面向网络流量异常检测的频谱感知图预训练与提示微调框架

罗海桐[1,2],张蔚瑶[1],林纯钢[1,2],孟绪颖[1,3],张玉军[1,4,5*]

(1. 中国科学院计算技术研究所,北京 100190;2. 中国科学院大学,北京 100190;3. 紫金山实验室,江苏南京 211111;
4. 中科南京信息高铁研究院,江苏南京 210008;5. 中国科学院大学南京学院,江苏南京 211135)

摘 要: 随着网络技术的演进,流量规模呈指数级增长,攻击手段(如协议混淆、跳跃连接等)日益隐蔽复杂,传统检测方法已难以应对。尽管图神经网络(Graph Neural Networks,GNNs)在建模流量拓扑依赖方面展现出潜力,但在现实网络安全场景中,普遍存在两大瓶颈:一是网络流量图显著的结构异配性,即异常流量倾向于与特征迥异的正常节点建立非典型连接,导致基于同配性假设的图神经网络失效;二是高质量异常标签极度稀缺,全参数微调易引发过拟合或知识负迁移。为此,本文提出一种面向网络流量异常检测的频谱感知图预训练与提示微调框架。该框架摒弃了传统图学习对同配结构与大量标签的依赖,其核心创新在于:(1)引入互补的频谱滤波器组,首次将捕捉稳定通信模式的低通信号与识别异常连接扰动的高通信号进行联合建模,从频域视角精准刻画流量的异配结构;(2)设计频谱感知的对比学习机制,通过最大化跨频域视图的表示一致性,在预训练阶段提取鲁棒的频率不变特征;(3)提出参数高效的提示微调策略,在冻结主干参数的前提下,利用可学习的提示向量自适应调节高低频通道的融合权重,实现向少样本下游任务的精准迁移。在 CICIDS2017、CICIDS2018 及 HIKARI2021 三个真实数据集上的实验表明,该方法在少样本场景下的检测性能全面优于现有基准模型,最高提升幅度超 20%,验证了其在复杂异配网络环境中的鲁棒性与实用性。

关键词: 网络异常检测;图神经网络;预训练;频谱图滤波器;提示微调;流量检测

基金项目: 国家自然科学基金(No.U24B600013,No.62372429)

中图分类号: TP393.0 **文献标识码:** A **文章编号:** 0372-2112(2026)01-0167-16

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250576

Spectral-Aware Graph Pre-training and Prompt Tuning Framework for Network Traffic Anomaly Detection

LUO Haitong[1,2], ZHANG Weiyao[1], LIN Chungang[1,2], MENG Xuying[1,3], ZHANG Yujun[1,4,5*]

(1. *Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*;
2. *University of Chinese Academy of Sciences*, *Beijing* 100190, *China*;
3. *Purple Mountain Laboratory*, *Nanjing*, *Jiangsu* 211111, *China*;
4. *Nanjing Institute of InforSuperBah*, *Nanjing*, *Jiangsu* 210008, *China*;
5. *University of Chinese Academy of Sciences*, *Nanjing*, *Nanjing*, *Jiangsu* 211135, *China*)

Abstract: With the evolution of network technologies, the scale of network traffic has grown exponentially, and attack methods (such as protocol obfuscation and skipping connections) have become increasingly covert and complex, posing unprecedented challenges to traditional detection methods. Although graph neural networks (GNNs) have demonstrated potential in modeling traffic topological dependencies, they generally face two major bottlenecks in real-world network security scenarios: first, the significant structural heterophily in network traffic graphs, where anomalous traffic tends to establish atypical connections with normal nodes possessing vastly different features, causing GNNs based on homophily assumptions to fail; second, the extreme scarcity of high-quality anomaly labels, where full-parameter fine-tuning easily induces overfitting or the negative transfer of pre-trained knowledge. To this end, this paper proposes a spectral-aware graph pre-training and prompt tuning framework tailored for network traffic anomaly detection. Abandoning the reliance of traditional graph learning paradigms on homophilic structures and massive labeled data, the core innovations of this framework lie in: (1) Introducing complementary spectral filters to jointly model low-pass signals (capturing stable communication patterns) and high-pass signals (identifying abnormal connection perturbations) for the first time during the pre-training phase, accu-

收稿日期:2025-06-30;录用日期:2025-12-26;责任编辑:覃怀银

*通信作者:张玉军

rately characterizing the strong heterophilic nature of network traffic from a frequency domain perspective; (2) Designing a spectral-aware contrastive learning mechanism to extract robust frequency-invariant features by maximizing representational consistency across cross-frequency views; (3) Proposing a parameter-efficient prompt tuning strategy that, while freezing backbone parameters, utilizes learnable prompt vectors to adaptively adjust the fusion weights of high- and low-frequency channels, achieving precise transfer to downstream few-shot tasks. Experiments on three real-world network security datasets, including CICIDS2017, CICIDS2018, and HIKARI2021, demonstrate that the proposed method comprehensively outperforms existing baseline models in detection performance under sample-scarce scenarios. With a maximum improvement exceeding 20%, these results verify the robustness and practicality of the proposed method in complex and heterophilic network environments.

Keywords: network anomaly detection; graph neural networks; pre-training; spectral graph filters; prompt tuning; traffic classification

Foundation Item(s): National Natural Science Foundation of China (No.U24B600013, No.62372429)

0 引言

在现代信息系统中,网络已成为联接基础设施、终端设备与各类服务的重要枢纽。随着云计算、物联网和智能设备的普及,网络流量规模呈指数级增长[1],随之而来的安全威胁也愈发复杂。现实中,各类异常攻击(如命令与控制通信、横向移动、数据渗漏等)频繁出现,常通过协议混淆、低频访问、跳跃连接等策略绕过传统规则检测[2-3]。这些攻击往往不再具有明显的特征模式,而是表现为结构扰动与行为偏离的复合形式,显著提升了检测难度。同时,实际部署环境中高质量标注数据极其稀缺:一方面,新型攻击方式不断演化,人工标注难以及时覆盖其多样性;另一方面,异常样本在整体网络流量中比例极低,导致严重的数据不平衡问题[4-5]。在此背景下,如何在有限标签资源下挖掘网络流量中的潜在结构信息,构建具备鲁棒性与泛化能力的检测模型,成为网络安全研究的核心问题之一。

近年来,图神经网络(Graph Neural Networks, GNNs)[6-7]因其对复杂结构关系的建模能力,被广泛应用于网络流量异常检测。将每条网络流量抽象为图中的一个节点,不同流量之间的通信关系构成边,使得模型能够基于图结构学习行为关联。然而,这类方法普遍依赖大量高质量标注数据进行训练,在面对标签稀缺、攻击演化快速的现实场景时,模型泛化能力有限,迁移性与鲁棒性不足。为应对这一挑战,受自然语言处理领域范式转移的启发,一种图预训练(Graph Pre-training)[8-10]与提示微调(Prompt Tuning)[11-14]构成的新型图学习范式逐渐兴起。

提示微调技术的核心旨在解决传统“预训练-微调(Pre-training, Fine-tuning)”范式中存在的瓶颈。传统微调通常需要针对下游任务调整模型全部参数,这不仅计算成本高昂,且当预训练任务(如掩码重建)与下游任务(如异常分类)目标不一致时,在下游标注样本极度稀缺的场景下,极易因过拟合导致预训练知识的“负迁移”或灾难性遗忘[11]。相比之下,提示微调通过引入轻量级的可学习向量(即“提示向量”),将下游任务重构为与预训练任务形式一致的目标。这种机制在冻结预训练主干参数的前提下,有效弥合了目标差异,且由于仅需优化极少量参数,显著降低了模型对大规模标注数据的依赖。因此,即便在仅有少量样本的条件下,该范式也能激活预训练阶段习得的通用结构知识,实现向特定检测任务的高效迁移。随着该技术从自然语言处理向图学习领域的成功扩展,这一范式凭借卓越的参数效率与在少样本场景下强劲的泛化潜力,为解决网络流量异常检测中的数据匮乏问题提供了突破性的新思路。

然而,现有“图预训练+提示微调”范式在应用于网络流量异常检测任务时,面临显著的适配难题。这一范式多数构建在图的同配性(homophily)假设之上[15-17],即认为图中相邻节点在语义上应具有相似的属性或标签,邻接结构所蕴含的上下文关系有助于学习更具判别性的节点表示。这一假设在社交网络、推荐系统等场景中成立,但在网络流量图中却难以满足。在以流量为节点的图建模方式下,正常流量节点通常围绕协议、端口、方向等属性聚集,具有稳定的局部相似性;而异常流量节点由于其刻意规避检测的行为特征,与大量正常节点构成非典型连接,其属性与邻居之间往往存在显著差异,表现出强异配性(heterophily)结构特征。在这种异配背景下,传统基于同配性构建的自监督任务(如邻居一致性建模、上下文特征预测)在预训练阶段难以捕捉异常流量的行为模式;而在提示微调阶段,模型往往沿袭预训练的同配性偏置,在下游任务中也难以有效调整对这类异常流量的表征能力,限制了整体模型的检测性能[15]。

已有研究表明[16,18-19],图结构中的异配性特征可以通过频域视角加以刻画:邻居节点的相似性通常反映在图信号的低频成分中,而节点间的结构突变与差

异性则主要由高频分量承载。这种频域视角赋予了模型进行频谱感知的潜力:即将图结构数据视为信号,其中低频分量对应图中平滑、相似的结构(如同配性下的正常通信),而高频分量则对应图中剧烈变化、差异化的部分(如异配性下的异常连接)。因此,一个有效的异常检测模型必须能够敏锐地感知并区分这两种信号。基于此洞见,本文提出一种面向网络流量异常检测的频谱感知图学习框架 NetGPrompt(Network traffic Graph Prompt tuning),旨在利用该原理突破异配结构建模与低标签条件下的适应性瓶颈。

首先,为精准建模网络流量图中的异配性,NetGPrompt 引入一对互补的频谱滤波器:低通滤波器用于捕捉正常流量节点之间稳定一致的低频连接结构,高通滤波器则用于识别异常流量引发的高频突变与非典型连接,实现对同配与异配结构特征的联合建模。

其次,在预训练阶段,本文构建了一种基于频谱通道的对比学习机制,将同一节点在高低频通道下的表示作为正样本,不同节点间的跨频表示作为负样本,驱动模型在无标签条件下学习频率敏感且鲁棒的结构嵌入,增强对潜在异常连接的区分能力。

最后,在提示微调阶段,本文为每个频率通道引入独立的可学习提示向量,动态调节高低频通道的融合权重。该机制在主干模型参数冻结的前提下,支持结构自适应通道选择与参数高效迁移,尤其适用于异常样本稀缺的检测任务。

综上,NetGPrompt 通过频域建模与提示引导机制协同作用,有效缓解了现有范式在异配结构与标签稀缺场景下的性能瓶颈。实验结果表明,在 CICIDS2017、CICIDS2018 和 HIKARI2021 三个真实网络异常检测数据集上,NetGPrompt 的检测性能均显著优于现有方法,最高提升超 20%,展现出广泛的实用价值与推广潜力。

1　相关工作

1.1　网络流量异常检测

网络流量异常检测作为保障网络安全的关键手段,经历了从基于专家规则的方法到基于数据驱动的模型演进。早期检测系统[20]依赖于人工规则和已知攻击签名,虽然具有高精度和可解释性,但难以应对快速演化的攻击和变种。为提升通用性,研究者引入了基于机器学习的方法[21-25],如支持向量机(Support Vector Machine, SVM)[23]、决策树(Decision Tree, DT)[24]、K-近邻(K-Nearest Neighbor, KNN)[25]等,通过提取流量统计特征进行分类。这些方法在特定环境中取得一定成效,但通常依赖特征工程,泛化能力弱,且无法建模时空依赖关系。

近年来,深度学习方法逐渐被用于异常检测任务[26-28],尤其是循环神经网络(Recurrent Neural Network, RNN)[26]、卷积神经网络(Convolutional Neural Network, CNN)[27]和自动编码器(AutoEncoder, AE)[28]等结构,可自动学习高阶特征并建模流量的时间动态。然而,这些模型多数将流量视作独立样本处理,忽略了流量之间潜在的交互关系和拓扑结构,难以挖掘攻击中的结构模式。例如,控制服务器与被控主机之间的异常连接往往构成图中关键的攻击路径,这种拓扑信息在传统模型中常被忽略。

因此,越来越多研究开始尝试将网络流量建模为图结构[29-31],引入图神经网络进行结构感知的异常检测。但现有方法仍多基于同配性图结构建模[17],仅利用样本之间的相似性,缺乏对异常样本的专门建模能力,这是本研究所关注的关键问题。

1.2　图神经网络

GNNs 近年来成为图结构数据建模的主流方法,广泛应用于社交网络分析、推荐系统、蛋白质预测等领域。代表性模型如图卷积网络(Graph Convolutional Networks, GCN)[6]通过频域近似完成邻居聚合,图注意力网络(Graph ATtention network, GAT)[7]引入注意力机制实现节点间关系的自适应建模,图采样聚合网络(Graph Sample and AggreGatE, GraphSAGE)[32]设计归纳式采样策略,提升了大规模图学习的扩展性。

然而,将 GNN 应用于异常检测任务中仍面临关键挑战[17]。异常行为在图中往往呈现出离散、稀疏、边缘化的结构特征,且与正常行为的连接方式存在显著差异,这种异质连接结构常表现为“异配性”(heterophily)——即异常节点连接的邻居节点在语义上并不相似。此时,传统 GNN 的同配性假设将导致错误的信息传播,甚至掩盖关键异常模式[18,33]。

为缓解这一问题,研究者提出了多阶聚合[24]、自适应特征增强[18]等策略,从不同尺度刻画图结构的异质性;亦有工作[17,34]以频域视角引入多频谱滤波器,联合建模同配与异配信号。然而,这些方法普遍依赖大量有监督标注,在异常检测这类标签极其稀缺的场景下其有效性受到严重限制,凸显了开发适用于低资源、异配环境的新型图学习范式的必要性。

1.3　图预训练和提示微调

传统图神经网络通常依赖大量高质量的有监督数据进行训练,当标注数据稀缺时,模型的泛化能力与鲁棒性显著下降。为缓解这一问题,近年来研究者开始探索图预训练与提示微调相结合的新型图学习范式,以提升模型在低资源场景下的迁移能力与结构适应性。

图预训练的核心思想是在大规模无标签图上通过自监督任务学习通用的结构表示,并将其迁移至下游任务进行轻量调优。代表性方法包括深度图信息最大化方法(Deep Graph Infomax,DGI)[8]、图对比学习方法(Graph Contrastive Learning,GraphCL)[9],它们通常基于同配性假设设计对比学习或互信息最大化目标,以增强局部结构与全局语义的一致性。然而,这类方法普遍偏向保留图信号的低频成分,难以有效建模结构突变、异常连接等高频特征,限制了其在如异常检测等高频敏感任务中的适用性。

另一方面,传统图预训练模型在迁移阶段多采用全参数微调(fine-tuning),这在K-shot或极少样本设定下容易导致过拟合与知识遗忘问题[11]。为提升参数效率与任务适应性,提出提示微调作为一种高效微调策略。该方法通过引入少量可学习提示向量,引导冻结主干模型激活已有知识,实现任务特定调优。提示学习最初应用于语言模型[35-37],近年来逐渐扩展至图领域,典型方法如图提示方法(Graph Prompt,GPrompt)[11]、图预训练和提示微调方法(Graph Pre-training and Prompt Tuning,GPPT)[14]和图提示特征方法(Graph Prompt Feature plus,GPF-plus)[13],它们通过图级或子图级提示引导模型统一适应不同图任务,显著提升了迁移效率与泛化能力。尽管上述方法在同配结构任务中表现出色,但普遍缺乏对图频谱特性的显式建模,尤其在处理异配性结构时存在鲁棒性不足的问题。

因此,本文提出的NetGPrompt方法系统性整合了频谱感知的图预训练与结构提示调优机制,旨在解决现有范式对图频谱特性建模不足,尤其是在处理异配结构时鲁棒性差的问题。在预训练阶段,NetGPrompt引入高/低通滤波器构建互补的频谱视图,设计节点级对比学习任务以同时捕捉低频稳定结构与高频异常结构特征,实现频域不变性建模;在提示微调阶段,模型在主干参数冻结的前提下引入提示向量对不同频率通道进行门控融合,支持任务感知的结构适配与高效迁移。实验验证表明,该方法显著缓解了异配结构与标签稀缺带来的迁移瓶颈,提升了模型对高异配性的非典型连接模式的检测能力。

1.4 频域图神经网络

频域分析作为一种强大的理论工具,在通信等信号处理领域[38-40]已被广泛应用并取得了巨大成功。受此启发,研究者将这一思想从规则的欧几里得数据推广到了结构更为复杂的图数据上,形成了图信号处理(Graph Signal Processing,GSP)这一前沿领域。与传统信号的傅里叶变换类似,图信号处理[41]也定义了图上的“频率”。具体而言,图的“频谱”源于拉普拉斯矩阵的特征值分解。该矩阵是图拓扑结构的代数表示,其特征值构成了图频谱中的频率。其中,较小的特征值对应图上的低频分量,代表着信号在图中变化平缓、局部相似的区域(同配性);而较大的特征值则对应高频分量,代表信号变化剧烈、存在局部突变或差异的区域(异配性)。

基于该理论,频域图神经网络(Spectral Graph Neural Networks,Spectral GNNs)应运而生。早期的代表性工作如GCN[6],其核心思想便是对频域上的图卷积操作进行近似,从而在空间域上实现高效的邻居特征聚合,这在本质上是一种低通滤波操作。这种设计在处理同配性图时表现出色,但同时也限制了模型捕捉高频信息的能力。为了克服这一局限性,后续工作致力于设计更具表达能力的频谱滤波器。例如,小波变换图神经网络(Beta Wavelet Graph Neural Network,BWGNN)[17]专门为异常检测任务设计了高通/带通滤波器,以直接提取图中的高频异常信号。多项式图对比学习(Polynomial Graph Contrastive Learning,PolyGCL)[16]则利用多项式滤波器生成互补的低通与高通视图,用于图的自监督对比学习。

这些研究充分证明了频域分析在建模复杂图结构时的巨大潜力。然而,如何将这些强大的频谱建模能力与“预训练+提示微调”这一新兴的参数高效范式相结合,以解决标签稀缺场景下的网络异常检测问题,仍是一个有待探索的方向。本文提出的NetGPrompt正是为了弥补这一空白,通过设计频谱感知的预训练和提示机制,旨在实现对网络流量图结构的高效、鲁棒建模。

2 本文方法

为应对网络流量异常检测中常见的结构异配性强、频谱差异显著、标注稀缺等挑战,本文提出一种融合频谱建模与提示微调机制的图异常检测框架——NetGPrompt。该方法利用高低通滤波器建模不同频域特征,通过频谱感知的预训练学习多频段结构特征,并在微调阶段引入提示向量,实现参数高效的任务适应性调节,从而提升模型在多种异常类型下的泛化能力。整体架构如图1所示,核心呈现三模块联动逻辑:输入为网络流量图(节点代表单条流量,边依据流量间通信关联构建);左侧通过高低通滤波器分别提取正常流量的低频表征与异常流量的高频表征,解决结构异配性问题;上方通过跨频域正负样本对比学习完成频谱预训练,缓解标注稀缺;下方引入提示向量自适应融合频谱通道,冻结主干参数实现高效微调,最终经分类器输出异常检测结果。

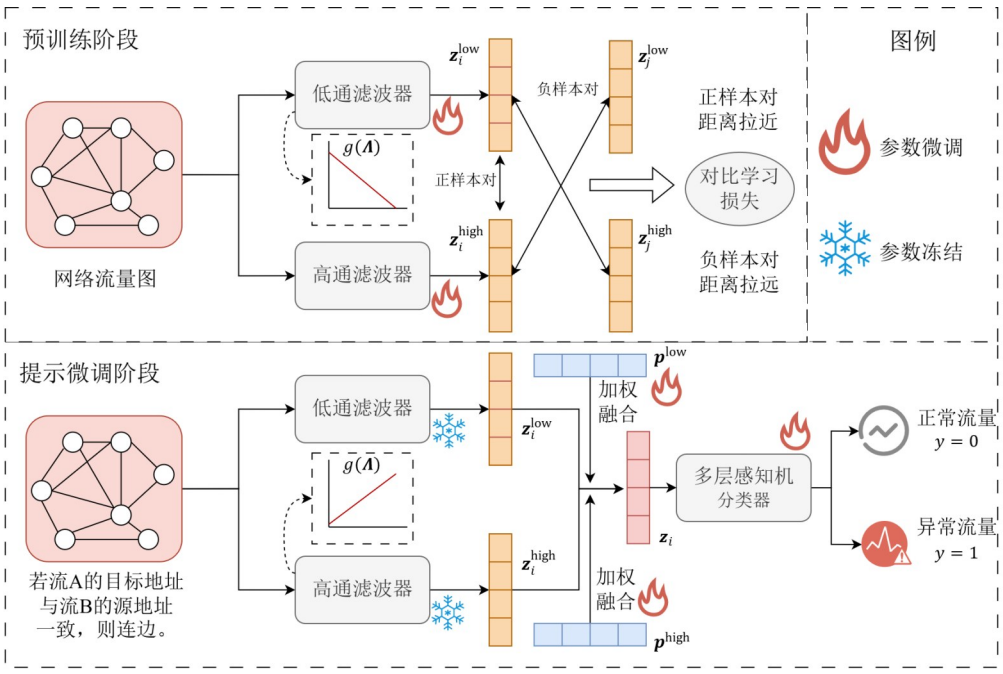


图 1　模型总体框架图

Figure 1　Overall framework of the model

2.1　问题建模与图构建

2.1.1　图构建

在实际网络安全场景中,原始网络流记录通常包括源/目的 IP(Internet Protocol)和端口、协议类型、连接持续时间、数据传输字节数等统计信息。本文将每条网络流表示为一个图节点,若两条流之间存在通信路径,则在其间建立连边。具体而言,设图 $G=(V,E)$ 表示网络流量图,节点集合 $V=\{v_1,v_2,\cdots,v_N,\}$ 表示 N 条网络流,每条流的特征 $\boldsymbol{x}_i$ 为其统计特征,组成特征矩阵为 $\boldsymbol{X}\in\mathbb{R}^{N\times d}$。在本文中,图中边 E 的构造遵循以下规则:若一条网络流 v_i 的目的 IP 地址与端口与另一条流 v_j 的源 IP 地址与端口相同,则认为这两条流之间存在通信关联,从而在图中建立 v_i 和 v_j 的边 e_{ij}。该构图策略可有效建模流之间的联动关系,有助于挖掘潜在的攻击链和异常传播路径。

2.1.2　问题建模

本文聚焦于二分类检测任务,即将所有异常类别统一建模为“异常”,与正常流量区分。由于异常流与正常流存在特征差异且存在连接,导致图结构呈现显著的异配性,即相邻节点特征或标签差异较大。传统基于同配性假设的 GNN 方法在此场景下常常失效,表现为表示退化与泛化能力差。

为解决上述挑战,本文引入图的“预训练与提示微调(Pre-training and Prompt Tuning)”学习范式,并将其应用于少样本(K-shot)网络异常检测任务中。本文采用以下两阶段优化流程:第一阶段预训练阶段,在大量无标签网络流图上设计自监督任务,预训练出具备丰富频谱知识的图表示模型 F_{θ^*};第二阶段提示微调阶段,在下游任务中,引入可学习的结构提示机制 P_ω,在冻结编码器参数的基础上实现结构感知的轻量微调。最终优化目标为

$$\omega^*=\arg\min_\omega L_{\text{down}}\left(F_{\theta^*}\left(P_\omega(G)\right)\right) \tag{1}$$

其中,L_{down} 表示下游节点分类的监督损失函数。在 K-shot 设定下,每个类别(正常或异常)仅提供少量(如 K 个)标注节点作为训练样本,显著提升了方法在标注稀缺与结构异配场景下的应用价值。通过将提示调优机制与频域建模相结合,本文提出的方法能够在复杂网络结构中实现结构敏感的迁移学习,提升少样本异常检测的准确性与稳健性。

2.2　频谱图滤波器设计

2.2.1　图频域建模理论基础

在图神经网络中,图卷积操作本质上可视为图拉普拉斯特征空间中的频域滤波过程[19]。将这一理论应用于网络流量图,是实现“频谱感知”的第一步。为适应图中复杂的拓扑特征与多变异常模式,如图 1 所示,NetGPrompt 框架构建了两个互补的图频域滤波器:低通滤波器用于提取同配性结构(如正常通信稳定拓扑),高通滤波器则用于捕捉异配性结构(如异常连接与攻击行为),它将抽象的频谱概念转化为了可操作的计算模块。

频谱图滤波器是图神经网络中建模节点关系的关键工具,其核心思想是通过图结构谱分解在频域设

计滤波器，实现对图信号低频、带通或高频成分的选择性提取。给定图 $G=(V,E)$，其邻接矩阵为 $\boldsymbol{A}\in\mathbb{R}^{N\times N}$，度矩阵为 $\boldsymbol{D}\in\mathbb{R}^{N\times N}$，归一化拉普拉斯矩阵定义为 $\boldsymbol{L}=\boldsymbol{I}-\boldsymbol{D}^{-1/2}\boldsymbol{A}\boldsymbol{D}^{-1/2}$，其中 $\boldsymbol{I}$ 为单位矩阵。拉普拉斯矩阵特征分解形式为 $\boldsymbol{L}=\boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^{\mathrm{T}}$，其中 $\boldsymbol{U}=[\boldsymbol{u}_1\,\boldsymbol{u}_2\cdots\boldsymbol{u}_N]$ 为正交特征向量矩阵，$\boldsymbol{\Lambda}=\mathrm{diag}(\lambda_1,\lambda_2,\cdots,\lambda_N)$ 为特征值对角矩阵，特征值 $\lambda\in[0,2]$ 表征频率特性，值越小频率越低。原始特征可通过傅里叶变换映射为频域特征信号 $\hat{\boldsymbol{X}}=\boldsymbol{U}^{\mathrm{T}}\boldsymbol{X}$。频谱滤波器的目标是在频域上对图信号进行加权处理，其一般形式为

$$\boldsymbol{Z}=g(\boldsymbol{L})\boldsymbol{X}=\boldsymbol{U}g(\boldsymbol{\Lambda})\boldsymbol{U}^{\mathrm{T}}\boldsymbol{X} \tag{2}$$

其中，$g(\boldsymbol{\Lambda})$ 表示对频率响应的滤波函数，可以设计为低通、高通或带通形式，以调控模型对不同频率分量的敏感性。例如，低通滤波器倾向于保留低频信号，即局部结构相似性，适用于同配图；而高通滤波器则突出高频信息，更适用于识别局部突变，如异配连接节点。

已有研究[41]证明频域滤波与空间域卷积存在等价转换关系，当 $\boldsymbol{C}$ 表示空间域卷积核时，满足：

$$\boldsymbol{Z}=\boldsymbol{C}\boldsymbol{X},\quad \boldsymbol{C}=\boldsymbol{U}g(\boldsymbol{\Lambda})\boldsymbol{U}^{\mathrm{T}} \tag{3}$$

在网络流量图中，异常流与正常流的特征差异导致图中同时存在局部相似性与局部差异性。单一的低频滤波器（如传统 GCN）往往无法有效捕捉到这些高频突变信号。因此，设计具备多频段响应能力的混合频域滤波器，成为建模网络异常行为的重要手段。

2.2.2 频域滤波器设计

为平衡计算效率与表征能力，受相关研究[19]启发，本文使用线性函数定义两个频域响应函数 $g_{\mathrm{low}}(\boldsymbol{\Lambda})$ 和 $g_{\mathrm{high}}(\boldsymbol{\Lambda})$ 分别构建低频与高频滤波器，并在实验部分对不同频域响应函数的兼容性进行分析。其中，低通滤波器保留图上变化缓慢的低频信号（如相似节点一致行为），采用线性衰减函数：

$$g_{\mathrm{low}}(\boldsymbol{\Lambda})=1-\frac{\lambda}{2} \tag{4}$$

该函数在 $\lambda=0$ 处响应最强，在 $\lambda=2$ 处趋于零，适合用于提取同配结构。该低通滤波器对应空间域操作等价于：

$$\boldsymbol{C}_{\mathrm{low}}=\frac{(\tilde{\boldsymbol{A}}+\boldsymbol{I})}{2} \tag{5}$$

其中，$\tilde{\boldsymbol{A}}=\boldsymbol{D}^{-1/2}\boldsymbol{A}\boldsymbol{D}^{-1/2}$，表明低通滤波器在邻居信息聚合时倾向提取相似特征。

与低通滤波器相反，高通滤波器放大信号在邻居之间的差异，即突出结构中的突变与不一致性。本文采用如下线性递增的频率响应函数：

$$g_{\mathrm{high}}(\boldsymbol{\Lambda})=\frac{\lambda}{2} \tag{6}$$

该函数在 $\lambda=0$ 处响应最弱，在 $\lambda=2$ 处响应最强，专注于放大高频成分并抑制平滑结构。其对应的空间域实现为

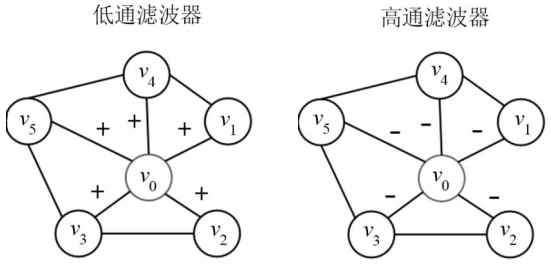
$$\boldsymbol{C}_{\mathrm{high}}=\frac{(\boldsymbol{I}-\tilde{\boldsymbol{A}})}{2} \tag{7}$$

该操作强调局部连接结构“跳变”，在邻域信息聚合时突出节点与邻居差异。

低通与高通滤波器的空域卷积效果如图 2 所示，以节点 v_0 为例，边上的正负号代表在聚合时对邻居节点特征的是加和还是相减。从图 2 可以看出，低通滤波器在聚合节点 v_0 的邻域信息时，会聚合其邻域信息均值，而高通滤波器在聚合其邻域信息时，会聚合节点与邻居的差值。通过双滤波器设计，NetGPrompt 分别得到低频和高频的表征：

$$\boldsymbol{Z}^{\mathrm{low}}=g_{\mathrm{low}}(\boldsymbol{L})\boldsymbol{X}\boldsymbol{W}^{\mathrm{low}},\quad \boldsymbol{Z}^{\mathrm{high}}=g_{\mathrm{high}}(\boldsymbol{L})\boldsymbol{X}\boldsymbol{W}^{\mathrm{high}} \tag{8}$$

其中，$\boldsymbol{W}^{\mathrm{low}}$ 和 $\boldsymbol{W}^{\mathrm{high}}$ 分别为低通滤波器和高通滤波器的权重矩阵；$\boldsymbol{Z}^{\mathrm{low}}$ 和 $\boldsymbol{Z}^{\mathrm{high}}$ 为低通和高通滤波器输出的特征矩阵，其中节点 v_i 的低频和高频表征为 $\boldsymbol{z}_i^{\mathrm{low}}$ 和 $\boldsymbol{z}_i^{\mathrm{high}}$。通过上述两个滤波器，NetGPrompt 能分别建模稳定的通信结构与异常结构扰动，为后续频谱引导的预训练与提示微调提供基础。



(a) 低通滤波器空间域示意图 (b) 高通滤波器空间域示意图

(a) Low-pass filter in the spatial domain (b) High-pass filter in the spatial domain

注：以中心节点 v_0 为例，边上的‘+’号代表在聚合时对邻居节点特征进行加和(平滑操作)，‘−’号则代表计算与邻居的特征差异(锐化操作)，直观展示了滤波器的不同作用。

图 2 低通与高通滤波器空间域卷积示意图

Figure 2 Schematic diagram of spatial domain convolution for low-pass and high-pass filters

2.3 频谱感知的预训练

为充分利用高低频滤波器在图结构中的互补性，本文设计的预训练机制旨在赋予模型“频谱感知”的能力。其核心思想是，通过一种双频谱视图的对比学习任务，驱动模型学习一种对频谱变化不敏感的、更本质的节点表示。具体而言（如图 1 左上部分所示），

同一节点经过高通和低通滤波器得到的两种表示被视为正样本对。通过最大化它们的表示一致性,模型必须学会超越频域通道的差异,转而捕捉节点内蕴的、跨频域不变的结构身份。这个过程不仅增强了模型对同配与异配结构的鲁棒性,更重要的是,它让模型内化了对图谱构成的理解,为后续微调提供了具备深刻结构洞察力的表示基础。这种方式也避免了对人工标签的依赖,特别适用于大规模、标注稀缺的网络异常检测场景。

如算法1所示,本文首先利用频域滤波器对输入图信号进行高通和低通变换,分别得到节点 v_i 的低频表征 $\boldsymbol{z}_i^{\text{low}}$ 和高频表征 $\boldsymbol{z}_i^{\text{high}}$。这两个频域通道分别编码了节点所处结构环境中的不同特性:低频表示强调局部一致性与稳定性,而高频表示捕捉结构突变和节点异常性。本文将同一节点在这两个视图下的表征 $(\boldsymbol{z}_i^{\text{low}},\boldsymbol{z}_i^{\text{high}})$ 作为正样本对,并将其与其他节点之间的表征作为负样本对,从而建立跨频谱的对比任务。

基于上述设计,本文采用标准的InfoNCE(Information Noise Contrastive Estimation)[42]损失函数对模型进行优化,目标函数定义如下:

$$L_{\text{pre}}=-\frac{1}{N}\sum_{i=1}^{N}\log\frac{\exp\left(\dfrac{\text{sim}\left(\boldsymbol{z}_i^{\text{low}},\boldsymbol{z}_i^{\text{high}}\right)}{\tau}\right)}{\displaystyle\sum_{j=1}^{N}\left(\exp\left(\frac{\text{sim}\left(\boldsymbol{z}_i^{\text{low}},\boldsymbol{z}_j^{\text{high}}\right)}{\tau}\right)+\exp\left(\frac{\text{sim}\left(\boldsymbol{z}_i^{\text{high}},\boldsymbol{z}_j^{\text{low}}\right)}{\tau}\right)\right)} \tag{9}$$

其中,$\text{sim}(\boldsymbol{a},\boldsymbol{b})=\dfrac{\boldsymbol{a}^{\mathrm{T}}\boldsymbol{b}}{\|\boldsymbol{a}\|\|\boldsymbol{b}\|}$ 表示余弦相似度;τ 为温度参数,用于调控正负样本之间的区分度。

该损失函数鼓励模型最大化频域内一致性,即提升同一节点在低频与高频通道下表征的一致性,同时抑制其与其他节点异频表示之间的相似度。这一频谱对比机制使得模型不仅能够对图结构中的稳定通信模式进行建模(低频响应),还能够增强对异常连接、跳变结构等局部扰动的感知能力(高频响应)。相比于仅在单一结构通道上进行编码的传统方法,该双视图机制更加全面地捕捉了网络图中的结构异质性与频谱多样性,为后续的少样本异常检测任务提供了强健的表示基础。

通过本预训练策略,模型能够有效地学习频率不变性与结构敏感性两种核心能力,即在面对不同攻击模式、不同通信结构下的网络流量时,仍能保持鲁棒与泛化的特征提取能力,为下游提示微调机制提供了良好的初始化与结构先验。

算法1　NetGPrompt预训练

输入: 无标签网络流量图 $G=(V,E)$,滤波器 $g_{\text{low}},g_{\text{high}}$,温度参数 τ

输出: 预训练好的编码器参数 θ^*

1.FOR each epoch DO

2.　通过低通滤波器计算低频表示:$\boldsymbol{Z}^{\text{low}}=g_{\text{low}}(\boldsymbol{L})\boldsymbol{X}\boldsymbol{W}^{\text{low}}$

3.　通过高通滤波器计算高频表示:$\boldsymbol{Z}^{\text{high}}=g_{\text{high}}(\boldsymbol{L})\boldsymbol{X}\boldsymbol{W}^{\text{high}}$

4:　根据式(9)计算对比损失 $\boldsymbol{L}_{\text{pre}}$

5:　反向传播并更新编码器参数 $\theta=\{\boldsymbol{W}^{\text{low}},\boldsymbol{W}^{\text{high}}\}$

6.END FOR

7.RETURN 训练好的参数 θ^*

2.4　提示引导的频谱微调

在标注样本极为有限的场景下,直接对预训练模型进行全参数微调往往会引发“负迁移”问题[14],即原有频谱知识被覆盖,模型性能反而下降。为此,近年来的研究提出“提示微调”范式,通过冻结模型主体参数,仅优化少量提示参数,在降低计算开销的同时实现预训练知识的有效迁移。

基于上述思想,如图1下半部分所示,本文在频谱预训练的基础上,进一步提出一种参数高效、结构感知的提示微调机制,以适应下游任务中频谱结构的多样性差异。该机制尤其适用于 K-shot 异常检测任务,在极少标注样本条件下,依然能实现良好的判别性能与结构迁移能力。

在不同下游任务中,模型对高频和低频特征的依赖程度存在显著差异。为此,本文设计的提示向量扮演了“频谱注意力”的角色,它允许模型根据下游任务的特定需求,自适应地感知并调控对不同频段信息的依赖程度。如算法2所示,本文设计了两个可学习提示向量 $\boldsymbol{p}^{\text{low}},\boldsymbol{p}^{\text{high}}\in\mathbb{R}^d$,分别作用于低通表征 $\boldsymbol{z}_i^{\text{low}}$ 和高通表征 $\boldsymbol{z}_i^{\text{high}}$。融合表征定义如下:

$$\boldsymbol{z}_i=\boldsymbol{p}^{\text{low}}\odot\boldsymbol{z}_i^{\text{low}}+\boldsymbol{p}^{\text{high}}\odot\boldsymbol{z}_i^{\text{high}} \tag{10}$$

其中,$\odot$ 代表维度级点乘操作,提示向量控制了不同频段表征在最终表征中的贡献权重。该机制能够使模型根据局部结构信息自动调节对频谱通道的依赖程度,从而实现更加精准、动态的结构感知建模。

在得到融合表征后,本文采用多层感知机(Multi-Layer Perceptron,MLP)构建轻量级分类器,用于对节点进行异常检测。其监督损失函数为交叉熵损失:

$$L_{\text{down}}(\omega;\theta^*)=-\frac{1}{N}\sum_{i=1}^{N}y_i\cdot\log\left(\text{Softmax}(\boldsymbol{W}\boldsymbol{z}_i+\boldsymbol{b})\right) \tag{11}$$

其中,$\boldsymbol{W}$ 和 $\boldsymbol{b}$ 分别为该分类器的权重和偏置;$y_i\in\{0,1\}$ 表示节点 v_i 的标签;0代表正常节点;1代表异常节点。

在微调阶段,预训练得到的频域滤波器参数 θ^*

(包括低频和高频滤波器的权重矩阵)保持冻结,微调的参数 ω 为提示向量和分类器参数,显著减少了训练所需样本与计算资源。通过提示向量对频谱通道进行精细调控,模型在少样本条件下依然能够实现对预训练知识的有效迁移,提升了对网络异常流量的检测能力。

算法2 NetGPrompt提示微调

输入: 带少量标签的图 G,预训练参数 θ^*,提示向量 $\boldsymbol{p}^{\text{low}}$,$\boldsymbol{p}^{\text{high}}$

输出: 训练好的提示向量 $\boldsymbol{p}^{\text{low}}$,$\boldsymbol{p}^{\text{high}}$ 和分类器参数

1.冻结编码器参数 θ^*

2.FOR each epoch DO

3. 根据式(8)分别计算低频表示 $\boldsymbol{z}_i^{\text{low}}$ 和高频表示 $\boldsymbol{z}_i^{\text{high}}$

4. 根据式(10)融合表征:$\boldsymbol{z}_i=\boldsymbol{p}^{\text{low}}\odot\boldsymbol{z}_i^{\text{low}}+\boldsymbol{p}^{\text{high}}\odot\boldsymbol{z}_i^{\text{high}}$

5. 根据式(11),使用 $\boldsymbol{z}_i$ 和标签 y_i 计算下游任务损失 L_{down}

6. 反向传播并仅更新提示向量和分类器参数

7.END FOR

8.RETURN 训练好的参数

3 实验结果与分析

3.1 实验设置

3.1.1 数据集

为了系统评估所提出的NetGPrompt方法在网络异常检测任务中的有效性与泛化能力,本文选用了三个具有代表性和挑战性的网络流量图数据集:CICIDS2017[43]、CICIDS2018[44]和HIKARI2021[45]。这三者涵盖了从传统攻击到新型隐蔽威胁的多样化异常行为,并体现出通信结构、攻击手段与时间特征的显著差异,为模型在不同网络环境下的鲁棒性测试提供了充分基础。数据集的具体统计信息列于表1。

表1 数据集统计表

Table 1 Statistical table of datasets

统计项	CICIDS2017	CICIDS2018	HIKARI2021
节点数量	87 423	267 187	29 718
边数量	951 082	618 629	54 267
异常节点占比	18.05%	3.56%	0.61%
特征维度	3	3	3

(1)CICIDS2017数据集:该数据集由加拿大网络安全研究中心发布,模拟了包含正常办公行为和多种典型网络攻击(如PortScan、Brute Force、Web攻击、Botnet等)的现实网络环境。数据覆盖了多个时间段和网络协议,具有较强的代表性。

(2)CICIDS2018数据集:该数据集是由加拿大CSE与CIC联合构建的更大规模入侵检测数据集,覆盖了10天的网络活动,模拟了多个用户角色(如员工、管理员)在正常办公场景下的真实操作行为,并注入了更广泛、更现代化的攻击类型,包括Botnet、Infiltration、Brute Force、Web攻击、恶意软件下载、SQL注入等。考虑到图的构建,本文只使用其带有IP地址的数据。

(3)HIKARI2021数据集:该数据集是近年发布的真实环境网络攻击数据集,由横滨国立大学基于现代企业网络环境构建,覆盖工控系统、桌面终端等多类通信实体。数据中注入了多种高级持续性威胁相关攻击,如命令与控制通信、横向移动、文件泄露等。

为保证实验效率与图结构稀疏性控制,本文对原始数据进行了采样处理,并按连接关系构建边集,完成图构建。在特征选择上,本文统一采用“持续时间”“源到目的字节数”和“目的到源字节数”这三项基础统计特征。选择这三维特征主要基于以下考量。(1)普适性:它们是网络流最基本、与协议无关的度量,适用于各类网络环境;(2)最小化特征工程依赖:使用基础特征可以更好地评估模型从图结构中学习和推理异常模式的能力,而非依赖复杂的特征工程,这更符合本研究的重点。

3.1.2 基准模型

为了充分地验证所提出方法的有效性,如表2所示,本文选取了三类具有代表性的基线模型进行对比,分别为:传统图神经网络模型、“预训练+微调”图模型,以及“预训练+提示调优”图模型。

第一类包括端到端图神经网络模型。该类模型在图结构上采用监督学习训练,并直接在同一图上进行推理。

(1)GCN[6]:采用频域图卷积构造拉普拉斯滤波器,实现节点邻居特征的聚合;

(2)GraphTransformer[46]:引入Transformer结构处理图任务,通过注意力机制建模长距离依赖;

(3)BWGNN[17]:基于频域分析构建图滤波器,将图中的异常信号识别为高频成分,并通过高通/带通滤波器提取高频特征,适用于异常检测。

第二类包括“预训练+微调”的图模型。该类方法通过自监督任务进行图模型预训练,随后在下游图任务上进行微调。

(1)GraphCL[9]:采用多种图增广策略(如节点扰动、边采样等)生成不同视图,进行对比学习以提高结构表示的一致性;

(2)PolyGCL[16]:频域自监督方法,利用多项式滤波器分别生成低通与高通视图进行对比学习,增强对异配图的适应能力。

第三类包括“预训练+提示调优“的图模型。该类方法将下游任务重构为提示微调范式,仅对少量提示参数进行优化,以实现更高效的迁移能力。

(1)GPrompt[11]:以子图相似性判别作为预训练

表2　基准模型概述

Table 2　Overview of baseline models

类别	模型名称	核心思想	实验目的
传统图神经网络	GCN, Graph-Transforme	单阶段端到端监督学习:不经过预训练,直接在下游任务的有标签数据上,通过邻居聚合或自注意力机制进行训练。	验证依赖同配性假设的传统方法在异配、少样本场景下的局限性。
	BWGNN	单阶段端到端监督学习:不经过预训练,同样只在有标签数据上训练,但其设计核心是利用频域滤波器专门提取异常特征。	对比同样利用频域信息的监督学习模型,验证其在少样本下的性能。
图预训练+微调	GraphCL, PolyGCL	两阶段范式(自监督预训练+全参数微调):先通过自监督任务预训练模型,然后在下游任务中对全部参数进行微调。	验证预训练的有效性,并与参数高效的提示微调进行对比。
图预训练+提示微调	GPrompt, GPF-plus	两阶段范式(自监督预训练+参数高效微调):预训练后冻结主干参数,仅通过优化少量提示参数来适配下游任务。	对比同为参数高效范式的模型,以凸显本框架频谱感知的优势。

目标,统一节点分类与图分类任务,通过提示模板将任务嵌入相似性预测框架,但主要偏向低频信息建模;

(2)GPF-plus[13]:通用的图提示调优框架,在输入特征空间中引入参数化提示向量,可适配任意图预训练模型。在本实验中采用其鲁棒性更强的变体版本GPF-plus进行对比。

3.1.3　评估指标

在图异常检测任务中,异常样本通常占据极少数比例,标签分布高度不均衡,常规准确率(Accuracy)等指标难以真实反映模型在识别少量异常节点方面的性能。因此,本文选用AUC(Area Under the ROC Curve)与PR-AUC(Area Under the Precision-Recall Curve)两项指标作为主要评估标准[47],以全面衡量模型在不平衡图结构中的检测效果。

其中,AUC衡量的是模型在所有可能阈值下对正负样本的区分能力,具有良好的全局判别解释力,能够反映模型整体的排序能力;而PR-AUC更加关注模型在高精度条件下的召回表现,特别适用于异常样本极少、负样本占据主导的任务场景,能更准确地衡量模型对“罕见但重要”异常行为的识别能力。

3.1.4　参数设置

本研究将模型训练划分为两个阶段:图预训练与提示微调。预训练阶段的学习率设定为1×10^{-3},提示调优阶段则设置为5×10^{-3},以适配不同训练目标对优化步长的敏感性。

本文将下游任务设定为小样本学习(5-shot learning),即每类数据(即正常样本和异常样本)仅随机采样5个样本用于提示调优,其余数据平均分为验证集和测试集。为确保结果的稳定性,本文对每项实验设置不同随机种子运行3次,并报告其平均结果。在训练过程中,模型共训练2 000轮(epoch),并基于验证集上AUC分数的最优值进行模型选择。全部实验均在搭载NVIDIA A100 40 GB GPU的计算环境中完成,深度学习框架为PyTorch 1.13.1。

在基准模型的实现方面:对GCN、GraphTransformer、GraphCL、GPrompt和GPF-plus,本文使用公开的图提示学习评估平台ProG[48]实现这些方法,并采用一致的2层图卷积结构以保证结构公平性。对BWGNN和PolyGCL,本文使用作者提供的原始代码进行复现。在涉及预训练阶段的模型中,均按照其源代码推荐的超参数进行预训练;在下游调优阶段,则统一采用与本文方法相同的学习率与训练轮数,以保证对比公平性。

3.2　性能比较

为全面验证本文提出的NetGPrompt框架在网络流量异常检测任务中的有效性,本文在三个具有代表性的网络安全数据集上与多种主流基准模型进行了对比实验。表3列出了所有对比方法在AUC和PR-AUC两项指标下的性能表现,其中每项指标的最优值以加粗标示,次优结果以下划线标示。

从表3可以看出,NetGPrompt在所有三个数据集上均取得了当前所有方法中的最优性能,显著优于图神经网络方法、图预训练方法以及图提示微调方法。基于实验结果,本文对不同数据集下的性能差异展开深入分析。

(1)NetGPrompt在不同数据集下的性能分析:NetGPrompt在三个具有显著差异的数据集上均表现出卓越的鲁棒性。具体而言,HIKARI2021数据集具有极强的异配性(异常仅占0.61%),导致基于平滑假设的GCN完全失效AUC仅0.447 2),而NetGPrompt在此极端场景下的PR-AUC达到0.174 8,显著优于次优模型BWGNN的0.156 8,证明了其在极少样本下精准

表3 不同方法在网络流量图异常检测任务中的评估指标及标准差

Table 3 Evaluation metrics and standard deviations for network traffic graph anomaly detection with different methods

方法		CICIDS2017		CICIDS2018		HIKARI2021	
		AUC	PR-AUC	AUC	PR-AUC	AUC	PR-AUC
传统图神经网络	GCN	0.826 5±0.022 2	0.444 8±0.037 7	0.597 7±0.086 2	0.053 8±0.001 1	0.447 2±0.019 6	0.017 0±0.005 7
	GraphTransformer	0.861 5±0.054 7	0.659 6±0.028 1	0.451 3±0.048 9	0.036 6±0.001 6	0.727 9±0.029 8	0.055 6±0.010 4
	BWGNN	0.873 1±0.015 1	0.618 6±0.031 9	0.757 0±0.043 6	0.075 4±0.013 1	<u>0.981 7±0.005 9</u>	<u>0.156 8±0.037 4</u>
图预训练+微调	GraphCL	0.869 2±0.062 1	0.631 7±0.052 4	0.404 1±0.009 6	0.035 6±0.000 0	0.550 2±0.269 8	0.034 5±0.040 3
	PolyGCL	0.862 0±0.062 1	<u>0.675 1±0.012 8</u>	0.674 0±0.108 1	0.066 5±0.030 3	0.981 2±0.001 4	0.142 8±0.011 2
图预训练+提示微调	GPrompt	0.899 2±0.002 2	0.503 1±0.005 3	0.793 4±0.117 4	0.116 9±0.062 7	0.980 8±0.001 0	0.146 0±0.011 9
	GPF-plus	<u>0.913 6±0.000 2</u>	0.523 3±0.003 1	<u>0.830 8±0.080 9</u>	<u>0.123 9±0.056 8</u>	0.980 9±0.000 9	0.149 9±0.017 2
	NetGPrompt	**0.933 1±0.013 6**	**0.687 2±0.014 5**	**0.935 9±0.047 3**	**0.330 6±0.161 9**	**0.982 4±0.001 4**	**0.174 8±0.011 7**

注:表格中加粗代表该数据集上该指标的最优性能,下划线代表该数据集上该指标的次优性能。

定位高价值异常的能力。在异常占比较高(18.05%),即包含部分同配结构的CICIDS2017数据集中,NetGPrompt依然取得了0.933 1的最佳AUC,验证了其双滤波器设计能同时兼顾低频同配模式与高频异配干扰,表现出优于单一频域模型的普适性。而在规模最大、攻击类型最复杂的CICIDS2018数据集上,NetGPrompt的优势最为显著,其PR-AUC达到0.330 6,相较于次优模型GPF-plus提升超过20个百分点,充分体现了提示微调机制在大规模复杂拓扑中,通过微调少量参数快速适配多样化攻击分布的强大能力。

(2)传统图神经网络对异配结构的局限性:传统GNN方法在处理网络流量图时表现出明显的不稳定性。特别是在HIKARI2021数据集上,GCN的AUC甚至低于随机预测水平0.5),这有力地证明了传统方法过度依赖"同配性假设"。面对由异常流量引发的非典型连接(强异配结构),仅依靠空间域的邻居平滑聚合难以捕捉真实的攻击模式,甚至会引入噪声。

(3)频谱建模捕捉结构扰动的有效性:基于频域建模的图异常检测方法(如BWGNN和PolyGCL)在所有基准模型中整体表现较好。特别是在GCN失效的HIKARI2021数据集上,它们均保持了极高的AUC水平。这说明通过高频通道建模结构跳变和局部扰动是识别网络异常的关键,也从侧面印证了本文所采用的"低通+高通"双通道建模思路的理论正确性。

(4)提示微调范式的参数高效性与迁移能力:"图预训练+提示微调"范式的整体效果优于仅进行全参数微调的方法。对比数据可见,GPrompt和GPF-plus在多个数据集上相较于GraphCL均有性能提升。这说明在少样本条件下,提示机制可以在参数有限的前提下,更高效地引导模型适配目标任务分布。而NetGPrompt则进一步将提示机制与频谱感知相结合,通过提示向量动态调整频谱通道权重,从而实现了全场景下的最优检测性能。

3.3 消融实验

为深入分析NetGPrompt各核心模块在网络流量图异常检测任务中的作用,本文设计了一系列消融实验,对模型中关键组件逐一移除,并在相同训练配置下评估其性能变化。具体包括以下四个变体模型。

w/o (without) Low Filter:移除低通图滤波器,仅保留高通通道,用于评估低频结构信息(如正常通信拓扑)对模型性能的影响。

w/o High Filter:移除高通图滤波器,仅保留低通通道,用于评估高频结构信息(如异常连接扰动)对异常检测的贡献。

w/o Pre-train:完全去除频谱对比预训练阶段,仅利用少量标注样本在下游任务中进行提示微调,以验证预训练阶段的有效性。

w/o Prompt:去除提示机制,仅对最终分类器进行微调,频谱编码器部分保持冻结,验证提示向量在结构融合与任务迁移中的作用。

消融实验结果如表4所示,可以得出以下几点主要结论。

(1)频谱双滤波器在不同网络环境下的互补性与差异化贡献:消融实验清晰地揭示了不同频率通道在特定数据集中的主导作用。

在HIKARI2021数据集中,移除高通滤波器(w/o High Filter)导致PR-AUC从0.174 8骤降至0.101 2,其降幅显著大于移除低通滤波器的情况(降至0.145 3)。这一结果与该数据集的高异配性特征高度吻合,证实了捕捉节点间差异的高频信号是识别此类隐蔽异常的关键。

相反,在CICIDS2017数据集中,移除低通滤波器(w/o Low Filter)带来的性能损失更为严重(PR-AUC从0.687 2降至0.561 3)。这表明在该环境下,正常流量表现出较强的局部一致性,捕捉这种稳定的通信拓扑(低频信息)对于区分异常同样至关重要。

而在CICIDS2018中,移除任一滤波器均会导致性能大幅退化(PR-AUC均降至0.13左右)。综上,高低频滤波器的联合建模并非简单地叠加,而是根据数据分布自适应地覆盖了从“通信模式一致性”到“连接结构突变”的多样化异常特征。

(2)频谱预训练对结构泛化能力的普适性提升:去除预训练阶段(w/o Pre-train)在所有三个数据集上均导致了显著的性能下降。特别是在CICIDS2017上,PR-AUC下降了约6个百分点。这表明,通过对比学习在大规模无标签图上习得的频谱不变性特征,能够为下游任务提供鲁棒的结构先验。在少样本条件下,这种初始化优势有效缓解了模型对有限标注数据的过度拟合,改善了泛化边界。

(3)提示微调机制对复杂结构分布的适配作用:移除提示向量(w/o Prompt)限制了模型对特定任务分布的动态调整能力。这一效应在结构最为复杂的CICIDS2018数据集上尤为明显,其PR-AUC从0.330 6跌至0.272 6,说明在面对多样化攻击模式时,提示机制通过自适应调节频谱通道权重,发挥了关键的“任务感知”调节作用。即使在结构相对单一的HIKARI2021上,移除提示机制也导致PR-AUC下降至0.149 2,证明了在冻结主干参数的前提下,提示微调仍能通过轻量级参数优化进一步细化判别空间,提升检测精度。

表4　消融实验结果

Table 4　Ablation study results

模型组合	CICIDS2017		CICIDS2018		HIKARI2021	
	AUC	PR-AUC	AUC	PR-AUC	AUC	PR-AUC
w/o Low Filter	0.915 3±0.007 9	0.561 3±0.028 1	0.873 2±0.055 9	0.136 8±0.040 9	0.981 2±0.001 8	0.145 3±0.014 3
w/o High Filter	0.920 0±0.007 9	0.588 9±0.063 5	0.875 6±0.049 9	0.139 0±0.048 7	0.971 2±0.001 5	0.101 2±0.008 6
w/o Pre-train	<u>0.922 5±0.005 8</u>	<u>0.625 4±0.018 7</u>	0.872 9±0.035 7	0.128 2±0.027 8	<u>0.981 7±0.001 3</u>	0.148 6±0.010 8
w/o Prompt	0.922 5±0.015 9	0.624 7±0.034 9	<u>0.932 8±0.044 4</u>	<u>0.272 6±0.105 8</u>	0.981 6±0.001 4	<u>0.149 2±0.011 6</u>
NetGPrompt(本文)	**0.933 1±0.013 6**	**0.687 2±0.014 5**	**0.935 9±0.047 3**	**0.330 6±0.161 9**	**0.982 4±0.001 4**	**0.174 8±0.011 7**

注:表格中加粗代表该数据集上该指标的最优性能,下划线代表该数据集上该指标的次优性能。

3.4　图滤波器兼容性实验分析

为探究频谱滤波器设计对NetGPrompt模型性能的影响,本文在保持模型整体结构不变的前提下,替换其默认的线性高/低通滤波器,分别采用BWGNN[17]和PolyGCL[16]中提出的频谱响应函数,其中BWGNN采用基于Beta分布构建的可学习带通滤波器,用于精确控制频率响应形状,PolyGCL采用基于Chebyshev插值的固定多项式滤波器。本节在CICIDS2017、CICIDS2018和HIKARI2021三个网络流量数据集上进行了兼容性实验,结果如图3和图4所示,其中w.BWGNN表示将模型的滤波器替换为BWGNN采用的滤波器,w.PolyGCL表示将模型的滤波器替换为PolyGCL采用的滤波器,NetGPrompt则为本文方法。

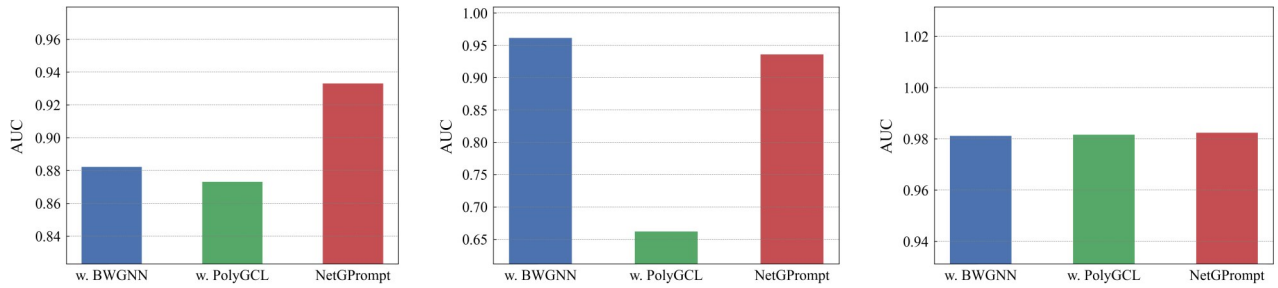
从实验结果可以观察到,不同滤波器的选择确实对模型的最终性能产生了显著影响。整体来看,NetGPrompt默认设计的线性频率响应在三个数据集上均取得较优性能,表现出较好的稳定性和鲁棒性。使用BWGNN的滤波器时,模型在CICIDS2017和HIKARI202上仍保持了较高的AUC和PR-AUC,但在CICIDS2018上性能略有波动,尤其在PR-AUC上出现一定程度的下降。相比之下,PolyGCL的多项式滤波器在CICIDS2018数据集上的表现则明显下降。

从对比中可以看出,NetGPrompt并未对滤波器形式做强约束,其整体结构具备较强的适配性。但同时也说明,在实际应用中,滤波器的频率响应特性与数据分布之间仍存在较强的耦合关系,选择合适的滤波器设计对于挖掘有效频谱特征具有重要意义。线性频率响应虽形式简洁,但在本实验中表现出更强的泛化能力,说明其在频谱对比学习框架中具备较高的实用价值。

3.5　训练数据规模对模型性能的影响

为评估NetGPrompt在小样本学习场景中的表现稳定性与可扩展性,本文进一步考察了不同训练样本数量(即K-shot设置)对模型性能的影响。实验中分别设置$K=5$、10、15和20,即每类样本(正常与异常)分别提供5~20条用于提示调优,其余数据用于验证与测试。在本实验中,本文保持预训练阶段不变,仅对下游提示调优阶段提供不同规模的标注样本进行训练,其余训练参数(优化器、学习率、迭代轮数等)和数据集划分方式均保持一致,以保证对比的公平性。实验结果如图5和图6所示,每张子图中横坐标代表每一类的训练集数量,纵坐标代表性能指标。

从实验结果可以观察到,NetGPrompt即便在5-shot的极低数据设置下,已能取得较优的检测效果,体现出其强小样本学习能力。随着训练样本数量从5增加至20,模型在CICIDS2017和CICIDS2018上的

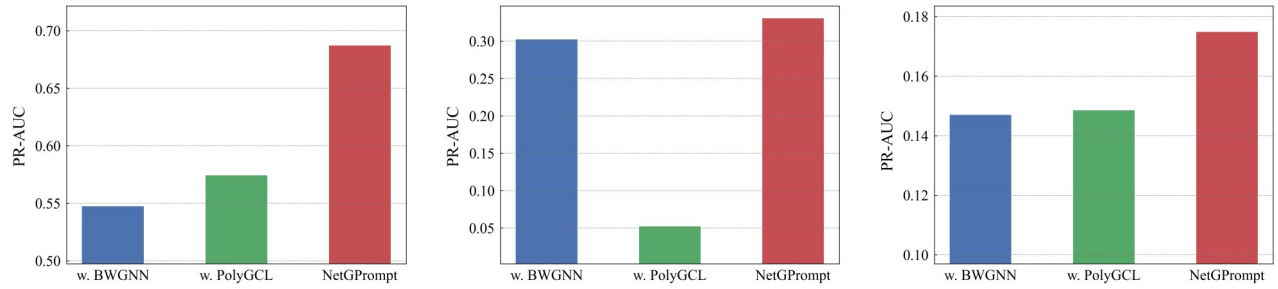


(a) 数据集CICIDS2017上AUC指标 (b) 数据集CICIDS2018上AUC指标 (c) 数据集HIKARI2021上AUC指标

(a) AUC metric on the CICIDS2017 dataset (b) AUC metric on the CICIDS2018 dataset (c) AUC metric on the HIKARI2021 dataset

图3 不同图滤波器在三个数据集上的AUC性能对比

Figure 3 Comparison of AUC performance of different graph filters on three datasets

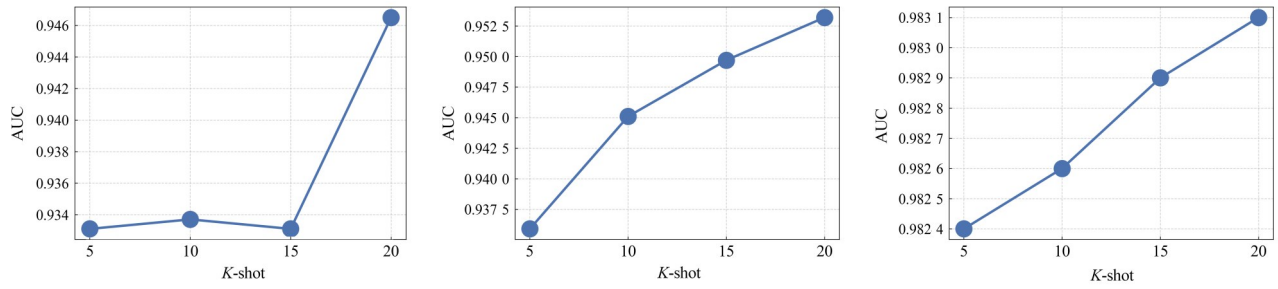


(a) 数据集CICIDS2017上PR-AUC指标 (b) 数据集CICIDS2018上PR-AUC指标 (c) 数据集HIKARI2021上PR-AUC指标

(a) PR-AUC metric on the CICIDS2017 dataset (b) PR-AUC metric on the CICIDS2018 dataset (c) PR-AUC metric on the HIKARI2021 dataset

图4 不同图滤波器在三个数据集上的PR-AUC性能对比

Figure 4 Comparison of PR-AUC performance of different graph filters on three datasets



(a) 数据集CICIDS2017上AUC指标 (b) 数据集CICIDS2018上AUC指标 (c) 数据集HIKARI2021上AUC指标

(a) AUC metric on the CICIDS2017 dataset (b) AUC metric on the CICIDS2018 dataset (c) AUC metric on the HIKARI2021 dataset

图5 训练集数量对模型AUC指标的影响

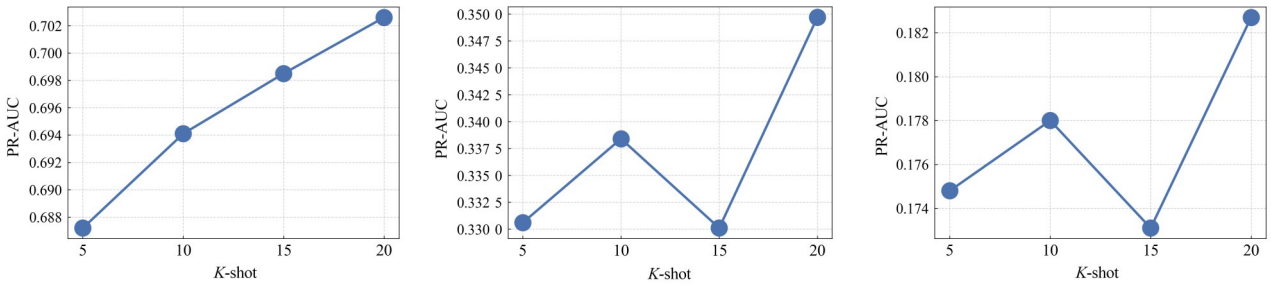
Figure 5 Impact of training set size on the model's AUC metric

AUC和PR-AUC分数总体呈现出稳步上升趋势，表明更多的训练信息有助于增强模型的判别能力和泛化性能。PR-AUC指标的变化相对缓慢，个别数据集在样本增多后略有波动，可能与异常样本在图中的稀疏分布或局部不平衡性有关。但整体来看，NetGPrompt在训练集规模扩大时仍能保持稳定且优越的性能，验证了其频谱建模与提示机制在低资源下的鲁棒性与扩展性。

3.6 参数效率分析

为量化验证本文所提提示微调机制的参数高效性，我们对比了NetGPrompt采用的参数高效微调与传统全参数微调在不同模型复杂度下的可训练参数量。本次分析覆盖了本文的实际实验场景以及两个更大规模的假设场景，结果如表5所示。

从表中可以清晰地看到，即便在本次实验的小规模场景中，NetGPrompt的微调方式已能节省超过55%



(a) 数据集 CICIDS2017 上 PR-AUC 指标　(b) 数据集 CICIDS2018 上 PR-AUC 指标　(c) 数据集 HIKARI2021 上 PR-AUC 指标

(a) PR-AUC metric on the CICIDS2017 dataset　(b) PR-AUC metric on the CICIDS2018 dataset　(c) PR-AUC metric on the HIKARI2021 dataset

图 6　训练集数量对模型 PR-AUC 指标的影响

Figure 6　Impact of training set size on the model's PR-AUC metric

的可训练参数。更重要的是,这一效率优势具备出色的扩展性:当模型规模扩大至中等(64 维)和较大(256 维)尺寸时,参数节省比例分别跃升至 82.39% 和 83.1%。数据清晰地表明,模型越复杂,NetGPrompt 在参数效率上的优势就愈发突出。这证明了本方法的出色扩展性,能够以极低的参数代价实现对大规模图预训练模型的有效适配,尤其适用于计算资源受限或需要快速部署的实际应用场景。

表 5　参数效率对比

Table 5　Comparison of parameter efficiency

场景	维度(输入层/隐藏层)	全参数微调	NetGprompt 微调	参数节省比例
实验场景	3 / 8	240	106	55.83%
假设场景 1	64 / 64	25 090	4 418	82.39%
假设场景 2	256 / 256	395 266	66 818	83.10%

4　结束语

本文围绕网络流量异常检测中结构异配与标签稀缺两大核心挑战,提出了 NetGPrompt——一种基于频域的预训练与提示微调的图学习框架。该方法从频域角度切入,设计互补滤波器对正常与异常流量的结构特征进行差异建模,并通过频谱视图对比学习提升预训练阶段的表征能力。在提示微调阶段,NetGPrompt 通过频率通道加权实现高效适配,避免了冗余参数引入。实验结果在多个真实数据集上全面验证了所提方法在异常检测的优势,其检测性能显著优于现有基准模型,充分证明了框架的实用性与鲁棒性。尽管 NetGPrompt 取得了优越性能,但仍存在一定局限性:其一,图构建策略基于 IP 与端口匹配,相对固定且维度单一,未能充分利用流量多维属性与时空特征,难以全面捕捉复杂攻击链条的动态关联;其二,线性滤波器虽泛化性强,但对特定攻击模式的适配性不足,难以精准匹配多样化威胁的频谱特征;其三,现有实验基于标准数据集,尚未充分验证大规模生产环境下的计算效率与实时检测能力,与实际部署需求存在差距。未来工作将围绕核心方向展开:一是深化动态图构建,探索基于多维流量属性或时空演化规律的构图策略,精准捕捉攻击链条演化;二是推进滤波器自适应化,将线性滤波器扩展为可学习或非线性形式,优化特定威胁环境下的检测精度;三是强化实际部署适配,研究大规模场景下的模型压缩与并行计算方案,全面评估计算效率与实时性能;同时持续优化结构感知提示策略,提升模型对复杂攻击形态的适配能力,为网络安全防护提供更可靠支撑。

参考文献

[1] 王晓曦, 王永吉, 周津慧, 等. 基于改进网络模型的大时滞网络拥塞控制算法[J]. 电子学报, 2005, 33(5): 842-846.
Wang Xiaoxi, Wang Yongji, Zhou Jinhui, et al. Congestion control algorithm based on improved model in large-delay networks[J]. Acta Electronica Sinica, 2005, 33(5): 842-846. (in Chinese)

[2] Tippe P, Tippe A, Keller J. Detecting and attributing tor-obfuscated malware communications through traffic fingerprinting[C]//Proceedings of the 2025 ACM Workshop on Information Hiding and Multimedia Security. San Jose: ACM, 2025: 74-79.

[3] 仇晶, 陈荣融, 朱浩瑾, 等. 基于溯源图的网络攻击调查研究综述[J]. 电子学报, 2024, 52(7): 2529-2556.
Qiu Jing, Chen Rongrong, Zhu Haojin, et al. A survey of

network attack investigation based on provenance graph[J]. Acta Electronica Sinica, 2024, 52(7): 2529-2556. (in Chinese)

[4] Ali Hassan Ahmed L, Hamad Y A M, Ali Abdalla A A M. Network-based intrusion detection datasets: A survey[C]// Proceedings of 2022 International Arab Conference on Information Technology. Abu Dhabi: IEEE, 2022: 1-7.

[5] 金正晗, 李建彬, 李敬豪, 等. 一种用于不平衡数据的新型网络异常流量检测方法[J]. 广西科学, 2024, 31(5): 966-975.
Jin Zhenghan, Li Jianbin, Li Jinghao, et al. A novel network abnormal traffic detection method for imbalanced network data[J]. Guangxi Sciences, 2024, 31(5): 966-975. (in Chinese)

[6] Jiang Bo, Zhang Ziyan, Lin Doudou, et al. Semi-supervised learning with graph learning-convolutional networks[C]// Proceedings of 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019: 11305-11312.

[7] Veličković P, Cucurull G, Casanova A, et al. Graph attention networks[C]//Proceedings of the 6th International Conference on Learning Representations. Vancouver: ICLR, 2018.

[8] Velickovic P, Fedus W, Hamilton W L, et al. Deep graph infomax[C]//Proceedings of the 7th International Conference on Learning Representations. New Orleans: ICLR, 2019: 4.

[9] You Yuning, Chen Tianlong, Sui Yongduo, et al. Graph contrastive learning with augmentations[C]//Proceedings of the 34th International Conference on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2020: 488.

[10] Xia Jun, Wu Lirong, Chen Jintao, et al. SimGRACE: A simple framework for graph contrastive learning without data augmentation[C]//Proceedings of the ACM Web Conference 2022. Lyon: ACM, 2022: 1070-1079.

[11] Liu Zemin, Yu Xingtong, Fang Yuan, et al. GraphPrompt: Unifying pre-training and downstream tasks for graph neural networks[C]//Proceedings of the ACM Web Conference 2023. Austin: ACM, 2023: 417-428.

[12] Sun Xiangguo, Cheng Hong, Li Jia, et al. All in one: Multi-task prompting for graph neural networks[C]//Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Long Beach: ACM, 2023: 2120-2131.

[13] Fang Taoran, Zhang Yunchao, Yang Yang, et al. Universal prompt tuning for graph neural networks[C]//Proceedings of the 37th International Conference on Neural Information Processing Systems. New Orleans: ACM, 2023: 2285.

[14] Sun Mingchen, Zhou Kaixiong, He Xin, et al. GPPT: Graph pre-training and prompt tuning to generalize graph neural networks[C]//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Washington: ACM, 2022: 1717-1727.

[15] Yu Xingtong, Zhang Jie, Fang Yuan, et al. Non-homophilic graph pre-training and prompt learning[C]//Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.1. Toronto: ACM, 2025: 1844-1854.

[16] Chen Jingyu, Lei Runlin, Wei Zhewei. PolyGCL: GRAPH CONTRASTIVE LEARNING via learnable spectral polynomial filters[C]//Proceedings of the 12th International Conference on Learning Representations. Vienna: ICLR, 2024.

[17] Tang Jianheng, Li Jiajin, Gao Ziqi, et al. Rethinking graph neural networks for anomaly detection[C]//Proceedings of the 39th International Conference on Machine learning. Baltimore: PMLR, 2022: 21076-21089.

[18] Bo Deyu, Wang Xiao, Shi Chuan, et al. Beyond low-frequency information in graph convolutional networks[C]// Proceedings of the 35th AAAI Conference on Artificial Intelligence. AAAI, 2021: 3950-3957.

[19] Luo Haitong, Meng Xuying, Wang Suhang, et al. Spectral-based graph neural networks for complementary item recommendation[C]//Proceedings of the 38th AAAI Conference on Artificial Intelligence. Vancouver: AAAI, 2024: 8868-8876.

[20] Roesch M. Snort-lightweight intrusion detection for networks[C]//Proceedings of the 13th USENIX Conference on System Administration. Seattle: USENIX Association, 1999: 229-238.

[21] Tavallaee M, Bagheri E, Lu Wei, et al. A detailed analysis of the KDD CUP 99 data set[C]//Proceedings of 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. Ottawa: IEEE, 2009: 1-6.

[22] Hearst M A, Dumais S T, Osuna E, et al. Support vector machines[J]. IEEE Intelligent Systems and Their Applications, 1998, 13(4): 18-28.

[23] 李康和, 黄震华. 基于噪声过滤与特征增强的图神经网络欺诈检测方法[J]. 电子学报, 2023, 51(11): 3053-3060.
Li Kanghe, Huang Zhenhua. Noise filtering and feature

enhancement based graph neural network method for fraud detection[J]. Acta Electronica Sinica, 2023, 51(11): 3053-3060. (in Chinese)

[24] Lee W, Stolfo S J, Mok K W. A data mining framework for building intrusion detection models[C]//Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland: IEEE, 1999: 120-132.

[25] Liao Yihua, Vemuri V R. Use of K-nearest neighbor classifier for intrusion detection[J]. Computers & Security, 2002, 21(5): 439-448.

[26] Vinayakumar R, Soman K P, Poornachandran P. Applying convolutional neural network for network intrusion detection[C]//Proceedings of 2017 International Conference on Advances in Computing, Communications and Informatics. Udupi: IEEE, 2017: 1222-1228.

[27] 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. Da Nang: IEEE, 2017: 712-717.

[28] Shone N, Ngoc T N, Phai V D, et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 41-50.

[29] Huoh T L, Luo Yan, Li Peilong, et al. Flow-based encrypted network traffic classification with graph neural networks[J]. IEEE Transactions on Network and Service Management, 2023, 20(2): 1224-1237.

[30] Zuo Xingtao, Fang Cheng, Han Ping. Network traffic anomaly detection based on spatio-temporal dynamic graph[C]//Proceedings of 2024 IEEE 14th International Conference on Electronics Information and Emergency Communication. Beijing: IEEE, 2024: 221-225.

[31] Sun Zhenlu, Teixeira A M H, Toor S. GNN-IDS: Graph neural network based intrusion detection system[C]//Proceedings of the 19th International Conference on Availability, Reliability and Security. Vienna: ACM, 2024: 14.

[32] Hamilton W L, Ying R, Leskovec J. Inductive representation learning on large graphs[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. Long Beach: Curran Associates Inc., 2017: 1025-1035.

[33] Abu-El-Haija S, Perozzi B, Kapoor A, et al. MixHop: Higher-order graph convolutional architectures via sparsified neighborhood mixing[C]//Proceedings of the 36th International Conference on Machine Learning. Long Beach: PMLR, 2019: 21-29.

[34] Duan Rui, Guang Mingjian, Wang Junli, et al. Unifying homophily and heterophily for spectral graph neural networks via triple filter ensembles[C]//Proceedings of the 38th International Conference on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2024: 2966.

[35] Lester B, Al-Rfou R, Constant N. The power of scale for parameter-efficient prompt tuning[C]//Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing. Punta Cana: Association for Computational Linguistics, 2021: 3045-3059.

[36] Li X L, Liang P. Prefix-tuning: Optimizing continuous prompts for generation[C]//Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long papers). Online: Association for Computational Linguistics, 2021: 4582-4597.

[37] Karimi Mahabadi R, Ruder S, Dehghani M, et al. Parameter-efficient multi-task fine-tuning for transformers via shared hypernetworks[C]//Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long papers). Online: Association for Computational Linguistics, 2021: 565-576.

[38] Hu Zhuhua, Bai Yong, Huang Mengxing, et al. A self-adaptive progressive support selection scheme for collaborative wideband spectrum sensing[J]. Sensors, 2018, 18(9): 3011.

[39] Li Xianghui, Hu Xianghui, Shen Chong, et al. TFF_aDCNN: A pre-trained base model for intelligent wideband spectrum sensing[J]. IEEE Transactions on Vehicular Technology, 2023, 72(10): 12912-12926.

[40] Hu Zhuhua, Bai Yong, Zhao Yaochi, et al. Adaptive and blind wideband spectrum sensing scheme using singular value decomposition[J]. Wireless Communications and Mobile Computing, 2017, 2017(1): 3279452.

[41] Chen Zhiqian, Chen Fanglan, Zhang Lei, et al. Bridging the gap between spatial and spectral domains: A unified framework for graph neural networks[J]. ACM Computing Surveys, 2024, 56(5): 126.

[42] Bachman P, Hjelm R D, Buchwalter W. Learning representations by maximizing mutual information across views[C]//Proceedings of the 33rd International Confer-

ence on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2019: 1392.

[43] Sharafaldin I, Habibi Lashkari A, Ghorbani A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Funchal: SciTePress, 2018: 108-116.

[44] 胡星高. 基于小样本的网络恶意流量检测技术研究[D]. 成都: 四川大学, 2021.
Hu Xinggao. Research on network malicious traffic detection technology based on few shot[D]. Chengdu: Sichuan University, 2021. (in Chinese)

[45] Fernandes R, Lopes N. Network intrusion detection packet classification with the HIKARI-2021 dataset: A study on ML algorithms[C]//Proceedings of 2022 10th International Symposium on Digital Forensics and Security. Istanbul: IEEE, 2022: 1-5.

[46] Shi Yunsheng, Huang Zhengjie, Feng Shikun, et al. Masked label prediction: Unified message passing model for semi-supervised classification[C]//Proceedings of the thirtieth International Joint Conference on Artificial Intelligence. Montreal: International Joint Conferences on Artificial Intelligence Organization, 2021: 1548-1554.

[47] Davis J, Goadrich M. The relationship between precision-recall and ROC curves[C]//Proceedings of the 23rd International Conference on Machine Learning. Pittsburgh: ACM, 2006: 233-240.

[48] Zi Chenyi, Zhao Haihong, Sun Xiangguo, et al. ProG: A graph prompt learning benchmark[C]//Proceedings of the 38th International Conference on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2024: 3023.

作者简介

罗海桐 男,1998 年 11 月出生于四川省达州市。中国科学院计算技术研究所博士研究生。主要研究方向为图神经网络、异常检测、大语言模型。
E-mail: luohaitong21s@ict.ac.cn

孟绪颖 女,1992 年 4 月出生于湖北省随州市。中国科学院计算技术研究所副研究员。主要研究方向为智能网络、流量分析、大模型加速。
E-mail: mengxuying@ict.ac.cn

张蔚瑶 女,1995 年 12 月出生于山东省德州市。中国科学院计算技术研究所特别研究助理。主要研究方向为联邦学习、流量检测。
E-mail: zhangweiyao17z@ict.ac.cn

张玉军 男,1976 年 6 月出生于河北省衡水市。中国科学院计算技术研究所研究员。主要研究方向为智能网络与系统、网络人工智能、网络安全。
E-mail: zhmj@ict.ac.cn

林纯钢 男,2000 年 1 月出生于福建省泉州市。中国科学院计算技术研究所博士研究生。主要研究方向为流量检测。中国电子学会会员编辑:E190184461A。
E-mail: linchungang22s@ict.ac.cn