一种基于 GSA-SVM 网络安全态势预测模型

陈玉鑫，殷肖川✉，谭　韧
(空军工程大学信息与导航学院，西安，710077)

摘要　针对支持向量机的参数选择问题，结合引力搜索算法(GSA)需要设置的参数少以及全局优化能力强的特点，提出了一种 GSA 优化 SVM 参数的网络安全态势预测模型(GSA-SVM)。首先把 SVM 的参数视作在空间中的物体，并将 SVM 在该参数下预测产生的预测值和实际值之间的均方误差 mse 作为目标优化函数，然后 GSA 通过模拟万有引力规律影响下物体的运动规律不断变化参数，最终找到 SVM 最优参数。最后根据最优参数建立网络安全态势预测模型。在 Matlab 平台采用 MIT Lincoln 实验室提供的 DARPA 1999 数据集进行仿真测试，仿真结果表明：相对于其它预测算法，GSA-SVM 提高了网络安全态势预测的准确度，加快了网络安全态势预测的速度，为网络安全态势预测提供了一种新的解决途径。

关键词　网络安全态势预测；支持向量机；引力搜索算法
DOI　10.3969/j.issn.1009-3516.2018.05.014
中图分类号　TP393.08　　**文献标志码**　A　　**文章编号**　1009-3516(2018)05-0078-06

A Network Security Situation Prediction Method Based on GSA-SVM

CHEN Yuxin, YIN Xiaochuan✉, TAN Ren
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: In order to more accurately master the laws of network security situation regular and prevent some network security threats, in view of the problem of parameter selection of Support Vector Machines, plus, the gravitational search algorithm (GSA) is characterized by few parameters needed and having great ability in global optimization, a network security situation prediction model (GSA-SVM) is proposed for GSA optimization SVM parameters. First, the parameters of SVM are treated as objects in space, and mean square error (MSE) of predicted value and actual value of SVM under this parameter is used as the objective optimization function, then GSA can find the optimal parameters of the SVM by simulating the law of gravitation, and finding the optimum parameter eventually. Finally, a network security situation prediction model is established according to the optimal parameters. Using DARPA 1999 data set provided by MIT Lincoln Laboratory in MATLAB platform, the simulation results show that GSA-SVM improves the accuracy of network security situation prediction and accelerates prediction of network security situation relative to other prediction algorithms. This provides a new way to solve problem of network security situation prediction.

Key words: network security situation awareness; SVM; gravitational search algorithm

收稿日期：2017-11-16
基金项目：国家自然科学基金(71503260)；陕西省工业科技攻关项目(2016GY-087)
作者简介：陈玉鑫(1993—)，男，甘肃临夏人，硕士生，主要从事网络与信息安全研究。E-mail：867433386@qq.com
通信作者：殷肖川(1961—)，男，湖北武汉人，教授，主要从事网络与信息安全、数字水印研究。E-mail：redstorm@live.cn

引用格式：陈玉鑫，殷肖川，谭韧. 一种基于 GSA-SVM 网络安全态势预测模型[J]. 空军工程大学学报(自然科学版)，2018，19(5)：78-83.
CHEN Yuxin, YIN Xiaochuan, TAN Ren. A Network Security Situation Prediction Method Based on GSA-SVM[J]. Journal of Air Force Engineering University (Natural Science Edition), 2018, 19(5): 78-83.

随着网络规模的增大，以及网络安全事件层出不穷，采取传统的网络安全措施会耗费大量的人力和物力，面对威胁时会很被动。网络安全态势预测[1-2]是网络安全态势感知中最关键的技术，首先是获取网络安全态势评估后得到的态势值，该值是用来反映当前网络安全状态，了解这些态势值的变化规律可以预测未来态势值的变化情况，可以让网络安全管理员提前感知到网络安全状态的变化方向，发现潜在的威胁，并有时间采取相应措施去预防，提高网络安全防护水平。态势值又相当于时间序列，可将研究的重点转向时间序列预测上来。时间序列预测本质上是回归问题，并且还具有非线性、时变性等特点。

时间序列预测方法预测精度低，不易描述数据之间过去和未来状态之间的联系。之后的神经网络[3]、证据理论[4]、支持向量机[5-6](SVM)等网络安全态势预测算法，在预测精度上都有所提高。SVM 与其它算法比较，具有收敛速度快、不易陷入局部寻优等优点。但参数选择往往没有相应的理论，需依靠大量经验和不断的尝试，耗费大量的时间。为优化参数，出现如遗传算法(GA)[7]、粒子群算法(PSO)[8]等各种优化算法与 SVM 相结合的预测模型。2009 年 Rashedi 等提出引力搜索算法(GSA)[9]是受物体间所受万有引力而运动的规律的启发，设计出的一种新的优化搜索算法，文献[8]中验证了其全局优化能力明显优于 PSO 算法。

因此针对态势预测中的预测精度问题，提出一种用 GSA 优化 SVM 参数的网络安全态势预测模型，该模型结合 GSA 需要设置的参数少以及全局优化能力强的特点，优化 SVM 参数。建立预测模型的预测效果优于 PSO-SVM 的预测模型。

1　相关理论

1.1　引力搜索算法

引力搜索算法(GSA)基本原理是万有引力定律，并假设在空间中所有粒子是有质量的，所在空间粒子不受任何阻力影响，在引力的作用下粒子之间不断靠近。所受引力大小与粒子间距离的平方成反比，惯性质量的乘积成正比。粒子间的引力作用表示为：

$$F=G\frac{M_1M_2}{R^2} \tag{1}$$

式中：F 是引力大小；G 是引力常数；M_1 和$_2$ 分别为两粒子的惯性质量；R 为两粒子之间的欧式距离。文献[10]指出在引力算法中用 R 替代 R^2 效果会更好。

粒子加速度受到力的作用后产生，加速度 $\boldsymbol{a}$ 定义如下：当一粒子受到力为 F，那么这个粒子的加速度取决于所受作用力和其本身的惯性质量 M，其计算公式为：

$$\boldsymbol{a}=\frac{F}{M} \tag{2}$$

假设有 N 个粒子，粒子 i 的位置在：

$$X_i=(x_i^1,x_i^2,\cdots,x_i^d,\cdots,x_i^n)\quad i=1,2,\cdots,N \tag{3}$$

式(3)中，粒子 i 在第 d 维空间中的位置为 x_i^d。粒子 i 在 t 时刻第 d 维受到粒子 j 的作用力为：

$$F_{ij}^d(t)=G(t)\frac{M_i(t)M_j(t)}{R_{ij}(t)+\varepsilon}(x_j^d(t)-x_i^d(t)) \tag{4}$$

式中：M_i 和 M_j 分别为粒子 i 和 j 的惯性质量$R_{ij}(t)$ 为粒子 i 和 j 的距离；$G(t)$为引力常量；ε 为很小的常量。

引力常量的计算遵从：

$$G(t)=G_0e^{-a\frac{t}{T}} \tag{5}$$

式中：初始引力常数为 G_0，$a\in[20,30]$；T 为最大迭代次数。

粒子 i 在时刻 t 受到其他粒子的引力为：

$$F_i^d(t)=\sum_{j=1,j\neq i}^{N}rand\ F_{ij}^d \tag{6}$$

在第 d 维粒子 i 对应的的加速度为：

$$a_i^d(t)=\frac{F_i^d(t)}{M_i(t)} \tag{7}$$

粒子 i 惯性质量 $M_i(t)$计算公式：

$$m_i(t)=\frac{f_i(t)-f_{\text{worst}}(t)}{f_{\text{best}}(t)-f_{\text{worst}}(t)}$$

$$M_i(t)=m_i(t)/\sum_{i=1}^{N}m_i(t) \tag{8}$$

式中：$f_i(t)$表示粒子 i 在 t 时刻的适应度函数值；$f_{\text{worst}}(t)$、$f_{\text{best}}(t)$分别为分别为 t 时刻整个粒子群最差适应度函数值和粒子群最佳适应度函数值。

粒子 i 在第 d 维的速度 $v_i^d(t)$和位置 $x_i^d(t)$分别表示为：

$$v_i^d(t)=rand\ v_i^d(t-1)+a_i^d(t) \tag{9}$$

$$x_i^d(t)=x_i^d(t-1)+v_i^d(t) \tag{10}$$

每次迭代过程中计算新的位置和速度后，转入下一次迭代，直到满足最大的迭代次数或者满足指定精度即可结束。

1.2　SVM 非线性回归预测原理

SVM 作为以统计学习理论[11]为原则实现的算法，在解决非线性、小样本等问题时很有效。SVM 非线性回归预测结合结构风险最小化理论[12]和 VC 维理论[13]，处在低维度的输入空间的数据 x 经过映射后处在高维特征空间，在高维特征空间进行线性

回归,构造最优决策函数。线性回归函数:

$$f(x)=\boldsymbol{w}^{\mathrm{T}}\phi(x)+b \tag{11}$$

采用 ε 不敏感损耗函数进行优化,通过函数的最小值寻找最优的回归函数:

$$\min\frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w}+C\sum_{i=1}^{n}(\xi_i+\hat{\xi}_i) \tag{12}$$

式中:C 是惩罚系数,即对误差的容忍度。C 越高,误差容忍度越差,同时会出现过拟合现象。C 取值若越小则相反,会造成欠拟合。选取的 C 过大或者过小其泛化能力都会受到影响。

约束条件:

$$\begin{cases}y_i-[\boldsymbol{w},\phi(x_i)]-b\leqslant\xi_i+\varepsilon\\ [\boldsymbol{w},\phi(x_i)]+b-y_i\leqslant\xi_i+\varepsilon\\ \xi_i\geqslant0,\hat{\xi}_i\geqslant0\end{cases} \tag{13}$$

式中:b 为偏移量;ε 为不敏感损耗函数;ξ_i、$\hat{\xi}_i$ 为松弛变量。

经二次规划后所获得的非线性回归函数:

$$f(x)=\sum_{i=1}^{n}(\beta_i-\beta_i^*)K(x_gx_i)+b \tag{14}$$

式中:支持向量机的核函数为 $K(x_gx_i)$,β_i、β_i^* 为拉格朗日乘子[14],非线性核函数选取 RBF[15] 作为核函数。

$$K(x_gx_i)=\exp\left\{-\frac{|x-x_i|^2}{\sigma^2}\right\} \tag{15}$$

gamma 是 RBF 函数中的一个参数。其值的选取影响着数据映射到新的特征空间后的分布,取值越大,支持向量越少,相反取值越小,支持向量越多。支持向量的个数又潜在地决定着训练与预测的速度。

RBF 公式里面的 gamma(简记为 g)如下:

$$k(x,z)=\exp(-\frac{d(x,z)^2}{2\sigma^2})=\exp(-g\,d(x,z)^2)\Rightarrow g \tag{16}$$

因此需要在 SVM 中进行参数寻优的参数分别为:误差惩罚系数 C 和核参数 gamma 其中,惩罚系数 C 掌握着分类间隔和允许样本之间误差的比例。核参数 g 主要在高维空间中影响样本数据间的分布。

2 网络安全态势预测模块

网络安全态势预测之前,需先对网络进行网络安全态势评估,态势评估是把与网络安全相关的多个属性值得到映射,将指标量化后的从整体上可反映当前网络安全状态。因此网络安全态势预测模块主要由 2 个部分组成:①网络安全态势评估模块;②网络安全态势预测。

2.1 网络安全态势评估

网络安全态势评估[16-17] 的过程是采用某种评估算法把当前时刻统计得到的各种影响网络安全的指标如带宽变化、用户访问该服务频率等进行融合,从宏观层面上反映总体安全状态变化的过程。本文根据文献[18]中的评估方法,采用层次化的评估方式。如图所示,该模型采取从下到上,先局部后全局的评估方式,从下到上分为攻击/漏洞层、服务层、主机层和网络层 3 个层次。

2.1.1 服务层评估

某个服务受到威胁主要与针对该服务的正常访问量、漏洞的脆弱性和受到攻击相关。定义 t 时刻服务 S_j 的威胁指数 $R_{S_j}(t)$ 为:

$$R_{S_j}(t)=f(\boldsymbol{\theta},\boldsymbol{C}_j(t),\boldsymbol{D}_j(t),\boldsymbol{N}(t),\boldsymbol{D}_D)=\boldsymbol{\theta}(\boldsymbol{C}_j(t)10^{\boldsymbol{D}_j(t)}+100\boldsymbol{N}(t)10^{\boldsymbol{D}_D}) \tag{17}$$

式中:$\boldsymbol{\theta}=(\theta_1,\theta_2,\cdots,\theta_h)$ 为用户访问向量,h 为一天之内所划分时间段,例如 $h=\{1,2,3\}$ 分别表示早(6:00~12:00)、中(12:00~18:00)、晚(18:00~24:00);F_i,$i=1,2,\cdots,h$ 表示在时间段 i 用户访问量。θ_i 和 F_i 关系如下:

$$\theta_i=\frac{F_i}{\sum_{i=1}^{h}F_i} \tag{18}$$

式中:$\boldsymbol{D}_j(t)=\{D_{ij}(t),D_{2j}(t),\cdots,D_{hj}(t)\}$、$\boldsymbol{C}_j(t)=\{C_{1j}(t),C_{2j}(t),\cdots,C_{hj}(t)\}$ 分别表示在 t 时刻遭受的威胁程度和遭受攻击的次数向量,$D_{ij}(t)=(D_{ij1},D_{ij2}\cdots,D_{iju})$,$C_{ij}(t)=(C_{ij1},C_{ij2}\cdots,C_{iju})$($i=1,2,\cdots,h$)表示第 i 时间段内 $t\sim t+\Delta t$ 的时间内,服务 S_j 遭受的威胁程度和所受攻击的次数,u 为 Δt 时间内攻击种类数,u 和 $\boldsymbol{C}_{ij}$ 的取值可以从攻击事件日志数据库中统计获得。$\boldsymbol{N}(t)=(N_1,N_2,\cdots,N_h)$ 为网络带宽占有率,$\boldsymbol{D}_D=(D_{D_1},D_{D_2},\cdots,D_{D_h})$($i=1,2,\cdots,h$)为遭受 DOS 攻击程度级别向量。$\boldsymbol{N}_i=(N_{i1},N_{i2},\cdots,N_{iv})$,$\boldsymbol{D}_{D_i}=(D_{D_{i1}},D_{D_{i2}},\cdots,D_{D_{iv}})$($i=1,2,\cdots,h$)分别为在第 i 时段网络带宽占用率和遭受 DOS 攻击程度级别,v 为在第 i 个时段内的分析时间窗口数。该服务受到威胁的程度随着 R_{S_j} 的值增大而变高。

2.1.2 主机层评估

对应某主机 H_k 存在的各类服务为 $\boldsymbol{S}_{H_kj}=\{S_1,S_2,\cdots,S_j\}$,$j$ 表示服务种类,不同类型服务对应的权重为 $\boldsymbol{V}=\{V_1,V_2,\cdots,V_j\}$,则对应主机威胁指数为:

$$R_{H_K}=\boldsymbol{V}\cdot\boldsymbol{S}_{H_kj} \tag{19}$$

2.1.3 网络层评估

某网络 $W=\{1,2,\cdots,n\}$,n 为主机号,其中某主机 i 的重要程度 I_i 受到对该主机访问量 F_i 的影响,定义重要性和访问量之间的关系:

$$I_i = F_i / \sum_{i=1}^{n} F_i \tag{20}$$

整个网络层所受的威胁值为 $R_W = I_i R_{H_i}$，并作为整个网络的态势值。

2.2　网络安全态势预测

选取态势值进行网络安全态势预测，态势值输入到 SVM，利用 GSA 参数寻优，寻优所得结果生成训练模型，适应度函数为训练预测值与实际值的均方误差 e_{ms}，e_{ms} 定义如下：

设 n 个训练预测值与实际值的误差为 ε_1、ε_2、…、ε_n 则：

$$e_{\mathrm{ms}} = \frac{\varepsilon_1^2 + \varepsilon_2^2 + \cdots, + \varepsilon_n^2}{n} \tag{21}$$

GSA 在迭代过程中终止条件的判断：是否满足最小精度或者是否到最大迭代次数。若满足则最终条件则该参数最终确定，并用于生成最优的网络安全态势预测模型。

检验预测效果算法归纳如下：

Step 1　经过态势评估后得到态势值样本 $\{E_1, E_2, \cdots, E_n\}$；

Step 2　选取前 $n-m$ 个态势值作为训练样本进行训练，用 GSA 参数寻优得到合适的参数生成训练模型；

Step 3　将训练所得模型用于预测获得后 m 个态势预测值：$\{\hat{E}_{n-m+1}, \hat{E}_{n-m+2}, \cdots, \hat{E}_n\}$；

Step 4　计算 e_{ms}，评估准确性。

3　实验验证

3.1　数据采集

为了验证 GSA-SVM 的态势预测效果，搭建实验环境拓扑见图 1，多台攻击机和 3 台分别开启 WWW、FTP 和 E-mail 服务的检测端的主机。攻击机使用 MIT Lincoln 实验室提供的 DARPA 1999 数据集[19-20]的部分数据，该数据集含有 DoS、R2L、U2R 和 Probe 4 类攻击。使用 tcpdump 命令发送数据包至检测端。在装有不同服务的检测端主机上使用 snort[21] 进行监控，不同主机上开放各种不同等级漏洞，设置相对应的报警规则，并记录触发相应报警的起止时刻。同时需记录检测端不同时刻对应端口带宽占用率变化，以及访问该服务的时刻。不同时刻之间的间隔为 1 h，以期得到用户访问量、遭受的威胁程度和遭受攻击的发生次数。采集后得到某一天从 6：00 开始到 24：00结束的 FTP 主机的威胁指数见图 2，可以看出攻击在早晨持续了 5 h 在 11：00 后到 14：00 之间趋于平稳，之后又持续进行攻击直到 20：00 后趋于平稳，说明该攻击活跃的时刻符合该攻击者的作息规律。网络管理员可以依此在攻击频繁发生的时间段内采取更高级别的安全防护措施。在攻击较弱的时间段内采取基本的防护措施。

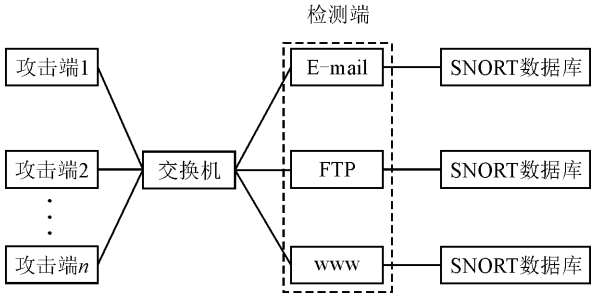

图 1　实验所用拓扑

Fig. 1　Topology of experiment

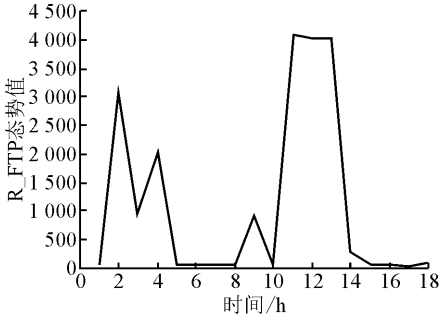

图 2　FTP 威胁指数

Fig. 2　Threat index of FTP

3.2　2 种算法迭代性能比较

为比较 GSA 和 PSO 迭代性能的不同，参照文献[22]中的测试方法，选用 Eggcrate 函数进行测试，见图 3。该函数有多个极值点，一个最小值，位于(0，0)，值为 0。GSA 和 PSO 初始粒子分布范围为 $x \in (-10, 10)$，$y \in (-10, 10)$，使用 matlab 运行 GSA，PSO 算法各 50 次，每一次运行 GSA 和 PSO 种群规模和最大迭代次数一致，如表 1。运行后的结论中 GSA 迭代寻优得到的最佳点的精度优于 PSO，见图 4～6，即 GSA 更靠近(0，0)点。

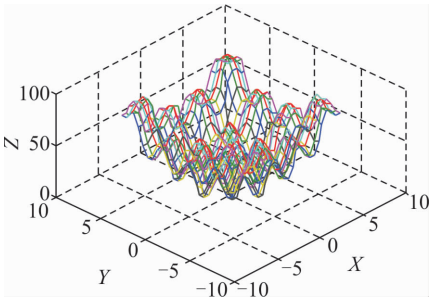

图 3　Eggcrate 函数

Fig. 3　Function of Eggcrate

表 1 GSA 和 PSO 参数

Tab. 1 Parameters of GSA and PSO

参数	GSA	PSO
种群规模	20	20
最大迭代次数	100	100

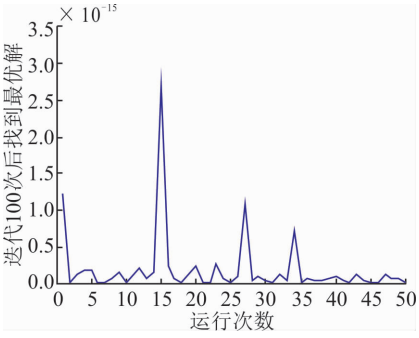

图 4 引力搜索算法最优解

Fig. 4 Optimum solution of GSA

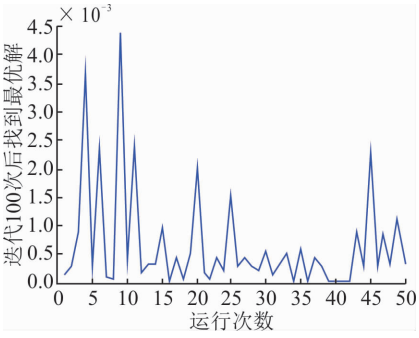

图 5 粒子群算法最优解

Fig. 5 Optimum solution of PSO

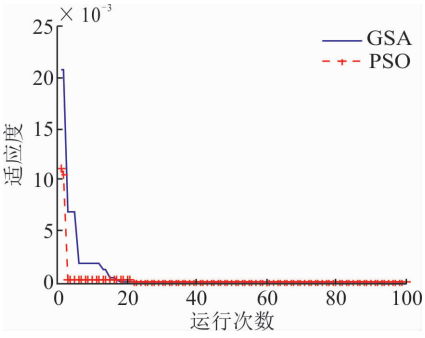

图 6 单次运行 PSO 和 GSA 适应度变化

Fig. 6 Fitness change between PSO and GSA of single operation

3.3 态势预测效果比较

采集从某 1 d 开始到第 103 d 的该网络的态势数据作为检测预测效果的数据集,由于数据的值跳动比较大,因此首先进行归一化:

$$\overline{x_i}=\frac{x_i-\min(x_i)}{\max(x_i)-\min(x_i)} \tag{22}$$

归一化后的属性值$\overline{x_i}\in[0,1]$。

将数据集分为训练集和预测集,训练集是从第 1 d 到第 80 d 的数据,预测集是从第 81 d 到第 103 d 的数据,使用 GSA-SVM 和 PSO-SVM 进行比较,比较过程中使用 2 种算法分别用训练集训练出各自的回归预测模型,训练得到的参数见表 2。用所训练得到模型预测 81～103 d 之间的数据,分别计算 2 种算法的 e_{ms} 的值,则 PSO 为 0.012 2,GSA 为 0.001 5,GSA 误差较 PSO 小,见图 7。GSA 预测的精度优于 PSO,之后进行反归一化,得到的结果见图 8。因此采用 GSA-SVM 可以更加准确地指导网络管理员做出相应的措施。

表 2 GSA、PSO 寻优到的参数 C 和 g

Tab. 2 Parametets C and g searched by GSA, PSO

参数	PSO	GSA
C	94.563 7	84.541 9
g	0.024 4	0.151 5
ε	0.01	0.01

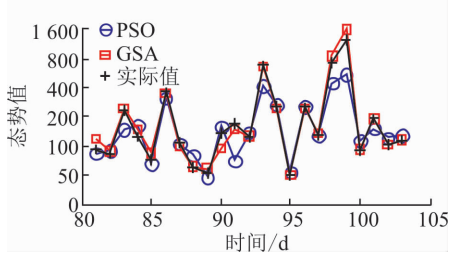

图 7 GSA 和 PSO 比较

Fig. 7 Comparing GSA with PSO

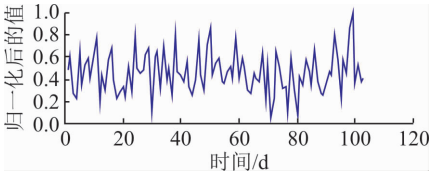

图 8 归一化后的数据

Fig. 8 Normalized data

4 结语

网络安全态势预测处在网络安全态势感知中的关键环节,本文提出了一种 GSA 优化 SVM 参数的网络安全态势预测模型,实验结果表明,相比于 PSO-SVM 态势预测模型,GSA-SVM 预测效果更好。预测结果可以更好地反映网络安全态势感知规律,更准确地指导网络管理员对网络安全做出有效的措施。

参考文献(References):

[1] CHEN W P, ZHI-GANG A O, YI-QIANG T U, et al. Network Situation Awareness Model Prediction Method Based on Genetic Optimization Support Vector Machine[C] // International Conference on Computer

Networks and Communication Technology. 2017.

[2] 文志诚，陈志刚，唐军，等. 基于时间序列分析的网络安全态势预测[J]. 华南理工大学学报(自然科学版)，2016，44(5)：137-143，150.
WEN Z C，CHEN Z G，TANG J，et al. Prediction of Network Security Situation on the Basis of Time Series Analysis[J]. Journal of South China University of Technology(Natural Science Edition)，2016，44(5)：137-143，150. (in Chinese)

[3] 邓勇杰，文志诚，姜旭炜. 基于灰色理论和 BP 神经的网络安全态势预测[J]. 微型机与应用，2015(20)：1-3.
DENG Y J，WEN Z C，JIANG X W. The Network Security Situation Prediction Based on Grey and BP Neural Network[J]. Microcomputer & Its Applications，2015(20)：1-3. (in Chinese)

[4] 石波，谢小权. 基于 D-S 证据理论的网络安全态势预测方法研究[J]. 计算机工程与设计，2013，34(3)：821-825.
SHI B，XIE X Q. Research on Network Security Situation Forecast Method Based on D-S Evidence Theory [J]. Computer Engineering and Design，2013，34(3)：821-825. (in Chinese)

[5] APOLLONI B，BASSIS S，MALCHIODI D. SVM with Random Labels[C]//Proceeding KES'07. Vietri sul Mare，Italy：Springer-Verlay Berlin，Heidelberg，2007：184-193.

[6] 张青松. 基于支持向量机的网络安全态势预测[D]. 大连：大连海事大学，2015.
ZHANG Q S. Network Security Situation Prediction Based on Support Vector Machine[D]. Dalian：Dalian Maritime University，2015. (in Chinese)

[7] 杨旭，纪玉波，田雪. 基于遗传算法的 SVM 参数选取[J]. 辽宁石油化工大学学报，2004，24(1)：54-58.
YANG X，JI Y B，TIAN X. Parameters Selection og SVM Based on Genetic Algorithm[J]. Journal of Liaoning University of Petroleum & Chemical Technology，2004，24(1)：54-58. (in Chinese)

[8] LONG Z，XUE M S，MING W Z. A Shot Boundary Detection Method Based on PSO-SVM[J]. Applied Mechanics and Materials，2012，130：3821-3825.

[9] RASHEDI E，NEZAMABADI-POUR H，SARYAZDI S. GSA：A Gravitational Search Algorithm[J]. Information Sciences，2009，179 (13)：2232-2248.

[10] 徐遥，王士同. 引力搜索算法的改进[J]. 计算机工程与应用，2011，47(35)：188-192.
XU Y，WANG S T. Enhanced Version of Gravitational Search Algorithm：Weighted GSA[J]. Computer Engineering and Application，2011，47(35)：188-192. (in Chinese)

[11] VAPNIK V. The Nature of Statistical Learning Theory[M]. New York：Springer-Verlag，1995：123-167.

[12] ROY K，BOAZ L. Learning Bayesian Network Classifiers by Risk Minimization[J]. International Journal of Approximate Reasoning，2012，53(2)：248-272.

[13] KLGSK P，KORZEN M. Sets of Approximating Functions with Finite Vapnik-Chervonenkis Dimension for Nearest-Neighbors Algorithms[J]. Pattern Recognition Letters，2011，32(14)：1882-1893.

[14] 戎海武. 关于拉格朗日乘数法的两点思考[J]. 高等数学研究，2013，16(4)：81-82.
RONG H W. Two Notes on the Method of Lagrange Multipliers[J]. Studies in College Mathematics，2013，16(4)：81-82. (in Chinese)

[15] LIN S L，ZHI L. Parameter Selection in SVM with RBF Kernel Function[J]. Journal of Zhejiang University of Technology，2007，35(2)：123-126.

[16] LIANG Y. An Approximate Reasoning Model for Situation and Threat Assessment [C]// International Conference on Fuzzy Systems and Knowledge Discovery. Haikou，China：IEEE Computer Society，2007：246-250.

[17] 肖道举，杨素娟，周开峰，等. 网络安全评估模型研究[J]. 华中科技大学学报(自然科学版)，2002，30(4)：37-39.
XIAO D J，YANG S J，ZHOU K F，et al. A Study of Evalution Model for Network Security[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition)，2002，30(4)：37-39. (in Chinese)

[18] 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.
CHEN X Z，ZHENG Q H，GUAN X H，et al. Quantitative Hierarchical Threat Evaluation Model for Network Security[J]. Journal of Software，2006，17(4)：885-897. (in Chinese)

[19] DARPA. MIT Lincoln Laboratory 1999 DARPA Intrusion Detection Evaluation Data Set[EB/OL]. [1999-09-01]. https://ll.mit.edu/ideval/data/1999data.html.

[20] LIPPMANN R，HAINES J W，FRIED D J，et al. Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation[J]. International Symposium on Recent Advances in Intrusion Detection，2000，34(4)：162-182.

[21] 宋劲松. Snort 2.0 入侵检测[M]. 北京：国防工业出版社. 2004.
SONG J S. Intrution Detection of Snort 2.0[M]. Beijing：National Defend Industry Press，2004. (in Chinese)

[22] 王文，王勇，王晓伟. 一种具有记忆特征的改进蝙蝠算法[J]. 计算机应用与软件，2014，31(11)：257-259，329.
WANG W，WANG Y，WANG X W. An Improved Bat Algorithm with Memory Characteristic[J]. Computer Applications and Software，2014，31(11)：257-259，329. (in Chinese)

(编辑：徐楠楠)