无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法

尹梓诺[①] 陈鸿昶[①] 马海龙[①②] 胡 涛[*①] 白禄鑫[①]

[①](信息工程大学信息技术研究所 郑州 450001)

[②](网络空间安全教育部重点实验室 郑州 450001)

摘 要：针对基于传统机器学习的网络流量异常检测方法受流量数据类别不平衡的影响检测性能较差的问题，该文提出一种无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法。首先，设计基于K-medoids的自适应小样本抽样算法(KAFS)，利用无监督聚类对各类流量动态自适应地抽取更具代表性的少量样本，使正常和攻击流量均衡，提高训练小样本学习模型的数据质量。然后，构建具有鲁棒损失函数的孪生多层感知机(SMLP)模型用于流量异常检测，该模型利用两个相同结构的多层感知机对训练集中的成对流量样本进行训练，捕捉跨流量特征的非线性关系，学习流量数据的异同，进一步提高对攻击流量的分类精度。实验结果表明，所提方法在CICIDS2017和CICIDS2018数据集上的检测准确率分别可达99.80%和98.26%。与其他方法相比，该方法对未知攻击的检出率分别提高了至少2.85%和1.73%，有效提升流量异常检测性能。

关键词：网络流量异常检测；类别不平衡；自适应抽样；孪生多层感知机

中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2025)07-2211-14

DOI: 10.11999/JEIT241115 **CSTR**: 32379.14.JEIT241115

1 引言

随着信息技术的进步，网络攻击等安全威胁不断增加。新型攻击和零日攻击的出现，给网络和信息系统带来了额外的安全风险。无论个人用户、企业还是政府组织都面临着日益增加和越发复杂的网络威胁。黑客通过各种手段寻找和利用网络系统中的漏洞，造成了重大的经济和安全风险。

面对攻击等安全威胁，网络流量异常检测引起研究人员的广泛关注，它通过监控和分析网络流量数据，及时发现潜在攻击或异常行为[1]，使网络管理员能够在网络和设备受到威胁前及时采取安全措施。当前网络中流量数据量呈指数级增长[2]，为人工智能的应用提供了沃土[3]。基于人工智能的流量异常检测研究[4–8]逐渐成为研究热点。传统机器学习(Machine Learning, ML)技术[9]等，更多依赖于特征选择。深度学习(Deep Learning, DL)[10]具有从大量输入流量数据中学习强大的高级潜在特征表示的优势。

然而，传统ML和DL技术的检测性能依赖于广泛且标记良好的可靠数据集[11]。在网络环境中，良性流量样本充足、易于采集，且子类型多样。带有攻击等恶意企图的异常流量所占的比例相对较小，且难以获得新的攻击流量。如果将不平衡流量直接输入到传统的深度学习模型中进行训练，会导致过拟合问题，难以有效检测出恶意流量[12]。此外，如果构建攻击流量充足且标记完整的可靠数据集，需要花费大量的时间、人力和资源。即使安全专家构建了符合标准的数据集，所消耗的时间也可能导致一些攻击策略过时，出现新的攻击流量。为了解决这一问题，部分研究使用数据增强技术[13–16]缓解数据的不平衡。然而，数据增强可能会在流量数据中引入噪声，影响训练效果。

小样本学习主要通过元学习模型进行预训练[17]，或通过生成模型增加数据样本[18]，或通过度量学习来测量样本间的相似性[19]等手段实现基于少量样本取得较好分类效果。它克服数据稀缺性的挑战，在计算机视觉等领域取得了重大的研究进展[20–22]。但其在网络流量异常检测中适应性和检测性能还有待改进和提高。受小样本学习中的度量学习技术的启发，该文将孪生网络应用于网络流量异常检测中，以缓解类不平衡问题的影响。但在孪生网络训练过程中，如果训练集中每类流量的多样性不足，模型可能无法捕捉到不同类间的特征差异，从而影响其检测性能。

针对上述问题，本文提出了一种无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法。首先设计了一种基于K-medoids的自适应小样本抽样(K-medoids-based Adaptive Few-shot

收稿日期：2024-12-19；改回日期：2025-05-14；网络出版：2025-06-03

*通信作者： 胡涛 hutaondsc@163.com

基金项目：雄安新区科技创新专项 (2022XAGG0111)，国家自然科学基金(62176264)

Foundation Items: Xiong'an New Area Science and Technology Innovation Special Project (2022XAGG0111), The National Natural Science Foundation of China (62176264)

Sampling, KAFS)算法。根据每类流量数据的特征分布，无监督自适应地将其划分为多个子类，并从中提取少量但具有代表性的流量样本用于训练。然后，构造了一个具有鲁棒损失函数的孪生多层感知机 (Siamese Multi-Layer Perceptron, SMLP)，并使用小样本流量训练集对其进行训练。该模型从流量特征数据中提取细微模式，实现有效流量异常检测。本文的主要贡献总结如下：

(1) 首先，对网络流量数据分析，评估流量统计特征在检测网络异常流量方面的有效性，为智能流量异常检测方法的开发提供了解释和见解。

(2) 提出了KAFS算法。根据每类流量中可能存在的多个子类，自适应地从每类流量中抽取具有代表性的少量流量构建小样本训练集，使各类别流量均衡，使后续模型能够有效对每类流量进行学习，避免向正常类倾斜。

(3) 设计了一种基于SMLP的流量异常检测模型。在该模型中构造了鲁棒损失函数，通过结合多层感知机(Multi-Layer Perceptron, MLP)编码损失和根据锚样本与正常或恶意流量样本间的距离计算的预测损失，提高对攻击流量检测的有效性。

(4) 实验表明，在只训练少量流量的情况下，本文方法在CICIDS2017和CICIDS2018数据集[23]上的检测准确率分别可达99.80%和98.26%。

2 研究动机

本节分析网络流量统计特征，从数据特征的角度解释流量数据对网络流量异常检测的有效性。

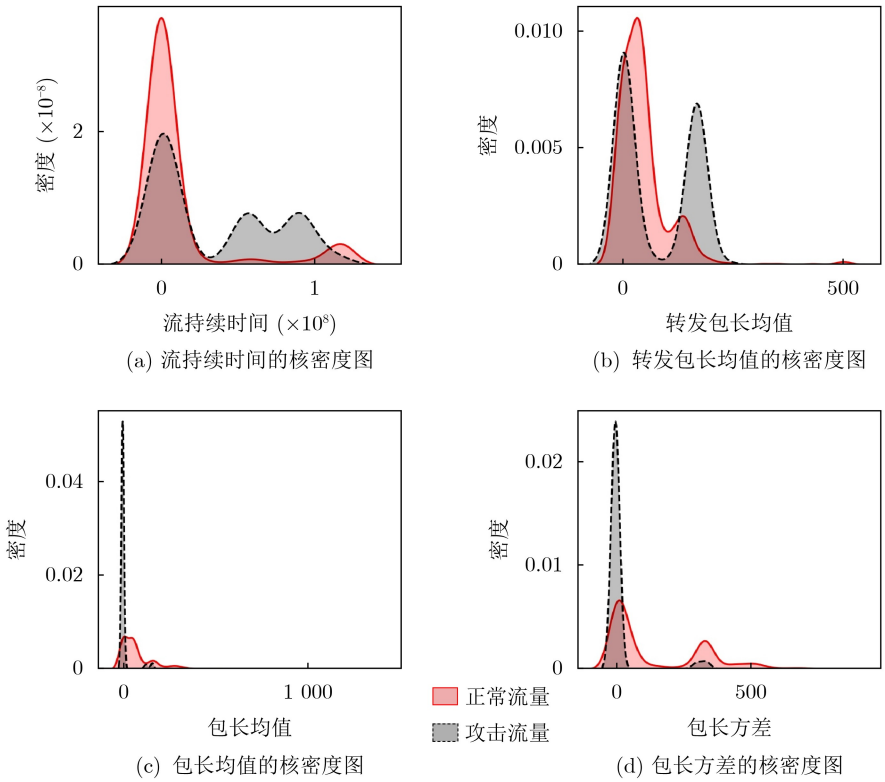
CICIDS2017和CICIDS2018数据集是全面且公开可用的流量异常检测数据集。这两个数据集涵盖了广泛的攻击类型，被认为具有代表性和多样性。本文选择这两个数据集主要包含以下3方面原因：

(1) 为了进行实验验证和评估，基准数据集必须被正确标注；

(2) DARPA1998和KDD CUP99等数据集过于陈旧，其中的攻击数据可能不适用于当前的网络环境；

(3) 为了使检测结果和分析更有说服力，基准数据集需要具备攻击多样性。

为了理解良性流量和攻击流量的差异，本节对网络流量统计特征的分布进行分析。核密度估计图用于绘制流量特征值的分布。图1和图2给出了两个数据集的流持续时间、转发数据包的平均大小、数据包长度的均值和标准差的核密度分布，其中红色部分对应正常流量特征，黑色部分对应恶意流量特征。核密度图显示了流量统计特征的概率密度函数的估计。如图1(a)和图2(a)所示，流持续时间是区分恶意流量和正常流量的一种重要特征。恶意流量的持续时间相对平均，比正常流量的持续时间长。由于网络中的正常流量主要用于一些信息交互等功



(a) 流持续时间的核密度图 (b) 转发包长均值的核密度图

(c) 包长均值的核密度图 (d) 包长方差的核密度图

图 1 CICIDS2017数据集中正常流量和攻击流量的4种典型特征的核密度图

能，因此可能会话时间相对较短，而恶意流量则可能倾向于发送和接收大量数据。正常软件产生的转发流量比恶意软件产生的具有恶意企图的转发流量少得多。因此，如图1(b)和图2(b)所示，在转发数据包的均值方面，正常流量相对于异常流量的分布重心偏左。图1和图2还绘制了数据包长度分布的均值和标准差的分布。如图1(c)和图2(c)所示，正常流量没有特定的数据包长，其均值分布可能更加分散。如图1(d)和图2(d)所示，攻击流的数据包长度更加一致和集中，标准差更小。事实上，本文已经对78维特征进行了全面的分析。但由于篇幅限制，本文仅选取部分关键特征进行相关分析。

综上所述，正常和攻击流量在统计特征上存在明显差异。因此，可以利用这些流量统计特征数据构建的特征向量来训练相应的检测模型。通过训练，模型能够区分正常流量和恶意流量，有效检测异常流量。

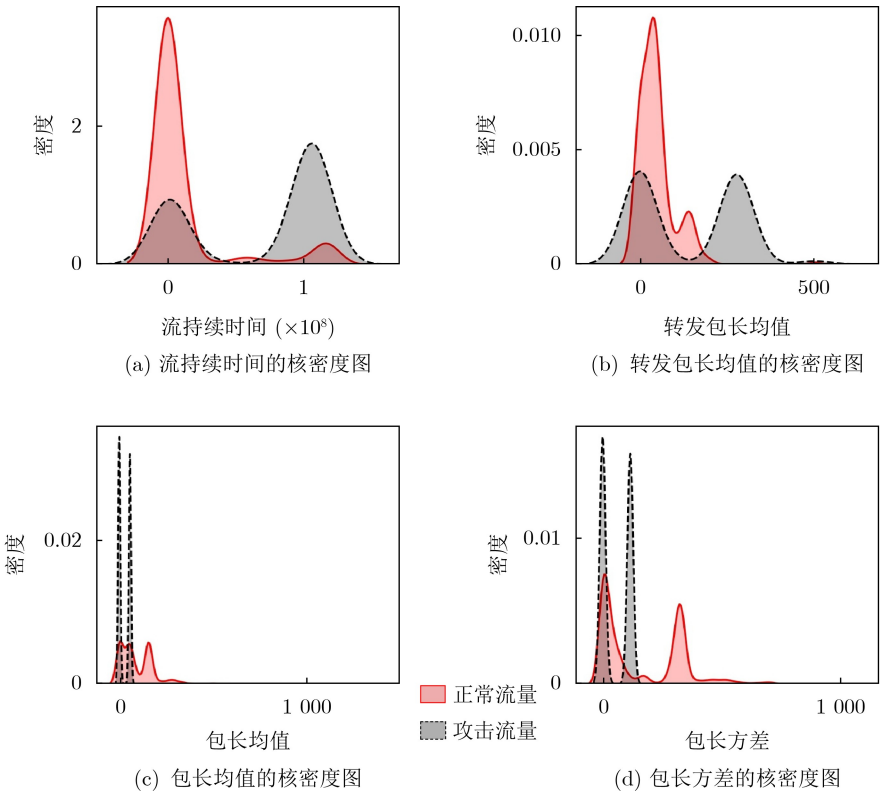
3　无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法

本节概述了无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法并介绍算法及模型实现。

3.1　总体概述

无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法的主要任务是基于少量具有代表性的流量样本检测网络中的恶意流量。该方法的结构如图3所示，其中包括两个关键部分：基于K-medoids的自适应小样本抽样算法和基于SMLP的流量异常检测模型。

所提方法的工作过程如下：在初始阶段，设计了一种基于K-medoids的自适应小样本抽样算法，以无监督的方式自适应地对正常和攻击流量样本抽样，为每类流量构造数量少且具有代表性的训练集。然后，将少量的正常和攻击流量样本共同组成的训练集输入孪生多层感知机中进行训练。计算特



(a) 流持续时间的核密度图　(b) 转发包长均值的核密度图

(c) 包长均值的核密度图　(d) 包长方差的核密度图

图 2 CICIDS2018数据集中正常流量和攻击流量的4种典型特征的核密度图

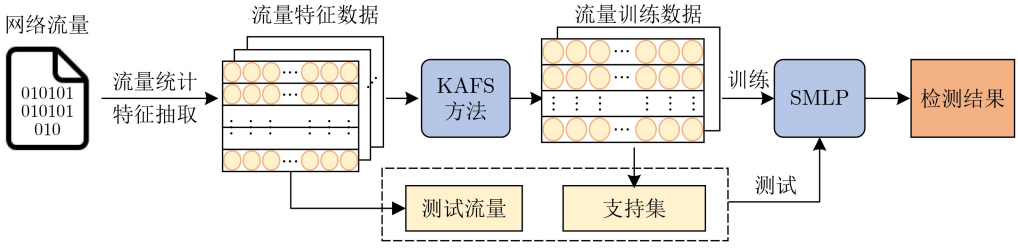


图 3 无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法的结构

征向量低维表示之间的距离，缩小同类流量样本低维向量表示间的距离，放大不同类流量样本低维向量表示间的距离，得到有效的检测模型来识别攻击流量样本。在测试阶段，将支持集和测试集输入模型。该模型计算流量测试样本的特征嵌入后，利用支持集中最相似的样本来识别待测样本的类别，从而识别恶意流量。

3.2 KAFS算法

为了平衡不同类别的数据，有必要从准确标记的原始流量数据中精确提取少部分有代表性的样本进行小样本学习。对于小样本流量训练集的构建，每个类别的训练样本数M是关键。通常情况下，M值固定且相同。但对于流量异常检测中的流量数据，若M值太低，算法会对样本量较多的正常流量学习不充分，造成过拟合；若M值太高，新的攻击类型数据量较少，其子类样本数量过少，不满足M需求。

根据第2节对流量特征的分析可以发现，网络中的正常流量由于功能和目的的不同，在连接特征、数据包大小的统计特征等方面有所不同，并且可能存在一些子类。同一攻击类数据可能会为了伪装成正常流量，在流量统计特征方面，表现出一些差异。如果对所有类别的流量数据提取相同数量的样本，则每一类流量数据的梯度对神经网络模型的权重和其他参数更新的贡献趋于相似，导致模型更倾向于学习在所有类别中均表现良好的特征表示，而忽略某些类别的特定特征。因此，在创建网络流量的小样本训练集时，为具有大量样本的类别构建可靠采样策略非常重要。此策略应考虑到流量的特征特点，以确保提取的样本代表该类别中的每个子类。

对于不同类别的流量样本，本文设计了一种基于K-medoids的自适应小样本抽样算法，其过程如图4所示。以对正常流量数据抽样为例，利用K-medoids算法对正常流量数据样本进行无监督聚类，产生多个子类。随后，从每个子类中随机抽取一个样本，形成正常流量的小样本训练集，用于模型训练。在K-medoids聚类过程中，子类的数量M至关重要。M不仅是子类的数量，也是每类样本的训练数据量。为确定M，本文利用聚类评价指标-CH指标(Calinski-Harabaz Index)来对聚类效果进行分析，选择聚类效果最优的M。CH指标的公式为

$$S(M)=\frac{\mathrm{Tr}(B_k)}{\mathrm{Tr}(W_k)}\cdot\frac{N-M}{M-1} \tag{1}$$

其中，N为待聚类的样本数，$\mathrm{Tr}(W_k)$表示所有簇的簇内距离平方和，$\mathrm{Tr}(B_k)$表示所有簇中心到全局簇中心距离平方加权和。S的取值范围是$(0,+\infty)$，S越大聚类效果越好。多次聚类后，确定M值如式(2)所示：

$$M=\min\{\arg\max_n\{S(2),S(3),\cdots,S(i)\}\} \tag{2}$$

其中，$\arg\max_n$表示最大的前n个CH值所对应的簇数。对于每类流量，需要提取多个样本，所以聚类数从2开始。得到M值后，从每个簇中随机抽取1个样本作为训练数据。对正常和攻击类流量重复上述抽样过程，最终构成一个全面覆盖所有流量类的训练集。

3.3 基于SMLP的流量异常检测模型

流量异常检测任务可以被抽象为对正常和攻击流量的分类任务。传统神经网络分类模型对各类流量的样本量要求很高。度量学习模型可以使神经网络学习识别不同类流量间的差异。孪生网络是度量学习模型的典型代表。它只需要少量的数据进行训练，并且对数据不平衡具有更强的鲁棒性，不易被干扰。因此，对于流量异常检测任务，可以在孪生网络架构下构建合适的神经网络，使模型仅学习少量的流量数据就能学会度量样本之间的异同，从而获得良好的检测性能。因此，本文构建SMLP模型，其结构如图5所示。

不同于传统神经网络分类模型直接输出对输入流量样本所属类别的预测结果，本文模型利用输入流量样本的特征嵌入输出流量样本间的距离。因此，更善于学习流量样本间的相似性和差异性。MLP通过训练权值参数来学习非线性函数。不同于其他神经网络，如卷积神经网络(Convolutional

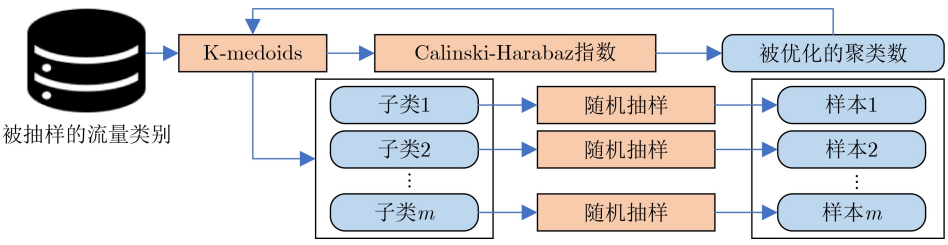


图 4 KAFS算法

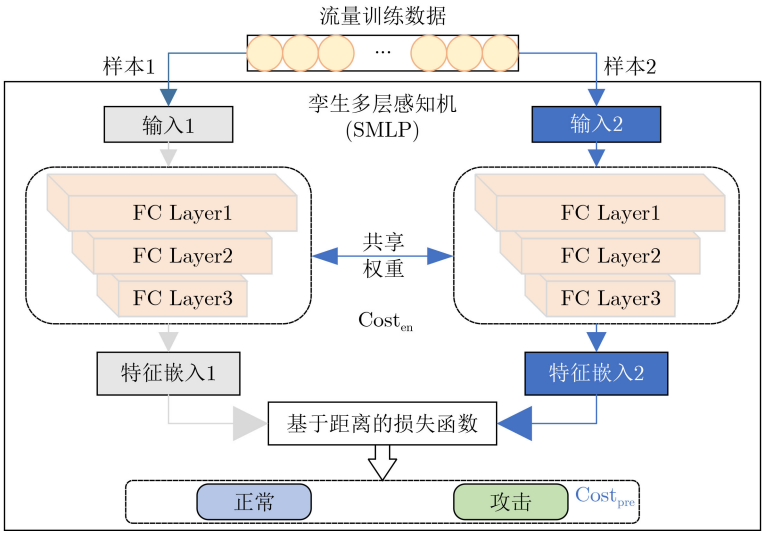


图 5 SMLP模型

Neural Network, CNN)关注局部特征提取，长短期记忆网络(Long Short-Term Memory Network, LSTM)关注样本间前后的时序关系，MLP更多关注不同特征间的关系，更适合学习小样本流量数据特征间的非线性关系。而且其具有较好的泛化能力，能较好适应新数据，因此在孪生网络架构中引入MLP。在MLP中主要使用全连接层，并引入dropout层减少过拟合。在训练中，将一对输入流量样本分别输入到两个相同的MLP中，通过多层神经网络，将流量特征数据转化为低维深度表示，然后计算这对流量特征嵌入间的距离，对同类流量，不断缩短其特征嵌入间的距离，对不同类别流量，不断扩大其特征嵌入间的距离。

具体来说，将给定流量样本$\boldsymbol{x}_i$作为一个输入样本，MLP对其提取特征嵌入的公式为

$$f(\boldsymbol{x}_i)=\mathrm{MLP}(\boldsymbol{x}_i,\boldsymbol{r}_\mathrm{e}) \tag{3}$$

其中，$\boldsymbol{r}_\mathrm{e}$为MLP的编码参数。

利用欧氏距离定义两个输入流量样本$\boldsymbol{x}_i$和$\boldsymbol{x}_k$的高层特征嵌入间的距离，其公式为

$$D(f(\boldsymbol{x}_i),f(\boldsymbol{x}_k))=\|f(\boldsymbol{x}_i)-f(\boldsymbol{x}_k)\|^2 \tag{4}$$

最后，该模型的输出基于全连接层softmax函数，其公式为

$$\mathrm{Output}(\boldsymbol{x}_i,\boldsymbol{x}_k)=\mathrm{Softmax}(\mathrm{FC}(D(f(\boldsymbol{x}_i),f(\boldsymbol{x}_k)))) \tag{5}$$

其中，softmax为激活函数，$\mathrm{Output}(\boldsymbol{x}_i,\boldsymbol{x}_k)$表示是否$\boldsymbol{x}_i$和$\boldsymbol{x}_k$属于同一类。

为提高对恶意流量的检测准确率，降低误报率，需要设计有效的损失函数。在损失函数设计中，本文将其分为两部分：在多层感知机编码过程中，产生了编码损失$\mathrm{Cost}_\mathrm{en}$；在距离度量部分，查询样本、正常样本和恶意样本之间的损失产生了预测损失$\mathrm{Cost}_\mathrm{pre}$。

利用MLP编码的损失来衡量孪生网络内部是否丢失关键信息。由于很难直接观察到编码过程的信息损失。相对熵可以基于理论和真实分布来量化信息损失。因此，对于输入流量特征样本$\boldsymbol{x}_i$的概率分布，通过保持原始特征的关键信息，同时最小化特征嵌入的数量来量化编码损失。编码损失的计算为

$$\mathrm{Cost}_\mathrm{en}=E\left[\sum_{\boldsymbol{x}_i}p(\boldsymbol{x}_i|f(\boldsymbol{x}_i))\log\left(\frac{p(\boldsymbol{x}_i|f(\boldsymbol{x}_i))}{q(\boldsymbol{x}_i|f(\boldsymbol{x}_i))}\right)\right] \tag{6}$$

其中，$p(\boldsymbol{x}_i|f(\boldsymbol{x}_i))$表示流量样本数据的真实分布，$q(\boldsymbol{x}_i|f(\boldsymbol{x}_i))$表示理论分布。

使用目标样本与正常流量样本和恶意流量样本间的距离来衡量孪生网络的预测损失，如式(7)所示

$$\begin{aligned}\mathrm{Cost}_\mathrm{pre}=\max\big(&\left(D\left(f\left(\boldsymbol{x}_i^\mathrm{t}\right),f\left(\boldsymbol{x}_i^\mathrm{a}\right)\right)\right.\\&\left.-D\left(f\left(\boldsymbol{x}_i^\mathrm{t}\right),f\left(\boldsymbol{x}_i^i\right)\right)+\lambda\right),0\big)\end{aligned} \tag{7}$$

其中，$\boldsymbol{x}_i^\mathrm{t},\boldsymbol{x}_i^\mathrm{a},\boldsymbol{x}_i^\mathrm{b}$分别表示目标流量样本、攻击流量样本和正常流量样本。$\lambda\in(0,1)$用于改善流量异常检测中的误报率的参数。在训练过程中通常$\lambda>0.5$。不断最大化损失函数$\mathrm{Cost}_\mathrm{pre}\le 0$。

为训练该模型，将上述两个损失函数集成计算，得到SMLP模型的整体损失，如式(8)所示

$$\mathrm{Loss}=\alpha\mathrm{Cost}_\mathrm{en}+\mathrm{Cost}_\mathrm{pre} \tag{8}$$

其中，α是调节编码损失的平衡系数。

该模型的训练过程包含特征编码和距离比较两步。在每个训练episode中，首先通过MLP将选取的目标样本$\boldsymbol{x}_k^\mathrm{t}$，攻击流量样本$\boldsymbol{x}_k^\mathrm{a}$和正常流量样本$\boldsymbol{x}_k^\mathrm{b}$编码为特征嵌入$f(\boldsymbol{x}_k^\mathrm{t}),f(\boldsymbol{x}_k^\mathrm{a}),f(\boldsymbol{x}_k^\mathrm{b})$。整个过程中的

损失函数根据式(6)–式(8)计算。通过不断最小化模型的总损失确定模型参数。

4 实验分析

4.1 实验设置和评估指标

为进行性能评估，实验环境设置为：Windows 10 操作系统、32 GB RAM的Intel(R) Core(TM) i7-8700 CPU, NVIDIA GeForce RTX 2060 GPU，使用Python3.7和TensorFlow实现算法。

在实验中，本文选择CICIDS2017和CICIDS2018作为基准数据集来评估所提方法和其他基线模型的性能。在这两个数据集中，正常流量可以达到数百万，而攻击类流量的最小数量只有几十条。不难发现，数据集中存在着严重的类别不平衡。CICIDS2017和CICIDS2018数据集均包含14种攻击，且其样本冗余。为方便实验，本文进行一定程度的过滤。对于CICIDS2017，使用15%的良性流量进行实验。同时，选择了表1所示的DDoS, DoS GoldenEye等6种攻击类型作为已知的攻击类型，将剩余的8种攻击作为未知攻击流量。与CICIDS2017相比，CICIDS2018更为复杂，数据量更大，因此抽取数据集中10%的数据进行实验。对于CICIDS-2018，选择Bot, Bruteforce等4种攻击大类作为已知攻击。将其余的DDOS attack-HOIC等5种子攻击作为未知攻击。采用KAFS算法采样后，训练数据的分布如表1和表2所示。

3.3节的SMLP的结构中各隐藏层节点数分别为1024-128-64，前两个隐藏层后接Dropout层，dropout rate为0.1。SMLP的性能可能受到超参数的影响，为了获得最佳的分类效果，使用网格搜索方法寻找最佳的超参数值。在测试阶段，进行了10倍交叉验证，以确保设置的超参数不受异常值的影响。SMLP在CICIDS2017和CICIDS2018上的损失值变化如图6所示。对于CICIDS2017和CICIDS2018，模型的损失值在前80次迭代中迅速下降。经过80～100次迭代后，损耗值趋于稳定。因此，本文将epoch设置为100，用于后续实验。同时设置batch-size为128，学习率为0.01。

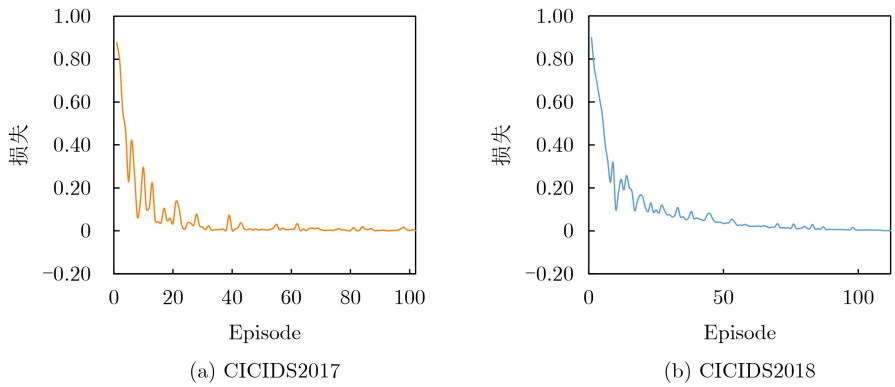
在量化分类模型的性能时，选择最广泛使用的评价指标，准确率、检出率、精确率和F1-score。准确率(Accuracy)为正确预测样本数与样本总数之比，用来量化模型准确检测的能力。检出率(Detection Rate, DR)为实际攻击类中被模型正确检测为攻击类的比例，用来量化模型正确检测攻击类的能力。精确率(Precision)为预测正确的攻击样本数与预测为攻击的总样本数之比。F1-score为Precision和DR的谐波平均值，是一种综合考虑检出率和精确率的评估指标。上述评估指标如式(9)所示

表 1 CICIDS2017数据集训练数据分布

类别	正常流量	攻击流量					
类型	正常流量	DDoS	DoS GoldenEye	PortScan	Bot	FTP-Patator	SSH-Patator
样本量	43	32	17	25	16	24	20

表 2 CICIDS2018数据集训练数据分布

类别	正常流量	攻击流量			
类型	正常流量	Bot	Brutefoce	DoS	Infiltration
样本量	29	42	12	25	20



(a) CICIDS2017 (b) CICIDS2018

图 6 SMLP模型在CICIDS2017和CICIDS2018数据集上的损失曲线

$$\left.\begin{aligned}
&\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}}\\
&\text{DR} = \frac{\text{TP}}{\text{TP}+\text{FN}}\\
&\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}}\\
&\text{F1-score} = \frac{2\times\text{precision}\times\text{DR}}{\text{precision}+\text{DR}}
\end{aligned}\right\} \tag{9}$$

其中，TP为正确识别为异常流量的样本数量；TN为正确识别为正常流量的样本数量；FP为错误识别为异常流量的正常流量样本数量；FN为错误识别为正常流量的异常流量样本数量。

4.2 实验结果及分析

(1) 流统计特征对所提模型检测性能的贡献分析：为探究所提方法的可解释性，利用沙普利可加性特征解释(Shapley Additive Explanations, SHAP)模型对无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法进行特征贡献度分析。通过量化流量统计特征对模型分类决策的影响权重，揭示关键特征与攻击行为间的内在关联机制。图7展示了在CICIDS2017与CICIDS2018数据集上贡献度排名前15位的特征对比结果，具体分析如下：

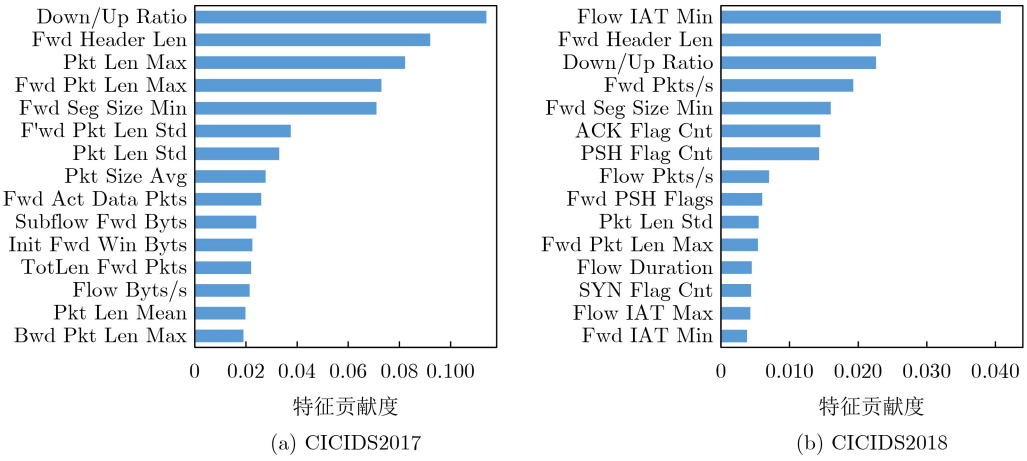
根据图7，两数据集中高贡献度特征的交集表明，“Down/Up Ratio”(下行/上行流量比)、“Fwd Header Len”(前向头部长度)及“Fwd Pkt Len Max”(前向最大包长)等方向性、协议结构与包长分布特征对检测性能具有普适性支撑作用。以“Down/Up Ratio”为例，其在正常流量中因下载行为主导呈现高值(下行流量显著高于上行)，而在DDoS/DoS攻击中因攻击者伪造请求导致上行流量激增(如图7中SHAP值分布所示)，服务器因资源枯竭致使响应流量锐减，该比值呈现断崖式下降。此现象验证了方向性流量比在区分突发性攻击与常规通信中的关键判别作用。而差异特征(如CICIDS2018中‘Flow IAT Min’的突出贡献)则反映了不同攻击场景下流量特征的敏感性差异。上述分析表明所提方法能有效捕捉流量统计特征与攻击行为的本质关联。

(2) KAFS算法的有效性验证：为检验KAFS算法的抽样效果，设计消融实验，比较了随机抽样(Random Sampling, RS)、顺序抽样(Sequential Sampling, SeS)和KAFS算法对CICIDS2017中流量数据的抽样能力。在实验中，仅改变抽样算法，其他条件保持不变。RS方法对流量样本数据按照抽样数量进行随机抽取。SeS方法依据样本集上样本顺序对各类别按照抽样数量抽取。由于各抽样方法可能具有随机性，对各抽样方法进行了5次实验。

不同抽样方法的检测结果如图8所示。在从大规模网络流量数据抽取少量流量样本的场景下，SeS算法的抽样效果很差。这是因为每类流量只抽取了前n个样本，在后续的流量中可能会有一些流量特征发生变化。抽取的少量流量特征数据不足以代表大规模的网络流量，对有效训练模型造成困难。RS方法优于SeS方法，但与KAFS算法相比仍有较大差距。KAFS算法构建的小样本流量集上训练的模型在4个评价指标上的结果均最高，更适合于构建小样本流量训练集。

(3) SMLP模型的有效性验证：本文在CICIDS-2017和CICIDS2018数据集上设计消融实验来测试SMLP模型的有效性。首先，利用KAFS方法构造训练集。然后，使用流量训练集分别训练Siamese CNN, Siamese LSTM和SMLP。训练完成后，本文比较3种孪生网络对待测样本的检测性能，检测结果如图9所示。

如图9(a)所示，无图案柱体表示SMLP模型在CICIDS2017上的流量异常检测性能。在CICIDS-



(a) CICIDS2017　　(b) CICIDS2018

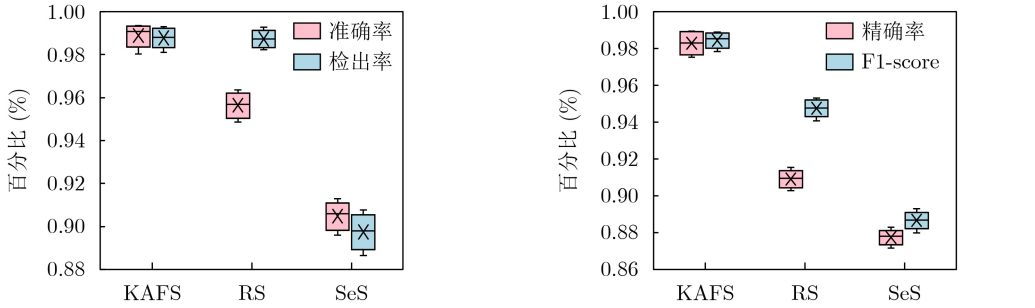
图 7 CICIDS2017和CICIDS2018数据集中流统计特征对模型检测性能的贡献

2017上，基于SMLP的流量异常检测模型在各检测指标上均优于Siamese CNN和Siamese LSTM。SMLP对CICIDS2017中的流量数据的准确率比Siamese CNN高2.53%，比Siamese LSTM高4.77%。SMLP模型对攻击的检出率比Siamese CNN高2.62%，比Siamese LSTM高5.12%

如图9(b)所示，无图案柱体表示SMLP模型在CICIDS2018上的流量异常检测性能。SMLP的精确率比Siamese CNN高4.10%，比Siamese LSTM高4.02%。在检出率方面，SMLP比Siamese LSTM提高了2.52%。原因是CNN模型主要用于捕捉局部特征，缺乏对全局特征之间相关性的把握。因此，Siamese CNN的检测性能低于基于SMLP的流量异常检测模型。LSTM模型常用于学习大量数据的时间关系。KAFS算法构建的小样本网络流量训练集不适合LSTM模型学习时间特征。Siamese LSTM的检测性能也低于基于SMLP的流量异常检测模型。

本文同样在这两个数据集上进行消融实验来验证本文损失函数的有效性。首先，利用KAFS方法构造流量训练集。然后，使用流量训练集分别训练使用标准损失函数的MLP模型和使用结合了编码和预测损失的SMLP模型。训练完成后，对比两模型对待测样本的检测性能，检测结果如图10所示。

根据图10，浅色柱状和深色柱状分别表示为使用标准损失函数的MLP模型和使用结合编码和预测损失的SMLP模型对异常流量的检测性能。不难



(a) 不同方法抽样后模型的检测准确率和检出率　(b) 不同方法抽样后模型的检测精确率和F1-score

图 8 不同抽样方法的检测结果的比较

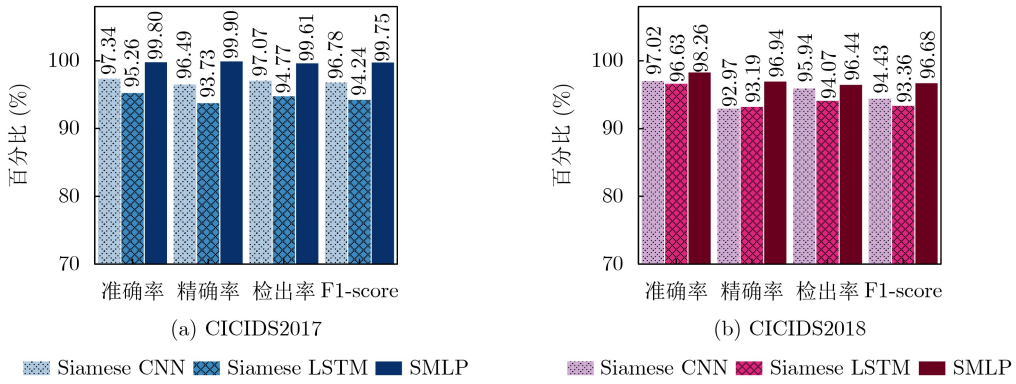


图 9 不同孪生网络对CICIDS2017和CICIDS2018数据集的检测性能

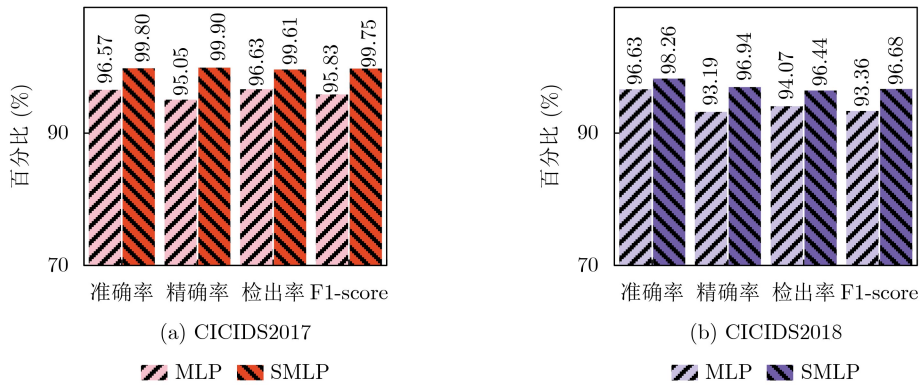


图 10 基于标准损失的MLP与融合编码和预测损失SMLP在CICIDS 2017和CICIDS2018数据集的检测性能对比

发现，SMLP模型相比MLP模型在4个检测指标上对两个数据集的检测性能都更高。SMLP模型对CICIDS2017中异常流量的检测准确率相比MLP模型提升了3.24%，精确率提升了4.85%，检出率提升了2.99%，F1-score提升了3.93%。对CICIDS2018中异常流量的检测，SMLP模型的准确率相比MLP模型提升了2.06%，精确率提升了5.89%，检出率提升了1.67%，F1-score提升了3.81%。这也验证了本文的结合编码和预测损失的SMLP模型的有效性。

(4) CICIDS2017上不同先进方法的比较：本文将无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法与其他应用于CICIDS2017数据集并在类不平衡和小样本问题上表现更好方法FC-Net [21], FS-IDS[22]和LIO-IDS[13]进行了比较。不同方法的结构差异和检测性能对比如表3所示。无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法与LIO-IDS相比，攻击流量的检出率差异不大。然而，LIO-IDS需要更多的训练样本进行训练。本文方法比其他3个检测方法具有更高的准确性、精确率和F1-score。与3种方法相比，所提方法在准确率、精确率和F1-score上分别最多提升了4.32%, 4.54%, 5.59%, 5.22%。

不同方法对CICIDS2017中未知攻击的检测性能如图11所示。结合表3，虽然LIO-IDS对测试集中攻击样本的检测性能相比FC-Net和FS-IDS更高，但对未知攻击流量的准确率、检出率和F1-score较低，仅为93.2%, 85.14%和86.72%。由于LIO-IDS对CICIDS2017中的已知攻击类充分学习，因此对已知攻击流量样本的性能较好。而对未知攻击难以适应，因此检测性能较差。而无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法能够更好地将未知攻击识别为攻击，对未知攻击的检测准确率、精确率、检出率和F1-score均最高，分别达到97.41%, 97.02%, 92.9%和94.93%。所提方法相比其他3种方法，检测准确率、精确率、检出率、F1-score分别最多提升了5.19%, 9.81%, 12.82%, 11.28%。通过对图11和表3的分析，所提方法在依据少量流量样本的情况下，对正常和攻击流量都保持较高的检测性能。

为了验证无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法的多分类能力，将该方法与FC-Net和FS-IDS对6种攻击流量的检测精确率和检出率进行了比较，结果如表4所示。根据表4，所提方法对这6类攻击的检测精确率均最高，对DDoS, DoS GoldenEye, PortScan, Bot, FTP-Patator和SSH-Patator的检测精确率相比其他两种方法分别至少提升1.15%, 4.03%, 6.70%, 0.83%, 0.11%和0.38%。所提方法在PortScan攻击上最可能出现误报，其原因是有些恶意端口扫描流量特征可能与正常行为相似，导致部分正常流量被错误判断为PortScan类别，因此会出现误报。所提方法对DDoS, DoS GoldenEye, PortScan, Bot和FTP-Patator攻击的检出率最高，对DDoS的检出率比FS-IDS提高了1.94%。与FC-Net相比，所提方法对Bot的检出率提高了1.20%。虽然无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法对

表 3　流量异常检测类别不平衡问题的先进方法的结构及检测结果对比(%)

方法	抽样方法	K值设定	模型	损失	准确率	检出率	精确率	F1-score
FC-Net	随机抽样	固定且相同	CNN and DNN	均方误差	95.67	95.28	94.32	94.80
FS-IDS	随机抽样	固定且相同	AE+CNN	均方误差	97.71	96.56	97.88	97.22
LIO-IDS	过采样	固定且相同	LSTM + I-OVO	分类交叉熵	97.56	99.24	95.08	97.11
本文方法	KAFS	自适应	SMLP	二进制交叉熵	99.80	99.61	99.90	99.75

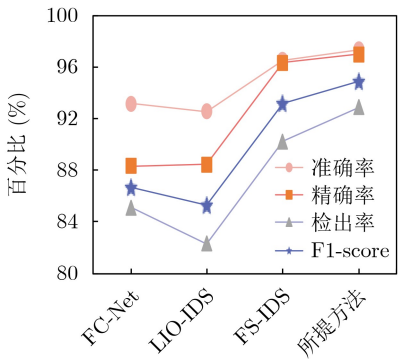


图 11 不同检测方法对CICIDS2017数据集中未知攻击的检测性能

表 4　不同方法的多分类精确率和检出率对比(%)

类型	方法					
	FC-Net		FS-IDS		所提方法	
	精确率	检出率	精确率	检出率	精确率	检出率
DDoS	98.45	97.62	98.36	97.97	99.58	99.87
DoS GoldenEye	89.77	99.52	96.07	99.28	99.94	99.54
PortScan	85.46	99.77	92.86	99.72	99.08	99.84
Bot	98.32	98.73	97.98	96.78	99.14	99.91
FTP-Patator	99.24	99.34	99.71	99.59	99.82	100.00
SSH-Patator	99.49	100.00	99.61	99.92	99.99	99.77

SSH-Patator的检出率略低于FC-Net，但差异不显著。

以上实验比较了所提方法和一些应用于CICIDS-2017类别不平衡问题上的先进方法的检测性能。本文还在CICIDS2017上比较几种先进的流量异常检测方法(VFBLS[6], HNN[7], DEIL-RVM[5]和FCL-SBLS[4])和无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法训练样本量、准确率、精确率、检出率和F1-score，如表5所示。通过表5中的对比发现，其他方法需要更多的样本(最大样本量为2 830 696)进行训练，以保证更好的检测性能。无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法在CICIDS2017上仅使用少量样本进行训练，准确率为99.80%，精确率为99.90%，检出率为99.61%，F1-score为99.75%。该方法整体性能与其他先进的检测方法持平且对流量数据量的要求低，表明无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法更适合于真实场景下的流量异常检测。

为进一步验证所提方法对检测性能的提升具有统计意义，本文在CICIDS2017数据集上对不同方法的检测性能进行5次实验并记录性能指标，然后利用t-test检测方法计算每种方法与所提方法在每个评估指标上的显著性水平，其结果如表6所示。不难发现，HNN与所提方法在CICIDS2017数据集上的检测准确率方面的统计显著性水平超过0.05，这说明检测性能差异可能是随机的，而HNN与所提方法在其他3个指标上的统计显著性水平均小于0.05，能够证明所提方法在性能上显著优于HNN方法。其他方法在4个检测指标上与所提方法的统计显著性水平均小于0.05。验证了所提方法对检测性能的提升具有统计意义。

(5) 在CICIDS2018上的不同先进方法的检测性能比较：对于CICIDS2018，比较了所提方法与在该数据集上表现更好的方法DSSTE+miniVGGNet [14]、ICVAE-BSM [15]和FL-IIDS[8]的训练样本量和检测性能，如表7所示。其他3种方法是需要较大训练样本量的数据增强方法。本文方法只需要少量的样本就可以训练出有效的模型，并对CICIDS2018实现更好的检测性能。其准确率为98.26%，精确率为96.94%，检出率为94.44%, F1-score为96.68%。相比其他3种方法，所提方法的准确率、精确率、检出率、F1-score分别最多提升了1.03%, 2.63%, 1.32%, 1.96%。无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法的检测性能指标均高于其他3种方法。

再次比较上述方法对不同已知攻击多分类检测精确率和检出率，如表8所示。无监督自适应抽样

表 5 所提方法与CICIDS2017上的先进方法检测性能的对比

方法	模型结构	样本数	准确率(%)	精确率(%)	检出率(%)	F1-score(%)
VFBLS	多特征广义学习系统	21942	97.39	96.90	97.60	97.25
HNN	CNN/LSTM+DNN	225745	99.84	99.98	99.13	99.55
DEIL-RVM	动态集成相关向量机	2830696	99.56	99.44	99.41	99.42
FCL-SBLS	联邦持续学习和堆叠广义学习系统	2264557	95.28	94.14	94.30	94.22
所提方法	KAFS和SMLP	177	99.80	99.90	99.61	99.75

表 6 现有先进方法与所提方法对CICIDS2017数据集在检测性能的统计显著性水平

方法	准确率	精确率	检出率	F1-score
VFBLS	1.60e–11	8.20e–13	1.58e–10	6.61e–11
HNN	0.20	2.30e–02	7.65e–05	2.49e–02
DEIL-RVM	1.48e–04	5.48e–06	2.36e–02	5.04e–04
FCL-SBLS	5.98e–14	3.89e–15	1.26e–13	5.15e–14

表 7 所提方法与CICIDS2018上的先进方法检测结果对比

方法	样本量	准确率(%)	精确率(%)	检出率(%)	F1-score(%)
DSSTE+miniVGGNeT	154034	97.26	94.46	95.18	94.82
ICVAE-BSM	1628599	97.83	96.30	95.42	95.86
FL-IIDS	75955	98.21	96.35	96.27	96.31
所提方法	141	98.26	96.94	96.44	96.68

与改进孪生网络结合的网络流量异常检测方法对Bruteforce, DoS和Infiltration攻击的检测精确率相比其他3种方法均最高。对Bot攻击的检测精确率虽略低于FL-IIDS，但仅相差0.32%。所提方法可能产生Infiltration的误报，这是由于渗透攻击通常利用合法协议导致其在一些基础流统计特征上与正常流量类似，在检测过程中可能会将少量正常流错误判定为Infiltration，从而产生误报。所提方法对Bot的检出率比ICVE-BSM高5.44%，比DSSTE+miniVGGNet高4.55%，比FL-IIDS略高0.05%。对于Infilteration，该方法比ICVAE-BSM提高1.73%，比DSSTE+miniVGGNet提高2.48%，相比FL-IIDS提高了16.24%。虽然对Bruteforce和DoS攻击的检出率略低于FL-IDS，但相差不多。结果证明了本文方法对CICIDS2018的少数类攻击流量仍然保持较高的检出率。

本文同样在CICIDS2018数据集上对不同方法的检测性能进行5次实验并记录性能指标，然后利用t-test检验方法计算在CICIDS2018数据集上的先进方法与所提方法在每个评估指标上的显著性水平，其结果如表9所示。不难发现，ICVAE-BSM、DSSTE+ miniVGGNeT和FL-IIDS方法在4个检测指标上与所提方法的统计显著性水平均小于0.05。结果显示所提方法在准确率、精确率、检出率、F1-score上的提升均显著优于现有方法，具有统计学意义的优势。

4种方法对CICIDS2018数据集中的未知攻击的检测性能如图12所示。在所对比的3种方法中， FL-IIDS的检测性能相对最好。所提方法相比3种对比方法对未知攻击的检测准确率至少提升了1.73%，精确率至少提升了5.17%，检出率至少提升了4.06%，F1-score至少提升了4.63%。在4种方法中，所提方法对CICIDS2018的未知攻击检测性能最好，验证了该方法在检测未知攻击上的有效性。

同时，在CICIDS2017和CICIDS2018数据集上，相比于已知攻击检测，所提方法对未知攻击的检测性能与现有先进方法的检测性能差异更显著。这是由于现有检测方法通常依赖于大量标注数据，容易对已知攻击过拟合，限制了其在面对未知攻击时的有效性，因此，他们对未知攻击的检测性能差。而本文方法通过KAFS抽取具有代表性的流量样本，使得训练样本质量更好，且SMLP模型通过学习流量数据的异同，对未知攻击流量也能保持较好的检测性能，缓解了现有方法的上述局限性，具有更强的适应性。

综上所述，无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法对CICIDS2017和CICIDS2018数据集的网络攻击流量数据保持了良好的检测性能。实验结果表明，该方法对网络流量异常检测中的类不平衡问题具有先进性和有效性。

5　结论

针对网络流量异常检测中攻击流量标记不足和流量类别不均衡的问题，本文提出一种无监督自适应抽样与改进孪生网络结合的网络流量异常检测方法。在该方法中，设计了一种基于K-medoids的自适应小样本抽样算法。该算法使用无监督聚类方法从多种流量数据中动态选择少量具有代表性的训练集。然后，构建孪生多层感知器，仅使用少量的流量输入样本计算样本之间的距离，并准确检测流量样本类别。为了提高训练效率，本文在SMLP中设计了一种鲁棒损失函数，将MLP编码过程中的编

表 8　与CICIDS2018上的先进方法多分类检测精确率和检出率对比(%)

类型	方法							
	ICVAE-BSM		DSSTE+ miniVGGNeT		FL-IIDS		所提方法	
	精确率	检出率	精确率	检出率	精确率	检出率	精确率	检出率
Bot	91.04	94.56	89.11	95.36	96.14	99.65	95.82	99.70
Bruteforce	92.29	94.37	89.08	95.24	92.36	100.00	93.86	99.61
DoS	92.52	93.81	91.99	92.59	97.16	98.40	97.51	95.87
Infiltration	87.72	93.77	87.38	93.08	93.91	82.06	95.65	95.39

表 9　现有先进方法与所提方法对CICIDS2018数据集在检测性能的统计显著性水平

方法	准确率	精确率	检出率	F1-score
ICVAE-BSM	2.99e–05	5.15e–06	2.30e–06	4.91e–07
DSSTE+ miniVGGNeT	6.18e–08	1.02e–11	2.42e–10	3.34e–10
FL-IIDS	6.27e–03	1.33e–08	4.19e–06	5.82E–04

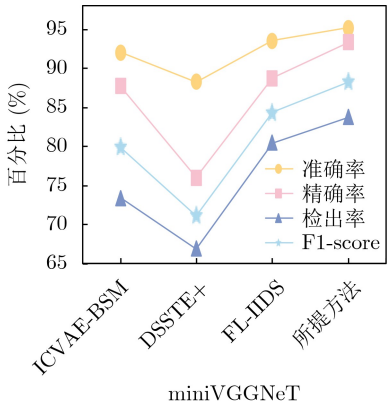


图 12 不同检测方法对CICIDS2018数据集中未知攻击的检测性能

码损失与基于锚点样本与正常样本和恶意样本之间距离的预测损失函数相结合。基于CICIDS2017和CICIDS2018数据集的多个实验表明，本文方法可以在训练较少流量样本的情况下，有效检测已知和未知攻击流量。在未来的研究中，本文将进一步探索有效的小样本网络流量异常检测方法，以提高检测模型和算法在真实网络中的准确性。

参 考 文 献

[1] 潘成胜, 李志祥, 杨雯升, 等. 基于二次特征提取和BiLSTM-Attention的网络流量异常检测方法[J]. 电子与信息学报, 2023, 45(12): 4539–4547. doi: 10.11999/JEIT221296.
PAN Chengsheng, LI Zhixiang, YANG Wensheng, *et al*. Anomaly detection method of network traffic based on secondary feature extraction and BiLSTM-attention[J]. *Journal of Electronics & Information Technology*, 2023, 45(12): 4539–4547. doi: 10.11999/JEIT221296.

[2] GUPTA N, JINDAL V, and BEDI P. CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems[J]. *Computers & Security*, 2022, 112: 102499. doi: 10.1016/j.cose.2021.102499.

[3] LEEVY J L and KHOSHGOFTAAR T M. A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data[J]. *Journal of Big Data*, 2020, 7(1): 104. doi: 10.1186/s40537-020-00382-x.

[4] HE Xiaoqiang, CHEN Qianbin, TANG Lun, *et al*. Federated continuous learning based on stacked broad learning system assisted by digital twin networks: An incremental learning approach for intrusion detection in UAV networks[J]. *IEEE Internet of Things Journal*, 2023, 10(22): 19825–19838. doi: 10.1109/jiot.2023.3282648.

[5] WU Zhijun, GAO Pan, CUI Lei, *et al*. An incremental learning method based on dynamic ensemble RVM for intrusion detection[J]. *IEEE Transactions on Network and Service Management*, 2022, 19(1): 671–685. doi: 10.1109/tnsm.2021.3102388.

[6] LI Zhida, RIOS A L G, and TRAJKOVIĆ L. Machine learning for detecting anomalies and intrusions in communication networks[J]. *IEEE Journal on Selected Areas in Communications*, 2021, 39(7): 2254–2264. doi: 10.1109/jsac.2021.3078497.

[7] LEI Shengwei, XIA Chunhe, LI Zhong, *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. doi: 10.1109/tnse.2021.3109644.

[8] JIN Zhigang, ZHOU Junyi, LI Bing, *et al*. FL-IIDS: A novel federated learning-based incremental intrusion detection system[J]. *Future Generation Computer Systems*, 2024, 151: 57–70. doi: 10.1016/j.future.2023.09.019.

[9] RESENDE P A A and DRUMMOND A C. A survey of random forest-based methods for intrusion detection systems[J]. *ACM Computing Surveys*, 2019, 51(3): 48. doi: 10.1145/3178582.

[10] SHAO Ling, WU Di, and LI Xuelong. Learning deep and wide: A spectral method for learning deep networks[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2014, 25(12): 2303–2308. doi: 10.1109/TNNLS.2014.2308519.

[11] 唐宏, 刘丹, 姚立霜, 等. 面向类不平衡网络流量的特征选择算法[J]. 电子与信息学报, 2021, 43(4): 923–930. doi: 10.11999/JEIT190992.
TANG Hong, LIU Dan, YAO Lishuang, *et al*. Feature selection algorithm for class imbalanced internet traffic[J]. *Journal of Electronics & Information Technology*, 2021, 43(4): 923–930. doi: 10.11999/JEIT190992.

[12] TELIKANI A, GANDOMI A H, CHOO K K R, *et al*. A cost-sensitive deep learning-based approach for network traffic classification[J]. *IEEE Transactions on Network and Service Management*, 2022, 19(1): 661–670. doi: 10.1109/tnsm.2021.3112283.

[13] GUPTA N, JINDAL V, and BEDI P. LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system[J]. *Computer Networks*, 2021, 192: 108076. doi: 10.1016/j.comnet.2021.108076.

[14] LIU Lan, WANG Pengcheng, LIN Jun, *et al*. Intrusion detection of imbalanced network traffic based on machine learning and deep learning[J]. *IEEE Access*, 2021, 9: 7550–7563. doi: 10.1109/ACCESS.2020.3048198.

[15] ZHANG Ying and LIU Qiang. On IoT intrusion detection based on data augmentation for enhancing learning on unbalanced samples[J]. *Future Generation Computer Systems*, 2022, 133: 213–227. doi: 10.1016/j.future.2022.03.007.

[16] BALASUBRAMANIAM S, VIJESH JOE C, SIVAKUMAR

T A, *et al*. Optimization enabled deep learning-based DDoS attack detection in cloud computing[J]. *International Journal of Intelligent Systems*, 2023, 2023: 2039217. doi: 10.1155/2023/2039217.

[17] LAKE B M and BARONI M. Human-like systematic generalization through a meta-learning neural network[J]. *Nature*, 2023, 623(7985): 115–121. doi: 10.1038/s41586-023-06668-3.

[18] KUMAR V and SINHA D. Synthetic attack data generation model applying generative adversarial network for intrusion detection[J]. *Computers & Security*, 2023, 125: 103054. doi: 10.1016/j.cose.2022.103054.

[19] YAN Mi, HUI S C, and LI Ning. DML-PL: Deep metric learning based pseudo-labeling framework for class imbalanced semi-supervised learning[J]. *Information Sciences*, 2023, 626: 641–657. doi: 10.1016/j.ins.2023.01.074.

[20] YAN Fei, LI Nianqiao, ILIYASU A M, *et al*. Insights into security and privacy issues in smart healthcare systems based on medical images[J]. *Journal of Information Security and Applications*, 2023, 78: 103621. doi: 10.1016/j.jisa.2023.103621.

[21] XU Congyuan, SHEN Jizhong, and DU Xin. A method of few-shot network intrusion detection based on meta-learning framework[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 3540–3552. doi: 10.1109/tifs.2020.2991876.

[22] YANG Jingcheng, LI Hongwei, SHAO Shuo, *et al*. FS-IDS: A framework for intrusion detection based on few-shot learning[J]. *Computers & Security*, 2022, 122: 102899. doi: 10.1016/j.cose.2022.102899.

[23] SHARAFALDIN I, LASHKARI A H, and GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]. The 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal, 2018: 108–116. doi: 10.5220/0006639801080116.

尹梓诺：女，博士生，研究方向为网络空间安全、网络流量异常检测等.

陈鸿昶：男，教授，研究方向为通信与信息系统、数据科学与人工智能等.

马海龙：男，教授，研究方向为网络空间内生安全技术、网络威胁智能检测以及新型网络体系等.

胡　涛：男，助理研究员，研究方向为新型网络体系结构等.

白禄鑫：男，硕士生，研究方向为卫星互联网、软件定义网络和网络安全等.

责任编辑：马秀强

A Network Traffic Anomaly Detection Method Integrating Unsupervised Adaptive Sampling with Enhanced Siamese Network

YIN Zinuo[①]　CHEN Hongchang[①]　MA Hailong[①②]　HU Tao[①]　BAI Luxin[①]

[①](*Information Technology Institute, Information Engineering University, Zhengzhou* 450001, *China*)

[②](*Key Laboratory of Cyberspace Security, Ministry of Education of China, Zhengzhou* 450001, *China*)

Abstract:

Objective　The increasing complexity of network architectures and the rising frequency of cyberattacks have heightened the demand for effective network traffic anomaly detection. While machine learning and deep learning approaches have been widely applied, their effectiveness is often limited by the class imbalance commonly observed in network traffic data. To address this limitation, this study proposes a network traffic anomaly detection method integrating unsupervised adaptive sampling with enhanced Siamese network. An adaptive sampling algorithm is developed to balance the distribution of normal and anomalous traffic, improving the representativeness of training data. A Siamese Multi-Layer Perceptron (SMLP) model is then trained using a robust loss function to capture both similarities and differences in traffic patterns. This architecture enhances the model's ability to identify anomalies, particularly under class-imbalance conditions. The proposed framework provides a scalable and data-efficient approach for improving the accuracy of network anomaly detection and reinforcing cybersecurity.

Methods　The proposed K-medoids-based Adaptive Few-shot Sampling (KAFS) algorithm applies unsupervised K-medoids clustering to group traffic data within each category based on feature distributions, forming multiple subclasses. From these, a small number of representative samples are adaptively selected to construct a

balanced few-shot training set. This approach maintains a proportionate representation of normal and attack traffic, reducing model bias toward the dominant normal class and ensuring more effective learning across categories. Sample quality is further improved by prioritizing representativeness during selection. For the constructed training set, a traffic anomaly detection model based on a SMLP is designed. The model's loss function combines encoding loss from the MLP with a prediction loss defined by the distance between anchor samples and corresponding normal or malicious samples. This structure enables the model to distinguish both similarities and subtle differences in traffic behavior, thereby enhancing the accuracy of attack traffic detection.

Results and Discussions The proposed network traffic anomaly detection method, which integrates unsupervised adaptive sampling with an enhanced Siamese network, demonstrates strong performance on the CICIDS2017 and CICIDS2018 datasets. As shown in Fig. 8, the SMLP model trained using traffic samples generated by the KAFS sampling algorithm achieves superior detection performance, confirming the effectiveness of the KAFS approach. In Fig. 9, detection accuracies of 99.80% and 98.26% are achieved for attack-class traffic in the CICIDS2017 and CICIDS2018 datasets, respectively. Evaluation metrics presented in Fig. 9 and Fig. 10 show that the proposed method consistently outperforms other Siamese network architectures and loss functions in terms of accuracy, precision, Detection Rate (DR), and F1-score, further supporting the validity of the SMLP design. As shown in Tables 4 and 6, the method attains detection performance comparable to that of state-of-the-art algorithms while using substantially fewer samples, highlighting its suitability for practical deployment where data availability may be limited. Statistical analysis of the results (Tables 5 and 8) confirms that the performance gains achieved by the proposed method are statistically significant. Fig. 11 and Fig. 12 further illustrate that the method delivers notable improvements over existing approaches in detecting unknown attack types, demonstrating its adaptability and robustness under evolving threat conditions.

Conclusions This study addresses the challenges of sparse attack traffic and class imbalance in network traffic anomaly detection by proposing a method that combines unsupervised adaptive sampling with an enhanced Siamese network. A KAFS algorithm is designed to dynamically select representative training sets using unsupervised clustering. To enable accurate detection with limited input samples, an SMLP is developed to compute distances between traffic samples. A robust loss function is introduced, incorporating both encoding loss from the MLP and prediction loss based on the distance between anchor, normal, and malicious samples, thereby improving training efficiency. Experimental validation using the CICIDS2017 and CICIDS2018 datasets confirm the method's effectiveness in detecting attack traffic with few samples. Future work will focus on further enhancing few-shot intrusion detection techniques to improve detection accuracy in real-world network environments.

Key words: Network traffic anomaly detection; Class imbalance; Adaptive sampling; Siamese Multi-Layer Perceptron (SMLP)