基于深度堆栈编码器和反向传播算法的网络安全态势要素识别

寇 广*① 王 硕② 张 达②

①(国防科技创新研究院人工智能研究中心 北京 100072)

②(信息工程大学 郑州 450001)

摘 要：网络安全态势要素识别的基础是对态势数据集进行有效的特征提取。针对反向传播(BP)神经网络对海量安全态势信息数据学习时过度依赖数据标签的问题，该文提出一种结合深度堆栈编码器和反向传播算法的网络安全态势要素识别方法，通过无监督学习算法逐层训练网络，在此基础上堆叠得到深度堆栈编码器，利用编码器提取数据集特征，实现了网络的无监督训练。仿真实验验证了该方法能有效提升安全态势感知的效能和准确度。

关键词：网络安全态势；反向传播神经网络；堆栈编码器；数据分析

中图分类号：TP311 **文献标识码**：A **文章编号**：1009-5896(2019)09-2187-07

DOI: 10.11999/JEIT181014

Recognition of Network Security Situation Elements Based on Depth Stack Encoder and Back Propagation Algorithm

KOU Guang① WANG Shuo② ZHANG Da②

①(*Artificial Intelligence Research Center*, *National Innovation Institute of Defense Technology*, *Beijing* 100072, *China*)

②(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The basis of the identification of network security situation element is to perform the feature extraction of situation data effectively. Considering the problem that the Back Propagation(BP) neural networks have excessive dependence on data labels when it has a learning of massive security situation information data, a network security situation element identification method is proposed, which combines deep stack encoder and BP algorithm. It trains the network layer by layer through unsupervised learning algorithm. On this basis the deep track encoder by stacking can be obtained. The unsupervised training of the network is realized when using the encoder to extract the characteristic of the data sets. It is verified by simulation experiments that the method can improve the performance and accuracy of situational awareness effectively.

Key words: Network security situation; Back Propagation(BP) neural network; Stack encoder; Data analysis

1 引言

随着网络规模的不断扩大，传统行业与互联网的结合越来越广泛，人们的工作生活已高度依赖于网络。但是目前网络安全问题凸显，国家互联网应急中心(CNCERT)发布的《我国互联网网络安全态势综述》[1]报告显示，2018年度拦截的恶意程序创下了历史新高。充斥着各种已知和未知威胁的网络空间安全环境受到了严峻挑战，而传统的安全产品或者技术只能单一地反映网络一项或某几项指标，已经无法满足管理人员及时掌握网络整体安全状况的需求。网络安全态势感知技术融合了入侵检测系统(Intrusion Detection System, IDS)、防火墙、病毒检测系统(Virus Detection System, VDS)等网络安全设备的大规模安全数据，通过安全大数据分析驱动安全防护应用，对网络安全状况与趋势呈现一个全面反映，从而实施网络预警与应急响应。因此，网络安全态势感知技术逐渐成为网络空间安全领域的研究热点。

在网络安全态势感知的过程中，管理员往往需要面对海量的安全数据，对于这些复杂、冗余的数据，由人直接去分析处理是十分困难的。网络安全态势要素识别，可以充分利用各类安全设备的大规

收稿日期：2018-11-05；改回日期：2019-03-18；网络出版：2019-04-16

*通信作者：寇广 kg5188@163.com

基金项目：国家自然科学基金(61303074)

Foundation Item: The National Natural Science Foundation of China (61303074)

模安全数据，分析数据之间的联系，采用定性和定量的方法对数据进行模式识别，帮助管理员判别网络安全状态，利用计算机的高速计算能力模仿人脑对非线性的态势数据进行处理分析，极大地节省了人力，提升了系统整体效率。由此可见，网络安全态势要素识别作为态势感知的基础，具有极其重要的研究价值和应用意义。

目前国内外众多学者在此领域开展了广泛研究。Srihari[2]提出了一种基于概念的要素提取方法，主要目的是提取安全态势识别要素。该方法的要素提取效果比较好，但也存在缺点，例如：对于入侵攻击种类考虑不全；数据来源单一；未对态势识别结果做进一步分析等。Zhang等人[3]提出了一种网络安全态势要素识别框架，该框架通过构建层次化的模型，对网络入侵进行监测分析，来达到网络安全态势评估的目的。由于该框架的核心是入侵检测，在理想环境下，网络的威胁主要来自入侵攻击，但是在现实环境中，受各种复杂因素的影响，识别的结果比较局限。韦勇等人[4]提出了基于信息融合的网络安全态势要素识别模型，该模型通过D-S(Dempster-Shafer)证据理论对网络安全态势要素进行数据融合，将不同网络安全设备的报警信息合理融合，达到了态势识别数据准备工作的目的，为态势识别打下了一定基础。但是在具体设计上，对网络安全态势识别的指标选取有遗漏，没有在时间维度上分析指标，导致识别结果失准。陈秀真等人[5]提出的层次化实时网络安全风险识别的方法，该方法使用互联网中部署的入侵检测系统信息，根据从下至上、由点及面的策略构建了一个分层安全态势识别模型。模型从3个层次计算网络态势，分别是系统服务、主机状态和网络结构。该方法有效减轻了管理员对告警数据的分析任务，同时层次化的结构使得态势展示更为直观。但是，该方法的实验分析数据来源单一，不能完全体现网络承受的攻击行为。受算法复杂度限制，不适用于大规模网络和多网段局域网。此外，Liu等人[6]提出了利用数据挖掘进行态势识别，目的是对安全态势要素进行融合。该方法的输入为网络系统的数据，利用数据挖掘的方法对海量数据进行融合分析，达到了态势识别的目的，是一种安全态势识别研究的新视角。但是存在冗余数据提取不完全、安全要素提取有缺失、时间复杂度过大等问题。

从上面的研究现状分析中可以看出，学者们从不同领域对网络安全态势要素识别进行了研究，例如模糊识别、粗糙集、贝叶斯网络、博弈论、证据理论等，很多优秀的模型被提了出来。在应用中，这些模型的实际效果存在一些不足，例如在识别过程中基本概率分配过度依赖领域知识和专家经验，先期经验知识库的建立和大量训练样本的选取代价较大，影响了网络安全态势准确度。

本文认为神经网络由于隐藏层数目和隐藏层神经元多，具有强大的表达数据能力，可以克服上述缺点，适合进行网络安全态势要素识别。在诸多神经网络中，反向传播(Back Propagation, BP)是应用较多的一种，用于态势要素识别也有很多的优点。特别是，2006年，Hinton等人[7]首次提出逐层无监督贪婪训练(Restricted Boltzman Machine, RBM)，再固定每层学习到的参数，最后堆叠成深层网络(Deep Belief Network, DBN)，从而完成网络的预训练，再利用有标签的数据对BP算法微调深层网络参数，在mnist数据库上取得了当时最好成绩。Erhan等人[8]更进一步认为这种机制实际上是一种正则化。从此之后，深度学习(Deep Learning, DL)逐渐成了机器学习领域的研究热点[9]。DL方法相继在图像识别、语音识别、自然语言处理、文本处理等方面大幅刷新基准库测试准确率。随着DL的发展，人们把BP神经网络看作编码器和解码器模型，在此基础上可以衍生出堆栈式自动编码器(Stack Auto-Encoder, SAE)、堆栈降噪自动编码器(Stack Denoising Auto-Encoder, SDAE)[10]、收缩自编码器(Contractive Auto-Encoder, CAE)[11]等。

2 结合深度堆栈编码器与BP算法的安全态势要素识别

BP神经网络的识别方法是基于网络态势数据有标签的前提下，但在实际的网络环境中，给每一条网络数据人工分类是不现实的，因此单纯依靠BP神经网络无法完成对实际网络的安全态势要素识别，针对BP神经网络的缺点，采用深度堆栈编码器对BP神经网络方法进行改进，构建深度堆栈编码器与BP算法结合的神经网络(以下简称改进型BP神经网络)以弥补BP神经网络在无监督数据下识别的不足[12]。

2.1 神经网络模型建立

以自动编码器(Auto Encoders, AE)作为改进型BP神经网络的基本结构，AE基于神经网络算法，将输入层的输入变换到隐藏层，隐藏层对输入重构输出。AE通过调整训练参数，当目标输出与初始输入近乎相等时，中间各层的权值就相当于输入数据的几种不同表示，它们就是数据的特征。AE的基本结构如图1所示。输入数据进入编码器，编码器产生一个编码，用于表示输入数据，为了确定这个编码可以表示输入数据，本文使用解码器对

编码进行解码，将重构后的输出与原始输入数据比对，如果二者相等，本文就承认这个编码的准确性。通过调整编码器和解码器的参数，令重构误差最小，就可以得到输入数据的另一个特征。

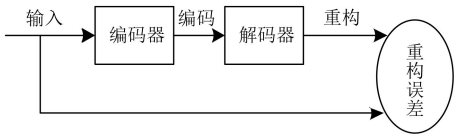


图 1 自动编码器的形象化表示

AE的输入与输出同为n维，隐藏层为m维。

编码过程是在输入层和隐藏层之间

$$h = f(x) = s_f(\boldsymbol{w}x+\boldsymbol{p}) \tag{1}$$

解码过程是在隐藏层和输出层之间

$$y = g(h) = s_g(\tilde{\boldsymbol{w}}h+\boldsymbol{q}) \tag{2}$$

其中，f, g分别代表编码与解码映射函数，s_f, s_g代表编码器和解码器的激励函数。一般，非线性变换可以使用多种函数，例如：sigmoid函数、tanh函数等。$\boldsymbol{w}$, $\tilde{\boldsymbol{w}}$分别表示$m \times n$和$n \times m$的权值矩阵，一般取$\tilde{\boldsymbol{w}} = \boldsymbol{w}^{\mathrm{T}}$。$\boldsymbol{p}$, $\boldsymbol{q}$为偏置向量。

对于AE的输入训练集$S = \{X^{(i)}\}_{i=1}^{N}$，AE整体重构误差函数为

$$J_{\mathrm{AE}}(\theta) = \sum_{x \in S} L(x, g(f(x))) \tag{3}$$

训练的目的是找到AE参数θ的整体重构误差最小值，这里取$\theta = \{\boldsymbol{w}, \boldsymbol{p}, \boldsymbol{q}\}$，根据输入输出的具体情况，重构误差函数$L$可以选择均方误差或交叉熵。当激励函数为sigmoid时，重构误差函数

$$L(x, y) = -\sum_{i=1}^{n}[x_i \ln(y_i)+(1-x_i)\ln(1-y_i)] \tag{4}$$

然后使用梯度下降算法最小化AE的代价函数，就可以得到参数θ。

常规的单层AE结构与单层神经网络十分相似，如图2所示。

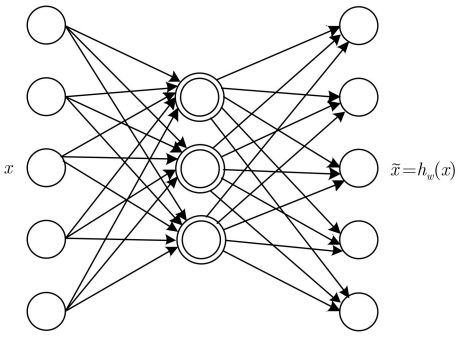


图 2 AE网络结构图

二者都是一个3层的神经网络，所不同的是，AE试图通过训练找到一个函数使得输入与输出尽量相等，即

$$h_{\boldsymbol{w}}(x) \approx x \tag{5}$$

换句话说，就是本文希望AE能够通过训练数据集的训练学习得到变换函数使得网络输出$\tilde{x} \approx x$。通过对AE结构参数的调整，我们可以发现训练数据的组成规律，举例来说，给定训练数据集为40维的矩阵，显然网络的输入输出神经元均为40个，设置网络的隐藏层神经元个数为20，这样就强制将输入的40维数据进行了压缩，也就是说，AE从网络的20个隐藏层节点中重构出了40个节点的输入数据。这一过程在输入数据完全随机时的难度相当巨大，AE经常难以从数据中获得相关特征。为此需要构建深度堆栈编码结构，深度堆栈编码器具有模型结构方便简洁，特征提取准确等优点，本文基于AE构建了一个用于网络安全态势要素识别的结合深度堆栈编码器和BP算法的神经网络模型。

改进型网络的具体形成过程如图3所示。

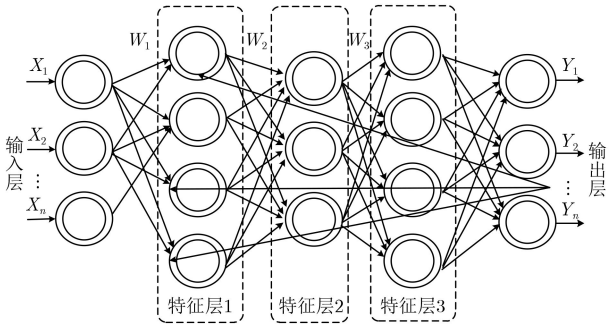


图 3 改进型神经网络形成图

改进型神经网络在AE的基础上进行了拓展，利用无监督逐层预训练方法和网络结构参数优化方法，以AE为基本单元构建深层堆栈编码网络，实现从无标签数据中获得多维复杂输入数据的分层特征值，得到原始数据的分布式特征表示。

无监督预训练阶段不同于有监督训练阶段，训练样本是用输入自身来代替标签。本文希望所提的网络能够很好给输入进行编码，最后通过解码网络去恢复出当时的数据。当我们训练完第1个AE后，所有训练样本经过编码器得到了特征，把这些特征再作为下一个AE的输入，再按照相同的方法去训练本文的网络。最后把训练好的网络堆叠在一起，形成深度堆栈网络。

至此，这个网络还不能用于态势要素识别，因为它还不会将一个输入和一种识别类型联系起来，它只是通过编码器提取得到了数据的特征并将其进

行重构输出。为了能够让编码器具有识别分类能力，我们需要使用少量有标签数据在有监督学习下微调网络参数，从而得到最终的网络。

2.2 训练算法

改进型BP神经网络的训练过程主要分为两步：第1步是网络的预训练，利用无标签数据对网络进行无监督训练，确定网络各层之间权值系数的范围空间，避免随机化的权值系数，利于下一步对网络结构的优化调整；第2步是对网络微调，选用BP算法利用少量有标签数据对经过预训练的网络进行微调，调整的关键是将整个堆栈编码器看作一个部分，使用有监督训练方法对网络各层参数及权值进行优化微调。具体训练算法如下：

预训练阶段：

步骤1 训练第1个AE，使得它的初始重构误差达到最低；

步骤2 将上一个AE的输出作为下一个AE的输入，按照上一步的要求进行训练；

步骤3 重复步骤2的过程，直到下一层的训练完成为止；

步骤4 最后一层的输出是下一个有监督层的输入，前面各层均保持不变，初始化有监督层参数。

通过对网络进行预训练，可以将参数空间限制在一个合理的范围内，便于下一步有监督训练对参数的微调，同时可以构建强度较大的网络结构，使得网络层次更深，网络稳定性和可靠性更好。

网络微调阶段：

步骤1 网络结构初始化，将之前经过预训练确定的参数输入网络，初始化网络的权值系数、偏置向量等参数；

步骤2 根据有标签数据利用BP算法对网络进行有监督训练，计算每一层的输出向量；

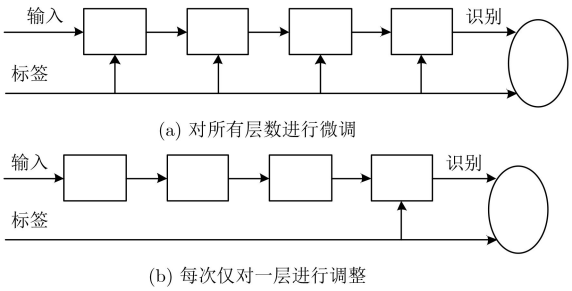
步骤3 计算网络中每一层的重构误差，据此对网络权值系数和偏置向量进行微调；

步骤4 将网络性能指标与预设的阈值进行比对，如果网络不能达到标准，则跳转到步骤2继续微调，直至网络达到预期的标准。

其中，根据有标签数据的数量，可以选择对所有层数进行微调，也可以选择只对末一层进行微调。当数据较为充分时，第1种微调方式是最好的选择，这种方式可以取得最好的效果，当有标签数据数量不足时也可以选择第2种方式。图4所示说明了这两种微调的方式：

改进型BP神经网络的训练算法流程图如图5所示：

网络映射函数$f: R^N \to R^M$在训练之后可以确定，这个函数即可以用于网络安全态势要素识别。



(a) 对所有层数进行微调

(b) 每次仅对一层进行调整

图 4 改进型BP神经网络的两种监督学习微调

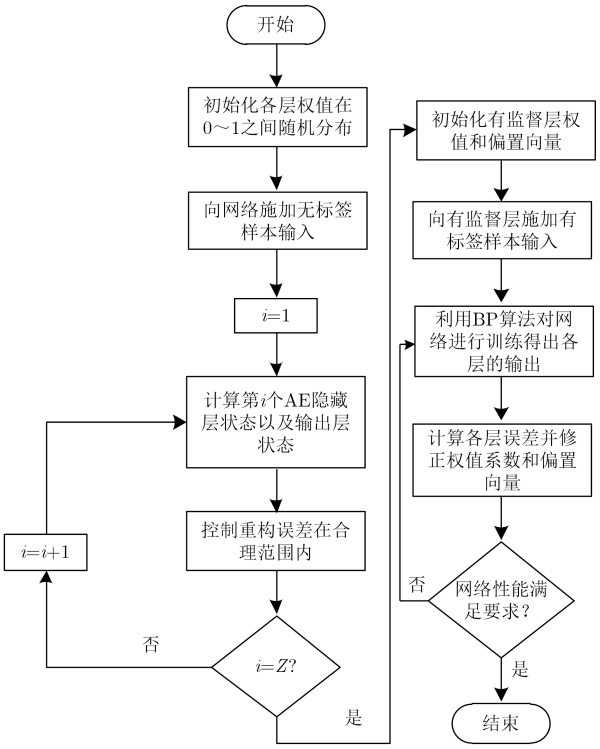


图 5 改进型BP神经网络训练算法流程

学习的过程，神经网络的主要任务是充分利用训练数据集中的样本所带来的信息建立学习模型。确切地说，对于一个输入x_i，经过学习训练的模型$y=f(x)$会产生一个输出y_i，如果这个输出y_i和训练数据集中对应的结果Y的差别足够小，就可以说这个模型的识别能力较好。反之，如果差别较大，该模型的识别能力则较差。训练系统通过不断的训练及调整，选择出一个最优模型，以达到对训练数据集的最好识别效果。参数的选择与确定是算法实施的关键，从丰富数据增加多样性和减少模型复杂度两个方面加以限定。在此通过两种方法进行约束，一是通过尺度、旋转等变换增加数据的多样性，从而增大训练样本集的大小，并给数据增加噪声，将惩罚因子添加到一般的目标函数后面，以此限制网络参数大小；二是不仅仅给输入数据增加噪声，也给隐藏层的特征值也增加噪声，在每次迭代时候，随机化让神经元休眠，不参与网络训练，休

眠的神经元可被认为不是网络的组成部分，但它们的权值需要被保留，这等同于完成一次训练要优化多个模型。对于每次的输入数据，网络的结构都会进行改变，使得权值的更改不取决于固定的隐藏网络神经元。

这样就完成了使用大量无标签数据进行无监督训练，少量有标签数据进行微调的整个训练过程，这个使用深度堆栈编码器改进的BP神经网络具有类似于生物神经网络的结构特征，在某些情况下具备人脑的功能。改进型BP神经网络具有多层隐藏层能对复杂数据进行特征提取，底层隐藏层与高层隐藏层相互配合可以完成数据特征的组合，提取数据的层次特征值。另外，改进后的网络的结构完全，用于非线性数据具有较大优势，具有并行性、分布式、自组织等优点[13]。

3　仿真实验

3.1　实验数据来源

(1) DARPA 1999数据集。选择该数据集的理由主要有两点：第一, DARPA1999中包含攻击事件种类丰富，能完整支撑安全态势要素识别算法的实验；第二，该数据集在网络安全态势感知领域已得到广泛的认可，使用它作为实验数据源，便于将本文实验算法和模型与其他的算法模型进行比对。DARPA 1999数据集总共包含了5个星期的评测数据。该数据集覆盖了Probe, Dos, R2L, U2R和Data共5大类58种常见的攻击形式，数据集中每条记录包含38个属性和1个类别标签，是现阶段最全面的网络安全数据集[14]；

(2) UNB ISCX 2012 Intrusion Detection Evaluation Dataset数据集。该数据集包含了1周7天的正常和异常网络活动数据。其中，网络异常活动主要有Infiltrating the network from inside, HTTP DoS, IRCbotnet-based DDoS attack和Brute Force SSH 4种。相对于DARPA 1999数据集，该数据集包含的攻击行为更为复杂，更加符合当前网络攻击的特点，且数据集为有标签形式，是全世界公开的入侵检测研究的最佳数据集之一[15]。

本实验都是在MSM8255GPU处理器，GTX660显卡，Windows10操作系统下运行，基于MATLAB编程实现的。对于数据集(1)，实验选取数据集中40000条数据为训练集合，5000条数据为测试集合，识别5类攻击类型。数据集的维度为38维。具体含义可以参考DARPA1999官方数据说明。对于数据集(2)，由于数据集的形式是将4种攻击的数据分别与正常网络行为数据混在一起，形成4天的数据集，其余3天为正常网络行为数据集。本文选取了星期四的数据进行实验，该天数据包含了正常网络行为和IRCbotnet-based DDoS攻击行为，抽取40000条数据作为训练集，5000条作为测试集，并依据文献[16]，选取了20个能够反映攻击行为的特征作为输入，即数据集的维度为20维，输出为两类(攻击或正常)。

3.2　实验流程与结果

主要有神经网络构建、神经网络训练和网络测试3步，实验流程如下：

步骤1　原始数据收集与处理。选择从数据集中导入原始数据，将选取的数据集进行分组，分别为训练样本和测试样本数据，并形成统一的数据格式存放到矩阵中；

步骤2　神经网络初始化。利用神经网络的非线性数据处理能力得到神经网络各层权值系数，从而确定神经网络的各层参数及整体结构；

步骤3　神经网络训练。将训练数据输入识别模型，训练确定神经网络的各层权值系数；

步骤4　神经网络识别。将测试数据输入神经网络进行安全态势要素识别，判断识别率是否高于设定下限，如果高于下限，则保存参数后微调重复步骤3，否则直接调整参数跳转到步骤3。

经过训练，可以确定神经网络的结构，根据数据集的格式选择网络基本节点数，测试数据集有38维，待分类的攻击类型为5类，所以网络的结构为，输出层有5个节点，输入层有38个节点，隐藏层层数、节点个数以及学习率等参数通过实验来确定。本文通过设置(隐藏层神经元个数、学习率、Dropout概率、权值衰减、识别率)参数组用来测试其中一个最好的作为BP神经网络在DARPA1999数据集和ISCX 2012数据集上的识别。为达到最佳效果，识别率均为多次测量取平均值。深度堆栈编码器里面的参数众多，在预训练阶段，需要调整的有网络深度、学习率、Dropout等，在网络微调阶段还需要设置学习率、Dropout等。选择方式还是通过Grid Search方式，为达到最佳效果，识别率均为多次测量取平均值。

本文分别选取BP神经网络和改进型BP神经网络的最佳参数设置，在给定不同样本的情况下将二者的识别率进行统计并对比，结果如表1所示

图6给出了BP神经网络和改进型BP神经网络用于安全态势要素识别准确率的曲线图。从图6中可以看出，随着训练数据的增多，改进型BP神经网络和BP神经网络的识别率都呈现出上升趋势。前者态势识别率折线较为稳定，波动较小，同等数量的训练样本下，改进型BP神经网络的识别率优于BP神经网络。

为了进一步说明本文算法在解决传统信息数据

表 1 不同样本数量下的BP神经网络和改进型BP神经网络识别率结果

样本数量	识别率	
	BP	改进BP
1000	0.893	0.940
3000	0.919	0.954
5000	0.924	0.953
7000	0.892	0.954
9000	0.960	0.972
11000	0.957	0.970
13000	0.901	0.987
15000	0.952	0.982
17000	0.963	0.965
19000	0.959	0.986
21000	0.964	0.972
23000	0.966	0.980
25000	0.958	0.989
27000	0.959	0.979
29000	0.965	0.984
31000	0.965	0.988
33000	0.961	0.988
35000	0.972	0.978
37000	0.972	0.992
40000	0.975	0.993

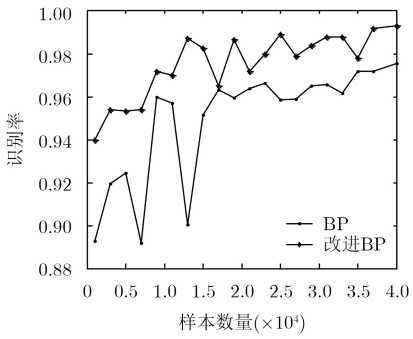


图 6 识别正确率比较

学习时过度依赖数据标签问题的有效性，进一步对比实验。分别选取了DARPA1999和ISCX 2012数据集中的20000条数据记录作为实验数据，其中训练集占比80%(即16000条)，测试集占比20%(即4000条)。针对此实验数据，通过去标签的方法，设计了训练集中标签占比不同的6组实验。特别说明：

(1) 训练集中标签占比10%，在16000条训练集中，有1600条数据有标签，14400条数据无标签；

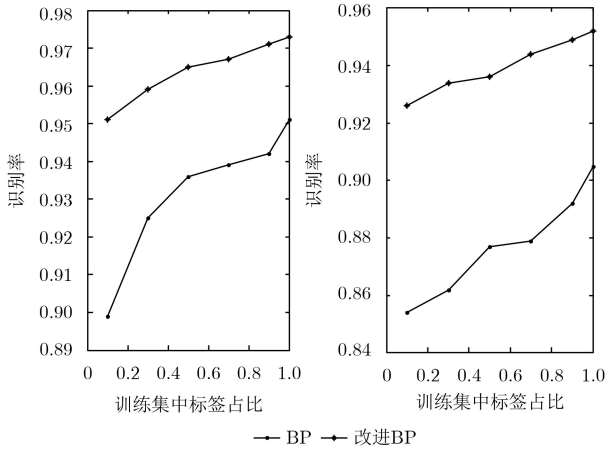
(2) 对于BP算法，可用训练样本仅为1600条有标签数据；而对于改进型BP算法，有16000条数据可用于预训练过程，1600条数据用于有监督的参数微调过程。

具体实验结果如表2：

表 2 不同标签占比下的BP神经网络和改进型BP神经网络识别率结果

训练集中标签占比(%)	识别率(DARPA1999)		识别率(ISCX 2012)	
	BP	改进BP	BP	改进BP
10	0.899	0.951	0.854	0.926
30	0.925	0.959	0.862	0.934
50	0.936	0.965	0.877	0.936
70	0.939	0.967	0.879	0.944
90	0.942	0.971	0.892	0.949
100	0.951	0.973	0.905	0.952

图7给出了不同标签占比下两种算法的识别率的曲线图。从图7中可以看出，在训练集数据大小固定条件下，随着训练集中标签占比的提高，改进型BP神经网络和BP神经网络的识别率都呈现出上升趋势：BP神经网络上升趋势快；改进型BP神经网络始终处于高识别率状态且上升趋势较缓。由此说明，改进型BP神经网络在态势识别率方面优于BP神经网络，且改进型BP神经网络能够充分利用无标签数据进行有效学习，能够解决传统信息数据学习时过度依赖数据标签问题。



(a) DARPA1999数据集结果 (b) ISCX 2012数据集结果

图 7 不同标签占比下两种算法识别率比较

利用无标签数据进行海量数据的无监督学习，充分发掘数据内在本质属性，利用少量有监督数据来进行网络的微调，极大提升识别能力。本文所采用的结合深度堆栈编码器和BP神经网络的模型及算法在训练的基础上得到测试结果的正确率最高达到99.8%(DARPA1999数据集)和97.2%(ISCX 2012数据集)，与BP神经网络相比有很大提高。

4 结束语

本文所提改进型BP神经网络识别方法，以自动编码器为基本组成单元，为网络安全态势要素识

别中无标签数据训练的实现提供了一种新的途径。本网络拓扑结构完整，具有良好的泛化能力。此外通过大量实验证实了基于深度堆栈编码器的改进型BP神经网络在网络安全态势要素识别上的有效性和准确性。

但是还存在几点不足需要下一步进行改进：

(1) 数据集种类还较单一。受时间和能力限制，本文的仿真实验只选取了两种较为权威的数据集进行试验，现实中的更复杂的网络面临更多的攻击类型，其安全态势要素识别将更加复杂，需进行实际测试；

(2) 网络参数设置效率低。本文针对神经网络安全态势要素识别进行了大量实验，根据实验结果从中选取了最优的网络参数设置，耗费了大量时间，在实际情况中应作出调整。

参 考 文 献

[1] 国家计算机网络应急技术处理协调中心. 2017年我国互联网网络安全态势综述[EB/OL]. http://www.cert.org.cn/publish/main/upload/File/situation.pdf, 2018.
National Internet Emergency Center. Summary of China's Internet security situation in 2018[EB/OL]. http://www.cert.org.cn/publish/main/upload/File/situation.pdf, 2018.

[2] SRIHARI R K. Situation awareness through concept-based information extraction[EB/OL]. http://www.dawnbreaker.com/vas05, 2015.

[3] ZHANG Songmei, YAO Shan, YE Xin'en, *et al*. A network security situation analysis framework based on information fusion[C]. The 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Chongqing, China, 2011: 326-332. doi: 10.1109/ITAIC.2011.6030216.

[4] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353–362.
WEI Yong, LIAN Yifeng, and FENG Dengguo. A network security situational awareness model based on information fusion[J]. *Journal of Computer Research and Development*, 2009, 46(3): 353–362.

[5] 陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885–897.
CHEN Xiuzhen, ZHENG Qinghua, GUAN Xiaohong, *et al*. Quantitative hierarchical threat evaluation model for network security[J]. *Journal of Software*, 2006, 17(4): 885–897.

[6] LIU Zhiming, LI Sheng, HE Jin, *et al*. Complex network security analysis based on attack graph model[C]. The 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control, Harbin, China, 2012: 183–186. doi: 10.1109/IMCCC.2012.50.

[7] HINTON G E, OSINDERO S, and TEH Y W. A fast learning algorithm for deep belief nets[J]. *Neural Computation*, 2006, 18(7): 1527–1554. doi: 10.1162/neco.2006.18.7.1527.

[8] ERHAN D, BENGIO Y, COURVILLE A, *et al*. Why does unsupervised pre-training help deep learning?[J]. *The Journal of Machine Learning Research*, 2010, 11: 625–660.

[9] BENGIO Y. Learning deep architectures for AI[J]. *Foundations and Trends in Machine Learning*, 2009, 2(1): 1–127. doi: 10.1561/2200000006.

[10] VINCENT P, LAROCHELLE H, LAJOIE I, *et al*. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion[J]. *The Journal of Machine Learning Research*, 2010, 11: 3371–3408.

[11] RIFAI S, VINCENT P, MULLER X, *et al*. Contractive auto-encoders: Explicit invariance during feature extraction[C]. The 28th International Conference on Machine Learning, New York, USA, 2011: 122-132.

[12] EVANS R and GREFENSTETTE E. Learning explanatory rules from noisy data[J]. *Journal of Artificial Intelligence Research*, 2018, 61: 1–64. doi: 10.1613/jair.5714.

[13] BRONSTEIN M M, BRUNA J, LECUN Y, *et al*. Geometric deep learning: Going beyond Euclidean data[J]. *IEEE Signal Processing Magazine*, 2017, 34(4): 18–42. doi: 10.1109/MSP.2017.2693418.

[14] LIPPMANN R, HAINES J W, FRIED D J, *et al*. The 1999 DARPA off-line intrusion detection evaluation[J]. *Computer Networks*, 2000, 34(4): 579–595. doi: 10.1016/S1389-1286(00)00139-0.

[15] SHIRAVI A, SHIRAVI H, TAVALLAEE M, *et al*. Toward developing a systematic approach to generate benchmark datasets for intrusion detection[J]. *Computers& Security*, 2012, 31(3): 357–374. doi: 10.1016/j.cose.2011.12.012.

[16] KONIDARIS G, KAELBLING L P, and LOZANO-PEREZ T. From skills to symbols: Learning symbolic representations for abstract high-level planning[J]. *Journal of Artificial Intelligence Research*, 2018, 61: 215–289. doi: 10.1613/jair.5575.

寇　广：男，1983年生，博士，副研究员，硕士生导师，研究方向为智能安全、智能算法等.

王　硕：男，1991年生，博士生，研究方向为网络安全.

张　达：男，1994年生，硕士生，研究方向为网络安全.