基于资源评价的信任管理模型

杨双双 郭玉翠 左赛哲 胡映然
(北京邮电大学理学院 北京 100876)

摘 要 针对P2P网络中交易的安全性问题,提出了一种基于资源评价的信任管理模型。首先给出评价节点行为信任的好评度的概念,用模糊综合评判的方法计算节点对交易的单次好评度,每次交易后的交易记录表由提供资源的节点的母节点进行管理和存储;当节点选择提供资源的节点时,不仅考虑对目标节点的直接信任度,还考虑此次交易资源的总好评度,在计算直接信任度时考虑了时效性和交易资源的重要程度两个因素,交易资源的总好评度的计算数据来源于该资源的评价节点给出的以往评价;最后引入了基于虚拟货币的激励机制,以有效地提高节点参与的积极性。仿真实验表明,该模型能有效抵制恶意节点的攻击,提高网络交易的成功率。

关键词 信任管理,资源评价,好评度,模糊综合评判,激励机制
中图法分类号 TP393 **文献标识码** A

Trust Management Model Based on Evaluation of Resources

YANG Shuang-shuang GUO Yu-cui ZUO Sai-zhe HU Ying-ran
(School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract Aiming at the safety problem in P2P network, a new trust management model based on evaluation of resources was proposed in this paper. A concept of praise degree was given firstly, and a single praise degree was computed by fuzzy comprehensive evaluation. The transaction log table was saved and managed by mother peers of the one provided resources. When a peer chose which peer to deal with, it considered not only the direct trust value but also the total praise degree of resource. An incentive mechanism based on virtual currency was imported finally to enhance the peers' positivity of participation. The experiment result shows that this trust management model can effectively resist the attack of malicious peers and increase the success rate of network transactions.

Keywords Trust management, Evaluation of resources, Praise degree, Fuzzy comprehensive evaluation, Incentive mechanism

P2P网络是近年来兴起的一种新的计算体系结构,它具有协作实体自治、应用边界开放、业务发展动态等性质,这些特性使得它在协同工作、分布式信息或资源共享、大规模并行计算、即时通信等领域得到广泛应用[1]。但也正是这些特性为计算机病毒、垃圾数据、伪造文件等在P2P网络上的传播提供了便利的条件。另外,由于缺乏激励机制,有25%的节点是free riders[2],它们只从其他节点下载资源,而不提供资源上传服务。这些都威胁着P2P网络的安全和发展。

最近发展起来的信任管理技术能够提高P2P网络的安全性。信任管理的概念是在1996年由Matt Blaze提出的[3],目前多种信任管理模型被提出来。根据信任建立的方式不同,信任管理模型可以分为基于策略和基于声誉的信任管理模型。基于策略的信任管理模型是通过凭证建立信任关系的,一个节点对其他节点的信任度量值只有信任和不信任两种,这种信任模型得出的结论过于绝对,不能很好地满足现实情况的需要。

基于声誉的信任管理模型是目前研究的热点。为了解决P2P网络的安全问题,人们提出将声望管理系统引入P2P环境,这些声望管理系统负责在网络中搜集节点的行为评价信息,并分析和计算节点的声望值,以较真实地反应节点的行为,从而帮助节点进行正确的决策[4]。

文献[4]提出了一种基于社会规则的声望模型,在基于社会规则的声望模型的基础上建立了一个用于非结构化对等网络的信任管理方案;文献[5]提出了一种基于"熟人"推荐的信任模型,每个节点利用自己的交易历史记录计算出对其他节点的本地信任值,然后通过矩阵迭代扩大节点的信任范围,最终形成节点的全局信任值;文献[6]在节点推荐的基础上提出了一种基于Peer-to-peer环境的信任模型,并给出了该模型的数学分析和分布式实现方法;文献[7]基于P2P网络的拓扑特性,把度较高的节点看作网络中的权威节点,提出了一个用于非结构化P2P网络的信任管理机制;文献[8]提出了一种基于概率统计方法的信任评价模型,该模型借鉴了人类社

到稿日期:2011-09-05 返修日期:2011-11-23 本文受国家自然科学基金项目(60973146),山东省自然科学基金(ZR2009GM036)资助。
杨双双(1987-),女,硕士生,主要研究领域为数学与信息安全,E-mail:yss_1987_love@163.com;郭玉翠(1962-),女,博士,教授,硕士生导师,主要研究领域为信任管理、偏微分方程;左赛哲(1986-),女,硕士生,主要研究领域为数学与信息安全;胡映然(1987-),女,硕士生,主要研究领域为信息安全。

会中的主观信任概念，利用概率统计方法计算节点的直接信任和推荐信任；文献[9]提出了一种适用于无线自组网的新的信任管理模型，它在引入风险值的同时，还加入了适应无线自组网的参数阈值。

以上提到的模型[4-9]中，节点在计算交易节点的信任值时只考虑了节点的历史行为，在量化交易资源的历史评价时方法相对简单。针对以上问题，本文给出了评价节点行为信任的好评度的概念，建立了一个基于资源评价的信任管理模型。当两个节点交易完成之后，用模糊综合评判的方法计算单次好评度；综合单次好评度得到总好评度，由总好评度和直接信任值的综合得到最终信任值，直接信任度的计算又考虑了时效性和交易资源的重要程度两个因素，节点根据最终信任值选择交易节点；在交易完成后，交易记录表由提供资源的节点的母节点进行管理和存储；最后模型引入基于虚拟货币的激励机制，可以有效地提高节点参与的积极性。仿真实验表明，该模型能有效抵制恶意节点的攻击，提高网络交易的成功率。

1 模型的建立

在本模型中，节点 a 对节点 b 的信任决策依据最终信任值。最终信任值包括直接信任值和交易资源的总好评度，下面介绍两部分的度量过程。

1.1 单次好评度和直接信任度的计算

定义 1(交易) 网络中两个节点之间发生一次资源的提供或获取为一次交易。

定义 2(评价节点) 节点 a 与节点 b 交易完成后，节点 a 根据节点 b 在本次交易过程中的表现以及节点 b 提供给节点 a 的资源的质量对节点 b 进行评价。在此，节点 a 即为评价节点。

定义 3(单次好评度) 评价节点对每一次交易过程中所获取资源和目标节点行为的满意程度。

当节点 a 与节点 b 交易完成后，评价节点 a 根据评价标准给出交易资源 S 的单次好评度。以下用模糊综合评判[10]的方法来计算单次好评度。具体步骤如下：

1)确定评判对象的因素集 $U=\{u_1,u_2,u_3,u_4,u_5\}$，这里 u_1,u_2,u_3,u_4,u_5 分别表示响应时间、下载速度、服务态度、文件完整性、文件满意度。

2)给出评判集 $V=\{v_1,v_2,v_3,v_4,v_5\}$，此处 v_1,v_2,v_3,v_4,v_5 分别表示完全符合要求、符合要求、基本符合要求、不符合要求、恶意欺诈。

3)单因素评判。即建立一个从 U 到 V 的模糊映射

$$\tilde{f}:U\to F(V)$$

$$x_i \mapsto \frac{r_{i1}}{v_1}+\frac{r_{i2}}{v_2}+\cdots+\frac{r_{i5}}{v_5}$$

其中，$0\leqslant r_{ij}\leqslant 1$，$i=1,2,\cdots,5$；$j=1,2,\cdots,5$。由 $\tilde{f}$ 诱导出模糊关系，得到模糊矩阵 $R=(r_{ij})_{5\times 5}$，称 R 为单因素评判矩阵。

4)模糊综合评判。由于不同节点对 U 中各因素有不同的侧重，需要对每个因素赋予不同的权重，用 U 上的一个模糊向量 $W=\{w_1,w_2,w_3,w_4,w_5\}$ 表示，并且 $\sum_{i=1}^{5}w_i=1(w_i\geqslant 0)$。按照模糊变换的原理，$X(i,j)=W\circ R$，其中“$\circ$”为模糊变换。根据最大隶属度原则，得出本次交易后评价节点 a 对节点 b 提供的资源 S 的评价。然后根据评价映射函数得出在时刻 t 节点 a 对节点 b 提供的资源 S 的单次好评度，用 $Score_a^t(b,S)$ 表示。

$$Score_a^t(b,S)=\begin{cases}1.00, & \text{完全符合要求}\\ 0.80, & \text{符合要求}\\ 0.60, & \text{基本符合要求}\\ 0.40, & \text{不符合要求}\\ 0.20, & \text{恶意欺诈}\end{cases}$$

每次交易之后都会有一个交易记录表，交易记录表由提供资源的节点的母节点来管理和存储。在本文中，节点 a 提交此次交易的交易记录表给 a 的母节点。母节点定义如下：

定义 4(母节点和子节点) 如果节点 m 负责存储和管理节点 n 的交易评价信息，那么节点 m 为节点 n 的母节点，节点 n 为节点 m 的子节点。为了提高安全性，一个节点可以有多个母节点，也可以有多个子节点。

下面根据直接信任度和资源的总好评度来计算最终信任值，首先给出直接信任度的概念。

定义 5(直接信任度) 节点 a 根据与节点 b 的直接交易经验得到的对节点 b 的信任程度，用 DT_a^b 表示。

为了体现直接信任度的动态性，我们在计算直接信任度时考虑了时效性，并将时效性量化，用 $T(t_i)$ 表示，令 $T(t_i)=e^{t_i-t_{now}}$，$T\in(0,1)$，即距离当前时间越近的交易对当前的直接信任度的影响越大，距离当前时间越远的交易对当前的直接信任度的影响越小。

在实际交易过程中，每次交易资源的重要性是不同的，可以认为针对重要性高的资源所实施的恶意行为带来的危害会更大。为了防止恶意节点通过对重要性低的资源提供良好服务来积累直接信任度，从而在提供重要性高的资源时实施恶意行为，本文定义了资源重要程度映射函数：

$$L_a(S_i)=\begin{cases}2, & S_i\text{ 很重要}\\ 1, & S_i\text{ 重要}\\ 0.5, & S_i\text{ 一般重要}\\ 0.1, & S_i\text{ 不重要}\end{cases}$$

直接信任度的计算公式如式(1)所示：

$$DT_a^b=\Big(\sum_{i=1}^{N_1(a,b)}L_a(S_{t_i})\times T(t_i)-\sum_{j=1}^{N_2(a,b)}L_a(S_{t_j})\times T(t_j)\Big)\Big/\sum_{i=1}^{N_1(a,b)+N_2(a,b)}L_a(S_{t_i})\times T(t_i) \quad (1)$$

式中，$N_1(a,b)$ 为节点 a 与节点 b 成功交易的次数，$N_2(a,b)$ 为失败交易次数。模型中规定单次好评度 $Score_a^t(b,S)$ 大于 0.5 的交易称为成功交易，否则称为失败交易。$L_a(S_i)$ 为在节点 a 看来交易资源 S_i 的重要程度。

1.2 总好评度的计算

定义 6(总好评度) 节点 a 通过综合所有评价节点对节点 b 的资源 S 的单次好评度计算出来的值，用 $GV_a(b,S)$ 表示。

资源 S 的评价节点集合中包括与节点 a 有过直接交易和无直接交易的两种节点。对于无直接交易的评价节点，模型引入行为相似度的概念，因为信任具有主观特性，节点 a 更愿意相信与自己行为相似的评价节点的评价。本文引入余弦相似函数来量化两个节点的行为相似度：

$$C_{ak}=(\sum_s X\cdot Y)/(\sqrt{\sum_s X^2}\cdot\sqrt{\sum_s Y^2})$$

$$X=Score_a^{t_1}(b,S),Y=Score_k^{t_2}(b,S)$$

式中，$Score_a(b,S)$是节点 a 对节点 b 提供的资源 S 的单次好评度，它们构成集合 $Score_a=(Score_a(b_1,S_1),Score_a(b_2,S_2),\cdots,Score_a(b_n,S_n))$。$C_{ak}$ 刻画了节点 a 与节点 k 之间行为的相似程度，其值越大，说明两个节点的行为越相近，节点 a 更容易相信节点 k 的评价。资源请求节点通过行为相似度来选择自己比较信任的评价节点(本文设定选择行为相似度在0.5之上的节点)，记作 $Tset$，有效地过滤掉了恶意节点的评价。然而行为相似度仅仅反映了节点之间的行为相似程度，行为相似的苛刻节点与宽容节点给出的评价仍会有差值，于是用向量的模 CC_{ak} 来量化两个评价节点的评价差值：

$$CC_{ak}=\sqrt{\sum_S|Score_a^{t_1}(b,S)-Score_k^{t_2}(b,S)|^2}$$

于是，在节点 a 看来，目标节点 b 拥有的资源 S 的总好评度由以下两部分得到：

$$GV_a(b,S)=GV_a'(b,S)+GV_a''(b,S) \tag{2}$$

$$GV_a'(b,S)=A/\sum_{k\in Fset}DT_a^k \tag{3}$$

$$GV_a''(b,S)=B/C \tag{4}$$

$$A=\sum_{k\in Fset}T(t_i)\times Score_k^{t_i}(b,S)\times DT_a^k$$

$$B=\sum_{h\in UFset}T(t_j)\times Score_h^{t_j}(b,S)\times P(h)\times(1-CC_{ah})$$

$$C=\sum_{h\in UFset}P(h)$$

式中，$Score_k^{t_i}(b,S)$为在时刻 t_i 评价节点 k 对节点 b 提供的资源 S 的单次好评度，DT_a^k 为节点 a 对节点 k 的直接信任度，$T(t_i)$为时间衰减函数，$P(h)$为节点 h 的声誉，$Fset$ 为节点 b 拥有的资源 S 的评价节点中与节点 a 有过直接交易的且 $DT_a^k<0$ 的节点集合，$UFset$ 为没有与节点 a 交易过且 $P(h)>0$ 的节点集合，$Tset=Fset\cup UFset$。

当节点 a 对评价节点 k 的直接信任度 DT_a^k 小于零时，我们认为节点 a 不信任节点 k，即节点 a 认为节点 k 是不诚实节点，所以不考虑该评价节点 k 给出的评价。

定义 7(声誉)　对一个节点的交互历史的综合评价，代表着这个节点的可信任强度，用 $P(a)$表示节点 a 的声誉。

为了避免恶意节点通过多次小规模成功交易来提高声誉，然后在大规模的交易中作假，模型中引入了交易量因子，交易量因子的大小直接反应了交易的重要程度，令

$$Q(a,t_i,1)=SUC/V,Q(a,t_i,0)=UNS/V$$

式中，SUC 是指在时刻 t_i 节点 a 向其他节点提供资源且交易成功的交易量；UNS 是指在时刻 t_i 节点 a 向其他节点提供资源但交易失败的交易量；V 是指平均交易量，即单位时间总交易量与总交易次数之比。声誉的计算公式如式(5)所示：

$$P(a)=\begin{cases}\sum_{i=1}^{n}Q_i'/(\sum_{i=1}^{n}Q_i'+\lambda\sum_{i=1}^{m}Q_i''), & n>0\\ 0, & n=0\end{cases} \tag{5}$$

$$Q_i'=Q_i(a,t_{r_i},1),Q_i''=Q_i(a,t_{k_i},0)$$

式中，n 为节点 a 向其他节点提供资源且交易成功的次数，m 为节点 a 向其他节点提供资源但交易失败的次数，λ 为惩罚因子。

1.3　交易节点选择

节点根据最终信任值来确定是否交易，节点 a 对节点 b 的最终信任值由直接信任度和资源的总好评度综合得到，如式(6)所示：

$$T(a,b)=DT_a^b+\alpha GV_a(b,S) \tag{6}$$

式中，α 为平衡系数，使得 $\alpha GV_a(b,S)$在(0,1)之间。

当节点 a 想要知道节点 b 拥有的资源 S 的交易评价信息时，首先向节点 b 的母节点 c 申请查询节点 b 的交易记录表，如表 1 所列。

表 1　节点 b 的交易记录表

交易时间	交易节点	交易资源	资源的重要程度	单次好评度	交易量因子
t_1	k_1	S_1	0.5	0.8	+0.3
t_2	k_2	S_2	1	0.6	−0.4

从表 1 中可以看出，每个节点的交易记录表包括交易时间、交易节点、交易资源、资源重要程度、资源的单次好评度、交易量因子。表 1 中列举了两条交易记录，其中第一条交易记录表示在时刻 t_1 节点 k_1 从节点 b 那里获取了资源 S_1，在节点 k_1 看来，此次获取资源 S_1 的重要程度为 0.5，给予此次交易资源的单次好评度为 0.8，交易量因子为+0.3，+号代表交易成功，−号代表交易失败。

2　信任模型的激励机制

由于本文模型中的计算都是基于以往交易的评价，因此每次交易后节点给出的评价对于网络交易的正常进行有重要的影响。为了提高节点的参与积极性和鼓励节点在交易之后给出公正的评价，本文提出了基于虚拟货币的激励机制。所谓的激励机制就是通过某种措施或行动，给予某个机体某种好处，调动其积极性和主动性，从而激发鼓励其更好地提供服务。在网络中所使用的、不能自由兑换成现实货币的货币称为虚拟货币。货币值作为节点的属性之一，可通过提供服务和有效评价获得。

当新节点 a 刚加入网络时，系统给予一定数量的虚拟货币，虚拟货币随着节点的行为波动变化。当节点的资源被其他节点获取或者节点给予的评价在有效范围内，其虚拟货币数量增加；相反，当节点获取某一资源时需要支付一定量的虚拟货币，如果虚拟货币不足，则无法获得资源。总的来说，虚拟货币是节点“财富”的象征，用来量化节点对网络的贡献程度以及获取资源的能力。

节点 a 根据上文中的信任决策选取了交易节点 b_x 之后，向节点 b_x 发出交易请求，在交易进行之前，节点 a 向节点 b_x 支付获取资源 S 相对应的虚拟货币，之后节点 b_x 与节点 a 进行交易，如果交易成功，节点 b_x 还可以把此次的交易货币中的一部分分给交易资源的评价节点。

3　仿真

本文的仿真实验在 Windows 7 环境下用软件 Matlab 7.7.0 实现。

在仿真试验中，设定 100 个节点和 1000 个资源，将资源随机分配给每个节点，并保证每个资源至少被一个节点拥有，本文将提供虚假资源并且故意给虚假资源高评价的节点称为恶意节点。以下模拟了随着恶意节点的增多，节点 a 对节点 b 的信任值的变化情况。

在无信任机制的情况下，利用所有评价节点给出的评价

(下转第 46 页)

表1 效率比较

方案	Liu等[8]方案	改进方案
离线计算量	6PM+3PA+1E+3I	3PM+2PA+1E
在线计算量	3M	2M+1I
离线存储量	2624 比特	2144 比特
在线密文长度	1280 比特	960 比特
解签密计算量	$2\hat{e}$+4PM+4PA+1I	$2\hat{e}$+2PM+2PA+1E

结束语 本文提出一个高效的基于身份在线/离线签密方案。在保证安全的前提下，改进的方案在线及离线签密的运算量、解签密的运算量比Liu等[8]的方案有所降低，并且减少了离线存储量，缩短了在线密文长度。

参 考 文 献

[1] Zheng Y. Digital signcryption or How to Achieve Cost(Signature Encryption)≤Cost(Signature)+Cost(Encryption) [C]// Proceeding of CRYPTO'97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]// Proceeding of CRYPTO'84, LNCS 196. Berlin: Springer-Verlag, 1984: 47-53

[3] Even S, Goldreich O, Micali S. On-line/offline digital signatures [C]// Proc. CRYPTO 89, LNCS 2442. 1989: 263-277

[4] An J, Dodis Y, Rabin T. On the Security of Joint Signature and Encryption [C]// Proc. EUROCRYPT 2002, LNCS 2332. 2002: 83-107

[5] Zhang F, Mu Y, Susilo W. Reducing security overhead for mobile networks [C]// AINA Workshop '05. 2005: 398-403

[6] Xu Z, Dai G, Yang D. An efficient online / offline signcryption scheme for MANET[C]// AINA Workshop '07. 2007: 171-176

[7] Dongdong S, Xinyi H, Yi M, et al. Identity-based on-line/off-line signcryption [C]// Network and Parallel Computing. 2008: 34-41

[8] Liu J, Baek J, Zhou J. Online/Offline Identity-Based Signcryption Re-visited [R]. Cryptology ePrint Archive. Report2010/274, 2010

[9] Boneh D, Franklin M. Identity based encryption from the Weil pairing [C]// Advances in Cryptology-Crypto'01, LNCS 2139. 2001

[10] Boneh D, Boyen X. Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles [C]// Proc. EUROCRYPT 2004, LNCS 3027. 2004: 223-238

[11] Boneh D, Boyen X. Short Signatures without Random Oracles [C]// Proc. EUROCRYPT 2004, LNCS 3027. 2004: 56-73

[12] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures [J]. Journal of Cryptology, 2000, 13(3): 361-396

(上接第 33 页)

值来计算节点之间的信任值。图1表明，节点 a 对节点 b 的信任值随着恶意节点的增多快速增大。而在本文模型中，通过综合考虑对目标节点 b 的直接信任度和交易资源的总好评度，在计算两个节点之间的信任值时利用相似度和声誉把评价节点集合进行了两次筛选，从而随着恶意节点的增多，节点 a 对节点 b 的信任值变化不大。图1表明，在本文信任模型下，网络中恶意节点的增多对信任值有较小的影响。实验说明本文信任机制可以有效抵制恶意节点。

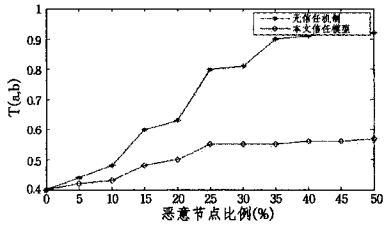

图1 信任值与恶意节点的关系

结束语 本文提出了一种基于资源评价的信任管理模型，提出了资源的总好评度的概念，在计算直接信任值时考虑了时效性和资源的重要程度两个因素，在计算节点的声誉时重点考虑了交易量因子的影响，以便很好地抑制节点通过小规模的成功交易来获取高的声誉值。引入激励机制，能有效地提高节点参与的积极性。分析及仿真表明，本文模型能较好地抵御恶意节点的攻击，提高网络交易的成功率。

参 考 文 献

[1] ORAM A. Peer-to-peer amassing the power of disruptive technology [M]. [S. l.]: O'Reilly Press, 2001

[2] Serious S, Gummadi P K, Gribble S D. A measurement study of P2P file sharing systems[C]// Kienzle M G, Shenoy P J, eds. Proc. of the Multimedia Computing and Networking 2002 (MMCN 2002). SPIE Press, 2002

[3] Blaze M, Feigenbaum J, Lacy J. Decent ralized trustmanagement [C]// Proceedingsof the 1996 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 1996: 164-173

[4] 贾兆庆，薛广涛，唐新怀，等. 非结构化 P2P 中的一种信任机制[J]. 计算机研究与发展，2010，47(4)：645-652

[5] Kamvar S D, Schollser M T, Garcia-Molainah. The eigentrust algorithm for reputation management in P2P networks[C]// Proceedings of the 12th International Conference on World Wide Web. New York: ACM, 2003: 640-651

[6] 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

[7] 贺明科，郝智勇. P2P 网络中基于网络拓扑特性的信任管理[J]. 计算机工程，2010(24)

[8] 吴鹏，吴国新，方群. 一种基于概率统计方法的 P2P 系统信任评价模型[J]. 计算机研究与发展，2008，45(3)：408-416

[9] 魏德健，贾智平，李新. 面向无线自组网的分布式信任管理模型[J]. 计算机应用，2011(1)

[10] 梁保松，曹殿立. 模糊数学及其应用[M]. 北京：科学出版社，2007：131-132

[11] 张仕斌，何大可，盛志伟. 信任管理模型的研究与发展[J]. 计算机应用研究，2006(07)：18-22