基于平衡生成对抗网络的海洋气象传感网入侵检测研究

苏新[1]，张桂福[1]，行鸿彦[2]，Zenghui Wang[3]

（1. 河海大学物联网工程学院，江苏 常州 231022；
2. 南京信息工程大学电子与信息工程学院，江苏 南京 210044； 3. 南非大学电气工程系，约翰内斯堡 1710）

摘 要：针对海洋气象传感网（MMSN）环境下海洋移动终端资源受限和网络流量不平衡导致网络入侵难以被准确检测的问题，提出了一种基于移动边缘计算的 MMSN 物理架构和一种基于平衡生成对抗网络的入侵检测模型。首先，利用改进的平衡生成对抗网络对不平衡数据进行数据增强。其次，利用基于分组卷积的轻量级网络对入侵数据进行分类。最后，通过计算机仿真证明了所提模型较传统数据增强模型具有更高识别各类攻击的能力，尤其是针对 MMSN 的少数类样本攻击。

关键词：海洋气象传感网；入侵检测；移动边缘计算；平衡生成对抗网络；分组卷积

中图分类号：TN929.52

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023078

Research on intrusion detection for maritime meteorological sensor network based on balancing generative adversarial network

SUN Xin[1], ZHANG Guifu[1], XING Hongyan[2], Zenghui Wang[3]

1. The College of IoT Engineering, Hohai University, Changzhou 213022, China
2. School of Electronics & Information Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China
3. Department of Electrical Engineering, University of South Africa, Johannesburg 1710, South Africa

Abstract: Aiming at the problem that the resources of maritime mobile terminals were limited and the network traffic was imbalanced in the MMSN (maritime meteorological sensor network) environment, which made it difficult to detect network intrusion accurately, a mobile edge computing based physical architecture of MMSN was proposed, and an intrusion detection model based on balancing generative adversarial network was proposed. First, an advanced balancing generative adversarial network was adopted to augment the imbalanced data. Then, a lightweight network based on group convolution was applied to intrusion data classification. Finally, compared with conventional data augmentation models, the computer simulation proves that the proposed model has a higher ability to recognize various attacks, especially minority class attacks on MMSN.

Keywords: maritime meteorological sensor network, intrusion detection, mobile edge computing, balancing generative adversarial network, group convolution

0 引言

伴随 5G 新基建系统的完善与 6G 标准的制定，海洋物联网（MIoT, maritime Internet of things）迎来了新的快速发展契机，并加快了我国海事信息系统和通信基础设施现代化[1]。海洋气象传感网（MMSN, maritime meteorological sensor network）作为 MIoT 不可或缺的组成部分，通过 IoT 设备与海上智能交通、海事智能感知和海洋气象灾害预警等系统共享关键的接口和信息[2-3]，并全方位地为 MIoT 服务提供精准的气象数据。

利用移动边缘计算（MEC, mobile edge com-

收稿日期：2022−11−30；**修回日期：**2023−02−20

基金项目：国家重点研发计划基金资助项目（No.2021YFE0105500）

Foundation Item: The National Key Research and Development Program of China (No.2021YFE0105500)

puting）将部分数据卸载到近端 MEC 服务器上处理，可以及时有效地处理各类海洋移动终端收集的海量数据[4]，满足低时延的海事应用服务需求。然而，IoT 和先进通信技术在带来便利的同时[5]，也使 MMSN 存在较大的攻击面。设备间的频繁信息交互易被入侵者侦测，进而增加了设备受到网络攻击的风险，甚至可能对整个 MMSN 造成严重的破坏。因此，为保障 MMSN 的完整性、可靠性以及可用性，亟须设计一个有效和可靠的安全机制。

防火墙、加密技术和入侵防御等传统的安全防御机制大多基于启发式和静态攻击签名[6]，难以识别网络中日益多样化的攻击。近年来，基于人工智能的网络入侵检测系统（NIDS, network intrusion detection system）已被广泛应用到智慧电网、工业 4.0 和车联网等领域，并可以提供更可靠的安全服务保障。然而，与传统陆地 IoT 入侵检测不同，设计面向 MMSN 的入侵检测面临如下挑战。

1) MMSN 中的海洋移动终端分布范围广泛且稀疏，缺乏中心基础设施，受到网络攻击的方式相对隐蔽，导致收集的网络流量数据呈现高度不平衡特性。这严重限制了现有入侵检测模型的性能。

2) 海洋无线通信环境复杂多变，各类海洋移动终端计算与存储资源差异大，能耗敏感度不一，移动终端的强异构性导致部分终端出现入侵检测任务处理超负荷情况，实现可持续的入侵检测是保障 MMSN 的关键。

通过参考 MEC 卸载技术在海洋观监测传感网的研究以及现有的入侵检测研究，结合 MMSN 中入侵检测存在的挑战，以提供高可靠、可持续的入侵检测能力为目标，本文研究了 MMSN 中的入侵检测技术，主要贡献如下。

1) 提出一种基于 MEC 的 MMSN 物理架构，海洋移动终端可将数据处理和入侵检测任务部分卸载至近端 MEC 服务器上处理，保障 MMSN 的低时延和安全服务需求。

2) 针对入侵检测数据不平衡问题，提出一种改进的平衡生成对抗网络（A-BAGAN, advanced balancing generative adversarial network）数据增强模型来生成少数类攻击样本，改善入侵检测分类器受训练数据集不平衡的影响。

3) 针对 MMSN 中海洋移动终端的强异构性，本文提出一种基于分组卷积神经网络的轻量级入侵检测分类器 LGCNN（lightweight group convolutional neural network），在准确识别各类攻击的同时，降低对终端计算与存储资源的消耗。

1　相关工作

1.1　智能型入侵检测系统

NIDS 用来实时监控网络数据传输的异常行为，同时对检测到的网络攻击采取可应对的安全响应措施[7]。NIDS 根据检测技术可以分为基于签名和异常数据[8]。前者通过已有攻击签名库对待检测数据特征进行匹配，该方法对已知攻击的识别效果较好，但是难以识别未知攻击。后者将正常数据与待检测数据之间的差异作为异常判断准则，其优点是可以检测出未知攻击，但常常伴随着较高的误报率。

近年来，基于机器学习（ML, machine learning）和深度学习（DL, deep learning）的智能型入侵检测方法已经得到深入的研究。文献[9]提出了一种基于互信息的最优特征选择算法，并利用最小二乘支持向量机（LSSVM, least squares support vector machine）进行入侵检测，提高了检测精度，但时间复杂度有所提高。文献[10]研究了特征选择对入侵检测分类器性能的影响，提出了一种基于余弦相似度的智能鸽群算法来选取最优特征子集，相较于传统算法具有更快的收敛速度。然而，该算法仍存在时间复杂度高的问题，且未对攻击分类。文献[11]实现了基于单类支持向量机的入侵检测模型，从直方图角度提取网络数据包的特征，提高了检测精度，但增加了训练复杂度和部署成本。上述基于传统 ML 的入侵检测方法在处理大量高维数据时出现能力不足的问题，并且不能很好地处理数据不平衡问题。

相较于 ML 的入侵检测，基于 DL 的方法因其具有强大的数据表达能力，通常可获得更好的检测性能。文献[12]在正常数据和异常数据的低维表示服从不同分布的假设下，提出了一种基于表示学习的异常检测方法，但该文献仅考虑了二分类情况。同时，为了降低模型的复杂度，文献[13]提出了一种轻量级的入侵检测模型，使用改进的自动编码器（AE, autoencoder）来提取数据的特征，获得了较高的检测率，但其未能对攻击进行有效分类。为了减少对经验性知识的依赖，文献[14]提出了一种基于卷积神经网络（CNN, convolutional neural network）的入侵检测模型，使用多目标优化算法搜索 CNN 结构，

可以在参数空间获得较优的解，但搜索需要的时间开销大，难以实时部署。文献[15]将 CNN 和长短期记忆（LSTM, long short-term memory）网络相结合，提出了一种分析时空特征的入侵检测模型，借助注意力机制充分融合时间和空间特征，提高了检测性能。然而，文献[15]提出的模型参数量庞大，无法应用于资源受限场景。文献[16]受群体分组决策启发，提出了一种新颖的 RANet 入侵检测模型，使用分组–门控卷积模块有效提取输入数据的特征，并减少了模型需要学习的参数量。为了进一步提高检测的准确率，文献[17]提出了一种多阶段入侵检测模型，使用人工蜂群算法选取特征，并使用黑寡妇算法来优化卷积 LSTM 结构的检测模型，在多个公共数据集上取得了较高的检测率。然而，文献[17]提出的模型复杂度高，占用资源大。文献[18]设计了一种可解释性多输出结构的神经网络入侵检测模型，利用二分类输出结果辅助多分类决策，并使用注意力机制来解释特征的重要性，但检测精度较低。上述 DL 的研究工作增强了对高维数据的表达能力，但是依然存在难以处理数据不平衡的问题。由此可见，这些模型并不能很好地识别出频率低的攻击。

入侵检测数据集是典型的不平衡数据集，而上述基于智能型 NIDS 的研究又极少关注少数类攻击样本的检测效果，致使入侵者可以有针对地发起少数类攻击，从而不可避免地存在数据泄露的风险。因此，亟须在入侵检测模型训练之前，对训练数据集进行平衡处理。

1.2 数据不平衡处理方法

数据不平衡指隶属某一类的样本数量远低于其他类别，该问题广泛存在于银行数据、医疗数据等领域。解决这一问题可以从算法和数据两方面入手进行研究。在算法方面，可以尝试去适应基于不平衡数据集的训练，进而提高少数类样本的识别精度，如代价敏感函数。然而，设计合适的代价系数矩阵需要专家知识，且相当复杂。在数据方面，可以通过增加少数类样本数量来处理不平衡问题，目前已经成为主流的研究方向。

在入侵检测领域，数据不平衡问题是制约检测性能的重要因素。这源于真实网络环境中收集到的原始流量大部分都是正常流量，某些低频率的攻击流量数量较少。因此，文献[19]构建了门控循环单元模型来检测网络中的分布式拒绝服务（DDoS, distributed denial of service）攻击，并使用合成少数过采样技术（SMOTE, synthetic minority oversampling technique）对训练集中少数类样本进行了扩充，取得了显著的性能优势。然而，该文献采用的数据集中正负样本分布与实际不符。此外，随机欠采样、自适应综合（ADASYN, adaptive synthetic）过采样和随机过采样（ROS, random over sample）技术也常用于入侵检测数据不平衡处理[20]。然而，传统的欠采样技术可能丢失多数类样本的有用信息，而过采样技术又无法很好地学习真实的数据分布且易受噪声点影响，导致生成的样本分布和真实数据分布差异很大。因此，上述传统数据增强方法不能充分地利用数据的深层次信息。这就表明不平衡数据的分布无法被准确地映射出来，同时可能对分类器的性能造成损害。

最近，生成对抗网络（GAN, generative adversarial network）在处理入侵检测数据不平衡问题上受到了极大的关注。文献[21]利用条件 GAN（CGAN, conditional GAN）来生成少数类攻击样本。使用前馈神经网络从网络流量中生成特征向量，再使用 CGAN 为少数类攻击生成新样本，提高了少数类攻击检测率。文献[22]受 SMOTE-SVM 数据合成思想启发，利用辅助分类器 GAN（ACGAN, auxiliary classifier GAN）来生成支持向量附近的困难样本。文献[23-24]与文献[22]相似，均采用 ACGAN 来生成少数类攻击样本，不同之处在于文献[23-24]将一维网络数据转化成二维图像数据。其中，文献[23]使用常规的顺序排列方式将一维网络数据转化为图像数据；而文献[24]则充分考虑图像中像素点与邻居点之间的相关性，运用 t-SNE（t-distributed stochastic neighbor embedding）技术将一维网络数据转化为二维图像数据。上述工作均未充分地考虑训练集中少数类样本的数量可能会导致 GAN 无法准确学习少数类样本分布的问题。例如，ACGAN 在不平衡数据集上训练时，判别器的 2 个输出是相互矛盾的，这可能使生成的样本无法兼顾真实性和类别属性[25]。此外，利用 GAN 作为数据增强的相关工作也并未使用度量性指标来衡量 GAN 生成的样本，缺乏对生成样本的有效性评估。值得说明的是，在计算机视觉领域可使用 IS（inception score）和 FID（Fréchet inception distance）来衡量 GAN 生成图像样本的质量，但上述指标在入侵检测领域并不适用[26-27]。

2　海洋气象传感网入侵检测系统

2.1　海洋气象传感网物理架构

图 1 展示了本文提出的基于 MEC 的 MMSN 物理架构，该架构主要由陆地云服务器、卫星、MEC 服务器和各类海洋移动终端组成。在 MMSN 中，MEC 服务器可以根据海域地理位置部署在不同基础设施上。对于近海区域和远海区域，MEC 服务器分别部署在海岛基站和远海基站上，该服务器集合可由 $S=\{s_1,s_2,\cdots,s_M\}$ 表示。对于每一个 MEC 服务器，均可通过卫星链路与陆地云服务器进行通信；船舶、海上浮标、无人机、探空气球和无人飞艇等移动终端在指定区域运行，这些移动终端集合表示为 $\mathrm{MT}=\{\mathrm{mt}_1,\mathrm{mt}_2,\cdots,\mathrm{mt}_L\}$；各移动终端上集成多个 IoT 设备用于收集温湿度、气压、风向、风速和能见度等气象数据，移动终端 mt_i 上的 IoT 设备集合表示为 $I_k=\{i_1,i_2,\cdots,i_N\}$，$1\leqslant k\leqslant L$。

为了缓解部分移动终端计算资源不足的问题，可以通过正交频分多址接入（OFDMA, orthogonal frequency division multiple access）通信方式向近端 MEC 服务器进行部分任务的卸载。此外，考虑到海洋区域辽阔而 MEC 服务器覆盖范围有限，对于未覆盖的移动终端可通过卫星通信与陆地云服务器通信。由于各类移动终端隶属不同的海事机构和企业，数据中存在敏感信息。因此，在本文构建的 MMSN 物理架构中，假设陆地云服务器和 MEC 服务器都是诚信可靠的，对移动终端的信息和数据内容不感兴趣，能够严格履行卸载任务处理与计算结果反馈职责，且各移动终端之间不进行任务卸载。与现有的集中式 MMSN 物理架构相比，本文通过引入 MEC 技术可显著降低各终端入侵检测的响应时间、能耗和丢包率，特别是存在网络流量负荷的情况下[28]。

2.2　面向海洋气象传感网的入侵检测

当各类海洋移动终端在指定区域工作时，IoT 设备每时每刻都在产生和收集数据，常见的 MMSN 访问会使这些设备容易受到网络攻击。在 MMSN 中，移动终端大至无人飞艇和货轮，小至无人水面艇、探空气球和海上浮标，根据移动终端的可用算力、存储资源、运行速率和安全程度等异构的特征属性[4]，入侵者能够有针对性地发起不同类型的攻击。

探测（Probe）攻击。无人飞艇、货轮等大型移动终端航速相对缓慢稳定，计算处理能力和存储能力强，能源充足，安全程度高。然而，大型移动终端部署的传统安全防御机制仍然存在一定的漏洞。入侵者可根据这些漏洞对大型移动终端发起探测攻击[29]，在不被发觉的情况下，收集有关 MMSN 的有价值信息、网络拓扑结构和设备特点（如设备的型号、功能和支持的网络协议等），为进一步攻击做准备。

DoS/DDoS 攻击。无人机、中型船舶等中型移动终端运行速率较快，计算处理能力和存储能力一

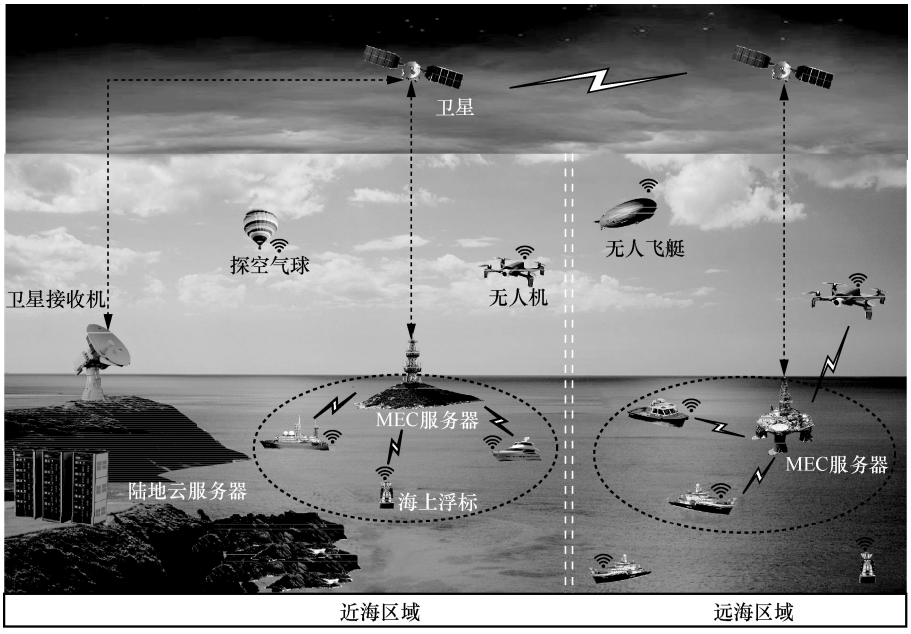


图 1　基于 MEC 的 MMSN 物理架构

般，能源较充足，安全程度一般。当中型移动终端频繁通过开放的无线信道与 MEC 服务器卸载通信时，容易被入侵者通过监听信道的方式发现[30]。这使入侵者可以在短时间内通过一对一或多对一的方式向这些目标发送大量的无效请求，导致设备不胜负荷，这可能会中断 MIoT 服务或者阻碍合法请求的实现，甚至可能导致上述移动终端偏离预定航线。

暴力破解攻击。海上浮标、无人水面艇和探空气球等小型移动终端计算处理能力和存储能力弱，能源受限，安全程度低。入侵者可通过枚举、字典等暴力破解方式对小型移动终端上的设备进行大量认证，从而获取设备信息和敏感数据。

因此，为避免海洋移动终端上的各类 IoT 设备在正常运行过程中受到网络攻击，在各移动终端和 MEC 服务器上部署 NIDS 来有效地检测网络攻击是至关重要的。NIDS 检测过程主要包括以下 4 个步骤：1) 各移动终端利用抓包工具对经过其 IoT 设备的网络流量进行捕获；2) 将捕获的原始数据包转化为观测值，每组观测值包含有关网络连接的统计信息和属性，这些观测值有助于识别网络攻击；3) 将上述观测值进行预处理后输入检测分类器中检测；4) 检测分类器根据输入数据进行判别，然后输出检测结果。

对于资源约束型移动终端，可将部分检测任务卸载到近端 MEC 服务器上处理，MEC 服务器可间歇性地访问陆地云服务器以提供足够的计算资源。本文假设从各移动终端捕获的网络数据具有相同的特征空间，且构建的 NIDS 拟在陆地云服务器上进行离线集中式训练，然后在线分布式部署到移动终端和 MEC 服务器上，因此检测模型的训练过程不会占用大量海洋移动终端的计算与存储资源。

3 基于平衡生成对抗网络的入侵检测模型

针对 MMSN 中存在的网络安全隐患，本文提出了一种基于平衡生成对抗网络（BAGAN, balancing generative adversarial network）的入侵检测模型，可以有效地降低 Probe、DoS/DDoS 和暴力破解等网络攻击的威胁。BAGAN 的入侵检测模型整体框架如图 2 所示，主要包括以下 3 个模块：1) 预处理模块将原始网络流量表征成向量，并划分训练集和测试集；2) 不平衡处理模块对训练数据进行增强；3) 检测模块利用增强后的混合数据集和测试集进行训练和测试。面向不平衡处理模块，本文提出了一种针对 MMSN 中缺乏少数类训练样本问题的平衡生成对抗网络数据增强算法，该算法可有效提高少数类攻击的识别精度；面向检测模块，本文构建了一种基于分组卷积的检测方案，用于解决 MMSN 中部分移动终端资源受限的问题。

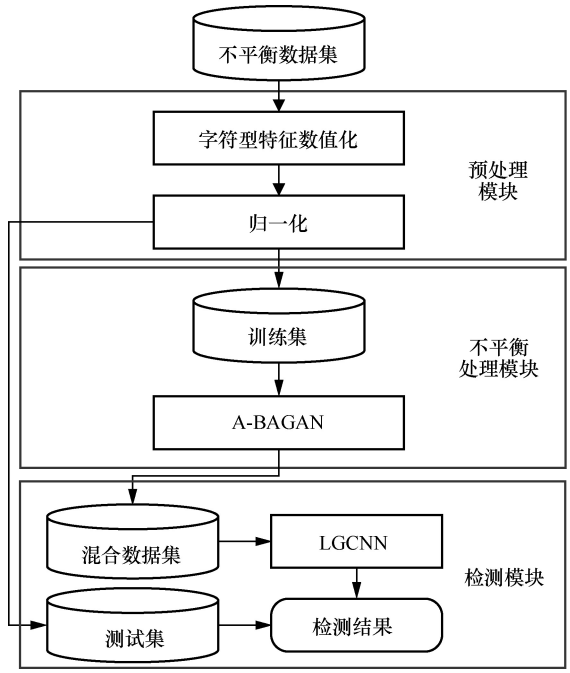


图 2 BAGAN 的入侵检测模型整体框架

3.1 不平衡处理模块

入侵检测数据不平衡容易提高少数类攻击漏检的概率，影响检测模型的分类性能。与传统的陆地 IoT 和车联网相比，MMSN 中的移动终端分布范围广泛且密度低，受到网络攻击的方式相对隐蔽，资源相对匮乏，部署环境复杂多变。这会导致在 MMSN 中收集到的网络数据不平衡的特性更加显著，严重制约现有检测模型的检测能力。为解决这一问题，可以利用 GAN 来生成少数类攻击样本。然而，传统 GAN 训练成功的概率依靠一定规模的样本数量[31]，直接使用传统 GAN 来处理不平衡的入侵检测数据，会严重抑制 GAN 对少数类攻击样本的建模能力。

BAGAN 主要用于解决 GAN 在不平衡图像数据集上生成少数类样本困难的问题[25]，其训练过程包括 3 个阶段，即 AE 训练阶段、GAN 初始化阶段和 GAN 训练阶段。AE 训练阶段不需要样本确切的类别信息，以无监督方式处理多数类和少数类样本，能够有效地学习所有类样本的公共特征。AE

训练完成后分别计算各类样本的潜在表示服从的高斯分布，并将其作为 GAN 训练阶段随机噪声的先验分布。然后，将 AE 的权重迁移到 GAN 中，作为 GAN 的初始状态，使 GAN 在训练前能够继承 AE 的先验知识，处于一个良好的初始状态。最后，对 GAN 进行对抗训练。其中，判别器为多节点输出结构，需要将样本与类别相匹配。

由于 MMSN 中入侵检测数据的高度不平衡特点，直接采用传统 BAGAN 来生成少数类攻击样本存在较大困难[32]。首先，在 AE 完成训练后，各类样本的潜在表示之间存在较大重叠区域，使生成的样本类别模糊，从而难以学习到良好的条件先验分布。其次，BAGAN 在对抗训练中进行优化所得到的交叉熵损失函数与 f 散度相关，增加了训练不稳定性；同时也未利用梯度惩罚来稳定 GAN 的训练过程[33-34]。针对上述 BAGAN 存在的问题，本文提出了一种改进的平衡生成对抗网络来生成少数类攻击样本。

具体地，针对样本类别模糊问题，通过改进条件变分自动编码器（ICVAE, improving conditional variational autoencoder）代替 BAGAN 中的 AE，其结构如图 3(a)所示，主要由编码器 En 和解码器 De 构成。其中，输入数据 $\boldsymbol{x}$ 传送至编码器中计算均值编码 $\boldsymbol{\mu}$ 和标准差编码 $\boldsymbol{\sigma}$；$\boldsymbol{\mu}$ 和 $\boldsymbol{\sigma}$ 再通过“重参数技巧”计算得到潜在表示向量 $\boldsymbol{z}$；最后，向量 $\boldsymbol{z}$ 联合类别信息 $\boldsymbol{y}$ 输入解码器中得到重构数据 $\hat{\boldsymbol{x}}$。当 $\forall \boldsymbol{x} \sim P_{\mathrm{r}}(\boldsymbol{x})$（$P_{\mathrm{r}}(\boldsymbol{x})$ 为真实数据分布）时，结合 ICVAE 的结构特点和最大似然准则可得不等式关系如下

$$\begin{aligned}&\log p_\theta(\boldsymbol{x}\mid\boldsymbol{y}) = D_{\mathrm{KL}}(q_\varphi(\boldsymbol{z}\mid\boldsymbol{x}) \| p_\theta(\boldsymbol{z}\mid\boldsymbol{x},\boldsymbol{y})) + \\ &\mathrm{ELBO} \geqslant \mathrm{ELBO} = \mathbb{E}_{q_\varphi(\boldsymbol{z}\mid\boldsymbol{x})}[\log p_\theta(\boldsymbol{x}\mid\boldsymbol{z},\boldsymbol{y})] - \\ &D_{\mathrm{KL}}(q_\varphi(\boldsymbol{z}\mid\boldsymbol{x}) \| p_\theta(\boldsymbol{z}\mid\boldsymbol{y}))\end{aligned} \tag{1}$$

其中，$D_{\mathrm{KL}}(\cdot\|\cdot)$ 表示 2 个分布之间的相对熵，$q_\varphi(\boldsymbol{z}\mid\boldsymbol{x})$ 表示通过编码器估计的后验分布，$p_\theta(\boldsymbol{x}\mid\boldsymbol{z},\boldsymbol{y})$ 表示重构结果，$p_\theta(\boldsymbol{z}\mid\boldsymbol{y})$ 表示先验分布。

本文设 $p_\theta(\boldsymbol{z}\mid\boldsymbol{y}) \equiv \mathcal{N}(\boldsymbol{0},\boldsymbol{I})$，满足 $\boldsymbol{z}$ 与 $\boldsymbol{y}$ 是解纠缠的条件，从而可以最大限度地促使编码器学习样本中的公共特征[35]。由式(1)知，ICVAE 在训练过程中需尽可能地提高证据下界（ELBO, evidence lower bound），即最小化样本重构误差和 $q_\varphi(\boldsymbol{z}\mid\boldsymbol{x})$ 与 $p_\theta(\boldsymbol{z}\mid\boldsymbol{y})$ 之间的相对熵损失，表示为

$$\begin{aligned}L_{\mathrm{ICVAE}} = &-\mathbb{E}_{q_{\varphi(\boldsymbol{z}\mid\boldsymbol{x})}}[\log p_\theta(\boldsymbol{x}\mid\boldsymbol{z},\boldsymbol{y})] + \\ &D_{\mathrm{KL}}(q_{\varphi(\boldsymbol{z}\mid\boldsymbol{x})} \| p(\boldsymbol{z}\mid\boldsymbol{y}))\end{aligned} \tag{2}$$

另外，针对 BAGAN 训练不稳定问题，本文对其结构进行了调整，GAN 结构如图 3(b)所示。首先，将判别器 D 中的多节点输出层 D_c 替换为原始 GAN 中的单节点输出层，并将样本类别信息输入生成器 G 和判别器 D 中。其次，结合 BAGAN 对少数类样本学习策略，可以从均匀的标签集合中随机采样来生成伪标签，但需要满足生成样本的数量等于真实样本的采样数量的条件。再次，设置随机噪声 $\boldsymbol{z}$ 服从 $P_{\boldsymbol{z}}(\boldsymbol{z}) \equiv p_\theta(\boldsymbol{z}\mid\boldsymbol{y})$ 分布且特定类样本的生成由输入类别信息控制。最后，判别器 D 的权重采取随机方式进行初始化，这是由于 D 的输入联合了类别信息导致其与 ICVAE 中的 En 输入不一致。

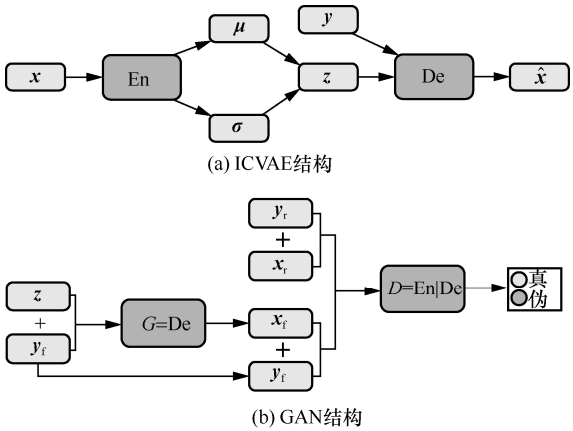


图 3　A-BAGAN 结构

在对抗训练过程中，对判别器 D 施加梯度惩罚 Wasserstein GAN（WGAN-GP, Wasserstein GAN with gradient penalty）和深度无悔分析 GAN 相结合的梯度约束项来稳定对抗训练[32]；结合样本和标签信息的匹配关系，对错误匹配标签的样本加以惩罚。因此，判别器 D 优化的损失函数 L_D 为

$$\begin{aligned}L_D = &-\varepsilon_{\boldsymbol{x}_{\mathrm{r}}\sim P_{\mathrm{r}}(\boldsymbol{x})}[\log D(\boldsymbol{x}_{\mathrm{r}},\boldsymbol{y}_{\mathrm{r}})] - \\ &\varepsilon_{\boldsymbol{z}\sim P_{\boldsymbol{z}}(\boldsymbol{z})}[\log(1-D(G(\boldsymbol{z},\boldsymbol{y}_{\mathrm{f}}),\boldsymbol{y}_{\mathrm{f}}))] - \\ &\varepsilon_{\boldsymbol{x}_{\mathrm{r}}\sim P_{\mathrm{r}}(\boldsymbol{x})}[\log(1-D(\boldsymbol{x}_{\mathrm{r}},\boldsymbol{y}_{\mathrm{w}}))] + \\ &\lambda\varepsilon_{\hat{\boldsymbol{x}}\sim P_{\hat{\boldsymbol{x}}}(\hat{\boldsymbol{x}})}[(\|\nabla_{\hat{\boldsymbol{x}}}D(\hat{\boldsymbol{x}},\boldsymbol{y}_{\mathrm{r}})\|_2 - 1)^2]\end{aligned} \tag{3}$$

其中，$\boldsymbol{y}_{\mathrm{r}}$、$\boldsymbol{y}_{\mathrm{f}}$ 和 $\boldsymbol{y}_{\mathrm{w}}$ 分别表示真实标签、伪标签和错误标签的独热形式，$\hat{\boldsymbol{x}} = \alpha\boldsymbol{x}_{\mathrm{r}} + (1-\alpha)\boldsymbol{x}_{\mathrm{f}}$，$\alpha \sim \mathcal{N}(0,1)$ 表示真实样本 $\boldsymbol{x}_{\mathrm{r}}$ 和生成样本 $\boldsymbol{x}_{\mathrm{f}} = G(\boldsymbol{z},\boldsymbol{y}_{\mathrm{f}})$ 的插值样本，λ 表示梯度惩罚因子。

生成器 G 在对抗训练中需要优化的损失函数 L_G 为

$$L_G = -\mathbb{E}_{z\sim P_z(z)}[\log D(G(\boldsymbol{z}, \boldsymbol{y}_{\mathrm{f}}), \boldsymbol{y}_{\mathrm{f}})] \tag{4}$$

A-BAGAN 模型训练算法如算法 1 所示。

算法 1 A-BAGAN 模型训练算法

初始化 编码器 En 的参数 $\boldsymbol{\theta}_{\mathrm{En}}$，解码器 De 的参数 $\boldsymbol{\theta}_{\mathrm{De}}$，生成器 G 的参数 $\boldsymbol{\theta}_G$，判别器 D 的参数 $\boldsymbol{\theta}_D$

1) 定义 ICVAE 训练阶段的迭代次数 T_1，批次大小 m_1
2) for t_1=1:T_1
3) 采样真实样本 $\{\boldsymbol{x}_{\mathrm{r}}^i\}_{i=1}^{m_1} \sim P_{\mathrm{r}}(\boldsymbol{x})$
4) 根据式(2)计算批样本的重构误差和相对熵损失之和的平均值
5) 利用 Adam 优化算法更新参数 $\boldsymbol{\theta}_{\mathrm{En}}$ 和 $\boldsymbol{\theta}_{\mathrm{De}}$
6) end for
7) 生成器 G 继承解码器 De 的权重，判别器 D 的参数随机初始化
8) 定义 GAN 训练阶段的迭代次数 T_2，批次大小 m_2，D 和 G 训练次数比 n_d
9) for t_2=1:T_2
10) for t_3=1:n_d
11) 采样真实样本 $\{\boldsymbol{x}_{\mathrm{r}}^i\}_{i=1}^{m_2} \sim P_{\mathrm{r}}(\boldsymbol{x})$
12) 为真实样本匹配错误标签 $\{y_{\mathrm{w}}^i\}_{i=1}^{m_2}$，$y_{\mathrm{w}}^i \sim U\{1,2,\cdots,C\} \setminus y_{\mathrm{r}}^i$，$C$ 为类别总数
13) 采样随机噪声 $\{\boldsymbol{z}^i\}_{i=1}^{m_2} \sim P_z(\boldsymbol{z})$，伪标签 $\{y_{\mathrm{f}}^i\}_{i=1}^{m_2}$，$y_{\mathrm{f}}^i \sim U\{1,2,\cdots,C\}$
14) 计算各插值样本 $\hat{\boldsymbol{x}}^i = \alpha \boldsymbol{x}_{\mathrm{r}}^i + (1-\alpha)\cdot \boldsymbol{x}_{\mathrm{f}}^i$，$\alpha \sim \mathcal{N}(0,1)$，$1 \leqslant i \leqslant m_2$
15) 根据式(3)计算判别损失 L_D
16) 利用 Adam 优化算法更新参数 $\boldsymbol{\theta}_D$
17) end for
18) 采样随机噪声 $\{\boldsymbol{z}^i\}_{i=1}^{m_2} \sim P_{\mathrm{r}}(\boldsymbol{x})$，伪标签 $\{y_{\mathrm{f}}^i\}_{i=1}^{m_2}$，$y_{\mathrm{f}}^i \sim U\{1,2,\cdots,C\}$
19) 根据式(4)计算生成损失 L_G
20) 利用 Adam 优化算法更新参数 $\boldsymbol{\theta}_G$
21) end for

3.2 检测模块

相比陆地通信环境，海洋无线传输环境更加复杂多变，MMSN 中存在大量的计算和存储能力较弱且能源受限的多种移动终端。为提供持续入侵检测能力，适当降低模型所需的计算与存储资源是迫切和必要的。因此，在构建检测模型时，本文借鉴了 AlexNet 中的分组卷积结构[36]。与普通卷积相比，分组卷积不仅占用资源更少且拥有一定的正则化作用。

由于网络数据为序列数据，本文使用的卷积均为一维卷积。LGCNN 结构如图 4 所示，主要由普通卷积层、分组卷积层、逐点卷积层和分类层组成。具体地，普通卷积层包含一层卷积和一层最大池化，用于对输入数据升维；分组卷积层包含上下 2 个分支，每个分支均为两层卷积，有利于上下分支学习到输入特征图不同通道的局部信息；逐点卷积层包含一个 1×1 卷积，用于融合特征图不同通道的信息，同时具有降维作用；分类层由两层全连接和一层 Softmax 构成，用于对输入特征的概率建模和分类，并在第一个全连接层后添加 Dropout 防止过拟合。

4 仿真实验结果与讨论分析

4.1 实验数据集选取

本文选取 NSL-KDD 和 CIC-IDS2017 数据集进行仿真实验。前者作为基准网络数据集，已经被广泛用于验证入侵检测模型的有效性。后者作为最新的数据测试集之一，能够较全面地代表当下的 MMSN 网络环境，有效地模拟真实 MMSN 的网络流量特性。

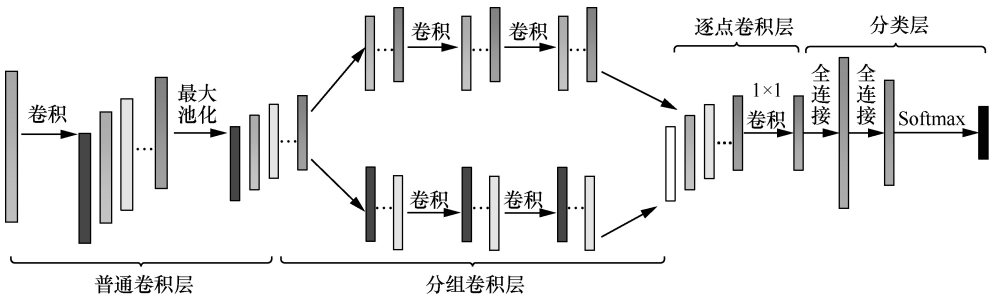


图 4 LGCNN 结构

NSL-KDD 数据集是在 KDDCup99 数据集的基础上删除冗余数据所生成的，各类样本呈现出高度不平衡特性。其中，训练集 KDDTrain+包含 21 种不同的攻击，并将这些攻击划分成 4 种攻击，即 DoS、Probe、U2R 和 R2L。测试集 KDDTest+将网络攻击细分为 37 种，包含众多未知攻击。训练集和测试集一共包括 148 517 条记录，每条记录含有 41 个有关网络连接的特征和一个标签，这 41 个特征中包含 3 个字符型特征和 38 个数值型特征，NSL-KDD 数据分布如表 1 所示。

表 1　　NSL-KDD 数据分布

数据集	Normal/条	DoS/条	Probe/条	U2R/条	R2L/条	总计/条
KDDTrain+	67 343	45 927	11 656	52	995	125 973
KDDTest+	9 711	7 459	2 421	200	2 754	22 544

CIC-IDS2017 数据集一共包括2 830 743 条记录，涵盖 DoS、暴力破解、Port Scan 和 Bot 等 14 种攻击。每条记录包括 78 个数值型特征和一个标签。本文首先对数据集进行数据清洗，删除了 1 358 条存在空字符的记录和 1 509 条存在无穷值的记录，然后将作用相似的攻击合并成一种攻击[37]，形成 6 种攻击。此外，因为该数据集过于庞大，使用全部的记录只会增加训练时长，不利于实验验证。因此，本文对 Benign、DoS 和 Port Scan 类型随机抽取部分记录，其余类型则保持不变，并按照 4:1 的比例划分训练集和测试集，如表 2 所示。

4.2　实验数据集预处理

NSL-KDD 数据集中存在字符型特征和数值型特征，且数值型特征取值范围差异很大，因此需要对数据进行预处理。对于字符型特征，本文使用独热编码进行转化。对于数值型特征，使用极小极大归一化方法将特征的取值范围限制在[0,1]。预处理后的数据维度从 41 扩展至 122。CIC-IDS2017 数据集中只包含数值型特征，因此仅对数据进行归一化处理，处理后的数据维度不变。

4.3　实验评估指标

本文使用平均欧氏距离（MED, mean Euclidean distance）和最大均值差异（MMD, maximum mean discrepancy）2 个统计指标来衡量生成样本的有效性，如式(5)和式(6)所示。MED 通过计算真实样本集 $\boldsymbol{X}_{\mathrm{r}}=\left\{\boldsymbol{x}_{\mathrm{r}}^{i}\right\}_{i=1}^{m}$ 和生成样本集 $\boldsymbol{X}_{\mathrm{f}}=\left\{\boldsymbol{x}_{\mathrm{f}}^{j}\right\}_{j=1}^{n}$ 的总体均值之间的欧氏距离来评估样本的相似性。MMD 使用核函数 $k:\boldsymbol{X}_{\mathrm{r}}\otimes\boldsymbol{X}_{\mathrm{f}}\to\mathcal{H}$ 将样本映射到再生希尔伯特空间 $\mathcal{H}$，计算投影后真实样本与生成样本的总体均值之差来衡量真实分布和生成分布的差异，⊗表示哈达玛积。

$$\mathrm{MED}(\boldsymbol{X}_{\mathrm{r}},\boldsymbol{X}_{\mathrm{f}})=\left\|\frac{1}{m}\sum_{i=1}^{m}\boldsymbol{x}_{\mathrm{r}}^{i}-\frac{1}{n}\sum_{j=1}^{n}\boldsymbol{x}_{\mathrm{f}}^{j}\right\|_{2}^{2} \tag{5}$$

$$\mathrm{MMD}^{2}(\boldsymbol{X}_{\mathrm{r}},\boldsymbol{X}_{\mathrm{f}})=\left\|\frac{1}{m}\sum_{i=1}^{m}k\boldsymbol{x}_{\mathrm{r}}^{i}-\frac{1}{n}\sum_{j=1}^{n}k\boldsymbol{x}_{\mathrm{f}}^{j}\right\|_{\mathcal{H}}^{2} \tag{6}$$

另外，采用精确率（Precision）、召回率（Recall）和 F1 值作为模型分类效果的评估指标。

4.4　仿真实验参数设置

本文仿真实验是在 Python3.8 和 Pytorch 1.10.0 环境下进行的。A-BAGAN 采用全连接结构，其参数设置如表 3 所示。LGCNN 参数设置如表 4 所示。为更好地分析本文模型的性能，本文还实现了 5 种数据增强模型作为对比，分别是 ROS、SMOTE、

表 2　　CIC-IDS2017 数据分布

数据集	Benign/条	DoS/条	Port Scan/条	暴力破解/条	Web Attack/条	Bot/条	Infiltration/条	总计/条
训练集	127 193	30 380	12 704	11 065	1 744	1 565	29	184 680
测试集	31 799	7 595	3 176	2 767	436	391	7	46 171

表 3　　A-BAGAN 参数设置

参数设置	NSL-KDD	CIC-IDS2017
编码器 En	122-256-128-64-32	78-85-128-64-32-15
解码器 De	37-64-128-256-122	22-32-64-128-85-78
训练周期/轮	30, 300	40, 500
批次大小/条	128, 128	128, 128
学习率	0.000 1, 0.000 2	0.01, 0.000 2

ADASYN、CWGAN-GP（conditional WGAN-GP）以及 BAGAN。

表 4 LGCNN 参数设置

参数	NSL-KDD	CIC-IDS2017
普通卷积层	[1,3]×8, poolsize:2	[1,3]×8, poolsize:2
分组卷积层	[1,2]×3, [1,2]×8	[1,2]×12, [1,2]×18
逐点卷积层	[1,1]×1	[1,1]×1
分类层	160-80-5, Dropout:0.5	128-64-7, Dropout:0.5
训练周期/轮	100	200
批次大小/条	256	1 024
学习率	0.000 5	0.001

4.5 实验结果分析

4.5.1 潜在表示可视化对比

首先，对比分析 BAGAN 和 A-BAGAN 中 AE 训练阶段学习之后的潜在表示，并利用 t-SNE 技术将潜在表示映射到二维平面可视化。图 5(a)和图 6(a)分别展示了 NSL-KDD 和 CIC-IDS2017 数据集在计算机仿真实验中 AE 训练阶段学习到的潜在表示可视化结果。从图 5(a)中可以看出，各类样本分布散乱且重叠现象明显。例如，R2L 与 Normal 样本的重叠比例较高，这是因为 R2L 是一种伪装式攻击，通常作用于数据包负载；其余部分与正常数据包的特点相似，因此 R2L 攻击样本与 Normal 样本区分度不大。同样地，如图 6(a)所示，在 CIC-IDS2017 实验中可以观察到类似的现象。

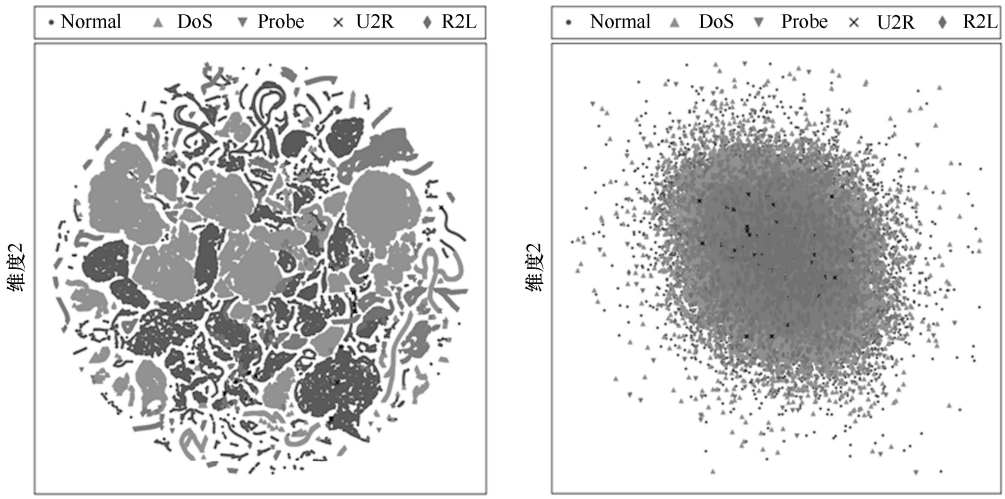
本文提出的 ICVAE 可以有效地学习不同类型样本之间的公共特征。从图 5(b)和图 6(b)可以看出，各类样本均匀地融合在一起，并难以通过某种规则推断出潜在表示所属的类别信息。这说明本文提出的 ICVAE 在训练后能够为 GAN 提供一个良好的初始状态，从而有助于在后续对抗训练中克服生成样本类别模糊的问题。

4.5.2 生成样本统计评估

为直观地评估 A-BAGAN 的生成能力，通过 MED 和 MMD 衡量真实攻击样本与生成攻击样本之间的相似性，并选取 ADASYN、CWGAN-GP 和 BAGAN 作为对比。具体评估结果如表 5 和表 6 所示。

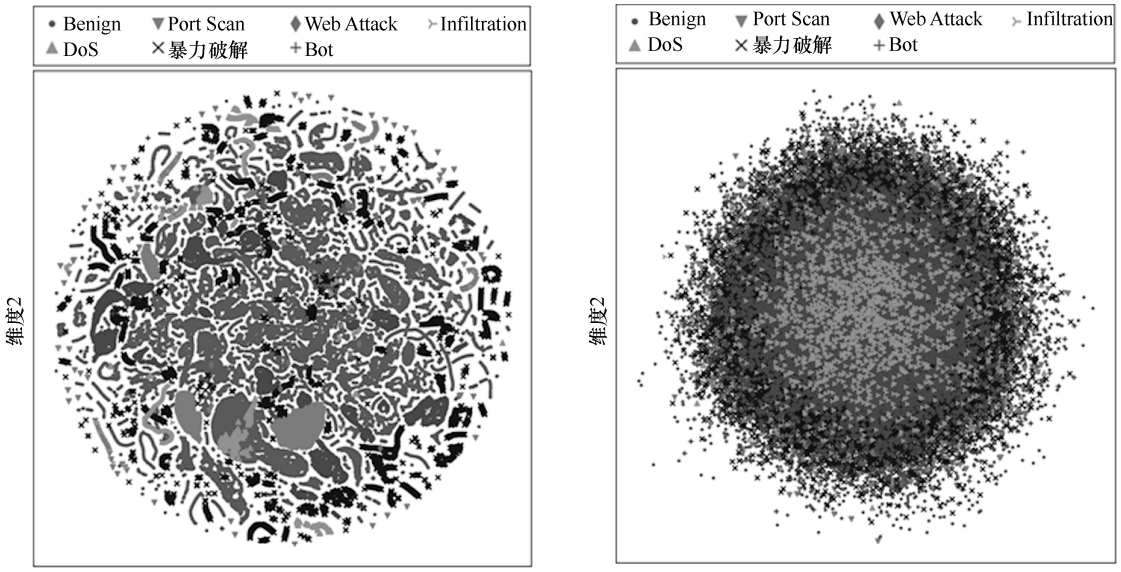
从表 5 可知，在 NSL-KDD 数据集生成样本的统计评估中，本文模型在 4 种生成的攻击样本上取得了总体最优的结果。其中，MED 最大值不超过 0.062 7，MMD 平均值为 0.075 0，这说明本文模型能够有效学到真实数据分布；ADASYN 在攻击样本生成中取得了整体最差结果。例如，DoS 类生成样本的 MED 和 MMD 分别为 5.482 5、2.531 2，这说明生成的 DoS 样本分布与实际分布差异大；CWGAN-GP 在攻击样本的生成中获得了总体次优的结果，这源于其采用 Wasserstein 距离作为度量，并引入了梯度惩罚；BAGAN 作为一种基于不平衡数据集的生成模型，并未表现出良好的统计结果，这是因为 BAGAN 并未解决类别模糊和训练不稳定的问题。

从表 6 可知，在 CIC-IDS2017 数据集生成样本的统计评估中，本文模型依然能够取得总体最优的结果；ADASYN 总体结果表现最差；CWGAN-GP 在 Infiltration 类生成样本表现出最差的统计结果，



(a) AE学习的潜在表示　　(b) ICVAE学习的潜在表示

图 5 NSL-KDD 数据集潜在表示可视化结果



(a) AE学习的潜在表示　　(b) ICVAE学习的潜在表示

图 6　CIC-IDS2017 数据集潜在表示可视化结果

表 5　　**NSL-KDD 攻击样本扩充的统计评估**

模型	DoS		Probe		U2R		R2L	
	MED	MMD	MED	MMD	MED	MMD	MED	MMD
ADASYN	5.482 5	2.531 2	0.915 6	0.501 9	0.163 8	0.262 5	0.109 0	0.224 2
CWGAN-GP	0.178 2	0.117 3	0.006 1	0.005 1	0.098 2	0.189 9	0.034 1	0.064 4
BAGAN	0.546 9	0.673 6	1.037 0	0.561 9	0.340 7	0.505 0	0.052 3	0.133 4
本文模型	0.003 7	0.009 7	0.022 7	0.014 1	0.062 7	0.256 2	0.009 7	0.019 8

表 6　　**CIC-IDS2017 数据集攻击样本扩充的统计评估**

模型	DoS		Port Scan		暴力破解		Web Attack		Bot		Infiltration	
	MED	MMD	MED	MMD	MED	MMD	MED	MMD	MED	MMD	MED	MMD
ADASYN	1.234 6	1.073 2	0.044 2	1.093 8	0.260 6	0.626 0	0.378 0	1.721 7	0.403 3	0.826 6	0.012 9	0.039 2
CWGAN-GP	0.001 8	0.003 7	0.017 4	0.267 4	0.078 7	0.138 5	0.143 3	2.373 5	0.007 9	0.060 0	4.078 1	4.374 4
BAGAN	0.130 5	0.157 3	0.018 8	0.683 8	0.012 9	0.029 4	0.017 0	0.101 3	0.028 1	0.063 7	0.263 9	0.792 7
本文模型	0.148 4	0.134 4	0.001 0	0.035 2	0.001 4	0.004 0	0.025 6	0.140 5	0.016 3	0.029 1	0.511 9	0.759 8

MMD 达到了 4.374 4；与 NSL-KDD 数据集实验中表现结果不同，BAGAN 在 DoS、暴力破解和 Bot 等攻击上的统计指标表现良好。上述分析表明，本文模型生成的样本兼顾真实性和类别属性，且在对抗训练过程中具有良好的稳定性，其效果优于传统的数据增强模型，这进一步体现了 A-BAGAN 应用于 MMSN 入侵检测数据不平衡处理是可行的。

4.5.3　检测模型性能分析

为分析本文数据增强模型对检测性能的改善情况，本节对比了 LGCNN 在原始数据集和其他 5 种数据增强的混合数据集上训练后的整体分类性能。在 NSL-KDD 数据集中，混合数据集中各类样本数量比例为 1:1，整体分类性能对比结果如图 7 所示；CIC-IDS2017 数据集仅对 Web Attack、Bot 和 Infiltration 类进行十倍数生成，生成数量分别为

15 696、14 085 和 2 871，该差异取决于数据集本身的性质，生成过多样本易造成冗余和噪声，整体分类性能对比结果如图 8 所示。

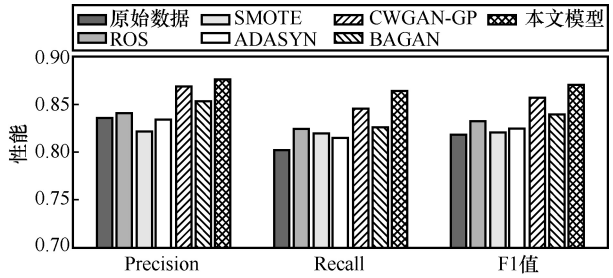


图 7　NSL-KDD 数据集中整体分类性能对比

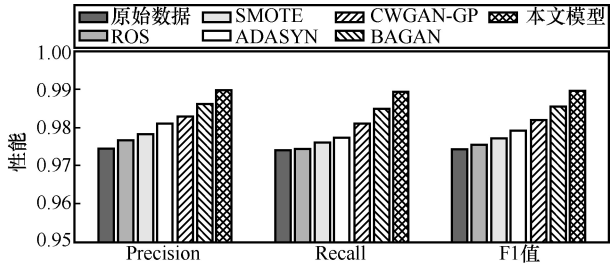


图 8　CIC-IDS2017 数据集中整体分类性能对比

由图 7 可知，在 NSL-KDD 数据集中，本文模型在 3 个指标上均取得了最优结果，其精确率、召回率和 F1 值分别为 0.876 2、0.864 2 和 0.870 2。相较于数据增强之前，提高了 0.040 5 的精确率、0.062 3 的召回率和 0.051 7 的 F1 值。相较于其余 5 种数据增强模型的平均性能，提高了 0.032 4 的精确率、0.038 2 的召回率和 0.035 5 的 F1 值。在原始数据集上训练后，分类器整体性能差是由部分攻击类型样本数量少导致的。ROS、SMOTE 和 ADASYN 等传统的数据增强模型取得了较差的性能，其最高的 F1 值为 0.832 5。CWGAN-GP 取得了次优的结果，在 3 个指标上的性能较均衡，但仍比本文模型低 0.013 3 的 F1 值。BAGAN 相比较于传统增强方法略有提升，其 F1 值为 0.839 4，提升效果并不显著。

由图 8 可知，CIC-IDS2017 数据集中各增强模型在精确率、召回率和 F1 值指标上呈现出较均衡的结果，且分类性能均优于原始数据集上的性能。ADASYN 相比较于 ROS 和 SMOTE，取得了更好的性能，其 F1 值达到了 0.979 2。BAGAN 整体性能优于 CWGAN-GP，取得了 0.986 2 的精确率、0.984 9 的召回率、0.985 5 的 F1 值的次优结果，这是因为 BAGAN 在该数据集生成了更加真实的样本。但本文模型相比较于 BAGAN，分别提升了 0.003 6 的精确率、0.004 5 的召回率和 0.004 1 的 F1 值。上述实验结果说明了本文模型优于对比模型，也验证了对 BAGAN 改进的有效性。

为更直观地评估本文模型与其他增强模型对少数类攻击的识别效果，本文从 2 个数据集中共选取 4 种少数类攻击用于对比，以综合指标 F1 值作为衡量指标，其对比结果如图 9 所示。从图 9 可以看出，本文模型对 U2R、R2L 和 Web Attack 类攻击均取得了最优结果，对 Bot 类攻击具有最高的竞争能力。

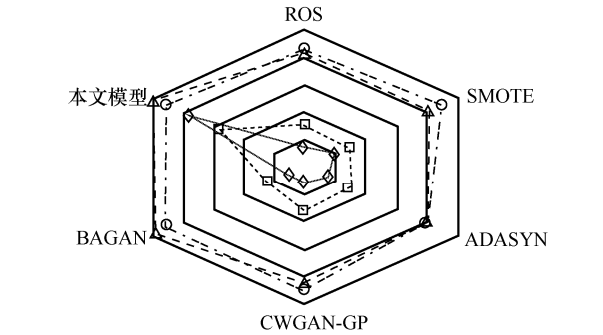


图 9　少数类攻击检测效果对比

最后，本文对比了几种入侵检测领域的最新研究，与文献[16,18,21,38]中提出的算法作为对比。NSL-KDD 数据集中不同算法的总体性能对比如表 7 所示。从表 7 可以看出，本文模型在召回率和 F1 值指标上展现出了最佳性能，而在精确率上取得次优结果。其中，F1 值达到了 0.870 2；相较于 RANet、ROULETTE、IGAN 和 LCVAE 分别提升了 0.044 5、0.090 8、0.028 5 和 0.062 3。

表 7　NSL-KDD 数据集中不同算法的总体性能对比

算法	Precision	Recall	F1 值
RANet	0.819 2	0.832 3	0.825 7
ROULETTE	0.828 5	0.804 3	0.779 4
IGAN	0.848 5	0.844 5	0.841 7
LCVAE	0.976 1	0.685 3	0.807 9
本文模型	0.876 2	0.864 2	0.870 2

由于在 CIC-IDS2017 数据集中数据设置不一致，本文实现了 LR（logistic regression）、SVM、MLP（multilayer perceptron）、CNN 和 LSTM 作为对比算法，不同算法的总体性能对比对比结果如表 8 所示。从表 8 可以看出，本文模型在精确率、召回率和 F1 值指标中均取得最优结果。其中，F1 值达到了 0.989 6；相较于 LR、SVM、MLP、CNN 和 LSTM 分别提升了 0.088 0、0.056 4、0.012 2、0.013 3 和 0.010 5。

表 8　CIC-IDS2017 数据集中不同算法的总体性能对比

算法	Precision	Recall	F1 值
LR	0.896 6	0.906 7	0.901 6
SVM	0.935 1	0.931 3	0.933 2
MLP	0.978 2	0.976 7	0.977 4
CNN	0.976 8	0.975 8	0.976 3
LSTM	0.979 6	0.978 7	0.979 1
本文模型	0.989 8	0.989 4	0.989 6

LGCNN 占用资源和模型大小如表 9 所示。从表 9 可以看出，本文提出的 LGCNN 具有较低的计算复杂度，其中，平均训练参数数量和浮点计算量（FLOP）分别为 18 786 个和 44 632 次，模型规模较小，这表明 LGCNN 具有轻量级性质，可满足 MMSN 的实际部署需求。

表 9　　LGCNN 占用资源和模型大小

数据集	训练参数数量/个	FLOP/次	模型大小/KB
NSL-KDD	22 940	34 688	92
CIC-IDS2017	14 632	54 576	62

5　结束语

本文描述了基于移动边缘计算的海洋气象传感网物理架构，并提出了一种基于平衡生成对抗网络的入侵检测模型。该模型利用 A-BAGAN 来解决入侵检测数据集不平衡的问题，构建基于分组卷积的 LGCNN 检测分类器以适应资源约束型海洋移动终端，并分别在公共网络数据集 NSL-KDD 和 CIC-IDS2017 上进行了计算机模拟仿真实验。实验结果表明，与传统的数据增强模型相比，A-BAGAN 生成的样本兼顾真实性和类别属性，且对抗训练过程稳定，能够有效提高入侵检测分类器的识别效果，尤其是针对少数类样本的攻击。未来，将结合深度强化学习研究移动边缘计算对 MMSN 入侵检测任务计算量的影响。此外，为进一步提高 MMSN 安全性，将结合迁移学习开展特征选择的入侵检测研究。

参考文献：

[1] XIA T T, WANG M M, ZHANG J J, et al. Maritime Internet of things: challenges and solutions[J]. IEEE Wireless Communications, 2020, 27(2): 188-196.

[2] YANG X, XING H Y. A data complementary method for thunderstorm point charge localization based on atmospheric electric field apparatus array group[J]. Digital Communications and Networks, 2021, 7(2): 170-177.

[3] LIU R W, NIE J T, GARG S, et al. Data-driven trajectory quality improvement for promoting intelligent vessel traffic services in 6G-enabled maritime IoT systems[J]. IEEE Internet of Things Journal, 2021, 8(7): 5374-5385.

[4] 苏新, 孟蕾蕾, 周一青, 等. 基于深度强化学习的海洋移动边缘计算卸载方法[J]. 通信学报, 2022, 43(10): 133-145.
SU X, MENG L L, ZHOU Y Q, et al. Maritime mobile edge computing offloading method based on deep reinforcement learning[J]. Journal on Communications, 2022, 43(10): 133-145.

[5] ASHRAF I, PARK Y, HUR S, et al. A survey on cyber security threats in IoT-enabled maritime industry[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2677-2690.

[6] SU X, WANG H, FU X, et al. Substring-searchable attribute-based encryption and its application for IoT devices[J]. Digital Communications and Networks, 2021, 7(2): 277-283.

[7] ANDERSON J P. Computer security threat monitoring and surveillance[R]. 1980.

[8] LI W J, WANG Y, JIN Z P, et al. Challenge-based collaborative intrusion detection in software-defined networking: an evaluation[J]. Digital Communications and Networks, 2021, 7(2): 257-263.

[9] AMBUSAIDI M A, HE X J, NANDA P, et al. Building an intrusion detection system using a filter-based feature selection algorithm[J]. IEEE Transactions on Computers, 2016, 65(10): 2986-2998.

[10] ALAZZAM H, SHARIEH A, SABRI K E. A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer[J]. Expert Systems with Applications, 2020, 148: 113249.

[11] DERHAB A, BELAOUED M, MOHIUDDIN I, et al. Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(3): 2366-2379.

[12] VU L, CAO V L, NGUYEN Q U, et al. Learning latent representation for IoT anomaly detection[J]. IEEE Transactions on Cybernetics, 2022, 52(5): 3769-3782.

[13] ZHAO R J, YIN J, XUE Z, et al. An efficient intrusion detection method based on dynamic autoencoder[J]. IEEE Wireless Communications Letters, 2021, 10(8): 1707-1711.

[14] CHEN Y, LIN Q Z, WEI W H, et al. Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of things in fog computing[J]. Knowledge-Based Systems, 2022, 244: 108505.

[15] LEI S W, XIA C H, LI Z, et al. HNN: a novel model to study the intrusion detection based on multi-feature correlation and temporal-spatial analysis[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(4): 3257-3274.

[16] ZHANG X Q, YANG F, HU Y, et al. RANet: network intrusion detection with group-gating convolutional neural network[J]. Journal of Network and Computer Applications, 2022, 198: 103266.

[17] KANNA P R, SANTHI P. Hybrid intrusion detection using MapReduce based black widow optimized convolutional long short-term memory neural networks[J]. Expert Systems with Applications, 2022, 194: 116545.

[18] ANDRESINI G, APPICE A, CAFORIO F P, et al. ROULETTE: a neural attention multi-output model for explainable network intrusion detection[J]. Expert Systems with Applications, 2022, 201: 117144.

[19] REHMAN S U, KHALIQ M, IMTIAZ S I, et al. DIDDOS: an approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)[J]. Future Generation Computer Systems, 2021, 118: 453-466.

[20] BAGUI S, LI K Q. Resampling imbalanced data for network intrusion detection datasets[J]. Journal of Big Data, 2021, 8(1): 1-41.

[21] HUANG S K, LEI K. IGAN-IDS: an imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks[J]. Ad Hoc Networks, 2020, 105: 102177.

[22] VU L, NGUYEN Q U. Handling imbalanced data in intrusion detection systems using generative adversarial networks[J]. Journal on Information Technologies & Communications, 2020, 2020(1): 1-13.

[23] YUAN D N, OTA K, DONG M X, et al. Intrusion detection for smart home security based on data augmentation with edge computing[C]//Proceedings of 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-6.

[24] ANDRESINI G, APPICE A, ROSE L D, et al. GAN augmentation to deal with imbalance in imaging-based intrusion detection[J]. Future Generation Computer Systems, 2021, 123: 108-127.

[25] MARIANI G, SCHEIDEGGER F, ISTRATE R, et al. BAGAN: data augmentation with balancing GAN[J]. arXiv Preprint, arXiv: 1803.09655, 2018.

[26] ZHU J X, MENG L L, WU W X, et al. Generative adversarial network-based atmospheric scattering model for image dehazing[J]. Digital Communications and Networks, 2021, 7(2): 178-186.

[27] BROPHY E, WANG Z W, SHE Q, et al. Generative adversarial networks in time series: a survey and taxonomy[J]. arXiv Preprint, arXiv: 2107.11098, 2021.

[28] ZHAO X, HUANG G Q, JIANG J, et al. Task offloading of cooperative intrusion detection system based on deep Q network in mobile edge computing[J]. Expert Systems with Applications, 2022, 206: 117860.

[29] HE Y, CHENG J G. User location privacy protection mechanism for location-based services[J]. Digital Communications and Networks, 2021, 7(2): 264-276.

[30] MINAHIL, AYUB M F, MAHMOOD K, et al. Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology[J]. Digital Communications and Networks, 2021, 7(2): 235-244.

[31] GURUMURTHY S, SARVADEVABHATLA R K, BABU R V. DELIGAN: generative adversarial networks for diverse and limited data[C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2017: 4941-4949.

[32] HUANG G F, JAFARI A H. Enhanced balancing GAN: minority-class image generation[J]. Neural Computing and Applications, 2023, 35(7): 5145-5154.

[33] GULRAJANI I, AHMED F, ARJOVSKY M, et al. Improved training of Wasserstein GANs[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2017: 5769-5779.

[34] KODALI N, ABERNETHY J, HAYS J, et al. On convergence and stability of GANs[J]. arXiv Preprint, arXiv:1705.07215, 2017.

[35] MAKHZANI A, SHLENS J, JAITLY N, et al. Adversarial autoencoders[J]. arXiv Preprint, arXiv:1511.05644, 2015.

[36] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[37] PANIGRAHI R, BORAH S. A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems[J]. International Journal of Engineering & Technology, 2018, 7(3): 479-482.

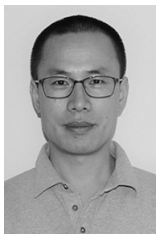
[38] XU X, LI J, YANG Y, et al. Toward effective intrusion detection using log-cosh conditional variational autoencoder[J]. IEEE Internet of Things Journal, 2021, 8(8): 6187-6196.

[作者简介]

苏新（1986− ），男，河北霸州人，博士，河海大学教授，主要研究方向为移动通信、边缘/雾计算、智慧海洋等。

张桂福（1999− ），男，江西赣州人，河海大学硕士生，主要研究方向为入侵检测、边缘/雾计算、智慧海洋等。

行鸿彦（1962− ），男，山西新绛人，博士，南京信息工程大学教授，主要研究方向为气象仪器设计与计量、信号检测与处理等。



Zenghui Wang（1979− ），男，博士，南非大学教授，主要研究方向为人工智能及其应用、自动控制等。