一种应用神经网络技术的威胁估计算法

邱浪波，　刘作良，　刘　明
(空军工程大学 电讯工程学院，陕西 西安　710077)

摘　要：在对现有威胁估计算法分析的基础上，结合神经网络技术，提出了基于BP神经网络模型的威胁估计算法，利用神经网络良好的自适应能力和自学习能力，通过样本数据训练，提高威胁估计算法的准确性和适应性。

关键词：威胁估计；神经网络；BP算法
中图分类号：E95；TP18　　**文献标识码**：A　　**文章编号**：1009-3516(2002)06-0025-04

威胁程度一般是指敌方目标对我方保卫目标进行侵犯的可能性及侵袭成功时可能造成的破坏程度。因此，对敌平台对我防区保卫目标的威胁程度的准确而及时的估计将是十分重要的。文献[1~2]都提出了基于多属性决策的威胁估计算法，因素权值的确定多采用专家评比的方式，而专家在评定时主要是基于其专业知识、经验，因此，评定结果带有一定的主观性和不确定性；同时，采用常权向量进行综合的算法，不能很好的解决各因素在不同状态下的组态问题，常使得在某些情况下评估结果与实际情况不符，不能很好的映射因素间的复杂关系；而且，模型本身不具备自学习能力，使其不能通过学习来进行自我修正，其适应性须得到提高。在此基础上，本文提出了基于神经网络模型的算法，利用神经网络良好的自适应能力、自学习能力和高度线性和非线性映射能力，通过样本数据训练，提高威胁估计的准确性和适应性。

1　BP神经网络模型

目前，神经网络信息处理技术的研究及应用日益拓宽。神经网络技术具有明显的优点：① 较强的收敛性及自适应自组织学习能力；②较好的容错性；③ 并行处理强、识别预测迅速准确、稳健性好。利用过去和现在的数据作学习样本集，通过某种非线性处理来建立模型，由此对系统变量的行为(状态)作出科学定量的估计。D. Rumelhart等人提出了误差反向传递学习算法(即BP算法)，实现了Minsky的多层网络设想，其模型如图1所示。

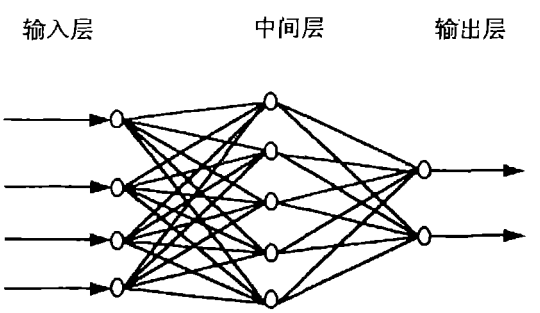

图1　BP神经网络模型

BP算法不仅有输入层节点、输出层节点，还可有一层或多层隐含层节点[3]。对于输入信号，要先向前传播到隐含层节点，经特性函数作用后，再把隐节点的输出信号传播到输出节点，最后给出输出结果。节点的特性函数要求是可微，通常选取S型函数，如

$$f(x)=\frac{1}{1-e^{-x/Q}}$$

式中Q为调整特性函数形式的Sigmoid参数。该算法的学习过程由正向传播和反向传播组成。在正向传播过程中，输入信息从输入层经隐含层逐层处理，并传向输出层。每一层神经元的状态只影响下一层神经

收稿日期：2002-01-10
作者简介：邱浪波(1977-)，男，四川自贡市人，硕士生，主要从事指挥自动化和信息处理研究.

元的状态。如果输出层得不到期望的输出,则转入反向传播,将误差信号沿原来的连接通道返回,通过修改各层神经元的权值,使得误差信号最小。一旦网络经过训练用于求解现实问题,则只需正向传播。

现给出 BP 算法学习的具体步骤:①从训练样例集中取一样例,作为输入信息输入到网络中;②由网络分别计算各层节点的输出;③计算网络的实际输出与期望输出的误差;④从输出层反向计算到第一个隐层,按一定的原则向减小误差方向调整网络的各个连接权值;⑤对训练样例集中的每一个样例重复以上步骤,直到对整个训练样例的误差达到要求时为止。

在以上步骤中,关键是第 4 步,必须确定如何沿减小误差的方向调整连接权值。以下作简要说明,符号约定如下:o_i—节点 i 的输出;net_j—节点 j 的输入;w_{ij}—层节点 i 到节点 j 的连接权值;η —学习因子;y_k,$\hat{y}_k$—分别为输出层上节点 k 的实际输出和期望输出。

显然,对于节点 j 有

$$net_j = \sum_i w_{ij} o_i ;\ o_j = f(net_j) \tag{1}$$

将误差函数定义为

$$e = \frac{1}{2} \sum_k (\hat{y}_k - y_k)^2 \tag{2}$$

连接权值的修改由下式计算:

$$w_{jk}(t+1) = w_{jk}(t) + \Delta w_{jk} \tag{3}$$

$$\Delta w_{jk} = -\eta \frac{\partial e}{\partial w_{jk}} ;\ \frac{\partial e}{\partial w_{jk}} = \frac{\partial e}{\partial net_k} \cdot \frac{\partial net_k}{\partial w_{jk}} \tag{4}$$

由式(1)可得

$$\frac{\partial net_k}{\partial w_{jk}} \cdot \frac{\partial}{\partial w_{jk}} \sum_j w_{jk} o_j = o_j \tag{5}$$

令:$\delta_k = \frac{\partial e}{\partial net_k}$,则:

$$\Delta w_{jk} = -\eta \frac{\partial e}{\partial w_{jk}} = -\eta \delta_k o_j \tag{6}$$

下面分 2 种情况计算 δ_k

1)当 k 为输出节点时,$o_k = y_k$,则

$$\delta_l = \frac{\partial e}{\partial net_k} = \frac{\partial e}{\partial y_k} \cdot \frac{\partial y_k}{\partial net_k} \tag{7}$$

由于

$$\frac{\partial e}{\partial y_k} = -(\hat{y}_k - y_k) ;\ \frac{\partial y_k}{\partial net_k} = f(net_k) \tag{8}$$

所以

$$\delta_k = -(\hat{y}_k - y_k) f(net_k) \tag{9}$$

$$\Delta w_{jk} = -\eta (\hat{y}_k - y_k) f(net_k) o_j \tag{10}$$

2)若 k 不是输出节点,则有

$$\delta_k = \frac{\partial e}{\partial net_k} = \frac{\partial e}{\partial o_k} \cdot \frac{\partial o_k}{\partial net_k} = \frac{\partial e}{\partial o_k} f'(net_k) ;\ \frac{\partial e}{\partial o_k} = \sum_m \delta_m w_{km} \tag{11}$$

所以

$$\delta_k = f'(net_k) \sum_m \delta_m w_{km} \tag{12}$$

从上述 BP 算法可以看出,BP 模型把一组样本的 I/O 问题变为一个非线性优化问题,它使用的是优化中最普通的梯度下降法。可以把 BP 神经网络看成是一个高度非线性映射。

2 建立威胁估计模型

严格的讲,威胁估计是一个较为复杂的问题,要考虑的因素很多,例如天气情况、地理环境、敌、我、邻军队的兵力部署及战斗力等。在对敌性目标进行威胁评估时必须综合考虑。在防空作战过程中,进行威胁估计通常考虑以下的因素:

1)目标类型:小型目标(空地导弹(AGM)、反辐射导弹(ARM)、巡航导弹、隐身飞机等)、大型目标(轰炸机、歼击轰炸机、强击机等)、武装直升机等;

2)目标的速度:如 300 m/s、500 m/s、1 400 m/s 等;

3) 目标的进入角: 如 5°、1 0°、1 5°等;

4) 目标的高度: 如 高空、中空、低空、超低空等;

5) 距被保卫目标距离: 如 100 km、200 km、300 km 等。

各因素相互间的关系复杂,不是简单的线性组合,在进行威胁估计时,要全面合理地考虑各种因素,给出一个威胁程度与各种因素的函数关系困难很大。神经网络技术是模拟人脑的思维方式和组织形式而建立起来的具有较好收敛性的高度线性与非线性复合数学模型,将能很好的解决威胁估计中的非线性问题。威胁估计的神经网络模型如图 2 所示。

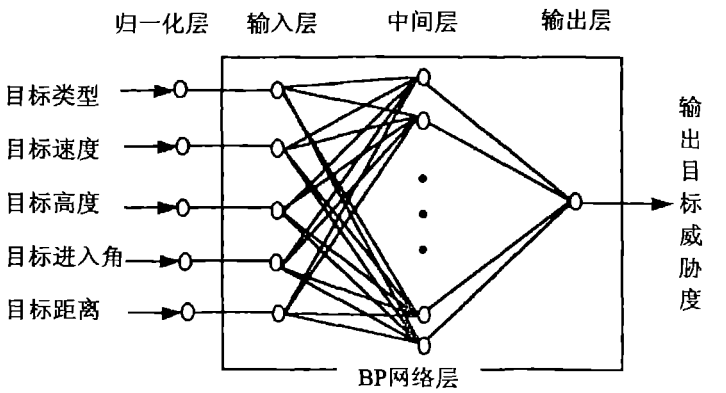

图 2　威胁估计 BP 神经网络模型

第一层为归一化层,共取 5 个节点,输入向量为目标类型、目标速度、目标高度、目标进入角、目标距我保卫目标的距离。为了减小输入各分量由于数值和类型的差异所带来的影响,特性函数为各因素威胁度函数,将因素的具体值转换为目标距离威胁、速度威胁、高度威胁等属性值。输出为经过归一化处理的各因素的威胁度;

第二层为 BP 网络输入层,共取 5 个节点,输出特性函数取 S 型函数;

第三层为隐层,此处取 8 个节点,输出特性函数取 S 型函数;

第四层为输出层,取 1 个节点,取 S 型函数。输出值为敌性目标对我保卫目标的威胁程度,采用[0 ~ 1]区间的连续数,主要为了便于对威胁程度的精确刻画以及对多威胁目标进行排序。

3　确定因素威胁度函数

参照文献[1],在确定各因素威胁度的属性值时,对定性因素,采用 G. A. Millar 的 9 级量化方法,对定量因素采取 9 级区间量化的方法,经归一化处理后,作为第一层的输出。具体量化如下:

1) 目标类型威胁:按小型目标、大型目标、武装直升机依次量化为 8、5、3;

2) 目标的速度威胁:按 0 ~ 1 800 m/s 等间隔 (200 m/s) 依次量化为 1 ~ 9;

3) 目标的进入角威胁:按.0° ~ 36°等间隔 (4°) 依次量化为 9 ~ 1;

4) 目标的高度威胁:按高空、中空、低空、超低空依次量化为 2、4、6、8;

5) 距被保卫目标的距离威胁:按 0 ~ 450 km 等间隔 (50 km) 依次量化为 9 ~ 1。

文献[1]对因素威胁度归一化处理时存在明显不足,将当前多来袭目标同一因素的最大威胁量化值归一化为 1,会丢失来袭目标对我保卫目标的绝对威胁程度信息,实际上其得出的只是当前各来袭目标对我保卫目标的相对威胁程度。所以,本文采用将因素威胁度量化最大值 9 归一化为 1 的基础上,完成来袭目标各因素威胁度量化值的归一化处理,在充分保留来袭目标绝对威胁程度的基础上,完成对来袭目标的威胁排序。

4　实例分析

算法验证时,引用了文献[1]的数据。η 初值取为 0. 001,为减少迭代次数和加快收敛速度,采用变步长法根据输出误差大小自动调整学习因子,优化学习因子 η 如下:

$$\eta = \eta + a \times (e(t) - e(t-1))/e(t-1)$$

其中,a 为调整步长,在[0,1]之间取值,此处取 0. 6。神经元间的连接权值初始化为[-0. 5,0. 5]之间的随机数。样本集如表 1 所示。

表 1 样本集

名 称	目标类型	目标速度 (m/s)	目标进入角 (°)	目标高度	目标距离 (km)	输出威胁度
目标 1	大型目标	400	5	中空	100	0.539
目标 2	大型目标	720	8	中空	150	0.637
目标 3	小型目标	1600	3	低空	300	0.741
目标 4	小型目标	1200	5	低空	260	0.669
目标 5	大型目标	280	10	超低空	140	0.567
目标 6	武装直升机	100	15	超低空	120	0.440
目标 7	大型目标	500	18	中空	260	0.487
目标 8	大型目标	370	20	低空	290	0.519
目标 9	小型目标	400	12	低空	300	0.595
目标 10	大型目标	230	22	中空	350	0.370
目标 11	武装直升机	80	9	低空	100	0.447

误差范围选定为 0.001,经过 1 758 次训练后,达到了误差范围,将表 2 数据作为验证数据代入计算。

表 2 验证数据

名 称	目标类型	目标速度 (m/s)	目标进入 (°)	目标高度	目标距离 (km)	输出威胁度
目标 1	小型目标	180	8	高空	180	0.490
目标 2	大型目标	280	17	高空	210	0.469
目标 3	大型目标	420	3	中空	290	0.562
目标 4	小型目标	600	18	低空	320	0.543

将几组数据代入模型运算,其结果与文献[1]所示排序结果基本一致,从而验证了该模型的有效性。同时,其结果更客观的反映了来袭目标对我保卫目标的威胁程度。基于神经网络模型的算法,利用实战背景中的样本数据,通过学习来进行自我修正,在一定程度上克服了专家评定结果带有的主观性和不确定性。同时,比较好地克服了采用常权向量进行综合所带来的组态问题,使得评估结果与实际情况更相符,很好的映射了因素间的复杂关系,提高了威胁估计的准确性和适应性。

参考文献:

[1] 周 林. 基于 MADM 的威胁评估排序模型[J]. 系统工程与电子技术,2001,25(1):18 - 19.

[2] 曲长文. 应用多属性决策的威胁评估方法[J]. 系统工程与电子技术,2000,22(5):26 - 29.

[3] 刘 铭,宁伟华,陈永革,等. 基于改进 BP 算法的装备效能评估[J]. 空军工程大学学报(自然科学版),2001,2(3):18 - 20.

(编辑:门向生)

A Threat Assessment Algorithm by Using the Neural Network Techniques

QIU Lang - bo, LIU Zuo - liang, LIU Ming

(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an Shaanxi 710077, China)

Abstract: Based on analyzing current models of threat assessment, combined with the neural network techniques, this paper presents a threat assessment algorithm based on BP algorithm. By utilizing the good abilities of adapting and self - learning of neural networks, the accuracy and adaptability of the threat assessment algorithm are improved.

Key Words: threat assessment; neural network; BP algorithm