文章编号：2096-1472(2020)-07-10-03
DOI:10.19644/j.cnki.issn2096-1472.2020.07.002

基于主成分分析和多层感知机神经网络的入侵检测方法研究

刘 辉

(上海理工大学信息化办公室，上海 200093)
✉liu_hui@usst.edu.cn

摘 要：针对现有入侵检测系统(Intrusion Detection System，IDS)检测方法准确率低，泛化能力弱，收敛速度慢，易陷入局部最优等问题，提出基于PCA(Principal Component Analysis)和多层感知机神经网络(MLP)的入侵检测模型。该模型首先对数据进行预处理和降维，然后使用该PCA-MLP模型进行训练并使用测试集测试模型的准确率，最后优化分类器的性能。实验表明，该模型可以提高入侵检测系统的准确率，具有很强的泛化能力。

关键词：入侵检测；主成分分析；神经网络；PCA-MLP模型
中图分类号：TP309 **文献标识码**：A

Research on Intrusion Detection based on Principal Component Analysis and Multilayer Perceptron Neural Network

LIU Hui

(*Information Office*, *University of Shanghai for Science and Technology*, *Shanghai* 200093, *China*)
✉liu_hui@usst.edu.cn

Abstract: Due to the low accuracy, weak generality, slow convergence and easily falling into local optimum of the existing intrusion detection system (IDS), an intrusion detection model based on PCA (Principal Component Analysis) and BP multilayer perceptron neural network is proposed. In this model, data preprocessing and dimension reduction are firstly conducted. Then, the PCA-MLP model is used for training and accuracy is tested. Finally, the performance of the classifier is optimized. The simulation results show that the model can improve the accuracy of intrusion detection system and has strong generality.

Keywords: intrusion detection; principal component analysis; neural network; PCA-MLP model

1 引言(Introduction)

随着全球信息化浪潮的兴起，截至2017年12月末我国互联网用户已达7.72亿，然而网络安全正面临着巨大挑战。近些年来世界各国面临的网络安全威胁度也在同步增加，例如“7号军火库”泄露，“棱镜门”事件，“WannaCry勒索病毒”事件等。2014年2月27日，中央网络安全和领导小组成立，2017年6月1日《中华人民共和国网络安全法》开始施行，没有网络安全就没有国家安全，表明网络安全已经上升到国家战略的高度。

入侵检测系统(Intrusion Detection System，简称IDS)是一种在发现可疑传输时发出警报或者采取主动防御措施的网络安全设备，它可以对网络传输进行即时监视，是防火墙之后的第二道防线[1]。随着机器学习和深度学习研究的不断深入，如何采用人工智能方法进行入侵检测研究已成为网络安全领域的研究热点。文献[2]提出了基于PCA和SVM(Support Vector Machines)的入侵检测算法，但是针对个别攻击类型准确率较低。文献[3]提出了改进朴素贝叶斯算法，通过降低维度，巧妙地引入属性加值算法，通过分类调控参数来提高效率和准确率。文献[4]通过对数据特征降维和权值修正提出了一种PCA-BP神经网络入侵检测方法，改进了BP神经网络

收敛速度慢的缺点，提高了检测性能。除此之外，如遗传算法、神经网络、K-means算法、隐马尔可夫模型等也经常用于入侵检测。

本文提出的基于主成分分析技术和多层感知机神经网络的入侵检测模型，首先对数据进行预处理，然后利用主成分分析技术进行降维，构建神经网络模型，最后通过实验验证了该模型的准确率。

2　主成分分析(Principal component analysis)

在数据维数比较多的情况下，首先要做的工作就是对其进行降维。降维是一种映射关系，在保证原有数据本质尽量不变的前提下，将数据的维度降低[5]。常用的降维技术有奇异值分解(SVD)、因子分析(FA)、主成分分析(PCA)等。本文采用PCA技术进行降维操作，其目的是在“信息”损失较小的前提下，将高维的数据转换到低维，从而减小计算量。样本的“信息量”指的是样本在特征方向上投影的方差。方差越大，则样本在该特征上的差异就越大，因此该特征就越重要[6]。具体步骤如下：

(1)标准化处理数据集。

(2)计算样本矩阵的相关系数矩阵。

(3)计算相关系数矩阵的特征值和相应的特征向量。

(4)选择主成分，并写出主成分表达式。

主成分分析可以得到p个主成分，并且各个主成分的方差是递减的。根据主成分的累积贡献率从p个主成分中选择k个贡献率较大的主成分，贡献率是指某个主成分的方差占全部方差的比重[7]。贡献率越大，该主成分所包含的原始变量的信息越强。

(5)计算主成分矩阵。

根据标准化的原始数据，分别代入主成分表达式，就可以得到各主成分下的各个样品的新数据，即为主成分矩阵。

3　多层感知机神经网络(Multilayer perceptron neural network)

Keras是由Python编写的基于Tensorflow的深度学习框架，使用该框架可以快速构建多层感知机神经网络(MLP)。使用Keras构建神经网络有以下步骤：首先可以通过一系列的层来定义神经网络，网络的第一层必须要定义预期输入维数，输出层激活函数决定了预测值的格式，如sigmoid、relu等激活函数；第二步编译网络，根据Keras的配置转换成可执行的格式，同时练设定一些参数；第三步训练网络，调整权重以拟合训练数据集。将使用反向传播算法对网络进行训练，并使用在编译时制定的优化算法以及损失函数来进行优化。第四步评价网络，使用全新的数据集来评估神经网络的预测性能。评价模型将会评价所有测试集中的输入输出对的损失值，以及在模型编译时指定的其他指标。

4　基于主成分分析和多层感知机神经网络的入侵检测模型(Intrusion detection model based on principal component analysis and multilayer perceptron neural network)

基于主成分分析和多层感知机神经网络的入侵检测模型(PCA-MLP)，如图1所示。该模型首先对数据预处理，例如将非数字型字符转换成数字型、归一化处理和标准化处理，以便进行计算。然后利用主成分分析法对训练数据和测试数据同时进行降维，以保证新的训练数据和测试数据处在同一个基中；接着将数据输入到PCA-MLP模型中进行训练，并优化各种指标，提高模型的准确率，最后测试PCA-MLP网络的性能。

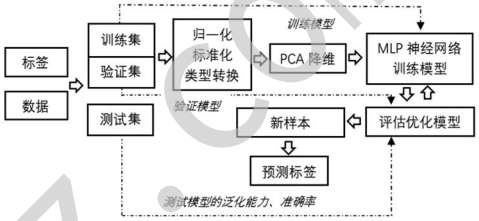


图1 基于主成分分析和多层感知机神经网络的入侵检测模型

Fig.1 Intrusion detection model based on principal component analysis and multilayer perceptron neural network

5　实验结果与分析(Experimental results and analysis)

5.1　实验数据集

本实验使用 KDD CUP 99数据集，该数据集包括全部训练集、10%训练集和corrected测试集。KDD CUP 99数据集中的每条记录都有41个属性和一个类别标签。每条记录被标记为一个正常类型或一个特定的攻击类型。数据集中标识类型共有5大类，40个小类[8]。本文的训练集和测试集分别为KDD CUP 99数据集中的10%训练样本和corrected的测试样本，其中10%训练集含494021条记录，本文将该数据集按照一定比例分为训练集和验证集用于模型的训练[9]，分布情况如表1所示。10%训练集中共出现22种攻击类型，而剩下的17种只在测试集中出现，这样设计的目的是检验分类器模型的泛化能力，对未知攻击类型的检测能力是评价入侵检测模型的重要指标。

表1 攻击类型正在数据集中分布情况

Tab.1 Distribution of attack types in data set

Tpyes	Train Set	Test Set	Train Set(%)	Test Set(%)
Normal	97278	60593	19.69	19.48
DOS	391458	229853	79.24	73.91
R2L	1126	16189	0.23	5.20
Probe	4107	4166	0.83	1.34
U2R	52	228	0.01	0.07
Total	494021	311029	100	100

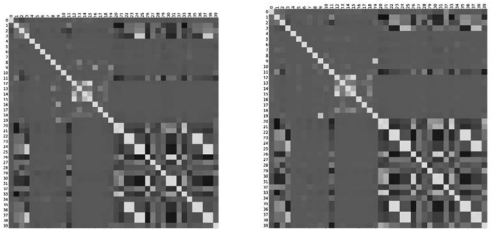
在实验之前需对数据进行预处理，将文本行数据转换成数值型数据，例如protocol_type字段，该字段有三种取值tcp、udp和icmp，转换后的对应关系为tcp 1、udp 2和icmp 3，同时使用该方法处理service、flag、label等字段。

5.2 实验过程

本实验在硬件环境为8GB内存、i7 3.4GHz CPU、500G硬盘的Windows 10操作系统下进行，利用Python作为仿真环境，实验采用 KDD CUP 99数据集，实验步骤如下。

(1)数据集归一化，由于个别字段的取值范围相差较大，因此需要做归一化处理以防止过拟合和收敛速度慢等问题的出现。使字段数据在[−1,1]，然后进行标准化。

(2)去除数据集中冗余属性，观察可知个别属性取值过于单一，全部取值为某一个固定值，删除该类属性。数据集的属性相关性矩阵如图2所示。



(a)训练集属性相关性矩阵 (b)测试集属性相关性矩阵

图2 训练集和测试集属性相关性矩阵

Fig.2 Correlation matrix of training set and test set

(3)特征提取，从数据集中提取有效特征，使用主成分分析技术对数据进行降维处理，根据特征的重要程度，达到对数据压缩的效果，同时最大限度地保持原有数据的信息。通过因子分析，如图3所示，当主因子为25个时较为合适。

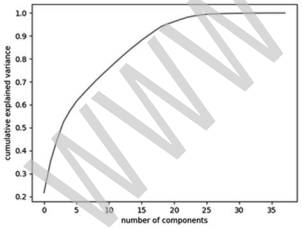


图3 降维过程

Fig.3 Dimension reduction process

(4)构建Sequential模型：采用三层神经网络即输入层、隐藏层、输出层，为了防止过拟合加入dropout层，训练过程中随机丢掉一定比例的数据。

(5)编译模型，在编译之前，对模型进行设置，其中包括优化器(Optimizer)选择、损失函数设定及定义指示列表等。

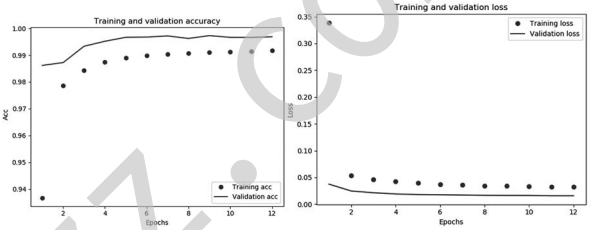
(6)训练模型，设置两个参数batchsize和epoch。①batchsize：批大小，即每次训练在训练集中取batchsize个样本训练；②epoch：迭代次数，一个epoch等于使用训练集中的全部样本训练一次。

(7)测试模型准确率和损失率，然后根据结果进行优化。

5.3 优化实验结果

神经网络模型在训练的过程中，需要配置很多参数，才能达到比较优的效果，这些参数的设置没有固定的原则，可以根据经验或者反复训练来调优。

如图4所示训练集上acc(准确率)处于上升趋势，loss(损失率)处于下降状态，但是随着epoch值得不断增大，在第9次迭代时acc达到了最优，此时loss几乎处于平稳状态，而后面的acc反而有一定程度的下降，这是过拟合的一个表现。因此可以认为epoch值取9较为合适，可以终止训练。



(a)训练集上准确率趋势图 (b)训练集上损失率趋势图

图4 训练集上准确率和损失率趋势图

Fig.4 Chart of accuracy rate and loss rate on training set

实验采用的数据集是稀疏的，所以采用自适用方法进行优化，常用的有 Adagrad、Adadelta、RMSprop、Adam。实验结果如表2所示，随着梯度变的稀疏，Adam比RMSprop效果会好，因此选择Adam作为优化器。

表2 常用优化器准确率对比

Tab.2 Comparison of accuracy of common optimizers

优化器	测试集准确率 (%)	测试集损失率(%)
Rmsprop	97.02	6.52
Adam	98.53	1.07
Adagrad	98.19	3.08
Adadelta	97.27	4.51

通过以上实验我们得出PCA−MLP模型正在测试集上表现十分突出，测集上准确率高达98.53%，使用测试集评估只用了25s，而且具有很强的泛化能力。

为了评估本算法在入侵检测上的性能，将其与赵广振等人[10]提出的基于PCA−PNN算法、黄思慧等人[11]提出的基于PCA−ELM模型、刘珊珊等人[12]提出的基于PCA−PSO−BP算法模型、刘婷等人[7]提出的PCA−GMM模型进行对比。如图5所示，本文所提出的PCA−MLP模型测试集准确率最高，优于其他算法。

(下转第9页)