网格资源访问的一种主观信任机制

陈建刚[1], 王汝传[1,2], 王海艳[1]
(1.南京邮电大学计算机学院,江苏南京 210003; 2.南京大学计算机软件新技术国家重点实验室,江苏南京 210093)

摘 要: 针对网格环境资源访问过程中的信任问题,为避免主观随意性,提出了基于贝叶斯函数的信任机制,通过判断并使用推荐能力最强的中间节点作为推荐者,搜索出对资源节点的信任链路,使用贝叶斯函数对由信任链路得到的资源节点的每种属性进行综合判断,最终确定是否访问该资源节点,模拟实验结果表明该信任模型的有效性.

关键词: 网格服务; 贝叶斯函数; 信任机制; 声望
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2006) 05-0817-05

A Subjective TrustMechanism of Resource Access in Grid

CHEN Jian-gang[1], WANG Ru-chuan[1,2], WANG Hai-yan[1]
(1. *Institute of Computer Science, Nanjing University of Post and Telecommunications, Nanjing, Jiangsu 210003, China;*
2. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu 210093, China*)

Abstract To solve the trust problem during resource access in grid service and to avoid subjective notion during the execution of subjective trust, the trust mechanism based Beta function is proposed. The trust relations are set up upon recommendations among nodes from the reference of social network relation. Through judging the recommendation ability of medium nodes according to the former interaction result with the method of probability and statistics, the best recommendation ability nodes are selected as the recommenders to search trust links according to the limitation of the requester about link recommendation value and recommendation number; the trust values of each attribute for the resource node presented by the last nodes on the trust links are synthesized with Beta function to decide whether the access to resource node can be enforced. The experimental result expresses its validity.

Key words grid service; beta function; trust mechanism; reputation

1 引言

网格计算已经发展成为计算机工业的一个重要领域,与分布式计算的不同之处在于,网格计算更加集中于资源共享和协同工作以及高性能的定位.跨越多个地域,在不同领域内为网格虚拟组织分配用户、资源并协调其服务是网格计算中基础性技术挑战.由于网格环境的大规模性、异构性、分布性,动态性和开放性等特点,传统的安全技术或者措施已经不能满足网格应用的需要.如网格系统中存在着多个管理域,安全机制对于不同管理域应能采用不同的策略,不能强制实施统一的策略和信任关系,而传统的安全机制不能适应这种多管理域的需要;在以前研究中,往往假定实体之间是相互合作的或事先约定好一些规则进行相互竞争,而这些假定和约定在网格环境中是不成立的.因而人们迫切需要对网格计算的安全策略进行专门系统的研究,并针对新的网格计算需要提出新的方法和思路.主观信任机制是目前研究解决开放网络环境下安全问题的热点,主观信任区别传统的认证机制,传统的认证主要用于证明身份,说明拥有该证书或令牌的实体是合法实体,而这并不等同于说明该实体就是可信的(有能力进行交互并且交互过程中不会出现欺诈行为).当前已经有一些对 P2P和 Adhoc等开放网络环境下的信任机制的研究,主要有以下几类信任模型:基于 Dempster-Shafer(D-S)证据理论[1~3]来刻画主观信任度,通过制定相应的规则对信任度进行分类评判(分为信任,不信任和不确定三类),这种评判过程带有人为的主观性;基于模糊集合的信任关

收稿日期: 2005-06-02; 修回日期: 2005-11-10
基金项目: 国家自然科学基金 (No. 60573141, No. 70271050); 江苏省自然科学基金 (No. BK2005146); 江苏省自然科学基金预研项目 (No. BK2004218); 江苏省高技术研究计划 (No. BG2004004, No. BG2005037, No. BG2005038); 江苏省计算机信息处理技术重点实验室基金 (No. kjs050001); 江苏省高校自然科学研究计划 (No. 05KJB520092)

系[4],需要建立信任集合的隶属函数,在交互结束判断信任值涉及到信任等级的划分问题,而这也带有很大主观随意性.目前网格环境中的信任模型也有如上两类:使用 D-S 证据理论的信任模型[5]和基于模糊逻辑的信任模型[6].而基于行为的网格信任模型[7]最早由 F A zzedin提出,该基于行为的网格信任模型以信任和声望作为度量,并引入了信任衰减函数来反映信任随时间而变的特性,但该模型没有解决推荐者恶意推荐的度量问题.为此, F A zzedin又提出了一个信任中介系统来扩展信任的范围[8],并且引入了准确度和诚实度作为度量从而解决了推荐者恶意推荐的度量问题.该方法的缺点在于对信任分级带有主观随意性,并且有较多的参数,而这些参数的取值也是主观确定的,另外整个信任计算过程也比较复杂.

纯粹从主观因素判断交互过程的信任程度的好坏带有随意性,对于同一个问题,不同实体从主观出发得出的结果也不一样,因而很难制定统一的标准,在实际中较难操作.相反,根据交互的成功与否从概率统计的角度来建立信任模型则更容易实现,交互成功与否是根据实体对这次交互的结果是否满意来进行评判,由于这种方法涉及到主观考虑的只是判断交互成功和交互失败,因而实体的主观判断因素较少.我们的网格资源访问的主观信任模型就是使用这种方法,该模型是在交互双方从未交互的前提下推导出的双方信任关系.由于网格环境中的跨域访问带有普遍性,因而这种场景也较常见.另外,我们认为信任问题不仅仅是一个安全问题[9],也是一个服务质量的问题.在网格资源访问过程中,用户可能关心自己提交的作业是否能够在资源提供节点处正常运行而作业信息没有泄露,也可能关心对方运行过程是否可靠,运行效率如何等别的属性.因而用户从自己利益出发,需要对资源进行多方面的考察,即对资源的各种属性提出要求,在对这些属性进行预先评判之后,用户可以决定是否访问该资源提供节点.在访问结束后用户根据访问过程中的日志记录对每一种属性都建立相应的信任关系,从而建立和更新信任值.由于用户和资源提供节点在此前从未发生过交互,这些资源属性就需要通过那些和资源提供节点发生过交互的中间节点的推荐活动来获得,从这些节点所评判的对资源提供节点的各种属性的信任情况,通过某种方式进行综合评估,从而决定是否交互.从以上考虑,我们认为主观信任机制的建立需要解决如下问题:

(1)信任关系的评估问题,即使用什么方法来对信任关系进行建模;

(2)推荐信任的建立问题,即如何通过中间节点的推荐来建立信任链路;

(3)信任链路的综合问题,即对所得到的信任链路怎样进行合成.

下面就针对这些问题来讨论我们的信任模型.

2 声望和直接信任关系的建立

2.1 推荐节点声望值的建立

根据社会网络关系,我们知道在交互双方没有接触过的前提下,实体都倾向于使用一些自己比较信任的中间实体作为推荐者来评判交互对方,而这些推荐者的推荐能力则可以通过他们的声望来表示,声望(Reputation)定义为一个实体对另一个实体能够行使推荐活动的能力、诚实性和可靠性的一种主观评判.通常声望越大,则越容易取得信任.在一定时期内,实体的声望通常体现为相对稳定的,因而能够用数学公式表示.根据社会经验,人们通常是通过多次交互过程来建立对对方的声望评估,而通常交互的结果有两种:交互成功和交互失败.在一定时间段内,两个实体间的交互成功概率表现为一个相对稳定值.当交互成功的次数越多,则认为对方的声望越大,反过来也一样,对方的声望值越大,则交互成功的次数越多,因而可以用交互成功的概率来表示对实体的声望值.

令 $Trans_{ab}=\{trans_{ab}(1),\ trans_{ab}(2),\ trans_{ab}(3),\ \cdots,\ trans_{ab}(n)\}$表示实体 A 和 B 间的交互数集合,其中 $trans_{ab}(m)$表示双方第 m 次交互的结果.根据交互成功与否,该结果表示为

$$\forall m,\ trans_{ab}(m)=\begin{cases}1, & m^{th}=\text{success}\\ 0, & m^{th}=\text{failure}\end{cases} \qquad (1)$$

这种交互分为两类:一类是专门的推荐活动,双方的交互过程就是建立这种推荐关系.实体根据和对方推荐结果得到的目的节点的交互成功与否进行评判,若交互成功则认为对方的这次推荐活动成功,相应地增加对其推荐能力的信任程度,该推荐实体的声望也就高.这类推荐活动对应于社会网络中的中介活动,如房屋租赁中介活动等.另外一类是双方从事某种特定交互(除了专门的推荐活动外)而得出的信任关系,根据交互的成功与否来确定对对方的信任值,这种信任虽不是为了推荐而建立的信任关系,但是可以将这种信任关系用于推荐活动,这从社会关系中的人际关系很好理解,比如通过交往你对对方比较熟悉,知道对方是值得信任的,因而就可以通过对方来获得一些信息,并且这种信息的可靠性也大.

对于专门的推荐活动,假定在一定时期内,实体的推荐行为是稳定的,因而该实体的声望也是一个固定的概率分布,设实体 A 通过实体 B 进行了 n 次推荐活动,其中实体 A 认为推荐成功的次数为 r,在考察实体 B 进行推荐活动的成功概率时,设其成功推荐的概率为 p,则在 n 次推荐活动中,出现推荐成功的次数为 r 的概率 p 服从二项式分布:

$$P(R=r)=C_n^r p^r(1-p)^{n-r},\quad 0<p<1 \qquad (2)$$

而在这 n 次推荐活动中,假设 $\{trans_{ab}(1),\ trans_{ab}(2),\ trans_{ab}(3),\ \cdots,\ trans_{ab}(n)\}$ 是容量为 n 的相互独立的简单子样,则根据式(1)和(2)得到似然函数为:

$$L(P) = \hat{p}^{\sum_{m\in success} trans_{ab}(m)}\left(1-\hat{p}\right)^{\sum_{m\in success} trans_{ab}(m)} = \hat{p}^{r}\left(1-\hat{p}\right)^{n-r} \tag{3}$$

由最大似然估计可以求出估计子 $\hat{p}$ 为:

$$\hat{p} = \frac{r}{n} \tag{4}$$

在什么条件下可以使用 $\hat{p}$ 作为对推荐实体的声望值, 为此我们引入贝努利定理[10]:

设 n_A 是 n 次独立重复试验中事件 A 发生的次数, p 是事件 A 在每次试验发生的概率, 则对于任意正数 $\varepsilon > 0$ 有

$$\lim_{n\to\infty} P\left\{\left|\frac{n_A}{n} - p\right| < \varepsilon\right\} = 1 \tag{5}$$

证明从略. 该定理表明事件发生的频率 $\hat{p} = n_A/n$ 依概率收敛于事件的概率 p, 就是说当 n 很大时, 事件发生的频率与概率有较大偏差的可能性很小, 由实际推断原理, 在实际应用中, 当交互次数很大时, 便可以用成功交互发生的频率 $\hat{p}$ 来代替成功交互的概率 p, 也就可以用来表示对推荐实体的声望值. 而对于有直接交互活动的节点作为推荐节点, 同样可以将他们交互的成功概率 p 作为对对方的信任值, 因而也可以使用 $\hat{p} = r/n$ 评价对对方的声望值. 在网格环境中, 每一个节点都维护着一张推荐信任表, 用来记录该节点的推荐节点和交互过的信任节点, 如表 1 所示. 在进行推荐活动中, 请求者就寻找交互次数 n 越大, $\hat{p}$ 值越大的节点作为推荐者, 这样得到的推荐结果也越可靠.

表 1　推荐信任表

交互实体	A	B	C	D	…
交互次数 (n)					
成功次数 (r)					
声望值 (p)					

2.2　资源访问过程中信任关系的建立

如前所述, 主观信任问题不仅仅是安全问题, 同时也体现为服务质量问题, 推而广之就是可信赖计算问题, 比如系统运行的稳定性和可靠性是其正常工作的先决条件. 因而请求者在访问资源提供节点时, 不仅要求资源提供节点能够保障作业的安全, 还要求其能够提供可靠的服务质量. 建立资源提供节点的属性集:

$ATTR = \{$稳定性, 诚实性, 资源运行的可靠性, 资源的易用性, 容错性, 运行效率, 成功率, …$\}$, 用 $ATTR = \{attr_0, attr_1, attr_2, \cdots, attr_n\}$ 表示, 其中 $attr_i$ 表示请求者对资源提供节点进行评判的第 i 种属性. 令

$$\forall\, i \in n,\ F(attr_i) = \begin{cases} 1, & attr_i = satisfaction \\ 0, & attr_i = non\_satisfaction \end{cases} \tag{6}$$

表示当访问过程中对第 i 种属性满意时, 相应对该属性赋值为 1, 不满意时赋值为 0.

在进行访问过程中, 实体通过访问结果, 对资源的每一种属性都进行相应的评价, 这种评价对于每种属性都是不同的, 比如运行的可靠性, 只要资源节点出现了一次系统崩溃, 则认为该系统可靠性不值得信任. 而对于这种访问的信任评判, 有两种考虑方式: 一种是和前面计算推荐者的声望相同, 采用成功访问的频度来表示; 另一种则是只强调本次访问的结果, 而不考虑以前的访问结果. 前一种方式虽然相对精确, 但是正如我们前面从贝努利定理中所分析的那样, 只有在访问次数 n 越大的前提下, 成功访问发生的频率 $\hat{p}$ 才越接近于访问成功的概率 p, 而这在和资源访问的节点中是很难达到的, 因为根据经验, 大多数节点访问资源的次数还是很少, 因而这种评价的可靠性也不高. 后一种方式虽然比较粗糙, 但是从请求者的角度出发, 更关心的是最近一段时间内和资源节点访问的结果, 倘若和资源节点最近一次访问的节点给出的信任评价都比较高, 满足请求者所期望的值, 则请求者也能够相信资源节点的能力. 因而我们采用后一种的评判方式. 访问结束后, 请求者对资源提供节点进行每种属性的评判, 给出或者更新评判结果, 如表 2 所示, 表中还给出了资源提供节点的标识 (ID), 用于说明访问的是哪个资源提供节点.

表 2　资源提供节点的信任表

	属性信任度					资源提供节点的标识 (ID)
	$attr_0$	$attr_1$	$attr_2$	…	$attr_n$	
信任值					…	

3　信任链路的建立

在建立信任链路时我们强调以下几点: (1)根据社会网络经验, 当信任链路越长, 则得到的最终推荐信任越不可靠, 假设中间推荐节点的声望值都为 0.9, 则经过 8次推荐之后, 得到的链路推荐值为 $0.9^8 = 0.43$, 这样的推荐值就难以使请求者相信最终结果, 因而需要对链路长度进行限制. 假设请求者要求的链路推荐值为不小于 p_0, 根据推荐链路的等效推荐系数关系式 $p = \prod_{i=1}^{r} p_i$, 其中 p_i 为链路上第 i 个推荐节点的声望值, 当中间节点 r 计算得到 $\prod_{i=1}^{r} p_i < p_0$ 时, 该推荐链路停止搜索. (2)中间推荐节点应该能够使用多少个其推荐信任表中的推荐节点, 中间节点使用的推荐节点越多, 则风险也就越大. 因为倘若该节点存在欺诈行为, 则后面的推荐节点都不可信, 因而中间节点的推荐节点应该限制在一个较小的 m 值, 而请求者则可以使用较多的推荐节点 (假设使用 m_{req} 个)进行搜索. 信任链路的具体搜索步骤如下:

(1)请求者 req 查询推荐信任表, 找出声望值 p 和交互次数 n 都最大的前 m_{req} 个实体 $\{d_i^0, d_j^0, d_k^0, \cdots\}$, 并对每个推荐节点 d_i^0 都发送消息: $\{\langle req, des\rangle, \{p_i^0, p_0\}, \{d_i^0, d_j^0, d_k^0, \cdots\}\}$

//其中 des 表示请求访问的资源节点, p_i^0 表示对推荐节点 d_i^0 的声望值

(2)对于每个 d_i^0

查找资源提供节点的信任表, 是否有请求访问的资源节点 des, 若有则返回请求者 req 消息:

$\{F(attr_i),\ i = 0, \cdots, n\}$

/返回对请求访问的资源节点的各种属性的信任值.

(3)存储消息 $\{\langle req, des\rangle, p_0\}$

/若后面还有相似搜索路径经过该实体, 则中止该路径搜索.

该实体完成搜索.

(4)若无, 则查找其推荐信任表中交互实体集合去掉 $\{d_i^0, d_j^0, d_k^0, \cdots\}$集合中的实体, 同样找出声望值 p 和交互次数 n 都最大的前 m 个实体 $\{d_i^1, d_j^1, d_k^1, \cdots\}$, 并对每个实体都发送消息: $\{\langle req, des\rangle, \{p_i^0 * p_i^1, p_0\}, \{d_i^0, d_j^0, d_k^0, \cdots, d_i^1, d_j^1, d_k^1, \cdots\}\}$

对于实体 d_i^1, 先检查 $p_i^0 * p_i^1$ 是否小于 p_0, 若小于, 则停止搜索.

若大于, 重复上面步骤(2)~(4), 只是消息内容要做些改动.

最终搜索得到的信任链路如图 1所示.

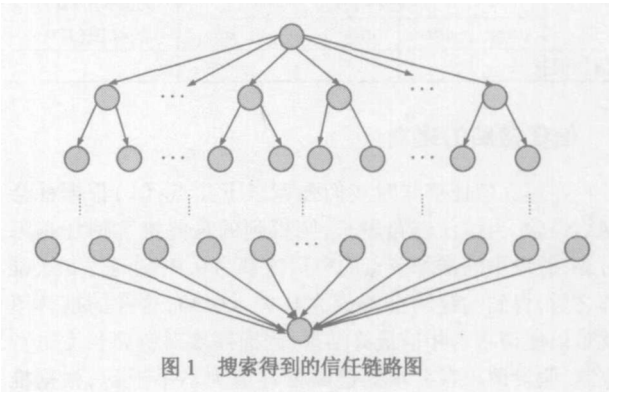

图 1 搜索得到的信任链路图

4 对推荐信任链路的合成计算

假定在一定时间内, 资源提供节点提供某类服务的能力是相对稳定的. 而不同最终推荐节点(信任链路上访问过资源提供节点的推荐节点)访问资源的过程都是相互独立的, 并且不同实体访问资源判断各种属性信任与否的标准相同. 因而当信任链路中的最终推荐节点得到的对资源提供节点的属性 $attr_i$ 信任数为 m_i, 而不信任数为 n_i 个, 等价于其中一个最终推荐节点独立访问资源提供节点 $m_i + n_i$ 次, 其中信任次数为 m_i, 而不信任次数为 n_i. 使用贝叶斯函数, 这种对属性 $attr_i$ 访问成功的概率 p_i 的密度函数为:

$$f(p_i) = \frac{p_i^{a-1}(1-p_i)^{b-1}}{B(a, b)} \tag{7}$$

其中 $B(a, b)$ 为 Beta 函数, 即有 $B(a, b) = \int_0^1 p_i^{a-1}(1-p_i)^{b-1}dp_i$

而 a, b 参数是先验假设得到的, 满足 $a>0$, $b>0$. 当选择适当的 a, b 值时, $B(a, b)$ 表示访问前实体根据别的情况(比如可能从第三方得到的关于对方的评价等)作出的关于资源提供节点的一种主观信任度. 据此密度函数, 当信任链路得到访问次数为 n, 并且其中对属性 $attr_i$ 的成功访问次数为 r_i 时, 则由式(7), 属性 $attr_i$ 的成功概率 p_i 的验后分布为 $Beta(a+r_i, b+n-r_i)$, 即有:

$$f(p_i \mid r_i, n, a, b) = \frac{p_i^{a+r_i-1}(1-p_i)^{b+n-r_i-1}}{B(a+r_i, b+n-r_i)} \tag{8}$$

设用户所要求的资源提供节点的属性 $attr_i$ 成功率为 p_{i0}, 置信度为 C_{i0}, 即应该有 Beta分布的累积分布函数

$$P(p_i \geqslant p_{i0}) = \int_{p_{i0}}^1 f(p_i \mid n, r_i, a, b)dp_i = \int_{p_{i0}}^1 \frac{p_i^{a+r_i}(1-p_i)^{b+n-r_i}}{B(a+r_i, b+n-r_i)}dp_i \geqslant C_{i0} \tag{9}$$

另外还可以从对资源提供节点的属性 $attr_i$ 的访问失败概率 q_i 来考虑, 设用户所要求的资源提供节点属性 $attr_i$ 失败率为 q_{i0}, 置信度为 D_{i0}, 因而有

$$P(q_i \leqslant q_{i0}) = \int_0^{q_{i0}} f(q_i \mid n, r_i, a, b)dq_i = \int_0^{q_{i0}} \frac{q_i^{a+r_i}(1-q_i)^{b+n-r_i}}{B(a+r_i, b+n-r_i)}dq_i \geqslant D_{i0} \tag{10}$$

其中 r_i 在此表示访问失败的次数.

由于请求者要求的不同属性 $attr_i$ 的重要性不同, 比如请求者可能更关心运行的稳定性而对资源提供节点运行的效率要求不高, 因而对不同属性所期望的成功率、失败率和置信度也不一样. 请求者对资源提供节点的各种属性都进行相应的运算, 并判断是否对其取得信任, 若对各种属性都取得相应的信任, 便可以决定访问该资源提供节点.

5 模拟仿真

在模拟实验过程中, 为了简化, 我们只考虑双方在完全未知的情况下(即无先验情况)进行访问的情况, 并只考虑资源提供节点属性 $attr_i$ 的失败概率 q_i, 可令 $a=1$, $b=1$, 对于"无先验"情况, 则根据式(10)有资源提供节点属性 $attr_i$ 的失败概率 q_i 的验后分布为

$$f(q_i \mid r_i, n, 1, 1) = \frac{q_i^{r_i}(1-q_i)^{n-r_i}}{B(1+r_i, 1+n-r_i)} \tag{11}$$

设资源提供节点属性 $attr_i$ 的固有失败率为 0~0.3, 在不同固有失败率下, 搜索得到的最终推荐节点数为 100~300中的随机数, 而其中访问失败的次数 r_i 满足正态分布 $N(\mu_i, \sigma_i)$, 其中 μ_i 为固有失败率, 而 σ_i 表示其误差程度, 假定 $\sigma_i = 0.1\mu_i$, 设请求者期望的资源提供节点属性 $attr_i$ 的失败率为 0.2 而置信度为 0.8 根据 $P(q_i \leqslant q_{i0}) = \int_0^{q_{i0}} f(q_i \mid n, r_i, 1, 1)dq_i = \int_0^{q_{i0}} \frac{q_i^{r_i}(1-q_i)^{n-r_i}}{B(1+r_i, 1+n-r_i)}dq_i \geqslant D_{i0}$ 有

$$P(q_i \leqslant 0.2) = \int_0^{0.2} f(q_i \mid n, r_i, 1, 1)dq_i = \int_0^{0.2} \frac{q_i^{r_i}(1-q_i)^{n-r_i}}{B(1+r_i, 1+n-r_i)}dq_i \geqslant 0.8 \tag{12}$$

在不同固有失败率的情况下, 我们分别进行了 100次实验, 其中对该属性取得信任的次数作为纵坐标, 而横坐标选为该资源提供节点属性 $attr_i$ 的固有失败率(0~0.3), 最终得到的实验结果如图 2所示. 从图中可以看出, 在该请求者

的置信度(0.8)下, 在固有失败率为 0~ 0.15范围内(小于 0.2), 100次实验对该属性都取得信任, 而在固有失败率为 0.15~ 0.25之间则有很陡的下降, 表明这时取得的信任次数明显减少, 而在 0.25之后则取得信任的次数都为 0, 说明该模型能很好的根据推荐链路提供的经验信息并依照请求者的需要, 从而计算出一个合理的信任值, 用于对被评估资源提供节点的属性的固有失败率进行判断.

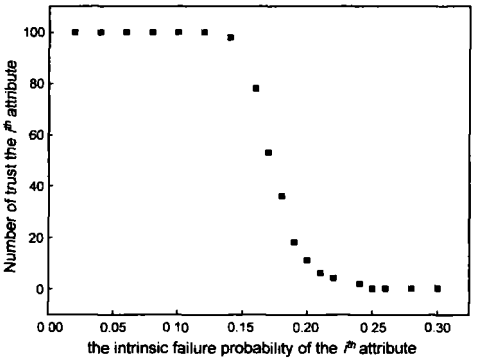

图 2　模拟结果

6 结论

本文针对网格资源访问过程中遇到的主观信任问题, 给出了一种使用贝叶斯函数的主观信任模型, 对该模型的模拟结果表明, 该模型能够很好地用于网格用户评估资源提供节点的属性的信任情况, 从而决定对资源的访问. 该模型的特点在于尽量减少了中间节点的主观随意性判断, 而将更多的主观判断留给请求者来处理, 即请求者可以自主地根据自己的需要, 通过对不同属性制定不同的置信度和期望失败率(成功率), 因而也不失灵活性. 另外通常人们通过推荐信任得到对对方的信任评判时, 会考虑中间结果的叠加和综合, 这也是目前考虑主观信任机制的一种方式. 而我们在搜索信任链路时, 由于使用的中间推荐者的声望值都最高, 不考虑声望值低的推荐者的行为, 并且在最后综合信任机制时采用的是对最终推荐节点的综合, 因而没有必要考虑中间结果的叠加过程, 通常认为他们给出的推荐结果都是正确的, 即使存在欺骗行为, 只要不是联合欺骗, 当最终推荐节点数目较多, 在进行评判时, 那些带有欺骗行为的节点也将淹没在这些数据中, 因而对最终评判结果影响不大.

参考文献:

[1] Josang A, Knapskog S J. A metric for trusted systems[A]. Proceedings of the 21st National Security Conference[C]. NSA, 1998. 16- 29.

[2] Yu B, Singh M P. Distributed reputation management for electronic commerce[J]. Computational Intelligence, 2002, 18(4): 535- 549.

[3] Yu B, Singh M P. Detecting deception in reputation management[A]. Proceedings of the Second International Joint Conference on Autonomous Agents and Multi-Agent Systems[C]. Melbourne, Australia, 2003. 73- 80.

[4] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401- 1408.
Tang W, Chen Z. Research of subjective trust management model on the fuzzy set theory[J]. Journal of Software, 2003, 14(8): 1401- 1408. (in Chinese)

[5] Lin C, Varadharajan V, Wang Y, Pruthi V. Enhancing grid security with trust management[A]. Services Computing Proceedings[C]. IEEE, 2004. 303- 310.

[6] Song S, Hwang K. Fuzzy trust integration for security enforcement in grid computing[A]. International Symposium on Network and Parallel Computing (NPC2004)[C]. Heidelberg: Springer-Verlag GmbH, 2004.

[7] Azzedin F, Maheswaran M. Evolving and managing trust in grid computing systems[A]. Electrical and Computer Engineering, IEEE CCECE 2002[C]. Canadian, 2002. 1424- 1429.

[8] Azzedin F, Maheswaran M. A trust brokering system and its application to resource management in public-resource grids[A]. 18th International Parallel and Distributed Processing Symposium (IPDPS'04)[C]. Santa Fe: IEEE Computer Society, 2004. 22- 32.

[9] 周明辉, 梅宏, 焦文品. 基于中间件的可定制信任管理框架[J]. 电子学报, 2005, 33(5): 820- 826.
Zhou Ming-hui, Mei Hong, Jiao Wen-pin. A customizable trust management framework based on middleware[J]. Acta Electronica Sinica, 2005, 33(5): 820- 826. (in Chinese)

[10] 盛骤, 谢式千, 潘承毅. 概率论与数理统计[M]. 北京: 高等教育出版社, 1997. 131- 139.

作者简介:

陈建刚　男, 1978年生于江西丰城, 南京邮电大学计算机学院2004级博士研究生. 主要研究方向为网格技术、信息安全等.

王汝传　男, 1943年生于安徽合肥, 教授、博士生导师, 主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等. E-mail: wangrc@njupt.edu.cn

王海艳　女, 1974年生于江苏扬州, 南京邮电大学计算机学院讲师, 硕士, 在读博士, 主要研究方向为计算机软件、计算机网络、信息安全、移动代理等.