Journal of System Simulation

Volume 29 | Issue 5 Article 30

6-3-2020

Combination Model of Network Security Situation Prediction Based on Cooperative Games

Ke Gang
Department of Computer Engineering, Dongguan Polytechnic, Dongguan 523808, China;

Combination Model of Network Security Situation Prediction Based on Cooperative Games

Abstract

Abstract: Influenced by a variety of complicated factors, the network security situation has many characteristics, such as highly nonlinear, time-varying, and mutant. It is difficult to predict accurately with a single prediction method. In response to this shortage, a new combined prediction model for network security situation was proposed based on cooperation policy theory. *The network security situation was predicted respectively by using the Elman neural network model, GM(1,1)model, support vector machine (SVM) mode. The Shapley value method of cooperative games was applied to determine the weight of each single prediction model, and the prediction results were weighted calculated to get the final combined prediction results of network security situation.* The actual network security data were used for simulation testing. The simulation results show that combination prediction model can effectively improve the network security situation prediction accuracy.

Keywords

network security situation, Elman neural networks, GM(1, 1), support vector machine(SVM), combination prediction

Recommended Citation

Ke Gang. Combination Model of Network Security Situation Prediction Based on Cooperative Games[J]. Journal of System Simulation, 2017, 29(5): 1153-1159.

第 29 卷第 5 期 系统仿真学报© Vol. 29 No. 5
2017 年 5 月 Journal of System Simulation May, 2017

基于合作对策论的网络安全态势组合预测模型

柯钢
(东莞职业技术学院计算机工程系，广东 东莞 523808)

摘要：网络安全态势受多种复杂因素影响，具有高度非线性、时变性、突变性等特点，使得传统上的单一预测模型存在预测精度低的问题。针对这一不足，结合合作策略论，提出一种新的网络安全态势组合预测模型。*通过 Elman 神经网络模型、GM(1, 1)模型、支持向量机模型分别对网络安全态势进行预测，运用合作对策中的 Shapley 值法，对单一模型的预测结果进行加权运算得到组合预测结果，对真实网络安全态势数据进行仿真测试。*仿真结果表明，组合预测模型有效提高了网络安全态势预测精度。

关键词：网络安全态势；Elman 神经网络；GM(1，1)；支持向量机；组合预测
中图分类号：TP393.08 文献标识码：A 文章编号：1004-731X (2017) 05-1153-07
DOI: 10.16182/j.issn1004731x.joss.201705030

Combination Model of Network Security Situation Prediction Based on Cooperative Games

Ke Gang
(Department of Computer Engineering, Dongguan Polytechnic, Dongguan 523808, China)

Abstract: Influenced by a variety of complicated factors, the network security situation has many characteristics, such as highly nonlinear, time-varying, and mutant. It is difficult to predict accurately with a single prediction method. In response to this shortage, a new combined prediction model for network security situation was proposed based on cooperation policy theory. *The network security situation was predicted respectively by using the Elman neural network model, GM(1,1)model, support vector machine (SVM) mode. The Shapley value method of cooperative games was applied to determine the weight of each single prediction model, and the prediction results were weighted calculated to get the final combined prediction results of network security situation.* The actual network security data were used for simulation testing. The simulation results show that combination prediction model can effectively improve the network security situation prediction accuracy.

Keywords: network security situation; Elman neural networks; GM(1,1); support vector machine(SVM); combination prediction

引言

随着计算机网络应用的深入，网络安全问题日益严重。依靠网络安全设备防火墙、入侵检测的防御方法属于被动防御，只能检测和报告已经发生的攻击行为和异常活动，无法预测下一阶段的网络安全状态。网络安全态势预测通过对网络安相关的要素进行综合分析，从总体上去感知当前网络的安全状态，同时对未来网络安全的状态进行预测，从而减轻网络管理者的数据压力，为决策者提供科学依据，这已经成为网络安全领域的研究热点。

收稿日期：2016-04-25 修回日期：2016-08-11；
基金项目：东莞市社会科技发展项目一般项目(2017507156388)；
作者简介：柯钢(1983-)，男，湖北黄石，硕士，讲师，研究方向为网络安全技术，智能算法。

自网络安全态势的概念被提出以来，国内外的学者对网络安全态势的预测问题进行了不少研究。目前的研究方法，主要有：(1) 基于神经网络的预测模型。谢丽霞[1]和蓝新波等[2]人利用神经网络对网络安全态势进行感知和预测，但神经网络存在参数设置复杂，易陷入局部最小值等缺陷，导致预测结果不理想。(2) 基于灰色关联模型、时间序列分析模型等的统计学预测模型。文献[3]利用灰色关联模型对网络安全态势进行预测，虽然灰色关联模型对网络安全态势的趋势大方向有很好的预测，适用于宏观预测，但是无法精确预测网络安全态势；文献[4]提出了一种基于线性理论的时间序列分析模型对网络安全态势进行预测，由于网络态势变化呈现非线性、突变性等特点，该模型预测的结果有很大误差。(3) 基于 SVM(support vector machine)支持向量机等的机器学习预测模型。文献[5]使用 SVM 支持向量机对网络安全态势进行预测，但是该模型存在参数优化的问题。

由于网络安全态势具有高度非线性、时变性、突变性等特点，采用单一预测模型很难预测准确，综合使用多种预测模型的组合预测模型引起了人们的关注。姚晔[6]提出一种基于熵值法的网络安全态势组合预测模型，综合了自回归预测模型、最小二乘支持向量机预测模型和 BP(Back-Propagation)神经网络预测模型，提高了网络安全态势预测精度。张安楠等[7]从频域的角度对数据分解和重构，提出基于小波变换与 LSSVM-ARIMA(Least Square Support Vector Machine-Autoregressive Integrated Moving Average Model)相结合的网络安全态势预测模型，并通过仿真实验验证了模型的有效性。但是目前的组合预测模型没有考虑指标间的相互影响，且对样本的依赖性较大，导致应用范围受限。

因此，本文选取 3 类预测模型中的典型模型，即 Elman 神经网络预测模型、GM(1, 1)预测模型和 SVM 支持向量机预测模型，并充分考虑各单个预测指标的相互作用关系，提出了一种基于合作对策论的网络安全态势组合预测模型，将各单一预测模型看成是组合预测这个合作对策中的局中人，合作的结果为组合预测的误差平方和，再按合作对策 Shapley 值法在各单一预测模型中进行分配，从而确定组合预测权系数。实际网络安全态势数据的仿真结果表明，该方法计算简便且能够有效提高网络安全态势的预测精度。

1 相关知识

1.1 网络安全态势预测原理

网络安全态势预测是指在网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及获取未来的发展趋势[8]，包括态势要素的提取、态势值计算和态势预测 3 个步骤。

(1) 态势要素提取：从网络数据流、网络设备日志、主机日志等采集网络安全事件的原始数据，并对原始数据进行筛选、简约、统一格式化等预处理，然后对数据进行分析，提取出网络安全的要素；

(2) 态势值计算：态势值计算是建立在态势要素提取的基础之上，主要是对获取到的态势要素进行加权计算，从而得到一个能反映某时刻网络运行状况的态势值；

(3) 态势预测：态势预测是建立在态势值计算的基础之上，是网络安全态势预测的最后环节。当前 M 个时刻的态势值利用态势预测模型计算得到以后 N 个时刻态势值，然后分析得到的态势值进而预测网络安全态势的变化趋势，为网络管理者提供决策支持。

1.2 单一预测模

(1) Elman 神经网络

在前馈式神经网络的基础上增加一个承接层，从而形成反馈型神经网络，使原本没有反馈信号的网络具备了历史记忆功能，从而增强了神经网络的非线性动态映射能力[9]，该网络被称为 Elman 神经网络。

Elman 网络输入与输出的非线性映射关系可以用如下公式表示：

$$\boldsymbol{y}(k)=g(w^3\boldsymbol{x}(k)) \tag{1}$$

$$\boldsymbol{x}(k)=f(w^1\boldsymbol{x}_c(k)+w^2(\boldsymbol{u}(k-1))) \tag{2}$$

$$\boldsymbol{x}_c(k)=\boldsymbol{x}(k-1) \tag{3}$$

式中：y, x, u, x_c 分别表示 m 维输出层向量、n 维中间层向量、r 维输入向量、n 维反馈状态向量；中间层分别与输出层和承接层相连，权值系数分别用 w^3 和 w^1 表示，而输入层则只与中间层相连，权值系数用 w^2 表示；$g(*)$是输出神经元的传递函数；$f(*)$是承接神经元的传递函数。

对其隐含层和输出层的训练函数分别取线性传递函数和正切 S 形传递函数。

$$E(w)=\sum_{k=1}^{n}(\boldsymbol{y}_k(\boldsymbol{w})-\tilde{\boldsymbol{y}}_k(\boldsymbol{w}))^2 \tag{4}$$

式中：$\boldsymbol{y}_k(\boldsymbol{w})$为目标输入向量。

(2) GM(1, 1)模型

灰色系统理论是基于关联空间光滑离散函数等概念定义灰导数与灰微分方程，进而用离散数据列建立微分方程形式的动态模型。灰色模型种类繁多，其中 GM(1, 1)模型是最为常用的用于一维时间序列预测的灰色模型[10]。其建模过程包括如步骤：

1) 原始数据 AGO 预处理

1-AGO 序列的定义如下：对一维时间序列 $x^{(0)}=(x^{(0)}(1),x^{(0)}(2),...,x^{(0)}(n))$ 进行累加操作，一次操作后得到新的数据序列。具体表示如下：

$$x^{(1)}=(x^{(1)}(1),x^{(1)}(2),...,x^{(1)}(n)) \tag{5}$$

式中：$x^{(0)}(i)$和 $x^{(1)}(i)$分别为由采样数据所组成的时间序列中的第 i 个数据，和由采样数据累加所得时间序列的第 i 个数据。

2) 建立 $x^{(1)}(i)$的一阶线性微分方程

$$\frac{\mathrm{d}x^{(1)}}{\mathrm{d}t}+a\,x^{(1)}=u \tag{6}$$

3) 构造均值向量 $\boldsymbol{B}$ 和常数项向量 $\boldsymbol{Y_n}$

$$\boldsymbol{B}=\begin{bmatrix}0.5(x^{(1)}(1)+x^{(1)}(2))\\0.5(x^{(1)}(2)+x^{(1)}(3))\\0.5(x^{(1)}(n-1)+x^{(1)}(n))\end{bmatrix} \tag{7}$$

$$\boldsymbol{Y_n}=(x^{(0)}(2),x^{(0)}(3),...,x^{(0)}(\mathrm{n}))^T \tag{8}$$

4) 求解灰参数 $\hat{a}$

$$\hat{a}=\begin{pmatrix}a\\u\end{pmatrix}=(B^TB)^{-1}B^TY_n \tag{9}$$

5) 求解 $x^{(1)}(t)$的一阶线性微分方程

$$\hat{x}^{(1)}(t+1)=(x^{(0)}(1)-\frac{u}{a})e^{-at}+\frac{u}{a} \tag{10}$$

6) 还原 $x^{(0)}$序列

$$\hat{x}^{(0)}(t+1)=\hat{x}^{(1)}(t+1)-\hat{x}^{(1)}(t) \tag{11}$$

7) 模型检验

对建立的灰色模型进行残差平均值、均方差比值、小误差概率的精度检验。

(3) SVM 模型

支持向量机(support vector machine，SVM)是一种新的机器学习方法，在非线性拟合、最优预测、模式识别等领域有着广泛应用[11-12]。不敏感损失函数 ε 被引入 SVM 分类模型，得到回归性支持向量机。其基本思想：在高维空间中寻找一个分类平面使得所有的训练样本离其距离最小，即最优分类平面。

设有 n 个训练样本对，记 $\{(x_i,y_i),i=1,2,...,n\}$，其中，$\boldsymbol{x}_i(\boldsymbol{x}_i\in R^d)$ 是第 i 个训练样本的输入列向量，$y_i\in R$ 为对应的输出值。

引入线性不敏感损失函数 ε 以及松弛变量 ξ_i,ξ_i^*，将回归拟合问题转化为以下优化问题：

$$\begin{cases}\min\dfrac{1}{2}\|w\|^2+C\sum\limits_{i=1}^{l}(\xi_i+\xi_i^*)\\ \text{s.t.}\begin{cases}y_i-w\Phi(\boldsymbol{x}_i)-\mathrm{b}\leqslant\varepsilon+\xi_i,\ i=1,2...,l\\ -y_i+w\Phi(\boldsymbol{x}_i)+\mathrm{b}\leqslant\varepsilon+\xi_i^*\\ \xi_i\geqslant 0,\xi_i^*\geqslant 0\end{cases}\end{cases} \tag{12}$$

其对偶问题为：

$$\begin{cases}\max\limits_{\boldsymbol{\alpha},\boldsymbol{\alpha}^*}[-\dfrac{1}{2}\sum\limits_{i=1}^{l}\sum\limits_{j=1}^{l}(\alpha_i-\alpha_i^*)(\alpha_j-\alpha_j^*)K(\boldsymbol{x_i},\boldsymbol{x_j})-\\ \qquad\sum\limits_{i=1}^{l}(\alpha_i+\alpha_i^*)\varepsilon+\sum\limits_{i=1}^{l}(\alpha_i-\alpha_i^*)y_i]\\ \text{s.t.}\begin{cases}\sum\limits_{i=1}^{l}(\alpha_i-\alpha_i^*)=0\\ 0\leqslant\alpha_i\leqslant C\\ 0\leqslant\alpha_i^*\leqslant C\end{cases}\end{cases} \tag{13}$$

式中：$K(\boldsymbol{x_i},\boldsymbol{x_j})=\Phi(\boldsymbol{x_i})\Phi(\boldsymbol{x_j})$ 为核函数。核函数选择为高斯核函数：$K(\boldsymbol{x_i},\boldsymbol{x_j})=\exp(-\frac{\|x_i-x_j\|}{2\sigma^2})$。

最终得到的回归函数为：

$$f(x)=\sum_{i=1}^{l}(\alpha_i-\alpha_i^*)K(\boldsymbol{x_i},\boldsymbol{x})+b^* \tag{14}$$

2 基于合作对策论的组合预测模型

合作对策论常用于在合作收益的各合作方之间的分配，充分考虑各个成员在合作中的重要性，其优点在于原理和结果被各个合作方视为公平。本文将合作对策论应用于网络安全态势的组合预测中，并作相应的修改。

2.1 合作对策论

对于同一预测对象，共有 m 种单一预测方法分别对其进行预测，在合作对策理论中，称这 m 种单一预测方法所组成的集合 $M=\{1,2,\cdots,m\}$ 为局中人集合[13]。

根据本文的实际应用，将合作对策论中的定义修改为：

定义 1：记 M 的所有子集为 2^M，若干个局中人联合在一起形成一个联盟 S，显然每一个联盟是 M 的一个子集。

定义 2：设 $M=\{1,2,\ldots m\}$，$s\subset M$，$v(s)$为定义在 2^M 集合上实值函数，令 $v(s)=-J(s)$，它满足

$$v(\Phi)=0 \tag{15}$$

$$v(M)\geqslant\sum_{i=1}^{m}v(\{i\}) \tag{16}$$

式中：$v(s)$为合作对策的特征函数；$J(s)$为联盟 s 最后得到的结果，即预测误差平方和；$v(s)$和 $J(s)$互为相反数。

定义 3：联盟得到的成果由参与合作的各种预测方法共同产生，定义 $v(s\cup\{i\})-v(s)$ 为第 i 种方法的贡献，其中 $s\subset M$。

在组合预测中，预测的总误差可以看作是联盟后得到的产生的最后结果。由于该结果是由参与合作的各种预测方法共同产生的，因此把总成果按照定义 3 中预测方法的贡献大小来进行分配，最后确定各个单一预测方法在组合预测中权重系数。

最大联盟 $v(M)$给予第 i 种方法的分配记为 x_i，$i=1,2,...m$，则有

$$\begin{aligned}
&x_1=v(\{1\}),\\
&x_2=v(\{1,2\})-v(\{1\}),\\
&x_3=v(\{1,2,3\})-v(\{1,2\}),\\
&\cdots\cdots\\
&x_m=v(M)-v(M-\{m\})
\end{aligned} \tag{17}$$

不同的编号次序会影响分配的结果，若把局中人 $m,m-1,\cdots 2,1$ 的编号改为 $1',2'...m'$，新的分配方案为：

$$\begin{aligned}
&x_1'=v(\{m\}),\\
&x_2'=v(\{m,m-1\})-v(\{m\}),\\
&x_3'=v(\{m,m-1,m-2\})-v(\{m,m-1\}),\\
&\cdots\cdots\\
&x_m'=v(M)-v(M-\{1\}).
\end{aligned} \tag{18}$$

基于上述分析，m 个局中人次序总数决定了分配方案共有 $m!$种。为了使分配的结果更加公平、合理，局中人的平均贡献被用来度量每个参与者贡献的大小。

平均贡献的定义如下：

$$\varphi_i(v)=\frac{1}{m!}\sum_{\pi}[v(s_\pi^i\cup\{i\})-v(s_\pi^i)] \tag{19}$$

其中：π 由 1, 2,$\cdots m$ 组成的所有 m 级排列，$\sum$为针对所有的 $m!$个不同的 m 个不同的 m 级排列求和，$s_\pi^i=\{j\mid \pi\ j<i\}$。

将满足 $s_\pi^i=s$ 排列归为一类，式(19)可表示为

$$\begin{aligned}
&\varphi_i(v)=\sum_{i\in s}\frac{(m-|s|)!(|s|-1)!}{m!}[v(s)-v(s-\{i\})],\\
&i=1,2,...m
\end{aligned} \tag{20}$$

将 $\varphi_i(v)$按照式(20)作归一化处理，最终得到组合预测的权重系数

$$l_i=\frac{v(M)}{\varphi_i(v)}\Big/\sum_{j=1}^{m}\frac{v(M)}{\varphi_j(v)},\ i=1,2,\cdots m \tag{21}$$

显然它们满足 $\sum_{i=1}^{m}l_i=1,\ l_i\geqslant 0,\ i=1,2,\cdots m$。

2.2 网络安全态势组合预测模型

本文提出的组合预测模型的计算步骤(图 1)为：

(1) 分别用 Elman 神经网络、GM(1, 1)和 SVM 这 3 种单一预测模型对网络安全态势进行预测，得到第 i 种预测模型在 t 时刻的预测值为 y_{it}，对应时刻的实际值记为 y_t。

(2) 计算误差信息矩阵

设第 i 种预测模型在时刻 $t(t=1,2,\cdots,n)$ 的预测误差为 e_{it}，$e_{it}=y_t-y_{it}$ 相应的预测误差向量为 $\boldsymbol{E}_i=[e_{i1},e_{i2},...,e_{in}]^T$，预测误差矩阵为 $\boldsymbol{e}=[E_1,E_2,\cdots,E_n]$，预测误差信息矩阵为

$$\boldsymbol{E}=\boldsymbol{e}^T\boldsymbol{e}=\begin{bmatrix} E_{11} & E_{12} & ... & E_{1n} \\ E_{21} & E_{22} & ... & E_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ E_{n1} & E_{n2} & ... & E_{nn} \end{bmatrix} \tag{22}$$

(3) 用方差倒数法给出一个初始的组合权系数的估计值。

$$L_i=\frac{e_i^{-1}}{\sum_{i=1}^{m}e_{ii}^{-1}} \tag{23}$$

(4) 利用式(18)计算单一预测模型组合 M 的每个子集及其对应的特征函数。

(5) 利用式(19)计算参与整个合作过程中各种单项预测方法的平均贡献。

(6) 对步骤(5)中计算得到的平均贡献作归一化处理，最后得到组合预测权重系数，最后得到组合预测值。

$$\hat{y}_t=\sum_{i=1}^{m}l_i\ \hat{y}_{it} \tag{24}$$

3 仿真实验

本文通过对某公司互联网 2010-06-11-2010-12-30 的网络安全监测数据进行采集，得到相应的实验样本数据，其采样频率为 1 天，为共有 160 个一维时间序列。本文所采集的 160 个样本中，以前 136 个数据作为训练样本，以后 24 个数据为测试样本。

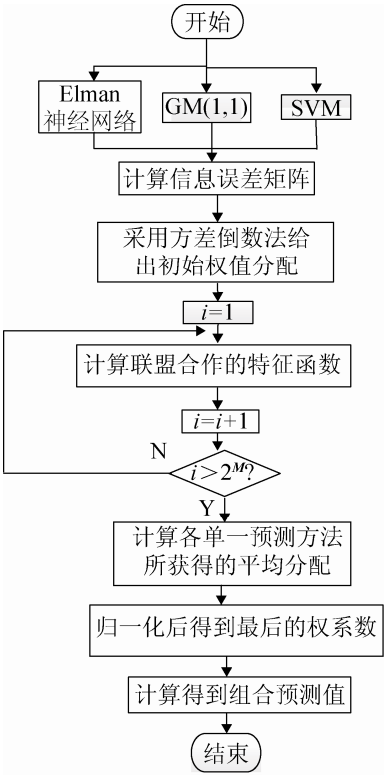

图 1 基于合作对策论的网络安全态势组合预测流程图
Fig. 1 Strategy of combination model of network security situation prediction based on cooperative games

首先，分别用 Elman 神经网络、GM(1, 1)和 SVM 三种单一预测模型对网络安全态势进行预测，比较各种单一预测模型的性能。其次，采用不同的组合预测模型对相同的样本进行预测，同样对预测的结果进行组合对单一预测和不同组合模型的比较。

图 2 是采用不同单一预测模型所得到的 2010-12-07-2010-12-30 日态势值的单步预测结果，每次预测一个值，共有 24 个值。Elman 神经网络和 SVM 都能够比较好地跟踪态势值的变化趋势，而 GM(1, 1)在前半段很好地预测出态势值的变化，但是当态势值出现转折下降时，其不能及时跟踪态势值的变化，存在一定的滞后性，减弱了其整体的预测效果。

图 3 给出了 3 种模型预测结果的相对误差的绝对值，Elman 神经网络模型的最大绝对误差为 1.74%，GM(1, 1)的最大绝对误差高达 3.71%，SVM 支持向量机模型的最大绝对误差为 1.22%。

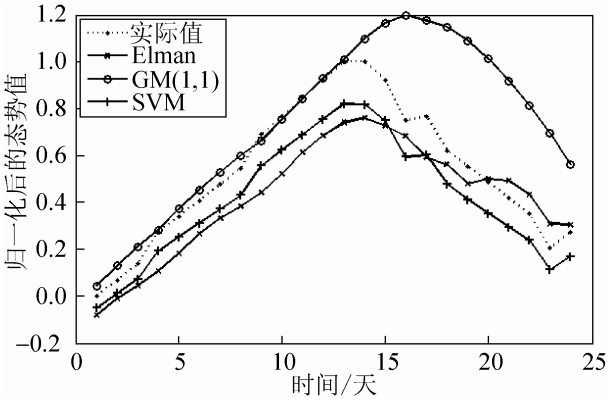

图 2 Elman, GM(1, 1), SVM 预测结果

Fig. 2 Prediction results of Elman, GM(1, 1) and SVM

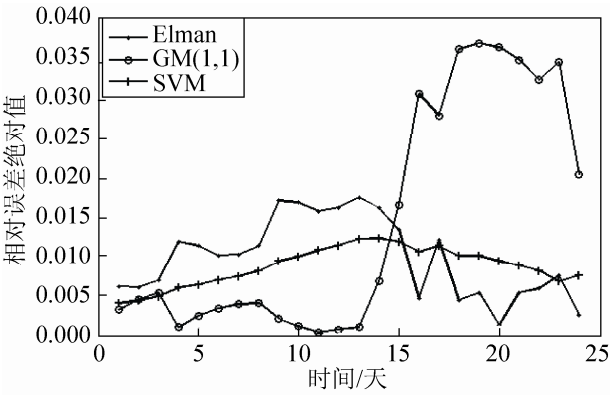

图 3 Elman, GM(1, 1), SVM 的绝对误差

Fig. 3 Absolute error of Elman , GM(1, 1) and SVM

为了证明本文提出模型的有效性，与文献[6-7]的组合预测模型进行了对比实验。图 4 为组合预测模型的预测结果，从曲线的拟合程度看，组合预测模型明显优于单一预测模型。

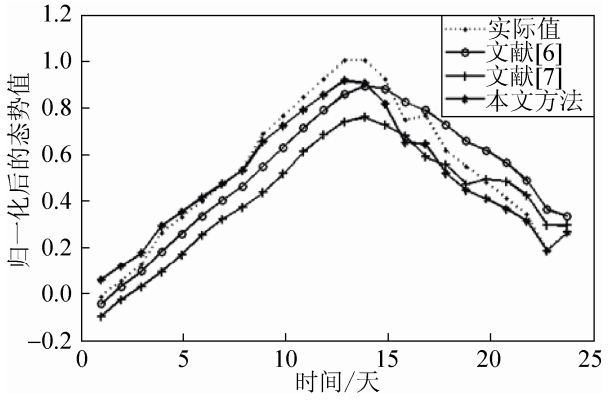

图 4 3 种组合预测模型的预测结果

Fig. 4 Predictive results of three combination forecasting models

为了进行更好的横向比较，本文采用常用于描述预测误差的两项指标 RMSE(Root Mean Squared Error)和 MAE(Mean Absolute Error)来评价预测精度，具体如表 1 所示。

表 1 各种模型预测性能对比

Tab. 1 Performance comparison of various models

单一预测模型	RMSE /%	MAE /%	组合预测模型	RMSE /%	MAE /%
Elman	1.09	0.97	文献[6]	0.71	0.65
GM(1,1)	2.05	1.44	文献[7]	0.86	0.85
SVM	0.89	0.86	本文方法	0.44	0.37

根据表 1 可以对比发现，所有单一预测模型中，SVM 预测的误差最小，其 RMSE 为 0.89%，MAE 为 0.86%，而 GM(1, 1)的误差最大，其 RMSE 为 2.05%，MAE 为 1.44%。采用组合预测模型的网络安全态势预测精度均优于单一预测模型，这是因为组合预测模型有效利用了各单一预测模型所蕴含的信息，对不同渠道得到的信息起到了融合的作用。此外，本文所提出的基于合作对策论的组合预测模型，其得到的预测结果整体精度高于其他组合预测模型。合作对策论按照局中人对联盟的贡献来分配权重，赋予了预测效果较好的 SVM 更大的权重，而对于预测效果较差的 GM(1,1)则赋予较小的权重，因此其组合预测的效果较好，而其他两种预测模型并不考虑各单项指标相互之间的影响，忽视了各个指标的预测精度存在差异，因此预测效果相对较差。

4 结论

网络安全态势在一定程度上呈现时变性、突变性、非线性的特点，单一的预测模型会导致某些测量点出现较大误差。本文基于类比的思想，将网络安全态势的组合预测问题类比成一个合作对策的问题，阐述了所提方法的基本思想和主要实现方法，最后通过仿真实验验证，该模型可以准确跟踪态势值的变化。通过实验对比，本文提出的组合预测模型使得预测精度得到较大的改善。

DOI: 10.16182/j.issn1004731x.joss.201705030

参考文献:

[1] 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): 1750-1761. (XIE Lixia, WANG Yachao, YU Jinbo. Network Security Situation Awareness based on Neural Networks [J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1750-1761.)

[2] 蓝新波, 李冬睿. 径向基函数神经网络在网络安全预测中的应用 [J]. 计算机测量与控制, 2014, 22(3): 836-838. (LAN Xinbo, LI Dongrui.Application of Radial Basis Function Neural Network in Forecast Network Security [J]. Computer Measurement & Control, 2014, 22(3): 836-838.)

[3] 汪财印. 灰色关联分析和支持向量机相融合的网络安全态势评估 [J]. 计算机应用研究, 2013, 30(6): 1859-1862. (WANG Caiyin. Assessment of Network Security Situation Based on Grey Relational Analysis and Support Vector Machine [J]. Application Research of Computers, 2013, 30(6): 1859-1862.)

[4] 徐茹枝, 常太华, 吕广娟. 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): 124-133. (XU Ruzhi, CHANG Taihua, LV Guangjuan. The Research on Prediction Method of Network Security Posture Based on Time Series [J]. Methematics in Practice and Theory, 2010, 40(12): 124-133.)

[5] 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. (ZHANG Xiang, HU Changzhen, LIU Shenghang, et al. Research on Network Attack Situation Forecast Technique Based on Support Vector Machine [J]. Computer Engineering, 2007, 33(11): 10-12.)

[6] 姚晔. 基于熵值法的网络安全态势组合预测模型 [J]. 计算机仿真, 2012, 29(4): 157-160. (YAO Ye. Combination Model of Network Security Situation Prediction Based on Entropy [J]. Computer Simulation, 2012, 29(4): 157-160.)

[7] 张安楠, 苏旸. 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 Annan, SU Yang. Research on Hybrid Prediction Method for Network Security Situation Based on Wavelet Transform [J]. Computer Simulation, 2014, 31(6): 282-286.)

[8] 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, 33(10): 5-10. (WANG Huiqiang, LAI Jibao, ZHU Liang, et al. Survey of Network Situation Awareness System [J]. Comuputer Science, 2006, 33(10): 5-10.)

[9] 尤马彦, 凌捷, 郝彦军. 基于Elman神经网络的网络安全态势预测方法 [J]. 计算机科学, 2012, 39(6): 61-63. (YOU Mayan, LING Jie, HAO Yanjun. Prediction Method for Network Security Situation Based on Elman Neural Network [J]. Computer Science, 2012, 39(6): 61-63.)

[10] 王小川, 史峰, 郁磊, 等. MATLAB神经网络43个案例分析 [M]. 北京: 北京航空航天出版社, 2013. (WANG Xiaochuan, SHI Feng, YU Lei, et al. 43 Case Studies on MATLAB Neural Network [M]. Beijing, China: Beijing Aerospace Press, 2013.)

[11] 黄宜, 赵光洲, 王艳伟. 基于Shapley值的中国能源消费组合预测模型研究 [J]. 能源工程, 2012(6): 5-9. (HUANG Yi, ZHAO Guangzhou, WANG Yanwei. Research on the Portfolio Prediction Methods of China Energy Consumption based on Shapley Value [J]. Energy Engineering, 2012 (6): 5-9.)

[12] Vapnik V N. Statistical learning theory [M]. New York, USA: John Wiley & Sons Inc., 1998.

[13] Abe S. Support vector machines for pattern classification [M]. London, UK: Springer-Verlag, 2010.

