软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(4):745−760 [doi: 10.3724/SP.J.1001.2011.03754]

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

采用排名反馈的 P2P 名誉评价模型*

李治军+, 姜守旭, 李晓义

(哈尔滨工业大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

Reputation Model with Feedback of Ranking for P2P Systems

LI Zhi-Jun+, JIANG Shou-Xu, LI Xiao-Yi

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

+ Corresponding author: E-mail: lizhijun_os@hit.edu.cn

Li ZJ, Jiang SX, Li XY. Reputation model with feedback of ranking for P2P systems. *Journal of Software*, 2011,22(4):745−760. http://www.jos.org.cn/1000-9825/3754.htm

Abstract: Some peers may receive service and information of low-quality from other peers in peer-to-peer (or P2P) networks. Reputation evaluation is the normal method used to reduce the above phenomena. P2P reputation, based on score feedback, is defective because it can not distinguish the malicious feedback from the erring feedback returned by honest peers. It needs long time to converge the reputation and evaluate feedback. It is inflexible and unnatural to depict the reputation of a peer through a lot of numbers. In fact, the reputation is used to determine the rank of the peers. A reputation model called RbRf (reputation based ranking feedback) based on the rank feedback, is presented in this paper. Mathematical models unfolds in this paper show that the influence of erring feedbacks attenuates with the exponential function of RbRf. The influence of unintended malicious feedbacks is attenuated with the polynomial function in RbRf. The intended collusive feedbacks are counteracted by the correct information introduced by these feedbacks. In summary, the defection of score feedback, such as the need of a second evaluation of the trust of feedback, does not in RbRf any longer because the RbRf uses rank feedback, instead of score feedback, and the RbRf can achieve a better effect when resisting to malicious attacks. All results are verified by experimental data.

Key words: P2P network; reputation evaluation; rank feedback; collusion attack

摘 要: P2P 网络中的节点很可能从另外的节点那里收到质量很差的服务和信息,名誉评价是解决该问题的常见方法.基于评分反馈的 P2P 名誉计算机制存在下述缺点:无法区分恶意评价和诚实节点给出错误评价间的差别;需要对评分可信度进行二次评价,使名誉计算速度减慢;用数字来表示节点名誉的方式不够自然.实际上,名誉评价的用途是确定节点可信度的相对顺序.因此,提出了一种基于排名反馈的 P2P 名誉评价机制 RbRf(reputation based ranking feedback).针对 RbRf 和其上的恶意攻击进行了数学建模和理论分析,结果表明,RbRf 中非恶意错误的影响随排名反馈的数量指数而衰减;一般恶意攻击对 RbRf 的影响随排名反馈数量的多项式而减小;对于有意设计的共谋攻击,由于必须给 RbRf 引入正确信息而导致了恶意攻击被有效中和.因此,RbRf 不仅由于不再反馈打分信息而不存在评分反馈引起的名誉评价问题(如不需要对反馈信息的可信度进行二次评价),而且具有更好的抵抗恶意攻击的

* 基金项目: 国家自然科学基金(60803148); 中央高校基本科研业务费专项资助(HIT.NSRIF.2010.047)
收稿时间: 2009-05-12; 修改时间: 2009-07-21; 定稿时间: 2009-10-10

能力.仿真实验验证了理论分析的结果.

关键词: P2P 网络;名誉评价;排名反馈;共谋攻击
中图法分类号: TP393 文献标识码: A

由于 P2P 网络对节点进入网络的控制较少,很多 P2P 系统甚至不作任何控制,对于这样的开放式系统,将不可避免地出现大量自私的、恶意的、或不具备提供某类服务能力的节点,这些节点将严重影响系统的整体性能.这一影响在 P2P 电子商务系统,如 Lightshare 中表现得尤为明显.在这样的系统中,服务提供者是否诚实可信,将直接决定客户收到服务的质量,决定着系统可用性.对于 P2P 文件共享和 P2P 流媒体系统,其中存在的 low-performing 节点也会导致系统可用性的严重降低.名誉评价是解决这一基本问题的一种合适手段,其基本方法是,通过名誉的计算来发现那些 low-performing 节点,从而在信息交换中尽量避免与这些节点进行交换[1−19].

目前的 P2P 名誉机制都以如图 1 所示的模型为基础[1−19]:请求节点 r 首先根据搜索条件搜出满足要求的目标节点集合 G;对于 G 中的每个节点 g,节点 r 在与 g 进行服务交换之前需得到 g 的名誉值;然后,根据节点名誉值大小对 G 中的节点进行排名,并返回给 P2P 用户;最后,由用户决定选取哪个节点来完成服务交换[1].g 的名誉评价是该过程的核心,节点 r 在计算 g 的名誉值时通常采取的方法是,节点 r 首先选取目击者集合 $W=\{w_1,w_2,\ldots,w_k\}$,每个 $w\in W$ 会产生一个对 g 的评价值 t_{wg},r 在这些名誉评价值的基础上,通过聚合函数计算出 g 的可信度 T_g.

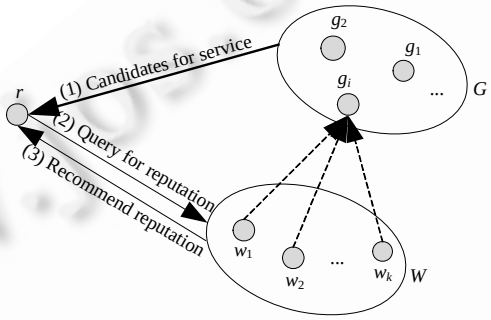


Fig.1 P2P reputation management model

图 1 P2P 名誉管理模型

目前,绝大多数 P2P 名誉评价机制都以公式(1)为基础来计算 T_g[2−4,9,11−18]:

$$T_g = W\times I + (1-W)\times R,\ R=\sum\nolimits_{w\in W} c_{rw}tr_{wg} \tag{1}$$

其中,I 是根据直接交互经验获得的可信度评价,R 是将推荐节点名誉反馈聚合后的结果.在计算 R 时,用 c_{rw} 表示节点 r 对节点 w 给出的名誉推荐值 tr_{wg} 的推荐可信度评价(也就是文献[5]中的 credibility of feedback),用这些推荐可信度作为权值来组合名誉反馈值,就能得出节点 g 的全局名誉值.除上述文献以外,许多 P2P 名誉管理的研究工作[5,6,10,14]也都以公式(1)为基础,通常表现为在公式(1)的基础上综合考虑其他因素.如,文献[5]就给出了在考虑反馈的 credibility 时结合节点相似度的思想,文献[6]在收集名誉反馈时发现并应用了名誉反馈具有的 power-law 分布特征,而文献[10]考虑了不同领域内节点可信度存在差异的事实.另外,其他一些 P2P 名誉的研究工作[7,16,18]虽然没有直接研究 T_g 的计算,但最终也都作用在 T_g 上.如:文献[7]给出了在名誉基础上如何构建合适的激励策略,文中的名誉计算也以公式(1)为基础;文献[18]中提出的 RETM 模型是在名誉反馈聚合之前,首先过滤那些无用的和会产生误导的推荐数据,从而提高计算结果的准确度.

以公式(1)为基础的名誉评价模型存在如下两方面的问题:(1) 需要评价推荐者(rater)的推荐可信度(credibility),即公式(1)中的 c_{rw}.在 P2P 这样的开放环境中,对推荐可信度的正确评价是很困难的;(2) 公式(1)中的 T_g 和推荐值 tr_{wg} 都是数(score),名誉评价就成为一个数值上的函数,而只依靠数字作为名誉反馈无法携带更为丰富的含义.另外,用数字作为名誉评价还存在评分标准统一等问题.

根据熟人推荐来认定一个人的可信度,是人类社会常用的方法(公式(1)体现的就是这样的方法).但对于P2P 这样的开放环境而言,该方法是否合适有待深入分析.

(1) 与人类社会相比,P2P 网络中节点交互的范围要大很多,所以名誉评价中的 rater 也非常多.rater 之间的能力各异,再加上 P2P 内在的自治特性,没有强烈的约束机制,使得在 P2P 网络中诚实的 rater 很可能对目标节点给出了错误评价.但在公式(1)中,这会导致这些诚实节点的 credibility 有所下降,被其他节点认为"不诚实".该现象常被称为信任关系的不确定性(造成这种不确定的一个主要原因是,节点的可信度是与时间和环境等上下文因素有关的,文献[19]对 P2P 节点间信任关系的这些特性进行了较好的总结).这种不确定性显然会导致公式(1)计算出的 T_g 偏离准确值,当诚实节点给出错误评价时会导致更差的负面效果.而在 P2P 名誉管理降低值 c_{rw} 后,又减小了诚实节点给出的正确评价而对名誉评价的正面影响.此时,公式(1)的加权求和计算方法不再合适.文献[11]对该问题进行了深入分析,并用大量的模拟实验来表明推荐在 P2P 名誉评价中并不能起到很好的效果.因此,文献[14]提出了一种不考虑 c_{rw} 的名誉聚合方法.即在公式(1)中将 c_{rw} 去掉,直接加和平均,并将其称为 AVG.模拟实验表明,AVG 方法能够取得较好的效果.

(2) 同样,由于 P2P 网络中节点交互范围的扩大,使得很多推荐节点对于请求节点是陌生的.此时,对于公式(1)中的 c_{rw} 也需要进行名誉评价.这就形成了间接信任关系链[9],需要进行多次迭代才能收敛,导致很低的名誉计算效率.当 P2P 网络达到一定规模以后,许多类似的名誉计算算法因效率太低而不再适用[19].文献[11]的模拟实验结果也表明了 AVG 方法的收敛速度很快,但 AVG 的无差别聚合方法对各类节点给出的名誉反馈不加以区别,在恶意节点较多的 P2P 环境中无法良好地工作.

另外,T_g 的正确计算依赖于 tr_{wg} 具有统一的评分标准.tr_{wg}=10 表示 w 认为 g 的名誉最高,而节点 w'给出的最高评分是 5,公式(1)聚合后有 T_g=7.5,显然不是 g 的正确评价.虽然 P2P 通常都对 tr_{wg} 的计算统一定义,如 $tr_{wg}=\max((sat(w,g)-unsat(w,g)),0)\Big/\sum_j \max((sat(w,g)-unsat(w,g)),0)$[4],但这样的定义并不适合于量化评价节点的所有能力,而且那些依靠 human computation[20]得出的节点评价也无法计入名誉评价模型中.对于度量节点可信度这样一个复杂特性,human computation 也许会成为一种重要的辅助手段.

实际上,节点的名誉值是被用来选取可信度较高的节点进行信息交换的.因此,名誉评价的基本用途是确定节点可信度的相对顺序.以此为基础,本文提出了一种基于排名反馈的 P2P 名誉评价模型(reputation based ranking feedback,简称 RbRf).在 RbRf 中,目击节点 w 针对目标节点 g 反馈一个节点序列:

$$R_f(w,g)=\langle p_1,p_2,...,p_m\rangle \tag{2}$$

其中,$\exists j\in\{1,\ldots,m\}$,有 $g=p_j$,R_f 是一个按节点可信度降序排名的序列(所以,本文称其为排名反馈名誉计算模型).此时,P2P 名誉评价模型如图 2 所示.

(1) 节点 r 搜索 P2P 网络中能够应答服务请求 Q 的节点集 G;

(2) 每个收到 Q 的节点 w 返回一个按节点名誉降序排名的反馈序列 $R_f(w,Q)$;

(3) 根据收到的序列集合,节点 r 进行名誉评价(即运行 RbRf);

(4) 节点 r 根据 RbRf 的结果选取部分节点 $O\subseteq G$ 进行信息交换.

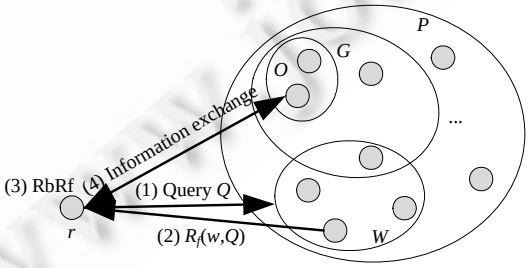


Fig.2 P2P reputation evaluation based on RbRf

图 2 基于 RbRf 的 P2P 名誉评价模型

RbRf 的输入是|W|个 R_f 序列,输出是 G 中前 k 个名誉最高节点形成的序列$\langle r_1,r_2,...,r_k\rangle$.

显然,RbRf 在根据 R_f 计算$\langle r_1,r_2,...,r_k\rangle$的过程只需要节点序列信息即可,无需对推荐可信度二次评价,也不必引入节点名誉值(score).同时,R_f 携带着更为丰富的含义,避免了以公式(1)为基础的名誉评价所存在的两方面问题.理论分析和仿真实验结果表明:

(1) RbRf 在处理信任关系的不确定性和提高名誉计算收敛速度方面明显优于目前的 P2P 名誉评价方法;
(2) RbRf 在对抗名誉的恶意攻击方面表现出更好的性能;
(3) RbRf 不会产生评分一致性问题.因此,本文提出的基于排名反馈的 P2P 名誉计算模型较好地解决了现有 P2P 名誉评价研究中出现的问题.

1 基于排名反馈的名誉计算模型

1.1 全局RbRf模型

为方便分析,首先假定对于由任何一个从 r 发起的查询 Q,P2P 中的任一节点 $p\in P$ 都能返回一个 $R_f(p,Q)$,且该序列包含了 P 中所有的节点,所以称其为全局 RbRf 模型.此时,r 将收到 $n=|P|$个反馈序列:

$$\begin{aligned} &R_f(1)=\langle p_{11},p_{12},...,p_{1n}\rangle\\ &R_f(2)=\langle p_{21},p_{22},...,p_{2n}\rangle\\ &...\\ &R_f(n)=\langle p_{n1},p_{n2},...,p_{nn}\rangle \end{aligned} \tag{3}$$

恶意节点导致 $R_f(i)$包含故意错误,不确定的信任关系会使 $R_f(i)$出现非恶意错误,都会导致错误的名誉评价.下面给出的 *k-Ranks* RbRf 名誉评价算法首先用来消除名誉评价信息中的非恶意错误.

定义 1(*k-Ranks* RbRf). 对于 $R_f(1),R_f(2),...,R_f(n)$,将 $R_f(i)$中的第 j 项记为 $R_f^j(i)$,*k-Ranks* RbRf 返回的 r_j $(1\leqslant j\leqslant k)$是序列$\langle R_f^j(1),R_f^j(2),...,R_f^j(n)\rangle$ 中出现频率最多的某一项 $R_f^j(m)$.

如果公式(2)中的每个 $R_f(i)$都正确地给出了节点的名誉排名序列,此时所有 $R_f(i)$都完全一样,则 *k-Ranks* RbRf 显然返回了正确的结果.现在分析,当 $R_f(i)$中出现一些随机错误(即由于不确定信息而导致的非恶意错误)时, *k-Ranks* RbRf 的工作效果.

定理 1. *k-Ranks* RbRf 能够有效消除 $R_f(p,Q)$中的非恶意错误.

证明:包含不确定性的 $R_f(p,Q)$其含义是指获得完整信息的节点会给出一个正确的评价结果,而其他节点会因为信息不完整而给出包含随机错误的评价,且这些随机错误是独立的.与恶意攻击的本质区别在于,在恶意攻击中,这些错误是有关联的,或者说是协同的.

从形式化角度,$R_f(p,Q)$中的不确定性是指 $R_f(i)$在排名位置 j 上或者正确,或者包含独立的随机错误.可以假定序列$\langle R_f^j(1),R_f^j(2),...,R_f^j(n)\rangle$ 中的正确评价 C_f^j 所占的比例是α,这样,也就有$(1-\alpha)n$ 个随机的错误评价 $E_f^j(i)$,独立的随机错误表明, $E_f^j(i)$ 等概率(概率为 $1/(n-1)$)选取了 $P/\{C_f^j\}$ 中的节点.

根据定义 1,*k-Ranks* RbRf 算法返回的 $r_j\neq C_f^j$ 当且仅当 $E_f^j(i)$ 中出现相同节点的次数不低于αn.该事件出现的概率等于在$(1-\alpha)n$ 个 $E_f^j(i)$ 中选出αn 个项相同,其他项任意选取(这样就包含了出现超过αn 个相同项的情况)的概率(其中用到了 $R_f^j(i),1\leqslant i\leqslant n$ 中的随机错误相互独立的事实):

$$\left(\frac{1}{n-1}\right)^{\alpha n}\times(n-1)=\left(\frac{1}{n-1}\right)^{\alpha n-1}.$$

该概率值乘以从$(1-\alpha)n$ 个 $E_f^j(i)$ 中选出αn 个项的组合数就是 $r_j\neq C_f^j$ 的概率:

$$\Pr(r_j\neq C_f^j)=\binom{(1-\alpha)n}{\alpha n}\times\left(\frac{1}{n-1}\right)^{\alpha n-1}\leqslant\frac{((1-\alpha)n)^{\alpha n}}{(\alpha n)!\times(n-1)^{\alpha n-1}}\approx\frac{1}{\alpha}((1-\alpha)^{\alpha})^n\times\frac{1}{(\alpha n-1)!}.$$

因此,只要α是一个确定的常数(不是 $O(1/p(n))$),$\Pr(r_j \neq C_f^j)$就是一个随 n 指数衰减为 0 的数.这表明,对于 *k-Ranks* RbRf 算法,只要收到一定规模的排名反馈信息,就能以非常显著的概率返回正确的排名 r_j,$1 \leqslant j \leqslant n$.如果在 $R_f(p,Q)$中没有恶意攻击,只存在信息不确定性时,α是一个常数的假设是合理的;而即使α非常小,由于 $\Pr(r_j \neq C_f^j)$存在的指数衰减性,随着收集的排名反馈数量的逐渐增大,*k-Ranks* RbRf 会很快返回正确结果.证毕. □

定理 1 表明,*k-Ranks* RbRf 能够有效消除名誉评价信息中的不确定性.但为了抵抗恶意攻击,即当 $R_f(p,Q)$中出现由共谋攻击引起的协同错误时,*k-Ranks* RbRf 需要进一步加以改造.定理 1 的证明过程表明,恶意攻击与信息不确定所导致的随机错误之间的根本区别在于,恶意攻击中 $E_f^j(i)$ 不再独立地等概率选取 $P/\{C_f^j\}$ 中的节点,而是一旦某 i 处的 $E_f^j(i)=e$ 时,一些共谋节点 c 给出的 $R_f^j(c)$ 不再独立地选取其他节点,而以远大于 $1/(n-1)$的概率(实际上是接近于 1 的概率)选取 e,即

$$\exists (c \in P \wedge c \neq i) \Pr(E_f^j(c) = e \mid E_f^j(i) = e) >> \frac{1}{n-1} \tag{4}$$

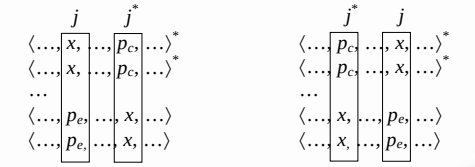
公式(4)给出了共谋攻击区别于不确定错误的数学含义,在此基础上,可以描述 *k-Ranks* RbRf 无法处理的恶意攻击.

定义 2(RbRf 的共谋攻击). 如果存在 j,使得序列$\langle R_f^j(1), R_f^j(2), ..., R_f^j(n)\rangle$ 中出现频率最多的某一项 $R_f^j(m) \neq C_f^j$,则称在$\langle R_f^j(1), R_f^j(2), ..., R_f^j(n)\rangle$ 处存在共谋攻击.假定 $R_f^j(m)$ 的正确排名为 j^*,即 $R_f^j(m) = C_f^{j^*}$,如果 $j>j^*$,则称为共谋哄抬(collusive boost attack,简称 CBA);如果 $j<j^*$,则称为共谋诋毁(collusive denigration attack,简称 CDA).

由于 RbRf 的工作原理是综合分析多个 $R_f(i)$后产生的结果,所以单个节点的恶意赞扬和恶意诋毁对 RbRf 没有任何影响,*k-Ranks* RbRf 都能有效消除(定理 1 的结果),与由于信息不确定性造成的错误没有区别.实际上,这两者也不应该有区别,因为诚实节点由于信息的不完整也完全可能得出与恶意节点相同的结论,这也是 RbRf 对传统的基于 score 的 P2P 名誉机制的一种改进.总之,定义 2 中给出的共谋攻击是 RbRf 唯一需要处理的攻击.

定理 2. *k-Ranks* RbRf 采用的独立观察公式(3)中每个列的方法不能处理定义 2 给出的共谋攻击.

证明:图 3 给出了一个共谋赞扬攻击的实例和一个共谋诋毁攻击的实例,其中:x 表示其他节点;$p_e(p_c)$表示 p 节点排名在错误(正确)的位置上,其中,不带有"*"号的排名反馈是共谋攻击给出的反馈.



(a) A case of CBA (b) A case of CDA

(a) 一个共谋哄抬实例 (b) 一个共谋诋毁实例

Fig.3 Two collusive attacks on RbRf

图 3 RbRf 上的共谋攻击

由于 *k-Ranks* RbRf 只根据图 3 中 j 列和 j^*列来完成 r_j 和 r_{j^*} 的计算,对于图 3 给出的两种情况,由于 $p_e=p_c=p$,所以只要将位置上下颠倒一下,图 3(a)的 j 列和 j^*列就与图 3(b)的 j 列和 j^*列完全一样.而 *k-Ranks* RbRf 在完成计算时,与公式(3)中各排名反馈的上下位置无关.

因此,*k-Ranks* RbRf 无法区分一个 CBA 和 CDA,也就无法处理共谋攻击.证毕. □

从定理 2 的证明过程可以看出:在计算 r_j 时,如果只观察$\langle R_f^j(1), R_f^j(2), ..., R_f^j(n)\rangle$, 那么,*k-Ranks* RbRf 无法处理共谋攻击;而即使在观察另一个序列$\langle R_f^{j^*}(1), R_f^{j^*}(2), ..., R_f^{j^*}(n)\rangle$ 时发现一个冲突($r_j = r_{j^*}$),*k-Ranks* RbRf 也仍然无法处理共谋攻击.造成这一结果的根本原因是,*k-Ranks* RbRf 独立地观察公式(3)中的每个列,使得图 3(a)的 j 列和 j^*列就与图 3(b)的 j 列和 j^*列对于 *k-Ranks* RbRf 没有差别.这就要求,在计算 r_j 时,综合观察 $R_f(i)$的每个排名位置,

即 $R_f(i)$整体对 r_j 的影响,这种影响可以通过与 $R_f(i)$关联的权值 $W(R_f(i))$来体现.针对图 3 的两种情况,如果能够设计合理的算法使得带“*”的行较不带“*”的行能关联显著不同的权值,此时,图 3 中 j 列和 j^*列中的各个位置不再可以上下颠倒,从而可以区分 CDA 和 CBA,亦即可以抵抗共谋攻击.

定义 3(加权 *k-Ranks* RbRf). 用一个[0,1]上的数值来刻画排名反馈 $R_f(i)$的权值,即 $W(R_f(i))\in[0,1]$,给每个 $R_f^j(i)$ 定义一个分值 $score(R_f^j(i))$:

$$score(R_f^j(i))=\sum_{R_f^j(w)=R_f^j(i)\wedge w\in\{1,\ldots,n\}}W(R_f(w)) \tag{5}$$

Weighted *k-Ranks* RbRf(加权 *k-Ranks* RbRf)返回的 $r_j(1\leqslant j\leqslant k)$就是 *score* 值最大的 $R_f^j(i)$.

定义 3 中 $R_f(i)$的权值定义为 $W(R_f(i))\in[0,1]$的含义是,将 $R_f(1),R_f(2),\ldots,R_f(n)$看成是 n 个可能事件,刻画排名反馈 $R_f(i)$的准确性(可信度)可信度.$W(R_f(i))$在含义与公式(1)中的值 c_{rw} 类似,但与 c_{rw} 存在本质的不同,$W(R_f(i))$是分析公式(3)时引入的一个数值,是公式(3)固有蕴含的,不需要存储和维护.

显然,当公式(5)中各 $W(R_f(i)),1\leqslant i\leqslant n$ 取相等的数值时,Weighted *k-Ranks* RbRf 就是 *k-Ranks* RbRf,*k-Ranks* RbRf 是 Weighted *k-Ranks* RbRf 的特例.因此,Weighted *k-Ranks* RbRf 同样满足定理 1,可以有效消除信息不确定性.同时,由于引入了权值,Weighted *k-Ranks* RbRf 也能有效处理共谋攻击.对共谋攻击的有效抵抗集中体现在 $W(R_f(i))$的定义上,公式(6)给出了一种简单的计算方法:

$$W(R_f(w))=\frac{1}{n}\sum_{k=1}^{n}\left(\sum_{R_f^k(w)=R_f^k(i)\wedge w\in\{1,\ldots,n\}}\frac{1}{n}\right) \tag{6}$$

公式(6)计算了项 $R_f^k(i)$ 在所有的 $R_f^k(w)$,$1\leqslant w\leqslant n$ 中出现的次数,该次数表明了 $R_f(i)$在位置 k 处的评价与其他所有 $R_f(w)$在相同位置上给出评价的一致程度;然后,将所有位置$(1\leqslant k\leqslant n)$的这种一致程度进行累加,反映了 $R_f(i)$与其他排名反馈的整体一致程度,可以用该值刻画 $R_f(i)$的可信度.

定理 3. 采用公式(6)的 Weighted *k-Ranks* RbRf 可以有效抵抗如下类型的共谋攻击:存在 $A\subseteq P$ 和 $j\in\{1,\ldots,n\}$,对于任意的 $a\in A$ 有 $R_f^j(a)=e\neq C_f^j$,并且其他位置 $j'\neq j,1\leqslant j'\leqslant n$, $R_f^{j'}(a)$ 等概率地随机选取 $P/\{e\}$中的节点.

证明:首先分析$\forall a\in A,R_f(a)$对 $r^{j'},j'\neq j$ 的影响.由于此时满足定理 1 的条件:$R_f(a)$在 j'处等概率地随机选取 $P/\{e\}$中的节点,等价于$R_f(a)$在j'处包含独立的随机错误.所以,Weighted *k-Ranks* RbRf 可有效消除这种不确定性.

定理的证明集中在分析 $R_f(a)$对 r^j 的影响上.对于返回结果 r^j,节点 e 获得的分值 $score(e)$是由下面两部分相加得出的:一部分由于 A 中的节点在位置 j 处给出的评价为 e,此部分的值为 $\sum_{a\in A}W(R_f(a))$;另一部分是在位置 j 处给出的随机错误评价 $R_f(i)$刚好等于 e 而造成的(由于 $e\neq C_f^j$),这一部分属于定理 1 中的独立随机错误.定理 1 表明,此部分对 r^j 的影响随 n 而呈指数衰减,可以忽略不计.

由公式(6),$W(R_f(a))$也由两部分组成:一部分是 $R_f(a)$在 j'处与其他节点评价的一致程度,可以用期望值代替公式(6)中的这种在j'处评价一致的次数.由于 $R_f^{j'}(a)$ 是从 n 个节点中等概率地随机选取(概率为 $1/n$),所以 $R_f^{j'}(a)$ 在公式(3)中第 j'列中出现次数的期望值为 1(定义随机变量 $B_i=1$,当 $R_f^{j'}(i)=R_f^{j'}(a)$;否则 $B_i=0$.显然,该期望值为 $E\sum_i B_i=\sum_i E(B_i)=n\times 1/n=1$).所以,此部分权值等于$(n-1)/n^2$;另一部分是 $R_f(a)$在 j 处与其他节点评价的一致程度,综合前面的分析结果,此部分权值等于 $1/n^2+|A|/n^2$($|A|/n^2$ 因为$|A|$个攻击者在位置 j 处给出的评价都为 e;$1/n^2$ 为 P/A 中的节点在位置 j 处给出的评价为 e 的期望次数).联立这些值,并令$|A|=\beta n$,

$$score(e)=|A|\times\left(\frac{n-1}{n^2}+\frac{1+|A|}{n^2}\right)=\beta(1+\beta).$$

同样的方法计算 $score(C_f^j)$:对于可信评价 $R_f(i)$,其 $R_f^j(i)$,$1\leqslant j\leqslant n$ 在公式(3)中的第 j 列出现的期望次数为 αn,而且 $R_f^j(i)=C_f^j$ 的 i 出现次数的期望值也为αn,联立后,有

$$score(C_f^j)=\alpha n\times\left(\frac{n\times\alpha n}{n^2}\right)=\alpha^2 n.$$

显然,随着 n 的增大,$score(e)<<score(C_f^j)$,且其差值是 n 的多项式,即有 $\Pr(r^j=e)=1/O(p(n))$,RbRf 选取 e 的概

率将以 n 的多项式速度衰减为 0.综上分析,Weighted *k-Ranks* RbRf 可以有效消除此类 $R_f(a)$的影响.证毕. □

定理 3 分析的共谋攻击是部分节点对节点 c 进行哄抬(即 CBA,对于 CDA 类似)的一类攻击:这些节点对 c 一致赞扬,而在其他排名位置随便选取.当恶意节点 c 控制一些 P2P 节点时,就可以实施对 c 的哄抬攻击.c“控制”的节点通常就是 c 用其他 ID 进入系统的“新节点”,这些新节点在其他大多数排名位置上随机产生节点填入.

推论 1. Weighted *k-Ranks* RbRf 能够有效消除带有随机错误的 $R_f(p,Q)$中包含的不确定性或恶意攻击.

推论 1 表明,Weighted *k-Ranks* RbRf 在绝大多数环境下可以正确工作,但不能应对针对 RbRf 设计的 SCA 攻击算法(如图 4 所示).由于该攻击针对 RbRf 设计,所以本文将其称为 Sophisticated Collusive Attack(简称 SCA).

Algorithm. SCA(Attack RbRf).
Input: Node c, boosting target c_1, boosting rank position k_1, query Q;
Output: Sophisticated malicious $R_f(c,Q)$.
(1) $c\rightarrow W$: $R_f(Q)$
(2) c chooses a rank $\{...,x,...,c_1,...\}$ from $R_f(Q)$
(3) c get the rank position (noted as k_2) of c_1
(4) exchange the elment of location k_1, k_2 in $\{...,x,...,c_1,...\}$,i.e. exchange x and c_1
(5) return $\{...,c_1,...,x,...\}$

Fig.4 Sophisticated collusive attack

图 4 SCA 攻击算法

定理 4. Weighted *k-Ranks* RbRf 不能抵抗 SCA 攻击.

证明:在分析 SCA 时,可以假定 c 从 $R_f(Q)$中选取的排名$\{...,x,...,c_1,...\}$是一个正确的排名;否则,由定理 3,Weighted *k-Ranks* RbRf 能有效处理 $R_f(c,Q)=\{...,c_1,...,x,...\}$.当$\{...,x,...,c_1,...\}$正确时,令公式(6)计算该排名的权值为 w.对于 $R_f(c,Q)=\{...,c_1,...,x,...\}$,设公式(6)计算该排名的权值 w':

$$|w-w'|=\frac{1}{n^2}\sum_{k=k_1,k_2}\left|\sum_{\{...,x,...,c_1,...\}^k=R_f^k(w)\wedge w\in\{1,...,n\}}1-\sum_{\{...,c_1,...,x,...\}^k=R_f^k(w)\wedge w\in\{1,...,n\}}1\right|\leqslant\frac{1}{n^2}|2(n-1)|\leqslant\frac{2n}{n^2}=\frac{2}{n}.$$

$|w-w'|=o(1)$表明,$R_f(c,Q)=\{...,c_1,...,x,...\}$的权值与一个正确排名的权值是不可区分的,所以 Weighted *k-Ranks* RbRf 中的权值没有作用,Weighted *k-Ranks* RbRf 等同于 *k-Ranks* RbRf.再由定理 2,有 *k-Ranks* RbRf 不能处理此类共谋攻击,因此定理 4 成立.证毕. □

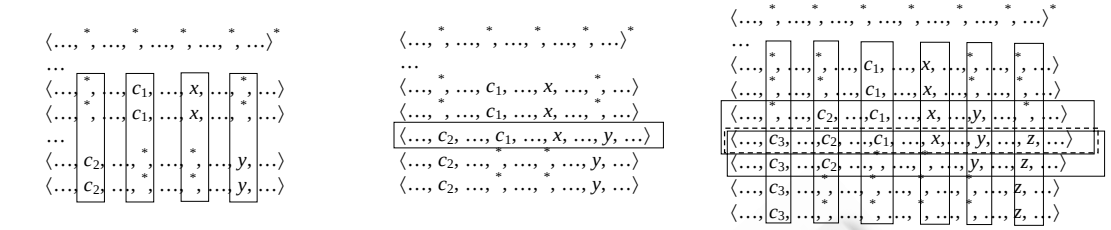
1.2 RbRf对SCA的处理

由于 SCA 排名$\{...,c_1,...,x,...\}$与一个正确排名$\{...,x,...,c_1,...\}$在 $n-2$ 个位置上完全相同,只在 2 个位置上不同,与 $n-2$ 的关系是 $O(1/p(n))$,所以很难构造一个能够有效区分这两个排名的可计算函数.定理 4 的证明过程也充分说明了这一点.而由于 RbRf 无法有效区分 SCA 排名和一个正确的排名,所以从算法本身出发,RbRf 不能有效对抗 SCA 攻击.

有趣的是,通过分析 SCA 排名可以看出:在 SCA 排名给 RbRf 引入少量恶意错误的同时,也使更多位置的正确排名信息进入 RbRf.对于上例,一个 SCA 排名$\{...,c_1,...,x,...\}$让 2 个位置 k_1 和 k_2 的错误排名参与到 RbRf 的计算中,但同时让其他 $n-2$ 个位置上的正确排名信息进入了 RbRf.这就说明,SCA 排名反而使 RbRf 在 k_1 和 k_2 以外的排名位置上更可能计算出正确的结果.所以,当系统中存在多个哄抬目标不同的 SCA 攻击时,就很可能出现如图 5(a)所示的情况.此时,一个哄抬 c_1 的 SCA 与一个哄抬 c_2 的 SCA 可以相互抵消(图 5(a)中的竖向矩形显示了这种中和效果),未对 RbRf 产生任何影响,可以认为 RbRf 完全“消除”了 SCA 的恶意影响.

显然,要想让多个哄抬目标的 SCA 排名集合不被中和的唯一方法是不同哄抬目标的 SCA 排名集合之间存在交集,即如图 5(b)所示的情形(图中的横向矩形包含的排名就是这样的交集).还有一点显然可知的事实是,只有当交集中元素的个数大于带“*”的排名(诚实的排名)个数时,SCA 攻击才能对 RbRf 产生影响.图 5(c)表明,当 RbRf 中同时存在 3 个哄抬目标 c_1,c_2,c_3 的 SCA 攻击时,也存在同样的中和效果.分析图中每个竖向矩形包含的节点集合,可对这个集合和图中横向虚线矩形包含元素的集合做交集.如果将这个交集中的元素从竖向矩形表示的集合中去掉(对于图 5(c)中最左边的竖向矩形,去掉的元素为 c_3),SCA 引入的正确评价(图 5(c)中的“*”号)个

数不小于 SCA 引入的恶意评价,多个哄抬目标的 SCA 被相互中和.这就表明,3 个哄抬目标的 SCA 对 RbRf 真正有效的攻击集中在这些 SCA 的交集上.这样的结论对于多于 3 个哄抬目标的 SCA 也是成立的.



(a) Case of counteraction of two SCAs (b) Case of intersection between two SCAs (c) Case of three SCAs in RbRf
(a) 两个 SCA 相互抵消的情况 (b) 两个 SCA 存在交集的情况 (c) 3 个 SCA 出现在 RbRf 中的情况

Fig.5 Some cases of several simultaneous SCAs
图 5 多个 SCA 攻击并存的几种类型

上面的分析表明,只要诚实的排名个数大于各哄抬目标 SCA 的交集大小,RbRf 就能有效“消除”SCA.假定 RbRf 中针对 m 个哄抬目标的 SCA 是无预谋的,设 n 个排名反馈 R_f 中诚实排名的个数为 t,对于剩下的 $n-t$ 个 SCA 排名中的每个排名独立等概率(概率为 $1/m$)地属于哄抬 c_i,$1\leqslant i\leqslant m$ 的 SCA.$n-t$ 个 SCA 排名中属于 m 个哄抬目标交集的排名个数(即交集的大小)的数学期望值为

$$(n-t)\times \Pr(\text{一个 SCA 排名对 } m \text{ 个目标同时哄抬})=(n-t)/(m^m).$$

RbRf 能够有效“消除”SCA 意味着

$$t\geqslant \frac{n-t}{m^m}\Rightarrow m^m+1\geqslant \frac{n}{t}\Rightarrow t\geqslant \frac{n}{m^m+1} \tag{7}$$

对于公式(7),当 $m^m=n$,即 $m=O(\log n)$时,只要保证 $t=O(1)$,就能有效“消除”SCA.

推论 2. 当 n 个排名反馈中同时存在 $O(\log n)$个不同哄抬目标的独立的 SCA 排名,且在这 n 个排名反馈中存在常数个诚实排名时,Weighted *k-Ranks* RbRf 仍能有效工作.

推论 2 给 RbRf 一个启发:如果能在已经收集的排名反馈中加入少量确定诚实的排名,就可以抵消 SCA 交集对 RbRf 的影响.由于节点在进行 RbRf 计算时,自己给出的排名也是 RbRf 的输入,通常可以假定这个排名一定诚实,所以在 RbRf 之前,节点 r 可以将自己给出排名的多个副本作为输入,本文将这种机制称为 *dupR*.对于 *dupR*,引入副本的数量应该尽量小,否则就会使 RbRf 陷入自己给出的排名中的非恶意错误之中,从而失去了名誉评价的意义.结合公式(7)的数量关系,本文将该值设置成一个很小的常数(通常取数值 2).

推论 2 表明,RbRf 能在独立的 SCA 下有效工作,但如果多个哄抬目标的 SCA 之间存在很大的相关性,这些 SCA 就不能互相中和,此时,RbRf 就不再能有效工作.为了与独立的 SCA 攻击相区别,本文将这类 SCA 称为共谋 SCA,简记为 CSCA.CSCA 需要在 P2P 网络中工作的节点真正共谋:这些节点$(c_1,c_2,...,c_m)$形成一个“整体”,对于名誉查询 $R_f(Q)$,c_i,$1\leqslant i\leqslant m$ 应答的排名反馈都是$\langle\ldots,c_i,\ldots,c_j,\ldots,c_k,\ldots,x,\ldots,y,\ldots,z,\ldots\rangle$.此时,$m$ 个 CSCA 排名在 m 个排名位置上与其他 $n-m$ 个诚实排名不一致(由于 Weighted *k-Ranks* RbRf 可以排除随机错误,这里假定 n 个排名中没有这样的随机错误),在其他 $n-m$ 个位置上与 $n-m$ 个诚实排名一致.因此,一个 CSCA 排名在 Weighted *k-Ranks* RbRf 中获得的权值为 $m\times m/n^2+(n-m)\times n/n^2=(m/n)^2-m/n+1=(m/n-1/2)^2+3/4\geqslant 3/4$.这表明,无论 m 如何取值,CSCA 排名都能参与到 RbRf 的计算中.这说明,RbRf 需要借助其他机制来抵抗 CSCA 攻击.

对于 CSCA 中的 m:(I) 当 $m=O(1)$时,由于 m 较 n 而言很小,这 m 个 CSCA 排名对 RbRf 的影响可被常数个诚实的排名消除,*dupR* 机制可发挥作用;(II) 当 $m=O(n)$且 $m<n/2$ 时,m 的规模大到 *dupR* 无法消除 CSCA,但由于 $m<n/2$,诚实排名能够将 CSCA 对 RbRf 的影响抵消(由于多个“整体”的 CSCA 共存时同样存在上面分析的中和效应,所以相当于只出现一个“整体”.此时,除了 m 个 CSCA 排名以外,其他 $n-m>n/2>m$ 个排名是诚实排名);(III) 当 $m=O(n)$且 $m\geqslant n/2$ 时,一半以上节点共谋给出一致的欺骗信息,RbRf 无法给出正确结果.对于 P2P 大规模

自治网络,半数以上节点形成 CSCA 的可能性很小;但如果节点只收集局部范围内的排名信息,而在局部容易形成共谋整体.此时,n 变小而 m 不变,形成如图 6 所示的有效 CSCA 攻击模式.本文将在第 1.3 节给出处理方法.

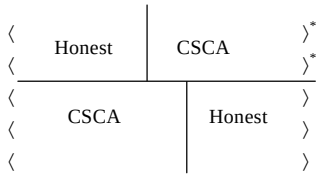


Fig.6 Representative scheme of effective CSCA

图 6 有效 CSCA 攻击的典型模式

1.3 在局部排名反馈上的RbRf

上面的结论都是针对全局 RbRf 模型的,但对于实际大规模 P2P 网络而言,全局 RbRf 的假设存在下面两点不足:(1) 针对 r 的名誉查询 Q,不是所有节点 $p\in P$ 都会给出其排名反馈 $R_f(p,Q)$;(2) 节点给出的排名反馈中通常不能包含所有节点.对于不足(1),由于 r 收到部分节点给出的排名反馈,所以 r 处 RbRf 的输入是 $n<|P|$个排名反馈,但在定理 1~定理 4 的证明中并不需要 $n=|P|$的条件,所以这种局部性对 RbRf 没有实质影响,后面的实验数据都是在收集部分排名反馈上获得的.对于不足(2),当 RbRf 的输入 R_f 只包括部分节点时,R_f 在排名位置上无法对应,图 3 中的竖向矩形就失去了意义,RbRf 算法不再正确,这是局部排名反馈对 RbRf 的主要影响.当 R_f 是 P 中部分节点的排名时,RbRf 要解决的主要问题是排名位置的对齐问题(APoLR):

定义 4(APoLR(align problem of local RbRf)). 给定一个包含部分节点的排名反馈 $R_f=\langle p_{i1},p_{i2},...,p_{ik}\rangle,k\leqslant n=|P|,R_f$ 上的 APoLR 就是寻找这样的一个包含 P 中全部节点的排名反馈 $R_{f'}=\langle \alpha_1,p_{i1},\alpha_2,p_{i2},\alpha_3,...,\alpha_k,p_{ik},\alpha_{k+1}\rangle$,其中,$\langle \alpha_1,\alpha_2,\alpha_3,...,\alpha_k,\alpha_{k+1}\rangle$是集合 $P/\{p_{i1},p_{i2},...,p_{ik}\}$上的一个置换且使 $R_{f'}$在 Weighted *k-Ranks* RbRf 中的权值最大.

APoLR 的基本要求是,在让补齐位置不影响原 R_f 可信度评价的前提下补齐 R_f 为 $R_{f'}$,所以 $R_{f'}$中引入的补齐节点不应该对其他排名的可信度评价产生影响.因此,定义 4 中的$\langle \alpha_1,\alpha_2,\alpha_3,...,\alpha_k,\alpha_{k+1}\rangle$并不需要是实际节点,只要占位即可,这些位置用占位符“#”代替.“#”按下述方式参与 RbRf 计算:对于出现“#”的排名,“#”表示与同一排名位置上任何节点都不一致,获得的计数为 0.因此,求解定义 4 的 ApoLR 时需在排名 R_f 的适当位置上填入“#”,使得修改过的局部排名 $R_{f'}$在尽量多的排名位置上出现一致评价(体现对齐的含义).图 7 给出了一个 APoLR 的问题实例和对齐后的结果.

(a) 4 local R_f (b) 4 $R_{f'}$ after align

(a) 4 个局部排名 R_f (b) 经过对齐后的 4 个 $R_{f'}$

Fig.7 An instance of APoLR

图 7 一个 APoLR 实例

显然,APoLR 就是多序列比对问题(multiple sequence align,简称 MSA),只要将 MSA 中的基因匹配对应为 APoLR 中的一致评价,则两个问题是完全一样的.所以,与 MSA 一样,APoLR 也是一个 NPC 问题,对于 n'个排名长度分别为 $k_1,k_2,...,k_{n'}$的局部排名 R_f,找出最优对齐结果 $R_{f'}$的算法复杂度通常为

$$O(k_1\times k_2\times...\times k_{n'})\approx O(k^{n'}) \tag{8}$$

因此,需要找到一种高效的近似算法.MSA 作为生物信息处理中的一个重要问题,存在大量的研究工作[21],本文将这些成果直接应用到求解 APoLR 中.

虽然只有部分节点给出的排名反馈 R_f 在本质上不会对 RbRf 造成影响,但在局部排名集合中出现 CSCA 情形(如图 6 所示)的可能性会增大.可以通过对获取 R_f 的过程进行控制来抵抗 CSCA.由于通常局部范围内的节点集合要比网络上随机选取的节点集合更可能形成共谋,在这样的假设基础上,节点 r 可以按下述方式控制 $R_f(Q)$ 查询:(1) 每个"局部团体"都只收集固定数量的(如 l 个)R_f;(2) r 能收到多个(如 g 个)不同"局部团体"返回的排名反馈.因此,本文设计了一个 $R_f(Q)$搜索应答协议 RFSP(rank feedback search protocol)(如图 8 所示),其中的 *RQW* 查询包按随机走动方式路由,目的是尽量避免在一个局部收集所有反馈.*RQW* 用两个 *TTL* 值(*TTL*1 和 *TTL*2)来控制查询包的路由,当图 8 中的节点 p 收到 *RQW* 包时,首先对 *TTL*2 减 1,当该值从 2l 减到 0 时,由该节点发起广播查询数据包 *RQB*.同时,该节点再产生一个 *TTL*1=*TTL*1−1,*TTL*2=2l 的 *RQW* 包继续随机游走.广播查询包 *RQB* 用来收集一个局部的名誉反馈,收到 *RQB* 数据包的节点给请求节点 r 发送名誉反馈应答包 *RQS*.RFSP 中的 *RQW* 可在 CSCA 中引入随机因素,为 RbRf 对 CSCA 的抵抗创造了条件.对于 RFSP 的工作效果,本文在第 2.2 节以抵抗 SCA 的能力为指标对 RFSP 进行了实验分析.

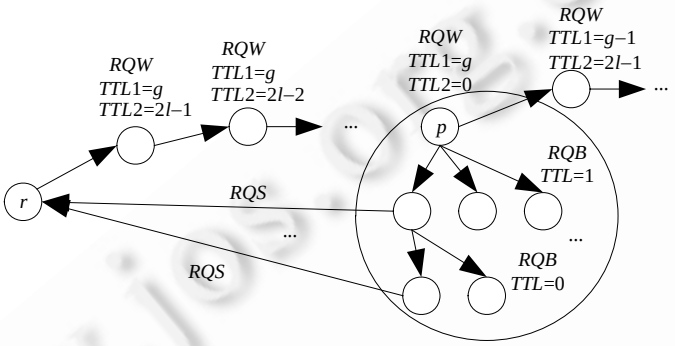


Fig.8 RFSP: Rank feedback search protocol

图 8 排名反馈搜索协议 RFSP

1.4 RbRf的实现

为应对实际 P2P 网络中出现的各种名誉评价问题(如名誉欺骗、局部排名等),RbRf 变成了一个需要由多个模块组成的完整系统,图 9 给出了 RbRf 系统的基本结构.

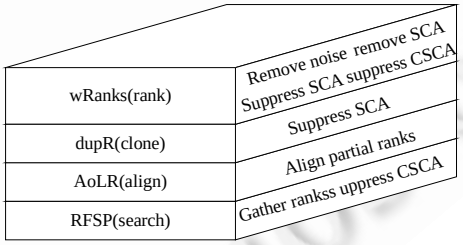


Fig.9 Fabric of RbRf

图 9 RbRf 的基本结构

2 RbRf 的实验验证

2.1 实验平台

本文采用 NetLogo 模拟工具对 RbRf 进行实验验证.NetLogo 是一个基于多 Agent 的 AI 群落模拟工具[22],由于若干典型的名誉评价机制已经在 NetLogo 上实现并得以深入分析[11],所以采用 NetLogo 作为实验平台可以方便地将 RbRf 与这些典型 P2P 名誉计算机制进行实验对比.本文用 NetLogo 的一个 Agent 模拟一个 peer 的行

为,将时间离散地分割为多个模拟周期,在每个模拟周期中:

(1) 网络中随机选取 50%(这是模拟实验中的一个可调参数,但该参数对实验结果几乎没有影响,所以本文只取 50%)的节点向网络中的节点发起查询;

(2) 启动名誉评价机制,并根据计算结果选取一个可信节点进行服务交互;

(3) 请求节点在交互结束后给出本次交互的评价,并将交易记录写在其历史列表中.

P2P 名誉机制的核心是,在存在大量恶意节点的 P2P 网络中找出可信节点进行服务调用,因此,成功交互次数在总的交互次数中所占的比率是名誉机制的直接表现,本文将以该比率作为基本实验评价参数.定义 η_g 为模拟过程中成功的服务个数,η_b 为失败服务个数,名誉评价的效果 R_E 定义为

$$R_E=\frac{\eta_g}{\eta_g+\eta_b} \tag{9}$$

2.2 RbRf的名誉评价效果

图 10 对 3 类有代表性的 P2P 名誉评价模型在同样的模拟实验场景下进行了实验对比:选取了 1 000 个 peer 组成无结构 P2P 网络.其中,20%(对应可调参数 *BadRatio*,简记为 *BR*)的节点是坏节点(即总回复失败的服务),其他节点回复成功服务的概率设置为 0.6~1.0 上均匀分布的随机数(体现出好节点在提供某类服务上的能力差异).其中,给出恶意名誉反馈(如果恶意节点 w 根据历史交互信息得出目标节点 g 的交易可信度为 $h\in[0,1]$,则 w 给出的名誉反馈 $tr_{wg}=1-h$)的推荐节点比率设为 20%(对应可调参数 *MalRatio*,简记为 *MR*).其中,每个节点以 0.8(对应可调参数 *CapRecom*)的概率正确地评价推荐节点的推荐可信度(体现为根据交易结果对公式(1)中的 c_{rw} 做出了正确调整,由于某些诚实的推荐节点能力不足,给出错误的名誉反馈会导致 c_{rw} 的调整出现错误,模拟参数 1−*CapRecom* 用来表示出现这种情况的可能性).

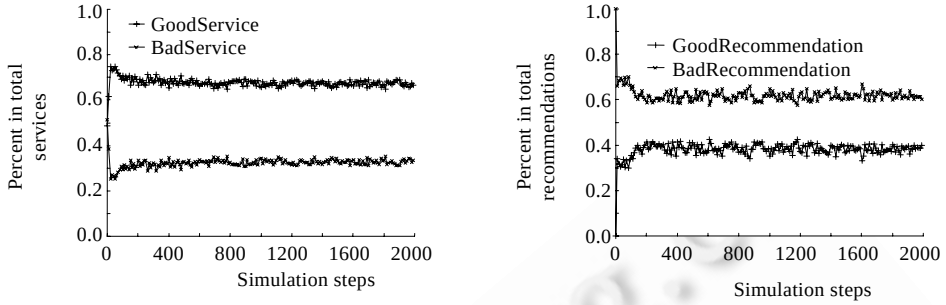
图 10(a)给出了文献[13]提出的基于公式(1)的典型加权名誉评价模型的效果 R_E,c_{rw} 评价了 rater 的推荐能力,其调整方法是 $c_{rw}=\alpha\times c_{rw}+(1-\alpha)\times e$.其中,$e\in\{-1,1\}$表示交易结果与 w 的推荐值之间是否一致.图 10(b)给出的是文献[11,12]提出的均值名誉评价模型的 R_E,其核心思想是,用 $R=(\sum_{w\in W}tr_{wg})/|W|$ 来代替公式(1)中 R 的计算.图 10(c)给出了 RbRf 的名誉评价效果,并且是部分节点形成排名反馈(即第 1.3 节描述的局部排名)后输入 RbRf 后产生的效果,这是由于,让系统中的 1 000 个节点都参与 RbRf 运算既不符合事实也没有意义.本实验中,推荐节点从节点集合中选取 10 个节点形成排名反馈 R_f,名誉评价节点将这些排名反馈对齐后再执行 RbRf.本文后续的 RbRf 实验中也都采用了同样方法,且 R_f 的长度也都设置为 10.

从图 10 可以看出,WRA 和 AVG 具有基本相同的成功服务比率,但 AVG 中的正确推荐数量较 WRA 明显要高.这一结果表明,在 P2P 这样的开放环境中,由于推荐节点会给出恶意的和“善意”的错误推荐信息,而开放环境又无法对其有效区分,所以 WRA 在聚合名誉时给推荐者一个权值反而较 AVG 的均值聚合会导致产生更多的错误评价.

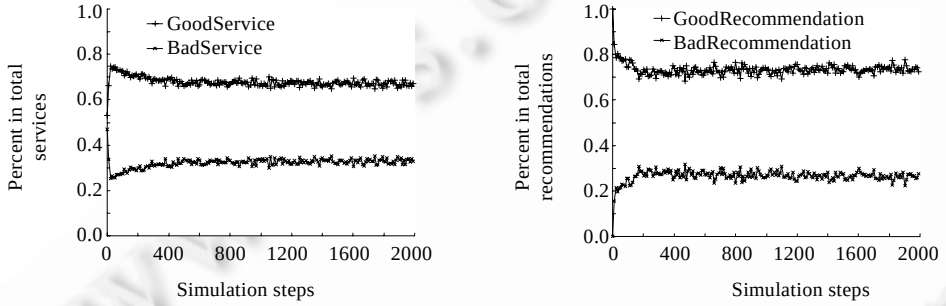
另一方面,WRA 中不相等的权值可以突出提供成功服务能力较高的目标节点(实验设置时,好节点的服务能力是 0.6~1.0 的均匀随机数),AVG 的聚合由于采用了相等的权值而没有这样的突出能力,所以,在上面的实验环境中,AVG 和 WRA 的优缺点抵消后产生接近相同的 R_E.实际上,此时两者的 R_E 已接近于不采用名誉机制的“盲交易”(可从图 11 的实验结果看出).相比 WRA 和 AVG,RbRf 与 AVG 一样,不需要评价推荐节点的可信度,又用 rank 中包含的信息实现与 WRA 一样的突出高能力好节点的功能,所以 RbRf 的 R_E 要明显地高得多.而对于图 10(c)中 R_E 在某些地方出现的明显下降,则是由于 rank 值很高,部分节点离线(本文的实验考虑了 P2P 节点的 churn)造成的.此时,大量的请求找到这些节点导致 R_E 下降.对于实际的 P2P 系统,网络中节点请求的多样性(实验中假定只有一种请求)会使这个问题所产生的影响有所降低.另外,可以在名誉评价中加入在线时间等因素来进一步减小该问题对 R_E 的影响.由于超出本文范围,将留待后续加以研究.

图 10 表现了 WRA,AVG 和 RbRf 这 3 类名誉聚合模型的评价效果和工作机理,可以看出,RbRf 在这个典型实验环境中表现出了明显优于 WRA 和 AVG 的名誉评价效果.图 11 对比了 3 类模型在各种实验环境设置下的

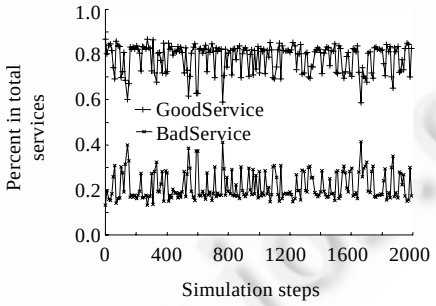
参数 R_E,结果表明,RbRf 在各种情况下,尤其是在系统中存在大量提供失败服务的节点和给出恶意推荐的节点时都能良好工作(图中的 Blind 是没有采用名誉机制的结果,表明网络中能够提供成功服务的节点比率,即 R_E.对于图 11 所示的 BR=0.6,在采用 Blind 机制时,R_E 只有 30%;而在采用 RbRf 时,R_E 为 80%以上,这说明 RbRf 能够有效地发现网络中可信度高的节点).



(a) R_E of weighted reputation aggregation (WRA)
(a) 加权名誉聚合模型的名誉评价效果



(b) R_E of average reputation aggregation (AVG)
(b) 均值名誉聚合模型的名誉评价效果



(c) R_E of rank feedback model (RbRf)
(c) 排名反馈评价模型的名誉评价效果

Fig.10 Effect of three representative reputation models
图 10 3 类典型名誉评价模型的效果

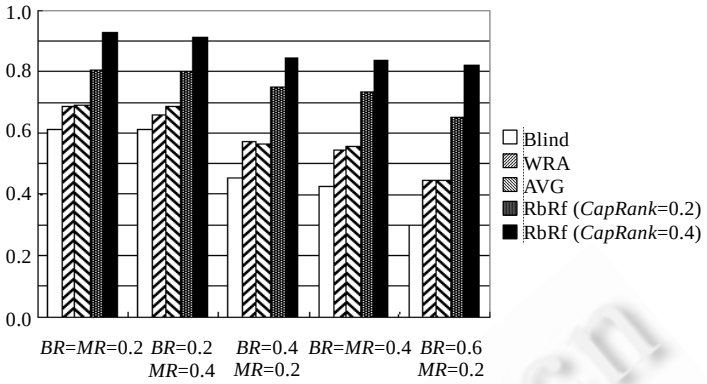


Fig.11 R_E of RbRf under various environments

图 11 各种实验环境下 RbRf 的名誉评价效果

2.3 RbRf应对共谋攻击的效果

图 11 表明,RbRf 较其他名誉评价模型更适应于存在大量非恶意错误的开放 P2P 环境,本节分析共谋攻击下 RbRf 的名誉评价效果.图 12 给出了在 CBA 攻击下 RbRf 的工作效果.不失一般性,这里,假定网络中有比率为 ColRatio(简记为 CR)的节点对网络中的某些节点进行共谋哄抬,本实验选取的哄抬目标是 1000×*BR*(这里,*BR* 设定为 20%)=200 个那些总给出失败服务的节点,即所有的 bad peers 都是哄抬目标,设计这样一种强大的攻击模式是为了突出各类名誉评价机制应对共谋攻击的能力.

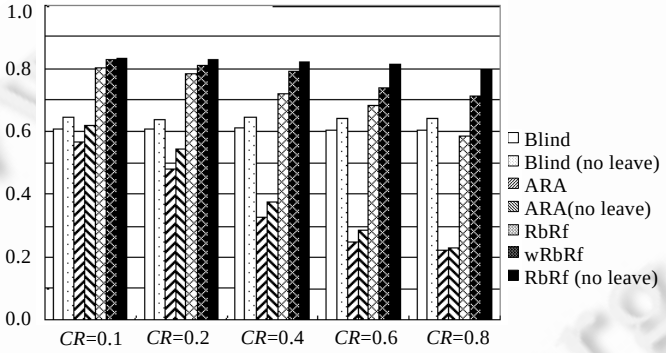


Fig.12 R_E of RbRf under collusive boost attack

图 12 RbRf 应对 CBA 攻击的效果

图 12 表明,即使在共谋攻击节点在整个网络中占据很大比例时,RbRf 较其他名誉机制也仍能较好工作.从图中 R_E 数值可以看出:当 *CR* 较大时(*CR*≥10%),现有的名誉评价模型 AVG 已经不能工作,导致成功服务数量比没有名誉评价机制的随机选取还要小;且会随着 *CR* 的增大而显著减小.相比而言,RbRf 即使在 *CR* 很大(*CR*=60%)时,名誉评价机制仍在发挥作用.而在 RbRf 上引入加权机制,即 wRbRf 可以在 *CR* 非常大(*CR*=0.8)时仍能有效工作.这表明,wRbRf 能够很有效地应对共谋攻击,这与前面的理论分析结果是一致的.另外,从图的数据还可以看出,wRbRf 受 *CR* 增大的影响很小,且节点动态变化时,wRbRf 受 *CR* 的影响要大一些.这是由于,随着 *CR* 的增大,wRbRf 选取出的候选服务节点变少,而节点振荡的概率是固定的,所以影响就要大一些.对于不考虑节点动态变化的 wRbRf,在各种 *CR* 设置下都能使 R_E 在 80%左右.这说明,共谋攻击几乎不会对 wRbRf 产生影响,而影响该 R_E 数值的是 wRbRf 算法本身的参数,这一点可以从图 14 看出.图 14 分析了 wRbRf 收集的排名反馈的个数(对应可调参数*#RankFbs*)对 R_E 的影响(可以看出,随着*#RankFbs* 的增大,RbRf 的效果显著增加).本节和上一节给出的实验结果都是在*#RankFbs*=10 时得出来的,设定*#RankFbs*=10 是由于现有的名誉评价模型要从节

点的邻居或二阶邻居中收集名誉反馈.本实验定义节点的邻居个数为 6,所以这里选取一个在 6 和 36 之间且很接近 6 的数作为*#RankFbs*,以增加 RbRf 和现有名誉评价模型的可比性.图 11 分析了 RbRf 处理诚实节点给出随机错误的能力,图 12 分析了 RbRf 应对共谋节点给出恶意错误的能力,结果表明,RbRf 在处理开放 P2P 网络中出现的名誉反馈错误时明显优于其他名誉评价.

对于专门针对 RbRf 构造的一类特殊的共谋攻击 SCA,图 13 给出了 wRbRf 应对 SCA 的效果分析.结果表明,多哄抬目标 SCA(对应图中的 SCA-mbo)不仅对 wRbRf 的评价效果没有影响,还因反馈中引入的大量正确信息而使评价效果变得非常好(明显高于图中的 CBA),与推论 2 一致(这是 RbRf 机制显著优于其他名誉评价机制的又一体现).而对于单哄抬目标的 SCA(对应图中的 SCA-sbo,单目标 SCA 就是 CSCA),wRbRf 的评价效果显著下降.而由图中 SCA-sbo(with RFSP)可以看出,由 RFSP 引入的随机因素使得 wRbRf 能够有效降低 CSCA 产生的负面影响.另外,图 13 中的 SCA-mbo(with *dupR*)和 SCA-sbo(with RFSP+*dupR*)分析了 *dupR* 机制对 SCA 的影响.结果表明,*dupR* 机制具有抑制 SCA 攻击的能力,符合前文的理论分析.

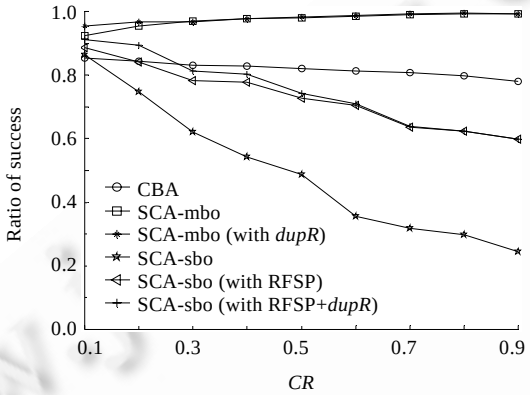


Fig.13 R_E of wRbRf under sophisticated collusive attack

图 13 wRbRf 应对 SCA 攻击的效果

2.4 RbRf的效率

RbRf 在具有良好名誉评价效果的同时,也具有较高的效率,下面我们从评价时间、存储空间和通信负载 3 个方面分析 RbRf 的效率.在每次需要进行可信度评价时,RbRf 首先从 P2P 网络上收集到一定数量的排名反馈,然后在本地应用 wRbRf 算法处理这些排名反馈.所以,RbRf 的时间开销就是在本地执行的 wRbRf 算法的时间开销,这里的时间开销主要集中在诸如权值计算、排名对齐等运算上.通过图 14 的结果可以看出,RbRf 的输入规模通常都较小(在 6~36 之间),所以,对于目前的构成 P2P 网络主体的 PC 机而言,这样的时间开销并不影响 RbRf 的可用性.而对于空间开销,只需在运算过程中存放一定数量(由图 14 可知,这个值通常很小)的排名反馈,其他需长期维护的信息(如路由表等)直接使用 P2P 系统现有的即可,所以,空间复杂性和相应的维护代价要明显低于现有的 P2P 名誉评价机制(这些机制

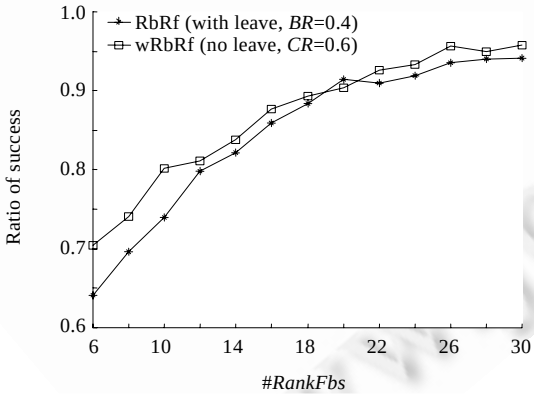


Fig.14 R_E of RbRf (wRbRf) under different number of rank feedbacks

图 14 排名反馈数量对 RbRf 和 wRbRf 的影响

通常都需维护一个推荐节点表).所以,影响 RbRf 效率的关键是通信负载,即 RbRf 需要的排名反馈个数 #*RankFbs*.图 14 详细分析了该参数对 R_E 的影响,可以看出,即使网络中存在大量的动态节点和恶意节点,当收集的排名反馈个数超过 20 时,RbRf 就能发挥很好的名誉评价效果(R_E 接近或超过 95%,几乎达到上界).20(排名反馈个数)也远小于二阶邻居节点个数 36,这表明,RbRf 在取得良好效果的同时,通信代价相比其他名誉评价机制而言还要小一些.

3 结束语

本文提出了一种基于排名反馈的 P2P 名誉评价模型 RbRf,RbRf 与现有的 P2P 名誉评价机制存在两方面的显著不同:(1) 推荐节点给出的名誉反馈不再是一个分值,而是一个排名序列.相比一个数字而言,排名反馈携带了更丰富的含义,可以让 P2P 名誉评价机制有效地应对 P2P 的复杂环境及其上存在的各类恶意攻击;(2) 在进行 P2P 名誉聚合时,只需处理推荐节点给出的排名反馈即可,无需评价推荐节点的可信度,也不需要维护推荐节点的信息,推荐节点给出的反馈信息只在本次名誉评价中发挥作用.对于类 P2P 的开放式网络环境而言,这种与历史无关的计算在效率和性能上面更优(BT 中的 TFT 体现了同样的思想).

本文从理论上对 RbRf 处理随机错误的能力进行了建模和分析,在此基础上,又定义了区别于随机错误的针对 P2P 名誉的恶意攻击系列:CBA,SCA,CSCA,并在 RbRf 框架中设计了应对这些恶意攻击的方法.对这些方法的数学建模和理论分析表明,RbRf 中随机错误的影响随排名反馈的数量呈指数衰减,CBA 对 RbRf 的影响随排名反馈数量的多项式而减小,SCA 由于必须给 RbRf 引入正确信息而导致恶意攻击在 RbRf 中可被有效中和.总之,RbRf 在处理开放网络环境的复杂因素和抵抗恶意攻击两个方面都表现出优于其他 P2P 名誉评价机制的能力,仿真实验也充分验证了上述结果.另外,对于在实际环境中只能收集到部分排名反馈的局部 RbRf 和排名反馈的搜索获取,本文也给出了详细的处理方法.

References:

[1] Marti S, Garcia-Molina H. Taxonomy of trust: Categorizing P2P reputation systems. Computer Networks, 2006,50(4):472−484. [doi: 10.1016/j.comnet.2005.07.011]

[2] Resnick P, Zeckhauser R, Friedman E, Kuwabara K. Reputation systems. Communications of the ACM, 2000,43(12):45−48. [doi: 10.1145/355112.355122]

[3] Cornelli F, Damiani E, Vimercati SDC, Paraboschi S, Samarati P. Choosing reputable servents in a P2P network. In: Lassner D, ed. Proc. of the 11th Int'l World Wide Web Conf. New York: ACM Press, 2002. 376−386. [doi: 10.1145/511446.511496]

[4] Kamvar SD, Schlosser MT, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. In: Richter V, ed. Proc. of the 12th Int'l World Wide Web Conf. New York: ACM Press, 2003. 640−651. [doi: 10.1145/775152.775242]

[5] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. on Knowledge and Data Engineering, 2004,16(7):843−857. [doi: 10.1109/TKDE.2004.1318566]

[6] Zhou RF, Hwang K. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans. on Parallel and Distributed Systems, 2007,18(4):460−473. [doi: 10.1109/TPDS.2007.1021]

[7] Papaioannou TG, Stamoulis GD. Reputation-Based policies that provide the right incentives in peer-to-peer environments. Computer Networks, 2006,50(4):563−578. [doi: 10.1016/j.comnet.2005.07.024]

[8] Almenarez F, Marin A, Diaz D, Sanchez J. Developing a model for trust management in pervasive devices. In: Werner B, ed. Proc. of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec). Washington: IEEE Computer Society Press, 2006. 267−272. [doi: 10.1109/PERCOMW.2006.41]

[9] Sun Y, Yu W, Han Z, Liu KJR. Trust modeling and evaluation in ad hoc networks. In: Miller A, ed. Proc. of the Global Telecommunications Conf. (Globecom). New York: IEEE Communications Society Press, 2005. 1862−1867. [doi: 10.1109/GLOCOM.2005.1577971]

[10] Papaioannou TG, Stamoulis GD. Achieving honest ratings with reputation-based fines in electronic markets. In: Belding E, ed. Proc. of the 27th IEEE Annual IEEE Conf. on Computer Communications (Infocom). New York: IEEE Communications Society Press, 2008. 1040−1048. [doi: 10.1109/INFOCOM.2008.158]

[11] Liang ZQ, Shi WS. Analysis of ratings on trust inference in open environments. Performance Evaluation, 2008,65(2):99−128. [doi: 10.1016/j.peva.2007.04.001]

[12] Liang ZQ, Shi WS. PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing. In: Sprague RH, ed. Proc. of the 38th Hawaii Int'l Conf. on System Sciences. Hawaii: IEEE Computer Society Press, 2005. 201−210. [doi: 10.1109/HICSS.2005.493]

[13] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks. In: Kamkar M, ed. Proc. of the 3rd Int'l Conf. on Peer-to-Peer Computing (P2P). Washington: IEEE Computer Society Press, 2003. 150−157. [doi: 10.1109/PTP.2003.1231515]

[14] Srivatsa M, Xiong L, Liu L. Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks. In: Ellis A, ed. Proc. of the 14th World Wide Web Conf. New York: ACM Press, 2005. 422−431. [doi: 10.1145/1060745.1060808]

[15] Dou W, Wang HM, Jia Y, Zou 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

[16] Jiang SX, Li JZ. A reputation-based trust mechanism for P2P e-commerce systems. Journal of Software, 2007,18(10):2551−2563 (in Chinese with English abstract). http://www.jos.org.cn/1000- 9825/18/2551.htm [doi: 10.1360/jos182551]

[17] Zhang Q, Zhang X, Wen XZ, Liu JR, Ting Shan. 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 [doi: 10.1360/jos170096]

[18] Tian CQ, Zou SH, Wang WD, Cheng SD. A new trust model based on recommendation evidence for P2P networks. Chinese Journal of Computers, 2008,31(2):270−281 (in Chinese with English abstract).

[19] Li XY, Gui XL. Research on dynamic trust model for large scale distributed environment. Journal of Software, 2007,18(6): 1510−1521 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1510.htm [doi: 10.1360/jos181510]

[20] Luis A, Ginosar S, Kedia M, Liu R, Blum M. Improving accessibility of the Web with a computer game. In: Proc. of the ACM Special Interest Group on Computer-Human Interaction Conf. on Human Factors in Computing Systems. New York: ACM Press, 2006. 79−82. [doi: 10.1145/1124772.1124785]

[21] Notredame C. Recent evolutions of multiple sequence alignment algorithms. PLOS Computational Biology, 2007,3(8):1405−1408. [doi: 10.1371/journal.pcbi.0030123]

[22] Wilensky U. Netlogo. 2009. http://ccl.northwestern.edu/netlogo

附中文参考文献:

[15] 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

[16] 姜守旭,李建中.一种 P2P 电子商务系统中基于声誉的信任机制.软件学报,2007,18(10):2551−2563. http://www.jos.org.cn/1000-9825/18/2551.htm [doi: 10.1360/jos182551]

[17] 张骞,张霞,文学志,刘积仁,Ting Shan. 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 [doi: 10.1360/jos170096]

[18] 田春岐,邹仕洪,王文东,程时端.一种基于推荐证据的有效抗攻击 P2P 网络信任模型.计算机学报,2008,31(2):270−281.

[19] 李小勇,桂小林.大规模分布式环境下动态信任模型研究.软件学报,2007,18(6):1510−1521. http://www.jos.org.cn/1000-9825/18/1510.htm [doi: 10.1360/jos181510]

李治军(1977－),男,内蒙古伊盟人,博士,副教授,CCF 高级会员,主要研究领域为 P2P 网络,普适计算,动态网络,操作系统.

姜守旭(1968－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为 P2P 网络,数据库,传感器网络,普适计算.

李晓义(1981－),男,硕士,主要研究领域为 P2P 网络,激励机制.