P2P 环境中基于粒子群算法的信任模型

陈 军[1,2],高 雅[2],刘莉平[2]
CHEN Jun[1,2],GAO Ya[2],LIU Li-ping[2]

1.惠州学院 计算机科学系,广东 惠州 516015
2.中南大学 信息科学与工程学院,长沙 410083
1.School of Computer Science,Huizhou Academy,Huizhou,Guangdong 516015,China
2.School of Information Science and Engineering,Central South University,Changsha 410083,China
E-mail:gaoyacrystal@gmail.com

CHEN Jun,GAO Ya,LIU Li-ping.Trust model based on PSO in P2P.Computer Engineering and Applications,2009,45(32):75-79.

Abstract: There are many malicious nodes spreading false information in P2P networks,because of its open and anonymous characteristics.So it is of great importance to build a sound mechanism of trust in the P2P environment.To avoid the shortage of the existing trust model,the paper provides a Trust Model based on PSO.In the model,after initializing the particle swarm,each particle can update the speed and location according to its information,then produce a new particle with better value.Doing that process continually and implementing the global search of the space,finally,they can get a better overall value,that is the better trust path in the networks.The simulation results show that it can get the overall optimum solution in a relatively short time after many times of iteration,and the more times it iterates,the better the trust path is.It can be proved that the algorithm can prevent the fraud.
Key words: trust model;Particle Swarm Optimization algorithm;BBK trust model;preventing the fraud

摘 要:P2P 系统的开放和匿名等特征,使其成为一些恶意节点发布虚假信息的温床,因此在 P2P 环境中构建一个完善的信任机制显得尤为重要。针对现有信任模型对于寻找信任路径速度慢且难以防止联合欺诈等缺点,提出了一种适合 P2P 环境的基于粒子群算法的信任模型。在 BBK 信任模型的基础上引入粒子群算法,将信任路径转化为每个粒子,通过对粒子速度和位置的更新来寻找信任度高的路径,最终再根据 BBK 模型得出全局信任度。通过数学分析和证明,该模型具有较好的防止联合欺诈的性质。实验表明,算法效率较高,较其他算法具有明显优势。
关键词:信任模型;粒子群算法;BBK 信任模型;防止联合欺诈
DOI:10.3778/j.issn.1002-8331.2009.32.024 **文章编号**:1002-8331(2009)32-0075-05 **文献标识码**:A **中图分类号**:TP391

1 信任模型研究现状

自 Peer-to-Peer 网络出现后,它受到越来越多的关注。P2P 将现在主流的 Internet 服务棋式——客户/服务, 回归到 end-to-end 的原则当中[1]。P2P 并不严格地区分服务提供者和消费者,参与的实体(peer)之间都是平等的,每一个实体既可提供服务也可使用服务,P2P 计算体系结构目前已广泛应用于对等协作、资源共享、知识管理等领域。现在,基于 P2P 的商务、政务以及科学协作计算等活动逐渐成为一种主流应用模式。但在 P2P 网络中存在一些恶意行为,如提供假信息、散播广告、传播病毒和蠕虫等。为解决这一类问题,引入信任机制,在分布式计算环境中为交互双方建立信任关系。在传统的网络环境(如 Internet)和应用(如电子商务)中,信任关系的建立依赖于可信的第三方,比如认证中心(CA)。只要个体持有该 CA 所颁发的证书即被认为是可信的,同时,恶意用户必须承担(法律)责任。然而,在目前广泛存在的 Peer-to-Peer 环境中(如文件共享应用),有一种排斥 CA 的倾向,这主要基于以下几点考虑:(1)集中式的认证往往伴随着额外的费用和开销,而 P2P 环境通常追求零开销[2],用户自愿参与网络自由交易并且不准备为自己的行为负(法律)责任;(2)对单点失效的顾虑,这里指的单点失效有两方面的含义:①物理上的,即可信(认证)服务器的崩溃导致整个 P2P 系统的崩溃;②社会或法律意义上的单点失效,即由于政治法律等原因导致可信(认证)服务器无法正常工作从而致使 P2P 系统崩溃(Napster 的崩溃即是一个此类例子)。因此,对于目前日益广泛的诸多 Peer-to-Peer 环境,建立一种新

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.2005CB321800);国家自然科学基金(the National Natural Science Foundation of China under Grant No.60573127);湖南省自然科学基金(the Natural Science Foundation of Hunan Province of China under Grant No.06JJ30032)。
作者简介:陈军(1962-),男,副教授,主要研究领域为 P2P,计算机网络;高雅(1985-),女,硕士研究生,主要研究领域为可信计算,分布式网络,无线 Mesh 网络;刘莉平(1970-),女,博士,讲师,主要研究领域为可信计算,分布式网络。
收稿日期:2009-06-10 **修回日期**:2009-08-03

的分布式信任机制是十分必要的。这种必要性不仅体现在用户对 P2P 网络的有效使用上,也体现在有利于网络的良性发展上。

在社会网络中,信任关系是人际关系的核心,个体间的信任度往往取决于其他个体的推荐。同时,作为推荐者的可信度也决定其推荐个体的可信度。实际上,这种互相依赖的信任关系组成了一个所谓的信任网络[3](Web of trust)。在这样的信任网络中,任何个体的可信度都不是绝对可靠的,但可以作为其他个体决定其交互行为的依据。基于信任网络的 Peer-to-Peer 系统与人际网络有很大的相似性[4],这表现在:(1)网络中的个体在与其他个体的交互中会留下零星的"信用"信息;(2)个体对于交互对象具有充分的选择权;(3)个体往往不看重绝对的可靠性或服务质量,即个体可以忍受少量错误的选择带来的损失,比如文件共享应用;(4)个体有义务为网络中的其他个体提供推荐信息。因此,这为借鉴社会学研究的某些结论提供了可能。

目前,围绕信任模型展开了一系列研究。文献[5]提出了基于 PKI 的信任模型,在这个系统中,存在若干领袖节点,领袖节点主要负责整个网络的监督工作,并定期报告违规的节点,这些领袖节点的合法性通过 CA 颁发的证书加以保证,这类系统往往是有中心依赖性的,其在扩展性和单点失效性上都存在问题,如 eDonkey 在网络中分布的许多服务器[6]。另一种信任模型是基于局部推荐的信任模型,如 Cornelli 和 Gnutella[7]提出的改进建议。但该模型存在的最大问题是反馈信息的积累比较慢,必须要两个节点间反复进行交易才能获取足够的信息以保证先验概率计算的准确性。在稍大规模的 P2P 网络中,则很难获得对网络中所有节点的完整的信任信息。文献[8]提出了全局可信度模型。为获取全局的节点可信度,该类模型通过邻居节点间相互满意度的迭代,从而获得节点全局的可信度。文献[9]在基于 EigenRep 的模型基础上提出了基于推荐的全局信任度算法模型,并在 P2P 网络的评价机制中引入了 SHA 密码算法,有效地解决了不共享、冒名、诋毁等恶意行为,但如果惩罚机制不完整,反而加重诋毁行为的危害,虽然运用了一些反诋毁的补救措施,但是没有根本地改变其性能。

上述信任模型都需要通过一定的算法得到多条信任路径,并根据所得到的多条信任路径进行综合计算得到一个综合信任值。目前研究中得到的寻找信任路径算法都或多或少存在一些缺陷,例如,Yahalom 等在文献[10]中提到的算法被证明是 NP 完全问题,他们在文献[11]中的算法把网络模型描述为树的结构,算法复杂度是对数阶的。Reiter-Stubblebine 提出了 PGP 中信任机制的 BDP 近似算法,得出了较多的不相交路径,但没考虑如何使各条路径的信任度进行优化,不能防止联合欺骗的行为。白保存等改进了 Reiter-Stubblebine 的算法,其中利用了 Dijstra 算法,但在复杂的网络环境中运行效率较低。文献[12]提出了基于蚁群算法的信任路径寻找算法,但该算法不能有效地避免联合欺诈行为的发生。

鉴于此,将粒子群算法引入到信任模型当中,提出了基于粒子群算法的信任模型(PSO Trust Model,PSOT)。利用粒子群算法得到了多条较优信任路径,进而根据公式综合计算系统的信任度。较以往算法效率高,更适于连续空间的搜索问题,并且可以有效防止联合欺诈行为。

2 信任度机制

Abdul-Rahman 认为在分布式的体系中信任是非理性的,是一种经验的体现,不仅要有具体的分类内容,而且还应该有信任程度的划分,并提出了一些基于此观点的信任度评估模型,信任度评估模型主要涉及以下几个问题:信任的表述和度量,由经验信息推荐所引起的信任度推导,以及信任度的合并运算。不同的信任度评估模型在上述问题的处理上存在差异。Beth 等人在此基础上率先进行了基于信任的逻辑推理,又对其量化了一种估算信任度的方案,并得出了在多个认证服务中心信任关系的传递以及推理规则,也称为 BBK 方案[13]。在 BBK 信任评估模型中,赋予信任度一个实数值 V,$V\in[0,1]$,0 代表完全不信任,1 代表完全信任,实体可以通过设置信任阈值来确定目标信任与否。在现在的信任关系中,信任主要由经验信息推荐所得,因此,文中主要考虑推荐信任。推荐信任 R(Recommend Trust),表示为 $P\mapsto Q$,D,$R\in[0,1]$,R 代表 P 对 Q 的推荐其他实体能力的信任程度。

在信任评估模型中,信任往往要通过推荐来获得,而对于同一个信任关系,往往有很多的推荐者,必须综合他们的推荐信息以得到对目标的信任度,从而最终判断目标可信与否。Beth 给出了信任的推理规则(定理 1),以及信任度的计算规则,如公式(1)所示。

定理 1 $R\times R\mapsto R$

信任度计算规则:

$$V_1\cdot V_2=V_1V_2 \tag{1}$$

Beth 评估模型还给出了推荐信任度以及直接信任度的综合计算公式。

推荐信任度:

$$V_{COM}=\frac{1}{n}\sum_{i=1}^{n}V_i \tag{2}$$

设共有 n 条平行的推荐路径,其推荐信任度分别为(V_1,V_2,$\cdots$,V_n),则综合推荐信任度 V_{COM} 为各条推荐路径推荐信任度 V_i 的算术平均值。

采用信任度的机制后,实体间建立信任往往通过中间实体的信任推荐的关系建立信任,并依此计算出信任度,为用户对目标实体可信与否提供判断依据。如上所言,在信任建立过程中建立单条验证路径 $s\mapsto c_1\mapsto c_2\mapsto\cdots\mapsto t$,假设 tr 为信任度,则 $tr_s^t=\prod_{s\mapsto t}tr$。总的信任度为每段路径信任度的乘积。这条路径是很脆弱的,路径中任何一个节点出现问题,将直接影响对目标判断的结果。为了降低风险,可以有两种途径:一是限定路径的长度或跳数;二是采用多条路径来综合判断目标。文中选择了通过限定路径中的跳数来降低风险。

3 基本粒子群优化算法

粒子群算法首先由 Kennedy 和 Eberhart 于 1995 年提出[14],是一种基于迭代的进化计算方法。在粒子群优化的过程中,鸟群中的每只鸟根据对环境的适应度飞行到较好的区域,将每只鸟看作 D 维搜索空间中的一个没有体积的微粒,在搜索空间中以一定的速度飞行。这个速度根据它本身的飞行经验以及同伴的飞行经验进行动态调整。

基本 PSO 公式如公式(3)~(6)所示。设搜索空间是 D 维的,粒子群中第 i 个粒子的位置用 $x_i=(x_{i1},x_{i2},\cdots,x_{id})$ 表示,第 i 个粒子的速度表示为 $v_i=(v_{i1},v_{i2},\cdots,v_{id})$。第 i 个粒子搜索的最好位置记为 $p_i=(p_{i1},p_{i2},\cdots,p_{id})$,整个粒子搜索到的最好位置记

为 $p_g=(p_{g1},p_{g2},\cdots,p_{gl})$。对于每一个粒子,其第 d 维($1\leqslant d\leqslant D$)根据如下等式变化:

$$\begin{cases} v_{id}(t+1)=w\times v_{id}(t)+c_1.r_1\times(p_{id}(t)-x_{id}(t))+c_2.r_2\times(p_{gd}(t)-x_{id}(t)) & (3)\\ v_{id}=v_{\max},\text{if } v_{id}>v_{\max} & (4)\\ v_{id}=-v_{\max},\text{if } v_{id}<-v_{\max} & (5)\\ x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) & (6)\end{cases}$$

其中:r_1、r_2 是介于[0,1]之间的随机数;c_1、c_2 是加速度系数,一般取 $c_1=c_2=2$;w 是惯量因子;$v_{\max}$ 是常数,限制了速度的最大值,由用户设定。粒子在解空间内不断更新个体极值与全局极值进行搜索,直到达到规定的迭代次数或满足规定的误差标准为止。粒子在每一个位置飞行的速度不能超过算法设定的最大速度。

4　基于粒子群算法的信任模型

4.1　算法的基本思想

第 2 章介绍了由 Beth 等人提出的信任度机制。该机制通过将多条路径的推荐信任度综合求平均得出全局的信任度,这样得出的全局信任度具有较好的稳定性并可以防止联合欺诈。因此,也采用 Beth 等人提出的信任度机制,并在此基础上,将粒子群算法引入到信任模型当中,提出了基于粒子群算法的信任模型(PSOT)。利用粒子群算法得到了多条较优信任路径,进而根据公式综合计算系统的信任度。

基于粒子群的思想寻找信任路径,从多目标优化的角度出发,搜索所有节点从源节点 s 到目标节点 t 之间满足条件的一组多目标 Pareto 非劣解。基本思想是:首先产生一定数目的粒子,每一种路径方案编码为一个粒子,每一个粒子利用本身信息、局部较优信息和全局较优信息三个信息,产生具有更高目标准则值的新粒子。这一过程不断进行迭代,实现在解空间的并行全局搜索;算法停止时,得到一组粒子集合,对应了多条收敛于 Pareto 优化或近似优化路径的组合集。经过多次的迭代,并利用第 2 章中提出的信任度机制,对多次迭代求平均便可计算出整个系统的信任度。

把信任关系网络拓扑图抽象为图 $G=((V,E),s,t,M)$,如图 1 所示。V 为节点集,每个节点代表一个实体,E 为矢量边集,代表信任关系。每个矢量值的范围是[0,1],tr_k^j 代表节点 j 对节点 k 的推荐信任值。$s\in V,t\in V$,s 代表源节点,t 代表目标节点,M 代表信任路径的最大跳数,信任路径 $s\rightarrow c_1\rightarrow c_2\rightarrow\cdots\rightarrow t$ 途经的节点数为 m,$m\leqslant M$。一条信任路径上的推荐信任值为:

$$P_l=\prod_{ij\in E_l} tr_k^j \qquad (7)$$

这里 E_l 为路径 P_l 上的矢量集。

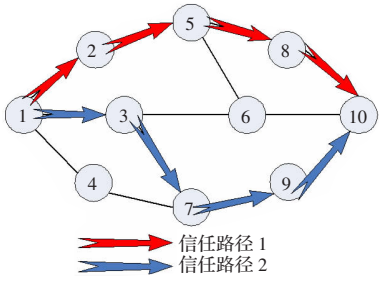

图 1　网络节点拓扑示意图

第 i 个粒子的位置 x_i 表示的是一条从 s 到 t 的路径方案,那么第 i 个粒子的适应值可表示为:

$$f(x_i)=\prod_{jk\in x_i} tr_k^j \qquad (8)$$

对于信任路径,应使 $f(x_i)$ 越大越好,即粒子的最好位置 p_g 应在最大的 $f(x_i)$ 处取得。由 BBK 信任评估模型[10]可知,多条信任路径 $P_1,P_2,\cdots,P_l$ 综合计算后得到的最终推荐信任值为:

$$Trust_{s\rightarrow t}=\frac{1}{l}\sum_{i=1}^{l}P_l \qquad (9)$$

基于粒子群算法的信任模型的算法流程如图 2 所示。其中,产生粒子的过程重复进行,直到算法停止为止,此时经过多次更新的 p_g 即为粒子的最好位置。最后根据公式(9)输出结果。

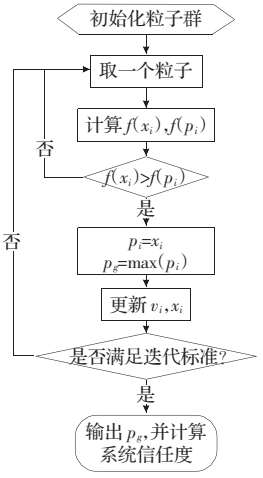

图 2　算法流程示意图

4.2　算法的设计

4.2.1　算法描述

根据第 3 章描述的粒子群算法以及 4.1 节信任路径的寻找算法,将基于粒子群思想的信任路径寻找算法描述如下:

(1) Initialize particle_swarm PS　//初始化粒子群
(2) DO
(3) for i=1 to particle_swarm_Size
(4) {
(5) calculate the fitness value $f(x_i)$ of the ith particle according to formula (8)
(6)　if $f(x_i)>f(p_i)$then $p_i=x_i$　//更新 p_i
(7)　$p_g=\max(p_i)$　//更新 p_g
(8)　for d=1 to DimensionSize
(9)　{
(10)　update v_{id},x_{id} according to formula (3) to (6);
(11)　}
(12)}
(13)While termination criterion is met.
(14)return p_g;
(15)calculate $Trust_{s\rightarrow t}$ according to formula (9).

4.2.2　初始化粒子群

首先对图 G 中的所有节点进行编号,图 G 中节点 V 的个数即为粒子群中粒子的维数 d。因为,拓扑图 G 中的信任节点数不变,采用整数定长编码的方式,将信任路径映射为粒子空间中的个体。粒子个体中第一维和最后一维位置总是图中的顶点 s、t,取值分别为 1 和 d,粒子位置的每一维的值是图 G 中相应位置对应的节点的编号,如果对应位置的节点不在信任路径中,则取 0。

假设粒子 $x_i=(x_{i1},x_{i2},\cdots,x_{id})$ 表示信任路径的一个解，其中 d 为图 G 中顶点的个数，并且从左到右编号。x_{i1} 和 x_{id} 的取值分别为 1 和 d，其他 $x_{ij}(j=2,3,\cdots,d-1)$ 的取值为 0 或者节点的编号(2~d-1)。例如，对于图 G 中某粒子编码如下所示：$x_i=(1,0,3,0,0,0,7,0,9,10)$，表示一条经过第 1,3,7,9,10 号节点的信任路径，如图 1 的信任路径 2 所示。算法为了降低风险，设定了信任路径中包含节点数的最大值 M，因此 $x_i=(x_{i1},x_{i2},\cdots,x_{id})$ 的各个维度的值中非零值的最大个数为 M。这在初始化粒子群时需要进行约束。

该文利用随机方法产生一组满足约束条件的从 s 到 t 的初始组合路径集。设初始粒子群规模为 N，$Constr(PS)$ 表示从集合 PS 中选取满足约束的组合路径；$RandS(S,T)$ 表示利用随机方法选择 s 到 t 的一条路径。具体过程如下：

Begin

(1)$PS\leftarrow\phi$

(2)while(|PS|<N)

(3)$PS\leftarrow PS\cup$Constr($RandS(S,T)$)

(4)Goto(2)

(5)Output PS

End

4.2.3　粒子群的运算

在该模型中，每个粒子代表一条路径。因此，对于每条路径，都会有一个 $f(x)$，如前所述，用 $f(x)$ 表示每条路径的信任度，并根据 4.2.1 节算法描述的第(6)、(7)行，对 p_i 和 p_g 进行更新。对于每个粒子，其每一维都有其 v_{id}、x_{id}，因此，在初始化粒子群时，便对其进行带约束的随机初始，更新过程依据公式(10)、(11)。

$$v_{id}(t+1)=w\times v_{id}(t)+c_1.r_1\times(p_{id}(t)-x_{id}(t))+c_2.r_2\times(p_{gd}(t)-x_{id}(t)) \quad (10)$$

$$x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) \quad (11)$$

4.3　算法防联合欺诈性证明

在网络中，往往存在着大量的欺诈行为[15]。欺诈无非是颠倒黑白，把“好的”节点说成“坏的”，把“坏的”节点说成“好的”，由于该算法使用了粒子群优化算法，在寻找过程中是逐步寻找较优路径。在算法运行过程中，寻找非劣解，淘汰劣解，这样就可以有效防止联合欺诈行为[16]。

首先，针对一条路径来说，例如，对于路径：

$s\rightarrow c_1\rightarrow c_2\rightarrow c_3\rightarrow c_4\rightarrow t$

$tr_{c_1}^{s}=0.85$，$tr_{c_2}^{c_1}=0.87$，$tr_{c_3}^{c_2}=0.15$，$tr_{c_4}^{c_3}=0.26$，$tr_{t}^{c_4}=0.92$

假设其中只有 c_3 为有欺诈行为的节点，c_3 对 c_4 的推荐信任值很低，那么这条路径的推荐信任值 $P_l=0.026\,5$，这条路径很可能被淘汰。假设 c_3、c_4 进行联合欺诈，令 $tr_{c_4}^{c_3}=0.91$，那么 $P_l=0.092$，仍然很低，依然会被淘汰。因此可以看出，只要 c_2 对 c_3 做出正确的判断，即 $tr_{c_3}^{c_2}$ 很低，那么这条路径的推荐信任度就会很低，进而被淘汰。因此，在该算法中，对于一条路径来说，只要良好节点能够做出正确评估，那么就可以有效防止联合欺诈行为。

除此之外，对于整个网络来说，也可以证明，网络的节点数、信任路径设置的跳数以及网络中的坏节点个数之间当存在一定关系时，便可以保证所选路径一定不含坏节点。例如，含有 10 个节点网络，坏节点数为 1，从 s 到 t 共 5 条路径可以到达，那么用该算法选择之后的信任路径必不会含有坏节点，因为有算法来保证选择信任度高的路径。但是如果坏节点数为 5，其他条件均不变，则该算法就不能保证选出的路径一定不含有坏节点。因此，给出如下的条件来保证路径中一定不包含坏节点。

已知：网络中的节点个数为 N，所含坏节点的百分比为 α，信任路径中所含节点个数为 M，两两节点直接连通的概率为 p。

结论：网络中从 s 到 t 存在的路径共 $C_{N-2}^{M-2}\cdot p^{M-1}$ 条。并且有：当 $C_{N-2}^{M-2}\cdot p^{M-1}>N\cdot\alpha$ 时，算法选出的信任路径中一定不含坏节点；当 $C_{N-2}^{M-2}\cdot p^{M-1}\leqslant N\cdot\alpha$ 时，算法选出的信任路径中可能不含坏节点，但是因为算法使用的是寻找全局非劣解的方法，所以可从最大程度上避免坏节点的存在。

5　实验及分析

实验环境为 100 M 局域网，微机配置为 Pentium IV 2.52 GHz/1 G，Windows 2003 Server/XP，用 MATLAB 实现。实验模拟了 100 个节点，且节点间的信任度随机分布的信任模型。为了让模型更接近实际，每个节点平均与 20 个以上节点有直接信任关系。先产生粒子群算法的参数：粒子群种群数量 num_swarm=100，公式(1)中更新所需参数 $c_1=c_2=2$，r_1、r_2 是介于[0,1]之间的随机数，w=0.729。

5.1　实验 1：算法的有效性

算法的有效性可以通过算法的收敛时间来评价，收敛得越快有效性越好。通过算法的迭代次数与所得路径信任度的关系来考察算法的有效性，即所得结果收敛时所迭代的次数越少，算法的有效性越好[17]。算法分别运行 20 次取平均值。

实验 1 首先将每条路径所包含的节点数，即跳数固定为 5，模拟种群规模分别为 100、200、300 时所得到的信任路径的信任度随迭代次数变化的关系，得到的结果如图 3 所示。

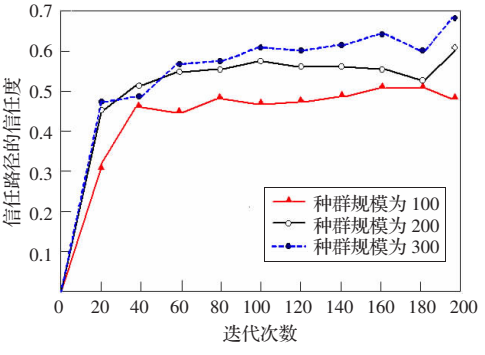

图 3　算法有效性

由图 3 可以看出，算法可以在大约迭代 40 次时就找到较优信任路径，并收敛于此，当循环次数增加时，信任度并没有明显提高了。说明该算法的有效性较好。

5.2　实验 2：跳数对算法有效性影响

实验 2 选取种群规模为 100，分别仿真了路径中的跳数为 3、6、9 时所得到信任路径的信任度与迭代次数之间的关系，以此来观察跳数对算法有效性的影响。所得结果如图 4 所示。

由图 4 可以看出，当设置跳数为 3 时，所描绘的信任度曲线在迭代 20 次时就可以收敛了，跳数为 6 时的信任度曲线在大约迭代 100 次时开始收敛，而跳数为 9 时的信任度曲线要在大约迭代 140 次时才可以收敛。因此，可以说明跳数对算法的有效性是有一定影响的：当跳数逐渐增大时，算法收敛所需要迭代的次数逐渐增大，即有效性会逐渐降低。同时，图 4 也显示了当跳数较小时选择的信任路径的信任度较高。Beth 等人定义

的信任度机制中信任度均为[0,1]之间的数,因此,从理论上分析也应该是跳数设置较小时,路径的信任度较大。

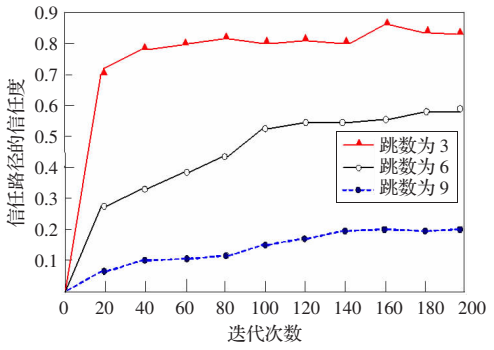

图 4　跳数对算法有效性的影响

6　结论

提出了一种新的适用于 P2P 环境的基于粒子群算法的信任模型。该模型通过多次循环选出全局的非劣解,即较优信任路径,并最终根据 BBK 信任模型将得出的多条较优路径的信任度求平均得出系统信任度。并通过实验证明了算法可在一定程度上有效防止联合欺诈行为,在性能和可靠性上也优于其他算法,可适应现实复杂网络环境的动态变化。

参考文献:

[1] Wu Xu,He Jing-sha,Xu Fei.An enhanced trust model based on reputation for P2P networks[C]//IEEE International Conference on Sensor Networks,Ubiquitous,and Trustworthy Computing,Taichung,Taiwan.[S.l.]:IEEE Press,2008:67-73.

[2] Chen R,Yeager W.Poblano:A distributed trust model for P2P networks TR-I4-02-08[R].Palo Alto:Sun Microsystem,2002.

[3] Caronni G,Sriram R D.Walking the Web of trust[C]//Proceedings of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.[S.l.]:IEEE Press,2000:153~159.

[4] Oram A.Peer-to-Peer:Harnessing the power of disruptive technology.[M].Sebastopol:O'Reilly Press,2001:222-238.

[5] Altman J.PKI security for JXTA overlay networks TR-12-03-06[R].Palo Alto:Sun Microsystem,2003.

[6] Aibrecht K,Ruedi A R.Clippee:A large-scale client/peer system TR-410[R].Swiss Federal Institute of Technology,2003.

[7] Cornelli F,Damiani E,De Capitani S,et al.Choosing reputable servents in a P2P network[C]//Proc of the 11th International World Wide Web Conf,Hawaii,2002:411-499.

[8] Kamvar S D,Schlosser M T.EigenRep:Reputation management in P2P networks[C]//Proceedings of the 12th International World Wide Web Conf,Budapest,2003:123-134.

[9] 窦文,王怀民,贾焰,等.构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J].软件学报,2004,15(4):571-583.

[10] Yahalom R,Klein B,Beth T.Trust relationships in secure systems-a distributed authentication perspective[C]//Proc 1993 IEEE Symp on Research in Security and Privacy,1993:150-164.

[11] Yahalom R,Klein B,Beth T.Trust-based navigation in distributed systems[J].Computing Systems,1994,7(1):45-73.

[12] 高承实,王建政,张栋.基于蚁群算法的信任路径寻找算法[J].计算机工程与应用,2007,43(15):131-133.

[13] Beth T,Borcherding M,Klein B.Valuation of trust in open networks[C]//Proc Computer Security-ESORICS 94,1994:3-18.

[14] Kennedy J,Eberhart R C.Particle swarm optimization[C]//Proceedings of the IEEE Conference on Neural Networks.Perth:IEEE Press,1995:1942-1948.

[15] Wang Y,Vassileva J.Trust and reputation model in Peer-to-Peer networks[C]//Proceedings of the 3rd International Conference on Peer-to-Peer Computing,Sweden,September2003:150-157.

[16] Selcuk A,Uzun E,Pariente M.A reputation-based trust management system for P2P networks[C]//Proceedings of IEEE International Symposium on Cluster Computing and the Grid,Chicago,IL,April 2004:251-258.

[17] Zhou R,Hwang K.PowerTrust:A robust and scalable reputation system for trusted P2P computing[J].IEEE Transactions on Parallel and Distributed Systems,2007,18(5).

(上接 62 页)

```
        Right_f[i+1]=(Right_f[i]+Pos_f[i])>>1;
        Row_f[i+1]=Row_f[i]+Pos_f[i];
        if(i==n)goto flag1;
        else goto flag2;}
      if(i>1)
      { i=i-1;goto flag3;}
      cout<<"num="<<mun<<endl;
      delete[]Left_f;delete[]Right_f;
      delete[]Row_f;delete[]Ban_f;
      delete[]Allow_f;
    }
    void main()
    { int n;
      cout<<"input queen \'s num:";
      cin>>n;
      test(n);
    }
```

3　算法分析

N 皇后问题的位运算算法与 N 皇后问题的普通算法相比,在执行效率上有很大的提高,通过对 n=12、13、14、15 和 16 进行计算,它们各自的运行时间见表 1。

表 1　位运算算法与普通递归回溯算法执行时间比较表

皇后个数 n	12	13	14	15	16
解的个数	14 200	73 712	365 596	2 279 184	14 772 512
位运算算法/s	0.070	0.371	2.203	13.559	93.634
普通递归回溯算法/s	2.163	14.240	107.284	685.005	5 381.839

通过表 1 可知,用位运算算法解决 N 皇后问题的执行时间比普通递归回溯算法快 30 倍以上,平均速度快 40 倍左右,因而,将位运算用于求解 N 皇后问题,能够取得很好的效果。

参考文献:

[1] 王晓东.计算机算法设计与分析[M].北京:电子工业出版社,2001:132-135.

[2] 张世禄,潘大志,冯天敏.C 语言程序设计[M].北京:电子工业出版社,2005:18-20.

[3] 白艳萍,杨明.一类求解八皇后问题的神经网络模型[J].山西大学学报:自然科学版,2001,24(1):22-25.

[4] 周康,同小军,许进.基于闭环 DNA 模型的八皇后问题算法[J].计算机工程与应用,2007,43(6):4-6.

[5] 刘娟,欧阳建权,陈良军.用混合遗传算法求解 N 皇后问题[J].湘潭大学自然科学学报,2007,29(2):37-41.