小 型 微 型 计 算 机 系 统 2008 年 月 第 期
Journal of Chinese Computer Systems Vol. No. 2008

一种基于市场模型的对等网络声誉管理机制

陈 欢[1]，陈贵海[1]，李振华[1]，曹晓梅[2]

[1](计算机软件新技术国家重点实验室(南京大学)，江苏 南京 210093)

[2](南京邮电大学 计算机学院，江苏 南京 210003)

E-mail ： gchen@nju.edu.cn

摘 要：传统的声誉管理机制依赖于反馈信息的真实性，然而对等网络中理性节点的自私行为和恶意节点的共谋行为产生虚假的反馈信息，制约了声誉管理机制的真实和有效性，为此本文提出了一种基于市场模型的声誉管理机制 MMRM。在 MMRM 中，节点能够获得的资源服务水平与它对系统的贡献直接关联；用户无法通过不真实的反馈信息为自己牟利，有效抑制了理性用户作弊的潜在动机；并且能够抵御恶意节点的各种攻击所造成的危害。实验模拟结果表明，MMRM 能够帮助系统中的不同用户获取不同水平的服务，有效引导理性用户诚实合作，及时发现并对抗网络中恶意节点的各种攻击。

关键词：对等网络；市场模型；声誉管理机制

中图分类号：TP **文献标识码：**A **文章编号：**

A Market Model based Reputation management Mechanism for Peer-to-Peer Networks

CHEN-Huan[1]，CHEN Guihai[1]，LI Zhenhua[1]，CAO Xiaomei[2]

[1] *(National Laboratory for Novel Software Technology (Nanjing University), Nanjing 210093, China)*

[2] *(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)*

Abstract: As P2P networks grow larger, the selfishness of rational nodes and collusions of malicious nodes challenges traditional P2P reputation management mechanisms, which suffer from various attacks based on false feedbacks. In this paper, a market model based reputation management mechanism (MMRM) is proposed, in which the members in the system can gain from the system with proportional to its contribution. MMRM removes the incentive of users to give false feedbacks and encourages them to serve other peers. Meanwhile, it discovers malicious behaviors and mitigates their endangerment. The simulation results prove it can encourage honest behavior and cooperation of rational nodes and handle different kinds of attacks launched by malicious nodes.

Key words: Peer-to-Peer; market model; reputation management mechanism

1 引言

对等网络中系统的开放性使它能够更为有效的利用因特网上边缘计算机的闲置资源，节点的自由性发掘了因特网中的潜在用户，参与构成系统的主体是大量随意自由流动的用户。然而系统的开放性和节点的自由性使对等网络缺乏对参与者的有效约束，导致占网络主体的理性节点的自私行为难以控制，针对对等网络的恶意行为难以根除。研究表明，在以文件共享为目的的对等网络中，大部分节点都有“搭便车”的行为，恶意节点可以上载垃圾文件，伪造文件，甚至在系统中传播病毒。例如 Napster 中 20%-40%的节点和 Gnutella 中 70%的节点共享很少或不共享资源[1,2]，Kazaa 中有超过 50%的音频文件是被污染的[1]，针对 Gnutella 的 VBS.Gnutella 蠕虫病毒也非常流行[4]。

为了对参与者进行有效约束，人们将声誉管理系统引入对等网络，通过声誉管理系统在网络中搜集节点的行为评价信息，由此分析和计算节点的声誉值，并用节点的声誉值作为反映节点历史行为的度量，尽量选择良性节点进行交互。

基金项目：国家自然科学基金项目：实用化对等网络技术的研究（60573131）；江苏省高技术研究项目：无线传感网与因特网融合技术及应用（BG2007039）资助 作者简介：**陈欢**，女，1984 年生，硕士研究生，研究方向为：对等网络的信任机制；**陈贵海**，男，1963 年生，教授，博士生导师，CCF 高级会员，主要研究领域为并行与分布式计算；**李振华**，男，1983 年生，硕士研究生，研究方向：对等网络，分布式流媒体处理；**曹晓梅**，女，1974 年生，博士，讲师，主要研究领域为无线网络安全。

然而很多声誉管理系统过于依赖节点的反馈意见，但又无法保证反馈意见的真实性，恶意节点可以通过注入虚假的反馈信息干扰系统的正常运行[4,5]。

本文提出了一种基于市场模型的声誉管理机制(Market Model based Reputation management Mechanism, MMRM)，其中节点的可用货币从系统层次综合反映了节点历史行为，节点的买方/卖方可信度从用户层次衡量了节点交易诚信度。具体来讲，每个节点可以出售自己的资源以换取货币，也可以使用货币购买自己所需的资源；卖方节点可以随时调整自己的策略，自由地对资源进行定价；买方节点根据价格和可信度选取最合适的卖方节点；通过货币与资源的转移实现买卖方之间的交易。实验模拟结果表明，MMRM 中的指标参数能够真实全面地描述节点性质，帮助系统中的不同用户获取不同质量水平的服务，有效引导理性用户诚实合作，及时发现并对抗网络中恶意节点的各种攻击。

本文是这样组织的：第 2 部分总结已有工作和不足之处；第 3 部分具体描述了 MMRM 的评价指标和工作流程，讨论 MMRM 如何引导理性节点放弃自私行为；第 4 部分分析 MMRM 如何应对对等网络中恶意节点的常见攻击行为；第 5 部分进行实验模拟说明 MMRM 的有效性；第 6 部分是结论与进一步的工作。

2 相关工作

目前已有许多声誉管理系统被提出，根据信用值的计算方法分为推荐信任[5-11,17,18]和虚拟货币[12-14]两大类。基于推荐信用的声誉管理机制根据参与用户的反馈计算每个节点的信用值，以 EigenTrust[4]模型为例：一个节点对其他节点的信任值组成本地信任向量，各节点的信任向量组成信任矩阵，通过分布式迭代计算得到各个节点的全局信任值。该机制在一定程度上消除了恶意攻击，但却产生了恶意推荐的问题，一个低声誉的节点可以通过服务高信誉节点来迅速提升自己的声誉值。虚拟货币类型的声誉模型结合对等网络中节点具有服务器和客户端双重身份的特点，对每个节点的货币进行累计，节点的货币在提供服务时增多，在获取服务时减少。在虚拟货币声誉模型中，货币的计算同样受节点反馈信息真实性的影响，例如恶意节点可以声称没有收到约定的服务，以拒绝支付货币。

最近，许多研究者尝试使用不同的方法避免不真实的反馈信息带来的不利影响。Srivatsa 等通过统计数据分析节点行为模式[7]，但是这种方法需要中心权威的服务器处理历史信息，与对等网络的分布性本质相悖；Lee 等[15]和 Feldman 等[16]通过在可信节点之间共享的历史信息中寻找信任链来减少不真实反馈的危害；还有一些信誉系统在考虑信任推荐时加入了推荐实体的可信性的概念，其中加权综合的方案最为常见[9,17,18]。但是这两种方法的通信代价很大且可扩展性较差。虚拟货币的解决方案中 Jakobsson 等[12]和 Vishnumurthy 等[13]提出的系统不能有效抵御虚假反馈信息，Zhang Z 等[14]的方案结合了货币与信任度对节点进行评价，但是没有区分节点扮演的角色，并且缺少对“网络波动”现象的考虑。

为了克服上述问题，为动态无制约的对等网络提供有效的声誉管理系统，本文在上述两类声誉管理系统的基础上提出了一种基于市场模型的声誉管理机制——MMRM。在 MMRM 中，可信度从用户层次描述其他节点对该节点行为的满意程度，可用货币从系统层次反映了节点对系统的贡献与索取。与同类工作相比，MMRM 的优点主要体现在以下 3 个方面：(1)通过对资源和服务定价引入差异性服务，督促参与节点为系统做贡献，从动机上减少了理性节点“搭便车”的行为；(2)在 MMRM 机制中，遵守规则的诚实反馈是节点的最优策略，”吹捧”和”诋毁”等恶意行为都将消耗恶意节点自身的资源，从而提高了恶意节点做虚假评价的代价；(3)不依赖于中心权威机构存储节点历史信息，能够有效适应对等网络的分布式特性，其通信路由可以借助对等网络原有的路由协议，开销不大。

3 基于市场模型的声誉管理机制

3.1 假设

本文考虑以资源共享为目的的对等网络，参与资源共享系统的节点可以分为良性节点，理性节点和恶意节点。良性节点遵守系统规则，为系统提供良好的资源和服务水平;理性节点希望能够最大化自身利益，在可为自身谋取利益的时候有时会破坏系统规则；恶意节点可能结成共谋同盟，通过破坏预定规则影响整个系统的正常工作。

MMRM 机制以基于 DHT 的 P2P 路由协议为基础，这种鲁棒的路由协议保证节点之间消息传递的可靠性。为了防止攻击者刻意选择节点标识符发动 Sybil 攻击，系统为每个节点随机分配标识符。同时为了保证在系统中传播的消息无法被恶意节点复制，伪造或篡改，我们假定系统消息通过某种算法进行了加密。

3.2 术语和评价指标

首先介绍 MMRM 中的一些常用术语：

买方节点(Buyer)：资源的索取者，支付货币购买资源。

卖方节点(Seller)：资源的提供者，出售资源兑换货币。

参与系统的节点可以随时扮演资源的买方节点和卖方节点两个角色。

监督者集合(Supervisors)：假设系统中个数为 n 的参与者集合 $P=\{P_1, P_2, \ldots\ldots P_n\}$，节点具有唯一的节点标识符。每个参与节点都将由系统自动分配给它们一些监督者，其职责就是记录，存储并维护其声誉信息。 在基于 DHT 的对等网络中，对于任意节点 P_i，可以在节点标识符上使用 s 个全局可知的哈希函数映射到 s 个节点组成监督者集合 $S(P_i)$。如果某些节点在网络中不存在，则由其后继节点替补。

服务质量(Quality of Service，简称 QoS)是网络上互相通信的用户之间关于信息传输与共享的质量约定。一般来说，带宽是最主要的决定因素，卖方节点分配给买方节点的带宽越大，传输速率越快，传输所需的时间也越短。相比抽象的服务质量的难以描述，传输所需的时间是一个很容易测量的数据，MMRM 将服务所需的时间作为衡量服务质量的要素。

交易规模(*Transaction_Size*)：买卖节点在交易之前会就服务质量，交易成功需支付的货币金额签订合约。合约中约定的货币金额就是本次交易的规模，交易规模的大小直接反映了此次交易的重要程度。

正常/非正常货币收入(In_Money_N, In_Money_{AN})：买方节点确认交易成功后，卖方节点的正常货币收入增加合约中约定的金额。若买方节点提出投诉意见，卖方节点的非正常货币收入增加合约中约定的金额。

正常/非正常货币支出(Out_Money_N，Out_Money_{AN}):买方节点确认交易成功后，买方节点的正常货币支出增加合约中约定的金额。若卖方节点提出投诉意见，买方节点的非正常货币支出会增加合约中约定的金额。

MMRM 中节点的声誉使用三个指标进行评价：

公式 1(可用货币)　可用货币($Avail\_Money$)是节点可以支配购买其他资源的等价物。

$$Avail\_Money = In\_Money_N - Out\_Money_N - Out\_Money_{AN}$$

可用货币的多少决定了节点可以选择的资源和服务水平，MMRM 通过刺激节点增加自己的可用货币达到激励共享的目的，增加可用货币的方法只有分享资源，为其他节点提供满意的服务。理性节点的“搭便车”行为将使得理性节点消耗自身的可用货币，无法继续从系统中购买资源。

MMRM 中通过买方和卖方可信度两个指标从用户层次描述节点行为。

公式 2(卖方可信度) 卖方可信度($Seller\_Reliability$)衡量节点作为卖方节点参与交易的诚信度。

$$Seller\_Reliability = In\_Money_N/(In\_Money_N + In\_Money_{AN})$$

节点的非正常货币收入越多，节点的卖方可信度越低，越难找到交易者兑现货币。

公式 3(买方可信度)　买方可信度($Buyer\_Reliability$)衡量节点作为买方节点参与交易的诚信度。

$$Buyer\_Reliability = Out\_Money_N/(Out\_Money_N + Out\_Money_{AN})$$

节点的非正常货币支出越多，节点的买方可信度越低，越难从其他节点处购买资源。

3.3 MMRM 的评价流程

MMRM 中任意一次交易活动的流程如图 1 所示：

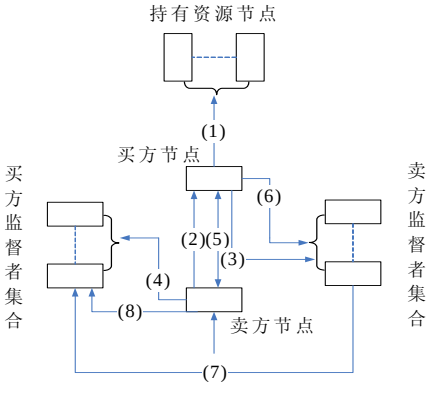

Fig1. The workflow of MMRM

图 1. MMRM 的工作流程

(1) 买方节点发出资源请求信息并提供可用货币和买方可信度信息。

(2) 愿意提供资源的卖方节点回应请求信息，并提供交易规模、服务质量(QoS)以及卖方可信度信息。

(3) 买方节点选定卖方节点，从卖方监督者集合处验证卖方节点提供的卖方可信度信息是否真实。

(4) 卖方节点从买方监督者集合处验证买方节点提供的可用货币和买方可信度信息是否真实。

(5) (3)(4)验证为真时，双方节点拟定合同约定交易规模与服务质量，并在可预期的时间内完成资源传输。

(6) 买方节点发送反馈消息给卖方监督者集合，满意本次交易时为交易成功的消息，不满意时为投诉消息，后者更新卖方节点的可用货币和卖方可信度等信息。

(7) 卖方监督者集合转发买方的反馈消息给卖方节点和买方监督者集合；

(8) 卖方节点发送反馈消息给买方监督者集合，后者更新买方节点的可用货币和买方可信度等信息。

3.4 讨论

3.4.1　抵抗说谎行为

MMRM 的工作流程能够保证参与节点提供信息的真实性，如下可能的说谎行为均会被发现并惩罚：

(1) 步骤 1 中如果买方节点提供虚假的可用货币和买方可信度信息，卖方节点会在步骤 4 的验证中发现；

(2) 步骤 2 中如果卖方节点提供虚假的卖方可信度信息，买方节点会在步骤 3 中的验证中发现；

(3) 步骤 6 中买方节点提供虚假反馈消息的情况会在 3.5 的实例分析中详细解释；

(4) 步骤 8 中如果卖方节点提供虚假反馈消息，会与步骤 7 中卖方监督者集合转发的买方反馈信息矛盾，被买方监督者集合发现。

3.4.2　监督者集合的可靠性

由 3.1 的假设，节点是无法选择自己的节点标识符的，且节点的监督者集合是根据全局可知的哈希函数集随机选择的，避免了恶意节点刻意安排自己成为特定某个节点的监督者之一的情况。某些节点监督者集合中包含恶意节点，通过大多数原则来统一监督者集合的意见可以过滤恶意节点的虚假信息。如果恶意节点想要控制某个节点的声誉信息，就必须控制该节点的监督者集合中的超过一半的成员，否则监督者集合提供的信息就是可信的。

公式 4(监督者集合可信的概率)[14]　假设在系统规模为 n，其中 m 个为恶意节点，监督者集合包含 s 个节点，监督者集合中恶意节点的数量不超过一半时该监督者集合提供的信息就是可信的，其概率为：

$$P_{trustworthy} = \sum_{i=0}^{\lfloor \frac{s}{2} \rfloor} \binom{s}{i} (\frac{m}{n})^i (1-\frac{m}{n})^{s-i}$$

假设在规模为 1000 的网络中存在 30%的节点为恶意节点，每个节点的监督者集合包含 10 个节点，按照公式 4，该集合可信的概率为 95.27%，表明监督者集合的大多数原则能够有效保证其提供的信息是可信的。

3.4.3　如何选择节点

卖方节点选择买方节点时，使用买方可信度预估卖方节点出售资源能够得到相应回报的概率，回应买方可信度高于一定预期的节点的资源请求。

买方节点选择卖方节点时，使用卖方可信度预估卖方节

点会如实按照合约规定提供资源的概率，过滤来自卖方可信度过低的节点的回复信息。过滤之后有不同的选择方法。譬如可用货币充足的节点选择可信度高的节点进行交易，而可用货币比较紧张的节点综合考虑卖方的可信度与交易规模的大小，选取“预期风险”最小的节点作为交易的卖方。

公式 5(预期风险) 预期风险(*Risk*)衡量了节点交易可能带来的损失。交易规模越大，则此次交易失败的损失越大，卖方可信度越低，则此次交易失败的可能性越大，预期风险也更大。

$$Risk = Transcation\_Size \times (1\text{-}Seller\_Reliability)$$

3.4.4 代价开销

在 MMRM 中，代价开销主要分为存储开销与通信开销两部分，与对等网络所采用的协议有关。 譬如在以 chord 为基础规模为 n 的对等网络中实现监督者集合规模为 s 的 MMRM，系统中的每个节点除维护 O(log n)个节点的路由信息外，各个监督节点上保存 pre 节点与 next 节点的路由信息以及包含监督节点的签名与时间戳的声誉信息。通信开销方面，买卖方节点间的互相定位需要 O(log n)的逻辑跳数，而节点与每个监督节点之间通信开销为 O(log n)，监督集合内更新声誉信息所需逻辑跳数为 O(s×log n)。总的来说 chord 中实现的 MMRM 中，系统中每个节点的存储开销为 Max(O(log n),O(s))，而通信开销为 O(s×log n)。

3.5 实例分析

两节点交易时，卖方的职责是提供符合约定的资源与服务，买方的职责是接受资源后按约支付。按照上文所述的协议流程，我们给出一次交易金额为 10 的的具体交易实例，按照交易可能的四种结果全面分析MMRM中双方节点声誉如何更新。交易双方的初始信息和更新结果如下表 1 所示。

Table1: An Instance of Transaction Update

表 1:交易实例更新

节点 \ 交易情况		初始情况	(1) 交易成功无投诉	(2) 只有买方节点投诉	(3) 只有卖方节点投诉	(4) 双方节点均投诉
买方节点 Buyer	Out_Money_N	10	20	20	10	10
	Out_Money_{AN}	10	10	10	20	20
	Avail_Money	30	20	20	20	20
	Buyer_Reliability	0.5	0.67	0.67	0.33	0.33
卖方节点 Seller	In_Money_N	10	20	10	20	10
	In_Money_{AN}	10	10	20	10	20
	Avail_Money	30	40	30	40	30
	Seller_Reliability	0.5	0.67	0.33	0.67	0.33

在MMRM中两节点交易时有一方恶意破坏合约会导致买卖双方互相投诉。从表 1 中对照(1)(4)两种情况，互相投诉时监督者采信投诉并同时惩罚双方节点因此失败的交易结果对双方都没有益处。理性节点与遵守规则的节点进行交易时，可选择的策略和收益对比如下表所示，拒绝支付或售价虚高的行为不会给自己带来预想的利益，反而会降低自己的可信度，理性节点是没有动机去这样做的。理性节点与恶意节点进行交易时，受到损害的理性节点同样会选择遵守规则进行投诉。因此理性节点最好的策略是合作，即 MMRM 能够引导理性节点遵守合约，诚实反馈。

Table2: Strategy-Income

表 2:策略-收益对比

	策略 A		策略 B		结论
	不合作	收益	合作	收益	
卖方履行合约时买方选择策略	投诉卖方提供的资源服务	可用货币减少买方可信度降低	诚实评价，支付约定的金额	可用货币减少买方可信度提高	收益 B> 收益 A；选择策略 B
买方履行合约时卖方选择策略	提供不符合约规定的服务而被投诉	可用货币不变，卖方可信度降低	提供符合合约规定的服务	可用货币增加，卖方可信度提高	收益 B> 收益 A；选择策略 B

3.6 波动现象

对等网络中波动现象十分常见，节点可以随时加入或离开，构成监督者集合的节点同样不能保证一直在线。在 P_i 使用 s 个不同的哈希函数 $H_1, H_2, \ldots\ldots H_s$ 映射到 s 个节点构成的监督者集合 $S(P_i)=\{S(P_i)_1, S(P_i)_2, \ldots\ldots S(P_i)_s\}$按照如下方法在波动的网络环境中维护节点 P_i 的声誉信息。

(1) 监督者 $S(P_i)_j$ 在本地保存监督者集合中的 pre 节点 $S(P_i)_{s-(s-i+1)\bmod s}$ 和 next 节点 $S(P_i)_{(j+1)\bmod s}$ 的路由信息；节点 P_i 的声誉信息包含监督节点的签名和时间戳。

(2) 监督者在线时，收到来自其他节点的更新消息后，由其中的一个监督者，譬如由 $S(P_i)_1$ 构造一个包含自身签名和时间戳的新的声誉信息的消息给 next 节点 $S(P_i)_2$， 如果 $S(P_i)_2$ 不在线，就发送包含监督者集合签名的原始声誉信息和包含自身签名的新声誉信息的消息给其后继节点，并更新本地保存的 next 节点；

接收该消息的节点查看 pre 节点是否需要更新，然后根据原始声誉信息和来自其他节点的更新消息计算新的声誉信息，如果与收到的新的声誉信息一致，就将自己的签名包含到该消息后，按照同样的方式将消息发送给 next 节点；

当该消息最终回到最初发出该消息的节点后，新的声誉信息就包含所有监督节点的签名，按照同样的顺序再传播一次，所有监督节点保存的声誉信息达到一致。

(3)监督者离开对等网络时，分为两种情况：

a.正常离开：节点在离开前传递自身保存的 *Pi* 的声誉信息给后继节点，并通知其他监督节点，对 MMRM 的正常工作不造成任何影响。

b.异常离开：节点在离开前不做任何传递工作。 监督者集合中的上一个节点会在下一次节点的声誉信息需要更新时发现该节点的离开，并将原始的声誉信息传送给后继节点，更新本地保存的 next 节点，后继节点可以替代离开节点的监督工作。

(4)监督者重新加入对等网络时，与其他的监督节点通信，得到最新的包含监督节点签名的声誉信息，并通知 pre 节点和 next 节点。

4 安全性分析

在对等网络中，恶意节点通过分享不真实的文件，提供虚假的反馈信息，甚至形成恶意团伙等手段诋毁诚实节点的声誉，提高自身声誉。典型攻击手段包括简单攻击，诋毁攻击，叛变者攻击，洗白攻击和共谋攻击等几类，下面对MMRM机制面临这几种攻击时的安全性做一分析：

4.1 简单攻击和诋毁攻击

简单攻击(Naive Attack)是指恶意节点作为卖方节点时，通过上载不真实的资源或者提供不符合约定的服务，欺骗其他节点的行为。在MMRM中与恶意节点交易后蒙受损失的节点会投诉对方，恶意节点的卖方可信度降低减少它们被选作卖方节点的可能性。

诋毁攻击(Bad-mouth Attack)是指恶意节点作为买方节点时，通过在交易后声称对方的服务不符合约定而拒绝支付相应货币，降低诚实节点的卖方可信度的行为。在MMRM中，持续的诋毁攻击会消耗恶意节点的可用货币，降低其买方可信度，减少其他节点选择它们作为买方节点的可能性。

4.2 叛变者攻击和洗白攻击

叛变者攻击(Betrayer Attack)是指网络中的恶意节点在加入网络的初期遵守系统规则，但在获得一定量的可用货币和较高的可信度后开始恶意行为。MMRM中恶意节点叛变以后，其他节点的投诉使其可用货币减少，可信度下降，降低了其他节点与它们交易的可能性。因为每次交易的影响因子只与其规模有关，开始通过一些小额交易累积可信度的叛变者在一次大额失败交易的影响下，可信度下降将非常迅速。

洗白攻击(Whitewashing Attack)是指恶意节点可信度很低，很难在网络中展开恶意活动时，离开系统，重新注册一个新的标识而成为系统的一个新人(Newcomer)。MMRM中新人缺少可用货币，初始的可信度又在一个比较低的水平，新人需要扮演诚实节点积累可用货币，提高可信度，演变为与叛变者攻击类似的情形。

4.3 共谋攻击

共谋(Collusion)是恶意节点之间通过合作操纵提升自己的声誉信息以对抗信任机制的行为。在MMRM中，这种操纵行为是难以实现的，其原因是：(1)恶意团体共谋增加其中一个节点的可用货币时需要消耗其他节点的可用货币；(2)恶意团体共谋增加其中一个节点的买方可信度时需要增加该节点正常节点支出，也就是在不断消耗该节点的可用货币，然而没有足够的可用货币的买方节点，是无法被其他节点选取作为买方交易的；(3)恶意团体共谋增加其中一个节点的卖方可信度时需要增加该节点的正常节点收入，也就是要将其他恶意节点的可用货币转移到该节点，而该节点的恶意行为会导致其可用货币减少，卖方可信度降低。恶意团体为了维持这个节点的卖方可信度，需要转移更多的可用货币到该节点，直至整个恶意团体的可用货币耗竭。

5 实验模拟

为了检验我们提出的声誉模型的有效性，我们依靠matlab工具仿真了一个使用chord协议的P2P的文件共享应用，并在这个应用上实现了MMRM，通过模拟节点活动检验了声誉管理模型对系统的影响。

5.1 实验参数

系统中不断有节点离开和加入，但节点数量保持不变，并假设各个文件的访问概率一样。实验具体参数与各个节点的初始货币和可信度信息如表3所示。

5.2 实验步骤和考察指标

实验过程中随机选取节点发出查询资源的请求，并根据自身策略选择卖方节点，最后进行货币转移和可信度更新。系统中三类节点按照以下的策略调整自己在系统中的行为：

良性节点作为买方节点时可信度阈值较高，在满足支付条件的情况下，优先选择高可信度的节点作为交易对象；作为卖方节点时，为系统提供较高质量的资源服务水平，平均售价也较高。

理性节点作为买方节点时可信度阈值设置较低，通过计算预期风险选择最合适的卖方节点。在可用货币能够满足自身使用时，理性节点采取“搭便车”的策略，不提供资源服务。可用货币逐渐减少到无法满足使用后，理性节点开始与其他节点共享资源。理性节点对自己的资源定价较低以降低其预期风险，吸引其他节点选取他作为卖方节点。

恶意节点在系统中模拟了多种恶意行为，包括简单攻击，叛变者攻击，共谋攻击等。最初它们在系统中扮演诚实的节点提升自己的可信度。开始进行恶意活动后，作为卖方节点提供虚假资源或报价虚高，作为买方节点拒绝支付甚至污蔑投诉对方，恶意节点间互相“吹捧”。当其可信度水平降低到一定程度时，则会丢弃自己的标识符，以新的身份加入到系统中。

实验的考察指标主要包括：

Table 3: Simulation Parameters

表3:实验参数

System 系统参数	节点数量	文件数量	交易规模	良性节点 比例	理性节点 比例	恶意节点 比例	监督者集合 大小
	4000	8000	[1，10]	0.2	0.5	0.3	10
Node 节点参数	初始货币	正常收入	非正常收入	正常支出	非正常支出	买方可信度	卖方可信度
	40	10	10	10	10	0.5	0.5

(1) 不真实资源下载的比例，即不真实资源下载的次数与总的资源下载次数比值。

(2) 网络中理性节点表现出共享性的比例。

(3) 良性节点与理性节点所享受的资源服务水平。

5.3 实验结果

首先考察不真实资源下载的比例，调整网络中不真实的资源比例分别为 25%，50%和 75%进行模拟。如图 2 所示，随着系统的运行，不真实文件下载的比例明显下降，除了不真实资源比例为 75%的一次仿真，其他两次不真实资源下载率都在前三轮模拟中很快下降到 10%以下，说明 MMRM 对抵御恶意节点上载的不真实资源是非常有效的。

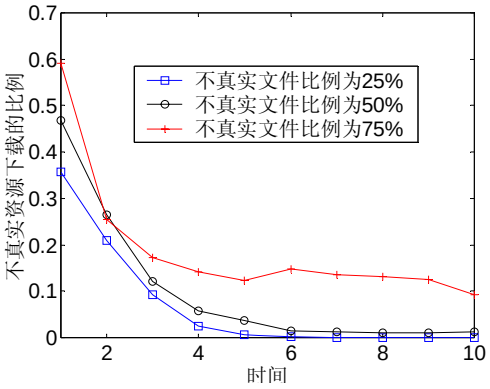

Fig2:The percentage of downloading inauthentic resource

图 2:不真实资源下载比例

然后观察系统中理性节点中转化为愿意共享资源节点的比例，当理性节点的可用货币无法满足下一次的购买需求时，理性节点开始出售资源以弥补可用货币的不足。图 3 显示，在一轮模拟之后 70%的理性节点表现出共享性。经过一段时间的积累，一些理性节点存储了足够的可用货币之后，又会表现出自私性。在第三轮实验以后，拒绝共享的理性节点的比例一直控制在 5%以内。这说明 MMRM 能够有效激励参与节点共享资源。

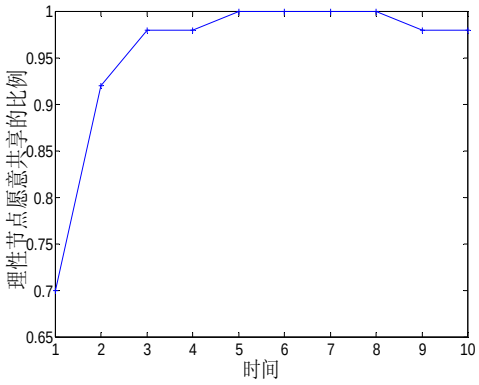

Fig 3 The percentage of sharing nodes in rational nodes

图 3:理性节点中表现出共享性的节点比例

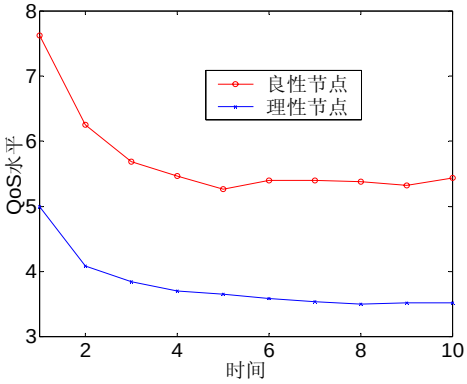

Fig4: Average QoS of benign nodes and rational nodes

图 4 节点得到的 QoS 的平均水平

最后考察良性节点与理性节点所得到的服务水平。交易成功时交易规模可以反映本次交易的服务质量；交易失败时本次交易的服务质量为 0。图 4 所示的是实验中统计良性节点与理性节点分别得到的平均服务质量。对应图 2 可以看出，前三轮实验后表现出共享性的理性节点增多，它们以较低价格提供资源使得整体的平均服务质量水平有所下降。对比两线又可以看出，良性节点优先选择可信度高的节点进行交易，失败概率较小，所得到的平均服务质量较高；而理性节点可用货币并不充裕，综合考虑预期风险的概念，通常选择售价较低的节点，失败的概率也较大，故得到的平均服务质量较低。这说明 MMRM 可以帮助系统提供差异性的服务。

6 结论与进一步的工作

本文提出了一个基于市场交易模型的声誉管理机制 MMPM，本文的主要创新点在于：(1) 使用买/卖方可信度从用户评价的衡量节点参与交易的诚信度，使用可用货币从系统的角度衡量节点对整个系统的贡献与索取；(2)通过对资源和服务定价引入差异性服务，督促参与节点为系统做贡献，从动机上减少了理性节点“搭便车”的行为；(3) 引导理性节点遵守预定规则，诚实反馈；(4)恶意节点从事恶意行为时，会消耗可用货币或降低其可信度，很难持续性地攻击对等网络。

针对常见攻击类型进行的安全性分析和最后的实验结果表明 MMRM 能够为系统中的不同用户提供不同质量水平的服务，有效引导理性用户诚实合作，及时发现并降低恶意节点的各种攻击所造成的危害。然而不足之处在于失败的交易过多时，总的货币单位减少速度过快会影响系统的正常运行。MMRM 利用了现成的基于 DHT 的对等网络路由协议，同样也会产生逻辑层与网络层不一致的问题，影响查询和更新效率。我们的下一步工作主要集中在大面积交易失败导致总的货币单位减少时如何调节总的货币量，是否有可用更低代价选取和维护监督者集合的方法以及不同可信度阈值的选取对 MMRM 有效性有何影响等方面。

References:

[1] Saroiu S, Gummadi PK, Gribble SD. A measurement study of peer-to-peer file sharing systems[A]. In: Kienzle MG, Shenoy PJ, eds. Proceedings of the SPIE, Vol. 4673, MMCN 2002[C], 156-170.

[2] Adar E, Huberman B. Free riding on gnutella[R]. Xerox PARC, August 2000.

[3] Liang J, Kumar R, Xi Y, Ross KW. Pollution in file sharing systems[A]. In: Proc. of the IEEE Infocom 2005.

[4]VBS.GnutellaWorm. http://securityresponse.symantec.com/avcenter/venc/data/vbs.gnutella.html

[5] Kamvar SD, Schlosser MT, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks[A]. In: Proc. of the 12th International WWW Conf[C]. New York: ACM Press, 2003. 640-651.

[6] Dellarocas C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior[A]. ACM Conference on Electronic Commerce[C], 2000, 150-157

[7] Srivatsa M, Xiong L, Liu L. Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks[A]. In: Ellis A, Hagino T, eds. Proc. of the WWW 2005[C]. Chiba: ACM Press, 2005. 422-431P.

[8] Dewan P and Dasgupta P. Securing reputation data in peer-to-peer networks[A]. Proceedings of PDCS 2004[C]. MIT Cambridge, USA. November 2004.

[9] Wang Y, Vassileva J. Bayesian network-based trust model in peer-to-peer networks[A]. LNCS Vol. 2872, Berlin: Springer-Verlag, 2003. 23-34.

[10] Venkatraman M, Yu B, Singh MP. Trust and reputation management in a small-world network[A]. Proceedings of ICMAS[C], 2000.

[11] Marti S, Garcia-Molina H. Identity Crisis: Anonymity vs. Reputation in P2P Systems[A]. Proceedings of IEEE 3rd International Conference on Peer-to-Peer Computing (P2P 2003).

[12] Jakobsson M, Hubaux JP, Buttyan L. A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks[A]. Proceedings of Financial Cryptography[C] 2003, LNCS, Vol. 2742, Springer-Verlag, 2003. 15-33.

[13] Vishnumurthy V, Chandrakumar S, Sirer EG. Karma: A secure economic framework for P2P resource sharing[A]. Proceedings of the 2005 Conf. of the Centre for Advanced Studies on Collaborative research[C]. IBM Press, 2005. 185-199.

[14] Zhang Z, Chen S, Yoon MK. March: a distributed incentive scheme for peer to peer networks[A]. Proceedings of the IEEE INFOCOM '07[C]. May 2007

[15] Lee S, Sherwood R, Bhattacharjee B. Cooperative peer groups in NICE[J]. Computer Networks, 2006, 50(7): 523-544.

[16] Feldman M, Lai K, Stoica I. Robust incentive techniques for peer-to-peer networks[A]. In: Breese JS, ed. Proceedings of the 5th ACM Conf. on Electronic Commerce[C]. New York: ACM Press, 2004. 102-111.

[17] 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.

[18] ZHANG Qian, ZHANG Xia, WEN Xue-Zhi,et al. Construction of Peer-to-Peer Multiple-Grain Trust Model [J]. Journal of Software, 2006, 17(1):96-107.

附中文参考文献

[17]窦文,王怀民,贾焰等.构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J].软件学报,2004,15(4):571-583.

[18] 张骞,张霞,文学志等. Peer-to-Peer 环境下多粒度 Trust 模型构造[J].软件学报,2006,17(1):96-107