对等网络信任机制研究

李勇军 代亚非
(北京大学计算机科学技术系 北京 100871)

摘 要 对等网络环境下的信任机制是作为一种新颖的安全问题解决方案被引入的,基本思想是让交易参与方在交易完成后相互评价,根据对某个参与方(主体)的所有评价信息,计算该主体的信任度,为对等网络中其他主体以后选择交易对象时提供参考.文中介绍了对等网络环境下信任的基本定义.深入剖析了信任机制与网络安全的关系,并讨论了信任机制的体系结构.根据信任机制研究的内容分别归纳总结了信任模型和信任推理方法的最新研究成果,并选取典型的信任模型进行了评述.最后探讨了目前研究中存在的问题,并展望了需要进一步研究的方向.

关键词 对等网络;信任模型;推理方法;典型信任算法;网络安全
中图法分类号 TP311 **DOI 号**: 10.3724/SP.J.1016.2010.00390

Research on Trust Mechanism for Peer-to-Peer Network

LI Yong-Jun DAI Ya-Fei
(*Department of Computer Science and Technology, Peking University, Beijing* 100871)

Abstract The trust mechanism for peer-to-peer (P2P) network had been proposed as a promising methodology to handle the complex security problems. The basic idea of the trust mechanism for P2P network is to let parties rate each other after the completion of a transaction, and use the aggregated ratings of a given party to derive a trust score, which can assist other parties in deciding whether or not to transact with that party in the future. In this paper, firstly the concepts of trust mechanism existing in the P2P network are summarized and presented. Secondly the relationship between trust mechanism and network security is analyzed and the framework of trust system is discussed. Thirdly the latest techniques on trust model and trust inference method are summarized respectively. Finally several typical trust model systems and their mathematical inference methods are described in details. The current problems of trust mechanism for P2P network and research trends in this area are also discussed.

Keywords peer-to-peer network; trust model; trust inference; classic trust algorithm; network security

1 引 言

在对等(Peer to Peer,P2P)网络中,不同的节点(peer)间直接连接,交换数据和服务.由于具有开放、灵活与健壮等特性,P2P 系统逐渐成为互联网上重要的应用之一.而 P2P 系统的匿名性、动态性和开放性等特性,使其呈现出恶意用户入侵及理性用户(free-rider)大量存在等安全隐患或自私行为.如何实现一种机制将 P2P 网络中的不良用户进行隔离,规避此类用户带来的安全风险,是 P2P 网络安全面临的主要问题.目前解决此类问题的研究多

收稿日期:2007-12-29;最终修改稿收到日期:2010-02-25.本课题得到国家"九七三"重点基础研究发展规划项目基金(2004CB318204)、国家自然科学基金(60673183)和 IBM 大学合作研究计划(JSA200811009)资助.**李勇军**,男,1973 年生,博士,讲师,主要研究方向为 P2P 计算、信任与信誉机制、社交网络.**代亚非**,女,1958 年生,博士,教授,博士生导师,主要研究方向为 P2P 计算、分布式存储和社交网络.

集中在信任(trust)与信誉(reputation)机制研究方面. Marsh[1]首次系统地论述了信任的形式化问题，为把信任机制应用到计算机系统中奠定了基础. 文献[2]提出并解决了 P2P 环境下信任管理存在的一些问题，是较早把信任引入到 P2P 系统的文献之一. 信任机制根据用户历史行为，预测用户未来行为，辅助其他用户做出合适的选择，而达到抵制系统中恶意或不良行为的目的.

信任与信誉机制的主要内容包括收集系统中节点间的历史交易记录，根据收集到的交易记录计算每个节点的可信度，依据节点的可信度决定是否进行交易. 研究的要点有：(1) 信任与信誉的表示方法，描述在系统中如何表示节点的信任和信誉，是信任与信誉机制研究问题的核心组件；(2) 信任与信誉的计算方法，如何利用节点或者用户的历史交易信息评估其可信任的程度或信誉；(3) 信任与信誉值的存储方式，计算出的节点可信度在系统中如何存储，关系到如何获取节点的信任与信誉值. 本文将依据信任与信誉机制的研究要点介绍对等网络中信任或信誉机制的最新研究成果.

作为一种解决 P2P 网络中安全隐患的机制，信任与信誉机制研究已经成为 P2P 领域研究者共同关注的热点. 近年来国内外出现了许多这方面的研究文献，其中不乏一些综述性文献. 文献[3-4]简要综述信任与信誉机制的国内外的研究进展，文献[5-6]综述了在线交易系统中的信任与信誉研究，但没有反映国内的研究成果. 为深入理解信任与信誉机制和发展趋势，对国内外这方面的研究工作有一个总体上的把握，详细而全面地评述信任与信誉机制研究进展工作十分有意义.

本文阐述了信任与信誉的概念以及与网络安全之间的关系；重点依据信任与信誉研究的三个要点全面介绍了目前该项研究工作的最新成果；并对几种比较典型的信任与信誉机制进行了讲评；最后指出了目前研究工作中存在的一些问题，并对发展趋势进行了展望.

2　信任机制背景

在社会活动中，人们在交易之前通常会根据双方直接交易的历史记录或者朋友的推荐信息，对交易活动的可靠性进行评价，依据评价结果决定是否进行交易. 在对等网络环境中，信任与信誉机制需要解决的问题类似于社会活动中的可靠性评价. 在交易之前，借助信任机制，交易双方可以彼此了解对方的可信程度，从而提高交易的安全系数，避免交易过程可能出现的安全隐患.

2.1　基本概念

目前关于信任没有统一的定义，本文综合文献[5,7-11]，给出信任的描述性定义以及信任具有的一些性质，并列出与信任相关的一些基本概念.

定义 1.　信任(trust)是一种建立在已有知识上的主观判断，是主体 A 根据所处的环境，对主体 B 能够按照主体 A 的意愿提供特定服务(或者执行特定动作)的度量.

定义 2.　直接信任(direct trust)是主体 A 根据与主体 B 的直接交易历史记录，而得出的对主体 B 的信任.

定义 3.　推荐信任(recommendation trust)是主体间根据第三方的推荐而形成的信任，也称间接信任.

定义 4.　信任度(trust degree)是信任的定量表示，也称可信度.

图 1 描述了上述定义之间的关系. 实体 A 对实体 B 的直接信任度记为 T_{AB}，实体 B 对实体 C 的直接信任度记为 T_{BC}. 而在实体 A 与实体 C 之间由于不存在直接交易的历史记录，实体 A 为获得实体 C 的可信度，需要求助实体 B. 根据实体 B 的推荐，实体 A 可以获得实体 C 的推荐信任 T_{AC}.

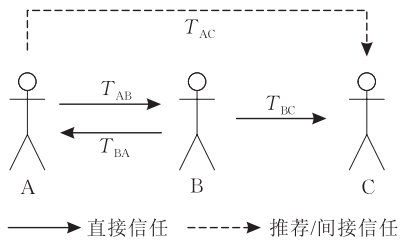

图 1　信任示例

信誉是一个与信任紧密相关的概念，但是信誉与信任又有区别. 为了说明二者之间的联系和区别，下面尝试给出对等网络中信誉的定义.

定义 5.　信誉是对节点已有服务的质量或特性的综合度量，反映节点履行其承诺服务的水平及网络中其它节点对其信任程度.

由此可见，信任是主动的，是一个主体对另一个主体某种能力的评价，建立在对历史交易的评估上；而信誉是被动的，是通过交互或资源共享的历史行为来预测该用户行为是否可信[10]，且信誉是可信信息的集合. 信誉是全局的概念，具有客观性，是网络中所有主体对某个主体评价的合计；而信任是局部

的概念,具有主观性,仅仅发生在两个主体之间.信任在一定程度上依赖于信誉,但是并不完全由信誉决定.图 2 为文献[10]中所列的 P2P 文件共享系统中的信任和信誉机制的关系图,图中 FP(file provider)为文件提供者.从图中可以看到信任和信誉机制的实现过程以及二者之间的关系.当一个 peer 要选择一个可信任的 FP 时,如果历史上曾有过与 FP 交互的经验,则在自己的可信 FP 数据库中找到一个可信度最高的 FP 与之交互;如果以前没有过与 FP 交互的经验或对 FP 了解较少,则从其他 peer 的推荐中,通过综合计算选择一个信誉值高的 FP 进行交互.通过这次交互的满意度对该 FP 进行评估,并更新对该 FP 的可信度,同时更新那些提供推荐的 peer 的可信度.这个实现机制有个前提假设就是信誉值高的 FP 的可信度也高.

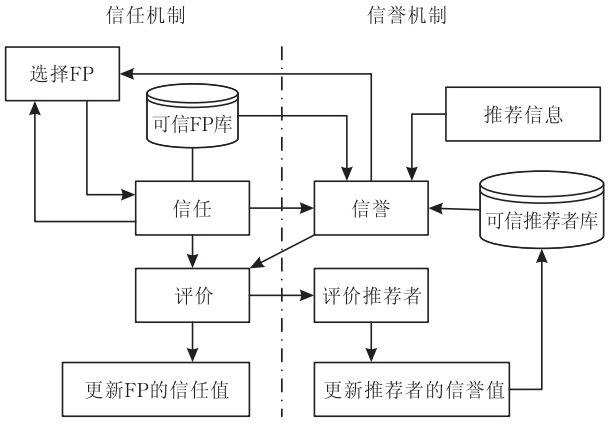

图 2 P2P 文件共享系统中可信和信誉机制

下面为了叙述简单,本文将信誉归为信任的概念中,认为信誉是信任的一种特殊情况,即信誉是网络中所有主体对某个主体的信任.在剩余部分除了特殊声明外,不刻意区分信任与信誉之间的差别.

2.2 信任机制与网络安全

通常来讲,网络安全的目的是提供一种保护机制,避免被保护的主体遭受恶意主体的攻击和非法存取.

在传统的网络安全机制中,被保护主体指的是服务提供者,恶意主体一般来自服务请求者.这种安全机制在文献[12]中被称为硬安全(hard security).信任机制提供的安全保护措施显然有别于传统安全机制所提供的,以文件共享系统为例说明,一个文件请求者(File Requestor,FR)在下载文件时,从多个候选 FP 中选择可信度最高的那个 FP 作为下载源.由此可看出,信任机制主要是保护 FR 的安全,避免 FR 下载到恶意文件.信任机制中的被保护主体是服务请求者;潜在的恶意用户是服务提供者.由信任机制提供的安全保护措施在文献[12]中称为软安全(soft security).表 1 中列举了传统安全机制和信任机制之间的区别.

表 1 信任机制与传统安全机制比较

	类型	被保护对象	潜在的恶意用户
信任机制	软安全	服务请求者	服务提供者
传统安全机制	硬安全	服务提供者	服务请求者

传统安全机制与信任安全机制之间也存在着联系.受传统安全机制保护的计算机或网络系统不易受到恶意节点的攻击,内部存在恶意程序(如木马)的可能性也会降低,此类系统的可信度就会高;相反那些没有安全机制保护的节点的可信度就会低.另外,在传统安全机制中也存在信任机制,主要依靠可信赖的第三方进行身份鉴别.这两种安全机制从不同的角度保护网络系统的安全,二者相互补充.

如同传统安全机制,随着用户对信任机制的了解,信任机制也受到一些恶意行为的干扰.这些恶意行为采用的方法主要表现为:(1)策略性地提供恶意服务;(2)提交虚假评价;(3)虚假推荐信任数据.恶意节点在实施上述方法是通常采用一定的策略来试图绕过信任机制,表现为不同的攻击行为,常采用策略主要包括:(1)行为摇摆,如先作为诚实用户提供服务,在得到信任后进行恶意行为,或者在小额交易上表现诚实而在大额交易上进行欺诈;(2)合谋作弊,如多个恶意节点联合进行欺诈,增加了行为隐蔽性;(3)利用多账号进行的攻击,造成此类攻击主要因为在对等网络中注册帐号基本上是无成本的以及网络中节点具有匿名性.这类攻击有女巫攻击(sybil attack)和漂白攻击(whitewashing).文献[4]对不同攻击行为进行了详细阐述和分类,针对每种恶意行为采取的抵抗策略进行了讲述.为使得信任机制能够更好的发挥其作用,在设计信任机制时需要了解各种恶意行为,并充分考虑抵抗恶意行为应采取的相应对策.恶意行为的存在也促进了信任机制的改进.

2.3 信任系统体系结构

信任系统体系结构主要说明评价数据以及可信度的存储方式,决定了主体之间的交互方式.目前主要有两种体系结构:集中式的体系结构和分布式的体系结构.本节只是简要介绍这两种不同的体系结构,详细的内容参见文献[5,11].

在集中式体系结构中,存在一个中心节点.每次

交易后，交易双方的相互评价都被送到中心节点. 中心节点根据收集到的所有评价信息计算每个主体的可信度，然后在中心节点公布，供其它节点在交易时参考. 这种体系结构优点是实现相对简单，由信任系统而引发的通信量较低；其缺点是系统过分依赖中心节点，中心节点是系统的瓶颈. eBay 中的信誉系统就采用了集中式的信任体系结构.

在分布式体系结构中，每次交易完成后，节点把交易评价存储在本地. 当一个节点需要计算另外一个节点的可信度时，首先从本地获得直接交易记录，计算对方的直接信任值. 如果两个节点之间不存在直接的交易记录或者直接交易的记录较少，就需要依靠邻居节点的推荐，而获得对方的推荐信任值. 一般来说，节点综合两种不同方式获取的信任值确定对方的可信度. 分布式体系结构的优点是消除了集中式结构中的瓶颈问题，鲁棒性更好；缺点是信任系统所引发通信量较大，通信协议也相对复杂. 现有的大多数信任机制采用了分布式体系结构.

3　信任值表示方法

信任值表示方法是指如何用数学的方法描述可信度的大小. 目前文献中出现的主要表示方法有：离散值、概率值、信念值、模糊值、灰色值以及信任云，其中后面 5 种表示方法反映了信任的不确定性.

3.1　离散信任值

人们比较习惯用离散变量表示信任的程度，因此很多文献[13-20]中采用了离散信任模型. 如文献[16]中，用 4 个离散值{G,L,N,B}表示请求服务的质量，每个值相应的服务质量描述如表 2. 主体在得到服务以后，根据自己的期望以及服务质量对服务进行评价，赋予服务表 2 中的某个值. 有些文献[17-19]仅用两个离散值{成功，不成功}量化服务的质量.

表 2　PET 模型中用到的 4 种不同的服务质量

服务质量	描述
好(G)	服务正确且服务质量好
一般 (L)	服务正确但服务质量欠佳，如服务不及时
未响应(N)	拒绝服务
拜占庭行为(B)	提供的服务是错误的甚至恶意的

离散信任值的优点是符合人们的表达信任的习惯，缺点是可计算性较差，需要借助映射函数把离散值映射成具体数值.

3.2　概率信任值

在概率信任模型[21-26]中，主体之间的信任度用概率值来表示. 主体 i 对主体 j 的信任度定义为 $\alpha_{i,j}\in[0,1]$，$\alpha_{i,j}$ 的值越大表示主体 i 对主体 j 越信任，0 表示完全不信任，而 1 则表示完全信任. 概率信任值一方面表示了主体之间的信任度，另一方面也表示了主体之间不信任的程度. 如 $\alpha_{i,j}=0.8$ 表示主体 i 对主体 j 的信任度为 0.8，不信任的程度为 0.2. 主体之间的信任概率可以理解为主体之间是否选择对方为交易对象的概率，信任概率低并不表示没有主体与之交易.

概率信任值的优点是有很多与概率相关的推理方法可以用于计算主体之间的信任度. 缺点是许多概率推理方法对一般用户来说，理解上有一定难度. 另外，该表示方法把信任的主观性和不确定性等同于随机性.

3.3　信念信任值

信念理论和概率论类似，差别在于所有可能出现结果的概率之和不一定等于 1，信念理论保留了概率论中隐含的不确定性[5,11]. 因为基于信念模型的信任系统在信任度的推理方法上类似于基于概率论的信任度推理方法，因此本文把信念信任值和概率信任值都归为概率型信任值.

文献[27-29]采用了信念表示主体的可信任度. 如在文献[27-28]中，引入 *opinion* 表示信任度，把 *opinion* 定义为一个四元组{b,d,u,a}. b,d,u 分别表示信任、怀疑、不确定. b,d,$u\in[0,1]$ 且 $b+d+u=1$. 主体的可信任度为 $b+au$，a 是一个系数，表示可信度中不确定所占的比例.

3.4　模糊信任值

信任本身就是一个模糊的概念，有些文献[30-38]用模糊理论来研究主体的可信度. 隶属度可以看成是主体隶属于可信任集合的程度. 模糊化评价数据以后，信任系统利用模糊规则根据这些模糊数据，推测主体的可信任程度.

文献[38]用多个模糊子集合 $T_i\in\mathcal{L}(X)(i=1,2,\cdots,n)$ 定义具有不同信任程度的信任集合. 如 $n=6$ 时，每个 T_i 的代表的信任集合的含义如表 3 所示.

表 3　6 种不同的信任模糊集合

模糊集	描述
T_6	完全信任
T_5	特别信任
T_4	很信任
T_3	信任
T_2	不太信任
T_1	不信任

因为这些模糊信任集合之间并不是非彼即此的

排他关系,很难说某个主体究竟属于哪个集合.在此情况下,用主体对各个模糊集合 T_i 的隶属度组成的向量描述主体的可信程度更具有合理性.如主体 x 的信任度可以用向量 $\boldsymbol{v}=\{v_0,v_1,v_2,\cdots,v_n\}$ 表示,其中 v_i 表示 x 对 T_i 的隶属度.

3.5 灰色信任值

灰色模型和模糊模型都可以描述不确定信息,但灰色系统相对于模糊系统来说,可用于解决统计数据少、信息不完全系统的建模与分析.目前已有文献[39]用灰色系统理论解决分布系统中的信任推理.

在灰色模型中,主体之间的信任关系用灰类描述.如文献[39]中,聚类实体集 $\boldsymbol{D}=\{d1,d2,d3\}$,灰类集 $\boldsymbol{G}=\{g1,g2,g3\}$,$g1,g2,g3$ 分别依次表示信任度高、一般、低.主体之间的评价用一个灰数表示,这些评价经过灰色推理以后,就得到一个聚类实体关于灰类集的聚类向量.如(0.324,0.233.0.800),根据聚类分析认为实体属于灰类 $g3$,表示其可信度低.

3.6 信任云

云模型是在模糊集理论中隶属函数的基础上提出来的[40-41],可以看作模糊模型的泛化.云由许多云滴组成.主体之间的信任关系用信任云(Trust Cloud)描述[42-43].信任云是一个三元组(Ex,En,Hx),其中 Ex 描述主体之间的信任度,En 是信任度的熵,描述信任度的不确定性,Hx 是信任度的超熵,描述 En 的不确定性.信任云能够描述信任的不确定性和模糊性.如文献[42]中,用一维正态云模型描述信任关系.设主体 A 对主体 B 的信任关系记为 $tc_{AB}=nc(Ex,En,He)$,$0\leq Ex\leq 1$,$0\leq En\leq 1$,$0\leq He\leq 1$.

4 信任计算(推理)方法

信任计算(推理)方法是指根据收集到的评价数据计算(推测)主体信任度的方法,计算(推测)方法不依赖于信任值表示方法.目前文献中常见到的计算方法有:加权平均法、贝叶斯方法、模糊推理方法以及灰色推理方法.

4.1 加权平均法

目前大多数信任机制采用此方法,包括一些经典的信任系统如 eBay①、Credence② 和 EigenTrust[23]等.该方法借鉴了社会网络中人之间的信任评价方法,其计算方法如式(1)所示.

$$T_{i,j}=\alpha\cdot(\beta\cdot R_d+(1-\beta)R_r)-\gamma R_i \quad (1)$$

其中 $T_{i,j}$ 表示主体 i 对主体 j 的信任值,R_d 是根据主体 i 与主体 j 之间的直接交易记录计算出的直接信任值,R_r 是主体 i 根据其他主体的推荐信息计算出的间接信任值,R_i 是交易带来的风险值,α、β、γ 分别表示不同的系数.

4.2 极大似然估计方法

极大似然估计方法(Maximum Likelihood Estimation,MLE)是一种基于概率的信任推理方法,主要适用于概率模型和信念模型.在信任的概率分布是已知而概率分布的参数是未知的情况下,MLE 根据得到的交易结果推测这些未知的参数,推测出的参数使得出现这些结果的可能性最大.如信任概率分布为 $p(x)$,主体 i 可信度为 t_i,主体 i 诚实推荐的概率等于其可信度,与主体 j 的交易结果为 $x_{i,j}$,主体 i 的邻居节点记为 $n(i)$,则 MLE 推测方法就可以归结为求解表达式(2)的最大值,

$$\max_{t_i}\arg\log\prod_{k\in n(i)}p(x_{i,k},t_i,l_k) \quad (2)$$

在文献[44]中,作者利用 MLE 方法估测主体的可信度.

4.3 贝叶斯方法

贝叶斯(Bayesian)方法是一种基于结果的后验概率(posterior probability)估计,适用于概率模型和信念模型.与 MLE 不同之处在于,首先为待推测的参数指定先验概率分布(prior probability),然后根据交易结果,利用贝叶斯规则(Bayes' rule)推测参数的后验概率.根据对交易评价可能出现的结果个数不同,为待推测参数指定的先验概率分布分为两种:Beta 分布和 Dirichlet 分布,其中 Beta 分布仅适合于二元评价结果的情况,是 Dirichlet 分布的一种特殊形式.限于篇幅,这里仅介绍基于 Dirichlet 分布的推理方法.

Dirichlet 分布适合于多元评价结果的情况,如表 2 所列的可能评价结果.假设评价有 k 种结果,每种结果出现的先验概率分布为均匀分布(uniform distribution),即每种出现的概率为 $1/k$.共有 n 次交易,且每次交易都给出评价,其中 $i(i=1,2,\cdots,k)$ 种评价出现的次数为 $m_i(\sum m_i=n)$.则待估测参数 p 的后验概率分布为

① http://pages.ebay.com/help/feedback/feedback-scores.html

② http://www.cs.cornell.edu/People/egs/credence/index.html

$$f(p,m,k)=\frac{1}{\int_0^1\prod_{i=1}^{k}x^{(m_i+C/k-1)}\mathrm{d}x}\prod_{i=1}^{k}p_i^{(m_i+C/k-1)} \quad (3)$$

其中，C 一个预先设定的常数，C 越大评价结果对参数 p 的期望值就越小，C 一般选为 k. 则第 i 种评价结果出现概率的 Bayes 估计期望值为

$$E(p_i)=\frac{m_i+C/k}{C+\sum_{i=1}^{k}m_i} \quad (4)$$

4.4　模糊推理方法

模糊推理方法主要适用于模糊信任模型. 图 3 是文献[37]中所述的模糊推理通用框架，分为 3 个过程：模糊化、模糊推理以及反模糊化. 模糊化过程把评价数据借助隶属函数进行综合评判，归类到模糊集合中. 模糊推理根据模糊规则推理主体之间的信任关系或者主体的可信度隶属的模糊集合. 推理规则示例如下所示：

IF *the Weighted Trustworthiness Value* is high
　AND *the Opinion Weight* is high
　AND *the Opinion Credibility* is high
THEN *Trustworthiness level* is high

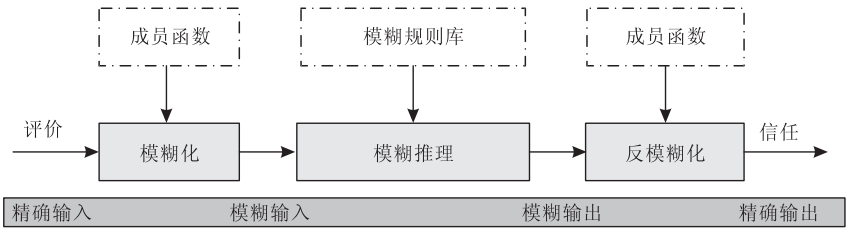

图 3　模糊推理的基本框架

形式化的推理规则可参见文献[38]. 反模糊化推理结果就可以得到主体的可信度.

4.5　灰色系统方法

灰色系统理论是我国学者[45]提出来的用于研究参数不完备系统的控制与决策问题的理论，并在许多行业得到广泛应用. 文献[39]提出了一种基于灰色系统理论的信誉报告机制，但目前基于灰色系统理论的信任机制研究还并不多. 基于灰色系统系统理论的推理过程如图 4 所示.

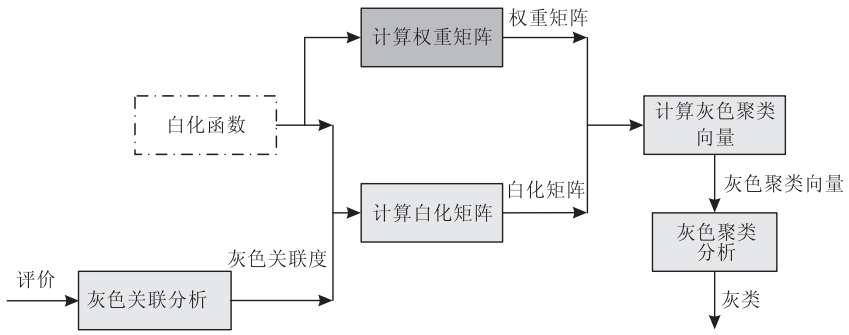

图 4　灰色推理的基本框架

在灰色推理过程中，首先利用灰色关联分析(Grey Relational Analysis)分析评价结果，得到灰色关联度(Grey Relational Degree)，即评价向量；如果评价涉及多个关键属性(比如文件共享系统中，对一个主体的评价可能涉及到下载文件的质量，下载速度等属性)，确定属性之间的权重关系；利用白化函数和评价向量计算白化矩阵；由白化矩阵和权重矩阵计算聚类向量，聚类向量反应了主体与灰类集(Grey Level Set)中每个灰类(Grey Level)的关系；对聚类向量进行聚类分析，就可以得到主体所属的灰类.

4.6　各种推理方法评述

加权平均法是目前研究中采用最多的信任计算(推理)方法，其主要特点是易于理解，方法简单且容易实现，对原始评价数据没有过多的要求.

极大似然推理方法和贝叶斯方法同属于基于概率论的推理方法. 概率论研究的是随机不确定现象的统计规律，目标是考察每种随机不确定现象出现结果的可能性大小，要求原始评价(样本)数据服从典型分布. 另外推理方法一般较为复杂，实现的系统复杂度较高.

模糊推理方法能够解决推理过程的不精确输入问题，简化推理过程的复杂性，推理过程容易理解. 但是选择隶属函数时，需要一定的先验知识.

灰色推理方法和模糊推理方法都可以解决含有

不确定因素的推理,灰色推理方法不需要先验知识,可以解决原始评价数据较少的信任计算问题,对原始评价数据没有过多的要求.

5 典型信任模型

许多学者使用不同的数学方法和工具建立了各种信任关系的模型.本节将根据其采用数学方法的不同,选取一些较新的典型的模型进行介绍和评述.

5.1 eBay 系统中的信任模型

eBay 系统中的信任模型(Trust Model in eBay System, TMBS)是目前应用比较成功的信誉系统之一,引起许多学者的关注.在 TMBS 中,每次交易完成以后,交易双方相互评价,评价信息主要包括正面评价(+1)、中性评价(0)、负面评价(−1)以及一个简短的对交易的评论(short comment),评论对信任值的计算没有影响.假设一次交易完成后,主体 i 对主体 j 的评价为 rt_{ij},则主体 i 信任值 $s_i=\sum_j rt_{ij}$.

TMBS 有一个集中式的体系结构,中心服务器用于存储和管理评价信息.其主要优点是算法简单易于实现,缺点是为考虑信任机制上下文以及对恶意评价的识别与惩罚.

5.2 EigenTrust 算法与 PowerTrust 算法

EigenTrust 算法[23]是一种利用信任的传递特性,由直接信任值计算全局信任值的信任算法.EigenTrust 认为直接信任值越高的节点推荐的信任值越可信,在计算全局信任时赋予较大权重.

假设节点 i 与节点 j 之间经过多次交易后,i 对 j 的直接信任为 s_{ij}.为降低恶意行为给算法带来的影响,EigenTrsut 对 s_{ij} 归一化处理.归一化后的直接信任值记为 c_{ij}.矩阵$[c_{ij}]$记为 $\boldsymbol{C}$.EigenTrust 利用式(5)经过多次迭代计算节点的全局信任值.

$$\boldsymbol{t}^{(k+1)}=(1-a)\boldsymbol{C}^{\mathrm{T}}\boldsymbol{t}^{(k)}+a\boldsymbol{p} \tag{5}$$

其中 $\boldsymbol{t}^{(k)}$ 是第 k 次迭代后的全局信任值向量,$\boldsymbol{p}$ 是可信节点的全局信任值.假设对等网络中节点数量为 n,其中可信节点数量为 m,则有 $t_i^{(0)}=1/n$,即节点全局信任值的初始值为均匀分布.如果节点 i 是可信节点,则 $p_i=1/m$;否则 $p_i=0$.EigenTrust 通过可信节点集合可以避免陷入合谋节点的恶意推荐的作弊圈套,使得每个节点的全局信任值都包含一部分来自可信节点的推荐信任值;另外也保证 C 的不可约性和非周期性,使得计算过程可收敛.

EigenTrust 在实现机制上提出了基于 DHT 的分布式计算方法.每个节点的信任值计算由其他节点来完成,这些节点为该节点的父节点.为防止父节点虚报问题,可以为节点指定多个父节点.

EigenTrust 的优点包括:(1)提出直接信任值越高的节点推荐的信任值越可信的思想;(2)算法和实现机制 d 都考虑了恶意行为对算法影响.其存在的缺点可以参见 PowerTrust 算法部分或文献[17,20].

PowerTrust 算法[20]从 3 个方面对 EigenTrust 算法的进行了改进:(1)可信节点集合的确定.PowerTrust 算法是通过对 eBay 中的评价信息进行分析发现节点间的评价存在的幂律关系,即存在少数 Power 节点,它们得到的评价数量显著地多于其它节点.PowerTrust 把这些 Power 节点组成可信节点集合,解决了 EigenTrust 算法预设可信节点在一些实际系统中缺乏可行性的问题;(2)迭代过程的收敛速度.在计算全局信任值过程中,PowerTrust 提出了向前看随机游走(Look-ahead Random Walk, LRW)的策略,每次迭代过程中,不仅考虑邻居节点的推荐信任值,而且考虑邻居的邻居的推荐信任,即信任矩阵 $\boldsymbol{R}=\boldsymbol{C}^2$.利用 LRW 策略使得迭代过程的收敛速度提高两倍多;(3)实现机制上.PowerTrust 借助 DHT 机制和 LPH(Locality Preserving Hashing)函数实现动态发现 Power 节点的方法,使 PowerTrust 能够适应节点的频繁加入和离开的动态环境.

PowerTrust 算法在抵抗恶意行为方面采取的机制类似于 EigenTrust 算法,但抵抗能力方面强于 EigenTrust 算法.这主要因为 PowerTrust 算法采用 Power 节点作为可信节点,这些 Power 节点相对于 EigenTrust 中的可信节点具有更高的可信度.

PowerTrust 算法主要优点体现在 EigenTrust 的改进上,其缺点包括:(1)计算信任值时没有考虑交易量大小,这容易使得恶意用户借助小额交易积累信任,而在大额交易上进行欺骗;(2)没有对恶意行为作出惩罚;(3)信任值没有体现评价的数量,恶意用户可采用多次正常交易掩盖其恶意行为.

5.3 PeerTrust 算法

PeerTrust 算法[26]利用反馈评价计算节点的直接信任值.算法提出了计算直接信任值时需要考虑的 5 个因素:(1)反馈评价,计算信任值需要的最基本要素;(2)交易的数量;(3)提供反馈评价的节点的可信度;(4)与交易相关的因素,如交易时间、交易额度等;(5)与交易环境相关的因素,如为提供反

馈的节点提供奖励等.结合上述要素，PeerTrust 给出计算信任值的模型，

$$T(u)=\alpha\cdot\sum_{i=1}^{I(u)}(S(u,i)\cdot Cr(p(u,i))\cdot TF(u,i))+\beta\cdot CF(u) \tag{6}$$

其中 $I(u)$ 节点 u 交易的数量，$p(u,i)$ 是第 i 次交易中与 u 进行交易的节点，$S(u,i)$ 是 $p(u,i)$ 在第 i 次交易后对 u 的评价，$Cr(v)$ 是节点的可信度，$TF(u,i)$ 是与节点 u 第 i 次交易相关的因素所产生的信任因子，$CF(u)$ 是与节点 u 相关的交易环境所产生的信任因素，α 和 β 是标准化信任值时的权重参数，且 $\alpha+\beta=1$.

PeerTrust 算法认为前 3 种因素是计算信任值的最基本要素，并对此进行了详细讨论.反馈评价是基于交易行为的，评价形式可以是多样性的，但计算信任值时需对评价进行归一化处理，即 $0\leq S(u,i)\leq 1$.参数 $Cr(v)$ 是评价 $S(u,i)$ 的可信任度，PeerTrust 介绍了两种度量方式：(1) 利用节点信任值作为计算 $Cr(v)$ 的依据，信任值越高的节点给出的评价越可信，这点类似于 EigenTrust 算法中的思想.(2) 利用两个节点评价相同交易的相似性计算节点的评价可信度，两个节点评价越相似，则对方的评价信息越可信.文献[19]度量评价权重时采用了相似度的思想.

在考虑后两种因素时，PeerTrust 认为对金额大、时间近的交易行为的评价赋予较大的权重在一定程度上可以抵抗恶意行为的破坏；奖励提供评价信息的节点，能够激励节点交易后积极反馈评价.

PeerTrust 抵抗恶意行为能力方面主要体现在：(1) 归一化评价信息可以避免恶意节点过高或过低的评价；(2) 计算信任时考虑交易数量可以避免恶意节点借助交易数量掩盖其恶意行为的目的；(3) 评价信息可信度可以降低恶意节点提供的评价在信任值计算中所在的比重；(4) 依据评价相似度度量评价的可信度还可以抵抗恶意节点的合谋攻击，因为恶意节点与正常节点间的评价相似度较低；(5) 计算信任值时考虑到交易额度可以防止恶意用户利用小额度交易积累信任而在进行大额度交易时进行欺骗的行为，考虑交易时间可以防止恶意节点在积累到一定信任后进行欺骗的行为；(6) PeerTrust 提出通过比较不同时间窗口内的信任值变化识别节点交易中是否存在恶意行为；(7) 借助 PKI 和数据副本技术可以保证评价数据的安全.

PeerTrust 的主要优点体现在对恶意行为的抵抗能力方面，另外还提出了激励用户提供评价信息的机制.不足之处主要包括：(1) 没有考虑对恶意行为的惩罚；(2) 未考虑大规模 P2P 环境下的计算收敛速度问题[20]；(3) 在大规模环境下，评价信息可能显得较为稀疏，利用相似性计算节点可信度时就会引起较大的误差.

5.4　基于信誉和风险评价信任算法

文献[46]提出一种基于信誉与风险评价的 P2P 系统信任模型 R²BTM(Reputation and Risk evaluation Based Trust Model)，该模型考虑到节点的动态行为影响信任度计算的不确定性，引入风险因素，并提出采用信息熵理论来量化风险，将实体之间的信任程度和信任的不确定性统一起来.

在 R²BTM 中，节点信任度是由信誉值和风险值两部分组成.用 T_{ij} 表示节点 i 对节点 j 的信任度，RE_j 和 RI_j 分别表示节点 j 的信誉值和风险值.α,γ 分别是两者的权重，则信任度 $T_{ij}=\alpha RE_j-\gamma RI_j$，$0\leq\alpha,\gamma\leq 1$.

信誉值 RE_j 由两部分组成：局部信任 R_{ij} 和推荐信任 AR_j.局部信任 R_{ij} 根据节点 i 与节点 j 之间的直接交易记录计算，在计算时引入了与时间相关的衰减函数.把节点 i 与节点 j 直接的交易分为 n 个交易时间段，R_{ij} 为

$$R_{ij}=\sum_{k=1}^{n}f_kR_{ij}^k\Big/\sum_{k=1}^{n}f_k \tag{7}$$

其中 f_k 是时间段 k 内交易的衰减因子，R_{ij}^k 是时间段 k 内节点 i 与节点 j 的局部信任值.

推荐信任 AR_j 是根据节点 j 的邻居节点的推荐计算得到的.在决定推荐权重时，R²BTM 考虑了推荐者的信誉值、rater 对推荐者直接交互经验值、推荐者与 ratee 的交易次数以及交易日期 4 个方面的因素.推荐信任 AR_j 的计算方法如式(8)：

$$AR_j=\frac{\sum_{r=1}^{n}w_rR_{rj}}{\sum_{r=1}^{n}w_r} \tag{8}$$

其中 n 表示推荐者的数量，w_r 是第 r 个推荐者的权重，R_{ij} 是节点 i 对节点 j 的局部信任度.

假设推荐节点数量为 n，节点信誉值 RE_j 的计算方法为

$$RE_j=\begin{cases}0.5, & R_{ij}=0\text{ 且 }n=0\\ \beta R_{ij}+(1-\beta)AR_j, & n\neq 0\end{cases} \tag{9}$$

在 R²BTM 中，引入信息论中信息熵的理论来

描述风险.风险量化方法为

$$RI_j = \frac{\sum_{i=I,N,M} f(i)H(\rho_i)}{f(M)} \tag{10}$$

其中 ρ_i 是置信度,$f(x)$ 是评价函数.具体概念和符号解释可参见文献[46].

R^2BTM 抵抗恶意行为方面的能力体现在:(1)算法考虑了风险,使得信任值受恶意行为影响更为敏感;(2)通过比较某个推荐节点的推荐信任值与所有推荐节点的推荐信任值之间的偏离程度是否超过所有推荐信任值的标准方差,可以判断出异常推荐;(3)推荐信任的权重与推荐节点自身的信任值相关,可消弱恶意节点的恶意推荐;(4)给定时间段内的不良评价数量异常时,要求评价节点提供交易证明;(5)在直接评价数量足够多的情况下,如果推荐信任与直接信任存在偏差,忽略推荐信任.

R^2BTM 是信任计算模型中涉及因素较全面的模型.其主要优点包括:(1)计算信任度时,考虑了风险因素;(2)考虑了不同时间段交易记录对信誉值计算的影响;(3)引入信息论中信息熵的理论来描述风险;(4)决定推荐权重时不仅考虑推荐者的信誉值,还考虑了其他方面的影响.其不足之处在于:(1)决定推荐权重时考虑了多方面的因素,没有给出具体量化方法;(2)没有考虑交易量大小对信誉值的影响,可能会引起有些节点依靠小额交易骗取信任后,进行大额的恶意活动;(3)未给出算法实现,比如信誉值的存储等,这些可能影响到算法的实施.

5.5 Dirichlet 信任算法

文献[47]提出了一种基于 Dirichlet 分布的信任算法.假设用户对其他用户或服务的评价有 k 个不同的离散级别(如表 2 是 4-级别的示例),那么信任算法中对应 Dirichlet 分布的状态空间的势是 k.

经过 n 个时间段以后,对用户 y 的累积评价用向量 $\boldsymbol{R}_{y,n}=\{R_y(i), i=1,2,\cdots,k\}$ 表示.向量 $\boldsymbol{r}_{y,t}=\{\boldsymbol{r}_{y,t}(i), i=1,2,\cdots,k\}$ 表示时段 t 内对用户 y 的评价.向量 $\boldsymbol{r}_y^x=\{\boldsymbol{r}_y^x(i), i=1,2,\cdots,k\}$ 表示时段 t 内用户 x 对用户 y 的评价,如果评价为第 i 个级别(如表 2 中的 G),则向量 $\boldsymbol{r}_y^x$ 中的第 i 个元素对应的值为 1,其他的元素对应值为 0.假设 $\boldsymbol{M}$ 表示在时间段 t 内所有对用户 y 评价过的用户集合,则有 $\boldsymbol{r}_{y,t}(i)=\sum_{x\in M}\boldsymbol{r}_y^x(i)$.

考虑到用户的评价随时间衰减,引入衰减因子 λ,$0\leq\lambda\leq1$.经过 $(t+1)$ 个时间段后,对用户 y 的累积评价为

$$\boldsymbol{R}_{y,(t+1)} = \lambda \cdot \boldsymbol{R}_{y,t} + \boldsymbol{r}_{y,(t+1)} \tag{11}$$

对用户 y 的最终评价用向量 $\boldsymbol{R}_y$ 表示,$R_y(i)$ 表示对第 i 个级别的累计评价值.如果用每个评价级别(状态空间中的一个元素)对应的概率期望值表示信任度或者信誉值,则有

$$S_y(i) = \frac{R_y(i) + Ca(i)}{C + \sum_{k=1}^{n} R_y(k)} \tag{12}$$

其中 C 和 $a(i)$ 的含义可以参见 5.2 节.

Dirichlet 信任算法主要精力用在如何利用 Dirichlet 概率分布理论计算信任值上,未对算法抵抗恶意行为的能力进行过多的考虑.算法在计算过程中引入时间衰减因子,可抑制部分恶意用户在累计一定信任值后进行恶意交易的行为.

基于 Dirichlet 分布的信任算法主要优点有:(1)利用概率期望值表示信任度,体现了信任的不确定性;(2)给出计算信任度的方法,计算方法简单且易于实现;(3)给出了一个具体的算法示例.但是该算法还存在一些不足之处:(1)没有考虑如何识别恶意评价以及对恶意评价的惩罚;(2)算法中仅仅利用直接评价结果计算信任度,没有考虑推荐信任;(3)和 R^2BTM 模型类似,在计算信任度时,没有考虑到交易量大小.

5.6 模糊信任算法

文献[37]提出了一种基于模糊推理的信任评估方法(Fuzzy-based Trust Evaluation,FTE),该方法包括 3 个模型:(1)交易之前,对候选交易主体的信任(trustworthiness)评估模型;(2)交易完成以后,主体信任度的评估值与主体真实行为之间的差异评价模型;(3)每次交易后,调整推荐主体可信程度(Agent Credibility,AC)的模型.

正如图 4 所示,基于模糊推理的信任评价方法由模糊化、模糊推理以及反模糊化等过程组成.FTE 中,模糊化过程有 3 个输入参数:加权信任值(Weighted Trustworithiness Value,WTV)、信念权重(Opinion Weight,OW)和主体可信性(Agent Credility,AC).

计算 WTV 时,考虑两方面的数据,直接交易记录和推荐交易记录.假设 S 是交易数量,t_{val} 是交易评价,n 是当前时间,m 是评价时间,则 WTV 计算方法如式(13):

$$WTV = \frac{\sum_{s=1}^{S}\left[\mathrm{e}^{-(n-m)/D}((t_{val}-t_{min})/(t_{max}-t_{min}))\times5\right]}{S} \tag{13}$$

式(13)说明：(1) WTV 是所有交易记录的加权值；(2)在加权之前，所有交易记录规格化到[0,5]区间内；(3)交易记录对 WTV 的贡献随着时间呈指数衰减，其中 D 是衰减系数.

另一个参数 OW 主要用于推荐主体上，如果推荐主体与被评价主体之间的交易越多，则信任评估越准确，即 OW 越高. 主体的 AC 越高表示该主体的推荐信息越可信，AC 初始时均为 2.5，随着系统运行不断调整.

WTV、OW 和 AC 模糊化时采用三角型的隶属函数. 依据模糊化后的数据进行信任推理. 4.4 节所示的规则是一个典型的推理过程使用的规则. FTE 算法共有 3 个输入参数且每个参数上有 3 个模糊集(High、Medium 和 Low)，因此规则库最多有 27($3^3=27$)条规则. 模糊推理后得到信任的模糊值. 经过反模糊化，就可以得到数值化的信任值. FTE 算法采用了平方和的方根(root-sum-square)的反模糊化方法. 限于篇幅，详细的反模糊化过程见文献[37]中的 3.3 节.

FTE 算法用相关性(Correlation)、承诺(Commitment)、清晰(Clarity)和影响(Influence)的方法论(CCCI)评价主体信任度的评估值与主体真实行为之间的差异. 目的用于改善主体的执行能力和服务质量. 在计算此相关性时，考虑三方面的因素：(1)承诺，主体双方之间在交易前的承诺条款(Criterion)；(2)清晰，承诺是否清晰，能够普遍理解且被双方接受；(3)影响或者重要性，每个条款的重要性.

通过调整 AC 值，可促使主体推荐真实的交易信息. 调整 AC 的原则是：(1)增加那些与真实值(C_R)相近的实体的 AC 值，减少那些与 C_R 差别较大的实体的 AC 值；(2) AC 值增长较缓慢，但降低较快. 文献[37]分别选择钟型(bell-shaped)函数和指数函数作为 AC 值的加强函数和惩罚函数.

FTE 算法抵抗恶意行为能力主要表现在 3 个参数的计算上面：(1)计算 WTV 时考虑到交易数量、评价数据归一化及评价时间等；(2)计算参数 OW 时考虑到推荐节点与被推荐节点之间的交易数量，数量越多 OW 越高；(3)利用参数 AC 可有效抑制恶意节点的虚假推荐，参数 AC 可动态调整以适应环境变化.

FTE 采用模糊推理的方法计算主体之间的信任度. 其主要优点是：(1)基于模糊逻辑的推理方法符合信任不确定这一特性，且可处理不准确的评价；(2)每次交易后，动态调整推荐主体的可信性(AC)；(3)考虑了对恶意推荐的惩罚；(4)详细给出信任的模糊推理过程中的计算方法. 其不足之处在于：(1)未给出 OW 的计算或评估方法；(2)在基于模糊逻辑的推理过程中，如何选择隶属函数具有一定的挑战性，FTE 中采用了常用的隶属度函数，其效用未作评判；(3)文中只给出利用 FTE 计算的实例，未就算法的有效性用仿真或者实验的方法进行验证；(4)算法在具体实现方面还可以进一步展开，如数据存储等，这些因素会影响到算法的性能.

5.7　灰色信任算法

文献[39]提出了一种基于灰色系统理论的信任报告机制(Prestige Reporting Mechanism based on Gray System Theory，PRMGST). PRMGST 证明了灰色信任度在 t 时刻存在的充分必要性，其推理方法包括灰色关联分析和灰色聚类等算法.

在 PRMGST 中，由被评价的实体组成的集合为聚类实体集. 评价实体(客户)组成的集合称为客户集. 被评价属性称为关键属性，其组成关键属性集. 所有灰类组成灰类集，记作 $\boldsymbol{G}=\{g_k \mid k=1,2,\cdots,r\}$. 用灰类 g_k 表示客户对聚类实体的灰色信任度，如表示产品质量的灰类可分为质量好、质量一般以及质量差等.

PRMGST 利用味集群的方法采集原始数据，屏蔽恶意评价行为. 味集群的详细定义可以参见文献[39]，其主要思想就是味集群中的客户对同一个聚类实体的所有关键属性的评价相近，每一个味集群有且仅有一个核心，所有味集群的核心组成核心集. 将客户对关键属性的评分与核心集中所有核心对关键属性的评分相比，如果偏离超出了一定范围，则可认为该评分无效，如果无效评分超过限制的次数时，认为该客户为恶意客户.

假设 $\delta_{ih}=\{\delta_{ih}(1),\delta_{ih}(2),\cdots,\delta_{ih}(u),\cdots,\delta_{ih}(q)\}$ 表示所有味集群对聚类实体的关键属性 a_h 的评价，其中 $\delta_{ih}(u)$ 表示第 u 个味集群的评价. 根据评价数据利用灰色关联分析可以计算出所有聚类向量的评估向量.

图 5 是文献[39]给出的白化函数 $f_{hk}(x)$，$E(\lambda_{hk},1)$为转折点，$f_{hk}(T_i(a_h))=0.81$ 表示评分值 $T_i(a_h)$ 属于 g_k 灰类的可能性为 0.81. 权重矩阵定义为 $\boldsymbol{W}=(w_{hk})$，$1\le h\le e$，$1\le k\le r$. 其中 $w_{hk}=\lambda_{hk}/(\lambda_{1k}+\lambda_{2k}+\cdots+\lambda_{hk}+\cdots+\lambda_{ek})$. 实体的白化矩阵为 $\boldsymbol{F}_i=(f_{hk}(T_i(a_h)))$. 根据得到的权重矩阵和白化矩阵，利用灰类聚类分析计算客户对聚类实体的灰色

信任度.

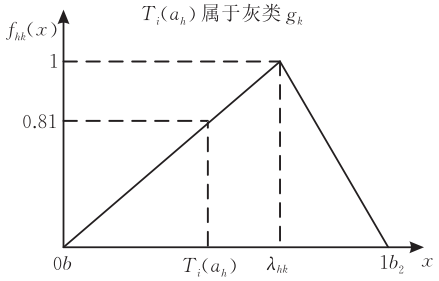

图 5 灰类白化函数

PRMGST 抵抗恶意行为的能力体现在:(1)算法以味集群为单位收集原始评价信息,能够有效地抑制恶意节点的虚假评价或推荐;(2)用灰关联分析处理数据对评估向量进行灰色聚类评估,为每个节点的评价赋予相应的权重,可限制恶意节点的评价对信任值的影响.

PRMGST 首次提出基于灰色系统理论的信任推测算法.其主要优点包括:(1)用灰类表示信任度,体现出信任的不确定性;(2)给出了信任推测的基本评估算法,灰色关联分析和灰色聚类分析;(3)算法中采用味聚集识别恶意评价;(4)在计算一个实体的信任度时,综合考虑到对不同属性评价.不足之处在于:(1)仅仅识别出恶意评价,未恶意评价行为进行惩罚;(2)计算信任时,没有考虑实体间的推荐信任;(3)在算法实现上,还有一些工作需要展开,比如白化函数选择,评价信息的计算和存储等问题,这些可能会影响到算法性能以及可扩展性.

5.8 基于云模型信任算法

文献[42]提出了一种普适计算环境下基于云模型的信任模型(Cloud-Based Trust Model,CBTM).普适计算环境下的信任模型,对 P2P 网络也具有借鉴意义,这里只是关注算法本身,不涉及具体的实现环境.信任云的定义如 3.6 节所述,CBTM 算法中给出了信任云的传递以及合并算法.

在没有直接交互关系情况下,两个实体之间的信任度就需要通过依靠其他实体的推荐进行计算.假设有$(n+1)$个实体分别为$E_1,E_2,\cdots,E_n,E_{n+1}$,这些实体组成一条信任路径,$E_1$对于$E_{n+1}$的信任云$tc(Ex,En,He)$为

$$\begin{cases} tc(Ex,En,He)=tc_1\otimes tc_2\otimes\cdots\otimes tc_n=\\ \qquad\qquad\prod_{i=1}^{n}tc_i(Ex_i,En_i,He_i)\\ Ex=\prod_{i=1}^{n}Ex_i\\ En=\min\left(\sqrt{\sum_{i=1}^{n}En_i^2},1\right)\\ He=\min\left(\sum_{i=1}^{n}He_i,1\right) \end{cases} \tag{14}$$

在计算信任关系时,如果两个实体之间存在多条推荐信任路径,就需要把不同路径上的信任云合并成一个信任云.假设实体 E 对实体 E' 的信任 $tc(Ex,En,He)$是合并 n 条不同路径上的信任而得到的,第 i 条路径上的信任为 $tc_i(Ex_i,En_i,He_i)$,则信任云 $tc(Ex,En,He)$为

$$\begin{cases} tc(Ex,En,He)=tc_1\oplus tc_2\oplus\cdots\oplus tc_n=\\ \qquad\qquad\sum_{i=1}^{n}tc_i(Ex_i,En_i,He_i)\\ Ex=\frac{1}{n}\sum_{i=1}^{n}Ex_i\\ En=\min\left(\frac{1}{n}\sum_{i=1}^{n}En_i,1\right)\\ He=\min\left(\frac{1}{n}\sum_{i=1}^{n}He_i,1\right) \end{cases} \tag{15}$$

CBTM 首次提出基于云模型的信任推测算法.主要优点是:(1)用云模型将信任程度和不确定程度表现出来,理论上更加合理;(2)CBTM 给出了信任计算中的两种基本方法:推荐信任计算方法和不同信任云的合并方法.CBTM 算法描述较简单,还存在一些不足:(1)没有充分考虑算法抵抗恶意行为的能力;(2)没有涉及如何利用主体之间的评价信息构建信任云;(3)在算法实现上,还有一些工作需要展开,比如主体之间信任的初始化,评价信息或者信任云的存储等问题,这些可能会影响到算法性能以及可扩展性.

5.9 各种模型比较

参照文献[9]中表 1 所列的模型比较指标,对本节描述的各种信任模型进行比较,结果如表 4 所示.

表 4 典型信任模型的比较

模型	TMBS	EigenTrust/PowerTrust	PeerTrust	R²BTM	Dirichlet	FTE	PRMGST	CBTM
动态性	是	是	是	是	是	是	是	是
上下文因素	否	是	是	是	是	是	否	否
危险评估	否	否	否	是	否	是	否	否
实现	是	是	是	否	是	否	否	否
信心因素	否	是	是	是	是	是	否	是
历史交易	否	是	是	是	是	是	是	是

（续　表）

模型	TMBS	EigenTrust/PowerTrust	PeerTrust	R^2BTM	Dirichlet	FTE	PRMGST	CBTM
第三方因素	否	是	是	是	是	否	是	是
信任对象	否	否	否	否	否	否	否	否
反馈协议	否	否	否	是	否	否	否	否
数学方法	算术	加权平均	加权平均	加权平均	贝叶斯推测	模糊逻辑	灰色理论	云理论
真实性	不好	好/很好	很好	好	好	不好	不好	很好
可扩展性	较高	较高	较高	高	较高	较高	较低	低
健壮性	很差	好/很好	很好	很好	差	差	好	差

6　存在问题与展望

6.1　当前研究存在的问题

对等网络中的信任机制问题经过多年研究取得了一定成果，但在理论或者实现方面还存在以下问题：

（1）缺乏统一的信任模型的性能评价标准. 目前已有研究中提出了很多信任模型，如何合理地比较这些信任模型之间性能差异是一件比较困难的工作，主要原因是没有一个统一的评价标准. 已有研究大多采用模拟实验的办法进行评价，缺乏针对实际数据的评价.

（2）从上面介绍的典型信任算法可以看出，在已有的研究中，大多数信任模型缺少算法的实现部分，如数据存储与访问、数据传输协议等，这些可能会影响到算法的性能和可扩展性，直接关系到算法在实际系统中的应用.

（3）在研究信任机制问题时，目前关注的焦点多在信任算法本身上，比如算法有效性和健壮性等，而轻视了一个重要问题，如何激励用户积极提供评价信息，尤其是负面的评价信息. 文献[48]研究表明，eBay 系统中仅有 60.7%的买方和 51.7%的卖方向系统提供了评价信息；而买方提供的评价中负面信息仅占 0.6%，卖方提供评价信息中负面信息也不过 1.6%. 依据不完全的评价信息计算出的信任值，并不能够反映系统的真实情况.

已有研究中的激励措施主要是采用对提供诚实评价的用户进行奖励的办法，如何判断评价的真实性是此类研究的重点. 文献[49]通过比较前后两个接受同一服务的不同用户给出的评价是否一致来判断前者是否诚实，并对诚实用户进行奖励. 该激励机制没有对非诚实的评价作出惩罚，恶意用户可依靠提供不诚实评价促使诚实用户得不到奖励，最终导致激励机制失效. 另外，文献[49]中没有考虑恶意用户之间的合谋或策略撒谎行为对激励机制的影响. 文献[50-51]利用 Pinocchio 模型判断用户评价的准确性，依据准确性奖励用户. 评价具有主观性，用户间的评价标准差异性较大，判断用户评价准确性时应该考虑用户的个性. Pinocchio 模型中也没有考虑合谋或策略性撒谎对激励机制的影响. 文献[52]通过计算前后两个接受同一服务的不同用户给出的评价之间的相关性决定奖励的多少. 为得到奖励前后评价应保持一致，提供诚实评价是纳什均衡. 这与文献[49]所述激励机制类似，因此文献[52]与文献[49]存在类似的不足，此外所有用户都采取撒谎策略也可到达纳什均衡. 文献[53]认为交易双方对同一个服务的评价不一致肯定存在撒谎行为，对存在撒谎行为的双方都进行相应的惩罚. 诚实用户也受到惩罚，这对诚实用户是不公平的，可能会影响用户参与的积极性. 此激励机制同样存在用户评价标准差异带来的问题. 另外，该激励机制中也没有考虑恶意用户之间的合谋评价带来的影响.

（4）识别和过滤非诚实或虚假评价是一个信任系统需要解决的问题，因为非诚实或虚假评价会影响信任度的准确性. PeerTrust[26] 利用节点的信任值或者节点之间评价的相似性确定节点的可信度，计算推荐信任时赋予可信度较高的节点较大权重，依此减轻非诚实评价带来的影响. TrustGuard[54] 计算信任值时考虑到当前信任、历史信任以及信任波动，可有效抵抗策略摇摆攻击；借助交易凭证防止恶意用户提交虚假评价；另外采用 PeerTrust 相同的方法较少非诚实评价对计算信任值的影响. PeerTrust 和 TrustGuard 的不足之处如 5.3 节所述. 文献[55]利用 Bayesian 理论评估某个用户的评价与大多数人评价的偏离程度，当偏离较大时就认为该用户的评价是不公平的. 因该算法采用统计学方法，当评价信息较稀少或评价信息较分散时会影响到算法准确性. 文献[56]认为推荐者的评价越接近自己的评价则推荐者越可信. 当两种评价之间的差异超过给定阈值时，认为推荐者撒谎. 个体之间评价标准的差异性会直接影响推荐者的可信度. 文献[57]提出了一种 P2P 环境下的可识别不公平评价的初步

框架,框架还需进一步完善,如该框架中的激励机制.

(5)标识(identity)管理是信任机制中需要研究的内容之一.如果缺乏对标识的管理,使得恶意主体容易洗脱自己的"罪恶"历史.文献[58]认为把所有未知用户按恶意用户对待,可以提高信任系统的性能.文献[59]认为惩罚所有新用户可以减少系统中的漂白用户(Whitewasher)数量.这两种方法虽然可以降低系统中的恶意用户数量,但也会降低诚实的新用户加入系统的积极性,而影响系统规模.文献[60]认为采用自适应新用户的合作策略相对于采用欺骗所有新用户的合作策略能够提供高系统的总体性能,但对于那些每次重新进入系统表现为诚实新用户的漂白者显得无能为力.文献[61]利用中心信任机制能够保证为系统中的每个用户分配一个 ID,同时保证用户的匿名性,但中心信任机制不适合于动态的对等网络环境.文献[62]利用恶意节点的资源(通信、存储和计算)是有限的以及增加系统假设条件来限制恶意用户产生多余的 ID,以抗击女巫攻击.正如文献[62]指出的那样这些假设条件在大规模的对等网络中显得有些苛刻且不易满足.

6.2 展 望

结合第 6.1 节中提出的问题,在对等网络环境下信任机制研究中,可在以下几个方面进一步展开研究:

(1)统一的信任模型评价体系.通过评价体系中给出的评价指标可以客观公正地比较不同信任模型之间的差异,目前已有国外学者[63-64]开始关注这方面的工作.

(2)信任模型实现问题.这方面的工作主要研究信任数据的存储与访问策略以及数据在对等节点之间安全传输协议等.另外,许多信任模型涉及到较为复杂的数学推导过程,算法的实现复杂度也是需要研究的问题.

(3)信任机制中的激励问题.信任机制除了要研究信任的运行机制,提供一套完善的激励机制也是必不可少的.文献[45]的研究结果也表明,在缺乏激励机制的情况下,用户提供评价信息的积极性不是很高.

(4)主体标识管理.主要研究信任系统中采用何种方式给节点分配标识以及节点是否可以随意变更其标识.防止恶意节点借此漏洞洗刷或隐藏其恶意的历史记录.

(5)能更准确地反映主观信任不确定性的信任模型以及结合人工智能等方法的信任推理机制也值得研究.

7 结束语

目前 P2P 环境下的信任机制研究得到国内外学者的广泛关注.通过在 P2P 中引入信任机制,以期解决其面临的安全问题.本文在综述信任机制最新研究进展的基础上,探讨了需要进一步研究的问题.然而由于 P2P 网络和人类社会具有许多相似性,这就造成信任机制较为复杂,需要研究的问题很多.P2P 网络中的信任机制研究对于其它计算环境,如普适计算环境、Ad Hoc 网络,也具有借鉴意义.

致 谢 感谢审稿人提出的评审意见,这些评审意见对提高论文水平有很大帮助!

参 考 文 献

[1] Marsh S P. Formalising trust as a computational concept [Ph. D. dissertation]. University of Stirling, Stirling, 1994

[2] Karl A, Zoran D. Managing trust in a Peer-2-Peer information system//Proceedings of the 10th International Conference on Information and Knowledge Management. Atlanta, Georgia, USA, 2001: 310-317

[3] Huang Quan-Neng, Song Jia-Xing, Liu Wei-Dong, Zhang Jun. Survey of reputation system on Peer-to-Peer network. Mini-Micro Systems, 2006, 27(7): 1175-1181(in Chinese)
(黄全能,宋佳兴,刘卫东,张军. 对等网络信誉机制研究综述.小型微型计算机系统,2006,27(7):1175-1181)

[4] Feng Qin-Yuan, Dai Ya-Fei. Survey on trust mechinism for P2P network. Communications of CCF, 2007, 3(3): 31-40 (in Chinese)
(冯沁原,代亚非. P2P 网络信任机制综述. 中国计算机学会通讯,2007,3(3):31-40)

[5] Audun J, Roslan I, Colin B. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2007, 43(2): 618-644

[6] Ruohomaa S, Kutvonen L, Koutrouli E. Reputation management survey//Bob W ed. Proceedings of the 2nd International Conference on Availability, Reliability and Security. Piscataway: IEEE Computer Society Press, 2007: 103-111

[7] Artz D, Gil Y. A survey of trust in computer science and the Semantic Web. Web Semantics, 2007, 5(2): 58-71

[8] Ramchurn S, Huynh D, Jennings N R. Trust in multi-agent systems. Knowledge Engineering Review, 2004, 19(1): 1-25

[9] Li Xiao-Yong, Gui Xiao-Lin. Research on dynamic trust model for large scale distributed environment. Journal of

Software，2007，18(6)：1510-1521(in Chinese)
(李小勇，桂小林. 大规模分布式环境下动态信任模型研究. 软件学报，2007，18(6)：1510-1521)

[10] Lin Chuang，Feng Fu-Jun，Li Jun-Shan. Access control in new network environment. Journal of Software，2007，18(4)：955-966(in Chinese)
(林闯，封富君，李俊山. 新型网络环境下的访问控制技术. 软件学报，2007，18(4)：955-966)

[11] Audun J. Trust and reputation systems//Aldini A，Gorrieri R eds. Foundations of Security Analysis and Design. LNCS 4677. Berlin：Springer-Verlag，2007：209-245

[12] Lars R，Sverker J. Simulated social control for secure Internet commerce//Catherine M ed. Proceedings of the 1996 Workshop on New Security Paradigms. New York：ACM Press，1996：18-25

[13] Abdul-Rahman A，Hailes S. Supporting trust in virtual communities//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Los Alamitos，2000：132

[14] Cahill V，Shand B，Gray E，et al. Using trust for secure collaboration in uncertain environments. IEEE Pervasive Computing，2003，2(3)：52-61

[15] Carbone M，Nielsen M，Sassone V. A formal model for trust in dynamic networks//Cerone A，Lindsay P eds. Proceedings of the International Conference on Software Engineering and Formal Methods (SEFM'03). Los Vaqueros：IEEE Computer Society，2003：54-61

[16] Liang Z Q，Shi W S. PET：A PErsonalized trust model with reputation and risk evaluation for P2P resource sharing//Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Piscataway：IEEE Computer Society，2005：201-211

[17] Dou Wen，Wang Huai-Min，Jia Yan，Zou Peng. A recommendation-based Peer-to-Peer Trust model. Journal of Software，2004，15(4)：571-583(in Chinese)
(窦文，王怀民，贾焰，邹鹏. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型. 软件学报，2004，15(4)：571-583)

[18] Zhang Qian，Zhang Xia，Wen Xue-Zhi，Liu Ji-Ren，Ting Shan. Construction of Peer-to-Peer multiple-grain Trust model. Journal of Software，2006，17(1)：96-107(in Chinese)
(张骞，张霞，文学志，刘积仁，Ting Shan. Peer-to-Peer 环境下多粒度 Trust 模型构造. 软件学报，2006，17(1)：96-107)

[19] Li Jin-Tao，Jing Yi-Nan，Xiao Xiao-Chun，Wang Xue-Ping，Zhang Gen-Du. A trust model based on similarity-weighted recommendation for P2P environments. Journal of Software，2007，18(1)：157-167(in Chinese)
(李景涛，荆一楠，肖晓春，王雪平，张根度. 基于相似度加权推荐的 P2P 环境下的信任模型. 软件学报，2007，18(1)：157-167)

[20] Zhou R F，Hwang K. PowerTrust：A robust and scalable reputation system for trusted Peer-to-Peer computing. IEEE Transactions on Parallel and Distributed Systems，2007，18(4)：460-473

[21] Chang Jun-Sheng，Wang Huai-Min，Ying Gang. DyTrust：A time-frame based dynamic trust model for P2P systems. Chinese Journal of Computers，2006，29(8)：1301-1307(in Chinese)
(常俊胜，王怀民，尹刚. DyTrust：一种 P2P 系统中基于时间帧的动态信任模型. 计算机学报，2006，29(8)：1301-1307)

[22] Jiang Shou-Xu，Li Jian-Zhong. A reputation-based trust mechanism for P2P e-commerce systems. Journal of Software，2007，18(10)：2551-2563(in Chinese)
(姜守旭，李建中. 一种 P2P 电子商务系统中基于声誉的信任机制. 软件学报，2007，18(10)：2551-2563)

[23] Sepandar D K，Mario T S，Hector G M. The EigenTrust algorithm for reputation management in P2P networks//Proceedings of the 12th Intertational Conference on World Wide Web. Budapest Hungary，2003：640-651

[24] Karl K，Mogens N. From simulations to theorems：A position paper on research in the field of computational trust//Gerhard G，Juris H，Jan van L eds. Formal Aspects in Security and Trust. LNCS 4691. Springer，2007：97-111

[25] Zoran D，Karl Aberer. P2P reputation management：Probabilistic estimation vs. Social networks. Computer Networks，2006，50(4)：485-500

[26] Xiong L，Liu L. PeerTrust：Supporting reputation-based trust for Peer-to-Peer electronic communities. IEEE Transactions on Knowledge Data Engineering，2004，16(7)：843-857

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

[28] Audun J. Trust-based decision making for electronic transactions//Yngstrom L，Svensson T eds. Proceedings of the 4th Nordic Workshop on Secure Computer Systems (NORDSEC'99). Kista：Stockholm University Press，1999：1-21

[29] Yu B，Singh M P. An evidential model of distributed reputation management//Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems. Bologna，Italy，2002：294-301

[30] Manchala D W. Trust metrics，models and protocols for electronic commerce transactions//Papazoglou M P，Takizawa M，Kramer B，Chanson S eds. Proceedings of the 18th International Conference on Distributed Computing Systems. Los Vaqueros：IEEE Computer Society，1998：312-321

[31] Sabater J，Sierra C. REGRET：A reputation model for gregarious societies//Proceedings of the 4th International Workshop on Deception，Fraud and Trust in Agent Societies，in the 5th International Conference on Autonomous Agents. Montreal，Canada，2001：61-69

[32] Sabater J，Sierra C. Reputation and social network analysis in multi-agent systems//Proceedings of the 1st International

Joint Conferenceon Autonomous Agents and Multiagent Systems. New York: ACM Press, 2002: 475-482

[33] Sabater J, Sierra C. Social ReGreT, a reputation model based on social relations. ACM SIGecom Exchanges, 2002, 3(1): 44-56

[34] Aringhieri R, Damiani E, De Capitani Di Vimercati S, Paraboschi S, Samarati P. Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems. Journal of the American Society for Information Science and Technology, 2006, 57(4): 528-537

[35] Song S S, Hwang K, Zhou R F, Kwok Y K. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 2005, 9(6): 24-34

[36] Griffiths N. A fuzzy approach to reasoning with trust, distrust and insufficient trust//Klusch M, Rovatsos M, Payne T R eds. Proceedings of 10th International Workshop on Cooperative Information Agents. LNCS 4149. Heidelberg: Springer-Verlag, 2006: 360-374

[37] Schmidt S, Steele R, Dillon T S, Chang E. Fuzzy trust evaluation and credibility development in multi-agent systems. Applied Soft Computing Journal, 2007, 7(2): 492-505

[38] Tang Wen, Chen Zhong. Research of subjective trust management model based on the fuzzy set theory. Journal of Software, 2003, 14(8): 1401-1408(in Chinese)
(唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究. 软件学报, 2003, 14(8): 1401-1408)

[39] Xu Lan-Fang, Hu Huai-Fei, Sang Zi-Xia et al. A prestige reporting mechanism based on gray system theory. Journal of Software, 2007, 18(7): 1730-1737(in Chinese)
(徐兰芳, 胡怀飞, 桑子夏等. 基于灰色系统理论的信誉报告机制. 软件学报, 2007, 18(7): 1730-1737)

[40] Li De-Yi, Meng Hai-Jun, Shi Xue-Mei. Membership clouds and membership clouds generator. Journal of Computer Research and Development, 1995, 32(6): 15-20(in Chinese)
(李德毅, 孟海军, 史雪梅. 隶属云和隶属云发生器. 计算机研究与发展, 1995, 32(6): 15-20)

[41] Li De-Yi, Liu Chang-Yu. Study on the Universality of the normal cloud model. Engineering Science, 2004, 6(8): 28-34(in Chinese)
(李德毅, 刘常昱. 论正态云模型的普适性. 中国工程科学, 2004, 6(8): 28-34)

[42] He R, Niu J W, Zhang G W. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing//Pan Y et al eds. Proceedings of the 3rd International Symposium on Parallel and Distributed Processing and Applications—ISPA 2005 Workshops. LNCS 3758. Berlin, Heidelberg: Springer-Verlag, 2005: 541-552

[43] He R, Niu J W, Hu K. A novel approach to evaluate trustworthiness and uncertainty of trust relationships in Peer-to-Peer computing//Wei D et al eds. Proceedings of the 5th International Conference on Computer and Information Technology. Los Vaqueros: IEEE Computer Society, 2005: 382-388

[44] Despotovic Z, Aberer K. Probabilistic prediction of peers' performance in P2P networks. Engineering Applications of Artificial Intelligence, 2005, 18(7): 771-780

[45] Deng Ju-Long. Grey System Theory Tutorial. Wuhan: Huazhong University Press, 1990(in Chinese)
(邓聚龙. 灰色系统理论教程. 武汉: 华中理工大学出版社, 1990)

[46] Tian Chun-Qi, Zou Shi-Hong, Tian Hui-Rong et al. A new trust model based on reputation and risk evaluation for P2P networks. Journal of Electronics & Information Technology, 2007, 29(7): 1628-1632(in Chinese)
(田春岐, 邹仕洪, 田慧蓉等. 一种基于信誉和风险评价的分布式 P2P 信任模型. 电子与信息学报, 2007, 29(7): 1628-1632)

[47] Josang A, Haller J. Dirichlet reputation systems//Werner B eds. Proceedings of the 2nd International Conference on Availability, Reliability and Security Vienna. Los Vaqueros: IEEE Computer Society, 2007: 112-119

[48] Resnick P, Zeckhauser R. Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system//Baye M R ed. Advances in Applied Microeconomics. Amsterdam: Elsevier, 2002, 11: 127-157

[49] Jurca R, Faltings B. An incentive compatible reputation mechanism//Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems. New York: ACM Press, 2003: 1026-1027

[50] Alberto F, Evangelos K, Sven O. Pinocchio: Incentives for honest participation in distributed trust management//Jensen C D et al eds. Proceedings of the 2nd International Conference on Trust Management(iTrust 2004). LNCS 2995. Berlin Heidelberg: Springer-Verlag, 2004: 63-77

[51] Evangelos K, Petros Z, Nischal M P. Jiminy: A scalable incentive-based architecture for improving rating quality//Stolen K et al eds. Proceedings of the 4th International Conference on Trust Management(iTrust 2006). LNCS 3980. Berlin Heidelberg: Springer-Verlag, 2006: 221-235

[52] Miller N, Resnick P, Zeckhauser R. Eliciting informative feedback: The peer-prediction method Source. Management Science, 2005, 51(9): 1359-1373

[53] Papaioannou T G, Stamoulis G D. An incentives' mechanism promoting truthful feedback in Peer-to-Peer systems//Proceedings of the 2005 IEEE International Symposium on Cluster Computing and the Grid. Cardiff, UK, 2005, (1): 275-283

[54] Srivatsa M, Xiong L, Liu L. Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks//Proceedings of the 14th International World Wide Web Conference. Chiba, Japan, 2005: 422-431

[55] Withby A, Jøsang A, Indulska J. Filtering out unfair ratings in Bayesian reputation systems//Proceedings of the 7th International Workshop on Trust in Agent Societies. Utrecht, Netherlands, 2004

[56] Huynh T D, Jennings N R, Shadbolt N. On handling inaccurate witness reports//Proceedings of the 8th International Workshop on Trust in Agent Societies. Utrecht, Netherlands, 2005: 63-77

[57] Tien Tuan Anh Dinh, Tom Chothia, Mark Ryan. A trusted infrastructure for P2P-based marketplaces//Proceedings of the 9th International Conference on Peer-to-Peer Computing (P2P'09). Seattle, USA, 2009: 151-154

[58] Marti S, Garcia-Molina H. Identity Crisis: Anonymity vs. Reputation in P2P systems//Proceedings of the 3rd International Conference on Peer-to-Peer Computing. Linköping, Sweden, 2003: 134-141

[59] Feldman M, Papadimitriou C, Chuang J, Stoica I. Free-riding and whitewashing in Peer-to-Peer systems//Proceedings of the ACM SIGCOMM 2004 Workshops. Portland, USA, 2004: 228-235

[60] Lai K, Feldman M, Stoica I. Incentives for cooperation in peer-to-peer networks//Proceedings of the 2nd Workshop on Economics of Peer-to-Peer Systems. Berkeley, USA, 2003

[61] Friedman E, Resnick P. The social cost of cheap pseudonyms. Journal of Economics and Management Strategy, 2001, 10(2): 173-199

[62] Douceur J R. The sybil attack//Proceedings of the International Workshop on Peer-to-Peer Systems. Cambridge, USA, 2002

[63] Liang Z Q, Shi W S. Analysis of ratings on trust inference in open environments. Performance Evaluation, 2008, 65(2): 99-128

[64] Conner William, Iyengar Arun, Mikalsen Thomas et al. A trust management framework for service-oriented environments//Proceedings of the WWW 2009. Madrid, Spain, 2009: 891

LI Yong-Jun, born in 1973, Ph.D., lecturer. His current research interests include distributed computing, trust and reputation, social network.

DAI Ya-Fei, born in 1958, Ph. D., professor, Ph. D. supervisor. Her current research interests include P2P computing, distributed storage and social network.

Background

This research is partly supported by the National Basic Research Program of China (973 Program) under grant No. 2004CB318204, the National Natural Science Foundation of China under grant No. 60673183, University-IBM Joint Project under grant No. JSA200811009.

As Peer-to-Peer application becomes popular on the Internet, its security problems receive considerable attentions from the academic community and the internet industry. Because of the characteristics inherent in the Peer-to-Peer network, traditional IT security solutions are not applicable any more. One of the popular approaches to this problem is to deploy trust mechanism or reputation system in P2P applications. The underlying goal in all Trust mechanism or Reputation systems is to predict a peer's future actions, given the knowledge of its past behaviors. The distributed peer-to-peer applications and other forms of online collaboration are all based on mutual trust, which enables transacting peers to overcome the uncertainty and risk inherent in the environment. To gain an intimate knowledge of trust mechanism and its development trend, as well as its research situation at home and abroad, it is especially worthwhile that making an survey on Trust and Reputation system for P2P Network.