基于深度强化学习模型融合的海洋气象传感器网络入侵检测方法

张文潇，苏新，顾依凌
（河海大学信息科学与工程学院，江苏 常州 213000）

摘　要：海洋气象传感器网络（MMSN, maritime meteorological sensor network）有别于传统陆地组网，入侵检测任务在海洋气象传感器网络场景下面临着新的挑战。利用卫星通信技术设计一种海洋气象传感器网络卫星检测方法，分析海洋气象传感器网络的网络结构和特点。从算法和损失函数的角度入手，对提高入侵检测系统（IDS, intrusion detection system）检测性能的方法展开研究，提出了一种基于深度强化学习模型融合的海洋气象传感器网络入侵检测方法。首先，建立改进损失函数的轻量梯度提升机（LightGBM, light gradient boosting machine）、一维卷积神经网络（1D-CNN, 1D conventional neural network）和二维卷积神经网络（2D-CNN, 2D conventional neural network）分类器，综合提取海洋气象传感器网络入侵检测数据的时序特征和空间特征。其次，根据模型融合技术中的堆叠和平均原理，设计一个基于以上基分类器的模型融合方法，采纳基学习器的优势而规避其劣势，从而提高系统整体检测性能。最后，仿真实验结果表明，所提的入侵检测方法能够有效地提高入侵检测系统对少数类攻击数据的检测性能，并提高系统的稳健性。

关键词：海洋气象传感器网络；入侵检测系统；模型融合；焦点损失函数
中图分类号：TN929.52
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00454

Intrusion detection based on deep reinforcement learning model fusion for maritime meteorological sensor networks

ZHANG Wenxiao, SU Xin, GU Yiling
College of Information Science and Engineering, Hohai University, Changzhou 213000, China

Abstract: Maritime meteorological sensor networks (MMSN) differ from traditional land-based networks, presenting new challenges for intrusion detection tasks. A satellite-based detection method for maritime meteorological sensor networks was designed using satellite communication technology. The network structure and characteristics of maritime meteorological sensor networks were analyzed in this method. Research was conducted on improving the detection performance of intrusion detection systems (IDS) from the perspectives of algorithms and loss functions. A maritime meteorological sensor network intrusion detection method based on the fusion of deep reinforcement learning models was proposed. Firstly, light gradient boosting machine (LightGBM), 1D conventional neural network (1D-CNN), and 2D conventional neural network (2D-CNN) classifiers with improved loss functions were established to comprehensively extract the temporal and spatial features of the intrusion detection data in maritime meteorological sensor networks. Secondly, a model fusion method was designed based on the stacking and averaging principles of model fusion technology. This method leveraged the strengths of the base classifiers and mitigated their weaknesses, thereby enhancing the overall system detection performance. Finally, simulation experiment results demonstrate that the proposed intrusion detection method can effectively improve the detection performance for a few types of attack data and enhance the robustness of the system.

收稿日期：2024−09−29；**修回日期：**2024−12−03
通信作者：苏新，leosu8622@163.com
基金项目：国家自然科学基金资助项目（No. 62371181）；常州市政策引导类计划国际科技合作/港澳台科技合作项目（No. CZ20230029）
Foundation Items: The National Natural Science Foundation of China (No. 62371181), The Changzhou Science and Technology International Cooperation Program (No. CZ20230029)

Key words: MMSN, IDS, model fusion, focal loss function

0 引言

海洋面积占地球表面积的71%，对气候的形成及变化影响极大，而极端海洋气候事件的发生会给沿海自然生态环境和社会经济发展带来严重的挑战[1]。卫星通信在海洋通信方面发挥了很大的作用。首先，卫星通信覆盖范围大，能够全球覆盖、连接偏远海域的船只和岸上设备。其次，卫星通信技术能够与其他技术协同，形成更可靠的海上通信网络。此外，卫星通信有助于海上物联网设备和传感器网络的数据收集和传输，能够增强海上安全。海洋气象传感器网络（MMSN, maritime meteorological sensor network）是一个具备监测、预告、服务等功能的大型综合传感器网络。通过气象站、浮标、观测船等观测设备对海洋气象、水文、水质和海底地质等数据进行长期、连续、实时的监测、传输和分析，为全球气候和海洋气象的精确预测以及突发性气象灾害的科学决策提供数据支持[2]。MMSN的建设和发展有助于维护国家海洋战略利益、降低海洋气象灾害损失、促进海洋基础科技创新等，网络安全是MMSN的重要建设前提之一。

随着网络技术快速发展，网络入侵事故也随之频发[3]。MMSN中，设备节点遭受攻击或者未经授权的访问，将导致网络功能损伤或者隐私泄露等问题，从而造成重大损失。因此，在MMSN中部署具备主动检测和防护能力的入侵检测系统（IDS, intrusion detection system）已成为保证网络安全的关键需求。

IDS作为重要的安全工具，在无线传感器网络（WSN, wireless sensor network）[4-5]、物联网（IoT, Internet of things）[6-7]和工业控制系统（ICS, industry control system）[8-9]等传统陆地网络和系统中已得到了广泛的应用。然而，与传统地面组网相比，MMSN在部署环境、网络结构、网络功能、数据流量和易感攻击类型等方面有其特异性，所以入侵检测任务在MMSN场景中面临着新的技术挑战。首先，目前的MMSN仍在发展建设阶段，与之适配的IDS同样处于完善过程中，因此现有IDS对于MMSN场景的适配性较低；其次，MMSN节点中所采集到的数据量级更大、类别分布更加不平衡——关键性攻击数据仅占极小比例，却隐含极大威胁，对IDS分类器的训练和预测均极为不利，将使分类器在训练过程中产生严重的分类偏向性，从而导致预测结果错误地倾向于正常数据[10]；最后，MMSN IDS中检测分析模块得出的检测结果直接决定反馈与响应模块所作的处理决策，即根据检测出的不同攻击类型作出针对性响应活动以保证目标系统安全，而现有IDS的分类器通常注重正常与攻击样本的二分类结果，对具体每种攻击类型的检测要求较低，对其中少数类攻击的检测关注度则更为匮乏，上述因素增大了IDS对MMSN进行针对性安全保护的难度。基于上述分析，本文结合现有技术与MMSN的结构特性，提出了一种基于模型融合的MMSN入侵检测方法，提高了MMSN场景中入侵检测任务对少数类攻击样本的检测性能。本文主要贡献如下。

1) 针对MMSN场景中的网络安全保护问题，根据节点分布地理位置将MMSN划分为空、天、地、海4个子网络，分别对网络结构和承担功能进行介绍。

2) 针对少数类攻击样本检测关注度匮乏的问题，提出了一种基于模型融合的MMSN入侵检测方法。该方法使用轻量梯度提升机（LightGBM, light gradient boosting machine）、一维卷积神经网络（1D-CNN, 1D conventional neural network）和二维卷积神经网络（2D-CNN, 2D conventional neural network）分类器作为基学习器，综合提取MMSN入侵检测数据集的时序特征和空间特征，并基于模型融合技术中的堆叠和平均原理设计模型融合方法，采纳基学习器优势而规避其劣势，提高了系统的整体检测性能。

3) 对于本文所提的基于模型融合的入侵检测算法，使用焦点损失函数替换基学习器中原有多分类交叉熵损失函数，并设计特征组合的划分方式，以提高分类器对于少数类样本的关注度和分类器泛化性。

1 相关工作

1.1 海洋气象传感器网络

海洋气象环境是沿海社区生活的重要组成部

分。对气温、气压、湿度、风速、风向和海浪高度等环境要素[11]的海洋气象的监测和预测，能够为海洋灾害预警、海洋资源开发等活动提供重要依据。随着信息化和智能化进程的推进，将海洋气象监测与大数据、人工智能等技术相结合，能够满足海洋信息连续、实时、立体监测的下一代MMSN的发展和应用。

MMSN系统架构如图1所示，MMSN物理空间覆盖高空、低空、近岸、海面和水下区域，主体结构包括环境要素监测设备、通信网络系统、数据处理中心和信息共享平台。环境要素监测设备包括气象观测卫星、岛礁气象站、船舶气象站、浮标和气象气球等设备，负责实时连续监测、采集海洋环境信息[12]；通信网络系统由各气象设备所搭载的通信模块以及专用于信息交换的通信基站等通信设备联结而成，保障信息和指令的低延迟传递；数据处理中心和信息共享平台负责收集、存储、处理和分发海洋气象数据，并提供信息共享和服务功能，以支持各种应用和用户需求。MMSN为科学研究、应用服务、决策支持等提供了强有力的技术支持，在海洋科学研究、海洋资源开发、海洋环境保护和海洋经济发展等领域有重要作用。

从节点的地理位置分布来看，下一代MMSN可以被划分为覆盖高空区域的天基子网络、覆盖近岸区域的地基子网络、覆盖低空区域的空基子网络和覆盖海面和水下区域的海基子网络。其中，天基网络主要由卫星组成，卫星通信在海洋通信方面发挥了很大作用，能够与其他技术结合共同保证海上安全。文献[13]利用卫星通信使船只能够与陆地站点进行可靠的实时信息交换，并提供船只实时位置、航线和速度等信息，同时船只能够利用卫星通信及时接收天气预报和预警。该文献还提到了卫星通信与边缘计算和机器学习模型联合进行异常检测和风险管理。文献[14]中卫星通信是海上物联网（MIoT, maritime Internet of things）的重要组成部分，能够与无人机（UAV, unmanned aerial vehicle）通信和地面通信网络结合使用，形成更可靠的海上通信网络。下一代MMSN的4个子网有机结合，结构上紧密连结，功能上互相补充，协同实现海洋信息监测、传输和处理。MMSN中每个子网络的主要节点构成和承担功能见表1。相较于传统的结构简单、节点种类单一、覆盖范围较小的WSN[15-16]，下

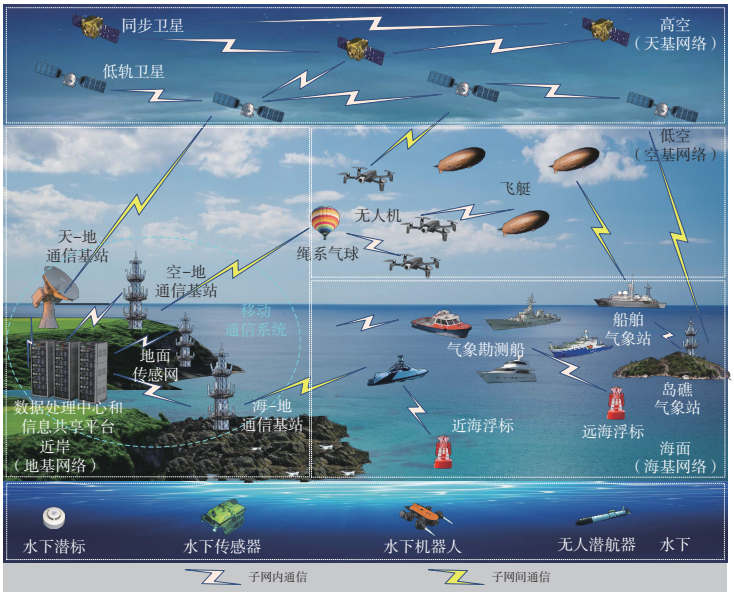


图1　MMSN系统架构

表1　MMSN中每个子网络的主要节点构成和承担功能

子网络	节点构成	网络功能
空基网络	无人机、飞艇、气球、地面基站等	信息采集、紧急救援、临时通信
天基网络	同步卫星、低轨卫星等	导航定位、信息采集、通信中继
地基网络	移动通信系统、通信基站、地面传感器网络等	网络通信、信息采集、子网络状态监控、信息处理与共享
海基网络	浮标、船舶、基站、水下探测设备等	信息采集、导航定位、海域通信

一代 MMSN 具有节点种类多样[17-18]、结构层次复杂[19]、数据传输量大、数据流类分布极端不平衡、覆盖范围大和部署环境恶劣的特点。

1.2 入侵检测算法

随着人工智能技术的不断发展，越来越多的算法和模型被应用于 IDS 的构建。非监督式深度学习（DL, deep learning）中的经典 *K* 均值（*K*-means）聚类算法，能够从无标签数据中发现聚类结构，并将与该结构偏离的样本判定为异常。文献[20]提出了一种基于 *K*-means 聚类和局部异常因子（CBLOF, cluster-based local outlier factor）模型的异常检测方法，能够实现较为细粒度的异常检测。然而，仅依赖聚类方法进行异常检测的适用场景较为有限。相比之下，非监督式机器学习（ML, machine learning）模型虽然结构较为简单，但由于入侵检测数据集的复杂性和多样性，准确性难以得到保证。常见的监督式机器学习算法包括决策树（DT, decision tree）、随机森林（RF, random forest）和支持向量机（SVM, support vector machine）等。文献[21]提出了一种基于决策树和支持向量机的三层分布式结构，通过设计 4 个二分类 SVM 检测器，并结合自适应机制，优化了系统的训练时间，但对于新型、未知以及异常攻击的检测准确性较低。尽管监督式机器学习算法在检测精度和复杂环境适应性方面存在挑战，但它们对硬件资源的要求较低，因此在资源受限的小型节点上具有明显的优势。

在非监督式深度学习算法方面，文献[22]提出了一种基于堆叠自动编码器（SAE, stacked autoencoder）与流聚类相结合的方法，利用数据偏离聚类中心的情况来识别异常。然而，该方法并未专门针对入侵检测任务进行优化，因而缺乏较强的环境适应性。非监督学习的一个显著优势是可以处理无标记数据，但随着入侵检测数据集的标记信息日益完善，监督式学习在实际应用中显示出了更广泛的适用性[23]。常见的监督式深度学习算法包括卷积神经网络（CNN, convolutional neural network）和长短时记忆（LSTM, long short-term memory）网络等。例如，文献[24]提出通过构建深度可分离卷积（DSC, depthwise separable convolution）与 LSTM 的级联结构，增强模型对数据空间与时间特征的捕捉能力，从而提升了检测精度，但此方法依然面临网络结构复杂度较高的挑战。监督式深度学习算法凭借其深层结构，在入侵检测领域具备优势，但仍难以兼顾多类别检测精度与效率。因此，对于 MMSN IDS 分类器在多类别攻击数据检测中的表现问题，提出了基于模型融合的优化方法。

1.3 模型融合方法

模型融合[25]（model fusion）是机器学习和数据挖掘领域中常用的处理策略，核心原理为组合多个模型（同质或者异质）并整合预测结果，提高模型的泛化能力，避免过拟合，实现系统整体预测性能的改善。在入侵检测任务中通常采用的模型融合技术包括投票（voting）、平均（averaging）、堆叠（stacking）[26]、混合（blending）、Bagging[27-28]、Boosting[29-30]等。

在过去的研究中，文献[31]通过对降维模块中所用的自编码器进行基于模型融合技术的改进，得到了栈式自编码器，解决了过拟合问题，以获得更优的特征提取效果。其改进方法采用堆叠思想，将原有单个浅层自编码器转换为主、副编码器的堆叠，使得过拟合风险有所下降，模型收敛速度有所提升。然而，该文献中模型融合思想仅被应用于特征提取，并未对分类过程作出直接改进。文献[32]同样采用了模型融合技术中的堆叠思想，对 IDS 分类器进行改进，将决策树（DT, decision tree）、*K*-近邻（KNN, *K*-nearest neighbor）、深度神经网络（DNN, deep neural network）和随机森林（RF, random forest）4 个分类器作为基学习器，构建深度堆叠网络（DSN, deep stacked network）模型，实现了入侵检测性能的有效提升。然而，该文献所提的方法在 NSL-KDD 数据集上的检测结果显示，虽然整体检测准确率较高，但对于少数类攻击数据的检测性能仍然一般。文献[33]针对入侵检测模型的综合性能，基于模型融合中的堆叠思想，提出了堆叠集成（SE, stacking ensemble）的入侵检测方法。该方法将异构学习器作为基学习器、支持向量机作为元学习器，组合得到了综合性能最高的入侵检测分类模型。然而，该文献在设计仿真实验时采用的数据集并不具备 MMSN 入侵检测数据集的极端不平衡特性，因而该文献所提的入侵检测方法难以证明其在 MMSN 场景中的适配性。

基于上述研究，本文提出了一种适配 MMSN 场景的入侵检测任务，且针对数据集中少数类攻击数据检测性能提升的入侵检测方法。本文所提的基于

模型融合的MMSN入侵检测方法使用焦点损失函数取代多分类交叉熵损失函数，并建立LightGBM分类器和1D-CNN、2D-CNN分类器，采用堆叠和平均的思路将上述分类器作为基分类器进行模型融合，得到最终入侵检测模型。

2　基于改进LightGBM和CNN的入侵检测算法

本文所提的MMSN场景中基于模型融合的入侵检测算法使用文献[34]中所提出的基于CVAE-GAN的不平衡数据集处理方法增强分类器类别权重分配模块，并根据LightGBM内置的特征重要性评估功能对MMSN入侵检测数据集中的特征根据相对重要性进行排序；将LightGBM的预测结果作为新特征，并与部分高重要性重用特征结合，用于训练2D-CNN；最后将LightGBM、1D-CNN和2D-CNN分类器所得的预测结果加权平均，得到最终预测结果。本节以下内容将具体介绍所提算法用到的模块。

2.1　基于LightGBM的入侵检测分类器搭建

MMSN的特征之一是网络节点间流转传输海量数据，这意味着IDS对所用算法的效率有较高的要求，特征选择方法能够保留对分类决策作用最大的重要特征，同时提高分类模型性能，减少过拟合。梯度提升决策树（GBDT, gradient boosting decision tree）利用集成的思维，将多个基础的弱学习器（决策树）相结合以进行迭代训练，捕捉数据中的深层复杂关系，从而提高总体检测精度、降低误报率[35]。LightGBM是一个并行、高效的GBDT算法实现框架，具备更快的训练速度和更低的内存消耗，并且支持分布式训练，对大规模数据的处理具备优势。

在LightGBM之前出现的优秀GBDT实现框架——极限梯度提升XGBoost算法，是一种基于预排序的决策树集成算法，能够通过遍历计算信息增益精确找到最优特征分割点，但也伴随着空间、时间开销大的问题。LightGBM在XGBoost的基础上做出系列优化，在保证分类器检测能力的同时，大大地提升了算法运行效率，即基于Histogram的决策树算法、决策树的按叶生长（leaf-wise）策略、基于梯度的单边采样（GOSS, gradient-based one-side sampling）算法和互斥特征捆绑（EFB, exclusive feature bundling）算法等。

1) 基于Histogram的决策树算法

基于Histogram的决策树算法，即直方图算法。连续特征离散化示意图如图2所示，该算法将连续的浮点型特征值离散化处理，将其划分为有限数目的离散区间，并构造对应宽度的直方图，直方图每个区间的高度为特征值落入该区间的频数。然后，LightGBM通过遍历每个特征直方图的离散值选取最佳分割点。该算法将连续特征值划分至离散的数值区间，简化了数据的表达，减少了构建决策树时候选分割点的数目，优化了分割点的选择方式，很大程度上降低了内存占用和计算开销[36]。连续特征离散化的处理方式虽然降低了分割点选取的精度，但是GBDT的学习策略——多个弱学习器的集成——使得单棵树的非精确分割对于模型整体起到一定的防止过拟合的作用，最终LightGBM的结果精度受影响不大甚至表现更优。

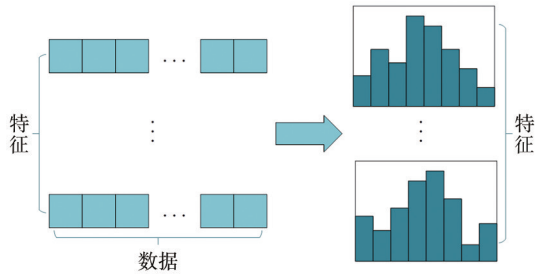


图2　连续特征离散化示意图

2) leaf-wise策略

对于单棵决策树的生成，除直方图算法，LightGBM还采用了具有深度限制的leaf-wise策略。leaf-wise策略如图3所示，其中，格纹节点通常是内部节点，表示在决策过程中的中间步骤或条件判断。在这些节点上，算法会根据某个特征或属性来决定下一步应该向左还是向右移动，即选择哪个分支继续前进。斜纹节点通常表示叶子节点，是决策树的终端节点。在叶子节点上，算法会输出最终的决策或预测结果。相较于XGBoost使用的按层生长（level-wise）策略，leaf-wise策略寻找当前所有叶节点中分裂增益最大者进行分裂操作，并在整棵树范围内循环。leaf-wise这种选择性的节点分裂有效地降低了系统开销，并且在同等分裂次数下能够取得更好的学习效果。但是该策略存在产生较深决策树导致过拟合的问题，因此LightGBM添加了限制决策树最大深度的参数以避免过拟合。

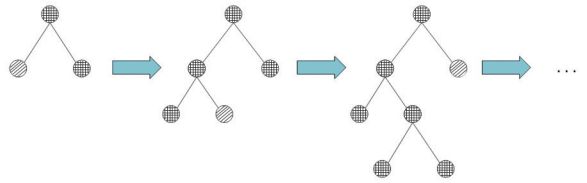


图3　leaf-wise 策略

3) 基于梯度的单边采样算法

GOSS 算法认为，相较于梯度较小的样本，梯度较大的样本能够贡献更多信息增益，因此，GOSS 算法保留大梯度样本，而对小梯度样本进行随机采样，仅保留其中少部分样本。LightGBM 使用组合得到的样本数据计算信息增益，并在计算时增加小梯度样本的权重系数以平衡该部分样本的缺失。LightGBM 通过使用 GOSS 算法，实现了在不影响训练效果的同时，减少了信息增益计算过程中的样本数目，优化了系统运行效率。

4) 互斥特征捆绑算法

EFB 算法可以将互斥特征绑定形成组合特征，无损、有效地降低了特征维度，提升了训练效率。该算法增强了 LightGBM 对具备高维稀疏特征的样本集的处理能力。

对于 MMSN 入侵检测数据集具有极端不平衡特性数据集样本的问题，LightGBM 中还包含了类别权重参数“class_weight”（该参数出现在 Scikit-learn 风格接口下；原生接口下的 lgb.Dataset 数据格式同样包含权重调节参数“weight”），原理是通过设置该参数的值，为各类别进行权重映射，例如增加少数类权重以提高模型在训练过程中对该类的关注度。归一化权重的计算式为

$$w = \frac{n}{k \times m} \tag{1}$$

其中，k 为类别数，n 为样本总数，m 为该类别所含样本数。默认情况下，各类别权重均为 1。然而，手动设置类别权重不可靠，性能一般的权重组合会导致分类器误判概率增加，即召回率表现良好而精确率严重下降。因此，本文采用文献[34]中所提的基于 CVAE-GAN 的不平衡数据集处理方法增强 LightGBM 模型的类别权重平衡模块，提高分类器的检测性能。

此外，LightGBM 内置了特征重要性评估功能，该功能将特征重要性可视化，帮助用户直观地了解各特征对于预测目标的贡献程度。LightGBM 提供了以下两种重要性评估方法。

1) 基于分裂次数（split importance）的重要性：计算并统计每个特征被用于节点分裂的次数，以此作为特征重要性的标准，出现次数越多，特征重要性越高。该重要性衡量了决策树生长过程中特征被用的频率。

2) 基于特征增益（gain importance）的重要性：将特征分裂时的信息增益作为特征重要性的标准，信息增益越大，特征重要性越高。该重要性是特征对模型效果提升程度的量化。

基于特征增益的重要性评估考虑到了特征对系统性能的提升效果，被认为具备更多信息量、更有意义、更能反映特征对模型检测能力的贡献程度，因此更加常用。本文算法根据 LightGBM 所给出的基于特征增益的重要性评估，得到特征对检测结果贡献程度的排序，选择贡献较高的特征并在后续训练中重复使用，实现了模型检测能力和泛化能力的提高。

2.2　基于 CNN 的入侵检测分类器搭建

MMSN 入侵检测数据集是一维的序列数据，部分特征包含连接持续时间、数据包流量大小和数量等时序特征。在本文算法构建过程中，选择搭建结构简单的 1D-CNN 和 2D-CNN 分类器，利用其并行计算、局部特征提取和参数共享等优势，分别提取 MMSN 入侵检数据集的时序特征和空间特征[37]。

1D-CNN 是一种针对序列数据的处理模型，例如，时间序列和文本数据等；2D-CNN 用于处理二维数据，应用场景包括图像分类和目标检测等。所使用的 CNN 分类器具备经典的 CNN 层结构，此外，本文在进行模型搭建时添加了批标准化（BN, batch normalization）层和随机失活（Dropout）层。

BN 层：通过对每个批次的输入数据进行归一化处理，使其服从标准正态分布，以减少内部协变量偏移，使隐藏层的输入分布更加稳定，加速网络收敛，提高训练速度。此外，BN 层起到了减少梯度消失和梯度爆炸问题、降低了网络过拟合风险的作用。

Dropout 层：同样是减少网络过拟合风险的常用技术，原理为在训练过程中随机丢弃部分神经元，以降低神经元之间的依赖关系，避免对某些特征的过度依赖，提高模型的泛化能力。

1D-CNN 的一维卷积层和池化层可以并行处理不同序列局部，具有快速高效的序列信息处理能力，能够针对性地提取 MMSN 入侵检测数据集中序列样本的时序特征；2D-CNN 长于提取二维图像

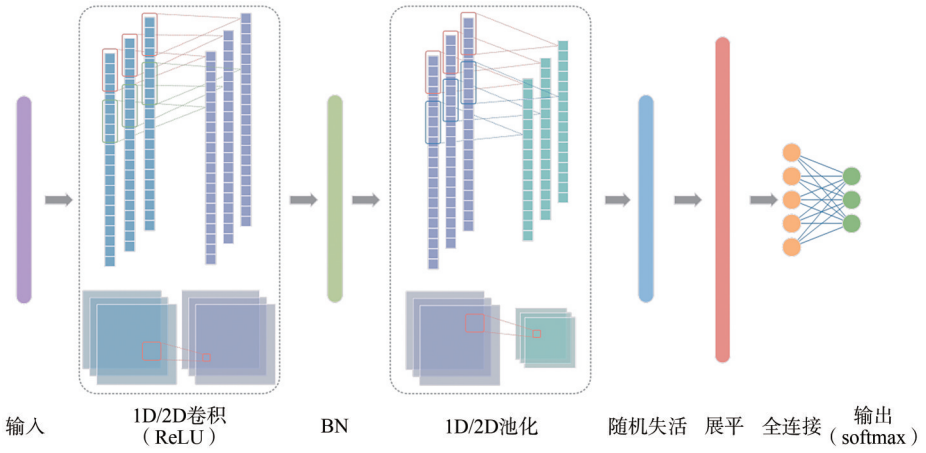


图4　1D/2D-CNN模型结构

的空间结构和模式等特征。因此，本文采用两种CNN分类器对MMSN入侵检测数据集进行时序特征和空间特征的综合提取。此外，CNN模型具有的参数共享机制使模型参数量有效减少，并在一定程度上提高了模型的泛化能力。1D/2D-CNN模型结构如图4所示，包含一个激活函数为ReLU的一维或者二维卷积层、一个BN层、一个最大池化层、一个丢弃值为0.5的Dropout层和一个全连接层，最后使用softmax激活函数输出类别预测概率。模型具体参数设置将在实验仿真部分说明。

2.3　焦点损失函数

焦点损失函数是一个用于解决数据集类别不平衡问题的损失函数[38-39]，在目标检测任务中表现出色。针对MMSN入侵检测数据集的极端不平衡特性，本文在搭建LightGBM-CNN检测模型时，考虑使用基于算法的解决方案，将焦点损失函数移植至所提算法中，代替模型训练过程中的多分类交叉熵损失函数，以进一步强化分类器模型对于少数类样本的识别能力。

机器学习中的损失函数，也称代价函数，在模型训练阶段作用，负责衡量模型预测结果与真实值之间的误差程度，是模型性能的一个量化评估。通过反向传播，迭代更新参数，优化该函数使其值最小化，实现对模型检测能力的提升。

分类模型中常用的损失函数为交叉熵损失函数，二分类交叉熵函数为

$$\mathrm{CE}=-\frac{1}{n}\sum_{i=1}^{n}\left[y_i\,\mathrm{lb}\,p_i+\left(1-y_i\right)\mathrm{lb}\left(1-p_i\right)\right] \tag{2}$$

其中，n为样本数目，y_i为真实值，p_i为预测结果（概率值）。应用该损失函数时，默认情况下所有类别样本被同等对待，然而在正负样本分布极端不平衡的情况下，占比较多的负样本更易于被成功检测，而占比极少的正样本则反之，因此，模型预测结果将倾向于易于分类的常见样本，而忽视罕见类别。

为解决以上问题，焦点损失函数在交叉熵损失函数的基础上引入了一组调制因子，函数为

$$\mathrm{FL}\left(p_t\right)=-\alpha\left(1-p_t\right)^{\gamma}\mathrm{lb}\left(p_t\right) \tag{3}$$

其中，α为正样本的权重，用于控制正负样本权重比，取值范围为[0, 1]；p_t为模型对样本的预测概率；γ为用于控制焦点损失函数的聚焦程度的超参数，取值范围为[0, 5]。当样本被正确分类时，p_t值接近1，$(1-p_t)^{\gamma}$值接近0，焦点损失函数值趋近于0；而当样本被错误分类或者难以分类时，p_t值接近0，焦点损失函数值趋近于$-\mathrm{lb}\,p_t$。由此可知，焦点损失函数通过引入调制因子，抑制了易分类样本的损失，增加了对难分类样本的关注，从而实现了模型对类别分布不平衡场景的处理。

考虑真实世界MMSN入侵检测数据集的类别分布极端不平衡的特性，在多分类检测模型搭建过程中，使用拓展至多分类环境的焦点损失函数取代LightGBM和ID-CNN模型中的多分类交叉熵函数，优化模型参数。多分类焦点损失函数为

$$\mathrm{FL}\left(p_c\right)=-\alpha_c\left(1-p_c\right)^{\gamma}\mathrm{lb}\,p_c \tag{4}$$

其中，α_c为第c类样本的权重，p_c为softmax函数所输出的预测为第c类的概率值。

2.4　模型融合思路设计

文献[34]针对数据源的基于CVAE-GAN的不平衡数据集处理方法初步完成了MMSN IDS的特征工程，而系统的整体性能还需要对分类器加以优化

和改进。本文所提的基于改进 LightGBM-CNN 的入侵检测算法使用模型融合技术，对复杂 MMSN 入侵检测数据集进行深度挖掘，结合 LightGBM 的高效、灵活和高准确性，以及 1D-CN 和 2D-CNN 分类器对于时序特征和空间特征的有效提取优势，从而提高系统整体检测性能。

对于模型融合技术，融合方法和参数设置是应用的关键。本文采用的模型融合方法主要基于堆叠和平均思想，使用 LightGBM、1D-CNN 和 2D-CNN 作为学习器，LightGBM 为树模型，CNN 为卷积神经网络模型，相关性较低的异质模型融合有利于提高系统检测精度和泛化性，基于 LightGBM 与 CNN 的模型融合思路如图 5 所示。

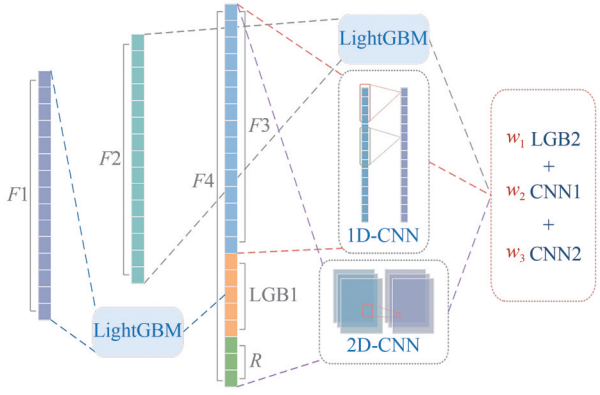


图 5　基于 LightGBM 与 CNN 的模型融合思路

根据图 5，模型融合思路实现步骤如下。

步骤 1　分别使用特征组合 $F1$ 和 $F2$ 训练 LightGBM 模型，得到对数据集的预测结果 LGB1 和 LGB2（包含对训练集和测试集的预测结果）。

步骤 2　使用特征组合 $F3$ 训练 1D-CNN 模型，得到预测结果 CNN1。

步骤 3　将 LGB1 的预测结果作为新特征与特征组合 $F3$ 组合，同时重复使用部分高重要性原始特征 R，令特征组合 $F4$=$F1$+LGB1+R，并使用其训练 2D-CNN 模型，得到预测结果 CNN2。

步骤 4　将预测结果 LGB2、CNN1 和 CNN2 加权融合得到最终预测结果 w_1LGB2 + w_2CNN1 + w_3CNN2，其中，w_1、w_2 和 w_3 为权重。

3　实验与分析

3.1　实验环境及参数设置

本文仿真实验基于 Ubuntu 操作系统，硬件平台为 Intel(R) Core(TM) i9-12900K CPU 处理器、128 GB 内存、NVIDIA RTX 3090 显卡。代码运行环境为 Visual Studio Code 代码编辑器、Python 3.6.13、Tensorflow 1.15.0 和 Keras 2.3.1 等支持模块。

搭建 LightGBM 模型，并使用网格搜索法进行参数调优，LightGBM 模型参数设置见表 2。1D-CNN 模型结构包含一个输入层、一个一维或者二维卷积块、一个 Dropout 层、一个全连接层和一个输出层，CNN 模型参数设置见表 3，焦点损失函数参数设置见表 4。

表 2　LightGBM 模型参数设置

参数描述	参数设置
学习率	0.05
迭代次数	1 000
树最大深度	24
单棵树叶节点个数	490
最小叶节点样本数	39
叶节点样本权重之和	0.3
特征随机采样频率	0.6
样本随机采样频率	0.3
L1 正则化参数	0.08
早停轮次	50
交叉验证折数	5

表 3　CNN 模型参数设置

参数描述	参数设置
学习率	0.001
批量大小	512
训练周期	10
卷积层神经元数目	128
全连接层神经元数目	64

表 4　焦点损失函数参数设置

参数	参数设置
α	0.25
γ	2

3.2　实验数据集选取

仿真实验中，使用文献[34]中经过平衡化处理的 NSL-KDD 数据集模拟 MMSN 物理模型环境中的入侵检测数据流分布。文献[34]对原始 NSL-KDD 数据集的处理从数据源角度入手，有效地消除了 NSL-KDD 数据集的不平衡性，提高了分类器对其中少数类的检测能力。在本文仿真实验设计中，该数据集能够近似代表经过平衡化处理后的 MMSN 入侵检测数据集，同时排除数据不平衡的干扰，清晰、客观地验证了所提方法的性能。

NSL-KDD 数据集平衡前后的数据分布见表 5。其中，训练集为经过平衡化处理的 KDDTrain+子

集，测试集为KDDTest+子集。NSL-KDD数据集包含4类攻击数据，又可细分为39小类，其中22类仅在训练集中出现，而剩余17类仅在测试集中出现，即训练集与测试集数据样本类型分布不同。表5中的Normal表示正常数据，其余为4类攻击数据。

表5　NSL-KDD数据集平衡前后的数据分布

项目		Normal	Probe	DoS	U2R	R2L	总计
训练集	平衡前	67 343	11 656	45 927	52	995	125 973
		53.46%	9.25%	36.46%	0.04%	0.79%	100%
	平衡后	64 077	11 656	43 614	12 113	14 747	146 207
		43.83%	7.97%	29.83%	8.28%	10.09%	100%
测试集		9 711	2 421	7 458	200	2 754	

3.3　实验评估指标

为测试所提的MMSN入侵检测方法对分类器性能的提升，使用常用的分类算法评估指标对检测结果进行评估。实验中，真阳性（TP, true positive）、真阴性（TN, true negative）、假阳性（FP, false positive）和假阴性（FN, false negative）样本数目构成混淆矩阵，混淆矩阵见表6。

表6　　混淆矩阵

对比项	预测为攻击数据	预测为正常数据
实际为攻击数据	TP	FN
实际为正常数据	FP	TN

混淆矩阵是MMSN IDS分类器对各类型数据分类能力最基本、最直观的衡量方法。此外，使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）、假阳性率（FPR, false positive rate）、F1分数（F1-score）等常用指标进行评估。

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{5}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{6}$$

$$\text{Recall}(\text{TPR}) = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{7}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{8}$$

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{9}$$

以上指标中，准确率衡量分类器整体的攻击样本检测准确性；精确率、召回率和假阳性率衡量部分结果中分类器对网络攻击预测结果正确的比重；F1-score为精确率和召回率的调和平均数，兼顾二者性能，平衡精确率和召回率间的矛盾。最后，精确率-召回率（P-R, precision-recall）曲线和受试者工作特征（ROC, receiver operating characteristic）曲线也被用于所提方法的性能评估。

3.4　模型融合过程特征组合划分

系统训练过程中，考虑所使用的基学习器较少，为尽可能提高模型差异性以提高模型泛化能力，降低过拟合风险，增强整体融合效果，使用不完全相同的特征组合对模型进行训练。

对于平衡化后的NSL-KDD数据集，使用与文献[34]相同的数据预处理方法，将所得到的49维特征视作原始特征，本文所提的模型融合过程所使用的3组组合特征$F1$、$F2$、$F3$存在90%（37维）共有特征和10%（4维）独有特征，以弱化模型对于同质特征组合的依赖，每个特征组合各自包含41维特征。

在训练过程中，将部分特征重复使用能够降低过拟合风险，因此，在构建特征组合$F4$时，除了LightGBM对数据集预测所得到的5维特征，还加入了LightGBM中重要性评估模块所给出的，根据信息增益排序所得对模型分类贡献程度最大的3维原始特征。最终特征组合$F4$由49维特征组成。特征组合分布见表7。

表7　　特征组合分布

特征组合编号	$F1$	$F2$	$F3$	$F4$
特征维度	41	41	41	49

3.5　实验结果分析

在LightGBM模型的训练过程中，采用了K折（K-fold）交叉验证方法，K值取为5。5折交叉验证在一次训练后即获得5个不同的LightGBM模型，分别对数据集做出预测，并对预测结果取平均，该过程即完成了一次同质学习器的模型融合。数据集包含正常数据类型Normal和4种不同的攻击类型：Probe、DoS、U2R和R2L。交叉验证的方法能够充分利用训练集中的数据信息，使模型预测结果更稳健，提高模型泛化性并减少过拟合。

NSL-KDD数据集特征相对重要性如图6所示，展示了LightGBM模型内置的重要性评估模块对NSL-KDD数据集的49维特征基于特征增益的相对重要性排序。在文献[34]中，PCA降维处理保留了信息量最大的特征，因此LightGBM所给出的特征重要性排序基本符合序号排列，特征“1”“2”“0”（特征组合R）作为对模型分类贡献最大的特征被复制后加入原有特征组合，高重要性特征的重用一

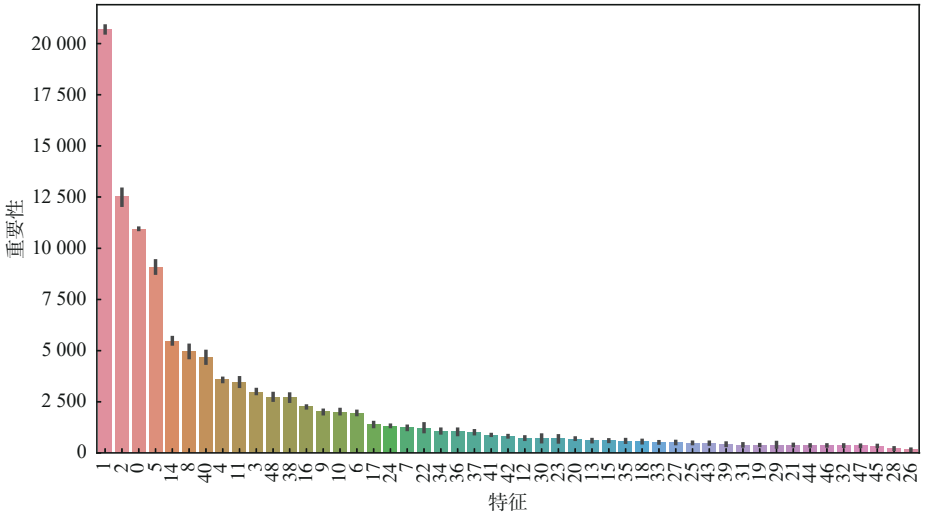


图6　NSL-KDD数据集特征相对重要性

定程度上减少了验证集上的训练误差，起到了减少过拟合的作用。

使用网格搜索法查找LightGBM最佳参数组合见表2，学习率设置为0.05，迭代次数为1 000，早停轮次为50，在实验中通常训练至500轮左右停止，由于数据集尺寸较大，树最大深度和单棵树叶节点个数分别设置为24和490。使用特征组合$F1$、$F2$分别训练使用焦点损失函数的LightGBM，并分别用训练完成的分类器对训练集和测试集进行预测，得到预测结果LGB1和LGB2。

预测结果LGB2评估指标见表8，显示了相同参数设置下，使用特征组合$F2$训练、使用多分类交叉熵函数作为损失函数的LightGBM，所得预测结果的评估分数。由第2.3节中对焦点损失函数的介绍可知，该函数作用于类分布不平衡的数据集，提高了对难分类样本的关注。在NSL-KDD数据集中，U2R类和R2L类作为极端少数类，在使用焦点损失函数（focal_loss）的情况下，精确率、召回率和F1分数3个指标的检测结果（加下划线部分）均明显优于传统的多分类交叉熵损失函数（categorical_crossentropy），模型整体检测准确率提升了0.44%，由此证明了本文所提算法对损失函数进行置换的必要性和有效性。

表8　　预测结果LGB2评估指标

	评估指标	Precision	Recall	F1-score	Accuracy
focal_loss	Normal	0.740 5	0.959 7	0.836 0	0.804 2
	Probe	0.758 2	0.839 3	0.796 7	
	DoS	0.960 0	0.821 3	0.885 2	
	U2R	0.593 2	0.175 0	0.270 3	
	R2L	0.737 8	0.224 8	0.344 6	
categorical_ crossentropy	Normal	0.775 7	0.959 0	0.857 7	0.799 8
	Probe	0.635 1	0.836 0	0.721 8	
	DoS	0.955 9	0.822 2	0.884 0	
	U2R	0.235 7	0.165 0	0.194 1	
	R2L	0.664 6	0.192 1	0.298 0	

本文所搭建的1D-CNN模型具体结构如第2.2节所述，模型参数设置见表3，学习率设置为0.001，批量大小为512，训练10个周期。使用特征组合$F3$对使用焦点损失函数的1D-CNN进行训练，得到预测结果CNN1，预测结果CNN1评估指标见表9。

表9　　预测结果CNN1评估指标

评估指标	Precision	Recall	F1-score	Accuracy
Normal	0.792 3	0.953 7	0.865 5	0.805 9
Probe	0.618 3	0.796 8	0.696 3	
DoS	0.934 5	0.827 8	0.877 9	
U2R	0.580 0	0.145 0	0.232 0	
R2L	0.719 9	0.281 8	0.405 0	

特征重用前后1D-CNN训练阶段焦点损失函数如图7所示，展示了使用特征组合$F3$与原始特征中前3维高重要性特征相结合所得的新特征组合，在其他参数设置相同的情况下训练1D-CNN，训练集和验证集焦点损失函数变化曲线对比。由图7可知，将部分特征重复使用后，训练集上的损失函数曲线几乎不变，而验证集上的损失函数则有所下降，各类别检测评估指标和模型检测准确率也变化不大，可知重复使用部分特征的确起到了提高模型泛化性的作用。为了避免过多重复特征出现而导致模型快速过拟合，模型融合中仅复制对分类器预测

贡献最大的 3 维特征（特征组合 R）进行重复使用。将预先得到的预测结果 LGB1 与特征组合 $F3$、R 相结合，得到特征组合 $F4$。

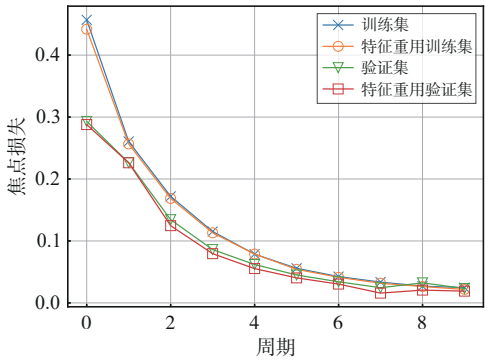


图 7　特征重用前后 1D-CNN 训练阶段焦点损失函数

本文所搭建的 2D-CNN 模型具体结构如第 2.2 节所述，模型参数设置见表 3。使用特征组合 $F4$ 训练分类器 2D-CNN，得到预测结果 CNN2，预测结果 CNN2 评估指标见表 10。由表 10 可知，经过特征组合，预测结果 CNN2 中 R2L 类在精确率、召回率和 F1 分数 3 项评估指标上均有明显提升。相较于 LGB2 分别提升了 18.80%、33.01% 和 34.37%，相较于 CNN1 分别提升了 16.68%、26.98% 和 27.51%。其他类各评估指标整体变化不大，但检测准确率相较于预测结果 LGB2 和 CNN1 分别提高了 1.91% 和 1.64%。

表 10　　预测结果 CNN2 评估指标

评估指标	Precision	Recall	F1-score	Accuracy
Normal	0.784 6	0.912 0	0.843 5	0.820 5
Probe	0.729 8	0.823 2	0.773 7	
DoS	0.902 9	0.817 6	0.858 1	
U2R	0.525 4	0.155 0	0.239 4	
R2L	0.886 7	0.551 6	0.680 1	

将预测结果 LGB2、CNN1 和 CNN2 加权融合，权重 w_1、w_2 和 w_3 分别为 0.3、0.2 和 0.5，即最终预测结果为 w_1LGB2 + w_2CNN1 + w_3CNN2。最终预测结果评估指标见表 11。

表 11　　最终预测结果评估指标

评估指标	Precision	Recall	F1-score	Accuracy
Normal	0.783 6	0.934 6	0.852 4	0.824 2
Probe	0.728 5	0.809 2	0.766 7	
DoS	0.923 3	0.818 6	0.867 8	
U2R	0.543 9	0.155 0	0.241 2	
R2L	0.879 6	0.512 0	0.647 2	

对预测结果 LGB2、CNN1、CNN2 和最终预测结果进行联合分析，表 8~表 11 中标红部分为数据集中每个类评估指标综合表现最优，标蓝部分为表现次优，标灰部分为表现最差。

由表 8 可知，LGB2 内对于 Probe、DoS 和 U2R 的检测均获得了最佳表现，但对于其他两类样本的检测表现欠佳；由表 9 可知，CNN1 获得了对于正常数据流的最佳检出表现，但其他类上的检测表现一般，推测正常数据较攻击数据更适用于时序特征的提取；由表 10 可知，特征组合 $F4$ 的应用以及空间特征的提取令 CNN2 获得对于少数类 R2L 检测的最佳表现；由表 11 可知，尽管模型融合后所得的最终预测结果没在任何一类样本的检测中获得最优，但在 Normal、U2R 和 R2L 类上均获得了次优表现，且检测准确率 82.42% 为 4 个系统中最优。此外，其他 3 份预测结果中均包含对至少一类样本的最差检测，而模型融合使得最终预测结果吸收了其他基学习器的优势而规避其劣势，系统整体稳健性更强。又由第 1.1 节所述可知，对少数类攻击样本准确检测是 MMSN IDS 的关键，也是系统优化的首要目标，因此，综合考虑认为模型融合后所得的最终预测结果获得了最好的表现。

最终预测结果混淆矩阵如图 8 所示，显示了即使模型融合方法相对有效地提高了系统对于少数类样本的检测能力，但由于原始训练集中所含样本过少（U2R 类为 52 个，R2L 类为 995 个），且训练集与测试集攻击类型分布不同，分类器对其的检测仍然受到数据集质量的限制。

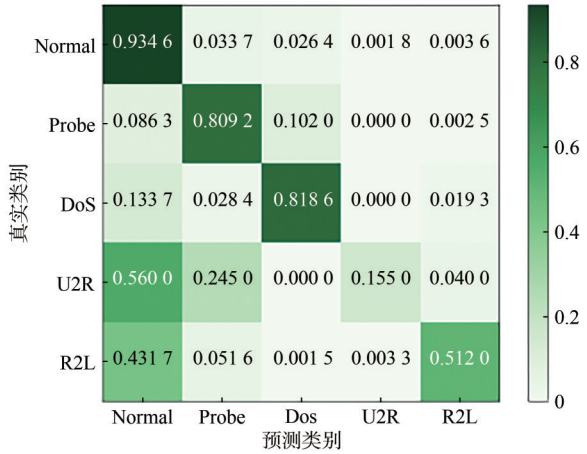
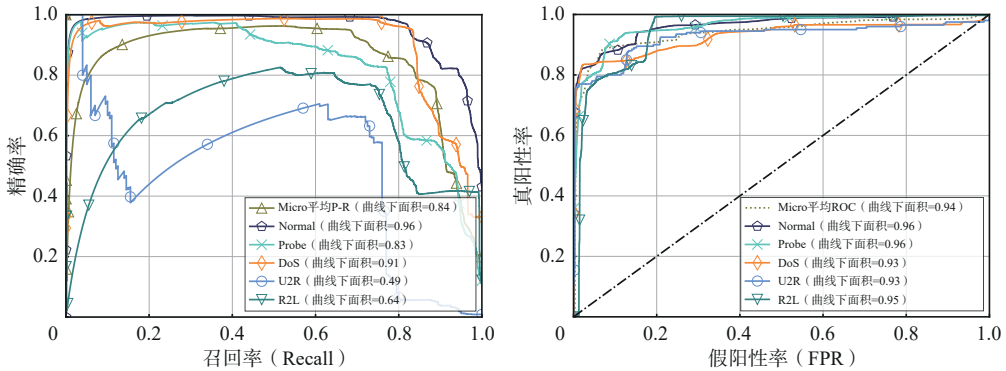


图 8　最终预测结果混淆矩阵

最终预测结果 P-R、ROC 曲线如图 9 所示，为最终预测结果的多分类 P-R 曲线和 ROC 右上角的程度判断分类器对于每一类样本的分类性能，本文所



(a) 最终预测结果P-R曲线　　(b) 最终预测结果ROC曲线

图9　最终预测结果P-R、ROC曲线

提的基于改进LightGBM-CNN的入侵检测算法在Normal、Probe和DoS类上均表现良好，而在少数类U2R和R2L上受实验所用NSL-KDD数据集质量影响表现稍逊。受到实验数据集不平衡特性及第3.2节中所述训练集、测试集数据攻击样本类型的不同分布影响，Micro平均P-R曲线下面积为0.84。根据图9(b)中ROC曲线下面积接近于1的程度判断分类器性能，各类别的ROC曲线下面积均达到较高水平，其Micro平均ROC曲线下面积为0.94。

DoS攻击下本文所提方法与其他实验评估指标对比见表12，为本文所提的模型融合算法在DoS攻击下的精确率、召回率、F1分数与基础方法深度神经网络（DNN, deep neural network）、ADASYN、SNGAN[40]、MAGNTO[41]、TACGAD-IDS[42]和TMG-IDS[43]算法的对比实验。由表12中的数据可知，本文所提算法在精确度和F1分数上都有较大的提升。与其中性能最好的MAGENTO相比精确率和F1分数分别提升了11.3%和0.88%，但是召回率方面存在明显不足，可知本文所提的入侵检测算法虽然达到了较好的性能水平，但仍然，有很大的提升空间。

表12　DoS攻击下本文所提方法与其他实验评估指标对比

算法	Precision	Recall	F1-score
DNN	0.739 0	0.912 4	0.816 6
ADASYN	0.636 4	0.826 6	0.719 8
SNGAN	0.772 9	0.923 0	0.841 3
MAGENTO	0.810 3	0.913 9	0.859 0
TAGGAD-IDS	0.806 4	0.929 8	0.863 7
TMG-IDS	0.794 4	0.912 9	0.849 6
本文所提算法	0.923 3	0.818 6	0.867 8

4　结束语

本文针对入侵检测任务在MMSN场景中所面临的新挑战，在对MMSN场景特点的研究的基础上，考虑从算法和分类器层面入手，对MMSN IDS分类器性能的提高方式进行研究，并提出了一种基于模型融合的MMSN入侵检测方法。同时使用卫星通信的方法完成部分子网络的设计。首先，该方法建立了改进损失函数的LightGBM、1D-CNN、2D-CNN分类器，使用焦点损失函数替换原始的多分类交叉熵函数，提高了模型对于难以分类的少数类样本的关注程度；其次，运用模型融合技术中的堆叠和平均思想，设计基于以上基分类器的模型融合方法，吸收基学习器优势而规避其劣势；最后，通过设计特征组合划分的方式——保留独有特征以及部分特征重复使用，以提高系统泛化性。仿真实验结果验证了本文所提方法的性能。本文仅对独立MMSN IDS在多分类尤其是少数类的检测性能提升方面展开研究，而MMSN作为大型综合网络体系，多个IDS的协同作用是未来的发展方向。因此，在未来的工作中，将考虑对分布式系统中IDS群的联合应用进行建模，探索系统检测精度和时间效率等性能指标的优化方案。

参考文献：

[1] 王利兵. “海洋中国”的人类学议题[J]. 东南学术, 2024(3): 119-128.
WANG L B. The anthropological issues of “maritime China”[J]. Southeast Academic Research, 2024(3): 119-128.

[2] 苏新, 张桂福, 行鸿彦, 等. 基于平衡生成对抗网络的海洋气象传感器网络入侵检测研究[J]. 通信学报, 2023, 44(4): 124-136.
SU X, ZHANG G F, XING H Y, et al. Research on intrusion detection for maritime meteorological sensor network based on balancing generative adversarial network[J]. Journal on Communications, 2023, 44(4): 124-136.

[3] LIU J M, GAO Y B, HU F J. A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM[J]. Computers & Security, 2021, 106: 102289.

[4] WANG L Y, ZHANG X M, LI D M, et al. Multi-sensors space and time dimension based intrusion detection system in automated vehicles[J]. IEEE Transactions on Vehicular Technology, 2024, 73(1): 200-215.

[5] LIU G Y, ZHAO H Q, FAN F, et al. An enhanced intrusion detection model based on improved KNN in WSNs[J]. Sensors, 2022, 22(4): 1407.

[6] KUMAR A, ABHISHEK K, GHALIB M R, et al. Intrusion detection and prevention system for an IoT environment[J]. Digital Communications and Networks, 2022, 8(4): 540-551.

[7] SHA K W, YANG T A, WEI W, et al. A survey of edge computing-based designs for IoT security[J]. Digital Communications and Networks, 2020, 6(2): 195-202.

[8] WANG W P, WANG Z R, ZHOU Z F, et al. Anomaly detection of industrial control systems based on transfer learning[J]. Tsinghua Science and Technology, 2021, 26(6): 821-832.

[9] XUE Y W, PAN J, GENG Y Y, et al. Real-time intrusion detection based on decision fusion in industrial control systems[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024, 2: 143-153.

[10] PEI W B, XUE B, ZHANG M J, et al. A survey on unbalanced classification: how can evolutionary computation help?[J]. IEEE Transactions on Evolutionary Computation, 2024, 28(2): 353-373.

[11] LIANG P, YAO Z D, JIAN L. Marine meteorological observation technology and application based on large floating platform[C]// Proceedings of the 2019 International Conference on Meteorology Observations (ICMO). Piscataway: IEEE Press, 2019: 1-4.

[12] LI Y, YANG P, SI H, et al. The integrated observation system for shore-based marine environment: a case from China[J]. IET Conference Proceedings, 2021, 2020(2): 78-83.

[13] ALGARNI A, ACARER T, AHMAD Z. An edge computing-based preventive framework with machine learning integration for anomaly detection and risk management in maritime wireless communications[J]. IEEE Access, 2024, 12: 53646-53663.

[14] HUO Y M, DONG X D, BEATTY S. Cellular communications in ocean waves for maritime Internet of things[J]. IEEE Internet of Things Journal, 2020, 7(10): 9965-9979.

[15] ULLAH I, QIAN S Y, DENG Z X, et al. Extended Kalman filter-based localization algorithm by edge computing in wireless sensor networks[J]. Digital Communications and Networks, 2021, 7(2): 187-195.

[16] SWAIN R R, KHILAR P M, DASH T. Multifault diagnosis in WSN using a hybrid metaheuristic trained neural network[J]. Digital Communications and Networks, 2020, 6(1): 86-100.

[17] HOUGHTON I A, SMIT P B, CLARK D, et al. Performance statistics of a real-time Pacific Ocean weather sensor network[J]. Journal of Atmospheric and Oceanic Technology, 2021, 38(5): 1047-1058.

[18] MOMBER A W, WILMS M, BRÜN D. The use of meteorological and oceanographic sensor data in the German offshore territory for the corrosion monitoring of marine structures[J]. Ocean Engineering, 2022, 257: 110994.

[19] MOLTMANN T, TURTON J, ZHANG H M, et al. A global ocean observing system (GOOS), delivered through enhanced collaboration across regions, communities, and new technologies[J]. Frontiers in Marine Science, 2019, 6: 291.

[20] BITTON R, SHABTAI A. A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1164-1181.

[21] TENG S H, WU N Q, ZHU H B, et al. SVM-DT-based adaptive and collaborative intrusion detection[J]. IEEE/CAA Journal of Automatica Sinica, 2018, 5(1): 108-118.

[22] HARUSH S, MEIDAN Y, SHABTAI A. DeepStream: autoencoder-based stream temporal clustering and anomaly detection[J]. Computers & Security, 2021, 106: 102276.

[23] YANG Z, LIU X D, LI T, et al. A systematic literature review of methods and datasets for anomaly-based network intrusion detection[J]. Computers & Security, 2022, 116: 102675.

[24] 张志飞, 刘峰, 葛祎阳, 等. 一种基于深度可分离卷积和注意力机制的入侵检测方法[J]. 物联网学报, 2023, 7(1): 49-59.
ZHANG Z F, LIU F, GE Y Y, et al. An intrusion detection method based on depthwise separable convolution and attention mechanism[J]. Chinese Journal on Internet of Things, 2023, 7(1): 49-59.

[25] DESHMUKH S, KHATIK V, SAXENA A. Robust fusion model for handling EMG and computer vision data in prosthetic hand control[J]. IEEE Sensors Letters, 2023, 7(9): 6004804.

[26] WU W T, XIA Y S, JIN W Z. Predicting bus passenger flow and prioritizing influential factors using multi-source data: scaled stacking gradient boosting decision trees[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(4): 2510-2523.

[27] WU B Y, QIU W R, JIA J X, et al. Landslide susceptibility modeling using bagging-based positive-unlabeled learning[J]. IEEE Geoscience and Remote Sensing Letters, 2021, 18(5): 766-770.

[28] KHAN P W, BYUN Y C. Optimized dissolved oxygen prediction using genetic algorithm and bagging ensemble learning for smart fish farm[J]. IEEE Sensors Journal, 2023, 23(13): 15153-15164.

[29] WANG S, CHANG J M. Privacy-preserving boosting in the local setting[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4451-4465.

[30] DONG M Q, YAO L N, WANG X Z, et al. Gradient boosted neural decision forest[J]. IEEE Transactions on Services Computing, 2023, 16(1): 330-342.

[31] 陈虹, 王瀚文, 金海波. 融合改进自编码器和残差网络的入侵检测模型[J]. 计算机工程, 2024, 50(2): 188-195.
CHEN H, WANG H W, JIN H B. Intrusion detection model combining improved self-encoder and residual network[J]. Computer Engineering, 2024, 50(2): 188-195.

[32] TANG Y, GU L, WANG L. Deep stacking network for intrusion

detection[J]. Sensors (Basel, Switzerland), 2021, 22(1): 25.

[33] CHEN C, SONG Y F, YUE S H, et al. FCNN-SE: an intrusion detection model based on a fusion CNN and stacked ensemble[J]. Applied Sciences, 2022, 12(17): 8601.

[34] 苏新, 田天, Ziyang Gong, 等. 基于异常行为的海洋气象传感器网络的入侵检测方法研究[J]. 通信学报, 2023, 44(7): 86-99.
SU X, TIAN T, GONG Z Y, et al. Research on intrusion detection method of marine meteorological sensor network based on anomalous behaviors[J]. Journal on Communications, 2023, 44(7): 86-99.

[35] ZHANG Z D, JUNG C. GBDT-MO: gradient-boosted decision trees for multiple outputs[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(7): 3156-3167.

[36] ZHANG Y M, YU W Q, LI Z Y, et al. Detecting Ethereum ponzi schemes based on improved LightGBM algorithm[J]. IEEE Transactions on Computational Social Systems, 2022, 9(2): 624-637.

[37] CUI X T, LI X S, ZHENG X L, et al. Driving behavior primitive classification using CNN-based fusion models[J]. IEEE Access, 2024, 12: 56344-56355.

[38] CHEN G C, QIN H B. Class-discriminative focal loss for extreme imbalanced multiclass object detection towards autonomous driving[J]. The Visual Computer, 2022, 38(3): 1051-1063.

[39] TIAN J, TSAI P W, ZHANG K, et al. Synergetic focal loss for imbalanced classification in federated XGBoost[J]. IEEE Transactions on Artificial Intelligence, 2024, 5(2): 647-660.

[40] MIYATO T, KATAOKA T, KOYAMA M, et al. Spectral normalization for generative adversarial networks[EB/OL]. arXiv preprint, 2018, arXiv: 1802.05957.

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

[42] DING H W, CHEN L Y, DONG L, et al. Imbalanced data classification: a KNN and generative adversarial networks-based hybrid approach for intrusion detection[J]. Future Generation Computer Systems, 2022, 131: 240-254.

[43] DING H W, SUN Y, HUANG N N, et al. TMG-GAN: generative adversarial networks-based imbalanced learning for network intrusion detection[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 1156-1167.

[作者简介]

张文潇（2000– ），女，河海大学信息科学与工程学院硕士生，主要研究方向为入侵检测、边缘/雾计算等。

苏新（1986– ），男，博士，河海大学信息科学与工程学院教授，主要研究方向为移动通信、边缘/雾计算、智慧海洋等。

顾依凌（2001– ），女，河海大学信息科学与工程学院硕士生，主要研究方向为入侵检测、边缘/雾计算、嵌入式系统等。