CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 40 卷第 6 期 2018 年 6 月
Vol. 40, No. 6, Jun. 2018

文章编号:1007-130X(2018)06-0977-07

面向选择推荐节点的 P2P 网络信任模型*

马满福[1,2],何春玲[1,2]

(1.西北师范大学计算机科学与工程学院,甘肃 兰州 730070;2.甘肃省物联网工程研究中心,甘肃 兰州 730070)

摘　要:对等网(P2P)具有开放性、匿名性等特点,节点之间的交互类型复杂多样并且具有较小的重复交互性,导致其节点之间的信任关系难以确定。提出一种基于选择节点的 P2P 网络信任模型,通过直接信任和推荐信任得到节点综合信任值。选择推荐节点时,使用推荐节点与交互节点信任值相似度作为标准,以其信任差值最小的推荐节点作为被选择节点;同时,针对共谋团体的团伙欺骗,提出连带惩罚机制以及对提供可靠消息节点的奖励机制。仿真实验结果表明,该模型不但具有抗恶意节点攻击的能力,同时还具有较高的自适应能力。

关键词:对等网络;信任;挂起;激励机制

中图分类号:TP393　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2018.06.003

A P2P network trust model for selecting recommended nodes

MA Man-fu[1,2], HE Chun-ling[1,2]

(1. College of Computer Science & Engineering, Northwest Normal University, Lanzhou 730070;
2. Gansu IOT Research Center, Lanzhou 730070, China)

Abstract: Due to the openness and anonymity of Peer-to-Peer (P2P), the types of interactions between nodes are complex and diverse, and they have small repetitive interactions, which makes it difficult to define the trust relationship between nodes. Based on selected nodes, we propose a P2P network trust model, and obtain comprehensive trust value through direct trust and the recommended trust for each node. Recommendation nodes whose trust value is closest to the interactive nodes are selected, that is to say, nodes with the smallest trust difference are selected. We also propose a joint punishment mechanism and an incentive mechanism to prevent gang cheating of the conspiracy group. Simulation experiments show that the trust model is not only capable of resisting attacks of malicious nodes, but also has a high self-adaptability.

Key words: P2P; trust; pending; incentive mechanism

1　引言

对等网络 P2P(Peer-to-Peer)的开放、节点匿名以及不同节点之间的松耦合等特点使得一些恶意行为、非法内容、垃圾数据等肆意传播,从而导致了一系列的安全问题。另外,由于奖励、惩罚机制的缺乏,使得一些节点进入了懒人模式(只下载文件,不上传文件)。国内外相关研究表明:制约 P2P 发展的重要因素是节点之间的信任问题。针对信任,学者们已经展开了大量的研究,但这些研究普遍存在的问题是:多数只将节点信任度作为服务选择的依据,即该类系统根据节点的历史交易反馈信息为节点计算信任等级[1-6]。当存在多个可选服务时,信任等级高的节点成为首选。这样做可以在一定程度上抑制节点的一般恶意行为,但在应付许

* 收稿日期:2016-12-25;修回日期:2017-04-26
基金项目:国家自然科学基金(71263045);甘肃省科技支撑计划(1204FKCA162)
通信地址:730070 甘肃省兰州市西北师范大学计算机科学与工程学院
Address: College of Computer Science & Engineering, Northwest Normal University, Lanzhou 730070, Gansu, P. R. China

多针对信任模型本身的一些攻击,如不诚实反馈、协同作弊及策略型攻击等恶意行为的过程中表现出来的有效性与健壮性仍然不够。节点与节点之间不存在制约关系,这更方便了一些恶意行为的大肆传播。

针对以上缺陷,本文提出了面向选择节点的P2P网络信任模型。在本模型中各节点之间不仅仅存在直接信任和推荐信任,而且还涉及到交互节点的信任值。为此,本文准备了两套应对方案:第一套方案为找出综合直接信任和间接信任均值最接近的信任值节点,此节点会有一个专门指针指向与均值信任相接近节点的IP。另外,此节点在向另外一个节点推荐信任时,会根据本节点自身收到的推荐信任的权值加自身通过直接交易信任值的权值,把信任值推荐给下一个节点;方案二为:使用推荐节点与交互节点信任值相似度来寻找选择节点的IP。这样,存有相似兴趣的节点以一个双链接的形式存在。如果某节点出现恶意行为,那么与它相连接的所有节点均会受到不同程度的信任值削减。同样,如果一个节点有好的信誉,那么与其相关的节点也会得到不同程度的信任值提升。这样做,既可以防止节点的恶意行为,也可以防止节点的不诚实推荐以及节点协同恶意行为等。

2 相关工作

目前,随着P2P的迅速发展以及广阔的市场,出现了大量基于P2P的信任模型。文献[6]提出了一个适用于P2P电子社区的局部信任模型,节点的可信度是对以往该节点向其他节点提供服务的水平的综合评价;文献[7]通过给不同评价者的反馈值分配一个适当的权重,提出了分布式架构;文献[8]通过研究移动P2P节点的信任关系的变化与网络使用者的兴趣、爱好的等变化的对应关系,提出了一种基于增强的稳定组模型的信任评估方法;文献[9]给出了一种基于信誉的信任模型,此模型被用来计算云基础设施提供商的可信性;文献[10]为了解决传统信任模型无法处理冲突程度高而引起的信任计算不准确问题,采用重新分配冲突概率与引入权重系数的策略,提出一种改进的D-S(Dempster-Shafer)证据理论的P2P系统信任模型DSETTM(Trust Model Based on D-S Evidence Theory for P2P networks),并将其用于P2P网络的信任建模;文献[11]建议将节点 i 的档案点沿Terrace树根节点的方向做一定的迁移,使节点信任度的分布更加平衡,路由效率更高;文献[12]针对P2P系统的动态开放等固有特征使其面临严重的行为问题,提出了一种P2P环境下的基于反馈的Web服务选择信任模型;文献[13]采用对评价信息汇集并使用一些相似度或排名比较算法得到最终信任值,提出一种基于反馈相关性的P2P网络信任模型;文献[14]提出了一个加权大多数算法WMA(Weighted Majority Algorithm),算法的思想是对不同推荐者的推荐分配不同的权重,根据权重来聚合相应的推荐,并根据交互的结果来动态地调整相应权重。

上述方案在解决P2P信任方面做了很多有益的尝试,且取得了一定的成果,但是由于这些模型关心的重点是参与交互的节点,所以没有将推荐节点作为一个重要的参考指标进行计算,这将使交易节点在推荐信任方面处于被动状态。基于此,本文提出了面向选择推荐节点的P2P网络信任模型。

3 面向选择节点的P2P网络信任模型

根据共同兴趣群将节点分为三种类型:普通节点 N、推荐节点或间接节点 IN 以及直接交易节点 DN。对于 N,它在不参与交易时,是闲置节点;而 IN 作为推荐节点在推荐信任值被采纳时会得到一个指针指向该资源节点的 IP;DN 是动作的接受者以及发出者,它是交易的关键节点,它的父节点有可能是 N 也有可能是 IN。图1是选择节点的P2P网络结构图,图中描绘了三个小型网络组成的一个大型网络。目标节点如果不是共同兴趣群里的,也可以进行正常的互动,例如节点 DN_4 位于 C 群落里,而 IN_1 和 IN_2 分别在 A 群落里和 B 群落里,并且他们可以通过不同节点进行互动。网络中任意节点 N_i 同时扮演着三种角色,它不但是用户节点、管理节点,同时还是监测节点。管理节点只提供信任数据的存取;监测节点负责对与它进行交互节点的监测,一旦发现某节点 N_i 发生异常,就会立即报警。

本模型的基本思想是节点根据直接交易以及相邻节点所推荐的间接信息按一定比例建立对目标节点的信任关系。此外,此节点搜索出与均值信任相近的节点,并在指针序列中添加指向该节点 IP 的指针。如果目标节点(例如 IN_1)想要和节点 DN_1 互动,那么节点(DN_1)就要通过本身与节点 N_1 的交易信任值以及与 N_1 邻节点的推荐信任值相结合,从而生成对 N_1 的信任值;然后根据算法,

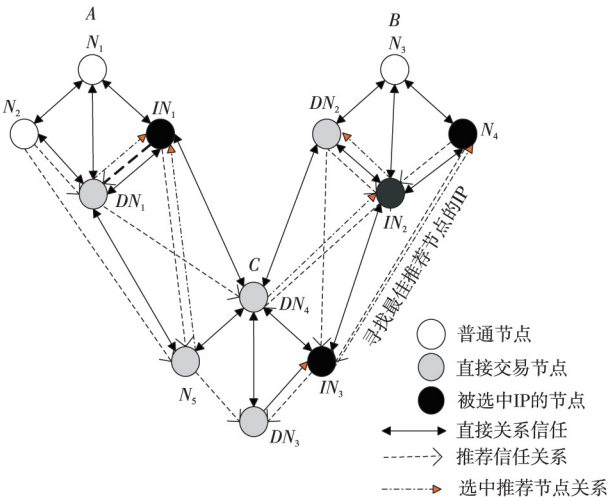

Figure 1 P2P network structure of the selected node

图 1 选择节点的 P2P 网络结构图

在 DN_1 指针序列中生成一个指针指向与信任均值相接近的节点,这里假定 IN_1 为被选中的节点。假如某一节点被怀疑为恶意节点,那么与它有联系的所有节点的信任值都会受到缩减;与此相反,如果某一节点受到好评,那么与它有关的节点的信任值都会有不同程度的增加。

按照各节点的不同状态,节点可划分为普通状态、交互状态和挂起状态。图 2 是节点三种状态之间的转换关系。图 3 中普通状态和交互状态是可逆的转换:当某个节点向另一节点主动发起交互申请时,被发起交互的节点同意请求时,这两个节点便由普通状态变为交互状态;当交互完成,这两个节点又恢复普通状态。但是,交互状态与挂起状态之间是不可逆的,他们之间只有一条路径:交互节点在交互期间如果信任值小于或等于 0 时($r \leqslant 0$),那么交互状态将被挂起,即变为挂起状态;被挂起的节点只有等到等待的事件发生时才可以重新初始化信任值,变为普通状态。

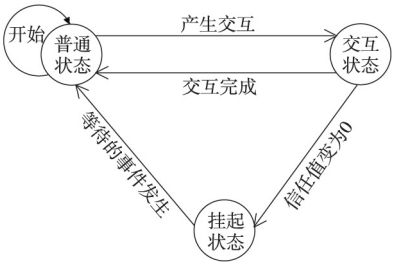

Figure 2 Transition diagram between states

图 2 各状态之间转换关系图

3.1 模型的工作流程

信任模型是建立在综合信任的主观性、复杂性以及不确定性等特点基础之上的一种信任关系框架,是对节点之间信任关系的综述。信任模型的建立是为了给节点服务提供信任度较高的信任目标作为交互目标,从而高效地完成交互任务。

首先,为每个节点进行信任值的初始化,初始值为 0.5;其次,本模型根据节点是否发生交互依次去处理发生的事件:如果没发生交互,则节点继续保持它原有的初始化信任值;反之,本文就会依次去计算节点的推荐信任值 IR_i 、推荐信任均值 AIR、添加指针 P、直接信任值 DR 以及计算综合信任值 SR ;最后,根据计算的综合信任值 SR 来判断该节点的状态以及是否实施奖惩机制:如果 SR 的值小于或等于零时,要报警。一旦进入这一阶段,本节点不仅要被挂起,其它与之相关的节点也会受到不同程度的惩罚;如果 SR 的值大于零,对提供可信的节点进行信任值奖励并储存下该节点的综合信任值 SR ,这也意味着此次交互成功完成。具体流程如图 3 所示。

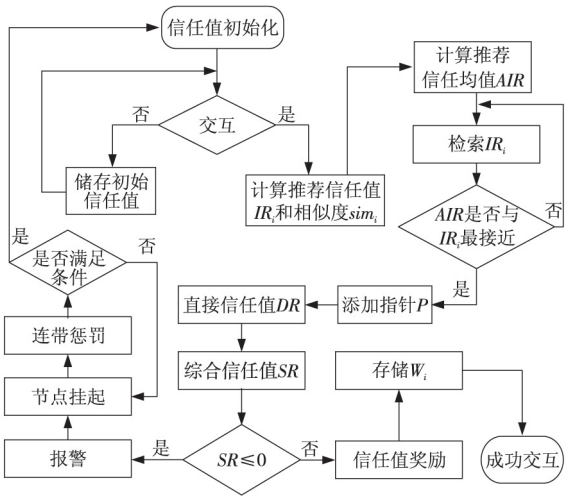

Figure 3 Flow chart of the model

图 3 模型流程图

3.2 模型的定义及其表示

3.2.1 信任值的计算

定义 1(局部信任度) 在交互期间内节点 N_s 、N_k 之间交易了 T_{sk} 次,则局部信任度(直接信任度)可定义为:

$$DR_{sk} = (N_s, N_k) = \begin{cases} \sum_{s=1,k=1}^{T_{sk}} F(N_s, N_k), T_{sk} \neq 0 \\ 0, T_{sk} = 0 \end{cases} \tag{1}$$

其中,DR_{sk} 为节点 N_s 对 N_k 的直接信任值,即节点 N_s 对节点 N_k 的直接交互反馈。当 $DR_{sk} = 0$ 时,表示节点 N_s 与节点 N_k 之间不存在交互,即节点 N_s 对节点 N_k 的直接信任值为 0。

定义 2(推荐信任度) 令 IR_i 为节点 N_s 与节

点 N_k 在交互过程中的 N_k 下游的节点,即推荐主题的集合为 $A_i=\{n_1,n_2,\cdots,n_g\}$,设 n_g 的推荐信任度为 IR_{n_g},$g=1,2,\cdots,n$,则 N_s 共接纳的推荐信息 ZIR 与推荐信息的信任均值 AIR 为:

$$ZIR=IR_{n_1}+IR_{n_2}+\cdots+IR_{n_g}=\sum_{z=1}^{g}IR_{n_z} \tag{2}$$

$$AIR=\frac{\sum_{z=1}^{n_g}IR_{n_z}}{n_g} \tag{3}$$

定义 3(综合信任) 综合信任是在推荐信任以及局部信任(直接信任)之上,根据它们不同的权重相结合的信任度。具体为:

$$SR=(1-\varepsilon)*IR_i+\varepsilon*DR \tag{4}$$

其中,ε 为信任的权重参数,且 $0\leqslant\varepsilon\leqslant1$,权重随着节点的不同会有不同的数值。

相似度是推荐节点自身的信任值与交互节点信任值的相似度。本文将推荐节点的推荐信任度与平均推荐相似度之差的最小值作为最后指针所指的推荐节点。具体计算公式如下:

$$sim_i=\begin{cases}0, IR_i<0, IR_i>1\\ \dfrac{IR_i-\min IR_i}{MaxV+\min IR_i}+\dfrac{IR_i}{\min IR+MaxV}, \\ \qquad \min IR_i\leqslant IR_i<MaxV\\ 1, IR_i\geqslant MaxV\end{cases} \tag{5}$$

$$sim=\alpha^{m(t_i,t_d)}sim_i \tag{6}$$

其中,式(5)代表间接相似度,$MaxV$ 是参与交互节点的信任值;$\min IR_i$ 代表文中对推荐节点所提出的最小信任值;式(6)是引入时间衰减因子 α 计算相似度;$m(t_i,t_d)$ 表示从 t_i 到 t_d 所经历的时间(按照某一周期计算)。

3.2.2 信任信息的分布式存储

本文在文献[15]提出的 Tuerrace 拓扑基础上规划了信任信息存储机制。如图 4 所示,以中心点 a 为上游节点,其存储数据是通过公式(4)计算所得的综合信任值以及指向推荐信任的某个节点 N_i 的指针。其中,指针序列是用来存放指向推荐信任值节点地址的指针,这是一块特殊的缓存空间。当某节点需要同上一级节点进行交互时,首先查看上一级节点的综合信任值(推荐信任值和直接信任值)是否满足要求,一旦满足,此节点的指针就会指向该节点。其次,(b,c,d) 为中心节点的下游节点,这些节点所存数据与中心节点所存数据不同,相比中心节点,下游节点所存数据很少,只保存综合信任值和指针,这样大大节约了节点的空间资源。以此类推,位于下游的节点皆按此方式存储数据。

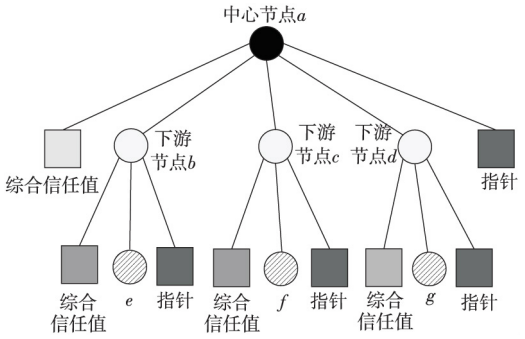

Figure 4 Storage structure of trust data

图 4 信任信息存储结构图

3.2.3 节点挂起惩罚激励机制

在本文中,如果某节点 N_i 出现异常,则与它有关的所有节点的信任值都会受到缩减,本文称此为连带惩罚或反向惩罚。

定义 4(信任值减小) 由于权重值的不同,所以推荐信任的节点与局部信任(直接信任)会按其权重的多少来决定各自信任值缩减的多少。其中,局部信任值与推荐信任值缩减计算公式如下所示:

$$CDR=CR*\eta \tag{7}$$

$$CIR=CR*\lambda \tag{8}$$

式(7)表示受罚时,局部信任节点的信任值的缩减计算;式(8)表示受罚时,推荐信任节点信任值的缩减计算。其中,CR 为当前出现异常节点的信任值,λ 与 η 分别为推荐信任和局部信任(直接信任)的权重参数。

挂起节点定义为暂时被淘汰出交互的节点。由于网络的容错能力有限,在异常节点到达预定信任值下限时,P2P 网络就会对节点进行合理安排。其中,出现异常的节点就会被强制禁止与其他节点进行交互,此时,该节点将会进入挂起状态。具体执行过程如图 5 所示。

节点已存在,但由于信任值达到下限值,必须创建挂起状态使节点进入惩罚状态。此时的节点不但接受信任值被削减的惩罚,且不可进入交互状态。审核是由各个正常节点经过一段时间的观察以及测试等来判断此节点是否知错改过,通过审核来决定是否给受惩罚节点重新进入交互的权利。一旦信任值被减到零,此节点就会进入惩罚状态。信任值为零是节点的下限。如果被惩罚节点通过审核,那么它就会重新获得一次机会与其它节点进行交互。恢复后的信任值是最初被赋予的值,它也

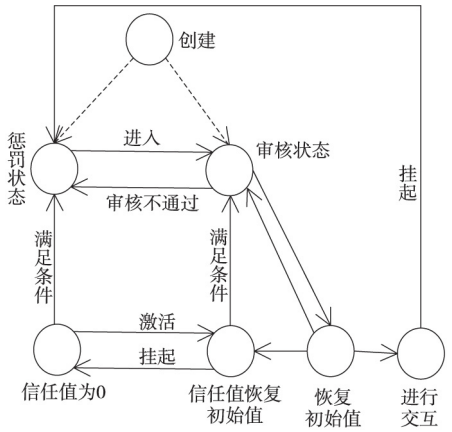

Figure 5 Sketch map of the node hanging up punishment mechanism

图 5 节点挂起惩罚机制示意图

是惩罚节点通过审核的一个重要条件。通过审核且审核合格,受罚节点可以被允许进行信任值的初始化并且与正常节点进行交互。

本模型根据 P2P 网络具有开放式、匿名性、无中心等一系列的特性,以及传统的安全机制如基于 PKI 安全机制并不能很好地保障节点的安全,提出基于节点挂起惩罚的激励机制,本机制的建立主要有两个目的:(1)减少节点资源的浪费;(2)使得本系统更加人性化。

3.3 信任算法

关于节点选择算法,设 AIR 为推荐节点的推荐均值,在推荐信任集合 ζ 中,IR_i 为 ζ 的子集,从 ζ 中找出与 AIR 的相似度最高的子集 IR_i,并将指针 P 指向该推荐节点的 id;其次,计算出直接信任值,根据这两步,利用公式(4)计算出综合信任值 SR。其算法的具体实现如算法 1 所示。

算法 1 信任算法

输入:推荐信任值 IR_i,直接信任值 DR。

输出:$credit$,sim。

```
1 begin
2 k → size; //推荐信任值节点的个数
3 for each IR_i in ξ//遍历 ξ 集合中的 IR_i
4   If IR_i≤1 ‖ IR_i≥-1//计算推荐信任均值
5     SIR=SIR+IR_i;//总推荐信任值的计算
6     sim_l←根据公式(5);
7     sim^a← 根据公式(6);
8   Else continue;/*不满足条件就跳过此节点继续计算下一个节点的信任值*/
9   end for;
10  AIR← 根据公式(3);
11  ζ←ζ∪{IR_i};/*把每个推荐节点的推荐信任值存入 ζ*/
12  for each IR_i in ξ
13    compute f(AIR,IR_i);/*计算 AIR 与 ζ 中每个 IR_i 的相似度*/
14    Choose the highest similarity of IR_k;
15    P→ID_(IR_k);//指针指向被选中的推荐节点
16  end for;
17  SR← 根据公式(4);
18  output the credit of SR;//输出当前信任值
19  output the sim^a and sim_l;/*输出相似度 sim^a 和 sim_l*/
20  release other IR_(ζ-1);
21 end
```

本文所提出的算法,因其没有复杂的迭代计算过程,所以具有良好的计算收敛性。首先,在计算推荐信任均值 AIR 时,需要遍历所有推荐节点(被推荐节点的下游一级推荐节点)的推荐信任值,因此其时间复杂度为 $O(n)$,其空间复杂度为 $O(n)$;其次,推荐信任均值 AIR 与推荐信任值相匹配的算法中,其时间复杂度为 $O(n)$,空间复杂度为 $O(n)$。

异常节点的检测与挂起算法如算法 2 所示。

算法 2 异常节点的检测与挂起算法

输入:节点状态 $STATE$。

输出:$STATE$。

```
1 DetectandHungNode(ε);//ε 为与交互相关的节点集
2 Get(ID,SR,STATE);/*获取节点的 ID(地址)、SR(当前信任值)、STATE(状态)*/
3 if (STATE==0)
4   If satisfy the condition do//如果满足条件
5     Initialization(SR);//初始化节点信任值
6   end if;
7 end if;
8 if (STATE==1)
9   if (SR≤0)//节点处在交互态,但信任值变为零
10    state=0;
11    Hand up this node;//将状态变为零,节点挂起
12  end if;
13 end if
```

$STATE$ 代表节点状态,是检测节点是否异常的第一道关卡,取值为 0 或 1,简化了节点的检测。

4 仿真实验与分析

4.1 仿真环境及其参数

本节建立了多个仿真实验来检测信任模型的效果。仿真实验在 Eclipse Enterprise Workbench Version:2014 JDK 1.7 上进行,其系统运行环境

为 Windows 7 旗舰版 X64 位,通过 Matlab 环境将运算数据生成图表。仿真参数的设定值见表 1。

Table 1 Simulation parameters

表 1 仿真参数表

仿真参数	缺省值
交互节点信任值 *maxva*	0.52
交互节点提供最小信任值 *minva*	0.3
时间衰减因子 α	0.5～0.7
信任的权重 ε	0.4
节点挂起数目 M	0～20

仿真过程探究了不同节点推荐信任度以及推荐节点自身的信任度与参与交互节点信任度。此外,相似度引入了衰减因子 α 来仿真信任值的变化。

4.2 推荐节点选择的仿真

首先,仿真实验按照设定的参数完成初始化后,分别针对推荐节点信任度与交互节点信任度以及推荐节点推荐信任相似差的计算仿真,验证本模型抗拒恶意节点的效果及自适应性。

表 2 和表 3 是仿真的三组数据。表 2 中跳过的节点预示不在选择范围内,而相似度越高的节点越有可能被选中;表 3 中数据差值越大表示节点越不容易被选中,相反,差值越小表示节点越容易被选中。

另外,仿真这三组数据分别代表三种不同的选择:第一组的情况是交互节点可以根据相似度进行选择,也可以根据差值进行选择;第二组的情况适应于根据差值进行选择;第三组的情况适应于根据相似度进行选择。不同节点可以根据自身及网络环境的不同选择测量标准,这样做既降低了恶意节点的破坏概率,也提高了网络的自适应能力。

4.3 相似度变化仿真

α 的设定是为了保证相似度的有效性。如图 6 所示,相似度随时间的增加而减少。本文将 α 设置了三个值。

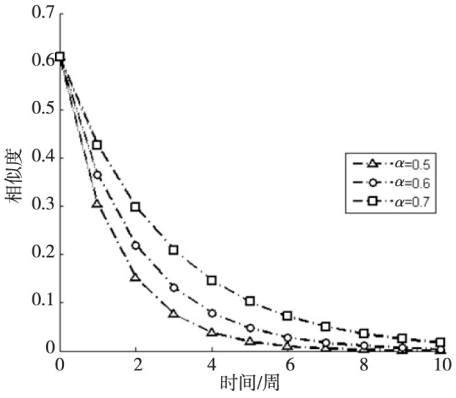

Figure 6 Similarity changes with time

图 6 相似度随时间的变化

Table 2 Trust similarity between the recommendation node and the interaction node

表 2 推荐节点信任度与交互节点信任度相似度

分组		节点									
		一	二	三	四	五	六	七	八	九	十
第一组	信任值	0.5	0.21	0.35	0.6	0.65	0.43	0.75	0.8	0	0
	相似度	0.85	跳过	0.49	1	1	0.68	1	1	跳过	跳过
第二组	信任值	0.4	0.7	0.4	0.35	0.75	0.43	0.3	0	0	0
	相似度	0.61	1	0.61	49	1	0.68	0.37	跳过	跳过	跳过
第三组	信任值	0.0	0.6	0.5	0.4	0.7	0.56	0.53	0	0	0
	相似度	跳过	1	0.85	0.6	1	1	1	跳过	跳过	跳过

Table 3 Recommended trust value difference

表 3 推荐信任度差值

分组		节点									
		一	二	三	四	五	六	七	八	九	十
第一组	推荐信任值	0.42	0.51	0.7	0.2	0.9	0.8	0.3	0.41	−1	0
	差值	0.096	0.186	0.376	0.124	0.576	0.476	0.024	0.086	1.324	0.324
第二组	推荐信任值	0.32	0.6	0.5	0.43	0.75	0.34	0.23	−1	−1	0
	差值	0.203	0.483	0.383	0.313	0.633	0.223	0.113	1.117	1.117	0.117
第三组	推荐信任值	−1	0.5	0.45	0.35	0.6	0.75	0.4	−1	−1	0
	差值	1.005	0.495	0.445	0.345	0.595	0.745	0.395	1.005	1.005	0.005

由图 6 可以明显看出,当 $\alpha=0.5$ 时,相似度下降较快;当 $\alpha=0.6$ 时,相比前者下降速度有所减缓;当 $\alpha=0.7$ 时,相似度下降速度明显缓慢。α 的取值是由节点自身及网络环境所决定的。

5 结束语

移动 P2P 网络环境的开放性、匿名性等特点使节点之间的信任关系显得尤为重要,因此节点之间的信任问题成为目前的一个热门研究。本文提出了一种基于选择节点的 P2P 网络信任模型。在此模型中,节点被划分为三类,并给出了这三种类型节点之间的转化关系。与此同时,本文还给出了基于挂起惩罚的激励机制,这与现有信任模型相比大大节约了节点资源。仿真实验表明,本文所提出的模型不仅具有抵抗恶意节点、节约资源的特点,且也具有较好的自适应性和自治性。接下来的工作是研究基于选择节点 P2P 信任模型的效率,包括推荐信任节点的检索效率以及推荐信任均值计算效率等。

参考文献:

[1] Khambatti M, Dasgupta P, Ryu K D. A role-based trust model for peer-to-peer communities and dynamic coalitions[C]// Proc of the 2nd IEEE International Information Assurance Workshop, 2004: 141-154.

[2] Almenarez F, Marin A, Diaz D. Developing a model for trust management in pervasive devices[C]// Proc of the 3rd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2006), 2006: 1-5.

[3] Marti S, Garcia-Molina H. Limited reputation sharing in P2P systems[C]// Proc of the 5th ACM Conference on Electronic Commerce, 2005: 91-101.

[4] Jordi S M, Paolucci M. On representation and aggregation of social evaluations in computational trust and reputation models [J]. International Journal of Approximate Reasoning (Elsevier), 2007, 46: 458-483.

[5] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks[C]// Proc of the 2nd International Workshop on Agents and Peer-to-Peer Computing, 2004: 23-34.

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

[7] Abawajy J. Establishing trust in hybrid cloud computing environments[C]// Proc of IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011: 118-125.

[8] Wu Xu. Enhanced stable group model-based trust evaluation scheme for mobile P2P networks[J]. Chinese Journal of Computers, 2014, 37(10): 2118-2127. (in Chinese)

[9] Pawar P S, Rajarajan M, Nair S K, et al. Trust model for optimized cloud services[C]// Proc of the 6th IFTP International Conference on Trust Management, 2012: 97-112.

[10] Gao Wei, Zhang Guo-yin, Song Kang-chao, et al. P2P trust based on D-S evidence theory[J]. Computer Engineering, 2012, 38(1): 114-119. (in Chinese)

[11] Zhang Qian, Zhang Xia, Wen Xue-zhi, et al. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96-107. (in Chinese)

[12] Chen Wen-dong, Li Min-qiang, Zhao Qing-zhan. Research of web service selection trust model on P2P environment[J]. Journal of Computer Science, 2015, 42(1): 113-118. (in Chinese)

[13] Wang Yong, Hou Jie, Bai Yang, et al. Survey on feedback correlation based dynamic trust model for P2P systems[J]. Computer Science, 2013, 40(2): 67-74. (in Chinese)

[14] Yu B, Singh M P, Sycara K. Developing trust in large-scale peer-to-peer systems[C]// Proc of the 1st IEEE Symposium on Multi-Agent Security and Survivability, 2004: 1-10.

[15] Dou Wen, Wang Huai-min, Jia Yan, et al. A recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15(4): 571-583. (in Chinese)

附中文参考文献:

[8] 吴旭. 基于增强稳定组模型的移动 P2P 网络信任评估方法[J]. 计算机学报, 2014, 37(10): 2118-2127.

[10] 高伟, 张国印, 宋康超, 等. 一种基于 D-S 证据理论的 P2P 信任模型[J]. 计算机工程, 2012, 38(1): 114-119.

[11] 张骞, 张霞, 文学志, 等. Peer-to-Peer 环境下多粒度 Trust 模型构造[J]. 软件学报, 2006, 17(1): 96-107.

[12] 陈文东, 李敏强, 赵庆展. 基于 P2P 环境下的 Web 服务选择信任模型研究[J]. 计算机科学, 2015, 42(1): 113-118.

[13] 王勇, 侯洁, 白杨, 等. 基于反馈相关性的 P2P 网络信任模型[J]. 计算机科学, 2013, 40(2): 67-74.

[15] 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.

作者简介:

马满福(1968-),男,甘肃甘谷人,博士,教授,研究方向为分布计算和移动计算。**E-mail**: 798686265@qq.com

MA Man-fu, born in 1968, PhD, professor, his research interests include distributed computing, and mobile computing.

何春玲(1989-),女,山东菏泽人,硕士生,CCF 会员(59436G),研究方向为物联网。**E-mail**: 2596714116@qq.com

HE Chun-ling, born in 1989, MS candidate, CCF member (59436G), her research interests include Internet of things.