DOI: 10.13382/j.jemi.B2306954

特征增强的改进 LightGBM 流量异常检测方法*

陈万志[1] 赵 林[1] 王天元[2]
(1.辽宁工程技术大学软件学院 葫芦岛 125105;2.国网辽宁省电力有限公司 营口 115005)

摘 要:针对机器学习在流量异常检测中存在选择特征过于依赖专家经验、原始特征表达能力不足、数据受噪声和离群点影响导致模型鲁棒性差以及处理非平衡海量高维数据时少数异常类检测率低等问题,提出一种特征增强的改进 LightGBM(light gradient boosting machine)流量异常检测方法。首先,采用隔离森林(isolation forest, iForest)实现异常值处理,并利用异常值处理后的数据训练引入全局平均池化(global average pooling, GAP)的一维卷积去噪自编码器(convolutional denoising autoencoder, CDAE),间接地消除数据中的噪声,得到原始特征的低维增强表达。然后,采用自适应合成采样(adaptive synthetic, ADASYN)对异常值处理后的数据实现数据增强并运用训练完成的 CDAE 进行特征提取,将得到的低维特征作为 LightGBM 的输入,训练并进行贝叶斯参数寻优。最后,通过得到的 CDAE+LightGBM 组合模型实现对异常流量的精准分类。在 NSL-KDD 数据集上所提方法的五分类准确率和 F1 分数分别达到了 87.80%和 87.75%,能够有效提升检测精度,增强未知攻击的检测能力。在 CICIDS2017 场景数据集上的测试进一步验证了所提方法可行性,且优于与同类型的深度学习算法。

关键词: 流量异常检测;隔离森林;卷积去噪自编码器;自适应合成采样;LightGBM
中图分类号: TP393;TN911.7 **文献标识码**: A **国家标准学科分类代码**: 510.40

Improved LightGBM for traffic anomaly detection method with feature enhancement

Chen Wanzhi[1] Zhao Lin[1] Wang Tianyuan[2]
(1. College of Software, Liaoning Technical University, Huludao 125105, China; 2. State Grid Yingkou Electric Power Company of Liaoning Electric Power Supply Co., Yingkou 115005, China)

Abstract: Focusing on the problems of machine learning in traffic anomaly detection, including reliance on expert experience for feature selection, insufficient expression ability of raw features, poor robustness of models due to noise and outliers in data, and low detection rates for minority classes in imbalanced high-dimensional datasets, an improved LightGBM for Traffic Anomaly Detection Method with Feature Enhancement is proposed. Firstly, the isolation forest (iForest) method is utilized to handle outliers, and the data processed by outlier treatment is used to train an one-dimensional convolutional denoising auto-encoder (CDAE) with global average pooling (GAP), which indirectly eliminates noise in the data and obtains low-dimensional enhanced expressions of original features. Then, adaptive synthetic sampling (ADASYN) is applied to the data after outlier treatment for data augmentation, and the trained CDAE is used to extract features. The obtained low-dimensional features are used as input for LightGBM, which is trained and optimized with Bayesian parameter tuning. At last, the precision classification of anomalous traffic is achieved through the utilization of the obtained CDAE+LightGBM ensemble model. The proposed method attains accuracy rates of 87.80% and F1 scores of 87.75% in a five-class classification task on the NSL-KDD dataset. Experimental results demonstrate that the proposed approach significantly enhances detection accuracy and reinforces the capability to identify unknown attacks. The test on CICIDS2017 scene data set further verifies the feasibility of the proposed method, which superior to the same type of deep learning algorithm.

Keywords: traffic anomaly detection; isolation forest; convolutional denoising auto-encoder; adaptive synthetic sampling; LightGBM

收稿日期:2023-10-13 Received Date: 2023-10-13
*基金项目:国家重点研发计划(2018YFB1403303)、辽宁省教育厅高校科研基金(2021LJKZ0327)项目资助

0 引　言

随着云计算、大数据、物联网等新兴技术的快速发展,数以亿计的网络接入点和用户设备的接入给网络空间安全带来了巨大的困难和挑战,传统防御手段难以对抗未知复杂的网络攻击。流量异常检测作为一种保护网络和系统安全的有效手段,被广泛用于检测网络流量恶意行为[1]。随着人工智能的发展,研究人员将流量异常检测视为一个分类问题,通过运用机器学习和深度学习等方法来提升异常流量检测的准确性和效率,并取得了一定的成果。

基于机器学习的流量异常检测方法依靠专家经验提取特征实现异常流量识别。其代表算法主要包括K近邻算法(K-nearest neighbor, KNN)[2]、决策树(decision tree, DT)[3]、LightGBM[4]、随机森林(random forest, RF)[5]等。然而随着人们对现代通信技术的依赖和大量未知的攻击不断涌现,机器学习方法面临着对新型攻击识别能力差、虚警率高、特征设计和特征选择过度依赖研究人员[6]等问题。

基于卷积神经网络(convolutional neural network, CNN)、循环神经网络(recurrent neural network, RNN)、自编码器(autoencoder, AE)等深度学习技术[7-10]通过自动提取网络数据的高级抽象表示,实现对异常流量的准确识别[11]。尹梓诺等[12]通过采用1DCNN-BiLSTM的模型提取流量数据特征并进行分类,通过注意力机制对分类有用的特征赋予更高的权重,以提高少数攻击类的检出率。梁欣怡等[13]通过采用IQR异常值处理和自编码器数据增强,将半自监督模型提取高维流量特征和自监督特征组合作为CNN-BiLSTM模型的输入,从而有效地提高了流量异常检测精度。Agarap等[14]提出一种结合门控循环单元(gated recurrent unit, GRU)和SVM的异常流量检测方法,实验表明,相较GRU-softmax, GRU-SVM更能够提升模型的检测能力。深度学习的出现和发展在一定程度上打破了传统机器学习算法依赖人工提取特征的局限,但是依然存在许多有待解决的问题。一方面,一个高质量的数据集对模型的训练起着至关重要的作用,然而在真实的网络环境中,网络流量数据中往往存在大量噪声和离群点,对模型训练会产生很大的负面影响。另一方面,真实网络环境中,正常网络数据与不同类别异常数据在数量上往往不成比例,模型在训练的过程中会导致决策边界倾向于正常样本,导致对异常数据的识别上表现不佳。

目前,针对网络流量中正常网络流量与异常网络流量样本数量失衡问题,常见的解决方法主要分为数据级、算法级及集成学习3类[15]。数据级方法通过改变原始样本分布改善类的不平衡程度,其代表方法有随机过采样(random over sampler, ROS)[16]、ADASYN[17]、合成少数过采样技术(synthetic minority oversampling technique, SMOTE)[18]等,但是存在着合成少数类样本时可能导致过拟合、引入噪声以及样本边缘化分布等问题。算法级方法通过考虑不同误分类情况下代价的差异,引入设计的代价敏感函数解决类别不平衡问题,但是存在着设计复杂、不同问题适用性以及计算开销大等问题。集成学习通过将多个单一分类器组合在一起,采用投票机制来有效地避免单个分类器可能产生的预测偏差,但是存在着子模型选择困难等问题。

综上所述,针对网络流量异常检测问题,研究者们提出了一系列创新性的方法和模型,以应对在特征提取、数据不平衡,噪声干扰等方面的挑战。但部分方法未充分考虑数据中噪声和异常值对模型性能的双重影响,导致模型鲁棒性差、处理数据不平衡时过采样易放大数据中的噪声,影响模型泛化能力以及在面对高维数据时,如何精确选择关键特征等挑战。因此,本文从数据预处理、特征提取和检测3方面提出强化数据预处理与特征增强的改进LightGBM流量异常检测方法。

本文的主要贡献如下:

1)提出一种两阶段数据预处理方法。第1阶段采用iForest去除数据集中的部分离群点后训练CDAE,减少异常值对模型训练的影响,从而提高模型的鲁棒性。第2阶段,在异常值处理后的数据集的基础上采用ADASYN生成新的样本,解决类别不平衡的问题。然后运用训练完成CDAE得到原始特征的低维增强表达并训练LightGBM,进一步对少数异常类的检测率。

2)将设计的CDAE和LightGBM模型组合实现流量异常检测。CDAE能够抑制输入数据中的噪声,使模型更专注于学习数据中的真实特征,提高特征的可区分性和表达性。LightGBM是一种基于直方图的决策树算法,具有高效处理大规模数据集的能力,还可以通过调整正负样本的权重比例,使模型更加关注少数类别,从而在不平衡数据集上提高模型性能。

1 相关技术

1.1 自编码器(AE)

AE[19]是一种无监督的深度学习技术,与主成分分析法类似,但是能够提供比主成分分析法更加强大的性能。它能够在最小化损失的前提下重构数据,建立数据特征由高维到低维映射。其通常由编码器、隐藏层和解码器3部分构成。编码器通过映射函数 $h=f(\boldsymbol{x})$ 将向量 $\boldsymbol{x}$ 映射到隐藏层 h,参数为 θ_f,解码器通过映射函数 $\hat{x}=g(h)$

将隐藏层表示映射回原始输入空间,参数为 θ_g。其中 f、g 为 sigmod、tanh 等非线性激活函数,θ 为编码器和解码器的权重和偏置向量,$\hat{x}$ 为原始向量 $\boldsymbol{x}$ 的重构。在训练过程中通过最小化 L1 或 L2 损失函数定义的重建误差来进行优化,其网络结构如图 1 所示。

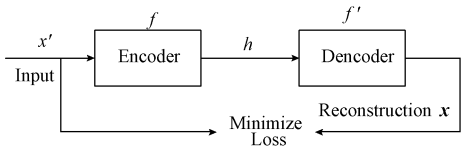


图 1　自编码器架构

Fig. 1　Autoencoder architecture

降噪自编码器(denoising auto encoder, DAE)是对传统 AE 的一种改进和正则化变体。通过对输入数据引入一个数据损坏的过程,如在原始数据中引入噪声或将原始数据以一定概率随机置零等,迫使模型在训练过程中去除噪声等损坏因素,重构原始未被损坏的数据。通过利用噪声作为正则化机制,DAE 既可以避免过拟合又能够学习到具有鲁棒性的隐藏层压缩特征表示,从而有效地提高模型的泛化能力。

1.2　iForest

iForest[20]是一种无监督的异常检测方法,它利用了异常的两个定量特性:异常实例占数据总体规模的比重较小、异常实例的属性值与正常实例的属性值有很大的不同,通过对数据集进行递归的随机划分构造完全生长的隔离树将每个数据区分开来。由于异常实例对隔离的敏感性,异常实例被隔离在树的根部附近。这样便可以用少量的条件将数据中的异常值检测出来。

iForest 算法中每颗隔离树(iTree)都是完全二叉树结构,其构造步骤为:给定一个数据样本 $X=\{x_1,x_2,\cdots,x_n\}$,随机选择一个属性 q 并在该属性的最大最小值间随机选择一个分隔值 p,使用属性 q 的值记为 $x_i(q)$,对每个数据 x_i 进行划分。如果 $x_i(q)<p$,将数据放在左子树,反之放在右子树,递归构造 iTree 直至满足以下条件之一:1)树达到高度限制;2) X 中只剩下一条数据或所有数据具有相同的值。假设所有的实例都是不同的,当 iTree 完全成长时,每个实例都与外部节点隔离,此时外部节点的数量为 n,内部节点的数量为 $n-1$,其总节点数为 $2n-1$。

隔离树全部构造完成后,需使用测试数据评估生成的隔离林,将测试数据遍历每颗 iTree,通过数据落在隔离林叶子结点的位置计算每棵树的高度平均值,平均高度低于阈值的数据即为候选离群点数据,计算离群值的公式为:

$$s(x,n)=2^{-\frac{E(h(x))}{c(n)}} \tag{1}$$

其中,$h(x)$ 是数据点 x 从根节点到 x 所在叶子结点的路径长度,$E(h(x))$ 是所有隔离林集合的 $h(x)$ 的平均值,$c(n)$ 是二叉搜索树中搜索不成功的平均路径长度:

$$c(n)=2H(n-1)-\left(\frac{2(n-1)}{n}\right) \tag{2}$$

其中,$H(i)$ 为谐波数,$H(i)=(Ln(i)+\gamma)$,γ 为欧拉常数;n 为叶子结点数。$c(n)$ 用来归一化 $h(x)$。若 s 接近与 1,则被认定为离群点,若 $s<0.5$,则为正常点。

1.3　ADASYN

ADASYN 使用密度分布作为准则来自动确定每个少数数据示例需要生成的合成样本的数量,在密度较低的区域生成更多的合成实例填充这些数据空间中的空白区域,增加样本的多样性,帮助模型更好地捕捉那些难以区分的少数类样本的特征。在密度较高的区域生成较少的合成实例,避免过度合成引入的噪声问题。且由于合成的样本是基于真实样本插值得到,因此能够保留原有的特征信息,既避免简单的复制粘贴导致的信息损失,又增加分类器对少数类的泛化能力,提高分类的准确性和召回率。

1.4　LightGBM

LightGBM 是一种基于梯度的单边采样(GOSS)和互斥特征捆绑(EFB)的 GBDT 模型。为解决 GBDT 模型在确定最优分割点上消耗大量时间导致模型训练时间较长的问题,LightGBM 在决策树的特征选择和分割点的确定上采用直方图算法。通过将原始的连续特征值放入容器中,并使用这些容器来构建模型,极大地减少了分割点选择的时间消耗,提高了模型的训练和预测效率。同时,为了减少每次迭代的样本数量,加强对预测效果差的样本的训练,引入 GOSS 算法,通过计算每个样本的梯度大小,筛选出梯度较大的实例,然后对梯度较小的实例进行一定比例的随机抽样,加强对在预测中容易产生误差的样本的训练。此外,LightGBM 引入了 EFB 来捆绑数据中的互斥特征,进一步降低了模型的计算复杂度,并采用 leaf-wise 生长策略通过减少训练数据并加入最大深度限制以避免生成较深的决策树减少过拟合风险,从而提高了算法的效率和准确性。

2　改进的 CDAE 和 LightGBM 流量异常检测模型

2.1　总体框架

在真实的网络环境中,网络流量数据可能因为某些突发事件或人为采集时的失误而出现与常态不符的数

值,且由于正常类样本数量庞大,离群点[21]的存在容易与其他少数攻击类样本产生类间或类内重叠现象,进而导致模型在训练过程中的误判,影响模型检测性能。考虑到对异常值的检测效率和计算开销,选择 iForest 实现高效的异常值处理,改善数据分布,提高模型检测准确率。

在面对非平衡的海量高维流量数据时,模型训练过程往往过于偏向学习多数类样本特征,而忽略了少数类样本的重要信息,从而影响了对少数类攻击的检测效果。对少数类样本过采样是解决数据失衡的常见方法。然而,过度采样可能会在原始数据中引入大量噪声,并且新生成样本的分布可能导致决策边界变得模糊。ADASYN 具有基于密度准则和样本插值的特性,能够在处理过异常值后的数据集上生成少数类样本时尽量保持原始样本分布的形态,避免过度引入噪声和样本边缘化分布,从而有助于保持决策边界的清晰性,提升模型的整体检测能力。

网络空间中的数据流具有空间性和时序性,传统的 AE 采用全连接层结构无法捕捉到数据的局部特征和空间关系,因此采用基于一维卷积神经网络的 CDAE 实现特征提取,并消除数据中的噪声。考虑到对数据增强可能会在原始数据中引入噪声,破坏样本原始分布,增加计算开销,因此使用异常值处理后数据训练 CDAE,提高模型的特征学习能力。

CDAE 和 LightGBM 的结合可以充分利用两种模型的优势。CDAE 能够学习数据的抽象特征表示,而 LightGBM 则可以在这些特征基础上进行更深入的学习和组合,从而形成一个更强大的集成模型。鉴于 LightGBM 存在多个需要调整的参数,采用贝叶斯优化算法来寻找最佳的 LightGBM 参数组合,以进一步提升模型性能,提出的流量异常检测整体框架如图 2 所示。

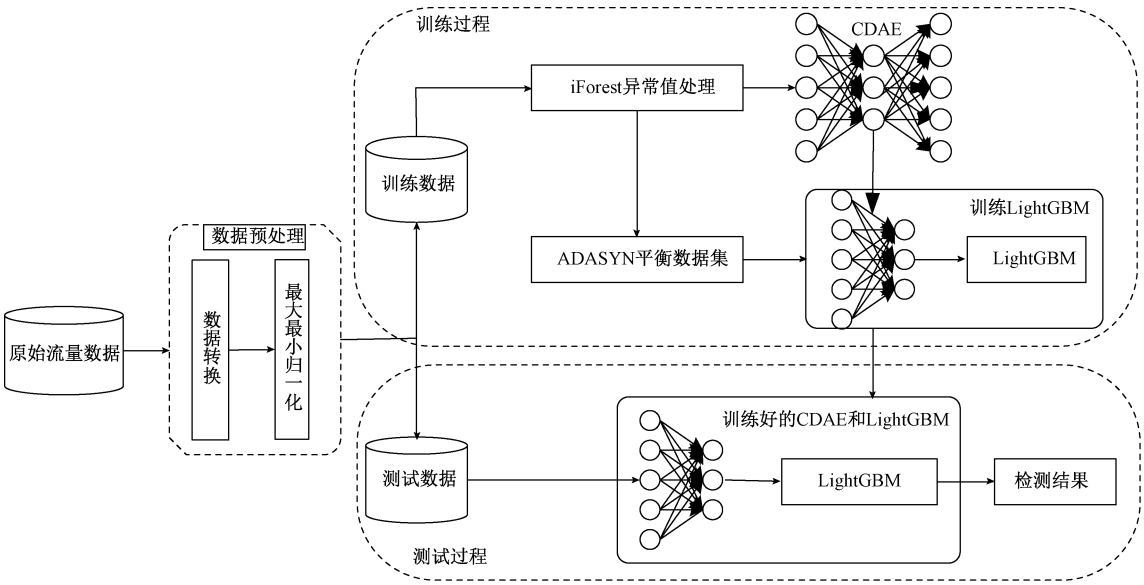


图 2　总体框架

Fig. 2　Overall framework structure

为了更好地提取高级流量特征表示,CDAE 采用两组一维卷积(1D CNN)层-最大池化(Max Pooling)层的组合完成局部空间特征提取,并将得到的特征输入全局平均池化(global average pooling, GAP)[22]层为每个类别生成一个特征图。通过计算每个特征图的平均值来减少特征维度、加强特征映射和类别之间的对应,减少模型过拟合风险。然后,在 GAP 层后添加两层全连接层,实现对提取的特征的全局整合,从而获取更高层次的抽象特征表示。CDAE 解码器使用一维反卷积层和上采样层完成对原始数据的重构,其模型结构如图 3 所示。

2.2　检测流程

所提方法的流量异常检测算法流程如图 4 所示,其具体的检测步骤描述如下:

1)对数据集的预处理包括数据清洗、字符型特征数值化、归一化、离群点检测、平衡数据集。

(1)数据清洗

原始流量数据集中可能存在特征值为“NAN”或“infinity”的样本,这些无效样本无法用于模型的训练和测试,需要将此类样本删除。

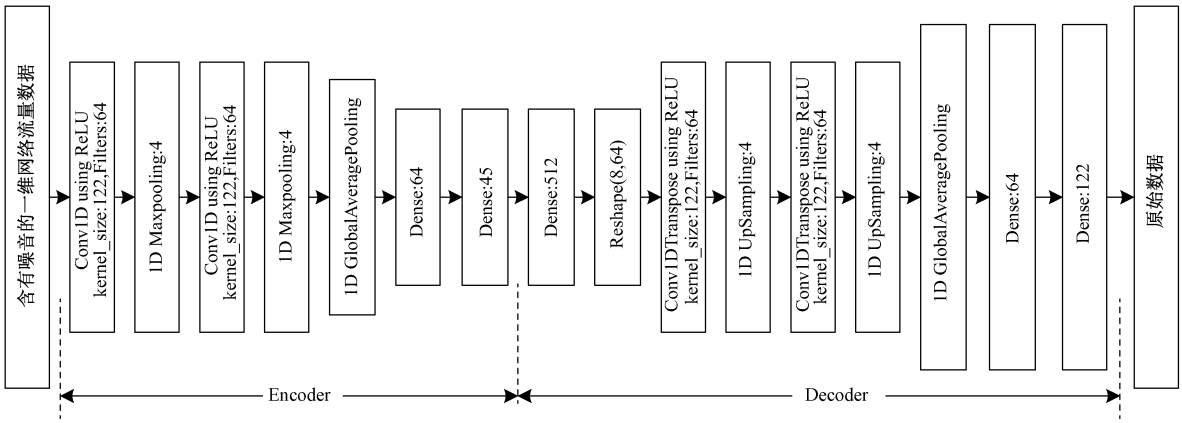


图 3　CDAE 网络架构

Fig. 3　CDAE network architecture diagram

(2)字符型特征数值化

NSL-KDD 数据集中包含数值型和字符型特征,为满足模型训练阶段输入数据为数值型,采用独热编码将 protocol_type、service、flag 这 3 个特征的字符表示转换为二进制数值特征,剩下的 39 个特征经处理增强为 120 个。

(3)归一化

由于原始数据可能具有不同的尺度和单位,数据的差异可能会对某些算法产生不良影响。因此采用最大最小归一化将原始数据进行缩放,将其映射到特定的范围内消除不同特征之间的量纲差异。其公式为:

$$x^* = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{3}$$

其中,x 为特征值,$x_{\min}$、$x_{\max}$ 分别为特征值的最大值和最小值。

(4)iForest 异常值处理

在数据预处理阶段忽略对数据中的离群值进行处理,往往导致训练后的模型在检测性能方面表现不佳。通过分析 NSL-KDD 数据集的数据分布发现,源字节数(src_bytes)、目的字节数(dst_bytes)和连接持续时间(duration)这 3 个特征的分布存在显著差异。为了防止离群点对模型检测结果产生影响,在实验过程中采用 iForest 仅去除正常类样本中的部分离群值。这样的决策有以下 3 个方面的考虑:①正常类样本数量明显多于其他 4 种攻击类样本,且其特征值相对较为稳定。模型在训练过程中可能会将正常样本中的离群点误判为异常。②完全去除所有离群点会造成一定的信息损失,从而影响模型的训练和性能。③异常类样本数量较少,其中的离群点可能更能够反映特定类别攻击的特征。去除这些离群点可能会使模型无法充分学习到该类攻击的关键特征。通过在正常类样本中有选择地移除部分离群点,能够更好地平衡正常样本和异常样本之间的关系,从而有效地提升模型的检测性能和泛化能力。

2)基于 CDAE 的流量特征提取

在处理大规模高维流量数据时,降低流量数据中的噪声,同时增强原始特征的表达能力,对于流量异常检测显得尤为关键。传统的基于评估特征重要性的特征选择方法虽然能够降低数据维度,但却难以增强原始特征的表达能力。而 PCA 等线性降维方法则难以捕捉数据之间的非线性关系。CDAE 能够表征线性变换和非线性变换,学习到强大的特征表示,抑制数据噪声,降低数据维度。因此采用基于 CDAE 的流量特征提取算法,其训练过程描述如下:

(1)将 NSL-KDD 数据集中的第 i 个样本、表示为 m 维特征向量 $\boldsymbol{x}_i \in R^m$,对其加入高斯噪声获得损坏流量样本 x'_i。在编码器中通过使用滤波器 w 对输入流量应用卷积操作构建特征映射,实现局部特征提取,其计算公式为:

$$h_i = f(w \otimes \boldsymbol{x}_i + b) \tag{4}$$

其中,h_i 为得到的特征图、b 为偏置值、$f(\cdot)$ 为卷积计算的非线性激活函数 ReLU,⊗代表卷积操作。

卷积操作后,使用 Max Pooling 对得到特征图下采样,提取每个块中的最大值作为窗口的特征值,其计算公式为:

$$h_{i+1} = \text{maxdown}_{l,t}(C) \tag{5}$$

其中,C 代表卷积面,l、t 代表对卷积面进行 $l \times t$ 块大小的下采样,h_{i+1} 表示池化操作之后的特征图。

经过两组卷积池化操作之后,将卷积之后结果送入 GAP 层得到 $1 \times k$ 个特征图,k 表示卷积结果中的特征图个数。

$$gap_i = avg(feature\_map_i) \tag{6}$$

其中,i 代表第 i 个特征图,$avg(\cdot)$ 代表该特征图的数值求平均值。

将得到 k 个特征图送入两层全连接层实现对全局特

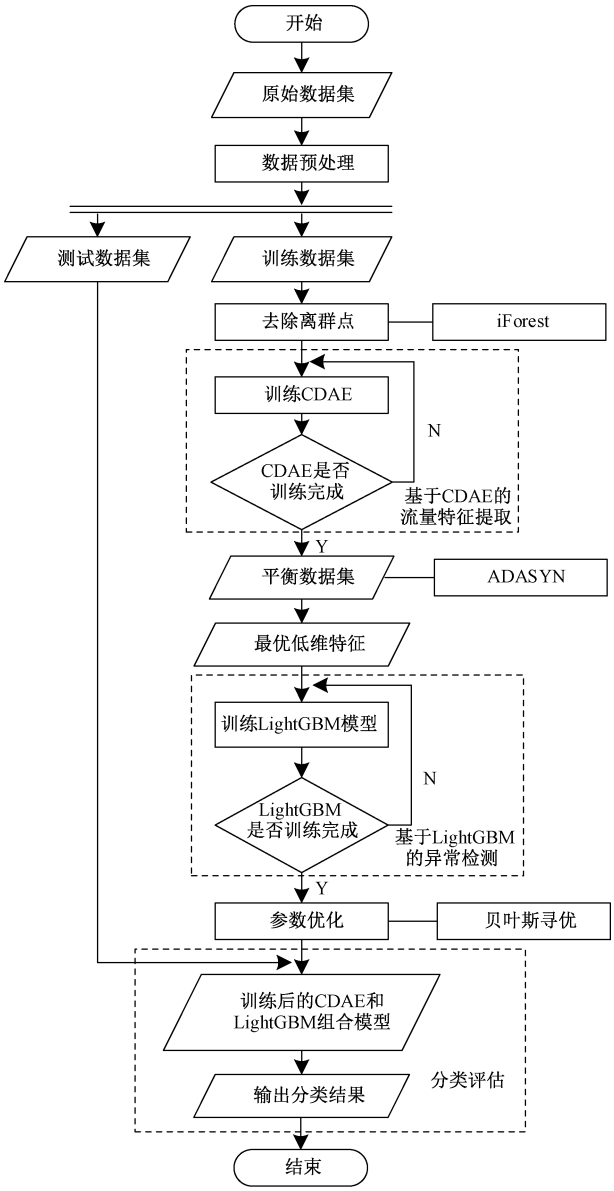


图4　检测流程

Fig. 4　Detection procedures

征的整合,最终得到编码器瓶颈层的特征表示。

(2)在解码器阶段,将编码器中得到的 k 个特征图,使用 Reshape 层将其转换为[特征个数,通道数]形式,满足一维反卷积层和上采样的输入。使用两组一维反卷积层和上采样层对原始数据重构,其公式为:

$$h_{j+1} = g(h_j * \hat{w} + b) \tag{7}$$

其中,h_j 表示解码器的输入、h_{j+1} 表示卷积之后得到的特征图、$g(\cdot)$ 为卷积计算的非线性激活函数 ReLU,$*$ 代表反卷积操作、$\hat{b}$ 为偏置值。

将一维反卷积和上采样得到的特征图使用式(6)生成 k 个特征图,使用两层全连接层和 Reshape 层完成原始向量的重构。

(3)最后,采用均方误差作为最小化原始未加噪声的流量数据与经过解码器输出数据之间的重构误差来优化网络参数,其表达式为:

$$L(W,b) = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{2}\| x_i - g(f(x'_i))\|^2\right) \tag{8}$$

其中,第 1 项为输入与输出之前的均方误差,n 为输入神经元个数,x_i 为输入的第 i 个样本。

3) ADASYN 平衡数据集

NSL-KDD 是一个不平衡的数据集,为了确保模型能够有效地学习到少数类样本的特征,提高对少数类样本的检测率,本文采用 ADASYN 平衡数据集,其处理过程如下:

步骤(1)分别计算 NSL-KDD 数据集中各个类别的样本数量,将小样本数量相加记为 m_s,大样本数量相加记为 m_l。

步骤(2)计算类别不平衡度 $d = m_s/m_l, d \in (0,1]$。

步骤(3)计算合成少数类样本数 $G = (m_l - m_s) \times \beta$, $\beta \in [0,1]$。其中 β 为生成合成数据后数据集的平衡度,$\beta = 1$ 表示加入合成新数据后数据集达到完全平衡状态。G 表示多数类与少数类的差值。

步骤(4)对于每个少数类实例 $x_i \in m_s$,根据 n 维空间中的欧氏距离,求出 K 个最近邻居,并计算比值 $r_i = \Delta_i/K, i = 1,\cdots,m_s$。$\Delta_i$ 是 x_i 的 K 个最近邻属于多数类的实例数,因此 $r_i \in [0,1]$。

步骤(5)根据 $\hat{r}_i = r_i / \sum_{i=1}^{m_s} r_i$ 正则化 r_i,那么 r_i 为概率分布($\sum \hat{r} = 1$),计算每个少数类样本周围多数类的情况。

步骤(6)计算每个少数样本 x_i 需要生成的合成数据样本数量 $g_i = \hat{r} \times G$。

步骤(7)在每个待合成的少数类样本周围 K 个邻居中选择一个少数类样本 x_{zi},根据以下公式进行合成 $s_j = x_i + (x_{zi} - x_i) \times \lambda$。

4)基于 LightGBM 的异常检测

利用 CDAE 对数据增强后的新数据进行特征提取,使用增强后的特征训练 LightGBM 分类器并使用贝叶斯优化进行参数寻优。最后将测试集输入训练完成的模型测试模型性能。

3　实验设计与结果分析

为验证所提方法有效性和可行性,所有实验均在 AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz CPU,16.0 GB RAM 硬件环境和 Windows 11 操作系统,开源深度学习框架 TensorFlow-GPU 2.4.2 软件环境下进

行,采用 Python3. 8 编程语言实现算法。

3. 1　数据集描述

1) NSL-KDD 数据集:是网络入侵检测领域性能评价基准 KDDCUP99 数据集的改进版,不仅消除了 KDDCUP99 中大量的冗余数据,而且还对训练集和测试集划分比例重新进行了调整。数据集中包含有 KDDTrain+、KDDTest+、KDDTrain+_20Percent、KDDTest-21 等 4 个文件。其中,KDDTest+中包含了 17 种在 KDDTrain+中未出现过的攻击,这使得 NSL-KDD 数据集更符合真实世界的数据分布,更适合于网络入侵检测实验。攻击行为包括 Dos、Probe、U2R 和 R2L 四种。每条样本包括 41 个特征和 1 个标签。实验使用 KDDTrain+作为训练集,KDDTest+作为测试集,其数据分布如表 1 所示。

表 1　NSL-KDD 数据集

Table 1　Dataset of NSL-KDD

类别	训练集(KDDTrai+)		测试集(KDDTest+)	
	样本数	IR%	样本数	IR%
Normal	67 343	100. 00	9 711	100. 00
DoS	45 927	68. 20	7 458	33. 08
Probe	11 656	17. 30	2 421	10. 74
R2L	52	0. 08	2 754	12. 22
U2R	995	1. 48	200	0. 89
总计	125 973	-	22 544	-

2) CICIDS2017 数据集:加拿大网络安全研究室于 2017 年在真实环境收集 1 周网络数据得到的数据集,其中星期一收集的数据仅包含正常数据,星期二~星期五收集正常数据和攻击数据,旨在收集真实、先进且多样性的网络数据用于评测现有入侵检测系统的可靠性。数据集中主要包含 8 个文件,共 3 119 345 条样本,每个样本 78 个特征。其中每条样本包含 1 个正常标签和 14 个攻击标签,本文将全部攻击数据与部分正常数据(避免失衡)拼接为实验数据集,其数据分布如表 2 所示。

3. 2　评价指标

为了有效地评估所提模型的性能,通过混淆矩阵(见表 3)计算流量异常检测常用的 4 个分类指标:准确率(Accuracy)、精确率(Precision)、检测率(detection rate, DR)和 F1 分数(F1-score)来评价所提网络流量异常检测算法的分类性能,其公式如式(9)~(12)所示。其中,TP(true positive)为被正确分类为攻击的样本数,FP(false positive)为被错误分类为攻击的正常样本数,TN(true negative)为被正确分类为正常的样本数,FN(false negative)是将攻击样本错误地归类为正常数。

Accuracy 是被正确预测的测试样本占所有测试样本的比例。取值范围为[0,1],值越大表示模型的分类性能越好。其定义为:

表 2　CICIDS2017 数据集

Table 2　Dataset of CICIDS2017

类别	描述	样本数
正常数据	BENIGN	529 918
攻击数据	Dos Hulk	231 073
	PortScan	158 930
	DDoS	128 027
	DoS GoldenEye	10 293
	FTP-Patator	7 938
	SSH-Patator	5 897
	DoS Slowloris	5 796
	DoS Slowhttptest	5 499
	Bot	1 966
	Web Attack-Brute Force	1 507
	Web Attack-XSS	652
	Infiltration	36
	Web Attack-SQL Injection	21
	Heartbleed	11
总计	-	1 087 564

表 3　混淆矩阵

Table 3　Confusion matrix

实际	预测值	
	异常	正常
异常	*TP*	*FN*
正常	*FP*	*TN*

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

Precision 是所有预测攻击样本中实际攻击样本所占的比例。取值范围为[0,1],值越大表示模型的分类性能越好。其定义为:

$$Precision = \frac{TP}{TP + FP} \tag{10}$$

DR 也称为召回率(Recall),是模型预测的攻击样本数占实际攻击样本总数的比例。DR 越大,模型的分类性能越好,取值范围为[0,1]。其定义为:

$$DR = Recall = \frac{TP}{TP + FN} \tag{11}$$

F1-score 为 Precision 和 DR 的调和平均值。取值范围为[0,1],值越大表示模型的分类性能越好。F1-score 评分相对于准确率而言,更适合于对不平衡数据集的分类结果进行性能评价。其定义为:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{12}$$

3. 3　超参数对模型性能的影响

模型参数的选择对模型性能的影响至关重要。本文通过在 NSL-KDD 数据集上对 CDAE+LightGBM 模型进行大量参数优化实验,在 LightGBM 参数保持随机初始值的

情况下,最终确定 CDAE 模型采用 Relu 作为隐藏层的非线性激活函数,均方误差作为损失函数、Adam 作为优化器,其具体结构及参数如图 3 所示。此外,通过实验确定 CDAE 瓶颈层最佳节点数以及高斯噪声比例,实验结果如图 5、6 所示。图 5 表明在不对模型输入加入噪声的情况下,当瓶颈层节点数在[40,50]之间时,模型在训练集和测试集上准确率趋于稳定。图 6 表明在瓶颈层节点数为 45 时,高斯噪声比例在[0.4,0.5]区间准确率最高,经过多次实验发现噪声比为 0.4 时模型性能最好。因此,实验中瓶颈层节点数设为 45,噪声比设为 0.4。

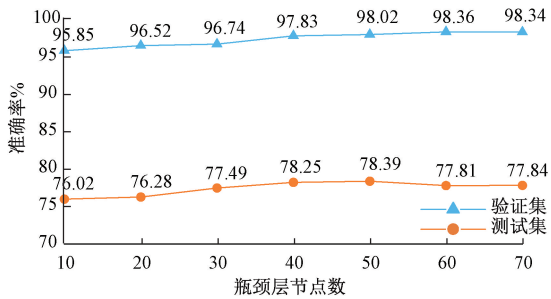


图 5　不同瓶颈层节点个数的模型准确率

Fig. 5　Model accuracy with different bottleneck layer node counts

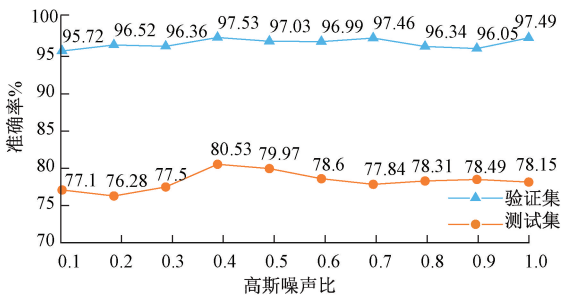


图 6　不同噪声比例下的模型准确率

Fig. 6　Model accuracy at different noise ratios

隔离森林中主要影响模型性能的参数主要有隔离森林的叶子结点数(n_estimators)、训练数据中异常数据的数量占比数(contamination)。正常样本中的离群点去除过少无法改善过采样后与其他类型样本之间的重叠问题。而去除过多会则导致一定的信息损失,当过采样合成的攻击样本过多,容易改变原始数据分布,模型可能会过度拟合这些合成样本,从而导致对其他样本的检测性能下降。因此需要设置合适的参数确保对少数攻击类样本过采样后,既可以保证多数类样本的检测率又可以提升对少数类样本的检测率。实验中使用控制变量法分别采取不同的 estimators 和 contamination 值,得到不同的训练集训练 CDAE,测试 ADASYN 数据增强前后 LightGBM 在 KDDTest+数据集上的表现。其中,CDAE 采用上文设置好的参数,LightGBM 使用随机初始化的参数,实验结果如图 7 所示。

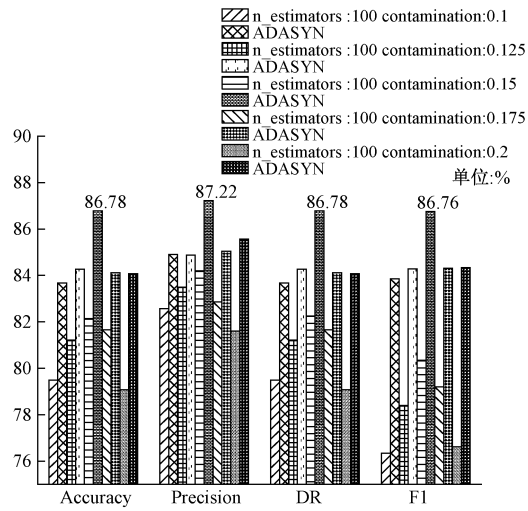


图 7　不同 contamination 对模型性能的影响

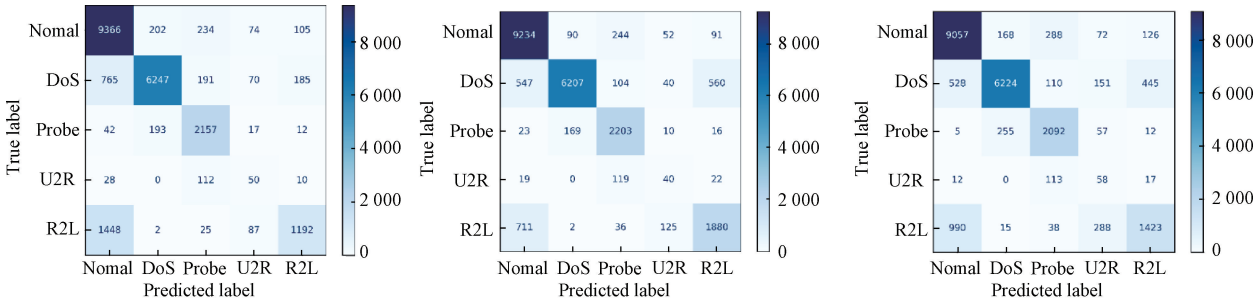
Fig. 7　Impact of different contamination on odel performance

在图 7 中可以看出,当 estimators 值为默认参数 100 时,contamination=0.15,模型取得了最佳性能,准确率达到 86.78%,精确率为 87.22%,检测率为 86.78%,F1 分数为 86.76%。然而,当 contamination>0.15 时,模型的综合检测能力开始下降。图 8 中的混淆矩阵揭示了这一趋势背后的原因。当 contamination=0.1 时,模型在正常样本检测方面表现较好,但对攻击样本的检测效果欠佳;当 contamination = 0.2 时,则呈现相反的情况。当 contamination=0.15 时,模型能够平衡地兼顾正常样本和少数攻击样本的检测率。

为了测试不同的 n_estimators 参数取值对模型性能的影响,在 contamination= 0.15 的情况下进行参数优化实验,实验结果如图 9 所示。从图中可以看出,当 estimators 取值为 300 时,模型的准确率为 87.05%、精确率为 87.47%、检测率为 87.05%、F1 分数为 86.57%,模型的整体性能得到了进一步的提升。LightGBM 分类器中影响模型分类性能的参数较多,人工试错法需要的代价太大,花费时间过长。贝叶斯优化可以利用完整的历史信息提高参数空间的搜索效率。因此,所提方法采用 Python 导入 bayes_opt 库的 BayesianOptimization 函数来实现贝叶斯算法对 LightGBM 分类器的参数寻优,实验结果如图 10 所示。

经贝叶斯优化后的分类准确率为 87.80%、精确率为 88.20%、检测率为 87.80%、F1 分数为 87.75%,模型整体性能得到了明显的改善。

LightGBM 参数的具体含义和取值如表 4 所示。



(a) Contamination=0.1时的混淆矩阵
(a) Confusion matrix for contamination = 0.1

(b) Contamination=0.15时的混淆矩阵
(b) Confusion matrix for contamination = 0.15

(c) Contamination=0.2时的混淆矩阵
(c) Confusion matrix for contamination=0.2

图 8　不同 contamination 取值下的混淆矩阵

Fig. 8　Confusion matrix for different values of contamination

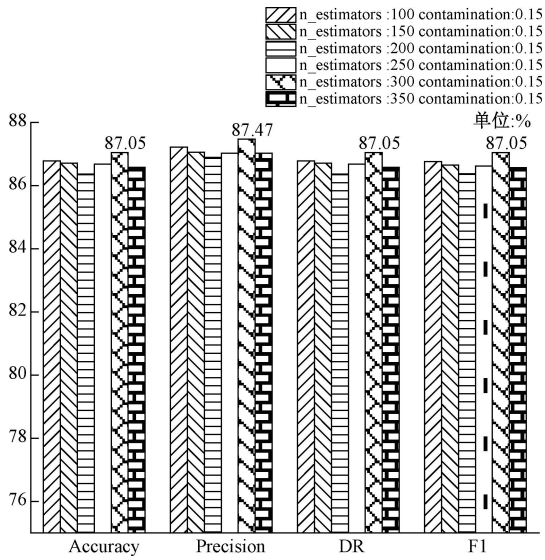


图 9　不同 n_estimators 对模型性能的影响

Fig. 9　Effect of different n estimators on model Performance

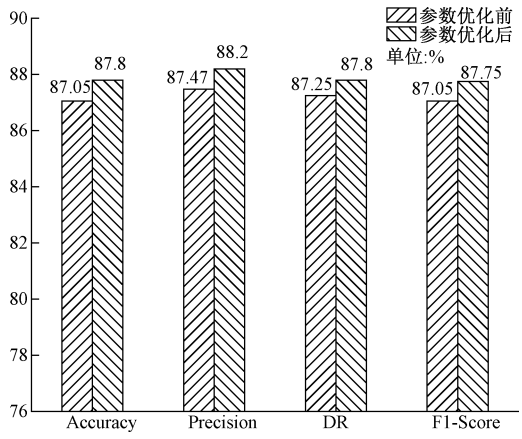


图 10　参数优化前后模型性能对比

Fig. 10　Comparison of model performance before and after parameter optimization

表 4　LightGBM 参数说明及取值

Table 4　LightGBM parameter descriptions and values

参数	参数说明	值
num_leaves	单棵树的最大叶子数	885
min_data_in_leaf	每个叶子节点的最小样本数	619
learning_rate	学习率	0. 435
feature_fraction	每棵树的特征数	0. 112
bagging_fraction	每次迭代使用的数据量	0. 530
min_gain_to_split	分裂的最小增益	0. 1
max_depth	树的最大深度	1
num_boost_round	树的个数	428

3. 4　消融实验

为验证 iForest、ADASYN、CDAE、LightGBM 4 种方法结合使用的可行性，在 NSL-KDD 数据集上进行了消融实验，实验结果如图 11 所示。

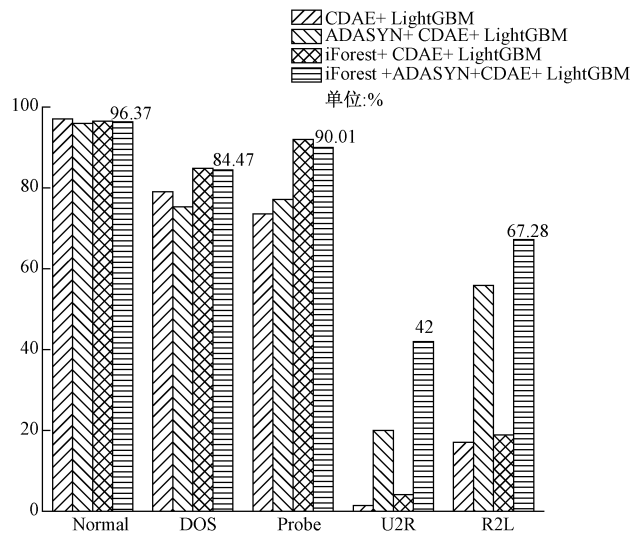


图 11　消融实验结果

Fig. 11　Ablation results

从图11的消融实验结果表明,与基线模型CDAE+LightGBM相比,在不对数据中的异常值处理的情况下,直接使用ADASYN对U2R、R2L两个少数类样本上采样会使模型对其他类别样本检测率下降。而在去除Normal类样本中的部分离群点后,在对Normal类样本检测率有轻微的下降的情况下,模型对4种少数攻击类的检测率有明显的提升。在其后采用ADASYN平衡数据集,模型对Normal、Probe、DoS类样本极小的精度损失下,保证了对U2R、R2L两个少数类样本的检测率,实验结果充分说明了所提方法的有效性。

3.5　与其他数据增强算法的比较

本节通过与其他不同的数据增强算法进行对比实验,旨在验证利用ADASYN对数据预处理对后续分类模型整体性能提升的有效性。实验对比结果如图12所示。在对比实验中,选择几种常见的数据增强算法作对比,包括ROS、SMOTE、Borderline SMOTE[23]。对比算法分别是在数据增强前去除了数据中的离群点,利用去除离群点的数据集训练CDAE模型。然后将使用不同数据增强算法增强后的数据输入训练好的CDAE模型进行降维,使用降维后的特征作为输入LightGBM分类器的输入,得到分类器在不同数据集上的检测性能。

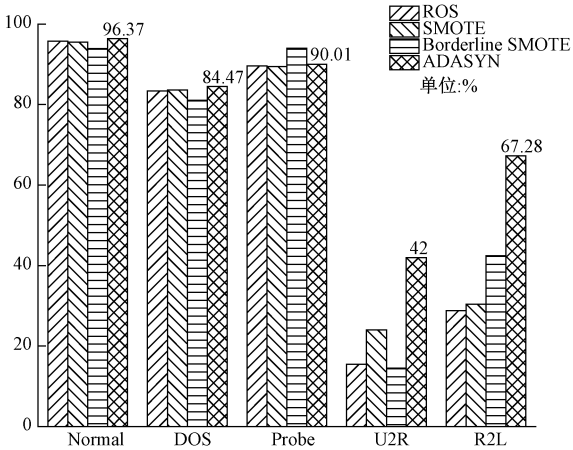


图12　不同数据增强算法下模型分类检测率

Fig. 12　Model classification detection rate under different data enhancement algorithms

从图12中可以看出相对于其他数据增强算法,经过ADASYN处理的数据在5种攻击类型中具有最高的检测精度,尤其是U2R和R2L的检测精度。且由于KDDTest+中还包含了大量的未知攻击类型没有出现在KDDTrain+中,但是检测准确率仍然很高,这说明ADASYN通过插值生成样本增强了模型识别未知攻击的能力。

相较ADASYN,其他4种数据增强算法检测性能并不理想的主要原因是因为ROS只是对原始数据的过采样,没有考虑数据分布和生成样本的多样性,SMOTE和Borderline SMOTE则是基于K近邻原则对原始样本的随机合成,虽然在一定程度上保证了生成样本的多样性,但是对于少数类别样本密集分布的区域,二者可能会在边界区域生成大量合成样本,从而形成大量噪声,导致决策边界过于复杂,增加分类器分类难度。而ADASYN通过在少数实例的密度较低的特征空间区域中生成更多的合成实例,且在密度较高的特征空间区域生成较少的合成实例,保证了不同类型样本之间边界可分。此外合成的样本是基于真实样本进行插值得到的,增加了样本的多样性,从而提升了模型对未知攻击的检测能力。

3.6　同一数据预处理下与其他模型的比较

为验证所提方法能够更好地对不平衡数据集进行分类,在保持相同的实验环境、参数分别设计了基于KNN、RF、DAE+GRU[12]、CAFÉ+CNN[24]以及DAE+ LightGBM的流量异常检测模型。其中,除了DAE+ LightGBM和DAE+GRU模型在训练阶段采用与本文数据预处理和训练步骤一样外,其余模型均在iForest和ADASYN组合对数据集预处理的情况下训练模型,对比实验结果如表5所示。

表5　与不同检测模型的比较结果

Table 5　Results of comparison with differentdetection models　　(%)

模型	Accuracy	Precision	DR	F1-score
KNN	79.63	79.29	79.63	78.73
RF	81.37	81.54	80.48	78.38
DAE+GRU	85.68	86.29	85.68	85.56
CAFÉ+CNN	83.34	83.35	83.44	82.60
DAE+LightGBM	85.39	85.86	85.39	85.28
CDAE+LightGBM	87.80	88.20	87.80	87.75

由表5可知,CDAE+LightGBM模型在各个指标方面均优于其他5种模型,主要原因有3点:1)仅使异常值处理后的数据训练CDAE,避免了由于数据增强导致的误判问题。2)CDAE采用一维卷积层,使得它在训练过程中学习到了数据的高级特征,并抑制数据中噪声,提高特征学习的质量和数据表征的稳定性。3)新训练集上U2R和R2L样本与Normal类样本数量相当(见表1),但是Probe和DoS类样本数量相对较少。因此,通过贝叶斯优化调整LightGBM权重参数,使得LightGBM分类在过程中关注少数样本,进一步提高整体的检测能力。

对于传统的机器学习模型KNN而言,数据中冗余特征的存在会引入噪声和无关信息,导致KNN算法在计算相邻样本时受到干扰,从而影响分类性能。RF虽然内置了特征重要性评估机制,但在原始特征的表征能力可能不足以支持模型高效学习。DAE+GRU模型在第一次特征提取时,全连接层的DAE在处理序列数据时不能充分捕捉到局部特征模式和时序信息,提取的特征作为GRU

的输入,影响了其后续分类能力,并且 GRU 不具有在不平衡数据集上的自适应调节能力,使其整体性能略次于本文模型。CAFÉ+CNN 采用基于上下文感知的特征提取算法提取特征并将网络流量数据变换为图像格式,使用 CNN 实现异常流量识别,其特征提取算法远不及深度学习模型,且忽略了网络流量中的时序关系,导致其检测性能不佳。而 DAE + LightGBM 模型的检测能力次于 DAE+GRU,是因为其忽略了数据中的时序信息。从实验结果上看,采用基于一维卷积神经网络的 CDAE 提取特征和 LightGBM 流量异常检测可以获得更好的检测效果。

3.7　与其他检测模型的比较

为了验证所提模型的优越性,在 NSL-KDD 数据集上与现有文献中的最新模型进行对比,所有模型均使用 KDDTrain+作为训练集,KDDTest+作为测试集,比较的性能指标包括 Accuracy、Precision、DR 和 F1-score。比较对象包括 AE-DNN[25]、AE-CNN-BiLSTM-AE[13]、GMM-WGAN-IDS[26]。实验结果如表 6 所示。由表 6 可知,CDAE+LightGBM 模型的分类准确率为 87.80%,精确率为 88.20%,检测率为 87.80%,F1 分数为 87.85%,除了在精确率上略低于 GMM-WGAN-IDS 模型,其他指标均优于对比模型。实验结果表明,将 iForest 与 ADASYN 结合用于对数据集预处理以及将 CDAE 与 LightGBM 结合用于高维数据降维、特征增强和高效样本分类具有一定的研究意义,为流量异常检测方法提供了新思路。实验结果表明该方法切实可行,能够有效地提高流量异常检测准确率。

表 6　NSL-KDD 数据集上与现有模型的比较结果

Table 6　Results of comparison with existing models on the NSL-KDD dataset　　(%)

模型	Accuracy	Precision	DR	F1-score
AE-DNN[25]	87.00	80.37	87.00	86.88
AE-CNN-BiLSTM-AE[13]	85.70	84.70	87.50	85.10
GMM-WGAN-IDS[26]	86.59	88.55	86.59	86.88
CDAE+LightGBM	87.80	88.20	87.80	87.75

3.8　可行性验证

为了验证所提模型的可行性,将 CICIDS2017 数据集的星期一的正常数据与星期二~星期五的攻击数据组合,按照 3∶7 比例划分测试集和训练集训练模型并与同类型的深度学习算法进行了比较,实验流程与 NSL-KDD 数据集一致,实验结果如表 7 所示。从表 7 中可以看出,本文模型准确率达到 99.82%,精确率达到 99.84%,检测率达到 99.82%,F1 分数达到 99.84%,与其他模型相比模型性能最优。这是由于本文在数据预处理阶段第 1 阶段中使用去除离群点之后数据集训练 CDAE,既抑制了数据中的噪声又规避了直接过采样导致引入新的离群点对训练模型产生的负面影响,在第 2 阶段利用 CDAE 对过采样后的数据集进行特征提取既克服了数据不平衡问题,又将更具有区分能力的特征 LightGBM 模型作为输入,使模型对异常流量的识别能力得到大大提高。

表 7　CICIDS2017 数据集上与现有模型的比较结果

Table 7　Results of comparison with existing models on the CICIDS2017 dataset　　(%)

模型	Accuracy	Precision	DR	F1-score
K-means SMOTE+AE[27]	99.16	98.16	98.28	98.22
CNN-BiLSTM-Attention[12]	99.52	99.51	98.98	99.24
self-taught learning+SAE[28]	94.95	94.69	83.07	88.50
KSAIDS[29]	99.16	98.16	98.28	98.22
CDAE+LightGBM	99.82	99.84	99.82	99.84

4　结　论

为了提高网络流量异常检测中对少数攻击的检测精度,克服数据类别不平衡的缺陷,提出一种特征增强的改进 LightGBM 流量异常检测方法。采用两阶段数据预处理和两阶段模型训练法。第 1 阶段采用 iForest 实现异常值处理,消除离群点对模型训练的负面影响,并训练改进的 CDAE 模型。利用 CDAE 在加入噪声的数据中重构原始数据,实现高维流量特征的降维与真实特征的提取。第 2 阶段,在异常值处理的基础上采用 ADASYN 平衡数据集,采用训练后的 CDAE 提取特征并训练 LightGBM 来进一步关注数据中的关键特征和信息,提高模型的综合性能。通过在数据集 NSL-KDD 和 CICIDS2017 上的实验结果表明,所提模型在综合性能方面表现出良好的潜力,可作为一种有竞争力的候选方法用于网络流量异常检测。下一步研究重点在更复杂场景验证提出方法的有效性,并进一步探索其改进方法应用于从真实网络中获取的网络流量数据中。

参考文献

[1] SU Y, QI K, DI C, et al. Learning automata based feature selection for network traffic intrusion detection[C]. 2008 IEEE Third International Conference on Data Science in Cyberspace, Guangzhou, China, 2018: 622-627.

[2] 任家东, 刘新倩, 王倩, 等. 基于 KNN 离群点检测和随机森林的多层入侵检测方法[J]. 计算机研究与发展, 2019, 56(3):566-575.
REN J D, LIU X Q, WANG Q, et al. An multi-level intrusion detection method based on KNN outlier detection and random forests[J]. Journal of Computer Research and Development, 2019, 56(3):566-575.

[3] GAO X, SHAN C, HU C, et al. An adaptive ensemble

machine learning model for intrusion detection[J]. IEEE Access, 2019, 7:82512-82521.

[4] YAO R, WANG N, LIU Z, et al. Intrusion detection system in the smart distribution network: A feature engineeringbased AE-LightGBM approach [J]. Energy Reports, 2021, 7:353-361.

[5] 周杰英, 贺鹏飞, 邱荣发, 等. 融合随机森林和梯度提升树的入侵检测研究[J]. 软件学报, 2021, 32(10):3254-3265.
ZHOU J Y, HE P F, QIU R F, et al. Research on intrusion detection based on random forest and gradient boosting tree[J]. Journal of Software, 2021, 32(10): 3254-3265.

[6] LIU J, GAO Y, HU F. A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM [J]. Computers & Security, 2021, 106:102289.

[7] 杨杰, 唐亚纯, 谭道军, 等. 多通道自编码器深度学习的入侵检测方法[J]. 计算机科学与探索, 2020, 14(12):2050-2060.
YANG J, TANG Y CH, TAN D J, et al. Intrusion detection method of multi- channel autoencoder deep learning[J]. Journal of Frontiers of Computer Science and Technology, 2020,14(12):2050-2060.

[8] LI Z, QIN Z, HUANG K, et al. Intrusion Detection Using Convolutional Neural Networks for Representation Learning[M]. Neural Information Processing, 2017: 858-866.

[9] DU B, XIONG W, WU J, et al. Stacked convolutional denoising auto-encoders for feature representation[J]. IEEE Transactions on Cybernetics, 2017, 47(4): 1017-1027.

[10] BINBUSAYYIS A, VAIYAPURI T. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM[J]. Applied Intelligence, 2021, 51(10):7094-7108.

[11] SHONE N, NGOC T N, PHAI V D, et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1):41-50.

[12] 尹梓诺,马海龙,胡涛. 基于联合注意力机制和一维卷积神经网络-双向长短期记忆网络模型的流量异常检测方法[J]. 电子与信息学报, 2022, 44:1-10.
YIN Z N, MA H L, HU T. A traffic anomaly detection method based on the joint model of attention mechanism and one-dimensional convolutional neural network-bidirectional long short-term memory[J]. Journal of Electronics & Information Technology, 2022, 44:1-10.

[13] 梁欣怡, 行鸿彦, 侯天浩. 基于自监督特征增强的CNN-BiLSTM网络入侵检测方法[J]. 电子测量与仪器学报, 2022, 36(10):65-73.
LIANG X Y, XING H Y, HOU T H. CNN-BiLSTM network intrusion detection method based on self-supervised feature enhancement [J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(10):65-73.

[14] AGARAP A F M. A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data[C]. The 2018 10th International Conference on Machine Learning and Computing, Macao, China, 2018: 26-30.

[15] 李艳霞, 柴毅, 胡友强, 等. 不平衡数据分类方法综述[J]. 控制与决策, 2019, 34(4):673-688.
LI Y X, CHAI Y, HU Y Q, et al. Review of imbalanced data classification methods[J]. Control and Decision, 2019, 34(4):673-688.

[16] LEMAÎTRE G, NOGUEIRA F, ARIDAS C K. Imbalanced-learn: A Python toolbox to tackle the curse of imbalanced datasets in machine learning[J]. The Journal of Machine Learning Research, 2017, 18(1): 559-563.

[17] HE H, BAI Y, GARCIA E A, et al. ADASYN: Adaptive synthetic sampling approach for imbalanced learning[C]. IEEE World Congress on Computational Intelligence, Hong Kong, China, 2008: 1322-1328.

[18] MA X, SHI W. Aesmote: Adversarial reinforcement learning with smote for anomaly detection[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 943-956.

[19] HINTON G E, SALAKHUTDINOV R R. Reducing the dimensionality of data with neural networks[J]. Science, 2006, 313(5786): 504-507.

[20] LIU F T, TING K M, ZHOU Z H. Isolation forest[C]. IEEE International Conference on Data Mining, Pisa, Italy, 2008: 413-422.

[21] SMITI A. A critical overview of outlier detection methods[J]. Computer Science Review, 2020, 38: 100306.

[22] LIN M, CHEN Q, YAN S. Network in network[J]. 2013: ArXiv Preprint arXiv:1312.4400.

[23] HAN H, WANG W Y, MAO B H. Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning[C]. International Conference on Intelligent Computing, Hefei, China, 2005: 878-887.

[24] SHAMS E A, RIZANER A, ULUSOY A H. A novel context-aware feature extraction method for convolutional neural network-based intrusion detection systems[J].

Neural Computing and Applications, 2021, 33(20): 13647-13665.

[25] IERACITANO C, ADEEL A, MORABITO F C, et al. A novel statistical analysis and autoencoder driven intelligent intrusion detection approach [J]. Neurocomputing, 2020, 387: 51-62.

[26] CUI J, ZONG L, XIE J, et al. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data [J]. Applied Intelligence, 2023, 53(1): 272-288.

[27] 蹇诗婕,刘岳,姜波,等. 基于聚类过采样和自动编码器的网络入侵检测方法[J]. 信息安全学报,2023,8(6):121-134.
JIAN SH J, LIU Y, JIANG B, et al. Network intrusion detection using cluster oversampling and auto-encoder[J]. Journal of Cyber Security,2023,8(6):121-134.

[28] QURESHI A S, KHAN A, SHAMIM N, et al. Intrusion detection using deep sparse auto-encoder and self-taught learning[J]. Neural Computing and Applications, 2020, 32: 3135-3147.

[29] SHAMS E A, RIZANER A, ULUSOY A H. A novel context-aware feature extraction method for convolutional neural network-based intrusion detection systems [J]. Neural Computing and Applications, 2021, 33(20): 13647-13665.

作者简介

陈万志(通信作者),2015 年于辽宁工程技术大学(中国测绘科学研究院联合培养)获得博士学位,现为辽宁工程技术大学副教授,硕士生导师,主要研究方向为人工智能与智能信息处理、网络与信息安全和工控软件与数据分析。

E-mail: chenwanzhi@ lntu. edu. cn

Chen Wanzhi (Corresponding author) received his Ph. D. degree from Liaoning Technical University (China Academy of Surveying and Mapping Science Joint Cultivation) in 2015. Now he is an associate professor and master's degree supervisor in Liaoning Technical University. His main research interests include artificial intelligence and intelligent information processing, network and information security and industrial control software and data analytics.

赵林,2021 年于辽宁工程技术大学获得学士学位,现为辽宁工程技术大学硕士研究生,主要研究方向为网络安全和入侵检测。

E-mail: 2766191688@ qq. com

Zhao Lin received his B. Sc. degree from Liaoning Technical University in 2021. Now he is a M. Sc. candidate at Liaoning Technical University. His main research interests include network security and intrusion detection.