doi：10.13413/j.cnki.jdxblxb.2023245

基于改进的 CNN-Transformer 加密流量分类方法

高新成[1]，张 宣[2]，樊本航[2]，刘 威[2]，张海洋[2]
（1. 东北石油大学 现代教育技术中心，黑龙江 大庆 163318；
2. 东北石油大学 计算机与信息技术学院，黑龙江 大庆 163318）

摘要： 针对传统加密流量分类模型对特征提取不足导致分类准确率较低等问题，使用深度学习技术，提出一种基于改进的卷积神经网络结合 Transformer 的加密流量分类模型. 为提高分类精度，首先将数据集切割填充并完成标准化处理；然后采用 Transformer 网络模型中的多头注意力机制捕获长距离的特征依赖，利用卷积神经网络提取局部特征；最后加入 Inception 模块实现多维特征提取和特征融合，完成模型训练和加密流量分类. 在公共数据集 ISCX VPN-non-VPN 2016 上进行实验验证，实验结果表明，该模型的分类准确率达 98.5%，精确率、召回率和 F_1 值均达 98.2%以上，相比其他模型分类效果更优.

关键词： 加密流量分类；卷积神经网络；多头注意力机制；特征融合
中图分类号： TP393.08 **文献标志码：** A **文章编号：** 1671-5489(2024)03-0683-08

Improved CNN-Transformer Based Encrypted Traffic Classification Method

GAO Xincheng[1], ZHANG Xuan[2], FAN Benhang[2], LIU Wei[2], ZHANG Haiyang[2]
(1. *Modern Education Technology Center, Northeast Petroleum University, Daqing* 163318, *Heilongjiang Province, China*;
2. *School of Computer and Information Technology, Northeast Petroleum University, Daqing* 163318, *Heilongjiang Province, China*)

Abstract: Aiming at the problem of insufficient feature extraction resulting in low classification accuracy of the traditional encrypted traffic classification model, we proposd an encrypted traffic classification model based on an improved convolutional neural network combined with Transformer by using deep learning techniques. In order to improve the classification accuracy, firstly, we cut and filled the dataset, and completed standardization processing. Secondly, the multi-head attention mechanism in the Transformer network model was used to capture long-distance feature dependencies, and the convolutional neural network was used to extract local features. Finally, the Inception module was added to achieve multi-dimensional feature extraction and feature fusion, and the model training and encrypted traffic classification were completed. The experimental verification was conducted on the ISCX VPN-non-VPN 2016 public dataset, the experimental results show that the classification

收稿日期： 2023-06-12.

第一作者简介： 高新成(1979—)，男，汉族，博士，教授，从事网络安全、网络管理和大数据应用的研究，E-mail：gxc@nepu.edu.cn.
通信作者简介： 张 宣(1997—)，男，汉族，硕士研究生，从事网络安全和流量分类管理的研究，E-mail：dyzx@stu.nepu.edu.cn.

基金项目： 国家自然科学基金(批准号：61702093)、中国高校产学研创新基金(批准号：2021ITA02011)和黑龙江省教育科学规划重点项目(批准号：GJB1423357).

accuracy of the proposed model reaches 98.5%, with the precision rate, recall rate and F_1 value all exceeding 98.2%, which show better classification effect compared with other models.

Keywords: encrypted traffic classification; convolutional neural network; multi-head attention mechanism; feature fusion

随着加密技术在网络传输过程中的广泛应用[1],网络加密流量所占比例越来越大.而流量加密技术在保障了用户隐私安全的同时,也给恶意流量软件躲避网络安全检测带来了便利[2].因此,提升加密网络流量的分类精度,有效分离出恶意流量[3-4]已成为流量分类领域中的研究热点.基于机器学习的方法具有便于理解、计算速度快、精确率高等优点[5],但需要人工提取特征,受主观因素的影响.基于深度学习[6-7]的方法能自动提取特征,已逐步用于加密流量识别领域[8],但深度学习方法所用的分类模型存在结构复杂、网络层数深、计算开销成本高等问题[9].

针对上述问题,本文以卷积神经网络(convolutional neural network, CNN)作为基础模型进行改进,提出一种加密网络流量的分类方法.首先,针对CNN模型无法处理超长序列信息、捕获全局特征能力弱的问题,引入Transformer[10]编码多头注意力机制,将Transformer模型和CNN模型有效融合,将Transformer模型所提取的长距离特征输入到改进的CNN模型中,更全面地获取全局数据特征信息,提高其序列建模的能力.其次,针对CNN模型特征学习能力不足的问题,加入Inception机制,以不同卷积层并联的方式进行合并,实现多尺度特征提取.通过Inception模块的多个并行分支可捕捉不同级别的特征,在Inception模块中使用1×1的卷积核减少通道数,有助于缓解梯度消失的问题.同时,使用全局平均池化层和卷积层代替计算量过大的全连接层,可减少网络参数,加快计算速度,避免出现过拟合问题,从而提高模型的泛化能力.

1 相关工作

随着互联网的高速发展,各种类型的网络流量逐渐增多,传统基于端口匹配的方法已无法满足当前流量分类的需求.Moore等[11]采用基于传统端口匹配技术的效果只有约60%的准确率;Madhukar等[12]将该方法应用在P2P流量上,结果表明该方法更不适用于该类型流量;文献[13]将K-means与K近邻算法相融合,规避了基于深度包检测方法的不足;文献[14]采用了各种不同的机器学习算法,并对这些算法的优化进行研究,达到较好的分类精度;Draper-Gil等[13]使用了K近邻算法等机器学习模型,采用会话中的时序相关特征对加密流量数据进行分类研究.机器学习方法在流量分类的研究上虽取得了一定进展,但该方法无法对未知的流量进行正确分类.基于机器学习的分类方法提取严重依赖专家系统知识,分类受主观因素制约的负面影响无法规避.

基于深度学习的方法可有效避免基于机器学习方法在特征设计上的缺陷,目前已广泛应用于加密流量分类任务中.Wang等借鉴了其他领域的分类技术将其应用在流量分类中,提出了一种针对异常流量的策略[15],并进一步提出了一种基于一维卷积神经网络的方法进行加密流量分类[16].

2 本文分类方法

2.1 模型设计

本文模型设计以CNN网络为基础并融合Transformer的优点,重点改进两部分.一是通过Transformer模型提取特征,再用CNN模型对这些特征进行分类.使用Transformer模型的输出作为CNN模型的输入,将预处理过的加密流量数据集传入Transformer编码器部分,通过编码器中的多头注意力机制捕捉到数据长距离的特征依赖,并对其特征信息进行重加权操作;二是对CNN模型加入Inception模块进行改进,实现多尺度融合,使特征信息的提取更精确,保证后续的模型训练过程特征信息不丢失.

本文模型总体架构如图1所示.流程如下:首先,将原始加密流量数据经预处理作为模型输入;其次,Transformer编码器的输入由词表编码和位置编码进行求和操作,将结果输入到多头注意力层

中，再通过前馈网络进行输出，其中层之间使用层归一化操作；再次，经过一层卷积池化和拼接层中间嵌入 Inception 模块进行多层次特征提取和特征融合；最后，使用 Softmax 分类器完成分类结果输出.

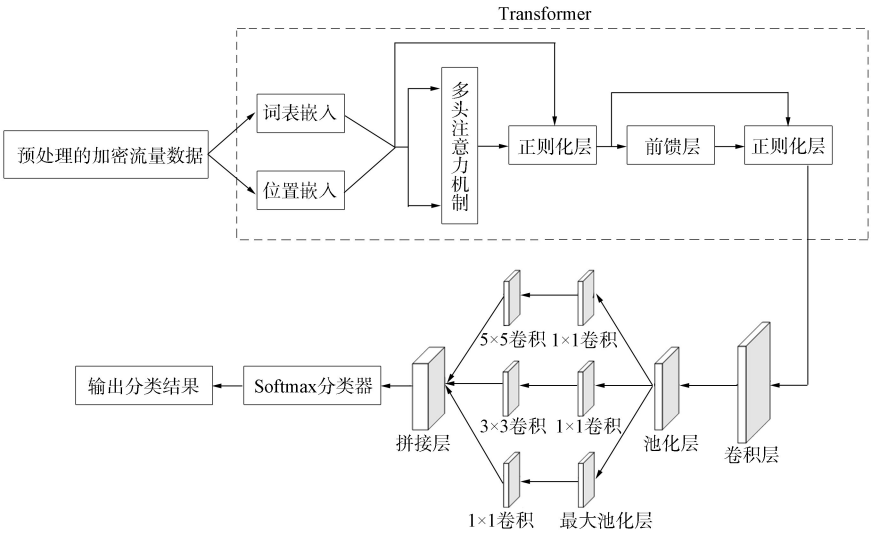


图 1　本文模型总体架构

Fig. 1　Overall architecture of proposed model

2.2　Transformer 编码器

输入数据为一个序列，使用 Transformer 模型对该序列进行编码，得到一个由 Transformer 模型输出的特征向量序列，将该序列送到 CNN 模型进行分类. 而 CNN 模型的输入需要一个固定大小的张量，因此需要将特征向量序列转化为一个张量，本文将这些特征向量取一个平均值，将它们连接在一起形成一个固定大小的张量.

Transformer 的结构包括编码器(Encoder)和解码器(Decoder)两部分，本文使用 Transformer 的编码器结构，该结构主要由多头自注意力机制和前馈神经网络组成. Transformer 编码器是一种基于注意力机制的序列模型，在处理长序列时效果更好. 模型在编码序列过程中，将注意力集中在输入序列中的其他位置上，每个位置都可以计算与其他位置的相关信息，得到一个重要性权重分布. 通过以下步骤计算位置 i 与其他位置的相关性得分.

1) 计算查询 $\boldsymbol{Q}$(Query)：将位置 i 的特征映射为查询向量 $\boldsymbol{q}_i$，用于寻找与该位置相关的信息.

2) 计算键 $\boldsymbol{K}$(Key)：将所有位置的特征映射为键向量 $\boldsymbol{k}_j$，用于表示每个位置的信息.

3) 计算值 $\boldsymbol{V}$(Value)：将所有位置的特征映射为值向量 $\boldsymbol{v}_j$，作为被查询位置 i 的信息.

4) 计算注意力权重：通过计算查询向量 $\boldsymbol{q}_i$ 与所有位置键向量 $\boldsymbol{k}_j$ 之间的内积，再进行 Softmax 操作，得到位置 i 对其他位置的注意力权重.

5) 加权求和：将所有位置的值向量 $\boldsymbol{v}_j$ 按注意力权重进行加权求和，得到位置 i 的新特征表示.

通过上述步骤，每个位置都可以根据其与其他位置的关联程度获得全局信息. 同时，Transformer 编码器采用多头注意力机制，可并行学习多个不同类型的依赖关系，进一步提高了其序列建模能力. 自注意力机制是将序列与自身进行匹配，提取内部之间的依赖关系，通过不同的线性变换对 $\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}$ 进行投影，将不同的注意力机制结果进行拼接. 自注意力机制的计算公式为

$$\mathrm{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_k}}\right), \tag{1}$$

其中 d_k 表示通道维度. 结果为注意力矩阵，其值表示了 $\boldsymbol{Q}$ 与 $\boldsymbol{K}$ 之间的关联程度.

多头注意力机制并行使用多个自注意力机制，学习不同类型数据之间相互依赖的关系：

$$\mathrm{MultiHead}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{Concat}(\mathrm{Head}_1,\mathrm{Head}_2,\cdots,\mathrm{Head}_h)\boldsymbol{W}, \tag{2}$$

$$\mathrm{Head}_i=\mathrm{Attention}(\boldsymbol{Q}\boldsymbol{W}_i^{\boldsymbol{Q}},\boldsymbol{K}\boldsymbol{W}_i^{\boldsymbol{K}},\boldsymbol{V}\boldsymbol{W}_i^{\boldsymbol{V}}), \tag{3}$$

本文选取 $h=4$，即由 4 个自注意力机制组成.

Transformer 编码器中的前馈神经网络是全连接型的，该结构涵盖了两个线性变换，其中前馈神经网络可表示为

$$\mathrm{FFN}(x)=\max\{0,xW_1+b_1\}W_2+b_2. \tag{4}$$

线性变换在不同位置需要调整不同的参数. 由于缺少位置信息，因此自注意力层的位置通常未知，考虑使用位置自注意力代替注意力机制，嵌入可学习的相对位置编码. 每个注意力头使用一个可训练的相对位置编码，其值仅取决于像素与像素之间的距离，将自注意力机制表示为

$$\mathrm{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\mathrm{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_k}}+\boldsymbol{B}\right)\boldsymbol{V}. \tag{5}$$

2.3 改进 CNN 模型

针对加密流量数据，当网络层次较浅时，传统的 CNN 模型无法提取到更深层次的特征，会导致模型的分类精度较差，网络的层次过深则会导致模型计算速度慢. 为减少参数量并解决梯度消失的问题，本文设计以 CNN 模型为基础嵌入 Inception 模块[17]，实现多尺度特征融合，Inception 模块能对尺寸较大的矩阵进行降维处理，并能进行不同尺度的特征提取.

Inception 设计思想：将不同的卷积层和最大池化层通过并联的方式连接在一起形成一个更深层的矩阵. Inception 模块可以反复堆叠形成巨大的网络结构，从而达到最简单的方式，即对网络的深度和宽度进行高效率的扩充，以提高网络性能，并避免过拟合风险. 本文采用的 Inception 模块由卷积核大小为 3×3，5×5 的卷积层和一个最大池化层组成，在该模块中以串联的方式分别对上述 3 个结构加入 1×1 的卷积层用于控制输出的特征维度，并在卷积层的后面连接批归一化层以有效增加模型的鲁棒性. Inception 模块的网络结构如图 2 所示.

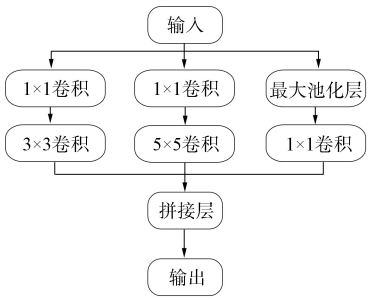


图 2 Inception 模块结构

Fig. 2 Inception module structure

在 Inception 模块中 3 个不同大小卷积核的卷积层前面添加 1×1 的卷积层，并在池化层的后面连接 1×1 的卷积层，而 1×1 的卷积无法扩大感受野效果，因此对通道数进行修改，以达到降低输出特征维度的目的. 在该模块的最后连接批归一化层，将上一层改进 Inception 模块的输出作为该层的输入，将输入数据减均值方差，使网络的超参数设定更灵活，不仅能加快网络的收敛速度，还能增加模型的鲁棒性. 令网络层输入的 x 分布接近，并且分布在(0,1)内，能提高函数的迭代优化效果，通过数据的标准化处理将输入数据 x 映射为 $\hat{x}_i$，并对每个 Batch 进行规范化处理：

$$\hat{\chi}_i\leftarrow\frac{x_i-\mu_B}{\sqrt{\sigma_B^2+\varepsilon}}, \tag{6}$$

$$\hat{\mu}_B=\frac{1}{|B|}\sum_{x\in B}x, \tag{7}$$

$$\hat{\sigma}_B^2=\frac{1}{|B|}\sum_{x\in B}(x-\hat{\mu}_B)^2+\varepsilon, \tag{8}$$

其中：$\hat{\mu}_B$ 表示平均值；$\hat{\sigma}_B^2$ 表示方差；常量 $\varepsilon>0$，确保分母不为 0，保证了在经验方差估计值可能消失的状态下也不会出现分母为 0 的情况.

3 实验及结果分析

实验设备为 Gen Interl(R) Core(TM) i7-12700H 处理器，32 GB 内存，NVIDIA GeForce RTX3050(8 GB)显卡，编程语言为 Python 3.9，实验模型训练库为 Pytorch 1.11.0.

3.1 数据集

本文实验采用 UNB ISCX VPN-nonVPN 2016 公开加密流量数据集，该数据集由 15 种非 VPN 和

VNP 加密流量，将其划分为 12 个类别并取对应标识名，涵盖 6 种常规加密流量和 6 种 VPN 加密流量，数据集信息列于表 1.

表 1　数据集信息

Table 1　Information of dataset

流量类型	应用名称	流量类型	应用名称
Chat	ICQ,AIM,Skype	VPN-Chat	Facebook,Hangouts
Email	Email,Gmain	VPN-Email	(SMPT,POP3,IMAP)
File	Ftps,Sftp,Skype	VPN-File	Ftps,Sftp,Skype
Streaming	Vimeo,Netfix	VPN-Streaming	Spotify,YouTube
Voip	Facebook,Hangouts	VPN-VoIP	Skype,Voipbuster
P2P	uTorrent,Bittorrent	VPN-P2P	uTorrent,Bittorrent

3.2　数据集处理

本文实验在进行分类任务前，需对数据集进行预处理获得标准数据集，数据集处理流程如图 3 所示. 先将 15 种类别的数据集合并成 12 种类别，并将 pacapng 格式文件转换成 pcap 文件以便于后续操作；然后完成数据集中与流量特征无关的域名服务段(DNS)，与分类任务无关的以太网头 MAC 地址以及填充字段(Padding)清除工作，以提升数据分类处理效率；最后完成数据切割和标准化处理.

图 3　数据集处理流程

Fig. 3　Processing flow of dataset

分析数据集中各种类型的数据长占比，结果列于表 2. 由表 2 可见，97.7%的数据长度均在 1 500 B 以下，仅 358 条(2.3%)数据长度大于 1 500 B. 将数据长度定为 1 500 B，并将数据长度大于 1 500 B的数据进行截取，数据长度小于 1 500 B 的数据将其末尾填充 0，最后将数据转换为标准大小的流量矩阵.

表 2　数据长度区间占比

Table 2　Proportion of data length intervals

数据长度/B	0～200	201～1 200	1 201～1 500	1 500 以上
条数/k	13 378	420	6 497	358
占比/%	64.8	2.0	30.9	2.3

3.3　评估指标

本文使用的数据集属于类别不平衡的数据集，为验证本文改进的 CNN-Transformer 模型分类性能，使用准确率(Accuracy)、精确率(Precision)、召回率(Recall)和 F_1-Score 四个指标完成分类模型性能评估. 各评价指标计算公式分别为

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

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

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

$$F_1\text{-Score}=\frac{2\times\text{Precsion}\times\text{Recall}}{\text{Precision}+\text{Recall}},\tag{12}$$

其中 TP 真阳表示预测为正例的正例，TN 真阴表示预测为负例的负例，FP 假阳表示预测为正例的负例，FN 假阴表示预测为负例的正例.

3.4 实验结果分析

3.4.1 消融实验

1) Transformer 编码器验证. 为验证本文分类模型融入 Transformer 编码器的有效性，实验通过改变不同数量的多头注意力机制对 Transformer 解码器结构进行对比，实验结果列于表 3. 表 3 中 Initial-model 为未添加 Transformer 编码器，2-Transformer,4-Transformer,6-Transformer 中的自注意力层的个数分别为 2,4,6.

表 3 不同头数 Transformer 模型结果对比

Table 3 Comparison results of Transformer model with different number of heads

模型	Accuracy	Precison	Recall	F_1-Score
Initial-model	0.912 4	0.905 1	0.892 1	0.894 7
2-Transformer	0.937 5	0.917 0	0.903 4	0.908 5
4-Transformer	0.964 0	0.943 2	0.952 1	0.946 6
6-Transformer	0.964 7	0.945 6	0.958 0	0.948 0

由表 3 可见，未添加 Transformer 编码器的分类模型各评估指标均为最低. 在加入多头注意力机制后，头数为 4 以内时的各指标均增长，当头数为 4,6 时，评估指标基本一致，而头数为 6 时，参数量的增多会导致训练时间大幅度增加. 可见，Transformer 编码器结构能有效解决 CNN 捕获全局能力弱的问题，提高了模型的分类性能.

2) Inception 模块验证. 为验证 CNN 网络中加入 Inception 模块的有效性，本文针对 Inception 模块结构进行对比实验，实验结果列于表 4. 表 4 中 Initial-model 的结构未添加 Inception 模块，1-CNN 加入了 Inpection 模块，且 Inception 的内部结构由 3×3 卷积并联组成，2-CNN 的 Inception 内部结构由 3×3+5×5 卷积并联组成，3-CNN 的 Inception 内部结构是以 3-CNN 的结构为基础添加了最大池化层，在两个卷积和最大池化层前后分别连接 1×1 卷积层控制输出的特征维度.

表 4 不同结构 CNN 分类结果对比

Table 4 Comparison of classification results of different structural CNN

模型	Accuracy	Precison	Recall	F_1-Score
Initial-model	0.948 5	0.928 0	0.907 5	0.915 5
1-CNN	0.955 0	0.934 3	0.937 8	0.936 6
2-CNN	0.968 0	0.938 9	0.932 1	0.941 3
3-CNN	0.973 3	0.950 4	0.944 5	0.953 5

由表 4 可见，Initial-model 的各项性能指标相比其他 3 种模型均有不足，其中 3-CNN 的性能提高最明显. Accuracy,Precision,Recall 和 F_1-Score 四个性能指标与未添加 Inception 模块的 CNN 相比分别提高了 2.48,2.24,3.70,3.80 个百分点. 可见，对 CNN 网络添加 Inception 模块能达到更高的分类精度.

3.4.2 与主流分类模型对比

为验证本文分类模型的优越性，将本文模型与 1D-CNN,2D-CNN 和 GAN+CNN 三个常见的分类模型进行对比. 本文模型在数据集 ISCX 上进行服务类型 12 种分类的准确率与其他 3 个常见的深度学习模型对比实验结果列于表 5.

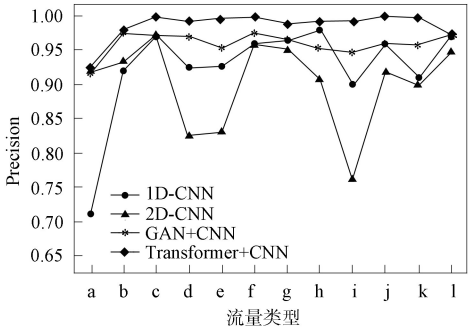
表 5 不同模型在数据集 ISCX 上的准确率对比

Table 5 Comparison of accuracy of different models on ISCX dataset

分类模型	Accuracy/%	分类模型	Accuracy/%
1D-CNN	95.5	GAN+CNN	96.3
2D-CNN	92.3	CNN-Transformer	98.5

由表 5 可见，同样对服务类型的流量进行流量分类任务，本文模型相比 1D-CNN,2D-CNN 和 GAN+CNN 三个模型，总体准确率分别提升了 3.0,6.2,2.2 个百分点，因此本文模型优于其他 3 个常见分类模型的分类准确率.

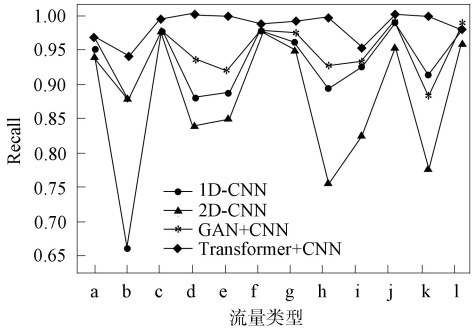
下面通过对比 12 种类别在不同模型上的性能指标数值对本文模型分类性能进行全面评估. 图 4～图 6 分别为本文模型与其他 3 个模型的性能指标对比分析结果.



a. Chat; b. Email; c. File; d. P2P; e. Streaming; f. Voip; g. VNP_Chat; h. VPN_Email; i. VPN_File; j. VPN_P2P; k. VPN_Streaming; l. VNP_Voip.

图 4　不同模型在各类别上的准确率

Fig. 4　Accuracy of different models on each category

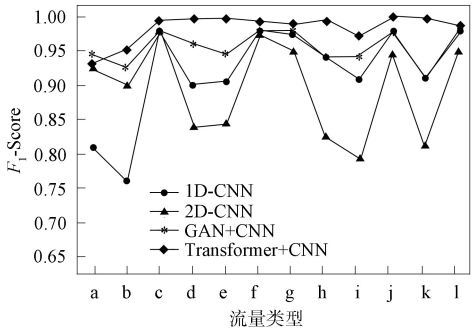


a. Chat; b. Email; c. File; d. P2P; e. Streaming; f. Voip; g. VNP_Chat; h. VPN_Email; i. VPN_File; j. VPN_P2P; k. VPN_Streaming; l. VNP_Voip.

图 5　不同模型在各类别上的召回率

Fig. 5　Recall rate of different models on each category

由图 4 可见，本文模型的精确率远高于其他 3 个分类模型，File，P2P，Streaming 等 9 种类别的准确率均达 99％以上. 由图 5 可见，本文模型在 P2P 和 VPN_P2P 上的召回率达 100％，在 File，Streaming 等 9 种类别上的召回率均达 98％以上. 由图 6 可见，本文模型在 File，P2P，Streaming 等 9 种类别的 F_1 值均达 98％以上. 实验结果表明，本文模型与主流加密流量分类方法相比分类性能优异，且本文所有实验是在不平衡数据集上完成的，若对数据集进行平衡化处理，实验效果会更显著.



a. Chat; b. Email; c. File; d. P2P; e. Streaming; f. Voip; g. VNP_Chat; h. VPN_Email; i. VPN_File; j. VPN_P2P; k. VPN_Streaming; l. VNP_Voip.

图 6　不同模型在各类别上的 F_1 值

Fig. 6　F_1 values of different models on each category

综上所述，针对现有加密流量分类方法存在特征提取效果较差的问题，本文考虑以 CNN 网络为基础模型，引入 Transformer 编码器多头注意力机制和 Inception 思想，提出了一种改进 CNN 和 Transformer 相结合的加密流量分类模型. 该模型既发挥了 CNN 捕获局部特征的优势，使用 Inception 模块实现多尺度融合特征，又充分利用了 Transformer 善于捕捉长距离的特征依赖，两种网络相结合达到长短兼顾的分类效果. 通过与 1D-CNN，2D-CNN 和 GAN＋CNN 等分类模型进行对比验证，实验结果表明，本文分类方法能有效提高数据整体的分类精度.

参　考　文　献

[1] GUO L L, WU Q Q, LIU S L, et al. Deep Learning-Based Real-Time VPN Encrypted Traffic Identification Methods [J]. Journal of Real-Time Image Processing, 2020, 17(9): 1-12.

[2] 沈记全，魏坤. 融合残差网络的 CR-BiGRU 入侵检测模型 [J]. 吉林大学学报(理学版)，2023，61(2)：353-361. (SHEN J Q, WEI K. CR-BiGRU Intrusion Detection Model by Fusing Residual Networks [J]. Journal of Jilin University (Science Edition), 2023, 61(2): 353-361.)

[3] 张志宏，刘传领. 基于灰狼算法优化深度学习网络的网络流量预测 [J]. 吉林大学学报(理学版)，2021，59(3)：619-626. (ZHANG Z H, LIU C L. Optimization of Deep Learning Network for Network Traffic Prediction Based on Gray Wolf Algorithm [J]. Journal of Jilin University (Science Edition), 2021, 59(3): 619-626.)

[4] 闫伟，张军. 基于时间序列分析的网络流量异常检测 [J]. 吉林大学学报(理学版)，2017，55(5)：1249-1254. (YAN W, ZHANG J. Network Traffic Anomaly Detection Based on Time Series Analysis [J]. Journal of Jilin

University (Science Edition), 2017, 55(5): 1249-1254.)

[5] 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.

[6] 高新成, 李强, 王莉利, 等. 基于改进遗传算法的自适应卷积神经网络 [J]. 计算机技术与发展, 2022, 32(10): 132-136. (GAO X C, LI Q, WANG L L, et al. Adaptive Convolutional Neural Network Based on Improved Genetic Algorithm [J]. Computer Technology and Development, 2022, 32(10): 132-136.)

[7] XUE B, YI W J, JING F, et al. Complex ISAR Target Recognition Using Deep Adaptive Learning [J]. Engineering Applications of Artificial Intelligence, 2021, 97: 104025-1-104025-9.

[8] 曾宏志, 史洪松. 半监督技术和主动学习相结合的网络入侵检测方法 [J]. 吉林大学学报(理学版), 2021, 59(4): 936-942. (ZENG H Z, SHI H S. Network Instrusion Detection Method Combining Semi-supervised Technology and Active Learning [J]. Journal of Jilin University (Science Edition), 2021, 59(4): 936-942.)

[9] 邓昕, 刘朝晖, 欧阳燕, 等. 基于 CNN CBAM-BiGRU Attention 的加密恶意流量识别 [J]. 计算机工程, 2023, 49(11): 178-186. (DENG X, LIU C H, OUYANG Y, et al. Encrypted Malicious Traffic Recognition Based on CNN CBAM-BiGRU Attention [J]. Computer Engineering, 2023, 49(11): 178-186.)

[10] VASWANI A, SHAZEER N, PARMAR N, et al. Attention Is All You Need [C]//International Conference on Neural Infromation Processing Systems. New York: ACM, 2017: 6000-6010.

[11] MOORE A W, PAPAGIANNAKI K. Toward the Accurate Identification of Network Applications [C]// International Workshop on Passive and Active Network Measurement. Berlin: Springer, 2005: 41-54.

[12] MADHUKAR A, WILLIAMSON C. A Longitudinal Study of P2P Traffic Classification [C]//14th IEEE International Symposium on Modeling, Analysis, and Simulation. Piscataway, NJ: IEEE, 2006: 179-188.

[13] DRAPER-GIL G, LASHKARI A H, MAMUN M S I, et al. Characterization of Encrypted and VPN Traffic Using Yime-Related [C]//Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP). New York: ACM, 2016: 407-414.

[14] 连晓伟, 马垚, 陈永乐, 等. 基于载荷特征与统计特征的 Shodan 流量识别 [J]. 计算机工程, 2021, 47(1): 117-122. (LIAN X W, MA Y, CHEN Y L, et al. Identification of Shodan Traffic Based on Load Characteristics and Statistical Characteristics [J]. Computer Engineering, 2021, 47(1): 117-122.)

[15] WANG W, ZHU M, ZENG X W, et al. Malware Traffic Classification Using Convolutional Neural Network for Representation Learning [C]//2017 International Conference on Information Networking (ICOIN). Piscataway, NJ: IEEE, 2017: 712-717.

[16] WANG W, ZHU M, WANG J L, et al. End-to-End Encrypted Traffic Classification with One-Dimensional Convolution Neural Networks [C]//2017 IEEE International Conference on Intelligence and Security Informatics. Piscataway, NJ: IEEE, 2017: 43-48.

[17] 孙懿, 高见, 顾益军. 融合一维 Inception 结构与 ViT 的恶意加密流量检测 [J]. 计算机工程, 2023, 49(1): 154-162. (SUN Y, GAO J, GU Y J. Fusion of One-Dimensional Inception Structure and ViT for Malicious Encrypted Traffic Detection [J]. Computer Engineering, 2023, 49(1): 154-162.)

(责任编辑: 韩 啸)