基于时空融合异质图神经网络的加密流量分类方法

张祝育，高丽婷
（河北建筑工程学院　信息工程学院　河北省智慧城市感知与智能计算重点实验室，河北　张家口　075000）

摘　要：针对现有图神经网络加密流量分类模型对图结构质量高度敏感、未区分数据包头部与载荷功能差异，导致分类精度受限的问题，提出一种基于时空融合异质图神经网络的加密流量分类方法。该方法基于点间互信息构建字节级异质图，通过图采样与聚合网络提取拓扑特征，结合双向长短期记忆网络捕捉流量时序规律，设计交叉门控机制实现特征自适应融合。在 ISCX Tor-nonTor 公开数据集上的实验结果表明，该方法分类准确率达 91.35%，综合性能优于主流基线模型，可为加密流量精细化管控提供支撑。

关键词：加密流量分类；图神经网络；时空特征融合；异质图构建；交叉门控融合
中图分类号：TP309;TP393　　**文献标志码：**A　　**DOI:**10.19358/j.issn.2097-1788.2026.07.002

中文引用格式：张祝育，高丽婷. 基于时空融合异质图神经网络的加密流量分类方法[J]. 网络安全与数据治理，2026，45(7)：9-15.
英文引用格式：Zhang Zhuyu，Gao Liting. STM-GraphSAGE based encrypted traffic classification method[J]. Cyber Security and Data Governance，2026，45(7)：9-15.

STM-GraphSAGE based encrypted traffic classification method

Zhang Zhuyu，Gao Liting
（Hebei Key Laboratory of Smart City Perception and Intelligent Computing，
College of Information Engineering，Hebei University of Architecture，Zhangjiakou 075000，China）

Abstract：To address the problem that existing graph neural network-based encrypted traffic classification models are highly sensitive to the quality of graph structure and fail to distinguish the functional differences between packet headers and payloads，which leads to limited classification accuracy，this paper proposes an encrypted traffic classification method based on a spatio-temporal fusion heterogeneous graph neural network. This method constructs byte-level heterogeneous graphs via pointwise mutual information，extracts topological features through the graph sample and aggregate network，captures the temporal patterns of traffic with a bidirectional long short-term memory network，and designs a cross-gated mechanism to realize adaptive feature fusion. Experimental results on the public ISCX Tor-nonTor dataset demonstrate that the proposed method achieves a classification accuracy of 91.35%，outperforms mainstream baseline models in comprehensive performance，and can provide support for the refined management and control of encrypted traffic.

Key words：encrypted traffic classification；graph neural networks；spatio-temporal feature fusion；heterogeneous graph construction；cross-gated feature fusion

0　引言

随着加密技术的广泛普及，流量加密在保障用户通信隐私的同时，也为恶意流量隐匿提供了可乘之机，给网络安全管控带来严峻挑战[1]。加密流量分类是网络安全防护的重要技术。现有基于深度学习的加密流量分类方法主要分为序列建模与图建模两大范式。其中，以卷积神经网络（Convolution Neural Network，CNN）、长短期记忆网络（Long Short-Term Momory，LSTM）为代表的序列模型虽实现了端到端分类[2]，但受限于一维序列的建模约束，无法挖掘流量字节间的全局拓扑关联[3]。以图神经网络（Graph Neural Network，GNN）为代表的图建模方法虽弥补了序列模型的拓扑特征挖掘短板[4]，但仍存在语义区分不足[5]、特征融合机制简单[6]两大核心瓶颈，在高匿名加密流量的细粒度分类场景中性能受限。

针对上述问题，本文提出一种基于图采样与聚合

（Graph Sample and Aggregate，GraphSAGE）网络与双向长短期记忆网络（Bidirectional LSTM，BiLSTM）的时空融合异质图加密流量分类模型（Spatio-Temporal Fusion Heterogeneous Graph Model for Encrypted Traffic Classification Based on GraphSAGE，STM-GraphSAGE）。本文的主要贡献如下：

（1）基于点间互信息构建数据包头部与载荷的字节级异质子图，配套双重独立嵌入层，解决了现有同质图建模对两类数据功能差异区分不足的问题，有效降低了图结构噪声干扰。

（2）设计时空特征协同提取架构，通过 GraphSAGE 与 BiLSTM 分别提取流量空间拓扑特征与时序演化规律，引入跳跃知识机制缓解图神经网络过平滑问题，实现时空特征的高效互补提取。

（3）提出交叉门控自适应特征融合机制，实现头部与载荷特征的交叉筛选与自适应融合，解决了传统特征拼接的交互不足问题，显著提升了流量特征的判别能力。

1 相关工作

现有加密流量分类的深度学习方法主要分为序列建模与图神经网络建模两大主流分支。

序列建模方法上，Lin 等人[7]提出 ET-BERT 预训练模型，通过大规模未标记流量学习数据报级上下文表示；Park 等人[8]提出 MLETC 模型，实现字节、字段、数据包三级粒度的特征学习；Wang 等人[9]提出 App-Net 模型，结合 BiLSTM 与 CNN 提取流量时序与局部特征。但此类方法受限于一维序列建模范式，无法挖掘流量字节间的全局拓扑关联，在高匿名流量场景下细粒度识别能力不足。

在图神经网络建模方向上，GNN 凭借对非结构化图数据的强拓扑建模能力，为加密流量的拓扑特征挖掘提供了新的技术路径。现有研究多将流量转化为图分类任务，通过构建流量交互图完成特征提取：Shen 等人[10]提出 GraphDApp 模型，基于数据包长度与方向构建流量交互图实现分类；喻晓伟等人[11]结合流量交互图与图卷积网络，进一步提升了拓扑特征挖掘能力。但现有基于 GNN 的方法仍存在两大技术局限：其一，大多采用同质图统一建模数据包头部与载荷，未区分二者的功能语义差异，拓扑特征挖掘缺乏针对性；其二，时空特征融合多采用简单拼接方式，缺乏自适应的特征交互与筛选机制，特征判别能力受限，难以适配高匿名加密流量的细粒度分类场景。

2 方法构建

2.1 整体架构

STM-GraphSAGE 模型的整体处理流程分为 6 个核心模块：数据预处理模块、基于点互信息（Pointwise Mutual Information，PMI）的字节级流量图构建模块、双重嵌入层模块、GraphSAGE 图特征编码模块、交叉门控自适应特征融合模块以及 BiLSTM 时序建模与分类模块。整体架构如图 1 所示。

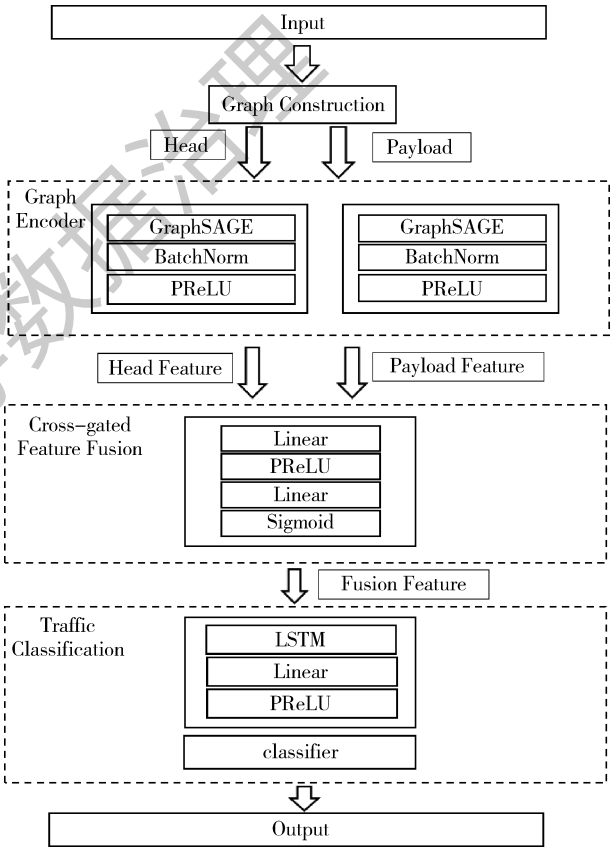

图 1　整体架构图

首先，对原始流量数据完成会话解析、预处理与头部-载荷语义分离；其次，基于 PMI 分别为头部与载荷构建字节级独立异质图；通过双重独立嵌入层完成字节节点的高维语义映射，保证头部与载荷特征在独立语义空间完成编码，避免语义混淆；而后，采用双路并行的 GraphSAGE 编码器，分别提取头部与载荷异质图的空间拓扑特征，通过跳跃知识机制缓解图神经网络过平滑问题，生成高判别力的单包头部与载荷特征；经交叉门控融合机制，实现头部与载荷特征的双向交叉筛选与自适应融合；最终，将连续数据包的融合特征序列输入 BiLSTM，捕捉流量会话层面的时序演化规律，通过全连接层与 Softmax 分类器输出最终分

类结果。

2.2 基于 PMI 的字节级流量图构建

数据包头部为协议控制字段，具有固定格式与强字节关联规律；载荷为加密后的数据，字节分布高度随机化，仅存在与应用行为相关的弱关联规律。统一建模会导致图结构噪声干扰严重，拓扑特征挖掘缺乏针对性。为此，根据现有方法[12]，本文基于点间互信息[13]构建字节级流量图。因头部与载荷的字节语义规律存在本质差异，本文为二者分别构建独立异质图，具体构建流程如下。

2.2.1 图节点定义

数据包原始字节为 8 位无符号整数，取值范围 0~255，本文将每个唯一字节值定义为一个独立节点，图节点总数不超过 256 个，节点初始特征为对应字节值。

2.2.2 基于 PMI 的边构建

PMI 是量化两个事件共现关联强度的经典指标，本文采用 PMI 计算字节间的关联度，其计算公式如式（1）所示：

$$\mathrm{PMI}(i,j)=\log_2\left(\frac{p(i,j)}{p(i)\cdot p(j)}\right) \tag{1}$$

式中，$p(i)$、$p(j)$分别为字节 i 和字节 j 在滑动窗口内出现的边缘概率，$p(i,j)$ 为字节 i 和字节 j 在同一滑动窗口内的联合共现概率。

基于 PMI 计算结果，本文定义图的邻接矩阵 $\boldsymbol{A}$ 如式（2）所示：

$$\boldsymbol{A}_{ij}=\begin{cases}1,\mathrm{PMI}(i,j)>0\\0,\mathrm{Otherwise}\end{cases} \tag{2}$$

式(2)表明，仅当两个字节的 PMI 值大于 0 时，判定二者存在正相关语义关联，为对应节点间创建无向边并以 PMI 值作为边权重；否则不建边，以此过滤无意义的噪声关联，降低图结构冗余。

TCP/UDP 协议头部的典型字段长度为 1~4 字节，故本文设置滑动窗口大小为 5，遍历预处理后的头部与载荷字节序列，统计窗口内字节的出现与共现频次并计算全量字节对 PMI 值，为每个数据包的头部与载荷分别构建独立无向异质图，作为后续双路空间特征提取模块的输入。

2.3 双重嵌入层

相同字节值在头部与载荷中语义存在本质差异，共用嵌入层会导致语义混淆。因此本文设计双重嵌入层，采用两个不共享参数的独立嵌入层，分别对头部与载荷的字节节点进行高维映射。

设嵌入维度为 d_0，字节取值的总数量为 $K=256$，则头部嵌入矩阵 $\boldsymbol{E}_{\mathrm{header}}\in\mathbb{R}^{K\times d_0}$ 与载荷嵌入矩阵 $\boldsymbol{E}_{\mathrm{payload}}\in\mathbb{R}^{K\times d_0}$ 分别为两个嵌入层的可学习参数，每个字节值通过查表的方式，从对应的嵌入矩阵中获取其高维嵌入向量，作为图神经网络的初始输入特征。

嵌入维度需平衡特征表征能力、模型参数量与过拟合风险。256 个唯一字节值的语义表征需足够的维度空间保证特征区分度；同时维度不宜过高，避免参数量爆炸与过拟合。预实验结果表明：嵌入维度为 32 时，特征表征能力不足，分类准确率仅为 87.64%；嵌入维度为 64 时，准确率提升至 90.21%；嵌入维度为 128 时，参数量提升 1 倍，训练速度下降 40%，且出现轻微过拟合，准确率仅提升 0.13 个百分点。综合考虑表征能力、计算开销与泛化性能，最终选定嵌入维度为 64。

2.4 流量图特征编码

本文采用 4 层堆叠的 GraphSAGE 构建图特征编码器，并为头部与载荷异质图分别设置两路参数完全独立的编码器，两路编码器并行计算、互不干扰。编码器的计算分为邻居聚合、节点特征更新、跳跃知识特征融合、图级特征生成四个步骤，完整计算流程如下。

2.4.1 邻居聚合

对于图中任意目标节点 v，第 l 层网络首先对其所有邻居节点的特征进行均值聚合，生成邻居聚合特征，实现节点邻域拓扑信息的聚合，计算公式如式（3）所示：

$$\boldsymbol{m}_{N(v)}^{(l)}=\sum\nolimits_{u\in N(v)}\frac{\boldsymbol{h}_u^{(l-1)}}{|N(v)|} \tag{3}$$

式中，$N(v)$为节点 v 的一阶邻居节点集合，$\boldsymbol{h}_u^{(l-1)}$ 为第 $l-1$ 层网络输出的邻居节点 u 的特征向量，$|N(v)|$为节点 v 的邻居节点数量，$\boldsymbol{m}_{N(v)}^{(l)}$ 为第 l 层网络生成的节点 v 的邻居聚合特征。

2.4.2 节点特征更新

完成邻居聚合后，将目标节点自身的上一层特征与邻居聚合特征进行拼接，通过线性变换与非线性激活函数，生成当前层的节点特征，实现节点自身特征与邻域拓扑信息的融合，计算公式如式（4）所示：

$$\boldsymbol{h}_v^{(l)}=\mathrm{PReLU}(\boldsymbol{w}^{(l)}\,\mathrm{CONCAT}(\boldsymbol{h}_v^{(l-1)},\boldsymbol{m}_{N(v)}^{(l)})) \tag{4}$$

其中，$\boldsymbol{h}_v^{(l-1)}$为第 $l-1$ 层网络输出的目标节点 v 的特征向量，$\boldsymbol{w}^{(l)}$为第 l 层网络的可学习权重矩阵，CONCAT(·)为特征拼接操作，PReLU 为带参数的修正线性单元激活函数。

在激活函数与归一化设计上，本文做了两处针对性优化：

一是激活函数选择。选用 PReLU 而非传统的 ReLU 函数作为非线性激活函数。其优势在于，PReLU 为负值输入设置了可学习的斜率参数，解决了 ReLU 函数的神经元死亡问题，同时可通过不同通道的差异化斜率，实现类似通道注意力的特征筛选效果，更适配加密流量字节特征的细粒度表征需求。

另一个是批量归一化操作。在每一层 GraphSAGE 的特征更新后，均加入批量归一化（BatchNorm）操作，将特征分布归一化至标准正态分布，有效缓解深度网络训练中的内部协变量偏移问题，加速模型收敛，同时抑制过拟合。

2.4.3 跳跃知识特征融合

为缓解深层 GNN 过平滑问题，本文引入跳跃知识机制，将 4 层 GraphSAGE 网络输出的节点特征进行全拼接，保留不同网络层的多尺度拓扑信息，其中浅层网络捕捉字节间的局部邻域关联，深层网络捕捉全图的全局拓扑规律。通过多尺度特征融合，避免深层网络节点特征同质化，计算公式如式（5）所示：

$$\boldsymbol{h}_v^{\text{Final}}=\text{CONCAT}(\boldsymbol{h}_v^{(1)},\boldsymbol{h}_v^{(2)},\boldsymbol{h}_v^{(3)},\boldsymbol{h}_v^{(4)}) \tag{5}$$

其中，$\boldsymbol{h}_v^{\text{Final}}$ 表示节点 v 的最终嵌入特征向量，$\boldsymbol{h}_v^{(1)}$，$\boldsymbol{h}_v^{(2)}$，$\boldsymbol{h}_v^{(3)}$，$\boldsymbol{h}_v^{(4)}$ 分别为第 1 至 4 层 GraphSAGE 输出的节点特征向量。

2.4.4 图级特征生成

完成节点级多尺度特征融合后，通过全局均值池化操作，将所有节点的特征聚合为统一维度的图级特征向量，实现从节点级特征到数据包级图特征的映射。对头部异质图与载荷异质图的编码结果分别执行该操作，得到头部特征 $\boldsymbol{g}_h$ 与载荷特征 $\boldsymbol{g}_p$，计算公式如下：

$$\boldsymbol{g}_h=\frac{\boldsymbol{h}_1^{\text{final}}\oplus\cdots\oplus\boldsymbol{h}_{|v|}^{\text{final}}}{|V_h|} \tag{6}$$

$$\boldsymbol{g}_p=\frac{\boldsymbol{h}_1^{\text{final}}\oplus\cdots\oplus\boldsymbol{h}_{|v|}^{\text{final}}}{|V_p|} \tag{7}$$

式中，V_h、V_p 分别为头部异质图与载荷异质图的节点集合，$|V_h|$、$|V_p|$为对应图的节点数量。最终生成的 $\boldsymbol{g}_h$ 与 $\boldsymbol{g}_p$ 将作为下游交叉门控自适应特征融合模块的输入，完成头部与载荷特征的深度融合。

2.5 交叉门控自适应特征融合

经双路 GraphSAGE 编码器分别编码后，可得到头部异质图的全局特征与载荷异质图的全局特征，其中头部特征承载 TCP/UDP 协议的控制语义与流量交互的基础规则信息，载荷特征则对应加密应用的行为模式与业务交互特征，二者的特征分布、判别贡献度随加密流量类型呈现显著的动态异质性。

为实现对两类特征维度的精细化权重分配，本文构建两路参数完全解耦的双层非线性门控网络，分别从头部特征与载荷特征中学习对应维度的重要性权重向量。对于头部特征 $\boldsymbol{g}_h$，头部门控网络以两层全连接层为基础结构，先通过线性变换与 PReLU 非线性激活完成特征的高维映射，挖掘特征维度间的非线性关联，再经 Sigmoid 函数将输出值归一化至(0,1)区间，生成头部门控向量 $\boldsymbol{s}_h$。同理，载荷门控网络以载荷特征 $\boldsymbol{g}_p$ 为输入，通过结构一致但参数完全独立的双层非线性网络，生成载荷门控向量 $\boldsymbol{s}_p$，相关计算公式如下：

$$\boldsymbol{s}_h=\text{Sigmoid}(\boldsymbol{w}_{h2}^{\text{T}}\text{PReLU}(\boldsymbol{w}_{h1}^{\text{T}}\boldsymbol{g}_h+\boldsymbol{b}_{h1})+\boldsymbol{b}_{h2}) \tag{8}$$

$$\boldsymbol{s}_p=\text{Sigmoid}(\boldsymbol{w}_{p2}^{\text{T}}\text{PReLU}(\boldsymbol{w}_{p2}^{\text{T}}\boldsymbol{g}_p+\boldsymbol{b}_{p1})+\boldsymbol{b}_{p2}) \tag{9}$$

式中，$\boldsymbol{w}_{*1}^{\text{T}}$，$\boldsymbol{w}_{*2}^{\text{T}}$，$\boldsymbol{b}_{*1}$，$\boldsymbol{b}_{*2}$ 分别代表线性层的权重与偏置，$\boldsymbol{s}_h$、$\boldsymbol{s}_p$ 为头部门控与载荷门控向量，$\boldsymbol{g}_h$、$\boldsymbol{g}_p$ 为对应图级特征。其中 PReLU 激活函数为负值输入设置了可学习的斜率参数，避免了 ReLU 函数易出现的神经元失活问题，保证门控网络对细粒度特征关联的非线性拟合能力；Sigmoid 函数则将权重值约束在（0，1）区间，使门控向量的每个元素与输入特征对应维度逐元素关联，作为对应维度的重要性系数，值越接近 1 代表该维度特征的判别力越强，越接近 0 则代表该维度为冗余噪声特征。

交叉筛选后的载荷特征与头部特征的计算公式如式（10）所示：

$$\boldsymbol{z}=\text{CONCAT}(\boldsymbol{s}_h\odot\boldsymbol{g}_p,\boldsymbol{s}_p\odot\boldsymbol{g}_h) \tag{10}$$

式中，⊙为点积，CONCAT(·)为通道拼接操作，最终生成数据包级的综合融合特征 $\boldsymbol{z}$。

2.6 基于 BiLSTM 的时序特征建模与分类

经交叉门控自适应特征融合得到的数据包级特征，仅能表征单包内的字节拓扑关联，而加密流量的应用行为模式本质蕴含于连续数据包的时序演化规律中。为此，本文构建基于双向长短期记忆网络（BiLSTM）的时序特征提取模块，挖掘流量会话的长程时序依赖与双向交互特征，为分类任务提供会话级的动态行为表征。

对于单条加密流量会话，取连续 T 个数据包的融合特征，按时间顺序构建时序输入序列 $\boldsymbol{Z}=[z_1,z_2,\cdots,z_T]$，其中 z_t 为第 t 个数据包交叉门控融合后的特征向量，T 为时序序列长度。本文采用两层双向 LSTM 构建时序编码器，其由前向与后向两个独立的 LSTM 分支构成，分别沿时间正、反方向捕捉流量序列的前向演化规律与反向依赖关系，完整刻画客户端–服务器双向交互的时序特征；LSTM 单元通过遗忘门、输入门、输

出门的门控机制实现时序信息的选择性传递，有效解决传统循环神经网络的长序列梯度消失问题。经 BiLSTM 编码后，取序列最后一个时刻的双向隐藏状态拼接结果 $\boldsymbol{H}_T$，作为整条流量会话的全局时序特征输入分类器。

分类器采用两层全连接结构，第一层以 PReLU 为激活函数完成特征的非线性映射，配合 Dropout 层抑制模型过拟合；第二层通过 Softmax 激活函数输出流量类别的预测概率分布，最终预测结果可用式（11）表示：

$$\hat{\boldsymbol{y}}=\text{Softmax}(\text{Classifier}(\text{BiLSTM}(\boldsymbol{z}_1,\boldsymbol{z}_2,\cdots,\boldsymbol{z}_T))) \tag{11}$$

本文采用多分类交叉熵函数作为模型端到端训练的损失函数，计算公式如式（12）所示：

$$\mathcal{L}=-\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C}y_{ic}\log(\hat{y}_{ic}) \tag{12}$$

式中，N 为训练批次内的样本数量，C 为加密流量分类的总类别数，y_{ic} 为第 i 个样本真实标签的 one-hot 编码，$\hat{y}_{ic}$ 为该样本属于第 c 类的预测概率。

3 实验与结果分析

3.1 实验环境

本实验基于 PyTorch 深度学习框架与 PyTorch Geometric 图神经网络库实现，所有实验均在搭载 NVIDIA RTX 3080 GPU 的硬件平台上完成。模型训练采用 Adam 优化器，批次大小 32，初始学习率 5×10^{-4}，最大训练轮数 100，采用余弦退火与早停防止过拟合。核心超参数设置：字节节点嵌入维度 64，4 层 GraphSAGE 隐藏层维度 128，PMI 滑动窗口大小 5，2 层 BiLSTM 隐藏单元数 256。

3.2 数据集与数据预处理

本实验采用公开标准的 ISCX Tor2016 匿名流量数据集，该数据集覆盖 Tor 网络下 7 类典型应用流量，分别为音频、网页浏览、即时聊天、文件传输、邮件、P2P、视频。

实验按 9∶1 的比例完成训练集与测试集的类别内划分，保证类别平衡且无数据泄露：训练集每类 18 000 条，总计 126 000 条；测试集每类 2 000 条，总计 14 000 条，全数据集类别完全平衡。

数据预处理环节，完成流量会话的字节级解析与头部-载荷分离，基于点间互信息 PMI 分别构建头部与载荷的字节级无向异质图，同步完成节点特征编码、图结构归一化处理，最终输出标准化图数据集。

3.3 对比实验

本文选用以下三种模型作为对比模型。

GRAIN[14]：GRAIN 传统机器学习基线，基于流量统计特征实现分类。

App-Net[9]：App-Net 序列建模基线，结合 CNN 与 LSTM 提取流量时序与局部特征。

GraphDApp[10]：GraphDApp 图神经网络基线，基于同质流量交互图实现分类。

所有实验均在 ISCX Tor2016 数据集上完成，结果如表 1 所示。

表 1　不同算法在 ISCX Tor2016 数据集上的分类性能对比

算法	准确率/%	精确率/%	召回率/%	F1 值/%
GRAIN[14]	70.14	58.53	58.46	58.34
App-Net[9]	73.43	56.92	56.74	56.68
GraphDApp[10]	52.86	33.57	23.09	22.92
本文算法	91.35	91.21	91.28	91.24

由表 1 可见，本文 STM-GraphSAGE 模型在 4 项核心指标上均大幅优于所有基线模型，分类准确率达 91.35%，较性能最优的基线模型 App-Net 提升 17.92 个百分点。

模型训练过程的损失变化如图 2 所示。

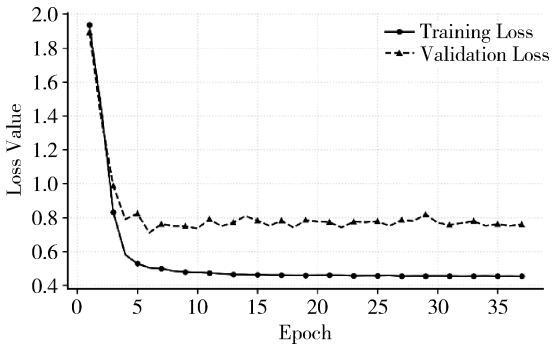

图 2　模型训练损失曲线

由图 2 可见，模型训练损失与验证损失均随迭代轮次增加快速下降，迭代 10 轮后进入平稳收敛阶段；全程两条曲线无明显背离，无损失发散现象，模型训练过程稳定，未发生过拟合。

模型的训练过程准确率变化情况如图 3 所示。

由图 3 可见，训练与验证曲线趋势高度一致，迭代 10 轮后快速平稳收敛，无过拟合现象。

模型分类结果的混淆矩阵如图 4 所示。

从图 4 可见，模型对音频、网页浏览、文件传输、

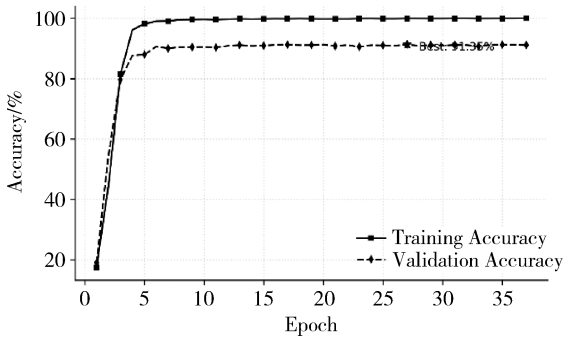

图 3　模型训练准确率曲线

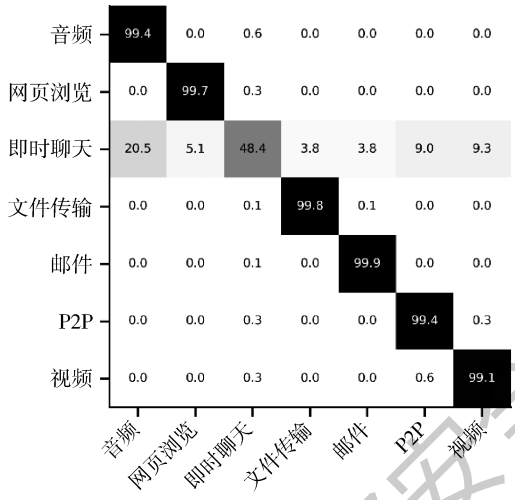

图 4　模型分类结果的混淆矩阵

邮件类流量识别准确率接近 100%，仅即时聊天类流量存在少量误分，整体分类稳定性优异。

3.4　消融实验

为量化验证本文 STM-GraphSAGE 模型各核心创新模块的性能贡献，采用控制变量法在 ISCX Tor2016 数据集上开展消融实验，通过剥离、替换核心组件设置消融变体。

（1）移除 Payload 图分支，仅保留 Header 图分支，记为 A_Header；

（2）移除 Header 图分支，仅保留 Payload 图分支，记为 A_Payload；

（3）移除 BiLSTM 时序模块，仅保留空间拓扑特征提取模块，记为 A_BiLSTM；

（4）移除交叉门控融合机制，头部与载荷特征采用直接拼接方式融合，记为 A_Concatenation。

消融实验结果如表 2 所示。

实验结果表明：仅保留 Header 图分支时模型仍保持较高性能，而仅保留 Payload 图分支时分类效果极差，说明流量头部信息包含核心判别特征，头部-载荷双异质图建模是模型性能的基础；移除 BiLSTM 时序模块后准确率下降 4. 26 个百分点，验证了时序建模对流量序列规律捕捉的关键作用，时空双路架构可实现特征优势互补；将交叉门控替换为特征直接拼接后，模型准确率下降 22. 26 个百分点，充分证明该机制可实现特征的自适应筛选融合，是提升特征判别力的核心设计。

表 2　消融实验结果

算法	准确率/%	精确率/%	召回率/%	F1 值/%
A_Header	88. 29	88. 27	88. 27	88. 22
A_Payload	19. 29	19. 15	19. 22	19. 18
A_BiLSTM	87. 09	86. 95	87. 02	86. 98
A_Concatenation	69. 09	68. 95	69. 02	68. 98
本文算法	91. 35	91. 21	91. 28	91. 24

综上，本文完整模型核心指标均优于所有消融变体，各创新模块均对分类性能有正向贡献。

4　结论

本文提出一种基于 STM-GraphSAGE 模型的加密流量分类方法，通过将流量报文头与载荷构造为字节级无向图，利用图神经网络自适应学习流量拓扑与字节关联特征，实现细粒度匿名流量端到端分类。实验结果表明，该方法相比传统序列模型能更有效地挖掘流量潜在结构信息，在匿名流量分类任务中具备更优的特征表达与分类性能。

然而该方案仍存在局限：短会话类流量因特征稀疏性存在分类瓶颈，同时图结构建模也带来一定计算开销。未来可从多方面优化改进：针对短流量设计图数据增强策略以提升弱特征场景性能；对模型进行轻量化改造，降低资源消耗以适配实时部署需求；并将方法拓展至多类加密流量场景，进一步增强模型泛化能力。

参考文献

[1] 龚碧,刘建,唐小妹,等. 加密流量智能化分析技术:现状、进展与挑战[J]. 电子与信息学报,2026,48(3):1180-1197.

[2] 王晓. 端到端的加密流量分类方法研究[D]. 上海:上海理工大学,2024.

[3] 杨宇,唐东明,李驹光,等. 基于时空特征自适应融合网络的流量分类方法[J]. 电子测量技术,2024,47(3):661-674.

[4] 刘涛涛,付钰,俞艺涵,等. 基于并行流量图和图神经网络的加密流量分类方法[J]. 通信学报,2025,46(6):45-59.

[5] 燕齐鸿,杨文军. 基于 GraphSAGE 和图注意力网络的加密流量分类模型[J/OL]. 计算机工程,1-14[2026-04-01]. ht-

tps://doi.org/10.19678/j.issn.1000-3428.0252324.

[6] 张家琪,岳鹏飞,王钢,等.加密流量分析中的特征建模与学习范式研究综述[J/OL].计算机工程与应用,1-25[2026-04-04].https://link.cnki.net/urlid/11.2127.TP.20260310.1734.002.

[7] Lin Xinjie, Xiong Gang, Gou Gaopeng, et al. ET-BERT: a contextualized datagram representation with pre-training transformers for encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2022. Lyon: Association for Computing Machinery, 2022: 633-642.

[8] Park J T, Choi Y S, CHO B S, et al. Multi-level pre-training for encrypted network traffic classification[J]. IEEE Access, 2025, 13:68643-68659.

[9] Wang Xin, Chen Shuhui, Su Jinshu. App-Net: a hybrid neural network for encrypted mobile traffic classification[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops. Toronto: IEEE, 2020: 1-6.

[10] Shen Meng, Zhang Jinpeng, Zhu Liehuang, et al. Accurate decentralized application identification via encrypted traffic analysis using graph neural networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16:2367-2380.

[11] 喻晓伟, 陈丹伟.基于注意力机制的图神经网络加密流量分类研究[J].信息安全研究, 2023,9(1):13-21.

[12] Zhang Haozhen, Yu Le, Xiao Xi, et al. TFE-GNN: a temporal fusion encoder using graph neural networks for fine-grained encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2023. Austin: Association for Computing Machinery, 2023:2066-2075.

[13] Yao Liang, Mao Chengsheng, Luo Yuan. Graph convolutional networks for text classification[C]//Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence. Honolulu: AAAI Press, 2019:7370.

[14] Zaki F, Afifi F, Razak S A, et al. GRAIN: granular multi-label encrypted traffic classification using classifier chain[J]. Computer Networks, 2022, 213:109084.

(收稿日期: 2026-04-17)

作者简介:

张祝育 (2002-), 通信作者, 女, 硕士研究生, 主要研究方向: 计算机网络与信息安全。E-mail: 2407463975@qq.com。

高丽婷 (1973-), 女, 硕士, 副教授, 主要研究方向: 计算机网络及数据安全、大数据分析与应用。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部