第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0143—03 文献标识码：A 中图分类号：TP309

基于信任和推荐的 P2P 信誉模型

席 菁[1]，王 源[2]，陆建德[2]
(1. 苏州大学计算机学院，苏州 215006；2. 江苏省计算机信息处理技术重点实验室，苏州 215006)

摘 要：分析现有信誉模型，提出一种使用信任机制和推荐机制的 P2P 信誉模型，利用决策树思想优化该模型。给出一种在分布式 P2P 系统中存取全局信任值的方法，解决了单点失效问题。实验结果表明，该模型对信任值的估算准确度以及判别虚假节点的能力高于现有模型。
关键词：对等网；信誉模型；信任值；推荐

P2P Reputation Model Based on Trust and Recommendation

XI Jing[1], WANG Yuan[2], LU Jian-de[2]
(1. School of Computer, Soochow University, Suzhou 215006;
2. Jiangsu Provincial Key Laboratory of Computer Information Processing Technology, Suzhou 215006)

【Abstract】 This paper analyzes existing reputation models, proposes a P2P reputation model using trust mechanisms and recommendation mechanisms, and optimizes the model by the mentality of decision tree. It puts forward a method that can access global trust value in distributed P2P system, and resolves signal peer invalid problem. Experimental results prove that this model is better than existing models in estimating trust value accuracy and distinguishing untrue peers.
【Key words】 P2P; reputation model; trust value; recommendation

1 概述

P2P 技术是目前计算机网络技术研究领域的一个热点。P2P 系统允许任何用户共享资源且无须通过中央服务器。在传统网络中，可以较容易地解决依靠单一服务器的网络信任问题。但在 P2P 网络中，节点之间的信任问题成为阻碍 P2P 发展的难点之一。为了确定大量未知节点之间的信任关系，出现了基于不同方法的各种信誉模型。P2PRep[1]是基于投票的信誉机制，它可以在 Guntella 上添加一层信誉安全协议，用于在资源搜索后进行节点选择。文献[2]提出一种基于 P-Grid 的结构化信誉模型，该模型只记录节点的负面评价，没有量化信任值。EigenTrust[3]是一种流模型，其优点是计算可信度时基于全局范围，客观性较高，但其性能很低且没有考虑“冒名”问题。针对电子商务的应用，文献[4]提出 PeerTrust 模型和因素集合概念，但该模型无法作为一种通用模型推广。

上述信誉模型没有很好地处理推荐和信任的关系，且效率较低。鉴于此，本文提出一种实用性较高的新信誉模型。

2 现有 P2P 信誉模型

现有 P2P 信誉模型具有多样性，根据所采用节点信任方式的不同，主要分为以下 4 类：

(1)基于 PKI 的模型。有少数领袖节点，领袖节点的合法性通过 CA 颁发的证书加以保证。基于此类模型的系统一般都是中心依赖的，易发生单点失效问题。

(2)基于局部推荐的模型。节点通过询问有限的节点获取某个节点的可信度，一般采用局部广播获取节点信任度。此类系统得到的信任度较片面，容易受到非可信节点和恶意节点的攻击。

(3)基于数据签名的模型。不追求节点可信度，只强调数据可信度，通过数据签名保证数据可信度。该类系统文件保存的数据签名数据量很大，且验证这些签名须花费大量时间。

(4)全局可信度模型。获取节点的全局可信度，通过邻居节点间相互满意度的迭代，获取节点的全局可信度。此类系统获得的信任值较全面，但节点间的通信开销很大。

结合以上 4 类模型的优点，本文给出一种完全分布式 P2P 环境下的全局信誉模型，如图 1 所示。

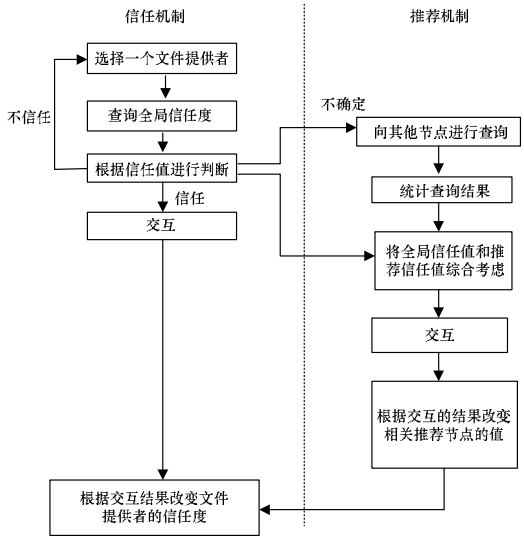

图 1 基于信任和推荐的 P2P 信誉模型

上述模型采用信任和推荐 2 种机制来确定节点的信任度，避免了单点失效问题，且有效遏制了 P2P 系统中虚假节

基金项目：江苏省自然科学基金资助项目(BK2004039)
作者简介：席 菁(1984－)，女，硕士研究生，主研方向：计算机网络，网络安全；王 源，硕士研究生；陆建德，教授
收稿日期：2008-07-10 **E-mail：**210513071@suda.edu.cn

点的欺骗行为。模型分成 2 个部分，即信任机制模型和推荐机制模型，本文介绍相关的重要技术并给出具体的信任度计算方法。

3 信任机制的实现

信任和推荐机制在现有 P2P 信誉机制中已被广泛使用，但对它们的定义目前还没有达成共识。本文采用如下定义：

(1)信任，基于自己的亲身经验确定节点的信任度。

(2)信誉，节点根据自己的一贯行为所享受的声誉。

(3)推荐，基于从其他用户获得的推荐信息确定节点的信任度。

3.1 全局信任值的影响参数

本文在信任机制中综合考虑信任与信誉，使两者复合成为全局信任值。它是节点在网络中表现的集中体现。是由与之发生过交易的其他节点对它的局部推荐以及这些节点的全局可信度决定的。因此，不能仅考虑其他节点对该节点在交易过程中的看法，还要考虑评价该节点的其他节点的可信度。假设节点 i 对节点 j 的评价信任度为 P_{ij}，经过 k 次交易后，节点的全局信任值为 T_{ik}，则任意节点的全局可信度为

$$T_{1(K+1)}=P_{12}T_{2K}+P_{13}T_{3K}+P_{14}T_{4K}+\cdots+P_{1n}T_{nK}$$

$$T_{2(K+1)}=P_{22}T_{2K}+P_{23}T_{3K}+P_{24}T_{4K}+\cdots+P_{2n}T_{nK}$$

…

其中，评价信任度由多方面因素共同决定，本文主要考虑以下因素[4]：

(1)从其他节点获得的反馈信息显示的满意度。信任机制通过交易节点的反馈信息计算节点信任度，节点在交易过程中得到的反馈信息可以很好地反映节点在系统中的被认知度。现有系统通常只考虑这一个因素，通过将反馈信任度简单相加来确定节点的信任值。例如在 eBay 中，将满意度分成 3 种，即(-1,0,+1)，交易失败为-1，交易成功为+1，介于中间的为 0。在此类系统中，只要简单增加交易次数就能提高节点信任度。在上述情况下，会产生交易 10 次都成功的节点，其信任度低于交易 20 次、失败 5 次的节点的现象。

(2)节点交易次数。考虑节点交易次数时，要综合考虑交易次数与交易结果。

(3)交易的内容差异。此因素在多数模型中都未被考虑到。一个节点可能因为交易了大量音乐文件而获得很高信任度，但这不能表示交易其他类型的文件时，该节点具有同样的可信度。同样，一个恶意节点可能通过大量小宗交易获取高额信任度，而在进行大宗交易时进行欺骗。

(4)节点对系统的贡献。节点在系统中作为文件提供者上传的文件越多，说明该节点对系统的贡献越大，与对系统贡献小的节点相比，应得到更多信任值来提升节点优先级。同样，提供反馈信息更多的节点可以获得更高信任值。

(5)节点的交易额在不同时段所占权值。P2P 网络中有一些恶意节点可能通过在早期交易中得到的较高信任值进行欺骗，如果可以合理安排节点的交易权值分配，将有效制止该行为。

本文给出式(1)，用于评价信任值。

$$p_{ij}=\alpha\times\frac{S(p,j)-F(p,j)}{C(p)}+\beta\times\frac{S_{(p,j)}-F(p,j)}{C_{(p)}}+\gamma\times CF(p)+\delta\times IF(p) \qquad (1)$$

其中，$S(p,j)$为节点 p 对节点 j 的满意交易次数；$F(p,j)$为节点 p 对节点 j 的不满意交易次数；$C(p)$为节点 p 总的交易次数；$S_1(p,j)$为节点 p 在近期对节点 j 的满意交易次数；$F_1(p,j)$为节点 p 在近期对节点 j 的不满意交易次数；$C_1(p)$为节点 p 在近期的总交易次数；$CF(p)$为节点一致性参数；$IF(p)$为节点贡献参数。式(1)分为 4 个部分，即 $\alpha, \beta, \gamma, \delta$，它们的值均在[0,1]内，且 $\alpha+\beta+\gamma+\delta=1$，分别表示影响信任值的各个因素在评价信任值的计算中所占比重。

3.2 全局信任度的存储和查询

本文采用完全分布式 P2P 结构，没有用于存储全局信任度的集中服务器。全局信任度分散存储在各个节点中，因此，采用什么样的组织结构进行节点全局信任值的存储成为难点之一。现在普遍采用的方式大多基于 CAN, Chord, Pastry 和二叉树等算法。

本文给出一种基于 P-Grid 中逐级匹配路由的查找算法，使用哈希函数构建满二叉树，以进行节点定位的组织结构。为了降低查找深度，将全局值分别存储在不同节点中，如图 2 所示。假设网络中共能容纳 2^{10} 个节点，每个存储全局值的信任节点中可以存储 2^5 个节点。树中的每个非叶子节点均有一个指向下一条路由的指针，而叶子节点中含有指向下一个节点的指针，进入网络中的节点先根据哈希函数进行分类以确定节点全局值的存储节点。在本文设计的系统中，节点标识符通过计算节点 IP 地址产生。

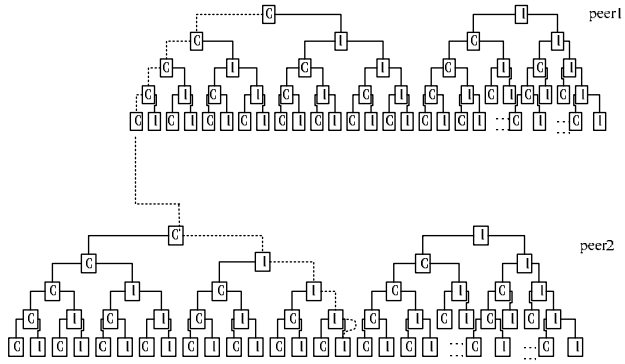

图 2 全局信任度查询树

3.2.1 全局信任度的存储

节点的全局信任值用基于树的结构来存储，在图 2 中可以看到，在网络初始化时期，网络中就建立网络中能容纳节点上限的满二叉树(例如：网络中一共能容纳 2^{30} 个节点，则需要建立一棵深度为 30 的满二叉树)，一个新节点加入网络，只需在它的相应节点处插入全局值即可。例如：对于一个 IP 地址为 198.10.10.1 的新加入节点，通过哈希函数可以得到它的关键字为 15(0000001111)，如图 2 中虚线所示，以此关键字逐级查找，在查找到的节点中加入此节点的初始全局值即可。

3.2.2 全局信任度的查询

在本文设计的全局信任值存储树中，所有全局信任值均存储在最底层节点的叶子节点中，可以方便地存储和查找全局值，但在网络容量很大的情况下，会使存储全局值的节点过多，网络负载加重。本文采用 P-Grid 中的路由查找算法，使节点中存在的子树个数大于 1，以减轻网络负载。

图 3 描述了路由查找过程，节点中维护多棵子树，不同子树的树根分别代表不同节点。要查找关键字为 00×××××的节点时，先查找节点 p1 的路由表，得知要到 p2 中查找，然后查找节点为 p1 的路由表，知道要到 p1 中查找，在 p1 中找到树根为 p2 的子树(表示此次查找从节点 p2 路由而来)，继续向下查找，直到关键字查找完毕。如果查询到此关键字没有全局值，则说明此节点在网络中不存在，是一个虚假节点。

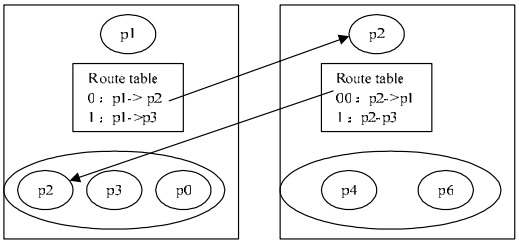

图 3　路由查找过程

3.3　信任阈值

根据 3.1 节获得全局信任度 T_u 后，需要确定节点是否可信，此时须解决阈值问题。本文给定 2 个阈值 t_1,t_2(t_1<t_2)，当 T_u>t_2 时，认为节点完全可信；当 t_1<T_u<t_2 时，认为节点不一定可信，要通过进一步查询来确定；当 T_u<t_1 时，认为节点不可信。

阈值的选定对整个系统而言具有重要意义，其值须根据不同应用要求和所处环境做相应改变。

4　推荐机制的实现

推荐机制只有在 t_1<T_u<t_2 的情况下才进行，节点 v 希望与节点 u 进行交易，当通过 T_u 不能完全确定节点是否可以信任时，节点 v 会向其邻居节点发出请求，用于查询节点 u 的信任值。形成对节点 u 的推荐信任度 R_u。

$$TR_u=\alpha\times T_u+\beta\times R_u \tag{2}$$

其中，TR_u 是通过信任和推荐双重机制得到的节点 u 的最终信任值；α, β 分别表示全局信任值和推荐信任值在 TR_u 中所占的比例，且 α, β 必须满足 $\alpha+\beta=1$。

4.1　推荐信任度 R_u 的计算

本文采用基于权重的方式计算推荐信任度，在推荐过程中遵循在传递过程中普遍采用的 2 种信任传递规则：信任衰减原则和信任聚合原则。

图 4 中的 a, b, c, d 为 P2P 网络中的节点。$T_{(a,b)}$表示 a 对 b 的信任度，$T_{(b,c)}$表示 b 对 c 的信任度。通过 b 作为推荐者得到的推荐信任度 $T_{b(a,c)}\leq\min(T_{(a,b)},T_{(b,c)})$(根据信任衰减原则)。同理，通过 d 作为推荐者得到的推荐信任度 $T_{d(a,c)}\leq\min(T_{(a,d)},T_{(d,c)})$。推荐度复合后，$a$ 对 c 的总推荐信任度 $T_{(a,c)}\geq\min(T_{b(a,c)},T_{d(a,c)})$(根据信任聚合原则)。

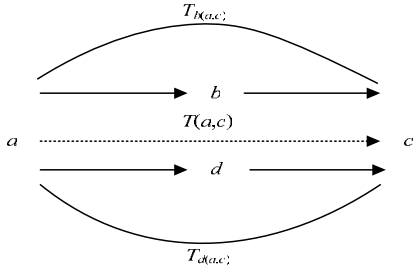

图 4　传递模型

本文采用的推荐信任值的合成方式满足上述原则，并引入了推荐信任强度的概念，用于定量表现推荐信任值的衰减。推荐信任强度为

$$S_{ac}=T_{ak}\times S_{kc} \tag{3}$$

其中，k 为 a, c 之间的推荐实体。

如果是直接信任，则 S_{kc} 等价于 T_{kc}。如图 4 所示，假设通过 b 作为推荐者得到的推荐信任强度为 S_{ac1}，通过 d 作为推荐者得到的推荐信任强度为 S_{ac2}。

$$R_u=\frac{S_{ac1}\times T_{b(a,c)}+S_{ac2}\times T_{d(a,c)}}{S_{ac1}+S_{ac2}} \tag{4}$$

4.2　阈值选定

与 3.3 节所述类似，得到 TR_u 后要选定一个阈值来判断节点最终是否可信。对于阈值 t_3 的选定应根据应用和环境不同而有所不同，但必须满足 t_1<t_3<t_2。TR_u 大于 t_3 说明节点可信，可以进行交易，反之说明节点不可信，需要寻找另一个满足要求的节点进行交易。

5　仿真实验及结果分析

为了验证模型的可靠性和可行性，本文用 JBuilder9.0 和 JXTA2.2 构建模拟实验平台，设置与实际应用相近的实验场景，并进行模拟实验。

实验 1　根据文献[5]提供的数据，比较第 4 节给出的计算推荐信任度方法和证据理论(D-S)[5]。设 T 为节点真实的信任值，T'为通过计算得到的信任值。实验结果如图 5 所示，其中，$\S=1-|T'-T|/T$。由图 5 可知，本文采用的推荐模型可以较成功地计算出推荐信任值。

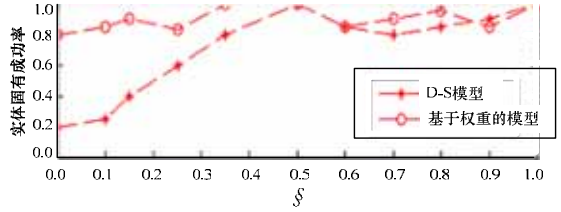

图 5　2 种模型的推荐信任度比较

实验 2　比较本文模型与文献[2]模型。设 P2P 环境中的节点总个数为 128，虚假、恶意节点在总节点中所占百分比为 25%。实验结果如图 6 所示，可以发现，当交易次数增加时，本文所用模型的交易成功率趋近于 1。

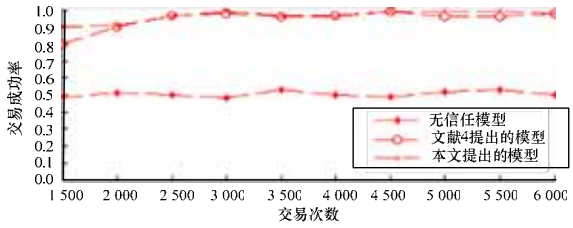

图 6　交易成功率比较

6　结束语

现有 P2P 系统使用的信誉模型通常只采用信任机制和推荐机制中的一种，且多数都建立在中心依赖的基础上，容易产生单点失效问题。本文方案可以较有效地避免上述问题，但仍然有待完善。

参考文献

[1] Cornelli F, Damiani E, Capitani S D. Choosing Reputable Servents in a P2P Network[C]Proc. of the 11th International World Wide Web Confererce. Honolulu, Hawaii, USA: [s. n.], 2002.

[2] Aberer K, Despotovic Z. Managing Trust in a Peer-2-Peer Information System[C]//Proc. of the 10th Int'1 Conference on Information and Knowledge Management. Atlanta, Georgia, USA: [s. n.], 2002.

[3] Josang A, Ismail R, Boyd C. A Survey of Trust and Reputation for Online Sercice Provision[Z]. (2005-06-01). http://security.dstc.edu.au/staff/ajosang.

[4] Li Xiong, Ling Liu. A Reputation-based Trust Model for Peer-to-Peer Ecommerce Communities[C]//Proc. of ACM Conference on Electronic Commerce. [S. l.]: ACM Press, 2003: 228-229.

[5] 杨　静, 夏素贞, 顾君忠. 基于 P-Grid 的数字媒体信息共享研究[J]. 计算机应用, 2004, 24(5): 10-13.