

# 普适环境中基于模糊理论的信任评估模型

王 琴, 郭亚军, 徐 芬

WANG Qin, GUO Ya-Jun, XU Fen

华中师范大学 计算机科学系, 武汉 430079

Department of Computer Science, Central China Normal University, Wuhan 430079, China

E-mail: wqjx@163.com

WANG Qin, GUO Ya-Jun, XU Fen. Fuzzy logic-based trust evaluation model in pervasive computing environment. Computer Engineering and Applications, 2008, 44 (3): 170-172.

**Abstract:** In pervasive computing environment, trust management have become a cornerstone for information security. For study the fuzziness of subject trust and the dynamics of trust relationships between various subjects, the paper presents a model to evaluate user's trustworthiness based on fuzzy theory of fuzzy mathematics. This model introduces the fuzzy theory to the fuzziness and dynamics of trust relationships, and evaluates the factors which affect the trust subject, then gains a total trustworthiness to make sure that whether it may trust the subject for alternation. The model can evaluate the user's trustworthiness completely, security and reliability of pervasive behavior can be guaranteed greatly, and provides a new method to handle uncertainty in trust management for pervasive computing.

**Key words:** trust management; fuzzy theory; trustworthiness evaluation; fuzzy integration evaluation

**摘 要:** 信任管理是当前普适环境中信息安全研究的热点。为了解决主观信任的模糊性和主体之间信任关系的动态性,在模糊数学中的模糊理论的基础上,提出了一个用户信任度的评估模型。该模型是将模糊理论应用到信任关系的不确定性和动态性上,对影响信任主体的主要因素进行综合评估,得出一个总的信任度来确定是否可以信任主体以便进行交互。该模型可以全面地评估用户的信任度,很大程度上保证了普适行为的安全可靠,为处理普适计算的信任管理的不确定研究提供了一个新的方法。

**关键词:** 信任管理; 模糊理论; 信任度评估; 模糊综合评估

文章编号: 1002-8331(2008)03-0170-03 文献标识码: A 中图分类号: TP301

## 1 引言

普适计算是信息空间与物理空间的融合,在这个融合的空间中人们可以随时地、透明的获得数字的服务。普适计算以人的需求为中心,从根本上改变了人去适应机器计算的被动式服务思想,而是用户在不被打扰的前提下主动、动态的接受网络服务。它在服务方式和灵活性上的突破是普适计算模式成为信息时代中计算模式的又一个里程碑。

普适计算具有相当广阔的应用前景,但是前提条件是网络的安全问题得到较好的解决,在以无线接入技术为主的普适计算网络中,传统的安全模式已经不能够满足普适计算的安全要求。要实现和推广普适计算网络,安全问题是一定要妥善彻底的解决。虽然目前的安全机制相对于传统的而言有了一些改进,但仍然无法从根本上解决问题。在一个大的应用系统中,用户向系统的授权者提出服务请求,但都无法直接信任用户,因此他必须使用由熟知用户的第三方所提供的信息(通常授权者只在某种程度上相信第三方提供的某类信息)。这种信任和委托关系使得网络中的授权不同于传统的访问控制。信任管理方法正是为了解决上述问题而提出的一种访问控制机制。

信任一般地表达了关于人或所提供服务的诚实、可信、能力、可靠性等的信仰。X.509v4 中对信任的定义:“一般来说,如果一个实体假定另一个实体会严格地按照它所期望的那样行动,那么就称它信任那个实体。”信任是信任者对被信任者的一种预期,这种预期可以具有不同的程度,我们用信任度来衡量这种可信任程度,信任可以从完全不信任到完全信任。信任可划分为直接信任和推荐信任。两个实体之间根据直接经验和讨论的信任而直接建立起来的信任关系称为直接信任。推荐信任是指两个实体以前没有建立起信任关系,但根据可信的第三方或一系列可信的第三方而建立起来的一种信任关系或潜在的信任关系。

信任是非理性的,是一种经验的体现,不仅要有具体的内容,还应有序度的划分, Beth 等人的 BBK 信任度评估模型<sup>[1,2]</sup>和 J. sang 模型<sup>[3]</sup>等都是基于此观点的信任度评估模型。BBK 信任模型用经验的概念表示信任,但该模型的直接信任关系仅建立在没有否定经验的实体之间,过于严格。J. sang 模型一个基于主观逻辑的信任模型,在对经验的评价中引入了不确定因素,其实质是利用了证据理论,它认为信任的主观性和不确定性与

基金项目: 湖北省自然科学基金 the Natural Science Foundation of Hubei Province of China under Grant No.2005ABA243; 中国博士后基金 (China Postdoctoral Science Foundation No.20070410953)。

作者简介: 王琴 (1982-), 女, 硕士研究生, 主要研究领域为信息安全、普适计算; 郭亚军 (1965-), 男, 博士, 副教授, 主要研究领域为计算机安全与保密、普适计算; 徐芬 (1982-), 女, 硕士研究生, 主要研究领域为信息安全、普适计算。

随机性是等同的,但主观信任作为一种认知现象,其主观性和不确定性主要表现为模糊性,而对主观信任进行形式化研究的主要困难也在于如何对这种模糊性进行建模。

由于信任的模糊性的存在,普适计算中的信任关系是很难被评估的。如果一个信任关系依靠一个基于模糊信息的主观判断,它将会是很不确定的,并且任何和那种信任关系有关的操作都会导致不可预料的结果。所以,为了操纵一系列信任相关的活动,灵活性在信任策略的执行中是必不可少的。例如,如果不能找到一个匹配策略,那么就不能简单地否定一个交叉领域的访问需求。当发现了某个要求的目的后,可能会发现它在另外一个不同的格式或几个策略的联合上符合另外一个策略。这就将模糊性引入到信任管理中,因为这个要求的目的可能是不太明确的,或者该要求本身就是模糊的,或者这个将实施的策略可能是模糊的。将模糊逻辑应用到信任管理中能够帮助我们在普适计算中处理不确定性。

## 2 基于模糊理论的信任评估模型

1965年美国加州大学伯克利分校电气工程系的 Zadeh 教授创立了模糊集合理论<sup>[4]</sup>,在此基础上发展起模糊理论,模糊逻辑则是模糊理论体系的一部分。模糊逻辑是解决人工智能的重要途径之一,它通过引入模糊隶属度函数、模糊关系以及模糊推理规则等概念,可以处理现实世界中大量不确定的信息<sup>[5-8]</sup>。模糊逻辑理论拓展了数学研究成为一个合成物的存在性,它平衡着质量和数量,这包含着一定的模糊性。

所谓信任度是指对某个实体的行为和性能能否达到所期望值的可靠性。这个值是由很多因素决定的动态值,范围可从“完全不信任”到“完全信任”。直接信任是指2个实体间根据以往的直接交往行为得出的信任等级关系。实体的声誉是指其他实体通过观察其过去行为并根据其表现而得出的综合期望值。在进行信任决策时,当2个实体间没有直接交往接触时,可借助对方的声誉(间接信任)抉择。当实体间长期没有直接或间接信任接触时,其信任关系会随时间而衰减。

信任度评估模型主要涉及以下问题:(1)信任的表述和度量;(2)由经验推荐所引起的信任度推导和综合计算。但并非只是解决了以上问题后就可以得到一个好的信任度评估模型,在这个的基础上仍存在着一些问题需要解决:(1)用户之间的信任度仅用信任、不信任、不确定来刻画,若两用户的100次交易中仅有一次失信,那么评价应是完全信任、完全不信任还是不确定呢?信任度59与60差别在哪里呢?(2)不同用户的信用评价往往没有一个可供衡量比较的具体标准。综上所述,信任度具有模糊性和不确定性。

综合评估是对受到多个因素制约的对象作出总评价。对一个主体的评估最终是对它的信任度评估,计算某一主体的信任度,由于从多个方面评价,难免带有模糊性和主观性,因此采用模糊数学方法综合评估将使结果尽量客观、真实。所以,本文将模糊逻辑引入到信任管理的研究中,提出了基于模糊理论的综合信任评估模型,设法解决信任管理中的与不确定性相关的问题。

### 2.1 信任向量描述

信任管理中所有与信任相关的信息的来源,或者用信任关系建立的实体,用集合 $X=\{x_1, x_2, \dots, x_n\}$ 来表示,其中 $x_i(i=1, 2, \dots, n)$ 表示开放网络环境中的主体<sup>[9]</sup>。

定义1 设论域为非空集合 $X$ ,对于任意的 $x \in X$ 给定了如下映射: $X \rightarrow [0, 1], x \mapsto \mu_A(x) \in [0, 1]$ 则称由序偶组成的集合 $A=\{x|\mu_A(x)\}$ 为模糊集合,称 $\mu_A(x)$ 为 $x$ 对 $A$ 的隶属函数(表示为 $A(x)$ )。对某个具体的 $x$ 而言,称 $\mu_A(x)$ 为 $x$ 对 $A$ 的隶属度。

定义2  $X$ 中所有的模糊集的集合将被表示为 $\Phi(X)$ 。然后用多个模糊子集合 $T_j \in \Phi(X) (j=1, 2, \dots, m)$ 定义具有不同信任度的信任集合,即用离散的标度 $j(j=1, 2, \dots, m)$ 来描述主体信任的高低。

在实际环境中,决定各主体之间的信任关系时很难明确地判断某个主体究竟是属于哪一个信任的子集合。按照模糊集合理论的思想,某个主体对某个信任的子集合 $T_j$ 不能简单地用“是”或“否”来描述,即各主体与信任集合 $T_j$ 之间并不是“非此即彼”的关系,应该说还包含有“亦此亦彼”的模糊关系。因此,可以使用主体 $x_i(i=1, 2, \dots, n)$ 对各个 $T_j(j=1, 2, \dots, m)$ 的隶属度 $\mu_{ij}=\mu_{T_j}(x_i)$ 所构成的向量来描述主体的信任度,这才更加符合主体信任的实际情况。

定义3 设 $T_j \in \Phi(X) (j=1, 2, \dots, m)$ 为具有不同信任度的子集合,主体 $x_i(i=1, 2, \dots, n)$ 为 $X$ 中的元素,把 $x_i$ 对各个 $T_j$ 的隶属度 $\mu_{ij}$ 所构成的向量称为信任向量(信任度)。

在实际应用中,描述各主体的属性或特征时,可以用有限个模糊参数来刻画各主体。这里所刻画的属性或特征相当于主体对某个模糊参数的隶属度。比如在信任域中,可以根据主体的历史信誉度,社会身份,社会地位等参数来刻画各主体的属性或特征。那么,用这有限个模糊参数 $T_j(j=1, 2, \dots, m)$ 来刻画各主体的属性或特征值所构成的向量 $\Psi(x_i) \in \{\mu_{i1}, \mu_{i2}, \dots, \mu_{im}\}$ 作为主体 $x_i(i=1, 2, \dots, n)$ 的信任向量。

由于隶属度的客观存在性,主体 $x_i$ 对各个 $T_j$ 的隶属度也可以通过以下两种途径获得:一种是采用模糊综合评估的方法,对信任关系进行评价和综合计算,计算出主体 $x_i$ 的信任向量;二是通过对其它主体所提供的关于 $x_i$ 的信任信息(比如其他主体提供的关于 $x_i$ 的直接信任和推荐信任的有关信息)进行分析,推导出 $x_i$ 的信任向量。这样,借助于模糊集合理论,把各主体关于各信任类型的信任关系用信任向量来表示,比较客观地反映了主观信任地实际情况。各主体的信任向量是开放式网络中其他主体对该主体建立信任的依据,因此主体信任向量的确定是模糊信任模型需解决的关键问题之一。

### 2.2 信任度的评估模型

在开放式网络环境中,各主体的信任度是由多方面的因素决定的,因而在确定各主体的信任向量时必须考虑多方面的因素。但由于主体间的信任具有模糊性,在研究的各问题域中也蕴藏着很难准确描述的决策,因而对各主体信任的综合评估同样也具有模糊性。在模糊理论中,模糊综合评估是一种受多种因素影响的评估决策,并以此作出全面评价的一种十分有效的多因素决策方法。

综合评估是对受到多个因素制约的对象作出总评价。由于从多个方面评价,难免带有模糊性主观性,因此采用模糊综合评估将其结果尽量客观、真实。

设因素集为 $U=\{u_1, u_2, \dots, u_n\}$ ,评估集为 $E=\{e_1, e_2, \dots, e_m\}$ ,评估集所对应的等级量化值为 $Y=\{Y_1, Y_2, \dots, Y_m\}$ ,因素评估矩阵 $R=(r_{ij})_{n \times m}$ ,对于给定的因素集的权重为 $W=\{w_1, w_2, \dots, w_n\}$   
 $Q(U), \sum_{i=1}^n w_i=1$ ,综合评估为 $V=W \cdot R$ ,则称 $(U, E, R)$ 构成一个

模糊综合评估模型, U、E、R、W 是此模型的四个要素。其中,“。”

为模糊变换运算符,其运算过程为  $v_j = \bigvee_{i=1}^n (w_i \wedge r_{ij})$  ( $j=1, 2, \dots, m$ ), 和  $\bigwedge$  为 Zadeh 算子 (分别表示 max 和 min 运算); 因素集 U 为构成信任类型的所有属性; 评价集是描述对某个主体所作的不同等级的评估, 评价的等级为 m 级 (与信任集合的等级相对应); W 为各因素的权重分配集, 表示各因素在综合评估中的相对重要性; 因素评估矩阵 R 表示对各因素作出各种评价的可能性 (比如  $r_{ij}$  表示对  $u_i$  作出  $e_j$  评价的可能性)。

设  $f: U \rightarrow V, u_i \mapsto f(u_i) = \{r_{i1}, r_{i2}, \dots, r_{in}\} \subseteq V, i=1, 2, \dots, n$ , 则称由模糊映射  $f$  得到的矩阵  $R = (r_{ij})_{n \times m}$  为因素评估矩阵, 即  $R = (f(u_i))_{n \times m} = (r_{ij})_{n \times m}, i=1, 2, \dots, n, j=1, 2, \dots, m$ 。

以上定义说明, 在评估过程中, 只需根据主体的具体情况确定属性的特征值, 就可以根据属性的特征函数计算出对属性的各种评估的可能性, 从而构造出因素评估矩阵 R。

通过上述模糊综合评估, 就可以得到主体的信任向量:

$$V = \{v_1, v_2, \dots, v_m\} = \{w_1, w_2, \dots, w_n\} \circ R$$

模糊综合评估模型是一个从到的模糊变换, 即由各因素的权重分配集 W 与因素评估矩阵 R 进行模糊运算。“得到各主体的信任向量。

得出主体的综合评估值 (信任向量/信任度) 之后, 使用评估集中各评估值  $Y = \{Y_1, Y_2, \dots, Y_n\}$  所对应的等级量化值对主体的评估结果进行量化处理  $w = \bigvee_{i=1}^n (Y_i \wedge v_i)$ , 最后得出最终评估结果的量化值。如果该值大于某个预定的值就认为是可信的, 否则认为是不可信的。这样就可以从对信任的模糊性转换到确定性, 从而能更好的进行正常的交互。

3 实例分析

根据以上所建模型, 下面将用一个详细的例子来进行说明分析, 本文通过计算主体的综合信任度来确定主体是否值得信任, 而信任度的确定与用户对主体的历史信誉、服务能力、入侵抵抗能力、自身个性、社会背景的不同要求相关, 因此用以上的 5 个要素作为因素参数进行分析。

(1) 建立评估对象因素集  $U = \{u_1, u_2, \dots, u_5\}$ , 权重分配为  $W = (0.4, 0.2, 0.1, 0.2, 0.1)$ 。在本方案中, 确定权重分配是项关键工作, 可以根据不同类型的应用确定。

(2) 建立评估集为  $E = \{e_1, e_2, \dots, e_6\} = \{\text{完全信任, 非常信任, 很信任, 一般信任, 有点信任, 不信任}\}$ , 其等级量化值为  $Y = \{Y_1, Y_2, \dots, Y_6\} = \{1.0, 0.8, 0.6, 0.4, 0.2, 0.0\}$ 。

(3) 建立因素评估: 假设对此主体进行的 100 次评估中, 各因素在各个等级的分布如表 1 所示。则评价矩阵为:

$$R = \begin{bmatrix} 0.6 & 0.1 & 0.2 & 0.1 & 0 & 0 \\ 0.5 & 0.3 & 0.1 & 0.05 & 0.05 & 0 \\ 0.4 & 0.2 & 0.1 & 0.1 & 0.1 & 0.1 \\ 0.5 & 0.2 & 0.1 & 0.1 & 0.05 & 0.05 \\ 0.4 & 0.4 & 0.05 & 0.1 & 0.05 & 0 \end{bmatrix}$$

表 1 等级分布

因素	信任等级					
	完全信任	非常信任	很信任	一般信任	有点信任	不信任
历史信誉	60	10	20	10	0	0
服务能力	50	30	10	5	5	0
入侵抵抗能力	40	20	10	10	10	10
自身个性	50	20	10	10	5	5
社会背景	40	40	5	10	5	0

(4) 综合评估:

$$V = W \circ R = \{v_1, v_2, \dots, v_6\} = \{0.52, 0.2, 0.135, 0.09, 0.035, 0.02\}$$

(5) 用等级量化值  $Y = \{Y_1, Y_2, \dots, Y_n\}$  对主体的评估结果进行量化处理后得出最终结果的量化值。如果该值大于某个预定的值 (在此处假定为 0.6) 就认为是可信的, 否则认为是不可信的。

根据上面输入的等级量化值  $Y = \{Y_1, Y_2, \dots, Y_6\} = \{1.0, 0.8, 0.6, 0.4, 0.2, 0.0\}$  可知, 该主体的最终评估结果为:  $w = \bigvee_{i=1}^6 (Y_i \wedge v_i) = 0.804$ , 即认为该结果是可信的。

4 结论

普适计算被视为未来网络应用的主流。模糊评估是一种综合评估, 是将多人的意见通过合适的算法综合考虑得到一种模糊性的评估结论。本文中所建立的信任评估模型很好解决了普适计算中对主体信任如何获得的问题。本文所提出的信任模型可以作为一种直观而有效的评价工具, 为普适计算环境中的主体信任决策提供有效支持, 很大程度上保障了网络的安全可靠性。(收稿日期: 2007 年 6 月)

参考文献:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management[C]// Dale J, Dindot G. Proc of the 17th Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 164-173.

[2] Beth T, Borcherding M, Klein B. Valuation of trust in open networks[C]// Proc 1994 the European Symposium on Research in Security. Berlin: Springer-Verlag, 1994: 3-18.

[3] Josang A. A logic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 2001, 9 (3): 279-311.

[4] 扎德 L. A. 模糊集合、语言变量及模糊逻辑[M]. 陈国权, 译. 北京: 科学出版社, 1982.

[5] 丁卫平, 顾卫江. 模糊逻辑推理在电子病历智能辅助诊断系统中的应用研究[J]. 南通大学学报: 自然科学版, 2006, 12 (4): 77-81.

[6] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14 (14): 1401-1408.

[7] 李仁发, 钟少宏. 基于信任普适计算环境下的信任模型[J]. 科学技术与工程, 2005, 5 (8): 476-480.

[8] 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): 532-533.