基于改进 BP 神经网络的 ATM 系统信息安全评估方法

吴志军，王璐，史荣

（中国民航大学 电子信息工程学院 智能信号与图像处理（天津市）重点实验室，天津 300300）

摘 要：根据 ATM 系统 3 层体系结构，针对 ATM 系统面临的信息安全问题，提出了应用人工神经网络（ANN）技术来评估 ATM 系统信息安全的思想；设计了基于改进的 BP ANN 的 ATM 系统 3 层神经网络评估模型。根据建立的 BP 神经网络模型，以 ATM 信息系统主要信息安全指标作为训练样本，通过学习和训练找出输入与输出之间的内在联系，用训练好的 BP 网络对 ATM 信息系统进行评估，并将评估结果与传统的评估方法进行比较。实验结果表明，提出的评估模型具有很强的自适应性和容错能力，适用于复杂的 ATM 信息系统的安全性评估。实验数据与实际 ATM 信息系统的运行状态相吻合。

关键词：人工神经网络；空中交通管理；安全评估；评估模型；BP 算法

中图分类号：TP309.1 **文献标识码**：A **文章编号**：1000-436X(2011)02-0150-09

Approach of information security assessment for ATM system based on improved BP model of artificial neural network

WU Zhi-jun, WANG Lu, SHI Rong

(Tianjin Key Laboratory for Advanced Signal Processing, School of Electronics & Information, Civil Aviation University of China, Tianjin 300300, China)

Abstract: ATM system was divided into 3 layers for the purpose of evaluating its information security. An evaluation model was proposed by using a 3-layer artificial neural network (ANN) based on improved BP model. The major information security indicators of ATM system were used as the training samples, which were adapted to find the intrinsic links between the input and output by learning and training process. An experiment was conducted by using the well-trained ANN network to evaluate the security of ATM system. The experimental results show that the proposed ANN evaluation model can indicate the practical running status of ATM system precisely. It is highly adaptive and fault-tolerant.

Key words: artificial neural network; air traffic management; security assessment; evaluation model; BP algorithm

1 引言

空中交通管理(ATM, air traffic management)信息系统是以航空通信（C）、导航（N）、监视（S）为基础，通过网络或数据链（data link）将自动化系统设备连接起来，实现地面管制人员对航空飞行器的可靠通信、精确导航和实时监视的保障航空交通安全运输的重要技术支持之一。

ATM 系统的信息安全对航空交通安全至关重要。一旦其出现问题可能导致的后果有 2 种：第 1

收稿日期：2010-02-03；**修回日期**：2010-05-15

基金项目：国家自然科学基金委员会与中国民用航空总局联合基金资助项目（60776808）；天津市应用基础及前沿技术研究计划基金资助项目（09JCYBJC00400）；2010 年度中央高校基本科研业务费中国民航大学专项（ZXH2010B004）

Foundation Items: The National Natural Science Foundation of China and Civil Aviation Administration of China (60776808); The Natural Science Foundation of Tianjin (09JCYBJC00400); The 2010 Basic Operational Outlays for the Research Activities of Centric University, Civil Aviation University of China (ZXH2010B004)

种是航空机场大面积航班延误或取消，造成旅客滞留机场；第 2 种则可能导致灾难性的航空事故发生。2 种结果都会造成巨大的经济损失或可能造成很大的社会影响。近年来，国际上航空机场由于信息安全事件导致大面积航班延误和旅客滞留现象时有发生。例如：2008 年 2 月英国希思罗机场处理旅客行李的计算机出现故障，导致数千名旅客的航班被延误或取消；2005 年 8 月全美多家机场的电脑系统都受到病毒的影响，受影响的机场有纽约、旧金山、迈阿密、洛杉矶、休斯顿、达拉斯及拉雷多，造成大量旅客滞留机场；2001 年日本成田国际机场由于受到“红色代码 II”蠕虫病毒的侵袭，日本航空公司的计算机售票和检票系统出现故障，造成数千人滞留机场达 2h；2000 年北京首都机场圣诞节前夕，电脑系统曾 5 度发生故障，造成电脑当机航班延误，超过 1 000 名旅客被迫滞留。

由于民航是涉及到国家领空安全、经济安全和社会安全的重点信息化行业。因此，对航空 ATM 信息系统的安全性评价是国家信息安全防御战略中的一项重要任务。通过信息安全评价可以科学地分析 ATM 信息系统的整体安全现状，做到防患未然。

2　相关工作

在 ATM 信息安全方面，世界上航空大国均制定了本国航空方面的信息安全保障计划。典型代表是美国联邦航空管理局（FAA，federal aviation administration）的 ISS（information system security）计划[1,2]。美国 MITRE 公司的 Marshall D. Abrams[3] 提出了美国 FAA 系统安全测试和评估的完整方案和具体方法。

人工神经网络（ANN，artificial neural network）在信息安全评估方面的研究，国际上已经取得了很多成果。特别是在类似于电力网络这样的国家重点信息保障系统，ANN 的应用十分普遍，最新的研究成果：Swarup K S[4]和 Corthis P B[5]提出了采用 ANN 进行系统安全评估的方法；Dong-Mei Zhao 和 Jin-Xing Liu 等[6]将模糊理论与小波（wavelet）神经网络结合起来，提出了一种基于模糊神经网络的信息安全评估方法；Yuansheng Huang 和 Chengfang Tian[7]将 BP 神经网络与专家系统（ES, experts system）结合起来，提出了一种实际评估信息系统中的风险因素及其权重（weight）的方法；申健[8]研究了网络安全进行综合评估的方法和应用，概述了采用 ANN 对网络安全评估的思路；赵冬梅和刘海峰等[9,10]研究了基于 BP 神经网络的信息安全风险评估方法，以及基于模糊神经网络的信息安全风险评估模型；刘海燕和王维锋等[11]研究了基于神经网络的信息系统安全性综合评估模型；刘燕[12]研究了基于模糊神经网络的信息安全风险评估的方法及实证；Dong-Mei Zhao 等[13]研究了基于神经网络的风险评估的方法；Yuansheng Huang 等[14]研究了基于 BP 神经网络的资产投资风险模糊综合评估模型和专家系统；于群和冯玲[15]提出了基于 BP 神经网络的网络安全评价的方法；任伟和蒋兴浩等提出了基于径向基 RBF(radial basis function)神经网络的网络安全态势预测方法[16]。但目前 ANN 在信息安全评估中的应用还很不成熟，特别是针对具体的应用环境时，在信息系统的信息安全评估中，目标属性间的关系绝大多数为非线性关系，一般的方法很难反映这种关系；许多问题的信息来源不完整，评价规则常常相互矛盾，甚至无条理可循；人们通常难以准确地描述方案各目标间的相互关系，更无法用定量关系式来表达它们之间的权重分配。因此，可能采取的方法有很大区别。

本文根据 ATM 系统层次化的体系结构，采用具有 3 层结构的 ANN 反向传播(BP, back propagation)模型与之对应，利用 ANN 的并行性、容错性和自学习的特点，以及 ANN 具有以任意精度逼近任何连续的非线性函数的功能[17]，来准确地反映 ATM 系统中的复杂关系，达到准确评估其信息安全性的目的。

3　基于 ANN BP 模型的 ATM 系统的信息安全评估方法

ATM 系统是一个结构和组成复杂的综合应用平台，而 ANN 是解决复杂关系的技术。为了能够更好地将 ANN 应用到 ATM 系统的信息安全评估中，必须找出它们之间的对应关系。

3.1　ATM 系统介绍

ATM 系统包括：空间导航和通信卫星系统、空中机载电子系统和地面空中交通管制(ATC, air traffic control)系统，以及平面通信网络和信息服务系统。其涉及与空中交通管理运行相关的通信、导航、监视、气象、情报、空中交通管制等方面的数据资料，以及相关硬件，如通信设备、通信介质、雷达导航设备、气象设备、航行情报设备等[18]。将 ATM

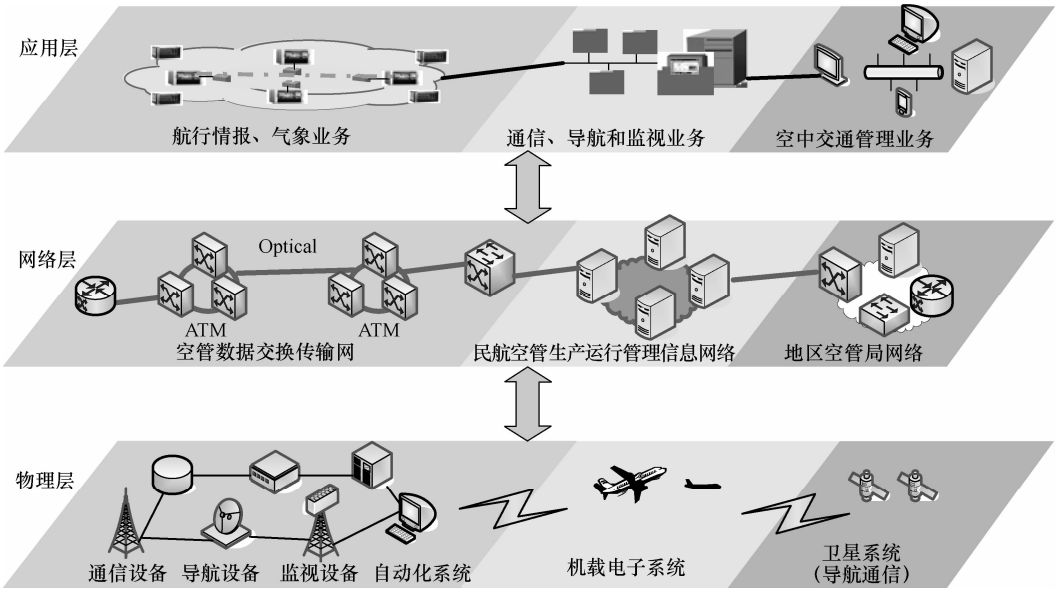


图 1　ATM 系统的 3 层结构

系统进行科学的分层处理，是进行 ATM 系统信息安全评估的前提。

本文将 ATM 系统的体系结构分为 3 个层次，如图 1 所示。

1) 最低层为新航行系统 CNS 层（物理层），包括 ATM 系统的所有基础设施：空管系统中地面通信、导航、监视和自动化设备系统，空中机载电子系统以及空间卫星系统。

2) 中间层为数据传输层（网络层），包括空管骨干 ATM 网络、民航空管生产运行管理信息网络和地区空管局网络。

3) 最高层为空管业务层（应用层），包括航行情报、气象业务，通信、导航和监视业务，以及空中交通管理 ATM 业务。

ATM 系统信息安全技术体系的设计根据 ATM 系统的 3 层结构，在每个层次设计相应的信息安全保障技术措施，包括设备冗余备份、数据链加密和认证、防火墙和入侵检测等。

3.2　ANN 的 BP 模型

ANN 的 BP 模型是一种多层前馈神经网络，其网络权值的调整采用的是后向传播方法。BP 网络模型通常分为输入层、隐含层和输出层，其中隐含层还可能不止一个。其网络模型如图 2 所示。

在图 2 所示的 3 层前馈网中，输入向量为 $\boldsymbol{X}=(x_1,x_2,\cdots,x_i,\cdots,x_n)^{\mathrm{T}}$，隐含层输出向量为 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_j,\cdots,y_m)^{\mathrm{T}}$，输出层输出向量为 $\boldsymbol{O}=(o_1,o_2,\cdots,o_k,\cdots,o_l)^{\mathrm{T}}$，期望输出向量为 $\boldsymbol{d}=(d_1,d_2,\cdots,d_k,\cdots,d_l)^{\mathrm{T}}$。输入层与隐含层之间的权值矩阵 $\boldsymbol{V}=(V_1,V_2,\cdots,V_j,\cdots,V_m)$，其中，列向量 $\boldsymbol{V}_j$ 为隐含层第 j 个神经元对应的权向量；隐含层到输出层之间的权值矩阵 $\boldsymbol{W}=(W_1,W_2,\cdots,W_k,\cdots,W_l)$，其中，列向量 $\boldsymbol{W}_k$ 为输出层第 k 个神经元对应的权向量。

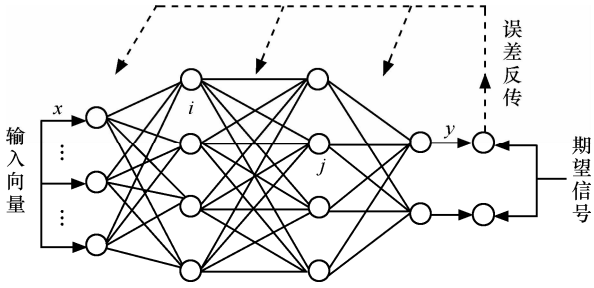


图 2　BP 网络模型

3.3　ATM 系统信息安全评估的 BP 神经网络模型

本文设计的 ATM 系统安全评估的 BP 神经网络模型如图 3 所示。

ATM 系统的 3 层结构与 BP 神经网络的对应关系如下。

1) CNS 层为物理层（即通信、导航和监视传感器设备），是为 ATM 系统提供各种信息的传感器系统。对应 BP 神经网络的输入层，输入向量：$\boldsymbol{X}=(x_1,x_2,\cdots,x_i,\cdots,x_n)^{\mathrm{T}}$。其中，$x_i$ 表示某种传感器设备的输出信号。

2) 网络层为传输层，是传输各种 ATM 信息的复杂网络系统，对应于 BP 神经网络的隐含层，输出向量：$\boldsymbol{Y}=(y_1,y_2,\cdots,y_j,\cdots,y_m)^{\mathrm{T}}$。其中，$y_j$ 表示

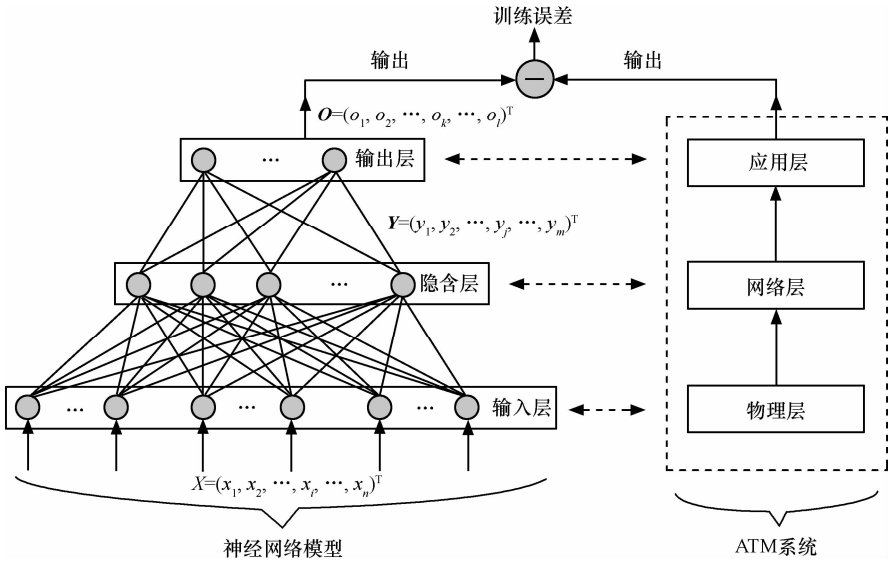


图 3　ATM 系统信息安全评估的 BP 神经网络模型

某种 ATM 信息。

3) 应用层为输出层，为 ATM 系统提供的最终业务数据信息，是 ATM 最终要得到和使用的信息，对应于 BP 神经网络的输出层，输出向量：$\boldsymbol{O}=(o_1,o_2,\cdots,o_k,\cdots,o_l)^{\mathrm{T}}$。其中，$o_k$ 表示某种经过处理后可以使用的 ATM 信息。

该 ANN 评估模型是一个多输入、单输出的系统。本文用已经训练好的 BP 网络取代传统的评估方法对空管信息系统进行评估，通过 ANN 给出评估结果。

3.3.1　网络误差与权值调整

当网络输入与期望输出不等时，存在输出误差 E：

$$E=\frac{1}{2}(d-O)^2=\frac{1}{2}\sum_{k=1}^{l}(d_k-o_k)^2 \tag{1}$$

将以上误差定义式展开至隐含层有

$$E=\frac{1}{2}\sum_{k=1}^{l}[d_k-f(\mathrm{net}_k)]^2=\frac{1}{2}\sum_{k=1}^{l}[d_k-f(\sum_{j=0}^{m}\omega_{jk}y_j)]^2 \tag{2}$$

将式(2)进一步展开至输入层有

$$\begin{aligned}E&=\frac{1}{2}\sum_{k=1}^{l}\{d_k-f[\sum_{j=0}^{m}\omega_{jk}f(\mathrm{net}_j)]\}^2\\&=\frac{1}{2}\sum_{k=1}^{l}\{d_k-f[\sum_{j=0}^{m}\omega_{jk}f(\sum_{i=0}^{n}v_{ij}x_i)]\}^2\end{aligned} \tag{3}$$

由式(3)可以看出，网络输入误差是各层权值 ω_{jk}、v_{ij} 的函数，因此调整权值可以改变误差 E。显然，调整权值的原则是使误差不断变小，因此应该使权值的调整量与误差的梯度下降成正比，即：

$$\begin{aligned}&\Delta\omega_{jk}=-\eta\frac{\partial E}{\partial\omega_{jk}},\Delta v_{ij}=-\eta\frac{\partial E}{\partial v_{ij}},\\&j=0,1,2,\cdots,m;\quad k=1,2,\cdots,l;\\&i=0,1,2,\cdots,n;\quad j=1,2,\cdots,m\end{aligned} \tag{4}$$

式(4)中负号表示梯度下降，常量 $\eta\in(0,1)$ 表示比例系数，在训练中反映了学习速率。可以看出 BP 算法属于 δ 学习规律类，即为误差的梯度下降算法。

3.3.2　BP 算法推导

下面推导 3 层 BP 算法权值调整的计算式。对于输出层有

$$\Delta\omega_{jk}=-\eta\frac{\partial E}{\partial\mathrm{net}_k}\frac{\partial\mathrm{net}_k}{\partial\omega_{jk}},\quad j=0,1,2,\cdots,m;\ k=1,2,\cdots,l \tag{5}$$

对于隐含层有

$$\Delta v_{ij}=-\eta\frac{\partial E}{\partial\mathrm{net}_j}\frac{\partial\mathrm{net}_j}{\partial v_{ij}},\quad i=0,1,2,\cdots,n;\ j=1,2,\cdots,m \tag{6}$$

下面对输出层和隐含层各定义一个误差信号令：$\delta_k^0=-\dfrac{\partial E}{\partial\mathrm{net}_k}$ 和 $\delta_j^y=-\dfrac{\partial E}{\partial\mathrm{net}_j}$，将第 1 个误差信号进行综合，则可以将表达式(5)改写成

$$\Delta\omega_{jk}=\eta\delta_k^0 y_j \tag{7}$$

同理，将第 1 个误差信号进行综合后，则可以将表达式(6)的权值调整式子改写成

$$\Delta v_{ij}=\eta\delta_j^y x_i \tag{8}$$

综上，只要计算出表达式(7)和式(8)中误差信号 δ_k^0 和 δ_j^y，权值调整的计算推导即可完成。对于输

出层， δ_k^0 可以展开为

$$\delta_k^0 = -\frac{\partial E}{\partial \text{net}_k} = -\frac{\partial E}{\partial o_k}\frac{\partial o_k}{\partial \text{net}_k} = -\frac{\partial E}{\partial o_k} f'(\text{net}_k) \quad (9)$$

对于隐含层 δ_j^y 可以展开为

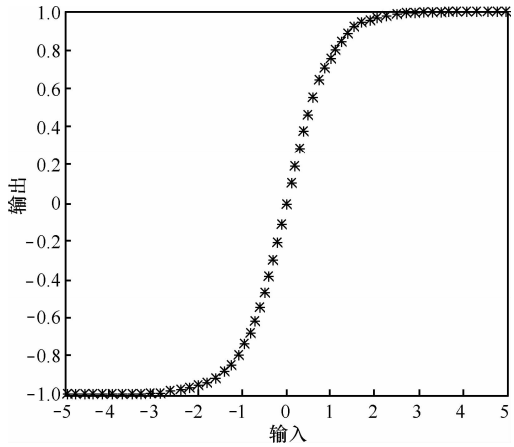
$$\delta_j^y = -\frac{\partial E}{\partial \text{net}_j} = -\frac{\partial E}{\partial y_j}\frac{\partial y_j}{\partial \text{net}_k} = -\frac{\partial E}{\partial y_j} f'(\text{net}_j) \quad (10)$$

以上是2个误差信号的推倒过程，将表式(9) 和式(10)代回到式(7)和式(8)中，得到 3 层网络的 BP 学习算法的最终权值调整公式为

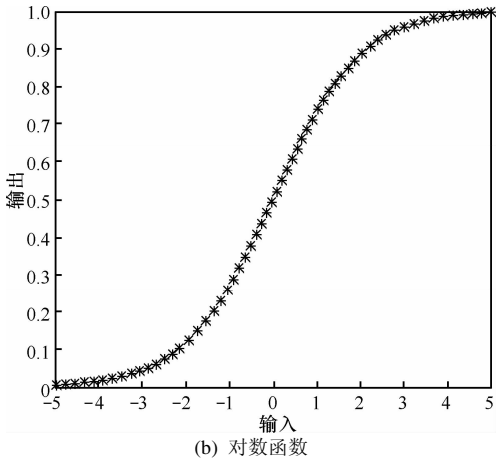
$$\Delta w_{ij} = \eta \delta_k^0 y_j = \eta (d_k - o_k) o_k (1 - o_k) y_j \quad (11)$$

$$\Delta v_{ij} = \eta \delta_j^y x_i = \eta (\sum_{k=1}^{l} \delta_k^0 \omega_{jk}) y_j (1 - y_j) x_i \quad (12)$$

BP算法要求BP网络的每个神经元的激活函数必须是处处可微的。BP 网络通常采用 Sigmoid 型的对数或正切特性函数和线性函数。其中，正切和对数函数曲线如图 4 所示。



(a) 正切函数



(b) 对数函数

图 4 正切、对数函数曲线

Sigmoid 型函数具有非线性放大系数功能，它可以把输入信号从负无穷大到正无穷大，变成从–1到 1 之间的输出。对较大的输入信号，放大系数较小;而对较小的信号，放大系数较大。所以采用 Sigmoid 激活函数可以处理和逼近非线性的输入/输出关系。BP 网络算法流程如图 5 所示。

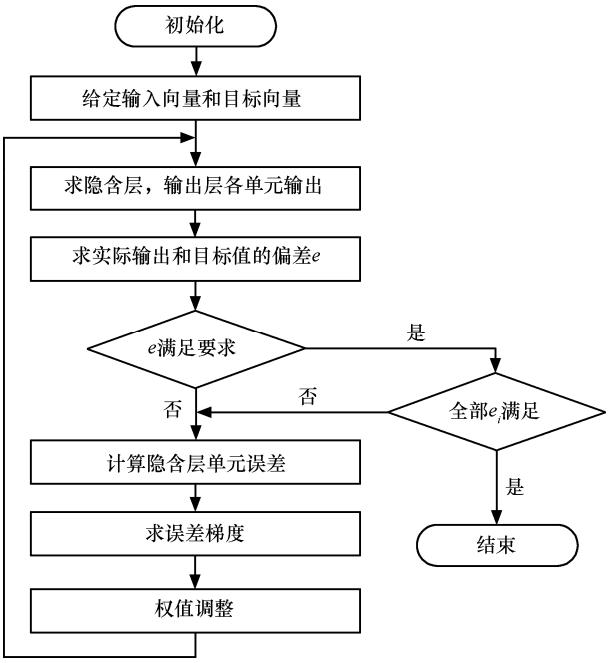


图 5 BP 网络算法流程

网络学习结束后，并不马上进行推断，还需用一定数量的典型实例对训练过程进行检验。若网络输出与实际输出之间的误差过大，则认为网络推断能力不强，需要调整网络参数，重新进行训练，直到学习误差与检验误差均符合要求为止。这样网络误差便有了良好的推断能力。

4 仿真及测试

应用 ATM 系统实际的运行数据对本文提出的评估方法进行仿真和测试。ATM 系统实际的运行数据来自于中国民航各地区空管单位的值班记录。该值班记录是依据《中国民用航空通信导航监视系统运行、维护规程》[19]中设计的记录表。本文将这些 ATM 系统设备的运行记录数据作为样本数据，在设计的 ANN BP 评估模型中进行学习。

ATM 系统信息安全保障的最终目标是保障 ATM 系统设备的正常工作，主要表现指标有：设备运行正常率和设备完好率。

1) 设备运行正常率。

设备运行正常率的计算方法为

$$\text{设备运行正常率}=\frac{\text{计划运行时间（小时数）}-\text{不正常运行时间（小时数）}}{\text{计划运行时间（小时数）}}\times 100\% \tag{13}$$

其中，计划运行时间是指波道或台站（系统）按上级计划应该保证正常运行的总时间（小时数），以每日规定工作的时间累积计算，累积期限分月、季和年度 3 种；不正常运行时间是指波道或台站 (系统)工作中断或不能提供正常保障的时间(小时数)。

2) 设备完好率。

设备完好率的计算方法为

$$\text{设备完好率}=\frac{\text{设备总台数}-\text{故障设备总台数}}{\text{设备总台数}}\times 100\% \tag{14}$$

其中，设备总台数为服役期内的设备总台数；故障设备总台数为服役期内的故障设备总台数。

ATM 系统设备运行正常率和完好率必须达到的要求如表 1 所示[19]。

表 1　　设备运行正常率和完好率要求

设备名称	设备正常率	设备完好率
无线通信设备	99.98%	90%
有线通信设备	99.97%	90%
导航设备	99.98%	90%
监视设备	99.98%	90%
航管自动化设备	99.99%	90%

根据《中国民用航空通信导航监视系统运行、维护规程》[19]中设备的分类，本文选取了目前 ATM 系统中常用的设备作为评价的对象；并根据国家《信息安全技术—信息系统安全等级保护定级指南》[20]的要求，本文对 ATM 系统中保护对象的安全等级进行了划分。

1) ATM 系统中基础运行样本数据的选取。

ATM 系统中基础运行样本数据的选取来自以下 ATM 系统中具体的设备。

① 无线通信设备：甚小口径终端（VSAT, very small aperture terminal）卫星系统和甚高频（VHF, very high frequency）数据链系统。

② 有线通信设备：内话系统。

③ 导航设备：多普勒全向信标（DVOR, doppler vhf omni-direction range）系统、盲降（ILS, instrument landing system）系统、测距机（DME, distance measurement equipment），GPS 系统。

④ 监视设备：二次雷达（SSR, secondary surveillance radar）系统和自动相关系统（ADS, automatic dependent system）。

⑤ 航管自动化设备：飞行计划、飞行情报和监控系统。

上述设备是 ATM 系统设备的典型代表，能够全面反映出 ATM 系统设备的安全状态。从这些设备系统的运行记录数据提取的 ATM 系统信息安全评价指标能全面准确地反映出 ATM 系统的状况与技术质量特征，并且评价结果能反映 ATM 系统的合理性、完好性及安全可靠性。

因此，本文基于以上的条件，从通信、导航、监视和自动化 4 个方面选取了主要的 12 个影响因素作为评价指标，构成了 ATM 系统评价指标体系。

2) 安全等级的划分。

根据国家《信息安全技术—信息系统安全等级保护定级指南》[20]的要求，本文将 ATM 系统的信息安全评估结果分为 5 个等级，分别代表：很安全、比较安全、安全、危险和很危险。其中，每个等级表示的范围代表网络的实际输出值，如表 2 所示。

表 2　　安全等级划分

安全等级	网络输出值
A	0.85~1.00
B	0.70~0.85
C	0.60~0.70
D	0.45~0.60
E	0.00~0.45

在上述工作的基础上，本文对设计的基于 BP 神经网络的 ATM 系统安全性进行了模拟仿真，并采用 ATM 系统实际运行的数据进行了测试。

4.1　仿真

根据设计的 ATM 系统安全评估的 BP 神经网络，由于 ATM 系统中包含很多的子系统，以及广域网和局域网，所以设计的网络中隐含层的内容十分复杂。对于 ANN 网络的设计，隐含层中神经元的个数很大程度上影响网络的测试性能。

针对实际的 ATM 系统，考虑从 ATM 系统中选取的 12 个实际设备作为评价因素。确定设计的网络输入层与隐含层，以及隐含层与输出层之间的传

递函数采用对数函数。考虑到网络的规格和学习时间，选用 Trainlm 函数对函数进行训练。其参数设置如表 3 所示。

表 3 训练参数设置

参数名称	参数值
最大训练步数 epochs	1 000
最小误差 goal	0.01
show	20
其他参数	默认值

其中，最小误差 0.01 是根据《中国民用航空通信导航监视系统运行、维护规程》[19]中设备正常率和设备完好性的最小误差要求来设定的。

训练样本来自 12 组 ATM 系统的实际运行数据。采用大量的 ATM 系统实际运行数据，经过反复实验，结果表明隐含层中神经元的个数为 25 时，网络的性能最佳。因此，选取 12 组数据作为训练样本（如表 4 所示）。

为了验证提出的评价网络模型的性能，本文在 MATLAB 仿真环境中，对网络进行了初始化，利用函数 Trainlm 对网络进行训练。设目标值为 0.01，当训练到 3 步之后，训练结果为 0.001 052 69，网络误差达到了设定的误差要求。训练结束后，网络训练收敛的效果如图 6 所示。

为了进一步检验训练后网络的性能，本文对训练结果作进一步仿真分析。利用 postreg 函数可以对网络仿真的输出结果 A 和目标输出 T 作非线性回归分析，并得到两者的相关系数，可以得知网络对目标数据的逼近效果，从而可以作为网络训练结果优劣的判别依据。取拟合度 R=0.999 时，非线性回归分析结果如图 7 所示。

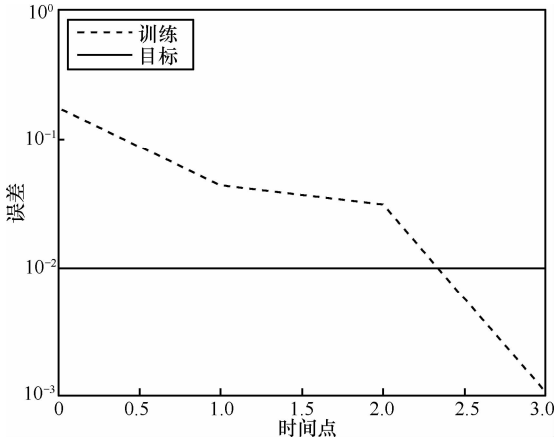


图 6 网络训练收敛

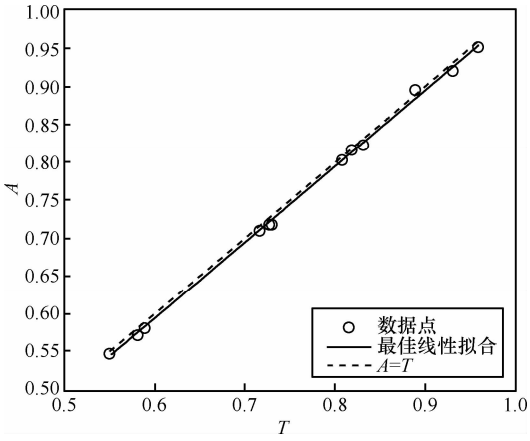


图 7 网络非线性回归

本文利用网络的仿真输出矢量（ATM 系统设备的实际运行效果）和目标矢量（ATM 系统设备的信息安全评价指标）之间的线性回归分析，并把得到的目标矢量对网络输出的相关系数作为网络性能的重要评价标志。当网络性能处于良好状态并达到一定程度时，网络模拟值应该和网络实际输出值相等，即处于坐标轴第一象限的对角线上。此时，截距等

表 4 训练样本

评估指标	卫星系统	VHF 系统	内话系统	DVOR 系统	ILS 系统	DME 系统	SSR 系统	ADS 系统	GPS 系统	飞行计划	飞行情报	监控系统
1	1.0	1.0	1.0	0.98	1.0	0.9	0.96	1.0	1.0	1.0	0.98	1.0
2	0.84	0.82	0.81	0.85	0.86	0.74	0.80	0.84	0.86	0.81	0.82	0.84
3	0.76	0.72	0.72	0.69	0.79	0.56	0.68	0.76	0.74	0.75	0.70	0.71
4	0.61	0.59	0.51	0.53	0.70	0.39	0.64	0.68	0.65	0.60	0.46	0.52
5	0.96	0.94	0.90	0.89	0.90	0.90	0.92	0.94	0.92	0.94	0.92	0.91
6	0.82	0.80	0.80	0.79	0.84	0.80	0.81	0.82	0.81	0.79	0.82	0.86
7	0.74	0.76	0.71	0.72	0.76	0.70	0.72	0.74	0.71	0.69	0.65	0.69
8	0.59	0.50	0.51	0.54	0.70	0.41	0.58	0.60	0.64	0.50	0.44	0.48
9	0.93	0.91	0.96	1.00	0.91	0.89	0.94	0.92	0.93	0.92	1.00	0.94
10	0.87	0.85	0.85	0.87	0.83	0.71	0.80	0.82	0.83	0.82	0.86	0.85
11	0.79	0.77	0.74	0.75	0.72	0.63	0.71	0.76	0.71	0.72	0.70	0.71
12	0.67	0.66	0.52	0.59	0.68	0.44	0.62	0.58	0.59	0.58	0.50	0.44

表 5　　测试样本

评估指标	卫星系统	VHF 系统	内话系统	DVOR 系统	ILS 系统	DME 系统	SSR 系统	ADS 系统	GPS 系统	飞行计划	飞行情报	监控系统
1	0.95	0.96	0.95	0.91	0.92	1.0	0.91	0.89	0.89	0.85	0.94	0.98
2	0.84	0.94	0.83	0.80	0.81	0.76	0.82	0.81	0.80	0.77	0.80	0.81
3	0.77	0.78	0.71	0.73	0.71	0.58	0.71	0.74	0.74	0.74	0.79	0.77
4	0.67	0.69	0.52	0.56	0.68	0.43	0.60	0.64	0.61	0.56	0.51	0.48
5	0.72	0.86	0.65	0.69	0.54	0.484	0.77	0.58	0.59	0.68	0.60	0.64

于 0；斜率等于 1；拟合度等于 1。在实际应用中，通常取拟合度 $R>0.80$ 即可。最后，得到 BP 神经网络模拟值与实际输出之间的非线性回归方程为

$$A=0.998T+(-0.004\,18)(R=0.999) \quad (15)$$

训练结果表明：提出的 ATM 系统信息安全评价的 ANN BP 模型可以达到《中国民用航空通信导航监视系统运行、维护规程》[19]中提出的误差指标规定；提出的网络性能满足 ATM 系统复杂组成和环境的要求。

4.2　测试

本文对提出的 ATM 系统信息安全评价的 ANN BP 模型采用实际 ATM 系统运行中发生的信息安全事件记录数据进行了测试。其思路是把具体的信息安全事件采用事件相关进行数据采样，制作成测试样本，通过数据回放的方式对本文提出的评价模型进行测试。

本文根据 ATM 系统的实际运行状态，选取了 5 种不同情况下的测试样本数据，如表 5 所示。

本文利用上面训练好的网络，采用表 5 中的测试样本数据，对提出的网络性能进行了测试。测试结果如表 6 所示。

表 6　　测试结果

评估指标	期望输出	实际输出	相对误差	输出等级
1	0.898	0.884	1.57%	A
2	0.801	0.797	0.50%	B
3	0.675	0.665	1.49%	C
4	0.590	0.589	0.16%	D
5	0.436	0.429	1.61%	E
平均	0.680	0.672	1.06%	

从测试结果可以看出，5 种情况符合之前对 ATM 系统的信息安全等级的设定。表现在 ATM 系统设备的正常率和完好率方面，如果统计时仅考虑当前安全事件的影响，而其余时间均为正常的情况，则可以计算出由于信息安全事件的出现，导致 ATM 系统设备的正常率和完好率方面的变化。

测试结果表明：本文提出的网络具有一定的可行性，网络具有性能稳定、准确度高、误差小等优点，并且测试结果与实际情况相吻合，具有一定的实用性。

5　结束语

本文利用将 ANN BP 模型应用到 ATM 系统的信息安全评估中，提出了基于 ANN BP 的 ATM 系统信息安全评估模型，解决了 ATM 系统信息安全保障措施之间复杂的交联关系，并采用仿真和测试 2 种方法对提出的模型进行了验证。仿真结果表明该模型设计符合 ATM 系统的非线性特性，能够很好地反映 ATM 系统的安全运行状态。测试结果表明该模型误差达到了《中国民用航空通信导航监视系统运行、维护规程》[19]中设备正常率和设备完好性的误差要求。利用本文提出的评价模型，可以对 ATM 系统面临的信息安全威胁和发生的信息安全事件进行分析和研究，指导 ATM 系统信息安全保障系统的设计和实施。最终目的是及时揭示 ATM 系统中可能存在的安全隐患，封堵存在的系统漏洞，杜绝信息安全事件发生，很好地保障空中交通运输的安全高效运行。

本文在今后的研究中将采用 ANN 的径向基 RBF 模型进行 ATM 系统的信息安全评估，并将其实验结果与 BP 模型的结果进行比较，对误差和评估准确性等方面进行分析，寻找 ATM 系统的信息安全评估的最佳方法。

参考文献：

[1] Information Systems Security (ISS). Federal Aviation Administration (FAA), Information Technology (IT)[R]. Research and Development (R&D) Workshop, 2008.

[2] Federal Plan for Cyber Security and Information Assurance Research and Development[R]. Interagency Working Group on Cyber Security and Information Assurance Subcommittee on Infrastructure and Sub-

committee on Networking and Information Technology Research and Development, 2006.

[3] MARSHALL D. Abrams. FAA System Security Testing and Evaluation[R]. MITRE Technical Report, 2003.

[4] SAEH I S, KHAIRUDDIN A. Static security assessment using artificial neural network[A]. Power and Energy Conference IEEE 2nd International[C]. 2008.1172-1178.

[5] SWARUP K S, CORTHIS P B. ANN approach assesses system security[J]. Computer Applications in Power, 2002,15(3):32-38.

[6] ZHAO D M, LIU J X, ZHANG Z H. Method of risk evaluation of information security based on neural networks[A]. Machine Learning and Cybernetics, 2009 International Conference on Volume 2[C]. 2009.1127-1132.

[7] HUANG Y S, TIAN C F, FANG W. Fuzzy comprehensive evaluation mode on the investment risk of real estate based on BP neural network and expert system[A]. E-Business and Information System Security, 2009. EBISS '09[C]. 2009.1-5.

[8] 申健. 网络安全综合评估方法的研究及应用[D]. 兰州大学, 2005.
SHEN J. Investigate and Apply the Mode of Assess the Secu-Rity of Computer Networks[D]. Lanzhou University, 2005.

[9] 赵冬梅, 刘海峰, 刘晨光. 基于 BP 神经网络的信息安全风险评估[J]. 计算机工程与应用, 2007, 43(1): 139-141.
ZHAO D M, LIU H F, LIU C G. Risk assessment of information security based on BP neural network[J]. Computer Engineering and Applications, 2007,43(1):139-141.

[10] 赵冬梅, 刘海峰, 张军鹏. 基于模糊神经网络的信息安全风险评估模型[J]. 计算机工程与应用, 2009, 45(17):116-118.
ZHAO D M, LIU H F, ZHANG J P. Mode of risk assessment of information security based on fuzzy neural network[J]. Computer Engineering and Applications, 2009,45(17):116-118.

[11] 刘海燕，王维锋，蔡红柳.一个基于神经网络的信息系统安全性综合评估模型[J]. 计算机工程与科学，2008, 30(11):16-18.
LIU H Y, WANG W F, CAI H L. A comprehensive security evaluation model of information systems based on artificial neural networks[J]. Computer Engineering and Science, 2008,30(11): 16-18.

[12] 刘燕. 基于模糊神经网络的信息安全风险评估研究及实证[J]. 中国电子商务, 2009, (9): 64.
LIU Y. Research and demonstration the risk assessment of information security based on fuzzy neural network[J]. Chinese Electronic Commerce, 2009, (9): 64.

[13] ZHAO D M, LIU J X, ZHANG Z H. Method of risk evaluation of information security based on neural networks[A]. Machine Learning and Cybernetics, 2009 International Conference[C]. 2009. 1127-1132.

[14] HUANG Y S, TIAN C F, FANG W. Fuzzy compreh-ensive evaluation mode on the investment risk of real estate based on BP neural network and expert system[A]. International Conference on E-Business and Information System Security 2009 (EBISS '09)[C]. 2009. 1-5.

[15] 于群, 冯玲. 基于 BP 神经网络的网络安全评价方法研究[J]. 计算机工程与设计, 2008,29(8):1963-1966.
YU Q, FENG L. Attribute-weighted clustering algorithm based on rough set[J]. Computer Engineering and Design, 2008,29(8): 1963-1966

[16] 任伟, 蒋兴浩, 孙锬锋. 基于RBF神经网络的网络安全态势预测方法[J]. 计算机工程与应用, 2006. 42(31): 136-144.
REN W, JIANG X H, SUN T F. RBFNN-based prediction of networks security situation[J]. Computer Engineering and Applications, 2006,42(31):136-144

[17] 杨行峻, 郑君里. 人工神经网络[M]. 北京: 高等教育出版社, 1992.
YANG X J, ZHENG J L. Artificial Neural Network[M]. Beijing: Higher Education Press, 1992.

[18] 中国民航局空中交通管理局. 空中交通管理介绍[EB/OL]. http://www.atmb.org.cn/kgjj.asp.2010.
Air Traffic Management Bureau of China. Introduction to air traffic management[EB/OL]. http://www. atmb.org.cn/kgjj.asp.2010.

[19] 中国民航局空管局. 中国民用航空通信导航监视系统运行、维护规程[S]. 2004.
Air Traffic Management Bureau. Civil Aviation Administration of China, Communication, Navigation, and Surveillance System Operation, Maintenance Procedures of China Civil Aviation[S]. 2004.

[20] 全国信息安全标准化技术委员会. 信息安全技术—信息系统安全等级保护定级指南[S]. 2007.
National Information Security Standardization Technical Committee. Information Security Technology Protection Guide of Information System Security Classification Level[S]. 2007.

作者简介：

吴志军（1965-），男，新疆库尔勒人，中国民航大学教授、博士生导师，主要研究方向为网络与信息安全。

王璐（1985-），男，河南洛阳人，中国民航大学硕士生，主要研究方向为网络与信息安全。

史荣（1984-），女，河北邯郸人，中国民航大学助教，主要研究方向为网络与信息安全。