DOI:10.19651/j.cnki.emt.2416648

基于冠状病毒群体免疫算法的工控入侵检测*

王浩楠 兰艳亭 方 炜
(中北大学电气与控制工程学院 太原 030000)

摘 要:工业 4.0 改革使工业化与信息化进程不断交叉深入,工业控制系统(ICS)数据的非线性、高维度等特点使传统入侵检测方法不再适用。设计了一种基于冠状病毒群体免疫算法(CHIO)的工控入侵检测模型,将 Fisher-Score 与核主成分分析(KPCA)结合,对数据进行特征提取,有效降低了数据复杂度,通过引入自适应与差分进化策略改进了冠状病毒免疫算法,增强了算法的搜索性能。最后将改进后的算法应用到支持向量机(SVM)模型进行参数寻优,使用密西西比大学天然气管道数据集进行了仿真实验。实验结果表明:改进后的模型在检测准确率及检测速度上与传统模型相比都具有较大优势,检测率可达 97.1%。

关键词:工业控制系统;冠状病毒群体免疫算法;支持向量机;差分进化;核主成分分析
中图分类号:TP309;TN802 **文献标识码**:A **国家标准学科分类代码**:520.6020

Intrusion detection for industrial control system based on coronavirus herd immunity optimizer algorithm

Wang Haonan Lan Yanting Fang Wei
(School of Electrical and Control Engineering, North University of China, Taiyuan 030000, China)

Abstract: Industrial 4.0 revolution has led to a deeper integration of industrialization and digitalization, resulting in industrial control systems (ICS) characterized by nonlinear and high-dimensional data. These complexities render traditional intrusion detection methods ineffective. In this study, we propose an intrusion detection model for ICS based on the coronavirus herd immunity optimizer (CHIO). The model leverages Fisher-Score and kernel principal component analysis (KPCA) for feature extraction, effectively reducing the complexity of the data. To enhance the search performance of the CHIO, adaptive mechanisms and differential evolution strategies are incorporated. The improved algorithm is then applied to a support vector machine (SVM) for parameter optimization. The performance of the model is validated using the natural gas pipeline dataset from the University of Mississippi. Experimental results demonstrate that the proposed model offers significant improvements in both detection accuracy and speed compared to traditional methods, achieving a detection rate of 97.1%.

Keywords: industry control system; coronavirus herd immunity optimizer; support vector machine; differential evolution; kernel principal component analysis

0 引 言

传统工业控制系统(industrial control system, ICS)在工业生产中负责控制和协调各种设备按照要求执行各种任务。工业 4.0 的到来伴随着工业设备的升级,工业控制系统具有的实时性高,计算资源有限,升级困难等特点给入侵检测带来了一定的困难,准确率与检测时间都无法保证[1]。

目前研究人员针对不同工控系统提出了多种入侵检测方法,按照检测方法可分为误用入侵检测和异常入侵检测[2]。误用入侵检测是通过建立一个攻击行为特征库,将监控到的行为与这些特征进行匹配来识别入侵行为。严彪等[3]从网络实体、工控操作以及工控操作流程 3 个方面分别建立白名单规则,然后结合对应的算法进行入侵检测。冯剑等[4]提出一种为工控网络流量建立 1 个时间序列模型并结合样本熵进行入侵检测的检测算法。吕峰等[5]提出一种基于动态防御策略的石油石化工控网络安全防护框架,能够实时感知并阻断多种工控网络威胁。然而,由于依赖已知攻击模式,误用检测无法有效应对未知的新攻击方式,

收稿日期:2024-08-10
* 基金项目:山西省科技重大专项计划"揭榜挂帅"项目(202101010101017)资助

且容易产生误报。

异常入侵检测则是基于系统正常运行模式的偏差来进行检测的方法。在异常检测方法中机器学习由于其无需先验知识,可直接在模型中学习的优势成为了工业控制系统入侵检测的研究热点。Rajesh 等[6]将合成少数类采样技术(synthetic minority oversampling technique, SMOTE)与支持向量机(support vector machine,SVM)结合,提出了一种新的 SVM-SMOTE 方法来对数据采集及监视(supervisory control and data acquisition,SCADA)系统进行入侵检测并取得了良好的效果,由于未对数据进行特征提取,导致检测时间较长。Zhou 等[7]为提高工业机械臂系统的安全性提出了一种基于粒子群算法(particle swarm optimization algorithm, PSO)的 PSO-H-SVM 实时入侵检测系统,系统能及时处理攻击,然而这导致硬件资源要求较高且检测准确率较低。张子迎等[8]在处理数据集时在核主成分分析(kernel principal component analysis, KPCA)过程中加入 Fisher-Score 算法,实验表明使用降维后的数据集有效提高了向量机效率,但使用的改进算法复杂导致检测时间较长。王华忠等[9]提出一种改进的鲸鱼算法(improved whale algorithm, IWOA)来优化 SVM 入侵检测模型的参数,模型检测正确率明显提高,由于未对数据集进行降维导致面对高维度的工控数据集时检测速度较慢。赵志达等[10]改进了麻雀算法(improved sparrow search algorithm, ISSA)对梯度提升框架(light gradient boosting machine, LightGBM)入侵检测模型进行参数优化,验证了该方法在处理大量工业数据时有较大优势,然而算法的收敛速度一般。

上述研究中使用的算法对支持向量机的核函数和惩罚参数[11]寻优时,限于算法结构较为复杂,寻优时间通常较长,收敛速度较慢,面对高维的工控数据时模型检测时间会大幅增加。本文的冠状病毒群体免疫算法[12-13](coronavirus herd immunity optimizer, CHIO)与传统算法相比,CHIO 算法结构简单,参数少,搜索速度较快[14],其在路径规划[15],电力系统参数优化[16],医学特征选择[17],复杂电网构建[18]等领域都有学者研究应用。但 CHIO 算法的搜索性能主要依靠繁殖参数 BRr 和社交距离 r,由于算法的 BRr 是固定参数,这导致算法收敛速度慢,易陷入局部最优,搜索性能不佳。

本文将核主成分分析法与 Fisher-Score 算法结合预先对工控数据进行有效降维,利用自适应与差分进化策略改进算法性能,使用改进后的算法对 SVM 的参数进行寻优,建立了基于冠状病毒群体免疫的工控入侵检测模型。结果表明新的检测模型具有更好的性能指标,能够满足 ICS 对实时性,准确性的要求。

1 冠状病毒群体免疫算法的改进

1.1 冠状病毒群体免疫算法

在全球疫情肆虐期间,Mohammed Azmi Al-Betar 受到新冠病毒传播方式的启发,于 2021 年提出了一种新的优化算法,即冠状病毒群体免疫算法。

该算法是对病毒在群体中传播的模拟,将个体按照距离划分为了"易感""感染""免疫"3 种不同状态,分别采取不同的交叉变异方法,算法的群体免疫思想如图 1 所示。CHIO 循环结构主要有 6 个步骤:

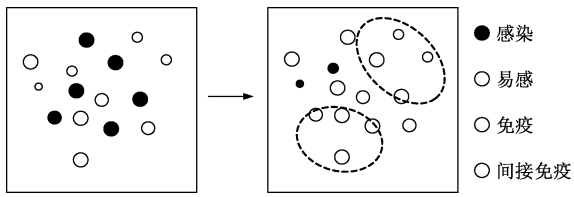

图 1 群体免疫概念

Fig. 1 Illustration of herd immunity

步骤 1)初始化参数

C_0:最初感染个体数,初始设置为 1;

Max_Itr:最大迭代数,作为迭代过程的结束判据;

HIS:种群大小;

n:目标问题的维度;

BRr:基本繁殖参数,其控制病毒的传播速度;

Max_age:最高患病年龄,一旦个体感染且达到最大寿命时,个体只有两种状态要么痊愈要么死亡。

步骤 2)产生初始种群

生成一个 $HIS \times n$ 的种群矩阵:

$$\boldsymbol{HIP} = \begin{bmatrix} x_1^1 & x_2^1 & \cdots & x_n^1 \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{HIS} & x_2^{HIS} & \cdots & x_n^{HIS} \end{bmatrix}$$

目标函数表达形式为:

$$\min_x f(x)\, x \in [lb, ub] \tag{1}$$

个体随机产生公式为:$x_i^j = lb_i + (ub_i - lb_i) \times U(0,1), \forall i = 1,2,\cdots n$. 同时每个个体用状态矢量 S 来标记状态,0 为易感,1 为感染,2 为免疫。

步骤 3)群体免疫进化

第 j 个个体 x^j 的基因 x_i^j 更新原则如式(2),其根据社交距离 $r(r \in rand(0,1))$决定:

$$x_i^j(t+1) = \begin{cases} C(x_i^j(t)) = x_i^j(t) + r \times (x_i^j(t) - x_i^C(t)), \\ r \in [0, \dfrac{1}{3}BR_r) \\ N(x_i^j(t)) = x_i^j(t) + r \times (x_i^j(t) - x_i^N(t)), \\ r \in [\dfrac{1}{3}BR_r, \dfrac{2}{3}BR_r) \\ R(x_i^j(t)) = x_i^j(t) + r \times (x_i^j(t) - x_i^R(t)), \\ r \in [\dfrac{2}{3}BR_r, BR_r) \end{cases} \tag{2}$$

步骤 4)更新群体免疫种群

通过更新后的个体 $x^j(t+1)$ 计算免疫率(即适应度值) $f(x^j(t+1))$，若适应度更优(比如：$f(x^j(t+1)) < f(x^j(t))$)，此时若 $S=1$，则年龄矢量 A 对应的 A_j 就加 1。

状态矢量 S 的更新规则：

$$S_j \leftarrow \begin{cases} 1, f(x^j(t+1)) < \dfrac{f(x)^j(t+1)}{\Delta f(x)} \wedge S_j = 0 \wedge \\ is\_Corona(x^j(t+1)) \\ 2, f(x^j(t+1)) > \dfrac{f(x)^j(t+1)}{\Delta f(x)} \wedge S_j = 1 \end{cases} \tag{3}$$

在式(3)中，当新个体 $x^j(t+1)$ 变为被感染状态时，$is\_Corona(x^j(t+1))$ 的数值变为 1。$\Delta f(x)$ 是免疫率(适应度)的平均值比如 $\dfrac{\sum_{i=1}^{HIS} f(x_i)}{HIS}$。

步骤 5)感染个体的死亡

在最大迭代次数(Max_Itr)内，已感染个体的免疫率($f(x^j(t+1))$)达到年龄上限(Max_age)无法更新，此时判断此个体死亡。为避免算法陷入局部最优，以公式 $x_i^j = lb_i + (ub_i - lb_i) \times U(0,1), \forall i = 1,2,\cdots n.$ 为规则重新生成个体，x^j 的状态矢量 A_j 和 S_j 都置 0。

步骤 6)判断终止

重复步骤 3)～6)，直到达到最大迭代次数。

1.2　自适应差分冠状病毒群体免疫算法

本文提出的自适应差分冠状病毒群体免疫算法(adaptive differential evolution coronavirus herd immunity optimizer，AEDCHIO)引入协方差矩阵的最大特征值来对 BRr 进行动态调整，可有效增强算法的搜索能力。由于群体免疫进化规则较为单一，搜索效果一般，利用采用差分进化策略增强种群搜索能力，使种群进化更加高效，寻优效果更好。

1)动态 BRr 调整策略

种群中每个个体 x_i 为一个 n 维向量，种群大小为 HIS，种群矩阵为 $\boldsymbol{X} \in \mathbb{R}^{HIS \times n}$。首先计算种群矩阵的协方差矩阵：

$$\sum = \frac{1}{HIS-1}(X-\boldsymbol{\mu})^{\mathrm{T}}(X-\mu) \tag{4}$$

其中，$\boldsymbol{\mu}$ 是种群的均值向量：$\boldsymbol{\mu} = \dfrac{\sum_{i=1}^{HIS} x_i}{HIS}$

由于协方差矩阵的特征值和特征向量可以反映种群各个方向上的分布情况，故使用最大的特征值 $\lambda_{\max}$ 来衡量种群多样性，越大的特征值代表种群多样性越高：

$$\lambda_{\max} = \max(eig(\sum)) \tag{5}$$

根据动态参数控制理论[19]，动态 BRr 的调整公式可写为：

$$BRr(t+1) = BRr(t) \times (1 + \alpha \cdot \frac{\lambda_{\max}(t) - \theta}{\theta}) \tag{6}$$

其中，t 为当前迭代次数。α 控制 BRr 的变化速度，较大的 α 使 BRr 能更快调整，较小的 α 则使 BRr 变化更平滑。θ 是多样性阈值，可用于判断种群多样性是否足够高。当 $\lambda_{\max} > \theta$ 时，BRr 变大，算法增加全局搜索性能。$\lambda_{\max} < \theta$ 时，BRr 变小，算法寻求局部最优。

2)个体差分进化

在群体免疫策略基础上，利用差分进化理论[20]提升算法的寻优能力。其中主要操作为个体的变异，交叉及选择。

变异：对每个个体 x_i，在种群中使用 3 个随机选择的不同个体 x_{r1}, x_{r2}, x_{r3} 生成变异个体 v_i：

$$v_i = x_{r1} + F \cdot (x_{r2} - x_{r3}) \tag{7}$$

其中，F 为变异因子，其表达式为：$F = 0.5 + rand(0,1) \times 0.2$

交叉：使用交叉率 p 结合目标个体 x_i 与变异个体 v_i 构造新个体 u_i：

$$u_{i,j} = \begin{cases} v_{i,j}, & if\ rand(0,1) \leqslant p\ or\ j = j_{rand} \\ x_{i,j}, & \text{其他} \end{cases} \tag{8}$$

其中，j_{rand} 是[1，n]中的随机整数。交叉率 p 的表达式为：$p = 0.9 - rand(0,1) \times 0.1$

选择：若新个体 u_i 的适应度值优于个体 x_i，则接受新个体：

$$x_i = \begin{cases} u_i, & f(u_i) < f(x_i) \\ x_i, & \text{其他} \end{cases} \tag{9}$$

1.3　算法性能测试

为全面评估改进后算法的性能，选取了 4 个经典函数，其中 Levy N. 13 及 Ackley 为多局部最小函数，Rosenbrock 及 Dixon-Price 为谷形函数，函数的表达式，变量个数及变量范围如表 1 所示。

为确保算法的可靠性，将 ADECHIO 与 CHIO 和免疫算法[21](immune algorithm，IA)进行比较，种群大小设置为 100，维度设置为 30，最大迭代次数为 500，进行 100 次实验并取平均值，得到算法的平均收敛曲线图如图 2～5 所示。

从图 2～5 可以看出，改进后的算法虽然在初期寻优能力一般，但随着迭代次数增加，算法可跳出局部最优解并有效克服了算法早熟的问题。且自适应策略平衡了算法的全局与局部的搜索，使算法更加稳定。

2　ADECHIO-SVM 入侵检测模型

ADECHIO-SVM 入侵检测模型构建的算法流程如图 6 所示。

模型可分为 3 个部分：

1)数据预处理：

采用 Fisher-Score[8]对数据集进行特征选择构建新的特征子集，使用 KPCA 方法对筛选出的特征子集作降维处理。将降维后的数据集划分为训练集与测试集，为了降低数据间的影响，故使用归一化方法 $\hat{x} = (x - x_{\min})/(x_{\max} - x_{\min})$ 将数据集中在[0，1]上。

表 1 测试基准函数

Table 1 Test bench functions

函数名	函数表达式	变量	范围
Levi N. 13	$f(x)=\sin^2(3\pi x_1)+(x_1-1)^2[1+\sin^2(3\pi x_2)]+(x_2-1)^2[1+\sin^2(2\pi x_2)]$	30	$[-10,10]$
Ackley	$f(x)=-20\cdot\exp(-0.2\cdot\sqrt{\frac{1}{n}\sum_{i=1}^{n}x_i^2})-\exp(\frac{1}{n}\sum_{i=1}^{n}\cos(2\pi x_i))+20+\exp(1)$	30	$[-32,32]$
Rosenbrock	$f(x)=\sum_{i=1}^{n-1}[100(x_{i+1}-x_i^2)^2+(x_i-1)^2]$	30	$[-30,30]$
Dixon-Price	$f(x)=(x_1-1)^2+\sum_{i=2}^{n}i(2x_i^2-x_{i-1})^2$	30	$[-10,10]$

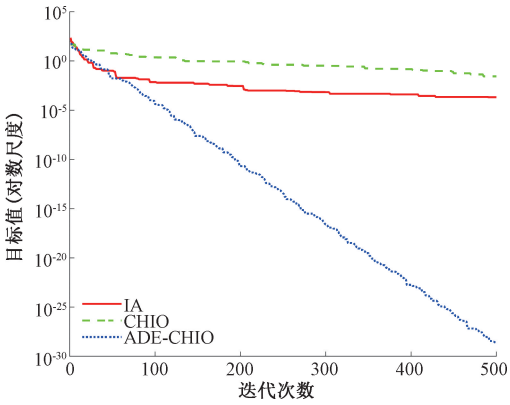

图 2 Levi 函数收敛曲线

Fig. 2 The convergence curve of the Levi function

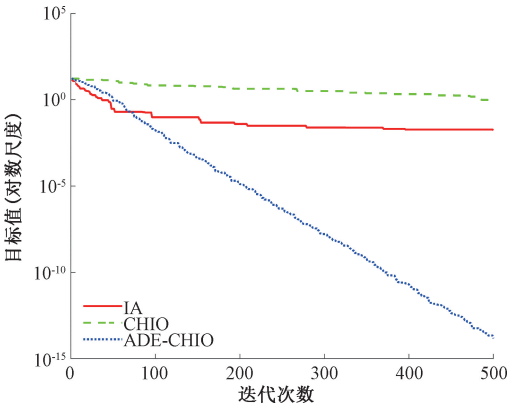

图 3 Ackley 函数收敛曲线

Fig. 3 The convergence curve of the Ackley function

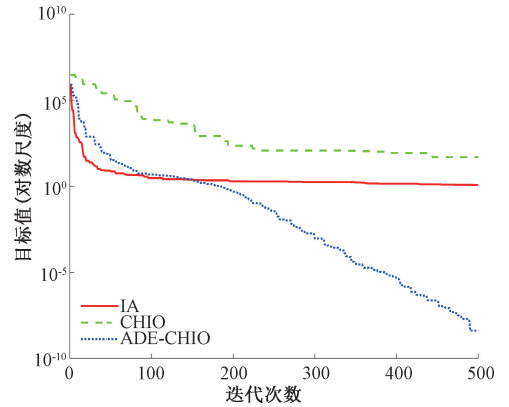

图 4 Rosenbrock 函数收敛曲线

Fig. 4 The convergence curve of the Rosenbrock function

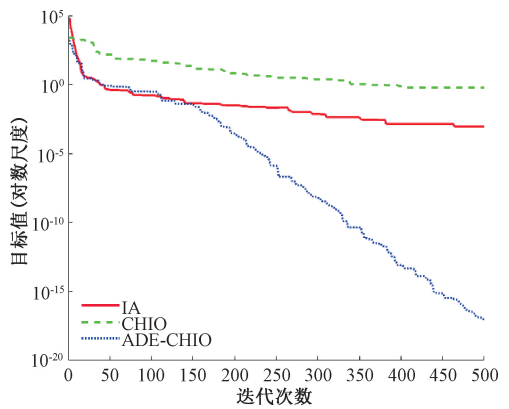

图 5 Dixon-price 函数收敛曲线

Fig. 5 The convergence curve of the Dixon-price function

2)建立检测模型:

初始化免疫种群,利用免疫个体传递的参数 g 和 C 构造 SVM 模型并训练,由于涉及多分类问题,故采用一对一(one versus one, OVO)方法构建 $k(k-1)/2$ 个分类器,使用投票法实现工控入侵检测的多分类。

将返回的模型入侵检测准确率的相反数作为适应度值,按照算法更新规则对种群进行更新,达到迭代上限后返回最优参数构建入侵检测模型。

3)模型验证:

将构建好的入侵检测模型对之前划分好的训练集进行检测,通过准确率、误报率、漏报率及检测时间评估该模型的入侵检测效果。

3 仿真实验

3.1 数据集预处理

本文使用的数据集是由密西西比州立大学基础设施

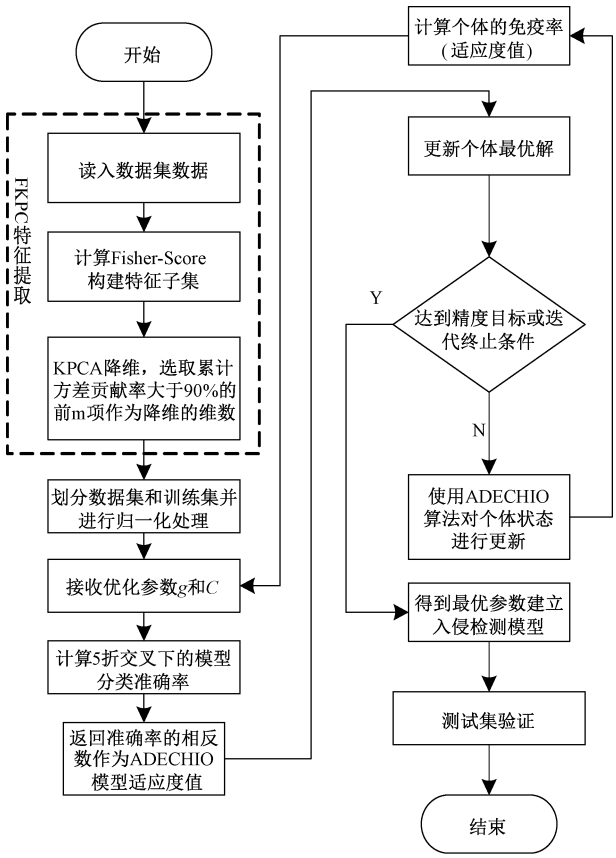

图 6　FKPCA-ADECHIO-SVM 算法流程

Fig. 6　The flow of the FKPCA-ADECHIO-SVM algorithm

保护中心于 2014 年建立的工控入侵检测标准数据集。数据集中包含 26 个特征和 1 个标签值[22]。攻击形式与分类标签如表 2 所示。

表 2　攻击形式及仿真分类标签

Table 2　Attack modalities and simulated classification labels

标签值	类别	量值
0	Normal	正常数据
1	NMRI	简单的恶意响应注入攻击
2	CMRI	复杂的恶意响应注入攻击
3	MSCI	恶意状态命令注入攻击
4	MPCI	恶意参数命令注入攻击
5	MFCI	恶意功能命令注入攻击
6	DoS	拒绝服务攻击
7	RECO	侦察攻击

在数据集中随机选取 1 000 条包含正常及异常的样本作为样本集，计算每个特征的 Fisher-Score 并降序排列综合选取需要的特征子集的维数。如图 7 所示，当添加第 14 个特征时，综合贡献度达到了最高值，此时入侵检测模型的性能最好。

经特征选择后，对新特征子集进行 KPCA 降维，降维后结果如图 8 所示，以累计贡献率大于 90% 为标准选择前 8 维组成新的数据集。

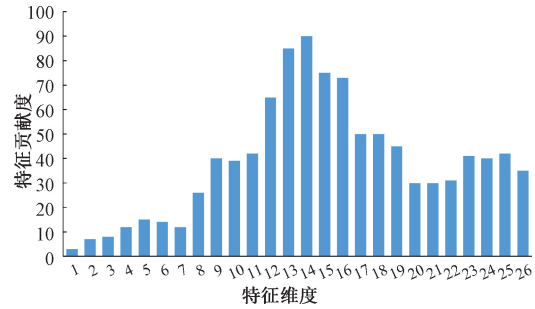

图 7　特征综合贡献度变化曲线

Fig. 7　Variation curve of feature comprehensive contribution

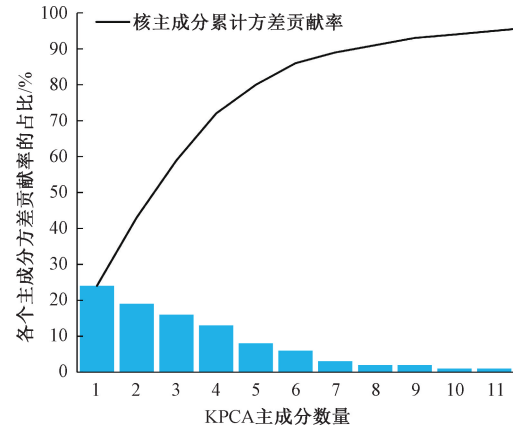

图 8　KPCA 降维结果

Fig. 8　KPCA dimensionality reduction results

从表 3 可看出，将 FKPCA 与 SVM 结合后模型的检测时间大幅缩短，准确率也提升了 6.7%，验证了 FKPCA 算法的有效性。

表 3　特征提取检测结果对比

Table 3　Comparison of feature extraction detection results

特征提取方法	准确率/%	精确率/%	检测时间/s
SVM	82.32	84.45	293.12
PCA-SVM	85.42	85.22	252.54
KPCA-SVM	87.57	86.23	224.89
FKPCA-SVM	89.02	89.10	202.78

3.2　算例仿真

1）参数设置

文中所有算法使用 MATLAB 实现，实验在 Intel(R) Core(TM) i7-8565U CPU @ 1.80 GHz，8 G 内存，matlab2021b 上实现。从数据集中抽取 800 组数据作为训练集，400 组数据作为测试集，测试集中每种标签测试 50 个数据。

算法的种群大小设置为 100，维数设置为 2，最大迭代

次数为 100,最大年龄设为 100,初始传播率 BRr 设置为 0.01 时寻优效果好[12],α 取 0.1,θ 取 1.1。SVM 分类模型的惩罚参数 C 和内核参数 g 采用实数编码且寻优范围都为[0.01,100]。

2) 仿真结果分析

(1)训练效果分析

在训练过程中,本文比较了改进鲸鱼算法[9],免疫算法[21],改进麻雀算法[10]及 CHIO 对 SVM 优化参数的效果,经过实验,得到了各个优化 SVM 训练过程的训练精度与迭代次数关系曲线。得到如图 9 的迭代效果图。

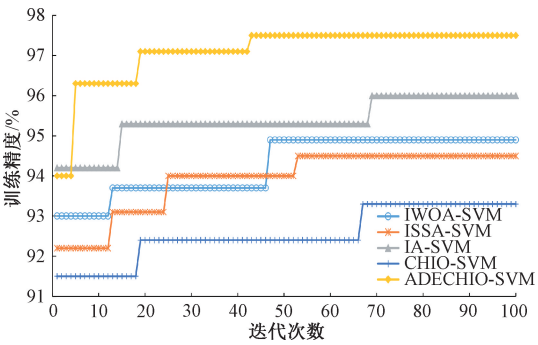

图 9　不同算法优化 SVM 的准确率对比

Fig. 9　Comparison of training accuracy of SVM optimized by different algorithms

由图 9 可知,从优化精度来看,ADECHIO 的准确率最高,虽然 IA 算法初期搜索效果较好,但随着迭代次数增加,本文的改进算法训练精度更高。从收敛速度看,改进后的 CHIO 算法在迭代至 43 代时已经基本收敛,收敛速度略快于 IWOA 及 ISSA,明显快于 IA 及 CHIO 算法。对比 CHIO 算法可以看到,CHIO 算法收敛慢,寻优能力较差的问题得到明显改善。

(2)总体检测效果对比

本文采用准确率、误报率、漏报率及检测时间[23]作为入侵检测评价标准,使用各个算法模型对数据集进行了检测,测试 200 次取平均值,得到的检测结果如表 4 所示。

表 4　各优化算法入侵检测对比

Table 4　Comparison of intrusion detection results of various optimization algorithms

算法	准确率/%	误报率/%	漏报率/%	检测时间/s
IWOA-SVM	94.92	2.92	1.87	193.18
IA-SVM	95.76	2.46	1.62	230.65
ISSA-SVM	94.58	1.87	1.23	189.67
CHIO-SVM	93.32	3.74	1.65	146.82
ADECHIO-SVM	97.1	1.44	0.51	152.72

从表 4 可知,使用 AEDCHIO 算法优化的 SVM 入侵检测模型对测试集效果最好,虽然比 CHIO 算法慢 5.9 s,但其准确率可达 97.1%,而 IA 算法在准确度上虽然与本文算法接近,但检测时间过长。且改进后的算法在误报率及漏报率上明显优于其他算法。而 CHIO 算法虽然检测时间最短,但准确度却低于其他算法。

(3)各种攻击类别检测效果对比

密西西比大学的数据集中包含 8 种状态,使用 ADECHIO-SVM 对每种攻击形式(包括正常状态)进行识别。图 10 是各个算法对攻击形式的检测效果。

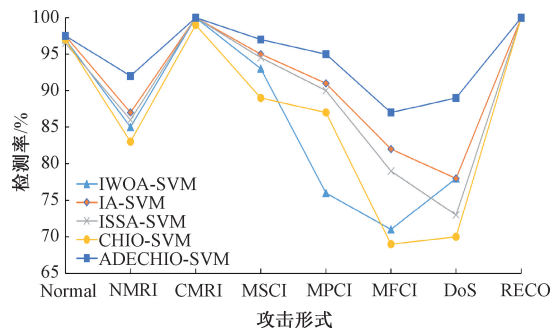

图 10　不同攻击形式的检测效果对比

Fig. 10　Comparison of detection effects of different attack forms

从图 10 可以看出,使用改进后的冠状病毒群体免疫算法在每种攻击上都有较好的检测效果,尤其是对 NMRI、MPCI、MFCI 和 Dos 的检测效果明显好于经过 IWOA、IA、ISSA 和 CHIO 优化过的 SVM 检测模型。同时也可从图中知道各个算法对 CMRI 和 RECO 都有着接近 100%的检测率。

同时为了更好地观察 ADECHIO-SVM 模型对每种攻击的预测结果,绘制了真实值和预测值的对比图,如图 11 所示。

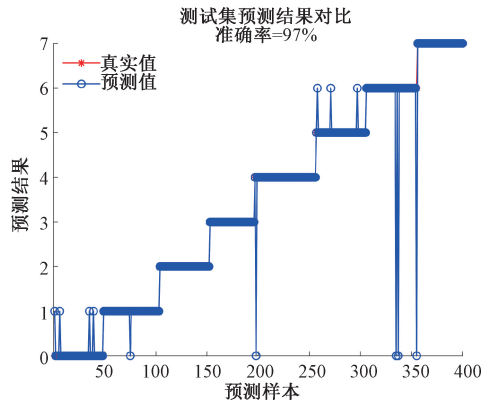

图 11　测试集仿真结果

Fig. 11　Simulation results on the test dataset

图 11 可以观察到一次测试集的分类预测的具体情况,其预测效果基本与图 7 对应,本次分类预测对所有攻击都有较高的识别率,其中对 NMRI(标签 2)、CMRI(标签 3)及 RECO(标签 7)的预测更是达到了 100%。

4　结　　论

本文在对工控数据集进行有效降维后，在 CHIO 算法的基础上引入自适应及差分进化策略，有效提高了算法的搜索能力。实验结果表明，改进后的算法提高了 SVM 模型的分类能力，检测速度和准确率都有明显优势，优化参数后的入侵检测模型面对非线性，高维度的工控数据，能够快速准确地检测入侵，满足了工业控制系统入侵检测的需求。

参考文献

[1] 马标，金映言，那幸仪，等. 工业控制系统入侵检测技术研究综述[J]. 计算机应用与软件，2023，40(5)：10-18，43.
MA B，JIN Y Y，NA X Y，et al. A summary of research on industrial control system intrusion detection technology[J]. Computer Applications and Software，2023，40(5)：10-18，43.

[2] 金忠峰，李楠，刘超，等. 工业控制系统入侵检测技术研究综述[J]. 保密科学技术，2018(3)：18-25.
JIN ZH F，LI N，LIU CH，et al. A survey of intrusion detection techniques for industrial control systems[J]. Journal of Security and Technology，2018(3)：18-25.

[3] 严彪，尹丽波，应欢，等. 基于白名单机制的工控分级入侵检测算法[J]. 通信技术，2018，51(4)：907-912.
YAN B，YIN L B，YING H，et al. Hierarchical intrusion detection algorithm based on white list for industrial control network[J]. Communications Technology，2018，51(4)：907-912.

[4] 冯剑，朱峰，周康韵，等. 基于 OPC UA 和样本熵的工业入侵检测算法研究[J]. 自动化仪表，2023，44(5)：29-36，41.
FENG J，ZHU F，ZHOU K Y，et al. Research on industrial intrusion detection algorithm based on OPC UA and sample entropy[J]. Automation Instrumentation，2023，44(5)：29-36，41.

[5] 吕峰，黄河，姜亚光，等. 基于动态防御策略的石油石化工控网络安全防护方法[J]. 数字技术与应用，2023，41(7)：212-215.
LYU F，HUANG H，JIANG Y G，et al. A network security protection method for petrochemical industrial control systems based on dynamic defense strategy[J]. Digital Technology and Application，2023，41(7)：212-215.

[6] RAJESH L，PENKE S. Evaluation of machine learning algorithms for detection of malicious traffic in SCADA network[J]. Journal of Electrical Engineering & Technology，2022，17(2)：913-928.

[7] ZHOU Y L，XIE L，PAN H. Research on a PSO-H-SVM-based intrusion detection method for industrial robotic arms[J]. Applied Sciences，2022，12(6)：2765.

[8] 张子迎，潘思辰，王宇华. 基于单类支持向量机的工业控制系统入侵检测[J]. 哈尔滨工程大学学报，2022，43(7)：1043-1050.
ZHANG Z Y，PAN S CH，WANG Y H. Research on ICS intrusion detection methods based on one class support vector machine[J]. Journal of Harbin Engineering University，2022，43(7)：1043-1050.

[9] 王华忠，程奇. 基于改进鲸鱼算法的工控系统入侵检测研究[J]. 信息网络安全，2021，21(2)：53-60.
WANG H ZH，CHENG Q. Research on intrusion detection of industrial control system based on improved whale algorithm[J]. Information Network Security，2021，21(2)：53-60.

[10] 赵志达，王华忠. 基于 ISSA-LightGBM 的工控入侵检测研究[J]. 华东理工大学学报(自然科学版)，2023，49(5)：735-743.
ZHAO ZH D，WANG H ZH. Research on industrial control system intrusion detection based on ISSA-LightGBM[J]. Journal of East China University of Science and Technology(Natural Science Edition)，2023，49(5)：735-743.

[11] 陈剑，杨惠杰，季磊，等. 基于 AOA 优化 SVM 的轴承故障诊断方法研究[J]. 电子测量技术，2023，46(15)：165-169.
CHEN J，YANG H J，JI L，et al. Method of bearing fault diagnosis based on SVM optimized by AOA algorithm[J]. Electronic Measurement Technology，2023，46(15)：165-169.

[12] Al-BETAR M A，ALYASSERI Z A A，AWADALLAH M A，et al. Coronavirus herd immunity optimizer(CHIO)[J]. Neural Computing and Applications，2021，33(10)：5011-5042.

[13] 武晓朦，袁榕泽，李英量，等. 基于新冠病毒群体免疫算法的有源配电网优化调度[J]. 系统仿真学报，2023，35(12)：2692-2702.
WU X M，YUAN R Z，LI Y L，et al. Optimized scheduling of distribution network with distributed generation based on coronavirus herd immunity optimizer algorithm[J]. Journal of System Simulation，2023，35(12)：2692-2702.

[14] DALBAH L M，Al-BETAR M A，AWADALLAH M A，et al. A coronavirus herd immunity optimization(CHIO) for travelling salesman problem[C]. International Conference on Innovative Computing and Communications，2022：717-729.

[15] DALBAH L M, AL-BETAR M A, AWADALLAH M A, et al. A modified coronavirus herd immunity optimizer for capacitated vehicle routing problem[J]. Journal of King Saud University-Computer and Information Sciences,2022,34(8):4782-4795.

[16] RANI N, MALAKAR T. Assessment of effective reactive power reserve in power system networks under uncertainty applying coronavirus herd immunity optimizer(CHIO) for operation simulation[J]. Electric Power Systems Research,2023,220:109267.

[17] ALWESHAH M, ALKHALAILEH S, AL-BETAR M A, et al. Coronavirus herd immunity optimizer-with greedy crossover for feature selection in medical diagnosis[J]. Knowledge-Based Systems, 2021, 235: 1-19.

[18] NADERIPOUR A, ABDULLAH A, MARZBALI M H, et al. An improved corona-virus herd immunity optimizer algorithm for network reconfiguration based on fuzzy multi-criteria approach[J]. Expert Systems with Applications,2022,187:115914.

[19] ZHANG H T, SUN J Y, TAN K CH, et al. Learning adaptive differential evolution by natural evolution strategies [J]. IEEE Transactions on Emerging Topics in Computational Intelligence,2022, 7(3):872-886.

[20] SONG Y J, CAI X B, ZHOU X, et al. Dynamic hybrid mechanism-based differential evolution algorithm and its application[J]. Expert Systems with Applications,2023,213:118834.

[21] 李耀. 基于 IA-SVM 的电力工控系统流量异常检测技术研究[D]. 长沙:湖南大学,2022.
LI Y. Research on traffic abnormality detection technology for electric power industrial control system based on IA-SVM[D]. Changsha:Hunan University,2022.

[22] 陈冬青,张普含,王华忠. 基于 MIKPSO-SVM 方法的工业控制系统入侵检测[J]. 清华大学学报(自然科学版),2018,58(4):380-386.
CHEN D Q, ZHANG P H, WANG H ZH. Intrusion detection for industrial control systems based on an improved SVM method [J]. Journal of Tsinghua University(Science and Technology),2018,58(4):380-386.

[23] 胡聪,徐敏,洪德华,等. 基于改进 K-medoids 聚类和 SVM 的异常用电模式在线检测方法[J]. 国外电子测量技术,2022,41(2):53-59.
HU C, XU M, HONG D H, et al. Online detection method for abnormal electricity model behavior based on improved K-medoids clustering and SVM [J]. Foreign Electronic Measurement Technology, 2022, 41(2): 53-59.

作者简介

王浩楠,硕士研究生,主要研究方向为工业控制系统信息安全。

E-mail: S202215020@st.nuc.edu.cn

兰艳亭(通信作者),副教授,硕士生导师,主要研究方向为智能控制与数据融合。

E-mail: lytcyb@foxmail.com

方炜,副教授,主要研究方向为工业控制系统及智能控制。

E-mail: fangwei@nuc.edu.cn