一种基于似然BP的网络安全态势预测方法

唐成华 余顺争
(中山大学电子与通信工程系 广州 510275)

摘 要 态势预测是网络安全态势感知的高级阶段。为了解决依赖于专家赋予权值、缺乏自学习的态势数据处理方法在复杂网络系统中的局限,提出了一种基于似然BP的网络安全态势预测方法,将BP神经网络引入态势预测领域,并用极大似然误差函数代替传统的误差函数,通过态势评估模型建立的态势序列作为训练输入序列,在反向传播过程中实现对指定参数权值的自学习调整,该方法能充分利用网络越复杂、粒度越细、效率就越高的特点,实验表明了该方法具有较好的态势预测效能,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,态势感知,态势预测,神经网络,似然BP
中图法分类号 TP393.08 **文献标识码** A

Method of Network Security Situation Prediction Based on Likelihood BP

TANG Cheng-hua YU Shun-zheng
(Department of Electrical and Communication Engineering, Sun Yat-Sen University, Guangzhou 510275, China)

Abstract Situation prediction is the advanced stage of network security situation awareness. For purpose of resolving the limitations of depending on experts giving weight, lacking of self-learning on data processing in complex network system, a method of network security situation prediction based on likelihood BP was proposed. The BP neural network was introduced to the situation prediction area, and the traditional error function was replaced by the maximum likelihood error function. The situation sequences established through the situation assessment model were used as the training input sequences, and the self-learning adjustment of the appointed parameters' values was implemented in the process of back propagation training. The new method can make full use of the characteristics of the network more complex, finer grain size, the higher the efficiency. Experimental results show that the method has good performance of situation prediction, and provides a new solution for network security situation prediction.

Keywords Network security, Situation awareness, Situation prediction, Neural networks, Likelihood BP

网络安全态势感知是目前网络安全领域的一个研究热点,主要围绕安全态势要素的获取、安全态势的评估、安全态势的预测和态势的可视化等方面进行研究[1,2],较多的研究成果在于对网络安全态势要素的提取和安全态势评估技术[3],而作为网络安全预警的前提,态势预测技术仍然是一个难题。由于攻击信息的不确定性、模糊性和多变性等特点,态势预测涉及到计算机科学、军事战略学和政治等多个学科,其重要性关系到人们的生活安全和国家安全。自1997年以来,美、英等国一直在进行网络安全预警技术的研究,美国国防信息系统局成立了网络战战术预警中心,并针对各个信息基础设施提出了长达15年的分阶段实现预警的系统计划。"9.11"事件后,欧盟加快了"建立电子信息安全计划"实施步伐,要求严格检查基础设施信息网络系统的预警和应急能力。英国King's College London学院国际安全分析中心(ICSA)在信息战攻击威胁测评和预警方面进行了深入研究,提出了智能化预警决策系统[4]。Kijewski研究了一个用于早期预警与攻击识别的原型系统框架[5],文献[6]提出了面向大规模网络的入侵检测与预警系统体系结构,CMU/SEI领导的CERT/NetSA[7]开发了SILK,旨在对大规模网络安全态势进行实时监控,在潜在的、恶意的网络行为变为无法控制之前进行识别、响应和预警,并给出相应的对付策略。

当前的网络安全态势预测技术大多作为态势评估技术的一部分,即对网络安全态势做出评价后,再对是否进行预警方面做出参考,采用的方法主要有多传感器数据融合方法[8]、层次分析法[9]、灰色关联分析法[10]、流分析法[11]等,然而这些方法都有一个共同的缺点,即过分依赖于专家给定的关于安全态势要素的初始权值,在系统运行过程中对权值的修改也必须由人来参与,一些算法不具有自学习性。在较小的网络环境中,这些处理方式可以被接受,但在复杂网络环境中,仅凭专家经验难以确定各态势要素的重要性,因而要求态势评估算法必须具有自学习性,能够通过自身的运行减少专家经验带来的误差影响。现有的自学习算法基本是有监督的学

到稿日期:2008-12-24 返修日期:2009-03-09 本文受国家高技术研究发展计划(863)项目(2007AA01Z449),国家自然科学基金-广东联合基金重点项目(U0735002),中国博士后科学基金项目(20070420793)资助。

唐成华(1974-),男,博士后,主要研究方向为网络信息安全等,E-mail:tchbox@163.com;**余顺争**(1958-),男,教授,博士生导师,主要研究方向为网络信息安全等。

习，即需要网络管理员对评估的结果给出一个评价，作为学习的反馈，再通过算法的学习功能对态势要素的权值进行调整，这种外部评价方法在复杂网络环境下也难以凑效，因为数据种类繁多，管理员自身难以进行分析判断，而且管理员的主观误判的概率要比小规模网络中高得多。

针对以上问题，本文提出一种基于似然 BP 的网络安全态势预测方法，该方法自学习核心部分采用比较成熟的 BP 人工神经网络算法。为了避免算法对所有态势要素样本点进行内插，舍弃传统的最小方差误差函数，引入极大似然估计，重新定义误差函数，考虑了样本误差和噪声对网络训练的影响，并能从全局的角度实现对网络的无监督学习，探讨了一种新的网络安全态势预测途径。

1 传统 BP 前馈网络算法

传统 BP 前馈网络算法的实质是利用样本集：

$$(X_i, Y_i = f(X_i)), X \in R^P, Y \in R^M, i = 1,2,\cdots,N \quad (1)$$

对给定的网络进行训练，通过不断调整网络中的权值 W，找到一个最优的 W^*，并进行网络建模，得到一个最优的函数逼近，使网络输出 $\hat{Y} = g(X_i, W)$ 趋于样本的期望输出 Y_i。

考虑一个 M 层 BP 前馈网络，每层神经元数量为 N_m，$(m = 1,2,\cdots,M)$，其基本网络方程可表示为：

$$y_i^m = f((W_i^m)^T Y^{m-1}) \quad (2)$$

式中，$i = 1,2,\cdots,N_m$，表示第 m 层神经元序号；y_i^m 表示网络第 m 层第 i 个神经元的输出；$f(\cdot)$ 为 S 型非线性传递函数：$f(x) = 1/(1+e^{-x})$；$(W_i^m)^T$ 为第 m 层的第 i 个神经元与第 $m-1$ 层所有神经元的连接加权组成的向量转置；Y^{m-1} 为第 $m-1$ 层所有神经元的输出组成的向量：$Y^{m-1} = [1, Y_1^{m-1}, Y_2^{m-1}, \cdots, Y_{N_{m-1}}^{m-1}]^T$。

设网络输出 $\hat{y}_i^m = f(X_i, W)$，真实输出 $\bar{y}_i^m = f(X_i)$，样本输出 $y_i^m = f(X_i) + \xi_i$，则输出层神经元拟合偏差 $e_i = y_i^m - \hat{y}_i^m$，真实偏差 $\bar{e} = \bar{y}_i^m - \hat{y}_i^m$，则按照传统 BP 算法最小方差法获得的 LS 型网络误差函数为：

$$E_{LS} = \sum_{i=1}^{N} \phi(e_i) = \sum_{i=1}^{N} e_i^2 \quad (3)$$

BP 前馈网络算法是有导师指导的训练算法，通过调节网络权值，使得误差函数式(3)最小化。训练算法的导出是基于梯度下降算法，即沿误差函数的负梯度方向搜索最优网络加权，加权调整公式为：

$$W(t+1) = W(t) + \mu(-\nabla E(t)) \quad (4)$$

式中，$W(t)$ 为第 t 个迭代步的权值；$\nabla E(t)$ 为误差函数在 $W(t)$ 处的梯度；μ 为训练速度系数。

BP 算法的误差函数曲线表面是凸凹不平的，训练速度系数 μ 的取值影响到训练收敛速度，甚至出现发散的情况，近年来已有许多学者研究在训练过程中动态调整 μ 的值来优化网络[12-14]。为了方便描述，本文仍根据经验取为常数。

2 基于极大似然估计的改进 BP 网络

成功地运用 BP 算法进行系统辨识依赖于训练样本的质量，因为 BP 训练算法不考虑训练样本的误差，使用最小方差法获得的误差函数 E_{LS} 仅当偏差服从独立的且恒等的高斯分布时才能产生最佳值，E_{LS} 指导整个学习过程的最终目标是使所有的样本的拟合误差机会均衡地趋向于零，即网络输出逼近于每个受噪声污染的样本输出，而不是真实的输出，因此在样本中含有噪声的情况下，会导致实际应用中迭代次数越多，训练误差越小，而泛化能力却越差，效率反而明显降低，因为此时是使辨识模型内插所有的训练样本，而不是逼近真正的对象模型，导致辨识模型偏离[15]，这种不考虑前向操作时网络输入和输出样本的误差，无法保证辨识参数的可靠性。

基于极大似然估计的误差函数考虑了样本的误差，在训练样本时能够在考虑网络逼近行为的同时对噪声分布进行估计，以便抵消由噪声甚至严重干扰对数据的污染，从而得到更有效的逼近效果。

2.1 极大似然估计法的研究

极大似然估计的基本思想是构造一个自变量为模型参数 θ 的函数 $L(\theta)$，这个函数是变量 Y 的联合概率密度：$f(Y,\theta)$，参数估计的极大似然法就是选取参数 $\hat{\theta}$，使得似然函数 $L(\theta)$ 达最大值：

$$\hat{\theta} = ARG \max_{\theta \in \Theta} L(\theta) \quad (5)$$

对于给定的一组与参数 θ 有关的观测量 $Y = \{Y_1, Y_2, \cdots, Y_N\}$，因为观测结果是在被估计参数为某一定值的条件下取得的，所以 $f(Y,\theta)$ 实质上是条件概率密度函数，即 $f(Y,\theta) = f(Y|\theta)$，连续应用贝叶斯公式，可得似然函数：

$$f(Y_N|\theta) = f(y(N), Y_{N-1}|\theta) = \cdots = \prod_{i=1}^{N} f(y(i)|Y_{i-1}) \quad (6)$$

因为对数函数是单调函数，所以可设定似然函数为 $\ln f(Y|\theta)$。当观测数据足够多时，根据中心极限定理，可合理假定 $f(y(i)|y_{i-1},\theta)$ 服从高斯分布：

$$f(y(i)|y_{i-1},\theta) = [2\pi\sigma^2(i)]^{-1/2} \exp\{-\frac{[y(i) - \hat{y}(i)]^2}{2\sigma^2(i)}\} \quad (7)$$

式中，$\hat{y}(i) = E(y(i)|Y_{i-1})$，是条件均值；$\sigma^2(i) = \mathrm{cov}[y(i)|Y_{i-1}]$，是条件协方差。

2.2 基于极大似然估计的误差函数

对数据集中学习样本 (X_i, Y_i^m)，$(i = 1,2,\cdots,N_m)$，给定一组权值 W，由于误差的存在，网络输出向量 $\hat{y}_i^m$ 相对于权值 W 的条件概率密度为：

$$l(W) = P(\hat{y}_i^m|W) \quad (8)$$

如果样本之间统计是无关的，则连续应用贝叶斯公式得到所有样本的联合概率密度，即样本的似然函数为：

$$L(W) = P(\hat{y}_1^m, \hat{y}_2^m, \cdots, \hat{y}_{Nm}^m|W) = \prod_{i=1}^{Nm} p(\hat{y}_i^m|W) \quad (9)$$

如果网络模型正确，则所有的样本输出与实际输出之间的差别主要来源于输出样本的噪声，因此主要考虑拟合偏差，设样本输出误差服从高斯分布，则网络输出向量相对于权值 W 和高斯分布参数的条件密度函数为：

$$P(\hat{y}_i^m|W,\mu,\sigma) = (2\pi|Cy_i|)^{-1/2} \exp\{-\frac{(y_i^m - \hat{y}_i^m)^T (y_i^m - \hat{y}_i^m)}{2Cy_i}\} \quad (10)$$

式中，$Cy_i = \mathrm{cov}[\hat{y}_i^m|y_{i-1}^m]$，是输出样本的条件协方差矩阵，体现了输出样本的误差结构；拟合偏差 $(y_i^m - \hat{y}_i^m)$ 则作为样本误

差的均值。

根据极大似然理论，在 μ,σ 参数确定的条件下，使似然函数 $L(W)$ 最大的 W^* 为 W 的最优估计，即：

$$L(W^*,\mu,\sigma) = \max L(W,\mu,\sigma) \tag{11}$$

显然等价于使以下误差函数最小：

$$E(W,\mu,\sigma) = -2\ln L(W,\mu,\sigma) \tag{12}$$

因此，新的网络误差函数为：

$$E(W,\mu,\sigma) = \sum_{i=1}^{N_m}\frac{(y_i^m-\hat{y}_i^m)^T(y_i^m-\hat{y}_i^m)}{Cy_i}+2\sum_{i=1}^{N_m}\ln|Cy_i|+2N_m\ln\sqrt{2\pi} \tag{13}$$

略去常数项，最终的网络误差函数即为：

$$E(W,\mu,\sigma) = \sum_{i=1}^{N_m}\frac{(y_i^m-\hat{y}_i^m)^T(y_i^m-\hat{y}_i^m)}{Cy_i} \tag{14}$$

这样构建的网络，本文称之为似然 BP 网络。

与传统的误差函数式(3)相比，这里考虑了样本的协方差，即样本的误差。另外，当 $L(W^*,\mu,\sigma)$ 取最大值，即训练样本的偏差在趋于期望 μ 的误差中心曲面上时，学习强度最大，偏差以更快的速度趋于零，能抵抗样本自身的误差和噪声对学习的干扰。

2.3 似然 BP 网络反向学习过程

设训练样本集为 $(X_i,Y_i=f(X_i))$，$X\in R^P$，$Y\in R^M$，$i=1,2,\cdots,N$ 的多输入单输出的前向神经网络，其网络输出和样本输出分别为 $\hat{y}_i^m$，y_i^m，令 n 为迭代次数，w_{mh} 表示输入层与隐层之间的权值，w_{hp} 表示隐层与输出层之间的权值，修改这些权值是通过沿误差函数的负梯度方向反向学习方式来完成的，因此，误差信号的反向传播过程中首先计算权值修正量：

$$\Delta w_{mh} = -\mu\cdot\frac{\partial E(n)}{\partial w_{mh}} = -\mu\sum_{i=1}^{N_m}\frac{2e_i}{Cy_i}\cdot\frac{\partial e_i}{\partial w_{mh}} \tag{15}$$

$$\Delta w_{hp} = -\mu\cdot\frac{\partial E(n)}{\partial w_{hp}} = -\mu\sum_{i=1}^{N_m}\frac{2e_i}{Cy_i}\cdot\frac{\partial e_i}{\partial w_{hp}} \tag{16}$$

根据式(4)，对权值 w_{mh} 和 w_{hp} 进行修正：

$$\begin{cases} w_{mh}(n+1)=w_{mh}(n)+\Delta w_{mh} \\ w_{hp}(n+1)=w_{hp}(n)+\Delta w_{hp} \end{cases} \tag{17}$$

3 基于似然 BP 的网络安全态势预测模型

3.1 态势评估建模

态势评估是态势感知的核心，是态势预测的基础，它是对当前安全态势的一个动态理解过程，通过识别态势要素信息，确定它们之间的关联关系，根据所受到的威胁程度生成相应的安全态势图，来反映网络的当前安全状况。

根据目标网络所提供的各种服务、主机和系统所处于的网络安全威胁态势，建立态势评估模型。采用文献[9]提供的网络安全态势评估服务威胁指数 R_S、主机威胁指数 R_H 和系统威胁指数 R_L 的量化计算方法，并考虑其中的攻击严重度 D、服务重要性 V 和主机重要性 W 参数的权重。

定义 1 函数 F_S 表示 t 时刻目标网络的服务安全态势状况，记为：

$$F_S(S,C,N,D,t)=N(t)\cdot 10^{D(t)} \tag{18}$$

式中，S 表示目标网络当前所提供的某种服务；C 表示该服务受到的攻击种类；N 表示服务所受到的攻击的次数；D 表示攻击的严重程度；$N(t)$ 表示 t 时刻攻击的严重程度；$D(t)$ 表示 t 时刻攻击所发生的次数。

定义 2 函数 F_H 表示 t 时刻目标网络的主机安全态势状况，记为：

$$F_H(H,V,F_S,t)=V\cdot F_S(t) \tag{19}$$

式中，H 表示目标网络中的主机；V 表示服务在主机开通的所有服务中所占权重。

定义 3 函数 F_L 表示 t 时刻目标网络的系统安全态势状况，记为：

$$F_L(L,W,F_H,t)=W\cdot F_H(t) \tag{20}$$

式中，L 表示目标网络中的系统；W 表示主机在被评估局域网中所占重要性的权重。

3.2 态势预测建模

态势预测是态势感知的目的，是网络安全预警的前提，它是根据历史网络安全态势信息和当前网络安全态势信息来预测未来的网络安全趋势，为决策者制定安全策略提供依据。

在评估当前网络态势的基础上，建立基于似然 BP 的网络安全态势预测模型，用于实现网络安全态势的非线性时间序列预测。

定义 4 在 t(尽可能小)时间段内，从态势数据库中选择一个态势序列，作为未来网络安全态势预测模型的输入序列，记为 $X^{(0)}=(x_1^{(0)},x_2^{(0)},\cdots,x_n^{(0)})$，其中 $x^{(0)}t\geqslant 0,t=1,2,\cdots,n$；$X^{(1)}$ 是 $X^{(0)}$ 的 1-AGO 序列，记为 $X^{(1)}=(x_1^{(1)},x_2^{(1)},\cdots,x_n^{(1)})$，其中：

$$x_t^{(1)}=\sum_{i=1}^{t}x_i^{(0)},t=1,2,\cdots,n \tag{21}$$

根据定义 1 和定义 4，可得到针对目标网络的服务安全态势预测函数模型：

$$F_S(t+(n+1))=f(\sum_{i=1}^{n}F_S(t+i)) \tag{22}$$

由此可见，待识别参数 $F_S(t+(n+1))$ 与 $\sum_{i=1}^{n}F_S(t+i)$ 之间存在某种非线性映射关系。

同理可得目标网络的主机和系统安全态势预测函数模型，这里不再赘述。

根据 Kolmogorov 多层神经网络映射存在的定理，其非线性映射关系可以用三层的前馈人工神经网络近似的实现。如果用人工神经网络建立起这个映射关系，那么将各已知时间态势序列作为网络输入，网络输出就是要辨识的态势预测值。本文要求在 $F_S(t+(n+1))$ 和时间 $(t+(n+1))$ 的取值范围内，根据定义 1、定义 2 和定义 3 给出的网络服务、主机和系统的态势评估方法取得网络训练所需要的样本，应用似然 BP 的算法对网络进行训练，具体步骤如下：

1) 根据历史和当前的网络安全态势信息数据，分别建立关于服务、主机和系统的多输入单输出的态势预测 BP 人工神经网络模型 $P(\hat{y}_i^m|W)$ 和相应的网络误差函数 $E(W)$：

$$P(\hat{y}_i^m|W)=(2\pi|Cy_i|)^{-1/2}\exp\{-\frac{(y_i^m-\hat{y}_i^m)^T(y_i^m-\hat{y}_i^m)}{2Cy_i}\} \tag{23}$$

$$E(W)=\sum_{i=1}^{N_m}\frac{(y_i^m-\hat{y}_i^m)^T(y_i^m-\hat{y}_i^m)}{Cy_i} \tag{24}$$

式中，$\hat{y}_i^m$ 和 y_i^m 分别为第 m 层第 i 个神经元的实际输出和期望输出，对应于态势预测值；对于每个单点输入传播过程中的流程参量，式中 W 分别代表态势评估模型中的攻击严重度 D、服务重要性 V 和主机重要性 W 参数。

2) 训练该神经网络，使拟合偏差（$y_i^m - \hat{y}_i^m$）趋于零，对各权值进行自学习调整，寻找最优的参数组合，最后输出训练后的态势预测模型，网络输出就是我们所要辨识的下一时刻关于服务、主机或系统的态势预测值。在实际环境中，实时训练该网络，可得关于态势预测的拟合曲线。

4 仿真实验与结果

4.1 实验方法与环境

为了验证基于似然 BP 的网络安全态势预测模型的有效性和合理性，对训练输出的预测值与实际值进行比较，并测试模型训练对系统性能的影响。

实验网络环境中配置有 Linux Ubuntu 8.04 LTS /Inter Core 2 Duo E7200/2G/250G 主机，SUN，IBM 等大型服务器，并以多层路由器、千兆交换机、IDS、防火墙和光缆等构建成较复杂的网络。利用 Domain 2.2，Namp3.5 和 Trinity v3 等工具对受保护的某服务器进行攻击，采集 IDS、防火墙和系统的日志信息并进行分析，每 12 小时对该服务器内的服务和主机本身的安全态势做出评估，每次评估的值与以前的评估值一起建立时间序列，作为输入量，进入似然 BP 网络模型进行训练，最后依次输出各时刻的态势预测值，并在下一时刻计算出实际的态势评估值，进行比较。

4.2 实验步骤及结果

首先进行关于服务的安全态势预测。实验得到服务器上的 ftp，telnet，rpc，dns，socks，www 等服务受到的攻击次数，按照定义 1 评估出各服务的安全态势。试验中取得连续的 60 个 FTP 服务的安全态势值，用前面的 45 个作为训练样本，后 15 个作为测试样本，经预处理后，输入似然 BP 网络，对网络进行训练。预设定训练速度系数 $\mu=0.6$，目标误差 goal=0.0001，运行大约 34.327s 后，达到目标误差，迭代次数为 6295。

在对服务进行基于似然 BP 网络的态势预测的试验中，同时进行了使用普通 BP 网络的对比实验，发现经过迭代 11274 次后仍未达到目标误差，而时间已占用 153.231 秒。图 1 给出了基于似然 BP 网络的关于 FTP 服务的态势预测结果。最后综合考虑服务器上的各种服务，按照定义 2 评估出服务器主机的安全态势值，同样的方法得出基于似然 BP 网络的关于主机的态势预测结果，如图 2 所示。

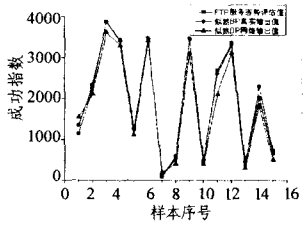

图 1 基于似然 BP 的 FTP 服务安全态势预测

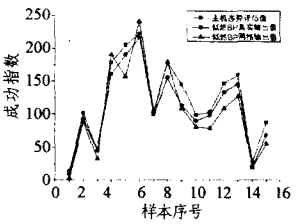

图 2 基于似然 BP 的主机安全态势预测

从图 1 和图 2 可以看出，基于似然 BP 的人工神经网络态势预测值能较好地逼近系统真实评估值，具有较好的预测效果。

由于 BP 神经网络的应用效果较依赖于其计算速度和对系统性能的影响，因此，有必要测定应用该算法后系统性能的变化情况。本文不考虑态势评估过程对系统的影响，只考虑基于似然 BP 的态势预测过程对系统性能的影响。通过测定网络训练的时间和训练结束后 CPU 的占用率变化发现，系统稳定后整体性能有所下降，但不高于 4%，因此是可以接受的，如图 3 和图 4 所示。

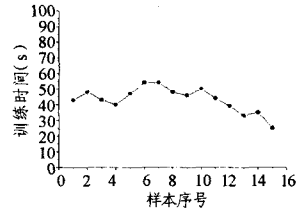

图 3 似然 BP 的训练时间

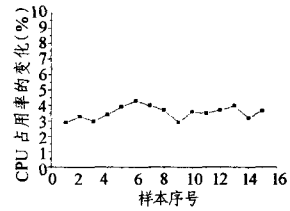

图 4 似然 BP 训练结束后 CUP 占用率变化

结束语 网络安全态势预测技术对于发现潜在的、恶意的攻击行为，降低网络攻击带来的危害，制定合适的网络安全策略，提高网络的应急响应能力等都有着重要的意义。本文将 BP 人工神经网络引入态势预测领域，并对其进行改进做了探讨，建立了基于似然 BP 的网络安全态势预测模型，实验表明，在可接受的系统性能影响范围内，该方法能有效地预测网络安全态势。需要指出的是，实验中以 12 小时为时间段对安全态势进行预测，粒度较大，测点较少。实际上，对于 BP 人工神经网络，输入信息越少，收敛速度就越慢，因此，该方法对于细粒度时间段的安全态势预测会有更好的表现。下一步的工作是对预测模型进行完善，对训练过程进行优化。

参 考 文 献

[1] Endsley M R. Toward a theory of situation awareness in dynamic systems[J]. Human Factors, 1995, 37(1): 36-24

[2] Batsell S G, Rao N S, Shankar M. Distributed intrusion detection and attack containment for organizational cyber security[EB/OL]. http://www.ioc.ornl.gov/projects/documents/containment.pdf, 2006

[3] 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

[4] US Infrastructure Assurance Strategic Roadmaps. Strategies for preserving our national security[R]. Sandia National Laboratories, Sand Report. 1998: 98-1496

[5] Kijewski P. ARAKIS-An early warning and attack identification system[C] // Proc of the 16th Annual First Conference. Dudapest, Hungary, 2004

[6] 胡华平，张怡，陈海涛，等. 面向大规模网络的入侵检测与预警系统研究[J]. 国防科技大学学报，2003，25(1)：21-25

[7] Gates C, Collins M, Duggan M, et al. More netflow tools: for performance and security[C] // Proc of the 18th Large Installation Systems Administration Conference. Atlanta, Georgia, USA, 2004

[8] Bass T. Intrusion detection systems and multi-sensor data fusion: creating cyberspace situational awareness[J]. Communication of the ACM, 2000, 43(4): 99-105

[9] 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

[10] 赵国生，王慧强，王健. 基于灰色关联分析的网络可生存性态势评估研究[J]. 小型微型计算机系统，2006，27(10)：1861-1864

[11] Bearavolu R, Lakkaraju K, Yurcik W. NVisionIP: An animated state analysis tool for visualizing netFlows[EB/OL]. http://www.cert.org/flocon/2005/presentations/NVisionIPFlocon2005.pdf, 2005

（下转第 168 页）

```
<profileURI>
  ......
</profileURI>
<profileName>UML.sec</profileName>
 <name>用户</name>
 ......
        <uml.sequencediagram.model.SyncMessageModel>
        // 顺序图同步消息模型
          <name>登录()</name>
          <stereoType>access</stereoType>
          ......
```

图 5(b)　网上交易系统包含安全属性顺序图的 xml 描述

```
......
<packagedElement xmi:type="uml:Stereotype"
xmi:id=" " name="access">
    <ownedAttribute xmi:id=" " name="base_
      Abstraction" association=" ">
      <type xmi:type="uml:Sequence" href="pathmap:// UML_
        METAMODELS/UML.metamodel. uml#Abstraction"/>
    </ownedAttribute>
</packagedElement> ......
```

图 6　UMLsec profile 文件片段

```
<uml.classdiagram.model.ClassModel>
        <name>access</name>
          <children>
            <uml.classdiagram.model.AttributeModel>
            // access类的属性
              <name>anonymous</name>
            // 确定访问方式：是否匿名访问
              <type>boolean</type>
            </uml.classdiagram.model.AttributeModel>
            <uml.classdiagram.model.OperationModel>
            // access类的操作
              <name>session</name>
            // 匿名访问：设置session失效时间
              <type>string</type>
              <name>name</name>
            // 实名访问：验证用户名、密码
              <type>string</type>
              <name>password</name>
              <type>string</type>
              <name>IP</name>
            // 记录访问者的IP地址
              <type>string</type>
            </uml.classdiagram.model.OperationModel>
          </children>
</uml.classdiagram.model.ClassModel>
```

图 7　《access》构造型对应的平台相关描述

得到系统集成安全性建模的 PIM 之后，可通过 XSLT (Extensible Stylesheet Language Transformations，扩展样式表转换语言)制定针对不同平台的转换规则，实现向 PSM 的转换，即将 PIM 中的安全属性映射到指定平台，最终使安全策略在所开发的软件中得以实现。为了使转换过程易实现、易操作、易修改，所有 PIM，PSM 均保存为 xml 文件。针对不同的应用系统，在相同的开发平台下，安全属性模型构建完成之后，可使用相同的转换策略实现安全属性模块。与传统建模方法相比，profile 文件对安全属性进行了有效的划分，明确了添加在每种图形之上的具体构造型，并使其具有指定的意义，作为模型转换的基础。图 7 给出了构造型《access》对应的 PSM 描述。为防止系统访问人数过载，需对匿名使用者设置访问时长，其限制可根据应用系统的类型及访问用户身份、数量的要求决定，在即将超时之前给予登录系统提示，直至会话关闭，同时匿名访问时，权限受到一定控制。而实名访问比较容易控制使用系统的用户数量上限。为防止恶意攻击，两种访问方式均需记录用户的 IP 地址。Profile 中的其他构造型以类似方法描述。

3.4　支持工具

为支持本文介绍的集成安全分析的模型驱动软件开发方法，在开源的 Eclipse 平台下开发了安全建模工具。该工具作为 Eclipse 插件使用，提供 UML 建模功能，并将模型保存为 xml 格式。在完成系统 PIM 模型建立之后，通过菜单加载 UMLsec profile。根据预先定义的 profile 文件可对相应的模型添加构造型，实现对软件安全性建模。

结束语　现代信息社会对计算机的依赖，主要表现为对软件的依赖。计算机软件已经成为信息基础设施中至关重要的环节。提高软件质量，保障软件安全性，具有巨大的社会价值和经济价值。

本文提出了一种集成安全分析的模型驱动软件开发方法，它采用 UML 安全扩展机制建立系统安全相关的平台无关模型，从而将软件的安全性分析提前到了设计的早期，实现了 MDA 方法中软件安全属性的建模，降低了后期开发的风险与成本。在进一步的工作中，需要深入研究不同应用领域软件系统存在的典型安全问题，设计出具有针对性的 UMLsec profile，并将该方法应用于更多的软件项目中。

参 考 文 献

[1] 周新蕾. 软件安全性分析技术及应用[J]. 质量与可靠性，2005(3)：37-40

[2] Miller J，Mukerji J，et al. Model driven architecture[EB/OL]. Ormsc/2001-07-01：Needham，Object Management Group，2001，1-31. http：//www.omg.org/cgi-bin/doc? ormsc/2001-07-01

[3] de Miguel M A，Briones J F，Silva J P，et al. Integration of safety analysis in model- driven software development[J]. IET Software，2008，2(3)：260-280

[4] Jürjens J，Munich T. UMLsec：Presenting the Profile[EB/OL]. http：//www.omg.org/news/meetings/workshops/DOCsec-2002_Proceedings/01-2_Juergens_UMLsec_Tutorial.pdf

[5] Jürjens J，Munich T. Secure Software Architecture Description using UML [EB/OL]. http：//wiki.lassy.uni.lu/tiki-download_file.php? fileId=165

[6] Best B，Jürjens J，Nuseibeh B. Model- based Security Engineering of Distributed Information Systems using UMLsec[C]// 29th International Conference on Software Engineering (ICSE 2007). Washington：IEEE，2007：581-590

(上接第 100 页)

[12] Kim Yong soo，Kim Sung-ihl. Fuzzy neural network model using a fuzzy learning vector quantization with the relative distance [C] //Proc of the 7th International Conference on Hybrid Intelligent Systems. Kaiserlautern，2007

[13] Behera L，Kumar S，Patnaik A. On adaptive learning rate that guarantees convergence in feedforward networks [J]. IEEE Transactions on Neural Networks，2006，17(5)：1116-1125

[14] Kuo Ming-jen，Lin Tsung-chih. Dynamical optimal training for behavioral modeling of nonlinear circuit elements based on radial basis function neural network[C] // Proc of the Asia-Pacific Symposium on Electromagnetic Compatibility and 19th International Zurich Symposium on Electromagnetic Compatibility. Singapore，2008

[15] Sh Hosseini，Ch Jutten. Maximun likelihood neural approximation in presence of additive colored noise[J]. IEEE Transactions on Neural Networks，2002，13(1)：117-131