DOI: 10.19783/j.cnki.pspc.246133

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

席 磊[1,2]，白芳岩[1]，王文卓[1]，彭典名[1]，陈洪军[1]，李宗泽[1]

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

摘要： 虚假数据注入攻击(false data injection attack, FDIA)严重威胁电力信息物理系统的安全稳定。针对已有 FDIA 检测算法无法精确定位受攻击位置的局限性，提出了一种基于精英余弦变异融合的海马优化算法优化深层极限学习机(deep extreme learning machine, DELM)的 FDIA 检测定位算法。首先，该算法将极限学习机和极限学习机自编码器相结合得到了具备强特征表达能力的 DELM。然后，通过海马优化算法对 DELM 的偏置和输入权重进行择优，用于改善算法指标不稳定的问题。同时在捕食阶段引入精英余弦变异算法以提升海马的收敛速度与 DELM 的精度。最后，将系统量测数据作为输入特征，利用 DELM 得到节点状态标签，从而实现污染状态量的定位。通过在 IEEE 14 节点系统和 IEEE 57 节点系统进行大量仿真对比分析，验证了所提算法在准确率、精确率、召回率及 F_1 值等检测定位性能方面均具有明显优势，能够实现 FDIA 的精确定位。

关键词： 电力信息物理系统；虚假数据注入攻击；海马优化算法；深层极限学习机

Cyber-physical power system FDIA detection based on seahorse optimized deep extreme learning machine

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

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

Abstract: False data injection attack (FDIA) poses a serious threat to the security and stability of cyber-physical power systems. To address the limitations of the existing FDIA detection algorithms, ones that fail to precisely locate the attacked positions, an FDIA detection and localization algorithm based on elite cosine variation fusion of the seahorse optimization algorithm optimized deep extreme learning machine (DELM) is proposed. First, the algorithm combines the extreme learning machine and an auto-encoder to obtain the DELM with strong feature expression ability. Then, the bias and input weight of the DELM are optimized by the seahorse optimization, to improve the algorithmic index instability. Meanwhile, the elite cosine variation algorithm is introduced in the predation stage to further improve the convergence and accuracy of the DELM. Finally, system measurement data are used as input features to obtain the bus state labels using DELM, to realize the localization of the contaminated state variables. Through a large number of simulation comparative analyses in the IEEE 14-bus and 57-bus systems, it is verified that the proposed algorithm has obvious advantages in the detection and localization performance, such as accuracy, precision, recall, and F_1 score, and it can achieve the precise localization of an FDIA.

This work is supported by the National Natural Science Foundation of China (No. 52277108 and No. 52477104).

Key words: cyber-physical power system; false data injection attack; sea-horse optimization; deep extreme learning machine

0 引言

随着智能电网的加速发展，传统电力系统逐渐演变成与信息控制设备和通信传感网络深度融合[1-3]的电力信息物理系统(cyber-physical power system, CPPS)。近年来，针对 CPPS 的网络攻击愈发频繁，由于状态估计中的坏数据检测(bad data detection, BDD)[4]对于不良数据的辨识具有局限性，作为主流

基金项目： 国家自然科学基金项目资助(52277108，52477104)

网络攻击模式之一的虚假数据注入攻击(false data injection attack, FDIA)[5-7]可以篡改数据采集与监控系统(supervisory control and data acquisition, SCADA)[8]和相量测量单元(phasor measurement unit, PMU)[9]中的母线电压、节点功率注入及线路潮流等量测数据，使电力调度控制中心误判当前运行状态，严重威胁 CPPS 的安全稳定。

近年来，面向 FDIA 的检测从机理上主要分为基于数据驱动[10-14]和基于模型驱动[15-18]的检测算法。基于模型驱动的检测算法高度依赖电网模型，其精度和效率在很大程度上受电网建模准确性的影响。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，因此模型驱动不适用于复杂 CPPS。基于数据驱动的 FDIA 检测主要包括神经网络[10-11]、深度学习[12-13]和聚类算法[14]。该类方法具有强大的计算能力和较少的训练参数，且检测速度快，适用于复杂 CPPS。文献[10]采用离散小波变换和神经网络构建了攻击检测算法，从多时段状态估计结果中提取时-频特征，并利用神经网络对特征进行学习以判断电网是否受到攻击，通过仿真分析验证该算法有较高的检测准确率。文献[11]使用长短期记忆自编码器学习正常状态，再利用无监督学习评估每个样本的重建残差来检测自动发电控制系统中是否存在 FDIA。文献[12]采用将深度学习引入 network 中的 Deepwalk 算法，能够将攻击场景图中的节点映射为低维向量，进而区分攻击对电网造成危害的严重程度。文献[13]提出了一种分布式检测框架，利用边缘计算的优势构建轻量级检测器，并结合深度学习实现特征提取，在 IEEE 14 节点系统和 IEEE 39 节点系统中均有较好的检测效果。文献[14]通过聚类、过滤和线性插值生成攻击伪样本，设计基于过采样技术的量测数据平衡方法，并构建改进级联机器学习的检测算法，对于小样本数据仍有良好性能。上述方法虽然能够实现复杂 CPPS 的 FDIA 检测，但不能实现对 FDIA 的精确定位，以致后续难以恢复被篡改数据。

文献[19]引入了一种基于短时傅立叶变换的深度学习定位模型，首先使用 BDD 机制筛除低质量数据，再利用短时傅立叶变换将过滤后的量测数据从时域变换到时频域并输入到双通道卷积神经网络中，提取时频域特征进行训练和学习，以此定位 FDIA 的位置。文献[20]利用卷积神经网络(convolutional neural network, CNN)分析量测数据的不一致性，实现了对电网异常节点的定位检测。但由于深度学习算法的网络结构复杂，并且网络层间的耦合需要调整众多超参数，这不仅增大了算法对数据集的过度拟合风险，并且延长了训练时间，影响了算法的响应能力。

文献[21]提出了基于极限学习机(extreme learning machine, ELM)的 FDIA 检测算法，能够实现 FDIA 的定位，但 ELM 单隐层的结构，使其面对复杂的高维 CPPS 量测数据[22-24]进行数据挖掘时，对于潜在特征的表达存在困难，导致其对 FDIA 的定位精度不足。因此，本文试图采用特征表达能力更强的深层 ELM[25]，即将深层极限学习机(deep extreme learning machine, DELM)作为检测算法以提高 FDIA 的定位精度。然而，通过长期探索发现，DELM 的输入权重和偏置的随机性可能导致算法指标不稳定。

文献[26]提出了海马优化(sea-horse optimization, SHO)作为元启发式算法，适合求解函数优化问题，能够对 DELM 中的输入权重和偏置进行快速寻优，以解决 DELM 的输入权重和偏置的随机性导致算法指标不稳定的问题。然而，因 SHO 在处理高维数据时容易使海马个体陷入局部最优，导致适应度函数收敛精度低且收敛速度慢，从而影响 DELM 的定位精度。因此，本文将 SHO 与精英余弦变异(elite cosine variation, ECV)算法深度融合为精英海马优化(elite sea-horse optimization, ESHO)算法，即在 SHO 捕食阶段引入 ECV，增强了 SHO 在处理高维数据时海马向最优解进化的能力，以避免海马个体陷入局部最优，提高适应度函数的收敛精度和收敛速度，进而获得 DELM 输入权重和偏置的最优解。

故本文采用 ESHO 优化 DELM 中的输入权重和偏置，进而构建基于 ESHO-DELM 算法的 FDIA 检测定位算法，以解决对 FDIA 检测定位精度不足的缺陷。在不同攻击场景中进行对比实验，以验证所提算法用于 FDIA 检测定位的可行性，且相较于其他算法，所提算法具有更优越的检测定位性能。

1　FDIA

FDIA 以监测系统[27-29]采集的电气量测数据作为攻击对象，FDIA 原理如图 1 所示，其攻击向量的构建基础是状态估计方程[30-31]。CPPS 状态估计常用的交流潮流模型如式(1)所示。

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

式中：$\boldsymbol{z}$ 表示系统量测值，$\boldsymbol{z}=(z_1,z_2,\cdots,z_m)^{\mathrm{T}}$，$m$ 表示测量的数量；$\boldsymbol{x}$ 表示系统状态变量，$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)^{\mathrm{T}}$，$n$ 表示系统状态变量的数量；$\boldsymbol{e}$ 表示测量误差，$\boldsymbol{e}=(e_1,e_2,\cdots,e_m)^{\mathrm{T}}$，服从均值为 0 的高斯分布，且其中元素的标准差为 σ；$h(\cdot)$ 表示量

测值与状态变量之间的非线性关系。

当残差小于检测阈值时，表明未发现虚假数据，设检测阈值为 τ，此时系统的残差 r 如式(2)所示。

$$r=\left\|\boldsymbol{z}-h(\boldsymbol{x})\right\|_2\leqslant\tau \tag{2}$$

式中，$\left\|\bullet\right\|_2$ 表示 L2 范数。

攻击者构建攻击向量 $\boldsymbol{a}$ 并注入到 CPPS，攻击后系统的量测值 $\boldsymbol{z}^{\mathrm{A}}$ 如式(3)所示。

$$\boldsymbol{z}^{\mathrm{A}}=\boldsymbol{z}+\boldsymbol{a}=h(\boldsymbol{x}^{\mathrm{A}})+\boldsymbol{e} \tag{3}$$

式中，$\boldsymbol{x}^{\mathrm{A}}$ 表示攻击后的系统状态变量。此时攻击后的系统残差 r^{A} 如式(4)所示。

$$r^{\mathrm{A}}=\left\|\boldsymbol{z}^{\mathrm{A}}-h(\boldsymbol{x}^{\mathrm{A}})\right\|_2=\left\|\boldsymbol{z}-h(\boldsymbol{x})+\boldsymbol{a}-[h(\boldsymbol{x}^{\mathrm{A}})-h(\boldsymbol{x})]\right\|_2 \tag{4}$$

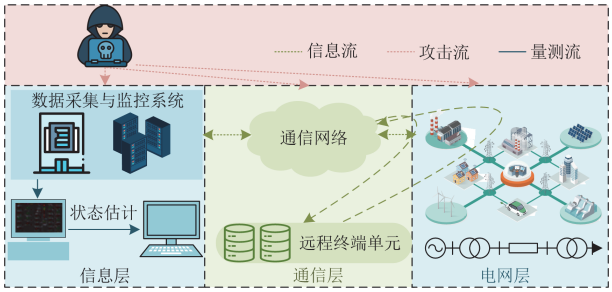


图 1 FDIA 原理

Fig. 1 Principle of FDIA

现有的 FDIA 大多是针对仅存在 SCADA 的近似直流模型，当 PMU 纳入交流状态估计时，这些攻击模型的准确度不理想，因此，文献[32]提出了一个普适性更高的非线性网络攻击模型，该模型可以同时处理 SCADA 和 PMU 的量测数据，本文采用该攻击模型来构建虚假数据，使线路过载进而实现 FDIA，其构建攻击的约束条件如式(5)所示。

$$\text{objective}:\min\left\|\boldsymbol{z}^{\mathrm{A}}-h(\boldsymbol{x}^{\mathrm{A}})\right\|_0 \tag{5}$$

式中，$\left\|\bullet\right\|_0$ 表示 L0 范数。通过式(5)求解 L0 范数来最小化攻击向量中非零元素的个数，以稀疏化攻击向量，提高攻击的隐蔽性。为使 FDIA 可行性更强，假设攻击者通过式(6)改变 SCADA 和 PMU 的量测值，使目标线路传输功率突破允许上限，从而达到攻击目的。

$$\sqrt{(P_l+\Delta P_l^{\mathrm{A}})^2+(Q_l+\Delta Q_l^{\mathrm{A}})^2}\geqslant S_l^{\max} \tag{6}$$

式中：P_l 和 Q_l 分别表示线路 l 的有功功率和无功功率；ΔP_l^{A} 和 ΔQ_l^{A} 分别表示由攻击引起的有功功率增量和无功功率增量；$S_l^{\max}$ 表示线路 l 的视在功率最大值。为使发电机的功率在机组输出的允许范围内，设置约束条件如式(7)所示。

$$\min(P_{\mathrm{G}q},Q_{\mathrm{G}q})\leqslant(P_q^{\mathrm{A}},Q_q^{\mathrm{A}})\leqslant\max(P_{\mathrm{G}q},Q_{\mathrm{G}q}) \tag{7}$$

式中：$\min(P_{\mathrm{G}q},Q_{\mathrm{G}q})$ 和 $\max(P_{\mathrm{G}q},Q_{\mathrm{G}q})$ 分别表示第 q 台发电机功率容量的下限和上限；P_q^{A} 和 Q_q^{A} 分别表示攻击后第 q 台发电机的有功功率和无功功率。线路过载后 SCADA 和 PMU 的量测数学模型如式(8)所示。

$$\begin{cases}(I_{ij}^{\mathrm{re}},I_{ij}^{\mathrm{im}})=f_{(V_i^{\mathrm{A}},\theta_i^{\mathrm{A}})}^{\mathrm{pmu}}\\(P_i^{\mathrm{A}},Q_i^{\mathrm{A}},P_{ij}^{\mathrm{A}},Q_{ij}^{\mathrm{A}})=f_{(V_i^{\mathrm{A}},\theta_i^{\mathrm{A}})}^{\mathrm{scada}}\end{cases} \tag{8}$$

式中：I_{ij}^{re} 和 I_{ij}^{im} 分别表示攻击后与节点 ij 相连线路的电流相量的实部和虚部；P_i^{A} 和 Q_i^{A} 分别表示攻击后节点 i 的有功注入功率和无功注入功率；P_{ij}^{A} 和 Q_{ij}^{A} 分别表示攻击后与节点 ij 相连线路的有功功率潮流和无功功率潮流；V_i^{A} 和 θ_i^{A} 分别表示攻击后节点 i 的电压幅值与相角；$f_{(\cdot)}^{\mathrm{pmu}}$ 和 $f_{(\cdot)}^{\mathrm{scada}}$ 分别表示 PMU 和 SCADA 的量测函数。此外，攻击区域内的状态变化会影响边界节点状态，为使其不受攻击影响，边界节点状态变量的约束如式(9)所示。

$$x_{\mathrm{bound}}=x_{\mathrm{bound}}^0 \tag{9}$$

式中，x_{bound}^0 和 x_{bound} 分别表示攻击前后的边界节点状态变量。

通过在 IEEE 14 节点系统和 IEEE 57 节点系统进行仿真测试，该攻击模型能够成功躲避 BDD 机制，验证了该攻击模型的可行性和隐蔽性。

2 ESHO-DELM 检测定位算法

本文提出了基于 ESHO-DELM 的 FDIA 检测定位算法，将 DELM 作为检测定位 FDIA 的分类器，并利用 ESHO 算法对 DELM 的偏置和输入权重进行优化，以提高算法的精度和稳定性，进而实现 FDIA 的精确定位，为调度控制中心提供精准的攻击位置，降低 FDIA 对电网的损害。

2.1 深层极限学习机(DELM)

ELM 属于单隐层神经网络，因其训练参数少、学习速度快、泛化能力强的优点[33-35]，已成功应用于不同领域。ELM 分为输入层、隐含层和输出层 3 个部分，对于一个包含有 N 个样本的训练集 $(\boldsymbol{x}_s,\boldsymbol{y}_s)$，$\boldsymbol{x}_s$ 表示输入特征，$\boldsymbol{y}_s$ 表示真实标签。$\boldsymbol{x}_s$ 通过输入层输入到网络内部，采用激活函数计算得到隐含层参数，再根据隐含层参数与输出权重计算得到输出标签 $\boldsymbol{o}_s$，并与 $\boldsymbol{y}_s$ 比较以判断结果是否正确。一个有 L 个隐含层神经元的单隐含层神经网络 $\boldsymbol{o}_s$ 如式(10)所示。

$$\boldsymbol{o}_s=\sum_{k=1}^{L}\boldsymbol{\beta}_k g(\boldsymbol{\omega}_k\cdot\boldsymbol{x}_s+b_k),s=1,\cdots,N \tag{10}$$

式中：$\boldsymbol{\beta}_k$ 表示第 k 个隐含层神经元与输出层间的输出权重；$g(\cdot)$ 表示激活函数；$\boldsymbol{\omega}_k$ 表示输入层和第 k 个隐含层神经元间的输入权重；b_k 表示第 k 个隐含层神经元的偏置。式(10)可简化为 $\boldsymbol{O}=\boldsymbol{H}\boldsymbol{\beta}$，其中，$\boldsymbol{H}$ 为隐含层神经元的输出矩阵；$\boldsymbol{\beta}$ 为输出权重；$\boldsymbol{O}$ 为期望输出。

根据最小二乘原理，通过式(11)得到输出权重。

$$\boldsymbol{\beta}=\boldsymbol{H}^{+}\boldsymbol{O} \tag{11}$$

式中，$\boldsymbol{H}^{+}$ 为矩阵 $\boldsymbol{H}$ 的 Moore-Penrose 广义逆矩阵。

由于 ELM 对于潜在特征的表达存在困难，且存在对 FDIA 定位精度不足的问题。因此，本文采用将 ELM 和 ELM 自编码器(ELM-auto encoder, ELM-AE)相结合的 DELM。图 2 为 DELM 结构图，设其层数为 g，DELM 通过对输入特征逐层学习，直至最后一层对前一层隐含层神经元的输出进行分类，从而实现 FDIA 的精准定位。

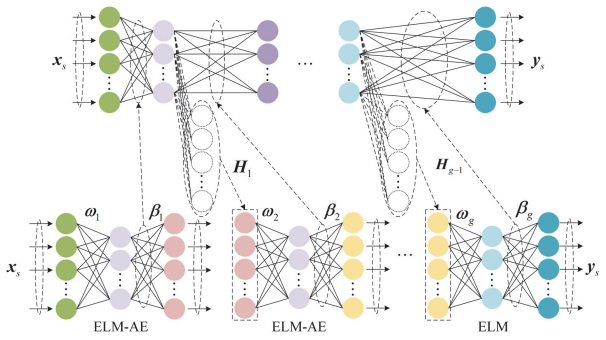


图 2 DELM 结构图

Fig. 2 DELM structure diagram

根据 ELM-AE 的特征表达能力，将它作为 DELM 的基本单元，能够学习到原始数据中更抽象和有用的特征，进而使 DELM 的训练速度更快，兼具深度学习算法自主特征提取和极限学习机训练速度快的优势，能够更好地学习高维 CPPS 量测数据，提高 FDIA 精确定位的能力。

2.2 精英海马优化(ESHO)算法

DELM 的输入权重和偏置的随机性可能导致 FDIA 定位精度不稳定，因此本文采用优化算法对输入权重和偏置寻优，以提高算法指标稳定性。

首先选取具有强寻优能力和高收敛精度[36]的粒子群优化(particle swarm optimization, PSO)、蝴蝶优化算法(butterfly optimization algorithm, BOA)、白鲨优化(white shark optimization, WSO)、灰狼优化(grey wolf optimization, GWO)以及 SHO 算法，设置迭代次数为 100，种群个数为 30，基于 F13 基准测试函数进行仿真，收敛曲线如图 3 所示。

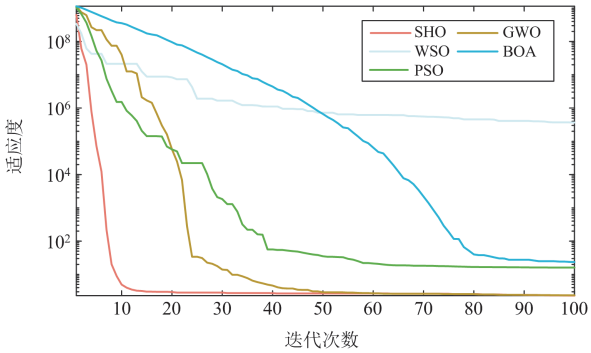


图 3 优化算法收敛曲线

Fig. 3 Convergence curves of optimization algorithms

由图 3 可知，基于 F13 测试函数的测试，SHO 的收敛精度和收敛速度明显优于 WSO、GWO、PSO 和 BOA，因此本文选用 SHO 寻求 DELM 输入权重和偏置的最优解。

2.2.1 海马优化(SHO)算法

SHO 作为一种基于群体智能的元启发式算法，其灵感来自自然界中海马的运动、捕食和繁殖行为。

海马运动阶段：为了权衡探索和开发的性能，取 r_1 为分界点，其大于 0 时用于局部开发，小于 0 时用于全局搜索。因此运动可以分为以下两种情况。

第一种情况：当正态随机值 r_1 位于分界点右侧时，它主要实现 SHO 的局部开发。海马 $\boldsymbol{H}_w$ 沿着螺旋运动向最佳个体 $\boldsymbol{H}_{\text{best}}$ 移动，并使用 Levy 分布来模拟海马的移动步长，这有利于在迭代早期以较大概率跨越至更优位置，避免了 SHO 的过度局部开发。此时海马的新位置如式(12)所示。

$$\boldsymbol{H}^{1}_{\text{new}}(t+1)=\boldsymbol{H}_w(t)+D(\lambda)((\boldsymbol{H}_{\text{best}}(t)-\boldsymbol{H}_w(t))\times a\times b\times c+\boldsymbol{H}_{\text{best}}(t)) \tag{12}$$

式中：$\boldsymbol{H}^{1}_{\text{new}}$ 表示海马运动阶段的新位置；t 为当前迭代次数；$D(\lambda)$ 表示服从参数 λ 的 Levy 分布，$0<\lambda<2$；a、b、c 表示螺旋运动下坐标的三维分量，推动更新搜索位置，$a=\rho\times\cos(\theta)$，$b=\rho\times\sin(\theta)$，$c=\rho\times\theta$，其中，ρ 表示由 μ 和 ν 定义的长度，$\rho=\mu\times e^{\theta\nu}$，$\mu$ 服从 $N(0,\sigma^2)$ 分布，θ 为随机值，范围为 $[0,2\pi]$，ν 服从 $R(0,1)$ 分布。

第二种情况：在漂移作用下，r_1 位于分界点左侧时，进行 SHO 探索。探索操作对于避免 SHO 的局部极值非常重要，在这种情况下，采用布朗运动模拟海马的另一个移动长度，以确保其在搜索空间中更好地探索，此时海马新位置如式(13)所示。

$$\boldsymbol{H}^{1}_{\text{new}}(t+1)=\boldsymbol{H}_w(t)+\eta\times d\times\psi\times(\boldsymbol{H}_w(t)-\psi\times\boldsymbol{H}_{\text{best}}(t)) \tag{13}$$

式中：η 表示[0,1]之间的随机数；d 表示常数系数；ψ 表示服从标准正态分布的期望值。

综上所述，这两种情况可以得到海马在运动阶段第 $t+1$ 次迭代时的新位置。

捕食行为：海马在捕食前期根据运动阶段进行位置调整，调整后的海马位置 $\boldsymbol{H}_{\text{new}}^{1.5}$ 如式(14)所示。

$$\boldsymbol{H}_{\text{new}}^{1.5}(t)=\boldsymbol{H}_{\text{new}}^{1}(t)\times(\urcorner(T_{\text{u}}+T_{\text{l}}))+b_{\text{u}}\times T_{\text{u}}+b_{\text{l}}\times T_{\text{l}} \tag{14}$$

式中：$\urcorner$ 为逻辑判断符；T_{u} 和 T_{l} 分别为当前海马相对于上界和下界的位置；b_{u} 和 b_{l} 分别表示上界和下界。

设计临界值 r_2 以区分海马是否捕食成功。由于最佳位置在一定程度上表示猎物的大致位置，因此成功捕食强调了 SHO 的开发能力。若 $r_2>0.1$，则意味着海马的捕食是成功的，即海马比猎物移动得更快，最终将其捕获；否则，当捕食失败时，两者的响应速度与之前相反，这意味着海马倾向于探索搜索空间。海马捕食时的数学模型如式(15)所示。

$$\boldsymbol{H}_{\text{new}}^{2}(t+1)=\begin{cases}\alpha\times(\boldsymbol{H}_{\text{best}}(t)-\eta\times\boldsymbol{H}_{\text{new}}^{1.5}(t))+\\ \quad(1-\alpha)\times\boldsymbol{H}_{\text{best}}(t), & r_2>0.1\\ (1-\alpha)\times(\boldsymbol{H}_{\text{new}}^{1.5}(t)-\eta\times\boldsymbol{H}_{\text{best}}(t))+\\ \quad\alpha\times\boldsymbol{H}_{\text{new}}^{1.5}(t), & r_2\leqslant 0.1\end{cases} \tag{15}$$

式中：$\boldsymbol{H}_{\text{new}}^{2}$ 表示海马捕食阶段的新位置；α 表示海马捕食时的移动步长因子；r_2 表示[0,1]之间的随机数；移动步长因子 α 的表达如式(16)所示。

$$\alpha=(1-t/T)^{(2t/T)} \tag{16}$$

式中，T 表示最大迭代次数。

繁殖行为：根据适应度值，种群被分为父体和母体，以便下一代更好地继承父体和母体中的特征，并避免迭代的过度局部化。种群划分方法如式(17)所示。

$$\begin{cases}\boldsymbol{D}^{\text{M}}=\boldsymbol{H}_{\text{sort}}^{2}(1:E_{\text{pop}}/2)\\ \boldsymbol{D}^{\text{W}}=\boldsymbol{H}_{\text{sort}}^{2}((E_{\text{pop}}/2+1):E_{\text{pop}})\end{cases} \tag{17}$$

式中：$\boldsymbol{D}^{\text{M}}$ 和 $\boldsymbol{D}^{\text{W}}$ 分别表示被种群区分的父体和母体，两群体随机交配产生新的后代；$\boldsymbol{H}_{\text{sort}}^{2}$ 表示所有 $\boldsymbol{H}_{\text{new}}^{2}$ 按照适应度升序排列；E_{pop} 表示种群数量。后代 $\boldsymbol{H}_{p}^{\text{offspring}}$ 的表达式如式(18)所示。

$$\boldsymbol{H}_{p}^{\text{offspring}}=\eta\boldsymbol{H}_{p}^{\text{M}}+(1-\eta)\boldsymbol{H}_{p}^{\text{W}} \tag{18}$$

式中：p 为 $[1,E_{\text{pop}}/2]$ 内的正整数；$\boldsymbol{H}_{p}^{\text{M}}$ 和 $\boldsymbol{H}_{p}^{\text{W}}$ 分别表示从父体和母体群体中随机选择的个体。

SHO 能够缓解由分类器随机参数造成的 FDIA 仿真指标不稳定的问题，从而使 DELM 获得更强的泛化能力，以实现更准确的 FDIA 检测定位。

2.2.2 精英余弦变异(ECV)算法

尽管 SHO 在探索方面有较好的表现，但海马在靠近猎物时容易因探索范围不足无法得到最优解，以致算法陷入局部最优，从而导致适应度函数收敛精度低、收敛速度慢。所以在 SHO 捕食阶段，引入精英余弦变异算法，以加快算法向最优解进化，从而提高 SHO 的收敛精度和速度，使其快速准确地实现 DELM 输入权重和偏置的择优。将上述策略与海马位置调整方式相结合，可以得到

$$\boldsymbol{H}_{\text{new}}^{1.5}(t)=\begin{cases}\boldsymbol{H}_{\text{new}}^{1}(t)\times(\urcorner(T_{\text{u}}+T_{\text{l}}))+b_{\text{u}}\times T_{\text{u}}+b_{\text{l}}\times T_{\text{l}}, & \eta\geqslant\varepsilon\\ B\times\cos(\delta)\times\boldsymbol{H}_{\text{best}}(t), & \eta<\varepsilon\end{cases} \tag{19}$$

式中：B 表示 $\cos(\delta)$ 的振幅；δ 表示随机数，介于 $[0,2\pi]$ 之间；ε 表示余弦变异控制参数，设置为 0.2，$\eta<\varepsilon$ 时进行精英海马余弦变异，反之仍使用 SHO 原开发策略。振幅 B 的表达如式(20)所示。

$$B=\text{e}^{(-f\times(t/T))} \tag{20}$$

式中，f 表示形状控制系数，设置为 100。B 的值随迭代次数的增加非线性递减。

因此，通过在海马捕食阶段引入 ECV 得到 ESHO。在寻优算法中，适应度值的选取对评价指标的高低有较大影响，本文设置 ESHO 的适应度值为 DELM 对攻击数据训练集检测定位的错误率。通过海马移动、捕食和繁殖行为，不断迭代更新种群位置；并利用 ECV 中余弦函数的周期特性，使海马在当前最优位置邻域内高效进行精细化开发，以寻找最低的错误率；即证明 DELM 在当前输入权重和偏置下有最优的训练效果，并将此时 DELM 的输入权重和偏置作为最优解进行测试，进而实现对 FDIA 的精确定位。

2.3 ESHO-DELM 检测定位流程

本文利用 ESHO 的寻优特性，对 DELM 的输入权重和偏置进行迭代寻优。算法流程如图 4 所示，通过对 SHO 的最佳位置更新策略进行改进，提高了 SHO 的收敛精度和速度，进而达到优化 DELM 的输入权重和偏置的目的，提高了算法指标的稳定性和 FDIA 精确定位能力。

3 算例分析

3.1 攻击模型的构建

根据攻击者掌握的 CPPS 配置信息(网络拓扑和线路参数等)，构建两种不同场景下的攻击算例，即攻击者掌握 IEEE 14 节点系统全局网络信息和 IEEE 57 节点系统部分网络信息。图 5 为两个节点系统的

拓扑结构。对于 IEEE 14 节点系统，PMU 的部署节点为节点 4 和 6；对于 IEEE 57 节点系统，PMU 的部署节点为节点 4、10、15、20、24、29、32、37、41、48 和 54，各节点系统 SCADA 和 PMU 的量测数据分布如表 1 所示。

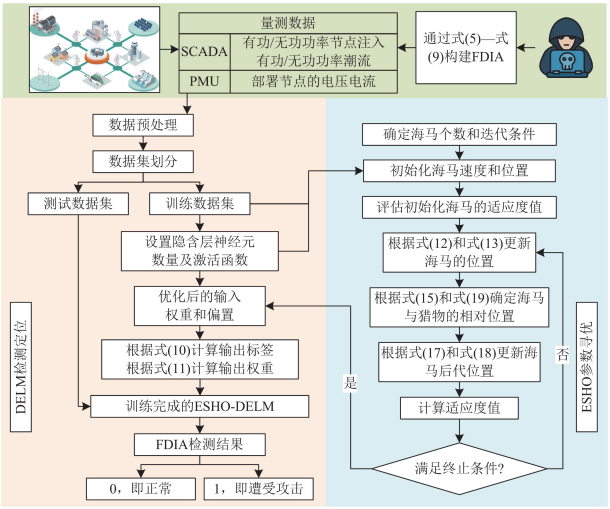
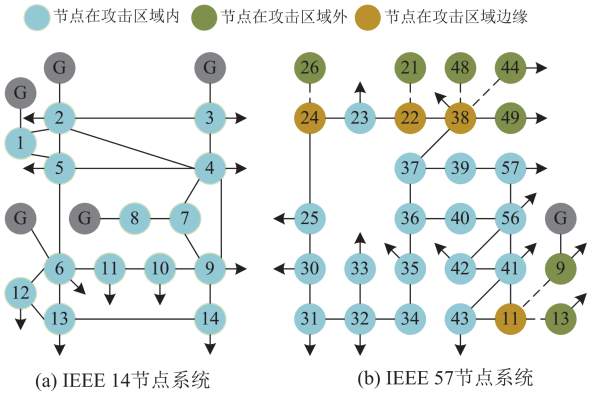


图 4　ESHO-DELM 流程图

Fig. 4 Flowchart of ESHO-DELM



(a) IEEE 14节点系统　(b) IEEE 57节点系统

图 5　系统拓扑

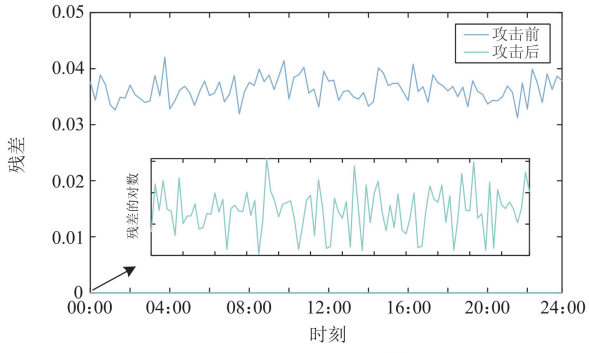
Fig. 5 System topology

表 1　各系统量测数据数量

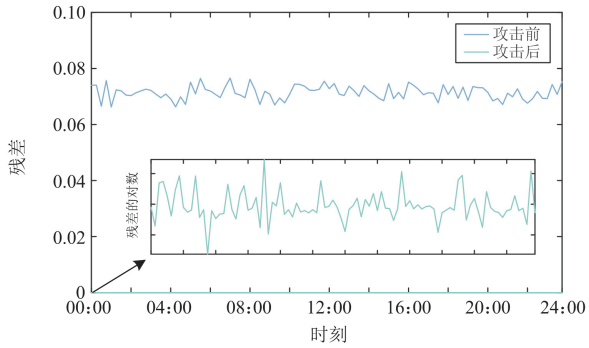
Table 1 Quantity of measurement data for each system

量测设备	IEEE 14 节点系统	IEEE 57 节点系统
SCADA	82	327
PMU	22	92

为验证所提攻击模型的通用性，对两个系统进行仿真测试。图 6 为攻击前后的最大归一化残差，结果显示，IEEE 14 节点系统和 IEEE 57 节点系统攻击后的残差远小于攻击前的残差，验证了所提攻击模型能够绕过电力系统的 BDD 机制，即攻击是隐蔽的。



(a) IEEE 14节点系统



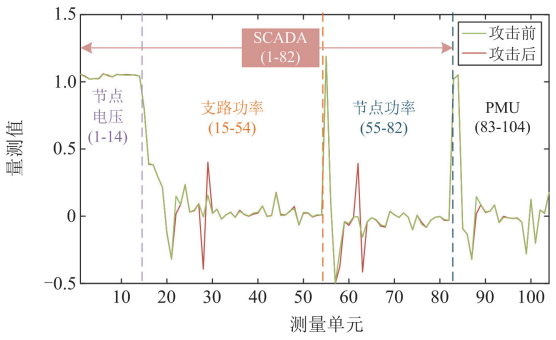
(b) IEEE 57节点系统

图 6　攻击前后的残差

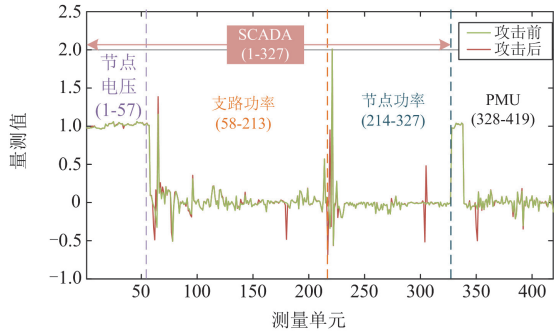
Fig. 6 Residuals before and after attack

图 7 为两节点系统攻击前后量测数据的对比，遭受攻击的节点及其所连线路的量测值在攻击前后有明显偏离，没有直接连接的节点量测攻击前后基本无变化，总体偏离较小。以此验证了攻击模型的可行性。

图 8 和图 9 分别为两节点系统攻击前后电压的相角和幅值，为便于对比攻击前后的电压相角和幅值，将数据归一化并简单转换。结果显示，受攻击线路的节点电压幅值和相角偏移较大，未被攻击线路的节点电压的相角与幅值基本无变化。综上，FDIA 仅会使目标线路相连节点状态变量发生显著改变，进一步验证了攻击模型的隐蔽性。



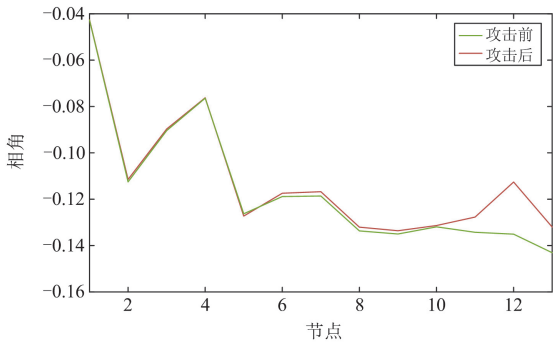
(a) IEEE 14节点系统



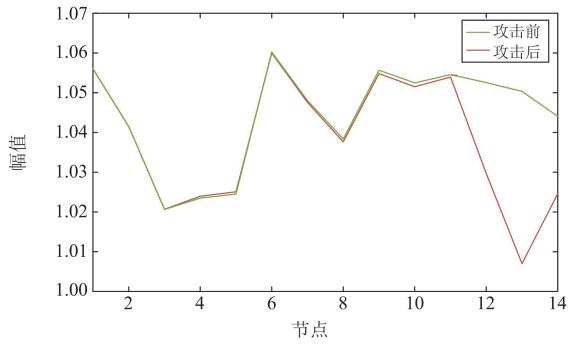
(b) IEEE 57节点系统

图 7 攻击前后的量测值

Fig. 7 Measurement data before and after attack



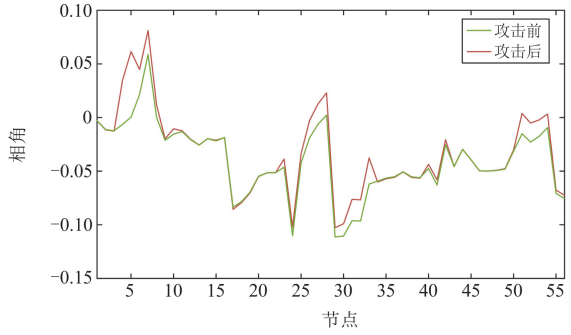
(a) IEEE 14节点系统相角



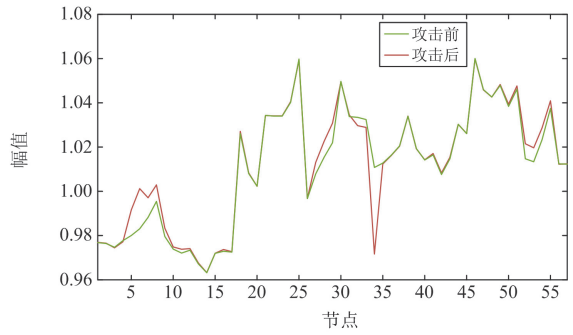
(b) IEEE 14节点系统幅值

图 8 IEEE 14 节点系统攻击前后的电压

Fig. 8 IEEE 14 bus system voltage before and after attack



(a) IEEE 57节点系统相角



(b) IEEE 57节点系统幅值

图 9 IEEE 57 节点系统攻击前后的电压

Fig. 9 IEEE 57 bus system voltage before and after attack

3.2 检测定位仿真分析

为验证 ESHO-DELM 在 CPPS 受到 FDIA 时具有优异的检测定位能力，采用攻击模型在 IEEE 14 节点系统和 IEEE 57 节点系统实施攻击后的攻击数据作为检测定位数据集，其中输入为 SCADA 和 PMU 采集的量测数据；输出为节点电压的相角与幅值状态。在 Matlab 中对所提算法和对比算法进行仿真测试，并选取 1860 组数据作为训练集，620 组数据作为测试集。通过式(10)和式(11)得到 DELM 的输出结果，基于 DELM 的输出标签判断 CPPS 中各节点是否遭受攻击，并确定被攻击的具体位置。以 IEEE 57 节点系统为例，随机选择 5 组测试数据分析。如图 10 所示，1 表示该节点遭受攻击，0 表示该节点状态正常。

样本	测试集电压相角						测试集电压幅值					
	P1	P2	P3	...	P56	P57	A1	A2	A3	...	A56	A57
N1	0	1	1	...	1	0	0	1	1	...	1	0
N2	0	0	1	...	0	1	0	0	1	...	1	1
N3	0	1	0	...	1	1	0	1	0	...	1	1
N4	0	0	0	...	0	0	0	0	0	...	0	0
N5	0	1	0	...	1	0	0	1	0	...	1	0

图 10 FDIA 检测定位原理

Fig. 10 Principle of FDIA detection and localization

其中前 57 列为电压相角状态，后 57 列为电压幅值状态，第 1 个节点为参考节点不受攻击。以样本 3 为例，P2、P56 和 P57 为 1，表明节点 2、56 和 57 的电压相角遭受攻击；A2、A56 和 A57 为 1，表明节点 2、56 和 57 的电压幅值遭受攻击；其余为 0 表明该位置状态正常。据此可以得出定位标签，并将此标签与测试集标签进行对比即可判断出定位结果是否准确。

3.2.1 评价指标

根据表 2 对算法输出结果进行定义，并采用以

下 5 个指标评价算法性能。

表 2 检测混淆矩阵

Table 2 Detection confusion matrix

节点标签	检测正例	检测负例
真实正例	T_P	F_N
真实负例	F_P	T_N

1) 准确率：对全部输出数据进行判断。

$$A=\frac{T_N+T_P}{T_N+F_N+T_P+F_P} \tag{21}$$

式中：A 为准确率；T_N 为真负例；T_P 为真正例；F_N 为假负例；F_P 为假正例。

2) 精确率：表示识别为正例标签中识别正确的比例。

$$P=\frac{T_P}{T_P+F_P} \tag{22}$$

式中，P 为精确率。

3) 召回率：表示算法识别正例标签的有效性。

$$R=\frac{T_P}{T_P+F_N} \tag{23}$$

式中，R 为召回率。

4) F_1 值：表示召回率和精确率的调和平均数，是对算法的综合考查。F_1 值的表达如式(24)所示。

$$F_1=2\times\frac{P\times R}{P+R} \tag{24}$$

5) ROC 曲线(receiver operating characteristic curve)：反映了正报率与误报率之间的相对关系。其中，AUC(area under curve)值为 ROC 曲线与坐标轴围成的面积，AUC 值越接近 1，算法性能越好。

3.2.2 算例一：掌握全局信息的 FDIA

考虑一般攻击模型的特例，即假设攻击者在掌握 CPPS 完整信息的情况下，研究所提算法的检测定位性能。图 11 为 IEEE 14 节点受到攻击后，8 种算法在各个节点上的检测定位准确率，其中坐标顺时针方向按节点顺序排列电压的相角和幅值状态，因节点 1 的相角与幅值为参考值，所以删除该节点标签，检测定位标签为 26 个。通过仿真结果可知，BP 神经网络总体效率较差且稳定性不足，平均准确率仅为 91.34%；KNN 的 FDIA 检测定位准确率约为 93%，相较于 BP 神经网络有显著提升且稳定性更佳；而 ELM 的平均准确率为 94.34%，从各节点准确率看，较前述算法有明显优势；相较于单隐层的 ELM，作为深度网络的 CNN 平均准确率进一步提升至 95.40%; DELM 通过正交化设计有效去除特征以外的噪声，削弱了特征之间的负面影响，因

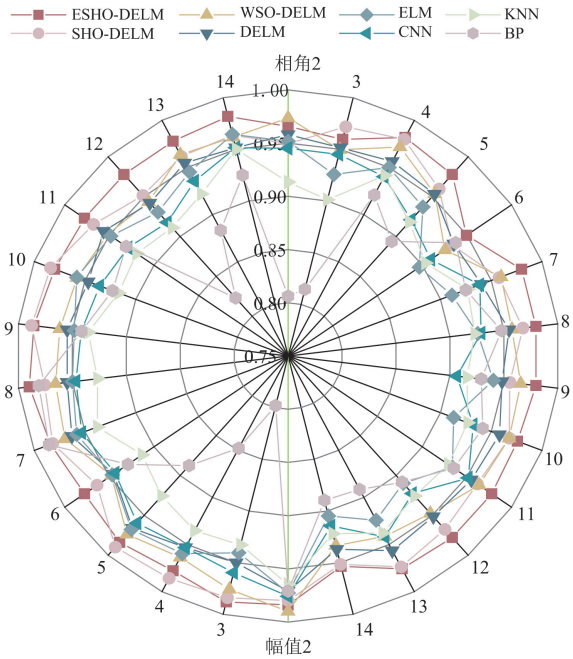


图 11 IEEE 14 节点系统下不同算法的攻击定位准确率

Fig. 11 Attack location accuracy of different algorithms in IEEE 14 bus system

此其定位准确率优于 CNN，高达 95.59%。

为了进一步提高 DELM 检测定位的稳定性，本文通过优化算法对 DELM 的输入权重和偏置进行寻优，并对比了不同优化算法的效果。在 DELM 的基础上引入 WSO，其准确率提升至 96.21%，稳定性有明显改善；进一步加入 SHO 后，DELM 的平均准确率为 96.93%，相对于 WSO，不仅准确率有所提升，而且稳定性更佳。由此可见，SHO 较 WSO 在 DELM 参数择优上更具优势；在 SHO-DELM 基础上，融入能够提高海马收敛速度和改善海马局部最优问题的 ECV 后，ESHO-DELM 的准确率达到了 97.86%，且收敛精度更高。图 12 为 ESHO 和 SHO 在 IEEE 14 节点系统中的收敛曲线，ESHO 较 SHO 有更低的适应度值，即训练的错误率更低，有效改善了 SHO 收敛精度低的局限性。验证可得，在相同条件下，ESHO-DELM 算法的检测定位准确率相对其他算法有明显优势。

图 13 为各算法准确率、精度、召回率、F_1 值和 AUC 的对比结果，ESHO-DELM 的召回率相比于 SHO-DELM、WSO-DELM、DELM、ELM、CNN、KNN 和 BP 分别提高了 1.29%、2.97%、3.75%、7.21%、4.00%、6.21%和 6.46%，由此验证了所提算法具有更优的检测定位性能，能精确识别并定位受攻击的状态量。

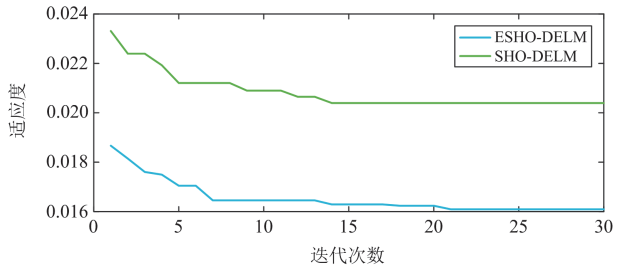


图 12 IEEE 14 节点系统收敛曲线

Fig. 12 IEEE 14 bus system convergence curves

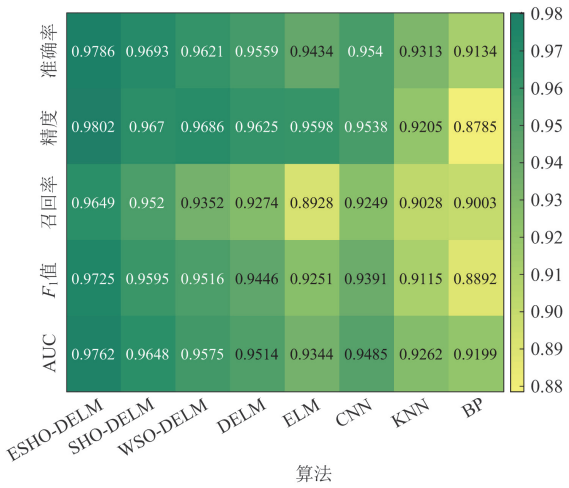


图 13 IEEE 14 节点系统对比算法指标

Fig. 13 Comparison algorithm indicators of IEEE 14 bus system

各算法在 IEEE 14 节点系统的 ROC 曲线如图 14 所示。ROC 曲线越趋近于左上角，则曲线与横坐标所围面积 AUC 值越大，即算法性能越好。相较于对比算法，ESHO-DELM 的 ROC 曲线最趋近于左上角，表明本文所提算法的识别能力更优，在 FDIA 检测定位中具有显著优势。

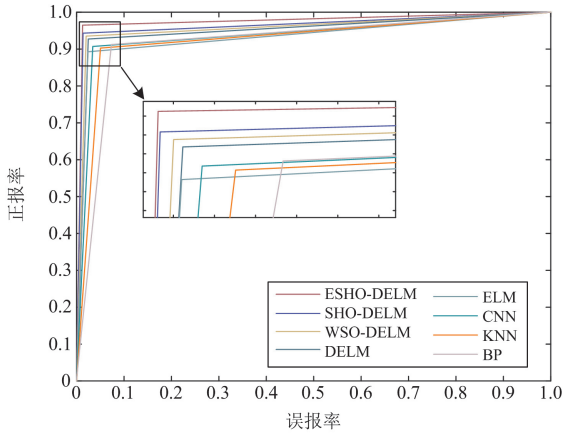


图 14 IEEE 14 节点系统 ROC 曲线

Fig. 14 ROC curves of IEEE 14 bus system

3.2.3 算例二：掌握部分信息的 FDIA

实际上攻击者难以获取系统全部的拓扑结构和参数信息，为实现较隐蔽的攻击效果，需精心设计虚假数据以满足线路拓扑与潮流约束，且需对部分未知信息进行估计，尽可能缩小篡改后状态估计的残差。因此本算例主要研究攻击者在掌握电网部分拓扑信息的情况下，各检测定位算法的有效性，与 IEEE 14 节点系统相比更具普适性。

图 15 为各算法的节点准确率结果，ESHO-DELM 在 IEEE 57 节点系统的平均准确率为 95.15%，较其他对比算法有明显优势，SHO-DELM、WSO-DELM、DELM、ELM、CNN、KNN 和 BP 的准确率分别为 94.18%、92.47%、91.06%、89.94%、90.06%、89.33% 和 87.52%。相较于 IEEE 14 节点系统，IEEE 57 节点系统的综合指标较低，因为 IEEE 57 节点系统数据的维度远大于 IEEE 14 节点系统数据的维度，而高维数据对检测定位精度影响较大；且经过隐含层神经元多次降维后，会丢失原始数据中的部分信息，各量测值之间的关联性变弱，使算法在学习时产生困难，但在相同系统下，ESHO-DELM 较其他算法仍具有最高的平均准确率。

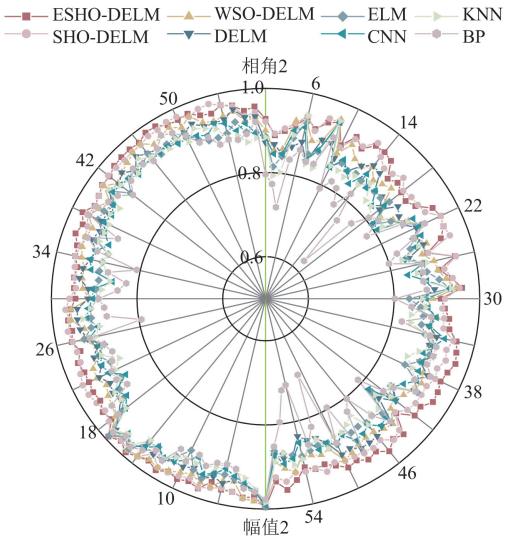


图 15 IEEE 57 节点系统下不同算法的攻击定位准确率

Fig. 15 Attack location accuracy of different algorithms in IEEE 57 bus system

图 16 为 ESHO 和 SHO 在 IEEE 57 节点系统上的收敛曲线对比，SHO 适应度值在第 15 次迭代后基本不再变化，保持在 2.60%左右，收敛性能较差；而 ESHO 在第 25 次迭代后依然能够找到更优解，较 SHO 有更低的适应度值 2.32%，即训练的错误率更低，准确率更高。这表明在相同条件下，ESHO-

DELM 的检测定位能力较其他算法有较大优势。

图 17 为 IEEE 57 节点系统的评估指标，ESHO-DELM 的召回率相比于 SHO-DELM、WSO-DELM、DELM、ELM、CNN、KNN 和 BP 分别提高了 3.08%、6.06%、9.43%、11.33%、11.48%、13.20%和 11%，可以直观地看出，所提算法在 IEEE 57 节点系统能够更好地识别并精确定位受污染的状态量，从而实现 FDIA 精确定位。

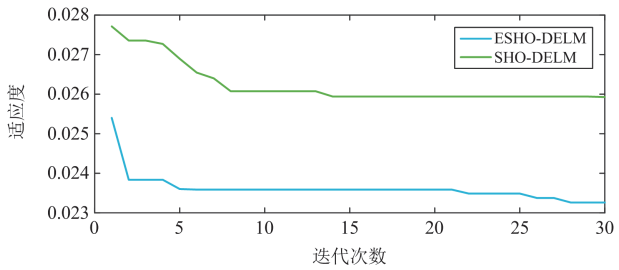


图 16 IEEE 57 节点系统收敛曲线

Fig. 16 Convergence curves of IEEE 57 bus system

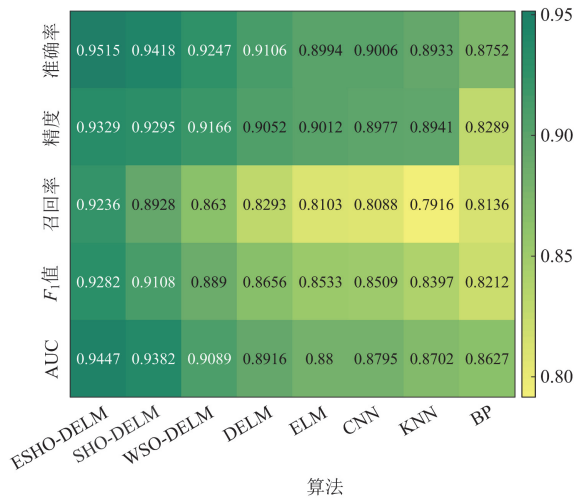


图 17 IEEE 57 节点系统对比算法指标

Fig. 17 Comparison algorithm indicators of IEEE 57 bus system

各算法在 IEEE 57 节点系统的 ROC 曲线如图 18 所示。ESHO-DELM 具有最高的 AUC 值 0.9447，即识别能力最强；其余 7 种算法的 AUC 值分别为 0.9382、0.9089、0.8916、0.8800、0.8795、0.8702 和 0.8627。所提算法能够在较低的误报率情况下准确识别出被攻击的节点状态量，验证了在相同系统与攻击场景下所提算法的优越性；且在处理复杂高维的 CPPS 量测数据时，所提算法综合指标均高于其他算法，进一步验证了其优良的泛化性能。

3.2.4 算法耗时分析

为体现本文 DELM 在处理复杂多维的电网量测数据的优势，本文将 DELM、CNN、KNN 和 BP 的训练与测试耗时进行了对比。各算法的耗时对比如表 3 所示。

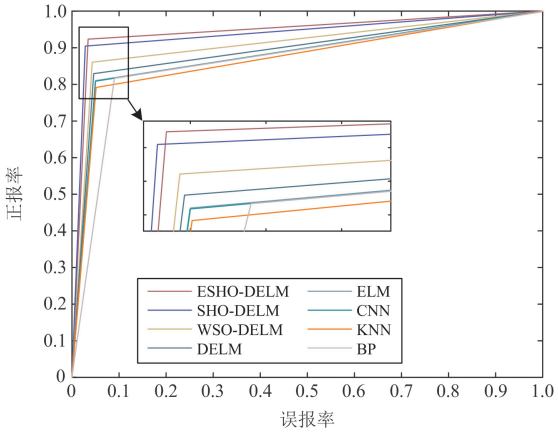


图 18 IEEE 57 节点系统 ROC 曲线

Fig. 18 ROC curves of IEEE 57 bus system

表 3 算法耗时对比

Table 3 Comparison of algorithm time consumption

s

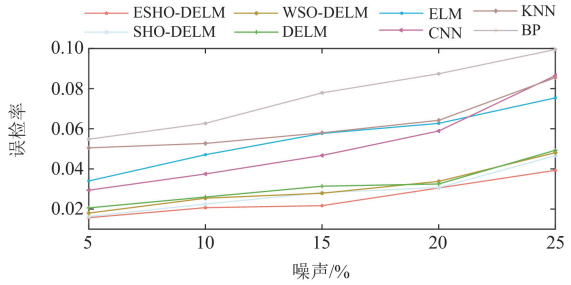
定位算法	IEEE 14 节点系统		IEEE 57 节点系统	
	训练时长	测试时长	训练时长	测试时长
DELM	**0.110 562**	**0.008 042**	**0.471 688**	**0.014 693**
CNN	10.279 535	0.027 561	43.018 018	0.061 714
KNN	2.264 820	2.138 420	4.105 700	4.060 83
BP	9.078 629	0.100 334	30.959 203	0.105 932

DELM 的训练测试用时少于其他算法，验证了 DELM 相较于其他 3 种算法响应速度更快，且随着量测数据维度增大仍有明显优势。结合热力图的定位指标分析，在不同的攻击场景下，能更精确识别污染状态量。在 ESHO 对 DELM 的输入权重和偏置寻优后具有更优的检测定位性能。

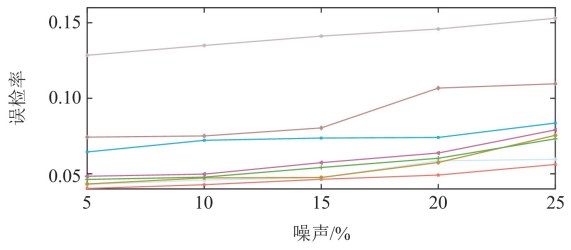
3.2.5 算法鲁棒性分析

为进一步对不同噪声下所提算法的鲁棒性进行验证，本文基于两节点系统，在量测数据中分别加入 5%、10%、15%、20%及 25%五个标准等级的噪声，以分析检验各个算法的抗干扰能力。各算法在两节点系统的鲁棒性仿真结果如图 19 所示，在 IEEE 14 节点系统中，随着噪声水平升高，ESHO-DELM 的误检率缓慢上升，即使当噪声标准为 25%时，其误检率依然低于 0.04；而其他算法在实现 FDIA 检测定位时，误检率所受影响相对较大，以 BP 神经网络为例，当噪声标准为 5%时，攻击误检率为 0.0548；随着噪声水平升高，误检率的增长幅度较大，最高达到了 0.0995。原因在于当噪声水平升高时，该算

法相较于 ESHO-DELM 难以区分受到干扰后的正常量测与异常量测之间的差异，从而导致被误判为正常的受攻击数据的比例较高，部分攻击数据无法被发现以致 FDIA 检测定位效率大打折扣，对电力系统造成更大威胁。



(a) IEEE 14节点系统



(b) IEEE 57节点系统

图 19 各算法鲁棒性分析

Fig. 19 Robustness analysis of each algorithm

在 IEEE 57 节点系统的误检率测试中，因 ELM、KNN 以及 BP 神经网络的结构简单，面向更复杂的节点系统量测数据时算法表现进一步变差；而 ESHO-DELM 在不同标准等级噪声干扰下，较其他算法仍然能够保持较低误检率。进一步说明本文所提算法对不同节点系统中不同噪声等级的量测数据均有更优的检测定位能力，验证了 ESHO-DELM 具有更优的抗噪声能力，定位性能更具鲁棒性。

4 结论

针对已有 FDIA 检测算法无法精确定位受攻击位置的局限性，本文提出一种基于 ESHO 优化 DELM 的 FDIA 检测定位算法。将 ELM 和 ELM-AE 相结合得到了具备强特征表达能力的 DELM，并利用 ESHO 对 DELM 的输入权重和偏置寻优，从而提高了算法指标的稳定性和检测定位精度。

通过在 IEEE 14 节点系统和 IEEE 57 节点系统进行仿真测试，将注入攻击后的残差与检测阈值 τ，以及攻击前后的量测和状态量分别比较，对非线性网络攻击模型的隐蔽性进行评估，通过对仿真结果分析可知，该攻击模型能够成功躲避 BDD 机制，验证了该攻击模型的可行性和隐蔽性。

在 IEEE 14 节点系统和 IEEE 57 节点系统进行大量仿真测试，以评估 ESHO-DELM 的 FDIA 检测定位性能。测试结果表明，该算法不依赖系统的拓扑结构和模型参数，在面向复杂的高维 CPPS 量测数据时，DELM 能有效提取特征，具有良好的泛化性能，与其他算法对比，该算法的评价指标均有明显优势，即具备更强的 FDIA 检测定位能力。

参考文献

[1] WANG Qi, LI Feng, TANG Yi, et al. Integrating model-driven and data-driven methods for power system frequency stability assessment and control[J]. IEEE Transactions on Power Systems, 2019, 34(6): 4557-4568.

[2] 田猛, 王先培, 董政呈, 等. 基于拉格朗日乘子法的虚假数据攻击策略[J]. 电力系统自动化, 2017, 41(11): 26-32.
TIAN Meng, WANG Xianpei, DONG Zhengcheng, et al. Injected attack strategy for false data based on Lagrange multipliers method[J]. Automation of Electric Power Systems, 2017, 41(11): 26-32.

[3] 汤奕, 李梦雅, 王琦, 等. 电力信息物理系统网络攻击与防御研究综述(二)检测与保护[J]. 电力系统自动化, 2019, 43(10): 1-9, 18.
TANG Yi, LI Mengya, WANG Qi, et al. A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection[J]. Automation of Electric Power Systems, 2019, 43(10): 1-9, 18.

[4] 王先培, 田猛, 董政呈, 等. 输电网虚假数据攻击研究综述[J]. 电网技术, 2016, 40(11): 3406-3414.
WANG Xianpei, TIAN Meng, DONG Zhengcheng, et al. Survey of false data injection attacks in power transmission systems[J]. Power System Technology, 2016, 40(11): 3406-3414.

[5] 苏盛, 吴长江, 马钧, 等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术, 2014, 38(11): 3115-3120.
SU Sheng, WU Changjiang, MA Jun, et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]. Power System Technology, 2014, 38(11): 3115-3120.

[6] XIAHOU Kaishun, LIU Yang, WU Qinghua. Decentralized detection and mitigation of multiple false data injection attacks in multiarea power systems[J]. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 2022, 3(1): 101-112.

[7] 吴英俊, 汝英涛, 刘锦涛, 等. 基于集员滤波的自动发电控制系统虚假数据注入攻击检测[J]. 电力系统自动

化, 2022, 46(1): 33-41.
WU Yingjun, RU Yingtao, LIU Jintao, et al. False data injection attack detection for automatic generation control system based on set-membership filtering[J]. Automation of Electric Power Systems, 2022, 46(1): 33-41.

[8] 王琦, 邰伟, 汤奕, 等. 面向电力信息物理系统的虚假数据注入攻击研究综述[J]. 自动化学报, 2019, 45(1): 72-83.
WANG Qi, TAI Wei, TANG Yi, et al. A review on false data injection attack toward cyber-physical power system[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.

[9] 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.

[10] 蒋正威, 张超, 孙伟乐, 等. 基于神经网络的电网假数据注入攻击检测方法研究[J]. 浙江电力, 2020, 39(11): 45-50.
JIANG Zhengwei, ZHANG Chao, SUN Weile, et al. Detection method of false data injection attack on power grid based on neural networks[J]. Zhejiang Electric Power, 2020, 39(11): 45-50.

[11] MUSLEH A S, CHEN G, DONG Z Y, et al. Attack detection in automatic generation control systems using LSTM-based stacked autoencoders[J]. IEEE Transactions on Industrial Informatics, 2023, 19(1): 153-165.

[12] 连祥龙, 钱瞳, 张银, 等. 基于 DeepWalk 算法的电力系统错误数据注入网络攻击分类方法[J]. 电力自动化设备, 2023, 43(3): 166-171.
LIAN Xianglong, QIAN Tong, ZHANG Yin, et al. Cyber attack classification method of false data injection in power system based on DeepWalk algorithm[J]. Electric Power Automation Equipment, 2023, 43(3): 166-171.

[13] 黄冬梅, 何立昂, 孙锦中, 等. 基于边缘计算的电网假数据攻击分布式检测方法[J]. 电力系统保护与控制, 2021, 49(13): 1-9.
HUANG Dongmei, HE Li'ang, SUN Jinzhong, et al. Distributed detection method for a false data attack in a power grid based on edge computing[J]. Power System Protection and Control, 2021, 49(13): 1-9.

[14] 董运昌, 王启明, 曹杰, 等. 基于过采样和级联机器学习的电网虚假数据注入攻击识别[J]. 电力系统自动化, 2023, 47(8): 179-188.
DONG Yunchang, WANG Qiming, CAO Jie, et al. Identification of false data injection attacks in power grid based on oversampling and cascade machine learning[J]. Automation of Electric Power Systems, 2023, 47(8): 179-188.

[15] CHAKHCHOUKH Y, ISHII H. Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations[J]. IEEE Transactions on Power Systems, 2016, 31(6): 4395-4405.

[16] JORJANI M, SEIFI H, VARJANI A Y. A graph theory-based approach to detect false data injection attacks in power system AC state estimation[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2465-2475.

[17] ZHAO Junbo, ZHANG Gexiang, LA SCALA M, et al. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1580-1590.

[18] KHALID H M, CHIH J. Immunity toward data-injection attacks using multisensor track fusion-based model prediction[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 697-707.

[19] CHEN Haoran, WANG Jun, ZHU Yonghai, et al. Deep learning based localization detection technique for false data injection attacks[C] // 2024 IEEE 4th International Conference on Power, Electronics and Computer Applications (ICPECA), January 26-28, 2024, Shenyang, China: 1313-1319.

[20] HEGAZY H I, TAG ELDIEN A S, TANTAWY M M, et al. Online location-based detection of false data injection attacks in smart grid using deep learning[C] // 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), November 24-26, 2022, Bali, India: 153-159.

[21] DOU Chunxia, WU Di, JIN Bo, et al. A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM[J]. CSEE Journal of Power and Energy Systems, 2022, 8(6): 1697-1707.

[22] 张有兵, 林一航, 黄冠弘, 等. 深度强化学习在微电网系统调控中的应用综述[J]. 电网技术, 2023, 47(7): 2774-2788.
ZHANG Youbing, LIN Yihang, HUANG Guanhong, et al. Review on applications of deep reinforcement learning in regulation of microgrid systems[J]. Power System Technology, 2023, 47(7): 2774-2788.

[23] 李刚, 刘燕, 宋雨, 等. 基于信息融合的电力大数据可视化预处理方法[J]. 广东电力, 2016, 29(12): 10-14.
LI Gang, LIU Yan, SONG Yu, et al. Visualization pretreatment method for electric power big data based on information fusion[J]. Guangdong Electric Power, 2016, 29(12): 10-14.

[24] 李峰, 王琦, 胡健雄, 等. 数据与知识联合驱动方法研究进展及其在电力系统中应用展望[J]. 中国电机工程

学报, 2021, 41(13): 4377-4390.
LI Feng, WANG Qi, HU Jianxiong, et al. Combined data-driven and knowledge-driven methodology research advances and its applied prospect in power systems[J]. Proceedings of the CSEE, 2021, 41(13): 4377-4390.

[25] ABBAS S, KHAN M A, REHMAN A, et al. Modeling, simulation and optimization of power plant energy sustainability for IoT enabled smart cities empowered with deep extreme learning machine[J]. IEEE Access, 2020, 8: 39982-39997.

[26] NGUYEN D, NGUYEN N T, TRAN Q, et al. Tradeoff different construction project goals in using a novel multi-objective sea horse algorithm[J]. Alexandria Engineering Journal, 2023, 82: 55-68.

[27] 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.

[28] 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): 3226-3236.
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): 3226-3236.

[29] 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.

[30] CHEN Bairen, LI Mengshi, XIAHOU Kaishun, 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): 1-11.

[31] 李经儒, 潘峰, 杨雨瑶, 等. 考虑源荷随机性与相关性的直流配电网量测概率优化配置方法[J]. 电测与仪表, 2024, 61(7): 138-145.
LI Jingru, PAN Feng, YANG Yuyao, et al. Stochastic optimal placement method of measurement for DC distribution network considering probability and correlation of source load[J]. Electrical Measurement & Instrumentation, 2024, 61(7): 138-145.

[32] 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.

[33] 龙干, 黄媚, 方力谦, 等. 基于改进多元宇宙算法优化 ELM 的短期电力负荷预测[J]. 电力系统保护与控制, 2022, 50(19): 99-106.
LONG Gan, HUANG Mei, FANG Liqian, et al. Short-term power load forecasting based on an improved multi-verse optimizer algorithm optimized extreme learning machine[J]. Power System Protection and Control, 2022, 50(19): 99-106.

[34] 孙世明, 岑红星, 白建民, 等. 基于集成 SAO 优化互相关熵极限学习机模型的变压器故障诊断方法[J]. 电测与仪表, 2024, 61(9): 56-64.
SUN Shiming, CEN Hongxing, BAI Jianmin, et al. Transformer fault diagnosis method based on integrated correntropy extreme learning machine model optimized by SAO[J]. Electrical Measurement & Instrumentation, 2024, 61(9): 56-64.

[35] 夏焰坤, 朱赵晴, 唐文张, 等. 基于改进秃鹰算法优化极限学习机的谐波发射水平估计[J]. 电力系统保护与控制, 2024, 52(1): 156-165.
XIA Yankun, ZHU Zhaoqing, TANG Wenzhang, et al. Harmonic emission level estimation method based on an improved bald eagle search optimized extreme learning machine[J]. Power System Protection and Control, 2024, 52(1): 156-165.

[36] 刘杰, 从兰美, 夏远洋, 等. 基于 DBO-VMD 和 IWOA-BILSTM 神经网络组合模型的短期电力负荷预测[J]. 电力系统保护与控制, 2024, 52(8): 123-133.
LIU Jie, CONG Meilan, XIA Yuanyang, et al. Short-term power load prediction based on DBO-VMD and an lWOA-BILSTM neural network combination model[J]. Power System Protection and Control, 2024, 52(8): 123-133.

收稿日期：2024-03-31；　　修回日期：2024-09-10

作者简介：

席　磊(1982—)，男，通信作者，博士生导师，教授，研究方向为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。E-mail: xilei2014@163.com

(编辑　许　威)