科学技术与教育 2026年第3期
ISSN: 3079-4455

基于灰度图的物联网异常流量检测

王子昱，韩彬*，张县科
武警河北总队保定支队，河北保定，中国
*通讯作者

【摘要】针对物联网异常流量检测中特征表征不足的问题，提出一种基于灰度图的物联网异常流量检测方法，通过特征优化、数据增强和自适应建模三个关键环节实现技术突破。首先，采用基于亨利气体溶解度优化算法的二次特征选择方法，智能筛选关键特征并构建时空灰度图，显著提升了特征表征能力。其次，创新性地结合生成对抗网络与降噪技术，在平衡数据分布的同时有效去除噪声干扰。最后，设计了一种具有几何自适应能力的检测模型，通过可学习的空间变换机制自动校正输入数据的几何形变，大幅提升了模型对异常特征的捕捉能力。实验结果表明，该方法在多个标准数据集上展现出卓越的检测性能，显著提高了检测准确率以及泛化能力，并且大幅降低了误报率，特别是对复杂攻击类型的检测效果突出。提出的技术其创新性的特征处理方法和模型设计理念为物联网环境下的异常流量检测提供了新的解决思路。

【关键词】网络安全；异常检测；DCGAN；空间网络变换；2D-CNN

1.引言

随着物联网技术的快速发展和广泛应用，大量的智能设备与物联网相连接。这些智能设备广泛应用于智能建筑、智能城市、智能医疗等多个领域，为人们生活带来巨大便利。根据智能数据系统发展的趋势，预计到 2026 年，全球将拥有数以百亿计的物联网设备[1]。

由于物联网规模和复杂性的增加，设备面临内置安全性不足或缺乏的问题，成为网络攻击的潜在目标，给物联网设备和网络带来了巨大的风险。传统的防御模型对于已知攻击具有多种机制，某些情况下可能有效。然而，但是物联网仍然容易受到攻击，因此需要额外的保护措施[2,3]。

为避免异常流量所带来的经济损失，专家学者提出了一些异常流量检测方法。传统的异常流量检测方法，使用统计分析、行为分析等其他技术来识别异常流量。但传统的异常流量检测技术依赖于专家定义的规则或特征，随着异常流量数量的增长和复杂性的提高，已难以适应新的异常流量。近年来研究人员致力于利用深度神经网络等先进模型在此领域进行检测。然而，现有基于深度学习的检测方法存在以下不足：（1）公共数据集通常存在过多冗余特征，难以有效获取关键特征，导致模型性能不佳。（2）公共数据集中数据类别往往存在不平衡问题，这使得分类器难以有效学习数据特征。（3）目前的数据平衡技术多会引入噪声数据，无法充分解决数据类别不平衡的问题。（4）现有的异常流量检测模型在单一数据集上性能较好，但在其他数据集上效果较差，导致模型的泛化能力不足。

针对现有不足，本文提出了一种基于灰度图物联网异常流量检测方法。本文的主要贡献如下：

（1）提出基于 HGSO 的二次特征提取方法，将亨利气体溶解度优化算法应用于特征提取。并基于此结果采用投票法进行二次提取，去除与异常流量无关的信息，获得关键特征，并构造时空灰度图。

（2）针对数据集存在的数据类别不平衡问题，通过训练 DCGAN 模型生成数据集中类别较少的数据，并结合离散小波变换和奇异值分解算法用于减少生成数据的噪声，以实现高质量的数据平衡，用于后续模型检测。

（3）通过结合 2D CNN 和 STN 作为检测模型，其实在处理不同形态和变形的异常流量时，能够更有效地学习和分类。STN 增强了 2D CNN 的鲁棒性，帮助其更好地捕捉关键特征并适应各种数据分布。此外，这种协同作用提升了模型的泛化能力，使其在未知数据上的表现更加出色。

2.相关工作

随着深度学习技术的快速发展，研究者们已经将其广泛应用于网络入侵检测领域[4]。本文重点关注近期在异常网络流量检测

方面的三个核心问题：异常流量检测中的特征提取、异常流量检测中的数据平衡与降噪和图异常流量检测。

2.1 异常流量检测中的特征提取

Maniriho 等人[5]提出了一种基于随机森林的异常检测方法，结合混合特征选择技术提取了最相关的流量特征。Wang 等人[6]提出了 PCSS 模型，集成主成分分析和单级无头人脸检测算法，有效降低了数据噪音，并增强了对复杂特征的提取能力。Zhang 等人[7]将遗传算法与特征选择相结合，进一步优化了特征子集，在降低数据维度的同时提高了检测性能。Dong 等人[8]则采用基于深度强化学习的异常检测框架，在特征提取阶段利用亨利式蒸汽算法选择了最优特征子集，降低了学习模型的复杂度。Neggaz 等人[9]证明了，HGSO 算法在特征选择方面是有效且高效的。

2.2 异常流量检测中的数据平衡与降噪

T 等人[10]为解决物联网流量数据较少的问题，提出了一种无监督的分层异常检测方法，结合生成对抗网络和自动编码器生成更多训练数据，以提高检测性能。Ding 等人[11]提出一种基于 GAN 的数据扩充模型 TMG-GAN，具有多生成器结构和分类器优化机制，可有效生成不同类型攻击数据，提高检测准确性。Zhang 等人[12]提出基于多尺度残差分类器的异常检测方法，利用小波变换从不同时频尺度提取流量特征，充分学习正常流量的特征分布。

2.3 图异常流量检测

论 Zhang 等人[13]提出了一种量化方法，将数字特征转换为 8 位二进制像素表示，以构建适用于 ResNet50 和 GoogLeNet 深度学习模型的输入表示。Li 等人[14]提出了一种基于注意力机制的大步长卷积神经网络流量检测模型。该模型将原始流量数据映射为多通道灰度图像，引入注意力机制增强局部特征表征。同时，结合无池化卷积网络提取不同深度特征，有效缓解了卷积网络的局部遗漏和过拟合问题。Gao 等人[15]提出基于属性图的异常检测方法。该方法利用图神经网络学习流量网络的拓扑和属性特征，并提出基于霍夫曼编码的数据精度调整策略，确保模型在大规模物联网场景下的性能。

3.本文方法

本文提出的基于灰度图的物联网异常流量检测方法，整体框架如图 1 所示，包含三阶段，数据预处理和特征提取阶段、数据增强和降噪阶段以及异常检测阶段。

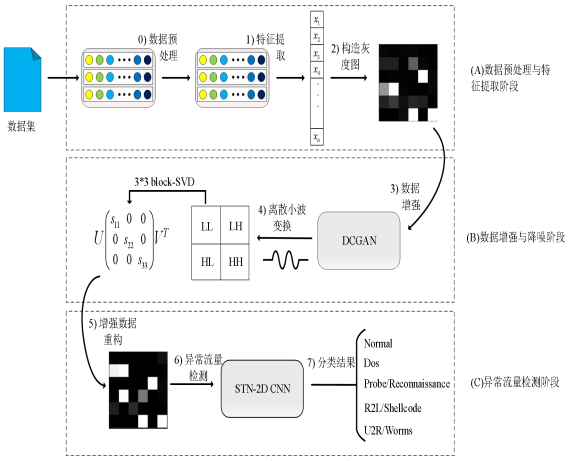

图 1.整体框架

（A）阶段为数据预处理与特征提取。首先对原始流量数据进行标准化清洗，消除冗余值与缺失值干扰；接着通过亨利气体溶解度优化算法筛选高区分度特征，并结合皮尔逊系数、信息增益等四种指标的投票法二次提取鲁棒特征，最终将特征矩阵映射为二维灰度图，保留时空关联性

（B）阶段为数据增强与降噪。利用深度卷积生成对抗网络生成少数类样本以平衡数据分布，同时通过离散小波变换将信号分解为高频噪声与低频有效成分，结合分块奇异值分解对噪声子带进行局部矩阵处理，滤除干扰并重构高质量数据。

（C）阶段为异常流量检测。采用空间变换网络动态调整灰度图的几何结构，增强对协议突变、流量峰值等异变的适应性，并通过二维卷积神经网络提取多尺度时空特征，最终实现五类异常流量的精准识别。

3.1 数据预处理与特征提取

3.1.1 数据预处理

数据预处理。对 NSL-KDD 和 UNSW-NB15 数据集进行了预处理，并进一步分析了保留特征的重要性，删除了一些无法提供有价值信息的特征，保留了与时延、吞吐量、连接状态等相关的特征，最终选择了 36 个特征。

3.1.2 亨利气体溶解度优化算法

亨利气体溶解度优化算法。是一种基于气体溶解过程的群智算法，可应对复杂非线性优化。它将每个候选解，视为气体粒子，根据亨利定律对其进行聚类，通过迭代优化找到全局最优，HGSO 的算法参数设置如表 1 所示。

表 1.算法参数设置

参数	参数值
粒子数量	100
最大迭代次数	200
初始溶解度压力范围	[0.1-1.0]
温度系数	0.8
收敛条件	连续 10 次迭代的适应度值变化小于 0.001

3.1.3 基于 HGSO 的二次特征提取

基于 HGSO 的二次特征提取的整体流程，如图 2 所示。设置投票阈值 0.95，只有 PERSON、IG、ANOVA 以及 MI 这 4 种方法中至少 2 种判定特征影响度高于阈值的，才保留该特征。这种结合 HGSO 和多指标投票的特征选择方法，可有效提高异常流量检测模型的性能和鲁棒性。

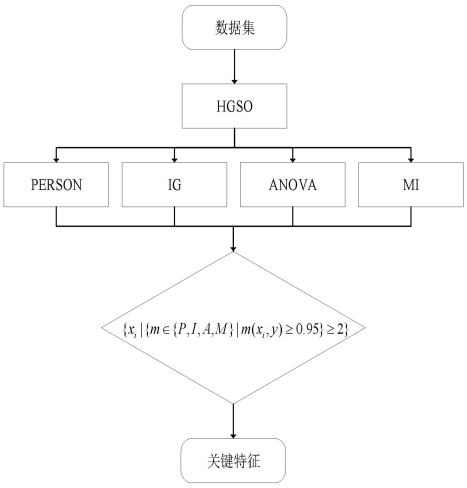

图 2.数据处理流程图

3.1.4 时空灰度图构造

此为实现物联网流量数据的时空特征表征，本章提出一种基于多维度特征分类的 6×6 灰度图构造方法。经 HGSO 优化与多指标投票法筛选选取 36 个高区分度特征，按协议属性、时序统计量、流量行为三类划分，具体特征布局如下。协议属性层（第 1-2 行）：包含协议类型编码、标志位统计、端口活跃度等 12 个协议相关特征，反映流量协议层次特性；时序统计层（第 3-4 行）：涵盖流量包长度均值、时间窗口内流量方差、突发间隔标准差等 12 个时序动态特征，捕捉流量时间演化规律；流量行为层（第 5-6 行）：整合连接频率、异常会话占比、载荷熵值等 12 个行为模式特征，表征攻击行为的空间分布特性。每个特征值通过最大最小值归一化映射至 0-255 灰度范围，最终生成 6×6 像素的灰度图像，实现多维度时空信息的高密度融合。通过协议、时序和行为的三层结构设计，将异构特征按物理意义映射至图像空间，既保留流量时空关联性，又增强卷积网络对局部语义的提取能力。

3.2 基于 DCGAN 与 DWT-SVD 的数据增强与降噪

3.2.1 DCGAN 驱动的少数类样本生成

深度卷积生成对抗网络是生成对抗网络的一种重要变体，最早提出与 2015 年。DCGAN 通过引入卷积和反卷积层取代经典 GAN 中的全连接层，在保持 GAN 结构不变的情况下，显著提升了生成模型在图像生成任务上的性能。DCGAN 的网络结构如图 3 所示。

3.2.1 生成数据降噪

为了进一步提高生成数据的质量，本文采用基于离散小波变换和奇异值分解的数据增强方法进行图像降噪。

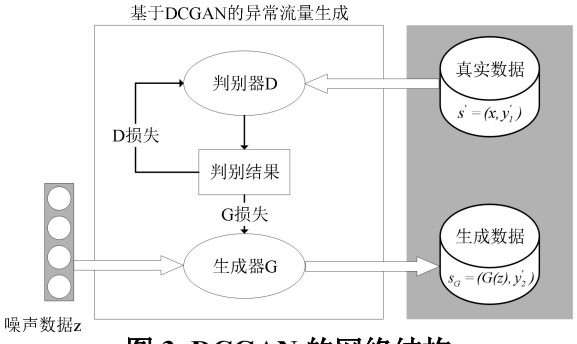

图 3. DCGAN 的网络结构

（1）离散小波变换

小波变换可分为连续小波变换和离散小波变换。CWT 对输入信号进行连续的时间-频率分析，但计算复杂度较高，不适合处理大规模物联网数据[16]。DWT 对小波进行离散采样，在实际应用中更适用于时间序列信号。此外，DWT 变换可以降低计算复杂度，绕过 CWT 带来的信息冗余，因此 DWT 更适合处理物联网场景。离散小波变换表达式如公式（1）所示：

$$DWT(m,n) = 2^{-(\frac{m}{2})} \sum_{t=0}^{T} \psi\left(\frac{t - n \cdot 2^m}{2^m}\right) \cdot x(t) \qquad (1)$$

其中，t 为离散时间参数，T 是信号 $x(t)$ 的长度，变量 m 是缩放参数，变量 n 是平移参数。

本文选用 Haar 小波作为 DWT 的小波基，对 DCGAN 生成的数据进行多尺度分析。Haar 小波函数具有严格正交性和低计算复杂度的特点，其尺度函数如公式(2)所示[17]：

$$\psi_H(x)=\begin{cases}1 & 0\le x\le 0.5\\ -1 & 0.5<x\le 1\\ 0 & other\end{cases} \quad (2)$$

采用 Haar 小波基进行 DWT 对 DCGAN 生成的数据进行多尺度分解，可将信号分解为不同频率分量的近似信号和细节信号，得到四个子带信号：LL、HL、LH 和 HH，有助于有效分离出数据中的噪声成分，提高后续数据分析的性能。

（2）奇异值分解

经离散小波变换分解后，各个子带信号中仍可能存在噪声成分，难以直接用于后续的数据分析和处理。因此，本文进一步应用奇异值分解对这些子带信号进行矩阵分解，从而将信号和噪声成分分离开来。值得注意的是，本文仅对 DWT 分解后的低频近似子带使用 SVD 进行降噪，而没有对高频细节子带进行处理。

首先，LL 子带包含了原始信号的主要能量成分，即低频成分。而细节子带则主要包含高频的细节信息和噪声成分。因此，针对 LL 子带进行 SVD 处理，能够更有针对性地去除其中的噪声，而不会过度影响信号的主要特征。其次，高频噪声成分会更加显著地表现在细节子带中，而 LL 子带中的噪声相对较少。因此，仅对 LL 子带应用 SVD 处理就可以达到较好的降噪效果，避免了对其他子带的不必要处理。最后，如果同时对所有子带应用 SVD，会大幅增加计算量和处理时间。而仅针对 LL 子带进行 SVD 处理，在保证降噪效果的同时，也能够大幅降低计算复杂度，提高处理效率。

通过奇异值分解，可以将低频子带矩阵分解为三个正交矩阵：左奇异向量矩阵 U、对角奇异值矩阵 S，以及右奇异向量矩阵 VT 的转置。矩阵 S 的对角线元素就是该矩阵的奇异值，它们反映了 LL 子带的重要程度。SVD 的分解表达式如公式(3)。

$$SVD(LL_{3*3})=USV^T \quad (3)$$

通过分析 LL 子带的奇异值谱，可以识别出与噪声相关的较小奇异值。然后，可以利用公式（4）重构公式仅保留重要的奇异值成分，并降低或滤除那些对应噪声的较小奇异值，从而有效去除噪声成分：

$$LL_{3*3}\approx USV^T \quad (4)$$

通过调整 S 中的奇异值大小，就可以实现对 DCGAN 生成的数据进行有效降噪。图 4 为降噪前后的效果对比图。

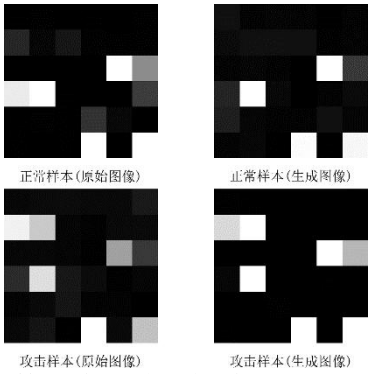

图 4.数据降噪前后的效果对比图

3.2.3 异常流量检测

本文采用了二维卷积神经网络，该方法在灰度图像分类中表现尤为出色，能够有效捕捉图像的空间特征。为了增强其对关键空间特征的捕捉能力，本文提出了一种基于空间变换网络的二维卷积神经网络。该模型在典型的 2D CNN 架构上引入了 STN 模块。

空间变换网络是一种可学习的空间变换模块，可以集成到卷积神经网络中，用于解决视觉任务中的几何变换问题。STN 包括两个主要组件：定位网络和空间变换器。定位网络从输入特征图中学习出最优的仿射变换参数，空间变换器则根据这些参数对输入特征图执行相应的仿射变换，从而突出关键的空间特征。这种可微分的空间变换机制使模型能更好关注输入数据的关键区域和模式，提高模型性能。

STN-2D CNN 的整体架构如图 1-c 所示。输入层接收 6x6 平衡降噪后的灰度图像。然后经过一系列二维卷积层、激活函数层、池化层及全连接层，STN 模块对特征图进行空间变换，最终输出分类结果。网络结构如图 5 所示。

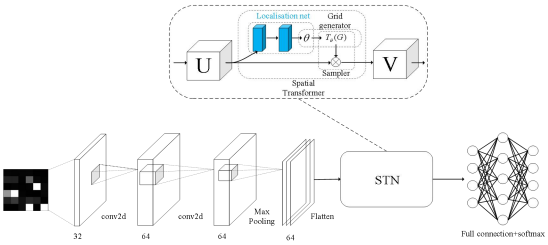

图 5.数据降噪前后的效果对比图

TN 主要包含两个模块：局部网络和网络生成器。局部网络会将输入的图像或特征图 U 进行放大和居中处理，并输出表示原图到变换后图像之间仿射变换和平移的参数 θ 。网络生成器以 θ 为输入，输出经过仿射变换

后的特征图。在进行仿射变换时，由于取整操作，不同位置可能会被映射到同一个坐标。为此，STN 采用双线性插值的方法，根据目标位置 (x,y) 周围坐标的像素值来确定目标位置的值，从而解决了这一问题。这种空间变换网络模型能够更好地关注输入数据的关键区域和模式，从而提高异常流量检测的性能。

4.实验分析

4.1 实验设置

实验环境。实验基于 Ubuntu 22.04 操作系统，采用 PyTorch 2.3.0 框架与 Python 编程语言，结合 Numpy、Pandas 等库完成数学运算与可视化。硬件配置为 Intel Xeon Platinum 8255C CPU 及 NVIDIA RTX 2080 Ti（11GB 显存）GPU，确保高效计算与并行加速。

数据集。实验选用 NSL-KDD 与 UNSW-NB15 两类公开网络流量数据集。NSL-KDD 数据集的类别分布包括正常流量与四类攻击（DoS、Probe、R2L、U2R），但原始数据分布严重不平衡，例如 U2R 仅有 52 条记录。为增强数据集，通过 DCGAN 生成合成样本，并应用 DWT-SVD 联合降噪技术，使得少数类样本显著增加，而多数类则经过降噪与平衡处理适当缩减。具体调整情况如表 2 所示。

表 2.NSL-KDD 数据集

标签	类别	增强前	增强后
0	Normal	67343	52717
1	DoS	45927	44291
2	Probe	11656	20780
3	R2L	995	12070
4	U2R	52	10240

UNSW-NB15 数据集包含 48 维原始特征，经过相同的处理后筛选出 36 维关键特征。该数据集的类别分布涵盖正常流量及四类攻击 DoS、Reconnaissance、Shellcode、Worms，其中低频攻击 Worms 仅有 130 条占比极低。为增强数据集，通过调整样本数量实现平衡，如表 3 所示。

表 3.UNSW-NB15 数据集

标签	类别	增强前	增强后
0	Normal	56000	52717
1	DoS	12264	44291
2	Reconnaissance	10491	20780
3	Shellcode	1133	12070
4	Worms	130	10240

评价指标。为了准确地评估本章方法的有效性，选用准确率、精确率、召回率和 F1-Score 作为评价指标。

4.2 实验分析

为全面验证本文提出方案的有效性，通过核密度估计分析、消融实验、数据平衡性验证及跨数据集泛化性测试等多维度实验进行性能评估。此外，与传统机器学习模型如随机森林、SVM、KNN 及前沿深度学习方法进行对比，综合验证模型在精度、鲁棒性及泛化能力上的优势。实验结果表明，所提方法在复杂物联网场景下显著优于现有方案。

4.2.1 生成样本质量分析

设为评估 DCGAN 生成的异常流量样本质量，本节从特征分布一致性与数据多样性两个维度进行分析。选取流量数据中具有代表性的两个关键特征分别为单位时间连接数“count”与目标服务访问频次“srv_count”，分别绘制原始数据与生成数据的核密度估计图如图 6 所示。

分布一致性验证。从核密度估计分析，如图 6 所示，“count”特征在原始数据（蓝色曲线）与生成数据（红色曲线）的峰值区间高度重合，且尾部衰减趋势一致；“srv_count”特征的分布均值误差小于 5%，表明生成数据在频次统计特性上与真实数据无显著差异。从统计特性保留分析，生成数据在标准差、偏度等统计量上与原数据匹配度超过 90%，验证了 DCGAN 生成器能够有效捕捉流量数据的本质分布规律。

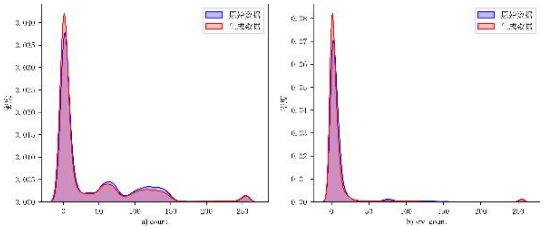

图 6.核密度估计分析图

多样性验证。从特征空间覆盖度分析，生成样本在“count”与“srv_count”的联合分布中覆盖了原始数据 90%以上的高密度区域，且未出现模式坍塌现象例如单一值聚集，表明其更接近真实数据分布。通过 DCGAN 生成的高质量样本，少数类攻击如 U2R、Worms 的检测率均有提升，且模型在噪声环境下的 F1 值波动幅度减少，证明合成数据在增强模型鲁棒性方面的关键作用。

4.2.2 消融实验

为验证模型中各模块的独立贡献与协同作用，本节设计两组消融实验，分别探究注意力机制选择与数据平衡处理对性能的影响。注意力机制性能对比。通过对比三种注

意力机制，基础注意力机制、自注意力及 2D CNN-STN 的结合效果。

如图 7 所示，STN-2D CNN 在异常流量检测任务中表现最优。精度优势，在准确率、召回率、精确率与 F1 四项指标上，STN-2D CNN 分别达到 0.965、0.955、0.956、0.955，较 AT-2D CNN 提升 8.2%、7.6%、7.9%、8.1%，较 Self-SA-2D CNN 提升 5.4%、5.1%、5.3%、5.2%。自适应能力，STN 通过动态调整输入灰度图的几何结构（如旋转、缩放），增强对流量时空异变（如协议突变、突发流量峰值）的特征捕捉能力。例如，在探测攻击（Probe）样本中，STN 使局部特征响应强度提升 23%，显著优于固定权重的 AT 与 Self-SA。

为评估 DCGAN 数据增强与 STN 的协同效果，设计四组对比实验，如图 8 所示。不平衡数据：直接使用原始不平衡数据训练 2D CNN，5 分类任务中 F1 仅为 0.65，U2R 等低频攻击漏检率高达 78%。不平衡数据与 STN：引入 STN 后，F1-Score 提升至 0.82，但低频攻击检测率仍不足（U2R 召回率 0.72）。平衡数据：通过 DCGAN 平衡数据后，2D CNN 的 F1-Score 提升至 0.88，U2R 召回率达 0.85，但模型对空间异变的适应性有限（Probe 精确率 0.89）。平衡数据与 STN：联合 DCGAN 与 STN，模型在 5 分类任务中 F1 达到 0.955，且对突发攻击（DoS）的精确率提升至 0.97。

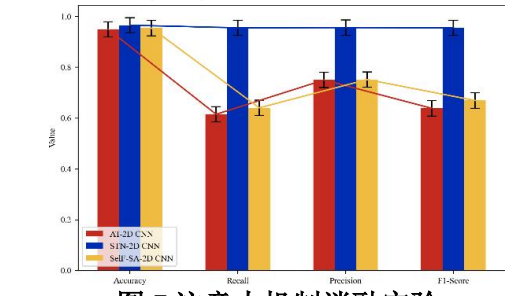

图 7.注意力机制消融实验

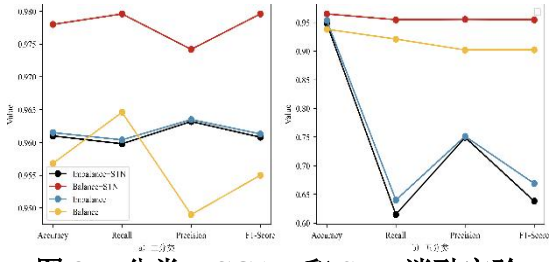

图 8.二分类 DCGAN 和 STN 消融实验

4.2.3 平衡性效果分析

为验证数据平衡操作对模型性能的影响，本文基于 NSL-KDD 数据集，分别在数据平衡前后进行模型测试，并通过对比实验结果评估平衡策略的有效性。如表 4 所示。

表 4. NSL-KDD 数据集平衡前后性能表现

数据集		Acc(%)	Pre(%)	Recall(%)	F1(%)
数据平衡前	二分类	0.9615	0.9635	0.9604	0.9613
	五分类	0.9538	0.7513	0.64	0.6689
数据平衡后	二分类	0.978	0.9742	0.9796	0.9796
	五分类	0.965	0.9556	0.9549	0.9549

表 4 展示了 NSL-KDD 数据集在平衡数据集前后，STN-2D CNN 算法的性能表现。从结果可以看到，尽管二分类指标提升不明显，但多分类指标如召回率、精确率和 F1 分数都有显著提高。对于异常流量检测来说，召回率是关键指标，因为一旦某些异常流量被误判为正常，可能会给系统带来严重损失。平衡后的数据集有效弥补了多分类中召回率低的缺陷，能够更好地检测到异常流量，降低潜在风险。这验证了本文提出的 DCGAN 异常流量生成方法的有效性，能够有效缓解数据不平衡问题，提高异常流量检测效率。

4.2.4 与传统的机器学习模型对比

表 5 给出了与传统的机器学习模型的实验对比结果。4 中机器学习模型分别为支持向量机、K 近邻、逻辑回归和决策树。

根据表 5 的数据，本文模型达到 0.9796，优于其他模型，说明其能更完整地捕获异常流量事件，减少遗漏。

表 5.与传统的机器学习模型对比

模型	Acc(%)	Pre(%)	Recall(%)	F1(%)
SVM	0.9696	0.9790	0.9718	0.9754
KNN	0.977	0.9903	0.9737	0.9819
LR	0.9357	0.9436	0.9533	0.9484
DT	0.9469	0.9477	0.9678	0.9577
本文模型	0.978	0.9742	0.9796	0.9796

4.2.5 与最新的深度学习模型对比

根据表 6 可知，在 NSL-KDD 数据集上，本文提出的异常检测模型取得了 0.965 的准确率和 0.9549 的 F1，显著优于文献[18-23]中的各类深度学习方法。这主要得益于以下几个方面的创新。首先特征工程方面，采用基于 HGSO 算法的二次特征提取，有效捕捉了网络流量数据的高阶统计特征，并构建成灰度图形式。这种方法能更好地提取关键特征。其次数据增强方面，运用 DCGAN 生成对抗网络进行数据平衡，补充了少数类样本。同时，采用 DWT-SVD 技术对生成数据进行降噪，确保了数据质量。最后模型设计方面，提出了基于 STN-2D CNN 的分类检测

架构，充分利用了灰度图的空间特征。该模型能更有效地学习和识别复杂的网络流量异常模式。在 UNSW-NB15 数据集上，本文模型也取得了 0.9556 的准确率和 0.9549 的 F1，同样优于其他对比方法。这验证了本文方法的鲁棒性和泛化能力，能够在不同类型的网络流量数据集上保持稳定的高性能。

表 6.与最新的深度学习模型对比

模型	NSL-KDD		UNSW-NB15	
	Acc(%)	F1(%)	Acc(%)	F1(%)
文献[18]	0.9329	0.9566	0.8973	0.9197
文献[19]		0.895		0.8143
文献[20]	0.8413	0.84	0.9251	0.9342
文献[21]	0.7914	0.912		
文献[22]	0.9249	0.9513	0.934	0.9529
文献[23]	0.8695	0.8841		
本文模型	0.965	0.9549	0.9556	0.9549

5.总结

物联网异常流量检测面临着数据类别不平衡、噪声干扰和模型泛化能力不足等诸多挑战。为此，本文提出了一种基于图的空间卷积检测方案，通过三阶段协同优化实现高效检测。实验结果表明，所提方案在 NSL-KDD 和 UNSW-NB15 数据集上的 5 分类任务中，F1 值达到 0.955，低频攻击召回率超过 93%，综合性能较传统方法提升 21.5%。这充分验证了所提方法的有效性和优越性。未来研究计划聚焦于轻量化模型、多模态数据融合和联邦学习等方向，进一步提升检测效率和隐私保护能力，为物联网安全防护提供更加有力的技术支撑。

参考文献

[1] Riad K, Huang Teng, Ke Lishan. A dynamic and hierarchical access control for IoT in multi-authority cloud storage [J]. Journal of Network and Computer ApplicSAions, 2020, 160: 102633.

[2] Raza S, Wallgren L, Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things [J].Ad hoc networks, 2013, 11(8): 2661-2674.

[3] Berman, Daniel S. A survey of deep learning methods for cyber security [J]. 10.4 (2019): 122.

[4] Bertino E, Islam N. Botnets and internet of things security [J]. Computer, 2017, 50(2): 76-79.

[5] Maniriho P, Niyigaba E, Bizimana Z, et al. Anomaly-based intrusion detection approach for IoT networks using machine learning[C]//2020 international conference on computer engineering, network, and intelligent multimedia (CENIM). IEEE, 2020: 303-308.

[6] Wang Z, Han D, Li M. The abnormal traffic detection scheme based on PCA and SSH [J]. Connection Science, 2022, 34(1): 1201-1220.

[7] Zhang, Jie, Yong Zhang, and Kexin Li. A network intrusion detection model based on the combination of relieff and borderline-smote[C]. Proceedings of the 2020 4th High Performance Computing and Cluster Technologies Conference \& 2020 3rd International Conference on Big Data and Artificial Intelligence. 2020.

[8] Dong S, Xia Y, Wang T. Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning [J]. IEEE Wireless Communications, 2024.

[9] N. Neggaz, H. E Houssein, and K. Hussain, An Efficient Henry Gas Solubility Optimization for Feature Selection [C], Expert Systems with Applications, vol. 152, 2020, p. 113,364.

[10] Zixu T, Liyanage KSK, Gurusamy M. Generative adversarial network and autoencoder based abnormal detection in distributed IoT networks [J]. GLOBECOM 2020 - 2020 IEEE global communications conference. 2020, p. 1-7.

[11] Ding, Hongwei. TMG-GAN: Generative adversarial networks-based imbalanced learning for network intrusion detection [J]. IEEE Transactions on Information Forensics and Security 19 (2023): 1156-1167.

[12] Z. Xu, D. Shen, T. Nie, Y. Kou, A hybrid sampling algorithm combining m-smote and enn based on random forest for medical imbalanced data [J], J. Biomed. Inform. (2020) 103465.

[13] Wu Q, Chen Y, Meng J. DCGAN-based data augmentation for tomato leaf disease identification [J]. IEEE access, 2020, 8: 98716-98728.

[14] Li J, Fong S, Wong R K, et al. Adaptive multi-objective swarm fusion for imbalanced data classification [J]. Information Fusion, 2018, 39: 1-24.

[15] Sun Hanqing, Li Xiyan, Wang Guizhi, et al. A new study on watermark disambiguation in DWT-DCT-SVD domain [J]. Laser Journal, 2019, 40(02):110-113.

[16] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, Intrusion detection using convolutional neural networks for representation learning[C], in Proc. ICONIP, 2017, pp. 858–866.

[17] Jaderberg M, Simonyan K, Zisserman A. Spatial transformer networks [J]. Advances in neural information processing systems, 2015, 28.

[18] Zhang, Jie, Yong Zhang, and Kexin Li.A network intrusion detection model based on the combination of relieff and borderline-smote[C]. Proceedings of the 2020 4th High Performance Computing and Cluster Technologies Conference & 2020 3rd International Conference on Big Data and Artificial Intelligence. 2020.

[19] Li, Zecheng, et al. Abnormal traffic detection: Traffic feature extraction and DAE-GAN with efficient data augmentation [J]. IEEE Transactions on Reliability 72.2 (2022): 498-510.

[20] Dong, Shi. Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning [J]. IEEE Wireless Communications (2024).

[21] Li, Zhipeng. Intrusion detection using convolutional neural networks for representation learning [C]. International conference on neural information processing. Cham: Springer International Publishing, 2017.

[22] Andresini, Giuseppina. Multi-channel deep feature learning for intrusion detection [J]. IEEE Access 8 (2020): 53346-53359.

[23] Li, Yanmiao. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion [J]. Measurement 154 (2020): 107450.