第31卷 第13期 计 算 机 工 程 2005年7月
Vol.31 № 13 Computer Engineering July 2005
·人工智能及识别技术· 文章编号：1000—3428(2005)13—0154—02 文献标识码：A 中图分类号：TP393.08

基于BP神经网络改进算法的入侵检测方法

危胜军，胡昌振，姜 飞
（北京理工大学网络安全技术实验室，北京 100081）

摘 要：对BP神经网络的算法进行改进：针对不同的训练样本，只激发网络中的部分神经元以产生输出。权值的调整只发生在与被激发的神经元相连弧线的权值上，而不是传统的BP神经网络需要对所有权值进行调整。实验结果表明，该算法在大样本训练网络时，可以显著提高网络的训练速度，减少训练的时间，同时还可以提高系统的检测率。

关键词：入侵检测；神经网络；BP算法；功能分布

An Intrusion Detection Method Based on Improved BP Neural Network Algorithm

WEI Shengjun, HU Changzhen, JIANG Fei
(Network Security Technique Laboratory, Beijing Institute of Technology, Beijing 100081)

【Abstract】The BP neural network algorithm is improved to detect intrusion. The improved method is as follows: according to different input, different part of network will be fired to generate output. The weights of the arcs only connected with fired neuron will be adjusted whereas all weights in traditional BP network must be adjusted. The experiment results indicate that this improved algorithm can increase learning speed and shorten training time. The results also show that the intrusion detection rate is improved.

【Key words】Intrusion detection；Neural network；BP algorithm；Function distribution

神经网络具有模式识别的功能，将神经网络用于入侵检测分类，也做了大量的研究工作。对于神经网络在入侵检测中的应用，前人所做的若干研究工作中大多数都是基于BP网络实现[1]。传统BP算法是一种梯度法，对于每个输入输出样本，网络的每个权值都影响着BP网络的输出结果，在网络的训练时需要通过反向误差传播进行调整，因而学习速度很慢。另外BP网络在实验中还暴露出很多性能上的不足[2]，诸如在训练大样本集时陷入局部极小、训练时间长不易收敛等。

本文提出一种BP神经网络的改进算法，将功能分布特性引入BP神经网络：对不同的输入，激发神经网络的部分神经元产生输出。这些激发的神经元形成激发路径。神经网络权值的学习只发生在激发路径的权值上。由于神经网络功能分布的实现，可以较好地改善算法的学习速率，降低平均误差，提高系统的识别率。

1 BP神经网络的改进算法

1.1 BP神经网络的基本结构

反向传播（BP）网络是典型的前馈型网络，从结构上它属于多层网络，包括输入层、隐含层和输出层。层与层之间采用全互联方式，同一层之间没有连接。网络中每一层权值都可以通过学习来调整，网络的基本处理单元（输入单元除外）为非线性输入与输出关系。

1.2 BP神经网络的学习算法

BP网络的学习过程包括输出计算和反向误差传播两部分。当给定网络的一个输入模式，它由输入层单元传到隐层单元，经隐单元逐层处理后再送到输出层单元，由输出层单元产生输出模式，该过程称为前向传播。如果输出响应与期望输出模式的误差不在要求的范围内，则转入误差反向传播。将误差值反向逐层传送，并修正各层的连接权值。对于一组给定的样本，重复输出计算和误差反向传播过程，直到训练模式都满足要求，网络训练完成。BP网络学习是有导师学习，学习算法是δ学习规则的推广。

设输入层有n个神经元。有两个隐含层，分别有k_1和k_2个神经元。输出层有m个神经元。神经元的激活函数采用sigmoid函数。具体的学习算法如下：

（1）计算网络的实际输出。对于每个输入模式$X=x_1,x_2,\cdots,x_n$，计算网络的实际输出：$Y=y_1,y_2,\cdots,y_m$。

（2）计算误差。对于训练集中的第p个样本，设期望的输出为$T=(t_{p1},t_{p2},\cdots,t_{pm})$。定义误差函数：$E_p=\frac{1}{2}\sum_{i=1}^{m}(t_{pi}-y_{pi})^2$。对于训练集合中的所有样本，其总误差为：$E=\sum_p E_p$。

（3）权值的调整。利用梯度下降法求误差函数的极小值，w_{ij}的更新量Δw_{ij}由下式表示：

$$\Delta w_{ij}\propto -\eta\frac{\partial E}{\partial w_{ij}}$$

其中η为学习速率。

作者简介：危胜军（1975—），男，博士生，研究方向为网络安全技术；胡昌振，教授；姜 飞，工程师
定稿日期：2004-05-26 **E-mail：**buxy@bit.edu.cn

1.3 改进的 BP 神经网络算法

参考文献[3]提出了一种具有功能分布特性的学习网络的结构和算法。由于该种网络与神经网络在结构、学习算法以及功能上的相似性，本文将文献提出的功能分布的思想引入到神经网络中。实验结果证明了该方法的可行性，以及对系统性能的改善作用。

针对不同的输入，神经网络激发不同的部分。激发的神经元形成一条激发路径。具体的算法描述如下：

（1）所有的输入神经元无条件激发。

（2）隐含层的神经元之间进行竞争，具有最大绝对值输出的神经元激发。对每次前向过程的一次竞争，设有 n_l 个数量的神经元激发。这 n_l 个数量的神经元的输出绝对值最大。下标 l 表示第 l 次竞争。设隐含层的数量为 L，则最多有 L 次竞争。n_l 需要预先分配一个正整数。

（3）所有的输出神经元无条件激发。

在上述 3 步中，被激发的神经元的总数为 $N(t)$：

$$N(t)=\sum_{l=1}^{L} n_l + N_{in} + N_{out}$$

其中 N_{in} 为输入层神经元的数量，N_{out} 为输出层神经元的数量。这些 $N(t)$ 个激发的神经元形成激发路径，实现功能分布。

对神经网络的学习算法进行如下修改：针对训练样本，权值的调整只发生在激发路径的权值上。传统 BP 神经网络中，针对每个训练样本需要对网络中的所有权值进行调整。

该改进方法的基本思想是：如果神经元激发后的输出值很小，则忽略掉该神经元对其后各层神经元的影响。

2 BP 神经网络改进算法识别仿真

下面给出一个仿真事例来证明改进算法的可行性且网络的性能有所改善。网络的结构采用含有两个隐含层的 BP 网络，输入层有 2 个神经元，隐含层各有 10 个神经元，输出层只有 1 个神经元。因为含有两个隐含层，所以竞争的次数 L 为 2。将 n_1 和 n_2 的值分别设置为 1 和 2。对图 1 所示的输入输出关系进行建模。当输入位于第 1、3 象限，输出为 1，输入位于 2、4 象限，输出为 0。输入数据分布于以（1,1），（-1,1），（1,-1），（-1,-1）为中心的 2d×2d 大小的正方形内。

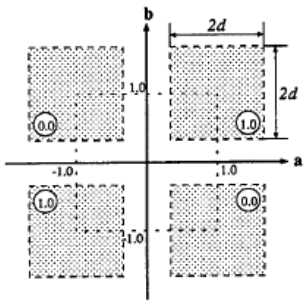

图 1 输入与输出之间的关系

分别采用改进算法和传统算法实现上述分类。仿真的初始条件为：权值和偏置的学习速率 $\eta=0.1$，激活函数 $f(x)=(1-e^{-x})/(1+e^{-x})$，权值的初始值是（-1.0,1.0）之间的随机数。

图 2 为实验中得到的改进算法和传统算法的学习曲线。通过对比发现，传统算法的学习曲线相对于改进算法存在更多的波动。随着 d 的变大，波动更加明显。学习曲线表明改进算法在非线性和不连续函数的实现上优于传统算法。

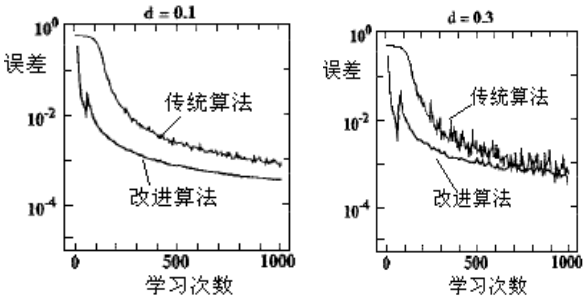

图 2 改进算法和传统算法的学习曲线

3 入侵检测实验设计

我们考虑将网络数据包的特征转化为可供神经网络学习的模式值，仅对 Back DoS，Buffer_Overflow，Guess_Passwd，Imap，Ipsweep Probe5 类经常出现的攻击进行基于改进算法和传统算法的对比识别实验，给出实验结果，对结果进行分析。

3.1 攻击数据源分析

数据采用 DARPA 1998[4]入侵检测评估数据库作为训练数据和测试数据。数据库包含 500 万条用于训练的 TCP/ IP 连接记录和 200 万条用于测试的记录。训练数据带有标记(正常或某种攻击)，按时间先后排序。每条记录含 41 个特征，分为 4 类：基本 TCP 特征，与有效载荷有关的特征，基于时间的流量特征和基于主机的流量特征。

取其中 20 000 条包含有以上 5 类攻击的记录，一半作为训练，另一半作为测试。其中正常连接 4 625 个，攻击连接 15 375 个。针对网络的攻击与以下基于时间的流量特征[5]的 9 项特征联系紧密，它们均为“在过去 2s 内”累积计算得到的连续量：Count (与当前连接去往相同主机的连接数)，Serror-rate (具有 SYN 错误的连接在 Count 中所占的百分比)，Rerror-rate (具有 REJ 错误的连接在 Count 中所占的百分比)，Same-srv-rate (提供同一网络服务的连接在 Count 中所占的百分比)，Diff-srv-rate (提供不同网络服务的连接在 Count 中所占的百分比)，Srv-count (与当前连接所提供的服务相同的连接数)，Srv-serror-rate (具有 SYN 错误的连接在 Srvcount 中所占的百分比)，Srv-rerror-rate (具有 REJ 错误的连接在 Srv-count 中所占的百分比)，Srv-diff-host-rate (去往不同主机的连接在 Srv-count 中所占的百分比)。针对主机的攻击与以下 6 项 TCP 连接个体的最敏感特征联系紧密：Duration(以秒为单位的连接的长度)，Dst-bytes (连接的目的端口发送的以字节为单位的数据量)，Src-bytes (连接的源端口发送以字节为单位的数据量)、Wrong-fragment (连接中出错桢的数目)，Urgent(连接中带有紧急指针的数据包的数目)，Num-failed-logins(连接中登录失败的次数)。以上 6 项均为连续量。将以上 15 项特征转化为网络的输入。

3.2 基于改进算法和传统算法的检测结果比较分析

神经网络采用如下结构：输入层的节点数为 15 个，隐含层的节点数为 20 个，输出节点数为 3 个。将改进算法的 n_1 和 n_2 都设置为 7，即每次竞争有 7 个具有最大绝对值输出的神经元激发。

（下转第 158 页）

如果在适应实例中引用的以前成功修改的实例和当前提取的实例相似的话，就把适应实例中的第3部分(修改历史)推荐给用户(图 1，步骤 3) 。由于提取的修改历史只是一个参考过程，并不能保证修改成功，因此就需要用户去修改或者精练修改次序。CBA 系统将记录用户的修改过程，存储在一个新的适应实例中，以便用来处理相似的修改过程(图 1，步骤 7) 。将当前提取的实例放入到适应实例的第 2 部分，同时将用户精练的修改规则序列放入到适应实例的第 3 部分。基于这种修改规则序列，适应实例的第 1 部分，即改写能力也可以放入到适应实例中去(图 1，步骤 8) 。通过这些步骤，就完成了一个实例的修改，同时也增加了一个新的适应实例(修改规则实例) 。

2.4 CBA 方法的评价

在建立 CBR 系统的时候，通常是先建立实例，而不会去建立适应实例，这就会出现一个问题，可能在实例库中存在足够多的实例，但适应实例库却缺少足够的适应实例，也就是缺少足够的修改规则序列。所以，在建立 CBA 系统的时候，就会面临两个问题：一是如何建立实例库；二是如何建立适应实例库，这需要足够的专家知识来建立一系列的修改规则。由于需要同时建立两个实例库，这无疑就增加了建立一个使用 CBA 系统的难度。而且，整个 CBA 系统要进行两个相似度的计算：一个是用户输入问题与实例库中存在的实例之间的相似度的计算，另一个是系统识别的修改能力与适应实例库中的修改能力的相似度的计算，而两种相似度的计算无疑会增加实例提取的难度。

3 结论

由以上分析可见，CBR 系统的研究呈现出一种不平衡。最困难的是实例修改技术，相关的研究却很少。鉴于实例修改的复杂性，CBR 系统应该是一个以 CBR 为基础、结合其他人工智能方法的混合型系统。本文在分析各种实例的修改方法的基础上，提出了将实例推理技术应用到修改规则库的建立，解决了单纯地运用规则推理进行实例修改所遇到的建立规则库的困难，为实例的修改提供了有益的借鉴。

参考文献

1 Lou Mather M. Issues and Application of Case-based Reasoning in Design[M]. Lawrence Erlbaum,1997

2 毛　权. 基于实例原型的设计方法及设计支持系统的研究[D]. 武汉: 华中理工大学,1995

3 周　馨, 刘溪涓, 钟廷修.工程设计中基于遗传算法的实例修改技术[J].设计理论与方法,2001,2(2):10-11

4 毛　权, 肖人彬, 周　济. CBR 中基于实例特征的相似实例检索模型研究[J]. 计算机研究与发展,1997,34(4):257-263

5 刘长毅, 徐　诚, 廖文和. CBD 中实例参数调整的诊断和判别[J]. 计算机应用,2002,22(9):97-99

6 应保胜,高全杰. 实例推理和规则推理在 CAD 中的集成研究[J]. 武汉科技大学学报,2002,25(1):61-65

7 Vong C M, Leungb T P, Wong P K. Case-based Reasoning and Adaptation in Hydraulic Production Machine Design[J]. Engineering Applications of Artificial Intelligence, 2002,15:567-585

(上接第 155 页)

初始条件为：学习速率为 0.15，动力因子为 0.075，$f(x)=1/(1+e^{-x})$。初始权值和阈值为（-1.0,1.0）之间的随机数。

实验的环境如下：Intel 公司 CPU，主频 1GHz、256MB 内存、Windows 2000 Server 操作系统环境。图 3 给出了改进算法和传统算法的学习曲线，表明改进算法的最小平均误差比传统算法的最小平均误差小，且学习速度快。表 1 为具体的训练时间和稳定时的最小平均误差。

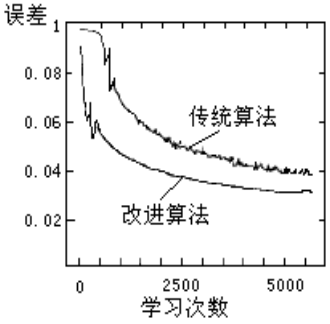

图 3 改进算法和传统算法的学习曲线比较

表 1 两种网络的训练时间和误差比较

训练时间		最小平均误差	
改进算法	传统算法	改进算法	传统算法
4 分钟 36 秒	8 分钟 30 秒	0.027 081	0.045 642

表 2 为对测试数据中所有攻击的检测率统计，表明针对大部分攻击基于改进算法的检测率都有一定程度的提高。

表 2 基于两种算法的检测率比较

攻击名称	检测率/ %	
	改进算法	传统算法
Back DoS	98.5	98.4
Buffer_Overflow	96.2	95.5
Guess_Passwd	93	92.9
Imap	71.4	72.6
Ipsweep Probe	100	100

4 结论

针对不同的输入，神经网络激活不同的部分进行识别，以此实现功能分布。通过仿真证实改进算法的性能优于传统算法。对攻击的识别实验结果表明，改进后的算法不仅能够很好地识别攻击，而且性能优于传统算法。

参考文献

1 Fox K, Henning R, Reed J,et al. A Neural Network Approach Towards Intrusion Detection. Tech. Rep., Harris Corporation, 1990-07

2 Cannady J, Mahaffey J. The Application of Artificial Neural Networks to Misuse Detection: Initial Results. Proceedings of First International Workshop on the Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium, 1998-09-14

3 Hirasawa K, Oka S, Sakai S, et al. Learning Petri Network with Route Control. In Proc. IEEE Int. Conf.Systems,Man,Cybernetics,1995: 2706-2711

4 Mukkamala S, Janoski G, Sung A. Intrusion Detection: Support Vector Machines and Neural Networks[DB/OL].http://www.computer.org/students/looking/2002fall/3.pdf, 2002

5 KDD2CUP299 Task Description[EB/OL]. http://kdd.ics.uci.edu/databases/kddcup99/task. html