文章编号：1000-3673（2011）04-0176-07 中图分类号：TP 393 文献标志码：A 学科代码：470·4054

基于支持向量机和粒子群算法的信息网络安全态势复合预测模型

高昆仑[1]，刘建明[2]，徐茹枝[3]，王宇飞[3]，李怡康[3]

（1. 中国电力科学研究院 信息与通信研究所，北京市 海淀区 100192；2. 国网信息通信有限公司，北京市 宣武区 100761；3. 华北电力大学 控制与计算机工程学院，北京市 昌平区 102206）

A Hybrid Security Situation Prediction Model for Information Network Based on Support Vector Machine and Particle Swarm Optimization

GAO Kunlun[1], Liu Jianming[2], XU Ruzhi[3], WANG Yufei[3], LI Yikang[3]

(1. Information & Communication Department of China Electric Power Research Institute, Hardian District, Beijing 100192, China;
2. State Grid Information & Telecommunication Company Limited, Xuanwu District, Beijing 100761, China;
3. School of Control and Computer Engineering, North China Electric Power University, Changping District, Beijing 102206, China)

ABSTRACT: A security situation prediction model for information network based on support vector machine (SVM) and particle swarm optimization (PSO) is proposed. By use of sliding window, in the proposed model a continuous time series that is partially linearly dependent is constructed by security situation values sampled from original discrete time monitoring points, and taking the time series as the sample set of security situation data the SVM is trained to generate a prediction model. During the training of SVM, the PSO algorithm is used to search for the optimal training parameters of SVM to reduce the blindness in the selection of SVM parameters and improve precision of prediction. Through the experiments based on on-site installation and monitoring data of a lot of power enterprise information networks, the effectiveness of the proposed security situation prediction model is verified.

KEY WORDS: security situation of information network; regression prediction; support vector machine; particle swarm optimization; time series

摘要：提出一种基于支持向量机和粒子群算法的网络态势复合预测模型。模型使用滑动窗口方法将各原始离散时间监测点的安全态势值构造成部分线性相关的连续时间序列，以其作为安全态势数据样本集对支持向量机加以训练，生成预测模型。在支持向量机训练过程中，利用粒子群算法搜寻支持向量机的最优训练参数，以降低支持向量机参数选择的盲目性，提高预测精度。最后通过基于大量电力企业信息网络现场安全监测数据的实验，验证了复合预测模型的有效性。

关键词：信息网络安全态势；回归预测；支持向量机；粒子群算法；时间序列

基金项目：国家电网公司科技项目(B11-09-109)。

0 引言

随着电力系统信息化水平的提高与信息安全工作的推进，电力企业信息安全防护已经从单一威胁(如恶意代码、网络攻击)防护阶段进入到综合安全管理阶段，在全面部署各类安全防护产品基础上，电力企业越来越关注安全态势的感知以及安全事件的预测与预防。

网络安全态势是指由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势。特别注意，态势是一种状态、趋势，是一个整体和全局的概念，任何单一的情况或状态均不能称为态势[1]。当前普遍采用网络态势值来评价当前网络的安全态势。网络态势值的计算原理是将当前时间监测点信息网络的各种运行特征参数监测值依照特定算法通过综合计算得到，其中较典型的网络态势值计算算法有层次分析法[2-3]、贝叶斯网络算法[4]等。由网络态势值的计算原理可以看出，网络态势值可以在很大程度上反映网络当前的安全状况。

若根据历史上各已知时间监测点的网络态势值，能够推算出未来时间监测点的网络态势值，则可以依据预测的网络态势值发布未来电力信息网络安全告警。由此可知，如何设计预测模型来精确

预测未来网络态势值，就成为各电力企业信息网络安全告警的重要环节，所以对预测模型的研究具有很强的理论和现实意义。

预测模型的工作原理是将原始目标问题(离散时间监测点的态势值预测问题)抽象成一个连续时间序列上的回归预测问题[5]，并利用人工智能算法构造预测模型求解该回归预测问题。目前预测网络态势值的代表性方法有以下几种：文献[6]使用 BP 神经网络(back propagation neural network，BPNN)构造预测模型；文献[7]使用径向基函数神经网络(radial basis function neural network，RBFNN)作为预测模型；文献[8]使用马尔可夫链结合灰色理论构造预测模型；文献[9]使用支持向量机(support vector machine，SVM)作为预测模型。从上述文献可以看出，当前网络态势值预测模型的研究重点在于如何利用人工智能算法构造出高精度的预测模型。但上述代表性方法均存在各自问题：经过近几年研究发现，文献[6-7]采用的神经网络方法本身具有参数选取困难、易陷于局部极小点、网络收敛速度慢和容易过拟合等难于克服的问题[10]；文献[8]中马尔可夫链结合灰色理论方法的缺陷在于建立模型困难，需要大量数学公式推导；支持向量机虽然与神经网络相比具有收敛速度快、抗过拟合能力强等优点，但文献[9]单独使用 SVM 做预测模型也存在 SVM 训练过程参数选取盲目性的问题。综上所述，预测模型的设计关键在于选择恰当的人工智能算法并对所选人工智能算法做参数优化，以提高预测模型准确度。

针对预测模型设计的关键问题，提出一种由支持向量机和粒子群优化算法(particle swarm optimization，PSO)组成的复合预测模型。复合预测模型利用滑动窗口方式生成安全态势样本集，通过粒子群算法优化支持向量机训练参数的方式完成对样本集的训练，以得到最终预测模型，并使用最终预测模型对未来时间点的信息网络态势值做准确预测和告警发布。

1　复合预测模型算法原理

1.1　支持向量机原理

支持向量机是 Vapnik 和 Cortes 于 1995 年提出的一种基于统计学习理论的机器学习方法，现已成为近年来机器学习研究的一项重大成果[11]。其核心思想是：对于 n 维欧氏空间 $\mathbf{R}^n$ 上分类问题(或回归问题)，通过寻找一个 $\mathbf{R}^n$ 上的实值函数 $g(\boldsymbol{x})$，以利用决策函数 $f(\boldsymbol{x})=\mathrm{sgn}[g(\boldsymbol{x})]$ 来推断任意输入 $\boldsymbol{x}$ 所对应的输出值 $\boldsymbol{y}$[12]。

确定 $g(\boldsymbol{x})$的方法是构造一个与原始分类问题(或回归问题)对偶的非线性规划问题并求解，以此确定函数 $g(\boldsymbol{x})$。求解非线性规划问题时需要将原欧氏空间 $\mathbf{R}^n$ 中的变量 $\boldsymbol{x}$ 通过变换 $\boldsymbol{\Phi}$ 映射到 Hilbert 空间，如式(1)，从而得到 Hilbert 空间中的线性规划问题并求解。

$$\mathbf{R}^n \to \text{Hilbert},\quad \boldsymbol{x} \to \boldsymbol{x}=\boldsymbol{\Phi}(\boldsymbol{x}) \tag{1}$$

而支持向量机中核函数 $K(\boldsymbol{x},\ \boldsymbol{x}')$的作用正是通过内积变换实现 $\boldsymbol{\Phi}$ 变换[13]，即

$$K(\boldsymbol{x},\boldsymbol{x}')=\boldsymbol{\Phi}(\boldsymbol{x})\cdot\boldsymbol{\Phi}(\boldsymbol{x}') \tag{2}$$

此时原 $\mathbf{R}^n$ 空间上的决策函数变成式(3)。

$$f(\boldsymbol{x})=\mathrm{sgn}[\boldsymbol{\omega}^{\mathrm{T}}\cdot\boldsymbol{\Phi}(\boldsymbol{x})+\boldsymbol{b}] \tag{3}$$

式中 $\boldsymbol{\omega}$、$\boldsymbol{b}$ 分别为权重和阈值。

1.2　粒子群算法原理

粒子群算法是一种具有很强全局寻优能力的群智能优化算法[14]。其核心思想是在 n 维解空间初始化一个含有若干个粒子的种群，种群中每个粒子代表一个 n 维可行解并具备各自的速度 $\boldsymbol{v}$($\boldsymbol{v}$ 是 n 维向量)，并构造一个种群适应度函数 F，同时设定适应度函数 F 的最小值 ε ($\varepsilon\geq 0$)及种群最大迭代次数 T，其中 ε 也是适应度函数 F 的收敛判别条件[15]。粒子在解空间中根据自身飞行经验和群体飞行经验调整自己的飞行轨迹，向最优点靠拢。由于粒子在飞行过程中同时受种群历史最优位置 $\boldsymbol{g}_{\mathrm{best}}$ 和自身历史最优位置 $\boldsymbol{p}_{\mathrm{best}}$ 共同作用，因而粒子飞行轨迹具有记忆特性，从而可以快速到达最终最优位置[16]。

2　基于支持向量机的复合预测模型设计

2.1　复合预测模型模块结构

复合预测模型由 3 部分组成，包括结果展示模块、核心预测模块、数据库模块。其中数据库模块主要负责存储各个历史时间监测点的态势值和按照时间序列方法生成的安全态势样本数据集；核心预测模块主要负责安全态势样本数据集的生成、支持向量机训练生成预测模型、粒子群算法搜寻支持向量机最优训练参数；结果展示模块负责将预测的态势值动态地显示给用户并根据预测的态势值发布告警。复合预测模型的结构图及数据流见图 1。

复合预测模型的工作过程分为 3 个阶段：

1）安全态势样本构造。数据库模块中存储的历史态势值先送入核心预测模块中的数据处理子

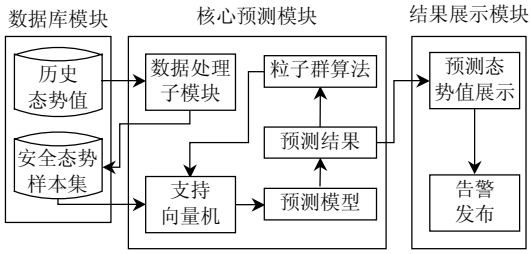

图 1 复合预测模型模块结构

Fig. 1 Construction of hybrid forecast model

模块，由其按照滑动窗口方法生成安全态势样本集，并按照一定比例划分为训练样本集和测试样本集，再存回数据库模块。

2）生成预测模型。此阶段主要由 SVM 和粒子群算法合作完成。SVM 从数据库模块读出安全态势样本集中的训练样本集，并结合粒子群算法传递给 SVM 的初始训练参数完成第 1 次训练，得到初始预测模型。然后 SVM 再读取测试样本集，并利用初始预测模型完成测试样本的态势值预测，得到初始预测结果，再使用粒子群算法中的适应度函数 F 计算初始预测结果与测试样本集中真实态势值的误差，若满足 F 收敛条件，则初始预测模型即为最终预测模型，否则粒子群算法迭代并传递第 2 组训练参数给 SVM，由 SVM 重新读取训练样本集进行第 2 次训练得到第 2 代预测模型，再利用测试样本集检验此代预测模型精度，以此类推，直至得到满足 F 收敛条件的最终预测模型为止。

3）未来安全态势预测及告警发布。根据上一阶段得到的最终预测模型准确预测未来时间监测点的安全态势值，并根据预测安全态势值发布相应的网络安全告警。

由复合预测模型的结构图和工作过程可以看出核心预测模块是其关键部分，下面详细介绍核心预测模块的设计。

2.2 核心预测模块详细设计

2.2.1 数据处理子模块设计

根据某种计算方法[2-4]得到的网络安全态势值可以看作单一变量因素影响的简单时间序列，即每一个时间监测点对应一个网络态势值。因此在构造安全态势样本集时，复合预测模型采用滑动窗口动态生成的方式。假设已知时间监测点 1,2,…,n，对应的网络态势值分别为 $a_1, a_2, \ldots, a_n$，并且设定窗口大小为 m，则第 1 条样本记录为 $a_1, a_2, \ldots, a_m$，由此预测得到 m+1 时间监测点的网络态势值 a_{m+1}，此时再构造第 2 条样本记录 $a_2, a_3, \ldots, a_{m+1}$，并预测 m+2 时间监测点的网络态势值 a_{m+2}，以此类推。构造方法如图 2 所示，复合预测模型设定 m 为 3，即滑动窗口大小是 3。

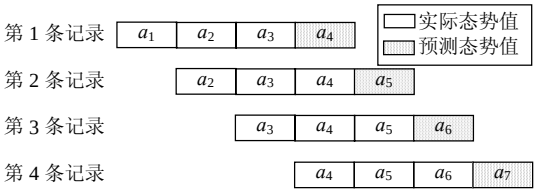

图 2 安全态势样本集生成

Fig. 2 Security situation samples generated

假设当前复合预测模型将预测未来某时间监测点 t 的态势值，并且时间监测点 t–k 之前的态势值均已根据实际情况计算得到，则在预测时间点 t 的态势值时，就使用 t–k 之前的实际态势值覆盖之前的预测值，以防预测误差累计。

数据处理子模块负责将安全态势样本集划分为训练样本集和测试样本集，其中训练样本集由支持向量机训练以得到初始预测模型，而预测样本集被用于检测初始预测模型的预测精度。值得注意的是，在划分训练样本集和测试样本集时，要尽量保证两者之间不存在交集，相互之间完全独立，即开集测试，这样得到的预测模型才有实际应用价值。

2.2.2 支持向量机子模块的设计

支持向量机用于回归预测能够从大量历史数据的学习过程中准确地拟合目标回归问题的趋势曲线，从而实现精确预测。复合预测模型具体选用 v-SVR。相对于其他支持向量机，v-SVR 的优势在于：其他支持向量机对应的非线性规划中都包含惩罚参数 C，而参数 C 的取值体现了对最小化训练错误和最大化间隔这两个目标之间的权衡，但从物理意义上讲 C 本身并没有实际含义，而 v-SVR 中的参数 v 却有其实际意义。

参数 v 的物理含义涉及到“间隔错误训练点”和“支持向量”的概念。设 $\boldsymbol{\alpha}^*=(\alpha_1^*,\ldots,\alpha_l^*)^{\mathrm{T}}$ 是支持向量机求出的 Hilbert 空间中关于非线性规划的对偶问题的解，则称在训练集中 $\boldsymbol{\alpha}^*$ 对应的输入 $\boldsymbol{x}_i$ 为支持向量，并且当 $\boldsymbol{\alpha}^*$ 对应的分量 α_i^* 非零时，间隔错误训练点被定义为没有被“充分”正确划分的训练点。

设支持向量个数为 p，间隔错误训练点个数为 q，训练总样本数为 n，则参数 v 的物理含义为：$v \le p/n$，即 v 是支持向量个数所占总训练样本数的下界；$v \ge q/n$，即 v 是间隔错误训练点个数占总训练样本数的上界。同时由历史经验已知，当训练样本数 $n\to\infty$时，v 以 1 的概率趋近于 p/n。

复合预测模型使用Gauss径向基函数[17]作为核函数，其公式为

$$K(\boldsymbol{x},\boldsymbol{x}')=\mathrm{e}^{-\|\boldsymbol{x}-\boldsymbol{x}'\|^2/\sigma^2} \tag{4}$$

式中：$\boldsymbol{x}'$为核函数中心；σ为函数的宽度参数，控制了函数的径向作用范围。Gauss 径向基函数的特点是局部作用特性强，即当$\boldsymbol{x}$远离$\boldsymbol{x}'$时函数取值很小，从而可以快速实现支持向量机的内积变换，即从$\mathbf{R}^n\rightarrow$Hilbert 空间的变换。

2.2.3　粒子群算法子模块的设计

粒子群算法子模块的设计主要包括种群初始参数设定和构造适应度函数 F。

由数据处理子模块构造好的训练样本集输入到支持向量机进行训练，以得到初始预测模型用于对测试样本集做模型预测精度分析。但支持向量机对训练参数的选取非常敏感，训练参数选取恰当与否将直接决定最终预测模型的准确度，因此复合预测模型利用粒子群算法对支持向量机中 3 个关键训练参数进行寻优，分别是惩罚因子 C、核函数核宽参数σ和损失函数参数ε[12]。其中：参数 C 决定支持向量机的复杂度以及对大于ε的拟合差的惩罚程度，C 取值太大或者太小均易产生过学习或欠学习现象；参数σ表示高维特征空间的精确结构，σ的作用是控制与支持向量机对应的非线性规划问题最优解的复杂度，σ取值太大或太小均会降低支持向量机的泛化能力；参数ε表示对估计函数在样本数据上误差的期望，ε 的取值越大，支持向量数目越少，解的表达就越稀疏，但太大的ε值会降低计算的精度。因而需要构造一个三维解空间，C、σ和ε分别被表示为三维空间中的一维。复合预测模型中粒子群算法具体工作过程：先定义适应度函数 F，设测试样本的总平均误差为ψ，则 F 定义为

$$F_i=\psi_i \tag{5}$$

给定 F 的阈值ε=0.05，当 $F\le\varepsilon$时迭代结束，即复合预测模型总体正确率为 0.95。

随机构造由 i 个粒子组成的初始种群，并给初始种群中所有粒子赋以初始位置 X_i^1 及初始速度 V_i^1，并计算初始种群中每个粒子的 $F(i)$，若初始种群粒子的 $\min(F(i))\le\varepsilon$，则取 $\min(F(i))$的粒子作为待求问题的最优解，否则按式(6)(7)更新粒子速度和位置，即进行种群迭代。

$$V_i^{k+1}=\omega_i V_i^k+C_1\cdot r_1\cdot(p_{\mathrm{best}i}-X_i^k)+C_2\cdot r_2\cdot(g_{\mathrm{best}i}-X_i^k) \tag{6}$$

$$X_i^{k+1}=X_i^k+V_i^{k+1} \tag{7}$$

$$\omega_i=\omega_1-\frac{\omega_1-\omega_{i-1}}{k},\quad \omega_0=\omega_1, i=1,\ldots,n \tag{8}$$

式(6)中：p_{best} 为粒子经过的个体最优位置；g_{best} 为种群经过的最优位置；k 为迭代次数；i 为种群规模；r_1 和 r_2 为[0, 1]之间的随机数；C_1 和 C_2 为 2 个学习因子；ω为惯性权重，ω初值取 0.8。在公式(6)中ω决定了粒子群算法的寻优收敛能力，当ω较大时全局收敛能力较强，当ω较小时局部收敛能力较强，所以ω的更新公式(8)可以保证粒子群算法在前期全局收敛能力强，后期局部收敛能力强。当在某次迭代中出现 $\min(F(i))\le\varepsilon$或者迭代次数达到 T，则算法终止。粒子群算法中其他参数的设定见表 1。

表 1　粒子群参数预设值

Tab. 1　The parameters of PSO

粒子群参数	预设值
种群规模	20
初始惯性权重(ω_1)	0.8
终止惯性权重(ω_2)	0.3
学习因子(C_1=C_2)	2
(C、σ和ε)范围	(0.1, 500 00), (0.1, 1), (0.1, 10)
粒子速度区间	0~0.5
最大迭代次数(k)	200

2.3　复合预测模型完整工作流程

复合预测模型的工作流程如图 3 所示。

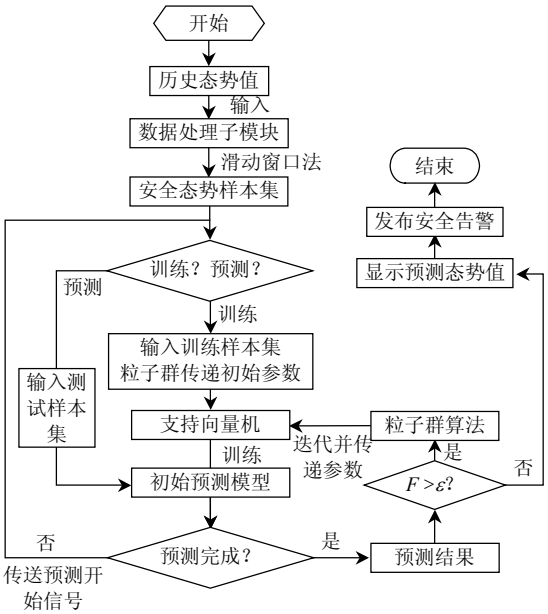

图 3　复合预测模型工作流程

Fig. 3　Working flow chart of hybrid forecast model

3　实验及分析

3.1　生成实验数据集

为验证复合预测模型的有效性，且便于横向比较当前常用的网络态势预测方法，现设计实验数据集如下：选用 20 个电力企业互联网边界连续 150 d

的现场监测数据(源于现场网络及安全设备的安全事件日志)作为原始实验样本，先利用文献[2]的层次分析法计算出 150 d 每日的网络态势值，再按照滑动窗口方法构造容量为 148 条的实验样本集，其中窗口大小设定为 3，第一条样本的时间序列为“1^{st}、2^{ed}、3^{rd}”，最后一条样本的时间序列为“148^{th}、149^{th}、150^{th}”。取前 130 条样本做为训练样本集，后 18 条组成测试样本集，训练样本集与测试样本集完全独立，即开集测试，测试样本集中每天的态势值如表 2 所示。

表 2 测试样本集

Tab. 2 The testing samples set

样本点	131^{th}	132^{th}	133^{th}	134^{th}	135^{th}
态势值	1.151	0.889	0.471	0.358	0.339
样本点	136^{th}	137^{th}	138^{th}	139^{th}	140^{th}
态势值	0.427	0.401	1.208	0.946	0.417
样本点	141^{th}	142^{th}	143^{th}	144^{th}	145^{th}
态势值	0.367	0.367	0.464	0.375	1.179
样本点	146^{th}	147^{th}	148^{th}	149^{th}	150^{th}
态势值	0.879	0.289	0.347	0.412	0.336

3.2 基于粒子群优化支持向量机训练参数的态势预测实验

实验所用粒子群算法和支持向量机均由 JAVA 编写，将构造好的训练样本集输入到复合预测模型，得到最终预测模型，其模型参数由粒子群算法迭代得出，再将测试样本输入到最终预测模型，以得到最终预测结果。在对测试样本做预测时，要用上一条样本的真实态势值替代上一条样本的预测值，以防止预测误差累积。设某一时间监测点的实际网络态势值为 $\hat{y}$，预测值为 y，则该时间监测点的预测相对误差 ψ_i 可以定义为

$$\psi_i = \frac{\|\hat{y}_i - y_i\|}{y_i} \times 100\% \tag{9}$$

测试样本总体平均误差定义为

$$\psi = \frac{1}{n}\sum_{i=1}^{n}\psi_i \tag{10}$$

粒子群最终传递给支持向量机的训练参数为 C=173、σ=0.0046、ε=0.5，粒子群算法的 F 曲线见图 4。从图 4 可见，F 在第 20 代左右基本趋于稳定，最终在第 86 代收敛于 ε，即 $\psi \leq 5\%$。实验结果见图 5。

3.3 预测算法横向比对实验

为进一步验证复合预测模型的有效性，分别选取 BP 神经网络方法、未经参数优化的 SVM 方法和复合预测模型进行横向比较。BP 神经网络采用 2 层结构，权重矩阵和阈值矩阵使用默认值；未经参数优化的 SVM 使用 v-SVR 的默认参数。为更明显地展示几种方法的实验结果，现定义 3 种比较指标：

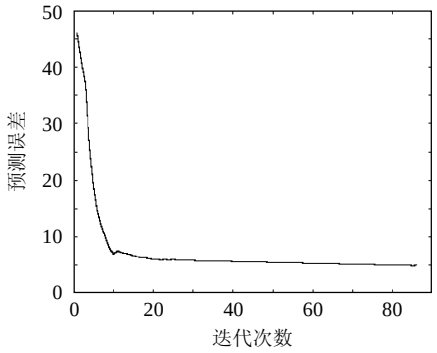

图 4 适应度函数

Fig. 4 The curve of fitness function

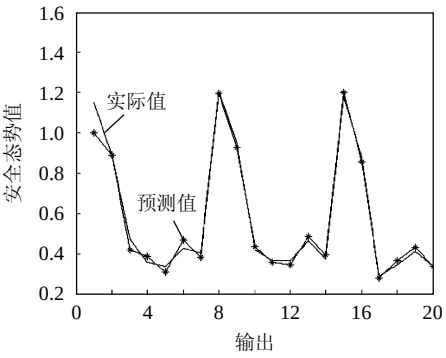

图 5 粒子群优化支持向量机训练参数的实验结果

Fig. 5 The experiment results of PSO optimized SVM training parameters

$$\text{最小样本误差}=\min\psi_i \tag{11}$$

$$\text{最大样本误差}=\max\psi_i \tag{12}$$

$$\text{平均误差}=\psi \tag{13}$$

比对实验结果见表 3，预测曲线见图 6。

表 3 表明，相对于复合预测模型，另外 2 种预测算法准确度较差，特别是最大样本误差偏高，分

表 3 横向比对实验结果

Tab. 3 The experimental results comparison

实验方法	最小样本误差/%	最大样本误差/%	平均误差/%
BP 神经网络	0.19	88.23	20.13
SVM	2.16	87.74	14.92
PSO 优化 SVM	0.00	13.03	4.94

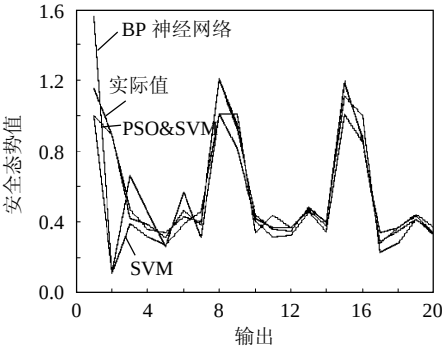

图 6 横向比对曲线

Fig. 6 The comparing curve

析其原因如下：首先，使用 BP 神经网络做预测模型，不可避免神经网络易陷于局部极小点、收敛速度慢、权重和阈值选取困难等问题；其次，使用未经参数优化的 SVM 做预测模型，在预测时由于使用 SVM 的默认参数，导致训练盲目性太大，即求得的最终预测模型并不是原始回归预测问题所对应的非线性规划最优解；最后，以上 2 种横向比较算法都存在严重的过拟合问题，因而对于网络态势值的突变点(如图 6 中从时间监测点 1 到时间监测点 2 的态势值变化)很难适应，才会出现单个样本误差超过 50%的情况。而基于粒子群优化支持向量机训练参数的复合预测模型，因为粒子群算法会随着测试样本的不断输入动态调整支持向量机的训练参数，所以可以在保证预测精度的同时，最大可能地克服过拟合问题。

目前复合预测模型已经成功应用到某电力公司的安全监测系统中，图 7 为该系统中网络态势值预测功能截图。

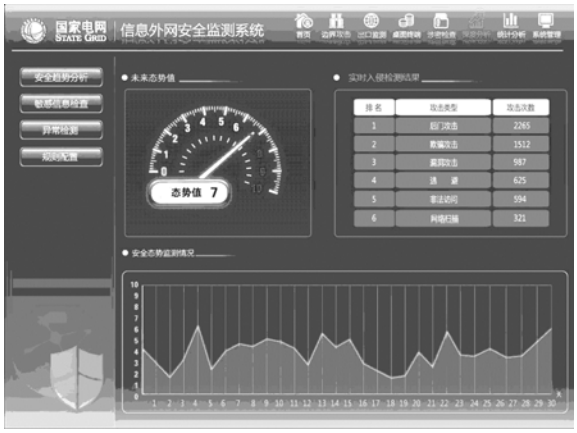

图 7　信息网络安全监测系统

Fig. 7　The monitoring system of information network

4　结论

本文提出的网络态势值复合预测模型，在支持向量机训练过程中利用粒子群优化算法动态地为其搜寻最优训练参数，从而将 2 种人工智能算法有机地结合在一起，改善了复合预测模型的预测精度，解决了原有态势值预测方法中普遍存在的、由于预测模型参数选取困难引起的态势值预测准确率低的问题。在安全态势数据集生成过程中，利用滑动窗口方法将原本离散的监测数据改造成具有部分线性相关性的连续数据样本，进一步提高了复合预测模型的可靠性和有效性。

基于 20 个电力企业互联网边界现场监测数据的网络态势值预测实验结果表明，复合预测模型在预测准确率方面优势明显，特别是在网络态势值出现突变的情况下，仍能保持较高的预测准确性，并且复合预测模型的最大样本误差不超过 15%。在设计实验样本集时，因为训练样本集和测试样本集不存在交集，即保证了 100%开集测试，所以复合预测模型的泛化能力和有效性均得到保证。

如何进一步提高复合预测模型的预测精度并且缩短数据处理时间，是未来的研究重点。

参考文献

[1] 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，2006，10(2)：5-10．
Wang Huiqiang，Lai Jibao，Zhu Liang，et al．Survey of network situation awareness system[J]．Computer Science，2006，10(2)：5-10(in Chinese)．

[2] 陈秀镇，郑庆华，管晓宏．层次化网络安全威胁态势量化评估方法[J]．软件学报，2006，17(4)：885-897．
Chen Xiuzhen，Zheng Qinghua，Guan Xiaohong．Quantitative hierarchical threat evaluation model for network security[J]．Journal of Software，2006，17(4)：885-897(in Chinese)．

[3] 李雄伟，周希元，杨义先．基于层次分析法的网络攻击效果评估[J]．计算机工程与应用，2005，24(49)：157-159．
Li Xiongwei，Zhou Xiyuan，Yang Yixian．Study on the evaluation methods of the attack effect of network based on AHP[J]．Computer Engineering and Applications，2005，24(49)：157-159(in Chinese)．

[4] 邓歆，孟洛明．基于贝叶斯学习的告警相关性分析[J]．计算机工程，2007，33(12)：40-42．
Deng Xin，Meng Luoming．Analysis of alarm correlation based on bayesian learning[J]．Computer Engineering，2007，33(12)：40-42(in Chinese)．

[5] Elattar E E，Goulermas J，Wu Q H．Electric load forecasting based on locally weighted support vector regression[J]．IEEE Translations on Systems，Man，and Cybernetics，Part C：Applications and Reviews，2010，40(4)：438-447．

[6] 陈涛，龚正虎，胡宁．基于改进 BP 算法的网络态势预测模型[C]//2009 全国计算机网络与通讯学术会议．中国深圳：中国电子学会通信学分会，2009：93-99．

[7] 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，2006，31(40)：136-144．
Ren Wei，Jiang Xinghao，Sun Tanfeng．RBFNN-based prediction of networks security situation[J]．Computer Engineering and Applications，2006，31(40)：136-144(in Chinese)．

[8] 王晋东，沈柳青，王坤，等．网络安全态势预测及其在智能防护中的应用[J]．计算机应用，2010，30(6)：1480-1488．
Wang Jindong，Shen Liuqing，Wang Kun，et al．Network security status forecasting and its application in intelligent defense[J]．Journal of Computer Applications，2010，30(6)：1480-1488(in Chinese)．

[9] 张翔，胡昌振，刘胜航，等．基于支持向量机的网络攻击态势预测技术研究[J]．计算机工程，2007，11(3)：10-12．
Zhang Xiang，Hu Changzhen，Liu Shenghang，et al．Research on network attack situation forecast technique based on support vector machine[J]．Computer Engineering，2007，11(3)：10-12(in Chinese)．

[10] 邓万宇，郑庆华，陈琳，等．神经网络极速学习方法研究[J]．计算机学报，2010，2(9)：279-287．
Deng Wanyu，Zheng Qinghua，Chen Lin，et al．Research on extreme

learning of neural networks[J]. Chinese Journal of Computers，2010，2(9)：279-287(in Chinese).

[11] 韩中合，朱霄珣. 基于信息熵的支持向量回归机训练样本长度选择[J]. 中国电机工程学报，2010，30(20)：112-116.
Han Zhonghe，Zhu Xiaoxun. Selection of training sample length in support vector regression based on information entropy[J]. Proceedings of the CSEE，2010，30(20)：112-116(in Chinese).

[12] 郭创新，朱承治，张琳，等. 应用多分类多核学习支持向量机的变压器故障诊断方法[J]. 中国电机工程学报，2010，30(13)：128-134.
Guo Chuangxin，Zhu Chengzhi，Zhang Lin，et al. A fault diagnosis method for power transformer based on multiclass multiple-kernel learning support vector machine[J]. Proceedings of the CSEE，2010，30(13)：128-134(in Chinese).

[13] 王雷，张瑞青，盛伟，等. 基于支持向量机的回归预测和异常数据检测[J]. 中国电机工程学报，2009，29(8)：92-96.
Wang Lei，Zhang Ruiqing，Sheng Wei，et al. Regression forecast and abnormal data detection based on support vector regression[J]. Proceedings of the CSEE，2009，29(8)：92-96(in Chinese).

[14] 杨耿煌，温渤婴. 基于量子行为粒子群优化–人工神经网络的电能质量扰动识别[J]. 中国电机工程学报，2008，28(10)：123-129.
Yang Genghuang，Wen Boying. Identification of power quality disturbance based on QPSO-ANN[J]. Proceedings of the CSEE，2008，28(10)：123-129(in Chinese).

[15] 姚舜才，潘宏侠. 粒子群优化同步电机分数阶鲁棒励磁控制器[J]. 中国电机工程学报，2010，30(21)：91-97.
Yao Shuncai，Pan Hongxia. Fractional order PID controller for synchronous machine excitation using particle swarm optimization [J]. Proceedings of the CSEE，2010，30(21)：91-97(in Chinese).

[16] 李奇，陈维荣，刘述奎，等. 基于自适应聚焦粒子群算法的质子交换膜燃料电池机理建模[J]. 中国电机工程学报，2009，29(20)：119-124.
Li Qi，Chen Weirong，Liu Shukui，et al. Mechanism modeling of proton exchange membrane fuel cell based on adaptive focusing particle swarm optimization[J]. Proceedings of the CSEE，2009，29(20)：119-124(in Chinese).

[17] 陈勇强，刘开培. 一种基于径向基函数动态阈值模型的机组状态监测方法[J]. 中国电机工程学报，2007，27(26)：96-101.
Chen Yongqiang，Liu Kaipei. A condition monitoring method of generators based on RBF dynamic threshold model[J]. Proceedings of the CSEE，2007，27(26)：96-101(in Chinese).


高昆仑

收稿日期：2011-01-10。

作者简介：

高昆仑(1972)，男，博士研究生，主要研究方向为电力系统信息安全，E-mail：gkl@epri.sgcc.com.cn；

刘建明(1955)，男，博士生导师，教授级高级工程师，研究方向为信息与通信技术、多媒体技术，E-mail：jianming-liu@sgcc. com.cn；

徐茹枝(1966)，女，副教授，研究方向为网络信息安全，E-mail：xuruzhi@ncepu.edu.cn；

王宇飞(1982)，男，硕士研究生，研究方向为网络信息安全、人工智能，E-mail：WallYFul@gmail.com；

李怡康(1986)，女，硕士研究生，研究方向为网络信息安全、数据库系统，E-mail：liyikang_2008@126.com。

（责任编辑　李兰欣）