神经网络算法在智能体IDS系统中的应用

孙 剑，许家珆

(电子科技大学应用数学学院 成都 610054)

【摘要】结合网络入侵和主机入侵方面的检测能力，构建了基于智能体的分布式入侵检测系统的体系结构模型。重点讨论了神经网络入侵检测算法。针对传统的BP网络在入侵检测应用中学习收敛时间和性能上的不足，提出了变速度回归神经网络(采用了批处理技术和动量方法)检测算法，通过对网络数据集的测试表明，该算法较传统BP网络，其学习训练次数大大降低，学习能力显著提高。

关 键 词 入侵检测系统； 智能体； 分布式入侵检测； 入侵检测算法； BP神经网络

中图分类号 TP393.08 文献标识码 A

Research of Neural Network Algorithm in Agent-Based Intrusion Detection System

Sun Jian，Xu Jiayi

(School of Applied Mathematic, UEST of China Chengdu 610054)

Abstract This paper designs an Agent-based Distributed Intrusion Detection System. The DIDS system combines host-based intrusion detection and network-based intrusion detection functions. It can be used to protect large area network and have relatively good expansibility. This paper also discusses the implementation of BP neural network in intrusion detection. Because of the traditional BP NN's weakness in learning time and performance, variable learning rate BP regression neural network (batch and momentum techniques are also used) are designed. The algorithm has been tested on a network data set. The result showed that it had much better performance than traditional BP NN.

Key words intrusion detection system; agent; distributed intrusion detection system; intrusion detection algorithm; back propagation neural network

入侵检测系统(Intrusion Detection System, IDS)是对计算机网络系统中的入侵行为进行自动检测的系统。其结构分为基于主机，基于网络和分布式三种类型。由于分布式入侵检测系统(Distributed Intrusion Detection System, DIDS)，可以实现入侵检测的分布式处理，具有很好的实时性和可扩展性，已成为研究的热点。入侵检测方法分为误用检测(misuse detection)和异常检测(anomaly detection) 两类。误用检测的优点是误报率低，检测速度快，但不能发现攻击特征库中没有事先指定的攻击行为，所以无法检测层出不穷的新攻击。异常检测是通过建立用户正常行为模型，以是否显著偏离正常行为为依据进行入侵检测。异常检测有一定的误报率，但有可能发现新的攻击行为。目前异常检测技术和分布式体系结构是入侵检测研究的前沿和热点。

1 基于智能体的分布式入侵检测系统体系结构

智能体(Agent)是指分布式系统或协作系统能自主发挥作用的计算实体，它具有自主性、交互性、反应

收稿日期：2003 – 06 – 26
基金项目：国防科研基金资助项目
作者简介：孙 剑(1981 –)，男，硕士生，主要从事信息技术与计算智能方面的研究；许家珆(1945 –)，女，教授，主要从事信息安全，网络多媒体信息处理方面的研究.

性和主动性的特征。

1.1 系统整体介绍

将基于主机和基于网络的入侵检测功能相结合，建立了基于智能体技术的分布式入侵检测系统的体系结构模型，如图1所示。主机和网络的入侵检测分别由基于主机的Agent与基于网络的Agent实现，通过移动Agent的协调实现相互通信，及入侵检测功能的分布式处理，所以系统具有很好的可扩充性。

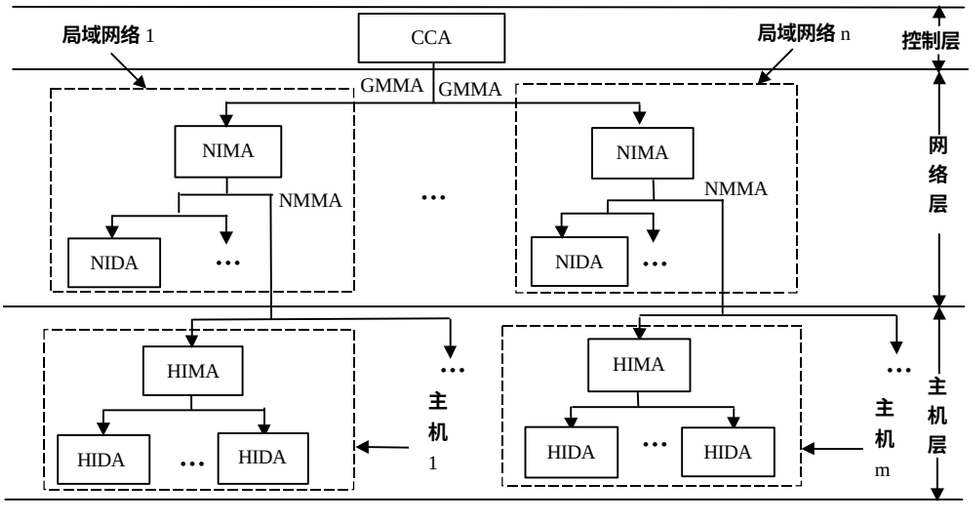

图1 基于智能体的分布式入侵检测系统的体系结构

1.2 系统各组成Agent介绍

主机入侵检测代理(Host Intrusion Detection Agent，HIDA)：

分布于网络的各个终端系统上，自主的完成主机的某一方面的入侵检测功能。检测数据来源于主机上的审计记录和系统调用序列。每台主机上多个 HIDA通过主机监控代理协调完成主机入侵检测功能。

主机入侵监控代理(Host Intrusion Monitor Agent，HIMA)：

分布于网络各个主机终端，且在各个终端上唯一。负责管理和协调分布在相应主机上入侵检测代理(HIDA)，并向所在局域网络的网络入侵监控代理报告入侵信息和数据。

网络入侵检测代理(Network Intrusion Detection Agent，NIDA)：

分布于大型网络的各个局域网上，收集和检测所在网络上的网络信息，向所在网段的NIMA提供入侵测试的结果和数据，并将测试结果和数据反馈给网段内的各主机监控代理(HIMA)。

网络入侵监控代理(Network Intrusion Monitor Agent，NIMA)：

分布于大型网络各个局域网络，且在各个局域网络上唯一。负责控制和管理所在网络上的网络入侵监控代理(NIDA)和主机入侵监控代理(HIDA)，并向整个网络的中央控制代理报告入侵信息和数据。

中央控制代理(Central Control Agent，CCA)：

对整个入侵检测系统进行控制和管理，接收来源于各个局域网络的入侵检测结果和数据，并将控制和管理信息提供给相关的网络入侵监控代理。主要用于防范大范围的网络入侵活动。

移动Agent：

1) 网络监控移动代理(Network Monitor Movable Agent，NMMA)：由网络入侵监控Agent产生，实现网络入侵监控Agent与所在局域网络中的主机监控Agent(HIDA)、网络入侵检测Agent(NIDA)之间的协作和交互。一方面将接收到的各个主机和网络的入侵检测系统的检测结果和数据提供给所在局域网络的网络入侵监控Agent。另一方面，将网络入侵监控Agent的控制和管理信息传达给相应的主机入侵监控 Agent和网络入侵检测代理。

2) 全局监控移动代理(Global Monitor Movable Agent，GMMA)：由中央控制Agent产生，实现中央控制Agent与各个网络入侵监控Agent的交互和协作。一方面将接收到的各个网络的入侵监控Agent的信息提供给中央控制 Agent，以便中央控制Agent对整个系统的管理和控制。另一方面，将中央控制Agent的控制和管理

信息传达给相应的网络入侵监控Agent。

2　神经网络入侵检测算法

入侵检测算法是入侵检测系统的核心部分。神经网络检测技术具有很强的非线性映射能力和学习能力，成为异常检测技术的研究热点。BP网络是实际应用最广泛的神经网络形式,但传统BP网络训练时间较长，学习性能不理想。为改进神经网络的性能，在隐含层中加入了反馈信号，同时综合可变学习速率算法、动量技术和批处理技术，生成变速度回归BP神经网络，并应用于入侵检测中，相对于原始的BP网络，大大提高了入侵检测的性能和速度。

2.1　变速度回归BP神经网络结构

如图2所示，变速度回归BP神经网络在传统的BP网络结构基础上，在隐含层加入了一个反馈信号，形成了如下的回归网络。图中各参数分别表示：WI为输入层到隐含层的权系数；WI_{bias}为偏差单元系数；WR为回归信号权数；$\sigma(\cdot)$为隐层结点的非线性激活函数,取为对数S函数；WO为隐含层到输出层的权系数；WO_{bias}为偏差单元的权系数；D为延迟一个单位时间的单元；NI为输入层神经元个数；NH为隐含层神经元个数；NO为输出层神经元个数；$I_{j(k)}$为该神经网络在k时间的第j个输入；$x_{j(k)}$为第j个隐含层结点的输入；$y_{(k)}$为递归神经网络的k时间的输出；⊕为线性累加。

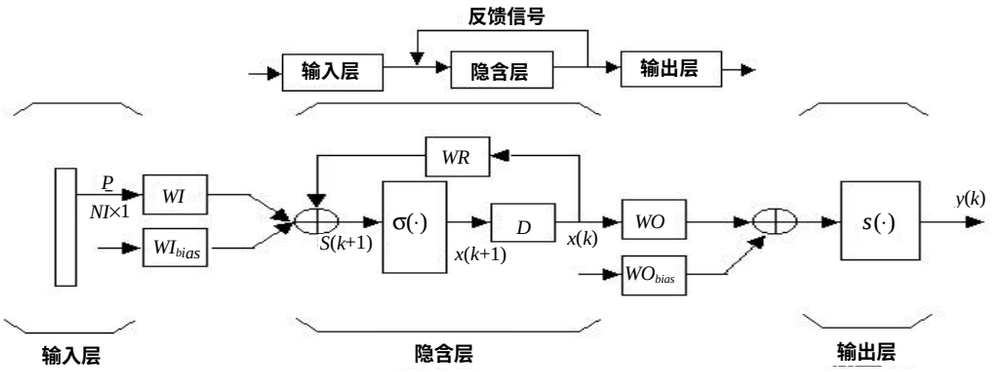

图2　变速度回归BP网络结构图

加入反馈信号后,隐含层输出为

$$x_j(k)=\sum_{i=1}^{NH}WR_{ij}x_{i(k-1)}+\sum_{i=1}^{MH}WI_{ij}I_i(k)+WI_{bias(j)}\quad j=1,2,\cdots,NH$$

反馈信号的权值学习公式为：$\Delta WR_{ij}(k)=b\times e_i(k)\times x_j(k)\quad (i,j=1,2,\cdots,NH)$；$b$为学习速度，$e$为输出层的误差。

2.2　该网络在传统BP网络算法基础上的改进算法

2.2.1　可变学习速度算法(Variable Learning Rate Backprogation,VLBP)

规则如下：

1) 如果均方误差(在整个训练集上)权值在更新后增加了,且超过了某个设置的百分数x(典型值为1%～5%)，则权值更新被取消，学习速度被乘以一个因子b(0<b<1),并且动量系数g(如果有的话)被设置为0。

2) 如果平方误差在权值更新后减少，则权值更新被接受，而且学习速度将被乘以一个因子h>1。如果g被设置为0，则恢复以前的值。

3) 如果平方误差的增长小于x，则权值更新被接受，但学习速度保持不变。如果g过去被设置为0，则恢复到以前的值。

2.2.2　动量技术

为了平滑网络训练的收敛曲线的震荡，即提高网络的收敛性能，每次学习的权值改变可以综合利用本次训练和上一次训练的权值改变。因此第k次训练的权值改变公式为

$$\Delta W'(k)=l\Delta W(k-1)+(1-l)\Delta W(k)$$

$$\Delta b'(k) = l\Delta b(k-1) + (1-l)\Delta b(k) \qquad 0 \le l \le 1$$

2.2.3 批处理技术

整个训练集都提交网络后才更新参数。平均所有样本计算出的权值改变，以得到更精确的梯度估计。每次批处理记为网络的一次训练。

2.3 检测算法测试

为测试改进后的网络在入侵检测应用中的效果，采用美国哥伦比亚大学计算机科学系入侵检测研究组提供的网络入侵测试数据集(http://www1.cs.columbia.edu/ids/HAUNT/dwripperutils/)。数据属性包括了网络数据包的包头信息、网络连接和传输信息和时间戳信息等。该数据集提供了三种数据Normal, Smurf5, Imapdexploit，其中Normal为正常数据，Smurf5,Imapdexploit是两种异常数据。从数据集中提取了909条混合数据集合(包括三种类型的数据)，分别用改进前后的网络进行训练。训练中每次批处理记为网络的一次训练。收敛指标为均方差，隐含层神经元个数取为10。

2.4 对混合数据集的神经网络训练

对三种类型的混合数据集进行训练学习，将每条数据转换为一个数值型的向量作为网络输入，Normal数据、Smurf5数据、Imapdexploit数据的目标输出向量分别为(1,0,0)、(0,1,0)、(0,0,1)，分别用n和C表示训练次数及收敛指标，图3为训练100次指标收敛情况比较，图4和图5是收敛指标均为0.05时变速度回归BP网络和一般BP网络的训练情况。由图4可见，变速度回归BP网络在训练的前期收敛指标下降速度较一般BP网络要快得多，当网络收敛指标趋于稳定时，变速度回归网络的收敛指标大大低于一般网络的收敛指标,即当收敛指标相等时,变速度回归网络相对于一般BP网络训练次数大大下降。

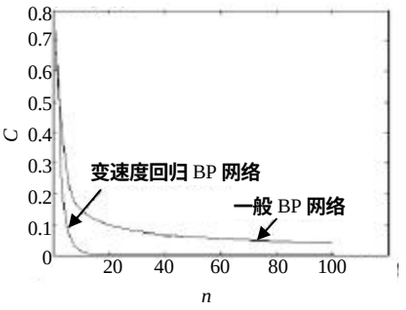

图3 两种网络训练对比

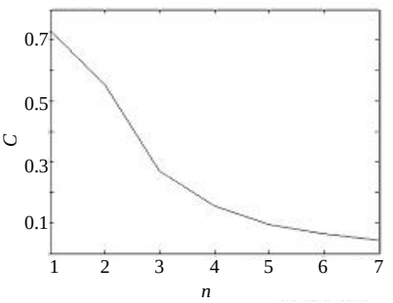

图4 变速度回归BP网络训练情况

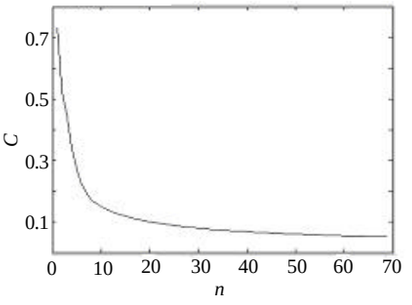

图5 一般BP网络训练情况

3 结 束 语

本文构建了基于智能体的分布式入侵检测系统的体系结构模型，针对传统BP神经网络在入侵检测应用中学习性能的不足，综合采用变学习速度算法、批处理技术和动量方法，提出了变速度回归神经网络入侵检测算法，通过对网络数据集的测试，相对于传统BP网络，检测效率和学习性能大大提高。

参 考 文 献

[1] 何炎祥, 陈莘萌. Agent与多Agent系统的设计与应用[M]. 武汉：武汉大学出版社, 2001

[2] 罗 敏, 张焕国, 王丽娜. 基于数据挖掘的网络入侵检测技术[J]. 计算机科学, 2003, 30(2): 105-107

[3] Yang Xiangrong, Song Qinbao, Shen Junyi. Implementation of sequence patterns mining in network intrusion detection system[M-CD]. IEEE 2001.0-7803-7010-4/01: 19-23

[4] Muhammad M S, Brian J G. Information security on Internet enterprise managed intrusion detection system(EMIDS) [M-CD]. IEEE 2001, 0-7 803-7 406-1/01: 234-238

[5] Cannady J. Applying CMAC-based on-line learning to intrusion detection[M-CD]. IEEE 2000, 0-7 695-0 619-4/00: 405-410

编 辑 刘文珍