doi:10.3969/j.issn.1000-436x.2012.z1.019

分布式环境下信任路径选择性搜索及聚合研究

秦艳琳，吴晓平，高键鑫
（海军工程大学 信息安全系，湖北 武汉 430033）

摘 要：针对现有基于信誉的信任模型在刻画节点推荐可信度、推荐信任路径搜索及合成算法方面存在的问题，提出基于时间衰减因子、推荐吻合度因子及交互成功率因子的推荐可信度更新算法，进而给出一种新的分布式环境下推荐信任路径选择性搜索算法，该算法以邻居节点间推荐可信度、评分相似度、路径长度等作为控制条件，能直接在搜索过程中规避恶意节点，选择包含有效推荐信息的路径进行搜索并停止对冗余路径的搜索。最后采用一种改进的 D-S 证据理论合成算法对搜索得到的信任路径进行聚合。仿真实验表明，与已有模型相比，所提模型具有较强的抵制各种恶意节点攻击的能力。

关键词：分布式网络；信任模型；推荐可信度；推荐信任路径；D-S 证据理论
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0148-09

Research on selective trust-path search and aggregation in distributed environment

QIN Yan-lin, WU Xiao-ping, GAO Jian-xin
(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: Current trust models based on reputation had some disadvantages in characterizing recommendation credibility and dealing with Trust-Path Search and aggregation. To solve these problems, an updating algorithm for recommendation credibility was proposed considering factors of time decay, recommendation inosculation and success transaction rate. Furthermore, a selective search-algorithm for trust-path in distributed environment was presented. The algorithm uses recommendation credibility, evaluation similarity and trust-path length as its control parameters and can evade malicious nodes directly in the process of searching. It can also stop the search for unnecessary trust-paths and execute the search for paths containing valuable recommendation. Lastly, trust aggregation method was given by using an advanced combining algorithm in D-S theory of evidence. Simulation results show that compared with existing trust models, the proposed model is more robust on defending attacks of various malicious nodes.

Key words: distributed network； trust model; recommendation credibility; recommendation trust path; D-S theory of evidence

1 引言

现今计算机为了达到资源共享及高使用率的目标，大都采用分布式的结构，即由多个软件服务组成的动态协作系统。地域分散的多个组织又通过 Internet 动态结盟构成一种大规模分布式网络计算环境，如当前流行的普适计算、P2P 计算、网格、服务计算等。在这些计算环境中，节点拥有更多的

收稿日期：2012-07-01
基金项目：国家自然科学基金资助项目(71171198)；国家自然科学基金青年基金资助项目(61100042)
Foundation Items: The National Natural Science Foundation of China (71171198)；The National Natural Science Foundation of China (Project for Youth) (61100042)

自由,节点之间的交互也更加频繁和复杂。各主体往往隶属于不同的权威管理机构，拟交互主体很可能分布在陌生的网络环境中从而很难建立起一种信任关系。这就使得各类恶意节点能进入网络，提供欺骗服务，滥用网络资源，给合法用户造成不同程度的损失。在大规模分布式系统中引入信任机制的研究已经受到了重视，信任机制可以使节点在交互前评价对方的信任度，从而判定交互的安全性、可靠性，抵制恶意节点的攻击。

目前，国内外相关学者基于不同数学理论开展了适用于各种开放分布式网络系统中信任模型的研究，研究成果共同推动了信任建模理论的不断发展，但仍有一些问题没有得到很好的解决。

1) 目前基于信誉的信任模型在计算推荐节点的推荐可信度时方法不一，部分模型直接将推荐可信度等同于直接信任度，部分模型虽进一步细化了推荐可信度的影响因素，但并不完善；

2) 现有的大多数信任模型仍建立在洪泛搜索结果的基础上讨论推荐信任的传递与聚合，部分模型虽考虑到洪泛搜索结果中信任路径的相互依赖问题，但都是对已搜索得到的推荐信任网络进行了简化或依赖关系消除，并未在搜索过程中直接实现信任路径的选择性搜索，造成搜索效率不高，难以避免恶意节点进入推荐信任网络，进而不利于推荐信任路径的高效合成。

针对上述问题，本文在分析邻居节点间推荐可信度影响因素的基础上，给出了新的推荐可信度随时间更新算法,进而提出了以邻居节点间推荐可信度、评分相似度、路径长度等作为控制条件的选择性推荐信任路径搜索策略,对搜索结果的聚合算法则采用了一种改进的 D-S 证据理论合成算法以有效处理冲突较大的推荐信息,得到更趋合理的合成结果。

论文第 2 节介绍了相关工作，第 3 节给出了具体的推荐可信度更新算法，讨论了一种推荐信任路径选择性搜索算法，并在搜索得到的推荐信任网络的基础上，结合一种改进的 D-S 证据合成方法给出了节点推荐信任度的聚合算法，第 4 节进行了仿真实验及实例分析，第 5 节对全文进行总结。

2　相关工作

在信任机制研究中,通常利用节点之间的交互经历来建立信任关系。当缺乏直接交互经历时,就需要使用来自第三方的推荐信息来建立推荐信任（信誉），这就需要对推荐者的推荐可信程度进行量化处理，各类信任模型提出各自不同的处理方法。

部分信任模型[1~3]直接将邻居节点间的直接信任度作为推荐可信度，事实上并不符合人类社会的认知规律，交互能力强仅代表该节点执行某些动作的能力较强，并不完全代表该节点在为其他节点提供推荐信息时的诚信度更高，也即可能出现交互能力很强却为其邻居提供虚假信息的情况。文献[4]提出了一个针对恶意推荐者的信任模型，针对服务节点所提供的文件来评价其推荐的可靠程度。文献[5]定义了可疑交易来识别虚假反馈。文献[6]提出了一种区分服务信任与反馈信任的概率信任获取方法，增强了信任模型抵抗恶意实体策略行为攻击的能力。

文献[7]提出推荐可信度由请求节点与反馈节点的交易密度因子和评分相似度共同决定，该方法未考虑反馈节点的诚实性，具有一定的片面性。文献[8]又对上述方法进行了改进，提出推荐节点的推荐可信度由评分相似度和交易差异因子共同决定，但交易差异度因子利用推荐节点及请求节点对目标节点直接信任度的差值来刻画，而在大多数情况下只有当请求节点对目标节点的直接经验不足时，才会搜集其他节点的推荐信任，因此得出的交易差异度因子也缺乏依据。

文献[9]引入了更新幅度和更新力度 2 个参数来更新推荐可信度，并通过考察请求节点与推荐节点间的评价差异（由二者对目标节点的直接信任偏差和评价相似度共同决定）来决定推荐可信度的增减，在请求节点对目标节点的直接交互经验不足时并不能公正的对推荐节点的推荐可信度进行奖惩。

文献[10]用成功推荐次数对推荐总次数的比率来刻画节点反馈可信度，没有考虑反馈可信度随时间衰减情况且对虚假推荐的惩罚力度不够。

在信任传递与聚合研究方面，部分文献[10~17]仍建立在洪泛搜索的基础上对推荐信任网络进行分析聚合。

文献[10]研究了证据信任模型中的信任传递和聚合，基于图论对信任网络中相互依赖路径进行了消除，并采用证据合成规则对消除依赖路径后的信任子图进行信任聚合。但该模型也是建立在洪泛搜索结果的基础上，在信任路径搜索效率上并未提高且搜索结果中包含各类恶意节点，导致证据冲突量

大，合成结果可能与实际情况不符。

文献[15]提出一种传递信任网络分析方法，通过分裂洪泛搜索得到的信任图中引发信任路径间依赖关系的边和节点来获得规范信任图，也即各条信任链相互独立的信任网络。

文献[17]基于洪泛搜索结果将信任网中推荐链的依赖关系分为无依赖关系与依赖关系，依赖关系又分为部分依赖与完全依赖，并给出了相应的解决策略。

文献[18]提出基于多影响因素的网格信任传播算法，对节点的交互能力和诚实能力进行了区分，但并未给出节点诚实能力的具体刻画方法，搜索算法对大量相互依赖的搜索路径未加取舍，导致算法效率不高且搜索结果存在大量冗余信息。

为此，本文在给出新的推荐可信度更新算法的基础上提出了一种选择性推荐信任路径搜索策略，该搜索策略符合人类的心理认知习惯，贴近人类社会信任网络的形成机理，能直接在搜索过程中规避恶意节点，停止对蕴含冗余信息的推荐路径的搜索，搜索得到的推荐信任网络可直接进行推荐信任的聚合运算。聚合算法采用了改进的 D-S 证据理论合成算法，在一定程度上削弱了信任网络中少量伪装节点不实推荐的影响。

3 一种新的信任路径选择性搜索策略及聚合算法

3.1 基本概念

定义 1 大规模分布式网络环境下，信任是关于各对等节点安全、可靠、高效且低风险的执行某种特定动作的可能性的主观测度和预期，其主要由 2 部分组成，即直接信任度与推荐信任度。

定义 2 推荐可信度是节点 i 对其推荐节点 j 提供的推荐信息的信赖程度，记为 Cr_{ij}。

定义 3 推荐吻合度 r_{ji} 表示某一时间段 Δt 内 j 向 i 提供的关于目标节点 O 的推荐信息与 i 与 O 最终交互结果的吻合程度，规定 j 向 i 提供的关于 O 的推荐信任度较高（较低），而 i 与 O 交互成功（失败），则本次推荐为吻合推荐，否则为不吻合推荐，推荐吻合度可定义为 $r_{ji}=\dfrac{\Delta t\text{内}j\text{对}i\text{吻合推荐次数}}{\Delta t\text{内}j\text{对}i\text{推荐总次数}}$。

定义 4 交互成功率 r'_{ij} 为时间段 Δt 内节点 i 与节点 j 之间进行直接交互的成功次数与总次数的比率，即 $r'_{ij}=\dfrac{\Delta t\text{内}i\text{与}j\text{交互成功次数}}{\Delta t\text{内}i\text{与}j\text{交互总次数}}$。

3.2 推荐可信度更新算法

本文对邻居节点间的推荐可信度进行了全面分析，引入了时间衰减因子，推荐吻合度因子及交互成功率因子对邻居节点间的推荐可信度进行更新：

$$Cr_{ij}^{t}=\begin{cases}Cr_{ij}^{t_0}\theta^{\Delta t}+(1-Cr_{ij}^{t_0}\theta^{\Delta t})(\beta_1 r_{ji}+\beta_2 r'_{ij})\\ -Cr_{ij}^{t_0}\theta^{\Delta t}[\gamma_1(1-r_{ji})+\gamma_2(1-r'_{ij})],t>0\\ 0.5,t=0\end{cases}\quad(1)$$

其中，Cr_{ij}^{t} 是当前时刻节点 i 对其邻居 j 的推荐可信度，$Cr_{ij}^{t_0}$ 是节点 i 在本地存储的原有的邻居 j 的推荐可信度，$\Delta t=t-t_0$；θ 为推荐可信度随时间衰减因子，$0<\theta\leqslant 1$，该因子的引入主要使节点 i 更加关注节点 j 近期的推荐行为而逐渐减少对节点 j 过期的推荐可信度评价的依赖程度；β_1 为节点 i 对 j 提供吻合推荐的奖励因子，γ_1 则为节点 i 对 j 提供不吻合推荐的惩罚因子，且有 $0<\beta_1<\gamma_1<1$；β_2 为节点 i 对 j 在时间段 Δt 内成功交互的奖励因子，γ_2 则为节点 i 对 j 在时间段 Δt 内失败交互的惩罚因子，且有 $0<\beta_2<\gamma_2<1$；通常情况下，还可以规定 $\beta_1>\beta_2$，$\gamma_1>\gamma_2$ (这是因为 i 对 j 吻合推荐的奖励力度应大于它们之间直接交互成功的奖励力度，而 i 对 j 不吻合推荐的惩罚力度也应大于它们之间交互失败的惩罚力度)且 $0<\beta_1+\beta_2<1$, $0<\gamma_1+\gamma_2<1$。另外，本文规定在初始时刻邻居节点间的推荐可信度为 0.5。上述推荐可信度更新算法融合了以下思想。

1) 推荐可信度随时间动态变化，节点将更加关注其邻居推荐节点近期的行为；

2) 推荐可信度应随诚实的推荐行为提高而随着虚假的推荐行为降低，且诚实的推荐行为使得推荐可信度增加缓慢而虚假的推荐行为使得推荐可信度急剧下降；

3) 推荐可信度也在一定程度上与两邻居节点间的直接交互经验相关（这符合人类社会的认知规律，即人们往往倾向于接受与自己交往密切且行为能力较强的人的推荐信息）。为简化推荐可信度的更新算法，上述算法中未考虑邻居节点间的评价相似度因子，而直接将该因子作为下文信任路径搜索算法的控制条件之一。

3.3　推荐信任路径选择性搜索算法

首先，对按照文献[19]中的方法搜索得到的信任网络中的信任路径，如图 1 所示，进行分析以确定相互依赖路径的取舍。

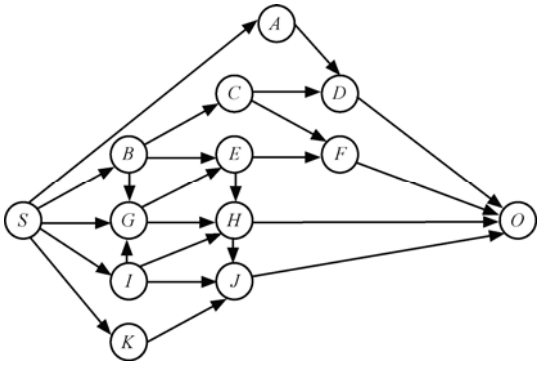


图 1　请求节点 *S* 与目标节点 *O* 间的推荐信任网络

图 1 中存在相互独立的推荐信任路径，如 *S*→*B*→*E*→*F*→*O* 与 *S*→*G*→*H*→*O*，同时存在大量相互依赖的信任路径，如 *S*→*A*→*D*→*O* 与 *S*→*B*→*C*→*D*→*O*，*S*→*B*→*G*→*H*→*O* 与 *S*→*G*→*H*→*O* 等。在这些相互依赖的信任路径中，有相当一部分推荐路径蕴含冗余信息，可在搜索过程中舍弃而不影响最终对目标节点推荐信任的评判。下面将对信任网络中相互依赖的路径进行分析，以决定相关路径的取舍。

1) *S*→*I*→*J*→*O* 与 *S*→*K*→*J*→*O*，经由 2 条路径向 *S* 反馈的推荐信息均为节点 *J* 关于目标节点 *O* 的直接交互经验，但 *S* 对 *J* 提供的关于目标节点 *O* 的推荐信息的信赖程度将由两条路径共同决定，因此 2 条信任路径对目标节点的推荐信任度计算存在同等重要的价值。同理，*S*→*B*→*C*→*F*→*O*、*S*→*B*→*E*→*F*→*O* 与 *S*→*G*→*E*→*F*→*O* 3 条路径同时搜索也是必要的。

2) *S*→G→H→*O*、*S*→*B*→*G*→*H*→*O* 与 *S*→*I*→*G*→*H*→*O*，按照人类社会的认知规律，*S* 将直接采纳其邻居节点 *G* 提供的来自于 *H* 关于目标节点 *O* 的推荐信息，而不会通过第三方即 *B* 或 *I* 搜集来自于 *G* 的相关信息，因此在推荐路径搜索过程中应停止对第 2、3 两条路径的搜索而直接进行第 1 条路径的搜索。类似的，*S*→*G*→*H*→*O* 与 *S*→*G*→*E*→*H*→*O* 也应停止对第 2 条路径的搜索。

3）*S*→*G*→*H*→*O* 与 *S*→*G*→*H*→*J*→*O*，由于节点 *H* 与目标节点 *O* 有足够的直接交互经验，它将直接把关于 *O* 的推荐信息经由 *G* 反馈给 *S*，而不需再向其邻居 *J* 请求关于 *O* 的推荐信息，因此搜索过程中应停止第 2 条路径的搜索。

4）*S*→*B*→*C*→*D*→*O* 与 *S*→*B*→*C*→*F*→*O*，2 条路径虽然部分重合，但是 *S* 通过第 1、2 条路径得到的推荐信息分别来自于节点 *D* 及 *F* 对 *O* 的直接信任，因此 2 条路径的同时搜索是必要的。

在对推荐信任网络中相互依赖的路径进行详细分析后，将给出具体的推荐信任路径选择性搜索算法。

算法 1　选择性信任路径搜索算法 STPSA

每个节点预先计算其相邻节点的推荐可信度（按照式(1)计算）和评价相似度（按照文献[19]中的方法计算）并存储在本地。

输入：信任请求者 *Re*，目标节点 *Ob*，　*Re* 的相邻节点集合 *Neighbor*(*Re*)

输出：信任路径集合 $Set(path_{\mathrm{Re},Ob})$

Info 数据结构：

{上级节点标识向量 p;

已发送节点标识集合 rSet(R);

目标结点 ob;

实际推荐节点对目标节点的直接信任度 dt;

回传信息标识 flag}

请求节点 *Re* 发送搜索信息算法 STPSA1：

1) Info_1.p= *Re*;

2) Info_1. rSet(R)=*Neighbor*(*Re*);

3) Info_1.ob=*Ob*;

4) Info_1.dt=null;

5) Info_1.flag=false;

6) for(所有 $R_i \in Neighbor(Re)$)

7) { If($Cr^{t}_{\mathrm{Re}\to R_i} \geqslant \eta$ && $\mathrm{Similarity}_{\mathrm{Re}\to R_i} \geqslant \tau$)

8) {向 R_i 发送 Info_1 信息；

9)　}

10) }

11) 开启监听线程，持续预定时间

12) if(收到监听信息 Info_2)

13) {

14)　$Set(path_{\mathrm{Re},Ob}) = Set(path_{\mathrm{Re},Ob}) \cup \mathrm{Info}_2.\mathrm{p}$;

15) }

16) return $Set(path_{\mathrm{Re},Ob})$;

中间节点 *Mi* 以收到 Info 数据包为事件，处理此事件的算法为 STPSA2。

STPSA2 算法：

输入：上级节点发送信息 Info_1；本节点 *Mi* 的

相邻节点集合 *Neighbor*(*Mi*)

输出：本节点发送信息 $Info_2$

17) if($Info_1$.flag=true)

18) {

19) 向 $Info_1$.p 向量序列中本节点前一节点发送 $Info_1$;

20) *Mi* 终止 STPSA2 算法;

21) }

22) $Info_2$.p=$Info_1$.p+*Mi*.toString();

23) $Info_2$. rSet(R)= $Info_1$. rSet(R) ⋃ *Neighbor*(*Mi*);

24) $Info_2$.ob= $Info_1$.ob;

25) for(所有 $R_i \in Neighbor(Mi)$ && $R_i \notin Info_1.p \bigcup Info_1.rSet(\mathrm{R})$)

26) {

27) if(R_i=*Ob*)

28) {$Info_2$.dt= DT_{Mi}^{Ob}

29) $Info_2$.flag=true;

30) 向 $Info_1$.p[$Info_1$.p.length()]节点发送 $Info_2$;

31) }

32) else if(Info1.p.length<*l*&& $Cr^t_{Mi \to R_i} \geqslant \eta$ && $\mathrm{Similarity}_{Mi \to R_i} \geqslant \tau$)

33) {

34) $Info_2$.flag=false;

35) 向 R_i 发送 $Info_2$;

36) }

37) }

图 2 为使用算法 STPSA 搜索得到的结果。

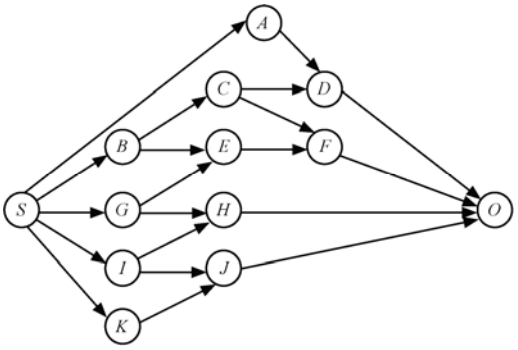


图 2 使用本文搜索算法得到的推荐信任网络

3.4 基于改进 D-S 证据理论的信任路径合成算法

定义 5 2 节点间直接交互信任的识别框架 Θ 为集合{*DT*（交互信任）、¬*DT*（交互不信任）}，Θ 的幂集 2^{Θ} 为{ Φ，{*DT*}，{ ¬*DT* }，{*DT*,¬*DT*}}。节点间的直接交互信任关系采用三元组{*m*({*DT*})，*m*({ ¬*DT* })，*m*({*DT*,¬*DT*})}描述，其中 *DT* 表示交互信任，¬*DT* 表示交互不信任，{*DT*,¬*DT*}表示不能确定，且有 *m*({*DT*})+*m*({ ¬ *DT* })+*m*({*DT*, ¬ *DT*})=1。当前时刻节点 *i* 对 *j* 的直接信任关系可以表示为

$$DT_i^j = \{m_i^j(\{DT\}), m_i^j(\{\neg DT\}), m_i^j(\{DT, \neg DT\})\}$$

其中，$m_i^j(\{DT\}) = c_{i,j}\dfrac{s_{i,j}}{s_{i,j}+f_{i,j}}$，$m_i^j(\{\neg DT\}) = c_{i,j}\dfrac{f_{i,j}}{s_{i,j}+f_{i,j}}$，$m_i^j(\{DT, \neg DT\}) = 1 - c_{i,j}$，$s_{i,j}$ 为 *i* 与 *j* 直接交互成功的次数，$f_{i,j}$ 为 *i* 与 *j* 直接交互失败的次数，$c_{i,j}$ 为区间(0,1]上的数，表示由 *i* 与 *j* 直接交互经验得到的直接信任的可靠性。

定义 6 推荐可信的识别框架 Θ 为集合{C*R*（推荐可信）、¬C*R*（推荐不可信）}，Θ 的幂集 2^{Θ} 为{ Φ，{C*R*}，{ ¬*CR* }，{C*R*,¬C*R*}}。节点间的推荐可信关系采用三元组{*m*({*CR*})，*m*({ ¬C*R* })，*m*({C*R*,¬C*R*})}描述，其中 *CR* 表示推荐可信，¬*CR* 表示推荐不可信，{*CR*,¬*CR*}表示不能确定，且有 *m*({*CR*})+*m*({ ¬*CR* })+*m*({*CR*,¬*CR*})=1。当前时刻节点 *i* 对 *j* 的推荐可信关系可以表示为

$$CR_i^j = \{m_i^j(\{CR\}), m_i^j(\{\neg CR\}), m_i^j(\{CR, \neg CR\})\}$$

其中，$m_i^j(\{CR\}) = e_{i,j}Cr_{ij}^t$，$m_i^j(\{\neg CR\}) = e_{i,j}(1 - Cr_{ij}^t)$，$m_i^j(\{CR, \neg CR\}) = 1 - e_{i,j}$，$e_{i,j} \in (0,1]$，表示由式(1)计算的 *i* 对 *j* 的推荐可信度 Cr_{ij}^t 的可靠性。

3.4.1 *S* 对各反馈节点推荐可信度的合成算法

由于请求节点 *S* 最终得到的推荐信息分别来自于目标节点 *O* 的邻居节点 $W_i(1 \leqslant i \leqslant r)$（图 2 中的 *D*、*F*、*H*、*J*），把这些节点称为实际推荐节点。下面利用证据理论和搜索到的有效推荐信任路径合成实际推荐节点的推荐可信度。

文献[10]在采用证据理论融合多源推荐信息时，没有考虑证据之间存在冲突的情况，事实上在证据高冲突或完全冲突的情况下使用传统的证据合成方法会出现融合结果与实际情形不符或失效等问题。为此，本文采用以下方法对证据 $E_i(1 \leqslant i \leqslant n)$进行合成。

1) 计算 $K_i = \sum_{j=1, j \neq i}^{n} \sum_{A_i \cap A_j = \Phi} m_i(A_i) m_j(A_j)$；

2) 根据 K_i 的大小对所有证据 E_i 进行编号，K_i

最小的证据编号为 L_1，K_i 最大的证据编号为 L_M，K_i 相等或近似相等的证据编号相同。

3) 对具有相同编号 $L_s(1\leqslant s\leqslant M)$的证据计算其间的冲突量，并按下式进行合成。

$$m(A)=\begin{cases}0, A=\Phi\\ \dfrac{\sum\limits_{A_i\cap B_j\cap\cdots=A} m_1(A_i)m_2(B_j)\cdots}{1-\sum\limits_{A_i\cap B_j\cap\cdots=\Phi} m_1(A_i)m_2(B_j)\cdots}, \text{冲突小于0.5}\\ \sum\limits_{A_i\cap B_j\cap\cdots=A} m_1(A_i)m_2(B_j)\cdots+\\ q(A)\sum\limits_{A_i\cap B_j\cap\cdots=\Phi} m_1(A_i)m_2(B_j)\cdots, \text{冲突大于0.5}\end{cases}$$

其中，$q(A)=\dfrac{n_A}{n}$（n 为不同命题的统计次数，n_A 为支持命题 A 的所有证据中 BPA 不小于 0.5 的证据数。合成后的新证据记为 E_{L_s} $(1\leqslant s\leqslant M)$。

4) 对合成后的新证据仍利用式(2)按照 $E_{L_1},E_{L_2},\cdots,E_{L_M}$ 的顺序两两合成，即 E_{L_1} 与 E_{L_2} 合成，结果再与 E_{L_3} 合成，依次类推，可得最终的合成结果。

下面给出请求节点 S 对实际推荐节点 $W_i(1\leqslant i\leqslant r)$推荐可信度的合成算法。

算法 2　推荐可信度合成算法

Combine-C$R(i,j)$

{if(j 为 i 的邻居节点)

　return CR_i^j；

else{for(i 的所有邻居节点 v_k)

{ $CR_i^j=\underset{k}{\oplus}(CR_i^{v_k}\otimes$ Combine-$CR(v_k,j))$；}}}

算法中的“$\oplus$”按照给出的改进后的证据合成算法进行运算，“$\otimes$”按照下述规则进行运算。

若推荐信任路径为：$A\rightarrow B\rightarrow C$，则

$$CR_A^C=CR_A^B\otimes CR_B^C$$

其中，$m_A^C(\{CR\})=m_A^B(\{CR\})\times m_B^C(\{CR\})$，

$m_A^C(\{\neg CR\})=m_A^B(\{\neg CR\})\times m_B^C(\{\neg CR\})$，

$m_A^C(\{CR,\neg CR\})=1-m_A^C(\{CR\})-m_A^C(\{\neg CR\})$。

3.4.2　S 对目标节点 O 推荐信任度的合成算法

利用算法 2 得到 S 对各实际推荐节点 $W_i(1\leqslant i\leqslant r)$的推荐可信关系后，即可合成 S 对目标节点 O 的推荐信任

$$RT_S^O=\underset{1\leqslant i\leqslant r}{\oplus}RT_S^{W_iO}=\underset{1\leqslant i\leqslant r}{\oplus}(CR_S^{W_i}\tilde{\otimes}DT_{W_i}^O)$$，

其中，“$\oplus$”按照给出的改进后的证据合成算法进行运算，“$\tilde{\otimes}$”按照以下规则运算。

$m_S^{W_iO}(\{RT\})=m_S^{W_i}(\{CR\})\times m_{W_i}^O(\{DT\})$，

$m_S^{W_iO}(\{\neg RT\})=m_S^{W_i}(\{CR\})\times m_{W_i}^O(\{\neg DT\})$，

$m_S^{W_iO}(\{RT,\neg RT\})=1-m_S^{W_iO}(\{RT\})-m_S^{W_iO}(\{\neg RT\})$。

4　实例及仿真分析

仿真实验使用 QueryCycleSimulator 模拟 P2P 环境下的文件共享应用,同时实现了本文模型、Eigen Trust 及文献[10]中的信任模型。仿真环境设置如表 1 所示。

表 1　**仿真环境设置**

参数名	描述	值
N	网络节点总数	1 000
N_f	文件总数	10 000
θ	时间衰减因子	0.9
β_1	吻合推荐的奖励因子	0.2
γ_1	不吻合推荐的惩罚因子	0.5
β_2	成功交互的奖励因子	0.05
γ_2	失败交互的惩罚因子	0.1
η	推荐可信度阈值	0.8
τ	评价相似度阈值	0.6
l	路径长度限值	4

假设网络中的节点依据行为表现分为以下几种。

1) 正常节点，该类节点无论在提供服务与对其他节点的推荐都是真实的；

2) 简单恶意节点（SM），始终提供恶意服务和恶意推荐的节点；

3) 策略恶意节点（TM），为掩盖自己的恶意行为，以较高概率(0.7)为其他节点提供可靠服务，同时以较低概率（0.3）对其他节点给出符合实际的评价；

4) 合谋节点（CM），合谋欺诈的 SM、TM 类恶意节点形成协同作弊的团体，每个节点竭力夸大同一团体内的同伙或同时贬低某些节点的信任度或伪造信任度；

5) 伪装节点（DM），某些节点在通过提供可靠服务和有效推荐得到高信任度后，对其恶意同伙做出虚假推荐或诋毁正常节点。

假设网络中恶意节点比例为[0.1~0.5]，仿真周期为 100 次，仿真次数为 3 次，实验结果取均值。成功交互是指请求节点从响应节点准确无误的下载到所需要的文件，否则为一次失败交互。成功交互率能够体现信任模型在抵制恶意节点攻击方面的能力强弱。图 3、4、5、6 分别显示仿真网络内存在 SM，TM，CM 和 DM 4 类恶意节点时，随着恶意节点比例变换，系统的成功交互率变化情况。

由图 3 可知，随着 SM 类恶意节点比例的增加，成功交互率均维持在一个较高的水平，这说明 3 种信任模型都能比较容易的识别此类恶意节点，而使用本文的信任路径搜索策略，直接将此类节点排除在信任网络之外，因此相较其他 2 类信任模型而言本文模型对该类恶意节点攻击的抵制能力更强。

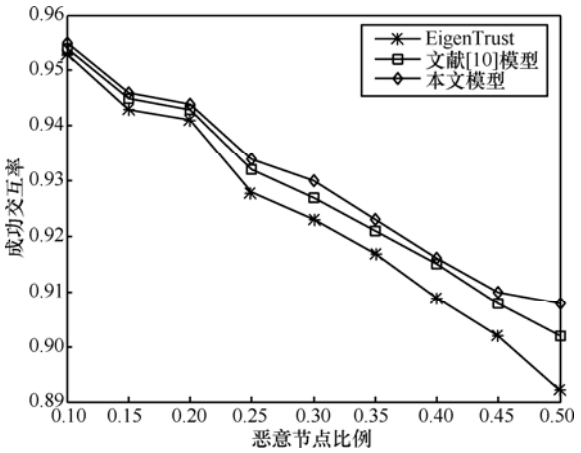


图 3　SM 攻击下成功交互率对比

图 4 是随着 TM 类恶意节点比例变化 3 种信任模型下系统成功交互率的对比情况。由于 EigenTrust 方案将推荐可信度等同于直接信任，部分恶意推荐信息在信任度计算中被赋予较高权重，导致请求节点的误判率升高，系统成功交互率下降较快。文献[10]虽区分了直接信任与推荐可信度，但推荐可信度简单的用诚实推荐数占总推荐数的比例刻画，且信任模型建立在洪泛搜索的基础上，部分 TM 类节点进入推荐网络，其提供的恶意推荐在一定程度上被请求节点采纳，导致系统成功交互率的有所降低。本文模型提出的推荐可信度算法对节点不吻合推荐及提供虚假服务的惩罚力度远大于对吻合推荐及提供可靠服务的奖励力度，因此经过一段时间的仿真，TM 类节点的推荐可信度将迅速降低，同时结合评价相似度的搜索控制条件，此类节点将在搜索过程中被排除在推荐信任网络之外，使系统不受此类节点虚假推荐的影响，进而维持较高的成功交互率。

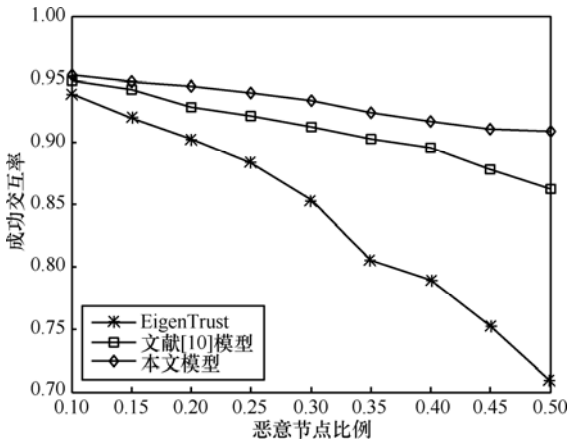


图 4　TM 攻击下成功交互率对比

图 5 是仿真网络中存在 CM 类节点时系统成功交互率的对比情况。由于 EigenTrust 对此类恶意节点缺乏足够的识别与惩罚机制，造成系统成功交互率的下降。文献[10]中的信任模型通过多条推荐链之间依赖关系的消除与聚合，减轻了 CM 类节点提供的不实推荐的影响，但由于其推荐可信度刻画不细致等原因，使得成功交互率仍有一定程度的降低。本文模型的推荐可信度更新算法使合谋节点的推荐可信度迅速降低从而直接被排除在推荐信任网络之外，因此系统受 CM 类节点的虚假推荐的影响很小，能够保持较高的成功交互率。

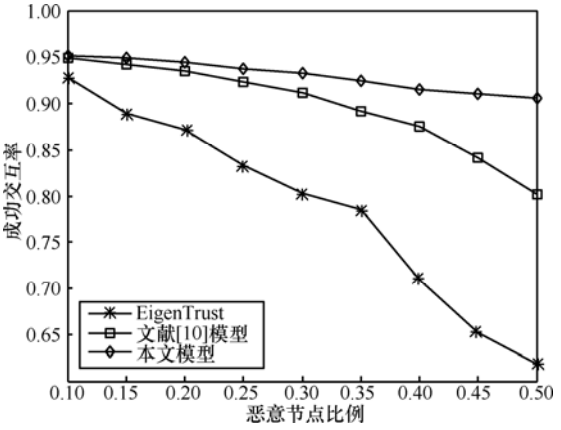


图 5　CM 攻击下成功交互率对比

图 6 是 3 种信任模型下系统成功交互率随 DM 类节点比例增加的对比情况。可以看出，EigenTrust 无法抵制此类恶意节点的攻击。文献[10]中的信任模型使用一般的证据合成方法对推荐信息进行合成，导致当部分伪装节点提供与其他诚实推荐节点

冲突较大的虚假信息时，合成结果受影响较大，并且在伪装节点提供虚假推荐后对该节点的推荐可信度未采取及时的惩罚更新机制，从而使系统成功交互率降低。本文使用改进的 D-S 证据理论合成方法，减轻了冲突信息对合成结果的影响，且推荐可信度更新算法中引入时间衰减因子和严格的惩罚因子，使得伪装节点在提供虚假推荐后，其推荐可信度迅速降低，从而很快被排除在推荐信任网络之外，进而使系统维持较高的成功交互率。

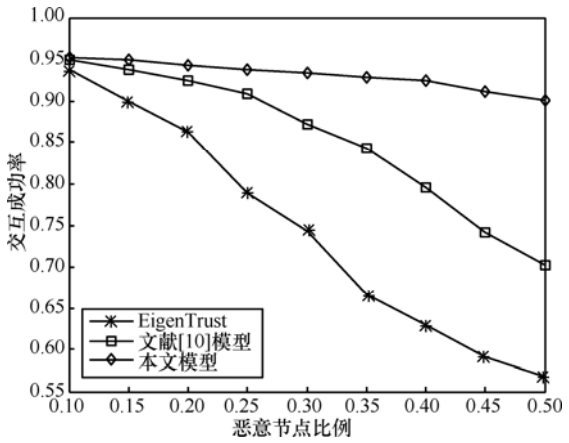


图 6　DM 攻击下成功交互率对比

通过下例也可以说明，伪装节点恶意推荐的影响在改进的证据理论合成过程中也被削弱。

例 1　假设 $CR_S^{W_1}$ ={0.85, 0.10, 0.05}，$DT_{W_1}^O$ ={0.82, 0.15, 0.03}；$CR_S^{W_2}$ ={0.85, 0.08, 0.07}，$DT_{W_2}^O$ ={0.02, 0.97, 0.01}; $CR_S^{W_3}$ ={0.80, 0.15, 0.05}，$DT_{W_3}^O$ ={0.81, 0.12, 0.07}。计算可得

$RT_S^{W_1O}$ = {0.697, 0.128, 1.175},

$RT_S^{W_2O}$ ={0.017, 0.824 5, 0.158 5},

$RT_S^{W_3O}$ = {0.648, 0.096, 0.256}。

可以看出，节点 W_2 提供的推荐信息与 W_1、W_3 提供的推荐信息存在较大冲突（可能为伪装节点的不实推荐）。

按照一般证据合成规则进行合成的结果为 RT_S^O ={0.555 9, 0.414 0, 0.030 1}，按照改进后的证据合成规则进行合成后的结果为

$\tilde{R}T_S^O$ ={0.635 9, 0.355 7, 0.008 4}

结果表明，若使用一般的证据合成方法进行合成，则合成结果（即请求节点 S 对 O 的推荐信任）受 W_2 提供的推荐信息的影响较大，可能产生误判。但是使用改进后的证据合成方法，将削弱 W_2 提供推荐信息的影响，合成结果贴近 W_1 与 W_3 提供的推荐信息。

5　结束语

本文对大规模分布式网络环境中邻居节点间推荐可信度的影响因素进行了分析，给出了一种新的推荐可信度随时间更新算法，并在此基础上提出了以推荐可信度、评分相似度及路径长度等作为控制条件的选择性推荐信任路径搜索算法，该搜索算法能直接在搜索过程中规避恶意节点，停止对冗余路径的搜索同时保留对有价值的推荐路径的搜索，符合人类的心理认知习惯。本文采用了改进的 D-S 证据理论合成算法对搜索得到的推荐信任网络直接进行推荐信任的聚合运算。仿真实验和实例分析结果表明，本文模型克服了已有模型的部分局限性，增强了系统抵御各类恶意节点攻击的能力。

参考文献：

[1] KAMWAR S D, SCHLOSSER M T, HECTOR GARCIA-MOLINA. The eigentrust algorithm for reputation management in P2P networks[A]. Proceedings of the 12th International Conference on World Wide Web[C]. Budapest, Hungary, 2003. 640-651.

[2] 李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报, 2009, 32(3):405-416.
LI X Y, GUI X L. Trust quantitative model with multiple decision factors in trusted network[J]. Chinese Journal of Computers, 2009,32(3): 405-416.

[3] 李小勇, 桂小林. 动态信任预测的认知模型[J]. 软件学报, 2010, 21(1):163-176.
LI X , GUI X L. Cognitive model of dynamic trust forecasting[J]. Journal of Software, 2010, 21(1):163-176.

[4] LEE S Y , KOWN O H, KIM J, *et al*. Agents and Peer-to-Peer Computing[M] . Heidelberg : Springer , 2008. 111-122.

[5] MEKOUAR L, IRAQI Y, BOUTABA R. Detecting malicious peers in a reputation-based peer-to-peer system[EB/OL]. http://bcr2.uwaterloo.ca/ ~iraqi/Papers/Conferences/CCNC2005. pdf,2005.

[6] SWAMYNATHAN G, ZHAO B Y, KEVIN C, *et al*. Globally decoupled reputations for large distributed networks[J]. Advances in Multimedia,2007,(1):12-25.

[7] 胡建理, 吴泉源, 周斌.一种基于反馈可信度的分布式 P2P 信任模型[J]. 软件学报, 2009, 20(10): 2885-2898.
HU J L, WU Q Y, ZHOU B. Robust feedback credibility-based distributed P2P Trust model[J]. Journal of Software, 2009, 20(10): 2885-2898.

[8] 胡建理, 周斌, 吴泉源. P2P 网络中具有激励机制的信任管理研究[J].通信学报, 2011,32(5):22-32.

HU J L, ZHOU B, WU Q Y. Research on incentive mechanism integrated trust management for P2P networks[J].Journal on Communications, 2011, 32(5):22-32.

[9] 于真, 申贵成, 刘丙午等. 一种 P2P 网络信任模型 METrust[J]. 电子学报, 2010,38(11):2600-2605.
YU Z, SHEN G C, LIU B W, *et al*. METrust: a trust model in P2P networks[J].Chinese Journal of Electronics，2010, 38(11):2600-2605.

[10] 蒋黎明, 张琨, 徐建等. 证据信任模型中的信任传递与聚合研究[J]. 通信学报, 2011, 32(8):91-100.
JIANG L M, ZHANG K, XU J, *et al*. Research on trust transitivity and aggregation in evidential trust model[J]. Journal on Communications, 2011, 32(8):91-100.

[11] 张明武, 杨波, 禹勇. 基于 D-S 理论的分布式信任模型[J]. 武汉大学学报(理学版),2009,55(1):41-44.
ZHANG M W, YANG B, YU Y. Distributed trust model based on D-S theory[J]. Journal of Wuhan University(Nat Sci Ed) ,2009, 55(1): 41-44.

[12] CHEN H G, WU H F, CAO X, *et al*. Trust propagation and aggregation in wireless sensor networks[A]. Japan-China Joint Workshop onFrontier of Computer Science and Technology[C]. Wuhan, China, 2007.

[13] JØSANG A, GRAY E, KINATEDER M. Simplification and analysis of transitive trust networks[J]. Web Intelligence and Agent System, 2006,4(2):139-161.

[14] YANG W Z, HUANG C H, *et al*.A general trust model based on trust algebra[A]. Proceedings of International Conference on Multimedia Information Networking and Security[C]. Wuhan,China,2007.

[15] JØSANG A. Optimal trust networks anaysis with subjectivelogic[A]. The Second International Conference on EmergingSecurity Information, Systems and Technologies[C]. France, 2008.

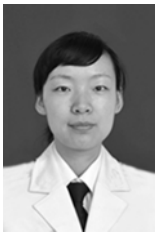
[16] CHEN Y X, ZHANG M, ZHU H, *et al*. Average transitive trustworthy degrees for trustworthy networks [A]. Proceedings of the 4th InternationalConference on Rough Sets and Knowledge Technology[C].Gold Coast, Australia,2009.

[17] 苏锦钿, 郭荷清, 高英. 基于信任网的推荐机制[J]. 华南理工大学学报(自然科学版)，2008，36(4):98-103.
SU J D, GUO H Q, GAO Y. Recommendation mechanism based on Web of trust[J]. Journal of South China University of Technology(Natural Science Edition), 2008, 36(4):98-103.

[18] 张琳, 王汝传, 王海艳. 基于多影响因素的网格信任传播算法[J]. 通信学报, 2011, 32(7):161-168.
ZHANG L, WANG R C, WANG H Y. Trust transitivity algorithm based on multiple influencing factors for grid environment[J]. Journal on Communications, 2011, 32(7): 161-168.

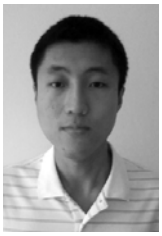
[19] 苗光胜, 冯登国, 苏璞睿. P2P 信任模型中基于行为相似度的共谋团体识别模型[J]. 通信学报, 2009, 30(8): 2-9.
MIAO G S, FENG D G, SU P R. Colluding clique detector based on activity similarity in P2P trust model[J]. Journal on Communications, 2009, 30(8): 2-9.

作者简介：



秦艳琳（1980-），女，河南安阳人，海军工程大学博士生、讲师，主要研究方向为动态信任管理理论及网络安全。

吴晓平（1961-），男，山西新绛人，海军工程大学教授、博士生导师，主要研究方向为信息安全及系统工程。



高键鑫（1989-），男，山东淄博人，海军工程大学硕士生，主要研究方向为移动自组网信任建模。