doi:10.3969/j.issn.1000-436x.2013.z1.016

基于模糊 Petri 网的网络风险评估模型

高翔，祝跃飞，刘胜利，费金龙，刘龙
(解放军信息工程大学 数学工程与先进计算国家重点实验室，河南 郑州 450002)

摘 要：针对网络安全风险评估过程中存在的复杂性，以资产、脆弱性和威胁为安全评估的关键因素，建立安全分析的层次化评估指标体系。引入可信度概念，提出了一种基于模糊 Petri 网的安全风险评估模型以及模糊推理算法，同时结合层次分析法，采取定性与定量分析相结合的方法进行安全评估。实例分析表明：与传统的综合风险评估方法相比，基于模糊 Petri 网的风险评估方法给出的结果更加准确和科学。因此，该方法更适合应用于实际的网络系统风险评估中。

关键词：安全风险评估；模糊 Petri 网；建模；层次分析法
中图分类号：TP301 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0126-07

Risk assessment model based on fuzzy Petri nets

GAO Xiang, ZHU Yue-fei, LIU Sheng-li, FEI Jin-long, LIU Long
(State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: Aiming at the complex in the process of network security risk assessment, the asset, vulnerability and threat were used as the major factors in security assessment to establish the hierarchical index system for security assessment. The concept of credibility was introduced, and the security risk assessment model and fuzzy reasoning algorithm based on fuzzy Petri net were also proposed, making use of fuzzy Petri nets method joined together with the AHP to analyze the question, and combining qualitative analysis and quantitative analysis together. The example analysis shows that the obtained results are more accurate and scientific compared with traditional assessment methods. Therefore, this method is an effective network system risk assessment method.

Key words: security risk assessment; fuzzy Petri net; modeling; analytic hierarchy process

1 引言

随着微博、社交网络和即时通信的普及与发展，互联网信息日益纷繁庞杂，网络信息的安全问题变得十分突出。为了保证网络系统的正常运行，需要对网络进行风险评估，主动发现安全隐患，根据评估结果采取对应的措施以减少经济损失。安全风险评估是指从风险管理角度，运用定性及定量的分析方法和手段，系统地分析信息、信息系统资产所面临的人为和自然的威胁，以及这些威胁事件一旦发生可能造成的危害程度[1]。而对网络系统进行建模与分析是网络安全风险评估中一种行之有效的方法。

目前，基于模型的风险评估方法已取得了一些成果。常见的模型有攻击图模型[2]、博弈模型[3]、攻击树模型[4]、威胁传播模型[5]，从不同角度分析和评估系统安全反映了网络系统的状态变化，但这些模型存在一定的问题，例如：1)在评估中存在模糊因素不便统计；2)不适于对经验知识进行建模与推理；3)不易通过模型进行仿真从而分析系统的性能；4)缺乏直观的图形实现方法。相比之下，Petri 网作为一种基于图形的数学建模工具，由于具有直观形象的特点，适合于描述异步、并行的系统而被广泛地应用于信息系统建模分析和性能评价。但是

收稿日期：2013-06-18
基金项目：国家自然科学基金资助项目(60902102)；郑州市科技创新团队基金资助项目(10CXTD150)
Foundation Items: The National Natural Science Foundation of China (60902102); The Program of Zhengzhou Science and Technology Innovation Team Project (10CXTD150)

传统 Petri 网不能有效描述评估指标的模糊性，而模糊 Petri 网(FPN)[6]是基本 Petri 网的扩展，容易处理评估指标的不确定性和模糊性，所以能够较好地对模糊知识建模和推理。

在对网络风险评估的不确定性、模糊性的推理判断中，由于模糊 Petri 网更符合人类的思维和认知方式，并且具有较好的并行处理能力，所以用模糊 Petri 网描述和分析风险事件的模糊性和并发性具有广泛的意义。本文提出了一种基于模糊 Petri 网的网络安全风险评估模型，将风险评估看作是多个阶段动态决策的模糊知识推理过程，并在每一阶段建立基于模糊 Petri 网的安全评估体系。给出了一种基于模糊 Petri 网的系统风险模糊推理算法(SRFRA, system risk fuzzy reasoning algorithm based on fuzzy Petri net)，同时结合层次分析法[7]，定性与定量分析相结合地进行网络安全评价。另外，通过分析风险因素事件的可信度，使评估结果更加准确和客观，在一定程度上避免了传统评估方法存在的主观性和片面性问题。

2　网络安全风险评估指标体系

2.1　评估准则

在网络安全风险评估中，构建评估指标体系是最为关键的环节，它将直接影响评估的全面性、合理性及有效性，但影响网络安全程度的各种因素存在不确定性的问题，为此必须进行深入分析以确定它们在安全评估中的相对重要性。

影响网络系统安全的因素有资产的影响、脆弱性的严重程度和威胁的破坏程度等[8]。其中，对资产的影响主要指信息系统数据资产和物理资产由于意外操作或者自然灾害所造成的破坏，且资产越重要，影响程度越大；脆弱性的严重程度主要指系统中的缺陷能够增加系统被攻击的可能性，且资产的脆弱性严重程度越高，被威胁利用造成的危害就越大；威胁的破坏程度主要指由于非授权的操作对信息系统资产保密性、完整性和可用性的影响程度，这里的威胁主要来自于人员，如网络攻击。这里将资产分析、脆弱性分析和威胁分析的相关结果作为网络安全风险评估的基本准则。

2.2　指标体系的构建

由于网络安全风险评估的复杂性，本文将该问题分解成若干部分，形成不同的层次，同一层次的元素对下一层次的某些元素起支配作用，同时它又受到上面层次元素的支配。如图 1 所示，网络安全风险评估体系由影响因素事件构成，共分为 3 层。最高层为一级指标（即网络安全风险评估），目的是获得系统的风险评估值和风险等级；中间层为二级指标（即风险评估的 3 个准则：资产分析、脆弱性分析和威胁分析）；最下层为三级指标（即要考虑的风险因素事件），本文建立了 9 个三级指标。

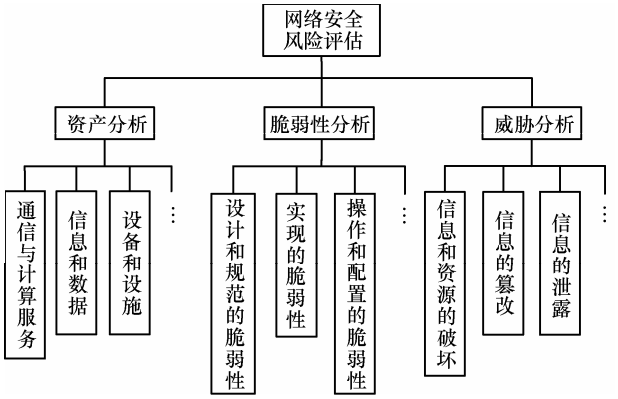

图 1　网络安全风险评估体系

3　FPN 评估模型及推理算法

3.1　相关定义

定义 1　模糊 Petri 网可以描述为一个九元组

$$FPN = (P, T, D, \boldsymbol{IN}, \boldsymbol{OUT}, F, W, R, M)$$

其中，$P = \{p_1, p_2, \cdots, p_n\}$ 是库所的有限集合；$T = \{t_1, t_2, \cdots, t_n\}$ 为变迁的有限集合；$D = \{d_1, d_2, \cdots, d_n\}$ 为命题的有限集合；$\boldsymbol{IN}: P \to T$ 为变迁输入矩阵，$\boldsymbol{IN} = \{\alpha_{ij}\}$，$\alpha_{ij} \in \{0,1\}$，当 p_i 是 t_j 的输入时，$\alpha_{ij} = 1$，当 p_i 不是 t_j 的输入时，$\alpha_{ij} = 0$；$\boldsymbol{OUT}: T \to P$ 为变迁输出矩阵，$\boldsymbol{OUT} = \{\beta_{ij}\}$，$\beta_{ij} \in \{0,1\}$，当 p_i 是 t_j 的输出时，$\beta_{ij} = 1$，当 p_i 不是 t_j 的输出时，$\beta_{ij} = 0$；$F: T \to [0,1]$ 表示变迁的可信度函数，每个变迁都有相应的可信度，$F(t_j) = \mu_j \ (j = 1,2,\cdots,m)$，$\mu_j$ 表示模糊规则 t_j 的置信度；$W: P \to [0,1]$ 表示库所 p_i 的可信度函数，$W(p_i) = \{w_i\}$，$i = 1,2,\cdots,n$；$R: P \to D$，相关函数，表示库所到命题的映射，即库所对应的命题；$\boldsymbol{M}(0)$ 是 $n \times q$ 阶的初始状态矩阵，其元素 m_{ij}^0 是 p_i 在 j 等级的初始状态值，$n \times q$ 表示 n 个库所在 q 个等级中的状态，$\boldsymbol{M}(k)$ 为发生了 k 次变迁后的状态矩阵。

定义 2 根据经验或一段时期观察值判断一个事物或现象的可信程度期望值称为可信度。命题的可信度 w_n 可表示为 $CF(e)$；规则的可信度 μ_j 可表示为 $CF(h,e)$，即表示当前提条件 e 所对应的证据为真时，它对结论 h 为真的支持程度。h 的计算公式为

$$CF(h)=CF(h,e)\cdot\max(0,CF(e)) \tag{1}$$

定义 3 设 A 是论域 U 上的一个集合，其特征函数表示为 $\mu A(x):U\to[0,1]$。对 $\forall x\in U$，$\mu A(x)\in[0,1]$ 是一个其元素 x 属于 A 的程度的一个函数，称为隶属函数。由此上述命题的可信度 w_i 和规则置信度 μ_j 都可以由隶属函数来刻画，其取值范围为 $[0,1]$。

定义 4 风险等级评价矩阵 $\boldsymbol{Q}$，设评估矩阵为 $\boldsymbol{Q}=(10,8,6,4,2)$，其中，10 表示风险等级为“高”；8 表示风险等级为“较高”；6 表示风险等级为“中”；4 表示风险等级为“较低”；2 代表风险等级为“低”。

3.2 模糊产生式规则的 FPN 表示

模糊 Petri 网为模糊产生式规则建立了一个直观的图形化模型，同时也为模糊推理建立了结构化的推理机制。FPN 的每个变迁对应一个规则，这里表示评估状态的改变，变迁的输入库所和输出库所分别表示规则的前提条件和结论命题，这里可以表示评估指标状态。

模糊产生式规则的一般形式为

Type1 如果 $d_1(w_1)$ 与 $d_2(w_2)$ 与…与 $d_n(w_n)$，那么 $d_g(w_g)(CF=\mu_j)$

Type2 如果 $d_1(w_1)$ 或 $d_2(w_2)$ 或…或 $d_n(w_n)$，那么 $d_g(w_g)(CF=\mu_j)$

其中，$d_1,d_2,\cdots,d_n$ 表示一组前提，d_g 表示若干结论，$w_1,w_2,\cdots,w_n,w_g$ 是命题的可信度，$\mu_j\in[0,1]$ 是规则的置信度。以上 2 类模糊推理规则可用图 2、图 3 的 FPN 模型来表达。以上目标命题的可信度可通过图 2 和图 3 求解，本文拟采用第二类模糊推理规则计算目标命题的可信度。

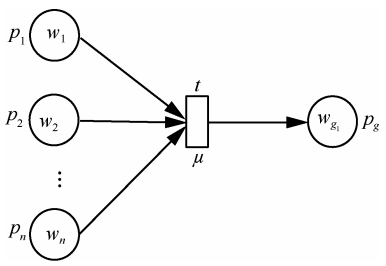

图 2 第 1 类模糊产生式的 FPN 模型

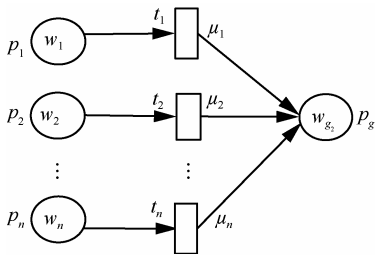

图 3 第 2 类模糊产生式的 FPN 模型

$$w_{g_1}=\min(w_1\mu,w_2\mu,\cdots,w_n\mu) \tag{2}$$

$$w_{g_2}=\max(w_1\mu_1,w_2\mu_2,\cdots,w_n\mu_n) \tag{3}$$

3.3 权重系数计算

将层次分析法用于相关权重系数计算，其计算步骤如下。

1) 由专家逐层对两两元素进行比较，根据 1~9 比例标度法确定其相对重要度，建立判断矩阵 $\begin{bmatrix}a_{11}a_{12}\cdots a_{1n}\\a_{21}a_{22}\cdots a_{2n}\\\vdots\\a_{n1}a_{n2}\cdots a_{nn}\end{bmatrix}$，$a_{ij}$ 表示要素 a_i 对要素 a_j 的相对重要度。

2) 根据方根法计算各元素的相对权重 $\boldsymbol{W}=(W_1,W_2,\cdots,W_n)$。其中，$m_i=\sqrt[n]{a_{i1}a_{i2}\cdots a_{in}}$

$$W_i=\frac{m_i}{\sum_{i=1}^{n}m_i} \tag{4}$$

计算矩阵的最大特征根为

$$\lambda_{\max}=\sum_{i=1}^{n}\frac{a_{i1}W_1+a_{i2}W_2+\cdots+a_{in}W_n}{nW_i} \tag{5}$$

3) 计算判断矩阵的一致性指数 CI。

$$CI=\frac{\lambda_{\max}-n}{n-1} \tag{6}$$

其中，n 为判断矩阵的阶数，若 $CI<0.1$，表明矩阵一致性成立。

3.4 模糊推理算法

定义 5 在图 3 中，也可以用 ν_j 表示变迁 t_j 的置信度，表示各个条件命题影响目标命题的权重，且满足 $\nu_1+\nu_2+\cdots+\nu_n=1$，$0<\nu_j<1\ (j=1,2,\cdots,n)$。

设 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{E}$ 均为 $n\times q$ 阶矩阵，$\boldsymbol{D}$ 为 n 维向量，则

加法算子 $\oplus$：$\boldsymbol{C}=\boldsymbol{A}\oplus\boldsymbol{B}\Leftrightarrow\boldsymbol{C}_{ij}=\max(a_{ij},b_{ij})$ (7)

直乘算子⊗： $\boldsymbol{E}=\boldsymbol{D}\otimes\boldsymbol{B}\Leftrightarrow e_{ij}=d_i\times b_{ij}$　(8)

在给出相关定义的基础上，本文提出了一种模糊推理算法 SRFRA，在对系统进行安全评估时，影响系统安全的各因素事件转换为 FPN 的库所，而评估状态转变的过程转换为 FPN 的变迁。具体实现如下。

系统风险模糊推理算法(SRFRA)

将网络安全风险评估体系转变为模糊 Petri 网，由模糊 Petri 网的定义可以求出输入矩阵 $\boldsymbol{IN}$ 和输出矩阵 $\boldsymbol{OUT}$，通过专家评价以及层次分析法可确定初始状态矩阵 $\boldsymbol{M}(0)$、变迁的置信度向量 $\boldsymbol{V}=\{v_j\}$。这里，矩阵 $\boldsymbol{M}(0)$ 中元素 m_{ij}^0 表示事件 p_i 在风险等级 j 的初始状态，置信度 v_j 表示系统中各个因素事件影响系统安全的权重。

输入：输入矩阵 $\boldsymbol{IN}$，输出矩阵 $\boldsymbol{OUT}$，置信度向量 $\boldsymbol{V}$，评价矩阵 $\boldsymbol{Q}$，初始状态矩阵 $\boldsymbol{M}(0)$

输出：系统风险评估值

Step1　令 $k=0$，变迁输入因素为真的可信度为 $\boldsymbol{IN}^{\mathrm{T}}\boldsymbol{M}(k)$，变迁触发后输出库所的可信度为 $\boldsymbol{V}\otimes\boldsymbol{OUT}$。

Step2　计算变迁发生后的下一个状态：$\boldsymbol{M}(k+1)=\boldsymbol{M}(k)\oplus[\boldsymbol{V}\otimes\boldsymbol{OUT}][\boldsymbol{IN}^{\mathrm{T}}\boldsymbol{M}(k)]$。

Step3　若 $\boldsymbol{M}(k+1)\neq\boldsymbol{M}(k)$，令 $k=k+1$，转 Step2。

Step4　如果 $\boldsymbol{M}(k+1)=\boldsymbol{M}(k)$，则停止计算。

Step5　计算各库所事件的评价指标 $\boldsymbol{F}=\boldsymbol{M}(k)\boldsymbol{Q}^{\mathrm{T}}$，其中，$\boldsymbol{F}$ 为 n 维向量，该向量的最后一个元素对应系统的一级评价指标，表示为 f_n。

Step6　调用事件可信度推理子算法可得 w_g，计算系统综合风险评估值 $S=f_nw_g$。

在该算法中，系统的综合风险评估值由事件发生的可信度 w_g 与其相应的评价指标 f_n 共同决定。同理，各指标的风险评估值可由类似方法求出。推理算法中采用了矩阵运算，充分地利用了模糊 Petri 网的并行处理能力，推理过程更加简单和易于实现。

事件可信度推理子算法

定义 6　*npw* 集合，存放所有库所名和库所的可信度，存放格式为

$$npw=\{p_1,w_1,p_2,w_2,\cdots,p_n,w_n\}$$

定义 7　*nbf* 集合，存放模糊规则的置信度、变迁的直接输入库所名 $BP(t_j)$ 和直接输出库所名 $FP(t_j)$，存放格式为

$$ubf=\{\mu_1,BP(t_1),FP(t_1),\mu_2,BP(t_2),FP(t_2),\cdots,\mu_n,BP(t_n),FP(t_n)\}$$

定义 8　*nps* 集合，存放开始库所名集合，存放格式为

$$nps=\{p_{s1},p_{s2},\cdots,p_{ss}\}$$

输入：*npw* 集合，*nbf* 集合，*nps* 集合

输出：目标事件可信度 w_g

Step1　令 $l=1$，m 为 *nbf* 集合中 t_j 的个数，***END*** 为结束标志。

Step2　取出 *nps* 中的第 l 个库所名 p_s。

Step3　若 $(p_s=\boldsymbol{END})$，输出推理结果，算法结束。

Step4　For(int $j=1;j\leqslant m;j++$)

a)　If $(p_s\in BP(t_j))$

b)　$\{p_g\leftarrow FP(t_j)$；

c)　$w_g\leftarrow w(p_s)\cdot\mu_j$；

d)　If$(w_g=0)$，即当目标库所 p_g 的可信度值未知时；

e)　$w(p_g)\leftarrow w_g$；

f)　Else　$w(p_g)\leftarrow\max(w_g,w(p_g))\}$。

Step5　若 $p_g\notin nps$　将 p_g 插入到 *nps* 集合的结束标志前。

Step6　令 $l++$，转 Step2。

3.5　算法复杂性分析

基于FPN评估模型的系统风险模糊推理算法(SRFRA)的关键是库所下一状态公式：$\boldsymbol{M}(k+1)=\boldsymbol{M}(k)\oplus[\boldsymbol{V}\otimes\boldsymbol{OUT}][\boldsymbol{IN}^{\mathrm{T}}\boldsymbol{M}(k)]$ 以及目标事件可信度 w_g 的求解。这里，$\boldsymbol{M}(k)$ 为 $|P|\times q$ 阶矩阵，$\boldsymbol{IN}$ 和 $\boldsymbol{OUT}$ 为 $|P|\times|T|$ 阶矩阵，其中，$|P|$ 为 FPN 模型中库所的个数，$|T|$ 为变迁的个数，q 代表风险评价的等级。易知在该公式中共进行了 2 次矩阵相乘计算，因此其时间复杂度为 $O(|T|\times|P|\times q+|P|\times|T|\times q)$。另外，易求得子算法的时间复杂度为 $O(ml)$。分析可见，整个算法的复杂度可以满足系统风险评估的需求。

4　实例分析

4.1　实验描述

为了验证该模型和推理算法的可行性，以某大学校园网为例，由相关部门提供的资料对其进行网

络安全风险评估。首先建立风险层次评估指标体系，如图 1 所示。

4.2 模型构建与计算过程

Step1 构建 FPN 模型。根据模糊 Petri 网的定义，用命题 d_1、d_2、d_3、d_4、d_5、d_6、d_7、d_8、d_9、分别表示规则的前提条件，d_{a}、d_{b}、d_{c}、d_{g} 表示目标状态。其中，d_1 表示通信与计算服务；d_2 表示信息和数据；d_3 表示设备和设施；d_4 表示设计和规范的脆弱性；d_5 表示实现的脆弱性；d_6 表示操作和配置的脆弱性；d_7 表示信息和资源的破坏；d_8 表示信息的篡改；d_9 表示信息的泄露；d_{a} 表示资产分析结果，判断资产易遭受破坏的可信度；d_{b} 表示脆弱性分析结果，判断系统中存在脆弱性的可信度；d_{c} 表示威胁分析结果，判断系统面临威胁的可信度；d_{g} 表示最终的系统安全分析结果，判断系统总体存在风险的可信度。

已知模糊产生式规则如下：

R1：如果 $d_1(w_1)$ 或 $d_2(w_2)$ 或 $d_3(w_3)$，那么 $d_{\mathrm{a}}(w_{\mathrm{a}})$；

R2：如果 $d_4(w_4)$ 或 $d_5(w_5)$ 或 $d_6(w_6)$，那么 $d_{\mathrm{b}}(w_{\mathrm{b}})$；

R3：如果 $d_7(w_7)$ 或 $d_8(w_8)$ 或 $d_9(w_9)$，那么 $d_{\mathrm{c}}(w_{\mathrm{c}})$；

R4：如果 $d_{\mathrm{a}}(w_{\mathrm{a}})$ 或 $d_{\mathrm{b}}(w_{\mathrm{b}})$ 或 $d_{\mathrm{c}}(w_{\mathrm{c}})$，那么 $d_{\mathrm{g}}(w_{\mathrm{g}})$；

根据网络安全风险评估指标体系以及专家规则，同时结合层次分析法可得其对应的 FPN 模型如图 4 所示。

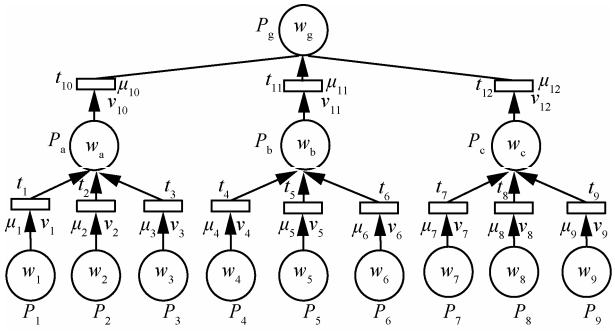

图 4 网络安全风险评估体系的 FPN 模型

Step2 计算因素事件发生的可信度。根据专家知识库，可令上述规则中命题的可信度分别为 $w_1=0.6$，$w_2=0.7$，$w_3=0.9$，$w_4=0.5$，$w_5=0.8$，$w_6=0.6$，$w_7=0.7$，$w_8=0.9$，$w_9=0.8$。变迁 $t_1\sim t_{12}$ 表示相对应因素事件对网络系统安全的影响，令规则变迁的规则置信度 μ_j 为 $U=\{\mu_j\}=\{0.8,0.7,0.6,0.5,0.6,0.8,0.4,0.5,0.3,0.8,0.5,0.6\}$，求取命题 d_{a}、d_{b}、d_{c}、d_{g} 的可信度 w_{a}、w_{b}、w_{c}、w_{g}。

将上述数据用于作者的推理算法进行实例推理，可得命题 d_{a} 的 $w_{\mathrm{a}}=0.54$，说明资产存在风险，可信度为 0.54。命题 d_{b} 的 $w_{\mathrm{b}}=0.48$，说明系统中存在脆弱性弱点，可信度为 0.48。命题 d_{c} 的 $w_{\mathrm{c}}=0.45$，说明系统面临网络威胁，可信度为 0.45。目标命题 d_{g} 的 $w_{\mathrm{g}}=0.432$，说明该系统总体存在风险的可信度为 0.432。

Step3 求解评价指标。根据输入输出矩阵定义可得输入矩阵 $\boldsymbol{IN}$ 和输出矩阵 $\boldsymbol{OUT}$，安全评估指标体系中指标的评估向量可由专家评判法确定。例如，由专家对风险因素的概率评价，得到三级指标因素的事件 P_1 的风险评估向量如表 1 所示。

表 1 P_1 风险等级区间量化表

评估等级	评估向量
高(8~10)	0.2
较高(6~8)	0.2
中(4~6)	0.2
较低(2~4)	0.3
低(0~2)	0.1

依照以上方法，可确定每个三级指标的风险评估向量，通过分析历史数据得到 FPN 各库所的初始标识 $\boldsymbol{M}(0)$。

$$\boldsymbol{M}(0)=\begin{bmatrix}0.2&0.2&0.2&0.3&0.1\\0.0&0.4&0.2&0.3&0.1\\0.4&0.4&0.1&0.1&0.0\\0.1&0.2&0.4&0.2&0.1\\0.1&0.3&0.3&0.2&0.1\\0.4&0.4&0.1&0.1&0.0\\0.0&0.0&0.1&0.5&0.4\\0.1&0.1&0.4&0.4&0.0\\0.0&0.1&0.4&0.3&0.2\\0.0&0.0&0.0&0.0&0.0\\0.0&0.0&0.0&0.0&0.0\\0.0&0.0&0.0&0.0&0.0\\0.0&0.0&0.0&0.0&0.0\end{bmatrix}$$

各指标之间的权重（即变迁的置信度向量 $\boldsymbol{V}$）可以采用层次分析法进行计算。例如，求解三级指标 P_1,P_2,P_3 的权重系数，采用 $1\sim9$ 比例标度法建立

判断矩阵 $\boldsymbol{R}$ 。

$$\begin{pmatrix} 1 & 2 & 7/4 \\ 1/2 & 1 & 5/3 \\ 4/7 & 3/5 & 1 \end{pmatrix}$$

根据 3.3 节的式(4)可得：$\boldsymbol{W}=(0.481,0.298,0.222)$，即 $v_1=0.481$，$v_2=0.298$，$v_3=0.222$，由式(5)求得矩阵的最大特征根为 $\lambda_{\max}=3.046$，由式(6)求得一致性指标为 $CI=0.023<0.1$，表明判断矩阵一致性成立。由上述方法可得各变迁的置信度向量为：$\boldsymbol{V}=$ {0.481, 0.298, 0.222, 0.248, 0.448, 0.304, 0.362, 0.199, 0.439, 0.474, 0.306, 0.220}。

由推理算法进行程序迭代得到最终的 $\boldsymbol{M}(k)$ 。

$$\boldsymbol{M}(2)=\boldsymbol{M}(3)=\begin{bmatrix} 0.200 & 0.200 & 0.200 & 0.300 & 0.100 \\ 0.000 & 0.400 & 0.200 & 0.300 & 0.100 \\ 0.400 & 0.400 & 0.100 & 0.100 & 0.000 \\ 0.100 & 0.200 & 0.400 & 0.200 & 0.100 \\ 0.100 & 0.300 & 0.300 & 0.200 & 0.100 \\ 0.400 & 0.400 & 0.100 & 0.100 & 0.000 \\ 0.000 & 0.000 & 0.100 & 0.500 & 0.400 \\ 0.100 & 0.100 & 0.400 & 0.400 & 0.000 \\ 0.000 & 0.100 & 0.400 & 0.300 & 0.200 \\ 0.185 & 0.304 & 0.178 & 0.256 & 0.078 \\ 0.191 & 0.301 & 0.264 & 0.170 & 0.007 \\ 0.020 & 0.064 & 0.291 & 0.392 & 0.233 \\ 0.151 & 0.251 & 0.230 & 0.261 & 0.091 \end{bmatrix}$$

由最终的矩阵推理结果可得该校园网综合风险的评判向量为

$$(0.151 \quad 0.251 \quad 0.230 \quad 0.261 \quad 0.091)$$

通过加权平均可得目标事件的评判指标为 6.12。

Step4　风险值的综合集成。上述评判指标与目标事件的可信度 w_g 相乘，即为系统的综合风险评估值：2.643 8，所以根据该值可判断该系统综合风险等级为“较低”，结果和实际安全状况相符。同理，由各个风险因素事件的可信度以及评价指标可以求出相应的风险评估值和风险等级。最后得出结论：该校园网面临的综合风险影响不大，其中，数据和设备资产相对严重，应该加强安全防御；风险程度可以接受，暂时不需要准备下次评估。

4.3　结果分析与比较

以上述评估结果为例，将本文提出的评估方法与传统的综合评估方法进行比较和分析。传统的基于层次分析法的综合评估方法[9,10]是将各个评估指标的评估结果进行综合，得到最终评估结果，但评估结果往往不够准确，这是由于其仅考虑了评估指标本身，而忽略了评估指标所对应因素事件发生的可信度。本文提出的方法综合考虑了各种因素，通过推理可得目标事件的可信度和相应的评价指标，而二者之积为系统的风险评估值，从而在一定程度上避免了主观性问题，使评估结果更加科学和准确。

5　结束语

本文主要讨论了模糊 Petri 网模型及其推理算法在网络安全风险评价中的应用。首先将影响网络安全的各因素转化为 FPN 的库所，通过专家知识库以及层次分析法得到模型需要的相关参数，之后利用给出的模糊推理算法对某校园网的安全性进行分析。该方法不仅能够判断系统综合的风险等级，而且还能判断各个因素事件以及中间事件的风险等级，具有简单和有效的特点。实验结果表明，FPN 评估模型及推理算法是有效可行的。

参考文献：

[1] 冯登国，张阳，张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7):10-18.
FENG D G, ZHANG Y, ZHANG Y Q. Survey of information security risk assessment[J]. Journal on Communications, 2004, 25(7):10-18.

[2] 吴迪, 连一峰, 陈恺等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报，2012, 35(9):1938-1950.
WU D, LIAN Y F, CHEN K, *et al*. A security threats identification and analysis method based on attack graph[J]. Chinese Journal of Computers, 2012, 35(9):1938-1950.

[3] LIANG X N, XIAO Y. Game theory for network security[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1):472-486.

[4] MOORE A, ELLISON R, LINGER R. Attack Modeling for Information Security and Survivability[D]. Pittsburgh: Carnegie Mellon University, 2001.

[5] 陈锋, 刘德辉, 张怡等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展, 2011, 48(6):945-954.
CHEN F, LIU D H, ZHANG Y, *et al*. A hierarchical evaluation approach for network security based on threat spread model[J]. Journal

of Computer Research and Development, 2011, 48(6):945-954.

[6] VALETTE R, CARDOSO J, DUBOIS D. Monitoring manufacturing systems by means of Petri nets with imprecise markings[A]. IEEE International Symposium on Intelligent Control[C]. 1989. 233-238.

[7] QIN L. AHP-Based Teaching Evaluation Index System of Weighs[M]. Informatics and Management Science VI, 2013. 449-457.

[8] 付钰, 吴晓平, 叶清等. 基于模糊集与熵权理论的信息系统安全风险评估研究[J]. 电子学报, 2010, 38(7):1489-1494.
FU Y, WU X P, YE Q, *et al*. An approach for information systems security risk assessment on fuzzy set and entropy-weight[J]. Acta Electronica Sinica, 2010, 38(7):1489-1494.

[9] ZHANG Y J, DENG X Y, WEI D J, *et al*. Assessment of e-commerce security using AHP and evidential reasoning[J]. Expert Systems with Applications, 2012, 39(3):3611-3623.

[10] 赵冬梅, 马建峰, 王跃生. 信息系统的模糊风险评估模型[J]. 通信学报, 2007, 28(4):51-56.
ZHAO D M, MA J F, WANG Y S. Model of fuzzy risk assessment of the information system[J]. Journal on Communications, 2007, 28(4): 51-56.

作者简介：

高翔（1984-），男，辽宁大连人，信息工程大学博士生，主要研究方向为形式化建模与验证、网络与信息安全。

祝跃飞（1962-），男，浙江杭州人，信息工程大学教授、博士生导师，主要研究方向为应用数学。

刘胜利（1973-），男，河南周口人，博士，信息工程大学副教授、硕士生导师，主要研究方向为网络信息安全。

费金龙（1979-），男，河南郑州人，信息工程大学讲师，主要研究方向为网络信息安全。

刘龙（1983-），男，河南郑州人，硕士，信息工程大学助教，主要研究方向为网络与信息安全。