基于数据增强与特征挖掘的异常流量检测方法

安义帅[1]，付钰[1]，俞艺涵[2]，刘涛涛[1]
（1.海军工程大学信息安全系，湖北 武汉 430033；2.海军工程大学作战运筹与规划系，湖北 武汉 430033）

摘　要：针对现有异常流量检测方法存在的少数类识别精度不足及深度特征提取能力受限等问题，提出一种基于数据增强与特征挖掘的异常流量检测方法。首先，通过渐进式采样的条件生成对抗网络生成符合真实数据分布的合成样本，有效缓解类别不平衡导致的学习偏差问题；其次，基于皮尔逊相关系数计算特征关联矩阵，将流量数据转化为图结构表示，构建图数据集；最后，设计具有分层注意力机制的多层图卷积网络，通过多级邻域聚合策略实现局部与全局特征的层次化提取与融合，显著增强模型对关键特征的识别能力。实验结果表明，该方法在UNSW-NB15和CIC-IDS-2017数据集上的多分类准确率分别达到89.71%和99.84%，展现出良好的检测性能。

关键词：异常流量检测；深度学习；生成对抗网络；关联特征挖掘；图神经网络
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025145

Anomaly traffic detection method based on data augmentation and feature mining

AN Yishuai[1], FU Yu[1], YU Yihan[2], LIU Taotao[1]
1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China
2. Department of Operational Operations and Planning, Naval University of Engineering, Wuhan 430033, China

Abstract: To address the limitations of existing anomaly traffic detection methods, such as insufficient recognition accuracy for minority classes and limited deep feature extraction capabilities, a anomaly traffic detection method based on data augmentation and feature mining was proposed. Firstly, a progressive sampling-based conditional generative adversarial network was employed to generate synthetic samples that conform to the distribution of real data, effectively mitigating learning bias caused by class imbalance. Secondly, a feature correlation matrix was calculated using the Pearson correlation coefficient, transforming traffic data into graph-structured representations to construct a graph dataset. Finally, a multi-layer graph convolutional network with a hierarchical attention mechanism was designed, in which local and global features were hierarchically extracted and fused through a multi-level neighborhood aggregation strategy, significantly enhancing the model's capability to identify key features. Experimental results demonstrate that the proposed method achieves multi-class classification accuracy of 89.71% and 99.84% on the UNSW-NB15 and CIC-IDS-2017 datasets, respectively, showcasing its superior detection performance.

Keywords: anomaly traffic detection, deep learning, generative adversarial network, feature correlation mining, graph neural network

收稿日期：2025–04–12；**修回日期：**2025–08–14
通信作者：俞艺涵，yuyihan333@163.com
基金项目：国家自然科学基金资助项目（No.62102422）；河南省科技攻关基金资助项目（No.242102211070）
Foundation Items: The National Natural Science Foundation of China (No.62102422), The Key Science and Technology Research Project of Henan Province (No.242102211070)

0　引言

随着互联网技术的快速发展，网络应用在促进经济和社会进步的同时，也带来了显著的安全挑战。在日常网络环境中，用户行为、数据传输以及服务请求等基础操作均可能成为网络攻击的潜在目标。异常流量检测作为一种融合多种异常检测技术的网络流量分析方法，旨在通过识别流量中的异常模式，及时发现恶意攻击、网络入侵及数据泄露等安全威胁[1]。其在保障网络服务稳定性和信息安全可靠性方面具有重要的理论价值和实践意义。

现阶段，异常流量检测方法可分为传统方法、机器学习方法和深度学习方法3类。基于端口特征分类技术和深度包检测机制的传统方法虽可通过人工预设的规则实现基础流量识别[2]，但其特征选择高度依赖领域专家经验，在应对复杂攻击模式时因缺乏自适应学习机制导致泛化性能显著衰减。机器学习方法借助支持向量机、决策树等算法实现统计特征的自动化学习[3-4]，在一定程度上解决了上述问题，然而这类方法对非线性特征关联的建模能力明显不足，在处理高维流量数据时易引发“维度灾难”。深度学习方法凭借其端到端的表征学习优势，可通过自编码器[5]、卷积神经网络[6]和残差网络[7]等模型实现对非线性特征的深层提取，但其实际应用仍面临显著技术挑战：一方面，网络流量数据固有的类别分布不平衡特性导致模型对少数类攻击的检测精度显著低于多数类样本；另一方面，欧几里得空间建模范式的局限性使得特征间的高阶关联关系难以被有效捕捉，高维特征空间中关键异常模式因缺乏拓扑关联建模而导致漏检率上升。

针对上述问题，本文提出一种基于数据增强与特征挖掘的异常流量检测方法——CFC-Net（CW-GAN-FCM-GCN network）。该方法融合了条件Wasserstein生成对抗网络（CWGAN）、特征关联性挖掘（FCM）和图卷积神经网络（GCN）的技术优势，以提升检测性能。其核心流程包含3个阶段：首先，基于渐进式采样的CWGAN生成少数类攻击样本，有效缓解数据分布不平衡导致的学习偏差问题；其次，通过计算特征间的皮尔逊相关系数构建特征关联矩阵，将流量特征映射为包含拓扑结构的图数据表示；最后，基于分层注意力机制的多层GCN模型实现增强数据集的层次化特征提取与分类识别。本文的主要贡献如下。

1)提出了一种基于渐进式采样策略的CWGAN样本生成方法，通过生成器与判别器的对抗博弈生成高质量少数类样本，有效缓解类别不平衡问题，提升检测性能。

2)设计了一种基于特征关联性的图数据集构建方法，通过皮尔逊相关系数量化特征关联度，构建以特征为节点的拓扑结构，将原始特征数据映射为图节点属性，为GCN提供包含结构信息的输入表示。

3)提出了一种改进的GCN（IGCN, improved-GCN）框架，通过局部邻域聚合和分层注意力池化的协同机制，实现样本数据中多层次特征信息与拓扑结构信息的联合提取，提升模型的表征能力与检测鲁棒性。

4)在UNSW-NB15[8]和CIC-IDS-2017[9]数据集上的实验结果表明，本文方法在多分类准确率、F1分数等指标上显著优于现有方案，有效解决了数据不平衡与特征关联挖掘不充分的技术问题，为实际网络环境中的异常流量检测提供了理论与技术支撑。

1　相关研究工作

1.1　早期规则匹配方法

早期的异常流量检测方法主要依赖人工设计的固定规则实现流量分类。文献[10]提出一种基于数据挖掘技术的流量特征建模方法，用于检测和分析分布式相关异常事件，在处理高维数据时表现出较强的鲁棒性。文献[11]采用变换域分析理论，通过时间窗口提取转换域特征检测异常流量，不仅减少了计算开销，还在一定程度上提高了检测的实时性。文献[12]则从Web日志中提取特征，结合多种降维技术识别异常流量，实验表明，该方法能够高效地从高维数据中实时检测异常。然而，上述基于规则库的方法依赖预定义的攻击特征，无法适应当前快速变化的网络环境。

1.2　传统机器学习方法

随着机器学习技术的快速发展，基于人工特征设计的模型在异常流量分类领域得到了广泛应用。文献[13]提出了一种结合增强随机森林和合成少数类过采样技术的异常流量检测方法，有效缓解了小规模样本训练不足的问题，在NSL-KDD数据集上实现了78.47%的测试准确率。然而，该方法的实

验仅基于单一数据集，其在不同数据集上的泛化能力仍需进一步验证。文献[14]提出了一种基于秃鹰搜索优化算法改进的随机森林方法，在提升分类准确率的同时显著减少了训练时间。然而，该方法的参数设置与优化过程较为复杂，限制了其在实际应用中的可扩展性。文献[15]提出了一种基于多尺度残差分类器的异常流量检测方法，该方法融合时间观测尺度与频域分解尺度，通过残差网络深度挖掘重构误差中的判别信息，在多个数据集上实现了高检测精度和低误报率。然而，其参数调整复杂，计算成本较高。文献[16]提出了一种集成学习方法，通过多种监督学习分类器与用于无线传感器网络的软件定义网络解决方案（SDN-WISE）的深度集成，在低资源消耗的环境下实现了高精度分布式拒绝服务（DDoS）攻击检测。然而，该方法仅在模拟攻击场景下进行验证测试，其对真实环境的适应性及响应实时性有待验证。

尽管上述传统机器学习方法在异常流量检测中取得了一定成果，但仍存在泛化能力不足、计算资源需求高、实时性差以及对数据质量依赖性强等问题。

1.3 现代深度学习方法

为克服传统机器学习技术的局限性，研究者逐渐将深度学习技术引入异常流量检测领域，利用其强大的自动特征提取能力进一步提升检测性能。文献[17]提出一种基于多通道对比学习的异常流量检测方法，通过多通道对比学习实现特征重构，在CIC-IDS-2017数据集上实现了98.43%的准确率。然而，该方法依赖三元组损失函数进行对比学习，若样本选择不当，可能导致训练效果不佳。文献[18]提出一种结合残差网络（ResNet）、Transformer和双向长短期记忆网络（BiLSTM）的异常流量检测模型，融合了网络流量的时间和空间特征，在多个开源数据集上实现了较高的准确率。然而，该模型参数较多，不利于实际部署。文献[19]提出一种基于多实例学习的多粒度异常流量检测方法，能够处理海量、高维且类别不平衡的数据，在多个数据集上实现了效率提升。然而，其核心参数需手动调整，在包粒度上进行过滤时容易产生误判。

随着生成模型的发展，变分自编码器（VAE, variational autoencoder）和生成对抗网络（GAN）等技术的出现为异常流量检测提供了新的研究思路。研究者开始从数据层面展开研究，通过生成少数类异常样本缓解类不平衡问题，从而提高检测性能。文献[20]提出一种改进的条件自编码器方法，能够捕捉观测数据的复杂分布并生成指定类别的样本，在NLS-KDD数据集上显著提升了检测精度。然而，该方法对未知攻击的检测性能有限。文献[21]提出一种结合GAN和主成分分析（PCA）的异常流量检测方法，通过特征选择与降维技术提取流量的基本模式，实现了稳定且鲁棒的检测性能。然而，该方法在处理高维数据时计算复杂度较高。文献[22]提出一种基于伪异常的异常流量检测方法，结合高效特征提取框架与去噪自编码生成对抗网络，在NSL-KDD和UNSW-NB15数据集上分别达到了98.6%和98.5%的精确度。然而，其特征提取框架中时间窗口大小的选择对检测性能的影响较大。文献[23]提出一种引入判别异常值的异常流量检测方法，通过雾计算提升模型的分布式训练效率，在UNSW-NB15和CIC-IDS-2017数据集上分别取得了80.10%和82.30%的准确率。文献[24]提出一种不平衡生成对抗网络，在保证计算效率的同时提高了少数类样本的检测率，改善了整体的检测性能。然而，其对大规模数据的处理效率有待提升。

随着网络环境的日益复杂，图神经网络（GNN, graph neural network）凭借其处理非欧几里得数据的独特优势，逐渐成为异常流量检测领域的研究热点。文献[25]提出一种改进的GNN模型，通过保存流记录及其关系图结构信息，在CIC-IDS-2017数据集上取得了99.00%的F1分数，并在对抗性攻击下表现出良好的鲁棒性。然而，其图构建的复杂度较高。文献[26]提出一种名为边增强型图采样与聚合（E-GraphSAGE）的异常流量检测方法，通过捕捉图的边缘特征和拓扑信息，在多个基准数据集上的关键分类指标均优于对比方法。然而，其在高维特征嵌入时的计算开销较大。文献[27]提出一种基于双网络中心性的聚类算法，结合多头注意力机制的门控图卷积网络，在模拟数据集上实现了高异常识别率和低检测时间，同时保持了较低的内存消耗。然而，该方法对高速移动节点场景适应性有限。

综上所述，现有方法已在异常流量检测任务中取得了较好的成绩，但也在不同层面上存在不足，综合对比结果如表1所示。为兼顾生成模型和图神

表 1　　现有方法对比

方法类型	文献	核心技术	数据集	优点	局限性
早期规则匹配方法	文献[10]	熵特征提取，符号化聚类，频繁图模式挖掘	Abilene IP 级采样流数据	可区分相关与独立异常，分布式架构，计算开销低	特征工程依赖性强，泛化性能弱
	文献[11]	S 变换时频分析，源–目的流（OD）分组，高频特征分离	Abilene 真实流量数据	对高频异常敏感，滑动窗口优化效率	计算复杂度高，混合攻击检测弱
	文献[12]	2-gram 特征编码，多降维策略、Nyström 在线扩展	Apache HTTP 日志	在线扩展效率高，多降维适配不同场景	依赖明文日志，扩展映射（DM）算法实时性弱
传统机器学习方法	文献[13]	混合采样，增强随机森林，攻击相似性修正	NSL-KDD	有效处理数据不平衡问题，少数类样本检测率高	手动设定矩阵阈值，计算复杂度较高
	文献[14]	秃鹰搜索优化降维，调整基尼系数（Gini）系数和投票策略关注少数类样本	UNSW-NB15	少数类攻击检测率提升	参数设置依赖经验，可能陷入局部最优
	文献[15]	小波变换多尺度特征提取，多路径残差重构误差	KDD99、NSL-KDD、UNSW-NB15、CIC-IDS-2018	对高维数据降维效果显著，潜在特征挖掘充分	分解尺度和窗口大小需手动优化
	文献[16]	SDN-WISE 嵌入最大似然比（ML）检测模块，多分类器协同	自建数据集	支持实时异常检测，资源消耗低	依赖 SDN-WISE 控制器，泛化能力有限
现代深度学习方法	文献[17]	多通道对比学习，交叉相关矩阵特征增强	CIC-IDS-2017、KDDCUP99	多通道特征增强提升分类精度	未知攻击的泛化能力有待验证
	文献[18]	残差注意力双向长短期记忆网络（Res-TranBiLSTM）模型并行处理时空特征	NSL-KDD、CIC-IDS-2017、MQTTset	融合时空特征，检测准确率高	模型参数较多，部署困难
	文献[19]	包生成过滤，多粒度分类	CIC-IDS-2018、KDD99、DoH2020、UNSW-NB15	大规模数据处理效率高，对不平衡数据鲁棒	性能略低于单例模型，核心参数需手动调优
	文献[20]	对数双曲余弦损失函数优化生成与重构平衡	NSL-KDD	生成样本多样性高，少数类识别能力强	未知攻击类型检测效果有限
	文献[21]	主成分分析特征降维，GAN 样本生成	Kaggle 网络流量数据集	准确率高，训练过程稳定	高维数据处理时计算复杂度较高
	文献[22]	数据包窗口特征提取，多去噪自编码（DAE）数据增强	NSL-KDD、UNSW-NB15、Kitsune	处理高维空间时效率高	窗口大小和特征选择需手动优化
	文献[23]	雾计算环境实现分布式训练，降低通信开销	UNSW-NB15、CIC-IDS-2017	支持实时检测，对高维数据表征能力强	雾节点通信开销大
	文献[24]	朴素贝叶斯特征嵌入，生成高质量数据	UNSW-NB15、CIC-IDS-2017、NSL-KDD、Kyoto 2006	误报率低，模型可解释性强	大规模数据处理效率有待提升
	文献[25]	主机连接图表示流量关系，捕捉结构模式	CIC-IDS-2017	对抗攻击的鲁棒性强	图构建复杂度高
	文献[26]	扩展图采样与聚合（GraphSAGE）算法，支持边缘特征和拓扑信息处理	物联网僵尸网络数据集（BoT-IoT）、遥测与操作网络物联网数据集（ToN-IoT）、NetFlow 格式的遥测与操作网络物联网数据集（NF-ToN-IoT）、NetFlow 格式的物联网僵尸网络数据集（NF-BoT-IoT）	边缘分类能力强，支持大规模数据的高效处理	高维特征嵌入计算开销大
	文献[27]	多头自注意力机制与门控图卷积网络，长鼻浣熊优化算法（Coati）优化簇头选择	移动自组网（MANET）环境下的模拟数据集	检测率高，适应 MANET 节点移动性	对高速移动节点场景适应性有限

经网络的优势，本文提出了CFC-Net，该方法不仅有效解决了类别不平衡问题，还通过挖掘流量特征间的关联关系，充分捕捉数值特征与结构特征，显著提升了检测性能。

2　相关理论基础

2.1　生成对抗网络

GAN是一种融合博弈论、概率论、优化理论及深度学习等多学科理论的生成模型，其核心机制源于博弈论中的“极小化极大”策略。该模型由生成器（G, generator）与判别器（D, discriminator）构成对抗框架，生成器通过映射随机噪声向量至数据空间，生成逼近真实分布的样本；判别器则负责区分真实样本和生成样本。二者通过对抗博弈优化参数，逐步缩小生成分布与真实分布的差异，进而实现数据增强，缓解类不平衡问题带来的影响。然而，传统的GAN基于詹森–香农散度（JS，Jensen-Shannon）度量分布差异，如图1所示，当分布无重叠时无法准确刻画差异，导致训练过程中常出现模式崩溃与稳定性问题。

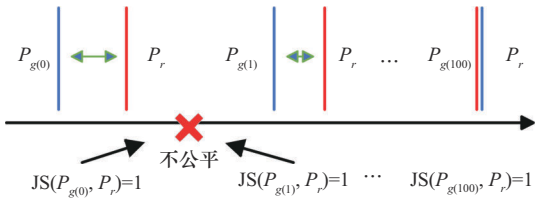

图1　JS散度的局限性

为解决上述缺陷，Wasserstein生成对抗网络（WGAN）引入Wasserstein距离替代JS散度，其通过计算将一个分布转换为另一个分布的最小“搬运成本”，有效度量非重叠分布差异，其目标函数定义为

$$\max_{D\in 1-\text{Lipschitz}}\left\{E_{x\sim p_x}\left[D(x)\right]-E_{x\sim p_g}\left[D(x)\right]\right\} \quad (1)$$

其中，x表示真实流量数据样本，p_x表示真实数据分布，p_g表示生成数据分布，$D\in 1-\text{Lipschitz}$表示对于任意输入x_1和x_2，判别器的输出满足$\|D(x_1)-D(x_2)\|\leqslant\|x_1-x_2\|$，从而保证了判别器的梯度稳定性。

针对网络异常流量数据类别分布高度不平衡的固有特性，本文提出一种基于渐进式采样策略的条件Wasserstein生成对抗网络（SS-CWGAN, step-wise sampling conditional Wasserstein GAN）模型，其结构如图2所示。

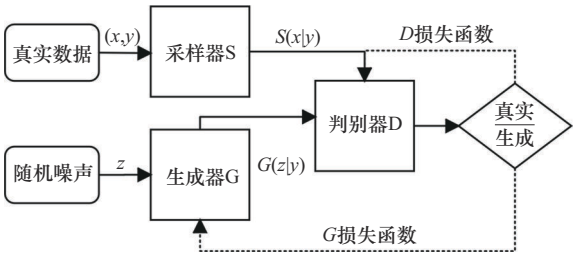

图2　SS-CWGAN模型结构

SS-CWGAN模型在WGAN理论框架基础上，通过将类别标签作为条件变量引入生成对抗网络，构建条件约束机制以提升生成样本的类别辨识度与质量。创新性地设计渐进式扩展采样空间的训练策略，在对抗学习过程中采用层次化训练范式。初始阶段聚焦基础特征学习，随后通过动态调整采样空间的层次化训练机制，逐步增强模型对细粒度特征的刻画能力。这种渐进式训练方法有效缓解了生成器过早收敛于局部最优解所导致的模式崩溃现象，在保证生成样本质量的同时显著提升了异常流量样本的多样性。由于SS-CWGAN模型基于WGAN改进而来，因此其判别器损失函数可表示为

$$\max_{D\in 1-\text{Lipschitz}}\left\{E_{\hat{x}\sim p_x}\left[D(\hat{x}|y)\right]-E_{\hat{x}\sim p_g}\left[D(\hat{x}|y)\right]\right\} \quad (2)$$

生成器的目标函数可表示为

$$\min_G\left\{-E_{z\sim p_z}\left[D(G(z|y)|y)\right]\right\} \quad (3)$$

其中，$\hat{x}$表示采样流量数据样本，y表示类别标签，z表示服从高斯分布的噪声向量。

2.2　图卷积神经网络

GCN是一种突破欧几里得空间限制的深度学习架构，其核心思想源于谱图理论、流形学习及消息传递机制。传统卷积神经网络在处理图像等规则网格数据时表现出色，但面对网络流量等特征间存在复杂拓扑关联的非欧几里得数据时，因缺乏平移不变性而建模能力受限。GCN通过推广卷积操作至图结构数据，实现对节点特征与拓扑关系的联合建模，为异常流量检测中的高阶关联特征挖掘提供了理论支撑。标准GCN通过邻域聚合机制更新节点表示，其单层操作定义为

$$\boldsymbol{H}^{(l+1)}=\sigma\left(\tilde{\boldsymbol{D}}^{-\frac{1}{2}}\tilde{\boldsymbol{A}}\tilde{\boldsymbol{D}}^{-\frac{1}{2}}\boldsymbol{H}^{(l)}\boldsymbol{W}^{(l)}\right),\boldsymbol{H}^{(0)}=\boldsymbol{X} \quad (4)$$

其中，$\boldsymbol{X}\in\mathbb{R}^{N\times F}$代表图结构数据的特征矩阵，表示有$N$个节点，每个节点包含$F$个特征属性，$\tilde{\boldsymbol{A}}=\boldsymbol{A}+\boldsymbol{I}$表示添加自环的邻接矩阵（$\boldsymbol{A}$是图结构数据的邻接矩阵，$\boldsymbol{I}$是单位矩阵），$\tilde{\boldsymbol{D}}_{ii}=\sum_j\tilde{\boldsymbol{A}}_{ij}$表示度矩阵，$\boldsymbol{H}^{(l)}$表示第$l$层节点特征，$\boldsymbol{W}^{(l)}$表示第$l$层的可学习权重矩阵，$\sigma(\cdot)$表示非线性激活函数。

GCN通过多层堆叠实现层次化特征提取，浅层通过聚合一阶邻域信息，捕捉单条流量局部结构模式；深层通过k阶邻域（k-hop）聚合，学习跨流量的全局拓扑规律。然而，标准GCN在深层卷积过程中易稀释局部异常模式，在异常流量检测中易导致细粒度攻击漏检。此外，全局平均等传统池化操作容易忽略节点重要性差异，导致过平滑问题。

针对上述问题，本文提出了IGCN模型，该模型通过分层注意力机制计算节点级注意力权重，实现差异化特征聚合，并结合局部图卷积与全局注意力池化实现层次化特征融合。上述2个过程的数学表达式为

$$\boldsymbol{\alpha}_{ij}=\frac{\exp\left(\text{LeakyReLU}\left(\boldsymbol{a}^{\mathrm{T}}\left[\boldsymbol{W}\boldsymbol{h}_i\|\boldsymbol{W}\boldsymbol{h}_j\right]\right)\right)}{\sum\limits_{k\in\mathcal{N}_i}\exp\left(\text{LeakyReLU}\left(\boldsymbol{a}^{\mathrm{T}}\left[\boldsymbol{W}\boldsymbol{h}_i\|\boldsymbol{W}\boldsymbol{h}_j\right]\right)\right)}\tag{5}$$

$$\boldsymbol{h}_G=\sum_{i=1}^{N}\beta_i\boldsymbol{h}_i,\beta_i=\frac{\exp\left(\boldsymbol{q}^{\mathrm{T}}\tanh\boldsymbol{V}\boldsymbol{h}_i\right)}{\sum\limits_j\exp\left(\boldsymbol{q}^{\mathrm{T}}\tanh\boldsymbol{V}\boldsymbol{h}_i\right)}\tag{6}$$

其中，$\boldsymbol{h}_i$表示节点i的特征信息，$\boldsymbol{a}$为可学习向量，$\boldsymbol{W}$为权重矩阵，$\mathcal{N}_i$为节点i的邻居集合，$\boldsymbol{q}$为查询向量，$\boldsymbol{V}$为投影矩阵，β_i表示节点i的全局重要性权重。通过式(5)~式(6)的协同机制，IGCN可显著增强模型对关键异常模式的辨识能力，提高异常流量的检测精度。

3　异常流量检测

针对类别不平衡与特征关联挖掘不充分的挑战，本文分别从数据层、表示层和模型层出发，构建了涵盖数据预处理、数据增强、图数据集构建和异常流量检测的系统化解决方案，其总体架构如图3所示。首先，通过数据预处理提升数据质量，并基于SS-CWGAN生成符合真实分布的少数类样本，缓解学习偏差；其次，利用皮尔逊相关系数构建特征关联图，将流量数据转化为包含结构信息的图数据集；最后，通过IGCN的层次化特征提取与分层注意力机制实现局部邻域特征与全局结构特征的融合，提升关键特征识别能力。

3.1　数据预处理

在深度学习任务中，数据质量的优劣从根本上决定了模型学习的上限，为提升数据质量，本文对原始数据进行了预处理操作，具体步骤如下。

1) 数据清洗。在监督学习过程中，标签缺失样本无法提供有效的监督信息，其存在会破坏损失函数的可导性。设数据集$D=\{x_i,y_i\}_{i=1}^{N}$，当$y=$NaN时，监督损失函数$\mathcal{L}(\theta)=l\left(f_\theta(x_i),y_i\right)$会因无法计算$\nabla_\theta l$而失效。为保证数据的有效性，本文在实验过程中移除了缺失类别标签的无效样本。

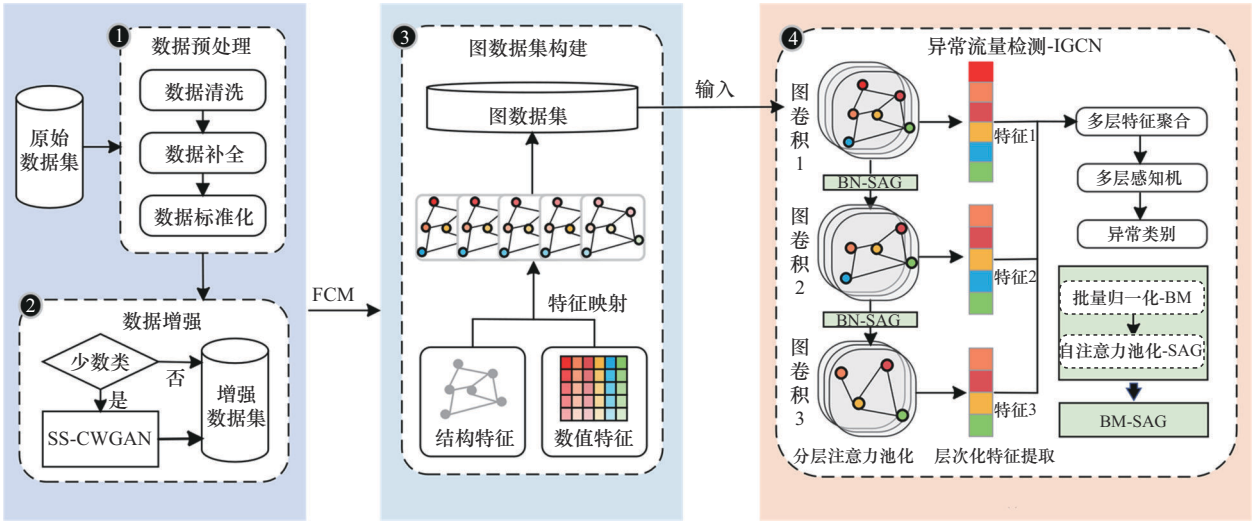

图3　CFC-Net异常流量检测总体框架

2) 数据补全。图卷积计算依赖连续可导的数值运算，空缺值的存在会破坏数据的数学连续性，导致矩阵运算报错、梯度反向传播中断以及模型参数更新失效等问题。为保证数据的完整性，同时兼顾异常流量数据类别不平衡和特征分布偏斜的特性，本文决定对可能存在的空缺值进行补全。假设特征j服从对数正态分布$X_j = \mathrm{LogNormal}\left(\mu,\sigma^2\right)$。

当使用中位数$\mathrm{Median}\left(X_j\right)$填充缺失值时，其数学期望

$$E_{\mathrm{median}} = \left|\mathrm{Median}\left(X_j\right) - x_{\mathrm{true}}\right| \leqslant C\sigma \tag{7}$$

其中，C为常数，σ为标准差，因而中位数填充误差受σ线性约束，对离群点不敏感。

当使用均值进行填充缺失值时，其数学期望

$$E_{\mathrm{mean}} = \left|\mu - x_{\mathrm{true}}\right| \propto \mathrm{e}^{\sigma^2} \tag{8}$$

其中，μ为样本均值。若DDoS攻击产生超大流量包，即存在离群点时，σ^2会显著增大，进而使均值被拉向尾部，导致误差呈指数级增长。

尽管中位数填充时的时间复杂度为$O(n\mathrm{lb}n)$高于均值填充的$O(n)$，为准确反映数据的中心趋势，避免因少数异常样本而产生偏差，进而提升模型整体的检测性能，本文仍采用基于中位数的差值方法对空缺值进行补全处理。

3) 数据标准化。为进一步优化特征空间，保证特征一致性，本文对字符型特征实施数值化编码，并基于Z-score标准化方法对所有数值特征进行归一化处理，最终构建了符合机器学习建模要求的规范化数据集。

3.2 数据增强

由于纳什均衡的不稳定性，传统GAN及其衍生模型在实际训练过程中往往会因判别器的快速优化导致生成器陷入局部最优。为保证对抗训练过程的动态优化，生成高质量少数类样本以缓解类不平衡问题，本文提出了SS-CWGAN模型，其核心改进在于渐进式采样策略的建构，具体实现方法如算法1所示。

算法1 数据增强方法

输入 规范化数据集$\left(\boldsymbol{X}',\boldsymbol{y}'\right)$，少数类标签集合$C_{\mathrm{minor}} = \left\{c_1,c_2,\cdots,c_k\right\}$，最大迭代次数$T$，采样率$\rho$

输出 增强数据集$\left(\boldsymbol{X}'_{\mathrm{aug}},\boldsymbol{y}'_{\mathrm{aug}}\right)$

for $t \leftarrow 1$ to T do//渐进式采样

$\boldsymbol{X}'_s,\boldsymbol{y}'_s \leftarrow \mathrm{Samper}\left(\boldsymbol{X}',\boldsymbol{y}',C_{\mathrm{minor}},\rho\right)$

//样本生成

$z \sim \mathcal{N}\left(0,\boldsymbol{I}_{d_z}\right)$//随机噪声

$\boldsymbol{X}_g \leftarrow \mathrm{Generator}\left(z|\boldsymbol{y}'_s = C_{\mathrm{minor}}\right)$

//判别器训练

$\mathcal{L}_D = \max_{D\in 1-\mathrm{Lipschitz}}\left\{E_{x\sim p_s}\left[D\left(x|y\right)\right] - E_{x\sim p_g}\left[D\left(x|y\right)\right]\right\}$

$\theta_D \leftarrow \theta_D - \eta\nabla\theta_D\mathcal{L}_D$//参数更新

//生成器更新

$\mathcal{L}_G \leftarrow \min_G\left\{-E_{z\sim p_z}\left[D\left(G\left(z|y\right)|y\right)\right]\right\}$

$\theta_G \leftarrow \theta_G - \eta\nabla\theta_G\mathcal{L}_G$//参数更新

//数据增强

$\boldsymbol{X}'_{\mathrm{aug}},\boldsymbol{y}'_{\mathrm{aug}} \leftarrow \mathrm{Concat}\left(\boldsymbol{X}'_s,\boldsymbol{X}_g\right)$, $\mathrm{Concat}\left(\boldsymbol{y}'_s,\{\mathrm{minor\_label}\}\right)$

return $\boldsymbol{X}'_{\mathrm{aug}},\boldsymbol{y}'_{\mathrm{aug}}$

由算法1可知，该模型在原CWGAN模型的基础上通过设计线性扩张的采样率序列实现了采样分布$P_s^{(t)}$依总变差距离收敛至真实分布P_{data}的效果，这一收敛特性保障了生成对抗过程中的动态优化性质。在初始阶段，生成器优先学习多数类主导模式（如DDoS攻击），通过约束采样空间显著抑制损失函数振荡；在生成对抗的终局阶段，生成器逐渐聚焦于少数类长尾模式（如心脏出血漏洞（Heartbleed）），避免了高维空间中的梯度冲突现象。

3.3 图数据集构建

图卷积的运算机制依赖图的拓扑结构，为充分挖掘异常流量数据中的特征关联与结构模式，本文将图级别分类任务作为核心目标，通过构建图结构化表示融合流量数据的特征信息和结构信息。

在网络流量场景中，DDoS攻击等典型异常中包速率λ、包长度L等特征存在的显式线性约束，如带宽模型$B = \lambda \times L \times 8$。采用皮尔逊相关系数（PCC）$R\left(X_j,X_k\right) = \dfrac{\mathrm{Cov}\left(X_j,X_k\right)}{\sigma_{X_j}\sigma_{X_k}} \in [-1,1]$量化特征间的依赖关系，不仅可以充分捕捉流量数据中的线性关系，还为图拓扑结构的稀疏化处理提供了标准化度量。此外，当样本数量为n、特征维度为d时，

相较于时间复杂度为$O\left(n^2d^2\right)$的互信息法，其计算复杂度$O\left(nd^2\right)$更契合网络流量实时检测需求。

尽管PCC难以直接捕捉非线性关联，但GCN可以通过多层邻域聚合机制实现间接建模。根据图信号处理理论，图卷积本质上是在图拓扑结构上执行的高阶多项式滤波，当存在特征路径$X_j \to X_k \to X_m$时，即使$R\left(X_j,X_m\right) \approx 0$，即$X_j$与$X_m$直接线性相关性弱，信号仍可通过中间节点$X_k$的迭代聚合传递非线性依赖关系。

在实际的构建过程中，本文将原始流量特征j映射为节点v_j，并将其特征值x_j映射为节点值$x_i^{(j)}$以保留原始特征的微分信息，这一操作确保了GCN卷积层可直接访问特征数据，避免了信息损失。与此同时，本文以PCC值构建加权边，通过阈值τ控制关联矩阵的边密度，以此来平衡计算效率与结构有效性。由图卷积的k阶邻居传播理论可知，当τ过低时，容易引入弱相关边，导致图结构噪声增加，进而引发GCN的过平滑问题；而τ设置过高又会割裂关键特征间的关联路径，阻碍信息传递，导致模型欠拟合问题。网络流量统计表明，80%的显著特征关联满足$|\boldsymbol{R}|\geqslant 0.6$，基于此，本文基于默认值$\tau = 0.65$构建加权关联矩阵以有效保留流量数据中的核心关联模式，同时过滤90%的弱相关边，从而降低图卷积过程的计算复杂度。

3.4　异常流量检测模型

传统GCN模型凭借对非结构特征的捕获能力在异常流量检测任务中取得了显著成效。然而，随着网络层数的增加，容易丢失节点间的区分性，出现过平滑问题。为充分利用各卷积层的特征信息，提升模型的表征能力，本文提出了IGCN框架，其实现过程如图4(c)所示，具体的实现方法如算法2所示。

算法2　异常流量检测方法

输入　图数据集$\mathcal{G} = \left\{G_i,y_i\right\}_{i=1}^{n}$，图卷积层数$L$，隐藏层维度$d_h$

输出　检测结果$\hat{y} \in \mathbb{R}^{n \times k}$（$k$为类别数）

1) //模型初始化

2) $\mathrm{GConv}_l \leftarrow \mathrm{GraphConv}\left(d_{\mathrm{in}},d_h\right), \forall l \in \{1,\cdots,L\}$

3) $\mathrm{BN}_l \leftarrow \mathrm{BatchNorm}\left(d_h\right)$

4) $\mathrm{AttPool}_l \leftarrow \mathrm{AttentionPool}\left(d_h\right)$

5) $\mathrm{MLP} \leftarrow \mathrm{MultiLayerPerceptron}\left(L \cdot d_h,k\right)$

6) for $i \leftarrow 1$ to n do

7) $\quad \boldsymbol{H}_i^{(0)} \leftarrow \boldsymbol{V}_i\left(\boldsymbol{V}_i \in G_i\right)$//初始化节点特征

8) $\quad \boldsymbol{F}_{\mathrm{global}} \leftarrow [\cdot]$//全局特征

9) $\quad$//特征提取与聚合

10) $\quad$ for $l \leftarrow 1$ to L do

11) $\quad\quad \boldsymbol{H}_i^{(l)} \leftarrow \mathrm{ReLU}\left(\mathrm{GConv}_l\left(\boldsymbol{H}_i^{(l-1)},\boldsymbol{E}_i\right)\right)$//图卷积，$\boldsymbol{E}_i$表示与节点$i$相关的边信息

12) $\quad\quad \boldsymbol{H}_i^{(l)} \leftarrow \mathrm{BN}_l\left(\boldsymbol{H}_i^{(l)}\right)$//批量归一化

13) $\quad\quad \boldsymbol{a}^{(l)} \leftarrow \mathrm{AttPool}_l\left(\boldsymbol{H}_i^{(l)}\right)$//自注意力池化

14) $\quad\quad \boldsymbol{H}_{\mathrm{pool}}^{(l)} \leftarrow \sum_{j=1}^{n_i} a_j^{(l)} h_j^{(l)}$

15) $\quad\quad \boldsymbol{F}_{\mathrm{global}} \leftarrow \boldsymbol{F}_{\mathrm{global}} \oplus \boldsymbol{H}_{\mathrm{pool}}^{(l)}$//特征聚合，其中$\oplus$表示注意力权重融合

16) $\hat{y}_i \leftarrow \mathrm{Softmax}\left(\mathrm{MLP}\left(\boldsymbol{F}_{\mathrm{global}}\right)\right)$//检测结果

17) return $\hat{y}$

由图4(c)可知，相较于传统GCN，IGCN通过层次化特征提取和分层注意力池化机制实现对过平滑问题的缓解。

在层次化特征提取层面，传统GCN依赖一阶邻域聚合，虽可通过增加网络层数捕捉高阶拓扑关系，却不可避免导致节点特征在多层传播中逐渐同质化。IGCN则通过自适应k阶邻域加权聚合框架，直接将k阶邻域（k≥1）特征纳入卷积运算，通过多层级传播范式实现“局部拓扑–全局结构”的渐进式特征融合。这种设计避免了传统模型因过度依赖深层网络引发的特征坍塌问题，使模型能在更少的层数内捕获高阶依赖关系，从根本上降低了过平滑发生的概率。

在分层注意力池化层面，IGCN在每层卷积后通过自适应学习特征维度的重要性权值，动态抑制与任务无关的冗余特征，进而引导模型聚焦于更具判别性的关键特征。同时，跨层特征融合策略进一步将多层级特征空间的非线性特征组合生成多尺度增强表示，避免单一高层特征因过度平滑而丢失细节。这种“动态筛选–跨层融合”机制，确保了节点表示在高阶聚合过程中仍能保留差异化特征。

4　实验与结果分析

4.1　数据集说明

UNSW-NB15数据集由澳大利亚新南威尔士大学研究团队于2015年发布，用于替代KDD Cup 1999数据集，为异常流量分析提供更贴近真实网络环境的数据支持。数据集涵盖多种攻击类型和正常流量，能反映当前网络威胁多样性，为网络安全研究与应用提供重要数据基础，流量样本分布如表2所示。

表2　　UNSW-NB15流量样本分布

类别	训练样本数/个	测试样本数/个
Normal	56 000	37 000
DoS	12 264	4 089
Fuzzers	18 184	6 062
Analysis	2 000	677
Backdoor	1 746	583
Exploits	33 393	11 132
Generic	40 000	18 871
Reconnaissance	10 491	3 496
Shellcode	1 133	378
Worms	130	44
合计	175 341	82 332

CIC-IDS-2017数据集由加拿大网络安全研究所于2017年发布，是当前规模较大且极具代表性的异常流量检测基准数据集，包含多种正常与异常流量，提供80多个特征属性，可全面反映现代网络流量多样性与复杂性，为相关研究提供高质量数据支持。因实验条件限制，本文选取周三数据集实验，流量样本分布如表3所示。

表3　　CIC-IDS-2017流量样本分布

类别	训练样本数/个	测试样本数/个
Benign	351 719	87 964
DoS Hulk	183 998	46 126
DoS GoldenEye	8 307	1 986
DoS Slowloris	4 648	1 148
DoS Slowhttptest	4 444	1 055
Heartbleed	8	3
合计	553 124	138 282

4.2　实验设置

实验环境：编程语言为Python 3.9，深度学习框架为PyTorch，集成开发环境为PyCharm 2018。硬件配置包括NVIDIA RTX 4090D GPU（24 GB显存）和AMD EPYC 9754 128核处理器（18 vCPU）。

参数设置：涵盖了数据采样、模型训练和优化策略等多个方面，旨在通过合理的超参数配置提升模型性能。实验采用Adam优化器并结合交叉熵损失函数，以优化模型训练过程并避免梯度弥散问题。通过科学调整学习率、批处理大小和迭代轮次等关键参数，为后续的性能评估提供了可靠的基础。具体如表4所示。

表4　　模型参数设置

模块	参数	设置值
SS-CWGAN	迭代轮次	500
	采样率	0.25
	批处理大小	64
	优化器	Adam
	学习率	0.0008
IGCN	迭代轮次	500
	批处理大小	256
	优化器	Adam
	权重衰减系数	5×10^{-4}

上述实验环境与参数设置确保了模型训练的高效性与稳定性，为性能评估提供了可靠基础。

4.3　性能评价指标

在完成异常流量分类任务之后，本节实验以准确率（Acc, accuracy）、召回率（Rec, recall）、精确率（Pre, precision）、F1分数（F1-Score）以及误报率（FAR, false alarm rate）5个评价指标，综合评价模型的性能。各指标的计算式为

$$\mathrm{Acc}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{FP}+\mathrm{TN}+\mathrm{FN}} \tag{9}$$

$$\mathrm{Rec}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{10}$$

$$\mathrm{Pre}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \tag{11}$$

$$\mathrm{F1\text{-}Score}=\frac{2\mathrm{Pre}\times\mathrm{Rec}}{\mathrm{Pre}+\mathrm{Rec}} \tag{12}$$

$$\mathrm{FAR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{13}$$

其中，真阳性（TP, true positive）表示正类别中被正确分类样本的数量，真阴性（TN, true negative）表示负类别中被正确分类样本的数量，假阳性（FP, false positive）表示正类别中被错误分类样本的数量，假阴性（FN, false negative）是负类别中被错误分类样本的数量。通过对上述评价指标的综合分析，能够全面评估模型的分类性能，验证本文方法的有效性和实际应用价值。

4.4　生成模型训练

在使用GAN进行数据生成时，判别器的损失值达到零和博弈状态的标志是其对真实数据和生成数据的判别能力趋于平衡。当判别器对真实数据和生成数据的输出概率均接近0.5时，表明其无法有效区分真实数据与生成数据，此时GAN达到了纳什均衡状态，对应的损失值为$\ln 0.5 \approx 0.693$。

对于CWGAN而言，其损失函数采用Wasserstein距离替代JS散度，因此损失值不会收敛于0.693。在理想情况下，当生成器生成的样本分布p_g与真实数据分布p_r完全一致时，Wasserstein距离$W\left(p_r,p_g\right)=0$。此时，判别器对真实数据和生成数据的评分应该相等，因此，判别器的损失函数可表示为

$$L_D = E_{x\sim p_r}\left[D\left(x|y\right)\right] - E_{z\sim p_z}\left[G\left(z|y\right)|y\right] \approx 0 \qquad (14)$$

此时，判别器的损失曲线将收敛至接近0的值。此外，由于判别器的梯度满足一阶利普希茨（1-Lipschitz）连续性，梯度惩罚项也会趋近于0，因此CWGAN的整体损失函数将趋近于0。

为验证本文SS-CWGAN模型的有效性，以UNSW-NB15数据集中的DoS和Backdoor这2类样本为例，计算了在训练过程中判别器的损失值。DoS类数据生成训练过程中判别器的损失函数如图4所示，Backdoor类数据生成训练过程中判别器的损失函数如图5所示。

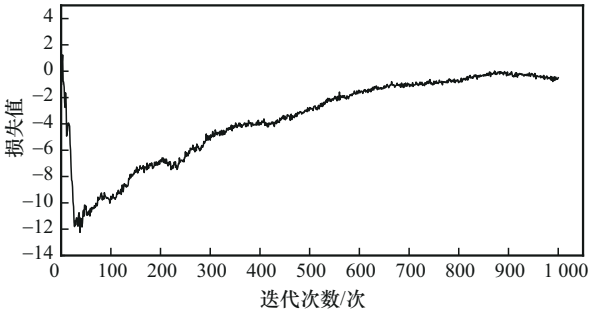

图4　DoS类数据生成训练过程中判别器的损失函数

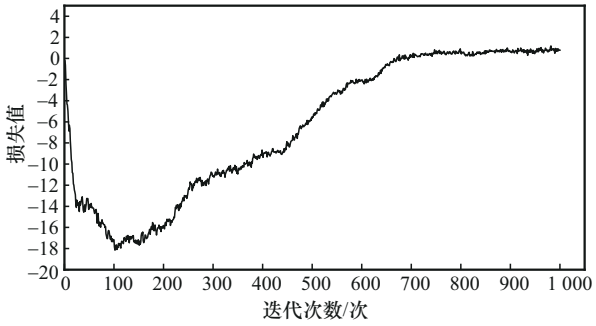

图5　Backdoor类数据生成训练过程中判别器的损失函数

由图4和图5可知，在数据生成的初始阶段，2类数据的判别器损失值均接近于0。随着迭代次数的增加，生成器生成的数据质量逐步提升，导致判别器的损失值显著下降。随后，在生成器与判别器的对抗博弈过程中，判别器的损失值逐渐回升，并最终收敛于近0的稳定状态。这一现象表明生成模型的训练达到了纳什均衡，即生成器能够生成与真实数据分布高度一致的样本，而判别器无法有效区分生成样本与真实样本。基于此，可以认为本文模型生成的样本具有较高的可靠性，能够有效缓解异常流量数据集中的类别不平衡问题，从而改善下游分类任务中模型对多数类样本的过拟合倾向。

为规避生成对抗训练中的模式崩溃问题，本文提出了渐进式采样策略，通过采样率的线性扩张机制确保网络动态优化过程的稳定性。在实际过程中，以固定步长（$\Delta r = 0.25$）逐步提升SS-CWGAN的采样率进行训练。不同采样率下分类模型的运行时长如图6所示。

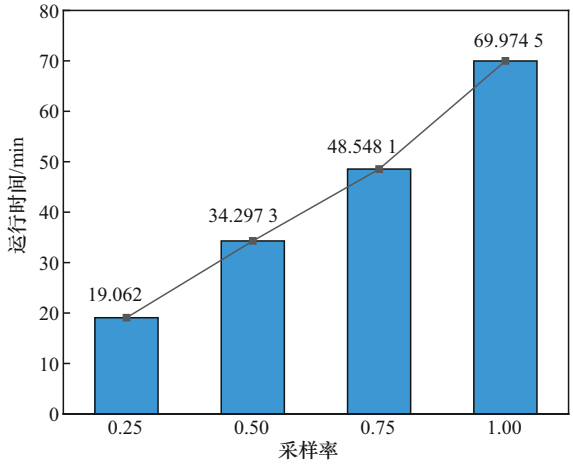

图6　不同采样率下分类模型的运行时长

实验数据显示，当采样率从初始值逐步提升至上限时，单次训练耗时由开始的约19 min递增至约

70 min，近似呈现线性增长趋势。这一现象表明，随着样本空间复杂度提升，生成器在逐步扩展的采样空间中始终保持稳定收敛，未出现样本多样性失控导致的发散现象，且判别器始终能有效区分真假样本。时间消耗的线性增长佐证了模型的动态优化机制——生成器依序学习从多数类主导模式到少数类长尾特征的分布结构，此过程规避了传统GAN在高维空间中的梯度冲突问题。该线性增长本质上是SS-CWGAN为实现质量与多样性平衡的必要代价，相较于指数级增长的时间消耗（如模式崩溃时出现的训练振荡），线性特性印证了本文模型通过总变差距离收敛抑制模式崩溃的理论优势。

4.5　分类模型训练

为充分挖掘流量数据中的邻域特征与结构特征，本文构建了IGCN异常流量检测模型，在实际的模型训练中，分别对采样率为0.25、0.50、0.75和1.00的生成数据进行特征学习。以UNSW-NB15数据集为例，不同采样率下分类模型训练过程中的损失函数如图7所示。

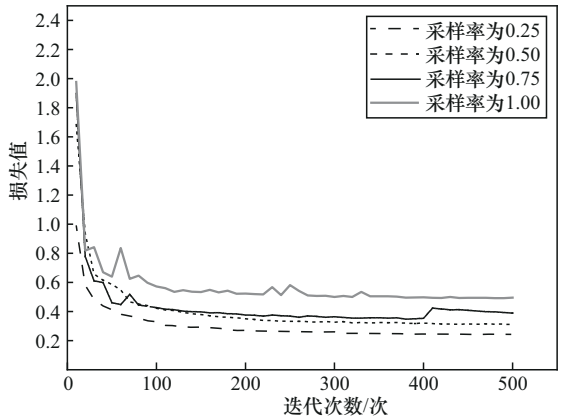

图7　不同采样率下分类模型训练过程中的损失函数

从图7可以看出，经过多次迭代训练后，本文提出的分类模型在不同采样率数据集下的损失函数均能够较好地收敛。然而，不同采样率数据集对应的损失函数最终收敛于不同的稳定值，且随着采样率的增加，损失值逐渐增大，模型收敛所需的迭代次数也显著增加。为深入分析这一现象的原因，本文进一步对比了不同采样率下分类模型的性能指标，具体结果如表5所示。

由表5可知，当采样率为0.25时，分类模型在5个性能指标上均达到最优，随着采样率的增加，模型性能呈现下降趋势。当采样率为1.00时，训练集的准确率、精确率、召回率和F1分数较采样率为0.25时分别下降了2.86%、2.42%、2.69%和2.38%，同时，误报率增加了0.32%。

表5　不同采样率下分类模型性能对比结果

采样率	数据集	Acc	Pre	Rec	F1-Score	FAR
0.25	训练集	92.50%	92.57%	92.34%	91.99%	0.83%
	测试集	91.78%	91.99%	91.78%	91.72%	0.91%
0.50	训练集	91.58%	91.78%	91.59%	91.54%	0.93%
	测试集	91.61%	91.88%	91.62%	91.57%	0.93%
0.75	训练集	90.19%	90.75%	90.18%	90.95%	1.00%
	测试集	91.02%	91.14%	91.04%	90.81%	0.99%
1.00	训练集	89.64%	90.15%	89.65%	89.61%	1.15%
	测试集	89.71%	90.24%	89.72%	89.68%	1.14%

出现这一现象的原因在于，低采样率下的SS-CWGAN主要关注对基础特征的表征，对细粒度特征的刻画能力不足。因此，生成样本的特征较为单一，无法充分表征所有样本的真实分布，使得分类模型能够快速捕获关键特征并达到较高性能，但这种性能提升并不能完全反映真实场景下的检测能力。随着采样率提高，少数类特征的多样性增加，生成器能够生成质量更高、多样性更好的增强数据，但分类模型需要更多迭代轮次才能达到稳定状态。此外，数据复杂性的增加导致分类模型性能指标略有下降，尽管这些结果并非最优，但更能反映实际场景下的真实检测水平。本文模型与其他检测方法的详细对比分析将在后续章节展开。

4.6　类平衡方法对比

数据增强作为异常流量检测的上游任务，是实现高性能异常检测的关键环节。只有在数据增强过程中生成高质量的数据，有效缓解原始数据集中的类别不平衡问题，才能在下游分类任务中取得优异的检测效果。为验证本文类平衡方法的有效性，将其与传统的采样方法及主流的生成模型方法进行对比。考虑到真实网络环境中不同攻击类型通常需要不同的防御策略，单纯的二分类检测难以满足实际要求，因此本文在实验设计对比分析中直接以多分类异常流量检测为目标，具体对比结果如表6所示，其中加粗字体表示最优结果。

由表6可知，在UNSW-NB15数据集上，本文方法在多个性能指标上均优于其他6种对比方法。

表6　本文方法与传统的采样方法以及深度生成模型方法对比结果

数据集	方法	Acc	Pre	Rec	F1-Score	FAR
UNSW-NB15	随机采样（ROS）[28]	81.70%	77.32%	94.49%	85.05%	33.96%
	合成少数类过采样（SMOTE）[28]]	82.44%	78.05%	94.77%	85.60%	32.65%
	自适应合成采样（ADASYN）[28]	82.15%	77.76%	94.65%	85.38%	33.16%
	WGAN[29]	81.49%	84.71%	82.51%	83.60%	—
	CWGAN[29]	85.59%	86.11%	85.57%	85.84%	—
	VAE-CWGAN[30]	87.58%	89.22%	87.58%	88.39%	8.85%
	本文方法	89.71%	90.24%	89.72%	89.68%	1.14%
CIC-IDS-2017	VAE-CWGAN[30]	99.79%	99.79%	**99.79%**	99.79%	0.19%
	ROS[31]	99.76%	99.81%	99.76%	99.77%	—
	SMOTE[31]	99.76%	99.83%	99.76%	99.77%	—
	ADASYN[31]	99.76%	99.83%	99.76%	99.77%	—
	随机欠采样结合合成少数类过采样（RUS+SMOTE）[32]	99.72%	99.81%	99.72%	99.75%	—
	K均值聚类欠采样结合合成少数类过采样（K-means+SMOTE）[32]	99.70%	99.81%	99.70%	99.74%	—
	本文方法	**99.84%**	**99.97%**	99.74%	**99.83%**	**0.12%**

其主要原因在于，传统欠采样方法可能导致多数类样本信息丢失，从而降低模型对多数类的检测精度；而过采样方法基于差值运算生成新样本，容易引入冗余数据，影响模型的训练效果。相比之下，WGAN、条件生成对抗网络（CGAN）及变分自编码条件 Wasserstein 生成对抗网络（VAE-CWGAN）方法通过学习原始数据的内在分布生成了质量更高的样本。然而，WGAN 和 CGAN 未引入梯度惩罚项，存在梯度消失和模型崩溃的风险，且可能生成无意义样本，导致其性能较差。VAE-CWGAN 引入变分子编码器（VAE）提前学习输入数据的空间分布，弥补了 GAN 可能生成无意义样本的缺点，但其特征提取仍局限在欧几里得域，无法捕捉特征间的高维非线性关系，故而在多分类任务中性能稍显不足。本文方法结合了 CWGAN 和 GCN 的优势，不仅解决了类不平衡问题，还能够充分捕捉流量数据的数值特征和结构特征，具备更全面的特征提取能力，因而实现了最优的检测性能。

在 CIC-IDS-2017 数据集上，本文方法的表现同样略优于其他方法，尤其是在精确率和误报率方面的提升较为显著，表明其在分类准确性和减少误报方面具有更强的能力。尽管在召回率上略低于 VAE-CWGAN，但差异仅在百分位级别，整体性能仍然非常出色。

对于 CIC-IDS-2017 数据集而言，现有的大多数类平衡方法在准确率、精确率、召回率以及 F1 分数 4 个性能指标上均能达到 99% 以上的检测效果。这主要归因于 CIC-IDS-2017 数据集本身的高质量、多样性和代表性。从特征工程的角度来看，该数据集在生成过程中进行了详细的特征提取，涵盖了流量持续时间、数据包大小、协议类型等丰富的网络流量特征，为模型提供了充分的信息以捕捉异常流量的模式。此外，尽管 CIC-IDS-2017 数据集中异常流量与正常流量的比例不完全平衡，但其数据分布相对合理，未出现极端不平衡现象，这使得模型在训练过程中能够更好地学习各类流量的内在特性，从而在分类任务中取得较好的结果。

本文方法在 UNSW-NB15 和 CIC-IDS-2017 数据集上的优异表现，证明其不仅在单一数据集的类平衡任务中表现突出，还能够适应不同的数据分布和网络环境。这种跨数据集的稳定性表明，本文方法能够有效应对不同类型的异常流量，具备较强的鲁棒性，有望为多样化的网络安全需求提供可靠的技术支持。

4.7　多分类方法对比

上述类平衡方法的对比结果验证了本文方法在

数据增强方面的有效性。为进一步评估本文方法在异常流量检测中的性能，本文将其与近年来提出的方法进行对比，具体结果如表7和表8所示。

表7 UNSW-NB15数据集上对比结果

方法	Acc	Pre	Rec	F1-Score
文献[22]	80.10%	81.90%	81.90%	81.90%
文献[29]	85.59%	86.11%	85.57%	85.84%
文献[33]	87.70%	88.46%	87.70%	85.44%
文献[34]	77.16%	82.63%	79.91%	81.25%
本文方法	**89.71%**	**90.24%**	**89.72%**	**89.68%**

表8 CIC-IDS-2017数据集上对比结果

方法	Acc	Pre	Rec	F1-Score
文献[17]	98.43%	99.69%	92.69%	96.06%
文献[18]	99.15%	99.15%	99.14%	99.14%
文献[22]	82.30%	76.50%	76.30%	76.40%
文献[35]	95.86%	96.85%	94.79%	95.81%
文献[36]	99.45%	99.75%	99.55%	99.66%
文献[37]	99.60%	99.60%	99.60%	99.60%
文献[38]	98.71%	95.97%	85.13%	90.22%
本文方法	**99.84%**	**99.97%**	**99.74%**	**99.83%**

由表7可知，本文方法在UNSW-NB15数据集的多分类任务中表现优异，在准确率、精确率、召回率和F1分数上分别提升了2.01%~12.55%、1.78%~8.34%、2.02%~9.81%和3.84%~8.43%。在5种多分类对比方法中，文献[34]的方法的检测性能较弱，主要原因是其基于传统混合采样技术，缺乏对原始数据深层特征的学习能力，检测性能易受噪声数据的影响。文献[22]和文献[29]的方法通过引入GAN进行数据生成，显著提升了检测性能。其中，文献[29]的方法基于Wasserstein距离计算损失，并将类别信息作为生成条件，生成数据的质量更高，因而检测性能优于文献[22]。文献[33]的方法结合了基于高斯混合模型聚类和WGAN数据生成技术，能够更好地处理类不平衡问题。此外，该方法通过引入堆叠自编码器，进一步增强了深度特征提取能力，提升了检测性能。然而，其分类模块由卷积神经网络和长短期记忆网络共同构建，忽略了特征之间的关联关系，因而其检测性能仍不及本文方法。

由表8可知，相较于现有方法，本文提出的检测方案在CIC-IDS-2017数据集上展现出显著的性能优势。以最具代表性的评价指标F1分数为例，本文方法的性能提升幅度介于0.17%~23.43%，相较于性能表现优异的文献[36]和文献[37]方法，本方法分别实现0.17%和0.23%的提升，对于接近100%的性能指标而言，这种提升幅度已较为显著。文献[37]采用空洞卷积扩展特征感知范围，结合门控循环单元捕捉流量时序动态，并通过通道注意力机制强化关键特征，有效解决了深度学习模型在异常检测中存在的特征丢失与重要性失衡问题。文献[36]则构建分层检测架构，通过小波变换将网络流量分解为高频与低频分量，再利用卷积长短期记忆网络（CNN-LSTM）分别提取空间与时间特征，显著提升了检测精度。然而，上述2种方法均依赖多技术融合，模型架构复杂，在实际工程部署中可能面临计算资源需求高、维护成本大等挑战。

综合来看，本文方法在异常流量检测任务中展现出更高的分类准确性、更低的误报率以及更好的平衡检测能力。无论是在复杂的UNSW-NB15数据集，还是在多样化的CIC-IDS-2017数据集上，本文方法均表现出强大的适应性与鲁棒性，能够有效应对不同类型的异常流量检测任务，有望为网络安全防护提供有力的技术支持。

5 结束语

本文提出一种基于数据增强与特征挖掘的异常流量检测方法——CFC-Net。该方法通过引入渐进式采样策略的样本生成方法较好地解决了数据不平衡问题，在生成高质量少数类样本的同时避免了对抗训练过程中的模式崩溃风险，尽管在低采样率下的生成数据可能无法充分表征真实数据分布，导致检测性能虚高，但其仍可部署于智能家居等轻量级物联网设备中，满足高响应时速、低安全级别设备的异常检测需求。此外，本文方法通过层次化特征提取和分层注意力机制有效解决了深度特征提取不充分的问题，在提高检测精度的同时缓解了图卷积计算中的过平滑问题。在UNSW-NB15和CIC-IDS-2017数据集上的实验结果证明了本文方法在异常流量检测任务中的有效性，同时与现有方法的对比实验进一步验证了其在多个指标上的性能优势。

当然，本文方法仅在2个开源数据集上进行了实验，相当于在封闭稳态环境下进行检测，默认假

设数据分布、特征属性及异常类别的静态性。实际的网络环境是完全开放且动态变化的，异常流量检测任务中的假设条件随时可能变化。因此，未来研究将聚焦于开放动态任务环境下的异常流量检测，探索更安全可信的检测方法，以提升模型在真实网络环境中的检测性能与适用性。

参考文献：

[1] 杨宏宇, 张豪豪, 成翔. 基于多尺度注意力特征增强的异常流量检测方法[J]. 通信学报, 2024, 45(11): 88-105.
YANG H Y, ZHANG H H, CHENG X. Abnormal traffic detection method based on multi-scale attention feature enhancement[J]. Journal on Communications, 2024, 45(11): 88-105.

[2] HO T, CHO S J, OH S R. Parallel multiple pattern matching schemes based on cuckoo filter for deep packet inspection on graphics processing units[J]. IET Information Security, 2018, 12(4): 381-388.

[3] MA Q, SUN C, CUI B J, et al. A novel model for anomaly detection in network traffic based on kernel support vector machine[J]. Computers & Security, 2021, 104: 102215.

[4] LIU C, GU Z, WANG J. A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning[J]. IEEE Access, 2021, 9: 75729-75740.

[5] BOVENZI G, ACETO G, CIUONZO D, et al. A hierarchical hybrid intrusion detection approach in IoT scenarios[C]//Proceedings of the GLOBECOM 2020 - 2020 IEEE Global Communications Conference. Piscataway: IEEE Press, 2020: 1-7.

[6] HOOSHMAND M K, HOSAHALLI D. Network anomaly detection using deep learning techniques[J]. CAAI Transactions on Intelligence Technology, 2022, 7(2): 228-243.

[7] 王健, 陈琳, 王凯崙, 等. 基于时空图神经网络的应用层DDoS攻击检测方法[J]. 信息网络安全, 2024, 24(4): 509-519.
WANG J, CHEN L, WANG K L, et al. Application layer DDoS detection method based on spatio-temporal graph neural network[J]. Netinfo Security, 2024, 24(4): 509-519.

[8] MOUSTAFA N, SLAY J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set[C]//Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS). Piscataway: IEEE Press, 2015: 1-6.

[9] 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. Setúbal: Science and Technology Publications, 2018: 108-116.

[10] ZHOU Y J, HU G M, WU D P. A data mining system for distributed abnormal event detection in backbone networks[J]. Security and Communication Networks, 2014, 7(5): 904-913.

[11] JIANG D D, XU Z Z, ZHANG P, et al. A transform domain-based anomaly detection approach to network-wide traffic[J]. Journal of Network and Computer Applications, 2014, 40: 292-306.

[12] JUVONEN A, SIPOLA T, HÄMÄLÄINEN T. Online anomaly detection using dimensionality reduction techniques for HTTP log analysis[J]. Computer Networks, 2015, 91: 46-56.

[13] WU T, FAN H H, ZHU H J, et al. Intrusion detection system combined enhanced random forest with SMOTE algorithm[J]. EURASIP Journal on Advances in Signal Processing, 2022(1): 39.

[14] LU C W, CAO Y X, WANG Z B. Research on intrusion detection based on an enhanced random forest algorithm[J]. Applied Sciences, 2024, 14(2): 714.

[15] DUAN X Y, FU Y, WANG K. Network traffic anomaly detection method based on multi-scale residual classifier[J]. Computer Communications, 2023, 198: 206-216.

[16] BHAYO J, SHAH S A, HAMEED S, et al. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks[J]. Engineering Applications of Artificial Intelligence, 2023, 123: 106432.

[17] LUO J, ZHANG Y Y, WU Y N, et al. A multi-channel contrastive learning network based intrusion detection method[J]. Electronics, 2023, 12(4): 949.

[18] BHARDWAJ S, DAVE M. Enhanced neural network-based attack investigation framework for network forensics: identification, detection, and analysis of the attack[J]. Computers & Security, 2023, 135: 103521.

[19] JIANG X, ZHANG H R, ZHOU Y. Multi-granularity abnormal traffic detection based on multi-instance learning[J]. IEEE Transactions on Network and Service Management, 2024, 21(2): 1467-1477.

[20] XU X, LI J, YANG Y, et al. Toward effective intrusion detection using log-cosh conditional variational autoencoder[J]. IEEE Internet of Things Journal, 2021, 8(8): 6187-6196.

[21] CHANGALA R, KAYALVILI S, FAROOQ M, et al. Using generative adversarial networks for anomaly detection in network traffic: advancements in AI cybersecurity[C]//Proceedings of the 2024 International Conference on Data Science and Network Security (ICDSNS). Piscataway: IEEE Press, 2024: 1-6.

[22] LI Z C, CHEN S Y, DAI H S, et al. Abnormal traffic detection: traffic feature extraction and DAE-GAN with efficient data augmentation[J]. IEEE Transactions on Reliability, 2023, 72(2): 498-510.

[23] YAO W, SHI H, ZHAO H. Scalable anomaly-based intrusion detection for secure Internet of Things using generative adversarial networks in fog environment[J]. Journal of Network and Computer Applications, 2023, 214: 103622.

[24] RAO Y N, SURESH BABU K. An imbalanced generative adversarial network-based approach for network intrusion detection in an imbalanced dataset[J]. Sensors, 2023, 23(1): 550.

[25] PUJOL-PERICH D, SUAREZ-VARELA J, CABELLOS-APARICIO A, et al. Unveiling the potential of graph neural networks for robust intrusion detection[J]. ACM SIGMETRICS Performance Evaluation Review, 2022, 49(4): 111-117.

[26] LO W W, LAYEGHY S, SARHAN M, et al. E-GraphSAGE: a graph neural network based intrusion detection system for IoT[J]. arXiv Preprint, arXiv: 2103.16329, 2021.

[27] REKA R, KARTHICK R, SARAVANA RAM R, et al. Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET[J]. Computers & Security, 2024, 136: 103526.

[28] ZHANG G L, WANG X D, LI R, et al. Network intrusion detection based on conditional Wasserstein generative adversarial network and cost-sensitive stacked autoencoder[J]. IEEE Access, 2020, 8: 190431-190447.

[29] MA Z X, LI J, SONG Y F, et al. Network intrusion detection method based on FCWGAN and BiLSTM[J]. Computational Intelligence and Neuroscience, 2022, 2022(1): 6591140.
[30] 刘涛涛, 付钰, 王坤, 等. 基于VAE-CWGAN和特征统计重要性融合的网络入侵检测方法[J]. 通信学报, 2024, 45(2): 54-67.
LIU T T, FU Y, WANG K, et al. Network intrusion detection method based on VAE-CWGAN and fusion of statistical importance of feature[J]. Journal on Communications, 2024, 45(2): 54-67.
[31] SONG J M, WANG X J, HE M S, et al. CSK-CNN: network intrusion detection model based on two-layer convolution neural network for handling imbalanced dataset[J]. Information, 2023, 14(2): 130.
[32] ZHANG H P, HUANG L L, WU C Q, et al. An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset[J]. Computer Networks, 2020, 177: 107315.
[33] CUI J Y, ZONG L S, XIE J H, et al. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data[J]. Applied Intelligence, 2023, 53(1): 272-288.
[34] JIANG K Y, WANG W Y, WANG A L, et al. Network intrusion detection combined hybrid sampling with deep hierarchical network[J]. IEEE Access, 2020, 8: 32464-32476.
[35] DING H W, CHEN L Y, DONG L, et al. Imbalanced data classification: a KNN and generative adversarial networks-based hybrid approach for intrusion detection[J]. Future Generation Computer Systems, 2022, 131: 240-254.
[36] WANG K, FU Y, DUAN X Y, et al. Abnormal traffic detection system in SDN based on deep learning hybrid models[J]. Computer Communications, 2024, 216: 183-194.
[37] JI C P, YU H F, DAI W. Network traffic anomaly detection based on spatiotemporal feature extraction and channel attention[J]. Processes, 2024, 12(7): 1418.
[38] YU X C, HUANG Y, ZHANG Y, et al. Network intrusion traffic detection based on feature extraction[J]. Computers, Materials & Continua, 2024, 78(1): 473-492.

[作者简介]

安义帅（1997– ），男，山西忻州人，海军工程大学博士生，主要研究方向为人工智能、网络安全。

付钰（1982– ），女，湖北武汉人，博士，海军工程大学教授、博士生导师，主要研究方向为信息安全、人工智能。

俞艺涵（1992– ），男，浙江金华人，博士，海军工程大学讲师，主要研究方向为隐私保护、信息安全。

刘涛涛（1996– ），男，江西吉安人，海军工程大学博士生，主要研究方向为人工智能、信息处理、网络安全。