新型对等网络信任控制模型分析

唐 静[1,2], 沈乐平[1]

(1. 华南理工大学 工商管理学院, 广州 510641, lindatang_303@163.com; 2. 广东外语外贸大学 国际经济贸易研究中心, 广州 510641)

摘 要: 为了对网络中自私行为作出有效监督,形成有效的信任关系,同时解决传统 client-server 环境中的单点失效与瓶颈效应问题. 通过对社会关系网络中人际关系的观察以及采用 IT 治理思想,对其中的直接信任度算法和推荐信任度算法进行改进,形成了一种新型的 P2P 信任算法 P-Trust. 实验结果表明,在网络访问成功率和在服务热点问题上,新型的 P-Trust 算法可以有效提高网络访问命中率和成功率,以及实现网络的负载均衡. 因此,将直接信任和推荐信任两方面综合得到的新型 P-Trust 信任算法可以有效的解决 P2P 网络中的信任问题和服务器瓶颈问题.

关键词: IT 治理;对等网络;信任控制;推荐值;节点

中图分类号: TP309 **文献标志码:** A **文章编号:** 0367-6234(2010)07-1172-05

Analysis of a new P2P trust control model

TANG Jing[1,2], SHEN Le-ping[1]

(1. School of Business Administration, South China University of Technology, Guangzhou 510641, China, lindatang_303@163.com; 2. Research Center for International Trade & Economic, Guangdong University of Foreign Studies, Guangzhou 510641, China)

Abstract: In order to efficiently monitor the selfish behavior in networks, form reliable relations and solve problems such as the single point of failure or bottleneck effect in traditional client-server environments, we adopt a novel P2P trust arithmetic named P-Trust based on the social people trust relation mechanism and the idea of IT governance, in which the direct trust arithmetic and the recommend trust arithmetic are modified. The P-Trust integrates the direct trust value and the recommended trust value to create the final trust value. Simulations prove that the P-Trust arithmetic can tackle the P2P trust problem in a simple and efficient way.

Key words: IT governance; P2P networks; trust control; recommended value; nodes

IT 治理是一个管理、问责制和监督的系统,其主要的目标是提高公司的竞争力和财务绩效. 在 P2P 网络[1]中,由于资源共享是节点的自愿行为,所以没法保证服务的质量,这主要表现在欺诈现象和自私现象上[2]. 对于一个公司而言,如果不懂 P2P 的设定,容易造成硬盘账号、客户信息资料等在使用者不知情的情况资料外泄等严重问题. 例如将商业机密、用户下载被分享出去. 以 Genutella 为例,在 P2P 网络中,有 25% 的节点提供假文件,10% 的节点给整个 P2P 网络提供的 87% 的文件资源,20% 的节点提供的 98% 的共享文件,大多数节点会随意的终止正在提供下载的文件的共享. 为了加强监督系统,必须对这些自私行为作出监督和惩罚. 因此,本文在 P2P 网络中建立一套完善的节点信任机制来保证服务的质量. 当用户访问共享资源时,对于多个提供相同服务的节点,首选信任度高的节点来提供服务.

收稿日期: 2010-03-10.

基金项目: 教育部人文社科基金资助项目(09YJC790053); 广东外语外贸大学'211 工程' 资助项目(GDUFS2009-10-15).

作者简介: 唐 静(1979—),女,博士研究生,讲师;
沈乐平(1960—),男,教授,博士生导师.

1 现有典型信任模型

1.1 基于 PKI 的信任模型

在这类系统中,系统中存在少数中心节点,通过 CA 颁发的证书来保证中心节点的合法性,节点的可信度由中心节点来负责. 这类系统存在中心依赖,容易单点失效. 这类系统的实例有 On sale Exchange, Donkey 等[3-4].

1.2　基于局部推荐的信任模型

在这类系统中，节点通过局部广播的方式，访问局部范围内的有限节点来得到目标节点的可信度，其获得的信任度往往具有局部性和片面性等. 如 Cornelli 对 Gnutella 的改进建议[5-6] 中采用的就是这种方法.

1.3　数据签名信任模型

该方法不是计算节点的信任度，而是计算数据的可信度. 当节点得到共享数据后，对共享数据的真实性进行判断，如果认可数据的真实性，则对该数据进行签名认证，签名越多的数据，可信度越高. 但该方法仅针对数据文件共享的应用，同时无法防止集体欺诈行为. 目前流行的文件共享应用就是采用 Kazaa 方法.

1.4　全局可信度模型

为获取全局的节点可信度，该类模型通过邻居节点间相互满意度的迭代，从而获取节点全局的可信度. Stanford 的 EigenRep[7] 采用的就是这种全局信任度模型. 但是该模型没有考虑惩罚因素，同时该模型的协议实现没有考虑网络的性能开销，每次交易都会导致在全网络范围内的迭代.

针对上述几种 P2P 信任模型各有优势和不足的情况，本文提出一种新型的信任度算法，该算法将更加简单有效. 通过对社会关系中人际信任关系的观察，注意到两个事实：1）即在信任的建立过程中，最初的信任比较容易建立，并且信任度上升比较快，当信任度上升到一定程度后，信任度会以较慢的速度上升；同时，与信任度上升相比较而言，信任度的下降速度很快，即信任失去容易建立难. 事实上也是如此，对于提供成功服务的节点，下次继续提供成功服务的可能性远比提供失败服务的节点提供失败服务的可能性要小，这样也更符合实际；2）信任是可以相互推荐的，个体间的信任度某种程度也取决于其他个体的推荐；同时，作为推荐者的可信度也决定其推荐个体的可信度. 实际上，这种互相依赖的信任关系组成了一个所谓的信任网络（Web of trust）[8]. 在这样的信任网络中，任何个体的可信度都不是绝对可靠的，但可以作为其它个体决定其交互行为的依据. 基于信任网络的 P2P 系统与人际网络有很大的相似性.

本文通过对社会人际信任关系的观察，提出了基于无结构 P2P 网络的信任模型 P-Trust，并通过仿真实验对该模型进行了研究检验. 仿真结果说明，P-Trust 模型可以很好的改善 P2P 网络中的服务质量，同时有效的惩治欺骗行为.

2　P-Trust 算法的分析

2.1　算法核心思想

P-Trust 算法得到的信任度实际上是一种综合信任度，它包含两个方面：直接信任度和推荐信任度[9]. 直接信任度来自于节点自身对共享节点的一个信任度的评价，它是基于节点对共享节点的访问历史记录；推荐信任度来自于相邻节点的推荐. 计算相邻节点对目标节点的推荐值，同时考虑相邻节点的信任值来得到推荐信任度，最后综合两种信任度得到最终的节点信任度.

2.2　定义直接信任（T_{ij}）

直接信任度表示节点 i 根据历史访问记录信息得到的对节点 j 的信任度，表示为 T_{ij}.

由于考虑信任度建立过程的特殊性：对一个陌生人的信任度从 0 到某个较低程度是较容易的，但是当到达某个高度 threshold 后，再继续提高就比较难了，只能以较慢的速度提高；同时，信任度的降低速度是很快的，只要有一次错误的欺骗，可能会导致信任丧失怠尽. 因此设计了一种特别的算法来模拟计算信任度[10]. 该算法为："低值启动，指数增加，乘法减少，加法增大".

1）低值启动节点 i 对节点 j 的信任度从一个较低的数值开始，表示为初始值 TS_{ij}. 对于每一个陌生节点，即在此之前没有访问过的节点，$TD_{ij} = TS_{ij} = 1$.

2）指数增加. 从节点 i 第 1 次访问节点 j 开始，信任度大小在开始按照指数规律增长. 节点 i 成功访问一次 j，信任度变为 2；节点 i 第 2 次成功访问 j，信任度变为 4；节点 i 第 3 次成功访问 j，信任度变为 8. 依此类推，当信任度到达门限值 threshold 时，则按照加法增大. 这也符合现实实际，对于一个陌生人，你的信任可能会随着成功的接触，信任度上升很快，但是当上升到某个程度后，会很难或者以很慢的速度继续增加信任度.

3）乘法减少. 当欺骗发生时，信任值必须减少. 当连续的 i 成功访问 j 后，某一次 i 访问 j 失败，即 j 对 i 提供虚假的共享信息，则欺骗发生. 欺骗的发生后，信任度会极速下降，下降到当前值的 1/2. 即 $TD_{ij} = TD_{ij}/2$.

4）加法增大. 加法增大有两种情况：① 当信任度到达门限值后，如果节点 i 继续成功访问节点 j，则之后的信任度虽然增加，但是增加速度会明显减慢，比较谨慎，每次只是 + 1，即：$TD_{ij} = TD_{ij} + 1$；② 当节点 i 受到节点 j 的欺骗，降低了对 j 的信任度后，当再次发生节点 i 对节点 j 的成功访

问,此时,信任度也是采用加法增大来提高信任度,$TD_{ij} = TD_{ij} + 1$.

2.3 定义推荐信任(TR_{ij})

在计算节点 i 对节点 j 的信任度时,会遇到一些特殊的情况,一个明显的例子:节点 i 刚刚才加入 P2P 网络,因为它没有访问任何其它节点,这时它就没有保存任何其它节点的信任度,即对于其它任意一个节点的信任度均相同,均为1. 但是实际事实并非如此,已有的网络在之前的运行过程中,已经对节点 j 有了一个相对明确的信任度,即其它节点访问过 j,对 j 已经计算了信任度;此时,节点 i 查询周围邻居节点来得到对节点 j 的信任度.

计算推荐值要在一定的范围内计算,本文采用树型结构来表示节点 i 以及周围邻居节点的拓扑结构. 以节点 i 为树根,以邻居节点为树枝中间节点或叶子节点,其中,叶子节点距离树根的距离为 K,即计算范围半径为 K,采用随机 K 步漫游来计算推荐信任度. 在进行 K 步漫游信任度计算时,采用广度优先的计算方法. 查询计算过程如图 1 所示.

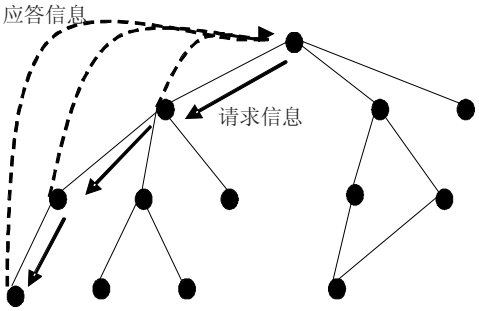

图 1 推荐信任度查询

首先节点 i 向节点其子节点发送查询请求信息,子节点根据自身存储的对节点 j 的信任度,向节点 i 返回该信任度,同时将该查询请求信息向自身的下一级子节点进行转发,该转发信息中包含了最初请求信息的节点,即根节点的接口信息,下一级子节点查询自身对节点 j 的信任度,然后直接将信任度信息传送给根节点 i,依此类推,直到搜索的深度为 k,则整个推荐信任度过程结束. 在此过程中,计算的是一种局部的信任度推荐,因为整个网络的信任度推荐信息查询开销太大,同时,有限的局部也可以在很大程度上反应节点的真实信任值.

节点 i 得到中间节点和叶子节点返回的关于节点 j 的信任度后,根据式(1)计算得到对于节点 j 的信任度. 此时采用求算术平均值的方法,平等的看待每一个邻居节点的推荐信任度.

$$TR_{ij} = (TD_{kj} + TD_{mj} + TD_{nj} + \cdots + TD_{pj})/N. \tag{1}$$

式中:TD_{xj} 为中间节点或者叶子节点 x 对节点 j 的直接信任值,其值根据定义推荐信任(TR_{ij})的算法计算得到.

随着节点 i 访问其它节点的次数增多,根据访问结果的成功与否,节点 i 逐渐建立起对其它节点的直接信任值,同时根据直接信任值,可以判断哪些节点不可信,哪些节点更可信一些. 此时,对待邻居的信任度推荐不再是平等对待了,对于直接信任度高的节点,显然要给予其推荐信任度更高的权值,对于不太可信的邻居节点,推荐信任度的权值相应要低一些. 这种情况和现实生活实际相吻合,对于信任度高的朋友推荐的人,对它的信任度肯定要比信任度低的朋友推荐的人的信任度要高许多. 因此,此时计算推荐信任度就不能继续使用式(1),而要使用式(2)来计算.

$$TD_i = TD_{ik} + TD_{im} + TD_{in} + \cdots + TD_{ip},$$
$$TR_{ij} = \frac{TD_{ik}}{TD_i}TD_{kj} + \frac{TD_{im}}{TD_i}TD_{mj} + \frac{TD_{in}}{TD_i}TD_{nj} + \cdots + \frac{TD_{ip}}{TD_i}TD_{pj}. \tag{2}$$

式中:TD_i 为在信任度推荐树中节点 i 对中间节点和叶子节点的直接信任度和. 在式(2)中,通过不同直接信任度对总直接信任度的比值来体现不同节点推荐的权重.

2.4 定义综合信任(T_{ij})

节点 i 对节点 j 的信任度最终由两个方面的信任度综合生成:1)节点 i 通过与节点 j 的交互而获得的直接信任度 TD_{ij};2)节点 i 通过 K 步漫游法访问邻居节点得到的推荐信任度 TR_{ij},二者的值分别由式(1)和式(2)得到. 本文采用线性方法来综合 TD_{ij} 和 TR_{ij},得到节点 i 对节点 j 的最终信任度.

$$T_{ij} = aTD_{ij} + (1 - a)TR_{ij}, \quad (0 \leqslant a \leqslant 1). \tag{3}$$

式中:a 为一个定义的常数,来平衡直接信任度和推荐信任度. 在最终的信任度中,直接信任度和推荐信任度各占一定比例,二者所占比例大小由 a 来决定. a 也表明了用户对自身信任度评估结果的相信程度. 如果用户更信任自身信任度评估结果,则 a 值相对设定要大一些,否则就设定为较小的值. 同时在节点 i 刚刚加入 P2P 网络时,a 值应该设计的比较小,因为此时节点 i 对其他节点的信任度完全要由邻居节点推荐信任度决定;当节点 i 加入 P2P 网络一段时间后,此时节点 i 已经对 P2P 网络有了一定的了解,此时要调大 a 值,以符合实际情况.

3 模型中的几个关键性问题

1)节点 i 对节点 j 的直接初始信任度 TS_{ij} 的

设定. TS_{ij} 应该设置一个合理的值，大小正适中. 如果 TS_{ij} 太大，则不太符合实际，因为对陌生人的信任度不可能太高；如果 TS_{ij} 太小，则导致信任度的上升会很慢. 本文取 TS_{ij} 值为 1.

2）节点直接信任度的门限值 threshold. threshold 的设定应该遵循：① threshold 不能太高，如果太高，则导致直接信任度会上升太快，同时由于是按照指数增长，若 threshold 太高，则直接信任度很快会上升到太高；②threshold 不能太低，太低的门限值会限制直接信任度的增加.

3）对欺骗节点的惩罚问题. 在本文中，对于提供虚假信息的欺骗节点，将其信任度降低 1/2. 由于对节点成功访问一次，信任度仅仅 +1，因此此算法可以有效的惩罚欺骗节点.

4）随机 K 步漫游的步长 K 值. 在查询节点的推荐信任度时，采用随机 K 步漫游的算法来实现. 在 P2P 网络中，一般根据网络的规模来设定 K 值，网络规模大的，K 值设计大些，网络规模小，则 K 值设定小些.

5）比例常数 a 的确定. a 用来平衡直接信任度和推荐信任度的比重，在二者之间要根据实际情况和用户的偏好来确定其大小.

6）服务热点问题. 在本信任度模型中，通过在信任度为 $[\max T_{ij},\ \max T_{ij}/2]$ 的节点中随机选取一个作为服务节点来实现负载的均衡. 图 2 为随机选取示意图.

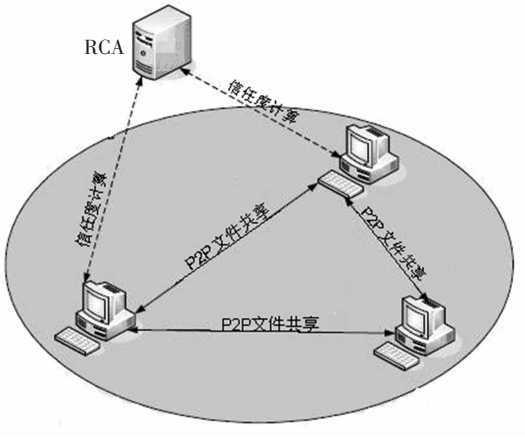

图 2　随机选取示意图

4　仿真实验和结果

仿真实验主要针对两个指标进行模拟：1）当存在欺骗节点时，欺骗节点访问率和访问成功率的变化规律. 欺骗节点指提供虚假共享信息的节点. 验证随着访问次数的增加，系统能否有效的惩罚虚假节点，迅速的提高访问成功率. 2）服务热点问题. 模拟本文算法的服务热点处理方法，将其与每次选择最大信任度的节点算法相比较，分析本算法是否有效实现负载均衡.

4.1　访问成功率

仿真实验提供文件下载，仿真网络规模为 1 000 个节点，共享 10 000 个文件，文件随机的被分配到各个真实节点上，当节点成功下载某个文件后，该节点即拥有了该文件，同时共享该文件，系统中的真实共享文件副本会逐渐增加；如果下载为虚假文件，则节点删除该下载虚假文件，评估信任度后重新搜索下载.

本实验模拟当虚假节点占总节点数 50% 时，随着访问次数增加访问欺骗率的变化趋势以及访问成功率的变化规律. 在实验中，分别通过 P-Trust 算法计算信任度来下载文件和通过普通的随机选择一个满足条件的文件来下载文件两种算法来模拟，对比二者的结果. 每个节点每次随机选择下载的文件，下载文件 1 000 次. 其中，threshold = 16，K = 3，节点比例常数 a = 0.5.

设总访问次数为 a，访问到文件的次数为 b，其中，欺骗访问为 c，成功访问为 d. 则访问欺骗率 $AC = c/b$，访问成功率 $AS = d/a$. 其中，访问欺骗率的变化规律如图 3 所示，访问成功率的变化规律如图 4 所示. 其中，平滑曲线为真实曲线经过平滑处理后得到.

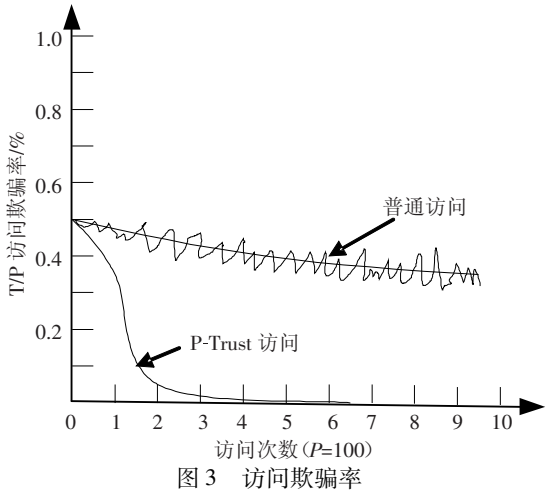

图 3　访问欺骗率

通过实验发现，对于访问欺骗率，P-Trust 算法的结果下降的很快，即很快就不会在访问欺骗节点了，因为欺骗节点的信任度下降很快，而成功节点的信任度上升很快；但是对于普通访问算法，由于同等对待所有节点的信任度，所以即使访问次数增多，虽然访问欺骗率也会下降，但仍会有较大的访问欺骗率. 对于访问成功率，P-Trust 算法的结果随着访问次数的增多，很快上升，最终为 1；但是对于普通访问算法，虽然访问成功率也会

上升,但是幅度较小.

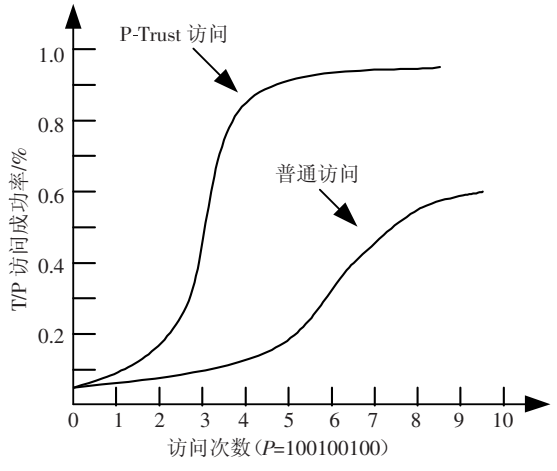

图 4 访问成功率

4.2 服务热点

分别应用 P-Trust 算法的服务热点处理方法和每次选择最大信任度节点的算法,进行模拟实验,验证 P-Trust 算法的性能. 为了简化实验,取 10 个节点,将 1 个共享文档同时发布在其中的 10 个上提供下载,每个节点下载 100 次,节点中不包含虚假节点.

实验结果如图 5 所示,基于 P-Trust 算法的节点选择可以有效的消除服务热点问题,实现负载均衡.

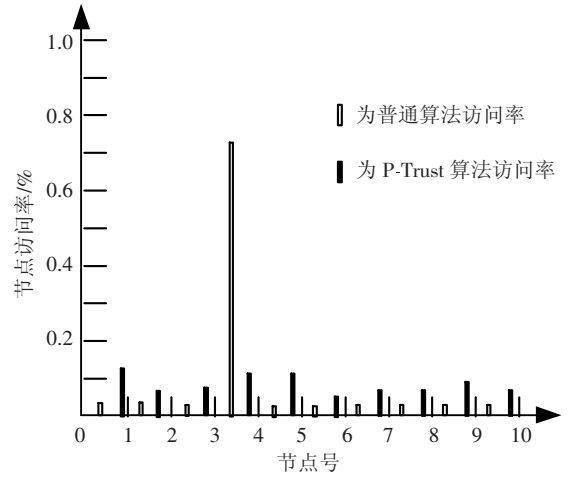

图 5 P-Trust 算法与普通算法节点访问对比图

在 P2P 网络中,使用 P-Trust 信任度算法可以在很大程度上提高访问的访问成功率,惩罚欺骗节点,均衡系统的负载;但是目前模型在资源访问上仅仅考虑了访问成功和访问失败两种情况,真实的情况是 P2P 网络共享资源中存在许多在某种程度上符合访问要求,但又不完全符合要求的资源.

5 结 论

1)本文提出的 P-Trust 信任度算法,是在对社会人际信任关系观察的基础上生成的.

2)P-Trust 算法得到的信任度实际上是一种综合信任度,包含两方面:直接信任度和推荐信任度.

3)对于访问成功率,P-Trust 算法的结果随着访问次数的增多,很快上升,最终为 1. 但是对于普通访问算法,虽然访问成功率也会上升,但是幅度较小. 基于 P-Trust 算法的节点选择可以有效的消除服务热点问题,实现负载均衡.

参考文献:

[1] ORAM A. Peer to Peer: Harnessing the Power Of Disruptive Technologies[R]. New York: O'Reilly & Associates, 2001:135 – 154.

[2] CARONNI G. Walking the Web of trust[C]//Proceedings of the 9th IEEE International Workshops on Enabling Technologis: Infrastructures for Collaborative Enterprises. Washington: IEEE Computer Society, 2000:153 – 158.

[3] DOU Wen, WANG Huaimin, JIA Yan, *et al.* A recommendation based peer-to-peer trust model [J]. Journal of Software, 2004, 15(4): 571 – 583.

[4] CORNELLI F, DAMIANI E, De CAPITANI Di VINERCATI S, *et al.* Choosing reputable servents in a P2P network[C]//Proceedings of the 11th International World Wide Web. New York: ACM, 2002: 376 – 386.

[5] ABDUL-RAHMAN A, HAILES S. A distributed trust model[C]//Proceedings of the 1997 Workshop on New Security Paradigms. New York: ACM, 1997: 48 – 60.

[6] BLAZE M, FEIGENBAUM J, IOANNIDIS J, *et al.* The role of trust management in distributed systems security [C]//Secure Internet Programming: Security Issues for Mobile and Distributed Objects. London: Springer-Verlag, 2001: 185 – 210.

[7] KAMVAR S, SCHLOSSER M, GARCIA-MOLINA H. Eigenrep: Reputation management in P2P networks [C]//Proceedings of the 12th International World Wide Web Conference. New York: ACM, 2003: 123 – 134.

[8] KHARE R, RIFKIN A. Weaving a Web of trust[J]. Journal World Wide Web, 1997,2(3):77 – 112.

[9] SELCUK A A, UZUN E, PAR IENTE M R. A reputation-based trust management system for P2P networks [C]//Proceedings of the 2004 IEEE International Symposium on Cluster Computing and the Grid. Washington: IEEE Computer Society, 2004: 251 – 258.

[10] KHAMBATTI M, DASGUPT A P, RYU K D. A role-based trust model for peer to peer communities and dynamiccoaliti ons[C]//Second IEEE International Information Assurance Workshop. Washington: IEEE Computer Society, 2004: 141 – 154.

(编辑 张 红)