一种基于模糊理论的 P2P 系统动态可信模型 *

杨 润, 文志诚, 李岩岩
(湖南工业大学 计算机与通信学院, 湖南 株洲 412008)

摘 要: 针对现有的 P2P 系统信任模型在信任度的计算上过于复杂的问题,提出了一种基于模糊理论的动态可信度等级模型 DTD(dynamic trust degree model)。该模型在通过对信任度的传递进行细粒度的分析,设计了一种计算对信任值传递的计算方法,并结合对直接信任度和推荐信任的多级别综合评价而获得最终的信任度。模型将 P2P 系统中信任的计算转换为了一种可计算的表达式,简化了信任的计算过程,使信任的计算变得更加灵活。

关键词: 对等网络(P2P); 信任; 模糊理论; 信任模型
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0168-06
doi:10.3969/j.issn.1001-3695.2012.01.048

Dynamic trust model for P2P network based on fuzzy theory

YANG Run, WEN Zhi-cheng, LI Yan-yan
(*College of Computer & Communication, Hunan University of Technology, Zhuzhou Hunan* 412008, *China*)

Abstract: In the traditional P2P trust system, a very complex issue is how to calculate the trust value. This paper introduced a trust degree based fuzzy theory model named DTD. This model not only designed a calculation of transfomed trust by the fine-grained analysis, but also got the final turst value with a multilevel comprehensive evaluation method for direct trust and recommended trust. The model transformed compute trust to a computable expression in P2P system, and simplified the process of trust calculation, made the calcution of the trust become fexible.

Key words: peer-to-peer(P2P); trust; fuzzy theory; trust model

0 引言

P2P 系统是 Internet 中极其重要的应用系统之一。其自身具有分散控制、自治性和可扩展性等特性。在 P2P 系统中,节点或实体可以互相共享文件、CPU 资源和磁盘空间,因此,在分布式系统中,P2P 系统变得越来越具有吸引力。在过去,P2P 技术常用于匿名节点间的共享文件,随着应用的推广,其逐渐流行于用户团体间相互提供资源共享服务。例如,多媒体资源的下载和应用、科学研究文档的共享、桌面系统的共享等一系列的资源共享服务。这些类型的服务系统大都被称为社会网络系统或者是以群组为中心的系统[1]。在这些系统中,节点之间的连接一般是通过某些特殊的关系实现的。例如,F2F(friend-to-friend)就是一个典型的社会网络系统,在这个系统中,节点间的直接连接是通过朋友关系实现的,而节点间的间接连接则是通过朋友的朋友关系实现的[2]。但是,系统中的资源共享是应该有保护方式的。因此,以群组为中心的 P2P 系统在保留了开放式系统优点的前提下,对其进行了有机的扩展用于提高系统的可靠性。

在 P2P 系统中,用户的隐私是必须得到保护的。在以群组为中心的系统中,对敏感信息的访问也必须被严格控制。所以,在系统中采用细粒度的访问控制是比较好的方法之一。然而,用户总是需要同未知的实体进行交互,这就产生了如何在这些陌生实体间进行交互控制的问题。传统的访问方法是封闭和静态的,并且不能处理来自未知实体的请求。比较好的方法则是在人类社会的信任机制基础上,对实体间的信任值采取分布式计算的方法。在 1996 年,Blaze 等人[3]提出了分布式信任管理的概念,但它仅通过访问权限验证来实现分布式信任管理,且没有实现鉴别。Herzberg 等人[4]利用基于 XML 的 TPL 描述基于角色的访问控制策略,将证书信息与访问控制策略完全分开,根据主体证书、资源拥有者设定角色赋予策略以及证书签署者角色来映射客户主体的角色,但它没有解决与委派相关的问题。王炬等人采用访问控制列表实现多主体中的信任管理,对多主体系统的访问权限的委派采用代理许可证,但委派模型过于简化,只使用于相对简单的、封闭的多主体系统中。

在目前的 P2P 系统中,主要的工作都在实现对根据相关的信誉系统中用信誉值对节点信任等级的表示[5]。因为信誉值只能反映信任值的某些属性,所以其不能完全地等价于信任值。信任值的计算应该尽可能多地采用信任值的属性,这样才能更加准确地表达出信任的等级。

本文主要探讨了在 P2P 系统中如何建立一种可扩展且灵活的访问控制机制,提出了一种基于访问控制的信任等级评级框架,并建立了一个面向访问控制的信任模型,实现了信任值的定量表达和计算。

收稿日期: 2011-06-18; **修回日期**: 2011-08-02 **基金项目**: 国家自然科学基金资助项目(60773110)

作者简介: 杨润(1984-),男,硕士研究生,主要研究方向为可信软件(58032382@qq.com);文志诚(1972-),男,副教授,博士,主要研究方向为软件工程、可信软件;李岩岩(1986-),女,硕士研究生,主要研究方向为可信软件.

1　信任的引入

1.1　信任的属性

信任是从社会科学中引入的一个概念。信任的特性是在分布式系统中建立信任模型的基础。在社会科学中包括很多分支,包括社会学、哲学、心理学、商学、经济学和政治学。在信任的研究方面,有很多的理论都已经提出,例如 20 世纪 90 年代初的甘比特(Gambetta)模型[6] 和哈丁(Hardin)模型[7] 等。在社会科学中,信任的定义和特征都已经有很好的研究。如甘比特认为信任是非理性的,是一种经验的体现,不仅要有具体的内容,还应有程度的划分,并提出了一些基于此观点的信任模型[6]。这个定义体现了如下的一些观点:a)信任是一种主观的观念;b)信任的本质也是主观的。结合那些社会科学中关于信任的相关研究,信任的性质可以被初步总结为以下几条:

a)信任是主观的。这就意味着不同的多个实体对同一个实体的评价可能是不同的。

b)信任是模糊的。所以它不能被描述成某个直观的数字,但可以拥有多个等级。

c)信任是不确定的。因为一个信任实体不可能从信任评价系统中获取所有的信任信息,而且这些信任评价的结果也不总是确定的。

d)信任是非对称的、多变的且广泛传播的。信任的评价可以在一定范围内影响到这个实体的下一步动作。

e)信任的可传递性。有些学者相信信任是可以传递的,就像在现实世界里,陌生人之间能够通过某个中间信任关系相互交流,但有些则持反对意见。如若 I 信任 J 且 J 信任 K,并不能得出 I 信任 K。随着信任的分布式计算的进一步研究,有学者指出,在添加某些限制性条件的情况下,信任可以做到某种程度的传递。例如 Josang 模型中[8],如果 J 向 I 推荐 K,那么 I 可以在某种程度上信任 K,这就意味着信任已经被传递了。但是,这种信任的传递削弱了信任的可信度。基于以上分析,本文给出了关于信任传递时的定义:

定义 1　信任传递

$$\text{If } I \xrightarrow{T_{ij}} J,\ J \xrightarrow{T_{jk}} K,\ \text{and } J \Rightarrow K;\ I \text{ then } I \xrightarrow{T_{ik}} K,$$
$$\text{and } T_{ik} = f(T_{ij}, T_{jk})\ T_{ik} \leqslant T_{ij}, T_{ik} \leqslant T_{jk} \qquad (1)$$

其中:$I \xrightarrow{T_{ij}} J$ 表示,节点 I 信任节点 J,且其信任度为 T_{ij},,$T_{ij} \in [0,1]$;$J \Rightarrow K$:I 表示,J 向 I 节点推荐了节点 K,且 J 对 K 的推荐信任度为 T_{jk},$T_{jk} \in [0,1]$。

进行访问控制的目的是为了保护信息的安全性和完整性[9]。因此,在访问控制的范围内,信任可以看成是一种为了保护信息的安全性和完整性而特殊分级的主观概率实体。

在一些特殊的背景下信任的语义可以更好地描述其属性。保护信息的安全性和完整性的能力将是信任的两个最重要的属性。除此之外,通过引用信任在人类社会中的评价机制,信誉也被作为信任的一种属性,用来反映其他人的意见对信任的影响。为了更加清楚地描述出信任的属性,可以把这些属性进一步划分成几个子属性。这些子属性的定义如下:

a)保护信息安全性的能力,包括以下几个子属性:保密的能力;规范的权限管理;自我保护的能力;在请求实体和被请求实体间有可靠的通信路径。

b)保护信息的完整性的能力,包括以下几个子属性:规范运作为实体能够按照预先定义好的方式运作;诚信即实体能够遵守其所承诺的行为;友善,即任何实体都不能攻击或者损害主实体。

1.2　P2P 系统中的信任图

在以群组为中心的 P2P 系统中,每个实体都有同其他实体的信任关系。如果一个实体集中的实体都被实体 I 直接信任,则该实体集称为信任组 I,记为 TrustGroup(I)。因为每个组中的实体也可能有它本身的信任组,所以信任组中的实体有可能是相交的,如图 1 所示。

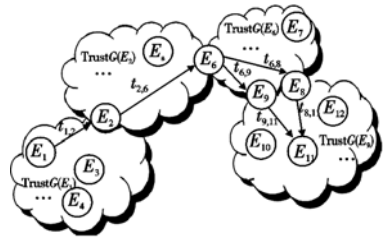


图1　实体间的信任关系

定义 2　信任链。有实体 I、J、K,如果($\exists J$)(($J \in$ TrustG(I)) $\wedge J \in$ TrustG(K) $\wedge J \Rightarrow C$:A),则,I、J、K 是一条信任链,记做 TrustChain(I,J)。

定义 3　信任图。所有从实体 E_i 到实体 E_j 的信任链构成了一个有向图,这个有向图是由顶点集 E 和顶点间的弧组成,记做 TrustGraph(E_i,E_j)。$E_p \xrightarrow{T_{pq}} E_q$ 表示从 E_p 到 E_q 的弧。

1.3　信任度的访问控制框架

在 P2P 社会网络中,一个实体可以把自己拥有的特权委托给在一定条件下其所信任的实体,这样做的好处是可以使特权通过信任图进行传播,使得这个群组用户所拥有的资源可以动态扩大。如图 2 所示,在 DTD 中,被请求实体到请求者之间在信任图中所计算出来的信任度可以表示成其信任值,且这个信任值是用来作出访问决定的基础。

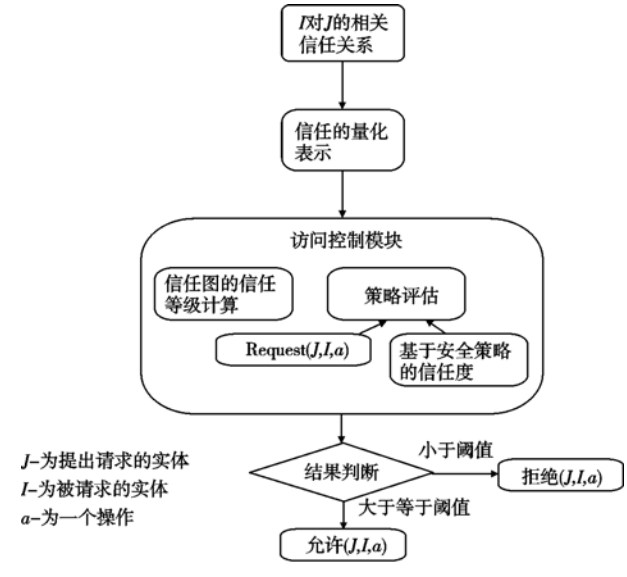


图2　动态可信度等级模型DTD

DTD 主要由三个功能部分构成,即信任的定量表示、基于信任度计算的信任图,信任评估策略。信任的定量表示功能代表了在 TrustGraph(I,J)中的直接信任。基于信任度计算的信任图功能把 TrustGraph(I,J)当做输入,计算 I 对 J 的信任值。

基于安全策略的信任度定义了请求者之间的信任值和资源的运作关系,其可以被描述成一个二元组:DTD _ Policy ($T_{阈值}$,operation a)。

这个二元组表示,如果请求者的信任值满足 $T \geqslant T_{阈值}$,则请求者所要求的操作 a 将被允许;否则,该操作将被拒绝。

评估策略功能:假设有请求 request(J,I,a),请求者的信任值为 T_{ij},为安全策略 DTD_Policy$_i$(T_0,o)输入。如果 T_{ij} 满足 $T_{ij} \geqslant T_0$,则请求 request(J,I,a)将被处理;否则请求 request(J,I,a)将被拒绝。

DTD 的核心是对信任的定量表达和在信任图上对信任值的计算。

2 动态可信度等级模型 DTD

2.1 信任的定量表达

在信任的定量表达上的主要障碍是:信任是模糊的,且不能作准确的界定和用正常的逻辑去分析。尽管模糊本身也是一种不确定性,但其并不等于随机的不确定性[10]。因此,仅在概率的基础上去描述信任是不那么合理的。1965 年,美国科学家 Zadeht 提出了模糊集理论,扩大了对数学的模糊概念,并且作为一种定量的模糊概念表达的有力工具被广泛接受。在本文中,模糊集是用于表达信任的基本理论,且用来表示信任的一些属性具有概率的不确定性。

在人类社会中,信任度的表示被分成了一些等级,如优秀、良好、一般等。为了准确表达信任的概念,定义了一个信任的向量。向量中的每个维度对应一个信任等级,且一个维度上某个实体的值代表该实体在这个等级中的关联度。

定义 4 信任向量。T 表示一个模糊集,D 表示一个由 n 个信任等级构成的评价集合:$D = \{D_1, D_2, D_3, \cdots, D_n\}$。定义信任实体 u 为一个信任向量,$T(u) = \{D_1(u), D_2(u), D_3(u), \cdots, D_n(u)\}$,$D_i(u)(i = 1,2,\cdots,n)$表示实体 u 在信任等级 D_i 中的关联度,$\sum_{i=1}^{n} D_i(u) = 1$,则 $T(u)$ 表示一个信任向量。

在本文中,关联度是可以直接通过信任等级的语义所指定的。评估集合 D 定义为 $D = \{D_1, D_2, D_3 D_4, D_5\}$,其中 D_1 = 差,D_2 = 较差,D_3 = 中等,D_4 = 良好,D_5 = 优秀。为了实现信任的定量表达,D_i 应该被量化表示。$D_i(i = 1,2,\cdots,5)$都是为了进一步描述信任向量 V_{Di}。其定义如下:

$$V_D = \{V_{D1}, V_{D2}, V_{D3}, V_{D4}, V_{D5}\} =$$
$$\{\{0.65, 0.35, 0.00, 0.00, 0.00\}, \{0.25, 0.50, 0.25, 0.00, 0.00\}, \{0.00, 0.25, 0.50, 0.25, 0.00\}, \{0.00, 0.00, 0.25, 0.50, 0.25\}, \{0.00, 0.00, 0.00, 0.35, 0.65\}\}$$

2.2 直接信任的表示

2.2.1 多等级综合评价模型

信任是一个复杂的概念,量化和评估信任自然也是一个复杂的过程。根据模糊集理论,模糊综合评估是一个解决复杂量化评估的有效方法。这个方法的主要思路是:首先分析能够影响评估结果的相关元素,然后评估每个元素,最后整合所有的评估结果获得最终定量评估的值。

因此,在本文中,信任的属性被描述成一种分层的结构,信任评价模型被定义成一种多等级的综合模型。信任的一个属性可以被看成一个元素,这些元素集被定义如下:

$$ET = \{ET_1, ET_2, ET_3\}$$

ET 是信任的相关元素的集合。

信息的安全性定义成元素集 ET_1 = Security = $\{s_1, s_2, s_3, s_4\}$ = {保密的能力,规范的权限管理,自我保护的能力,在请求实体和被请求实体间有可靠的通信路径};信息的完整性定义成元素集 ET_2 = Integrity = $\{\text{Int}_1, \text{Int}_2, \text{Int}_3\}$ = {规范运作,诚信,友善};信息的信誉定义成元素集 ET_3 = Reputation = {信誉}。

定义 5 多等级信任综合评估模型。该模型包括两个部分:

a)假设有 $ET_i(i = 1,2,3\cdots,n)$。用评估集 $D = \{D_1, D_2, D_3, D_4, D_5\}$ 对 ET_i 中的每个二级元素作评估,可以得到一个评估矩阵 $R = (r_{ij})_{n \times 5}$,$R$ 为一个模糊关系,表示每个元素 e_i 属于某个信任级别的可能性。ET_i 中元素的权值表示为 $W = \{w_1, w_2, \cdots, w_n\}$,且 $\sum_{i=1}^{n} w_i = 1$,二级元素的综合评估结果为 V_i,$V_i = \{v_1, v_1, \cdots, v_5\}$,且 $V_i = W \circ R$,$\circ$为合成运算。

b)在 V_i 基础上构成的评估矩阵 $R = [V_1, V_2, V_3]^{\mathrm{T}}$。设元素 E 的权值为 $W = \{w_1, w_2, w_3\}$,且 $\sum_{i=1}^{3} w_i = 1$。那么多等级信任综合评估的结果就为 V,$V = W_{1 \times k} \circ R_{k \times 5}$,$k = 1,2,3$。

在定义 5 中,合成运算“$\circ$”对结果有着很大的影响。而“$\circ$”有多种的执行方式,如 M($\wedge$,$\vee$),$M(\cdot, \vee)$,$M(\cdot, \oplus)$,$M(\cdot, +)$和 $M(\wedge, \oplus)$。

$M(\cdot, \vee)$中,“$\circ$”运算和做实数的乘法计算一样,“$\vee$”运算为扎德计算。因此,合成运算“$\circ$”在定义 5 中可以表示成如下形式:

$$V_j = \bigvee_{i=1}^{n} (w_i \cdot r_{ij}) (j = 1,2,\cdots,5) \tag{2}$$

2.2.2 信誉值的计算

请求者实体可以通过发送信任等级请求给他所交互过的其他实体,用来获得其想要了解的实体信誉值。请求者实体所获得的响应有可能是随机的,且响应的可靠性也不能保证,这就造成了信誉值评估结果的随机性和未确定性。借鉴其他的一些 P2P 信誉系统,本文用概率统计的方法来计算信誉值:

用 A 和 B 分别来表示请求者实体和被请求者实体,且 A 从其他 n 个实体获得了关于 B 的信任值评价。那么,A 对 B 的信誉值评价将为

$$B_{\text{reputation}} = \frac{\sum_{i=1}^{n} t_{i,B}}{n} \tag{3}$$

2.2.3 用层次分析法确定权重

在多等级综合评价模型中,元素权值的表示对模型的可行性有很大的影响。权值是一个模糊的概念,因此,如何确定它也是一个问题。有的方法建议,在有序加权多准则特征值的基础上进行多层次分析[11]。多层次分析法的原则是,在元素集

中比较任意两个元素的重要性,用所有的比较结果构造判断矩阵,然后计算判断矩阵中相应特征向量的特征根。特征向量表示的是所有元素的权重向量。判断矩阵的一致率由其最大特征向量表示,当一致率小于 0.10 时,从判断矩阵所得到的权向量才是合理的。由层次分析法可以客观地描述主观的概念,由其来决定的元素的重要性级别,比较符合人的思维和现实世界的习惯,所以该方法被认为是一种有效的方法。

在安全方面,信任元素的重要性主要取决于被保护实体的安全策略,而其安全策略又根据不同的安全目标而不同,且受到制定这些策略的人员所具有的经验所影响。例如,一些实体的安全目标强调的是信息的隐秘性,而有些实体却更关注于信息的完整性。因此,一个元素相关的隐秘性或者完整性可能在不同的情况下有不同的权值。

对于集合 $ET=\{ET_1,ET_2,ET_3\}=\{\text{Security},\text{Integrity},\text{Reputa tion}\}$,隐秘性和完整性分别对应了元素 Security 和元素 Integrity。在集合 $\text{Security}=\{s_1,s_2,s_3,s_4\}=\{$保密的能力,规范的权限管理,自我保护的能力,在请求实体和被请求实体间有可靠的通信路径$\}$中,s_1 和 s_2 是影响信息隐秘性的最重要元素,s_3、s_4 则次之。

基于以上的比较分析,可以建立一个判断矩阵,且用层次分析法可以获得集合 Security 的权重 W_{sec}:

$$W_{\text{sec}}=\{W_{s1},W_{s2},W_{s3},W_{s4}\}=\{0.347,0.527,0.075,0.050\}$$

在元素集 $\text{Integrity}=\{\text{In}_1,\text{In}_2,\text{In}_3\}=\{$规范运作,诚信,友善$\}$中,集合中的三个元素对信息的完整性而言都很重要,但是相比较而言,规范的运作对于完整性比诚信和友善要更加重要一点。因此,集合 Integrity 的权重 W_{inte}:

$$W_{\text{inte}}=\{W_{\text{In1}},W_{\text{In2}},W_{\text{In3}}\}=\{0.600,0.200,0.200\}$$

在元素集 ET 中,元素 Reputation 只是一个参照物而并非关键元素,而元素 Security 和 Integrity 显然比 Reputation 要重要,因此,应用层次分析法,可以获得 ET 的权重 W_{ET}:

$$W_{ET}=\{W_{ET1},W_{ET2},W_{ET3}\}=\{0.454,0.454,0.092\}$$

W_{sec}、W_{inte}、W_{ET}的一致率分别为 0.028,0,0,都小于 0.10,由此说明,这些集合的权重是合理的。

2.3　推荐信任的计算

在推荐信任中对信任向量的连接和组合是最基本的操作。连接将会减少被连接实体的信任值,其对应模糊集中的交操作;组合操作将会增加被组合实体的信任值,其对应模糊集中的并操作。在模糊集中,这些交和并操作是由多种计算器一起实现的。"∧"和"∨"即扎德(Zadeh)计算器,可以给出最大和最小操作数。扎德计算对某些应用来说显得太粗糙,因此,在扎德定理结构的基础上引入了三角范数和三角余范数。除了扎德计算器外,还有其他的细粒度计算器,如概率计算器、Einstein 计算器、Hamacher 计算器等。Einstein 计算器与其他的计算器相比较而言,粗糙度显得比较适中,其主要特征为:按照增强和递减规则进行信任向量的连接和组合,如下所示:

$$0\leqslant A(x)\varepsilon B(x)\leqslant\min(A(x),B(x)) \tag{4}$$

ε 表示 Einstein 交操作计算器。

$$\max(A(x),B(x))\leqslant A(x)\overset{*}{\varepsilon}B(x)\leqslant 1 \tag{5}$$

$\overset{*}{\varepsilon}$表示 Einstein 并操作计算器。

由此可见,Einstein 计算器是比较适合信任向量的连接和组合计算的。

设 A、B 为两个模糊集,则 Einstein 模糊计算器 ε 和$\overset{*}{\varepsilon}$可以定义为

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

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

$A(x)$ 和 $B(x)$ 分别代表模糊集 A 和 B 的关系度函数。

在本文中,操作"⊙"和"⊕"都是为了进一步描述信任向量的连接和组合操作。设有两个信任向量 $V_1=\{v_1^1,v_2^1,\cdots,v_M^1\}$,$V_2=\{v_1^2,v_2^2,\cdots,v_M^2\}$,应用 Einstein 计算器定义这两个信任项链的连接和组合操作如下:

V_1 连接 V_2:

$$V=V_1\odot V_2=\{v_1,\cdots,v_M\}=\{v_1^1\varepsilon v_1^2,v_2^1\varepsilon v_2^2,\cdots,v_M^1\varepsilon v_M^2\}$$

V_1 组合 V_2:

$$V=V_1\oplus V_2=\{v_1,\cdots,v_M\}=\{v_1^1\overset{*}{\varepsilon}v_1^2,v_2^1\overset{*}{\varepsilon}v_2^2,\cdots,v_M^1\overset{*}{\varepsilon}v_M^2\}$$

2.4　信任等级的计算

在 DTD 中,在请求者与被请求实体间的信任可以由推荐信任得到,且可以被信任图所描述。正如定义 3 所定义的那样,信任图是由节点间的反复连接和组合直接信任所得到,即如图 1 所示,且信任度的计算过程是相当复杂的。

对于一个信任图来说,如果把其中的弧看做运算对象,连接和组合操作看做运算符,那么这个信任图就可以看成一个表达式。假设进一步用数学方法对运算对象和运算符进行分析,那么对信任度的计算就可以转换成普通的表达式计算,这使得信任度的计算变得相对容易许多。

定义 6　信任弧

设在信任图 Trust$G(E_i,E_k)$ 中有节点集 E,$A\in E$,$B\in E$,$[A\to B,t_{AB}]$定义为一条从 A 到 B 的弧,其表示 A 信任 B 且信任度为 t_{AB}。$[A\to B,t_{AB}]$也可以表示成信任弧(A,B,t_{AB})的形式。信任弧可以被看成是信任链的一种特殊形式。

定义 7　弧的连接和组合

设"·"和"+"分别代表连接和组合操作,则对于$[A\to B,t_{AB}]$和$[B\to C,t_{BC}]$来说,$[A\to B,t_{AB}]\cdot[B\to C,t_{BC}]$表示在信任链 TrustChain$(A,C)$中,弧$[A\to B,t_{AB}]$通过节点 B 连接了弧$[B\to C,t_{BC}]$,且 TrustChain$(A,C)=[A\to B,t_{AB}]\cdot[B\to C,t_{BC}]=[A\to B\to C,t_{AB},t_{BC}]$。$[A\to C,t_{AC}]+[B\to C,t_{BC}]$表示$[A\to C,t_{AC}]$和$[B\to C,t_{BC}]$在节点 C 上进行了组合。

定义 8　信任图表达式

一个信任图 Trust$G(E_i,E_k)$ 可以被表示成由弧和"·""+""()"等操作所组成的表达式,定义这个表达式的形式为 exp(Trust$G(E_i,E_k)$):

$$\exp(\text{Trust}G(E_i,E_k))=(\text{TrustArc}(E_m,E_n),((),\cdot,+))E_m,E_n\in E$$

其中,操作的优先级顺序为:(),·,+。

以图 1 中所示为例,E_1 到 E_{11} 的信任图表达式为

$$\exp(\text{Trust}G(E_1,E_{11}))=[E_1\to E_2,t_{1,2}]\cdot[E_2\to E_6,t_{2.6}]\cdot$$

$$([E_6\rightarrow E_8,t_{6,8}]\cdot[E_8\rightarrow E_{11},t_{8,11}]+$$
$$[E_6\rightarrow E_9,t_{6,9}]\cdot[E_9\rightarrow E_{11},t_{9,11}])$$

如何生成信任图表达式是信任度计算的关键。因此,可以考虑在信任图 Trust$G(E_1,E_m)$中用一条虚拟的弧来迭代计算其表达式 exp(Trust$G(E_1,E_m)$)。

定义 9　虚拟弧

在信任图中,一个节点如果是一条以上弧的末端节点的话,称其为汇聚点。设 E_j 为一个汇聚点,E_1 为另外一个节点($E_1\neq E_j$),且 TrustArc(E_1,E_j)为一条从 E_1 到 E_j 的虚拟弧,则其定义如下:

$$\text{VTrustArc}(E_1,E_j)=[E_1\Rightarrow E_j,t_{1,j}]=\exp(\text{Trust}G(E_1,E_j))$$

VTrustArc(E_1,E_j)中的 E_1 和 E_j 对应信任图中的 E_1 和 E_j,信任度 $t_{1,j}$为 E_1 对 E_j 的推荐信任。随后的汇聚节点,如 E_k,假设 E_k 用 E_j 当做中间推荐节点,则 VTrustArc(E_1,E_j)就是构成 E_1 到 E_k 的信任图表达式 exp(Trust$G(E_1,E_k)$)的一部分。如果请求节点 E_m 是信任图 Trust$G(E_1,E_m)$中的终结汇聚点,则其信任图表达式 exp(Trust$G(E_1,E_m)$)将包含在该信任图中的所有迭代虚拟弧。虚拟弧的迭代算法描述如下:

a)对于信任图 Trust$G(E_1,E_m)$,其包括 m 个节点:

$$\text{TrustChain}_i(E_1,E_m);i=1,\cdots,k$$

可以通过正向或者逆向算法来搜索含有 k 节点的信任链。

b)在信任链 TrustChain$_i(E_1,E_m)$($i=1,\cdots,k$)中搜索从起始实体 E_1 到目标实体 E_m 的所有实体,并且在碰到最终汇聚节点 E_m 前反复执行以下操作:

(a)判断是否汇聚节点。如果发现在 TrustChain$_i(E_1,E_m)$($i=1,\cdots,k$)中,E_j 拥有两个以上不同的,那么 E_j 被判定为一个汇聚节点。

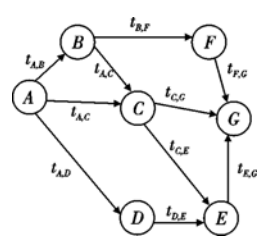
(b)定义虚拟弧。在信任链 TrustChain$_i(E_1,E_m)$($i=1,\cdots,k$)中,用虚拟弧 VTrustArc(E_1,E_j)代替信任链 TrustChain$_i(E_1,E_j)$($i=1,\cdots k$),并且移除重复的链。

c)如果 TrustChain$_i(E_1,E_j)$($i=1,\cdots,n$)中最后 n 条链($n\leqslant k$)中,都不包含任何汇聚节点,即可得到其信任图表达式 exp(Trust$G(E_1,E_m)$)。

d)对于每一个汇聚节点 E_j,$j\in[2,m]$,在 exp(Trust$G(E_1,E_m)$)中用 exp(Trust$G(E_1,E_j)$)代替虚拟弧 VTrustArc(E_1,E_j),这样就可以消除掉所有的虚拟弧并且得到最终的信任图表达式 exp(Trust$G(E_1,E_m)$)。

虚拟弧迭代算法首先用一个信任链集来表示信任图 Trust$G(E_i,E_k)$,然后找出汇聚节点并且在虚拟图 Trust$G(E_i,E_c)$中搜寻和操作这些信任链,其后用虚拟弧 VTrustArc(E_1,E_c)来替代它们。同时,在从起始节点 E_i 开始搜索操作的时候,为了避免过多的迭代操作,可以把信任链进行简化后再进行搜索和替代操作。因此,虚拟弧迭代算法可以很好地减小信任度计算的复杂性。

以图 3~5 为例可以进一步说明虚拟弧迭代算法。图 3(a)是一个从 A 到 G 的信任图,其包含七个节点。如图 3(b)所示,$A\sim G$ 之间有七条信任链。在信任链表达式中忽略了每条信任弧的信任度。



(a)

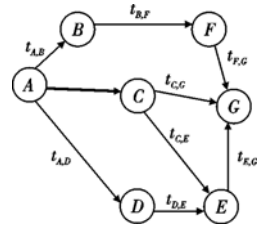
$\text{TrustChain}_1:[A\rightarrow B\rightarrow F\rightarrow G]$
$\text{TrustChain}_2:[\underline{A\rightarrow C}\rightarrow G]$
$\text{TrustChain}_3:[A\rightarrow D\rightarrow E\rightarrow G]$
$\text{TrustChain}_4:[\underline{A\rightarrow B\rightarrow C}\rightarrow E\rightarrow G]$
$\text{TrustChain}_5:[A\rightarrow B\rightarrow F\rightarrow E\rightarrow G]$
$\text{TrustChain}_6:[\underline{A\rightarrow C}\rightarrow E\rightarrow G]$
$\text{TrustChain}_7:[\underline{A\rightarrow B\rightarrow C}\rightarrow G]$

(b)

图 3　信任图 Trust$G(A,G)$和其包含的信任链

通过搜索七条信任链,第一个汇聚节点 C 被找到。在图 3(b)中相关的信任链已经被标记出来。信任图 Trust$G(A,C)$由两条被标记的信任链$[A\rightarrow B\rightarrow C]$和$[A\rightarrow C]$组成,如图 3(a)所示。然后,在此基础上就可以构建一条虚拟弧 VTrustArc$(A,C)=[A\Rightarrow C]$,并可以在信任链集中替代掉 TrustChain(A,C),替代后的结果如图 4(a)所示。

继续在图 4(a)中搜索信任链,并可以找到第二个汇聚节点 E。Trust$G(A,E)$在图 4(b)中已经标记,如图 4(a)中所示。



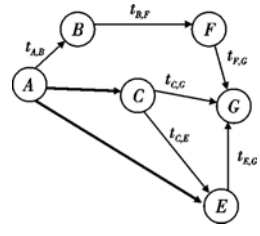
(a)

$\text{TrustChain}_1:[A\rightarrow B\rightarrow F\rightarrow G]$
$\text{TrustChain}_2:[A\Rightarrow C\rightarrow G]$
$\text{TrustChain}_3:[\underline{A\rightarrow D\rightarrow E}\rightarrow G]$
$\text{TrustChain}_4:[\underline{A\Rightarrow C\rightarrow E}\rightarrow G]$
$\text{TrustChain}_5:[\underline{A\rightarrow B\rightarrow F\rightarrow E}\rightarrow G]$

(b)

图 4　虚拟弧迭代算法的迭代过程

被标记的三条信任链可以组成新的虚拟信任弧 VTrustArc$(A,E)=[A\Rightarrow E]$,并也可以在信任链集中替代掉 TrustChain(A,E),这样就可以得到简化后的信任链,如图 5 所示。



(a)

$\text{TrustChain}_1:[A\rightarrow B\rightarrow F\rightarrow G]$
$\text{TrustChain}_2:[A\Rightarrow C\rightarrow G]$
$\text{TrustChain}_3:[A\Rightarrow E\rightarrow G]$

(b)

图 5　进行虚拟弧迭代算法后的最终结果

在图 5(a)所示的信任链集中,不包含除了终结节点 G 外的任何汇聚节点。其信任图如图 5(b)所示。由此可以得到 Trust$G(A,C)$的信任图表达式为

$$\exp(\text{Trust}G(A,G))=[A\Rightarrow E\rightarrow G]+[A\rightarrow B\rightarrow F\rightarrow G]+$$
$$[A\Rightarrow C\rightarrow G]=[A\Rightarrow E]\cdot[E\rightarrow G]+[A\rightarrow B]\cdot[B\rightarrow F]$$
$$\cdot[F\rightarrow G]+[A\Rightarrow C]\cdot[C\rightarrow G]$$

虚拟弧$[A\Rightarrow C]$和$[A\Rightarrow E]$的信任图表达式如下:

$$[A\Rightarrow C]=\exp(\text{Trust}G(A,C))=[A\rightarrow C]+[A\rightarrow B]\cdot[B\rightarrow C]$$
$$[A\Rightarrow E]=\exp(\text{Trust}G(A,E))=[A\Rightarrow C]\cdot[C\rightarrow E]+[A\rightarrow D]\cdot$$
$$[D\rightarrow E]+[A\rightarrow B]\cdot[B\rightarrow F]\cdot[F\rightarrow E]$$

2.5　把信任图表达式转换成可计算的数学表达式

一个信任图表达式需要转换成可计算的数学表达式才能去计算信任度。所以在信任图表达式的基础上,定义了其转换

规则:从每条弧中提取信任度 t 用其替代这些弧本身的信任度,如弧[$A \rightarrow B, t_{A,B}$]可以用 $t_{A,B}$ 来替换。对式(1)中的信任图表达式,利用以上的转换规则可以得到其数学表达式:

$$t_{1,11} = t_{1,2} \cdot t_{2,6} \cdot (t_{6,8} \cdot t_{8,11} + t_{6,9} \cdot t_{9,11}) \quad (6)$$

在式(6)中关于信任度 $t_{i,j}$ 的"·"和"+"操作并没有确定。因此,可以通过定义不同的操作内容就可以应用于不同的信任度计算方法下,增强了其适用性。例如,在本文提出的信任度计算方法下,$t_{i,j}$ 被定义为信任向量 $V_{A,B}$,"·"和"+"操作被定义为连接⊙和并操作⊕。由此,得到式(6)在 $E_1 \sim E_{11}$ 之间的数学表达式为

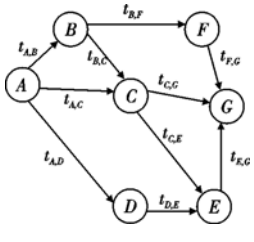
$$V_{1,11} = V_{1,2} \odot V_{2,6} \odot (V_{6,8} \odot V_{8,11} \oplus V_{6,9} \odot V_{9,11}) \quad (7)$$

通过计算式(7),就可以得到 E_1 到 E_{11} 的信任向量。

3　实验与结果分析

基于上文所述的 P2P 信任模型和对应算法,开发了 1 个 DTD 系统用于测试和分析信任计算模型。

以图3 所示信任图 Trust$G(A,G)$ 为实验实例,信任图节点间的信任向量已给出,如图6(b)所示。当 G 发送一个交易请求给 A 后,A 就开始在信任度计算模型 DTD 下利用信任图 Trust$G(A,G)$ 计算对 G 的信任度。其计算过程和结果如图7 所示。



(a)

$t_{AB} = [0.0283, 0.0567, 0.1338, 0.3756, 0.4053]$
$t_{AC} = [0.0300, 0.0925, 0.2125, 0.3599, 0.3051]$
$t_{AD} = [0.1304, 0.1621, 0.2100, 0.2954, 0.2735]$
$t_{BC} = [0.1897, 0.1337, 0.1253, 0.2776, 0.2735]$
$t_{BF} = [0.2220, 0.1972, 0.1277, 0.2003, 0.2526]$
$t_{CG} = [0.0395, 0.2384, 0.3810, 0.2422, 0.0987]$
$t_{DE} = [0.0085, 0.0792, 0.2895, 0.4053, 0.2174]$
$t_{EG} = [0.0394, 0.1102, 0.1847, 0.3241, 0.3413]$
$t_{FE} = [0.0010, 0.0828, 0.3016, 0.3959, 0.2196]$
$t_{CE} = [0.2265, 0.2074, 0.1023, 0.1883, 0.2753]$
$t_{FG} = [0.0227, 0.0848, 0.2072, 0.3591, 0.3260]$

(b)

图6　信任图 Trust$G(A,G)$ 及其节点间的信任向量值

图7　信任度的计算过程及结果

如图7 所示,通过逆向搜索算法找出从 A 到 G 的七条信任链;利用虚拟弧迭代算法获得其信任图表达式 exp(Trust$G(A,G)$),虚拟弧 TrustArc(A,C) 和 TrustArc(A,E) 在图7 中用"#C"和"#E"表示。在得到 Trust$G(A,G)$ 的信任图表达式后,可以转换成由信任向量和"⊙"计算和"⊕"计算所构成的可计算的数学表达式。通过计算就可以得出信任向量 $V_{A,G} = [0.1439, 0.1161, 0.1375, 0.3074, 0.2951]$ 和其信任度 $t_{A,G} = 0.8282$。

在上述实验中,如图6(b)所示,按照本文 2.1 节中的划分,有四条信任链获得了"优秀"的信任等级评定,五条信任链获得了"良好"的信任等级评定,只有两条信任链被评为"中等"和"较差"。在计算结果中 $t_{A,G} = 0.8282$,属于等级"良好"。通过图2 中 DTD 模型的描述可知,$t_{A,G}$ 将被输入判断模块中。假设 A 的安全策略为 DTD_Policy(0.6, operation x),这就意味着只有当请求者的信任度不小于0.6 时,其请求的操作 operation x 才会被允许执行。而 $t_{A,G} = 0.8282$,因此,来自陌生实体 G 的交易请求将会被允许执行。

4　结束语

在本文中,实现了一个基于模糊理论的动态可信度等级模型 DTD。该模型在对信任的过程进行了语义描述的基础上对信任进行了细粒度的访问控制,并通过分析信任的模糊性和不确定性,在模糊集理论和概率论的基础上建立了一个对直接信任度的多级别综合评价方法用来表示直接信任和间接信任。通过运用层次分析法获得元素的权值,并结合信任度传递的计算方法计算其最终的信任度。

参考文献:

[1] 窦文. 信任敏感的 P2P 拓扑构造及其相关技术研究[D]. 长沙:国防科学技术大学,2003.

[2] KRISHNAN R, SANDHU R, NIU J, *et al*. Formal models for group-centric secure information sharing, S-TR-2009-002[R]. San Antonio: Department of Computer Science, The University of Texas, 2009.

[3] BLAZE M, FEIGENBAUM J, LACY J. Decentralized-trust management[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1996, **10**(5): 164-173.

[4] HERZBERG A, MASS Y, MIHAELI J, *et al*. Access control meets public key infrastructure, or assigning roles to strangers[C]//Proc of IEEE Symposium on Security and Privacy. California: IEEE Computer Society, 2000: 2-14.

[5] 吴鹏,吴国新,方群. P2P 网络信誉机制研究综述[J]. 计算机科学,2009, **36**(6): 26-28.

[6] GAMBETTA D. Trust: making and breaking cooperative relations [M]. Basil Blackwell, 1988: 213-237.

[7] HARDIN R. The street-level epistemology of trust[J]. Polit Society, 1993, **21**(4): 505-529.

[8] JOSANG A. The beta reputation system[C]//Proc of the 15th Eletronic Commerce Conference. 2002: 324-337.

[9] HUANG J, NICOL D. A calculus of trust and its applications to PKI and identity management[C]//Proc of the 8th Symposium on Identity and Trust on the Internet. New York: ACM Press, 2009: 23-37.

[10] ZADEH L A. Fuzzy sets[J]. Inf Control, 1965(8): 338-353.

[11] GUO Y J. Theory, method and application of comprehensive evaluation [M]. Beijing: Science Press, 2007.

[12] 刘亮,周兴社,秦峰. Peer-to-Peer 计算模型及其安全对策[J]. 计算机应用研究,2003, **16**(3): 78-81.

[13] 朱俊茂,杨寿保,樊建平,等. Grid 与 P2P 混合计算环境下给予推荐证据推理的信任模型[J]. 计算机研究与发展,2005, **42**(5): 797-803.

[14] 张骞,张霞,文学志,等. Peer-to-Peer 环境下多粒度 Trust 模型构造[J]. 软件学报,2006, **17**(1): 96-107.

[15] 李之棠,祝幼菁,王阜东. 一种完全匿名的 P2P 网络信任模型[J]. 计算机工程与科学,2006, **28**(11): 9-15.