基于多粒度级联森林优化算法的网络入侵检测模型研究*

刘学朋，于东升，胡铁娜，李京儒，陈广勇，曲　洁
（公安部第三研究所网络安全等级保护中心，北京　100142）

摘　要：针对大规模网络入侵方式层出不穷，为应对多形态下的网络安全威胁，提出一种基于多粒度级联森林优化算法的网络入侵检测模型。首先对原始数据进行预处理，然后融合 Fisher Score 算法对不同特征信息进行权重选择排序，最后将其排序后的特征信息送入级联森林的卷积层和森林层，对特征信息进行深度表达和分类，从而得到精准的分类结果。经 KDD 99 数据集进行验证，在不同测试集占比为 90%、70% 和 30% 三组实验情况下，分别实现了 98.20%、99.00%、99.27% 的分类精度。实验结果证明，所提算法能够准确识别多种网络攻击，为现有网络入侵检测提供有效区分依据。

关键词：Fisher Score；随机森林；级联森林；网络入侵
中图分类号：TP391　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.11.002
引用格式：刘学朋，于东升，胡铁娜，等. 基于多粒度级联森林优化算法的网络入侵检测模型研究［J］. 网络安全与数据治理，2024，43(11)：7-12.

Research on network intrusion detection model based on multi-granularity cascaded forest optimization algorithm

Liu Xuepeng, Yu Dongsheng, Hu Tiena, Li Jingru, Chen Guangyong, Qu Jie
(Network Security Level Protection Center of the Third Research Institute of the Ministry of Public Security, Beijing 100142, China)

Abstract: To address the ever-evolving and diverse nature of large-scale network intrusions and the subsequent cybersecurity threats, this paper proposes a network intrusion detection model based on the Multi-Granularity Cascaded Forest (GCForest). The model initially preprocesses raw data, subsequently incorporates the Fisher Score algorithm to rank different feature information by their weights, and ultimately feeds the ranked feature information into the convolutional layer and forest layer of the cascaded forest for deep feature expression and classification, thereby achieving precise classification results. Validation using the KDD 99 dataset demonstrates that under three experimental scenarios with training set proportions of 90%, 70%, and 30%, the model achieves classification accuracies of 98.20%, 99.00%, and 99.27% respectively. The experimental results prove that the proposed algorithm in this paper can accurately identify various network attacks, providing an effective basis for distinguishing and detecting network intrusions in existing systems.

Key words: Fisher score; random forest; cascade forest; network intrusion

0　引言

随着大数据和云计算等信息技术的不断发展和应用，网络攻击方式层出不穷，攻击者往往对特定网络进行匿名攻击，从而导致网络崩溃[1-2]。网络入侵检测作为网络安全的重要组成部分，它是根据网络流量数据以及各种 IDS 数据判断主机正常行为或异常行为，以便在网络攻击出现时做出相应策略。现有入侵检测方式主要分为传统机器学习和深神经网络，针对入侵检测数据的高维因素，检测算法的精度和效率成为了研究热点。

传统机器学习入侵检测算法模型研究中，Lin 等人[3]提出了一种融合了主成分分析与随机森林技术的入侵检测算法，该算法首先通过主成分分析算法对输入的原始数据特征进行高效降维处理，以去除冗余信息并保留关键特征，随后采用随机森林算法对这些降维后的特征进

*基金项目：基本科研业务费专项资金项目（KYC24363）

行分类识别。这种结合策略显著提升了检测的准确率，实现了对潜在入侵行为的有效甄别，但忽略了奇异值对特征表达影响因素，进而造成误检、漏检的出现。Wang 等人[4]在应对高维数据挑战时，引入了 One-R 快速属性选择机制来优化随机森林模型。此方法不仅缓解了随机森林在选择属性时因过度随机性导致的效率瓶颈，还有效减少了误检与漏检的发生，提升了系统性能。另一方面，Hu 等人[5]则结合 Snort 的传统机器学习能力与随机森林的离群点检测优势，设计了一种混合入侵检测系统。该系统在保持高检测率的同时，也实现了低误报率，展现了良好的检测效能。然而，值得关注的是，文献［4－5］所提出的方法在特征处理上存在一定的局限性，它们未能充分考虑特征的物理含义，从而限制了通过正则化表达来进一步筛选和优化有效特征的可能性。

在深神经网络应用于入侵检测的领域研究中，Ren 等人[6]创新性地结合了 KNN 算法预处理离散特征，并与多层次随机森林模型相结合，成功在 KDD CUP99 数据集上高效识别出 Probe、U2R、R2L 等多种网络攻击类型。另一项研究中，Ren 等人[7]则构建了一个融合随机森林与 K 均值算法的混合入侵检测系统，该系统在提升检测准确性的同时，也保持了较低的误检率。然而，值得注意的是，无论是文献［6］还是文献［7］中的方法，均未充分重视数据中的冗余特征问题，它们主要聚焦于模型精度的提升，却在一定程度上忽视了模型的鲁棒性构建。这意味着，尽管这些模型在特定数据集上表现出色，但在面对非特定或未知数据集时，可能会遭遇误检和错检的风险增加。Gou 等人[8]在研究中尝试通过引入随机性机制来减轻冗余特征对随机森林模型检测性能的负面影响，这一策略确实在一定程度上提升了模型的检测效果。然而，这种随机选择特征的方法也伴随着潜在的风险，即有可能在减少冗余特征的同时，不经意地削弱了有效特征的表达力，进而对模型的最终检测结果准确性造成不利影响。

上述研究主要集中在模型检测精度提升，但忽略了特征有效表达不充分和冗余特征干扰等问题。此外，针对入侵检测真实场景下的数据集不平衡问题并未对训练数据占比进行深入对比研究，不能有效衡量检测模型是否具有较强鲁棒性。

基于此，本文提出了一种多粒度级联森林优化算法的网络入侵检测模型，对源数据进行归一化预处理，避免奇异值特征在计算过程种造成误差，然后通过 Fisher Score 法对特征进行排序选择，从而获得特征子集，将特征子集作为特征数据传输给卷积层，利用卷积计算特性对其特征进行深度挖掘，将挖掘信息通过级联层森林对其分类，进而有效识别复杂多变的网络攻击。实验结果表明，本文算法在入侵检测过程具有较高的准精确率和较低的误检率，相对传统算法有一定优势。

1　多粒度级联森林优化算法入侵检测模型

本文提出了一种多粒度级联森林优化算法入侵检测模型，其流程如图 1 所示，该模型涵盖了五个核心处理节点。首先，数据预处理阶段是第一步，旨在对源数据中的奇异值及其他不规则异常进行标准化和归一化处理，以确保数据的一致性和可分析性。其次，特征工程阶段融入 Fisher Score 算法，对特征进行选择、排序和剔除等操作，该过程在不影响有效特征信息表达的前提下，能有效剔除冗余信息下的无关特征，仅保留类内类间方差权重较高，影响分类识别精度的关键特征信息特征。同时在建模及评估过程中，会对数据标签进行独热编码，并将其处理后的数据输入至训练模型中，通过反复的迭代与优化，使得模型能够准确地表达入侵特征信息。最终，利用训练好的模型对原始流量攻击类型进行分类，实现对网络入侵类型的有效识别。

2　实验步骤

2.1　预处理

预处理的目的是为了确保数据处理和分析过程中深层次地展示数据特性[9]，在不削弱有效特征的前提下清除数据中的噪声、不一致性和冗余等信息，以确保后续分析使用的数据是干净、准确的，真实有效表达模型预测能力。

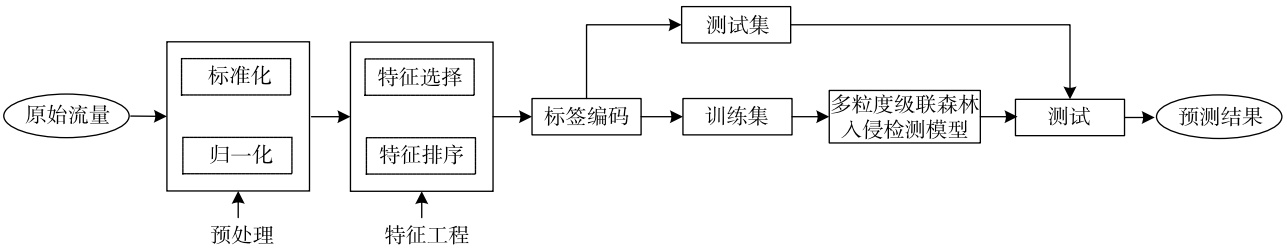

图 1　多粒度级联森林优化算法入侵检测流程图

2.1.1 标准化、归一化

本实验选用的是 KDD 99 入侵检测数据集，该数据集具有类间信息关联度小、类内信息关联度大等特性，上述特性将导致不同类别之间的数据特征差异较大，增加模型识别和区分不同类别的难度。同时类间信息关联度过小，导致在预测新数据时，尤其是当新数据点接近于类别边界时，模型的预测准确性会下降。为了提高类间特征方差，减少类内特征方差，对其源数据进行标准化处理，进而提高模型性能和准确性。具体如式（1）所示：

$$x' = \frac{x - \bar{x}}{s} \tag{1}$$

同时，为了加快模型训练，减少数据的偏差，还对其标准化数据进行了归一化处理，将其特征信息控制在［0，1］间，削弱奇异值干扰。具体如式（2）所示：

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{2}$$

2.1.2 特征选择、排序

特征选择作为特征工程的重要环节，能够剔除冗余特征以及相关性较弱的特征，捕捉数据中的关键信息，增强模型预测结果的解释性[10]，避免高维数据中出现“维度灾难”，推动模型迭代有效特征信息并充分表达，降低模型对特征信息的计算时间和复杂度。

近年来，多数研究学者尝试使用多标记特征选择算法方式对其有效特征和冗余特征进行区分，本质上是利用最大相关项和最小冗余性，类似于类内特征排序，忽略了特征间的信息相关性，导致特征间相关性较高的特征被削弱。

因此，本文采用 Fisher Score 算法对 KDD 99 入侵检测数据进行特征选择，通过计算每个特征的类间方差（反映不同类别之间的差异）与类内方差（反映同一类别内部的差异）的比值，筛选出 KDD 99 入侵检测数据集最具鉴别能力的特征子集，并对其特征子集进行重组排序，改善特征选择的有效性和合理性，降低过拟合风险，促进入侵检测模型能更好地理解源数据。

其中，Fisher Score 特征选择算法分为过滤式选择、包裹式选择和嵌入式选择，本文采用的是过滤式选择，过滤式 Fisher Score 特征算法能够多尺度地划分子空间，去除冗余性较大的特征，进而得到新的重组排序特征。过滤式 Fisher Score 计算如式（3）所示：

$$J_{\text{fisher}}(k) = \frac{x_B^{(k)}}{x_W^{(k)}} \tag{3}$$

其中，$J_{\text{fisher}}(k)$ 为定义第 k 个特征在数据集上的 Fisher Score；$S_B^{(k)}$ 为第 k 个特征在数据集上的类间方差，$S_W^{(k)}$ 为第 k 个特征在数据集上的类内方差，如式（5）所示；在本文中，入侵检测源数据的 k 特征个数分别为 41。

$$s_B^{(k)} = \sum_{i=1}^{c} \frac{n_i}{n} (m_i^{(k)} - m^{(k)})^2 \tag{4}$$

其中，n 表示样本数，这里为 5 类，$n=5$；n_i 表示第 i 类样本的个数，本文选取的 KDD 99 数据集 1 类数据 391 458 条，2 类数据 4 107 条，3 类数据 1 126 条，4 类数据 52 条，共 494 021 条；$m_i^{(k)}$ 表示第 i 类样本在第 k 个特征上的取值的均值；$m^{(k)}$ 表示所有类别的样本在第 k 个特征上的取值的均值。

$$s_W^{(k)} = \frac{1}{n} \sum_{i=n} \sum_{x \in \omega_i} (x^{(k)} - m_i^{(k)})^2 \tag{5}$$

其中，$x^{(k)}$ 表示样本 x 在第 k 个特征上的取值。

由式（3）可知，类间方差越大，类内方差越小，Fisher Score 就越大，其特征在模型训练中权重越高，特征表达越充分。

图 2 和表 1 分别为 KDD 99 数据集 Top 30% 特征占比趋势和特征占比权重 Top 30% 特征值。表 1 中，通过 Finsher Score 算法类内与类间方差计算得知，diff_ srv_ rate、dst_ host_ diff_ srv_ rate、srv_ diff_ host_ rate 等特征在全部特征中权重占比最高，分别为 31.39%、14.97% 和 12.89%；而其余特征 flag、land、wrong_ fragment 等 17 个特征参数权重占比为 0%，可推测此类特征参数在 KDD 99 入侵检测数据集中为冗余特征，此类特征会占用模型对其有效特征表达权重，干扰有效特征的准确表达。因此，准确的特征子集不仅能够有效增强特征的可解释性，还能提高模型的鲁棒性，较好地识别网络攻击类型。

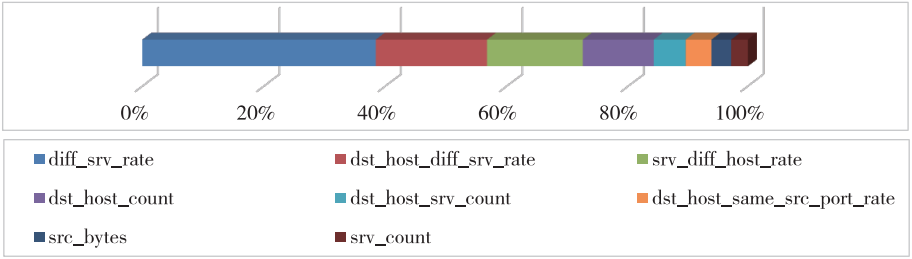

图 2　KD D99 30% 特征 Finsher Score 占比图

表 1　KDD 99 30% 特征 Finsher Score 值

序号	特征	Finsher Score/%
01	diff_ srv_ rate	31. 39
02	dst_ host_ diff_ srv_ rate	14. 97
03	srv_ diff_ host_ rate	12. 89
04	dst_ host_ count	9. 56
05	dst_ host_ srv_ count	4. 37
06	dst_ host_ same_ src_ port_ rate	3. 53
07	src_ bytes	2. 70
08	srv_ count	2. 29

2.2　多粒度级联森林入侵检测模型

该部分为多粒度扫描级联森林模型，用于原始流量入侵检测数据攻击类型预测。针对预处理、特征选择和特征排序处理后源数据仍存在的数据类比不平衡、类间特征表达不充分等问题，本文提出一种基于多粒度级联森林优化算法的网络入侵检测模型，通过多粒度级联森林的卷积结构对其类间有效特征进行多尺度表达，挖掘有效特征类内、类间的特征信息，提升入侵检测数据攻击类别预测的准确性，降低误检、错检的发生；通过级联森林的级联结构改善数据类比不平衡，增强多粒度级联森林优化算法模型的鲁棒性。具体多粒度级联森林优化算法检测模型如图 3 所示。

由图 3 多粒度级联森林优化算法检测模型可知，该算法由左右两部分组成。第一部分为多粒度扫描结构，是通过滑动窗口对输入数据进行多粒度扫描，生成多个子样本，并利用随机森林（完全随机森林和普通随机森林）对子样本进行特征提取，生成丰富的特征表示。此算法类似于卷积神经网络（Convolutional Neural Networks，CNN）中的滑动窗口机制，本文是将 Finsher Score 特征选择后的初始化子集作为特征数据传输给卷积层，利用卷积计算特性通过滑动窗口对其特征进行深度挖掘。第二部分为级联森林，将挖掘信息拼接，借助级联层森林对其不同层间的特征学习，并输出新的特征表示，进而有效识别攻击类型。具体步骤如下：

（1）确定滑动窗口大小：本文源数据特征数为 41 个，分别设置了大小为 10、20 和 30 的三组窗口对源数据特征进行扫描。

（2）滑动窗口采样：根据三组窗口大小，分别为不同滑动窗口设置了步长为 1、2 和 3 的模型参数，对其源数据特征进行上采样，生成多个特征子样本。具体计算公式如（6）所示：

$$k = (n - r) / c + 1 \tag{6}$$

其中，k 为样本的计算个数，n 为样本长度，r 为滑动窗口大小，c 为步长。

（3）随机森林训练：对于每个子样本，分别训练两个随机森林，完全随机森林（completely-random tree forest），用于随机选择一个特征在树的每个节点进行分割，直到满足停止条件；普通随机森林（random forest），用于在分裂时从随机选择的特征子集中选择最优分裂特征。

（4）特征向量生成：每个子样本在两个随机森林训练下会得到类别概率向量，将所得类别概率向量与源数据特征进行拼接，生成一个高维的特征向量，并将其作为级联层的输入数据。

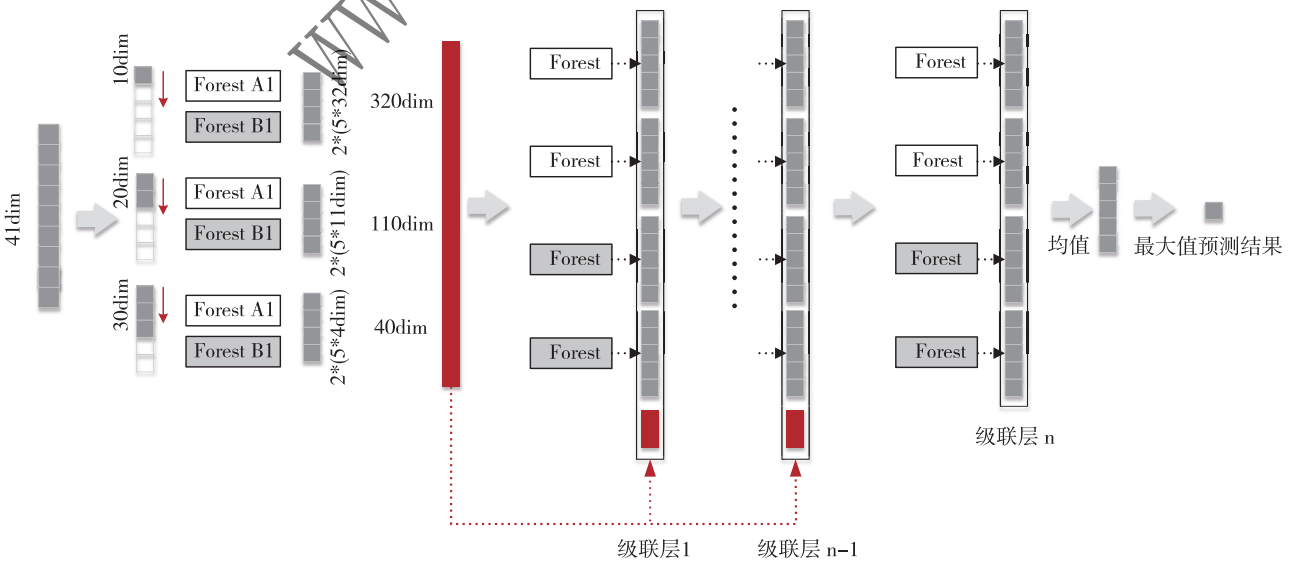

图 3　多粒度级联森林优化算法检测模型

（5）构建级联层：在级联结构中，不同级联间的层数具有数据共享的优势，当上一层数据处理完成之后，将作为下一层级联的输入，并且将上一层与下一层的信息进行融合，得到新的特征。

（6）自适应层数确定：将新的特征再次进行层与层之间的循环，保证每一层深林与深林之间的数据得到增强。

（7）预测结果输出：实现源数据特征的深层表达，进而对其源数据特征实现分类。

3 实验分析

3.1 数据库

本文采用 KDD 99 数据集中 10% 的数据子集作为试验数据，共 494 021 条数据[11-12]。该数据集是目前网络入侵检测中所使用的比较权威的公共数据集，共有 9 个分类变量和 32 个连续型变量。目标变量有 5 个类别，分别为正常（Normal）、提权攻击（User to Root，U2R）、远程权限获取（Remote to Local，R2L）、端口扫描（Probe）、拒绝服务攻击（Denial of Service，DoS）。具体数据类别占比如表 2 所示：

表 2 KDD 99 数据集

	Normal	U2R	R2L	Probe	DoS
数据量	97 278	52	1 126	4 107	391 458
占比/%	19.69	0.01	0.23	0.83	79.24

由表 2 可知，KDD 99 数据集存在明显数据不平衡现象，不同攻击类比数据占比权重相差较大，如 U2R 攻击类别仅占比全部数据的 0.01%，将导致多粒度级联森林优化算法检测模型在训练过程中缺少对 U2R 等特征的标记，进而模型鲁棒性不足，出现对新数据 U2R 攻击类型原始流量预测不准确等现象。因此，增加不同特征类内和类间的特征信息挖掘尤为重要，能够有效改善特征占比权重低的情况下对其有效特征的多尺度表达。

3.2 评价指标

本文在验证不同数据集下模型精度时，借助混淆矩阵对比各类的预测与真实值。混淆矩阵如表 3 所示。

表 3 混淆矩阵

	预测正常	预测异常
实际正常	TP	FN
实际异常	FP	TN

其中，TP 代表真实类和预测类均为正的个数，TN 代表真实类和预测类均为反的个数，FP 代表真实类为反但预测类为正的个数，FN 代表真实类为正但预测类为反的个数[13]。通过上述指标计算准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 F1。具体计算公式如下：

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{7}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{8}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{9}$$

$$F1 = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}} \tag{10}$$

3.3 实验结果及对比分析

为验证本文模型具有较好的鲁棒效果，分别在实验过程设置了三组不同比例的训练集和测试集，以验证该模型的检测效果。其中，测试集占比分别为 90%、70% 和 30% 三组不同比例，检测模型的测试结果如表 4 所示。

表 4 不同测试集占比下的检测结果

测试集占比/%	TP	TN	FP	FN	Accuracy/%	Precision/%	Recall/%
90	19 381	80 251	909	909	98.20	95.52	95.52
70	15 389	62 732	392	392	99.00	97.52	97.52
30	6 641	26 933	123	123	99.27	98.18	98.18

由表 4 可知，本文模型在三组不同测试集占比情况下，识别精度均保持在 98.83% 左右。三组实验中，通过 Finsher Score 特征选择选择，削弱冗余特征，结合多粒度扫描的卷积特征，依旧保持 1.2% 误检率，能够较好地对不同类别的网络入侵特征进行识别，其类内及类间多尺度入侵特征信息不仅对多粒度扫描的多尺度信息获取发挥黑盒作用，对模型的级联森林预测也提供了充足特征依据，验证了文中提出的多粒度级联森林优化算法网络入侵检测模型，具有一定的可行性。

上述对比实验中，分别从数据占比和模型优势两个角度验证本文算法对入侵事件准确识别的有效性。为进一步突出本文算法的优势，与传统算法和深度学习算法分别进行了比较，如表 5 所示。

表 5 本文算法与其他算法相比（%）

机器学习算法		深度学习算法	
算法	准确率	算法	准确率
文献［3］	90.30	文献［6］	95.47
文献［4］	99.80	文献［7］	95.00
文献［5］	95.00	文献［8］	99.95
本文算法	98.20	本文算法	98.20

由表5可知，与传统算法的对比，文献［3］使用主成分分析算法对源数据特征进行降维，但忽略了奇异值对特征表达影响因素。文献［4］使用One-R快速属性选择来解决高维数据时随机森林模型在选择属性时过度随机，采用200条数据进行测试验证，检测精度相对较高，但不能较好体现其模型的鲁棒性。文献［5］利用Snort的传统机器学习进行检测，忽略了冗余特征对类内类间有效特征的影响，不能对有效特征进行正则表达。以上算法均未对现实场景中多个关键特征来决定整体的预测方向进行进一步优化。

与深度学习算法的相比，文献［6］通过使用KNN法削弱离散特征后再结合多层次随机森林来检测网络攻击的方法。文献［7］利用随机森林和K均值算法进行异常检测构建了一个混合入侵检测系统，一定程度上提高了准确率并维持较低的误检率，但均忽略了真实场景下对源数据冗余特征分析的存在，通过调节模型参数提高检测精度，无法具有较好的鲁棒性。文献［8］通过引入随机性来降低冗余特征对模型检测的影响，在小数据量的基础上模型具有较好的识别精度，但上述算法均为对其特征的类内和类间特征进行相关性计算，仅对其固定数据具有较好的识别精度，当冗余特征超过一定限度，其模型鲁棒性可能随之下降。

实验结果表明，本文提出的多粒度级联森林优化算法的网络入侵检测模型，通过对源数据进行归一化预处理，避免奇异值特征在特征计算过程种造成误差，然后通过Fisher Score法对特征进行排序选择，去除冗余及类内和类间值较低的特征，保留权重较高的特征，利用卷积计算特性对其特征进行深度挖掘，将挖掘信息通过级联层森林对其分类，识别真实场景下复杂多变的网络攻击，具有较高的准确率和较低的误检率，相对现有对比算法具有一定优势。

4　结论

本文提出的基于多粒度级联森林优化算法的网络入侵检测模型，通过Fisher Score优化算法整合多粒度学习机制与级联森林的强大分类能力，不仅有效提升了对未知和复杂网络攻击行为的识别精度，还显著增强了系统的鲁棒性和泛化能力，改善了真实数据不平衡，模型鲁棒性低，导致的误检率高等问题。

随着网络技术的不断发展和网络攻击手段的日益翻新，将继续深化对该模型的研究与优化，包括但不限于引入更先进的特征选择方法、动态调整模型参数以适应实时变化的网络环境，以及探索与其他机器学习或深度学习技术的融合应用，为构建更加安全、可靠的网络空间贡献智慧与力量。

参考文献

［1］AXELSSON S. Research in intrusion-detection systems: a survey［R］. Technical report 9817. Department of Computer Engineering, Chalmers University of Technology, 1998.

［2］KWON D, KIM H, KIM J, et al. A suoey of deep learning-based network anomaly detection［J］. Cluster Computing, 2017: 1－13.

［3］林伟宁，陈明志，詹云清，等. 一种基于PCA和随机森林分类的入侵检测算法研究［J］. 信息网络安全，2017（11）：50－54.

［4］王翔，胡学钢，杨秋洁. 基于One-R的改进随机森林入侵检测模型研究［J］. 合肥工业大学学报（自然科学版），2015，38（5）：627－630，711.

［5］胡宏，陈彦萍. 基于随机森林算法的混合入侵检测系统研究［J］. 西安文理学院学报（自然科学版），2013，16（3）：68－71.

［6］任家东，刘新倩，王倩，等. 基于KNN离群点检测和随机森林的多层入侵检测方法［J］. 计算机研究与发展，2019，56（3）：566－575.

［7］任晓芳，赵德群，秦健勇. 基于随机森林和加权K均值聚类的网络入侵检测系统［J］. 微型电脑应用，2016，32（7）：21－24.

［8］苟继军，李均华，陈晨，等. 基于随机森林的网络入侵检测方法［J］. 计算机工程与应用，2020（2）：82－88.

［9］黄沛. 过滤式无监督特征选择算法研究［D］. 广州：华南理工大学，2023.

［10］刘荣烨. 最大相关最小冗余的无监督特征选择算法的研究及其应用［D］. 青岛：中国海洋大学，2024.

［11］MOORTHY M, SATHIYABAMA S. A study of intrusion detection using data mining［C］//IEEE International Conference on Advances in Engineering, Science and Management. IEEE, 2012：8－15.

［12］PRIYALAKSHMI V, DEVI R. Analysis and implementation of normalisation techniques on KDD'99 data set for IDS and IPS［J］. 2023. DOI：10. 1007/978－981－19－6634－7_ 5.

［13］JIANG Z, ZHOU C. Application of multi-objective differential evolution algorithm in computer network intrusion detection system［J］. Procedia Computer Science, 2023, 228：1059－1067.

（收稿日期：2024－09－14）

作者简介：

刘学朋（1996－），男，硕士研究生，主要研究方向：网络安全、入侵检测。

于东升（1975－），男，硕士研究生，主要研究方向：网络安全、等级保护。

曲洁（1978－），通信作者，女，硕士研究生，副研究员，主要研究方向：网络安全。E-mail：qujie@ gass. cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部