文章编号:1671 - 6833(2008)01 - 0035 - 04

基于模糊影响图理论的信息安全风险评估

张 锟,葛 磊,王春新,戴 锋

(解放军信息工程大学 信息工程学院,河南 郑州 450002)

摘 要:在系统分析信息安全风险要素的基础上,针对评估过程中威胁发生的可能性及信息资产的价值难以量化处理的问题,引入了模糊影响图算法.根据定性分析绘制了信息安全风险影响图,应用模糊影响图评价算法计算出信息安全风险发生的概率,得出了信息安全风险评估结论.结论表明,应用模糊影响图评价信息安全风险关键在于确定结点状态与频率之间以及结点之间的模糊关系,该方法是一种定性与定量结合,既简便又实用的评估算法,为信息安全风险评估提供了一种新思路.

关键词:模糊影响图;信息安全;风险评估

中图分类号:TP 309 **文献标识码**:A

0 引言

信息安全风险评估是对信息在产生、存储、处理、传输等过程中的保密性、完整性、可用性、可控性、不可否认性等信息安全属性遭到破坏的可能性及由此产生的后果所作的评价或估计.经过多年的研究探索和应用实践,有很多风险评估的理论与方法已经应用到信息安全风险评估领域,如BP 神经网络方法[1]、贝叶斯网络方法[2]、概率影响图方法[3]等等.但在信息安全风险评估过程中,由于安全事件发生的可能性很难通过统计数据得到准确的先验概率以及信息资产尤其是无形资产的价值难以准确估计,因此,笔者将模糊影响图方法引入信息安全风险评估过程,将难以量化的风险因素运用模糊理论进行描述,并应用文献[4 - 5]提出的模糊影响图算法对信息安全风险进行评估.评估结果表明:该方法不但可以减少获取大量统计数据的困难,而且还可以用模糊关系矩阵有效表述结果之间的相互影响.

1 模糊影响图及其评价算法

影响图是由结点集合和有向弧集合构成的无环有向图[6-9],根据其性质不同可以分为概率影响图和决策影响图等等.而模糊影响图则采用模糊理论描述结点的状态、频率之间及结点之间的模糊关系.模糊影响图中有 3 种类型的模糊集:状态模糊集、频率模糊集、模糊关系(一种特殊形式的模糊集,表现为模糊矩阵).当关系层确定后,模糊影响图在数值层上采用状态模糊集和频率模糊集描述结点的数据结构,在函数层上采用模糊关系描述变量间的关系[4-5].

在模糊影响图中,令结点 Y 表示无直接前序结点,如图 1 所示.

定义概率论域 $U = \{u_1, u_2, \cdots, u_m\}$,其中 $u_i \in [0,1] (i = 0,1,\cdots,m)$.在实际中概率论域是连续的,我们假设概率是离散的且论域 U 是有限集.

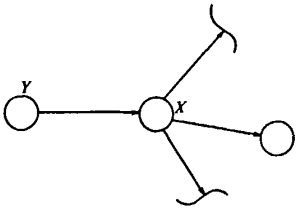

图 1 影响图示意图 1

Fig. 1 Influence diagram 1

定义 $\tilde{f}_j^Y (j = 1,2,\cdots,n)$ 是论域 U 上的频率模糊集,则结点 Y 的频率模糊向量为

$$\tilde{\boldsymbol{f}}^Y = \{\tilde{f}_1^Y, \tilde{f}_2^Y, \cdots, \tilde{f}_n^Y\}^T$$

由 U 与 $\tilde{\boldsymbol{f}}^Y$ 确定了一个频率模糊矩阵 $\boldsymbol{R}_Y^F$,该模糊矩阵的元素 $\mu_{\tilde{f}_j^Y}(u_i)$ 表示结点 Y 某种状态发生的频率 $\tilde{f}_j^Y$ 与概率 u_i 之间的模糊关系.

收稿日期:2007 - 11 - 10;修订日期:2007 - 12 - 22

基金项目:军事科研"十五"计划课题(05QJ109 - 010)

作者简介:张 锟(1980 -),女,河南郑州人,解放军信息工程大学硕士研究生,主要从事信息管理理论的研究,E-mail:happygegewu@126.com.

定义 $\tilde{S}_k^Y(k=1,2,\cdots,p)$ 表示结点 Y 的某种模糊状态,则结点 Y 的模糊状态向量为

$$\tilde{S}^Y = \{\tilde{S}_1^Y,\tilde{S}_2^Y,\cdots,\tilde{S}_p^Y\}^T.$$

由 $\tilde{f}^Y$ 与 $\tilde{S}^Y$ 确定了结点某种可能发生的状态与频率之间的模糊关系 $\tilde{R}_Y^{F-S}$,该模糊矩阵的元素 $\mu_{\tilde{S}\tilde{f}}(\tilde{f}_j^Y)$ 表示结点 Y 的模糊频率 $\tilde{f}_j^Y$ 与模糊状态 $\tilde{S}_k^Y$ 之间的相关性.

若独立结点 Y 的某种模糊状态 $\tilde{S}_k^Y$ 与发生的概率 u_i 之间的模糊矩阵用 $\tilde{R}_Y^S$ 表示,则

$$\tilde{R}_Y^S = \tilde{R}_Y^F \circ \tilde{R}_Y^{F-S} \tag{1}$$

该矩阵的元素为

$$\mu_{\tilde{S}\tilde{f}}(u_i) = \max_{j=1}^{n}\{\min[\mu_{\tilde{f}\tilde{f}}(u_i),\mu_{\tilde{S}\tilde{f}}(\tilde{f}_j^Y)]\}$$

定义结点 X 的模糊状态 $\tilde{S}_l^X(l=1,2,\cdots,q)$ 是有限论域 $V=\{v_1,v_2,\cdots v_w,\}$(其中 $v_h\in[0,1];h=0,1,\cdots,w$) 上的模糊集. 则由 V 与 $\tilde{S}_l^X$ 确定了一个模糊矩阵 $\tilde{R}_X^{S-V}$.

若结点 Y 是结点 X 唯一的前序结点,定义 $\tilde{R}_{YX}$ 表示由结点 Y 到结点 X 的状态模糊关系,该模糊矩阵的元素表示结点 Y 的模糊状态 $\tilde{S}_k^Y$ 与结点 X 的模糊状态 $\tilde{S}_l^X$ 之间的相关性,该相关性我们可以根据问题的性质通过定性分析来获得. 则矩阵

$$\tilde{R}_X = \tilde{R}_Y^S \circ \tilde{R}_{YX} \circ \tilde{R}_X^{S-V} \tag{2}$$

表示论域 U 与 V 之间的模糊相关性.

下面我们再来考虑多个紧前结点的情形,若 X 是由 m 个随机结点 $Y_1,Y_2,\cdots,Y_m$ 为其紧前结点的结点,如图2所示.

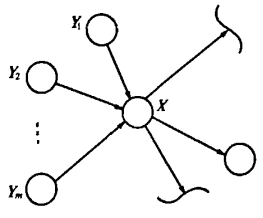

图2 影响图示意图2

Fig.2 Influence diagram 2

定义 $\tilde{R}_{Yi}^S$ 表示结点 Y_i 所确定的模糊状态矩阵,$\tilde{R}_{YiX}^S$ 表示从结点 Y_i 到结点 X 的状态模糊关系,根据式(2),则由结点 Y_i 与结点 X 所确定的论域 U 与 V 之间的模糊相关性

$$\tilde{R}_{Yi,X} = \tilde{R}_{Yi}^S \circ \tilde{R}_{YiX} \circ \tilde{R}_X^{S-V} \tag{3}$$

则由结点 X 与其所有紧前结点 $Y_1,Y_2,\cdots,Y_m$ 所确定的论域 U 与 V 之间的联合相关性

$$\tilde{R}_X = \tilde{R}_{(Y1,X)} \cup \tilde{R}_{(Y2,X)} \cup \cdots \cup \tilde{R}_{(Ym,X)} \tag{4}$$

最后从模糊矩阵 $\tilde{R}_X$ 中选取使本行的和与其所对应概率的乘积在所有行中最大的一行作为随机结果的隶属度. 假设第 k 行对应的和与本行概率乘积为最大值,则每一随机结果的概率函数为

$$P(u_i) = \mu_{ki}/\sum_i \mu_{ki} \tag{5}$$

2 基于模糊影响图的信息安全风险评估

信息安全风险的产生主要源于以下因素:信息系统的脆弱性、网络攻击的技术水平、安防措施的严密程度、信息资产的价值等等. 笔者根据信息安全风险产生的内在联系绘制了信息安全风险模糊影响图,如图3所示. 其中,结点1表示网络攻击的技术水平,结点2表示安防措施的严密程度,结点3表示信息系统的脆弱性,结点4表示信息资产的价值,结点5表示威胁发生的可能性,结点6表示信息安全风险.

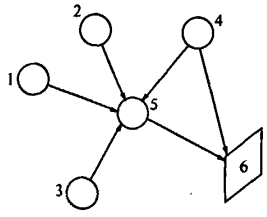

图3 信息安全风险模糊影响图

Fig.3 Influence diagram of information security risk

定义概率论域 $U=\{0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0\}$. 在此论域上,我们定义五个频率模糊集:高($H$)、中($M$)、低($L$)、非常高($VH$)、非常低($VL$).

$$H = \{\frac{0.7}{0.5},\frac{0.8}{0.7},\frac{0.9}{0.9},\frac{1.0}{1.0}\},$$

$$M = \{\frac{0.3}{0.2},\frac{0.4}{0.7},\frac{0.5}{1.0},\frac{0.6}{0.7},\frac{0.7}{0.2}\},$$

$$L = \{\frac{0.1}{1.0},\frac{0.2}{0.7},\frac{0.3}{0.4},\frac{0.4}{0.2}\},$$

$$VH = \{\frac{0.7}{0.2},\frac{0.8}{0.4},\frac{0.9}{0.8},\frac{1.0}{1.0}\},$$

$$VL = \{\frac{0.1}{1.0},\frac{0.2}{0.5},\frac{0.3}{0.2}\}.$$

定义结点1的模糊状态向量为 $\tilde{S}_1=\{TF,TS_E,TT\}^T$,其中 TF、TS_E、TT 分别代表攻击者技术水平为一级、二级、三级,其对应的频率模糊向量为 $\tilde{f}_1=\{L,M,H\}^T$,根据式(1)有:

$$\tilde{R}_1^S = \tilde{R}_1^F \circ \tilde{R}_1^{F-S} =$$

$$\begin{pmatrix} & H & M & L \\ 0.1 & 0 & 0 & 1.0 \\ 0.2 & 0 & 0 & 0.7 \\ 0.3 & 0 & 0.2 & 0.4 \\ 0.4 & 0 & 0.7 & 0.2 \\ 0.5 & 0 & 1.0 & 0 \\ 0.6 & 0 & 0.7 & 0 \\ 0.7 & 0.5 & 0.2 & 0 \\ 0.8 & 0.7 & 0 & 0 \\ 0.9 & 0.9 & 0 & 0 \\ 1.0 & 1.0 & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} & TF & TS_E & TT \\ H & 0 & 0 & 1 \\ M & 0 & 1 & 0 \\ L & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} & TF & TS_E & TT \\ 0.1 & 1.0 & 0 & 0 \\ 0.2 & 0.7 & 0 & 0 \\ 0.3 & 0.4 & 0.2 & 0 \\ 0.4 & 0.2 & 0.7 & 0 \\ 0.5 & 0 & 1.0 & 0 \\ 0.6 & 0 & 0.7 & 0 \\ 0.7 & 0 & 0.2 & 0.5 \\ 0.8 & 0 & 0 & 0.7 \\ 0.9 & 0 & 0 & 0.9 \\ 1.0 & 0 & 0 & 1.0 \end{pmatrix}.$$

如1攻击者技术水平为一级,则5威胁发生的可能性非常高(VH);如 1 攻击者技术水平为二级,则 5 威胁发生的可能性为中(M);如攻击者技术水平 1 为三级,则 5 威胁发生的可能性为低(L). 根据(3) 式有

$$\tilde{R}_{(1,5)} = \tilde{R}_1^S \circ \tilde{R}_{(1,5)} \circ \tilde{R}_5^{S-V}$$

$$= \begin{pmatrix} & TF & TS_E & TT \\ 0.1 & 1.0 & 0 & 0 \\ 0.2 & 0.7 & 0 & 0 \\ 0.3 & 0.4 & 0.2 & 0 \\ 0.4 & 0.2 & 0.7 & 0 \\ 0.5 & 0 & 1.0 & 0 \\ 0.6 & 0 & 0.7 & 0 \\ 0.7 & 0 & 0.2 & 0.5 \\ 0.8 & 0 & 0 & 0.7 \\ 0.9 & 0 & 0 & 0.9 \\ 1.0 & 0 & 0 & 1.0 \end{pmatrix} \circ \begin{pmatrix} & VH & M & L \\ TF & 1 & 0 & 0 \\ TS_E & 0 & 1 & 0 \\ TT & 0 & 0 & 1 \end{pmatrix} \circ \begin{pmatrix} & VH & M & L \\ 0.1 & 0 & 0 & 1.0 \\ 0.2 & 0 & 0 & 0.7 \\ 0.3 & 0 & 0.2 & 0.4 \\ 0.4 & 0 & 0.7 & 0.2 \\ 0.5 & 0 & 1.0 & 0 \\ 0.6 & 0 & 0.7 & 0 \\ 0.7 & 0.2 & 0.2 & 0 \\ 0.8 & 0.4 & 0 & 0 \\ 0.9 & 0.8 & 0 & 0 \\ 1.0 & 1.0 & 0 & 0 \end{pmatrix}^T =$$

$$\begin{pmatrix} & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 1.0 \\ 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 1.0 \\ 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.7 \\ 0.3 & 0 & 0 & 0.2 & 0.2 & 0.2 & 0.2 & 0.2 & 0.4 & 0.4 & 0.4 \\ 0.4 & 0 & 0 & 0.2 & 0.7 & 0.7 & 0.7 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.5 & 0 & 0.2 & 0.2 & 0.7 & 1.0 & 0.7 & 0.2 & 0 & 0 & 0 \\ 0.6 & 0 & 0.2 & 0.2 & 0.7 & 0.7 & 0.7 & 0.2 & 0 & 0 & 0 \\ 0.7 & 0.5 & 0.5 & 0.4 & 0.2 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 \\ 0.8 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0.9 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.0 & 1.0 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

定义结点 2 的模糊状态向量为 $\tilde{S}_2 = \{SF, SS_E, ST\}^T$,其中 SF, SS_E, ST 分别代表一级、二级三级安防措施,其对应的频率模糊向量为 $\tilde{f}_2 = \{VL, L, M\}^T$,其对结点 5 威胁发生可能性的影响分别为:非常低(VL)、低(L)、高(H). 定义结点 3 的模糊状态向量为 $\tilde{S}_3 = \{OF, OS_E, OT\}^T$,其中 OF、OS_E、OT 分别代表一级、二级、三级系统安全漏洞,其对应的频率模糊向量为 $\tilde{f}_3 = \{M, H, VH\}^T$,其对结点5威胁发生可能性的影响分别为:低($L$)、中($M$)、高($H$). 定义结点 4 的模糊状态向量为 $\tilde{S}_4 = \{AF, AS_E, AT\}^T$,其中,$AF$、$AS_E$、$AT$ 分别代表一级、二级、三级信息资产,其对应的频率向量为 $\tilde{f}_4 = \{L, M, H\}^T$,其对威胁发生可能性的影响分别为:非常高($VH$)、中($M$)、低($L$). 根据结点 1 的计算方法,同理可得

$$\tilde{R}_{(2,5)} =$$

$$\begin{pmatrix} & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 1.0 \\ 0.1 & 1.0 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.2 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.3 & 0.4 & 0.4 & 0.4 & 0.2 & 0 & 0 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.4 & 0.2 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0.5 & 0.7 & 0.7 & 0.7 \\ 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.7 & 0.9 & 1.0 \\ 0.6 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.7 & 0.7 & 0.7 \\ 0.7 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\tilde{R}_{(3,5)} =$$

$$\begin{pmatrix} & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 1.0 \\ 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.4 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 1.0 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.6 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.7 & 0.2 & 0.2 & 0.2 & 0.5 & 0.5 & 0.5 & 0.2 & 0 & 0 & 0 \\ 0.8 & 0 & 0 & 0.2 & 0.7 & 0.7 & 0.7 & 0.4 & 0.4 & 0.4 & 0.4 \\ 0.9 & 0 & 0 & 0.2 & 0.7 & 0.9 & 0.7 & 0.5 & 0.7 & 0.8 & 0.8 \\ 1.0 & 0 & 0 & 0.2 & 0.7 & 1.0 & 0.7 & 0.5 & 0.7 & 0.9 & 1.0 \end{pmatrix},$$

$$\tilde{R}_{(4,5)} =$$

$$\begin{pmatrix} & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 1.0 \\ 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.4 & 0.8 & 1.0 \\ 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.4 & 0.7 & 0.7 \\ 0.3 & 0 & 0 & 0.2 & 0.2 & 0.2 & 0.2 & 0.2 & 0.4 & 0.4 & 0.4 \\ 0.4 & 0 & 0 & 0.2 & 0.7 & 0.7 & 0.7 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.5 & 0 & 0 & 0.2 & 0.7 & 1.0 & 0.7 & 0.2 & 0 & 0 & 0 \\ 0.6 & 0 & 0 & 0.2 & 0.7 & 0.7 & 0.7 & 0.2 & 0 & 0 & 0 \\ 0.7 & 0.5 & 0.5 & 0.4 & 0.2 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 \\ 0.8 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0.9 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.0 & 1.0 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

根据(4) 式可得

$$\tilde{R}_5 = \tilde{R}_{(1,5)} \cup \tilde{R}_{(2,5)} \cup \tilde{R}_{(3,5)} \cup \tilde{R}_{(4,5)} =$$

$$\begin{pmatrix} & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 1.0 \\ 0.1 & 1.0 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0.2 & 0.4 & 0.8 & 1.0 \\ 0.2 & 0.7 & 0.7 & 0.4 & 0.2 & 0 & 0 & 0.2 & 0.4 & 0.7 & 0.7 \\ 0.3 & 0.4 & 0.4 & 0.4 & 0.2 & 0.2 & 0.2 & 0.2 & 0.4 & 0.4 & 0.4 \\ 0.4 & 0.7 & 0.7 & 0.4 & 0.7 & 0.7 & 0.7 & 0.5 & 0.7 & 0.7 & 0.7 \\ 0.5 & 1.0 & 0.7 & 0.4 & 0.7 & 1.0 & 0.7 & 0.5 & 0.7 & 0.9 & 1.0 \\ 0.6 & 0.7 & 0.7 & 0.4 & 0.7 & 0.7 & 0.7 & 0.5 & 0.7 & 0.7 & 0.7 \\ 0.7 & 0.5 & 0.5 & 0.4 & 0.5 & 0.5 & 0.5 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.8 & 0.7 & 0.7 & 0.4 & 0.7 & 0.7 & 0.7 & 0.4 & 0.4 & 0.4 & 0.4 \\ 0.9 & 0.9 & 0.7 & 0.4 & 0.7 & 0.9 & 0.7 & 0.5 & 0.7 & 0.8 & 0.8 \\ 1.0 & 1.0 & 0.7 & 0.4 & 0.7 & 1.0 & 0.7 & 0.5 & 0.7 & 0.9 & 1.0 \end{pmatrix}.$$

下面,我们再来考虑结点 4,5 对结点 6 的影响. 若结点 4 信息资产的价值分别为一级、二级、

三级,则结点6信息安全风险非常高(VH)、中(M)、低(L),即$\tilde{R}_{(4,6)} = \tilde{R}_{(4,5)}$. 同时结点5威胁发生的可能性与结点6的信息安全风险成线性关系,即$\tilde{R}_{(5,6)} = E$. 则

$\tilde{R}_6 = \tilde{R}_5 =$

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	sum
0.1	1.0	0.7	0.4	0.2	0	0	0.2	0.4	0.8	1.0	4.7
0.2	0.7	0.7	0.4	0.2	0	0	0.2	0.4	0.7	0.7	4.0
0.3	0.4	0.4	0.4	0.2	0.2	0.2	0.2	0.4	0.4	0.4	3.2
0.4	0.7	0.7	0.4	0.7	0.7	0.7	0.5	0.7	0.7	0.7	6.5
0.5	1.0	0.7	0.4	0.7	1.0	0.7	0.5	0.7	0.9	1.0	7.6
0.6	0.7	0.7	0.4	0.7	0.7	0.7	0.5	0.7	0.7	0.7	6.5
0.7	0.5	0.5	0.4	0.5	0.5	0.5	0.2	0.2	0.2	0.2	3.7
0.8	0.7	0.7	0.4	0.7	0.7	0.7	0.4	0.4	0.4	0.4	5.5
0.9	0.9	0.7	0.4	0.7	0.9	0.7	0.5	0.7	0.8	0.8	7.1
1.0	1.0	0.7	0.4	0.7	1.0	0.7	0.5	0.7	0.9	1.0	7.6

而后从矩阵$\tilde{R}_6$中选取使本行的和与其所对应频率的乘积在所有行中最大的一行,根据式(5)计算可得

$$P(0.1) = 1.0/7.6 = 0.132,$$
$$P(0.2) = 0.7/7.6 = 0.092,$$
$$P(0.3) = 0.4/7.6 = 0.053,$$
$$P(0.4) = 0.7/7.6 = 0.092,$$
$$P(0.5) = 1.0/7.6 = 0.132,$$
$$P(0.6) = 0.7/7.6 = 0.092,$$
$$P(0.7) = 0.5/7.6 = 0.066,$$
$$P(0.8) = 0.7/7.6 = 0.092,$$
$$P(0.9) = 0.9/7.6 = 0.118,$$
$$P(1.0) = 1.0/7.6 = 0.132.$$

3 结论

笔者应用模糊影响图理论对信息安全风险进行了评估,整个评估过程及结果合理有效、简便实用. 评估结果表明,该方法是一种有效的评估方法,不但可以减少获取大量统计数据的困难,而且还可以用模糊关系矩阵有效表述结点之间的相互影响. 同时还表明,利用模糊影响图理论进行信息安全评估其关键不在于算法本身,而在于准确描述结点之间以及结点状态与发生频率之间的模糊关系,模糊关系的精确程度将直接影响到评估结果.

参考文献:

[1] 赵东梅,刘海峰,刘晨光. 基于BP神经网络的信息安全风险评估[J]. 计算机工程与应用,2007,43(1):139-131.

[2] 付 钰,吴晓平,严承华. 基贝叶斯网络的信息安全风险评估[J]. 武汉大学学报:理学版,2006,52(5):631-634.

[3] 王英梅,王胜开,陈国顺,等. 信息安全风险评估[M]. 北京:电子工业出版社,2007:144-164.

[4] 刘金兰,韩文秀,李光泉. 关于工程项目风险分析的模糊影响图方法[J]. 系统工程学报,1994,9(2):81-88.

[5] 程铁信,王 平,张伟波. 模糊影响图评价算法的探讨[J]. 系统工程学报,2004,19(2):177-182.

[6] 詹原瑞. 影响图理论方法与应用[M]. 天津:天津大学出版社,1995. 44-56.

[7] TAMIM T S. An influence diagramming based risk analysis system[D]. Boulder: University of Colorado at Boulder,1989.

[8] SHACHTER R D. Probabilitic inference and influence diagram[J]. Operation Research,1988,36(4):589-605.

[9] 于睿箭,冯允成. 影响图的基础理论和发展[J]. 北京航空航天大学学报,1994,20(4):10-11.

Information Security Risk Assessment Based on Fuzzy Influence Diagram

ZHANG Kun, GE Lei, WANG Chun-xin, DAI Feng

(School of Information Engineering, Information Engineering University, Zhengzhou 45002, China)

Abstract: Based on the analysis of the factors of information security risk systematicly, this paper applyed a method named fuzzy influence diagram in assessing process, aimming at the diffculty of handling the uncertainty information. The author made an influence diagram by qualitative analysis, and calculated the probability of security risk applying the theory, then drew a conclusion. The conclusion demonstrates that the key to applying the method is to comfirm the fuzzy relation. The method combining qualitative analysis and quantitative analysis is reasonable and convenient, which can reflect the circumstance of information security risk, so it provides a new method for information security risk assessment.

Key words: fuzzy influence diagram; information security; risk assessment