

网络安全态势预测技术研究

孙卫喜¹, 孙欢²

(1. 渭南师范学院 网络安全与信息化学院, 陕西 渭南 714099;
2. 西安电子科技大学 经济与管理学院, 陕西 西安 710071)

摘要:网络安全态势预测是防御网络安全威胁的关键。在对目前网络安全态势预测方法进行分析研究后, 给出支持向量机(SVM)与改进粒子群优化算法相结合的网络安全态势预测方法。该方法使用改进的粒子群优化算法来优化 SVM 的三个参数, 其充分利用了 SVM 收敛速度快、样本小、泛化能力强、机器学习的优点, 克服了 PSO-SVM 存在局部最优解及粒子早熟的问题。该方法更适用于具有时变性与非线性特征的网络安全态势预测, 且克服了使用线性方法进行网络安全态势预测带来的预测精度低、描述网络目前状态与未来状态关系困难的问题。实验结果表明, 使用该预测方法处理先前收集到的网络安全数据, 明显提高了网络态势的预测精度, 实现了对网络安全威胁的有效防御。

关键词:安全态势; 支持向量机; 粒子群算法; 态势预测

中图分类号: TP301.6

文献标识码: A

文章编号: 1673-629X(2019)04-0100-05

doi: 10.3969/j.issn.1673-629X.2019.04.021

Research on Network Security Situation Prediction Technology

SUN Wei-xi¹, SUN Huan²

(1. School of Network Security and Information Technology, Weinan Normal University,
Weinan 714099, China;
2. School of Economics and Management, Xidian University, Xi'an 710071, China)

Abstract: Network security situation prediction is the key to defending against network security threats. After the analysis and research of the current network security situation prediction methods, we present a new one combined with support vector machine (SVM) and improved particle swarm optimization. This method uses the improved particle swarm optimization to optimize the three parameters of SVM, and makes full use of the advantages of SVM such as fast convergence speed, small sample size, strong generalization and machine learning to overcome the problems of local optimal solution and particle premature in PSO-SVM. It is more suitable for the network security situation prediction with time-varying and nonlinear characteristics, and overcomes the problem of low prediction accuracy and difficult description of the relationship between the current state and the future state brought by the linear method in the network security situation prediction. Experiment shows that the proposed method has improved the prediction accuracy of the network situation by dealing with the previously collected network security data, and also has realized the effective defense of the network security threat.

Key words: security situation; support vector machine; particle swarm optimization; situation prediction

0 引言

如今人们在工作、学习、生活等方面享受网络带来极大便利的同时也为经常出现的网络安全问题感到困惑, 特别是互联网环境高速进化中网络安全威胁及网络攻击手段多样化已超越了防范措施的推出速度, 面对网络攻击行为规模化、常态化发展的趋势, 研究如何在网络攻击之前, 利用有效的防护措施及时发现攻击

行为并予以阻止就显得非常有意义。网络安全态势感知(network security situation awareness, NSSA)能对影响网络安全的各种因素进行解析、收集、综合处理; 建立数学模型; 给出评估网络安全的方法; 对网络安全进行预测。从而使网络管理者能及时利用可视化的网络安全预测系统, 对发现的网络安全弱点、预测到的威胁, 制定出相应的措施主动进行防御。

收稿日期: 2018-04-24

修回日期: 2018-08-29

网络出版时间: 2018-12-20

基金项目: 陕西省自然科学基金基础研究计划资助项目(2017JM6110); 渭南师范学院自然科学类研究项目(18YKS13)

作者简介: 孙卫喜(1965-), 男, 高级工程师, 研究方向为网络安全、网络应用; 孙欢(1990-), 男, 硕士研究生, 研究方向为管理决策分析。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20181219.1542.070.html>

1 网络安全态势感知

态势感知(situation awareness, SA)起源于军事领域,用于对复杂结构、影响因素众多、大范围事件的整体理解及快速决策处理。Time Bass 针对网络安全的复杂性于1999年提出了网络安全态势感知的概念^[1],虽然网络态势感知的标准定义目前还没有,但网络态势感知作用却很明确,即通过感知系统观测整个网络的安全情况,再依据观测到的数据对网络安全事件及时做出判断,并以可视化方式提供给管理者进行决策。数据挖掘与态势评估及态势预测被普遍认为是网络安全态势感知的三大关键技术,数据挖掘中力求准确、快速、全面地找到网络威胁事件;态势评估要求更为有效客观地评价网络安全态势;态势预测则强调预测网络安全的准确性,以便使网络管理者依据预测结果采取相应的措施,保护网络安全。

国外网络安全态势感知系统架构的建立主要采用的是集成化思想,卡内基梅隆大学 SEI 2005 年在网络态势感知系统中集成了 Netflow 工具,能对潜在的、恶意的网络攻击行为进行识别与响应,并做出相应的防御。King 等 2012 年在分类属性网络中运用深度包检测技术提供了深刻全面的态势感知结果^[2];Friedberg 等 2015 年给出了网络异常行为的态势感知基于事件自动关联的事件检测 AECID^[3]。

国内对网络安全态势感知的研究主要基于网络安全数据的全面获得,数据融合方法及数据之间的关联性分析,网络安全态势指标体系的建立,以及网络安全态势评估。

陈秀真等利用网络运行情况与告警信息数据,对网络结构及主机和服务发挥的作用进行系统分析,提取影响网络态势的多个因素,给出了网络安全态势计算方法和层次化的量化评估模型^[4],但其缺乏对网络攻击间的联系及整体性分析。韦勇等依据层次化的思想,对节点上的安全要素利用 D-S 证据理论做了融合,再按照节点、子网、全网层融合,最后获得网络态势值,从而在信息融合的基础上建立网络安全态势评估模型^[5],由于其有效处理了多源安全事件,使多源信息间的互补性得到了充分利用,从而使态势感知的准确性进一步提高,也使得在网络态势感知中多源信息融合优于单源的特征得到验证。刘效武等以数据信息从融合异质多传感器获得,再用支持向量机结合特征约简算法生成网络安全态势值,最后依据评价指标评价量化态势感知^[6]。

目前对 NSSA 的研究仍然处于探索阶段,主要存在的问题是:缺乏统一的理论体系指导及态势分级评价的客观性;前期的评价体系仍然缺乏宏观性及整体性;多属性多源潜在的内部态势信息及复杂的网络元

素间的关系无法展现;系统方面的研究及对网络态势结果溯源的较少。

2 网络安全态势预测模型的构建

2.1 网络安全态势预测

网络安全态势的预测以发生网络安全事件的数量、频率、网络受威胁程度等因素经过处理而获取反应网络态势的数据为根据。网络安全态势预测标准模型与方法目前并没有,发展较快的网络安全态势预测方法主要有:灰色预测、神经网络、时间序列预测法及支持向量机预测。

文中在对目前网络安全态势预测方法进行分析研究后,给出一种支持向量机与改进粒子群优化算法相结合的网络安全态势预测方法,即在 SVM 优点特征的基础上用改进的粒子群优化算法,通过用无体积无质量的粒子作为个体且规定各粒子的行为规则,使用个体之间的协作寻优在表现出复杂特性的整个粒子群中寻找最优解,进而优化支持向量机的三个参数。该方法克服了使用线性方法评估网络安全态势带来的预测精度低、描述网络目前状态与未来状态关系困难等问题,更适应网络安全态势变化时变性、非线性等特点。

2.2 支持向量机算法

为了解决复杂的模式识别问题,Vapnik 于 1963 年提出了支持向量机,该研究在 1992 年取得了较大进展^[7]并于 1995 年在统计学习理论的基础上给出了 SVM 分类器,较好地解决了线性不可分的问题^[8]。后续的学者们研究出:基于二叉树的多分类方法^[9]、序列最小优化训练算法(SMO)^[10]、多分类理论、决策导向非循环图法(DDAG)^[11]、1-a. r 方法^[12]。近年来相关学者们又研究出 Class-SVM、v-SVM、C-SVM 等算法,进一步完善了支持向量机的理论体系。张翔等在态势评估指标时间序列预测中采用支持向量回归预测的方法^[13];王庚等人用遗传算法的染色体编码优化支持向量机参数^[14]。

SVM 训练样本通过预设函数的支持向量机训练,函数的确定是在用不断拟合方法给出重要参数的基础上获得的。SVM 泛化能力强,对复杂的非线性数据与小样本数据的建模识别能力很好。

文中所给样本集为: $\{\{X_1, Y_1\}, \{X_2, Y_2\}, \dots, \{X_n, Y_n\}\}$, $X_i \in R^n$, 观测样本值 $Y_i \in R^n$, 设回归模型为:

$$f(x) = \omega^T x + b \quad (1)$$

其中, ω 为支持向量机法向量; b 为偏移量。

实现合理拟合样本集需要用到损失函数 ε , $|y_i - f(x_i)| = \max\{0, |y_i - f(x_i)| - \varepsilon\}$ 观测值与 $f(x_i)$

回归预测值间误差的相对值不能大于 ε , 因而:

$$\begin{cases} y_i - \omega \cdot x_i - b \leq \varepsilon \\ \omega \cdot x_i + b - y_i \leq \varepsilon \\ i = 1, 2, \dots, n \end{cases} \quad (2)$$

ε 损失函数稳定性好, 在不知道 SVM 训练样本分布特征的情况下误差不能直接计算。 $f(x)$ 按结构风险最小化 $\frac{1}{2} \|\omega\|^2$ 应该最小, 给出数值大于或等于零的松弛因子 $\xi_i \geq 0$ 和 $\xi_i^* \geq 0, i = 1, 2, \dots, n$, 则 SVM 的优化目标问题为:

$$\min(\frac{1}{2} \omega^T \omega + C \sum_{i=1}^n (\xi_i + \xi_i^*)) \quad (3)$$

s. t.

$$\begin{cases} y_i - \omega \cdot x_i - b \leq \varepsilon + \xi_i \\ \omega \cdot x_i + b - y_i \leq \varepsilon + \xi_i^* \\ \xi_i, \xi_i^* \geq 0 \end{cases} \quad (4)$$

惩罚因子 $C > 0$, 利用拉格朗日乘子求解, 即:

$$\begin{aligned} L(\omega, \xi_i, \xi_i^*) = & \frac{1}{2} \|\omega\|^2 + c \sum_{i=1}^n (\xi_i + \xi_i^*) - \\ & \sum_{i=1}^n \alpha_i (\varepsilon + \xi_i - y_i(\omega \cdot x) + b) - \\ & \sum_{i=1}^n \alpha_i^* (\varepsilon + \xi_i^* - y_i(\omega, x_i) + b) - \\ & \sum_{i=1}^n \eta_i \xi_i + \eta_i^* \xi_i^* \end{aligned} \quad (5)$$

分别对该函数的 $\omega, b, \xi_i, \xi_i^*$ 求偏导:

$$\begin{cases} \frac{\partial L}{\partial \omega} = \sum_{i=1}^n \omega - \sum_{i=1}^n (\alpha_i - \alpha_i^*) x = 0 \\ \frac{\partial L}{\partial b} = \sum_{i=1}^n (\alpha_i - \alpha_i^*) x_i = 0 \\ \frac{\partial L}{\partial \xi_i} = C - \alpha_{i-\eta} = 0 \\ \frac{\partial L}{\partial \xi_i^*} = C - \alpha_i^* - \eta_i^* = 0 \end{cases} \quad (6)$$

并满足:

$$\begin{cases} \alpha_i (\varepsilon + \xi_i - y_i + \omega \cdot x + b) = 0 \\ \alpha_i^* (\varepsilon + \xi_i^* - y_i + \omega \cdot x + b) = 0 \\ (C - \alpha_i) \xi_i = 0 \\ (C - \alpha_i^*) \xi_i^* = 0 \end{cases} \quad (7)$$

把式 6 代入式 4 获取优化目标函数, 给出 $K(x_i, x_j)$ 核函数来替换点积运算:

$$\min \frac{1}{2} \sum_{i=1}^n y_i (\alpha_i - \alpha_i^*) (\alpha_j - \alpha_j^*) K(x_i, x_j) - \sum_{i=1}^n \alpha_i (\alpha_i - \alpha_i^*) + \sum_{i=1}^n \varepsilon (\alpha_i - \alpha_i^*) \quad (8)$$

s. t.

$$\begin{cases} \sum_{i=1}^n \varepsilon (\alpha_i - \alpha_i^*) = 0 \\ \alpha_i, \alpha_i^* \in [0, C], i = 1, 2, \dots, n \end{cases} \quad (9)$$

于是, 问题就变为二次规划问题, 解该问题得到:

$$f(x) = \sum_{i=1}^n (\alpha_i - \alpha_i^*) K(x_i, x) + b, \alpha_i, \alpha_i^* \neq 0 \quad (10)$$

鉴于在支持向量机核函数中使用高斯核函数较好, 对高斯核函数做如下设定:

$$k(x, x_i) = \exp\left(-\frac{|x - x_i|^2}{\sigma^2}\right) \quad (11)$$

支持向量机预测模型如下:

$$f(x) = \sum_{i=1}^n (\alpha_i - \alpha_i^*) \exp\left(-\frac{|x - x_i|^2}{\sigma^2}\right) + b \quad (12)$$

其中, σ 表示高斯核函数宽度。

2.3 改进的粒子群优化算法

用 SVM 能从庞杂的网络安全因素中找出规律, 足以说明其对网络安全态势预测的有效性, 而传统确定 SVM 参数的方法如网络搜索法、穷举法及经验法存在耗时长、难以找到最优参数、模型的预测精度较低等问题, 分析前期对 SVM 用于网络安全态势预测的研究, 发现 SVM 参数的优化问题是决定预测精度的关键。支持向量机的主要参数有: 核函数的宽度 σ , 非线性问题最优解的复杂度用 σ 确定, σ 的取值关系支持向量机的泛化能力; 惩罚因子 C , 是过学习还是欠学习由 C 的取值过大或过小决定; 不敏感损失函数 ε , 支持向量数目和计算复杂度由 ε 确定, 其表示训练时的误差期望。支持向量机主要参数的选取决定其预测精度, 文中采用改进的粒子群优化算法对这三个参数进行优化。

粒子群优化算法 (PSO) 是以无体积无质量的粒子为个体, 且规定了单个粒子的行为, 使得整个粒子群特征表现多样化, 以粒子个体间的协作得到最优解。粒子群优化算法是一种全局优化进化算法, 有着进化初期需要调整的参数少、容易实现、概念简单、快速收敛等特征。但用 POS 优化 SVM 的三个主要参数时发现, 粒子群中当单个粒子搜索到某个局部最优解时会影响到其周围的其他寻优粒子, 导致它们快速靠近该粒子, 这样就会出现局部最优解及粒子早熟等问题。针对该问题, 引入了混沌优化算法对粒子群优化算法做了改进, 混沌优化算法具有全局性的优点, 其可以按某种规则一次性搜索一定范围内的所有情况, 当粒子群出现部分收敛后, 再按照粒子群变化的适应情况对粒子群最优值及情况差的粒子进行混沌变异, 使粒子

群优化算法避开部分最优的能力得到进一步的提高。

文中充分综合两种算法的优点计算 SVM 的三个参数。用混沌优化算法在参数选取时能使用普遍的参数选取法,不用考虑模型的变量维数和复杂度的特性,再利用混沌理论的规律性、遍历性、随机性等特点有效地解决了用 PSO 算法优化时出现的局部最优解及粒子早熟的问题,也就是用混沌变异算子对粒子群优化算法进行必要的改进,即在粒子群进化中确定粒子是否早熟依据粒子群适应度最优变化情况,若变化不大于确定值时,则对粒子群中优胜粒子的位置与速度进行更换,再用混沌变量映射非优胜粒子,然后把替换了的优胜粒子与使用混沌优化后的非优粒子组成新种群;使用混沌优化法对此时全局最优值进行扰动,以便增加寻找全局最优解的几率,使得粒子群经过本操作后避开出现局部最优优点的问题。粒子的速度与位置经混沌变量随机性初始化后,种群的遍历性及多样性得到进一步的提高。

2.4 提出的网络安全态势预测方法的预测步骤

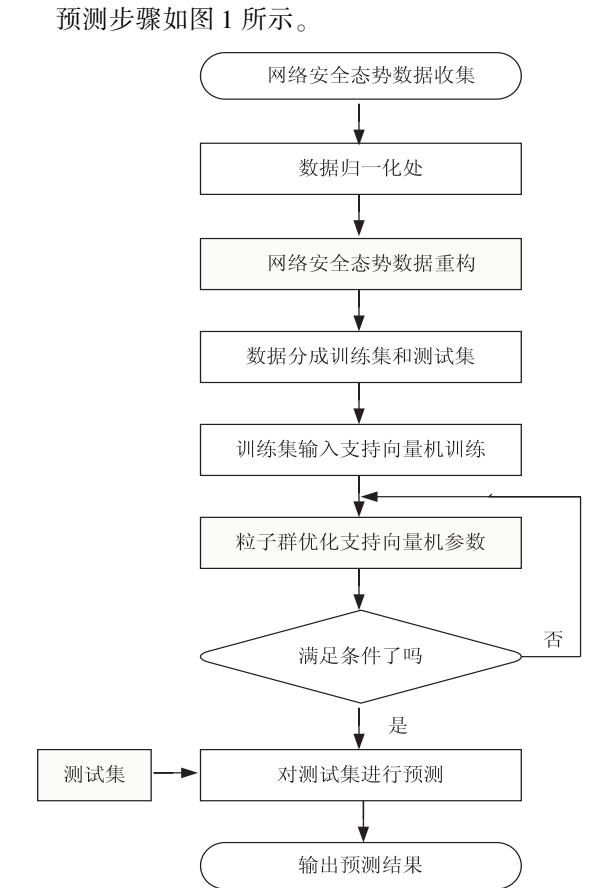


图 1 网络安全态势预测

(1)收集、整理网络安全态势数据,量化处理网络安全监测数据。

(2)数据归一化处理,影响网络安全态势的因素众多,有时收集到的数据差异明显,而支持向量机数据预测敏感区在(0,1)之间,故需要在(0,1)之间归类原

始的网络安全态势数据。

(3)在前两步的基础上,通过确定嵌入维数和时间延迟将一维的网络安全态势数据转换为多维样本态势数据。

(4)把获得的样本数据分为测试集与训练集两部分,把训练集数据输入 SVM 学习。

(5)SVM 主要参数的优化采用改进的粒子群优化算法,实现用最优参数建立预测模型。

(6)对测试集使用建立的预测模型进行预测,完成反归一化预测结果等处理,再依据得到的处理数据预测网络安全态势。

3 实验分析

3.1 网络安全态势数据的选取

选取某公司 2017 年 3 月 1 日 - 4 月 29 日和 5 月 1 日 - 6 月 29 日的安全测试数据,每天取样 4 回,安全测试数据按两月为一批,通过计算后每批各获得 240 个态势值,以相同的过程分别对两批数据进行实验,通过 MATLAB 7.5 进行实验。

3.2 预测网络安全态势模型的实现

累加所得的各组态势值,以获得新数据样本,实行归一化处理新数据样本。把 NSSA 时间延迟设定为 1,用试凑法得到的嵌入维数为 6,这样 SVM 就有了 1 个输出变量和 5 个输入变量,最后通过嵌入维数与延迟时间对获得的数据进行重构,生成 SVM 的测试集与训练集样本,再将生成的训练集样本数据输入到预测模型中学习。预测模型为改进的粒子群优化后的 SVM。

3.3 网络安全态势的预测

对文中所给网络安全态势预测模型进行通用性与有效性的检验。采用上述获得的两组重构数据,将未改进的 PSO-SVM 模型与改进后的模型分别进行预测,然后比较两种模型所得的预测结果。具体操作方法为:

(1)先将两组重构数据的前 200 个点作为训练样本,用于两种方法的训练及模型的构建;两组数据的后 40 个点作为测试样本,用于将两种模型的预测结果与实际值进行比较;

(2)分别将两组重构数据的训练样本输入 SVM 进行学习,SVM 的三个参数用改进的粒子群优化算法进行优化,获得第一批数据时 $\sigma = 5$, $\varepsilon = 0.001$, $C = 98$,第二批数据时 $\sigma = 5$, $\varepsilon = 0.001$, $C = 76.12$;

(3)用两组数据所获得的三个参数再分别将两组重构数据输入到支持向量机进行学习、训练,得到新模型的预测结果;

(4)如图 2 所示,比对未经处理的原始值、文中所

给方法得到的预测结果及未改进 PSO-SVM 得到的预测结果,比较误差如图 3 所示。

络安全威胁。

参考文献:

- [1] BASS T. Intrusion systems and multisensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.
- [2] HUBBALLI N, BISWAS S, NANDI S. Network specific false alarm reduction in intrusion detection system[J]. Security and Communication Networks, 2011, 4(11): 1339-1349.
- [3] KOTT A, WANG C, ERBACHER R F. Cyber defense and situational awareness [M]. [s. l.]: Springer International Publishing, 2014.
- [4] 陈秀真, 郑庆华, 管晓宏, 等. 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.
- [5] 韦 勇, 连一峰, 冯登国. 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.
- [6] 刘效武, 王慧强, 吕宏武, 等. 网络安全态势认知融合感控模型[J]. 软件学报, 2016, 27(8): 2099-2114.
- [7] BOSER B, GUYON L, VAPNIK Y. A training algorithm for optimal margin classifier [C]//Fifth annual workshop on computational learning theory. [s. l.]: [s. n.], 1992: 144-152.
- [8] 张小龙, 刘书炘, 刘满华, 等. 基于级联支持向量机融合多特征的人脸检测[J]. 计算机应用与软件, 2016, 33(4): 151-154.
- [9] 安金龙, 王正欧, 马振平. 一种新的支持向量机多类分类方法[J]. 信息与控制, 2004, 33(3): 262-267.
- [10] LIN V L, HSIEH J G, WU H K, et al. Three-parameter sequential minimal optimization for support vector machines [J]. Neurocomputing, 2011, 74(17): 3467-3475.
- [11] 权 文, 王晓丹, 王 坚, 等. 基于 SVM 概率输出与证据理论的多分类方法[J]. 计算机工程, 2012, 38(5): 167-169.
- [12] HSU C W, LIN C J. A comparison of methods for multiclass support vector machines [J]. IEEE Transactions on Neural Networks, 2002, 13(2): 415-425.
- [13] 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, 33(11): 10-12.
- [14] 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.

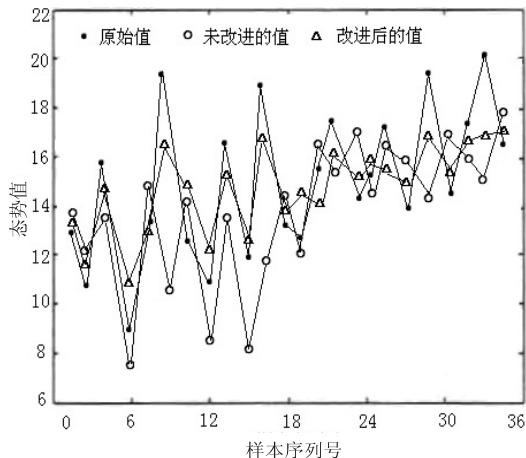


图 2 三种数据比较

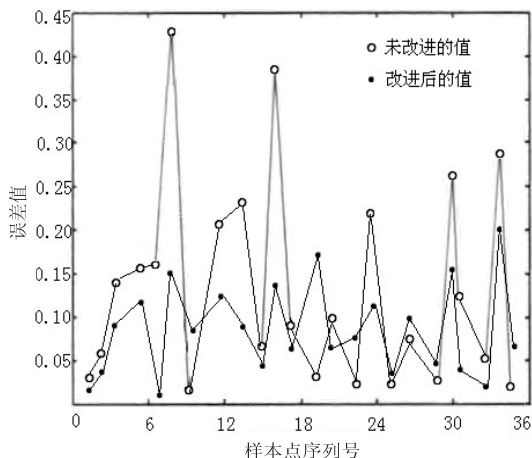


图 3 两种方法误差比较

结果表明,采用文中给出的网络安全态势预测方法,预测未来的网络安全状态精度高、误差小。

4 结束语

给出的采用支持向量机与改进粒子群优化算法相结合的网络安全态势预测方法,是基于实际问题展开的,理论基础深厚、可实施性强。实验结果表明,该方法进一步提高了网络安全预测的精确度及有效性。应用给出的网络安全态势预测模型,能对先前网络安全态势的变化趋势做出准确、客观的评估,很好地预测了后续的网络安全态势,便于网络管理者更好地应对网