文章编号:1671-9352(2026)03-0001-10 DOI:10.6040/j.issn.1671-9352.9.2025.002

基于路径签名表征学习的加密流量检测

闫雷鸣[1,2],周吉[2],张欢[3],陈先意[1,2]
(1.南京信息工程大学数字取证教育部工程研究中心, 江苏 南京 210044; 2.南京信息工程大学计算机学院、网络空间安全学院, 江苏 南京 210044; 3.南京市专利行政执法支队, 江苏 南京 210008)

摘要:针对加密流量间交互行为特征的提取存在不足等问题,提出了一种基于路径签名表征学习的加密流量检测方法(path signature feature representation learning, PSFREL),利用路径签名来表征流量间隐藏的、不受加密影响的交互行为特征,使用自动编码器提取字段级局部特征,并使用结合通道注意力机制的残差网络 Cam-resnet 提取流量全局特征,形成多粒度流量特征后进行加密流量检测。在 ISCX VPN-nonVPN 等 4 个加密流量数据集上的评测结果显示,PSFREL 的平均 *F*1 达到 94.91%。

关键词:加密流量;路径签名;特征工程;残差网络
中图分类号:TP309 **文献标志码**:A
引用格式:闫雷鸣,周吉,张欢,等. 基于路径签名表征学习的加密流量检测[J]. 山东大学学报(理学版),2026,61(3):1-10.

Encrypted traffic detection based on path signature features representation learning

YAN Leiming[1,2], ZHOU Ji[2], ZHANG Huan[3], CHEN Xianyi[1,2]
(1. Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, Jiangsu, China; 2. School of Computer Science & School of Cyber Science and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, Jiangsu, China; 3. Nanjing Patent Administrative Enforcement Detachment, Nanjing 210008, Jiangsu, China)

Abstract: Aiming at the problems of insufficient extraction of interactive behavioral features between encrypted flows, a PSFREL (Path Signature Feature Representation Learning) based encrypted flow detection method is proposed. Signature feature representation learning (PSFREL), which uses path signatures to characterize the hidden, unaffected by encryption interactions between traffic flows, uses an autoencoder to extract local features at the field level, and uses the residual network Cam-resnet, which combines the attention mechanism of the channel, to extract the global features of the traffic flow, forming a multi-granularity flow features for encrypted traffic detection. Comprehensive benchmarking across four encrypted network flow datasets (e.g., ISCX VPN-nonVPN) showcases the PSFREL framework's capability to attain a 94.91% mean *F*1-Score.

Key words: encrypted traffic; path signatures; feature engineering; residual network

0 引言

当前基于加密技术的应用日益广泛,众多应用通过加密协议,如 HTTPS、VPN 等进行数据传输,以提升通信的安全性。然而,这种加密机制也被恶意流量利用,使得传统基于明文特征的网络流量检测方法难以有效识别恶意流量。因此,有效识别加密流量不仅是应对网络安全挑战的关键技术需求,更是实现用户隐私保护、非法信息监管等维护国家安全的重要基础。

为了应对这一挑战,可以提取侧信道特征、明文特征和原始流量这 3 类特征,利用机器学习方法对加密

收稿日期:2025-01-13; **网络出版时间**:2026-01-19
基金项目:国家自然科学基金资助项目(62172292;62472229)
第一作者:闫雷鸣(1973—),男,副教授,博士,研究方向为人工智能与安全、大数据与安全、自然语言处理、数据挖掘.
E-mail:yan_leiming@163.com

流量进行分类[1]。现有研究大多基于统计特征的方法或基于原始流量的方法。基于统计特征方法的研究是假设不同类型的流量具有独特的统计特征,通过直接提取或计算流量样本属性统计值作为特征,例如包长和传输时间等。该类方法本质上是传统恶意流量检测方法的迁移,忽略了加密流量分析的内在逻辑性和层次性,难以系统地解决加密流量分析面临的困难[2-3]。基于统计特征的方法存在 2 方面问题:(1)特征提取高度依赖于专家经验,泛化能力有限;(2)不同特征之间独立性高,缺乏对流量交互行为特征的挖掘。

为此,一些研究工作尝试使用深层神经网络,从原始流量中自动提取深层次特征[4-8],并取得了一定的成效。Wang 等[9]利用数据包到达时间和数据包大小组成二维图像,并使用卷积神经网络对图片组成的数据集进行分类,对于 VPN 流量取得了较好的识别结果,但对于非 VPN 流量识别效果欠佳。基于原始流量的方法普遍存在的问题包括:(1)对加密流量特征的表征存在不足,未能充分提取加密流量的交互特征;(2)单一粒度的表征学习无法充分提取流量会话的行为特征。为了克服单一粒度特征的表征能力不足问题,基于多粒度特征进行加密流量检测的研究获得了一定的进展[10]。Xu[11]等探索了应用路径签名提取网络流量特征的方法,改善了 SVM、Random Forest 等传统机器学习方法的网络流量分类性能,但是受模型性能局限,可能无法充分提取加密流量中某些重要的、隐藏的深层特征。

针对现有方法的局限性,本文提出了一种新的加密流量检测方法——路径签名表征学习(path signature feature representation learning, PSFREL)。主要工作包括:(1)针对加密流量在包级粒度上的交互行为,利用路径签名和 LSTM 进行编码,提取具有一定不变性、不受加密影响的局部动态行为特征;(2)通过融合局部动态行为特征、字段级局部特征和全局流量特征,显著提高加密流量识别的准确性。

1 路径签名

路径签名(path signature)方法中的路径(path)被定义为一个将连续取值区间$[a,b]$转换到多维空间 R^d 的映射[12],其最简单的理解就是物体运动的轨迹,假定物体在二维平面上从 t_1 时刻持续运动到 t_2 时刻,每个时刻的位置都能用一个二维向量表示,这一轨迹就构成了一条路径,即 $X:[a,b]\rightarrow R^d$, $t\in[a,b]$, d 维路径可表示为

$$X_t=\{X_t^1,X_t^2,\cdots,X_t^d\}。\tag{1}$$

路径签名实际上是路径不同阶路径积分(path integral)的集合。假定存在 2 个一维路径 X_t 和 Y_t,且记 $X'_t=dX_t/d_t$,则定义路径积分为

$$\int_a^b Y_tX'_t\mathrm{d}t=\int_a^b Y_t\mathrm{d}X_t。\tag{2}$$

其意义就是在参变量由 a 变换至 b 时 Y_t 对 X_t 的积分,这一形式的路径积分是后续所有 n 阶路径积分的基础。对于一条多维的路径 $X:[a,b]\rightarrow R^d$,其一阶路径签名表达式为

$$S(X)_{a,t}^{n}=\int_a^t \mathrm{d}X_c^n,\ t\in[a,b]\ 。\tag{3}$$

其中,$Y_t=1$, $X_t=X_c^n$, X_c^n 表示路径 X 的第 n 个维度在 c 时刻的取值。结合积分的意义,路径积分实际上就是在计算矩形元的面积累加,以二维路径签名为例,其几何意义如图 1 所示。

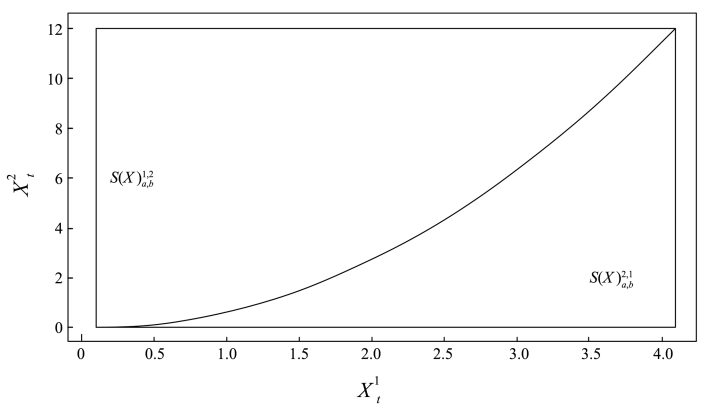

图 1 二维路径签名的几何意义

Fig.1 Geometric significance of two-dimensional path signatures

从路径积分的几何意义可以看出,路径积分有以下 2 个重要的性质:

(1)平移不变性。路径积分的结果实际上是由 Y_t 和 X_t 之间的相对关系所唯一确定的,与积分变量 X_t 的初始值 X_a 并没有什么关系,即,如果在 X_t-t 平面内进上下平移,并不会对积分值产生任何影响,表达式为

$$\int_a^b Y_t \mathrm{d}X_t = \int_a^b Y_t \mathrm{d}Z_t, \quad Z_t = X_t + C。 \tag{4}$$

(2) 重参数不变性。路径积分的计算结果只与 Y_t、X_t 的相对关系有关[22],而与参变量 t 没有关系。假定一条 path 的参变量由 a 变化至 b 时,Y_t、X_t 从[Y_0,X_0]变为[Y_1,X_1],而存在另一条 path 的参变量由 a 变化至 $2b$ 时,Y_t, X_t 也从[Y_0,X_0]变为[Y_1,X_1],这 2 条 path 的路径积分实际上没有区别,即路径积分和 X_t 瞬时速度无关,表达式为

$$\int_a^b Y_t \mathrm{d}X_t = \int_{k_1 a}^{k_2 b} Y_r \mathrm{d}X_r, \tag{5}$$

其中,$Y_t(X_t)=Y_r(X_r)$, $X_t(a)=x_r(K_1 a)$, $X_t(b)=x_r(K_2 b)$。

路径 $X:[a,b]\to R^d$ 的签名,用 $S(X)_{a,b}$ 表示,是 X 的所有迭代积分的集合(无限级数)

$$S(X)_{a,b}=(1,S(X)_{a,b}^{1},\cdots,S(X)_{a,b}^{d},S(X)_{a,b}^{1,1},S(X)_{a,b}^{1,2},\cdots,S(X)_{a,b}^{d,d},\cdots)。 \tag{6}$$

路径签名因其对时序数据平移不变性和重参数化不变性的独特优势,近年来被广泛应用于多个领域,展现了强大的特征表征能力。典型应用是金融领域时间序列分析,路径签名被用于捕捉股票价格、汇率等高维时间序列的动态模式。例如,Wang 等[13]将路径签名与 Transformer 架构融合,通过高阶路径签名提取长程依赖关系,实现了对高频交易数据的异常检测。在医疗领域,路径签名被用于分析患者运动轨迹(如帕金森病步态)以辅助诊断,Li 等[14]提出基于强化学习的路径签名优化方法,显著提升了运动康复评估的准确性。同时,路径签名在基因表达时序数据分析中展现了潜力。Guo 等[15]将路径签名与图神经网络结合,构建了基因调控网络的动态模型。

上述研究表明,路径签名在时序数据特征提取中具有普适性,其不变性特点可有效过滤噪声并保留关键交互行为,为将其引入加密流量检测提供了理论支持,同时也启发未来研究探索路径签名与其他深度学习模型的深度融合。

2　基于路径签名表征学习的加密流量检测框架

本文利用路径签名所具有的平移不变性和重参数化不变性等特点来描述流量之间的交互行为特征。利用路径签名提取特征主要有以下 2 个特点:

(1)路径签名可以完全确定一个数据路径,不受加密流量统计特征改变的影响;

(2)对于特定类型应用程序生成的流量,特征提取不受重参数化的影响。

因此,利用路径签名可以提取时序数据中一些重要的不变特性,有助于从加密流量中发现传统特征提取方法忽略的隐藏特征。

本文提出了一种基于路径签名表征学习(path signature feature representation learning, PSFREL)的加密流量检测框架,如图 2 所示。该框架采用端到端的模型架构,包括数据预处理、流量信息提取和流量分类 3 个模块。在数据预处理阶段,先通过网络流量工具解析会话包,进行必要的数据清洗操作,切分为统一流量大小,把流量转换成二维灰度图格式。在流量特征提取阶段,利用路径签名捕捉加密流量包级粒度特征,并提取流量间交互行为中隐藏的平移不变特征,然后输入 LSTM,进行时序编码;为了获得多种粒度的流量特征,提取了 26 个包级统计特征,并用自动编码器进行编码,作为局部特征的补充;设计了一个结合通道注意力的简化残差网络,从原始流量中提取全局特征。最后,将路径签名提取的局部交互行为特征、包级粒度的局部特征、全局流量特征这 3 种不同粒度的流量特征输入全连接层,进行流量检测和分类。

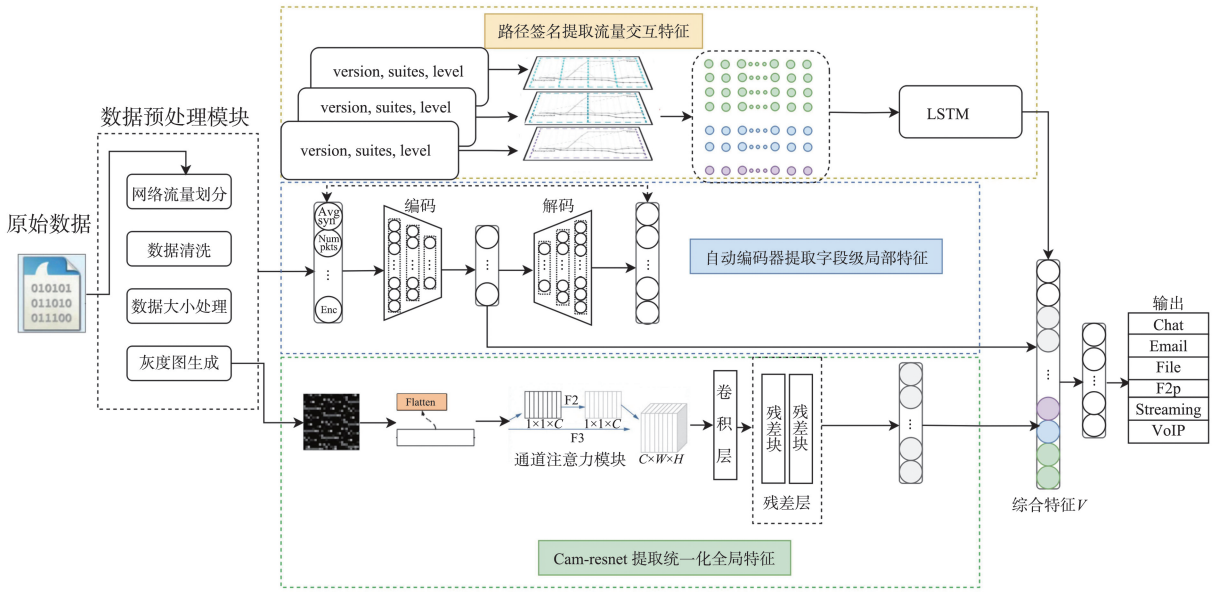

图 2 PSFREL 框架结构图

Fig.2 Frame structure of PSFREL

2.1 基于路径签名的加密流量特征提取

2.1.1 基于路径签名加密流量交互特征提取

在加密流量通信的初始阶段,通信双方通过握手交互来交换信息,这一过程可以被视为局部通信行为。局部通信行为包括 TCP 3 次握手和 TLS 加密握手 2 个关键阶段。尽管单独观察局部通信行为的任一阶段可能无法明显揭示流量的恶意性,但深入分析各阶段之间的交互行为却能显著提升对恶意流量的识别能力。文献[10]详细阐述了 3 种关键的交互行为模式,这些模式在恶意流量检测中具有重要的指示作用。

首先,不同报文字段间的交互有助于揭示恶意行为。例如,恶意客户端为了扫描发现服务器提供的服务,在建立连接时会尝试多种加密协议,但服务器只会响应其支持的特定加密协议,这种请求与响应的不一致性,暗示了潜在的恶意行为,其次,报文内字段间的交互同样是一个关键特征。在恶意加密流量中,Certificate 报文的 subject 和 issuer 字段可能指向低信誉的证书颁发机构或自签名证书;在 Server Key Exchange 报文中,如果密钥的变更与 ServerHello 报文的响应存在特定的交互模式,也可能提示存在恶意行为。

因此,提取这些交互行为特征,有助于恶意流量检测。但是因为不同交互行为的交互动作、频率、报文长度等都不相同,很难针对所有交互构建统一的特征。

本文利用路径签名的平移不变性和重参数化不变性,提取可量化表征的交互行为特征。如图 3 所示,在加密流量包级粒度层面,先将会话中的关键字段组成会话流序列,再将会话流的前 128 个字段序列作为计算路径签名的输入。设置滑动窗口,当窗口宽度为 2 时,提取相邻流量包之间的行为特征。这些序列可以表示为一维路径,其中每个数据包的长度对应于路径上的一个点,然后对 128 维提取深度为 3 的路径签名,如式(5)所示,后续的路径签名均可通过对前一阶的路径签名再求路径积分得到,将得到的特定维度的路径签名输入 LSTM,以便提取交互行为的时序特征,并进行编码。

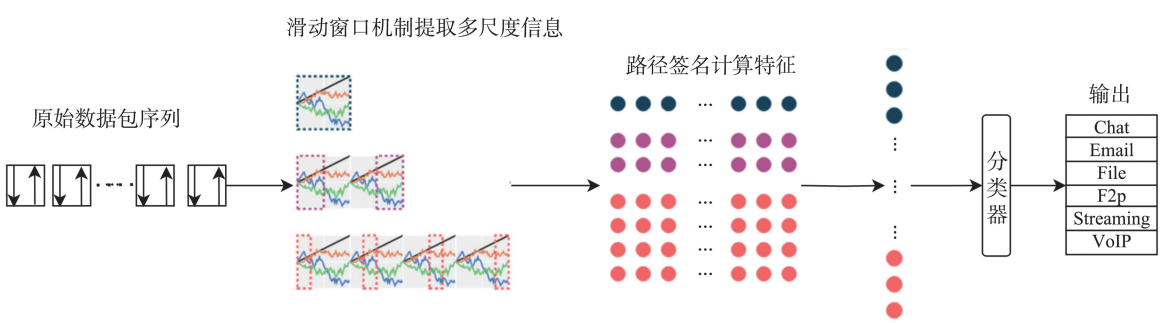

图 3 基于路径签名提取加密流量交互特征

Fig.3 Extract the interaction information between traffic based on path signatures

路径签名通过高阶路径积分(式 6)提取流量交互行为的几何特性,其平移不变性(式 4)确保特征不受初始值偏移影响,重参数化不变性(式 5)使其忽略时序采样频率差异。例如,恶意流量中频繁的协议试探行为(如 TLS 握手失败)会在路径签名的高阶项中表现为显著的非线性积分特征,而正常流量的稳定交互则呈现低阶线性特征。通过 LSTM 模型,这些特征进一步被编码为时序动态模式,弥补了传统统计特征对交互行为建模的不足。

2.1.2　加密流量全局特征提取

对于加密流量识别来说,并非所有特征都能够产生相同的作用。为了给重要的加密流量特征赋予更高的权重,本文对传统残差网络[16]进行简化,并引入通道注意力机制[17],以实现重点关注数据包长度、数据包持续时间、端口号等重要特征[11]。

残差网络提取网络流量特征时,主要面对的困难有:(1)训练所需的参数量大;(2)时空开销大,对重要特征捕捉能力不足[18]。针对上述问题,本文对 Resnet 网络结构进行简化,结合通道注意力机制,将该网络命名为 Cam-resnet,结构如图 2 下方所示。Cam-resnet 包含 4 个残差层,每个残差层包含 2 个残差块。优化后的残差网络能够在不增加过多参数和计算成本的情况下,有效增强网络的表征能力。

此外,关于残差网络的结构改造还包括:(1)将网络中的普通卷积替换成扩张卷积,引入扩张因子后,经过扩张卷积处理,有效增加模型的感受野,且输出相同维度的特征映射。(2)删除了池化层。池化层最直接的作用是对卷积操作的结果进行降维,以减少网络中参数的数量。但是过度池化,也可能忽略了加密流量中的一些重要特征。因此,在轻量化的网络结构中,删除池化层以保留更多有用信息。

在这一步中,利用 Cam-resnet 直接从原始流量中提取全局信息。因为使用该网络需要固定大小的输入,因此将原始流量统一到相同的大小。在本文中,原始流量统一为 784 字节($N=784$)。在所有流量统一化后,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。如图 4 所示,784 字节会话可以转化为 28 * 28 矩阵。

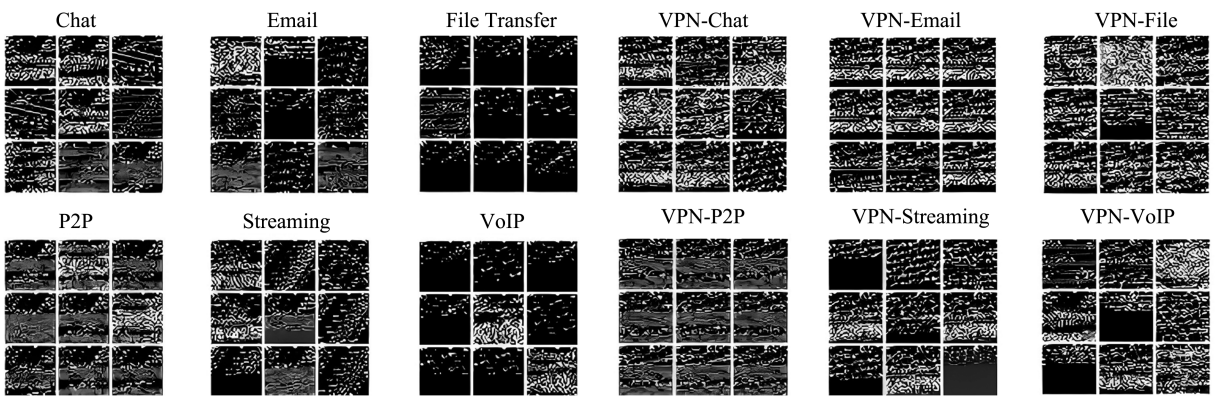

图 4　VPN 流量与非 VPN 流量可视图

Fig.4　Visualization of non-VPN Traffic and VPN Traffic

Cam-resnet 中的通道注意力通过全局平均池化生成通道权重

$$W_c=\sigma\left(W\cdot\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}F_c(i,j)\right),\tag{7}$$

其中,F_c 为第 c 个通道的特征图,σ 为 Sigmoid 函数。该机制使模型动态增强重要通道(如包长、端口号)的响应。在 VPN 流量中,高权重通道对应加密协议字段(如 TLS 版本号),使注意力机制能有效识别加密流量的关键标识。

2.1.3　原始加密流量字段级局部特征提取

从流量包内部中提取了 26 个典型的统计特征[19],这些特征可以用于弥补流量统一化后带来的特征缺失,例如 Num pkts(会话中的数据包数量)、Avg syn 标志(会话中具有 syn 标志的数据包的平均值)和 Duration 窗口流(会话中从第一个数据包到最后一个数据包的时间)等。受 Wang 等[20]的启发,除提取传统统计特征之外, 还加入了 Enc 比率特征,即流量持续时间和 Enc 流量持续时间之间的比率。Enc 特征比其他传统特征更适合表示加密流量的数据分布特征,且不再受到加密协议类型的限制,有助于提取数据包级别

的加密属性[21]。为了融合这些字段级的局部特征,在归一化过程之后,所有统计特征范围都转换为[0,1],然后利用自动编码器将这 26 个特征统一编码。

2.2 多粒度特征融合

已经提取的不同粒度的加密网络流量特征包括:(1)路径签名提取的表征流量间交互行为的动态局部特征;(2)通过自动编码器统一编码的局部统计特征;(3)Cam-resnet 提取的加密流量全局特征。合并后形成多粒度流量特征向量,然后利用全连接层进行加密流量分类,如图 2 所示。模型训练时的损失函数使用交叉熵,以及用 L1 范数作为正则项。

3 实验与结果分析

3.1 实验环境

本文的实验环境如下:操作系统为 Windows 10,开发系统为 python 3.9,CPU 为 AMD EPYC 7532 32-Core Processor,内存为 16 GB,显卡为 RTX3060,基于 pytorch1.7 完成模型构建。

3.2 评价指标

采用准确率 A、精确率 P、召回率 R 和 $F1$ 分数作为实验结果的评价指标。A 越大,表示模型的性能越好;P 越高,表示模型的误报率越低;R 越高,表示模型的漏检率越低;$F1$ 分数同时兼顾了分类模型的准确率和召回率,其中,真阴性 TN 表示数据为正常且预测为正常的数量,真阳性 TP 表示数据为异常且预测为异常的数量,假阴性 FN 表示数据为异常但预测为正常的数量,假阳性 FP 表示数据为正常但预测为异常的数量。

$$A=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}}, \tag{8}$$

$$P=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}}, \tag{9}$$

$$R=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}, \tag{10}$$

$$F1=\frac{2*R*P}{R+P}, \tag{11}$$

3.3 数据集

本文选取被广泛使用的 4 个公开数据集进行实验验证,(1)ISCX VPN-nonVPN :包含 14 种类别的流量,分别从不同的应用程序(例如 Skype、BitTorrent)捕获,包括 7 类普通业务流量(非 VPN)和 7 类 VPN 加密流量。(2)CIC-IDS2018:包含 HTTPS、SSH、TOR 等多种加密协议的流量,涵盖 DDoS、端口扫描等复杂攻击场景。(3)IoT-23:专为物联网设计的加密流量数据集,包含智能家居设备(如摄像头、温控器)的通信流量,加密协议以 MQTT-TLS 和 CoAP-DTLS 为主。(4)USTC-TFC2016:覆盖即时通讯(WhatsApp)、流媒体(Netflix)等应用场景的加密流量,包含 VPN 和非 VPN 流量混合样本。数据集信息如表 1 所示。

表 1 数据集属性

Table 1 Dataset properties

数据集	加密协议	流量类型	样本数量	类别数
ISCX VPN-nonVPN	HTTPS, VPN(OpenVPN/IPSec)	VPN 与非 VPN 混合流量	2.4×10^5	14
CIC-IDS2018	HTTPS, SSH, TOR	攻击流量(DDoS 等)	12.0×10^5	15
IoT-23	MQTT-TLS, CoAP-DTLS	物联网设备流量	3.5×10^5	10
USTC-TFC2016	HTTPS, QUIC	应用流量(视频、IM)	5.0×10^5	12

PSFREL 框架中有 3 个数据预处理步骤:流量分割、流量清洗和流量大小处理。通过统计分析,[0,784] Bytes 范围内的会话大小占流量的 84%,而只有 3%的会话大小在[784,1 024]字节的范围内,如图 5 所示。因此,原始流量统一截取数据包前 784 Byte,将 pcap 格式的流量文件转化为 28×28 像素的灰度图片。

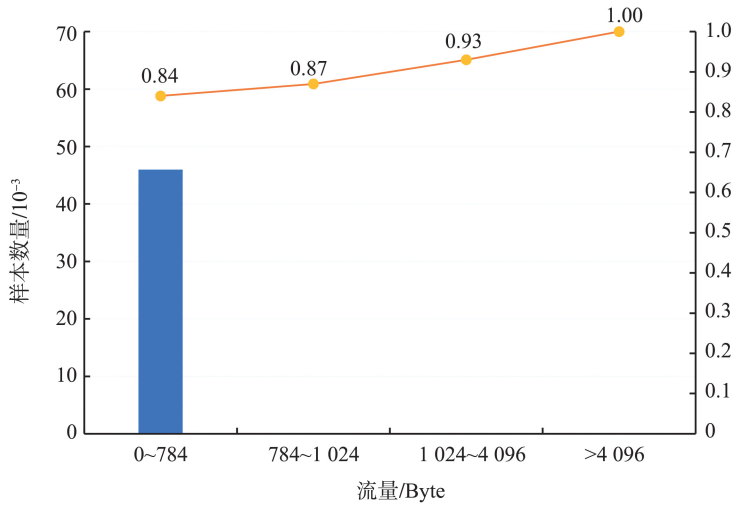

图 5　每个时间间隔中会话大小的百分比

Fig.5　Percentage of session size in each interval

3.4　实验结果与分析

3.4.1　对比实验

为了验证 PSFREL 的有效性和性能,本文在“ISCX VPN-nonVPN”等 4 个数据集上对不同模型的加密流量分类任务进行了 30 个实验,PSFREL 均取得了最佳实验结果,以下为 ISCX VPN-nonVPN 数据集的实验结果,如表 2 所示。

(1)残差网络有无结合通道注意力对分类结果的影响。从表 2 可以看出,结合了通道注意力机制的 Cam-resnet 相对于传统残差网络来说,模型的各项指标均有提高,说明结合了注意机制的 Cam-resnet 能够在不增加过多参数和计算成本的情况下,让模型更关注重要的特征。

(2)扩张卷积对最终性能的影响。如表 2 所示,从“Cam-resnet1D”到“Cam-resnet1D-Dilated”,模型的各项指标提高超过 2%。同样,在 2D 模型(如 Cam-resnet2D 和 Cam-resnet2D-dilated)的情况下,当使用扩张卷积时,模型的性能也有所提高。主要原因是扩张卷积可以增加模型流量特征提取时的感受野,并帮助模型做出判断。

表 2　PSFREL 与基线方法对比结果

Table 2　Comparison results of PSFREL with the baseline methods

方法	*A*	*P*	*R*	*F*1
CNN1D-Pooling	0.923 8	0.951 9	0.923 8	0.933 3
CNN1D-noPooling	0.954 9	0.967 3	0.954 9	0.958 8
CNN2D-Pooling	0.914 6	0.947 2	0.914 6	0.925 6
CNN2D-noPooling	0.946 4	0.962 9	0.946 4	0.951 9
Resnet1D	0.958 9	0.960 0	0.959 1	0.959 1
Cam-resnet1D	0.964 3	0.973 1	0.964 3	0.967 0
Cam-resnet1D-dilated	0.983 4	0.986 2	0.983 4	0.984 3
Cam-resnet2D	0.940 6	0.958 8	0.940 6	0.946 5
Cam-resnet2D-dilated	0.957 7	0.969 6	0.957 7	0.961 7
PSFREL	**0.996 3**	**0.996 6**	**0.996 5**	**0.996 5**

(3)有无池化层对最终结果的影响。如表 2 所示,无论是在 1DCNN 还是 2DCNN 中,移除池化层后,模型准确率都提高了约 3%,主要原因是在去除池化层后,原始流量可以保留更多重要的特征信息,并帮助模型做出判断。

(4)一维卷积层和二维卷积层对结果的影响。如表 2 所示,1D 卷积层模型的精度高于 2D 卷积层模型,证明了一维卷积层比二维卷积层更适合加密流量分类。

将流量大小统一到 784 字节后,通过实验发现使用扩张卷积优化传统残差网络中的普通卷积,并在去除池化层后能显著提高模型的性能。因此,本文使用结合了通道注意力机制的网络 Cam-resnet1D-dilated 并删

除池化层,再结合了路径签名提取的流量间全局行为特征和流量内统计特征后,最终使得 PSFREL 的准确率和 $F1$ 分数得到了进一步的提升。

为了进一步评估 PSFREL 的性能,与其他先进的模型进行了比较,结果如表 3 所示,PSFREL 在 ISCX VPN-nonVPN 数据集上的准确率高达 99.63%。总之,与其他几种方法相比,PSFREL 实现了最高的整体准确度、精度、召回率和 $F1$ 分数。对比的方法中,ETCPS[11]是较早使用路径签名的流量检测方法,该方法将二维路径签名作为单一流量特征,应用于 SVM、Random Forest 等传统机器学习方法,改善了算法性能,但是未能提出应用于深度学习模型的方法。PSFREL 将路径签名应用于提取流量中交互行为的时序特征,并用 LSTM 对时序特征进行编码,构造了融合自动编码器和 Cam-resnet 的深度学习模型框架。从测试结果来看,PSFREL 的准确率和 $F1$ 分数均略高于 ETCPS。

表 3 PSFREL 的结果与先进模型的比较

Table 3 Comparison of PSFREL's results with advanced models

方法	A	P	R	$F1$
FlowPic[20]	0.870 0	0.930 0	0.870 0	0.890 0
CNN1D[8]	0.850 0	0.850 0	0.860 0	0.860 0
Deep Packet-CNN[4]	0.960 0	0.970 0	0.960 0	0.970 0
Deep Packet-SAE[4]	0.970 0	0.960 0	0.900 0	0.970 0
CNN+LSTM	0.980 0	0.980 0	0.970 0	0.980 0
SPCaps[22]	0.960 0	0.970 0	0.960 0	0.970 0
ETCPS[11]	0.984 5	0.984 6	0.984 5	0.984 5
PSFREL	**0.996 3**	**0.996 6**	**0.996 5**	**0.996 5**

同时在 CIC-IDS2018、IoT-23 和 USTC-TFC2016 数据集上进行了上述的对比实验,部分结果如表 4 所示。在 CIC-IDS2018 数据集代表的复杂攻击场景中 ,PSFREL 的 $F1$ 达到 0.95,显著优于 ETCPS[11](0.91),其路径签名特征能有效捕捉 DDoS 攻击中的高频交互异常。在 IoT-23 数据集代表的物联网流量中,PSFREL 的 $F1$ 为 0.89,高于 Deep Packet[4](0.81),本文方法中 Cam-resnet 的注意力聚焦 MQTT-TLS 协议字段(如 Client ID)促进了算法性能改善。在 USTC-TFC2016 数据集代表的混合应用场景中,PSFREL 的 F1 达到 0.96,表明多粒度特征融合能适应视频流与即时通讯的混合流量分类。

表 4 多数据集实验结果($F1$ 分数)

Table 4 Results of multi-dataset experiments ($F1$ scores)

方法	ISCX VPN-nonVPN	CIC-IDS2018	IoT-23	USTC-TFC2016	平均 $F1$ Score
CNN+LSTM	0.980 0	0.860 0	0.780 0	0.890 0	0.877 5
ETCPS[11]	0.984 5	0.910 0	0.830 0	0.920 0	0.911 1
Deep Packet[4]	0.970 0	0.890 0	0.810 0	0.900 0	0.892 5
PSFREL	**0.996 5**	**0.950 0**	**0.890 0**	**0.960 0**	**0.949 1**

在 IoT-23 数据集上,PSFREL 的 $F1=0.89$,虽然未能超过 0.9,但仍高于其他基准方法。这主要是由于物联网设备流量中短会话占比高(平均包数<5),影响了各类方法的性能,也导致路径签名难以提取较长的交互特征。未来将探索自适应窗口大小的路径签名计算方法以优化此问题。

3.4.2 消融实验

为了验证本文模型各部分的有效性,从以下 2 方面设计消融实验:是否使用路径签名特征(PSF),是否使用结合通道注意力机制的网络 Cam-resnet。如表 5 所示,加入了路径签名特征后,模型效果有显著增加,准确率和 $F1$ 分数都提高了约 2%。路径签名捕捉的加密流量间包级粒度特征进一步丰富了流量的全局交互行为特征,其具有的唯一性和重参数化不变性等特点使其能够更好地表征流量之间的关联特征。

表 5 路径签名的消融对比

Table 5 Ablation comparison of path signatures

方法	A	P	R	$F1$
No PSF	0.972 9	0.979 1	0.972 9	0.974 9
With PSF	0.996 3	0.996 6	0.996 5	0.996 5

如表 6 所示,去除 Cam-resnet 后的模型各项性能指标显著下降,说明 Cam-resnet 所提取的全局流量特征是 PSFREL 中必不可少的重要特征;另外,Cam-resnet 的跳跃连接使得网络可以学习到输入数据的残差(即输出与输入之间的差异),这有助于 PSFREL 更快地学习到有效的特征表示,使其更好地适应数据的分布变化。

表 6　Cam-resnet 网络的消融对比

Table 6　Optimize the ablation comparison of residual networks

方法	*A*	*P*	*R*	*F*1
No Cam-resnet	0.745 0	0.877 4	0.744 9	0.791 2
With Cam-resnet	0.996 3	0.996 6	0.996 5	0.996 5

3.4.3　效率与资源消耗评估

为验证 PSFREL 的实用性,本文从时间效率和资源占用两方面对模型性能进行评估,对比模型包括 CNN+LSTM、ETCPS[11] 和 Deep Packet[4]。实验环境统一为:AMD EPYC 7532 CPU, RTX 3060 GPU, 16GB 内存,Batch Size = 64。

如表 7 所示,PSFREL 的单 epoch 训练时间高于 ETCPS,但低于 Deep Packet,这是由于多粒度特征融合增加了计算复杂度,但 Cam-resnet 的轻量化设计缓解了这一问题,使得 PSFREL 的参数量显著低于 Deep Packet,表明其轻量化设计有效控制了模型复杂度。PSFREL 的单 Batch 流量的平均检测时间也快于基线方法。除此之外,PSFREL 的 GPU 内存峰值为 3.5 GB,处于中等水平,可以部署在边缘设备(如防火墙)中。

表 7　时间效率与空间消耗对比

Table 7　Time efficiency versus space consumption

方法	参数量/MB	单 epoch 训练时间/s	Batch Size = 64 平均时间±标准差(秒/个)	GPU 内存峰值/GB
CNN+LSTM	12.4	42.3	0.85±0.03	3.2
ETCPS[11]	8.7	38.7	0.92±0.05	**2.5**
Deep Packet[4]	25.6	65.5	1.15±0.08	4.8
PSFREL	**15.3**	**55.8**	**0.78±0.02**	3.5

4　结论

针对传统加密流量检测方法存在特征表征不足和单一粒度等问题,且未充分提取流量间交互行为的特征不变性,本文提出一种基于路径签名表征学习的加密流量检测方法 PSFREL,利用路径签名来表征加密流量间的交互行为特征,并与流量字段级粒度的局部统计特征相结合,提取了更多加密后隐匿的有效流量特征,形成多粒度流量特征后增强流量的全局行为特征。实验表明,PSFREL 在多种加密协议(HTTPS、MQTT-TLS)和复杂场景(DDoS 攻击、物联网流量)中均表现出较强的泛化能力,其核心优势在于 2 点:(1)路径签名的协议无关性,即通过高阶积分过滤加密噪声,提取跨协议的交互行为本质特征;(2)注意力机制的场景适应性,即 Cam-resnet 动态聚焦不同场景的关键特征(如 DDoS 的攻击频率、物联网的 Client ID)。此外,模型对短会话流量的敏感性仍需进一步优化,未来将探索结合动态路径签名与图神经网络(GNN)建模会话关联性。

参考文献:

[1] 侯剑,鲁辉,刘方爱,等. 加密恶意流量检测及对抗综述[J]. 软件学报,2024,35(1):333-355.
HOU Jian, LU Hui, LIU Fangai, et al. A review of encrypted malicious traffic detection and countermeasure[J]. Journal of Software, 2024, 35(1):333-355.

[2] 陈子涵,程光,徐子恒,等. 互联网加密流量检测、分类与识别研究综述[J]. 计算机学报,2023,46(5):1060-1085.
CHEN CHENG Zihan, XU Guang, XU Ziheng, et al. A review of research on detection, classification and recognition of encrypted traffic on the internet[J]. Journal of Computing, 2023, 46(5):1060-1085.

[3] LONG G, ZHANG Z X. Deep encrypted traffic detection: an anomaly detection framework for encryption traffic based on parallel automatic feature extraction[J]. Computational Intelligence and Neuroscience, 2023, 2023:3316642.

[4] LOTFOLLAHI M, JAFARI S M, SHIRALI H Z R, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3):1999-2012.

[5] AGRAWAL S, SOHI B S. Feature optimization and performance evaluation of machine learning algorithms for identification of P2P traffic[J]. Journal of Advances in Information Technology, 2012, 3(2):107-114.

[6] WANG Z H, THING V L L. Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms[J]. Computers & Security, 2023, 128:103143.

[7] ZHAO J J, LI Q, HONG Y P, et al. MetaRockETC: adaptive encrypted traffic classification in complex network environments via time series analysis and meta-learning[J]. IEEE Transactions on Network and Service Management, 2024, 21(2):2460-2476.

[8] CHEN C, QU L F, AMIRPOUR H, et al. On the security of selectively encrypted HEVC video bitstreams[J]. ACM Transactions on Multimedia Computing, Communications, and Applications, 2024, 20(9):1-27.

[9] WANG Z H, WANG J R, LIU Y, et al. Privacy-preserving attribute-based access control scheme with intrusion detection and policy hiding for data sharing in VANET[J]. IEEE Internet of Things Journal, 2024, 11(13):23348-23369.

[10] 谷勇浩,徐昊,张晓青. 基于多粒度表征学习的加密恶意流量检测[J]. 计算机学报,2023,46(9):1888-1899.
GU Yonghao, XU Hao, ZHANG Xiaoqing. Encrypted malicious traffic detection based on multi-granularity representation learning[J]. Journal of Computing, 2023, 46(9):1888-1899.

[11] XU S J, GENG G G, JIN X B, et al. Seeing traffic paths: encrypted traffic classification with path signature features[J]. IEEE Transactions on Information Forensics and Security, 2022, 17:2166-2181.

[12] CHEVYREV I, KORMILITZIN A. A primer on the signature method in machine learning[EB/OL]. https://arxiv.org/abs/1603.03788

[13] WANG Y, ZHANG L, CHEN H. High-frequency trading anomaly detection via signature-transformer[J]. IEEE Transactions on Financial Informatics, 2023, 19(4):1234-1245.

[14] LI H, WANG Q, LIU Z. Reinforcement learning optimized path signatures for motion rehabilitation assessment[J]. ACM Transactions on Health Informatics, 2023, 10(3):1-18.

[15] GUO S, ZHOU T, LI H. Dynamic gene regulatory network modeling via path signature-GNN[J]. Bioinformatics, 2024, 40(1):1-10.

[16] ZHAO Z M, LI Z X, JIANG J L, et al. ERNN: error-resilient RNN for encrypted traffic detection towards network-induced phenomena[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 99:1-18.

[17] WANG Q L, WU B G, ZHU P F, et al. ECA-net: efficient channel attention for deep convolutional neural networks[C]// 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Seattle: IEEE, 2020:11534-11542.

[18] 麻文刚,张亚东,郭进. 基于LSTM与改进残差网络优化的异常流量检测方法[J]. 通信学报,2021,42(5):23-40.
MA Wengang, ZHANG Yadong, GUO Jin. Anomalous traffic detection method based on LSTM with improved residual network optimization[J]. Journal of Communications, 2021, 42(5):23-40.

[19] ZHANG S H, MA L F, LIU H J. Encryption-decryption-based event-triggered consensus control for nonlinear MASs under DoS attacks[J]. International Journal of Robust and Nonlinear Control, 2024, 34(1):132-146.

[20] WANG M N, ZHENG K F, LUO D, et al. An encrypted traffic classification framework based on convolutional neural networks and stacked autoencoders[C]//2020 IEEE 6th International Conference on Computer and Communications (ICCC). Chengdu: IEEE, 2020:634-641.

[21] WANG Z H, THING V L L. Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms[J]. Computers & Security, 2023, 128:103143.

[22] CUI S S, JIANG B, CAI Z Z, et al. A session-packets-based encrypted traffic classification using capsule neural networks [C] // 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Zhangjiajie: IEEE, 2019.

(编辑:祁业卿)