文章编号:1001 - 9081(2009)10 - 2603 - 03

一种移动环境中的 P2P 网络信任模型

陈世平[1,2],王佳炳[1],裘慧奇[2]
(1. 上海理工大学 光电信息与计算机工程学院,上海 200093; 2. 上海理工大学 信息化办公室,上海 200093)
(wjb0303101@126.com)

摘 要:针对移动 P2P 网络大规模分布式和高度动态性的特点,提出一种基于动态反馈机制的信任模型。该模型引入了距离因子和推荐因子两个参数来控制推荐信任链的规模,提高推荐信任度的准确性。模型将反馈机制和惩罚机制集成到节点间的近期信任度和长期信任度的更新计算之中,提高了模型随时间和历史变化的动态适应性。模拟实验表明,该模型具有很好的动态适应能力,能够有效隔离恶意节点。

关键词:移动 P2P;推荐信任;动态反馈;信任模型
中图分类号: TP393 **文献标志码**:A

Trust model for mobile P2P network

CHEN Shi-ping[1,2], WANG Jia-bing[1], QIU Hui-qi[2]
(1. *School of Optical-Electrical Computer Engineering, University of Shanghai for Science and Technology, Shanghai* 200093, *China*;
2. *Office of Information, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

Abstract: Since the mobile P2P network is characterized by large-scale distribution and high dynamics, a trust model based on dynamic feedback mechanism was proposed. Two new parameters, distance factor and recommend factor, were introduced to control the size of chain of recommended trust, so as to improve the veracity of recommend trust. In addition, the feedback mechanism and punishment mechanism were integrated into the calculation of the recent trust and long-term trust, so the trust model has better adaptability to the dynamics of trust. Simulation experiments show that the model has very good dynamic adaptability and is able to effectively isolate the malicious node.

Key words: mobile P2P; recommendation trust; dynamic feedback; trust model

0 引言

P2P 作为一种分布式计算模型,它在解决分布式环境下资源共享和任务协同的可扩展性、自组织、低成本以及负载均衡等方面具有明显的优势。目前,随着 P2P 的广泛应用和无线网络技术的发展,P2P 技术已经开始扩展其范围到移动计算领域,为移动用户的 P2P 应用提供了支撑。因此,针对移动环境中的 P2P[1] 研究成为一个新的研究领域,该领域将 P2P 技术与移动技术相结合,以 P2P 的方法来解决移动网络中的问题和满足移动环境中的需求。

与传统的 P2P 网络相比,移动环境中的 P2P 网络具有以下特征[2]。

1)高度动态性:移动环境中 P2P 网络的拓扑结构随着节点的移动性而动态变化,这会造成覆盖层和底层物理网络连接状态不匹配;节点加入和退出网络的频繁性与随机性更加突出,这会导致网络安全受到严峻挑战。

2)连接的不可靠性:移动网络和有线网络相比,连接的可靠性较差。

3)节点资源的限制:对移动设备的便携要求,使当前移动终端的计算处理能力、存储能力、能量供应等受到限制,这使其在贡献资源的同时必须考虑自身的能耗等因素。

以上这些移动环境中的 P2P 网络特征,使得该网络环境下的信任管理的分布式特性和高度动态性更加突出。现有的大多数 P2P 信任模型主要是针对固定网络,而且对各种影响信任因素的动态性没有给予考虑。文献[3]作者提出了一个基于模糊逻辑的动态信任模型,但它对实体行为的时间变化性考虑较少,模型的动态适应能力值得商榷。文献[4]作者提出一种聚类的多粒度信任模型,它在一定程度上考虑了移动 P2P 网络的特性,但是它的推荐信任计算需要较多的时空开销,模型具有较慢的计算收敛性,影响了模型的可扩展性。

移动网络环境下的 P2P 系统安全技术不仅需要考虑到 P2P 网络的固有属性,同时也需要考虑移动网络环境所具有的自身特性。本文提出一种基于动态反馈机制的信任模型来建立移动环境中 P2P 网络节点之间可靠的信任关系。这种信任模型采用了局部推荐方法,节点通过有限的传播次数向局部广播以获取某个节点的推荐信任度,同时,根据时间、历史和自信任的动态变化反馈到近期信任度和长期信任度的更新计算之中,这些方法十分适合于移动环境中的 P2P 网络信任管理。

1 基于动态反馈机制的信任模型

1.1 相关概念

根据信任机制[5],结合移动 P2P 网络的特征,首先给出一些描述性定义和符号表示。

定义 1 信任度就是信任的定量表示,它体现了节点间交互的满意程度。本文采用概率可能性方法来衡量交互的满

收稿日期:2009 - 04 - 07;**修回日期**:2009 - 06 - 10。
基金项目:国家自然科学基金资助项目(60573142);上海市重点学科建设项目(S30504)。
作者简介:陈世平(1964 -),男,浙江绍兴人,教授,博士,主要研究方向:P2P 计算、计算机网络通信、数据库、知识库; 王佳炳(1983 -),男,广西桂林人,硕士,主要研究方向:P2P 计算; 裘慧奇(1980 -),男,浙江绍兴人,硕士,主要研究方向:计算机网络。

意程度评价,0 表示不满意,1 表示完全满意,值越大表示满意程度越高。

定义 2 直接信任度就是在给定的上下文环境中一个节点根据直接接触行为的历史记录而得出的对另外一个节点的信任程度。本文用 $E(Q_i,Q_j)$ 表示节点 Q_i 和节点 Q_j 之间的直接信任度,它由节点 Q_i 根据自身与节点 Q_j 直接的交互经验获得。

定义 3 推荐信任度表示节点间通过第三方的间接推荐形成的信任度。推荐信任度主要是根据信任的传递性来计算得到。如图 1 所示,若节点 Q_1 需要向网络中其他与 Q_{10} 有过直接交互的节点查询 Q_{10} 的信任度,如节点 Q_7 与 Q_{10} 有过直接交互历史,那么 Q_1 可以通过信任链 $Q_1 \rightarrow Q_2 \rightarrow Q_7$ 得到一个对节点 Q_{10} 的推荐信任度。本文中节点 Q_i 和节点 Q_j 之间的推荐信任度用 $PR(Q_i,Q_j)$ 表示,那么上面 Q_1 通过信任链 $Q_1 \rightarrow Q_2 \rightarrow Q_7$ 得到的推荐信任度可用如下公式计算:$PR(Q_1,Q_{10}) = r(Q_1,Q_7) \times E(Q_7,Q_{10})$,其中推荐者的信任链加权因子 $r(Q_1,Q_7) = r(Q_1,Q_2) \times r(Q_2,Q_7)$。

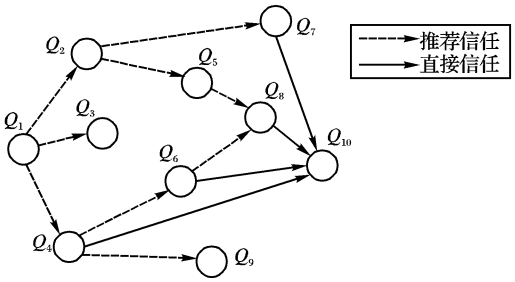

图 1 一个信任关系网络

定义 4 距离因子 ε 是一个控制推荐信任度请求传播深度的参数,它是一个大于等于 1 的整数。当传播的深度小于 ε 时,节点将请求转发给自己的邻居节点,否则停止转发。如图 1 所示,节点 Q_1 要得到节点 Q_{10} 的推荐信任度,$\varepsilon = 3$。网络中的移动设备可以根据自身的处理能力和存储能力、电池使用周期、下载速度和邻居节点的数量等影响因素来得到距离因子的大小,这样能较好控制信任链的规模和推荐信任度聚合运算速度。

定义 5 推荐因子 η 是节点对推荐者的信任因子的阈值,$\eta \in [0,1]$。只有推荐者的信任因子 $r \geqslant \eta$ 时,该推荐者的推荐信息是可信的,否则不可信。通过推荐因子,我们可以减少网络中的恶意节点不诚实的推荐行为,同时也能减少推荐信任聚合计算的时空开销。

定义 6 总体信任度是直接信任度和推荐信任度的加权平均。节点 Q_i 和节点 Q_j 之间的总体信任度用 $R(Q_i,Q_j)$ 表示。

定义 7 近期信任度 $RT(Q_i,Q_j)$ 表示节点 Q_i 对前面连续时间戳的近期信任度反馈和最近时间戳的总体信任度两方面综合考虑得到的对节点 Q_j 的信任值。

定义 8 长期信任度 $FT(Q_i,Q_j)$ 表示节点 Q_i 对前面连续时间戳的长期信任度反馈和最近时间戳的总体信任度两方面综合考虑得到的对节点 Q_j 的信任值。

定义 9 惩罚因子 δ 表示一个节点在与另一个节点的交互历史中,由于各种原因(如连接失败,恶意推荐等)导致的交互失败而得到的对该节点的惩罚程度参数。

定义 10 评价误差 d 表示两个节点对公共交互节点的评价差异。若节点 Q_i 和节点 Q_j 在时间戳 n 时刻的公共交互集合为 G,则 $d = \dfrac{\sum_{Q_z \in G} |E_n(Q_i,Q_z) - E_n(Q_j,Q_z)|}{\text{集合 } G \text{ 中元素个数}}$。

1.2 建立信任模型

节点 Q_i 对节点 Q_j 在基于连续的时间戳的直接交互过程中产生的信任满意度评价,即直接信任度集合 $E(Q_i,Q_j) = \{E_1(Q_i,Q_j),E_2(Q_i,Q_j),\cdots,E_n(Q_i,Q_j)\}$,$n > 0$,$n$ 表示时间戳。

节点 Q_i 为了得到其他节点对节点 Q_j 的评价,即推荐信任度。它需要将推荐请求在局部范围内传播,节点 Q_i 根据各种影响因素 $f_1,f_2,\cdots,f_n$ 和对应的权值 $a_1,a_2,\cdots,a_n$ 计算距离因子 $\varepsilon = \left\lfloor \sum_{k=1}^{n} f_k a_k \right\rfloor$。当传播深度小于等于 ε 时,节点将 Q_i 的推荐请求转发给满足 $r_n \geqslant \eta$ 条件的邻居节点,邻居节点的推荐信任因子 r_n 由式(1)计算得到:

$$r_n = \begin{cases} r_{n-1} - r_{n-1}\dfrac{d-\theta}{d+\theta}, & d \geqslant \theta \\ r_{n-1} + \dfrac{(1-r_{n-1})}{2}\dfrac{\theta-d}{d+\theta}, & d < \theta \end{cases} \tag{1}$$

其中 θ 为最大容忍评价误差。若邻居节点提供不诚实的推荐信息将会降低其推荐信任因子,提供诚实推荐信息将会提高其推荐信任因子。通过这样更新可以有效减少恶意节点特别是合伙欺骗节点提供的假推荐对信任值计算造成的影响。通过这种局部范围内的选择,最终可得到含有 L 个元素的推荐者集合 P,我们由式(2)计算推荐信任度:

$$PR_n(Q_i,Q_j) = \frac{\sum_{k=1}^{L} r_n(Q_i,P_k)E_n(P_k,Q_j)}{\sum_{k=1}^{L} r_n(Q_i,P_k)} \tag{2}$$

根据定义 6,节点 Q_i 对节点 Q_j 在时间戳 n 时刻的总体信任度可由式(3)计算获得:

$$R_n(Q_i,Q_j) = \frac{\omega_1 E_n(Q_i,Q_j) + \omega_2 PR_n(Q_i,Q_j)}{\omega_1 + \omega_2} \tag{3}$$

其中 ω_1,ω_2 分别为直接信任度和推荐信任度的权重因子。

惩罚因子:

$$\delta_n(Q_i,Q_j) = \frac{f_n(Q_i,Q_j)}{s_n(Q_i,Q_j) + f_n(Q_i,Q_j)} \tag{4}$$

其中:$s_n(Q_i,Q_j)$ 表示节点 Q_i 和节点 Q_j 正常交互的次数,$f_n(Q_i,Q_j)$ 表示节点 Q_i 和节点 Q_j 累积的通信事件失败的次数。惩罚因子将集成于近期信任度和长期信任度之中,对连接不稳定或不合作的移动节点给予惩罚。

在第 n 个时间戳的时刻,节点 Q_i 对节点 Q_j 的近期信任度更新函数可以使用式(5)计算获得:

$$RT_n(Q_i,Q_j) = \alpha_n RT_{n-1}(Q_i,Q_j) + (1-\alpha_n)R_n(Q_i,Q_j) \tag{5}$$

其中反馈因子:

$$\alpha_n = \begin{cases} \alpha_{n-1}, & f_n(Q_i,Q_j) = f_{n-1}(Q_i,Q_j) \\ \alpha_{n-1}[1-\delta_n(Q_i,Q_j)], & f_n(Q_i,Q_j) > f_{n-1}(Q_i,Q_j) \end{cases}$$

反馈因子越小,先前的信任历史就越容易被忽略,这体现了信任的减少是容易的,而信任的增加是建立在稳定的良好交互记录基础之上的。反馈机制的引入让模型具有了强化学习的能力,它使得近期信任度对新发生的交互行为有足够的敏感性,提高了信任模型的动态适应能力。

在第 n 个时间戳的时刻,节点 Q_i 对节点 Q_j 的长期信任度更新函数可以使用式(6)计算获得:

$$FT_n(Q_i,Q_j) = \frac{(n-1)FT_{n-1}(Q_i,Q_j) + R_n(Q_i,Q_j)}{n} \times [1-\delta_n(Q_i,Q_j)] \tag{6}$$

为了提高模型的安全性,节点 Q_i 对节点 Q_j 最终的信任评估结果 T_n 取 RT_n 与 FT_n 两者之中的最小值:

$$T_n(Q_i,Q_j) = \min[RT_n(Q_i,Q_j),FT_n(Q_i,Q_j)] \quad (7)$$

2　模拟实验结果及分析

为了评测模型的动态适应和对恶意推荐隔离的性能,本文用仿真软件对模型进行仿真,表 1 为参数设置。节点信任度初始化为 0.5,每个节点平均发出 20 次交互请求,每次交互间隔 1 s。本文也对模型在不同网络规模下的系统开销做了评测,并与 MGT 模型[4]进行比较。

表 1　模拟实验参数说明

类别	参数	缺省值
运行环境	节点总数	100
	交互次数	2000
模型参数	距离因子 ε	2
	推荐因子 η	0.6
	直接信任度权重因子 ω_1	0.6
	推荐信任度权重因子 ω_2	0.4
	反馈因子 α	0.1
	惩罚因子 δ	0.01
	最大容忍评价误差 θ	0.15

2.1　动态性评估

为了考察模型对信任值动态变化的适应能力,本文设计三个实验来模拟节点信任值三种类型的动态变化过程。节点在交互过程中有以下三种动态变化:1)合作→不合作;2)不合作→合作;3)不合作→合作→不合作。

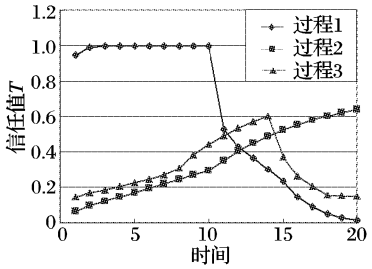

图 2　三种动态过程的信任值变化

图 2 的过程 1 曲线显示了合作节点在突然不合作的情况下,信任值会急剧下降,体现了信任值容易丧失的特点。过程 2 曲线表示不合作节点需要在长时间的合作情况下其信任值才有缓慢的增加,体现了信任值不容易提高的特点。过程 3 曲线的变化更加直观地体现了信任值不易获取、容易丢失的特性,这正如人类社会中的信任关系一样,信任的提高是要一个长期积累的过程,而一次不良的信任记录会导致以前好不容易建立起来的良好信任迅速丧失。

2.2　恶意推荐行为模拟

模拟恶意推荐时,假设推荐因子 $\eta = 0.6$。模型通过评价误差 d 与最大容忍评价误差 θ 的比较来判断推荐节点在该时刻有无恶意推荐行为,通过对行为的判断后对其信任因子 r 更新,更新后的 r 与 η 比较,低于 η 的推荐节点将其隔离在推荐节点集合之外。这里我们模拟三种特性的节点:动态恶意推荐节点、诚实推荐节点和无反馈机制的恶意推荐节点。

图 3 中的诚实节点因为提供真实的推荐而得到奖励,其信任因子不断增加。动态恶意节点先提供诚实的推荐信息以获取较高的信任因子,当它提供不诚实的推荐后,它的信任因子迅速减少,之后其摇摆行为使得它很难恢复到原来的信任值。而无反馈评价机制的恶意节点在相同情况下,其信任因子在 η 上下波动,其恶意推荐行为不能被有效隔离。因此,本模型中对恶意节点的惩罚力度较大,能比较理想地区分节点推荐信息的真假,隔离恶意推荐节点。

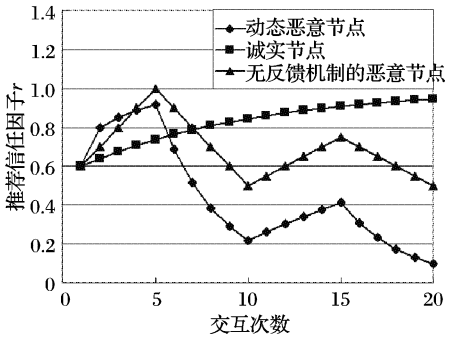

图 3　推荐节点的信任因子变化

2.3　模型系统开销评估

本模型的系统开销通过推荐信任度聚合计算时间和平均存储开销两个参数来进行评估,这两个参数反映了模型计算的收敛性和可扩展性。这里将本文模型与多粒度信任模型(Multiple Granularity Trust model,MGT)模型做比较。

图 4 为在不同网络规模下两个模型的推荐信任度聚合计算时间的比较,可以看出本文模型需要较少的聚合计算时间,而 MGT 需要较多的聚合计算时间,这是因为本模型采用局部推荐,根据距离因子和推荐因子来调节聚合计算的规模。这说明了本文有较好的运算收敛速度。同时也可以看出,随着网络规模的增大,本文模型的聚合计算时间缓慢增加,而 MGT 的聚合计算时间迅速增加,表明随着网络规模的增大,本文模型具有更好的可扩展性。

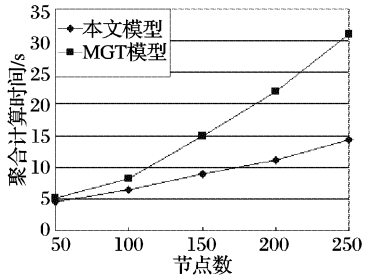

图 4　模型推荐信任聚合计算时间比较

图 5 为不同网络规模下模型平均存储开销的比较,可以看出本文模型需要较少的平均网络存储开销,而 MGT 计算全局信任度需要较多的空间开销。两个模型的平均存储开销随着节点数量的增加都缓慢减少,说明随着网络规模的增加,网络存储平均分布在各个节点之中。

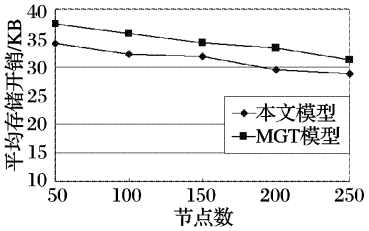

图 5　模型平均存储开销比较

3　结语

通过本文的工作,我们可以得出结论:基于动态反馈机制的信任模型考虑了时间、历史和信任关系的变化因素,它不但能适应移动环境下的P2P网络环境的高度动态性和分布

(下转第 2610 页)

STTP 就不能获得有效的数字资源 m_i。 证毕。

另外,STTP 在争端解决中的行为是可验证的,所发送的解密密钥的有效性可由 CA 签名确保。

3.4 交易拓扑的保密性分析

交易拓扑的保密性是多方交换协议特有的一个性质,即最终发生的交易行为对外部是保密的。在本文协议中,每个消息都是被加密传输的,除了对应实体外都不能解密消息,因此不能从消息文本中获得交换实体信息。另外,由图 1 可知交换对象协商是单向发布信息,如果不能获得所有消息文本中的实体信息,那就不能通过交换对象协商过程获得成功配对的交换实体对。可见,本文协议的交易拓扑是保密的。

4 结语

本文提出一种适合 P2P 网络的去中心化多方公平交换协议,协议分为四个阶段,采用交叉验证理论进行有价资源的认证和验证,采用离线半可信第三方进行争端解决,较好地解决了资源验证、交换对象协商和自动争端解决等问题。协议的公平性依赖于交叉验证理论的可证明正确性以及交换实体与 STTP 之间信道的可恢复性。

对本文协议的形式化分析和仿真实验将是我们下一阶段的工作重点。另外,协议在交换对时间敏感的资源时较为脆弱,这是由于恶意实体可任意延迟解密密钥到达指定实体的时间,这也是基于离线第三方交换协议难以解决的一个重要问题[18],这个难题也是我们下一步需要研究的方向。

参考文献:

[1] ASOKAN N, SCHUTER M, WAIDNER M. Optimistic protocols for multi-party fair exchange, RZ 2892[R]. Zurich: IBM Research Division, 1996.

[2] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchanges[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. New York: ACM Press, 1997: 7 - 17.

[3] ONIEVA J A, ZHOU JIAN-YING, LOPEZ J. Non-repudiation protocols for multiple entities [J]. Computer Communications, 2004, 27(16): 1608 - 1616.

[4] KREMER S, MARKOWITCH O. A multi - party non - repudiation protocol [C]// Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures. Netherlands: Kluwer, 2000: 271 - 280.

[5] 韩志耕,罗军舟. 一个公平的多方不可否认协议[J]. 计算机学报, 2008, 31(10): 1705 - 1715.

[6] 刘义春. P2P 组合交易的公平支付协议[J]. 计算机工程, 2008, 34(18): 171 - 173.

[7] INSOO K, JISEON K, INGOO H, *et al*. Multi-party fair exchange protocol using ring architecture model [J]. Computers & Security, 2001, 20(5): 422 - 439.

[8] FRANKLIN M, TSUDIK G. Secure group barter: Multi-party fair exchange with semi-trusted neutral parties [J]. Heidelberg: Springer-Verlag, 1998: 90 - 102.

[9] BAO FENG, DENG R, NGUYEN K Q, *et al*. Multi-party fair exchange with an off-line trusted neutral party [C]// DEXA: Proceedings of the 10 th International Workshop on Database & Expert Systems Applications. Washington, DC: IEEE Computer Society Press, 1999: 858 - 862.

[10] 杜红珍,张建中. 一个新的带离线半可信第三方的多方公平交换协议[J]. 计算机应用研究, 2006, 23(7): 248 - 250.

[11] 李艳平,张建中. 带离线半可信第三方的多方交换协议[J]. 西安电子科技大学学报: 自然科学版, 2004, 31(5): 811 - 814.

[12] MUKHAMEDOV A, KREMER S, RITTER E. Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model[C/OL]. [2009 - 01 - 01]. http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/MKR-fcrypto05.pdf.

[13] GONZALEZ-DELEITO N, MARKOWITCH O. Exclusions and related trust relationships in multi-party fair exchange protocols [J]. Journal of Electronic Commerce Research and Application, 2007, 6(3): 343 - 357.

[14] ARORA G, HANNEGHAN M, MERABTI M. P2P overlay network to support E-commerce [C/OL]. [2009 - 01 - 01]. http://www.cms.livjm.ac.uk/pgnet2006/Programme/Papers/2006-101.pdf.

[15] ARORA G, HANNEGHAN M, MERABTI M. P2P commercial digital content exchange [J]. Journal on Electronic Commerce Research and Applications, 2005, 4(3): 250 - 263.

[16] 秦志光,罗绪成. P2P 共享系统中无需专用 TTP 的公平交换协议[J]. 电子科技大学学报, 2008, 35(4): 698 - 701.

[17] 赵洋,秦志光,蓝天,等. 一种适用于 P2P 环境的乐观公平交换协议[J]. 计算机应用, 2007, 27(8): 1881 - 1883.

[18] RAY I, RAY I, NATARAJAN N. An anonymous and failure resilient fair-exchange e-commerce protocol [J]. Decision Support Systems, 2005, 39(10): 267 - 292.

[19] KREMER S, MARKOWITCH O, ZHOU J. An intensive survey of non-repudiation protocols [J]. Computer Communications, 2002, 25(17): 1606 - 1621.

(上接第 2605 页)

式特点,而且具有较强的恶意行为检测能力,同时该模型考虑了移动 P2P 网络中移动终端的计算性能的差异和推荐信任的可扩展性。

参考文献:

[1] WALKERDINE J, LOCK S. Towards secure mobile P2P systems [C]// ICIW: Proceedings of the Second International Conference of Intern and Web Applications and Services. Washington, DC: IEEE Computer Society, 2007: 6.

[2] 欧中洪,宋美娜,战晓苏,等. 移动对等网络关键技术[J]. 软件学报, 2008, 19(2): 404 - 418.

[3] DUMA C, SHAHMEHRI N, CARONNI G. Dynamic trust metrics for peer-to-peer systems [C]// Proceedings of the 16th International Workshop on Database and Expert Systems Applications. Washington, DC: IEEE Computer Society, 2005: 776 - 781.

[4] 任艳,任平安,吴振强,等. 移动 P2P 网络中的多粒度信任模型[J]. 计算机工程与应用, 2009, 45(6): 137 - 140.

[5] 马新新,耿技. 对等网络信任和信誉机制研究综述[J]. 计算机应用, 2007, 27(8): 1935 - 1938.

[6] WANG LEI, ZHU YAN-QIN, JIN LAN-FANG, *et al*. Trust mechanism in distributed access control model of P2P networks [C]//Proceedings of the 7th IEEE/ACIS International Conference of Computer and Information Science. Portland: IEEE Press, 2008: 19 - 24.

[7] WANG Y, VASSILEVA J. Bayesian network trust model in peer-to-peer networks[C]//Proceedings of the 2nd International Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004: 23 - 34.

[8] 李小勇,桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6): 1510 - 1521.