文章编号:1000-582X(2007)01-0086-03

基于信任网络的网格资源发现机制*

李 静[1,2],陈蜀宇[3],文俊浩[3]
(1. 重庆大学 计算机学院,重庆 400030;2. 重庆教育学院 计算机与现代教育技术系,重庆 400067;
3. 重庆大学 软件学院,重庆 400030)

摘 要:如何有效地发现网格的计算资源和存储资源是影响网格性能的重要因素,已有的资源查找方法难以适应网格规格. 利用网格结点之间存在的信任关系构建资源信任网络,并给出了信任网络构建的原理和方法. 将主动发现和被动发现相结合,应用小世界原理,获得了优化的时间复杂度,发送了网格资源发现性能. 分析表明,该模型在网格环境中具有良好的效果,是一种可靠、安全的方法.

关键词:网格;资源发现;信任网络;安全性
中图法分类号:TP311 **文献标识码**:A

在网格和对等网络中,由于资源的广域分布和动态性,以及现有 Internet 存在的带宽和延迟限制以及网络的不可靠性,广域范围内的资源定位将在很大程度上影响网格的性能. 因此,需要一种有效的资源查找方法解决广域资源的快速定位问题. 已有的一些资源查找方法难以适应其规模. 泛洪法在最坏的情况下遍历所有结点,其时间复杂度和对网络带宽造成的影响都不能容忍;集中查找算法用一个信息结点专门存放所有资源结点的位置信息,将会形成性能瓶颈和单点崩溃的问题;路由转发算法[1]中每个结点必须维护全局其它所有结点的路由,路由表占用空间过大;分布式哈希表(DHT)算法[2-3]利用杂凑(hashing)的方式,将数据和结点运算成一个键值(key),利用键值来完成数据的放置与维护. 但由于这些算法并没有考虑网络实际拓扑结构,因而即使是邻近的 2 个结点仍有可能经过很长的搜寻路径才能取得数据,严重降低了路由的效率. 以上方法都没有考虑资源安全性问题.

笔者利用网络结点之间普遍存在的信任关系提出了一种资源发现方法,实现网格中资源安全的、可靠的、高效的发现. 第 1 部分介绍 SARTN 信任网络的建立,第 2 部分提出了一个基于信任社区的资源发现算法,第 3 部分给出了该方法的分析评价等.

1 信任网络的建立

1.1 信任关系

信任反映的是某实体对其他实体未来行为的主观期望. 信任与周围环境(context)密切相关,它是对历史经验的总结. 信任具有十分广泛的含义,在不同领域信任所指的内容及其特点是不完全相同的. 在计算机网络的结点之间存在广泛的信任关系:如通过访问搜索引擎寻找所需的信息线索,隐含着信任其所提供的线索;从一个 FTP 服务器下载程序,隐含着信任该服务器上不会包含病毒、木马等有害资源(尽管有时与实际不符). 在网格中,一些结点发布对另一些资源结点的路由信息,隐含了前者对后者真实性的信任;资源需求结点根据其它结点所提供的路由信息发现资源,也隐含了对这些中间结点的信任. 文章称相关结点之间的信任关系构成的网络为信任社区. 人们在分布式网络、普适计算、对等计算、自组织网络等多个领域中提出了众多信任模型[4-7],采用信任网络安全传递信息是一种行之有效的方法. 在网格环境中,为了获得安全和可靠的资源,笔者建立了一个资源安全和可靠性信任网络 SARTN(secure and available resource trust network).

对 SARTC 信任网络中的信任关系,根据参考文献[4-8]等,笔者作出如下定义:

定义 1 设 A、B 为 *SARTN* 信任网络中任 2 个结点,B 结点对 A 结点的信任程度为 0.9,记作(B,A,0.9),这是指:如果信任网络的信任阈值低于 0.9,B 结点认为 A 结点是可信任的,即从 A 结点传给 B 结点的资源发布内容,B 结点可以接受并转发;同时 A 结点同意与 B 结点建立信任关系. 称 B 结点是 A 结点的

* 收稿日期:2006-08-20
作者简介:李静(1974-),女,重庆大学博士研究生,主要从事网格和网络安全等方面的研究. 陈蜀宇,男,教授,博士生导师,电话(Tel.):023-61656128;E-mail:sychen@cqu.edu.cn.

信任邻居，A 结点是 B 结点的可信结点. 信任程度最大值为 1.

定义 2　信任关系是非对称的，即$(A,B,1)$不等于$(B,A,1)$；

定义 3　信任邻居是逻辑上的而不是物理上的.

定义 4　信任网络拓扑是网状的.

定义 5　信任社区中源结点 A 通过信任关系到达目标结点 B，称为 A 到 B 之间的信任链. 在任意一对结点之间可能存在多条信任链.

定义 6　信任关系是可传递的. 可以参考网络安全领域的一些信任传递模型[5]. 为方便计算，笔者使用了一个简化的信任传递模型. 如有$(A,B,0.8)$，$(B,C,0.5)$，则有$(A,C,0.4)$，即 A、C 之间的信任程度是 A，B 和 B，C 信任程度的乘积. 如果 A，C 之间有多条信任链，取跳数短的信任链，如果跳数最短的信任链有多条，取各条信任链所得信任程度的平均值为 A，C 之间信任程度，公式如下：

$$T_{AC}=\frac{\sum_{i=1}^{m}T_{ACi}}{m}. \tag{1}$$

其中 m 为跳数最短的信任链条数，T_{ACi} 为各条信任链所得信任程度. 为避免信任社区内传递信任的失真，给予信任链最短跳数一个阈值，信任链最短跳数超过此阈值者，不计算传递信任程度.

1.2　建立信任网络

为建立 SARTN，作如下假设：

假设 1　建立信任关系的代价较高，打破信任关系的代价较低. 这表明 2 个结点之间建立信任需要较长时间的诚实交往，打破信任可能只需少数几次非诚实的行为，这符合人们的认知习惯.

假设 2　信任网络的网络拓扑具有 Power Law 规律. 研究表明，许多现实网络，如 Internet 骨干、WWW 页面链接、人们的社会关系网络等，其结点“度”的分布都具有同样的规律，即“度”为 K 的结点的分布概率满足以下公式：$P(k)\propto k^{t}$，其中，$1<t<\infty$，随网络的不同而不同. Power Law 分布的含义可以简单解释为在网络中少数结点有较高的“度”，多数结点的“度”较低.“度”较高的结点与其他结点的联系比较多，通过它找到待查信息的概率较高. 在信任网络中，称信任别人为信任“度”，被别人信任为可信“度”. 少数结点被多数结点所信任，具有较高的可信“度”. 这与人们的社会关系网络具有相似性，假设是合理的.

通常将 SARTN 信任网络建立方法描述如下：

1）结点的信任表. 每个结点维护 3 张表，1 张为信任邻居表，每个表项记录了 1 个信任邻居结点的信息（IP 地址、当前状态等）；1 张为可信结点表，每个表项记录了 1 个可信结点的信息（IP 地址、结点信任程度、当前状态等）；1 张为可信资源发布表，每个表项记录了 1 个可信资源的信息（IP 地址、资源信任程度、当前状态等）. 3 张表统称为信任表. 由于 1 个结点可能有不止 1 个资源，有的资源可靠性高一些，有的资源低一些，故把结点和资源信任程度分开考虑，但无疑资源信任程度会影响结点信任程度.

2）初始化. 一个新加入网格的结点，当它希望加入信任网络时，它首先要与网络中的一个已知成员结点联系，并获取该结点地址信息，该结点将充当新加入结点的引导结点（bootstra pnode）. 在 SARTC 中，新结点 N 通过向周围的结点广播发送网络查询消息的方法发现物理距离较近且信任邻居较多的网格成员结点. 其他成员结点在接收到该消息后，将返回一个应答消息，应答消息中还应包含该成员结点的身份信息（IP 地址、信任邻居数、当前状态等）. 为了降低网络开销，该广播消息的初始化 TTL 值将基于网络规模设置为一个较小值，仅当无任何结点返回应答时，再将该 TTL 值逐倍增大. 新结点的可信结点表一开始仅仅包括它的引导结点，另外 2 张表为空. 引导结点将新结点加入到其信任邻居表中.

3）获得引导结点的信任. 虽然新结点无条件信任引导结点，但并未获得引导结点的信任. 作为自己的信任邻居，引导结点会给予新结点发布少量资源的机会，赋予新结点一个初始结点信任程度和初始资源信任程度. 如果该资源可靠性较高，会以步长 Rstep1 增加其资源信任程度，同时以步长 Nstep1 增加新结点的结点信任程度，Rstep1 大于 Nstep1；如果该资源可靠性不高，会以步长 Rstep2 减少其资源信任程度，同时以步长 Nstep2 减少新结点的结点信任程度，Rstep2 大于 Nstep2. 注意，根据假设 1，Rstep2 大于 Rstep1，Nstep2 大于 Nstep1.

4）信任获得方式. 信任关系按其获得方式，分为直接信任和推荐信任. 直接信任是指通过实体之间的直接交互信息得到的信任关系；推荐信任是指通过中间实体获得的对目标实体的信任关系. 新结点与引导结点之间是直接信任关系，新结点可进一步通过引导结点利用公式（1）扩展自己的信任邻居表和可信结点表.

5）结点向自己的信任邻居和可信结点发放数字证书，证书中包含结点自身的公钥.

2　资源发现算法

资源发现可分为被动发现和主动发现 2 种方式. 主动发现方式需要用户主动地从发布渠道去寻找发布资源（Pull），如基于 Web 的信息发布；在被动发现方式下，资源所有者主动地将发布资源推介到用户（Push）. 系统中研究者使用了被动发现和主动发现相

结合的方式,具体步骤如下:

1)资源结点先向自己的信任邻居发布资源,再通过它们转发信息,这些结点又称为资源路由者.

2)资源路由者 S 将资源发布信息通过自己的信任邻居向外传递.向外传递时以 $1/d$ 的概率选取目标结点 T,其中 $d=||S-T||$ 是 S 和 T_f 两结点间的跳数.

3)资源需求者的可信邻居中各结点按可信"度"的高低排序.从可信"度"最高的结点 A 开始搜索资源,如果未找到,依次搜索可信"度"较高的结点上所发布的资源.

4)要是在直接可信邻居中均未找到所需资源,从 A 的可信邻居中继续寻找资源发布信息.也就是说,以资源需求者为根,其可信邻居为枝叶形成 1 棵树,那么在这棵树上按照宽度优先的规则来搜索资源发布信息.

5)如果有多个资源符合查询条件,用户会选择具有最高信任程度的资源.

6)找到所需资源后,资源需求者 Q 向资源结点 R 发出请求,后者向前者发送数字证书,证书中包含结点自身的公钥.Q 将应用对象用 1 次 1 密产生的会话密钥加密,又将会话密钥用 R 的公钥加密,同时附上 Q 数字证书,发送到 R. R 用私钥解密会话密钥,又用会话密钥解密应用对象,使应用对象安全到达资源结点.当从资源提取返回结果时,R 同样产生 1 次 1 密的会话密钥,将返回结果用会话密钥加密,又将会话密钥用 Q 的公钥加密,可以使返回结果安全到达资源需求者.

3 分析评价

定理 在 SARTN 信任网络中资源查找的平均跳数为 $O(\log^2\sqrt{n})$,其中 n 为网络结点数.

证明 SARTN 信任网络中资源的发布符合 Kleinberg 小世界模型[9]. Kleinberg 提出如果将 $n\times n$ 个结点放入一个二维网格中并且每个结点都有一些短链和仅一条长链,采用贪婪路由能够以平均 $O(\log^2 n)$ 跳在任何一对结点间传送消息.这个模型提出结点 S 应以 d^{-r} 的概率选取长链彼端 T,其中 $d=||S-T||$ 是 S 和 T 两结点间的曼哈顿距离,r 是底层拓扑的维度.SARTN 信任网络中资源的发布按跳数的多少来选择长短链,底层拓扑的维度为 1.故资源发布信息向外传递时以 $1/d$ 的概率选取目标结点 T,符合 Kleinberg 小世界模型.

参照文献[9]中定理 2 的一个相似的证明过程,可以得到路由的平均路径跳数是 $O(\log^2\sqrt{n})$.

证毕.

按小世界原理建立起来的资源发布信任社区,使距离资源需求者较近的资源具有更大的几率被选择,保持了资源的局部性(locality),减轻了网络负担.同时由于长链的存在,使任意 2 个结点可以在较少的跳数内相连接,减小了网络的直径.

4 结 论

资源发现是网格研究中的一个重要课题.笔者采用分布式方法构建了一个动态信任社区,并提出基于信任社区的资源发现方法,将资源主动发现和被动发现相结合,具有安全性、可靠性和高效性,并能保持资源的局部性,是在网格环境中资源发现的一个可行的方法.

参考文献:

[1] 李伟,徐志伟,卜冠英,等. 网格环境下一种有效的资源查找方法[J]. 计算机学报, 2003, 26(11): 1546-1549.

[2] RATNASAMY S, FRANCIS P, HANDLEY M. et al. A scalable content addressable network [C]//ACM special interest grou pon data communication (SIGCOMM) 2001. New York: ACM Press, 2001:161-172.

[3] STOICA I, MORRIS R, KARGER D. et al. Chord: a scalable peer-to-peer looku pservice for internet applications [C]// ACM Sigcomm. New York: ACM Press, 2001: 2-10.

[4] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks [A]. ESORICS 94 [C]. Brighton: Springer-Verlag, 1994: 239-247.

[5] YU B, MUNINDAR SINGH P. An evidential model of distributed reputation management [C]// Proceedings of First International Joint Conference on Autonomous Entities and Multi-Entity Systems. New York:[s. n.], 2002.

[6] ABERER K, DESPOTOVIC Z. Managing trust in a peer to peer information system [C]//Proceedings of the 10th International Conference on Information and Knowledge Management. New York:[s. n.],2001.

[7] ABDUL RAHMAN A, HAILES S. A distributed trust model [C]//New security paradigms workshop. New York: ACM Press, 1997: 2-10.

[8] 包秀国,胡铭曾,方滨兴. 一种基于对等网的资源主动发布方法[J]. 小型微型计算机系统, 2004, 25(4):526-530.

[9] KLEINBERG J. The small world phenomenon: an algorithmic perspective[C]// 32nd ACM Symposium on Theory of Computing, New York:[s. n.], 2000.

(下转第 101 页)

Effective Expressions for Momenta Normalization and Renormalization to $e-\bar{e}$ Loop propagator

CHEN Zhou-niu[1,2], FANG Zhen-yun[1], JIANG Zai-fu[1],
CHEN Wen-suo[1], GAO Fei[1,2] PENG Chuan-qian[1]

(1. College of Mathematics and Physics, Chongqing University, Chongging 400030, China;
2. Department of local student management, Communication College, Chongqing 400035, China)

Abstract: In the electromagnetic minimum coupling model, the authors study the expansion of the finite quantity function in the momenta renormalization $e-\bar{e}$ loop propagator function, and find that if they use the matrix function expansion they can approach the separation of the finite quantity function, but also can get a strictly analytic solution for one dimension integral calculation method of it. This will give an effective new way to study the question about the exact solving to the renormalization finite quantity function.

Key words: $e-\bar{e}$ propagator; momenta renormalization; momenta normalization; matrix function expansion method.

(编辑　姚　飞)

(上接第88页)

Mechanism of Resource Discovery Based on Trust Network

LI Jing[1,2], CHEN Shu-yu[3], WEN Jun-hao[3]

(1. College of Computer Science, Chongqing University, Chongqing 400030, China;
2. Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067, China;
3. College of Software Engineering, Chongqing University, Chongqing 400030, China)

Abstract: How to effectively locate resources is a very important factor affecting the performance of Grid environment. The authors propose a novel method which utilizes trust relations existed implicitly among network nodes to construct a secure and available resource trust network(SARTN), meanwhile provide the theory and method of SARTN. Combining passively discovery with actively discovery, applying Small World theory, optimized time complexity is achieved, and the performance of Grid resource discovery is promoted. Through analysis, the proposed solution is scalable, secure and efficient in Grid.

Key words: grid; resource discovery; trust network; security

(编辑　侯　湘)