信息安全风险模糊群决策评估方法

吕俊杰[1],王元卓[2]
LV Jun-jie[1],WANG Yuan-zhuo[2]

1.北京工商大学 商学院,北京 100048
2.中国科学院 计算技术研究所,北京 100190
1.School of Business,Beijing Technology and Business University,Beijing 100048,China
2.Institute of Computing Technology,Chinese Academy of Sciences,Beijing 100190,China
E-mail:lvjj@th.btbu.edu.cn

LV Jun-jie,WANG Yuan-zhuo.Information security risk evaluation method based on fuzzy matrix and group decision. Computer Engineering and Applications,2010,46(12):17-20.

Abstract: Aiming at solving the difficulty of obtaining objective date on information security,this paper proposes an information security risk evaluation method based on fuzzy matrix and group decison.Firstly,the language estimates of risk probability and risk outcome are related to triangular fuzzy number.Secondly,a formulation for aggregating opinions and a method to select the positive and negative ideal solution are put forward.Then the threat severity about risk can be derived.Finally,an example is given to illustrate the application of the proposed method.

Key words: information security;risk evaluation;triangular fuzzy number;group decision

摘 要:信息安全风险评估是对信息安全进行风险管理的最根本依据,信息安全风险评估的客观性和准确性对保障信息系统安全起着重要作用。针对信息安全风险数据难以获取、不确定性较多的特点,给出了一种基于模糊评价矩阵的信息安全风险群决策评估方法。首先将语言评价转化为定量的模糊评价,利用三角模糊数来建立信息安全风险的可能性矩阵和损失矩阵,然后通过对专家意见的集结,得到信息安全风险矩阵。其次给出了三角模糊数风险矩阵正理想解和负理想解的选取方法,以及风险严重程度的比较依据,对威胁的风险大小进行分析与评判。最后通过一个算例对该方法进行了说明。

关键词:信息安全;风险评估;三角模糊数;群决策
DOI:10.3778/j.issn.1002-8331.2010.12.005 **文章编号**:1002-8331(2010)12-0017-04 **文献标识码**:A **中图分类号**:TP309

1 引言

20世纪90年代以来,随着经济全球化和世界科技革命,信息技术、信息产业和信息网络蓬勃发展,社会信息化程度不断加深,信息对国家、组织和个人发展的影响日益增加、日益突出。国家、企业和个人对信息安全性要求也变得越来越高。与此同时,各种黑客利用系统安全弱点不断地开展新型攻击,网络攻击群体的规模迅速扩大,攻击水平飞速提高,攻击所造成的影响也不断严重, 信息系统所面临的安全风险和威胁日趋严重。信息系统安全问题单凭技术是无法得到彻底解决的,管理与技术相结合的观点也日益被学术界和实业界所接受。其中,信息系统安全风险评估占有重要的地位,它是信息系统安全的基础和前提。

2007年颁布的国家标准《信息安全技术信息安全风险评估规范》GB/T20984-2007中定义信息安全风险评估是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机密性、完整性和可用性等安全属性进行评价的过程[1]。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。信息安全风险评估是风险管理的最根本依据,只有在准确评估的基础上,才能合理部署和利用信息安全的信任体系、监控体系和应急处理等重要的基础设施,确定合适的安全措施,从而确保机构具有完成其使命的信息安全保障能力。

2 信息安全风险评估的研究现状

信息安全风险是指由于资产的重要性、人为或自然的威胁以及利用信息系统及其管理体系的脆弱性,导致安全事件发生所造成的影响[1]。信息安全风险的构成中有3个主要的关键要素,分别是资产、威胁和脆弱性。信息安全风险评估的首要工作就是识别出信息资产、威胁、脆弱性以及它们之间的关系,对风

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60803123);中国博士后科学基金特别资助项目(China Postdoctoral Science Foundation under Grant No.200902101)。

作者简介:吕俊杰(1979-),女,博士,讲师,主要研究方向为网络及信息安全评估,决策理论,风险管理;王元卓(1978-),男,博士,助理研究员,主要研究方向为计算机网络及信息安全分析与评估,随机模型、博弈模型等。

收稿日期:2010-01-15 **修回日期**:2010-03-09

险发生的可能性和严重程度进行评价,然后才能开展信息安全风险评估和风险管理。

在信息安全风险评估中,对于威胁的严重程度,及其发生的可能性,人们总是通过“严重”、“一般”等语言评价项来进行评价,在这种情况下往往不能利用精确的数据准确地表达实际的风险情况。模糊集合论则是处理模糊现象的有效工具[2-3]。在信息安全问题中,由于人们对于风险信息的判断往往是模糊的,一个较实用的方法就是采用语言评价项来代替精确数[4-5],威胁对资产的影响及威胁发生的可能性都可以通过语言评价项来表达,而这些语言评价项又可以通过三角模糊数来刻画[6-7]。

模糊集理论被广泛应用于排序模型中[8-11],群体决策及相关的信息集结方法为充分利用专家意见提供了依据[12-18]。利用模糊集理论进行信息安全风险评估的文献近年也逐渐涌现。其中,文献[19]是利用模糊理论对各种威胁的重要性分层次比较得到威胁的排序;文献[20]则是将威胁分类为对风险可能性的影响和损失的影响对威胁进行排序。文献[21-22]也利用模糊算法来处理风险问题。文献[23]通过对威胁频率的灵敏度分析来进行信息安全风险评估。然而,这些文献都没有考虑到威胁与脆弱性、资产间一对多、多对一的对应关系,影响了评估的合理性。该文将这种关系通过矩阵表示出来,提出信息安全风险模糊群决策评估方法。

3 信息安全模糊群决策评估方法

信息安全风险评估的难点,一方面是必须将专家意见转化为量化指标,才能为风险管理提供定量化的参考依据。而且专家评价的群决策个体中,即可能由权威专家起关键作用,也可能是多个专家意见的均衡统一,所以对专家意见的集结方式对评估结果也起到至关重要的作用。另一方面,同一种威胁可能会利用同一种资产的不同的脆弱性对资产构成影响。类似的,同一种威胁也可能会利用同一种脆弱性对不同的资产构成影响。所以威胁与脆弱性和资产的一对多、多对一或者多对多的对应关系只有被准确地识别出来,才能够正确地进行评估,有效地采取防控措施,确保信息系统的安全。该文提出的基于模糊矩阵的信息安全风险群决策评估方法就可以有效地解决上述问题。

3.1 语言评价条件下的信息安全风险评估矩阵

设有多个专家个体所组成的专家群体 $E=(e_1,e_2,\cdots,e_K)$,资产集 $A=(a_1,a_2,\cdots,a_l)$,威胁集 $T=(t_1,t_2,\cdots,t_m)$,脆弱性集 $U=(u_1,u_2,\cdots,u_n)$。对于信息安全的风险评估问题,可以表述为,对于每种威胁的信息安全风险度的排序。在评估中,采用的信息有:风险发生的损失矩阵$\tilde{\boldsymbol{X}}=[\tilde{x}_{ij}]_{n\times l}$和可能性矩阵$\tilde{\boldsymbol{Y}}=[\tilde{y}_{ij}]_{m\times n}$。其中,$\tilde{x}_{ij}$为第 i 种脆弱性对第 j 种资产的影响程度,即第 i 种脆弱性被利用所造成第 j 种资产的损失,损失程度由 0~10 的数字代表。$\tilde{y}_{ij}$为第 j 种脆弱性被第 i 种威胁利用的可能性,可能性由 0~1 间的数字代表。$\tilde{\boldsymbol{X}}=[\tilde{x}_{ij}]_{n\times l}$和$\tilde{\boldsymbol{Y}}=[\tilde{y}_{ij}]_{m\times n}$均由专家的语言评价项构成。专家对可能性和损失的评价结果都划分为相当低、低、一般低、中等、一般高、高和非常高 7 个等级。

表 1 给出语言变量与三角模糊数之间的对应关系。通过表 1 可以将语言评价项转化为三角模糊数,因此可以依据三角模糊数及其运算性质确定企业的信息安全风险。

3.2 信息安全风险评估矩阵集结

在信息安全风险评估中,为了避免个别专家评价的误差,更有效地集合专家的集体智慧,首先要分别对可能性矩阵和损失矩阵的专家评价值进行集结。

表 1 关于风险可能性程度的语言评价项与三角模糊数的关系

语言评价项	可能性对应三角模糊数	损失对应三角模糊数
相当低	(0,0,0.1)	(0,0,1)
低	(0,0.1,0.3)	(0,1,3)
一般低	(0.1,0.3,0.5)	(1,3,5)
中等	(0.3,0.5,0.7)	(3,5,7)
一般高	(0.5,0.7,0.9)	(5,7,9)
高	(0.7,0.9,1.0)	(7,9,10)
非常高	(0.9,1.0,1.0)	(9,10,10)

以损失矩阵为例,假设专家权重向量为 $\boldsymbol{\omega}^j=(\omega_1^j,\omega_2^j,\cdots,\omega_K^j)$,并且满足 $0\leqslant\omega_k^j\leqslant1(k=1,2,\cdots,K)$,$\sum_k\omega_k^j=1$。为了避免个别专家由于经验不足,或对该方面不熟悉等原因,而形成的干扰项影响,尽可能综合绝大多数专家的意见,提出了如下的集结方法。

首先,计算任两个专家 e_p 和 e_q 对于同一种脆弱性 i 对于同一项资产 j 的损失影响的赋值差距。即计算两个三角模糊数$\tilde{y}_{ij}^p=(\tilde{y}_{ij1}^p,\tilde{y}_{ij2}^p,\tilde{y}_{ij3}^p)$和$\tilde{y}_{ij}^q=(\tilde{y}_{ij1}^q,\tilde{y}_{ij2}^q,\tilde{y}_{ij3}^q)$的距离:

$$d_{ij}(p,q)=\sqrt{\frac{1}{3}(\tilde{y}_{ij1}^p-\tilde{y}_{ij1}^q)^2+(\tilde{y}_{ij2}^p-\tilde{y}_{ij2}^q)^2+(\tilde{y}_{ij3}^p-\tilde{y}_{ij3}^q)^2}\quad(1)$$

然后计算专家 e_k 对于同一种脆弱性 i 对于同一项资产 j 的损失影响的赋值与其他所有专家赋值的平均距离:

$$d_{ij}(k)=\frac{1}{K-1}\sum_{\substack{h=1\\h\neq k}}^{K}d_{ij}(k,h)\quad(2)$$

$d_{ij}(k)$越小,说明专家 e_k 的意见与其他专家意见越一致,$d_{ij}(k)$越大,说明专家 e_k 的意见越偏离其他专家的意见。

然后,将 $d_{ij}(k)$进行规范化:

$$D_{ij}(k)=\frac{d_{ij}(k)}{\max_k d_{ij}(k)}\quad(3)$$

综合考虑决策个体的权威和决策个体意见与群体意见的相近程度,得到集结专家意见的重要性程度:

$$\omega_{ij}(e_k)=\alpha\omega_k^j+(1-\alpha)\cdot(1-D_{ij}(k))\quad(4)$$

其中 α 为权系数,且 $0\leqslant\alpha\leqslant1$。$\alpha$ 的大小反映最终决策者的偏好。α 越大,说明最终决策者更倾向于专家个体的权威,α 越小,说明最终决策者更倾向于整个专家群体的意见。

同理,也可以获得专家关于可能性矩阵的集结权重。

计算信息安全风险,首先要根据这一方法,集结各专家给出的可能性矩阵和损失矩阵。

假定有 K 位专家 $E=(e_1,e_2,\cdots,e_K)$参与信息安全风险评估,记专家 e_k 给出的损失矩阵为$\tilde{\boldsymbol{X}}^k=[\tilde{x}_{ij}^k]_{n\times l}$,可能性矩阵为$\tilde{\boldsymbol{Y}}^k=[\tilde{y}_{ij}^k]_{m\times n}$。根据上述的集结方法,可以将每位专家给出的评估信息分别集结为群的损失矩阵$\tilde{\boldsymbol{X}}=[\tilde{x}_{ij}]_{n\times l}$和群的可能性矩阵$\tilde{\boldsymbol{Y}}=[\tilde{y}_{ij}]_{m\times n}$。其中,

$$\tilde{x}_{ij}=w_{ij}(e_1)\otimes\tilde{x}_{ij}^1\oplus w_{ij}(e_2)\otimes\tilde{x}_{ij}^2\oplus\cdots\oplus w_{ij}(e_K)\otimes\tilde{x}_{ij}^K$$
$$(i=1,2,\cdots,n;j=1,2,\cdots,l)\quad(5)$$

$$\tilde{y}_{ij}=w_{ij}(e_1')\otimes\tilde{y}_{ij}^1\oplus w_{ij}(e_2')\otimes\tilde{y}_{ij}^2\oplus\cdots\oplus w_{ij}(e_K')\otimes\tilde{y}_{ij}^K$$
$$(i=1,2,\cdots,m;j=1,2,\cdots,n)\quad(6)$$

式中,符号“$\otimes$”和“$\oplus$”分别表示模糊数乘法和加法运算。$w_{ij}(e_k)$

和 $w_{ij}(e_k')$分别表示损失矩阵和可能性矩阵的集结权重。

根据三角模糊数的扩展原理，$\tilde{x}_{ij}$和$\tilde{y}_{ij}$仍为三角模糊数，其中，$\tilde{x}_{ij}^k$可用三角模糊数分别表示为$\tilde{x}_{ij}^k=(a_{ij}^k,b_{ij}^k,c_{ij}^k)(i=1,2,\cdots,n;j=1,2,\cdots,l)$，$\tilde{y}_{ij}^k$可用三角模糊数分别表示为$\tilde{y}_{ij}^k=(d_{ij}^k,f_{ij}^k,g_{ij}^k)(i=1,2,\cdots,m;j=1,2,\cdots,n)$。则有

$$a_{ij}=w_{ij}(e_1)\times a_{ij}^1+w_{ij}(e_2)\times a_{ij}^2+\cdots+w_{ij}(e_K)\times a_{ij}^K \quad (i=1,2,\cdots,n;j=1,2,\cdots,l) \tag{7}$$

$$b_{ij}=w_{ij}(e_1)\times b_{ij}^1+w_{ij}(e_2)\times b_{ij}^2+\cdots+w_{ij}(e_K)\times b_{ij}^K \quad (i=1,2,\cdots,n;j=1,2,\cdots,l) \tag{8}$$

$$c_{ij}=w_{ij}(e_1)\times c_{ij}^1+w_{ij}(e_2)\times c_{ij}^2+\cdots+w_{ij}(e_K)\times c_{ij}^K \quad (i=1,2,\cdots,n;j=1,2,\cdots,l) \tag{9}$$

$$d_{ij}=w_{ij}(e_1')\times d_{ij}^1+w_{ij}(e_2')\times d_{ij}^2+\cdots+w_{ij}(e_K')\times d_{ij}^K \quad (i=1,2,\cdots,m;j=1,2,\cdots,n) \tag{10}$$

$$f_{ij}=w_{ij}(e_1')\times f_{ij}^1+w_{ij}(e_2')\times f_{ij}^2+\cdots+w_{ij}(e_K')\times f_{ij}^K \quad (i=1,2,\cdots,m;j=1,2,\cdots,n) \tag{11}$$

$$g_{ij}=w_{ij}(e_1')\times g_{ij}^1+w_{ij}(e_2')\times g_{ij}^2+\cdots+w_{ij}(e_K')\times g_{ij}^K \quad (i=1,2,\cdots,m;j=1,2,\cdots,n) \tag{12}$$

信息安全风险取决于风险发生的可能性与风险发生后的严重程度。

记信息安全风险矩阵为$\tilde{\boldsymbol{R}}=[\tilde{r}_{ij}]_{m\times n}$，$\tilde{r}_{ij}$表示第 i 种威胁给第 j 种资产带来的风险。则

$$\tilde{\boldsymbol{R}}=[\tilde{r}_{ij}]_{m\times n}=[\tilde{y}_{ij}]_{m\times n}\otimes[\tilde{x}_{ij}]_{n\times l} \tag{13}$$

3.3　信息安全威胁等级排序

将风险矩阵$\tilde{\boldsymbol{R}}=[\tilde{r}_{ij}]_{m\times n}$规范化为矩阵$\tilde{\boldsymbol{F}}=[\tilde{f}_{ij}]_{m\times n}$，令$\tilde{r}_{ij}=(a_{ij},b_{ij},c_{ij})$，则

$$\tilde{f}_{ij}=\left(\frac{a_{ij}}{c_*^*},\frac{b_{ij}}{c_*},\frac{c_{ij}}{c_*}\right) \tag{14}$$

其中 $c_j^*=\max_i c_{ij}$。

假设对于风险评估矩阵中每一项威胁 i 构成的风险，其理想解和负理想解分别为 A_i'、A_i''，其中

$$A'=(\tilde{v}_{i1}',\tilde{v}_{i2}',\cdots,\tilde{v}_{in}'),(i=1,2,\cdots,m) \tag{15}$$

$$A''=(\tilde{v}_{i1}'',\tilde{v}_{i2}'',\cdots,\tilde{v}_{in}''),(i=1,2,\cdots,m) \tag{16}$$

理想状态下，希望信息安全风险发生的可能性和产生的损失都为 0，最不希望的是风险值全部达到最大，因此，针对风险规范化矩阵，令

$$\tilde{v}_{ij}'=(0,0,0),(j=1,2,\cdots,n) \tag{17}$$

$$\tilde{v}_{ij}''=(1,1,1),(j=1,2,\cdots,n) \tag{18}$$

威胁 a_i 所带来的风险值与理想解 A'和负理想解 A''的距离 d_i'以及 d_i''可以采用距离公式进行计算：

$$d_i'=\sum_{j=1}^{n}d(\tilde{f}_{ij},\tilde{v}_{ij}'),(i=1,2,\cdots,m) \tag{19}$$

$$d_i''=\sum_{j=1}^{n}d(\tilde{f}_{ij},\tilde{v}_{ij}''),(i=1,2,\cdots,m) \tag{20}$$

其中函数 $d(\cdot,\cdot)$为两个三角模糊数之间的距离。

因此威胁 a_i 所带来的风险与负理想解的贴近度为：

$$cc_i=\frac{d_i'}{d_i'+d_i''} \tag{21}$$

根据威胁与负理想解贴近度的大小可以对威胁进行严重程度排序，与负理想解的贴近度越高，说明风险越大。据此可以开展风险管理，对威胁程度较高的资产采取较多的管理措施。

4　算例

某公司进行信息安全风险评估，为了简化问题的求解，假设组织识别出的资产包括有形资产(a_1)和数据与文档(a_2)两类；识别出的脆弱性为物理保护措施不足(u_1)、对资产的监控不足(u_2)，以及访问控制措施不严格(u_3)三方面；识别出的威胁为非授权访问(t_1)和资产丢失(t_2)。专家 e_1、e_2、e_3 组成的评估小组根据识别出的资产、威胁、脆弱性，分别对风险发生的可能性和风险发生后的损失进行评价。假设 3 个专家的水平相当，他们对可能性和损失的评估意见重要性相同，也就是说

$$w_{ij}(e_k)=\frac{1}{3},i=1,2,3;j=1,2;k=1,2,3$$

$$w_{ij}(e_k')=\frac{1}{3},i=1,2;j=1,2,3;k=1,2,3$$

下面通过表 2 和表 3 分别给出专家对损失矩阵和可能性矩阵的评估情况。

表 2　损失矩阵评价值

脆弱性种类	专家群体					
	专家 1		专家 2		专家 3	
	a_1	a_2	a_1	a_2	a_1	a_2
u_1	高	一般低	非常高	中等	高	一般低
u_2	一般高	中等	中等	一般低	中等	中等
u_3	中等	非常高	中等	非常高	一般低	高

表 3　可能性矩阵评价值

脆弱性种类	专家群体					
	专家 1		专家 2		专家 3	
	t_1	t_2	t_1	t_2	t_1	t_2
u_1	高	一般高	高	一般高	一般高	一般高
u_2	一般高	一般高	中等	中等	中等	高
u_3	高	一般低	非常高	一般低	高	低

利用表 1 将语言评价项转化为三角模糊数，然后利用公式(5)和公式(6)分别对专家的意见进行集结。

集结后的损失矩阵为：

$$\tilde{\boldsymbol{X}}=\begin{bmatrix}(7.67,9.33,10.00) & (1.67,3.67,5.67)\\(3.67,5.67,7.67) & (2.33,4.33,6.33)\\(2.33,4.33,6.33) & (8.33,9.67,10.00)\end{bmatrix}$$

集结后的可能性矩阵为：

$$\tilde{\boldsymbol{Y}}=\begin{bmatrix}(0.63,0.83,0.97) & (0.37,0.57,0.77) & (0.77,0.93,1.00)\\(0.50,0.70,0.90) & (0.50,0.70,0.87) & (0.067,0.23,0.43)\end{bmatrix}$$

因此风险矩阵$\tilde{\boldsymbol{R}}=[\tilde{r}_{ij}]_{m\times n}=[\tilde{y}_{ij}]_{m\times n}\otimes[\tilde{x}_{ij}]_{n\times l}$，为：

$$\tilde{\boldsymbol{R}}=\begin{bmatrix}(7.98,14.69,21.94) & (8.32,14.51,20.37)\\(5.84,11.50,18.39) & (2.57,7.82,14.91)\end{bmatrix}$$

根据公式(14)将$\tilde{\boldsymbol{R}}$规范化，得到矩阵$\tilde{\boldsymbol{F}}$：

$$\tilde{\boldsymbol{F}}=\begin{bmatrix}(0.36,0.67,1.00) & (0.41,0.71,1.00)\\(0.27,0.52,0.84) & (0.13,0.38,0.73)\end{bmatrix}$$

按照公式(17)和公式(18)选取理想解与负理想解，并按照公式(19)和公式(20)计算各被选方案与理想解和负理想解的距离，进而计算各威胁方式与负理想解的贴近度，得到：

$$cc_1=\frac{d_1'}{d_1'+d_1''}=\frac{1.47}{1.47+0.84}=0.64$$

$$cc_2=\frac{d_2'}{d_2'+d_2''}=\frac{1.07}{1.07+1.15}=0.48$$

因此风险的严重程度排序:非授权访问(t_1)>资产丢失(t_2)。

5 结论

利用三角模糊数来建立信息安全风险的可能性矩阵和损失矩阵,然后通过对专家意见的集结,得到信息安全风险矩阵,再通过每种威胁造成的风险与理想解和负理想解的距离比较,对威胁的风险大小进行分析与评判。通过实例可以看出,由于模糊数和集结方法的引用,不但吸收了专家个体意见,而且对各个专家的意见进行了平衡。而且通过对威胁距离公式的构建,为风险的评判提供了有力的依据,使信息安全风险评价结果更加科学合理。该文所给出的基于模糊评价矩阵的信息安全风险群决策评价方法简单、实用,具有一定的工程应用价值。

参考文献:

[1] GB/T 20984—2007 信息安全技术信息安全风险评估规范[S].2007.

[2] Kosko B.Neural networks and fuzzy systems[M].Englewood Cliffs,NJ:Prentice Hall,1992.

[3] 何新贵.模糊知识处理的理论与技术[M].北京:国防工业出版社,1994.

[4] Kacprzyk J.Group decision making with a fuzzy linguistic majority[J].Fuzzy Sets and Systems,1986,18:105-118.

[5] Herrera F,Herrera Viedma E.Linguistic decision analysis:Steps for solving decision problems under linguistic information[J].Fuzzy Sets and Systems,2000,115:67-82.

[6] 徐泽水,达庆利.基于模糊语言评估的多属性决策方法[J].东南大学学报,2002,32(4):656-658.

[7] 徐泽水.不确定多属性决策方法及应用[M].北京:清华大学出版社,2004.

[8] 吴诗辉,杨建军,郭乃林.三角模糊矩阵博弈的最优策略研究[J].系统工程与电子技术,2009,31(5):1231-1234.

[9] Mikhailov L.Group prioritization in the AHP by fuzzy preference programming method[J].Computers & Operations Research,2004,31(2):293-301.

[10] Mikhailov L,Tsvetinov P.Evaluation of services using a fuzzy analytic hierarchy process[J].Applied Soft Computing,2004,5(1):23-33.

[11] Mikhailov L.A fuzzy approach to deriving priorities from interval pairwise comparison judgements[J].European Journal of Operational Research,2004,159(3):687-704.

[12] 张发明,郭亚军.一种基于两阶段协商的群体评价方法[J].系统工程与电子技术,2009,31(7):1647-1650.

[13] 陈岩,樊治平.基于语言判断矩阵的群决策逆判问题研究[J].系统工程学报,2005,20(2):211-215.

[14] Yager R.Uncertainty modeling and decision support[J].Reliability Engineering & System Safety,2004,85(1):341-354.

[15] 徐泽水.基于不同类型残缺判断矩阵的群决策方法[J].控制与决策,2006,21(1):28-33.

[16] 周世忠,朱建军,刘思峰.多元不确定性偏好信息集结的目标规划方法[J].系统工程理论与实践,2008(3):118-124.

[17] Wang Y M,Yang J B,Xu D L.A two stage logarithmic goal programming methods for generating weights from interval comparison matrices[J].Fuzzy Sets and Systems,2005,152(1):475-498.

[18] Zhu J J,Liu S X,Wang M G.Integration of weights model of interval numbers comparison matrix[J].Acta Automatica Sinica,2005,31(3):434-439.

[19] 王奕,费晓洪,蒋蘋.FAHP 方法在信息安全风险评估中的研究[J].计算机工程与科学,2006,32(9):4-12.

[20] 胡伟,李铁克,崔建双.基于模糊层次分析法的信息安全风险评估[J].网络安全技术与应用,2005(6):32-35.

[21] 肖龙,戚湧,李千目.基于 AHP 和模糊综合评判的信息安全风险评估[J].计算机工程与应用,2009,45(22):82-85.

[22] 穆成坡,黄厚宽,田盛丰.基于模糊综合评判的入侵检测报警信息处理[J].计算机研究与发展,2005,42(10):1679-1685.

[23] 杨洋,姚淑珍.一种基于威胁分析的信息安全风险评估方法[J].计算机工程与应用,2009,45(3):94-96.

(上接 16 页)

[5] Perona P,Malik J.Scale space and edge detection using anisotropic diffusion[J].IEEE Trans on Pattern Analysis and Machine Intelligence,1990,12(7):629-639.

[6] Catté F.Image selective smoothing and edge detection by nonlinear diffusion[J].SIAM Journal on Numerical Analysis,1992,29(1):182-193.

[7] Lin Zhou-chen,Shi Qing-yun.An anisotropic diffusion PDE for noise reduction and thin edge preservation[C]//Proc Tenth International Conference on Image Analysis and Processing.Venice:IEEE Computer Society,1999:102-107.

[8] Gilboa G,Sochen N,Zeevi Y Y.Forward-and-backward diffusion processes for adaptive image enhancement and denoising[J].IEEE Trans on Image Processing,2002,11(7):689-703.

[9] 陈虎,周朝辉,王守尊.基于数学形态学的图像去噪方法研究[J].工程图学学报,2004(2):116-119.

[10] 张黄群,于盛林,白银刚.形态学图像去噪中结构元素选取原则[J].数据采集与处理,2008,23(S1):81-83.

[11] Saha P K,Udupa J K,Odhner D.Scale-based fuzzy connected image segmentation:Theory,algorithms,and validation[J].Computer Vision and Image Understanding,2000,77:145-174.

[12] Saha P K,Udupa J K.Scale-based diffusive image filtering preserving boundary sharpness and fine structures[J].IEEE Trans on Medical Imaging,2001,20(11):1140-1155.

[13] Chen K.Adaptive smoothing via contextual and local discontinuities[J].IEEE Trans on Pattern Analysis and Machine Intelligence,2005,27(10):1552-1567.

[14] Canny J.A computational approach to edge detection[J].IEEE Trans on Pattern Analysis and Machine Intelligence,1986,8(6):679-698.