基于双模型的半监督流形混合流量分类方法*

马　可[1]，何明枢[1]，蔡晶晶[2]，王小娟[1]
（1. 北京邮电大学　电子工程学院，北京　100876；2. 永信至诚科技集团股份有限公司，北京　100089）

摘　要：深度学习技术在网络流量分类领域中得到广泛应用，但存在对大量数据的依赖以及过拟合问题。为解决该问题，提出了一种结合双模型协作与流形混合的半监督深度学习方法。该方法使用教师-学生架构，通过移动指数平均辅助模型学习过程，从而提升模型的泛化性能，并于模型的特征空间中进行数据的流形混合，能够有效改善模型的决策边界，进一步增强模型的鲁棒性。实验结果表明，在不同数据类别，数据量为 1 000 的条件下，方法在三种网络流量数据集上都能达到 90% 以上的准确率，并在更少量数据的条件下保持较高的分类精度。

关键词：流量分类；半监督学习；流形混合；教师-学生模型
中图分类号：TP393.08　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097-1788.2026.01.001

中文引用格式：马可，何明枢，蔡晶晶，等. 基于双模型的半监督流形混合流量分类方法［J］. 网络安全与数据治理，2026，45(1)：1-8.
英文引用格式：Ma Ke，He Mingshu，Cai Jingjing，et al. A semi-supervised manifold mixup traffic classification method based on Mean-Teacher［J］. Cyber Security and Data Governance，2026，45(1)：1-8.

A semi-supervised manifold mixup traffic classification method based on Mean-Teacher

Ma Ke[1]，He Mingshu[1]，Cai Jingjing[2]，Wang Xiaojuan[1]
（1. School of Electronic Engineering，Beijing University of Posts and Telecommunications，Beijing 100876，China；
2. Integrity Technology Group Inc.，Beijing 100089，China）

Abstract：Deep Learning techniques have been widely applied in the field of network traffic classification. However，there still exist various challenges，including dependency on large scale data and overfitting. To address these issues，a semi-supervised deep learning method combining mean teacher and manifold mixup is proposed. This method employs a teacher-student architecture，utilizing Exponential Moving Average（EMA）to assist the model learning process and to enhance the generalization capability of model. Additionally，manifold mixup in the feature space effectively refines the model's decision boundary，strengthening robustness. Experimental results demonstrate that with only 1 000 samples per class，the method achieves over 90% accuracy across three network traffic datasets while maintaining outstanding performance under few-shot condition.

Key words：traffic classification；semi-supervised learning；manifold mixup；teacher-student model

0　引言

网络流量分类（Traffic Classification）技术能够精准识别不同应用程序或服务所产生的网络流量，同时探测出潜在的威胁流量，这对于维护网络安全与稳定运行具有关键意义。如今，互联网技术呈现出日新月异的发展态势，网络流量也随之呈现出爆炸式增长以及复杂化的特点。流量加密技术，诸如广泛运用的 TLS/SSL 协议，在切实保障用户隐私和数据安全方面成效显著。然而，这种加密技术的广泛应用也给网络流量分类带来了前所未有的挑战。

传统的流量分类方法，例如基于端口的方法，主要依据流量五元组中的端口号信息来推断应用类型。然而，面对当下动态端口和端口伪装技术，尤其是针对日益复杂的加密流量，这类简单依赖端口或明文载

*基金项目：国家自然科学基金（62402053，62227805）；中央高校基本科研业务费专项资金（2025KYQD17（BUPT））

荷的方法已经暴露出明显的局限性，难以满足实际需求。随着研究的不断深入，机器学习（Machine Learning）方法被引入到流量分类领域。但目前的机器学习方法大多依赖于人工设计的流量特征，这在很大程度上限制了其泛化能力，使其难以应对复杂多变的网络环境。而深度学习（Deep Learning）方法虽具备自动从原始数据中提取有效特征的优势，但对大量标记数据存在高度依赖性，而在网络安全领域，获取大规模、高质量的标记流量数据成本高昂。同时，当训练数据规模不足、代表性不强或存在偏差时，深度模型因其高复杂度和海量参数，极易学习到数据中的噪声而非普适规律，从而导致过拟合问题，降低了模型在真实网络环境中的泛化能力。

鉴于上述问题，本文提出了一种基于教师－学生双模型的半监督流形混合流量分类方法（Manifold Mixup Mean Teacher，M3T）。教师－学生架构（Mean Teacher，MT）是一种利用双模型架构的先进方法。在该架构中，学生模型借助梯度下降方法，利用标记数据与无标记数据进行更新迭代；而教师模型则采用移动指数平均（Exponential Moving Average，EMA）方式更新参数，凭借其更为稳定的输出，对学生的模型学习过程进行有效监督，进而显著提升模型的泛化性能。在此基础上，本研究进一步引入由教师模型引导的流形特征混合机制，于教师模型的深层特征空间中运用流形混合（Manifold Mixup）方法，构建起“教师特征扰动－学生动态对齐”的双向优化框架，以此增强模型对特征扰动的鲁棒性，同时优化决策边界，使其更适应复杂的流量分类场景。

综上所述，本文的主要贡献为：

（1）提出教师模型引导的流形特征混合机制，将流形混合迁移至教师模型的深层特征空间，构建“教师特征扰动－学生动态对齐”双向优化框架。利用教师 EMA 参数提供的稳定特征表达，避免学生模型早期特征的不确定性干扰。

（2）通过三项损失的协同，在模型框架中实现基础分类、一致性对齐与决策边界平滑的联合优化。交叉熵损失保证基础分类能力；一致性损失强制学生输出与教师输出对齐，实现一致性正则化，缓解模型过拟合问题；混合损失增强模型对特征扰动的鲁棒性，优化决策边界平滑。

（3）提出一种基于教师－学生架构的半监督流形混合网络流量分类模型框架，在多个流量数据集上评估预训练模型，结果显示能够普遍取得 90% 以上的准确率。

1 相关工作

1.1 流量分类

现有的网络流量分类技术包括基于端口识别和基于深度数据包检测的技术、依靠统计特征的机器学习技术以及深度学习算法[1]。

早期的网络流量分类方法根据数据包的端口号将流量数据按不同的服务协议分类，可以实现对简单流量的快速分类，但不适用于复杂的网络环境[2]。为了解决早期方法存在的问题，研究人员根据流量的有效载荷数据和统计特征识别复杂流量中的特定应用场景，如 Fernandes 等[3]提出了 LW-DPI 框架，通过检查有限数量的数据包的内容或给定数据包的一小部分负载来对网络流量进行分类；Hubballi 等[4]利用网络流中提取的 n 位二进制字符串长度来对网络流量进行分类。然而这种方法无法分析经过加密的流量数据，能够利用的信息有限。

机器学习方法脱离了对数据包端口号或内容的依赖，根据统计特征来实现加密流量分类。例如，AppScanner[5]使用基于数据包大小的统计特征训练随机森林分类器；Dias 等[6]使用数据包到达时间、十进制值的平均值和 IP 数据报长度的平均值等特征训练机器学习模型，对实时应用程序流量进行分类。机器学习方法可以有效分析具有复杂特征的加密流量，但依赖于专家设计的统计特征，缺乏泛化能力，且需要消耗较多计算资源。

深度学习方法近年来已成为一种主流的流量分类方法，它可以通过训练神经网络从原始数据包中自动提取特征，摆脱了对于手动设计特征的依赖。Lin 等[7]提出了 TSCRNN，结合卷积神经网络（Convolutional Neural Networks，CNN）与循环神经网络（Recurrent Neural Network，RNN），通过从网络流数据中提取时间与空间特征来实现流量分类。Lotfollahi 等[8]提出了一种深度数据包框架，结合了 CNN 和堆叠自编码器（Stacked Autoencoder，SAE）以实现应用程序识别。深度学习方法的缺点在于需要大量监督数据来捕获有效特征，且容易在不平衡的数据中学习到有偏差的表示。

1.2 流量表示

在实际场景中，网络流量包含广泛的数据类别，这些数据类别因上层应用程序、承载协议或传输目的而异。为了保证分类检测的准确性，选择适当粒度的流量表示方案对于准确理解流量至关重要。传统的机器学习方法受模型参数和拟合能力的限制，

通常采用在数据包或流级别使用压缩的统计特征，例如数据包大小的分布或到达间隔时间。但是，这些特征容易受到过度压缩的影响，导致原始数据中固有的重要信息丢失。深度学习尝试利用原始流量提取特征，然而，神经网络经常忽略数据包中的关键信息，并通过学习次要的数据特征而引入不必要的偏差。为了解决这些问题，需要选择一种有效的网络流量表示方案，在有效消除偏差的同时保留原始流量信息。

1.3 混合

混合（Mixup）是一种数据增强方法，通过将两个样本的数据和标签按一定比例插值来生成一个新的样本。这种方法易于实现且具有良好效果，无需原始数据领域的背景知识即可生成大量的训练数据，被广泛应用于自然语言处理、图像、语音处理等多个领域。Zhang 等[9]提出了 TreeMix，通过组成句法分析将句子分解为子结构，并通过混合将它们重新组合成新句子。Verma 等[10]提出 GraphMix，实现与图神经网络（Graph Neural Network，GNN）联合训练全连接网络。Zhang 等[11]提出 Contrastive-mixup，将混合技术应用于语音数据。而在网络流量分类领域，Hou 等[12]提出了一种自训练混合决策树方法，通过使用混合技术在标记数据稀缺条件下有效提升网络攻击流量的分类性能。尽管如此，混合技术在网络流量分类，特别是基于加密流量图像化表示的应用方面，相关研究仍相对较少，未得到充分的探讨。因此，本研究将流形混合策略引入半监督流量分类框架中，探索其在该领域的应用潜力，凸显了本研究对相关领域的补充贡献。

2 M3T 模型

本节介绍 M3T 模型的主要内容，图 1 展示了方法的模型框架。如图 1 所示，M3T 模型以教师 - 学生模型作为主要结构，接收经过预处理的网络流量数据。作为一种半监督学习方法，模型接受标注数据与无标注数据，图中 x 代表输入模型的数据，y 代表其中标记数据所对应的标签。标注数据输入到学生模型中，结合标签 y 计算出交叉熵损失 L_{ce}，训练学生模型。无标注数据输入到学生模型与教师模型当中，通过指数移动平均与均方误差计算一致性损失 L_{con} 进行模型协作训练，并生成伪标签 y_p 用于流形混合。流形混合机制应用于教师模型的隐藏层中，通过计算混合损失 L_{mixup} 提升模型性能。三种损失结合构成模型的总损失函数，用于反向传播，更新模型参数。

2.1 数据预处理

原始的网络流量数据需要经过一定的预处理流程后再输入到模型之中，其处理流程如图 2 所示。数据的预处理步骤为：

（1）流量切分：在原始的 PCAP 格式流量文件中，流量数据可按照流或会话的粒度进行切分。流定义为具有相同五元组（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议）的数据包集合，会话定义为源 IP 地址、源端口与目的 IP 地址、目的端口可互换的双向流组成的数据包集合。通过流量切分，将包含多个流/会话的原始大 PCAP 文件切分为多个只包含单个流/会话的小 PCAP 文件。需要强调的是，此步骤使用五元组仅作为聚合数据包的流标识符，而非依赖端口号等信息进行分类。本文的分类依据是聚合后流的整体数据特征。

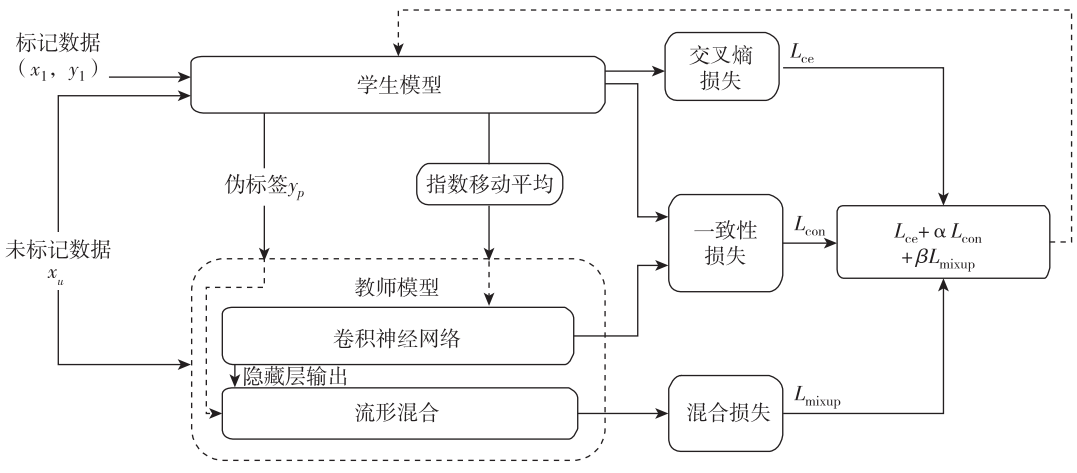

图 1 模型总体框架

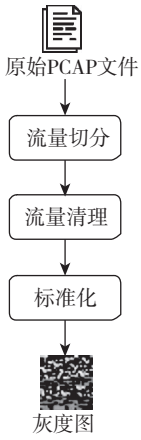

图 2　数据预处理流程

（2）流量清理：清理重复文件与应用层信息为空的流/会话。在神经网络训练过程中，重复数据包含相同信息，可能导致训练偏差。

（3）标准化：将所有文件的长度修改为 784 个字节。对于长度超过 784 字节的文件，将超出部分删除，仅保留前 784 字节；对于长度少于 784 字节的文件，在文件末尾补充空字符至指定长度。该长度可对应转换为 28 ×28 的图像，是利用图像作为流量表示的常用基准设置，在文献［8］、［12］等工作中被采用并验证了其有效性。该长度通常能覆盖 TCP/IP 头部及初始数据包的有效载荷，足以捕获区分不同应用类别的关键特征。

标准化处理后，将固定长度为 784 字节的文件以 28 ×28 的灰度图形式输出，每个字节以一个像素表示，保存为 PNG 格式，作为模型的输入数据。

2.2　教师 - 学生架构

教师 - 学生架构是一种半监督学习框架，包含两个相同的神经网络模型，分别称为学生模型与教师模型。将相同的数据添加随机高斯噪声，分别输入学生模型与教师模型。学生模型首先利用标记数据进行监督学习，通过神经网络提取数据特征，并对未标记数据进行分类。教师模型通过 EMA 进行参数更新，计算公式为：

$$\theta_t^T = \gamma\theta_{t-1}^T + (1-\gamma)\ \theta_t^S \tag{1}$$

其中 θ_t^T 表示教师模型在第 t 个训练步骤中的权重参数；θ_t^S 表示学生模型在第 t 个训练步骤中的权重参数，通过模型计算损失反向传播更新；γ 表示平滑系数。在第 1 个训练步骤中，令平滑系数 $\gamma=0$，使 $\theta_1^T=\theta_1^S$，作为教师模型的初始参数。在参数更新过程中，教师模型相比学生模型具有更稳定的参数，这是因为教师模型并非像学生模型那样直接通过梯度下降进行大幅度更新，而是通过 EMA 将其当前参数与学生模型的新参数进行融合。这种更新机制使得教师模型的参数变化更为平缓，有助于减少噪声等因素引起的波动，从而更有效地整合学生模型在训练过程中的知识积累。

教师 - 学生架构的核心在于鼓励学生模型与教师模型的输出保持一致，学生模型在学习过程中需要尽量与教师模型的预测结果相匹配，这种一致性正则化有助于提升模型的泛化能力和鲁棒性。方法通过在损失函数中引入一致性损失来约束两个模型的输出，进而实现一致性正则化。训练过程中，学生模型与教师模型分别输入经随机高斯噪声扰动的流量数据 x，包含标记数据 x_l 与未标记数据 x_u，即：

$$x = x_l + x_u \tag{2}$$

学生模型在第 t 个训练步骤输出预测值 $f_S(x,\ \theta_t^S)$，其中标记数据 x_l 的预测值为 $f_S(x_l,\ \theta_t^S)$，结合标记数据标签 y 计算监督学习的交叉熵（Cross Entropy，CE）损失：

$$L_{ce} = \mathrm{CE}(f_S(x_l,\ \theta_t^S),\ y) \tag{3}$$

教师模型在第 t 个训练步骤输出预测值 $f_T(x,\ \theta_t^T)$，结合学生模型输出 $f_S(x,\ \theta_t^S)$，通过均方误差（Mean Square Error，MSE）计算一致性损失：

$$L_{\mathrm{con}} = \mathrm{MSE}(f_T(x,\ \theta_t^T),\ f_S(x,\ \theta_t^S)) \tag{4}$$

方法中学生模型与教师模型采用相同的网络结构。网络结构基于卷积神经网络，以单通道 28 ×28 的图像作为输入，随后依次经过三组卷积层，每个卷积块由卷积、批归一化和 LeakyReLU 激活函数组成。第一组卷积层输出通道为 128，第二组为 256，第三组为 128。每组卷积层后均接有最大池化操作以实现特征下采样，最后通过自适应平均池化将特征图降为 1 ×1。展平后，将特征输入到全连接层，按数据类别数输出预测结果。

在方法中选择结构较为简单的神经网络，主要基于以下几点考虑：首先，简单的网络结构参数较少，计算效率高，能够显著降低训练和推理过程中的计算资源消耗，适合在资源有限硬件条件下运行；其次，结构简单的模型更易于分析和调试，有助于排除复杂结构带来的干扰因素，从而更专注于半监督学习方法本身的效果评估；此外，简单网络在小样本或标签稀缺的场景下更不易过拟合，能够更好地反映算法的泛化能力；最后，采用 CNN 作为基线模型，有助于与其他方法进行公平对比，突出半监督学习策略带来的性能提升。

2.3 流形混合

混合机制可以有效提高模型的泛化能力和鲁棒性，而流形混合是在混合的基础上实现的拓展，该方法将数据的混合操作从输入层转移到模型的隐藏层，促使模型在特征空间中学习更加一致和鲁棒的特征表示。这种混合方式使得模型的隐藏层特征必须同时考虑不同数据点的特征组合，从而增强了模型对数据流形结构的理解。

通过在隐藏层中进行混合，流形混合能够帮助模型减少对输入特征的过度依赖，进一步提高模型的鲁棒性。此外，这种混合方式还能使模型的决策边界在特征空间中更加平滑，降低过拟合的风险，提升模型在面对未知数据时的泛化能力。

本文提出方法中，由于教师模型具有更稳定和鲁棒的特征表示，在其隐藏层进行流形混合时，可以充分利用教师模型的优势，使得生成的混合特征更加可靠和具有指导意义。实际应用过程中，提取教师模型卷积层2的输出，针对每一条数据 x_h，在输出内随机选取另一条数据 x_r 与其混合，生成混合数据：

$$\text{mixed\_}x_h = \lambda \times x_h + (1-\lambda) \times x_r \tag{5}$$

其中，λ 服从参数为0.2的Beta分布，即：$\lambda \sim \text{Beta}(0.2, 0.2)$。混合数据 $\text{mixed\_}x_h$ 输入到教师模型后续层，输出混合数据预测结果 f_{mixup}。

方法在损失函数中引入混合损失来约束模型对于混合数据的预测与混合标签的一致性。由于输入到教师模型中的数据 x 包含标记数据与未标记数据，对于未标记数据需要提供伪标签用于流形混合损失值的计算，方法取学生模型对未标记数据 x_u 的预测值 $f_S(x_u, \theta_t^S)$ 作为伪标签，即 $y_p = f_S(x_u, \theta_t^S)$。计算混合损失公式为：

$$L_{\text{mixup}} = \lambda \times \text{CE}(f_{\text{mixup}}, y_h) + (1-\lambda) \times \text{CE}(f_{\text{mixup}}, y_r) \tag{6}$$

其中，CE（·）表示交叉熵函数；y_h 为数据 x_h 的标签；y_r 为数据 x_r 的标签；$y_h, y_r \in y + y_p$。

综合交叉熵损失、一致性损失、混合损失，模型的总损失函数为：

$$L = L_{\text{ce}} + \alpha L_{\text{con}} + \beta L_{\text{mixup}} \tag{7}$$

其中，α，β 分别代表一致性损失与混合损失的权重系数，用于平衡不同损失之间的相对重要性。计算出总损失函数后，模型通过反向传播实现参数更新，优化分类性能。

3 实验设计与分析

3.1 实验环境

实验中使用的方法模型通过 PyTorch 0.4.1 部署，在 Ubuntu 20.4 服务器上实现，服务器的中央处理器为 Intel（R）Xeon（R）Silver 4216 CPU @ 2.10 GHz，图形处理器为 NVIDIA GeForce RTX 2080 Ti。

3.2 数据集

实验中使用了五种公开的网络流数据集，分别是USTC-TFC2016、CIC-DoS2017、CICIoT2023、CIC-DDoS2019和TII-SSRC-23。

USTC-TFC2016数据集由中国科学技术大学的研究者分享[13]，包含10种正常流量与10种异常流量数据；CIC-DoS2017[14]、CICIoT2023[15]、CIC-DDoS2019[16]都是由加拿大网络安全研究所提供的公开数据集，包含多种良性网络流量与攻击流量；TII-SSRC-23也是一种包含多种良性及攻击流量的公开网络流数据集[17]。

对数据集的处理如上一节所述，将原始的PCAP格式文件经切分、清理、标准化处理后转换为图像文件，作为模型的输入。

3.3 评估指标

为评估模型在实验中的表现，使用准确率（Accuracy，Acc）、召回率（Recall，Rec）、精确率（Precision，Pre）、F1分数（F1 Score，F1）作为评估指标，计算公式分别如下：

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{8}$$

$$\text{Rec} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{9}$$

$$\text{Pre} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{10}$$

$$\text{F1} = 2 \times \frac{\text{Pre} \times \text{Rec}}{\text{Pre} + \text{Rec}} \tag{11}$$

以上公式中，TP代表被模型分类为正常的正常样本数量，TN代表被模型分类为异常的异常样本数量，FP代表被模型分类为正常的异常样本数量，FN代表被模型分类为异常的正常样本数量。

3.4 对比实验

为验证所提出方法的性能，实验选取ERNN[18]、DeepPacket、TSCRNN、LSTM-Att[19]、YaTC[20]五种代表性基线模型，在三种数据集上与所提出方法进行对比。基线模型涵盖了经典方法与近年先进方法，如DeepPacket是将流量表示为图像并使用CNN分类的开创性工作之一，YaTC是近年来在该领域取得高性能的先进模型。通过与这些方法的比较，可以全面评估M3T在不同技术路线对比下的性能水平。

实验选用了CIC-DDoS2019、CICIoT2023、USTC-TFC2016三种数据集，主要原因是这三个数据集规模

较大、代表性强，且部分基线模型在这些数据集上有公开结果或易于复现，便于进行性能对比。对于三种数据集，设置训练集中每种类别的数据量为1 000，测试集中每种类别的数据量为250，标记数据占所有数据的30%。

实验结果如表1所示，所提出方法在CIC-DDoS2019数据集上达到0.928 3的准确率，在USTC-TFC2016数据集上达到0.993 3的准确率，表现优于其他基线模型；在CICIoT2023数据集上达到0.936 7的准确率，表现优于ERNN、DeepPacket、TSCRNN、LSTM-Att四种模型，与YaTC持平。对比结果表明所提出方法具有良好的网络流量分类检测性能。

表1　不同方法在CIC-DDoS2019、CICIoT2023、USTC-TFC2016数据集上的对比结果

	CIC-DDoS2019				CICIoT2023				USTC-TFC2016			
	Acc	Rec	Pre	F1	Acc	Rec	Pre	F1	Acc	Rec	Pre	F1
ERNN	0.678 7	0.751 1	0.678 7	0.675 2	0.719 1	0.719 1	0.734 0	0.712 0	0.836 7	0.836 7	0.839 7	0.817 1
DeepPacket	0.865 5	0.865 5	0.886 9	0.870 6	0.714 0	0.724 4	0.713 5	0.712 2	0.976 2	0.976 8	0.976 8	0.976 5
TSCRNN	0.891 6	0.891 6	0.900 3	0.892 8	0.753 0	0.766 5	0.752 8	0.756 8	0.979 5	0.980 4	0.980 0	0.980 0
LSTM-Att	0.917 8	0.917 8	0.927 5	0.920 1	0.716 0	0.724 7	0.713 6	0.714 5	0.977 5	0.978 2	0.977 8	0.977 8
YaTC	0.876 9	0.876 9	0.883 2	0.839 7	0.933 6	0.933 6	0.936 0	0.932 1	0.960 3	0.960 3	0.963 9	0.960 0
M3T	0.928 3	0.910 8	0.912 7	0.911 5	0.936 7	0.936 7	0.937 8	0.936 5	0.993 3	0.993 3	0.993 0	0.993 3

3.5　消融实验

所提出方法分别利用双模型架构与流形混合机制来获得良好的分类检测性能。为了进一步验证两种机制的贡献，在五种数据集上进行了消融实验，旨在更全面地验证本文所提组件的普适性和有效性。实验对比了CNN模型、MT模型、混合MT模型与所提出的M3T模型的表现，结果如图3所示。其中MT、混合MT、M3T的神经网络架构与CNN一致，混合MT在MT的基础上在教师模型输入层加入混合机制，M3T在MT的基础上加入了流形混合机制。

实验结果显示，MT在不同数据集上的表现均强于CNN，证明了其架构的有效性。混合MT在多数数据集上的表现弱于MT，分析认为这是由于网络流量的图像化表示具有结构化的特性，将其直接插值混合会产生无意义的“伪流量”样本，这种噪声反而干扰了模型的学习。然而，本文提出的M3T取得了最佳性能，显著优于MT和混合MT。结果表明，在模型的深层特征空间中进行混合是有效的。因为在特征空间中，模型已经提取了有意义的抽象模式，对其进行插值等价于在语义上平滑决策边界，从而能学习到更加鲁棒的特征表示。这一对比表明了教师－学生架构与流形混合机制对分类效果提升的贡献，并且流形混合机制在教师－学生架构的基础上实现性能提升，体现了两种机制相辅相成的效果。

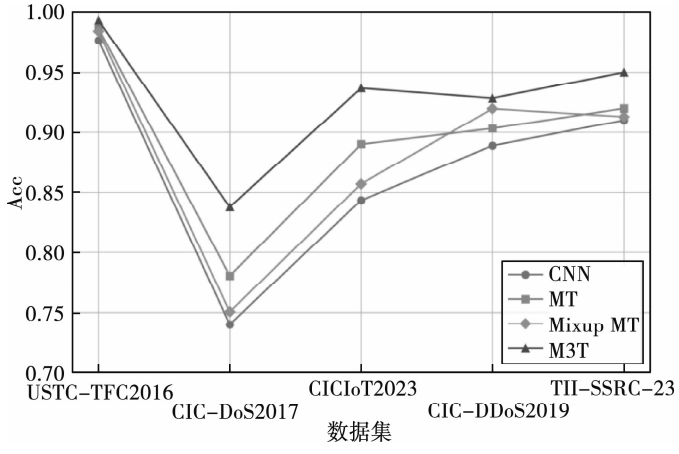

图3　五种数据集下的消融实验结果

3.6　少样本（Few-shot）实验

教师－学生架构是一种半监督学习架构，可利用少量标记样本提升模型学习性能。而流形混合机制包含数据增强的效果，可以在少样本条件下生成额外的训练样本，保持模型的训练效果。为了验证所提出方法在少样本条件下的性能，实验选取CIC-DDoS2019作为代表性数据集，设计了不同数据比例的比较实验。将数据集中每个类别的数据量设置为500，并分别随机选择其中70%、40%、10%的样本进行实验。如图4所示，比较结果表明，ERNN、DeepPacket、TSCRNN、LSTM-Att四种模型受样本数量影响明显，其F1分数都出现了明显的下降；YaTC作为一种预训练方法受数据量减少的影响较小；而本文提出的方法在不同数据量下的F1分数保持稳定，且分数高于其他基线模型，取得了最好的结果。实验结果表明，所提出的方法在少样本条件下仍具有良好的分类检测性能。

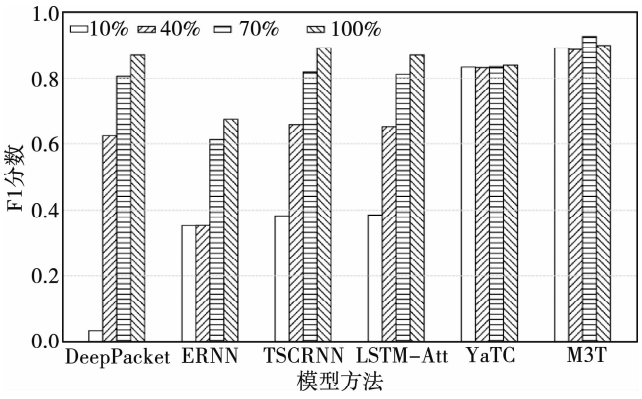

图 4　CIC-DDoS2019 数据集上的少样本实验结果

3.7　可视化对比实验

为验证流形混合机制对模型决策边界的作用，实验使用 t-SNE 降维技术，选取数据类别适中的 CICIoT2023 数据集，将 MT 与 M3T 在数据集上的输出结果进行了可视化，如图 5 所示。图中黑框部分分别标记了数据集中名称为 DDoS_SlowLoris 与 Mirai_greip_flood，Recon_PortScan 与 MITM_ArpSpoofing 的数据之间的二维边界。通过对比可见，M3T 中不同类别数据之间的边界相比于 MT 更加明确。实验表明，混合流形机制对于提高模型鲁棒性、改善模型决策边界具有明显作用。

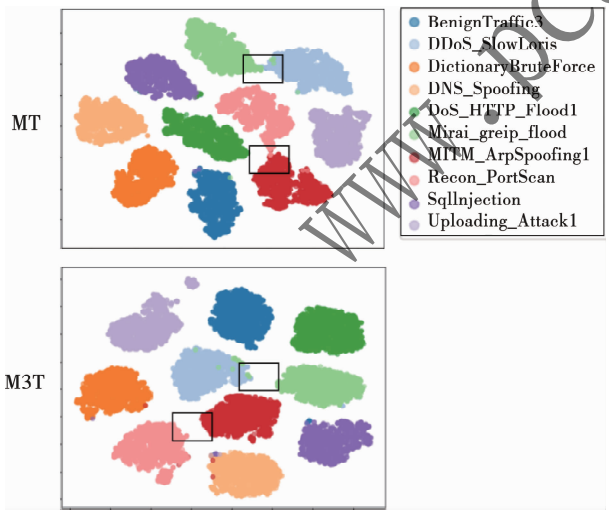

图 5　CICIoT2023 数据集下的分类结果输出可视化对比

4　结论

现有的深度学习技术在流量分类任务中存在对大量数据的依赖性以及过拟合的问题，为此，本文提出了一种结合教师－学生架构与流形混合的半监督方法，并设计多种实验验证其效果。

实验结果显示，本文所提出的模型结构可以有效提升深度学习模型的预测精度，在少量样本条件下能够保持较高精度，并对模型的分类决策边界具有明显的平滑作用。未来，可以通过更改神经网络结构等方法进一步对模型进行改进。

参考文献

[1] AZAB A, KHASAWNEH M, ALRABAEE S, et al. Network traffic classification: techniques, datasets, and challenges [J]. Digital Communications and Networks, 2024, 10 (3): 676－692.

[2] MADHUKAR A, WILLIAMSON C. A longitudinal study of P2P traffic classification [C]//14th IEEE International Symposium on Modeling, Analysis, and Simulation. IEEE, 2006: 179－188.

[3] FERNANDES S, ANTONELLO R, LACERDA T, et al. Slimming down deep packet inspection systems [C]//IEEE INFOCOM Workshops 2009. IEEE, 2009: 61－66.

[4] HUBBALLI N, SWARNKAR M, CONTI M. BitProb: probabilistic bit signatures for accurate application identification [J]. IEEE Transactions on Network and Service management, 2020, 17 (3): 1730－1741.

[5] TAYLOR V F, SPOLAOR R, CONTI M, et al. AppScanner: automatic fingerprinting of smartphone apps from encrypted network traffic [C]//2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016: 439－454.

[6] DIAS K L, PONGELUPE M A, CAMINHAS W M, et al. An innovative approach for real-time network traffic classification [J]. Computer Networks, 2019, 158: 143－157.

[7] LIN K, XU X, GAO H. TSCRNN: a novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT [J]. Computer Networks, 2021, 190: 107974.

[8] 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.

[9] ZHANG L, YANG Z, YANG D. TreeMix: compositional constituency-based data augmentation for natural language understanding [J]. arXiv preprint arXiv: 2205.06153, 2022.

[10] VERMA V, QU M, KAWAGUCHI K, et al. GraphMix: improved training of GNNs for semi-supervised learning [C]// Proceedings of the 35th AAAI Conference on Artificial Intelligence, 2021, 35 (11): 10024－10032.

[11] ZHANG X, JIN M, CHENG R, et al. Contrastive-mixup learning for improved speaker verification [C]//ICASSP 2022－2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022: 7652－7656.

[12] HOU Y, TEO S G, CHEN Z, et al. Handling labeled data insufficiency: semi-supervised learning with self-training mixup

decision tree for classification of network attacking traffic [J]. IEEE Transactions on Dependable and Secure Computing, 2022.

[13] WANG W, ZHU M, ZENG X, et al. Malware traffic classification using convolutional neural network for representation learning [C]//2017 International Conference on Information Networking (ICOIN). IEEE, 2017: 712 -717.

[14] JAZI H H, GONZALEZ H, STAKHANOVA N, et al. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling [J]. Computer Networks, 2017, 121: 25 -36.

[15] NETO E C P, DADKHAH S, FERREIRA R, et al. CICIoT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment [J]. Sensors, 2023, 23 (13). DOI: 10. 3290/s23135941.

[16] SHARAFALDIN I, LASHKARI A H, HAKAK S, et al. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy [C]//2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019: 1 -8.

[17] HERZALLA D, LUNARDI W T, ANDREONI M. TII-SSRC-23 dataset: typological exploration of diverse traffic patterns for intrusion detection [J]. IEEE Access, 2023, 11: 118577 -118594.

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

[19] YAO H, LIU C, ZHANG P, et al. Identification of encrypted traffic through attention mechanism based long short term memory [J]. IEEE Transactions on Big Data, 2019, 8 (1): 241 -252.

[20] ZHAO R, ZHAN M, DENG X, et al. Yet another traffic classifier: a masked autoencoder based traffic transformer with multi-level flow representation [C]//Proceedings of the 37th AAAI Conference on Artificial Intelligence, 2023, 37 (4): 5420 -5427.

（收稿日期：2025 -10 -20）

作者简介：

马可（2001 -），男，硕士研究生，主要研究方向：网络安全、深度学习。

何明枢（1995 -），通信作者，男，博士，副教授，主要研究方向：网络威胁分析。E-mail：hemingshu@ bupt. edu. cn。

蔡晶晶（1981 -），男，教授级高级工程师，主要研究方向：网络安全。

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，即视作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，本刊支付的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