◎博士论坛◎

分布式网络环境下实体行为信任的评估方法

田立勤[1,3],林 闯[2],杨 扬[1]
TIAN Li-qin[1,3],LIN Chuang[2],YANG Yang[1]

1.北京科技大学 信息工程学院,北京 100083
2.清华大学 计算机科学与技术系,北京 100084
3.华北科技学院 计算机系,北京 101601
1.Information Engineering School,University of Science and Technology Beijing,Beijing 100083,China
2.Department of Computer Science and Technology,Tsinghua University,Beijing 100084,China
3.North China Institute of Science and Technology,Beijing 101601,China
E-mail:tianliqin@tsinghua.org.cn

TIAN Li-qin,LIN Chuang,YANG Yang.Behavior trust computation in distributed network.Computer Engineering and Applications,2008,44(17):1-5.

Abstract: With the development of the distributed network,more and more applications need to establish the trust,especially among the stranger entity,due to the complicated environment of the share resource.Because the share system is open,dynamic and uncertain,so it is difficult for the nodes to master all the security information,which leads to the undependability and security threat.So far,some of the trust model has been given,but they still have some limitations.Some model don't distinguish trusted-evidence from the no trusted-evidence,it may cause the cheating from the malice node; Some model only update node's trust and ignore updating of the recommendation-node's trust which not only don't punish the cheating of the recommender but also don't encourage the recommendation.So how to get a comprehensive computation of the trust,which embodies the characteristic of the trust,still is an important thing to research.Comprehensive methods of trust computation,such as updating of the evidence and recommender's trust,direct trust computation and recommendation trust computation,are discussed.Also the authors discuss the trust recommendation structure such as sequent,parallel,sequent-parallel and network structure.The trust evaluation in this paper,which can keep down the cheating and reflects the trust characteristic such as subjectivity,dynamic,no-transitivity and so on,is practical and scalable.The authors also give a new notion of the homogeneous recommender and heterogeneous recommender,by distinguishing the two kinds of the recommendation,can get more accurate trust evaluation.

Key words: distributed network;computation of the behaviour trust;analysis of the trust

摘 要:随着分布式网络的发展,网络的资源环境变得越来越复杂和难以预测,使得越来越多的应用需要建立信任,特别是在本来互不相识的实体之间建立信任。主要给出了较全面反映信任特性的信任计算方法,首次给出了证据更新的计算方法,在此基础上给出了基于客观证据的直接信任、推荐信任和推荐者自身信任更新的计算公式,并在计算中增加了可信度因子,使得通过计算得到的信任自包含可信度;提出了同构推荐者和非同构推荐者的概念和基于这两者的不同的信任计算方法,提高了信任评估的可信度;论述了信任推荐的4种拓扑结构及其计算方法。最后分析了计算方法体现出信任的主观性、动态性、非传递性和受历史影响等特性。方法具有实用、防欺骗和可扩展特点,可直接用来指导实际网络的信任计算。

关键词:分布式网络;行为信任计算;信任分析
DOI:10.3778/j.issn.1002-8331.2008.17.001 **文章编号:**1002-8331(2008)17-0001-05 **文献标识码:**A **中图分类号:**TP393

基金项目:国家重点基础研究发展规划(973)(the National Grand Fundamental Research 973 Program of China under Grant No.2006CB708301);国家自然科学基金(the National Natural Science Foundation of China under Grant No.60673187);教育部科技创新培育重点项目(No.707005);诺基亚研究生科研创新基金;河北省科学技术研究与发展指导计划项目(No.07213570)。

作者简介:田立勤(1970-),男,副教授,博士研究生,硕士生导师,研究方向是计算机网络,工作流模型,网络安全和可信网络;林闯(1948-),男,教授,博士生导师,主要研究领域为计算机网络系统性能评价、随机Petri网、可信网络与可信计算等;杨扬(1955-),男,教授,博士生导师,主要研究领域为计算机网络,多媒体通信和图像处理等。

收稿日期:2008-02-04 **修回日期:**2008-03-13

1 引言

在日常生活中,信任决择几乎每天都要发生。在分布式网络环境中,网络实体之间也存在着信任关系,同样需要进行信任抉择,如何确认实体间的信任关系已成为分布式网络环境下的一个重要的研究内容,也是近年来许多网络研究者的研究热点[1-4]。信任不仅包括对实体身份的信任,也包括对实体行为的信任[5,6]。传统的安全机制被用来提供授权和认证,解决了身份信任的问题,但并不能处理行为信任。

分布式网络资源共享环境是开放的、动态的,不确定的,这些特性使得主体之间不可能完全相互掌握所有的安全信息,因此导致了协作的不可靠性,增加了更多的安全威胁。但对于每个实体,调用可信任的资源以保障正常使用是最基本的要求之一,因此需要在实体间建立信任关系,特别是在陌生实体之间建立信任关系,并依此来指导实体间的协作策略。

信任是一个复杂的概念,来源于社会科学中,难于严格的定义。在信息技术里,信任可以定义为:在一个特定的环境里对一个实体行为的可靠性、安全性、可依赖性和能力的一种信念[7]。它涉及到对实体的安全性、可靠性、性能和服务价格等诸多方面的信念,信任使得被信任者能够使用或操作信任者所拥有的资源或者影响信任者是否使用被信任者提供的服务。信任的特性有:(1)主观性;(2)动态性;(3)非传递性;(4)受以前交往历史的影响性[8]。

目前虽然一些相应的计算模型已经提出,但都不够理想,有的计算方法不具有信任"慢升快降"的特征,不能体现"日久见人心"的信任原则和防止恶意实体的欺骗[9];有的只对需要交往的实体进行信任评估,忽略了推荐者的信任更新,没有把推荐者的推荐与它自身的信任关联起来,从而可能出现推荐欺骗,同时也不能起到激发推荐者推荐积极性的作用[10];有的没有考虑信任的主观特性,没有区分同构推荐者和非同构推荐者,严重影响了推荐信任可信度[4]。所以如何根据行为证据给出简单实用、有效全面的信任评估方法仍是一个重要的研究问题。给出了较全面反映信任特性的信任计算方法,包括证据更新、直接信任评估、间接信任评估和推荐者信任更新的计算公式,方法较全面体现了信任的主观、动态、非传递以及受交往历史影响等特性、具有简单实用、防欺骗和可扩展等特点,可直接用于指导实际网络的信任计算。

2 行为证据的更新计算

所有实体信任的建立、管理、更新和维护都直接或间接地建立在各种行为证据基础之上的,所以如何获得行为证据,证据的数据结构,证据的计算、更新等都会直接影响到信任评估的可信度、性能和可扩展性。因此,行为证据是计算实体信任的基础,实体间建立信任就是通过证据的不同组合来表达对某一有实际意义行为的信念,如,要求高安全中等性能且低费用的数据传输的信任路径选择等,下面首先给出行为证据的概念。

定义 1 行为证据是指实体可直接检测获得的或经过简单计算获得的用来评估与其交往的其他实体的某一属性(如性能属性,安全属性,可靠性属性等)的基础数值,也是进一步用来评估其他实体整体信任的依据,本文用 et 表示。常见的证据有:服务响应时间,数据传输率,连接建立延迟,传送延迟,连接释放时延等,根据需要还可以加入和删除其他证据。

证据的获取可以利用像网络流量检测[7]以及入侵检测[8]等系统得到,本文不作为讨论的重点。本文证据的数据结构只包括实体需要考虑的各种在[0,1]范围之内的原证据、当前证据,参见表 1,该表并不保留每次实体交往的所有证据,所以具有可扩展性。原证据初始值可取最低默认值 $thr0$。根据当前证据来更新原有的证据,这样来动态地维护实体间的证据更新。最后一列是实体之间的交往时间,它作为计算实体间在长时间没有交往时,信任随时间推移逐渐减小的依据。在该表中暂时只考虑了数据完整性,响应时间,数据传输率和时延等证据,根据不同的需要其他的证据项也可加入,w_i 是计算信任和属性的权值。

表 1 实体证据的数据表

证据名称	数据完整性	响应时间	带宽	…	时延	交往时间
原证据值 et_{old}	et_{old_1}	et_{old_2}	et_{old_3}	…	et_{old_m}	以前的平均时间 t_{ave}
各项权值 w_i	w_1	w_2	w_3	…	w_m	
当前证据值	et_{new_1}	et_{new_2}	et_{new_3}	…	et_{new_m}	当前时间 t_{cur}

每一个证据的更新都是在原证据的基础上进行的,初始原证据可以取最低信任临界值 $thr0$,根据当前交往所检测到的新证据的值来更新原有的证据,如果新的证据大于原有的证据,则证据增加,否则减少。浮动值的大小是以新证据值与原有证据的差为基数来计算的,证据更新计算方法见公式(1)。

$$et'_{new}=\begin{cases}et_{old}+et_{old}\times(et_{new}-et_{old})\times\beta^{(et_{new}-thr0+\frac{1}{n})} & et_{new}\geqslant thr0\\ et_{old}+et_{old}\times(et_{new}-et_{old})\times\beta^{(et_{new}-thr0)} & et_{new}<thr0\end{cases}\quad(1)$$

其中 et_{new},et_{old} 分别为新证据和原证据,et'_{new} 是更新后的证据,$thr0$ 为信任临界值,$0<\beta<1$ 是主观的信任调节因子,$\beta^{(et_{new}-thr0+\frac{1}{n})}$,$\beta^{(et_{new}-thr0)}$ 分别称为信任更新控制部分和非信任更新控制部分,n 是实体间交往的总次数。

此证据更新公式具有如下性质,用一个定理来描述:

定理 1 在新证据增长幅度相同的情况下,新证据在信任临界值之上的证据更新幅度一定小于新证据在信任临界值之下的证据更新幅度。

证明:设在信任临界值之上的新证据为 et^a_{new},在信任临界值之上的新证据为 et^b_{new},由已知得 $\left|(et^a_{new}-et_{old})\right|=\left|(et^b_{new}-et_{old})\right|$,并且有 $et^a_{new}>thr0>et^b_{new}$,则 et^a_{new} 和 et^b_{new} 证据更新增长幅度之比为:

$$\frac{\left|et_{old}\times(et^a_{new}-et_{old})\times\beta^{(et^a_{new}-thr0+\frac{1}{n})}\right|}{\left|et_{old}\times(et^b_{new}-et_{old})\times\beta^{(et^b_{new}-thr0)}\right|}$$

由于 $\left|(et^a_{new}-et_{old})\right|=\left|(et^b_{new}-et_{old})\right|$,所以 $=\left|\beta^{(et^a_{new}-thr0+\frac{1}{n})}\right|\Big/\left|\beta^{(et^a_{new}-thr0)}\right|$。

这是两个指数函数之比,由于 $0<\beta<1$,$et^a_{new}>thr0>et^b_{new}$,所以 $\left|\beta^{(et^a_{new}-thr0+\frac{1}{n})}\right|<1$ 而 $\left|\beta^{(et^b_{new}-thro)}\right|>1$,故 $\left|\beta^{(et^a_{new}-thr0+\frac{1}{n})}\right|\Big/\left|\beta^{(et^b_{new}-thr0)}\right|<1$。

定理 1 说明,在新证据幅度增长相同的情况下,如果新证据在信任范围内,则增长速度慢,体现"日久见人心"的信任原则,如果在不信任范围内,则信任下降速度加快,体现对不信任行为的惩罚力度。

β是主观的信任调节因子,当实体处在陌生的或者危险环境时,可以将β设置为较小的值,当处在高信任环境时,可以将β调高,这体现了实体为适应环境而采取的信任更新的主观特性。对于陌生实体或交往次数很少的实体信任建立开始会很缓慢(因为$\beta^{(et_{new}-thr0+\frac{1}{n})}$较小),随着交往次数的增多,$n$逐渐增大,信任的建立越来越容易(因为$\beta^{(et_{new}-thr0+\frac{1}{n})}$逐渐增大)。说明该计算方法具有自适应性。

3　基于AHP的直接信任计算

前面论述的是行为证据的更新方法,行为证据是软硬件直接测量获得的,具有客观性,但信任最初是从社会学衍生出来的,因此具有主观性,笼统性等特性,这种社会学科的信任不利于量化为网络实体的行为信任。为此,根据实际应用需求和功能特性将整体的实体行为信任进行逐层分解,将综合的、笼统的实体行为信任分解为若干行为信任属性,再将行为信任属性继续细化为可用软硬件直接测量的行为信任证据,这样可以有效解决可信网络中实体行为信任的笼统性和不确定性问题。例如将实体的行为信任划分为安全信任属性S,性能信任属性P等,根据要求还可以继续划分,如消费信任属性,可靠性信任属性等。

用矩阵的方法求实体的行为信任属性,设n表示实体行为信任包含信任属性的项数,p表示所有信任属性中包含信任证据项数的最大值,没有达到最大值p的可以让对应的权值为0,$et_{ij}\in[0,1]$表示第i个信任属性的第j个证据,$w_{ij}\in[0,1]$表示第i个信任属性的第j个信任证据的权值。

证据矩阵$\boldsymbol{E}=\begin{bmatrix} et_{11} & \cdots & et_{1f} & \cdots & et_{1p} \\ \vdots & & & & \vdots \\ et_{i1} & \cdots & et_{if} & \cdots & et_{ip} \\ \vdots & & & & \vdots \\ et_{n1} & \cdots & et_{nf} & \cdots & et_{np} \end{bmatrix}$,权值矩阵$\boldsymbol{WE}=\begin{bmatrix} w_{11} & \cdots & w_{1f} & \cdots & w_{1p} \\ \vdots & & & & \vdots \\ w_{i1} & \cdots & w_{if} & \cdots & w_{ip} \\ \vdots & & & & \vdots \\ w_{n1} & \cdots & w_{nf} & \cdots & w_{np} \end{bmatrix}$,这里的权值$w_{ij}$为0的可能性有:属性的证据项数没有达到最大值$p$或者服务提供者对相应的证据不感兴趣。计算信任属性的公式为$\boldsymbol{E}*\boldsymbol{WE}^{\mathrm{T}}$,结果只取主对角线值或只计算主对角线的值就可以了,这样就得到各个信任属性值了。有了信任的属性值,就可以计算信任了,设实体信任的属性向量$\boldsymbol{A}$为$\begin{bmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{bmatrix}$,信任属性的权值向量$\boldsymbol{WA}=\begin{bmatrix} w_1 \\ \vdots \\ w_i \\ \vdots \\ w_n \end{bmatrix}$,则实体行为信任的计算公式为:$\boldsymbol{beh}=\boldsymbol{A}*\boldsymbol{WA}^{\mathrm{T}}=(a_1\cdots a_i\cdots a_n)(w_1\cdots w_i\cdots w_n)=\sum_{i=1}^{n}a_iw_i$,在信任的计算中,如何科学确定证据和属性的权值是非常重要的,采用层次分析法(AHP)来确定这些权值和进行层次组合计算,更详细计算步骤请参考[11],这里不在赘述。

信任具有随时间衰减的特性,即,当实体之间长时间不交往时,信任会随着时间的流逝逐渐变小,引入时间衰减因子$\psi(t)$来表示这个特性,其中$t=t_{cur}-t_{ave}$,t_{cur}是当前发生交往的时间,t_{ave}是以前发生交往的平均时间,则随时间衰减的信任计算方法为:

$$trust\_dir_A^{new}(B)=trust\_dir_A^{old}(B)*\psi(t_{cur}-t_{ave})$$

在实际系统中$\psi(t)$可根据具体情况确定,例如令$\psi(t)=\frac{1}{\sqrt[6]{t}}$(天),计算结果见表2。

表2　一个随时间衰减的信任变化表

初始信任值	一个月后的值	3个月后的值	半年后后的值	1年后的值
0.9	0.51	0.43	0.38	0.34

4　考虑推荐者类型的间接信任计算

由于信任具有主观性,即使实体计算得到相同的信任值,由于不同的实体对权值的选择不同,所以信任的侧重点和本质可能相差很大。因此必须考虑推荐者类型是否相同,是否同构这个因素。

4.1　基于同构推荐者的间接信任计算

当一个实体想得到另一个陌生实体的信任值时,一种是给一个默认的最低信任值,慢慢谨慎接触(因为信任具有"慢升快降"的特性),通过不断交往获得信任,这种计算的缺点是信任的建立非常慢;另一种是从其他信任实体获得该陌生实体的信任值,从而可以快速得到该实体的信任值。计算信任值时不仅要考虑推荐者推荐的信任值,同时还要考虑实体对推荐者的信任程度以及实体是否与推荐者具有同构,先给出同构推荐者的概念。

定义2　同构推荐者是指请求推荐的实体与推荐者对被推荐者有相同的"评估类型",这包括两个方面的内容:首先有相同的评估证据,其次在计算信任时有相应的相同权值。由于信任具有主观性,不同实体评估的证据可以不同,权值可以不同,所以即使有相同的信任值其含义可能大不相同。这个条件要求推荐者关心的证据跟请求实体关心的证据相同且权值也相同。

如果同构推荐者有陌生实体的信任值称该推荐者为直接同构推荐者,如果该推荐者没有陌生实体的信任值,它需要再找其他实体继续推荐,这样就形成了一个推荐链(如图5所示),此时该推荐实体称为间接同构推荐者。

如果实体A有一个可信的同构推荐者M对实体B进行推荐,见图1,设推荐的信任值为$trust_M(B)$,则实体A通过推荐者M对实体B的信任值不仅与推荐值有关而且与对推荐者的信任有关,计算公式为:

$$trust_A(B)=trust_A(M)\times trust_M(B)$$

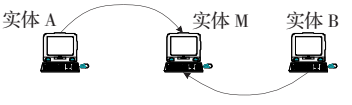

图1　实体A通过实体M对实体B的信任推荐

如果实体A还有陌生同构实体S的推荐,也同样可以用这个公式计算,不同的是要在二者之间加权值w_i,i=1,2,并且满足$w_1+w_2=1$,通常$w_1>w_2$,因为对自己信任实体的信任大于对陌生实体的信任,合起来的计算为公式(2):

$$trust_A(B)=w_1\times trust_A(M)\times trust_M(B)+w_2 trust_S(B) \quad (2)$$

其中$trust_S(B)$表示陌生实体对B的信任。

4.2　基于非同构推荐者的间接信任计算

上面讨论了如何根据同构推荐者推荐的信任值来评估信任值,这也是许多论文[9,10]都用的基于推荐的信任计算公式,这

些论文没有区分同构推荐者和非同构推荐者,但由于信任具有主观性,即使实体得到相同的证据值,由于不同的实体对证据权值的选择不同,所以计算的信任值可能相差很大。因此如果仅仅根据信任值的传递来计算推荐的信任值是有很大误差的,这时必须传递直接测量的证据值才能计算出真实信任值,对于非同构推荐者的计算需要先根据公式(2)计算出间接证据值(即把公式(2)中的信任值替换为证据值),再根据直接信任计算公式计算出综合信任值,基于非同构推荐者的信任计算流程图见图 3。由于额外传递的只是实 A 感兴趣的证据值,并不会带来太大的信息流量,故不影响信任评估的可扩展性。

性质 1　基于非同构推荐者的信任计算时,实体 A 先计算间接证据再计算组合信任和先组合证据再计算间接信任结果是相等的。

实体 A 先计算间接证据,再计算组合信任的公式为 $\sum_{i=1}^{m} w_{A_i}(trust_A(M)\times et_{M_i})=\sum_{i=1}^{m} w_{A_i}\times trust_A(M)\times et_{M_i}$,先组合证据再计算间接信任 $\left(\sum_{i=1}^{m} w_{A_i}\times et_{M_i}\right)\times trust_A(M)=\sum_{i=1}^{m} w_{A_i}\times trust_A(M)\times et_{M_i}$,两者相等。

4.3　多推荐者的间接信任计算

4.3.1　多推荐的推荐拓扑结构

多个推荐者组成的推荐拓扑结构有 4 种组合,第一种是全部由直接推荐者组成的并联结构,参见图 2;第 2 种是由多个推荐者组成的一条单独的串联结构,参见图 4;第 3 种是前两种结构的组合,它是多条串联结构的再并联,参见图 5,称为串并联结构,第 4 种是前 3 种结构的任意组合可以组成更复杂的推荐拓扑图,称为网状结构。

并行结构和串行结构都是串并联结构的特殊情形。例如,图 2 的并联结构可以看成是由 n 条最简单的只有一个推荐实体组成的串联结构组成的串并联结构。

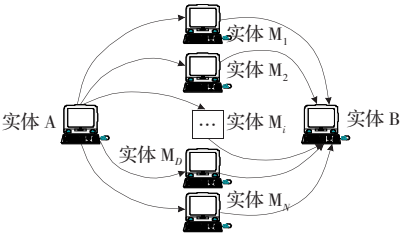

图 2　由 N 个推荐实体组成的推荐 B 的并联结构

4.3.2　并联推荐结构的信任计算

并联结构的信任计算有多种策略:乐观策略是在所有的 n 个推荐中取 $trust_A(K)\times trust_K(B)$ 的最大者,其中 $K=1\cdots n$;悲观策略是取所有的最小者,这两种策略由于太极端使用的场合较少,下面是两种不同的计算策略。

设有 n_1 个信任实体,n_2 个陌生实体组成的推荐 B 的并联结构,则算术平均策略的计算方法参见公式(3)

$$trust_A(B)=w_1\times\frac{\sum_{K=1}^{n_1} trust_A(K)\times trust_K(B)}{n_1}+w_2\times\frac{\sum_{S=1}^{n_2} trust_S(B)}{n_2}\quad(3)$$

一些论文[9,10]使用下面的加权平均策略公式来计算并行结构的信任 $trust_A(B)=w_1\times\frac{\sum_{K=1}^{n_1} trust_A(K)\times trust_K(B)}{\sum_{K=1}^{n_1} trust_A(K)}+w_2\times\frac{\sum_{S=1}^{n_2} trust_S(B)}{n_2}$,这将与信任的基本性质产生矛盾,用一个定理来分析。

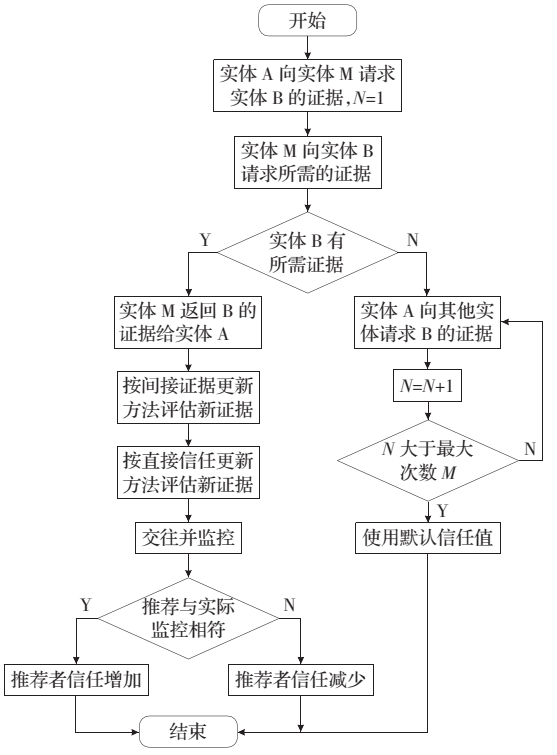

图 3　基于非同构推荐者的信任计算流程图

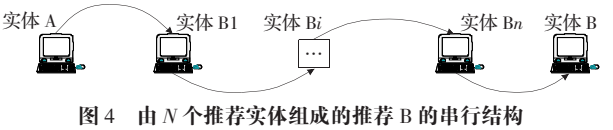

图 4　由 N 个推荐实体组成的推荐 B 的串行结构

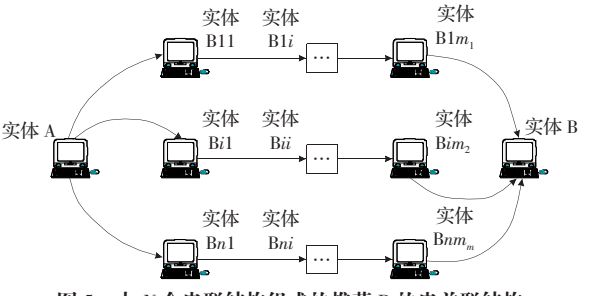

图 5　由 N 个串联结构组成的推荐 B 的串并联结构

从串并联结构和公式 $trust_A(B)=trust_A(M)\times trust_M(B)$ 中很容易看出下列性质:

性质 2　实体 A 对实体 B 的间接信任在推荐者 M 对实体 B 的信任不变的情况下与实体 A 对推荐者 M 的信任成正比,随着对推荐者信任的增加而增加的。

定理 2　基于加权平均计算策略的并联结构的信任计算是不符合性质 2 所述性质的,但基于算术平均策略的并联结构的信任计算是符合性质 2 所述性质的。

证明:设由 N 个分支组成的并联结构(参见图 2),A 对推荐实体 M_i 的信任值和 M_i 对的 B 信任值数据分别为 m_i,n_i,现计算 A 对 B 的信任。

按加权平均计算由 N 个分支组成的并联结构的信任为 $\frac{\sum_{i=1}^{N} m_i\times n_i}{\sum_{i=1}^{N} m_i}$,为了说明问题,设 $n_1=n_2=\cdots=n_N=n$,其计算结果为 n,

由于计算结果与 m 无关,所以即使增加实体 A 对推荐实体 M_i 的信任值 m_i,结果仍然是 n,这与性质 2 是矛盾的。

如果用算术平均策略计算,当 $n_1=n_2=\cdots=n_N=n$ 时,计算结果为 $\sum_{i=1}^{N} m_i\times n/N$,它是随着对推荐者信任的增加而增加的。所以只有基于算术平均策略所得到的信任是可用的。另外当并行结构只剩下一个分支时,这时并行结构就变为串行结构,设 $m_1=m_2=\cdots=m_N=m, n_1=n_2=\cdots=n_N=n$, 按串行结构公式计算结果为 $m\times n$,但按并行结构的加权平均计算时结果是 n,这说明特殊与一般的统一性在这个计算式是矛盾的。如果按算术平均计算,两者是统一的都是 $m\times n$。

由于算术平均固有的缺点, 当推荐值浮动很大的时候,算术平均策略就不能很好反映推荐的可信度,这时可以用方差对推荐值进行修正。

4.3.3　串联推荐结构的信任计算

串联结构的信任会随着信任的逐层推荐越来越低,是多个信任的累乘,其计算公式为:$trust_A(B)=trust(b_1)\times trust_{b_1}(b_2)\cdots\times trust_{b_n}(b)$。注意:串联结构的推荐会使信任降得很快,例如,设实体相互的信任值是 0.9,经过 5 个推荐者,信任值就低于 0.6,经过 10 个推荐者,信任值已经接近 0.3。

4.3.4　串并联推荐结构的信任计算

串并联结构的信任计算类似于并联结构,只不过和的每一项是由串联结构的计算得到:

$$\frac{\sum_{K=1}^{n} trust_A(B_{K1})\times trust_{B_{K1}}(B_{K2})\cdots\times trust_{BKn}(B)}{n}$$

4.3.5　网状推荐结构的信任计算

对于网状结构,通过将其中的结构并行分解,最终可以将复杂的网状结构分解为始端为 A 终端为 B 的串并联结构,所以仍然可以用串并联结构的信任计算公式计算。

4.4　基于激励机制的推荐者的信任更新计算

推荐者在充当推荐的中介作用时也应该对推荐的信任值的真实性负责,更不能欺骗,计算公式应该能体现这一个特性,思路是采用在每次推荐者推荐后,对推荐者的信任重新评估核实的方法来保证。如果被推荐对象的信任值和实际交往得出的结论相差很大,例如,假如推荐值是可信的,但实际交往中发现被推荐者是不可信的,则推荐者的信任值就会降低,反之,假如推荐值是可信的,实际交往中发现被推荐者也是可信的,则推荐者的信任值就会增加,这样既鼓励了推荐又避免了不负责任的推荐。推荐者新的信任值 rec_{new} 的计算见公式(4):

$$\begin{cases} rec_{old}+rec_{old}\times\beta_{inc}, \\ \quad rect(B), rt_A(B)>thr0, \text{或 } rect(B), rt_A(B)<thr0 \\ rec_{old}-rec_{old}\times\beta_{dec} \\ \quad rect(B)>thr0, rt_A(b)<thr0, \text{或 } rect(B)<thr, rt_A(B)>thr0 \end{cases} \tag{4}$$

其中,$rt_A(B)$是交往后得出的实际信任值,$rect(B)$是推荐的信任值。rec_{old}是原来推荐者的信任值。计算方法同样具有“慢升快降”的规则,即在公式中参数满足 $\beta_{inc}<\beta_{dec}$。

5　计算方法的特性分析

5.1　计算方法体现了信任特性

主观性:从公式(1)、直接信任计算公式和公式(4)可知,通过调整信任调节因子 β,参数 β_{inc} 和 β_{dec} 可以体现实体对信任和推荐者所持的乐观或悲观态度。通过调整权值 w_i 体现实体对信任的不同理解和有所侧重。

动态性:信任值随着实体间的交往不断的被新计算的结果所取代,这种动态变化不仅仅体现在直接交往的实体,同时也体现在推荐者的信任值的不断更新。另一个动态变化体现在实体在长时间不交往时信任会随时间的流逝而逐渐降低。

非传递性:即如果 A 信任 B,B 信任 C,A 并不一定信任 C。这是因为,一方面信任的传递会使信任降低,从而有可能降到低于信任的最低值,例如,假设信任的最低值是 0.5,低于 0.5 为不可信,并设 A 对 B 和 B 对 C 的信任均为 0.7,根据信任推荐公式 2,则 A 对 C 信任是 0.49,它属于不可信任范畴,因此 A 不信任 C。另一方面信任不仅仅只与某个实体 B 有关,还与其它实体的推荐有关,根据公式(3)可知,某个实体只在信任评估中占一小部分作用。

5.2　计算方法具有防欺骗性

计算方法具有防欺骗特性,这是因为:(1)是通过调节信任调节因子 β 来调节信任持续稳定增长,体现“日久见人心”的信任原则,而不是“一见钟情”的信任原则,防止低信任实体经过几次欺骗性的 “高信任交往” 后信任值很快上升的欺诈行为;(2)是通过对推荐者的信任进行更新的策略,防止推荐者的信任欺骗;(3)是在信任的计算中,通过增大大家共同推荐的平均值(也称信誉)的权值来达到“群众的眼睛是雪亮的”的信任规则,因为信誉值是众多实体共同评估得出的,不是个别实体评估得出的,所以有更高的可信度,从而防止了个别实体的欺骗行为(见公式(5))。(4)区分了同构推荐者和非同构推荐者,使得信任计算的可信度得到了提高。

5.3　计算方法的可扩展性和性能

信任评估具有可扩展性是因为实体只存储每个实体的原有的证据值和最近一次交往所得到的证据值,根据新证据值不断更新原有的证据值,并不保留每次交往的所有证据,所以具有可扩展性。另外,当某个实体的信任达到较高且稳定地维持在某个高度时,为了性能问题,不需要每次交往都更新信任值,可以间隔一段较长时间 Δt 再更新, 这样就可以提高整个信任评估系统的性能。

在实际计算中,要注意信任的涟漪问题。当一个实体想从其他信任实体中获得某个实体的信任值时,需要向所有信任关系的实体发出请求,这就像水中泛起的涟漪,如果这些邻居实体也不知道,就用同样的方法再泛起涟漪,这种计算信任值的方法可采用迭代的方法计算,每个涟漪的计算参见公式(3),当一圈一圈涟漪泛起时,这种迭代的计算量非常大,通常迭代的次数不要超过 6 次,否则不仅影响性能而且当迭代次数超过 7 次时,通过信任的传递计算的结果已经很低,不如直接使用初始默认的信任值进行计算。

前面讨论的是当实体 A 没有实体 B 的信任值时, 要向其他实体请求该实体的信任值,并通过上面计算公式计算出该实体的信任值。事实上,即使 A 有实体 B 的信任值,由于单独实体交往的次数和经验毕竟是有限的,因此得出的信任结论也是比较片面的,所以如果能从其他尽可能多的实体得到某个实体的信任值,那么信任值的可靠性就会大大提高。所以一个合理的计算方法是既要考虑到 A 对 B 的直接信任, 又要考虑其他实体对 B 的间接信任,综合二者,则 A 对 B 的总的信任值计算为公式(5),它由三部分组成,第一部分是直接信任,第二部分

(下转 48 页)