DOI：10.13334/j.0258-8013.pcsee.240744 **文章编号**：0258-8013 (2025) 19-7468-13 **中图分类号**：TM 73 **文献标识码**：A

基于自适应差分进化-模糊宽度学习系统的 FDIA 定位检测方法

席磊[1]，陈洪军[2]，彭典名[2]，王文卓[2]，白芳岩[2]

(1. 梯级水电站运行与控制湖北省重点实验室(三峡大学)，湖北省 宜昌市 443002；
2. 三峡大学电气与新能源学院，湖北省 宜昌市 443002)

FDIA Localization Method Based on Adaptive Differential Evolution and Fuzzy Broad Learning System

XI Lei[1], CHEN Hongjun[2], PENG Dianming[2], WANG Wenzhuo[2], BAI Fangyan[2]

(1. Hubei Provincial Key Laboratory for Operation and Control of Cascaded Hydropower Station (China Three Gorges University), Yichang 443002, Hubei Province, China; 2. College of Electrical Engineering and New Energy, China Three Gorges University, Yichang 443002, Hubei Province, China)

ABSTRACT: As a key component of the energy internet, cyber-physical power systems face the threat of false data injection attacks. Detection techniques for such attacks often neglect the localization of the attack injection, and research attempting to solve this problem has difficulty balancing detection accuracy and computation time. Therefore, this paper proposes a false data injection attack localization method based on adaptive differential evolution-fuzzy broad learning system. The proposed algorithm employs a fuzzy broad learning system with a transversal network structure to constitute the localization algorithm, which realizes the fast detection. Meanwhile, an adaptive differential evolution algorithm is proposed to perform feature selection on the measured data and eliminate the redundant features, which effectively improves the accuracy of the algorithm for location detection. Extensive simulations in IEEE-14 and 57-node systems verify that the proposed method is capable of precise localization of spurious data injection attacks, and has better accuracy, precision, recall, and F1-score compared with multiple traditional detection algorithms.

KEY WORDS: energy internet; cyber-physical power systems; false data injection attack; fuzzy broad learning system; differential evolution

摘要：作为能源互联网的关键组成部分，电力信息物理系统面临着虚假数据注入攻击的威胁。针对此类攻击的检测技术往往忽视攻击注入位置的定位检测，而试图解决这一问题的研究难以在检测精度和计算时间上取得平衡。因此，该文提出一种基于自适应差分进化-模糊宽度学习系统的定位检测方法。所提算法采用具有横向网络结构的模糊宽度学习系统构成定位检测算法，实现定位检测的快速响应。同时，提出一种自适应差分进化算法对量测数据进行特征选择，剔除其中的冗余特征，有效地提升算法的定位检测精确性。在 IEEE-14 和 57 节点系统中进行大量仿真，验证所提方法能够对虚假数据注入攻击进行精确定位，且与多种传统检测算法相比，具有更佳的准确率、精度、召回率和 F1-Score。

关键词：能源互联网；电力信息物理系统；虚假数据注入攻击；模糊宽度学习系统；差分进化

0 引言

能源互联网(energy internet，EI)的提出和发展加速了传统电网的智能化，电力信息物理系统(cyber-physical power system，CPPS)[1-3]逐渐成熟。作为 EI 的实现手段[4]，CPPS 中信息系统与物理系统的密切耦合[5-6]促进了能源网络中各类设备间的信息交流，提高了电网的感知性能和自适应能力，但也带来严峻的网络安全挑战。

EI 中物理设备的协调与交互以 CPPS 网络通信作为支撑，而虚假数据注入攻击(false data injection attack，FDIA)利用通信之间的漏洞，篡改系统的量测数据，破坏系统状态估计[7]，从而诱导控制中心做出错误决策[8]，造成经济和安全危害。结构良好的 FDIA[9-10]具有隐蔽性好、灵活性高和破坏力强等特

基金项目：国家自然科学基金项目(52277108, 52477104)；宜昌市自然科学研究项目(A23-2-001)。

Project Supported by National Natural Science Foundation of China (52277108, 52477104); Yichang Municipal Natural Science Foundation (A23-2-001).

点，被认为是对 CPPS 安全最具挑战性的威胁之一。

实现对 FDIA 的检测是保护 CPPS 免受此类攻击威胁的必要措施。在 CPPS 已有的安全防护机制中，入侵检测系统通过分析系统的流量和行为模式检测潜在的入侵行为。但文献[11]指出，该系统通常不具备对特定协议深入分析的能力，无法直接应用于解释电力数据和参数，检测结果存在高误报率的问题。随着技术的发展，提出了诸多先进检测方法。文献[12]综述近年来的相关文献，并将已有检测方法划分为基于数据驱动和模型驱动两类。

基于模型驱动的检测方法是国内外研究中的常用方法[13-16]，具有较强的可解释性和移植性。但此类方法的实现高度依赖电网模型，其精度和效率在很大程度上受制于电网建模的准确性。由于愈加智能化的电网呈现出高度复杂的非线性特征，建立一个准确的电网模型愈发具有挑战性，因此，模型驱动的检测方法在实际应用中难以实施。

数据驱动的检测方法利用人工智能算法挖掘量测数据中的离群特性，进而实现检测 FDIA。文献[17]关注电网的边缘特征，将动态边缘条件滤波器融入图卷积运算中，用来处理不同图形结构的数据集，在 FDIA 的检测中展现出有效的可扩展性；文献[18]融合迁移学习和深度信念网络，利用源域无标签样本逐层训练网络，再配合目标域训练适配层和微调全网络，克服受攻击标签样本稀缺的问题；文献[19]考虑数据不平衡的影响，利用改进的生成对抗网络重新平衡正常和受攻击的数据样本，并采用极端随机树对其进行分类，实现高精度的攻击检测；集成学习解决了权值和偏置随机性网络的不稳定问题，文献[20]使用高斯随机分布和拉丁超立方体采样对基础分类器的权重进行初始化，提升了集成极限学习机的检测泛化性能；文献[21]提出一种多头图注意力网络和时间卷积网络相结合的 FDIA 检测方法。该方法考虑电网拓扑的连接关系与量测数据的空间相关性，实现检测模型在空间维度的可解释性。

上述研究虽然避免了模型驱动方法依赖参数的缺陷，但忽略了对攻击注入位置的定位检测问题。而精确定位 FDIA 对防御措施[22]的部署尤为重要。现有研究多采用深度学习实现定位检测。如文献[23-24]基于卷积神经网络(convolutional neural network，CNN)提出不同的网络结构，利用 CNN 的分析量测数据的不一致性，实现对量测异常的定位检测；文献[25]利用门控循环单元表征测量数据的时间相关性，并将其集成至变分自编码器中，提出一种有效的 FDIA 定位检测框架。虽然深度学习方法展现出优异的定位检测性能，但往往需要丰富的训练数据和复杂的网络结构，且网络层间的耦合需要大量的超参数，这使整体算法容易与数据集过度拟合消耗大量时间，难以具备快速响应能力。

为克服上述缺陷，具有横向网络结构的宽度学习系统(broad learning system，BLS)[26]被提出，其通过伪逆快速计算输出权重，避免对整体算法的重新训练。因此，BLS 算法在训练时间上远少于深度网络算法。在此基础上，文献[27]将 Takagi-Sugeno 模糊理论融入 BLS 中，提出模糊宽度学习系统(fuzzy BLS，FBLS)，该方法用一组模糊子系统替代传统的特征节点，利用模糊系统的逻辑推理能力处理输入的原始数据，有效提升 BLS 处理不确定和非线性问题的能力。此外，FBLS 保留 BLS 的基本机构，仍然具备快速学习的优势。

然而，在面临高维数据特征时，FBLS 中间层节点往往会传递一些不相关或冗余的数据特征，显著影响算法的泛化能力和检测精度。特征选择[28]是处理特征冗余的有效技术，从原始特征中选择特征子集降低特征维度。所选子集虽小但涵盖的信息量能够有效识别目标，一定程度上能够提高算法的检测性能。近年来，进化计算技术在特征选择方法的设计中受到关注。文献[29]对应用此类技术实现特征选择进行概述。其中，差分进化(differential evolution，DE)算法因其简单、高效的优点被许多研究采用；文献[30]提出一种改进的 DE 算法，通过从丰富的策略池中选择进化策略，提高最优解的求解精度，但该方法因处理不同任务时需重新设计策略池而缺乏适用性；文献[31]将相关性测度融入 DE，增强 DE 的收敛速度，但在处理大规模的特征选择时，该方法会因静态变异因子和交叉概率而缺乏探索能力，从而陷入局部最优的困境。

因此，本文将一种自适应策略融入 DE 中对变异因子及交叉概率进行优化，提出基于自适应差分进化-模糊宽度学习系统(adaptive differential evolution FBLS，ADE-FBLS)的 FDIA 定位检测方法。所提方法首次应用 FBLS 对 FDIA 进行定位检测，并采用 ADE 算法剔除原始数据的冗余，降低特征维度以提升 FBLS 的泛化能力和检测性能。通过在不同攻击场景下进行大量仿真实验，验证所提

方法的有效性。

1 问题描述

1.1 FDIA 及 BDD 原理

针对 CPPS 中的 FDIA 如图 1 所示。虚假数据的注入是一个多阶段的复杂过程，为绕过或破坏电网的安全防护，攻击者通常以发电厂、变电站和通信信道等作为依托来发起攻击。CPPS 对调度中心内部的通信防护手段十分严密[32]，攻击难以渗透。而布置在 CPPS 中的传感器分布广泛且众多，保护措施无法全面覆盖，安全性相对薄弱，因此，FDIA 往往对传感设备间的通信发起。

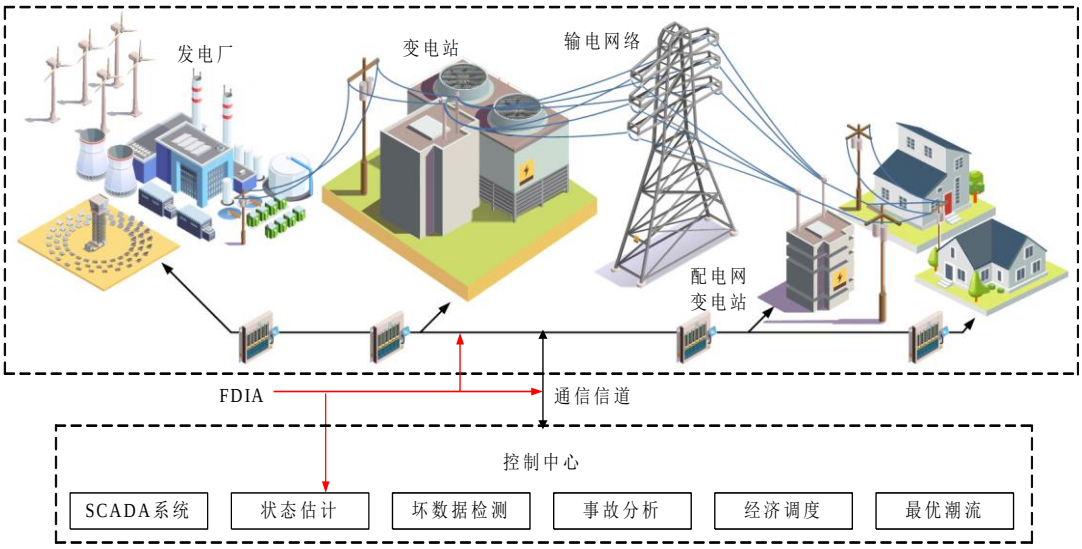


图 1 CPPS 中的 FDIA 示意图

Fig. 1 Schematic diagram of FDIA in CPPS

攻击者通过向远程终端单元采集的量测数据中注入攻击向量，干扰电网正常的状态估计[33]，造成状态变量偏移，进而误导调度中心做出错误决策，从而达到攻击目的。考虑 n 个节点的交流电网，正常状态下的状态估计可表述为

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{1}$$

式中：$\boldsymbol{z}\in\mathbb{R}^m$ 为 m 维的量测值；$\boldsymbol{x}\in\mathbb{R}^{2n}$，为 $2n$ 维的系统状态变量；$\boldsymbol{h}$ 为前两者之间的非线性映射关系；$\boldsymbol{e}\in\mathbb{R}^m$ 为服从高斯分布的随机测量误差。状态估计的目的是从仪表量测值 $\boldsymbol{z}$ 和测量噪声 $\boldsymbol{e}$ 中估计出系统状态 x。

传统的坏数据检测器(bad data detection，BDD)[34]通过残差分析检测并剔除具有较大误差和隐匿性较弱的异常数据。残差的表达式为 $\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{h}(x)$，若残差的 L2 范数大于预定义的阈值 τ，则认为系统中存在异常数据；反之，则不存在。

为绕过上述检测机制，攻击者向原始量测值 $\boldsymbol{z}$ 中注入攻击向量 $\boldsymbol{a}$，使控制中心收到的量测数据变为 $\boldsymbol{z}_a=\boldsymbol{z}-\boldsymbol{a}$。使用 $\boldsymbol{z}_a$ 进行状态估计得到的状态估计值也同样受到影响。此时，攻击后的系统残差 $\boldsymbol{r}_a$ 为

$$\begin{aligned}\boldsymbol{r}_a=\boldsymbol{z}_a-\boldsymbol{h}(\hat{\boldsymbol{x}}_a)=\ &\boldsymbol{z}-\boldsymbol{h}(\hat{\boldsymbol{x}})+\boldsymbol{a}-[\boldsymbol{h}(\hat{\boldsymbol{x}}_a)-\boldsymbol{h}(\hat{\boldsymbol{x}})]=\\ &\boldsymbol{r}+\boldsymbol{a}-[\boldsymbol{h}(\hat{\boldsymbol{x}}_a)-\boldsymbol{h}(\hat{\boldsymbol{x}})]\end{aligned} \tag{2}$$

式中 $\hat{\boldsymbol{x}}$ 和 $\hat{\boldsymbol{x}}_a$ 为攻击前后状态变量的估计值。若攻击者精心设计后的攻击向量 $\boldsymbol{a}=\boldsymbol{h}(\hat{\boldsymbol{x}}_a)-\boldsymbol{h}(\hat{\boldsymbol{x}})$，则可保持攻击前后系统残差保持一致，即 $\boldsymbol{r}_a=\boldsymbol{r}$，成功躲过 BDD，篡改量测数据，实现 FDIA。

1.2 FDIA 模型

以往的攻击手段通常使用线性直流模型[35]来近似电网的非线性交流模型，这与实际交流电网运行情况相悖，缺乏普适性和有效性。随着信息技术与现代电网的紧密结合，CPPS 中布置的同步相量测量单元(phasor measurement unit，PMU)[36]设备逐渐增加，基于数据采集与监控(supervisory control and data acquisition，SCADA)系统的状态估计器向混合状态估计器发展。因此，如果攻击者只篡改由 SCADA 采集的量测数据将难以逃避控制中心的识别。为此，本文采用一个更具通用性的非线性网络 FDIA 模型[20]对配置了一定数量 PMU 设备的交流电力系统实施攻击，通过篡改 SCADA 和 PMU 采集的量测数据使某条传输线路过载。

攻击模型由以下优化问题表述：

$$\text{Objective: min} \left\| \boldsymbol{z}_a^{\mathcal{O}_A} - \boldsymbol{h}(x_a) \right\|_0 \tag{3}$$

$$\text{s.t.} \quad \sqrt{(P_a^l)^2 + (Q_a^l)^2} \geq S_{\max}^l \tag{4}$$

$$\min(P_{Gk}, Q_{Gk}) \leq (P_a^i, Q_a^i) \leq \max(P_{Gk}, Q_{Gk}) \tag{5}$$

$$(P_a^i, Q_a^i, P_a^{ij}, Q_a^{ij}, I_a^{ij}) = f(V_a, \theta_a) \tag{6}$$

$$x_a^{\mathcal{O}_B} = x_{\text{ini}}^{\mathcal{O}_B} \tag{7}$$

式中：$\mathcal{O}_A$ 为攻击者可访问的攻击区域；下标 a 为受到攻击后对应的量测数据和状态变量；l 为目标攻击支路；$S_{\max}^l$ 为支路 l 上视在功率的最大值；上标 i、j 为系统的节点索引；Gk 为发电机节点索引；f 为基本电路定律；$\mathcal{O}_B$ 为攻击区域的边界节点集合；下标 ini 为变量初始值；x 为边界节点状态变量集合。式(4)为过载约束，其使攻击后目标支路上的传输功率突破允许上限，造成过载；式(5)约束节点攻击后的节点注入功率在发电机输出的允许范围内。式(6)对攻击后的量测数据加以约束，使之满足基本的电路定律；此外，攻击区域内的状态变化可能影响边界节点状态变化[33]，因此，式(7)对边界节点状态进行约束，区域外的状态变量不受攻击影响。

求解上述优化问题，攻击者便可得到使目标线路过载的最优攻击向量。攻击的有效性和通用性将在 2 节中验证。

2　ADE-FBLS

2.1　FBLS

BLS 在宽度方向上构造网络，具备快速的计算性能，但其简单的网络结构在处理复杂数据时表现不佳。为了增强 BLS 处理非线性问题的能力，FBLS 将 BLS 和 TS 模糊系统相结合，形成一个混合神经-模糊网络。其结构示意图如图 2 所示，图 2 左侧展开为模糊子系统具体结构。FBLS 保留 BLS 的基本结构，但用一组模糊子系统取代 BLS 的特征节点，模糊子系统能够在训练阶段捕获更多的数据特征和模式，使算法能够更好地适应未知数据，减少过拟合的风险。

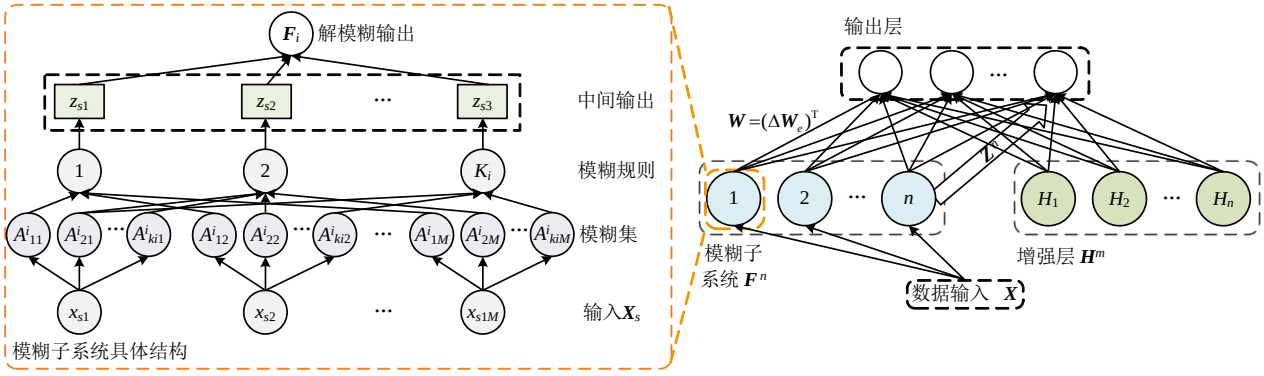


图 2　FBLS 的结构示意图

Fig. 2　Schematic diagram of the structure of the FBLS

设 FBLS 系统由 n 个模糊子系统和 m 组增强节点组成，第 i 个模糊子系统有 K_i 条模糊规则，第 j 组增强节点有 L_j 个节点。给定数据集 $\boldsymbol{X}=(x_1,\cdots,x_N)\in\mathbb{R}^{N\times M}$，样本特征 $\boldsymbol{x}_s=(x_{s1},x_{s2},\cdots,x_{sM})$，$s=1,2,\cdots,N$，输出数据为 $\boldsymbol{Y}=(y_1,\cdots,y_N)\in\mathbb{R}^{N\times C}$。式中：$N$ 为样本数；M 为输入数据的维数；C 为输出数据的维数。在第 i 个模糊子系统中，若 x_{s1} 与 A_{k1}^i 一一对应，则 $z_{sk}^i = f_k^i(x_{s1},x_{s2},\cdots,x_{sM}) = \sum_{t=1}^{M}\alpha_{kt}^i x_{st}$，$k=1,2,\ldots,K_i$，$i$ 为随机系数，模糊子系统的隶属函数为高斯函数 $\mu_{kt}^i=\exp[-(x-c_{kt}^i/\sigma_{kt}^i)^2]$，式中：$c_{kt}^i$ 为中心；σ_{kt}^i 为宽度。各模糊规则的加权输出为 $\omega_{sk}^i = \tau_{sk}^i/\sum_{k=1}^{k_i}\tau_{sk}^i$。其中 $\tau_{sk}^i=\prod_{t=1}^{M}\mu_{kt}^i(x_{st})$。

FBLS 算法的具体步骤如下。

步骤 1：在均匀分布[0,1]的范围内初始化函数 f_k^i 的系数 α_{kt}^i。

步骤 2：对于第 i 个模糊子系统，使用 K-means 方法对输入数据 $\boldsymbol{X}$ 进行聚类，得到 K_i 个聚类中心；通过聚类中心初始化高斯隶属函数的中心 c_{kt}^i，并设置隶属函数的宽度 $\sigma_{kt}^i=1$；通过式(8)计算第 s 个输入样本的中间输出 $\boldsymbol{Z}_{si}$ 和去模糊化输出 $\boldsymbol{F}_{si}$：

$$\begin{cases} \boldsymbol{Z}_{si}=(\omega_{s1}^i z_{s1}^i, \omega_{s2}^i z_{s2}^i, \cdots, \omega_{sK_i}^i z_{sK_i}^i) \\ \boldsymbol{F}_{si}=[\sum_{k=1}^{K_i}\omega_{sk}^i(\sum_{t=1}^{M}\delta_{k1}^i\alpha_{kt}^i x_{st}),\cdots,\sum_{k=1}^{K_i}\omega_{sk}^i(\sum_{t=1}^{M}\delta_{kc}^i\alpha_{kt}^i \cdot \\ \quad x_{st})]=\sum_{t=1}^{M}\alpha_{kt}^i x_{st}(\omega_{s1}^i,\cdots,\omega_{sK_i}^i)\begin{bmatrix}\delta_{11}^i & \cdots & \delta_{1C}^i \\ \vdots & \ddots & \vdots \\ \delta_{K_{i1}}^i & \cdots & \delta_{K,C}^i\end{bmatrix} \end{cases} \tag{8}$$

式中 δ_{kc}^i 为引入参数，用以在后续步骤中使用伪逆

时减少权重的数量，从而降低计算复杂度。

随后计算所有输入样本的中间输出 $\boldsymbol{Z}_i$ 和解模糊输出 $\boldsymbol{F}_i$：

$$\begin{cases}\boldsymbol{Z}_i=(Z_{1i},Z_{2i},\cdots,Z_{Ni})^{\mathrm{T}}\in\mathbb{R}^{N\times K_i}\\ \boldsymbol{F}_i=(F_{1i},F_{2i},\cdots,F_{Ni})^{\mathrm{T}}\triangleq\boldsymbol{D}\boldsymbol{\Omega}^i\boldsymbol{\delta}^i\in\mathbb{R}^{N\times C}\end{cases}\tag{9}$$

式中 $\boldsymbol{D}=\mathrm{diag}\{\sum_{t=1}^{M}\alpha_{kt}^i x_{1t},\cdots,\sum_{t=1}^{M}\alpha_{kt}^i x_{Nt}\}$。

步骤 3：计算所有模糊子系统 $\boldsymbol{Z}^n$ 的中间输出。

$$\boldsymbol{Z}^n=(Z_1,Z_2,\cdots,Z_n)\in\mathbb{R}^{N\times(K_1+K_2+,\cdots,+K_n)}\tag{10}$$

步骤 4：计算第 j 组增强节点 $\boldsymbol{H}_j(j=1,2,\cdots,m)$的输出和增强层 $\boldsymbol{H}^m$ 的整体输出：

$$\begin{cases}\boldsymbol{H}_j=\xi_j(Z^nW_{h_j}+\beta_{h_j})\in\mathbb{R}^{N\times L_j}\\ \boldsymbol{H}^m=(H_1,H_2,\cdots,H_m)\in\mathbb{R}^{N\times(L_1+L_2+\cdots+L_m)}\end{cases}\tag{11}$$

步骤 5：计算所有模糊子系统 F^n 的解模糊输出：

$$\boldsymbol{F}^n=\sum_{i=1}^{n}F_i=\sum_{i=1}^{n}\boldsymbol{D}\boldsymbol{\Omega}^i\boldsymbol{\delta}^i\triangleq\boldsymbol{D}\boldsymbol{\Omega}\boldsymbol{\Delta}\in\mathbb{R}^{N\times\mathbb{C}}\tag{12}$$

式中，$\boldsymbol{\Omega}=(\boldsymbol{\Omega}^1,\cdots,\boldsymbol{\Omega}^n)\in\mathbb{R}^{N\times(K_1+K_2+\cdots+K_n)}$，$\boldsymbol{\Delta}=[(\boldsymbol{\delta}^1)^{\mathrm{T}},\cdots,(\boldsymbol{\delta}^n)^{\mathrm{T}}]^{\mathrm{T}}\in\mathbb{R}^{(K_1+K_2+\cdots+K_n)\times C}$。

步骤 6：最后利用伪逆计算由$\boldsymbol{\Delta}$和 W_e 组成的输出参数矩阵 $\boldsymbol{W}$：

$$\boldsymbol{W}=\begin{bmatrix}\boldsymbol{\Delta}\\ \boldsymbol{W}_e\end{bmatrix}=(\boldsymbol{D}\boldsymbol{\Omega},\boldsymbol{H}^m)^{+}\boldsymbol{Y}=\boldsymbol{A}^{+}\boldsymbol{Y}\tag{13}$$

式中：$\boldsymbol{W}_e\in\mathbb{R}^{(L_1+L_2+\cdots+L_m)\times C}$ 为增强层与输出层之间的连接权值；$\boldsymbol{A}^{+}=(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}$；$\boldsymbol{A}=(\boldsymbol{D}\boldsymbol{\Omega},\boldsymbol{H}^m)$。

2.2 ADE

差分进化算法[38]因其出色的并行计算性能而被广泛应用，具有算法逻辑简单、计算效率高、鲁棒性好等优点。主要由种群初始化、突变、交叉和选择 4 个步骤组成。首先，初始化种群，对种群进行突变操作后得到突变载体；然后，对突变载体和目标个体进行交叉操作，得到试验向量；最后，试验向量和目标个体通过在选择操作中比较各自的适应度值竞争进入下一轮迭代的机会。差分进化进行特征选择的步骤如下。

步骤 1：种群初始化，在量测数据构成的 D 维特征空间中随机初始化具有 N_{P} 个个体，每个个体由 D 维向量组成：

$$\boldsymbol{x}_i^j=x_{\min}^j+\mathrm{rand}[0,1](x_{\max}^j-x_{\min}^j)\tag{14}$$

式中：$i=1,2,\cdots,N_{\mathrm{P}}$；$j=1,2,\cdots,D$；rand(0,1)返回[0,1]内的随机值；$x_{\min}^j$ 和 $x_{\max}^j$ 分别表示第 j 维变量的上界和下界。

步骤 2：突变过程，在每次迭代过程中，随机从种群中抽取 3 个个体进行突变操作，突变种群 $\vec{v}_{i,g}=[v_{i,g}^1,\ldots,v_{i,g}^D]$ 由式(15)给出。

$$\boldsymbol{v}_{i,g}=\boldsymbol{x}_{t_1,g}+F(\boldsymbol{x}_{t_2,g}-\boldsymbol{x}_{t_3,g})\tag{15}$$

式中：$t_1,t_2,t_3\in[1,\cdots,N_P]$ 满足 $t_1\neq t_2\neq t_3\neq i$；$g$ 为种群迭代次数；F 为变异因子，数值为 0~1。

步骤 3：交叉过程，将亲代向量与突变向量进行交叉操作以生成试验个体，增加种群个体的多样性。

$$u_{i,g}^j=\begin{cases}v_{i,g}^j, & \mathrm{rand}[0,1]\le C_{\mathrm{R}}\ \text{或}\ j=j_{\mathrm{rand}}\\ x_{i,g}^j, & \text{其他}\end{cases}\tag{16}$$

式中：$u_{i,g}^j$ 为交叉后的种群；C_{R} 为交叉概率；j_{rand} 为[1,D]范围内的随机整数。

步骤 4：选择过程，将交叉产生的试验个体 $\boldsymbol{u}_{i,g}$ 与亲代个体 $\boldsymbol{x}_{i,g}$ 进行比较，根据适应度值竞争进入下一轮迭代的机会。

$$\boldsymbol{x}_{i,g+1}=\begin{cases}\boldsymbol{u}_{i,g}, & \boldsymbol{u}_{i,g}\text{优于}\ \boldsymbol{x}_{i,g}\\ \boldsymbol{x}_{i,g}, & \text{其他}\end{cases}\tag{17}$$

变异因子和交叉概率是差分进化算法中两个至关重要的控制参数，对差分进化算法的整体性能有重要影响。传统 DE 中，这两个参数通常选取固定值，这使算法可能会过早地聚焦于局部最优而忽略更好的全局解，或因过分探索而无法在合理时间内收敛到优质解，即导致搜索效率低下。为克服这些局限性，本文设计一种自适应策略动态调整变异因子和交叉概率。

在进化前期使 F 尽可能大，以便种群迅速逼近全局最优解，避免陷入局部最优。而到迭代的后期，种群聚集在全局最优解周围，此时调整 F 值尽可能小以提高搜索精度找到全局最优解。F 的自适应策略表达式为

$$F=F_{\max}-(F_{\max}-F_{\min})\times(g/G)^2\tag{18}$$

式中：下标 min 和 max 为 F 的最大值和最小值；G 为最大迭代次数。

C_{R} 控制进入选择操作的突变个体的数量。当 C_{R} 值较大时，后代种群从亲代继承的信息较少，种群更新主要依靠突变过程，既丰富了种群的多样性，又提高了全局搜索能力。如果 C_{R} 值较小，则迭代产生的子代的搜索将主要集中在亲代的周围，这将缩小优化范围，提高收敛速度，有利于局部优化。C_{R} 的自适应策略表达式如下：

$$C_{\mathrm{R}}=\begin{cases}C_{\mathrm{R}}+(C_{\mathrm{R\,min}}-C_{\mathrm{R\,max}})\dfrac{f_i-f_{\mathrm{mean}}}{f_{\mathrm{best}}-f_{\mathrm{mean}}}, f_i\geq f_{\mathrm{best}}\\ C_{\mathrm{R}}, f_i<f_{\mathrm{best}}\end{cases}\tag{19}$$

式中：f_i 为个体适应度值；f_{mean} 平均适应度值；b_{best} 为迭代过程中的最佳适应度值。

2.3　定位检测流程

检测 FDIA 是否存在被定义为单标签二分类问题，基于此，本文将定位检测 FDIA 视为多标签二分类问题。在仿真中，分类检测方法的输入为来自 SCADA 和 PMU 的量测数据，这些数据包括节点电压、节点有功、无功功率注入、支路有功、无功潮流以及部分支路电流向量。在生成 FDIA 数据集时，将输出标签与母线状态变量相对应，每个标签都被定义为二元值 0 和 1，分别代表正常状态和受攻击状态。因而，检测方法的输出则为节点系统对应状态变量是否遭受攻击的二元值。

所提定位检测方法的具体流程如图 3 所示。相关步骤介绍如下。

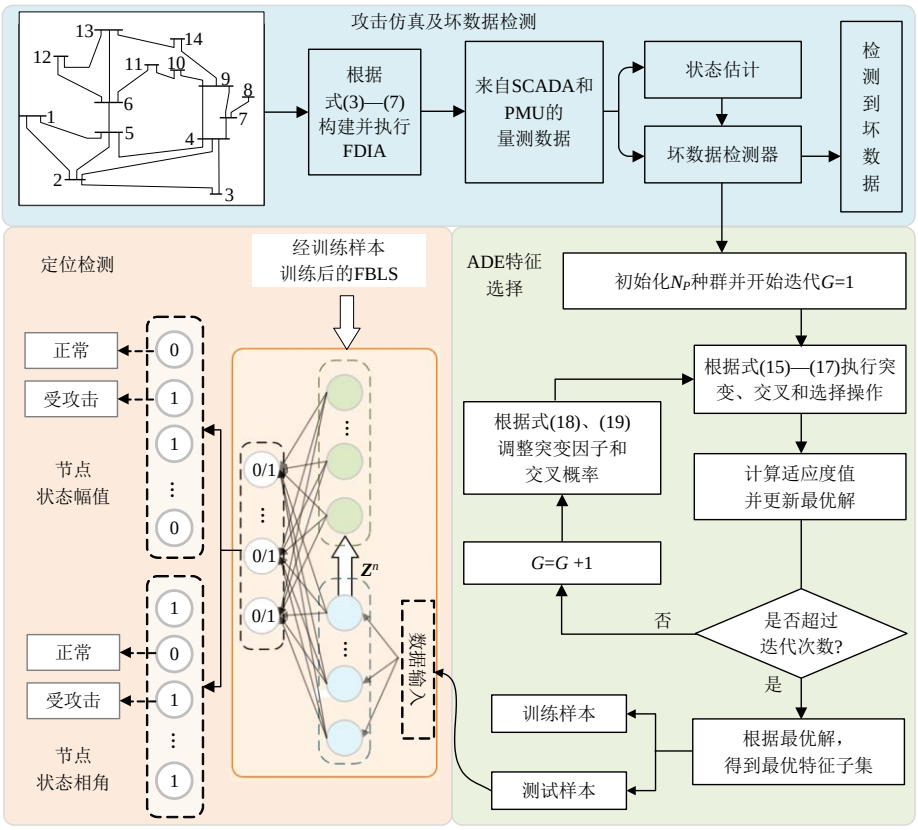


图 3　ADE-FBLS 定位检测流程图

Fig. 3　Flowchart of ADE-FBLS localization detection

步骤 1：攻击者获取电网相关信息，根据攻击模型执行式(3)—(7)对量测数据中注入攻击向量。

步骤 2：CPPS 对采集自 SCADA 和 PMU 的量测数据进行状态估计，初步检测并剔除坏数据。

步骤 3：将步骤 2 处理后的量测数据作为本文所提方法的输入，采用 ADE 对其进行特征选择，具体过程如图 3 所示。

步骤 4：特征选择后的特征子集输入到预训练的 FBLS 中来对正常和异常的分类边界进行学习，最后，输出对应二元值判断状态变量是否遭受 FDIA。

3　仿真分析

3.1　FDIA 仿真及分析

根据攻击者对 CPPS 配置信息(网络拓扑和线路参数等)的不同掌握程度，可以发动的攻击类型[37]总体可分为两类，即攻击者知晓电网完整的配置信息和攻击者无法获取电网全部的配置信息。前者考虑最为恶劣的情况，攻击者无须顾忌对某一区域的攻击是否会导致其他区域的级联反应，攻击造成的影响最为严重；后者考虑较为普遍的情况，由于电网的保护措施，攻击者无法获取电网全部的配置信息，仅能够通过技术手段掌握部分区域的配置信息。在这种情形下，攻击者发动攻击需要考虑边界约束，需要限制攻击导致的影响不会扩散到其他区域，从而到达隐匿的效果。为接近真实的 CPPS 运行场景，攻击仿真实验数据选取某地区调度中心的真实负荷数据。

本文在攻击及检测仿真中均考虑以上两种攻击场景。算例 1：在 IEEE-14 节点系统上，攻击者具有完整的电网配置信息；算例 2：在 IEEE-57 节点系统上，攻击者仅掌握部分配置信息。两个节点系统的拓扑结构示意图如图 4 所示。

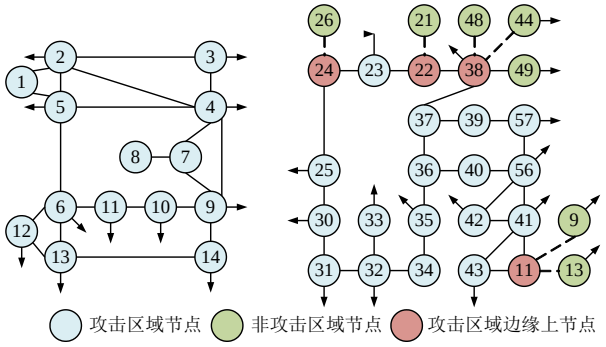


图 4 两个算例的拓扑结构示意图

Fig. 4 Schematic of the topology of the two examples

在 IEEE-14 节点系统下，设计攻击策略在 2-14 时使线路 6-13 过载。同样，在 IEEE-57 节点系统下在 2-14 时使线路 25-30 过载。算例 1 所选攻击线路为随机选择，算例 2 的攻击线路限制在掌握的信息范围内。所选时间段包含了日负荷的高峰、平均和低谷时段，具有代表性。两个算例攻击前后的残差如图 5 所示，两种情形下攻击后残差值均在 0.3 以下，低于 99.7%置信水平下的 BDD 检测阈值，成功地规避了 BDD 机制，验证了攻击具有隐蔽性和可行性。

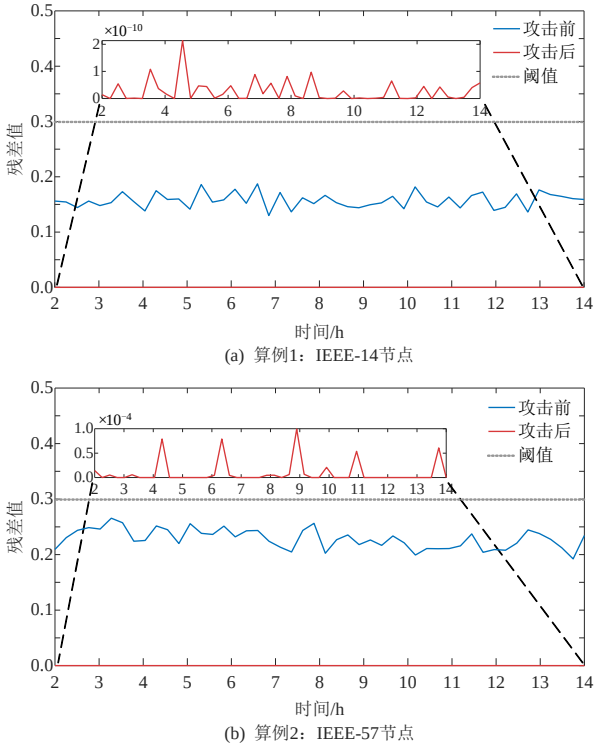


图 5 攻击前后残差

Fig. 5 Residuals before and after attack

未被 BDD 检测并剔除的量测数据会被控制中心用于错误的状态估计，进而得到错误的系统状态变量。若这些状态变量进一步被用于进行 CPPS 的监控、控制和优化操作，则最终会导致线路过载或其他级联故障，达到攻击者的攻击意图。图 6 展示了攻击前后两个系统的状态量的变化情况。由于攻击的目的是使目标线路过载，因而在状态变量的影响上具有一定随机性，但总体影响与目标线路保持相关。在算例 1 中，相角和幅值偏移量最大发生在目标攻击线路两端节点、13 节点及其相连节点，6 节点的状态变化较小。同样，在算例 2 中，影响最大的是 25 和 30 节点的状态变量，其中对 25 节点的相角影响较小。

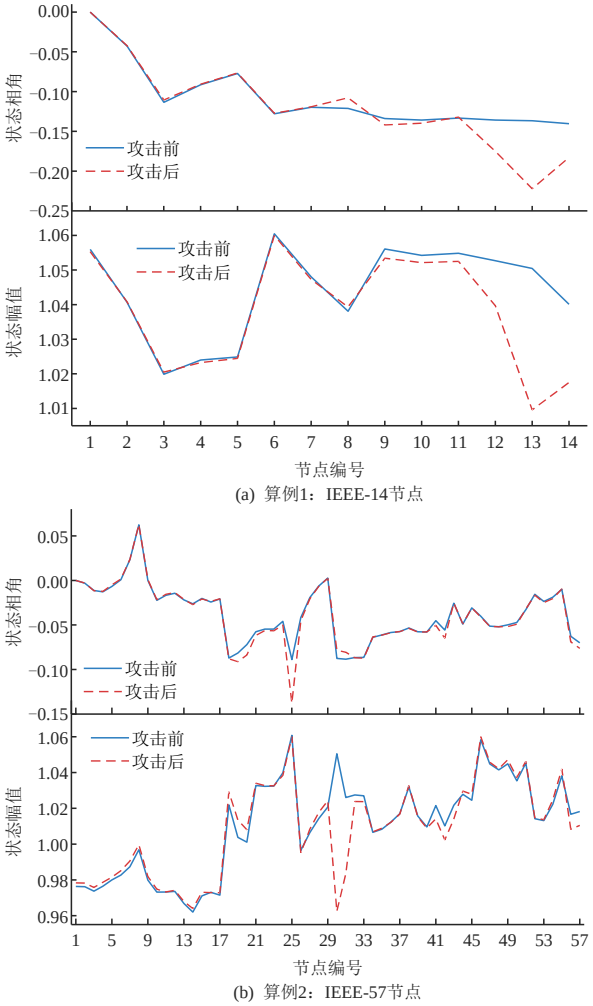


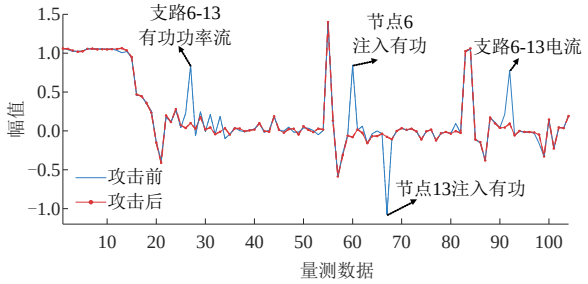
图 6 攻击前后的状态变化

Fig. 6 State change before and after the attack

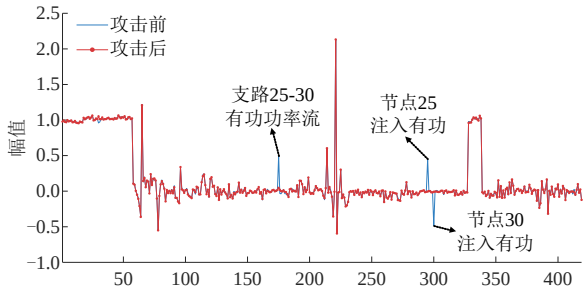
由图 5、6 可知，无论是攻击者知晓全局还是部分信息，都能够设计出精细的攻击向量，使攻击后的残差低于残差检验的阈值，且远低于攻击前的残差，绕开 BDD 机制并成功实施攻击。这表明即

便是配备了 PMU 装置的 CPPS 也难以通过传统的残差检验法来识别 FDIA。

图 7 展示了两个算例攻击前后量测数据的变化。由图 7 可知，受攻击影响最大的是目标攻击线路上的潮流和线路两端节点的注入功率量测，其次是与该节点直接相连的支路和节点相关量测，对没有直接连接的量测基本无影响。由两个算例可以发现，由于攻击者仅知道部分配置信息，因此，发动攻击考虑的约束较多，所以算例 2 中受影响较大的量测数据较少。图 7 还表明，攻击者只需要针对目标线路篡改少量的量测仪表，就能以较低的成本发起攻击。



(a) 算例1：IEEE-14节点



(b) 算例2：IEEE-57节点

图 7　攻击前后量测数据变化

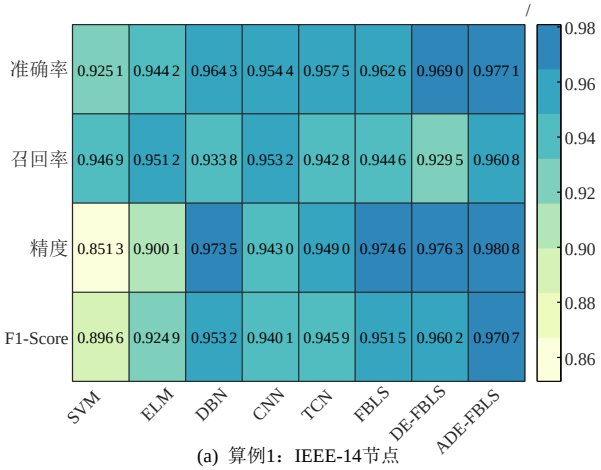
Fig. 7　Measurement data change before and after attack

3.2　定位检测仿真及分析

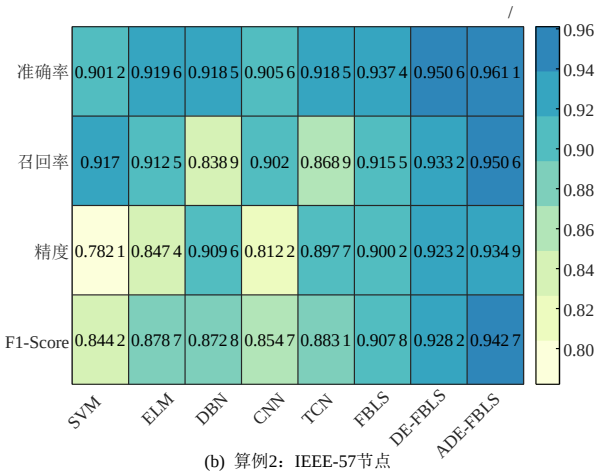
通过对上述算例下的攻击模型进行多次采样，获取用于 FDIA 定位检测的数据集合。其中，每条样本包含所有量测设备的数据特征和各节点电压幅值、相角的实时状态。在检测指标方面，本文从多标签二分类的角度实现对 FDIA 的定位检测，因此，可采用经典二元分类指标评估检测算法的性能。所选指标为准确率、精度、召回率、F1-Score 和受试者工作特征(receiver operating characteristic curve，ROC)曲线。

此外，通过将 ADE-FBLS 与 DE-FBLS、FBLS、时间卷积网络(temporal convolutional network，TCN)、CNN、深度置信网络(deep believe network，DBN)、极限学习机(extreme learning machine，ELM)和支持向量机(support vector machine，SVM)的检测结果进行对比分析，验证了 ADE-FBLS 在定位检测问题上存在显著优势。

ADE-FBLS 与其他算法在两种攻击算例下的定位检测指标对比结果如图 8 所示。在算例 1 中，IEEE-14 节点的网络结构简单，量测数据的特征维度不高，携带的冗余信息较少。因此，采用特征选择后的 ADE-FBLS 与未使用特征选择的 FBLS 性能表现差距较小，但仍有小幅度提升。从指标上看，前者在准确率、召回率和精度分别提升 1.45%、1.62%和 0.62%。F1-Score 表示精度和召回率的调和平均值，衡量算法的综合检测能力。所有算法中，ADE-FBLS 性能最佳，相较于 FBLS 提升 1.92%。此外，由于无法调整进化参数，DE 算法进行特征选择时无法收敛到最优解，这使 DE-FBLS 在召回率上的表现不如 FBLS。



(a) 算例1：IEEE-14节点



(b) 算例2：IEEE-57节点

图 8　两种算例下各算法的检测指标

Fig. 8　Detection index of each algorithm under two examples

在算例 2 中，IEEE-57 的量测数据呈现高维特征，相比于 14 节点系统的 104 维，57 节点系统有 419 维。因此，所有算法均受到影响，性能不如算

例 1 中的表现。但采用 ADE 进行特征选择，去除冗余特征后的 ADE-FBLS 与 FBLS 差距变得明显，召回率提升最大为 5.51%，综合指标 F1-Score 提升 3.49%。此外，相较于 DE-FBLS 可以看出，DE 处理高维特征数据是有效的，但仍然面临陷入局部最优解的困境。结合两种算例下的性能表现来看，合理的特征选择可以明显改善 FBLS 在高维特征时的表现。

各检测算法在两种算例下的训练和测试用时如表 1 所示。横向网络结构的 FBLS 的总体运行时间明显短于传统检测算法 SVM、ELM 和深度学习算法 DBN、CNN 和 TCN，具备更快的检测响应速度。DE-FBLS 和 ADE-FBLS 相比，前者不仅检测指标不如后者，且由于收敛速度较慢，前者的运行时间也较长，这表明 ADE 特征选择的效率优势更加明显，验证了所提自适应策略的有效性。此外，由于特征选择需要迭代逼近最优解，所以 ADE-FBLS 和 DE-FBLS 在总体运行用时上都长于 FBLS。结合图 8 的性能指标来看，耗费略多的时间实现更好的检测性能是值得的。

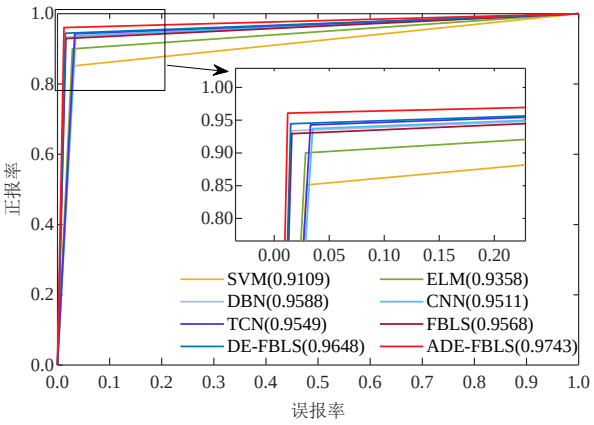
表 1 各检测方法的训练与测试用时

Table 1 Training and testing time of each testing method

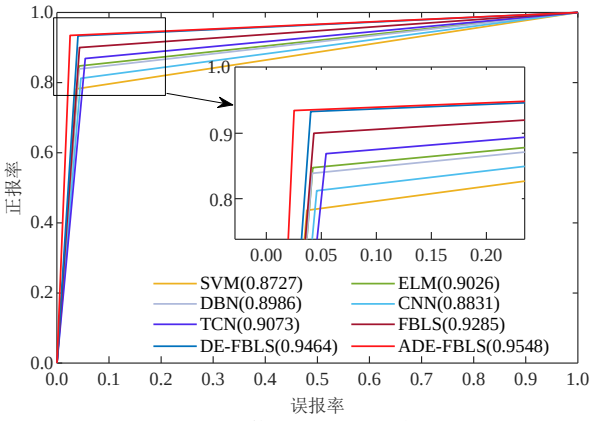
检测方法	算例 1：IEEE-14 节点		算例 2：IEEE-57 节点	
	训练用时/s	测试用时/s	训练用时/s	测试用时/s
ADE-FBLS	0.297 9	0.073 6	6.257 2	0.253 7
DE-FBLS	0.517 6	0.112 0	8.114 6	0.421 6
FBLS	0.138 6	0.036 6	2.517 2	0.106 7
TCN	74.055 4	0.203 1	474.012 8	1.931 5
CNN	49.978 4	0.331 7	200.256 7	0.527 8
DBN	0.511 3	0.051 2	0.757 2	0.073 6
ELM	2.606 7	0.009 3	21.720 1	0.024 5
SVM	9.662 7	0.007 3	14.121 1	0.010 6

各检测算法在两种算例下的 ROC 曲线如图 9 所示，ROC 曲线与坐标轴围成的面积记为曲线下面积(area under curve，AUC)，图例括号内为 AUC 值。ROC 曲线越趋近于左上角，AUC 值越大，算法的检测效果越好。如果检测算法性能优越，AUC 值会随着正报率的增加会越发逼近于 1。如果检测算法类似于随机猜测，则正报率将随误报率线性增加，AUC 值在 0.5 附近。两种算例中，本文所提方法最接近左上角，AUC 值最大，优于其他算法，这意味着所提算法能够在低误报率的代价下实现高精度识别，进一步验证了其泛化能力和综合检测性能。

为更好体现出对 FDIA 注入节点的定位检测，



(a) 算例1：IEEE-14节点



(b) 算例2：IEEE-57节点

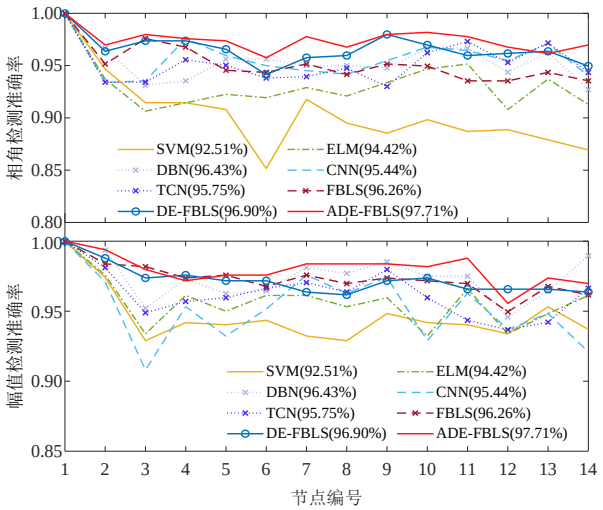
图 9 各检测算法的 ROC 曲线

Fig. 9 ROC curves of each detection algorithm

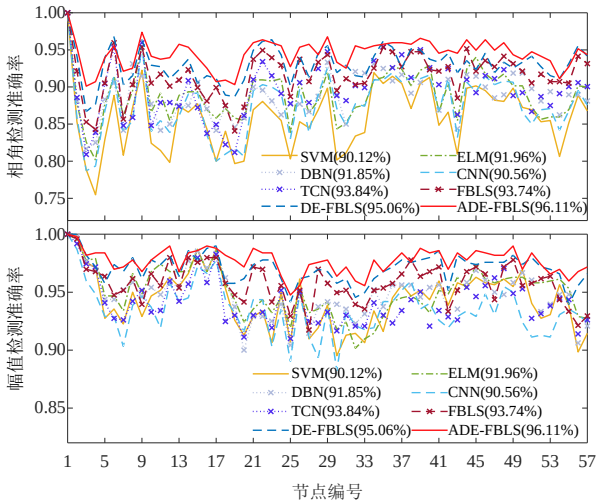
本文对各个算法在每个节点上的检测准确率展示在图 10 中。图 10 中上侧为节点相角检测准确率，下侧为幅值检测准确率，图例括号内为整体检测的平均准确率。

算例 1 中，FBLS 相比于经典的检测算法 SVM 和 ELM 在检测准确率上具有一定优势，在各个节点上幅值和相角检测准确率均占优，且趋势相对平稳。而与深度学习算法 CNN 相比，FBLS 优势较小，且在一些节点的准确率上不如前者。采用特征选择改进后的 DE-FBLS 未收敛到最优解，因此，在 FBLS 的基础上提升并不多，仅为 0.64%。具有自适应策略的 ADE-FBLS 在整体准确率上最优，相较于 FBLS 提升 1.45%，较前 5 个算法分别高出 5.20%、3.29%、1.28%、2.27%和 1.96%，且大部分的节点检测准确率保持领先。这表明所提方法在小节点系统上，具有更稳定、可靠的检测效果。

在算例 2 中，57 节点系统的量测数据维度较高，其数据间的耦合呈现出复杂的非线性。对于复杂的高维数据，浅层网络 SVM 和 ELM 不具备复杂的非线性表达能力，而 CNN 会面临过拟合的困境。因



(a) 算例1：IEEE-14节点



(b) 算例2：IEEE-57节点

图 10　节点定位检测准确率

Fig. 10　Node location detection accuracy

此，整体准确率都有所下降并且在各个节点上的幅值和相角准确率波动明显。FBLS 同样受到影响，但模糊系统的融入提高了其处理非线性问题的能力，因此，与传统检测算法相比，FBLS 在各状态变量上的检测准确率仍然比较平稳。与算例 1 相比，经特征筛选后的 ADE-FBLS 定位检测准确率下降幅度最小，在总体上仍保持最优的检测性能。

需要注意的是，无论是 IEEE-14 节点系统还是 IEEE-57 节点系统，节点 1 均被设置为参考节点，因此，所有算法在节点 1 上的检测准确率均为 100%。综上，在应用时可以综合考虑实际工程需要，选择具有更高检测精度 ADE-FBLS 或更快响应速度的 FBLS 检测 CPPS 中的 FDIA。

为验证本文所提算法在大规模测试系统中的适用性和有效性，选择 IEEE-118 节点系统作为测试平台，对攻击者在掌握系统局部信息情况下的 FDIA 的定位检测进行了仿真实验。考虑到篇幅限制，此部分的实验结果和及其分析见附录 A。

4　结论

CPPS 的网络安全对 EI 至关重要，针对 CPPS 中对 FDIA 检测这一难题，传统的检测算法忽视了攻击注入位置的定位检测。而已有的定位检测算法大都需要较长的训练时间，无法很好地在检测精度和耗费时间上取得平衡。因此，本文将 CPPS 中的 FDIA 定位检测视作多标签二分类问题，针对上述问题提出基于 ADE-FBLS 算法的 FDIA 定位检测方法。

所提方法的基本检测器 FBLS 具备快速检测的响应能力，但检测准确率受到高维数据的影响，面对高维复杂数据时，其泛化性和检测精确性差。针对这一问题，本文引入特征选择方法 ADE 处理 FBLS 数据传递中的冗余信息和不相关特征，在面对高维数据时，定位检测精度得到显著提高。本文在 IEEE-14 和 57 节点系统上构建了不同的攻击情形，并进行大量仿真实验，分析并验证了所采用攻击模型的有效性。以攻击算例为基础，对所提检测算法进行大量定位检测实验，验证了所提检测方法的有效性。且在与 SVM、ELM、DBN、CNN、TCN、FBLS 和 DE-FBLS 7 种算法的对比中，ADE-FBLS 在准确率、精度和召回率等方面展现出更佳的定位检测性能。此外，所提方法属于基于数据驱动的检测方法，不依赖于 CPPS 的网络模型，能够从量测样本中自动分析特征从而检测出异常数据，具有较强的可扩展性。

所提算法在 FDIA 问题的检测精度和响应速度间取得了较好的平衡，但当系统场景发生变化时，算法需要进行短暂的离线训练，而无法实时更新参数，这是下一步工作需要解决的问题。

参考文献

[1] 李卓，谢耀滨，吴茜琼，等. 基于深度学习的电力系统虚假数据注入攻击检测综述[J]. 电力系统保护与控制，2024，52(19)：175-187.
LI Zhuo，XIE Yaobin，WU Qianqiong，et al. Review of deep learning-based false data injection attack detection in power systems[J]. Power System Protection and Control，2024，52(19)：175-187(in Chinese).

[2] 席磊，董璐，程琛，等. 基于混合黑猩猩优化极限学习机的电力信息物理系统虚假数据注入攻击定位检测[J]. 电力系统保护与控制，2024，52(14)：46-58.

XI Lei，DONG Lu，CHENG Chen，et al．TLocation detection of a false data injection attack in a cyber-physical power system based on a hybrid chimp optimized extreme learning machine[J]．Power System Protection and Control，2024，52(14)：46-58(in Chinese)．

[3] 樊强，刘东，王宇飞，等．电力信息物理系统形态演进关键技术及其进展[J]．中国电机工程学报，2024，44(21)：8341-8352．
FAN Qiang，LIU Dong，WANG Yufei，et al．Key technologies and trends of cyber physical power system morphology evolution[J]．Proceedings of the CSEE，2024，44(21)：8341-8352(in Chinese)．

[4] 王伟胜，李光辉，何国庆，等．面向新型电力系统的新能源并网控制挑战与展望[J]．新型电力系统，2023，1(2)：145-160．
WANG Weisheng，LI Guanghui，HE Guoqing，et al．Challenges and prospects of grid connection control of renewable energy for new power systems[J]．New Type Power Systems，2023，1(2)：145-160(in Chinese)．

[5] 辛保安，李明节，贺静波，等．新型电力系统安全防御体系探究[J]．中国电机工程学报，2023，43(15)：5723-5731．
XIN Baoan，LI Mingjie，HE Jingbo，et al．Research on security defense system of new power system[J]．Proceedings of the CSEE，2023，43(15)：5723-5731(in Chinese)．

[6] 席磊，白芳岩，王文卓，等．基于海马优化深层极限学习机的电力信息物理系统 FDIA 检测[J]．电力系统保护与控制，2025，53(4)：14-26．
XI Lei，BAI Fangyan，WANG Wenzhuo，et al．Cyber-physical power system FDIA detection based on seahorse optimized deep extreme learning machine[J]．Power System Protection and Control，2025，53(4)：14-26(in Chinese)．

[7] 刘增稷，王琦，薛彤，等．电力系统中数据驱动算法安全威胁分析及应对方法研究[J]．中国电机工程学报，2023，43(12)：4538-4553．
LIU Zengji，WANG Qi，XUE Tong，et al．Research on security risks and defense methods of data-driven algorithms in power systems[J]．Proceedings of the CSEE，2023，43(12)：4538-4553(in Chinese)．

[8] 陈清清，苏盛，畅广辉，等．电力信息物理系统内部威胁研究综述[J]．南方电网技术，2022，16(6)：1-13．
CHEN Qingqing，SU Sheng，CHANG Guanghui，et al．Review on the research of insider threat of cyber physical power system[J]．Southern Power System Technology，2022，16(6)：1-13(in Chinese)．

[9] 杨玉泽，刘文霞，刘耕铭，等．不完全信息下计及残差污染的虚假数据注入攻击研究[J]．中国电机工程学报，2025，45(19)：7481-7492．
YANG Yuze，LIU Wenxia，LIU Gengming．Research on false data injection attack with incomplete information and residual pollution[J]．Proceedings of the CSEE，2025，45(19)：7481-7492(in Chinese)．

[10] 张程彬，崔明建，张梓枭，等．考虑攻击偏好的三相不平衡配电系统分布式 FDIA 检测[J]．电力系统保护与控制，2024，52(24)：109-119．
ZHANG Chengbin，CUI Mingjian，ZHANG Zixiao，et al．Distributed FDIA detection for three-phase unbalanced distribution systems considering attack preferences[J]．Power System Protection and Control，2024，52(24)：109-119(in Chinese)．

[11] LIU Ting，SUN Yanan，LIU Yang，et al．Abnormal traffic-indexed state estimation：a cyber－physical fusion approach for Smart Grid attack detection[J]．Future Generation Computer Systems，2015，49：94-103．

[12] 杨玉泽，刘文霞，李承泽，等．面向电力 SCADA 系统的 FDIA 检测方法综述[J]．中国电机工程学报，2023，43(22)：8602-8621．
YANG Yuze，LIU Wenxia，LI Chengze，et al．Review of FDIA detection methods for electric power SCADA system[J]．Proceedings of the CSEE，2023，43(22)：8602-8621(in Chinese)．

[13] CHEN Biyun，LI Hongbin，ZHOU Bin．Real-time identification of false data injection attacks：a novel dynamic-static parallel state estimation based mechanism [J]．IEEE Access，2019，7：95812-95824．

[14] 郭方洪，郑祥康，邓超，等．直流微电网无界虚假数据注入网络攻击检测与系统恢复方法[J]．电力系统自动化，2023，47(2)：146-153．
GUO Fanghong，ZHENG Xiangkang，DENG Chao，et al．Detection and system recovery method against unbounded false data injection network attack on dc microgrid[J]．Automation of Electric Power Systems，2023，47(2)：146-153(in Chinese)．

[15] ZHOU Tailin，XIAHOU Kaishun，ZHANG Li，et al．Real-time detection of cyber-physical false data injection attacks on power systems[J]．IEEE Transactions on Industrial Informatics，2021，17(10)：6810-6819．

[16] 陈碧云，李弘斌，李滨．伪量测建模与 AUKF 在配电网虚假数据注入攻击辨识中的应用[J]．电网技术，2019，43(9)：3226-3234．
CHEN Biyun，LI Hongbin，LI Bin．Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network[J]．Power System Technology，2019，43(9)：3226-3234(in Chinese)．

[17] CHEN Bairen，WU Q H，LI Mengshi，et al．Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks[J]．Protection and Control of Modern Power Systems，2023，8(2)：1-12．

[18] 郭方洪，易新伟，徐博文，等. 基于深度信念网络和迁移学习的隐匿 FDI 攻击入侵检测[J]. 控制与决策，2022，37(4)：913-921.
GUO Fanghong，YI Xinwei，XU Bowen，et al. Stealthy FDI Attack detection based on deep belief network and transfer learning[J]. Control and Decision，2022，37(4)：913-921(in Chinese).

[19] 夏云舒，王勇，周林，等. 基于改进生成对抗网络的虚假数据注入攻击检测方法[J]. 电力建设，2022，43(3)：58-65.
XIA Yunshu，WANG Yong，ZHOU Lin，et al. False data injection attack detection method based on improved generative adversarial network[J]. Electric Power Construction，2022，43(3)：58-65(in Chinese).

[20] WU Ting，XUE Wenli，WANG Huaizhi，et al. Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system[J]. IEEE Transactions on Industrial Informatics，2021，17(3)：1892-1904.

[21] 苏向敬，邓超，栗风永，等. 基于 MGAT-TCN 模型的可解释电网虚假数据注入攻击检测方法[J]. 电力系统自动化，2024，48(2)：118-127.
SU Xiangjing，DENG Chao，LI Fengyong，et al. Interpretable detection method for false data injection attack on power grid based on multi-head graph attention network and time convolution network model[J]. Automation of Electric Power Systems，2024，48(2)：118-127(in Chinese).

[22] XUE Wenli，WU Ting. Active learning-based XGBoost for cyber physical system against generic ac false data injection attacks[J]. IEEE Access，2020，8：144575-144584.

[23] HEGAZY H I，ELDIEN A S T，TANTAWY M M，et al. Online location-based detection of false data injection attacks in smart grid using deep learning[C]//Proceedings of 2022 IEEE International Conference on Internet of Things and Intelligence Systems. BALI，Indonesia：IEEE，2022：153-159.

[24] WANG Shuoyao，BI Suzhi，ZHANG Y J A. Locational detection of the false data injection attack in a smart grid：a multilabel classification approach[J]. IEEE Internet of Things Journal，2020，7(9)：8218-8227.

[25] WANG Yufeng，ZHOU Yangming，MA Jianhua，et al. A locational false data injection attack detection method in smart grid based on adversarial variational autoencoders [J]. Applied Soft Computing，2024，151：111169.

[26] CHEN C L P，LIU Zhulin. Broad learning system：an effective and efficient incremental learning system without the need for deep architecture[J]. IEEE Transactions on Neural Networks and Learning Systems，2018，29(1)：10-24.

[27] FENG Shuang，CHEN C L P. Fuzzy broad learning system：a novel neuro-fuzzy model for regression and classification[J]. IEEE Transactions on Cybernetics，2020，50(2)：414-424.

[28] BUCHAIAH S，SHAKYA P. Bearing fault diagnosis and prognosis using data fusion based feature extraction and feature selection[J]. Measurement，2022，188：110506.

[29] NGUYEN B H，XUE Bing，ZHANG Mengjie. A survey on swarm intelligence approaches to feature selection in data mining[J]. Swarm and Evolutionary Computation，2020，54：100663.

[30] WANG Xubin，WANG Yunhe，WONG K C，et al. A self-adaptive weighted differential evolution approach for large-scale feature selection[J]. Knowledge-Based Systems，2022，235：107633.

[31] WANG Peng，XUE Bing，LIANG Jing，et al. Feature clustering-assisted feature selection with differential evolution[J]. Pattern Recognition，2023，140：109523.

[32] 梁志宏，严彬元，洪超，等. 基于状态空间分解的电力系统虚假数据注入攻击检测与防御方法[J]. 南方电网技术，2025，19(06)：39-50.
LIANG Zhihong，YAN Binyuan，HONG Chao，et al. Detection and Defense Methods for False Data Injection Attack in Power Systems Based on State-Space Decomposition[J]. Southern Power System Technology，2025，19(06)：39-50(in Chinese).

[33] 郭剑波，王铁柱，罗魁，等. 新型电力系统面临的挑战及应对思考[J]. 新型电力系统，2023，1(1)：32-43.
GUO Jianbo，WANG Tiezhu，LUO Kui，et al. Development of new power systems：challenges and solutions[J]. New Type Power Systems，2023，1(1)：32-43(in Chinese).

[34] 席磊，田习龙，余涛，等. 基于相关特征-多标签级联提升森林的电网虚假数据注入攻击定位检测[J]. 南方电网技术，2024，18(5)：39-50+61.
XI Lei，TIAN Xilong，YU Tao，et al. Locational Detection of False Data Injection Attack in Power Grid Based on Relevant Features Multi-Label Cascade Boosting Forest[J]. Southern Power System Technology，2024，18(5)：39-50+61(in Chinese).

[35] 韩智涵，翟桥柱，周玉洲，等. 适用于新型电力系统调度和规划的数学模型框架及碳排放指标分析[J]. 新型电力系统，2024，2(3)：297-311.
HAN Zhihan，ZHAI Qiaozhu，ZHOU Yuzhou，et al. Mathematical model for new type power system scheduling and planning and analysis of carbon emission indices[J]. New Type Power Systems，2024，2(3)：297-311(in Chinese).

[36] YANG Qiang，JIANG Le，HAO Weijie，et al. PMU

placement in electric transmission networks for reliable state estimation against false data injection attacks[J]. IEEE Internet of Things Journal，2017，4(6)：1978-1986.

[37] LIU Xuan，LI Zuyi. False data attacks against AC state estimation with incomplete network information[J]. IEEE Transactions on Smart Grid，2017，8(5)：2239-2248.

[38] STORN R，PRICE K. Differential evolution-a simple and efficient heuristic for global optimization over continuous spaces[J]. Journal of Global Optimization，1997，11(4)：341-359.

附录 A IEEE-118 节点系统实验结果及分析

各算法在 IEEE-118 测试系统上的定位检测结果如附图 A1—A3 所示。当仅掌握局部系统信息时，攻击者对已知区域内发起 FDIA 致使某条线路过载，从而使系统状态变量发生偏移。而相比于前两个算例，大规模测试系统的维度更加庞大，量测数据维度达 736 维。因而，在针对某一线路发起攻击时，需要篡改的量测数据占比总量较少，表现出明显的稀疏性，这使受攻击样本与正常样本间存在不平衡。因此，此种情况下选取单一的准确率指标将有失偏颇。F1-Score 为召回率和精度的加权平均值，同时考虑了算法对 FDIA 的漏检和误检情况，F1-Score 越大，则综合检测性能越佳。从实验结果可以看出，本文所提算法在大规模测试系统中仍然具有最优的检测性能，且相比于 FBLS 和 DE-FBLS，其 F1-Score 分别提升 4.64%和 2.51%，验证了所提自适应差分进化技术在处理大规模数据集时的优势。

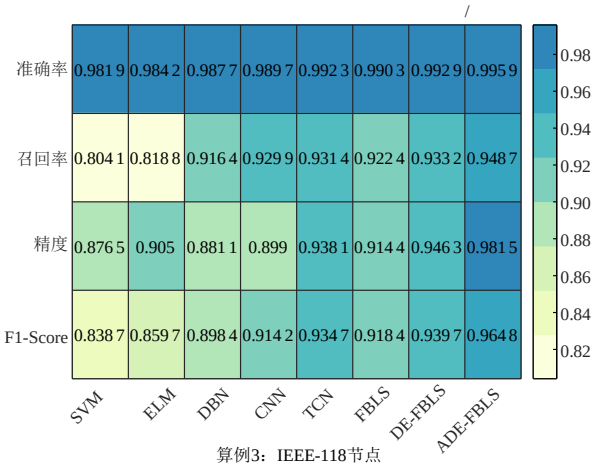


图 A1 算例 3 下各算法的检测指标

Fig. A1 Detection index of each algorithm under two examples

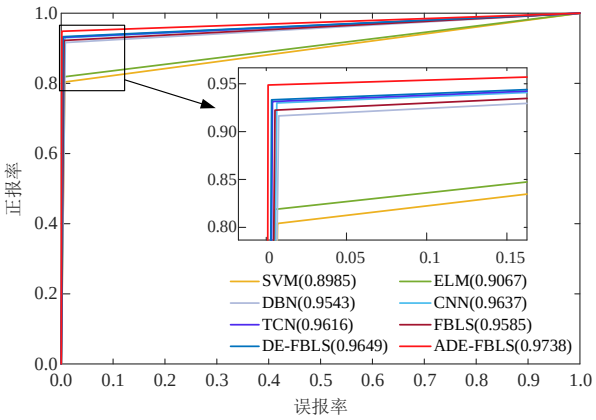


图 A2 各检测算法的 ROC 曲线

Fig. A2 ROC curves of each detection algorithm

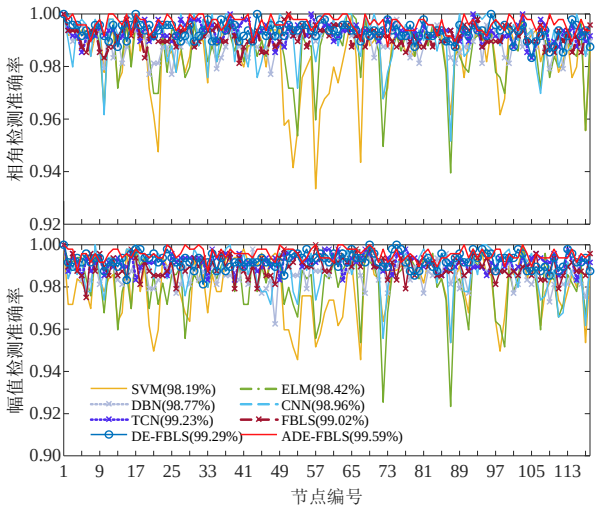


图 A3 节点定位检测准确率

Fig. A3 Node location detection accuracy

在线出版日期：2025-02-24。
收稿日期：2024-04-19。

席磊

作者简介：

席磊(1982)，男，博士，教授，博士生导师，从事电力系统运行与控制、自动发电控制、信息物理系统网络攻击与防御、智能控制方法研究，xilei2014@163.com。

(编辑 张文鑫，张蕾)