山西大学学报(自然科学版)48(3):481—491,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2023116

基于注意力的多特征融合加密流量识别方法

孙文茜,翟江涛*,刘光杰,许成程
(南京信息工程大学 电子与信息工程学院,江苏 南京 210044)

摘　要:针对当前加密流量识别研究中因神经网络架构导致特征信息提取不充分的问题,本文提出了一种基于注意力的多特征融合加密流量识别方法。所提方法聚焦于加密流量的层次结构特点,设计了两个并行的网络分支进行特征提取,分支一采用残差神经网络(Residual Neural Network, ResNet)提取流量的原始特征,分支二利用不规则大小卷积核组成的Inception-CNN(Convolutional Neural Networks)提取流的统计特征进行表征以补偿流量裁剪带来的信息损失。此外,本文将统计特征由现有的灰度图转换成RGBA图像的形式作为输入来帮助模型更有效地提取特征。两个分支提取到的特征被合并为新的特征向量输入到通道注意力模块中进行加权,以增强流量特征的表征能力。实验结果表明,该模型较现有典型的加密流量分类方法具有更好的表现,精度、召回率和*F*1-score均有明显提高,其中综合性能指标*F*1-score较现有方法平均提高了6%。

关键词:加密流量;残差神经网络;特征融合;流量识别
中图分类号:TP309　　**文献标志码**:A　　**文章编号**:0253-2395(2025)03-0481-11

Attention-based Multi Feature Fusion Encrypted Traffic Recognition Method

SUN Wenqian, ZHAI Jiangtao*, LIU Guangjie, XU Chengcheng
(*School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing* 210044*, China*)

Abstract: To address the issue of insufficient feature information extraction caused by neural network architecture in current encrypted traffic recognition research, this paper proposes a multi-feature fusion encrypted traffic recognition method based on attention mechanism. The proposed method focuses on the hierarchical structure characteristics of encrypted traffic and designs two parallel network branches for feature extraction. Branch one uses residual neural network(ResNet) to extract the original features of traffic, while branch two uses an Inception-CNN composed of irregular-sized convolution kernels to extract statistical features of traffic for characterization and compensate for the information loss caused by traffic cropping. In addition, this paper converts the statistical features from the existing grayscale image to the RGBA image format as input to help the model more effectively extract features. The features extracted by the two branches are merged into a new feature vector and input into the channel attention module for weighting to enhance the representation ability of traffic features. The experimental results show that the proposed model performs better than existing typical encrypted traffic classification methods, with significantly improved accuracy, recall rate, and *F*1-score, among which the comprehensive performance metric *F*1-score is increased by an average of 6% compared to existing methods.

Key words: encrypted traffic; residual neural network; feature fusion; traffic identification

收稿日期:2023-04-05;**接受日期**:2023-06-21
基金项目:国家自然科学基金(61931004;62072250);国家重点研发计划(2021QY0700)
作者简介:孙文茜(1999—),女,江苏连云港人,硕士研究生,研究方向为多媒体与信息安全。E-mail:1421626314@qq.com
* **通信作者**:翟江涛(ZHAI Jiangtao),E-mail:jiangtaozhai@nuist.edu.cn
引文格式:孙文茜,翟江涛,刘光杰,等.基于注意力的多特征融合加密流量识别方法[J].山西大学学报(自然科学版),2025,48(3):481-491. DOI:10.13451/j.sxu.ns.2023116.

0 引言

随着互联网的快速发展,来自不同应用的网络流量迅速增加。而对网络流量进行有效地监测和识别,以提高网络的服务质量[1]、加强网络的管理以及保障数据的安全性[2]显得十分重要。识别流量最快速、最简单的方法是使用端口号[3]。在早期发展中,每一个网络应用都会被指定固定的端口号。例如,安全套接层(Secure Sockets Layer,SSL)协议相关应用使用80端口,远程终端协议(Terminal Network,TELNET)相关应用使用23端口等。但是,随着技术的不断发展,该方法不能适用于非标准端口或新定义的端口,动态端口技术的出现导致基于端口的流量识别方法准确率开始下降[4],深度包检测技术(Deep Packet Inspection,DPI)应运而生[5],DPI使用预定义的模式来检查数据包应用层中的有效负载。近年来,越来越多的应用程序在传输数据时使用加密通信,给上述两种传统的流量分类方法带来了极大挑战。为此,专家们开始在加密流量分类任务上使用机器学习和深度学习的方法。根据不同的输入数据,研究可以分为两类:基于统计特征的方法和基于原始流量的方法。具体而言,基于统计方法的基本思想是不同类型的应用会产生不同的流量特征。基于原始流量的方法是使用卷积神经网络从原始流量中自动提取并学习特征。然而,基于统计特征方法的分类性能很大程度上取决于特征的质量,基于原始流量方法的主要缺点是数据预处理过程中的文件裁剪操作会导致信息丢失。为解决上述问题,本文提出了一种基于注意力的多特征融合加密流量识别方法,有效弥补原始流量信息损失的同时提升了分类性能。

1 相关工作

基于统计特征的流量分类方法是假设不同类型流量的统计特征是唯一的。Moore等[6]首先针对几种不同的网络流量类型提取了200多种统计特征,然后使用了多种机器学习分类器对实验方法做出评估,证明了基于统计特征方法的有效性。之后的专家研究内容大都基于这个思路,主要包含两方面,一是对网络流量特征集的设计与挑选,二是对流量分类算法的选择与优化。Taylor等[7]利用数据包长度序列来表示网络流量,并结合机器学习方法,可以实现较好的流量识别效果;Cao等[8]从模糊化方向考虑了流和包两种级别的数据,并从中挑选出流量的34个相关统计特征,这种方法虽然可以弥补模糊化带来的不足,但是这些特征是在特定网络场景下总结规律得到的,扩展性相对较低。虽然当前已经提出了很多种统计特征,但是部分特征对于流量分类的贡献并不明显,且基于统计特征的方法需要研究者掌握丰富的经验来挑选特征,会花费不少的时间和精力。为了弥补统计方法的不足,专家们开始尝试将深度学习的知识应用到流量分类领域,使用神经网络自动从原始流量中学习特征。Wang等[9-10]首先提出将原始流量字节转换为灰度图的形式,然后使用卷积神经网络提取原始流量特征从而对加密流量进行分类,该方法避免了人工提取统计特征,不需要掌握专业的知识就可以对流量进行分类。基于这个思路,各种基于深度学习的流量分类方法开始涌现。Lotfollahi等[11]开发了“Deep Packet”框架,这个框架使用了两种模型:卷积神经网络和堆叠式自编码器,其中,堆叠式自编码器将流量分类为主要类别,卷积神经网络用于检测流量的应用类型,这种方法有效证明了卷积神经网络在流量分类研究中的可行性;He等[12]则针对特征选择方面对流量分类方法进行改进,该方法只提取了会话的前几个有效载荷字节,并将其转换为灰度图的形式输入到模型中,从而实现了对流量更快速、更方便地分类。为了充分利用数据包之间的关系,Huoh等[13]提出结合流量的原始字节和元特征,并将其作为图神经网络(Graph Neural Network,GNN)的输入,在加密网络流量分类方面表现出了优越性。针对传统单模态方法特征信息提取不充分的问题,Lin等[14]提出了一种多模态训练框架。该框架利用统计特征和流量负载去学习加密流量中的隐藏信息,通过将两者的优势相结合,可以达到较好的分类效果。Izadi等[15]则提出了将深度学习和数据融合技术结合的流量分类方法,该方法由卷积神经网络(Convolutional Neural Net-

works,CNN)、深度信念网络(Deep Belief Network,DBN)和多层感知机(Multi-Layer Perception,MLP)模型组成,通过提取和合成异构多模态输入中的信息来提高模型性能。然而其中大多数神经网络要求其输入是固定尺寸,因此首先要对原始加密流量进行统一,这将导致部分文件的信息丢失,尤其是有关网络流量整体结构的信息,这将对分类性能造成影响。

综上所述,在关于加密流量分类的研究中,基于统计的方法虽然可以获得较高的精度,但也存在明显的不足。其分类性能很大程度上取决于特征的质量,并且需要花费大量的人力和时间对特征进行设计。同时,研究者们需要针对不同类型的分类任务单独设计网络流量特征合集,代价较高。而基于原始流量的方法大都限制流量文件的大小而导致信息丢失。

基于上述问题,本文提出了一种基于注意力的多特征融合加密流量分类模型,有效解决了特征提取过程中的信息损失问题,本文的主要贡献包括如下:

(1)本文设计了一种双分支并行架构,即分别使用残差神经网络(Residual Neural Network,ResNet)和Inception-CNN提取流量原始特征及统计特征,最后将两个通道提取到的特征融合成新的流量特征向量,使模型可以通过更丰富的特征获取输入与输出之间的非线性关系。

(2)本文提出提取网络流的前$m\times m$个数据包中的四个特征(大小、到达时间、协议、方向)并表示成基于RGBA图像形式,克服了原有基于灰度图方法无法充分利用数据包长度特征的问题。

(3)本文方法在公共数据集"ISCX VPN-nonVPN"[16]和"ISCX Tor-nonTor"[17]上与六种经典模型和四种主流算法作出比较。实验结果表明,本文所提方法在加密流量分类上的表现优于现有方法。

2 本文方法

近年来,深度学习在加密流量分类方面的应用已成为研究热点。然而,深度神经网络需要一个固定大小的输入,因此原始流量数据需要处理成尺寸一致的流量图像,但是这会引起部分流量信息的丢失。此外,流量的结构信息也会因进行裁剪和填充操作导致丢失,例如我们将无法确定会话中数据包的个数以及会话的持续时间。

为解决上述问题,本文提出了一种基于ResNet[18]与Inception-CNN[19]的加密流量分类方法。该方法使用ResNet从原始网络流量中提取特征,并使用Inception-CNN对流量的统计特征进行学习以弥补ResNet因数据修剪造成的信息损失。统计特征是由网络流中的前$m\times m$个数据包中的四个特征(大小、到达时间、协议、方向)表示成的RGBA图像。因为结合了原始流量信息,所以不需要针对不同的任务单独设计特征集。ResNet和Inception-CNN中的输出特征将被合并为新的特征向量。最后,将这些新的特征向量输入通道注意力模块进行加权然后实现对加密流量的分类。该分类方法的网络结构如图1所示。

2.1 Inception-CNN学习统计特征

在实验中,网络流的前$m\times m$个数据包中的四个特征(大小、到达时间、协议、方向)被转化为四通道的RGBA彩色图像作为输入,这样可以更全面地展现网络流中的各种特征和变化。例如,用户数据报协议(User Datagram Protocol,UDP)和传输控制协议(TransmissionControl Protocol,TCP)等协议在传输数据时伴随的时间、大小等特征信息会有所不同,通过图像化表征这些差异,可以有效地反映出数据包的特征信息,同时也能够直观地展现数据包之间的时空关系,充分利用各个特征之间的关联性,从而提取更丰富的特征。我们也可以更好地对不同类型的加密流量进行分析和识别。其次,图像中每个像素都代表了一定的信息,RGBA图像能够捕捉到数据流中的每一个细节,从而提高模型分类的精度和可靠性。

为了更好地学习流量图像的特征,本文在CNN模型中引入了Inception模块,以多尺度特征融合的方式提取更丰富的特征。所设计的模块由1×1卷积层、3×3卷积层、5×5卷积层、最大池化层和拼接层组成,结构如图2所示。它们以不同的感受野提取到不同级别的特征,这

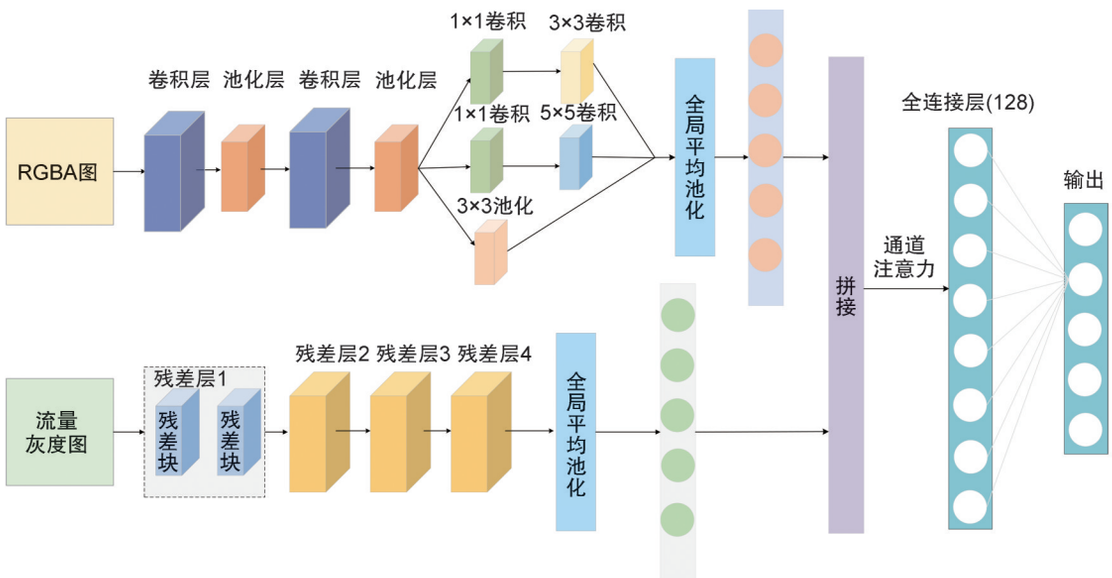

图1 本文所提双通道分类模型网络结构

Fig. 1 Network structure of the dual channel classification model proposed in this paper

种方式可以增强模型对于输入数据的表征能力,进而提高分类准确度。

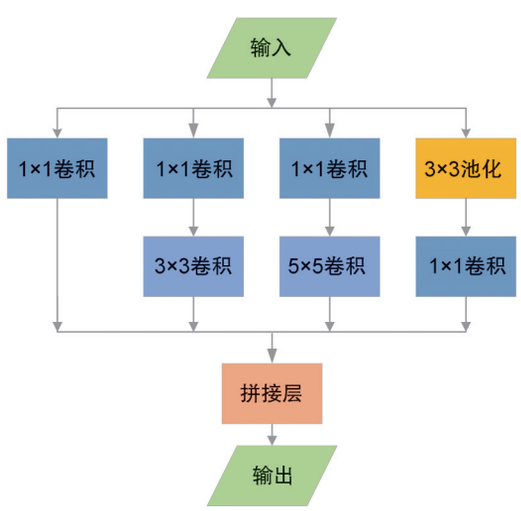

图2 Inception模块结构图

Fig. 2 Structural diagram of Inception module

通过引入Inception模块,模型可以在不增加深度的情况下扩大网络的宽度,提取更丰富的特征以弥补传统神经网络模型在特征提取方面的不足。为了处理因网络宽度扩大而带来的维度增加问题,在Inception模块中的池化层后面以及卷积层前面添加了1×1卷积层,用于缩减Inception模块输出特征的维度,从而降低模型的复杂度。

使用不同尺度的卷积核对流量图像进行处理可以得到不同尺度的特征图,这样可在获得卷积核感受视野内相邻像素的关系时,还可以学习到网络流内部不同大小数据包的特征。这些特征被提取后进行多尺度聚合,能够让网络模型学习到更丰富的特征。

在Inception模块中,卷积层后面连接了批量归一化层(Batch Normalization,BN),该层能够对每个输入批次进行归一化操作,为输入中每个特征计算均值和标准差。即对每个特征进行标准化处理,使得特征分布符合均值为0,方差为1的标准正态分布,可以消除不同数据分布对网络带来的不良影响,如网络泛化能力和训练速度下降等问题。BN的计算如公式1所示。

$$X_{ij}=\gamma_{ij}\frac{H_{ij}^{k}-\mu_{ij}}{\sigma_{ij}}+\beta_{ij}, \tag{1}$$

其中H_{ij}^{k}是训练第k条数据时,第j层的第i神经元模型的输出值;μ_{ij}、σ_{ij}分别是均值和方差;σ_{ij}、β_{ij}是两个学习参数,可以将数据从标准化空间映射回原始的特征空间。

2.2 ResNet学习原始特征

自从AlexNet网络[20]在图像分类比赛中取得突破性成果之后,卷积神经网络的发展趋势就是层级的不断加深和扩展,但卷积神经网络在层数逐渐增加时,会产生退化的现象,分类模型的参数量和计算量也随之增大,极大地降低了网络的收敛效果。为优化卷积神经网络因

层级不断累加而引起的退化问题,文献[21]提出了残差神经网络(ResNet)。它的新增网络层不再是盲目地参照原有的低级网络,而是通过模型来拟合残差映射。残差神经网络新增的快捷连接(Shortcut Connections)使得在网络浅层提取到的特征信息不仅可以传递到直接相连的层,还可以跨越中间的层级,以更直接的方式传输到深层网络中。此外,这些新增的连接方式并不会增加多余的参数量,也不会增大模型的计算复杂度。这样在保护数据信息完整度的同时,也降低了模型训练的复杂度。残差块的结构图如图3所示。

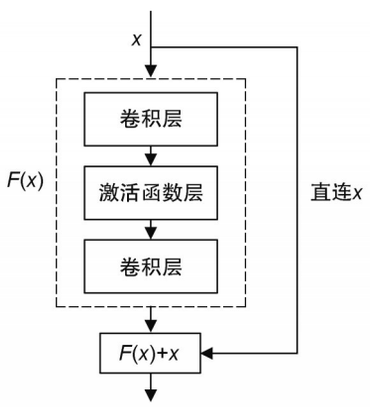

图3 残差结构图

Fig. 3 Structural diagramof residual

在神经网络中,池化层的目的主要是为了减少参数和计算量,提高模型分类效率,防止过拟合。但在本加密流量识别实验中,经过处理后的流量数据并不大。并且由于本文中经数据预处理生成的流量特征图像来源于网络流量数据,与计算机视觉领域丰富的图像细节纹理特征不同,过多的池化层会引起其特征维度下降,导致丢失较多关键的特征信息,无法准确描述网络流量的行为特征,进而影响模型识别准确率。经实验验证,使用去除池化层的神经网络模型,原始流量可以保留更多有用的信息来帮助模型做出判断,从而提升识别性能。此外,Wang等[9]的实验还有效验证了在流量分类中,使用1D-CNN会比使用2D-CNN的分类效果要更好。这是因为原始流量在结构上可以看成是序列,它的结构与本文形式相似,所以可以采用适用于处理文本的一维卷积网络来对原始流量进行特征提取。因此对于原始流量提取模块,我们使用了去除池化层的一维ResNet模型。

本文网络流量识别模型中的ResNet参层共18层,模型结构和各层参数如表1所示。

表1 ResNet-18模型结构

Table 1 Structure of ResNet-18 model

层级	过滤窗口	输入	输出
1	1×3,32	1×784	32×784
2−5	{(1×3,32),(1×3,32)}×2	32×784	32×784
6−9	{(1×3,64),(1×3,64)}×2	32×784	64×364
10−13	{(1×3,128),(1×3,128)}×2	64×364	128×182
14−17	{(1×3,256),(1×3,256)}×2	128×182	256×91
18	自适应平均池化层	256×91	256×1

2.3 注意力机制模块

注意力机制是一种被广泛应用于计算机视觉[22]以及自然语言处理领域的技术,它可以帮助模型学习更关键的信息,提升分类准确率。本文将流量数据转换为用原始流量生成的灰度图像和用统计特征生成的RGBA图像,使用ResNet和Inception-CNN对它们分别进行特征提取、融合,然后对新生成的融合特征进行分类,参照注意力机制在其他领域分类上的应用,本文通过引入注意力机制模块可以对融合后的特征向量赋予相应的权重,帮助模型从中获取到更关键、更有利于分类的特征,同时忽略一些无关的冗余特征。

通道注意力模块的作用是关注特征图不同通道的重要程度,并对更重要的通道赋予更高的权重。如图4所示,该模块将经过卷积池化操作得到的特征图作为输入,并通过全局平均池化层(Global Average Pooling,GAP)和全局最大池化层(Global Max Pooling,GMP)并行地对空间维度进行压缩,得到两个$C\times1\times1$的特征向量(其中C为输入特征图的通道数)。这两个特征向量被输入一个共享的多层感知器MLP中,该MLP由两个全连接层构成,其神经元个数分别为$C/8$,C,用于通道的降维和增维,以拟合通道间的相关性。最后将两个输出相加并进行sigmoid激活操作,得到维度为$C\times1\times1$的通道权值向量,通道权值向量再与原始输入特征图相乘,从而对不同的通道赋予对应的权重。通道权值向量的计算公式如式(2)所示:

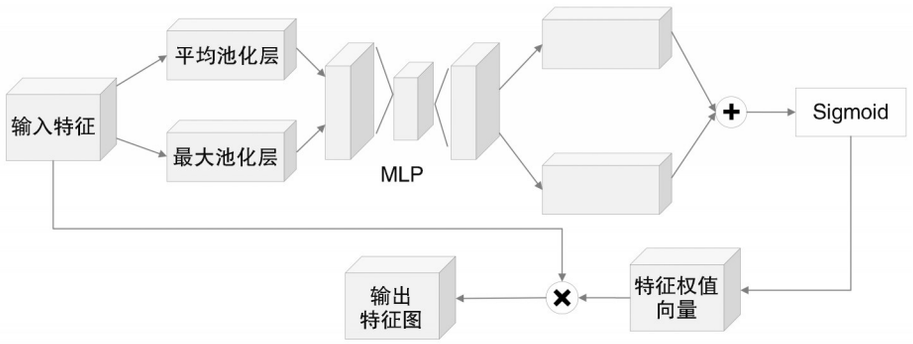

图4 通道注意力模块

Fig. 4 Channel Attention Module

$$M_c(F)=\sigma(\mathrm{MLP}(\mathrm{GAP}(F)+\mathrm{MLP}(\mathrm{GMP}(F))))。\quad(2)$$

3 实验结果与分析

3.1 实验环境

本文实验的主机配置:操作系统为64位Windows10操作系统,CPU为Intel core i7-9700H/ 3.00 GHz,32 GB内存,开发环境为Python3.10.2,所有实验均使用PyTorch完成。本文在训练神经网络时,选择将交叉熵损失函数来作为衡量加密流量分类模型性能的指标,其输出是介于0和1之间的概率值,定义如公式3所示:

$$H(y,p)=-\sum_{i}^{M}y_i\log(P_i),\quad(3)$$

其中M为类别的总数,P_i表示每个类别的概率。

本文随机抽取了90%的数据作为训练集,剩下的作为测试集。本文采用小批量梯度下降法,大小设置为128,学习速率为0.001,训练回合数为100 epochs。

3.2 评价标准

在本实验中我们使用了四个指标来评价流量分类模型的性能,分别为:准确率、精度、召回率和$F1$-Score。在多分类问题中,我们使用准确率来评价分类方法的整体性能,使用精度和召回率来评价实验在各个类型中的分类效率,$F1$值用来反映整体指标性能。混淆矩阵的定义如表2所示,我们假设此时对于预测值和实际值只有两个输出,即Positive和Negative。

有了混淆矩阵之后,我们可以给出准确率、精度、召回率和$F1$-score这四个指标的计算方式,如公式(4)—公式(7)所示:

表2 混淆矩阵定义

Table 2 Definition of confusion matrix

输出	Positive	Negative
Positive	TP	FP
Negative	FN	TN

准确率Acc(Accuracy):表示被正确分类的流量数量与整个测试集数量之比,如式(4)所示:

$$Acc=\frac{TP+TN}{TP+TN+FP+FN}。\quad(4)$$

精度P(Precision):表示被正确分类为某一类型的流量的数量与被归为这个类型的所有流量样本数量之比,如式(5)所示:

$$P=\frac{TP}{TP+FP}。\quad(5)$$

召回率R(Recall):表示被正确分类为某一流量类型的流量数量与所有真实属于此类流量样本数量之比,如式(6):

$$R=\frac{TP}{TP+FN}。\quad(6)$$

$F1$-score:$F1$分数用于同时测量精度和召回率,它可看作为模型精度和召回率的调和平均,如式(7):

$$F1=\frac{2\times R\times P}{R+P}。\quad(7)$$

3.3 实验数据集

在目前已公开的流量数据集中,涉及加密识别方面的数据相对较少。“ISCX VPN-nonVPN”数据集是当前研究加密流量领域常用的数据集,是由Draper-Gil等在2016年提出的[16],其中包括7种常规加密流量和7种虚拟专用网络(Virtual Private Network,VPN)隧道传输流量。但是作者对于该数据集只是做出了简

单介绍,并没有给出这些数据的对应标签,这就造成一些流量所属类型出现模糊不清的情况。对于Browsing以及VPN-Browsing两类流量,例如Facebook_video既可划分为Browsing,也可划分为Streaming。因此,本文选择将类模糊的流量进行删除。最终,本文实验选择其中6种常规加密流量和6种VPN隧道传输加密流量作为训练和测试的样本。此外,为了充分验证本文方法的可行性,实验还使用了“ISCX Tor-nonTor”数据集,该数据集是由University of New Brunswick(UNB)发布的,涵盖了来自十几种应用(facebook,skype等)的8种类别加密网络流量。在这两个公开的数据集中,主要包括两种可提取的数据特征,分别为流量的统计特征和原始网络流量,原始网络流量即原始的pcapng和pcap格式的数据包。我们首先会对原始流量进行数据预处理工作,并提取实验所需的四个统计特征然后转换为RGBA图,表3—表4分别介绍了这两个数据集的流量类别、每一种类别流量包含的内容以及样本数。

表3 “ISCX VPN-non VPN”数据集描述

Table 3 Description of "ISCX VPN non VPN" dataset

流量类型	应用程序	样本数
Chat	AIM chat,ICQ,Skype,Facebook,Hangout	1 313
VPN-chat		256
Email	Email,Gmail	677
VPN-Email		143
File	Skype,SFTP,FTPS	12 381
VPN-File		456
P2P	Bittorrent,uTorrent	1 181
VPN-P2P		265
Streaming	Vimeo,YouTube,Netflix,Spotify	1 751
VPN-Streaming		523
VOIP	Facebook,Skype,Hangout,VOIP buster	37 292
VPN-VOIP		718

在从流量中提取信息之前,我们需要先进行数据预处理,过程包括流量切分、流量清洗、图片生成和NPY(NumPy Array File Format)转换。本文所采用的流量数据均来自公开数据集“ISCX VPN-nonVPN”和“ISCX Tor-nonTor”,处理的样本数据集均为PCAP(Packet Capture数据包捕获)格式的文件。具体数据处理步骤如下:

1)流量切分:首先按照五元组信息将PCAP格式的网络流量划分成双向会话流,即要求源IP地址、源端口、目的IP地址、目的端口以及传输层使用的协议均相同,并将会话流保存为PCAP格式。

表4 “ISCX Tor-non Tor”数据集描述

Table 4 Description of "ISCX Tor non Tor" dataset

流量类型	应用程序	样本数
Audio	Vimeo,YouTube	1 868
Browsing	Firefox,Chrome	29 947
Chat	AIM chat,ICQ,Facebook,Hangout	344
Email	SMPTS,POP3S,IMAPS	283
File	Skype,SFTP,FTPS	1 794
P2P	Bittorrent,uTorrent	20 828
Video	Vimeo,YouTube	1 887
VOIP	Facebook,Skype,Hangouts	613

2)流量清洗:为了防止流量部分信息影响实验性能评估,我们首先需要对流量进行匿名化处理,每个流量类别在数据集中都有一个唯一的IP地址,如果不删除IP地址和媒体访问控制地址(Media Access Control Address,MAC),模型可能会产生过拟合。此外,实验还会去除流量数据集中的重复的文件或者空文件,避免在训练的时候影响模型的分类性能。

3)图片生成:在对原始流量进行统一大小之前,我们先提取流量的统计特征,然后对原始流量进行裁剪,即超过规定长度的会话文件会被裁剪,而长度不足要求的会话会在最后用0x00填补至规定长度,会话中的每个字节对应灰度像素值;例如,0x00表示黑色,0xFF表示白色,然后我们将会话文件转换成灰度图的形式。对于统计特征提取,该步骤中每个子流由$m\times m$个数据包组成,从中提取每个数据包的大小、到达间隔时间、方向和传输协议,从而得到$4\times m\times m$个特征向量。还应该注意的是,提取的特征在[0,1]范围内使用min-max方法进行归一化。为了标准化到达间隔时间,我们将其最大值设置为1秒,对于每个数据包,如果到达间隔时间大于1,则将到达间隔时间设置为1;对于数据包大小,最大选择为1 500字节。对于每个数据包,如果大于1 500字节则将数据包大小设置为1。然后,将数据包大小除以1 500进行归一化;对于报文方向,与第一个报文方向相同的报文设置方向为0,否则为1。协议为

UDP的报文设置协议为0,协议为TCP的报文设置协议为1。每个数据包由获得的图像中的一个RGBA条目表示。

4)NPY转换:NPY格式是深度学习中常见的文件格式之一。这里将灰度图和RGBA图转化成NPY格式的文件,NPY文件中包含了流量中对应的负载信息或者统计信息。

3.4 消融实验

本文添加的通道注意力模块由全局最大池化层和全局平均池化层并行连接构成。为了体现所采用的通道注意力模块网络结构的优势,本文与不使用通道注意力模块以及分别使用最大池化和平均池化的通道注意力模块的分类模型进行了对比实验,实验结果如表5所示。

表5 使用不同通道注意力模块分类结果对比

Table 5 Comparison of classification results using different channel attention mechanisms

模型	*Acc*	*P*	*R*	*F*1
无通道注意力	0.992 5	0.987 8	0.974 4	0.975 3
全局最大池化	0.992 9	0.982 2	0.980 1	0.981 2
全局平均池化	0.993 0	0.986 4	0.981 9	0.984 1
本文方法(最大池化+平均池化)	**0.994 1**	**0.993 1**	**0.984 4**	**0.988 7**

3.5 实验结果

为了证明基于通道注意力机制的多特征融合加密流量识别模型的有效性,本文使用了几种经典的模型在“ISCX VPN-nonVPN”数据集和“ISCX Tor-nonTor”数据集上各进行了7次实验。数据集的实验最终结果,包括准确率、精度、召回率以及*F*1-score值如表6—表7所示。实验所用的模型都经过了细致的迭代调优,挑选出最适合的参数从而保证每个模型都能达到最好的效果。

实验结果表明,本文方法对“ISCX VPN-nonVPN”数据集的12类加密流量分类的准确率达到了99.4%以上。同时,可以看出对于原始流量分类,使用一维卷积的效果明显优于二维卷积,且丢弃池化层后的分类准确率也有明显上升。

表6 “ISCX VPN-nonVPN”数据集分类结果

Table 6 Classification results on the "ISCX VPN non VPN" dataset

模型	*Acc*	*P*	*R*	*F*1
CNN1D-Pooling	0.930 6	0.926 5	0.893 0	0.904 6
CNN1D-noPooling	0.947 7	0.940 7	0.920 7	0.929 8
CNN2D-Pooling	0.912 9	0.906 8	0.892 5	0.899 0
CNN2D-noPooling	0.929 8	0.919 2	0.903 5	0.910 4
ResNet1D	0.990 8	0.978 4	0.961 0	0.968 5
ResNet2D	0.974 7	0.958 9	0.944 4	0.950 5
本文方法	**0.994 1**	**0.993 1**	**0.984 4**	**0.988 7**

表7 “ISCX Tor-nonTor”数据集分类结果

Table 7 Classification results on the "ISCX Tor nonTor" dataset

模型	*Acc*	*P*	*R*	*F*1
CNN1D-Pooling	0.968 0	0.866 1	0.838 6	0.847 9
CNN1D-noPooling	0.972 0	0.877 3	0.820 5	0.841 5
CNN2D-Pooling	0.957 6	0.857 1	0.782 3	0.813 9
CNN2D-noPooling	0.964 4	0.853 5	0.805 5	0.823 4
ResNet1D	0.991 2	0.947 3	0.948 5	0.947 7
ResNet2D	0.980 3	0.935 5	0.938 6	0.936 6
本文方法	**0.993 8**	**0.963 2**	**0.966 3**	**0.964 5**

此外,为了展现本文所提出识别模型相对于当前主流的加密流量识别方法在分类性能上的优势,我们与当前典型文献中的流量分类算法进行比较。同时,为了更好地展现融合特征的优越性,我们在对比实验中添加了集成学习中的软投票机制,对比结果如表8—表9所示。

为了更全面地证明本文方法在加密流量识别中的性能表现,我们使用精确率、召回率和*F*1-Score对每类的流量识别都进行了更精细的评价。图5显示了以上五种实验方法对公开数据集“ISCX VPN-nonVPN”中每类流量的精确率对比。在所有流量类别中,除了“VPN_FT”

表8 不同方法在“ISCX VPN-nonVPN”数据集实验结果对比

Table 8 Comparison of experimental results of different methods on the "ISCX VPN nonVPN" dataset

算法	分类模型	*Acc*	*P*	*R*	*F*1
文献[10]	CNN	0.895 3	0.911 7	0.893 2	0.901 1
文献[13]	GNN	0.931 5	0.927 0	0.915 8	0.919 5
文献[15]	Fusion(CNN, DBN, MLP)	0.976 9	0.956 2	0.948 8	0.951 8
集成学习	软投票(ResNet、Inception-CNN)	0.991 1	0.978 8	0.973 7	0.976 1
本文方法	**基于通道注意力的多特征融合**	**0.994 1**	**0.993 1**	**0.984 4**	**0.988 7**

表9 不同方法在“ISCX Tor-nonTor”实验结果对比

Table 9 Comparison of experimental results of different methods on the "ISCX Tor nonTor" dataset

算法	分类模型	*Acc*	*P*	*R*	*F*1
文献[10]	CNN	0.953 5	0.851 8	0.795 4	0.799 7
文献[13]	GNN	0.989 6	0.94	0.931	0.935 4
文献[15]	Fusion(CNN, DBN, MLP)	0.990 0	0.948 3	0.923 6	0.935 3
集成学习	软投票(ResNet、Inception-CNN)	0.992 2	0.944 6	0.948 0	0.946 0
本文方法	**基于通道注意力的多特征融合**	0.993 8	0.963 2	0.966 3	0.964 5

的精确率比文献[15]稍低外,本文方法对其他几类流量识别的精确率均高于文献[10]、文献[13]、文献[15]以及集成学习的方法。图6显示了以上五种实验方法对公开数据集“ISCX VPN-nonVPN”中每类流量的召回率对比。在所有流量类别中,除了“VPN_Streaming”的召回率比文献[15]稍低外,本文方法对其他几类流量识别的召回率均高于文献[10]、文献[13]、文献[15]以及集成学习的方法。图7显示了以上五种实验方法对公开数据集“ISCX VPN-nonVPN”中每类流量的*F*1-Score对比。在所有流量类别中,本文方法对所有类别流量识别的*F*1-score均高于文献[10]、文献[13]、文献[15]以及集成学习的方法。并且在12类加密的网络流量中,对于样本数较大的流量类型,如P2P、VOIP等,五种分类模型都有较好的表现。但是对于VPN_Email、Email、VPN_Streaming等样本数较少的流量类别,CNN和GNN的分类效果较差。其中CNN在少数类上的精度基本在78%到85%之间。对于VPN_Email类别,GNN的*F*1-score只有71%。对于CNN, DBN, MLP的融合模型以及集成学习方法,其在小样本类别上的*F*1-score值分布在90%~96%之间。而本文所提模型在所有类别上的*F*1-score基本达到96%以上,相对于CNN和GNN在少数类的分类性能上有明显提升。整体结果表明本文所提模型在加密流量上的分类性能优于当前主流的分类算法。从三种评价指标的整体对比结果来看,相比于文献[10]、文献[13]、文献[15]和集成学习,本文提出的分类方法在各个类别之间的分类结果浮动相对较小。说明本文方法针对不同类别的加密流量可以实现更稳定的分类,面对小样本类别也可以实现高精度分类,具有更强的泛化能力。

综合实验结果可以得出,使用本文方法对加密流量数据进行学习,总体分类准确率可达到99.4%,并且针对每种类型流量的各项分类

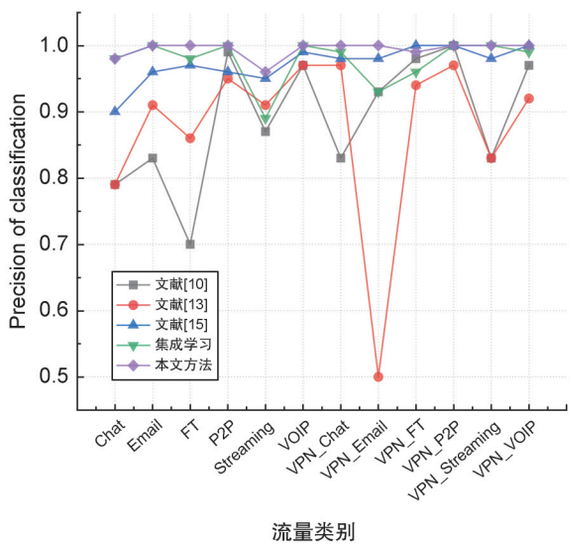

图5 不同方法在“ISCX VPN-nonVPN”数据集上精度的比较

Fig. 5 Comparison of precision among different methods on the "ISCX VPN nonVPN" datasets

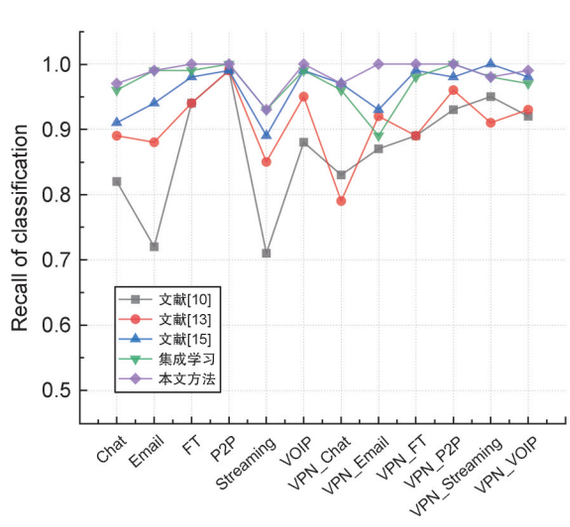

图6 不同方法在“ISCX VPN-nonVPN”数据集上召回率的比较

Fig. 6 Comparison of recall rates among different methods on the "ISCX VPN nonVPN" datasets

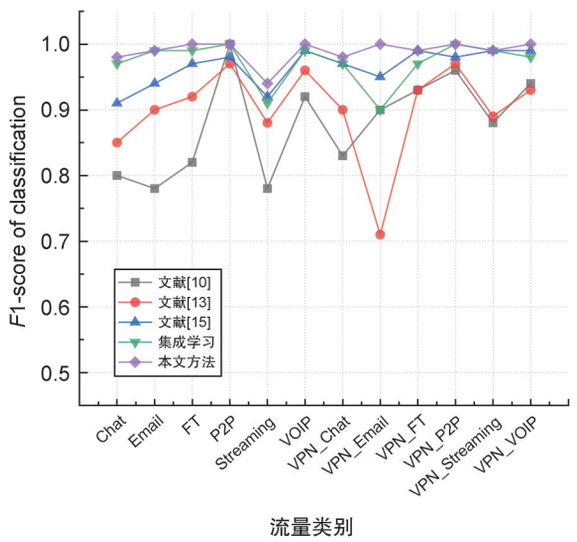

图7 不同方法在“ISCX VPN-nonVPN”数据集上*F*1-score的比较

Fig. 7 Comparison of *F*1-score among different methods on the "ISCX VPN nonVPN" datasets

指标都取得了良好的效果,整体均优于文献[10]、文献[13]、文献[15]以及集成学习的方法。

4 结论

为了更好地挖掘原始加密流量的特征信息,同时避免信息损失,本文结合ResNet、Inception-CNN以及通道注意力机制提出了一种基于注意力的多特征融合加密流量识别方法。所提方法使用两个分支分别提取原始流量特征信息与数据包统计特征信息。此外,本文添加了通道注意力模块用于赋予每个通道不同的权重,从而使模型更集中于神经网络提取到的关键特征,增强流量的表征能力。本文在“ISCX VPN-nonVPN”数据集上进行了多重验证,在已有研究的基础上进行了对比试验,论证了实验的可行性以及本文设计的基于注意力的多特征融合加密流量识别方法具有更好的识别效果。

参考文献:

[1] AZAB A, KHASAWNEH M, ALRABAEE S, *et al*. Network Traffic Classification: Techniques, Datasets, and Challenges[J]. *Digit Commun Netw*, 2022. DOI: 10.1016/j.dcan.2022.09.009.

[2] LIN P, HU Y S, LIN Y Y, *et al*. PEAN: A Packet-level End-to-end Attentive Network for Encrypted Traffic Identification[C]//2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). Haikou, Hainan: IEEE, 2022: 267-274. DOI: 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00061.

[3] ZHENG W P, ZHONG J H, ZHANG Q Z, *et al*. MTT: an Efficient Model for Encrypted Network Traffic Classification Using Multi-task Transformer[J]. *Appl Intell*, 2022, **52**(9): 10741-10756. DOI: 10.1007/s10489-021-03032-8.

[4] DAI J B, XU X L, GAO H H, *et al*. SHAPE: A Simultaneous Header and Payload Encoding Model for Encrypted Traffic Classification[J]. *IEEE Trans Netw Serv Manag*, 2023, **20**(2): 1993-2012. DOI: 10.1109/TNSM.2022.3213758.

[5] OKONKWO Z, FOO E, LI Q Y, *et al*. A CNN Based Encrypted Network Traffic Classifier[C]//Proceedings of the 2022 Australasian Computer Science Week. New York: ACM, 2022: 74-83. DOI: 10.1145/3511616.3513101.

[6] MOORE A W, ZUEV D. Internet Traffic Classification Using Bayesian Analysis Techniques[C]//Proceedings of the 2005 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems. New York: ACM, 2005: 50-60. DOI: 10.1145/1064212.1064220.

[7] TAYLOR V F, SPOLAOR R, CONTI M, *et al*. Robust Smartphone App Identification *via* Encrypted Network Traffic Analysis[J]. *IEEE Trans Inf Forensics Secur*, 2018, **13**(1): 63-78. DOI: 10.1109/TIFS.2017.2737970.

[8] CAO J, FANG Z, QU G, *et al*. An Accurate Traffic Classi fication Model Based On Support Vector Machines[J]. *Int J Netw Manag*, 2017, **27**(1): e1962. DOI: 10.1002/nem.1962

[9] 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). Da Nang, Vitenam: IEEE, 2017: 712-717. DOI: 10.1109/ICOIN.2017.7899588.

[10] 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 (ISI). Beijing, China: IEEE, 2017: 43-48. DOI: 10.1109/ISI.2017.8004872.

[11] LOTFOLLAHI M, SIAVOSHANI M J, ZADE R S H,

et al. Deep Packet: a Novel Approach for Encrypted Traffic Classification Using Deep Learning[J]. *Soft Comput*, 2020, **24**(3): 1999−2012. DOI: 10.1007/s00500-019-04030-2.

[12] HE Y J, LI W. Image-based Encrypted Traffic Classification with Convolution Neural Networks[C]//2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC). New York: IEEE, 2020: 271−278. DOI: 10.1109/DSC50466.2020.00048.

[13] HUOH T L, LUO Y, LI P L, *et al*. Flow-based Encrypted Network Traffic Classification with Graph Neural Networks[C]//IEEE Transactions on Network and Service Management. New York: IEEE, 2022: 1224−1237. DOI: 10.1109/TNSM.2022.3227500.

[14] LIN P, YE K J, HU Y S, *et al*. A Novel Multimodal Deep Learning Framework for Encrypted Traffic Classification[J]. *IEEE/ACM Trans Netw*, 2023, **31**(3): 1369−1384. DOI: 10.1109/TNET.2022.3215507.

[15] IZADI S, AHMADI M, RAJABZADEH A. Network Traffic Classification Using Deep Learning Networks and Bayesian Data Fusion[J]. *J Netw Syst Manage*, 2022, **30**(2): 25. DOI: 10.1007/s10922-021-09639-z.

[16] DRAPER-GIL G, LASHKARI A H, MAMUN M S I, *et al*. Characterization of Encrypted and VPN Traffic Using Time-related Features[C]//Proceedings of the 2nd International Conference on Information Systems Security and Privacy. Roma, Italy: SCITEPress, 2016: 407−414. DOI: 10.5220/0005740704070414.

[17] HABIBI LASHKARI A, DRAPER GIL G, MAMUN M S I, *et al*. Characterization of Tor Traffic Using Time Based Features[C]//Proceedings of the 3rd International Conference on Information Systems Security and Privacy. Porto, Portugal: SCITEPress, 2017: 253−262. DOI: 10.5220/0006105602530262.

[18] 徐洪平, 马泽文, 易航, 等. 基于卷积循环神经网络的网络流量异常检测技术[J]. 信息网络安全, 2021(7): 54−62. DOI: 10.3969/j.issn.1671-1122.2021.07.007.
XU H P, MA Z W, YI H, *et al*. Network Traffi c Anomaly Detection Technology Based on Convolutional Recurrent Neural Network[J]. *Netinfo Secur*, 2021(7): 54−62. DOI: 10.3969/j.issn.1671-1122.2021.07.007.

[19] MA Z H, LI K Y, LI Z Y, *et al*. Encrypted Traffic Classification Based on a Convolutional Neural Network[J]. *J Phys: Conf Ser*, 2022, **2400**(1): 012056. DOI: 10.1088/1742-6596/2400/1/012056.

[20] QIN J Y, LIU G J, DUAN K. A New Imbalanced Encrypted Traffic Classification Model Based on CBAM and Re-weighted Loss Function[J]. *Appl Sci*, 2022, **12**(19): 9631. DOI: 10.3390/app12199631.

[21] MA X L, ZHU W B, WEI J L, *et al*. EETC: An Extended Encrypted Traffic Classification Algorithm Based on Variant Resnet Network[J]. *Comput Secur*, 2023, **128**: 103175. DOI: 10.1016/j.cose.2023.103175.

[22] OBESO A M, BENOIS-PINEAU J, GARCÍA VÁZQUEZ M S, *et al*. Visual vs Internal Attention Mechanisms in Deep Neural Networks for Image Classification and Object Detection[J]. *Pattern Recognit*, 2022, **123**: 108411. DOI: 10.1016/j.patcog.2021.108411.