深度学习网络流量分类方法研究

吴伟毅 冯沛林 邓正伟 王宇博

联通数字科技有限公司，北京市，100000；

摘要：随着加密通信协议的广泛应用与网络行为日益复杂，传统流量分类方法在准确性与泛化能力上面临严峻挑战。深度学习凭借其强大的特征表征能力与模型自适应性，在网络流量分类领域展现出明显优势。本文系统梳理了主流深度学习模型（卷积神经网络、循环神经网络与 Transformer）在不同数据结构与场景下的应用表现，结合常用数据集与预处理策略，分析其适用边界与性能差异。进一步探讨小样本稀缺、模型可解释性弱、实时性差等关键挑战，并提出融合式模型发展趋势。构建兼顾精度、效率与鲁棒性的深度流量分类体系，是当前研究与工程落地的核心议题。

关键词：深度学习；网络流量分类；卷积神经网络；Transformer

DOI：10.69979/3041-0673.26.02.034

引言

网络流量分类是确保网络有效管理和增强网络安全防御的关键。近年来，随着动态端口和加密技术的普及，传统的网络流量分类方法的应用范围受到了局限。随着深度学习在时间序列预测和图像处理等领域的成功，如卷积神经网络、循环神经网络等深度学习网络被广泛应用于网络流量分类领域。相较于传统方法，深度学习方法能够从大规模数据集中自动学习特征，降低对人工干预的需求，显著提升网络流量识别和分类的效率及准确率，更加适应当前复杂的网络环境[1]。

1 网络流量分类的技术演进与深度学习引入背景

1.1 网络流量分类方法的历史回顾

网络流量分类的轨迹呈现“从规则到学习、从报文到会话”的脉络。早期依赖端口号与协议栈固定字段，工程实现简洁，但面对动态端口与应用复用即刻失灵。随后转向深度包检测，直接检索负载特征串，精细到字节级，却对加密与变形极为脆弱。统计学习阶段兴起后，研究者围绕流层特征构建样本，常用包长分布、到达间隔、方向序列、连接持续时长等指标，配合支持向量机与随机森林取得稳定收益，代价是繁重的人工特征工程与场景迁移成本。回望三十余年的积累，可以看到方法重心逐步脱离协议语义本身，转而抓取“行为外显信号”。这一转变提示后续路线：在加密占优与业务多样的现实语境下，表征学习能力强、泛化边界宽的模型更具生命力[2]。

1.2 加密与变异流量对传统方法的冲击

加密流量成为常态，负载层几乎不可见，使深度包检测与基于明文字段的匹配陷入“信息贫瘠”。传输层安全协议与基于用户数据报协议的快速连接协议进一步压缩可观测空间，握手可见字段减少，复用与拥塞控制改变时序纹理；同一域名承载多应用，标签随时漂移，统计特征出现交叠。应用侧还常引入流量填充、包长扰动、节奏伪装等策略，导致传统特征在高噪声环境下判别力下滑。工程经验表明，依赖少量刚性字段的方案最先退化；依赖手工特征的方案面临跨网络迁移不稳；依赖单一时间尺度的方案难以刻画长短程依赖[3]。冲击的本质在于“可见性预算”被压缩，而分类任务又要求稳定而细腻的表征，这直接催生对更强表征学习范式的需求。

1.3 深度学习引入网络流量分类的合理性

深度学习契合流量数据的层次与时序结构：卷积神经网络可在包长与方向序列的局部邻域提取稳健纹理，循环神经网络及长短时记忆网络擅长建模突发与周期交织的时序关系，转换器模型借助自注意力在长程依赖与多尺度模式间自适应分配权重。表征学习免于繁琐人工特征工程，能在加密语境下从元数据与序列形态中提炼“行为签名”，并通过迁移学习与对比学习提升跨场景稳定性。与传统范式相比，深度模型为“从协议语义识别”转向“从行为表征识别”提供技术抓手，同时保留与领域知识融合的空间，如以协议先验约束注意力分布、以流会话结构指导采样。由此形成一条清晰路径：以端到端表征为核心，以可解释与可部署为约束，构建适配现代网络生态的分类体系[4]。

2 主流深度学习模型在网络流量分类中的应用分析

2.1 数据集与预处理策略

深度学习模型在网络流量分类任务中的表现高度依赖数据的结构与预处理策略，而“会话粒度、特征空间与切片长度”三者之间的平衡，构成了训练有效模型的基础约束。当前工程实践中常见三种处理路径：其一，使用 CICFlowMeter 工具将原始 pcap 文件转化为双向流，并提取包括包长、速率、方向等在内的 80 余项统计特征，适用于浅层神经网络或传统树模型；其二，构建以包长、方向与到达间隔为核心的时序序列，供一维卷积或循环网络挖掘微观节奏；其三，进行字节级编码，将握手字段或原始负载映射为 token 序列，引入预训练机制与注意力机制展开建模，尤适用于加密通信环境[5]。采样和切片的策略对模型评估的可信度构成实质影响。为避免样本间信息泄漏，需保证同一五元组不跨训练集与测试集；面对如 BoT-IoT 这类类别极度不均的样本分布，应采用重采样或代价敏感型损失函数提升泛化能力。实验分割应涵盖跨场景与跨时间域，以测试模型能否真正捕捉流量行为本质，而非依赖数据集的静态偏差。多个公开数据集如 CSE-CIC-IDS2018、VPN-nonVPN2016 及 USTC-TFC2016 已形成事实标准，为模型比较与方法迭代提供了坚实支撑（见表 1）。

表 1 近年来典型数据集与模型应用要点对照

数据集 / 场景	时间与规模要点	任务与标签	常见预处理方法	代表模型范式
CSE-CIC-IDS2018	2018 年采集，包含 50 台攻击机与 420 台受害终端，共提取 80+流特征	涉及暴力破解、DoS/DDoS、Web 入侵等 7 类攻击场景	pcap → 双向流（CICFlowMeter）；标准化处理；确保无信息泄漏	1D-CNN/TCN 提取局部模式，LSTM 汇聚时序；Transformer 处理长依赖
VPN-nonVPN2016（ISCX）	涵盖 14 类应用，会话包含 VPN 与非 VPN 流量	面向加密应用协议分类	会话切片处理；构建包长、方向、间隔序列；字节级编码可选	1D-CNN，CNN-LSTM 混合模型；支持字节级 Transformer
BoT-IoT	构建于真实物联网环境中，样本分布极度不均	聚焦于二分类与多类僵尸网络/入侵检测任务	提取统计特征；使用重采样与代价敏感策略；测试阶段保持原始分布	轻量 CNN 适用于边缘设备；中心侧采用 Transformer 增强鲁棒性
USTC-TFC2016	覆盖 20 类正常与恶意流量，适合多任务学习	应用识别与恶意软件家族分类	采用 USTC-TK 工具链进行预处理；提取序列结构或字节特征	图像化 CNN 与序列 LSTM 混合建模；尝试字节级注意力机制

2.2 卷积神经网络（CNN）

卷积神经网络（Convolutional Neural Network, CNN）在处理网络流量中的局部结构方面展现出显著优势。具体而言，两种编码方式较为常见：一是将流量数据转化为“流量图像”，如包长与方向叠加成二维矩阵，用二维卷积提取模式纹理；二是保留时间序列结构，以一维卷积识别短程依赖，如突发、重传与保活节奏。前者有利于可解释性建模，后者则契合流量本身的微观平稳性。在实际部署中，CNN 常与注意力机制或自动调参框架（如 Optuna）协同工作，以适应不同业务流的节奏与协议差异。在加密流量分类任务中，通道注意力机制的引入能够显著提升模型对关键信号片段的聚焦能力，减少长尾类别被掩盖的风险。此外，CNN 在边缘部署中的效率优势尤为明显，卷积核共享机制天然适配低延迟与高吞吐场景，配合网络剪枝与知识蒸馏技术可构建轻量级模型。工程经验表明，浅层 1D-CNN 在区分 TLS/QUIC 中的内容分发与交互式应用中表现稳定。近期的中文研究中，多尺度时间卷积的引入增强了对多频段干扰的抵御力，也进一步拓展了卷积模型的表达边界。

2.3 循环神经网络（RNN）与长短时记忆网络（LSTM）

循环神经网络（Recurrent Neural Network, RNN）及其扩展结构长短时记忆网络（Long Short-Term Memory, LSTM）在处理具有时间依赖的网络流量序列方面表现出独特的优势。网络中的交互通常包含“请求—响应—空闲—重试”等典型节奏，RNN 系列模型能够有效捕捉这些微观动态变化，适用于模型识别复杂的往返行为和通信模式切换。在面向长时会话或弱标签样本的任务中，采用“会话分片 + 隐状态贯通”策略，有助于在控制计算复杂度的前提下保持上下文连续性。然而，该类模型易受分布偏移影响，尤其在归一化处理以全样本为参考时，验证集与测试集之间的统计漂移会被掩盖，带来评估偏差。此外，RNN 系统在处理冗长片段时存在过拟合风险，需结合 dropout、标签平滑及窗口对齐等正则手段进行结构约束。从应用角度看，RNN/LSTM 更常作为组合模型中的后处理单元，与前段 CNN 模块配合完成纹理提取与时序整合。实验数据如 VPN-nonVPN2016 与 USTC-TFC2016 均表明，具备时间记忆能力的模型在多协议混合与跨场景迁移中展现出更好的稳健性。中文实践经验也表明，流量序列建模中的数据泄漏排查不可忽视，应作为与模型优化同等优先的核心环节。

2.4 Transformer 模型初探

Transformer 模型因其自注意力机制（Self-Attention）

在捕捉长程依赖方面的优势，逐渐成为网络流量分类领域的新兴技术路径。相较于传统序列模型，其在处理跨包关联与上下文信息建模方面表现出更高灵活性，特别适用于 TLS/QUIC 加密通信场景中原始字节的 token 级建模。近年来，多项中文研究提出以“字节编码 + 预训练任务”为核心的方案，即在不依赖明文特征的条件下，通过模型自主学习协议内部的行为语法，实现跨场景、跨协议的泛化能力提升。同时，层次化注意力机制的引入（如包级注意力与流级注意力的叠加）有效缓解了会话内的信息冗余问题，使模型更专注于高价值片段。然而，Transformer 的实际应用门槛不容忽视，其对计算资源和训练数据量提出更高要求，通常不宜直接部署于资源受限的边缘设备。工程上更推荐将其纳入分层体系中：边缘侧利用 CNN 快速筛查，中心侧再由 Transformer 模块进行精细分类；若对实时性要求严格，可借助模型蒸馏技术将其能力转化为浅层模型部署。整体而言，Transformer 的引入代表了从“局部特征建模”向“跨包语义建模”的跃迁，为构建更具鲁棒性的网络流量识别体系提供了新的思路。

3 深度学习流量分类中的关键挑战与优化方向探析

3.1 小样本与不平衡类别问题

网络流量数据天然存在严重类别不均与标签稀疏现象，特别是在工业协议与攻击样本中表现尤为突出。大多数主流模型在面对主类别优势占据训练分布时，往往陷入过拟合主模态而忽略边缘流量的困境。这一结构性偏差导致识别率偏向常规流量，削弱系统的泛化能力。当前研究尝试引入迁移学习、小样本生成与代价敏感训练策略应对此难题，但仍难在保持精度的同时避免误报攀升。因此如何构建具备少样本感知与极端不均鲁棒性并存的分类框架，已成为深度学习方法走向实用化的关键挑战之一。

3.2 模型可解释性困境

深度模型在性能提升的同时，也引入了结构复杂性与推理不透明的双重障碍。尤其在加密流量识别场景中，模型输出往往缺乏可验证的决策依据，使网络管理员在响应判定结果时难以建立信任闭环。现有的可视化方法如 Grad-CAM 或注意力热图虽可揭示局部聚焦区域，但难以对整体预测机制进行因果层级解析。进一步而言，模型可解释性不仅关涉用户理解，更牵涉到安全防御策略的溯源与合法合规的风险证明，其缺失可能使系统面临误判无法澄清的被动局面，构成部署壁垒。

3.3 实时性与资源开销问题

高性能深度模型在推理阶段普遍伴随显著资源消耗，尤其在边缘网络环境下表现出部署受限。复杂结构如多层注意力与长序列建模在延迟与吞吐间的平衡难以兼顾，不适用于需要低响应时延的入侵检测或移动设备端识别任务。尽管模型压缩、量化与蒸馏技术在一定程度上缓解了计算压力，但仍难完全适配多变流量下的动态负载场景。如何在维持分类精度的同时降低算力成本，并在异构设备上实现弹性部署，构成深度学习流量识别体系进一步扩展的现实瓶颈。

3.4 未来融合模型趋势展望

深度学习在网络流量分类中的应用正逐步迈向“多模态协同、结构融合、任务自适应”的新范式。图神经网络已在会话关系建模中展现优势，适合处理跨节点行为传导特性；而多尺度卷积与跨窗口注意机制的耦合，也为捕捉多粒度时间语义提供新途径。未来模型将更倾向引入上下游协同学习机制，例如结合用户行为日志、协议元数据与时序包流构建联合嵌入空间，从而提升语境感知能力与跨协议鲁棒性。国产深度学习平台（如飞桨 PaddlePaddle）与国产芯片协同优化路径，也为行业级落地提供生态支撑，预示流量分类技术即将进入工程可控与模型可信并重的新阶段。

4 结语

本文围绕深度学习在网络流量分类中的实践与挑战，分析了典型模型在不同编码结构、任务场景下的适应特性，指出当前方法在面对小样本稀缺、特征可解释性差与计算开销大的现实环境中仍存不足。未来研究应聚焦于轻量模型设计、跨域泛化能力提升及多模态融合路径，推动深度模型向高效、可控、可部署方向发展，为构建智能化、可信赖的网络安全防护体系奠定基础。

参考文献

[1]孙弘扬. 基于深度学习的网络流量分类方法研究[D]. 齐鲁工业大学,2024.
[2]孔镇,董育宁. 一种基于深度学习的网络流量细粒度分类方法[J]. 南京邮电大学学报(自然科学版),2021,41(3):100-108.
[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):166-174.
[4]王勤凡,翟江涛,陈伟,等. 一种基于图卷积神经网络的加密流量分类方法[J]. 电子测量技术,2022,45(14):109-115.
[5]徐正. 基于深度学习的网络流量分类方法研究[D]. 青岛理工大学,2025.