DOI:10.19651/j.cnki.emt.2519098

基于多层次特征融合的不平衡网络流量异常检测方法*

申明娜 王佩雪 孟永伟 户佳乐
(中原工学院计算机学院 郑州 451191)

摘 要:针对现有网络流量异常检测方法因数据不平衡和特征提取能力不足导致准确率低的问题,提出一种基于多层次特征融合的不平衡网络流量异常检测方法。通过 CGAN-SMOTE 算法平衡数据分布;在特征提取阶段,利用门控循环单元捕捉时间序列数据中的长期依赖关系,并结合注意力机制自适应分配权重,提取关键时间局部特征;同时,采用双向长短时记忆神经网络和平均池化,提取数据时间全局特征;最后,将提取的时间局部与全局特征融合,利用改进的卷积神经网络提取空间维度特征,从而增强模型对异常数据的识别能力。在公开数据集上的实验结果表明,本文提出的异常检测模型相比现有多种方法具有更优的检测性能。

关键词:异常检测;特征提取;双向长短期记忆网络;自注意力;门控循环单元;卷积神经网络
中图分类号:TN915.08 **文献标识码**:A **国家标准学科分类代码**:510.40

Multi-level feature fusion for imbalanced network anomaly detection

Shen Mingna Wang Peixue Meng Yongwei Hu Jiale
(School of Computer Science, Zhongyuan University of Technology, Zhengzhou 451191, China)

Abstract: This study presents a multi-level feature fusion approach for imbalanced network traffic anomaly detection to overcome the accuracy limitations of existing methods caused by data imbalance and insufficient feature extraction. The proposed framework first employs CGAN-SMOTE algorithm to balance data distribution, then utilizes gated recurrent units with attention mechanisms to capture long-term dependencies and extract discriminative temporal local features through adaptive weight allocation. Concurrently, bidirectional long short-term memory networks with average pooling are applied to obtain comprehensive temporal global features. These extracted temporal features are subsequently fused and processed by an enhanced convolutional neural network to learn spatial representations, significantly improving anomaly recognition capability. Experimental validation on public datasets confirms the superior detection performance of our model compared to various state-of-the-art methods.

Keywords: anomaly detection; feature extraction; bidirectional long short-term memory; self-attention; gated recurrent unit; convolutional neural network

0 引 言

随着网络技术的迅猛发展,网络攻击事件日益增多,网络安全已成为全球关注的焦点。网络流量异常检测系统作为保障网络安全的关键技术,主要任务是监测和识别网络流量中的异常行为,但随着攻击手段的复杂和多样化,传统的网络流量异常检测系统难以识别零日攻击和未知攻击[1]。近年来,深度学习技术广泛应用于网络流量异常检测领域,并展现出显著的检测成效。文献[2]通过多头注意力从多个维度提取特征,利用多层双向长短期记忆(bidirectional long short-term memory network,BiLSTM)捕捉长距离依赖关系,并使用门控高速连接减轻网络中的梯度消失问题。文献[3]构建三层堆叠长短期记忆网络(long-short termmemory,LSTM)和带跳跃连接线的改进残差神经网络实现对 NSL-KDD 数据集的入侵检测,但处理大规模数据集时计算复杂度较高,对某些罕见攻击类型的检测率低。文献[4]利用三层膨胀卷积和改进的卷积块注意力模块增强提取高级特征的能力,通过双向门控循环

收稿日期:2025-06-14
*基金项目:国家自然科学基金(62302540)、河南省重点研发专项(251111212000)、中原工学院自然科学基金 (K2023MS017)项目资助

单元(bidirectional gated recurrent unit,BiGRU)深入捕捉特征间的长期依赖关系,但网格效应会破坏数据的固有拓扑结构,进而影响 BiGRU 的时序精度。文献[5]提出一种基于卷积神经网络(convolutional neural network,CNN)和 BiGRU 的异常检测模型,但该模型结构的特征提取能力有限,难以充分捕获网络流量数据中的复杂特征。文献[6]通过 CNN 提取非线性特征,BiGRU 提取时序特征,并利用注意力机制区分特征重要性,但对决策边界附近的少数类样本分类效果仍存在改进空间。文献[7]使用合成少数类过采样技术(synthetic minority over-sampling technique,SMOTE)处理不平衡数据,难以适应高维复杂数据的非线性分布特征,导致合成样本偏离真实数据分布规律。

通过上述分析,为解决网络入侵流量中数据不平衡和特征提取不充分,导致检测准确率低的问题。本文提出一种基于多层次特征融合的不平衡网络流量异常检测方法。本文的创新点:

1)设计 CGAN-SMOTE 采样算法,先利用条件生成对抗网络(conditional generative adversarial network,CGAN)生成高真实性样本,后使用 SMOTE 进行插值扩充,双重增强少数类数据。

2)设计一种基于多层次特征融合的不平衡网络流量异常检测模型,利用 GRU 模块和 BiLSTM 模块有效提取时间维度的局部和全局信息,并结合 CNN 模块捕捉空间特征,提升异常检测的准确性。

3)在 NSL-KDD、UNSW-NB15 和 Kyoto2016 数据集上评估分类性能,验证所提的检测模型。实验表明,本文模型在准确率、精确度、召回率和 F1 分数上均优于现有模型。

1 相关研究

网络异常流量检测作为信息安全领域的一个重要研究方向,其核心目标是通过监测和分析网络流量中的异常模式,及时发现潜在的恶意行为、网络攻击或系统故障[8]。近年来,网络流量异常检测技术已从传统的规则和统计方法发展为基于机器学习和深度学习的先进方法。

基于机器学习的网络异常流量检测主要依赖于支持向量机、随机森林、K 最近邻[9]等算法,通过分析网络流量的特征来识别异常。文献[10]通过融合多维特征空间信息捕捉网络异常数据的复杂模式,并采用支持向量机分类方法提升异常检测的准确性。文献[11]提出一种基于加权策略的异常检测方法,通过随机森林筛选关键特征并分配属性权重,采用 K 近邻算法实现异常识别,但传统机器学习方法因分类器固有局限导致检测精度不足。随着深度学习的发展,研究者正探索将其应用于网络异常检测以提升性能。

基于深度学习的网络异常流量检测利用深度神经网络自动从大量数据中提取特征。深度学习模型如 CNN[12]和循环神经网络及其变体在特征提取方面具有显著优势。文献[13]在卷积层加入批量归一化,并通过 Flatten 操作过渡到全连接层,同时引入 Dropout 层增强模型的泛化能力。文献[14]采用 1 D-CNN 来捕捉数据中的局部模式,并结合 BiGRU 来深入挖掘数据的时间序列特性。文献[15]通过注意力机制对分类任务中的关键特征进行加权,依据其重要性分配权重,从而增强对罕见攻击类型的检测能力。文献[16]采用 SMOTE 过采样技术平衡数据集,结合深度特征合成提取高阶特征,并通过跳跃连接机制增强 CNN 不同层级间的特征融合能力。文献[17]使用改进的鱼鹰优化算法来选择网络流量中最相关和最重要的特征,降低特征的维度,并设计 1 D 深度残差收缩网络的分类器。文献[18]融合多层 BiGRU 和改进的前馈神经网络,采用数据过采样技术和半监督学习训练方式评估网络流量异常检测中的性能。文献[19]将注意力机制与深度堆叠自编码器相结合,对入侵数据进行编码和转换,以改善卷积层的特征提取能力。然而,在实际网络环境中,异常流量与正常流量比例严重失衡,导致模型对少数类样本学习不足;同时,现有方法在特征提取方面存在局限性,难以充分捕获流量数据之间的复杂特性。

2 本文方法

2.1 网络流量异常检测整体框架

传统网络流量异常检测方法由于特征提取能力不足,往往难以充分捕捉流量数据中的复杂模式,导致检测准确率降低。为了提高网络流量异常检测的准确率,本文提出一种基于多层次特征融合的不平衡网络流量异常检测模型,整体框架如图 1 所示。该网络模型主要由数据预处理、数据平衡处理、网络流量异常检测模型和检测结果评估组成。

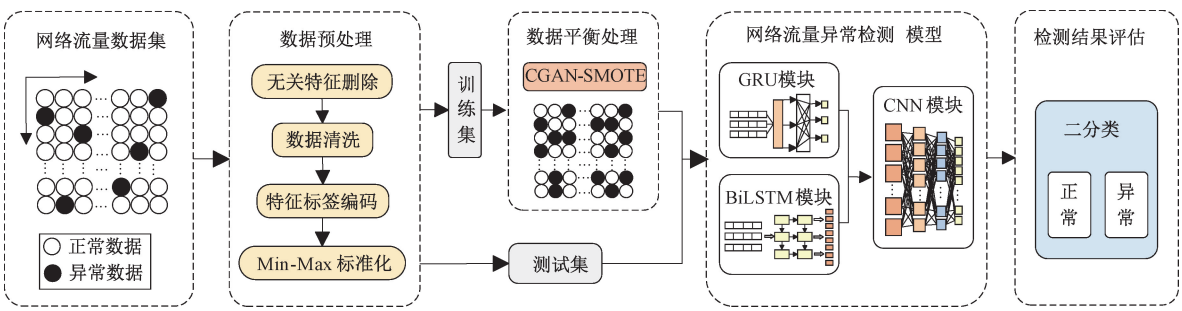

图 1 网络流量异常检测整体框架

Fig. 1 Overall framework of network traffic anomaly detection

1)数据预处理:删除无关特征、数据清洗、非数值型数据利用标签编码转换为数值型、数值型数据使用 Min-Max 标准化缩放到一定的范围。

2)数据平衡处理:利用 CGAN-SMOTE 算法对少数类别样本采样,保持数据的多样性和复杂性,使数据集达到平衡。

3)网络流量异常检测模型:通过 GRU 模块捕捉长期依赖性,提取时间局部特征;同时,利用 BiLSTM 模块捕捉序列的双向依赖及复杂非线性模式,提取时间全局特征。将时间局部和全局特征融合通过改进的 CNN 模块提取空间特征,最终实现高效分类。

4)检测评估模块:在 UNSW_NB15 数据集、NSL-KDD 数据集和 Kyoto2016 数据集上用准确率、精确率、召回率和 F1 值 4 个关键指标来评估模型的性能。

2.2　基于改进的 CGAN-SMOTE 混合采样方法

CGAN 通过对少数类样本进行对抗训练,生成具有高度真实性的合成样本。CGAN 的框架图如图 2 所示。但 CGAN 生成样本存在边缘分布偏离真实数据分布的问题。在此基础上,引入 SMOTE 在 CGAN 生成样本与原始样本构成的混合特征空间中进行二次采样,有效增加样本多样性,使少数类样本分布更加均匀。CGAN 的目标函数为:

$$\min_{G}\max_{D}V(D,G)=\mathrm{E}_{x\sim Pr}\{\log[D(\boldsymbol{x}\mid\boldsymbol{y})]\}+\mathrm{E}_{z\sim Pz}[\log(1-D(G(\boldsymbol{z}\mid\boldsymbol{y})))] \tag{1}$$

式中:D 是判别器、G 是生成器、$\boldsymbol{x}$ 为真实样本、Pr 为真实样本分布、Pz 为随机噪声、$\boldsymbol{z}$ 为随机噪声、E 为期望值。

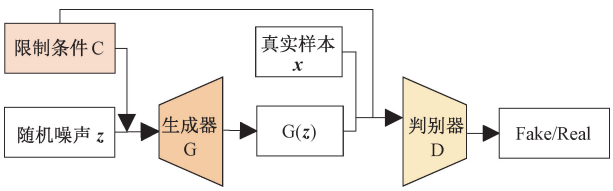

图 2　CGAN 框架图

Fig. 2　Framework diagram of CGAN

CGAN-SMOTE 采样的具体算法如算法 1 所示。

2.3　网络流量异常检测方法

为提升特征提取能力,本文设计一种基于多层次特征融合的不平衡网络流量异常检测方法,如图 3 所示。GRU 模块动态计算序列中元素之间的关系,增强与类别相关特征的权重,提取时间局部特征;BiLSTM 模块捕捉流量数据的整体趋势和全局行为模式,进一步提取全局特征;CNN 模块通过对融合后的时序特征进行空间维度建模,实现多尺度特征增强,从而提升流量异常检测的准确率。

1) GRU 模块提取时间局部特征

GRU 可以更好地处理长序列数据时遇到的梯度消失和梯度爆炸问题,有效地捕捉长距离依赖关系。GRU 结构图如图 4 所示。

在 GRU 模型中,输入向量 $\boldsymbol{X}=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_{n-1},\boldsymbol{x}_n\}$

算法 1:CGAN-SMOTE 采样算法

输入:原始数据集 $\boldsymbol{X}$

输出:平衡后的数据集 $\boldsymbol{X}'$

```
for c∈T do
    提取类别 c 的样本子集 X_c={(x,y)∈X|y=c}
    初始化生成器 G:R^L×R→R^d 判别器 D:R^d×R→[0,1]
    for epoch=1 to E do
        for 批量数据 B ⊆ X_c do
            采样噪声 z~N(0,I)
            生成假样本 x=G(z,c)
            计算判别器损失 D_loss=BCE(D(x,c),1)+BCE(D(x̃,c),0)
            更新判别器参数
            重新采样噪声 z~N(0,I)
            计算生成器损失 G_loss=BCE(D(G(z,c),c),1)
            更新生成器参数
        end for
    end for
    采样噪声矩阵 Z∈R^{K×L}
    生成样本 X''_c={G(z,c)|z∈Z}
    更新数据集 S=S∪{(x,c)|x∈X''_c}
end for
D=D∪S
计算各类样本数 n_c=|{(x,y)∈X|y=c}|, ∀c∈{0,1,…,C−1}
设定目标样本数 n'_c=max({n_c})
for c∈T do
    while n_c<n'_c do
        随机选择样本 x 及其近邻 x_nn
        生成样本 x_new=x+λ(x_nn−x), λ~U(0,1)
        更新数据集 X=X∪{(x_new,c)}
        n_c=n_c+1
    end while
end for
输出平衡后的数据集 X'=X
```

通过 GRU 层进行处理,每个时间步的输入 $\boldsymbol{x}_t$ 处理结果是一个隐藏状态 $\boldsymbol{h}_t$。隐藏状态 $\boldsymbol{h}_t$ 是通过更新门 $\boldsymbol{z}_t$ 和重置门 $\boldsymbol{r}_t$ 的计算得到的,这些门控制着信息的流动。GRU 的计算过程如式(2)~(5)所示。

$$\boldsymbol{z}_t=\sigma(\boldsymbol{W}_z\boldsymbol{x}_t+\boldsymbol{U}_z\mathbf{h}_{t-1}+\boldsymbol{b}_z) \tag{2}$$

$$\boldsymbol{r}_t=\sigma(\boldsymbol{W}_r\boldsymbol{x}_t+\boldsymbol{U}_r\boldsymbol{h}_{t-1}+\boldsymbol{b}_r) \tag{3}$$

$$\tilde{\boldsymbol{h}}_t=\tanh(\boldsymbol{W}_h\boldsymbol{x}_t+\boldsymbol{U}_n(\boldsymbol{r}_t\odot\boldsymbol{h}_{t-1})+\boldsymbol{b}_h) \tag{4}$$

$$\boldsymbol{h}_t=(1-\boldsymbol{z}_t)\odot\boldsymbol{h}_{t-1}+\boldsymbol{z}_t\odot\tilde{\boldsymbol{h}}_t \tag{5}$$

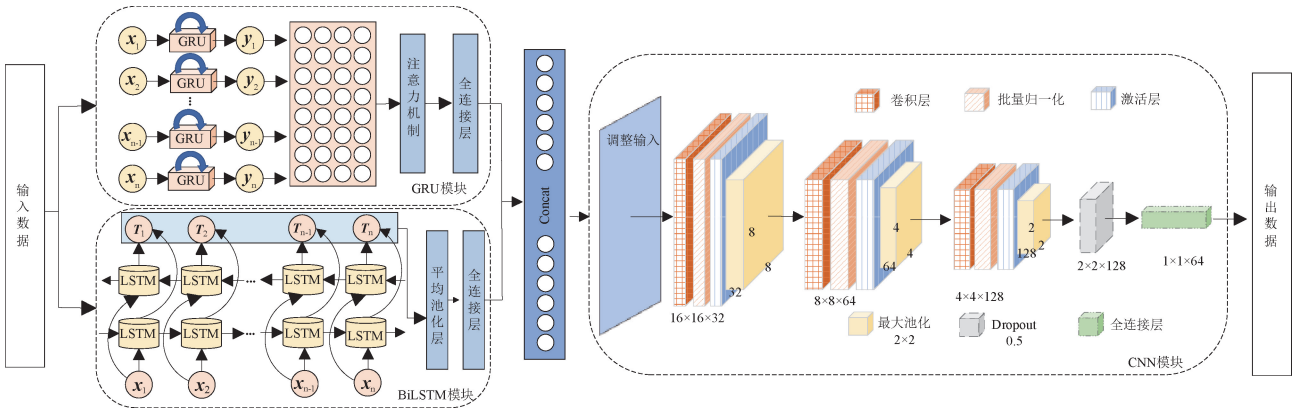

图 3 网络流量异常检测模型结构图

Fig. 3 Architecture diagram of the network traffic anomaly detection model

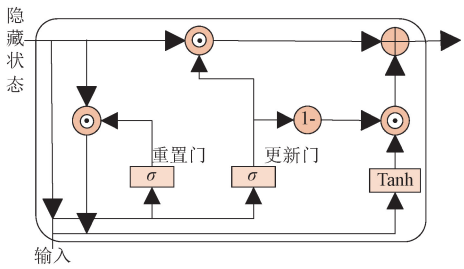

图 4 GRU 结构图

Fig. 4 Structure diagram of GRU

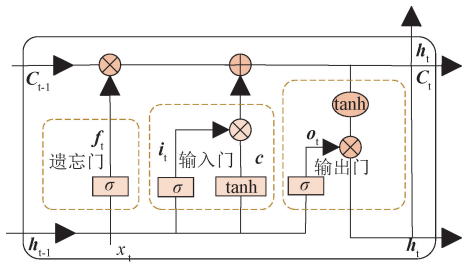

图 5 LSTM 结构

Fig. 5 Structure of LSTM

式中:$\boldsymbol{W}$ 是 $\boldsymbol{x}t$ 权重矩阵、$\boldsymbol{b}$ 是偏置项、σ 是 sigmoid 激活函数、$\boldsymbol{U}$ 是上一时刻隐藏状态的权重矩阵、tanh 是双曲正切激活函数,$\odot$ 表示 Hadamard 积。

将 GRU 得到的输出值 $\boldsymbol{Y}=\{\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_{n-1},\boldsymbol{y}_n\}$ 输入到 Attention 机制中,为输入序列中的每个元素分配权重,增强模型对关键特征的表示能力。Attention 机制的计算过程如式(6)~(10)所示。

$$\boldsymbol{Q}_i=\boldsymbol{W}^Q\boldsymbol{y}_i,\boldsymbol{K}_i=\boldsymbol{W}^K\boldsymbol{y}_i,\boldsymbol{V}_i=\boldsymbol{W}^V\boldsymbol{y}_i \tag{6}$$

$$E_{ij}=\boldsymbol{Q}_i\cdot\boldsymbol{K}_j^{\mathrm{T}} \tag{7}$$

$$S_{ij}=\frac{E_{ij}}{\sqrt{d_k}} \tag{8}$$

$$\alpha_{ij}=\frac{\exp(S_{ij})}{\sum_{j=1}^{n}\exp(S_{ij})} \tag{9}$$

$$\boldsymbol{C}_i=\sum_{j=1}^{n}\alpha_{ij}\boldsymbol{V}_j \tag{10}$$

式中:$\boldsymbol{Q}_i$ 为查询值,$\boldsymbol{K}_j$ 为键值,$\boldsymbol{W}^Q$、$\boldsymbol{W}^K$ 和 $\boldsymbol{W}^V$ 为权重矩阵,T 代表转置,E_{ij} 为注意力得分,d_k 为键向量的维度,S_{ij} 表示缩放后点积,a_{ij} 为注意力权重,$\boldsymbol{C}_i$ 为上下文向量。

2) BiLSTM 模块提取时间全局特征

LSTM 网络是一种特殊的 RNN,能够有效地存储和提取长期信息,结构如图 5 所示。

LSTM 结构包括输入门 $\boldsymbol{i}_t$、遗忘门 $\boldsymbol{f}_t$ 和输出门 $\boldsymbol{o}_t$,以及临时记忆状态 $\tilde{\boldsymbol{c}}_t$、当前记忆状态 $\boldsymbol{c}_t$ 和最终隐藏层状态 $\boldsymbol{h}_t$。计算式(11)~(16)描述了 LSTM 的计算过程。

$$\boldsymbol{i}_t=\sigma(\boldsymbol{W}_i\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_i) \tag{11}$$

$$\boldsymbol{f}_t=\sigma(\boldsymbol{W}_f\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_f) \tag{12}$$

$$\boldsymbol{o}_t=\sigma(\boldsymbol{W}_o\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_o) \tag{13}$$

$$\tilde{\boldsymbol{c}}_t=\tanh(\boldsymbol{W}_c\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_c) \tag{14}$$

$$\boldsymbol{c}_t=\boldsymbol{f}_t\cdot\boldsymbol{c}_{t-1}+\boldsymbol{i}_t\cdot\tilde{\boldsymbol{c}}_t \tag{15}$$

$$\boldsymbol{h}_t=o_t\cdot\tanh(\boldsymbol{c}_t) \tag{16}$$

LSTM 是单向的,只能从前向后传递信息。为更好地捕捉序列中长期依赖关系,用 BiLSTM 对序列 $\boldsymbol{X}=\{\boldsymbol{x}_1,\boldsymbol{x}_2\cdots,\boldsymbol{x}_n\}$ 双向编码,拼接前向与后向隐藏状态,再经平均池化得到全局特征。BiLSTM 结构图如图 6 所示。

$$\boldsymbol{H}_t=[\overrightarrow{\boldsymbol{h}_t}^{\text{前向}},\overleftarrow{\boldsymbol{h}_t}^{\text{后向}}] \tag{17}$$

式中:$\boldsymbol{H}_t$ 表示 t 时刻经前向输出和反向输出拼接后的最终输出结果。

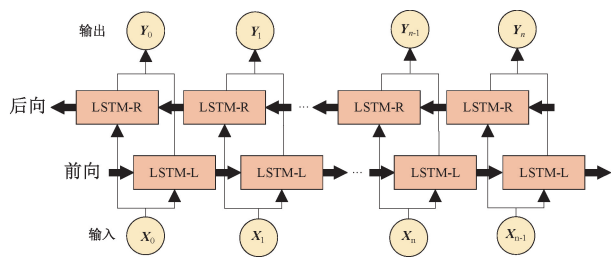

图 6 BiLSTM 结构图

Fig. 6 Structure diagram of BiLSTM

3）CNN 模块提取空间特征

改进的 CNN 模块包括卷积层、批量归一化层、激活层、最大池化层、Dropout 层和全连接层，结构图如图 7 所示。将 GRU 模块输出的时间局部特征与 BiLSTM 模块输出的时间全局特征融合后输入 CNN 模块提取空间特征，捕捉流量数据中的局部模式和空间依赖关系，最终通过全连接层和分类函数实现分类。

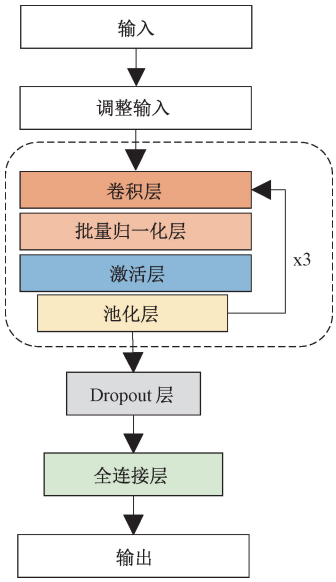

图 7　CNN 模块结构图

Fig. 7　Structure diagram of the CNN module

3　实验结果及分析

在实验阶段，搭建了一个 Windows 10 操作系统的实验平台，配备 Intel Core i5-1035G1 CPU 以及 NVIDIA GeForce MX350 独立显卡，16 GB 的系统内存。开发环境为 Python 3.7.6，深度学习框架采用 PyTorch 1.13.1。

3.1　实验数据集与处理

本文采用入侵检测常用的 UNSW-NB15、NSL-KDD 和 Kyoto2006 网络流量数据集进行评估测试，以验证所提方法在不同网络环境和攻击类型下的有效性。

UNSW_NB15 数据是由澳大利亚新南威尔士大学的网络安全实验室提供的。每条数据共有 45 个特征，UNSW_NB15 数据集分布情况如表 1 所示。

NSL-KDD 数据集是对 KDD Cup 1999 的改进，解决原数据集的多个缺陷，成为入侵检测研究的重要基准。该数据集中的每条数据记录包含 43 个特征维度，分布情况如表 2 所示。

Kyoto 2006 数据集是一个公开可用的真实网络流量蜜罐数据集。本实验选取的是 Kyoto 2006 数据集中 2006 年采集的数据，每个会话有 24 个属性。Kyoto2006 数据集分布情况如表 3 所示。

表 1　UNSW_NB15 数据集分布情况

Table 1　Distribution of the UNSW_NB15 dataset

数据集	类名	训练集	测试集
UNSW_NB15	Normal	56 000	37 000
	Generic	40 000	18 871
	Exploits	33 393	11 132
	Fuzzers	18 184	6 062
	DoS	12 264	4 089
	Reconnaissance	10 491	3 496
	Analysis	2 000	677
	Backdoor	1 746	583
	Shellcode	1 133	378
	Worms	130	44
总计		175 341	82 332

表 2　NSL-KDD 数据集分布情况

Table 2　Distribution of the NSL-KDD dataset

数据集	类名	训练集	测试集
NSL-KDD	Normal	67 343	9 711
	DoS	45 927	7 949
	Probe	11 656	2 421
	R2L	995	2 709
	U2R	52	54
总计		12 593	22 544

表 3　Kyoto2006 数据集分布情况

Table 3　Distribution of the Kyoto2006 dataset

数据集	类名	训练集（80%）	测试集（20%）
Kyoto2006（2006）	Normal	200 062	49 894
	known Attack	3 033 712	758 407
	Unknown Attack	76 545	19 279
总计		3 310 319	827 580

首先对网络流量数据集进行数据预处理。数据预处理包括特征删除、数据清洗、非数值型特征标签编码、数值型特征标准化步骤。对 UNSW_NB15、NSL-KDD 和 Kyoto 2006 三个网络流量数据集进行预处理：删除无关特征（如 Id、IP 地址等），检测并均值填充缺失值，对非数值型特征（如 Protocol 协议类型、Service 服务类型等）进行标签编码；对所有数值型特征进行 min-max 归一化处理。如式（18）所示：

$$\boldsymbol{X}_{\text{norm}}=\frac{\boldsymbol{X}-M_{\min}}{M_{\max}-M_{\min}} \tag{18}$$

式中：$\boldsymbol{X}$ 为原始数据点、$\boldsymbol{M}_{\min}$ 和 $\boldsymbol{M}_{\max}$ 为数据集中同一维度下的最小值和最大值、$\boldsymbol{X}_{\text{norm}}$ 为归一化后的数据点。

3.2　评估标准

为了验证本文模型的性能，通过混淆矩阵计算出准确

率(Accuracy)、精确度(Precision)、召回率(Recall)和 F1 值作为模型评估指标。

$$Accuracy = \frac{TP + FN}{TP + TN + FP + FN} \tag{19}$$

$$Precision = \frac{TP}{TP + FP} \tag{20}$$

$$Recall = \frac{TP}{TP + FN} \tag{21}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{22}$$

3.3 实验结果分析

在本次实验中,对模型的超参数进行配置:批次的样本数设置为 64,学习率设为 0.001,隐藏层设置 64。卷积核大小为 3,卷积层 1、2 和 3 的输出通道分别设置为 32、64 和 128,最大池化层窗口大小设置为 2,Dropout 率为 0.5。采用 Adam 优化器,并以交叉熵损失函数作为损失的度量标准训练模型,迭代训练次数为 20。在 Kyoto2016 数据集损失值如图 8 所示。

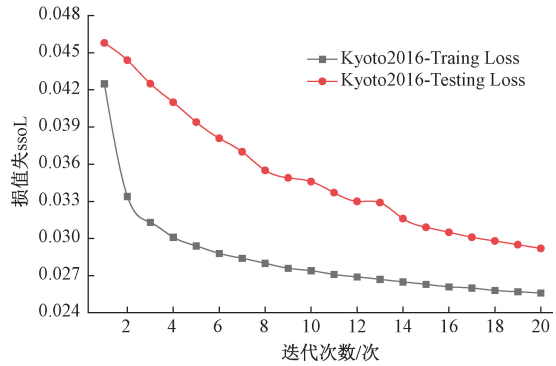

图 8 Kyoto2016 数据集损失函数图

Fig. 8 Loss function curve on Kyoto2016 dataset

为解决数据不平衡问题,使用 CGAN-SMOTE 方法增加少数类的样本数量。对数据集中少数类数据先进行 CGAN 采样,在此基础上,进行 SMOTE 采样,使得数据集平衡。数据集的原始数据和平衡后的数据分布如表 4 所示。

表 4 少数类样本平衡前后的数据分布

Table 4 Data distribution before and after minority class sample balancing

数据集	类名	平衡前	平衡后
UNSW_NB15	Analysis	2 000	11 095
	Backdoor	1 746	10 152
	Shellcode	1 133	10 995
	Worms	130	10 052
NSL-KDD	R2L	995	10 995
	U2R	52	11 052
Kyoto2006	Normal	200 062	3 200 062
	Unknown Attack	76 545	3 076 545

为了探究不同模块对模型性能的贡献,本文进行了消融实验,分别测试以下模块组合的性能:GRU 子模块、BiLSTM 子模块、CNN 子模块、GRU + BiLSTM 模块、GRU+CNN 模块、BiLSTM+CNN 模块以及本文模型。实验结果如表 5 所示。本次消融实验是在 3 个公开数据集上对不同模块组合的表现进行对比,实验结果表明,本文提出的模型能够有效提升网络流量异常检测的整体性能,证明了模型的合理性和有效性。

表 5 消融实验对比结果(平均值)

Table 5 Comparison results of ablation experiments (Mean) %

模型	UNSW_NB15				NSL-KDD 数据集				Kyoto2006 数据集			
	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值
GRU	86.881	88.084	87.257	88.442	88.269	87.002	96.584	91.741	96.081	99.181	96.005	97.902
BiLSTM	85.971	89.241	86.461	87.937	89.610	87.174	96.893	92.476	93.765	99.098	93.556	96.574
CNN	86.892	89.145	87.442	88.184	91.014	89.910	97.669	93.311	96.525	99.201	96.485	98.124
GRU+BiLSTM	89.735	91.252	95.598	89.734	89.904	87.326	96.623	92.562	94.901	99.203	94.802	97.224
GRU+CNN	85.271	88.953	93.064	96.859	90.278	89.219	97.871	93.014	96.091	99.201	96.043	97.884
BiLSTM+CNN	87.690	90.891	94.325	90.320	90.672	90.342	97.742	93.274	96.487	99.215	96.443	98.019
本文模型	90.241	94.128	97.114	90.702	92.090	91.944	97.876	93.358	98.622	99.254	98.498	99.178

在本文模型的 CNN 模块中,主要采用了最大池化层作为池化操作,并与平均池化层和软池化层进行对比实验。由表 6 可知,最大池化层在模型性能上优于平均池化层和软池化层,能够有效提升模型的整体性能。

为验证本文模型的有效性,实验选取 MHA-BiLSTM、AlertNet、GSOOA-IDDRSN、SEMI-GRU 和 ADSAE-CNN 五种对比模型,在 UNSW_NB15、NSL-KDD 和 Kyoto2006 数据集上进行性能比较。表 7 表示每组实验重复 5 次的平均值与标准差。实验结果表明,本文模型在 UNSW_NB15 数据集上取得 90.242% 的准确率、94.128% 的精确率、97.114% 的召回率和 90.702% 的 F1 值;在 NSL-KDD 数据集的各项指标分别提升 0.494%~13.075%、0.023%~21.704%、0.355%~17.601% 和 0.484%~14.913%;在 Kyoto2006 数据集上,相较于表现最优的 SEMI-GRU 模型,准确率和精确率分别提高 0.316% 和 0.59%,相比 ADSAE-CNN 模型的 F1 值提升 0.574%。

表 6　不同池化层性能对比(平均值±标准差)

Table 6　Performance comparison of pooling layers (Mean ± SD)　%

池化层	UNSW-NB15 数据集				NSL-KDD 数据集				Kyoto2006 数据集			
	准确率	精确率	召回率	F1	准确率	精确率	召回率	F1	准确率	精确率	召回率	F1
平均池化	86.364	90.145	87.158	84.210	91.521	91.137	94.621	92.488	96.924	99.068	96.893	98.346
软池化	88.281	92.031	95.562	89.104	90.142	89.413	96.567	92.894	97.563	99.153	97.527	98.996
最大池化	90.241	94.128	97.114	90.702	92.090	91.944	97.876	93.358	98.622	99.254	98.498	99.178

表 7　模型二分类性能结果(平均值±标准差)

Table 7　Performance results of models for binary classification (Mean ± SD)　%

数据集	模型	准确率	精确率	召回率	F1 值
UNSW_NB15	MHA-BiLSTM[2]	65.163±0.121	65.287±0.387	89.946±0.205	71.120±0.209
	AlertNet[16]	78.025±0.461	93.942±0.142	73.472±0.325	82.880±0.241
	GSOOA-1DDRSN[17]	80.325±0.352	80.894±0.214	83.135±0.274	77.878±0.352
	SEMI-GRU[18]	89.293±0.601	92.174±0.113	89.823±0.643	88.146±0.326
	ADSAE-CNN[19]	89.0132±0.267	88.748±0.301	88.079±0.450	88.639±0.357
	本文模型	90.242±0.418	94.128±0.246	97.114±0.311	90.702±0.331
NSL-KDD	MHA-BiLSTM[2]	79.015±0.363	91.721±0.218	92.452±0.352	78.275±0.341
	AlertNet[16]	81.009±0.362	70.240±0.341	96.732±0.245	82.965±0.365
	GSOOA-1DDRSN[17]	80.423±0.412	84.293±0.382	80.275±0.326	78.472±0.403
	SEMI-GRU[18]	89.992±0.401	87.739±0.495	97.524±0.057	92.815±0.264
	ADSAE-CNN[19]	91.596±0.251	91.921±0.243	97.290±0.143	92.874±0.326
	本文模型	92.090±0.347	91.944±0.229	97.876±0.221	93.358±0.415
Kyoto2006	MHA-BiLSTM[2]	95.898±0.142	96.213±0.328	97.978±0.267	97.936±0.113
	AlertNet[16]	95.344±0.224	95.364±0.251	98.402±0.341	97.621±0.246
	GSOOA-1DDRSN[17]	98.261±0.266	98.427±0.297	97.710±0.311	95.579±0.253
	SEMI-GRU[18]	98.306±0.243	98.664±0.364	98.801±0.235	96.697±0.126
	ADSAE-CNN[19]	97.321±0.301	98.621±0.381	98.072±0.286	98.604±0.273
	本文模型	98.622±0.238	99.254±0.486	98.498±0.385	99.178±0.207

3.4　性能稳定性能力分析

为全面评估模型性能的稳定性和实验可重复性，本节在 UNSW_NB15、NSL-KDD 和 Kyoto2016 三个标准数据集上进行 5 次独立重复实验。图 9 详细展示 5 次独立实验在 3 个数据集上的评估结果。图 10 展示 5 次实验的指标平均值和标准差。实验结果表明，本文提出的模型在不同数据集上均展现出稳定的性能表现和良好的可重复性。

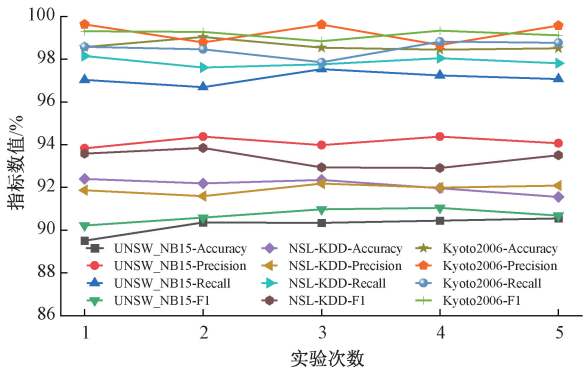

图 9　多数据集实验指标对比图

Fig. 9　Metric comparison across multiple datasets

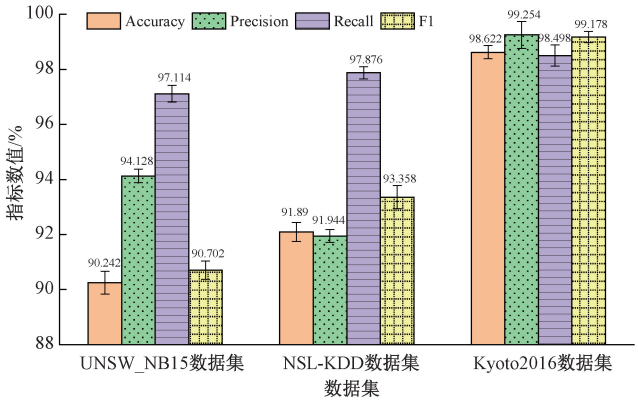

图 10　评估指标均值与标准差分布

Fig. 10　Distribution of evaluation metrics(Mean ± SD)

3.5 实际部署可行性分析

为评估模型在实际应用中的可行性,本节从计算复杂度和运行时性能两个维度进行分析。表8展示模型各组成模块的参数量和计算量(FLOPs),并对比了在不同数据集上的训练收敛所需时间、批量推理延迟(64批次)。

表8 各模块性能对比

Table 8 Performance comparison of modules

数据集	模块	参数量	FLOPs/M	收敛时间/h	推理延迟/ms
UNSW_NB15 Input Dim=42	GRU	30 464	3.77	1.06	13.32
	BiLSTM	70 144	8.52		
	CNN	103 233	24.00		
NSL-KDD Input Dim=41	GRU	29 504	3.64	0.76	17.31
	BiLSTM	67 584	8.30		
	CNN	103 937	23.80		
Kyoto2016 Input Dim=21	GRU	23 360	2.59	3.43	10.39
	BiLSTM	51 200	5.51		
	CNN	98 561	23.10		

4 结 论

本研究针对网络流量异常检测中存在数据类别不平衡、特征提取能力不足导致检测准确率受限问题,提出一种基于多层次特征融合的不平衡网络流量异常检测方法。通过引入CGAN-SMOTE解决数据分布不均衡问题;利用GRU模块提取序列数据的时间局部特征;采用BiLSTM模块提取时间全局特征;最后通过改进的CNN架构实现时空特征的深度融合。在UNSW_NB15、NSL-KDD和Kyoto2016三个数据集上的实验验证表明,该模型在准确率、精确率、召回率和F1值4项关键指标上均显著优于现有方法。后续研究将重点优化模型计算效率,开发适用于边缘设备的轻量化版本,并在更复杂的实际网络环境中验证其泛化能力,以促进该技术在网络安全防护体系中的实际部署和应用。

参考文献

[1] ALAM N, AHMED M. Zero-day network intrusion detection using machine learning approach [J]. International Journal on Recent and Innovation Trends in Computing and Communication, 2023, 11(8s): 194-201.

[2] 叶文冰,詹仕华. 基于MHA-BiLSTM的网络流量异常检测方法[J]. 现代信息科技,2024,8(2):65-69.
YE W B, ZHAN SH H. Anomaly detection method of network traffic based on MHA-BiLSTM [J]. Modern Information Technology, 2024, 8(2): 65-69.

[3] 麻文刚,张亚东,郭进. 基于LSTM与改进残差网络优化的异常流量检测方法[J]. 通信学报,2021,42(5):23-40.
MA W G, ZHANG Y D, GUO J. Abnormal traffic detection method based on LSTM and improved residual neural network optimization[J]. Journal on Communications, 2021, 42(5): 23-40.

[4] 许东园,曹争光,黄春麟. 基于改进CBAM和BiGRU的入侵检测模型[J]. 计算机技术与发展,2024,34(9):88-93.
XU D Y, CAO ZH G, HUANG CH L. Intrusion detection model based on improved CBAM and BiGRU [J]. Computer Technology and Development, 2024, 34(9): 88-93.

[5] 王嘉铭,杨凯. 基于CNN-BiGRU的网络入侵检测研究[J]. 信息记录材料,2024,25(7):180-183.
WANG J M, YANG K. Research on network intrusion detection based on CNN-BiGRU [J]. Information Recording Materials, 2024, 25(7): 180-183.

[6] 杨晓文,张健,况立群,等. 融合CNN-BiGRU和注意力机制的网络入侵检测模型[J]. 信息安全研究,2024,10(3):202-208.
YANG X W, ZHANG J, KUANG L Q, et al. A network intrusion detection model integrating CNN-BiGRU and attention mechanism [J]. Journal of Information Security Research, 2024, 10(3): 202-208.

[7] WANG S, BALAREZO J F, KANDEEPAN S, et al. Machine learning in network anomaly detection: A survey[J]. IEEE Access, 2021, 9: 152379-152396.

[8] HAFEEZ I, ANTIKAINEN M, DING A Y, et al. IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge[J]. IEEE Trans on Network and ServiceManagement, 2020, 17(1): 45-59.

[9] 陈万志,张国满,王天元. 基于特征耦合泛化的流量异常检测方法[J]. 电子测量与仪器学报,2024,38(2):120-130.
CHEN W ZH, ZHANG G M, WANG T Y. Traffic anomaly detection method based on feature coupling generalization[J]. Journal of Electronic Measurement and Instrumentation, 2024, 38(2): 120-130.

[10] 戚永军,刘晓硕,贾正正,等. 基于SVM的网络流量异常检测[J]. 北华航天工业学院学报,2024,34(2):1-4.
QI Y G, LIU X SH, JIA ZH ZH, et al. Network traffic anomaly detection based on SVM[J]. Journal of North China Institute of Aerospace Engineering,

2024，34(2)：1-4.

[11] 张凡，高仲合，牛琨. 基于 KNN 的网络流量异常检测研究[J]. 通信技术，2021，54(5)：1235-1239.
ZHANG F，GAO ZH H，NIU K. Research on network traffic anomaly detection based on KNN[J]. Communications Technology，2021，54(5)：1235-1239.

[12] 倪志伟，行鸿彦，侯天浩，等. 基于生成对抗网络和混合时空神经网络的入侵检测[J]. 电子测量技术，2024，47(2)：17-24.
NI ZH W，XING H Y，HOU T H，et al. Intrusion detection based on generative adversarial networks and hybrid spatio-temporal neural networks[J]. Electronic Measurement Technology，2024，47(2)：17-24.

[13] 詹鸿辉，程仲汉. 基于卷积神经网络的异常流量鉴别方法[J]. 成都信息工程大学学报，2023，38(6)：668-672.
ZHAN H H，CHENG ZH H. Identification method of abnormal traffic based on convolution neural network[J]. Journal of Chengdu University Of Information Technology，2023，38(6)：668-672.

[14] 陈虹，齐兵，金海波，等. 融合 1D-CNN 与 BiGRU 的类不平衡流量异常检测[J]. 计算机应用，2024，44(8)：2493-2499.
CHEN H，QI B，JIN H B，et al. Class-imbalanced traffic abnormal detection based on 1D-CNN and BiGRU[J]. Journal of Computer Applications，2024，44(8)：2493-2499.

[15] 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，2023，45(10)：3719-3728.
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，2023，45(10)：3719-3728.

[16] AL-TURAIKII，ALTWAIJRY N. A convolutional neural net-work for improved anomaly-based network intrusion detection[J]. Big Data，2021，9(3)：233-252.

[17] ZUO F，ZHANG D，LI L，et al. GSOOA-1DDRSN：Network traffic anomaly detection based on deep residual shrinkage networks[J]. Heliyon，2024，10(11)：e32087.

[18] 李海涛，王瑞敏，董卫宇，等. 一种基于 GRU 的半监督网络流量异常检测方法[J]. 计算机科学，2023，50(3)：380-390.
LI H T，WANG R M，DONG W Y，et al. Semi-supervised network traffic anomaly detection method based on GRU[J]. Computer Science，2023，50(3)：380-390.

[19] GENG Z，LI X，MA B，et al. Improved convolution neural network integrating attention based deep sparse auto encoder for network intrusion detection[J]. Applied Intelligence，2025，55(2)：1-17.

作者简介

申明娜(通信作者)，硕士研究生，主要研究方向为网络流量异常检测。

E-mail：MingNaS@163.com

王佩雪，硕士，副教授，主要研究方向为信息安全。

E-mail：peipeiw@zut.edu.cn

孟永伟，博士，讲师，主要研究方向为网络与信息安全。

E-mail：ywmeng@zut.edu.cn

户佳乐，硕士研究生，主要研究方向为态势感知。

E-mail：jiale_hu2024@163.com