基于 RAN-RBF 神经网络的网络安全态势预测模型

甘文道[1] 周 城[1] 宋 波[2]
(重庆通信学院网络安全实验室 重庆 400035)[1]
(重庆通信学院应急通信重庆市重点实验室 重庆 400035)[2]

摘 要 为了更准确地获悉网络安全态势的发展情况,提出了一种基于资源分配网络径向基函数(Resource Allocating Network Radical Basis Function,RAN-RBF)神经网络的网络安全态势预测(Network Security Situation Prediction,NSSP)模型。该模型采用资源分配网络算法对网络安全态势样本进行聚类,得到神经网络的隐含层节点数,引入剪枝策略删除对网络贡献不大的节点,用改进的粒子群算法(Modified Particle Swarm Optimization,MPSO)对神经网络的中心、宽度、权值进行优化,对未来网络安全态势进行预测。利用校园网网络管理部门提供的数据进行的仿真实验表明,相对于 K-均值 RBF 神经网络预测模型,该模型可以得到更合适的 RBF 神经网络结构和控制参数,提高了预测精度,更加直观地反映了网络安全态势的总体情况,为网络安全管理员提供了态势图。

关键词 资源分配网络径向基函数(RAN-RBF)神经网络,网络安全态势预测(NSSP),改进的粒子群算法(MPSO),态势图

中图法分类号 TP309 **文献标识码** A

Network Security Situation Prediction Model Based on RAN-RBF Neural Network

GAN Wen-dao[1] ZHOU Cheng[1] SONG Bo[2]
(Laboratory of Network Security,Chongqing Communication Institute,Chongqing 400035,China)[1]
(Chongqing Key Laboratory of Emergency Communication,Chongqing Communication Institute,Chongqing 400035,China)[2]

Abstract In order to know the development of network security situation more accurately,a model of network security situation predicition (NSSP) based on resource allocating network radical basis function (RAN-RBF) neural network was proposed. The model uses the algorithm of resource allocating network to cluster the samples of network security situation,and get the number of the hidden layer nodes of neural network,introducing pruning strategies to remove nodes that contribute little to the network,the neural network of centers,widths and the weights are optimized by modified particle swarm optimization (MPSO) algorithm,to predict the future network security situation. Using the data provided by the network management department of campus network simulation experiments show that compared with K-means clustering RBF neural network prediction model,the model can get more appropriate RBF neural network structure and control parameters,to improve the accuracy of the predictions,more directly reflects the overall situation of the network security situation and provide situation map for the network security administrators.

Keywords Resource allocating network radical basis function (RAN-RBF) neural network,Network security situation prediction (NSSP),Modified particle swarm optimization (MPSO),Situation map

网络安全态势感知(Network Security Situation Awareness,NSSA)[1]源于空中交通监管态势感知(Air Traffic Control,ATC)[2],在航天飞行、军事战场、核反应控制、空中交通监管以及医疗应用调度等领域得到广泛应用[3]。文献[4]中指出,网络安全态势感知是指:在大规模网络环境中,对能够引起网络态势发生变化的各种安全要素进行获取、理解、显示,并以此来预测网络未来的发展趋势。

为了解决网络安全态势预测(NSSP)中的难点问题,国内外学者做了积极的探索研究。国外对网络安全态势感知的研究起步较早,在态势预测方面,R. K. Saha 等人提出了一种基于线性回归的预测方法[5],实现了对网络带宽的优化和对网络态势的感知;Joel Brynielsson 和 Stefan Arnborg 提出了一种基于贝叶斯网络的态势感知和预测模型[6],将博弈论工具应用于预测领域,与贝叶斯网络相结合,实现对作战指挥控制的辅助决策等。国内虽然研究起步较晚,但是做了大量研究工作,并且提出了很多网络安全态势预测方法和模型。清华

本文受国家自然科学基金项目(61272043),重庆市基础与前沿研究重点项目(cstc2013jjB40009)资助。
甘文道(1990-),男,硕士生,主要研究方向为信息安全,E-mail:ganwendao@qq.com;周 城(1963-),男,副教授,硕士生导师,主要研究方向为信息安全;宋 波(1990-),男,硕士生,主要研究方向为软件无线电。

大学的谢丽霞等人[7]提出了一种基于 RBF 神经网络的网络安全态势预测方法，并利用自适应遗传算法对神经网络做了优化；哈尔滨工程大学的王慧强等人[8]提出了基于多类支持向量机理论的网络安全态势感知模型；上海交通大学的任伟等人[9]利用网络安全态势值具有非线性时间序列的特点，提出了基于 K 均值 RBF 神经网络的网络安全态势预测方法等。经过研究分析，RBF 神经网络的隐含层节点数和相关控制参数直接影响了其预测精度，所以对样本的合理聚类和相关控制参数的优化对于提高预测精度显得尤为重要。

为了更准确地获悉网络安全态势的发展情况，本文提出了一种基于资源分配网络径向基函数(Resource Allocating Network Radical Basis Function，RAN-RBF)神经网络的网络安全态势预测模型。该模型首先对网络安全态势样本 RAN 聚类，得到更合适的隐层节点数，用改进的粒子群算法(MPSO)对神经网络的中心、宽度、权值进行优化，对未来网络安全态势进行预测。

1 RBF 神经网络结构

RBF 神经网络是一种 3 层前向网络，它通过非线性基函数的线性组合来寻找样本间的线性映射关系，并利用此映射关系实现预测。RBF 神经网络由输入层、隐含层和输出层构成，如图 1 所示。输入层由 n 个感知神经元组成，作用是建立外部输入变量与内部神经元的连接；隐含层有 h 个隐含节点，实现输入变量映射到隐含层空间的非线性变换；输出层有 m 个输出层节点，实现隐含层输出的线性变换，得到最终预测结果。

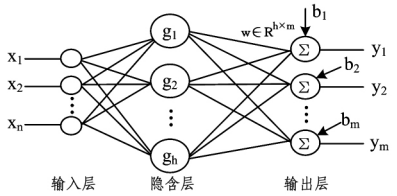

图 1 RBF 神经网络结构图

RBF 神经网络的核心部分是隐含层。对于 n 维输入向量 X，第 i 个隐含层节点的输出为：

$$\phi_i = g_i(X, c_i), X=[x_1, x_2, \cdots, x_n], i=1,2,\cdots,h \tag{1}$$

其中，c_i 是第 i 个隐含层神经元的数据中心；$g(x, c_i)$ 是基函数，选取常用的高斯函数，形式如下：

$$g(x, c_i) = \exp\left(-\frac{\| x-c_i \|}{2\sigma_i^2}\right), i=1,2,\cdots,h \tag{2}$$

式中，网络的拓展宽度为 σ_i，$\| \cdot \|$ 是欧氏范数。

网络输出层第 j 个神经元节点的输出为隐含层节点输出的线性加权聚合：

$$y_j = \sum_{i=1}^{h} w_{ij}\phi_i + b_j, j=1,2,\cdots,m \tag{3}$$

式中，w_{ij} 为输出层第 j 个神经元与隐含层第 i 个神经元的连接权值；b_j 为输出层第 j 个神经元的阈值。

2 RAN-RBF 神经网络预测模型

本文以网络安全态势感知的通用模型为基础，结合所做的研究工作，提出了一种基于 RAN-RBF 神经网络的网络安全态势预测模型，如图 2 所示。

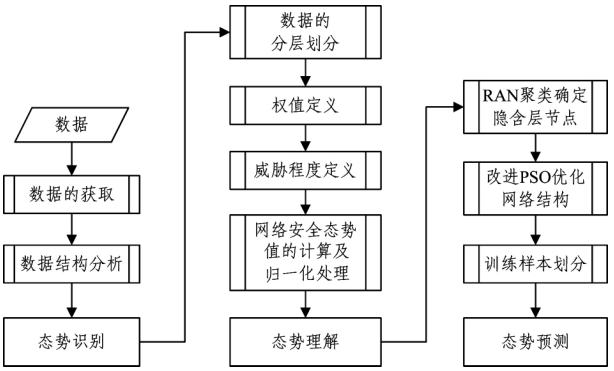

图 2 模型框架结构

模型由 3 个阶段构成，每个阶段有对应的工作任务，具体情况如下。

1)态势识别：主要是对网络安全数据的获取，本文主要是从校园网网络管理部门捕捉黑客攻击数据；

2)态势理解：主要是对获取的数据做分析处理，从数据类型、数据结构分析，然后根据数据对安全事件的统一设置做分层划分、权值定义、威胁程度定义、加权平均和归一化等处理，得到网络安全态势值；

3)态势预测：主要利用 RAN 算法样本聚类、MPSO 算法优化训练 RBF 神经网络，找到样本间的非线性映射关系来预测网络安全态势，最后做出态势预测分析。

1)、2)两个阶段将在仿真实验及分析部分具体介绍，现主要对阶段 3)作详细分析。

3 RAN 聚类确定隐含层节点

3.1 隐含层节点数的确定

RBF 神经网络隐含层节点的多少直接影响了其预测能力。当隐含层节点个数选取太少时，网络的预测精度很低，不能满足预测要求；当隐含层节点个数选取太多时，虽能提高网络的预测精度，但也提高了网络复杂度，训练时间延长[10]，并且开销也增大。所以应该综合考虑来确定隐含层节点数，同时也反映出人为确定隐层节点个数的弊端。

为了能找到更为合适的隐含层节点个数，结合文献[11，12]中提出的资源分配网络(RAN)算法来解决隐含层节点个数难以确定的问题。根据预测需要，我们建立 n-h-1 资源分配网络(RAN)，其与 RBF 网络完全一样，如图 3 所示。

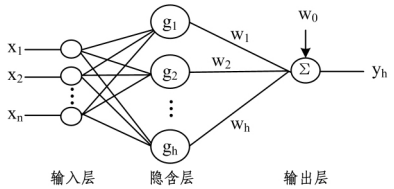

图 3 RAN 结构图

RAN 网络的输出为：

$$y_h(k) = w_0 + \sum_{i=1}^{h} w_i g(X, c_i), 1 \leqslant k \leqslant L \tag{4}$$

式中，w_0 为阈值，k 为隐层节点编号，L 为隐层节点计数器。

假设样本输入序列为：

$$S(i) = \{(x_i, y_i), i=1,2,\cdots,N\} \tag{5}$$

利用两组样本数据$(x_1,y_1),(x_2,y_2)$初始化网络参数：

$$w_0=y_1,w_1=y_2-y_1,c_1=x_2,\sigma_1=\mu\delta_{\max}^2 \tag{6}$$

其中，$\mu\in(0,1)$，σ_1 为隐含层节点初始扩展宽度，$\delta_{\max}$为输入样本 x_i 之间的最大距离。

判定是否增加 x_i 为“新”的误差准则和距离准则：

$$|e_k|=\|y_h(k)-T(k)\|>\varepsilon \tag{7}$$

$$d_i=\|x_i-c_{nearest}\|=\min_{1\leqslant k\leqslant L}\|x_i-c_k\|>\delta_i \tag{8}$$

其中，$T(k)$为网络期望输出，$c_{nearest}$为距 x_i 最近的隐层节点中心，$\delta_i=\max\{\gamma\delta_{\max},\delta_{\min}\}$，$\gamma\in(0,1)$为衰减常数，$\varepsilon$ 为期望的精度。

当同时满足误差准则和距离准则时，增加一个新的隐含层节点，并设置节点参数，否则不增加：

$$w_{L+1}=e_k,c_{L+1}=x_i,\sigma_{L+1}=\gamma d_i \tag{9}$$

3.2 隐含层节点数的优化

RAN 算法确定隐含层节点数的过程中有可能产生冗余节点，结合文献[13]中的“裁剪”方法，通过剪枝策略消除冗余，方法如下。

1)计算每次的隐层节点输出：

$$\phi_i^n=\exp\left(-\frac{\|x-c_i\|}{2\sigma_i^2}\right),i=1,2,\cdots,h \tag{10}$$

2)找到隐层节点输出值最大的神经元，记为 $\phi_{\max}^n$，将所有输出值统一规范化：

$$r_i^n=\left|\frac{\phi_i^n}{\phi_{\max}^n}\right|,i=1,2,\cdots,h \tag{11}$$

3)经过 L 次的输入输出，若 $r_i^n<\theta,\theta$ 为判别阈值，说明该隐含层节点的相关性太小，可以忽略，则删除该隐含层节点。

4 改进粒子群算法优化 RBF 神经网络

4.1 基本粒子群算法(PSO)

基本粒子群算法(PSO)是一种基于个体协作与竞争来完成复杂空间中搜索最优解的方法，每一个粒子表征问题的一个解，所有的粒子都有一个被目标函数决定的适应值，它们以一定的速度在搜索空间中飞行，根据自身及同伴的飞行经验进行动态调整，迭代搜索最优值。

PSO 的数学描述：假设在一个 D 维搜索空间中，有 m 个粒子组成一个群体。空间中第 i 个粒子的位置向量和速度向量分别为：

$$\overrightarrow{x_i}=(x_{i1},x_{i2},\cdots,x_{iD}),i=1,2,\cdots,m \tag{12}$$

$$\overrightarrow{v_i}=(v_{i1},v_{i2},\cdots,v_{iD}),i=1,2,\cdots,m \tag{13}$$

它在迄今为止搜索到的最优位置为：

$$\overrightarrow{p_i}=(p_{i1},p_{i2},\cdots,p_{iD}),i=1,2,\cdots,m \tag{14}$$

整个粒子群搜索到的最优位置为：

$$\overrightarrow{p_g}=(p_{g1},p_{g2},\cdots,p_{gD}) \tag{15}$$

寻优过程中位置和速度的动态调整：

$$\overrightarrow{v_{id}}(t+1)=\omega v_{id}(t)+P_1+P_2,d=1,2,\cdots,D \tag{16}$$

$$P_1=c_1rand(p_{id}-x_{id}(t)) \tag{17}$$

$$P_2=c_2rand(p_{gd}-x_{id}(t)) \tag{18}$$

$$x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) \tag{19}$$

其中，惯性权值 $\omega=0.9$，加速因子 $c_1=c_2=2$，$rand$ 是在$[0,1]$上均匀分布的随机数，$x_{id}\in[-x_{\max},x_{\max}]$，$v_{id}\in[-v_{\max},v_{\max}]$，$v_{\max}$选取每维宽度的 15%，并且在迭代过程中有如下更新关系：

$$x_{id}=\begin{cases}x_{\max}, & x_{id}>x_{\max}\\ -x_{\max}, & x_{id}<-x_{\max}\end{cases} \tag{20}$$

$$v_{id}=\begin{cases}v_{\max}, & v_{id}>v_{\max}\\ -v_{\max}, & v_{id}<-v_{\max}\end{cases} \tag{21}$$

4.2 粒子群算法的改进

基本粒子群算法具有易陷入局部极值点、进化后期收敛较慢等缺点[13]。在参数上做动态调整，但是若加速因子太大，粒子可能错过最优解，导致算法不收敛；若惯性权值下降过快，很容易陷入局部最优解，不能找到全局最优解，导致精度下降。综上考虑，做出如下改动：

1)动态调整惯性权值。使惯性权值随迭代次数的增加动态下降，即 ω 随着迭代次数 I 增加，由 $\omega_{\max}$动态减小至 $\omega_{\min}$，如下式所示：

$$\omega(I)=\omega_{\max}-\frac{I}{I_{\max}}\cdot e^{\left(\frac{I_{\max}-I}{I_{\max}}\right)}(\omega_{\max}-\omega_{\min}) \tag{22}$$

其中，I 为当前迭代次数，$I_{\max}$为最大迭代次数(1000 次)，$\omega_{\max}=0.9$，$\omega_{\min}=0.47$。

动态调整惯性权值大小，使粒子群能够避免过早陷入局部最优解，从而收敛到全局最优解。

2)均衡调整加速因子。使加速因子 c_1 随迭代次数 I 的增加，由 $c_{1\max}$减小至 $c_{1\min}$；使加速因子 c_2 随迭代次数 I 的增加，由 $c_{2\min}$增加至 $c_{2\max}$。如下式所示：

$$c_1(I)=c_{1\max}-\frac{I}{I_{\max}}\cdot e^{\left(\frac{I_{\max}-I}{I_{\max}}\right)}(c_{1\max}-c_{1\min}) \tag{23}$$

$$c_2(I)=c_{2\max}-\frac{I_{\max}-I}{I_{\max}}\cdot e^{\left(\frac{I}{I_{\max}}\right)}(c_{2\max}-c_{2\min}) \tag{24}$$

其中，$c_{1\max}=c_{2\max}=2$，$c_{1\min}=c_{2\min}=0.1$。

加速因子 c_1 的减小可以提高算法的收敛速度，c_2 的增加使粒子间的相互沟通性增强，通过均衡调整更易得到全局最优解。

4.3 优化 RBF 神经网络

MPSO 优化 RBF 神经网络的步骤如下：

1)采集样本数据，用 RAN 算法对样本聚类，得到隐含层节点个数。

2)用剪枝策略，删除相关性很小的节点，确定隐含层节点个数。

3)确定粒子编码结构，将基函数中心值 c_i、扩展宽度 σ_i 和输出权值 w_i 作为粒子参数编码，初始化粒子种群，粒子的速度和位置随机产生，迭代计数器 $I=1$。

4)对每个粒子，用式(25)计算适应度，比较其适应度与其经历最好位置的适应度，如果更好，更新 p_{id}。

均方根误差适应度函数：

$$RMSE=f=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y(i)-y_h(i))^2} \tag{25}$$

式中，N 表示样本容量，$y(i)$为网络安全态势真实值，$y_h(i)$为网络安全态势期望输出值。

5)对每个粒子，比较其适应度与群体经历最好位置的适应度，如果更好，更新 p_{gd}。

6)用式(16)－式(19)调整粒子的速度和位置。

7)重复步骤 4)－6),直到 I_{max}和满足精度要求为止。

8)将最终的 p_{gd}解码输出 RBF 神经网络结构参数,学习训练网络。

9)结束运算。

5 基于校园网的仿真实验及分析

5.1 样本数据预处理

本文采用校园网网络管理部门获取的黑客攻击数据,统一设置各类网络安全事件的威胁程度,则可以用当天安全事件告警统计值作为当天的网络安全态势值[14],选取其中的 120 天的告警数量统计值按图 4 方法分层计算网络安全态势值。

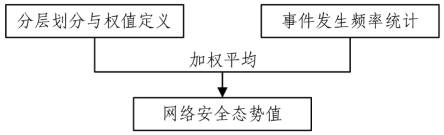

图 4 网络安全态势值的计算

(1)分析校园网网络管理部门提供的数据,可以得知一次网络攻击的周期为 3 天左右,所以神经网络输入向量维数$n=3$,输出向量维数 $h=1$,即利用前 3 天的网络安全态势值预测未来 1 天网络安全态势值。网络安全态势训练样本划分方法如表 1 所列。

表 1 网络安全态势训练样本划分

次数	三维输入向量	一维输出向量
1	x_1, x_2, x_3	x_4
2	x_2, x_3, x_4	x_5
…	…	…
100	$x_{100}, x_{101}, x_{102}$	x_{103}

(2)RBF 神经网络的训练样本数量 $N=100$。根据 RBF 神经网络特性,过多的训练会影响近期的网络安全态势值特点;过少的训练则会严重影响预测精度。所以取 100 作为训练样本数量,选取 20 个样本作为测试样本。图 5 示出校园网捕捉到的数据 2015 年 4 月 16 日到 2015 年 8 月 13 日的网络安全态势值归一化处理结果,归一化公式为:

$$\hat{x}=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{26}$$

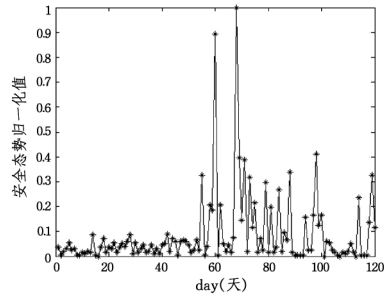

图 5 网络安全态势值的归一化

5.2 仿真性能分析

将归一化后的网络安全态势值样本进行 RAN 聚类,聚类结果为 5 类,确定隐含层节点数为 5,即构建 3-5-1 的 RBF 神经网络预测模型。

(1)为了验证 MPSO 算法对 RBF 神经网络的优化性能,分别给出 PSO 和 MPSO 优化 RBF 神经网络参数前后得到的预测结果,如图 7、图 8 所示。

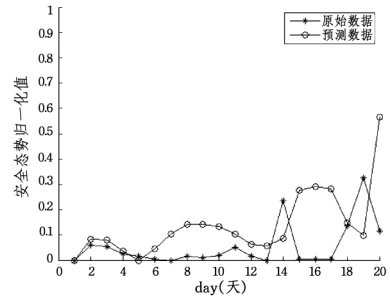

图 6 直接 RBF 预测结果

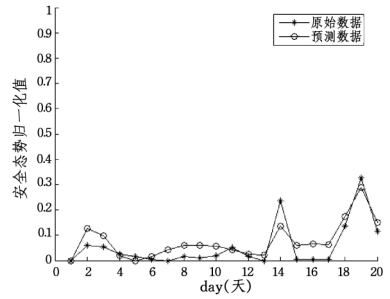

图 7 PSO 优化后的预测结果

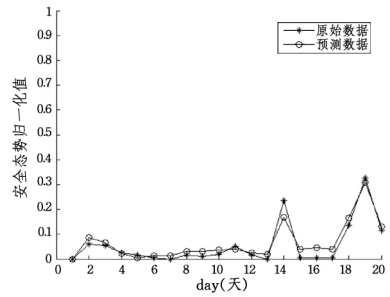

图 8 MPSO 优化后的预测结果

为了进一步体现 MPSO 优化性能的优越性,选取平均相对误差(MAPE)和均方根误差(RSME)两个性能指标进行定量比较,对比结果如表 2 所列。

平均相对误差指标:

$$MAPE=\frac{1}{N}\sum_{i=1}^{N}\frac{|y(i)-y_h(i)|}{y(i)} \tag{27}$$

其中,N 表示样本容量,$y(i)$为网络安全态势真实值,$y_h(i)$为网络安全态势期望输出值。均方根误差指标按式(25)计算。

表 2 PSO 优化 RBF 前后的定量对比

	直接 RBF	PSO 优化	MPSO 优化
MAPE	0.1133	0.0338	0.0186
RSME	0.1700	0.0440	0.0253

从表 2 中对比结果可知,MPSO 优化之后的平均相对误差和均方根误差都明显小于 PSO 优化前后的平均相对误差和均方根误差。定量对比结果可以证明 MPSO 优化 RBF 神经网络明显提高了网络安全态势预测精度。

(2)预测结果分析

从网络安全管理员角度出发,从图 8 中可以看出网络第 13－15 天和第 17－20 天受到黑客攻击,第 14 天和第 18－19 天的预测结果呈现出高威胁态势,提醒网络安全管理员须做好应对措施。值得关注的是,第 15－17 天真实值接近 0,而预测值并不为 0,呈现中威胁态势,提醒网络安全管理员威胁

状态并未解除；第 13－15 天很可能是黑客的试探性攻击，说明网络系统存在安全漏洞，因此要及时采取预防措施，避免受到黑客的再次攻击。

(3)为了验证本文预测模型的优越性，采用 K-均值 RBF 神经网络预测模型做了相同的实验，预测结果如图 9 所示。

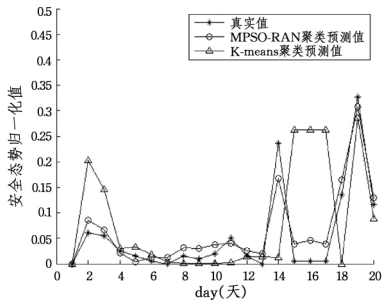

图 9　网络安全态势预测结果对比

为了进一步验证本文预测模型的优越性，同样选取 MAPE 和 RMSE 两个指标作定量对比，比较结果如表 3 所列。

表 3　神经网络结构与预测误差的比较

	本文预测模型	K-均值预测模型
隐节点数	5	9
MAPE	0.0186	0.0780
RSME	0.0253	0.1229

K-均值 RBF 神经网络的隐含层节点数根据经验法来确定，通过实验确定 K-均值 RBF 神经网络的隐含层节点数为 9 时预测结果较好。

表 3 的结果显示，本文的预测模型的隐含层节点数少于 K-均值预测模型的隐含层节点数，本文预测模型的平均相对误差和均方根误差均低于 K-均值预测模型。定量对比结果证明了本文预测模型的预测精度高于 K-均值预测模型的。

从图 9 和表 3 的结果可以看出，本文预测模型有着较好的预测能力，原因在于 RAN 聚类中的“剪枝”策略使本文预测模型的神经网络结构更为精简，K-均值 RBF 神经网络的结构较为冗余。

6　应用性分析

(1)可扩展性

本文模型可以结合中间件技术进行接口封装，在网络管理软件中调用接口，利用捕获的数据实现网络安全态势预测，给出态势图并分析得出威胁程度。

(2)实时性

本文模型是利用前 3 天的真实历史数据预测未来 1 天的网络安全发展态势，通过捕捉的真实数据更新模型所需数据，调用模型实现预测。本文利用 MATLAB 软件对模型进行仿真，程序运行时间很短，可以实现实时性与计算复杂度的平衡。

(3)预警性

通过本文模型的网络安全态势预测，可以为网络安全管理员预警网络安全状况，变过去的被动防御为主动应对，提醒网络安全管理员检测网络系统漏洞，对网络安全事件进行分析，并及时采取应对处理措施。

结束语　本文提出了一种基于 RAN-RBF 神经网络的网络安全态势预测模型。基于校园网网络环境，通过仿真实验验证了 MPSO 算法对 RBF 神经网络参数的优化性能，对比了 RAN-RBF 神经网络和 K-均值 RBF 神经网络预测模型，结果表明，本文预测模型预测结果较为精确，可以结合中间件技术实现与网络管理软件的同步配合；同时，为网络安全管理员提供了预测态势图，使其能提前采取预防和应对措施，变被动防御为主动应对。

下一步工作主要围绕以下方面展开：

1)大规模网络情况下的网络安全态势预测；

2)网络安全态势预测模型在军事中的应用；

3)网络安全态势感知的可视化研究。

参 考 文 献

[1] Bruce P. Software and network security[J]. Network Security, 2004(10):4-5

[2] 李硕，戴欣，周渝霞. 网络安全态势感知研究进展[J]. 计算机应用研究，2010，27(9)：3227-3232

[3] Endsley M R. Situation awareness in aviation systems[M]. Hillsdale, N J: Lawrence Erlbaum, 1999

[4] 王慧强，赖积保，朱亮，等. 网络态势感知系统研究综述[J]. 计算机科学，2006，33(10)：5-10

[5] Saha R K, Chang K C, Yin Xiao-yan. A Linear Predictive Bandwidth Conservation. Algorithm for Situation Awareness[EB/OL]. http://volgenau.gmu.edu/~kchang/publications/conference_pdf/CON_9_A_LINEAR.PDF

[6] Brynielsson J, Arnborg S. Bayesian Games for Threat Prediction and Situation Analysis[EB/OL]. http:// www.nada.ktk.se/~joel/IF04-1125.ps

[7] 谢丽霞，王亚超，于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版)，2013，53(12)：1750-1760

[8] Liu Xiao-wu, Wang Hui-qiang, Lai Ji-bo, et al. Multiclass Support Vector Machines Theory and Its Data Fusion Application in Nrtwork Security [J]. IEEE, 2007, 5(7): 6349-6352

[9] Ren W, Jiang X, Sun T. RBFNN-based prediction of networks security situation [J]. Computer Engineering and Applications, 2006, 42(31): 136-138

[10] 李方伟，郑波，朱江，等. 一种基于 AC-RBF 神经网络的网络安全态势预测方法[J]. 重庆邮电大学学报(自然科学版)，2014，26(5)：576-581

[11] 张辉，柴毅. 一种改进的 RBF 神经网络参数优化方法[J]. 计算机工程与应用，2012，48(20)：146-149

[12] Man Chun-tao, Wang Kun, Zhang Li-yong. A new training algorithm for RBF neural network based on PSO and simulation study[C]// Proc of IEEE Intl Conf on Computer Science and Information Engineering. 2009: 641-645

[13] 刘进军. RBF 神经网络的改进及其应用[D]. 兰州：兰州大学，2008

[14] Hassan A. IP traceback: a new Denial-of-Service dete-rent? [J]. IEEE Security & Privacy, 2003(3): 24-31