基于优化的堆叠集成区块链 DDoS 攻击检测方法

王春东[1,2,3],郑泽霖[1,3]
(1. 天津理工大学 计算机科学与工程学院,天津 300384;
2. 天津公安警官职业学院,天津 300382;
3. 计算机病毒防治技术国家工程实验室,天津 300384)

摘　要:分布式拒绝服务(Distribute Denial of Service,DDoS)攻击是常见的网络攻击手段之一,对于影响力日益增长的区块链网络构成了较大的威胁。包含堆叠法(Stacking)在内的集成学习模型在 DDoS 攻击检测方面有很大前景,而 Stacking 在面对不同类型数据集时需要调整学习器组合。该文使用 Stacking 方法检测区块链 DDoS 攻击,利用贝叶斯优化确定各学习器超参数,同时还使用算术优化算法(Arithmetic Optimization Algorithm,AOA)选择基学习器的组合,来解决需要手动调节学习器的问题。在区块链网络攻击流量数据集和比特币交易所交易数据上分别进行了实验,通过准确率、攻击数据漏报率和宏平均精准率三种评价指标进行对比,该方法在这两种不同类型数据集上的性能均优于其他三种常见的集成学习算法。还通过改变实验数据集大小探究出攻击检测性能会随着数据集的增大而上升。通过实验可以证明该方法可以有效检测不同类型数据集上的区块链 DDoS 攻击。

关键词:网络空间安全;区块链;DDoS 攻击检测;集成学习;堆叠;算术优化算法
中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1673-629X(2025)02-0054-09
doi:10.20165/j.cnki.ISSN1673-629X.2024.0310

Optimized Stacking Ensemble Learning Blockchain DDoS Attack Detection Method

WANG Chun-dong[1,2,3],ZHENG Ze-lin[1,3]
(1. School of Computer Science and Engineering,Tianjin University of Technology,Tianjin 300384,China;
2. Tianjin Public Security Police Profession College,Tianjin 300382,China;
3. National Engineering Laboratory for Computer Virus Prevention and Control Technology,Tianjin 300384,China)

Abstract:Distribute Denial of Service (DDoS) is one of the common network attack methods,which poses a significant threat to the increasingly influential blockchain network. Ensemble learning models,including the Stacking method,have great potential in DDoS attack detection,and Stacking requires adjusting the combination of learners when facing different types of datasets. We use the Stacking method to detect blockchain DDoS attacks,use Bayesian optimization to determine the hyperparameters of each learner,and also use the Arithmetic Optimization Algorithm (AOA) to select a combination of base learners to solve the problem of manually adjusting learners. The experiments are conducted on blockchain network attack traffic datasets and Bitcoin exchange trading data,and the comparison is carried out by three evaluation indicators:accuracy,attack data omission rate,and macro average accuracy. The proposed method is superior to the other three common ensemble learning algorithms in terms of performance on these two different types of datasets. We also explore how the attack detection performance increases with the increase of the experimental dataset size. Through experiments,it can be proven that the proposed method can effectively detect blockchain DDoS attacks on different types of datasets.

Key words: cyberspace security; blockchain; distribute denial of service attack detection; ensemble learning; stacking; arithmetic optimization algorithm

0　引　言

分布式拒绝服务(Distribute Denial of Service)攻击是互联网一直以来所面临的经典威胁,它在发动时会调用大量数据发送节点,通过集体行为极大地干扰

收稿日期:2024-06-29　　**修回日期**:2024-10-30
基金项目:国家自然科学基金联合基金项目(U1536122);国家重点研发计划"区块链"重点专项(2023YFB2703900)
作者简介:王春东(1969-),男,博士,教授,博导,CCF 会员(16230M),研究方向为网络信息安全、区块链;郑泽霖(2000-),男,硕士研究生,研究方向为区块链攻击检测。

攻击目标提供正常服务的能力[1]。即便相关的科学研究和商业方案已经很多,但因为其可不依赖某一特定安全漏洞实施,且防御成本远高于攻击成本,DDoS 攻击从未减弱。相反在目前物联网迅速扩张的情况下,更多缺乏安全保障的设备成为了潜在的攻击源,攻击者可以轻松控制大量具有天然弱安全性的物联网设备资源以发动恶意攻击[2]。根据华为公司公布的《2023 年全球 DDoS 攻击现状与趋势分析》,DDoS 攻击频次继续呈增长趋势,2023 年全年 DDoS 攻击频次为 2022 年攻击频次的 1.6 倍,为 2021 年攻击频次的 1.8 倍。在攻击强度方面,2023 年月度平均峰值带宽最大值为 121 Gbps,首次突破 100 Gbps,攻击强度也呈逐年上升的趋势[3]。

物联网、人工智能以及区块链等技术的不断进步为智慧城市、智慧工业以及智慧农业等智能场景的发展奠定了基础。海量的物联网设备在被制造时大多数都存在缺少防火墙软件和密钥口令较弱等安全问题。当这些存在安全隐患的物联网设备在物联网生态环境中运行时就极易被攻击者使用 Mirai 和 Aidra 等恶意代码感染进而被控制[4]。区块链技术可以为物联网提供点对点直接互联的传输方式,还可以充分利用分布在不同位置的数以亿计闲置设备,这使得物联网与区块链的融合应用越来越多。同时区块链技术在金融、医疗、教育等多个领域的重要性不断上升,因此区块链安全方面的研究也日益受到关注。

尽管区块链是可验证且不可变的,但它也容易受到不同的攻击。DDoS 攻击者可以通过让区块链网络充斥更多交易等方式来降低系统速度,使得用户无法进行交易或参与挖矿,甚至可能导致少数矿工进行集中挖矿,从而破坏区块链规则,对区块链网络产生重大影响。位于日本东京的比特币交易所 Mt. Gox 曾报告多起由于黑客利用 DDoS 攻击引起的安全事件,导致其损失了数亿美元,最终申请破产[5]。因此需要针对区块链 DDoS 攻击进行相关研究。

目前 DDoS 攻击的种类繁多且复杂,国内外对于 DDoS 攻击检测的方法研究主要集中于三大类,分别是基于统计的方法、基于传统机器学习的方法和基于深度学习的方法[6]。在基于统计的检测方法中,David 等人[7]在 DDoS 攻击检测时通过计算广义熵来识别攻击流量,并根据网络条件对阈值进行自动调整,但该方法仅计算了两种流量属性的熵值,且实验数据集较老,不能有效地模拟如今的网络真实环境。王智等人[8]提出了一种基于多级检测模块的方法,通过联合熵和半监督模型来检测软件定义网络中的 DDoS 攻击。基于统计的方法在研究过程中使用信息熵作为一个指标已较为常见,但大部分现有研究在熵值度量方式和计算熵值所采用的特征上选择较少,缺乏有效的对比,导致误报率较大。同时该类方法中设定的相关阈值以及规则等常需要有足够经验的专业人员进行人工设定,自适应性相对较差。

近年来为了提升分类效果,深度学习成为了很多研究的主要内容。Cil 等人[9]通过训练深度神经网络实现了 DDoS 攻击检测,在 CIC-DDoS 2019 数据集上取得了较好的分类准确率。Dai 等人[10]提出了一种基于区块链网络层的跨多层卷积神经网络模型的分布式 DDoS 攻击流量检测方法,从多个层次感知攻击流量的详细特征,在 CSE-CIC-IDS 2018 和区块链网络层真实数据的混合数据上取得了较好的准确率。深度学习的检测方法可以通过将稀疏特征映射为更低维度的稠密特征来更有效地表现离散特征,但不适用于包含连续性数值特征的数据集[11]。而且由于神经网络的参数量较大,其前馈速度相较于其他两类检测方法会更慢,在面对大规模攻击流量时存在检测性能的压力。

基于传统机器学习的检测方法中,Tonkal 等人[12]基于近邻成分分析提出了一种 DDoS 检测方法,该方法利用近邻成分分析对数据特征进行重要性评分,并生成重要特征子集来训练决策树(Decision Tree, DT)、支持向量机(Support Vector Machines, SVM)等多种传统机器学习模型用于 DDoS 检测。Sahoo 等人[13]提出了一种基于 SVM 的 DDoS 检测模型,利用核主成分分析将流量进行数据降维,使用改进的核函数降低噪声特征对分类的影响,并使用遗传算法对分类器 SVM 进行优化。在检测区块链 DDoS 攻击上,J. Eduardo 等人[14]在以太坊上研究了一种发送大量价值较低的交易的低价 DoS(under-price DoS)攻击的影响,得出低价 DoS 攻击会使平均待处理时间增加 42.16% 的结论,同时使用多种传统机器学习模型对攻击进行检测,证明了传统机器学习技术在检测低价 DoS 攻击的应用中性能表现较好,并指出随机森林(Random Forest, RF)的检测效果最好。Sayadi 等人[15]利用 SVM 识别正常比特币交易中的异常值,应用 K-means 聚类将相似的异常值与同类型的异常值进行分组,但此方法在检测 DDoS 攻击时有较大的误报率。基于传统机器学习的检测方法在实际训练过程中,易受到数据集不平衡以及特征不具备代表性等问题的影响,导致模型无法适应多种检测环境,存在泛化性弱、适用性差等问题[16]。

集成学习是通过在数据集上构建多个学习器进行学习,并使用某种规则将全部结果进行整合,从而获得比单一学习器更高的泛化性能的策略。Abdulla 和 Hasoun[17]对集成学习检测 DoS 攻击进行回顾,指出混合策略的结果优于单一算法的最准确结果。同时他们

指出采用集成堆叠(Stacking)方式的集成学习方法来解决网络攻击问题具有巨大的前景,并且可以通过试验各种学习器的组合和模型中的迭代次数来进行改进。

综上所述,目前已有多种 DDoS 攻击检测方法,但是仍存在着检测时间较长、模型泛化性较弱以及面对不同类型数据集适用性较差等问题。同时针对区块链网络的 DDoS 攻击检测方法相对较少。因此该文提出了一种基于算术优化算法(Arithmetic Optimization Algorithm,AOA)优化的 Stacking 集成学习区块链 DDoS 攻击检测方法。

该文的主要工作有:(1)采用贝叶斯优化调节超参数和 Stacking 集成学习方法检测区块链 DDoS 攻击,能够提升模型性能,降低模型受到特征不具备代表性以及数据集不平衡等问题的影响,增加模型的泛化性;(2)提出了 AOA-Stacking 模型,在面对不同类型的数据集时,可以由 AOA 算法动态地选取评价指标最高的一组学习器组合作为 Stacking 模型的基学习器,从而使得模型适用于不同数据集,提高了模型的适用性;(3)使用了区块链网络攻击流量数据集[18](BNaT)和比特币交易所交易数据[19]这两种不同类型的区块链 DDoS 攻击数据集进行实验,验证了 AOA-Stacking 模型在不同数据集上均获得了较好的性能。

1 基础理论

1.1 贝叶斯优化

贝叶斯定理是以概率论为基础的,能够根据事物特征计算其成为某种类型的概率大小,即可以计算出后验概率。在 B 事件已经发生的前提下,A 事件与 B 事件同时发生的概率的计算公式为:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \tag{1}$$

贝叶斯优化假设了一个函数关系,这个函数关系是“黑盒”函数,虽不能通过梯度下降的方式获得最优解,但是可以通过先验的样本点根据贝叶斯定理得到这个函数的后验分布。通过对目标函数形状的学习,选择最有希望的组合进行下一步迭代,直至找到最优解。

1.2 算术优化算法

数字通过加法、减法、乘法和除法这四种方法得到了不同程度的缩放,这个过程与算法寻优的方式极其相似,因此 Abualigah 等人[20]在 2021 年提出 AOA 算法,AOA 算法流程如图 1 所示。AOA 算法在初始化阶段会从一组随机生成的候选解 X 开始,在每次迭代中将得到的最优解视为至今为止获得的全局最优解。通过数学优化加速器(Math Optimizer Accelerated,MOA)确定接下来的具体算法搜索阶段,MOA 的数学表达式为:

$$\mathrm{MOA(C\_Iter)} = \mathrm{Min} + \mathrm{C\_Iter} \times \left(\frac{\mathrm{Max} - \mathrm{Min}}{\mathrm{M\_Iter}}\right) \tag{2}$$

式中,MOA(C_Iter)表示第 t 代的数学优化器加速函数的值,C_Iter 表示到目前为止的迭代次数,M_Iter 表示最大迭代次数,Max 和 Min 分别表示数学优化器加速函数的最大值和最小值。

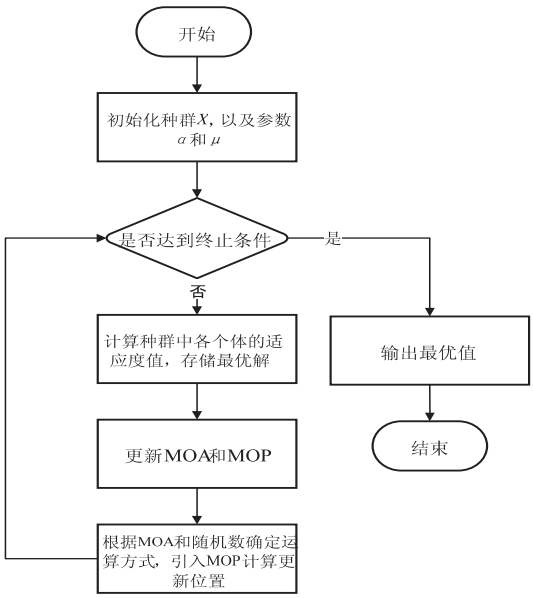

图 1 AOA 算法流程

之后比较 MOA 与在(0,1)之间的随机数 r_1 的大小,当 r_1 > MOA 时进入勘探阶段,执行乘法以及除法的运算方式;否则进入开发阶段,执行加法以及减法的运算方式。在算法搜索阶段引入数学优化器概率(Math Optimizer Probability,MOP),其数学表达式为:

$$\mathrm{MOP(C\_Iter)} = 1 - \frac{\mathrm{C\_Iter}^{1/\alpha}}{\mathrm{M\_Iter}^{1/\alpha}} \tag{3}$$

式中,MOP(C_Iter)表示第 t 代的数学优化器概率函数的值,C_Iter 表示到目前为止的迭代次数,M_Iter 表示最大迭代次数,α 是控制迭代寻优过程中搜索精度的敏感参数。

勘探阶段具有高维度的分散性,可以在较少的迭代次数推断出接近最优的解,执行全局搜索操作。同时为了勘探尽量不同的区域和产生更加多元的解,算法考虑了随机比例系数。勘探阶段位置更新的数学表达式为:

$$x_{i,j}(\mathrm{C\_Iter}+1) = \begin{cases} x_j^* \div (\mathrm{MOP}+\varepsilon) \times ((\mathrm{UB}_j - \mathrm{LB}_j) \times \mu + \mathrm{LB}_j), \\ \quad r_2 > 0.5 \\ x_j^* \times \mathrm{MOP} \times ((\mathrm{UB}_j - \mathrm{LB}_j) \times \mu + \mathrm{LB}_j), \mathrm{otherwise} \end{cases} \tag{4}$$

式中,$x_{i,j}(\mathrm{C\_Iter}+1)$ 表示第 i 个解的第 j 个维度下一次迭代的值,x_j^* 表示到目前为止所有解中第 j 维度的最优值,UB_j 和 LB_j 分别表示第 j 维度的上界和下界,ε 为防止分母为零而设置的小整数,r_2 为一个(0,1)之间的随机数,μ 表示调节搜索过程的控制参数并且根据多次实验确定其设定为 0.5。

开发阶段利用较低的分散性可以更容易接近目标,执行局部搜索操作。加减两种运算符在几个密集区域上对搜索区域进行深入探索,协助勘探阶段的搜索策略在保持候选解多元性的同时寻找最优解。开发阶段位置更新的数学表达式为:

$$x_{i,j}(\mathrm{C\_Iter}+1)=\begin{cases}x_j^* \div \mathrm{MOP}-((\mathrm{UB}_j-\mathrm{LB}_j)\times\mu+\mathrm{LB}_j), r_3>0.5\\ x_j^* \times \mathrm{MOP}+((\mathrm{UB}_j-\mathrm{LB}_j)\times\mu+\mathrm{LB}_j), \mathrm{otherwise}\end{cases} \tag{5}$$

1.3　集成学习

根据基学习器集成模式的不同,集成学习算法主要可分为并行化(Bagging)方式集成学习算法、序贯(Boosting)方式集成学习算法和堆叠(Stacking)方式集成学习方法。以 RF 为代表的 Bagging 算法会对数据集进行多次随机重采样得到多个训练集,并训练得到多个学习器,使用投票法等方式组合训练后的学习器。Bagging 算法的最终效果受基学习器性能以及数据集是否平衡的影响程度很大。以 XGBoost 为代表的 Boosting 算法会串行训练学习器,迭代中减少数据集中被正确分类数据的权重,最终根据表现加权组合基学习器。因此 Boosting 算法会更加倾向于学习错误率高的数据,更容易受到数据集中离群的错误数据影响。Stacking 则利用多种算法分类器训练原始数据,可以集成其他集成算法的优点。

2　区块链 DDoS 攻击检测方法

该文提出基于集成学习的 DDoS 攻击检测方法,Stacking 作为异质性的集成算法,可以集成多个不同的机器学习算法作为基分类器,因此受到基分类器性能以及数据集不平衡的影响相对较小。同时其性能普遍优于单个最优学习器性能且泛化性强,与 Bagging 算法和 Boosting 算法相比也更加稳定,因此该文采用 Stacking 集成学习的方法构建区块链 DDoS 攻击检测模型。

2.1　Stacking 方法

Stacking 是一种并行的集成学习算法,主要分为两层训练,第一层基学习层并行地训练出多个基学习器,之后将基学习器训练得到的结果汇总训练元学习器,即元学习器的输入是基学习器的输出。基学习层常使用 K 折交叉验证的方式,将原始训练集平分,选择其中一份作为验证集对学习器进行训练。Stacking 算法的模型结构如图 2 所示。

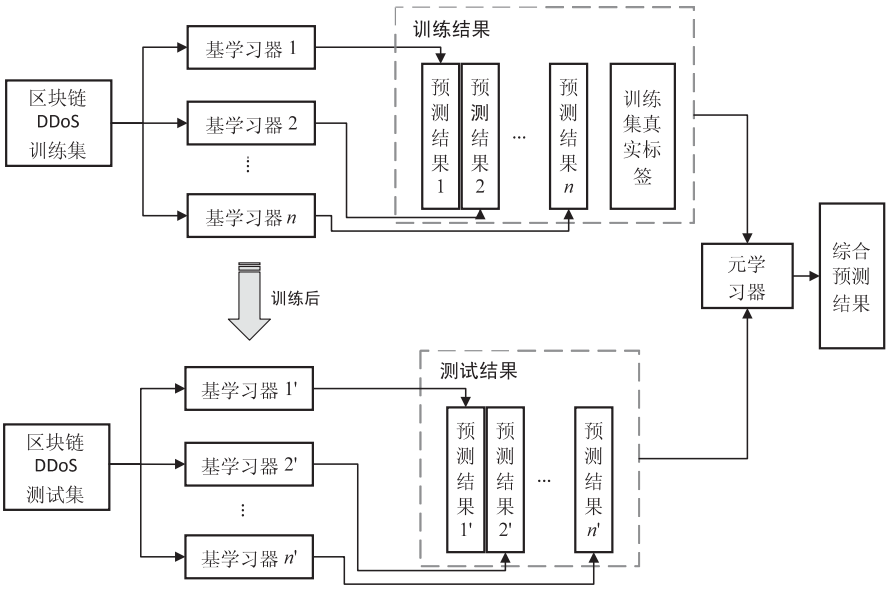

图 2　Stacking 模型结构

文中方法采用 5 折交叉验证,对于每个基分类器都采用相同的方式进行交叉验证。以基学习器 1 为例,将原始训练集随机均分为五份子数据集,每次选取其中的一份子数据集作为验证集,其余的四份作为训练集,经过训练会得到五个验证集预测值,把它们合并在一起作为预测结果 1。将原始测试集以相同的操作输入至训练后的基学习器 1' 中,对五个预测结果做求均值处理得到预测结果 1' 。

对于多个不同的基分类器进行多次上述重复操作以获得多个特征,将这些特征组合成元学习器的输入数据集。元学习器通过学习基学习器的预测结果,进行组合和加权等方式以最大化整体模型的性能,生成

最终的预测结果。

通过 Stacking 方法,不同基学习器的各自优势均可以得到充分体现。但是在实现过程中还要考虑基学习器之间的配置问题,比如各基学习器之间的相关性应当尽量减小,从而使得模型之间的优势可以互补。同时各基学习器之间的性能差距过大也会很大程度地影响整体模型的性能表现。

2.2 基学习器配置

Stacking 中的学习器配置问题一直是学者们研究讨论的热点,如有多个基学习器可供选择,其组合方式的数量会呈指数级增长,如果简单通过遍历的方式来选取最优组合会导致计算成本的大幅增加。目前 Stacking 学习器配置方法多采用的是固定搭配,即对于某个具体问题和数据集设计单独的 Stacking 模型,这种方式对于数据变化的适用性和灵活性较差。目前 AOA 算法已应用于多个领域,且显著具有结构简单、收敛速度快等优势,故该文的检测方式运用 AOA 算法进行动态最优基学习器组的搜索。在文中方法中,Stacking 的基学习器配置可以由公式 6 表示。

$$I = \{B' \cdot M \mid B' \subseteq B\} \tag{6}$$

式中,B 表示基学习器池中的所有候选学习器,B' 表示被选择的基学习器组合,M 表示元学习器。

I 中每一个学习器配置 x 所对应的 Stacking 模型在验证集上进行预测得到的验证集准确率 $A(x)$ 会被作为评价指标。即 x 对应个体的二进制串为 C_x,其适应度值的表达式为:

$$\text{Fitness}(C_x) = A(x) \tag{7}$$

文中方法使用 AOA 的目标就是在 I 中找到评价指标最优的学习器配置 x^*,其表达式为:

$$x^* = \text{argmax}\{A(x)\} \tag{8}$$

在确定了基学习器的配置方式后,为了进一步提升模型性能,还要考虑各学习器超参数的选择。

2.3 学习器超参数选择

超参数是在模型训练之前需要手动设定的参数,超参数控制了模型的结构以及学习的过程,一定程度决定了模型的性能。超参数的设定过程中需要不断调整超参数数值使得模型的预测值尽量与真实值靠近,这个过程被称为超参数优化。现有的超参数优化方法主要包括网格搜索、随机搜索以及贝叶斯优化方法[21]。网格搜索使用暴力穷举的方式,计算量较大,只适合较小规模的参数空间;随机搜索的速度虽然较快,但是容易遗漏重要信息;贝叶斯优化相较于网格搜索和随机搜索是序贯的,可以具有记忆并从迭代过程中不断学习,从而可以在更少的迭代次数中得到最优解。因此,文中方法使用贝叶斯优化进行超参数的选择。

记 $f(x)$ 是从超参数向量 x 到模型泛化性能的映射,其中 $x \in X$,$X \subseteq R^l$,X 为 l 维的超参数空间。假定已知的数据集合为 $D_{1:t} = (x_i, y_i)$,$i = 1, 2, \cdots, t$。该方法中 y_i 是模型在超参数 x_i 的情况下使用训练集通过五折交叉验证得到的准确率平均值。则超参数优化过程中使用的贝叶斯定理公式为:

$$P(f \mid D_{1:t}) = \frac{P(D_{1:t} \mid f)P(f)}{P(D_{1:t})} \tag{9}$$

式中,$P(f \mid D_{1:t})$ 是后验概率,为未知目标函数 $f(x)$ 通过已知数据集合 $D_{1:t}$ 不断修正的依据。贝叶斯超参数优化的目标是在超参数空间内寻找使得模型泛化性能最优的 l 维超参数 x^*。优化方向上,由于文中方法的评估标准是准确率,贝叶斯优化建模为最大化问题,因此贝叶斯超参数优化的目标为:

$$x^* = \text{argmax} f(x) \tag{10}$$

2.4 AOA-Stacking 方法

通过对集成学习具体方法、基学习器配置方式和学习器超参数选择等具体细节的设计确定,该文提出了一种基于 AOA 优化的 Stacking 集成学习区块链 DDoS 攻击检测方法,其总体结构如图 3 所示。

首先针对不同的数据集进行相应的数据预处理,数据预处理可以去除噪声,使数据集更加适应模型训练和预测的需求。其工作流程主要为获取数据集的原始特征信息,对于原始数据集中如交易 ID、时间戳等唯一属性进行去除。识别和清除所有重复的数据。在识别到数据缺省后,对缺失值进行补充。然后无量纲化处理数据,无量纲化分为归一化和标准化,该文选择数据标准化对数据进行缩放。针对不同的数据集将数据的标签值转化为数值,二分类数据集用 0、1 两个数值编号,三分类数据集转化为 0 到 2 的数值编号,编号与输入的标签顺序一一对应。

之后将预处理得到的标准数据集进行拆分,划分为训练集、验证集以及测试集。所有基学习器层的算法都使用训练集通过贝叶斯超参数优化算法进行优化和训练,同时因为基学习器的性能最优不代表组合后的 Stacking 模型性能一定最优,所以对每个参与了贝叶斯参数优化的算法都选取不少于两个性能较优的模型放入基学习器池中参与基学习器的选择和构建。

使用 AOA 算法初始化一个二进制序列,二进制序列中的每一位都与基学习器池中的某一个模型相对应,将对应的基学习器组与元学习器结合构建 Stacking 模型,通过 Stacking 模型对验证集的预测结果得到准确率数值并传回给 AOA 算法,AOA 算法更新二进制序列。如此循环直至到达 AOA 算法设定的最大迭代次数,输出性能最好的二进制序列,得到最优的基学习器组合。

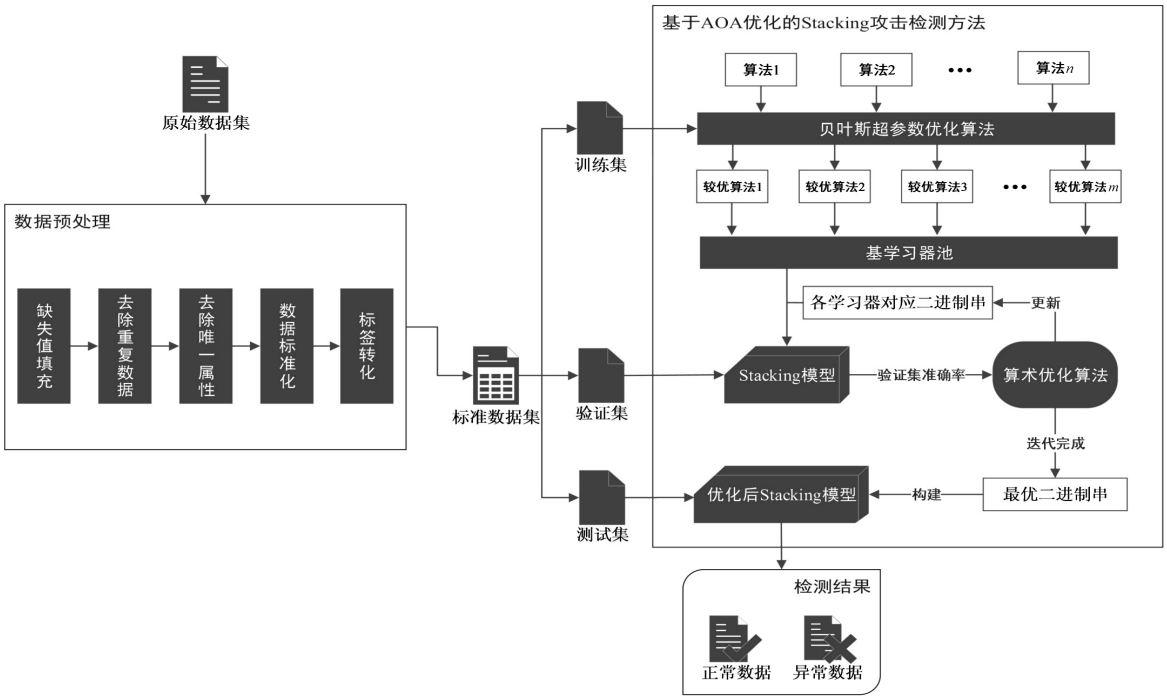

图 3　基于 AOA 优化的 Stacking 集成学习区块链 DDoS 攻击检测方法总体结构

3　实验与分析

3.1　实验设计

(1)实验环境。实验环境为 CPU Intel i7-8565U,内存 8 GB,Python 3.8.6。

(2)实验方案。为了验证 AOA-Stacking 检测方法的表现效果,使用决策树分类算法(DTC)、逻辑回归分类算法(LR)、K-近邻分类算法(KNN)、高斯朴素贝叶斯算法(GaussianNB)、岭分类算法(Ridge)和随机森林算法(RF)参与模型的构建,其中 GaussianNB 算法没有参数可供优化,其余学习器优化的超参数及寻优范围详见表 1。并且与目前主流的基于 Bagging 的 RF 算法以及基于 Boosting 的 XGBoost 和 AdaBoost 算法这三种集成学习算法进行了对比。

表 1　实验算法超参数优化

学习器	算法名称	寻优超参数及范围
基学习器	DTC	最大深度(50,500); 最大叶节点数(10,100)
	LR	最大迭代次数(5×10^1,5×10^3); 正则化系数的倒数(0.01,0.2)
	KNN	邻居节点数量(1,15)
	Ridge	正则化系数(1×10^{-7},1×10^{-2}); 类别关联权重={0:1,1:b}; b(1,32)
	RF	树的数量(3,15); 树的最大深度(2,32)
元学习器	LR	最大迭代次数(5×10^1,5×10^3); 正则化系数的倒数(0.01,0.2)

(3)评价标准。评价标准包括准确率(Accuracy,ACC)、区块链攻击数据漏报率(Missing Alarm Rate,MAR)以及精准率(Precision)。准确率表示分类模型正确分类的数据量在总数据量中的占比;漏报率表示分类模型漏报为非区块链攻击数据的实际类型为区块链攻击数据的数据量在区块链攻击数据中的占比;精准率表示分类模型正确分类的数据量在所有被分类为区块链攻击数据中的占比。

对于多分类问题,精准率仅是计算某一类别的性能指标,为了能够描述整体的检测性能,实验使用宏平均精准率(macro precision,macro-P)来代替精准率。宏平均是指在均值的计算过程中使每个类别具有相同的权重,宏平均精准率最终的计算结果是每个类别的精准率的算术平均值。

3.2 实验数据集

实验部分使用基于以太坊的区块链网络攻击流量数据集 BNaT 以及比特币交易所交易数据集两种不同类型的有关区块链 DDoS 攻击的数据集,以验证 AOA-Stacking 方法在不同类型的数据集上的效果。

Khoa 等人[18]搭建了以太坊私有链网络获得的可以用于研究的区块链网络层攻击流量的数据集 BNaT,该数据集的攻击类型包括四种典型的网络攻击,分别是暴力破解攻击(Brute Password,BP)、拒绝服务攻击(DoS)、交易泛滥攻击(Flooding of Transactions,FoT)以及中间人攻击(Man in the Middle,MitM)。其中拒绝服务攻击是该文研究的攻击类型,同时交易泛滥攻击是指攻击目标通过向区块链网络发送空交易或无意义交易来延迟 PoW 区块链网络,当以太坊网络每秒的交易数量突然达到峰值时,挖矿节点会遇到流量过大和待处理交易队列已满等问题从而破坏以太坊网络的可用性,符合 DDoS 攻击性质。因此,该文将拒绝服务攻击数据和交易泛滥攻击数据作为区块链 DDoS 攻击数据进行实验。实验将 BNaT 数据集中的部分正常流量数据、拒绝服务攻击数据和交易泛滥攻击数据进行融合,融合后得到实验数据集 Set1。

Mt. Gox 交易所曾是规模较大的比特币交易所,报告过多起由于黑客利用 DDoS 攻击引起的安全事件,导致其损失了数亿美元,最终申请破产。Chaganti 等人[22]在回顾区块链生态系统中拒绝服务攻击时指出,Mt. Gox 在破产并停止服务后,交易数据被公开披露,这些交易数据可供研究并且最受欢迎。实验过程中使用 Vasek 等人[19]提供的数据,选取了该交易所受到区块链 DDoS 攻击最频繁的 2013 年 4 月的交易数据作为实验数据集 Set2。

同时为了探究不同数据集大小对于实验结果的影响,在实验数据集 Set2 上拆分出数据集大小分别为 10 万条、30 万条、60 万条以及 100 万条的四个实验数据集,实验数据集分类如表 2 所示。

表 2 实验数据集分类

实验数据集	特征数量	数据集大小/万
Set1	21	14
Set21	19	10
Set22	19	30
Set23	19	60
Set24	19	100

3.3 实验结果与分析

AOA-Stacking 方法在实验数据集 Set21 上寻找最优基学习器配置的过程中,设置种群大小为 30,记录 AOA 算法每次迭代所得到的最优验证集准确率,得到的收敛曲线如图 4 所示。通过图 4 可以看出算法能够在较少的迭代次数获得较好的准确率,并在不断迭代的过程中继续逐渐提升准确率数值。

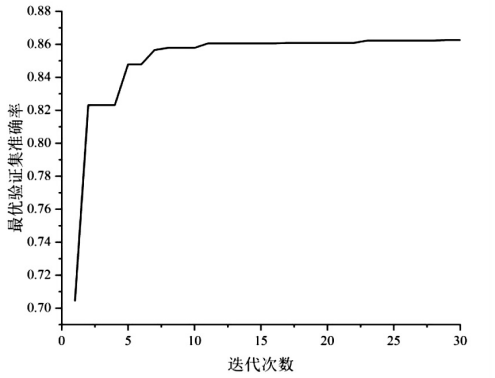

图 4 Set21 数据集上 AOA 算法收敛曲线

将 AOA-Stacking 与其他三种算法(RF、XGBoost 和 AdaBoost)分别在实验数据集 Set1 上进行实验,并且对准确率、攻击数据漏报率和宏平均精准率进行了对比,实验结果见表 3。

表 3 Set1 数据集上四种算法性能对比 %

模型	ACC	MAR	macro-P
RF	97.97	3.57	97.76
XGBoost	98.05	3.91	98.07
AdaBoost	97.48	5.28	97.60
AOA-Stacking	98.33	3.04	98.21

由表 3 的实验数据可知,相较于 RF、XGBoost 和 AdaBoost,AOA-Stacking 的准确率和宏平均精准率均最优,且攻击数据漏报率也最低。准确率分别提高了 0.36 百分点、0.28 百分点和 0.85 百分点,攻击数据漏报率分别降低了 0.53 百分点、0.87 百分点和 2.24 百分点,宏平均精准率分别提高了 0.45 百分点、0.14 百分点和 0.61 百分点。

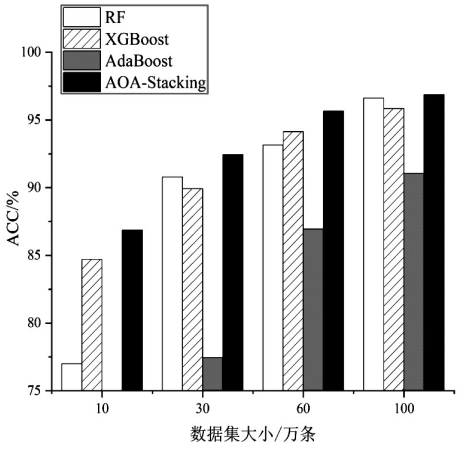

图 5 Set2 数据集上四种算法准确率对比

将 AOA-Stacking 与其他三种算法分别在实验数据集 Set2 上进行实验,图 5 为数据集大小分别为 10 万

条、30 万条、60 万条和 100 万条时四种算法的准确率对比。由于 AdaBoost 算法在实验数据集 Set21 上的各项性能均较差,会增大图表中坐标轴的刻度值范围,影响图表的直观性,因此在之后的图表中不再体现。

AdaBoost 算法在数据集大小为 10 万条所对应的准确率为 63.00%。通过图 5 可以看出,随着数据集大小的增加各算法的准确率也均随之上升,其中 AOA-Stacking 算法在所有数据集上的准确率都最高,并且在数据集较小的情况下优势更加明显。

图 6 是四种算法在 Set2 的四类数据集上攻击数据漏报率的对比图。AdaBoost 算法在数据集大小为 10 万条所对应的漏报率为 38.76%。通过图 6 可以看出攻击数据漏报率随数据集大小的增加而下降。RF 和 XGBoost 在数据集较大的情况下也能有较好的表现,但是图像上两个算法的线条多有交叉,说明两种算法在不同数据集上的漏报率不够稳定。AOA-Stacking 算法的漏报率始终处于最低状态,尤其在数据集较小的情况下,AOA-Stacking 算法的漏报率与其他算法对比有显著的降低。

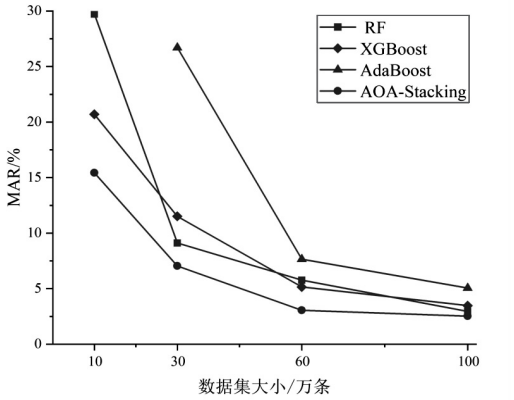

图 6　Set2 数据集上四种算法漏报率对比

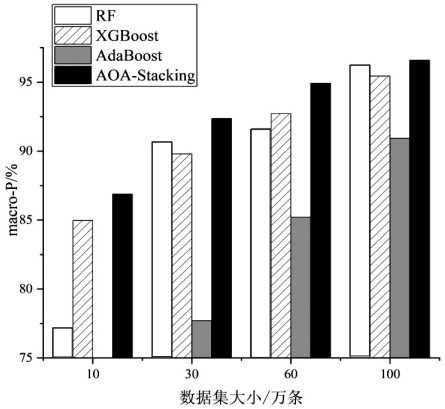

图 7　Set2 数据集上四种算法宏平均精准率对比

图 7 为四种算法在 Set2 的四类数据集上宏平均精准率的对比。AdaBoost 算法在数据集大小为 10 万条所对应的宏平均精准率为 62.87%。通过图 7 可以看出,随着数据集大小的增加各算法的宏平均精准率也均随之上升,同时 AOA-Stacking 方法在准确率和攻击数据漏报率均最优的情况下,仍能在各算法中保持最高的宏平均精准率。

经过上述各项指标之间的对比,可以充分地证明 AOA-Stacking 方法能够在不同类型的数据集上保持较好的模型性能,与其他三种集成学习算法相比 AOA-Stacking 方法可以在不同的数据集大小的情况下有效提高各项检测性能,有明显的优势,可以在区块链 DDoS 攻击检测中发挥显著效果。

4　结束语

该文提出一种基于 AOA 优化的 Stacking 集成学习 DDoS 攻击检测方法,结合了贝叶斯优化、算术优化算法和 Stacking 模型,可以适用于不同类型区块链 DDoS 攻击数据集。实验结果表明,该方法可以有效检测不同类型数据集上的区块链 DDoS 攻击,与其他集成学习算法相比有显著优势。下一步的研究将致力于验证基于集成学习的方法在真实网络环境的可用性并继续优化模型。

参考文献:

[1] LOTFALIZADEH H, KIM D S. Investigating real-time entropy features of DDoS attack based on categorized partial-flows[C]//14th international conference on ubiquitous information management and communication. Taichung: IEEE, 2020: 1-6.

[2] ALKADI O, MOUSTAFA N, TURNBULL B, et al. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks[J]. IEEE Internet of Things Journal, 2020, 8(12): 9463-9472.

[3] 天翼安全科技有限公司,联通数科安全,百度安全,等. 2023 年全球 DDoS 攻击现状与趋势分析[R/OL]. https://e.huawei.com/cn/material/networking/security/333e0bdd9694437e80aac4b436781fe3.

[4] MAKUVAZA A, JAT D S, GAMUNDANI A M. Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs)[J]. SN Computer Science, 2021, 2(2): 1-10.

[5] PARK J H, PARK J H. Blockchain security in cloud computing: use cases, challenges, and solutions[J]. Symmetry, 2017, 9(8): 164.

[6] JING X Y, YAN Z, PEDRYCZ W. Security data collection and data analytics in the Internet: a survey[J]. IEEE Communications Surveys and Tutorials, 2019, 21(1): 586-618.

[7] DAVID J, THOMAS C. Discriminating flash crowds from DDoS attacks using efficient thres holding algorithm[J]. Journal of Parallel and Distributed Computing, 2021, 152: 79-87.

[8] 王 智,张 浩,顾建军. SDN 网络中基于联合熵与多重聚类的 DDoS 攻击检测[J]. 信息网络安全,2023,23(10):1-7.
[9] CIL A E,YILDIZ K,BULDU A. Detection of DDoS attacks with feed forward based deep neural network model[J]. Expert Systems with Applications,2021,169:114520.
[10] DAI Q Y,ZHANG B,DONG S Q. A DDoS-attack detection method oriented to the Blockchain network layer[J]. Security and Communication Networks,2022,2022(1):5692820.
[11] 李颖之,李 曼,董 平,等. 基于集成学习的多类型应用层 DDoS 攻击检测方法[J]. 计算机应用,2022,42(12):3775-3784.
[12] TONKAL Ö,POLAT H,BAŞARAN E,et al. Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking [J]. Electronics,2021,10(11):1227.
[13] SAHOO K S,TRIPATHY B K,NAIK K,et al. An evolutionary SVM model for DDOS attack detection in software defined networks[J]. IEEE Access,2020,8:132502-132513.
[14] SOUSA J E A,OLIVEIRA V C,VALADARES J A,et al. Fighting under-price DoS attack in ethereum with machine learning techniques[J]. ACM SIGMETRICS Performance Evaluation Review,2021,48(4):24-27.
[15] SAYADI S,REJEB S B,CHOUKAIR Z. Anomaly detection model over blockchain electronic transactions [C]//2019 15th international wireless communications & mobile computing conference (IWCMC). Tangier:IEEE,2019:895-900.
[16] 黄屿璁,张 潮,吕 鑫,等. 基于深度学习的网络入侵检测研究综述[J]. 信息安全研究,2022,8(12):1163-1177.
[17] ABDULLA N N,HASOUN R K. Review of detection denial of service attacks using machine learning through ensemble learning[J]. Iraqi Journal for Computers and Informatics,2022,48(1):13-20.
[18] KHOA T V,SON D H,HOANG D T,et al. Collaborative learning for cyberattack detection in blockchain networks [J]. IEEE Transactions on Systems,Man,and Cybernetics:Systems,2024,54(7):3920-3933.
[19] VASEK M,THORNTON M,MOORE T. Empirical analysis of denial-of-service attacks in the bitcoin ecosystem[J]. Financial Cryptography and Data Security,2014,18:57-71.
[20] ABUALIGAH L,DIABAT A,MIRJALILI S,et al. The arithmetic optimization algorithm[J]. Computer Methods in Applied Mechanics and Engineering,2021,376:113609.
[21] SNOEK J,LAROCHELLE H,ADAMS R P. Practical Bayesian optimization of machine learning algorithms[C]//Advances in neural information processing systems. Lake Tahoe Nevada:Curran Associates Inc.,2012:2951-2959.
[22] CHAGANTI R,BOPPANA R V,RAVI V,et al. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges[J]. IEEE Access,2022,10:96538-96555.