基于多源双注意力与跨源一致性约束的智慧水务工业控制系统异常检测方法

胡浩[1] 廖玉婷[1] 马润翔[1] 史定川[1] 李敏[2*]

1.绵阳师范学院地理与环境学院，中国·四川 绵阳 621000

2.宜宾学院，中国·四川 宜宾 644000

摘要：针对智慧水务工业控制系统多源运行信息在语义、动态特征及关联关系上的差异，提出一种具有跨源一致性约束的多源双注意力双向长短期记忆网络（MSDA-BiLSTM-CCN）异常检测方法。模型保持物理运行侧、控制状态侧和网络代理侧的来源结构，利用来源内特征注意力与参数互不共享的 BiLSTM 进行变量重标定和时序建模，经多源融合后采用时间注意力聚合历史信息；并依据网络代理侧—控制状态侧的数据派生关系和控制状态侧—物理运行侧的闭环响应关系，引入双关系跨源一致性辅助约束。独立测试结果表明，模型 AP、F1 和 FPR 分别为 0.8522、0.7760 和 0.615%，较 BiLSTM 的 AP 和 F1 提高 28.16 和 23.44 个百分点；引入 CCN 后，AP 和 F1 进一步提高 5.07 和 4.85 个百分点。结果表明，该方法能够有效利用多源结构差异及跨源关联信息，可改善智慧水务工业控制系统的异常检测性能。

关键词：智慧水务；多源时序；双注意力；跨源一致性约束；异常检测

Anomaly Detection for Smart Water Industrial Control Systems Using Multi-Source Dual Attention and Cross-Source Consistency Constraints

Hu Hao[1], Liao Yuting[1], Ma Runxiang[1], Shi Dingchuan[1], Li Min[2*]

1.School of Geography and Environment, Mianyang Teachers' College, China Sichuan Mianyang 621000

2.Yibin University, China Sichuan Yibin 644000

Abstract: To address the differences in semantics, dynamic characteristics, and inter-source relationships among multi-source operational information in smart water industrial control systems,a Multi-Source Dual-Attention BiLSTM with Cross-Source Consistency Network (MSDA-BiLSTM-CCN) is proposed for anomaly detection.The model preserves the source structures of physical-operation, control-state,and network-proxy data. Source-wise feature attention and BiLSTM branches with non-shared parameters are employed for variable reweighting and temporal modeling,respectively,followed by multi-source fusion and temporal attention to aggregate historical information. In addition, auxiliary cross-source consistency constraints over two source relationships are introduced according to the data derivation relationship between the network-proxy and control-state sources and the closed-loop response relationship between the control-state and physical-operation sources.Results on the independent test set show that the proposed model achieves an AP of 0.8522,an F1 score of 0.7760,and an FPR of 0.615%.Compared with BiLSTM,AP and F1 are improved by 28.16 and 23.44 percentage points,respectively.After introducing CCN,AP and F1 are further improved by 5.07 and 4.85 percentage points,respectively.The results demonstrate that the proposed method can effectively exploit structural differences among multiple data sources and cross-source relational information,thereby improving anomaly detection performance in smart water industrial control systems.

Keywords: Smart water; Multi-source time series; Dual attention; Cross-source consistency constraint; Anomaly detection

0 引言

智慧水务工业控制系统持续产生工艺测量、控制状态等多类型时序数据，不同信息在数据形式、动态特征及相互关系上存在差异。异常不仅表现为局部变量偏离，也可能伴随时间依赖或相关运行信息关系的变化。因此，异常检测需要兼顾来源差异、时序依赖及相关信息之间的有效

关联[1-2]。

近年来，近年来，注意力机制[3]、图注意力与时空图方法[4]被用于多变量时序异常检测；相关研究进一步从时空关系建模[5-6]和变量关系挖掘[7]等方面增强异常表征，并将多层图注意力应用于工业控制场景[8]。对比学习[9-10]及其自监督、多粒度扩展[11-12]也逐步用于时序异常检测。工业控制与信息物理系统进一步利用变量关联及时空状态信息增强异常识别[13-14]。

针对上述问题，本文提出多源双注意力双向长短期记忆网络与一致性约束网络（Multi-source Dual-Attention BiLSTM with Cross-Source Consistency Network，MSDA-BiLSTM-CCN，MSDA-BiLSTM-CCN）异常检测模型。模型保持物理运行侧、控制状态侧和由控制状态历史变化派生的网络代理侧三类输入结构，在来源内部完成变量重标定与时序建模，并在融合后聚合窗口历史信息；同时依据网络代理侧—控制状态侧的数据派生关系和控制状态侧—物理运行侧的闭环响应关系，引入双关系跨源一致性约束作为训练辅助目标。模型性能通过统一实验协议下的对比、消融及参数敏感性实验进行验证。

1 数据集与多源时序样本构建

1.1 数据来源与任务定义

采用新加坡科技设计大学 iTrust 研究中心公开的 SWaT 水处理工业控制数据[15]。对 Normal 数据去重并移除 7 个结构性缺失字段，经时间排序与连续段识别后，共保留 946719 个时间点和 44 个原始变量，其中物理运行变量 24 个、控制状态变量 20 个。本文将异常检测定义为监督式窗口末端二分类，以长度为 T 的历史窗口作为输入，步长为 1，标签取窗口末端时刻的原始 Normal/Attack 状态；最终模型配置取 $T=60$。

1.2 多源特征构建与数据隔离

在 24 维物理运行和 20 维控制状态特征基础上，根据控制状态当前值及历史变化构造状态变化标记、60 步历史变化次数、状态持续时长和 60 步控制变化总量，形成 61 维网络代理侧控制行为特征，单个时间位置共 105 维输入。网络代理侧用于表征控制行为变化，并非独立采集的网络报文、五元组或工业协议流量。

数据按时间顺序划分为训练主体、内部验证集、外部验证集和测试集，有效窗口数分别为 610442、152522、107801 和 75541。标准化参数仅由训练主体估计；内部验证集用于训练监控与 TPE 候选配置评价，外部验证集用于判别阈值确定，测试集用于最终独立评价。所有特征统计和窗口构造均限制在所属数据分层与连续段内。

2 MSDA-BiLSTM-CCN 异常检测方法

2.1 模型总体框架

考虑物理运行侧、控制状态侧和网络代理侧在变量组成与动态特征上的差异，MSDA-BiLSTM-CCN 采用来源结构保持的分层建模方式。三类输入分别经过参数互不共享的来源内编码和特征注意力（Feature Attention，FA），再由参数互不共享的 BiLSTM 分支提取来源内时序表示；随后，三个分支的隐藏状态在相同时间位置沿特征维 Concat，并通过时间注意力（Temporal Attention，TA）聚合窗口历史信息。与此同时，CCN 从融合前的 BiLSTM 隐藏表示处分流，对具有明确关系依据的跨源表示施加辅助一致性约束，其投影结果不参与多源融合、TA 及最终分类。

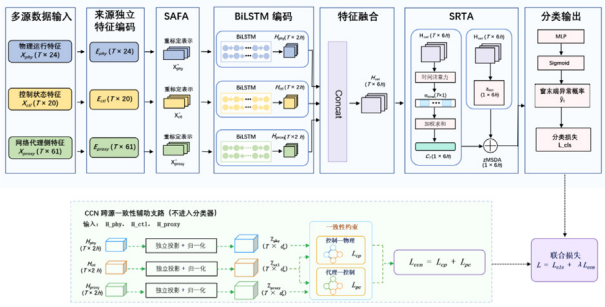


图 1 MSDA-BiLSTM-CCN 总体模型架构

2.2 来源内特征重标定与时序建模

三类输入分别经参数互不共享的来源内编码形成变量表示，编码前后变量维度与索引对应关系保持不变，不进行跨来源混合[16-17]。设来源索引为 s，时刻 t 的来源输入为 $\mathbf{x}_t^s$，来源内编码表示为：

$$\mathbf{e}_t^s = f_{\text{enc}}^s(\mathbf{x}_t^s;\theta_s), \qquad \mathbf{e}_t^s \in \mathbb{R}^{d_s} \tag{1}$$

其中，d_s 为对应来源的变量数，三组编码参数互不共享。FA 采用两层加性打分网络计算变量得分，并仅在各来源内部执行 Softmax 归一化和重标定：

$$\mathbf{q}_t^s = \mathbf{W}_{f,2}^s \tanh\left(\mathbf{W}_{f,1}^s \mathbf{e}_t^s + \mathbf{b}_{f,1}^s\right) + \mathbf{b}_{f,2}^s \tag{2}$$

$$\alpha_{t,j}^s = \frac{\exp\left(q_{t,j}^s\right)}{\sum_{k=1}^{d_s}\exp\left(q_{t,k}^s\right)}, \qquad \tilde{\mathbf{e}}_t^s = \boldsymbol{\alpha}_t^s \odot \mathbf{e}_t^s \tag{3}$$

物理运行侧、控制状态侧和网络代理侧分别在 24、20 和 61 维变量空间内独立计算注意力权重，而非在 105 维联合空间内统一归一化。重标定后的三类序列分别输入参数互不共享的 BiLSTM 分支，以学习来源内部的时序依赖[18-19]。对于窗口内第 τ 个时间位置，前向与反向隐藏状态沿特征维拼接为：

$$\mathbf{h}_\tau^s = \left[\overrightarrow{\mathbf{h}}_\tau^s, \overleftarrow{\mathbf{h}}_\tau^s\right], \qquad s \in \{\text{phy}, \text{ctl}, \text{proxy}\} \tag{4}$$

双向编码仅在当前历史窗口内部进行，不使用检测时刻之后的信息。

2.3 多源融合与时间信息聚合

完成来源内时序建模后，三个分支在相同时间位置沿特征维进行拼接：

$$\mathbf{h}_\tau = \left[\mathbf{h}_\tau^{\text{phy}}; \mathbf{h}_\tau^{\text{ctl}}; \mathbf{h}_\tau^{\text{proxy}}\right] \tag{5}$$

Concat 后得到保持时间位置对应关系的多源融合序列。考虑不同历史位置对窗口末端判别的贡献存在差异，在融合序列上采用 TA 进行时间维聚合[20]。第 τ 个历史位置的注意力得分及归一化权重为：

$$a_\tau = \mathbf{v}_T^{\top}\tanh(\mathbf{W}_T\mathbf{h}_\tau + \mathbf{b}_T), \qquad \beta_\tau = \frac{\exp(a_\tau)}{\sum_{k=1}^{T}\exp(a_k)} \tag{6}$$

并得到加权时序上下文：

$$\mathbf{c}_T = \sum_{\tau=1}^{T}\beta_\tau \mathbf{h}_\tau, \tag{7}$$

为保留与末端标签直接对应的状态信息，将时间上下文与窗口末端隐藏状态残差相加：

$$\mathbf{z} = \mathbf{c}_T + \mathbf{h}_T \tag{8}$$

所得 $\mathbf{z}$ 经 MLP 和 Sigmoid 映射后输出窗口末端异常概率。

2.4 双关系跨源一致性约束

为约束具有明确结构联系的跨源隐藏表示[30]。为利用已有结构联系，CCN 将多源融合前三个 BiLSTM 分支的完整时序表示投影至共同潜在空间，并依次进行 LayerNorm 和 L_2 归一化。两类一致性损失在批量维和时间维上计算相关归一化表示的平均平方欧氏距离：

$$L_{pc} = \frac{1}{BT}\sum_{b=1}^{B}\sum_{\tau=1}^{T}\left\|\mathbf{u}_{b,\tau}^{\text{proxy}} - \mathbf{u}_{b,\tau}^{\text{ctl}}\right\|_2^2 \tag{8}$$

$$L_{cp} = \frac{1}{BT}\sum_{b=1}^{B}\sum_{\tau=1}^{T}\left\|\mathbf{u}_{b,\tau}^{\text{ctl}} - \mathbf{u}_{b,\tau}^{\text{phy}}\right\|_2^2 \tag{9}$$

其中，L_{pc} 对应网络代理侧—控制状态侧的数据派生关系，L_{cp} 对应控制状态侧—物理运行侧的闭环响应关系。不设置网络代理侧—物理运行侧直接约束。两类一致性损失仅作为训练辅助项，与窗口末端分类损失共同构成联合目标：

$$L = L_{\text{cls}} + \lambda_{pc}L_{pc} + \lambda_{cp}L_{cp} \tag{10}$$

其中，L_{cls} 为窗口末端二分类损失，λ_{pc} 和 λ_{cp} 分别为两类一致性损失权重。CCN 的投影表示和一致性损失均不直接参与异常概率或阈值计算，推理阶段仅保留主分类路径。

3 实验结果与分析

3.1 实验设置与对比方法

为保证比较一致性，各模型采用相同的数据划分、重复实验方案和评价流程，结构特有参数按各自配置确定。所有模型均采用随机种子 42～46 重复 5 次，结果以均值 ± 样本标准差表示。考虑异常检测中的类别不均衡及工业控制场景对误报的敏感性，本文以以平均精度（Average Precision，AP）为主要评价指标，并采用 F1 和假阳性率（False Positive Rate，FPR）表征冻结工作点下的识别性能和误报水平。AP 由连续异常得分计算；F1 和 FPR 基于外部验证集确定的判别阈值计算。各模型—随机种子组合在外部验证集中从满足 FPR ≤ 2% 的候选工作点中选择 F1 最高的阈值，冻结后直接用于测试集。

MSDA-BiLSTM-CCN 的结构与主要训练超参数采用 Optuna TPE 联合搜索。共执行 150 次 Trial，每个候选配置仅利用训练主体更新模型参数，以 5 个固定随机种子在内部验证集上的平均 AP 作为主要评价依据，外部验证集和测试集均不参与超参数选择。最终模型采用 $T=60$，BiLSTM 单方向隐藏维度为 64、层数为 2，FA、TA 和 CCN 隐含维度均为 64，dropout 为 0.30，$\lambda_{pc}=\lambda_{cp}=0.05$；采用 AdamW 优化器，学习率为 1×10^{-3}，batch size 为 256，最大训练轮数为 100，早停耐心为 12，训练采样中异常与正常样本比例为 1∶3，pos_weight=1。

选对比模型包括 RF、XGBoost、1D-CNN、TCN、LSTM、BiLSTM、CNN-BiLSTM，以及 MB-BiLSTM、MB-BiLSTM+FA、MB-BiLSTM+TA 和 MSDA-BiLSTM，完整 MSDA-BiLSTM-CCN 的独立测试结果见表 1。

表 1 测试集上不同模型的主要检测性能（均值 ± 样本标准差）

模型	AP	F1	FPR
RF	0.2924 ± 0.0525	0.3135 ± 0.0440	0.01996 ± 0.00336
XGBoost	0.3933 ± 0.0501	0.4108 ± 0.0458	0.01940 ± 0.00127
1D-CNN	0.5169 ± 0.0417	0.5067 ± 0.0295	0.01766 ± 0.00302
TCN	0.5053 ± 0.0394	0.4855 ± 0.0324	0.01849 ± 0.00189
LSTM	0.4951 ± 0.0175	0.4828 ± 0.0091	0.01946 ± 0.00204
BiLSTM	0.5706 ± 0.0201	0.5416 ± 0.0165	0.01814 ± 0.00213
CNN-BiLSTM	0.6345 ± 0.0320	0.5835 ± 0.0242	0.01953 ± 0.00234
MB-BiLSTM	0.6651 ± 0.0268	0.5987 ± 0.0266	0.01209 ± 0.00584
MB-BiLSTM+FA	0.7260 ± 0.0394	0.6547 ± 0.0348	0.01127 ± 0.00484
MB-BiLSTM+TA	0.7546 ± 0.0304	0.6850 ± 0.0210	0.01011 ± 0.00240
MSDA-BiLSTM	0.8015 ± 0.0313	0.7275 ± 0.0374	0.00729 ± 0.00097
MSDA-BiLSTM-CCN	0.8522 ± 0.0218	0.7760 ± 0.0207	0.00615 ± 0.00148

表 2 外部验证集上来源与核心模块消融结果（均值 ± 样本标准差）

配置	AP	F1	FPR
仅物理运行侧	0.3518 ± 0.0641	0.3855 ± 0.0492	0.01750 ± 0.00353
去物理运行侧	0.4643 ± 0.0193	0.4788 ± 0.0195	0.01701 ± 0.00174
去控制状态侧	0.5734 ± 0.0199	0.5598 ± 0.0203	0.01174 ± 0.00121
去网络代理侧	0.5620 ± 0.0532	0.5510 ± 0.0335	0.01291 ± 0.00451
去 FA	0.6938 ± 0.0327	0.6540 ± 0.0134	0.00893 ± 0.00175
去 TA	0.6591 ± 0.0170	0.6226 ± 0.0193	0.01094 ± 0.00204
去 CCN	0.7325 ± 0.0280	0.6828 ± 0.0268	0.00852 ± 0.00080
完整模型	0.7614 ± 0.0343	0.7063 ± 0.0335	0.00680 ± 0.00162

完整模型取得最高 AP、F1 及最低 FPR，较 MB-BiLSTM 的 AP 和 F1 分别提高 18.71 和 17.73 个百分点，较 MSDA-BiLSTM 进一步提高 5.07 和 4.85 个百分点，表明多源双注意力建模与跨源一致性约束均能提升检测性能。

3.2 来源与核心模块消融

为分析不同输入来源及 FA、TA 和 CCN 的作用，在完整模型基础上分别进行来源和模块消融，各配置均重新训练，并采用相同的数据划分、随机种子和评价规则，结果见表 2。

来源消融结果表明，三类输入之间具有一定的信息互补性；模块消融结果表明，移除 FA、TA 或 CCN 后模型性能均有所下降，说明变量重标定、时间信息聚合及跨源一致性约束均有助于提升异常检测性能。

3.3 参数敏感性

在其余模型与训练配置保持不变的条件下，分别考察输入上下文长度 T 和一致性约束权重 λ 的单因素敏感性。其中，两类跨源一致性辅助损失采用相同权重并同步变化，结果见表 3。

表 3 输入上下文长度与一致性约束权重的单因素敏感性结果（均值 ± 样本标准差）

参数	取值	AP	F1
T	30	0.6372 ± 0.0212	0.6050 ± 0.0218
T	60	0.7614 ± 0.0343	0.7063 ± 0.0335
T	90	0.7233 ± 0.0360	0.6769 ± 0.0252
T	120	0.6810 ± 0.0331	0.6401 ± 0.0290
λ	0	0.7325 ± 0.0280	0.6828 ± 0.0268
λ	0.01	0.7397 ± 0.0188	0.6852 ± 0.0150
λ	0.03	0.7411 ± 0.0284	0.6890 ± 0.0269
λ	0.05	0.7614 ± 0.0343	0.7063 ± 0.0335
λ	0.08	0.7384 ± 0.0297	0.6875 ± 0.0274
λ	0.10	0.7047 ± 0.0254	0.6636 ± 0.0236
λ	0.20	0.6148 ± 0.0346	0.5927 ± 0.0283

当 T=60 时，λ=0.05 时模型性能最佳，继续增大两参数后性能均下降，表明输入上下文长度和一致性约束强度与模型性能呈非单调关系，过长的历史输入或过强的一致性约束未带来持续的性能增益。

4 结语

本文提出 MSDA-BiLSTM-CCN 异常检测方法，通过来源结构保持的多源双注意力建模和双关系跨源一致性辅助约束实现智慧水务工控异常检测。独立测试集上，模型 AP、F1 和 FPR 分别为 0.8522、0.7760 和 0.615%；引入 CCN 后，AP 和 F1 较 MSDA-BiLSTM 进一步提高 5.07 和 4.85 个百分点。消融结果表明，三类输入及 FA、TA、CCN 均对检测性能有积极作用。

参考文献：

[1] 谢丽霞，王嘉敏，杨宏宇等. 时间序列异常检测方法研究综述[J]. 中国民航大学学报，2024,42(3):1-12+18.

[2] 陈福荣，熊琛，李婷等. 时间序列异常检测综述[J]. 北京交通大学学报，2025,49(3):1-13.

[3] 杨超城，严宣辉，陈容均等. 融合双重注意力机制的时间序列异常检测模型[J]. 计算机科学与探索，2024,18(3):740-754.

[4] Zhao M, Peng H, Li L, et al. Graph attention network and informer for multivariate time series anomaly detection[J]. Sensors, 2024, 24(5): 1522.

[5] 肖刚，卢大鹏，郑文博等. 基于时空图注意力网络的多变量时序数据异常检测方法[J]. 浙江大学学报 (工学版)，2025,59(10):2134-2143.

[6] Zheng Y, Koh H Y, Jin M, et al. Graph spatiotemporal process for multivariate time series anomaly detection with missing values[J]. Information Fusion, 2024, 106: 102255.

[7] 胡智超，余翔湛，刘立坤等. 基于关系挖掘和注意力的多维时序异常检测[J]. 信息安全学报，2024,9(6):100-113.DOI:10.19363/J.cnki.cn10-1380/tn.2024.11.07.

[8] Lin L, Gu A, Min F, et al. Multi-level graph attention network-based anomaly detection in industrial control system[C]//Actuators. MDPI, 2025, 14(5): 210.

[9] 周丹，凌捷. 结合对比学习的双分支多维时间序列异常检测方法[J]. 计算机应用研究，2025,42(2):507-513. DOI:10.19734/j.issn.1001-3695.2024.07.0286.

[10] 吴雨露，凌捷. 基于双图与多层次对比的多变量时间序列异常检测方法[J]. 计算机应用研究，2026,43(3):

825-831.DOI:10.19734/j.issn.1001-3695.2025.07.0236.

[11] Darban Z Z, Webb G I, Pan S, et al. CARLA: Self-supervised contrastive representation learning for time series anomaly detection[J]. Pattern Recognition, 2025, 157: 110874.

[12] Xiao B W, Xing H J, Li C G. MulGad: Multi-granularity contrastive learning for multivariate time series anomaly detection[J]. Information Fusion, 2025, 119: 103008.

[13] 黄哲彬，杨根科. 基于关联差异的工业控制系统异常检测模型[J]. 微型电脑应用，2025,41(7):5-9.

[14] 孙海丽，黄炎，韩兰胜等. 基于无监督时空状态估计的信息物理系统细粒度异常诊断[J]. 通信学报，2025,46(7):45-59.

[15] Tang S, Ding Y, Wang H. Industrial control anomaly detection based on distributed linear deep learning[J]. Computers, Materials & Continua, 2025, 82(1): 1129-1150.

[16] 赵培，乔焰，胡荣耀等. 基于多域特征提取的多变量时间序列异常检测[J]. 计算机应用，2024,44(11):3419-3426.

[17] 蒋辉，闫秋艳，姜竹郡. 面向多元时间序列异常检测的对称正定自编码器方法[J]. 计算机应用，2024,44(10):3294-3299.

[18] 索逸凡，刘松华，郝秋智. 基于高阶特征聚合的时间序列异常检测方法[J]. 计算机应用，2026,46(4):1131-1138.

[19] 廖思睿，黄飞虎，战鹏祥等. DCDAD: 考虑上下文依赖差异化的时间序列异常检测模型[J]. 计算机科学，2025,52(6):106-117.

[20] 尹春勇，张不凡 . 基于多尺度的多变量时间序列异常检测模型[J]. 计算机应用，2026,46(3):790-797.

作者简介：第一作者：胡浩（2001-），男，汉族，四川广安人，硕士研究生，研究方向：生态环境信息智能处理。邮箱：2080025933@qq.com。

* 通讯作者：李敏（1975-），男，汉族，四川绵阳人，博士研究生，教授，研究方向：生态环境信息智能处理。邮箱：limin_mnu@163.com。