doi:10.3969/j.issn.1673-9833.2015.03.015

基于粗糙集神经网络的网络安全态势评估方法

姜旭炜，文志诚，邓勇杰

（湖南工业大学 计算机与通信学院，湖南 株洲 412007）

摘 要：为克服多源数据融合中存在信息高维、冗余和噪音等大量不确定性因素给网络安全态势评估带来的复杂影响，提出一种基于粗糙集神经网络的网络安全态势评估方法。该方法既利用粗糙集理论在机械学习、处理冗余信息和特征提取等方面的能力，又结合神经网络处理噪音和任意逼近能力构造出由指标层、离散层、规则层、决策层组成的态势评估模型，并与BP神经网络方法进行对比研究。仿真实验结果表明，所提方法偏差较少，更能客观、准确地分析网络安全状况。

关键词：粗糙集理论；粗糙集神经网络；态势评估

中图分类号：TP393 **文献标志码**：A **文章编号**：1673-9833(2015)03-0076-07

Network Security Situation Evaluation Based on Rough Set and Neural Network

Jiang Xuwei，Wen Zhicheng，Deng Yongjie

（School of Computer and Communication，Hunan University of Technology，Zhuzhou Hunan 412007，China）

Abstract：In order to overcome the complex influences of uncertain factors of information high dimension, redundancy and noise etc. in the multi-source data fusion on the network security situation evaluation, presents a network security situation assessment method based on rough set and neural network. This method uses rough set theory capabilities in machine learning, redundant information processing and feature extraction and combines with the neural network ability of dealing with noise and arbitrary approximation to construct the situation assessing model composed of index layer, discrete layer, rule layer and decision layer, and compares and studies it with BP neural network method. The simulation experiment shows that the method has less deviation and can analyze network security situation more objectively and accurately.

Keywords：rough set theory；rough set and neural network；situation assessment

1 背景知识

随着信息技术的不断发展，各种网络应用不断普及，人们对网络的信任度和依赖度不断提高；与此同时，网络安全问题日益严峻，安全漏洞、病毒入侵和黑客（DoS/DDoS）攻击等等网络安全事故也随之不断地增加；加之，Internet规模不断扩大，其复杂性和不确定性也随之增加，因此对于安全分析的难度不断地加大。传统的网络防御设备和技术无法对现有的网络安全状况进行有效、快捷地分析和防御。海量的网管信息非但不能更好地管理，反而增加了网络管理员的负担。在这种情况下，对网络面临的安全风险进行态势感知、分析，以及采取相应的防御手段成为目前网络安全研究的热门话题。

态势感知（situation awareness，SA）源自于航天飞行的人因研究，此后被广泛地应用于军事战

收稿日期：2015-03-19

作者简介：姜旭炜（1988-），男，湖南武冈人，湖南工业大学硕士生，主要研究方向为网络安全态势感知，E-mail：402342284@qq.com

通信作者：文志诚（1972-），男，湖南东安人，湖南工业大学副教授，博士，主要从事软件工程与网络安全方面的教学与研究，E-mail：zcwen@mail.shu.edu.cn

场、核反应控制系统、空中交通监管以及医疗应急调度等领域。1999 年，T. Bass[1]首次提出了网络态势感知（cyberspace situation awareness，CSA）的概念，并指出“基于融合的网络态势感知”将成为网络管理的发展方向。态势强调环境、动态性以及实体之间的联系，是一种状态、一种趋势、一个整体和全局的概念，任何单一的情况或状态都不能称之为态势。在实际网络环境中，由于网络的动态性和复杂性，传统的网络分析方法不能解决网络的实际问题，因此态势感知技术应运而生，决策者能够利用态势感知工具掌握全局变化规律，做出正确的决策。

网络安全态势感知（network security situation awareness，NSSA）是指在现实的网络环境中，在一定时间和空间内，对能引起网络安全态势发生变化的外界因素进行提取、评估和对未来的变化趋势进行预测。网络安全态势感知能实时地检测网络面临的安全风险，综合考虑各方面的影响因素，生成局部或全局的安全态势图，全面地动态分析网络安全状况，为提高网络安全性提供了可靠依据。

网络安全态势评估是网络安全态势感知技术中的核心与重点内容。目前，国内外提出了许多种关于网络安全态势评估与感知方法，主要包括证据理论[2]、D-S 理论（dempster-shafer）[3]、灰色系统理论、粗糙集理论（rough set theory）[4-5]、神经网络[6]、模糊逻辑[7]、熵理论[8]和专家系统等。然而在网络安全态势评估中存在大量的不确定性、不完备的因素（如信息维数大，指标冗余和噪音等）的影响，导致评估过程较为繁琐，评估结果的误差较大。运用单独的传统网络态势评估方法有很多，但是它们有 2 个共同的缺陷：1）在大规模网络环境中，管理者面临庞大且复杂的数据，影响因素较多，导致对态势要素提取不全面，冗余数据过多及计算复杂度过大会导致维数爆炸；2）先验知识不足和态势指标过于庞大。

本文提出一种基于粗糙集神经网络的网络安全态势评估方法，本方法以粗糙集和人工神经网络在数据融合方面为基础[9-10]，利用粗糙集理论的属性约简能力对攻击要素进行属性约简，求出最简指标规则来确定隐含层的数目，构造出由指标层、离散层、规则层（前件与后件）、决策层组成的神经网络评估模型。此方法是在保持整个网络处理能力的前提下，通过粗糙集理论处理冗余信息，遴选态势因子，精简评估规则集，从而优化神经网络中隐含神经元、精简神经网络的拓扑结构，减少冗余节点，提高神经网络的泛化能力。在对网络安全态势进行综合评估中，减少大量不可靠主观因素的影响，帮助网管人员更好地了解网络安全状况。

2　粗糙集理论

粗糙集理论（rough set theory）是由波兰数学家 Z. Pawlak 教授提出的一种新型处理模糊和不确定性知识的数学工具[11]，其主要思想是以不可分辨关系为基础，通过引入上近似集和下近似集来描述一个集合；其在保持信息系统分类能力不变的前提下，进行知识约简，最终导出问题分类的决策或分类规则。

粗糙集理论相比其他处理不精确问题的理论有着明显的优势，主要表现在没有任何数据集合之外的先验信息条件下，粗糙集能够比较客观地处理不精确问题，从海量历史数据信息中发现隐含知识，揭示潜在规律。但粗糙集理论不包含处理原始数据的机制，通常需要采用其他互补性的理论与之结合才能达到理想的效果，如神经网络、模糊数学等。

2.1　基本概念

设 $s=(U, R, V, f)$为一个知识表达系统，其中：论域 $U=\{x_1, x_2, x_3, \dots, x_n\}$为非空有限集合；$R$ 为非空属性集合，R 包括条件属性 C 和结果属性 D，即 $C\cup D=R$；V 为属性 $a\in R$ 的值域；$f: U\times R\rightarrow V$ 为一个单射信息函数，指定论域中任一个元素的属性值。

定义 1　设 $P\subseteq R$ 且非空，P 中所有等价关系的交集称为 P 上的一种不分辨（不可分）关系，记作 $[x]_{IND(P)}=\{(x,y)\in U\cdot U:\forall a\in P, a(x)=a(y)\}$或$[x]_{IND(P)}=\bigcap_{R\in P}[x]_R$。

定义 2　设 $s=(U, R, V, f)$为一知识表达系统，且 $B\subseteq R$，$X\subseteq U$，则 X 关于 B 的上近似集为$\underline{B}X=\{xU|[x]_{IND(B)}\subseteq X\}$；下近似集为$\bar{B}X=\{xU|[x]_{IND(B)}\cup X\neq\phi\}$。

定义 3　在一个知识表达系统中，假如给定$\underline{B}X$和$\bar{B}X$，那么正区域为 $POS_B(X)=\underline{B}X$，反区域$NEG_B(X)=U-\bar{B}X$，边界区域为 $BND_B(X)=\bar{B}X-\underline{B}X$。

定义 4　设 $X\subseteq U$ 且 $x\in U$，决策属性 D 对条件属性 C 的依赖度定义为$\gamma(C,D)=\dfrac{|POS_c(D)|}{|U|}$。

定义 5　设 $X\subseteq U$ 且 $x\in U$，集合 X 的粗糙隶属函数定义为$\mu_X^R(x)=\dfrac{|X\cap[x]_R|}{|[x]_R|}$。

其中：R 是不分明关系；$|\bullet|$表示集合的元素个数。

2.2　属性约简

在一个知识表达系统 $s=(U, A, V, f)$中，根据定义 1，若 $a\in P$ 且 $IND(P-\{a\})=IND(P)$，则表示在 P 中属性 a 是不必要的，否则表示在 P 中 a 是必要的。若$\exists a\in P$ 都是必要的，则表示 P 独立，否则表示 P 是依赖的。

求取约简属性需要满足以下条件：

设 $Q \subset P$，若 Q 是独立的且 $IND(Q)=IND(P)$，则表示 Q 是 P 的一个约简，称为 $RED(P)$，在实际情况下，存在多个约简，所有约简的交集构成的核，记作 $CORE(P)=\cup RED(P)$。

3 网络安全态势评估指标的处理

3.1 指标体系

在网络安全态势评估中，评价指标体系的择取是评价研究的关键，它会直接影响整个评价结果的精度；评价指标体系应尽可能地反映网络安全态势的基本特征及基本状况。本文将网络安全态势指标划分为4个独立的一级指标：脆弱性、容灾性、威胁性和稳定性。每个一级指标又包含若干个二级指标，具体如下：

1）与脆弱性有关的二级指标。有漏洞数目、安全设备数目、网络拓扑、关键设备的服务种类及开放端口数目等；

2）与容灾性有关的二级指标。有带宽、安全设备数目、子网内只要服务器支持的并发线程数、关键设备访问主流安全网络的频率等；

3）与威胁性有关的二级指标。有报警数目、带宽使用率、安全事件历史发生率、数据流入量、IP分布等；

4）与稳定性有关的二级指标。有关键设备平均存活时间、子网流量变化率、子网平均无故障时间、子网内存活关键设备数目等。

3.2 态势因子的筛选

在实际的大规模网络环境下，由于网络的巨型性、复杂性，在网络安全态势感知过程中，存在着众多的相互冲突、不完备、非确定的复杂观测指标，有些指标对态势感知起着关键性的作用，有些指标对态势感知的影响却十分微弱，指标之间也可能存在冗余。因此，态势指标的筛选直接影响到态势感知的效果和效率。

如何既能保持网络安全态势评估指标的全面性与代表性，又能保证指标体系的精简，成为构建评估指标体系的关键问题。粗糙集理论是一种数据分析理论，能够有效地利用属性重要度量对网络安全态势因子进行遴选[12]。

定义6 设 $S=(U,C\cup D)$是一个网络安全决策信息系统，$C=\{a_1, a_2, \cdots, a_n\}$为条件属性，将其做为网络安全态势评估指标，$D$ 是决策属性，可作为筛选结果。若 a_i 是离散型属性，则求其系统参数的重要性：$SGF(a, C, D)=\gamma(C, D)-\gamma(C-\{a\}, D)$，其中$\gamma(C-\{a\}, D)$为在 C 属性中缺少属性 a 后，条件属性对决策属性的重要程度。

利用粗糙集理论中重要性定义，根据定义4和定义6计算出态势因子对网络安全态势的重要性：

$$SGF(a_i, C, D)=\frac{|POS_C(D)|-|POS_{C-\{a_i\}}|}{|U|},$$

把态势因子作为决策信息表的条件属性，删除冗余和不重要的指标，从而优化网络安全态势评估指标。

4 基于粗糙集神经网络的评估模型

4.1 数据的预处理

有限离散化数据是粗糙集分析的基础，而在工程领域中原始数据包含了大量的连续数据。因此，在利用粗糙集约简之前，必须先对数据进行离散归一化处理，其目的是为了尽可能减少海量数据中有用信息的丢失，同时降低系统空间维数，减少指标的种类。目前主要采用的离散方法有等区间划分法、S法、L法、等频率划分发等，但不管是哪种离散方法，都必须保证离散后数据的维数尽可能少、每个属性尽可能少地拥有属性值的种类和尽量减少数据信息的丢失。本文采用了ROSETTA[13]中的Boolean Reasoning算法和Equal Frequency Binning算法进行离散化。

4.2 规则提取

在整个知识表达系统中，并非所有属性是同等重要的，有大量的属性可能存在冗余，因此进行属性的约简至关重要。然而条件属性 C 的最小约简属性并非只有一个，可能存在多个属性集，而要求取最小属性集已证明是一个NP问题；在实际的工程领域中，只需要求解出具有实际用途的最小约简属性集即可；规则过多或过少直接影响到神经网络评估结果的精确性。

本文选取文献[13]中基于粗糙集理论框架的表格逻辑数据分析工具包ROSETTA来得到最简规则，其决策规则提取步骤如下：

1）数据补齐。由于入侵监测数据中可能存在大量的不完整或损坏的数据，需要进行不完整数据的移除。通过利用ROSETTA自身的移除不完整数据功能模块对数据进行整理。

2）数据的离散化。由于粗糙集理论存在只能处理离散化数据的局限性，而实际大网络环境下的监测数据大多属于数值型数据，因此需要使用ROSETTA中的Boolean Reasoning算法和Equal Frequency Binning算法合理充分地对监测数据进行离散化处理。

3）属性约简。在原始数据中可能存在着大量的冗余属性，它们对评估结果起着微乎其微的作用。通

过 ROSETTA 中遗传算法对条件属性进行约简，以剔除不必要的属性，减少数据的采集。

4）规则生成。在步骤 3）的基础上，利用等价关系形成规则。但由于约简结果不是唯一的，产生的规则也是多个属性对应的简化规则。

5）规则约简。对约简决策表所得到的简化规则中每一条条件属性不一定都是必要的，因此需要属性约简来简化规则中不必要的条件属性值，从而得到最简规则集。

4.3　评估模型

基于粗糙集神经网络的网络安全态势评估方法的主要思想是：第一，对收集的入侵检测数据进行预处理，获取有用的数据集，从而得到原始信息决策表。第二，对原始数据集进行离散化处理和归一化处理，并将原始数据分为 2 组，一组为训练样本数据，另一组为测试样本数据。第三，利用粗糙集理论的属性约简能力得到拥有完备原始样本特征的最小决策规则集，从而利用最简指标规则来确定神经网络的规则层数。第四，通过训练数据对粗糙集神经网络进行训练，获得最小规则集对应的各项评估指标数，优化评估系统的输入结点数；最后，确定评估模型的网络结构、相关隶属度函数以及输入输出推理规则，并将测试样本数据输入评估系统，经过粗糙集和专业知识组成的规则推理确定当前网络安全运行状况。

粗糙集神经网络评估模型可以理解成基于神经网络的粗糙集推理系统。本文采用粗糙集模糊神经网络设计[14−16]，根据 4.2 节中提取的最简指标规则确定的神经网络来确定人工神经网络的隐含层层数和隐含层节点数目。设粗糙集神经网络的各神经元的连接权值、输入和输出分别表示为：W_i^i, I_i^i, O_i^i，其中 i 为层标，j 为层参数。其模型如图 1。

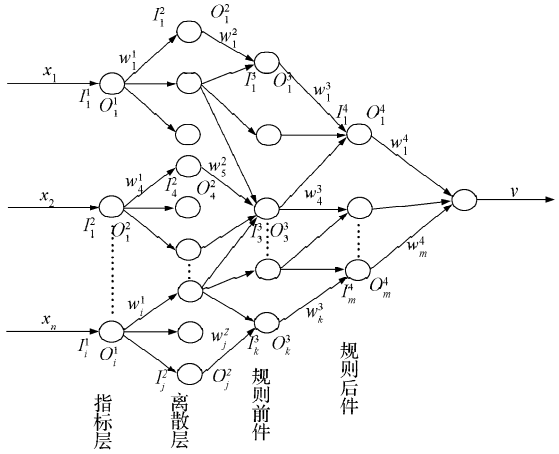

图1　粗糙集神经网络评估模型

Fig. 1　The rough set neural network evaluation model

第 1 层是输入层（或称为指标层），表示为网络安全态势评估系统的输入变量 $\boldsymbol{X}=\{x_1, x_2, \cdots, x_i\}^{\mathrm{T}}$，$x_i(i=1, 2, \cdots, n)$，即干扰网络安全性能的指标；结点个数是决策信息表中核属性的个数；该层神经元的连接权值为 $W_i^1=1$，其 $I_i^1=O_i^1$，$i=1, 2, \cdots, N$。

第 2 层是离散化层，分别将 n 个输入量 $x_1, x_2, \cdots, x_n$ 依照粗糙集理论的某种不可分辨关系进行等区间划分，将输入数据 x_i 离散为 r_i 个取值为[0, 1]的不同值，该结点数为离散属性值的个数。本文把高斯函数作为隶属度函数，该结点的连接权值 $W_i^2=1$，输入为 $I_i^2=O_i^1$，输出为：

$$O_i^2=u_i^j=\exp\left[-\left(\frac{x_i-c_{ij}}{\delta_{ij}}\right)^2\right], \tag{1}$$

式中：c_{ij}, δ_{ij} 分别是变量 x_j 离散化到 $r_i(j=1, 2, \cdots, r_i)$档的平均值和方差；

c_{ij}, δ_{ij} 分别为隶属度函数的中心和带宽；

$1 \leqslant i \leqslant N$，$1 \leqslant j \leqslant J$。

第 3 层是规则前件层，规则层依照粗糙集理论的规则约简能力进行规则提取，规则层神经元与第 2, 4 层神经元相连接，该神经元由前件和后件组成。该层是由第 3 层与第 2 层连接表示 1 条复杂的规则前件，每 1 个结点代表 1 条规则，且该层的结点数是最简决策表中规则的个数，构建一个不完全连接神经元，其连接权值为 1。该结点层输出为规则适应度 T_k：

$$T_k=\min(u_1^{j_1}, u_2^{j_2}, \cdots, u_N^{j_k}) \text{或} T_k=u_1^{j_1}\cdot u_2^{j_2}, \cdots, u_N^{j_k},$$

$$I_k^3=O_{j_1}^2\cdot O_{j_2}^2\cdot\cdots\cdot O_{j_N}^2, \tag{2}$$

$$O_k^3=I_k^3=u_1^{j_1}\cdot u_2^{j_2}, \cdots, u_N^{j_k}=\prod_{N=1}^{k}u_N^{j_k}。 \tag{3}$$

式（2）~（3）中：$u_1^{j_1}\cdot u_2^{j_2}, \cdots, u_N^{j_k}$ 表示第 2 层结点的输出值；$j_1, j_2, \cdots, j_k$ 为规则代号；k 为规则数。

第 4 层是规则后件层，该层由第 3 层与第 4 层中若干个神经元相连接。该规则层的结点数是最简决策表中决策属性的数目；由于最小决策指标有若干个，单独的决策指标不能很好地反映当前的网络安全状况，需要综合考虑决策指标。则归一化处理后，每个神经元的输入、输出为：

$$O_m^4=I_m^4=O_k^3\Big/\sum_{s=1}^{M}O_s^3。 \tag{4}$$

第 5 层是决策层，表示网络安全态势评估的综合评估值，该神经元的结点数为 1，神经元的输入、输出为：

$$I_l^5=\sum_{m=1}^{M}w_{lm}^5\cdot O_m^4,$$

$$v=O_l^5=I_l^5。 \tag{5}$$

式中 w_{lm}^5 为第 4, 5 层之间的连接权值。

4.4 参数的调整

本文利用BP算法[17]的空间搜索能力，逐步迭代，更新评估模型中第4~5层的连接权值，隶属度函数的中心和带宽，从而缩短学习训练时间。通过BP算法反复修正网络权值，从而得到期望的评估结果。定义其误差代价函数为：

$$E=\frac{1}{2}\sum_{r=1}^{R}(Y-y)^2, \tag{6}$$

式中：R 代表学习样本数；

Y 代表系统期望输出值；

y 代表网络实际输出值。

则有

$$\frac{\partial E}{\partial w_{lm}^5}=\frac{\partial E}{\partial y}\frac{\partial y}{\partial w_{lm}^5}=-(Y-y)O_m^4。 \tag{7}$$

参数调整步骤如下：

1）网络系数初始化。

2）输入已知学习样本，通过梯度下降BP算法迭代设计粗糙集神经网络结构（包括各层神经元的连接权值w_{lm}^5，隶属度函数的中心c_{ij}和带宽δ_{ij}），从而计算各层的神经元输出。

3）调整各参数，并从最后一层反向计算各权值的总误差影响，进一步对网络结构各连接权值及参数进行修改。

4）重复步骤2）~3），直到整个粗糙集神经网络收敛为止。其中第4，5层的连接权值为：

$$w_{lm}^5(k+1)=w_{lm}^5(k)-\eta\frac{\partial E}{\partial w_{lm}^5}。 \tag{8}$$

隶属度函数的中心c_{ij}为:

$$c_{ij}(k+1)=c_{ij}(k)-\eta\frac{\partial E}{\partial c_{ij}}。 \tag{9}$$

带宽δ_{ij}为：

$$\delta_{ij}(k+1)=\delta_{ij}(k)-\eta\frac{\partial E}{\partial \delta_{ij}}。 \tag{10}$$

以上各式中η>0，为学习率。

5 实验分析

5.1 实验数据

为了测验本文所提出的基于粗糙集神经网络的网络安全态势评估方法的合理性与正确性，笔者借用Matlab 7.0来进行仿真实验；以DARPA1999入侵检测数据集为基础，取监控数据100个样本作为实验数据。首先对原始数据进行归一化处理，其归一化公式为$x_i'=\frac{x_i-x_{\min}}{x_{\max}-x_{\min}}$，处理之后得到[0,1]的值；然后把100个实验数据分为90个训练样本集和10个测试样本集，进行本次的网络安全态势评估实验。

5.2 评估结果分析

由于考虑到文章篇幅问题，本文以威胁性指标为例，运用文献[6]提供的基于BP神经网络的网络安全态势评估方法和本文基于粗糙集神经网络的网络安全态势评估方法进行对比研究，分析粗糙集神经网络方法的优越性。

1）经过粗糙集理论的分析，分别筛选出9条二级指标：a表示报警数目；b表示带宽使用率；c表示安全事件发生率；d表示关键设备的服务分布；e表示数据流入量；f表示流入量的增长率；g表示不同协议数据包的分布；h表示不同大小数据包的分布；j表示流入网络数据包源IP分布。

设决策信息表中的条件属性为态势指标；决策属性分为：1表示高；2表示中；3表示低。经过粗糙集理论的约简和求核，得到表1所示最简决策信息表。

表1 最简决策信息表

Table 1 The simplest decision information table

规则	条件									决策 D
	a	b	c	d	e	f	g	h	j	
1	−	−	3	−	2	−	−	2	1	3
2	1	−	−	2	−	1	−	3	1	1
3	3	2	1	2	−	−	3	3	−	3
4	−	−	−	2	3	−	−	1	3	2
5	−	2	2	1	3	1	−	−	2	2
6	3	−	1	−	−	2	2	−	2	3
7	1	2	3	−	2	3	1	−	−	1
8	−	3	−	−	−	1	−	3	−	3
9	2	−	1	−	−	2	3	1	2	2
10	1	−	−	3	−	−	−	3	−	1

从而确定粗糙集神经网络的输入点为9个，离散层结点为27个，规则前件结点为10个，规则后件结点为3个，输出结点为1个，从而构建好粗糙集神经网络评估模型。通过Matlab 7.0的仿真实验，得到如表2所示测试样本的实际输出和期望输出的比较结果。

表2 粗糙集神经评估结果

Table 2 Rough set neural assessment results

样本编号	实际输出	期望输出	相对误差%	威胁等级
91	0.881	0.868	1.56	高
92	0.834	0.817	2.07	高
93	0.855	0.834	2.50	高
94	0.832	0.816	1.96	高
95	0.537	0.531	1.28	中
96	0.334	0.330	1.39	低
97	0.342	0.335	2.00	低
98	0.868	0.879	1.27	高
99	0.200	0.205	2.50	低
100	0.417	0.407	2.39	中

2）根据文献[6]中提供的基于BP神经网络评估方

法对本文提供的检测数据进行评估，该神经网络由9个输入结点、4个隐层结点、1个输出结点组成，其评估结果如表3所示。

表3　BP神经网络评估结果

Table 3　BP neural network evaluation results

样本编号	实际输出	期望输出	相对误差/%	威胁等级
91	0.886	0.868	2.03	高
92	0.845	0.817	3.31	高
93	0.887	0.834	5.98	高
94	0.863	0.816	7.59	高
95	0.560	0.531	5.19	中
96	0.365	0.330	9.59	低
97	0.354	0.335	5.67	低
98	0.850	0.879	3.29	高
99	0.202	0.205	5.16	低
100	0.389	0.407	4.42	中

对比表2和表3所示实验结果可知，基于粗糙集神经网络的网络安全态势评估方法比BP神经网络方法更加明显，而且采用粗糙集神经网络进行评估，使得测试样本的相对误差<2.50%，明显比BP神经网络评估方法的相对误差<9.59%要小，其主要在于运用粗糙集理论对评估指标和数据的冗余，高维处理，而且粗糙集神经网络的隐含层结点数客观性高，从而大大减少了不利因素对评估的影响。

综上所述：以粗糙集神经网络为基础的网络安全态势评估模型与专家期望结果非常接近，完全可以适应网络安全态势的综合评估。

6　结语

本文构建的基于粗糙集神经网络的网络安全态势评估模型，综合了粗糙集理论在处理不完备、不精确知识的能力和神经网络在数值上任意逼近的特点，既减少了冗余信息和噪音数据的不利影响、约简了网络安全态势评估指标、避免了因先验知识不足而产生的误差，又减少了粗糙集神经元的输入层结点数和隐含规则层结点数，从而优化了粗糙集神经网络的拓扑结构，缩短了态势评估的时间，同时也提高了模型的正确率。为今后的网络安全态势评估工作提供了一种可行的方法。

但粗糙集理论中约简求核[18-19]是一个NP难题，能否求解出符合实际用途的最简决策规则直接影响到评估精度，此问题还需要今后的进一步研究。

参考文献：

[1] Bass T. Intrusion Detection Systems and Multisensor Data Fusion：Creating Cyberspace Situational Awareness[J]. Communications of the ACM，2000，43(4)：99-105.

[2] Digioia G，Foglietta C，Oliva G，et al. Aware Online Interdependency Modeling via Evidence Theory[J]. International Journal of Critical Infrastructures，2013，9(1)：74-92.

[3] 刘效武，王慧强，吕宏武，等. 基于融合的网络安全量化感知[J]. 吉林大学学报：工学版，2013，43(6)：1650-1657.
Liu Xiaowu，Wang Huiqiang，Yu Hongwu，et al. Quantitative Awareness of Network Security Situation Based on Fusion[J]. Journal of Jilin University：Engineering and Technology Edition，2013，43(6)：1650-1657

[4] Huang C C，Tseng T L B，Fan Y N，et al. Alternative Rule Induction Methods Based on Incremental Object Using Rough Set Theory[J]. Applied Soft Computing，2013，13(1)：372-389.

[5] Jan G B，Bazan-Socha S，Buregwa-Czuma S，et al. Classifiers Based on Data Sets and Domain Knowledge：A Rough Set Approach[J]. Intelligent Systems Reference Library，2013，43(2)：93-136.

[6] 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.
Xie Lixia，Wang Yachao，Yu Jinbo. Network Security Situation Awareness Based on Neural Networks[J]. Journal of Tsinghua University：Natural Science Edition，2013，53(12)：1750-1760.

[7] 王　宏，龚正虎. 一种基于信息熵的关键流量矩阵发现算法[J]. 软件学报，2009，20(5)：1377-1383.
Wang Hong，Gong Zhenghu. Algorithm Based on Entropy for Finding Critical Traffic Matrices[J]. Journal of Software，2009，20(5)：1377-1383.

[8] 卓　莹，龚春叶，龚正虎. 网络传输态势感知的研究与实现[J]. 通信学报，2010，31(9)：54-63.
Zhuo Ying，Gong Chunye，Gong Zhenghu. Research and Implementation of Network Transmission Situation Awareness[J]. Journal on Communications，2010，31(9)：54-63.

[9] 王　刚，张志禹. 粗糙集结合BP神经网络的数据融合方法研究[J]. 西安理工大学学报，2006，22(3)，311-314.
Wang Gang，Zhang Zhiyu. Rough Set Method Combined with BP Neural Network Data Fusion[J]. Journal of Xi'an University of Technology，2006，22(3)，311-314.

[10] 盖伟麟，辛　丹，王　璐，等. 态势感知中的数据融合和决策方法综述[J]. 计算机工程，2014，40(5)，21-26.
Gai Weilin，Xin Dan，Wang Lu，et al. Data Fusion and Decision Methods of Situation Awareness[J]. Computer Engineering，2014，40(5)，21-26.

[11] Pawlak Z. Rough Sets and Intelligent Data Analysis[J]. Information Sciences，2002，147(1)：1-12.

[12] 卓　莹，何　明，龚正虎. 网络态势评估的粗糙集分析

模型[J]. 计算机工程与科学，2012，34(3)，1-5.
Zhuo Ying，He Ming，Gong Zhenghu. The Rough Set Model of Network Situation Assessment[J]. Computer Engineering and Science，2012，34(3)，1-5.
[13] Kaufmann K W，Lemmon G H，De Luca S L，et al. Practically Userful：What the ROSETTA Protein Modeling Suite Can Do for You[J]. Biochemistry，2010，49(14)：2987-2998.
[14] 巩 徽，冯 欣. 一种粗集模糊神经网络模型的研究及应用[J]. 计算机工程与科学，2010，32(6)：132-134.
Gong Hui，Feng Xin. Research and Application of a Kind of Rough Fuzzy Neural Network Model[J]. Computer Engineering and Science，2010，32(6)：132-134.
[15] 李千目，戚 湧，张 宏，等. 基于粗糙集神经网络的网络故障诊断新方法[J]. 计算机研究与发展，2004，41(10)，1696-1702.
Li Qianmu，Qi Yong，Zhang Hong，et al. A New Network Fault Diagnosis Method Based on RS-Neural Network[J]. Journal of Computer Research and Development，2004，41(10)，1696-1702.
[16] 郝丽娜，王 伟，吴光宇，等. 粗糙集-神经网络故障诊断方法研究[J]. 东北大学学报：自然科学版，2003，24(3)：252-255.
Hao Li'na，Wang Wei，Wu Guangyu，et al. Research on Rough Set-Neural Network Fault Diagnosis Method[J]. Journal of North Eastern University：Natural Science，2003，24(3)：252-255.
[18] 徐 权，倪世宏，张 鹏. 基于粗糙集的专家系统知识库约简研究[J]. 计算机测量与控制，2012，20(5)：1333-1335.
Xu Quan，Ni Shihong，Zhang Peng. A Research on Knowledge Base Reduction of Expert System Based on Rough Set[J]. Computer Measurement & Control，2012，20(5)：1333-1335.
[19] 王 杨，闫德勤，张凤梅. 基于粗糙集和决策树的增量式规则约简算法[J]. 计算机工程与应用，2007，43(1)：170-172.
Wang Yang，Yan Deqin，Zhang Fengmei. Rough Set and Decision Tree Based Incremental Rule Reduction Algorithm [J]. Computer Engineering and Application，2007，43(1)：170-172.
[17] 周开利，康耀红. 神经网络模型及其MATLAB仿真程序设计[M]. 北京：清华大学出版社，2005：1-254.
Zhou Kaili，Kang Yaohong. Neural Network Model and MATLAB Simulation Programming[M]. Beijing：Tsinghua University Press，2005：1-254.

（责任编辑：申 剑）

（上接第75页）

Li Chenggui，Zhao Liguo. Realization of Wireless Monitoring Network Based on LEACH Protocol for Human Physiological Parameters[J]. Automation and Instrumentation，2013 (6)：24-27.
[15] 徐合龙，纪金水. 基于FDMA点对多点通信在无线传感器网络中的设计与实现[J]. 西北民族大学学报：自然科学版，2010，31 (1)：41-48.
Xu Helong，Ji Jinshui. Dot to Multi-Dots Communication in Wireless Sensor Networks Design and Implementation Based on FDMA[J]. Journal of Northwest University for Nationalities：Natural Science，2010，31 (1)：41-48.
[16] 黄家露，杨 方，张衍林. 基于CC2430的温室无线传感器节点设计与应用[J]. 华中农业大学学报，2013，32(5)：119-123.
Huang Jialu，Yang Fang，Zhang Yanlin. Design and Application of Wireless Sensor Nodes Based on CC2430 in Greenhouses[J]. Journal of Huazhong Agricultural University，2013，32(5)：119-123.

（责任编辑：邓 彬）