计算机科学
COMPUTER SCIENCE

基于机器学习的异常流量检测模型优化研究

陈向效, 崔鑫, 杜秦, 唐浩耀

引用本文

陈向效, 崔鑫, 杜秦, 唐浩耀. 基于机器学习的异常流量检测模型优化研究[J]. 计算机科学, 2024, 51(6A): 230700051-5.

CHEN Xiangxiao, CUI Xin, DU Qin, TANG Haoyao. Study on Optimization of Abnormal Traffic Detection Model Based on Machine Learning [J]. Computer Science, 2024, 51(6A): 230700051-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700051

基于机器学习的异常流量检测模型优化研究

陈向效　崔　鑫　杜　秦　唐浩耀
山东理工大学计算机科学与技术学院　山东 淄博 255000
(651477787@qq.com)

摘　要　在软件定义网络(Software Defined Network,SDN)中,异常流量检测方法在实践中存在一些问题,主要体现在误报率高和虚警频繁等方面。为了应对网络中的异常流量攻击,研究人员开始探索机器学习异常流量检测方法。然而,机器学习方法面临着数据集庞大和数据维度高等挑战,这些因素影响了机器学习的效率和准确率,因此需要进行数据降维处理。主成分分析算法(Principal Component Analysis,PCA)作为基于线性变换的降维算法,存在一定的局限性,无法有效估计主成分。为了解决该问题,文中提出了一种改进的降维算法,即聚类高斯核主成分分析(C-means Gaussian Kernel Principal Component Analysis,CGKPCA),它扩展了非线性变换的能力。同时,还针对分类模型进行了改进,提出了改进的堆叠分类模型(Support Vector Machine Stacking,SVMS)。为了验证所提方法的有效性,文中使用开源数据集 KDDCPU99 和 UNSW-NB15 进行了实验。实验结果表明,所提出的二分类检测模型在性能指标上明显领先于其他模型。

关键词:软件定义网络;机器学习;堆叠模型;异常流量检测;聚类高斯核主成分分析
中图分类号　TP393

Study on Optimization of Abnormal Traffic Detection Model Based on Machine Learning

CHEN Xiangxiao,CUI Xin,DU Qin and TANG Haoyao
College of Computer Science and Technology,Shandong University of Technology,Zibo,Shandong 255000,China

Abstract　Anomaly traffic detection methods in software defined network(SDN) have some problems in practice,such as high false alarm rate and frequent false alarms. In response to abnormal traffic attacks in the network,researchers have started to explore machine learning methods for abnormal traffic detection. However,machine learning methods face the challenges of large data sets and high data dimensionality,which affect the efficiency and accuracy of its performance,and thus require data reduction processing. Principal component analysis(PCA),as a linear transformation-based downscale algorithm,has certain limitations and cannot effectively estimate the principal components. To overcome this challenge,this paper proposes an improved dimensionality reduction algorithm,namely C-means Gaussian kernel principal component analysis(CGKPCA),which extend the capability of non-linear transformation. Also,this paper improves on the classification model by proposing an improved stacking model SVMS (support vector machine stacking). To validate the effectiveness of the proposed algorithms,experimental validation is conducted using the open source datasets KDDCPU99 and UNSW-NB15. The testing results indicate that the binary classification detection model proposed in this paper is significantly ahead of other models in terms of performance metrics.

Keywords　Software defined network,Machine learning,Stacking model,Abnormal traffic detection,CGKPCA

1　引言

根据中国互联网络中心发布的第 51 次《中国互联网络发展状况报告》[1],截至 2022 年底,中国网民数已达 10.32 亿,继续保持增长。该报告显示中国在信息通信网络建设方面取得了巨大进展,并将未来重点放在网络安全防护上。

随着互联网技术的发展,网络流量不断增加,网络攻击和木马病毒在网络上肆意传播,因此网络安全成为研究者关注的焦点。传统的网络架构模型存在很多协议和封闭模式的问题,为了解决这些问题,引入软件定义网络 SDN[2]。SDN 通过解耦底层设备和控制层,实现了多功能应用和网络资源的池化。SDN 是目前网络领域中具备巨大发展潜力的技术。在数据网络中心、电信运营网络以及互联网公司等领域得到了广泛应用,国内外发展前景呈现一片光明的趋势。但是 SDN 的发展尚不成熟,SDN 网络的安全问题也困扰着众多学者。

近年来,国内外学者对网络架构进行了深入探讨和研究。同时电信网络中的架构、设备和组件也面临着革命性的挑战。2019 年 Lu 等从优化目标的角度研究了监控器配置问题,提出了一种很有前途的范式转变[3],即将控制平面和数据平面解耦,实现了网络的可编程配置。虽然 SDN 取得了一定进展,但也引发了一些新的安全性问题。Li 等[4]在 2022 年提出了基于半监督的流量异常检测方法,提高了二分类任务的性能,但是数据维度高,给数据特征训练带来了干扰。

基金项目:下一代互联网技术项目(NGII2019110)
This work was supported by the Next Generation Internet Technology Project (NGII2019110).
通信作者:崔鑫(cx@sdut.cn)

2 相关背景

2.1 SDN

SDN 技术是一种全新的网络可编程体系架构，与传统网络相比最大的特征就是可以对网络进行管理和编程。SDN 通过用户接口对网络进行编程管理来革新传统网络偏重静态、配置复杂、不利于运营维护人员管理的网络架构。尽管 SDN 解决了传统网络架构中的封闭模式和协议众多等问题，但是机器学习的检测模型仍然面临着处理大规模和高维度数据的挑战。

2.2 降维技术

国内外学者对这个挑战展开了广泛的研究。为了解决这些挑战，近年来数据处理领域又出现了降维计算的热潮，在这个领域中独立成分分析和主成分分析一直是主要的研究对象。这些算法旨在应对大规模和高维度数据的问题，以便更有效地处理和分析这些数据。

在异常流量检测系统中，为了解决检测率低的问题，Li 等于 2019 年提出了基于 MSPCA 的算法[5]，并结合小波多尺度分解，能够有效提高检测速度和准确率。然而，该模型的阈值系数经常波动，不利于动态调整和系统扩展。Wang 等于 2021 年提出了改进 IKPCA[6]融合贝叶斯深度神经网络算法，但是由于贝叶斯效率低下，因此其准确率提升不明显。Zhang 等于 2022 年提出了 PCA 应用于网络入侵检测[7]，并结合了卷积神经网络和随机森林算法。实验结果表明，这种方法明显改善了检测效果，但是提高了计算量，特征维度较高，增加了系统 CPU 计算量，增添了系统不稳定因素。2022 年 AI-Fawa'reh 创新地将 PCA 与深度神经网络模型相结合，并被应用于物联网入侵检测系统[8]，缩短了模型的检测时间，提高了安全性，但是在系统稳定性方面存在问题。

2.3 机器学习模型技术

早期的机器学习模型使用单一的模型，2021 年 Mohammadi 等提出了基于改进贝叶斯算法的入侵检测系统[9]，有效地提高了入侵检测的效率，但是预测准确率不高。为了进一步提高机器学习的准确率，出现了集成学习模型，如 Bagging，Boosting 以及 Stacking[10]。Islam 等于 2021 年提出了将 Stacking 模型[11]应用于 IOT 恶意流量分类检测方法。该方法通过融合多个分类模型，并从多角度观察预测数据，实验证明其能够有效检测物联网中的异常流量。Li 等于 2022 年提出了最大相关熵的 KPCA 异常检测方法[12]，可以有效抑制噪声提高泛化性能，该方法开创了核主成分分析的先河。Peng 等于 2023 年使用 PCA-DNMFSC 算法[13]来实现卫星遥测异常的自动检测，该方法具备实时检测卫星遥测数据异常的能力。同年 Zhuang 提出高斯核嵌入式分析学习[14]（GKEAL）来处理少样本类增量学习任务，研究表明该方法能在多方面有效提高数据集的性能。

本文提出了改进降维算法融合改进 Stacking 模型的方法，以进一步优化分类检测模型。当 SDN 网络中出现异常流量时，该异常能够被检测出，并保护网络安全。机器学习从数据角度更精确地识别出数据流量的特征，从而提高模型预测准确率，因此展开基于机器学习的入侵检测模型的相关研究，对于 SDN 网络的安全具有非常重要的意义。

目前，为了进一步提高模型的预测准确率，本文的主要研究包括两个方面：降维技术的应用和机器学习模型优化。本文对降维技术和集成学习模型进行了深入研究，通过这些深入研究，旨在提高模型的预测准确率。

3 相关研究

Zhao 等于 2023 年提出 SDN 网络边缘交换机异常检测[15]，该方法通过统计信息一致性判断异常传输行为，但存在误报问题，如链路丢包率过高以及漏报问题，如存在时间较短的异常流表。本研究的目标是提高二分类检测模型在网络异常流量检测方面的准确率。首先，通过改进 PCA 算法来处理网络流量特征值；其次，改进 Stacking 模型，改进后的 SVMS 模型使机器学习具备更高的准确率。SDN 的流程图如图 1 所示。

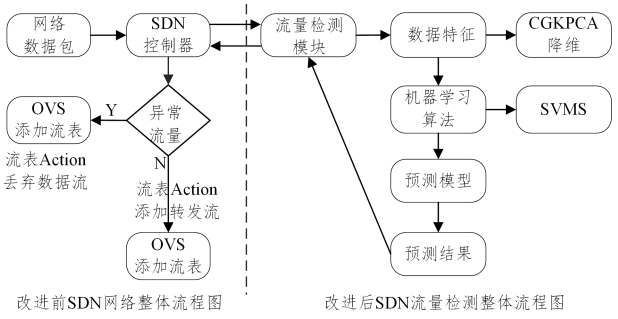

图 1 SDN 网络检测流程图

Fig. 1 Flow chart of SDN network detection

由图 1 可看出，本文采用机器学习的异常流量检测模块，并将其应用于 SDN 控制器。该模块的设计旨在通过机器学习方法来解决传统检测模块效率低的缺陷，主要改进包括对数据降维和分类模型的改进，下文将对这两个主要功能进行详细说明。

3.1 非线性核优化的 CGKPCA 算法

本文提出了高斯核主成分分析 CGKPCA，将该算法应用于非线性降维数据处理。通过这一技术，本文能够有效地处理那些线性不可分的数据集。异常流量分类系统如图 2 所示。

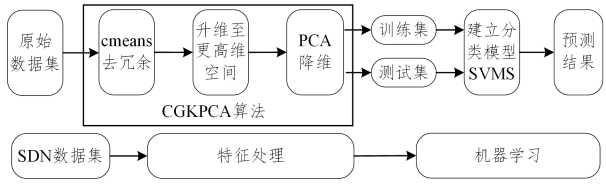

图 2 改进后异常流量分类系统

Fig. 2 Improved abnormal traffic classifiy system

该算法在保持有效信息量的前提下，能够有效地降低数据的维度，并消除冗余信息，从而减小计算负担，并提高检测模块的效率，提高了检测模块的准确率。CGKPCA 算法是对 PCA 算法的扩展和改进。在线性降维之前，CGKPCA 算法将非线性可分的数据映射到一个适合线性分类的高维新空间中，实现了对非线性关系的支持。但是高斯核扩展会占用大量计算机内存，这可能导致系统的稳定性下降。为了解决这一问题，本文采用以下步骤。首先，使用 C-means 聚类对数据进行预处理。C-means 聚类使用欧氏距离计算样本之间的距离，这种聚类方法有助于去除冗余数据，从而减少降维过程中内存的使用量，随后把预处理数据扩展到高维空间，然后运用

PCA 算法将数据进行线性投影到低维空间中。这种扩展使得 CGKPCA 算法不仅继承了 PCA 算法的优点，而且能够更好地处理数据样本间的非线性关系，同时减少系统内存的使用，从而更有效地分离出主成分分量。通过使用这种改进后的 CGKPCA 算法，本文在减少机器学习计算量的同时，仍能保持有效信息的提取。这对于处理非线性可分数据，并且在系统内存资源有限的情况下仍保持较好性能的机器学习任务非常有益。这种算法的改进使得异常流量检测模块能够更准确地识别异常流量，进一步保障了 SDN 网络的安全。因此，本文的创新点在于基于 PCA 算法的改进，即 CGKPCA 算法通过非线性到线性的扩展，更好地适应了数据的非线性关系，并有效地提高了异常流量检测模块的准确性。CGKPCA 流程图如图 3 所示。

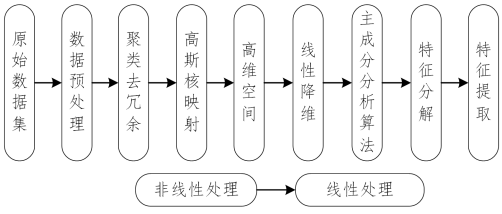

图 3　CGKPCA 流程图

Fig. 3　CGKPCA flow chart

CGKPCA 算法用 $\boldsymbol{X}$ 的每一列来表示一个样本，即 $\boldsymbol{X}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N]$，每个样本 $\boldsymbol{x}_i$ 为 K 维的向量。$K\times N$ 维矩阵 $\boldsymbol{X}$ 所在的空间称为样本空间。CGKPCA 算法的实现过程如下：

1）使用 C-means 算法计算样本间的距离，距离越短表示相似度越高。最终目标是形成紧凑且独立的簇。该算法以样本与类均值之间的误差平方和作为聚类准则函数，如式(1)所示：

$$J_e=\sum_{i=1}^{C}\sum_{y\in\Gamma_i}\|y-m_i\|^2 \tag{1}$$

其中，类均值 $m_i=\frac{1}{N_i}\sum_{y\in\Gamma_i}y$，$J_e$ 为聚类准则函数，它表示将 N 个样本分成 c 类时所产生的总误差平方和。

2）通过一个非线性映射 $\emptyset$ 将原始数据集 X 中的向量映射到高维空间(D 维空间)，这个高维特征空间称之为 F，将矩阵 $\boldsymbol{X}$ 中的所有样本都映射到 F 中，以便更好地处理数据样本间的非线性关系，得到 $D\times N$ 的新矩阵 $\phi(\boldsymbol{X})$。

3）将 $\phi(\boldsymbol{X})$ 进行中心化处理。

4）计算 $\boldsymbol{X}$ 的协方差矩阵，如式(2)所示：

$$\boldsymbol{C}_F=\frac{1}{N}\sum_{i=1}^{N}\phi(x_i)\phi(x_i)^{\mathrm{T}} \tag{2}$$

其中，$\boldsymbol{C}_F$ 是 $D\times D$ 阶矩阵。

5）求解协方差矩阵的特征向量 $\boldsymbol{p}$ 和特征值 λ，如式(3)所示：

$$\frac{1}{N}\sum_{i=1}^{N}\phi(x_i)\phi(x_i)^{\mathrm{T}}=\lambda p \tag{3}$$

6）并设矩阵 $\boldsymbol{K}=[\phi(\boldsymbol{X})]^{\mathrm{T}}\phi(\boldsymbol{X})$，其中 $\boldsymbol{K}$ 为 $N\times N$ 对称半正定矩阵，$K_{ij}=\phi(x_i)^{\mathrm{T}}[\phi(x_j)]$。通过代入并化简步骤 4）可得 $\boldsymbol{K}\cdot\boldsymbol{K}\alpha=\lambda\boldsymbol{K}\alpha$。不需要具体计算 $\phi(\boldsymbol{X})$，只需定义特征空间中向量的点积，就可以获得 $\boldsymbol{K}$。本文使用 Gaussian 函数作为核函数，如式(4)所示：

$$k(x,y)=\exp\left(-\frac{\|x-y\|^2}{2\sigma^2}\right)=\exp(-\gamma\|x-y\|^2) \tag{4}$$

7）在改进后采用欧氏距离来计算样本点之间的距离，通过欧氏距离更好地表示样本之间的差异，再用 PCA 做线性降维。其中 γ 值是超参数，它控制样本点在高维空间中的分布，值越大，数据越集中，数据将更容易区分，核函数如式(5)所示：

$$k(x,y)=\phi(\boldsymbol{x})^{\mathrm{T}}\varphi(\boldsymbol{y}) \tag{5}$$

其中，$k(x,y)$ 为核函数，可实现将低维向量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 投映在高维空间 F 中，高维向量 $\phi(\boldsymbol{x})$ 和 $\phi(\boldsymbol{y})$ 的点积表示空间中任意一点到某一中心点的欧氏距离。通过核函数计算矩阵 $\boldsymbol{K}$ 的特征值，得到相对应的特征向量 $\boldsymbol{a}$，如式(6)所示：

$$p=\sum_{i=1}^{N}\alpha_i\phi(x_i)=\varphi(\boldsymbol{X})\alpha \tag{6}$$

其中，$\boldsymbol{p}$ 为 D 维列向量，$\boldsymbol{a}$ 为 N 维列向量。

本文基于 PCA 线性可分进行改进形成 CGKPCA 算法，它继承了 PCA 算法的优点，并且高斯核函数有效地扩展支持非线性可分数据，并提高了异常流量检测模块的准确率。

3.2　改进的 SVMS 模型

由于传统单一机器学习模型的预测准确率不高，近年来为了解决这个问题，引出了集成学习模型。本文介绍的就是 Stacking 集成模型不同于 Bagging 和 Boosting 集成学习模型，它可将不同性质的学习模型拟合在一起。本文创新性地把不同性质的集成学习模型当成 Stacking 模型的第一层，第一层包括使用改进后的 SVM 模型和 ERT 模型，逻辑回归模型作为第二层拟合第一层模型，从而提高了整体的预测准确率。其中 Meta-Classifier 采用改进性 LR 模型。本文改进 SVM 模型采用 Sigmoid 函数作为 Kernel 函数，LR 模型也采用 Sigmoid 函数，这种改进能够有效拟合第一层模型，同时避免梯度消失的问题。通过改进基学习器和元学习器，Stacking 集成学习模型能够改善分类模型的整体性能。CGKPCA 的流程如图 3 所示。SVMS 模型的原理图如图 4 所示。

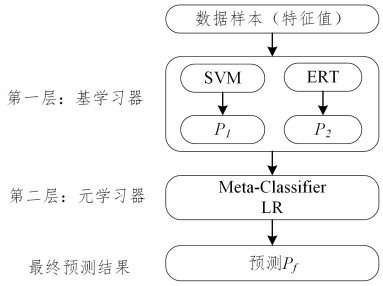

图 4　改进后的 SVMS 模型

Fig. 4　Improved SVMS model

改进型的机器学习模型的原理利用 Stacking 技术可以拟合多个不同性质分类模型的能力，通过改进 Stacking 模型的方法，即改进后 Stacking 模型由 SVM 和极端森林组成第一层，Stacking 第二层采用改进的 LR 模型用于拟合第一层的模型。SVMS 模型具备各种不同模型的特点，从不同角度对异常流量进行预测，极大地提高了模型的泛化能力。

本文通过提高机器学习的预测准确率来预测 SDN 网络中的流量是否异常，并使 SDN 控制器采取相应行动以保障 SDN 网络安全运行。为了提高检测模块的预测准确率，本文采取了两种关键优化方法。1）应用 CGKPCA 算法实现非线性降维，并利用该算法提高预测准确率。CGKPCA 算法能够在降低数据维度的同时处理数据样本之间的非线性关系。2）运用 SVMS 模型的特性，有效地优化模型的分类能力，

实现从不同角度、不同维度对数据特征进行训练学习，通过强大的 SVMS 模型极大地提高了模型的预测正确率。

4 实验结果及分析

4.1 实验环境

为了验证本文方法的有效性，本文的实验环境为 Windows10 操作系统，配备 12th Gen Intel Core i7 12700K CPU 和 64GB 内存。本文使用 VSCode 1.17.2 为集成开发环境，使用开发语言为 python3.9 和机器学习库 Scikit-learn 1.0.2。本文采用 CGKPCA_SVMS 模型对异常流量进行分类检测。

4.2 模型性能评价指标

为了比较不同模型的检测性能，本文选用以下性能评价标准：准确率 Accuracy、F1 分数、召回率 Recall 及精确率 Precision。TP 和 TN 分别代表了正确分类的正常样本和非正常样本；FN 和 FP 分别代表了错误分类的正常数据和非正常结果；其计算式如式(7)－式(10)所示：

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

$$Recall=\frac{TP}{TP+TN} \tag{8}$$

$$Precision=\frac{TP}{TP+FP} \tag{9}$$

$$F1=2\times\frac{Precision\times Recall}{Precision+Recall} \tag{10}$$

4.3 模型实验数据分析

本文基于 KDDCUP99 和 UNSW-NB15 数据集，通过超参数调优，使得分类模型能达到最佳性能。不同算法的性能评价如表 1、表 2 所列。

表 1 基于数据集 KDDCUP99 不同算法在异常流量检测上的性能对比

Table 1 Performance comparison of different algorithms in abnormal traffic detection based on dataset KDDCUP99

(%)

算法	AC	F1	Recall	Precision
GA[16]	93.37	99.70	99.80	99.56
SVM-RBF[17]	99.11	99.03	98.97	99.10
CA-FELM[18]	99.8	93.04	94.12	92.00
CGKPCA_SVMS	99.97	99.98	99.98	99.99

表 2 基于数据集 UNSW-NB15 不同算法在异常流量检测上的性能对比

Table 2 Performance comparison of different algorithms in abnormal traffic detection based on dataset UNSW-NB15

(%)

算法	AC	F1	Recall	Precision
SVM-RBF[17]	93.94	94.44	93.23	95.67
Stacking ensemble[19]	94.00	95.00	93.00	96.00
PCA_RF[20]	98.8	95.47	99.29	91.93
CGKPCA_SVMS	99.66	99.29	99.39	99.19

表 1 列出了不同算法在 KDDCUP99 数据集上的实验结果。从表 1 的性能指标上可以看出，本文提出的 CGKPCA_SVMS 模型对比 GA[16] 优化特征选择模型的预测准确率提高了 6.6%；本文模型对比 SVM-RBF[17] 集成算法模型的准确率提高了 0.86%，本文模型对比 CA-FELM[18] 主成分分析的模糊极限学习算法的准确率提高了 0.17%。根据本文的研究结果，CGKPCA_SVMS 优化模型在各项性能指标上都优于对比模型。

表 2 列出了不同算法在 UNSW-NB15 数据集上的实验结果。从表 2 所列的性能指标上可以看出，本文提出的 CGKPCA_SVMS 模型的性能对比 SVM-RBF[17] 模型准确率提高 5.72%；本文模型对比 Stacking 集成模型[19] 准确率提高 5.66%；本文模型对比 PCA_RF[20] 模型准确率提高 0.86%。本文提出的模型分类算法在分类准确率方面表现出更高水平，该模型在 Recall，Precision，F1 值上也取得了显著的提升。

结束语 本文提出了一种优化的分类模型算法，用于异常流量检测。首先，在建立模型的过程中应用 CGKPCA 算法，以解决特征维度高和数据冗余的问题。该算法能够有效降低数据集的维度，并提取出最重要的特征。其次，本文通过改进的分类模型 SVMS 提高分类模型的预测准确率。结果表明，本文提出的 CGKPCA_SVMS 模型算法对异常流量分类检测准确率较高，同时其召回率、精确率、F1 值也取得了显著的提升。因此改进后的方法对于异常流量的分类检测更为有效。综上所述，本文提出的机器学习异常流量检测方法 CGKPCA_SVMS 在实验中展现了较高的性能，能够有效地识别异常流量，为网络异常流量检测领域的研究和应用提供了有价值的参考。在下一步工作中，本文将继续对 CGKPCA_SVMS 方法进行改进，以进一步降低算法对于系统内存的占用率，进一步提高分类检测系统的性能。

参 考 文 献

[1] China Internet Network Information Center Releases the 51st Statistical Report on the Development Status of the Internet in China [J]. National Library Journal, 2023, 32(2): 39.

[2] ZHANG Y, CUI L, WANG W, et al. A survey on software defined networking with multiple controllers[J]. Journal of Network and Computer Applications, 2018, 103: 101-118.

[3] LU J, ZHANG Z, HU T, et al. A Survey of Controller Placement Problem in Software in Software-Defined Networking[J]. IEEE Access, 2019, 7: 24290-24307.

[4] LI H T, WANG R M, DONG W Y, et al. A GRU-based method for semi-supervised network traffic anomaly detection[J]. Computer Science, 2023, 50(3): 380-390.

[5] LI X, ZHANG X, ZHANG P, et al. Fault data detection of traffic detector based on wavelet packet in the residual subspace associated with PCA[J]. Applied Sciences, 2019, 9(17): 3491.

[6] WANG Y G, SHU Z Y, TIAN X. Incremental Kernel principle components subspace inference with mystrom approximation for Bayesian deep learning [J]. IEEE Access, 2021 (9): 36241-36251.

[7] ZHANG Z F, WANG L M. Research on network intrusion detection algorithms based on machine learning [J]. Computer Applications and Software, 2022, 39(10): 336-343.

[8] AL-FAWA'REH M, AL-FAYOUMI M, NASHWAN S, et al. Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior [J]. Egyptian Informatics Journal, 2022, 23(2): 173-185.

[9] MOHAMMADI M, RASHID T A, KARIM S H T, et al. A comprehensive survey and taxonomy of the SVM-based intrusion detection systems[J]. Journal of Network and Computer Applications, 2021, 178: 102983.

[10] KHOEI T T,AISSOU G,HU W C,et al. Ensemble learning methods for anomaly intrusion detection system in smart grid [C]// 2021 IEEE International Conference on Electro Information Technology(EIT). IEEE,2021:129-135.

[11] ISLAM F B,NWAKANMA C I,LEE J M,et al. Enhancing Malicious Activity Classification of IoT Network Traffic Characteristics using Stacked Ensemble Learning[C]// 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation(ETFA). IEEE,2021:1-4.

[12] LI Q Y,XINGH J. KPCA Anomaly Detection Method Based on Maximum Correlation Entropy[J]. Computer Science, 2022, 49(8):267-272.

[13] PENG Y,FENG S,JIA S,et al. Research on satellite anomaly detection method based on PCA-DNMFSC[J]. Computer Simulation,2023,40(1):48-52,142.

[14] ZHUANG H,WENG Z,HE R,et al. GKEAL:Gaussian Kernel Embedded Analytic Learning for Few-Shot Class Incremental Task[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023:7746-7755.

[15] ZHAO Y,YI P,ZHANG Z,et al. Anomaly detection method for SDN network edge switch[J]. Computer Science,2023,50(1):362-372.

[16] HONG S S,LEE E,KIM H. An Advanced Fitness Function Optimization Algorithm for Anomaly Intrusion Detection Using Feature Selection[J]. Applied Sciences,2023,13(8):4958-4985.

[17] ALMAIAH M A,ALMOMANI O,ALSAAIDAH A,et al. Performance Investigation of Principal Component Analysis for Intrusion Detection System Using Different Support Vector Machine Kernels[J]. Electronics,2022,11(21):3571-3586.

[18] SINGH C E,VIGILA S M C. Fuzzy based intrusion detection system in MANET [J]. Measurement: Sensors, 2023, 26: 100578.

[19] RAJAGOPAL S,KUNDAPUR P P,HAREESHA K S. A stacking ensemble for network intrusion detection using heterogeneous datasets[J]. Security and Communication Networks,2020,2020:1-9.

[20] DO XUAN C,THANH H,LAMN T. Optimization of network traffic anomaly detection using machine learning[J]. International Journal of Electrical & Computer Engineering (2088-8708),2021,11(3):2360-2370.

CHEN Xiangxiao, born in 1983, postgraduate. His main research interests include network security and so on.

CUI Xin, born in 1972, Ph.D, professor. Her main research interests include next-generation internet technology, network security, network big data and wireless sensor network.