Website：ycyk.brit.com.cn

PTNet：一种面向加密流量分类的半监督并行Transformer网络

冯舒文，李育恒，白旭洋
（北京遥测技术研究所 北京 100076）

摘要：随着网络加密协议的广泛使用，传统的网络流量分类技术面临很大的挑战。目前的方法具有以下局限性：一是模型高度依赖深度特征，这要求有标注训练数据集的规模足够大，否则模型难以在新的数据上进行泛化；二是模型仅专注于流量的一个模态特征，不同类别流量的同一模态的特征区分度可能不够明显。针对这些问题，本文提出了一种基于深度学习的加密流量分类模型Parallel Transformer Net（并行转换网络，PTNet）。该模型基于预训练-微调的半监督思想，充分利用网络中大量无标签流量数据进行预训练，然后在少量有标签数据的基础上进行微调。此外，该模型并行提取了载荷和包长序列两个模态的流量特征，进行多模态的特征融合，并在三种不同的流量分类任务与相应的数据集（Android、USTC-TFC和CSTNET-TLS1.3，均为公开的数据集）上都表现出很好的效果，分类准确率分别达到95%、98%和97%。

关键词：网络流量分类；加密流量；深度学习；PTNet
中图分类号：TP393; TP18 **文献标志码：**A **文章编号：**2095-1000(2024)03-0043-09
DOI：10.12347/j.ycyk.20231130001
引用格式：冯舒文，李育恒，白旭洋. PTNet：一种面向加密流量分类的半监督并行Transformer网络[J]. 遥测遥控，2024，45(3)：43–51.

PTNet: A Semi-supervised Parallel Transformer Network for Encrypted Traffic Classification

FENG Shuwen，LI Yuheng，BAI Xuyang
（Beijing Research Institute of Telemetry, Beijing 100076, China）

Abstract: With the widespread use of network encryption protocols, traditional network traffic classification technology has been challenged. The current method has the following limitations: first, the model is highly dependent on the depth feature, which requires the labeled training data set to be large enough in scale, otherwise the model will have difficulty generalizing to new data; second, the model only focuses on one modal feature of traffic, and the feature differentiation of the same mode of traffic from different categories may not be obvious. To solve these problems, a deep learning-based encryption traffic classification model called Parallel Transformer Net (PTNet) is proposed in this paper. Based on the semi-supervised idea of pre-training and fine-tuning, the model makes full use of a large amount of unlabeled traffic data on the network for pre-training, and then fine-tunes on the basis of a small amount of labeled data. Additionally, the model extracts the flow characteristics of load and packet length sequences in parallel to carry out multi-mode feature fusion. Three different traffic classification tasks and their corresponding datasets (Android, USTC-TFC, and CSTNET-TLS1.3) show good results, with classification accuracies reaching 95%, 98%, and 97%, respectively.

Keywords: Network traffic classification; Encrypted traffic; Deep learning; PTNet
Citation: FENG Shuwen, LI Yuheng, BAI Xuyang. PTNet: A Semi-supervised Parallel Transformer Network for Encrypted Traffic Classification[J]. Journal of Telemetry, Tracking and Command, 2024, 45(3): 43–51.

0 引言

网络流量分类是网络管理和网络安全领域的一项关键技术，旨在识别来自各种应用或Web服务流量的类别[1]，为后续流量处理奠定基础。近年来，随着互联网技术的飞速发展，加密流量被广

收稿日期：2023-11-30；修回日期：2024-03-06

泛应用于保护互联网用户的隐私和提高数据匿名性。然而，网络犯罪分子也利用加密流量来逃避监控，这给流量分类带来了很大的挑战。传统的从载荷中抓取数据报文中模式和关键字的方法，即深度包检测(Deep Packet Inspection, DPI)，无法应用于加密后的流量。因此，研究者们基于流量统计特征，采用机器学习算法对流量进行分类。这种方法对加密流量有效，但过于依赖专家经验进行特征提取。此外，由于加密技术的快速发展，针对特定类型加密流量的流量分类方法不能很好地适应新的环境或未知的加密策略[2]。因此，如何在多样的加密流量中捕捉隐式的、鲁棒的模式特征进行分类识别也是领域内的一大关键。为了解决上述问题，加密流量分类的方法也在不断地发展进步。

早期的流量分类方法是基于端口号的方法，但是这种方法不适用于加密流量分类，并且现在的应用程序会避免使用标准默认的注册端口号混淆其流量。后来TV Ede等[3]利用加密流量有效载荷和明文信息（如证书构造指纹，并对指纹匹配进行分类）进行检测，这种方法称之为数据包检测(Data Packet Inspection, DPI)。然而，这些方法不适用于新出现的加密技术(如TLS 1.3，传输层安全性协议1.3版)，因为明文变得更加稀疏或混淆。为此，一些研究人员[4,5]提取统计特征，采用经典机器学习算法对加密流量进行无明文处理。这些方法高度依赖专家设计的特征，泛化能力有限。随着深度学习技术的发展，采用深度学习[6,7]自动从原始流量中学习复杂模式进行流量识别，取得了显著的性能提升。然而，这些方法高度依赖于标记训练数据的数量和分布，并且只专注于流量的单个模态特征，容易造成模型偏差，难以适应新环境的流量。

近年来，预训练模型在自然语言处理[8]、计算机视觉[9]等广泛领域取得了重大突破，而多模态方法在文本、语音、视觉等方面取得了令人瞩目的发展。在加密流量分类领域，HE Hongye应用了预训练技术[10]，WANG Xin等提出了流量多特征的分类模型[11]，在VPN流量分类上都得到了明显改进。受此启发，本文将半监督预训练微调技术与多特征融合分类技术应用于加密流量分类中。

本文提出了一种新的加密流量分类半监督模型，称为Parallel Transformer Net。它旨在从大规模无标签的加密流量中学习到通用流量载荷与包长序列的特征表示。首先，将流量的载荷特征与序列特征转换为类似自然语言处理的令牌，在无标签的数据样本中进行掩码方式预训练；然后，结合特定的分类任务，使用少量有样本的数据集进行模型微调。

本文的主要内容如下：① 提出了一种加密流量分类的多模态预训练框架，该框架利用大规模未标记的加密流量载荷与包长序列来学习一系列加密流量分类任务的通用特征表示；② 针对流量两个模态数据，提出了基于掩码重构任务的预训练半监督模型；③ 提出的Parallel Transformer Net泛化能力强，在安卓移动加密应用分类、恶意软件流量分类、TLS 1.3上的加密应用分类这三个加密流量分类任务上性能较好。

1 问题定义

加密流量分类的目标是识别不同应用产生的网络流量，并将其划分为相应的类别[12]。本文模型专注于流量的载荷与包长序列特征提取，将流量按照数据抽象层次分为三个级别：字节、数据包和流。

①字节与数据包：网络流量由一段连续的数据报文组成，而每一个网络报文由若干个字节构成，在指定时间内的所有报文构成网络流量集R。R的定义如下：

$$\begin{aligned}&R=P^1,P^2,...,P^n,n=|R|\\&P^i=(X^i,B^i,T^i),1<i\leqslant n\\&X^i=(src_{\text{ip}},dst_{\text{ip}},src_{\text{port}},dst_{\text{port}},protocol)\\&B^i=\{byte^1,byte^2,...,byte^q\},0x00<byte^j\leqslant 0xff,1<j\leqslant q\\&T^i>0\end{aligned}\tag{1}$$

P^i表示流量的第i个数据包，一个数据包由一个五元组X、数据包内容B、起始时间T组成。

②流：流是由特定约束条件组成的一组数据包的集合，该约束条件即流中的各个数据包的X可以相同，也可以互换其原IP、原端口与目的IP、目的端口，符号化定义数据集中的第1个流被定义为：

$$f_l=\{P_l^1,P_l^2,...,P_l^m\},m=|f_l|\tag{2}$$

因此，原始的数据R也可以从流的角度被视作：

$$R'=\{f_1,f_1,...,f_k\},k=|R'|\tag{3}$$

给定一个数据集合R'与标签空间Z，建立一个函数映射$\phi(f_i)$，将R中的每一个f_i对应到标签空间中的一个标签中，即$\phi(f_i)=z_j$，其中z_j是标签空间Z的一个元素。

2　Parallel Transformer Net

2.1　模型整体结构

本章对多模态半监督加密流量分类模型PTNet进行了描述。首先，对PTNet的总体体系结构进行介绍，然后对它的每一个部件进行详细解释。

本文提出的PTNet体系结构包括两个分支，分别用于处理载荷和包长序列的流量特征。其中，除了对于模态深层特征提取的PTE层(Payload Transformer Encoder，有效载荷编码)与STE层(Sequence Transformer Encoder，序列载荷编码)的层数不同之外，两个分支其他的结构近乎对称。模型分为预训练状态与微调分类状态。PTNet模型整体结构如图1所示。

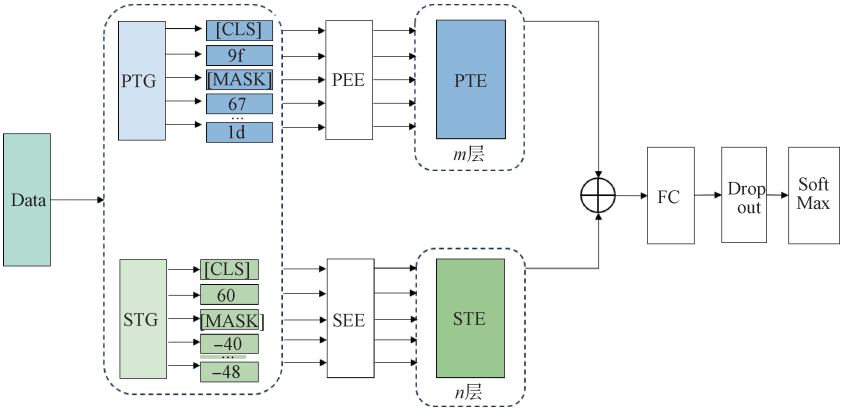

图1　PTNet模型整体结构

Fig. 1　The overall structure of PTNet

图1中，PTG(Payload Token Generation，载荷令牌生成编码器)模块和STG(Sequence Token Generation，包长序列令牌生成编码器)模块的功能分别是将载荷和包长序列转换成输入到Transformer编码器能处理的令牌数据。为了更好地在微调阶段进行分类，STG模块在将原始的载荷与包长序列数据转为令牌数据的同时，会在转换后的令牌数据前插入一个特殊的CLS(分类)令牌。这个令牌并不是由任何具体的数据转换而来，载荷与包长序列对应的CLS令牌在经历嵌入层与Transformer层的特征提取后，对应的特征向量能够视为流的全局特征表示[13]。PEE(Payload Embedding Encoder，载荷嵌入层编码器)和SEE(Sequence Embedding Encoder，包长序列嵌入层编码器)，分别用于生成载荷和包长序列的浅层特征。FC为全连接层，起到“分类器”的作用，对提取到的特征进行权重加权，从而实现对输入数据的分类。Dropout(脱落)层是在训练过程中随机将一些神经元“暂时移除”的层，可以防止模型在训练过程中过拟合，从而提高模型的泛化能力。Softmax函数是一种的激活函数，用于将神经网络的输出转换为概率分布，使得每个类别的预测概率之和为1。

数据整体训练过程为：模态数据首先需要进入PTG模块和STG模块，将载荷转换为“令牌”数据，然后两个模态的数据通过各自的嵌入层PEE和SEE，生成载荷与包长序列的浅层特征。这里的特征既包含原始的“令牌”，同时为了保留载荷与包长的时序信息，也加入了“位置”嵌入特征向量。随后，两个模态数据分别进入PTE和STE编码器进行深层次的特征提取。在预训练状态，需要对掩码的“令牌”输出进行掩码预测，以优化Transformer结构参数；在微调状态，提取各自Transformer编码器的CLS令牌输出向量，送入融合层进行分类。

2.2　令牌生成模块

2.2.1　载荷特征的令牌生成PTG

在真实的网络环境中，网络流量中包含了不同类别(如不同的应用、协议或服务)的各种流量，很难学习到一种稳定的、判别性的特征表示。对于加密流量的载荷特征提取，其实质是提取一些加密传输的握手信息，这部分信息通常位于传输

层及其以上的层次中，且通常位于一个流的前几个数据包。因此，对于一个会话流的载荷提取，设定提取流的前 n 个数据包的前 m 个字节，这种操作也有助于降低数据复杂度。在处理前 n 个数据包时，首先将每一个数据包的传输层以下的信息丢弃，然后将其 IP 地址与端口赋值 0，防止其对最终分类造成影响。对于流量载荷的最终表达，以字节为单位分割载荷数据，将载荷的每一个字节转化为 16 进制(“00”转“ff”)的字符串，最后将该字符串视为一个令牌数据，作为最终的 PEE 嵌入层输入。

2.2.2 包长序列特征的令牌生成 STG

在开放的网络环境中，不论流量是否加密，只要没有采用报文填充策略(使得所有的报文长度相同)，不同行为类型或者应用的流量包长序列会显现出一定的规律特性，这是基于包长序列特征分类方法的原理。此外，基于包长特征能够有效解决一些流量提取载荷特征贡献度不高的问题。受此启发，PTNet 模型融合了流量包长序列模态的数据，使得 PTNet 模型能够全面地分析流量，提取到的流量特征更加具备鲁棒性。因此，提取流量的前 k 个包的包长信息，设定从客户端到服务端的包长为正数，服务器到客户端的包长为负数，最后将每一个包长字符串视为一个令牌数据，作为最终的 SEE 嵌入层输入。

2.3 嵌入层

本文的嵌入层(PEE 和 SEE)通过令牌嵌入、位置嵌入的叠加来得到特征的最终嵌入。

令牌嵌入：从无标签流量生成的载荷语料库与包长序列语料库中，生成各自特征对应的字典查找表，使用字典查找表将令牌映射在表中对应索引，该索引作为令牌嵌入的输入，令牌的表示称为令牌嵌入 E_{token}[15]。输入令牌的最终隐藏向量为 $E_{\text{token}} \in R^H$，其中载荷与包长序列的嵌入维数 H 均设置为 768。

位置嵌入：流量数据的传输与顺序密切相关，由于注意力机制的影响，Transformer 在处理数据时不关注数据相对位置关系，因此使用位置嵌入来确保模型学习可以通过相对位置来关注令牌的时间关系。本文为每个输入标记分配一个与令牌嵌入相同维度的 H 维向量，以表示其在序列中的位置信息。将位置嵌入记为 $E_{\text{pos}} \in R^H$，其中嵌入维数 H 与上述令牌嵌入向量维度保持一致，设置为 768。

2.4 Transformer 编码层

2.4.1 预训练状态

在载荷方面，预训练的目的是训练一个具有字节编码能力的模型，该模型可以对浅层次的载荷嵌入向量进行进一步特征提取，形成深层次的载荷特征向量。受 BERT(Bidirectional Encoder Representation from Transformers，来自变换器的双向编码器表征量)模型的启发[8]，本文使用一种无监督预训练思想，神经网络随机屏蔽一定比例(实验中设置的比例为 15%)的网络数据包的字节(使用 MASK 令牌替换原始字节)，并尝试通过相邻字节恢复它们。预训练特征提取示意图如图 2 所示。

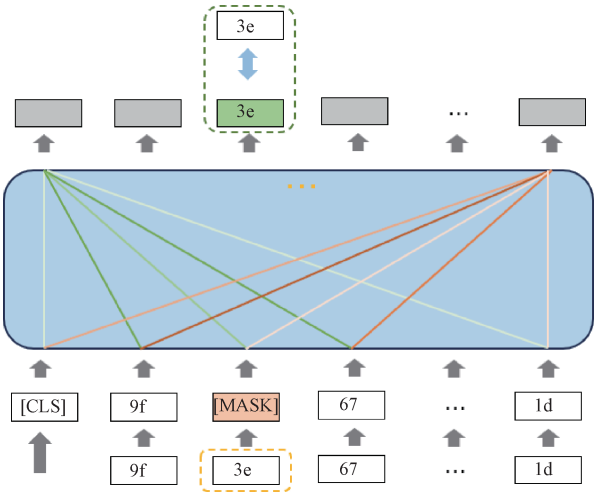

图 2 预训练特征提取示意图

Fig. 2 Pre-training feature extraction schematic diagram

在包长序列方面，预训练的目标是训练一个理解包长语义的模型。由于不同流量类型之间的包长序列具有一定的区分度，该模型可以通过掩码预测任务在大规模无标签数据上，充分提取包长序列的变换规律，使其有助于后续的分类表现。

本文选择 Transformer 作为训练模型，因为其自注意力机制允许每个令牌同时获取多个令牌的信息，从而提高了模型的表达能力和泛化能力。这种预训练方式有以下优点：

① 在预训练阶段，每个令牌的嵌入表示与其他令牌相关，因此整个流的载荷模态表示以及包长序列表示具有更强的统一性。

② 收集网络流量相对容易，但标注却很困难。由于预训练方法是无监督的，可以直接使用大量未标记的数据进行预训练，提高模型的编码能力，便于以后的模型扩展和更新。

Transformer 编码器的主要内容有多头自注意力机制、位置嵌入、剩余连接、层归一化和前馈网络。其核心部分主要是多头自注意力机制。注意力函数(Attention)的本质可以描述为一个 Query (Q)到一系列 Key-Value($K-V$)对的映射。在自注意力机制中，上述的 Q、K、V 都是由同一个值 x 分别经过三个不同的线性变换矩阵 W^Q、W^K、W^v 得到的。

自我注意机制是注意机制的一种变体，它较少依赖外部信息，更善于捕捉数据的内部相关性。多头自注意力机制的推理公式如下：

$$\text{Attention}(Q,K,V)=\text{softmax}\left(\frac{QK^{\mathrm{T}}}{\sqrt{d_k}}\right)V \tag{4}$$

$$head_i=\text{Attention}(QW_i^Q,KW_i^K,VW_i^V) \tag{5}$$

$$\text{MultiHead}(Q,K,V)=\text{Concat}(head_1,head_2,\ldots,head_h)W^O \tag{6}$$

其中 d_k 是矩阵 K 的维度，h 是多头自注意力的头数，不同的头部可以理解为多个独立并行的自注意力机制，每个自注意力机制关注序列的不同语义。因此，它可以关注网络流量数据包的不同部分。

在原始处理的令牌嵌入中，对于每一个流的载荷与包长序列，在开头添加一个 CLS 令牌。CLS 令牌将通过 Transformer 获得向量表示，同时由于自注意力机制，该向量集成了所有字节的信息，这些信息融合了不同的权重。由于 PTE 中的多头自注意力机制，在神经网络的拟合下，该向量最终可以学习到流级表示。预训练令牌嵌入示意图如图 3 所示。

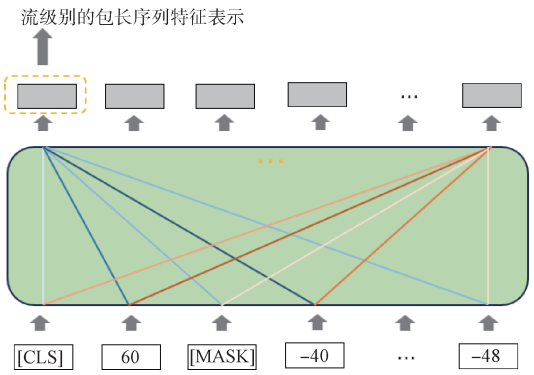

图 3　预训练令牌嵌入示意图

Fig. 3　Pre-training token embedded schematic diagram

2.4.2　微调状态

在微调状态下，舍弃预训练的掩码预测部分，将两个模态对应的[CLS]令牌嵌入向量 e_{pay}，e_{seq} 连接成 E_{f}，送入最终的分类层进行分类，如图 4 所示。

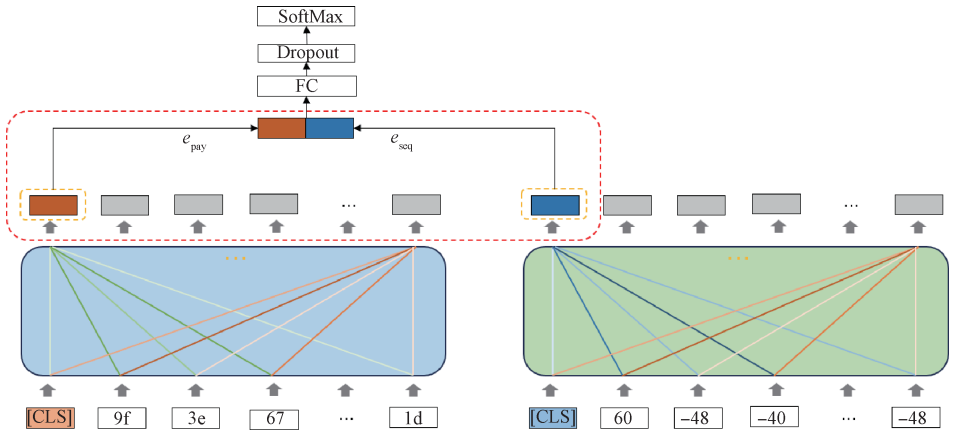

图 4　微调状态分类示意图

Fig. 4　Fine-tune the state classification diagram

公式如下所示：

$$E_{\text{f}}=\text{concat}(e_{\text{pay}},e_{\text{seq}}) \tag{7}$$

式中：e_{pay} 是 PEE 输出的令牌嵌入向量，e_{seq} 是 SEE 输出的令牌嵌入向量，E_{f} 是 CLS 令牌在 Transformer 中对应的编码向量。

2.5　分类层

该层使用两个全连接层加上 Softmax 层进行分类，全连接层可以将 E_{f} 转化为标签的概率分布。全连接的运算如下：

$$\widetilde{E}_{\text{f}}=\text{Re LU}(W_{\text{dense}}E_{\text{f}}),W_{\text{dense}}\in R^{H\times N} \tag{8}$$

N 是标签数目，定义输出 Z 为 $Z=[z_1,z_2,\ldots,z_n]$，代表在各个标签上的概率分布。

使用交叉熵损失函数，上述的概率分布与交叉熵损失可以被定义如下：

$$p_i = \frac{e^{z_i}}{\sum_j e^{z_j}},\ \text{loss} = \sum c_i \log(\mathrm{p}_i) \tag{9}$$

c_i只能是0或者1，表示当前数据是否对应该标签。

3 模型验证

本节通过3个加密流量分类任务来验证PTNet在解决不同加密场景下分类的有效性。然后，将PTNet模型与其他3种方法进行比较，并对模型的关键组成部分进行消融实验分析。

3.1 实验设置

3.1.1 数据集与下游任务

为了评估PTNet模型的有效性与泛化性，本文在几个公共数据集进行了加密流量分类任务的实验。任务与相应的数据集介绍如表1所示。

表1 数据集统计情况

Table 1 Statistics of data sets

任务	数据集名称	总样本数	标签个数
安卓移动加密应用分类	Android	48 714	24
加密恶意软件分类	USTC-TFC[14]	477 044	20
TLS1.3加密应用分类	CSTNET-TLS1.3[15]	46 372	120

任务1: 安卓移动加密应用分类任务。该任务是在标准的加密协议下，对安卓移动设备产生的流量进行应用流量分类。该数据集是本文实验人员于2022年10月到2023年11月，在安卓移动应用设备上针对常见的24类应用使用PCAPdroid工具进行抓包所得，并被命名为Android。

任务2: 加密恶意软件分类任务。该任务旨在区分真实环境中正常流量与恶意流量。实验采用USTC-TFC2016数据集，该数据集由中国科学技术大学王伟提供，由两部分组成：第一部分是2011年到2015年由捷克技术大学CTU研究人员在真实网络环境中收集的来自公共网站的十种恶意软件流量；第二部分是使用专业网络流量模拟设备收集的十种正常流量。

任务3: 基于TLS1.3的加密应用分类任务。该任务旨在针对新兴加密协议TLS1.3的加密流量进行分类识别。CSTNET-TLS1.3数据集是LIN Xinjie团队于2021年3月到7月在中国科技网(CSTNET)下收集，通过服务器名称指示字段(SNI)进行流量标注，数据集包含了120个应用程序类别。

3.1.2 数据预处理

由于包头可能会在具有强识别信息(如IP和端口[16,17])的有限集合中引入偏置干扰，并且地址解析协议(ARP)和动态主机配置协议(DHCP)的数据包与传输内容的特定流量无关，因此删除了TCP头中的以太网头、IP头、协议端口、ARP数据包和DHCP数据包。在微调阶段，随机从数据集的每个类中选择最多500个流。每个数据集按照8:1:1的比例分为训练集、验证集和测试集。

3.1.3 评估指标与实现细节

本文通过四个典型指标来评估和比较模型的性能，包括准确性(AC)、精度(PR)、召回率(RC)和F1分数[18,19]。通过计算每一类数据的AC、PR、RC和F1的平均值得到Macro Average[20](宏平均)，避免因多类数据之间的不平衡而导致结果偏倚。在预训练阶段，训练的batch-size大小为32，总步长为500 000，设置学习率为2×10^{-5}；在微调阶段，选取AdamW优化器，在预训练的模型参数的基础上进行5个epoch的微调，学习率设置为6×10^{-5}，batch-size大小为64，dropout设置为0.5。所有实验均在PyTorch1.12.0上实现，使用NVIDIA RTX 3090 GPU进行计算加速。

3.2 定量对比分析

本文将PTNet与各种先进的加密流量分类方法进行了比较，包括：

①统计特征方法：AppScanner[4]。

②深度学习方法：FS-Net[7]、Deeppacket[19]。

实验结果如表2所示。

安卓移动加密应用分类：根据表2所示，PTNet明显优于其他方法。本文的模型在准确率的表现上，相比使用载荷特征作为输入的DeepPacket深度学习方法和使用包长序列特征作为输入的FS-Net深度学习方法，分别取得了7.71%和47.35%的改进。

加密恶意软件分类：从表2所示的USTC-TFC的结果可以看出，PTNet在F1上达到了98.20%的最佳性能。但是其他对比算法模型在此数据集上同样表现不错。为了探究原因，在USTC-TFC数据集中，发现恶意流量在应用层中包含未加密的数据，这可能使得其他模型更容易进行分类，从而表现出较高的性能。

基于TLS1.3的加密应用分类：PTNet模型比FS-Net模型水平提高了10.67%，从86.39%提高到

表 2　定量对比结果表

Table 2　Quantitative comparison result table

数据集	模型	AC	PR	RC	F1
Android	AppScanner	0.385 9	0.259 4	0.252 3	0.244 0
	FS-Net	0.484 4	0.336 3	0.354 7	0.334 2
	DeepPacket	0.880 8	0.800 4	0.756 7	0.813 9
	PTNet	**0.957 9**	**0.958 0**	**0.958 0**	**0.958 0**
USTC-TFC	AppScanner	0.895 4	0.898 4	0.896 8	0.899 2
	FS-Net	0.884 6	0.884 6	0.892 0	0.884 0
	DeepPacket	0.964 0	0.965 0	0.963 1	0.964 1
	PTNet	**0.981 0**	**0.982 0**	**0.982 0**	**0.982 0**
CSTNET-TLS1.3	AppScanner	0.666 2	0.624 6	0.632 7	0.620 1
	FS-Net	0.863 9	0.840 4	0.834 9	0.832 2
	DeepPacket	0.801 9	0.431 5	0.268 9	0.402 2
	PTNet	**0.970 6**	**0.971 0**	**0.971 0**	**0.971 0**

97.06%。TLS1.3 在提高传输安全性的同时，也对 AppScanner 等基于统计特征的方法提出了新的挑战。PTNet 通过深度解析流量载荷与包长序列，将 F1 提高到 97.10%。这表明 TLS1.3 上加密的流量在载荷数据报文与包长序列上仍然具有隐式模式特征，PTNet 可以更好地利用这些模式特征进行分类。

3.3　消融实验分析

本节验证 PTNet 模型的关键组件对最终分类的贡献程度，实验任务设定为基于 TLS1.3 的加密应用分类，数据集使用 CSTNET-TLS1.3。

3.3.1　验证预训练有效性

本节将使用经过预训练的 Transformer 编码器 PTNet(完整模型)与没有经过预训练的 Transformer 编码器的 PTNet 进行对比，验证预训练的有效性，结果如图 5 所示。

从上图可以得出两点结论：

① 有预训练相较于没有预训练 Transformer 编码器，能提高模型的最终分类效果，最终的准确度从 95.32% 提高到了 97.28%。

② 使用预训练 Transformer 编码器，能够加速模型收敛。

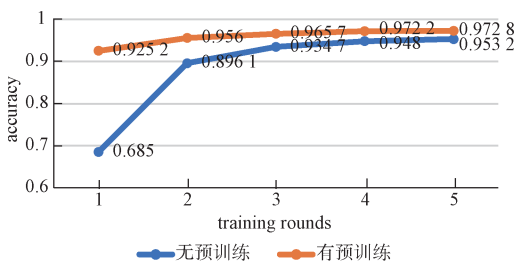

图 5　PTNet 与未预训练的 PTNet 结果对比图

Fig. 5　Comparison of PTNet and untrained PTNet results

3.3.2　验证不同特征对最终的有效贡献

本节分别除去 PTNet 模型的载荷特征通道与包长序列特征通道，即仅使用一种特征作为模型输入，验证两个特征融合对于最终分类性能表现的有效性，结果如图 6 所示。

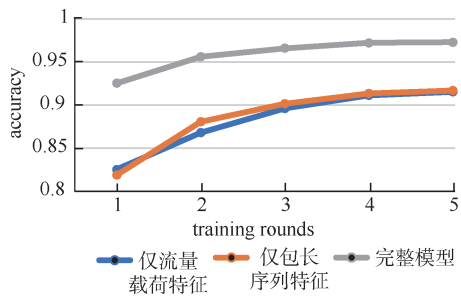

图 6　单特征训练模型对比图

Fig. 6　Single feature training model comparison diagram

从图 6 可以得出两点结论：

① 融合载荷特征与包长序列特征有助于最终模型的分类表现，这表明本模型每一个分支对于最终的分类效果都是有贡献的。

② 同时提取两个特征，有助于模型加速收敛。

4　结束语

本文提出了一种面向加密流量分类的半监督

并行Transformer网络来提高加密流量分类的性能。PTNet基于Transformer的端到端框架，通过融合流量载荷和包长序列两个特征，达到了较好的分类效果。在预训练阶段，对载荷和包长序列两个特征分别进行处理，通过对一些随机“流量载荷字节令牌”或“包长序列令牌”的屏蔽和恢复，来学习不同字节或流之间的关系。同时，Transformer中的多头自注意力机制可以从不同的角度关注数据特征的内容，整合来自不同角度的信息，有助于更准确地分类。实验结果表明，PTNet取得了比现有方法更好的结果。

参考文献

[1] SHI Hongtao, LI Hongping, ZHANG Dan, et al. An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification[J]. Computer Networks, 2018, 132: 81-98.

[2] REZAEI Shahbaz, LIU Xin. Deep learning for encrypted traffic classification: An overview[J]. IEEE Communications Magazine, 2019, 57, 5: 76-81.

[3] THIJS V E, RICCARDO B, ANDREA C, et al. 2020. FlowPrint: Semi-supervised mobile-app fingerprinting on encrypted network traffic[C]//Network and Distributed System Security Symposium(NDSS 2020), February 23-26, Catamaran Resort Hotel & Spa, San Diego, United States. San Diego: Internet Society, 2020: 1-18.

[4] VINCENT F T, RICCARDO S, MAURO C, et al. Robust smartphone app identification via encrypted network traffic analysis[J]. IEEE Transactions on Information Forensics and Security, 2018, 13, 1: 63-78.

[5] ANDRIY P, FABIAN L, JAN P, et al. Website fingerprinting at internet scale[C]// Annual Network and Distributed System Security Symposium(NDSS 2016), February 21-24, San Diego, CA, USA. San Diego: Internet Society, 2016: 1-15.

[6] LIN Kunda, XU Xiaolong, GAO Honghao. TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IioT[J]. Computer Networks, 2021, 190: 107974.

[7] LIU Chang, HE Longtao, XIONG Gang, et al. FS-Net: A flow sequence network for encrypted traffic classification[C]// IEEE Conference on Computer Communications, April 29 - May 2, 2019, Paris, France. IEEE INFOCOM, 2019: 1171-1179.

[8] JACOB D, CHANG M, LEE K, et al. BERT: Pre-training of deep bidirectional transformers for language understanding[C]//North American Chapter of the Association for Computational Linguistics: Human Language Technologies, June 2-7, 2019, Minneapolis, Minnesota, USA, 2019: 4171-4186.

[9] ALEXEY D, LUCAS B, ALEXANDER K, et al. An image is worth 16x16 words: transformers for image recognition at scale[C]//International Conference on Learning Representations(ICLR 2021), 2021. DOI: 10.48550/arXiv.2010.11929

[10] HE Hongye, YANG Zhiguo, CHEN Xiangning. PERT: payload encoding representation from transformer for encrypted traffic classification[C]//ITU Kaleidoscopef: Industry-Driven Digital Transformation, Dec 7-11, 2020, Ha Noi, Vietnam. IEEE, 2020: 1-8.

[11] WANG Xin, CHEN Shuhui, SU Jinshu. App-net: A hybrid neural network for encrypted mobile traffic classification[C]// IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), July 6-9, 2020, Toronto, ON, Canada. IEEE, 2020: 424–429.

[12] ACETO G, CIUONZO D, MONTIERI A, et al. Toward effective mobile encrypted traffic classification through deep learning[J]. Neurocomputing, 2020, 409: 306-315.

[13] LIN Peng, YE Kejiang, HU Yisheng, et al. A novel multimodal deep learning framework for encrypted traffic classification[J]//IEEE/ACM Transactions on Networking, 2023, 31(3): 1369-1384.

[14] WANG Wei, ZHU Ming, ZENG Xuewen, et al. Malware traffic classification using convolutional neural network for representation learning[C]//International Conference on Information Networking, January 11-13, 2017, Da Nang, Vietnam. IEEE, 2017: 712-717.

[15] LIN X, XIONG G, GOU G, et al. ET-BERT: A contextualized datagram representation with pre-training transformers for encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2022, April, 2022, Lyon, France. New York: Association for Computing Machinery, 2022: 633-642. DOI: 10.48550/arXiv.2202.06335.

[16] WANG Pan, LI Shuhang, YE Feng, et al. PacketCGAN: Exploratory study of class imbalance for encrypted traf-

fic classification using CGAN[C]//IEEE International Conference on Communications, June 7-11, 2020, Dublin, Ireland. IEEE, 2020: 1-7.

[17] LI Rui, XIAO Xi, NI Shiguang, et al. Byte segment neural network for network traffic classification[C]//International Symposium on Quality of Service, June 4-6, 2018, Banff, AB, Canada. IEEE, 2018: 1-10.

[18] MOHAMMAD L, MAHDI J S, RAMIN S H Z, et al. Deep packet: A novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24: 1999-2012.

[19] ASHISH V, NOAM S, NIKI P, et al. Attention is all you need[C]//The International Conference on Neural Information Processing Systems, Long Beach, California, USA, Decembers, 2017. New York: Curran Associates Inc., 2017: 6000-6010.

[20] LIU Chuan, WANG Wenyong, WANG Meng, et al. An efficient instance selection algorithm to reconstruct training set for support vector machine[J]. Knowledge-Based Systems, 2017, 116: 58-73.

[作者简介]

冯舒文　1992年生，硕士，工程师。

李育恒　1993年生，硕士，工程师。

白旭洋　1999年生，硕士，工程师。

(本文编辑：傅　杰)