# 基于Elman神经网络的网络安全态势预测方法

尤马彦 凌 捷 郝彦军
(广东工业大学计算机学院 广州 510006)

**摘 要** 准确把握网络系统的安全态势,能够为网络管理者做出安全防护的决策提供有效的信息。在评估当前网络安全态势的基础上,利用加权后得到的网络安全态势值的非线性时间序列的特点,提出了一种基于Elman神经网络的态势预测方法,它利用Elman网络具有动态记忆功能和对历史数据具有敏感性等优点,对网络安全态势进行预测。通过实验仿真表明,该方法能够准确有效地预测网络安全态势。

**关键词** 网络安全态势评估,态势预测,Elman神经网络
**中图法分类号** TP393 **文献标识码** A

## Prediction Method for Network Security Situation Based on Elman Neural Network

YOU Ma-yan LING Jie HAO Yan-jun
(School of Computer, Guangdong University of Technology, Guangzhou 510006, China)

**Abstract** Grasping the security situation of network system accurately, which can provide effective information, helps network managers to make security decisions. Based on the assessment of current network security situation, using the feature of nonlinear and time series, this paper presented a method of networks security situation prediction, based on Elman neural network, with the advantages of dynamic memory of Elman network and sensitivity of historical data, etc, to predict the network security situation. Finally, experiment shows that networks security situation can be effectively and accurately predicted with this method.

**Keywords** Network security situation assessment, Situation prediction, Elman neural network

网络的开放性、共享性以及互连程度的日益扩大,使得各种网络安全事件层出不穷,网络安全问题越发得到人们的重视。要保证网络系统的安全运行,采用传统的、单一的防御设备或者检测设备已经无法满足需求。从总体上认知网络系统的安全运行状况,真实、准确、客观地对网络安全态势进行评估与预测,使其逐渐成为当前网络安全领域的研究热点之一。在网络安全态势领域也有了很多开创性的研究:Bass Tim[1]在分析网络态势感知的概念后,提出了一个基于多传感器数据融合技术的网络安全态势框架;上海交通大学的陈秀真等人提出了层次化网络安全威胁态势评估模型[2];中国科技大学的Zhang Yong等提出了基于多角度分析的网络安全态势感知评估模型[3]。

安全态势评估(security situational awareness)是指感知和获取一定时间、空间环境中的安全元素,对获取的数据和信息进行整合和分析,并基于分析结果来预测其未来的发展趋势[4]。网络安全态势是某时刻由各种网络设备运行情况、网络服务状况及用户行为等因素构成的对整个网络安全的运行状况的宏观反映[2],它能直观地反映一个网络过去和当前的安全状况。网络态势安全评估是建立在对海量网络数据和安全事件的收集与分析的基础上,并对这些复杂、存在冗余的原始数据进行归并融合处理,整合出存在内在关联的安全信息,得到整个网络的安全状态,并合理地预测网络未来一段时间内网络安全状况可能的发展趋势。从而,能够为网络管理员了解网络的安全状况和做出有效的安全防范措施提供决策支持。

为了在评估预测过程中尽量减少主观随意性和认识模糊等不利因素的影响,本文在评估当前网络安全态势的基础上,利用加权后得到的网络安全态势值的非线性时间序列的特点,提出了一种基于Elman神经网络的网络安全态势预测方法。该方法利用了神经网络具有高度的非线性运算和映像能力[5],对信息的处理具有自组织、自学习的特点和较高精度的预测能力等优点。最后利用该方法对Honeynet组织收集的黑客攻击数据集进行实验仿真,并对实验结果进行误差分析,从而验证本网络安全态势预测方法的有效性。

## 1 Elman神经网络

### 1.1 Elman神经网络模型

Elman神经网络是Jeffrey L. Elman于1990年提出的一种简单递归网络(Simple Recurrent Network, SRN)模型[6],如图1所示。该网络在BP神经网络的基础上,通过引入反馈信号,使其具有历史记忆功能和非线性动态映射能力[7]。Elman网络除了具有输入层、隐含层和输出层单元外,还有一

到稿日期:2011-07-13 返修日期:2012-01-05 本文受广东省自然科学基金(9151009001000043),广东省教育厅育苗项目(LYM09066)和广东省教育部产学研合作项目(2011A090200068)资助。

尤马彦(1987—),男,硕士生,主要研究方向为网络信息安全等,E-mail:mayan_you@126.com;凌 捷(1964—),男,教授,硕士生导师,主要研究方向为网络信息安全等;郝彦军 男,博士,主要研究方向为网络信息安全等。

个从隐含层神经元的输出到网络输入的反馈连接，称为承接层。由于承接层的存在，网络的输入层接受两种信号：一种是来自外部的输入信号 $U(t)$，另一种是来自隐含层的反馈信号 $X_c(t)$。这就使其对历史数据具有敏感性，增加了网络自身处理动态信息的能力并具有较好的容错性。

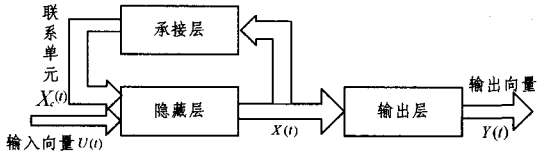


图 1　Elman 神经网络模型

### 1.2　Elman 网络学习算法

神经网络训练的任务是通过学习算法不断地调整网络的权值和阈值，使网络的输出与期望的误差达到最小。本文的 Elman 神经网络采用 LM(Levenberg-Marquardt)算法[8]，它是目前使用较为广泛的非线性最小二乘算法。该算法同时具有牛顿法和最速下降法的特点，处理非线性最优化问题有很快的收敛速度，且有较牛顿法显著减小的复杂性。

设第 $k$ 步网络的实际输出为 $y_k$，期望输出为 $\hat{y}_k$，网络的权值向量为 $w$，定义网络的误差函数为：

$$E_k(w)=\frac{1}{2}(\hat{y}_k-y_k)^{\mathrm{T}}(\hat{y}_k-y_k) \tag{1}$$

由 LM 算法，网络权值的调整率为：

$$\Delta w_k=[J_k^{\mathrm{T}}J_k+uI]^{-1}J_k^{\mathrm{T}}e_k \tag{2}$$

式中，$I$ 是单位矩阵，$e_k=(\hat{y}_k-y_k)$是第 $k$ 步网络的误差向量，$J_k$ 是网络误差 $e_k$ 对网络权值 $w$ 偏导数的雅可比矩阵，$u$ 是学习率参数，它在训练期间可以动态地修改。当 $u$ 较小时，式(2)趋向于牛顿算法；当 $u$ 较大时，式(2)趋向于最速下降梯度算法，故通过调整 $u$ 的值，LM 算法能够表示从牛顿法到最速下降梯度法的过渡，使得算法具有灵活性。

## 2　基于 Elman 神经网络的安全态势预测方法

### 2.1　基于 Elman 网络的态势预测建模

影响网络安全运行状况的因素是多方面的，如就主体而言，包括攻击者的意图、能力等，管理者的管理策略、态度等；就客体而言，包括网络环境、网络结构、设备性能等。所以，要客观、较全面、较准确地对一个网络的整体安全状况做出判定，并对其可能发展趋势进行预测，就必须建立一个合理的态势评估模型。

本文针对网络系统非线性和复杂性、其未来态势的随机性和不确定行等特点，利用 Elman 神经网络在复杂的非线性系统预测方面的优势，提出了基于 Elman 神经网络的网络安全态势评估与预测模型，如图 2 所示。

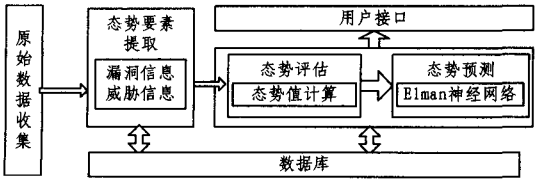


图 2　基于 Elman 网络的安全态势评估与预测模型

(1)原始数据收集

数据收集是网络态势评估的第(1)步，网络安全态势评估的研究按照数据源可分为基于系统配置信息和基于系统运行信息两大类[2]。系统配置信息可以通过漏洞扫描等技术手段来获取网络系统的服务、主机、网络等的漏洞信息；系统运行信息可以通过分析网络数据流、IDS 日志和网络设备性能数据等来了解网络系统受到攻击的状况。

(2)态势要素提取

第(2)步，必须对(1)收集到的海量、冗余的原始数据进行关联分析和归并处理，分类提取出影响网络运行状况的关键要素，并形成统一的数据格式存放到数据库中，以便下一步处理。

(3)态势值计算

态势值的计算是网络安全态势评估的关键，即通过第(2)步得到的态势要素进行加权定量计算得到反映网络某个时间段内安全状态的数值，它是态势预测的基础。本文参考了文献[2]提供的量化计算方法，从服务层、主机层和系统层来计算网络安全态势值。

**定义 1**　$F_{S_j}(t)$表示服务 $S_j$ 在 $t$ 时间段的安全态势指数，记为：

$$F_{S_j}(t)=\sum_{i=1}^{n}N_i(t)\cdot 10^{D_i(t)} \tag{3}$$

式中，$n$ 是 $S_j$ 在 $t$ 时间内受到攻击的种类；$N_i(t)$是 $S_j$ 在 $t$ 时间内受到第 $i$ 种攻击的次数；$D_i(t)$是第 $i$ 种攻击对 $S_j$ 的危害程度。

**定义 2**　$F_{H_k}(t)$表示主机 $H_K$ 在 $t$ 时间段的安全态势指数，记为：

$$F_{H_k}(t)=\sum_{j=1}^{m}V_j\cdot F_{S_j}(t) \tag{4}$$

式中，$m$ 表示主机 $H_K$ 在 $t$ 时间段开通的服务数；$V_j$ 表示服务 $j$ 在所有开通的服务中所占的权重。

**定义 3**　$F_L(t)$表示 $t$ 时刻的网络安全态势指数，记为：

$$F_L(t)=\sum_{k=1}^{c}W_k\cdot F_{H_k}(t) \tag{5}$$

式中，$c$ 表示网络内的主机数；$W_K$ 表示主机 $k$ 在网络内所占的重要性权重。

(4)态势预测

态势预测是态势评估的最后阶段，也是网络安全预警的前提。它利用历史和当前网络安全态势信息来预测未来的网络安全发展趋势。采用 Elman 神经网络在复杂的非线性系统预测方面的优势来建立安全态势预测模型，其网络结构如图 3 所示。

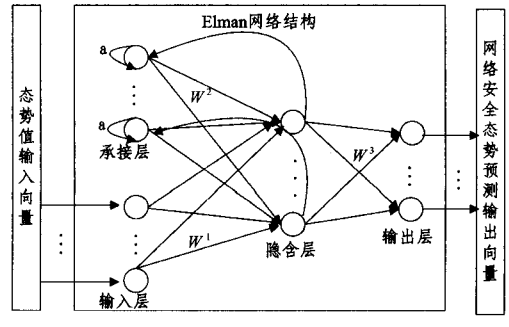


图 3　评估模型中 Elman 网络结构

### 2.2　评估模型中 Elman 网络结构及计算

图 2 所示评估模型中的态势预测的 Elman 神经网络结构如图 3 所示，它是由输入层、隐含层、承接层和输出层构成的反馈型递归网络。

在某 $t$ 时间内，从态势数据库中取出一个态势序列作为

Elman 神经网络的输入向量，记为 $U(t)$，并设 $X(t)$ 为隐含层输出，$X_c(t)$ 为承接层输出，$Y(t)$ 为网络的输出。

$$U(t)=(u_1,u_2,\cdots,u_n) \tag{6}$$

$$X_c(t)=X(t-1)+aX_c(t-1) \tag{7}$$

$$X(t)=f(W^1U(t-1)+W^2X_c(t)) \tag{8}$$

$$Y(t)=g(W^3X(t)) \tag{9}$$

式中，$u_i(u_i\geqslant 0,i=1,2,\cdots,n)$ 为某一时刻的安全态势值；$W^1$，$W^2$，$W^3$ 分别表示输入层到隐含层、承接层到隐含层、隐含层到输出层的连接权值矩阵；$a(0\leqslant a\leqslant 1)$ 为承接层自连接反馈增益因子；$f(\cdot)$ 为隐含层神经元的传输函数，一般采用 sigmoid 函数，本文采用 $f(x)=\frac{1-e^{-2x}}{1+e^{-2x}}$；$g(\cdot)$ 为输出神经元的传输函数，本文采用线性函数。

规定 $m$ 个学习样本：

$$P=(U_1,\cdots,U_m)$$

$$=((u_1,\cdots,u_n);\cdots;(u_m,\cdots,u_{n+m-1})) \tag{10}$$

对应的 $m$ 个教师样本 $Y=(u_{n+1},u_{n+2},\cdots,u_{m+n})$。在 Matlab 上建立 Elman 神经网络模型，通过对 Elman 神经网络的训练，使网络输出与期望的教师样本尽可能地接近，即使网络输出层的误差达到最小。

Elman 神经网络的训练学习过程如下：

(1)初始化：设置最大迭代次数 $k$、反馈增益因子 $a$、学习样本 $P$、教师样本 $Y$、目标误差 $\varepsilon>0$、学习率等参数，并随机生成初始网络权值向量 $w$。

(2)根据 Matlab 中的 newelm 函数来建立 Elman 神经网络。

(3)对网络进行迭代训练，每一步迭代过程如下所述：

a)计算网络输出：提交当前迭代的一个输入向量，计算出网络的输出向量；

b)将网络输出结果与期望的教师样本进行比较，使用式(1)计算出误差向量 $e_k$；

c)计算误差 $e_k$ 对权值 $w$ 的偏导数的雅可比矩阵 $J_k$；

d)调整学习率：在迭代过程中通过逐渐增大学习率参数，使该算法能够从牛顿法到最速下降梯度法过渡；

e)权值修正：使用式(2)计算出网络权值的调整率 $\Delta w_k$，并对权值进行更新：$w(k+1)=w(k)-\Delta w_k$；

f)停机测试：若误差 $e\leqslant\varepsilon$ 或达到最大迭代次数，则停止；否则，转向 a)进行下一步迭代。

## 3 实验仿真

### 3.1 实验环境与数据源

为了验证基于 Elman 神经网络的网络安全态势评估与预测方法的有效性与合理性，采用 Honeynet[9] 组织收集的黑客攻击数据集作为实验原始数据源。将原始数据集经过预处理后，根据上述 2.1 节提到的网络安全态势值计算方法进行态势值的计算，再在 Matlab 上建立 Elman 神经网络模型，并进行仿真预测。

实验中选取某一时间段共 10 周(70 天)的 Honeynet 网络攻击数据集作为态势值计算数据源，并以当天的攻击数据集计算当天的态势值，则 10 周共得到 70 个态势值。不同时间段的数据量差别很大，为了避免将数据直接用于训练而容易产生较大误差，需要对计算得到的态势值进行归一化处理。归一化公式如下：

$$\hat{x}=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{11}$$

式中，$x_{\max}$ 和 $x_{\min}$ 分别是态势值的最大值和最小值，$\hat{x}$ 是归一化值，$x$ 是当前态势值。归一化处理后的网络安全态势值如图 4 所示。

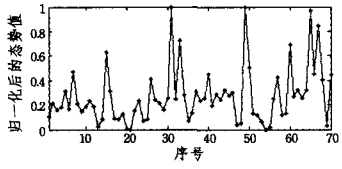


图 4 归一化网络安全态势值序列

### 3.2 网络模型参数的确定

选取前 9 周的态势值作为训练样本，后 1 周的态势值作为预测样本，每个样本以一周为周期单位，这样网络训练的输入层采用 7 个神经元，即输入向量 $U\in R^{1\times 7}$；网络输出采用 1 个神经元，即输出向量 $Y\in R^{1\times 1}$。也就是说，根据前一周的态势值来预测未来一天的态势值。

由式(10)可知学习样本 $P=\{U_1=(u_1,\cdots,u_7);\cdots;U_{56}=(u_{56},\cdots,u_{62})\}$，即学习样本数 $k=56$，对应的教师样本 $Y_d=(u_8,\cdots,u_{63})$。设定目标误差 $goal=1e-6$，学习速率 $u=0.05$，最大训练次数 $epochs=1000$，隐含层神经元数目根据经验公式 $n'=\sqrt{n+m}+r$(其中，$n$ 是输入神经元数目，$m$ 是输出神经元数目，$r\in[1,10]$)[5] 选取，经过多次实验，本文确定隐含层节点数为 10。

### 3.3 实验结果及分析

利用经过学习后的 Elman 神经网络预测数据集中的第 10 周的网络安全态势值，即利用 $u_{57}-u_{63}$(第 57 天到第 63 天的态势值)预测 $u_{64}$(第 64 天的态势值)，利用 $u_{58}-u_{64}$ 预测 $u_{65}$。依此类推，$-u_{63}\sim u_{69}$ 预测 $u_{70}$。预测结果和实际结果如图 5 所示。

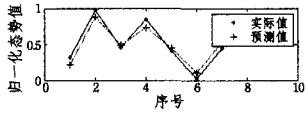


图 5 态势值预测结果序列

从图 5 可以看出，预测结果和实际结果比较吻合。下面对预测结果进行误差分析。定义平均绝对误差为 $MAE=\frac{1}{n}\sum_{i=1}^{n}|x_i-x_i'|$。其中 $x_i$ 是实际值，$x_i'$ 是预测值，$n$ 是预测个数。误差分析如表 1 所列。

表 1 预测数据误差分析

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 实际值 | 0.3204 | 0.9698 | 0.4547 | 0.8464 | 0.4038 | 0.0301 | 0.4475 |
| 预测值 | 0.2132 | 0.8841 | 0.4946 | 0.7315 | 0.4466 | 0.1102 | 0.5306 |
| 误差值 | 0.1072 | 0.0857 | −0.0399 | 0.1149 | −0.0428 | −0.0801 | −0.0831 |
| MAE | | | | 0.0791 | | | |

由图 5 和表 1 可以看出，Elman 神经网络对网络安全态势值有较高的预测精度，态势值的变化趋势与实际基本符合。

**结束语** 网络安全态势评估和预测能够从整体上反映网络的安全状况，发现网络系统的弱点和潜在的威胁，以及预测网络未来的发展趋势。本文提出了基于 Elman 神经网络的

(下转第 76 页)

由表3对比可知:3个方案中USPA的时间性能最优,计算量最小,综合效率最高;SPAS的时间性能最差,存储需求最低,综合效率最差;改进方案的效率较USPA稍差,在交互轮数、计算量、通信量方面均优于SPAS。因此,改进方案保持了USPA的高效性,相比SPAS更适用于对认证时延比较敏感的移动应用场合。

**结束语** 本文首先分析了USPA方案的安全性,指出该方案无法抵抗DoS攻击、重放攻击、Stolen-Verifier攻击和服务器仿冒攻击;然后结合USPA方案的高效性和SPAS方案的高安全性,给出了一个改进方案。安全性分析表明,新的改进方案弥补了USPA的安全缺陷,能够达到文献[4]所列出的全部9个安全目标,并且较好地解决了USPA方案中用户端和服务器端认证参数不一致问题;效率分析表明,改进方案在交互轮数、计算量、通信量方面均优于SPAS。综合来看,改进方案的实用性比USPA和SPAS有较大提高,非常适合于对安全需求较高的移动应用环境。

## 参 考 文 献


[1] Sandirigama M, Shimizu A, Noda M T. Simple and secure password authentication protocol[J]. IEICE Transactions on Communications, 2000, E83(B): 1363- 1365

[2] Lin C L, Sun H M, Hwang T. Attacks and solutions on strong-password authentication[J]. IEICE Transactions on Communications, 2001, E84(B): 2622-2627

[3] 虞淑瑶,叶润国,张友坤,等. 一种安全高效的强口令认证协议[J]. 计算机工程,2006,32(6):146-147

[4] Tsai C S, Lee C C, Hwang M S. Password Authentication Schemes: Current Status and Key Issues[J]. International Journal of Network Security, 2006, 3(2): 101-115

[5] 程英,高庆德. 一个强口令认证协议的漏洞研究[J]. 计算机科学,2009,36(10):106-116

[6] 于江,苏锦海,张永福. 基于USB-Key的强口令认证方案设计与分析[J]. 计算机应用,2011,31(2):511-513

[7] 秦小龙,杨义先. 强口令认证协议的组合攻击[J]. 电子学报,2003,31(7):1043-1045

[8] Wang Y Y, Liu J, Xiao F, et al. A more efficient and secure dynamic ID-based remote user authentication scheme[J]. Computer Communications, 2009, 32(4): 583-585

[9] Sandeep K S. Secure Dynamic Identity-Based Authentication Scheme Using Smart Cards[J]. Information Security Journal: A Global Perspective, 2011, 20(2): 67-77


(上接第57页)


[6] Srinivasan N, Paolucci M, Sycara K. Semantic Web Service Discovery in the OWL-S IDE[C]// Proceeding of the 39th Hawaii International Conference on System Sciences. Volume 06, 2006: 109

[7] 孙萍,蒋昌俊. 利用服务聚类优化面向过程模型的语义Web服务发现[J]. 计算机学报,2008,31(8)

[8] 李小林,张力娜,李卫斌. 一种基于QOS的扩展语义Web服务发现方法[J]. 重庆师范大学学报:自然科学版,2010,27(6)

[9] 喻坚,韩燕波. 面向服务的计算——原理与应用[M]. 北京:清华大学出版社,14

[10] Gruber T R. Toward Principles for the Design of Ontologies Used for Knowledge Sharing[R]. Padova: Stanford University, 2001

[11] Giuliano C, Lavelli A, Romano L. Relation extraction and the influence of automatic named-entity recognition[J]. ACM Transa-ctions on Speech and Language Processing(TSLP), 2007, 5(1): 11-23

[12] Noor N M M, Ali N H, Ibrahim N S. A new framework to extract WordNet lexicographer files for semi-formal notation: A preliminary study[C]// International Symposium on Information Technology. 2010: 1027-1031

[13] Shibata N, Kajikawa Y, Sakata I. How to measure the semantic rsimilarities between scientific papers and patents in order to discover uncommercialized research fonts: A case study of solar cells [C]// Technology Management for Global Economic Growth(PICMET), 2010 Proceedings of PICMET'10. 2010: 1-6

[14] Shi Lei, Fan Lei, Meng Zhen-zhen. The Research of Using Jena in the Semantic-based Online Learning Intelligent Behavior Analysis System[C]// Proceedings of the 2009 Fifth International Joint Conference on INC. 2009: 926-929

[15] Morohoshi H, Huang Run-he. A user-friendly platform for developing grid services over Globus Toolkit 3[C]// International Conference on Parallel and Distributed Systems (ICPADS). 2005: 668-674


(上接第63页)

网络安全态势评估方法,建立了评估与预测模型,并通过实验仿真和分析,验证了该方法的有效性。

## 参 考 文 献


[1] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems[C]// 1999 IRIS National Symp. on Sensor and Data Fusion. Laurel, 1999: 24-27

[2] 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)

[3] 舒南飞,牛少彰. 网络安全态势评估和预测的新进展[C]// 信息技术与应用学术会议. 2009: 267-273

[4] 韦勇,连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报,2009,32(4)

[5] 周开利,康耀红. 神经网络模型及其MATLAB仿真程序设计[M]. 北京:清华大学出版社,2005

[6] Eleman J L. Finding Structure in Time[J]. Cognitive Science, 1990, 14: 179-211

[7] 党小超,郝占军. 季节周期性Elman网络的网络流量分析与应用[J]. 计算机工程与应用,2010,46(28)

[8] Ham F M, Kostanic I. 神经计算原理[M]. 北京:机械工业出版社,2007

[9] http://old. honeynet. org

[10] 王宏伟,杨先一,金文标. 基于Elman网络的时延预测与改进[J]. 计算机工程与应用,2008,44(6):136-138