

DOI:10.3969/j.issn.1671-0673. 2026. 01. 015

MT:一种利用流量图像的加密流量分类方法

李洋洋¹, 刘永杰², 顾纯祥¹

(1.信息工程大学,河南 郑州 450001; 2.69012 部队,新疆 乌鲁木齐 830031)

摘要:为解决传统加密流量分类方法对流量特性利用不充分的问题,提出一种多维信息图像加密流量分类方法(MT)。首先,将流量转换为特殊的流量图片格式,图片中包含流量中独有的信息,包括包头、载荷和包长度序列。其次,使用 Transformer 架构提取流量图片中对分类有用信息的整体特征,使用 LSTM-FCN 模型提取流量图片中的长距离和短距离的时间序列特征。最后,使用双阶段融合分类器,将整体特征和时序特征分别送入对应的分类器中得到两个决策结果,经过特征融合分类器对整体特征和时序特征进行加权融合得到第 3 个决策结果,通过 3 个决策结果融合得到预测结果。实验结果表明,在多个公开数据集和自采集数据集下,MT 方法在分类任务中各项指标达到了优于所选基线方法的效果。

关键词:Transformer 架构; LSTM-FCN 模型; 流量图像; 流量分类; 双阶段融合分类器

中图分类号:TP393.0

文献标识码:A

文章编号:1671-0673(2026)01-0112-08

MT: an Encrypted Traffic Classification Method Utilizing Traffic Images

LI Yangyang¹, LIU Yongjie², GU Chunxiang¹

(1.Information Engineering University, Zhengzhou 450001, China; 2.Unit 69012, Urumqi 830031, China)

Abstract: To address the insufficient utilization of traffic characteristics in traditional encrypted traffic classification methods, a multidimensional information image-based encrypted traffic classification method, named MT (multi-dimensional information image encryption traffic classification method), is proposed in this paper. Firstly, traffic data is converted into a specialized traffic image format that incorporates unique information from traffic flow, including packet headers, payloads, and packet length sequences. Then, Transformer architecture is employed to extract global features relevant for classification from traffic images, while the LSTM-FCN(long short-term memory-fully convolutional network) model is utilized to capture both long-range and short-term temporal patterns within the sequential data. Finally, a two-stage fusion classifier is implemented, where the global and temporal features are fed into their respective classifiers to generate two initial decision outcomes. A feature fusion classifier subsequently performs weighted integration of these global and temporal features to produce a third decision. The final prediction is obtained through the fusion of these 3 decision results. Experimental results show that the MT method achieves superior performance across multiple evaluation metrics on both public and self-collected datasets, outperforming all selected baseline methods in the classification task.

Key words: Transformer architecture; LSTM-FCN model; traffic images; traffic classification; two-stage fusion classifier

收稿日期:2025-09-23;修回日期:2025-11-07

基金项目:国家重点研发计划(2023YFA1009500)

作者简介:李洋洋(2001—),男,硕士生,主要研究方向为网络空间安全。E-mail:2052147247@qq.com

网络流量分析在网络安全中具有重要作用,对于网络入侵检测以及后续针对性防护具有重要意义。网络流量分类技术是网络流量分析中的重要一环。传统的流量分类方法存在两个问题:1)对流量本身的特征利用不充分;2)模型的泛化能力有限。为对流量中特征进行更充分利用,提高分类效果,同时适应更多不同的流量分类场景,本文提出了一种基于深度学习流量分类方法:多维信息图像加密流量分类方法(Multi-dimensional Information Image Encryption Traffic Classification Method, MT)。本文主要工作如下:

1)提出了一种新型流量图像构造方法。考虑到加密流量拥有包长度、包头和载荷等多个维度特征,同时拥有数据包级别和流级别等不同粒度的特点,构造了一种能够表征其特性的流量图像。

2)设计了一个端到端的流量分类框架 MT。该框架通过并行的整体特征提取器与时序特征提取器分别捕捉流量的空间模式与时间依赖,最终通过双阶段融合分类器决策,实现了对多维度特征的学习与高效分类。

3)在多个公开数据集以及自采集数据集上进行了广泛验证。实验结果表明,MT 在多种加密流量分类任务中均取得了领先的准确率与 F1 分数,证明了其有效性。

1 相关工作

目前典型的网络流量分类方法主要有4种,分别是基于端口的方法、基于特征匹配的方法、基于数据统计原理的机器学习的方法和基于深度学习的流量分类方法。

1.1 基于端口和特征匹配的流量分类方法

网络发展早期,服务通常与固定端口绑定,使得基于端口号的流量分类方法直接有效。Moore等^[1]在2005年的研究即采用此类方法。然而,端口随机化技术的普及削弱了该方法的适用基础。

为应对上述挑战,研究重点转向基于负载特征匹配的方法,主要包括固定字符串匹配与正则表达式匹配两种技术路线^[2]。2010年,黄昆等^[3]提出一种面向深度包检测的紧凑正则表达式匹配算法。随着加密协议的广泛应用,网络数据多以密文传输,字节分布随机性增强,使得基于特征匹配的方法逐渐失效。

1.2 基于机器学习的流量分类方法

机器学习在文本分类等领域取得了很好的效

果,如K近邻算法(K-Nearest Neighbors, KNN)^[4]。流量与文本数据的相似性推动机器学习向流量分类迁移。2012年,张建等^[5]利用随机森林(Random Forest, RF)等机器学习算法进行流量分类。2016年,Draper-Gil等^[6]将K均值聚类算法(K-means)与KNN相融合,规避了基于深度包检测方法的不足。2019年,Cai等^[7]通过结合修正互信息和RF算法设计了一种新的混合特征选择算法,提高了流量分类效率。但机器学习应用于多类流量分类任务时,依赖专家手动设计特征成为主要瓶颈。

1.3 基于深度学习的流量分类方法

随着卷积神经网络(Convolutional Neural Network, CNN)等深度学习方法的提出,特征提取不再依赖人工设计,而可通过特定网络架构自动完成。2019年,Liu等^[8]提出FS-Net,使用循环神经网络(Recurrent Neural Network, RNN)与长短期记忆网络(Long Short-Term Memory, LSTM)实现流量分类;2020年,Lotfollahi等^[9]提出Deep packet,结合CNN与栈式自动编码器(Stacked Autoencoder, SAE);2021年,Lin等^[10]提出TSCRNN,融合CNN与RNN,提取抽象特征并学习时序信息。

2017年问世的Transformer凭借其编码器和解码器结构,在自然语言处理(Natural Language Processing, NLP)与计算机视觉(Computer Vision, CV)中表现优异,其架构被迁移至流量分类任务。2024年,Liu等^[11]提出ATVTISC,整合包视觉Transformer、LSTM与动态加权函数,取得良好效果。随后,研究人员探索基于Transformer的预训练方法,如ET-BERT^[12]、Lens^[13]、YaTC^[14]等,在部分场景性能突出。然而,由于流量数据中高级语义较为匮乏,预训练模型对分类任务性能的提升仍较为有限。

流量数据虽与自然语言有着类似的数据时序结构,但流量数据所蕴含的高级语义信息比自然语言少得多,且包头和载荷中包含的对分类有关的信息不均匀,数据包长度在流量分类中发挥重要作用。为探索能够充分利用流量特征的流量分类方法,本文提出一种综合考虑包头、载荷和包长度的流级别流量分类方法 MT。

2 利用流量图像的加密流量分类方法

MT由数据预处理、整体特征提取、时序特征提取和双阶段融合分类器4个模块组成,如图1所示。

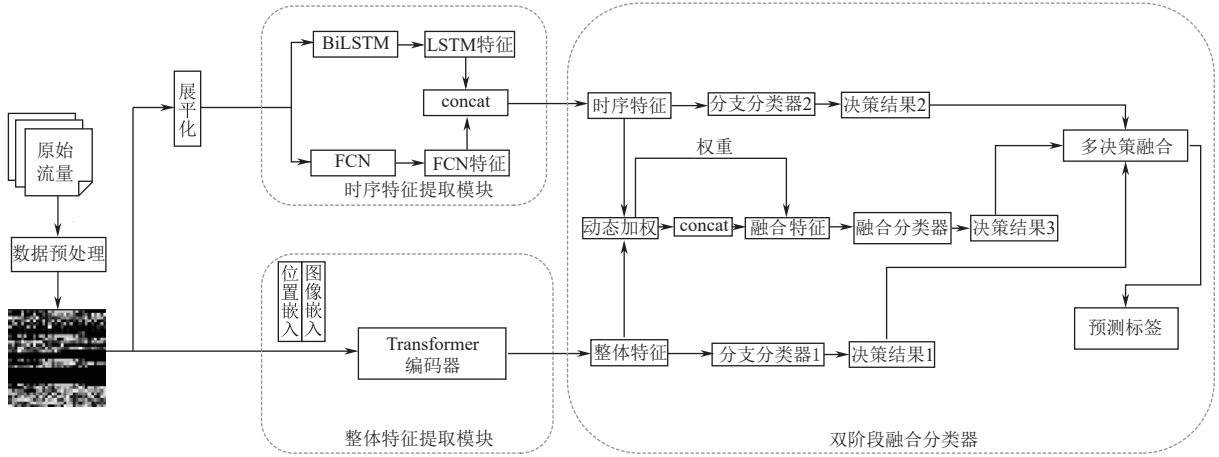


图1 MT框架整体流程图

2.1 数据预处理

原始流量包含结构不同的数据,为便于后续模块特征提取和模型学习,进行数据预处理。如图2所示,数据预处理包括划分流和生成流量图像两个步骤,将原始流量转换为流量图像。

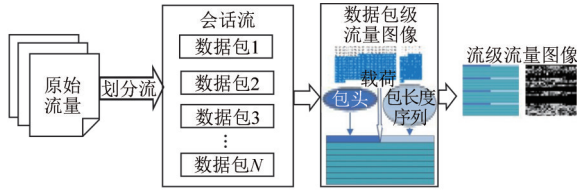


图2 数据预处理流程图

2.1.1 划分流

首先对原始数据使用五元组进行聚类,将原始数据转换为单向数据流。对这些原始数据的处理按照源IP、目的IP、源端口、目的端口、传输协议进行流的划分^[15]。

本文研究更有价值的双向会话流。因此,根据时间顺序对双向流的时间戳进行排序,将单向流组合成会话流,表示为^[11]

$$S_{\text{session}} = \{S \mid S \in (S_{A \rightarrow B} \cup S_{B \rightarrow A})\} \quad (1)$$

式中: $S_{A \rightarrow B}$ 表示源IP为A、目的IP为B的流; $S_{B \rightarrow A}$ 表示源IP为B、目的IP为A的流;符号 $\cup$ 表示合并操作,在合并过程中,按照时间戳对包进行排序。

2.1.2 生成流量图像

数据预处理阶段实施流量匿名化,剔除IP地址并随机化端口号,以消除敏感信息并增强数据隐私性,同时保留了其余12 Byte对分类有效的关键信息。

提取流中的包长度序列,该特征被证明对应用标识具有高度鉴别力。FS-Net^[8]仅依赖此特征,即在一个18类应用的公开数据集上取得了99.14%的真阳率。

载荷中拥有对分类有效的潜在信息,提取流中前4个数据包IP层载荷的前224个Byte。载荷长度超过224个Byte时,只提取前224个Byte的信息,载荷长度不足224 Byte时进行补零填充。

随后,依据本文设计的图像化框架,将处理后的包头信息、包长度序列及载荷内容分别映射至图像通道中。具体结构如图3所示,其中左侧为生成的流量灰度图像,右侧则示意了各信息在图像中的分布:红色表示除IP地址外的其余包头信息,绿色代表包长度序列,蓝色对应载荷部分。

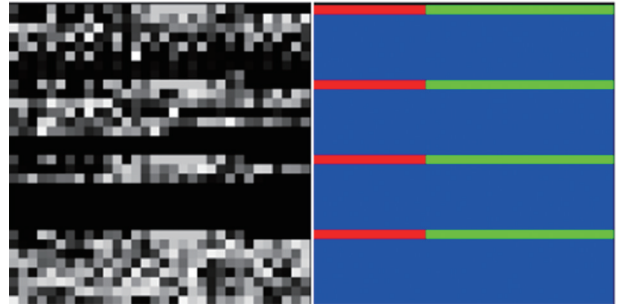


图3 流量图像示意

在图像生成过程中,每条流以前4个数据包为输入,构建32×32的灰度图像。每个数据包占用8行像素位置,其中首行包含12个像素位置的非IP包头信息及20个像素位置的包长度序列,其余7行用于存放载荷数据。在数据转换层面,包头与载荷中的原始字节值被直接映射到0~255的灰度区间,并作为对应的像素值填入图像。为了将包长度转换为图像像素值(0~255),建立如下映射机制:首先,统计所有流中数据包长度的最大值 $L_{\max}$ 与最小值 $L_{\min}$,随后通过以下公式将原始包长度 L 映射至灰度范围:

$$F(L) = \left\lfloor \frac{(L - L_{\min}) \times 255}{L_{\max} - L_{\min}} \right\rfloor \quad (2)$$

由于包长度序列在流级别分类中具有较高信息价值,本文在图像中对其进行了4次嵌入,以增强该特征对分类模型的影响。

2.2 时序特征提取

时序特征模块利用LSTM-FCN(Long Short-Term Memory-Fully Convolutional Network)网络进行特征的提取。LSTM-FCN是一种结合LSTM和全卷积网络的混合模型。LSTM-FCN结合了LSTM提取序列中的长距离依赖关系和FCN局部特征提取的能力,在数据序列分类中表现优异。

输入的 32×32 图像 S_n 被展平为一个包含1 024个元素的一维向量 L_n ,其中 n 代表第 n 个流量图像。展平具体流程如图4所示。图4将尺寸为 32×32 的流量图像,按行优先的顺序将其所有像素点重塑为一个维度为 $1 \times 1\,024$ 的特征向量。这一步骤旨在将二维空间结构转换为LSTM-FCN所要求的一维输入格式。

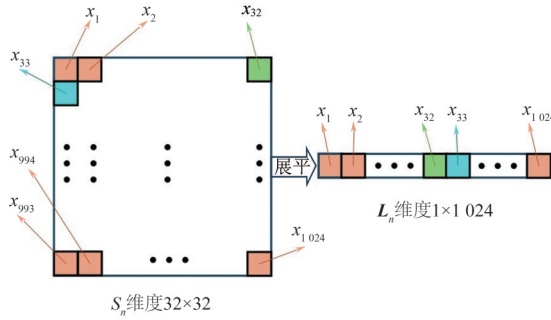


图4 展平步骤流程图

1)首先,进行双向LSTM特征提取:将序列输入双向LSTM,以捕获序列的前向与后向上下文信息。在最后一个时间步,将前向和后向的隐藏状态进行拼接,作为该分支的输出:

$$\vec{h}_t = \text{LSTM}_{\text{forward}}(L_n, \vec{h}_{t-1}) \quad (3)$$

$$\overleftarrow{h}_t = \text{LSTM}_{\text{backward}}(L_n, \overleftarrow{h}_{t+1}) \quad (4)$$

$$N_{\text{LSTM}}^n = [\vec{h}_T, \overleftarrow{h}_1] \quad (5)$$

式中: t 为时间步索引,即为序列中第 t 个位置,取值范围为 $1 \leq t \leq T$; T 为序列长度,即总时间步数; $N_{\text{LSTM}}^n \in \mathbf{R}^{2d_h}$ 为BiLSTM分支输出的特征向量; d_h 为LSTM隐藏层维度。

2)然后,利用FCN特征提取:将序列输入全卷积网络,通过一系列一维卷积层和非线性激活函数提取局部特征。该过程可表示为

$$R_{\text{FCN}}^n = \sigma(\text{Conv1d}_3(\sigma(\text{Conv1d}_2(\sigma(\text{Conv1d}_1(L_n))))) \quad (6)$$

式中: Conv1d_k 表示第 k 个一维卷积层; $\sigma(\cdot)$ 为激活函数; $R_{\text{FCN}}^n \in \mathbf{R}^{d_{fc}}$ 为FCN分支输出的特征向量; d_{fc} 为

FCN隐藏层维度。

3)最终,将两个分支提取的特征向量进行拼接,形成综合的时序特征 $F_s \in \mathbf{R}^{(2d_h + d_{fc})}$:

$$F_s = \text{Concat}(N_{\text{LSTM}}^n, R_{\text{FCN}}^n) \quad (7)$$

2.3 整体特征提取

Transformer因其独特的编码器和解码器结构可提取更深层次的语义表征,流量中也具有潜在独特的与分类有关的语义信息,研究人员利用该架构在流量分类领域进行应用,例如ET-BERT、YaTC、ATVTISC、PEAN^[16]等方法。本文利用Transformer编码器架构,对输入的流量图像进行特征提取。整体特征提取模块的工作过程如算法1所示。

算法1 整体特征提取

输入:流量图像 S_n ,Transformer编码器的个数 n_{layers} ,整体特征维度 d_{model}

输出:整体特征 F_g

1. $E_{\text{PK}} = \text{Embedding}(S_n)$
2. $E_{\text{P}} = \text{PositionEmbedding}(S_n)$
3. $E_1 = \text{Addition}(E_{\text{PK}}, E_{\text{P}})$
4. for $i = 1$ to n_{layers} do:
5. $L_{N_i} = \text{LayerNorm}(E_1)$
6. $W_{\text{mhsa}} = \text{MultiHeadSelfAttention}(L_{N_i}, d_{\text{model}})$
7. $C_R = \text{Addition}(W_{\text{mhsa}}, E_1)$
8. $E_1 = \text{FeedForward}(C_R, d_{\text{model}})$
9. end for
10. $F_g = E_1[R_{\text{CLS}}]$

首先,对图像 S_n 进行分片和嵌入(Embedding),将 32×32 的图片分割成256个 1×4 的局部图像块,其中每个局部图像块包含4个像素值,随后通过线性变换将每个图像投影到高维空间:

$$E_{\text{PK}} = \text{Embedding}(S_n) = W_e \cdot S_n + b_e \in \mathbf{R}^{256 \times d_{\text{model}}} \quad (8)$$

式中: W_e 为可学习的权重矩阵; b_e 为偏置项; d_{model} 为Transformer的隐藏维度。

然后,进行位置编码与输入嵌入。为保留图像分片的空间位置信息,引入位置编码:

$$E_{\text{P}} = \text{PositionEmbedding}(S_n) \in \mathbf{R}^{256 \times d_{\text{model}}} \quad (9)$$

将分片嵌入与位置编码逐元素相加,得到最终的输入嵌入表示:

$$E_1 = \text{Addition}(E_{\text{PK}}, E_{\text{P}}) \in \mathbf{R}^{256 \times d_{\text{model}}} \quad (10)$$

同时,在输入序列前添加一个可学习的分类令牌(Class Token) $R_{\text{CLS}} \in \mathbf{R}^{1 \times d_{\text{model}}}$,形成完整的输入序列 $E_1 \in \mathbf{R}^{257 \times d_{\text{model}}}$ 。

输入嵌入经过 n_{layers} 层Transformer编码器的逐层处理。对于每一层的处理如下:1)进行层归一化和多头注意力机制:

$$L_{N_i} = \text{LayerNorm}(E_1) \quad (11)$$

$$\mathbf{W}_{\text{mhsa}} = \text{MultiHeadSelfAttention}(L_{N_i}, d_{\text{model}}) \quad (12)$$

然后,经过残差连接:

$$\mathbf{C}_R = \text{Addition}(\mathbf{W}_{\text{mhsa}}, \mathbf{E}_1) \quad (13)$$

最后,通过前馈网络进行处理:

$$\mathbf{E}_1 = \text{FeedForward}(\mathbf{C}_R, d_{\text{model}}) \quad (14)$$

经过所有 Transformer 层处理后,取 $\mathbf{E}_1$ 中所有分类令牌 R_{CLS} 对应的输出作为整体特征表示:

$$\mathbf{F}_g = \mathbf{E}_1[R_{\text{CLS}}] \in \mathbb{R}^{d_{\text{model}}} \quad (15)$$

该全局特征聚合了所有流量图像分片的信息,能够有效捕捉图像的整体结构和语义内容。

2.4 双阶段融合分类器

双阶段融合分类器包含两个阶段的融合策略。特征级融合策略通过将时序特征和整体特征加权融合得到融合特征。决策级融合策略将时序特征、整体特征和经过特征级融合阶段得到的融合特征分别送入对应的分类器中,得到3个分类决策结果,对决策结果进行融合得到最终的预测结果。

2.4.1 特征级融合策略

利用特征融合函数将得到的时序特征 $\mathbf{F}_s$ 和整体特征 $\mathbf{F}_g$ 进行动态加权融合。然后送入分类器中得到融合路径的分类决策结果。具体见算法2。

算法2 特征级融合工作过程

输入:整体特征 $\mathbf{F}_g$, 时序特征 $\mathbf{F}_s$

输出:决策结果 R_{Result}^3

1. $\mathbf{F}_{g,\text{proj}} = \text{ReLU}(\text{Linear}(\mathbf{F}_g))$
2. $\mathbf{F}_{s,\text{proj}} = \text{ReLU}(\text{Linear}(\mathbf{F}_s))$
3. $\mathbf{R}_{\text{combined}} = \text{Concat}(\mathbf{F}_{g,\text{proj}}, \mathbf{F}_{s,\text{proj}})$
4. $\alpha_g, \alpha_s = \text{DynamicWeighting}(\mathbf{R}_{\text{combined}})$
5. $\mathbf{v} = \alpha_g \cdot \mathbf{F}_{g,\text{proj}} + \alpha_s \cdot \mathbf{F}_{s,\text{proj}}$
6. $R_{\text{Result}}^3 = \text{Softmax}(\text{Linear}(\text{ReLU}(\text{Linear}(\mathbf{v}))))$

算法中 Linear 表示全连接层, ReLU 表示激活函数, Concat 表示拼接操作, DynamicWeighting 表示动态加权机制^[11]。该机制依据动态加权函数,自动计算来自不同特征提取模块特征的最佳融合权重,省去了人工实验寻找权重的繁琐过程。函数中的温度系数用于调节权重平衡,防止特征模块失效^[17]。

2.4.2 决策级融合策略

为避免特征级融合可能导致错误累积现象,本文采用决策级融合策略。通过多个分类器的决策结果提升模型的泛化能力。同时,当某一特征的数据源质量较差时,多个决策融合策略仍可以提供较好的分类性能,提高整体分类模型的鲁棒性。如图1所示,在决策级融合阶段,将整体特征

送入分类器的决策结果1记为 R_{Result}^1 , 将时序特征提取送入分类器的决策结果2记作 R_{Result}^2 , 将特征级融合策略得到融合特征送入分类器的决策结果记作 R_{Result}^3 , 将最终决策结果记作 R_{Result} , 即:

$$R_{\text{Result}} = \beta R_{\text{Result}}^1 + \lambda R_{\text{Result}}^2 + R_{\text{Result}}^3 \quad (16)$$

式中, β 和 λ 是超参数, 可以控制不同决策结果所占的比重, 对最终预测分类结果产生影响。最终分类结果记为 $R_{\text{ClassResult}}$, 表示为

$$R_{\text{ClassResult}} = \text{ArgMax}(R_{\text{Result}}) \quad (17)$$

式中: $\text{ArgMax}(\cdot)$ 代表返回使函数最大的输入参数, 即选取总决策结果 $R_{\text{ClassResult}}$ 中概率最大的类别, 即为多个决策融合后得到的预测结果。

3 实验验证

实验设备为 Intel(R)Core(TM)i9-14900K 处理器, 64 GB 内存, NVIDIA GeForce RTX4070(16 GB) 显卡, 编程语言为 Python3.11, 实验模型训练库为 Pytorch 2.5。超参数 β 和 λ 的值均设置为 0.4。

3.1 数据集及实验设置

本文实验采用 ISCXVPN-nonVPN2016^[6]、ISCX-Tor2016^[18]、USTC-TFC2016^[19] 和自采集数据集共 4 个数据集, 划分 5 个不同的流量分类任务。其中自采集数据集中包含 24 种不同类型的恶意流量。

任务 1: 对 ISCXVPN-nonVPN2016 数据集中的 6 类 nonVPN 流量进行服务分类。任务 2: 对 ISCXVPN-nonVPN2016 数据集中的 6 类 VPN 流量进行服务分类。任务 3: 对 ISCXTor2016 数据集中 16 类流量进行服务类型检测。任务 4: 对 USTC-TFC2016 数据集中 17 类流量进行应用分类。任务 5: 是一个 25 分类任务, 数据来源于自采集数据集中的 24 类恶意流量, 以及 1 类从 ISCXVPN-NonVPN2016 中筛选出的正常流量, 旨在进行恶意流量与正常流量的精细识别。

3.2 评价指标

为系统评估 MT 模型在多分类任务中的性能, 本文采用准确率 (Accuracy) R_{Accuracy} 、宏 F1 值 (Macro-F1) $F1_{\text{Macro}}$ 两种评价指标进行衡量。其中, 真阳性 (True Positive, TP) N_{TP} 表示模型正确预测为正类的样本数; 假阳性 (False Positive, FP) N_{FP} 表示模型将负类错误预测为正类的样本数; 假阴性 (False Negative, FN) N_{FN} 表示模型漏判的正类样本数。

对于每个类别, 首先计算 3 类基础指标, 召回率 (Recall) R_{Recall} 反映模型捕捉正类的能力; 精确率 (Precision) $R_{\text{Precision}}$ 衡量预测正类的可靠性, 其数值

受 N_{FP} 直接影响; $F1$ 值作为召回率与精确率的调和平均数,用于权衡这两个指标。

$$R_{Recall} = \frac{N_{TP}}{N_{TP} + N_{FN}} \quad (18)$$

$$R_{Precision} = \frac{N_{TP}}{N_{TP} + N_{FP}} \quad (19)$$

$$F1 = 2 \times \frac{R_{Precision} \times R_{Recall}}{R_{Precision} + R_{Recall}} \quad (20)$$

针对 N_c 个类别的任务,采用宏平均策略消除类别规模偏差。该方法赋予所有类别同等权重,尤其适用于长尾分布数据。计算公式为

$$F1_{Macro} = \frac{1}{N_c} \sum_{i=1}^{N_c} F1_i \quad (21)$$

式中: N_c 代表类的数量; $F1_i$ 是第 i 个类的 $F1$ 分数。

整体准确率(Accuracy) A_c 的计算方式为

$$A_c = \frac{1}{S_{Total}} \sum_{i=1}^{N_c} N_{TP_i} \quad (22)$$

式中: N_{TP_i} 为第 i 个类别的模型正确预测为正类的样本数; S_{Total} 为所有类别样本总数; N_c 为类别数。

3.3 参数选择探究

为达到最好的分类效果,探索两个重要参数的取值:Transformer 编码器的层数 n_{layers} 和特征融合分类器中的温度系数。参数探究选择 ISCXVPN-nonVPN2016 数据集进行 12 类别服务划分实验。

1) Transformer 编码器的层数:进行实验来探究选取 Transformer 编码器层数。实验中,温度系数参数设置为 200,选取任务 5 进行实验。为更大程度遍历 n_{layers} 的范围,设置 n_{layers} 的个数为 2~12,步长为 2。实验结果见图 5。

由图 5 可得, n_{layers} 的值为 4 时已经达到很好的实验效果。考虑到 n_{layers} 的值越大会导致性能开销越大,因此,本文后续实验中 n_{layers} 的值选取为 4。

2) 温度系数:本节对特征融合分类器中超参数温度系数的选择进行研究。温度系数的选取从 1~800、跨度为 20 进行实验。实验结果见图 6。

在图 6 中可以看到,当温度系数为 100 时,实验准确率达到了最佳 99.01%。因测试集中各类别的样本量比较均衡,在样本均衡的场景下,准确率比 $F1$ 值更具实验价值。因此,本文后续实验中温度系数设置为 100。

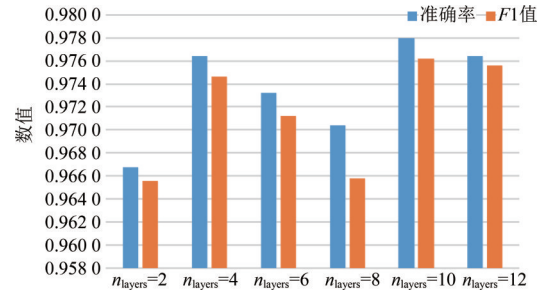


图5 不同 n_{layers} 值实验结果

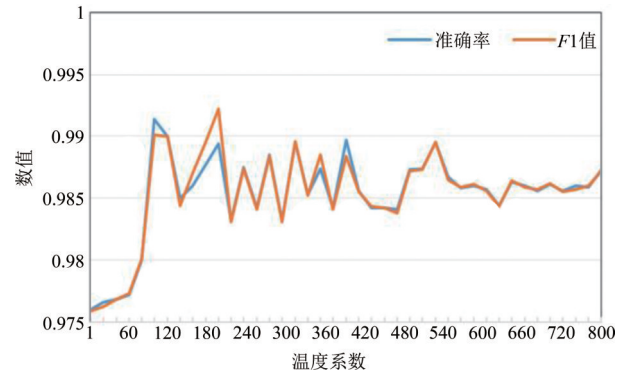


图6 不同温度系数下的实验结果

3.4 对比实验

将本文方法与近些年来表现优异的流量分类方法进行对比实验。首先评估 MT 在多种流量分类任务上的性能,并与 1D-CNN^[20]、Deep packet^[9]、TSCRNN^[10]、FS-Net^[8]、PEAN^[16] 等基线实验进行比较。实验结果如图 7 所示。

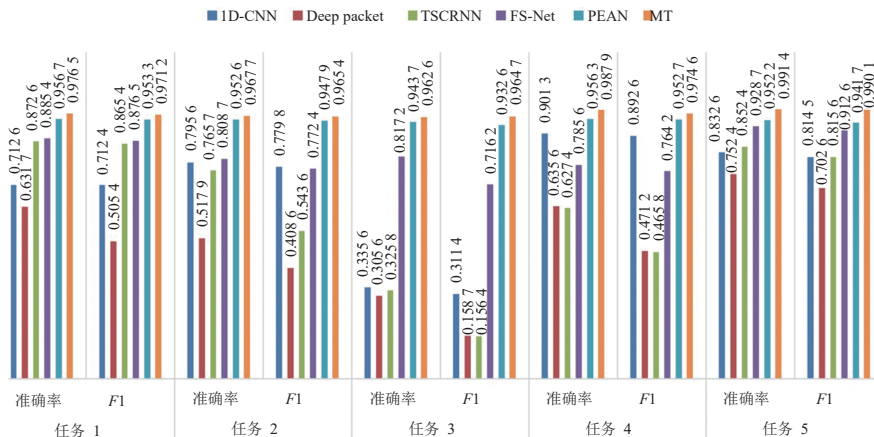


图7 MT和基线方法对比实验结果

由图7分析可得,本文方法在5个分类任务中均优于所有基线实验。在不同的分类任务中,其他基线方法受分类场景的影响较大,MT则在所有任务中表现优异,体现了MT对不同应用场景的适应性。

3.5 消融实验

为验证本文方法各个模块设计的合理性,分别对不同特征提取模块和双阶段融合策略进行消融实验。

3.5.1 特征提取模块消融实验

为探究整体特征和时序特征提取模块的有效性,本文针对这两个特征提取选取任务1模块进行消融实验,实验结果见表1。

表1 特征提取模块消融实验结果

模块设置	准确率	F1
CNN+时序	0.912 5	0.911 2
MT(w/o 整体)	0.902 4	0.905 5
MT(w/o 时序)	0.923 7	0.923 4
MT	0.976 5	0.971 2

表1中CNN+时序表示利用CNN代替本文的整体特征提取模块;MT(w/o 整体)表示本文方法去掉了整体特征提取模块,只采用时序特征提取模块进行实验;MT(w/o 时序)表示本文方法去掉了时序特征提取模块只采用整体特征提取模块进行实验。

由表1可得,完整的MT方法拥有最好的实验效果。整体特征提取模块使用Transformer编码器架构比CNN架构要更好。利用Transformer编码器架构的整体特征提取模块和利用LSTM-FCN的时序特征提取模块对分类效果都有重要影响。

3.5.2 双阶段融合策略消融实验

为验证本文双阶段融合策略的有效性,针对决策级融合和特征级融合进行消融实验。

本次实验设置了两个对照组,对照组1去掉了决策级融合策略,对特征级融合阶段得到的融合特征送入到分类器中得到的策略 R_{Result}^3 ,直接进行计算得到最终的预测结果 $R_{\text{ClassResult}}$,即

$$R_{\text{ClassResult}} = \text{ArgMax}(R_{\text{Result}}^3) \quad (23)$$

对照组2去掉了特征级融合策略,对整体特征和时序特征分别送入分类器中得到的决策结果 R_{Result}^1 和 R_{Result}^2 进行决策级融合,最终的预测结果 $R_{\text{ClassResult}}$ 表示为

$$R_{\text{ClassResult}} = \text{ArgMax}(R_{\text{Result}}^1 + R_{\text{Result}}^2) \quad (24)$$

采取任务1进行实验验证,结果如表2所示,其

中MT(w/o 决策级)是对照组1的实验结果,MT(w/o 特征级)是对照组2的实验结果。由实验结果可得,没有使用特征级融合策略或者决策级融合策略会使MT方法的性能下降,证明了双阶段融合策略的有效性。

表2 双阶段策略对MT方法影响的实验结果

策略设置	准确率	F1
MT(w/o 决策级)	0.950 1	0.948 7
MT(w/o 特征级)	0.940 3	0.932 1
MT	0.976 5	0.971 2

3.6 计算效率分析

为验证双阶段融合特征分类策略的实用性,选取任务1进行实验验证。在分类阶段,模型的吞吐量为单位时间内分类的样本数,而效率得分为准确率与吞吐量的乘积,代表单位时间内分类正确的样本数量,其数值越大表示正确分类的效率越高。从表3可以看出,双阶段融合策略的效率得分最高,表示其分类效率最高。

表3 MT方法效率分析实验结果

设置	准确率	吞吐量/s ⁻¹	效率得分
MT(w/o 决策级)	0.950 1	1 310.2	1 244.821 0
MT(w/o 特征级)	0.940 3	1 330.1	1 250.693 0
MT	0.976 5	1 291.8	1 261.442 7

4 结束语

本文介绍了一种新的网络流量分类方法MT,利用流量转换为图像的方法,在多种分类场景下均表现出优异性能。MT充分考虑了流量特征的整体结构特点和多维度特征,提出一种综合考虑载荷、包长度序列和流内数据包间关系等多维度特征的预处理方式。基于Transformer的整体特征提取方法能提取更深层次的分类信息。利用LSTM-FCN的时序特征提取模块能更好的提取包头、载荷和包长度序列中的长距离和短距离之间的性质。此外,设计的特征级和决策级双阶段融合策略,提高了模型的分类性能和鲁棒性。实验结果表明,与其他大部分基线方法相比,本文方法在多种场景下均展示了优异的分类能力。未来计划对双阶段特征性能进行进一步探索。

参考文献:

- [1] MOORE A W, PAPAGIANNAKI K. Toward the accurate

- identification of network applications[M]//DOVROLIS C. Passive and Active Network Measurement. Berlin, Germany: Springer, 2005:41-54.
- [2] 陈传通. 基于正则表达式匹配的网络流量识别系统的研究与实现[D]. 济南: 山东大学, 2013:17-25..
- [3] 黄昆, 张大方, 谢高岗, 等. 一种面向深度数据包检测的紧凑型正则表达式匹配算法[J]. 中国科学: 信息科学, 2010, 40(2):356-370.
- [4] WANG Z G, HAMZA W, SONG L F. K-Nearest Neighbor augmented neural networks for text classification[DB/OL]. (2017-08-25) [2025-11-06]. <https://arXiv.org/abs/1708.07863>.
- [5] 张建, 武东英, 刘慧生. 基于随机森林的流量分类方法[J]. 信息工程大学学报, 2012, 13(5):621-625
- [6] 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. Setúbal, Portugal: SciTePress, 2016:407-414.
- [7] CAI Z Z, JIANG B, LU Z G, et al. IsAnon: flow-based anonymity network traffic identification using extreme gradient boosting[C]//Proceedings of the 2019 International Joint Conference on Neural Networks. Piscataway, USA: IEEE, 2019:1-8.
- [8] LIU C, HE L T, XIONG G, et al. FS-Net: a flow sequence network for encrypted traffic classification[C]//Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications. Piscataway, USA: IEEE, 2019:1171-1179.
- [9] 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.
- [10] LIN K D, XU X L, GAO H H. TSCRNN: a novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT[J]. Computer Networks, 2021, 190:No.107974.
- [11] LIU Y, WANG X, QU B, et al. ATVITSC: a novel encrypted traffic classification method based on deep learning[J]. IEEE Transactions on Information Forensics and Security, 2024, 19:9374-9389.
- [12] LIN X J, XIONG G, GOU G P, et al. ET-BERT: a contextualized datagram representation with pre-training transformers for encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2022. New York, USA: ACM, 2022: 633-642.
- [13] WANG Q N, QIAN C, LI X C, et al. Lens: a foundation model for network traffic[DB/OL]. (2024-02-06) [2025-11-06]. <https://arXiv.org/abs/2402.03646>.
- [14] ZHAO R J, ZHAN M W, DENG X W, et al. Yet another traffic classifier: a masked autoencoder based traffic transformer with multi-level flow representation[C]//Proceedings of the AAAI Conference on Artificial Intelligence. Palo Alto, USA: AAAI Press, 2023, 37(4):5420-5427.
- [15] DAINOTTI A, PESCAPE A, CLAFFY K C. Issues and future directions in traffic classification[J]. IEEE Network, 2012, 26(1):35-40.
- [16] LIN P, YE K J, HU Y S, et al. A novel multimodal deep learning framework for encrypted traffic classification[J]. IEEE/ACM Transactions on Networking, 2023, 31(3): 1369-1384.
- [17] HINTON G, VINYALS O, DEAN J. Distilling the knowledge in a neural network[DB/OL]. (2015-03-09) [2025-11-06]. <https://arXiv.org/abs/1503.02531>.
- [18] 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. Setúbal, Portugal: SciTePress, 2017:253-262.
- [19] WANG W, ZHU M, ZENG X W, et al. Malware traffic classification using convolutional neural network for representation learning[C]//Proceedings of the 2017 International Conference on Information Networking. Piscataway, USA: IEEE, 2017:712-717.
- [20] WANG W, ZHU M, WANG J L, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics. Piscataway, USA: IEEE, 2017:43-48.

(编辑: 邵 华)