DOI:10.19651/j.cnki.emt.2518267

基于时空特征融合的网络异常流量检测方法

徐仪帆
(四川大学网络空间安全学院 成都 610065)

摘 要:针对传统网络异常流量检测模型存在数据时空特性利用不充分和泛化能力较差等问题,提出一种基于多头注意力机制和时空特征融合的网络异常流量检测方法。通过卷积神经网络(CNN)提取流量数据的空间局部特征,并引入多头注意力机制对特征进行多角度自适应重加权,从而提升模型对异常流量的敏感度。将重加权后特征输入双向长短期记忆网络(BiLSTM),挖掘流量数据中的长距离时序依赖关系。最后,利用 Softmax 对流量数据进行分类与识别。在公开数据集 NSL-KDD 和 CIC-IDS-2017 上开展实验,检测准确率分别为 85.40%和 99.41%,验证了该方法在异常流量检测任务中的有效性。

关键词:异常流量检测;注意力机制;卷积神经网络;长短期记忆网络
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

Network anomaly traffic detection method based on spatial-temporal feature fusion

Xu Yifan
(School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China)

Abstract: Aiming at the problems of insufficient utilization of data spatial-temporal characteristics and poor generalization ability of e traditional network traffic anomaly detection methods, a traffic anomaly detection method based on multi-head attention mechanism and spatial-temporal feature fusion is proposed. The convolutional neural network(CNN) is utilized for the extraction of the spatial local features presented within the traffic data. The multi-head attention mechanism is introduced to achieve multi-angle adaptive reweighting of key features through parallel computation of multiple attention heads, thus improving the sensitivity of the model to abnormal traffic. The re-weighted features are then input into the bidirectional long short-term memory network(BiLSTM) to mine the long-distance temporal dependencies in the traffic data. Finally, Softmax is used to classify and identify the traffic data. Experiments are carried out on the publicly available dataset NSL-KDD and CIC-IDS-2017 with a detection accuracy of 85.40% and 99.41%, respectively, which verifies the effectiveness of the method in the task of network traffic anomaly detection.

Keywords: traffic anomaly detection; attention mechanism; convolutional neural network; long short-term memory network

0 引 言

随着通信服务的快速发展和基础设施的日益完善,全球通信数据呈现几何倍数增长态势[1]。然而,随着数据量的激增和新兴应用场景的拓展,网络安全问题愈发严峻[2]。根据微软公司的统计数据,全球日均网络攻击行为已超 6 亿次。网络攻击不仅使用户面临数据泄露、身份盗用和系统控制权丧失等风险,还可能造成关键信息基础设施的瘫痪。因此,研究高效、准确的异常流量检测方法具有重要的理论和实践意义。

传统机器学习方法通常依赖于特征工程的构建,并通过分类算法来识别异常流量[3]。例如,Lu 等[4]利用主成分分析(principal component analysis, PCA)和秃鹰搜索算法完成特征处理,并使用随机森林分类器识别异常流量,取得了较好的检测性能。付子燨等[5]提出了一种结合支持向量机(support vector machine, SVM)和 K 近邻算法(k-nearest neighbor, KNN)的检测模型,在 NSL-KDD 数据集上开展实验,证实了模型对恶意流量的检测能力。然而,传统机器学习方法在面对大规模、海量数据时通常面临特征提取能力不足和模型泛化能力差等问题[6]。当遇到新型攻

收稿日期:2025-03-06

击时，这些方法的模型泛化能力较差，导致检测效果不理想。同时，新型网络攻击层出不穷，传统机器学习方法的局限性愈加显著，因此迫切需要引入先进技术来提升模型检测性能。

深度学习的快速发展为解决上述问题提供了新的思路。深度学习模型利用多层神经网络结构从海量、复杂数据中自动提取特征，有效克服了传统方法的局限性[7]。在深度学习模型中，卷积神经网络（convolutional neural network，CNN）通过构建多层卷积结构，能够有效提取流量数据的空间维度特征。例如，Geng 等[8]提出一种基于 CNN 和深度稀疏自编码器（attention based deep sparse auto encoder，ADSAE）的网络异常流量检测模型 ADSAE-CNN，通过 ADSAE 在数据预处理阶段扩展少数类样本，并利用 CNN 进行特征提取与分类，在 UNSW-NB15 数据集上检测准确率达 89.1%。同时，由于流量数据通常具有时间依赖性，循环神经网络（recurrent neural networks，RNN）在捕捉时序特征方面具有显著优势。因此，RNN 在流量数据分析中得到了广泛应用。例如 Narmadha 等[9]提出了一种基于 RNN 的变体网络 LSTM 的入侵检测模型，采用基于粒子群优化后的 LSTM 来建模和实现分类，在公开数据集 KDD99 dataset 上开展实验，证实了 LSTM 对异常流量的检测能力。然而，RNN 类方法难以捕捉数据空间特征。为解决这一问题，研究人员将 CNN 与 RNN 相结合，充分发挥两者在特征提取和建模方面的优势。例如，Halbouni 等[10]提出了一种基于混合深度学习的入侵检测方法 CNN-LSTM，利用 CNN-BiLSTM 提取时空特征，实验结果验证了混合网络的检测能力优于单一网络架构。上述方法充分证实了 CNN 与 RNN 类方法在提升检测模型性能方面具有显著的贡献。CNN 在捕捉数据中的空间特征方面具有显著优势，能有效识别流量中的局部模式和潜在异常。LSTM 凭借其强大的时序建模能力，可以同时依赖当前和上一时刻的输入，适用于处理具有长时间依赖性的流量数据。然而，现有异常流量检测模型通常采用固定权重，缺乏自适应地突出重要特征的能力，从而影响模型的准确性。同时，当前方法普遍依赖单一网络架构进行拟合学习，未能有效融合空间和时间信息，从而限制了模型对复杂流量模式的捕捉能力。

近年来，Transformer 凭借其多头注意力机制，通过并行处理输入数据的多个子空间，已在时间序列分析等领域广泛应用。针对网络流量数据，Transformer 可有效捕捉数据中长时间周期依赖和空间维度关联[11]，为异常检测工作提供新思路。然而，现有单一 Transformer 的方法大多集中在时序建模上，忽视了流量数据中潜在的局部空间特征，这导致模型无法充分利用空间维度的细粒度信息。

针对上述问题，本文设计一种结合多头注意力机制、CNN 和 LSTM 网络的网络模型。CNN 提取流量数据的空间局部特征，而多头注意力机制通过自适应的方式对不同通道进行重加权，从多个角度增强模型对异常流量的敏感度。经过重加权后的特征输入到 BiLSTM 中，挖掘流量数据中的长距离时序依赖关系。基于数据集 NSL-KDD 开展实验，验证所提模型对异常流量的识别能力。

1　基于多头注意力机制和时空特征融合的网络异常流量检测模型设计

1.1　CNN 提取数据空间局部特征

CNN 作为一种特殊的前馈神经网络，广泛应用于图像、视频等数据的特征提取。根据输入数据的维度，CNN 可分为 1 维卷积神经网络（1 dimension convolutional neural network，1D-CNN）、2D-CNN 和 3D-CNN。网络流量数据通常由一系列时间戳对应的网络连接和通信事件组成，属于典型的 1 维数据[12]。每个数据点对应一个时间节点的网络流量特征（例如源字节、目的字节等），这些数据点按时间顺序排列，形成时间序列。因此，本文采用 1D-CNN 来提取数据空间局部特征。

1D-CNN 包含一系列卷积层和池化层，通过交替连接构成深层网络，提取数据空间局部关联模式。卷积层通过一组可学习的卷积核自动提取输入数据的局部特征，且卷积核的权值共享机制显著减少了模型参数量，从而降低了计算开销[13]。池化层通过对局部区域进行下采样，不仅进一步减轻了模型的计算负担，而且有效抑制了过拟合的风险[14]。

1.2　MHSE 捕捉多尺度特征

CNN 在捕捉空间局部关联方面表现优异，但在面对具有不同尺度特征的复杂数据时，传统卷积操作难以有效捕捉全局特征信息[15]。为提升 CNN 对多尺度特征信息的感知能力，引入注意力机制，设计多头挤压激励机制（multi head squeeze excitation mechanism，MHSE）。

如图 1 所示，通过多个并行的挤压激励（squeeze excitation，SE）子模块来捕捉不同层次和尺度的特征信息，从而有效增强模型对多尺度信息的感知和学习能力。在每个子模块中，通过多个空洞卷积头并行处理输入数据。每个卷积头使用不同的膨胀因子来扩展感受野，从而在不同尺度上提取特征[16]。具体来说，当膨胀因子 $d=n$ 时，每 n 个输入被采样一次。

$$F(s)=\sum_{i=0}^{k-1} f(i)\cdot X_{s-d\cdot i} \tag{1}$$

其中，s 表示输入序列 X 中的元素，k 表示卷积核的大小，d 指膨胀因子。

经空洞卷积处理后，输入 SE 模块。SE 包含挤压和激励操作[17]。挤压（Squeeze）操作通过全局平均池化层生成输入特征的全局统计信息

$$Z_c=F_{sq}(x_c)=\frac{1}{H}\sum_{i=1}^{H} x_c(i) \tag{2}$$

其中，x_c 表示第 c 个通道的时序特征，H 表示特征维

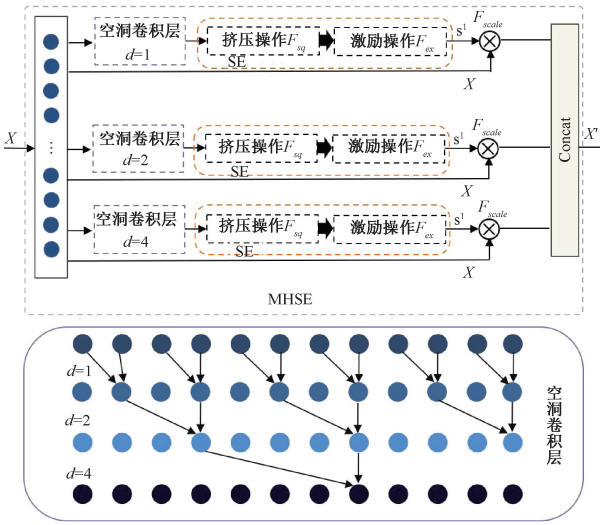

图 1　MHSE 框架结构

Fig. 1　MHSE framework structure

度的大小。

激励(Excitation)操作通过两个全连接层、激活函数 ReLU 和激活函数 Sigmoid,自适应地学习每个通道的加权系数。根据不同通道的重要性调整权重,从而使网络关注于更为关键的特征。

$$s = F_{ex}(Z_c, W) = \mathrm{Sigmoid}(\boldsymbol{W}_2 \mathrm{ReLU}(\boldsymbol{W}_1 z)) \tag{3}$$

其中,$\boldsymbol{W}_1$ 和 $\boldsymbol{W}_2$ 分别表示第 1、2 个全连接层的权重矩阵。

1.3　BiLSTM 提取长距离序列特征

网络流量数据具有明显的时序特性。网络攻击事件会导致连接持续时间、源 IP、目的 IP 和连接请求频率等特征的显著变化。因此,深入探究流量数据在时间尺度上的变化趋势,对于提升模型的检测效果至关重要。为有效捕捉流量数据的时序变化模式,引入双向长短期记忆网络(BiLSTM)。BiLSTM 是 LSTM 的变体,它保留了 LSTM 在长距离序列学习中的优势。

LSTM 通过输入门 i_t、遗忘门 f_t 和输出门 o_t 有选择性地保留、遗忘和传递时间序列中的信息[18]。LSTM 具体实现过程如下

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{4}$$

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \tag{5}$$

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{6}$$

$$\tilde{C}_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \tag{7}$$

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t \tag{8}$$

$$h_t = o_t \cdot \tanh(C_t) \tag{9}$$

其中,σ 为 Sigmoid 激活函数,x_t 为 t 时刻的输入序列,W 和 b 分别为权重和偏置项,$\tilde{C}_t$ 指临时单元状态,C_t 为当前单元状态,h_t 为时刻 t 的隐层状态。

然而,保障网络安全是一个持续的攻防博弈过程。网络攻击者通过研究历史流量模式来不断升级攻击手段。传统 LSTM 仅依赖历史数据建模,难以有效捕捉未来时间点语义信息。为了解决此问题,BiLSTM 引入双向结构,通过正向 LSTM 与反向 LSTM 分别捕捉正向、反向时间序列信息[19]。与 LSTM 相比,BiLSTM 的双向处理机制能同时利用过去和未来的语义信息,进而提高模型对复杂网络攻击模式的敏感度和检测精度。具体实现过程如下

$$h_t^{\mathrm{forward}} = \mathrm{LSTM}^{\mathrm{forward}}(h_{t-1}, x_t, C_{t-1}) \tag{10}$$

$$h_t^{\mathrm{backward}} = \mathrm{LSTM}^{\mathrm{backward}}(h_{t-1}, x_t, C_{t-1}) \tag{11}$$

$$h_t = [h_t^{\mathrm{forward}}, h_t^{\mathrm{backward}}] \tag{12}$$

其中,h_{t-1} 为 $t-1$ 时刻隐层状态。

最终,BiLSTM 能够更好地捕捉时间序列中的长期依赖关系,显著提高网络流量异常检测的准确性。通过结合 CNN、MHSE 和 BiLSTM 模块,本文设计的模型能够充分利用网络流量数据的空间局部特征和时间依赖关系,进一步提升异常流量检测的效果。

2　基于 MHSECNN-BiLSTM 的检测流程

图 2 展示了本文所提模型的检测流程。在模型训练之前,对原始数据集 NSL-KDD 进行数据预处理,主要包括字符特征数值化和数值特征归一化。对预处理后的数据,采用 MHSECNN-BiLSTM 网络进行拟合学习,其通过结合 CNN、MHSE 和 BiLSTM 的优点,充分发挥各自优势,有效解决了传统模型在突出重要特征和利用时空特性方面的不足。在 MHSECNN-BiLSTM 中,CNN 捕捉流量数据在空间维度上的特征关联,MHSE 通过多个并行的注意力头自适应地加权关键特征,而 BiLSTM 则致力于建模流量数据在时间维度上的特征依赖关系。最后,利用 Softmax 对流量数据进行分类与识别。

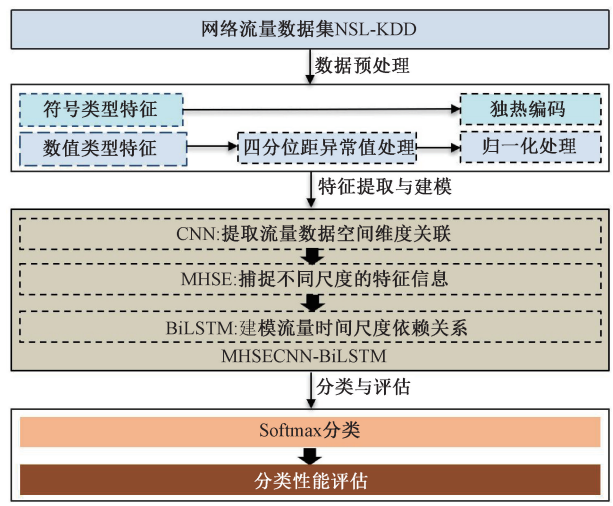

图 2　基于 MHSECNN-BiLSTM 的网络异常流量检测框架

Fig. 2　Network anomaly traffic detection framework based on MHSECNN-BiLSTM

2.1　数据预处理

数据集预处理步骤包括字符特征数值化和数值特征归一化。在数据集中，每条数据包含 38 个数值型特征和 3 个字符型特征。

对字符型特征进行数值化处理。由于训练模型无法直接处理字符型特征，通过 One-hot 编码将数据集中的字符特征转换为数值表示。经过 One-hot 编码后，字符特征 Protocol_type、service 和 type 分别被转化为 3 维、70 维和 11 维的数值型特征。

对于数值特征执行异常值处理和归一化处理。在异常值处理采用四分位距（inter-quartile range，IQR）方法，减少极端值对模型性能的影响。对于每个特征，计算其下四分位数（Q_1）和上四分位数（Q_3）和 IQR，并确定异常值边界（OB）。当特征值大于 OB，则其值替换为 OB。

$$\mathrm{IQR} = Q_3 - Q_1 \tag{13}$$

$$\mathrm{OB} = Q_3 - k \cdot \mathrm{IQR} \tag{14}$$

其中，Q_1 是所有样本按数值从小到大排序后第 25% 位置的取值；而 Q_3 是所有样本按数值从小到大排序后第 75% 位置的取值；k 用于调节异常值范围的系数。

此外，为消除不同特征量纲差异对模型性能的影响，利用 Min-Max 归一化将所有特征值映射到[0，1]范围。

2.2　检测流程

图 3 为 MHSECNN-BiLSTM 的检测流程。对于输入的网络流量数据，利用 CNN 进行拟合学习。CNN 包含两个卷积模块（Conv），其中 Conv1 和 Conv2 的滑动窗口尺寸为 3。在 Conv1 中卷积核数量为 64，而 Conv2 卷积和数量增加至 128。卷积层后依次引入批归一化层和 ReLU 激活函数层，以减少训练过程中的不稳定性和梯度消失问题。

接着，将经 CNN 处理后的特征输入 MHSE。MHSE 利用多个并行 SE 子模块，从不同角度增强重要特征权重。在每个 SE 子模块中，通过设置不同的卷积膨胀率 d，卷积层能够捕捉多层次和多尺度的特征信息，从而有效提高模型对不同尺度信息的感知和学习能力。每个 SE 模块包括全局平均池化层（global average pooling，GAP）、全连接层（fully connected layer，FC）、ReLU 层和 Sigmoid 层。GAP 层对输入特征进行通道级别压缩，计算特征均值。FC 对 GAP 结果进行自适应加权处理。通过 Sigmoid 输出每个通道的权重。多个 SE 模块并行工作，通过拼接（Concat）操作将这些特征融合，生成更丰富的多尺度信息。

经过 MHSE 模块处理的特征被传入 BiLSTM 网络。BiLSTM 通过双向处理机制同时捕获过去和未来的时序信息，进一步挖掘网络流量中的复杂时序依赖关系。最后，使用 Softmax 进行识别与分类。

3　实验结果与分析

3.1　实验数据集

为评估本文提出的模型对恶意流量的检测能力，基于两个主流公开数据集 NSL-KDD 和 CIC-IDS-2017 进行实验。

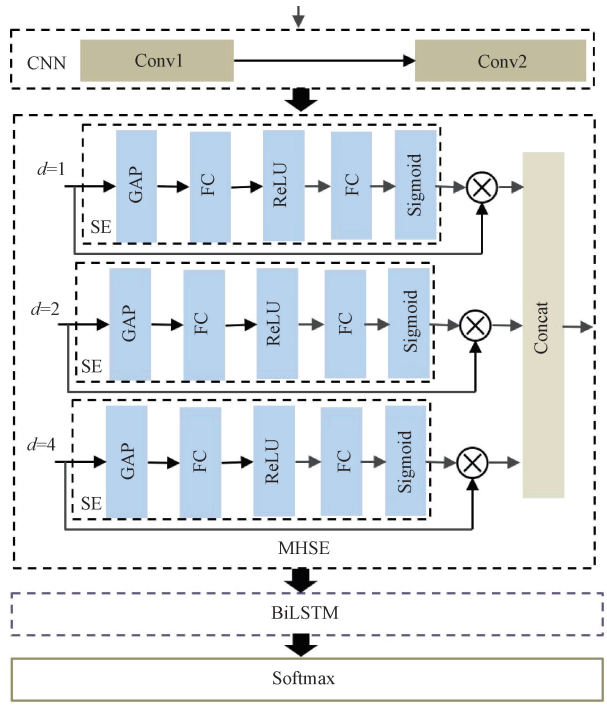

图 3　MHSECNN-BiLSTM 网络结构

Fig. 3　MHSECNN-BiLSTM network structure

NSL-KDD 数据集包含 4 个数据子集：KDDTrain＋、KDDTrain＋_20Precent、KDDTest＋和 KDDTest＋21[20]。在实验中，分别选择 KDDTrain＋和 KDDTest＋作为训练集和测试集。训练集 KDDTrain＋包含 125 973 个样本，测试集 KDDTest＋包含 22 544 条数据[21]。训练集 KDDTrain＋共包括 22 种不同类型的网络攻击样本，而测试集 KDDTest＋包括 39 种攻击类型。测试集中存在 17 种未在训练集中出现的新型攻击，这使得实验结果更贴近真实场景。

CIC-IDS-2017 数据集包含了 2 830 743 条流量数据[3]，考虑直接对全部数据进行分析耗时较长，利用周三数据子集开展实验。该子集包含 692 304 条样本，涵盖 5 种攻击类型。由于 Heartbleed 类型攻击样本仅出现 11 例，所占比例极小，因此将其剔除。按照样本标签以 4∶1的比例划分训练集和测试集。考虑本文目的是精准、高效地检测出恶意流量而非具体类别，因此将所有恶意流量标记为 1，正常流量标记为 0。

3.2　评价指标

为评估模型的性能，基于常见二分类指标准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 F1-score（F1-score）开展分析。TP 指异常网络流量被模型正确标记的数量，TN 表示正常流量被模型正确标记的数量，FP 指正常流量被模型误检测为异常通信数据的数量，FN 表示异常流量被模型误检测为正常通信数据的数量。

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

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

$$Recall = \frac{TP}{TP + TN} \tag{17}$$

$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{18}$$

3.3 实验结果与分析

实验平台的配置为 NVIDIA GeForce RTX 3060 Ti、Python 3.9 和 Tensorflow 2.10.0。MHSECNN-BiLSTM 参数信息如表 1 所示。

表 1　参数设置

Table 1　Parameter settings

参数设置	NSL-KDD	CIC-IDS-2017
Epoch	50	30
Batchsize	200	200
Dropout	0.1	0.5
Learning rate	0.001	0.001
Optimizer	Adam	Adam

1)消融实验

为分析各模块对网络异常流量检测性能的贡献,通过消融实验对比 MHSECNN-BiLSTM 及其单一组成部分在公开数据集 NSL-KDD 和 CIC-IDS-2017 上的实验结果。实验评估主要基于准确率(Accuracy)、精确率(Precision)、召回率(Recall)和 F1-score(F1-score)等二分类指标。

表 2 为采用 MHSECNN-BiLSTM 及其单一组成部分在公开数据集 NSL-KDD 上的实验结果。MHSECNN-BiLSTM 模型的 Accuracy 为 85.40%, Precision 为 83.06%,Recall 为 93.42%,F1-score 为 87.93%,模型训练时间为 4 258.8 s。MHSECNN-BiLSTM 模型综合了多头注意力机制和时序建模的优点,准确率最高,优于单一 CNN、MHSECNN 和 BiLSTM 模型,表明 MHSECNN-BiLSTM 在区分正常流量与攻击流量方面具有较强的分类能力。基于 Precision 指标开展性能评估,BiLSTM 模型表现最佳,精确率为 92.87%。Precision 较小说明大量正常流量被误识别为恶意通信流量。Recall 高表示模型能够有效捕捉大部分异常流量,漏报率低。异常流量检测任务更关注 Recall 指标下模型性能。在 Recall 指标中,MHSECNN-BiLSTM 相较于单一 CNN、MHSECNN 和 BiLSTM 性能分别提升了 20.33%、10.70%和 23.72%。此外,在综合评估指标 F1-score 上,MHSECNN-BiLSTM 模型性能依然远超其余模型。此外,MHSECNN 与 CNN 相比,准确率提高了 3.04%。这表明结合多头注意力机制的 MHSECNN 能够更好地处理特征的选择,增强了模型的异常流量检测能力。MHSE 注意机制通过捕捉不同尺度的特征信息并动态加权特征模型能够关注信息量最大的信道,提升对复杂攻击流量的识别能力。尽管 MHSECNN-BiLSTM 模型的训练时间为 1 516.2 s,时间开销大于单一模型,但在准确性等评估指标上的性能提升证明了其在网络异常流量检测领域的有效性。

表 2　MHSECNN-BiLSTM 与单一网络的实验对比(NSL-KDD)

Table 2　Experimental comparison between MHSECNN-BiLSTM and a single network(NSL-KDD)

模型	Accuracy/%	Precision/%	Recall/%	F1-score/%	时间开销/s
CNN	81.27	92.42	73.09	81.62	357.7
MHSECNN	84.31	88.94	82.72	85.72	462.8
BiLSTM	79.70	92.87	69.70	79.63	1 004.1
MHSECNN-BiLSTM	85.40	83.06	93.42	87.93	1 516.2

表 3 为 MHSECNN-BiLSTM 及其单一组成部分在数据集 CIC-IDS-2017 上的实验结果。MHSECNN-BiLSTM 模型的 Accuracy 为 99.41%,Recall 为 99.85%,均明显优于对比模型。F1-score 为 99.20%,表明 MHSECNN-BiLSTM 在综合评价指标上也具有极高的性能。虽然 MHSECNN-BiLSTM 的训练时间较长,达 4 258.8 s,但其在 Accuracy、Recall、F1-score 上提升显著,进一步证实了所提模型在网络异常流量检测领域的效果。

表 3　MHSECNN-BiLSTM 与单一网络的实验对比 (CIC-IDS-2017)

Table 3　Experimental comparison between MHSECNN-BiLSTM and a single network(CIC-IDS-2017)

模型	Accuracy/%	Precision/%	Recall/%	F1-score/%	时间开销/s
CNN	96.97	99.96	91.70	95.65	698.9
MHSECNN	97.29	99.23	93.27	96.16	947.5
BiLSTM	97.05	95.44	96.52	95.98	1 911.6
MHSECNN-BiLSTM	99.41	98.56	99.85	99.20	4 258.8

2)与现有工作进行对比

为进一步验证所提 MHSECNN-BiLSTM 模型的效果,与现有的异常流量检测模型进行对比。Fatani 等[22]提出了一种基于 CNN 和差分进化算法 TSODE 的异常流量检测模型,利用 CNN 作为特征提取器,并通过 TSODE 进行特征选择,旨在增强模型的检测精度。Eilaiz 等[23]设计了一种基于深度学习和群体智能的新型网络入侵检测技术,利用 CNN 从网络流量数据中提取和学习复杂特征的表示,通过卷尾猴搜索算法进行特征选择,旨在提高分类准确性。杨宏宇等[3]设计了一种基于多尺度注意力特征增强的网络异常流量检测模型 MSAFE-ATD,利用动态特征选择算法去除冗余特征,并通过密集 CNN 和多尺度注意力网络进行拟合学习,旨在同时捕捉流量数据的局部和全局关联。

表 4 展示了 MHSECNN-BiLSTM 模型与现有的几种异常流量检测模型在 NSL-KDD 数据集上的对比结果。通过与 TSODE、CNN-CapSA 和 MSAFE-ATD 对比,MHSECNN-BiLSTM 在 Accuracy 上达到 85.40%,优于 TSODE 和 CNN-CapSA 和 MSAFE-ATD。虽然 MHSECNN-BiLSTM 在 Precision 指标上不占优势,但 MHSECNN-BiLSTM 的整体表现较为均衡,在 Accuracy、Recall 等指标上展现了更强的优势。在 Precision 指标上,MSAFE-ATD 达到了 92.12%,高于其他模型。Precision 较高表明 MSAFE-ATD 模型对正常流量的识别能力较强,但其 Recall 相对较低仅为 77.88%。相比之下,MHSECNN-BiLSTM 的 Precision 略低,但在 Recall 和 F1-score 上表现更出色,说明所提模型更适用于异常流量检测任务。

表 4　与现有异常流量检测模型进行对比(NSL-KDD)

Table 4　Comparison with existing anomalous traffic detection models(NSL-KDD)　%

模型	Accuracy	Precision	Recall	F1-score
TSODE	77.38	83.64	77.38	77.08
CNN-CapSA	77.21	83.59	77.21	76.89
MSAFE-ATD	83.14	92.12	77.88	84.02
MHSECNN-BiLSTM	85.40	83.06	93.42	87.93

表 5 展示了 MHSECNN-BiLSTM 模型与现有模型在 CIC-IDS-2017 数据集上的对比结果。MHSECNN-BiLSTM 同样表现优异,Accuracy 为 99.41%,优于所有模型。MHSECNN-BiLSTM 的 Recall 达到了 99.85%,表明 MHSECNN-BiLSTM 能够精准捕捉几乎所有异常流量,有效降低了漏报率。尽管基于 Precision 指标略逊于对比模型 MSAFE-ATD(99.67%)和 CNN-CapSA(99.57%),MHSECNN-BiLSTM 在 Recall 和 F1-score 指标上的优势,使其在整体检测性能上优于其他模型。

表 5　与现有异常流量检测模型进行对比(CIC-IDS-2017)

Table 5　Comparison with existing anomalous traffic detection models(CIC-IDS-2017)　%

模型	Accuracy	Precision	Recall	F1-score
TSODE	96.48	94.75	95.63	95.19
CNN-CapSA	98.08	99.57	95.15	97.31
MSAFE-ATD	98.90	99.67	97.31	98.48
MHSECNN-BiLSTM	99.41	98.56	99.85	99.20

通过与现有异常流量检测模型的对比,MHSECNN-BiLSTM 展示了其在 Accuracy、Recall 和 F1-score 等关键指标上的优势,尤其是在 Recall 和 F1-score 上提升明显,验证了结合 CNN、多头注意力机制和 BiLSTM 在异常流量检测领域的优势。

4　结　　论

本文提出了一种基于多头注意力机制和时空特征融合的网络异常流量检测方法,对公共数据集 NSL-KDD 进行训练和测试。通过卷积神经网络(CNN)提取流量数据的空间局部特征,并结合多头注意力机制对特征进行多角度自适应加权,以增强模型对异常流量的敏感性。将加权后特征输入双向长短期记忆网络(BiLSTM),捕捉流量数据中的长时间时序依赖关系。最后,通过 Softmax 分类器进行识别与分类。在公开数据集 NSL-KDD 和 CIC-IDS-2017 上进行实验,所提方法分别达到了 85.40% 和 99.41%的检测准确率,验证了其在异常流量检测任务中的有效性。实验结果表明所提模型能在复杂网络环境中有效处理网络流量的时空依赖特征,表现出了较强的泛化能力。在后续工作中,进一步优化注意力机制,以便在更复杂的流量场景中提升检测效果。

参考文献

[1] 潘成胜,李志祥,杨雯升,等. 基于二次特征提取和 BiLSTM-Attention 的网络流量异常检测方法[J]. 电子与信息学报,2023,45(12):4539-4547.
PAN CH SH, LI ZH X, YANG W SH, et al. Anomaly detection method of network traffic based on secondary feature extraction and BiLSTM-Attention[J]. Journal of Electronics & Information Technology, 2023, 45(12): 4539-4547.

[2] ODIATHEVAR M, SEAH W K G, FREAN M, et al. An online offline framework for anomaly scoring and detecting new traffic in network streams[J]. IEEE Transactions on Knowledge and Data Engineering, 2021, 34(11): 5166-5181.

[3] 杨宏宇,张豪豪,成翔. 基于多尺度注意力特征增强的异常流量检测方法[J]. 通信学报,2024,45(11):88-105.
YANG H Y, ZHANG H H, CHENG X. Abnormal traffic detection method based on multi-scale attention

feature enhancement[J]. Journal on Communications, 2024, 45(11): 88-105.

[4] LU C W, CAO Y X, WANG Z B. Research on intrusion detection based on an enhanced random forest algorithm[J]. Applied Sciences, 2024, 14(2): 714.

[5] 付子燨, 徐洋, 吴招娣, 等. 基于增量学习的 SVM-KNN 网络入侵检测方法[J]. 计算机工程, 2020, 46(4):115-122.
FU Z X, XU Y, WU ZH D, et al. SVM-KNN network intrusion detection method based on incremental learning [J]. Computer Engineering, 2020, 46(4): 115-122.

[6] KUMAR G S C, KUMAR R K, KUMAR K P V, et al. Deep residual convolutional neural network: An efficient technique for intrusion detection system[J]. Expert Systems with Applications, 2024, 238: 121912.

[7] WANG S, CAO J, PHILLIP S Y. Deep learning for spatio-temporal data mining: A survey [J]. IEEE Transactions on Knowledge and Data Engineering, 2020, 34(8): 3681-3700.

[8] GENG ZH Q, LI X M, 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.

[9] NARMADHA S, BALAJI N V. Improved network anomaly detection system using optimized autoencoder-LSTM [J]. Expert Systems with Applications, 2025,273: 126854.

[10] HAIBOUNI A, GUNAWAN T S, HABAEBI M H, et al. CNN-LSTM: Hybrid deep neural network for network intrusion detection system[J]. IEEE Access, 2022, 10: 99837-99849.

[11] 王琦,张涛,徐超炜,等. 多尺度注意力融合与视觉 Transformer 方法优化的电阻抗层析成像深度学习方法[J]. 仪器仪表学报, 2024, 45(7): 52-63.
WANG Q, ZHANG T, XU CH W, et al. Optimized learning method for electrical impedance tomography with multi-scale attention fusion and vision transformer [J]. Chinese Journal of Scientific Instrument, 2024, 45(7): 52-63.

[12] 顾伟, 行鸿彦, 侯天浩. 基于网络流量时空特征和自适应加权系数的异常流量检测方法[J]. 电子与信息学报, 2024, 46(6): 2647-2654.
GU W, XING H Y, HOU T H. Abnormal traffic detection method based on traffic spatial-temporal features and adaptive weighting coefficients [J]. Journal of Electronics & Information Technology, 2024, 46(6): 2647-2654.

[13] ZHANG CH, WANG F, ZHOU D Y, et al. A CNN-based fault diagnosis method of multi-function integrated RF system using frequency domain scanning with lasso regression[J]. Knowledge-Based Systems, 2025, 309: 112836.

[14] NAJARAN M H T. An evolutionary ensemble convolutional neural network for fault diagnosis problem [J]. Expert Systems with Applications, 2023, 233: 120678.

[15] TONG J H, ZHANG Y. A real-time label-free self-supervised deep learning intrusion detection for handling new type and few-shot attacks in IoT Networks[J]. IEEE Internet of Things Journal, 2024, 11(19): 30769-30786.

[16] ARAUJ-FILHO P F, NAILI M, KADDOM G, et al. Unsupervised gan-based intrusion detection system using temporal convolutional networks [J]. IEEE Transactions on Network and Service Management, 2024, 20(4): 4951-4963.

[17] WANG T, YIN L F. A hybrid 3DSE-CNN-2DLSTM model for compound fault detection of wind turbines[J]. Expert Systems with Applications, 2024, 242: 122776.

[18] BAO T, ZAIDI S A R, XIE SH Q, et al. A CNN-LSTM hybrid model for wrist kinematics estimation using surface electromyography [J]. IEEE Transactions on Instrumentation and Measurement, 2020, 70: 1-9.

[19] GAO Y F, ZHENG J B, HUANG L P, et al. A novel BILSTM-CNN method for pattern recognition in real time under triple physical loads in lower extremity exoskeleton [J]. IEEE Sensors Journal, 2023, 23(14): 15689-15701.

[20] WU Y, LIN G, LIU L, et al. Masinet: Network intrusion detection for IoT security based on meta-learning framework [J]. IEEE Internet of Things Journal, 2024, 11(14): 25136-25146.

[21] 陈万志, 任鹏江, 王天元. 因素空间背景基的流量异常检测基点分类方法[J].电子测量与仪器学报,2024, 38(6):84-94.
CHEN W ZH, REN P J, WANG T Y. Traffic anomaly detection method based on fundamental point classification by factor space background basis [J]. Journal of Electronic Measurement and Instrumentation, 2024, 38(6): 84-94.

[22] FATANI A, ELAZIZ M A, DAHOU A, et al. IoT intrusion detection system using deep learning and enhanced transient search optimization [J]. IEEE Access, 2021, 9: 123448-123464.

[23] EILAIZ M A, AL-QANESS M A A, DAHOU A, et al. Intrusion detection approach for cloud and IoT environments using deep learning and capuchin search algorithm [J]. Advances in Engineering Software, 2023, 176: 103402.

作者简介

徐仪帆(通信作者),本科,主要研究方向为网络安全和人工智能。
E-mail:1927522735@qq.com