

基于和声搜索算法和相关向量机的网络安全态势预测方法

李 洁, 张兆薇*

(昆明理工大学 质量发展研究院, 昆明 650093)

(* 通信作者电子邮箱 zhaoweizhang2015@163.com)

摘 要: 针对当前网络安全时变性、非线性、预测评估难的现状, 提出一种基于和声搜索算法和相关向量机(HS-RVM)的网络安全态势预测方法, 以弥补现有预测方法在预测精度方面的不足。在预测过程中, 首先对网络安全态势样本集进行归一化处理 and 相空间重构; 然后, 通过利用和声搜索(HS)算法搜索相关向量机(RVM)最优的超参数, 以得到预测精度和速度都得到提升的网络安全态势预测模型; 最后, 采用 Wilcoxon 符号秩检验验证模型预测性能之间的差异性。仿真实例表明, 所提预测方法的平均绝对百分误差(MAPE)和均方根误差(RMSE)分别为 0.49575 和 0.02096, 预测性能优于改进和声搜索(IHS)算法优化的正则极速学习机(RELM)预测模型和 PSO 算法优化的支持向量机回归(PSO-SVR)模型, Wilcoxon 符号秩检验结果显示预测性能之间具有显著的差异性。所提预测方法能够较为精确描述网络安全态势变化规律, 有利于网络管理者及时掌握网络安全态势变化趋势。

关键词: 和声搜索算法; 相关向量机; 网络安全态势; Wilcoxon 符号秩检验; 预测

中图分类号: TP393; TP18 **文献标志码:** A

Network security situation prediction method based on harmony search algorithm and relevance vector machine

LI Jie, ZHANG Zhaowei*

(Quality Development Institute, Kunming University of Science and Technology, Kunming Yunnan 650093, China)

Abstract: To deal with the time-varying and nonlinear properties of network security and its difficulty in prediction assessment, a network security situation prediction method based on Harmony Search algorithm and Relevance Vector Machine (HS-RVM) was proposed to offset the prediction accuracy drawbacks of existing prediction methods. In the prediction process, network security situation samples were firstly normalized and phase space was reconstructed; then, Harmony Search (HS) algorithm was adopted to find out the optimal Relevance Vector Machine (RVM) hyper parameters to build the network security situation prediction model with improved prediction accuracy and velocity; finally, Wilcoxon signed rank tests were used to testify the difference of prediction performance. The simulation cases indicate that the Mean Absolute Percentage Error (MAPE) and the Root-Mean-Square Error (RMSE) of the proposed prediction method are 0.49575 and 0.02096 respectively, with a better prediction performance than the Improved Harmony Search (IHS) algorithm and Regularized Extreme Learning Machine (IHS-RELM) prediction model and PSO and Support Vector machine for Regression (PSO-SVR) prediction model. The outcome of Wilcoxon signed rank tests show there is a significant difference. The proposed method is capable to depict the changing rules of network security situation relatively, which is helpful for network administrators to control the changing tendency of network security situation in time.

Key words: Harmony Search (HS) algorithm; Relevance Vector Machine (RVM); network security situation; Wilcoxon signed rank test; prediction

0 引言

随着网络信息技术的快速发展, 世界经济和军事格局已经进入新常态, 网络安全已经深刻地影响着国家安全和经济建设。网络安全态势评估技术能够综合各方面的安全因素, 是世界各国争相研究的技术热点问题, 因此, 针对网络的安全态势感知是目前网络安全领域的一个研究热点^[1]。自 1999 年 Bass 正式提出了网络态势感知(cyberspace situation awareness)的概念后, 学术界很多学者开始致力于网络安全态

势预测问题的研究^[2]。目前学术界对于网络安全态势评估概念还未能给出统一的、全面的定义, 但“网络安全态势预测其本质是一个回归问题”是学术界共识。有学者提出利用时间序列预测方法研究网络安全态势预测问题^[3], 由于网络攻击的发生是不确定的, 攻击方式多变, 攻击信息模糊, 因此网络安全态势常常呈现出时变性、非线性^[4]等特点, 时间序列预测法在很多领域具有良好的适用性, 但时间序列预测法在处理具有非线性关系、非正态分布特性的网络态势值时间序列数据时, 预测精度不尽人意, 难以描述网络当前状态和未来

收稿日期: 2015-07-20; 修回日期: 2015-08-29。

基金项目: 云南省教育厅科学研究基金资助项目(2014Y081); 昆明理工大学人才培养项目基金资助项目(KKSY201458053)。

作者简介: 李洁(1977-), 女, 四川安岳人, 副教授, 博士, 主要研究方向: 数量经济、质量工程与管理; 张兆薇(1991-), 女, 重庆涪陵人, 硕士研究生, 主要研究方向: 网络安全、质量工程与管理。

状态之间关系^[5-6]。由于智能算法常常具备优异的非线性问题处理能力,能够应对网络安全态势预测中的不确定性和时变性等特征,因此近年来智能算法成为研究网络安全态势评估技术的重要工具,如神经网络^[7]和支持向量机(Support Vector Machine, SVM)^[8]等。其中,Vapnik等提出的支持向量机算法克服了人工神经网络(Artificial Neural Network, ANN)模型的理论缺陷^[9],是一种非线性预测能力非常强的方法,能在海量数据中识别和提取网络安全系统隐藏的规律,因而受到很多研究人员的推崇,但学者们在实际应用中发现,SVM存在自由参数多、支持向量数目易受样本量影响等不足^[10]。

Michael E. Tipping 于 2001 年在 SVM 基础上提出的相关向量机(Relevance Vector Machine, RVM)算法,是一种基于稀疏贝叶斯框架的机器学习算法,其很好地弥补 SVM 的不足,并同时具备了概率式预测能力、参数少、核函数选择不受 Mercer 条件限制等优点^[11]。但 RVM 的预测精度容易受到嵌入维数(r)和核参数(γ)影响,因此优化 r 和 γ 对于提升网络安全态势预测模型精度至关重要。Geem 等^[12]提出的和声搜索(Harmony Search, HS)算法,是一种新兴的智能优化算法。研究^[13]表明,HS 算法展示了比遗传算法(Genetic Algorithm, GA)、交叉验证法(Cross Validation, CV)、粒子群优化(Particle Swarm Optimization, PSO)算法等更好的全局寻优性能。鉴于此,针对网络安全态势非线性特点,本研究将充分发挥和声搜索算法全局寻优能力对 RVM 的超参数 r 和 γ 进行优化,以提升 RVM 回归预测模型的预测精度,并依托 Honeynet 数据集,验证基于和声搜索算法和相关向量机(Harmony Search algorithm and Relevance Vector Machine, HS-RVM)网络安全态势预测模型方法的有效性。

1 和声搜索算法

和声搜索(HS)算法类似于粒子种群算法的思路来源于鸟群捕食,其基本思想是源于音乐师搜索优美和声的现象。Geem 通过类比音乐和最优化问题的相似性而提出的一种具有全局随机搜索能力的启发式算法。HS 算法将产生 M 个初始解存入和声记忆库(Harmony Memory, HM)中;然后对各个初始解的各个分量以和声记忆考虑概率(Harmony Memory Considering Rate, HMCR)、音调微调概率(Pitch Adjusting Rate, PAR)、音调调节带宽(Bandwidth, BW),随机选择3个规则在 HM 中搜索新解,并判断新解是否优于 HM 中的最差解。若是最差解则替换,从而生成新的 HM,否则保持当前 HM 不变。通过不断迭代搜索全局最优解,直至完成 N_1 (算法迭代次数)次迭代为止^[14]。HS 算法基本流程如图1所示。

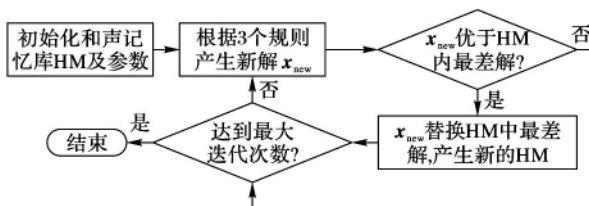


图1 HS 算法计算流程

2 网络安全态势 RVM 预测模型

RVM 在凭借在分类及预测方面的优异性能,已经在风能预测、故障诊断等领域得到广泛的应用,但是其在网络安全态

势预测领域的应用研究还颇为少见。

2.1 RVM 模型描述

给定网络安全态势训练样本集 $\{x_i, t_i\}_{i=1}^N, x_i \in \mathbf{R}^d, t_i \in \mathbf{R}$ 。网络安全态势 RVM 预测模型的输出为:

$$y(x, w) = \sum_{i=1}^N w_i K(x, x_i) + w_0 \quad (1)$$

其中: $K(x, x_i)$ 为 RBF(Radial Basis Function)核函数; w_i 为 RVM 预测模型的权值; N 为网络安全态势训练样本数。

假设目标是独立的,网络安全态势 RVM 预测模型采用与 SVM 相同的预测函数式(2):

$$t_n = y(x_n, w) + \varepsilon_n \quad (2)$$

其中: ε_n 为样本数据噪声,满足 $\varepsilon_n \sim N(0, \sigma^2)$ 的高斯分布(Gaussian distribution)。

网络安全态势训练样本集的似然函数如式(3)所示:

$$p(t | w, \sigma^2) = (2\pi\sigma^2)^{-\frac{N}{2}} \exp\left\{-\frac{1}{2\sigma^2} \|t - \Phi w\|^2\right\} \quad (3)$$

其中: $t = [t_1, t_2, \dots, t_N]^T$; $\Phi \in \mathbf{R}^{N \times (N+1)}$ 为网络安全态势训练样本集的设计矩阵,假定训练样本集的设计矩阵 $\Phi = [\phi(x_1), \phi(x_2), \dots, \phi(x_i), \dots, \phi(x_N)]^T$,则基函数向量 $\phi(x_i) = [1, k(x_i, x_1), \dots, k(x_i, x_N)]^T$ 。

为了避免通过最大似然法求出的最优 w 使经验风险最小化,采用稀疏贝叶斯(Bayesian)方法对权值 w 赋予先验的条件概率,具体的分布如式(4)所示:

$$p(w | \alpha) = \prod_{i=0}^N N(w_i | 0, \alpha_i^{-1}) \quad (4)$$

其中: $\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_M\}$ 是网络安全态势 RVM 预测模型的超参数; M 为超参数的个数,符合伽马分布(Gamma Distribution)。

根据 Bayesian 公式,对所有未知参数进行估计,后验公式如式(5)所示:

$$p(w, \alpha, \sigma^2 | t) = p(t | w, \alpha, \sigma^2) p(w, \alpha, \sigma^2) / p(t) \quad (5)$$

给定新的网络安全态势值 x_* ,相应网络安全态势目标预测值 t_* ,分布为:

$$p(t_* | t) = \int p(t_* | w, \alpha, \sigma^2) p(w, \alpha, \sigma^2 | t) dw d\alpha d\sigma^2 \quad (6)$$

由式(6)可得式(7):

$$p(w, \alpha, \sigma^2 | t) = p(w | t, \alpha, \sigma^2) p(\alpha, \sigma^2 | t) \quad (7)$$

由式(7)则有式(8):

$$p(w | t, \alpha, \sigma^2) = \frac{p(t | w, \sigma^2) p(w | \alpha)}{p(t | \alpha, \sigma^2)} = (2\pi)^{-\frac{(N+1)}{2}} |\Sigma|^{-\frac{1}{2}} \exp\left\{-\frac{1}{2}(w - \mu)^T \Sigma^{-1}(w - \mu)\right\} \quad (8)$$

式(8)中,后验协方差 Σ 和均值 μ 分别为:

$$\begin{cases} \Sigma = (\sigma^2 \Phi^T \Phi + A)^{-1} \\ \mu = \sigma^{-2} \Sigma \Phi^T t \end{cases} \quad (9)$$

其中 $A = \text{diag}(a_0, a_1, \dots, a_N)$ 。

对式(7)中超参数后验 $p(\alpha, \sigma^2 | t)$ 通过式(10)关于 α 最大化,来确定超参数后验的峰值。

$$p(\alpha, \sigma^2 | t) \propto p(t | \alpha, \sigma^2) p(\alpha) p(\sigma^2) \quad (10)$$

在一致超先验情况下,要想确定式(7)中超参数,仅需取 $p(t | \alpha, \sigma^2)$ 的最大值,即:

$$p(t | \alpha, \sigma^2) = (2\pi)^{-\frac{N}{2}} |\sigma^2 I + \Phi A^{-1} \Phi^T|^{-\frac{1}{2}} \cdot$$

$$\exp\left\{-\frac{1}{2}t^T(\sigma^2 I + \Phi A^{-1} \Phi^T)^{-1}t\right\} [0, 1] \quad (11)$$

2.2 模型优化超参数及预测

要想使式(11)中 $p(t|\alpha, \sigma^2)$ 获取最大值,必须获取相应的 α 和 σ^2 的解析表达式,采用反复迭代估计获取解析式,具体如式(12)和式(13)所示:

$$\alpha_i^{\text{new}} = \gamma_i / \mu_i^2 \quad (12)$$

$$(\sigma^2)^{\text{new}} = \|t - \Phi \mu\| / \left(N - \sum_{i=1}^N \gamma_i\right) \quad (13)$$

式(12)和(13)中, μ_i 为第 i 个后验平均权; $\gamma_i \equiv 1 - \alpha_i \Sigma_{ii}$, Σ_{ii} 为后验权协方差矩阵的第 i 个对角元素, N 为网络安全态势样本数据的个数。

式(12)服从正态分布,即有式(14):

$$p(t_* | t_{\text{MP}}, \sigma_{\text{MP}}^2) = N(t_* | y_*, \sigma_*^2) \quad (14)$$

给定网络安全态势输入值 x_* ,预测均值: $y_* = \mu^T \phi(x_*)$;方差: $\sigma_*^2 = \sigma_{\text{MP}}^2 + \phi(x_*)^T \Sigma \phi(x_*)$,则网络安全态势RVM预测模型的输出为: $y_* = (x_*; \mu)$ 。

2.3 基于HS算法的超参数寻优

超参数(嵌入维数(r)和核参数(γ))的设置对于网络安全态势RVM预测模型的性能有着重要影响。Geem提出HS算法时,已经通过实验验证了HS算法的非线性寻优能力,实验结果表明HS算法具备比遗传算法更好的搜索能力^[12-13],因此,本研究采用HS算法寻找网络安全态势RVM预测模型最优的超参数组合,使得RVM预测模型具有最好的分类性能,提高RVM预测模型的学习性能。基于HS算法的网络安全态势RVM预测模型参数寻优步骤具体如下。

步骤1 参数初始化设置。在进行RVM参数寻优之前,HS算法自身需要初始化的参数有:记忆库取值概率 $HMCR$,和声记忆库的大小 HMS (Harmony Memory Size),音调微调概率 PAR ,音调调节带宽 BW (Bandwidth),最大进化迭代代数为 T_{max} ,超参数 r 和 γ 的上、下限值向量分别是 x_{max} 和 x_{min} ,个体和声向量维数为 N 。

步骤2 初始化和声库。

利用 $x_{\text{min}} + rand1 \times (x_{\text{max}} - x_{\text{min}})$ 在相关向量机(RVM)超参数解空间中随机产生 HMS 个和声,随机产生的超参数值 x_N^{HMS} 和对应的目标函数值 $f(x^{\text{HMS}})$ 存储在种群中,构成了网络安全态势初始的和声库。用矩阵表示为:

$$HM = \begin{bmatrix} X^1 & f(x^1) \\ X^2 & f(x^2) \\ \vdots & \vdots \\ X^{\text{HMS}} & f(x^{\text{HMS}}) \end{bmatrix} = \begin{bmatrix} x_1^1 & x_2^1 & \cdots & x_N^1 & f(x^1) \\ x_1^2 & x_2^2 & \cdots & x_N^2 & f(x^2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{\text{HMS}} & x_2^{\text{HMS}} & \cdots & x_N^{\text{HMS}} & f(x^{\text{HMS}}) \end{bmatrix}$$

在该和声库中,每一行代表一个解, $rand1$ 为 $[0, 1]$ 区间的均匀随机数。

步骤3 计算适应度值。

和声库中的每一个和声实际上就是相关向量机(RVM)超参数(r, γ)的一个组合,利用相关向量机(RVM)在网络安全态势训练集上对每个和声为参数进行训练,并将在网络安全态势测试集上的分类准确率作为和声库中各和声的适应度值。

步骤4 生成新的和声。

根据式(15)从和声库中随机选取一个新的和声 x_i' ,按概率 PAR 对选取的和声进行音调微调,判断其是否满足 $rand2 < HMCR$;如果不满足 $rand2 < HMCR$,则在变量 X_i 中重

新生成一个新的和声。

$$\begin{cases} x_i' \in (x_i^1, x_i^2, \cdots, x_i^{\text{HMS}}), & rand2 < HMCR \\ x_i' \in X_i, & i = 1, 2, \cdots, N \end{cases} \quad (15)$$

其中: $rand2$ 为 $[0, 1]$ 区间的均匀随机数。

步骤5 更新和声记忆库。

计算由步骤4所产生的新和声的适应度,并根据式(16)进行和声库更新,生成新一代的和声库。

$$x^{\text{new}} = x'; f(x_i') < f(x^{\text{new}}) = \max_{i=1, 2, \cdots, HMS} f(x_i') \quad (16)$$

步骤6 判断算法是否终止。

若迭代次数达到 T_{max} ,则整个寻优过程结束,输出网络安全态势RVM模型的最优超参数组合(r, γ);否则,算法转到步骤4继续执行相关向量机(RVM)超参数(r, γ)的寻优任务。

步骤7 输出超参数最优解向量,按照式(14)构造超参数优化的网络安全态势RVM预测模型。

2.4 网络安全态势预测模型构建过程

构建网络安全态势的RVM预测模型主要步骤如下。

1) 从中选取 m 个网络安全态势样本作为训练样本集,其余 $n - m$ 个样本为测试集。对于网络安全态势训练样本集,选择Gaussian核函数作为RVM核函数,其表达式为: $k(x_i, x) = \exp(-\|x_i - x\|^2 / \gamma^2)$,构建如式(14)所示的网络安全态势预测RVM回归模型。同时,按照2.3节优化步骤,利用和声搜索算法的方法确定超参数组合(r, γ),获得了超参数优化的HS-RVM模型。

2) 在获得最佳超参数组合(r, γ)后,根据测试样本进行网络安全态势HS-RVM模型测试,将测试样本所得数据与实际数值进行对比,分析网络安全态势HS-RVM模型测试性能。

3 仿真实验

3.1 数据来源及处理

Honeynet组织收集的黑客攻击数据集是安全态势实验仿真常用的典型网络安全数据集,能够反映出黑客的攻击行为和体现出网络安全态势的变化规律^[14],因此,选择2000年7月5日到2000年12月3日的Honeynet数据集作为网络安全态势RVM预测模型的实验数据集,并同时参照文献[15]中计算网络安全态势值方法进行计算,计算得到126个网络安全态势值。另外,对所获得的网络安全态势样本数据按照式(17)进行归一化处理。最后,对归一化后的网络安全态势样本数据集进行相空间重构,可以构造119个样本对,选取前105个网络安全态势样本对作为网络安全态势RVM预测模型的训练集,后14个样本对作为模型的测试集。训练集如图2所示。

$$net_i' = \frac{net_i - net_{\min}}{net_{\max} - net_{\min}}; \quad i = 1, 2, \cdots, 119 \quad (17)$$

其中: net_i 表示网络安全态势样本数据归一化前的数值, net_i' 表示归一化后的值, net_{\max} 表示网络安全态势样本数据集中的最大值, net_{\min} 表示最小值。

3.2 仿真实验结果

为了验证基于HS算法超参数优化的网络安全态势HS-RVM预测模型具有更好的预测精度,将其与文献中已有的IHS-RELM(Improved Harmony Search and Regularized Extreme Learning Machine)预测方法^[16]、PSO-SVR(Particle Swarm Optimization and Support Vector machine for Regression)预测方

法^[17]进行比较。借助 Matlab R2009b 软件和 LibSVM 工具分别构建上述网络安全态势预测模型, 计算结果如图 3 所示。

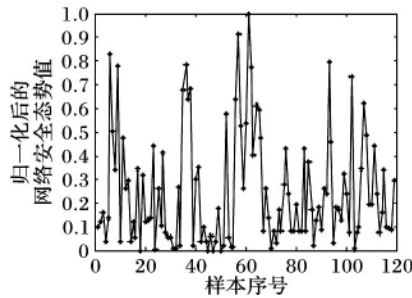


图2 网络安全态势值样本训练集

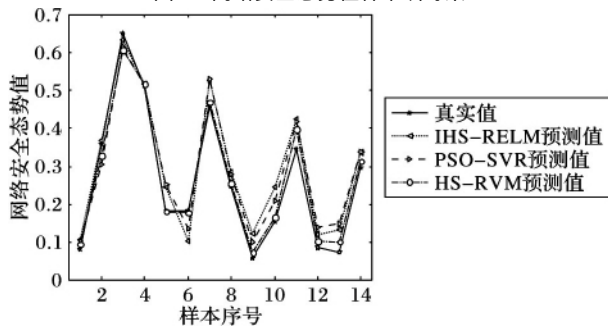


图3 不同模型的网络安全态势预测值

平均绝对百分误差 (Mean Absolute Percentage Error, MAPE) 和均方根误差 (Root Mean Square Error, RMSE) 能够很好地刻画模型性能, 因此将这两项性能指标应用于本文模型预测性能对比。显然, MAPE 和 RMSE 值越小, 则预测模型的精度越高。MAPE 和 RMSE 计算公式如下所示:

$$MAPE = \frac{1}{n} \sum_{i=1}^n \frac{|y_i' - y_i|}{y_i} \quad (18)$$

$$RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i' - y_i)^2} \quad (19)$$

其中: y_i' 为网络安全态势预测值; y_i 为网络安全态势实际值; $n = 1, 2, \dots, 14$ 。

根据式 (18) 和式 (19), IHS-RELM、PSO-SVR 和 HS-RVM 3 种网络安全态势预测模型的预测性能指标计算结果如表 1 所示。

表1 3 种模型预测性能对比

模型	MAPE	RMSE
IHS-RELM	0.526 17	0.024 19
PSO-SVR	0.512 47	0.022 62
HS-RVM	0.495 75	0.020 96

从表 1 可知, 从性能评价指标 MAPE 和 RMSE 来看, 基于 HS 算法的网络安全态势 RVM 预测模型的预测性能明显优于 PSO-SVR 模型和 IHS-RELM 模型。

3.3 模型检验

为了进一步验证模型之间在预测性能方面的差异性, 采用 Wilcoxon 单边符号秩检验方法进行验证, 结果如表 2 所示。

表2 Wilcoxon 符号秩检验

模型	N	秩	秩总和	P
(IHS-RELM) - (HS-RVM)	14	48	65	0.000
(PSO-SVR) - (HS-RVM)	10	42	32	0.000

表 2 中: N 表示 HS-RVM 模型的 MAPE 小于 IHS-RELM 模型和 PSO-SVR 模型 MAPE 的个数。从表 2 可知, P 值为 0.000, Wilcoxon 符号秩检验的结果显示: HS-RVM 预测方法与 PSO-SVR 模型和 IHS-RELM 模型在预测性能方面存在明显差异, 因此, 综合来看, 基于 HS-RVM 的网络安全态势预测模型是一种有效、高精度的预测模型。

4 结语

针对时间序列预测法描述刻画网络安全态势的非线性关系、非正态分布特性时性能不佳的问题, 本文充分考虑网络安全态势变化的复杂性、时变性和非线性等特点, 通过和声搜索算法 (HS) 优化相关向量机 (RVM) 超参数, 构建了基于 HS-RVM 的网络安全态势预测模型。通过利用和声算法对相关向量机超参数 (r, γ) 进行寻优, 然后构建网络安全态势 HS-RVM 预测模型。依托 Honeynet 数据集的仿真实验表明, 基于 HS-RVM 的网络安全态势预测模型能够精确描述网络安全态势变化规律, 从而有利于网络管理者及时掌握网络安全态势变化趋势, 更快地采取相应网络安全管理措施, 维护网络安全。

参考文献:

- [1] 韦勇, 连一峰, 冯登国, 等. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353 - 362. (WEI Y, LIAN Y F, FENG D G. A network security situational awareness model based on information fusion [J]. Journal of computer research and development, 2009, 46(3): 353 - 362.)
- [2] BASS T. Intrusion detection systems & multi-sensor data fusion: creating cyberspace situational awareness [J]. Communications of the ACM, 2000, 43: 99 - 105.
- [3] 徐茹枝, 常太华, 吕广娟, 等. 基于时间序列的网络安全态势预测方法的研究[J]. 数学的实践与认识, 2010, 40(12): 124 - 131. (XU R Z, CHANG T H, LYU G J, et al. The research on prediction posture based method of network security on time series [J]. Mathematics in practice and theory, 2010, 40(12): 124 - 131.)
- [4] YAN Z, LIU Z, DENG G. An approach to evaluating the network security in triangular fuzzy environment [J]. International journal of digital content technology and its applications, 2012, 6(19): 410 - 416.
- [5] 王庚, 张景辉, 吴娜. 网络安全态势预测方法的应用研究[J]. 计算机仿真, 2012, 29(2): 98 - 101. (WANG G, ZHANG J, WU N. Application research on network security situation prediction method [J]. Computer simulation, 2012, 29(2): 98 - 101.)
- [6] 张安楠, 苏畅. 基于小波变换的网络安全态势复合预测方法[J]. 计算机仿真, 2014, 31(6): 282 - 286. (ZHANG A N, SU Y. Research on hybrid prediction method for network security situation based on wavelet transform [J]. Computer simulation, 2014, 31(6): 282 - 286.)
- [7] LEE C M, KO C N. Time series prediction using RBF neural networks with a nonlinear time-varying evolution PSO algorithm [J]. Neurocomputing, 2009, 73(1): 449 - 460.
- [8] LI Y, JING J. A method of improved support vector machine for network security situation forecasting [J]. Advanced materials research, 2011, 187: 291 - 296.
- [9] ZHANG S, LI B, WANG B. The application of an improved integration algorithm of support vector machine to the prediction of network security situation [C]// Applied mechanics and materials. 2014, 513: 2285 - 2288.

(下转第 232 页)

- 39(3): 125 – 128.)
- [4] 王波. 滤波算法在图像增强中的应用研究[J]. 计算机仿真, 2013, 30(3): 364 – 367. (WANG B. Application of bilateral filtering algorithm in image enhancement [J]. Computer simulation, 2013, 30(3): 364 – 367.)
- [5] 汪成亮, 乔鹤松, 陈娟娟. 基于纹理复杂度的自适应分数阶微分算法[J]. 计算机工程, 2012, 38(7): 177 – 178. (WANG C L, QIAO H S, CHEN J J. Adaptive fractional differential algorithm based on texture complexity [J]. Computer engineering, 2012, 38(7): 177 – 178.)
- [6] GAN Z, YANG H. Texture enhancement though multiscale mask based on RL fractional differential [C]// Proceedings of the 2010 International Conference on Information Networking and Automation. Piscataway, NJ: IEEE, 2010: 333 – 337.
- [7] 杨柱中, 周激流, 晏祥玉, 等. 基于分数阶微分的图像增强[J]. 计算机辅助设计与图形学学报, 2008, 20(3): 343 – 348. (YANG Z Z, ZHOU J L, YAN X Y, et al. Image enhancement based on fractional differentials [J]. Journal of computer-aided design & computer graphics, 2008, 20(3): 343 – 348.)
- [8] PU Y, ZHOU J. A novel approach for multi-scale texture segmentation based on fractional differential [J]. International journal of computer mathematics, 2011, 88(1): 58 – 78.
- [9] 张志宝, 沈怀荣, 路振民, 等. 基于分数阶微分的遥感图像边缘检测方法[J]. 现代电子技术, 2014, 37(20): 99 – 102. (ZHANG Z B, SHEN H R, LU Z M, et al. Method on remote sensing image edge detection based on fractional order differential [J]. Modern electronics technique, 2014, 37(20): 99 – 102.)
- [10] 何春, 叶永强, 姜斌, 等. 一种基于分数阶微分模板的新型边缘检测方法[J]. 自动化学报, 2012, 38(5): 776 – 787. (HE C, YE Y Q, JIANG B, et al. A novel edge detection method based on fractional-order calculus mask [J]. Acta automatica sinica, 2012, 38(5): 776 – 787.)
- [11] 甘志凤, 杨红雨. 基于 R-L 分数阶微分梯度算子的边沿检测[J]. 计算机工程与设计, 2010, 31(21): 4342 – 4645. (GAN Z F, YANG H Y. Edge detection based on R-L fractional-order differential gradient operator [J]. Computer engineering and design, 2010, 31(21): 4342 – 4645.)
- [12] CAFAGNA D. Fractional calculus: a mathematical tool from the past for present engineers [J]. IEEE industrial electronics magazine, 2007, 1(2): 35 – 40.
- [13] 蒋伟, 陈辉. 基于分数阶微分和 Sobel 算子的边缘检测新模型[J]. 计算机工程与应用, 2012, 48(4): 182 – 185. (JIANG W, CHEN H. New edge detection model based on fractional differential and Sobel operator [J]. Computer engineering and applications, 2012, 48(4): 182 – 185.)
- [14] 苑玮琦, 李雪. 一种边缘检测效果评价方法的研究[J]. 微计算机信息, 2007, 23(11): 304 – 306. (YUAN W Q, LI X. Study on evaluating results of edge detectors [J]. Microcomputer information, 2007, 23(11): 304 – 306.)

Background

This work is partially supported by the National Natural Science Foundation of China (61174184) and the Major Science and Technology Project of Guangdong Province (2012A010800007).

WANG Chengxiao, born in 1991, M. S. candidate. His research interests include digital image processing, intelligent control, optimization algorithm.

HUANG Huixian, born in 1957, Ph. D., professor. His research interests include intelligent control, complex modeling and nonlinear control, intelligent control and urban intelligent transportation system, optimization algorithm.

YANG Hui, born in 1991, M. S. candidate. His research interests include digital image processing, intelligent control.

XU Jianmin, born in 1960, Ph. D., professor. His research interests include traffic information engineering and control, control theory, control engineering.

(上接第 202 页)

- [10] SONG G. Computer network security and precaution evaluation based on incremental relevance vector machine algorithm and ACO [J]. International journal on advances in information sciences and service sciences, 2013, 5(1): 120 – 127.
- [11] TIPPING M E. Sparse Bayesian learning and the relevance vector machine [J]. Journal of machine learning research, 2001, 1: 211 – 244.
- [12] GEEM Z W, KIM J H, LOGANATHAN G V. A new heuristic optimization algorithm: harmony search [J]. Simulation, 2001, 76(2): 60 – 68.
- [13] ZOU D, GAO L, LI S, et al. An effective global harmony search algorithm for reliability problems [J]. Expert systems with applications, 2011, 38(4): 4642 – 4648.
- [14] Honeynet Project. Know your enemy; statistics. 2001 [EB/OL]. [2015-05-10]. <http://old.org/papers/stats/>.
- [15] 肖汉杰, 桑秀丽. 相关向量机超参数优化的网络安全态势预测[J]. 计算机应用, 2015, 35(7): 1888 – 1891. (XIAO H J, SANG X L. Network security situation prediction based on hyper parameter optimization of RVM [J]. Journal of computer applications, 2015, 35(7): 1888 – 1891.)
- [16] 陈虹, 王飞, 肖振久, 等. 基于 IHS_RELm 的网络安全态势预测方法[J]. 计算机科学, 2013, 40(11): 108 – 111. (CHEN H, WANG F, XIAO Z J, et al. Method of network security situation prediction based on IHS_RELm [J]. Computer science, 2013, 40(11): 108 – 111.)
- [17] 陈虹, 王飞, 肖振久. 基于 PSO_SVR 的网络安全态势预测方法[J]. 计算机应用与软件, 2014, 31(8): 292 – 294. (CHEN H, WANG F, XIAO Z J. Network security situation prediction on method based on PSO_SVR [J]. Computer applications and software, 2014, 31(8): 292 – 294.)

Background

This work is partially supported by the Scientific Research Fund of Yunnan Provincial Department of Education (2014Y081), the Talent Training Project Fund of Kunming University of Science and Technology (KKS201458053).

LI Jie, born in 1977, Ph. D., associate professor. Her research interests include quantitative economics, quality engineering and management.

ZHANG Zhaowei, born in 1991, M. S. candidate. Her research interests include network security, quality engineering and management.