P2P环境下基于信誉的信任模型研究

胡建理[1,2] 吴泉源[1] 周 斌[1]

(国防科学技术大学计算机学院 长沙 410073)[1] (广州军区广州总医院信息科 广州 510010)[2]

摘 要 随着P2P(peer to peer)系统得到日益广泛的使用,其面临的服务欺骗和节点资源滥用等可信问题也越来越严重,传统的安全方案已经不能适应这种需求,基于信誉的信任模型为解决这类问题提供了一种新的思路。分析了信任与信誉的关系,给出了一种基于信誉的信任模型的基本运行框架,对当前典型的基于信誉的信任模型进行了综述与评论,并对这些模型进行了比较分析。最后讨论了当前研究存在的问题,并对未来的研究方向作了展望。

关键词 P2P,信任模型,信誉

中图法分类号 TP393.08 **文献标识码** A

Research on Reputation Based Trust Model for P2P Environment

HU Jian-li[1,2] WU Quan-yuan[1] ZHOU Bin[1]

(Institute of Networks & Information Security, School of Computer, National University of Defense Technology, Changsha 410073, China)[1]

(Information Department of Guangzhou General Hospital under Guangzhou Area Command, Guangzhou 510010, China)[2]

Abstract The more along with the wide application of P2P system, the more it will face some severe trust problems such as service faking and resource abusing by some malicious peers. The conventional security measures cannot be used to cater for this demand, whereas the reputation based trust model has given a key to them. Firstly, the relationship between trust and reputation was analyzed, and a basic running framework for the reputation based trust model was put forward. And then the overview and comparison for current classic reputation based trust models were made. Finally, the challenges of this field for future research were presented, as well as some problems existing in current research are discussed.

Keywords Peer-to-peer, Trust model, Reputation

信任管理[1-4]的基本思想是承认系统中安全信息的不完整性,系统的安全决策需要依靠可信任第三方提供附加的安全信息,它是一种基于凭证与策略的信任(也称为理性信任或客观信任)管理,其特点是相对精确、客观,表达为信任或不信任的两种选择,信任与活动没有直接的关系[5]。在传统的网络环境和应用中,一般采用理性信任管理来解决系统中的可信问题,即采用一种统一的方法来描述和解释安全策略、安全凭证和用于直接或委托授权关键性安全操作的信任关系。随着分布式系统的不断发展,以及对P2P环境下应用的深入研究,应用系统表现为由多个软件服务组成的动态协作系统。系统形态正从面向封闭的、熟识用户群体和相对静态的形式向开放的、公共可访问的和动态协作的服务模式转变。另外,在开放的分布式环境中,没有中心化的管理权威可以依赖,不能获得某一主体的全部信息,或者根本就不认识主体,这样请求者有可能对授权者施加破坏性行为,因而产生了基于信誉的信任(也称为感性信任或主观信任)管理,为解决P2P环境下新应用形式的安全可信问题提供了新的思路。

基于信誉的信任主要从信任的定义出发,使用基于信誉的信任模型来描述信任意向的获取和评估。基于信誉的信任模型认为,信任是主体对客体特定行为的主观可能性预期,取决于经验并随着客体行为的结果变化而不断修正[6]。在基于信誉的信任模型中,实体之间的信任关系分为直接信任关系和推荐信任关系,分别用于描述主体与客体、主体与客体经验推荐者之间的信任关系。也就是说,主体对客体的经验既可以直接获得,又可以通过推荐者获得,而推荐者提供的经验同样可以通过其他推荐者获得,直接信任关系和推荐信任关系形成了一条从主体到客体的信任链,而主体对客体行为的主观预期则取决于这些直接的和间接的经验。基于信誉的信任模型放弃了实体间的固定关系,认为信任是一种经验的体现。对信任进行量化或分级,并将其广泛应用于P2P环境下各种分布式应用(如Gnutella[7]及Kazaa[8]等)、电子商务(如eBay[9]和Amazon[10]等)和在线社区等领域,成为近年来研究的热点。

近几年,国内外许多学者借助社会关系中人际模型,使用各种不同的数学方法和工具,对P2P环境下各种分布式应用中的信任模型进行了大量的研究,取得了一些新的进展。本文综述了基于信誉的信任模型的研究进展。本文第1节给出了信任与信誉的相关定义;第2节描述了基于信誉的信任模型的基本运行机理;第3节详细概述并分析了几个有代表性的基于信誉的信任模型;第4节对当前工作存在的问题进行

到稿日期:2008-10-21 返修日期:2009-05-14 本文受国家973重点基础研究发展规划项目基金(2005CB321800),国家863高技术研究发展计划项目基金(2007AA010301),国家杰出青年科学基金(60625203)和国家自然科学基金(60873204)资助。

胡建理 博士,工程师,CCF会员,主要研究方向为分布式计算、信息安全等,E-mail:lxman82@gmail.com;吴泉源 教授,博士生导师,主要研究方向为人工智能、Web服务和信息安全等;周 斌 副教授,主要研究方向为分布式对象技术。

了分析;最后对全文作了总结与展望。

1 相关定义

信任与信誉是两个相互联系又有区别的概念,要对其相互关系进行准确界定,需要先从其定义出发。信任是人类社会的一种自然属性,通常被视为一种直觉上的概念加以理解,并没有形成一个准确和统一的定义[12]。根据个人经验的不同,对信任的理解存在差异;根据不同学者所处的背景、视角和所要解决的问题的不同,对信任的定义也不同。通过综合各种文献,本文对信任(Trust)给出如下定义。

定义 1 信任是在特定时段、特定上下文环境中授信方(Trustor)对受信方(Trustee)的诚实性(honesty)、安全性(security)、可靠性(reliability)和实力性(competence)的一种主观肯定。信任具有主观性、动态性、可度量性、上下文相关性和时间衰减性等特性。

定义 2(信誉,reputation) 也称声誉、信用度和信誉度。在文献[12]中,Jøsang 是这样定义的:"信誉是关于某个人或某件事的特征或者立场的大众观点。"

定义 3(信任度,trust degree) 就是信任程度的定量表示,也可以称为信任程度、信任值、信任级别、可信度等。

定义 4 局部信任度表示由所有与一个节点发生过直接交互的节点给出的关于该节点的直接信任度的有限聚合所形成的信任度量。

定义 5 全局信任度表示一个节点在整个系统中具有的信任度。任意节点的全局可信度由与之发生过交易行为的其他节点对它的局部看法以及这些节点的全局可信度来决定。

信誉与信任并不等价。Jøsang 给出了以下两句话,对此做出了很好的解释:

(1)因为你有很好的信誉,所以我信任你;

(2)尽管你的信誉不好,但是我仍然信任你。

假定这两句话和同一件事务有关,第一句话表明授信方知道受信方的信誉,并且将其信任建立在这种信誉的基础之上。第二句话表明授信方对受信方有一些私人性质的了解,譬如有过直接的交互或者具有某种亲密关系等,这些因素超过了受信方所具有的任何信誉的影响。这个例子表明,信任最终是一个个性化的主观现象,它取决于很多因素或证据,其中某些因素或证据的影响因子会高于其它因素的影响因子,而信誉只是其中的一种因素。

2 基于信誉的信任模型基本运行机理

当基于信誉的信任模型作为信誉系统的核心机制部署到分布式环境中时,在系统中一个节点(设为 i)与另一节点(设为 j)交易前,节点 i 希望了解节点 j 的信任等级时就会启动信任模型。一般情况下,当节点 i 需要节点 j 提供某种服务时会产生这种需求。其基本运行机理可通过如下几步进行描述:

Step1 节点 i 通过广播向网络中提出对节点 j 的信誉查询请求 $Req(i,j)$,如图 1 所示。

Step2 当网络中的节点收到这个请求后,检查自己是否与节点 j 直接交易过。如果没有,则忽略该请求(如图 2 中节点 k_n);否则,设该节点为 k(也可能是个节点集,设为 K,如图 2 中节点 k_1 与 k_2,也称为目击节点),节点 k 将这些历史信息 $Info(k,j)$发送给节点 i,如图 2 所示。

Step3 当节点 i 将所有返回的这些信息收集起来后,形成推荐信任度 $R(k,j)$,就结合自己对节点 j 的理解 $Info(i,j)$,以及自己对目击节点的可信度 $C(i,k)$计算 j 的可信度 $T(i,j)$,其公式大致如下:

$$T(i,j)=\alpha * Info(i,j)+\beta * R(k,j)$$

其中,$R(i,j)=\frac{\sum_{k\in K} Info(k,j) * C(i,k)}{|K|}$,$\alpha+\beta=1$。

这个公式分为两部分:第一部分是对自己和 j 交易的直接信息 $Info(i,j)$的计算,后一部分 $R(k,j)$是对其他节点提供的与节点 j 的交易信息 $Info(k,j)$的计算。一般给予自己的亲身体验更高的信任,因此通常 $\alpha>\beta$。当计算出 $T(i,j)$后,节点 i 根据自身的服务选择策略选择决定是否与具有相应 $T(i,j)$的节点作为服务提供节点。

Step4 当节点 i 与节点 j 交易之后,节点 i 就得更新对 j 的新的交易信息,这些信息不仅用于修改 $Info(i,j)$,还用来调整节点 i 对其他节点 k 的可信度 $C(i,k)$,并将最新的 $T(i,j)$发送到指定的存储系统中。

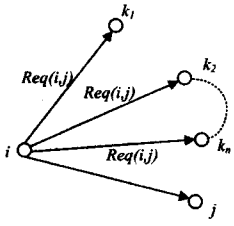

图 1 发送查询请求

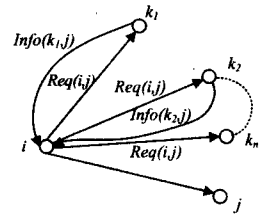

图 2 接收应答信息

信任模型是信誉系统中最关键的组成部分。除此之外,信誉系统中还包括信誉信息的存储机制、搜索机制(路由)和传输机制等。在面向具体的 P2P 应用环境、不同的应用需求及构建基于信誉的信任模型工具与策略上,其模型的表现形式与计算过程会有一定的差异,但其基本思想却是一致的。我们将在下一节对分布式环境下典型的基于信誉的信任模型进行分析与归纳。

3 典型的基于信誉的信任模型

许多学者研究各种分布式应用中动态的信任关系,并使用不同的数学方法和工具建立了信任关系的模型。本节将根据其采用数学方法的不同,选取一些新的、典型的模型进行介绍和评述。

3.1 EigenTrust

Kamvar 等人[13]针对 P2P 系统中文件共享系统提出一种基于信誉的全局信任模型 EigenTrust。在该模型中,任意节点的全局信誉决定于与之发生过交易行为的其它节点对其的局部看法以及所有这些节点的局部信誉全局聚合。如果以加权有向图 $G\langle V,E\rangle$来表示这种交互关系,设$|G|=n$,$V=\{i|\exists j,i\overset{R_{ij}}{\leftrightarrow}j\cdots$,其中 $i\overset{R_{ij}}{\leftrightarrow}j$ 表示节点 i,j 发生过交易。这样,实际上就构造了一个以加权有向图形式表示的社会网络。在该网络中,个体间的关系为由交易带来的评价关系,关系的强度为个体间的局部信任度。

当节点 i 需要了解任意节点 k 的全局信誉时,首先从 k 的交易伙伴(曾经与 k 发生过交易的节点)获知节点 k 的推荐信息,然后根据所有这些交易伙伴自身的局部可信度综合出

k 的全局信誉，即

$$T_k=\sum_j C_{ij} * T_{jk} \tag{1}$$

对于任意节点 i,j，C_{ij} 为节点 i 对节点 j 的局部信任度，T_i 为节点 i 全局信誉。

$$C_{ij}=\frac{Sat_{ij}-UnSat_{ij}}{\sum_j(Sat_{ij}-UnSat_{ij})} \tag{2}$$

其中，Sat_{ij} 和 $UnSat_{ij}$ 分别为节点 i 对 j 在历史交易中积累的满意次数和不满意次数。

正如 Bonachi 等人[14]指出，上述通过线性方程组求解节点中心性的方法存在可解性问题，为此 EigenTrust 提出的一个补救策略是：假定网络中始终预先存在一个固定的亚可信的节点集合 P，P 中的节点拥有至少 $T_{i(i\in P)}>\Psi$ 的全局可信度。在该假定的前提下，式(1)变为：

$$T_k=(1-\alpha) * \sum_j(C_{ij} * C_{jk})+\alpha * t_i \tag{3}$$

其中，$t_i=\begin{cases}0, & t_i\notin P\\ t_i=\dfrac{\Psi}{\alpha}(0<\alpha<1), & \text{otherwise}\end{cases}$，这保证了 C 的不可约性和非周期性，从而保证了式(3)对应线性方程组的可解性。

EigenTrust 模型具有如下优点：

(1)该模型对非结构化 P2P 系统中简单恶意节点、共谋恶意节点、基于振荡的策略性节点及组间共谋作弊行为有较好的抑制效果；(2)该模型在大规模分布式环境下的可扩展性与伸缩性较优，并且基于全局收敛，能更精确地反映系统中各节点的信誉状况，能更好地指导系统健康稳定地运行。

但该模型也存在明显的不足：

(1)迭代的收敛性假设不合理。EigenTrust 为解决模型的收敛性问题，先验性地确定一些具有比较高的不可更改的预信任节点。这样的假设一方面缺乏事实的合理性，另一方面在实际应用中如何操作也是较难解决的问题；(2)该模型中采用的全局迭代算法，其复杂度高达 $O(n^2)$(n 为系统规模)，这在很大程度上抑制了该模型的工程可行性；(3)模型没区分节点可信度与可靠度的概念，且粒度较粗，不能很好地解决同一节点在不同领域、不同方面的可信度计算问题。

3.2 PeerTrust

PeerTrust 是由 Li Xiong 等人[15]提出的一种针对 P2P 在线社区的基于信誉的信任模型。PeerTrust 模型在基于推荐构造信誉的原理上类似于 EigenTrust，都是基于节点间的相互推荐进行全局信誉评价。但是，从信誉评价的全面性和合理性角度出发，其中引入了更多的信誉评价因素，在具体的推荐算法上也更为复杂。PeerTrust 中任一节点 u 的信誉形如：

$$T(u)=\alpha * \sum_{i=1}^{I(u)}S(u,i) * Cr(p(u,i)) * TF(u,i)+(1-\alpha) * CF(u) \tag{4}$$

对应于一定的时间范围，$I(u)$ 为 u 对外提供服务的总数，$p(u,i)$，$S(u,i)$ 和 $TF(u,i)$ 分别为其中 u 的第 i 次服务的服务对象、获得的服务评价反馈和相关的服务上下文信息。$Cr(v)$ 为节点的反馈可靠程度，$CF(u)$ 为与环境相关的上下文。在模型中，通过一个调节因子 $\alpha(0<\alpha<1)$ 控制两部分信誉参数对节点信誉的影响。

在 PeerTrust 模型中，根据反馈可靠程度评价算法的不同，可以分为基于迭代的全局信任模型 PeerTrust-TVM 和基于相似度的局部信任模型 PeerTrust-PSM 两类。其中，PeerTrust-TVM 采用了与 EigenTrust 类似的做法，亦即使用节点的全局信誉度量节点反馈的可靠程度。而 PeerTrust-PSM 中，反馈可靠程度具体体现为所谓的节点反馈相似性。虽然从信誉的构造上，基于反馈相似性评价反馈的可靠程度较之以节点信誉作为反馈可信度的做法更具合理性，但是由于进行全局的反馈相似度计算通常会带来较高的计算代价，以此为基础构造全局信誉必然加重信誉计算的负担，因此该方法很难在全局信誉的构造上得到应用。

基于迭代的全局信誉模型 PeerTrust-TVM 形如：

$$T_{TVM}(u)=\alpha * \sum_{i=1}^{I(u)}S(u,i) * \frac{T(p(u,i))}{\sum_{i=1}^{I(u)}T(p(u,i))} * TF(u,i)+(1-\alpha) * CF(u) \tag{5}$$

其中，$P(u)$ 为 u 的所有服务对象的集合。

注意到，如果式(5)中令 $S(u,i)=\dfrac{\delta(i)}{\sum_{v\in P(u)}(Sat_{vu}-UnSat_{vu})}$，当 $S(u,i)$ 对应的是满意的评价时，$\delta(i)$ 为 1，反之为 -1，同时取 $\alpha=1$，$TF(u,i)=1$，$Cr(u)=T(u)$，则式(5)将退化为和式(4)相同的形式。这说明，相对于 EigenTrust 模型，PeerTrust 模型是更加通用和灵活的。

基于相似度的局部信任模型 PeerTrust-PSM 形如：

$$T_{PSM}(u)=\alpha * \sum_{i=1}^{I(u)}S(u,i) * \frac{\mathrm{Sim}(p(u,i),w)}{\sum_{j=1}^{I(u)}\mathrm{Sim}(p(u,j),w)} * TF(u,i)+(1-\alpha) * CF(u) \tag{6}$$

其中，$\mathrm{Sim}(v,w)=\sqrt{\dfrac{\sum_{x\in IJS(v,w)}\left(\frac{\sum_{i=1}^{I(x,v)}S(x,i)}{I(x,v)}-\frac{\sum_{i=1}^{I(x,w)}S(x,i)}{I(x,w)}\right)^2}{|IJS(v,w)|}}$，$IJS(i,j)$ 表示同时与节点 i 与节点 j 交互过的节点集合。

作为一种相对全面刻画在线社区安全可信因素的信任模型，PeerTrust 的优势主要体现在：

(1)引入了服务上下文信息 $TF(u,i)$ 作为信誉评价的参数，能够更好地反映节点实际贡献的差异，对节点信任的刻画更加准确。事实上，以 P2P 文件共享为例，从共享的代价和服务的可靠性上，1MB 的成功文件传输服务和 1GB 的成功文件传输显然具有很大的差异，然而包括 EigenTrust 和 P2PRep[16]等在内的大多数信誉机制在信誉构造的过程中都忽略了这一节点贡献事实上的差异。这一方面可能造成对节点信誉评价的不精确，另一方面会导致在基于信誉现实激励过程中事实上的不平等，为节点大量伪造虚假的服务评价创造了条件。

(2)基于归一化的参数 α 平衡收集的信誉信息和环境上下文因素使得信誉的构造更加全面和灵活。可以看到式(8)和式(9)中的信誉计算分为两部分：第一部分类似于 EigenTrust 的全局信誉模型，通过对节点收到的对其既有服务情况的评价的综合，预测其未来服务的可靠性；第二部分则通过环境相关的因素来对第一部分的结果进行调节。不同的 α 反映了不同情况下信誉评价对服务证据集合和环境因素的不同依赖程度，这无疑会使得信誉评价方式本身更加全面和灵活。

总体来看，PeerTrust 模型在信誉刻画的全面性和灵活性上较 EigenTrust 模型有了明显的进步，但是由于它和 EigenTrust 都采用了相似的线性信任模型，因而也有如下的不足：(1) PeerTrust-TVM 为全局信任模型，也存在如同 EigenTrust 的收敛性问题，且计算复杂度较高，这使其在大规模分

布式条件下的工程可行性大打折扣；(2)PeerTrust-PSM 为局部信任模型，只能由有限的直接交互节点计算出节点的信任度，并不能精确反映整个系统对该节点的全局判断；(3)模型中采用环境上下文作为对节点行为的激励因素，且缺乏对恶意节点的惩罚机制，激励效果明显不足。

3.3 Beth's model

Beth 等人[17]提出了基于经验和概率统计的信任评估模型，模型引入了经验的概念用以表述和度量信任，并给出了由经验推荐所引出的信任度的推导和综合计算公式。

在 Beth 信任度评估模型中，经验被定义为对某个实体完成某项任务的情况记录，对应于任务的成败，经验被分为肯定经验和否定经验。若实体任务成功，则对其肯定经验计数增加；若实体任务失败，则否定经验计数增加。模型中的经验可以由推荐获得，而推荐经验的可信度问题同样是信任问题。为此，模型将信任分为直接信任和推荐信任。直接信任定义为“若 P 对 Q 的所有(包括直接的或由推荐获得的)经验均为肯定经验，则 P 对 Q 存在直接信任关系”。当 Q 被信任时，Q 能成功完成任务的概率被用于评价这种信任关系，而概率的计算则取决于 P 对 Q 的肯定经验记录。Beth 采用以下公式描述直接信任度 $v_e(p)$ 与肯定经验记录的关系：

$$v_e(p)=1-\alpha^p \tag{7}$$

其中，P 是所获得的关于 Q 的肯定经验数，α 是对 Q 成功完成一次任务的可能性期望值。该公式是基于 Q 完成一次任务的可能性在[0,1]上均匀分布这一假设。推荐信任定义为“若 P 愿意接受 Q 提供的关于目标实体的经验，则 P 对 Q 存在推荐经验关系”。Beth 采用肯定经验与否定经验相结合的方法描述推荐信任度。推荐信任度与经验记录的关系采用如下公式描述：

$$v_r(p,n)=\begin{cases}1-\alpha^{p-n}, & p<n\\ 0, & \text{else}\end{cases} \tag{8}$$

其中，p,n 分别是 P 所获得的关于 Q 的肯定和否定经验数。

在 Beth 信任度评估模型中，经验可以通过推荐获得。而对于同一个信任关系，多个不同的经验推荐者可能形成多条不同的推荐路径。这就需要有一个计算方法能够推导并综合所有推荐路径的经验信息，以获得一致的信任度。Beth 分别对直接信任和推荐信任进行了讨论，并给出了相应的信任度推导和综合计算公式。假设 A 对 B 的推荐信任度为 V_1，B 对 C 的直接信任度为 V_2，B 对 D 的推荐信任度为 V_3，则 A 对 C 的直接信任度推导公式表述为

$$V_1 \odot V_2=1-(1-V_2)^{V_1} \tag{9}$$

A 对 D 的推荐信任度可以简单地表述为 $V_1 \cdot V_2$。Beth 模型还给出了推荐信任度综合计算公式：

$$V_{com}=\frac{1}{n}\sum_{i=1}^{n}V_i \tag{10}$$

其中，$V_i(i=1,\cdots,n)$ 是由单个推荐路径而推导出的信任度，综合推荐信任度 V_{com} 是这些单个信任度的简单算术平均。

设 $P_i(i=1,\cdots,m)$ 是推荐路径上各不相同的最终推荐实体，V_i· 表示其最终推荐实体为 P_i 的各条推荐路径的信任度，则直接信任度综合计算公式表述为

$$V_{com}=1-\prod_{i=1}^{m}\sqrt[n_i]{\prod_{j=1}^{n_i}(1-V_{i,j})} \tag{11}$$

该式考虑了同一个经验推荐者出现在不同推荐路径上的情况。相同的经验信息经不同的路径被多次传递，产生不同的推导结果。该式采用取推导值平均的方法得到一个唯一值。

该模型具有如下优点：(1)该模型对信任的划分与定义明确，利用概念分布的方法来表达信誉的主观性与不确定性，能较好地反映期待信誉的信任模型内涵；(2)该模型采用简单的算术平均或几何平均来计算推荐信任度与直接信任度，结构简单，在实际应用中易于部署，操作性强。

但该模型也存在明显的不足：(1)模型基于概率统计方法描述和度量信任关系，缺少信任理论基础，方法的合理性有待检验；(2)对信任度的计算仅采用简单的平均值处理，过于粗糙，不能有效防止 P2P 环境下恶意节点针对信誉系统本身进行的各种欺诈作弊和攻击行为；(3)对直接信任的定义比较严格，但模型中仅采用肯定经验对信任关系进行度量，过于片面，不能完整刻画实际信任关系。

3.4 Jøsang's model

Jøsang 等人[18,19]引入了事实空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系，并提供了一套主观逻辑(subjective logic)运算子用于信任度的推导和综合计算。

事实空间由一系列实体产生的可观察到的事件组成。实体产生的事件被简单地划分为肯定事件(positive event)和否定事件(negative event)。Jøsang 基于 Beta 分布函数描述二项事件(binary event)后验概率的思想，给出了一个由观察到的肯定事件数和否定事件数决定的概率确定性密度函数 pcdf，并以此来计算实体产生某个事件的概率的可信度。设概率变量为 θ，r 和 s，分别表示观测到的实体所产生的肯定事件和否定事件数，则 pcdf 公式表述为

$$\varphi(\theta|r,s)=\frac{\Gamma(r+s+2)}{\Gamma(r+1)\Gamma(s+1)}*\theta^r*(1-\theta)^s,$$
$$0\leqslant\theta\leqslant 1,r\geqslant 0,s\geqslant 0 \tag{12}$$

观念空间则由一系列对陈述的主观信任评估组成。主观信任度由三元组 $\omega=\{b,d,u\}$ 描述。该三元组满足：

$$b+d+u=1,\{b,d,u\}\in[0,1] \tag{13}$$

其中 b,d 和 u 分别描述对陈述的信任程度、不信任程度和不确定程度。Jøsang 使用式(14)将 ω 定义为事实空间中肯定事件数 r 和否定事件数 s 的函数：

$$\begin{cases}b=\dfrac{r}{r+s+1}\\ d=\dfrac{s}{r+s+1}\\ u=\dfrac{1}{r+s+1}\end{cases} \tag{14}$$

并认为 ω 与 pcdf 在主观信任度的表达上是等价的，也即可以通过事实空间的统计事件来描述主观信任度。

Jøsang 信任度评估模型提供了一套主观逻辑算子，用于信任度之间的运算。其主要的算子有合并(cojunction)、合意(consensus)和推荐(recommendation)。其中合并用于不同信任内容信任度的综合计算；合意根据参与运算的观念(信任度)之间的关系分为独立观念间的合意、依赖观念间的合意和部分依赖观念间的合意 3 类。所谓观念依赖是指观念是否部分或全部由观察相同的事件所形成，合意主要用于对多个相同信任内容信任度的综合计算，推荐主要用于对信任度的推导计算。

与 Beth 模型相比，Jøsang 模型对信任的定义较宽松，同时使用了事实空间中的肯定事件和否定事件对信任关系进行度量。它的主要优点有：

(1)模型引入事实空间与观念空间多角度来描述基于信誉的信任度，且在观念空间中明确区别信任度与不确定度，能较为全面地反映节点的信任度；(2)提供一套主观逻辑算子进行各种信任度的聚合，能比较方便、有效地得到节点的最终信任度。

因为它同样是一种基于概率分布的信任模型，同样存在 3.3 节中(1)所描述的问题。除此之外，还存在如下不足：(1)模型没明确区分直接信任和推荐信任，而是通过推荐算子来间接推导，这种方法缺乏信任理论支持，其逻辑的严格性有待考证；(2)该模型仅用事实空间的后验事件概率的方式来表达信任度，用观念空间中简单的数值计算来刻画信任关系与不确定度，方法过于粗糙，与 Beth 一样也不能有效地消除恶意推荐带来的影响。

$$st_{n+1}(a,b)=\begin{cases} st_n(a,b)+\alpha * rt(a,x)(e_{n+1}(x,b)-st_n(a,b)), & e_{n+1}(x,b)-st_n(a,b)\geqslant -\varepsilon \\ st_n(a,b)+\beta * rt(a,x)(e_{n+1}(x,b)-st_n(a,b)), & \text{else} \end{cases} \tag{15}$$

其中，$\alpha,\beta\in[0,1]$，$st_1(a,b),st_2(a,b),\cdots,st_{n-1}(a,b),st_n(a,b)$，$st_{n+1}(a,b)$是基于连续时间帧 a 对 b 的信任评价，$rt(a,x)*e(x,b)$表示推荐信任，α 和 β 分别为信任增加或者减少的学习因子。参数 $\varepsilon>0$ 规定了交互满意度评价时的误差容忍范围。如果交互的评价潜在地受噪音的影响，那么较高的学习因子会使信任评价产生较大的偏差。

长期信任定义为

$$lt_{n+1}(a,b)=\frac{w_s(n+1)}{n+1}\left[\frac{n}{w_s}lt_n(a,b)+rt(a,x_i)e_{n+1}(x_i,b)\right] \tag{16}$$

其中，$w_s(n)=n/\max(n,n_{\min})$反映了计算长期信任时，时间戳 n 的个数太小，不能反映出长期的历史累积信任。

惩罚因子定义为

$$pt_n(a,b)=\frac{macc_n(a,b)}{c+macc_n(a,b)} \tag{17}$$

其中，$macc_n(a,b)$表示累积的交互失败的次数，正常数 c 控制着惩罚因子趋向于 1 的速度。

信任度聚合函数定义为

$$t_n(a,b)=\min(st_n(a,b),lt_n(a,b)) \tag{18}$$

惩罚因子集成于近期信任、长期信任之中，即 $lt_n(a,b)=lt_n(a,b)(1-pt(a,b))$和学习因子 $\alpha=\alpha(1-pt(a,b))$。

该模型的主要优点是：(1)引入近期信任、长期信任、惩罚因子和推荐信任 4 个参数来反映节点信任度，通过反馈控制机制，动态调节计算节点的信任值的上述参数；(2)提出了用机器学习中强化学习的方法计算信任度，并用惩罚因子对学习因子进行了明确定义，所以该模型是一个自适应的系统；(3)对新发生的交互行为有足够的敏感性，提高了信任模型的动态适应能力；(4)通过惩罚机制，可以有效减少不诚实节点，特别是合伙欺骗节点提供的虚假反馈。

该模型的不足之处是：

(1)只根据邻居节点的推荐计算推荐信任值，计算得到的是一种局部信任度，影响了信任评估的准确性；(2)信任度取短期信任和长期信任中的最小值，虽然有利于提高安全性，但这也限制了模型的服务范围，许多节点的服务请求由于近期的一些误操作而会被拒绝。为了提高模型的适应能力，需要进一步改进。

3.6 Yao Wang's model

Yao Wang 等人[22]提出了基于贝叶斯(Bayesian)的信任模型。该算法的特点在于以信任的概率值作为节点的属性。

3.5 Claudiu's model

Claudiu 等人[20]提出了一种 P2P 环境下基于机器学习中强化学习[21]方法的动态信任模型。信任度的取值范围也是采用集合[0,1]。与其他 P2P 信任模型显著不同的是，它引入近期信任、长期信任、惩罚因子和推荐信任 4 个参数来反映节点信任度。节点 a 对 b 基于连续时间戳的近期信任 $st_{n+1}(a,b)$定义为强化学习的模型：

该模型中信任被分为两类：一类是基于文件提供者自身宣告的文件信息内容的真实品质和传送速度能力的可信度，另一类是进行评估推荐的其他节点可靠性的信任。此外，信任值被划分为两种值：满意(+1)和不满意(−1)。根据以上定义的属性，使用贝叶斯规划来表示评估节点和文件提供者间的信任值，并给出了一个根据其他节点的推荐来计算某一节点信任值的迭代公式：

$$r_{ij}=w_t * \frac{\sum_{l=1}^{k}(tr_{il} * tr_{lj})}{\sum_{l=1}^{k}tr_{il}}+w_s * \frac{\sum_{z=1}^{g}t_{zj}}{g} \tag{19}$$

其中，$w_t+w_s=1$；r_{ij}表示针对节点 j 提供的服务，节点 i 收到关于 j 的总的信任推荐值；k 与 g 分别表示可信参考与未知参考的数量；tr_{il}表示节点 i 对可信参考 l 的可信度；t_{lj}表示可信参考 l 对服务提供者 j 的可信度；t_{zj}表示未知参考 z 对服务提供者 j 的可信度。w_t 和 w_s 分别表示来自可信参考与未知参考推荐重要性的权重。

需要说明的是，推荐者包括两类：一类是可信参考，即大多数时候与节点 i 有类似的观点或偏好的节点，并且与服务提供节点 j 有直接交互历史，这类节点的可信度较高；另一类被称为未知参考，即对节点 i 而言没交互历史、完全陌生的节点，但与服务提供节点 j 有直接交互历史，这类节点的可信度相对较低。该模型使用贝叶斯公式的先验概率理论来预测一个节点将来行为的信誉，而这一预测的前提是基于和该节点有过历史交易记录的其他节点进行评估的概率值。

节点 i 是否选择服务提供者 j 提供的服务，决定于一个阈值 θ。如果 $r_{ij}>\theta$，则 i 会与 j 交易，否则不会。

该模型的优点是：(1)Bayesian 网络理论天然的不确定知识表达与推理特性比较符合基于信誉的信任模型不确定性和动态性特点，因此利用这一理论建模非常适合于这类信任模型的需求；(2)P2P 网络中节点的信任是面向领域与方面的，该模型利用 Bayesian 网络可以灵活地刻画不同的信任属性，并且综合不同方面的信任值。

但其缺点也十分明显：

(1)没有给出全局或局部的信任度评估模型，仅仅给出了一个基于推荐信任链的推荐信任模型，也没考虑直接信任在信任评估中的影响因素；(2)没有说明信任值的初始化问题，如两个实体进行初次交互时如何建立信任；(3)对可信参考与未知参考的界定缺乏明确的尺度与标准，实际操作难以控

制。

3.7 各模型的比较

表1对本节介绍的各模型算法进行了比较。表中提出了10个指标，前面6个指标对模型的各种特性进行了描述：Context aware，用来描述模型是否能对服务上下文(比如对文件共享服务来说，文件的大小、类型和传输带宽等)或环境上下文(主要可以反映环境因素对节点信誉的影响，比如节点所在的拓扑位置的特点以及节点的信誉特征等)进行感知的指标；Reputation scoring 用来描述模型中信任的评级方式，如eBay中采用的+1，0，−1的评分方式；Arith-mothod 表示模型的构建方式或机理；Implementation 表示该模型是否用数学方法实现；Decentralized 表示模型按控制方式分类的情况，即是集中式的还是分布式的或混合式的；Evaluation scope 表示模型的评估范围，即是局部的还是全局的。后面4个指标对模型的性能进行了多维刻画：Veracity 对模型中计算出的节点的信任度的精确程度进行了描述；Scalability 描述了模型的可伸缩性；Robustness 表示模型的抗攻击、防欺诈作弊行为的能力；Overhead 指模型的计算成本。

表1 典型的基于信誉的信任模型比较

Index Collection	EigenTrust	PeerTrust	Beth	Jøsang	Claudiu	Yao
Context aware	No	Yes	No	No	Yes	Yes
Reputation scoring	0 or 1	[0,1]	[0,1]	[0,1]	[0,1]	−1 or +1
Arith-method	Linear iteration	Linear iteration	Probability distribution	Probability distribution	Machine learning	Bayesian
Implementation	Yes	Yes	Yes	Yes	Yes	Yes
Decentralized	Yes	Yes	Yes	Yes	Yes	Yes
Evaluation scope	Global	Global/Local	Local	Local	Local	Local
Veracity	Good	Better	Low	Lower	Low	Good
Scalability	High	High	Low	Low	High	Low
Robustness	Good	Good	Low	Low	Best	Low
Overhead	High	Lower	Low	Low	High	Low

4 当前研究存在的问题

目前对基于信誉的信任模型的研究还处于起始阶段，存在一些明显的问题：

(1)对信任定义的观点不一致。“信任”最早在社会学与经济学中得到广泛的研究与应用，后来被引入到计算机科学。信任关系是最复杂的社会关系之一，也是一个非常复杂的主观心理认知过程，它取决于很多因素或证据，而信誉只是构成信任的因素之一。目前，计算机科学领域虽然结合不同的应用环境，对信任进行了大量的研究，但国内外对信任的定义还没形成统一的理解与认识。

(2)信任模型的多样性。基于应用背景和构建信任模型的方法与手段的多样性决定了信任模型的多样性。目前就P2P环境来说，信任模型主要用于电子商务、在线社区和资源共享服务，这些领域无中心化、全分布和匿名的特性导致节点的行为只取决于其自身的利益判断或行为准则，是其自主决策的结果，不受系统本身的控制，因此基于信誉的手段成为解决这类系统可信问题的首选。当然，针对某一具体应用背景，可以用多种策略与方法来构建基于信誉的信任模型，比如基于角色[23]、Bayesian[22]、模糊集[24]和确定性理论[25]等。

(3)模型中信任的表述和度量的合理性有待于进一步研究，许多模型倾向于采用事件概率的方式来表述和度量信任关系，都是基于一定的概率分布假设，缺少信任理论基础，方法的合理性有待检验。

(4)信任模型与信誉信息管理的P2P拓扑结构耦合性太强，模型缺乏普适性。

(5)目前大多数模型只停留在理论学术研究阶段，考虑到成本和实现的具体细节问题，不能在具体的应用中真正实现应用部署。对模型效用的评估大多通过实验仿真的手段作出分析判断，无法在实践中真正得到检验与优化。

(6)大多数模型的目的是实现系统中节点信任度的评估，而激励机制相对不足。目前对激励机制的研究大多基于微支付[26]或信誉的方式，实现对系统中不良行为的抑制及差异化服务。而通过微支付方式实现激励时多数模型只是通过简单的虚拟货币奖励机制，惩罚力度不够，不能真正有效地规范约束P2P环境下各节点的交易行为；通过信誉的方式实现激励时，往往只将信誉作为服务选到的依据，而较少考虑以之作为服务提供反馈的依据，并不能从本质上改变节点缺乏积极贡献动机的现状。

结束语 目前，有关P2P的应用日益广泛，但仍然缺乏有效的信任机制来提高系统整体的可用性。P2P系统中节点具有高度的自主性，节点间的状态具有动态性和不确定性，决定了其可信问题的特殊性。基于信誉的信任模型成为解决P2P环境中可信问题的一种非常有效的手段。本文对信任与信誉的定义与相互关系进行了分析，给出了基本的信任模型运行机理。在此基础上，对P2P环境下典型的基于信誉的信任模型做了分析与评述。现在对P2P环境下的信任问题的研究还处在起步阶段，在实际应用中还没有一个通用的解决方案，对信任和信誉机制的研究还有待进一步深化。随着包括P2P在内的分布式技术的不断发展，除了经典的可信问题外，各种新的可信问题正不断出现，需要对这些问题的内在机制与特点做更深入的研究与分析，以提出一种普适性、健壮性和可靠性更优的解决方案。具体来说，还需要在以下几个方面做进一步研究：

(1)理论研究。结合具体的应用环境进一步深入分析信任、信誉的表述、度量方式及相互关系，并对其合理性做形式化分析与验证。

(2)模型评价机理研究。一般模型大多以节点最终的信任度的高低作为交易或服务选择的唯一客观标准，而忽视一些应用场景下主观尺度的作用。

(3)信任模型通用化研究。为增强模型的普适性，进一步节省重复研究开发的成本，研究一种不仅可以适用于P2P环境下不同拓扑结构，而且不用或只需少量的修改就可以应用于其它分布式计算环境(如网格计算和普适计算等)的通用模型。

(4)模型的应用研究。将学术研究的成果转化为实际的生产力，将其产品化，并部署到实际的分布式应用环境中，不

(下转第16页)

tor map using digital watermarking method based on discrete Fourier transform[C]// International Geoscience and Remote Sensing Symposium (IGARSS). 2001(3):1191-1193

[21] Voigt M, Yang B, Busch C. Reversible watermarking of 2D-vector data[C]// Proceedings of the 2004 ACM Internation Workshop on Multimedia and security. Germany, Magdeburg, 2004: 160-165

[22] 姚惠明,周冠玲,杨义先,等. 一种基于矢量共享方案的 DCT 域上数字水印分存算法[J]. 计算机学报,2004,27(7):998-1003

[23] 李媛媛,许录平. 矢量图形中基于小波变换的盲水印算法[J]. 光子学报,2004,33(1):97-100

[24] Wen Q, Sun T F, Wang S X. Concept and application of zero watermark[J]. ACTA Electronica Sinica, 2003, 31(2): 214-216

[25] 李庆诚,窦毅. 数字水印的解释攻击与关联性特征[J]. 计算机应用研究,2005(5):115-117

[26] 邵承永,汪海龙,牛夏牧. 基于统计特征的二维矢量地图鲁棒水印算法[J]. 电子学报,2005,33(12):2312-2316

[27] 闵连权. 一种鲁棒的矢量地图数据的数字水印[J]. 测绘学报,2008,37(2):262-267

[28] 王忠军,王玉海,王豪. 一种鲁棒的矢量地图数字水印算法[J]. 测绘科学,2008,33(4):148-150

(上接第 6 页)

仅可以发挥其实际效用,还可以对其功能进行验证,以便进一步对其进行修正,使其更完善合理。

(5)模型构建方法研究。可以进一步结合计算机科学其它分支(如人工智能、机器学习)和其它学科或技术手段构建更有效、更合理、更实用的信任模型。

参 考 文 献

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

[2] Jøsang A, Tran N. Trust Management for E-Commerce. 2000

[3] Koutrouli E, Tsalgatidou A. Reputation-based trust systems for P2P applications: design issues and comparison framework[C]// LNCS 4083. 2006: 152-161

[4] Weeks S. Understanding trust management systems[C]// Proc. of the 2001 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2001: 94-105

[5] RFC 1422. Privacy Enhancement for Internet Electronic Mail, Part 2: Certificate-based Key Management

[6] Gambetta D. Can We Trust Trust [C]// Gambetta D, ed. Trust: Making and Breaking Cooperative Relations. Basil Blackwell, Oxford, 1990: 213-238

[7] The Gnutella Protocol Spec. v0.6, Intelligent Club Management in Peer-to-Peer Networks[C]// Proceedings of Workshop on Economics of P2P Systems (P2PECON '03). Berkeley, CA, 2003

[8] KaZaA file sharing network[EB/OL]. http://www.kazaa.com/, 2002

[9] Resnick P, Zeckhauser R. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system[C]// NBER Workshop on Empirical Studies of Electronic Commerce. California, 2000

[10] Rindova V P, Kotha S. Building reputation on the Internet: Lessons from amazon.com and its competitors. 2006-03-27

[11] McKnight D H, Chervany N L. The Meaning of Trust[R]. MISRC Working Paper Series 96-04. Management Information Systems Research Center, University of Minnesota, 1996

[12] Jøsang A, Ismail R, Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision[J]. Decision Support Systems, 2005

[13] Kamvar S D, Schlosser M T, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks[C]// Proceedings of the 12th International World Wide Web Conference. Budapest, Hungary: ACM Press, 2003: 640-651

[14] Bonachi P. Eigenvector-like Measures of Centrality for Asymmetric Relations[J]. Social Networks, 2001, 23(4): 191-201

[15] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities[J]. IEEE Transactions on Data and Knowledge Engineering (Special Issue on Peer-to-Peer Based Data Management), 2004, 16(7): 843-857

[16] Oram A. Peer-to-Peer: Harnessing the Power of Disruptive Technologies[M]. O'Reilly and Associates, 2001

[17] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Network[C]// Proceedings of the European Symposium on Research in Security. 1994

[18] Jøsang A. The right type of trust for distributed systems[C]// Meadows C, ed. Proceedings of the 1996 New Security Paradigms Workshop. Lake Arrowhead, CA: ACM Press, 1996

[19] Jøsang A. A model for trust in security systems[C]// Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. 1997

[20] Kaelbling L P, Littman M L, Moore A W. Reinforcement learning: A survey[J]. Journal of Artificial Intelligence Research, 1996, 4: 237-285

[21] Kinateder M, Baschny E, Rothermel K. Towards a generic trust model—Comparison of various trust update algorithms[C]// Proc. of the iTrust 2005. LNCS 3477. 2005: 177-192

[22] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks[C]// Moro G, ed. Proc. of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004: 23-34

[23] Khambatti M, Dasgupta P, Ryu K D. A role-based trust model for Peer to Peer communities and dynamic coalitions[C]// The Second IEEE International Information Assurance Workshop. New York: IEEE Press, 2004: 141-154

[24] Nefti S, Meziane F, Kasiranl K. A fuzzy trust model for e-commerce [C]// The 7th IEEE Int'l Confon E-Commerce Technology (CEC'05). Edinburgh, UK, 2005

[25] Wright T. A simple algorithm for tighter exact upper confidence bounds with rare attributes in finite universes [J]. Statistics & Probability Letters, 1997, 36(1): 59-67

[26] Golle P, Leyton-Brown K, Mironov I. Incentives for sharing in peer-to-peer networks [C]// Wellman M P, Shoham Y, eds. Proc. of the 3rd ACM Conf. on Electronic Commerce. New York: ACM Press, 2001: 264-267