个过程中,采用预先评估方案[39],将测试和训练穿插于同一批处理中,评估环境变化和批处理中数据点异常情况(如图2所示).

3.1.2　Optimize-ARCUS算法总览

Optimize-ARCUS算法是一个在线异常检测框架,

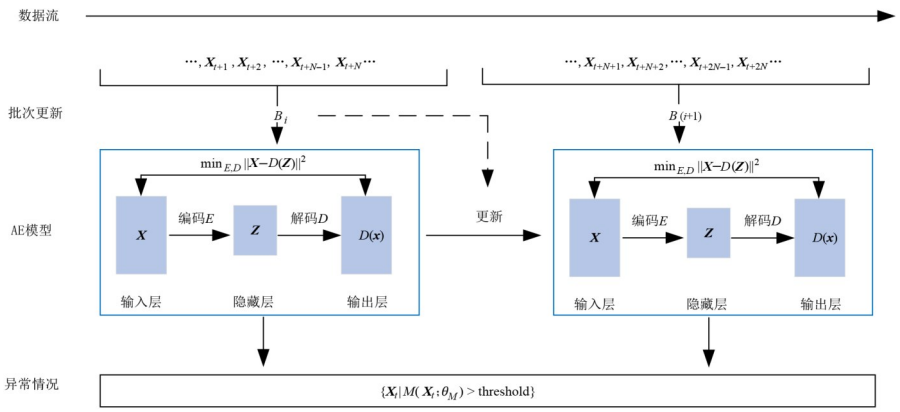


图2 基于批处理和AE模型的连续异常检测

主要是对自适应模型池进行改进优化，适用于任何基于AE的深度异常检测模型. ARCUS管理一个模型池，对一批数据流执行推理，更新模型池以适应批处理中检测到的新概念. Optimize-ARCUS算法主要添加了概念漂移检测算法[40,41]，优化模型的合并方式. Optimize-ARCUS算法的整个过程如图3和算法1所示.

Optimize-ARCUS算法首先利用第一批次数据创建模型，初始化模型池，对接下来的每一批次重复评估数据点的异常情况以及概念漂移自适应. 当前批次每个数据点的最终异常分数是将模型池中每个模型的异常分数标准化并与模型信度加权来综合决定. 模型池的自适应步骤为：首先，根据当前批处理来评估模型池的整体可靠性；其次，根据模型池可靠性变化情况，利用概念漂移检测算法评估漂移情况，根据漂移状态更新模型池，创建适应新概念的模型. 在这个过程中包含模型池中模型的合并，根据模型相似性的判断采取不同合并方式. 具体来说，如果当检测到概念漂移发生时，Optimize-ARCUS会利用当前发生概念漂移的批次和概念漂移警告存储的数据创建一个新模型适应概念漂移. 然后，将新模型与类似的现有模型合并以保持模型池尽可能紧凑. 如果检测到概念漂移警告时，Optimize-ARCUS将会记录当前批次发生概念漂移警告数据，但依然选择模型池中可靠性最高的模型进行增量更新. 若下一个批次检测到概念漂移，会将当前批次数据与下一个批次数据一起用来创建新模型，适应新概念. 若下一个批次未检测到概念漂移，会清除漂移存储数据，重置漂移状态. 如果未发生概念漂移但模型合适，Optimize-ARCUS会保留当前模型池，只更新模型池中可靠性最高的模型，重置漂移状态. 最后，Optimize-ARCUS返回当前批处理的异常分数. 下面将详细讨论Optimize-ARCUS的异常检测方法、概念漂移检测和模型合并优化的方式.

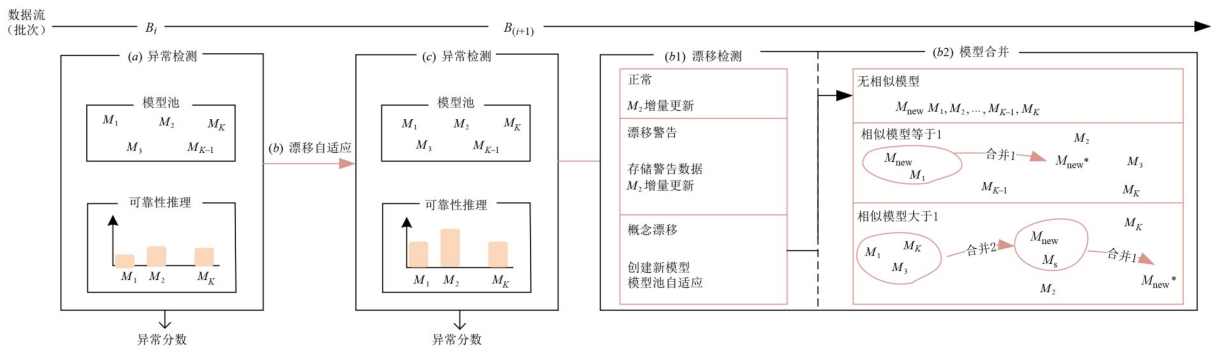


图3 Optimize-ARCUS算法总览

3.2 异常检测

Optimize-ARCUS中一个模型池是由若干不同的AE模型组成的集合$\{M_1, M_2, \cdots, M_K\}$. 它们共享架构，但具有不同参数. 值得注意的是，为了在有效性和效率之间找到平衡，创建新模型，产生开销过大. 因此，需要合并相似模型来保证模型池的紧凑和节约资源. 每个数据点的最终异常分数是由模型池中每个模型的异常分数和对应模型可靠性加权来综合确定. 与有监督不同的是，无监督在线异常检测无真实标签，不能立即得到模型错误率来评估模型的可靠性. Optimize-ARCUS主要是利用基于霍夫丁不等式的均差约束方法(Hoeffding's inequality-basedmean difference bound)[42]计算当

算法1　改进自适应模型池的在线异常检测算法

输入: 数据流 D_s,基于AE的异常检测模型 M, 相似性阈值 r

输出: 每个批次中数据点的异常分数 S

1. Initialize P,$M(B_{\text{Last}};\theta_M)$//初始化模型池 P,上一个批次的采样异常分数集
2. FOR each batch B_{Curr} of data points from D_s DO
3. /*异常检测*/
4. Calculate $M(B_{\text{Curr}};\theta_M)$ //计算当前批次的采样异常分数集
5. /*评估模型池 P 的可靠性 R_p 和模型的可靠性 R_M*/
6. $\varepsilon \leftarrow |\text{avg}(M(B_{\text{Curr}};\theta_M)) - \text{avg}(M(B_{\text{Last}};\theta_M))|$ //相邻批次中总体差异
7. $S_{\max} \leftarrow \max(\max(M(B_{\text{Curr}};\theta_M)) - \max(M(B_{\text{Last}};\theta_M)))$ //相邻批次中最大值之间的差异
8. $S_{\min} \leftarrow \min(\min(M(B_{\text{Curr}};\theta_M)) - \min(M(B_{\text{Last}};\theta_M)))$ //相邻批次中最小值之间的差异
9. $R_M \leftarrow e^{(b,\varepsilon,s_{\max},s_{\min})}$ //模型可靠性
10. $R_p \leftarrow 1 - \prod_i^k (1 - R_{M_i})$ //模型池的可靠性
11. /*概念漂移检测*/
12. Calculate P_i, S_i,$P_{\min}$, $S_{\min}$ //不可靠性、标准差、最小不可靠性、最小标准差
13. IF $P_i + S_i \geqslant P_{\min} + 3\times S_{\min}$ //概念漂移发生
14. Initialize M_{new} by B_{Curr} and warning_hist //初始化新模型
15. Sim_model$\leftarrow\{M_1,\cdots,M_K\}$ //相似性超出阈值 r 的模型
16. /*模型合并*/
17. IF K>1
18. $M_s \leftarrow \sum_{i=1}^{k} \text{merge}_2(R_{M_i},\theta_{M_i},N_{M_i})$//方式2合并相似模型
19. $M_{\text{new}}{}^* \leftarrow (N_{M_1}\theta_{M_1} + N_{M_2}\theta_{M_2})/(N_{M_1}+N_{M_2})$, reset drift //方式1合并相似模型
20. ELSE K=1
21. $M_{\text{new}}{}^* \leftarrow (N_{M_1}\theta_{M_1} + N_{M_2}\theta_{M_2})/(N_{M_1}+N_{M_2})$, reset drift
22. END IF
23. ELSE $P_i + S_i \geqslant P_{\min} + 2\times S_{\min}$ //漂移警告
24. Warning_hist $\leftarrow B_{\text{Curr}}$
25. Perform incremental update on M^* with B_{Curr} //增量更新可靠性最高的模型 M^*
26. ELSE Perform incremental update on M^* with B_{Curr}
27. END IF
28. RETURE S
29. END FOR

前批次的采样异常分数集 $M(B_{\text{Curr}};\theta_M)$ 和上一个批次的采样异常分数集 $M(B_{\text{Last}};\theta_M)$ 的差异统计显著性,从而评估模型的可靠性[26,43,44].

定理　(基于Hoeffding不等式的均值差界)给定 $[a_{\min},a_{\max}]$ 为界的独立随机变量 X 和 Y,样本均值之差的概率 $\overline{X}=\frac{1}{n}\sum_{i=1}^{n}X_i$ 和 $\overline{Y}=\frac{1}{m}\sum_{j=1}^{m}Y_j$ 会在一定范围之内,有:

$$\Pr\{|\overline{X}-\overline{Y}|\geqslant\varepsilon\}\leqslant e^{\frac{-2\varepsilon^2}{(n^{-1}+m^{-1})(a_{\max}-a_{\min})^2}} \tag{1}$$

推论　假设 X 和 Y 是模型 M 在当前批次和上一个批次返回的异常分数,令 $M(B_{\text{Curr}};\theta_M)$ 和 $M(B_{\text{Last}};\theta_M)$ 分别表示 X 和 Y 的异常分数集,推出概率范围,如式(2)所示:

$$\Pr\{|\overline{X}-\overline{Y}|\geqslant\varepsilon\}\leqslant e^{\frac{-2\varepsilon^2}{(b^{-1}+b^{-1})(s_{\max}-s_{\min})^2}}=e^{\frac{-b\varepsilon^2}{(s_{\max}-s_{\min})^2}} \tag{2}$$

其中,b 为批次大小(例如,$b=|B_{\text{Curr}}|=|B_{\text{Last}}|$),

$$\begin{cases}\varepsilon=|\text{avg}(M(B_{\text{Curr}};\theta_M))-\text{avg}(M(B_{\text{Last}};\theta_M))|\\ s_{\max}=\max(\max(M(B_{\text{Curr}};\theta_M)),\max(M(B_{\text{Last}};\theta_M)))\\ s_{\min}=\min(\min(M(B_{\text{Curr}};\theta_M)),\min(M(B_{\text{Last}};\theta_M)))\end{cases} \tag{3}$$

利用推论中的概率界式(2),异常得分的样本均值差的概率至多为 R_M(模型可靠性),因此,可推出单个模型 M 的可靠性,如式(4):

$$R_M=e^{\frac{-b\varepsilon^2}{(s_{\max}-s_{\min})^2}} \tag{4}$$

即当异常分数最大、最小值之间差异越大,相邻批次中总体差异越小,可靠性越高.

最后,利用模型的可靠性,将模型池中每个模型的异常评分标准化,并与模型信度加权来综合确定当前批次中每个数据点的最终异常分数. 给定模型池的一组模型 $\{M_1,M_2,\cdots,M_K\}$,以及相应可靠性 $\{R_{M_1},R_{M_2},\cdots,R_{M_K}\}$,在当前批次中每个数据点的异常分数 S,即 $C_p(x)$ 如式(5)所示:

$$C_p(x)=R_{M_i}\left(\frac{M_i(x;\theta_{M_i})-\text{avg}(M_i(B;\theta_{M_i}))}{\text{std}(M_i(B;\theta_{M_i}))}\right) \tag{5}$$

3.3　概念漂移检测

数据流随着环境的改变而演化,不可避免会产生概念漂移. 根据模型的可靠性推理,可推断出模型池可靠性:给定模型池 $P=\{M_1,M_2,\cdots,M_K\}$,模型池的可靠性 R_p 计算如式(6)所示:

$$R_p=1-\prod_i^k(1-R_{M_i}) \tag{6}$$

在ACURS方法中需要创建一个新模型来适应概念漂移,但训练一个新模型需要大量数据、时间和计算资源,因此,可能会造成模型容易不收敛或过拟合,泛化能力低等问题. ACURS方法中概念驱动推理模块,核心是计算当前数据点的异常分数以及评估是否发生概念漂移,然而,单凭模型可靠性小于0.95这一超参数阈值来判断概念漂移的发生是缺乏准确性的. 因此,本文结合自适应模型池的特点引入概念漂移检测算法[41,42],进一步确定概念漂移的发生.

概念漂移检测算法的主要思想是控制算法的在线错误率,在Optimize-ARCUS算法中加入概念漂移检测算法主要是控制模型池的在线不可靠性. 如果样本数据是稳定分布的,随着数据输入,模型池的不可靠性会逐渐下降;当概率分布发生变化时,模型的不可靠性会上升.

概念漂移检测算法为漂移水平设置2个阈值Warning和Drift，分别代表漂移警告和概念漂移发生．Warning等级意味着当样本数据中的第w个数据批次输入时，模型池的不可靠性达到了Warning值，有样本概率分布改变的前兆，但并不确定是否一定发生概念漂移，可能是受噪声影响．因此，Optimize-ARCUS算法会保存发生了漂移的批次数据，以便后续训练适合新概念模型．如果后续输入的批次没有让不可靠性降低，且当第d个数据批次输入时不可靠性达到了Drift值，则确定样本概率分布发生变化，为适应新样本数据，模型就将以w批次之后的数据进行学习；如果接连输入的数据批次让不可靠性降低，则说明漂移警告错误，并重置漂移状态．

关于Warning和Drift这2个阈值大小，是通过不可靠性的概率分布确定，该概率表示n个样本中的误差数量．对于足够多批次，二项分布近似于具有相同均值和方差的正态分布．假设当前批次有num_batch个，记为B，这样第B个批次时模型池的不可靠性就是模型池Flase的概率观测值P_i，即$1-R_p$，同时能计算此时的标准差S_i，如式(7)所示：

$$S_i=\sqrt{R_p(1-R_p)/B} \tag{7}$$

概念漂移水平可通过相应置信区间的置信水平来衡量．如图4所示，以不可靠性P_i、最新概念漂移之后不可靠性的最小值$P_{\min}$以及标准差S_i、$S_{\min}$(最新概念漂移之后)来计算概念漂移的发生，将漂移水平r_i定义为

$$r_i=\frac{P_i+S_i-P_{\min}}{S_{\min}} \tag{8}$$

当$r_i\geqslant 3$时，表明有99%概率模型池是不可靠的，发生了概念漂移；当$r_i\geqslant 2$时，则表明有95%概率模型池是不可靠的，有概念漂移发生的前兆，并发出漂移警告．

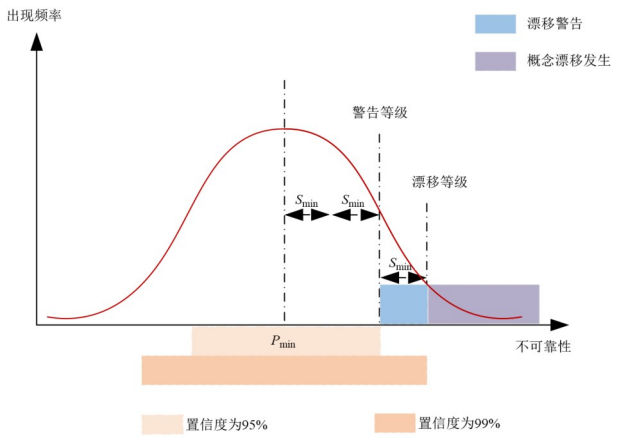


图4 漂移检测模型说明

Optimize-ARCUS算法会利用模型池的可靠性变化以及概念漂移检测算法主动检测概念漂移的发生，从而触发模型池，创建同结构不同参数的新模型以适应概念漂移．当未检测到概念漂移时，将选择模型池中可靠性最高的模型进行增量更新；如果检测到漂移警告时，将会记录漂移数据，保持增量更新；当发生真的概念漂移时，才会创建新模型，并利用当前批次的数据和漂移警告存储的数据训练新模型．这大大提高了新模型的性能和概念漂移是否发生的准确性．当创建新模型后，为保持模型池紧凑，通常会进行模型之间的相似性判断，当相似性高出阈值时，模型进行相应合并．

3.4 模型合并

3.4.1 相似性判断

潜在表征$\boldsymbol{Z}$通过基于AE的模型学习，期望包含最少但足够的输入信息．如果2个模型显示了相同输入的相似潜在表示，则这2个模型被不连接的相似概念批次更新过．为了消除模型池的冗余和避免过拟合，对相似模型进行合并操作．Optimize-ARCUS使用中心核对齐来测量2个模型的相似度，该方法常被用于深度学习模型的相似度判断[45]．给定一个输入$\boldsymbol{X}$和2个模型M_1、M_2，$\boldsymbol{Z}_1$、$\boldsymbol{Z}_2$分别是M_1和M_2学到$\boldsymbol{X}$的潜在表征，使用线性核L，模型相似度的计算表达如下：

$$\begin{aligned}\mathrm{CKA}(L^{\boldsymbol{Z}_1},L^{\boldsymbol{Z}_2})&=\frac{\mathrm{HSIC}(L^{\boldsymbol{Z}_1},L^{\boldsymbol{Z}_2})}{\sqrt{\mathrm{HSIC}(L^{\boldsymbol{Z}_1},L^{\boldsymbol{Z}_1})\mathrm{HSIC}(L^{\boldsymbol{Z}_1},L^{\boldsymbol{Z}_1})}}\\&=||\boldsymbol{Z}_1^{\mathrm{T}}\boldsymbol{Z}_2||_F^2/(||\boldsymbol{Z}_1^{\mathrm{T}}\boldsymbol{Z}_1||_F||\boldsymbol{Z}_2^{\mathrm{T}}\boldsymbol{Z}_2||_F)\end{aligned} \tag{9}$$

HSIC函数是希尔伯特-施密特独立准则，$\|\cdot\|_F$为Frobenius范数．经相关研究表明，在相同概念下训练模型的相似度通常大于0.8[17]．

3.4.2 联邦合并

在联邦学习中，通过随机梯度下降对具有相同参数初始化的局部模型进行优化时，参数平均已被证明等价于梯度平均，并收敛到全局模型．给出2个模型M_1和M_2，用于更新模型的批次数分别是N_{M_1}和N_{M_2}，参数分别是θ_{M_1}和θ_{M_2}，由于新建模型并没有对可靠性进行评估，当只存在一个相似模型时，将使用合并方式1，定义式(10)为

$$\theta_{M_{\mathrm{merged}}}=(N_{M_1}\theta_{M_1}+N_{M_2}\theta_{M_2})/(N_{M_1}+N_{M_2}) \tag{10}$$

当存在$K(K>1)$个相似模型时，针对这些模型将加入R_{M_K}可靠性参数进行合并，可靠性越高的模型参数占比越大，最后得到合并模型再与新建模型M_{new}合并，即合并方式2，定义式(11)和式(12)为

$$\begin{cases}\theta_{M_{\mathrm{merged}}}=\left(\dfrac{N_{M_1}\theta_{M_1}+N_{M_2}\theta_{M_2}}{(N_{M_1}+N_{M_2})}\right),K=1\\ \theta_{M_{\mathrm{sim\_merged}}}=\dfrac{(\theta_{M_{\mathrm{new}}}N_{M_{\mathrm{new}}}+\theta_{M_{\mathrm{merged\_sim}}}N_{\mathrm{merged\_sim}})}{(N_{M_{\mathrm{new}}}+N_{\mathrm{merged\_sim}})},K>1\end{cases} \tag{11}$$

$$\theta_{M_{\mathrm{merged\_sim}}}=\frac{(R_{M_1}\theta_{M_1}N_{M_1}+\cdots+R_{M_K}\theta_{M_K}N_{M_K})}{(N_{M_1}+N_{M_2}+\cdots+N_{M_K})} \tag{12}$$

Optimize-ARCUS根据模型池的可靠性监控环境变

化,当发生概念漂移时会触发模型池更新,通过创建新模型来适应新概念. 同时,为节约资源和保持效率,Optimize-ARCUS通过将新模型与超过相似阈值的最相似模型以图3中(*b*)的形式递归合并,形成一个紧凑的模型池.

4　实验结果与分析

4.1　实验设置

4.1.1　数据集及计算平台

本文使用了6个含有概念漂移的高维数据集进行综合实验,如表1所示. 合成数据集由MNIST[46]和FMNIST[47]通过模拟不同的概念漂移类型和持续时间生成,被广泛用于高维异常检测和数据流分类[48]. MNIST_A和FMNIST_A数据集模拟突变漂移,MNIST_G和FMNIST_G数据集则模拟渐进漂移. 对于真实数据集,GAS[49]和RIALTO[50]中概念漂移类型是未知的. GAS[49]是一个在气体输送平台上收集了36个月的数据集,包含监测6种纯气体物质的传感器值,其中,乙醛(CH_3CHO)被选为异常目标类. RIALTO[50]包含了威尼斯RIALTO桥20天中周围10座建筑视频记录的规范化RGB编码,建筑类设置0为异常目标类. 所有实验均在Intel(R) Core(TM) i5-12400F、32 GB RAM、1 TB HDD的Windows系统上进行. 深度学习算法主要在NVIDIA RTX3060的显卡上运行,安装了Python 3.9、Pytorch 1.9和TensorFlow 2.5等.

表1　用于评估的高维和概念漂移数据流

数据集	描述	维度	概念漂移类型	异常值
MNIST_A	手写的数字	784	突变、重现	任意的数字
MNIST_G	手写的数字	784	渐近、重现	任意的数字
FMNIST_A	时尚物品	784	突变、重现	随意的时尚单品
FMNIST_G	时尚物品	784	渐近、重现	随意的时尚单品
GAS	气体传感器值	128	未知	乙醛
RIALTO	一座桥附近建筑图像	27	未知	建筑类0

4.1.2　对比算法及评价指标

在进行对比实验时,本文使用了3种基于AE的异常检测算法(DAGMM[28]、RSRAE[29]、RAPP[30]),分别实例化Optimize-ARCUS和ARCUS[17]框架. 并将实例化后的异常检测算法与AE模型的流变体(sRAPP、sRSRAE、sDAGMM)进行对比. 未实例化模型的流变体是通过在数据流上连续馈送传入批次来增量训练模型所得. 为了全面评价,将Optimize-ARCUS实例化算法和基于RNN的算法(LSTM-AE[19]的流变体)、基于KDE的STARE[20]算法、基于局部离群因子的MiLOF[25]算法来进行对比实验. 同时,进行不同批次对比实验、消融实验、联邦合并计算成本实验和概念漂移自适应实验,证明Optimize-ARCUS的优化效果. 在异常检测中,异常数据比例非常小,属于不平衡数据集,通常使用AUC(Area Under the Curve)作为评价指标. AUC能有效避免用于验证异常分数的确切阈值在不同应用背景下可能有所不同的问题[51].

4.2　实验结果比较

4.2.1　整体算法的对比实验结果

对所有数据集,实验使用3种基于AE的异常检测算法实例化Optimize-ARCUS和ARCUS[17]框架,分别表示为$OARCUS_{RA}$、$OARCUS_{RS}$、$OARCUS_{DG}$和$ARCUS_{RA}$、$ARCUS_{RS}$、$ARCUS_{DG}$. 同时,还将这些算法与AE模型的流变体及其他在线异常检测算法进行对比. 本文分别在真实数据集和合成数据集上以AUC评价指标为例进行实验,结果如表2所示. 通过实验表明,无论概念漂移类型如何,Optimize-ARCUS实例在所有数据集的在线异常检测中都有最高准确性. Optimize-ARCUS实例化后的异常检测算法与原基础模型相比,准确度高出27.4%($OARCUS_{RA}$在FMNIST_A中). 在所有数据集的平均值上,准确度平均提升$OARCUS_{RA}$为20.2%、$OARCUS_{RS}$为23.6%、$OARCUS_{DG}$为17.0%,与未改进的自适应模型池算法相比,Optimize-ARCUS的准确率最高,高出13.7%($OARCUS_{RA}$在FMNIST_G中). 所有数据集的平均值,准确度平均提升$OARCUS_{RA}$为6.73%、$OARCUS_{RS}$为6.88%、$OARCUS_{DG}$为3.87%. 结果说明了Optimize-ARCUS算法的有效性,其中,RAPP模型检测效果最好.

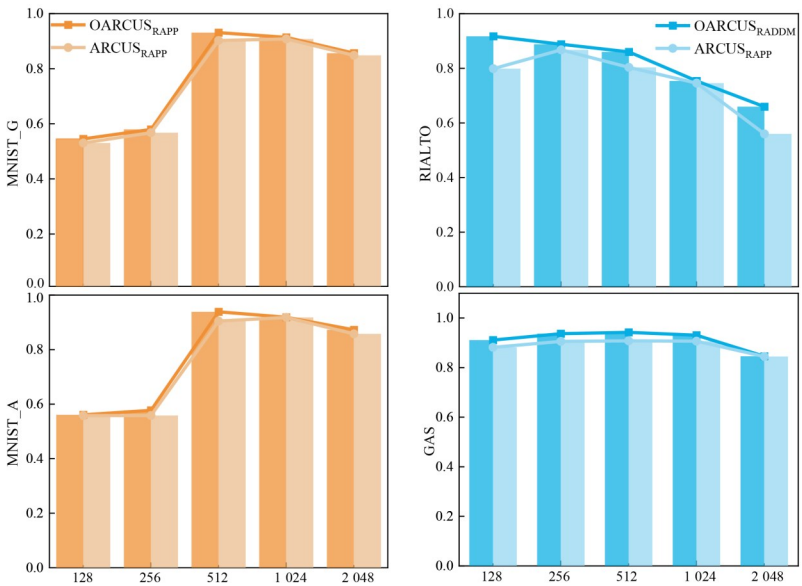
另外,本文将Optimize-ARCUS实例化后的异常检测算法与RNN及传统方法进行比较. 显然,无论在真实数据集还是合成数据集中,Optimize-ARCUS实例化后的方法在所有数据集中达到最高准确性. 具体来说,Optimize-ARCUS实例的准确率比其他算法最佳准确率高出16.7%($OARCUS_{RA}$在MNIST-GrdRec中),在所有数据集上,比sLSTM-AE平均高出28.4%、比STARE平均高出32.6%、比MiLOF平均高出42%. 本文是通过在数据流上连续传入批次,增量训练模型得到sLSTM-AE算法的异常检测结果及准确率.

4.2.2　不同输入批次下对比实验结果

为了测试Optimize-ARCUS算法的可拓展性,以及在不同大小批次的实验效果,本文将输入批次的大小设置为128、256、512、1 024以及2 048. 目的是利用RAPP模型实例化Optimize-ARCUS和ARCUS算法. 本文展示了4个具有代表性的数据集效果,如图5所示. 总的来说,Optimize-ARCUS在不同大小的输入批次中,准确率基本都有提升. 当输入速率为512批次时,无论是在真实数据集中还是在合成数据集中,表

表2 实例化AE模型总体性能比较(最高结果加粗表示)

算法	数据集					
	MNIST_A	MNIST_G	FMNIST_A	FMNIST_G	GAS	RIALTO
$OARCUS_{RA}$	**0.939**	**0.931**	**0.877**	**0.906**	**0.901**	**0.860**
$ARCUS_{RA}$	0.905	0.902	0.823	0.769	0.884	0.803
sRAPP	0.840	0.815	0.603	0.726	0.814	0.752
$OARCUS_{RS}$	0.649	0.668	0.630	0.569	0.585	0.655
$ARCUS_{RS}$	0.630	0.638	0.624	0.532	0.550	0.549
sRSRAE	0.580	0.526	0.515	0.448	0.536	0.455
$OARCUS_{DG}$	0.782	0.652	0.632	0.671	0.495	0.527
$ARCUS_{DG}$	0.767	0.648	0.615	0.656	0.440	0.511
sDGAMM	0.577	0.565	0.612	0.514	0.435	0.509
sLSTM-AE	0.662	0.772	0.622	0.630	0.408	0.617
STARE	0.574	0.576	0.574	0.566	0.635	0.532
MiLOF	0.460	0.434	0.460	0.494	0.589	0.456



(a) 合成数据集 (b) 真实数据集

图5 不同输入批次下对比实验结果

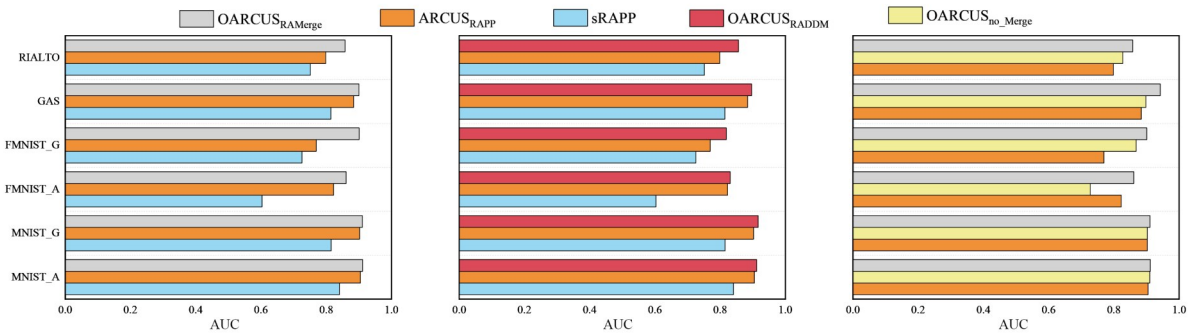
现效果都比较好. 因此,实验输入速率批次大小均为512.

4.2.3 消融实验结果

为证明Optimize-ARCUS中概念漂移检测和模型合并优化的有效性,对比了实例化模型的相应变体. $OARCUS_{RADDM}$只涉及基于自适应模型池融入概念漂移检测算法. $OARCUS_{RAMerge}$只涉及基于自适应模型池改进相似模型的合并方式. 在所有数据集上将$OARCUS_{RAMerge}$与sRAPP、$ARCUS_{RAPP}$进行对比实验,结果如图6所示,而其他Optimize-ARCUS实验结果也显示了相似趋势. 图6(*a*)显示,与单模型的流变体相比,$OARCUS_{RAMerge}$准确率分别比sRAPP和$ARCUS_{RAPP}$平均提升了18.6%和5.45%. 图6(*b*)显示,$OARCUS_{RADDM}$的准确率分别比sRAPP和$ARCUS_{RAPP}$平均提升了15.9%和3.1%. 从图6中可以看出,$OARCUS_{RADDM}$和$OARCUS_{RAMerge}$相对于sRAPP和$ARCUS_{RAPP}$的准确率都有所提升. 另外,如图6(*c*)所示,针对模型合并的方式进行对比实验,$OARCUS_{no_Merge}$代表并不涉及模型合并方法. 通过实验,可得出$OARCUS_{RAMerge}$基于相似性合并实现了更高准确性,比$OARCUS_{no_Merge}$平均提升5.2%. 因此,基于相似度合并,能有效提高模型的准确率,节约资源,保持模型池紧凑的同时保证适应概念漂移.

4.2.4 联邦合并计算成本实验

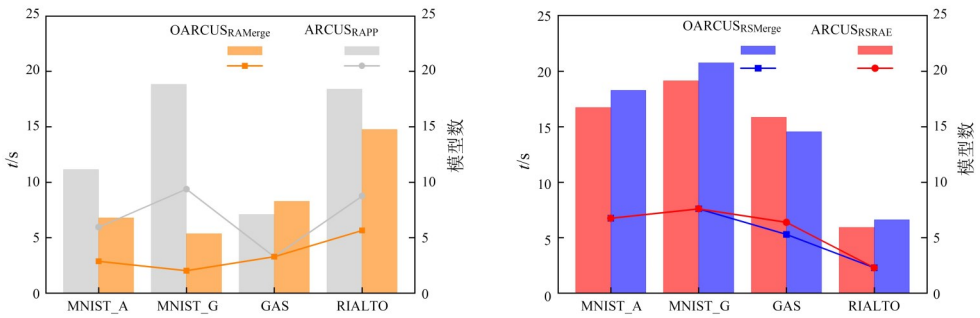
为了测试Optimize-ARCUS算法联邦合并时的计算成本和资源使用情况,本文针对联邦合并模块的平均



(*a*) $OARCUS_{RAMerge}$, $ARCUS_{RAPP}$和sRAPP　(*b*) $ARCUS_{RAPP}$, sRAPP和$OARCUS_{RADDM}$　(*c*) $OARCUS_{RAMerge}$, $ARCUS_{RAPP}$和$OARCUS_{no_Merge}$

图6　合并策略和概念漂移检测消融实验结果

消耗时间和模型池中平均生成模型数量进行实验. 本实验利用RAPP、RSRAE模型来实例化Optimize-ARCUS和ARCUS算法,其中,Optimize-ARCUS算法只涉及基于自适应模型池改进相似模型的合并方式. 展示在512批次输入下的实验效果,如图7所示. 整体上,在实例化模型后Optimize-ARCUS算法中联邦合并消耗时间会随着模型池中模型数量的增加而增加,且不同模型消耗时间是不同的. 对比ARCUS和Optimize-ARCUS算法,Optimize-ARCUS算法消耗的成本更高,但能避免生成不必要的模型.

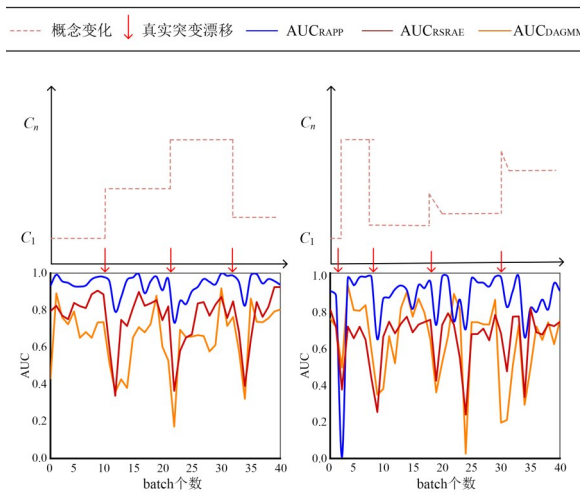


(*a*) 实例化RAPP模型　(*b*) 实例化RSRAE模型

图7　联邦合并平均消耗时间

4.2.5　概念漂移自适应实验

概念漂移自适应实验跟踪了具有已知突变漂移的MNIST_A和FMNIST_A数据集中模型池准确率的变化情况. 图8显示了Optimize-ARCUS实例化RAPP、RSRAE、DAGMM模型的代表性结果与概念$\{C_1, C_2, \cdots, C_n\}$和漂移点的真实趋势. 模型池在整个数据流中保持较高准确率,在真实的突然漂移后,模型异常检测的准确率在最初发生时存在短时间下落,但后续有明显回升趋势,并在下次概念漂移到来前,准确率保持在较高水平. 说明Optimize-ARCUS能及时检测并有效适应真实的概念漂移,提高异常检测精度.



(*a*) MNIST_A漂移　(*b*) FMNIST_A漂移

图8　概念漂移自适应实验

4.3　实验结果分析

从整体性能上来看,Optimize-ARCUS实例化不同AE模型的效果都比未实例化流变体的效果好,最高可高出40%. 同时,将Optimize-ARCUS与未改进的自适应模型池相比,Optimize-ARCUS的准确率有所提升,最高可高出14%. 另外,扩展到AE模型以外的其他先进异常检测算法,Optimize-ARCUS的异常检测性能有所提升,和基于RNN模型的在线异常检测方法相比,Optimize-ARCUS比其最佳准确率高出约16%. 最后,本文通过消融实验、不同批次下的对比实验、联邦合并计

算成本实验和概念漂移自适应实验，证明 Optimize-ARCUS 能有效处理数据流的复杂性和演化性，做到在线准确识别异常.

5 结论

为了在复杂且不断演变的数据流中在线识别异常，本文提出一种改进自适应模型池的在线异常检测框架 Optimize-ARCUS. 该框架可与基于 AE 的异常检测方法相结合，将 AE 模型实例化. Optimize-ARCUS 首先使用基于自动编码器的异常检测模型进行基本异常检测. 然后，为了自适应不断变化的数据流、解决概念漂移现象，结合自适应模型池基础，引入概念漂移检测算法进一步准确识别概念漂移，并设置概念漂移警告存储可能发生漂移的数据，增加更多数据训练概念漂移发生后的新模型、及时维护模型. 最后，利用联邦学习将模型池中相似模型进行合并，在保证模型池紧凑的同时有效提高在线识别欺诈. 在使用 6 个数据集的综合实验中，实例化 Optimize-ARCUS 后的异常检测精度比 AE 模型的流变体、实例化后原自适应模型池算法分别提升 20.2% 和 5.83%. 且比现有在线异常检测算法的最佳精度高出 16.7%. 总的来说，Optimize-ARCUS 在面对复杂多变数据流时，能自适应概念漂移，准确识别异常.

关于 Optimize-ARCUS 也有很多发展方向. 首先，本算法选择自动编码器作为默认模型来实例化自适应模型池，主要是因为它结构简单和无监督学习机制. 未来研究可将 Optimize-ARCUS 扩展到 AE 之外的深度学习模型. 比如，生成对抗模型、递归神经网络模型等. 值得注意的是模型相似度的概念应该针对特定模型进行调整. 其次，模型池中的模型结构是否可从单一模型扩展到多种模型组合也值得探究. 再次，在联邦合并计算成本的实验中，Optimize-ARCUS 的平均消耗时间是比较长的，需要减少资源成本消耗. 最后，模型池可采用其他自适应策略，不是从 0 开始初始化模型或基于联邦学习的模型合并. 例如，模型的初始化和更新也可以利用基于迁移学习的方法共享公共知识，进一步优化.

参考文献

[1] NASSIF A BOU, TALIB M ABU, NASIR Q, et al. Machine learning for anomaly detection: A systematic review[J]. IEEE Access, 2021, 9: 78658-78700.

[2] 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.
SUN H L, LONG X, HAN L S, et al. Overview of anomaly detection techniques for industrial Internet of Things[J]. Journal on Communications, 2022, 43(3): 196-210. (in Chinese)

[3] 金明, 丁蓉. 一种联合时域和空域残差的网络异常检测与节点定位方法[J]. 电子学报, 2023, 51(5): 1172-1178.
JIN M, DING R. Detection and localization of outlier nodes in wireless sensor networks via jointing temporal and spatial residuals[J]. Acta Electronica Sinica, 2023, 51(5): 1172-1178. (in Chinese)

[4] LU T Y, WANG L, ZHAO X Y. Review of anomaly detection algorithms for data streams[J]. Applied Sciences, 2023, 13(10): 6353.

[5] 刘帅, 乔颖, 罗雄飞, 等. 时序数据库关键技术综述[J]. 计算机研究与发展, 2024, 61(3): 614-638.
LIU S, QIAO Y, LUO X F, et al. Key techniques of time series databases: A survey[J]. Journal of Computer Research and Development, 2024, 61(3): 614-638. (in Chinese)

[6] 陆克中, 陈超凡, 蔡桓, 等. 面向概念漂移和类不平衡数据流的在线分类算法[J]. 电子学报, 2022, 50(3): 585-597.
LU K Z, CHEN C F, CAI H, et al. Online classification algorithm for concept drift and class imbalance data stream[J]. Acta Electronica Sinica, 2022, 50(3): 585-597. (in Chinese)

[7] PANG G S, SHEN C H, CAO L B, et al. Deep learning for anomaly detection: A review[J]. ACM Computing Surveys, 2021, 54(2): 38.

[8] WANG R Y, NIE K X, WANG T, et al. Deep learning for anomaly detection[C]//Proceedings of the 13th International Conference on Web Search and Data Mining. New York: ACM, 2020: 894-896.

[9] 蒋洪迅, 江俊毅, 梁循. 基于机器学习的信用卡交易欺诈检测研究综述[J]. 计算机工程与应用, 2023, 59(21): 1-25.
JIANG H X, JIANG J Y, LIANG X. Survey on credit card transaction fraud detection based on machine learning[J]. Computer Engineering and Applications, 2023, 59(21): 1-25. (in Chinese)

[10] CHOI K, YI J H, PARK C, et al. Deep learning for anomaly detection in time-series data: Review, analysis, and guidelines[J]. IEEE Access, 2021, 9: 120043-120065.

[11] SCHLIMMER J C, GRANGER R H. Incremental learning from noisy data[J]. Machine Learning, 1986, 1(3): 317-354.

[12] 文益民, 刘帅, 缪裕青, 等. 概念漂移数据流半监督分类综述[J]. 软件学报, 2022, 33(4): 1287-1314.
WEN Y M, LIU S, MIAO Y Q, et al. Survey on semi-supervised classification of data streams with concept drifts[J]. Journal of Software, 2022, 33(4): 1287-1314. (in

Chinese)

[13] SOUZA V M A, DOS REIS D M, MALETZKE A G, et al. Challenges in benchmarking stream learning algorithms with real-world data[J]. Data Mining and Knowledge Discovery, 2020, 34(6): 1805-1858.

[14] 韩光洁, 赵腾飞, 刘立, 等. 基于多元区域集划分的工业数据流概念漂移检测[J]. 电子学报, 2023, 51(7): 1906-1916.
HAN G J, ZHAO T F, LIU L, et al. Concept drift detection of industrial data flow based on multivariate region set partition[J]. Acta Electronica Sinica, 2023, 51(7): 1906-1916. (in Chinese)

[15] BHATIA S, JAIN A, LI P, et al. Mstream: Fast anomaly detection in multi-aspect streams[C]//Proceedings of the Web Conference 2021. New York: ACM, 2021: 3371-3382.

[16] YOON S, SHIN Y, LEE J G, et al. Multiple dynamic outlier-detection from a data stream by exploiting duality of data and queries[C]//Proceedings of the 2021 International Conference on Management of Data. New York: ACM, 2021: 2063-2075.

[17] YOON S, LEE Y, LEE J G, et al. Adaptive model pooling for online deep anomaly detection from a complex evolving data stream[C]//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York: ACM, 2022: 2347-2357.

[18] GUO T, XU Z, YAO X, et al. Robust online time series prediction with recurrent neural networks[C]//2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA). Piscataway: IEEE, 2016: 816-825.

[19] MALHOTRA P, RAMAKRISHNAN A, ANAND G, et al. LSTM-based encoder-decoder for multi-sensor anomaly detection[EB/OL]. (2016-07-01) [2023-08-01]. http://arxiv.org/abs/1607.00148.

[20] LI G, JUNG J J. Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges[J]. Information Fusion, 2023, 91(C): 93-102.

[21] WANG H Z, BAH M J, HAMMAD M. Progress in outlier detection techniques: A survey[J]. IEEE Access, 2019, 7: 107964-108000.

[22] QIN X, CAO L, RUNDENSTEINER E A, et al. Scalable kernel density estimation-based local outlier detection over large data streams[C]//22nd International Conference on Extending Database Technology (EDBT). Spain: OpenProceedings, 2019: 421-432.

[23] YOON S, LEE J G, LEE B S. Ultrafast local outlier detection from a data stream with stationary region skipping[C]//Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. New York: ACM, 2020: 1181-1191.

[24] YOON S, LEE J G, LEE B S. NETS[J]. Proceedings of the VLDB Endowment, 2019, 12(11): 1303-1315.

[25] SALEHI M, LECKIE C, BEZDEK J C, et al. Fast memory efficient local outlier detection in data streams[J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(12): 3246-3260.

[26] BLÁZQUEZ-GARCÍA A, CONDE A, MORI U, et al. A review on outlier/anomaly detection in time series data[J]. ACM Computing Surveys, 54(3): 56.

[27] HILAL W, GADSDEN S A, YAWNEY J. Financial fraud: A review of anomaly detection techniques and recent advances[J]. Expert Systems with Applications, 2022, 193: 116429.

[28] QI S. Deep Autoencoding gaussian mixture model for unsupervised anomaly detection[C]//International Conference on Learning Representations. Vancouver: OpenReview, 2018: 1-19.

[29] LAI C H, ZOU D M, LERMAN G. Robust subspace recovery layer for unsupervised anomaly detection[EB/OL]. (2019-03-30) [2023-08-01]. http://arxiv.org/abs/1904.00152.

[30] KIM K H, SHIM S, LIM Y, et al. Rapp: Novelty detection with reconstruction along projection pathway[C]//International Conference on Learning Representations. Ethiopia: OpenReview, 2020: 1-10.

[31] LU W N, CHENG Y, XIAO C, et al. Unsupervised sequential outlier detection with deep architectures[J]. IEEE Transactions on Image Processing, 2017, 26(9): 4321-4330.

[32] XIANG Q Y, ZI L L, CONG X, et al. Concept drift adaptation methods under the deep learning framework: A literature review[J]. Applied Sciences, 2023, 13(11): 6515.

[33] SUÁREZ-CETRULO A L, QUINTANA D, CERVANTES A. A survey on machine learning for recurring concept drifting data streams[J]. Expert Systems with Applications, 2023, 213: 118934.

[34] 穆栋梁, 韩萌, 李昂, 等. 概念漂移复杂数据流分类方法综述[J]. 计算机应用, 2023, 43(6): 1664-1675.
MU D L, HAN M, LI A, et al. Overview of classification methods for complex data streams with concept drift[J]. Journal of Computer Applications, 2023, 43(6): 1664-1675. (in Chinese)

[35] BANK D, KOENIGSTEIN N, GIRYES R. Autoencoders[EB/OL]. (2020-03-12) [2023-08-01]. http://arxiv.org/abs/2003.05991.

[36] FRIEDRICH B, SAWABE T, HEIN A. Unsupervised statistical concept drift detection for behaviour abnormality detection[J]. Applied Intelligence, 2023, 53(3): 2527-2537.

[37] ASHFAHANI A, PRATAMA M, LUGHOFER E, et al. DEVDAN: Deep evolving denoising autoencoder[J]. Neurocomputing, 2020, 390: 297-314.

[38] BHATIA S, JAIN A, SRIVASTAVA S, et al. MemStream: Memory-based streaming anomaly detection[C]// Proceedings of the ACM Web Conference 2022. New York: ACM, 2022: 610-621.

[39] GAMA J, SEBASTIÃO R, RODRIGUES P P. On evaluating stream learning algorithms[J]. Machine Learning, 2013, 90(3): 317-346.

[40] GAMA J, MEDAS P, CASTILLO G, et al. Learning with drift detection[C]//Brazilian Symposium on Artificial Intelligence. Berlin: Springer, 2004: 286-295.

[41] WANG X M, CHEN W, XIA J Z, et al. ConceptExplorer: Visual analysis of concept drifts in multi-source time-series data[C]//2020 IEEE Conference on Visual Analytics Science and Technology (VAST). Piscataway: IEEE, 2020: 1-11.

[42] XIONG W L, HE D F, MU J B, et al. Adaptive stochastic model predictive control via network ensemble learning[J]. International Journal of Systems Science, 2023, 54(16): 3013-3026.

[43] FRÍAS-BLANCO I, DEL CAMPO-ÁVILA J, RAMOS-JIMÉNEZ G, et al. Online and non-parametric drift detection methods based on hoeffding's bounds[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(3): 810-823.

[44] BIFET A, GAVALDÀ R. Learning from time-changing data with adaptive windowing[C]//Proceedings of the 2007 SIAM International Conference on Data Mining. Philadelphia: Society for Industrial and Applied Mathematics, 2007: 443-448.

[45] KORNBLITH S, NOROUZI M, LEE H, et al. Similarity of neural network representations revisited[EB/OL]. (2019-05-01)[2023-08-01]. http://arxiv.org/abs/1905.00414.

[46] 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.

[47] SHIN S Y, JO G, WANG G X. A novel method for fashion clothing image classification based on deep learning[J]. Journal of Information and Communication Technology, 2023, 22(1): 127-148.

[48] YANG Y J, WANG W, FU H Y, et al. On supervised feature selection from high dimensional feature spaces[EB/OL]. (2022-03-22)[2023-08-01]. http://arxiv.org/abs/2203.11924.

[49] VERGARA A, VEMBU S, AYHAN T, et al. Chemical gas sensor drift compensation using classifier ensembles[J]. Sensors and Actuators B: Chemical, 2012, 166/167: 320-329.

[50] LOSING V, HAMMER B, WERSING H. KNN classifier with self adjusting memory for heterogeneous concept drift[C]//2016 IEEE 16th International Conference on Data Mining (ICDM). Piscataway: IEEE, 2016: 291-300.

[51] CAMPOS G O, ZIMEK A, SANDER J, et al. On the evaluation of unsupervised outlier detection: Measures, datasets, and an empirical study[J]. Data Mining and Knowledge Discovery, 2016, 30(4): 891-927.

作者简介

项秋艳 女,1998 年 7 月出生,湖南省长沙人. 重庆师范大学计算机与信息科学学院计算机技术专业硕士. 研究方向为深度学习、异常检测、数据可视化.

E-mail: 2021210516082@stu.cqnu.edu.cn

訾玲玲 女,1981 年 12 月出生,辽宁阜新人. 重庆师范大学计算机与信息科学学院副教授. 研究方向为深度学习、计算机视觉、多媒体处理.

E-mail: lingling19812004@126.com

丛 鑫 男,1982 年 2 月出生,辽宁阜新人. 重庆师范大学计算机与信息科学学院副教授. 研究方向为云计算、虚拟网络映射、深度学习.