一种 Peer-to-Peer 环境下的综合信任模型

宋 伟, 卢正鼎, 李瑞轩, 於光灿

(华中科技大学 计算机科学与技术学院, 湖北 武汉 430074)

E-mail: sw_cyt@126.com

摘 要: 提供一种高效的信任模型是保证 P2P 系统高效、稳定的关键. 列举目前已有的信任模型, 并以节点自身兴趣为基础, 综合 P2P 网络中节点的推荐给出了一种 P2P 环境下的综合信任模型. 在 JXTA 架构上予以实现, 给出实验结果及分析.

关 键 词: 对等网络; 信任模型; 推荐

中图分类号: TP393 **文献标识码**: A **文 章 编 号**: 1000-1220(2006)05-0774-05

Integrated Trust Model for Peer-to-Peer Networks

SONG Wei, LU Zheng-ding, LI Rui-xuan, YU Guang-can

(*School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan* 430074, *China*)

Abstract: An effective trust model is the key of a P2P system's great efficiency and stabilization. Enumerate some known trust models and introduce a trust model using in P2P network based on interesting of peer itself and other peers' recommendations. And implement the integrated trust model on the JXTA framework, then do some simulating experiments, analyze the result of the simulating experiments at last.

Key words: Peer-to-Peer; trust model; recommendation

1 引 言

随着 Nepster 提供了一种不必通过中心服务器在用户之间共享 MP3 的程序在网上出现, Peer-to-Peer (简称 P2P) 这一全新网络拓扑结构在互联网上迅速崛起, 并在文件共享、多媒体播放等众多应用领域中显示出巨大优势. P2P 环境中没有中心服务器, 解决了服务器访问瓶颈问题的同时也带来了一些问题需要研究解决. 没有集中式服务器, 在 C/S 模式下已经很成熟的基于可信的第三方 (比如集中 CA) 鉴权方式来保证系统安全性就变得不可行了. 虽然目前 P2P 应用日益广泛, 但是仍然缺乏有效的管理机制来保证系统的安全性和服务质量. 这显著地表现在目前的应用中存在大量欺诈行为和不可靠的服务质量方面[1].

好的信任模型是保证网络提供高质量服务的关键. 目前, 已经有一些基于 Peer-to-Peer 环境下的信任模型, 大致可分为以下几类[2, 3]:

(1) 基于 PKI 的信任模型. 这类系统中, 存在少数被称为 Leader Peer 的节点, Leader Peer 负责监督整个网络运营状况, 定期向网络发出通告通知不可信任节点. 这些 Leader Peer 的合法性通过 CA 颁发证书加以保证. 因为引入了 CA 和 Leader Peer, 这类系统往往具有中心依赖性, 在系统的可扩展性方面具有缺陷.

(2) 基于局部推荐的信任模型[4, 5]. 这类系统中, 节点访问局部范围内的其它节点获取其它节点对待访问节点的推荐, 最终得到待访问节点的信任度.

(3) 数据签名. 该方法基于数据的可信度进行访问, 被用于文件的转发存储中. 用户下载完数据后, 如果认可数据的真实性就对数据进行签名认证, 因此可以认为获得签名越多的数据就是被越多用户确认的数据, 也相应的拥有较高的可信度. 这种方法只适合数据文件共享的应用环境, 同时无法防范集体的欺诈行为.

(4) 全局可信度模型. 该模型通过获得所有信任节点关于访问节点的可信度推荐来决定访问节点的可信度. 这种信任度是基于全局迭代产生的, 所以这种信任度可以认为是全局信任度.

上述各种 P2P 环境下的信任模型都有着本身的优势和不足, 本文将提出一种综合节点自身兴趣和周围节点推荐构造的综合信任评估模型. 在 JXTA 平台上将提出的综合信任模型加以实现, 进行仿真实验, 并给出实验结果和相关分析.

2 基于节点兴趣和推荐的综合信任模型

2.1 基于节点兴趣的信任评估

P2P 环境下, 节点把自己提供的服务信息发布到对等网中. 综合信任模型中, 为了使节点在访问服务时根据自身兴趣进行选择, 服务信息采用 XML 描述. 每个服务包含如下信

收稿日期: 2005-02-18 基金项目: 国家自然科学基金项目 (60403027) 资助; 湖北省自然科学基金项目 (2005ABA258) 资助; 软件工程国家重点实验室开放基金项目 (SKLSE05-07) 资助. 作者简介: 宋 伟, 男, 1978 年生, 博士研究生, 研究方向为分布式异构系统的安全; 卢正鼎, 男, 1944 年生, 博士生导师, 研究方向为分布式系统, 智能信息系统, 信息安全; 李瑞轩, 男, 1974 年生, 博士, 副教授, 研究方向为分布式异构系统, 分布式系统安全. 於光灿, 男, 1974 年生, 研究方向为系统安全.

息: 提供服务的节点 peerID, 标示服务的 serviceID, 服务的描述关键字. 举例如下:

```
<?xml version="1.0" encoding="utf-8" ?>
<service ID='service1' peerID='IDNumber1'>
  <keyword id='keyword1'>
    <value>value1</value>
  </keyword>
  <keyword id='keyword2'>
    <value>value2</value>
  </keyword>
</service>
```

发布服务时发布节点根据服务的内容提供多个关键字对服务进行描述, 当节点访问服务时, 根据自己的兴趣和服务描述关键字设定被访问节点的优先级. 这与社会的关系模型是相似的. 例如: 某个眼病病人, 他感兴趣的是哪个医院的眼科实力更强, 他可能会选择一家较远的眼科专科医院就诊, 而不选择一家更近的综合实力较强的医院. 这也是本文设计信任模型的基本思想, 基于节点的个人兴趣判断访问节点的优先次序. 这一点与 Poblano[6] 模型有相似之处.

表 1　PeerService 表结构

数据项	数据类型	数据说明
PeerID	Char	提供服务节点的 peerID
ServiceID	Char	标示服务的 serviceID
KeyWord	Char	服务描述关键字
AccessTimes	Integer	总访问次数
SuccessTimes	Integer	访问成功次数

综合信任模型中每个节点存储了两张 PeerService 和 AccessService 表, 存储了本节点访问过的 service 信息, 表结构分别如表 1 和表 2 所示.

表 2　AccessService 表结构

数据项	数据类型	数据说明
PeerID	Char	提供服务节点的 peerID
ServiceID	Char	标示服务的 serviceID
KeyWord	Char	服务描述关键字
AccessTime	Time	访问服务时间
AccessResult	bool	访问结果

PeerService 表记录节点在一定时间范围内访问服务的统计结果. AccessService 表记录节点在一定时间范围内访问服务的具体结果. 这里每个节点有一个 updatePeerService 服务, 用户根据情况, 设定数据时间范围和调用 updatePeerService 的时间间隔. 规定时间间隔和节点新上线的情况都会调用 updatePeerService 服务, 更新 AccessService 表. 将访问时间超出数据时间范围的记录清除, 之后在 AccessService 表的基础上重新生成 PeerService 表. 使得 PeerService 表中的记录始终在设定时间范围内, 不会因为拥有太多陈旧数据影响到信任模型的判断. updatePeerService 服务描述如下:

```
Delete * from AccessService where AccessTime< Now()-设定值;
Drop Table PeerService;
CREATE TABLE PeerService(PeerID char(20), ServiceID char(20), KeyWord char(30), AccessTimes Integer, SuccessTimes Integer)
Insert into PeerService (PeerID, ServiceID, KeyWord, AccessTimes) select PeerID, ServiceID, KeyWord, count(ServiceID) from AccessService group by AccessService.ServiceID
Insert into PeerService (SuccessTimes) select count(AccessService.ServiceID) from AccessService where PeerService.ServiceID= AccessService.ServiceID
```

节点访问对等网中服务时, 首先根据自己感兴趣的关键字, 在自己获取的服务通告中查找自己感兴趣的服务. 并对能够提供这类服务的所有可能的节点进行信任评估. 下面给出节点的信任评估定义: P_{ij} 表示节点 i 对节点 j 的信任度则

$$P_{ij}=\sum_{PeerID=j}\frac{SuccessTimes}{AccessTimes}\times\frac{AccessTimes}{\sum_{PeerID=j}AccessTimes}\times X=\sum_{PeerID=j}\frac{SuccessTimes}{\sum_{PeerID=j}AccessTimes}\times X \quad (j\neq any\ PeerID\ 时,\ P_{ij}=0) \tag{1}$$

$$X=\begin{cases}\lambda(\lambda>1) & Service\ 的\ KeyWord\ 与用户的兴趣匹配\\ 1 & Service\ 的\ KeyWord\ 与用户的兴趣不匹配\end{cases}$$

为保证 P_{ij} 在评估过程中始终有意义, 给定条件: $j\neq any\ PeerID$ 时, $P_{ij}=0$, 在评估的过程中, 待评估的节点 j, 可能在节点 i 的 PeerService 表中并不存在, 这种情况出现在当节点 i 对节点 j 进行信任评估, 但是节点 i 之前并没有访问过节点 j 时, 这时设置 $P_{ij}=0$.

公式 (1) 中 $\frac{SuccessTimes}{AccessTimes}$ 表示访问节点 j 上某服务的访问成功率, $\frac{AccessTimes}{\sum_{PeerID=j}AccessTimes}$ 表示该项服务在节点 i 对节点 j 进行访问的所有服务中所占比例, 访问次数越多的服务越能反映提供服务节点的服务质量. 例如: 节点 i 访问节点 j 上的服务 1000 次, 如果其中 500 次都是访问服务 1, 只有 50 次是访问服务 2, 就认为节点 i 对节点 j 提供的服务 1 更了解, 在对节点 j 进行信任评估时, 服务 1 的访问情况所占的比例就应该更大.

采用权值 X 对访问成功率 $\frac{SuccessTimes}{AccessTimes}$ 进行校正, 因为 $\lambda>1$, 就使得用户对于待评估节点提供的服务中, 那些自身感兴趣服务的访问情况更加敏感, 更容易选择提供自己感兴趣服务质量高的节点. λ 由用户自己确定, 在兴趣明确情况下, 可设置 λ 值偏大, 这样节点对于兴趣更加敏感, 只考查自己感兴趣的服务. 反之在对选择的服务不明确的情况下 (例如: 进行统计, 查询 QoS 较好的节点时), 可将 λ 值设置与 1 接近. 这时节点选择的就是提供服务综合表现更优秀的节点.

在 (1) 中根据节点提供的所有服务, 得到节点的信任评估采用求和的方式, 也可以根据实际情况确定具体的选择原则, 例如: max(), average(), min() 等方式.

2.2　采纳周围节点的信任推荐

基于各自节点兴趣的信任评估, 每个节点根据自己的兴趣访问信任度高的节点上的服务. 但是当节点新加入对等网

时, 节点初始化调用 updatePeerService 服务, 节点本身没有访问过任何服务, 表 PeerService 和 AccessService 为空, 让节点选择一个自己满意的服务会让节点显得无所适从. 这时有几种处理方法[7,8], 一种方法是, 通过访问集合点, 由集合点来推荐访问节点. 但是这样在新节点比较多时, 会使集合点的访问量过大, 偏向于集中式的访问. 而且要求集合点的访问量比较大, 才能针对各种类型的服务评估请求, 给出满意的信任评估. 即使用户不是新节点, 在用户的 AccessService 表中数据很少的情况下, 节点根据(1), 由于访问历史有限, 也不能得到最优化的访问路径. 这时如果也访问集合点, 将会给集合点带来很大的负担. 另一种方法是, 接受其余节点信任推荐的方法, 向周围节点发起评估请求, 接收其它节点对待选择节点的信任评估. 与访问集合点获取信任评估的方式相比, 采纳其它节点的信任推荐显得更适合 P2P 的网络环境. 这里首先介绍采纳信任推荐的方法.

首先给出一个推荐信任度的定义: 结点 i 向其它节点发出对结点 j 进行信任评估的请求, 信任评估请求范围为 $\varnothing(i)$, 节点 k 为 $\varnothing(i)$ 内的节点则信任推荐 T_j 表示为:

$$T_j = \sum_{k\in\varnothing(i)} P_{kj} \qquad (2)$$

其中 P_{kj} 为结点 k 对节点 j 由(1)式得到的信任度. $\varnothing(i)$ 的确定, 这里采用节点 i 向相邻结点发起信任评估请求时, 请求信息中包含一项跳数(Hop)信息, 请求每经过一个节点, 跳数值减 1, 当跳数不为 0 时, 收到评估请求的节点将请求信息向它的相邻节点继续传播. 当跳数为 0 或节点已经收到该条评估请求时, 抛弃该条评估请求信息. 如图1所示, 节点0向

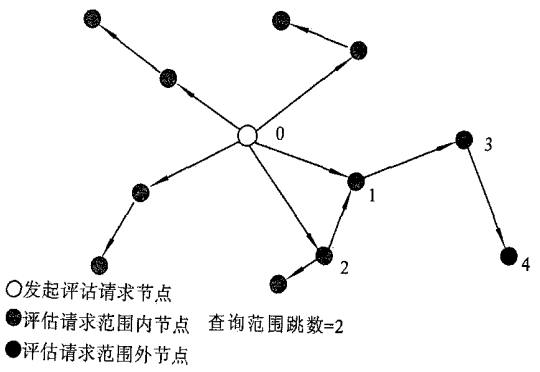

图 1 节点发起评估请求情况

周围节点发起跳数为 2 的评估请求, 节点 1 收到评估请求后将跳数减 1 继续向自己的相邻节点 3 传播, 节点 3 收到请求后将跳数减 1, 这时跳数为 0, 评估请求不会继续向 4 传播, 这样就设置了信任评估的范围. 当节点 2 收到节点 0 的评估请求后, 它也会把评估请求信息向节点 1 发送, 但是因为节点 1 已经收到过相同的评估请求, 就会把节点 2 传递的评估请求抛弃. 这样就抑制了冗余评估请求在网上的传播. 设置跳数的主要目的是为了控制对待测节点的信任推荐只在一个局部范围内进行, 减轻网络负担. 而且获得较远节点对待测节点的信任推荐, 对于自己决定节点的信任度也没有近距离节点的评估可靠.

继续考虑这样的问题, 是不是周围所有节点对待测节点的推荐都要平等对待呢? 答案应该是否定的, 很自然想到节点 k 对于节点 j 向节点 i 做的信任推荐应该与节点 k 本身在节点 i 的信任度相关, 下面对(2)式进行如下的改造

$$T_j = \sum_{k\in\varnothing(i)} P_{kj} \times (P_{ik} + \theta) \qquad (3)$$

在得到某个节点 k 关于待测节点的信任推荐时, 再与节点 i 对 k 的信任评估相乘, 这样自身信任度高的节点推荐的节点受到更大的重视, 这与社会关系中人际关系是相似的: 自己会更信任自己熟悉的朋友推荐给自己的陌生人, 而不信任自己不信任的人推荐给自己的陌生人. 周围有一些节点在没有被 i 访问时, 它们在节点 i 上的信任度 $P_{ik} = 0$, 增加 θ 是为了也可以利用这些节点的推荐信息. 当节点访问历史很少时, 周围很多节点的 $P_{ik} = 0$, 为了得到有效的信任评估需要借助其它节点的信任推荐, 这时可以把 θ 设置的大一些, 这样近似的将周围的节点公平对待不区分它们在本地节点上的信任度大小. 当节点拥有一些访问历史数据后, 可以把 θ 设置的小一些甚至 $\theta = 0$, 这样就使得 P_{ik} 占得比重更大, 信任度高的节点对待测节点的推荐受到更大的重视.

在(3)中采用求和的方式处理各个节点的信任推荐得到最终的推荐信任度, 也可以根据实际情况选择其它方式得到推荐信任度 T_j. 例如: 在为了保证最差环境下的服务质量可以按照 $T_j = \min_{k\in\varnothing(i)} (P_{kj} \times (P_{ik} + \theta))$ 得到推荐信任度, 当考虑最优情况下的服务质量可以按照 $T_j = \max_{k\in\varnothing(i)} (P_{kj} \times (P_{ik} + \theta))$ 获得推荐信任度. 也可以按照节点选择服务的原则选用其它的数学方法得到推荐信任度 T_j.

2.3 由自身信任评估和信任推荐得到综合信任评估结果

按照自身的访问兴趣由(1)得到节点自身对待测节点的信任评价 P_{ij}, 发布评估请求, 得到其它节点的评估应答, 再由(3)得到对待测节点的推荐信任评估 T_j. 下面的任务是如何将 T_j 和 P_{ij} 合并得到一个令人满意的综合信任结果. 这里采用线性综合的方法综合 T_j 和 P_{ij} 给出一个最终的综合评估结果 O_{ij}, 表达式如下:

$$O_{ij} = \alpha P_{ij} + (1-\alpha) T_j \qquad (0 \le \alpha \le 1) \qquad (4)$$

参数 α 是一个自定义常数, 在最终的综合评估结果中, 用户自己对待测节点的信任评价 P_{ij} 和得到的推荐信任评价 T_j 按照 α 各占一定的比例. 当用户更相信自己的信任评估结果 P_{ij} 时, 可以把 α 设置的相对大一些. $\alpha = 1$ 时, 不采纳其余节点的信任推荐, 节点只根据自己以往的访问结果进行信任评估. 节点 i 为新加入节点或者本身访问历史比较少时, 并不能根据自身的访问记录决定值得服务质量高的节点, 就需要把 α 值设置的小一些, 这时节点自身更依赖其余节点的推荐.

3 仿真实验和结果分析

3.1 实验环境及参数设置

在 JXTA 平台上已经将这种综合信任评估模型实现. 进行了一些仿真实验, 在仿真实验中, 对网络规模和提供服务进行一些限制. 设置实验规模包括 100 个节点, 提供服务是文件

下载服务, 每个节点提供两个文件下载服务. 仿真实验中一共有 10 个文件下载服务, 均匀分布在 100 个节点上, 每个下载服务包括两个描述关键字, 每个描述关键字会在两个下载服务中出现. 每个节点完成 100 次的随机服务访问, 积累访问记录. 在这 100 个节点中, 设置了 10 个节点每个节点提供一个无效服务, 10 个下载服务都有 1 个是无效的下载服务. 假设这 100 个节点都是在一个信任评估推荐范围内, 当节点发起信任评估请求时所有节点都会对评估请求响应.

在实验环境中, 如果所有节点提供的信任推荐都是真实的, 并且忽略网络传输和节点提供服务的能力. 每个节点至多在最初 PeerService 和 AccessService 表为空的情况下有 5% 的可能访问服务失败, 在这之后根据自己的访问历史和周围节点的推荐结果就可以成功访问服务. 因此可以认为理想情况下节点关于某个服务的访问成功率的数学期望是 E= 0.05×0.90+ 0.95×1= 0.995. 但是在实际的 P2P 网络环境下理想的情况是很难得到满足的, 下面设计一些具体实验环境, 进行实验并对实验结果进行分析. 因为综合信任评估模型中对节点信任推荐的采纳程度与推荐节点在评估请求节点处的信任度相关, 因此有必要区分提供虚假推荐的节点是否就是提供虚假服务节点进行考虑, 这里我们把只提供虚假推荐, 但是节点自身提供的服务是真实的情况下进行的实验称为Ⅰ类实验, 而把既提供虚假推荐, 节点自身提供的服务也是无效的情况下进行的实验称为Ⅱ类实验.

3.2　Ⅰ类实验结果及分析

在实际情况中, 我们不可能保证 P2P 网络中所有节点提供的信任推荐都是真实的, 下面设计这样的实验条件: 假设 100 个节点中有一部分节点恶意的向服务请求节点提供虚假的信任推荐. 我们设定, 所有恶意节点对于请求节点的恶意推荐都是基于请求节点感兴趣的服务进行的. 在这里我们设定(1)中的 λ= 2. 下面按照 α 的值和恶意节点的数量分别进行实验.

表 3　α= 0 实验结果

恶意节点数目	10	20	30	40	50
访问成功率	0.99	0.92	0.82	0.65	-

实验中分别设定(3)中的 α= 0, 0.5, 1, 分别表示节点完全依赖其余节点的推荐, 综合考虑自己得到的信任评估和推荐信任评估, 以及完全相信自己的信任评估三种情况. 让节点访问某特定服务 100 次, 记录成功访问次数, 得到实验数据如表 3、表 4 和表 5 所示.

表 4　α= 0.5 实验结果

恶意节点数目	10	20	30	40	50
访问成功率	0.99	0.95	0.90	0.83	0.75

表 5　α= 1 实验结果

恶意节点数目	10	20	30	40	50
访问成功率	0.99	0.98	0.99	0.97	0.98

从实验数据可以发现, 网络中存在恶意节点向访问节点提供虚假推荐的情况下, 节点自身采用不同的 α 值使得访问结果有很大不同. α= 0 时, 恶意节点在推荐请求范围内所占比例不大(小于 30%)的情况下, 访问成功率还是可以令人满意的, 但是当 P2P 网络中存在大量虚假推荐(大于 40%)时, 访问成功率就很低甚至无法进行访问. α= 0.5 时, 随着恶意节点的增加, 访问成功率会有所下降, 但是相比 α= 0 节点已经明显对于虚假的信任推荐有一定的抵御能力, 不会由于恶意节点的恶意推荐使得访问无法进行. 最后看 α= 1 的情况, 访问成功率与恶意节点的数目没有直接的联系.

从上面的实验中可以得出这样的结论: α= 0 完全信赖周围节点的推荐评估, 这种情况下节点完全依赖于 P2P 网络中其它节点的信任推荐, 由于 P2P 网络本身不可能保证所有的节点提供的信息都真实准确, 因此当网络中的虚假推荐很多时, 节点访问网络中的资源十分困难. 因此 α= 0 只适用于节点新加入对等组的情况, 这时需要依赖其余节点的推荐来判断待测节点的可信度. α= 1 表示节点完全依靠自身访问历史结果来判断待测节点的可信度, 这时综合信任模型退化为根据节点自身访问兴趣进行可信度判断的信任模型, 这适用于 P2P 网络中的恶意推荐很多的情况. 这种情况下节点完全屏蔽了外界节点的推荐, 但是这样也不能接收正确的推荐. α= 0.5 是一种适中的选择, 是综合信任模型评估原则的体现, 既考虑了节点自身的访问历史结果, 也兼顾了其他节点的信任推荐. 从上述实验数据中可以看到, 在 P2P 网络中恶意节点所占比例不是很大的情况下(小于 40%)可以获得满意的访问成功率(大于 80%)的. 从实验数据可以得出结论: 在实际的 P2P 网络环境中根据网络的状况和节点自身的情况选择合适的 α 值是获得满意访问成功率的关键. 采用线形综合自身信任评估结果 P_{ij} 和信任推荐 T_j 的方法得到综合信任评估结果, 即可以考虑自身访问历史又有效的利用了网络中节点的信任推荐, 可以获得一个满意的访问成功率.

3.3　Ⅱ类实验结果及分析

实际的 P2P 网络中, 往往更多的情况是提供虚假服务的节点也向信任评估请求节点发送恶意的信任推荐. 我们对这种情况设计实验, 并给出实验结果和分析.

表 6　α= 0 实验结果

访问次数	10	20	40	100
成功次数	7	14	30	82
失败次数	3	6	10	18

设定实验环境中有 40 个节点提供的服务都是无效的, 而且这些节点本身向访问节点进行的信任推荐也是虚假的. 每个文件下载服务的无效率都是 40%, 均匀分布在 40 个无效节点上, 同样设定(1)中的 λ= 2, 分别针对 α= 0, 0.5, 1 三种情况, 让所有节点对网络中的所有服务进行随机访问(模拟实际网络环境, 发现所有提供虚假服务的节点), 对某个节点针对某个服务的访问情况按照访问次数进行统计, 实验结果如表 6、表 7 和表 8 所示.

从实验结果可以发现, 当 α= 0 时, 随着访问次数的增加, 失败的访问次数基本按照线性递增, 但是在 100 次的访问成

功率上比Ⅰ类实验还是有很大提高(Ⅰ类实验为 65%, Ⅱ类实验为 82%), 当 α= 0.5 时, 随着访问次数的增加, 失败的访

表 7 α= 0.5 实验结果

访问次数	10	20	40	100
成功次数	7	16	34	94
失败次数	3	4	6	6

问次数逐渐趋向于稳定, 而且最终实验结果也有提高(Ⅰ类实验为 83%, Ⅱ类实验为 94%), α= 1 时, 实验结果与Ⅰ类实验基本相同. 由这个实验可以得到这样的结论: 综合信任模型在信任推荐的采纳中参照了推荐节点自身的信任度, 这样随着网络中访问量的增加, 恶意节点自身信任度在整个网络中降

表 8 α= 1 实验结果

访问次数	10	20	40	100
成功次数	8	17	36	96
失败次数	2	3	4	4

低, 可以有效的抑制 P2P 网络中提供虚假服务节点的恶意推荐, 当 α 设置合适时可以使节点获得满意的访问成功率.

3.4 兴趣选择实验结果及分析

综合信任评估模型按照节点自身的访问兴趣对要访问的节点进行信任评估, 引入节点兴趣有两个主要目的: 一是节点根据自身兴趣发现提供服务最优化的节点, 另外就是使得对等网中的节点提供的服务分工更加明确, 提供的服务更加专业. 下面设计一个兴趣选择实验, 并进行说明.

设置两个节点 A、B, 它们都提供两个下载服务, 节点 A 提供的两个下载服务 service1 和 service2 描述关键字不同, 分别为 key1、key2. 节点 B 提供的两个下载服务 service1 和 service3 描述关键字相同, 都为 key1. 让 100 个节点对 service1, service2 和 service3 进行随机的访问, 实验发现在对相同的 service1 进行的 127 次访问中, 其中有 98 次都是去向节点 B 访问 service1. 由于综合信任评估模型采用基于兴趣的信任评估, 这样当节点访问关键字为 key1 的服务 service1 时, 由于节点 B 提供另外的服务 service3 与 service1 类似(拥有相同的描述关键字), 按照(1)式由于 λ> 1 节点 B 得到的信任评估会比 A 更高. 这样基于兴趣的信任度评估使得在 P2P 网络中, 服务更加倾向于按照服务类型聚集, 使得节点提供更专业化的服务. 例如: 两个站点一个主要提供计算机类书籍下载, 另一个主要提供英语类书籍下载. 由于两个节点自身内部提供的服务具有相似性, 用户希望下载计算机类书籍时, 前者得到的信任评估会更高用户会优先访问前者. 这样节点提供专业化的服务就更容易被访问, 使得 P2P 网络中节点分工更加明确, 服务质量更好.

4 结论及展望

综合信任评估模型是综合节点自身兴趣和其余节点信任推荐得到的一种 P2P 环境下的信任评估模型. 综合信任评估模型采用完全分布式的信任评估方式, 并可以灵活地根据网络环境和周围节点情况设定模型参数, 通过实验显示这种评估模型在 P2P 的环境下有很大的实用价值.

在下一步的工作中, 可以基于综合信任评估模型对 P2P 网络做更进一步的研究. 例如: 如何将目前已经成熟的鉴权机制与 P2P 环境相结合提供对等组内的成员鉴权服务; 如何在综合信任评估模型中引入惩罚机制对恶意节点进行惩罚, 而不影响周围节点中正确的信任推荐; 将本体论和人工智能引入综合信任评估模型的服务发现过程中可以使得节点能够通过自身学习发现自身感兴趣的服务.

References:

[1] Gemano Caronni. Walking the Web of trust[C]. In: Proc. of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. IEEE Press, March 2000, 153-159.

[2] 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.

[3] Fabrizo. Cornelli, Ernesto Damiani, Sabrina De Capitani di Vimercati, etc. Choosing reputable servents in a P2P network [C]. In: Proc. of the 11th International World Wide Web Conference. Hawaii: ACM Press, May 2002, 376-386.

[4] Alfarez Abdul-Rahman, Sterhen Hailes. A distributed trust model[C]. In: Proc. of the 1997 New Security Paradigms Workshop. ACM, September 1997, 48-60.

[5] Matt Blaze, Joan Feigenbaum, John Ioannidis, et al. The role of trust management in distributed systems security[Z]. In: Secure Internet Programming: Issues in Distributed and Mobile Object Systems, volume 1603 of Lecture Notes in Computer Science, July 1999, 183-210.

[6] Rita Chen, William Yeager. Poblano: a distributed trust model for P2P networks[R]. Technical Report, TR-I4-02-08, Palo Alto: Sun Microsystem, 2002.

[7] Mao Chen, Jaswinder Pal Singh. Computing and using reputations for internet ratings[C]. In: Proc. of the third ACM Conference on Electronic Commerce, New York, NY, USA, October 2001, 154-162.

[8] Loren Terveen, Will Hill, Brien Amento, et al. PHOAKS: a system for sharing recommendations[J]. Communications of ACM, March 1997, 40(3): 59-62.