

基于半监督学习的Tor匿名网络加密流量分类方法研究

曹庆伟¹, 宫良一^{2,3}, 李雨芙^{2,3}, 莫秀良¹, 杨科¹, 袁亚丽⁴

(1. 天津理工大学, 天津 300384; 2. 中国科学院计算机网络信息中心, 北京 100083;
3. 中国科学院大学, 北京 101408; 4. 东南大学, 江苏 南京 211189)

摘要: Tor (the onion routing) 匿名网络的多层加密和动态中继机制, 给流量分类带来了巨大挑战。传统流量识别技术难以有效检测Tor匿名网络流量中的非法应用或网站流量。针对这一问题提出一种基于半监督学习的Tor匿名网络加密流量分类方法。该方法采用“预训练+微调”的统一框架, 通过充分挖掘无标签数据的价值提升分类效能。在预训练阶段, 设计了动态掩码机制, 通过逐步调整掩蔽比例增强模型的特征学习能力; 在微调阶段, 引入通道与空间注意力(channel and spatial attention, CSA)模块, 提升模型对局部关键区域的感知精度。该方法以Transformer为基础架构, 兼具自监督特征提取与判别能力增强能力。实验结果表明, 在ISCXTor2016与自采暗网数据集上, 所提方法在对8类典型流量进行分类时, 各项性能指标均超过98%, 展现出优异的泛化能力与应用价值。

关键词: Tor匿名网络流量; 半监督学习; 暗网; Transformer

中图分类号: TP393

文献标志码: A

DOI:10.11959/j.issn.2096-109x.2025070

Study of semi-supervised learning based encrypted traffic classification method for Tor anonymity network

CAO Qingwei¹, GONG Liangyi^{2,3}, LI Yufu^{2,3}, MO Xiuliang¹, YANG Ke¹, YUAN Yali⁴

1. Tianjin University of Science and Technology, Tianjin 300384, China

2. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100083, China

3. University of Chinese Academy of Sciences, Beijing 101408, China

4. Southeast University, Nanjing 211189, China

Abstract: The onion routing (Tor) anonymous network, due to its multi-layer encryption and dynamic relay mechanisms, posed significant challenges for traffic classification. Illegal applications or websites traffic hidden within Tor anonymous network traffic could not be effectively detected by traditional traffic identification techniques. To address this issue a semi-supervised learning-based method for encrypted traffic classification in Tor networks was proposed. A unified "pretraining + fine-tuning" framework was utilized to fully leverage unlabeled data. In the pre-training phase, a dynamic masking mechanism was introduced to gradually adjust the masking ratio, enhancing the model's ability to learn latent features. In the fine-tuning phase, a channel and spatial attention (CSA) module was integrated to improve the model's sensitivity to critical local regions. The overall approach was built on a Transformer-based architecture, combining self-supervised feature extraction with enhanced discriminative capability. Experimental results on the ISCXTor2016 dataset and a self-collected dark web traffic dataset showed that the

收稿日期: 2025-04-28; 修回日期: 2024-06-17

通信作者: 莫秀良, moxiuliang@163.com

基金项目: 国家重点研发计划 (2023YFB3106700)

Foundation Item: The National Key Research and Development Program of China (2023YFB3106700)

proposed method achieved over 98% across all performance metrics in classifying eight typical traffic categories, demonstrating excellent generalization ability and practical value.

Keywords: Tor anonymous network traffic, semi-supervised learning, dark Web, Transformer

0 引言

随着互联网技术的迅猛发展,网络空间已深度融入人类社会的生产、生活与交互体系。然而,在互联网的表层之下,存在一类高度匿名的通信网络——暗网,其凭借隐蔽性与匿名性引发了社会各界的广泛关注。以Tor^[1]为代表的暗网通信系统,凭借其多层加密与动态中继转发机制,在保护用户隐私方面具有显著优势,但同时也给网络安全带来了严峻挑战。研究表明,暗网流量的强加密特性与跳跃式路径结构,使得传统的流量识别^[2]与追踪方法在此类环境中效果有限。因此,深入分析暗网通信特征并研发有效的流量分类方法,对于遏制网络犯罪、增强安全防护能力具有重要意义。

针对Tor匿名网络中加密流量难以识别和分类问题,本文提出一种基于半监督学习的加密流量分类方法。该方法采用“预训练+微调”策略,通过充分利用未标注数据降低标注成本,并提升模型对复杂加密流量的建模能力。该方法构建在Transformer架构上,并在不同阶段分别实现了模块结构创新。

在预训练阶段,本文引入了动态掩码(dynamic masking, DM)机制^[3],通过逐步降低掩蔽比例(从0.9降至0.5),引导模型完成从稀疏表示到完整信息的渐进式学习,有效增强对暗网流量特征的理解能力。该机制提升了Transformer对复杂通信数据中隐含模式的建模效果。

在微调阶段,本文针对暗网流量灰度图的特征,设计了一种新型的Transformer编码器结构。该结构在传统的自注意力机制基础上融合了位置编码、多头注意力(multi-head attention, MHA)及通道与空间注意力(channel and spatial attention, CSA)模块,其中CSA模块整合了压缩激励(squeeze-and-excitation, SE)^[4]与空间注意力(spatial attention, SA)机制,结合多层感知器(multilayer perceptron, MLP),构建了紧凑高效的特征提取流程。该设计在捕捉局部细节与建模

全局依赖方面具有更强的表达能力,显著提升了模型在流量分类任务中的性能与泛化能力。

本文构建了一个涵盖浏览、聊天、音频、视频、电子邮件、互联网电话(VoIP)、对等网络(P2P)及文件传输8类典型应用的Tor流量数据集,用于验证所提方法的有效性。实验结果表明,本文方法在多分类任务中取得了超过98%的精确率,且在召回率与F1分数上均显著优于传统监督学习方法,从而证明了该方法在复杂加密流量环境下的识别能力、鲁棒性及实际应用价值。

1 相关工作

1.1 暗网与Tor匿名网络

暗网是指无法通过常规搜索引擎访问的网络部分。其起源于20世纪末,在隐私保护需求与非法活动隐匿需求的双重驱动下逐步发展。早期的暗网形态主要源于科研机构与军事部门为保障通信安全所构建的封闭网络。这类网络主要依赖访问控制与洋葱路由技术^[5]实现对外部窥探的防护。

在暗网的众多技术架构中,Tor匿名网络^[6]是目前最具代表性与影响力的架构之一。该技术由美国海军研究实验室于20世纪90年代中期提出,后续由美国国防高级研究计划局资助开发。2003年,Tor匿名网络正式版发布;2004年,在USENIX会议上,Tor的核心设计理念与实现代码被正式公开。

Tor匿名网络基于洋葱路由技术构建,通过多层加密与节点转发机制实现通信匿名性。其由分布于全球的志愿者节点组成,节点包含3类,即入口节点、中继节点和出口节点。这些节点各司其职,共同维持Tor匿名网络的稳定运行。

如图1所示,在Tor匿名网络通信过程中,客户端通过洋葱代理定期从目录服务器获取包含节点IP地址、公钥等关键信息的路由节点列表,用于后续构建通信链路。随后,客户端依次与入口节点、中继节点和出口节点进行密钥协商,分别生成共享密钥K1、K2和K3。

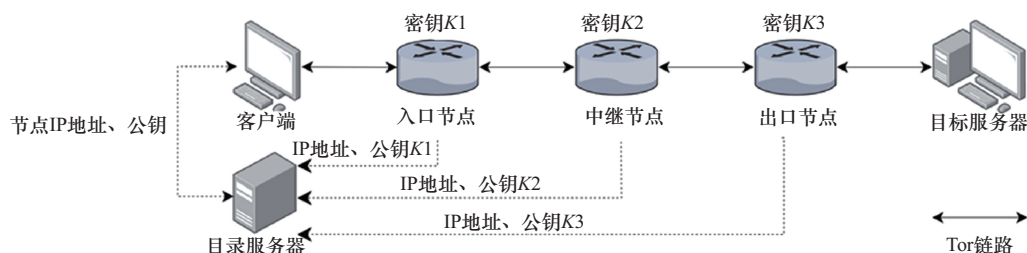


图1 Tor匿名网络通信原理

进入数据传输阶段后，客户端使用上述3个密钥按照从出口到入口的顺序（即 $K3 \rightarrow K2 \rightarrow K1$ ）对原始数据进行多层高级加密标准（AES）^[7]加密，形成 $K1(K2(K3(Data)))$ 的数据加密嵌套结构。数据在传输过程中由每个节点逐层解密，最终被还原为明文并发送至目标服务器。目标服务器返回的数据则经历相反流程：由各节点依次加密，客户端按顺序分别使用密钥 $K1$ 、 $K2$ 和 $K3$ 进行解密以获取原始数据。

Tor匿名网络的核心设计理念在于保护通信双方的身份隐私：入口节点能够识别客户端IP地址，却无法获取通信目标的信息；而出口节点虽知晓目标服务器的IP地址，却无法追踪客户端的身份；中继节点仅承担数据转发功能，既无法访问通信内容，也不能识别通信双方身份。正是这种分离机制，确保了仅客户端掌握完整的通信路径，从而实现高度匿名性。

由上述Tor匿名通信机制可知，其多层加密与节点转发策略虽能有效保障用户隐私，但也大幅提升了网络流量分析与识别的难度。因此，如何在不破坏原有加密机制的前提下，准确识别并分类Tor网络中的加密流量，已成为网络安全领域的重要研究课题。

1.2 Tor匿名网络加密流量分类技术

Tor匿名网络加密流量具有独特性质，对其进行精确分类至关重要，但同时也面临极大的挑战。从实际应用来看，准确识别和分类Tor匿名网络中的加密流量，对于加强网络安全防护、打击网络犯罪和维护健康的网络秩序具有重要的意义。借助高效的流量分类技术，可以更及时地识别潜在安全威胁，从而有针对性地制定并实施防护策略。目前，围绕Tor匿名网络加密流量分类的研究已取得一系列进展，相关探索主要集中在以下几个方向。

1.2.1 基于机器学习的方法

早期研究主要通过从暗网流量中提取统计特征（如数据包大小、到达时间间隔、数据包数量等），并采用支持向量机（support vector machine, SVM）、决策树、朴素贝叶斯等传统机器学习算法构建分类模型。例如，加拿大新布伦瑞克大学的研究团队在2016年发布的ISCXTor2016数据集中，便采用了基于统计特征的方法对Tor匿名网络流量进行分类^[8]。近年来，研究人员开始探索利用加密载荷^[9]特征提升Tor匿名网络流量分类性能。相关研究通过提取Tor匿名网络流量的加密载荷特征（如字节分布、熵等），并采用随机森林、SVM等机器学习算法构建分类模型。实验结果表明，这些特征在Tor匿名网络流量识别任务中具有较高的区分能力。

Iliadis等^[10]基于CIC-Darknet2020数据集，应用K近邻、多层感知器、决策树等算法，对Tor匿名网络流量进行二分类（良性流量与暗网流量）和多分类（Tor、非Tor、虚拟专用网络（VPN）和非VPN）。研究团队采用准确率、混淆矩阵、观测者操作特征曲线（ROC）等指标评估模型性能，同时结合参数微调和5折交叉验证对模型进行优化。

然而，传统机器学习方法高度依赖人工设计的特征，难以捕捉流量数据中的深层次语义信息，导致模型的泛化能力较弱，在复杂加密流量场景下分类效果受限。为此，研究者逐渐将目光转向深度学习技术，以期实现自动化特征提取与更强的流量数据表征能力。

1.2.2 基于深度学习的方法

Lashkari等^[11]于2020年提出了DIDarknet，这是一种基于深度图像的Tor匿名网络流量检测与表征方法。该方法的创新之处在于将流量数据转换为图像形式，进而利用卷积神经网络对图像

特征进行学习和分类,为Tor匿名网络流量分类提供了新的思路。Kirubavathi等^[12]训练了一个专门用于Tor匿名网络流量检测和表征的长短期记忆网络模型,该模型通过注意力机制聚焦关键时间序列特征,同时引入了局部可解释模型,有效提高了Tor匿名网络流量识别的准确率和可解释性。Zhu等^[13]提出了一种Tor匿名网络流量图的构建方法。该方法通过模拟客户端与远程服务器的交互过程,生成包含正向与反向节点的图结构,从而保留了流量交互中的方向、时序等关键特征,有效克服了传统方法对手工特征的依赖。在此基础上,研究团队设计了暗网图神经网络(darknet graph neural network, DGNN)架构^[14],将流量分类任务转化为图分类任务。该架构融合了注意力机制与图神经网络(graph neural network, GNN),注意力机制用于增强关键特征的权重,而多层GNN与MLP则协同完成特征提取与分类预测。模型训练以交叉熵作为损失函数,并基于Adam优化器(结合预热机制与余弦退火策略)进行参数更新。

尽管深度学习方法在暗网流量分类任务中表现出强大的特征学习与分类能力,但这类方法通常依赖大量高质量标注数据。在暗网环境下获取此类数据的成本极高,严重制约了模型的实际部署与应用。为破解这一困境,能够同时利用少量标注数据与大量未标注数据的半监督学习方法,逐渐成为该领域的研究热点。

1.2.3 基于半监督学习的方法

Lin等^[15]于2022年提出的ET-BERT模型采用半监督学习策略,首先在大规模未标注数据上进行自监督预训练,随后在少量标注数据上进行微调。该方法通过Datagram2Token机制将加密流量数据转换为Token序列,结合掩码突发流量单元模型与同源突发流量预测任务,建模字节上下文关系与传输结构。实验结果表明,ET-BERT在多个公开数据集上均表现出色,尤其在TLS 1.3等强加密环境中表现突出。

然而,ET-BERT在自监督阶段采用固定的预训练任务,缺乏对特征学习过程的动态调控,限制了其在复杂流量场景下对细粒度特征的建模能力。此外,其注意力机制设计相对简单,未能充

分捕捉通道与空间维度中的关键信息,仍存在优化空间。针对上述问题,本文提出了一种面向Tor匿名网络的半监督加密流量分类方法。

2 本文方法

本文提出的基于半监督学习的Tor匿名网络加密流量分类方法,旨在实现对大规模无标签加密流量的有效建模与精准分类。该方法构建在Transformer框架上,包含预训练与微调两个阶段。在预训练阶段,通过设计动态掩码机制,引导模型逐步挖掘并捕捉流量数据中的深层结构特征;在微调阶段,通过引入融合通道注意力与空间注意力的CSA模块,提升模型对细粒度行为特征的感知能力。该方法通过结构层面优化创新,有效提升了模型的分类精度与泛化能力,下文将详细阐述各阶段的具体设计思路与实现流程。

2.1 流量准备与采集

本文构建了一个包含8类典型暗网应用行为(浏览、聊天、音频、视频、电子邮件、VoIP、P2P与文件传输)的Tor加密流量数据集,用于模型的训练与测试。数据来源于公开数据集ISCXTor2016及真实暗网环境下的自采数据。其中,ISCXTor2016数据集结构规范、类别覆盖全面,有助于确保训练过程的标准性与分类结果的可比性;而自采数据则基于当前真实暗网环境构建,应用场景更贴近实际业务需求,流量特征丰富多样,能够有效评估模型在不同数据分布场景下的适应能力与泛化性能。两类数据源的结合使用,兼顾了样本的多样性、真实性与代表性,为分类实验提供了充分有效的数据支撑。

为构建自采数据集,研究人员需要在真实Tor匿名网络环境中使用Tor浏览器模拟多种典型用户行为。为此,首先需要将主机配置为通过Tor网桥进行连接,确保所有流量均经由Tor匿名网络传输^[16]。随后,通过访问各种Tor匿名网络服务模拟用户行为,实时捕获流量数据,并将流量数据保存为.pcap文件格式。具体采集过程如下。

1) 浏览流量:通过Tor浏览器访问不同类型Tor匿名网络网站(包括论坛、交易市场等),每完成一个网站的访问即生成一个独立流量文件

(记录用户的浏览行为), 共采集318个浏览流量文件。

2) 聊天流量: 通过Tor浏览器登录Skype即时通信工具, 模拟不同用户间的点对点聊天场景, 每个完整的聊天会话生成一个独立的流量文件(记录信息的发送与接收整个过程), 共采集347个聊天流量文件。

3) 音频流量: 通过Tor浏览器访问音频平台(如QQ音乐、网易云音乐), 模拟用户在线收听音乐行为。本文进行了多次音频流的播放, 在采集过程中, 每完成人工一次音频流的播放即产生一个流量文件, 共采集243个音频流量文件。

4) 视频流量: 通过Tor浏览器访问视频平台(如腾讯视频、爱奇艺等), 模拟用户观看视频行为。本文进行了多次视频流的播放, 在采集过程中, 每完成一次完整视频观看过程即生成一个流量文件, 共采集260个视频流量文件。

5) 电子邮件流量: 通过Thunderbird客户端配置Tor代理服务, 模拟用户收发电子邮件行为。每完成一次发送、接收或同步邮件操作即生成一个独立的流量文件, 共采集97个电子邮件流量文件。

6) VoIP流量: 在Tor匿名网络环境中使用Hangouts工具发起并接听语音电话, 每次完整通话过程生成一个独立的流量文件, 共采集201个VoIP流量文件。

7) P2P流量: 使用基于Tor匿名网络的文件共享平台(如Bittorrent), 从Kali Linux官方网站下载不同类型的.torrent文件, 模拟点对点文件上传、下载及数据交换行为。每完成一次文件交

换、上传或者下载操作即生成一个流量文件, 共采集257个P2P流量文件。

8) 文件传输流量: 通过Tor浏览器下载各种文件, 模拟文件传输行为。每完成一次文件下载操作即生成一个独立的流量文件, 共采集256个文件传输流量文件。

2.2 数据预处理方法

为实现原始流量的有效表征、剔除干扰信息, 同时兼顾数据的标准化与隐私保护需求, 本文设计了一套数据预处理流程, 并构建了多级流表示(multi-level flow representation, MFR)^[17]矩阵作为模型的输入基础。

数据预处理流程如图2所示, 首先根据IP地址、端口号与协议类型将Tor匿名网络流量分割为几条独立的数据流。为减少偏差, 需要去除以太网头部, 将端口号置零, 并对IP地址进行随机化处理(保留流量传输方向信息)。随后, 从每条数据流中提取5个相邻数据包, 将每个数据包拆分为80字节的报头部分与240字节的有效载荷部分。长度不足则用“0”填充, 长度超出则进行截断处理, 使每条数据流的5个数据包总长度固定为1600字节。将该固定长度数据重组为40×40的MFR矩阵, 从而有效压缩冗余信息。最终, 将MFR矩阵数值映射为8位像素值, 生成40像素×40像素的流量灰度图。通过上述流程, 原始流量数据被转化为统一分辨率的灰度图像矩阵, 为后续基于图像建模方法提取深层次语义特征提供了结构化的输入基础。

2.3 预训练模型设计

预训练阶段的核心目标是构建模型对加密流

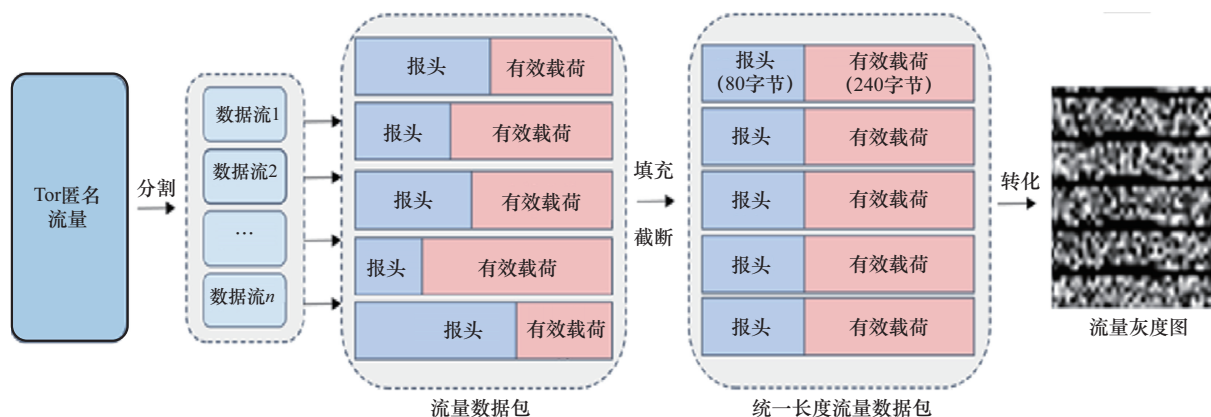


图2 数据预处理流程

量底层特征的感知能力。针对加密流量高度冗余与信息缺失并存的特性,本文设计了动态掩码机制,结合自监督学习目标,引导模型在稀疏输入条件下挖掘并学习数据的全局结构特征。

Tor 匿名网络流量分类模型如图 3 所示,在预训练阶段,根据输入流量的特征,本文设计了一种基于动态掩码机制的 Transformer^[18] 模型,其具体实现流程如下。

首先,将输入的 40 像素×40 像素无标签灰度图,按 2 像素×2 像素尺寸划分为互不重叠的图像块(patch)。由于原始图像为 40×40 像素,最终可以划分为 400 个 2×2 大小的 patch。随后,通过卷积嵌入操作,将每个 patch 映射为 192 维的特征向量。

为使模型具备捕获输入图像空间位置信息的能力,本文引入了位置编码(position embedding, pos_embed) 机制。该位置编码是一个形状为 (1, num_patches+1, embed_dim) 的张量,其中 num_patches 表示划分后的 patch 数量(即 400 个),embed_dim 表示每个 patch 通过卷积嵌入的维度

(即 192)。位置编码的嵌入过程可以表示为式(1)。

$$\mathbf{x}_{\text{embed}} = \mathbf{x}_{\text{patch}} + \text{pos_embed}[:, \text{num_patches} :, :](1)$$

其中, $\mathbf{x}_{\text{patch}}$ 表示 patch 的嵌入向量, $\mathbf{x}_{\text{embed}}$ 表示添加了位置编码的 patch 向量。

输入图像经过嵌入处理并添加位置编码后,将被送入动态掩码模块。该模块通过二进制掩码矩阵对部分 patch 进行随机掩蔽(1 表示掩蔽, 0 表示保留),迫使模型根据可见信息推断被掩蔽信息。掩蔽比例随训练进程动态调整,从而引导模型在不同阶段聚焦不同层次的特征学习。初期阶段,采用高掩蔽比例(如 0.9),仅保留少量可见 patch,迫使模型从有限的可见信息中挖掘全局关联,学习更丰富的底层结构表示;中期阶段,掩蔽比例逐步降低(如从 0.9 调整至 0.75 或 0.6),让模型逐步接触更多的真实信息,在多样化训练场景中提升泛化能力;后期阶段,掩蔽比例降至较低水平(如 0.5),此时模型可以访问接近完整的输入信息,进一步优化其对数据的理解能力和推理能力。整体遮蔽比例的动态变化关系可以表示为式(2)。

$$r(\text{step}) = \begin{cases} 0.9 - \frac{\text{step}}{0.5 \times \text{total_steps}} \times 0.1, & \text{step} \leq 0.5 \times \text{total_steps} \\ 0.8 - \frac{\text{step} - 0.5 \times \text{total_steps}}{0.333 \times \text{total_steps}} \times 0.2, & 0.5 \times \text{total_steps} < \text{step} \leq 0.833 \times \text{total_steps} \\ 0.6 - \frac{\text{step} - 0.833 \times \text{total_steps}}{0.167 \times \text{total_steps}} \times 0.1, & \text{step} > 0.833 \times \text{total_steps} \end{cases} \quad (2)$$

经掩蔽处理的输入序列将被送入 Transformer 编码器,借助该编码器多层自注意力机制有效捕捉各个 patch 之间的长距离依赖关系,进而生成图像的全局特征表示。接着,解码器基于编码后的

patch 向量重构原始图像的像素值,恢复被掩蔽区域。在训练过程中,采用均方误差(mean squared error, MSE) 作为损失函数,通过计算重构图像 y_{pred} 与真实图像 y_{real} 之间的差异,引导模型优化特

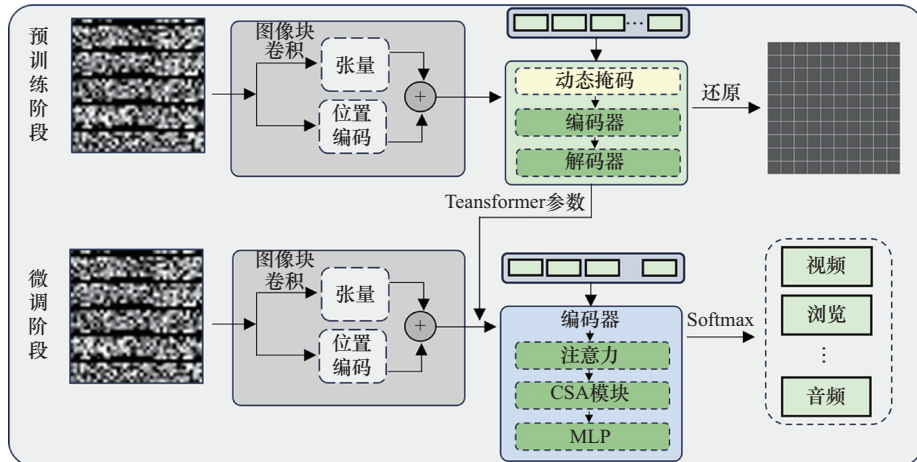


图 3 Tor 匿名网络流量分类模型

征推断和重建精度。该过程结合了自注意力机制与重构任务,使模型能够根据局部信息逐步还原数据全局结构,进而提升对加密流量图像的理解与推理能力。该损失函数的表达式如式(3)所示。

$$\text{LOSS} = \text{MSE}(y_{\text{real}}, y_{\text{pred}}) \quad (3)$$

经过预训练阶段的迭代优化,模型能够输出高质量的特征参数。这些参数将被保留下来,供微调阶段使用,从而使模型在缺乏大量标注数据的情况下,仍能够充分挖掘和利用真实暗网环境中未标注流量数据的价值。

2.4 微调模型设计

在预训练模型获得基础表示能力后,微调阶段将对预训练得到的特征进行精细调节,最终实现Tor加密流量的精准分类任务。为增强模型对局部关键特征区域的响应能力,本文在微调阶段设计了一种新型的Transformer编码器结构,如图4所示。该结构在传统自注意力机制的基础上,融合了位置编码、多头注意力、SE模块、SA模块和多层感知器。通过对上述模块和机制的精细化设计与有机组合,该编码器能够有效捕捉Tor匿名网络流量数据中不同尺度的局部细节与全局关联特征,从而有效提升分类准确率与模型的整体鲁棒性。具体而言,多头注意力机制在该编码器中承担着捕捉局部与全局特征相关性的关键作用。

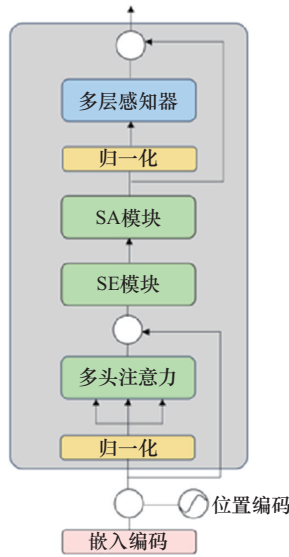


图4 编码器结构

对于输入的Tor匿名网络流量灰度图特征 $X \in \mathbb{R}^{B \times N \times D}$ (其中 B 表示批次大小, N 表示序列

长度, D 表示特征维度), 在注意力头数为16的条件下, 首先通过 W_Q 、 W_K 和 W_V 3个可学习矩阵进行线性映射, 生成查询 (Query)、键 (Key)、值 (Value) 3类向量, 其表达式如式(4)所示。

$$Q = XW_Q, K = XW_K, V = XW_V \quad (4)$$

随后, 计算注意力权重矩阵, 其表达式如式(5)所示。

$$\text{Attention}(Q, K, V) = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (5)$$

其中, d_k 表示键的维度。通过这种机制, 多头注意力能够在不同的表示子空间中并行捕捉Tor匿名网络流量灰度图的局部模式与通信行为特征, 有效提取跨区域依赖关系, 从而增强模型对复杂通信模式 (如P2P与VoIP通话) 差异的感知与区分能力。

为进一步增强模型对灰度图像细粒度特征的感知能力, 在多头注意力机制之后, 本文引入了CSA模块, 该模块由SE模块与SA模块顺次连接构成。

SE模块首先通过全局平均池化提取各通道的统计特征, 随后经由两层全连接网络生成通道注意力权重 W , 从而根据不同协议或内容类型在通道维度上的重要性动态调整特征强度。具体而言, SE模块的通道压缩比设为16, 即第一层全连接将通道维度降至原维度的1/16, 再通过第二层全连接将通道维度升至原维度, 从而有效建模通道间的依赖关系。该过程可以表示为:

$$W = \sigma(W_2 \cdot \text{ReLU}(W_1 \cdot \text{GAP}(X))) \quad (6)$$

其中, W_1 表示降维矩阵, W_2 表示升维矩阵, GAP表示全局平均池化, σ 表示Sigmoid激活函数。

SA模块则通过卷积操作学习空间注意力权重 M , 加强模型对关键空间区域 (如流量灰度图中异常通信模式区域) 的关注。具体而言, 该模块首先从通道维度对每个patch分别进行平均池化与最大池化, 将再将得到的特征图拼接后输入卷积核大小为7的一维卷积层进行特征融合, 最终通过Sigmoid函数生成归一化的注意力图。空间注意力的生成过程如式(7)所示。

$$M = \sigma(\text{Conv2D}([\text{AvgPool}(X); \text{MaxPool}(X)])) \quad (7)$$

所设计的 CSA 模块实现了通道与空间两个维度的联合特征重标定,使模型能够更加精准地区分流量图中具有代表性的局部变化,如短时高频数据传输(文件下载)与长时低频数据传输(网页浏览)的差异。

最终,经 CSA 模块增强后的特征表示被送入 MLP 进行非线性变换与特征融合。本文方法采用两层全连接结构,每层全连接后均依次接入 GELU 激活函数与 Dropout 操作,具体形式如下。

$$\text{MLP}(X) = \text{Dropout}(\text{GELU}(XW_1 + b_1))W_2 + b_2 \quad (8)$$

SA 模块通过增强特征空间的非线性变换能力,能够有效捕获 Tor 匿名网络流量中细粒度特征的组合模式与差异信息,为后续分类任务构建了判别性更强、信息更加丰富的特征表示。

从整体流程来看,本文设计的 Transformer 编码器在 Tor 匿名网络流量分类任务中展现出强大的特征提取与建模能力,多头注意力机制能够有效捕捉灰度图中不同区域之间的全局关联,CSA 模块通过动态感知通道与空间的重要性进一步凸显关键特征,而 MLP 模块则深化了非线性特征组合与表达能力。各模块和机制相互协作,构建起一套高效的 Tor 匿名网络流量灰度图特征优化与分类体系,显著提升了模型在复杂 Tor 匿名网络环境下的分类准确率与鲁棒性。

3 实验与结果分析

3.1 实验环境与数据集

本文实验使用 PyTorch 1.9.0 作为深度学习库,在 Python 3.8 与 CUDA 11.1 环境下实现所提模型。所有实验均运行于 Windows 服务器平台,硬件配置为 AMD Ryzen 7 9700X 处理器与 NVIDIA GeForce RTX 4080 SUPER 显卡(显存 16 GB)。

实验评估首先采用 ISCXTor2016 数据集,经预处理后共生成了 4 080 张灰度图。这些灰度图被随机分配到训练集和测试集中,其中训练集包含大约 80% 的灰度图,测试集包含剩余的大约 20% 的灰度图。具体的类分布将根据概率进行随机分配,因此实际的训练集和测试集大小可能会有所不同,具体分布如下:训练集包含 3 246 张灰度图,其中浏览类 410 张、聊天类 420 张、音

频类 403 张、视频类 404 张、电子邮件类 395 张、VoIP 类 392 张、P2P 类 413 张、文件传输类 409 张;测试集包含 834 张灰度图,其中浏览类 105 张、聊天类 106 张、音频类 105 张、视频类 108 张、电子邮件类 99 张、VoIP 类 119 张、P2P 类 96 张、文件传输类 96 张。

为验证所提模型的泛化能力,本文还使用自建数据集进行分类性能测试。该数据集共包含 3 799 张灰度图,按照相同的随机分配方式划分为训练集与测试集。训练集包含大约 80% 的图像,测试集包含剩余的大约 20% 的图像。训练集包含 3 054 张图像,其中浏览类 629 张、聊天类 501 张、音频类 385 张、视频类 326 张、电子邮件类 176 张、VoIP 类 381 张、P2P 类 343 张、文件传输类 313 张;测试集包含 745 张图像,其中浏览类 149 张、聊天类 126 张、音频类 98 张、视频类 74 张、电子邮件类 41 张、VoIP 类 100 张、P2P 类 94 张、文件传输类 63 张。

模型优化采用 AdamW 优化器,预训练阶段设置基础学习率为 1×10^{-3} 、批次大小为 128、最大训练步数为 150 000,微调阶段设置基础学习率为 2×10^{-3} 、批次大小为 64、最大训练轮数为 200。

3.2 评估指标

本文采用精确率(precision)、召回率(recall)、F1 分数(F1-score)和准确率(accuracy) 4 个指标评估所提方法的性能。这些指标的计算式分别如下。

$$\text{precision} = \frac{TP}{TP + FP} \quad (9)$$

$$\text{recall} = \frac{TP}{TP + FN} \quad (10)$$

$$F1\text{-score} = \frac{2 \cdot \text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \quad (11)$$

$$\text{accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (12)$$

其中,TP(true positives)表示预测为正,实际也为正的样本数量。FP(false positives)表示预测为正,实际为负的样本数量。TN(true negatives)表示预测为负,实际也为负的样本数量。FN(false negatives)表示预测为负,实际为正的样本数量。

3.3 实验结果

首先,使用训练集对模型进行预训练,学习通用的初始特征表示;随后,在预训练参数的基础上,结合少量标注数据进行微调,进一步优化模型参数以提升其在流量分类任务中的性能。表1展示了本文模型在ISCXTor2016数据集上的分类结果。

表1 本文模型在ISCXTor2016数据集上的分类结果

流量类型	准确率	精确率	召回率	F1分数
总体	98.56%	98.57%	98.56%	98.56%
音频	97.14%	98.08%	97.14%	97.61%
浏览	97.14%	99.03%	97.14%	98.08%
聊天	100%	99.07%	100%	99.53%
文件传输	97.92%	100%	97.92%	98.95%
电子邮件	100%	100%	100%	100%
视频	99.07%	97.27%	99.07%	98.17%
P2P	96.88%	95.88%	96.88%	96.37%
VoIP	100%	99.17%	100%	99.58%

从实验结果可以看出,本文模型在8类流量(音频、浏览、聊天、文件传输、电子邮件、视频、P2P和VoIP)分类任务中的精确率、准确率、召回率和F1分数都达到了较高的水平,总体指标接近99%,彰显出卓越的分类性能。为了更直观地分析模型在细粒度流量分类中的表现,本文绘制了分类结果混淆矩阵,如图5所示。

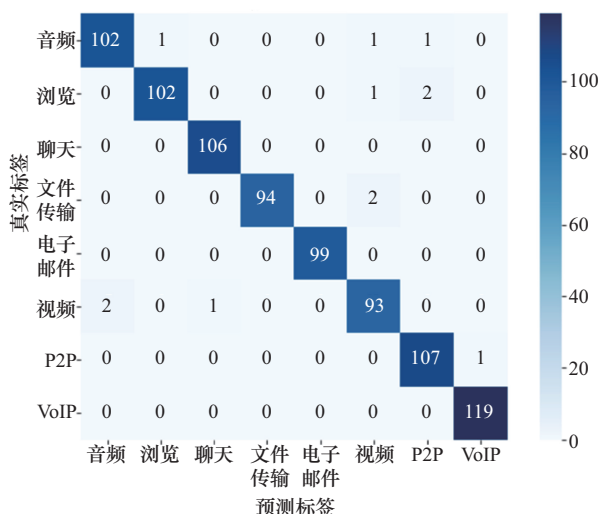


图5 分类结果混淆矩阵

混淆矩阵展示了8类流量的预测标签与真实标签之间的对应关系。其中,对角线数值表示分类正确的样本数量,而非对角线数值则为误分类样本数量。整体而言,本文模型在流量分类任务上表现优秀,尤其是在音频、聊天和VoIP类别中,正确分类的样本几乎覆盖全部真实样本,预测精度极高。尽管文件传输和电子邮件等类别存在少量误分类,但错误样本数量很少且分布较为分散。综上所述,本文提出的模型在8类流量分类任务中具有稳健的判别能力,大多数类别的分类准确率接近完美。

为验证本文模型的泛化能力,本文在基于ISCXTor2016数据集预训练的模型上,使用自建数据集进行微调,并对其分类性能进行了测试,本文模型在自建数据集上的分类结果见表2。

本文模型在自建数据集上的表现进一步验证了其强大的泛化能力。尽管该数据集在网络环境与数据分布方面与ISCXTor2016存在差异,但本文模型依然能够在各类流量中保持较高的分类准确率,总体精确率达到98.27%。尤其是在音频、聊天和VoIP等分类任务中,本文模型的表现出色,证明本文模型能够有效适应新数据集的特征分布。上述结果表明,经过预训练和微调的模型不仅在特定任务上表现优异,还具备在多样化网络环境中实现稳定、高效分类的能力,泛化性能优异。

表2 本文模型在自建数据集上的分类结果

流量类型	准确率	精确率	召回率	F1分数
总体	97.94%	98.27%	97.94%	98.10%
音频	100%	98.99%	100%	99.49%
浏览	98.66%	97.35%	98.66%	98.00%
聊天	100%	99.21%	100%	99.60%
文件传输	95.24%	95.24%	95.24%	95.24%
电子邮件	95.12%	97.50%	95.12%	96.30%
视频	98.65%	100%	98.65%	99.32%
P2P	96.81%	97.85%	96.81%	97.33%
VoIP	99.00%	100%	99.00%	99.50%

为更全面地评估模型在不同数据集上的分类性能,本文对比了模型在ISCXTor2016数据集与自建数据集上的性能指标,具体差值见表3。

表3 不同应用类型下模型分类性能差值（绝对值）

流量类型	准确率差值	精确率差值	召回率差值	F1 分数差值
音频	2.86%	0.09%	2.86%	1.88%
浏览	1.52%	1.68%	1.52%	0.08%
聊天	0.00%	0.14%	0.00%	0.07%
文件传输	2.68%	4.76%	2.68%	3.71%
电子邮件	4.88%	2.50%	4.88%	3.70%
视频	0.42%	2.73%	0.42%	1.15%
P2P	0.07%	1.97%	0.07%	0.96%
VoIP	1.00%	0.83%	1.00%	0.08%

从表3数据可以看出，本文模型在聊天、浏览和VoIP等交互性较强的流量类别中，各项指标差值较小，F1分数差值均低于0.1%，准确率差值不超过1.6%，表明本文模型在此类场景中具有良好的泛化能力。然而，在电子邮件和文件传输类别中，本文模型在自建数据集上的性能出现一定程度的下降，F1分数差值分别为3.70%和3.71%，准确率差值分别为4.88%和2.68%。这可能是由于该类流量在不同采集环境下的行为特征差异较大，本文模型判别边界不够稳定。此外，音频和视频类别的性能也存在一定波动，尤其是召回率差值较大，说明本文模型对多媒体流量的适应性尚有提升空间。

总体来看，本文模型尽管在部分类别上存在性能波动，但在多数流量类别上仍保持与ISCX-Tor2016数据集相近的分类水平，证明经过预训练和微调的模型具备较强的鲁棒性和跨域适应能力。

3.4 与主流检测方法的性能对比

为更好地展现本文方法的优势，本文将其与当前主流的流量分类方法进行对比。对比方法涵盖传统机器学习、深度学习和半监督学习等技术路线，具体包括：指纹构建方法FlowPrint^[19]；统计特征方法AppScanner^[20]；时序数据处理方法BiLSTM^[21]；机器学习方法^[22]K近邻（K-nearest neighbor, KNN）和随机森林（random forest, RF）；深度学习方法ConvNeXt^[23]和DF(deep fingerprinting)^[24]；半监督学习方法PERT^[25]、ET-BERT^[15]和YaTC^[17]。性能对比结果见表4。

从对比结果来看，部分现有方法虽然在准确率或精确率等单项指标上表现尚可，但整体性能存在明显短板。传统方法如FlowPrint和AppScan-

ner主要依赖静态指纹或统计特征构建，难以刻画加密流量复杂的时序与语义特征，导致其召回率和F1分数偏低，泛化能力有限。BiLSTM和KNN虽然在捕捉时序结构和处理低维特征上具备一定能力，但在处理高维异构特征时分类边界不够清晰，易产生误判。深度学习方法DF和ConvNeXt虽然在自动特征提取层面有所突破，但是在特征融合与上下文建模方面仍存在局限，难以充分挖掘流量行为之间的深层关系，限制了其在复杂场景下的分类性能。半监督学习方法PERT、ET-BERT和YaTC在标注样本不足场景下具备一定的优势，但其特征提取与融合能力有限，导致它们在复杂流量分类任务中的表现不及本文方法。

表4 不同方法的性能对比

流量类型	准确率	精确率	召回率	F1 分数
FlowPrint	90.92%	38.20%	36.61%	36.54%
AppScanner	67.22%	37.56%	44.22%	39.13%
BiLSTM	73.49%	72.84%	73.49%	72.04%
KNN	95.04%	93.34%	76.73%	84.23%
RF	89.24%	91.56%	56.75%	91.56%
ConvNeXt	76.56%	77.23%	76.56%	76.55%
DF	75.33 %	62.28%	60.10%	58.50%
PERT	76.82 %	44.24%	44.46%	43.45%
ET-BERT	97.50%	97.25%	96.55%	96.89%
YaTC	94.23%	94.39%	94.23%	94.22%
本文方法	98.56%	98.57%	98.56%	98.56%

相比之下，本文方法融合了预训练机制与精细化特征提取模块，显著提升了对多类Tor匿名网络流量的识别能力。在预训练阶段，通过自监督学习与动态掩码机制，实现了对原始Tor匿名网络流量的全局结构建模，使模型在面对分布复杂、特征混叠的数据集时具备更强的泛化能力。在微调阶段，引入CSA模块与多头注意力机制，优化分类边界，实现对关键细节特征的精准捕捉与类别间差异的深度建模，显著提升了模型对细粒度流量类别的识别能力。

实验结果表明，本文方法在准确率（98.56%）、精确率（98.57%）、召回率（98.56%）和F1分数（98.56%）上表现卓越，在细粒度分类任务中展现出较强的适应性和稳定性，尤其是在音频、聊

天和VoIP等分类任务中取得了较高的精确率，验证了其在复杂Tor匿名网络流量场景下的强大分类能力和泛化能力。

3.5 静态掩码与动态掩码对比实验

为验证动态掩码三段划分策略的有效性，本节在相同数据集与模型配置下，对比静态掩码与动态掩码的分类性能。静态掩码采用固定掩码率（掩码率为0.7、0.8、0.9）进行预训练，而动态掩码则通过三段划分机制自适应调整掩码范围。评价指标包括准确率、精确率、召回率和F1分数。实验结果见表5。

表5 静态掩码与动态掩码实验结果对比

掩码策略	准确率	精确率	召回率	F1分数
静态掩码0.7	97.48%	97.51%	97.48%	97.49%
静态掩码0.8	96.88%	96.93%	96.88%	96.89%
静态掩码0.9	98.08%	98.10%	98.08%	98.09%
动态掩码	98.56%	98.57%	98.56%	98.56%

实验结果表明，动态掩码在多项指标上优于静态掩码，验证了三段划分策略的合理性。相较于固定阈值的静态掩码，动态掩码能够根据训练阶段的特征学习需求动态调整掩码强度，更好地适应不同训练阶段的数据特征分布，从而提升模型的特征提取能力与分类精度。因此，在加密流量分类任务中，采用动态掩码策略是更优的选择。

3.6 消融实验

为评估预训练（PT）、DM、CSA三大模块对模型性能的贡献，本文设计了一系列消融实验，结果见表6。表中“-”表示移除对应模块。需要说明的是，由于DM模块依赖PT模块，因此“本文方法-DM-PT”等同于“本文方法-PT”，“本文方法-PT-CSA-DM”等同于“本文方法-PT-CSA”。

消融实验结果表明，PT、CSA和DM模块均对模型性能的提升有重要贡献。PT模块通过无监督预训练构建与任务无关的初始特征表示，不仅显著提升模型在下游任务中的泛化能力，还为CSA与DM模块提供稳定且具判别力的输入特征，保障后续注意力机制和掩码机制的有效性。CSA模块在Transformer基础上引入双重注意力机制，在通道维度增强关键特征响应，在空间维度聚焦重要区域，提升模型对复杂流量图像的感

知能力，尤其适用于局部异常与细粒度行为特征的识别。DM模块在预训练阶段引入动态掩码机制，强制模型从部分缺失的视角学习图像特征，从而增强模型的鲁棒性与多样化特征建模能力，在数据异常或数据不完整场景下优势突出。

表6 消融实验结果

模块	准确率	精确率	召回率	F1分数
本文方法	98.56%	98.57%	98.56%	98.56%
本文方法-CSA	96.15%	96.24%	95.96%	96.22%
本文方法-DM	97.18%	97.39%	97.18%	97.22%
本文方法-DM-CSA	98.26%	98.39%	98.26%	98.29%
本文方法-DM-PT	96.24%	97.16%	97.16%	96.26%
本文方法-PT-CSA-DM	95.30%	95.96%	95.84%	95.30%

值得注意的是，在实验中，移除DM与CSA模块（即“本文方法-DM-CSA”）后，模型性能下降幅度较小（准确率从98.56%降至98.26%）。这一现象与当前数据集的特性有关：在相对简单的数据分布下，DM和CSA模块的泛化能力未能完全发挥。DM模块通过动态掩码机制增强模型对缺失数据的鲁棒性，而CSA模块则通过注意力机制提升模型对关键特征的感知能力。然而，在当前数据集上，这些特性并未被充分激活，导致模块的作用不明显。

为验证DM和CSA模块在极端复杂场景下的泛化能力，研究人员在Obfs4混淆暗网流量数据集上进行了补充实验。Obfs4是一种广泛使用的暗网流量混淆工具，其通过随机填充、加密和协议模拟等手段将暗网流量伪装成普通HTTPS流量，极大地增加了分类难度。实验基于ISCX-Tor2016预训练模型，使用Obfs4数据集进行微调和测试。其中，训练集共2 098张灰度图（浏览类272张、聊天类317张、音频类448张、视频类302张、电子邮件类89张、VoIP类314张、P2P类89张、文件传输类267张），测试集共519张灰度图（浏览类56张、聊天类97张、音频类124张、视频类68张、电子邮件类26张、VoIP类73张、P2P类19张、文件传输类56张）。本文模型在Obfs4混淆暗网流量数据集上的分类结果见表7。

表 7 本文模型在 Obfs4 混淆暗网流量数据集上的分类结果

模块配置	准确率	精确率	召回率	F1 分数
本文方法（完整模型）	92.49%	92.62%	92.49%	92.49%
本文方法-CSA	84.97%	85.13%	84.97%	85.02%
本文方法-DM	85.36%	86.38%	85.36%	85.60%
本文方法-DM-PT	77.65%	78.25%	77.65%	77.83%
本文方法-DM-CSA	81.12%	81.73%	81.12%	81.06%
本文方法-PT-CSA-DM	76.30%	78.61%	76.30%	75.97%

结果表明，DM 和 CSA 模块的引入使模型在 Obfs4 混淆暗网流量分类任务中的准确率提升 11.37%（从 81.12% 提升至 92.49%），F1 分数提升 11.43%（从 81.06% 提升至 92.49%）。这一显著差异验证了 DM 和 CSA 模块在极端复杂场景下的泛化价值。

4 结束语

本文提出了一种新的 Tor 匿名网络加密流量分类方法，针对传统流量分类方法在 Tor 匿名网络动态流量场景下的困境，结合改进的半监督学习策略，通过引入独特的特征提取与融合机制来有效提升 Tor 匿名网络应用流量的分类性能。实验结果表明，所提方法在准确率、精确率、召回率和 F1 分数指标上显著优于现有主流方法，展现出优越的分类能力与鲁棒性。在后续研究中，将进一步优化动态掩码机制与注意力模块，同时探索多模态数据融合策略及更复杂的深度学习框架，进一步提升模型分类精确率与实际部署能力。

参考文献：

- [1] 罗军舟, 杨明, 凌振, 等. 匿名通信与暗网研究综述[J]. 计算机研究与发展, 2019, 56(1): 103-130.
- [2] LUO J Z, YANG M, LING Z, et al. Anonymous communication and darknet: a survey[J]. Journal of Computer Research and Development, 2019, 56(1): 103-130.
- [3] 翟明芳, 张兴明, 赵博. 基于深度学习的加密恶意流量检测研究[J]. 网络与信息安全学报, 2020, 6(3): 66-77.
- [4] ZHAI M F, ZHANG X M, ZHAO B. Survey of encrypted malicious traffic detection based on deep learning[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 66-77.
- [5] CHANG H W, ZHANG H, JIANG L, et al. MaskGIT: masked generative image Transformer[C]//Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2022: 11305-11315.
- [6] HU J, SHEN L, SUN G. Squeeze-and-excitation networks[C]//Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 7132-7141.
- [7] KUHN C, HOFHEINZ D, RUPP A, et al. Onion routing with replies[C]//Proceedings of the 27th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2021: 573-604.
- [8] DINGLELINE R, MATHEWSON N, SYVERSON P F. Tor: the second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004: 303-320.
- [9] ABDULLAH A M. Advanced encryption standard (AES) algorithm to encrypt and decrypt data[J]. Cryptography and Network Security, 2017, 16(1): 11.
- [10] 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: SciTePress, 2017: 253-262.
- [11] CHOOROD P, WEIR G. Tor traffic classification based on encrypted payload characteristics[C]//Proceedings of the 2021 National Computing Colleges Conference (NCCC). Piscataway: IEEE Press, 2021: 1-6.
- [12] ILIADIS A L, KAIFAS T. Darknet traffic classification using machine learning techniques[C]//Proceedings of the 10th International Conference on Modern Circuits and Systems Technologies. Piscataway: IEEE Press, 2021: 1-4.
- [13] LASHKARI A H, KAUR G, RAHALI A. DIDarknet: a contemporary approach to detect and characterize the darknet traffic using deep image learning[C]//Proceedings of the 10th International Conference on Communication and Network Security. New York: ACM, 2020: 1-13.
- [14] KIRUBAVATHI G, AMITHESH Y. Detection and characterization of darknet traffic using attention LSTM with XAI[C]//Proceedings of the 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS). Piscataway: IEEE Press, 2024: 1-7.
- [15] ZHU Y H, TAO J, WANG H T, et al. DGNN: accurate darknet application classification adopting attention graph neural network[J]. IEEE Transactions on Network and Service Management, 2023, 21(2): 1660-1671.
- [16] KINGMA D P, BA J, HAMMAD M M. Adam: a method for stochastic optimization[J]. arXiv Preprint, arXiv:1412.6980, 2014.
- [17] 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: ACM, 2022: 633-642.
- [18] BASSILY R, MORAN S, NANDI A. Learning from mixtures of private and public populations[J]. Advances in Neural Information Processing Systems, 2020, 33: 2947-2957.
- [19] 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 WashingtonDC: AAAI Press, 2023: 5420-5427.

- [18] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need[C]//Proceedings of the Advances in Neural Information Processing Systems. 2017: 5998-6008.
- [19] VAN-EDE T, BORTOLAMEOTTI R, CONTINELLA A, et al. FlowPrint: semi-supervised mobile-app fingerprinting on encrypted network traffic[C]//Proceedings of the 27th Annual Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020.
- [20] TAYLOR V F, SPOLAOR R, CONTI M, et al. Robust smartphone app identification via encrypted network traffic analysis[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 63-78.
- [21] SIAMI-NAMINI S, TAVAKOLI N, NAMIN A S. The performance of LSTM and BiLSTM in forecasting time series[C]//Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). Piscataway: IEEE Press, 2019: 3285-3292.
- [22] ILIADIS L A, KAIFAS T. Darknet traffic classification using machine learning techniques[C]//Proceedings of the 2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST). Piscataway: IEEE Press, 2021: 1-4.
- [23] LIU Z, MAO H Z, WU C Y, et al. A ConvNet for the 2020s[C]//Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2022: 11966-11976.
- [24] SIRINAM P, IMANI M, JUAREZ M, et al. Deep fingerprinting: undermining website fingerprinting defenses with deep learning[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 1928-1943.
- [25] HE H Y, YANG Z G, CHEN X N. PERT: payload encoding representation from Transformer for encrypted traffic classification[C]//Proceedings of the 2020 ITU Kaleidoscope: Industry-Driven Digital Transformation (ITU K). Piscataway: IEEE Press, 2020: 1-8.

[作者简介]



曹庆伟 (2000-), 男, 山西临汾人, 天津理工大学硕士生, 主要研究方向为暗网流量分析、网络空间安全。



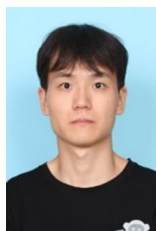
宫良一 (1987-), 男, 山东烟台人, 中国科学院计算机网络信息中心高级工程师, 主要研究方向为互联网安全、物联网安全。



李雨芳 (2000-), 女, 重庆人, 中国科学院大学硕士生, 主要研究方向为网络空间安全。



莫秀良 (1969-), 男, 天津人, 天津理工大学副教授, 主要研究方向为网络与信息安全。



杨科 (2002-), 男, 河北石家庄人, 天津理工大学硕士生, 主要研究方向为网络空间安全。



袁亚丽 (1986-), 女, 河南周口人, 东南大学副研究员, 主要研究方向为网络流量安全分析、协议逆向、漏洞挖掘、网络攻防、暗网、人工智能安全。