DOI:10.19651/j.cnki.emt.2210098

基于互信息和 GWB-LSSVM 的网络攻击检测模型*

赵 嘉 谷 良 吴 瑶
(国网山西省电力公司信息通信分公司 太原 030000)

摘 要: 检测和识别网络攻击对于防范高级可持续威胁等网络攻击行为、促进网络基础设施健康发展,保障网络设施安全稳定运行至关重要。本文利用互信息理论完成了网络流量数据中网络攻击行为的关键特征的选取,通过改进灰狼优化算法提出一种灰狼提升算法,并基于该算法和最小二乘支持向量机提出了 GWB-LSSVM 模型,该模型针对当前主要网络攻击形式显示出良好的检测性能,基于 NSL-KDD 数据集的实验结果表明其检测精度、检测率和检测准确率分别达到了 99.7%、99.3%和 99.1%;同部分已有研究工作相比,其检测精度最高提升约 2.58%,检测率最高提升约 3.98%,准确率最高提升约 3.78%,训练时间最高提升约 55.9%。

关键词: 攻击检测;灰狼提升算法;特征选择;互信息理论;最小二乘支持向量机
中图分类号: TP393.0 **文献标识码:** A **国家标准学科分类代码:** 520.3

Network attack detection model based on MI-GWB-LSSVM

Zhao Jia Gu Liang Wu Yao
(Information and Communications Branch, State Grid Shanxi Electric Power Company, Taiyuan 030000, China)

Abstract: Detecting and identifying cyber attacks is crucial to prevent cyber attacks such as advanced sustainable threats, promote the healthy development of network infrastructure, and guarantee the safe and stable operation of network facilities. In this paper, the key characteristics of network attacks in network traffic data are selected by using mutual information theory, a gray wolf boosting algorithm is proposed by improving the gray wolf optimization algorithm, and a GWB-LSSVM model is provided based on this algorithm and least squares support vector machine. The model shows good detection performance for the current main forms of network attacks. The experimental results based on NSL-KDD data set show that its detection precision, detection rate and detection accuracy reached 99.7%, 99.3% and 99.1% respectively. Compared with some existing research work, its detection precision is improved by up to about 2.58%, detection rate by up to about 3.98%, detection accuracy by up to about 3.78%, and the training time of the model by up to 55.9%.

Keywords: attack detection; gray wolf boosting algorithm; feature selection; mutual information theory; least squares support vector machine

0 引 言

网络是保障社会有序运转不可或缺的基础设施,如电力[1]、交通[2]等,尤其在新冠肺炎疫情冲击背景下,更加凸显网络在社会生活中无可替代的作用。然而,网络架构的开放性和其难以根治的系统漏洞使网络用户面临着严峻的安全挑战,如 DoS(denial-of-service)攻击不仅可以在短时间内瘫痪目标网络[3],更甚者如高级可持续威胁(advanced sustainable threats,APT)利用 probe、U2R(user-to-root)和 R2L(remote-to-local)等手段通过规避网络入侵检测系统检查进入目标网络长期隐藏,并伺机通过横向移动等手段在目标网络内窃取机密数据,给目标造成难以察觉的巨大损失。通常,APT 等攻击的主要目标是电力供应、能源、金融、政务、科研机构和教育系统等,给相应企业、政府及社会系统带来极大的网络安全威胁。

构建高灵敏度的网络入侵检测系统是预防包括 APT 等在内的网络攻击行为的主要手段。围绕入侵检测系统目前已有许多的科学研究,梳理当前的研究主要分为两类:基于传统机器学习的入侵检测方法和基于深度学习的入侵检测方法。基于机器学习的入侵检测方法研究主要包括:针

收稿日期:2022-05-24
* 基金项目:国网山西省电力公司科技项目(52051C21000G)资助

对 DoS 变种 LDoS 攻击模式,Tang 等[4]提出一种基于梯度提升决策树和逻辑回归模型(GBDT-LR)的针对 LDoS 攻击检测方法,该方法通过分析攻击环境下正常流量特征,基于 GBDT-LR 模型实现对正常和恶意流量的分类,但无法实现多种恶意攻击条件下的精确分类。Mohammad 等[5]利用 DBSCAN、Farnaaz 等[6]利用 random forest,Thaseen[7]利用 support vector machine 分别针对 DDoS 攻击进行了研究,然而上述研究并未验证其对其它攻击形式的检测性能。基于深度学习的入侵检测方法研究主要包括:针对 DDoS 攻击,Robsonv 等[8]提出基于快速分层深度卷积神经网络的入侵检测算法(Tree-CNN),并在模型顶层使用 SRS 激活函数使模型具有更好的泛化能力和学习速度,该模型识别率达到 97%,但该方法模型检测精度较低。Yue 等[9]针对 DoS 攻击提出基于 CNN 和 RNN 的集成检测算法,识别率达到 99.1%,但该方法计算开销较大。Song 等[10]将网络攻击视为恶意流量,基于分类思想利用 LSTM 和 XGBoost 集成算法实现了恶意流量分类识别,但该检测方法检测精度较低。Yu 等[11]提出一种基于多尺度卷积神经网络(MSCNN)的高精度入侵检测系统,通过不同尺度的卷积核特征提取有效提升了卷积检测精度,针对上述各类攻击的平均准确率提高了 4.37%。Wu 等[12]提出了 LuNet 模型,该模型针对 Probe 和 DoS 攻击的检测率达到 99%,但是对于 U2R 和 R2L 的识别率较低;Yang 等[13]针对 U2R 和 R2L 攻击提出基于改进密度峰值算法和深度置信网络的 MDPCA-DBN 算法实现攻击检测,该算法针对良性数据的识别准确率达到 97.38%,对于 U2R 和 R2L 的识别率分别达到 6.5% 和 17.25%。Yakubu 等[14]提出了基于双向长短期记忆网络的检测模型(Bi-LSTM),该模型检测精度达到 92.81%,但时间复杂度较高,训练时间达到 9 789 s;

针对基于机器学习的方法依赖人工特征工程较深和检测精度不够,而基于深度学习的检测方法计算成本过大等问题,本研究受灰狼捕猎的群体智慧启发,在借助互信息理论进行网络流量特征选择的基础上,提出一种灰狼提升算法优化的最小二乘支持向量机实现针对网络攻击高精度分类的模型。

本文的主要贡献包括:1)利用互信息理论实现对网络流数据的特征选择,有效减少计算时间开销;2)提出基于最小二乘支持向量机的分类器模型,能够有效检出当前主要的网络攻击模式;3)提出基于灰狼提升算法的分类器模型优化算法,能有效提升模型检测精度。

本文的组织结构如下:第 1 节回顾了本研究相关的研究进展,第 2 节介绍了分类器模型构建的基本理论,第 3 节给出了模型构建方法和流程,第 4 节通过实验验证了分类器模型的性能,第 5 节对研究进行了总结和未来工作的展望。

1　基本理论

1.1　互信息理论

互信息(mutual information,MI)[15]用来衡量两个变量之间相互依赖的程度,互信息值越大,表示两者相关性越高。它通常可以用来表示特征向量和标签之间的测度,在分类领域具有明显优势。互信息是两个变量联合分布 $p(x,y)$ 与边缘分布 $p(x)p(y)$ 的相对熵,其原理如式(1)所示。

$$I(X;Y)=H(X)-H(X\mid Y)=H(X)+H(Y)-H(X,Y)=\sum_{x\in X}p(x)\log\frac{1}{p(x)}+\sum_{y\in Y}p(y)\log\frac{1}{p(y)}+\sum_{x\in X}\sum_{y\in Y}p(x,y)\log\frac{1}{p(x,y)}=\sum_{x\in X}\sum_{y\in Y}p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \tag{1}$$

式(1)中,$H(X)$,$H(Y)$分别表示变量 X,变量 Y 的信息熵,其原理如式(2)所示。$H(X,Y)$表示变量 X 和变量 Y 的交叉熵,其原理如式(3)所示。

$$H(X)=-\sum_{x\in X}p(x)\log p(x) \tag{2}$$

$$H(X,Y)=-\sum_{x\in X}\sum_{y\in Y}p(x,y)\log p(x,y) \tag{3}$$

1.2　GWB 算法

灰狼(grey wolf optimizer,GWO)算法[16-17]模拟了自然界灰狼的等级层次和狩猎机制,灰狼主要包括四种类型,狼王 a,左右护法 b 和 c,其它灰狼个体 $d=\{d_1,d_2,\cdots,d_{n-3}\}$,狼群总会向狼王 a 和左右护法 b,c 移动,灰狼群的等级层次如图 1 所示。

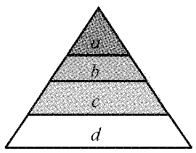

图 1　灰狼种群等级制度(从上到下优势递减)

标准灰狼算法的狩猎机制如下:

步骤 1)利用式(4)计算猎物与狼群各个体之间的距离,其中 $X_p(t)$ 表示第 t 次迭代后狼群中各个体的位置,$X(t)$表示第 t 次迭代后猎物的位置,C 为摆动因子,$r_1=rand(0,1)$,具体原理如式(5);

$$D=|CX_p(t)-X(t)| \tag{4}$$

$$C=2r_1 \tag{5}$$

步骤 2)根据适应度的大小择优选出 3 匹狼作为领导狼;

步骤 3)利用式(6)规定狼群其它个体向三匹领导狼前进的方向和步长;

$$A=a(2r_2-1) \tag{6}$$

步骤 4)利用式(7)、(8)更新狼群中个体的位置;

$$\begin{cases}D_{di\_a}=|CX_a(t)-X_{di}(t)|\\D_{di\_b}=|CX_b(t)-X_{di}(t)|\\D_{di\_c}=|CX_c(t)-X_{di}(t)|\\X_{di\_a}=X_a(t)-A_aD_{di\_a}\\X_{di\_b}=X_b(t)-A_bD_{di\_b}\\X_{di\_c}=X_c(t)-A_cD_{di\_c}\end{cases} \tag{7}$$

$$X_{di}=\frac{X_{di\_a}+X_{di\_b}+X_{di\_c}}{3} \tag{8}$$

由于经典灰狼优化算法在寻优化过程中容易陷入局部最优，近几年针对灰狼算法出现了多种优化算法[18-19]，本文提出与差分优化算法[20]相融合的灰狼提升算法(gray wolf boosting，GWB)。差分优化算法通过对种群进行变异、交叉、选择等机制产生新的种群得到最优解。

生成初始种群：原始种群存在 n 个个体，每个个体使用 d 维向量进行描述，可表示为：$X_i=\{X_{ij}\}=\begin{Bmatrix}X_{11} & X_{12} & \cdots & X_{1d}\\ X_{21} & X_{22} & \cdots & X_{2d}\\ \vdots & \vdots & \ddots & \vdots\\ X_{n1} & X_{n2} & \cdots & X_{nd}\end{Bmatrix}, i=1,2,\cdots,n, j=1,2,\cdots,d$，可以利用式(9)随机生成初始种群，其中 X_{ij}^u, X_{ij}^l 分别表示第 i 个个体的第 j 个变量的上界、下界。

$$X_i^*=\{X_{ij}^*\}=X_{ij}^l+rand(0,1)\times(X_{ij}^u-X_{ij}^l) \tag{9}$$

变异：通过使用种群中两个不同向量来干扰一个现有变量进行差分操作，实现变异，具体如式(10)，式中的 $X_a(g), X_b(g), X_c(g)$ 表示当前群体第 a, b, c 个个体，$v_i(g)$ 为第 i 个个体 X_i 对应的变异个体，F 为缩放因子。

$$v_i(g)=X_a(g)+F\times(X_b(g)-X_c(g)) \tag{10}$$

交叉：通过每个个体与其变异个体进行交叉操作，生成试验个体，具体如式(11)，式中的 CR 表示交叉概率因子。

$$u_t(g)=\begin{cases}v_t(g), rand(0,1)\leqslant CR \text{ 或 } t=rand(1,d)\\ X_t^*, rand(0,1)>CR \text{ 或 } t\neq rand(1,d)\end{cases} \tag{11}$$

选择：从原始个体和试验个体中选择更优的作为下一次迭代值，原理如式(12)。

$$X_i(t+1)=\begin{cases}u_t(g), f(u_t(g))\leqslant f(X_t^*)\\ X_t^*, f(u_t(g))>f(X_t^*)\end{cases} \tag{12}$$

通过以上的变异、交叉和选择操作，种群优化到下一代，重复上述步骤，直到迭代结束，得到种群最优解。

1.3　LSSVM 模型

假设数据集 S 有 N 个样本，每个样本有 m 个特征和 1 个标签，即：$S=\{(x_i,y_i)\}_{i=1}^N$，其中，$y_i\in\{0,1\}, x_i=(X_{i1},X_{i2},X_{i3},\cdots,X_{im})$ 且 $x_i\in R^m$。最小二乘支持向量机(least square SVM，LSSVM)使用非线性映射函数 $\varphi(x)$ 将低维样本映射到高维空间中进行回归估计[21]，LSSVM 的回归函数为式(13)，其中，w 表示权重向量，b 表示偏置变量。

$$y(x)=\omega^{\mathrm{T}}\varphi(x)+b \tag{13}$$

利用结构风险最小化的原则，LSSVM 的优化问题可描述为下面一个等式约束：

$$\begin{cases}\min\limits_{w,b,e_i}J(w,e_i)=\dfrac{1}{2}\|w\|^2+\dfrac{1}{2}\gamma\sum\limits_{i=1}^N e_i^2\\ s.t.\ y_i(w\cdot x_i+b)\geqslant 1-e_i, i=1,2,\cdots,N\end{cases} \tag{14}$$

利用拉格朗日乘子法将式(14)可以转换成无约束的拉格朗日目标函数 $L(w,b,e;a)$，表示为式(15)。

$$L(w,b,e;a)=J(w,e)-\sum_{i-1}^N a_i(y_i(w\cdot x_i+b)-1+e_i) \tag{15}$$

LSSVM 求解思路为：利用拉格朗日乘数法将原问题转化为对单一参数求解，令 $L(w,b,e;a)$ 分别对 w, b, e_i, a_i 求导等于 0，可表示为式(16)。

$$\begin{cases}\dfrac{\partial L}{\partial w}=0\Rightarrow w=\sum\limits_{i=1}^N a_i y_i x_i\\ \dfrac{\partial L}{\partial b}=0\Rightarrow\sum\limits_{i=1}^N a_i y_i=0\\ \dfrac{\partial L}{\partial e_i}=0\Rightarrow a_i=de_i, i=1,2,\cdots,N\\ \dfrac{\partial L}{\partial a_i}=0\Rightarrow y_i(w\cdot x_i+b)-1+e_i=0, k=1,2,\cdots,N\end{cases} \tag{16}$$

根据式(16)可以列出关于 a 和 b 的线性方程组，如式(17)，其中 $\boldsymbol{\Omega}$ 被称作核矩阵，可表示为式(18)。

$$\begin{bmatrix}0 & y^{\mathrm{T}}\\ y & \boldsymbol{\Omega}+I/\gamma\end{bmatrix}\begin{bmatrix}b\\ a\end{bmatrix}=\begin{bmatrix}0\\ 1_v\end{bmatrix} \tag{17}$$

$$\Omega_{ij}=y_iy_jx_ix_j=y_iy_jK(x_i,x_j), i,j=1,2,\cdots,N \tag{18}$$

考虑网络流量数据在时间上呈现出的线性特征，而高斯核函数相比线性核函数能够更好的刻画数据间的相似性，具有更好的针对线性数据的分类性能，因而这里将 LSSVM 中线性核函数优化为高斯核函数[22]，核函数如式(19)，优化后的 LSSVM 回归函数如式(20)。

$$K(x_i,x_j)=\exp\left(-\frac{\|x_i-x_j\|^2}{2\delta^2}\right) \tag{19}$$

$$y(x)=W\cdot\varphi(x)+b=\sum_{i=1}^N a_iK(x_i,x)+b \tag{20}$$

2　基于 MI-GWB-LSSVM 的网络攻击检测模型

2.1　数据预处理

针对数据集[23]中存在的数据类型多样、量纲不统一问题，分别采用二值转换、归一化方式进行数据预处理。

二值转换：利用字典的键值对实现字符型特征到数值型特征的转换，具体转换情况如表 1 所示。

归一化：归一化处理使得数据样本的值落到[0，1]之间，加快模型训练的速度，其处理方法如式(21)所示，其中 x 表示样本实际值，$x_{\min}, x_{\max}$ 分别表示样本数值中的最小值、最大值。

$$X=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{21}$$

2.2　基于 MI 理论的特征选择

经过数据处理后网络流量数据，包含了 41 维特征。为降低 LSSVM 模型分类计算消耗，首先进行特征选择，消除数据集中的冗余特征与不相关特征，以提高模型分类速度。

表 1　二值转换对应表

特征名称	转换前	转换后
Protocol	tcp	0
	udp	1
	icmp	2
Service	aol	0
	auth	1
	bgp	2
	…	…
	Z39-50	69
Label	normal	0
	其他类型	1

根据互信息理论,利用式(1)计算实验数据集中各特征与标签之间的互信息值,根据互信息值大小判断二者关联程度的高低。各特征与标签之间的互信息值如表 1 所示。由表 1 可知,数据集中 14 个特征的互信息值超过 0.2,显著高于剩余特征的互信息值,故选择这 14 个特征作为 LSSVM 的输入特征,而互信息值小于 0.2 甚至为 0 的特征属于模型的无效特征,其不仅无法提升检测精度 且将严重提高模型时间复杂度,故予以剔除。

表 2　各特征与标签之间的互信息值

特征列号	互信息值	特征列号	互信息值
12	0.417 1	28	0.064 4
4	0.416 1	40	0.064 0
26	0.373 9	18	0.062 0
39	0.364 8	24	0.057 7
25	0.362 4	8	0.038 2
30	0.347 2	10	0.026 3
3	0.346 9	13	0.022 2
38	0.328 5	16	0.020 1
29	0.303 2	5	0.020 0
6	0.301 7	17	0.006 2
35	0.230 4	15	0.005 9
34	0.216 7	9	0.004 7
33	0.215 8	19	0.004 7
37	0.207 4	11	0.001 9
23	0.177 1	1	0.001 3
36	0.126 1	14	0.001 3
32	0.124 7	7	0
31	0.110 4	20	0
41	0.091 7	21	0
2	0.069 2	22	0
27	0.065 3		

2.3　基于 GWB-LSSVM 的检测模型

参数配置高度影响 LSSVM 模型预测的精度,为此本文借助 GWO 算法对 LSSVM 的模型参数进行寻优处理。然而 GWO 算法在面临大规模高维数据时容易陷入局部寻优,从而延长算法训练时间,制约算法性能。为进一步提高算法的优化性能,本文通过改进 GWO 后的 GWB 算法在提升灰狼种群多样性的同时可以使灰狼算法遍历整个种群,增加了算法跳出局部极小值的几率,从而提高了算法的全局寻优能力。

GWB 算法实现步骤如下:

步骤 1)设置各项初始参数;设置 GWB-LSSVM 模型正则化参数 C 的范围为 0.1～300;核函数参数 δ 的搜索范围设置为:0.1～300,GWB 算法的种群规模为 12,最大迭代次数设置为 100;

步骤 2)初始化种群,并计算种群个体自适应度值,并按照大小确定值最高的三个个体为狼王和左右护法;选用对网络流量检测的准确率为优化算法的自适应度。

步骤 3)更新父代种群位置;

步骤 4)利用差分机制进行变异、交叉产生新子代个体;利用差分机制的选择步骤更新父代种群。

步骤 5)计算新种群所有个体的自适应度值,更新狼王和左右护法的位置;

步骤 6)判断迭代次数是否满足终止条件,满足输出 LSSVM 模型的最优参数。

GWB 算法的流程如图 2 所示。

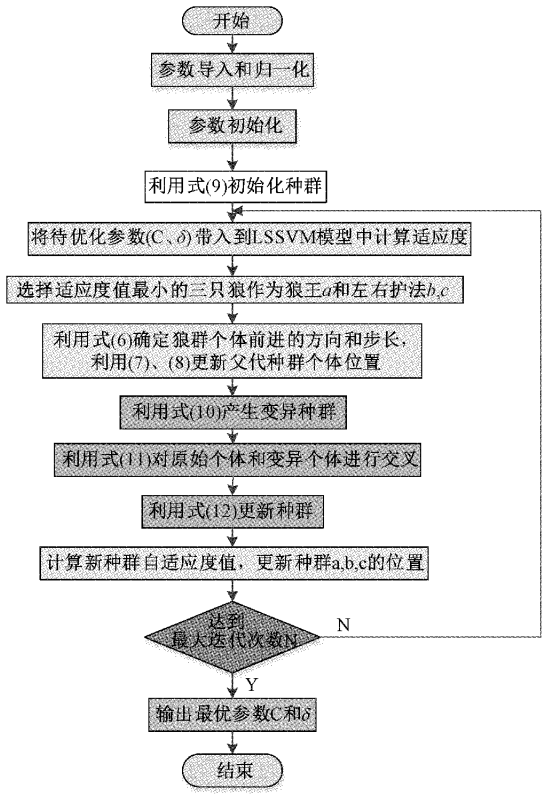

图 2　GWB 算法流程

2.4　建模流程

基于 MI-GWB-LSSVM 的网络攻击检测模型是一个由特征选择和分类器构成的两阶段检测模型，其检测框架图如图 3 所示。

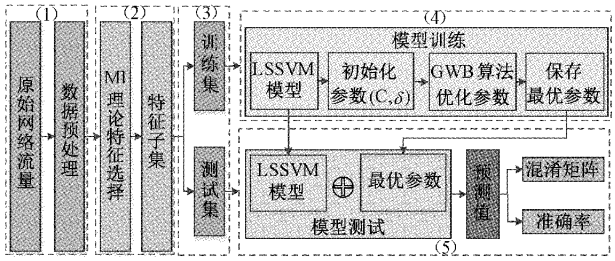

图 3　MI-GWB-LSSVM 检测框架

MI-GWB-LSSVM 的网络攻击检测模型主要步骤包括：

步骤 1)根据 2.1 节对数据进行预处理；

步骤 2)根据 2.2 节获得 LSSVM 模型的最优输入特征；

步骤 3)分割数据样本为训练集和测试集；

步骤 4)训练 LSSVM 模型，并利用 GWB 算法确定 LSSVM 模型的超参数；

步骤 5)采用测试集进行模型评估。

2.5　模型评估

MI-GWB-LSSVM 性能评价指标包括混淆矩阵、准确率、精度和检测率。混淆矩阵用来表示一个分类器结果的矩阵，其矩阵表示如表 3 所示，其中 TP 表示真阳率，FN 表示假阴率，FP 表示假阳率，TN 表示真阴率。准确率、精度和检测率的计算方法如式(22)～(24)。

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{22}$$

$$precision = \frac{TP}{TP + FP} \tag{23}$$

$$recall = sensitivity = DR = \frac{TP}{TP + FN} \tag{24}$$

表 3　混淆矩阵

真实标签 预测结果	正常	异常
正常	TP	FN
异常	FP	TN

3　仿真实验及分析

为验证模型有效性，选取 NSL-KDD 网络流量数据集[23]，并对数据集中的标签列进行重新标注，其中“0”表示正常数据，“1”表示存在攻击的异常数据，数据预处理后，从中随机选取 5 000 组数据进行仿真实验，其中前 4 000 组作为模型的训练集，剩余 1 000 组数据作为模型测试集。

3.1　特征选择对模型检测准确率的影响

针对原始数据存在冗余和不相关特征带来的计算量过大问题，根据 2.4 节步骤 2)计算数据集中各特征与标签列的 MI 值，并选取其中 MI≥0.2 的特征作为模型的输入。为验证 MI 特征选择的正确性，本文通过选取原始特征集和经 MI 选择后的特征集对 LSSVM 检测准确率的影响进行了对比验证，其结果如图 4 所示。

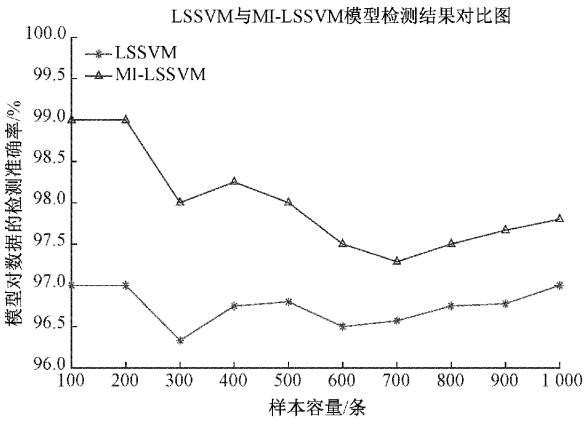

图 4　LSSVM 与 MI-LSSVM 模型检测结果

由图 4 可知，使用 MI 理论特征选择后 LSSVM 模型针对网络攻击检测的准确率在不同容量样本条件下平均提升约 2%，可见 MI 能够在有效消除冗余和不相关特征的同时能极大限度的保持数据集特征信息，在降低 LSSVM 模型计算量的同时能有效提升模型对网络攻击流量的检测准确率。

3.2　MI-GWB-LSSVM 模型改进性能分析

针对 LSSVM 模型参数最优化选择问题，本文借助 GWB 算法完成了模型参数的寻优处理。为量化分析 GWB 对 LSSVM 模型寻优的性能，横向对比了 LSSVM 在使用 GWO 和 PSO 算法[24]情况下的参数寻优能力，实验结果如表 4 和 5 所示。

表 4　MI-GWB-LSSVM 模型改进性能分析图

模型名称	准确率%	精度%	检测率%
MI-PSO-LSSVM	98.7	99.1	99.0
MI-GWO-LSSVM	98.9	99.4	99.0
MI-GWB-LSSVM	99.1	99.7	99.3

由图 5 可知，GWO 和 PSO 针对 LSSVM 模型的优化能力随着样本容量的增加呈现线性递增趋势而 GWB 则始终保持了相对比较平稳的优化能力，证明 GWB 在不同数据规模下具有更好的鲁棒性；同时，在不同的数据规模下 GWB 相较 GWO 和 PSO 都有更好的优化能力，虽然随着数据规模的增大，优化性能有所下降，但始终保持在最大约 2%，最小约 0.5%的优势，证明 GWB 较其它两种优化算法具有更好的优化性能。实验中 LSSVM 模型的最佳正则化

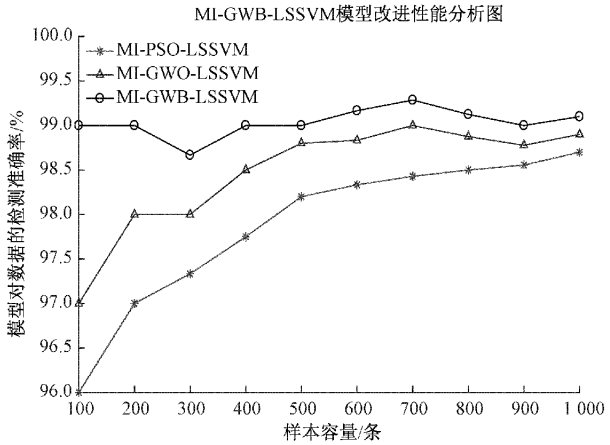

图 5　MI-GWB-LSSVM 模型改进性能分析图

参数和核函数分别为:191 和 2.945 1。

3.3　与现有研究的实验对比

目前网络攻击检测方面存在大量研究成果,为进一步评估 MI-GWB-LSSVM 模型性能,与文献[14]和[25]中提出的深度学习模型 Bi-LSTM 和机器学习模型 IGWO-BP 模型进行了对比,其中各模型时间复杂度分析如表 5 所示,其中 $Node_i$ 为 Bi-LSTM 网络中各层网络节点数。从表中能够发现本文算法和文献[25]总体算法时间复杂度均为 $O(n\log n)$,但就具体运算来看,本文算法首先在特征选择阶段通过特征相关性选择大幅度去除了冗余和不相关特征;其次在模型针对特征集的识别阶段,在非极大值情况下本文检测模型时间复杂度为 $O(43n)$,优于 BP 模型实际复杂度 $O(1\ 380\times n)$,且文献[25]算法在总体检测中仍需进行 500 次的迭代计算,因此导致其计算时间会更多。而文献[14]中共 4 层网络含 2 个隐藏层,通过其浮点运算次数近似计算其复杂度,大约为样本数据集(N_{data})$\times Node_i^2$,其中 $Node_i$ 表示第 i 层网络所含节点数,从中可以推算出,虽然在极大值情况下文献[14]时间复杂度低,但实际就瞬时固定数据量情况来看,其输入、隐藏层 1、隐藏层 2 和输出层网络节点数分别为 64、128、64、32 的情况下计算规模已经远超数据集本身大小,导致其计算时间畸高,三种算法消耗时间对比和检测性能对比如表 6 所示,由此可见,在有限数据集环境下,本文算法在计算时间消耗方面具有明显优势。在检测准确率、检测精度和召回率方面的对比如图 6 所示,可见在不同的评价指标中,本文算法较其它算法都取得了更好的效果。

表 5　模型复杂度对比分析表

模型	模块时间复杂度		总体时间复杂度
	模块名	时间复杂度	
本文	GWB	$O(n\log n)$	$O(n\log n)$
	LSSVM	$O(43n)$	
文献[14]	Bi-LSTM	$O(n\times\sum Node_i^2)$	$O(n)$
文献[24]	IGWO	$O(n\log n)$	$O(n\log n)$
	BP	$O(1\ 380\times n)$	

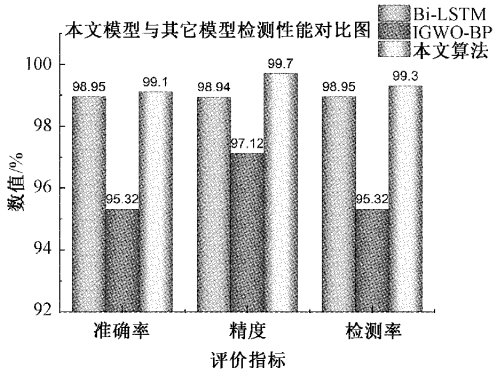

图 6　本文模型与其它模型检测性能对比图

表 6　本文模型与其它模型检测性能对比结果

模型名称	准确率/%	精度/%	检测率/%	时间
Bi-LSTM	98.0	98.09	97.88	1 081 s
IGWO-BP	95.32	97.12	95.32	1 046 s
本文算法	99.1	99.7	99.3	693 s

4　结　　论

长期以来面向网络攻击的入侵检测一直是网络安全研究中的一项重大挑战,本文基于机器学习技术提出一种称为 MI-GWB-LSSVM 网络攻击检测模型,该模型基于互信息理论的特征选择能有效消除数据中的冗余特征和无效特征,大幅降低了模型训练中的计算开销,基于提出的灰狼提升算法能够大幅度优化基于最小二乘支持向量机的网络攻击分类器检测模型的全局参数,使其针对主要攻击模式具有同已有研究相比更高的检测精度,检测率达 99.3%。基于 NSL-KDD 数据集的实验结果证明了 MI-GWB-LSSVM 网络攻击检测模型的性能和效率是高效和有效的。

参考文献

[1]　邵振国,张承圣,陈飞雄,等. 生成对抗网络及其在电力系统中的应用综述[J/OL]. 中国电机工程学:1-20[2022-06-11]. http://kns.cnki.net/kcms/detail/11.2107.tm.20220527.1803.007.html.

[2]　殷礼胜,魏帅康,孙双晨,等. 基于 FEEMD-SAPSO-BiLSTM 组合模型的短时交通流预测[J]. 电子测量与仪器学报,2021,35(10):72-81.

[3]　陈春谋. 基于流量阈值裁决分割机制的 WSN 网络抗 DDoS 算法研究[J]. 国外电子测量技术,2020,39(1):59-62.

[4]　DAN T, YAN Y D, ZHANG S Q, et al. Performance and features: mitigating the low-rate TCP-targeted DoS attack via SDN[J]. IEEE Journal on Selected Areas in Communications, 2021, 40(1): 428-444.

[5] MOHAMMAD N, ZARIFZADEH S, MOSTAFAVI S. A hybrid machine learning approach for detecting unprecedented DDoS attacks [J]. The Journal of Supercomputing, 2022,78(6):8106-8136.

[6] FARNAAZ N, JABBAR M A. Random forest modeling for network intrusion detection system[J]. Procedia Computer Science, 2016,89: 213-217.

[7] IKRAM S T, CHERUKURI A K. Intrusion detection model using fusion of chi-square feature selection and multi class SVM[J]. Journal of King Saud University Computer and Information Sciences, 2017,29(4): 462-472.

[8] MENDONCA R V, ARTHUR A M, RENATA L R, et al. Intrusion detection system based on fast hierarchical deep convolutional neural network [J]. IEEE Access,2021,9: 61024-61034.

[9] YUE C, WANG L D, WANG D R, et al. An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN[J]. IEEE Access, 2021,9:59527-59539.

[10] SONG C H, SUN Y Y, HAN G J, et al. Intrusion detection based on hybrid classifiers for smart grid[J]. Computers & Electrical Engineering, 2021, DOI: https://doi.org/10.1016/j.compeleceng.2021.107212.

[11] YU J, YE X J, LI H B. A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network[J]. Future Generation Computer Systems, 2022, 129, 399-406.

[12] WU P, GUO H. LUNET: A deep neural network for network intrusion detection [C]. 2019 IEEE Symposium Series on Computational Intelligence (SSCI),IEEE, 2019:617-624.

[13] YANG Y Q, ZHENG K F, WU C H, et al. Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks [J]. Applied Sciences, 2019, DOI: https://doi.org/10.3390/app9020238.

[14] IMRANA Y, XIANG Y P, ALI L, et al. A bidirectional LSTM deep learning approach for intrusion detection [J]. Expert Systems with Applications, 2021, DOI: 10.1016/j.eswa.2021.115524.

[15] SENGUPTA D, GUPTA P, BISWAS A. A survey on mutual information based medical image registration algorithms[J]. Neurocomputing, 2022,486,174-188.

[16] GHALAMBAZ M, YENGEJEH R J, DAVAMI A H. Building energy optimization using Grey Wolf Optimizer[J]. Case Studies in Thermal Engineering, 2021, DOI:10.1016/j.csite.2021.101250.

[17] MIRJALILI S, MIRJALILI S M, ANDREW L. Grey wolf optimizer[J]. Advances in engineering software, 2014,(69): 46-61.

[18] SINGH N, SINGH S B. A novel hybrid GWO-SCA approach for optimization problems[J]. Engineering Science and Technology, an International Journal, 2017,20(6): 1586-1601.

[19] THOBIANI FAL, KHATIR S, BENAISSA B, et al. A hybrid PSO and grey wolf optimization algorithm for static and dynamic crack identification[J]. Theoretical and Applied FractureMechanics, 2022, DOI: https://doi.org/10.1016/j.tafmec.2021.103213.

[20] NAHAK N, KUMAR R M. Damping of power system oscillations by a novel DE-GWO optimized dual UPFC controller[J]. Engineering Science and Technology, an International Journal,2017,20(4):1275-1284.

[21] LIANG Y, HU S S, GUO W S, et al. Abrasive tool wear prediction based on an improved hybrid difference grey wolf algorithm for optimizing SVM [J]. Measurement, 2022, DOI: 10.1016/j.measurement.2021.110247.

[22] 李玉,宫学亮,赵泉华.基于张量径向基核函数支持向量机的高光谱影像分类[J].仪器仪表学报,2020,41(12):253-262.

[23] Canadian Institute for Cybersecurity. The NSL-KDD dataset[EB/OL]. (2021-12-22). https://www.unb.ca/cic/datasets/nsl.html.

[24] SONG Y, XIE X D, WANG Y H, et al. Energy consumption prediction method based on LSSVM-PSO model for autonomous underwater gliders[J]. Ocean Engineering, 2021,230:108982.

[25] 王振东,刘尧迪,胡中栋,等.利用改进灰狼算法优化BP神经网络的入侵检测[J].小型微型计算机系统,2021,42(4):875-884.

作者简介

赵嘉,硕士研究生,助理工程师,主要研究方向为网络安全。
E-mail:1009893772@qq.com

谷良,硕士研究生,高级工程师,主要研究方向为网络安全。
E-mail:740304606@qq.com

吴瑶,硕士研究生,助理工程师,主要研究方向为网络安全。
E-mail:sxwuyao@163.com