

改进犹豫模糊集在信息安全风险评估上的应用

黄国庆^{1,2}, 肖 爽¹

(1 郑州大学 信息工程学院, 河南 郑州 450001;

2 空军第一航空学院 航空电子系, 河南 信阳 464000)

摘 要: 为有效解决信息安全风险评估时未知信息众多、专家会对评估分值犹豫的问题, 提出了使用改进犹豫模糊集对信息安全进行风险评估的方法. 方法思路是将心理预期与实际估计的数学关系转化成决策矩阵, 计算各底层指标权重, 利用低层指标和专家权重对决策矩阵加权, 最后用分数函数计算出评估结果. 采用该方法, 解决了信息安全风险评估过程中方案和专家决策的模糊性不能完全反映的问题, 同时使信息安全风险评估更符合客观实际. 实例分析证明, 该算法合理有效.

关键词: 信息安全; 风险评估; 犹豫模糊集; 心理预期; 决策矩阵

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2018)05-0105-04

The Application of Improved Hesitant Fuzzy set in Information Security Risk Assessment

HUANG Guo-qing^{1,2}, XIAO Shuang¹

(1 School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China;

2 Department of Aeronautical Electronics, The First Aeronautical College of Air Force, Xinyang 464000, China)

Abstract: To deal with the problem that much information is unknown and the experts will hesitate about the point value of evaluation, When information security risks are assessed, improved hesitant fuzzy set for information security risk assessment is proposed. The method's idea is transforming the actual estimation into the decision matrix of the fuzzy set and calculating the weight of each underlying index. Then, the decision matrix is weighted by the weight of underlying index and expert. The result is calculated using fractional function. This method is used to solve the problem that the fuzzy nature of the scheme and expert's decision-making in the information security risk assessment process which cannot be fully reflected and make the information security risk assessment more objective and practical. The example analysis shows that the proposed algorithm is Reasonable and effective.

Key words: information security; risk assessment; hesitant fuzzy set; expectations; decision matrix

1 引言

近些年来, 发生的信息安全事件无一不对国家和人民的财产安全造成巨大损失, 而且保证信息安全对军事领域的作用至关重要, 因此对信息安全风险的评估一直保持着较高的热度, 并取得了一系列成果. 比如: 文献[1]提出了对信息系统安全态势进行评估的方法, 文献[2]提出了针对信息安全风险的定性分析方法, 文献[3]进行了信息安全风险评估模

型的定量与定性对比等. 但是目前对信息安全风险评估研究的众多成果都存在着不能充分反映信息安全本身和专家决策的模糊性的问题. 并且它们的评估方法并不完全符合专家实际的评估过程.

近几年来, 犹豫模糊集在理论和应用上都得到了充分的研究^[4-7], 犹豫模糊集已经被证明能充分考虑到专家评估过程中犹豫的特点, 并且对模糊信息处理有着较好的效果^[8-9]. 改进的犹豫模糊集算法利用实际评估与预期结果的数学关系来形成模糊决策

矩阵,更符合专家处理问题过程的特点.改进的犹豫模糊集算法在处理信息安全风险评估的问题上更为合理有效.

2 犹豫模糊集概念

2.1 犹豫模糊集(HFS)

HFS 通常用式(1)来表示.

$$E = \{ (x, h_E(x)) \mid x \in X \} \quad (1)$$

式中, $h_E(x)$ 代表元素 $x \in X$ 在集合 E 中的可能隶属度,它的值 $V \in [0, 1]$. $h_E(x)$ 通常被叫做犹豫模糊元素(HFE)^[8].

2.2 犹豫模糊决定矩阵(HFDM)

HFDM 用式(2)表示.

$$H^k = (h_{ij}^k)_{m \times n} = \begin{pmatrix} h_{11}^k & h_{12}^k & \cdots & h_{1n}^k \\ h_{21}^k & h_{22}^k & \cdots & h_{2n}^k \\ \vdots & \vdots & \ddots & \vdots \\ h_{m1}^k & h_{m2}^k & \cdots & h_{mn}^k \end{pmatrix} \quad (2)$$

式中, h_{mn}^k 代表第 k 个专家对第 m 个方案的第 n 个指标评估的犹豫模糊元素.

2.3 犹豫模糊偏好关系(HFPR)

HFPR 的表示如式(3)所示.

$$R^k = (r_{ij}^k) = \begin{pmatrix} 0.5 & r_{12}^k & \cdots & r_{1n}^k \\ \cdots & 0.5 & \cdots & r_{2n}^k \\ \cdots & 1 - r_{ij}^k & \ddots & \vdots \\ \cdots & \cdots & \cdots & r_{nn}^k \end{pmatrix} \quad (3)$$

式中, r_{ij}^k 代表第 k 个专家对指标 i 和指标 j 重视的差别程度(若 $r_{ij}^k = 0.5$, 则 i 指标和 j 指标同等重要, 若 $r_{ij}^k = 1$ 则 i 指标绝对比 j 指标重要)^[9]. 而各指标的初步权重值 W_i 的计算公式为:

$$W_i = \frac{\sum_{k=1}^n r_{ik} - 0.5}{\frac{n(n-1)}{2}} \quad (4)$$

2.4 分数函数

让集合 $h = \{h^{(1)}, h^{(2)}, \cdots, h^{(Z)}\}$ 代表一个犹豫模糊元素(HFE), 那么它的分数函数为:

$$S_j = S_{h_j}(h) = \frac{1}{|h|} \sum_{i=1}^Z h^{(i)} \quad (5)$$

式中, j 代表该犹豫模糊元素对应的指标.

整个方案的分数函数为:

$$S_H(S_j) = \frac{1}{n} \sum_{j=1}^n S_j \quad (6)$$

式中, n 为指标的总数量.

3 改进犹豫模糊集

由于专家在进行信息风险评估时对风险的危害不易准确的量化, 文章采用预期理论与模糊集结合的方法来对信息安全风险进行量化.

HFDPM 的表示如式(7)所示.

$$E^k = (e_{ij}^k)_{m \times n} = \begin{pmatrix} e_{11}^k & e_{12}^k & \cdots & e_{1n}^k \\ e_{21}^k & e_{22}^k & \cdots & e_{2n}^k \\ \vdots & \vdots & \ddots & \vdots \\ e_{m1}^k & e_{m2}^k & \cdots & e_{mn}^k \end{pmatrix} \quad (7)$$

式中, e_{nm}^k 代表第 k 个专家对第 m 个方案的第 n 个指标评估的犹豫模糊决策值. 为了解决原有 HFS 不易量化, 反应决策值函数的凸凹性和初步评估值与最终信息安全风险评估值之间的增减关系等问题, 提出了改进犹豫模糊矩阵决策值的计算方法, 如下:

$$e_{nm}^k = \begin{cases} \frac{1-x^\alpha}{\lambda+1} & x \geq 0 \\ \frac{1+\lambda(-x)^\beta}{\lambda+1} & x < 0 \end{cases} \quad (8)$$

式中, $x = h_{nm}^k - L_n$ (L_n 代表对 n 指标的期望的安全评分值); λ 代表的是各指标评估值过低对风险所能造成的危害程度(λ 越大, 危害越大. 文章中假设各指标的值都为 2.25). 一般情况下使 $\lambda > 1$; 在评估值高于安全值时决策值随评估值的变化较小, 而在评估值低于安全值时决策值变化较大. 使 $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 1$. 从而当 $x \geq 0$ 时 e_{nm}^k 是凹函数, 当 $x < 0$ 时 e_{nm}^k 是凸函数, 从而达到以下效果: (1) 犹豫模糊决策值在评估值和安全值较接近时对评估值的变化较敏感; (2) 评估值过高或过低时, 评估值的改变对决策值影响较小. e_{nm}^k 为单调递减函数, 随着评估值的增加, 风险逐渐变小, 并且它的值在 0 到 1 之间 (易于模糊集分数函数处理). 当 $\alpha = 0.88, \beta = 0.88$ 时, x^α 和 $\lambda(-x)^\beta$ 的值能较好地与原始数据保持一致^[10].

4 信息安全风险评估指标

信息安全风险评估是利用信息和管理的技术对信息受到的安全风险进行评价的过程. 它评估考虑的因素主要有以下几方面: (1) 信息安全所受的威胁; (2) 信息系统本身的脆弱性被利用而导致恶性事件; (3) 恶性事件一旦发生所造成的损害^[11]. 文献[2] 通过研究给出了信息安全风险评估的指标体系, 如图 1 所示.

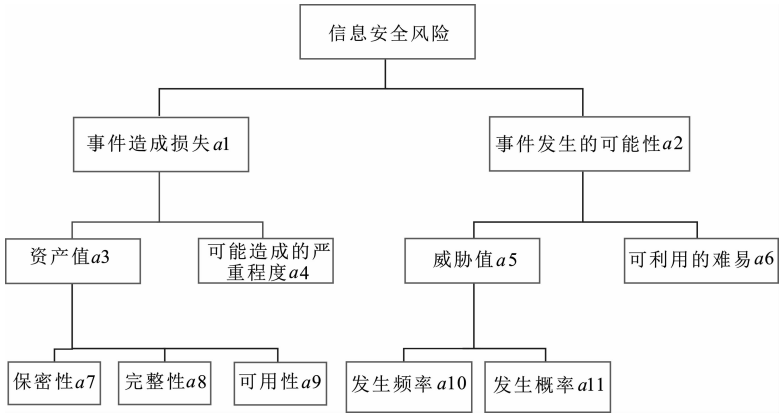


图 1 信息安全风险评估的指标体系

由于在风险评估实践中很难对指标进行量化的操作,所以一般情况下都采取专家直接对各要素指标赋值的方法^[2]。本文算法中评估值越高,信息安全风险越小。

5 评估算法的具体实现

本文算法中输入的是犹豫模糊决定矩阵(HFDM)、犹豫模糊偏好关系(HFPR)和对各指标的预期值 L ,各专家的权重 $W_1, W_2, \dots, W_n$ (由风险评估项目负责人根据各专家的能力和重要程度进行赋值),输出的是各方案的评估值。

步骤 1 根据各层指标的犹豫模糊偏好关系(HFPR),通过式(4)计算出各个指标的初步权重 $W_{a1}, W_{a2}, \dots, W_{a11}$ 。

步骤 2 计算各低层指标的最终权重:
 $W_1 = W_{a1} \times W_{a3} \times W_{a7}, W_2 = W_{a1} \times W_{a3} \times W_{a8},$
 $W_3 = W_{a1} \times W_{a3} \times W_{a9}, W_4 = W_{a1} \times W_{a4},$
 $W_5 = W_{a2} \times W_{a5} \times W_{a10}, W_6 = W_{a2} \times W_{a5} \times W_{a11},$
 $W_7 = W_{a2} \times W_{a6}$
(9)

步骤 3 根据犹豫模糊决定矩阵(HFDM)和对各指标的预期值 L (指标分别为保密性、完整性、可用性、可能造成的严重程度、发生频率、发生概率、可利用的难易),利用式(8)计算出犹豫模糊决策矩阵 E^k 。

步骤 4 计算犹豫模糊结果矩阵 B^k :
 $B^k = \begin{bmatrix} W_1 e_{11}^k & W_2 e_{12}^k & \cdots & W_7 e_{17}^k \\ W_1 e_{21}^k & W_2 e_{22}^k & \cdots & W_7 e_{27}^k \\ W_1 e_{31}^k & W_2 e_{32}^k & \cdots & W_7 e_{37}^k \end{bmatrix}$ (10)

步骤 5 根据式(5)、(6)计算各专家对于各方案的评估值 S^k (第 k 个专家对第 i 个方案的评估值)。

步骤 6 求出每个方案最终评估值 $Z_i =$

$\sum_{k=1}^n W_k S_i^k$ (Z_i 为第 i 个方案的最终评估值, n 为专家的总数量)。所得结果即为该方案的最终评估值。

5.1 条件假设

在查阅文献和充分研究信息安全风险评估的特点之后,本文对某一信息安全风险评估实例作如下假设。

(1) 参加此次信息风险评估的专家有两个,他们对文中 7 个指标的期望值的安全分值分别为:

$L_1 = \{0.6, 0.5, 0.7, 0.5, 0.4, 0.7, 0.6\},$
 $L_2 = \{0.5, 0.5, 0.6, 0.5, 0.4, 0.6, 0.7\}.$

专家的权重分别为 0.7 和 0.3。

(2) 本次评估两位专家判定的犹豫模糊偏好关系(HFPR)一致。

$R_{a0} = \begin{pmatrix} 0.5 & 0.6 \\ 0.4 & 0.5 \end{pmatrix}$,其中包括两个指标分别为:

事件造成的损失和事件发生的可能性。

$R_{a1} = \begin{pmatrix} 0.5 & 0.4 \\ 0.6 & 0.5 \end{pmatrix}$,其中包括两个指标分别为:

资产值和可能造成的严重程度。

$R_{a2} = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$,其中包括两个指标分别为:

威胁值和可利用的难易。

$R_{a3} = \begin{bmatrix} 0.5 & 0.7 & 0.3 \\ 0.3 & 0.5 & 0.4 \\ 0.7 & 0.6 & 0.5 \end{bmatrix}$,其中包括三个指标分

别为:保密性、完整性和可用性。

$R_{a5} = \begin{pmatrix} 0.5 & 0.7 \\ 0.3 & 0.5 \end{pmatrix}$,其中包括两个指标分别为:

发生频率和发生概率。

(3) 两位专家的犹豫模糊决定矩阵(HFDM)如式(11)所示:

$$\begin{aligned} H^1 &= \begin{bmatrix} \{0.4, 0.6\} & \{0.7\} & \{0.5, 0.6\} & \{0.6\} & \{0.5\} & \{0.6\} & \{0.7\} \\ \{0.6\} & \{0.2, 0.3\} & \{0.7\} & \{0.4, 0.7\} & \{0.6\} & \{0.6, 0.8\} & \{0.6\} \\ & \{0.6\} & \{0.4\} & \{0.8\} & \{0.5\} & \{0.7\} & \{0.8\} & \{0.3\} \end{bmatrix} \\ H^2 &= \begin{bmatrix} \{0.3, 0.5\} & \{0.6\} & \{0.4\} & \{0.4\} & \{0.4, 0.6\} & \{0.5, 0.6\} & \{0.9\} \\ & \{0.5, 0.7\} & \{0.3\} & \{0.6\} & \{0.5\} & \{0.6\} & \{0.7\} & \{0.8\} \\ & \{0.5\} & \{0.3, 0.5\} & \{0.7\} & \{0.3, 0.6\} & \{0.6\} & \{0.8\} & \{0.4\} \end{bmatrix} \end{aligned} \tag{11}$$

5.2 信息安全风险评估实例步骤

根据以上得到的信息,下面给出信息安全风险评估六个步骤.

步骤 1 根据式(4)得到各指标的初步权重值为: $(W_{a1}, W_{a2}, \cdots, W_{a11}) = (0.6, 0.4, 0.4, 0.6, 0.5, 0.5, 0.3333, 0.2333, 0.4334, 0.7, 0.3)$.

$$\begin{aligned} E^1 &= \begin{bmatrix} \{0.475\ 7, 0.307\ 7\} & \{0.475\ 7, 0.399\ 0\} & \{0.267\ 1\} & \{0.267\ 1\} & \{0.399\ 0\} & \{0.267\ 1\} & \{0.307\ 7\} \\ \{0.547\ 7, 0.475\ 7\} & \{0.307\ 7\} & \{0.399\ 0, 0.233\ 0\} & \{0.233\ 0\} & \{0.399\ 0, 0.267\ 1\} & \{0.307\ 7\} \\ \{0.307\ 7\} & \{0.399\ 0\} & \{0.267\ 1\} & \{0.307\ 7\} & \{0.201\ 0\} & \{0.267\ 1\} & \{0.547\ 7\} \end{bmatrix} \\ E^2 &= \begin{bmatrix} \{0.475\ 7, 0.307\ 7\} & \{0.267\ 1\} & \{0.475\ 7\} & \{0.399\ 0\} & \{0.307\ 7, 0.233\ 0\} & \{0.267\ 1, 0.307\ 7\} \\ \{0.233\ 0\} & \{0.307\ 7, 0.233\ 0\} & \{0.475\ 7\} & \{0.307\ 7\} & \{0.307\ 7\} & \{0.233\ 0\} & \{0.267\ 1\} & \{0.267\ 1\} \\ \{0.307\ 7\} & \{0.475\ 7, 0.307\ 7\} & \{0.267\ 1\} & \{0.475\ 7, 0.267\ 1\} & \{0.233\ 0\} & \{0.233\ 0\} \\ \{0.547\ 7\} \end{bmatrix} \end{aligned} \tag{12}$$

步骤 4:计算犹豫模糊结果矩阵 B^k 如式(13):

$$\begin{aligned} B^1 &= \begin{bmatrix} \{0.038\ 1, 0.024\ 6\} & \{0.013\ 0\} & \{0.049\ 5, 0.041\ 5\} & \{0.096\ 2\} & \{0.037\ 4\} & \{0.023\ 9\} \\ \{0.012\ 3\} & \{0.024\ 6\} & \{0.030\ 7, 0.026\ 6\} & \{0.032\ 0\} & \{0.143\ 6, 0.083\ 9\} & \{0.032\ 6\} \\ \{0.023\ 9, 0.016\ 0\} & \{0.012\ 3\} & \{0.024\ 6\} & \{0.022\ 3\} & \{0.027\ 8\} & \{0.110\ 8\} & \{0.028\ 1\} \\ \{0.016\ 0\} & \{0.037\ 5\} \end{bmatrix} \\ B^2 &= \begin{bmatrix} \{0.038\ 1, 0.024\ 6\} & \{0.015\ 0\} & \{0.049\ 5\} & \{0.143\ 6\} & \{0.043\ 1, 0.032\ 6\} \\ \{0.016\ 0, 0.018\ 5\} & \{0.012\ 3\} & \{0.024\ 6, 0.018\ 6\} & \{0.026\ 6\} & \{0.032\ 0\} & \{0.110\ 8\} \\ \{0.032\ 6\} & \{0.016\ 0\} & \{0.002\ 1\} & \{0.024\ 6\} & \{0.026\ 6, 0.017\ 2\} & \{0.027\ 8\} \\ \{0.171\ 3, 0.096\ 2\} & \{0.032\ 6\} & \{0.014\ 0\} & \{0.037\ 5\} \end{bmatrix} \end{aligned} \tag{13}$$

步骤 5 利用式(5)、式(6) 计算得到各专家对于各方案的评估值:

$$\begin{aligned} S_{11} &= 0.037\ 1, S_{21} = 0.037\ 7, S_{31} = 0.038\ 2; \\ S_{12} &= 0.043\ 8, S_{22} = 0.034\ 5, S_{32} = 0.041\ 7. \end{aligned}$$

步骤 6:求得最终的信息安全风险评估值为: $Z_1 = 0.039\ 1, Z_2 = 0.036\ 7, Z_3 = 0.039\ 2$.

5.3 结果分析

经结果分析得到 $Z_3 > Z_1 > Z_2$,方案 3 的风险值最大,需要着重加强管理和监控. 文章算法比以前提过的算法^[1-3,8],更为符合评估过程的客观实际,并能较好地反映专家决策和方案的模糊性,提高了信息安全风险评估的可靠性.

6 结束语

本文通过对信息安全风险评估过程的研究和分

析,提出使用改进的犹豫模糊集来进行信息安全风险评估. 改进的犹豫模糊集根据专家关于方案心理预期与实际估计的数学关系形成决策矩阵,使得信息安全风险评估的过程更为贴近实际. 而且犹豫模糊集也能更好地反映方案和专家决策的模糊性. 本文可为信息安全的风险评估提供新的研究思路.

步骤 2 根据式(9) 计算得到各底层指标的最终权重为: $(W_1, W_2, \cdots, W_7) = (0.08, 0.056, 0.104, 0.36, 0.14, 0.06, 0.2)$.

步骤 3 根据式(8) 得到犹豫模糊决策矩阵 E^k 如式(12)(本文示例中选取 $\alpha = 0.88, \beta = 0.88, \lambda = 2.25$):

参考文献:

[1] 付钰,吴晓平,叶清. 基于改进 FAHP—BH 的信息系统安全态势评估方法[J]. 通信学报,2009, 30(9): 135-140.

[2] 唐作其,陈选文,戴海涛,等. 多属性群决策理论信息安全风险评估方法研究[J]. 计算机工程与应用,2011,47(15):104-107.