文章编号：1003－1251(2026)04－0027－08

基于1DCNN-BiGRU和改进特征选择的网络入侵检测方法

冯雪佳，郭 崇，朱宏博

（沈阳理工大学 信息科学与工程学院，沈阳 110159）

摘 要：现有网络入侵检测方法因数据类别分布不均衡、特征冗余等问题而导致其多分类检测准确率较低，为此提出一种基于一维卷积神经网络－双向门控循环单元(1DCNN-BiGRU)和改进特征选择的网络入侵检测方法。在数据预处理阶段，引入合成少数类过采样技术(SMOTE)提高模型对少数类别特征的识别能力，采用信息增益方法和随机森林算法进行特征选择，选取对分类任务具有关键作用的特征；在模型训练阶段，先采用1DCNN提取局部关联特征，并引入多头自注意力机制，从全局视角捕获数据中不同位置元素之间的依赖关系，再通过BiGRU提取数据中的长距离时序关联特征，最后使用Softmax分类器实现多分类检测。实验结果表明，本文模型在NSL-KDD数据集和UNSW-NB15数据集上的多分类准确率分别达到99.65%和84.83%，较其他几种用于对比的主流入侵检测模型更具优势。

关 键 词：网络入侵检测；卷积神经网络；双向门控循环单元；多头自注意力机制；随机森林

中图分类号：TP393.08 **文献标志码**：A **DOI**：10.3969/j.issn.1003－1251.2026.04.004

Network Intrusion Detection Method Based on 1DCNN-BiGRU and Improved Feature Selection

FENG Xuejia，GUO Chong，ZHU Hongbo

（Shenyang Ligong University，Shenyang 110159，China）

Abstract：Existing network intrusion detection methods often exhibit low multiclass detection accuracy due to imbalanced class distributions and redundant features. To address these issues，we propose a network intrusion detection method based on a one-dimensional convolutional neural network combined with a bidirectional gated recurrent unit(1DCNN-BiGRU) and an improved feature-selection scheme. In the data preprocessing stage，the synthetic minority over-sampling technique (SMOTE) is employed to enhance the model's ability to recognize minority classes. Feature selection is carried out using an information-gain criterion together with a random forest algorithm to identify features that are most important for the classification task. During model training，a 1DCNN is first used to extract local correlation features；a multi-head self-attention mechanism is then incorporated to capture dependencies among elements at different positions from a global perspective；subsequently，a BiGRU is applied to model long-range temporal dependencies in the data. Finally，a Softmax classifier is used to perform multiclass detection. Experimental results show that the pro-

收稿日期：2025－06－09

基金项目：国家自然科学基金项目(62102272)；辽宁省教育厅高等学校基本科研项目(JYTMS20230184)；辽宁省自然科学基金项目(2023JH26/10300007)

作者简介：冯雪佳(2000—)，女，硕士研究生；郭崇(1980—)，通信作者，女，副教授，博士。

posed model achieves multiclass accuracies of 99.65% on the NSL-KDD dataset and 84.83% on the UNSW-NB15 dataset, demonstrating superior performance compared with several mainstream baseline intrusion-detection models.

Key words: network intrusion detection; convolutional neural networks; bidirectional gated recurrent unit; multi-head self-attention mechanism; random forest

网络技术的蓬勃发展为社会创造了巨大的经济效益,也极大地便利了人们的生活,但随之而来的网络空间安全问题也日益严峻。面对层出不穷且形式多变的网络攻击手段,构建高效、主动的网络安全防护系统成为维护网络空间安全稳定的核心任务。网络入侵检测系统(network intrusion detection system,NIDS)作为网络安全主动防御技术的重要组成部分,能够实时监测网络流量,精准识别异常行为模式。网络入侵检测方法是网络安全领域的重要研究内容。

随着大数据技术的不断发展和计算资源性能的显著提升,机器学习技术在网络入侵检测中的应用愈加受到关注,并取得了突破性进展[1]。Wang 等[2]提出了一种基于 K-means 聚类的网络流量入侵检测模型,可通过解析 TCP 数据包中的关键信息来检测僵尸网络攻击。Qazi 等[3]提出了一种基于一维卷积神经网络(1DCNN)的深度学习架构,在 CICIDS2017 数据集上的网络入侵检测准确率达到 98.96%。黄迎春等[4]基于强化学习将优先经验采样和近端策略优化裁剪算法应用于入侵检测,使用轻量级梯度提升机(LightGBM)作为分类器,在 NSL-KDD 数据集上的检测准确率达到 87.43%。

为应对入侵检测数据分布极端不平衡的情况,提高对少数类别数据的检测准确率,Albasheer 等[5]先通过合成少数类过采样技术(SMOTE)对少数类样本过采样,再利用编辑最近邻(ENN)算法剔除噪声样本,有效平衡了类分布,提升了模型对少数类攻击的检测能力。Dash 等[6]提出了基于优化长短时记忆(LSTM)网络的异常网络入侵检测模型,采用粒子群优化(PSO)算法、JAYA 算法和麻雀搜索算法(SSA)优化 LSTM 超参数,实验结果表明模型性能较优。

很多学者采用混合模型进行网络入侵检测,取得了较好的分类效果。Cui 等[7]提出了一种新型多模块集成入侵检测系统 GMM-WGAN-IDS,通过堆叠自编码器(SAE)进行特征提取,将高斯混合模型(GMM)和 Wasserstein 生成对抗网络(WGAN)相结合处理不平衡数据,应用 CNN-LSTM 进行分类,展现出良好的未知攻击检测能力。Zhang 等[8]构建了一种多头注意力机制与双向长短时记忆(BiLSTM)网络相结合的模型,该模型在 KDDCUP99、NSL-KDD、CICIDS2017 数据集上的检测准确率分别达到 98.29%、95.19%、99.08%。Sinha 等[9]提出了一种将 1DCNN 和 BiLSTM 相结合的模型,分别采用 1DCNN 和 BiLSTM 提取空间与长时序特征,模型的整体性能优于支持向量机(SVM)、LSTM 等现有模型。Al-Turaiki 等[10]提出了一种基于 CNN 的检测模型,用于网络攻击的二进制和多分类检测任务,在 NSL-KDD 和 UNSW-NB15 两个数据集上的实验结果均表现良好。Nguyen 等[11]提出了一种联邦无监督异常检测框架 FedPCA,显著提高了异常网络入侵检测性能。

尽管深度学习在一定程度上推动了入侵检测技术的发展,但面对数据分布极不平衡、特征冗余严重以及攻击类别复杂等情况时,仍存在分类性能波动大、关键特征提取能力不足等问题。同时,多数入侵检测方法忽视了深度模型训练之前的特征筛选环节,导致训练过程中处理大量冗余特征,增大了计算开销。

基于上述研究现状,本文提出一种基于 1DCNN 和双向门控循环单元(1DCNN-BiGRU)并引入多头自注意力机制的网络入侵检测模型:利用 1DCNN 提取网络流量的局部空间特征;使用 BiGRU 捕获序列数据的长期依赖关系;引入多头自注意力机制动态聚焦关键特征之间的交互作用,增强模型对复杂关联特征的学习能力。此外,本文采用信息增益(information gain,IG)方法与随机森林(random forest,RF)算法相结合的混合特征选择方法,以有效减少特征冗余。

1 相关理论

1.1 多头自注意力机制

多头自注意力机制源自对人类视觉的仿生模拟,该机制通过动态分配权重的方式,对输入数据中的关键特征赋予显著性权重,对非关键特征赋予

较低权重,从而实现对核心信息的重点关注[12]。

输入数据表示为 $\boldsymbol{S}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n)$,其中 n 表示序列长度,各向量 $\boldsymbol{a}_i(i=1,2,\cdots,n)$ 的特征维度为 d。在多头自注意力机制中,设注意力头的数量为 h,对于第 j 个注意力头($j=1,2,\cdots,h$),将输入矩阵 $\boldsymbol{S}$ 分别与该头对应的查询权重矩阵 $\boldsymbol{W}_j^{\mathrm{Q}}$($\boldsymbol{W}_j^{\mathrm{Q}}\in\mathbf{R}^{d\times d_{\mathrm{k}}}$)、键权重矩阵 $\boldsymbol{W}_j^{\mathrm{K}}$($\boldsymbol{W}_j^{\mathrm{K}}\in\mathbf{R}^{d\times d_{\mathrm{k}}}$)、值权重矩阵 $\boldsymbol{W}_j^{\mathrm{V}}$($\boldsymbol{W}_j^{\mathrm{V}}\in\mathbf{R}^{d\times d_{\mathrm{v}}}$)相乘,其中 d_{k} 是查询矩阵 $\boldsymbol{Q}$ 中每个查询向量的维度,也是键矩阵 $\boldsymbol{K}$ 中每个键向量的维度,d_{v} 是值矩阵 $\boldsymbol{V}$ 中每个值向量的维度。通过该线性变换得到查询矩阵 $\boldsymbol{Q}$、键矩阵 $\boldsymbol{K}$ 和值矩阵 $\boldsymbol{V}$,表达式为

$$\boldsymbol{Q}=\boldsymbol{S}\boldsymbol{W}_j^{\mathrm{Q}},\boldsymbol{K}=\boldsymbol{S}\boldsymbol{W}_j^{\mathrm{K}},\boldsymbol{V}=\boldsymbol{S}\boldsymbol{W}_j^{\mathrm{V}} \tag{1}$$

所有权重矩阵通过反向传播算法进行迭代优化,以增强模型对数据的拟合能力。

为量化特征间的相关性,将 $\boldsymbol{Q}$ 与 $\boldsymbol{K}^{\mathrm{T}}$ 相乘,经过缩放因子 $\sqrt{d_{\mathrm{k}}}$ 进行稳定性调整后,再采用 Softmax 函数进行归一化处理,得到第 j 个注意力头的输出结果(用 head_j 表示),即

$$\mathrm{head}_j(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_{\mathrm{k}}}}\right)\boldsymbol{V} \tag{2}$$

将 h 个头的输出结果 $\mathrm{head}_1,\mathrm{head}_2,\cdots,\mathrm{head}_h$ 拼接整合后,通过与可学习投影矩阵 $\boldsymbol{W}^0$($\boldsymbol{W}^0\in\mathbf{R}^{(hd_{\mathrm{v}})\times d}$)相乘,完成一次线性变换,得到最终输出(用 $\boldsymbol{T}$ 表示),即

$$\boldsymbol{T}=\mathrm{Concat}(\mathrm{head}_1,\mathrm{head}_2,\cdots,\mathrm{head}_h)\cdot\boldsymbol{W}^0 \tag{3}$$

1.2　信息增益方法

信息增益(也称为互信息),是基于信息论的一种特征评估指标,用于量化特征与目标变量之间的相关性[13]。信息论中的熵用于描述离散随机变量的不确定性程度,设 X 与 Y 为离散随机变量,$X\in\{x_1,x_2,\cdots,x_L\}$,$Y\in\{y_1,y_2,\cdots,y_M\}$,$X$ 的熵 $H(X)$ 定义式为

$$H(X)=-\sum_{l=1}^{L}p(x_l)\log_2 p(x_l) \tag{4}$$

式中 $p(x_l)$ 表示 X 取值为 x_l 的概率。

条件熵用于衡量在给定特征取某一特定值的情况下,类别标签仍存在的不确定性大小。用随机变量 X 表示给定特征、Y 表示类别标签,条件熵 $H(Y|X)$ 的定义式为

$$H(Y|X)=-\sum_{l=1}^{L}p(x_l)H(Y|X=x_l) \tag{5}$$

熵和条件熵的差值即为信息增益,用 IG(Y,X)表示,即

$$\mathrm{IG}(Y,X)=H(Y)-H(Y|X) \tag{6}$$

信息增益值反映了在了解特征 X 的相关信息后,分类标签 Y 的不确定性减小的程度。信息增益值越大,表明该特征所包含的用于分类的有效信息越丰富,在单变量特征选择中的重要程度越高。

1.3　随机森林算法

随机森林算法是一种集成学习方法,通过构建多棵决策树形成分类器集合。该算法一方面从原始训练集中进行样本子集的随机抽样(Bootstrap 采样),另一方面在节点分裂时仅考虑随机选取的部分特征,这种独特的训练机制使得每棵决策树都具备差异化的学习视角。随机森林算法通过量化特征在多棵决策树中的重要性,实现对特征重要性的有效评估,特征的重要性得分越高,说明该特征在随机森林算法的决策过程中起到的作用越大,对模型的预测结果影响也越显著。

2　基于 1DCNN-BiGRU 和改进特征选择的网络入侵检测方法

2.1　总体流程

本文提出的网络入侵检测方法总体流程如图 1 所示,具体说明如下。

1)在数据预处理阶段进行数据清洗、独热编码和最小 - 最大归一化。

2)在特征选择阶段,先通过信息增益方法筛选高判别性特征,再利用随机森林算法评估特征重要性,以保留高判别性信息。将信息增益方法与随机森林算法相结合,既能降低计算成本,又能提高特征选择准确率。

3)引入 SMOTE 过采样技术合成少数类样本,缓解因少数类样本不足导致的模型偏倚问题。

4)将处理好的数据输入本文提出的网络入侵检测模型。首先采用 1DCNN 高效捕捉局部关联;再引入多头自注意力机制,使模型能够在不同尺度上同时捕捉序列的长距离依赖关系与局部关联;最后通过 BiGRU 更充分地考虑上下文信息,增强特征表达的多样性。

2.2　数据预处理

本文采用数据清洗、独热编码和最小 - 最大归一化进行数据预处理。在数据清洗阶段进行数据集中缺失值的填补、异常值及重复记录值的清除。

1)独热编码

采用独热编码技术对非数值型数据进行向量化处理。该方法通过为各类别特征生成唯一的二

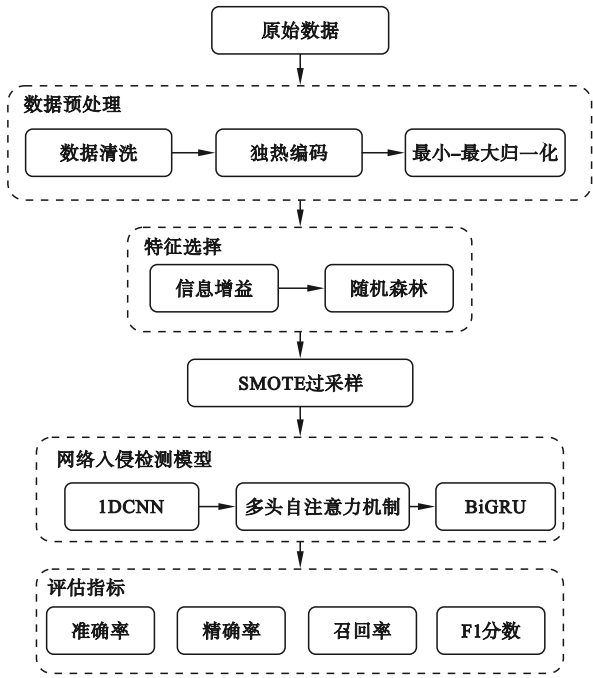

图 1 网络入侵检测方法总体流程

Fig. 1 The overall workflow of the network intrusion detection method

进制向量,将非数值型数据转化为数值型特征向量。本文针对数据集中 proto、state 和 service 三个类别特征实施编码操作。

2)归一化

采用最小–最大归一化方法将数值型特征的取值范围统一缩放到[0,1]区间内,旨在消除特征间的尺度差异,以提升模型的稳定性和训练效率。具体归一化公式为

$$F_i' = \frac{F_i - F_{\min}}{F_{\max} - F_{\min}} \tag{7}$$

式中:$F_{\min}$和 $F_{\max}$分别表示特征的最小值和最大值;F_i 为第 i 个原始特征值;F_i'为归一化后的第 i 个特征值。

2.3 模型结构

本文提出的网络入侵检测模型详细结构如图 2 所示。首先,将长度为 30 的特征向量序列输入 1DCNN 结构层中。由于网络流量特征在时间或特征维度上具有强烈的一维局部性,相较于将数据转换为二维格式后再应用于传统 CNN,1DCNN 可更高效地提取邻近时间特征。本文中 1DCNN 采用 30×128 卷积操作,即适配输入长度为 30、通道数(滤波器数量)为 128,采用尺寸为 5×5 的卷积核。然后,利用多头自注意力机制动态地计算输入序列中不同位置元素的重要性并赋予不同的权重,从而突出关键特征。注意力头数设为 4,每个头的键向量维度设置为 64,计算完成后,特征维度保持为 10×128。再后,采用 BiGRU 进一步学习时序特征。BiGRU 由正向与反向门控循环单元(GRU)组成,单个 GRU 单元隐层维度设为 128(双向拼接后输出维度为 256)。为防止过拟合,模型在多个层次上引入丢弃层,并在多头自注意力层输出与输入之间添加残差连接,结合层归一化稳定训练过程。最后,通过全连接层并经过 Softmax 激活函数处理,输出多类别检测结果(概率分布)。

3 实验结果与分析

3.1 实验配置

为验证本文提出模型的性能,搭建如下实验环境:在硬件方面,操作系统选用 Windows 11,配备 Intel i5-8265U CPU 处理器及 16 GB 内存;在软件方面,基于 Python 3.8.8 进行代码开发,深度学习框架采用 TensorFlow 2.17.1、Keras 3.5.0。

3.2 数据集和模型评估指标

使用公开可用的 NSL-KDD 数据集[14]和 UNSW-NB15 数据集[15]对本文模型进行全面评估。NSL-KDD 数据集作为经典 KDD Cup 99 数据集的优化版本,通过消除原始数据中的重复记录和冗余样本,显著改善了数据质量。该数据集主要包含 41 个属性特征,涵盖正常(Normal)、端口扫描等探测行为(Probe)、拒绝服务攻击(DoS)、远

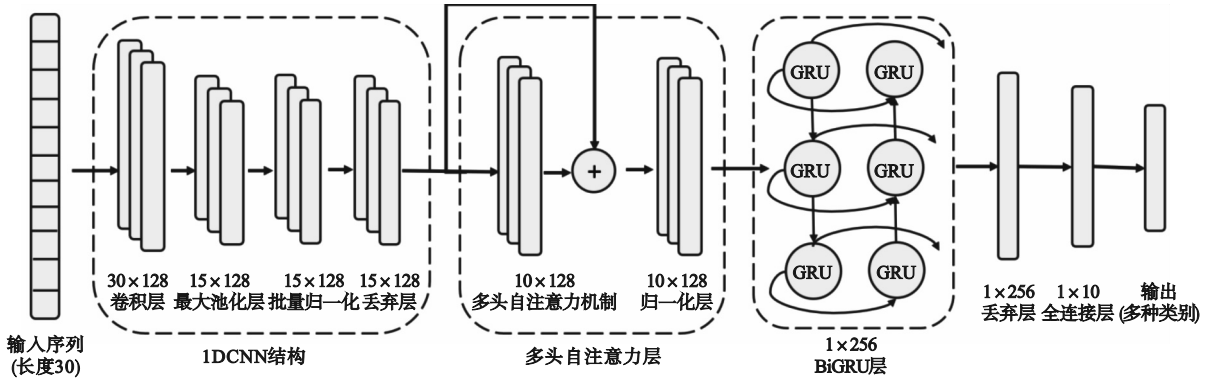

图 2　引入多头自注意力机制的 1DCNN-BiGRU 模型结构

Fig. 2　1DCNN-BiGRU model architecture incorporated with a multi-head self-attention mechanism

程到本地攻击(R2L)、用户到根攻击(U2R)等 5 种攻击类别,各攻击类别的样本分布详情如表 1 所示。

表 1　NSL-KDD 数据集的攻击类别样本分布

Table 1　The distribution of attack categories in NSL-KDD dataset

攻击类别	样本数量
Normal	77 232
DoS	53 387
Probe	14 363
R2L	3 416
U2R	119
总计	148 517

UNSW-NB15 数据集由澳大利亚网络安全中心于 2015 年使用 IXIA PerfectStorm 工具模拟真实网络环境生成。该数据集包含 49 个属性特征,涵盖 10 种典型攻击类别,具体包括模糊测试(Fuzzers)、分析攻击(Analysis)、后门攻击(Backdoor)、拒绝服务攻击(DoS)、漏洞利用(Exploits)、通用攻击(Generic)、侦察攻击(Reconnaissance)、外壳代码攻击(Shellcode)、蠕虫攻击(Worms)和正常(Normal),各类别样本在数据集中的具体分布情况详见表 2。

表 2　UNSW-NB15 数据集的攻击类别样本分布

Table 2　The distribution of attack categories in UNSW-NB15 dataset

攻击类别	样本数量
Normal	93 000
Analysis	2 677
Backdoor	2 329
DoS	16 353
Exploits	44 525
Fuzzers	24 246
Generic	58 871
Reconnaissance	13 987
Shellcode	1 511
Worms	174
总计	257 673

本文采用准确率、精确率、召回率和 F1 分数作为模型性能评估指标。准确率用于衡量模型对所有样本的整体预测正确性,定义为正确预测的样本数占总样本数的比例;精确率反映模型对正样本预测的精准程度,定义为预测为正的样本中实际为正的比例;召回率反映模型对正样本的捕捉能力,定义为实际为正的样本中被正确预测的比例;F1 分数作为精确率与召回率的调和平均值,用于综合评估模型在正负样本上的均衡表现。

3.3　特征选择

本节以 UNSW-NB15 数据集为例进行特征选择实验结果的详细分析。将通过信息增益方法与随机森林算法确定的特征重要性评分标准化后再加权求和,得到综合评分,筛选出综合评分排名前 30 的特征,这些特征的重要性排序情况如图 3 所示。

由图 3 可以看出:采用信息增益方法得到的评分较高的特征主要集中在前几项,如 sbytes、smean、sload 等;随机森林算法不仅考虑特征本身的贡献,更关注特征间的交互作用,采用随机森林算法得到的特征重要性评分整体上较高,尤其是 ct_dst_sport_ltm、ct_srv_src 等特征。综合来看,无论信息增益方法还是随机森林算法,前几个特征(如 sbytes、smean、sload 等)均得分较高,表明其在流量特征中起至关重要的作用,如 sbytes(字节数)反映了网络流量的数据传输规模大小,而 smean 和 sload 则与流量均值和负载状况相关。本文提出的特征选择方法能够显著降低数据维度,将通过特征选择得到的特征序列作为模型的输入,以保证其稳定运行。

3.4　模型训练结果分析

图4和图5分别展示了模型在NSL-KDD数

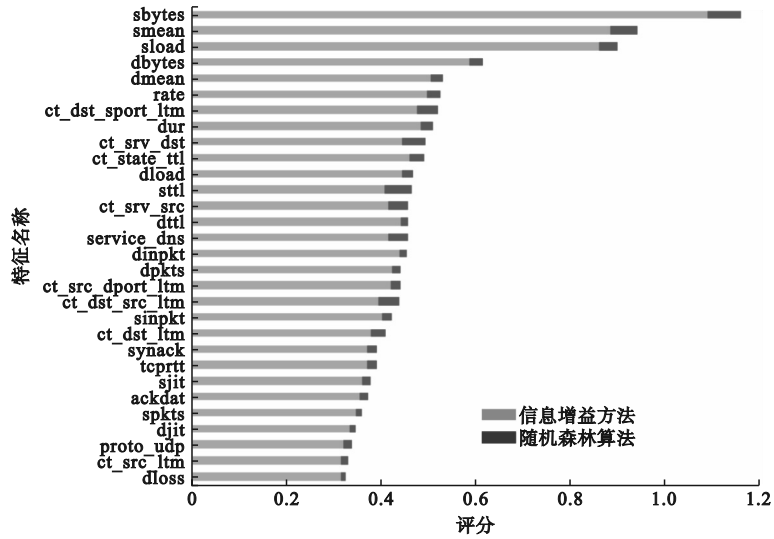

图 3 基于信息增益方法和随机森林算法的特征重要性排序

Fig. 3 Feature importance ranking based on information gain and random forest

据集和 UNSW-NB15 数据集上训练过程中的损失值与准确率变化曲线。对于 NSL-KDD 数据集:经过 200 轮的迭代,模型训练的损失值从初期的较高值(约 0.078)逐步降低并收敛,最终趋于稳定;准确率则从较高起点(约 96.7%)开始,随着训练轮次的增加逐步提升,最终稳定在 99.4% 左右。对于 UNSW-NB15 数据集:在训练 20 轮后,损失值趋于平稳;随着训练轮次增加,准确率表现为先快后慢的上升趋势,最终基本稳定在 84.0% 以上。模型在不同数据集上的训练过程中均表现出较好的收敛性。

本文模型在 NSL-KDD 数据集上的总训练用时为 7 636.50 s(约 127.28 min),在测试样本上的总预测耗时为 3.0 s,单样本平均分类时间为 0.101 ms;在 UNSW-NB15 数据集上的总训练用时为 2 266.60 s(约 37.78 min),在测试样本上的总预测耗时为 4.0 s,单样本平均分类时间为 0.077 6 ms。实验结果表明,模型在两个数据集上的单样本平均分类时间均远低于常见的在线服务延迟门槛(1 ~ 10 ms),符合在线实时入侵检测系统的延迟标准。

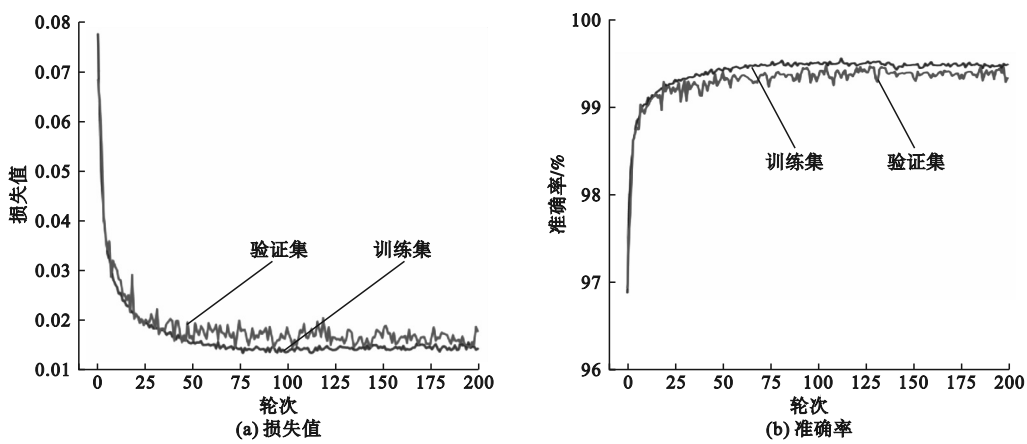

图 4 NSL-KDD 数据集上的模型训练损失值与准确率迭代变化曲线

Fig. 4 Iterative curves of training loss and accuracy on NSL-KDD dataset

3.5 消融实验

将本文模型中的各模块依次移除,分别在 NSL-KDD 和 UNSW-NB15 数据集上进行消融实验,实验结果如表 3 ~ 4 所示。在 NSL-KDD 数据集上:CNN-BiGRU 模型的性能显著优于单一模型(CNN 或 BiGRU),这是因为 CNN 虽擅长提取局部特征,但难以对长距离依赖关系建模,BiGRU 则恰好弥补了这一缺陷;本文提出模型的准确率和 F1 分数分别达到 99.65% 和 99.64%,与仅使用 CNN 的模型相比,分别提高了 4.48% 和 4.97%,

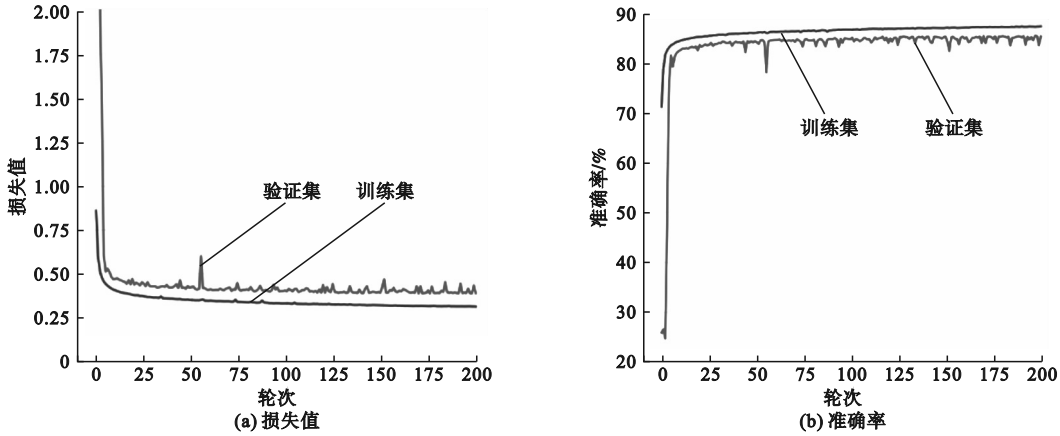

图 5　UNSW-NB15 数据集上的模型训练损失值与准确率迭代变化曲线

Fig. 5　Iterative curves of training loss and accuracy on UNSW-NB15 dataset

相较于 CNN-BiGRU 模型分别提高了 1.42% 和 2.15%,说明多头自注意力机制的引入能够有效捕捉输入序列中的关键特征并权衡其重要性,使模型聚焦于与攻击最相关的信息,从而显著提升了分类性能;此外,相比仅使用 BiGRU 的模型,本文模型的准确率和 F1 分数分别提高了 9.82% 和 10.16%,说明 1DCNN 在局部特征提取方面具有重要作用。在 UNSW-NB15 数据集上:CNN-BiGRU 模型的整体性能同样优于 CNN 或 BiGRU 单一模型;本文模型的准确率和 F1 分数分别达到 84.83% 和 84.86%,与 CNN-BiGRU 模型相比,分别提升了 3.04% 和 3.20%,进一步验证了多头自注意力机制在复杂场景下的特征增强能力。与单一 CNN 或 BiGRU 模型相比,本文模型均有显著的性能提升,说明 1DCNN、BiGRU 与注意力机制三者有效融合,兼具局部特征提取、长距离依赖关系建模和关键信息捕获的优势。

表 3　NSL-KDD 数据集上的消融实验结果

Table 3　Ablation study results on NSL-KDD dataset

模型	准确率/%	精确率/%	召回率/%	F1 分数/%
CNN	95.38	95.68	94.17	94.92
BiGRU	90.74	91.25	89.67	90.45
CNN-BiGRU	98.25	98.26	96.83	97.54
本文模型	99.65	99.84	99.45	99.64

表 4　UNSW-NB15 数据集上的消融实验结果

Table 4　Ablation study results on UNSW-NB15 dataset

模型	准确率/%	精确率/%	召回率/%	F1 分数/%
CNN	80.86	77.44	79.88	78.64
BiGRU	82.45	81.18	80.71	80.94
CNN-BiGRU	82.33	81.90	82.57	82.23
本文模型	84.83	85.16	84.57	84.86

3.6　对比实验

在相同的实验条件下,将本文模型与近年提出的几种主流入侵检测模型进行对比实验,结果如表 5 所示。

表 5　不同入侵检测模型的对比

Table 5　Comparison of different intrusion detection models

数据集	模型	准确率/%	F1 分数/%
NSL-KDD	SSA-LSTM[6]	97.89	97.30
	CNN-LSTM[7]	86.59	86.88
	Multi-Head Attention-BiLSTM[8]	95.19	97.00
	本文模型	99.65	99.64
UNSW-NB15	CNN-BiLSTM[9]	82.08	81.32
	MCNN-DFS[10]	80.51	81.00
	FEDPG[11]	81.95	87.77
	本文模型	84.83	84.86

由表 5 中 NSL-KDD 数据集上的实验结果可知:与 SSA-LSTM 模型相比,本文模型虽更为复杂,但由于采用了多头自注意力机制,对于 U2R、R2L 等罕见攻击的识别能力更优,在准确率和 F1 分数上分别提高了 1.80% 和 2.40%;与传统的 CNN-LSTM 模型相比,本文模型的准确率和 F1 分数分别提高了 15.08% 和 14.69%;与 Multi-Head Attention-BiLSTM 模型相比,由于本文采用了 BiGRU 结构,参数规模更加精简,特征交互更加高效,准确率提升了 4.68%。由 UNSW-NB15 数据集上的实验结果可知:与经典的 CNN-BiLSTM 模型相比,本文模型的准确率提升了 3.35%,F1 分数提升了 4.35%;与 MCNN-DFS 模型相比,本文模型在准确率与 F1 分数上均有提

升,综合性能更优,同时模型结构更为高效;FED-PG 模型的 F1 分数较高(87.77%),但其准确率较低(81.95%),表明该模型可能存在较高的误报率,本文模型的分类结果更加可靠。

4 结论

提出了一种基于 1DCNN-BiGRU 和改进特征选择的网络入侵检测方法。采用信息增益方法和随机森林算法评估特征的重要性,并使用 SMOTE 过采样技术解决数据类别分布不平衡问题;利用 1DCNN 提取流量数据的局部特征,引入多头自注意力机制通过自适应权重分配捕获关键特征,使用 BiGRU 挖掘流量序列的时序依赖关系。实验结果表明,本文提出模型在 NSL-KDD 数据集上的准确率达到 99.65%,在 UNSW-NB15 数据集上的准确率达到 84.83%,均高于其他对比入侵检测模型。

参考文献(References):

[1] 王玉芳,杨怀洲. 基于深度学习的网络入侵检测综述[J]. 无线互联科技,2024,21(7):122 – 124.
Wang Y F, Yang H Z. Review of network intrusion detection based on deep learning[J]. Wireless Internet Science and Technology, 2024, 21(7): 122 – 124. (in Chinese)

[2] Wang L X, Yang J H, Xu X H, et al. Mining network traffic with the k-means clustering algorithm for stepping-stone intrusion detection[J]. Wireless Communications and Mobile Computing, 2021, 2021: 6632671.

[3] Qazi E U H, Almorjan A, Zia T. A one-dimensional convolutional neural network (1D-CNN) based deep learning system for network intrusion detection[J]. Applied Sciences, 2022, 12(16): 7986.

[4] 黄迎春,任国杰. 基于 PER-PPO2 的入侵检测技术[J]. 沈阳理工大学学报,2024,43(5):7 – 13.
Huang Y C, Ren G J. Intrusion detection technology based on PER-PPO2[J]. Journal of Shenyang Ligong University, 2024, 43(5): 7 – 13. (in Chinese)

[5] Albasheer F O, Haibatti R R, Agarwal M, et al. A novel IDS based on Jaya optimizer and SMOTE-ENN for cyberattacks detection[J]. IEEE Access, 2024, 12: 101506 – 101527.

[6] Dash N, Chakravarty S, Rath A K, et al. An optimized LSTM-based deep learning model for anomaly network intrusion detection[J]. Scientific Reports, 2025, 15(1): 1554.

[7] Cui J Y, Zong L S, Xie J H, et al. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data[J]. Applied Intelligence, 2023, 53(1): 272 – 288.

[8] Zhang J Q, Zhang X, Liu Z J, et al. A network intrusion detection model based on BiLSTM with multi-head attention mechanism[J]. Electronics, 2023, 12(19): 4170.

[9] Sinha J, Manollas M. Efficient deep CNN-BiLSTM model for network intrusion detection[C]//Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition. Xiamen, China: ACM, 2020: 223 – 231.

[10] Al-Turaiki I, Altwaijry N. A convolutional neural network for improved anomaly-based network intrusion detection[J]. Big Data, 2021, 9(3): 233 – 252.

[11] Nguyen T A, Le L T, Nguyen T D, et al. Federated PCA on Grassmann manifold for IoT anomaly detection[J]. IEEE/ACM Transactions on Networking, 2024, 32(5): 4456 – 4471.

[12] Wang Y, Yang G C, Li S B, et al. Arrhythmia classification algorithm based on multi-head self-attention mechanism[J]. Biomedical Signal Processing and Control, 2023, 79: 104206.

[13] Yin Y H, Jang-Jaccard J, 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): 15.

[14] Su T T, Sun H Z, Zhu J Q, et al. BAT: deep learning methods on network intrusion detection using NSL-KDD dataset[J]. IEEE Access, 2020, 8: 29575 – 29585.

[15] Kasongo S M, Sun Y X. Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset[J]. Journal of Big Data, 2020, 7(1): 105.

(责任编辑:宋颖韬)