蔡云冰. 基于神经网络的网络流量分类算法[J]. 智能计算机与应用,2026,16(2):84-89. DOI:10.20169/j.issn.2095-2163.25081602

基于神经网络的网络流量分类算法

蔡云冰[1,2]

(1 公安部第三研究所, 上海 200030; 2 上海网络与信息安全测评工程技术研究中心, 上海 200030)

摘 要: 在数字化转型背景下,全球网络流量快速增长对网络治理技术体系提出新挑战。为提升入侵检测系统效能,提高网络流量分类的准确性,本文提出基于 YOLOv12 改进的网络流量分类模型,通过引入高效多尺度注意力结构,在保持计算复杂度不变的情况下有效解决了原有模型区域注意力机制在最终分类阶段的不足;同时采用 C3K2_RepLKNet 大卷积核架构扩展感受野,优化空间信息捕获能力,减少模型对局部纹理特征的过度依赖。实验结果表明,相较于现有技术方法,本文提出的模型在 USTC-TFC2016 基准数据集上取得了显著提升,其准确率、精确率、召回率和 $F1$ 值分别达到 99.22%、99.26%、99.17% 和 99.21%,充分展现了模型的卓越性能。本方法充分满足了网络流量分类领域对算法实时性和准确性的需求。

关键词: 网络流量分类; YOLOv12; 高效多尺度注意力结构; 大卷积核架构; USTC-TFC2016

中图分类号: TP391 **文献标志码**: A **文章编号**: 2095-2163(2026)02-0084-06

Network traffic classification algorithms based on neural networks

CAI Yunbing[1,2]

(1 The Third Research Institute of Ministry of Public Security, Shanghai 200030, China;
2 Shanghai Engineering Research Center for Network and Information Security Testing, Shanghai 200030, China)

Abstract: Under the context of digital transformation, the rapid growth of global network traffic has posed new challenges to the network governance technology framework. To enhance the performance of intrusion detection systems and improve the accuracy of network traffic classification, this paper proposes an improved network traffic classification model based on YOLOv12. By introducing an efficient multi-scale attention structure, the model effectively addresses the limitations of the original region-based attention mechanism in the final classification stage while maintaining computational complexity. Additionally, the model employs the C3K2_RepLKNet large kernel architecture to expand the receptive field, optimizing spatial information capture and reducing excessive reliance on local texture features. Experimental results demonstrate that compared to existing methodologies, the proposed model achieves significant performance improvements on the USTC-TFC2016 benchmark dataset, with accuracy, precision, recall, and $F1$ - score reaching 99.22%, 99.26%, 99.17%, and 99.21%, respectively. These results underscore the model's exceptional performance metrics. The proposed method fully addresses the demand for algorithmic real-time performance and accuracy in the field of network traffic classification.

Key words: network traffic classification; YOLOv12; efficient multi - scale attention structure; large convolution kernel architecture; USTC-TFC2016

0 引 言

随着物联网、5G 等技术的普及,网络流量规模呈指数级增长,其异构性、动态性及高维特征日益突出,对网络空间治理架构与技术体系提出了新挑战[1]。网络流量分类技术通过解析流量特征并结合模式识别,实现协议类型与威胁特征的精准识别,显著提升威胁识别效率与判定准确性,为资源调度、威胁预警及服务质量优化提供技术支撑[2]。在此背景下,网络流量分类技术的持续创新不仅是提升入侵检测系统效能的核心驱动力,更是构建主动防御体系、维护数字主权与国家安全的战略性技术基石。

在计算机网络领域,网络流量分类技术的研究进展始终与技术革新相辅相成。根据技术实现路径的不同,现有分类方法可归纳为:基于端口识别的流

作者简介: 蔡云冰(1999—),男,硕士研究生,主要研究方向:网络安全,深度学习。Email:caiyb@mctc.org.cn。

收稿日期: 2025-08-16

量分类方法、基于深度包(Deep Packet Inspection, DPI)检测的流量分类方法、基于传统机器学习的流量分类方法和基于深度学习的流量分类方法[3]。

当下,基于端口识别和 DPI 的流量分类方法仍作为基础技术存在,但其应用范围显著受限。端口识别通过匹配数据包的端口号与 IETF/IANA 标准映射规则推断流量类型,虽因简单高效而适用于内网或固定端口的非加密场景,却难以应对加密协议、动态端口分配及隧道技术带来的挑战,且易被攻击者利用非标准端口规避检测。基于 DPI 的方法[4]通过解析应用层内容实现精准分类,虽能识别未加密流量或加密元数据,但面对端到端加密时因无法解密内容而失效,且高计算开销使其难以在高吞吐量场景高效部署,同时新型协议和流量混淆技术进一步削弱其准确性。因此,两者独立应用仅限于特定受控环境或辅助性分析任务。

传统机器学习的流量分类方法结合人工设计的特征提取与监督模型进行分类。其流程包括从网络数据包提取统计特征和协议特征,而后输入预训练模型完成分类。Rookard 等学者[5]提出了一种基于深度 Q 网络的强化学习方法,旨在解决嵌入式系统、物联网设备等小型计算平台的网络攻击防护问题。余伟良等学者[6]提出 FastSplit-RF 算法,利用多臂赌博机策略替代随机森林节点分裂遍历,实现物联网流量快速分类。Monshizadeh 等学者[7]构建组合无监督架构,融合多种聚类算法,结合非欧几里得距离的新型相似性指标重构特征空间,最终实现了对未知流量的高效聚类。该类方法依赖人工特征工程与参数调优,具备强可解释性、计算需求适中,适合小到中等规模数据集,但性能受特征质量与覆盖范围限制,关键特征缺失会显著降低精度,且依赖标注数据,难以适应动态流量变化,因此多用于特征明确、标注数据充足但计算资源有限的场景。

基于深度学习的流量分类方法利用端到端深度神经网络直接从原始流量数据中提取特征并分类。其核心是运用 CNN、RNN、LSTM 或 Transformer 等模型的非线性建模能力,处理包含时序特性、统计特征及协议标识的多维度数据。张双全等学者[8]提出 HaoResNet,利用残差层缓解梯度问题并加速模型收敛,验证了残差网络在攻击检测中的有效性。魏德宾等学者[9]设计 GMTBLC 架构,融合 GMA-Transformer 与 Bi-LSTM。其中,PCMT 模块通过混合注意力提升全局特征捕捉,SFE 模块结合残差卷积和 Bi-LSTM 增强时空特征提取,动态加权融合机制提升分类性能。李道全等学者[10]改进 ViT 架构为 SA-ViT,采用 Longformer 稀疏注意力机制,通过滑动窗口、空洞滑窗与全局注意力的结合,将计算复杂度从 $O(n^2)$ 降至 $O(n)$,提升模型对局部和全局特征的表达能力。该类方法优势包括自动捕捉高阶特征关联、泛化能力强且借助 GPU/TPU 加速满足实时需求,但存在模型过拟合、计算资源消耗大及决策黑箱问题。

1　研究内容

现有研究表明,传统流量检测方法难以适应现代网络环境的实时性和多模态数据需求,其效能已无法满足应用要求。机器学习虽实现自动化分析,但依赖大量标注数据,影响部署效率,而深度学习通过端到端特征提取在复杂环境中更具适应性。因此,本文基于深度学习的流量分类方法进行研究,旨在提升现有分类方法的准确性。

1.1　网络架构

基于 Transformer 的图像分类模型虽性能优异,但因高计算复杂度、显存占用大及长训练推理时间,难以实际部署。其特征提取侧重全局依赖,存在局部细节表征不足的问题。布法罗大学与中科院提出的 YOLOv12[11]框架通过架构创新平衡了性能与效率,其区域注意力模块与残差高效层聚合网络降低了计算复杂度,维持大范围感受野,跨层特征融合缓解梯度弥散问题,提升稳定性。针对网络流量分类领域对轻量化架构与高效计算的需求,YOLOv12 模型凭借上述优势,成为该应用场景的理想方案。

本研究基于 YOLOv12 主干网络,通过引入高效多尺度注意力结构(Efficient Multi-scale Attention, EMA)[12]与重参数化大核网络(Reparameterized Large Kernel Net, RepLKNet)[13]优化网络流量分类适应性。针对 YOLOv12 区域注意力模块全局语义建模不足的问题,EMA 模块通过多尺度特征融合增强分类阶段的全局语义表征能力。针对 C3K2 结构需多层堆叠导致局部纹理依赖过强的缺陷,改进的 C3K2_RepLkBlock 模块采用大核设计直接扩展感受野,有效提升全局结构特征建模能力,显著增强特征表达。整体框架如图 1 所示。

1.2　高效多尺度注意力结构 EMA

针对图像分类任务,YOLOv12 通过区域注意力模块(A2 模块)与残差高效层聚合网络(R-ELAN)实现特征提取。然而,网络多尺度特征融合与通道权重分配存在局限。A2 模块虽以区域注意力机制

平衡计算成本与全局感受野,但其空间维度优化设计缺乏动态多尺度特征融合能力;R-ELAN 的块级残差结构虽改善梯度传播,但层间连接导致通道权重失衡。为此本文在分类模块前引入 EMA 模块,在保持计算复杂度前提下,通过多尺度特征协同、通道均衡加权及全局空间整合,系统提升了网络流量的表征质量与分类判别能力。

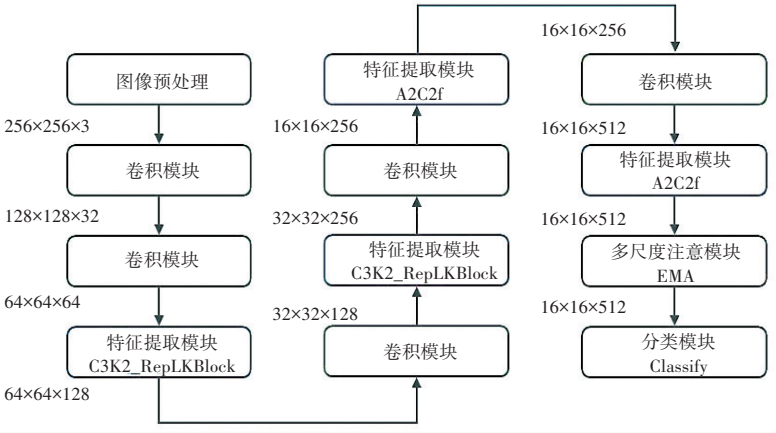

图 1 模型整体结构图

Fig. 1 Overall architecture diagram of the model

EMA 模块通过无通道缩减的多尺度分组策略与并行分支交互机制,增强了网络流量分类中的特征表达能力,其轻量化设计与 YOLO 实时检测框架兼容。EMA 模块结构如图 2 所示。由图 2 可知,输入特征图(B, C, H, W)经分组重塑为($B*G$, $C//G$, H, W),其中,B 表示批量大小,C 表示通道数,H 表示特征图的高度,W 表示特征图的宽度,G 表示分组数量。随后,分别沿高度和宽度方向进行自适应平均池化提取空间特征,拼接后通过 1×1 卷积融合并拆分生成空间注意力图,经 Sigmoid 调制后与分组特征相乘。调制后的特征经组归一化处理后,与另一路由 3×3 卷积提取的局部特征分别通过全局平均池化后经 Softmax 生成通道注意力权重,最终经矩阵乘法计算综合权重并重塑为原始维度,实现分组内多尺度空间与通道特征的协同整合。

1.3 大卷积核架构 C3K2_RepLKBlock

网络流量图像源于像素值直接映射原始数据包的字节信息,表现为缺乏像素间空间连续性,相邻像素无明确语义关联且零值区域易被误判噪声,因此仅依靠局部特征难以表征整体语义。YOLOv12 的 C3K2 模块采用小卷积核 Bottleneck 结构,受限于传统卷积结构感受野不足,难以捕捉全局上下文特征,易受局部纹理干扰,且堆叠加深会导致梯度传播困难。为此,本文采用大卷积核 RepLKBlock 替代 Bottleneck 结构,增强模型全局形状特征捕捉,规避了小卷积核堆叠结构对局部纹理的过度依赖。

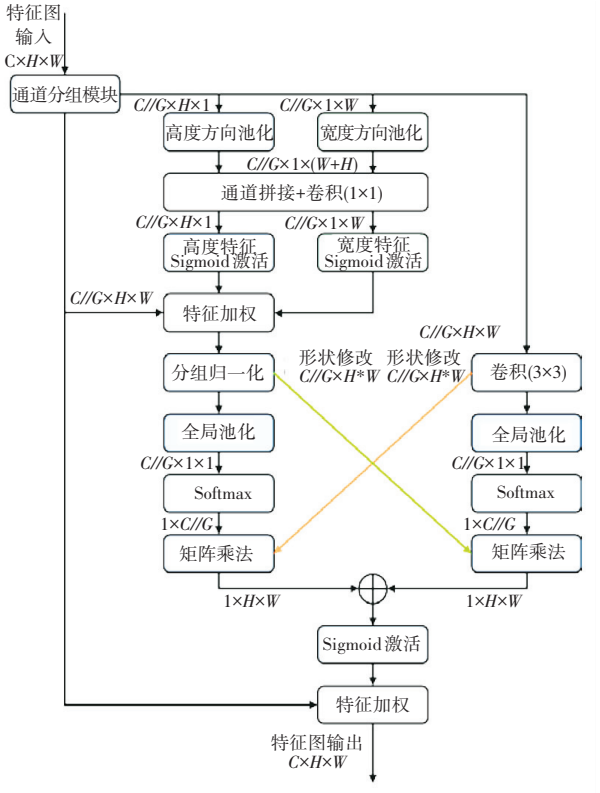

图 2 EMA 模块结构图

Fig. 2 Structure diagram of the EMA module

改进后的 C3K2_RepLKBlock 模块通过大核操作替代传统小核堆叠设计,直接扩展感受野以高效捕捉全局上下文信息。该架构通过跨阶段连接实现多尺度融合,在增强形状特征学习能力的同时提升对网络流量图像中周期性、突发性空间结构的敏感

性，最终实现分类鲁棒性的突破性提升。C3K2_RepLKBlock 模块结构如图 3 所示，输入特征经通道利用扩展卷积分割为 $[y_0, y_1]$ 两路，其中 y_0 保留原始特征信息，y_1 分支则依次通过 n 个级联的 RepLKBlock 单元进行深度处理。每个 RepLKBlock 单元先执行预归一化与通道扩展，随后采用 5×5 重参数化小核与 27×27 大核的深度可分离卷积组合建模长程依赖，经 ReLU 激活及通道恢复后，通过残差连接与随机深度正则化保持梯度稳定。所有 RepLKBlock 的输出与初始的 y_0、y_1 特征在通道维度进行拼接后形成 $(2 + n) \times c$ 维度张量（n 为 RepLKBlock 数量），最终经卷积层压缩至 C_2 通道完成特征整合。该设计通过大核卷积与轻量化结构的结合，在计算效率与模型表征能力间取得平衡。

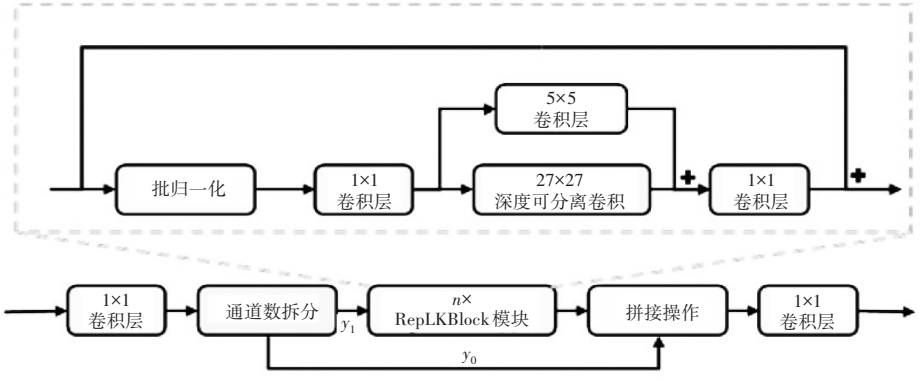

图 3　C3K2_RepLKBlock 模块结构图

Fig. 3　Structure diagram of the C3K2_RepLKBlock module

2　实验与分析

2.1　数据集处理

本研究采用 USTC-TFC2016 数据集[14]进行系统评估，该数据集由中科大团队构建，是为流量分类领域构建的开源基准数据集，用于区分恶意软件与正常网络流量。该数据集包含 10 类源自捷克理工大学 CTU-13 数据集的真实恶意软件流量及 10 种常见应用流量。数据集总容量 3.71 GB，采用标准化 pcap 格式存储，支持主流工具高效解析，为网络分析、入侵检测及模型鲁棒性与泛化能力评估提供高质量实验基准。

针对流量分类任务，本文采用基于双向会话的流量划分策略，其通过整合请求与响应的双向通信过程，相比单向数据流方法更完整地保留应用层语义特征。在数据表征层面，基于 OSI 模型 L7 层数据直接承载用户应用程序交互内容，用其进行实验可有效规避低层元数据冗余，提升分类模型特征聚焦度。关于数据集构建，解析 pcap 文件提取会话字节流，经标准化处理后线性映射至 8 位灰度空间，对前 1 024 字节实施固定长度截断或零填充处理，最终重构为 32×32 像素灰度图像以适配深度学习模型输入要求。

2.2　评价指标与实验配置

本研究采用准确率（Accuracy，AC）、精确率（Precision，PR）、召回率（Recall，RC）和 $F1$ 值（$F1$-score，$F1$）评估本文所提模型性能，其中 $F1$ 值作为精确率与召回率的调和平均数，能平衡两者权重并适应类别不均衡场景；召回率表示实际真实目标中正确识别的比例；精确率表示模型检测结果中真实样本的比例；准确率则衡量整体分类正确的样本占比。上述指标的计算公式如下：

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{1}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2}$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{3}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{4}$$

其中，TP、为真正例（True Positive），表示实际为正类且被模型正确预测为正类的样本数；FP、为假正例（False Positive），表示实际为负类但被误判为正类的数量；FN、为假反例（False Negative），表示实际为正类却被误判为负类的情况；TN、为真反例（True Negative），表示实际为负类且预测正确的样本。

实验基于 AMD R7 5700 G 处理器、NVIDIA RTX 4070 Ti Super 显卡及 64 GB 内存硬件配置，在 Windows 10 系统下采用 Python 3.8 与 PyTorch 1.12 框架构建模型。本文研究中针对提出的改进方案统

一设置训练 300 轮,批次大小 64,输入图像统一调整至 256×256 像素。采用 SGD 优化器并配置学习率线性衰减策略(初始 0.01 至终 0.000 1),通过渐进式衰减平衡训练速度与模型收敛效果以确保训练稳定性和优化效率。

2.3 分类实验结果

本研究在 USTC-TFC2016 数据集上进行了涵盖正常与恶意流量的 20 类网络流量分类实验。多分类结果见表 1,本研究提出的模型在该数据集上的多分类性能评估采用精确率、召回率和 *F*1 值作为评价指标。实验结果表明,在 BitTorrent、Neris、Outlook 和 Virut 等流量类别中,模型表现稍逊于其他类别,可能归因于在数据预处理阶段,将原始流量转换为灰度图像时,应用类别间的信息相似性导致生成的灰度图特征接近,从而影响了分类精度。除此以外,在其余流量类别中,本文所提模型均展现出良好的泛化能力,验证了其在网络流量分类任务中的有效性。

表 1 多分类结果

Table 1 Multi-class classification results %

流量类别	精确率	召回率	*F*1 值
BitTorrent	96.76	99.60	98.16
Cridex	100.00	100.00	100.00
Facetime	100.00	100.00	100.00
FTP	100.00	100.00	100.00
Geodo	99.26	99.70	99.48
Gmail	98.80	97.06	97.93
Htbot	99.66	98.66	99.16
Miuref	100.00	99.80	99.90
MySQL	100.00	99.72	99.86
Neris	97.74	97.51	97.62
Nsis-ay	99.67	99.34	99.50
Outlook	97.87	98.13	98.00
Shifu	99.90	99.90	99.90
Skype	100.00	100.00	100.00
SMB	100.00	99.82	99.91
Tinba	99.77	100.00	99.88
Virut	96.43	96.90	96.66
Weibo	100.00	97.59	98.78
WorldOfWarcraft	100.00	100.00	100.00
Zeus	99.30	99.65	99.47
平均值	99.26	99.17	99.21

2.4 对比实验结果

为系统评估本文所设计算法在网络流量分类任务中的性能表现,本研究将其与 HaoResNet、YaTC、SA-Vit 等主流方法进行了对比分析,相关结果见表 2。实验结果显示,传统方法的性能指标普遍低于深度学习方法,这表明深度学习方法在网络流量分类任务中展现出显著优势,有效验证了其技术先进性。本文所提方法在准确率、精确率、召回率及 *F*1 值四项核心指标上分别达到 99.22%、99.26%、99.17% 和 99.21%。具体而言,除召回率指标(99.17%)略低于 ET-BERT 算法(99.20%)外,其余指标均优于其他对比方法并达到最优水平。值得注意的是,本文用于特征提取的 backbone 以轻量化实时检测架构 YOLOv12s-cls 为基底进行了优化设计,在保持高效性的同时,其性能表现略优于复杂模型 ET-BERT,充分彰显了本方法架构设计上的优势。

表 2 对比实验结果

Table 2 Results of comparative experiments %

模型	准确率	精确率	召回率	*F*1 值
AppScanner[15]	89.50	89.80	89.70	88.90
BIND[16]	84.60	86.80	83.80	84.00
FlowPrint[17]	81.50	64.30	70.00	65.70
DF[18]	77.90	78.80	78.20	75.90
FS-Net[19]	88.50	88.50	89.20	88.40
GraphDApp[20]	87.90	82.30	82.60	82.30
DeepPacket[21]	96.40	96.50	96.30	96.40
FastTraffic[22]	96.90	96.60	95.00	95.50
SA-Vit[10]	97.50	97.20	97.50	97.30
HaoResNet[8]	—	—	98.70	98.70
PERT[23]	99.10	99.10	99.10	99.10
ETBERT[24]	99.20	99.20	**99.20**	99.20
YaTC[25]	97.90	—	—	96.60
本文	**99.22**	**99.26**	99.17	**99.21**

2.5 消融实验结果

为验证改进策略对网络流量分类任务的提升效果,本研究在 USTC-TFC2016 数据集上开展了消融实验。通过逐步移除各改进策略模块,对模型性能进行对比分析。实验结果见表 3。当逐步移除改进设计后,模型性能均出现显著下降。

表 3 消融实验结果

Table 3 Results of ablation experiment %

模型	准确率	精确率	召回率	*F*1 值
Base	99.02	99.09	98.86	98.95
Base+E	99.14	99.21	99.01	99.10
Base+E+R	**99.22**	**99.26**	**99.17**	**99.21**

注:base 表示原始 YOLOv12s-cls 模型,E 表示 EMA,R 表示 C3K2_RepLKBlock 模块

3　结束语

依据网络流量入侵检测的实际需求，本文提出了一种基于 YOLOv12 改进的网络流量分类模型。针对 YOLOv12s 分类网络在网络流量分类领域的不足进行了改进和优化，包括高效多尺度注意力结构 EMA，以及大卷积核设计模块以提高对网络流量图像的全局信息提取能力。实验结果表明，本方法达到了 99.22%的准确度，领先现有的诸多算法。本文算法可以满足网络流量的分类要求，具备极佳的实践意义。

参考文献

[1] 周磊，石怀峰，杨恺，等. 基于大语言模型的网络流量智能预测[J]. 计算机科学，2025，52(S1)：41-47.

[2] 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.

[3] 王影，王钢，高雲鹏，等. 基于深度学习的加密流量分类研究综述[J]. 计算机工程与应用，2025，61(21)：61-80.

[4] KHANDAIT P，HUBBALLI N，MAZUMDAR B. IoTHunter：IoT network traffic classification using device specific keywords[J]. IET Networks，2021，10(2)：59-75.

[5] ROOKARD C，KHOJANDI A. Applying deep reinforcement learning for detection of Internet-of-Things cyber attacks[C]// Proceedings of 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). Piscataway，NJ：IEEE，2023：389-395.

[6] 余伟良，高见，王润田. 基于轻量化随机森林算法的物联网流量分类[J]. 计算机工程与设计，2024，45(12)：3553-3559.

[7] MONSHIZADEH M，KHATRI V，KANTOLA R，et al. A deep density based and self-determining clustering approach to label unknown traffic[J]. Journal of Network Computer Applications，2022，207：103513.

[8] 张双全，殷中豪，张环，等. 基于残差卷积神经网络的网络攻击检测技术研究[J]. 信息网络安全，2025，25(2)：240-248.

[9] 魏德宾，江亲龙，温京龙，等. GMTBLC：基于深度学习的双模态网络流量分类[J]. 电信科学，2024，40(12)：93-106.

[10] 李道全，高洁，聂若琳，等. 基于改进 ViT 的网络流量分类方法[J]. 计算机工程与设计，2025，46(2)：431-437.

[11] TIAN Yuejie，YE Qixiang，DOERMANN D. Yolov12：Attention-centric real-time object detectors[J]. arXiv preprint arXiv，2502.12524，2025.

[12] OUYANG Daliang，HE Su，ZHANG Guodong，et al. Efficient multi-scale attention module with cross-spatial learning[C]// Proceedings of 2023 IEEE International Conference on Acoustics，Speech and Signal Processing (ICASSP). Piscataway，NJ：IEEE，2023：1-5.

[13] DING Xiaohan，ZHANG Xiangyu，HAN Jungong，et al. Scaling up your kernels to 31×31：Revisiting large kernel design in CNNs[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway，NJ：IEEE，2022：11963-11975.

[14] WANG Wei，ZHU Ming，ZENG Xuewen，et al. Malware traffic classification using convolutional neural network for representation learning[C]//Proceedings of 2017 International conference on information networking (ICOIN). Piscataway，NJ：IEEE，2017：712-717.

[15] TAYLOR V F，SPOLAOR R，CONTI M，et al. Robust smartphone App identification via encrypted network traffic analysis[J]. IEEE Transactions on Information Forensics Security，2017，13(1)：63-78.

[16] AL-NAAMI K，CHANDRA S，MUSTAFA A，et al. Adaptive encrypted traffic fingerprinting with bi-directional dependence[C]//Proceedings of the 32nd Annual Conference on Computer Security Applications. New York：ACM，2016：177-188.

[17] EDE V T，BORTOLAMEOTTI R，CONTINELLA A，et al. Flowprint：Semi-supervised mobile-app fingerprinting on encrypted network traffic[C]//Proceedings of Network and Distributed System Security Symposium (NDSS). San Diego：ISOC，2020：27.

[18] 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.

[19] LIU Chang，HE Longtao，XIONG Gang，et al. FS-Net：A flow sequence network for encrypted traffic classification[C]// Proceedings of the IEEE Conference on Computer Communications. Piscataway，NJ：IEEE，2019：1171-1179.

[20] 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 Security，2021，16：2367-2380.

[21] LOTFOLLAHI M，JAFARI SIAVOSHANI 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.

[22] XU Yuwei，CAO Jie，SONG Kehui，et al. FastTraffic：A lightweight method for encrypted traffic fast classification[J]. Computer Networks，2023，235：109965.

[23] HE Hongye，YANG Zhiguo，CHEN Xiangning. Payload encoding representation from transformer for encrypted traffic classification[J]. ZTE Communications，2021，19(4)：90-97.

[24] 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. New York：ACM，2022：633-642.

[25] 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 AAAI Conference on Artificial Intelligence. Washington，DC：AAAI，2023：5420-5427.