

神经网络在网络安全评价中的应用研究

姓名：吴东元 学号：201721220101

摘要：在科技高度发展的当今社会中，计算机网络技术已经逐渐应用到人们的生活、学习等不同的领域中。基于计算机网络的特性，网络为人们的生活带来便利的同时也存在着一定的信息安全隐患。在社会发展中，很多由于计算机网络安全隐患而引发的问题屡见不鲜，因此我们应当高度在重视对于计算机网络安全的评价。将神经网络应用到网络安全评价中，能够发挥出神经网络的优势，使得评价更加的全面。

关键词：神经网络 计算机网络安全 评价 粒子群算法

一、神经网络的评价原理

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。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。

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。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。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、易陷入局部小、全局搜索能力较差等缺陷，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。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：

$$\text{网络安全级别} = f(x_1, x_2, \dots, x_i, \dots, x_m) \quad (1)$$

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，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。

3.2 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。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 1。

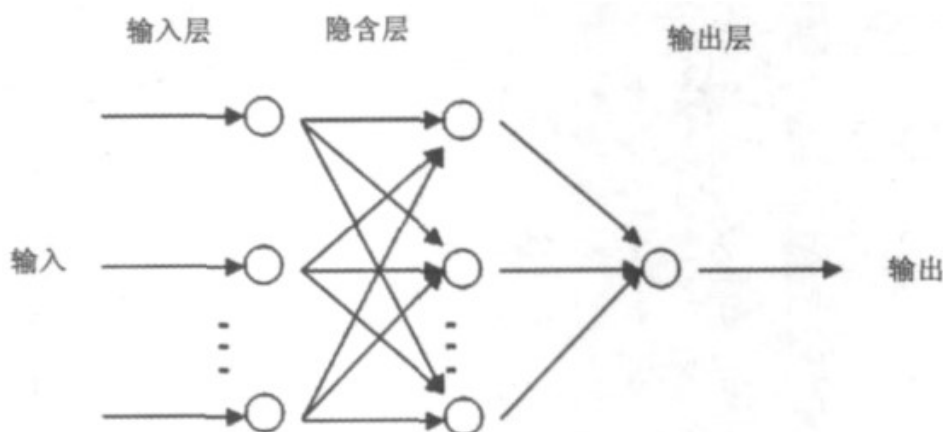


图 1 BP 神经网络结构图

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。

3.3 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 2 所示。

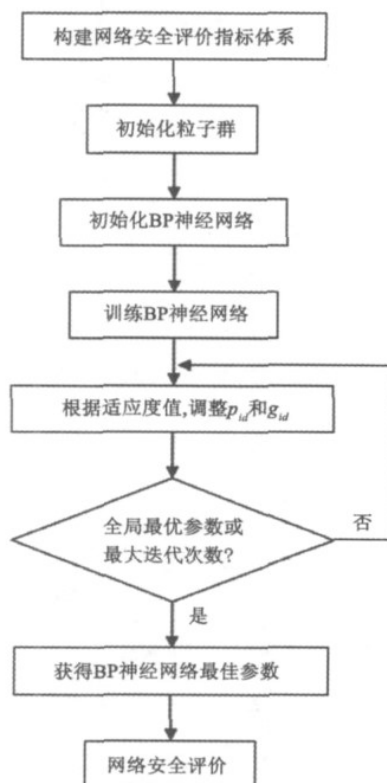


图 2 计算机网络安全的评价过程

4 仿真研究

4.1 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 — BPNPSO — 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 — BPNPSO — 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 — BPNPSO — 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。

4.2 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。

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陷，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.