文章编号: 1006 - 9348(2011) 11 - 0126 - 04

神经网络在计算机网络安全评价中的应用研究

武仁杰
(河北北方学院,河北 张家口 075000)

摘要: 研究计算机网络安全评价问题,计算机网络安全评价是一个多指标系统,计算机网络受到漏洞、病毒等入侵是一个复杂的非线性问题,传统线性评价方法不能准确描述各指标对评价结果影响且评价结果的精度低。为了提高计算机网络安全的评价精度,提出了一种粒子优化神经网络的计算机网络安全评价方法。首先通过专家系统挑选计算机网络安全评价指标,然后采用专家打分方法确定评价指标权重,最后将指标权重输入 BP 神经网络进行学习,BP 神经网络参数通过粒子群算法进行优化,获得计算机网络安全评价等级。仿真结果表明,相对于传统计算机网络安全评价模型,粒子优化神经网络加快计算机网络安全评价速度,提高了计算机网络安全的评价精度。

关键词: 粒子群算法; 计算机网络安全; 神经网络; 评价
中图分类号: TP393 文献标识码: B

Application Research of Computer Network Security Evaluation Based on Network Security

WU Ren - jie
(Hebei North University, Zhangjiakou Hebei 075000, China)

ABSTRACT: Research computer network security problem. There are nonlinear relations among the evaluation indexes, and it is difficult for an accurate mathematical model to describe the nonlinear relationship. In order to improve the evaluation accuracy of computer network security, we puts forward a combination model to evaluate the computer network security. The combination model used particle swarm optimization (PSO) to optimize the parameters of BP neural network, speed up the BP neural network's convergence speed, and enhance its global optimization ability, which effectively improved the accuracy of the evaluation model. Simulation results showed that compared with traditional BP neural network model, the combined model's learning ability is faster and global search ability is stronger, which effectively improves the evaluation accuracy of computer network security.

KEYWORDS: PSO; Computer network security; Neural network; Evaluation

1 引言

网络技术发展给人们的生活带来了便利,同时也为病毒、木马等一些破坏性程序的攻击网络利供方便,计算机网络安全受到越来越大的危险[1]。准确、科学地对网络所面临风险进行评价,并对风险进行有效防范,降低计算机网络安全问题所造成的损失[2]。

计算机网络安全受到多种因素的影响如: 入侵、漏洞、病毒等,而且各种多种因素互相关联,因素与评价结果之间为复杂的非线性关系,传统的评价方法如层次分析法、故障树分析法、灰色模型等进行计算机网络安全评价时不仅操作十分复杂,难以用准确描述出该非线性关系,使得评价精度相当低[3]。专家系统是主要与专家知识丰富度相关联,评价结果具有主观性,不客观,缺陷科学性,因此也不适合复杂的计算机网络安全评价。近年来,神经网络技术广泛迅速的发展,具有自学习能力、自组织和强大的自适应能力的人工智能算法,实现简单,具有较强的鲁棒性强。人工神经网络模型能够有效地克服传统统计模型的缺陷,通过对神经元之间的连接权值进行调整,对计算机网络安全与各属性之间的非线性规律进行捕捉,从而实现对计算机网络安全进行准确评价,十分适宜于对计算机网络安全进行评价[4]。BP 神经网络(BPNN) 是目前最为成熟、应用最广泛的一种神经网络,但由于 BP 神经网络是基于梯度下降算法,存在着训练速度慢、易陷入局极小、全局搜索能力较差等缺陷[5],影响应用范围,因此如何提高神经网络在计算机网络安全评价中的精度已成为计算机网络安全研究领域中的重点。

粒子群优化算法(PSO) 是一种新发展起来模拟鸟群飞

收稿日期: 2011 - 04 - 10 修回日期: 2011 - 05 - 12

行的仿生智能搜索算法，具有个体数目少、计算简单、全局优化性能好等优点，能够对神经网络参数进行优化[6]。针对计算机网络安全评价的特点，结合 BP 神经网络很好的非线性评价能力，本文提出一种 PSO 优化的 BP 神经网络的计算机网络安全评估模型。仿真结果表明，本文模型具有更快的收敛速度、更高的评价精度。

2 计算机网络安全评价的原理

计算机网络安全评价原理是在其评价标准的指导下，首先，确定评价的内容和范围，对网络的其本情况、安全状况、网络脆弱点进行分析，然后采取相关的评价方法进行评价，最后得出网络的安全级别，计算机网络安全评价数学模型为:

$$网络安全级别 = f(x_1, x_2, \cdots, x_i, \cdots, x_m) \quad (1)$$

其中，x_i 表示计算机网络安全评价因子，f 表示计算机网络安全评价模型。

从计算机网络安全评价模型可知，选择计算机网络安全评价因子和网络评价模型是至关重要的。计算机网络安全具有不确定性、非线性等特点，因此本文采用非线性逼近能力十分强的 *BP* 神经网络作为网络评价模型，采用专家选择计算机网络安全影响因素，并对其进行打分，确定其对评价结果的权重，来提高计算机网络安全评价精度。

3 PSO – BPNN 模型

3.1 计算机网络安全评价指标体选择

计算机网络是一个复杂的系统，其安全影响因素较多，要对其安全等级进行准确地评价，首先必须建立一个科学、完善的计算机网络安全评价指标体系。本文从计算机网络系统的管理安全、物理安全和逻辑安全的基础上，通过专家选择出计算机网络安全评价指标，具体见图 1，并通过专家系统对计算机网络安全评价指标进行打分，确定其权重。

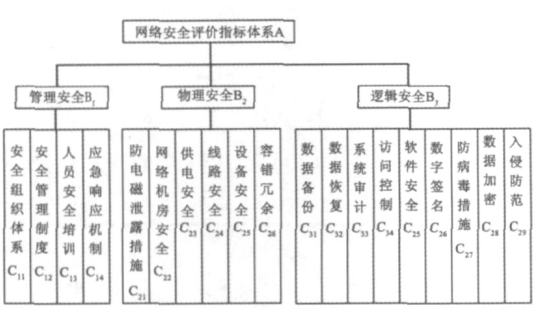

图 1 计算机网络安全评价指标体系

3.2 计算机网络安全指标的归一化处理

图 1 中构建的指标从不同的角度反映出计算机网络安全状况，由于各指标间的量纲不同，无法进行直接比较，为了使各指标间具有可比性和加快神经网络的收敛速度，本文对各指标进行了归一化处理:

1) 对于定性指标: 采用专家打分法确定其数据，同时对各指标进行了归一化处理。

2) 对于定量指标: 利用下列公式进行归一化处理。

正向型指标:

$$x_i' = (x_i - x_{i\min}) / (x_{i\max} - x_{i\min}) \quad (2)$$

式中: x_i' 表示指标为 x_i 的归一化标准值; $x_{i\min}$、$x_{i\max}$ 分别表示第 i 个指标的最小值和最大值。

3.3 计算机网络安全等级设定

根据指标的综合权重，可以对该计算机网络进行安全评价，根据相关研究，计算机网络安全等级分为安全(A)、基本安全(B)、不安全(C)、极不安全(D)共 4 个等级，将安全级别总分设为 1 分，则相应的安全级别及对应分值见表 1 所示。

表 1 计算机网络安全等级

级别	A	B	C	D
分值	1 ~ 0.85	0.85 ~ 0.7	0.7 ~ 0.6	0.6 ~ 0

3.4 BP 神经网络算法

BP 神经网络是按照误差逆向传播的一种多层前馈网络，是目前应用最广泛的神经网络模型之一[7]。其采用梯度下降算法，通过误差的反向传播对网络的权值和阈值不断进行调整，从而使神经网络的期望输出与实际输出之间的误差平方和最小。BP 神经网络的结构图见图 2。

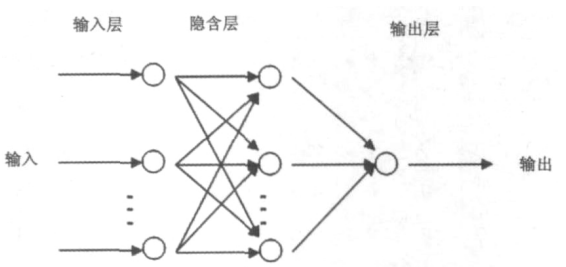

图 2 BP 神经网络结构图

BP 神经网络虽然具有较强的非线性逼近能力、算法简单、实现容易等优点，但是易陷入局部极值，从而难以保证收敛到全局极小点，全局搜索能力不强。此外，BP 神经网络是基于反向传播的梯度下降算法，其收敛速度慢，学习效果难以令人满意。为了克服 BP 神经网络本身所具有的局限性，本文利用 PSO 算法对 BP 神经网络进行了优化，优化步骤如下:

1) 对 BP 神经网络的结构、传递函数、目标向量等进行初始化。

2) 设置粒子群的规模、参数维数、迭代次数、动量系数、粒子的初始位置和初始速度。

3) 利用训练集对 BP 神经网络进行训练，并按照式(5)对各粒子的适应度值进行评价。

4) 对每个粒子的当前值和历史最好值进行比较，若当前

值优于历史最好值，则保存粒子的当前值为其个体的历史最好值；比较粒子群的当前值和其历史最好值，若其当前值更优，则保存当前值为其历史全局最好值。

5) 计算惯性权值。

6) 对每个粒子的位置和速度进行更新，分别记录每个粒子和粒子群的系统适应度值误差。

7) 判断系统适应度值误差，如果误差达到了设定的误差限值或超过了最大允许的迭代次数，则训练结束。此时粒子的历史全局最优位置即为 BP 神经网络的最佳权值和最优阈值。

3.5 计算机网络安全评价模型

本文利用 PSO－BPNNPSO－BPNN 模型对计算机网络安全进行评价，首先构建了计算机网络安全评价指标体系，然后，利用粒子群算法对 BP 神经网络进行优化，得到了 BP 神经网络的最佳权值和最优阈值，最后利用优化的 BP 神经网络模型进行计算机网络安全评价，其具体步骤见图 3 所示。

4 仿真研究

4.1 实验数据

由于有关计算机网络安全的数据集可共享的并不多，本文收集了 50 组不同规模的计算机网络安全评价有关数据，并将其进行了归一化处理，见表 2。将前 45 组数据作为 PSO－BPNN 的训练数据集，后 5 组数据作为测试数据集。

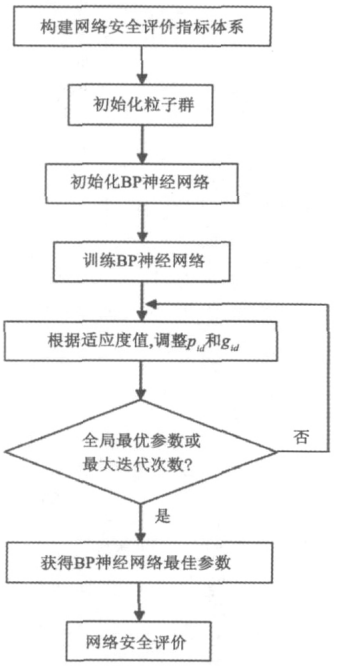

图 3 计算机网络安全的评价过程

表 2 计算机网络安全仿真数据集

序号	C_{11}	C_{12}	C_{13}	C_{14}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{37}	C_{38}	C_{39}	期望输出
1	1	0.8	0.8	0.8	1	0.8	0.85	0.8	0.72	0.8	0.92	0.87	0.85	0.8	0.93	1	0.8	0.8	0.9	0.85
2	1	1	0.8	0.8	1	0.9	0.85	0.8	0.77	0.8	0.93	0.9	0.9	1	0.95	1	0.8	0.6	0.9	0.88
3	0.4	0.4	0.2	0.2	0	0.3	0.25	0.4	0.43	0.4	0.47	0.55	0.45	0.4	0.47	0	0.4	0.2	0.4	0.33
4	0.8	0.8	0.6	0.6	0	0.6	0.65	0.6	0.67	0.6	0.81	0.72	0.75	0.6	0.82	0	0.8	0.4	0.7	0.67
5	0.6	0.4	0.4	0.2	0	0.5	0.5	0.4	0.61	0.6	0.62	0.61	0.65	0.4	0.55	1	0.6	0.2	0.6	0.50
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
46	0.4	0.6	0.4	0.4	0	0.4	0.45	0.4	0.52	0.4	0.65	0.63	0.7	0.6	0.67	0	0.6	0.4	0.6	0.46
47	0.6	0.8	0.6	0.6	0	0.5	0.65	0.6	0.63	0.6	0.77	0.75	0.7	0.6	0.81	0	0.6	0.4	0.7	0.61
48	0.8	0.8	1	0.6	1	0.8	0.8	0.8	0.78	0.8	0.89	0.85	0.9	0.8	0.91	1	0.8	1	0.8	0.85
49	0.2	0.4	0.2	0.2	0	0.3	0.3	0.2	0.27	0.2	0.33	0.37	0.25	0.2	0.35	0	0.2	0.2	0.4	0.24
50	0.8	0.8	0.4	0.6	1	0.5	0.6	0.6	0.64	0.6	0.75	0.77	0.8	0.6	0.78	0	0.6	0.4	0.7	0.63

4.2 模型参数设置

设置粒子群的种群规模 $m = 10$，学习因子 $c_1 = c_2 = 2$，将所有粒子作为 BP 神经网络中所有权值和阈值，粒子的初始位置随机产生，初始化粒子的初始位置和速度，最大迭代次数 $K = 500$。为了说明利用 PSO 算对 BP 神经网络的优化的效果，本文利用传统的 BP 神经网络作为对比模型，两种模型选择均利用 traingdx 作为网络的激发函数，目标误差等于 0.001。

4.3 BP 神经网络训练

利用计算机网络安全评价数据集的前 45 组数据对 BP 神经网络和 PSO－BPNNPSO－BPNN 模型进行了训练，由于篇幅所限，本文未列出训练曲线图。从训练过程中发现，传统的 BP 神经网络收敛速度很慢，在第 417 步时训练结束，误差为 0.000984，而 PSO－BPNNPSO－BPNN 模型在经过 312 迭代时其误差精度就达到了 0.000761，比传统的 BP 神经网络模型的误差精度高，从而说明了传统 BP 神经网络的收敛速度慢，易陷入了局部极小值，其整体寻优能力不强，大大影响了模型的评价精度。而 PSO－BPNNPSO－BPNN 模型由于

利用 PSO 算法对 BP 神经网络有效地进行了优化，不仅使得其整体寻优能力得到了极大的提高，网络训练速度加快，而且有效地提高了训练误差精度。

4.4 结果与分析

当两种神经网络达到预定的学习精度后，保存网络，然后利用测试集进行测试，测试结果见表 3。结果表明，传统的 BP 神经网络对 47 号计算机网络安全数据的评价结果是错误的，样本数据的安全等级为 C 级，即不安全，但是其评价结果却为极不安全，利用 PSO 优化的 BP 神经网络的评价正确率达到了 100%。从两种模型的均方根误差可知，传统的 BP 神经网络的均方根误差为 0.067，远远大于 PSO - BPNN 模型的均方根误差，其均方根误差只有 0.023，从而说明了利用 PSO 算法对 BP 神经网络的优化是成功的，不仅加快了网络的收敛速度，而且模型的评价精度得到了极大的提高。

表 3 评估结果比较

样本	安全等级	期望输出	BPNN	PSO - BPNN 模型
46	D	0.46	0.41	0.44
47	C	0.61	0.55	0.64
48	A	0.85	0.76	0.86
49	D	0.24	0.19	0.26
50	C	0.63	0.69	0.66
均方根误差			0.067	0.023

5 结束语

本文利用 PSO 算法和 BP 神经网络进行了有效地 PSO - BPNN，利用 PSO 算法对 BP 神经网络进行优化，充分地利用了 BP 神经网络超强的非线性函数逼近能力，利用 BP 神经网络对计算机网络安全进行评价，考虑到 BP 神经网络存在着收敛速度慢，易陷入局极小、全局搜索能力不强的缺限，利用 PSO 算法对 BP 神经网络的权阈值进行了有效的优化，从而获得 BP 神经网络最佳的权值和最优的阈值，使 BP 神经网络的参数得到了根本性的优化，有效地提高了计算机网络评价的精度。仿真结果表明，经过 PSO 算法优化的 BP 神经网络模型的全局搜索能力、评价精度、收敛速度都明显高于传统的 BP 神经网络，说明了利用 PSO 算法对 BP 神经网络的优化是成功的，为以后的网络评价提供了一种新的尝试。

参考文献:

[1] 楼文高，姜丽，孟祥辉. 计算机网络安全综合评价的神经网络模型 [J]. 计算机工程与应用，2007，43(32)：128 - 130.

[2] 冯妍，房鼎益，陈晓江. 一个计算机网络安全风险评估模型的研究与设计 [J]. 计算机应用与软件，2007，24(5)：28 - 31.

[3] 于群，冯玲. 基于 BP 神经网络的计算机网络安全评价方法研究 [J]. 计算机工程与设计，2008，29(8)：1963 - 1966.

[4] 高会生，郭爱玲. SVM 和 ANN 在计算机网络安全风险评估中的比较研究 [J]. 计算机工程与应用，2008，44(34)：116 - 118.

[5] 孙亚. 基于粒子群 BP 神经网络人脸识别算法 [J]. 计算机仿真，2008，25(8)：201 - 204.

[6] 李宁，邹彤，孙德宝. 带时间窗车辆路径问题的粒子群算法 [J]. 系统工程理论与实践，2004，(4)：130 - 135.

[7] 邓凯，赵振勇. 基于遗传 BP 网络的股市预测模型研究与仿真 [J]. 计算机仿真，2009，26(5)：316 - 319.

[作者简介]

武仁杰(1965 -)男(汉族)，河北怀安人，副教授，硕士，主要研究方向：计算机网络与信息处理。

(上接第 77 页)

因此在设计搜索算法时，既要保证捕获目标的概率，又要尽量减少搜索的时间，还要考虑到拦截器的姿态机动能力。本文假设目标相对于拦截器的方位偏差服从正态分布，在此基础上设计了渐开线式等线速律扫描的搜索算法。而后以固体推力器为基础，给出了由最终滑模控制方法得到的姿态跟踪控制器。最后仿真表明了搜索算法与姿态控制器有效性。

参考文献:

[1] 姜玉宪，张华明. 导弹中制导末段的最优搜索 [J]. 航空航天大学学报，2002，28(6)：695 - 698.

[2] 曹泽阳，高虹霓. 照射制导雷达自主搜索仿真模型 [J]. 航空计算技术，2001，31(4)：28 - 32.

[3] 刘世勇，吴瑞林，周伯昭. 大气层外拦截弹末制导段的目标搜索算法 [J]. 飞行力学，2004，22(4)：37 - 40.

[4] 张景瑞，荆武兴，徐世杰. 空间飞行器大角度姿态跟踪机动问题研究 [J]. 飞行力学，1999，17(3)：87 - 91.

[5] 张德雄，王照斌. 动能拦截器的固体推进剂轨控和姿控系统 [J]. 推进技术，2001，(2)：37 - 41.

[6] 吴启星，刘世勇，张为华. 大气层外拦截器末端轨控方案分析 [J]. 航天控制，2007，25(3)：17 - 22.

[作者简介]

张 旭(1984 -)，男(汉族)，山东省聊城市人，博士研究生，主要研究领域为动能拦截器制导控制技术；

周 军(1966 -)，男(汉族)，江苏常州市人，教授，博士研究生导师，主要研究领域：现代控制理论及应用；

呼卫军(1979 -)，男(汉族)，陕西延安市人，副教授，硕士研究生导师，主要研究领域：飞行器制导控制与仿真。