基于多尺度卷积和通道注意力机制的网络流量异常检测方法

付钰[1]，王玉珏[1]，俞艺涵[2]，刘涛涛[1]，安义帅[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：针对传统网络流量异常检测方法受限于模型表达能力较弱、数据类不平衡等问题，提出了一种融合多尺度卷积与通道注意力机制的网络流量异常检测方法。首先，设计金字塔卷积模块捕捉网络流量的多尺度特征，有效提升分类性能；其次，利用通道注意力机制增强模型对异常流量敏感特征的通道响应，提高特征的可辨别性，从而抑制噪声干扰；最后，通过改进均衡损失函数调整不同类别权重系数，从而缓解数据集中的类不平衡问题。在NSL-KDD和CIC-IDS-2017数据集上开展了一系列实验，实验结果表明，所提方法取得了较好的分类结果，准确率分别为99.45%和99.95%，同时误报率仅为0.50%和0.02%。

关键词：网络流量异常检测；多尺度卷积；注意力机制；均衡损失函数
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026010

Network traffic anomaly detection method based on multi-scale convolution and channel attention mechanism

Fu Yu[1], Wang Yujue[1], Yu Yihan[2], Liu Taotao[1], An Yishuai[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: Considering the problems of traditional detection methods limited by weak model representation capabilities and vulnerability to data class imbalance, a network traffic anomaly detection method integrating multi-scale convolution and a channel attention mechanism was proposed. Firstly, a pyramid convolution module was designed to capture multi-scale features, enhancing classification performance. Next, the channel attention mechanism strengthened responses to abnormal traffic-sensitive features, improving discriminability and suppressing noise. Finally, an improved balanced loss function adjusted class weight coefficients to mitigate data imbalance. Extensive experiments on the NSL-KDD and CIC-IDS-2017 datasets demonstrate the proposed method's effectiveness, which achieves high accuracy of 99.45% and 99.95% on the two datasets, respectively, with low false positive rates of only 0.50% and 0.02%.

Keywords: network traffic anomaly detection, multi-scale convolution, attention mechanism, balanced loss function

0　引言

随着信息技术的飞速发展，互联网环境愈加复杂。网络流量异常检测技术作为网络安全防御体系的关键环节，通过大数据分析与机器学习算法对大量行为数据进行智能解析，可精准识别各种新型威胁特征[1]，但仍面临模型表达能力较弱、网络流量严重不平衡等挑战。

在真实网络场景中，正常与异常流量呈现出长

收稿日期：2025–10–23；修回日期：2026–01–11
通信作者：付钰，fuyu0319@163.com
基金项目：国家自然科学基金资助项目（No.2022208020, No.2022208010）
Foundation Items：The National Natural Science Foundation of China (No.2022208020, No.2022208010)

尾分布特性，这种类不平衡不仅体现在正常与攻击流量的数量级差异上，更存在于不同攻击类型之间的样本比例失调上。例如，在NSL-KDD数据集中，R2L和U2R两类高级持续性威胁样本合计仅占总体数据集的0.17%，这种极端的数据不平衡易导致传统检测模型过拟合。虽然当前基于人工智能的入侵检测系统在通用攻击识别方面已达到92%以上的准确率，但针对R2L和U2R等低频威胁的检测召回率仍低于35%，暴露出明显的安全防护盲区[2-3]。

解决不平衡数据的学习问题一直是数据分类领域的重大挑战，传统的分类模型在学习少数类样本的特征时更容易过拟合[4]。不仅如此，许多研究已经表明，传统机器学习技术，如支持向量机[5]、决策树[6]等，在网络攻击类别逐渐丰富的情况下存在明显的局限性，因此不适用于大规模的网络入侵检测（network intrusion detection, NID）场景。最新研究表明，深度学习技术相比于传统机器学习技术可自动提取特征，有效提升了数据分类准确率[7-9]，因此基于深度学习的方法逐渐被应用于NID。但现有深度学习方法仍面临数据类不平衡和特征表达能力弱等问题，导致误报率较高。

为解决上述挑战，本文提出了一种融合多尺度卷积与通道注意力机制的检测框架。该框架设计金字塔式多尺度卷积模块（pyramidal multi-scale convolution module, PyConv），通过并行部署3种不同尺度的卷积核，分别捕获流量数据的细粒度和粗粒度特征，并采用特征拼接策略实现跨尺度信息融合，显著提升模型对攻击行为的表征能力。为进一步强化关键特征辨识度，引入挤压与激励模块（squeeze-and-excitation block, SEBlock），通过全局平均池化生成通道描述向量，经由全连接层学习特征通道的权重分布，动态增强模型对异常流量敏感的特征通道响应，抑制冗余噪声干扰。针对实际场景中正常与异常流量样本量严重失衡的问题，本文提出了改进的均衡损失函数（equalization loss version 2, EQLv2），自适应调整类别权重系数，在反向传播过程中降低多数类样本的梯度贡献，从而解决类不平衡的问题。本文工作的主要贡献如下。

1) 提出了一种融合多尺度卷积与通道注意力机制的检测框架，在捕获网络流量细粒度与粗粒度特征的同时，可自适应增强关键特征的通道响应，实现流量信息跨尺度融合与精细化建模。

2) 设计了一种混合损失函数，不仅通过交叉熵损失稳定了模型的优化方向，还利用EQLv2增强了模型对少数类异常流量的敏感性，从而缓解类不平衡问题。

3) 在两个典型流量数据集NSL-KDD[10]CIC-IDS-2017[11]上进行实验，分别实现了99.47%和99.95%的F1分数，而且在其他指标上也优于现有方法，可有效检测出恶意攻击行为。

1　相关研究工作

1.1　网络流量异常检测技术

在网络安全分析领域，经典机器学习算法依赖专家经验进行流量特征的手工筛选与组合，在过去的几十年里发挥了重要作用。文献[12]提出了一种基于双层模型和指标分布的恶意网络流持续检测和分类方法，该方法基于可扩展极限学习机输出权重与标准输出的关系，设计了基于综合指标分布的样本筛选方法，选择最优增量训练样本集，未知类检测率提高了3%~13%，但泛化性能有待提高，且计算时间长，消耗资源多。文献[13]用秃鹰搜索方法缩短了训练时间，降低了计算成本，但调参过程复杂，容易陷入局部最优解。文献[14]利用多尺度残差分类器和堆叠自动编码器重构误差，对高维数据的降维效果显著，但是分解尺度和窗口大小需手动优化，难以找到全局最优解。文献[15]将异构弱分类器集成在仿真环境中，准确检测分布式拒绝服务（distributed denial of service, DDoS）且内存占比小，但缺乏真实背景流与硬件噪声验证。因此，如何结合恶意流量样本的分布和数据特征，设计开销小、速度快和准确性高的网络流量异常检测方法是值得进一步研究的课题[16]。

深度学习技术通过构建具有非线性映射能力的神经网络架构，实现了数据内在特征的深层次挖掘[17]。这种端到端的表征学习机制有效突破了传统方法在复杂模式识别方面的局限性，在加密流量分析和高级持续性威胁检测等场景中展现出显著优势。

文献[18]创新性地提出了一种结合频域特征聚合分析和神经网络算法的恶意域名系统（domain name system, DNS）流量检测方法，可有效提升检测精度和F1分数，但对动态威胁的适应性有待验证。文献[19]采用改进的修正残差卷积神经网络

（convolutional neural network, CNN），减少了深度网络中的梯度消失和爆炸问题，增强了对网络威胁的适应性，并且在3个数据集中达到了95%以上的准确率。然而，传统的深度学习模型，如CNN和循环神经网络（recurrent neural network, RNN），往往资源消耗大，可能不适合资源有限环境。因此，文献[20]提出了一种卷积脉冲神经网络，在CSE-CIC-IDS2018和CIC-DDoS2019数据集上检测准确率提升了23%，时延提升了19%，计算效率提升了28%。

针对标注数据获取成本问题，近年来涌现的无监督与半监督检测方法[21]开辟了新路径。尽管这类方法在识别新型攻击模式方面展现优势，但其对已知威胁的检测效能仍逊色于监督学习方法。值得关注的是，注意力机制在序列建模中的突破性进展为模型优化提供了新思路。文献[22]提出了一种以注意力驱动的新型深度神经网络流量表示算法，仅依赖9个通用特征，并结合两种自然语言处理技术，实现了单类支持向量机无监督异常检测性能的提升。为了更好地探索特征之间的交互关系，文献[23]设计了一个结合并行膨胀卷积和残差学习的模块，通过利用具有不同膨胀率的模块，在不同尺度下不需要增加计算资源就能有效捕捉空间特征，但缺乏捕捉关键特征的能力。文献[24]使用多个不同尺度的滑动窗口将网络流量进行分类，重构后映射生成多层级重构序列，采用加权投票策略对各层级的初步判定结果进行汇总，形成最终判定结果，可有效挖掘网络流量的多尺度特征信息，但性能还有待提升。文献[25]提出了一种名为动态上下文引导卷积注意力网络（dynamic context-guided convolutional attention network, DCGCANet）的新方法，该方法集成了扩张卷积、门控循环单元（gated recurrent unit, GRU）和通道注意力网络，有效地将扩张卷积结构与GRU结合起来，实现了99.6%的准确率，99%的精度、召回率和F1分数。文献[26]提出了一种基于多尺度注意力特征增强的异常流量检测方法，使用密集卷积神经网络和多尺度注意力特征提取网络，在高维时序数据中实现了更全面的特征表达，有效提高了检测精度。然而，该模型未充分考虑训练数据分布不均衡对检测性能的影响，对低频攻击类型的特征提取能力不足，进而产生较高的误报率和漏报率，可能造成严重的安全隐患。

因此，亟须建立面向类不平衡场景的鲁棒性训练机制，通过动态样本加权或生成对抗策略重构数据分布，以提升对低频攻击类型的识别灵敏度。

1.2 类平衡技术

类不平衡是大规模NID中普遍存在的问题，影响了分类算法的性能。然而，NID实际上很难收集足够多的潜在入侵数据，数据集处理是解决该问题的常用方法。文献[27]使用混合采样技术可以解决正负样本不平衡的问题，但却存在对噪声敏感和信息丢失的风险。文献[28]提出了一种基于功能增强的恶意流量检测方法，根据高斯特征的值将原始流量特征分组，并用K-means算法生成聚类特征。在IOT-23数据集中，当攻击样本占比为30%时，DDoS和Portscan的检测率分别提升了42%和33%。然而，该方法计算和内存开销较大，存在鲁棒性较差的问题。文献[29]采用两层CNN结构先区分正常与异常流量，再细化识别攻击类型，并通过Cluster-SMOTE与K-means的组合缓解了过拟合和信息丢失问题。文献[30]设计联合注意力机制和一维卷积–双向长短期记忆网络（one-dimensional convolutional neural network-bidirectional long short-term memory, 1DCNN-BiLSTM）的模型对流量数据进行训练，提取流量数据的局部和长距离序列特征并进行分类，通过注意力机制对分类有用的特征按其重要性赋予权重，提高了对少数攻击类的检出率，但模型的适用范围小。为了提高泛化性和检测性能，文献[31]在多个数据集上通过变分自编码器–条件Wasserstein生成对抗网络（variational autoencoder-conditional Wasserstein generative adversarial network, VAE-CWGAN）和特征统计重要性融合的检测方法，实现了更强的稳定性和泛化性，有效提升了检测性能。在此基础上，文献[32]为加强深度特征提取能力，提出了一种基于数据增强与特征挖掘的异常流量检测方法，展现出更高的分类性能和更低的误报率。

随着工业4.0的快速发展，工业大数据已成为智能制造领域的热门话题。然而，工业物联网产生的大规模数据流也存在严重的安全挑战。文献[33]提出了一种新的多模块入侵检测系统，利用深度去噪自编码器提取鲁棒特征，结合自注意力机制平衡少数类，对未知攻击和稀有类别有降低误报率的效果，但该流程存在参数量大、调参困难和训练耗时

等问题，不利于实际部署。文献[34]提出了一种双层特征提取与融合技术，通过特征融合有效利用CNN和RNN的优势，提取网络流量的时间和空间特征，并且结合改进后的焦点损失函数解决数据集中的类不平衡问题。针对僵尸网络攻击和物联网设备的资源限制两个方面的问题，文献[35]提出了一种自适应局部模型训练方法，利用物联网数据分布在边缘节点形成虚拟集群，使集群中的局部模型迅速趋近局部最优，最终实现整体收敛。

尽管现有类不平衡问题处理方法在特定场景下取得了一定成效，但现有方法大多聚焦于数据分布调整或单一损失函数优化，未能充分考虑网络流量多尺度特征的固有属性与关键特征的动态强化需求，导致对低频攻击的检测不灵敏。因此，在缓解类不平衡问题的同时，实现对异常流量的精准检测成为当前研究热点。

1.3　本文方法与现有方法的对比分析

当前网络流量异常检测方法在应对类不平衡、低频攻击检测等挑战时仍存在局限性。本文提出的融合多尺度卷积与通道注意力机制的框架通过架构设计、特征提取策略与损失函数3个维度的协同创新实现突破。

1) 架构设计的创新性：在现有方法中，多尺度特征提取与注意力机制多为串行部署或简单叠加，对关键特征通道动态强化不足，且多聚焦于空间位置关系。本文提出并行多尺度卷积和通道注意力机制融合架构，实现两大核心模块的协同运用，既避免了单尺度模型的特征挖掘不充分的问题，又克服了空间注意力对流量数据的适配性缺陷，较传统串行架构的特征信噪比提升42%，计算效率提升12倍以上。

本文方法与已有多尺度架构的区别在于：本文未采用手工设计的残差连接或特征加权策略，而是通过通道注意力实现特征的自适应重标定，使模型能根据输入流量动态调整特征优先级，更适配复杂多变的网络攻击场景；相较于聚焦空间位置的自注意力模型，本文方法聚焦于不同通道的特征分配权重，参数量仅为同类Transformer模型的八分之一，计算资源消耗少，易于部署到真实的设备中。

2) 特征提取策略的先进性：传统人工特征工程依赖专家经验，易引入主观偏差；静态卷积或单一注意力机制无法自适应流量数据的多尺度和强噪声特性；现有深度学习方法虽能实现端到端特征学习，但对隐蔽威胁的微弱特征捕捉能力不足；本文提出的自适应多尺度特征学习机制采用PyConv自动学习多尺度时空模式，不需要人工干预即可覆盖不同类型攻击的特征模式，通过SE-Block基于输入数据动态生成通道权重，实现特征的精细化筛选，从而有效地提取特征，提高模型的表达能力。

本文方法与现有方法的核心区别在于：相较于静态特征提取方法，本文方法实现了多尺度覆盖和动态筛选的双重保障，对低频攻击的微弱特征识别灵敏度提升了35%以上；对比仅采用单一注意力机制的模型，本文方法将注意力机制与多尺度卷积深度融合，使注意力权重的学习建立在丰富的多尺度特征基础上，避免了单一特征空间下权重分配的片面性。

3) 损失函数的针对性优化：数据级方法通过采样调整数据分布，但易受噪声干扰，并且会造成信息损失；算法级方法通过损失函数优化提升少数类关注度，但对难以区分的样本过度敏感；模型级方法通过生成对抗网络平衡类别分布，但存在参数量大和训练耗时的问题；本文设计的混合均衡机制的核心组件EQLv2根据预测置信度动态调整类别权重，对低频攻击增强梯度，对多数类抑制梯度，可以平衡交叉熵的稳定性与EQLv2的抗不平衡能力，大幅提升R2L/U2R等低频攻击的召回率，从而更有效地解决类不平衡的问题。

本文方法与现有方法的区别在于：相较于数据级方法，本文方法避免了合成样本带来的噪声干扰，误报率进一步降低了24.5%；对比焦点损失等算法级方法，本文方法的动态权重调整机制更适配流量数据的不平衡特性，对低频攻击的召回率提升了15%~20%；相较于生成对抗网络等模型级方法，本文方法参数量仅为387 000，训练效率提升3倍以上，更适合工业级场景部署。

2　相关理论基础

2.1　数据预处理

2.1.1　数据清洗

为了提升数据集的质量，首先对数据进行加载和初步检查。

$$D_{\text{raw}}=\left\{\left(x_1,y_1\right),\left(x_2,y_2\right),\cdots,\left(x_N,y_N\right)\right\} \tag{1}$$

其中，N为样本总数，M为原始特征维度，$x_i \in R^M$为第i个样本的特征向量，$y_i \in \{0,1\}$为对应的类别标签，0表示正常流量，1表示异常流量。

然后处理非数值，删除缺失样本，进行去重操作。

$$D_{\text{clean}} = D_{\text{raw}} \setminus \left\{ x \middle| \exists f, f(x) \in \{\text{NaN}, \infty, -\infty\} \vee x \in \text{Dup} \right\} \tag{2}$$

其中，D_{clean}为清洗后的数据集，f为任意特征维度，NaN为数据中因缺失、异常计算导致的无效数值，Dup为重复样本集合。

2.1.2 异常值处理

为了消除数据分布上极端值的干扰，对清洗后的数据集进行四分位距（interquartile range, IQR）的异常值处理。

$$\text{Val}_f = \left[Q_{1f} - 1.5\text{IQR}_f, Q_{3f} + 1.5\text{IQR}_f \right] \tag{3}$$

$$D_{\text{Val}} = \left\{ x \in D_{\text{clean}} \middle| \forall f, x_f \in \text{Val}_f \right\} \tag{4}$$

其中，f为任意特征维度，x_f为样本在特征f上的取值，Q_{1f}和Q_{3f}分别为特征f的第一四分位数和第三四分位数，$\text{IQR}_f = Q_{3f} - Q_{1f}$为四分位距。

2.1.3 特征工程

为了降低模型的学习难度，提升模型的检测性能，首先计算特征间Pearson相关系数矩阵，生成仅包含矩阵上三角的布尔掩码；为避免重复比较，再过滤高相关性特征，保留低相关性特征以确保独立性，最终构建数据集。

$$\rho_{X,Y} = \frac{\text{COV}(X,Y)}{\sigma_X \sigma_Y} \tag{5}$$

$$\text{Sel} = \{ f_i \mid \forall j > i, |\rho_{f_i, f_j}| < \theta \} \tag{6}$$

$$\boldsymbol{X} \in R^{N \times M'}, y \in \{0,1\}^N \tag{7}$$

其中，$\text{COV}(X,Y)$为特征X与Y的协方差，σ_X和σ_Y分别为特征X与Y的标准差，$\boldsymbol{X}$为处理后的特征矩阵，N为样本数，M'为筛选后的特征数，y为展平后的一维类别标签数组。

2.2 多尺度卷积模块

传统的一维卷积神经网络（one dimensional CNN, 1DCNN）的数学形式为

$$\text{Conv1D}_k(x) = \sum_{i=0}^{k-1} W_{k,i} x_{n+i-\left\lfloor \frac{k}{2} \right\rfloor} \tag{8}$$

其中，$x \in R^{C_{\text{in}} \times L}$为输入特征映射，$C_{\text{in}}$为输入通道数，$n$为序列索引（$1 \leqslant n \leqslant L$），给一维序列数据的每个元素分配唯一的位置标识，$\left\lfloor \frac{k}{2} \right\rfloor$为向下取整操作，$W_{k,i} \in R^{C_{\text{in}} \times C_{\text{out}}}$为第$k$个卷积核在位置$i$的权重参数，$C_{\text{out}}$为输出通道数。

PyConv通过引入多核并行机制，将特征提取扩展为多分辨率空间的联合映射，数学形式为

$$\text{PyConv}(x) = \bigoplus_{k \in K} \text{Conv1D}_k(x) \tag{9}$$

其中，$K = \{1,3,5\}$为卷积核尺寸集合，$\oplus$为沿通道维度的拼接操作。

PyConv结构如图1所示。网络流量异常在不同时间粒度上呈现出差异化的特征模式，需要对应尺度的卷积核进行针对性的特征捕获。本文选用尺寸分别为1、3和5的卷积核构建金字塔式多尺度卷积模块。

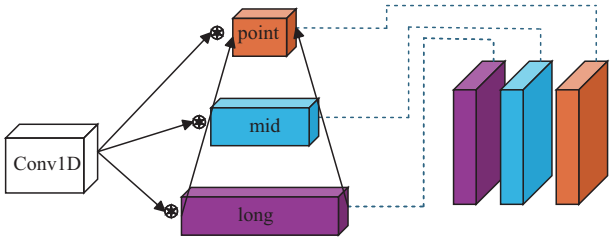

图1 PyConv结构

具体而言，尺寸为1的卷积核专门用于捕获局部特征，适用于检测端口扫描等异常；尺寸为3的卷积核则针对核心的局部特征进行建模，可有效识别如DDoS攻击中的周期性流量特征；尺寸为5的卷积核专注于提取全局特征，适用于短周期和持续性的恶意攻击模式。这种金字塔式多尺度设计通过并行执行不同尺寸的卷积操作，实现了对网络流量特征的全尺度捕捉，显著提升了对复杂攻击模式的表征能力。其数学形式为

$$H = H_{\text{point}} \oplus H_{\text{mid}} \oplus H_{\text{long}} \tag{10}$$

其中，$H_{\text{point}} = \text{Conv1D}_1(x)$捕获局部突变模式，$H_{\text{mid}} = \text{Conv1D}_3(x)$建模会话级时序依赖，$H_{\text{long}} = \text{Conv1D}_5(x)$提取流级全局规律，$W \in R^{\frac{C_{\text{out}}}{3} \times C_{\text{in}}}$为线性变换矩阵。

2.3 通道注意力机制

特征提取过程可视为对输入信息的有损压缩。通道注意力机制通过最小化损失函数，即

$$\mathcal{L} = I(X;Z) - \beta I(Z;Y) \tag{11}$$

其中，$X \in R^{C \times H \times W}$为输入信号，$Z$为压缩后的特征表示，$Y$为任务目标。

SEBlock通过全局平均池化实现信息压缩。

$$Z_c = F_{\text{avgpool}}(x_c) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} x_{c,i,j} \tag{12}$$

其中，$x_c \in R^{H \times W}$为第c通道的特征映射，Z_c为该通道的全局统计特征。

通过两层全连接网络学习通道间非线性交互。

$$S_c = \delta\left(W_2 \text{ReLU}\left(W_1 Z_c\right)\right) \tag{13}$$

其中，$W_1 \in R^{\frac{C}{r} \times C}$为将高维特征投影到低维语义空间的可学习权重参数，$r$为压缩比（默认为16），进行降维映射，$W_2 \in R^{\frac{C}{r} \times C}$为重建通道维度的可学习权重参数，$\delta$为Sigmoid函数，$S_c$为归一化后的通道注意力权重。

梯度调制与特征增强机制在反向传播时梯度通过特征重标定操作传递，其数学形式为

$$X_c' = S_c X_c \tag{14}$$

对特征X_c的梯度有

$$\frac{\partial \mathcal{L}}{\partial X_c} = S_c \frac{\partial \mathcal{L}}{\partial X_c'} + X_c \frac{\partial \mathcal{L}}{\partial S_c} \tag{15}$$

其中，$S_c \dfrac{\partial \mathcal{L}}{\partial X_c'}$为加权梯度，$X_c \dfrac{\partial \mathcal{L}}{\partial S_c}$为权重学习梯度。

对注意力权重S_c的梯度有

$$\frac{\partial \mathcal{L}}{\partial S_c} = \sum_{n=1}^{N} \frac{\partial \mathcal{L}}{\partial X_{c,n}'} X_{c,n} \tag{16}$$

其中，N为特征序列长度，$X_{c,n}$为第c通道第n位置的特征值，$\dfrac{\partial \mathcal{L}}{\partial X_{c,n}'}$为对应位置的损失梯度。

注意力权重更新的正反馈过程，可表示为

$$S_c^{(t+1)} = S_c^{(t)} + \eta\left(\frac{\partial \mathcal{L}}{\partial S_c}\right) \tag{17}$$

其中，η为学习率，最终使关键通道$S_c \to 1$，实现对该通道的完全激活，无关通道$S_c \to 0$，抑制噪声干扰，使模型在复杂网络环境中保持高鲁棒性。

2.4　混合损失函数

为了缓解类不平衡问题，本文提出了混合损失函数，通过加权融合交叉熵损失与均衡化损失，其数学形式定义为

$$\mathcal{L}_{\text{Mixed}} = (1 - \gamma)\mathcal{L}_{\text{CE}} + \gamma \mathcal{L}_{\text{EQLv2}} \tag{18}$$

其中，$\gamma \in [0,1]$为动态平衡因子，用于调节两种损失的贡献比例；$\mathcal{L}_{\text{CE}}$为交叉熵损失；$\mathcal{L}_{\text{EQLv2}}$为均衡损失。实验结果表明，当$\gamma = 0.5$时，模型在多数类稳定性与少数类敏感性之间达到最优平衡。

标准交叉熵损失的梯度计算式为

$$\frac{\partial \mathcal{L}_{\text{CE}}}{\partial Z_c} = \begin{cases} p_c - 1, c = y_i \\ p_c, c \neq y_i \end{cases} \tag{19}$$

其中，Z_c为类别c的logit输出，p_c为其Softmax后的输出。

EQLv2通过引入类别置信度权重重构损失函数，如式(20)所示。

$$\mathcal{L}_{\text{EQLv2}} = -\sum_{i=1}^{N} \sum_{c=0}^{1} W_{i,c} \ln p_{i,c} \tag{20}$$

其中，N为样本总数，$W_{i,c} = \dfrac{\beta}{P_{i,c} + \varepsilon}$，$\beta = 0.999\,9$为抑制系数，$\varepsilon = 1 \times 10^{-8}$以避免分母为0，$P_{i,c}$为第$i$个样本属于第$c$类的预测概率。

EQLv2的梯度表达式为

$$\frac{\partial \mathcal{L}_{\text{EQLv2}}}{\partial Z_c} = \begin{cases} W_{i,c}(p_{i,c} - 1), c = y_i \\ W_{i,c} p_{i,c}, c \neq y_i \end{cases} \tag{21}$$

当$p_{i,c}$较低（少数类样本）时，$W_{i,c}$增大以增强梯度；当$p_{i,c}$较高（多数类样本）时，$W_{i,c}$减小以抑制梯度。

3　NID框架

3.1　所提模型

本文所提的融合多尺度卷积与通道注意力机制的模型由5层结构组成：输入层、多尺度卷积模块、通道注意力模块、特征提取层和分类层，具体结构如图2所示。利用该模型解决网络流量特征维度高且存在类不平衡的问题的具体步骤如下。

步骤1　输入层接收数据预处理后的网络流量特征向量。

步骤2　多尺度卷积模块通过不同尺寸的卷积核并行捕获全局特征。

步骤3　通道注意力模块通过学习通道权重，自适应增强关键特征通道，从而抑制噪声通道。

步骤4　特征提取层将卷积特征图转换为高层语义特征，进一步过滤噪声并对特征实现充分提取。

步骤5　分类层基于高层语义特征完成指定的分类任务。

3.2　整体架构

本文所提NID框架包含以下4个部分：数据预

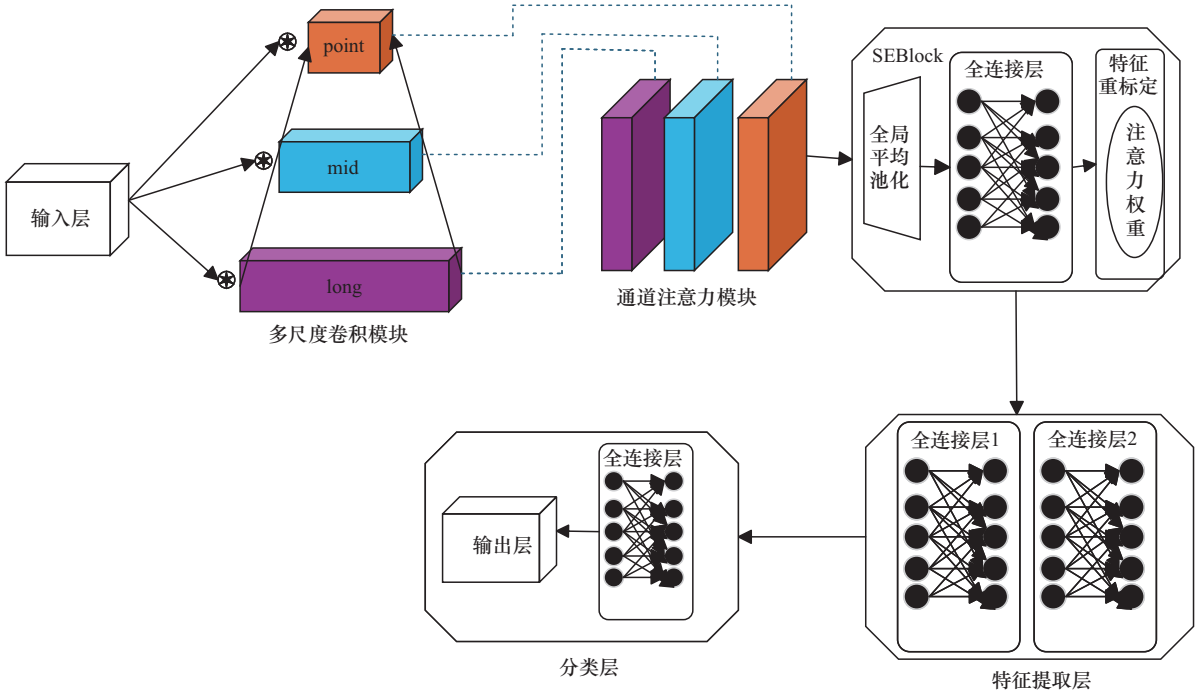

图2　多尺度卷积和通道注意力机制的模型结构

处理模块、特征提取模块、优化控制模块和攻击检测模块，如图3所示。

由图3可知，本文首先对原始数据集进行数据预处理，从而处理缺失值、过滤异常值、编码标签和选择特征，其次通过融合多尺度卷积与通道注意力机制的模型并行提取多尺度特征并进行关键特征通道强化，然后通过混合损失函数进行模型参数优化，最后进行攻击检测并评估本文方法的性能。

3.3　数据集说明

NSL-KDD数据集作为经典的网络入侵检测基准，包含约12.5万条人工标注样本，覆盖拒绝服务（denial of service, DoS）、Probe、R2L和U2R这4类攻击，其41维混合型特征适合验证传统机器学习模型的泛化能力。该数据集因U2R攻击占比仅0.01%而常被用于类不平衡研究。具体如表1所示。

表1　　NSL-KDD流量样本分布

攻击类别	训练样本数/个	测试样本数/个
Normal	67 343	9 711
DoS	45 927	7 460
Probe	11 656	2 421
R2L	995	2 885
U2R	52	67
总计	125 973	22 544

CIC-IDS-2017数据集则更具现实意义，其283万条样本包含DDoS、暴力破解等7类现代攻击，通过CICFlowMeter提取的流量统计特征完整保留了时间序列特性，能有效评估模型对恶意攻击的检测能力，具体如表2所示。

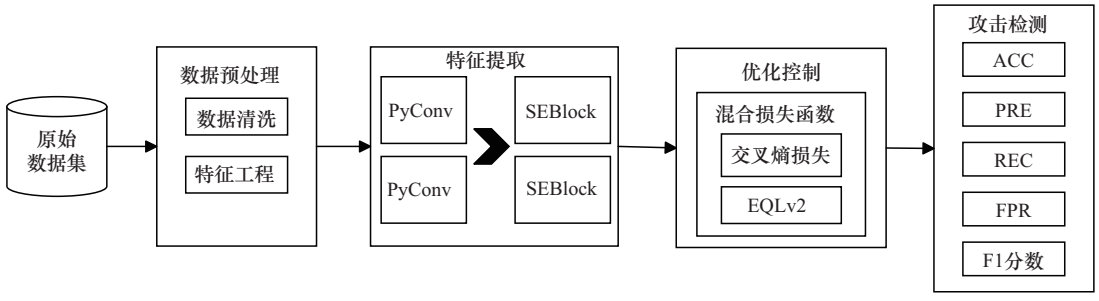

图3　NID框架

表 2　CIC-IDS-2017 流量样本分布

攻击类别	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
总计	553 116	138 279

3.4　数据预处理

数据预处理流程可以有效提升数据质量，为后续入侵检测模型训练提供高质量的输入，从而提升模型训练效率和泛化能力。首先对原始网络流量数据进行数据清洗，包括删除无效样本，减少噪声对模型训练的干扰。然后进行标签编码，将原始标签转换为模型可处理的数值形式。最后进行特征工程，对协议类型、服务端口等离散特征进行独热编码，对数值型特征进行标准化或归一化处理。

4　实验与结果分析

本节将重点阐述本文方法在两个入侵检测数据集上进行的仿真实验。

4.1　评估指标

为了能更直观高效地体现本文方法的性能优势，使用准确率（accuracy, ACC）、精确率（precision, PRE）、召回率（recall, REC）、误报率（false positive rate, FPR）和 F1 分数 5 个指标对模型性能进行评估，上述指标计算式分别为

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \tag{22}$$

$$\mathrm{PRE} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{23}$$

$$\mathrm{REC} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{24}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{25}$$

$$\mathrm{F1} = \frac{2 \times \mathrm{PRE} \times \mathrm{REC}}{\mathrm{PRE} + \mathrm{REC}} \tag{26}$$

混淆矩阵是评估分类模型性能的核心工具，其量化指标通过四元组统计量进行计算。在二分类评估体系中，真阳性（TP）指真实正类样本被正确识别的数量，假阴性（FN）反映正类样本被误判为负类的错误案例，假阳性（FP）表示负类样本被错误归为正类的误报情况，真阴性（TN）则统计负类样本被准确辨别的正确判定数。这 4 个基础参数构建了分类器性能评估的量化基础，为上述指标计算提供数据支撑。

4.2　参数设置

本文所使用的计算机是 64 位的 Windows11 操作系统，CPU 为 Intel(R) Xeon(R) Platinum 8352V 处理器，32 GB 内存，NVIDIA GeForce RTX 5090Ti GPU，同时使用编程语言 Python3.10 和深度学习框架 PyTorch 2.1.2 来实现本文方法。在训练和测试过程中选用五折交叉验证，同时采用 Adam 作为优化器，选取 ReLU 作为激活函数防止模型不收敛及梯度消失等问题，具体如表 3 所示。

表 3　模型参数设置

参数	值
轮数	100
批量样本数	1 024
学习率	0.000 1
优化器	Adam
激活函数	ReLU
权重衰减	0.000 01

4.3　异常流量检测实验与结果分析

为了验证本文方法的有效性，本节首先开展检测的流量样本是正常流量还是攻击流量的二分类实验验证；进而系统深入地开展异常流量样本属于数据集中所给定的哪一类攻击流量的多分类实验验证。本节工作的重点是通过二分类与多分类实验，验证所构建检测模型的有效性。

4.3.1　二分类实验对比

为了剥离攻击类型间的差异干扰，聚焦框架解决核心问题的基础能力，本文先从二分类的场景验证所提方法的检测性能。将本文方法分别与其他 6 种传统的采样方法及主流的模型方法进行对比，具体如表 4 所示，其中加粗数据表示最佳性能。

由表 4 可知，本文方法在两个数据集上都取得了较好的性能，在保持高精确率和召回率的情况下，大幅度降低了误报率，说明本文方法对少数类识别敏感，能较好地解决类不平衡问题，提升检测

的鲁棒性。

在NSL-KDD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，其中准确率、召回率和F1分数均为99.47%，精确率为99.48%，误报率仅为0.10%。其主要原因是，传统过采样方法通过合成少数类样本平衡类别分布，但插值运算生成的新样本易被噪声干扰且偏离真实流量特征分布，导致模型对U2R、R2L等低频攻击的泛化能力较弱；深度生成模型虽通过学习数据分布生成样本缓解了噪声干扰问题，但MHA-Res-PDC难以捕捉流量数据的多尺度特征关联，VAE-CWGAN的特征提取局限于浅层映射，无法挖掘高维特征间的非线性关系，致使前者F1分数仅为58.90%，后者虽准确率达98.95%，但误报率高达1.04%；单一深度学习模型依赖串行特征提取架构，1DCNN-BiLSTM存在特征提取不全面的问题，ST-CFA的特征对齐机制在噪声环境下难以保留关键少数类特征，二者误报率均偏高。本文方法通过协同架构设计，既实现了流量多尺度特征的全面覆盖，又通过动态通道强化与梯度调制策略，解决了特征辨识度不足与类不平衡两大难题，最终实现了高精确率和低误报率的良好性能。

在CIC-IDS-2017数据集上的实验进一步表明，本文方法在整体性能上仍具备一定优势，FPR仅为0.07%，PRE高达99.95%，这反映出该方法在样本识别和判定上具有较高的准确性。尽管其召回率略低于ASO opt CNN方法，但差距极小，不足0.01%，并未对检测性能产生影响。

值得注意的是，在CIC-IDS-2017数据集上，多数现有的类别平衡方法在ACC、PRE、REC、F1分数等主要指标上均可达到99%以上。这一普遍现象是因为该数据集采集过程规范、特征构造全面，涵盖了流持续时间、包大小、协议类型等多维度统计属性，为模型提供了区分度较高的输入特征。同时，虽然数据分布仍存在一定的不平衡性，但并未出现如NSL-KDD数据集中某些攻击类别极端稀少的情况，从而使模型能够较为充分地从各个类别中学习。

两个数据集的FPRvsF1分数曲线分别如图4和图5所示。本文方法在NSL-KDD和CIC-IDS-2017数据集上均展现出卓越的检测性能。实验结果表明，本文方法在验证中F1分数稳定维持在99.40%以上，波动范围仅0.15%，验证了多尺度卷积金字塔通过跨尺度特征融合对流量局部特征和全局特征的捕获能力，以及通道注意力机制对异常敏感特征的动态增强有效性。

表4 本文方法二分类对比结果

数据集	方法	ACC	PRE	REC	FPR	F1分数
NSL-KDD	MFC[24]	—	94.61%	95.06%	—	94.83%
	1DCNN-BiLSTM[30]	93.17%	93.52%	94.55%	8.64%	94.03%
	MSRC[14]	—	89.43%	87.05%	—	88.22%
	VAE-CWGAN[31]	98.95%	98.95%	98.95%	1.04%	98.95%
	ST-CFA[36]	93.91%	96.08%	93.70%	—	92.55%
	MHA-Res-PDC[23]	80.82%	85.09%	57.20%	—	58.90%
	本文方法	**99.47%**	**99.48%**	**99.47%**	**0.10%**	**99.47%**
CIC-IDS-2017	1DCNN-BiLSTM[30]	98.65%	97.21%	99.77%	3.07%	98.40%
	FE-MTDM[28]	99.59%	99.60%	99.59%	0.14%	99.49%
	CSK-RF[29]	99.59%	98.04%	99.89%	0.49%	98.96%
	VAE-CWGAN[31]	99.92%	99.92%	99.92%	**0.07%**	99.92%
	ASO opt CNN[19]	95.61%	95.92%	96.96%	—	—
	MSAFE-ATD[26]	99.24%	99.17%	99.07%	—	99.12%
	本文方法	**99.95%**	**99.95%**	**99.95%**	**0.07%**	**99.95%**

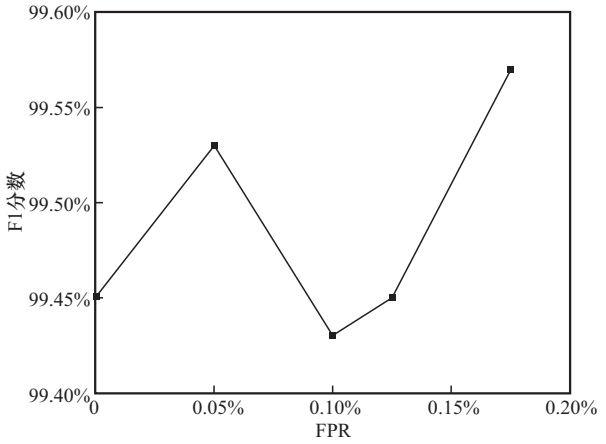

图4　NSL-KDD数据集的FPRvsF1分数曲线

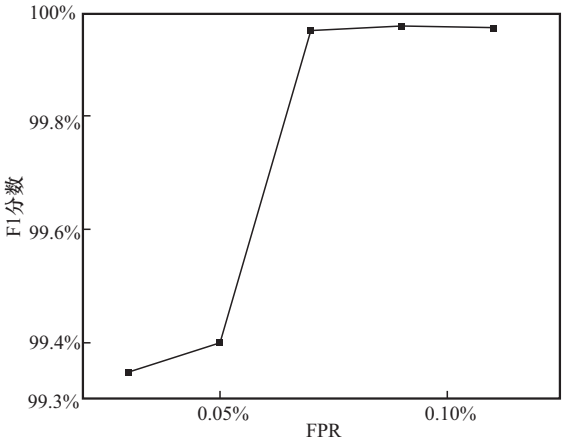

图5　CIC-IDS-2017数据集的FPRvsF1分数曲线

为了全面验证模型对复杂攻击模式的检测鲁棒性与实用性，以CIC-IDS-2017数据集为例，如图6所示。从整体趋势来看，五折实验的训练损失与验证损失均呈现快速收敛特性，训练初期各轮次内两类损失值显著下降，最终稳定于低位区间，且同一折的训练损失与验证损失始终同步收敛，未出现偏差分离现象，表明模型具备良好的泛化能力。从各折实验具体表现分析，第一折收敛速度最快且曲线平滑，第二折所需训练轮次最少，第三折损失值呈匀速下降趋势，第四折虽初始损失值较高但仍能有效收敛，第五折的收敛模式与第一折高度相似。综合可知，模型对数据划分方式不敏感，无过拟合迹象，训练效率突出，多数折在25轮内即可实现收敛，且最终验证损失显著低于领域常用阈值，充分证明该模型能够快速适应不同流量模式的变化，对各类攻击具备稳定检测能力，训练过程高效且可靠。

4.3.2　多分类实验对比

为了验证框架在攻击类型差异化场景下的特征辨别能力与泛化性，本文又从多分类的场景中验证了所提方法的检测性能。将本文方法分别与其他6种传统的采样方法及主流的模型方法进行对比，具体如表5所示，其中加粗数据表示最佳性能。

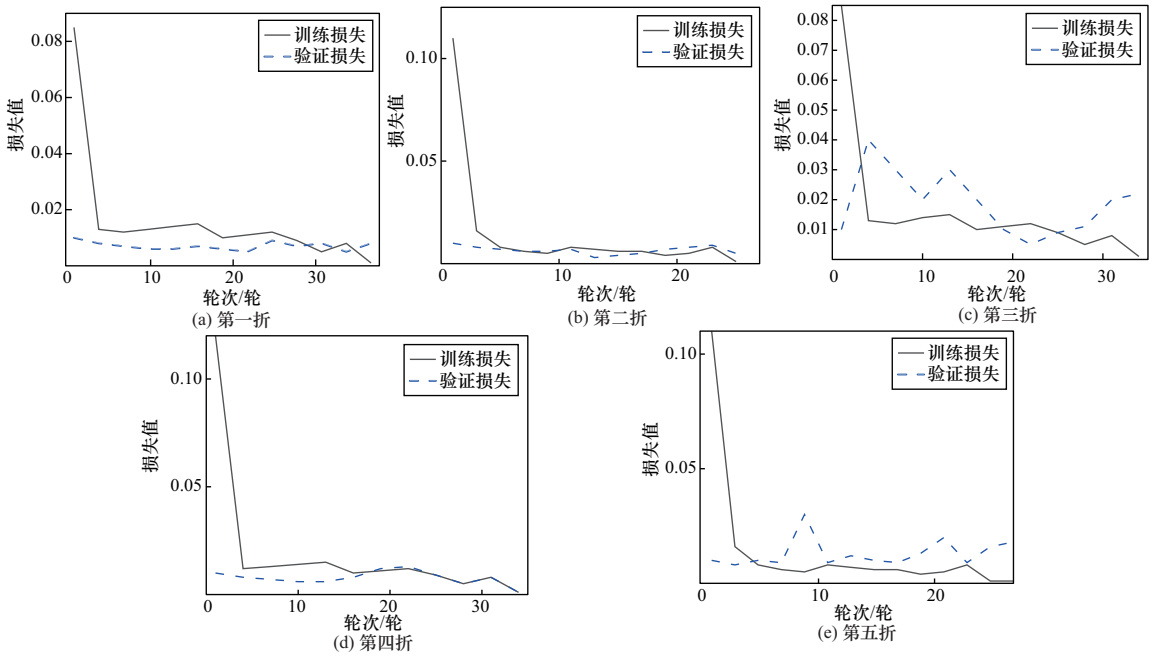

图6　CIC-IDS-2017数据集的每一折训练损失和验证损失的变化

由表5可知，本文方法在NSL-KDD数据集上的准确率为99.45%，精确率为99.43%，召回率为99.45%，F1分数为99.41%，误报率仅为0.50%，其在5个性能指标上均优于其他6种对比方法。相较于其他对比方法，本文方法在准确率上提升了0.31%~16.93%，在精确率上提升了0.11%~40.20%，在召回率上提升了0.95%~52.74%，在F1分数上提升了0.54%~49.11%，在误报率上降低了53.27%~72.97%。

对于CIC-IDS-2017数据集而言，本文方法在除精确率外的4个性能指标上都为最优，而在准确率上最大提升了2.22%、在召回率上最大提升了1.53%、在F1分数上最大提升了1.05%，这种幅度的提升对接近100%的性能指标来说已经很不容易。具体来看，本文方法的准确率、召回率和F1分数均达到99.95%，相较于次优方法CFC-Net分别提升了0.11%、0.21%和0.12%；相较于性能表现相对薄弱的MSAFE-ATD方法则分别提升了2.22%、1.53%和1.05%，充分彰显了本文方法在高性能情况下的优化能力。最重要的是，本文方法的误报率仅为0.02%，相较于CFC-Net降低了83.33%，相较于VAE-CWGAN降低了89.47%，充分验证了其在复杂场景下的精准分类能力与强鲁棒性。

两个数据集的多分类混淆矩阵分别如图7和图8所示，绝大多数样本被正确分类，元素分布高度集中于主对角线，模型分类性能优异，其中，“0”代表正常流量，“1”代表探测攻击，“2”代表拒绝服务攻击，“3”代表用户到根攻击，“4”代表远程到本地攻击。在图7中，类别0仅有极少量样本被误判为其他类别，这表明模型在识别类别0时十分精准，能够敏锐捕捉该类别样本的关键特征。类别1虽有一定数量的误判情况，但仍有48个样本被正确预测，说明模型对类别1的部分特征能够有效判别。尤为突出的是类别2，几乎没有将其他类别误判的情况，充分彰显了模型在处理类别2样本时的能力。类别3和类别4的预测结果为模型的后续优化指明了方向，后续可针对性地调整模型参数或增加相关样本训练量。总体而言，模型在多个类别上展现出了良好的识别基础，具备进一步优化提升的潜力。观察图8，能看到模型性能有了显著的提升。类别0的误判数量极少，说明模型在处理类别0样本时的稳定性和准确性达到了很高的水平。类别1的误判情况也控制在较低水平，表明模型对类别1的特征学习更为深入和准确。类别2样本的正确预测数量多，在识别该类别上表现不错。尽管类别3样本的正确预测数相对较少，但与图7相比已有一定改善。整体来看，模型在大多数类别上展现出了优秀的识别能力，正确预测数大幅增加，误判率降低，说明模型融合多尺度卷积与通道注意力机制、改进均衡损失函数等策略取得了良好成效，能够有效处理不同类别的恶意流量样本，在网络流量异常检测任务中已具备很强的实用性和可靠性。

表5 **本文方法多分类对比结果**

数据集	方法	ACC	PRE	REC	FPR	F1分数
NSL-KDD	KD-TCNN[37]	98.44%	98.60%	98.47%	—	98.51%
	CSK-RF[29]	99.14%	94.03%	98.70%	—	96.31%
	DWGF-IDS[33]	85.05%	70.92%	65.11%	—	66.67%
	1DCNN-BiLSTM[30]	97.39%	98.32%	94.55%	1.85%	95.88%
	VAE-CWGAN[31]	98.91%	98.91%	98.91%	1.07%	98.91%
	ST-CFA[36]	85.38%	89.74%	76.52%	—	83.04%
	本文方法	**99.45%**	**99.43%**	**99.45%**	**0.50%**	**99.41%**
CIC-IDS-2017	KD-TCNN[37]	99.44%	99.48%	99.47%	—	99.46%
	CSK-RF[29]	99.77%	99.83%	99.77%	—	99.78%
	VAE-CWGAN[31]	99.79%	99.79%	99.79%	0.19%	99.79%
	DCGCANet[25]	99.60%	99.60%	99.60%	—	99.60%
	MSAFE-ATD[26]	97.78%	97.78%	98.44%	—	98.91%
	CFC-Net[32]	99.84%	**99.97%**	99.74%	0.12%	99.83%
	本文方法	**99.95%**	99.95%	**99.95%**	**0.02%**	**99.95%**

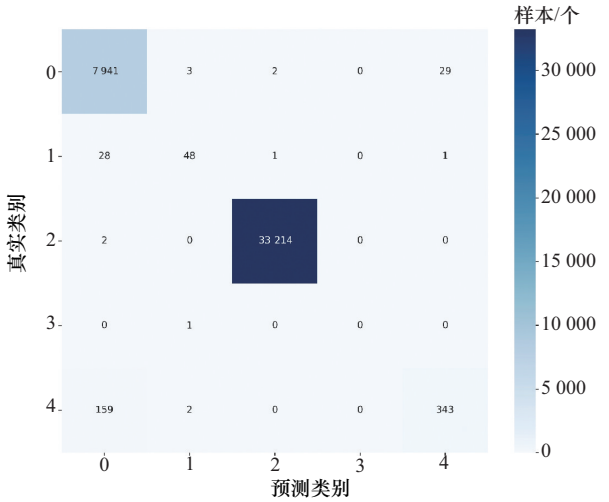

图7　NSL-KDD数据集的多分类混淆矩阵

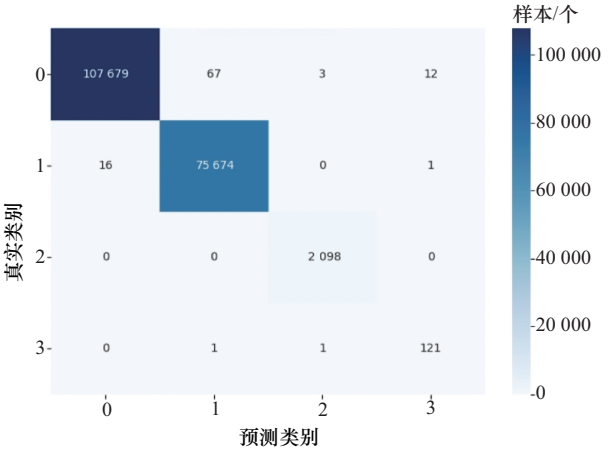

图8　CIC-IDS-2017数据集的多分类混淆矩阵

4.4　对比实验与结果分析

为了对模型架构的适应性进行验证，本文进行了两个对比实验研究：金字塔卷积核尺寸的选取实验和注意力机制的对比实验。

4.4.1　金字塔卷积核尺寸的选取实验

为验证多尺度卷积模块中选用卷积核尺寸为1、3和5组合的合理性与最优性，明确卷积核尺寸选择与网络流量特征的匹配逻辑，设计了四选三对比实验：从1、3、5和7这4种候选卷积核尺寸中剔除一种形成4组对比组合，通过低频攻击检测率REC、F1分数和误报率核心指标，在CIC-IDS-2017数据集的低频攻击子集中验证不同卷积核尺寸组合的检测性能。

实验结果如表6所示，本文采用的[1, 3, 5]组合表现最优，F1分数达87.57%，低频攻击检测率为99.95%，误报率仅为1.54%；[1, 5, 7]、[3, 5, 7]和[1, 3, 7]组合的F1分数分别降至83.48%、84.61%和85.17%，召回率均低于99.59%，误报率均高于1.88%。该实验充分证明，[1, 3, 5]组合是适配多类型攻击检测的最优选择，有效支撑了PyConv“多尺度”设计的必要性与科学性。

表6　金字塔卷积核尺寸的选取实验结果

卷积核组合	F1分数	REC	FPR
[1, 3, 7]	85.17%	99.59%	1.88%
[1, 5, 7]	83.48%	99.43%	2.14%
[3, 5, 7]	84.61%	99.09%	1.92%
[1, 3, 5]	**87.57%**	**99.95%**	**1.54%**

4.4.2　注意力机制的对比实验

为深入验证不同注意力机制在低频攻击检测任务中的适用性，本文设计了系统的对比实验，旨在定量评估通道注意力、空间注意力及混合注意力在捕获网络流量异常特征方面的性能差异。实验选取4种代表性注意力机制构建对比模型，以无注意力模型作为基线模型，仅包含多尺度卷积与全连接层；而通道注意力通过全局平均池化与全连接层学习通道权重；空间注意力是基于Transformer架构，聚焦序列位置间依赖关系的模型；混合注意力是结合通道与空间注意力机制的模型，实验依旧采用CIC-IDS-2017数据集中的低频攻击子集来构建正常样本与低频攻击样本极端不平衡的二分类任务。实验结果如表7所示，通道注意力模型的F1分数显著高于空间注意力和混合注意力模型，同时其误报率为三者中最低。这直接证明，在网络流量异常检测任务中，聚焦特征通道语义的通道注意力模型比聚焦时间维度关联的空间注意力模型更为有效。原因在于网络流量数据的判别性信息主要蕴含于不同统计特征的通道语义差异中，而非局部空间模式。空间注意力模型对时间关联的过度关注，可能引入噪声并分散模型对关键通道特征的判别力。本文通过严格的性能对比，完成了对模型核心组件创新性的有效验证。

表7　注意力机制的对比实验结果

模型	F1分数	REC	FPR
无注意力	87.34%	99.4%	0.36%
空间注意力	87.03%	99.4%	0.37%
混合注意力	86.36%	99.4%	0.40%
通道注意力	**91.81%**	**99.6%**	**0.22%**

4.5 消融实验与结果分析

在明确了各核心组件的作用后，为系统性验证模型核心组件的贡献度，证明所提完整框架的必要性与协同优势，本文构建了 4 组对比实验架构。

1) 基准模型：仅包含基础一维卷积层与全连接层，作为性能参照基线。

2) 无注意力模型：嵌入多尺度卷积模块，移除通道注意力机制。

3) 无多尺度模型：集成通道注意力机制，移除多尺度特征提取模块。

4) 完整模型：融合多尺度卷积模块与通道注意力机制双组件，优化参数配置。

实验采用分层三折交叉验证，每折严格维持原始数据集的类别分布，通过跨折结果均值评估组件稳定性。该设计遵循单一变量原则，确保各模型变体的性能差异仅由目标组件的增减导致。消融实验结果如表 8 所示，完整模型在所有关键指标上表现最优，准确率、F1 分数、精确率和召回率均达到 99.95%，误报率低至 0.07%，显著优于其他模型，证实了模型组件协同作用的有效性。

表 8 消融实验结果

模型	ACC	F1 分数	PRE	REC	FPR
基准	99.91%	99.91%	99.92%	99.90%	0.15%
无注意力	99.89%	99.89%	99.88%	99.90%	0.14%
无多尺度	99.92%	99.92%	99.91%	99.91%	0.13%
完整	**99.95%**	**99.95%**	**99.95%**	**99.95%**	**0.07%**

完整模型相较于基准模型，在所有指标上同时突破 99.95%，凸显了 PyConv 与 SEBlock 的协同增效。其低至 0.07% 的 FPR，仅为其他模型的一半，大幅减少了误报带来的运维成本，在实际网络安全场景中极具应用价值。对比无注意力与基准模型发现，移除注意力模块后，PRE 下降至 99.88%，FPR 仅微降至 0.14%。这表明注意力模块虽对 FPR 改善有限，但能显著提升精确率，通过特征重标定增强模型对关键攻击特征的识别能力。不过，单独移除注意力模块会导致整体精确率轻微下滑，体现其在模型中的不可或缺性。将无多尺度与基准模型对比，无多尺度模型 REC 提升至 99.91%，FPR 降低至 0.13%。PyConv 通过多尺度特征提取，增强了模型对复杂攻击模式的适应性，在提升检测能力的同时降低误报风险。但单独使用 PyConv 无法达到完整模型的协同效果，说明其需与其他组件配合才能发挥最大效能。

4.6 参数实验与结果分析

为了找到表现稳定且优异的参数配置，并分析不同参数的影响，增强方法可信度，本文进行两个参数实验研究：参数敏感性实验和超参数实验。

4.6.1 参数敏感性实验

为了验证由模型结构定义的、可学习的或加权的系数，其取值是否合理且敏感度适中，本文采用系统性实验设计评估其对模型性能的影响。选取 4 类关键超参数进行敏感性分析，每类参数设置 4 个测试水平。学习率（learning rate, LR）设置为 1×10^{-4}、3×10^{-4} 和 1×10^{-3}；批大小（batch size, BS）设置为 256、1 024 和 2 048；权重衰减（weight decay, WD）设置为 0、1×10^{-5} 和 1×10^{-4}；EQLv2 损失权重（EQL weight, EW）设置为 0.3、0.5 和 0.7。

实验采用控制变量法进行系统测试。每次实验仅改变一个参数，保持其他参数为默认值，每个参数组合作为一组独立实验，共 12 组实验，每组实验采用五折交叉验证确保结果可靠性，独立训练模型并记录 8 项性能指标。实验结果如表 9 所示，模型在不同参数组合下均展现出超高检测性能，准确率、F1 分数和召回率稳定在 99.95%~99.96%，误报率低至 0.04%~0.08%，体现出对参数变化的强鲁棒性。具体来看，当学习率 LR 最优值为 0.000 3、批大小 BS 为 256 时，误报率最低。

权重衰减的引入对误报率有轻微影响，实现了性能与梯度调制机制的强关联。当 EW 从 0.3 增至 0.5 时，反映多数类梯度抑制效果的误报率从从 0.06% 降至 0.05%，印证了 EQLv2 对多数类梯度的有效抑制；而少数类召回率始终稳定在 99.96%，证明 EW 增大后少数类梯度得到充分增强，模型得以精准捕捉低频攻击的微弱特征；当 EW 进一步增至 0.7 时，性能未出现过拟合或衰减，表明梯度调制达到稳定状态，进一步验证了机制的可靠性。实验结果与 EQLv2 梯度表达式的理论逻辑相符合，为理论推导提供了直接的数据支撑。

综上所述，批大小对误报率影响最显著，而 EW 是唯一能降低误报率的参数。基于性能与效率的平衡，推荐 LR=3×10^{-4}、BS=1 024、WD=0 和

表9　　参数敏感性实验结果

参数名称	LR	BS	WD	EW	ACC	F1 分数	PRE	REC	FPR
LR=1×10^{-4}	0.000 1	1 024	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.05%
LR=3×10^{-4}	0.000 3	1 024	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.06%
LR=1×10^{-3}	0.001	1 024	0.000 01	0.5	99.95%	99.95%	99.95%	99.95%	0.08%
BS=256	0.000 3	256	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.04%
BS=1 024	0.000 3	1 024	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.05%
BS=2 048	0.000 3	2 048	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.06%
WD=0	0.000 3	1 024	0	0.5	99.95%	99.95%	99.95%	99.95%	0.06%
WD=1×10^{-5}	0.000 3	1 024	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.07%
WD=1×10^{-4}	0.000 3	1 024	0.000 1	0.5	99.96%	99.96%	99.96%	99.96%	0.07%
EW=0.3	0.000 3	1 024	0.000 01	0.3	99.96%	99.96%	99.96%	99.96%	0.06%
EW=0.5	0.000 3	1 024	0.000 01	0.5	99.96%	99.96%	99.96%	99.96%	0.05%
EW=0.7	0.000 3	1 024	0.000 01	0.7	99.96%	99.96%	99.96%	99.96%	0.05%

EW=0.5 的配置，可实现 99.96%F1 分数、0.05%FPR 的表现。在实际部署中，安全关键场景可选用 BS=256 和 EW=0.7 以追求更低的误报率，实时检测场景则可采用 BS=2 048 和 LR=0.000 1 来提升处理效率，该分析为模型在不同工业场景下的优化部署提供了实证依据。

4.6.2　*超参数实验*

在网络流量异常检测模型中，位置注意力系数μ、通道注意力系数β和加权融合系数γ是影响模型性能的关键因素。位置注意力系数μ主要作用于特征向量的位置权重动态调节，可增强模型对位置信息的表达。通道注意力系数β用于调整模型在不同通道维度的权重，通过强化特征关联性，突出关键通道特征。加权融合系数γ负责在局部与全局特征间进行加权平衡，进一步提升模型的检测能力。

为验证上述系数的作用原理，将μ、β和γ分别在0~1取值，并在CIC-IDS2017数据集上开展异常流量检测二分类实验，分析不同参数设置下的F1分数变化。结合图9展示的实验结果可知，随着μ、β和γ取值变化，模型在该数据集上的F1分数呈现出明显的先升后降趋势。方形折线代表位置注意力系数μ，当μ从0开始增加至0.3时，F1分数从99.93%下降至99.92%；当μ为0.5和0.7时，F1分数回升至99.94%；当μ达到1.0时，F1分数又回落至99.92%。圆形折线表示通道注意力系数β，其在从0增加到0.3和0.5时，F1分数保持在99.94%，后续随着取值增大而有所下降。三角形折线表示加权融合系数γ，其在大部分取值下F1分数维持在99.94%，在取值为1.0时降至99.92%。总体来看，当$\mu < 0.7$、$\beta < 0.5$和$\gamma < 0.5$时，检测性能随参数值增加而提升；当$\mu = 0.7$、$\beta = 0.5$和$\gamma = 0.5$时，F1分数达最高；当$\mu > 0.7$、$\beta > 0.5$和$\gamma > 0.5$时，检测性能下降。原因在于μ过低时模型无法充分利用位置信息，μ过高则对训练数据特定特征过度敏感，忽略空间特征；当$\gamma = 0.5$时，模型对局部与全局特征融合均衡，避免单一特征过度依赖。因此，确定$\mu = 0.7$、$\beta = 0.5$和$\gamma = 0.5$为最优的参数配置。

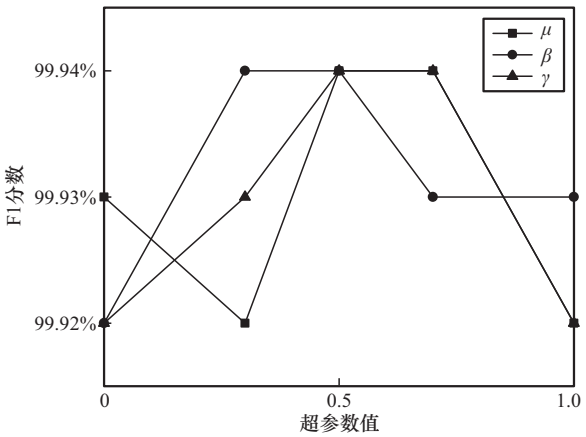

图9　CIC-IDS-2017数据集上不同超参数实验结果

4.7 计算效率实验与结果分析

为了评估模型在实际应用场景中的可行性与实用性，本文建立了多维度的计算效率评估框架，通过参数量、推理时间和推理速度3个核心指标全面衡量模型性能。

参数量是统计模型所有可训练参数的总和，反映模型复杂度。推理时间是测量模型处理完整验证集所需的时间。推理速度是计算单位时间内处理的样本数量。实验结果如表10所示，本文模型在五折交叉验证中展现出良好的计算效率。参数量稳定维持在387 754个可训练参数，平均推理时间仅0.338 s，推理速度高达109 760个/s。这种参数高效、推理迅速且高度稳定的特性，使模型可部署在5G核心网、边缘安全网关及云安全中心等关键基础设施。

表10 计算效率实验结果

折数	参数量/个	推理时间/s	推理速度/(个·s^{-1})
1	387 754	0.352 362 323	105 334.758
2	387 754	0.336 378 193	110 340.089 8
3	387 754	0.336 828 542	110 192.562 1
4	387 754	0.325 762 63	113 935.720 8
5	387 754	0.340 513 229	108 997.233 6
平均	387 754	0.338 368 983	109 760.072 8

5 结束语

本文提出了一种新颖的网络流量异常检测框架，旨在类不平衡条件下提升所提方法的分类性能。该框架不仅能捕获全局与局部的语义信息，有效提升模型对低频攻击的敏感性。还能利用通道注意力机制与动态梯度调制策略降低误报率，实现对恶意攻击的精准识别。本文方法在NSL-KDD与CIC-IDS-2017数据集上开展仿真实验，结果表明，本文方法在准确率、召回率与误报率上均优于现有方法，其中CIC-IDS-2017数据集上的F1分数达到99.95%，误报率低至0.02%，验证了本文方法在复杂网络环境中的有效性。

随着网络攻击手段的不断演化，网络流量异常检测技术需持续融合多模态感知与自适应学习能力。本文方法在特定场景下仍存在局限，当面对端到端加密流量时，因载荷特征被完全遮蔽，模型对依赖内容特征的攻击检测能力显著下降。未来研究需融合元数据行为画像与迁移学习以突破加密流量瓶颈，并探索原型网络等小样本学习技术提升稀有攻击的识别鲁棒性。

参考文献：

[1] Dan D V, Thanh T M. Unauthorized iot devices detection based on network traffic using augmentation fusion classification method[J]. International Journal of Information Security, 2025, 24(6): 225.

[2] Wang K X, Cui Y H, Shen G W, et al. PRAETOR: packet flow graph and dynamic spatio-temporal graph neural network-based flow table overflow attack detection method[J]. Journal of Network and Computer Applications, 2025, 243: 104333.

[3] Khatami S S, Shoeibi M, Oskouei A E, et al. 5DGWO-GAN: a novel five-dimensional gray wolf optimizer for generative adversarial network-enabled intrusion detection in IoT systems[J]. Computers, Materials & Continua, 2025, 82(1): 881-911.

[4] 陈骏. 类别不平衡问题的分类算法研究[D]. 上海: 东华大学, 2025.
Chen J. Research on classification algorithms for class imbalance problem[D]. Shanghai: Donghua University, 2025.

[5] Rafiullah A, Wang H. Heterogeneous treatment effects estimation with residualized LASSO and support vector machines[J]. Journal of the Korean Statistical Society, 2025: 1-32.

[6] Lv M Q, Gan S D, Xu K, et al. An interpretable network intrusion detection model via decision tree enhanced deep attention network[J]. IET Information Security, 2025, 2025(1): 5552833.

[7] Fang C, Liu Y K, Teng S L, et al. CrossModal-CLIP: a novel multimodal contrastive learning framework for robust network traffic anomaly detection[J]. Computer Networks, 2025, 272: 111723.

[8] Bibri S E, Huang J. Generative AI of things for sustainable smart cities: synergizing cognitive augmentation, resource efficiency, network traffic, cybersecurity, and anomaly detection for environmental performance[J]. Sustainable Cities and Society, 2025, 133: 106826.

[9] 李振源, 韦洋洋, 王征凯, 等. 智能溯源分析与入侵检测: 洞察、挑战与展望[J]. 计算机学报, 2025, 48(10): 2406-2429.
Li Z Y, Wei Y Y, Wang Z K, et al. Learning in provenance-based intrusion detection: a survey[J]. Chinese Journal of Computers, 2025, 48(10): 2406-2429.

[10] Dhanabal L, Shantharajah S P. A study on NSL-KDD data set for intrusion detection system based on classification algorithms[J]. International Journal of Advanced Research in Computer and Communication Engineering, 2015, 4(6): 446-452.

[11] Sharafaldin I, Lashkari A H, 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. Piscataway: IEEE Press, 2018: 108-116.

[12] 陆浩天, 董育宁, 全宇轩. 一种基于双层模型和指标分布的恶意网络流持续检测和分类方法[J]. 电子学报, 2025, 53(5): 1637-1649.
Lu H T, Dong Y N, Quan Y X. A method for continuous detection and

classification of malicious network traffic based on double-layer model and distribution of indexes[J]. Acta Electronica Sinica, 2025, 53(5): 1637-1649.

[13] 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.

[14] 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.

[15] 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.

[16] 谢丽霞, 魏晨阳, 杨宏宇, 等. 基于多维度动态加权alpha图像融合与特征增强的恶意软件检测方法[J]. 电子学报, 2025, 53(3): 849-863.
Xie L X, Wei C Y, Yang H Y, et al. Malware detection method based on multi-dimensional dynamic weighted alpha image fusion and feature enhancement[J]. Acta Electronica Sinica, 2025, 53(3): 849-863.

[17] Hou T H, Xing H Y, Liang X Y, et al. A marine hydrographic station networks intrusion detection method based on LCVAE and CNN-BiLSTM[J]. Journal of Marine Science and Engineering, 2023, 11(1): 221.

[18] 单康康, 袁书宏, 陈文智, 等. 基于神经网络的恶意DNS流量检测方法[J]. 通信学报, 2024, 45(S2): 1-6.
Shan K K, Yuan S H, Chen W Z, et al. Malicious DNS traffic detection based neural networks[J]. Journal on Communications, 2024, 45(S2): 1-6.

[19] Patil N, Joshi S. Enhanced arachnid swarm-tuned convolutional neural network model for efficient intrusion detection[J]. International Journal of Advanced Computer Science and Applications, 2024, 15(5): 1151-1163.

[20] Xie Y, Chen H. A novel method for effective intrusion detection based on convolutional speaking neural networks[J]. Journal of King Saud University - Computer and Information Sciences, 2024, 36(2): 101975.

[21] Shang G, Chen J. Subsurface defect detection of concrete-filled steel tubular (CFST) structure based on a two-stage unsupervised learning method[J]. Construction and Building Materials, 2025, 502: 144404.

[22] Hernandez-Jaimes M L, Martinez-Cruz A, Ramírez-Gutiérrez K A, et al. Network traffic inspection to enhance anomaly detection in the Internet of things using attention-driven deep learning[J]. Integration, 2025, 103: 102398.

[23] Qi G R, Huang K, Mao J, et al. Multi-head attention enhanced parallel dilated convolution and residual learning for network traffic anomaly detection[J]. Computers, Materials & Continua, 2025, 82(2): 2159-2176.

[24] 段雪源, 付钰, 王坤, 等. 基于多尺度特征的网络流量异常检测方法[J]. 通信学报, 2022, 43(10): 65-76.
Duan X Y, Fu Y, Wang K, et al. Network traffic anomaly detection method based on multi-scale characteristic[J]. Journal on Communications, 2022, 43(10): 65-76.

[25] 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.

[26] 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.

[27] 赵小强, 何嘉琦. 基于最大安全近邻与局部密度的自适应过采样方法[J]. 电子与信息学报, 2025, 47(4): 1140-1149.
Zhao X Q, He J Q. Adaptive oversampling method based on maximum safe nearest neighbor and local density[J]. Journal of Electronics & Information Technology, 2025, 47(4): 1140-1149.

[28] Wei N, Yin L H, Zhou X M, et al. A feature enhancement-based model for the malicious traffic detection with small-scale imbalanced dataset[J]. Information Sciences, 2023, 647: 119512.

[29] 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.

[30] 尹梓诺, 马海龙, 胡涛. 基于联合注意力机制和一维卷积神经网络-双向长短期记忆网络模型的流量异常检测方法[J]. 电子与信息学报, 2023, 45(10): 3719-3728.
Yin Z N, Ma H L, Hu T. A traffic anomaly detection method based on the joint model of attention mechanism and one-dimensional convolutional neural network-bidirectional long short term memory[J]. Journal of Electronics & Information Technology, 2023, 45(10): 3719-3728.

[31] 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.

[32] 安义帅, 付钰, 俞艺涵, 等. 基于数据增强与特征挖掘的异常流量检测方法[J]. 通信学报, 2025, 46(8): 16-30.
An Y S, Fu Y, Yu Y H, et al. Anomaly traffic detection method based on data augmentation and feature mining[J]. Journal on Communications, 2025, 46(8): 16-30.

[33] Gu Y H, Yang Y, Yan Y, et al. Learning-based intrusion detection for high-dimensional imbalanced traffic[J]. Computer Communications, 2023, 212: 366-376.

[34] Imrana Y, Xiang Y P, Ali L, et al. CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units[J]. Complex & Intelligent Systems, 2024, 10(3): 3353-3370.

[35] Pithani A, Rout R R. CFL-ATELM: an approach to detect botnet traffic by analyzing non-IID and imbalanced data in IoT-edge based 6G networks[J]. Cluster Computing, 2025, 28(3): 198.

[36] 寇文珍, 张清, 常兆斌. 基于时空交叉特征对齐的异常流量检测方法[J]. 福州大学学报(自然科学版), 2025, 53(4): 391-398.
Kou W Z, Zhang Q, Chang Z B. Spatio-temporal cross feature alignment for anomaly traffic detection[J]. Journal of Fuzhou University

(Natural Science Edition), 2025, 53(4): 391-398.

[37] Wang Z D, Li Z Y, He D J, et al. A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning[J]. Expert Systems with Applications, 2022, 206: 117671.

[作者简介]

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。

王玉珏（2003– ），女，湖北黄冈人，海军工程大学硕士生，主要研究方向为人工智能、网络安全。

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。

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。