ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.2, February 2007, pp.400−411
DOI: 10.1360/jos180400

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种有效的 Peer-to-Peer 自适应拓扑进化协议*

张 骞+, 张 霞, 刘积仁

(计算机软件国家工程研究中心(东北大学),辽宁 沈阳 110179)

An Efficient Adaptive Evolvement Protocol for Peer-to-Peer Topologies

ZHANG Qian+, ZHANG Xia, LIU Ji-Ren

(National Engineering Research Center for Computer Software (Northeastern University), Shenyang 110179, China)

+ Corresponding author: E-mail:lillyjill@tom.com, http://www.neu.edu.cn

Zhang Q, Zhang X, Liu JR. An efficient adaptive evolvement protocol for peer-to-peer topologies. *Journal of Software*, 2007,18(2):400−411. http://www.jos.org.cn/1000-9825/18/400.htm

Abstract: Current unstructured peer-to-peer (P2P) systems lack fair topology structures, and take no consideration for vicious action of peers. The mainly reason is that the topologies are not sensitive to peer's trust, and take no consideration for the trust computation of different domains. First, a domain-based P2P trust model is presented in this paper. Then, based on the trust model, a peer-level protocol for forming adaptive topologies for unstructured P2P networks is proposed. The protocol aims at the topologies evolution of embodied domains, and makes good peers locate good position and bad peers locate bad position in the corresponding domains, which guarantees the impartiality of topology. On the other hand, the protocol can restrain the vicious action of peers effectively, and also has the incentive capacity, which encourages peers to provide more authentic services in order to get more return on services. Analysis and simulations show that, compared with the current topologies, the resulting topologies are more efficient and more robust on security problems.

Key words: peer-to-peer network; adaptive topology; domain model; domain trust

摘 要: 现有的无结构 Peer-to-Peer(P2P)系统缺乏对拓扑公平性的考虑,并且不能对某些节点的恶意行为进行有效的抑制.其主要原因在于构造的拓扑对节点可信度的不敏感性,忽略了节点在不同领域中可信度的区别.据此,首先给出了基于领域的P2P信任模型的定义,然后在此基础上提出了一种针对无结构化P2P网络的自适应拓扑进化协议.该协议可以针对具体的领域进行拓扑进化,使得领域内的高可信节点占据相应领域拓扑的有利位置,低可信节点处于不利位置,从而体现拓扑的公平性.该协议同时能够对节点的恶意行为进行有效的抑制,并具有激励性质,鼓励节点提供更好的服务,以获得更高的回报率.分析和仿真结果表明,该协议较之现有协议,在拓扑的有效性和安全性等方面有较大的提高.

关键词: 对等网络;自适应拓扑;领域模型;领域可信度
中图法分类号: TP393 文献标识码: A

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2002AA4Z3120 (国家高技术研究发展计划(863))

Received 2005-11-17; Accepted 2006-02-23

虽然有关 Peer-to-Peer(简称 P2P)的应用日益广泛[1],但仍然缺乏有效的 P2P 拓扑构造机制来保证网络的良性发展[2].在无结构 P2P 网络中,Peer 节点之间的随意连接通常难以保证系统的安全性和有效性.一种可能的替代方法是采用结构化的 P2P 网络,并使用分布式哈希表(distributed hash table,简称 DHT)来放置和定位内容,使得基于关键词的查询可以在确定的复杂度内完成.然而,这种模式难以完全支持复杂的查询[3].因此,对无结构 P2P 网络中的拓扑构造机制进行研究是十分有意义的.

拓扑构造机制必须考虑节点的异构性.虽然异构性表现在诸多方面,但从很大程度上都可以归结于节点在可信度上的异构[2].因此,良好的可信度度量是 P2P 拓扑构造的基础.有研究表明[4],不同节点有着不同的偏好领域,节点在不同领域有着不同的可信度.虽然目前已经存在一些基于可信度的 P2P 拓扑构造方法[2,5],然而,这些方法所基于的可信度度量的粒度一般过于粗糙[6],不能针对具体领域计算节点的可信度,因而决定了其拓扑的粗糙性.粗糙性的表现之一就是某领域内的高可信节点通常因为其整体的可信度较低而处于拓扑中的不利位置,因而缺乏对拓扑公平性的考虑,不利于提高系统的整体服务质量.另外,现有的拓扑构造方法通常不能对节点的某些恶意行为进行有效的抑制,并缺乏对激励机制的考虑.

针对上述问题,本文首先给出了领域可信度(domain trust)的定义,领域可信度可以针对具体的领域度量节点的可信度.然后,在此基础上提出了一种自适应的 P2P 拓扑构造协议 MGP(multiple-granularity protocol).MGP 协议简单而有效,可以针对具体的领域对拓扑进行调整,并使得在任何一个领域拓扑内,该领域中的高可信节点都占据该领域拓扑的有利位置.这样造成的一种情况是,节点在某领域内处于拓扑的有利位置,然而在另一领域内却可能处于拓扑的不利位置.另外,MGP 协议还能对网络中存在的某些恶意行为进行有效的抑制,并具有激励性质.分析及仿真实验表明,MGP 协议较之现有拓扑构造协议,在有效性和安全性等方面有较大的提高.

1 相关工作

目前存在若干无结构 Peer-to-Peer 环境下的拓扑构造方法.文献[7]提出了一种拓扑调整方法,初始时,节点随意进行连接,每个节点跟踪其邻居节点的负载变化,负载过重时断开连接并选择性能(capacity)较高的其他节点重新连接.然而,该方法并没有对节点的性能进行很好的度量,并且没有考虑 P2P 网络中存在的 free-rider 问题[8],即在目前大多数 P2P 文件共享应用中,绝大多数的用户不共享任何文件,整个网络的运作依赖于少量用户的利他行为[2].另外,该方法也不能对 P2P 网络中存在的恶意行为进行有效的抑制,比如,某些恶意节点若被选作下载源,则上传虚假的文件企图欺骗其他节点.类似的拓扑调整方法也可见于文献[9,10].

文献[11]提出了一种面向内容的拓扑构造方法.在该方法中,被转发的搜索消息中包含已访问节点的内容信息,查询发起节点从返回的搜索消息中获得与其内容相似度最大的节点,并与该节点建立直接内部(internal)连接.同样,从搜索消息中获得与其相似度最小的节点,与该节点建立直接外部(external)连接.外部连接指向内容差异较大的节点,而内部连接指向内容相近的节点.该方法同样没有考虑节点的恶意行为.另外,在仿真实验中也没有考虑节点的动态特性.文献[12]的方法与文献[11]类似.在文献[3]的方法中,每个节点依据历史交易记录对邻居节点进行评分,并依据该评分分配其查询处理能力,即评分高的邻居节点,其发出的查询被处理的可能性也大.该方法没有涉及到节点间连接的添加和断开,并且没有考虑节点的恶意行为.

另外,目前还存在着基于聚类(cluster)的 P2P 拓扑构造方法.这类方法通常事先将网络划分为几个可能的领域,依据新加入节点自身提供的信息(通常是共享的文档),对这类信息应用一定的聚类方法,根据聚类的结果将节点划分到相关领域中.比如,文献[13]中的方法首先采用文档归类器对节点共享的文档进行归类,然后采用节点归类器将节点关联到相关领域.类似的方法还可见于文献[14,15]等.这类算法的主要缺陷在于:拓扑领域的划分严重依赖于文档的归类结果,而且基于文档的划分也使得这类方法不能很好地应用于诸如即时通信等应用中,因为在这类应用中节点通常不共享文档.另外,这类算法通常还需要设定全局性的领域划分模式,并且很少考虑 P2P 网络中存在的恶意行为,比如共享虚假的文档信息.

在混合(hybrid)P2P 环境中,目录节点(directory node)及其叶节点(leaf node)通常形成一个自治的领域,新加入的叶节点依据一定的策略(比如根据共享的文档类别)加入相关领域;而目录节点之间也通常采用上述基于聚

类的方法构造更大的自治领域.文献[16,17]是这类拓扑构造方法的代表.值得一提的是,文献[18]也将 P2P 网络基于领域划分为几个自治社区(community),每个社区有创建者(实际上类似于混合 P2P 中的目录节点)负责维护,节点加入相关社区需要区内成员的引荐,并且有创建者运行协同推荐算法评价区内成员的可信度,淘汰掉低可信节点.类似的算法也可见于文献[19,20].因为 MGP 方法应用的对象是无结构 P2P 拓扑,限于篇幅,这里不再与混合 P2P 环境下的拓扑构造方法进行详细的比较讨论.

在基于可信度的拓扑进化方法中,文献[2]提出了一种基于全局可信度的拓扑进化方法.该方法的主要缺陷是,全局可信度的存储及更新需要节点之间的协同才能完成,同时将导致较高的通信代价.据我们所知,文献[5]中的基于局部可信度的拓扑进化方法是目前已知的唯一与 MGP 类似的方法.为了便于描述,我们将文献[5]中的方法记为 SGP(single-grain protocol).MGP 方法实际上是对 SGP 方法的改进,因此,这里进行较为详细的讨论.SGP 采用了文献[21]中的可信度计算方法,节点 i 对节点 j 的局部可信度 $S_{i,j}$ 定义为

$$S_{i,j}=sat(i,j)-unsat(i,j) \tag{1}$$

其中,$sat(i,j)$和 $unsat(i,j)$分别表示从节点 i 的角度看,i 与 j 交易成功和失败的次数.每次交易完成之后,节点计算与其交易节点的可信度,并与其邻居节点的可信度进行比较,从而判定是否用当前交易节点取代可信度较低的邻居节点,并发起与交易节点的连接请求.收到连接请求的节点同样会依据其邻居节点的可信度来决定是否接受该连接.MGP 与 SGP 的相似之处在于,两者都是基于局部可信度进行的拓扑调整,不同之处有以下几点:

(1) SGP 所基于的可信度度量方法粒度过于粗糙,不能针对具体的领域计算节点的可信度,因而决定了其拓扑的粗糙性.而 MGP 所基于的可信度计算方法可以针对具体领域度量节点的可信度,因而其拓扑调整的粒度是基于领域的(见第 2 节和第 3 节).

(2) SGP 在进行拓扑调整时,仅考虑到了当前与之交易的节点与邻居节点的可信度比较;而在 MGP 中,不仅考虑到了当前交易节点,同时也考虑到了历史上与之交易的节点,即从全部交易节点中选出可信度最高的节点与邻居节点进行比较.因为新一轮的交易可能使邻居节点的可信度降低,同时,当前交易节点的可信度又不够高,因此,历史上有过交易的节点可能成为此时的最佳选择(见第 3 节).

(3) MGP 不仅可以基于领域进行拓扑进化,而且使得领域内的高可信节点占据该领域拓扑中的有利位置,低可信节点处于该领域拓扑中的不利位置.SGP 协议却无法取得同样的拓扑进化效果(见第 4.5 节和第 4.6 节).

实际上,MGP 协议同时也是一种激励机制,鼓励节点提供更好的服务,从而占据偏好领域拓扑中的有利位置,获得更高的服务回报率(见第 4.4 节).

(4) MGP 可以有效地对节点的某些恶意行为进行有效的抑制,而 SGP 协议因为忽略了可信度在不同领域中的区别,因此不能有效地对节点的恶意行为进行抑制(见第 4.2 节和第 4.3 节).

本文最后对 MGP 和 SGP 方法进行了对比测试,结果表明,MGP 较之 SGP 方法,在拓扑的有效性和安全性等方面有较大的提高.

2 模型的定义和表示

首先给出 P2P 网络模型的定义.

定义 **1**(**P2P** 网络). P2P 网络可以表示为无向图 $G=(V,E)$,其中:V 是节点集,对应网络中的 Peer 节点;E 是边集,表示 Peer 节点间的连接.任意节点 $u\in V,v\in V$,若$(u,v)\in E$,则必有$(v,u)\in E$.对于任意 $u\in V$,其邻居集记为 $N_u=\{v|(u,v)\in E\}$[5].

有研究表明[4,6],网络中每个 Peer 节点都有其偏好的领域,并且在不同领域具有不同的可信度,相关领域的可信度相互影响.因此,这里首先给出领域模型的定义,然后在此基础上给出领域可信度的定义.

定义 **2**(领域模型). 领域模型定义为一个加权图 $DM=(I,O,RO)$,I 是 DM 所在 Peer 节点在全局范围内的唯一标识,O 是描述节点偏好领域的本体有限集[22].$RO\subseteq O\times O\times N$($N$ 为自然数集合)构成图的加权边,表示图中各领域本体的相似度[23].相似度是[0,1]中的值,并记任意本体 x,y 的相似度为$\lambda_{x,y}$.

图 1 描述了一个领域模型的例子.该模型有 4 个本体,分别代表 music,math,computer 和 physics 这 4 个领域.

本体间连接的权重表示相关领域的相似程度,如 math 和 computer 的相似度为 0.45.为了便于描述,我们将节点 i 的偏好领域集记为 $DM_i.C.DM_i.C_m$ 表示 i 的第 m 个偏好领域.

值得一提的是,可以采用文献[6]中的聚类和查询扩展的算法来挖掘节点的偏好领域,并能对节点的偏好领域集进行动态更新.限于篇幅,这里不再详述,可参见文献[6].

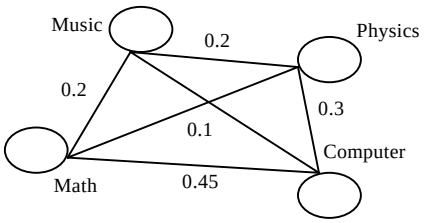

Fig.1 Domain model of peer node

图 1 Peer 节点的领域模型

定义 **3**(领域信任度). Peer 节点 u 对 v 在领域 k 内的可信度记为 $T_{u,v,k}$.该可信度来源于 u 与 v 在领域 k 及其相关领域交往的历史.

$$T_{u,v,k}=\beta\times(S_{u,v,k}-F_{u,v,k})+(1-\beta)\times\sum_{m=1}^{N_{u,k,\sigma}}\left(\frac{\lambda_{m,k}}{N_{u,k,\sigma}}\times(S_{u,v,m}-F_{u,v,m})\right) \tag{2}$$

记节点 u 的领域模型为 DM_u,u 的领域集为 $DM_u.C$,则 $N_{u,k,\sigma}=|\{m|m\in DM_u.C,\lambda_{m,k}\geq\sigma,m\neq k\}|$,其中:$\sigma$为相似度阈值;$\lambda_{m,k}$为领域 m 与 k 的相似度,即 $N_{u,k,\sigma}$为 u 的领域集中与 k 的相似度不小于σ的领域数目.$S_{u,v,k}$和 $F_{u,v,k}$分别代表 u 与 v 在 k 领域交易成功和失败的次数;m 表示 k 的相关领域,如图 1 中 *computer* 领域,在σ=0.4 的情况下,其相关领域为 *math*;β为权重因子,若节点 u 与 v 在领域 k 内的交易量很大,则β可以在(0.5,1)区间内取值;若领域 k 内的交易量很小,但在相关领域内的交易量很大,则可以通过相关领域的交易来估计 v 在领域 k 内的可信度.因为领域 k 内较小的交易量不足以反映节点的可信度,故此时β可以在(0,0.5)区间内取值;若领域 k 及其相关领域的交易量都很大,则可取β=0.5.综上,可设定$\beta=\dfrac{P_{u,v,k}}{P_{u,v,k}+P_{u,v,\sigma}}$,其中,$P_{u,v,k}$和 $P_{u,k,\sigma}$分别为 u 和 v 在 k 领域和其相关领域的交易量.

与文献[5]不同,上述定义可以针对某一具体领域对可信度进行量化,并且考虑了相关领域可信度间的相互影响,这正如数据库领域可信度的变化必然影响到计算机领域可信度的改变一样.文献[5]采用的可信度量化标准过于粗糙,只能从整体上衡量节点的可信度,因而决定了其拓扑的粗糙性.

另外,由定义 1 易知,影响 P2P 拓扑构造的另一个重要因素就是节点之间的连接性.由于人为的设置,或者是计算能力、网络带宽等资源的限制,Peer 节点通常只能连接到有限数目的其他节点.不妨设任意节点 u 所允许的最大连接数为 C_u,其中 u 的偏好领域集为 $DM_u.C$,则有,

$$C_u=\sum_{k=1}^{|DM_u.C|}C_{u,k} \tag{3}$$

其中,$C_{u,k}$表示节点 u 贡献给领域 k 的连接数.

3 MGP 协议

首先给出协议的几个原语及其语义.

Disconnection_request(u,v,k):节点 u 断开与 v 在 k 领域的连接,并向 v 发送断开消息;v 接收到该消息后,将 u 从其 k 领域邻居列表中删除.

Get_domain(u,D_u):获取节点 u 的全部偏好领域列表,并保存到 D_u 中.

Get_domain(u,$D_{u,k}$,k,σ):节点 u 获取领域 k 的相关领域列表,并保存到 $D_{u,k}$ 中.其中,σ为领域相似度阈值,即 $D_{u,k}=\{m|m\in DM_u.C,\lambda_{m,k}\geq\sigma,m\neq k\}$,$\lambda_{m,k}$为领域 m 与 k 的相似度.

Get_neighbor(u,$N_{u,k}$,k):获取节点 u 在领域 k 内的邻居列表,并保存到 $N_{u,k}$ 中.

Get_tranction(u,PR_u):节点 u 从本地缓存中获取与之交易的节点,并保存到 PR_u 中.

Add_neighbor(u,v,k):节点 u 将 v 添加为其 k 领域的新邻居,更新邻居列表.

在自适应拓扑协议中,Peer 节点扮演连接请求发起者和连接请求处理者两种角色.作为连接请求发起者,在每次交易(或多次交易)完成之后,节点需要更新本地邻居列表,向高可信节点发出连接请求;节点同时作为连接

请求处理者,处理其他节点发送的连接请求,并根据处理结果决定是否更新本地邻居列表.

任意节点 u 作为连接请求发起者的算法如下:

***Connect_sender*(*u*)** //交易完成后,节点 u 调整本地邻居列表,并向高可信节点发出连接请求

{

1. *Get_domain*(u,D_u)
2. *Get_tranction*(u,PR_u)
3. **For** each $k\in D_u$ **do**
4. *Get_neighbor*(u,$N_{u,k}$,k)
5. *Get_domain*(u,$D_{u,k}$,k,σ)
6. j=1 //j 为步骤 7 的循环控制变量,其目的在于循环处理多个不满足情况的连接
7. **For** j==1 **do** //循环判定是否存在可替换的邻居节点
8. j=0 //首先假定已经不存在可替换的邻居节点
9. $T_{u,v,k}=\min\{T_{u,v,k}|T_{u,v,k}=f(u,v,k),\ v\in N_{u,k}\}$
   //从 k 领域的邻居列表中获得该领域内可信度最小的节点,$f(u,v,k)$等同于式(2)
10. **If** $(PR_u-N_{u,k})\neq$Null **then**
11. $T_{u,j,k}=\max\{T_{u,j,k}|T_{u,j,k}=f(u,j,k),\ j\in PR_u-N_{u,k}\}$ //从在 k 领域未连接的交易节点中选出 k 领域可信度最大的节点.若 $T_{u,j,k}$=0,则 u 在 k 领域的当前邻居不变,即在 k 领域不作任何调整
12. **If** $C'_{u,k}<C_{u,k}$ **And** $T_{u,j,k}>0$ **And** *Connect_receiver*(u,j,k)=True **then**
    //节点 u 请求与 j 建立 k 领域的连接,若 j 同意连接,则 *Connect_receiver*(u,j,k)返回 True;否则为 False.
    $C'_{u,k}$ 为 u 在 k 领域的当前连接数,$C_{u,k}$ 表示节点 u 贡献给领域 k 的连接数
13. *Add_neighbor*(u,j,k) //u 将 j 添加为其 k 领域的新邻居
14. j=1 //可能还存在可添加的新邻居,故循环执行步骤 7
15. **Elseif** $C'_{u,k}=C_{u,k}$ **And** $T_{u,j,k}>T_{u,v,k}$ **And** *Connect_receiver*(u,j,k)=True **then**
16. *Add_neighbor*(u,j,k)
17. *Disconnection_request*(u,v,k)
18. j=1 //可能还存在可替换的邻居节点,故循环执行步骤 7

End if //与步骤 12 对应

End if //与步骤 15 对应

End For //与步骤 7 对应

End For //与步骤 3 对应

}

任意节点 j 作为连接请求处理者的算法如下:

***Connect_receiver*(*u*,*j*,*k*)** //j 处理 u 在 k 领域的连接请求

{

1. $T_{j,u,k}=f(j,u,k)$ //获得 u 在 k 领域的可信度
2. *Get_neighbor*(j,$N_{j,k}$,k)
3. $T_{j,u,k}=\min\{T_{j,v,k}|T_{j,v,k}=f(j,v,k),v\in N_{j,k}\}$
4. **If** $T_{j,u,k}<0$ **then**
   Return False
5. **Elseif** $C'_{j,k}<C_{j,k}$ **And** $T_{j,u,k}>0$ **then** // $C'_{j,k}$ 为 j 在 k 领域的当前连接数
6. *Add_neighbor*(j,u,k)
   Return True

7. **Elseif** $C'_{j,k}=C_{j,k}$ and $T_{j,u,k}>T_{j,v,k}$ **then**
8. *Add_neighbor*(*j*,*u*,*k*) //节点 *j* 将 *u* 添加为其 *k* 领域的新邻居
9. *Disconnection_request*(*j*,*v*,*k*) //节点 *j* 断开与 *v* 在 *k* 领域的连接
   Return True
10. **Else**
    Return False
    End if

}

由上述算法可以看出:在交易完成之后,任意节点 *u* 通过原语 *Get_domain*(*u*,D_u)获得其偏好领域集 D_u,通过原语 Get_tranction(*u*,PR_u)获得与之交易的节点集 PR_u;然后针对每一个偏好领域 *k*,从 PR_u 中选出该领域内可信度最高的节点,记为 *j*,若节点 *u* 在领域 *k* 的当前连接数未满且 $T_{u,j,k}>0$,同时在节点 *j* 同意与 *u* 在 *k* 领域建立连接的情况下,则 *u* 与 *j* 在领域 *k* 内建立直接连接;若当前连接数已满,则将 $T_{u,j,k}$ 与邻居节点在领域 *k* 内的可信度相比较,以判定是否替换可信度最低的邻居节点.

任意节点 *j* 在收到其他节点 *u* 在领域 *k* 内的连接请求时,计算节点 *u* 在领域 *k* 内的可信度 $T_{j,u,k}$.若 *j* 在领域 *k* 内的连接数未满,且 $T_{j,u,k}>0$,或者连接数已满,但存在 *j* 在 *k* 领域的邻居节点 *v*,使得 $T_{j,u,k}>T_{j,v,k}$,则接受该连接请求,否则拒绝该请求.

为了完成以上操作,任意节点 *u* 需要维护两个表,分别是历史记录列表(如图 2(a)所示)和邻居节点列表(如图 2(b)所示).

$DM_u.C_1$		
$ID_{i1,1}$	$S_{u,i1,1}$	$F_{u,i1,1}$
$ID_{i2,1}$	$S_{u,i2,1}$	$F_{u,i2,1}$
…	…	…
$ID_{ih,1}$	$S_{u,ih,1}$	$F_{u,ih,1}$
$DM_u.C_2$		
…		
$DM_u.C_m$		
$ID_{j1,m}$	$S_{u,j1,m}$	$F_{u,j1,m}$
…	…	…
$ID_{js,m}$	$S_{u,js,m}$	$F_{u,js,m}$

(a)

$DM_u.C_1$
$N\_ID_{i1,1}$
$N\_ID_{i2,1}$
…
$N\_ID_{ip,1}$
$DM_u.C_2$
…
$DM_u.C_m$
$N\_ID_{j1,m}$
…
$N\_ID_{jq,m}$

(b)

Fig.2 The data structure of peer *u*

图 2 Peer *u* 的数据结构

其中:$DM_u.C_1,\ldots,DM_u.C_m$ 表示节点 *u* 的各个偏好领域;$ID_{i1,1},ID_{i2,1},\ldots,ID_{js,m}$ 表示与 *u* 有过交易的节点标识,如 $ID_{js,m}$ 表示与 *u* 在 $DM_u.C_m$ 领域有过交易的节点标识;$N\_ID_{i1,1},N\_ID_{i2,1},\ldots,N\_ID_{jq,m}$ 表示 *u* 的邻居节点标识,如 $N\_ID_{jq,m}$ 表示 *u* 在 $DM_u.C_m$ 领域的邻居节点标识;$S_{u,i1,1},S_{u,i2,1},\ldots,S_{u,js,m}$ 和 $F_{u,i1,1},F_{u,i2,1},\ldots,F_{u,js,m}$ 分别表示与 *u* 在相应领域交易成功和失败的次数.

由 MGP 拓扑进化算法易知,假定节点的平均偏好领域数目和平均最大连接数分别为 *m* 和 *k*,则在最坏情况下,该算法维护网络拓扑的通信开销为 $O(m\times k\times(2+1))=O(m\times k)$.由于节点的偏好领域和连接数有限,因此,拓扑维护的通信开销不大;根据节点所维护的数据结构,且假定节点标识及交易成功和失败次数均为浮点型,占 8 个字节,则易得其存储开销为 $O(m\times P\times 3\times 8)+O(m\times k\times 8)\approx O(m\times k)+O(m\times P)$,其中,*P* 为节点存储的历史交易条目数.节点可设定 *P* 的上限,在交易条目数超过该上限时,依次删除低可信节点的交易记录,直至达到存储要求.

从以上分析可以看出,MGP 协议的优势主要体现在以下几个方面:

(1) MGP 协议是自适应的,每个节点仅依据自身的交易记录进行决策,因而减少了对全局性知识的依赖,从而保证系统具有良好的扩展性.

(2) 基于节点的领域可信度,可以将节点划分为多个可能的领域.有研究表明[4],相同偏好领域的节点更容易达成成功的交易.与 SGP 协议进行的对比测试表明,MGP 协议使得在具体的领域拓扑中,领域可信度高的节

点呈现出更好的聚集特性(见实验 5).

(3) MGP 协议可以使得初始随意连接的拓扑朝向具有良好公平性的拓扑进化.公平性体现在:基于领域可信度,节点通过自适应调整属于多个领域拓扑,并在不同领域拓扑中有着不同的拓扑位置.领域可信度高的节点在相应领域拓扑中处于有利位置,并呈现聚集特性,而领域可信度低的节点在相应领域拓扑中被排斥到网络边缘.良好公平性的拓扑可以提高系统整体的服务质量.与 SGP 协议相比,MGP 协议可以显著提高系统整体的服务质量(见实验 4).实际上,MGP 协议取得了与在各个域中独自运行 SGP 协议类似的效果,但现有的域形成算法大多数不是自适应的,因而 SGP 协议不能得到很好的应用,从而使得 MGP 协议的优势更加明显.

(4) MGP 协议具有激励性质,在保证公平性的同时,能够鼓励节点提供更好的服务.与 SGP 协议相比,MGP 具有更好的激励性质(见实验 3).

(5) MGP 可以将低可信节点排斥到拓扑的边缘,从而能够对网络中存在的某些恶意行为进行抑制[24].与 SGP 协议相比,MGP 协议在抑制恶意行为方面具有更加出色的表现(见实验 1 和实验 2).

4 实验及分析

我们进行了一系列实验来检验 MGP 协议的有效性和安全性,并与 SGP 协议进行了对比测试.

4.1 实验设置

所有实验都在一台 PC 机上完成,PC 机的配置为 CPU P IV1.6GHZ,内存 1GB,操作系统为 Windows XP.初始网络拓扑结构基于 Power-law,由 PLOD(power_law out_degree)[25]算法产生.Power-law[26]的含义是指节点的度数为 m 的概率与 m 的 $-\lambda$ 次幂成比例,即 $P(x=m)=c\times m^{-\lambda}$,其中,$\lambda$ 的取值范围为[2.2,2.4].

划分节点:有研究表明[13],可以基于偏好领域将 Peer 节点划分为不同的类别.同样有研究显示:P2P 网络中存在一类被称为 Freeriders 的节点[8],该类节点经常从其他节点获取资源,但本身却不共享任何资源;另外,网络中还存在着一类恶意节点[24],这类节点通常共享不真实的资源.因此,为了简化实验,这里将节点划分为以下几个类别:计算机类节点、音乐类节点、Freeriders 类节点和恶意节点,并依次简记为 C 类、M 类、F 类和 V 类节点.由文献[27]对真实 P2P 网络进行度量得出的结论可知,Freeriders 类节点数目约占总规模的 25%.因此,仿真实验设定 25%的节点为 Freeriders 类节点,并从中随机选择 10%规模的节点作为恶意节点,然后从剩余的节点中随机选择 35%规模的节点作为计算类节点,40%规模的节点作为音乐类节点.

内容设置:在实验中,节点共享文件的数量及类别的分配采用了文献[28]中的设置方法.在该方法中,文件可以唯一地用二元组(c,$rank$)来标识,其中:c 表示文件所属类别;$rank$ 表示文件在该类别中的排列,该排列满足 Zipf 定律*.

查询执行:查询模拟以周期为单位进行.在每个周期中,节点处于在线或离线两种状态.根据文献[29]的研究,84%的节点在线时间小于 1 个小时;而由文献[27]的研究可知,节点的在线概率与其共享的文件数目近似于正比例关系.因此,可根据节点共享的文件数目赋予其相应的在线概率,然后依据在线概率为其赋予相应的节点状态.处于在线状态的节点,需要依据一定的概率发布查询.查询的产生采用了文献[28]的方法.

4.2 实验1

该实验的目的是检验拓扑进化协议能否有效地将 F 类节点“排斥”到网络边缘.“排斥”到边缘意味着与“好”节点之间的拓扑距离加大,因而处于边缘的节点难以获得“好”节点提供的服务.实验对 MGP 和 SGP 协议进行了对比测试.这里,我们采用平均最短路径长度(the shortest path lengths)的方法来衡量节点在拓扑中位置的改变.即对任意节点 i,平均考虑 i 到网络中其余节点的最短路径长度,

$$spl_i=\frac{1}{|P\setminus i|}\sum_{j\in P\setminus i}ShortestPath(i,j) \tag{4}$$

* 根据文件流行频度(frequency)的降序对每个文件指定一个整数的阶次(rank),则频度与阶次的乘积近似为一个常数.

其中:P 表示计算机类和音乐类节点的集合,即 $P=C\cup M$;$P\backslash i$ 表示除节点 i 以外的剩余节点集合.

显然,对于 MGP 协议(如图 3 所示),在 47 个查询周期之后,F 类节点到 P 类节点的平均最短路径长度趋于无穷(相对于 SGP,MGP 有更多节点从网络中断开);P 类节点到 P 类节点的平均最短路径长度趋于一个常数,约为 3.1;C 类到 C 类节点的平均最短路径长度也趋于一个常数,约为 2.72;M 类到 M 类节点的平均最短路径长度趋于 2.3;然而,C 类到 M 类节点的平均最短路径长度却趋于 3.82,高于 C 类到 C 类节点的平均最短路径长度 2.72;同样,M 类到 C 类节点的平均最短路径长度趋于 3.9,也高于 M 类到 M 类节点的平均最短路径长度 2.3.

对于 SGP 协议(如图 4 所示),在 40 个查询周期之后,F 类节点到 P 类节点的平均最短路径长度约为 4.76;P 类节点到 P 类节点的平均最短路径长度则趋于 4.01.显然,SGP 协议并不能有效地将 F 类节点“排斥”到网络边缘,同时,其 P 类到 P 类节点的平均最短路径长度也大于 MGP 协议下的平均长度 3.1,2.72 和 2.3.其主要原因在于,SGP 协议根据节点的整体可信度进行拓扑调整,忽略了可信度在不同领域的区别,进而导致 F 类节点并不能被很好地区分,并被“排斥”到网络边缘.

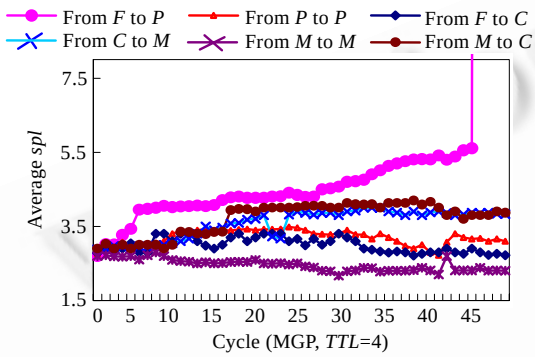

Fig.3 Average path length of Freeriders peers (MGP)

图 3 Freeriders 类节点的平均路径长度(MGP)

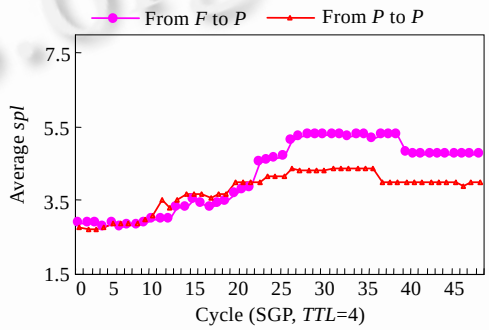

Fig.4 Average path length of Freeriders peers (SGP)

图 4 Freeriders 类节点的平均路径长度(SGP)

4.3 实验2

该实验的目的是检验拓扑进化协议能否有效地将 V(恶意)类节点“排斥”到网络边缘.将恶意节点“排斥”到网络边缘能够有效地减少其恶意行为产生的影响,这主要是因为处于边缘的节点与“好”节点之间的拓扑距离较大,这样就可以通过设置较小的 TTL(time-to-live)值,使得“好”节点发出的服务请求难以到达恶意节点,因而有效地避免了恶意节点的影响.

实验对 MGP 和 SGP 协议进行了对比测试,并采用式(4)的方法度量节点在拓扑中的位置变化(如图 5、图 6 所示).

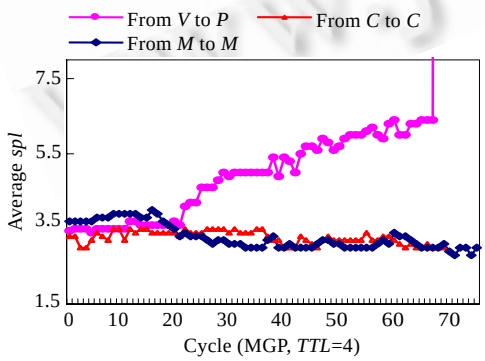

Fig.5 Average path length of malicious peers (MGP)

图 5 恶意节点的平均路径长度(MGP)

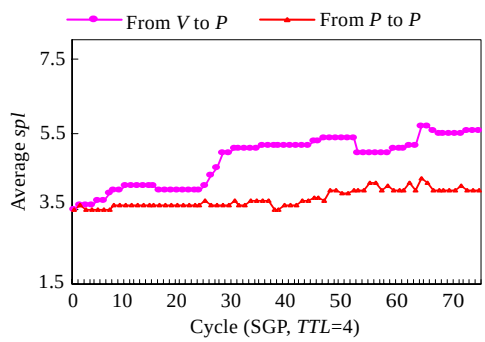

Fig.6 Average path length of malicious peers (SGP)

图 6 恶意节点的平均路径长度(SGP)

如图 5 所示,对于 MGP 协议而言,在 67 个周期执行之后,V 类节点到 P 类节点的平均最短路径长度趋于无穷,因而该协议可以有效地将恶意节点“排斥”到网络边缘.因为节点通常关心的是到其他同类节点的平均最短路径长度,因此,我们仅考察了 MGP 协议下的 C 类到 C 类、M 类到 M 类节点的平均最短路径,其长度分别趋近于 3 和 2.8.由此推出,可以通过减小 TTL 的设置,避免恶意节点接受到查询,从而减少其恶意的影响.

在 SGP 协议下(如图 6 所示),V 类节点到 P 类节点的平均最短路径长度趋于 5.6,因而该协议不能有效地将恶意节点“排斥”到网络边缘.P 类节点到 P 类节点的平均最短路径长度趋于 4,远大于 MGP 协议下的平均长度 3 和 2.8.显然,这将导致搜索效率的降低,因为较大的最短路径长度通常意味着较高的通信开销.

4.4 实验3

该实验的目的是检验上传更多的真实文件能否带来更大的回报率(requiting ratio),“好”的拓扑应该给上传文件多的节点以更多的回报.这里,我们以真实查询响应占查询总响应的比例来度量回报率的大小.

由上述实验可知,拓扑在 67 个查询周期之后趋于稳定.因此,实验选取 67~100 之间的周期作为观测周期.节点 i 的回报率 Ro_i 定义为

$$Ro_i = \frac{1}{N_i} \times \sum_{j=1}^{N_i} \frac{S_{i,j}}{S_{i,j} + F_{i,j}} \tag{5}$$

其中,N_i 表示节点 i 在全部观测周期内发起的查询数目;$S_{i,j}$ 和 $F_{i,j}$ 分别表示节点 i 在第 j 次查询中收到真实响应和虚假响应的数目.MGP 和 SGP 协议对比测试的结果如图 7 所示.

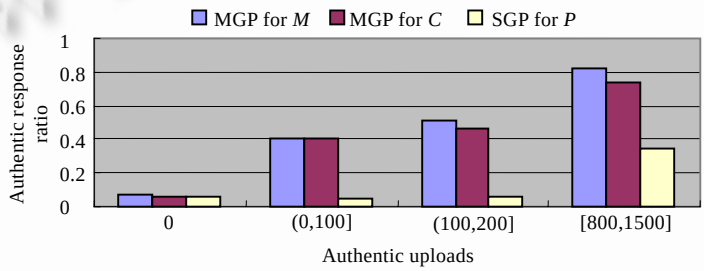

Fig.7 The relationship between authentic response ratio and authentic file number

图 7 真实响应率与真实文件数量的关系

显然,MGP 和 SGP 协议都体现了节点共享的真实文件越多,其回报率也就越高的特性.然而,共享文件数量在 1 000 个左右的节点数量仅占节点规模的约 7%,理应得到较高的回报率.在 MGP 协议中,其回报率高达 82%;而在 SGP 协议中,其回报率仅有 35%,这严重降低了用户的满意度.对于文件数量在 100 个左右的节点,这类节点应该处于拓扑的中间位置,其回报率也应该处于 50%左右.显然,对 MGP 协议的观测结果接近理想情况,而在 SGP 协议中,这类节点的回报率却不足 10%.综上易知,MGP 协议显然比 SGP 协议更具优势.MGP 将同类的“好”的节点聚集在一起,这使得“好”的节点更容易获得较高的回报率,而 SGP 协议不能根据具体领域对拓扑进行调整,节点通常因为整体可信度较低而处于拓扑的不利位置,这是导致其回报率较低的原因.

4.5 实验4

该实验的目的是考察真实查询响应占查询总响应数目的比例随查询周期的变化情况,以检验进化协议能否有效提高系统整体的服务质量.实验仅对网络中“好”的节点进行了考察,即 C 类和 M 类节点.真实响应比例的高低,通常体现了查询效果的好坏及查询效率的高低,因为在相同步数(hop)内,真实响应的比例越高,其平均单位步数的真实响应比例也就越高.因此,节点可以通过设置较小的 TTL 值而得到较为满意的结果,同时也降低了通信开销.

实验对 MGP 和 SGP 协议进行了对比测试,以查询周期作为基本的采样点,并采用真实响应率(authentic response ratio)和平均真实响应率(average authentic response ratio)两个指标作为度量的标准.周期 i 的真实响应率 AR_i 和平均真实响应率 $AR_{i,average}$ 分别定义为

$$AR_i=\frac{S_i}{S_i+F_i},\ AR_{i,average}=\delta\times\frac{S_i}{N_i\times(S_i+F_i)} \tag{6}$$

其中,S_i 和 F_i 分别表示周期 i 中真实响应和虚假响应的次数;N_i 表示周期 i 中产生的查询数目;δ是调节因子.

由图 8 可以看出:在执行 45 个查询周期之后,MGP 协议下的真实响应率区间趋近于[0.82,1],而 SGP 协议下的真实响应率区间趋近于[0.2,0.57];在平均真实响应率的比较中(如图 9 所示),MGP 协议的优势更加明显,在 45 个查询周期之后,MGP 协议下的平均真实响应率区间趋近于[1.3,2],SGP 协议下的平均真实响应率区间趋近于[0.3,0.6].与初始真实响应率和平均真实响应率比较,SGP 协议甚至呈现下降的趋势,而 MGP 协议的上升走势较为明显.造成这种状况的主要原因在于:基于 MGP 协议所做的拓扑调整可以使"好"的节点在不同领域拓扑中趋向于聚集,而"坏"的节点则被"排斥"到相应领域拓扑的边缘;而 SGP 协议却难以做到这一点.

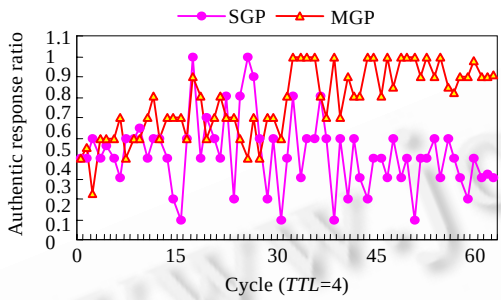

Fig.8 Authentic response ratio (MGP vs. SGP)

图 8 真实响应率(MGP vs. SGP)

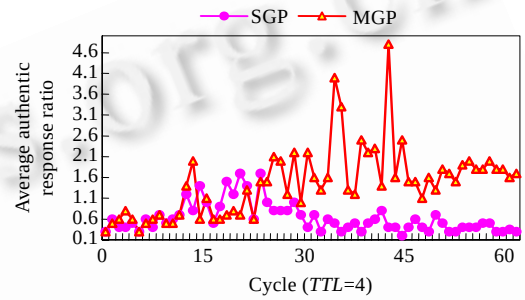

Fig.9 Average authentic response ratio (MGP vs. SGP)

图 9 平均真实响应率(MGP vs. SGP)

4.6 实验5

该实验的目的是检验节点间的连接与其偏好领域相似度之间的关系.根据文献[13]的研究,节点发出的查询通常与其偏好领域相关;而文献[4]的研究表明,相同偏好领域的节点更容易达成成功的交易.因此,"好"的拓扑应该使偏好领域相近的节点聚集在一起,这样,节点发出的查询可以在较短的步数内得到真实的响应,降低了通信开销,同时也提高了用户满意度.根据文献[28]的研究,偏好领域相似度可以转化为节点之间的内容相似度.连接(i,j)对应的内容相似度[30]定义如下:

$$S(i,j)=\frac{1}{N_{i,j}}\times\sum_{t=1}^{N_{i,j}}\frac{|Cf_{i,t}\cap Cf_{j,t}|}{|Cf_{i,t}|+|Cf_{j,t}|-|Cf_{i,t}\cap Cf_{j,t}|} \tag{7}$$

其中:$N_{i,j}=|DM_i.C\cup DM_j.C|$;$DM_i.C$ 和 $DM_j.C$ 分别表示节点 i 与 j 的偏好领域集;$Cf_{i,t}$ 表示节点 i 在 t 领域共享的文件集,$Cf_{i,t}\cap Cf_{j,t}$ 表示节点 i 与 j 在 t 领域拥有的相同文件集.测量结果如图 10 所示.

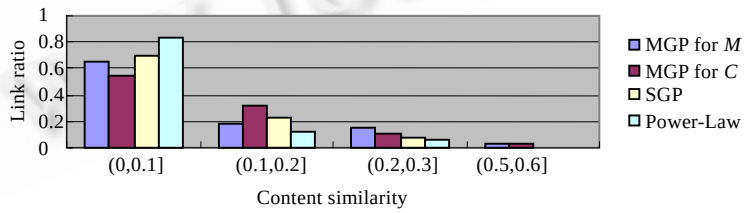

Fig.10 The relationship between Link ratio and content similarity

图 10 连接率与内容相似度的关系

由结果可以看出,多数连接对应的相似度介于 0~0.1 之间.这主要是因为网络中只有约 7%的节点共享 1 000 个左右的文件,68%的节点共享 100 个左右的文件,文件数量差别过大;再者,由于初始生成的 Power-Law 拓扑并没有考虑节点的差别,某些 F 类节点初始可能拥有较多的连接,这也是导致多数连接对应的相似度介于 0~0.1 之间的原因.另外,相似度的大小也与相似度度量函数相关.因此,这里着重对各个拓扑进行相对量的比较.显然,MGP 协议在(0.2,0.3)和(0.5,0.6)两个相似度区间中表现出明显的优势,尤其是在(0.5,0.6)区间中不存在对应

的 SGP 和 Power-Law 拓扑中的连接,而与该区间对应的 MGP 拓扑中连接数的比例达到了 3.5%.造成这种状况的根本原因在于,MGP 协议的拓扑调整可以针对具体的领域进行;而 SGP 拓扑对不同种类的节点不加区分,导致其拓扑的低效性.

5 结 论

本文提出了领域可信度的定义,并在此基础上给出了一个基于领域可信度的自适应 P2P 拓扑进化协议 MGP.MGP 协议可以针对具体的领域进行拓扑调整,体现了拓扑的公平性.该协议同时能够对节点的恶意行为进行有效的抑制,并具有激励性质,鼓励节点提供更好的服务,以获得更高的回报率.分析和仿真表明,MGP 协议在有效性和安全性等方面比现有协议有较大的提高.

References:

[1] Bawa M, Cooper BF, Crespo A, Daswani N, Ganesan P, Garcia-Molina H, Kamvar S, Marti S, Schlosser M, Sun Q, Vinograd P, Yang B. Peer-to-Peer research at Stanford. ACM SIGMOD Record, 2003,32(3):23−28.

[2] Dou W. The research on trust-aware P2P topologies and constructing technologies [Ph.D. Thesis]. Changsha: National University of Defense Technology, 2003 (in Chinese with English abstract).

[3] Sun Q, Garcia-Molina H. SLIC: A selfish link-based incentive mechanism for unstructured peer-to-peer networks. In: Lai TH, Okada K, eds. Proc. of the 24th IEEE Int'l Conf. on Distributed Computing Systems. New York: IEEE Press, 2004. 506−515.

[4] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks. In: Moro G, ed. Proc. of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004. 23−34.

[5] Condie T, Kamvar SD, Garcia-Molina H. Adaptive peer-to-peer topologies. In: Lambrix P, Duma C, eds. Proc. of the 4th Int'l Conf. on Peer-to-Peer Computing. New York: IEEE Press, 2004. 53−62.

[6] Zhang Q, Zhang X, Wen XZ, Liu JR, Shan T. Construction of peer-to-peer multiple-grain trust model. Journal of Software, 2006, 17(1):96−107 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/96.htm

[7] Chawathe Y, Ratnasamy S, Breslau L, Shenker S. Making Gnutella-like P2P systems scalable. In: Crowcroft J, Wetherall D, eds. Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM Press, 2003. 407−418.

[8] Bernardo EA. Huberman A. Free riding on Gnutella. Techniqal Report, SSL-00-63, Palo Alto: Xerox PARC, 2000.

[9] Cooper BF, Garcia-Molina H. Ad hoc, self-supervising peer-to-peer search networks. ACM Trans. on Information Systems, 2005, 23(2):169−200.

[10] Lv Q, Ratsnasamy S, Shenker S. Can heterogeneity make Gnutella scalable? In: Druschel P, Kaashoek M F, Rowstron AIT, eds. Proc. of the 1st Int'l Workshop on P2P Systems. Berlin: Springer-Verlag, 2002. 94−103.

[11] Sakaryan G, Unger H. Influence of the decentralized algorithms on topology evolution in P2P distributed networks. In: Unger H, Tutsch D, eds. Proc. of the Design, Analysis, and Simulation of Distributed Systems (DASD 2003). San Diego: SCS Press, 2003. 12−18.

[12] Sakaryan G, Unger H. Topology evolution in P2P distributed networks. In: Hamza MH, ed. Proc. of the IASTED: Applied Informatics (AI 2003). Calgary: ACTA Press, 2003. 791−796.

[13] Crespo A, Garcia-Molina H. Semantic overlay networks for P2P systems. In: Moro G, Bergamaschi S, Aberer K, eds. Proc. of the 3rd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004. 1−13.

[14] Song JT,Sha CF, Yang ZY, Zhu H. Study on construction and searching of semantic peer-to-peer networks. Journal of Computer Research and Development, 2004,41(4):645−652 (in Chinese with English abstract).

[15] Klampanos IA, Jose JM. An architecture for information retrieval over semi-collaborating peer-to-peer networks. In: Omicini A, Wainwright RL, eds. Proc. of the 2004 ACM Symp. on Applied Computing. New York: ACM Press, 2004. 1078−1083.

[16] Asvanund A, Krishnan R. Content-Based community formation in hybrid peer-to-peer networks. In: Callan J, Fuhr N, Nejdl W, eds. Proc. of the SIGIR Workshop on Peer-to-Peer Information Retrieval, the 27th Annual Int'l ACM SIGIR Conf. New York: ACM Press, 2004. 24−34.

[17] Loser A, Naumann F, Siberski W, Nejdl W, Thaden U. Semantic overlay clusters within super-peer networks. In: Aberer K,

Koubarakis M, Kalogeraki V, eds. Proc. of the Int'l Workshop on Databases, Information Systems and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2003. 33−47.

[18] Wang Y, Vassileva J. Trust-Based community formation in peer-to-peer file sharing networks, In: Zhong N, ed. Proc. of the IEEE/WIC/ACM Int'l Conf. on Web Intelligence (WI 2004). New York: IEEE Press, 2004. 341−348.

[19] http://www.orkut.com

[20] http://www.tribe.net

[21] Kamvar S, Schlosser M, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. In: Chen YFR, Kovacs L, Lawrence S, eds. Proc. of the 12th Int'l World Wide Web Conf. New York: ACM Press, 2003. 640−651.

[22] Chen G, Lu RQ, Jin Z. Constructing virtual domain ontologies based on domain knowledge reuse. Journal of Software, 2003,14(3): 350−355 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/350.htm

[23] Maedche A, Staab S. Measuring similarity between ontologies. In: Gomez-Perez A, Benjamins RV, eds. Proc. of the European Conf. on Knowledge Acquisition and Management. Berlin: Springer-Verlag, 2002. 251−263.

[24] Daswani N, Garcia-Molina H. Query-Flood DoS attacks in Gnutella. In: Sandhu R, ed. Proc. of the ACM 9th Conf. on Computer and Communications Security. New York: ACM Press, 2002. 181−192.

[25] Palmer C, Steffan J. Generating network topologies that obey power-law. In: Gavalas D, Greenwood D, Ghanbari M, eds. Proc. of the IEEE Global Telecommunication Conf. (GLOBECOM 2000). San Francisco: IEEE Press, 2000. 434−438.

[26] Ripeanu M. Peer-to-Peer architecture case study: Gnutella network. Technical Report, TR-2001-26, Chicago: University of Chicago, 2001.

[27] Saroiu S, Gummadi PK, Gribble SD. A measurement study of peer-to-peer file sharing systems. In: Kienzle MG, ed. Proc. of the Multimedia Computing and Networking 2002 (MMCN 2002). Bellingham: SPIE Press, 2002. 156−170.

[28] Schlosser M, Condie T, Kamvar S. Simulating a file-sharing P2P network. In: Proc. of the 1st Workshop on Semantics in P2P and Grid Computing. 2002. http://www.stanford.edu/~sdkamvar/papers/simulator.pdf

[29] Wilcox-O'Hearn B. Experiences deploying a large-scale emergent network. In: Druschel P, Kaashoek F, Rowstron A, eds. Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. Berlin: Springer-Verlag, 2002. 104−110.

[30] Leake DB, Maguitman A, Cannas A. Assessing conceptual similarity to support concept mapping. In: Haller SM, Simmons G, eds. Proc. of the 15th Int'l Florida Artificial Intelligence Research Society Conf. Menlo Park: AAAI Press, 2002. 168−172.

附中文参考文献:

[2] 窦文.信任敏感的 P2P 拓扑构造及其相关技术研究[博士学位论文].长沙:国防科学技术大学,2003.

[6] 张骞,张霞,文学志,刘积仁,Ting Shan.Peer-to-Peer 环境下多粒度 Trust 模型构造.软件学报,2006,17(1):96−107. http://www.jos.org.cn/1000-9825/17/96.htm

[14] 宋建涛,沙朝锋,杨智应,朱洪.语义对等网构造及搜索机制的研究.计算机研究与发展,2005,41(4):645−652.

[22] 陈刚,陆汝钤,金芝.基于领域知识重用的虚拟领域本体构造.软件学报,2003,14(3):350−355. http://www.jos.org.cn/1000-9825/14/350.htm

张骞(1979－),男,山东金乡人,博士生,主要研究领域为数据管理,P2P 计算.

刘积仁(1955－),男,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络,数据管理.

张霞(1965－),女,博士,教授,CCF 高级会员,主要研究领域为数据库技术,P2P 计算.