文章编号:1671-4598(2024)12-0088-08 DOI:10.16526/j.cnki.11-4762/tp.2024.12.013 中图分类号:TP393.08 文献标识码:A

基于 BOA-DF-LightGBM 的入侵检测方法

蒋子昂[1]，朱志亮[1]，翁德华[1]，伍默然[1]，叶 南[2]
(1. 温州大学 电气数字化设计技术国家地方联合工程研究中心，浙江 温州 325035；
2. 亚龙智能装备集团有限公司，浙江 温州 325102)

摘要：入侵检测模型在训练时经常面临数据不平衡问题，即其中正常行为的样本数量远远超过异常入侵行为的样本数量；为解决数据不平衡问题，将深度森林和 LightGBM 结合作为入侵检测模型，其中通过深度森林中的多粒度扫描生成更丰富的特征作为 LightGBM 的输入，从而提升分类器的性能；并且深度森林生成的特征表示可以提高少数类样本的可分性，配合 LightGBM 的权重调整机制，可以更好地处理不平衡数据问题，并通过全局搜索能力强大的棕熊优化算法对模型进行参数调优进一步提升模型的预测准确度；经 UNSW_NB15 数据集验证所提方法，BOA-DF-LightGBM 模型较其他模型指标更为优异，预测准确率达到 95.15%，较 DF 提升了近 2%；为进一步验证其对数据不平衡问题的能力，通过更严苛的数据不平衡实验得出，BOA-DF-LightGBM 模型在数据不平衡实验中的准确率为 94.23%，较 DF 提升了 2.68%，较神经网络模型提升了 3.42%；验证了 BOA-DF-LightGBM 在数据不平衡情况下的有效性和优异性。

关键词：入侵检测；集成学习；棕熊优化算法；深度森林

Intrusion Detection Method Based on BOA-DF-LightGBM

JIANG Ziang[1], ZHU Zhiliang[1], WENG Dehua[1], WU Moran[1], YE Nan[2]
(1. Wenzhou University, National-Local Joint Engineering Research Center of Electrical Digital Design Technology, Wenzhou 325035, China;
2. Yalong Intelligent Equipment Group Co., Ltd., Wenzhou 325102, China)

Abstract: Intrusion detection models often face the problem of data imbalance during training, that is, the number of samples of normal behavior far exceeds the number of samples of abnormal intrusion behavior. In order to solve the problem of data imbalance, the deep forest and LightGBM are combined as an intrusion detection model, in which richer features are generated by multi-granularity scanning in the deep forest as the input of LightGBM, so as to improve the performance of the classifier. Moreover, the feature representation generated by deep forest can improve the distinguishability of minority samples, and with the weight adjustment mechanism of LightGBM, it can better deal with unbalanced data problems, and the brown bear optimization algorithm with powerful global search ability is used to tune the parameters of the model to further improve the prediction accuracy of the model. The proposed method is verified on the UNSW_NB15 dataset, and the BOA-DF-LightGBM model is better than other model indicators, with the prediction accuracy reaching 95.15%, which is nearly 2% higher than DF. In order to further verify its ability to solve the problem of data imbalance, the accuracy of the BOA-DF-LightGBM model in the data imbalance experiment is 94.23%, which is 2.68% higher than that of DF and 3.42% higher than that of neural network model. The effectiveness and superiority of BOA-DF-LightGBM in the case of data imbalance are verified.

Keywords: intrusion detection; ensemble learning; brown bear optimization algorithm; deep forest

0 引言

随着能源互联网系统的数字化和智能化程度不断提升，基于互联网的能源系统面临着越来越多的网络安全挑战，如恶意软件攻击、网络钓鱼、拒绝服务攻击等。能源互联网涉及供电设备、能源信息系统、数据通信等多个关键组件的互联，其安全风险可能导致对系统数据的篡改、设备的损坏、系统运行的异常等问题，严重影响能源系统的可靠性和稳定性。能源互联网入侵检测通过监测和分析系统的运行情况，能够识别潜在的网络入侵行为[1]。因此，能源互联网入侵检测的背景与意义在于提高系统的安全防护能力，防止潜在的网络攻击和安全威胁对系统造成的损害，保障能源供应的安全与可靠性。

目前，入侵检测的主流方案包括数理统计的流量检测[2]、基于流量特征的模式匹配[3]和基于机器学习算法[4]。数理统计方法精确度高，能够通过统计分析检测到异常流量和攻击行为。但计算量大，导致实时性较差，无法快速

收稿日期:2024-06-28； **修回日期**:2024-08-05。
基金项目:温州市科研项目(ZF2022003)。
作者简介:蒋子昂(1999-),男,硕士研究生。
朱志亮(1982-),男,博士,副教授。
引用格式:蒋子昂,朱志亮,翁德华,等.基于 BOA-DF-LightGBM 的入侵检测方法[J].计算机测量与控制,2024,32(12):88-95.

响应实时网络威胁；而特征匹配方案具有良好的实时性能够快速检测并响应已知的攻击模式，但依赖于预定义的规则和特征库，难以应对新型和变种攻击，适应性较差；而基于机器学习建模的方法通过历史数据建立模型，不仅不需要预先制定规则，还能持续学习和更新，兼具实时性和灵活性，因而受到众多研究者的关注。例如，文献［5］提出了一种混合特征选择方法，用于多类网络异常检测，使用多层感知器（MLP）网络并结合了信息增益（IG）和随机森林（RF）两种过滤方法，以减少特征子集搜索空间从而实现网络异常检测；文献［6］采用了网格搜索交叉验证（GSCV）参数搜索技术和支持向量机（SVM）的径向基函数（RBF）内核，算法简单但易过拟合，对复杂数据处理能力有限；文献［7］采用了决策树和 KNN 等软计算技术，通过预处理数据、特征选择、主成分分析（PCA）降维、标准化和归一化等方法来提高模型的准确性，虽提升了准确率，但模型稳定性仍需加强。文献［8］提出了一个基于注意力机制的双向长短期记忆（Bi-LSTM）模型，针对不同领域的网络数据提出了解决领域偏移问题的方法，通过将 HTTP 流量建模为自然语言序列来实现入侵检测。文献［9］结合了随机森林（RF）和自编码器（AE）两种模型，通过 RF 分类器的概率输出确定样本是否属于攻击，引入 AE 模块以降低误报率。文献［10］提出了基于卷积神经网络—门控循环单元—联邦学习（CNN-GRU-FL）的分布式入侵检测方法。此外，提出了新的参数聚合机制以提高在数据质量和数量差异情况下的模型质量，并设计了基于信任的节点选择机制来改善联邦学习的收敛能力。提升了在数据质量差异情况下的参数聚合性能和效率。文献［11］使用 WaveNet 堆叠卷积操作，结合 BiGRU 进行模型训练与分类，通过多个数据集验证了模型的性能。文献［12］首先使用主成分分析（PCA）进行特征降维，然后使用降维后的低维特征构建随机森林（RF）、贝叶斯网络、线性判别分析（LDA）和二次判别分析（QDA）等分类器来设计入侵检测系统，并开发了一种基于均匀分布的平衡方法，以处理入侵数据集中少数类实例的不平衡问题。文献［13］将 CNN 与 LSTM 结合，从时空层面考虑网络入侵数据特征，通过 L2 正则化和 dropout 方法来解决过拟合问题，取得较高的检测准确率。文献［14］使用鲸鱼优化算法对 XGboost 模型进行参数寻优应用于网络入侵检测。文献［15］提出使用人工蜂群算法应对计算机网络 DDoS 攻击入侵检测，选择不同的特征子集得到 DOS 攻击检测的离散信息，实现对组合网络流量数据间的攻击信息特征提取和聚类分析，解决计算机网络 DDoS 攻击检测过程中的连续多变量优化问题[15]。尽管当前研究者们在网络入侵检测领域已取得一定成果，但仍存在一些问题。如：入侵检测的效率低，将合法操作误判为恶意行为，产生误报，导致资源和时间的浪费，降低系统的可靠性[16]。入侵检测数据集中正常行为和恶意行为的比例可能存在不平衡，导致模型更倾向于预测出现频率更高的类别，而忽略其他潜在的风险[17]。

针对上述问题，将深度森林和 LightGBM 结合，作为入侵检测模型，其中通过深度森林中的多粒度扫描生成更丰富的特征作为 LightGBM 的输入，从而提升分类器的性能。并且深度森林生成的特征表示可以提高少数类样本的可分性，配合 LightGBM 的权重调整机制，可以更好地处理不平衡数据问题，深度森林和 LightGBM 的结合利用了两种不同的学习方法，能够有效避免单一模型的局限性，提高整体模型的泛化能力。最后通过全局搜索能力强大的棕熊优化算法对模型进行参数调优进一步提升模型的预测准确度。可以平衡不同类别数据的重要性，提高对恶意行为的检测率，缓解入侵检测数据不平衡的问题。经 UNSW_NB15 数据集验证所提方法，BOA-DF-LightGBM 模型较其他模型指标更为优异，预测准确率达到 95.15%，较 DF 提升了近 2%。为进一步验证其对数据不平衡问题的能力，通过更严苛的数据不平衡实验得出，BOA-DF-LightGBM 模型在数据不平衡实验中的准确率为 94.23%，较 DF 提升了 2.68%，较神经网络模型提升了 3.42%。充分验证了本文提出模型对于解决入侵检测数据不平衡问题的有效性。

1　BOA-DF 算法模型

1.1　深度森林

深度森林[18]（DF，deep forest）是一种深度模型，由南京大学的周志华教授团队提出，因其结合了随机森林和深度神经网络的特点，受到了人工智能学术界和工业界的广泛关注。

深度森林包括多粒度扫描和级联森林两部分。

1）多粒度扫描（Multi-Grained Scanning）是一种用于特征提取的方法，它在处理数据（尤其是序列数据和图像数据）时，可以增强特征表示的多样性和鲁棒性。这种方法借鉴了卷积神经网络（CNN）中的局部感受野（receptive field）的概念，通过不同粒度（窗口大小）的扫描，提取多尺度的特征表示，多粒度扫描的结构如图 1 所示。其具体步骤包括：滑动窗口扫描、局部特征提取、特征拼接和输入级联层等。

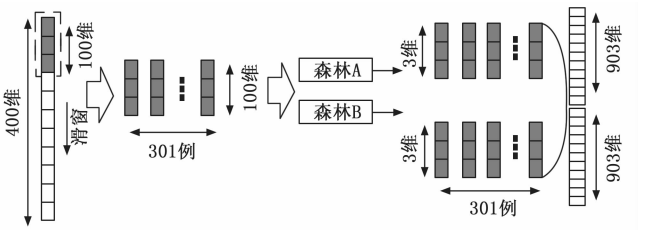

图 1　多粒度扫描结构图

（1）滑动窗口扫描：对输入数据应用不同大小的滑动窗口，进行局部特征的提取。

（2）局部特征提取：在每个窗口上训练随机森林或完全随机森林，得到局部区域的特征表示。

（3）特征拼接：将不同粒度的特征拼接在一起，形成多尺度的特征向量。

(4) 输入级联层：将这些多尺度特征向量输入到深度森林的级联结构中，逐层进行特征提取和分类。

2) 级联森林 (Cascade Forest) 是深度森林 (Deep Forest) 模型的核心架构之一。级联森林通过多层次的结构，逐层提取特征并进行分类，类似于深度神经网络中的多层感知器。每一层级联森林由多个随机森林和完全随机森林组成，这些森林共同工作以逐步提高模型的预测能力。

级联森林采用逐层处理和决策的方式，每一层接收上一层的输出作为输入，通过多组随机森林进行进一步处理。具体步骤如图 2 所示。

(1) 初始特征输入：最初的输入特征直接来自于原始数据。

(2) 层级处理：在每一层中，使用多组随机森林和完全随机森林来处理输入特征，生成每组森林的输出。

(3) 输出拼接：将每组森林的输出拼接在一起，形成该层的输出特征。

(4) 逐层处理：将当前层的输出特征作为下一层的输入，继续进行处理，直到达到预定的层数。

(5) 最终决策：在最后一层，使用输出特征进行最终的分类或回归决策

1.2 棕熊优化算法

棕熊优化算法 (BOA，brown-bear optimization algorithm) 由 Tapan 等人[19]于 2022 年根据棕熊的交流方式提出的，具有寻优速度快、求解精度高等优势。该优化算法包括棕熊的脚底气味标记和嗅探行为两个阶段。其中棕熊在脚底气味标记时表现出特定的行为特征，如行走时的步态、谨慎的步伐以及脚底在地面凹陷处的扭转。

假设在一个区域内，棕熊的不同群体是随机产生的，它们有固定数量的脚底气味标记，不同群体的每一个标志都具有鲜明的特征，并保留在领土内。区域内群体随机初始化的数学表达式如式 (1) 所示：

$$P_{i,j} = P_{i,j}^{\min} + \lambda(P_{ij}^{\max} - P_{i,j}^{\min}) \tag{1}$$

其中：$P_{i,j}$是第 i 群棕熊的第 j 个脚底标记。$P_{i,j}^{\min}$和 $P_{i,j}^{\max}$分别是脚底标记的最小范围和最大范围。λ 是均匀分布在 [0，1] 范围内的任意随机数。如果一个区域内的群体总数用 N_{pop}来定义，每一群体中脚底标记的总数 (即决策变量的数量) 用 D 来定义，则解集 $\boldsymbol{P}$ 表示为式 (2)：

$$\boldsymbol{P} = \begin{bmatrix} P_{1,1} & \cdots & P_{1,D} \\ \vdots & \ddots & \vdots \\ P_{N_{\text{pop}},1} & \cdots & P_{N_{\text{pop}},D} \end{bmatrix} \tag{2}$$

假设算法的总迭代次数为 N_{iter}，则上述每个特征的出现次数等于$\frac{N_{\text{iter}}}{3}$。

行走时的步态特征：步行时根据特征步态形成的脚部气味痕迹持续到总迭代次数的前三分之一，即$\frac{N_{\text{iter}}}{3}$，其可以如式 (3)：

$$P_{i,j,k}^{\text{new}} = P_{i,j,k}^{\text{old}} - (\theta_k \alpha_{i,j,k} P_{i,j,k}^{\text{old}}) \tag{3}$$

其中：$P_{i,j,k}^{\text{new}}$是第 i 组棕熊在第 k 次迭代中更新的第 j 个脚部标记，$P_{i,j,k}^{\text{old}}$是同一次迭代中第 i 组棕熊之前的第 j 个脚部标记。$\alpha_{i,j,k}$是在 [0，1] 范围内均匀分布的任意随机数，与第 i 组熊第 k 次迭代的第 j 次脚底标记相关。θ_k 是第 k 次迭代的发生因子，它随迭代次数的增加而线性增加。定义为当前迭代次数与总迭代次数的比值，表示为式 (4)：

$$\theta_k = \frac{C_{\text{iter}}}{N_{\text{iter}}} \tag{4}$$

其中：C_{iter}为当前迭代次数。

谨慎的步伐特性：一只棕熊过去常常重复地踩在前面的踏板上，以便让同类的其他成员更容易看到它，其可以如式 (5) 所示：

$$P_{i,j,k}^{\text{new}} = P_{i,j,k}^{\text{old}} - F_k(P_{j,k}^{\text{best}} - L_k P_{j,k}^{\text{worst}}) \tag{5}$$

其中：$P_{j,k}^{\text{best}}$和 $P_{j,k}^{\text{worst}}$分别是第 k 次迭代中棕熊种群中第 j 个最佳和第 j 个最差的踏板气味标记。F_k 是第 k 次迭代的

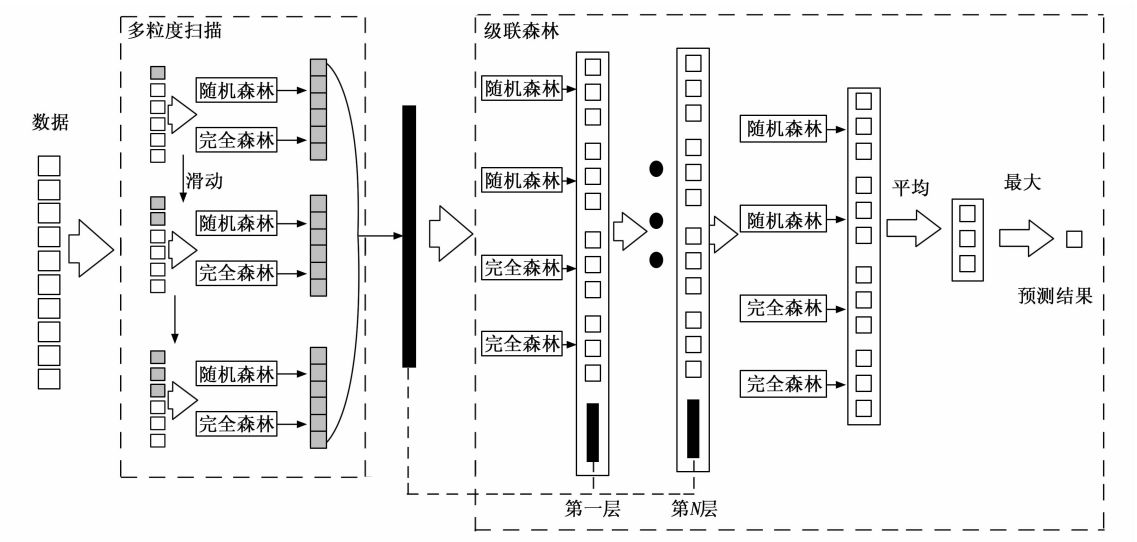

图 2 深度森林结构图

阶跃因子，它的值取决于发生因子 θ_k，如式（6）所示：

$$F_k = \beta_{1,k}\theta_k \tag{6}$$

其中：$\beta_{1,k}$是第 k 次迭代时［0，1］范围内的任意随机数。k 是第 k 次迭代的步长。在这里加入它是为了展示如何从整个人口的最佳和最差脚底标记的可用信息来修改脚底标记。步长 L_k 取 1 或 2 的值。

根据步长 L_k 的不同，雄性棕熊会小心地向前或向后迈一步，以形成新的踏痕。数学上，步长 L_k 表示为：

$$L_k = round(1+\beta_{2,k}) \tag{7}$$

其中：$\beta_{2,k}$是均匀分布在［0，1］范围内的任意随机数。

扭脚特征：脚底标记的更新是由扭脚特征来定义的。群体中每只雄性棕熊扭脚的角速度表示为：

$$w_{i,k} = 2\pi\theta_k\gamma_{i,k} \tag{8}$$

式中，$w_{i,k}$为第 k 次迭代时扭转的第 i 次角速度。$\gamma_{i,k}$是在［0，1］范围内均匀分布的随机数。棕熊只会把脚扭到先前的脚印上，这些脚印离最好的脚印更近，离最坏的脚印远。这个特性是通过式（9）来定义的：

$$P^{new}_{i,j,k} = P^{old}_{i,j,k} + w_{i,k}(P^{best}_{j,k} - |P^{old}_{i,j,k}|) - w_{i,k}(P^{worst}_{j,k} - |P^{old}_{i,j,k}|) \tag{9}$$

嗅探行为：通过嗅脚部发出的标记来控制了它们在领地内的行动，在棕熊的每一个群体成员中都很常见。熊开始嗅探在领地内随机选择的踏板标记，向属于自己群体的脚部标记移动，并留下其他踏板标记。其行为的数学建模如式（10）所示：

$$P^{new}_{i,j,k} = \begin{cases} P^{old}_{m,j,k} + \lambda_{j,k}(P^{old}_{m,j,k} - P^{old}_{n,j,k}) & \text{if} \quad f(P^{old}_{m,k}) < f(P^{old}_{n,k}) \\ P^{old}_{n,j,k} + \lambda_{j,k}(P^{old}_{n,j,k} - P^{old}_{m,j,k}) & \text{if} \quad f(P^{old}_{n,k}) < f(P^{old}_{m,k}) \end{cases} \tag{10}$$

其中：$P^{old}_{m,j,k}$是第 m 组熊在第 k 次迭代中第 j 次更新的踏板标记。$P^{old}_{m,j,k}$和 $P^{old}_{m,j,k}$分别是第 m 组和第 n 组熊在第 k 次迭代中的第 j 个踏板标记，$m \neq n$ $f(P^{old}_{m,k})$ 和 $f(P^{old}_{n,k}$ 是第 k 次迭代时对第 m 组和第 n 组熊的适应度函数值。$\lambda_{j,k}$是第 j 次迭代时第 k 次踏板标记在［0，1］范围内的均匀分布随机数。

重复上述两种行为，将更新的种群和旧的种群中较好的一组熊被保留并移动到下一次迭代，直到满足任何终止条件。

1.3　BOA-DF-LightGBM 算法模型

如图 3 所示，将深度森林和 LightGBM 结合作为入侵检测模型，其中通过深度森林中的多粒度扫描生成更丰富的特征作为 LightGBM 的输入，从而提升分类器的性能。深度森林中的级联层可以将前一层的输出特征与原始输入特征组合在一起，形成新的特征集。这样，模型能够充分利用原始特征和通过级联层生成的高级特征。其生成的特征表示可以提高少数类样本的可分性，配合 LightGBM 的权重调整机制，可以更好地处理不平衡数据问题。并且对于入侵检测这类高维数据级联层可以通过多层次的特征提取和组合，降低数据的维度复杂性。

并且深度森林和 LightGBM 的结合利用了两种不同的学习方法，能够有效避免单一模型的局限性，提高整体模型的泛化能力。最后通过全局搜索能力强大的棕熊优化算法对模型进行参数调优进一步提升模型的预测准确度。

本文提出模型的调整超参数如表 1 所示，分为 DF 参数和 LightGBM 参数。其中 DF 的参数，n _ estimators 表示指定每个级联层中的估计器数量；n _ trees 表示指定每个估计器中的树的数量；n _ bins 表示指定特征离散化的箱数，较小的值意味着会考虑较少的分割点；criterion 用于衡量分割质量的函数，支持的标准包括用于基尼不纯度的 gini 和用于信息增益的 entropy。

表 1　参数描述

模型	参数	范围	描述
DF	n_estimators	［2，100］	每个级联层中的估计器数量
	n_trees	［2，100］	估计器中的树的数量
	n_bins	［2，225］	指定特征离散化的箱数
	criterion	［Gini，entropy］	衡量分割质量的函数
Light GBM	num_leaves	［1，100］	树叶数量
	max_depth	［1，100］	树的最大深度
	min_data_in_leaf	［1，200］	最小数据叶
	learning_rate	［0.01，1］	学习率

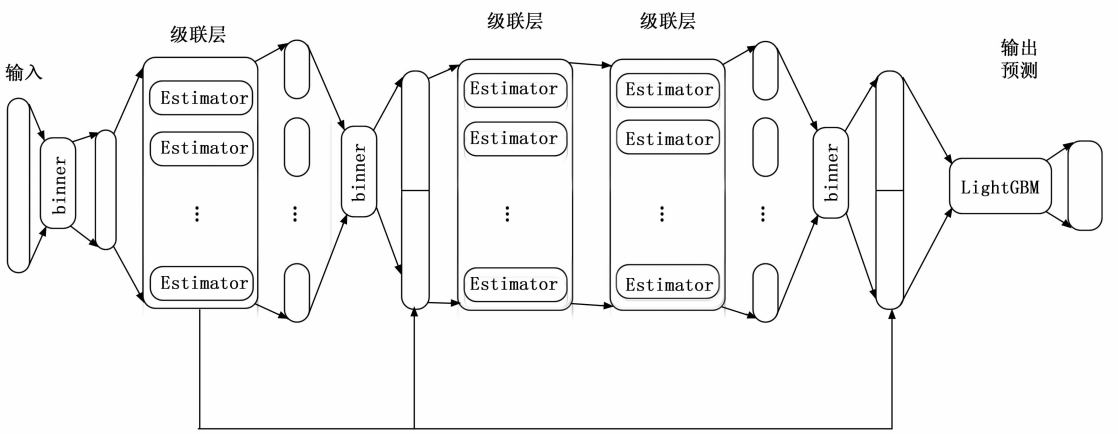

图 3　DF-LightGBM 模型

BOA-DF 的训练与参数优化的过程如图 4 所示。具体步骤如下：

首先，将数据按 1.3 节进行预处理，将一些非数字特征转化为数字特征，并将差距较大的特征进行归一化，避免因数据中的特征差距太大使得模型训练困难。

然后，根据要优化参数，初始化标记的维度为 4 维，可以表示为 X：

$$X_{i(t)} = \{X_{i(t)}^{\text{n\_estimators}}, x_{i(t)}^{\text{n\_trees}}, x_{i(t)}^{\text{n\_bins}}, \cdots, x_{i(t)}^{\text{criterion}}\} \tag{11}$$

其中：$X_{i(t)}$ 表示 DF 要优化的参数。

最后，根据各维度参数的取值范围，限定 BOA 的搜索空间，局部和全局搜索使得 DF 准确率最大的标记（超参数）即如式所示：

$$F_{i(t)} = (X_{i(t)} \rightarrow DF)[\text{Accuracy}] \tag{12}$$

每一轮迭代，确定当前最优搜索参数：

$$X_{\text{best}(t)} = max(F_{i(t)}, X_{\text{best}(t-1)}) \tag{13}$$

算法不断迭代直到满足终止条件，输出当前最优搜索标记，即为 DF-LightGBM 模型对该数据分类能力的最优参数。

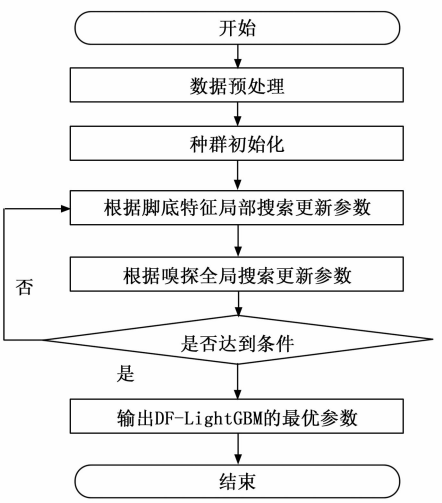

图 4 BOA-DF 的训练流程

2 实验与结果分析

2.1 实验环境及设置

本文实验的电脑配置为 12th Gen Intel（R）Core（TM）i9-12900K 的处理器、64 GB 的内存和 64 位 Windows10 操作系统，使用 Pycharm 编辑器和 Sklearn 和 Tensorflow 框架。棕熊优化算法的参数设置如表 2 所示，表 3 给出了经过 BOA 优化后的 DF 和 LightGBM 的参数组。

表 2 BOA 参数设置

参数	值	描述
Lb	[2,2,2,0,1,1,0.01]	下限
Ub	[225,20,1,1,100,100,100,200,1]	上限
Popsize	10	种群大小
Iter	100	优化次数

表 3 优化后的 DF-LightGBM 参数设置

参数	值
n_estimators	5
n_trees	76
n_bins	206
criterion	entropy
num_leaves	86
max_depth	33
min_data_in_leaf	108
learning_rate	0.180 45

2.2 数据集与数据预处理

UNSW-NB15 数据集[19]是一个用于网络入侵检测的公开数据集，由澳大利亚新南威尔士大学的网络安全实验室开发。该数据集模拟了真实网络环境中的网络流量，包含 22 个网络流量等各种常见的网络攻击和正常流量，其包含基本流量统计特征，流量数量、持续时间、协议类型等；传输层的特征，TCP 头部信息、TCP flags 等；内容的特征，payload 相关信息等；流的特征，包括流的相关信息、时间的特征及不同时间窗口内的流量统计信息等。每个数据样本都标记了不同类型的网络入侵，包括 DoS（拒绝服务攻击）、Reconnaissance（侦察）、Analysis（分析）等。这些标记对于训练监督学习模型非常重要，以便模型能够识别和分类不同类型的网络入侵。

首先，对数据进行 ONE-HOT 编码，将数据中的非数字特征转化为数字特征。然后，将数字特征按式（11）进行最大最小特征缩放到［0，1］范围之间，避免因数据中的特征差距太大使得模型训练困难和部分重要特征所匹配的权重较小降低模型的性能的问题。

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{14}$$

其中：$x_{\max}$为最大值，$x_{\min}$为最小值。

再将数据的标签进行 Label 编码，将标签转换为机器学习模型能够理解和处理的数字形式，从而使模型能够更好地进行学习和预测，同时也可以节省内存空间和计算资源。最后，按 7∶3 的比例将 UNSW-NB15 数据集划分，其中正常类型总计 93 000 个样本，划分后训练集 64 974 个样本，测试集 28 026 个样本，具体划分结果如表 4 所示。

表 4 UNSW-NB15 数据集类型

入侵类型	总计/个	训练集/个	测试集/个	标签
Analysis	2 677	1 893	784	0
Backdoor	2 329	1 633	696	1
Dos	16 353	11 395	4 958	2
Exploits	44 525	31 197	13 328	3
Fuzzers	24 246	17 022	7 224	4
Generic	58 871	41 282	17 589	5
Normal	93 000	64 974	28 026	6
Reconnaissance	13 987	9 794	4 193	7
Shellcode	1 511	1 054	457	8
Worms	174	127	47	9

2.3　模型评估

为了有效地评估和比较不同模型的性能，本文使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 F_1 等指标评价模型[20]。

准确率（Accuracy）是指模型预测到的正常与恶意节点的正确的样本数量与总样本数量之比。即正确预测正常与恶意节点的样本数占总样本数的比例。计算公式为：

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{15}$$

其中：TP 表示真正例（模型将正类别正确地预测为正类别）、TN 表示真负例（模型将负类别正确地预测为负类别）、FP 表示假正例（模型将负类别错误地预测为正类别）、FN 表示假负例（模型将正类别错误地预测为负类别）。

精确率（Precision）是指模型在所有预测的正常与恶意节点为正类别的样本中，实际为正类别的比例。即预测为正类别且实际为正类别的样本数占预测为正类别的样本总数的比例。计算公式为：

$$Precision = \frac{TP}{(TP + FP)} \tag{16}$$

召回率（Recall）：召回率是指实际为正类别的样本中，被模型预测为正类别的比例。即真正例占实际为正类别的样本总数的比例。计公式为：

$$Recall = \frac{TP}{(TP + FN)} \tag{17}$$

F_1 值：F_1 值是精确率和召回率的调和平均。它综合考虑了模型的查准率和查全率。F_1 值越高，表示模型在精确率和召回率之间取得了更好的平衡。计算公式为：

$$F_1 = \frac{2(Preciosion * Recall)}{(Preciosion + Recall)} \tag{18}$$

2.4　BOA-DF-LightGBM 同类对比实验

为说明本文提出模型的有效性，将本文模型与 DF 模型，DF-LightGBM 模型，GA-DF-LightGBM 模型进行对比。其中 GA-DF-LightGBM 为使用遗传算法进行参数优化。

如表 5 所示，本文所提方法各项指标最好，其中本文所提方法较 DF 准确率提高了 2%，达到了 95.15%，并且本文方法较使用遗传算法进行参数优化模型的准确率更高。这说明棕熊优化算法较遗传算法具有更强的全局搜索能力，能够更好地找出全局最优参数避免陷入局部最优。

表 5　BOA-DF-LightGBM 同类对比实验指标　　%

模型	准确度	召回率	精确率	F_1
DF	93.55	93.55	93.73	93.59
DF-LightGBM	94.93	94.93	94.95	94.94
GA-DF-LightGBM	94.98	94.98	95.01	94.99
BOA-DF-LightGBM	**95.15**	**95.15**	**95.18**	**95.16**

ROC 曲线展示了模型的真正例率和假正例率之间的权衡。曲线下的面积（AUC，area under the curve）是衡量模型性能的指标，*AUC* 值越大，模型性能越好。如图 5 所示，实线为本文所提方法，点线为 DF-LightGBM，虚线为 DF-LightGBM，点虚线为 DF，由图中可知本文提出模型的效果更好。

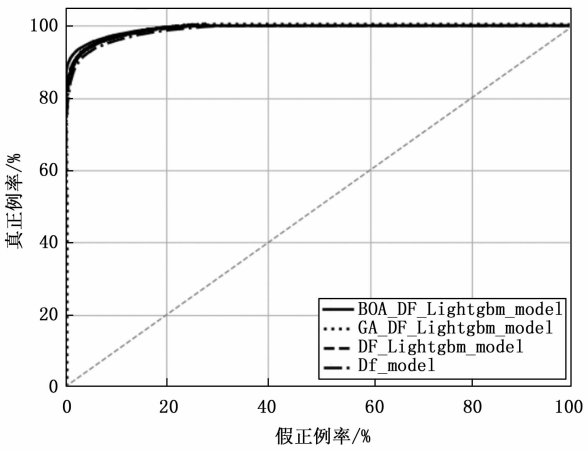

图 5　模型 ROC 曲线

PR 曲线展示了模型的精确率（Precision）和召回率（Recall）之间的关系。*PR* 曲线对于处理类别不平衡的数据集尤其有用，因为它能够更好地反映模型在检测少数类时的表现。如图 6 所示，本文所提方法在检测少数类时性能更好。

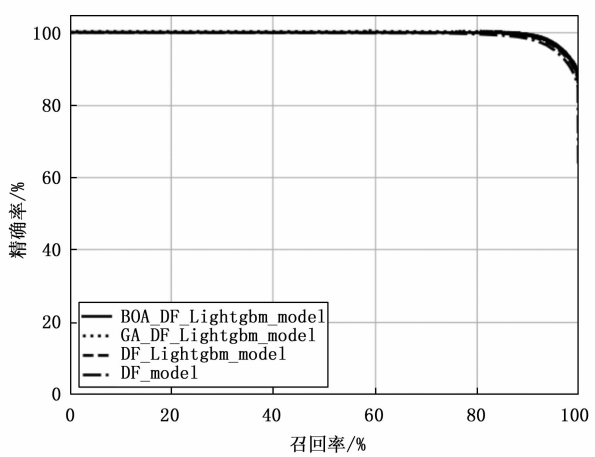

图 6　模型 PR 曲线

如图 7 所示，在 UNSW _ NB15 数据集中，本文所提模型的总识别正确样本最多，验证了本文提出模型对于入侵检测数据不平衡问题的有效性。

2.5　与其他模型的对比实验

为了更好地验证本文所提模型对入侵检测的有效性，本文使用逻辑回归、KNN、决策树（Decision Tree）、MLP、DF、GRU、LSTM 和 CNN-LSTM 等模型与本文所

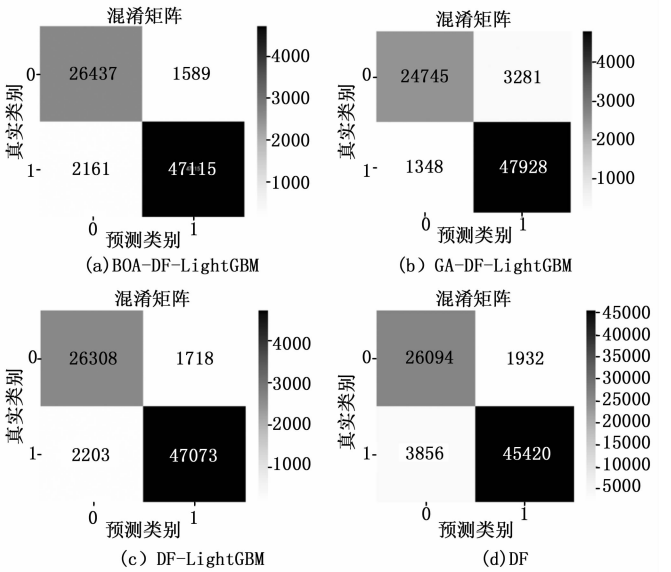

图 7 各模型的混淆矩阵

提方法进行对比分析。

如表 6 所示，在 UNSW _ NB15 数据集中，逻辑回归的入侵检测准确率为 89.93%，KNN 的入侵检测准确率为 91.78%，Decision Tree 的入侵检测的准确率为 93.70%，Extra Tree 的入侵检测准确率为 94.74%，Random Forest 的入侵检测准确率为 94.96%，MLP 入侵检测准确率为 93.29%，DF 的入侵检测准确率为 94.98%，GRU 的入侵检测准确率为 93.15%，LSTM 的入侵检测准确率为 93.21%，CNN-LSTM 的入侵检测准确率为 93.27%，DF-LightGBM 的入侵检测准确率为 94.93%，GA-DF-LightGBM 的入侵准确率为 94.98%，本文所提方法的入侵检测准确率为 95.15%，其中本文所提方法的准确率最高。除此外所提方法的各项指标都优于其他模型，验证了本文所提方法的有效性和优异性。

表 6 各模型的入侵检测指标 %

数据集	模型	*Accuracy*	*Recall*	*Precision*	F_1
UNSW_NB15	LogisticRegression	89.93	89.93	90.29	89.68
	KNN	91.78	91.78	91.81	91.79
	Decision Tree	93.70	93.70	93.70	93.70
	MLP	93.29	93.29	93.41	93.32
	GRU	93.15	93.15	93.19	93.16
	LSTM	93.21	93.21	93.28	93.23
	CNN-LSTM	93.27	93.27	93.28	93.28
	DF	93.55	93.55	93.73	93.59
	DF-LightGBM	94.93	94.93	94.95	94.94
	GA-DF-LightGBM	94.98	94.98	95.01	94.99
	BOA-DF-LightGBM	**95.15**	**95.15**	**95.18**	**95.16**

2.6 数据不平衡实验

为验证本文提出模型解决入侵检测数据不平衡问题的有效性。本节将进行更为严苛的数据不平衡实验进行验证。本节将上述训练集中的入侵类型数据减少 40%以形成更为严苛的数据不平衡情况。具体数据集分割情况如表 7 所示。表中的 Normal 类型数据数量不变，其余入侵类型的训练集变为原先的 60%，测试集数量不变。

表 7 数据不平衡实验数据集分割

入侵类型	训练集/个	测试集/个	标签
Analysis	1 135	784	0
Backdoor	979	696	1
Dos	7 161	4 958	2
Exploits	18 718	13 328	3
Fuzzers	10 213	7 224	4
Generic	24 769	17 589	5
Normal	64 974	28 026	6
Reconnaissance	5 876	4 193	7
Shellcode	632	457	8
Worms	76	47	9

与上文相同使用了逻辑回归、KNN、决策树（Decision Tree）、Extra Tree、Random Forest、MLP、DF、GRU、LSTM 和 CNN-LSTM 等模型与本文所提方法进行对比分析。其结果如表 8 所示。由表 8 可看出当数据不平衡情况加重后，模型出现了不同程度的下降。其中 CNN-LSTM 模型下降了 2.46%；DF 模型下降了 2%，DF-LightGBM 模型下降了 1.92%；GA-DF-LightGBM 模型下降了 1.91%；本文提出模型 BOA-DF-LightGBM 下降了 0.92%。在此情况下本文提出模型较 DF 模型预测准确度提高了 2.68%。由数据可知本文提出模型在更严重的数据不平衡情况下表现良好，并且 DF-LightGBM 等模型的下降程度相较于传统神经网络模型等表现也较好，验证了 DF-LightGBM 对于解决数据不平衡问题的有效性和优越性。而 BOA-DF-LightGBM 模型的准确率较 GA-DF-LightGBM 提高了 1.11%，说明了棕熊优化算法较遗传算法具有更强的全局搜索能力，能够更好地找到全局最优解不会陷入局部最优。

表 8 各模型数据不平衡实验入侵检测指标 %

数据集	模型	*Accuracy*	*Recall*	*Precision*	F_1
UNSW_NB15	LogisticRegression	80.13	80.13	80.29	80.08
	KNN	85.78	85.78	85.31	85.79
	Decision Tree	85.10	85.71	85.12	85.14
	MLP	87.17	87.17	87.21	87.34
	GRU	89.05	89.05	89.15	89.11
	LSTM	89.77	89.77	89.98	89.93
	CNN-LSTM	90.81	90.81	90.88	90.85
	DF	91.55	91.55	91.73	91.59
	DF-LightGBM	93.01	93.01	93.05	93.04
	GA-DF-LightGBM	93.12	93.12	93.07	93.09
	BOA-DF-LightGBM	**94.23**	**94.23**	**94.28**	**94.26**

3　结束语

互联网入侵检测通过监测和分析系统的运行情况，检测潜在的网络入侵行为。可以防止潜在的网络攻击和安全威胁对系统造成的损害，保障能源供应的安全与可靠性。本文针对入侵检测的效率低和入侵检测数据集中正常行为和恶意行为的比例可能存在不平衡，导致模型更倾向于预测出现频率更高的类别，而忽略其他潜在的风险等问题，提出了一种基于 BOA-DF-LightGBM 的入侵检测方法。

将深度森林和 LightGBM 结合作为入侵检测模型，更好地处理不平衡数据问题，提高整体模型的泛化能力。并通过全局搜索能力强大的棕熊优化算法对模型进行参数调优进一步提升模型的预测准确度。可以平衡不同类别数据的重要性，提高对恶意行为的检测率，缓解入侵检测数据不平衡的问题。经 UNSW _ NB15 数据集验证所提方法，BOA-DF-LightGBM 模型较其他模型指标更为优异，预测准确率达到 95.15%，较 DF 提升了近 2%。为进一步验证其对数据不平衡问题的能力，通过更严苛的数据不平衡实验得出，BOA-DF-LightGBM 模型在数据不平衡实验中的准确率为 94.23%，较 DF 提升了近 2.68%，较神经网络模型提升了近 3.42%。充分验证了本文提出模型对于解决入侵检测数据不平衡问题的有效性。

参考文献：

[1] 王国华. 基于机器学习的配电网电力信息物理系统入侵检测方法研究 [D]. 兰州：兰州交通大学，2022.

[2] RAJAPAKSHA S, KALUTARAGE H, AL-KADRI M O, et al. Ai-based intrusion detection systems for in-vehicle networks: a survey [J]. ACM Computing Surveys, 2023, 55 (11): 1-40.

[3] DASH S K, DASH S, MAHAPATRA S, et al. Enhancing DDoS attack detection in IoT using PCA [J]. Egyptian Informatics Journal, 2024, 25: 100450.

[4] BHAYO J, SHAH S A, HAMEED S, et al. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks [J]. Engineering Applications of Artificial Intelligence, 2023, 123: 106432.

[5] YIN Y H, JANGJJ, XU W, et al. IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset [J]. Journal of Big Data, 2023, 10 (1): 16-26.

[6] ANYANWU G O, NWAKANMA C I, LEE JM, et al. RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network [J]. Ad Hoc Networks, 2023, 140: 103026.

[7] SINGH K S, SINGH K J. Network intrusion detection system using decision tree and KNN algorithm [C] //Proceedings of the 2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control (PARC), IEEE, 2024: 275-280.

[8] WANG X, LIU J, ZHANG C. Network intrusion detection based on multi-domain data and ensemble-bidirectional LSTM [J]. EURASIP Journal on Information Security, 2023 (1): 5.

[9] WANG C, SUN Y, WANG W, et al. Hybrid intrusion detection system based on combination of random forest and autoencoder [J]. Symmetry, 2023, 15 (3): 568.

[10] ZHAI F, YANG T, CHEN H, et al. Intrusion detection method based on CNN - GRU - FL in a smart grid environment [J]. Electronics, 2023, 12 (5): 1164.

[11] KIM Y, CAMACHO D, CHOI C. Real-time multi-class classification of respiratory diseases through dimensional data combinations [J]. Cognitive Computation, 2024, 16 (2): 776-787.

[12] ABDULHAMMED R, FAEZIPOUR M, MUSAFER H, et al. Efficient network intrusion detection using pca-based dimensionality reduction of features [C] //Proceedings of the 2019 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2019: 1-6.

[13] ABDALLAH M, AN LE KHAC N, JAHROMI H, et al. A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs [C] //Proceedings of the Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021: 1-7.

[14] 闫海涛，张之义，朱晓明，等. 基于 WOA-XGBoost 模型的网络入侵检测 [J]. 计算机测量与控制，2023，31 (3)：127-133.

[15] 田小芳. 基于人工蜂群算法的计算机网络 DDoS 攻击检测方法 [J]. 计算机测量与控制，2023，31 (12)：28-33.

[16] 徐东方，徐洪珍，邓德军. 基于 CNN-BLSTM-XGB 的入侵检测 [J]. 计算机工程与设计，2024，45 (3)：676-83.

[17] 毛智超，吴黎兵，马亚军，等. 基于 DBN 与带注意力机制 GRU 的 CAN 总线入侵检测模型 [J]. 武汉大学学报（理学版），2023，69 (5)：598-608.

[18] ZHOU Z H, FENG J. Deep forest [J]. National Science Review, 2018, 6 (1): 74-86.

[19] MOUSTAFA N, SLAY J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) [C] //Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS). IEEE, 2015.

[20] 王　楠，侯　涛，牛宏侠. 多尺度特征融合的铁轨异物入侵检测研究 [J]. 西安交通大学学报，2024，58 (9)：139-153.