面向分布式系统访问控制的信任度量化模型

郎波

（北京航空航天大学 软件开发环境国家重点实验室，北京 100083）

摘 要：通过引入社会学中信任的研究成果，定义了分布式系统访问控制中信任的具体语义、基本特性与上下文相关属性。针对信任的主观性、模糊性与不确定性，采用模糊数学与概率论相结合的方法，给出了信任的数学定义，建立了包括信任综合评价与信任计算的信任度量化模型。该模型综合了访问控制背景下信任相关的各种因素，符合推荐信任的衰减与增强规律。

关键词：访问控制；信任量化表达；信任计算；分布式系统

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2010)12-0045-10

Access control oriented quantified trust degree representation model for distributed systems

LANG Bo

(State Key Lab of Software Development Environment, Beijng University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Based on the research fruit of social trust in sociology, the semantics, properties and elements of trust in the context of access control of distributed systems were defined. By combining fuzzy set theory with probability theory, a mathematical definition of trust was given, a quantified trust degree representation model including an integrated trust evaluation model and a trust calculating algorithm was established. The model integrates multiple elements of trust, and is in accordance with the decreasing and enhancing rules of the recommended trust.

Key words: access control; trust quantificational expression; trust calculating; distributed system

1 引言

基于 Internet 的 P2P 系统强调节点对等、节点自治，具有可扩展性强、动态性强的特点，已经成为一种重要的计算模式。由于缺乏集中的管理和控制，P2P 系统中很容易混入恶意节点。为了对 P2P 系统中敏感信息进行保护，防止恶意节点的攻击，需要对系统中的资源进行细粒度的访问控制。而 P2P 应用中，用户之间常常是陌生的，因此一个节点无法对所有用户的标识以及权限进行预先定义。现有成熟的访问控制模型如 RBAC、DAC 等是基于标识的、封闭式的，即访问控制机制只能对已经定义的用户授权，无法处理陌生用户的访问请求。因此，如何对陌生用户进行授权，就成为 P2P 系统访问控制中急需解决的问题。

人类社会是一个巨大的复杂的系统。系统中的

收稿日期：2009-03-18；**修回日期**：2010-05-20

基金项目：国家自然科学基金资助项目（60573037）；国家高技术研究发展计划（“863”计划）基金资助项目（2007AA010301-02）；北京航空航天大学软件开发环境国家重点实验室探索性自主研究课题基金资助项目（SKLSDE-2009ZX-06）

Foundation Items: The National Natural Science Foundation of China (60573037); The National High Technology Research and Development Program of China (863 Program) (2007AA010301-02); The Foundation of the State Key Laboratory of Software Development Environment of Beijing University of Aeronautics and Astronautics (SKLSDE-2009ZX-06)

实体（人、公司、企业等）之间的交互是基于彼此的信任关系。因此，人们提出将人类社会的信任机制引入到大规模分布式计算中，作为系统实体之间交互时的决策依据。这样的思想直到 1996 年美国 AT&T 实验室的 Blaze 等人提出信任管理（TM, trust management）概念并开发出相应工具后，才引起人们的广泛关注，成为目前分布式访问控制研究中的热点[1,2]。在 Blaze 等人提出的信任管理中，用户之间通过签发公钥证书建立信任关系，信任取值于集合{0，1}，即信任与不信任，并且通过一种逻辑语言描述安全策略与公钥证书集合，通过逻辑推理确定给定的公钥（集）是否满足指定的安全策略，从而做出访问控制决策。这种方法虽然能够清晰表达信任，但却无法表达信任的不同程度。信任度是客观存在的，人们认识到利用信任度可以更加有效地实现分布式系统中的各种安全控制，因此已经引起了分布式计算领域的关注。在访问控制领域，信任度将使安全策略的定义更加清晰、明确，并可以针对不同信任度制定不同的安全策略，从而实现细粒度的访问控制。目前，虽然出现了基于概率论、主观逻辑、模糊数学等信任度表达方法[3~6]，但由于信任概念的复杂性，还没有形成一种公认的成熟理论，而针对访问控制的信任量化模型也还没有形成。本文将深入分析分布式系统访问控制背景下信任特性，并以此为依据，综合运用多种数学工具，建立一种面向访问控制的信任表达与计算的数学模型。

本文的内容组织如下：在相关研究中将主要分析现有信任表达的相关理论与方法；第 2 节在分析社会学中信任特性的基础上，指出访问控制中信任的含义、特性与属性；第 3 节中将利用模糊数学定义信任概念的数学表达；第 4 节将以模糊数学为基础并结合概率论，建立面向访问控制的直接信任表达模型；第 5 节将基于模糊集合运算，提出间接信任的计算方法；第 6 节将给出所提出信任量化表达模型的验证实例；最后对全文进行总结。

2 相关研究

1996 年 Blaze 和 Chu 等人将信任管理的概念引入到分布式计算领域，研究开发了 PolicyMaker/KeyNote 和 REFEREE 等信任管理系统[1,2]。在这些系统中，将用户间授权代理关系和系统的安全策略用策略语句(policy statements)进行描述。PolicyMaker/KeyNote 和 REFEREE 以用户请求和相应的策略语句描述为输入，输出为决策结果。在 Blaze 等人提出的信任管理模型中，信任取值为 0 或 1，而 Gambetta，AdulRahman 等认为，信任是具有不同程度的[7,8]。围绕信任度的量化表达，国内外也出现一些研究，并提出了几种典型的信任表达与推理模型。比较有代表性的是 Beth 等人提出的信任评估方法，Josang 提出的基于主观逻辑的信任模型等。

Beth 模型[3]提出了直接信任与间接信任的概念，这种信任的分类被后续很多信任模型采用。Beth 给出了基于经验的直接信任度量以及推荐信任的推导与综合公式。Beth 信任度量与推导的基本思想是：以实体完成任务的期望为基础，根据肯定经验与否定经验计算出实体能够完成任务的概率，以此概率作为实体信任度的度量。在对多个信任值进行综合时，采用的是简单的求均值的方法。Beth 模型在直接信任的度量中，只采用肯定经验进行计算，以及信任综合时简单采用了均值方法，这些都与信任关系的真实含义存在偏差。

Josang 提出的基于主观逻辑的信任推理模型[4]，基于证据空间与观念空间的概念描述信任关系，并定义了主观逻辑算子用于信任度的合并、推荐等推理。证据空间由一系列实体产生的可观察到的事件组成，这些事件分为肯定事件与否定事件。Josang 基于 Beta 分布函数描述二项事件后验概率的思想，给出了一个由肯定事件数与否定事件数决定的概率确定性密度函数 *pcdf*，并以此计算实体产生某个事件概率的可信程度。观念空间（opinion space）由对实体信任程度的一系列评估组成，每个评估由三元组 $w=\{b, d, u\}$描述，其中 b、d、u 分别表示信任程度、不信任程度和不确定程度，且 $b+d+u=1$, b、d、$u\in[0,1]$。Josang 认为 w 与 *pcdf* 在主观信任度的表达上是等价的，即可以通过证据空间的统计事件来描述主观信任度，并给出了基于肯定事件与否定事件的计算公式。Josang 模型使用三元组而不是 Beth 模型中的单一数值来描述信任度，并且采用肯定事件与否定事件的概率度量信任关系。因此，Josang 模型与 Beth 模型都基于概率论，实际上是将信任的主观性与模糊不确定性视为随机性。

基于信任的主观性与模糊性，人们提出利用模糊数学研究信任的量化表达。北京大学唐文、陈钟等人考察了信任的模糊性，运用模糊集合理论对信任管理问题进行了研究，给出了一种包括信任类型

的定义、信任的评价、信任的形式化表示以及信任关系的推导方法[5]。

通过分析信任的特性可以发现，信任的主观性、模糊性与不确定性是不等同于随机性的，因此单纯利用概率论表达信任并不完全符合信任的特性。而信任的主观性与模糊性更适合使用模糊数学理论进行表达。另外，社会学研究成果表明，信任是依赖于一定的环境或上下文的，脱离特定的环境谈论信任是没有意义的。因此，访问控制背景下的信任量化度量模型的研究应该是结合访问控制中信任的特性，并依据信任特性选取相关数学理论作为信任量化表达的数学基础。本文正是在这种思想指导下开展信任度量化表达研究的。

3　访问控制中信任的含义与属性

3.1　信任的含义与特性

社会科学中的许多分支，如社会学、心理学、商学、经济学与政治等领域都涉及到信任的概念，对信任的含义和信任的特性也进行了充分的研究，并且已经出现了一些相对成熟的信任理论，如 Diago Gambetta，Russel Hardin 等人提出的信任理论[7,9]。在社会科学中对信任的一种典型的定义是由 Gambetta 给出的。他认为信任是关于主体在一定背景下执行某种特定动作的可能性的主观测度[7]。这个定义表明信任是一种主观判断，所有的信任本质上都是主观的，这种主观性源自于信任在很大程度上依赖于观察者；信任不是二值的，也即不是“非此即彼”的，信任是具有“度”的；另外信任还依赖于一定的背景，脱离背景的信任是没有意义的。综合上述社会学中的诸多相关研究，可以确定信任具有下列特性，其中信任的主观性、特定性、模糊性与不确定性是信任的基本特性。

1) 主观性：信任依赖于评价实体，不同的实体对同一个实体可能有不同的信任评价。

2) 特定性：信任是特定于某种背景的。不同的背景下，信任具有不同的属性。信任的属性是进行信任评估时应考虑的因素。

3) 模糊性：信任是语义范畴的概念，不是用具体的数值来表达的，也不能只分为信任与不信任，信任是具有“度”或多种等级的。

4) 不确定性：由于在判定实体信任度时，无法获得全部信息，因此信任具有不确定性。

5) 非对称性：即 A 对 B 的信任值不一定等于 B 对 A 的信任值。

6) 传播性：实体之间信任关系的变化会影响其他实体之间的信任关系。

7) 动态性：实体之间的信任关系不是持久不变的，受实体行为的影响，随之动态变化。合法诚信的行为将会提高信任值，反之则降低信任值。

实体之间的信任关系可以分为 2 类：直接信任和推荐信任。直接信任是指 2 个实体之间曾经有过直接的交互，从而建立了一种信任关系。推荐信任是指 2 个实体 A 与 B 之间没有过直接交互，B 对于 A 是陌生实体，但 A 和 B 之间存在一个由多个实体通过信任关系构成的信任链，则 A 可以通过信任链上实体的推荐建立对 B 的信任关系。

3.2　访问控制中信任的属性

不同背景下信任的具体含义与属性是不同的。访问控制背景下信任的属性，是指对实体的信任进行评估决定是否进行访问授权时应该考虑的因素。因此，这些属性应该从访问控制目标出发进行分析与确定。

欧共体标准 ECITSEC 中定义的信息安全包括 5 个方面：机密性（confidentiality），即信息不被非法泄露或窃取；完整性（integrity），即信息不被非法篡改；可用性（availability），即信息不被非授权占用。ECITSEC 和最早提出访问控制概念的 Butler Lampson 等人都曾分析指出，实现机密性、完整性与可用性的安全机制存在本质的差别[10,11]：可用性不但与信息有关，而且还与其他资源有关，而机密性与完整性只与信息相关。机密性与完整性可以通过定义精确的、全局的、一致的系统特性来描述，它们具有“可计算性”，而可用性却不具有“可计算性”。系统特性“可计算性”的含义是，如果某种特性的定义能够使人们明确判定系统是否具有该特性，则这种特性在计算机科学中称为具有“可计算性”。可计算性进一步意味着可以定义数学算法对这些特性进行验证。因此对于机密性与完整性可以利用实现这些数学算法的计算机程序验证系统是否具有这些特性，而其他的系统特性如可用性、可靠性等则本质上是不可计算的[12]。ECITSEC 与 Lampson 等人还明确指出访问控制成为保证机密性与完整性的基础。通过实施访问控制，可以验证一个系统具有很高程度的机密性与完整性。因此，基于信任的访问控制方法是以保护信息的机密性、完整性为目标，基于对请求者信任属性的评估

决定是否允许其访问请求，信任的量化表达是基于信任访问控制的基础与关键。

以上述人类社会信任的定义与特性为基础，本文在信任的表达与推理的研究中，以访问控制为背景，分析确定信任的上下文属性，并以信任的特性为依据，采用适当的数学工具建立信任的表达与推理模型。首先给出访问控制中实体信任的含义。

定义 1 （访问控制中的信任），访问控制中实体的信任，是从保证被访问客体机密性与完整性的角度，对一个实体的行为所进行的可信度评估。

本文从访问控制的目标出发，层层分析分布式系统访问控制背景下信任应该考虑的因素，作为信任的属性，并以可扩展的信任属性树的形式表达出来，如图 1 所示。实体信任特性主要包括保护信息机密性能力、保护信息完整性能力以及信誉几个方面。信誉是其他实体对被评估实体信任水平的评价，在进行信任评估时，应该作为一个因素。而保护信息机密性能力、保护信息完整性能力又包括若干方面的属性。

1) 保守机密性：是否能够保证不泄露从访问中获取的保密性信息。

2) 权限传播的规范性：是否能够不向不可信用户传递访问权限。

3) 自我防护能力：自身的防护能力，保证自己不被恶意代码利用。

4) 通信链路的可靠性：请求者与资源拥有者之间的链路的安全性。

5) 操作规范性：是否能够按照预定的资源访问方式进行资源的访问。

6) 诚实性：它所提出的访问要求与它的行为是否一致，是否能严格遵守它自己的承诺。

7) 友好性：不发起对资源的恶意攻击。

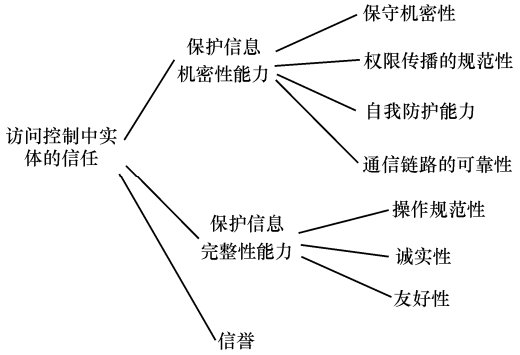


图 1 访问控制背景下信任的属性树

3.3 信任量化表达的基本思想

信任表达的目标是建立信任的可计算数学模型。而该模型的建立，应该依据信任的特性，并借助有效的数学工具进行。而信任的主观性、模糊性与不确定性作为信任的重要特性，是选择信任描述数学理论时主要考虑的特性。

信任表达的首要难点在于其具有模糊性，无法用常规的精确逻辑来描述和分析。虽然模糊性也是一种不确定性，但却不等同于随机不确定性，所以基于概率论来描述信任存在一定的局限，并且信任的不确定性是由于信任的某些因素的不确定性所导致的。美国控制论专家 Zadeh 于 1965 年提出的模糊数学理论将数学研究的对象扩大到具有模糊性的概念，是对模糊概念量化表达的有效理论工具[13]。因此，本文认为模糊数学可以作为信任表达的基本数学工具，而对于某些具有不确定性的信任因素可以利用概率论进行表达。综上所述，本文将选取模糊数学为基本数学依据并结合概率论建立信任量化表达模型。首先将基于模糊集合论给出“信任”这个模糊概念的数学定义；然后将模糊数学与概率论有机结合，建立直接信任的模糊综合评判模型；最后基于模糊集合运算提出间接信任的计算方法。

4 信任概念的数学定义

如何将语义范畴内的信任用数字形式表达出来，是信任量化表达中需要首先解决的问题。在现实世界中，实体间的信任程度通常是由不同等级的程度副词来评价的，如可信任程度很好、一般等。因此，本文将首先基于模糊数学给出信任评价等级及其数学定义，在此基础上给出信任的数学定义。

设 $U=\{u_0,u_1,\cdots,u_n\}$ 为大规模分布式系统中相互交互的实体集合，其中 u_i (i=0,1,2,$\cdots$,n)表示单独的实体。

定义 2 （信任评价集），D_i (i=1, 2,$\cdots$,M)是 U 上的模糊集合，且 $U=D_1\cup D_2\cup\cdots\cup D_M$，任意 $D_i\cap D_j=\varnothing$，$i, j\in$ [1,M]且 $i\neq j$，则称 D 为 U 上的等级模糊子集合。令 M=5，并定义 D_j 的语义如下。

D_1：表示“差”子集合；

D_2：表示“比较差”子集合；

D_3：表示“一般”子集合；

D_4：表示“比较好”子集合；

D_5：表示“很好”子集合；

则集合 $D=\{D_i \mid i=1, 2, \cdots, M\}$（$M$=5）即 D={差，

比较差，一般，比较好，很好 }是一个 U 上的评价等级的集合，或称为信任评价集。

定义 2 定义了信任评价集 D，但 D 中的每一个元素 $D_i \in D(i=1,2,\cdots,5)$仍然是模糊的概念。信任概念的量化表达，需要首先对评价等级 D_i 进行量化。本文将评价等级 D_i 表达为模糊向量，称为信任评价等级向量。信任评价等级向量中，D_i 对 D 中每个等级的隶属度理论上可通过隶属度函数表示。

定义 3 （信任评价等级向量），设 V_D 为评价集 D 的评价等级向量的集合，则 $V_D=\{V_{D_1},V_{D_2},V_{D_3},V_{D_4},V_{D_5}\}$，其中 $V_{D_i}=\{v_1,v_2,\cdots,v_5\}$，$v_j \in [0,1]$，$j=1,2,\cdots,5$，$V_{D_i}$ 表示了等级 $D_i(D_i \in D, i=1,2,\cdots,5)$ 对各评价等级的隶属度，称为评价等级向量。

由于信任的主观性，每个主体的判定标准都不同。本文依据评价等级的语义，分析得出评价等级 D_i 对于信任评价集中各等级的隶属度，近似符合正态分布 $N(D_i,\sigma^2)$，并定义了评价等级向量：

$\boldsymbol{V}_D=\{V_{D_1},V_{D_2},V_{D_3},V_{D_4},V_{D_5}\}$ ={{0.67, 0.33, 0.00, 0.00, 0.00}, {0.25, 0.50, 0.25, 0.00, 0.00}, {0.00, 0.25, 0.50, 0.25, 0.00}, {0.00, 0.00, 0.25, 0.50, 0.25}, {0.00, 0.00, 0.00,0.33, 0.67}}。

由于信任的模糊性，所以很难准确判断实体信任属于哪个评价等级，而且实体信任对某个评价等级的隶属关系不能简单地用“真”或“假”这样的二值函数来表达，因此用实体信任对各个评价等级的隶属度所构成的信任向量来描述信任是更合理的。向量的每一维对应一个信任等级，该维上的取值表示实体对该等级的隶属度。下面给出信任向量的具体定义。

定义 4 （信任向量），模糊向量 $\boldsymbol{V}=\{v_1,v_2,\cdots,v_M\}$ (M=5)表示实体 x 的信任度，其中 v_i 表示 x 对信任等级 D_i(i=1, 2,⋯,M)的隶属度，则称向量 $\boldsymbol{V}$ 为信任向量。

例如，若某信任属性评价结果为“很好”，则根据上述 V_D 的定义，该信任属性的模糊向量为{0, 0, 0, 0.33, 0.67}。

5　访问控制中直接信任的量化表达

5.1　直接信任量化表达模型的基本结构

信任是一个复杂的概念，因而对信任的评估与量化表达也是一个复杂的过程。模糊综合评判是模糊数学中对复杂概念进行量化评价的有效方法。模糊综合评判的基本思想，是分析确定影响模糊概念评判结果的相关因素，然后分别对每个因素作出评价，最后将各因素的评价结果采取一定的数学手段进行综合，得到复杂概念的量化评价值。本文中的直接信任量化表达模型就是采用模糊综合评判方法的一种信任综合评价模型。模型中以上文提出的访问控制中信任属性树为信任因素集合，对于具有模糊性和主观性的因素利用评价集进行评价，而对于具有不确定性的因素，利用概率论方法进行表达，然后将各因素评价结果表达为评价矩阵，并将其与因素的权重进行模糊变换得到信任向量。

信任的复杂性决定要考虑的信任因素很多，如图 1 所示，这一方面是权重分配很难确定，另一方面，由于权重分配需要满足归一性，即各权重值 w_i 要满足 $\sum w_i=1$，所以每一因素分得的权重必然很小，而较小的权重在进行模糊变换时常常被“淹没”，从而在综合评价中不能合理反映各个因素的作用。因此，基于模糊数学中解决这类问题的分层方法，本文将信任因素集分为 2 个层次，建立多级信任综合评价模型。

设 E 为访问控制中信任相关的因素集，将 E 分为 3 个不相交的子集 E_1=C={c_1,c_2,c_3,c_4}={保守机密性，权限传播的规范性，自我防护能力，通信链路的可靠性}，E_2=IN={in_1,in_2,in_3}={操作规范性，诚实性，友好性}，E_3=R={r}={信誉}，则 $E=\{C,IN,R\}$ 称为第 1 级因素集，而 C，IN，R 为第 2 级因素集。

定义 5 （信任综合评价模型），信任综合评价模型分为如下 2 个部分。

1) 对信任因素的第 1 级因素 $E=\{e_1,e_2,\cdots,e_n\}$，利用评价集 $D=\{d_1,d_2,\cdots,d_m\}(m=5)$ 进行评价，得因素评判矩阵 $\boldsymbol{R}=(r_{ij})_{n*m}$，$\boldsymbol{R}$ 是一个模糊关系（relation），表示对各个因素 e_i 作各种等级评价的可能性。设因素集 E 的权重为 $W=\{w_1,w_2,\cdots,w_n\}$，且 $\sum_{i=1}^{n} w_i=1$，综合评判将得到模糊向量 $\boldsymbol{V}$，$\boldsymbol{V}=\{v_1,v_2,\cdots,v_m\}$，且 $\boldsymbol{V}=\boldsymbol{W}\circ\boldsymbol{R}$，其中，∘为模糊算子。

2) 将二级信任因素集 E 的各个第 2 级因素集合 E_i (i=1,2,3)，利用 1）中描述的方法进行综合评价，得到因素 E_i 的信任向量 $\boldsymbol{V}_i$，并由 $\boldsymbol{V}_i$(i=1,2,3)构成 E 的一级因素评价矩阵 $\boldsymbol{R}$，$\boldsymbol{R}=[V_1,\ V_2,\ V_3]^{\mathrm{T}}$。设各因素 E_i(i=1,2,3)权重为 W={w_1,w_2,w_3},则信任评价向量 $\boldsymbol{V}_{1\times5}=\boldsymbol{W}_{1\times k}\circ\boldsymbol{R}_{k\times5}(k=1,2,3)$，其中,∘为模糊算子。

定义 5 中模糊关系的合成算子“∘”的选择是非常重要的。

在广义模糊运算下，$v_j=(w_1 \dot{\wedge} r_{1j}) \dot{\vee} (w_2 \dot{\wedge} r_{2j}) \dot{\vee} \cdots \dot{\vee} (w_n \dot{\wedge} r_{nj})$ (j=1，2，…，5)，其中“$\dot{\wedge}$”和“$\dot{\vee}$”分别是广义模糊“与”运算和广义模糊“或”运算，记作 $M(\dot{\wedge},\dot{\vee})$。从理论上讲，这 2 种广义模糊运算具有无穷种模型，但在通常的实际应用中，人们普遍采用的模型有：$M(\wedge,\vee)$型、$M(\cdot,\vee)$型、$M(\cdot,\oplus)$型、$M(\cdot,+)$型和 $M(\wedge,\oplus)$型等。这几种数学模型各有特点，$M(\wedge,\vee)$是主因素决定型的综合评判，$M(\cdot,\vee)$和 $M(\wedge,\oplus)$是主因素突出型的综合评判，与 $M(\wedge,\vee)$接近，但比 $M(\wedge,\vee)$更精细，所得结果在一定程度上反映了非主要指标；$M(\cdot,\oplus)$则均衡兼顾，体现出整体特性。经过分析认为主因素突出型的综合评判最适合于信任评估，所以本文选择 $M(\cdot,\vee)$作为模糊关系的合成算子“∘”，即用普通的实数乘法·作为矩阵运算中的乘，以∨作为运算中的和，∨是 Zadeh 算子，表示 max 运算。运算公式如下：

$$v_j=\bigvee_{i=1}^{m}(w_i r_{ij}),\ j=1,2,\cdots,M$$

通过综合评价得出的信任向量是以模糊集合的形式对信任进行量化表达。本文进一步将确定的一种信任向量转换到一个在区间[0,1]内的数值来更直观表达信任。模糊向量到数值的转换，常见的方法包括最大隶属度法、加权平均法等。本文采用一种兼顾加权平均和最大隶属度原则的方法，以加权平均法为基础，尽可能不丢失信息，又可以在不同程度上突出主因素的作用。由信任向量 $v=\{v_1,v_2,\cdots,v_n\}$得到信任值 *value* 的计算公式如下。

$$Value=\sum_{i=1}^{n} e_i v_i^k \Big/ \sum_{i=1}^{n} v_i^k \tag{1}$$

式(1)中 e_i是等级为 v_i时参数的规定值，幂次指数 k 表示主因素的突出程度。本文经过多次计算比较，发现 k=3 时主因素的突出程度与其他因素的兼顾程度比较合适。

5.2 基于层次分析法的因素权重确定方法

在信任的综合评判中，每个因素的重要程度是不同的，从而对最终的评判结果的影响程度也将不同。在多层信任综合评估模型中，以因素的权重表示该因素在综合评判中的重要程度，权重也是一个模糊概念。目前有多种确定权重的方法，其中的层次分析法是一种多指标权重排序的特征值方法，是对人们的主观做客观描述的一种有效方法[14]。该方法符合人们常用的两两比较判断重要性的思维习惯，简捷实用，因此本文采用这种方法确定信任评估模型中的权重参数。

层次分析法的基本思想是对因素进行两两重要性比较，以标度值表示比较结果并将所有结果构造为判断矩阵。根据判断矩阵求出最大特征根所对应的特征向量即为各评价因素的权重向量。而最大特征根是计算判断矩阵一致性指标的重要因子。判断矩阵的一致性越好，表明权重分配是合理的。

设 u_i 表示评价因素，$u_i \in U(i=1,2,\cdots,n)$。$u_{ij}$ 表示 u_i 对 u_j (j=1,2,…,n)相对重要性数值，u_{ij} 的取值依据判断矩阵标度表[14]。u_{ij} (i=1,2,…, j=1,2,…)构成了判断矩阵 $\boldsymbol{P}$。$\boldsymbol{P}$ 的最大特征根所对应的特征向量就是评价因素的权重向量。

$\boldsymbol{P}$的最大特征根所对应的特征向量可以采用方根法求得：设$\boldsymbol{W}=(w_1,w_2,\cdots,w_n)^{\mathrm{T}}$为 $\boldsymbol{P}$ 的特征向量，则

$$w_i=\frac{w_i'}{\sum_{j=1}^{n} w_j'},\quad i=1,2,\cdots,n \tag{2}$$

其中，$w_i'=\sqrt[n]{\prod_{j=1}^{n} w_j'}$，即 w_i'是 $\boldsymbol{P}$ 中第 i 行元素乘积的 n 次方根。而 $\boldsymbol{P}$ 的最大特征根

$$\lambda_{\max}=\frac{1}{n}\sum_{i=1}^{n}\frac{(\boldsymbol{PW})_i}{w_i} \tag{3}$$

其中，$(\boldsymbol{PW})_i$ 表示向量 $\boldsymbol{PW}$ 的第 i 个元素。用上述方法得到的权重分配的合理性，需要对判断矩阵 $\boldsymbol{P}$ 的一致性进行检验。检验公式为：$CR=CI/RI$，CR 是判断矩阵的随机一致性比率，CI 是判断矩阵的一般一致性指标，且 $CI=\frac{1}{n-1}(\lambda_{\max}-n)$，$RI$ 是判断矩阵的平均随机一致性指标，层次分析法中提供了 9 阶以下 RI 的值，因此 RI 的值可查表获得。当 CR<0.10 时，即认为判断矩阵具有满意的一致性，说明各因素权重分配是合理的。

在集合 $C=\{c_1,c_2,c_3,c_4\}$=｛保守机密性，权限传播的规范性，自我防护能力，通信链路的可靠性｝中，c_1与 c_2直接影响到信息的机密性，是重点考察的因素；而 c_3与 c_4是影响信息机密性的间接因素，不是关键因素。本文利用层次分析法可计算得到 C

的权重集合: $W_C=\{w_{c_1},w_{c_2},w_{c_3},w_{c_4}\}=\{0.347, 0.527, 0.075, 0.050\}$。

在集合 $IN=\{in_1,in_2,in_3\}=$ {操作规范性，诚实性，友好性}中，3 个因素对于保证信息的完整性都很重要。诚实性与友好性的重要程度相当，而操作规范性要稍重要于其他 2 个因素。则可得到 C 的权重集合：$W_{IN}=\{w_{IN_1},w_{IN_2},w_{IN_2}\}=\{0.600,0.200,0.200\}$。

在信任因素集 $E=\{e_1,e_2,e_3\}=\{C,IN,RE\}=${保护信息机密性能力，保护信息完整性能力，信誉}中，信誉只是提供一定的参考信息，并不是关键的因素，而其他 2 个因素则是关键的需要重点考虑的。保护信息机密性能力与保护信息完整性能力同样重要，而且它们都明显重要于信誉。计算得到 C 的权重集合：$W_E=\{w_{E_1},w_{E_2},w_{E_3}\}=\{0.454,0.454,0.092\}$。

依据式（3），计算得到因素集合 C，IN，E 的判断矩阵一致性比率分别为 0.028，0，0，均小于 0.10, 说明这些因素集合中各因素的权重分配是合理的。

5.3　信誉的概率统计计算方法

信誉是其他实体对被评估实体可信程度的评价。在人类社会中，人们在对一个陌生人进行信誉评估时，会在自己认识的人当中进行询问。而被询问者为保护自己的隐私，往往不会过多反映自己的主观意见，而会以一种比较客观的方式进行评价。参考现实中的这种信誉获取方法，本文在对实体的信誉进行评估时，评价实体向与自己有过交往的所有实体发出对被评估实体的可信度评价请求。而所有被请求的实体，都根据被评估实体与自己交往中的表现给出评价。在这种方式下，由于评价实体能够搜集到的反馈数是随机的，而且反馈的可信程度也是不确定的，从而使信誉的评估具有随机不确定性。为此，本文引入概率统计的方法，建立信誉的模糊概率统计计算公式。

实体 X 对被询问实体 Y 的可信程度的计算，将采用 Y 成功访问 X 资源的次数与 Y 总访问请求次数的比值。如果评价实体 A 共搜集到对实体 B 的 n 个可信评价，则 A 求得这 n 个评价的平均值作为对 B 的信誉评价值。定义 6 给出信誉的计算公式定义。

定义 6　（信誉计算方法）设实体 A 对实体 B 进行信誉评价，并且 A 获取了其他 n 个实体对 B 的可信程度评价，实体 i(i=1,2,…,n)对 B 的可信程度评价表达为

$$\frac{\text{B成功访问实体 } i \text{ 的次数}}{\text{B对实体 } i \text{ 的访问请求次数}}$$

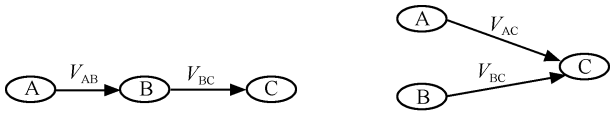
则 A 对 B 的最后信誉评价值为

$$\text{B 的信誉}=\frac{\sum_{i=1}^{n}\frac{\text{B成功访问实体}i\text{的次数}}{\text{B对实体}i\text{的访问请求次数}}}{n}$$

同时本文还定义了信誉值与评估等级的对应关系，可获得因素集 E 中 RE 的评价向量 V_{RE}。

6　基于 Einstein 算子的间接信任计算方法

2 个陌生实体之间的信任关系，是由多个推荐信任向量的连接与合并 2 种基本结构复合而成，如图 2 所示。因此如何由连接与合并关系得到新的信任向量，就是间接信任（推荐信任）计算中的基本问题。本文认为这是通过已知信任向量计算得到新的信任向量的过程，适宜采用模糊数学中模糊集合的“交”和“并”运算。



(a) 信任链的连接结构　　(b) 任链的合并结构

图 2　信任链的 2 种典型结构

在模糊集合交和并的运算中，交和并算子的确定将直接影响到推荐信任计算的准确性。∧和∨是 2 个实现交、并运算的算子，称为 Zadeh 算子。它们是对 2 个隶属函数取最小值和最大值运算，相对来说有些粗糙。因此，人们在 Zadeh 算子∧和∨的公理化结构即三角模和三角余模的基础上，设计了其他三角模和三角余模组成对偶模，继而定义多种相应于交、并运算的许多加细模糊算子，如概率算子、Einstein 算子、Hamacher 算子等。

设 A、B 为模糊集合，则 Einstein 算子 $\dot{\varepsilon}$ 与 $\overset{+}{\varepsilon}$ 的定义如下：

$$(A\cap B)(x)=A(x)\dot{\varepsilon}B(x)=\frac{A(x)B(x)}{1-(1-A(x))(1-B(x))}$$

$$(A\cup B)(x)=A(x)\overset{+}{\varepsilon}B(x)=\frac{A(x)+B(x)}{1+A(x)B(x)}$$

其中，$A(x)$和 $B(x)$分别表示 x 对模糊集合 A、B 的隶属度。

对于信任向量 $\boldsymbol{V}_1=\{v_1^1,v_2^1,\cdots,v_M^1\}$，$\boldsymbol{V}_2=\{v_1^2,v_2^2,\cdots,v_M^2\}$，则可利用 Einstein 算子定义下列运算。

$\boldsymbol{V}_1$、$\boldsymbol{V}_2$的连接：

$$\boldsymbol{V}=\boldsymbol{V}_1\cap\boldsymbol{V}_2=\{v_1,\cdots,v_M\}=\{v_1^1\dot{\varepsilon}v_1^2,v_2^1\dot{\varepsilon}v_2^2,\cdots,v_M^1\dot{\varepsilon}v_M^2\}\quad(4)$$

$\boldsymbol{V}_1$、$\boldsymbol{V}_2$ 的合并：

$$\boldsymbol{V}=\boldsymbol{V}_1\cup\boldsymbol{V}_2=\{v_1,\cdots,v_M\}=\left\{v_1^1\overset{+}{\varepsilon}v_1^2,v_2^1\overset{+}{\varepsilon}v_2^2,...,v_M^1\overset{+}{\varepsilon}v_M^2\right\} \tag{5}$$

Einstein 算子 $\dot{\varepsilon}$ 和 $\overset{+}{\varepsilon}$ 粗糙程度适中，并且依据三角模和三角余模的定义，得出 Einstein 算子具有这样的特性：$0\leqslant A(x)\dot{\varepsilon}B(x)\leqslant\min(A(x),B(x))$，$\max(A(x),B(x))\leqslant A(x)\overset{+}{\varepsilon}B(x)\leqslant 1$，这种特性与信任在传递与合并中的衰减与增强特性相符，因此本文采用 Einstein 算子实现间接信任中的信任连接与合并运算。

7　信任量化表达模型的实例测试

本文所提出的上述直接信任评估模型与间接信任计算模型已经在信任评估软件中实现。本节将给出一个信任表达与计算的实例，对本文提出的信任量化表达模型进行测试与分析。

测试用例如图 3 所示，图中 A、B、C、D、E、F、G、H、I 为分布式系统中的实体。图中 2 个节点之间的有向弧表示弧的开始节点对终止节点存在一定程度的直接信任关系，而没有直接连接的 2 个节点之间是陌生节点。

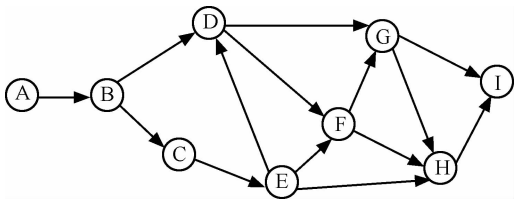


图 3　信任关系

正如上文所定义，本例中的信任因素 E={C，IN，RE}={{保守机密性，权限传播的规范性，自我防护能力，通信链路的可靠性}，{操作规范性，诚实性，友好性},信誉}，各因素的权重为：

$$W_C=\{w_{c_1},w_{c_2},w_{c_3},w_{c_4}\}=\{0.347,0.527,0.075,0.050\}$$

$$W_{IN}=\{w_{IN_1},w_{IN_2},w_{IN_2}\}=\{0.600,0.200,0.200\}$$

$$W_E=\{w_{E_1},w_{E_2},w_{E_3}\}=\{0.454,0.454,0.092\}$$

直接信任的计算依据定义 5，信任向量到信任值的转换采用式(1)，而间接信任的计算采用式(4)与式(5)。图 3 中的 10 个实体之间的直接信任关系评价以及量化表达结果见表 1。

表 1 中，例如 A 对 B 各信任因素的评价结果是：在保守机密性、操作规范性、自我防护能力等方面很好；在权限传播的规范性、友好性、信誉等方面较好；而在通信链路可靠性、诚实性等方面较差。如果对 B 的信任程度进行定性评价，综合考虑到各种因素的评价值与重要程度，结果将是在较好与很好之间，而利用直接信任表达模型计算得到的信任值为 0.913，表明该信任关系的定量计算结果与定性分析结果基本相符。

图 3 中，实体 A 与除了实体 B 之外的其他实体

表 1　　**信任网络的初始化**

直接信任	评价结果	信任向量	信任值
A→B	((很好,较好,很好,较差),(很好,较差,较好),较好)	[0.028 4, 0.056 8, 0.133 9, 0.364 3, 0.416 7]	0.913
B→C	((较好,差,一般,较好),(很好,差,较好),较差)	[0.189 7, 0.133 8, 0.125 4, 0.277 6, 0.273 5]	0.757
B→D	((一般,较差,很好,较好),(较好,差,较差),较差)	[0.146 0, 0.208 9, 0.230 1, 0.271 8, 0.143 1]	0.619
C→E	((较好,一般,较差,差),(很好,差,较好),很好)	[0.226 5, 0.207 4, 0.102 3, 0.188 3, 0.275 3]	0.624
D→F	((较差,一般,较好,差),(很好,差,较好),较差)	[0.198 2, 0.150 8, 0.125 4, 0.260 6, 0.265 0]	0.722
D→G	((较好,一般,较好,差),(很好,差,较好),较差)	[0.189 7, 0.133 8, 0.125 4, 0.277 6, 0.273 5]	0.757
E→D	((较差,较好,一般,较好),(很好,差,较差),较差)	[0.146 0, 0.208 9, 0.167 7, 0.229 4, 0.248 0]	0.695
E→F	((差,较差,一般,较好),(较好,差,较差),很好)	[0.249 2, 0.255 6, 0.173 3, 0.186 4, 0.135 4]	0.474
E→H	((很好,较差,较好,较好),(很好,较差,较好),很好)	[0.028 3, 0.056 8, 0.150 4, 0.375 5, 0.388 9]	0.895
F→G	((很好,很好,较好,一般),(较好,较差,很好),较好)	[0.022 7, 0.084 9, 0.207 2, 0.359 1, 0.326 0]	0.853
F→H	((较好,一般,较好,较差),(很好,差,一般),差)	[0.161 9, 0.167 7, 0.164 6, 0.254 9, 0.250 8]	0.733
G→H	((较好,很好,很好,较差),(差,较差,较好),很好)	[0.210 9, 0.146 6, 0.090 6, 0.244 9, 0.306 9]	0.756
G→I	((较好,一般,较差,差),(很好,差,较好),很好)	[0.188 4, 0.222 8, 0.125 1, 0.188 4, 0.275 4]	0.664
H→I	((差,一般,很好,较好),(较好,差,较好),较好)	[0.166 7, 0.141 9, 0.239 1, 0.310 0, 0.142 3]	0.673

都是陌生实体，但却存在着推荐信任关系。根据本文给出的间接信任的计算方法，可以得出 A 对图中其他实体间接信任的信任值，见表 2。A 与 E 之间存在着 $A \xrightarrow{0.913} B \xrightarrow{0.757} C \xrightarrow{0.624} E$ 推荐信任关系。人类社会中，信任是随着信任链逐级衰减的。虽然 A 很信任 B，但 B 对 C 以及 C 对 E 的信任程度却一般，按照人们的经验 A 对 C 的信任也将很一般，甚至偏差。按照式（4）得到 A 对 E 的间接信任是 0.433。从实体 A 到实体 D 有 2 条推荐路径：$A \xrightarrow{0.913} B \xrightarrow{0.619} D$ 和 $A \xrightarrow{0.913} B \xrightarrow{0.757} C \xrightarrow{0.624} E \xrightarrow{0.695} D$，从 2 条推荐路径上分别得到 A 对 D 的信任值为 0.364 与 0.585，虽然在每条路径上都有信任度的衰减，但 A 对 D 的信任值依据式(5)把 2 个信任链的值进行合并，最终得到 A 对 D 的间接信任值为 0.610，比单条信任链上获得的信任值有所加强。上述例子表明，信任在进行连接或合并运算后，其衰减与增强的程度是合适的，并且根据 Einstein 算子的性质，将保证结果在[0，1]区间取值，因此式(4)与式(5)定义的间接信任计算公式是有效的。

表 2　　间接信任计算

间接信任	信任向量	信任值	用时(ms)	推荐路径(条)
A→C	[0.018 1, 0.025 3, 0.057 9, 0.416 1, 0.482 5]	0.644	16	2
A→E	[0.268 3, 0.174 0, 0.050 0, 0.246 5, 0.261 0]	0.433	31	3
A→D	[0.182 5, 0.269 8, 0.190 4, 0.261 9, 0.095 2]	0.610	32	5
A→F	[0.202 6, 0.202 6, 0.111 1, 0.346 4, 0.137 2]	0.565	62	7
A→G	[0.152 8, 0.165 6, 0.114 6, 0.420 3, 0.146 4]	0.669	63	9
A→H	[0.087 4, 0.094 2, 0.066 9, 0.491 8, 0.259 5]	0.748	78	12
A→I	[0.129 7, 0.167 3, 0.062 7, 0.414 2, 0.225 9]	0.692	109	14

实体间直接信任的表达与间接信任的计算为基于信任的访问控制提供了可能。假设信任决策的临界值为 0.6，即当被请求实体对请求者信任值的计算结果大于 0.6 时，则将允许请求者访问，否则拒绝访问。从表 1 可以看出，实体 A 对 E 以及 F 的信任度评价均小于 0.6，所以 A 将拒绝陌生实体 E 和 F 的访问请求；而实体 C、D、G、H、I 的信任值都大于 0.6，所以当这些与 A 相互陌生但存在推荐信任关系的实体向 A 发出访问请求时，将被允许。

8　结束语

本文在深入分析分布式系统访问控制中信任的语义、基本特性与上下文相关属性的基础上，建立了信任度量化表达模型。该模型通过可调整的权重参数，有机地综合了与信任相关的多种因素；间接信任的计算，符合现实社会中信任传递的衰减与多方推荐增强信任的规律。因此，本文提出的信任度量化表达模型能够比较准确并且科学地将信任在机器世界中表达出来，以此为基础，实体能够基于信任度的量化数值制定访问控制策略并进行访问决策，从而实现动态、细粒度访问控制，为大规模分布式系统提供了对陌生用户的有效控制方法。

本文所提出的信任度量化表达模型与同类研究相比有如下优点。①面向访问控制，对访问控制背景下的信任进行了充分分析与表达；②将模糊数学与概率论有机融合，使得所建立的信任量化表达模型更加符合访问控制中信任的属性特征；③对访问控制中的信任度量进行了全面、系统地研究，包括信任概念的数学定义、直接信任表达与间接信任计算等。该模型不仅可以直接应用于基于信任的大规模分布式系统访问控制，还对分布式系统其他背景下信任的应用具有参考价值。后续工作将以信任度量化模型为基础，研究基于信任的访问控制中信任的自主传播、信任关系发现，以及基于信任的决策方法等问题。

参考文献：

[1] BLAZE M, FEIGENBAUM J, KEROMYTIS A D. Keynote: trust management for public-key infrastructures[J]. Lecture Notes in Computer Science, 1999, 1550:59-63.

[2] CHU Y H, FEIGENBAUM J, LAMACCHIA B, *et al*. Referee: trust management for web applications[J]. World Wide Web Journal, 1997,(2): 127-139.

[3] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks[A]. Proceedings of the European Symposium on Research in Security(ESORJCS)[C]. Brighton: Springer-Verlag, 1994.3-18.

[4] JOSANG A, HAYWARD, POPE S. Trust network analysis with subjective logic[A]. Proceedings of the Australasian Computer Science Conference (ACSC'06)[C]. Hobart, 2006.85-94.

[5] 唐文, 胡建斌, 陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展, 2005, 42(10): 1654-1659.
TANG W, HU J B, CHEN Z. Research on a fuzzy logic-based subjective trust management model[J]. Journal of Computer Research and Development, 2005, 42(10): 1654-1659.

[6] 鲍宇, 曾国荪, 曾连荪等. P2P 网络中防止欺骗行为的一种信任度计算方法[J]. 通信学报, 2008, 29(10):215-222.

BAO Y, ZENG G S, ZENG L S, *et al*. Reputation computation based on new metric in P2P network[J]. Journal on Communications, 2008, 29(10):215-222.

[7] GAMBETTA D. Trust: making and breaking cooperative relations[M]. Basil Blackwell, 1988.

[8] ABDUL-RAHMAN A, A Framework for Decentralised trust reasoning[D]. University of London, 2004.

[9] HARDIN R. The street-level epistemology of trust[J]. Politics and Society, 1993, 21(4):505-529.

[10] ISO 7498-2, OSI security architecture[S]. 1989.

[11] LAMPSON B W. Protection[A]. Proc 5th Princeton Conf on Information Sciences and Systems[C]. Princeton, 1971.437-443.

[12] HARRISON M A, RUAAO W L, Protection in operating systems[J]. Communications of the ACM, 1976, 19(8): 461-471.

[13] ZADEH L A. Fuzzy sets[J]. Information and Control, 1965(8): 338- 353.

[14] 郭亚军. 综合评价理论、方法及应用[M]. 北京: 科学出版社, 2007.
GUO Y J. Theory, Method and Application of Comprehensive Evaluation[M]. Beijing: Science Press, 2007.

作者简介：

郎波（1968-），女，辽宁东港人，博士，北京航空航天大学教授，主要研究方向为信息安全和分布式计算。

（上接第 44 页）

nodes in wireless sensor networks[J]. ACM Transactions in Information and Systems Security, 2008, 11(3): 1-37.

[15] BANERJEE T, XIE B, *et al*. Achieving fault tolerance in data aggregation in wireless sensor networks[A]. Globcom 2007[C]. Washington, DC, USA, 2007. 926-930.

作者简介：

王良民（1977-），男，安徽潜山人，江苏大学副教授，主要研究方向为安全无线传感器网络、容忍入侵理论与方法等。

郭渊博（1975-），男，陕西周至人，解放军信息工程大学副教授，主要研究方向为无线网络安全、容忍入侵理论与方法等。

詹永照（1962-），男，福建尤溪人，江苏大学教授，主要研究方向为分布式计算系统与人机交互技术。