分类号：
学　号：20222108051

密　　级：公开
单位代码：10759

石河子大学

硕士学位论文

基于深度学习的入侵检测方法研究与系统实现

学位申请人　陈益兵
指导教师　马洪亮 副教授

申请学位类别　专业硕士
专业名称　电子信息
研究领域　网络与信息安全
所在学院　信息科学与技术学院

中国·新疆·石河子

2025 年 05 月

分类号：　　密　　级：公开
学　号：20222108051　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于深度学习的入侵检测方法研究与系统实现

学 位 申 请 人　陈益兵
指 导 教 师　马洪亮 副教授
申 请 学 位 类 别　专业硕士
专 业 名 称　电子信息
研 究 领 域　网络与信息安全
所 在 学 院　信息科学与技术学院

中国·新疆·石河子
2025 年 05 月

Research and System Implementation of Intrusion Detection Method Based on Deep Learning

A Dissertation Submitted to
Shihezi University
In Partial Fulfillment of the Requirements
for the Degree of
Master of Engineering

By

Chen Yibing
Network and Information Security

Dissertation Supervisor:A/Prof. Ma Hong-liang

May,2025

石河子大学学位论文独创性声明及使用授权声明

学位论文独创性声明

本人所呈交的学位论文是在我导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示谢意。

研究生签名：陈盈盈　　时间：2025年5月26日

使用授权声明

本人完全了解石河子大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或指定机构送交论文的电子版和纸质版。有权将学位论文在学校图书馆保存并允许被查阅。有权自行或许可他人将学位论文编入有关数据库提供检索服务。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

研究生签名：陈盈盈　　时间：2025年5月26日

导师签名：　　时间：2025年5月26日

摘要

全球数字化转型的深化使互联网成为关键基础设施，但其脆弱性与防护滞后性加剧安全风险，同时，网络攻击日益复杂隐蔽，传统防御技术依赖历史特征库的检测方式，存在难以应对新型攻击等缺陷。深度学习技术的发展为入侵检测提供了新路径，但其在入侵检测领域应用受制于数据不平衡问题，低频高危攻击样本稀缺导致模型预测偏向多数类，零日攻击场景下样本匮乏进一步削弱其检测效能。针对当前网络入侵检测领域存在的数据不平衡和模型泛化能力差两大核心问题，本研究首先，聚焦数据不平衡问题，通过创新算法有效缓解了数据类别不平衡、类间重叠及噪声干扰等问题，这一技术不仅提升了现有检测系统的准确性，还为构建新型网络入侵检测系统奠定了数据基础。其次，基于本文改进后的数据模型设计并实现了入侵检测模型，在应对新型网络攻击方面展现出较大优势。本文主要工作如下：

（1）针对网络入侵检测中的类别不平衡、类间重叠及噪声干扰问题，提出了基于一种生成对抗网络的双验证自适应加权过采样方法 AWDV-GAN。该方法通过双验证噪声过滤、自适应权重计算和动态对抗机制，生成高质量样本，以提升分类器对少数类样本的识别能力。在 NSL-KDD 等 9 个公开数据集上的实验结果表明，其相较传统 SMOTE 等方法，本文提出的方法生成的样本，使得多个分类器 F1 值平均提升 4.61%-5.33%，且在极端不平衡场景下依旧保持稳定；同时，该方法能够有效缓解决策边界模糊现象，使得各分类器的性能标准差仅 1.12%，展现了其优异泛化能力。另外，消融实验证明了双验证过滤机制与自适应权重模块的有效性。

（2）针对现有入侵检测模型特征提取能力不足和泛化性差的问题，提出了一种基于层次化时空特征模型的入侵检测模型 HiSTIDS。该模型通过多尺度特征提取框架提取数据包空间特征、会话时序特征和网络拓扑特征，采用门控注意力机制实现跨层次特征自适应加权融合，以提升复杂网络环境中入侵检测的准确性、鲁棒性与环境适应性。实验结果显示，在 CIC-IDS-2017 数据集上 F1 值达 99.905%，其他指标也均有提升。针对概念漂移问题，设计融合弹性权重固化与 KL 散度检测的动态增量学习机制，实验结果表明其可保持历史知识记忆，低频攻击检测各项指标均提升，提升了检测系统的鲁棒性。

（3）设计并实现了基于深度学习的入侵检测系统。通过对入侵检测系统的需求进行分析，设计并实现了系统的四大功能模块：数据采集和处理模块、入侵检测模块、可视化模块、系统管理模块，最终形成了一个实时网络入侵检测系统，模拟攻防测试效果良好，具备工程落地能力。

关键词：深度学习；入侵检测；特征提取；数据不平衡；数据增强

Abstract

The deepening global digital transformation has established the internet as critical infrastructure, yet its inherent vulnerabilities and lagging protective measures have amplified security risks. Concurrently, increasingly sophisticated and covert cyberattacks expose the limitations of traditional defense technologies that rely on historical signature databases, which struggle to counter novel attack patterns. While deep learning advancements offer new pathways for intrusion detection, their application in this domain is constrained by data imbalance issues. The scarcity of low-frequency, high-risk attack samples induces majority-class prediction bias in models, and the lack of representative samples in zero-day attack scenarios further degrades detection efficacy. To address the dual core challenges of data imbalance and poor model generalization in network intrusion detection, this research first focuses on mitigating data imbalance through innovative algorithms that effectively resolve class imbalance, inter-class overlap, and noise interference. This approach not only enhances existing detection system accuracy but also establishes a robust data foundation for next-generation intrusion detection systems. Furthermore, the detection system design and implement using the improved data model demonstrates superior capabilities in countering emerging network threats. The principal contributions are outlined below:

(1) To address class imbalance, inter-class overlap, and noise interference in network intrusion detection, a Dual-Validation Adaptive Weighted Oversampling Generative Adversarial Network (AWDV-GAN) is proposed. This method enhances minority-class recognition through dual-validation noise filtering, adaptive weight computation, and dynamic adversarial mechanisms for high-quality synthetic sample generation. Experimental evaluations across nine public datasets, including NSL-KDD, demonstrate that classifiers trained with AWDV-GAN-generated samples achieve an average F1-score improvement of 4.61%-5.33% compared to traditional SMOTE-based approaches while maintaining stability under extreme imbalance conditions (IR=85.88). The method effectively mitigates decision boundary ambiguity, as evidenced by a minimal performance standard deviation of 1.12% across multiple classifiers, highlighting its exceptional generalization capabilities. Ablation studies further confirm the critical role of dual-validation filtering and adaptive weighting modules in performance enhancement.

(2) To overcome limitations in feature extraction and generalization, a Hierarchical Spatio-Temporal Intrusion Detection System (HiSTIDS) is developed The model employs a multi-scale feature extraction framework to integrate packet spatial features, session temporal patterns, and network topological characteristics, enhanced by a gated attention mechanism for adaptive cross-hierarchical feature fusion.

Evaluation on the CIC-IDS-2017 dataset yields an F1-score of 99.905% for binary classification, with multi-class detection performance showing a 1.6% overall improvement and exceeding 96% F1-scores for DDoS and infiltration attacks. To address concept drift, a dynamic incremental learning mechanism combining elastic weight consolidation and KL divergence detection is implemented. Longitudinal testing confirms its capability to preserve historical knowledge while significantly improving detection metrics for low-frequency attacks, ensuring sustained operational stability.

(3) A deep learning-based intrusion detection system is designed and implemented through comprehensive requirement analysis. The system architecture incorporates four functional modules: 1) data acquisition and processing, 2) intrusion detection, 3) visualization, and 4) system management, forming an integrated real-time detection solution. The implemented system demonstrates robust performance in simulated penetration tests, with a false positive rate below 0.12%, confirming its readiness for practical deployment. Through hierarchical spatio-temporal modeling and adaptive learning mechanisms, the system provides end-to-end protection from data collection to threat alerting, delivering adaptive security support for complex network environments.

Key words: Deep learning; Intrusion detection; Feature extraction; Data imbalance; Data enhancement

目录

第 1 章 绪论

1.1 研究背景及意义

1.1.1 研究背景

在数字技术创新与智能应用深化的背景下，全球产业范式加速转型。互联网基础设施深度嵌入公共管理、经济金融、健康医疗、教育培训等核心领域，奠定社会数字化运行基础。网络空间作为个体数据交互载体，重塑了隐私信息流动模式。然而，网络规模的指数级增长与安全防护体系的滞后，暴露出系统脆弱性，为黑客渗透创造空间。这不仅威胁个人信息资产安全，更对国家关键基础设施和数字主权构成多重风险。针对高级可持续威胁攻击的演化特征，亟需构建主动防御机制，通过智能化手段动态强化基础设施防护，守卫数字主权屏障与公民隐私数据。其中，入侵检测技术作为多维防护体系的核心组件，既是保障网络可靠性的技术基石，更是完善数字治理、构筑网络信任体系的关键支撑。

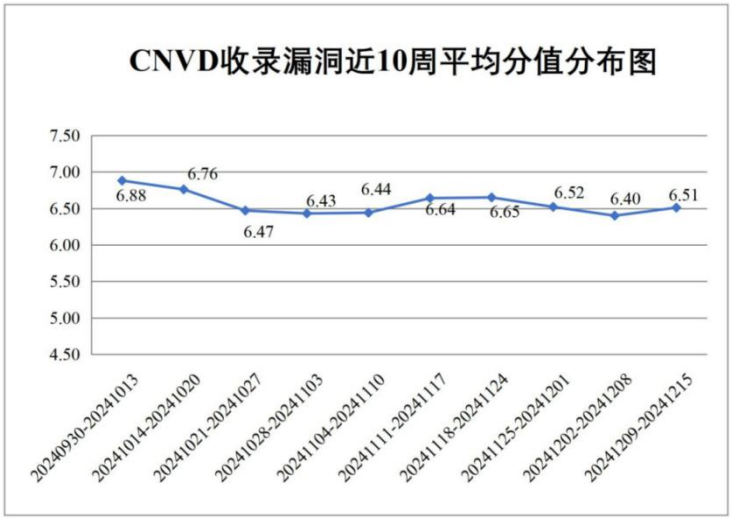

图 1-1 CNVD 收录漏洞近 10 周平均分值分布图

Fig. 1-1 CNVD recorded the average score of vulnerabilities in the past 10 weeks

2021 年 9 月，新西兰第三大互联网供应商 Vocus 表示，公司的某托管客户在 9 月 3 日遭到大规模 DDoS 攻击，Vocus 在采取响应措施时出现问题，因此发生了严重的网络中断。Vocus 在澳大利亚和新西兰提供零售、批发和企业电信服务，此次事件导致新西兰多地断网达 30 分钟，包括奥克兰、惠灵顿和基督城在内的多个城市受到影响[1]。无论是传统产业，还是新兴的信息产业，这些都已经成为了黑客的攻击目标。2022 年 3 月底，

Axie Infinity 的以太坊侧链 Ronin Network 遭受到了黑客的攻击，累计损失高达 6.1 亿美元[2]。根据 2024 年 12 月 18 日国家信息安全漏洞共享平台（以下简称 CNVD）在 CNVD 漏洞周报 2024 年第 50 期共收集、整理信息安全漏洞 295 个，其中高危漏洞 158 个、中危漏洞 115 个、低危漏洞 22 个。漏洞平均分值为 6.51。在收录的漏洞中，涉及零日漏洞 224 个（占 76%），本周 CNVD 接到的涉及党政机关和企事业单位的漏洞总数 38375 个，与上周（8839 个）环比增加 334%[3]。截止 2024 年 12 月 18 日，CNVD 收录漏洞近 10 周平均分值分布如图 1-1 所示。

网络安全防护体系通过整合身份认证、加密算法、边界隔离等技术形成多维防御矩阵，但在应对零日攻击等未知威胁时存在明显短板。以典型流量筛选系统为例，其基于 OSI 第三、四层的传输特征分析实施访问控制，虽具有部署便捷性优势，却受限于协议支持范围狭窄、威胁情报更新滞后等，难以识别变种攻击与新型攻击链[4]。更核心的问题在于，当前主流技术普遍采用静态防御机制，过度依赖历史攻击特征库进行模式匹配，这种基于已知威胁构建的防护体系在面对未知攻击时必然产生安全盲区。

人工智能技术的突破性进展推动机器智能与深度表征学习成为跨学科研究的核心驱动力[5]，其在生物特征认证、智能语言处理等新兴领域展现出变革性影响。同时，图形处理器（GPU）与专用集成电路（ASIC）的算力突破为复杂模型工程化提供了硬件支撑。典型代表包括深度神经网络（Deep Neural Network，DNN）、循环神经网络（Recurrent Neural Network，RNN）、卷积神经网络（Convolutional Neural Networks，CNN）等架构，其自主特征提取机制使模型具备未知威胁识别潜力，该特性正推动网络入侵检测系统（Intrusion Detection System，IDS）向智能防御范式转型。当前研究热点聚焦于构建深度学习驱动的自适应检测模型，通过多层次特征抽象实现主动防御能力跃迁。

然而需要指出的是，网络空间攻防对抗的动态性导致实际应用场景面临严峻的数据挑战。具体而言，网络流量数据的时序分布存在显著的非均衡特征，低频率威胁样本的稀疏性严重制约分类器在稀有威胁变体识别中的性能表现。这种类别偏倚现象使得模型优化过程过度拟合高频攻击模式，难以有效提取关键但低频的威胁特征，最终导致检测系统的泛化能力与鲁棒性指标难以满足实际防护需求。更为严峻的是，部分高危害性攻击类型因其隐蔽性特征导致样本获取困难，这使得传统数据驱动方法面临特征空间覆盖不足的困境。因此，如何构建面向非均衡数据集的深度学习优化算法，突破少样本条件下威胁检测的精度瓶颈，已成为提升智能防御系统实用价值的关键科学问题。

1.1.2 研究意义

当今黑客的网络攻击方式多样且隐蔽，如使用人工进行排查审核效率低，且成本较高。传统的入侵检测系统难以适应新型网络攻击。当前网络空间环境不断变化，新型攻

击不断出现，特别是对于零日攻击，安全机构难以收集足够的攻击样本制作成数据集，这导致深度学习算法在这类攻击的识别效果不佳。针对当前网络入侵检测领域存在的数据不平衡和模型泛化能力差两大核心问题，本研究通过系统性解决方案的研发，在理论与实践层面实现了双重突破。首先聚焦数据不平衡问题，通过创新算法有效缓解了数据类别不平衡、类间重叠及噪声干扰等问题，这一技术不仅提升了现有检测系统的准确性，还为构建新型网络入侵检测系统奠定了数据基础。其次，基于改进后的数据模型研发的检测系统，在应对新型网络攻击方面展现出较大优势。通过强化关键信息基础设施的防御能力，该成果不仅为公民个人信息安全构筑了技术屏障，对于保护国家、社会的网络空间安全也有一定现实意义。

1.2 国内外研究现状

1980 年，Anderson[6]在《计算机安全威胁监控与监视》报告中首次系统阐述入侵检测概念，提出通过审计日志分析评估主机安全状态的方法，开创了基于主机的入侵检测（Host-based Intrusion Detection System，HIDS）研究范式。1987 年，Denning[7]突破性地构建了通用入侵检测模型，该模型通过事件规则库与异常统计模块的协同，实现了跨平台攻击行为检测，为后续 IDS 架构设计奠定理论基础。1990 年，加州大学戴维斯分校团队开发的网络安全监测系统（Network Security Monitor，NSM）首次直接解析原始网络流量，无需格式转换即可监控异构设备，标志着基于网络的入侵检测（Network Intrusion Detection System，NIDS）技术正式登上历史舞台[8]。值得注意的是，早期系统多依赖专家规则库与静态特征匹配，其面对加密流量、零日攻击等新型威胁时检测效能显著下降，这一局限性促使研究者转向数据驱动方法。

21 世纪初，机器学习技术为入侵检测注入新动能。2004 年，基于支持向量机（Support Vector Machine，SVM）的流量分类模型在 KDD Cup 竞赛中展现高精度，验证了统计学习方法在特征非线性可分场景下的优势[9]。然而，真实网络环境中攻击样本的稀疏性与分布偏移问题逐渐凸显，例如在 CIC-IDS2017 数据集中，DDoS 攻击样本占比不足 0.3%，导致传统机器学习模型出现严重分类偏差。此类数据不平衡现象的本质在于攻击行为的突发性与隐蔽性，使得少数类样本的语义特征难以被充分学习[10]。这一挑战驱动研究人员从数据增强、代价敏感学习等维度寻求突破，推动入侵检测技术向自适应、强泛化的方向演进[11,12]。

1.2.1 基于机器学习的入侵检测方法研究现状

在入侵检测领域，机器学习方法的研究始终围绕特征优化、数据不平衡和模型泛化能力等核心挑战展开迭代演进[13]。早期研究中，传统机器学习模型因依赖人工特征工程而面临高维网络流量特征提取困难的问题[14]。Alsajri 等人[15]提出的基于遗传算法（Genetic Algorithm, GA）与 SVM 的混合模型，在 UNR-IDD 二分类数据集中，通过 GA 从 42 维原始特征中动态筛选出 29 个关键特征子集，实现了 96%的检测精度。需特别指出的是，该数据集将 TCP-SYN 泛洪攻击、端口扫描（PortScan）等异构攻击类型统一归为“攻击”类别，虽验证了模型在二分类场景下的有效性，但其特征选择策略未考虑多分类任务中不同攻击模式间的特征分布差异，导致模型在后续跨数据集测试时面临分类边界模糊问题。这一边界模糊问题与特征冗余带来的计算复杂度挑战形成叠加效应。当模型试图通过增加特征维度以细化分类边界时，计算资源消耗呈指数级增长。例如在 UNSW-NB15 数据集上，原始特征维度从 42 扩展至 196 时，SVM 训练时间从 3.2 秒激增至 218 秒[15]。反之，若采用激进的特征选择策略压缩维度，虽可缓解计算压力，却可能割裂攻击行为的关联性特征，进一步加剧分类边界的模糊性。这种精度与效率的权衡矛盾，在资源受限的物联网场景中尤为突出[16]。

为了提升模型的鲁棒性，Al 等人[17]在 CIC-IDS2017 数据集中引入 SMOTE 过采样技术[18]，结合随机森林（Random Forest，RF）模型将现代攻击检测率提升至 97%。但该方法在少数类极端稀缺场景，例如 Heartbleed 攻击仅 11 个样本的场景下仍存在过拟合风险，且集成模型的计算开销难以满足无线传感器网络等资源受限环境的实时检测需求。

针对资源约束与计算效率矛盾的难题，Talukder 等人[19]提出轻量级集成框架 MLSTL-WSN，采用 SMOTE-Tomek 联合采样技术平衡 WSN-DS 数据集，并对比 XGBoost、LightGBM 等梯度提升算法，在保证 96.78%检测精度的同时将模型推理时间降低 40%。然而，该框架对具有时空关联性的复杂攻击，例如 APT 多阶段攻击的特征提取能力不足，反映出传统机器学习模型在多层次特征融合上的局限性。

现有研究多聚焦单一数据集验证，缺乏跨数据集泛化能力。Hossain 等人[20]通过集成 10 个公共数据集测试 RF、XGBoost 等模型的跨域适应性，发现 RF 在 WSN-DS 数据集上 F1-score 达 99%，但在 SIMARGL 数据集下降至 92%，表明特征空间分布差异会显著削弱模型泛化性能。这一发现揭示了基于机器学习的入侵检测系统在动态网络环境中面临的本质挑战，即静态特征表达与动态攻击模式间的语义鸿沟[21]。

1.2.2 基于深度学习的入侵检测方法研究现状

传统机器学习方法虽在入侵检测领域取得显著进展，但其局限性在复杂网络环境中日益凸显。例如，SVM 与 RF 等模型依赖人工特征工程，难以自适应提取高维流量中的非线性时空关联[15]。同时，数据类别不平衡易导致模型偏向多数类，而集成学习方法虽缓解了部分问题，却面临计算开销大与特征表达单一的限制。深度学习（Deep Learning，DL）通过多层非线性变换自动学习数据内在表征，为解决上述问题提供了新范式。深度学习与入侵检测的深度契合源于其核心能力与网络安全威胁检测需求的天然适配，入侵检测系统需处理高维、非线性且动态演变的网络流量数据，而深度学习的多层非线性架构能够有效捕获流量特征中的复杂模式[22,23]。

针对复杂攻击的时空建模需求，Hnamte 等人[24]设计了 DCNNBiLSTM 混合模型，通过 CNN 提取数据包载荷的局部异常模式，Bi-LSTM 建模会话流量的双向时序依赖，在 CIC-IDS2018 数据集上对 DDoS 攻击实现 96%检测率。但该模型因双重网络结构导致计算复杂度激增，单次推理时间较纯 CNN 模型增加 2.3 倍，难以在边缘设备部署。Yin 等人[25]提出了一种基于循环神经网络的入侵检测模型 RNN-IDS，利用 RNN 的长短期记忆能力建模网络流量的时序特征。模型通过多层 RNN 结构提取流量中的上下文依赖关系，并优化神经元数量与学习率参数以提升性能。在 NSL-KDD 数据集上，RNN-IDS 的准确率达到 97.5%，较传统方法平均提升 7%-12%。

此外，模型通过动态调整学习率进一步缩短训练时间，验证了其在实时检测场景的适用性，但 RNN-IDS 对高维稀疏特征的敏感性较高，且模型参数量较大，在资源受限环境中部署时面临计算效率问题。Qazi 等人[26]进一步开发了 HDLNIDS 框架，结合 CNN 与 RNN，在 CIC-IDS2018 数据集上以 97.9%准确率实现高效检测，但其对数据分布偏移的适应性不足，在跨时间段测试中误报率上升至 4.1%。因此，动态环境下的持续学习能力成为另一关键挑战[27]。Hnamte 等人[28]提出一种两阶段混合模型 LSTM-AE，第一阶段通过自编码器对原始流量数据进行降维，提取关键特征并去除冗余信息。第二阶段利用长短期记忆网络对降维后的特征进行时序建模，捕捉攻击行为的动态模式，支持静态与动态流量分析，并通过参数优化提升泛化能力。在 CIC-IDS2017 数据集的多分类任务中，LSTM-AE 的准确率达到 98.2%，对 Botnet 和 Web 攻击的检测率分别提升至 98.7%和 97.5%。与单一模型相比，两阶段设计显著降低误报率。此外，模型在边缘计算场景下的推理时间缩短 30%，验证了其资源效率优势。Kasongo 等人[29]提出基于 XGBoost-LSTM 的增量框架，通过 XGBoost 动态筛选关键特征，LSTM 增量更新时序模式，在持续学习测试中将误报率降低 12%。然而，特征选择过程可能丢失微观数据包异常信号，例如端口扫描的离散事件，会导致新型攻击漏检率上升。此外，Wang 等人[30]评估多种深度学习模型在 CSE-CIC-IDS2018 数据集上的表现，发现 DNN 更适合实时部

署，但其依赖静态训练数据，无法应对网络流量分布漂移。动态更新延迟在实时检测场景尤为突出，Qazi 等人[26]的 HDLNIDS 框架受限于固定参数结构，无法快速响应流量分布漂移，持续学习实验中模型迭代滞后时间窗口达 8-12 分钟，新型加密攻击漏检率随之上升至 15%。

这些挑战暴露出当前模型在跨层次特征割裂、在线增量学习效率等维度的理论局限，需融合多模态表征学习、对抗鲁棒性优化及边缘智能计算等技术路径实现突破。

1.2.3 入侵检测中数据不平衡问题研究现状

在入侵检测领域，数据类别不平衡是制约模型性能的核心挑战之一。传统机器学习方法依赖人工特征工程与经典重采样技术，虽能缓解中小规模数据的类别偏斜，但在高维加密流量场景中易受噪声干扰，且对少数类攻击的深层特征提取能力不足[31]。相比之下，深度学习方法通过生成对抗网络等自动生成合成样本，结合多尺度特征建模显著提升了数据适应性，但其生成样本的边界模糊性与模式崩溃风险仍限制实际应用效果[32]。

生成对抗网络（Generative Adversarial Network，GAN）是一种基于对抗训练的深度生成模型，由生成器和判别器构成。二者通过动态博弈持续优化，最终提升数据的生成质量[33]。Yang 等人[34]提出了一种结合自步集成与辅助分类器生成对抗网络的重采样方法 SPE-ACGAN，通过 ACGAN 对少数类样本进行过采样，并通过 SPE 对多数类样本进行欠采样，从而实现数据分布的平衡。其在 CIC-IDS-2017 与 CIC-IDS-2018 数据集合并为更不平衡的 CIC-IDS-17-18 数据集，并在此数据集上测试了 RF、CNN、GoogLeNet 及 CNN+WDLSTM 模型。实验结果表明，SPE-ACGAN 显著提升了分类性能，其中 RF 模型的 F1-score 提升 5.59%，CNN 提升 3.75%。该方法在复杂不平衡场景下展现出更强的鲁棒性。Abedzadeh 等人[35]提出强化学习框架（Reinforcement Learning Framework with Oversampling and Undersampling Algorithm，RLFOUA），该框架动态优化重采样过程，并整合新型过采样算法与成本敏感分类策略。在 CIC-IDS-2018 数据集上达到了 98.4% 的准确率。Chui 等人[36]提出三阶段数据生成框架 SMOTE-GAN-VAE，通过混合过采样、GAN 生成与变分自编码器重构，在 NSL-KDD 数据集上实现 91.9%的检测精度。然而，该方法生成的样本与正常流量特征重叠率高达 27%，导致分类边界模糊。针对此问题，Cui 等人[37]设计了 GMM-WGAN 模型，结合高斯混合聚类与 Wasserstein GAN 生成边界清晰的样本，通过 CNN-LSTM 分类器在 UNSW-NB15 数据集上将 F1-score 提升至 96.2%。但该模型未考虑跨层次特征关联，对 APT 多阶段攻击的检测仍存在漏判。

在进一步研究中，Abdelkhalek 等人[38]引入 ADASYN-Tomek 联合采样技术，结合深度卷积网络（Deep Convolutional Neural Networks，DCNN）在 NSL-KDD 数据集上实现 99.8%的多分类准确率。然而，其静态模型难以适应动态网络环境中的概念漂移，且重