大数据背景下基于PCA-DELM的入侵检测研究

王振东，王思如，王俊岭，李大海

（江西理工大学 信息工程学院，江西 赣州 341000）

摘　要：恶意攻击类型及形式不断变化，攻击量逐渐增加，传统神经网络模型架构在提高模型精度、减少模型计算量、提高推理速度等方面起着重要作用，然而，传统模型架构搜索时需消耗大量计算资源，且泛化能力不高。对此，需提出针对大数据背景下网络攻击的解决方案。基于深度学习在网络安全方面的应用，在入侵检测领域结合主成分分析方法（PCA）并使用深度极限学习机（DELM）进行研究，设计一种轻量级神经网络PCA-DELM，在保留传统神经网络模型架构优点的同时，减小计算资源，提升泛化能力。仿真结果表明，相较于其他算法，优化后的轻量级神经网络模型PCA-DELM在不同的数据集上能显著提高入侵检测能力，加快检测速率。

关键词：入侵检测；网络安全；深度极限学习机；主成分分析；深度学习

DOI：10.11907/rjdk.222219　　开放科学（资源服务）标识码（OSID）：

中图分类号：TP309　　**文献标识码：**A　　**文章编号：**1672-7800(2023)012-0185-07

Research on Intrusion Detection Based on PCA-DELM in the Background of Big Data

WANG Zhendong, WANG Siru, WANG Junling, LI Dahai

(*School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou* 341000, *China*)

Abstract: The types and forms of malicious attacks are constantly changing, and the number of attacks is gradually increasing. Traditional neural network model architecture plays an important role in improving model accuracy, reducing model computation and improving reasoning speed, etc. However, traditional model architecture requires a lot of computing resources in search, and its generalization ability is not high. In this regard, it is necessary to propose solutions for network attacks in the context of big data. Based on the application of deep learning in network security, combined with principal component analysis (PCA) and deep Extreme Learning Machine (DELM) in the field of intrusion detection, a lightweight neural network PCA-DELM is designed to reduce computing resources and improve generalization ability while retaining the advantages of traditional neural network model architecture. The simulation results show that compared with other algorithms, the optimized lightweight neural network model PCA-DELM can significantly improve the ability of intrusion detection and speed up the detection rate on different data sets.

Key Words: intrusion detection; network security; extreme learning machine; principal component analysis; deep learning

0　引言

随着互联网的普及和计算机技术的更新发展，网络中产生的数据规模愈发庞大，其中存在着大量的网络攻击行为威胁互联网环境和网络安全。再加之5G、云计算和物联网等技术的广泛应用，数据在互联网中的传输速度极大提高，大数据时代来临，其集中化、高透明、大规模的特征为信息安全维护带来了巨大挑战。因此，大数据背景下的网络信息安全是目前各界聚焦的关键难题。为应对上述问题，防火墙作为一种安全设备被广泛应用，通过管理员们所制定的安全规则防止某些数据流的传播，提高了接收数据流的准确性。然而，仅凭借防火墙自身无法辨别出正常数据流和异常数据流，入侵检测（Intrusion Detection，ID）

收稿日期：2022-10-17

作者简介：王振东（1982-），男，博士，江西理工大学信息工程学院副教授、硕士生导师，研究方向为无线传感器网络、智能物联网、大数据和信息安全；王思如（1998-），女，江西理工大学信息工程学院硕士研究生，研究方向为网络入侵检测；王俊岭（1976-），男，博士，江西理工大学信息工程学院副教授、硕士生导师，研究方向为分布式计算、计算机视觉；李大海（1975-），男，博士，江西理工大学信息工程学院副教授、硕士生导师，研究方向为分布式系统、服务质量（QoS）控制、分布式系统自学资源调度控制。本文通讯作者：王思如。

作为具有主动防御能力并能动态检测入侵行为的一种新型安全机制，已逐渐成为大数据时代下网络安全的关键技术。传统入侵检测方法对检测效率、检测规模、检测体系结构等存在某些限制，而智能入侵检测技术应用模糊信息识别、规则产生式专家系统、数据挖掘、机器学习及深度学习等技术，极大提高了入侵检测率和检测速度，最大可能地防御病毒入侵。

当前，入侵检测技术相关研究大多聚焦在以下3个方面：①基于数据挖掘的入侵检测，如王意洁等[1]基于同一网络威胁行为的预警间存在特定关系这一思想，应用数据挖掘算法寻找隐匿在数据分布背后的关系，并依据所发现的关联信息数据对威胁行为序列进行重构；②基于机器学习的入侵检测，Martins等[2]提出对抗性机器学习方法被应用于入侵及恶意软件检测场景中，实验结果表明，该方法在恶意软件及入侵检测中有效；③基于神经网络的入侵检测，Yang等[3]将改进的卷积神经网络（Convolutional Neural Networks，CNN）算法应用于无线网络模型，并进行相应的入侵检测，该算法优化的模型与其他机器学习算法相比，在执行效率和分类准确率等指标上均有良好效果，相比于传统入侵检测分类模型有明显提升。Yang等[4]针对物联网安全问题，结合LM算法优化速度快、鲁棒性强的特点，提出LM-BP神经网络模型，并将其应用于入侵检测系统，该模型通过LM算法对传统BP神经网络的权值阈值进行优化，再利用BP算法对数据集进行分类，具有更高的检测率和更低的虚警率，但学习速率较低。Wang等[5]利用深度卷积神经网络（CNN）学习网络数据流量的低层空间特征，然后利用LSTM网络学习高层时间特征，设计出一种新型网络入侵检测模型HAST-IDS，该模型通过多组基准测试，其结果表明HAST-IDS在准确率、检测率等方面均优于其他已有方法，提高了入侵检测实时性。

深度学习是神经网络的进一步发展，也是对人工智能技术的加强，它通过模仿人脑机制分析处理数据，利用深度神经网络，将模型处理得更为复杂，从而使模型对数据的理解更加深入，例如图像、声音和文本[6]。深度学习已经在控制领域[7]、自然语言处理[8]、情感分析[9]等领域取得成效，这些成果也证明了深度学习是具有实用性的分类识别工具。在入侵检测领域，Khan等[10]提出两阶段深度学习模型，第一阶段将网络流量分为正常和异常两类，第二阶段将第一阶段得到的特征状态作为检测的附加特征，该模型的优点在于从无标记的网络数据中提取有用的特征表示。Su等[11]在注意力机制与双向长短期记忆（BLSTM）的前提下，设计了交通异常检测模型BAT，该模型可快速有效地提高异常检测能力。Lee等[12]开发了基于事件分析的人工智能系统，用于处理数据并更好地运用不同的人工神经网络方法。

综上，虽然上述模型在入侵检测过程中展现出优越的性能，但在大数据时代下，数据流量的高速传输和庞大规模这两个特性要求入侵检测模型必须具有良好的实时性，若不能及时处理高速传输的网络流量，模型将出现严重时滞现象，无法抵御实时网络的安全威胁。因此，上述模型还存在以下问题：①两阶段深度学习模型中第一阶段在面对海量的网络数据时会大幅增加时间成本；②仅在一个数据集上的测试结果不能展现模型的泛化性和可移植性；③模型评价指标系统单一，没有其他评价指标进行交叉分析，不够全面。对此，本文在大数据背景下提出了一种轻量级神经网络的入侵检测模型（PCA-DELM），模型首先使用主成分分析方法（Principal Component Analysis，PCA）对含有正常或攻击的网络数据进行降维处理，这在庞大的数据集上能大幅减少时间成本，加快分类速率。鉴于极限学习机优秀的表征能力，将其引入到入侵检测领域，结合自动编码器（Auto Encoder，AE）对数据进行监督分类，再在UNSW-NB15数据集上进行二分类和多分类实验，测试其入侵检测性能并验证模型可移植性，最后在实时网络流量CIDDS-001数据集上模仿验证该模型在实际复杂的网络中对入侵行为的检测能力。以上实验均通过多个评价指标交叉分析本文分类模型与传统分类算法、经典机器学习分类器分类结果，实验结果表明，本文所提出的智能入侵检测方法在准确率、精确率、真正率等指标上有显著提高。

1 深度极限学习机

1.1 极限学习机

极限学习机（Extreme Learning Machine，ELM）[13]是一种针对于单隐层前馈神经网络（Single-hidden Layer Feed-forward Neural Network，SLFN）[14]的机器学习算法。与传统的SLFN算法不同，ELM可随机选择输入层权重和隐藏层偏置，输出层权重通过最小化由训练误差项和输出层权重范数的正则项构成的损失函数，依据Moore-Penrose广义逆矩阵理论计算求出[15]。相比于传统神经网络需人工设置大量参数，极限学习机训练参数更少、学习速度更快、泛化能力更强。

给定有N个标记样本数据的训练集，$k(x_i,t_i),x_i=[x_{i1},\cdots,x_in]^T\in R^n$表示第$i$个样本示例，$t_i=[t_{i1},\cdots,t_{im}]^T\in R^m$是每个样本示例所对应的标签，$n$表示训练数据集的特征个数，$m$表示训练数据集的类别个数。若样本$x_j$对应第$k$类，则将标签$x_j$的第$k$个值设定为1，剩余$(m-1)$个值设成-1。如图1所示，ELM的网络结构和单隐层前馈神经网络相似。

包含L个隐藏节点的ELM表示如下：

$$\begin{aligned}&\sum_{i=1}^{L}\beta_iG\left(\alpha_i,b_i,x_j\right)=t_j,\\&\alpha_i\in R^n,b_i\in R,\beta_i\in R^m,\\&j=1,2,\cdots,N\end{aligned}\tag{1}$$

$\beta_i=[\beta_{i1},\beta_{i2},\cdots,\beta_{im}]^T$是整个输出层的权重系数，$\beta_{i1}$

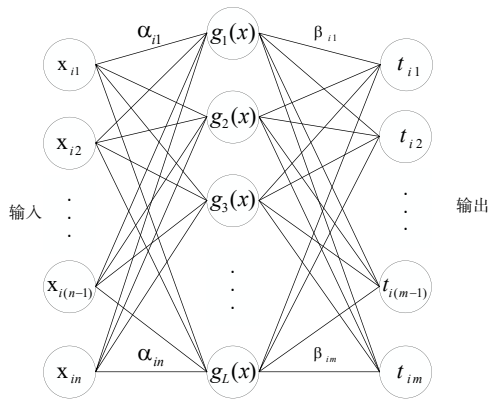

Fig. 1　ELM network structure

图1　ELM网络结构

代表 $g_1(x)$ 和 t_{i1} 两个神经元之间的权重系数，$\alpha_i = [\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{im}]^T$ 是连接输入层和第 i 个隐含层的输入权重，b_i 是第 i 个隐藏层的偏置，$G(\alpha_i, b_i, x_j)$ 是第 i 个隐藏层的输出矩阵。若第 i 个隐藏层的激活函数为 $g(x)$，则隐藏层的输出为：

$$G\left(\alpha_i, b_i, x_j\right) = g\left(\alpha_i \cdot x_j + b_i\right) \tag{2}$$

式(1)用矩阵形式表示为：

$$H\beta = T,$$

$$H = \begin{bmatrix} G\left(\alpha_1, b_1, x_1\right) & \cdots & G\left(\alpha_L, b_L, x_1\right) \\ \vdots & \ddots & \vdots \\ G\left(\alpha_1, b_1, x_N\right) & \cdots & G\left(\alpha_L, b_L, x_N\right) \end{bmatrix}_{N \times L} \tag{3}$$

$$\beta = \begin{bmatrix} \beta_1^T \\ \vdots \\ \beta_L^T \end{bmatrix}_{L \times m}, T = \begin{bmatrix} t_1^T \\ \vdots \\ t_N^T \end{bmatrix}_{N \times m}$$

为达到输出数据的期望值，训练网络后需得出参数最优值，使：

$$\min_{\alpha_i, b_i, \beta_i} \left\| H\left(\alpha_i, b_i\right)\beta_i - T \right\| = \left\| H\left(\hat{\alpha}_i, \hat{b}_i\right)\hat{\beta}_i - T \right\|, \quad i = 1, \cdots, L \tag{4}$$

深度极限学习机最终是要最小化实际输出和期望输出间的误差，也即最小化损失函数：

$$J\left(\alpha_i, b_i|, \beta_i\right) = \sum_{j=1}^{N}\left(\sum_{i=1}^{L}\beta_i g\left(\alpha_i \cdot x_j + b_i\right) - t_j\right)^2 \tag{5}$$

ELM算法中参数 (α_i, b_i) 是随机生成，因此也唯一确定。其解决方法可以转化为：

$$\beta = \arg\min_{\beta} \| H\beta - T \| \Rightarrow \beta = \left(H^T H\right)^{-1} HT \tag{6}$$

根据文献[16]可知，要求解的范数最小且唯一。为提高模型泛化能力，加入了正则项，求解问题则转化为：

$$\min_{\beta \in R^{L \times m}} \frac{1}{2}\| \beta \|^2 + \frac{\lambda}{2}\| H\beta - T \|^2 \tag{7}$$

其中，λ 是正则化系数，其解如下：

$$\beta = \left(\frac{I}{\lambda} + H^T H\right)^{-1} H^T T \tag{8}$$

其中，I 是单位矩阵。

1.2　基于ELM的表征学习

1.2.1　基于极限学习机的自编码器

自动编码器(Auto Encoder，AE)是一种无监督神经网络模型，它利用输入 X 自身作为监督，通过训练神经网络模型期望得到一个重构输出 X'。因此AE无需标记训练数据。在ELM中引入AE的思想，使ELM的输入也被视为目标输出，即输出 $Y = X$，引入自编码器的极限学习机ELM-AE(Extreme Learning Machineasan Auto Encoder)的网络结构如图2所示。

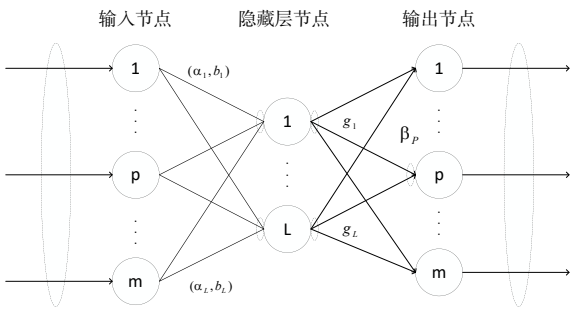

Fig. 2　ELM-AE network structure

图2　ELM-AE网络结构

简言之，ELM-AE类似于一个逼近器，其目标是尽可能让网络的输出与输入相同，同时使隐藏层的输入参数 (α_i, b_i) 随机生成后正交。其优势如下：

(1)可将输入数据映射到不同或等维度的空间，实现维度压缩、稀疏表达或等维度的特征表达。

(2)可清除特征之外的噪声，使特征之间分布更为均匀和线性独立，提高系统泛化性。

ELM-AE的输出可由式(1)转化为式(9)求出。

$$\begin{aligned} & x_j = \sum_{i=1}^{L}\beta_i G\left(\alpha_i, b_i, x_j\right), \\ & \alpha_i \in R^m, b_i \in R, \beta_i \in R^m, \\ & j = 1, 2, \cdots, N, \\ & \alpha^T\alpha = I, b^T b = 1 \end{aligned} \tag{9}$$

其中，α 是由 α_i 构成的矩阵，b 是由 b_i 构成的向量。

针对维度压缩和稀疏表达，隐藏层的输出权重 β 可由式(8)转化为式(10)求出。

$$\beta = \left(\frac{I}{\lambda} + H^T H\right)^{-1} H^T X \tag{10}$$

其中，$X = [x_1, \cdots, x_N]$ 是输入数据。

针对同维度的特征映射，权重 β 可由式(11)计算求出。

$$\beta = H^{-1}T \tag{11}$$

由文献[16]可知，$\beta^T\beta = I$。

1.2.2　深度极限学习机

基于ELM-AE的3种不同的特征表达功能，可以将其作为深度极限学习机(Deep Extreme Learning Machine，DELM)的基础模块。与传统深度学习算法相同，DELM应用逐层贪婪的方式训练网络，DELM每个隐藏层的输入权

重都用ELM-AE初始化，执行分层无监督训练。与传统深度学习算法相比，DELM没有反向微调的步骤。

DELM的目的是使输出信息无限逼近原输入信息，其基本思想是通过对每一层的训练，最大程度地减小重构误差，最终得到输入信息的高级特性。DELM模型的主要训练步骤则是将原始输入信息样本X视为下一个ELM-AE的目标输出($X_1 = X$)，从而得到输出权值β_1。然后，将DELM的第一个隐藏层的目标输出矩阵H_1，当作下一个ELM-AE的输入和目标输出($X_2 = H_1$)，依次逐步地展开训练，最后一层用ELM训练，可以使用式(6)求解DELM的最后一个隐藏的输出矩阵β_{i+1}。DELM每一层隐藏层的输入权重矩阵为$W_{i+1} = \beta_{i+1}^T$。

2 基于PCA-DELM的入侵检测算法

2.1 PCA数据降维设计

主成分分析PCA(Principal Component Analysis)是统计学中的一种降维方法，它通过削减特征向量的数量降低矩阵维度。在神经网络中，可以采用PCA减少输入数据样本的特征维度，从而降低神经网络模型计算量，提升模型计算速度。假设给定原始数据集$A = \{a_{11}, a_{12}, a_{ij}, \cdots, a_{mn}\}$，其中$i$代表样本数据，$j$表示对应样本的特征维度，$m$和$n$分别表示样本个数和特征数量，数据集矩阵可用式(12)表示。

$$A_{m*n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & & a_{mn} \end{bmatrix} = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \tag{12}$$

PCA采用线性变换将原始数据变量转变成非线性相关的数据变量。通过求出协方差矩阵的特征向量和特征值，保留累计贡献率超过85%的特征向量，用原始数据矩阵乘以特征向量矩阵得到一个新的特征矩阵，从而降低维度。式(13)定义了数据集中不同维度上的均值μ。

$$\mu = \frac{1}{n}\sum_{j=1}^{n} z_i \tag{13}$$

使用式(14)计算样本点在不同维度上的偏差。

$$\varphi = x_{m*n} - \mu \tag{14}$$

数据集协方差矩阵H定义为。

$$H = \frac{1}{n}\varphi\varphi^T \tag{15}$$

对输入数据集协方差矩阵做奇异值分解(Singular Value Decomposition，SVD)可以得到一组特征值和特征向量$(\lambda_1, \mu_1), (\lambda_2, \mu_2), \cdots, (\lambda_n, \mu_n)$，它表示协方差矩阵$H$的$n$组特征值和特征向量，将原始数据映射到协方差矩阵中$k$个最大特征值所对应的特征向量张成的子空间中。式(16)给出了k的确定方法。

$$\sum_{j=1}^{k} \lambda_j / \sum_{j=1}^{n} \lambda_j \geq \beta \tag{16}$$

其中，β是子空间的特征值之和与原始空间的所有特征值之和的比值。选取最大的k个特征值后，可生成一个大小为$m*k$的矩阵B，按照式(17)将原始数据投影到k维子空间中。

$$y = A^T\varphi \tag{17}$$

式(12)—式(17)给出了去除不同特征间相关性的具体步骤。分别在两个数据集上调用上述方法实现降维。依据经验将β设置为0.85，并由式(16)在UNSW-NB15数据集和CIDDS-001数据集上分别保留前14、前6个特征向量，这种方法在消除不同维度相关性的同时，还可减少模型在训练过程中的存储开销。

PCA降维的时间复杂度为$O(min(m^3, k^3))$，m是样本数量，k为经PCA降维后保留的子空间维数。显然，$k < n$，故而$k^3 << n^3$，则文中使用PCA的时间复杂度近似为$O(k^3)$，与使用原样本相比，其开销相对较小。因此，即使模型在数据预处理阶段采取PCA降低特征维度维会增加消耗时长，但降维后模型运算量极大减少，为模型训练节省了更多时间，更好地满足了大数据环境下对入侵检测模型时效性的要求。

2.2 算法流程

本文提出的PCA-DELM入侵检测算法需通过3个阶段，检测前先对数据作预处理，然后用PCA对数据集进行降维处理，最后通过具有深度学习能力的极限学习机(Deep Extreme Learning Machine，DELM)对数据进行监督分类，完成入侵检测过程。PCA-DELM入侵检测流程包括以下步骤，流程如图3所示。

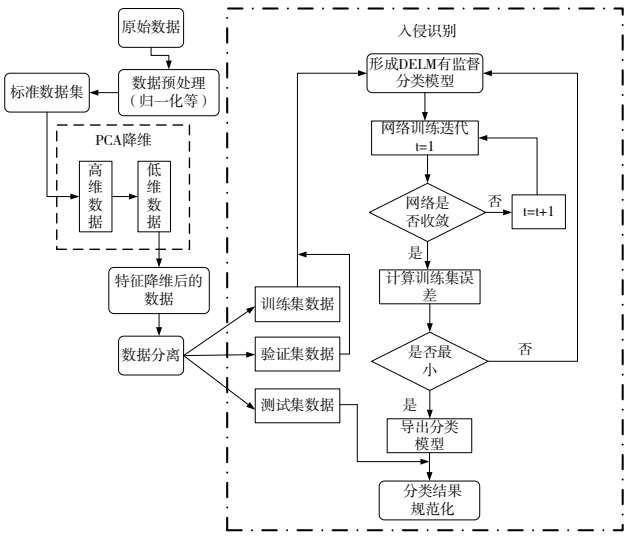

Fig. 3 Flow of DELM intrusion detection

图3 PCA-DELM入侵检测流程

(1)数据预处理。标准化UNSW-NB15和CIDDS-001数据集，对数据进行归一化处理后得到数值型数据，形成标准化数据集。

(2)定义DELM神经网络模型参数。根据寻参实验结果可知，网络迭代100次，隐含层共3层，在7070-120时，

网络分类性能最佳。

（3）PCA降维。对预处理后的高维数据集进行降维并得到低维表示的数据。

（4）数据分离。将降维后的数据按比例分为训练集、验证集、测试集。

（5）形成DELM有监督分类模型，将训练集和验证集数据输入到DELM分类模型中进行训练，调整模型。

（6）输出最优的DELM分类模型。

（7）输入测试集数据并输出分类规范化结果。

3　实验设置与分析

本文共做了2组实验。①在UNSW-NB15数据集及CIDDS-001数据集上进行二分类实验，在2个数据集上验证PCA-DELM入侵检测算法模型的分类检测性能；②在上述数据集上进行多分类实验，进一步验证该模型的网络分类性能及泛化能力，在实际包含不同攻击的复杂网络中对入侵行为的检测能力进行验证。

UNSW-NB15数据集包含2×10^5条数据，共49个特征。除正常数据外，还包含Fuzzers、Analysis、Backdoors、Dos、Exploits、Generic、Reconnaissance、Shellcode及Worms在内的9种攻击。CIDDS-001数据集包含6.8×10^5条数据，是来自于网络中的实时流量，包括在内部服务器（Web、文件、备份和邮件）和外部服务器（文件同步和Web服务器）上捕获的实时流量，包括14个特征。

3.1　评价指标

为更好地评估本文模型及算法的有效性，在二分类实验中，将数据集中的攻击合并为Abnormal，记为2，正常数据Nornal记为1。利用入侵检测准确率（Accuracy，Acc）、精确率（Precision，P）、真正率（True Postive Rate，TPR）、假正率（False Postive Rate，FPR）、F值、召回率（Recall）等指标对二分类实验进行评价。具体计算方法参考文献[17]。

3.2　分类性能分析实验

实验环境为Windows10，64位操作系统，处理器Intel（R）Core（TM）i5-6500CPU3.20GHz，安装内存（RAM）8.00GB，仿真环境是MatlabR2017b。在进行二分类和多分类实验前为验证PCA-DELM的分类性能，与ELM、DELM方法在UCI的Iris和Wine数据集上做了分类对比试验。本文提出的PCA-DELM分类器在所测试的数据集上的分类精度不低于ELM和DELM分类器，在Iris数据集上的分类准确率高达100%，在Wine数据集上的分类准确率高达93%。

3.3　二分类实验

仿真实验中，使用UNSW-NB15数据集和CIDDS-001数据集上进行入侵测试，将本文所提出的分类模型PCA-DELM与ELM分类模型、SOM网络分类模型、深度神经网络分类模型（DNN、DBN）、经典机器学习分类器进行对比实验，通过各种评价指标对算法模型进行比较，验证算法模型的性能。将数据集分为训练集和测试集，进行入侵检测仿真实验，各算法在两个数据集上的二分类测试结果如表1、表2所示。

Table 1　UNSW-NB15 binary classification test results

表1　UNSW-NB15二分类测试结果

Algorithm	Accuracy	Precision	Recall	F1-score	Time
DT	0.763 8	0.721 6	0.961 2	0.824 3	15 763 s
ELM	0.765 1	0.723 7	0.927 5	0.813	3 098 s
SVM	0.686 5	0.651 3	0.927 1	0.765 1	>20 h
SOM	0.449 4	NaN	0	NaN	200 s
DNN	0.734 2	0.720 2	0.845 9	0.778	>17 h
DBN	0.681 2	0.659 4	0.870 6	0.750 4	>17 h
DELM	0.742 1	0.696 2	0.943 2	0.801 1	3 218 s
本文	0.734 9	0.683 5	0.965 7	0.800 5	2 987 s

Table 2　CIDDS-001 binary classification test results

表2　CIDDS-001二分类测试结果

Algorithm	Accuracy	Precision	Recall	F1-score	Time
DT	0.937 4	0.957 2	0.949 7	0.953 4	17 987 s
ELM	0.817 6	0.817 6	1	0.899 6	3 987 s
SVM	0.892	0.998 3	0.869 3	0.929 4	>25 h
SOM	0.182 4	NaN	0	NaN	390 s
DNN	0.817 6	0.817 6	1	0.899 6	>20 h
DBN	0.976 6	0.996 2	0.869 6	0.928 6	>20 h
DELM	0.992 5	0.998 5	0.992 3	0.995 4	4 337 s
本文	0.817 6	1	1	0.899 6	3 872 s

由二分类实验结果可知，在UNSW-NB15和CIDDS-001数据集上，PCA-DELM入侵检测模型的测试准确率分别为73.49%、81.76%，在CIDDS-001数据集上的准确率较高。PCA-DELM方法在准确率方面十分稳定，波动较小，且处于较高的检测水平。

由表1可知，在UNSW-NB15数据集上，除SOM方法外，其余算法检测准确率均达60%以上，由于该数据集较为分散，分类难度高，故准确率普遍偏低。其中，PCA-DELM的准确率、精确率、召回率及F值分别为73.49%、68.35%、96.57%、80.05%，与较为稳定的SVM分类器相比分别高出4.84%、3.22%、3.86%、3.54%，在时间方面，PCA-DELM用时要少19 h以上。

由表2可知，DELM方法的检测准确率最高，为99.25%，接近100%，比效果最差的SOM高出81.01%，次优的分类模型为DBN，准确率为97.66%，在传统的机器学习分类器中，DT表现最佳。PCA-DELM的测试准确率在80%以上，且精确率、召回率为100%，时间为3 872 s，除去效果最差的SOM，时间在其余算法中最少。

综上，SVM分类器的性能在不同的数据集上能够保持相同的范围，且维持较高的准确率。然而，PCA-DELM分类模型的准确率与其他方法相比，在两个数据集上均较高且稳定，且高出0%~70.47%。当精确率和召回率发生冲突

时，对模型性能的比较会困难得多，但 F 值能够兼顾精确率和召回率，因此可看作是调和平均，以更好地对模型进行评价。实验结果表明，SVM 和 DT 分类器表现较好，说明 SVM 和 DT 方法适合二分类问题，但深度神经网络总体性能明显优于经典机器学习算法，在二分类方面颇具优势。

3.4 多分类实验

本文使用的 2 个数据集均为非平衡数据集，各攻击之间有所差异，故进行多分类实验，利用各种评价指标进一步分析各算法的入侵检测性能，验证比较算法模型可靠性。表 3 和表 4 为各算法模型多分类详细结果。

Table 3 UNSW-NB15 multi-classification test results(1)

表 3 UNSW-NB15 多分类测试结果(1)

Algorithm	Normal			Fuzzers			Analysis			Backdoors			DoS		
	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC
DT	0.748	0.051	0.849	0.426	0.127	0.650	0.083	0.033	0.525	0.249	0.051	0.599	0.129	0.028	0.551
ELM	0.647	0.132	0.813	0.280	0.082	0.794	0	0.006	0.495	0	0	0.500	0.444	0.053	0.775
SVM	0.874	0.456	0.709	0	0	0.500	0	0	0.500	0	0	0.500	0	0	0.500
SOM	0.424	0.961	0.138	0	0	0.500	0	0	0.500	0	0	0.500	0.219	0.737	0.295
DNN	0.694	0.315	0.664	0	0.001	0.500	0	0	0.501	0	0	0.500	0	0	0.501
DBN	0.870	0.457	0.700	0	0	0.500	0	0	0.500	0	0	0.500	0.005	0.001	0.502
DELM	0.576	0.140	0.809	0.097	0.040	0.580	0	0	0.500	0.009	0	0.505	0.025	0.003	0.772
本文	0.581	0.130	0.823	0.102	0.043	0.568	0	0	0.500	0.012	0	0.513	0.032	0.003	0.783

Table 4 UNSW-NB15 multi-classification test results(2)

表 4 UNSW-NB15 多分类测试结果(2)

Algorithm	Exploit			Generic			Reconnaissance			Shellcode			Worms		
	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC	TPR	FPR	AUC
DT	0.639	0.080	0.780	0.967	0.004	0.981	0.759	0.015	0.872	0.524	0.011	0.756	0.136	0.001	0.568
ELM	0.629	0.115	0.853	0.963	0.002	0.981	0.720	0.132	0.883	0	0	0.500	0	0	0.500
SVM	0.023	0.010	0.507	0.969	0.321	0.824	0	0	0.500	0	0	0.500	0	0	0.500
SOM	0	0	0.500	0	0	0.500	0	0	0.500	0	0	0.500	0	0	0.500
DNN	0.287	0.183	0.443	0.969	0.348	0.824	0	0	0.500	0	0	0.459	0	0	0.500
DBN	0.017	0.010	0.503	0.970	0.324	0.822	0	0	0.500	0	0	0.500	0	0	0.500
DELM	0.773	0.377	0.713	0.963	0.081	0.943	0	0	0.501	0	0	0.500	0	0	0.500
本文	0.781	0.368	0.721	0.964	0.081	0.944	0.001	0	0.510	0	0	0.500	0	0	0.500

在 UNSW-NB15 数据集上，包含正常数据和 9 种攻击。对于 Normal，PCA-DELM 与 DT 的 AUC 值最高，分别为 0.823 1、0.848 5，AUC 值最小的是 SOM，为 0.138 0。SOM、DELM、PCA-DELM 的真正率低于 60%，其余算法高于 64%，其中最高的是 SVM 分类器，高达 87.35%，但 DT 和 PCA-DELM 的假正率很低，分别为 5.05%、12.98%。对于 Fuzzers 攻击，SVM、DNN、SOM、DBN 的真正率为 0%，除 DNN 算法的假正率和 AUC 值分别为 0.5%、49.96% 外，上述其余算法的假正率和 AUC 值均为 0%，ELM 的 AUC 值最高，为 79.43%。对于 Analysis 攻击，除 DT 算法的真正率为 8.27%，其余算法的真正率均为 0%，DT、ELM 的假正率分别为 3.31%、0.64%，其余算法的假正率均为 0%，各算法的 AUC 值均在 0.5 左右。对于 Backdoors 攻击，DT、DELM、PCA-DELM 算法的真正率分别为 24.87%、0.86%、1.21%，其余算法的真正率为 0%，各算法的 AUC 值均在 0.5 左右。对于 Dos 攻击，除 ELM 算法的真正率最高为 44.44% 外，其余算法的真正率均低于 22%，PCA-DELM 的效果最好，AUC 值最高，为 0.783 2。对于 Exploit 攻击，PCA-DELM 的真正率为 78.1%，AUC 值为 0.721 3，对于 Generic 攻击，除 SOM 算法外，其余算法的真正率均能达到 95% 以上，其中 DBN 最高为 96.95%，PCA-DELM 的真正率为 96.43%，除 SOM 算法外，其余算法模型表现较好，AUC 值均能达到 0.8 以上。对于 Reconnaissance 攻击，所有算法模型的 AUC 值均在 0.5 以上，其中 ELM 的真正率最高，为 13.21%。对于 Shellcode 攻击，AdaBoost、DT 的真正率分别为 7.14%、52.38%，假正率分别为 0.2%、1.11%，其余算法的真正率和假正率均为 0%，大部分算法的 AUC 值为 0.5，包括本文提出的 PCA-DELM 模型。对于 Worms 攻击，仅 DT 的真正率为 13.64%，其余算法均为 0%，除 DT 的 AUC 值为 0.567 7，其余算法的 AUC 值为 0.5。

在 CIDDS-001 数据集上，对于 Normal，PCA-DELM 的真正率高达 95.99%，且 AUC 值高达 0.964 9；对于 Attackers，DELM 与 AdaBoost 算法的 AUC 值最高，分别为 0.923 1、1，其余算法的 AUC 值均在 0.5 上下，所有算法的假正率趋近于 0% 或者为 0%；对于 Suspicious，除 SOM 算法外，其余算法的真正率均达到 85% 以上，其中 DNN 的真正率为 100%，PCA-DELM 的真正率为 97.31%，AUC 值为 0.707 6，模型性能优于大部分其他算法模型；对于 Unknown，PCA-DELM 的真正率仅 31.55%，但其 AUC 值为 0.642 9，假正率低至 2.98%，其余算法的 AUC 值大部分集中在 0.5 左右；对于 Victim，DT、SOM 的真正率为 100%，DELM 算法的真正率为 99.45%，剩余算法的真正率为 0%，DT、DELM 的 AUC 值分别为 0.957 5、0.990 5，其余算法均低于 0.6。图 4 和图 5 分别为两个数据集上的 ROC 曲线，直观地说明了 AUC 及

真、假正率之间的联系。表5为各算法在不同数据集上检测所花费的时间，显然，PCA-DELM模型检测时间明显少于其他算法，更具实时性，在大数据时代下更具优势。

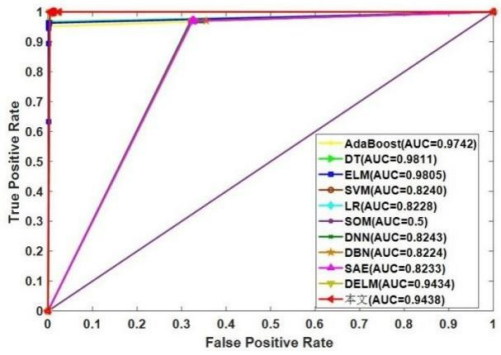

Fig. 4　UNSW-NB15-Generic ROC curve

图4　UNSW-NB15-Generic ROC曲线

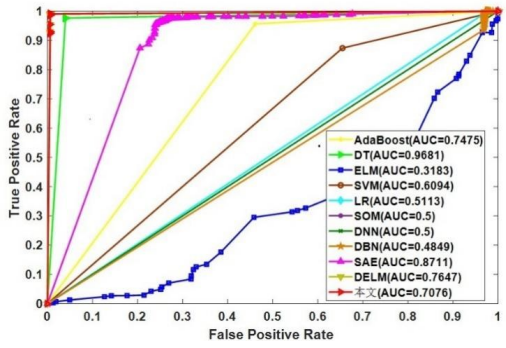

Fig. 5　CIDDS-001-Suspicious ROC curve

图5　CIDDS-001-Suspicious ROC曲线

Table 5　Time execution evaluation indicators

表5　时间执行评价指标

Algorithm	DT	ELM	SVM	SOM	DNN	DBN	DELM	本文
UNSW-NB15	8 763 s	2 432 s	>24 h	140 s	>12 h	>12 h	2 678 s	2 345 s
CIDDS-001	9 087 s	4 321 s	>28 h	200 s	>15 h	>15 h	4 531 s	4 213 s

二分类实验及进一步的多分类实验结果表明，在准确性方面，PCA-DELM模型性能明显优于经典神经网络和经典机器学习算法，在二分类和多类方面都有很大优势，在其他评价指标上也体现出较大优势。

4　结语

本文利用PCA的降维能力，设计了一种基于主成分分析的强化深度极限学习机分类模型，并提出了PCA-DELM模型。一方面，使用PCA保证模型对数据的特征降维能力；另一方面，利用DELM保证对数据快速分类的能力。实验结果表明：①PCA-DELM入侵检测模型的数据分类性能稳定，不管是复杂高维数据，还是攻击类型多数据集，都能实现较优的入侵检测效果，且不敏感于特定数据集；②PCA-DELM入侵检测模型成功解决了现有方法（数据挖掘、传统机器学习等方法）存在的准确率、精确率、召回率、真正率等指标偏低的问题；③在2个网络入侵检测数据集上，PCA-DELM入侵检测模型与现有方法相比，在各类评价指标上均具有明显优势。特别是在实时网络数据集CIDDS-001上仍能表现稳定。PCA-DELM入侵检测模型为车联网、物联网等不同领域的安全问题方面提供全新、可行的解决方案及思路。本文采用的是有监督分类模型，因此对真实网络环境中未知攻击的检测还存在一定局限性。未来工作中，将考虑引入生成对抗网络（Generative Adversarial Networks，GAN）学习正常样本的检测入侵行为且不受限于特定样本的特性，以提升对未知攻击的检测率。

参 考 文 献：

[1] WANG Y J，CHENG L，MA X K. Survey of alert-correlation based on network threat detection techniques[J]. Journal of National University of Defense Technology，2017，39(5)：128-138.
王意洁，程力，马行空. 运用警报关联的威胁行为检测技术综述[J]. 国防科技大学学报，2017，39(5)：128-138.

[2] MARTINS N，CRUZ J M，CRUZ T，et al. Adversarial machine learning applied to intrusion and malware scenarios：a systematic review[J]. IEEE Access，2020(8)：35403-35419.

[3] YANG H，WANG F. Wireless network intrusion detection based on improved convolutional neural network[J]. IEEE Access，2019(7)：64366-64374.

[4] YANG A，ZHUANSUN Y，LIU C，et al. Design of intrusion detection system for internet of things based on improved bp neural network[J]. IEEE Access，2019(7)：106043-106052.

[5] WANG W，SHENG Y Q，WANG J L，et al. HAST-IDS：learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection[J]. IEEE Access，2018(6)：1792-1806.

[6] HINTON G E，SALAKHUTDINOV R R. Reducing the dimensionality of data with neural networks[J]. Science，2006，313 (5786)：504-507.

[7] YAN Z，XU Y. A multi-agent deep reinforcement learning method for cooperative load frequency control of multi-area power systems[J]. IEEE Transactions on Power Systems，2020，37(6)：4599-4608.

[8] OTTER D W，MEDINA J R，KALITA J. K. A survey of the usages of deep learning for natural language processing[J]. IEEE Transactions on Neural Networks and Learning Systems，2021，33(2)：604-624.

[9] LI C，WANG J，WANG H，et al. Visual-texual emotion analysis with deep coupled video and danmu neural networks[J]. IEEE Transactions on Multimedia，2020，24(6)：1634-1646.

[10] KHAN F A，GUMAEI A，DERHAB A，et al. A novel two-stage deep learning model for efficient network intrusion detection[J]. IEEE Access，2019(7)：30373-30385.

[11] SU T，SUN H，ZHU J，et al. BAT：deep learning methods on network intrusion detection using NSL-KDD dataset[J]. IEEE Access，2020 (8)：29575-29585.

[12] LEE J，KIM J，KIM I，et al. Cyber threat detection based on artificial neural networks using event profiles[J]. IEEE Access，2019 (7)：165607-165626.

[13] HUANG G B，ZHU Q Y，SIEW C K. Extreme learning machine：Theory and applications[J]. Neurocomputing，2006，70(1/3)：489-501.

[14] YU H，SUN C，YANG W，et al. AL-ELM：one uncertainty-based active learning algorithm using extreme learning machine[J]. Neurocomputing，2015(166)：140-150.

[15] HUANG G B. An insight into extreme learning machines：random neurons，random features and kernels[J]. Cognitive Computation，2014，6 (3)：1-15.

[16] JOHSON W B. Extensions of Lipschitz mappings into a Hilbert space [J]. Contemporary Mathematics，1984，43(26)：189-206.

[17] SHONE N，NGOC T N，PHAI V D，et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence，2018，2(1)：41-50.

（责任编辑：孙　娟　周星宇）