DOI:10.19651/j.cnki.emt.2518661

基于 CPO-BiLSTM-KAN 的网络恶意流量检测方法研究*

刘凤春 王子贺 杨爱民 袁书娟 孔闪闪
(华北理工大学理学院 唐山 063210)

摘 要:随着网络攻击手段的多样化和流量特征的复杂化,网络恶意流量的检测面临着越来越严峻的挑战。传统的流量检测方法在准确性和可靠性方面逐渐无法满足现代网络环境的需求,尤其是在高维数据和复杂攻击模式的情况下。为解决上述问题,本文提出了一种基于冠豪猪优化算法、双向长短期记忆网络和 Kolmogorov-Arnold 网络的网络恶意流量检测模型。该模型利用双向长短期记忆网络捕捉流量数据的双向时序特征,结合 Kolmogorov-Arnold 网络的非线性映射增强特征表达能力,并通过冠豪猪优化算法优化超参数提升模型性能。采用 CIC UNSW-NB15 增强数据集进行实验,实验结果表明,模型在二分类和多分类任务中准确率分别达到 99.12%和 94.15%,显著优于其他模型。此外,模型在应对类别不均衡时,特别增强了对 Backdoor 和 Worms 等少数类样本的检测能力。

关键词:恶意流量检测;双向长短期记忆网络;Kolmogorov-Arnold 网络;冠豪猪优化算法
中图分类号:TP393;TN918.4 **文献标识码**:A **国家标准学科分类代码**:520.2090

Research on the detection method of network malicious traffic based on CPO-BiLSTM-KAN

Liu Fengchun Wang Zihe Yang Aimin Yuan Shujuan Kong Shanshan
(College of Science, North China University of Science and Technology, Tangshan 063210, China)

Abstract: With the diversification of network attack means and the complication of traffic characteristics, the detection of network malicious traffic is facing increasingly severe challenges. Traditional traffic detection methods gradually fail to meet the needs of modern network environments in terms of accuracy and reliability, especially in the case of high-dimensional data and complex attack patterns. To address the above issues, this paper proposes a network malicious traffic detection model based on the Crested Porcupine Optimization Algorithm, Bidirectional Long Short-Term Memory Network, and Kolmogorov-Arnold Network. The model uses the Bidirectional Long Short-Term Memory Network to capture the bidirectional temporal features of traffic data, combines the nonlinear mapping of the Kolmogorov-Arnold Network to enhance feature expression capabilities, and optimizes hyperparameters through the Crested Porcupine Optimization Algorithm to improve model performance. Experiments are conducted using the CIC UNSW-NB15 enhanced dataset. The experimental results show that the model achieves accuracies of 99.12% and 94.15% in binary classification and multi-classification tasks, respectively, significantly outperforming other models. In addition, when dealing with class imbalance, the model particularly enhances the detection capability for minority class samples such as Backdoor and Worms.

Keywords: malicious traffic detection; bidirectional long short-term memory network; Kolmogorov-Arnold network; crowned porcupine optimization algorithm

0 引 言

随着网络攻击手段的不断演进,传统的网络流量检测方法面临着前所未有的挑战。网络攻击类型的多样化和恶意活动手段的复杂化,导致传统检测模型在准确性和可靠性方面难以满足现代网络环境的需求[1]。在 2024 年《网络

收稿日期:2025-04-23
* 基金项目:河北省网络信息安全及风险防范综合治理研究(20230203095)项目资助

空间安全科技热点回眸》报告中指出,全球网络空间安全形势依然严峻,各种新兴威胁和技术挑战层出不穷,尤其是高级持续性威胁攻击和勒索攻击的频发,严重威胁着全球网络空间安全[2]。与此同时,网络流量模式的复杂性以及大规模数据的急剧增长,使得流量检测系统的工作变得愈加困难。因此,开发一种既能保持高效性,又能准确识别恶意流量的先进检测模型,显得尤为重要[3]。

近年来,深度学习技术在恶意流量检测中展现了巨大的潜力,卷积神经网络(convolutional neural network,CNN)发挥着重要作用。特别是循环神经网络(recurrent neural network,RNN)及其变种——长短期记忆网络(long short-term memory,LSTM)[4],这些模型因能够捕捉时间序列数据中的时序依赖关系而备受关注。研究人员广泛探索将深度学习、特征融合与群智能优化算法引入恶意流量检测技术中,以提升模型的表达能力与泛化性能,并取得了一定成果。

在基于深度学习检测方面,深度学习模型在恶意流量检测中展现出强大的时序建模与特征学习能力。LSTM 及其变体双向长短期记忆网络(bidirectional long short-term memory,BiLSTM)因擅长捕捉流量数据的时序依赖关系被广泛应用。Jiang 等[5]提出并行 CNN-LSTM 结构,同时提取空间与时间特征,有效提升了检测精度。Bamber 等[6]结合递归特征消除与 CNN-LSTM 模型,在 NSL-KDD 数据集上实现 95%的准确率和 94%的 F1 分数。倪志伟等[7]提出基于改进生成对抗网络和混合时空神经网络的入侵检测模型,提高了检测准确率。此外,Volpe 等[8]结合 LSTM 与佩特里网实现实时攻击检测,Yang 等[9]使用 BiLSTM 与注意力机制提升了关键特征关注能力。

特征融合与非线性映射技术也得到了深入研究。戚子健等[10]构建双向门控循环单元与 CNN 并行结构,并结合注意力机制在多分类任务中获得 99.77%的准确率。Shi 等[11]提出融合双向编码器表示转换与 LSTM 的模型,捕捉全局上下文与时序关系。刘拥民等[12]设计堆叠自编码器与 Wasserstein 生成对抗网络结构,以堆叠自编码器进行特征压缩、Wasserstein 生成对抗网络实现少数类扩展,显著提升模型的特征判别能力。Liu 等[13]提出的 KAN 网络(Kolmogorov-Arnold networks,KAN)在特征增强方面具有提高。陈万志等[14]提出基于特征耦合泛化的异常检测方法,通过基于密度的噪声应用空间聚类去噪、最小冗余最大相关特征排序及贝叶斯优化随机森林,在 NSL-KDD 数据集上实现 91.79%的准确率。

在超参数优化与动态调整策略上,研究人员也进行了诸多尝试。在复杂网络结构下,超参数配置对模型性能具有决定性影响[15]。粒子群优化算法(particle swarm optimization,PSO)、遗传优化算法(genetic algorithm,GA)、冠豪猪优化算法(crested porcupine optimizer,CPO)以及鹈鹕优化算法(pelican optimization algorithm,POA)等被广泛应用。Kishore 等[16]使用混沌粒子群优化对 BiLSTM 进行调参,在车联网环境中检测率达 99.94%。Barik 等[17]提出加权条件逐步对抗网络与 PSO 融合框架,将粒子群优化与对抗训练结合,应对对抗样本风险。Kayyidavazhiyil 等[18]通过增强遗传算法进行特征选择,提升多模型检测精度。Papalkar 等[19]提出结合乌鸦搜索算法和灰狼优化算法对 CNN 超参数进行优化,在 MNIST 和 CIFAR-10 数据集上分别达到了 98.9%和 91.5%的准确率,表现优于传统优化方法。彭菲桐等[20]提出基于 GA 优化 CNN-LSTM 组合网络的轨道电路故障诊断方法,通过 GA 搜索最优网络结构与参数,使故障识别率提升至 99.28%。

尽管现有网络恶意流量检测研究在结构设计、特征提取和优化算法应用上成果显著,但仍面临关键挑战。多数深度学习模型采用单向 LSTM 或简单时序结构,对攻击流量前后依赖关系建模不足,识别复杂行为序列效果差;特征融合方法多为线性或静态权重机制,难以刻画高维流量数据的非线性关联,适应多样化攻击模式能力弱;部分研究虽引入优化算法调整模型参数,但这些方法常陷入局部最优、搜索精度有限、依赖初值,与深度模型融合不深,无法实现结构级调参。针对以上问题,本文一种基于冠豪猪优化算法、双向长短期记忆网络和 Kolmogorov-Arnold 网络的网络恶意流量检测模型(CPO-BiLSTM-KAN)。具体改进如下:

1)在特征提取阶段,将 BiLSTM 引入 KAN 网络并进行结合,构建 BiLSTM-KAN 特征提取模块。首先,BiLSTM 从双向捕捉流量数据的时序特征,然后再进入 KAN 网络,KAN 网络通过非线性映射对 BiLSTM 提取的特征进行高维变换,增强特征的非线性表达能力,避免复杂流量特征信息丢失。

2)使用 CPO 对 BiLSTM-KAN 模型的超参数进行优化。CPO 模拟冠豪猪防御行为在搜索空间内全局寻优,避免陷入局部最优,提升模型训练效率和性能。

3)采用多维度评估指标对优化后的 BiLSTM-KAN 模型进行性能评估,确保其在实际网络恶意流量检测场景中的准确性和鲁棒性。

1 基于 CPO-BiLSTM-KAN 的恶意流量检测模型

1.1 双向长短期记忆网络

LSTM 是 RNN 的一种变体,用于捕捉时间序列数据中的长期依赖性。LSTM 通过输入门、遗忘门和输出门 3 个门控机制解决了传统 RNN 中的梯度消失问题。然而,传统 LSTM 在需要同时从过去和未来信息中提取特征的任务中无法充分利用前后文的双向信息。

BiLSTM 通过正向和反向两个 LSTM 同时处理输入序列,能够充分捕捉时间序列中的双向上下文信息[21]。其结构如图 1 所示。

在本实验中,不同攻击模式在数据序列的不同位置有不同时间依赖性的表现,BiLSTM 能从正向和反向捕捉不

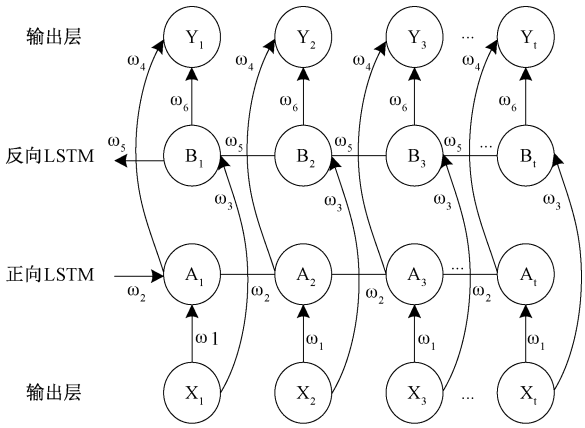

图 1　BiLSTM 结构图

Fig. 1　BiLSTM structure diagram

同时间的依赖性，充分利用流量数据的前后时间依赖特征，捕捉更丰富的时序信息，提供更全面的信息展示。公式如下：

$$\boldsymbol{A}_t = f_1(\boldsymbol{W}_1\boldsymbol{x}_t + \boldsymbol{W}_2\boldsymbol{A}_t - 1) \tag{1}$$

$$\boldsymbol{B}_t = f_2(\boldsymbol{W}_3\boldsymbol{x}_t + \boldsymbol{W}_5\boldsymbol{B}_t + 1) \tag{2}$$

$$\boldsymbol{Y}_t = f_3(\boldsymbol{W}_4\boldsymbol{A}_t + \boldsymbol{W}_6\boldsymbol{B}_t) \tag{3}$$

其中，$\boldsymbol{Y}_t$、$\boldsymbol{A}_t$、$\boldsymbol{B}_t$ 表示每层的计算结果；$\boldsymbol{W}_i$ 表示每一层输入的权重；$i = 1,2,\cdots,t$。输出层 $\boldsymbol{Y}_t$ 的计算结果由正向隐藏层、反向隐藏层以及不同权重值通过计算得到。正向隐藏层与反向隐藏层 $\boldsymbol{B}_t$ 两者相互独立，计算结果只与自身前一层的输出结果相关。

1.2　Kolmogorov-Arnold Networks

KAN 网络是基于 Kolmogorov-Arnold 展开理论的，其核心思想是将输入特征通过非线性映射到更高维的空间。这个映射使得输入的低维特征能够在高维空间中得到更有效的表达，增强了模型的表达能力。相较于传统神经网络，KAN 通过引入非线性核函数实现高维映射，不仅能突破线性模型和简单激活函数的局限，还能更精准地刻画输入特征间复杂的非线性关联，显著提升模型对复杂数据结构的拟合能力。其结构图如图 2 所示。

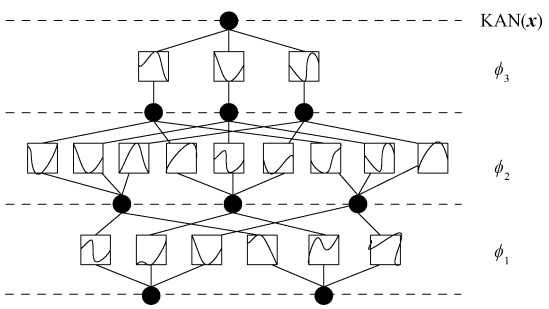

图 2　KAN 网络结构图

Fig. 2　KAN network structure diagram

在 KAN 网络中，输入特征通过非线性基函数进行变换，得到高维的特征表示。映射公式如下：

$$\boldsymbol{y} = \sum_{i=1}^{m} \boldsymbol{\alpha}_i \cdot \varphi_i(\boldsymbol{x}) \tag{4}$$

其中，$\boldsymbol{x}$ 表示 BiLSTM 网络层提取的特征，$\boldsymbol{\alpha}_i$ 表示可训练的权重，$\varphi_i(\boldsymbol{x})$ 表示非线性基函数。

1.3　冠豪猪优化算法

CPO 是一种新兴的自然启发式优化算法，灵感来源于冠豪猪在自然环境中面对捕食者时的防御行为[22]。CPO 模拟冠豪猪的 4 种主要防御策略：视觉、听觉、气味和物理攻击，分别对应算法中的探索和开发过程。算法通过模仿这些防御行为，在搜索空间内进行全局优化，寻找问题的最优解。

1)种群初始化与动态调整

CPO 的种群初始化在给定的搜索空间内随机生成个体的位置。通过该方式，保证了种群的多样性，避免了早期收敛。初始化公式如式(5)所示。

$$\boldsymbol{X}_i^{0} = \mathrm{LB} + rand() \cdot (\mathrm{UB} - \mathrm{LB}) \tag{5}$$

其中，LB 表示搜索空间上限，UB 表示搜索空间下限，$rand()$ 表示生成一个[0,1]之间的随机数。

为了避免种群过早收敛，CPO 引入了循环种群减少策略。该策略通过定期移除并重新加入个体的方法，保持种群的多样性，帮助算法加速收敛。调整公式如式(6)所示。

$$N_{new} = (N_{\max} - N_{\min}) \bmod C \tag{6}$$

其中，N_{new} 表示新生成种群的个体数，$N_{\max}$ 和 $N_{\min}$ 分别表示当前种群的最大和最小个体数，C 表示循环次数。

2)防御行为

CPO 通过模拟冠豪猪的防御行为，帮助算法在搜索空间中高效地找到全局最优解。冠豪猪面对捕食者时会采取以下 4 种防御策略：

(1)视觉防御阶段

当冠豪猪察觉到捕食者时，它通过抬起并扇动其刺毛，向捕食者施加威胁。此时，捕食者可能选择远离或继续接近。CPO 通过正态分布生成随机值来决定捕食者的行为，进而更新个体的位置。其公式为如式(7)所示。

$$\boldsymbol{X}_i^{t+1} = \boldsymbol{X}_i^{t} + \alpha \cdot (\boldsymbol{X}_{best} - \boldsymbol{X}_i^{t}) + \beta \cdot \boldsymbol{y}_i \tag{7}$$

其中，$\boldsymbol{X}_i^t$ 是第 i 个个体在第 t 代的当前位置，$\boldsymbol{X}_{best}$ 表示全局最优解，$\boldsymbol{y}_i$ 表示捕食者的位置，α 和 β 表示调整步长的系数。

(2)听觉防御阶段

冠豪猪在遭遇捕食者时，会发出威胁性的声音以驱赶捕食者。CPO 模拟这种行为时，通过生成随机噪声来影响个体的移动。随机噪声的强度决定了捕食者的行为，进而调整搜索路径。其公式为：

$$\boldsymbol{X}_i^{t+1} = \boldsymbol{X}_i^{t} + \gamma \cdot (\boldsymbol{X}_r - \boldsymbol{X}_i^{t}) + \delta \cdot U \tag{8}$$

其中，$\boldsymbol{X}_r$ 表示随机选择的个体位置，γ 和 δ 表示控制步长的参数，U 表示随机噪声，决定捕食者是远离还是靠近冠豪猪。

(3)气味防御阶段

冠豪猪通过释放恶臭气体来防止捕食者靠近。在

CPO 中,气味防御策略通过模拟气味的扩散过程来调整个体的搜索路径,增强算法的多样性和随机性。其公式为:

$$\boldsymbol{X}_i^{t+1} = \boldsymbol{X}_i^t + \lambda \cdot (\boldsymbol{S}_i - \boldsymbol{X}_i^t) \tag{9}$$

其中,$\boldsymbol{S}_i$ 表示气味扩散源,λ 表示控制扩散速率的参数。

(4)物理攻击防御阶段

当捕食者接近时,冠豪猪会进行物理反击。CPO 通过模拟物理攻击来提高个体的搜索能力,避免陷入局部最优。此防御策略采用非弹性碰撞模型表示。其公式为:

$$\boldsymbol{X}_i^{t+1} = \boldsymbol{X}_i^t - \alpha \cdot (\boldsymbol{X}_i^t - \boldsymbol{X}_{best}) + \boldsymbol{F}_i \tag{10}$$

其中,$\boldsymbol{F}_i$ 表示由非弹性碰撞计算得到的力,α 表示收敛速度因子。

1.4 CPO-BiLSTM-KAN 模型

本文提出的基于 CPO-BiLSTM-KAN 的网络恶意流量检测模型结构主要由输入层、双向长短期记忆网络模块、KAN 网络模块、冠豪猪优化算法模块以及流量检测输出层构成。模型整体结构图和流程图分别如图 3 和 4 所示。

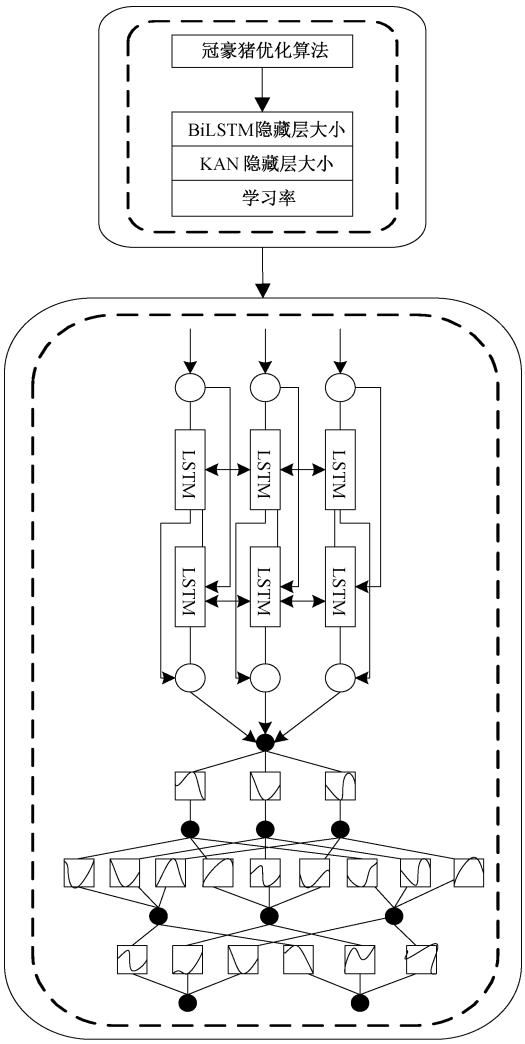

图 3 CPO-BiLSTM-KAN 结构图

Fig. 3 Structure diagram of CPO-BiLSTM-KAN

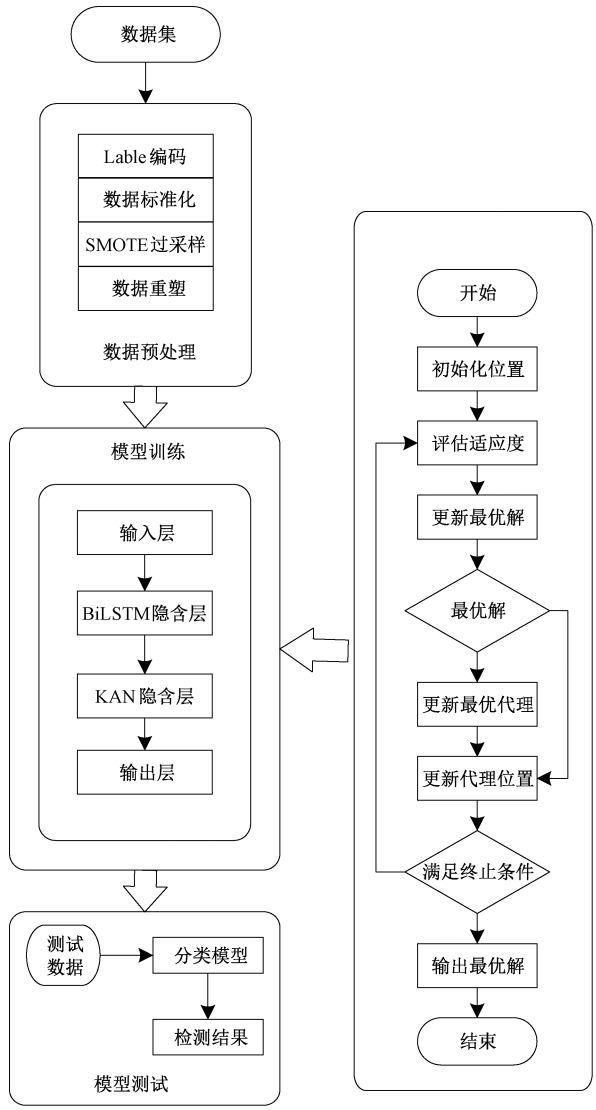

图 4 模型整体流程图

Fig. 4 Overall flowchart of the model

预处理后的数据通过 DataLoader 进行批量加载,并依次送入 BiLSTM 模型进行处理。BiLSTM 通过双向传播机制在每个时间步上分别获取序列正向和反向的隐藏状态,并将这两个方向的输出拼接成更丰富的特征向量;然后,经过 BiLSTM 拼接的特征向量输入到 KAN 层进行进一步处理。

KAN 层利用核映射对特征向量进行非线性变换,从复杂的特征中提取更深层次的信息;接着进入全连接层对处理过的特征进行整合,将经过核映射处理的特征映射到类别空间;最后在进入到输出层得到最后的分类结果。伪代码如算法 1 所示。

2 实验结果与分析

本文在多分类和二分类问题上分别进行实验,以此来评估模型的性能表现。在训练过程中将本实验的训练批次

算法 1：CPO-BiLSTM-KAN

1. 数据初始化及预处理
2. 定义并初始化带 KAN 层的 BiLSTM 模型
3. 设置 CPO 优化参数：
   目标函数：*obj_function*；参数范围：lb，ub，kb；种群数量：num_agent；最大迭代次数：max_iter
4. 随机初始化种群位置
5. 初始化 *best_agent* = None，*best_score* = ∞
6. CPO 优化过程：
   for t = 1 to max_iter do：
      for i = 1 to num_agents do：
         计算适应度：$fitness[i] = obj\_function(positions[i])$
         更新最优解：if $fitness[i] < best\_score$ then $best\_score = fitness[i]$
      end for
      for i = 1 to num_agents do：
         生成随机数 r_1，r_2
         更新位置：$new\_position = positions[i] + alpha * r_1 + beta * r_2$
         对新位置应用边界约束：$new\_position = clip(new\_position, lb, ub, kb)$
         计算新适应度：$new\_fitness = obj\_function(new\_position)$
         更新最优解：if $new\_fitness < best\_score$ then $best\_score = new\_fitness$
      end for
   end for
7. 使用最优参数训练模型
8. 在测试集上评估模型
9. 生成分类报告

设置为 50 次。此外本实验还选取了 CNN、RNN、LSTM、PSO-BiLSTM-KAN、GA-BiLSTM-KAN 和 POA-BiLSTM-KAN 在同一数据集进行实验和性能的对比，并选取 BiLSTM、LSTM-KAN、BiLSTM-KAN、CPO-BiLSTM 和 CPO-LSTM-KAN 进行消融实验。实验结果中用 PSO 代表 PSO-BiLSTM-KAN，GA 代表 GA-BiLSTM-KAN，POA 代表 POA BiLSTM-KAN。

2.1　数据集介绍

本实验应用公开数据集 CIC UNSW-NB15 Augmented Dataset 对模型进行评估。CIC UNSW-NB15 Augmented Dataset 数据集是由加拿大网络安全研究所与新南威尔士大学联合发布。该数据集是对原始 UNSW-NB15 数据集的增强版本。相比于 NSL-KDD、KDD-Cup99、CIC IDS2017 和原始 UNSW-NB15 数据集，该数据包含了更复杂的网络流量模式以及更丰富的特征，可以更好地模拟现代网络环境中的恶意攻击和正常流量。CIC UNSW-NB15 Augmented Dataset 数据集由 447 915 条流量数据组成，每条流量由 77 种不同特征描述构成。在标签特征栏中包含 9 个攻击类别和 1 个正常类别。流量类型以及各类别流量数量如表 1 所示。

由于 CIC UNSW-NB15 Augmented 数据集具有类别分布不平衡的问题，所以将原始数据集以 80%和 20%的比例将其划分为训练和测试数据集，在划分过程中，采用分层抽样方法来确保每个类别在训练集和测试集中的比例一致，并使用 SMOTE 过采样方法将训练集少数类样本进行数据增强，确保每个类别在训练集中的样本更加平衡，避免模型在训练过程中偏向于多数类样本提升，提升模型

表 1　CIC UNSW-NB15 Augmented 数据集样本分布

Table 1　Sample distribution of the CIC UNSW-NB15 Augmented dataset

攻击类型	数量
Generic	4 632
Dos	4 467
Analysis	385
Backdoor	452
Shellcode	2 102
Exploits	30 951
Fuzzers	29 613
Reconnaissance	16 735
Worm	246
总攻击数量	89 583
正常流量	358 332
总数量	447 915

对少数类样本的检测能力。

2.2 评价指标

为全面评估本文模型 CPO-BiLSTM-KAN 在网络恶意流量检测任务上的有效性和可行性,本文采用以下评价指标:

1)准确率(Accuracy):准确率表示模型正确分类的样本占总样本的比例,是最直观的评价指标。计算公式如式(11)所示。

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

其中,TP(true positive)表示真正例,即模型正确识别出的恶意流量样本数;TN(true negative)表示真负例,即模型正确识别出的正常流量样本数;FP(false positive)表示假正例,即模型将正常流量误判为恶意流量的样本数;FN(false negative)表示假负例,即模型将恶意流量误判为正常流量的样本数。

2)精确率(Precision):精确率表示模型预测为恶意的流量中,实际为恶意的比例,反映了模型预测结果的可靠性。计算公式如式(12)所示。

$$\text{Precision} = \frac{TP}{TP + FP} \tag{12}$$

3)召回率(Recall):召回率表示实际为恶意的流量中,被模型正确识别出的比例,反映了模型对恶意流量的识别能力。计算公式如式(13)所示。

$$\text{Recall} = \frac{TP}{TP + FN} \tag{13}$$

4)F1 度量(F1 Score):F1 度量是精确率和召回率的调和平均数,能够综合反映模型的性能。计算公式如式(14)所示。

$$\text{F1} = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{14}$$

2.3 实验环境

本实验使用的操作系统为 Ubuntu 9.4.0-lubuntul~20.04.2,GPU 为 NVIDIA GeForce RTX 3090,内存 24 GB,使用 Python 3.8 编程,使用 Pytorch 深度学习框架。

2.4 二分类实验

在二分类实验中,模型的输入层有 77 个节点,输出层有两个输出维度。应用 softmax 作为激活函数,将正常流量和恶意流量进行分类。

模型首先使用训练集数据进行训练,训练结束之后使用测试集数据对该模型进行评估。各模型在二分类的整体性能对比如表 2 所示。

从表 2 中可以看出,本文模型的准确率达到 99.12%,明显高于其他 6 种模型,这表明本文模型的有效性,在网络恶意流量检测方面性能更加突出;其次,本文模型在召回率、准确率和 F1 度量上均高于其他 6 种模型。本文模型的精确率为 99.15%,表明该模型在恶意流量检测方面的误判率更低;本文模型的召回率为 99.20%,表明该模型在捕捉恶意流量方面更强;F1 度量是精确率与召回率的综合体,本文模型的 F1 度量为 99.17%,表明该模型具有更轻的预测能力。

表 2 各模型在二分类中性能对比

Table 2 Performance comparison of each model in binary classification

模型	Precision	Recall	F1-score	Accuracy
CNN	0.956 3	0.955 8	0.956 1	0.955 6
RNN	0.957 5	0.958 2	0.957 8	0.957 3
LSTM	0.966 4	0.967 1	0.966 7	0.966 2
PSO	0.978 0	0.978 7	0.978 3	0.977 5
GA	0.976 0	0.976 7	0.976 4	0.976 1
POA	0.979 5	0.980 1	0.979 8	0.979 3
本文模型	0.991 5	0.992 0	0.991 7	0.991 2

综上所述,本文模型在准确率、精确率、召回率和 F1 度量上均有较好的性能,这表明本文模型具有较好的泛化性,适用于网络恶意流量检测方面的工作。

2.5 多分类实验

在多分类实验中,输入同样为 77 的特征向量,但与二分类不同是,输出层有 10 个输出节点,使用 softmax 作为激活函数,检测输入的流量分别属于哪个类别。各模型在多分类实验中的整体的准确率如表 3 所示。

表 3 各模型在多分类中整体准确率

Table 3 Overall accuracy rates of each model in multiple classifications

模型	Accuracy
RNN	0.898 8
LSTM	0.900 8
CNN	0.888 7
PSO	0.926 8
GA	0.929 7
POA	0.930 8
CPO-BiLSTM-KAN	0.941 5

从表 3 可以看出,与其他模型相比,本文模型在多分类实验中整体的准确率的测试结果是最优,达到了 94.15%,而且比其他模型分别提高了 4.27%、4.07%、5.28%、1.47%、1.18%和 1.07%,表明本文模型能够更有效地学习网络流量特征,并且能够提高恶意流量的检测能力。

各个模型在检测网络流量时的精确率如表 4 所示,各个模型在检测网络流量时的 F1 度量如表 5 所示。

从表 4 可以看出,本文模型在检测不同流量类型时表现出较高的精确率,并且优于其他模型。首先,在正常流量(Benign)类别中,本文模型的精确率达到 99.95%,表明本文模型能准确区分正常流量与其他恶意流量。对于恶意流量的检测,本文模型在不同恶意流量的精确率与其他模型相比均有提升,特别是对于少数类样本 Worms 和 Backdoor 类别准确率分别为 52.17%和 78.09%,明显高

表 4　各模型在多分类中的精确率

Table 4　Accuracy rates of each model in multiple classifications

类别	RNN	LSTM	CNN	PSO	GA	PAO	本文模型
Benign	0.999 8	0.999 8	0.999 9	0.989 9	0.993 6	0.991 6	0.992 5
Analysis	0.247 3	0.274 8	0.245 5	0.331 3	0.194 4	0.223 7	0.353 3
Backdoor	0.237 1	0.055 3	0.124 7	0.502 0	0.573 8	0.735 3	0.780 9
DoS	0.293 4	0.294 0	0.324 7	0.453 3	0.619 0	0.655 2	0.656 2
Exploits	0.885 4	0.877 1	0.902 2	0.737 7	0.732 4	0.767 4	0.910 7
Fuzzers	0.638 3	0.633 8	0.739 8	0.606 6	0.602 6	0.596 8	0.714 8
Generic	0.598 5	0.640 4	0.622 4	0.744 8	0.730 4	0.759 9	0.789 6
Reconnaissance	0.676 6	0.798 6	0.818 3	0.831 3	0.861 3	0.819 8	0.862 3
Shellcode	0.220 7	0.183 1	0.175 3	0.342 9	0.376 5	0.352 0	0.387 4
Worms	0.008 9	0.015 4	0.008 3	0.269 2	0.083 3	0.414 6	0.521 7

表 5　各模型在多分类中的 F1 度量

Table 5　F1 metrics of each model in multi-classification

类别	RNN	LSTM	CNN	PSO	GA	PAO	本文模型
Benign	0.986 6	0.986 8	0.986 6	0.986 6	0.988 0	0.987 3	0.987 6
Analysis	0.387 6	0.393 6	0.384 2	0.142 9	0.123 9	0.065 2	0.408 5
Backdoor	0.323 9	0.101 2	0.205 1	0.391 9	0.453 6	0.403 2	0.466 2
DoS	0.342 2	0.351 6	0.354 5	0.221 5	0.233 5	0.173 5	0.402 1
Exploits	0.665 5	0.689 0	0.639 0	0.739 1	0.749 7	0.750 8	0.754 8
Fuzzers	0.625 6	0.631 4	0.622 3	0.691 1	0.715 8	0.712 5	0.717 6
Generic	0.647 2	0.677 2	0.657 5	0.624 9	0.659 2	0.658 1	0.662 5
Reconnaissance	0.701 9	0.729 1	0.732 7	0.729 5	0.740 3	0.735 6	0.749 3
Shellcode	0.303 9	0.264 1	0.263 8	0.137 1	0.210 5	0.210 4	0.272 2
Worms	0.017 5	0.019 6	0.016 4	0.186 7	0.054 8	0.327 8	0.333 3

于其他模型。上述表明，本文模型能够有效减少误报，提高恶意流量检测的有效性。

从表 5 可以看出，本文模型在检测多数恶意流量类别的 F1 度量显著高于其他模型，尤其在 Backdoor、Exploits、Fuzzers 和 Worms 类别上的提升尤为明显，分别为 46.62%，75.48%，71.76%和 33.33%。对于正常流量 F1 度量达到 98.76%。上述表明文方法能够更精准地捕捉恶意流量的特征，减少误分类情况。

综上所述，本文模型在网络恶意流量检测中具有明显优势，在多类别恶意流量检测的精确率和 F1 度量均有出色表现，表明本文模型具有较强的区分能力和鲁棒性，并且证明本文模型在多样化的恶意流量检测中的适用性和潜力。

2.6　消融实验

为了验证各个模块如冠豪猪优化模块、BiLSTM 模块和 KAN 网络模块对性能表现的贡献程度设置消融实验，相关实验结果如表 6 所示。

表 6　消融实验结果

Table 6　Ablation experiment results

模型	Precision	Recall	F1-score	Accuracy
BiLSTM	0.968 5	0.969 0	0.968 7	0.968 2
BiLSTM-KAN	0.976 5	0.977 1	0.976 8	0.976 3
LSTM-KAN	0.975 4	0.976 2	0.975 8	0.975 3
CPO-BiLSTM	0.970 5	0.971 1	0.970 8	0.970 3
CPO-LSTM-KAN	0.977 4	0.978 1	0.977 7	0.977 2
本文模型	0.991 5	0.992 0	0.991 7	0.991 2

从表 6 可以看出，BiLSTM-KAN 和 LSTM-KAN 的精确率分别为 97.65%和 97.54%，前者模型优于后者模型，

表明 BiLSTM 在处理时序相关的流量数据时比单向 LSTM 具有更强的特征学习能力,能够更好地捕捉恶意流量的时间依赖性;其次,对比 BiLSTM-KAN 与 BiLSTM 的实验结果,添加 KAN 网络模块后,模型的精确率和召回率均有所提升,F1 度量提升了 0.81%,表明 KAN 网络通过知识注意力机制有效增强了恶意流量的特征提取能力,使得模型在恶意流量检测任务中能够更准确地区分正常流量与恶意流量。另一方面,CPO-BiLSTM 相较于 BiLSTM-KAN,虽然保持了较好的流量检测能力,但由于缺少 KAN 网络模块,其精度和召回率较低,表明单一的 CPO 无法完全弥补特征选择上的不足。然而,当 CPO 与 KAN 网络结合后,CPO-LSTM-KAN 相较于 LSTM-KAN 在精确率、准确率、召回率和 F1 的值均有所提升,表明 CPO 在优化训练策略方面的重要作用,能够增强模型的稳定性,并进一步提升网络流量的检测能力。

本文模型在实验结果中取得最佳性能,整体的准确率和 F1 度量分别达到了 99.12%和 99.17%,同时精确率达到了 99.15%,相比 BiLSTM-KAN 和 CPO-BiLSTM,分别提升了 1.5%和 2.1%,进一步验证了 CPO、BiLSTM 和 KAN 网络之间的协同作用对于恶意流量检测的有效性。

另外为了验证本文模型在少数类网络流量检测的性能,将本文模型与传统模型在 CIC UNSW-NB15 Augmented 数据集的少数类样本进行网络恶意流量检测。在该数据集中,Analysis、Backdoor 和 Worms 样本数量分别为 385、452 和 246,但在对这些流量类型的训练集均使用了 SMOTE 过采样,以增加少数类样本的数量,减少类别不均衡对模型的影响。各模型在对各少数类网络流量检测的精确率如表 7 所示。

从表 7 可以看出,在 RNN、CNN 和 LSTM 模型中,Backdoor 精确率分别为 23.71%、12.47%和 5.53%,Worms 类别的精确率分别为 0.89%、0.83%和 1.54%,表明过采样方法的使用未能明显提升传统模型在少数类网络流量的检测性能。相比之下,本文模型在 Analysis、Backdoor 和 Worms 类别上的精确率分别达到了 35.33%、78.09%和 52.17%,与其他模型相比较有显著提升,表明本文模型在少数类网络流量的检测能力得到增强。

综上所述,KAN 网络通过自适应注意力机制增强了少数类样本的特征提取能力,使模型更精准地学习 Analysis 和 Backdoor 等少数类网络类别的模式特征,而 CPO 通过优化训练策略,避免了多数类样本的主导效应,使 Worms 等低频类别的检测能力得到了显著提升。CPO-BiLSTM-KAN 能够有效提高少数类恶意流量检测的精准度。

表 7 各模型对少数类样本检测的精确率

Table 7 The accuracy rates of each model for detecting minority class samples

类别	Analysis	Backdoor	Worms
RNN	0.247 3	0.237 1	0.008 9
CNN	0.245 5	0.124 7	0.008 3
LSTM	0.274 8	0.055 3	0.015 4
BiLSTM	0.302 7	0.720 9	0.254 7
BiLSTM-KAN	0.339 6	0.772 7	0.415 2
LSTM-KAN	0.288 5	0.183 0	0.058 4
CPO-BiLSTM	0.319 1	0.739 3	0.320 6
CPO-LSTM-KAN	0.327 3	0.490 2	0.105 3
PSO	0.331 3	0.502 0	0.269 2
GA	0.194 4	0.573 8	0.083 3
POA	0.223 7	0.735 3	0.414 6
CPO-BiLSTM-KAN	0.353 3	0.780 9	0.521 7

2.7 性能分析

为评估模型的运算时间效率与计算资源消耗情况,本文对不同模型的程序运行时间和内存占用进行了对比分析,实验结果如图 5 所示。

在运行时间方面,传统模型因网络结构简单,运行时间较短;而采用群智能优化算法的复杂模型,由于参数搜索过程产生计算开销,运行时间增加。本文提出的 CPO-BiLSTM-KAN 模型运行时间为 7 134.65 s,凭借 CPO 算法高效的全局寻优能力,在保障检测精度的同时减少了超参数搜索的迭代次数,运行效率优于 PSO、GA 等同类优化模型,较传统优化算法节省 20%~30%的计算耗时。

在内存消耗方面,模型内存占用为 3 949.57 MB,得益于 KAN 网络的优化设计,通过非线性映射操作实现特征维度的高效计算,内存利用效率显著优于 PSO-BiLSTM-KAN 和 GA-BiLSTM-KAN。并且内存占用控制在合理范围。

实验结果表明,该模型在实现高精度恶意流量检测的同时,兼顾了计算效率与资源消耗,适用于对实时性和部署成本要求较高的网络安全场景。

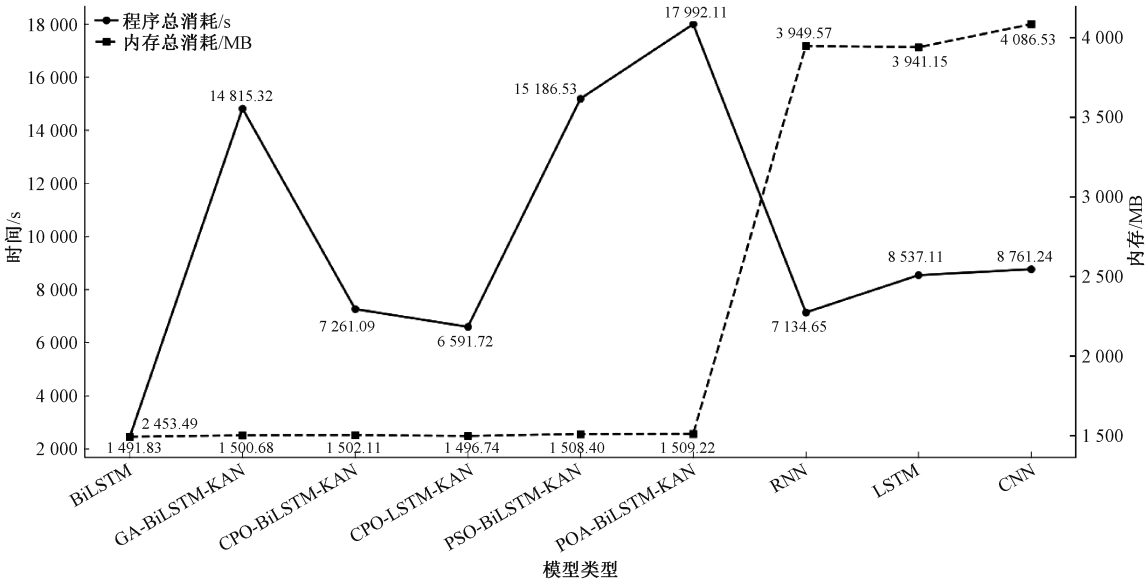

图 5　不同模型程序总消耗和内存总消耗对比图

Fig. 5　Comparison chart of total program consumption and total memory consumption of different models

3　结　　论

针对目前日益复杂的网络环境，原有的恶意流量检测模型难以取得有效的检测效果。本文提出的 CPO-BiLSTM-KAN 模型在恶意流量检测任务中表现出显著的优势。通过引入冠豪猪优化算法对模型超参数的优化，模型的性能得到了进一步提升。与 BiLSTM 和 KAN 网络结合后，模型能够更能有效地捕捉恶意流量的时序依赖和非线性特征，提高了对复杂攻击模式的适应能力。实验结果表明，该模型在二分类和多分类任务中的性能均优于传统的流量检测模型，特别是在少数类恶意流量的检测中显示了较强的识别能力。同时，在运算时间效率与计算资源消耗方面，本模型在不同规模网络环境中均展现出较好的适应性。但是本文模型对于少数类恶意流量样本的识别精确率仍有待提高，未来可以进一步研究数据集中少数类样本的不平衡问题，寻求合适的方法增强少数类样本数量，进一步提高模型准确率。

参考文献

[1]　付钰，王坤，段雪源，等. 面向软件定义网络的异常流量检测研究综述[J]. 通信学报，2024，45(3)：208-226.
FU Y，WANG K，DUAN X Y，et al. A survey study on anomaly traffic detection for software-defined networking[J]. Journal on Communications，2024，45(3)：208-226.

[2]　苏璞睿，冯登国. 2024 年网络空间安全科技热点回眸[J]. 科技导报，2025，43(1)：102-117.
SU P R，FENG D G. A review of technological hotspots in cyberspace security in 2024[J]. Science & Technology Review，2025，43(1)：102-117.

[3]　DURGARAJU S，VEL D V T，MADATHALA H. The evolution of cyber threats and defenses：A review of innovations and challenges[C]. IEEE International Conference on Mobile Computing and Sustainable Informatics(ICMCSI)，2025：117-123.

[4]　AL-SELWI S M，HASSAN M F，ABDULKADIR S J，et al. RNN-LSTM：From applications to modeling techniques and beyond—systematic review[J]. Journal of King Saud University-Computer and Information Sciences，2024，36(5)：102068.

[5]　JIANG R，WENG Z，SHI L，et al. Intelligent botnet detection in IoT networks using parallel CNN-LSTM fusion[J]. Concurrency and Computation：Practice and Experience，2024，36(24)：e8258.

[6]　BAMBER S S，KATKURI A V R，SHARMA S，et al. A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system[J]. Computers & Security，2025，148：104146.

[7]　倪志伟，行鸿彦，侯天浩，等. 基于生成对抗网络和混合时空神经网络的入侵检测[J]. 电子测量技术，2024，47(2)：17-24.
NI ZH W，XING H Y，HOU T H，et al. Intrusion detection based on generative adversarial networks and hybrid spatiotemporal neural networks[J]. Electronic Measurement Technology，2024，47(2)：17-24.

[8]　VOLPE G，FIORE M，LA GRASTA A，et al. A Petri net and LSTM hybrid approach for intrusion

detection systems in enterprise networks[J]. Sensors (Basel, Switzerland), 2024, 24(24): 7924.

[9] YANG Y, TU S, ALI R H, et al. Intrusion detection based on bidirectional long short-term memory with attention mechanism[J]. Computers, Materials and Continua, 2022, 74(1): 801-815.

[10] 戚子健,柳毅. 基于双向 GRU 和 CNN 的恶意网络流量检测方法[J]. 计算机应用与软件, 2024, 41(12): 334-340.
QI Z J, LIU Y. A malicious network traffic detection method based on bidirectional GRU and CNN[J]. Computer Applications and Software, 2024, 41(12): 334-340.

[11] SHI Z, LUKTARHAN N, SONG Y, et al. Tsfn: A novel malicious traffic classification method using BERT and LSTM[J]. Entropy, 2023, 25(5): 821.

[12] 刘拥民,许成,黄浩,等. 基于 SAE 和 WGAN 的入侵检测方法研究[J]. 计算机工程与科学, 2025, 47(2): 256.
LIU Y M, XU CH, HUANG H, et al. Research on intrusion detection method based on SAE and WGAN[J]. Computer Engineering and Science, 2025, 47(2): 256.

[13] LIU Z, WANG Y, VAIDYA S, et al. KAN: Kolmogorov-Arnold networks[J]. ArXiv Preprint arXiv:2404.19756,2024.

[14] 陈万志,张国满,王天元. 基于特征耦合泛化的流量异常检测方法[J]. 电子测量与仪器学报,2024,38(2): 120-130.
CHEN W ZH, ZHANG G M, WANG T Y. Traffic anomaly detection method based on feature coupling generalization[J]. Journal of Electronic Measurement and Instrumentation, 2024, 38(2): 120-130.

[15] SI B, NI Z, XU J, et al. Interactive effects of hyperparameter optimization techniques and data characteristics on the performance of machine learning algorithms for building energy metamodeling[J]. Case Studies in Thermal Engineering, 2024,55: 104124.

[16] KISHORE C R, RAO D C, NAYAK J, et al. Improved particle swarm optimization based bidirectional-long short-term memory for intrusion detection system in internet of vehicle[J]. Arabian Journal for Science and Engineering, 2025, 50: 12357-12386.

[17] BARIK K, MISRA S, FERNANDEZ-SANZ L. Adversarial attack detection framework based on optimized weighted conditional stepwise adversarial network[J]. International Journal of Information Security, 2024, 23(3): 2353-2376.

[18] KAYYIDAVAZHIYIL A. Intrusion detection using enhanced genetic sine swarm algorithm based deep meta-heuristic ANN classifier on UNSW-NB15 and NSL-KDD dataset[J]. Journal of Intelligent & Fuzzy Systems, 2023, 45(6): 10243-10265.

[19] PAPALKAR R R, JADHAV J, PATTEWAR T, et al. WACSO: Wolf crow search optimizer for convolutional neural network hyperparameter optimization[J]. Neural Processing Letters, 2025, 57(2): 31.

[20] 彭菲桐,徐凯,吴仕勋,等. 基于智能优化深度网络的轨道电路故障诊断研究[J]. 电子测量与仪器学报,2024, 38(2):219-230.
PENG F T, XU K, WU SH X, et al. Research on track circuit fault diagnosis based on intelligent optimization deep network[J]. Journal of Electronic Measurement and Instrumentation, 2024, 38(2): 219-230.

[21] 梁宏涛,刘硕,杜军威,等. 深度学习应用于时序预测研究综述[J]. 计算机科学与探索, 2023, 17(6): 1285-1300.
LIANG H T, LIU SH, DU J W, et al. A survey on deep learning applications in time series prediction[J]. Journal of Frontiers of Computer Science & Technology, 2023, 17(6): 1285-1300.

[22] ABDEL-BASSET M, MOHAMED R, ABOUHAWWASH M. Crested porcupine optimizer: A new nature-inspired metaheuristic[J]. Knowledge-Based Systems, 2024, 284: 111257.

作者简介

刘凤春,硕士,教授,主要研究方向为网络空间安全建模、人工智能与大数据和计算机应用技术。
E-mail:18849778@qq.com

王子贺,硕士研究生,主要研究方向为网络安全与深度学习。
E-mail:wangzihe@stu.ncst.edu.cn

杨爱民(通信作者),博士,教授,主要研究方向为网络应用安全、医学大数据与智能辅助诊疗研发。
E-mail:aimin@ncst.edu.cn

袁书娟,硕士,副教授,主要研究方向为数学建模及人工智能大数据的应用。
E-mail:yuanshujuan@ncst.edu.cn

孔闪闪,博士,副教授,主要研究方向为网络信息安全、大数据、数学建模和云计算。
E-mail:kongss@ncst.edu.cn