

基于并联分支特征融合的网络入侵检测模型

杨天宇¹, 王恒¹, 马自强^{1,2}, 崔梦真¹, 唐妍¹, 王英翔¹

(1. 宁夏大学信息工程学院; 2. 宁夏大学宁夏“东数西算”人工智能与信息安全重点实验室, 宁夏银川 750021)

摘要: 网络入侵检测系统能有效检测、识别网络攻击。针对现有模型无法完整表述流量信息且多分支模型无法很好地融合各支路提取特征的问题, 提出一种并联分支特征融合的检测网络入侵。在特征提取方面, 通过BiGRU提取全局时间特征, 采用叠层先验注意力网络提取原始流量的空间特征; 在分支融合方面, 提出一种自适应的特征融合方法动态融合多维度特征。在CICIDS2018数据集上的实验表明, 所提模型的多分类准确率、检测率和误报率效果良好; 在NSL-KDD、UNSW-NB15数据集上的泛化能力实验表明, 所提模型在实时恶意流量检测中对未知恶意流量的检测能力良好。

关键词: 网络安全; 深度学习; 特征融合; 通道先验注意力机制; 流量检测

DOI: 10.11907/rjdk.242064

中图分类号: TP309

文献标识码: A

文章编号: 1672-7800(2026)003-0150-07

扫描二维码阅读全文:



Network Intrusion Detection Model Based on Parallel Branch Feature Fusion

YANG Tianyu¹, WANG Heng¹, MA Ziqiang^{1,2}, CUI Mengzhen¹, TANG Yan¹, WANG Yingxiang¹

(1. School of Information Engineering, Ningxia University; 2. Ningxia Key Laboratory of Artificial Intelligence and Information Security for Channeling Computing Resources from the East to the West, Ningxia University, Yinchuan 750021, China)

Abstract: The network intrusion detection system can effectively detect and identify network attacks. To address the issues of existing models failing to fully describe traffic information and multi-branch models being unable to effectively integrate features extracted from each branch, a model with parallel branch feature fusion is proposed for network intrusion detection. In terms of feature extraction, global temporal features are extracted using BiGRU, while stacked prior attention networks are employed to capture spatial features of raw traffic. Regarding branch fusion, an adaptive feature fusion method is introduced to dynamically integrate multi-dimensional features. Experiments on the CICIDS2018 dataset demonstrate that the proposed model achieves favorable results in multi-class classification accuracy, detection rate, and false positive rate. Generalization capability tests on the NSL-KDD and UNSW-NB15 datasets further confirm the model's effective detection of unknown malicious traffic in real-time malicious traffic detection.

Key Words: network security; deep learning; feature fusion; channel prior attention mechanism; traffic detection

0 引言

随着物联网(Internet of Things, IoT)、云计算和大数据相关技术与服务的飞速发展,网络安全形势日益严峻。网络攻击者利用社会工程学、恶意软件、零日漏洞等攻击手段入侵网络系统,获取隐私信息或破坏网络系统。为了解决上述问题,本文提出一种基于深度学习技术的入侵检测

模型应对网络攻击^[1,2]。

近年来,研究人员使用多种深度学习技术提升网络攻击检测的准确率和泛化能力。在不同场景提取流量特征时, Kumari等^[3]提出一种基于卷积神经网络(Convolutional Neural Network, CNN)的16层网络框架NID-VGG16提取流量时间序列和协议特征,使用一维CNN-BiLSTM模型进行分类。同时,为了对不同类别的攻击和不同大小的特征保持一致的有效性,将多级、多尺度的特征与数据增强方

收稿日期: 2025-01-13

基金项目: 宁夏回族自治区重点研发计划一般项目(2022BDE03008)

作者简介: 杨天宇(2000-), 男, 宁夏大学信息工程学院硕士研究生, 研究方向为网络入侵检测; 王恒(1975-), 男, 博士, 宁夏大学信息工程学院教授, 研究方向为网络空间安全、自然语言处理; 马自强(1990-), 男, 博士, 宁夏大学信息工程学院副教授, 研究方向为计算机系统安全、区块链应用安全; 崔梦真(2001-), 女, 宁夏大学信息工程学院硕士研究生, 研究方向为流量分析、恶意代码检测; 唐妍(2001-), 女, 宁夏大学信息工程学院硕士研究生, 研究方向为流量识别、模型安全; 王英翔(1997-), 女, 宁夏大学信息工程学院硕士研究生, 研究方向为流量识别、高级逃逸技术识别。本文通讯作者: 王恒。

法相结合,在两个测试数据集中效果优秀。Binbusayyis等^[4]设计了用于检测云计算环境的网络威胁模型,使用RBFSVR方法提取网络数据包的属性特征且训练时间更少,并对不同的攻击使用混合VGG19-2DCNN分类器进行分类,以提取包含SYN、ACK标志位的网络数据包来检测、阻止SYN洪泛(SYN Flood)攻击。实验表明,该算法在3个测试数据集中都取得了良好的检测效果。Ren等^[5]为了提升模型检测准确率、解决小样本类不平衡问题,提出分层结构CNN-Attention网络CANET,通过混合CNN与注意力机制对测试数据集进行时空特征提取,以提升准确率和对少数类别的检测效果。Li等^[6]提出一种基于深度学习的工业物联网入侵检测方法,结合CNN与双向长短期记忆网络(BiLSTM)提取流量特征,先对数据集进行预处理,再通过一维卷积提取具有时序关系的特征,以提升模型检测能力。陈虹等^[7]针对恶意流量分类的不平衡数据,首先使用改进的合成少数类过采样技术borderline-SMOTE与基于高斯混合模型的欠采样聚类技术进行流量数据特征平衡处理,其次使用1D-CNN提取数据的局部特征,最后利用一种双向门控循环单元BiGRU提取数据中的时序特征,以提升模型检测率。Zhu等^[8]提出CMTSNN模型高效识别物联网的异常加密流量,结合时间序列与空间特征提取确保特征的鲁棒性。

在流量检测的分支关联关系研究中,卷积网络设计主要关注深度、滤波器大小和特征通道数量等因素。研究表明,先采用分支结构将计算过程拆分为并行的不同分支线程,聚合多个输出,以显著提升模型性能。Wang等^[9]提出一种结合多分支网络和垂直阻塞聚合(FedVB)的联邦网络入侵检测系统的新型多分支模型,集成二分类器仅传输有效的梯度,可提升攻击类型识别的准确性,减少通信与计算开销。Shi等^[10]提出一种多模态混合分支并行网络入侵检测模型MHPN,首先针对网络流量数据中的丰富特征和复杂攻击手段,从网络流量的统计信息与原始负载中提取特征,其次分别构建卷积神经网络和长短期记忆网络作

为不同的分支进行特征提取,最后通过特征融合和Cos-Margin分类器进行分类。Cai等^[11]提出一种基于度量学习的混合并行深度学习模型高效地检测网络入侵行为,模型顶部分支采用全卷积神经网络,底部分支采用传统卷积神经网络。研究表明,两个分支并行工作可增强分支间的特征关联性。Song等^[12]提出一种基于TCN、BiGRU与注意力机制的网络入侵检测方法TGA,结合局部、全局时间特征,并利用自注意力机制捕捉序列中不同分支的相关性以提升模型性能。Huma等^[13]提出一种基于注意力机制的卷积神经网络ACNN,以检测物联网中的网络攻击。模型分支结合了Inception架构与空间注意力机制,优化了特征提取和定位,提升了检测准确性和效率。

虽然上述研究都取得了显著效果,为网络入侵检测作出了贡献,但仍有改进之处:①现有部分方法无法完整地提取时间、空间和统计等方面的入侵流量特征;②现有部分模型将各分支结果进行拼接,未考虑分支间复杂的关联关系,影响了模型检测效果,或直接将多个特征串联在一起,影响了各特征之间的相关性信息。

为此,本文提出了一种并联分支特征融合的网络入侵检测模型(Parallel Spatio Temporal Fusion Model, PSTFM)。首先,将数据集进行清洗和数字化等预处理操作,采用叠层先验注意力残差网络与BiGRU分别提取空间特征和时序特征的原始流量;其次,利用多维度特征融合模块使两个分支的特征相互调整,以捕获两个分支特征的关联关系;最后,将融合的特征输入全连接层进行恶意入侵流量分类。

2 并联分支特征融合模型

2.1 特征提取

图1为PSTFM网络结构,包括空间特征提取模块与时序特征提取模块,两个模块并行使用以避免串行带来的信息丢失问题,从而提升模型检测效果。

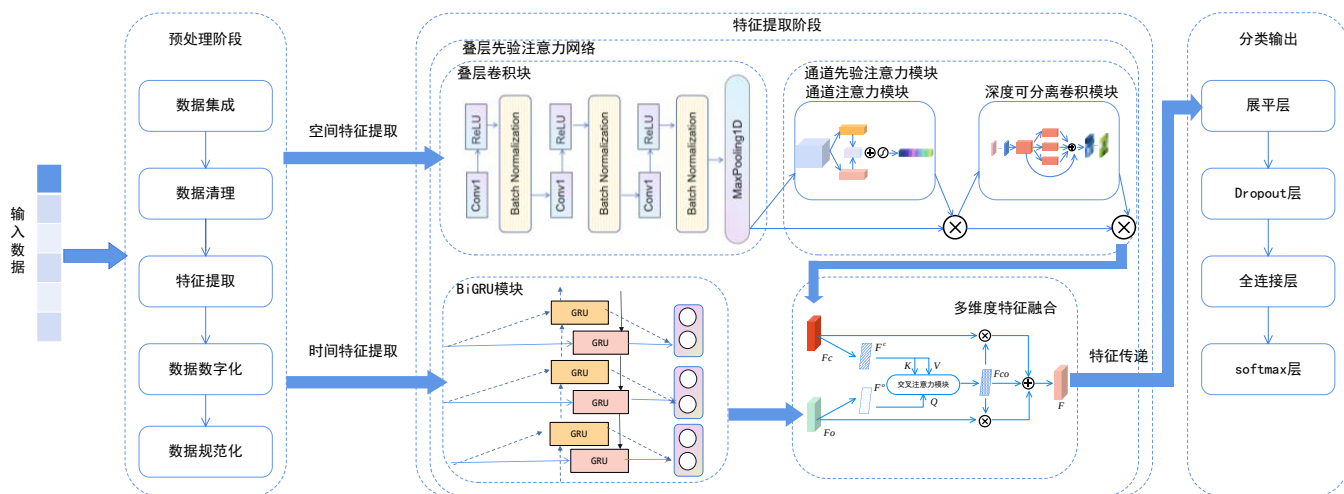


Fig. 1 PSTFM network structure

图1 PSTFM网络结构

2.1.1 空间特征提取

本文设计了叠层先验注意力网络来提取流量空间特征。其中,叠层卷积块通过逐渐提取更高级别的特征表示,以增强网络对复杂模式的表达能力;通道先验注意力模块自适应地调整每个通道的权重,提升网络对关键特征的关注度,以提升网络分析入侵流量的性能。

叠层卷积块是一种专门处理一维数据的卷积神经网络模块,引入了特征图概念描述卷积层输出的多维矩阵,旨在从输入数据中提取流量局部特征,以表示输入数据在不同层级上的特征表征。首先,对VGG网络进行改进,叠层卷积块采用3个连续的一维卷积层,卷积核大小为3,步长为1,填充操作使用的是“零填充”(在输入序列两端填充零值),以保持输出与输入序列长度一致^[14];其次,在每个卷积层后添加ReLU激活函数与批量归一化,使模型训

练更稳定、收敛更快;最后,利用最大池化层进行下采样操作,以减少特征图的尺寸并提取重要特征。

图2为通道先验注意力模块结构,是一种结合了深度可分离卷积(Depthwise Separable Convolutional Blocks, DSCB)与通道注意力机制的先进神经网络组件,旨在优化一维网络处理入侵流量数据的效率。在网络训练前,通过特征和模式分析优化注意力机制,考虑流量数据中的特征和模式,在训练过程中引导模型更好地关注关键特征。具体为:首先,利用通道注意力机制的动态权重调整策略,基于输入数据的平均池化与最大池化结果,通过卷积操作和ReLU激活函数生成Sigmoid门控输出^[15];其次,通过注意力权重加权输入数据,增强模型对关键特征的表达能力;最后,模型通过预先计算的通道注意力向量,在训练过程中关注更具信息量的特征。

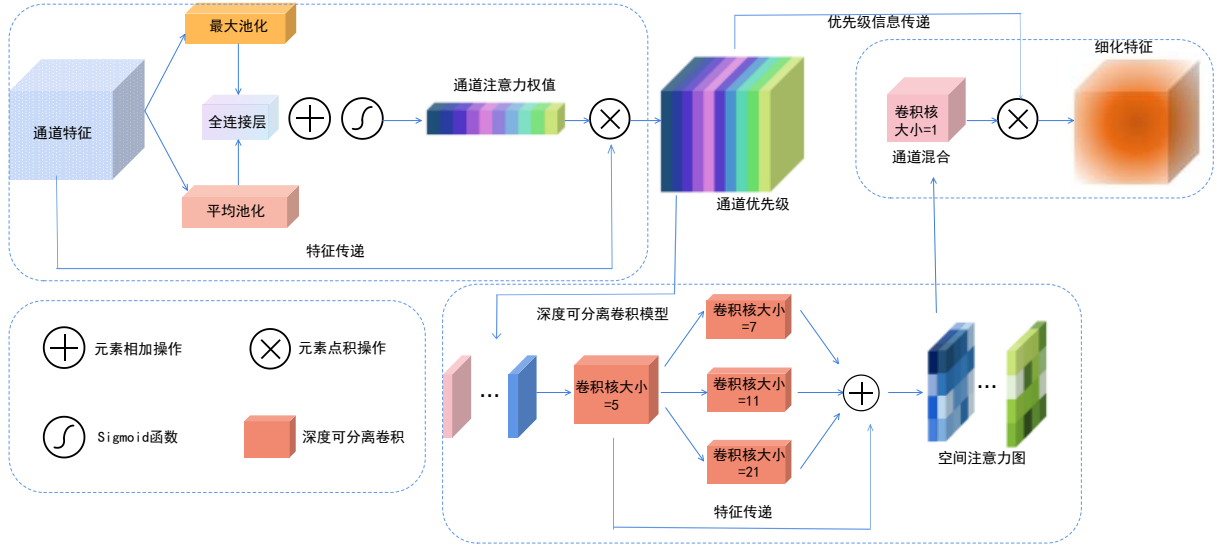


Fig. 2 Channel prior attention module structure

图2 通道先验注意力模块结构

本文对深度可分离卷积模块进行改进,使用不同大小的卷积核捕捉流量数据中的多尺度空间结构^[16]。具体地,小卷积核(5)能捕捉更细微的局部细节与纹理信息;中等卷积核(7)能在局部区域内有效地捕捉中等尺度特征,达到局部细节和全局信息之间的平衡;大卷积核(11、21等)具有更大的感受野,可捕捉更大范围的全局信息与上下文关系,适合处理较大的结构或整体形状。实验表明,当卷积核为5、7、11、21时,模型的特征提取效果最好。

通道先验注意力模块的设计结合了通道注意力与深度可分离卷积的优点,强化了模型对关键特征的捕捉能力和识别网络入侵攻击的能力。具体为:首先,通过逐点卷积进一步整合特征,与注意力加权输入相乘,实现重要特征与空间结构的有机结合;其次,通过逐点卷积调整输出维度,以满足神经网络后续层对数据处理的需求。

$$CA(x) = \sigma \left(Conv_2 \left(ReLU \left(Conv_1 \left(AvgPool(x) \right) \right) + Conv_1 \left(MaxPool(x) \right) \right) \right) \quad (1)$$

式中: x 为输入特征图; $AvgPool(x)$ 为平均池化结果;

$MaxPool(x)$ 为最大池化结果; $Conv_1$ 、 $Conv_2$ 分别为两个卷积操作; σ 为sigmoid激活函数。

深度可分离卷积块的计算公式为:

$$DBCABlock(x) = Conv_3 \left(\left(\sum_{i=1}^4 DConv_i \left(CA \left(Conv_2 \left(GELU \left(Conv_1(x) \right) \right) \right) \right) \right) \cdot CA \left(Conv_1(x) \right) \right) \quad (2)$$

首先,输入特征图 x 经过 $Conv_1$ 卷积进行降维并引入非线性特征,再应用GELU激活函数增强特征表达能力;其次,特征图通过一个 $Conv_2$ 卷积、通道注意力模块CA动态调整特征通道权重,以突出重要特征;再次,DSCB引入4个不同尺度的深度卷积操作捕捉多尺度特征信息, $Conv_3$ 起到整合、提炼特征的重要作用;最后,将输出特征图与通道注意力模块结果相乘,以确保模型有效利用输入信息。

2.1.2 时序特征提取

本文通过BiGRU提取流量时序特征,能在一定程度上

缓解传统循环神经网络(Recurrent Neural Network, RNN)存在的梯度爆炸和消失问题。BiGRU是GRU的一种变体形式,可通过正序、逆序两种方式学习数据的时序关系,通过BiGRU网络处理流量特征得到时序特征。

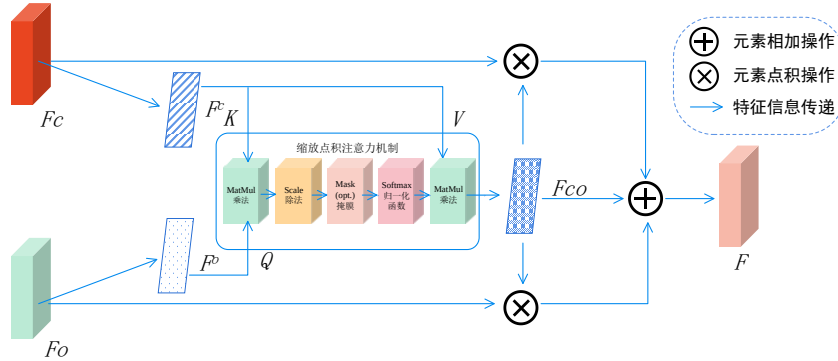


Fig. 3 Feature fusion model architecture

图3 特征融合模型结构

首先,为了融合各维度特征图的上下文时序信息,通过平均池化得到 $1 \times H \times W$ 大小的特征图 F_c 、 F_o ,并构建 Key(K)、Value(V)和 Query(Q);其次,对空间维度的特征 F_c 执行下采样操作,以确保空间与时间维度特征 F_c 、 F_o 尺寸一致;再次,将构建的特征输入缩放点积注意力模块,以获取融合特征 F_o ,以反映空间与时间维度特征的关联语义;最后,应用 Sigmoid 函数,沿通道维度得到关联语义 F_{co} 的语义分布权重矩阵 W_{co} 。具体计算公式为:

$$F_{co} = \text{Softmax}\left(\frac{KQ^T}{\sqrt{d}}\right)V \quad (3)$$

式中: d 为特征维度。

考虑到空间与时间维度特征在提升模型性能时的重要性有所不同。本文设计了一种自适应特征融合函数,利用关联语义分布权重矩阵 W_{co} 约束两类特征。

$$F = (1 - W_{co}) \otimes F^c + W_{co} \otimes F^o \quad (4)$$

式中: F 表示融合后的特征; W_{co} 为关联语义分布权重矩阵,以动态调整空间和时间特征的融合比例; F^c 表示空间维度特征; F^o 表示时间维度特征。

本文通过逐元素点乘操作对两种特征进行融合运算,确保模型在处理不同类型信息时的灵活性和适应性。这种自适应特征融合方法有助于提升模型整体性能,充分挖掘空间、时间特征在不同任务中的相对重要性,可显著提升模型的准确性和鲁棒性。

3 实验数据处理

3.1 实验数据集

本文实验数据来源于公开数据集 CICIDS2018(具有大量的样本数据量),选择了10天内包含攻击流量的样本^[17]。其中,实验数据集包含 PCAP、CSV 格式文件,CSV 格式文件由 CICFlowMeter-V3 生成,包含10个 CSV 文件,

2.2 特征融合

为了挖掘两个分支间更有效的关联关系,参考文献[17]构建特征融合模块以获得两个分支的联合特征,如图3所示。

约1 600万实例。此外,恶意流量分包括 Bruteforce、Dos、DDOS、Infiltration、Bot 和 Web 攻击等6类,在真实网络环境中较为常见,对系统影响相大、范围广,可造成用户数据泄露、系统漏洞利用等严重问题^[18]。

表1为 CICIDS2018 数据集的特征。本文仅使用8个 CSV 文件将数据集分成3类:10%用于测试,其余样本以9:1的比例划分为训练、验证样本^[18,19]。

Table 1 Details of CICIDS2018 dataset features

表1 CICIDS2018数据集特征细节

特征名称	特征简短介绍	数据类型
Active mean	数据流在空闲之前处于活动状态的平均时间	Float
Bwd Pkt Len Mean	反向模式网络数据包的平均大小	Float
Dst Port	目标端口号	Integer
Flow Duration	发生连接的持续时间	String
Idle Std	数据流在激活之前处于空闲状态的标准偏差时间	Float
...	...	...
Protocol	用于数据连接的协议	Integer

3.2 预处理

本文对原始数据集的预处理操作为:

(1)数据整合。首先,从 CICIDS2018 数据集中选取8天的流量样本;其次,将8个 CSV 文件整合在一起;最后,将14个不同的标签重新分类为7类,包括1个良性标签和6个恶意标签,数据集大小合计6 GB。

(2)数据清洗。数据集中的异常流量会对训练产生影响,因此删除包含 NaN、Infinity 和 null 值的行。数据清洗前,良性样本为5 567 951个,恶意样本为2 103 173个;数据清洗后,良性样本为5 538 387个,恶意样本为2 102 418个。

(3)特征处理。CICIDS2018数据集共有79个属性和1个标签,由于时间戳对网络入侵流量识别存在轻微影响,本文已将其删除。

(4)数据数字化。one-hot 编码方法将分类特征转换为数字变量。

(5)数据归一化。规范化数据特征可平衡每个特征值的大小,确保深度学习模型在反向传播时收敛,降低较大特征值对模型的影响。实验中,选择Min-Max归一化方法将数值特征归一化到 $[0,1]$ 。

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (5)$$

式中: x' 为归一化数据; x 为当前数据; $\min(x)$ 为最小数据值; $\max(x)$ 为最大数据值。

4 实验结果与分析

4.1 实验环境

本文实验使用Xeon(R) Platinum 8352V处理器,独立显卡为NVIDIA GeForce RTX 4090,基于Keras学习框架,Python版本为3.7,模型优化器为Adam,交叉熵损失函数为categorical_crossentropy。在训练过程中,模型样本数的批处理大小为256,实验轮数为200。

4.2 性能指标

本文采用混淆矩阵作为评价指标, TP (真阳性)表示在数据集中异常流量被正确识别为异常的实例数量, TN (真阴性)表示正常流量的实例被准确地识别为正常的实例数量, FP (假阳性)表示异常流量被错误地识别为正常流量的实例数量, FN (假阴性)表示被错误识别为异常的正常流量实例数量。同时,通过准确性、误报率、检测率和 F_1 -score评估模型性能。

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

$$fpr = \frac{FP}{FP + TN} \quad (7)$$

$$dr = recall = \frac{TP}{TP + FN} \quad (8)$$

$$F_1(F_1 - score) = 2 \times \frac{precision \times recall}{precision + recall} \quad (9)$$

4.3 消融实验

为了进一步论证叠层先验注意力网络、BiGRU网络及特征融合模块的有效性,进行了多组消融实验以比较不同结构的模型性能,包括PSTFM、仅提取流量的空间特征的PSFM、仅提取流量的时序特征的PTFM、删除特征融合模块且仅采用拼接方式融合空间特征和时序特征的PSTM、将提取空间特征和时间特征模块串行连接的STFM。消融实验结果如表2所示。

由表2可知,在仅使用空间特征或时序特征的情况

Table 2 Results of ablation experimentt

表2 消融实验结果 (%)				
模型名称	准确率	精度	F1值	FPR值
PSTFM	98.21	98.13	98.16	1.3
PSFM	96.35	97.14	96.74	2.5
PTFM	97.15	97.23	97.19	2.0
PSTM	97.47	97.56	97.51	1.5
STFM	97.67	97.79	97.72	1.5

下,模型准确率相较于PSTFM分别下降1.86%、1.06%,验证了同时考虑空间特征与时序特征的模型相较于仅考虑单一特征的模型表现更好。在删除特征融合模块后,仅采用拼接方式融合空间特征与时序特征的模型性能相较于PSTFM下降0.24%,相较于仅提取时序特征的模型而言只提升0.32%,证明了简单的拼接空间特征与时序特征无法有效利用这两种特征,进一步验证了特征融合模块的有效性。将提取空间特征与时间特征模块串行连接改为并行连接后,模型性能提升0.54%,原因为并行连接通过同时提取不同特征、增强多样性、减少信息传递瓶颈,可能有效避免信息丢失。

综上,本文模型在准确率、精度、F1值和FPR值的表现最好,模型结构和模块更合理。

4.4 比较实验

本文基于CICID2018数据集,选择4种在特征提取和分支关联方面较为优异的深度学习模型,以比较所提模型的性能,如表3所示。

Table 3 Detection performance of 5 models on the CICIDS2018

dataset				
表3 5种模型在CICIDS2018数据集下的检测效果 (%)				
模型	准确率	精度	F1值	FPR值
TCN-BiGRU-Attention	97.83	97.85	97.84	1.8
CNN-BiLSTM	97.36	96.72	97.54	2.9
CANET	96.35	96.68	96.51	2.5
ACNN-IDS	97.11	97.36	97.23	1.9
PSTFM(本文模型)	98.21	98.13	98.16	1.3

TCN-BiGRU-Attention结合了时间卷积网络(Time Convolutional Network, TCN)与双向门控循环单元(BiGRU),能有效提取网络流量序列的局部和全局时间特征,TCN专注于捕捉短期的局部时间信息,BiGRU能学习更长时间范围内的全局特征,模型通过自注意力机制捕捉序列中不同分支之间的相关性,有助于理解不同时间点特征间的关联,增强了特征提取深度和广度^[12]。CNN-BiLSTM结合了一维卷积神经网络(1D-CNN)与双向长短期记忆网络(BiLSTM),能同时提取空间特征和时间特征,CNN在局部特征提取上表现优越,BiLSTM则专注于学习时序特征,尽管该模型通过拼接融合了空间和时间特征,但未充分考虑分支之间的关联关系,可能导致信息冗余和丢失^[6]。CANET采用分层结构结合CNN与注意力机制,专注于提取局部时空特征,通过组合多层CA块使模型深入学习网络攻击数据的多层次特征,在特征提取过程中应用注意力机制在不同分支上关注重要特征,以增强特征间的关联性^[5]。ACNN-IDS是基于注意力的CNN模型,可利用空间注意机制提取流量数据中的关键区域特征,预训练的Inception架构有助于捕捉多尺度特征,尽管ACNN-IDS能关注关键区域,但在时序特征提取和分支关联上存在不足,未能充分挖掘空间和时间特征间的关系^[13]。

由表 3 可知,所提模型分类性能较高,在准确率、精度、F1 值和 FPR 值上表现出色,原因为 CANET、ACNN-IDS 模型采用残差网络与注意力机制只能提取流量空间特征,并未考虑时序特征。其中,CNN-BiLSTM 通过拼接的方式融合空间特征与时序特征,未考虑两种特征的关联关系;TCN-BiGRU-Attention 未使用更高效的特征融合模块,无法充分利用两种特征间的关联关系。

4.5 泛化能力分析

在网络入侵检测领域,NSL-KDD、UNSW-NB15 是两个广泛使用的主流数据集,各具独特的流量特点^[20,21]。NSL-KDD 数据集经过了精心设计和预处理,通过删除重

复、冗余和不相关的流量样本,改进了原始的 KDDCup99 数据集,包含 5 个主要的攻击类别,每个类别下又细分多个子类别;UNSW-NB15 数据集包含 10 个攻击类别,每个类别代表一种特定的网络攻击类型,流量特点在于其更新性和代表性,包含近年来出现的一些新型攻击,使研究者能更好地了解 and 应对最新的网络威胁。

本文在 NSL-KDD、UNSW-NB15 数据集中,将比较模型与本文模型进行检测,如表 4 所示。由此可知,本文模型在 NSL-KDD 和 UNSW-NB15 数据集上与 CANET 模型性能相近,但相较于其他模型优势明显,具有较好的泛化能力。

Table 4 Detection performance of 5 models based on NSL-KDD and UNSW-NB15 datasets

表 4 基于 NSL-KDD 和 UNSW-NB15 数据集 5 种模型检测效果 (%)

模型	NSL-KDD				UNSW-NB15			
	准确率	精度	F1 值	FPR 值	准确率	精度	F1 值	FPR 值
TCN-BiGRU-Attention	98.89	98.78	98.83	1.50	88.97	97.87	93.20	1.76
CNN-BiLSTM	99.22	99.60	99.41	0.43	88.84	98.52	93.43	1.82
CANET	99.77	99.72	99.74	0.18	89.39	98.93	93.92	0.87
ACNN-IDS	98.21	98.32	98.26	0.58	87.54	97.35	92.18	2.55
PSTFM(本文模型)	99.80	99.82	98.16	0.18	90.10	99.14	94.40	0.76

4.6 实时流量检测

为了评估本文模型在线检测实时恶意流量的能力,收集了真实网络环境下 1 天的流量数据,数据清洗后的数据集大小为 11 GB,包含了 CICIDS2018 数据集中未出现的 6 种恶意流量数据(Tor 恶意软件、CVE 漏洞数据库、Web-Shell 恶意脚本、FastTunnel 内网穿透攻击、Lanproxy 局域网穿透攻击、NPS 网络性能监视攻击)。同时,将收集的数据集与原 CICIDS2018 数据集的测试集相结合形成增强数据集,大小为 40 GB,以检测 5 种模型的性能,如表 5 所示。由此可知,本文模型具备了识别未知恶意流量攻击的能力,在真实网络环境下的性能指标均优于其他模型。

Table 5 Detection performance of 5 models based on enhanced dataset

表 5 基于增强数据集 5 种模型检测效果 (%)

模型	准确率	精度	F1 值	FPR 值
TCN-BiGRU-Attention	97.67	97.52	97.59	2.0
CNN-BiLSTM	97.15	96.45	96.80	3.5
CANET	95.89	96.41	98.15	2.9
ACNN-IDS	97.01	96.89	96.95	2.5
PSTFM(本文模型)	98.12	98.03	98.07	1.5

5 结语

本文针对现有网络入侵检测模型在特征提取和特征融合方面的不足,提出一种并联分支特征融合的网络入侵检测模型。首先,通过叠层先验注意力网络与 BiGRU 网络分别提取流量的空间特征、时序特征;其次,利用特征融合

模块挖掘两种特征之间的关联关系,以有效融合特征。

实验表明,所提模型在 CICIDS2018 数据集及其他两个数据集上的多分类准确率、检测率和误报率均优于其他模型,在网络入侵检测中的优越性和泛化潜力较高。同时,本文模型在实时恶意入侵流量的在线能力评估中的表现也十分出色,进一步验证了其有效性和实用性。

未来,将考虑在模型中引入无监督或半监督方法,以完善模型并提升其对未知攻击的识别能力,为网络入侵检测领域的发展提供参考与启示。

参考文献:

[1] LI Z W, DENG Z H, YE C R, et al. A network intrusion detection method based on ICNN-MMD[J]. Software Guide, 2023, 22(12): 173-177.
李卓文,邓在辉,叶彩瑞,等. 基于 ICNN-MMD 的网络入侵检测方法[J]. 软件导刊, 2023, 22(12): 173-177.

[2] HUANG H B, WAN L, ZHU K. Research on intrusion detection method based on transformer[J]. Software Guide, 2022, 21(9): 121-128.
黄海彬,万良,褚堃. 基于 Transformer 的入侵检测方法研究[J]. 软件导刊, 2022, 21(9): 121-128.

[3] KUMARI R, DURGA N, GAYATHRI T, et al. Advanced NID-VGG16 with orca predation optimization based IDCNN-BiLSTM for network intrusion detection [C]// 14th International Conference on Cloud Computing, Data Science & Engineering, 2024: 840-845.

[4] BINBUSAYYIS A. Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment [J]. Expert Systems with Applications, 2024, 238: 121758.

[5] REN K, YUAN S, ZHANG C, et al. CANET: a hierarchical CNN-attention model for network intrusion detection [J]. Computer Communications, 2023, 205: 170-181.

- [6] LI A, YI S. Intelligent intrusion detection method of industrial Internet of Things based on CNN-BiLSTM [J]. Security and Communication Networks, 2022(1): 5448647.
- [7] CHEN H, QI B, JIN H B, et al. Class-imbalanced traffic abnormal detection based on 1D-CNN and BiGRU [J]. Computer Application, 2024, 44(8): 2493-2499.
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.
- [8] ZHU S, XU X, GAO H, et al. CMTSNN: a deep learning model for multi-classification of abnormal and encrypted traffic of Internet of Things [J]. IEEE Internet of Things Journal, 2023, 13(10): 11773-11791.
- [9] WANG Y, ZHENG W, LIU Z, et al. A federated network intrusion detection system with multi-branch network and vertical blocking aggregation [J]. Electronics, 2023, 12(19): 4049.
- [10] SHI S, HAN D, CUI M. A multimodal hybrid parallel network intrusion detection model[J]. Connection Science, 2023, 35(1): 2227780.
- [11] CAI S, HAN D, YIN X, et al. A hybrid parallel deep learning model for efficient intrusion detection based on metric learning[J]. Connection Science, 2022, 34(1): 551-577.
- [12] SONG Y, LUKTARHAN N, SHI Z, et al. TGA: a novel network intrusion detection method based on TCN, BiGRU and attention mechanism [J]. Electronics, 2023, 12: 2849.
- [13] HUMA Z E, AHMAD J, HAMADI H, et al. ACNN-IDS: an attention-based CNN for cyberattack detection in IoT[C]// 2024 2nd International Conference on Cyber Resilience, 2024: 1-6.
- [14] SIMONYAN K, ZISSERMAN A. Very deep convolutional networks for large-scale image recognition [DB/OL]. <https://arxiv.org/abs/1409.1556>.
- [15] BASTIDAS A A, TANG H. Channel attention networks [C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019: 881-888.
- [16] HUANG H, CHEN Z, ZOU Y, et al. Channel prior convolutional attention for medical image segmentation [J]. Computers in Biology and Medicine, 2024, 178: 108784.
- [17] CHEN Y C. Abnormal traffic detection for ship network based on multi-scale fusion attention [J]. Radio Engineering, 2024, 54(8): 2040-2047.
陈育才. 基于多维度融合注意力的舰船网络异常流量检测[J]. 无线电工程, 2024, 54(8): 2040-2047.
- [18] SHARAFALDIN I, LASHKARI A H, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization [EB/OL]. <https://www.semanticscholar.org/paper/Toward-Generating-a-New-Intrusion-Detection-Dataset-Sharafaldin-Lashkari/a27089efabc5f4abd5ddf2be2a409bff41f31199>.
- [19] KHAN M A, KIM J. Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset [J]. Electronics, 2020, 9(11): 1771.
- [20] DHANABAL L, SHANTHARAJAH S. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms [EB/OL]. https://e-tarjome.com/storage/btn_uploaded/2019-07-13/1563006133_9702-etarjome-English.pdf.
- [21] MOUSTAFA N, SLAY J. The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set [J]. Information Security Journal A Global Perspective, 2016, 25: 18-31.
- [22] TAVALLAE M, BAGHERI E, LU W, et al. A detailed analysis of the KDD CUP 99 data set [C]// Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009: 1-6.

(责任编辑: 刘嘉文)