一种细粒度的基于灰色关联度的P2P信任模型①

陈 伟[1] 欧阳旦[2] 汤光明[1]

(1.解放军信息工程大学 电子技术学院 河南 郑州 450003; 2.空军电子技术研究所 北京 100095)

摘 要: 已有的 P2P 网络信任模型过于粗糙，对反馈评价进行综合的能力不足。针对这一问题，提出了一种细粒度的基于灰色关联度的 P2P 信任模型 GM_TRUST，根据节点的兴趣和专长将节点化分为不同的域，通过对具体服务各属性评价的综合得出直接信任。引入记忆因子来刻画信任随时间衰减的特性，并利用基于灰色相关度的方法来量化推荐信任的准确度。分析与实验均表明本模型与以往的信任模型相比，能够更准确地评估出节点的信任值，对动态恶意节点和不诚实反馈节点的攻击具有很好的抑制能力。

关键词: P2P; 域; 反馈; 灰色关联度; 信任模型

A Fine-Grained Trust Model for P2P Networks Based on Grey Relation

CHEN Wei[1], OU YANG Dan[2], TANG Guang-Ming[1]

(1. Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China;
2. Institute of Electronic Technology, Beijing 100095, China)

Abstract: The present peer-to-peer trust models are too coarse and lack ability of synthesizing the feedback. This paper presents a new fine-grained trust model for P2P networks based on grey relation. The peers are divided into different regions according to interest and speciality, and the direct trust is gained by colligating the evaluation for all attributes of one service. A memory factor is introduced to describe the characteristic that trust trail off along with time. The grey relation is used to measure the accurateness of feedback. Analysis and experiments show that compared with existing models, the proposed model evaluates peer's trust value more accurately and it has better capability to resist the attack by the dynamic malice peers and peer's dishonest feedback.

Keywords: peer-to-peer; region; feedback; grey relation; trust model

1 引言

随着 P2P 网络应用的深入和广泛，国内外越来越多的学者致力于 P2P 信任问题的研究。A Josang[1, 2]提出了基于主观逻辑的信任管理模型，引入了证据空间和观念空间的概念来描述和度量信任关系。但该模型没有明确区分直接信任和推荐信任，无法有效地消除恶意推荐带来的影响。Beth 信任管理模型[3, 4]引入了经验的概念来表达和度量信任关系，并给出了由推荐所引出的信任度推导和综合计算公式。但该信任管理模型简单地应用概率模型对主观信任进行建模，在对多个推荐信任值进行综合时，简单地采用了均值的方法，因而不能真实地反映信任关系的真实情况，无法很好地消除恶意推荐所带来的影响。

上述模型还存在一个问题，就是都没有体现出节点的个性。文献[5]中指出，节点在不同的应用领域、同一应用领域的不同侧面应该体现出不同的特性。例如同一节点在提供下载服务和提供协同计算时可能表现出不同的合作程度，在文件下载时，由于节点的响

① 收稿时间:2009-10-27;收到修改稿时间:2009-12-08

应时间、下载速度、文件质量等不同，节点也表现出不同的信任度。

针对上述问题，本文提出了一个细粒度的基于灰色关联的 P2P 信任模型——GM_TRUST，根据服务的类型将节点化分为不同的域，对服务的不同属性(如响应时间、下载速度等)进行细化，并利用灰色综合评价法来量化推荐信任的准确度，据此赋予各反馈相应的权值。分析与实验均表明本模型与以往的信任模型相比，能够更准确地评估出节点的信任值，对多类动态恶意节点和不诚实反馈节点的攻击具有很好的抑制能力。

2 GM_TRUST信任模型

2.1 相关描述

将信任的主体记为 S，客体记为 O，主体对客体的信任值由直接信任值和推荐信任值两部分组成，记为 R_{SO}。S 对 O 的直接信任值定义为 DT_{SO}，S 获取的对 O 的推荐信任值定义为 R_{SO}。

节点根据专长和兴趣的不同被化分到不同的域，每个域由多个节点组成，域设置域管理员，并为域管理员设置一个副本，用于备份管理员所保存的信息。节点 ID 记为 ID_i，$i=1,2\cdots$，兴趣向量定义为：$V_{(ID_i)}=(V_1,V_2,\cdots V_n)$，节点提供服务时的服务质量的属性集合记为 $A=\{a_1,a_2\cdots a_k\}$，主体在接受一次服务 V_n 后，对客体本次服务质量属性的评价定义为向量 $E(V_n)=(e_1,e_2,\cdots e_k)$，$-1\le e_k\le 1$。节点在本地设置一张信任表，用于保存与该节点有过直接交易的节点的信任信息。表的结构如表 1 所示。

表 1　信任关系表

节点 ID	兴趣向量	服务质量属性	直接信任	交易总次数	成功交易次数	最近信任更新时间
ID_1	$V_{(ID_1)}$	$(e_1,e_2,\cdots e_k)_1$	DT_1	n_1	ns_1	T_1
ID_2	$V_{(ID_2)}$	$(e_1,e_2,\cdots e_k)_1$	DT_2	n_2	ns_2	T_2
…	…	…	…	…	…	…

同时，域管理员为各成员也保存一张表，记录节点的平均直接信任值：$\overline{DT_j}=\sum_{i=1}^{n_j}DT_{ij}$ (表示所有与 j 有过交互的节点对 j 直接信任的平均值)、该节点交易过的节点 ID 集合、以及各成员的信任信息。

2.2 直接信任

直接信任是指主体 S 通过与客体 O 的直接交互历史经验得出的对客体的评价，将其定义为

$$DT_{SO}^{(n)}=(1-\eta)DT_{SO}^{(n-1)}+\eta E(V_n)*w^T$$

其中 w 为 $E(V_n)$ 中各服务质量属性评价所占权重的向量，

$$\eta=\begin{cases}\alpha, E(V_n)*w^T<0\\ \beta, E(V_n)*w^T>0\end{cases},(0<\beta<\alpha)$$

为记忆因子，此取值可以保证模型在计算信任值时，成功交易使信任值增加缓慢，而失败交易使信任值降低相对较快，可以有效地惩罚节点的恶意行为，激励节点持续地进行良好的交互。同时，动态的恶意节点企图通过提供几次好的服务，积累到一定信任值后再进行恶意行为的节点，为此也会付出沉重的代价。记忆因子必须选取一个适当的值，过大可能导致历史信任值衰减过快，过小可能导致初始加入的节点很难积累起交互所需的信任值，为此应当根据具体应用为最近加入的节点赋予合理的初始值。

2.3 推荐信任

推荐信任的思想来源于人际网络，当一个个体 A 想要了解另一个不太了解或者完全陌生的个体 B 时，A 通常会向自己熟悉的人群 C 咨询关于 B 的情况，然后综合 C 反馈回来的信息，得出对 B 的综合判断，这个结果一般与 B 的实际比较吻合。

有感于人类社会网络，我们采用如下模式得出 P2P 网络的推荐信任：

(1) 节点 S 要与节点 O 交易，查询与 O 的交易历史，得出对 O 的直接信任值；

(2) 如果 S 没有与 O 发生过交易，或者对 O 的直接信任值小于某一阈值，则 S 向自己熟悉的节点(推荐节点)发出关于 O 的推荐信任查询请求；

(3) 推荐节点集根据自己的本地信任表，向 S 发送查询结果；

(4) S 根据返回的信息，向域管理员查询与自己和推荐节点都有过交互的一组公共节点，以及对这组公共节点的直接信任值；

(5) 域管理员向 S 发送查询结果;

(6) S 根据返回的查询信息,基于灰色关联分析[6]的方法，为各推荐节点的推荐信任赋予相应的权值，并综合出对 O 的推荐信任值。

设 $\{R_1,R_2,R_3\cdots R_k\}$ 为提供推荐服务的节点集合，$\{C_1,C_2,C_3\cdots C_n\}$ 为与节点 S 和 $\{R_1,R_2,R_3\cdots R_k\}$ 都有过交易历史的公共节点集合，则信任关系如图 1 所示，

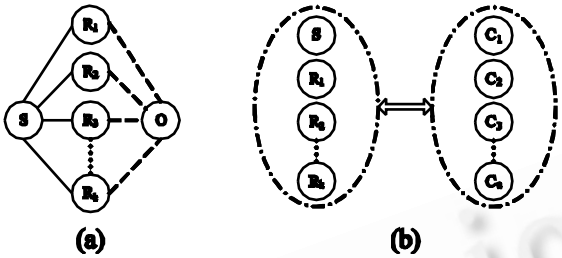

图 1　信任关系图

$RT_{so}=\sum_{i=1}^{k}DT_{io}*W_i$ 表示推荐信任，W_i 为所有 k 个推荐节点提供的推荐信任值中，节点 R_i 的推荐权值。假定主体倾向于相信与自身评价相似的节点，即对同一节点的评价越接近主体的节点，其提供的推荐值在整个评价中所占的权值越高，节点与主体的相似度用灰色关来衡量。

S 对 $\{C_1,C_2,C_3\cdots C_n\}$ 中各节点的直接信任组成的向量记为 $\left(DT_{SC_1},DT_{SC_2},DT_{SC_3},\cdots DT_{SC_n}\right)$，S 及 $\{R_1,R_2,R_3\cdots R_k\}$ 中各节点对 $\{C_1,C_2,C_3\cdots C_n\}$ 中各节点的直接信任组成的矩阵记为

$$\begin{bmatrix} DT_{SC_1} & DT_{SC_2} & \cdots & DT_{SC_n} \\ DT_{R_1C_1} & DT_{R_1C_2} & \cdots & DT_{R_1C_n} \\ DT_{R_2C_1} & DT_{R_2C_2} & \cdots & DT_{R_2C_n} \\ \cdots & \cdots & \cdots & \cdots \\ DT_{R_kC_n} & DT_{R_kC_2} & \cdots & DT_{R_kC_n} \end{bmatrix}$$

由灰色关联分析法知，由于 S 是评价的主体，节点肯定是最相信自己，我们以 $\left(DT_{SC_1},DT_{SC_2},DT_{SC_3},\cdots DT_{SC_n}\right)$ 为最优指标集，将矩阵

$$\begin{bmatrix} DT_{SC_1} & DT_{SC_2} & \cdots & DT_{SC_n} \\ DT_{R_1C_1} & DT_{R_1C_2} & \cdots & DT_{R_1C_n} \\ DT_{R_2C_1} & DT_{R_2C_2} & \cdots & DT_{R_2C_n} \\ \cdots & \cdots & \cdots & \cdots \\ DT_{R_kC_n} & DT_{R_kC_2} & \cdots & DT_{R_kC_n} \end{bmatrix}$$

进行均值化处理后，得到矩阵 $E=\left[v_{ij}\right]$，其中 $v_{ij}=\frac{DT_{R_iC_j}}{DT_{SC_j}},i=1,2,\cdots k,j=1,2,\cdots n$，则

$$L_{ij}=\frac{\min\limits_i\min\limits_j\left|v_{0j}-v_{ij}\right|+\rho\max\limits_i\max\limits_j\left|v_{0j}-v_{ij}\right|}{\left|v_{0j}-v_{ij}\right|+\rho\max\limits_i\max\limits_j\left|v_{0j}-v_{ij}\right|},\quad i=1,2,\cdots k;j=1,2,\cdots n$$

其中，ρ 为分辨系数，通常取 0.5。L_{ij} 表示 $DT_{R_iC_j}$ 与 DT_{SC_j} 的灰色关联系数。设评价指标的权值相同，则 $r_i=\frac{1}{n}\sum_{j=1}^{n}L_{ij}$，则令 $W_i=\frac{r_i}{\sum_{i=1}^{k}r_i}$。主体 S 综合所有推荐节点得到的对客体 O 的推荐信任值为：$RT_{so}=\sum_{i=1}^{k}DT_{io}*W_i$。

2.4 综合信任值的计算及更新

综合信任值由直接信任和推荐信任两部分组成：

$$R_{SO}=\sigma DT_{SO}+(1-\sigma)RT_{SO},\quad \sigma=\frac{\lambda k}{1+k};$$

k 为最近一个时间段内成功交易的次数。例如当时，在某一时间段内当主体与客体成功交易 1000 次后，σ 的值变为 1，主体将会完全依赖自己的直接信任对客体进行评价，而不必依赖推荐信任。

信任值的更新有两种驱动机制：基于时间驱动的信任更新机制和基于事件驱动的信任更新机制。本文中假设信任更新不是很频繁，因此采用基于事件驱动的信任更新机制。当然也可以采用基于时间驱动以及基于时间_事件混合驱动的信任更新方式，在此不作过多讨论。

本模型中，为了保证信任数据的安全和计算的效率，每个节点对其他节点的信任值进行本地存储，同时域管理员也存储了各成员节点的信息。进行信任计算时，节点只需在本地信任信息表和域管理员中进行相关信息查询便可得出所需的信任值。每次交易完毕后，节点更新本地信任信息，同时将更新信任发往所在的域管理员及其副本。

2.5 开销评估

本模型中，若域规模为 n，网络规模为 N，普通节点只需存储直接交易节点的信任信息，而域管理员需再存储一个域中成员信息表，所需的存储规模都比较小。通信开销主要来自于 S 的推荐信任查询，其复杂度为，而在 eigenRep[7]模型中,任意节点的任意一次交易都会引起迭代，迭代通过其交易伙伴在全网络范围扩散,直到所有节点的全局可信度在连续两次迭代的结果小于某个系统指定的极小常量,其消息复杂

度为。实际上分域以后，域的规模 n 远小于实际的网络规模 N。因此，本模型可以在有限的开销范围内得出信任值，即便在网络规模增大 N 的时候，实际域的规模 n 也不会过快增长，不必担心开销过大的问题。

3　仿真实验及结果分析

本文采用 MATLAB7.0 对提出的模型进行了仿真实验，主要比较本模型与传统的粗粒度的信任模型的性能,以及本模型与 JOSONG 的信任模型在抑制恶意节点方面的性能，评价的指标均为交互成功率，即交互成功次数占总交互次数的比率。

仿真 1：

在恶意节点仅占 5%情况下，比较了本模型与传统的信任模型的性能。假设恶意节点总是提供不诚实的服务，而诚实的节点总是提供诚实的服务。假设共有 1000 个实体进行交互，在本模型中根据节点的兴趣不同将节点分为五个不同的域，进行 2000 次交易。而在传统的模型中这 1000 个节点不分域，直接进行 2000 次交易。各参数设置为：$\alpha=0.2,\beta=0.1$，$\rho=0.5$，$\lambda=1.0001$，直接信任初始值为 $DT_{SO}^{(0)}=0.5$，对交互次数进行抽样后，交互成功率与交互次数之间的关系如图 2 所示。

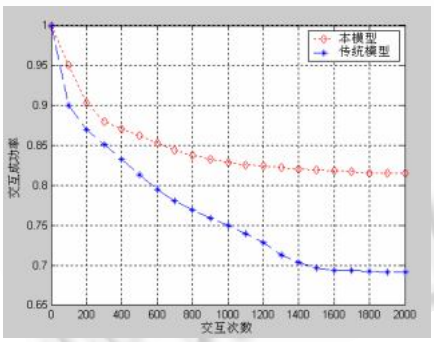

图 2 本模型于传统模型交互成功率比较

通过实验可以看出随着交互次数的增多，使用本模型与传统信任模型，交互成功率都将趋于稳定，但传统模型的交互成功率远远低于本模型。这是由于传统信任模型没有考虑节点的具体交易内容，而只是粗糙地给出节点信任值，这个信任值并不能表达节点的兴趣和专长。例如，两个正常节点 A、B，A 要进行资源下载，B 的特长是进行协同计算而不提供资源下载，但通过提供良好协同计算服务积累了较高的信任值，而 A 根据这个信任值误选择与 B 进行交互，却得不到自己想要的服务，会在信任评估时给 B 一个很低的信任值。此时，虽然没有恶意节点或者恶意节点数目很少，网络中的交互成功率依然很低。

而本模型是针对节点的具体交易内容给出的信任值，并且对节点服务质量属性进行了综合评价，因此得出的信任值相对要准确很多，并且能够很快使网络趋于稳定。

仿真 2：

在恶意节点不断增加的情况下，比较了本模型与 Josang 信任模型、Beth 信任管理模型的交互成功率。假设恶意节点总是提供不诚实的服务，而诚实的节点总是提供诚实的服务。恶意节点中协同作弊的概率为 1/2,诋毁、夸大和重入的概率均为 1/6。假设有 1000 个实体进行交互，每个节点交互次数为 5000 次。实验中，本模型的相关参数与实验一一致。随着恶意节点的增多，交互成功率的变化趋势如图 3 所示。

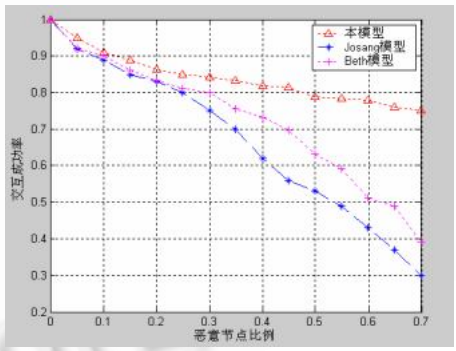

图 3 本模型于 Josang 模型和 Beth 模型交互成功率变化趋势比较

可以看出，由于 Josang 信任模型和 Beth 信任管理模型缺乏对恶意节点的抑制，随着恶意节点比例的增加，交互成功率将很快下降。而本模型使用了灰色相关度来评价推荐节点的推荐准确度，并且以自己的评价为最优指标，在综合推荐信任时对诋毁、夸大、重入、协同作弊等恶意行为具有严格的筛选和识别机制，产生了极强的抑制作用，因此在恶意节点大量存在的情况下，仍能保证较高的交互成功率。

4　结语

本文在分析 P2P 网络特性的基础上，提出了一个细粒度的基于灰色关联 P2P 信任模型，根据服务类型

的不同将节点化分为不同的域，在进行信任评价时，对具体服务的各服务质量属性进行加权评价，并且引入记忆因子来刻画信任随时间衰减的特性，得出的信任值更为准确可靠，更具动态适应能力。在计算推荐信任时，利用灰色相关度来度量推荐节点的推荐准确度，可以很好地抑制不诚实节点的诋毁、夸大、协同作弊等恶意行为，当网络中恶意节点比例较高时，仍能够保证较高的成功交互率。本模型所需样本量少，数据结构简单，可操作性强，将其与具体的 P2P 网络应用相结合将是下一步的研究方向。

参考文献

1 Josang A, Knap skog SJ. A Metric for Trusted Systems, Global IT Security. Wien: Austrian Computer Society, 1998. 541－549.

2 Josang A. Trust-based Decision Making for Electronic Transactions. Proc. of the 4th Nordic Workshop on Secure Computer System (NORDSEC'99). http://security.dstc.edu.au/staff/ajosang/paper.html.

3 Beth T, Boreherding M, Klein B. Valuation of trust in open networks. Gollmann D. Proc. of the European Symposium on Research in Security (ESOR ICS). Brighton: Springer-Verlag, 1994. 3－18.

4 Abdul-Rahman A, Hailes S. A Distributed TrustModel. Proc. of the 1997 New Security Paradigms Workshop. Cumbria: ACM Press, 1998. 48－60.

5 任艳,任平安,吴振强,马建峰.移动 P2P 网络中的多粒度信任模型.计算机工程与应用, 2009,45(6):130－140.

6 邓聚龙.灰色系统理论教程.武汉:华中理工大学出版社, 1990. 128－134.

7 Kamvar S, Schlosser M. The EigenTrust Algorithm for Reputation Management in P2P Networks. WWW, Budapest, Hungary, 2003.