梯形模糊数的信息安全风险群决策评估方法

吴叶科[1],宋如顺[1],陈 波[2]

(1. 南京师范大学 数学科学学院, 江苏 南京 210046;
2. 南京师范大学 计算机科学与技术学院, 江苏 南京 210046)

[摘要] 针对含有语言评价信息的群决策问题,将梯形模糊数引入信息安全风险评估中,提出了一种基于梯形模糊数的信息安全风险群决策评估方法. 首先,用梯形模糊数来表达决策者的评价信息,然后给出梯形模糊数判断矩阵的集结步骤,最后通过计算各威胁所带来的风险与负理想解的相对贴近度,对威胁程度进行排序. 通过实例分析,说明了该方法的可行性和有效性.

[关键词] 语言变量,梯形模糊数,群决策,信息安全风险评估,理想点法
[中图分类号] TP309 [文献标识码] A [文章编号]1672-1292(2011)01-0051-05

Group Decision Making for Information Security Risk Assess Method Based on Trapezoidal Fuzzy Number

Wu Yeke[1], Song Rushun[1], Chen Bo[2]

(1. School of Mathematics Sciences, Nanjing Normal University, Nanjing 210046, China;
2. School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, China)

Abstract: In view of the group decision-making problem based on linguistic terms, a group decision making for information security risk assess method based on trapezoidal fuzzy number was proposed with the introduction of trapezoidal number into information security risk assessment. Firstly, the language estimate information was transformed to trapezoidal fuzzy number, then the aggregation steps of collective trapezoidal fuzzy number complementary judgment matrix are given, finally the ranking of all threads was judged by the relative closeness between risks and negative ideal solution. An example is given to illustrates the practicability and validity of this method.

Key words: linguistic variable, trapezoidal number, group decision making, information security risk assessment, TOPSIS

随着计算机技术和网络技术的迅猛发展,信息技术被广泛地应用于各行各业,社会发展对信息资源的依赖越来越高. 由于信息系统自身的缺陷以及与其相连的网络环境的开放,敏感信息的泄露、计算机病毒的泛滥、黑客的入侵等,导致信息系统面临巨大的安全风险. 通过近几年来对信息安全的不断研究,人们对信息安全内涵的认识不断深入,从最初的信息保密性发展到了信息的完整性、可用性、可控性和不可否认性,进而又提出和发展了“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等众多方面的基础理论和专业技术. 同时,人们逐渐认识到:解决信息系统安全问题单凭技术是不够的,还要加强管理. 其中,信息安全风险评估起着重要的作用,它是信息系统安全的基础和前提[1]. 通过信息安全风险评估,能够了解信息系统当前的安全状态,针对性地采取安全措施,进而提升信息系统的生存能力.

由于信息安全风险评估的复杂性、不确定性,用模糊数来表达模糊信息及评估者模糊偏好已经相当普遍. 文献[2]将三角模糊数和层次分析法(Analytic Hierarchy Process, AHP)结合,提出了改进的三角模糊数评价方法,并将其运用到网络安全的风险评估中,提高网络安全评价的客观性和有效性. 信息安全风险评估过程中一般涉及多个评估专家或组织,个体独立评估结论往往具有片面性,为了减小评估结果的偏差,在风险评估过程中引入风险评估群决策. 文献[3]提出了一种结合 FAHP(fuzzy AHP)和群组决策的风险量化评估方法,利用 FAHP 处理主观评估判断结果,实现了综合考虑风险发生概率和风险损失的偏好排

收稿日期: 2010-09-29.
通讯联系人: 宋如顺,教授,硕士生导师,研究方向:信息网络安全保密技术. E-mail:05085@njnu.edu.cn

序,建立群组偏好排序线性规划模型,降低了个体评估决策的不确定性. 文献[4]利用三角模糊数建立了信息安全风险的可能性矩阵和损失矩阵,通过对专家意见的集结,得到信息安全风险矩阵,并对威胁的风险大小进行了分析和评判. 虽然梯形模糊数的隶属函数的形状比三角模糊数的隶属函数形状复杂,但其具有良好的近似计算性质,且三角模糊数是其特例,故梯形模糊数更能反映客观事物的不确定性,表达决策者的主观性,更具一般性. 文献[5]建立了基于梯形模糊数期望值的多维偏好群决策模型,通过实例证实了梯形模糊数应用于多属性群决策方法的可行性和有效性. 然而,在对威胁的严重程度及其发生的可能性大小判断的时候,很难以精确的数值表示,但可以用语言评价值表示. 本文将专家对风险评估的语言评价信息转化为梯形模糊数,并引入群决策方法,综合考虑决策者权重和意见的一致性程度,对威胁程度的大小根据相对贴近度的数值进行排序. 最后,将整个算法应用于解决某信息系统的安全风险评估,证明了该算法的有效性.

1　信息安全风险评估

所谓的信息安全风险评估是指依据有关信息安全技术与管理标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程. 它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性,并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响,即风险值[6].

风险计算的形式化表示为: 风险值 $= R(A,T,V) = R(L(T,V),F(Ia,Va))$. 其中,$R$ 表示安全风险计算函数; A 表示资产; T 表示威胁; V 表示脆弱性; Ia 表示安全事件所作用的资产价值; Va 表示脆弱性严重程度; L 表示威胁利用资产的脆弱性导致安全事件发生的可能性; F 表示安全事件发生后产生的损失.

2　梯形模糊数信息安全风险群决策评估原理与步骤

2.1　信息安全风险群决策评估的数学描述

设多人决策(专家)群体集 $E = (E_1,E_2,\cdots,E_P)$, $W = (W_1,W_2,\cdots,W_P)$ 是决策群集的权重向量,反映了群决策集中决策者的权威程度,其中 $0 < W_p < 1$, $\sum_{p=1}^{p} W_p = 1$. 经专家集体讨论,确定信息系统面临的威胁集 $T = (T_1,T_2,\cdots,T_l)$,存在的脆弱性集 $V = (V_1,V_2,\cdots,V_m)$,拥有的资产集 $A = (A_1,A_2,\cdots,A_n)$,专家 E_p 给出的具有语言形式的安全事件发生可能性矩阵 $\boldsymbol{X}^p = [\boldsymbol{x}_{ij}^p]_{l\times m}$,安全事件发生后造成的损失矩阵 $\boldsymbol{Y}^p = [\boldsymbol{y}_{jk}^p]_{m\times n}$. 其中,$\boldsymbol{x}_{ij}^p$ 表示专家 E_p 评判威胁 T_i 利用脆弱性 V_j 的可能性程度; $\boldsymbol{y}_{jk}^p$ 表示专家 E_p 评判脆弱性 V_j 被成功利用后对资产 A_k 的影响程度. 本文中专家给出的模糊语言评价等级与梯形模糊数的转换关系如表1所示.

表1　语言评价等级与梯形模糊数的转换关系

Table 1　Transition between the language describe and trapezoid fuzzy numbers

语言评价项	梯形模糊数
很高	(0.8,0.9,1,1)
高	(0.6,0.75,0.75,0.9)
中	(0.3,0.5,0.5,0.7)
低	(0.1,0.25,0.25,0.4)
很低	(0,0,0.1,0.2)

2.2　梯形模糊数群决策信息安全风险评估的步骤

由专家给出的具有语言形式的安全事件发生可能性矩阵,和损失矩阵的群决策的步骤相同. 不失一般性,本文以安全事件发生的可能性决策矩阵为例,对专家评价集结为群评价的步骤作介绍.

步骤1　将语言信息评价矩阵转化为梯形模糊数决策矩阵.

对照表1中语言评价项与梯形模糊数的对应关系,将决策者给出的具有语言形式的评价信息转换为相应的梯形模糊数. 如将专家 E_p 给出的可能性语言评价矩阵 $\boldsymbol{X}^p = [\boldsymbol{x}_{ij}^p]_{l\times m}$,转化为梯形模糊数决策矩阵,记为 $\overline{\boldsymbol{X}}^p = [\overline{\boldsymbol{x}}_{ij}^p]_{l\times m}$,其中 $\overline{\boldsymbol{x}}_{ij}^p = (a_{ij}^p,b_{ij}^p,c_{ij}^p,d_{ij}^p)$.

步骤2　规范梯形模糊数原始决策矩阵.

为了消除不同物理量纲对决策结果的影响,必须对模糊决策矩阵进行规范化处理. 对越大越优型指标和越小越优型指标分别按如式(1)、(2)进行规范化处理,以形成规范化模糊决策矩阵 $\widetilde{\boldsymbol{X}}^p = [\tilde{\boldsymbol{x}}_{ij}^p]_{l\times m}$,记 $\tilde{\boldsymbol{x}}_{ij}^p = (\tilde{a}_{ij}^p,\tilde{b}_{ij}^p,\tilde{c}_{ij}^p,\tilde{d}_{ij}^p)$.

$$\tilde{\boldsymbol{x}}_{ij}^p = \left(\frac{a_{ij}^p}{d_{j^*}^p},\frac{b_{ij}^p}{d_{j^*}^p},\frac{c_{ij}^p}{d_{j^*}^p},\frac{d_{ij}^p}{d_{j^*}^p}\right), \tag{1}$$

$$\tilde{\boldsymbol{x}}_{ij}^{p} = \left(\frac{a_{j-}^{p}}{d_{ij}^{p}}, \frac{a_{j-}^{p}}{c_{ij}^{p}}, \frac{a_{j-}^{p}}{b_{ij}^{p}}, \frac{a_{j-}^{p}}{a_{ij}^{p}}\right). \tag{2}$$

其中,$d_{j*}^{p} = \max_{i}\{d_{ij}^{p}\}$,$d_{j-}^{p} = \min_{i}\{a_{ij}^{p}\}$.

步骤 3 集结个体评估结果为群体一致性评估结果.

为了做出群体决策,关键是将个体评价集结为群体一致性评价. 首先采用文献[7]计算两梯形模糊数相似度的方法衡量两位专家 E_p 和 E_q 对第 i 种威胁利用第 j 种脆弱性的可能性判断的一致性相似度:

$$S_{ij}^{pq} = S(\tilde{\boldsymbol{x}}_{ij}^{p}, \tilde{\boldsymbol{x}}_{ij}^{q}) = 1 - \frac{|\tilde{a}_{ij}^{p} - \tilde{a}_{ij}^{q}| + |\tilde{b}_{ij}^{p} - \tilde{b}_{ij}^{q}| + |\tilde{c}_{ij}^{p} - \tilde{c}_{ij}^{q}| + |\tilde{d}_{ij}^{p} - \tilde{d}_{ij}^{q}|}{4}. \tag{3}$$

为了反映某一专家的评价与其余专家评价的一致性,引入个体平均度指标 S_{ij}^{p}. 专家 E_p 的个体平均度指标 S_{ij}^{p} 按式(4)计算:

$$S_{ij}^{p} = \frac{1}{P-1}\left(\sum_{p=1, p\neq q}^{p} S_{ij}^{pq}\right). \tag{4}$$

为了便于比较,将各专家的个体平均度进行归一化处理,可得到专家 E_p 的个体相对一致度指标 SR_{ij}^{p},计算公式为:

$$SR_{ij}^{p} = \frac{S_{ij}^{p}}{\sum_{p=1}^{p} S_{ij}^{p}}. \tag{5}$$

将专家 E_p 的决策意见与其他群体专家意见的相对一致程度以及其权威性程度(权重),通过线性组合成为组合一致度指标 C_{ij}^{p},即决策者对群体决策的贡献度:

$$C_{ij}^{p} = \alpha W_p + (1-\alpha) SR_{ij}^{p}. \tag{6}$$

式中,α 为联接系数,反映了决策者权重相对于与其他决策者意见相符程度的重要性. 如果 $\alpha > 0.5$,则集结决策者评估意见时看重的是权威专家的个体意见; 如果 $\alpha < 0.5$,则看重的是决策群体的一致意见; 如果 $\alpha = 0.5$,则是一个折中的情况. 以线性组合的方式将决策者权重与一致性度量相合成而构造的组合一致性指标,较好地体现了权威性与一致性的原则.

将式(6)计算的决策者对群体决策的贡献度作为加权因子,按式(7)把各专家关于安全事件发生可能性的规范化的模糊决策矩阵集结为所有决策者关于可能性的群体模糊综合决策矩阵 $\boldsymbol{P} = (\boldsymbol{p}_{ij})_{l\times m}$:

$$\boldsymbol{p}_{ij} = (C_{ij}^{1} \otimes \tilde{\boldsymbol{x}}_{ij}^{1}) \oplus (C_{ij}^{2} \otimes \tilde{\boldsymbol{x}}_{ij}^{2}) \oplus \cdots \oplus (C_{ij}^{p} \otimes \tilde{\boldsymbol{x}}_{ij}^{p}), \quad i = 1,2,\cdots,l,\ j = 1,2,\cdots,m. \tag{7}$$

按照上述相同的步骤,求出所有决策者关于安全事件发生后造成的损失的群体模糊综合决策矩阵 $\boldsymbol{L} = (\boldsymbol{l}_{jk})_{m\times n}$,其中 $\boldsymbol{l}_{jk} = (C_{jk}^{1} \otimes \tilde{\boldsymbol{y}}_{jk}^{1}) \oplus (C_{jk}^{2} \otimes \tilde{\boldsymbol{y}}_{jk}^{2}) \oplus \cdots \oplus (C_{ij}^{p} \otimes \tilde{\boldsymbol{y}}_{ij}^{p})$,$j = 1,2,\cdots,m, k = 1,2,\cdots,n$.

采用相乘法,计算出信息安全风险的模糊综合决策矩阵

$$\boldsymbol{R} = (\boldsymbol{r}_{ij})_{l\times n} = \boldsymbol{P} \otimes \boldsymbol{L}. \tag{8}$$

式中,符号"⊗","⊕"分别表示梯形模糊数的乘法和加法运算.

步骤 4 梯形模糊数精确化.

信息安全的模糊综合决策矩阵 $\boldsymbol{R} = (\boldsymbol{r}_{ij})_{l\times n}$ 中的每一个元素 $\boldsymbol{r}_{ij}$ 依然是梯形模糊数,记为 $\boldsymbol{r}_{ij} = (e_{ij}, f_{ij}, g_{ij}, h_{ij})$. 为了便于比较,采用文献[8]的方法按式(9)对其进行模糊数精确化处理:

$$\tilde{r} = (e_{ij} + f_{ij} + g_{ij} + h_{ij})/4,\ i = 1,2,\cdots,l,\ j = 1,2,\cdots,n. \tag{9}$$

从而得到了精确化综合决策矩阵 $\tilde{\boldsymbol{R}} = (\tilde{r}_{ij})_{l\times n}$,其中 $\tilde{r}_{ij}$ 是一个由梯形模糊数 r_{ij} 转化而来的一个实数.

步骤 5 利用理想点法(TOPSIS)确定理想解(PIS)和负理想解(NIS).

利用文献[9]的理想点法,由精确化综合决策矩阵 $\tilde{\boldsymbol{R}} = (\tilde{r}_{ij})_{l\times n}$,分别按式(10)和(11)确定决策问题的理想解集 G^{*} 和负理想解集 G^{-}. 在信息安全中,理想解就是信息系统的风险值最小,信息系统处于非常安全的状态,负理想解就是信息系统的风险值最大,信息系统处于极端危险的状态.

$$G^{*} = \{g_1^{*}, g_2^{*}, \cdots, g_l^{*}\} = \{(\min_{i} r_{ij} \mid i = 1,2,\cdots,l),\ j = 1,2,\cdots,n\}. \tag{10}$$

$$G^{-} = \{g_1^{-}, g_2^{-}, \cdots, g_l^{-}\} = \{(\max_{i} r_{ij} \mid i = 1,2,\cdots,l),\ j = 1,2,\cdots,n\}. \tag{11}$$

步骤 6 按相对贴近值对威胁排序.

按照加权欧氏距离平方定义按式(12)和式(13)计算出每个威胁 t_j 偏离理想解的距离 d_j^* 和远离负理想解的距离 d_j^-:

$$d_j^* = \sqrt{\sum_{i=1}^{l}(r_{ij} - g_i^*)^2},\ j = 1,2,\cdots,n. \tag{12}$$

$$d_j^- = \sqrt{\sum_{i=1}^{l}(r_{ij} - g_i^-)^2},\ j = 1,2,\cdots,n. \tag{13}$$

最后,采用式(14)的比例式计算出各威胁所带来的风险与负理想解的相对贴近度,并按值的大小排序. 其中,$0 \leqslant CC_j \leqslant 1$,理想状态下 CC_j 为 0,如为负理想状态,则 CC_j 接近 1. 一般情况下,CC_j 处于 0,1 之间,CC_j 值越大,说明威胁对信息系统的危害最大. 根据排序的结果,有针对性地采取安全措施,提升系统的安全性.

$$CC_j = \frac{d_j^*}{d_j^* + d_j^-}. \tag{14}$$

3　案例分析

以某信息系统进行信息安全风险评估为例,应用上述方法进行信息安全风险评估. 为计算简便,根据信息安全风险评估规范[6]并结合该信息系统的实际情况,选取的威胁包括篡改信息(T_1),业务抵赖(T_2),非授权访问(T_3);脆弱性包括管理脆弱性(V_1)和技术脆弱性(V_2);资产的保密性(A_1),完整性(A_2),可用性(A_3). 邀请信息安全风险评估领域的 3 位专家,根据专家的专业水平和权威性分配权重 $W = (0.4, 0.3, 0.3)$;专家给出的具有语言形式的安全事件发生可能性,安全事件发生后造成的损失评价信息分别如表 2、表 3 所示.

表 2　专家给出的具有语言形式的可能性决策信息

Table 2　The linguistic decision-making information of possibility gave by experts

		V_1	V_2
E_1	T_1	中	高
	T_2	高	低
	T_3	中	很高
E_2	T_1	高	很高
	T_2	低	中
	T_3	高	高
E_3	T_1	中	高
	T_2	中	中
	T_3	高	高

表 3　专家给出的具有语言形式的损失决策信息

Table 3　The linguistic decision-making information of loss gave by experts

		A_1	A_2	A_3
E_1	V_1	高	中	中
	V_2	高	低	高
E_2	V_1	很高	高	中
	V_2	高	高	中
E_3	V_1	高	高	中
	V_2	高	中	低

首先,按照信息安全风险群决策评估方法的步骤 1 ~ 3 将评估专家的语言信息评价矩阵转化为梯形模糊数矩阵,按式(1)或(2)进行规范化处理,按式(3)计算评估专家之间的相似度,再按式(4)、(5)计算出专家个体平均一致度指标和个体相对一致度指标,在将个体决策矩阵集结为群体决策矩阵时,取 $\alpha = 0.5$,采用折中情形,兼顾权威专家的意见和决策群体的一致性意见. 集结后得到可能性群体的模糊综合决策矩阵 $\boldsymbol{P}$ 和损失的群体模糊综合决策矩阵 $\boldsymbol{L}$:

$$\boldsymbol{P} = \begin{bmatrix} (0.432 & 0.638 & 0.638 & 0.844) & (0.684 & 0.338 & 0.855 & 0.964) \\ (0.383 & 0.568 & 0.569 & 0.755) & (0.241 & 0.431 & 0.431 & 0.625) \\ (0.550 & 0.736 & 0.736 & 0.922) & (0.694 & 0.831 & 0.867 & 0.968) \end{bmatrix},$$

$$\boldsymbol{L} = \begin{bmatrix} (0.708 & 0.854 & 0.885\ 1) & (0.580 & 0.790 & 0.790\ 1) & (0.394\ 0.657\ 0.657\ 0.920) \\ (0.645\ 0.786\ 0.786\ 0.969) & (0.365\ 0.567\ 0.567\ 0.770) & (0.430\ 0.647\ 0.647\ 0.863) \end{bmatrix}.$$

利用相乘法,计算出信息安全风险的模糊综合决策矩阵 $\boldsymbol{R}$ 后,进行模糊数精确化,得到精确的综合非模糊决策矩阵 $\tilde{\boldsymbol{R}}$:

$$\tilde{\boldsymbol{R}} = \begin{bmatrix} 1.265 & 1.013 & 1.001 \\ 0.864 & 0.734 & 0.699 \\ 1.328 & 1.092 & 1.066 \end{bmatrix}.$$

按照公式(10)、(11)找到理想解和负理想解,并按公式(14)计算出各威胁与负理想解的贴近度,如表4所示.

根据排序结果,发现非授权访问(T_3)对信息系统的威胁最大,其次是篡改信息(T_1),最后是业务的抵赖(T_2). 据此,需根据不同的安全强度,有针对性地控制不同级别的访问权限.

表4 威胁与负理想解相对贴近度的排序

Table 4 The ranking of the relative nearness degree between threat and negative-ideal solutions

	d_j^*	d_j^-	CC_j	排序
T_1	0.446 7	0.361 2	0.552 9	2
T_2	0.394 1	0.758 1	0.342 0	3
T_3	0.511 6	0.352 6	0.592 0	1

4 结语

本文将评估专家给出的具有语言信息评价转化为梯形模糊数来处理,为防止风险评估过程中个人评判的片面性,引入风险评估群决策,将专家个人的评判集结成群体的评判结果,得到群体一致性的可靠的评价结果. 通过计算各威胁所带来的风险与负理想解的相对贴近度,对威胁程度进行排序. 通过实例可以看出,由于梯形模糊数和群决策方法的引入,不但吸收了专家个体的意见,还对各专家的意见起到平衡的作用. 但联接系数 α 的精确选择,目前还没有更好的解决办法,这是今后进一步需要研究的工作.

[参考文献](References)

[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 Dengguo, Zhang Yang, Zhang Yuqing. Survey of information security risk assessment[J]. Journal of China Institute of Communications, 2004,25(7):10-18. (in Chinese)

[2] 陈治宏,卢国明,吴晓华,等. 基于 AHP 的群决策风险评估方法[J]. 计算机应用,2009,29(6):125-127.
Chen Zhihong, Lu Guoming, Wu Xiaohua, et al. Risk assessment method for group decision-making with AHP[J]. Journal of Computer Applications, 2009,29(6):125-127. (in Chinese)

[3] 秦大力,张利,李吉慧. 基于 FAHP 的信息安全风险群组决策评估方法[J]. 计算机应用研究,2009,26(7):2 744-2 746.
Qin Dali, Zhang Li, Li Jihui. Group decision making to risk assessment of information security based on FAHP[J]. Application Research of Computers, 2009,26(7):2 744-2 746. (in Chinese)

[4] 吕俊杰,王元卓. 信息安全风险模糊群决策评估方法[J]. 计算机工程与应用,2010,46(12):17-20.
Lü Junjie, Wang Yuanzhuo. Information security risk evaluation method based on fuzzy matrix and group decision[J]. Computer Engineering and Applications, 2010,46(12):17-20. (in Chinese)

[5] 刘於勋,沈轶,谢妞妞. 基于梯形模糊数期望值的多维偏好群决策模型[J]. 控制与决策,2009,24(9):1 377-1 379.
Liu Yuxun, Shen Yi, Xie Niuniu. Group decision-making model for multidimensional analysis of preference on trapezoid fuzzy number expected values[J]. Control and Decision, 2009,24(9):1 377-1 379. (in Chinese)

[6] 中华人民共和国国家质量监督检验检疫总局. GB/T20984-2007 信息安全技术: 信息安全风险评估规范[S]. 北京: 中国标准出版社,2007.
General Administation of Quality Supervision, Inspection and Quarantine of the Perople's Republic of China. GB/T20984-2007 Information security technology——Risk assessment specification for information security[S]. Beijing: Standards Press of China, 2007. (in Chinese)

[7] Olcer A I, Odabasi A Y. A new fuzzy attributive group decision making methodology and its application to propulsion/manoeuvring system selection problem[J]. Journal of Operational Research, 2005,166:93-114.

[8] Wang J W, Cheng C H, Huang K C. Fuzzy hierarchical TOPSIS for supplier selection[J]. Applied Soft Computing, 2009(9):377-386.

[9] Yang T, Hung C C. Multiple-attribute decision-making methods for plant layout design problem[J]. Robotics and Computer-Integrated Manufacturing, 2007(23):126-137.

[责任编辑: 严海琳]