ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.10, October 2009, pp.2885−2898
doi: 10.3724/SP.J.1001.2009.03554

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

一种基于反馈可信度的分布式 P2P 信任模型*

胡建理[1,2+], 吴泉源[1], 周 斌[1], 刘家红[1]

[1](国防科学技术大学 计算机学院,湖南 长沙 410073)

[2](广州军区广州总医院 信息科,广东 广州 510010)

Robust Feedback Credibility-Based Distributed P2P Trust Model

HU Jian-Li[1,2+], WU Quan-Yuan[1], ZHOU Bin[1], LIU Jia-Hong[1]

[1](School of Computer, National University of Defense Technology, Changsha 410073, China)

[2](Department of Information, Guangzhou General Hospital under Guangzhou Area Command, Guangzhou 510010, China)

+ Corresponding author: E-mail: lxman82@gmail.com, http://www.nudt.edu.cn

Hu JL, Wu QY, Zhou B, Liu JH. Robust feedback credibility-based distributed P2P trust model. *Journal of Software*, 2009,20(10):2885−2898. http://www.jos.org.cn/1000-9825/3554.htm

Abstract: The open, sharing and anonymous nature of peer-to-peer (P2P) networks has made it popular in many large-scale distributed applications over the Internet. However, due to the fact that resource-sharing activity of a peer in P2P networks is a volunteer behavior and it is not responsible for its irresponsible bartering history, the trust relationship between participants can not be constructed only on the traditional trust mechanism. A feasible resolution derived from the trust relationship in social networks, is to establish a reputation based global trust model. The previous work about the global trust model is mostly based on the assumption that the peer with higher trust value will provide more honest feedbacks, and make the quality of feedback of a peer be approximately equal to that of service of the peer. However, this is not always true. To solve this problem, this paper proposes a robust feedback credibility (FC) based distributed P2P global trust model (FCTrust), to quantify and evaluate the trustworthiness of participants, and gives the mathematic analyses and distributed implementation method. Theoretical analyses and simulation experiments show that FCTrust has advantages in combating various malicious behaviors such as dishonest feedbacks from malicious peers, the collusion and the strategic attacks to the trust model itself, over the current global trust models, and demonstrates more robustness and effectiveness.

Key words: peer-to-peer; trust; global trust model; feedback credibility; information storage

摘 要: 开放、共享与匿名的 Peer-to-Peer(简称 P2P)网络已经取得了越来越多的应用,无中心对等的特性也吸引了越来越多的用户.但由于其网络中的节点不受约束,资源的共享是用户自愿的行为,因此节点间的信任很难通过传统的信任机制建立.一种可行的解决方案是借鉴人际网络中的信任关系,建立一种基于信誉的全局信任模型.已有的

* Supported by the National Natural Science Foundation of China under Grant No.60873204 (国家自然科学基金); the National Basic Research Program of China under Grant No.2005CB321800 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant Nos.2007AA010301, 20060101Z1067, 2005AA112030 (国家高技术研究发展计划(863)); the National Natural Science Fund for Distinguished Young Scholars of China under Grant No.60625203 (国家杰出青年科学基金)

Received 2008-11-28; Accepted 2008-12-30

工作基本建立在信任度高的节点其反馈也更可信这个假设的基础上,将节点的反馈质量简单地等同于服务质量.针对这一问题,提出了一种基于节点反馈可信度的分布式 P2P 全局信任模型(简称 FCTrust),用于量化和评估节点的可信程度,并给出了模型的数学表述和分布式实现方法.分析及仿真实验结果表明,FCTrust 较已有的全局信任模型在遏制更广泛类型的恶意节点攻击的有效性、迭代计算的收敛性及消息成本上有较大提高.

关键词: 对等网络;信任;全局信任模型;反馈可信度;信息存储

中图法分类号: TP393 **文献标识码:** A

目前,有关 P2P 的应用日益广泛[1],但仍然缺乏有效的信任机制提高系统整体的可用性[2],这非常显著地表现为应用中大量欺诈行为的存在以及不可靠的服务质量[1].以众多的文件共享应用为例,25%的文件是伪造文件(faked file),同时,不负责任的用户随意地终止(文件上载)服务,使得服务质量无法得以较好的保证.因此,有必要建立一种新的分布式信任机制,这已经成为当前的研究热点之一[3−6].

在传统的网络环境中,往往通过可靠的第三方(如认证中心 CA)来建立信任关系,但这种集中式的信任机制并不适合于 P2P 网络[3].已有的工作[3−8]显示,借鉴人际网络中的信任关系建立有效的基于信誉的信任模型,能够有效地抑制节点资源滥用与欺诈等恶意行为.

目前存在的基于信誉的信任模型[3−8]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.当存在多个可选服务时,信任等级高的节点成为首选,并且混淆节点“服务质量”与“反馈质量”的区别.这样做可以在一定程度上抑制节点的一般恶意行为,但在应付许多针对信任模型本身的一些攻击行为,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.除此之外,还存在信任模型迭代计算收敛成本与消息代价过高的问题.如果这些问题不能很好地解决,不仅会直接导致信任机制无法有效发挥作用,还会造成系统本身运行效率低下、管理上混乱的局面,进一步加重其他不良行为的影响,对系统的健康运行和良性发展带来诸多隐患.

针对上述不足,本文旨在建立一种 P2P 环境下基于反馈可信度的信任模型,并给出了相应的基于 Terrace[3] 的分布式存储方案及求解算法.仿真实验结果表明,与已有的信任模型[3,6]相比,FCTrust 信任模型在收敛速度、消息成本方面有较大的提高,并能更有效地抑制更广泛类型的恶意节点的攻击行为.

本文第 1 节分析相关工作.第 2 节给出模型的数学表述与收敛性分析.第 3 节具体阐述全局信任度的分布式计算的实现过程,包括分布式存储机制与信任求解算法.第 4 节给出信任模型的仿真实验结果及分析.最后总结全文并指出下一步的研究工作.

1 相关工作

1994 年,Marsh 首先系统论述了信任的形式化问题.他从信任的概念出发,对信任内容和信任程度进行划分,并从信任的主观性入手提出信任度量的数学模型[9].随后,Adul-Rahman 等学者[10]则针对互联网社群中的信任度评价问题给出基于分布的反馈信息的信任度评价模型.在此之后,围绕如何更为合理、准确地刻画节点的信任问题,许多学者分别从各自的角度针对 P2P 环境下不同的应用模式提出了许多形式各异的信任管理模型[3−8].

将这些信任模型归纳起来可以分为两类,即依赖于第三方与不依赖第三方的信任模型.前者的典型代表,如基于 PKI 的信任模型.这类系统中,有一个或一组权威节点维护一个可信的节点集合.这些权威节点可以颁发证书给可信的新加入的节点,节点以证书作为其身份的凭证使用网络中的资源,这类系统往往是中心依赖的,与 P2P 的分布式属性不相符合,存在单点失效问题.不依赖于可信第三方的信任模型主要有两类:基于微支付的模型和基于社会信任网络的模型.在基于微支付的模型[11]中,节点接受服务需支付一定的虚拟货币,提供服务可以获得虚拟货币.然而,这需要一个完整的计费系统跟踪记录每一笔小额交易,因此不具有工程可行性[12].

基于社会信任网络的模型借鉴社会学有关信任的研究成果,又可分为局部信任模型和全局信任模型.在局部信任模型系统中,节点通过询问有限的其他节点以获取它们对某个节点的推荐度,再综合自己和该节点交互的历史经验,确定节点的信任度.在这类系统中,往往采取简单的局部广播的手段,其获取的节点信任度也往往

是局部的和片面的[3].全局信任模型通过邻居参与者间相互满意度的迭代计算得到代表系统全局视图的节点信任度,其特征是系统中每个节点在某一时刻都有一个唯一的全局信任度,不随评价主体及反馈节点集的不同而不同.这类模型的构建方法一般是基于节点入度(in-degree)的中心性测量(centrality-measurement)[13]方法,任意节点的全局信任度取决于与之发生过交易行为的其他节点对它的局部看法以及这些节点的全局信任度,EigenTrust[6]和窦文的模型[3]是这类模型的典型代表(这里不作详细介绍,有兴趣的读者可参考相关文献).虽然这两个模型都是通过迭代的方法计算节点的全局信任度,并利用分布 Hash 机制存储节点的全局信任信息,但它们都没考虑节点反馈可信度的概念,均以节点的全局信任度本身作为反馈度的权重,即假设具有高全局信任度的节点其反馈也更加可信(其不合理性讨论见第 2.3 节).为此,本文提出一种基于反馈可信度的分布式 P2P 全局信任模型 FCTrust,它具有如下几个特点:

(1) 它是一种基于反馈可信度的全局信任模型,节点在提供反馈时,除了考虑反馈节点本身的全局信任度以外,还考虑该节点的反馈可信度,使得该模型在处理一些恶意节点攻击行为的有效性与健壮性上,明显优于 EigenTrust 及窦文的模型;

(2) 在构建反馈可信度计算模型时,充分考虑节点间的交互频繁程度与节点间的评分行为的相似程度,能够较好地识别出恶意节点的不诚实反馈及协同作弊行为,给予具有更低反馈可信度节点以更低的权重,从而能够有效地抑制这类节点的恶意行为;

(3) 对 Terrace 树存储机制进行了改进,解决了高可信节点档案存放到低可信节点引起节点负载过重、信任度查找效率过低的问题,使节点的消息路由效率大为提高;

(4) 较已知的全局模型,在迭代计算收敛及消息成本上性能有较大的提高.

2 FCTrust 全局信任模型

2.1 模型的定义与表示

首先给出满意度评价函数与局部信任度的定义,然后给出了反馈可信度的定义,最后引出了全局信任度的定义.

定义 1(满意度评价函数). 节点交互之后彼此提交满意度的评价,我们可将节点 i 对节点 j 交互满意度的评价定义为 Map 函数 $f(i,j)$:

$$f(i,j)=\begin{cases}1, & \text{totally satisfactory}\\ 0, & \text{totally unsatisfactory}\\ e(\in(0,1)), & \text{else}\end{cases} \tag{1}$$

我们采用概率可能性的方法来区分节点提供的不同服务质量,1 表示节点 i 对节点 j 完全满意,0 表示节点 i 对节点 j 完全不满意,值越大表示满意度越高.

定义 2(局部信任度). 即归一化的局部满意度.在时间区间 t(t 视具体的应用而定,如 6 个月)内,假设节点 i 和节点 j 之间交互的次数为 m,则直接信任评价可定义为

$$D_{ij}=\begin{cases}\dfrac{\sum_{k=1}^{m}f(i,j)}{m}, & m\neq 0\\ 0, & m=0\end{cases} \tag{2}$$

D_{ij} 是节点 i 根据直接交易历史对节点 j 作出的信任评价,也即节点 i 对节点 j 提供的反馈.当 m=0 时,表示节点 i 与节点 j 之间没有交互历史,我们将节点 i 对节点 j 的局部信任度设定为 0.

定义 3. 反馈可信度是用来刻画反馈节点(服务消费者)对评价主体(服务提供者)提供的反馈信息真实、准确程度的度量.进行信任评价时,具有更高反馈可信度的节点提供的反馈信息可信度更高,因此给予更高的权重;相反地,我们给予具有较低反馈可信度的节点的反馈意见以更低的权重.一般来说,反馈可信度与以下几种因素相关:

(1) 节点间的交互频繁程度.一般来说,交易越多,则节点间的反馈可信度越高;

(2) 节点间的评分行为的相似程度.节点 i 与参考节点 j 的评分相似性越高,则说明 i 与 j 对网络中其他节点的看法越一致.

我们引入交易密度因子 $TNum_{ij}$ 来描述节点 i 与 j 交易的频繁程度,并定义交易密度因子为

$$TNum_{ij}=\frac{m}{n}\times\beta^{\frac{1}{m}},\beta\in(0,1)\cap m\neq 0 \tag{3}$$

其中,m 表示节点 i,j 之间交易的次数,n 表示节点 i 与所有其他节点交易的总次数.当 m=0 时,令 $TNum_{ij}$=0;β为交易密度调节常数,引入该常数是为了更合理地描述节点间交易频繁程度的实际状况,使之更准确地反映节点交易密度的差异,如:对任意节点 a,b,c,a,b 之间交易对应的 m 与 n 值分别为 500,1 000;a,c 之间的交易对应的 m 与 n 分别为 5,10.显然,如果没有引入调节因子,会出现 $Tnum_{ab}$=$Tnum_{ac}$=0.5 的情况.而实际情况是由于 a,b 之间交易的绝对次数少而使其反馈可信度有所折扣,$Tnum_{ab}$>$Tnum_{ac}$ 更符合实际情况.显然,$TNum_{ij}$ 值越大,意味着节点交互的经验就越多,对其产生的局部信任评价的可信度就越高.

我们将描述节点间评分行为的相似性的量记为 $TSim_{ij}$,用来表征节点行为的一致性.设节点 i 与节点 j 的公共交互节点集合记为 $CSet(i,j)$,那么节点 i 和节点 j 对公共交互节点评价差异 $TDif_{ij}$ 可定义为

$$TDif_{ij}=\frac{\sum_{k\in CSet(i,j)}|D_{ik}-D_{jk}|}{|CSet(i,j)|} \tag{4}$$

设节点 i 对节点 j 容忍的最大评价偏差为 θ,则我们可以将 $TSim_{ij}$ 定义为

$$TSim_{ij}=\begin{cases}TSim_{ij}+\dfrac{(1-TSim_{ij})}{2}\times\left(1-\dfrac{TDif_{ij}}{\theta}\right), & TDif_{ij}<\theta\\ TSim_{ij}-\dfrac{TSim_{ij}}{2}\times\left(1-\dfrac{\theta}{TDif_{ij}}\right), & \text{else}\end{cases} \tag{5}$$

综合上述两种因素,我们可定义反馈可信度 Cr_{ij} 为

$$Cr_{ij}=TNum_{ij}\times TSim_{ij} \tag{6}$$

因此,由以上分析可以看出,反馈节点交易次数越多,评分行为一致性越强,则其反馈可信度也越高.

定义 4. 称矩阵 $R=(R_{ij})$为反馈品质矩阵,其元素 $R_{ij}=D_{ij}\times Cr_{ij}$.与一般网络信任关系矩阵$(D_{ij})$不同,反馈品质矩阵不仅考虑了各节点提供的局部信任评价信息,而且考虑了节点本身的反馈可信度,这两种信息聚合很好地刻画了反馈信息的实际信任状况.

定义 5. 网络 N 中对任意节点 i 的全局信任度为 T_i,其定义为

$$T_i=\sum_{j\in K}D_{ji}\times Cr_{ji}\times T_j \tag{7}$$

其中,K 为与 i 曾经交互过并对 i 提供过反馈评价的节点集合.用节点 j 对节点 i 的反馈可信度作为节点 j 提供的局部信任信息的权重,能够有效地遏制节点不诚实反馈、协同作弊和策略性攻击等恶意行为,第 4.4.3 节仿真实验证实了这一点.

设全局信任度向量 $T=[T_1,T_2,\ldots,T_n]^T$,则公式(7)的矩阵形式为

$$T=R^T\times T \tag{8}$$

其中,R 为定义 4 所描述的反馈品质矩阵.

2.2 全局信任度迭代计算收敛性分析

基于公式(8)的迭代收敛与否,决定了全局信任度向量 T 的解的存在性.下面用迭代矩阵 R^T 的范数小于 1 来证明此迭代法的收敛性.

定理 1. 对于任意初始向量 $T^{(0)}$,基于公式(8)的简单迭代法 $T^{(k+1)}=R^T\times T^{(k)}$收敛.

证明:上述迭代收敛的充分条件是矩阵 R^T 的范数$\|R^T\|_1<1$[14].

因为 $\| R^T \|_1 = \max_i \sum_j | D_{ij} \times Cr_{ij} | \le \max_{i,j} | Cr_{ij} | \times \max_i \sum_j D_{ij} \le \max_{i,j} | Cr_{ij} |$,由公式(6)可知,

$$\max_{i,j} | Cr_{ij} | = \max_{i,j} | TNum_{ij} \times TSim_{ij} | < \max_{i,j} | TNum_{ij} | \times \max_{i,j} | TSim_{ij} | < \max_{i,j} | TSim_{ij} | < 1.$$

也即$\|R^T\|_1<1$.命题得证. □

2.3 全局信任模型的进一步讨论

由第 1 节所述,一般全局信任模型构建思路为:任意节点的全局信任度由与之发生过交易行为的其他节点对它的局部信任度以及这些节点本身的全局信任度聚合而成.这种设计方法基于如下假设:提供高质量服务的节点提供的反馈更可信;提供低质量服务的节点,其反馈更不可信.这种方法存在的问题是没有合理区分节点所承担的“提供服务”与“提供反馈”的两种角色,以“服务质量”代替“反馈质量”.实质上,它们是两个不同的概念,代表节点在网络系统中所承担的两种职能,即向其他节点提供服务以及提供反馈(推荐),两种职能并不存在必然的关联,如提供高质量服务的节点,出于一定的目的完全可以向某些节点提供不诚实的反馈;而提供低质量服务的节点可能是由其固有的客观条件所决定的(如有限的资源),它也可以向其他节点提供诚实的反馈.因此,这类方法有一定的局限性,恶意节点可以根据此算法的特点来操纵甚至颠覆信誉系统.

由于这类方法并没有考虑节点反馈可信度的概念,因而不能很好地解决 P2P 系统中节点的不诚实反馈、协同作弊等可信问题.相比较而言,由于 FCTrust 信任模型引入了该机制,充分考虑了节点间交互的频繁程度,使节点的信任评价更加精确.同时,利用节点间评分行为一致性评估机制能够有效识别并抑制更广泛类型的恶意节点的攻击行为,保障 P2P 系统正常有序地运行.

3 全局信任度的分布式计算的实现

全局信任度的分布式计算的实现涉及 3 个相关的方面,即信任信息的分布式存储、存储的安全性保证及分布式求解算法.

3.1 信任信息的分布式存储

我们基于文献[3]提出的 Terrace 拓扑设计了面向 FCTrust 的信誉信息分布存储机制.Terrace 拓扑是一种基于 DHT 技术的结构化拓扑,通过 Terrace,网络中的所有节点投影到一个逻辑 *d*-tree 上,并赋予节点全局唯一的逻辑地址,逻辑地址的编码基数为 *d*-tree 的阶.例如,如果用八进制表示逻辑地址,则 *d* 为 8.树的最大空间由系统规模决定,例如,设逻辑空间为 IPv4 地址空间的投影,则逻辑空间的大小为 $0\sim2^{32}-1$.空间(树)中每个节点拥有 *d* 个逻辑地址.以图 1 为例,图中地址由八进制表示,则除根节点最大扇出为 7 以外,其余逻辑树节点的最大扇出为 8.从根节点起,每一个节点的子节点都是该节点逻辑地址在下一个基数位的列举,而节点自身包含当前基数位的所有列举(根节点例外,它没有第 0 位子树).通过均匀的 Hash,节点可以将对象(或对象索引)投影到同样的逻辑地址空间.

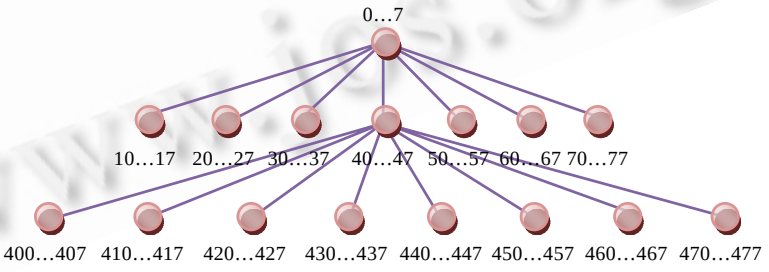

Fig.1 Diagram of the logical space of 8-tree based Terrace

图 1 阶为 8 的 Terrace 树逻辑空间示意图

定义 6. 在 P2P 系统中,任意节点 i 在 Terrace 树中所处的层次记为 $Layer(i)$.

定义 7. 在 P2P 系统中,任意两个节点 i 与 j 在 Terrace 树中所处的层次之差记为 $LayerDif(i,j)$:

$$LayerDif(i,j)=Layer(j)-Layer(i).$$

Terrace 树的构造是节点信任度相关的,其构造策略保证树的上层节点的信任度大于或等于树的下层节点信任度,高可信节点占据 Terrace 拓扑的上层,而低可信节点则处于拓扑的下层.这种机制能够有效地保证高可信节点在实际信任管理与 P2P 应用中承担更多的负载,达到负载平衡的效果.但该拓扑在存储节点信任信息时没有考虑档案点间的异构性,某些高可信节点的档案可能存放在低可信节点上.高可信度通常意味着高访问量,档案点需要面对的是频繁的信任度更新及计算,这对于计算能力、网络带宽等都非常有限的低可信档案点而言可能成为严重的负载.

例如,Terrace 树通过一个均匀的 Hash 函数(例如 SHA-1)HDT 将节点 i 的标识 ID_i 投影到 Terrace 中的某个节点逻辑地址 d 上,记为 $d=HTD(ID_i)$,d 所对应的 Terrace 节点称为节点 i 的档案点,记为 k.节点 i 的信任信息就存储在 i 的档案点 k 上.如果 $LayerDif(i,k)>0$,说明节点 k 位于节点 i 的下层.由于 Terrace 采用的是“先上后下”的路由,因此,某节点要查询节点 i 的信任度信息,从 Terrace 树的根节点定位到 k 需要路由更长路径,需要更多的消息开销.不仅如此,k 作为用户节点的全局信任度 $T_k<T_i$,会出现上述的高可信节点的档案存放在低可信节点上的现象.因此,本文采用文献[15]所提出的方法,将节点 i 的档案点向沿 Terrace 树根节点的方向作一定的迁移,使节点信任度的分布更加平衡,路由效率更高;反之,当 $LayerDif(i,k)<0$,则说明节点 k 位于 i 的上层,与 Terrace 树根节点更加接近,不需要对 k 的位置作进一步的调整.对消息成本的性能仿真见本文第 4.4.2 节.

如图 2(a)所示,以一个阶为 3 的 Terrace 树为例,节点 j 要将节点 i 的信任信息写入其档案点,我们进行 $HTD(ID_i)=121$,则节点 j 通过路由定位到节点 k,即 k 为节点 i 的档案点.而 $LayerDif(i,k)=Layer(k)-Layer(i)=3-2=1$,则由上述改进策略,将 k 沿根节点的方向移动 1 个节点到 g,即将 i 的档案写入节点 g,如图 2(b)所示.

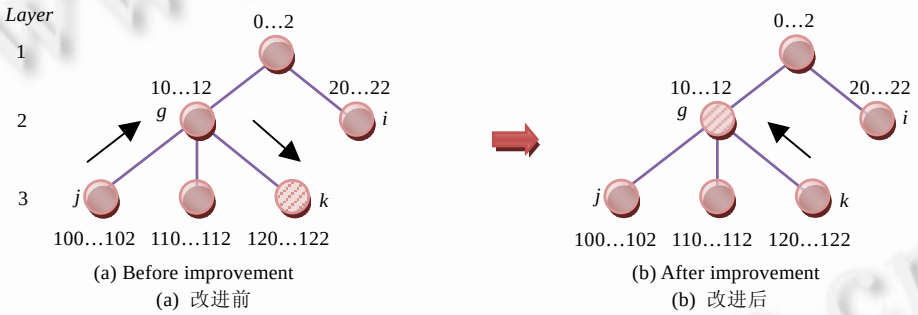

Fig.2 Comparison of Terrace based trust information storage mechanism improved between before and after

图 2 基于 Terrace 的改进前后的信任信息存储机制

具体来说,对应于 RBTrust 的信任模型,节点信誉计算的相关信息存放在其对应的逻辑节点上.设节点 i 的档案点为 d,则 d 至少需要包含一个如表 1 所示的数据结构.

Table 1 Structure of documentary point d of peer i

表 1 节点 i 的档案点 d 的数据结构

ID_i				$T_i^{(k+1)}$
ID_{j1}	$EVal_{j1}$	Num_{j1}	$TNum_{j1}$	$T_{j1}^{(k)}$
ID_{j2}	$EVal_{j2}$	Num_{j2}	$TNum_{j2}$	$T_{j2}^{(k)}$
…	…	…	…	…
ID_{ji}	$EVal_{ji}$	Num_{ji}	$TNum_{ji}$	$T_{jT}^{(k)}$

如表 1 所示,ID_i 为节点 i 的标识;$ID_{j1},\ldots,ID_{ji}$ 为节点 i 的反馈节点的标识;$EVal_{j1},\ldots,EVal_{ji}$ 为与 i 发生过交易

的节点提供的满意度评价;$Num_{j1},\ldots,Num_{ji}$ 和 $TNum_{j1},\ldots,TNum_{ji}$ 分别为与 i 发生过交易的节点在一段时间内(长度与具体的应用有关)与 i 交易的次数与所有其他节点发生交易的总次数; $T_{j1}^{(k)},...,T_{jT}^{(k)}$ 为反馈节点当前的全局信任度; $T_i^{(k+1)}$ 为由 d 计算出的节点 i 目前的全局信任度.

3.2 安全性分析

我们将 Terrace 作为上层 P2P 应用网络的底层支撑,即由 Terrace 作为底层的信任管理的基础设施,为上层结构化或非结构化 P2P 应用体系提供必要的信任保障.由于 Terrace 采用了单向 Hash 的方法,即节点加入拓扑时获取逻辑地址是随机的,无法根据节点的某个特征(如 IP 地址等)预先决定节点的逻辑地址,这为信任度的匿名放置的安全性带来一定优势.相对于 Terrace,CAN 和 Chord 的节点加入采用了双向 Hash 的方法,节点在拓扑中的逻辑地址由节点的某些属性预先决定(如 Chord 中节点的逻辑地址由其 IP 地址的 Hash 值决定,CAN 由节点的 ID 决定),因此,节点在拓扑中的逻辑位置固定,造成了任意节点与其档案点之间存在一一对应的关系(忽略拓扑的动态因素),从而为节点与其档案点之间的协同作弊带来便利.

与传统的分布式系统一样,基于 Terrace 的信任度查询请求、应答中同样面临着信任消息的篡改与保密性问题.我们可以以对称或非对称加(解)密机制、数字签名和报文摘要等传统安全技术为基础,设计开发相应的访问控制策略与身份认证机制,并集成到基于 Terrace 树的信任信息存储机制中,以保障 FCTrust 模型的信任信息在传输与通信中的安全性.关于这方面的内容,在下一步对信任模型 FCTrust 作进一步的完善与扩展时将加以系统的研究,本文不作重点论述.

3.3 分布式求解协议

首先给出协议的几个原语及其语义:

- *Put*(ID_v,ID_u,$EVal_{uv}$):节点 u 将对节点 v 的满意度评价 $EVal_{uv}$ 写入 Terrace 树中逻辑地址为 $HDT(ID_v)$的档案点,*HDT* 为 Hash 函数,下同.用户通过该原语将节点交易成功后的评价信息保存到 Terrace 树相应的逻辑地址中;
- *Put*(ID_v,ID_u,Num_{uv},$TNum_{uv}$):节点 u 将在一段时间内与节点 v 交易的次数 Num_{uv} 及与其他节点交易的总次数 $TNum_{uv}$ 写入 Terrace 树中逻辑地址为 $HDT(ID_v)$的档案点.用户通过该原语将任意节点 u 与 v 在一段时间内的交易次数写入它与其他节点总交易次数保存到 Terrace 树相应的逻辑地址中;
- *Get*(ID_v,ID_u,N_u,TN_u):从 Terrace 树中逻辑地址为 $HDT(ID_v)$的档案点数据结构中读取节点 u 与节点 v 交易次数及其与其他节点交易总次数信息,并分别存入本地变量 N_u 与 TN_u 中.用户通过该原语获取任意节点 u 交易次数的相关信息;
- *Get*(ID_v,ID_u,$EVal_{uv}$):从 Terrace 树中逻辑地址为 $HDT(ID_v)$的档案点数据结构中读取节点 u 对 v 的满意度评价信息.用户通过该原语获取任意节点 u 对其他节点的满意度评价信息;
- *Get*(ID_v,T_v):从 Terrace 树中逻辑地址为 $HDT(ID_v)$的档案点数据结构中读取节点 v 的全局信任度并写入本地变量 T_v 中.用户通过该原语获取任意节点 v 的当前全局信任度;
- *ReCalFeedbackCr*(ID_v,ID_u,Cr_{uv}):计算任意节点 u 对 v 的反馈可信度的过程,并将最终结果存入本地变量 Cr_{uv} 中;
- *ReCalGlobalTrust*(ID_v,ID_u,T_v):计算任意节点 v 全局信任度的过程,并将最终结果存入本地变量 T_v 中;
- *TransFinish*(ID_v):节点每次与其他节点进行交易,最终通过该原语评估交易是否结束.ID_v 为交易对方(服务提供方),其值为 True 表示一次交易完成,否则表示未完成.

这样,任意节点 u 同时具有两个角色,即既是 P2P 网络一般用户节点,同时也是某(几)个用户节点的档案点.节点 u 作为用户节点的算法如下:

```
Procedure Evaluate(ID_v){
    If (TransFinish(ID_v)==True){
    Eval_uv←Call (1)
```

$Put(ID_v,ID_u,EVal_{uv})$;
$Get(ID_v,ID_u,N_u,TN_u)$;
N_u++;
TN_u++;
$Put(ID_v,ID_u,N_u,TN_u)$;}
$ReCalFeedbackCr(ID_v,ID_u,Cr_{uv})$;
$ReCalGlobalTrust(ID_v,ID_u,T_v)$;}

节点 u 作为档案点时求解反馈可信度算法:

Procedure $ReCalFeedbackCr(ID_v,ID_u,Cr_{uv})$**{**
$TSim=ts_0$;
$Get(ID_v,ID_u,N_u,TN_u)$;
$TNum_{uv} \leftarrow \frac{N_u}{TN_u} \times \beta^{\frac{1}{N_u}}$;
for ($k \in CSet$){
$Get(ID_v,ID_k,EVal_{kv})$;
$D_{kv} \leftarrow Call$ (2);
$TDif_{kv} \leftarrow Call$ (4);
$TSim_{kv} \leftarrow Call$ (5);
$Cr_{kv} \leftarrow Call$ (6);}}

节点 u 作为档案点时求解全局信任度算法:

Procedure $ReCalGlobalTrust(ID_v,ID_u,T_v)$**{**
for ($k \in FSet$){
$Get(ID_v,ID_u,EVal_{uv})$;
$Get(ID_v,T_v)$;
$D_{kv} \leftarrow Call$ (2);
$Cr_{kv} \leftarrow ReCalFeedbackCr(ID_v,ID_k,Cr_{kv})$;}
$T_v \leftarrow \sum_{j \in FSet} D_{ji} \times Cr_{ji} \times T_j$;}

由以上分析可知,节点 u 与节点 v 发生交易后,通过 $Put(ID_v,ID_u,EVal_{uv})$将 u 对 v 的满意度评价信息 $EVal_{uv}$ 写入 v 的档案点,通过 $Get(ID_v,ID_u,N_u,TN_u)$获取节点 u 与 v 的交易次数及总交易次数信息后,对该信息进行更新,然后利用原语 $Put(ID_v,ID_u,N_u,TN_u)$将更新后的 N_u 与 TN_u 分别写入 v 的档案点.之后便触发了两个过程: $ReCalFeedbackCr(ID_v,ID_u,Cr_{uv})$与 $ReCalGlobalTrust(ID_v,ID_u,T_v)$,计算得到节点 v 的最终全局信任度.

在EigenTrust中,任意节点 i 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信任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 $O(n^2)$.消息开销造成该协议仅仅适用于小规模网络.

在本文实现的 FCTrust 算法中,节点 v 的信任度的重新计算仅需要利用原语 $Get(ID_v,T_v)$获取所有与 v 有过交易的其他节点的全局信任度,以及利用 $ReCalFeedbackCr(ID_v,ID_u,Cr_{uv})$获取节点反馈节点的推荐可信度信息.交易结束后,利用 $Put(ID_v,ID_u,EVal_{uv})$与 $Put(ID_v,ID_u,N_u,TN_u)$将评价信息与交易次数信息写入 v 的档案点,并触发全局信任度的重新计算.因此,消息复杂度为 $O(n)$,其中,n 为系统规模.实际上,节点 v 的反馈节点集一般远小于网络的规模,而且只有最近一段时间内的评价与反馈才有效,因此,算法的消息开销比一般信任模型[6]要小得多(仿真见第 4.4.2 节).

4 系统性能分析

为了评估 FCTrust 信任模型的性能,本文设计了 3 组仿真实验,即模型信任度迭代收敛性仿真实验,以考察 FCTrust 的收敛性能;信任模型的消息代价仿真实验,以检验 FCTrust 迭代计算的消息成本;信任模型的有效性仿真实验,以验证 FCTrust 在抑制恶意节点攻击的有效性与健壮性.

4.1 仿真环境设置

本文的仿真实验的背景是 P2P 网络下的文件共享应用.仿真的网络环境为:节点总数为 1 000 个,文件个数为 10 000 个,文件在各节点均匀随机分布,正常节点的度数为 3,恶意节点的度数为 6,各参数的具体设置见表 2.仿真中,假设能对系统中的所有文件成功定位,并且系统中每一个文件都至少被一个正常节点拥有.同时,假设对于新节点有 10%的被选择概率.本文仿真了 100 个查询周期,每个节点在整个仿真过程中可完成 100 次交易.

Table 2 Simulation parameter settings

表 2 仿真参数设置

Notations	Parameter descriptions	Initial values
N	Total number of peers in community	1 000
N_f	Total number of files	10 000
P_{res}	Possibility responding the service request	1
Nd	Degree of the normal peer	3
Md	Degree of the malicious peer	6
β	Transaction density regulatory constant	0.5
TTL	Forwarding depth of the recommendation link	4
θ	The maximum deviation one peer allows for the other	0.1

为了便于对比,我们还实现了 EigenTrust 模型及窦文的模型(记为 Douwen).同时,我们还对 P2P 系统中未使用任何信任模型的情况进行了仿真实验,在这种情况下,节点每次随机选取下载源进行下载,记为 NoTrust.实验的仿真硬件平台配置为 AMD Athlon™ 64 X2 Dual 1.9GHZ,1GMB 内存;仿真软件基于 Java 实现.

4.2 节点类型定义

P2P 网络中的节点分为两大类:正常节点和恶意节点.正常节点无论在提供服务(上载)上还是在对其他节点的反馈评价上都是真实的.恶意节点不提供真实的(上载)服务,或对其他节点提供不诚实的信任反馈,甚至诋毁正常节点.为了评估 FCTrust 信任模型遏制恶意节点攻击的有效性,我们构造了以下几类恶意节点:

(1) 简单的恶意节点:这是最基本的一类恶意节点,即只提供恶意服务的节点,记为 SMS(simply malicious peer);

(2) 不诚实推荐节点:这类节点只提供不诚实推荐,包括两种类型,即夸大推荐与诋毁反馈(统一记为 simply malicious recommendation peer,简称 SMR).这类节点没有形成协同作弊的团体,其恶意行为完全是各节点的单一表现;

(3) 协同的恶意节点:此类恶意节点形成了协同作弊的团体,为内部成员提供真实服务,并夸大团体内同伙的信任评价,但是对团体外部节点提供虚假服务,并诋毁其信任评价.这类节点我们记为 CM(collusive malicious peer);

(4) 策略型恶意节点:策略型恶意节点可分为许多种,这里我们考察其中一种典型的策略型节点:节点视情况以不同的概率提供可信服务,信任度高时以较低概率提供可信服务;当信任度低时又以较高概率提供可信文件,从而使自己的信任度始终维持在系统规定的可信门限之内,企图不被信任系统觉察.我们记此类节点为 SMP(strategic malicious peer).

4.3 性能评价指标

实验中,为了评估 FCTrust 信任模型的性能,我们设定了几项评价指标,它们分别为成功交易率、收敛速度、平均消息代价和系统信任误差度.

成功交易率(successful transaction rate,简称 STR),即整个系统成功交易次数在所有交易次数中所占的比例,

在上述的仿真实验案例下,STR 直观地反映了信任模型的应用效果.

收敛速度体现了信任模型信任聚合的速度.当系统处于初始状态时,所有节点的全局信任度相等,节点选择下载源具有随机性.经过一段时间的交易,正常节点获得高的信任度,被选作下载源的可能性增大,网络的成功交易率维持在较高的水平;反之,恶意节点则受到信任模型的抑制和惩罚,其信任度被限定在较低的水平(以很高的概率低于正常节点的信任度).基于此,在仿真实验中,我们可以利用网络中所有正常节点总的失败下载的次数随仿真周期的变化规律来反映信任模型的收敛速度.随着节点交易的进行,信任模型经过一定的迭代周期,各节点的信任度出现明显的差异.服务质量好、信任度高的正常节点具有更高的机会被选为下载源,网络中失败下载次数逐渐趋近于 0.如果经过较少的周期,网络中失败下载的次数便趋近于 0,说明算法收敛较快;反之则说明模型收敛较慢.我们引入符号 TID(total inauthentic downloads)表示每个仿真周期结束时统计所有正常节点所观察到的总的失败下载次数.除此之外,通过在不同系统规模变化的条件下,观察信任模型迭代计算收敛所需的迭代次数(convergence iteration number,简称 CIN),也能反映模型的收敛效果.因此,本文利用这两项指标来评价 FCTrust 的收敛性能,详见第 4.4.1 节的仿真实验.

消息代价是指在信任维护与管理过程中,所有与信任信息操作相关查询、定位及读写操作所引起的消息负载的总和.该项指标体现了信任模型在实施具体的信任度求解及更新过程中所涉及的信任度相关操作的成本.对 FCTrust 而言,主要体现了下列过程实施中所消耗的消息成本:当节点在实施交易之前,对节点信任度的查询定位;交易后,利用一系列原语(如第 3.3 节中的 $Put(ID_v,ID_u,EVal_{uv})$与 $Get(ID_v,ID_u,N_u,TN_u)$等原语)对各节点的信任度进行求解更新.本文中,我们利用每个节点的平均消息代价(average message transmission counts per peer,简称 AMTCP)来描述系统在进行信任迭代过程中单个节点所承担的平均消息代价,反映了信任模型分布求解时每个节点的平均消息消耗成本,可作为信任模型消息代价的评价指标.

为了评估 FCTrust 信任模型在信任评估过程中的准确性,我们引入系统信任误差度指标,它用来描述系统中所有节点平均信任评价误差水平,记为 TAE(trust aggregation error).我们定义系统当前的 TAE 为

$$TAE=\sqrt{\frac{\sum((T_i-T_i')/T_i)^2}{n}} \tag{9}$$

其中,T_i 与 T_i' 分别表示节点 i 的实际全局信任度和测量所得的全局信任度,n 为系统规模.TAE 的值越小,表示信任模型评估精度更高.这就意味着模型能够根据节点的实际信任等级更有效地对恶意行为进行遏制与惩罚,从而更加客观地对系统中各节点提供差异化的服务.因此,本文中将其作为我们评价模型有效性的一项指标.

4.4 仿真实验

4.4.1 FCTrust 的收敛性仿真实验

该实验主要考察 FCTrust 信任模型在信任迭代计算中的收敛性能.我们从两个方面进行仿真实验:一是评估 FCTrust 信任模型收敛所需迭代次数(CIN)随系统规模的变化关系;二是检验交易失败总次数(TID)随迭代周期的变化规律.

实验 1. CIN 随系统规模变化仿真.

为了便于比较,我们还对 EigenTrust 进行了仿真.从图 3 可以看出,随着系统规模的变化,FCTrust 收敛迭代的次数远远小于 EigenTrust 对应的次数.在迭代开始时,两者对应的初始值基本相同.随着迭代规模的增大,FCTrust 对应的 CIN 对系统规模变化不太敏感,变化幅度不大,伸缩性较强.当系统规模达到 4 000 时,FCTrust 对应的 CIN 为 33,与其初始值相差不大.而 EigenTrust 的 CIN 对系统规模较为敏感,一直有较大的增幅.当系统规模达到 4 000 时,其对应的 CIN 为 380,这验证了 FCTrust 的收敛性能明显优于 EigenTrust.

实验 2. TID 随仿真周期的变化仿真.

图 4 给出了在网络中 SMS 类恶意节点数占 40%的情况下,分别使用 3 种信任模型选择下载源时,交易(下载)失败总次数 TID 趋于 0 的速度.可以看到,使用 FCTrust 信任模型,随着迭代周期的进行,对应的 TID 从第 3 个周期就表现出明显的优势,到第 35 个周期,其对应的 TID 就趋近于 0,几乎完全遏制了 SMS 类恶意节点的不良行为,使失败下载情况不再发生.这进一步说明,FCTrust 信任模型在收敛效率与抑制 SMS 类恶意节点的效果(这一

点在第第 4.4.3 节仿真实验中有专门分析)上其性能优于 EigenTrust 模型与 Douwen 模型.

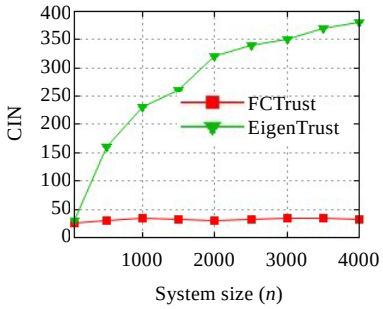

Fig.3 Varying tendency of CIN with system size

图 3 CIN 随系统规模的变化规律

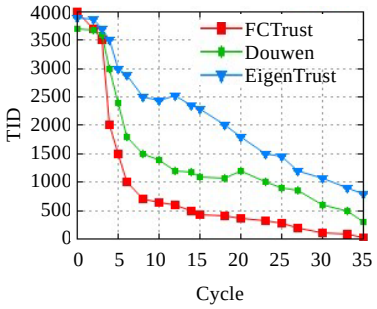

Fig.4 Varying tendency of TID with simulation cycle

图 4 TID 随仿真周期的变化规律

4.4.2 消息代价仿真实验

实验 3. AMTCP 随仿真周期的变化仿真.

图 5 给出了 3 种模型条件下节点的平均消息成本随模型迭代周期的变化规律.从图中可以看出,FCTrust 的平均消息代价随着迭代的进行基本上呈线性的规律上升;Douwen 的变化趋势与 FCTrust 基本相近,其对应的 AMTCP 比 FCTrust 稍高,但不是很明显.与 Douwen 模型相比,虽然 FCTrust 信任模型中因为引入了反馈可信度,在迭代计算中 $Put(ID_v,ID_u,Num_{uv},TNum_{uv})$原语和 $Get(ID_v,ID_u,N_u,TN_u)$原语的操作会增加一部分消息成本,但由第 3.1 节中对信任度存储机制的改进,信任信息的查找路由效率更高,因而其消息成本相对降低.上述仿真结果很好地验证了这一点.EigenTrust 对应的 AMTCP 随迭代周期上升很快,也验证了我们在第 3.3 节中所作的分析.

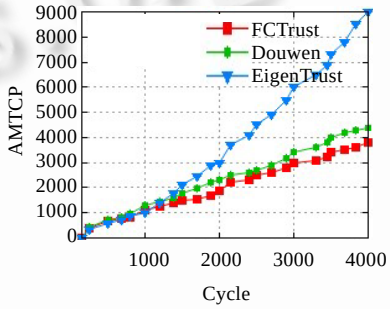

Fig.5 Varying tendency of AMTCP with simulation cycle

图 5 AMTCP 随仿真周期的变化规律

4.4.3 FCTrust 的有效性仿真实验

实验 4. SMS 类仿真及讨论.

SMS 类仿真是指网络中的恶意节点都为 SMS 类.该实验主要是为了检验不同规模的 SMS 类节点对本文提出的信任模型 FCTrust 的影响.为了便于比较,我们还在同样的条件下对 Douwen,EigenTrust 及 NoTrust 进行了仿真.从图 6 可以看出,在系统中没有恶意节点时,STR 都可以达到将近 100%.随着 SMS 类恶意节点数的增多,NoTrust 曲线下降得最快,当 SMS 节点数达到 50%时,它对应的 STR 只有将近 20%.其他 3 种模型中,Douwen 与 FCTrust 在抑制 SMS 类节点的性能方面相近,EigenTrust 的效果与前两者有一定的差距,当 SMS 节点达到 50%时,其对应的 STR 不足 50%,而前两者相应的值则为 75%左右.上述结论验证了我们的 FCTrust 信任模型在抑制 SMS 类节点的恶意行为上的有效性.这是因为 EigenTrust 模型假设了一个亚可信节点集合 P(EigenTrust 通过该假定确保迭代的收敛.本实验将 P 的规模设为 100,其信任

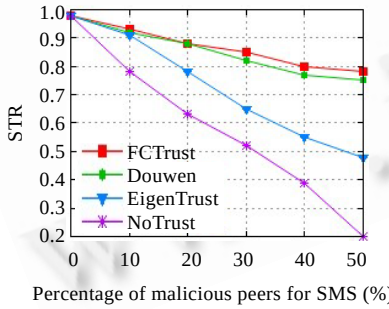

Fig.6 Varying tendency of STR with the percentage of SMS peers

图 6 STR 随不同规模的 SMS 的变化规律

度始终保持为 0.5),因而系统初起时,节点具有较小的盲目性,因此,其 STR 与 FCTrust 相当.然而在网络中,固定部分节点具有先天的较高的信任度,这一假定本身在实际中是不合理的,也较难操作.同时,由于 EigenTrust 的模型缺乏对恶意节点的惩罚,所以,随着 SMS 节点的比例增高,其 STR 也有较大幅度的下降.而对于 Douwen 模型,它与 FCTrust 模型属于同一类信任模型,在识别并抑制 SMS 上功效相近,仿真中也说明了这一点.

实验 5. SMR 类仿真及讨论.

SMR 类节点恶意行为具有一定的隐蔽性,它作为服务提供者是为节点提供对之交易过的正常节点提供真实的服务,从而维持一定的信任度,但作为推荐者角色时却提供不诚实的推荐.这类节点试图通过提供不诚实推荐的方式来扰乱信任模型的正常工作,企图破坏网络的有效性.对于不同规模的 SMR 类节点,我们的实验结果如图 7 所示.由于 EigenTrust 只是简单地将“服务质量”代替“反馈质量”,没有“反馈可信度”的概念,因此不诚实推荐对其影响不是十分明显.对 FCTrust 而言,从图 7 可以看出,随着 SMR 类节点的比例不断增高,其 STR 有一定程度的下降,但下降规模不是很大.当 SMR 节点比例达到 50%时,对应的 STR 仍可达到将近 88%,这个结果很好地验证了本文的第 3.3 节所讨论的 FCTrust 能够有效抑制不诚实反馈的结论.而对于 Douwen 模型,因为该模型中在设计时考虑了恶意节点诋毁与夸大对信任模型的影响,因而在系统 50%的节点为 SMR 类节点时,其 STR 仍可达到 81%.为了进一步说明 FCTrust 模型处理 SMR 类恶意节点的有效性,我们考察了系统信任误差度(TAE)随 SMR 类节点的变化规律,实验结果如图 8 所示.由图 8 可以看出,FCTrust 模型在整个仿真过程中对应的 TAE 最小,说明在 SMR 类恶意节点条件下,由于考虑了反馈可信度,FCTrust 模型的信任评估准确度更高,其信任评价更能反映节点的实际信任状况,能够更有效地对 SMR 类恶意节点进行识别,因而在遏制 SMR 类节点的恶意行为中表现出更高的有效性.

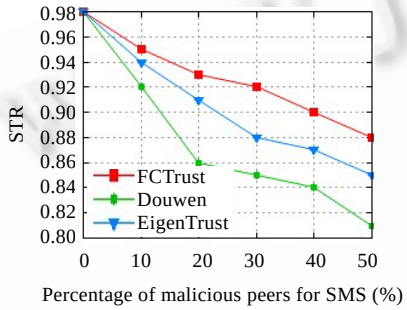

Fig.7 Varying tendency of STR with the percentage of SMR peers

图 7 STR 随不同规模的 SMR 的变化规律

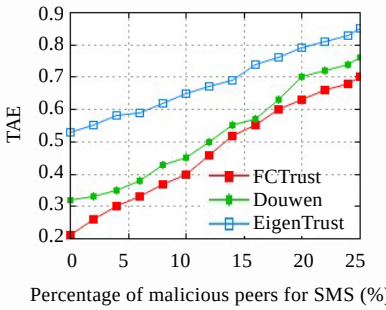

Fig.8 Varying tendency of TAE with the percentage of SMR peers

图 8 TAE 随不同规模的 SMR 的变化规律

实验 6. CM 类仿真及结论.

CM 类恶意节点彼此“相识”,它们具有更强的协同作弊能力.从图 9 可以看出,随着 CM 类节点的增加,恶意节点很容易获取较高的信任度.由于 EigenTrust 缺乏惩罚机制,造成系统的有效交易(下载)明显下降.与之相反,由于在我们的 FCTrust 模型中引入了反馈可信度机制,可对协同作弊节点夸大组内成员的信任度而诋毁组外节点信任度的恶意行为进行有效的识别并给予相应的惩罚,从而保证协同作弊中的恶意节点夸大与诋毁行为被明显抑制,使 STR 维持在一个较高的水平.而因为 Douwen 信任模型中集成了应对协同作弊的惩罚机制,使它与 EigenTrust 比较也能达到一个较好的效果.如图 9 所示,当 CM 类恶意节点达到 50%时,其对应的 STR 仍能达到 85%,而 Douwen 与 EigenTrust 模型对应的值分别为 65%和 35%.以上仿真结果验证了 FCTrust 在应付协同作弊的恶意节点攻击所表现的健壮性与有效性.为了进一步说明 FCTrust 模型在抑制 CM 类节点恶意行为的有效性,我们考察了 FCTrust 与 EigenTrust 模型在不同规模的 CM 类节点(2%与 10%的 CM 类节点)条件下,系统信任误差度(TAE)随 CM 类节点组规模的变化规律,实验结果如图 10 所示.由图 10 可以看出,在两种规模的 CM 类节点环境下,随着协同作弊组规模的增大,FCTrust 模型对应的 TAE 曲线均位于 EigenTrust 之下,说明 FctTrust 模型对

应的系统信任误差度均小于 EigenTrust 的对应值,其精度更高,抑制 CM 类恶意节点的有效性与健壮性也更强.

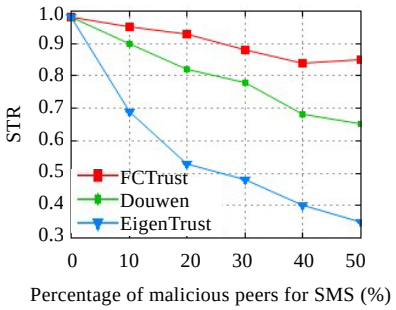

Fig.9 Varying tendency of STR with the percentage of CM peers

图 9 STR 随不同规模的 CM 的变化规律

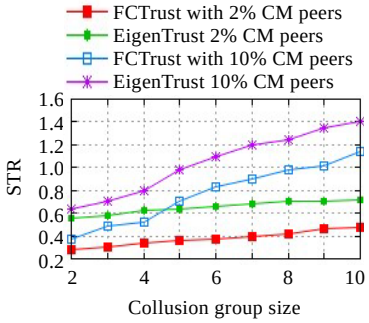

Fig.10 Varying tendency of TAE with collusion group size

图 10 TAE 随协同作弊组规模的变化规律

实验 7. SMP 类仿真及结论.

图 11 对比了 3 种模型在 SMP 类策略型恶意节点攻击下 STR 的变化情况,仿真中假设若信任度低于 0.5 则为不可信节点,同时假设策略恶意节点在其信任度高于 0.6 时以 0.2 的概率提供可信上载服务,在信任度低于 0.6 时以 0.6 的概率提供真实服务.从图 11 可以看出,FCTrust 与 Douwen 模型的变化趋势基本相同,所对应的 STR 也较为接近,当 SMP 类节点比例达到 50%时,FCTrust 与 Douwen 模型对应的 STR 分别为 0.78 与 0.72,FCTrust 的有效性略优于 Douwen.而对于 EigenTrust,由前面分析可知,由于 EigenTrust 对恶意节点缺乏足够的惩罚机制,在应付 SMP 类策略型节点攻击时更显现出它的劣势,图 11 的仿真结果较好地印证了这一点.

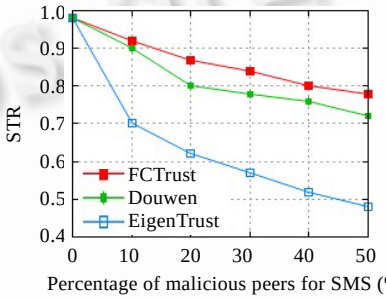

Fig.11 Varying tendency of STR with the percentage of SMP peers

图 11 STR 随不同规模的 SMP 的变化规律

5 结论及下一步工作

本文提出了一种 P2P 环境下基于反馈可信度的全局信任模型,给出了该模型的数学分析及分布式实现方法,并对其信任存储机制进行了改进.分析和仿真结果表明,该模型较已有的全局信任模型在遏制更广泛类型的恶意节点攻击的有效性、迭代计算的收敛性及消息成本上有较大提高.

本文的研究并未考虑 P2P 信任存储机制的安全性,这是决定该模型是否能在实际环境中成功应用的关键因素;另一个需要进一步关注的是如何结合本文提出的信任机制进一步研究相应的激励机制,不仅对系统中表现好的节点予以奖励(赋予更高的信任度和权限),而且对恶意节点实施更加严厉的惩罚(使其信任度降到一个很低的水平,并且无法获取一定质量的服务).这两方面是下一步研究的重点.

致谢 在此,我们向对本文工作给予支持的同行表示感谢,感谢他们对本文提出的深入而有建设性的改进意见,并对本文审稿人的辛勤工作表示感谢.

References:

[1] Zhang Q, Sun Y, Liu Z, Zhang X, Wen XZ. Design of a distributed P2P-based grid content management architecture. In: llow J, ed. Proc. of the 3rd Communication Networks and Services Research Conf. New York: IEEE Press, 2005. 339−344.

[2] Adar E, Huberman A. Free riding on Gnutella. Technical Report, CSL-00-3, Palo Alto: Xerox PARC, 2000.

[3] Dou W, Wang HM, Jia Y, Zhou P. A recommendation-based peer-to-peer trust model. Journal of Software, 2004,15(4):571−583 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/571.htm

[4] Khambatti M, Dasgupta P, Ryu KD. A role-based trust model for peer-to-peer communities and dynamic coalitions. In: Cole JL, Wolthusen SD, eds. Proc. of the 2nd IEEE Int'l Information Assurance Workshop. New York: IEEE Press, 2004. 141−154.

[5] 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.

[6] Kamwar SD, Schlosser MT, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. In: Proc. of the 12th Int'l Conf. on World Wide Web. Budapest, 2003. 640−651. http://www.eecs.harvard.edu/~michaelm/CS222/eigentrust.pdf

[7] Aberer K, Despotovic Z. Managing trust in a peer-to-peer information system. In: Proc. of the 10th Int'l Conf. on Information and Knowledge Management (ACM CIKM). New York, 2001. 310−317. http://lsirpeople.epfl.ch/despotovic/CIKM2001-trust.pdf

[8] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities. IEEE Trans. on Data and Knowledge Engineering (Special Issue on Peer-to-Peer Based Data Management), 2004,16(7):843−857.

[9] Marsh S. Formalising trust as a computational concept [Ph.D. Thesis]. Scotland: University of Stirling, 1994.

[10] Abdul-Rahman AHS. A distributed trust model. In: Proc. of the 1997 New Security Paradigms Workshop. Cunbria: ACM Press, 1998. 48−60. https://eprints.kfupm.edu.sa/17505/1/17505.pdf

[11] Golle P, Leyton-Brown K, Mironov I. Incentives for sharing in peer-to-peer networks. In: Wellman MP, Shoham Y, eds. Proc. of the 3rd ACM Conf. on Electronic Commerce. New York: ACM Press, 2001. 264−267.

[12] Buragohain C, Agrawal D, Suri S. A game theoretic framework for incentives in P2P systems. In: Shahmehri N, Graham RL, Carroni G, eds. Proc. of the 3rd Int'l Conf. on Peer-to-Peer Computing (P2P 2003). Los Alamitos: IEEE Press, 2003. 48−56.

[13] Bonacich P, Lloyd P. Eigenvector-Like measures of centrality for asymmetric relations. Social Networks, 2001,23(4):191−201.

[14] Shi WM, Yang HF, Wu YS, Sun X. Numerical Analysis. 2nd ed., Beijing: Beijing Institute of Technology Press, 2004. 91−93 (in Chinese).

[15] Zhang Q, Zhang X, Wen XZ, Liu JR, Ting S. 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

附中文参考文献:

[3] 窦文,王怀民,贾焰,邹鹏.构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型.软件学报,2004,15(4):571−583. http://www.jos.org.cn/1000-9825/15/571.htm

[14] 史万明,杨骅飞,吴裕树,孙新.数值分析.第 2 版,北京:北京理工大学出版社,2004.91−93.

[15] 张骞,张霞,文学志,刘积仁,Ting S.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

胡建理(1976－),男,湖北武汉人,博士,工程师,CCF 会员,主要研究领域为分布式计算,信息安全.

周斌(1971－),男,博士,副研究员,主要研究领域为分布式计算,Web 服务,网络安全.

吴泉源(1941－),男,教授,博士生导师,主要研究领域为分布式计算,人工智能,专家系统.

刘家红(1980－),男,博士生,CCF 学生会员,主要研究领域为分布式计算,面向服务的计算,事件流处理.