研究与开发

结合自适应数据增强和集成学习的机载网络入侵检测研究

周茂辉[1]，刘文琪[1]，李艳军[1]，宫艺姝[2]
（1. 南京航空航天大学民航学院，江苏 南京 210016；
2. 新疆通达低空科技有限公司，新疆 石河子 832000）

摘　要：机载网络入侵检测可能面临异常样本稀缺和数据分布不平衡的双重挑战，传统方法难以同时保证检测精度和泛化能力。为此，结合多视图对比稀疏自编码器（multi-view contrastive sparse autoencoder，MCSAE）的数据增强方法，提出一种改进分层抽样集成学习的联合优化方法。首先，针对异常样本缺失问题，设计MCSAE，通过多视图数据增强和对比学习策略，在稀疏自编码器框架下学习更具判别性的潜在表示，并利用重输入对比机制优化异常样本生成质量，有效缓解数据稀疏性带来的模型偏差。其次，针对类别不平衡问题，提出改进分层抽样策略，在传统分层抽样基础上引入全局特征保留机制，避免局部采样导致多数类分布失真，确保分类器能够学习数据的完整统计特性。最后，结合F1分数自适应加权集成学习，融合随机森林、长短期记忆（long short-term memory，LSTM）网络等多样化基分类器，动态调整模型权重，进一步提升对少数类攻击的检测能力。实验结果表明，相较于现有方法，所提方法在机载网络数据集上的召回率提升5.2%，F1分数提升3.7%，为复杂网络环境下的入侵检测提供了可靠解决方案。

关键词：分布不平衡；多视图对比稀疏自编码器；分层抽样；集成学习
中图分类号：TN915.08；TP309
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2026050

Research on airborne network intrusion detection combining adaptive data augmentation and ensemble learning

Zhou Maohui[1], Liu Wenqi[1], Li Yanjun[1], Gong Yishu[2]
1. College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
2. Xinjiang Tongda Low-altitude Technology Co., Ltd., Shihezi 832000 , China

Abstract: Airborne network intrusion detection may face the dual challenges of scarce abnormal samples and unbal-

收稿日期：2025−07−23；**修回日期：**2025−11−25
通信作者：刘文琪，3066813038@qq.com
基金项目：江苏省研究生科研与实践创新计划项目（No.KYCX25_0620）；新疆生产建设兵团科技计划资助项目（No.2025AB070，No.2025AB068）
Foundation Items: The Project of Jiangsu Province Graduate Research and Practical Innovation Program (No.KYCX25_0620), Supported by Science and Technology Program of XPCC (No.2025AB070, No.2025AB068)

anced data distribution. Traditional methods are difficult to simultaneously guarantee detection accuracy and generalization ability. Therefore, combined with the data augmentation method of multi-view contrastive sparse autoencoder (MCSAE), a joint optimization method with improved hierarchical sampling ensemble learning was proposed. Firstly, for the problem of missing abnormal samples, a MCSAE was designed. Through multi-view data augmentation and contrastive learning strategies, a more discriminative latent representation was learned under the framework of sparse autoencoder, and the quality of abnormal sample generation was optimized by the re-input contrast mechanism, effectively alleviating the model deviation caused by data sparsity. Secondly, for the problem of class imbalance, an improved hierarchical sampling strategy was proposed. On the basis of traditional hierarchical sampling, a global feature retention mechanism was introduced to avoid the distortion of the majority class distribution caused by local sampling, ensuring that the classifier can learn the complete statistical characteristics of the data. Finally, combined with F1 score adaptive weighted ensemble learning, diverse base classifiers such as random forest and LSTM were integrated to dynamically adjust the model weights, further improving the detection ability for minority class attacks. The experimental results show that, compared with the existing methods on the airborne network dataset, the proposed method has a 5.2% increase in recall rate and a 3.7% increase in F1 score. This provides a reliable solution for intrusion detection in complex network environments.

Key words: distribution imbalance, multi-view contrastive sparse autoencoder, stratified sampling, ensemble learning

0 引言

随着航空电子系统智能化水平的提升，机载网络在现代航空器综合化信息架构中得到广泛应用。在此背景下，机载网络的安全问题日益受到关注。攻击者可能通过远程入侵或内部破坏，严重威胁航空器的正常运行与数据安全。近年来，网络入侵检测技术的迅速发展，为航空电子系统的安全防护构建了重要的安全屏障[1]。

当前，基于深度学习的网络入侵检测技术在航空机载网络安全领域取得了显著进展。深度神经网络模型能够从高维复杂的网络流量中自动提取关键特征，有效提升了对复杂攻击行为的检测能力。然而，机载网络数据通常存在明显的不平衡特性，即正常样本占绝大多数，而异常样本相对稀少，这使得模型在训练过程中容易出现过拟合或对少数类检测能力不足的问题。为解决这一难题，研究者从数据层与模型层提出了多种改进方法[2]，这些方法可以归纳为数据过采样和数据生成两类。文献[3]系统评估了多种过采样策略，包括合成少数类过采样、支持向量机过采样、边界过采样以及基于聚类的K均值（K-means）等方法，验证了不同过采样方法对提升检测性能的影响。文献[4]结合改进的条件变分自编码器与深度神经网络生成符合特定入侵类别的新样本，从而平衡了训练数据并提升了少数类的检测精度。此外，使用对抗神经网络生成新的样本也是解决数据不平衡问题的重要方法[5-7]。生成对抗网络通过估计少数类样本的高斯分布获取潜在先验知识，用于潜在空间生成高质量样本，从而有效缓解样本不平衡带来的性能下降。

除了数据不平衡问题，机载网络在实际应用中还面临异常样本稀缺及标签不完整的挑战。传统有监督模型依赖充足的带标签数据，而在标注困难或攻击类型未知的场景下，其检测能力与泛化性能会显著下降。针对这类问题，研究人员从集成学习、对比学习、迁移学习和可解释神经网络等多个方面开展研究。集成学习方法通过集成多种模型，如卷积神经网络[8]（convolutional neural network，CNN）、长短期记忆（long short-term memory，LSTM）网络[9]和随机森林[10]（random forest，RF）等，发挥各自的优势，从而

提高模型的检测效率。文献[11]提出了结合过采样技术优化的多层集成模型，用于机载网络入侵检测。文献[12]提出融合混合采样策略与集成分类的方法，显著提升了检测效果。文献[13]设计的自适应入侵检测系统（adaptive intrusion detection system，AdaptIDS）则采用堆叠集成等深度学习技术，提供了高检测效能和计算效率的自适应入侵检测方案。文献[14]提出结合稀疏自编码器与综合马氏距离的异常检测方法，通过学习正常样本的稀疏特征表示来识别偏离分布的异常行为，在欺骗攻击检测中取得较低的误报率。对比学习方法作为一种自监督学习范式，为无标签或异常样本稀缺场景提供了新的研究思路[15-17]。该方法通过构建正负样本对，使模型在特征空间中拉近同类样本、拉远异类样本，从而获得具有判别性的潜在表示。迁移学习方法[18]将网络入侵数据转化成图像数据，再将预训练的模型迁移到网络入侵数据上，也能有效提高模型检测准确率。此外，将网络拓扑结构等物理信息融入神经网络以提高模型可解释性，也是目前较为先进的解决方法[19-21]。

尽管现有研究在不平衡数据处理和无监督异常检测方面取得了积极进展，但仍存在一些不足。一方面，大多数方法仅在单一视角下提取特征，缺乏对多视图特征间的关联建模，难以充分利用机载网络数据的多维属性；另一方面，现有稀疏自编码器在潜在空间的特征一致性约束不足，导致模型的泛化性能和稳定性受到限制。此外，传统的异常检测模型通常采用固定阈值或经验阈值，未能在特异性与准确率之间实现有效平衡。针对以上问题，本文提出一种基于多视图对比稀疏自编码器（multi-view contrastive sparse autoencoder，MCSAE）的航空网络异常检测方法。在稀疏自编码器的基础上，引入多视图结构，通过视图间对比学习与重输入对比机制，从同一样本的不同视角中学习多样化且一致的潜在表示，从而优化潜在空间的稀疏性与一致性。同时，本文结合验证集样本，设计了一种综合特异性与准确率的自适应阈值选择方法，以实现对正常与异常网络流量的更精确区分。

1　方法

本文提出了一种融合MCSAE、分层抽样与集成学习（stratified sampling and ensemble learning，SSEL）的异常检测方法，构建了“特征增强–样本均衡–集成优化”的三阶段检测框架。该方法首先通过MCSAE实现数据增强，利用视图间特征对比学习与稀疏约束强化高维少样本数据的特征判别能力，为后续检测任务提供更鲁棒的特征表示；随后针对数据集中的类别不平衡问题，采用改进分层抽样策略动态调整类别抽样比例，构建多个类间分布均衡的训练子集，从数据层面降低模型对多数类样本的过度拟合偏差；最后在平衡子集的基础上，引入性能互补的多种基分类器构建集成学习框架，通过自适应融合各子集的检测结果，充分发挥不同分类器对复杂模式的捕捉优势。本文方法的技术路线如图1所示。

1.1　基于稀疏自编码器的数据增强方法

在异常检测任务中，为了更有效地建模正常样本的潜在分布，MCSAE数据增强方法被提出。MCSAE模型包括3个主要部分：多视图稀疏自编码器模块、视图间对比学习模块和重输入模块。这些模块通过联合优化目标协同工作，最终生成鲁棒的潜在空间表征。给定输入数据$X\in\mathbf{R}^{n\times k}$（其中$n$为样本数量，$d$为特征维度），通过构建$V$个独立初始化的稀疏自编码器，分别生成多视图的潜在表示和重构输出。第v个视图的编码与解码过程分别定义为：

$$\begin{cases} z^{(v)}=f_{\mathrm{enc}}^{(v)}(X) \\ \hat{X}^{(v)}=f_{\mathrm{dec}}^{(v)}\left(z^{(v)}\right) \end{cases} \tag{1}$$

其中，$z^{(v)}\in\mathbf{R}^{n\times k}$为潜在表示，$k$为隐藏层神经元

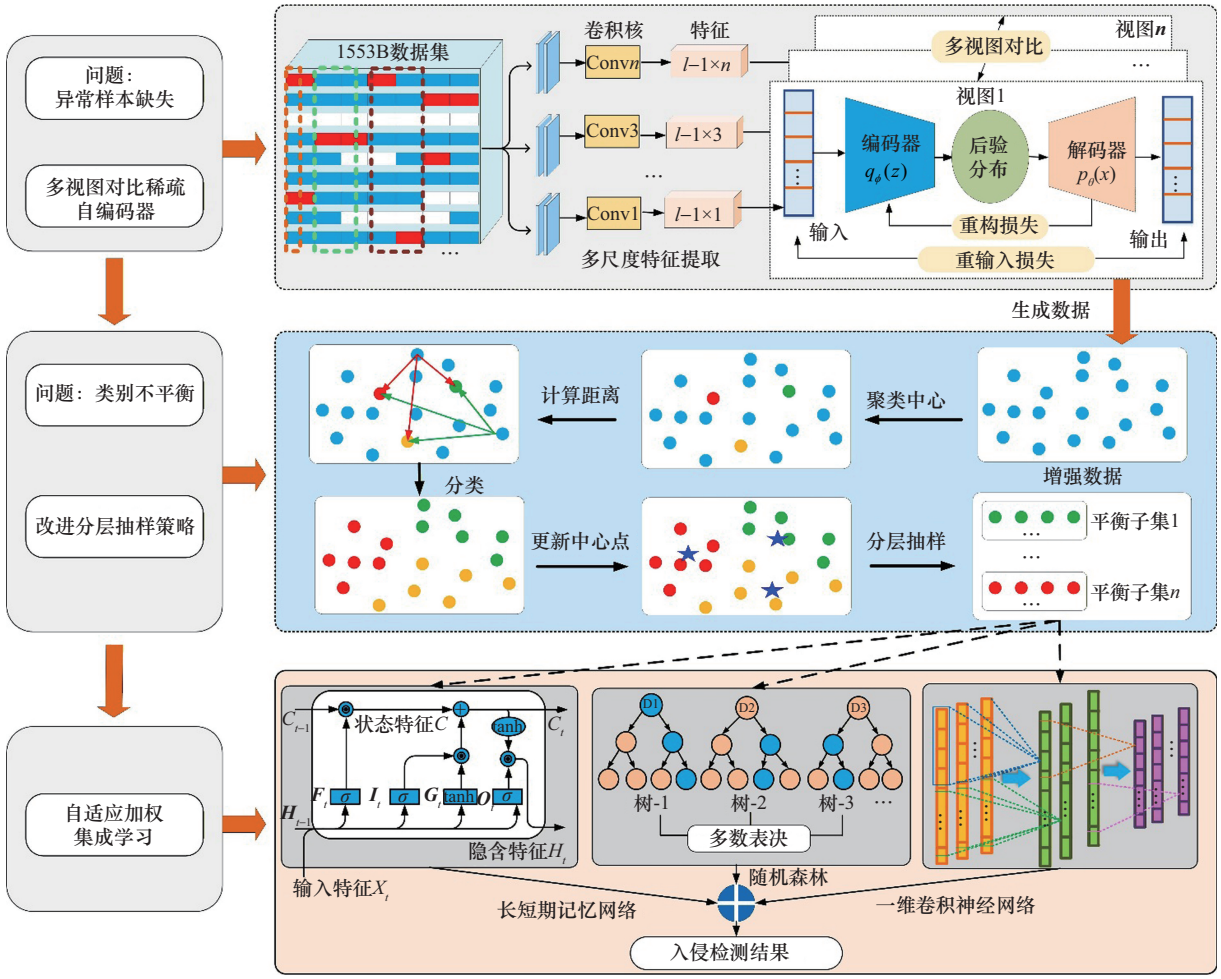

图1　本文方法的技术路线

数量，f_{enc}和f_{dec}分别为第v个视图的编码器和解码器。在训练过程中使用最小化重构误差和稀疏正则化项对编码器和解码器进行约束。稀疏性约束的核心是对隐藏层单元的平均激活值进行正则化，以限制其激活频率。本文使用修正线性单元（rectified linear unit，ReLU）作为激活函数。为了引入稀疏性，需要计算隐藏层神经元的平均激活值$\hat{\rho}_j$，使其接近于某个较小的稀疏目标，本文设隐藏层神经元的目标稀疏度$\rho=0.05$，$\hat{\rho}_j$的计算式为：

$$\hat{\rho}_j=\frac{1}{m}\sum_{i=1}^{m}h_j(x^{(i)}) \tag{2}$$

其中，m表示样本数量，$h_j(x^{(i)})$表示第i个样本输入时第j个隐藏层神经元的激活值，$\hat{\rho}_j$表示第j个隐藏单元的平均激活值。最终，编码器和解码器的损失函数分为重构损失和稀疏正则化两部分，这两部分的计算式为：

$$\begin{cases}\mathcal{L}_{\text{reconstruction}}=\|x-\hat{x}\|^2\\ \mathcal{L}_{\text{sparsity}}=\sum_{j=1}^{n}\left[\rho\ln\frac{\rho}{\hat{\rho}_j}+(1-\rho)\ln\frac{1-\rho}{1-\hat{\rho}_j}\right]\end{cases} \tag{3}$$

其中，n表示隐藏单元数量，$\rho=0.05$表示希望隐藏层神经元的平均激活值接近的目标稀疏程度。

在多视图机制下，为了保证同一样本在不同视图中潜在表示的一致性，本文引入了视图间对比学习模块。设样本x_i在第v个和第w个视图的潜在表示分别为$z_i^{(v)}$和$z_i^{(w)}$，视图间对比损失定义为：

$$\mathcal{L}_{\text{contrast}}=\frac{1}{n}\sum_{i=1}^{n}\sum_{v=1}^{V}\sum_{w\neq v}\left\| z_i^{(v)}-z_i^{(w)}\right\|^2 \tag{4}$$

通过拉近同一样本的潜在表示，同时间接拉远正常样本与异常样本的潜在分布，该模块增强了潜在空间的区分能力。

重输入模块进一步优化潜在空间的表示一致性和稳定性。给定样本x_i的重构结果$\hat{x}_i^{(v)}$，其潜在表示为$z_{\text{re}}^{(v)}=f_{\text{enc}}^{(v)}(\hat{x}_i^{(v)})$。通过对比输入样本与重构样本的潜在表示，重输入损失定义为：

$$\mathcal{L}_{\text{re-input}}=\frac{1}{n}\sum_{i=1}^{n}\sum_{v=1}^{V}\left\| z_i^{(v)}-z_{\text{re}}^{(v)}\right\|^2 \tag{5}$$

为优化潜在空间的一致性、稀疏性和重构质量，MCSAE的总损失函数由以下部分组成：

$$\begin{aligned}\mathcal{L}_{\text{total}}=&\mathcal{L}_{\text{reconstruction}}+\lambda_1\mathcal{L}_{\text{sparsity}}+\\&\lambda_2\mathcal{L}_{\text{contrast}}+\lambda_3\mathcal{L}_{\text{re-input}}\end{aligned} \tag{6}$$

其中，$\mathcal{L}_{\text{reconstruction}}$为重构损失，用于确保输入样本与重构结果的相似性，$\mathcal{L}_{\text{sparsity}}$为稀疏正则化，用于提升潜在表示的简洁性，$\mathcal{L}_{\text{contrast}}$为视图间对比损失，用于优化同一样本在不同视图下潜在表示的一致性，$\mathcal{L}_{\text{re-input}}$为重输入损失，用于增强潜在空间的鲁棒性，权重$\lambda_1=\lambda_2=\lambda_3=0.5$，用于平衡各部分损失。

1.2　数据增强步骤

伪异常样本的生成基于正常数据集中偏离聚类中心最远的样本，通过加权平均和距离筛选生成具有异常特征的新样本，具体步骤如下。

步骤 1　远距离样本的识别。首先，对正常数据执行聚类分析，获取全局质心作为正常分布的中心点。聚类使用*K*-means算法，其质心通过最小化所有样本与聚类中心的欧氏距离确定：

$$\text{centroid}=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{7}$$

其中，x_i为第i个正常样本，n为正常样本的总数。随后，计算每个样本到质心的欧氏距离d_i：

$$d_i=\left\| x_i-\text{centroid}\right\|_2=\sqrt{\sum_{j=1}^{d}(x_{ij}-\text{centroid}_j)^2} \tag{8}$$

其中，d为特征维度，x_{ij}为样本x_i的第j个特征。根据距离值排序，选取距离最大的前k个样本构成远距离样本子集$\{x_1',x_2',\cdots,x_k'\}$。

步骤 2　加权平均融合。在远距离样本子集的基础上，利用加权平均技术生成新的可能的异常样本。假设远距离样本子集为$\{x_1',x_2',\cdots,x_k'\}$，生成可能的异常样本的过程如下。

（1）随机选择m个远距离样本$\{x_1',x_2',\cdots,x_k'\}$进行融合。

（2）为每个选中样本分配权重$\alpha_i(i=1,2,\cdots,m)$，权重从预定义区间$[\alpha_{\min},\alpha_{\max}]$的均匀分布中随机采样。

（3）新样本x_{new}由选中样本的加权和生成：

$$x_{\text{new}}=\sum_{i=1}^{m}\alpha_i x_i' \tag{9}$$

其中，$\sum_{i=1}^{m}\alpha_i=1$。加权平均过程确保了新生成样本既继承了远距离样本的特征，又具有一定的随机性和多样性。

步骤 3　生成伪异常样本。生成可能的异常样本后，通过与正常数据质心的距离筛选真正具有异常特性的样本。设生成样本x_{new}的质心距离为：

$$d_{\text{new}}=\left\| x_{\text{new}}-\text{centroid}\right\|_2 \tag{10}$$

当$d_{\text{new}}>\tau$时，x_{new}被认为异常样本，其中τ为距离阈值，用于区分正常样本和异常样本。阈值$\tau=\text{Max}(\left\| x_{\text{normal}}-\text{centroid}\right\|_2)$表示正常样本到质心距离的最大值，确保筛选出的样本具有明显的异常特性。

2　分层抽样集成学习

2.1　分层抽样

为提升简单基分类器的训练效能，并缓解原始数据的类别不平衡问题，需要先对不平衡数据进行针对性预处理。

步骤1 初始化聚类中心。采用*K*-means++算法的初始化策略确定多数类（正常类）样本的初始聚类中心：从多数类样本中随机选择1个样本作为第一个簇中心，后续簇中心通过轮盘赌法从剩余样本中选取（距离已选中心越远的样本被选中的概率越高），最终确定k个初始聚类中心：

$$\{C_1, C_2, \cdots, C_k\} \tag{11}$$

其中，C_i表示第i个簇。

步骤2 样本分配至簇。计算多数类所有样本点到每个簇中心的欧氏距离，将每个样本点分配至距离最近的簇中，完成首轮聚类划分。对于每个簇C_i，计算中心点μ_i到每个样本点的距离，并按距离从近到远排序。

$$d_{i,j} = |x_j - \mu_i| \tag{12}$$

其中，x_j表示簇C_i中的第j个样本点，$d_{i,j}$表示样本点x_j到中心点μ_i的距离。

步骤3 迭代更新聚类结果。基于步骤2的分类结果，计算每个簇内所有样本的特征平均值，将其作为该簇的新中心；重复步骤2（重新计算样本到新中心的距离并分配类别）和本步骤（更新中心），直至簇中心位置收敛或达到最大迭代次数，最终得到稳定的k个簇。

步骤4 确定子集数量与划分子样本。计算训练集中正常类与异常类样本的数量比值x，取最接近的整数n作为平衡子集的数量。对每个簇内样本按到簇中心的距离由近及远排序，通过循环分配方式将排序后的样本划分为n个子样本集，确保每个子样本集包含数量相近的样本，且保留簇内特征分布特性。

$$n = [x] \tag{13}$$

将排序后的样本列表按循环分配的方法划分为n个子样本集$\{S_1, S_2, \cdots, S_n\}$，每个子样本集包含数量相近的样本点。

$$S_j = \left\{ x_{j+k\cdot n} | k = 0, 1, \cdots, \frac{|C_i|}{n} \right\} \tag{14}$$

其中，$j = 1, 2, \cdots, n$。

步骤5 构建平衡子集。依次将步骤4中得到的n个正常类样本子集与异常类样本组合起来，形成n个平衡的子集。每个平衡子集包含数量相近的正常类样本和异常类样本。

2.2 集成学习

为处理机载网络入侵检测中的不平衡数据问题，本文采用了改进分层抽样方法，将训练数据集划分为5个平衡子集，旨在保留正常类样本的原始特征空间，这保证了基分类器的准确性。鉴于机载网络数据集具有显著的时间关联性特征，本文针对性选取对时间序列数据处理能力较强的CNN、LSTM和RF模型作为集成学习的基学习器。

本文使用验证集评估每个基分类器的性能，计算其在验证集上的F1分数。F1分数是精确率（precision）和召回率（recall）的调和平均值。为了更好地融合多个分类器的预测结果，本文根据基分类器在验证集上的F1分数，对其进行加权。F1分数的计算式为：

$$\mathrm{F1} = \frac{2 \times \mathrm{precision} \times \mathrm{recall}}{\mathrm{precision} + \mathrm{recall}} \tag{15}$$

其中，$\mathrm{precision} = \dfrac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$，$\mathrm{recall} = \dfrac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$。本文引入惩罚加权策略，将每个基分类器的权重$w_i$设定为其F1分数的倒数，以便使性能差的分类器获得较小的权重。w_i的计算式为：

$$w_i = \frac{1}{\mathrm{F1}_i} \tag{16}$$

其中，$\mathrm{F1}_i$是第i个基分类器在验证集上的F1分数。基分类器在测试集上对每个类别的预测概率进行加权融合。假设第i个基分类器对样本x的类别j的预测概率为$P_{i,j}(x)$，则加权后的最终预测概率$P_j(x)$为：

$$P_j(x) = \frac{\sum_{i=1}^{M} w_i \cdot P_{i,j}(x)}{\sum_{i=1}^{M} w_i} \tag{17}$$

最终的分类结果是加权后预测概率最大的类别，即：

$$\hat{y}(x)=\text{argmax}_j P_j(x) \tag{18}$$

3　实验结果与分析

3.1　1553B 航空数据总线数据集

航空数据总线是机载网络中用于数据传输的重要通道，其中 MIL-STD-1553（1553B）航空数据总线广泛应用于航空电子和卫星平台中，其安全性直接影响飞行器的稳定运行。1553B 总线数据集由以色列本·古里安大学的研究人员在 2019 年创建，旨在模拟简化的飞行控制系统中采用的 MIL-STD-1553B 总线架构。该系统由一个总线控制器和多个远程终端组成，并通过模拟常规的非周期性通信来伪装潜在的恶意终端，从而实现对总线的攻击注入，生成了 3 组非顺序数据集和 3 组顺序数据集。

上述 1553B 的 3 组顺序数据集的分布见表 1，该数据集的主要挑战在于异常样本的缺失和数据分布的不平衡。训练数据集中完全没有异常样本，仅包含正常数据，这使得模型难以学习异常行为的特征；测试数据集虽然包含异常样本，但比例极低，3 组顺序数据集中异常样本的占比分别为 11%、1.26% 和 0.14%。这种情况下，传统机器学习方法对严重失衡的数据进行训练，容易过度关注正常样本，忽略异常样本特征，导致检测结果失真。针对机载网络 1553B 数据集异常样本缺失与数据分布严重失衡的问题，本文提出的方法是首先采用 MCSAE 方法进行异常样本的数据增强，再通过构建平衡子集开展入侵检测实验。

表 1　1553B 的 3 组顺序数据集的分布

数据集	训练集		测试集	
	正常样本	异常样本	正常样本	异常样本
数据集 1	1 278	0	13 664	1 690
数据集 2	3 029	0	14 945	190
数据集 3	6 013	0	14 289	20

3.2　检测结果比较

为证明所提方法的优越性，在机载网络 1553B 数据集 1 上与先进的异常检测方法进行比较，其入侵检测结果对比见表 2。实验采用精确率、召回率和 F1 分数作为模型性能的评价标准。

表 2　入侵检测结果对比

方法	精确率	召回率	F1 分数	运行时间/s
CNN	0.863	0.919	0.890	9.2
RF	0.922	0.897	0.909	11.3
LSTM	0.967	0.924	0.945	54.9
Genereux[17]	0.983	0.513	0.673	68.8
He[20]	0.958	0.708	0.816	56.4
BO-TPE[14]	0.972	0.954	0.968	70.6
WKG[21]	0.986	0.970	0.978	80.4
本文方法	0.989	0.976	0.982	61.5

不同方法的性能对比如图 2 所示。由表 2 和图 2 可知，CNN、RF 和 LSTM 作为本文所提方法的基学习器，单独应用在机载 1553B 数据总线中的入侵检测存在显著局限性，主要体现在未充分考虑数据不平衡性，导致模型对少数类异常样本的检测能力不足，表现为召回率较低、F1 分数偏低。Genereux 方法尽管精确率较高，但其依赖于数据包的时间特性，在面对复杂的多类别入侵行为时难以捕捉异常模式，召回率不足 0.6，且 F1 分数也较低，这表明该方法无法有效识别多样化的入侵行为，仅适用于入侵模式固定、异常特征单一的场景。He 方法虽将精确率提升至 0.958，但召回率仅为 0.708，说明该方法对异常样本的识别存在严重不足，容易忽略实际入侵事件，在入侵行为多样化和复杂化的机载环境下存在重大风险。在运行时间方面，本文方法与最新机载方法（WKG 和 BO-TPE 方法）相比，运行时长并没有增加。最新提出的 WKG 和 BO-TPE 方法在各项指标方面都表现优异，但由于算法复杂程度明显提高，检测时间较长。

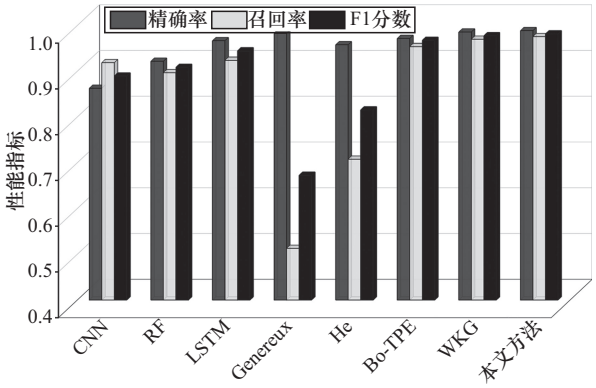

图2　不同方法的性能对比

与上述方法相比，本文提出的集合MCSAE的数据增强方法和分层抽样的集成学习方法在处理不平衡数据时，综合考虑了数据的全局特征和局部边界，通过数据增强扩充少数类有效样本量，配合改进分层抽样确保各类别特征的充分学习，既避免了随机过采样引入的噪声和虚假样本，又增强了模型对少数类的识别基础。同时，采用F1分数自适应加权策略平衡了各基分类器对多数类与少数类的学习偏差，缓解了模型对少数类的忽略问题。由于自适应加权能够根据类别复杂度调整分类器的贡献，本文方法在提高召回率的同时，保持了高精确率，最终在F1分数方面显著优于其他方法，达到了精确率与召回率的理想平衡。本文方法不仅能够准确捕捉多样化的异常入侵行为，同时避免了过采样引入的误分类问题，具有更强的泛化能力和适应性。

3.3　类簇数的确定

在*K*-means++算法中，类簇数对聚类效果影响很大，本文对训练集中的正常样本使用不同的类簇数进行实验，使用轮廓系数来评估聚类效果，以选取最好的聚类效果来进行后续实验。轮廓系数随类簇数的变化情况见表3。

根据轮廓系数确定最优类簇数k，由表3可知，当k=4时，轮廓系数最大，因此，令k为4。本文使用*K*-means++算法将训练集中的正常样本聚为4类，使用*T*分布随机邻域嵌入（T-distributed stochastic neighbor embedding，TSNE）进行降维可视化。类簇数为4时正常样本的聚类可视化结果如图3所示。由图3可知，类簇数为4时，正常样本的聚类结果较为均衡，效果良好。

表3　轮廓系数随类簇数的变化情况

k	轮廓系数
2	0.334
3	0.334
4	0.386
5	0.301
6	0.260
7	0.246
8	0.228
9	0.237
10	0.250

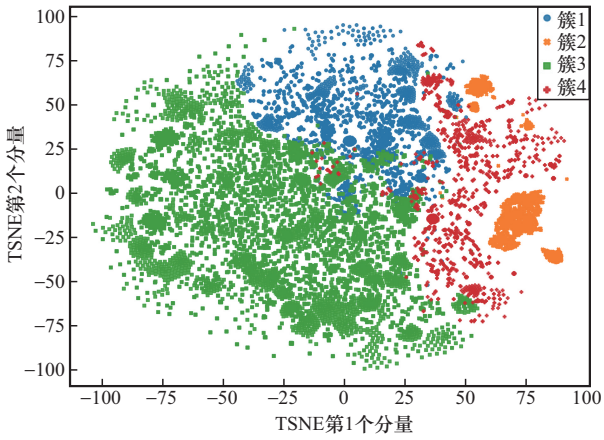

图3　类簇数为4时正常样本的聚类可视化结果

3.4　消融实验

消融实验旨在从所提模型的最佳表现出发，通过逐步移除模型的新增模块，观察各评价指标的变化，以评估每个组件对整体性能的贡献。消融实验结果见表4。其中，ME为MCSAE与集成学习的入侵检测方法；SE为分层抽样与集成学习的入侵检测方法；MS为MCSAE与分层抽样的入侵检测方法；MSE为MCSAE与SSEL方法集成过程中不使用F1分数加权策略的入侵检测方法。

表4　消融实验结果

方法	精确率	召回率	F1 分数
ME	0.860	0.842	0.851
SE	0.754	0.724	0.739
MS	0.873	0.857	0.865
MSE	0.875	0.860	0.868
本文方法	0.989	0.976	0.982

由表4可知，在数据集1上，ME方法与本文方法相比，其召回率和F1分数明显更低，说明MCSAE数据增强模块为集成模型提供了更优质的特征输入，优于传统过采样。SE方法的性能也低于本文方法，说明MCSAE生成的增强样本优于随机过采样，数据增强策略对于样本缺失具有重要的作用。MS方法没有集成学习机制的作用，其稳定性和泛化能力弱于本文方法，表明CNN、RF和LSTM这3种模型集成能弥补单一模型缺陷。MSE方法没有使用自适应加权模块，其F1分数下降，说明动态加权策略对平衡基学习器偏差具有重要作用，F1分数自适应加权模块成功平衡了CNN、RF、LSTM集成学习的检测偏差，优化了集成结果。

4　结束语

针对机载网络中普遍存在的异常样本缺失与数据不平衡难题，本文提出的融合MCSAE与改进分层抽样集成学习的异常检测方案，形成了“样本增强–特征学习–集成优化”的解决方案。实验结果验证了该方案的有效性，在1553B总线数据集上，所提方法不仅实现了对异常样本的高检测率，更通过特征学习与集成优化的协同作用显著降低了误报率，能够精准区分恶意流量与正常流量，为航空总线系统的异常检测提供了一种鲁棒性强、性能优越的新思路。后续研究将围绕两大方向改进：一是在保障检测准确率不显著下降的前提下，通过模型剪枝、参数量化或轻量化网络结构设计，降低MCSAE模型的计算复杂度与参数量；二是结合机载网络数据的时序特性与轻量化目标，探索将模型与高效特征提取模块（如注意力机制简化版、轻量化卷积单元等）结合，进一步提升入侵检测的实时响应效率，以更好地适配机载系统资源受限、低时延的应用需求。

参考文献：

[1] De Santo D, Malavenda C S, Romano S P, et al. Exploiting the MIL-STD-1553 avionic data bus with an active cyber device[J]. Computers & Security, 2021, 100: 102097.

[2] Hayaeian Shirvan M, Moattar M H, Hosseinzadeh M. Deep generative approaches for oversampling in imbalanced data classification problems: a comprehensive review and comparative analysis[J]. Applied Soft Computing, 2025, 170: 112677.

[3] Mujahid M, KıNa E, Rustam F, et al. Data oversampling and imbalanced datasets: an investigation of performance for machine learning and feature engineering[J]. Journal of Big Data, 2024, 11(1): 87.

[4] Yang Y Q, Zheng K F, Wu C H, et al. Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network[J]. Sensors, 2019, 19(11): 2528.

[5] Jo W, Kim D. OBGAN: Minority oversampling near borderline with generative adversarial networks[J]. Expert Systems with Applications, 2022, 197: 116694.

[6] Dayan O, Wolf L, Wang F, et al. Optimizing AI for mobile malware detection by self-built-dataset GAN oversampling and LGBM[C]//Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR). Piscataway: IEEE Press, 2023: 60-65.

[7] Zhang Y L, Liu Y C, Wang Y, et al. An ensemble oversampling method for imbalanced classification with prior knowledge via generative adversarial network[J]. Chemometrics and Intelligent Laboratory Systems, 2023, 235: 104775.

[8] Kim J, Kim J, Kim H, et al. CNN-based network intrusion detection against denial-of-service attacks[J]. Electronics, 2020, 9(6): 916.

[9] Imrana Y, Xiang Y P, Ali L, et al. A bidirectional LSTM deep learning approach for intrusion detection[J]. Expert Systems with Applications, 2021, 185: 115524.

[10] Wali S, Ali Farrukh Y, Khan I. Explainable AI and random for-

est based reliable intrusion detection system[J]. Computers & Security, 2025, 157: 104542.

[11] Li H, Ge H J, Sang Y Q, et al. An optimized multi-layer ensemble model for airborne networks intrusion detection[J]. Applied Soft Computing, 2024, 167: 112282.

[12] Le T T H, Shin Y, Kim M, et al. Towards unbalanced multiclass intrusion detection with hybrid sampling methods and ensemble classification[J]. Applied Soft Computing, 2024, 157: 111517.

[13] Elsayed M A, Wrana M, Mansour Z, et al. AdaptIDS: adaptive intrusion detection for mission-critical aerospace vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 23459-23473.

[14] Li H, Sang Y Q, Ge H J, et al. Anomaly detection of aviation data bus based on SAE and IMD[J]. Computers & Security, 2024, 137: 103619.

[15] 张重生, 陈杰, 李岐龙, 等. 深度对比学习综述[J]. 自动化学报, 2023, 49(1): 15-39.
Zhang C S, Chen J, Li Q L, et al. Deep contrastive learning: a survey[J]. Acta Automatica Sinica, 2023, 49(1): 15-39.

[16] Ahmed H, Traore I, Quinan P, et al. A collection of datasets for intrusion detection in MIL-STD-1553 platforms[M]//Artificial Intelligence for Cyber-Physical Systems Hardening. Cham: Springer International Publishing, 2023: 81-100.

[17] Généreux S J J, Lai A K H, Fowles C O, et al. MAIDENS: MIL-STD-1553 anomaly-based intrusion detection system using time-based histogram comparison[J]. IEEE Transactions on Aerospace and Electronic Systems, 2020, 56(1): 276-284.

[18] 刘文琪, 胡涛, 闫洁, 等. 基于DeepInsight和迁移学习的入侵检测技术[J]. 工程科学学报, 2024, 46(12): 2238-2245.
Liu W Q, Hu T, Yan J, et al. Network intrusion detection technology based on DeepInsight and transfer learning[J]. Chinese Journal of Engineering, 2024, 46(12): 2238-2245.

[19] Zhou M H, Li Y J, Cao Y Y, et al. Physics-informed spatio-temporal hybrid neural networks for predicting remaining useful life in aircraft engine[J]. Reliability Engineering & System Safety, 2025, 256: 110685.

[20] He D J, Liu X X, Zheng J J, et al. A lightweight and intelligent intrusion detection system for integrated electronic systems[J]. IEEE Network, 2020, 34(4): 173-179.

[21] Liu W Q, Li S J, Gao C, et al. An adaptive graph neural network-based intrusion detection system for airborne network[J]. Engineering Applications of Artificial Intelligence, 2025, 152: 110851.

[作者简介]

周茂辉（1996–），男，南京航空航天大学民航学院博士生，主要研究方向为航空器机电系统测试性设计与验证、航空器故障智能诊断、航空安全等。

刘文琪（1997–），女，南京航空航天大学民航学院博士生，主要研究方向为航空器机载网络入侵检测、航空安全等。

李艳军（1969–），男，南京航空航天大学民航学院教授、博士生导师，主要研究方向为航空器故障诊断与健康监测、适航审定及验证技术、飞机改装设计及适航审定、航空维修工程及管理。

宫艺姝（1993–），女，新疆通达低空科技有限公司科创副总经理，主要研究方向为低空起降安全、低空气象探测与预警。