

文章编号: 1000-5013(2009)06-0637-05

一个用于多个实体信任度评估的模糊数学模型

郭玉翠¹, 王励成², 钮心忻²

(1. 北京邮电大学 理学院;
2. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876)

摘要: 以信任度评价指标的可用性、可靠性、完整性、安全防护性、可维护性、以及机密性等 6 个因素为出发点, 建立信任评价指标体系. 在此基础上, 考虑到信任的主观性及主体对客体评价、判断所具有的模糊性, 选用模糊综合评价方法, 建立一种与数字系统信任管理相关的、可用于多个实体信任度评估的数学模型. 对 3 个样本实体的信任状况进行实证研究, 结果可为数字系统的信任管理提供依据.

关键词: 信任管理; 信任度评估; 模糊综合评价; 模糊数学

中图分类号: **文献标识码:** A

网络时代的安全通信、安全商务交易等数字活动的前提是信任. 信任管理是信息安全的一个重要方面, 而信任度评估是实现信任数字化、信任管理自动化、智能化的关键问题. Blaze 等最先提出信任管理概念, 他们以概率作为实体信任度的度量^[1-2], 以主体对客体完成任务的期望为基础, 根据肯定经验和否定经验计算出实体能够完成任务的概率, 并以此概率作为客体信任度的度量, 给出了信任推导规则和信任度的计算方法. J. φsang 等^[3-7] 提出基于主观逻辑的信任度评估模型, 引入了证据空间和观念空间的概念来描述和度量信任关系, 并定义了一组主观逻辑运算符用于信任度的推导和综合计算. Beth 等^[8] 引入了经验的概念来表述和度量信任关系, 并且给出了由经验推荐所引出的信任度推导和综合计算公式. 研究信任的表示和评估模型成果还有不少^[9-11]. 然而, 文^[12]指出, 目前的这些模型都还需要进一步优化, 朝着既能准确刻画客观事实, 又尽量简单实用的方向发展. 值得特别提出的是, 应该着重研究软件可信性度量模型, 可信计算迫切需要这方面的理论支持. 本文在研究数字系统中信任评价指标的基础上, 探讨模糊数学在信任评价中的应用, 构建信任度评估的模糊综合评价模型.

1 数字系统信任度评价指标体系

评价是指为达到一定的目的, 利用特定的指标, 比照统一的标准, 采用规定的方法, 对事物做出价值判断的一种认识活动. 要对数字系统的信任度进行评价, 就必须建立其评价体系, 并以此为标准对所讨论的对象进行比照、评估. 对于数字系统, 其信任度的评价指标主要有可用性、可靠性、完整性、安全防护性、可维护性、以及机密性等 6 个因素, 所建立的信任评价指标体系如表 1 所示.

表 1 数字系统信任评价指标体系

Tab. 1 Trust evaluation index
system of the digital systems

评价指标	指标内容
可用性	系统或实体在当前时刻是可信的
可靠性	系统或实体被证明在一段时间内是可信的
完整性	系统或实体具有良好的运行质量
安全防护性	系统或实体对外来侵袭的抵御能力
可维护性	系统在运行过程中是可以维护的
机密性	文件数据等不为未授权实体所知

2 模糊数学综合评价模型的构建

以评价体系为标准, 选用模糊综合评价方法, 建立了一种与数字系统信任管理相关的、可用于多个实体信任度评估的数学模型. 综合评价是对多种因

收稿日期: 2008-12-23

作者简介: 郭玉翠(1962-), 女, 教授, 主要从事应用数学与信息安全的研. E-mail: yucui_g@163.com.

基金项目: 国家重点基础研究发展计划(973 项目)资助(2007CB310704)

素所影响的事物或现象做出总的评价,即对评判对象的全体,根据所给的条件,给每个对象赋予一个实数,通过总分法或加权平均等计算方法得到综合评分,再据此排序择优.

设进行模糊评价时,所考虑的 m 种因素(或指标)的集合 $U = \{u_1, u_2, \dots, u_m\}$, n 个评语的集合 $V = \{v_1, v_2, \dots, v_n\}$. 它们的元素个数和名称,均可根据实际问题的需要由主体主观规定. 比如在数字系统信任度模型中,评语的集合可取为

$$V = \{\text{完全信任, 倾向信任, 中等信任, 倾向不信任, 完全不信任}\}.$$

当然根据具体情况,评语集 V 也可以有不同的选取. 由于各种因素所处的地位不同,作用也不一样,当然权重也不同,因而评判也就不同. 实体对 n 种评判并不是绝对地肯定或否定,因此综合评价应该是 V 上的一个模糊子集,即 $B = \{b_1, b_2, \dots, b_n\} \quad (V)$. 其中, $b_j (j = 1, 2, \dots, n)$ 反映了第 j 种评判 v_j 在综合评价中所占的地位(即 v_j 对模糊集 B 的隶属度: $B(v_j) = b_j$). 综合评价 B 依赖于各个因素的权重,它应该是 U 上的模糊子集 $A = (a_1, a_2, \dots, a_m) \quad (U)$, 且 $\sum_{i=1}^m a_i = 1$. 其中, a_i 表示第 i 种因素的权重. 因此,一旦给定权重 A ,相应地可得到一个综合评价 B .

若用 $r_{i,j}$ 表示第 i 个元素对第 j 种评语的隶属度,则因素论域与评语论域之间的模糊关系可以用评价矩阵来表示,有

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & \dots & r_{1,n} \\ r_{2,1} & r_{2,2} & & r_{2,n} \\ \dots & & & \dots \\ r_{m,1} & r_{m,2} & \dots & r_{m,n} \end{bmatrix}.$$

式中, $0 \leq r_{i,j} = \mu_R(u_i, v_j) \leq 1, i = 1, 2, \dots, m; j = 1, 2, \dots, n$. A 与 R 的合成就是 B . B 可以看作是评价者综合各种因素后对被评对象作出的最终评价,即模糊综合评判. 于是,模糊综合评判的数学模型为

$$B = A \cdot R = (a_1, a_2, \dots, a_m) \cdot \begin{bmatrix} r_{1,1} & r_{1,2} & \dots & r_{1,n} \\ r_{2,1} & r_{2,2} & & r_{2,n} \\ \dots & & & \dots \\ r_{m,1} & r_{m,2} & \dots & r_{m,n} \end{bmatrix} = (b_1, b_2, \dots, b_n).$$

关于评价矩阵 R 的建立,有如下 2 个命题.

命题 1 设 $X = \{x_1, x_2, \dots, x_m\}$, $Y = \{y_1, y_2, \dots, y_n\}$.

(1) 给定模糊映射,即

$$f: X \rightarrow (Y), x_i \mapsto f(x_i) = B = \frac{r_{i,1}}{y_1} + \frac{r_{i,2}}{y_2} + \dots + \frac{r_{i,n}}{y_n} = (r_{i,1}, r_{i,2}, \dots, r_{i,n}) \quad (Y), \quad i = 1, 2, \dots, n$$

以 $(r_{i,1}, r_{i,2}, \dots, r_{i,n}) (i = 1, 2, \dots, n)$ 为行构造一个模糊矩阵,就可以唯一确定模糊关系为

$$R_f = \begin{bmatrix} r_{1,1} & r_{1,2} & \dots & r_{1,n} \\ r_{2,1} & r_{2,2} & & r_{2,n} \\ \dots & & & \dots \\ r_{n,1} & r_{n,2} & \dots & r_{n,n} \end{bmatrix}.$$

其中, $R_f(x_i, y_i) = r_{i,j} = f(x_i)(y_i)$.

(2) 给出模糊关系,有

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & \dots & r_{1,m} \\ r_{2,1} & r_{2,2} & & r_{2,m} \\ \dots & & & \dots \\ r_{n,1} & r_{n,2} & \dots & r_{n,m} \end{bmatrix}.$$

可令 $f_R: X \rightarrow (Y), x_i \mapsto f_R(x_i) = (r_{i,1}, r_{i,2}, \dots, r_{i,m}) \quad (Y)$, 其中 $f_R(x_i)(y_i) = r_{i,j} = R_f(x_i, y_i)$, $(i = 1, 2, \dots, n, j = 1, 2, \dots, m)$; f_R 是 X 到 Y 的模糊映射. 于是,也就确定了模糊映射 f_R .

命题 2 设 $X = \{x_1, x_2, \dots, x_n\}$, $Y = \{y_1, y_2, \dots, y_m\}$.

(1) 给定模糊关系,有

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & \dots & r_{1,m} \\ r_{2,1} & r_{2,2} & & r_{2,m} \\ \dots & & & \dots \\ r_{n,1} & r_{n,2} & \dots & r_{n,m} \end{bmatrix}, \quad A = (a_1, a_2, \dots, a_n) \quad (X).$$

这可以确定一个模糊线性变换,即

$$T_R \quad (X) \quad (Y), \\ A / \quad T_R(A) = A \cdot R = B = (b_1, b_2, \dots, b_m) \quad (Y).$$

其中, $b_j = \sum_{i=1}^n a_i \cdot r_{i,j} (j=1,2,\dots,m)$,称 T_R 是由模糊关系 R 诱导出的.

(2) 若给定了模糊线性变换 $T_R \quad T_R = A \cdot R$,并给定了 m ,则由模糊关系方程可以确定模糊矩阵 R ,从而也确定了模糊关系 R .

根据命题 1 和命题 2,需要建立一个从 U 到 U 的模糊变换 T .如果对每一个因素 u_i 单独作一个评判 $f(u_i)$,可以看作是 U 到 V 的模糊变换 f ,即 $f \quad U \quad (V) \quad u_i | \quad f(u_i) \quad (V)$.由 f 可诱导出一个 U 到 V 的模糊线性变换 T_f ,并把 T_f 看作为由权重 A 得到的综合评价 B 的数学模型.

3 实例分析

(1) 信任管理评价矩阵的建立. 根据分析可知,对实体的信任度进行评估,需要从系统或实体的可用性、可靠性、完整性、安全防护性、可维护性和机密性 6 个方面着手. 由此,组成数字系统信任管理因素集合 $U = \{u_1, u_2, \dots, u_6\}$. 将一个系统或实体的可信水平分为完全可信、倾向可信、中等可信、倾向不可信和完全不可信五等,并由此构成评语集合为

$$V = \{ \text{完全可信, 倾向可信, 中等可信, 倾向不可信, 完全不可信} \} = \{v_1, v_2, \dots, v_5\}.$$

设 $R = \{r_{i,j}, (i=1,2,\dots,5; j=1,2,\dots,6)$ 是从 V 到 U 的模糊关系,即是一个模糊子集, $r_{i,j}$ 表示被评对象第 i 种评语在第 j 个因素达到的可能程度. 现在假设选取 3 个实体作为评价对象(D), 另外有 30 个实体保持对这 3 个待评实体信任评价指标的 6 个方面的记录(即评价). 从记录上可知,待评实体 d_1 的评价结果:6 个实体的记录为完全可信,7 个实体的记录为倾向可信,14 个实体的记录为中等可信,3 个实体的记录为倾向不可信和 0 个实体的记录为完全不可信.

综合 30 个实体对待评实体 d_1 的 u_1 的评价向量为(0.20,0.23,0.47,0.10,0.00). 同理,可得到 30 个实体对实体 d_1 的 u_2, u_3, u_4, u_5 等 u_6 各个因素的评价向量分别为(0.07,0.10,0.37,0.30,0.17), (0.20,0.37,0.17,0.17,0.10), (0.37,0.43,0.13,0.00,0.07), (0.20,0.47,0.17,0.10,0.07)和(0.03,0.00,0.23,0.60,0.13). 于是得到对实体 d_1 的信任水平的评价矩阵为

$$R_1 = \begin{bmatrix} 0.20 & 0.07 & 0.20 & 0.37 & 0.20 & 0.03 \\ 0.23 & 0.10 & 0.37 & 0.43 & 0.47 & 0.00 \\ 0.47 & 0.37 & 0.17 & 0.13 & 0.17 & 0.23 \\ 0.10 & 0.30 & 0.17 & 0.00 & 0.10 & 0.60 \\ 0.00 & 0.17 & 0.10 & .07 & 0.07 & 0.13 \end{bmatrix}.$$

采用同样的数据处理方法,可得到对实体 d_2 和实体 d_3 的信任水平的评价矩阵分别为

$$R_2 = \begin{bmatrix} 0.03 & 0.50 & 0.67 & 0.30 & 0.40 & 0.07 \\ 0.10 & 0.27 & 0.20 & 0.40 & 0.37 & 0.37 \\ 0.47 & 0.13 & 0.03 & 0.17 & 0.00 & 0.40 \\ 0.20 & 0.10 & 0.07 & 0.07 & 0.17 & 0.07 \\ 0.20 & 0.00 & 0.03 & 0.07 & 0.07 & 0.10 \end{bmatrix}, \\ R_3 = \begin{bmatrix} 0.00 & 0.03 & 0.00 & 0.30 & 0.10 & 0.07 \\ 0.07 & 0.20 & 0.20 & 0.30 & 0.17 & 0.07 \\ 0.23 & 0.17 & 0.63 & 0.27 & 0.67 & 0.20 \\ 0.17 & 0.57 & 0.13 & 0.07 & 0.03 & 0.57 \\ 0.53 & 0.03 & 0.03 & 0.07 & 0.03 & 0.10 \end{bmatrix}.$$

(2) 作模糊线性变换 T_R . 将评价集中的完全可信、倾向可信、中等可信、倾向不可信和完全不可信分别赋予数值 5,4,3,2 和 1,则评价集中各等级的权重分别是 0.33,0.27,0.20,0.13,0.07. 由此可得到权重向量为

$$A = [a_1, a_2, a_3, a_4, a_5, a_6] = [0.33, 0.27, 0.20, 0.13, 0.07].$$

由模糊评价矩阵得到模糊线性变换 T_R ,对实体在 d_1 来说,则有

$$B_1 = A \circ R_1 = [0.24, 0.17, 0.23, 0.27, 0.24, 0.15].$$

采用相同的处理方法,可得到对实体 d_2 和 d_3 的信任管理评价分别为

$$B_2 = [0.17, 0.28, 0.29, 0.25, 0.26, 0.22],$$

$$B_3 = [0.12, 0.18, 0.20, 0.25, 0.22, 0.16].$$

从而可得到 3 个样本实体模糊线性变换的集合 B .

(3) 信任评价指标权重的频数统计. 信任评价的 6 个指标内容组成因素集 $U = \{u_1, u_2, \dots, u_n\}$. 现在组织 50 个用户,根据权重分配对每个因素 $u_j (j = 1, 2, \dots, 6)$ 进行单项因素的权重统计试验.

() 对于因素 $u_i (i = 1, 2, \dots, n)$,在它的权重 $w_{i,j} (j = 1, 2, \dots, 50)$ 中找出最大值 M_i 和最小值 m_i ,即 $M_i = \max\{w_{i,j}\}; m_i = \min\{w_{i,j}\} j = 1, 2, \dots, 50$.

() 选取整数 $P = 5$,利用公式 $(M_i - m_i) / P$ 计算出对权重分组的组距,并将其分成 5 组.

() 计算落在各组内权重的频数与频率.

() 根据频数与频率的分布情况,将最大频率所在分组的值作为因素 u_i 的权重 $w_i (i = 1, 2, \dots, 6)$,从而得到权重向量 $w = (w_1, w_2, \dots, w_6)$. 按照这种处理方式得到数字系统评价集中各因素的权重,可用性、可靠性、完整性、安全防护性、可维护性和机密性 6 个指标的权重(权重数据是标准化并经近似的结果)分别为 0.25,0.10,0.20,0.10,0.20,0.15.

(4) 信任度的模糊综合评价计分. 确定了数字系统影响信任的各因素的权重,便可得到 3 个样本实体 D 的模糊综合评价计分向量为

$$W = w \circ B = [0.22, 0.24, 0.185].$$

即 $w_1 = 0.22, w_2 = 0.24, w_3 = 0.18$,因而 3 个样本实体的信任水平高低顺序为 d_2, d_1, d_3 . 3 个实体的各信任指标单项得分的计算过程为

$$P = B^T \cdot \text{diag}(w) = \begin{bmatrix} 0.24 & 0.17 & 0.23 & 0.27 & 0.24 & 0.15 \\ 0.17 & 0.28 & 0.29 & 0.25 & 0.26 & 0.22 \\ 0.12 & 0.18 & 0.20 & 0.25 & 0.22 & 0.16 \end{bmatrix} \cdot \begin{bmatrix} 0.25 & & & & & \\ & 0.10 & & & & \\ & & 0.20 & & & \\ & & & 0.10 & & \\ & & & & 0.20 & \\ & & & & & 0.15 \end{bmatrix} = \begin{bmatrix} 0.06 & 0.02 & 0.05 & 0.03 & 0.05 & 0.02 \\ 0.04 & 0.03 & 0.06 & 0.03 & 0.05 & 0.03 \\ 0.03 & 0.02 & 0.04 & 0.02 & 0.04 & 0.02 \end{bmatrix}.$$

样本实体信任各指标单项得分计算结果,如表 2 所示. 通过表 2 可以看出,实体 d_3 对评价因素各指标都处于最低水平,因而是信任度最差的;实体 d_2 虽然可用性方面低于实体 d_1 的分值为 0.02,但在可靠性、完整性、和机密性方面都优于实体 d_1 ,而在安全防护和可维护性方面与实体 d_1 持平,从而信任度是最好的.

4 结 束 语

应用模糊数学的模糊综合评判模型,能较好地解决了熟悉系统中实体的信任评价问题,对多个实体的信任水平

表 2 样本实体信任指标单项结果
Tab.2 Index trust the results of physical samples of the individual

因素	w_i	d_1	d_2	d_3
u_1	0.25	0.06	0.04	0.03
u_2	0.10	0.02	0.03	0.02
u_3	0.20	0.05	0.06	0.04
u_4	0.10	0.03	0.03	0.02
u_5	0.20	0.05	0.05	0.04
u_6	0.15	0.02	0.03	0.02
合计	1.00	0.22	0.24	0.18



进行高低排序,为数字系统的信任管理提供依据.应用模糊集合和模糊规则进行推理,能够表达过渡性界限或定性的知识和经验,特别适用于精确数学难于表示的不确定系统.

参考文献:

- [1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]. Proceedings of the 1996 IEEE Symposium on Security and Privacy. New York: IEEE Computer Society Press, 1996: 164-173.
- [2] BLAZE M, FEIGENBAUM J, IOANNIDIS J, et al. RFC 2704: The KeyNote Trust Management System Version 2 [EB/OL]. [2005-02-16]. http://www.cnpa.gov.net/Class/Rfcen/200502/3756_2.html.
- [3] J ØSANG A, KNAPSKOG S J. A metric for trusted systems: Global IT security[M]. Wien: Austrian Computer Society, 1998: 541-549.
- [4] J ØSANG A. Trust-based decision making for electronic transactions[C]. YNGSTROM L, et al. Proc of the 4th Nordic Workshop on Secure Computer Systems. Kista: Stockholm University Press, 1999: 1-21.
- [5] J ØSANG A. The right type of trust for distributed systems[C]. Meadows C. Proceedings of the New Security Paradigms Workshop. Lake Arrowhead: ACM Press, 1996: 119-132.
- [6] J ØSANG A. A model for trust in security systems[C]. Proceedings of 2nd Nordic Workshop on Secure Computer System Systems. Philadelphia: ACM Press, 1997.
- [7] J ØSANG A. A subjective metric of authentication[C]. Quisquater J. Proceedings of the ESORICE '98. Brighton: Springer-Verlag, 1998: 329-344.
- [8] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]. Gellman D. Proceedings of European Symposium on Research in Security. Brighton: Springer-Verlag, 1994: 3-18.
- [9] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型[J]. 软件学报, 2003, 14(8): 1401-1408.
- [10] 袁禄来, 曾国荪, 王伟. 基于 Dempster-Shafer 证据理论的信任度评估模型[J]. 武汉大学学报: 理学版, 2006, 52(5): 627-630.
- [11] 张艳群, 张辰. 基于模糊理论的信任度评估模型[J]. 计算机工程与设计, 2007, 28(3): 532-534.
- [12] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学(E辑): 信息科学, 2007, 37(2): 129-150.

A Fuzzy Mathematical Model for Trust Evaluation to More Entities

GUO Yu-cui¹, WANG Li-cheng², NIU Xin-xin²

(1. School of Science, Beijing University of Posts and Telecommunications;

2. State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract: Taking six factors, such as availability, reliability, integrity, safety, maintainability and confidentiality as the starting point of trust evaluation index, a trust assessment index system is built up. Base on this and considering the subjectivity of trust and fuzziness of opinion and estimation for subject to object, a fuzzy synthetic evaluation method is selected and a mathematical model associated trust management of digital system and used in more entities is established. The process of evaluation using the model is demonstrated for three examples. The result of evaluation can provide gist for trust management of digital systems.

Keywords: trust management; trust evaluation; fuzzy synthetic evaluation; fuzzy mathematics

(责任编辑: 黄仲一 英文审校: 吴逢铁)