一种激励相容的P2P信誉模型

胡建理[1] 周 斌[2] 周 瑜[3] 吴泉源[2]
(广州军区广州总医院信息科 广州 510010)[1] (国防科学技术大学计算机学院 长沙 410073)[2]
(广西桂林76140部队 桂林 541001)[3]

摘 要 针对现有的信任模型不能很好地处理P2P网络环境中恶意节点提供虚假服务的欺诈行为,及不积极提供诚实推荐的问题,提出了一种激励相容的P2P信誉模型(简称ICRM)。该模型使用时间区间的概念来标示经验和推荐的时间特性,利用直接信任度、推荐信任度及推荐可信度等机制来精确描述节点的实际信任等级,并引入参与层次来度量节点提供推荐的积极程度,从而有效地识别与抑制不同类型的恶意节点,激励节点积极提供诚实推荐。仿真实验表明,ICRM能够有效地抑制恶意节点的欺诈行为及不诚实反馈行为,并能有效解决节点推荐积极性不高的问题。

关键词 对等网络,信誉模型,激励相容机制,推荐可信度
中图法分类号 TP393 **文献标识码** A

Incentive Compatible Reputation Model for P2P Networks

HU Jian-li[1] ZHOU Bin[2] ZHOU Yu[3] WU Quan-yuan[2]
(Information Department of Guangzhou General Hospital under Guangzhou Area Command, Guangzhou 510010, China)[1]
(School of Computer, National University of Defense Technology, Changsha 410073, China)[2]
(Unit 76140 of PLA, Guilin 541001, China)[3]

Abstract An important challenge regarding peer's trust valuation in peer-to-peer(P2P) networks is how to cope with such issues as the fraudulent behaviors and the dishonest feedback behaviors from malicious peers, and the issue of inactive recommendations to others. However, these issues cannot be effectively addressed by the existing solutions. Thus, an incentive compatible reputation management model for P2P networks, named ICRM, was proposed to solve them. In ICRM, the metric of time zone is used to describe the time property of the transaction experience and the recommendation. Three other metrics such as the direct trust value, the recommendation trust value and the recommendation credibility, based on the metric of time zone are applied to express accurately the final trust level of a peer. Furthermore, the participation level is introduced as the metric to identify a peer's activeness degree. Theoretical analysis and simulation experiments demonstrate that, ICRM can effectively suppress the malicious behaviors such as providing unreliable services, or giving dishonest feedbacks to others in the P2P networks. What's more, it also can incent peers to offer recommendations to others more actively.

Keywords P2P, Reputation model, Incentive compatible mechanism, Recommendation credibility

1 引言

近年来,P2P技术在文件共享、分布计算、电子市场和信息管理领域获得了广泛的应用。但P2P系统由于开放和动态的本质,其收益与风险并存。已有的工作[1-5]显示,建立有效的基于信誉的信任模型能够成功地规避风险。但现有的多数基于信誉的信任模型不能准确地反映节点实际的信任状况,不能有效激励节点积极提供诚实推荐。

针对传统信任模型的不足,本文旨在建立一种P2P网络环境下激励相容的信誉管理模型ICRM。ICRM使用时间区间的概念来标示经验和推荐的时间特性,充分考虑不同信任的来源及机理,使用直接信任度、推荐信任度及推荐可信度来精细刻画各种信任之间的差异,精确描述节点的实际信任等级,并引入参与层次来度量节点是否积极提供推荐,从而有效地识别与抑制不同类型的恶意节点,激励节点积极提供诚实推荐,促进P2P系统的健康运行和良性发展。分析与仿真实验表明,ICRM模型不仅可以有效地抑制恶意节点的欺诈行为,而且可以激励节点积极提供诚实推荐。

到稿日期:2010-11-25 返修日期:2011-02-24 本文受广州市科技计划项目(2010Y1-C971),广东省自然科学基金博士启动项目基金(9451001002003920),国家自然科学基金(60873204),国家973重点基础研究发展规划项目基金(2005CB321800),国家863高技术研究发展计划项目基金(2007AA010301)和国家杰出青年科学基金(60625203)资助。

胡建理(1976—),男,博士,工程师,CCF会员,主要研究方向为分布式计算、信息安全等,E-mail:lxman82@gmail.com;周 斌(1971—),男,博士,副研究员,硕士生导师,主要研究方向为分布式计算、Web服务、网络安全;周 瑜(1977—),男,工程师,主要研究方向为Web服务、网络安全等;吴泉源(1941—),教授,博士生导师,主要研究方向为人工智能、Web服务和信息安全等。

本文第 2 节分析了相关工作；第 3 节给出了信任评价算法及数学表述；第 4 节阐述了基于推荐可信度的激励机制；第 5 节对信誉模型进行了仿真实验及结果分析；最后总结全文并指出下一步的研究工作。

2 相关工作

围绕如何更为合理准确地刻画节点的信任，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。在已有信任模型中，基于信誉的信任建模是目前研究人员关注得比较多的一个方向。Li Xiong 提出 PeerTrust[2,5]，从多个角度对 P2P 中的信誉构造进行了论述，其模型考虑全面，引入了节点对交互的反馈、反馈的可信度、节点参与交互的次数、交易的属性和节点所在社区多个因素度量节点的可信程度；Yao Wang 提出基于 Bayesian Network 的信誉模型[6]；Cornelli 则针对 Gnutella 中的信誉管理机制进行改进，提出了 P2PRep[7] 及改进的 XRep[8]；Yu 和 Singh 通过社会机制实现了信誉管理[9]；Kamvar 等人采用社会网络分析中的基于节点入度(in-degree)的中心性测量方法(Centrality Measurement)[10]，提出了基于推荐的全局信誉模型 EigenTrust[1]。但这类模型主要是为抑制 P2P 网络中某种特定的恶意行为而提出的，较少考虑对节点积极诚实推荐的激励问题，激励效果不足。

激励机制应当对积极提供诚实推荐的节点给予奖励，对不愿意提供推荐和提供不诚实推荐的节点予以惩罚，进而引导节点以我们希望的积极诚实的方式参与到信誉系统中。提供激励的方法的目的是如何使信誉机制激励相容(incentive-compatible)[4]，也就是说，如何使积极诚实的提供推荐是理性节点的最优选择，以符合其自身利益最大化的要求。这类方法近年来得到了广泛的研究，现有的鼓励节点积极提供诚实推荐的激励机制可以分为两类[2]：基于微支付的激励机制[11]和基于信誉的激励机制。在基于微支付的激励机制中，节点接受服务需支付一定的虚拟货币，提供服务或推荐可以获得虚拟货币。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，其不具有工程可行性[12]。

基于信誉的激励机制的特点是，根据节点在参与信誉系统中的行为表现，即是否积极提供诚实推荐，通过一定的策略来引导节点按照系统所期望的方式参与到信誉系统中。然而当前对基于信誉的激励机制的研究存在的局限性主要体现在，往往只是将信誉作为服务选取的依据，而较少考虑将其作为提供服务反馈的依据。因此，为了解决这一问题，本文提出一种激励相容的 P2P 信誉模型，引入推荐可信度及参与层次机制，并以此作为节点是否积极提供诚实推荐的依据，激励节点积极提供诚实推荐。

3 信任评价算法

定义 1(节点信任度) 节点信任度由两部分组成，即直接信任度与推荐信任度。直接信任度是评价主体依据其与客体的直接交互经验对评价客体的信任评价；推荐信任度是由评价主体根据推荐节点提供的评价信息形成的对客体的信任评价。用 i,j,k 分别表示评价主体、评价客体与推荐实体，用 T_{ij} 表示节点 i 对节点 j 的信任度，其计算公式为：

$$T_{ij}=\begin{cases}\alpha * D_{ij}+(1-\alpha) * R_{ij}, & K\neq\phi,\alpha\in[0,1]\\ 0.5, & K=\phi,D_{ij}=0\end{cases} \tag{1}$$

式中，D_{ij} 表示节点 i 对节点 j 的直接信任度，R_{ij} 表示节点 i 对节点 j 的推荐信任度，K 为推荐节点集合，α 为信任度调节因子。在 ICRM 中，规定新加入系统的节点的信誉度为 0.5，文献[13]中指出 P2P 系统中恶意节点毕竟还是少数，因此对新加入节点的猜疑是导致系统整体性能不高的缘由，由于节点动态地加入或者离开，在证实新节点不可信之前部分相信它将会使系统更有效。

定义 2(时间衰减函数) 为了提高信任评价的准确性和动态适应能力，把一段时间分为若干个时间区间，设为 $t_1,t_2,\cdots,t_n$，时间帧长度可以根据具体的应用场景来确定。定义第 k 个时间区间内发生的交易在计算信任度时相比当前的时间区间(第 n 区间)的交易折扣幅度函数称为衰减函数，表示为：

$$g(k)=g_k=\rho_{fade}^{n-k}\quad \rho_{fade}\in(0,1)\cap k\in[1,n] \tag{2}$$

式中，ρ_{fade} 为时间衰减率。

定义 3(直接信任度) 节点交互之后彼此提交满意度的评价，可将节点 i 对节点 j 交互满意度的评价定义为 Map 函数 $f(i,j)$：

$$f(i,j)=\begin{cases}1, & \text{totaly satisfactory}\\ 0, & \text{tataly unsatisfactory}\\ e(\in(0,1)), & \text{else}\end{cases} \tag{3}$$

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。

在时间区间 t 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：

$$D_{ij}^t=\begin{cases}\dfrac{\sum_{k=1}^{m}f(i,j)}{m}, & m\neq 0\\ 0, & m=0\end{cases} \tag{4}$$

为了准确地计算节点信任度，信任模型必须区分不同时期交易对计算信任度的影响。目前比较一致的做法是为不同时期的交易按当前距离的远近程度分配不同的权重，距离目前越近，赋予的权重越高；距离目前越远，给予的权重越小。因此，利用式(2)所定义的衰减函数 $g(k)$，赋予新的信任评价经验更高的权重，定义直接信任度模型为：

$$D_{ij}=\frac{\sum_{k=1}^{n}g_k * D_{ij}^k}{\sum_{k=1}^{n}g_k} \tag{5}$$

式中，$g(k)=\rho_{fade}^{n-k}$ 是时间区间 t_k 内交易的衰减因子，且 $0<f_k<f_{k+1}<1,1\leqslant k<n$。

定义 4(推荐信任度) 推荐信任度是由评价主体综合各推荐节点提供的直接信任评价形成的对客体的信任评价。影响推荐信任度的因素包括推荐节点提供的对评价客体的直接信任度及推荐节点的推荐可信度，另外它还具有时间相关性，即推荐节点近期推荐行为的信任程度更高。因此，将节点 i 对节点 j 的推荐信任度定义为：

$$R_{ij}=\frac{\sum_{k\in K}D_{kj} * Cr_k * g_k}{\sum_{k\in K}Cr_k * g_k} \tag{6}$$

式中，K 为推荐节点集合。

定义 5(推荐可信度) 推荐可信度用来描述推荐节点提供的节点信任信息真实准确的信心指标。设 Cr_{ij}^t 为第 k 次推荐后节点 i 对节点 j 的可信度，则：

$$Cr_{ij}^{k+1}=\begin{cases}Cr_{ij}^{k}+\delta(1-Cr_{ij}^{k})(1-\varepsilon), & 0\leqslant\varepsilon\leqslant 1,k>0\\ Cr_{ij}^{k}-\gamma Cr_{ij}^{k}(1-1/\varepsilon), & \varepsilon>1,k>0\\ 1/2, & k=0\end{cases}\quad(7)$$

式中，参数 $0<\delta<\gamma<1$，k 为推荐次数；$\varepsilon=|R_{ij}^{k}-D_{ij}^{k}|/s_{ij}$，$s_{ij}$ 为所有推荐节点对节点 j 的直接信任度的标准偏差。推荐可信度计算模型能够有效标识出不诚实节点。

4 基于推荐可信度的激励机制

在对 ICRM 模型进行适当扩展的基础上，通过一个相对公平的服务区分机制来激励节点积极诚实提供推荐。服务区分机制定义了两个服务区分参数：参与层次和推荐可信度（参见定义 5），参与层次度量节点提供推荐是否积极。使用参与层次和推荐可信度来标识节点提供推荐的行为特征：是否积极提供诚实推荐。

4.1 参与层次

在时间 t 时节点 i 对节点 j 的参与层次记为 l_{ij}^{t}，l_{ij}^{t} 可以使用如下步骤进行计算。

节点 i 根据推荐节点获得在 t 时间单元内节点 i 对节点 j 提供的推荐的总数，记为 I_{ij}^{t}，定义提供推荐数目的门槛值 $I_{\max}$，参与层次使用式(8)定义：

$$l_{ij}^{t}=\begin{cases}\dfrac{I_{ij}^{t}}{I_{\max}}, & \text{if } I_{ij}^{t}\leqslant I_{\max}\\ 0, & \text{else}\end{cases}\quad(8)$$

因此，节点 i 对节点 j 提供的推荐越多，其参与层次越高。当提供推荐的数目到达指定的门槛值 $I_{\max}$ 时，其参与层次达到最大值 1；当 I_{ij}^{t} 等于 0 时，也就是节点 i 没有为节点 j 提供推荐信息，可以赋予 l_{ij}^{t} 较低的值。因此，可以在参与层次和推荐可信度这两个参数的基础上构造一个简单的信誉信息交换算法来实现服务区分。

4.2 信誉信息交换算法

如果节点 i 对节点 j 的参与层次 $l_{ij}^{t}>\delta_l$，则节点 i 就可以认为节点 j 是积极提供推荐的节点，δ_l 是节点是否积极提供推荐的判定门槛值，$0<\delta_l<1$。同理，如果节点 i 对节点 j 的推荐可信度 $Cr_{ij}^{t}>\delta_c$，则节点 i 就可以认为节点 j 是诚实提供推荐的节点，δ_c 是节点是否诚实的判定门槛值，$0<\delta_c<1$。

当节点 i 收到节点 j 的信誉信息查询请求时，查看其本地数据库是否有目标节点的交互评价信息，如果没有，则忽略该请求，否则根据节点 j 的参与层次和推荐可信度进行相应的处理：

(1)如果 $l_{ij}^{t}>\delta_l$ 且 $Cr_{ij}^{t}>\delta_c$，则节点 i 认为节点 j 是积极诚实提供推荐的节点，把关于目标节点的推荐发送给节点 j。

(2)如果 $l_{ij}^{t}>\delta_l$ 且 $Cr_{ij}^{t}<\delta_c$，则节点 i 认为节点 j 是积极发送不诚实推荐的节点，忽略其信誉信息查询请求。

(3)否则，节点 i 以可能性 $p=(1-\eta)*l_{ij}^{t}+\eta*Cr_{ij}^{t}$ 来提供推荐，$0\leqslant\eta\leqslant 1$，通常取 $\eta>0.5$，这样能够抑止节点偶尔的欺骗行为。

基于上述信誉信息查询处理策略，如果节点 j 在信誉系统中采用不参与的策略，则其它节点接受到来自节点 j 的信誉信息查询请求时会以较低的概率回答该请求，使得节点 j 不能获得有用的信誉信息，导致节点 j 的信誉机制不能有效发挥作用。因此，若节点 j 希望获得有用的信誉信息，就需改变它的行为，积极参与到信誉系统中来。如果节点 j 采用积极诚实的参与策略，当节点 i 接受到来自节点 j 的信誉信息查询请求时会提供推荐（如果节点 i 和被评价节点发生过交互）。如果节点 j 积极地提供不诚实的推荐，那么节点 i 就会忽略其信任查询请求。

```
Procedure ReplyRepInfo(i,δl,δc,η,l_ij^t,Cr_ij^t)
//节点 i 收到节点 j 的关于节点 s 的查询处理请求 rw(j,s,ttl,t) 时，作如下处理：
upon(receipt of a rw(j,s,ttl,t) message at peer i) do
//节点 i 的本地数据库中有和节点 s 交互的评价记录
  if(i has interacted with s in the last D time units)
//计算发送推荐的可能性 p
    if(l_ij^t>δl)
      if(Cr_ij^t>δc)
        p=1;
      else
        p=0;
    else
      p=(1-η)*l_ij^t+η*Cr_ij^t;
//以可能性 p 应答节点 j 的信任查询处理请求，发送推荐
      with(probability p) do
        rec_is^t⇐⟨D_ij^t,ρ_ij^t⟩;
        send rec_is^t to j;
      end do
    else
      ignore message;
    end if
  //如果查询深度 ttl 不等于 0，向节点 j 提供引荐
    if(ttl≠0)
      A⇐getRandomNeighbor(b); //b 为分支因子
      For each peer k in A do
  //向节点 j 发送引荐
        send a witness(s,k,t) to j;
      end do
    end if
  end do
```

5 仿真分析

本文的仿真实验背景是 P2P 网络下的文件共享应用。仿真的网络环境参数的具体设置如表 1 所列。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。

表 1 仿真参数设置

Notations	Parameter descriptions	Initial values
N	total number of peers	1000
ρ_{fade}	time fading rate	0.8
δ	credibility regulatory factor	0.4
γ	credibility regulatory factor	0.8
α	trust regulatory factor	0.5
δ_l	threshold for judging recommendation activeness	0.6
δ_c	threshold for judging peer's honesty	0.8
η	recommendation credibility weight for the challenge-response possibility	0.6
I_{max}	threshold for the number of recommendation	20

为了便于对比，我们还实现了 EigenTrust 模型。试验评估标准是成功交易率（Successful Transaction Rate，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，STR

直观地反映了信任模型的应用效果。实验的仿真硬件平台配置为 Intel(R) Pentium(R) Dual E2200@2.2GHz,2GMB 内存;仿真软件基于 Java 实现。

P2P 网络中的恶意节点根据其行为的特征划分为两大类:恶意服务节点与恶意推荐节点。恶意服务节点即专门提供恶意资源(服务)的节点,这是最基本的一类恶意节点,我们将其记为 MSP(Malicious Service Peer)。至于恶意推荐节点即向其它节点提供不诚实反馈的节点,如果将其与是否积极推荐这一标准关联,可分为 4 种情况:不积极的诚实节点(记为 IHP,Inactive Honest Peer)、不积极的不诚实节点(记为 IDP,Inactive Dishonest Peer)、积极诚实节点(记为 AHP,Active Honest Peer)和积极不诚实节点(记为 ADP,Active Dishonest Peer)。

5.1 MSP 仿真及讨论

MSP 类仿真是指网络中的恶意节点都为 MSP 类。该实验主要为检验不同规模的 MSP 类节点对本文提出的信任模型 ICRM 的影响。为了便于比较,我们还在同样的条件下对 EigenTrust 进行了仿真。从图 1 可以看出,随着 SM 类恶意节点数的增多,两类模型对应的曲线都在下降,但 ICRM 下降幅度小于 EigenTrust。当 MSP 节点数达 50%时,前者对应的 STR 约为 71%,而后者只有近 48%。上述结论验证 ICRM 信任模型在抑制 SM 类节点的恶意行为上的有效性。

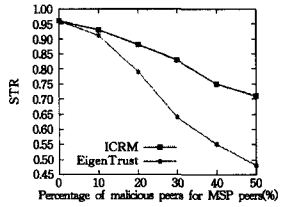

图 1 STR 随不同规模的 MSP 的变化规律

5.2 获得诚实推荐的数目

图 2 显示了 4 种不同类型的节点获得的诚实推荐数随时间的变化情况。从图中可以看出,在开始阶段 4 种类型的节点都获得很少的诚实推荐信息,在获得诚实推荐的数目上没有明显的差别。随着交互经验的累积,诚实节点具有足够的经验进行推荐,进而建立较高的推荐可信度。最终 4 种类型的节点获得的诚实推荐的数量关系为 AHP>IHP>IDP>ADP,积极诚实的节点获取最多的诚实推荐,不积极的诚实节点和不积极不诚实节点次之,积极的不诚实节点获得的诚实推荐数目最少。这使得不积极和不诚实的节点从自身利益的角度出发会改变策略,转为积极提供诚实的推荐。

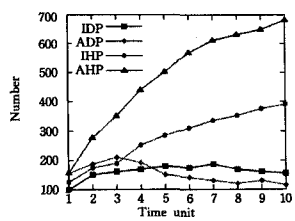

图 2 获得的诚实推荐数

5.3 错误决策数

图 3 显示了 4 种类型的节点错误的信任决策数随时间的变化情况。节点缺乏诚实的推荐会导致其作出错误的决策,如把提供高质量服务的良好行为节点划分为不良行为节点,把提供低质量服务的节点划分为良好行为节点。从图中可以看出,随着交互经验的累积,每种类型的节点其错误决策数逐渐减少,由于诚实推荐的帮助,积极提供诚实推荐的节点作出的错误决策最少,积极提供不诚实推荐节点作出的错误决策最多,它们建立了同样的数量关系 AHP<IHP<IDP<ADP。

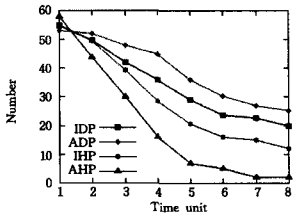

图 3 错误决策数

从上述两个实验可以看出,本章提出的激励机制能够对积极提供诚实推荐的节点提供正确的激励,因为它们总能够比不积极、不诚实的节点获得更多的好处,所以激励机制是有效的。

结束语 本文提出了一种 P2P 网络环境下激励相容的信誉模型,并对模型的实际效果进行了模拟实验,分析和仿真表明,本文提出的模型克服了已有模型的部分局限性,可以有效地遏制多种类型恶意节点的攻击行为,激励节点积极提供诚实推荐。本文的研究并未详细探讨恶意节点利用复杂的策略性行为改变及合伙欺骗方式对系统的攻击,也未具体阐明 P2P 信誉信息的分布式存储机制与信任求解算法,这些都是下一步研究的重点。

参 考 文 献

[1] Kamwar S D, Schlosser M T, Garcia-Molina H. The eigentrust algorithm for reputation management in P2P networks [C]// Proceedings of the 12th International Conference on World Wide Web. Budapest, Hungary, 2003:640-651

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

[3] Cornelli F, Damiani E, di Vimercati S D C, et al. Choosing reputable servents in a P2P network [C]// Proceedings of the 11th World Wide Web Conference. Honolulu, Hawaii, USA, 2002

[4] Dellarocas C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior [C]// Proceedings of the 2nd ACM Conference on Electronic Commerce. Minneapolis, MN, USA, 2000:150-157

[5] Xiong L, Liu L. A reputation-based trust model for peer-to-peer ecommerce communities [C]// Proceedings of the 4th ACM conference on Electronic commerce(CEC'03). San Diego, CA, US, ACM Press 2003:228-229

[6] Wang Y, Vassileva J. Bayesian Network-Based Trust Model in P2P Networks [C]// Proceedings of Agents and Peer-to-Peer Computing, Second International Workshop (AP2PC 2003). Melbourne, Australia, IEEE Computer Society, 2003:372-378

[7] Cornelli F, Damiani E, Vimercati S C, et al. A reputation-based approach for choosing reliable resources in peer-to-peer networks [C]// Proceedings of 9th ACM Conf. on Computer and Communications Security (CCS' 02). Washington DC, USA, ACM Press, 2002:207-216

[8] Dellarocas C. The Digitization of Word-of-Mouth: Promise and Challenges of Online Reputation Mechanism [J]. Management Science, 2006, 49(10): 1407-1424

[9] Yu B, Singh M P. A Social Mechanism of Reputation Management in Electronic Communities [C]// Proceedings of Fourth International Workshop on Cooperative Information Agents (CIA 2000). Boston, USA, 2000: 154-165

[10] Wasserman S. Social Network Analysis: Methods and Applications (1st ed) [M]. Cambridge: Cambridge University Press, 1994

[11] Golle P, Leyton-Brown K, Mironov I. Incentives for sharing in peer-to-peer networks[C]// Wellman MP, Shoham Y, eds. Proceedings 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[C]// Shahmehri N, Graham R L, Carroni G, eds. Proceedings of the 3rd Int'l Conf. on Peer-to-Peer Computing (P2P 2003). Los Alamitos: IEEE Press, 2003: 48-56

[13] Friedman E, Resnick P. The social cost of cheap pseudonyms [J]. Journal of Economics and Management Strategy, 2001, 10 (2): 173-199

(上接第 35 页)

两种算法的存储空间大小对比如图 3 所示。图 4 给出的是 Goodrich 认证跳表算法和 ASL-DHT 算法在元素认证时进行 Hash 计算次数的对比。

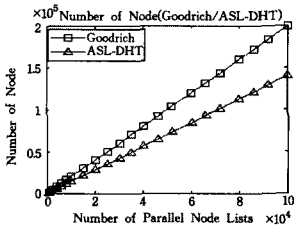

图 3 算法空间大小对比(Goodrich/ASL-DHT)

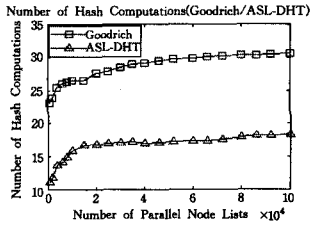

图 4 Hash 计算次数对比(Goodrich/ASL-DHT)

图 5 和图 6 给出的是 Goodrich 和 ASL-DHT 算法元素插入时更新节点数目和插入算法的运行时间对比。

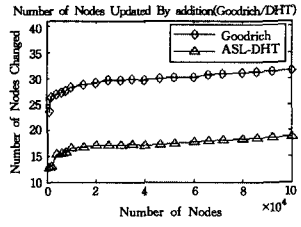

图 5 元素插入时更新节点数目对比(Goodrich/ASL-DHT)

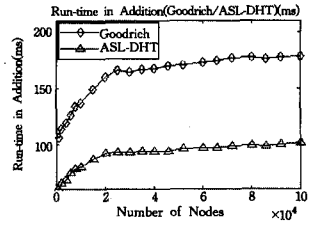

图 6 插入算法的运行时间对比(Goodrich/ASL-DHT)

Goodrich 和 ASL-DHT 算法元素删除时更新节点数目和元素删除算法的运行时间对比如图 7 和 8 所示。

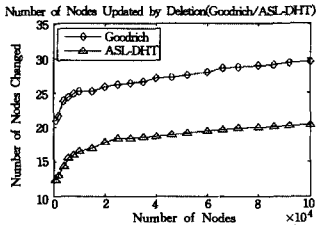

图 7 元素删除时更新节点数目对比(Goodrich/ASL-DHT)

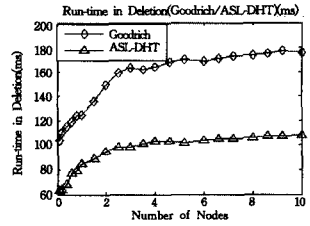

图 8 删除算法的运行时间对比(Goodrich/ASL-DHT)

以上的实验结果表明,在存储空间大小、元素插入时更新节点数目、元素插入算法的运行时间、元素删除时更新节点数目、元素删除算法的运行时间等方面,ASL-DHT 算法均优于 Goodrich 认证跳表算法。

结束语 针对 Goodrich 认证跳表算法存在的问题提出数据存储方案和哈希方案相分离的思想,并依据此思想设计并实现了一种新的基于有向哈希树的认证跳表算法,从而有效地解决了 Goodrich 认证跳表的节点哈希值冗余和节点哈希值重计算量大的问题。理论代价分析和实验比较结果表明,ASL-DHT 在存储空间大小、元素插入时更新节点数目、元素插入算法的运行时间、元素删除时更新节点数目和元素删除算法的运行时间方面都优于 Goodrich 认证跳表算法,具有很高的效率和可行性及重要的理论价值。

参 考 文 献

[1] Tamassia R. Authenticated Data Structures[C]// Proceedings of the Algorithms-ESA 2003. LNCS, September 2003: 2-5

[2] Papamanthou C, Tamassia R. Time and Space Efficient Algorithms for Two-Party Authenticated Data Structures[C]// Proceedings of ICICS 2007. LNCS, 2007: 1-15

[3] Crosby S A, Wallach D S. Super-efficient Aggregating History-independent Persistent Authenticated Dictionaries [C]// Proceedings of ESORICS 2009. LNCS, June 2009: 671-688

[4] 周永彬,卿斯汉,薛源,等. 基于时间约束的认证字典分类方法 [J]. 计算机科学,2004,31(7):20-22

[5] Muñoz J L, Forne J, Esparza O, et al. Certificate revocation system implementation based on the Merkle hash tree[J]. International Journal of Information Security, 2004, 2(2): 110-124

[6] Blibech K, Gabillon P. CHRONOS: an authenticated dictionary based on skip lists for timestamping systems[C]// Proceedings of the 2005 Workshop on Secure Web Services. ACM Press, Nov 2005: 84-90

[7] 朱勤,于守健,乐嘉锦,等. 外包数据库系统安全机制研究[J]. 计算机科学,2007,34(2):152-156

[8] 咸鹤群,冯登国. 外包数据库模型中的完整性检测方案[J]. 计算机研究与发展,2010,47(6):1107-1115

[9] Goodrich M, Tamassia R, Schwerin A. Implementation of an authenticated dictionary with skip lists and commutative hashing [J]. DISCEX II, 2001, 55(9): 889-903

[10] Pugh W. Skip lists: a probabilistic alternative to balanced trees [J]. Communications of the ACM, 1990, 33(6): 668-676

[11] Tamassia R, Triandopoulos N. Computational bounds on hierarchical data processing with applications to information security [C]// Proceedings of ICALP 2005. LNCS, 2005, 3580: 153-165

[12] Xu Jian, Zhou Fu-cai, Li Xin-yang, et al. Hierarchical Data Processing Model and Complete Tree Key Management Mechanism [C]// Proceedings of ICYCS 2008. IEEE Computer Society, Nov 2008: 1606-1612