基于小波神经网络的服务器预警系统

陈 波[1]，于 泠[2]

(1. 解放军理工大学通信工程学院 南京 210007; 2. 南京师范大学计算机系 南京 210097)

【摘要】提出了采用紧致型小波神经网络来构建服务器预警系统，将小波和神经网络直接融合，使网络训练过程从根本上避免了局部最优等非线性优化问题，小波神经元的低相关性，也使得小波神经网络有更快的收敛速度；将服务器中的日志数据数值化后进行网络训练，获得一个基于小波神经网络的入侵分类器。实验结果，表明小波神经网络系统自适应能力强、学习速度快、预警精度高、在入侵检测领域有良好的实用性。

关 键 词 小波神经网络; 服务器; 日志; 入侵检测

中图分类号 TP393.0235 文献标识码 A

A Wavelet Neural Network-Based Server Warning System

CHEN Bo[1]，YU Ling [2]

(1. Institute of Communication Engineering, PLA University of Science and Technology Nanjing 210007;

2. Dept. of Computer Science, Nanjing Normal University Nanjing 210097)

Abstract A server warning system based on wavelet neural network is presented. Wavelet neural network is a kind of neural networks, which combines wavelet theory with neural network theory, that is wavelet function forming neuron, it avoid the problem of nonlinear optimizations, such as local optimization. WNN has fast convergence because of the low correlation of wavelet neuron. In this system ,the WNN was trained by using numbered records of system log files in server and the classifier for intrusion detection can be obtained. The experimental result shows that the performance of this system is highly adaptive , the learning speed is fast, and the rate of warning accurate is high, so it is practicable in intrusion detection.

Key words wavelet neural network; server; log; intrusion detection

由于入侵模式的多样性，入侵检测策略和模型也具有多种不同的类型，较为流行的有基于统计方法、专家系统和神经网络方法的模型。统计方法的不足之处在于统计检测对事件发生的次序不敏感，依赖于审计数据或用户行为的分布要符合高斯分布等假设，但实际的用户行为具有随机性，这样的假设可能导致较高的误警率。专家系统虽然可以弥补统计技术的不足，但专家系统入侵检测难以科学地从各种入侵手段中抽象出全面的规则化知识，而且规则只能包含已知的攻击行为，却不包含未知的攻击行为。此外，专家系统所需处理的数据量过大，影响其效率。几相比较，神经网络方法是一种较为有效的入侵检测方法[1]。

小波神经网络(Wavelet Neural Network, WNN)是结合小波变换良好的时频局域特性与传统人工神经网络的自学习功能而形成的[2, 3]。小波神经网络通过小波分解进行平移和伸缩变化，所得到的级数具有小波分解的一般逼近函数的性质与分类特征，并且由于小波神经网络引入了两个新的参变量即伸缩因子和平移因

收稿日期：2003 – 12 – 25
基金项目：江苏省政府资助项目(BR2003015)；江苏省高校自然科学重点资助项目(03KJA52066)
作者简介：陈 波(1972 –)，男，博士生，讲师，主要从事网络信息安全、人工智能方面的研究.

子，从而使其具有更灵活有效的函数逼近能力，以及更强的模式识别能力和容错能力。由于其建模算法不同于普通神经网络的反向传播 (Back Propagation, BP)算法，故可有效地克服普通人工神经网络模型固有的缺陷。本文提出并实现了基于紧致型小波神经网络的服务器预警系统。

1 系统结构

入侵者通常会在系统日志中留下它们的踪迹，因此，充分利用系统的日志文件和审计信息是检测入侵的必要手段[4]。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，通过分析日志文件和审计信息，能够发现成功的入侵或入侵企图。本文提出的基于紧致型小波神经网络的服务器预警系统由数个模块组成，其结构如图1所示。

1) 数据采集模块。收集系统中的各种审计日志。服务器在其日志中记录了大量关于用户存取行为的信息，这些信息是设计入侵预警系统时的基础信息。

2) 日志监视模块。负责更新日志的传递，是使得系统能够实时响应攻击事件而设立的一个重要模块。

3) 数据预处理模块。将收集到的日志数据转换为系统能够识别的格式。

4) 网络学习模块。利用小波神经网络进行学习训练和校验，获得一个基于小波神经网络的入侵检测器。对于新的、随机发生的事件，可以作为入侵检测器的输入进行预测。当小波神经网络学会系统正常工作模式后，能够对偏离系统正常工作的事件作出反应，进而可以发现新的攻击模式。

5) 预警模块。如果检测到入侵行为的发生，预警模块通过发出声音、弹出对话框、发送E-mail及短信等多种形式，立即通知网络安全管理员采取适当的防范措施。

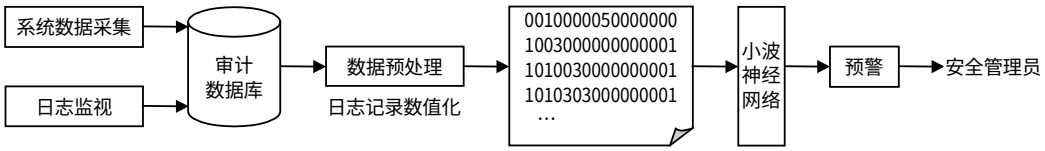

图1 基于小波神经网络的服务器预警系统结构图

2 主要技术思想和方法

2.1 小波神经网络(WNN)

小波分析和神经网络的结合有下述两种途径：1) 松散型结合，即小波分析作为神经网络的前置处理手段，为神经网络提供输入特征向量；2) 紧致型结合[5~7]，即小波分析和神经网络直接融合，以小波函数形成神经元。

采用了紧致型小波神经网络结构，即在一个径向基函数(Radial Basis Function, RBF)神经网络中，各隐层激活函数由一个小波函数系构成。

从输入层输入的矢量信号$\boldsymbol{x}$ 经过中间层网络激励函数$\psi((\boldsymbol{x}-b_i)/a_i)$映射，得到一组由小波基函数$\psi((\boldsymbol{x}-b_1)/a_1)$，$\psi((\boldsymbol{x}-b_2)/a_2)$，…，$\psi((\boldsymbol{x}-b_n)/a_n)$表达的神经元变换。该组变换再经过与变换系数$w_i$的相乘运算，最后由输出层求和输出 $f(\boldsymbol{x})=\sum_{i=1}^{n} w_i\psi(\frac{\boldsymbol{x}-b_i}{a_i})$。

与RBF和多层感知器(Multiplayer Perceptron，MLP)神经网络相比，WNN有以下优点：

1) WNN采用具有良好局部化特征的小波函数作为基函数，这类函数能保证输入只在局部区域有响应，因此可以避免收敛过慢的问题；

2) WNN是RBF网络的推广，其基函数是正交小波基，网络节点权重之间相关冗余度很小，对某一权重训练不会影响其他权重，因而具有更快的收剑速度；

3) 当输入信号样本空间非均匀分布时，小波神经元的良好局部特征和多分辨率学习实现了与信号的良好匹配，使得WNN有更强的自适应能力和更高的预警精度。

2.2　分类小波神经网络

上述的小波神经网络，在给定输入/输出对$[x_i,y_i]$ (i=1,2,…，n) 时，可用于逼近相应的输入/输出关系。在本文的小波神经网络系统中，为了能处理多维的输入，采用了如图2所示的分类小波神经网络结构。

小波特征分类器可用下式表示为：$\hat{f}_n = f(u_n) = f\left[\sum_{k=1}^{K} w_k \sum_{m=1}^{M} x_m \psi\left(\frac{x_m - b_k}{a_k}\right)\right]$，式中，$\hat{f}_n$ 表示第n次训练输出结果，M表示输入层单元数，K表示隐层单元数，以 w_k 表示隐层第k个单元与输出层之间的连接权值，而 $f(u) = \frac{1}{1+\mathrm{e}^{-u}}$ 为一sigmoid函数。$\psi(\boldsymbol{x})$ 采用Morlet母小波，有：$\psi(\boldsymbol{x}) = \cos(1.75\boldsymbol{x})\mathrm{e}^{-x^2/2}$。

图2中有两层权值，但只有一次综合，这是因为两层之间没有非线性。对于服务器攻击检测这个二分类问题，分类参数w_k、b_k、a_k 可用 $E = \frac{1}{2}\sum_{n=1}^{N}(d_n - \hat{f}_n)^2$ 优化，在 $E = \frac{1}{2}\sum_{n=1}^{N}(d_n - \hat{f}_n)^2$ 中，d_n 是希望分类的输出，且 $d_n = \begin{cases} 0 & \text{正常} \\ 1 & \text{异常} \end{cases}$。

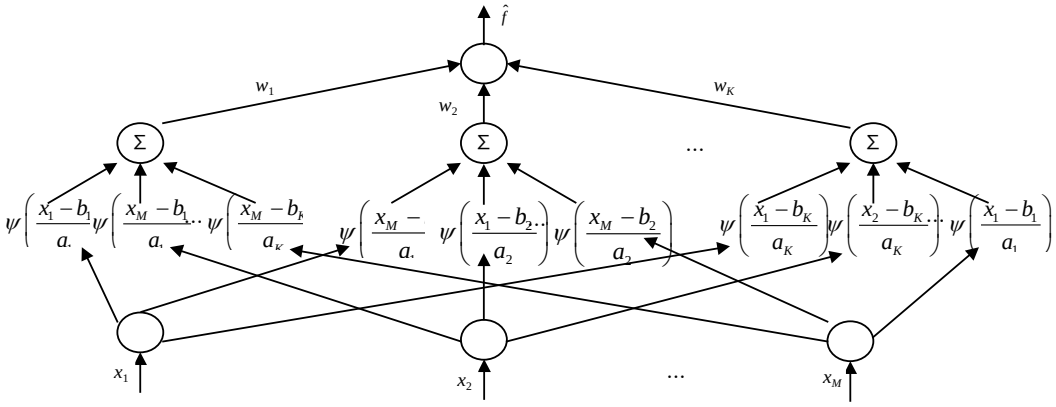

图2　分类小波神经网络结构图

2.3　网络训练算法

本系统中小波神经网络的训练算法步骤如下：

1) 初始化网络参数为伸缩因子a_k和平移因子b_k，以及网络连接权重w_k 赋以随机的初始值；

2) 输入学习样本矢量$\boldsymbol{X}$= (x_1，x_2，…，x_M)，及相应的期望输出 d；

3) 网络自学习，利用当前网络参数计算出网络的输出 $\hat{f}_n = f\left[\sum_{k=1}^{K} w_k \sum_{m=1}^{M} x_m \psi\left(\frac{x_m - b_k}{a_k}\right)\right]$；

4) 计算瞬时梯度，令 $x_i' = (x_i - b_k)/a_k \quad (i = 1,2,\cdots,M)$, $f'(u) = \partial f(u)/\partial(u) = f(u)[1 - f(u)]$，则瞬时梯度分别为：

$$g(w_k) = \frac{\partial E}{\partial w_k} = -\sum_{n=1}^{N}\sum_{m=1}^{M}(d_n - \hat{f}_n) f'(u_n) x_m \cos(1.75x_m') \exp(-x_m'^2/2)$$

$$g(b_k) = \frac{\partial E}{\partial b_k} = -\sum_{n=1}^{N}\sum_{m=1}^{M}(d_n - \hat{f}_n) f'(u_n) x_m w_k [1.75\sin 1.75x_m' \exp(-x_m'^2/2) + \cos 1.75x_m' \exp(-x_m'^2)x_m'] / a_k$$

$$g(a_k) = \frac{\partial E}{\partial a_k} = x_m' g(b_k)$$

5) 误差反向传播，在网络训练过程中，令 $\Delta w_k^{\text{new}} = -\eta\frac{\partial E}{\partial w_k^{\text{old}}} + \alpha\Delta w_k^{\text{old}}$，$\Delta a_k^{\text{new}} = -\eta\frac{\partial E}{\partial a_k^{\text{old}}} + \alpha\Delta a_k^{\text{old}}$，$\Delta b_k^{\text{new}} = -\eta\frac{\partial E}{\partial b_k^{\text{old}}} + \alpha\Delta b_k^{\text{old}}$，调整参数 a_k, b_k, w_k，有：

$$a_k^{\text{new}} = a_k^{\text{old}} + \Delta a_k^{\text{new}}，\quad b_k^{\text{new}} = b_k^{\text{old}} + \Delta b_k^{\text{new}}，\quad w_k^{\text{new}} = w_k^{\text{old}} + \Delta w_k^{\text{new}}$$

当误差函数值小于预先设定的某个值，则停止网络学习，否则返回输入学习样本矢量步骤。

以上步骤不断进行，使网络表现出较强的灵活性和较高的逼近能力。

3 实验及结果

3.1 服务器日志格式及其数值化编码

本系统的实验环境为Unix系统。为了从庞大的审计信息中提取出与安全相关的信息，首先需对历史审计文件进行预处理，产生用户会话矢量。用户会话包括login和logout之间的所有事件。会话矢量$\boldsymbol{A}=\langle a_1, a_2, \cdots, a_n\rangle$描述单一会话过程中用户进行的各种事件数量。会话开始于login，终止于logout。本文在实验中监视15种事件，如：登录的时间(User_Login)、登录失败(User_Login_fail)、写文件失败(File_Write_fail)、打开文件失败(File_Open_fail)等一些敏感事件。

为了小波神经网络能对日志文本进行学习，必须对日志进行数值化，然后再将其作为神经网络的输入结点值。训练集TrainSet={[x_i, y_i]}(i=1, 2, …, n)中，输入量x_i占15位，分别对应于15个事件，即x_i=(User_Login,boot_login,Guest_login,User_Login_fail,SU_ok,SU_fail,who_finger_ ps, cat_vi,ls_ok, ls_fail, rm_mv, File_Open_fail, File_Read_password, File_Write, File_Mode,)；输出量y_i占1位，“ 1 ”表示异常，“ 0 ”表示正常。

3.2 实验及结果分析

把在实验环境中获得的正常和入侵情况下的1 600条日志记录分成三部分，一部分用于训练小波神经网络(学习样本533个)；另一部分用于验证网络的可用性(验证样本533个)；最后一部分用于网络模型真正入侵检测(预测样本534个)，预测出错实例数为26。实验过程中：

1) 训练指标能在很短的时间内达到。当训练时间(T)达到186个时间单位时，网络误差Error (E)就小于0.1了。训练过程误差变化情况如图3所示。

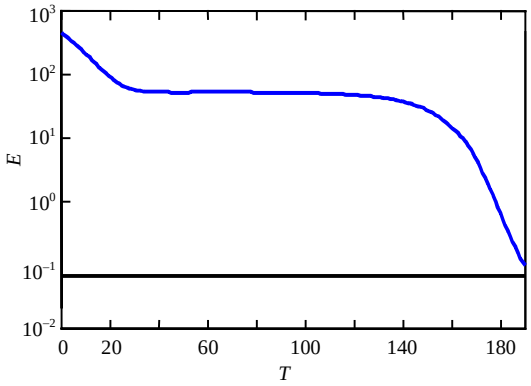

图3 训练过程误差变化曲线

2) 预警正确率很高。预警正确率= (1–预测出错实例数/预测样本总数)×100%=(1–26/534)×100%= 95.13%。

3) 采用大量实例对小波神经网络进行训练，使其获得预测能力，这一过程可以是完全抽象的计算，无需强调对数据分布的假设，无需向神经网络解释知识的细节，神经网络可以根据已有的实例自动掌握系统的各个度量之间的内在关系。

4) 当小波神经网络学会了系统正常的工作模式后，能够对偏离系统正常工作的事件作出反应，进而可以发现一些新的攻击模式。

实验结果表明，基于小波神经网络的服务器预警系统的自适应能力强、学习速度快、预警度高，在入侵检测领域有良好的实用性。今后将进一步运用小波神经网络于入侵检测，以提高入侵检测系统的检测精度、实时响应性能、检测未知入侵行为能力等。

参 考 文 献

[1] 刘美兰, 姚京松. 神经网络在入侵检测系统中的应用[J]. 计算机工程与应用, 1999, 35(6): 37-42

[2] Zhang Q, Benvenise A.Wavelet network[J]. Proc IEEE Trans on Neural Network, 1992, 3(6): 889-898

[3] Bakshi B R, Stephanopoulos G. Wave-net: A multiresolution, hierarchical neural network with localized learning[J]. AIChE Journal, 1993, 39(1): 57-80

[4] 王丽娜. 网络多媒体信息安全保密技术[M]. 武昌: 武汉大学出版社, 2003

[5] Delyon B, Juditsky A, Benveniste A. Accuracy analysis for wavelet approximations[J]. IEEE Trans. on Neural Network., 1995, 6(2): 332-348

[6] 焦李成. 神经网络的应用与实现[M]. 西安: 西安电子科技大学出版社, 1996

[7] 阎平凡, 张长水. 人工神经网络与模拟进化计算[M]. 北京: 清华大学出版社, 2000

编 辑 熊思亮