基于改进小波神经网络的信息安全风险评估

赵冬梅[1] 刘金星[2] 马建峰[3]
(河北师范大学信息技术学院 石家庄 050016)[1] (空军第一航空学院 信阳 464000)[2]
(西安电子科技大学计算机学院 西安 710071)[3]

摘 要 由于信息安全风险评估具有非线性、不确定性等特点,采用传统的数学模型进行信息安全的风险评估存在一定的局限性。将人工神经网络(ANN)理论、小波分析及粒子群优化算法有机结合,提出了粒子群-小波神经网络(PWNN)的信息安全风险评估方法。首先,采用模糊评价法对信息安全的风险因素的指标进行量化,对神经网络的输入进行模糊预处理;其次,采用粒子群优化算法对小波神经网络进行训练。仿真结果表明,提出的改进的小波神经网络模型可实现对信息系统的风险因素级别的量化评估,克服现有的评估方法所存在的主观随意性大、结论模糊等缺陷,具有更强的学习能力、更快的收敛速度。

关键词 信息安全,风险评估,小波神经网络(WNN),粒子群,优化
中图法分类号 TP309 **文献标识码** A

Risk Assessment of Information Security Based on Improved Wavelet Neural Network

ZHAO Dong-mei[1] LIU Jin-xing[2] MA Jian-feng[3]
(School of Information Technology, Hebei Normal University, Shijiazhuang 050016, China)[1]
(The First Aeronautics College of PLAAF, Xinyang 464000, China)[2] (School of Computer Science, Xidian University, Xi'an 710071, China)[3]

Abstract Based on the uncertainty and complexity of risk assessment of information security and limitations of the application of the traditional mathematical models in risk assessment of information security, we proposed an evaluating method of risk assessment of information security based on particle swarm-wavelet neural network(PWNN) by means of integrating the artificial neural networks, wavelet analysis and particle swarm optimization algorithm. Firstly, the risk factors were quantized by fuzzy evaluation method, and the input of ANN was fuzzily pre-treated. Secondly, the wavelet neural network was trained by particle swarm optimization algorithm. The simulation results show that risk level of the information system can be evaluated quantitatively by the PWNN model proposed in this paper, and the shortcomings of current assessment methods can be overcome, such as more subjectivity, randomness and fuzzy conclusion, and PWNN has better learning ability and more faster convergence rate than that of the current methods.

Keywords Information security, Risk assessment, Wavelet neural network(WNN), Particle swam, Optimization

目前国内外关于信息安全风险评估的研究成果主要包括基于概率统计的 ALE-based[1]、OCTAVE 方法[2]、SP800-30[3]、SP800-42[4]、PRA[5]等。这些标准和方法或为单纯定性分析方法,或虽给出了定量计算方法,但实施过于繁琐。

由于信息安全风险评估的复杂性、非线性、不确定性及实时性强等特点,采用传统的数学模型进行信息安全的风险评估存在一定的局限性,评估方法带有较大的主观随意性和模糊性,在操作上比较复杂,缺乏自学习能力。而人工神经网络具有常规方法所不具备的智能特性,可以处理不确定性问题,具有自学习和获取知识的功能,适宜处理非线性问题。

小波神经网络的训练普遍采用梯度下降法,它依赖于初始权值的选择,收敛速度缓慢且容易陷入局部最优。

粒子群算法采用基于种群的全局搜索策略,通过惯性权重协调全局搜索与局部搜索,能以较大的概率保证最优解,克服了梯度下降法局部最优的缺陷。通过将小波神经网络与粒子群优化算法有机结合以构建改进的小波神经网络,提出了基于粒子群优化算法的小波神经网络模型(PWNN),用于信息安全风险评估,以实现对信息安全风险影响因素的风险等级的有效评估。

1 信息安全风险评估

信息安全风险评估,就是从风险管理角度,运用科学的方法和手段,系统地分析网络与信息系统所面临的威胁及其存在的脆弱性,评估安全事件一旦发生可能造成的危害程度,提出有针对性的抵御威胁的防护对策和整改措施,以防范和化解信息安全风险,或者将风险控制在可接受的水平,从而最大限度地保障网络和信息安全。

在信息安全风险评估过程中,风险计算是确定风险级别

到稿日期:2009-03-17 返修日期:2009-06-01 本文受国家自然科学基金项目(60573036),河北省自然科学基金项目(F2009000136)资助。
赵冬梅(1966-),女,博士,教授,主要研究方向为信息安全等,E-mail:zhaodongmei666@126.com;刘金星(1964-),男,博士,教授,主要研究方向为人工智能等;马建峰(1963-),男,教授,博士生导师,主要研究方向为信息安全等。

的一个重要阶段。其主要程是：

(1)对信息资产进行识别，并对资产赋值；

(2)对威胁进行分析，并对威胁发生的可能性赋值；

(3)识别信息资产的脆弱性，并对弱点的严重程度赋值；

(4)根据威胁和脆弱性计算安全事件发生的可能性；

(5)结合信息资产的重要性和在此资产上发生安全事件的可能性计算信息资产的风险值[6]。

风险计算以下面的范式形式化加以说明：

风险值$=R(A,T,V)=R(L(T,V),F(Ia,Va))$

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；Ia 表示安全事件所作用的资产价值；Va 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。

风险值的确定涉及到风险评估的结果及风险控制措施的制定，是风险评估过程的重点和难点。R 是一个复杂函数，不是一个线性关系。

2 基于粒子群-小波神经网络的信息安全风险评估

在信息安全风险评估中，风险因素主要是从产生风险因素的威胁、脆弱性及其相互关系来评价，首先分析系统的资产、存在的威胁及脆弱性，然后从威胁出现的频率、脆弱性的严重程度、资产的价值等各个评价指标来评价风险因素的级别。这些评价指标存在着很大的模糊性和不确定性，常规方法难以衡量。而且这些量与风险因素的风险级别之间存在非线性关系和动态变化规律，常规方法难以处理。为解决这一问题，本文利用模糊系统具有被人容易理解的表达能力和神经网络具有极强的自适应能力的特点，将二者有机结合，实现对不确定和模糊的风险因素的风险等级的评估。在小波神经网络的训练上采用粒子群优化算法，以解决收敛速度慢和局部最优缺陷。

2.1 整体结构

本文所构造的基于小波神经网络的信息安全的风险评估模型由两部分组成：第一部分是模糊系统；第二部分是小波神经网络。应用模糊评价法量化风险评估指标。应用小波神经网络对指标进行风险级别的评估。将神经网络的输入表示为模糊隶属度。采用的模型是单隐含层的小波神经网络模型。网络的输入特征量是风险因素的各个评价指标，包括资产的保密性、完整性和可用性价值、脆弱点转换为报酬的难易程度、脆弱点的严重程度、脆弱点的易用程度以及威胁的技术含量等。将这些指标经过量化处理和一致性处理后，作为神经网络的输入量输入，经过小波神经网络的学习算法，网络的输出特征量为风险因素的风险级别。小波神经网络的变换函数采用 Morlet 小波基函数，网络训练采用粒子群优化算法。

2.2 输入量的模糊预处理

由于人工神经网络适合定量数据，对于定性指标的分析缺乏相应的处理能力，而风险因素的指标值又有很大的不易确定性，因此本文采用模糊评价法对信息安全风险因素的指标进行量化，即将模糊系统的输出作为神经网络的输入。具体实现方法是：

(1)通过对资产、威胁、脆弱性以及威胁和脆弱性的关联分析，找出信息安全的风险因素。

(2)根据模糊评价法，构造风险因素集 $U=\{u_1,u_2,\cdots,u_n\}$。

(3)构造评判集。对各风险因素的评价从资产的保密性、完整性和可用性价值、脆弱点转换为报酬的难易程度、脆弱点的严重程度、脆弱点的易用程度以及威胁的技术含量等方面进行[7]。专家对各风险因素逐个给出风险程度评语，将各个指标的评语分为 m 个等级，评判集为 $V=\{v_1,v_2,\cdots,v_m\}$。

(4)专家给出各因素的评语，构造模糊映射 $f:U\to F(V)$，$F(V)$ 是 V 上的模糊集全体，$u_i\to f(u_i)=(r_{i1},r_{i2},\cdots,r_{im})\in F(V)$，映射 f 表示风险因素 u_i 对评判集中各评语的支持程度。令风险因素 u_i 对评判集 V 的隶属向量 $R_i=\{r_{i1},r_{i2},\cdots,r_{im}\}$，$i=1,2,\cdots,n$，得到隶属度矩阵 R。

(5)因为评判集中各个指标程度的高低直接影响风险大小，所以对评判集中每个评价指标赋予不同的权重[8]。设权重分配集为 $A=(a_1,a_2,\cdots,a_n)$。由模糊变换的运算，有：

$$B=A\cdot R^T=(a_1,a_2,\cdots,a_m)\begin{bmatrix} r_{11} & r_{21} & \cdots & r_{n1} \\ r_{12} & r_{22} & \cdots & r_{n2} \\ \vdots & \vdots & & \vdots \\ r_{1m} & r_{2m} & \cdots & r_{nn} \end{bmatrix}=(b_1,b_2,\cdots,b_n) \quad (1)$$

B 为各风险因素在某一评价下的权重，反映了风险因素的评价值，而且其值是在(0,1)之间，可作为 BP 神经网络的输入量。

2.3 粒子群-小波神经网络学习算法

2.3.1 小波神经网络结构

小波神经网络是把小波分析理论与神经网络理论相结合，主要研究方向为小波与 BP 神经网络相融合[9,10]。本文采用的小波神经网络是用非线性小波基取代了 BP 网络中传统的非线性 Sigmoid 函数，小波基采用 Morlet 母小波。非线性函数的拟合通过用所取的非线性小波基进行线性叠加来实现，即用小波级数的有限项拟合。本文确定的小波神经网络基本结构如图 1 所示。

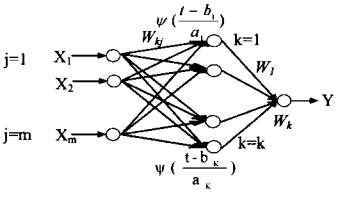

图 1 小波神经网络结构图

非线性函数 $y(t)$ 可用小波 $\psi_{a,b}(t)$ 进行如下拟合：

$$\hat{y}(t)=\sum_{k=1}^{K}w_k\psi\left(\frac{t-b_k}{a_k}\right) \quad (2)$$

其中，$\hat{y}(t)$ 为非线性函数 $y(t)$ 的拟合值序列。w_k 表示输出层与中间层第 k 个单元之间的连接权；K 为小波基个数。b_k 和 a_k 分别为小波基的平移因子和伸缩因子。

隐含层激励函数采用 Morlet 母小波：

$$\psi(t)=\cos(1.75t)\exp\left(-\frac{t^2}{2}\right) \quad (3)$$

2.3.2 粒子群优化算法

粒子群优化算法(PSO)由 Kennedy 和 Eberhart 在 1995 年提出，源于对鸟群觅食的研究，其基本思想是通过群体中个体之间的协作和信息共享来寻求最优解[11]。

在PSO系统中，每个粒子在空间中运动，并由一个矢量决定其运动方向和位移。粒子追随当前的最优粒子运动，并经多次搜索得到最优解。

PSO算法数学表示如下[12]：

设搜索空间为 D 维，总粒子数为 n。第 i 个粒子位置表示为向量 $X_i=(x_{i1},x_{i2},\cdots,x_{iD})$；粒子每次迭代中追随最优粒子在空间搜索，直至找到最优解。在每次迭代中，粒子通过跟踪两个最优解进行更新：一个是第 i 个粒子本身的过去最优位置 $P_i=(p_{i1},p_{i2},\cdots,p_{iD})$，二是整个种群目前找到的最优解 P_g；第 i 个粒子的位置变化率(速度)为向量 $V_i=(v_{i1},v_{i2},\cdots,v_{iD})$。每个粒子的位置按下式进行变化：

$$v_{id}(t+1)=W*v_{id}(t)+c_1*rand()*(p_{id}(t)-x_{id}(t))+c_2*rand()*(p_{gd}(t)-x_{id}(t)) \quad (4)$$

$$x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) \quad (5)$$

其中，c_1，c_2 为正常数，称为加速因子，也叫学习因子；$rand()$ 为[0,1]之间的随机数；W 称为惯性因子，是粒子上一次的速度对本次飞行速度的影响因子，W 较大有利于跳出局部极小点，W 较小有利于算法收敛。式(4)中右边共有3项：粒子上一次的速度与惯性因子的乘积、粒子自身行为的差异比较、粒子群体行为的差异比较。

2.3.3 小波神经网络的训练算法

小波神经网络(WNN)的训练一般采用梯度下降法，这是一种局部搜索算法，网络极易陷入局部最小值。根据粒子群优化算法的原理，采用粒子群算法替代梯度下降法，对小波神经网络进行参数训练。结果表明，迭代步数、收敛精度均有很大提高。

应用粒子群算法优化小波神经网络(PWNN)算法的步骤为：

(1)按照图1所示，小波的伸缩因子为 a_k，平移因子为 b_k，网络连接权重为 w_{ki} 和 w_k。

粒子群规模设为 n 个。每个粒子的位置向量为：

$$present(i)=[w_1,w_2,\cdots,w_k,a_1,a_2,\cdots,a_k,b_1,b_2,\cdots,b_k]$$

$$i=1,2,\cdots,n$$

其中，k 为隐含层神经元个数。

初始化 n 个粒子的位置向量、速度向量 v，其中每个粒子向量的元素随机产生。

输入学习样本为 $x_l(i)$，相应的期望输出为 y_l。其中，$l=1,2,\cdots,L$，L 为输入样本数量。

(2)隐含层激励函数采用Morlet母小波，如式(3)所示。利用粒子群算法式(4)，式(5)对每个粒子的位置向量present和速度 v 进行迭代更新，并且记录每个粒子的历史最优位置 p_i^d(第 i 个粒子第 d 次迭代的历史最优位置向量)和所有粒子中的全局最优位置向量 g^d。

粒子的适应度定义为第 d 次迭代后网络实际输出 $\hat{y}$ 与期望输出 y 间的最小均方差：

$$E=\frac{1}{2}\sum_{l=1}^{L}[y_l-\hat{y}_l^d]^2 \quad (6)$$

其中，$d=1,\cdots,D$，D 为最大迭代次数。

记录对应于 p_i^d 和 g^d 的系统的适应度 E_i^d 和 E^d。

(3)当 E^d 小于预先设定的某个误差值，则停止网络的学习，否则返回步骤(2)。

(4)利用最终得到的全局最优值 g 计算网络输出，得到最终的拟合曲线。

3 实验仿真

以某信息系统为例进行了风险评估实验。首先分析信息安全风险因素。针对相关风险因素，将其资产的保密性、完整性和可用性价值、脆弱点转换为报酬的难易程度、脆弱点的严重程度、脆弱点的易用程度以及威胁的技术含量等作为输入特征量，共计7个输入特征量。输出特征量为风险事件的风险级别，1个输出量。组织专家对风险事件进行评估，给出各风险事件的评估值作为样本集。以30组输入和输出特征量作为神经网络的学习样本，样本取自某保险公司信息系统的评价结果，输入为风险事件的特征量，输出为专家评定结果。其中20组作为训练样本，10组检验训练网络。对网络进行训练，使其在输入和输出之间建立一个非线性映射关系。小波网络的变换函数采用Morlet小波基函数；小波网络隐含层为8个神经元。应用粒子群训练小波神经网络，算法用MATLAB程序语言编程来实现。粒子群规模设为50个，加速因子 $c_1=c_2=1.8$。惯性因子 W 的取值既要考虑到避免陷入局部极小，又要保证收敛性。初始阶段惯性因子 W 选较大的值(0.8)，有利于跳出局部极小值。然后逐步递减，以保证算法的收敛性，利用一个线性公式使其逐步递减至0.4。

取20组样本作为小波神经网络的训练样本，对网络进行训练，训练集的输出误差以及循环次数如图2所示。图中横坐标为循环迭代次数，纵坐标为误差变化。网络权值经过95次迭代调整后，误差精度低于预先设置。

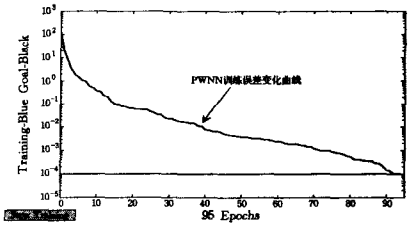

图2 PWNN训练集的输出误差以及循环次数

为了检验训练网络的泛化能力，对剩余10组数据进行仿真，即用已建立的非线性映射关系求10组输入的输出。PWNN仿真结果与专家评估结果的对比如图3所示。“o”表示网络仿真结果，“+”表示专家评估结果。

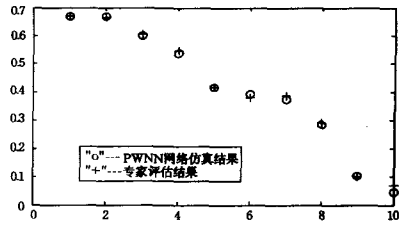

图3 PWNN仿真结果与专家评估结果的对比

PWNN训练过程中的误差变化情况与梯度下降法训练小波神经网络(WNN)误差变化情况的对比如图4所示。图中横坐标为循环迭代次数，纵坐标为误差变化。通过实验对比，利用粒子群优化算法训练小波神经网络具有更快的收敛

速度，精度更高。

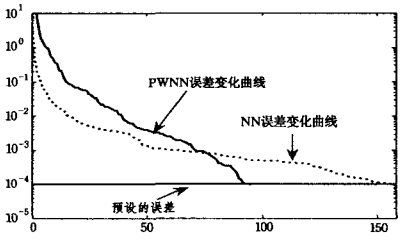

图 4　PWNN 训练与 WNN 训练对比

结束语　本文提出了一种基于改进的小波神经网络的信息安全风险评估方法，针对信息系统安全风险评估实践，构造出符合信息系统安全风险评估的模糊系统。针对信息系统安全风险评估的不确定性和当前评估手段的主观性，提出一种小波神经网络训练方法。针对小波神经网络中梯度下降法存在收敛速度慢和可能造成局部最优等问题，应用粒子群优化算法对小波神经网络进行训练。仿真结果表明，算法性能优良，为信息安全风险评估提供了可行的算法支持。

参 考 文 献

[1] David R, George G. Risk: A Practical Guide for Deciding What's Really Safe and What's Dangerous in the World Around You [D]. New York: Houghton Mifflin Company, 2002

[2] Maiwald E. Network Security: A Beginner's Guide [D]. The McGraw-Hill Companies, Inc, 2001

[3] Whitman M E, Herbert J. Principles of Information Security [M]. Canada: GEX Publishing Services, 2003

[4] ISO/IEC 17799. Information Technology-Code of practic for information security management[S]. 2000

[5] MnSCU. Security Risk Assessment - Applied Risk Management [R]. Minnesota State Colleges & Universities, 2002, 7

[6] GB/T 20984-2007《信息安全技术 信息系统的风险评估规范》[S]. 中华人民共和国国家标准, 2007

[7] 赵冬梅，马建峰，王跃生. 信息系统的模糊风险评估模型[J]. 通信学报, 2007, 28 (4): 51-56

[8] Zhao Dongmei, Wang Changguang, Ma Jianfeng. A risk assessment method of the wireless network security[J]. Journal of Electronics, 2007, 24(3): 428-432

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

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

[11] Kennedy J, Eberhart R C. Particle swam optimization [C] // Proc. IEEE Int'l Conf. on Neural Networks. Perth, Australia, 1995: 1942-1948

[12] Eberhart R C, Shi Y. Particle swarm optinization: developments, applications and resources[C]// Proc. Congress on Evolutionary Computation 2001. Piscataway, NJ: IEEEE Press, 2001: 81-86

(上接第 74 页)

实现多节点集群 P2P 系统，然后将两者进行对比实验。在实现的过程中，规定集群中的节点数最大为 20。同时为了简化实现，集群中的节点仅仅通过链表连接在一起，没有进行集群内的 Gnutella 实现。

在进行模拟测试时主要基于查询跳数和查询延迟进行查询开销的评估。查询跳数是进行一次基于关键字的查询时经过的节点的个数。而每经过一个节点时，都会产生一定的系统延迟，一次查询操作中每一跳查询延迟的总和就是总的查询延迟。

模拟测试时，从节点数量 256 开始依次增加，对比两个系统的查询跳数和查询延迟，结果如图 5 和图 6 所示。

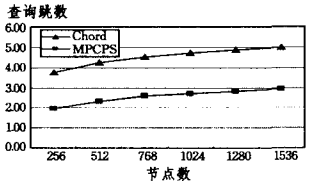

图 5　查询跳数模拟结果

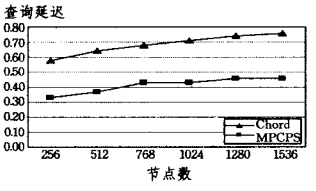

图 6　查询延迟模拟结果

模拟结果显示多节点集群 P2P 系统(MPCPS)的性能相比 Chord 系统有较大的提高。这主要是因为在节点相同的条件下，由于节点聚集，使得多节点集群 P2P 系统 Chord 环上的有效节点数大量减少。例如，当有 256 个节点时，Chord 系统的环上有 256 个节点，而多节点集群 P2P 系统的环上的有效节点数(集群数)为 13 左右。

5　多节点集群 P2P 系统应用

多节点集群 P2P 系统通过对经典的结构化 P2P 算法的改造，解决了结构化 P2P 算法中普遍存在的问题。主要体现在几个方面：(1)解决了节点失效造成资源丢失的问题；(2)提高了资源下载速度；(3)实现了模糊查询的功能，并且系统的性能还略有提高。因此多节点集群 P2P 系统是一个好的结构化 P2P 系统。

使用多节点集群的方法将资源同时存储在多个节点中，提高了系统资源的安全性和下载速度。再加上模糊查询功能的实现，使得多节点集群 P2P 系统非常适合作为 P2P 文件存储系统的底层实现。

参 考 文 献

[1] Karger D, Lehman E, Leighton F, et al. Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web[C]// Proceedings of the 29th Annual ACM Symposium on Theory of Computing. 1997: 654-663

[2] Zhao Y, Kubiatowicz J, Joseph A. Tapestry: An infrastructure for fault-tolerant wide-area location and routing[R]. UCB/CSD-01-1141. Berkeley: University of California, 2000

[3] Stoica I, Morris R, Liben-Nowell D, et al. Chord: A Scalable Peer-to-peer Lookup Protocol for Internet Applications [J]. IEEE/ACM Transactions on Networking, 2003, 11(1): 17-32

[4] Ratnasamy S, Francis P, Handley M, et al. A scalable content addressable network[C]// Proc. ACM SIGCOMM. 2001

[5] Ripeanu M, Foster I, Iamnitchi A. Mapping the gnutella network: properties of large-scale peer-to-peer systems and implications for system design[J]. IEEE Internet Computing Journal Special Issue on Peer-to-Peer Networking, 2002, 6(1): 1-2

[6] Cohen B. Incentives Build Robustness in Bit Torrent[C]// Proceedings of the 1st Workshop on the Economics of Peer-to-Peer Systems. Berkeley, CA, USA, 2003