文章编号:1007-5321(2021)04-0041-08　　**DOI**:10.13190/j.jbupt.2021-019

一种基于风险传播的信息系统风险评估方法

杨宏宇[1,2]，张　乐[2]，张　良[3]
(1. 中国民航大学 安全科学与工程学院，天津 300300；2. 中国民航大学 计算机科学与技术学院，天津 300300；
3. 亚利桑那大学 信息学院，图森 AZ 85721)

摘要：传统信息系统的风险评估方法未考虑节点的状态变化和风险的传播方向，且评估结果的准确性受专家主观性的影响，对此，提出了一种基于风险传播的信息系统风险评估方法. 首先，确定节点的初始状态转移概率矩阵，并根据攻击属性对矩阵进行修正，得到节点状态转移概率；其次，基于系统风险传播网络拓扑图和节点属性值计算节点在各方向的传播概率；然后，利用三参数区间数方法获取节点威胁事件的量化值；最后，根据风险评估方法计算各节点的风险值. 实验结果表明，基于风险传播方法的评估流程更客观、合理，可提高信息系统风险评估的整体性和准确性.

关　键　词：风险评估；风险传播；状态转移概率；传播概率；三参数区间数
中图分类号：TP309　　**文献标志码**：A

An Information System Risk Assessment Method Based on Risk Propagation

YANG Hong-yu[1,2]，ZHANG Le[2]，ZHANG Liang[3]
(1. College of Safety Science and Engineering，Civil Aviation University of China，Tianjin 300300，China；
2. College of Computer Science and Technology，Civil Aviation University of China，Tianjin 300300，China；
3. College of Information，University of Arizona，Tucson AZ 85721，USA)

Abstract：Traditional information system risk assessment methods do not consider the state change of nodes and the direction of risk propagation，and the accuracy of the evaluation results is affected by the subjectivity of experts. To solve these problems，an information system risk assessment method based on risk propagation is proposed. First，the initial state transition probability matrix of the node is determined，and the node state transition probability is obtained by modifying the matrix according to the attack attributes. Then，the propagation probability of nodes in all directions is calculated based on the topology network and node attribute value. Next，the three-parameter interval number method is used to obtain the quantitative value of node threat events. Finally，the risk value of each node is calculated according to the risk assessment method. Experimental results show that the proposed methodis more objective and reasonable，and it improves the integrity and accuracy of the risk assessment of information systems.
Key words：risk assessment；risk propagation；state transition probability；propagation probability；three-parameter interval number

随着信息系统种类的增多，信息系统暴露的安全　　问题也日益增加，所采取防护措施的方案具有一定的

收稿日期：2021-02-02
基金项目：国家自然科学基金民航联合研究基金项目(U1833107)
作者简介：杨宏宇(1969—)，男，教授，E-mail:yhyxlx@hotmail.com.

盲目性和被动性,因此,为解决传统方案存在的被动性问题,信息系统安全风险评估技术成为研究热点.

许硕等[1]提出一种基于D数层次分析法与灰色理论的信息安全风险评估方法,引入D数理论改进模糊偏好关系,降低了评估信息的不确定性,但不一致度系数的取值由评估专家决定,增加了专家主观性对评估结果的影响. 赵刚等[2]提出一种基于灰色网络威胁分析(G-ANP, gray analytic network process)的信息系统安全风险评估方法,能够利用已知的少量信息,更客观地反映风险要素互相依赖、互相影响的关系,但要求评估信息必须完整. Antonio等[3]提出用模糊层次分析法对信息系统进行风险评估,降低了评估信息的模糊性且提高了系统风险评估的准确性,但该方法在建立专家矩阵时未考虑专家权重的差异性对系统风险评估结果的影响. Hong等[4]提出基于动态风险传播的信息安全风险评估方法(ISRADRP, information security risk algorithm based on dynamic risk propagation),将风险传播因素引入信息系统风险评估,使得系统风险评估包括外部风险,但未考虑被传播节点的状态变化和传播方向对评估结果的影响. Feng等[5]提出一种分析风险因素因果关系和脆弱性传播的方法,根据贝叶斯网络建立风险要素之间的因果关系,计算最大的系统风险估计值,但未考虑专家经验的差异性对评估结果的影响.

综上所述,现有信息系统风险评估方法受专家主观性影响较大,量化结果很难反映系统风险情况;同时,仅针对单一系统,未考虑各系统之间的关联性、节点状态变化和风险传播方向对评估结果的影响. 为此,提出了一种基于风险传播的信息系统风险评估方法.

1 信息系统风险评估方法

所提出的风险评估方法流程如图1所示,处理过程如下.

1) 网络拓扑构建. 以子系统中的组件为节点,以组件数据交互关系为边,构建网络拓扑.

2) 节点状态转移概率计算与属性值计算. 首先,基于三参数区间数计算威胁事件量化值;然后,根据系统中节点的状态集合,计算各状态间的转移概率,确定初始状态转移概率矩阵,并根据攻击属性值对矩阵修正得到节点各状态修正后的转移概率;最后,根据节点的保密性、完整性和可利用性计算节点资产值,分析节点存在的漏洞,根据通用漏洞评分系统(CVSS, common vulnerability scoring system)确定节点漏洞的脆弱性值.

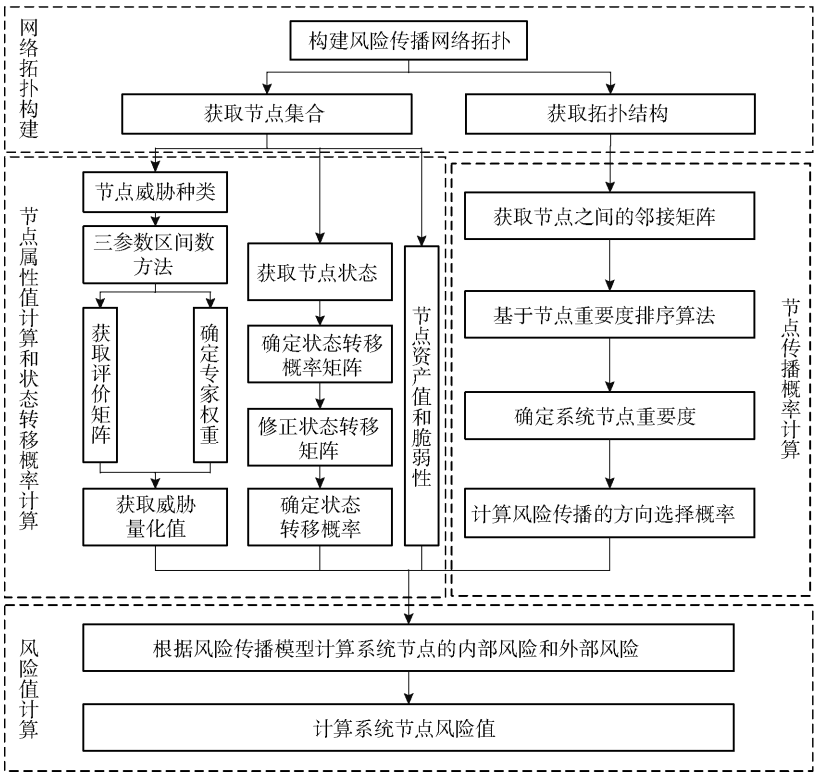

图1 系统风险评估方法流程

3）节点传播概率计算. 首先,根据系统的拓扑结构图确定节点间的邻接矩阵;其次,基于PageRank算法[6]计算节点的 PageRank 值;然后,根据节点的PageRank 值、资产值和出入度值计算节点的重要度;最后,根据节点的重要度计算节点在各方向的传播方向选择概率.

4）风险值计算. 首先,根据各子系统内部节点之间的交互关系和各节点的属性值,计算各节点因自身脆弱性受到外部威胁所导致的直接风险和间接风险,并对各节点的风险累加求和,得到各子系统的内部风险;然后,根据各子系统间节点之间的交互关系,计算节点因相邻系统中节点的间接影响所导致的外部风险,并对各节点的外部风险累加求和,可得各子系统的外部风险;最后,对各子系统的内外部风险累加求和,得到系统的总风险.

2　节点状态转移概率与节点属性值

2.1　状态转移概率

1）确定状态转移概率矩阵

根据文献[7]中网络安全状态的分析过程,当系统中的节点受到威胁事件的影响,节点状态会发生改变,为此,将节点状态划分为安全状态(G)、入侵状态(B)和攻破状态(Y). 将系统的威胁事件划分为漏洞类事件(E_{v})、入侵事件(E_{b})、获取权限事件(E_{c})和无安全事件(φ)四类威胁事件(E),定义 $E\in\{\varphi, E_{\mathrm{v}}, E_{\mathrm{b}}, E_{\mathrm{c}}\}$. 此外,将节点防护措施($D$)划分为节点中不存在对威胁的任何防护措施($\phi$)、节点中存在对威胁事件提前检测的措施($D_{\mathrm{s}}$)、节点中存在阻止威胁事件发生的措施($D_{\mathrm{f}}$)和存在对威胁发生后及时修复节点的措施($D_{\mathrm{r}}$),定义 $D\in\{\phi, D_{\mathrm{s}}, D_{\mathrm{f}}, D_{\mathrm{r}}\}$. 威胁事件和防护措施会影响节点的状态,若 t 时刻节点处于状态 s_i,在此状态下,发现节点中存在安全事件 E_j,或执行了针对该安全事件的防护措施 D_j,则导致节点在$t+1$ 时刻转变为状态 s_j,该节点的状态转移过程可表示为

$$s_i \xrightarrow{E_j\cup D_j} s_j, s_i, s_j\in\{G,B,Y\}$$

则基于威胁事件和防护措施的博弈,可得节点某状态转移矩阵为

$$\boldsymbol{M}=\begin{bmatrix} S_{E_1,D_1} & S_{E_1,D_2} & S_{E_1,D_3} & S_{E_1,D_4}\\ S_{E_2,D_1} & S_{E_2,D_2} & S_{E_2,D_3} & S_{E_2,D_4}\\ S_{E_3,D_1} & S_{E_3,D_2} & S_{E_3,D_3} & S_{E_3,D_4}\\ S_{E_4,D_1} & S_{E_4,D_2} & S_{E_4,D_3} & S_{E_4,D_4}\end{bmatrix}$$

根据矩阵 $\boldsymbol{M}$ 可得状态 s_i转移到状态 s_j的节点状态转移概率为

$$p_{i,j}=\frac{N_{i,j}}{16} \tag{1}$$

其中:$N_{i,j}$为节点从状态 s_i转移为状态 s_j在矩阵 $\boldsymbol{M}$ 中的数量,即 S_{E_i,D_j}等于状态 s_j的数量,从状态 s_i转移为其他状态的数目之和为 16. 根据各状态的概率分布,可得初始状态转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & p_{12} & p_{13}\\ p_{21} & p_{22} & p_{23}\\ p_{31} & p_{32} & p_{33}\end{bmatrix}$$

2）修正状态转移概率矩阵

根据攻击者属性建立修正函数,修正初始状态转移概率,修正函数为

$$H=\sum_{i,j\in S} A_{\mathrm{m}}(i)\frac{A_{\mathrm{c}}(i)}{10A_{\mathrm{r}}(j)} \tag{2}$$

其中:A_{m}为攻击者的类型,A_{c}为攻击者的能力,A_{r}为完成攻击所需要的资源. 根据文献[7],A_{m}分为专业人员、熟练攻击者和初始攻击者,$A_{\mathrm{m}}(i)\in\{1/25, 4/25, 4/5\}$. A_{c}为攻击者的能力,将其划分为高、中、低,$A_{\mathrm{c}}(i)\in\{100,10,1\}$. A_{r}为所需资源,将其划分为需要大量资源、需要部分资源和不需要资源,$A_{\mathrm{r}}(j)\in\{100,10,1\}$. 攻击所需资源相对攻击者的类型对节点状态转移概率影响较弱,因此采用系数 10 对函数进行调整.

根据节点转变前和转变后的状态,对 A_{m},A_{c}和 A_{r}的取值进行划分,各属性的划分是指节点的当前状态转移为另一种状态所必须的条件组合;然后根据各状态转移到另一种状态的属性值组合计算相应的修正函数值,利用 H 对从状态 $s_i\rightarrow s_j$的初始状态转移概率 $p_{i,j}$修正,可得修正后的状态转移概率为

$$p'_{i,j}=Hp_{i,j} \tag{3}$$

修正初始状态转移概率矩阵 $\boldsymbol{P}$ 中各状态间的转移概率,则可得修正函数对初始状态转移概率矩阵 $\boldsymbol{P}$ 修正后的状态转移概率矩阵为

$$\boldsymbol{P}'=\begin{bmatrix} p'_{11} & p'_{12} & p'_{13}\\ p'_{21} & p'_{22} & p'_{23}\\ p'_{31} & p'_{32} & p'_{33}\end{bmatrix}$$

2.2　节点属性值

1）节点资产值

根据系统资产的表现形式[8],确定各资产的种类,并分析各资产对节点的影响程度,分析节点资产

的价值和安全状况;然后对节点资产的保密性、完整性和可利用性进行量化,则节点 $S_{i,m}$ 的总资产值为

$$a_{s_{i,m}}=\frac{C+I+A}{3} \tag{4}$$

其中:C 为保密性赋值,I 为完整性赋值,A 为可利用性赋值. 根据 GB/T 20984—2007[9],分析资产对系统的影响程度,可将保密性、完整性和可利用性的赋值划分为很高、高、中等、低、很低 5 类,对应赋值为 5,4,3,2,1.

2) 节点威胁事件量化值计算

基于三参数区间数[10-11]提出了威胁事件的量化方法,降低了信息系统风险评估过程中专家主观性地给出评估结果带来的影响. 威胁事件量化值的计算包括 6 个步骤.

步骤 1 分析节点中存在的威胁事件,令节点的威胁事件数量为 n,请 m 位专家对选取的威胁事件进行评估,综合专家对威胁事件的评价结果,获取三参数区间的评价矩阵 $\boldsymbol{Z}$.

步骤 2 根据文献[11]确定威胁事件的类型,并获取规范化的三参数区间评价矩阵 $\boldsymbol{Z}'$.

步骤 3 根据熵值理论计算威胁事件的信息熵值和权重值,则威胁事件 k 的熵值为

$$H_k=\gamma\left(-\frac{1}{\ln m}\sum_{i=1}^{m}\frac{b_{i,k}}{\sum_{i=1}^{m}b_{i,k}}\ln\frac{b_{i,k}}{\sum_{i=1}^{m}b_{i,k}}\right)+(1-\gamma)\left(-\frac{1}{\ln m}\sum_{i=1}^{m}\frac{V_{i,k}}{\sum_{i=1}^{m}V_{i,k}}\ln\frac{V_{i,j}}{\sum_{i=1}^{m}V_{i,k}}\right) \tag{5}$$

其中:$b_{i,k}$ 为专家 i 评价事件 k 的三参数区间重心点,$k\in\{1,2,\cdots,n\}$;$V_{i,k}$ 为三参数区间数的方差;γ 为决策者的判断系数,$0\leqslant\gamma\leqslant1$,通常决策者的判断系数取值为 0.6. 根据上述熵值,威胁事件 k 的权重值为

$$W_k=\frac{1-H_k}{\sum_{i=1}^{n}(1-H_i)} \tag{6}$$

步骤 4 计算步骤 2 中规范化评价矩阵 $\boldsymbol{Z}'$ 的正、负理想解分别为

$$\overline{\boldsymbol{Z}}=(r_1,r_2,\cdots,r_n),r_i=\max_{1\leqslant j\leqslant m}r_{i,j},1\leqslant i\leqslant n$$

$$\overline{\boldsymbol{X}}=(r_1,r_2,\cdots,r_n),r_i=\min_{1\leqslant j\leqslant m}r_{i,j},1\leqslant i\leqslant n$$

步骤 5 计算正、负理想解与评价向量间的综合距离及贴近度,有

$$\overline{d}_{\mathrm{p},i}=\sum_{k=1}^{n}w_{t_{h_k}}d(\boldsymbol{Z}_{i,k},\overline{\boldsymbol{Z}}) \tag{7}$$

$$\overline{d}_{\mathrm{m},i}=\sum_{k=1}^{n}w_{t_{h_k}}d(\boldsymbol{Z}_{i,k},\overline{\boldsymbol{X}}) \tag{8}$$

$$N_i=\frac{\overline{d}_{\mathrm{m},i}}{\overline{d}_{\mathrm{m},i}+\overline{d}_{\mathrm{p},i}} \tag{9}$$

其中:$d(Z_{i,k},\overline{\boldsymbol{Z}})$ 为各区间的三维欧氏距离;$\overline{d}_{\mathrm{p},i}$ 为专家 i 的正综合距离;$\overline{d}_{\mathrm{m},i}$ 为专家 i 的负综合距离;$Z_{i,k}$ 为专家 i 对威胁事件 k 规范化的三参数区间;N_i 为规范化的三参数区间与正负理想解的贴近度,$i\in\{1,2,\cdots,m\}$.

步骤 6 根据贴近度计算各专家权重和威胁事件的量化值,则专家 i 的相对权重为

$$w_i=\frac{N_i}{\sum_{j=1}^{m}N_j} \tag{10}$$

其中 $j\in\{1,2,\cdots,m\}$.

根据专家权重和威胁事件的初始重心点,得威胁事件 k 的量化值为

$$T_k=\sum_{i=1}^{m}w_ig_i \tag{11}$$

其中 g_i 为专家 i 对威胁事件 k 规范化前的三参数区间的重心点.

3) 威胁利用脆弱性的概率计算

脆弱性值越大,被威胁利用的概率就越大. 因此,威胁利用脆弱性的概率为

$$\rho(k,u)=\frac{v(u)}{\sum_{i=1}^{U}v(i)} \tag{12}$$

其中:$\rho(k,u)$ 为威胁事件 k 利用脆弱性 u 的概率,U 为节点中威胁事件 k 能够利用的脆弱性数量,$v(u)$ 为根据 CVSS 确定的脆弱性 u 的量化值.

3 节点传播概率

1) 节点重要度

根据系统风险传播网络拓扑图和 PageRank 算法,得节点的 PageRank 值为

$$\boldsymbol{\beta}'=h\boldsymbol{X}\boldsymbol{\beta}+(1-h)\boldsymbol{e} \tag{13}$$

其中:$\boldsymbol{X}$ 为节点间的邻接矩阵,$\boldsymbol{\beta}$ 为节点初始PageRank值向量,各节点初始 PageRank 值为 $1/n$,n 为节点的数量. 根据文献[6],阻尼系数 h 取值为 0.85,$\boldsymbol{e}$ 为向量,且各维度的值为 1. 用当前得到的 $\boldsymbol{\beta}'$ 替代 $\boldsymbol{\beta}$,直至 $\boldsymbol{\beta}'$ 达到收敛,则可得各节点的 PageRank 值;然后,结合节点的资产值和出入度,得节点 i 的重要度为

$$O_i = \frac{\left(\dfrac{L_i + d_i}{\sum_{j=1}^{n}(L_j + d_j)} + a_i\right)}{\sum_{k=1}^{n}\left(\dfrac{L_k + d_k}{\sum_{j=1}^{n}(L_j + d_j)} + a_k\right)} \tag{14}$$

其中：L 为节点的 PageRank 值，d 为节点的出入度和，a 为节点的资产值.

2）节点传播方向选择概率

根据重要度值计算节点在某方向的传播概率. 如果某节点的指向节点数量为 N，且每个被指向节点的重要度值为 O_k，则各方向的传播方向选择概率为

$$\mu(i,j) = \frac{O_j}{\sum_{k=1}^{N} O_k} \tag{15}$$

其中 $\mu(i, j)$ 为节点 i 向节点 j 传播的概率.

4　风险值

1）内部风险

在某子系统内部，子系统的风险主要由各节点的风险组成，则子系统内部风险为

$$R(S_i) = \sum_{m=1}^{F} R(S_{i,m}) + \sum_{m=1}^{F}\sum_{n=1}^{F} R(S_{i,m} \rightarrow S_{i,n}) \tag{16}$$

其中：F 为子系统 S_i 内部节点数量，$R(S_{i,m})$ 为节点自身风险值，$R(S_{i,m} \rightarrow S_{i,n})$ 为节点间的传播风险值. 节点自身的风险值为

$$R(S_{i,m}) = a_{S_{i,m}} \sum_{k=1}^{K} W_k T_k \left\{ \sum_{u=1}^{U} [v(u)\rho(k,u)\tau_m] \right\} \tag{17}$$

其中：K 为节点 $S_{i,m}$ 中威胁事件数量，W_k 为威胁事件 k 在系统中的相对权重，τ_m 为节点状态转变为不安全状态的概率. 根据 $\boldsymbol{P}'$ 可获得各状态转变为不安全状态的概率. 节点间的传播风险为

$$R(S_{i,m} \rightarrow S_{i,n}) = a_{S_{i,n}} \mu(S_{i,m}, S_{i,n}) \times \left\{ \sum_{k=1}^{K} W_k T_k \sum_{u=1}^{U} [v(u)\rho(k,u)\tau_n] \right\} \tag{18}$$

其中：$\mu(S_{i,m}, S_{i,n})$ 为节点间传播方向选择的概率，表示节点 $S_{i,m}$ 向节点 $S_{i,n}$ 传播的概率.

2）外部风险

子系统受到的外部风险指其他子系统中的节点与该子系统中的节点存在数据交互而导致的风险，则子系统的外部风险为

$$R(S_i \rightarrow S_j) = \mu(S_i, S_j) \sum_{m=1}^{G_i}\sum_{n=1}^{G_j} \left\{ a_{S_{j,n}} \mu(S_{i,m}, S_{j,n}) \times \left[\sum_{k=1}^{K} W_k T_k \sum_{u=1}^{U} (v(u)\rho(k,u)\tau_n) \right] \right\} \tag{19}$$

其中：G_j 为子系统 S_j 内部节点的数量，G_i 为子系统 S_i 内部节点的数量，$\mu(S_i, S_j)$ 为子系统 S_i 向 S_j 传播方向的选择概率. 子系统的重要度为节点重要度的累加和，通过式(15)可求得子系统间传播方向的选择概率.

3）总风险

$$Q = \sum_{i=1}^{J} R(S_i) + \sum_{j=1}^{J}\sum_{k=1}^{J} R(S_j \rightarrow S_k) \tag{20}$$

其中 J 为子系统的数量.

5　实验与结果

5.1　实验环境设置

为验证所提出的基于风险传播的信息系统风险评估方法的可行性，实验中采用一台 Dell Precision 7920 Tower 工作站，考虑了 3 种不同类型的虚拟机，在 VMware Workstation Pro 上创建各类虚拟机的数据应用存储系统如图 2 所示.

该系统由 3 部分组成，分别为备份部分(S_1)、存储部分(S_2)和应用部分(S_3)，根据子系统的数据传输规则，经处理得到的系统风险传播网络拓扑如图 3 所示.

5.2　节点属性值和状态转移概率

1）节点状态转移概率

根据 2.1 节分析各状态在威胁事件和防护措施博弈后的状态，建立各状态转移矩阵；再由式(1)计算各状态转移到其他状态的概率，可得初始状态转移概率矩阵 $\boldsymbol{P}$. 由式(2)和式(3)对 $\boldsymbol{P}$ 修正，可得修正后的状态转移概率矩阵 $\boldsymbol{P}'$.

$$\boldsymbol{P} = \begin{bmatrix} 0.718\,5 & 0.187\,50 & 0.093\,75 \\ 0.250\,0 & 0.562\,50 & 0.187\,50 \\ 0.250\,0 & 0.031\,25 & 0.718\,75 \end{bmatrix}$$

$$\boldsymbol{P}' = \begin{bmatrix} 0.719 & 0.131 & 0.064 \\ 0.002 & 0.396 & 0.116 \\ 0.067 & 0.008 & 0.316 \end{bmatrix}$$

2）节点资产值

根据节点的保密性、完整性和可利用性，运用式(4)计算各节点的资产值，结果如表 1 所示.

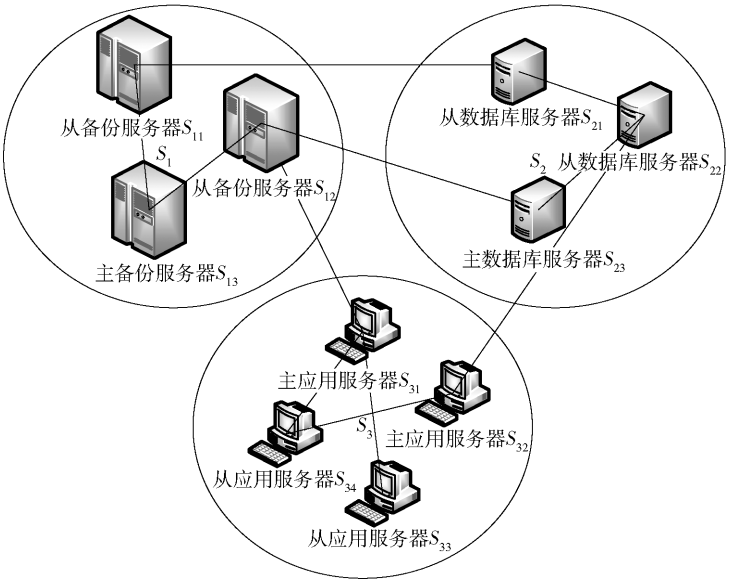

图2 数据应用存储系统网络拓扑结构

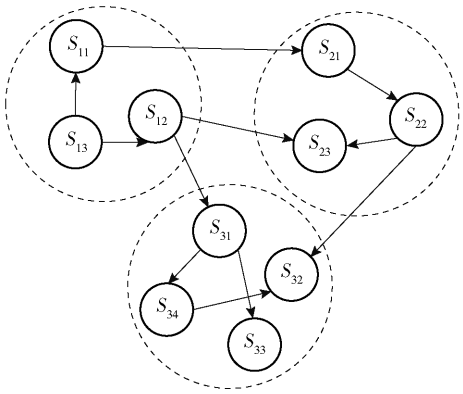

图3 系统风险传播网络拓扑图

3）威胁事件量化值

系统中存在6类威胁事件，分别为后门、恶意代码、访问控制、授权、违法入侵和恶意外部链接. 根据5位专家对威胁事件的评价结果，可得三参数评价矩阵. 将威胁事件划分为成本型事件和效益型事件，分别对各事件规范化处理，可得规范化评价矩阵 $\boldsymbol{Z}'$. 根据式(5)和式(6)计算威胁事件熵值和相对权重值，结果如表2所示.

表1 节点资产值

节点	保密性	完整性	可利用性	资产值
S_{11}	5	5	4	4.67
S_{12}	3	4	5	4.00
S_{13}	4	4	3	3.67
S_{21}	4	5	5	4.67
S_{22}	2	5	3	3.33
S_{23}	2	4	4	3.33
S_{31}	4	3	3	3.33
S_{32}	3	4	4	3.67
S_{33}	4	5	3	4.00
S_{34}	4	3	4	3.67

$$\boldsymbol{Z}'=\begin{bmatrix}
[0,0.33,0.66] & [0,0.33,0.66] & [0,0.25,0.25] & [0.25,0.25,0.50] & [0.25,0.50,0.75] & [0,0.50,1.00] \\
[0.33,0.33,0.66] & [0.33,0.66,0.66] & [0.25,0.25,0.50] & [0.25,0.50,0.75] & [0.75,0.75,1.00] & [0.25,0.50,0.75] \\
[0.33,0.66,1.00] & [0.33,0.33,0.66] & [0.25,0.50,0.75] & [0,0.25,0.25] & [0.50,0.75,0.75] & [0.50,0.50,1.00] \\
[0,0.33,0.33] & [0.66,0.66,1.00] & [0.25,0.50,1.00] & [0.25,0.75,1.00] & [0,0.25,0.50] & [0.50,0.75,1.00] \\
[0.33,0.66,0.66] & [0.33,0.66,1.00] & [0,0.25,0.50] & [0,0.25,0.25] & [0.25,0.75,0.75] & [0.75,0.75,1.00]
\end{bmatrix}$$

由式(7)～式(10)计算出5位专家的相对权重，分别为 $w_1=0.118$，$w_2=0.261$，$w_3=0.231$，$w_4=0.193$，$w_5=0.197$；再由式(11)计算出威胁事件的量化值，分别为 $T_1=2.027$，$T_2=2.212$，$T_3=2.7$，$T_4=2.735$，$T_5=3.175$，$T_6=4.471$.

5.3 节点传播概率与风险值

1）节点传播概率

由式(13)和式(14)计算出各节点的重要度，结果如表3所示. 根据式(15)计算节点在各方向传播概率，结果如表4所示.

表 2　威胁事件熵值及权重值

威胁事件	熵值	权重值
1	0.941	0.127
2	0.946	0.116
3	0.916	0.181
4	0.871	0.277
5	0.943	0.123
6	0.918	0.176

表 3　节点属性值

节点	脆弱性	威胁	$v(i)$	传播节点	O_i
S_{11}	存在 SQL 注入漏洞	恶意代码	5	$\{S_{13}\}$	0.106 237
S_{12}	未使用锁定功能	违法入侵	3	$\{S_{13}\}$	0.119 653
S_{13}	打开了不必要的端口	违法入侵	3	Φ	0.093 065
S_{21}	未使用日志记录功能	不合法链接	3	$\{S_{11}\}$	0.106 559
S_{22}	禁用安全审核功能	违法入侵	3	$\{S_{21}\}$	0.111 646
S_{23}	允许远程登陆	访问控制	3	$\{S_{12},S_{22}\}$	0.089 299
S_{31}	存在 XSS 漏洞	后门	5	$\{S_{12}\}$	0.111 139
S_{32}	打开了不必要的端口	违法入侵	3	$\{S_{22},S_{34}\}$	0.094 126
S_{33}	未使用日志记录功能	不合法链接	3	$\{S_{31}\}$	0.075 020
S_{34}	未使用锁定功能	违法入侵	3	$\{S_{31}\}$	0.093 343

表 4　节点风险传播方向选择概率

被传播节点	脆弱性	传播节点	传播概率
S_{11}	存在 SQL 注入漏洞	S_{13}	0.470 304
S_{12}	登陆失败时没有使用锁定功能	S_{13}	0.529 696
S_{21}	没有使用日志记录功能	S_{11}	1.000 000
S_{22}	禁用安全审核功能	S_{21}	1.000 000
S_{23}	允许数据库管理员远程登陆	S_{12}	0.445 519
S_{23}	允许数据库管理员远程登陆	S_{22}	0.486 842
S_{31}	存在 XSS 漏洞	S_{12}	0.554 481
S_{32}	打开了不必要的端口	S_{22}	0.513 158
S_{32}	打开了不必要的端口	S_{34}	1.000 000
S_{33}	没有使用日志记录功能	S_{31}	0.445 585
S_{34}	登陆失败时没有使用锁定功能	S_{31}	0.554 415

2）节点风险值

由节点相关属性值和式(16)～式(20)计算出各节点的风险值,结果如表 5 所示. 通过实验验证了所提方法对信息系统进行风险评估的有效性. 分析可知,相对其他节点,节点 S_{21} 的风险值相对较高,节点 S_{13} 的风险值在系统中最低. 因此,应该及时地对节点 S_{21} 进行防御保护,防止发生系统安全事件.

表 5　节点总风险值

节点	风险值	节点	风险值
S_{11}	2.257	S_{23}	1.012
S_{12}	1.671	S_{31}	1.792
S_{13}	0.838	S_{32}	2.012
S_{21}	2.851	S_{33}	2.142
S_{22}	1.385	S_{34}	0.975

5.4　节点风险评估对比实验

为验证计算节点风险值的准确性,在与 5.1 节相同的实验环境下,分别用文献[2]中的 G-ANP 方法、文献[4]的 ISRADRP 算法和所提方法进行节点风险评估对比实验,结果如图 4 所示.

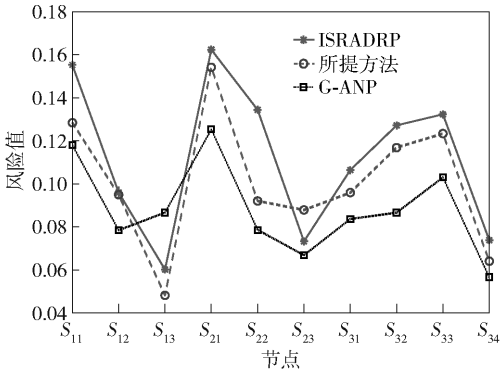

图 4　节点风险值对比图

由对比结果可知,所提风险评估方法比其他方法的风险评估结果更准确,原因如下.

1）所提方法得到的节点风险值大于 G-ANP 方法. 当使用 G-ANP 方法进行信息系统风险评估时,未考虑威胁传播性,如果有多个节点发生威胁作用时,G-ANP 方法仅简单地进行风险损失的累加求和,并不能基于威胁传播系统地进行风险评估,得到的节点风险值相对较小.

2）所提方法得到的节点风险值小于 ISRADRP 方法. 当使用 ISRADRP 方法进行信息系统风险评估时,未考虑被传播节点的防御措施,一旦某个节点被威胁影响,节点的状态会立刻转变为不安全状态,且 ISRADRP 方法在各方向的传播概率相等,故 ISRADRP 方法所得的风险值大于所提方法得到的评估结果.

3）所提方法引入状态转移概率,当节点被威胁影响时,节点状态会由于威胁事件和防御措施的博弈而发生改变,更符合节点状态转移的实际情况. 所提方法引入节点传播方向选择概率,通过计算节

点的重要度确定传播节点在各方向的风险传播概率,使得各方向风险传播概率存在差异性. 通过计算节点的内部风险和外部风险使得评估结果更加科学、准确.

6 结束语

针对传统信息系统风险评估方法准确性低,且评估结果受专家主观性影响等问题,提出一种基于风险传播的信息系统风险评估方法,该方法不仅考虑节点内部风险,也考虑节点外部风险,使评估风险值更加合理准确. 此外,风险传播路径也会影响最终的评估结果,因此,未来重点将分析传播路径对最终评估结果造成的影响.

参考文献:

[1] 许硕, 唐作其, 王鑫. 基于D-AHP与灰色理论的信息安全风险评估[J]. 计算机工程, 2019, 45(7): 194-202.
Xu Shuo, Tang Zuoqi, Wang Xin. Information security risk assessment based on D-AHP and grey theory[J]. Computer Engineering, 2019, 45(7): 194-202.

[2] 赵刚, 吴天水. 结合灰色网络威胁分析的信息安全风险评估[J]. 清华大学学报(自然科学版), 2013, 53(2): 1761-1767.
Zhao Gang, Wu Tianshui. Information security risk assessment based on G-ANP[J]. Journal of Tsinghua University (Science and Technology), 2013, 53(2): 1761-1767.

[3] Antonio R, Ortega F, Ramrio C. A method for the evaluation of risk in IT projects[J]. Expert Systems with Applications, 2016, 45(C): 273-285.

[4] Hong Q, Jian W T, Zheng T, et al. An information security risk assessment algorithm based on risk propagation in energy Internet[C]//2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). Beijing: IEEE, 2017: 1-6.

[5] Feng N, Wang H J, Li M Q. A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis[J]. Information Sciences, 2014, 6: 57-73.

[6] Brin S, Page L. The anatomy of a large-scale hyper textual web search engine[J]. Computer Networks and ISDN Systems, 1998, 30(1): 107-117.

[7] 席荣荣, 云晓春, 张永铮, 等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报, 2015, 38(4): 749-758.
Xi Rongrong, Yun Xiaochun, Zhang Yongzheng, et al. An improved quantitative evaluation method for network security[J]. Chinese Journal of Computers, 2015, 38(4): 749-758.

[8] Whitman M, Mattord H, Whitman, et al. Principles of information security[M]. Beijing: Tsinghua University Press, 2003: 60-64.

[9] 中国国家标准化管理委员会. 信息安全风险评估规范: GB/T 20984—2007[S]. 北京: 中国标准出版社, 2007: 6-8.
The standardization administration of China. Information security risk assessment specification: GB/T 20984—2007[S]. Beijing: Standards Press of China, 2007: 6-8.

[10] 黄玉洁, 唐作其, 梁静. 基于信息熵与三参数区间的信息安全风险评估[J]. 计算机工程, 2018, 44(12): 178-183.
Huang Yujie, Tang Zuoqi, Liang Jing. Information security risk assessment based on information entropy and three-parameter interval[J]. Computer Engineering, 2018, 44(12): 65-69.

[11] 林健, 姜永. 基于三参数区间数型偏好序的群决策方法[J]. 山东大学学报(理学版), 2011, 46(7): 65-69.
Lin Jian, Jiang Yong. Information security risk assessment based on information entropy and three-parameter interval[J]. Journal of Shandong University (Natural Science), 2011, 46(7): 65-69.