DOI: 10.19783/j.cnki.pspc.240042

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

席 磊[1,2]，董 璐[2]，程 琛[2]，田习龙[2]，李宗泽[2]

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

摘要：针对已有检测方法无法对虚假数据注入攻击(false data injection attack, FDIA)进行精确定位的问题，提出了一种基于混合黑猩猩优化极限学习机(extreme learning machine, ELM)的电力信息物理系统 FDIA 的定位检测方法。首先，使用 ELM 作为分类器，用于提取电力数据特征并检测系统各节点的异常状态。然后，采用一种具有全局搜索能力且局部收敛速度更快的混合黑猩猩优化策略，用于寻找 ELM 最优隐藏层神经元数量。建立基于混合黑猩猩优化 ELM 的检测方法，实现对 FDIA 的精准定位，有利于后续防御措施的实施。最后，在 IEEE 14 和 IEEE 57 节点系统中进行大量仿真对比实验。结果表明，所提方法具有更佳的准确率、查准率、查全率和 F_1 值，对 FDIA 能够进行更为精准的定位检测。

关键词：电力信息物理系统；虚假数据注入攻击；极限学习机；黑猩猩优化

Location detection of a false data injection attack in a cyber-physical power system based on a hybrid chimp optimized extreme learning machine

XI Lei[1,2], DONG Lu[2], CHENG Chen[2], TIAN Xilong[2], LI Zongze[2]

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

Abstract: Existing detection methods cannot accurately locate a false data injection attack (FDIA). Thus a location detection method based on a hybrid chimp optimized extreme learning machine (ELM) is proposed for FDIA in a cyber-physical power system. First, an ELM is used as a classifier to extract the features of power data and detect the attacked state of each bus in the system. Then, a hybrid chimp optimization with global search and faster speed of local convergence is adopted to optimize the number of hidden layer neurons of the ELM. Thus, a detection method is established to realize the accurate location detection against FDIA. This is conducive to the implementation of subsequent defense measures. Finally, a large number of simulation experiments are carried out in IEEE14 and IEEE57 bus systems. The results show that the proposed method has better accuracy, precision, recall and F_1 score. This means this method can carry out more accurate location detection against FDIA.

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

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

0 引言

“双碳”目标[1]加速了电力系统与现代先进通信信息技术的碰撞融合[2]，电力信息物理系统(cyber-physical power system, CPPS)[3]逐渐发展成熟，但网络系统面临风险[4]威胁的概率也不断增加。其中，虚假数据注入攻击(false data injection attack, FDIA)[5-7]与不同形式的攻击[8]相比，更具隐藏性[9]和攻击性等特点，可通过通信信道、数据采集与监视控制系统(supervisory control and data acquisition, SCADA)[10]、相量测量单元(power management unit, PMU)[11]等物理设备侵入 CPPS。

基金项目：国家自然科学基金项目资助(52277108)

近年来，检测 FDIA 的方法可分为两类：基于系统模型[12-15]的检测方法和基于机器学习[16-18]的检测方法。基于系统模型的检测方法包括图论检测法[12-13]和状态估计检测法[14-15]。文献[12]将整个网络用图表示，寻找已检测到的离群点的邻接点，以此识别当前状态估计结果中的异常值。文献[13]利用相角马尔可夫图的 Kron 简化，将 FDIA 检测问题分解为若干局部边缘最大似然估计问题。文献[14]利用预测值与量测值之间的一致性，将该测量一致性检验与测量残差分析的结合与异常数据相比较。文献[15]利用最优递归滤波器算法同时动态估计系统状态和攻击信号，以实时检测攻击并进行补偿。

基于机器学习的 FDIA 检测方法包括强化学习[16]、支持向量机(support vector machine, SVM)[17]、循环神经网络[18]等。文献[16]利用所构建的集成分类器处理难以分类的样本，以有效区分非攻击类故障与 FDIA。文献[17]利用主成分分析法将历史数据投影到低维空间以简化计算，并训练分布式 SVM 以检测 FDIA。文献[18]将小波变换和深度神经网络相结合，提取系统在空间和时间域的动态特征，利用时间序列数据区分系统的正常状态与 FDIA。

虽然上述方法能对 FDIA 进行存在性[9]检测，但是无法对 FDIA 进行故障定位[19]。为使系统安全可靠地运行，不仅需要检测到 CPPS 的异常状态，还需要迅速准确地锁定攻击位置，以进行后续的防御措施。极限学习机(extreme learning machine, ELM)[20-21]应运而生。文献[20]将 FDIA 的检测问题转化为多标签二分类问题，利用预测值与真实值之间的一致性，通过聚合一系列 ELM 来检测 FDIA，并识别了其确切位置。文献[21]提出一种基于灰狼优化多隐藏层极限学习机的方法，从多标签二分类的角度出发，成功检测到系统中异常的状态量，并获取了 FDIA 的位置。

然而，ELM 中隐藏层神经元的数量对检测方法的泛化性能和稳定性有直接影响。若隐藏层神经元数量过少，则会导致所提取的信息量不足以表征训练样本特征，产生欠拟合问题；若隐藏层神经元数量过多，则会使网络结构复杂化而徒增训练时间，并发生过拟合。为此，文献[22]采用差分进化方法优化基于结构自适应分层 ELM 的隐藏层神经元数量和正则化因子，使所提方法对复杂故障具有较高的检测精度和容错能力。文献[23]利用人工免疫系统对 ELM 的输入参数进行优化，在检测网络异常时具有更好的收敛性。文献[24]将遗传算法与在线顺序 ELM 相结合，搜索隐藏层的最优参数，使所提算法性能优越。

虽然上述方法能优化 ELM 的参数，但是忽视了局部收敛，这会使优化算法总在重复的结果中进行筛查，减缓收敛速度，而依据局部收敛得到的信息进行全局搜索能更灵活地处理每次的寻优结果。为此，本文将具有局部收敛能力的黑猩猩优化(chimp optimization, ChO)[25]引入 ELM 中，对 ELM 隐藏层神经元的数量进行寻优，进而形成 ELM^{ChO} 算法，加快局部收敛从而获得全局最优解。然而，通过长期探索发现，基于群体智能优化策略的 ChO 遵循最优保存策略[26]，即在算法优化前期，随机初始化的种群优劣会影响算法的收敛速度。

为此，本文在 ELM^{ChO} 的优化前期引入对立学习(opposite-based learning, OBL)[27]策略，进而形成 OBL-ELM^{ChO} 算法。通过同时产生当前个体和相应的对立个体来增强群体多样性，进而加快算法优化前期的收敛速度。然而，ChO 中随从型黑猩猩个体总是根据领导型黑猩猩的平均位置来更新自己的位置，在算法优化后期，这种无差别的更新规则易使黑猩猩的位置更新陷入局部最优，从而导致收敛速度明显变慢甚至停止。

为此，本文在 OBL-ELM^{ChO} 算法的优化后期引入精英对立学习(elite opposite-based learning, EOBL)[28]策略，进而形成 OBL-ELM^{ChO}-EOBL 算法。在提高种群多样性的基础上，本文通过从当前种群中选择一些精英个体产生对立解来避免探索重复区域，从而提高算法优化后期的收敛速度。然而，本文经过多次实验发现，上述算法在优化后期存在开发能力较弱的问题。

为此，本文在 OBL-ELM^{ChO}-EOBL 的优化后期引入柯西变异(Cauchy mutations, CM)[29]策略，进而形成 OBL-ELM^{ChO}-CMEOBL 算法。在最优解位置上利用柯西算子进行扰动得到新解，以解决算法优化后期开发能力较弱而易陷入局部最优的问题。故本文提出一种基于 OBL-ELM^{ChO}-CMEOBL 的 FDIA 定位检测方法，并从多标签二分类的角度来看待和解决定位检测问题。在 IEEE 14 和 IEEE 57 节点系统中进行对比实验和消融实验，实验结果验证所提方法具有有效性，且相比于其他方法，所提方法的定位检测性能更优越。

1　FDIA 模型

注入 FDIA 的 CPPS 整体框架如图 1 所示。融入大量新能源[30]的智能电网向远程终端单元(remote terminal unit, RTU)实时发送数据，该数据通过通信网络传至监控设备 SCADA 与 PMU 进行报告，为状态估计提供数据基础。其中，坏数据检测[31]通过

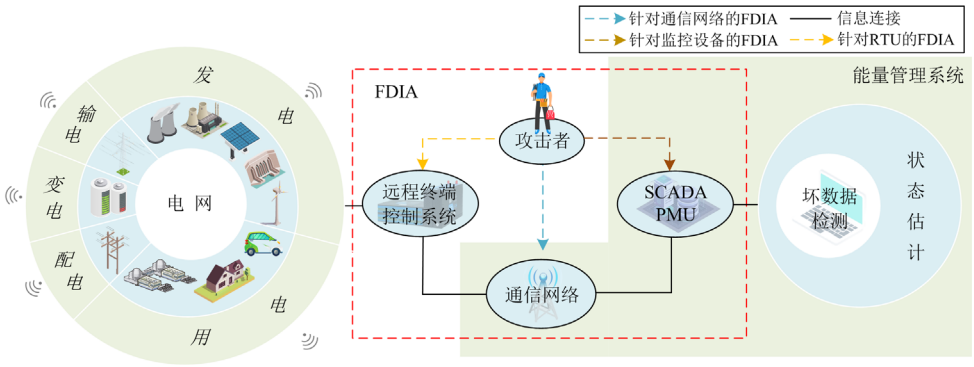


图 1 注入 FDIA 的 CPPS 整体框架图

Fig. 1 Overall framework of CPPS injected into FDIA

判断量测采样数据中是否存在坏数据来提高状态估计的可靠性，最终调度中心将数据反馈给电网，以维持电力系统的正常运行。在此框架下，FDIA 可针对 RTU、通信网络、监控设备进行数据攻击。本文通过篡改 SCADA 与 PMU 采集的线路潮流数据来对 CPPS 发起有效攻击。

目前，多数 FDIA 仅采用 SCADA 量测值来建立模型，并假设攻击者能够完全掌握网络信息来发起攻击。然而，由于结合 SCADA 与 PMU 的混合状态估计应用更加广泛，所以仅利用 SCADA 量测数据的模型并不准确，针对 PMU 量测的攻击也会带来风险。同时，因为网络信息不稳定且受到高度保护，所以该类攻击缺乏普适性。

为此，文献[32]提出一种更一般的攻击模型，采用 SCADA 和 PMU 混合量测数据，且仅需掌握部分攻击区域参数便能实施 FDIA。一般分为以下两个时期，如式(1)所示。

$$\begin{cases}(P_i^*,Q_i^*,P_{ij}^*,Q_{ij}^*,V_i^*,\theta_i^*,I_{ij}^{\mathrm{re}*},I_{ij}^{\mathrm{im}*})= \\ \qquad \arg\min[J_{1k}(P_{Gk})+J_{2k}(Q_{Gk})] \\ \min\left\|\boldsymbol{z}^{\Omega_{\mathrm{A}}}-h^{\Omega_{\mathrm{A}}}(\boldsymbol{x}_{\mathrm{A}})\right\|_0\end{cases} \tag{1}$$

式中：P_i^* 为有功注入；Q_i^* 为无功注入；P_{ij}^* 为有功潮流；Q_{ij}^* 为无功潮流，P_i^*、Q_i^*、P_{ij}^* 和 Q_{ij}^* 均为 SCADA 量测值；V_i^* 为电压幅值；θ_i^* 为相角；$I_{ij}^{\mathrm{re}*}$ 为电流向量实部；$I_{ij}^{\mathrm{im}*}$ 为电流向量虚部，V_i^*、θ_i^*、$I_{ij}^{\mathrm{re}*}$ 和 $I_{ij}^{\mathrm{im}*}$ 均为 PMU 量测值；P_{Gk} 和 Q_{Gk} 分别为第 k 个发电机的有功功率和无功功率；J 表示代价函数；下标 A 表示受到攻击；$\boldsymbol{z}^{\Omega_{\mathrm{A}}}$ 为攻击区域 Ω_{A} 中的量测向量；$h^{\Omega_{\mathrm{A}}}(\boldsymbol{x}_{\mathrm{A}})$ 表示量测向量和受到攻击的状态向量 $\boldsymbol{x}_{\mathrm{A}}$ 之间的关系。约束条件详见文献[32]。

在该攻击模型下，假设电力系统将量测数据全部传到控制中心，则在正常状态下，状态估计的量测方程如式(2)所示。

$$\boldsymbol{z}=h(\boldsymbol{x})+\boldsymbol{e} \tag{2}$$

式中：$\boldsymbol{z}$ 表示量测向量；$\boldsymbol{x}$ 表示状态向量；$\boldsymbol{e}$ 表示量测噪声，假设其由独立的高斯随机变量组成，即 $\boldsymbol{e}\sim\mathrm{N}(0,\sigma^2)$，标准差为 σ；$h(\bullet)$ 表示量测量与状态量之间的函数关系。

然而，作为能量管理系统[33]基础数据支撑[34]的状态估计是网络攻击的主要目标。为检测系统中可能存在的网络攻击，利用 L2 范数检测器对坏数据进行检测。当最大归一化残差值 $\|L\|$ 小于检测阈值[35] τ 时，认为系统不存在坏数据；反之则认为坏数据已被检测到并进行抑制和清除。

假设攻击者具备系统拓扑知识及破坏状态估计数据的能力，构建攻击向量 $\boldsymbol{a}$ 注入电力系统，则受到攻击的状态估计量测向量 $\boldsymbol{z}_{\mathrm{A}}=\boldsymbol{z}+\boldsymbol{a}$。此时，受攻击后的残差值 $\|L_{\mathrm{A}}\|$ 如式(3)所示。

$$\|L_{\mathrm{A}}\|=\|\boldsymbol{z}_{\mathrm{A}}-h(\boldsymbol{x}_{\mathrm{A}})\|=\|(\boldsymbol{z}-h(\boldsymbol{x}))-(h(\boldsymbol{s})-\boldsymbol{a})\| \tag{3}$$

式中：$\|\bullet\|$ 表示 L2 范数；$\boldsymbol{s}$ 表示受 $\boldsymbol{a}$ 影响的状态变量偏差向量；$\boldsymbol{x}_{\mathrm{A}}=\boldsymbol{x}+\boldsymbol{s}$ 表示受攻击后的状态向量。显然，当 $a_i<h(s_i)$ 时，$\|L_{\mathrm{A}}\|<\tau$，其中，a_i 表示攻击向量中第 i 个分量，s_i 表示受到相应影响的第 i 个状态变量偏差分量，上述不等式表明攻击者能够绕过坏数据检测，向系统中注入攻击向量来影响状态估计，使状态变量产生较大偏差，最终实现 FDIA。

2 OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 定位检测方法

CPPS 中通常存在复杂的高维量测数据，对此，本文提出一种基于 ELM$^{\mathrm{ChO}}$ 的 FDIA 检测方法，即采用 ELM 对 CPPS 中的数据进行特征提取并对 FDIA 输出结果进行分类，利用 ChO 优化 ELM 隐藏层参数，以提高全局搜索能力和局部收敛速度。

为进一步提高算法性能，在优化前期，利用 OBL 策略加快优化前期的收敛速度，在优化后期，利用 CMEOBL 策略改善优化后期收敛速度较慢及开发能力较弱的问题，进而形成 OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 算法来对 FDIA 实现更快速更精准的定位检测，减小其对 CPPS 的伤害并降低经济损失。

2.1 极限学习机(ELM)分类器

ELM 通过随机选择输入权值计算输出权值，大大减少了求解时间和因误差而陷入局部最优[35]值的可能性，提高了运算效率和泛化性能。多个领域的相关工作表明 ELM 能够准确且快速地完成分类任务[36]。

当单隐藏层神经网络模型[36]的训练集有 p 个攻击样本时，ELM 的输出函数如式(4)所示。

$$\boldsymbol{u}(\boldsymbol{v}_i)=\sum_{j=1}^{n}\boldsymbol{b}_j g(\boldsymbol{w}_j\cdot\boldsymbol{v}_i+\boldsymbol{\eta}_j)\ ,\ i=1,2,\cdots,p \tag{4}$$

式中：$\boldsymbol{v}_i$ 为输入向量；$\boldsymbol{u}(\cdot)$ 为输出向量；n 为 ELM 的隐藏层神经元总数；$\boldsymbol{b}_j$ 为连接 j 个隐藏层节点和输出层节点的权重向量；$g(\cdot)$ 为隐藏层的激活函数；$\boldsymbol{w}_j$ 为连接第 j 个输入层节点和隐藏层节点的权重向量；$\boldsymbol{\eta}_j$ 为第 j 个隐藏层神经元的阈值；$g(\boldsymbol{w}_j\cdot\boldsymbol{v}_i+\boldsymbol{\eta}_j)$ 为第 j 个隐藏层神经元相对于输入样本 $\boldsymbol{v}_i$ 的输出。

本文将 FDIA 定位检测问题看作多标签二分类问题，将每个节点的电压幅值和相角分别对应一个标签。ELM 按式(5)规则对输出变量进行分类。

$$\begin{cases}\boldsymbol{u}\geqslant 0.5\rightarrow\boldsymbol{u}=1\\ \boldsymbol{u}<0.5\rightarrow\boldsymbol{u}=0\end{cases} \tag{5}$$

据此分类结果判断状态变量是否正常，标记为 0 或 1，以获取受攻击的准确位置，以 IEEE 14 节点系统为例，ELM 实现定位检测过程如图 2 所示。ELM 将输出变量分类并标记为 0 和 1，并在 IEEE 14 节点系统中形成维度为 2480×28 的矩阵，其中，行向量共有 2480 个，表示 2480 个数据集，列向量共有 28 个，表示 28 个标签，该标签按照先相角后幅值的顺序，对 14 个节点相应的 28 个标签进行排列。第 1 个行向量为 $(0,1,0,\cdots,0,0,1)$，表示第 2 个节点的电压相角状态量和第 14 个节点的电压幅值状态量受到攻击；第 2 个行向量为全 0 行，表示 14 个节点的电压相角和幅值状态量均未受到攻击。

2.2 黑猩猩优化(ChO)策略

ChO 按不同智力与能力将黑猩猩分为驱动者(driver, d)、阻碍者(barrier, b)、追赶者(chaser, c)和攻击者(attacker, a)。捕猎过程具体如下：驱动者仅跟踪猎物，以防惊动猎物；阻碍者在树上占据位置以阻碍猎物在树枝间随意移动；追赶者通过快速移

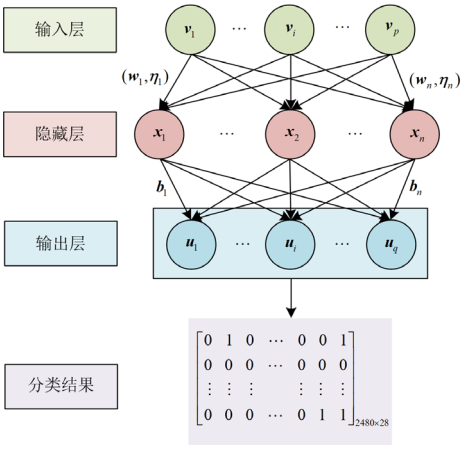


图 2 基于 FDIA 的 ELM 定位检测实现图解

Fig. 2 Realization diagram of ELM location detection based on FDIA

动来追赶猎物；攻击者通过预测猎物的逃生路线来迫使其退至追赶者的捕猎范围内，以实施抓捕动作。黑猩猩驱动和追赶猎物的数学模型[25]如式(6)所示。

$$\boldsymbol{X}_{\mathrm{chimp}}(t+1)=\boldsymbol{X}_{\mathrm{prey}}(t)-\boldsymbol{k}\cdot\boldsymbol{d} \tag{6}$$

式中：$\boldsymbol{X}_{\mathrm{chimp}}$ 表示某一领导型黑猩猩个体的位置向量；t 表示当前迭代次数；$\boldsymbol{X}_{\mathrm{prey}}$ 表示猎物所在位置向量；$\boldsymbol{d}$ 表示领导型黑猩猩与猎物之间的距离，$\boldsymbol{d}=\left|\boldsymbol{c}\boldsymbol{X}_{\mathrm{prey}}(t)-\boldsymbol{m}\boldsymbol{X}_{\mathrm{chimp}}(t)\right|$，其中，$\boldsymbol{c}$ 表示位置向量的系数向量，$\boldsymbol{m}$ 为混沌因子，表示混沌移动的影响；$\boldsymbol{X}_{\mathrm{prey}}$ 为猎物的位置向量；$\boldsymbol{k}$ 表示距离向量的系数向量。系数向量 $\boldsymbol{k}$ 和 $\boldsymbol{c}$ 的表达如式(7)和式(8)所示。

$$\boldsymbol{k}=f\cdot(2\cdot\boldsymbol{r}_1-1) \tag{7}$$

$$\boldsymbol{c}=2\cdot\boldsymbol{r}_2 \tag{8}$$

式中：$\boldsymbol{r}_1$ 和 $\boldsymbol{r}_2$ 表示[0, 1]中的均匀分布随机向量；f 在迭代过程中从 2.5 非线性地减小到 0。

为模拟黑猩猩的种群行为，假设第一个可用的最佳解决方案中的 4 种领导型黑猩猩能够了解到潜在猎物的位置，因此保留 4 个最佳解，随从型黑猩猩根据最佳黑猩猩随机更新自己的位置。每个最佳解决方案都是根据最优黑猩猩的位置来调节各自与猎物之间的距离，从而通过最后的攻击得到最优解。该智能群体捕猎的数学模型如式(9)—式(11)所示。

$$\begin{cases}\boldsymbol{d}_{\mathrm{a}}=\left|\boldsymbol{c}_1\boldsymbol{X}_{\mathrm{a}}-\boldsymbol{m}_1\boldsymbol{X}\right|,\ \ \boldsymbol{d}_{\mathrm{b}}=\left|\boldsymbol{c}_2\boldsymbol{X}_{\mathrm{b}}-\boldsymbol{m}_2\boldsymbol{X}\right|\\ \boldsymbol{d}_{\mathrm{c}}=\left|\boldsymbol{c}_3\boldsymbol{X}_{\mathrm{c}}-\boldsymbol{m}_3\boldsymbol{X}\right|,\ \ \boldsymbol{d}_{\mathrm{d}}=\left|\boldsymbol{c}_4\boldsymbol{X}_{\mathrm{d}}-\boldsymbol{m}_4\boldsymbol{X}\right|\end{cases} \tag{9}$$

$$\begin{cases}\boldsymbol{X}_1=\boldsymbol{X}_{\mathrm{a}}-\boldsymbol{k}_1\cdot\boldsymbol{d}_{\mathrm{a}},\ \boldsymbol{X}_2=\boldsymbol{X}_{\mathrm{b}}-\boldsymbol{k}_2\cdot\boldsymbol{d}_{\mathrm{b}}\\ \boldsymbol{X}_3=\boldsymbol{X}_{\mathrm{c}}-\boldsymbol{k}_3\cdot\boldsymbol{d}_{\mathrm{c}},\ \boldsymbol{X}_4=\boldsymbol{X}_{\mathrm{d}}-\boldsymbol{k}_4\cdot\boldsymbol{d}_{\mathrm{d}}\end{cases} \tag{10}$$

$$\boldsymbol{X}(t+1)=\frac{\boldsymbol{X}_1+\boldsymbol{X}_2+\boldsymbol{X}_3+\boldsymbol{X}_4}{4} \tag{11}$$

式中：$\boldsymbol{d}_{\mathrm{a}}$、$\boldsymbol{d}_{\mathrm{b}}$、$\boldsymbol{d}_{\mathrm{c}}$和$\boldsymbol{d}_{\mathrm{d}}$分别表示当前黑猩猩与攻击者、阻碍者、追赶者和驱动者黑猩猩间的距离；$\boldsymbol{c}_1$、$\boldsymbol{c}_2$、$\boldsymbol{c}_3$和$\boldsymbol{c}_4$分别表示对应位置向量的系数向量；$\boldsymbol{X}_{\mathrm{a}}$、$\boldsymbol{X}_{\mathrm{b}}$、$\boldsymbol{X}_{\mathrm{c}}$和$\boldsymbol{X}_{\mathrm{d}}$分别表示4种领导型黑猩猩的位置信息；$\boldsymbol{m}_1$、$\boldsymbol{m}_2$、$\boldsymbol{m}_3$和$\boldsymbol{m}_4$分别表示对应的混沌因子；$\boldsymbol{X}$表示当前某一黑猩猩个体所在位置信息；$\boldsymbol{X}_1$、$\boldsymbol{X}_2$、$\boldsymbol{X}_3$和$\boldsymbol{X}_4$分别表示4种黑猩猩更新后的位置信息；$\boldsymbol{k}_1$、$\boldsymbol{k}_2$、$\boldsymbol{k}_3$和$\boldsymbol{k}_4$分别表示对应距离向量的系数向量；$\boldsymbol{X}(t+1)$表示当前黑猩猩在4只最优黑猩猩的引导下移动的当前位置。

2.3 对立学习(OBL)策略

针对ChO在迭代前随机初始化的种群优劣会影响算法的收敛速度这一问题，本文引入OBL策略。因为初始群体通常不是最优群体，所以需要不断寻优以找到最合适的群体，在这一过程中，因为无法明确最佳解决方案，所以通过同时产生当前解和对立解是必要的，即将原始种群与对立种群合并，种群规模由n扩展为$2n$，以增大优化初始阶段寻得最优群体的可能性，从而加快优化前期的收敛速度。因此，本文在优化前期利用当前个体产生对立解激活更多群体，以在全局范围内进行均匀探索。

将上述策略与ChO相结合，得到

$$\boldsymbol{X}_i^* = \varepsilon_1 \cdot (\max(\boldsymbol{X}_{\mathrm{best}}) + \min(\boldsymbol{X}_{\mathrm{best}})) - \boldsymbol{X}_i \tag{12}$$

式中：ε_1为[0,1]之间的任意数；$\boldsymbol{X}_i$表示种群的第i个解；$\boldsymbol{X}_i^*$表示$\boldsymbol{X}_i$的对立解；$\boldsymbol{X}_{\mathrm{best}}$表示当前最优个体；$\max(\boldsymbol{X}_{\mathrm{best}})$和$\min(\boldsymbol{X}_{\mathrm{best}})$分别表示当前最优个体的最大值和最小值。

2.4 精英对立学习(EOBL)策略

虽然攻击型黑猩猩能够预测猎物逃跑路线，但是随从型黑猩猩总是根据领导型黑猩猩的平均位置来更新位置，尤其是在优化后期，这种无差别的更新规则会使黑猩猩因位置资源受限而陷入局部最优。为此，在ChO优化前期引入OBL策略的前提下，本文在优化后期引入EOBL策略，根据适应度值排序，从当前规模为$2n$的种群中选择n个更加合适的个体作为精英，以有效扩大种群搜索范围并避免探索重复区域，在提高种群多样性的基础上提高算法收敛速度。

将上述策略与ChO相结合，得到

$$\boldsymbol{X}_i^{\mathrm{e}*} = \varepsilon_2 \cdot (\boldsymbol{X}_i^{\mathrm{e}} + \boldsymbol{X}_i^{\mathrm{w}}) - \boldsymbol{X}_i^{\mathrm{e}} \tag{13}$$

式中：$\boldsymbol{X}_i^{\mathrm{e}}$表示$\boldsymbol{X}_i$的第$i$个精英解，即最优解；$\boldsymbol{X}_i^{\mathrm{e}*}$表示$\boldsymbol{X}_i^{\mathrm{e}}$的精英对立解；$\boldsymbol{X}_i^{\mathrm{w}}$表示当前最差个体；$\varepsilon_2$为[0,1]之间的任意数。

2.5 柯西扰动(CM)策略

经过多次实验发现，上述算法在优化后期的开发能力较弱。为此，本文在优化后期引入突变分布来帮助黑猩猩脱离局部最优，提高其开发能力。虽然高斯分布在突变分布中应用更为广泛，但是与原点附近的峰值相较，柯西分布逼近于0的速度更小，故源于柯西分布的CM具有更强的扰动能力，因此，本文在优化后期引入CM策略，更新优化后期的精英对立位置，在最优解位置上进行扰动变异操作得到新解，有效提高算法在优化后期逃离局部空间的开发能力。

将上述策略与ChO相结合，得到

$$\boldsymbol{X}_i^* = \boldsymbol{X}_i^{\mathrm{e}*} \cdot (1 + \tan(\pi \cdot (t/M - 0.5))) \tag{14}$$

式中，M为最大迭代次数，显然，$t/M \in (0, 1)$。

2.6 FDIA检测与定位

假设攻击者能够从CPPS中获取信号，并能在状态估计中顺利躲避坏数据检测，故本文将攻击模型的输出作为分类检测方法的输入。考虑到每次按同一比例划分同一数据集会导致模型过拟合，因此本文首先将数据集打乱，再按照3：1的比例将其划分为训练集和测试集，以提高ELM的泛化能力。为提高分类器的检测精度，本文引入ChO策略对ELM隐藏层神经元数量进行寻优，提高其全局搜索能力和局部收敛速度。为进一步改善$\mathrm{ELM}^{\mathrm{ChO}}$的性能，本文在优化前期引入OBL策略以加快前期收敛速度，在优化后期引入CMEOBL策略以提高后期收敛速度和开发能力。基于此，最终构建了OBL-$\mathrm{ELM}^{\mathrm{ChO}}$-CMEOBL方法定位检测FDIA，并对受到攻击的状态量进行辨识和清除，有效避免了FDIA对CPPS的影响。具体流程如图3所示。

3 算例分析

为验证交流攻击模型和分类检测方法的有效性和准确性，本文在Matlab R2017b中将IEEE 14和IEEE 57节点系统作为测试环境进行仿真实验，节点系统的拓扑如图4所示。

1) 攻击模型所用数据取自2016年广东东莞调度中心，分辨率为15 min。攻击模型利用Matpower来获取节点系统的拓扑结构和线路参数，并利用Yalmip求解器对式(2)所示的状态方程进行求解。

2) IEEE 14和IEEE 57节点系统在攻击模型中各生成2480组数据，利用本文所提方法与其他方法对该数据集进行对比实验和消融实验，以训练不同分类器并测试其性能。最大迭代次数均设置为500次。

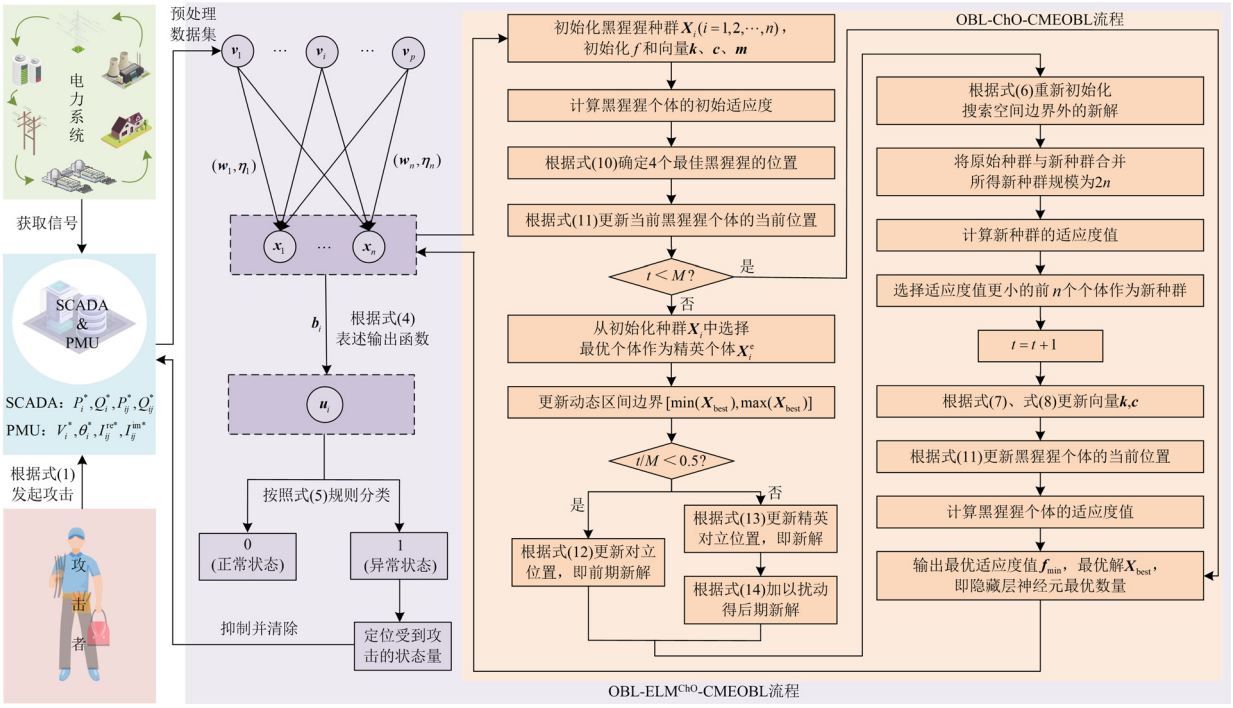
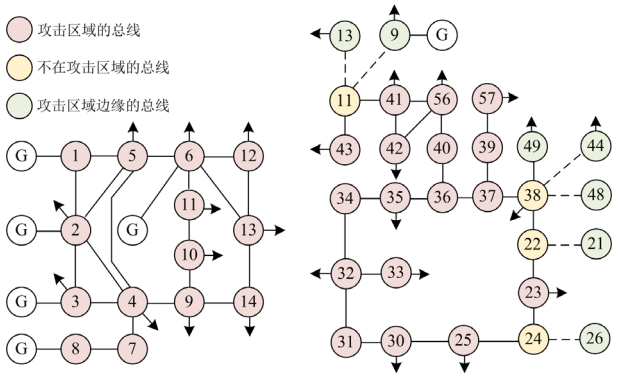


图 3 FDIA 定位检测整体框架图

Fig. 3 Overall flow chart of FDIA location detection



(a) IEEE 14 节点系统　(b) IEEE 57 节点系统

图 4 节点系统拓扑图

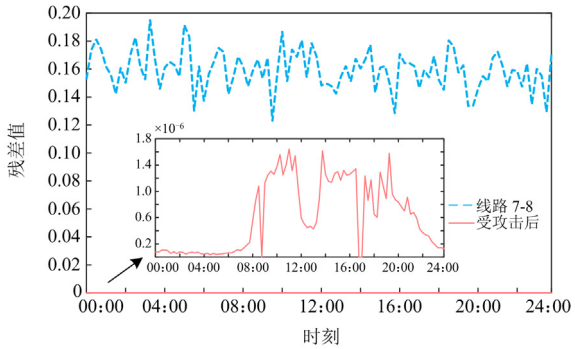
Fig. 4 Topology of the bus system

3.1 攻击仿真分析

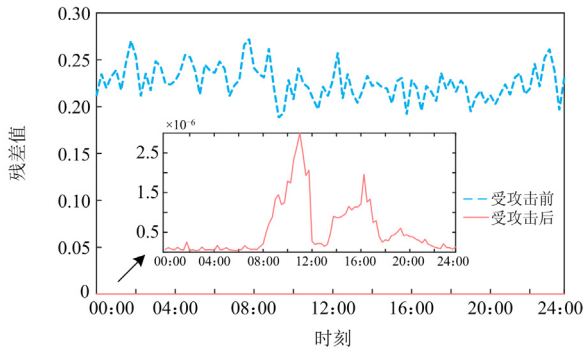
为保证数据和实验结果的可靠性，在进行 FDIA 检测仿真之前，本文首先对攻击仿真结果进行分析，不仅在 IEEE 14 节点系统下构建信息完整的攻击模型，而且为考虑更实际的情况，在 IEEE 57 节点系统下建立具有部分信息的攻击模型。在 IEEE 14 节点系统中，因为与线路 7-8 相关的节点最少，若攻击者使该线路过载，则可以发起最为隐蔽的攻击，所以本文选取线路 7-8 为攻击对象。由于 IEEE 节点系统仅拥有部分信息，故本文在有限的攻击区域中任意选择线路实施攻击。

图 5 为 IEEE 14 和 IEEE 57 节点系统实施全天攻击前后的最大归一化残差结果图。以图 5(a)为例，IEEE 14 节点系统在攻击前的残差分布在[0.1229, 0.1925]内，而攻击后残差的最大值仅为1.644×10^{-6}，即攻击后残差远小于攻击前残差。这表明攻击者能够成功躲避坏数据检测。分析图 5(b)数据仍然可得上述结论。

图 6 为两个系统攻击前后的电压幅值状态量变化。以图 6(b)为例，在 IEEE 57 节点系统中，第 30 个节点处发生最大偏差，此时电压相角状态变量在攻击前为 1.023，攻击后为 0.949，二者仅差 0.074，总体来看电压幅值状态变量在攻击前后变化不大。这表明，即便节点状态因遭受攻击而发生变化，攻击者仍然可以绕过坏数据检测。分析图 6(a)数据仍然



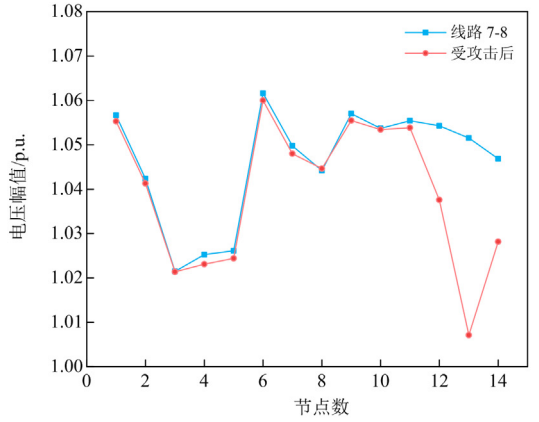
(a) IEEE 14节点系统



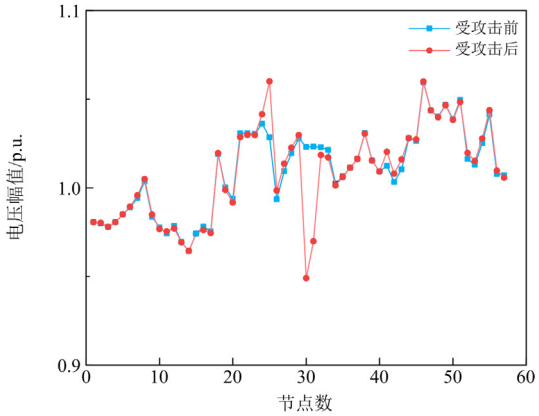
(b) IEEE 57节点系统

图 5 攻击前后最大归一化残差对比

Fig. 5 Comparison of the maximum normalized residuals before and after the attack



(a) IEEE 14节点系统



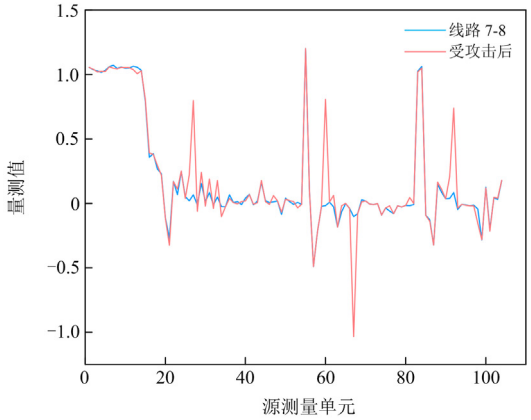
(b) IEEE 57节点系统

图 6 攻击前后电压幅值状态量对比

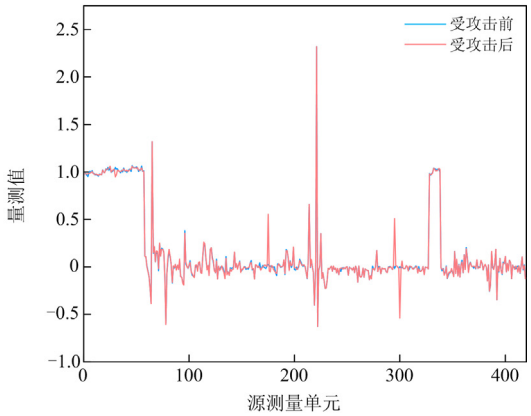
Fig. 6 Comparison of voltage magnitude state before and after the attack

可得上述结论。

图 7 为两个系统攻击前后的量测量对比。显然，攻击线路的量测量在攻击前后偏差最大，与此相关的线路的量测量在攻击前后也受到影响，与此无关的线路的量测量则在攻击前后影响甚微。结果证明，攻击者只需使目标线路过载就能实现 FDIA。



(a) IEEE 14节点系统



(b) IEEE57 节点系统

图 7 攻击前后量测量对比

Fig. 7 Comparison of quantity measurement before and after the attack

经攻击仿真结果验证，攻击者在两个节点系统中均能绕过坏数据检测发起攻击，故本文能将攻击模型输出数据用作 FDIA 检测方法的输入数据。

3.2 性能评估指标

针对二分类问题，根据检测结果真实类别和分类器预测类别的不同组合，将数据划分为真正例、假正例、真反例和假反例，定义如表 1 所示。

表 1 混淆矩阵中的数据类别

Table 1 Data categories in the confusion matrix

数据		预测类别	
		正例	反例
真实类别	正例	T_p	F_p
	反例	F_n	T_n

为避免因数据类别不平衡而使精度出现误导性结果，采用混淆矩阵加以度量。

1) 查准率：针对所有预测为正例的数据计算正例所占比。

$$P=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{P}}} \tag{15}$$

式中：P 为查准率；T_{P} 为真正例；F_{P} 为假正例。

2) 查全率：针对实际与预测相同类别的数据计算正例占比。

$$R=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{n}}} \tag{16}$$

式中：R 为查全率；F_{n} 为假反例。

3) F_1 值：为了平衡查准率和查全率这两个指标，将二者的调和平均数合成一个指标，即 F_1 值。

$$F_1=2\cdot\frac{P\cdot R}{P+R} \tag{17}$$

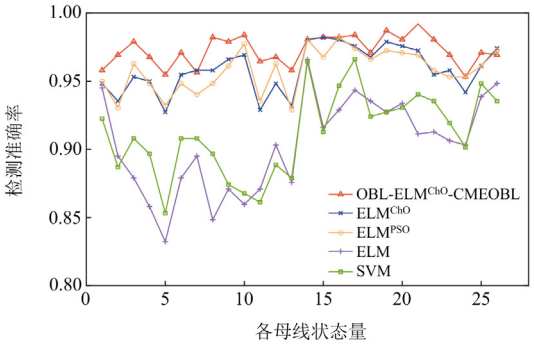
各个指标数值越大，分类器性能越优。

3.3 检测仿真分析

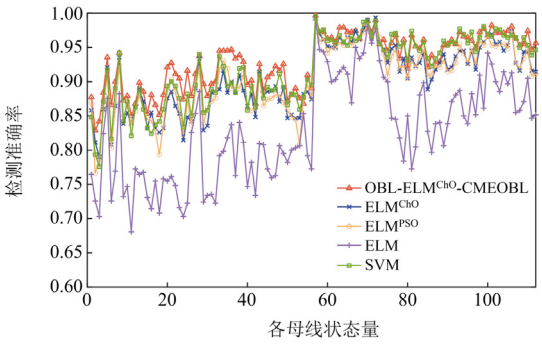
为验证所提方法检测CPPS中遭受FDIA的性能，本文进行 4 组性能评估实验：在 IEEE 14 和 IEEE 57 节点系统下，基于攻击模型[31]产生的数据集，本文所提 OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 与基本 ELM$^{\mathrm{ChO}}$[37]、同采用群智能策略的 ELM$^{\mathrm{PSO}}$[38]、同为经典分类方法的 ELM[20]和 SVM[17]这 5 种检测方法作对比实验；基于相同数据集，本文对 OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 作消融实验。考虑到攻击者对电网拓扑信息的掌握程度不同，本文在不同攻击场景下进行检测仿真实验。

3.3.1 对比分析

图 8 展现了两系统各母线状态检测准确率，其中，横坐标状态变量是按照节点顺序先相角后幅值来排列的标签数目。以 IEEE 14 节点系统为例，共 28 个标签，如图 2 的分类结果矩阵所示。因为删掉 1 个参考节点，相应减少 2 个标签，所以共 26 个标签，即为横坐标所示。纵坐标表示不同分类方法的每个标签对应的检测结果，该结果由检测方法所判断的结果和测试集真实值对比而得。综上，二者共同体现了不同分类方法在定位检测方面的性能优劣。如图 8(a)所示，在 IEEE 14 节点系统中，OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 的平均准确率为 97.883%，较 ELM$^{\mathrm{ChO}}$、ELM$^{\mathrm{PSO}}$、ELM 和 SVM 分别提高 1.752%、1.849%、7.540%和 6.623%。如图 8(b)所示，在 IEEE 57 节点系统中，本文所提方法的平均准确率为 92.960%，显著高于其他对比方法。显然，与 IEEE 14 节点系统相比，该系统正确率整体下降。这是因为 IEEE 57 节点系统数据有 419 维，远大于 IEEE 14 节点系统数据的 104 维，而高维数据对检测精度的影响较大。另外，机器学习通过多次降维克服维度灾难，但这会造成原始数据中部分信息的丢失，使原本相互关联的数据割裂，最终导致 IEEE 57 节点系统准确率更低。但是总体来看，本文所提方法在两系统中的平均准确率均为最高。



(a) IEEE 14节点系统

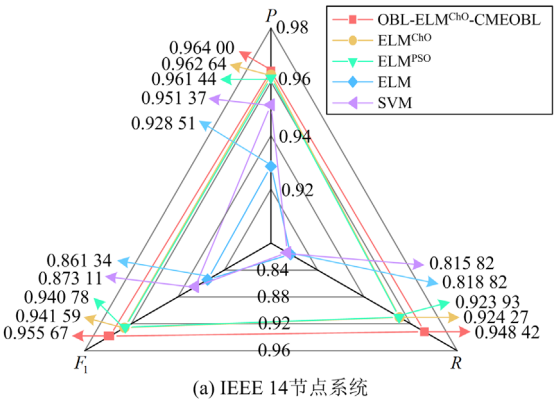


(b) IEEE 57节点系统

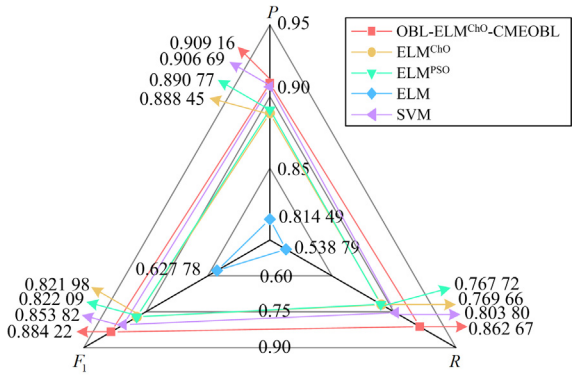
图 8 对比实验中受攻击状态定位检测准确率

Fig. 8 Attacked state location detection accuracy in comparison experiment

图 9 为两系统混淆矩阵中其他评价指标结果。以综合指标 F_1 值为例，图 9(a)中 OBL-ELM$^{\mathrm{ChO}}$-CMEOBL 方法较 ELM$^{\mathrm{ChO}}$、ELM$^{\mathrm{PSO}}$、ELM 和 SVM 方法分别提高 1.495%、1.583%、10.952%和 9.456%；



(a) IEEE 14节点系统



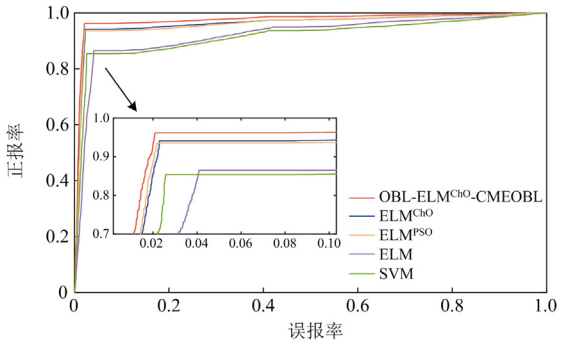
(b) IEEE 57节点系统

图 9 对比实验中性能评估指标结果

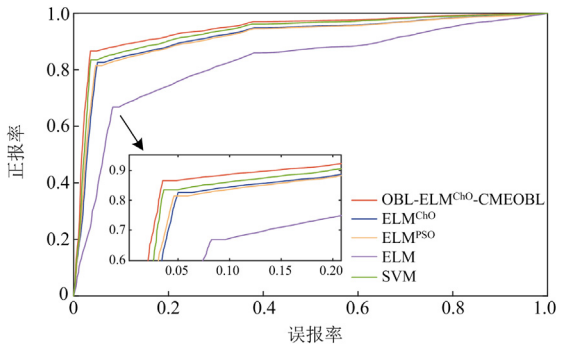
Fig. 9 Results of performance evaluation indexes in comparison experiment

图 9(b)中 5 种方法的 F_1 值分别为 88.422%、82.209%、82.198%、62.778%和 85.382%。这表明所提分类方法在查准率、查全率和 F_1 值这 3 项指标上均具有更优的值，能更准确且全面地识别并定位受到攻击的状态量。

图 10 为两系统受试者工作特征(receive operating characteristic, ROC)曲线图，表示数据正报率与误报率之间的关系。ROC 曲线下的面积(area under curve, AUC)值越接近于 1，即曲线拐点越靠近左上角，正报率越大，性能越优异。图 10(a)中 OBL-ELM^{ChO}-CMEOBL 方法的 AUC 值为 97.12%，显著高于其他 4 种方法；图 10(b)中本文所提方法的 AUC 值较图例所示其他 4 种方法依次提高 4.243%、4.440%、11.711%和 2.177%，即 OBL-ELM^{ChO}-CMEOBL 方法的 AUC 值在两系统中均最接近于 1，识别能力更强。



(a) IEEE 14节点系统



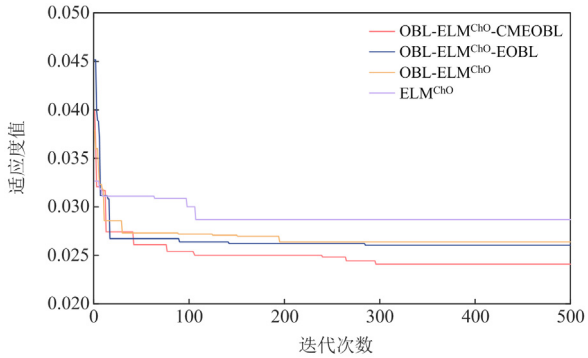
(b) IEEE 57节点系统

图 10 对比实验中 ROC 曲线

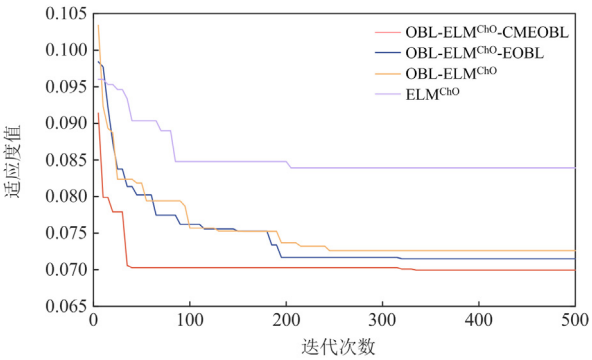
Fig. 10 ROC curve in comparison experiment

3.3.2 消融分析

为进一步分析 OBL-ELM^{ChO}-CMEOBL 方法中各组成部分的有效性，本文将 CM、EOBL、OBL、ChO 这 4 项改进措施依次消去，得到 OBL-ELM^{ChO}-EOBL、OBL-ELM^{ChO} 和 ELM^{ChO} 和 ELM 这 4 种检测方法，该部分采用以上方法作对比实验，测试新方法的表现，如图 11—图 14 所示。



(a) IEEE 14节点系统



(b) IEEE 57节点系统

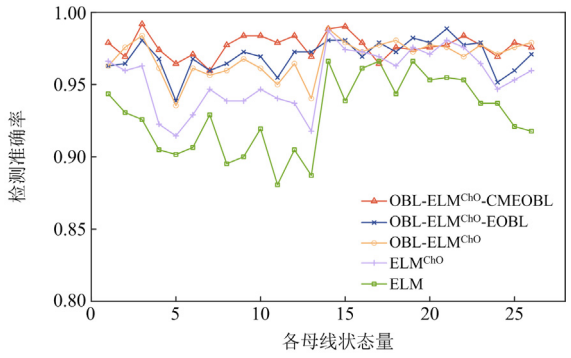
图 11 消融实验中迭代曲线

Fig. 11 Iteration curve in ablation experiment

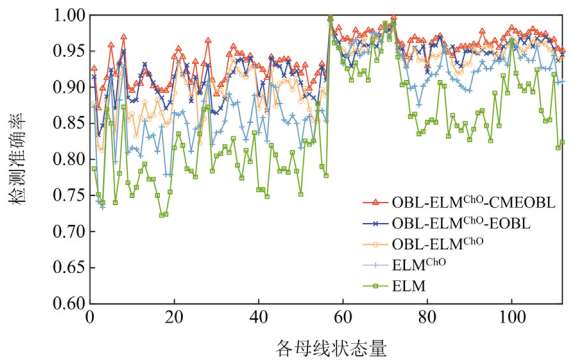
图 11 对 4 种优化方法的迭代曲线进行对比，以体现改进措施方法的全局寻优和搜索能力。因为 ELM 在分类过程中并不对参数进行寻优，所以此类图像不讨论 ELM。如图 11(a)所示，OBL-ELM^{ChO}-CMEOBL 在第 296 次迭代时适应度取得最小值，其值为 0.024 08，OBL-ELM^{ChO}-EOBL、OBL-ELM^{ChO} 和 ELM^{ChO} 分别在第 285、195 和 107 次迭代时达到

全局收敛。本文所提方法在第 67 次迭代时适应度取得最小值，其值为 0.069 95，其他 3 种方法分别在第 64、49 和 41 次迭代时达到全局收敛，如图 11(b)所示。此外，以第 500 次迭代为例，在两系统中，OBL-ELM^{ChO}-CMEOBL 方法的适应度值较图例所示其他 3 种方法变化最大，即所提方法的收敛速度最快。结果表明，当迭代次数相同时，OBL-ELM^{ChO}-EOBL、OBL-ELM^{ChO} 和 ELM^{ChO} 这 3 个方法的适应度值均显著减小，这表明，每项改进措施均对提高检测方法的准确率起着重要的积极作用，而所提方法具有更强的全局搜索能力和更高的局部收敛效率。

图 12 展现了两系统的检测准确率。如图 12(a)所示，OBL-ELM^{ChO}-CMEOBL 方法的平均准确率较图例所示其他 4 种方法分别提高了 6.970%、2.016%、0.545%和 0.377%；图 12(b)中本文所提方法的平均准确率为 94.496%，显著高于其他 4 种方法。结果证明，图例所示 5 种检测方法的平均准确率变化具有单调性，而本文所提方法的平均准确率高于其他方法。



(a) IEEE 14节点系统

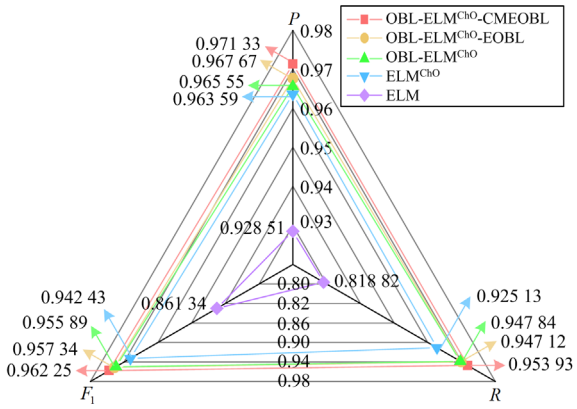


(b) IEEE 57节点系统

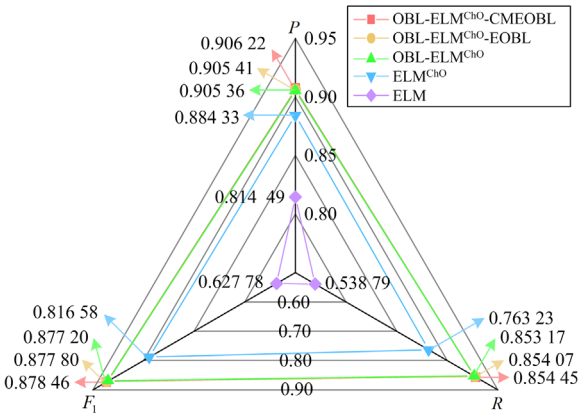
图 12 消融实验中受攻击状态定位检测准确率

Fig. 12 Attacked state location detection accuracy in ablation experiment

图 13 为混淆矩阵中其他评价指标结果。以综合指标 F_1 值为例，图 13(a)中 OBL-ELM^{ChO}-CMEOBL 较其余 4 种检测方法分别提高 0.513%、0.665%、2.103%和 11.715%，本文所提方法的 F_1 值为 87.846%，显著高于其他 4 种检测方法。显然，5 种方法的各项评价指标数值呈单调性变化，即在改进过程中，这 5 种方法在定位检测方面的全面性和准确性不断提高，最终使得本文所提方法表现最为优越。



(a) IEEE 14节点系统



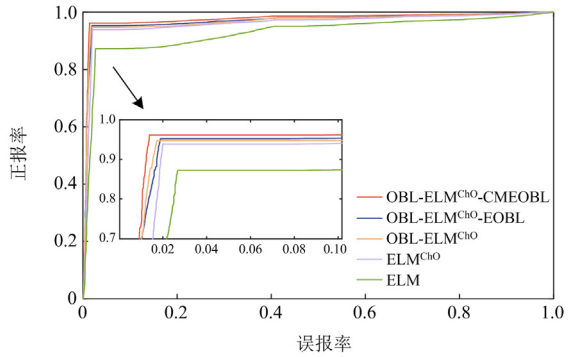
(b) IEEE 57节点系统

图 13 消融实验中性能评估指标结果

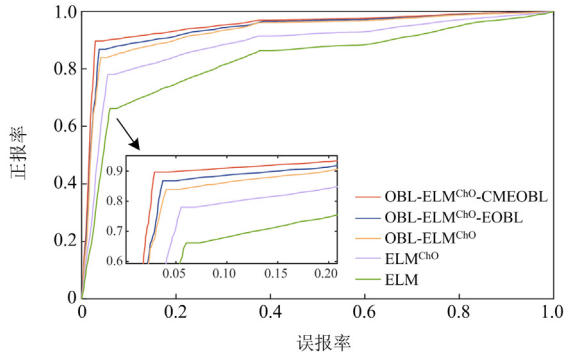
Fig. 13 Results of performance evaluation indexes in ablation experiment

图 14 为两系统的 ROC 曲线。图 14(a)中 5 种检测方法的 AUC 值分别为 97.55%、96.93%、96.74%、96.06%和 92.72%，图 14(b)中 OBL-ELM^{ChO}-CMEOBL 方法的 AUC 值为 94.98%，较其余 4 种方法分别提高 1.161%、2.008%、7.116%和 13.045%。这表明每项改进措施都对模型识别异常状态的准确率产生积极影响，而本文所提方法的识别能力更为突出。

以上 4 组实验结果表明，较同等检测方法，本文所提 OBL-ELM^{ChO}-CMEOBL 检测方法在识别与定位异常状态方面，不但具备更优的全局搜索和局部最优能力，而且具有更高的准确性和全面性。此外，在信息度不同的节点系统中，本文采用不同方法对受到攻击的状态量进行检测对比，实验结果表



(a) IEEE 14节点系统



(b) IEEE 57节点系统

图 14 消融实验中 ROC 曲线

Fig. 14 ROC curve in ablation experiment

明 OBL-ELM^{ChO}-CMEOBL 方法更适用于 FDIA 的检测与定位。

4 结论

针对 CPPS 遭受 FDIA 时无法精确定位这一问题，本文将其看作多标签二分类问题，在同时考虑 SCADA 和 PMU 量测量的前提下，分别在 IEEE 14 和 IEEE 57 节点系统构建攻击模型，提出一种基于 OBL-ELM^{ChO}-CMEOBL 的 FDIA 定位检测方法。

所提方法将 ELM 作为检测 FDIA 的分类器，用于特征提取和异常状态检测，并利用 ChO 策略对 ELM 隐藏层神经元的数量进行寻优，以更快的局部收敛速度获得全局最优解，并在前期采用 OBL 策略扩大了搜索范围以加快前期收敛速度，在后期采用 CMEOBL 这一混合策略提高了优化后期的收敛速度及开发能力，从整体上看，大幅提高了 ChO 策略的全局搜索能力，有效改善了局部收敛速度慢的问题，从而提高了分类器的定位检测精度。

在两系统中分别进行了对比实验和消融实验。消融实验结果验证了每项改进措施均具有有效性，对比试验结果证明了本文所提 OBL-ELM^{ChO}-CMEOBL 方法具有更优的全局搜索能力和更高的局部收敛效率，能够在保证分类器特征提取能力的同时，更准确且全面地检测并定位受到攻击的状态量，实现了对 FDIA 更为精准的检测与定位。

参考文献

[1] 席磊, 金澄心, 李彦营, 等. 基于信息松弛的多态能源协调控制方法研究[J]. 电力系统保护与控制, 2023, 51(9): 1-12.
XI Lei, JIN Chengxin, LI Yanying, et al. A polymorphic energy-coordinated control strategy based on information relaxation[J]. Power System Protection and Control, 2023, 51(9): 1-12.

[2] 郑瑶, 张颉, 姚文轩, 等. 基于空间特征的电网同步量测虚假数据注入攻击检测[J]. 电力系统自动化, 2023, 47(10): 128-134.
ZHENG Yao, ZHANG Jie, YAO Wenxuan, et al. Spatial feature based detection of false data injection attack on synchronous grid measurements[J]. Automation of Electric Power Systems, 2023, 47(10): 128-134.

[3] 张晶晶, 吴佳瑜, 齐先军, 等. 基于网络依存关系的 CPPS 连锁故障分析及风险评估[J]. 电力系统保护与控制, 2023, 51(5): 164-171.
ZHANG Jingjing, WU Jiayu, QI Xianjun, et al. Cascading failure analysis and risk assessment of CPPS based on network dependency[J]. Power System Protection and Control, 2023, 51(5): 164-171.

[4] CHEN Biyun, YANG Zhihao, ZHANG Yiyi, et al. Risk assessment of cyber attacks on power grids considering the characteristics of attack behaviors[J]. IEEE Access, 2020, 8: 148331-148344.

[5] 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): 265-276.

[6] 谢云云, 严欣腾, 燕子敖, 等. 面向交直流混联电网的虚假数据注入攻击策略优化[J]. 电力工程技术, 2023, 42(4): 94-101.
XIE Yunyun, YAN Xinteng, YAN Zi'ao, et al. Strategy optimization of false data injection attack on AC-DC hybrid systems[J]. Electric Power Engineering Technology, 2023, 42(4): 94-101.

[7] 李欣, 易柳含, 刘晨凯, 等. 基于数据驱动的电力系统虚假数据注入攻击检测[J]. 智慧电力, 2023, 51(2): 30-37.
LI Xin, YI Liuhan, LIU Chenkai, et al. False data injection attacks detection in power system based on data-driven algorithm[J]. Smart Power, 2023, 51(2): 30-37.

[8] HAO Weijie, YAO Pengchao, YANG Tao, et al. Industrial

cyber-physical system defense resource allocation using distributed anomaly detection[J]. IEEE Internet of Things Journal, 2022, 9(22): 22304-22314.

[9] 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.

[10] WU Yingjun, RU Yingtao, LIN Zhiwei, et al. Research on cyber attacks and defensive measures of power communication network[J]. IEEE Internet of Things Journal, 2023, 10(9): 7613-7635.

[11] 李浩, 张禄亮, 栾云飞, 等. 基于子系统划分和注入电流比的配电网故障定位方法[J]. 电力系统保护与控制, 2023, 51(8): 63-72.
LI Hao, ZHANG Luliang, LUAN Yunfei, et al. Fault location method for a distribution network based on subsystem division and injection current ratio[J]. Power System Protection and Control, 2023, 51(8): 63-72.

[12] JORJANI M, SEIFI H, VARJANI A. 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.

[13] MOSLEMI R, MESBAHI A, VELNI J. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4930-4941.

[14] 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.

[15] KHALAF M, YOUSSEF A, EL-SAADANY E. Joint detection and mitigation of false data injection attacks in AGC systems[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 4985-4995.

[16] CAO Jie, WANG Da, QU Zhaoyang, et al. A novel false data injection attack detection model of the cyber-physical power system[J]. IEEE Access, 2020, 8: 95109-95125.

[17] ESMALIFALAK M, LIU Lanchao, NGUYEN N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2017, 11(3): 1644-1652.

[18] YU JAMES J, HOU Yunhe, LI VICTOR O. Online false data injection attack detection with wavelet transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271-3280.

[19] LUO Jian, LIU Yao, CUI Qiushi, et al. Single-ended time domain fault location based on transient signal measurements of transmission lines[J]. Protection and Control of Modern Power Systems, 2024, 9(2): 61-74.

[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] 席磊, 何苗, 周博奇, 等. 基于改进多隐层极限学习机的电网虚假数据注入攻击检测[J]. 自动化学报, 2023, 49(4): 881-890.
XI Lei, HE Miao, ZHOU Boqi, et al. Research on false data injection attack detection in power system based on improved multi layer extreme learning machine[J]. Acta Automatica Sinica, 2023, 49(4): 881-890.

[22] XIONG Guojiang, XIE Xuan, YUAN Zixia, et al. Differential evolution-based optimized hierarchical extreme learning machines for fault section diagnosis of large-scale power systems[J]. Expert Systems with Applications, 2023, 233.

[23] TIAN Huiyuan, LI Shijian, WU Tianqi, et al. An extreme learning machine based on artificial immune system[J]. Computational Intelligence and Neuroscience, 2018: 3635845.

[24] ZHANG Peng, HUANG Yanping, LI Mengting, et al. Fault diagnosis method of analog circuit based on GA-OS-ELM[C] // 2020 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), 2020: 273-278.

[25] KHISHE M, MOSAVI M. Chimp optimization algorithm[J]. Expert Systems with Applications, 2020, 149: 113338.

[26] 王敏, 唐明珠. 融合对立学习的混合灰狼优化算法[J]. 计算机科学与探索, 2017, 11(4): 673-680.
WANG Min, TANG Mingzhu. Hybrid grey wolf optimization algorithm with opposition-based learning[J]. Journal of Frontiers of Computer Science and Technology, 2017, 11(4): 673-680.

[27] TIZHOOSH H. Opposition-based learning: a new scheme for machine intelligence[C] // International Conference On Computational Intelligence For Modelling, Control And Automation And International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA- IAWTIC'06), 2005, 1: 695-701.

[28] ZHOU Xinyu, WU Zhijian, WANG Hui. Elite opposition-based differential evolution for solving large-scale optimization problems and its implementation on GPU[C]//

2012 13th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2012: 727-732.

[29] 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 improved bald eagle search optimized extreme learning machine[J]. Power System Protection and Control, 2024, 52(1): 156-165.

[30] 解立辉, 席磊. 强化学习在自动发电控制中的研究进展与展望[J]. 三峡大学学报(自然科学版), 2023, 45(5): 133-141.
XIE Lihui, XI Lei. Research progress and prospects of reinforcement learning in automatic generation control[J]. Journal of China Three Gorges University (Natural Science), 2023, 45(5): 133-141.

[31] 李青芯, 孙宏斌, 盛同天, 等. 变电站状态估计中互感器虚假数据注入攻击分析[J]. 电力系统自动化, 2016, 40(17): 79-86.
LI Qingxin, SUN Hongbin, SHENG Tongtian, et al. Injection attack analysis of transformer false data in substation state estimation[J]. Automation of Electric Power Systems, 2016, 40(17): 79-86.

[32] 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.

[33] LIU Yun, GOOI H, LI Yuanzheng, et al. A secure distributed transactive energy management scheme for multiple interconnected microgrids considering mis-behaviors[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 5975-5986.

[34] 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.

[35] SÖNMEZ Y, TUNCER T, GÖKAL H, et al. Phishing web sites features classification based on extreme learning machine[C]// 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018: 1-5.

[36] 席磊, 王艺晓, 何苗, 等. 基于反向鲸鱼-多隐层极限学习机的电网 FDIA 检测[J/OL]. 中国电力: 1-12[2024-04-09]. http://kns.cnki.net/kcms/detail/11.3265.TM.20240205.1356.006.html.
XI Lei, WANG Yixiao, HE Miao, et al. FDIA detection in power grid based on opposition-based whale optimization algorithm and multi-layer extreme learning machine[J/OL]. Electric Power: 1-12[2024-04-09]. http://kns.cnki.net/kcms/detail/11.3265.TM.20240205. 1356.006.html.

[37] 成燕, 庄飞鸯, 徐万万, 等. 基于改进的极限学习机光伏出力短期预测[J]. 现代电力, 2023, 40(5): 679-686.
CHENG Yan, ZHUANG Feiyang, XU Wanwan, et al. Short-term prediction of photovoltaic output based on improved extreme learning machines[J]. Modern Electric Power, 2023, 40(5): 679-686.

[38] AHILA R, SADASIVAM V, MANIMALA K. An integrated PSO for parameter determination and feature selection of ELM and its application in classification of power system disturbances[J]. Applied Soft Computing, 2015, 32: 23-37.

收稿日期：2024-01-08； 修回日期：2024-04-26

作者简介：

席 磊(1982—)，男，教授，博士，博士生导师，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

董 璐(2000—)，女，硕士研究生，研究方向为信息物理系统网络攻击与防御; E-mail: lu15275425765@163.com

李宗泽(2001—)，男，通信作者，硕士研究生，研究方向为信息物理系统网络攻击与防御。E-mail: lizongze0608@163.com

(编辑 许 威)