

基于卷积神经网络的加密流量分类方法

谢绒娜, 马铸鸿, 李宗俞, 田野
(北京电子科技学院, 北京 100070)

摘要: 针对传统加密网络流量分类方法准确率较低、泛用性不强、易侵犯隐私等问题, 提出了一种基于卷积神经网络的加密流量分类方法, 避免依赖原始流量数据, 防止过度拟合特定应用程序的字节结构。针对网络流量的数据包大小和到达时间信息, 设计了一种将原始流量转换为二维图片的方法, 直方图中每个单元格代表到达相应时间间隔的具有相应大小数据包的数量, 不依赖数据包有效载荷, 避免了侵犯隐私; 针对 LeNet-5 卷积神经网络模型进行了优化以提高分类精度, 嵌入 Inception 模块进行多维特征提取并进行特征融合, 使用 1×1 卷积来控制输出的特征维度; 使用平均池化层和卷积层替代全连接层, 提高计算速度且避免过拟合; 使用对象检测任务中的滑动窗口方法, 将每个网络单向流划分为大小相等的块, 确保单个会话中训练集中的块和测试集中的块没有重叠, 扩充了数据集样本。在 ISCX 数据集上的分类实验结果显示, 针对应用流量分类任务, 准确率达到 95% 以上。对比实验结果表明, 训练集和测试集类型不同时, 传统分类方法出现了显著的精度下降乃至失效, 而所提方法的准确率依然达到了 89.2%, 证明了所提方法普适于加密流量与非加密流量。进行的所有实验均基于不平衡数据集, 如果对数据集进行平衡化处理, 准确率可能会进一步提高。

关键词: 加密流量; 卷积神经网络; 深度学习; 特征融合; 模型优化

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022077

Encrypted traffic classification method based on convolutional neural network

XIE Rongna, MA Zhuhong, LI Zongyu, TIAN Ye

Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Aiming at the problems of low accuracy, weak generality, and easy privacy violation of traditional encrypted network traffic classification methods, an encrypted traffic classification method based on convolutional neural network was proposed, which avoided relying on original traffic data and prevented overfitting of specific byte structure of the application. According to the data packet size and arrival time information of network traffic, a method to convert the original traffic into a two-dimensional picture was designed. Each cell in the histogram

收稿日期: 2021-12-27; 修回日期: 2022-08-14

通信作者: 田野, 674600206@qq.com

基金项目: 国家重点研发计划(2017YFB0801803)

Foundation Item: The National Key R&D Program of China(2017YFB0801803)

引用格式: 谢绒娜, 马铸鸿, 李宗俞, 等. 基于卷积神经网络的加密流量分类方法[J]. 网络与信息安全学报, 2022, 8(6): 84-91.

Citation Format: XIE R N, MA Z H, LI Z Y, et al. Encrypted traffic classification method based on convolutional neural network[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 84-91.

represented the number of packets with corresponding size that arrive at the corresponding time interval, avoiding reliance on packet payloads and privacy violations. The LeNet-5 convolutional neural network model was optimized to improve the classification accuracy. The inception module was embedded for multi-dimensional feature extraction and feature fusion. And the 1*1 convolution was used to control the feature dimension of the output. Besides, the average pooling layer and the convolutional layer were used to replace the fully connected layer to increase the calculation speed and avoid overfitting. The sliding window method was used in the object detection task, and each network unidirectional flow was divided into equal-sized blocks, ensuring that the blocks in the training set and the blocks in the test set in a single session do not overlap and expanding the dataset samples. The classification experiment results on the ISCX dataset show that for the application traffic classification task, the average accuracy rate reaches more than 95%. The comparative experimental results show that the traditional classification method has a significant decrease in accuracy or even fails when the types of training set and test set are different. However, the accuracy rate of the proposed method still reaches 89.2%, which proves that the method is universally suitable for encrypted traffic and non-encrypted traffic. All experiments are based on imbalanced datasets, and the experimental results may be further improved if balanced processing is performed.

Keywords: encrypted traffic, convolution neural network, deep learning, feature fusion, model optimization

0 引言

网络流量中包含众多有分析价值的信息, 如何智能化地处理和分析网络数据, 成为网络安全领域的研究热点^[1]。近年来, 隐私数据和隐私保护愈发引起人们重视, 数据传输过程中普遍使用各种加密技术, 加密流量在网络流量中占据越来越大的比重^[2]。加密流量在保护隐私安全的同时, 给流量监测和流量识别问题带来了困难。如何高效准确地分类识别加密网络流量数据, 从而有效检测恶意流量, 成为网络安全领域的研究热门。

传统的网络流量分析方法, 如负载分析^[3]和基于端口^[4]方法, 在精度和性能上出现了显著下降^[5]。机器学习 (ML, machine learning) 方法已经普遍应用于网络流量分析^[6]。但是机器学习方法存在的问题是识别效果高度依赖于所提取的特征, 基于深度学习的方法则可以避免这一问题, 被逐步应用于加密流量识别领域并取得了一定成果^[7-15]。Wei 等^[7]提出了使用卷积神经网络模型进行加密流量识别, 将流量数据标准化后使用前 784 字节作为模型的输入, 在数据集上进行了评估, 并与决策树方法进行了比较, 结果显示精度上有明显提高。Xiao 等^[8]设计了扩展字节段神经网络用于网络流量分类, 将数据包分为头段和负载端再送入自编码器中, 在数据集上的检验表明

其在应用程序识别任务和网站识别任务上性能有显著提高。朱文斌^[9]等提出了一种基于多种构图方式的网络流量图像分类方法, 考虑使用不同的构图方式将数据包转换为流量图像。Rezaei 等^[10]基于时间序列结合一维卷积神经网络对 5 种应用程序进行了分类, 结果表明该方法可应用于高带宽业务网络。Lotfollahi 等^[11]使用堆叠式自编码器和卷积神经网络对网络流量进行分类, 在应用识别任务中, 该分类方法的准确率达到 98%。Chen 等^[12]利用核希尔伯特空间的重生成嵌入将时间序列数据转为图像, 在协议和应用分类任务上取得了较好的效果。Ertam 和 Avci^[13]使用遗传算法 (GA) 提取特征, 应用基于极限学习机在数据集上进行实验, 实验结果获得了 95% 以上的准确率。Lopez-Martin 等^[14]和 Wang 等^[15]分别使用了循环神经网络和卷积神经网络针对应用进行识别, 两项研究的共同之处是使用前 6~30 个数据包内容作为输入, 虽然网络模型和数据集等不同, 但两者都具有较高的准确率。

由于以上方法多数专注于数据包的有效负载内容, 这些方法依赖于原始数据, 存在因过度拟合特定应用程序的字节结构, 而无法应对未知应用程序的问题。同时, 这些方法在使用虚拟专用网络 (VPN, virtual private network) 等加密技术的情况下均出现一定程度的性能下降。此外, 这些方法依赖于数据包的有效负载内容, 一定程度

上侵犯了隐私。

针对传统网络流量识别方法的不足, 本文对传统的卷积神经网络(CNN, convolutional neural network)模型进行了改进优化, 提出了一种面向图片的加密流量识别方法, 主要贡献包括以下两个方面。

1) 利用深度学习中神经网络可以避免人工特征提取的特点, 提出了一种基于卷积神经网络的分类模型。针对当前分类方法在特征学习方面的不足, 在卷积神经网络模型中嵌入了 Inception 模块, Inception 模块中使用多个卷积层以不同的感受野分别提取特征, 之后将提取到的特征进行融合, 通过更多数量的特征来更好地学习输入输出之间非线性的关系, 提高了分类精度。同时, 模型使用全局平均池化层和卷积层替代全连接层, 在减少网络参数加快计算速度的同时避免过拟合, 提高了模型的泛用能力。

2) 针对数据包的有效负载内容可能会造成过拟合和无法应对未知应用程序的问题, 提出了一种利用数据包的到达时间以及大小等信息将流量数据转换为图片的方法, 避免了人工提取特征, 可以处理单向流的短时间窗口而不是只能应用于双向会话。同时, 所提方法不依赖于数据包的有效负载内容, 避免了侵犯隐私, 且在加密与非加密流量上具有普适性。

1 基于卷积神经网络的加密流量识别方法

为了提高模型的泛用能力, 避免过拟合于某

一特定应用程序流量, 本文使用数据包的时间和大小相关信息生成图像作为模型的输入, 一方面提高模型运算速度和模型泛用能力; 另一方面确保模型不依赖于数据包的有效负载内容, 避免了隐私侵犯。为了避免实际训练中模型不能有效提取到不平衡流量种类的流量特征, 进而影响模型分类精度, 该模型在传统 CNN 的基础上嵌入了 Inception 模块以达到多尺度特征融合的目的, 保证少量数据特征提取量; 使用卷积层和平均池化层的组合取代了传统的全连接层, 降低了运算负担, 提高了模型识别的速度。

基于上述原则, 本文提出的卷积神经网络总体架构如图 1 所示, 将原始网络流量数据根据提出的图像生成方法转换为图片作为模型的输入; 在两次卷积池化操作中插入 Inception 模块进行多层次提取特征和特征融合, Inception 模块可以复用更多特征, 提高特征张量宽度和对特征的囊括性; 在最终输出之前, 使用一个卷积层和全局平均池化层的组合代替全连接层, 减少网络中的训练参数, 避免过拟合。卷积层的卷积核大小为 1×1 , 卷积核的数量由最终分类的类别数 N 决定。卷积层的输出送入平均池化层后最终得到维度为 $(1, 1, N)$ 的输出向量。在模型的最后, 使用 Softmax 激活函数进行最终的分类。

1.1 基于数据包到达时间和大小的图像转换方法

网络流量分类领域的大部分研究专注于数据包本身的有效负载内容, 造成模型过拟合于特定数据字节段, 无法识别网络中新出现的应用程序

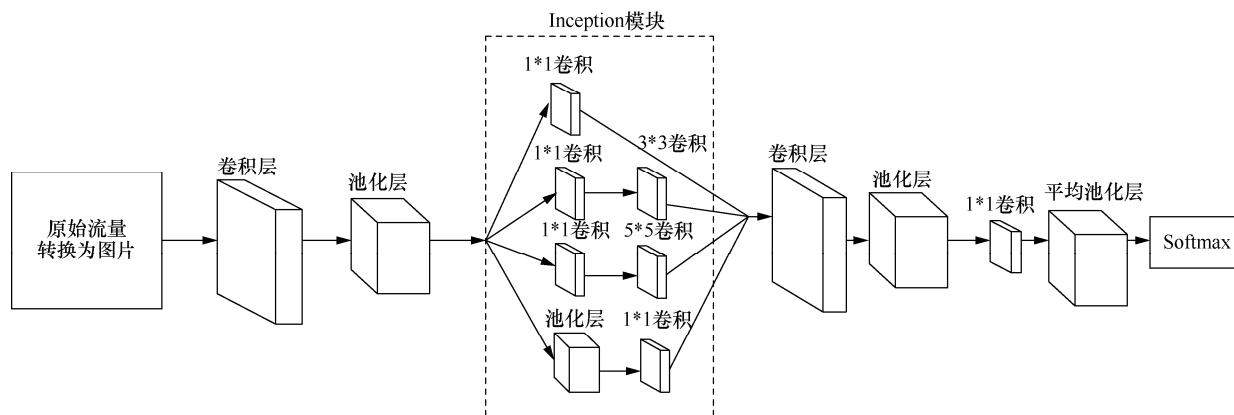


图 1 卷积神经网络总体架构

Figure 1 Overall architecture of convolution neural network

流量,也无法有效识别加密流量。同时,基于数据包本身的有效负载内容在一定程度侵犯了隐私。本文避免从数据包自身有效负载内容入手,针对数据包的时间和大小相关信息,设计了一种将流量数据转化为二维直方图的方法。处理流程如图2所示,步骤如下。

1) 网络流量划分: 本文将具有相同五元组{源IP地址,源端口号,目的IP地址,目的端口号,协议}的网络数据包看作属于同一种应用产生的流量,称为单向流。以单向流为基本单位将pcap原始文件进行拆分,其中pcap文件是正常用的数据报存储格式。

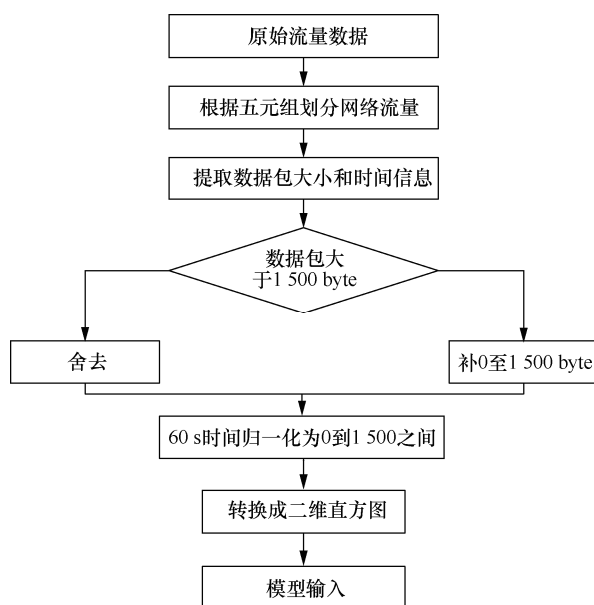


图2 原始数据转换成图片的处理流程
Figure 2 The process of converting raw data into pictures

2) 记录提取: 从每个单向流中提取IP包大小、到达时间作为关键记录输入神经网络。关键记录定义为{IP包大小,到达时间}。由于卷积神经网络需要一个统一的输入维度,而实际中数据包的大小往往是不固定的,在输入神经网络前关键记录需要进行标准化处理。大部分计算机最大传送单元(MTU)的大小为1500 byte,因此设定标准大小为1500 byte,将大于1500 byte的数据包舍弃(这部分数据包数量小于整体数量的5%),对大小不足1500 byte的数据包使用0 byte进行补齐。

3) 直方图生成: 将关键记录中的IP包大小

和到达时间集成到二维直方图中,这些二维直方图可以看作一个有效载荷大小的数组。为了方便,将二维直方图设置为正方形图像。定义直方图的X轴为到达时间,根据定义,通过减去单向流中第一个包的到达时间来标准化所有数据包的到达时间值。将后续包到达时间值规范化处理,归一化为0到1500之间(即30s映射到1500)。定义直方图的Y轴为数据包的大小。将所有标准化后的数据对插入二维直方图中,直方图中每个单元格的意义是到达相应时间间隔的具有相应大小数据包的数量。得到的结果是1500*1500的直方图,直方图中值的总和等于原始时间窗口中IP包的总数(不包括忽略的部分),本文使用直方图作为神经网络的最终输入。

1.2 基于Inception模块的特征融合

传统的卷积神经网络在网络层次较浅时难以提取到深层次的特征,对于网络流量分类问题,这制约了模型的性能。解决此问题的常见方法是增加网络深度,即在模型中增加更多的网络层,这会造成网络复杂度大大提升,增加了计算成本且训练过程中容易退化。采用Inception模块,可以在增加网络深度和宽度的同时减少参数,在提取特征的同时减小计算负担。

为了避免数据量较小的流量类别在训练中模型提取特征不足而影响最终的分类效果,同时提高其他类别的识别精度,在设计卷积神经网络模型时添加了Inception模块。Inception模块通过对多个不同感受野进行特征提取,并进行多尺度特征融合,提高卷积神经网络提取到的特征丰富性和完善性。Inception模块由不同卷积核大小的卷积层和池化层组成,可以通过不同的局部感受野来多维度提取特征并进行融合。如图3所示,本文中的Inception模块由卷积核大小分别为1*1、3*3、5*5的3个卷积层和1个最大池化层组成。

为了提高训练速度,在卷积前和池化后分别使用1*1卷积来控制输出的特征维度以便于特征融合。为了控制梯度爆炸,加快网络的训练和收敛速度,Inception模块的卷积层后连接了BN(批量归一化)层。之后使用ReLU激活函数对数据进行处理,ReLU激活函数的定义如式(1)所示。

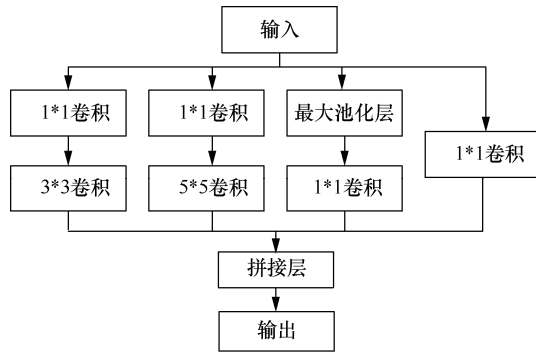


图 3 Inception 模块结构

Figure 3 Inception module structure diagram

$$f(x) = \begin{cases} 0, & x \leq 0 \\ x, & x > 0 \end{cases} \quad (1)$$

2 实验与结果分析

本文实验设计分为 3 个部分。第一部分是有效性验证，目的是证明模型未受过拟合影响，实验结果真实有效。第二部分是性能验证，目的是证明添加 Inception 模块的 CNN 性能优于传统 CNN 性能。第三部分是泛用性验证，目的是证明所提方法同时适用于加密流量与非加密流量。

2.1 实验数据集与数据预处理

本文实验所使用的数据集为“UNB ISCX VPN-nonVPN 2016”^[16]加密流量数据集和部分收集的聊天流量，数据集中包括两大类，分别是 VPN 和非 VPN 加密流量，流量以 pcap 文件形式存储。使用包含足够样本数量的 5 个类别的组合数据集：Voip、Chat、File、Streaming、Browsing。

为了增加训练集的样本数量，同时减少过拟合，将每个单向流划分为大小相等的块，每个会话划分为 30 s 大小的块^[16]，重叠时间为 15 s，该方法来源于对象检测任务中滑动窗口的使用^[17]。例如，5 min (300 s) 的会话可以由 10 个非重叠会话块组成 (10×30=300)，也可以由 19 个重叠会话块组成 (19×30-18×15=300)。需要注意的是，扩充数据集的操作是在将所有会话划分为训练集和测试集之后进行的，以确保单个会话中训练集中的块和测试集中的块没有重叠。最终所使用的数据集的各类样本数量如表 1 所示。

表 1 数据集样本分布数量

Table 1 Number of sample distribution of dataset

服务类别	样本数量	服务类别	样本数量
File	2 192	VPN_File	2 093
Browsing	6 182	VPN_Browsing	4 895
Voip	6 317	VPN_Voip	5 876
Streaming	1 593	VPN_Steaming	612
Chat	1 241	VPN_Chat	964

2.2 实验评价指标

本文使用深度学习领域常见的评价指标准确率 (Accuracy) 来对实验模型进行评价，其定义如式(2)所示。

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \quad (2)$$

其中，TP 是被模型预测为正类的正样本，TN 是被模型预测为负类的负样本，FP 是被模型预测为负类的负样本，FN 是被模型预测为负类的正样本。

2.3 实验结果与分析

(1) 有效性验证

为了减少过拟合，本文使用 dropout 技术防止对训练数据进行复杂的协同适应。将数据集随机拆分为占比 0.85 的训练集和占比 0.15 的测试集。训练周期为 30 个周期，如图 4 所示，网络在运行 VPN 中 Browsing 流量分类任务时，在 10~15 个 epoch 后达到了收敛，并且训练曲线和测试曲线之间的方差较小，表明本文结果是真实有效的，模型没有受到过拟合的影响。

(2) 性能验证

为了体现所提分类模型中所采用的 Inception 模块的优势，本文与未添加 Inception 模块的传统 CNN 分类模型进行了对比实验。实验结果如表 2 所示。由表中数据可以看出，5 种应用程序类别在添加了 Inception 模块的网络上各项性能指标均优于未添加 Inception 模块的普通 CNN，其中样本数量较少的 Browsing 和 Chat 流量效果提升明显，5 种应用类别分别提高了 1.8%、1.5%、1.6%、4.2% 和 4.8%。由实验结果可知，添加 Inception 模块帮助模型提取到了更丰富的特征，实现了更优的分类性能，特别是面对少样本数据时，效果提升明显。

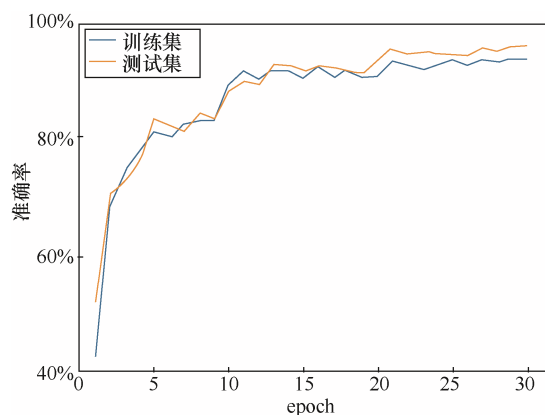


图 4 准确率增长曲线
Figure 4 Accuracy growth curve

表 2 两种 CNN 模型准确率比较
Table 2 Comparison of the accuracy of two classification models

类别	添加 Inception 模块 CNN 准确率	普通 CNN 准确率
File	93.4%	91.6%
Browsing	95.2%	93.7%
VoIP	99.8%	98.2%
Streaming	99.6%	95.4%
Chat	97.2%	92.4%

(3) 泛用性验证

本文提出的方法针对加密流量与非加密流量具有普适性，为证明模型的普适性，设计了对比实验。根据流量是否使用了加密技术，将流量数据分为两个数据集，对于每一个应用类别，使用模型在一个训练集上进行训练，并分别在两个测试集上进行测试，每个测试集都包含特定类别的样本，实验结果如表 3 所示：对角线上的值（加粗部分）显示了当测试集由与训练集相同的流量类别和加密技术组成时的准确率。

从表 3 的实验结果可以看出（对角线加粗部分），在训练集和测试集具有相同的流量类别的情况下，模型具有良好的分类效果，分类准确率均高于 90%，最好效果达到 99.4%。

从实验结果可知（未加粗部分），在训练集和测试集分别由使用了加密技术和未使用加密技术的流量数据组成时，模型依然具有良好的分类效果，多数类别的分类准确率高于 90%。只在 Chat 这一类别上出现了差异。这可能是由于加密技术改变了 Chat 流量类别的独特特征，其

与 Browsing 流量类别特征在一定程度上具有相似性。在实验过程中发现，模型将一部分 Chat 流量误识别为 Browsing 流量，难以区分 Chat 流量和 Browsing 流量是模型准确率下降的主要原因。

表 3 不同种类流量在加密与非加密数据集上的准确率比较

Table 3 Comparison of the accuracy of various types of traffic in encrypted and unencrypted data sets

类别		准确率	
		非 VPN	VPN
File	NonVPN	98.5	93.2
	VPN	91.1	99.4
Browsing	NonVPN	97.8	97.3
	VPN	89.9	98.4
VoIP	NonVPN	99.4	99.6
	VPN	96.1	98.7
Streaming	NonVPN	99.1	98.6
	VPN	91.3	99.3
Chat	NonVPN	96.2	79.4
	VPN	81.7	99.2

同时，本文设计与部分相近研究工作^[7,9]的对比实验。实验结果基于相同的“UNB ISCX VPN-nonVPN 2016”数据集，如表 4 所示：在训练集和测试集类型相同时，本文提出的方法准确率为 97.6%，高于端到端加密流量分类模型^[7]的 96.8%和基于多种构图的分类模型^[9]的 95.4%；且本文所提模型在训练集和测试集类型不同时依然可以对网络流量进行识别，而其余两种模型均出现了显著的精度下降乃至失效（准确率在 50%左右波动），这是本文模型相比其他模型独有的优势。

通过上述实验，证明所提方法在面对单一流量分类问题上有着极高的准确率，且同时普适于加密流量与非加密流量，这是所提方法的优势。值得一提的是，本文并没有对数据集进行平衡化处理，所有实验均是在不平衡数据集上进行的。如果对数据集进行平衡处理，实验结果可能会进一步提升。

3 结束语

本文针对网络流量传统识别方法准确率较

表 4 不同模型实验结果比较
Table 4 Comparison of experimental results of different models

模型类别	训练集与测试集类型相同时是否可以识别流量	训练集与测试集类型不同时是否可以识别流量	训练集与测试集类型相同时的识别准确率	训练集与测试集类型不同时的识别准确率
本文模型	是	是	97.6%	89.2%
端到端分类模型	是	否	96.8%	53.1%
基于多种构图的分类模型	是	否	95.4%	55.8%

低、泛用性不强、侵犯隐私且不具备普适性等问题，提出了基于卷积神经网络的加密流量分类方法，利用网络流量中时间和数据大小相关信息，将网络流量转换为二维直方图，设计了一个嵌入 Inception 模块的改进 CNN 模型，通过添加 Inception 模块实现多特征融合，提高了模型的分类精度，相比普通 CNN，最大提升效果达到了 4.8%。该方法不会过拟合于某一特定应用程序流量，避免了侵犯隐私，可以同时普适用于加密流量与非加密流量，实验结果验证了所提方法的有效性，在应用程序分类问题上准确率达到 95% 以上。未来将考虑在模型设计中引入注意力模块，增加流量特征的特征能力，进一步提高分类性能。

参考文献：

- [1] 李艳霞, 柴毅, 胡友强, 等. 不平衡数据分类方法综述[J]. 控制与决策, 2019, 34(4): 673-688.
LI Y X, CAI Y, HU Y Q, et al. A summary of the classification methods of unbalanced data[J]. Control and decision-making, 2019, 34(4): 673-688.
- [2] 王攀, 陈雪娇. 基于堆栈式自动编码器的加密流量识别方法[J]. 计算机工程, 2018, 44(11): 140-147.
WANG P, CHEN X J. Encrypted traffic identification method based on stack automatic encoder[J]. Computer Engineering, 2018, 44 (11): 140-147.
- [3] FINSTERBUSCH M, RICHTER C, ROCHA E, et al. A survey of payload-based traffic classification approaches[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1135-1156.
- [4] DAINOTTI A, PESCAPE A, CLAFFY K C. Issues and future directions in traffic classification[J]. Network IEEE, 2012, 26(1): 35-40.
- [5] 骆子铭, 许书彬, 刘晓东. 基于机器学习的 TLS 恶意加密流量检测方案[J]. 网络与信息安全学报, 2020, 6(1): 77-83.
LUO Z M, XU S B, LIU X D. TLS malicious encryption traffic detection scheme based on machinelearning[J]. Journal of Network and Information Security, 2020, 6 (1): 77-83.
- [6] REZAEI S, LIU X. Deep learning for encrypted traffic classification: an overview[J]. IEEE Communications Magazine, 2019, 57(5): 76-81.
- [7] WEI W, MING Z, WANG J, 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). 2017: 43-48.
- [8] XIAO X, XIAO W, LI R, et al. EBSNN: extended byte segment neural network for network traffic classification[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 10(1).
- [9] 朱文斌, 马秀丽. 多种构图方式下的加密流量分类[J]. 电子测量技术, 2021, 44(12): 87-92.
ZHU W B, MA X I. Classification of encrypted traffic under multiple composition methods[J]. Electronic Measurement Technology, 2021, 44 (12): 87-92.
- [10] REZAEI S, LIU X. How to achieve high classification accuracy with just a few labels: a semi-supervised approach using sampled packets[J]. arXiv preprint arXiv:1812.09761, 2018.
- [11] LOTFOLLAHI M, JAFARI SIAVOSHANI M, SHIRALI HOSSEIN ZADE R, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.
- [12] CHEN Z, HE K, LI J, et al. Seq2img: a sequence-to-image based approach towards ip traffic classification using convolutional neural networks[C]//2017 IEEE International Conference on Big Data. 2017: 1271-1276.
- [13] ERTAM F, AVCI E. A new approach for internet traffic classification: GA-WK-ELM[J]. Measurement, 2017, 95:135-142.
- [14] LOPEZ-MARTIN M, CARRO B, SANCHEZ-ESGUEVILLAS A, et al. Network traffic classifier with convolutional and recurrent neural networks for internet of things[J]. IEEE Access, 2017, (99): 1-1.
- [15] WANG W, ZHU M, ZENG X, et al. Malware traffic classification using convolutional neural network for representation learning[C]//2017 International conference on information networking (ICOIN). 2017: 712-717.
- [16] DRAPER-GIL G, LASHKARI A H, MAMUN M S I, et al. Characterization of encrypted and VPN traffic using time-related[C]// Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP). 2016: 407-414.
- [17] SZEGEDY C, TOSHEV A, ERHAN D. Deep neural networks for object detection[J]. Advances in Neural Information Processing Systems, 2013: 26.

[作者简介]



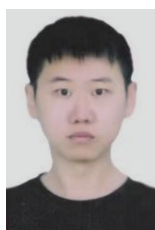
谢绒娜（1976- ），女，山西永济人，北京电子科技学院教授，主要研究方向为网络与系统安全、访问控制、密码工程。



李宗俞（1999- ），女，河南上蔡县人，北京电子科技学院硕士生，主要研究方向为信息安全。



马铸鸿（1999- ），男，河南邓州人，北京电子科技学院硕士生，主要研究方向为信息安全。



田野（1997- ），男，内蒙古赤峰人，北京电子科技学院硕士生，主要研究方向为信息安全。