基于梯度协同与特征融合的加密流量检测

卢嘉中[1,2,3,4],余 坤[1,2,3*],刘小垒[5],张小松[6]

(1. 成都信息工程大学网络空间安全学院(芯谷产业学院),四川成都 610225;
2. 先进密码技术与系统安全四川省重点实验室,四川成都 610225;
3. 先进微处理器技术国家工程研究中心(工业控制与安全分中心),四川成都 610225;
4. 成都信息工程大学人工智能学院,四川成都 610225;
5. 国家工程物理交叉科学研究中心,四川绵阳 621000;
6. 电子科技大学信息与软件工程学院,四川成都 611731)

摘 要: 随着物联网(Internet of Things,IoT)设备的广泛部署和网络通信的快速发展,加密流量已成为主流传输形式,但同时也为后门攻击和针对性投毒攻击等高级威胁提供了隐蔽通道。为应对加密恶意流量检测这一关键安全挑战,本文提出基于梯度协同与特征融合网络的加密流量检测模型,专用于提升网络中加密恶意流量的检测能力。该模型包含两大核心模块:特征融合模块与梯度协同模块,显著增强模型对复杂加密流量模式的表征学习能力。在特征融合模块中,该模型充分利用卷积神经网络(Convolutional Neural Network,CNN)的局部特征提取优势以及知识增强网络(Kolmogorov-Arnold Networks,KAN)的全局特征建模能力,实现局部与全局特征的高效深度融合。为进一步提升子模型间的协同性与鲁棒性,梯度协同机制使多个子模型能够实时动态共享梯度并联合优化损失函数,从而在训练过程中相互引导、纠错,强化对多样化加密恶意流量模式的捕获。该机制不仅缓解了局部与全局特征学习间的冲突,还显著提升了模型对隐蔽加密攻击流量的敏感性。在多个公开加密流量数据集上的实验结果表明,本文所提出的模型相较现有方法在F1分数上提升约7%,实现了对加密恶意流量的高精度分类。

关键词: 加密流量;流量检测;特征融合;梯度协同

基金项目: 国家自然科学基金(No.62102049);四川省自然科学基金(No.2025ZNSFSC0507);先进密码技术与系统安全四川省重点实验室开放基金(No.SKLACSS-202402,No.SKLACSS-202307)

中图分类号: TP393.08;TN911.7 **文献标识码:** A **文章编号:** 0372-2112(2026)02-0532-12

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20251021

Encrypted Traffic Detection Based on Gradient Collaboration and Feature Fusion

LU Jiazhong[1,2,3,4], YU Kun[1,2,3*], LIU Xiaolei[5], ZHANG Xiaosong[6]

(1. *School of Cybersecurity* (*Xin Gu Industrial College*), *Chengdu University of Information Technology*, *Chengdu*, *Sichuan* 610225, *China*;
2. *Advanced Cryptography and System Security Key Laboratory of Sichuan Province*, *Chengdu*, *Sichuan* 610225, *China*;
3. *SUGON Industrial Control and Security Center*, *Chengdu*, *Sichuan* 610225, *China*;
4. *School of Artificial Intelligence*, *Chengdu University of Information Technology*, *Chengdu*, *Sichuan* 610225, *China*;
5. *National Interdisciplinary Research Center of Engineering Physics*, *Mianyang*, *Sichuan* 621000, *China*;
6. *School of Information and Software Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* , *Sichuan* 611731, *China*)

Abstract: With the widespread deployment of Internet of Things (IoT) devices and the rapid development of network communications, encrypted traffic has become the mainstream transmission form. However, it also provides covert channels for advanced threats such as backdoor attacks and targeted poisoning attacks. To address the critical security challenge of encrypted malicious traffic detection, this paper proposes an encrypted traffic detection model based on gradient collaboration and feature fusion networks, specifically designed to enhance the detection capability of encrypted malicious traffic in networks. The model consists of two core modules: the feature fusion module and the gradient collaboration module, which significantly improve the model's ability to learn representations of complex encrypted traffic patterns. In the feature fusion module, the model fully leverages the local feature extraction advantages of convolutional neural networks (CNN) and the global feature modeling capabilities of knowledge-augmented networks (KAN) to achieve efficient deep fusion of local and global features. To further enhance the collaboration and robustness among sub-models, the gradient collaboration mecha-

收稿日期:2025-12-28;录用日期:2026-02-09;责任编委:赵瑞杰
*通信作者:余坤

nism enables multiple sub-models to dynamically share gradients in real-time and jointly optimize the loss function, thereby guiding and correcting each other during training, and strengthening the capture of diverse encrypted malicious traffic patterns. This mechanism not only alleviates conflicts between local and global feature learning but also significantly improves the model's sensitivity to covert encrypted attack traffic. Experimental results on multiple public encrypted traffic datasets show that the proposed model achieves an improvement of approximately 7% in F1 score compared to existing methods, enabling high-precision classification of encrypted malicious traffic.

Keywords: encrypted traffic; traffic detection; feature fusion; gradient collaboration

Foundation Item(s): National Natural Science Foundation of China (No.62102049); Natural Science Foundation of Sichuan Province(No.2025ZNSFSC0507); Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (No.SKLACSS-202402, No.SKLACSS-202307)

0 引言

随着物联网(Internet of Things,IoT)设备的爆发式增长和网络通信技术的迅猛演进,加密流量已成为主流传输形式。然而,这也为后门攻击和针对性投毒攻击等高级威胁提供了天然的隐蔽通道[1-2]。攻击者不断采用更隐匿、更复杂的手段,使传统安全防御机制面临严峻挑战。加密恶意流量检测因此成为现代网络安全领域的核心研究方向。传统检测方法,如基于规则匹配和统计特征分析,在早期威胁防范中取得一定成效,但面对演化迅速、形态多样的现代攻击往往力不从心。当前主流加密流量检测方法主要存在两大瓶颈。

(1)特征建模能力不足:现有方法通常仅关注单一维度特征建模,如局部统计信息或全局流量关联关系,难以同时捕捉局部与全局特征间的互补信息。在高并发、低时延的加密流量场景下,攻击模式更加隐蔽,传统方法难以有效应对。例如,DDoS攻击的流量波动可能呈现大规模全局模式,而仅依赖局部特征的模型难以准确识别。局部特征(如包长度、协议类型、时间间隔)可刻画微观流量模式,全局特征(如流量时序特性或网络拓扑结构)则反映攻击的宏观行为。然而,传统方法往往从单一视角建模流量,忽略局部与全局特征的协同作用,导致在复杂攻击场景下易产生漏报或误报。

(2)动态环境适应性欠缺:随着IoT设备的广泛部署,网络流量的复杂性和动态性显著增强,对检测方法的适应能力提出更高要求。网络环境、用户行为及攻击策略的持续变化导致流量模式不断演变,而许多传统方法依赖固定特征和静态规则,难以适应此类变化。例如,动态切换的网络拓扑可能改变攻击路径,使传统流量分析失效。一旦流量模式发生显著变化,静态模型的检测性能将急剧下降。同时,某些恶意攻击在初期可能呈现可识别模式,但攻击者往往迅速调整策略以逃避检测。为应对这些挑战,检测方法必须具备动态自适应能力,能够快速学习并调整以适应新流量模式,保持稳定检测性能。

为解决上述难题,本文提出梯度协同机制,并据此设计了一种新型加密恶意流量分类模型,该融合卷积神经网络(Convolutional Neural Network,CNN)[3]与知识增强网络(Kolmogorov-Arnold Networks,KAN)[4]的结构优势,旨在全面建模加密流量的局部与全局特征。具体而言,本文的模型包含四大核心模块:局部特征提取模块、全局特征建模模块、特征融合模块以及梯度协同模块。局部特征提取模块基于CNN高效提取包长度、时间间隔、协议标识符等微观模式特征。全局特征建模模块利用KAN动态捕捉流量的时序分布与全局依赖关系,构建宏观行为特征。为更贴近真实网络环境,模型并非一次性访问完整训练集构建全局特征,而是按时间顺序逐样本输入,动态构建全局表征。特征融合模块基于注意力机制,根据特征重要性动态分配权重,在局部与全局特征建模基础上实现精准融合。梯度协同模块是模型的核心,专为解决多模块特征学习中优化方向不一致问题而设计。与传统知识蒸馏方法[5]的"教师-学生"单向学习机制不同,梯度协同采用双向互学习机制,使两个子模型在各自专长领域相互学习。

具体而言,在训练过程中,各模块通过共享梯度信息动态调整参数。局部特征提取模块与全局特征建模模块的梯度信号实时交换共享。各子模块不仅在反向传播中更新自身参数,还接收来自其他模块的梯度信号,实现特征学习的全模块协同优化。该机制确保局部细粒度建模与全局宏观抽象的互补性。梯度协同不仅克服了学生模型难以超越教师模型的局限,还缓解了传统深度学习中的梯度消失问题,提升了模型训练稳定性和收敛速度。

本文主要贡献包括:(1)提出梯度协同机制,通过共享反向传播梯度信息增强不同模型模块的协同学习,使整个网络更高效、精准地优化训练过程,在IoT动态环境中,该机制提升模型适应性,使其在复杂高速网络条件下仍能稳定运行,同时,梯度协同通过跨模块协调优化增强特征建模能力,捕获更层次化、多

样化的特征表征，弥补现有方法在特征提取上的不足，相较传统知识蒸馏，梯度协同既保留模型间信息传递优势，又突破学生模型难以超越教师模型的瓶颈，并缓解深度学习中的梯度消失问题，提升训练稳定性和收敛速度；(2)设计特征提取与融合方法，局部模块聚焦捕获数据流中细粒度的包级特征，全局模块采用动态建模与注意力机制，构建流量序列的整体行为特征与依赖关系，通过在特征融合阶段引入注意力机制，实现局部与全局信息的精准整合，显著提升加密恶意流量检测精度，在IoT场景中，该方法适应异构流量模式，有效捕获低频长依赖攻击行为，提升检测能力；(3)提出加密恶意流量分类模型，基于特征融合与梯度协同，增强了内部模块间协作，同时适配多种网络环境，包括网络流量、加密流量及IoT场景，展现出强大适应性，在多个公开数据集上的实验表明，本文的模型在检测准确率、误报率等关键指标上显著优于现有方法，分类精度提升高达7%。

1 相关工作

加密恶意流量检测是网络安全领域的关键研究方向，已从多个视角得到广泛探讨。随着网络结构与流量行为的日益复杂化，传统检测方法的局限性愈发凸显。本节聚焦三种主流技术路线对加密恶意流量检测的最新进展进行综述：基于规则的方法、基于特征的方法以及基于深度学习的方法。

基于规则的加密恶意流量检测方法是最为经典的技术路线。该类方法预定义一系列规则或签名，与网络流量进行匹配以判别是否存在恶意行为。Ayo等人[6]提出Bot-FFX僵尸网络检测框架，利用基于规则的遗传算法识别僵尸网络活动。该方法通过计算域名往返时延标准差、谷歌点击量均值及遗传阈值等特征实现域名分类。然而，当攻击手法演化时，若规则未能及时更新，检测性能将显著下降。孙剑文等人[7]提出了一种名为MTAttention的端到端恶意流量检测方法，对网络行为流量的异构标头特征和有效负载进行统一编码。马博文等人[8]提出了一种基于后门攻击的恶意流量逃逸方法。通过在训练过程中将有毒的训练样本与干净的样本混合，将后门嵌入到分类器中。Afzal等人[9]提出一种基于规则过滤与状态关联的异常检测模型，在规则生成阶段通过状态关联实现时序距离分析以定义规则。Uszko等人[10]开发了一种针对5G WLAN异常规则检测系统，结合机器学习模型通过包分析模块与预定义规则提升效率。对于去认证攻击等场景，依据去认证帧与客户端发送帧计数设定阈值，当去认证帧计数超过客户端帧总数与阈值之和时触发告警。然而，此类方法依赖完整数据集进行规则生成与模型训练，而动态环境中的数据呈增量式到达，无法一次性获取完整数据。这种静态训练机制难以捕捉数据分布的时序演变，导致规则匹配准确率下降。

基于特征的加密恶意流量检测方法侧重分析网络流量的统计与行为模式，以区分正常与恶意活动。但实际应用中，该类方法普遍存在仅关注局部特征提取(如包序列、字节分布、协议特定特征)或全局特征构建(如整体流量行为模式)的局限，单一依赖任一维度均难以全面刻画网络流量的复杂性。Berkay Celik等人[11]提出一种评估恶意软件心跳流量传输层特征空间的框架，仅利用防篡改特征区分恶意流量与合法应用流量。然而，随着伪装恶意软件为HTTP流量等规避技术的演进，该框架检测能力受到影响。Mao等人[12]提出一种流量分类方法，综合TLS、TTL、字节分布、包序列等特征设计MLP与CNN模型，但该方法聚焦局部特征而忽略全局特征。赵荻等人[13]提出了一种针对安全套接层和传输层流量的图表示方法，并构建了基于图卷积神经网络的加密恶意流量识别框架GCN-RF，该方法将流量转化为图结构。Fei等人[14]提出基于卡方检验的EFS-CST算法用于恶意流量检测，将训练时间缩短高达48.9%。Ferriyan等人[15]开发TLS2Vec方法，基于Word2Vec检测加密恶意流量，通过三步流程利用TLS握手与载荷特征在会话终止前实现检测。许小龙等人[16]提出融合切比雪夫图加权网络与深度强化学习的双层优化框架，通过精准流量预测实现车联网边缘计算的高效任务卸载并提升系统计算速率，但该方案未纳入能耗约束，且在隧道等复杂无信号场景下的适配性不足。王承祥等人[17]提出面向6G的无线信道语义建模方法，将信道语义分为状态、行为、事件三层级并结合车载ISAC(Integrated Sensing and Communication)实测完成建模与信道生成，但该研究仅基于28 GHz车载场景验证，在多频段、复杂室外场景的泛化性仍需验证。唐博麟等人[18]提出一种新型的时间序列特征提取方法，该方法通过分析数据包的空序列，提取加密网络流量的关键行为特征，并结合自注意力机制的长短时记忆网络来训练并对流量进行分类。Han等人[19]提出基于图整合理论(Graph Iintegration Theory，GIT)的加密流量入侵检测方法，利用包长度构建图结构，通过GIT将节点信息转化为图分类问题。然而，采用卡方检验进行特征选择可能忽略潜在复杂关系，影响检测准确性。因此，此类基于特征的检测方法在全局与局部特征整合方面存在局限。局部特征虽可精细化攻击模式识别，但需结合全局特征方能全面表征恶意流量行为的复杂性。全局与局部特征的平衡与融合已成为

提升检测性能的关键。在此背景下,深度学习方法的引入为加密恶意流量检测提供了新思路,尤其是知识蒸馏技术可有效传递多样化知识以提升检测性能。

基于知识蒸馏的深度学习方法在加密恶意流量检测中展现出显著优势。Zhu 等人[20]提出轻量级恶意流量检测模型 LKD-STNN,基于知识蒸馏构建,自适应温度函数在知识传递全过程实时调节温度,并结合损失函数与权重更新提升性能。Zhou 等人[21]提出 RG-GLD 异常流量检测模型,采用图神经网络(Graph Neural Networks,GNN)与知识蒸馏构建,通过独特图重构策略以数据通信为节点、特定规则为边构建图,利用 GAT(Graph Attention Network)与 MLP(Multi-Layer Perceptron)提取结构与流量特征进行蒸馏。然而,将流量转化为有向图可能导致大量局部特征丢失,影响检测性能。Lu 等人[22]提出一种结合微网络架构与生成对抗网络(Generative Adversarial Networks, GAN)的新型对抗样本防御算法,旨在最小化训练成本的同时提升分类精度。Huang 等人[23]提出 DIST 知识蒸馏方法,针对学生与教师模型预测差异显著的问题引入基于相关性的损失函数,以皮尔逊相关系数替代 KL(Kullback-Leibler)散度,降低精确对齐需求。但该方法在复杂或高度专业化数据分布任务中表现受限,学生模型过度依赖教师模型关系信息,限制其对动态场景的适应性。戚子健等人[24]提出一种基于双向 GRU(Gated Recurrent Unit)和 CNN 的恶意网络流量检测方法,使用双向 GRU 和 CNN 并行地提取网络流量数据的时间特征和空间特征。Lu 等人[25]提出基于时间间隔的恶意流量分析方法。Niu 等人[26]提出 KDDRL 领域不变表示学习方法,针对知识蒸馏中的领域泛化问题,设计多学生网络并进行两阶段知识蒸馏,学习领域不变表示同时保留领域特定特征。Yang 等人[27]提出分层自监督增强知识蒸馏方法 HSSAKD(Hierarchical Self-Supervision Augmented Knowledge Distillation),引入辅助自监督增强任务,从多尺度特征图派生软自监督增强分布作为丰富暗知识用于蒸馏。但自监督增强任务设计可能不够有效,未能充分提取有价值知识。Lu 等人[28]提出利用 MPNNKDDRL(Message Passing Neural Network for Knowledge-Driven Deep Reinforcement Learning)的入侵检测方法。Yang 等人[29]提出利用教师分类器作为语义评估器评估双模型表征,捕获所有特征维度的高阶结构信息。然而,在处理高度非线性特征关系时,准确性易受影响,难以精准评估学生表征。

本文提出将 KAN 网络全局特征与 CNN 局部特征通过特征融合方式相结合,并引入共享反馈机制实现协同优化,解决现有方法中局部与全局特征建模割裂的问题。据此提出了基于梯度协同与特征融合网络的加密流量检测模型。与传统仅关注单维度特征的方法不同,本文采用联合损失计算与梯度协同机制,在提升分类性能的同时实现快速收敛。

2　数据集

为全面评估所提加密恶意流量检测模型在真实加密通信环境中的性能,本研究选用了两个专为加密流量分析设计的公开基准数据集:ISCXVPN2016 和 ISCXTor2016。这两个数据集均由加拿大网络安全研究所发布,分别捕获了通过 VPN 加密隧道和 Tor 匿名网络传输的真实应用流量,涵盖浏览、邮件、即时通信、流媒体、文件传输、语音通话、P2P 等多种主流网络服务类型,并包含正常用户行为与多种隐蔽恶意行为,具有极高的真实性、完整性和代表性,是当前加密恶意流量检测领域公认的标准评估数据集。

ISCXVPN2016 数据集通过在真实用户操作环境下使用 OpenVPN 构建加密通道,同步采集了相同应用行为的非加密原始流量与对应 VPN 加密流量,为研究加密前后流量特征变化及加密通道下恶意行为检测提供了理想的对照基础。数据集以会话为单位存储为 PCAP(Packet Capture)文件,保留完整的时间戳、五元组信息和加密载荷,覆盖了多种典型攻击场景,包括恶意软件通信、命令与控制信道建立、数据渗漏等,使模型能够在不依赖明文内容的情况下学习加密流量的统计模式与行为异常。

ISCXTor2016 数据集则聚焦于 Tor 匿名网络中的多跳加密通信,所有流量均经过多层洋葱式加密路由传输,彻底混淆了传输层及以上的内容与来源信息。数据集同样包含七类主流应用,但全部在 Tor 环境中生成,模拟了正常匿名浏览与多种恶意匿名攻击行为,如暗网服务访问、匿名 C&C 通信、隐蔽数据外传等,为验证模型对高匿名性、多层嵌套加密恶意流量的识别能力提供了极具挑战性的测试场景。

由于加密机制使得传统基于载荷解析或端口匹配的检测方法完全失效,本文在数据预处理阶段采用时序流量统计特征建模策略,将原始 PCAP 文件按时间顺序切分为固定时窗的动态流量序列,提取包长度序列、到达时间间隔、传输方向序列以及总包数、总字节数、平均包长、长度方差、间隔熵、突发放包率等一系列与加密无关的统计特征作为模型输入。这些特征全部来源于加密载荷外部的元数据,确保检测过程无需解密即可实现高区分度表征。通过将流量视为连续演化的时序信号,模型能够有效捕获加密恶意流量的微观突变模式与宏观行为规律,显著提升对高隐蔽性攻击的敏感性和鲁棒性。本文基于上述两个

数据集进行全面交叉验证，以充分检验模型在真实加密网络环境中的泛化能力和实际部署价值。

3 模型

本节详细阐述了所提出的加密恶意流量检测模型，该模型以特征融合与梯度协同为核心机制，旨在实现对高隐蔽性加密攻击流量的精准识别。模型通过双通道特征建模路径——局部图像化通道与全局结构化通道，分别捕获加密流量的微观模式与宏观行为规律，并通过梯度协同机制实现两路径间的动态优化协同，从而显著提升模型在复杂加密场景下的分类性能与鲁棒性。模型整体架构如图1所示。

3.1 数据预处理

为适配模型的双通道输入结构，本文设计了两条差异化的数据预处理流水线：结构化特征通道用于向KAN模块提供全局时序表征输入；图像化特征通道则将原始流量转换为灰度图像，供CNN模块提取局部空间模式。双通道预处理策略确保输入特征的多样性与互补性，使模型能够同时从微观与宏观视角全面刻画加密流量的行为特性。

在结构化特征通道中，原始PCAP文件被解析为高维向量序列，以适应KAN的符号化全局建模需求。利用Wireshark对流量包进行深度解析，提取包括包长度序列、到达时间间隔（Inter-Arrival Time，IAT）、传输方向标志、协议类型编码、窗口内包数统计、字节总量、平均/方差/熵等在内的多维度通信特征。这些特征全面覆盖了加密流量的静态属性与动态演化规律，为KAN模块构建长期依赖关系与整体行为模式提供了坚实基础。为消除量纲差异对模型学习的影响，所有结构化特征均经过Z-score标准化处理，确保各维度在训练过程中的贡献均衡。

在图像化特征通道中，原始字节流被重构为固定尺寸的灰度图像，以充分利用CNN在局部模式捕获上的先天优势。具体而言，从每个会话的PCAP载荷中截取前784字节（若不足则零填充），直接按原始字节值映射至8×8或28×28灰度图像素网格（像素值范围0~255），不进行归一化或二值化处理，以保留字节分布的原始统计特性。该图像化表示将加密流量的字节序列转化为空间分布模式，使CNN能够有效提取突发放包、协议指纹残留、填充模式等隐蔽局部特征，显著增强对加密通道下微观异常的敏感性。

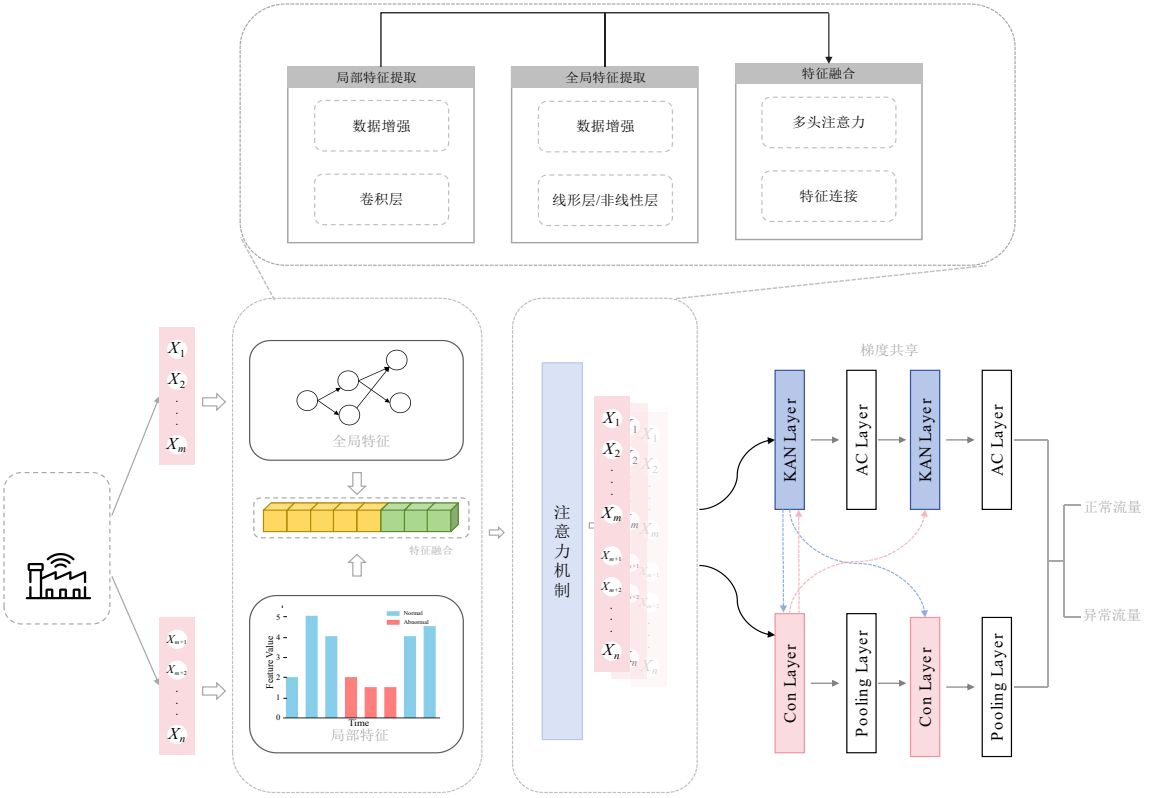


图1 GFFNet模型整体架构

Figure 1 Overall architecture of the GFFNet model

3.2 特征融合

特征融合模块是模型实现多尺度表征整合的核心环节,其目标是通过深度耦合结构化通道与图像化通道的异构特征,构建兼具全局语义理解与局部细节感知的统一高维表征空间,从而显著提升模型对加密恶意流量的鉴别能力。针对加密流量在传输层以上完全混淆的特性,该模块摒弃传统基于明文语义的融合方式,转而从统计行为模式与空间分布规律两个正交维度协同建模,确保在不依赖解密的前提下实现对隐蔽攻击的精准捕获。

在结构化特征通道中,特征提取突破单一粒度限制,采用包级-流级的双层递进式建模策略。设某通信流由N个数据包组成,第i个包的静态属性向量可表示为$\boldsymbol{x}_i=\left[L_i,\Delta t_i,d_i,w_i,\cdots\right]$,其中$L_i$为包长度,$\Delta t_i$为时间戳偏移,$d_i$为方向标志,$w_i$为滑动窗口统计量等微观属性。经包级特征提取器$f_p(\cdot)$编码后,得到包级表征$\boldsymbol{h}_i^{(p)}=f_p(\boldsymbol{x}_i)$。随后,根据五元组$(sIP,dIP,sPort,dPort,proto)$将属于同一通信上下的包集合为逻辑流$F=\left\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N\right\}$,并在流粒度上计算统计行为特征:

$$\boldsymbol{z}_{\mathcal{F}}=\left[\mu_L,\sigma_L^2,H_L,r_{\text{burst}},\rho_{\text{auto}},T_{\text{dur}},\bar{\tau}\right] \tag{1}$$

其中:μ_L,σ_L^2,H_L分别表示包长序列的均值、方差与熵;r_{burst}为突发发送率;ρ_{auto}为时序自相关系数;T_{dur}为流持续时长;$\bar{\tau}$为平均到达间隔。为了在微观与宏观尺度间实现信息交互,流级上下文向量$\boldsymbol{z}_{\mathcal{F}}$被广播追加至该流内每个包的表征尾部。

在图像化特征通道中,原始字节流被完整保留并映射为二维灰度图像,其中像素值与字节的十进制取值一一对应,映射过程可形式化为

$$I_{m,n}=B_{(m-1)\times 28+n} \tag{2}$$

其中:$B_k\in[0,255]$表示第k个字节值。该过程表示将加密载荷的熵分布模式转化为空间纹理结构,使卷积神经网络$f_{\text{cnn}}(\cdot)$能够自动学习字节序列中的局部相关性与协议指纹残留特征,最终输出图像化特征向量$\boldsymbol{h}^{(i)}=f_{\text{cnn}}(I)$。这类特征对加密通道下的微小扰动高度敏感,尤其适用于检测伪装为正常通信的隐蔽攻击流。

最终,两个通道的高层特征$\boldsymbol{h}^{(s)}$与$\boldsymbol{h}^{(i)}$在全连接层前进行动态加权融合。为避免简单拼接导致的维度膨胀与信息冗余,引入轻量级权重函数$g(\cdot)$计算通道重要性权重:

$$\alpha_s=\frac{\exp\left(g(h^{(s)})\right)}{\exp\left(g\left(h^{(s)}\right)\right)+\exp\left(g\left(h^{(i)}\right)\right)} \tag{3}$$

并通过加权求和得到最终融合表征:

$$\boldsymbol{h}_{\text{fuse}}=\alpha_s h^{(s)}+\alpha_i h^{(i)} \tag{4}$$

该动态加权机制使模型在不同攻击场景下能够自适应地调整关注重点:当流量呈现显著时序异常时,模型强化流级统计特征;当通信表现出隐蔽字节模式时,则增强图像化表征的权重,从而实现全局最优的特征互补与信息增益。融合后的高维表征$\boldsymbol{h}_{\text{fuse}}$将输入后续分类头,完成加密恶意流量的端到端判别。

3.3 梯度协同

在模型的训练过程中,梯度协同机制被设计为双通道特征学习的核心协同引擎,其根本目标在于打破结构化通道与图像化通道之间的信息孤岛,实现跨模态的动态互指导与优化协同。该机制通过在反向传播阶段引入双向梯度信号交换,使任一通道的梯度更新不仅依赖自身预测误差,还能实时参考另一通道在相同输入样本上的特征表征与损失反馈,从而从根本上解决单一通道特征表达能力不足的瓶颈,构建起局部与全局表征间的闭环互补优化路径。

梯度协同在损失计算阶段同步触发:两个通道分别基于自身输出与真实标签计算独立损失L_{CNN}和L_{KAN}。为实现自适应的梯度贡献分配,本机制引入基于损失倒数的动态权重计算公式:

$$W_{\text{CNN}}=\frac{\frac{1}{L_{\text{CNN}}}}{\frac{1}{L_{\text{CNN}}}+\frac{1}{L_{\text{KAN}}}},\ W_{\text{KAN}}=\frac{\frac{1}{L_{\text{KAN}}}}{\frac{1}{L_{\text{CNN}}}+\frac{1}{L_{\text{KAN}}}} \tag{5}$$

其中:W_{CNN}表示图像化通道的自梯度权重,W_{KAN}表示结构化通道的自梯度权重。该权重设计确保损失较小的通道在当前迭代中具有更高的可信度,其自梯度信号在更新中占据主导;而损失较大的通道则更多接受来自对侧的指导梯度,以加速纠错与收敛。

各通道的最终更新梯度由自梯度与跨模态指导梯度加权合成,具体计算公式如下:

$$G_{\text{CNN}}=W_{\text{CNN}}G_{\text{CNN,self}}+\left(1-W_{\text{CNN}}\right)G_{\text{KAN}\to\text{CNN}} \tag{6}$$

$$G_{\text{KAN}}=W_{\text{KAN}}G_{\text{KAN,self}}+\left(1-W_{\text{KAN}}\right)G_{\text{CNN}\to\text{KAN}} \tag{7}$$

其中:$G_{\text{CNN,self}}$和$G_{\text{KAN,self}}$分别为CNN与KAN通道基于自身损失反向传播得到的原始自梯度;$G_{\text{KAN}\to\text{CNN}}$表示KAN通道对CNN参数的梯度指导,$G_{\text{CNN}\to\text{KAN}}$同理。该跨模态梯度通过在对侧损失上对本通道参数求导获得,承载了另一视角下的优化方向建议。

通过上述双向互馈机制,结构化通道能够借助图像化通道捕获的局部空间模式弥补时序建模中的细节缺失,而图像化通道则通过结构化通道的全局统计约束避免陷入局部噪声干扰。两个通道在训练过程中形成持续的正向强化循环,逐步构建起更加鲁棒、多层次的加密流量表征。梯度协同机制的引入不仅显著增强了双通道间的协作深度,更从优化层面重塑

了特征融合的有效性,最终实现模型对复杂加密攻击模式的高敏感性、高鲁棒性以及训练效率与检测性能的全面跃升。

3.4 梯度协同

本文的模型采用端到端的双通道并行处理框架,深度整合图像化特征通道与结构化特征通道,通过特征融合模块与梯度协同机制实现多尺度表征的动态耦合与协同优化。模型的设计核心在于全面挖掘加密流量在空间分布与时序行为两个正交维度上的多层次模式,从而构建对高隐蔽性恶意通信的鲁棒判别能力。

输入流量经预处理后分流进入两条平行路径:图像化通道将原始字节流映射为28×28灰度图像,送入轻量级CNN主干(由多层卷积-批归一化-ReLU-池化单元堆叠而成),自动提取局部字节模式、填充结构残留与协议指纹碎片等微观空间特征;结构化通道则将解析得到的包级与流级统计向量序列输入KAN网络,通过其符号化可解释基函数层动态建模长期时序依赖、流量节奏波动与全局统计异常。两通道在深层特征空间中经注意力引导的加权级联融合,生成统一的高维联合表征。

融合特征随即流入梯度协同优化模块。在每一训练批次中,CNN与KAN分别基于自身输出计算分类损失,并依据前述动态权重公式 W_{CNN} 与 W_{KAN} 实现双向梯度交换与加权聚合,形成最终的更新梯度流。该机制确保两通道在优化过程中互为参考、相互纠偏,最终通过全连接分类头输出恶意流量概率。

模型的整体训练流程采用联合端到端优化策略,分类损失采用交叉熵函数,优化器选用带权重衰减的Adam变体。得益于梯度协同的正则化效应,模型在训练中表现出更快的收敛速度与更强的抗过拟合能力。实验表明,本文的模型在ISCXVPN2016与ISCXTor2016等真实加密流量数据集上,相比单一通道基线与传统融合方法,在检测准确率、F1分数与误报率等关键指标上均取得显著提升,充分验证了双通道协同架构在加密恶意流量检测任务中的优越性。

4 实验

4.1 数据增强

本文基于ISCXVPN2016与ISCXTor2016两个真实加密流量数据集开展全面实验评估,数据涵盖主流应用类型的正常通信与多种隐蔽恶意行为,包括VPN隧道下的C&C通信、数据渗漏、恶意软件更新,以及Tor网络中的匿名攻击流量。原始数据以PCAP格式存储,包含完整的时间戳、五元组信息与加密载荷。为确保模型训练的有效性与特征表征的鲁棒性,所有原始流量在特征提取前均经过系统化的清洗、转换与增强处理。数据集的具体介绍如表1所示。

表1 数据集介绍

Table 1 Dataset description

数据集	服务	类别	样本数量
ISCX-VPN2016	Skype、Facebook、YouTube、Gmail、Hangouts等	BROWSING、CHAT、FILE-TRANSFER、MAIL、P2P、VOIP、Streaming	1.7×10^5
ISCXTor2016	浏览、邮件、聊天、流媒体、文件传输、VoIP等	AUDIO、BROWSING、CHAT、FILE-TRANSFER、MAIL、P2P、VIDEO、VOIP	1.15×10^5

首先执行数据清洗流程,遍历所有会话记录,剔除因捕获中断导致的残缺包或空载荷样本;对缺失字段(如部分IAT因超时未记录)统一填补为0;对出现无穷大(Infinity,INF)或非数值(Not a Number,NaN)的统计特征进行零值替换,确保后续数值计算的稳定性。同时,为避免IP地址字符串对模型的干扰,将源/目的IP统一转换为32位二进制整数向量(点分十进制→整数→二进制编码),既保留了地址的空间结构信息,又便于嵌入层学习潜在的网络拓扑模式。

随后进行标准化归一化处理,采用Min-Max归一化公式将所有连续型统计特征映射至[0,1]区间:

$$X_{\mathrm{normalized}}=\frac{X-X_{\min}}{X_{\max}-X_{\min}} \tag{8}$$

其中:X为原始特征值,$X_{\min}$和$X_{\max}$分别为该特征在训练集上的最小值与最大值。该操作有效抑制了量纲差异导致的梯度主导问题,确保包长度、IAT、字节总量等高动态范围特征不会压制低方差但高判别性的模式(如突发放包率、方向熵等),为双通道协同学习奠定均衡的特征基础。

为进一步提升模型对加密流量分布漂移的适应性,本文引入时序一致性数据增强策略。具体而言,在训练阶段对每个会话的PCAP序列施加以下增强操作:(1)随机时窗平移(在会话内滑动截取子序列,模拟攻击阶段性触发);(2)轻微包间隔扰动(在IAT上叠加高斯噪声$N(0,\sigma^2)$,σ自适应于原间隔均值);(3)字节填充变异(在载荷末尾随机追加0~16字节零填充,模拟协议填充策略差异)。这些增强手段在不破坏语义的前提下显著扩展了训练样本的多样性,增强了模型对加密通道下动态攻击模式的泛化能力。

4.2 数据增强

为真实模拟加密流量检测任务中标记数据极度稀缺的现实场景,本研究采用1:99极端不平衡划分策略将ISCXVPN2016与ISCXTor2016数据集划分为训练集与测试集,即仅1%样本用于监督训练,其余99%作为无标签测试集进行零样本泛化评估。该划分方式迫使模型在极少量标记指导下学习普适的加密行为表征,充分检验GFFNet在低监督、高泛化条件下的鲁棒性与迁移能力。

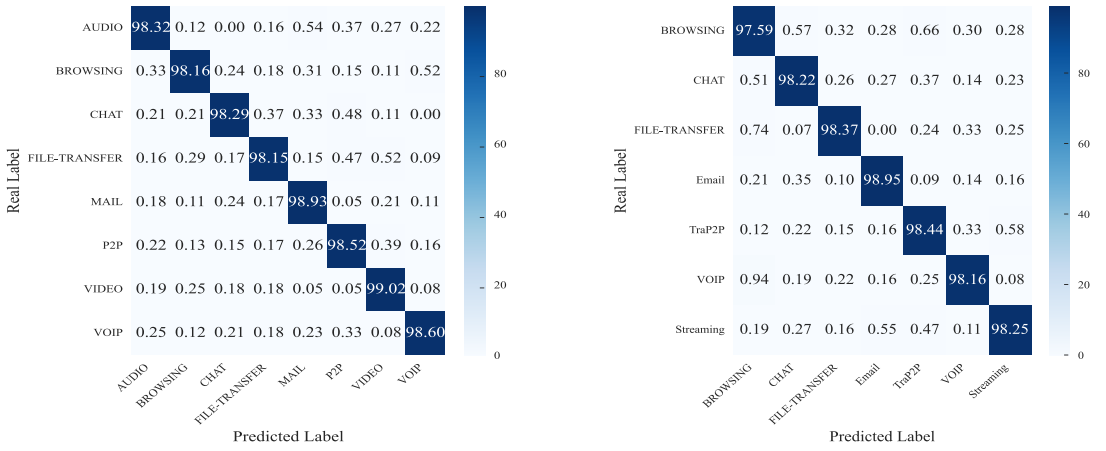
本文的模型由CNN图像化子网络与KAN结构化子网络双支并行构成,联合端到端优化。CNN子网络采用轻量级卷积主干,包含两层卷积-批归一化-ReLU激活单元(卷积核尺寸分别为5×5与3×3,通道数逐层扩增至32→64)与两层最大池化层(池化窗口2×2,步幅2),后接全局平均池化与全连接投影层,实现从28×28灰度流量图像到128维局部特征向量的端到端映射。优化器使用Adam,学习率固定为0.001,配合余弦退火调度策略动态衰减。

KAN子网络则以符号化可解释架构为核心,包含一层线性输入投影与一层非线性Kolmogorov-Arnold基函数层(基函数宽度设为3,网格区间自适应划分),将高维结构化统计特征(约80维)压缩并重构为128维全局语义表征,兼顾长期依赖建模与计算效率。KAN子网络采用独立Adam优化器,初始学习率设为0.000 5,以适应其对梯度尺度更敏感的训练动态。

双子网络通过前述特征融合模块与梯度协同机制实现深度耦合:融合特征维度为256维,分类头为两层MLP(256→128→2),输出恶意/正常二分类logits。整体模型训练采用联合交叉熵损失,在每个训练批次中同步计算L_{CNN}与L_{KAN},并依据动态权重公式执行梯度交换与参数更新。批量大小设为128,最大训练轮数100轮,提前停止阈值基于验证集F1分数(耐心值10)。所有实验在单张NVIDIA RTX 4060 GPU上完成,PyTorch框架实现。

4.3 实验结果

本文对提出的模型在不同数据集上的实验结果进行了分析。在ISCXTor2016数据集上,该模型的准确率(accuracy)达到98.73%,精确率(precision)为98.93%,召回率(recall)为98.22%,F1分数则为98.57%。同样,在ISCX-VPN2016数据集上,本文提出的模型也展现出优异性能,其准确率达98.45%,精确率为98.52%,召回率为98.22%,F1分数为98.37%。此外,本文还在一个加密数据集上对该模型进行了评估。为更直观地呈现结果,图2展示了本文提出的模型在两个数据集上的混淆矩阵,其中对角线数值代表正确分类结果,非对角线数值则代表错误分类结果。



(a) ISCXTor2016　　(b) ISCX-VPN2016

图2　混淆矩阵

Figure 2　Confusion matrix

这些混淆矩阵表明,本文提出的模型在多个数据集上均表现出色。这些可视化结果清晰反映出,该模型具备强大的区分能力,能够准确识别正常流量与各类网络威胁。值得注意的是,在大多数流量类别中,该模型的真阳性率都极高,尤其在检测恶意流量、Patator攻击、DDoS攻击、Heartbleed漏洞以及各类Web攻击时表现突出。这些结果进一步验证了该模型在网络威胁检测任务中的可靠性与高精度。

为全面体现本文的模型在该领域的竞争力,本文进一步将其与多种现有方法进行对比,并在相同数据集上对所有方法开展测试。通过实验对比,本文以图形形式呈现了该模型与这些方法在多个关键性能指

标上的结果。

首先，在 CICIDS-2018 数据集上，本文模型与 HDLNIDS 方法[30]、RCLN 方法[31]的性能进行了对比，结果如图 3 所示。如图所示，在 ISCXTor2016 数据集上，本文提出的模型的性能优于 HDLNIDS 和 RCLN 两种方法，在多个关键指标上均具备优势。这表明本文的模型能更高效地捕捉网络流量中的潜在特征，从而实现正常流量与恶意流量的精准区分。本文模型的优异性能不仅得益于其多级特征提取机制，还源于梯度共享机制的引入，该机制可在特征学习过程中促进模型内部子模型间的有效协同。在训练过程中我们观察到，与 HDLNIDS 和 RCLN 方法相比，本文模型的收敛速度显著更快。这是因为高效的梯度共享机制能在模型内部不同模块间有效传递梯度，进而实现稳定的优化过程。

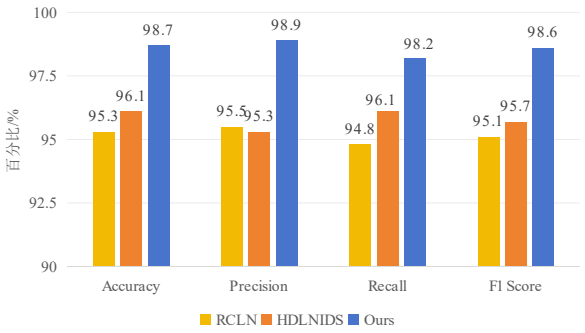


图 3 ISCXTor2016 数据集上三种模型的比较

Figure 3 Comparison of three models on the ISCXTor2016 dataset

接下来，本文探究模型在 ISCX-VPN2016 数据集上的性能表现，并将其与 Ning 等人[32]所引用的其他几种方法进行对比，结果如图 4 所示。本文的模型实现了显著更高的准确率，这进一步验证了其在不同场景下的鲁棒性与优异性能。

为进一步验证本文模型的广泛适用性，本文选取了一个加密流量数据集 ISCX-Tor2016。该数据集包含加密网络流量，对模型的识别能力构成了较大挑战。我们将 GLADS[33]方法和 CMFTC[34]方法进行了对比实验，结果如表 2 所示。

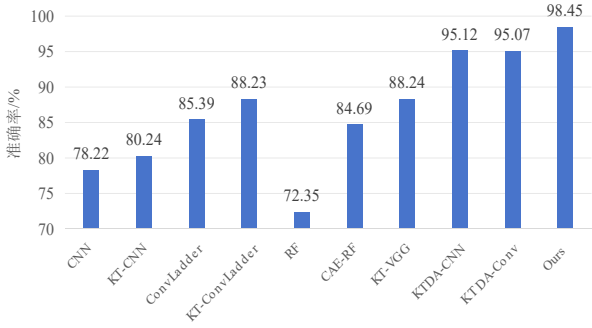


图 4 ISCXVPN2016 上各种方法准确率的比较

Figure 4 Comparison of accuracy of various methods on ISCXVPN2016

表 2 ISCX-Tor2016 数据集上的性能对比

Table 2 Performance comparison on the ISCX-Tor2016 dataset

Model	T2-Traffic Type (7-Class)	
	Accuracy/%	F1-score/%
Distiller[35]	96.82	72.94
1D-CNN[36]	96.34	71.46
2D-CNN[37]	96.40	75.71
MLP[38]	90.57	38.65
MLP[39]	95.54	64.50
HYBRID[40]	95.76	65.76
1D-CNN	96.34	71.46
GLADS[33]	97.95	86.77
CMFTC[34]	97.36	78.13
GFFNet(Ours)	98.70	98.60

4.4 消融实验

为进一步探究本文模型的核心模块对模型整体性能的贡献，本文设计了一些实验，对比了有无梯度共享机制和特征融合的情况。通过这些实验，观察各模块的必要性和有效性。消融实验结果如图 5 所示，对应以下六种模型配置：CNN 指仅使用 CNN 模块进行特征提取和训练，不包含梯度共享或特征融合的模型；KAN 指仅使用 KAN 模块进行特征提取和训练，不包含梯度共享或特征融合的模型；带特征融合的 CNN（CNN+Fusion）指在 CNN 基础上添加特征融合模块，并将融合后的特征送入 CNN 进行训练和分类的模型；带特征融合的 KAN（KAN+Fusion）指在 KAN 基础上添加特征融合模块的模型；CNN-KAN 指不对数据进行特征融合处理，直接将数据输入 CNN 和 KAN，且训练过程中两个子模型共享梯度的模型；GFFNet 指完整的 t 模型，包含梯度共享和特征融合两种机制。

从图 5 可以清晰地看出，不同模块的引入会产生特定影响。结果表明，传统的 CNN 和传统的 KAN 模型性能有限，准确率较低。然而，当添加特征融合模块后，准确率有明显提升。与单一特征相比，CNN 模型的准确率有所提升，KAN 模型的准确率也一样。此外，具有梯度共享机制的模型在协同训练准确率更高，但仅靠梯度共享机制不足以达到最优性能。在六种配置中，完整的模型表现最佳。这表明，梯度共享机制与特征融合机制的结合有效发挥了两者的协同优势。

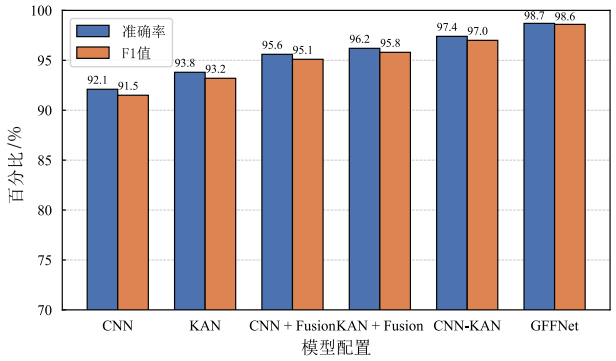


图5　消融实验

Figure 5　Ablation experiment

5　结束语

本文的模型在加密恶意流量检测任务中展现出显著的性能优势,尤其在VPN与Tor双重加密场景下实现了高精度、高鲁棒性的异常识别。其核心竞争力源于梯度协同机制与多尺度特征融合策略的深度耦合:CNN通道精准捕获字节空间中的局部扰动模式,KAN通道动态建模时序统计中的全局行为演化,二者通过基于损失倒数的动态加权梯度交换实现实时互指导与协同优化,有效打破了传统单模态方法在特征表达上的瓶颈。这种双向互馈学习范式不仅显著提升了模型对高隐蔽性攻击的敏感性,还充分满足了真实网络环境中标记数据稀缺的部署需求。

特征融合模块通过注意力引导的加权级联,进一步强化了局部与全局表征的互补性。在复杂多变的加密流量中,该模块能够自适应地聚焦于当前最具判别力的特征维度,例如在突发放包攻击中强化流级统计,在协议伪装场景中突出图像化纹理残留,从而确保模型在高动态、高噪声环境下的检测稳定性与精度,显著超越依赖固定规则或单一视角的传统方法。

尽管性能优异,本文的模型仍存在一定局限性。由于采用双子网络并行架构,训练过程受制于计算负载最重的通道,整体迭代时延较轻量单模型有所增加;同时,跨通道梯度交换虽提升了协作效率,但同步开销在超大批次训练中仍不可忽视。未来优化方向包括:(1)引入异步梯度更新策略,允许快通道先行迭代并缓存指导信号,减少等待瓶颈;(2)设计自适应计算分配机制,根据当前损失动态调整各通道的计算资源占比;(3)探索模型蒸馏与结构剪枝,在保持性能的前提下压缩推理延迟,以适配边缘设备部署。

综上,本文的模型通过创新的梯度协同与多模态融合范式,为加密恶意流量检测提供了高效、可解释、强泛化的解决方案。未来工作将在保持检测精度的同时,持续优化计算效率与资源占用,推动模型从实验室基准向实际网络安全系统的平滑迁移。

参考文献

[1] Ahn S, Yi H, Lee Y, et al. Hawkware: Network intrusion detection based on behavior analysis with ANNs on an IoT device[C]//2020 57th ACM/IEEE Design Automation Conference. Piscataway: IEEE, 2020: 1-6.

[2] Hameed S, Khan F I, Hameed B. Understanding security requirements and challenges in Internet of Things (IoT): A review[J]. Journal of Computer Networks and Communications, 2019, 2019: 9629381.

[3] Hinton G, Vinyals O, Dean J. Distilling the knowledge in a neural network[PP/OL]. V1. arXiv (2015-03-09)[2025-12-28]. https://doi.org/10.48550/arXiv.1503.02531.

[4] Liu Ziming, Wang Yixuan, Vaidya S, et al. KAN: Kolmogorov-arnold networks[C/OL]//International Conference on Learning Representations (ICLR). Vienna: 2024. https://proceedings.iclr.cc/paper_files/paper/2025/file/afaed89642ea100935e39d39a4da602c-Paper-Conference.pdf.

[5] Peng Zhiliang, Huang Wei, Gu Shanzhi, et al. Conformer: Local features coupling global representations for visual recognition[C]//2021 IEEE/CVF International Conference on Computer Vision. Piscataway: IEEE, 2021: 357-366.

[6] Ayo F E, Awotunde J B, Folorunso S O, et al. A genomic rule-based KNN model for fast flux botnet detection[J]. Egyptian Informatics Journal, 2023, 24(2): 313-325.

[7] 孙剑文, 张斌, 李红宇, 等. 自监督学习驱动的注意力增强恶意流量检测方法[J]. 网络与信息安全学报, 2025, 11(2): 136-151.
Sun Jianwen, Zhang Bin, Li Hongyu, et al. Harnessing self-supervised learning to boost malicious traffic detection with enhanced attention[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 136-151. (in Chinese)

[8] 马博文, 郭渊博, 马骏, 等. 基于后门攻击的恶意流量逃逸方法[J]. 通信学报, 2024, 45(4): 73-83.
Ma Bowen, Guo Yuanbo, Ma Jun, et al. Escape method of malicious traffic based on backdoor attack[J]. Journal on Communications, 2024, 45(4): 73-83. (in Chinese)

[9] Afzal R, Kumar Murugesan R. Rule-based anomaly detection model with stateful correlation enhancing mobile network security[J]. Intelligent Automation & Soft Computing, 2022, 31(3): 1825-1841.

[10] Uszko K, Kasprzyk M, Natkaniec M, et al. Rule-based system with machine learning support for detecting anomalies in 5G WLANs[J]. Electronics, 2023, 12(11): 2355.

[11] Berkay Celik Z, Walls R J, McDaniel P, et al. Malware traffic detection using tamper resistant features[C]// MILCOM 2015 - 2015 IEEE Military Communications Conference. Piscataway: IEEE, 2015: 330-335.

[12] Mao Qian, O'Neill C, Bao Ke. A feature-based network traffic classification approach[J]. International Journal of Network Security, 2023, 25(5): 821-828.

[13] 赵荻, 尹志超, 崔苏苏, 等. 基于图表示的恶意TLS流量检测方法[J]. 信息安全研究, 2024, 10(3): 209-215.
Zhao Di, Yin Zhichao, Cui Susu, et al. Malicious TLS traffic detection based on graph representation[J]. Journal of Information Security Research, 2024, 10(3): 209-215. (in Chinese)

[14] Fei Chao, Xia Nian, Tsai P W , et al. An effective feature selection algorithm for machine learning-based malicious traffic detection[C]//2024 19th Asia Joint Conference on Information Security. Piscataway: IEEE, 2024: 1-8.

[15] Ferriyan A, Thamrin A H, Takeda K, et al. Encrypted malicious traffic detection based on Word2Vec[J]. Electronics, 2022, 11(5): 679.

[16] 许小龙, 方子介, 齐连永, 等. 车联网边缘计算环境下基于深度强化学习的分布式服务卸载方法[J]. 计算机学报, 2021, 44(12): 2382-2405.
Xu Xiaolong, Fang Zijie, Qi Lianyong, et al. A deep reinforcement learning-based distributed service offloading method for edge computing empowered Internet of vehicles[J]. Chinese Journal of Computers, 2021, 44(12): 2382-2405. (in Chinese)

[17] 王承祥, 黄杰, 王海明, 等. 面向6G的无线通信信道特性分析与建模[J]. 物联网学报, 2020, 4(1): 19-32.
Wang Chengxiang, Huang Jie, Wang Haiming, et al. 6G oriented wireless communication channel characteristics analysis and modeling[J]. Chinese Journal on Internet of Things, 2020, 4(1): 19-32. (in Chinese)

[18] 唐博麟, 王晨飞, 江帆, 等. 基于网络流时空序列的加密流量分类[J]. 计算机应用与软件, 2024, 41(3): 297-302.
Tang Bolin, Wang Chenfei, Jiang Fan, et al. Encrypted traffic classification based on network flow time-space series[J]. Computer Applications and Software, 2024, 41(3): 297-302. (in Chinese)

[19] Han Ying, Wang Xinlei, He Mingshu, et al. Intrusion detection for encrypted flows using single feature based on graph integration theory[J]. IEEE Internet of Things Journal, 2024, 11(10): 17589-17601.

[20] Zhu Shizhou, Xu Xiaolong, Zhao Juan, et al. LKD-STNN: A lightweight malicious traffic detection method for Internet of Things based on knowledge distillation[J]. IEEE Internet of Things Journal, 2024, 11(4): 6438-6453.

[21] Zhou Xiaokang, Wu Jiayi, Liang Wei, et al. Reconstructed graph neural network with knowledge distillation for lightweight anomaly detection[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(9): 11817-11828.

[22] Lu Jiazhong, Wang Chenli, Huang Yuanyuan, et al. An adversarial example defense algorithm for intelligent driving[J]. IEEE Network, 2024, 38(6): 98-105.

[23] Huang Tao, You Shan, Wang Fei, et al. Knowledge distillation from a stronger teacher[C]//Proceedings of the 36th International Conference on Neural Information Processing Systems. New York: ACM, 2022: 33716-33727.

[24] 戚子健, 柳毅. 基于双向GRU和CNN的恶意网络流量检测方法[J]. 计算机应用与软件, 2024, 41(12): 334-340.
Qi Zijian, Liu Yi. Malicious network traffic detection method based on bidirectional gru and cnn[J]. Computer Applications and Software, 2024, 41(12): 334-340. (in Chinese)

[25] Lu Jiazhong, Chen Kai, Zhuo Zhongliu, et al. A temporal correlation and traffic analysis approach for APT attacks detection[J]. Cluster Computing, 2019, 22(S3): 7347-7358.

[26] Niu Ziwei, Yuan Junkun, Ma Xu, et al. Knowledge distillation-based domain-invariant representation learning for domain generalization[J]. IEEE Transactions on Multimedia, 2024, 26: 245-255.

[27] Yang Chuanguang, An Zhulin, Cai Linhang, et al. Knowledge distillation using hierarchical self-supervision augmented distribution[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(2): 2094-2108.

[28] Lu Jiazhong, Lan Jin, Huang Yuanyuan, et al. Anti-attack intrusion detection model based on MPNN and traffic spatiotemporal characteristics[J]. Journal of Grid Computing, 2023, 21(4): 60.

[29] Yang Jing, Zhu Xiatian, Bulat A, et al. Knowledge distillation meets open-set semi-supervised learning[J]. International Journal of Computer Vision, 2025, 133(1): 315-334.

[30] Qazi E U H, Faheem M H, Zia T. HDLNIDS: Hybrid deep-learning-based network intrusion detection system[J]. Applied Sciences, 2023, 13(8): 4921.

[31] Long Jing, Liang Wei, Li Kuanching, et al. A regularized cross-layer ladder network for intrusion detection in industrial Internet of Things[J]. IEEE Transactions on In-

dustrial Informatics, 2023, 19(2): 1747-1755.
[32] Ning Jinhui, Gui Guan, Wang Yu, et al. Malware traffic classification using domain adaptation and ladder network for secure industrial Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(18): 17058-17069.
[33] Dai Jianbang, Xu Xiaolong, Xiao Fu. GLADS: A global-local attention data selection model for multimodal multitask encrypted traffic classification of IoT[J]. Computer Networks, 2023, 225: 109652.
[34] Dai Jianbang, Xu Xiaolong, Gao Honghao, et al. CMFTC: Cross modality fusion efficient multitask encrypt traffic classification for efficient management of IIoT[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 3989-4009.
[35] Aceto G, Ciuonzo D, Montieri A, et al. DISTILLER: Encrypted traffic classification via multimodal multitask deep learning[J]. Journal of Network and Computer Applications, 2021, 183: 102985.
[36] Wang Wei, Zhu Ming, Wang Jinlin, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//2017 IEEE International Conference on Intelligence and Security Informatics. Piscataway: IEEE, 2017: 43-48.
[37] Huang He, Deng Haojiang, Chen Jun, et al. Automatic multi-task learning system for abnormal network traffic detection[J]. International Journal of Emerging Technologies in Learning (IJET), 2018, 13(4): 4-20.
[38] Zhao Ying, Chen Junjun, Wu Di, et al. Multi-task network anomaly detection using federated learning[C]//Proceedings of the 10th International Symposium on Information and Communication Technology. New York: ACM, 2019: 273-279.
[39] Sun Haifeng, Xiao Yunming, Wang Jing, et al. Common knowledge based and one-shot learning enabled multi-task traffic classification[J]. IEEE Access, 2019, 7: 39485-39495.
[40] Lopez-Martin M, Carro B, Sanchez-Esguevillas A, et al. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things[J]. IEEE Access, 2017, 5: 18042-18050.

作者简介

卢嘉中　男，1988年7月生，四川成都人。成都信息工程大学副教授。发表SCI论文30余篇，发明专利6项，出版网络安全专著2本，撰写网络安全研究报告4份。长期从事网络攻击检测与溯源、网络舆情分析方面的研究工作。
E-mail: ljz@cuit.edu.cn

余　坤　男，1992年7月生，山西大同人。成都信息工程大学硕士研究生。主要从事网络攻击检测、恶意流量识别、日志异常检测方向的研究。
E-mail: 3230809006@stu.cuit.edu.cn

刘小垒　男，1996年9月生，江苏盐城人。国家工程物理交叉科学研究中心副研究员。长期从事面向装备智能系统的可信人工智能、网络与数据安全等方面的研究工作。中国电子学会会员编号：E190037480S。
E-mail: luxaole@gmail.com

张小松　男，1968年6月生，四川成都人。电子科技大学教授、博导。以第一完成人获2019年度国家科技进步奖一等奖、2012年度国家科技进步奖二等奖。长期从事网络安全方面的研究工作。中国电子学会会员编号E190018142F。
E-mail: johnsonzxs@uestc.edu.cn