doi:10.3969/j.issn.1000-436x.2013.07.019

基于改进 D-S 证据理论的信任评估模型

张琳[1,2,3]，刘婧文[1]，王汝传[1,2,3]，王海艳[1,2,3]

（1. 南京邮电大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003；
3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210003）

摘 要：针对已有的信任证据模型不能快速有效地处理分布式网络中存在的恶意攻击，且缺乏关于三元信任关系组的信任归一方法，提出了一种基于改进 D-S 证据理论的信任模型，在此基础上，提出了基于持续序列的基本可信度函数和基于评估函数的信任评估方法，使得模型能更快地抑制恶意节点，并且评估结果更贴近现实值。通过分析与仿真，验证了本模型具有抑制聚集信任攻击的有效性和健壮性，同时信任评估方法更具合理性和准确性。

关键词：D-S 证据理论；信任评估模型；基本概率分配函数；类概率函数

中图分类号：TP393 **文献标识码：**A **文章编号：**1000-436X(2013)07-0167-07

Trust evaluation model based on improved D-S evidence theory

ZHANG Lin[1,2,3], LIU Jing-wen[1], WANG Ru-chuan[1,2,3], WANG Hai-yan[1,2,3]

(1.College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; 2.Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China; 3. Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education Jiangsu Province, Nangjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: The existing trust evidence models cannot deal with malicious attacks in the distributed net quickly and effectively, and are lack of a trust normalization method that can measure relationship described by a triple set, so a trust model based on the improved D-S evidence theory was proposed. On this basis, basic trust value function based on continuous sequences and trust evaluation method based on evaluation function were also proposed to inhibit malicious nodes in a higher speed, and to enable the prediction results to be closer to the fact. Analysis and simulation show that this model has better effectiveness and robustness to deal th the aggregating trust attack, and trust evaluation method has better reasonableness and accuracy.

Key words: D-S evidence theory; trust evaluation model; basic probability assignment function; class probability function

1 引言

网络技术的出现和发展为全球资源的高效利用和共享提供了一个便利的环境。由于如今网络自身的异构、动态、开放、大范围共享资源的特性，使得资源提供者与资源使用者双方在进行作业交互时需要依据相互之间的信任关系，而信任关系的建立就是一个信任评估过程。因此，信任评估受到了国内外学者的广泛关注。

现有的信任评估模型根据其处理信任证据方

收稿日期：2012-07-02；**修回日期：**2012-09-03

基金项目：国家自然科学基金资助项目(61170065，61171053，61203217，61103195，61201163，61202354) ；**江苏省自然科学基金资助项目**(BK2011755，BK2011072，BK2012436)；**江苏省科技支撑计划(工业)基金资助项目**(BE2011189，BE2012183，BE2012755)；**省属高校自然科学研究重大基金资助项目**(12KJA520002)；**南京邮电大学科研基金资助项目**(NY212063)；**江苏高校优势学科建设工程基金资助项目**(yx002001)

Foundation Items: The National Natural Science Foundation of China (6117 5，61171053，61203217，61103195，61201163，61202354); The Natural Science Foundation of Jiangsu Province(BK2011755，BK2011072，BK2012436);Scientific & Technological Support Project (Industry) of Jiangsu Province(BE2011189、BE2012183、BE2012755); Natural Science Key Fund for Colleges and Universities in Jiangsu Province (12KJA520002); The Science Foundation of NJUPT (NY212063); The Priority Academic Program Development of Jiangsu Higher Education Institutions(yx002001)

式主要有基于贝叶斯[1,2]、基于云模型[3~5]和基于模糊数学[6,7]等的信任模型，这些都是根据某些客观数据统计形成的模型。其中，前两类模型用概率来表示信任的不确定性，但是必须要事先给出知识的先验概率或随机概率分布，而后一类模型用隶属函数解决信任的不确定性。由于 D-S 证据理论具有直接表达“不精确”和“不确定”的能力，并提供了基于不完备信息进行不确定性推理的方法，适合用于解决开放环境中不确定性信息计算问题，因此，基于 D-S 证据理论的信任模型近年来备受关注。但是，当前国内外学者提出的 D-S 信任证据模型仍然存在着以下问题。

1) 在基于 D-S 证据理论的信任模型中，选择适合的基本类概率分配(BPA)函数(在文献[8]中又被称为基本可信度函数)对信任评估的准确性有较大的影响。大多数信任证据模型[9,10]中提出的基本可信度函数都是基于古典概率的，忽略了不同信任证据对信任值有不同的影响；有些模型[11]为了抵御恶意节点的攻击在 BPA 函数中加入了时间衰减因子，而忽略了恶意节点的一个特性，即会持续提供不可信服务，因此相对而言，只考虑时间因子的模型抵御恶意节点的效率较低。

2) 现有的大多数信任证据模型都用三元信任关系组$\langle m\{T\}, m\{-T\}, m\{T,-T\}\rangle$定量或定性地表示信任。在文献[8,12]的定量模型中，通常用三元信任关系组中的基本信任函数$m\{T\}$或 D-S 理论的信任函数$bel\{T\}$表示信任值，而忽略了不可信分量和不确定分量对信任值的影响。在文献[11]的定性模型中，用粗略比较 2 个信任关系中每个分量增长的大小来判断哪个实体更可信，而忽略了不同分量对信任度的不同影响程度。

针对以上问题，本文提出了基于改进 D-S 证据理论的信任评估模型。该模型的基本可信度函数考虑了具有奖惩效果的持续序列，并且以 D-S 证据理论中评估函数为基础，提出了一种定量的信任归一化算法。

2 基于改进 D-S 证据理论的信任模型

在分布式网络中存在着很多节点，根据行为角色的不同将其分为评价主体（用户）、评价客体和用户代理（UA, user agent）帮助用户存储、更新和处理信任信息。当评价主体 i 对评价客体 j 进行信任评价时，UA 根据从本地证据库中获取的关于评价客体 j 的证据序列和推荐者集合中获取的间接信息计算出评价客体 j 的信任值。具体模型如图 1 所示。

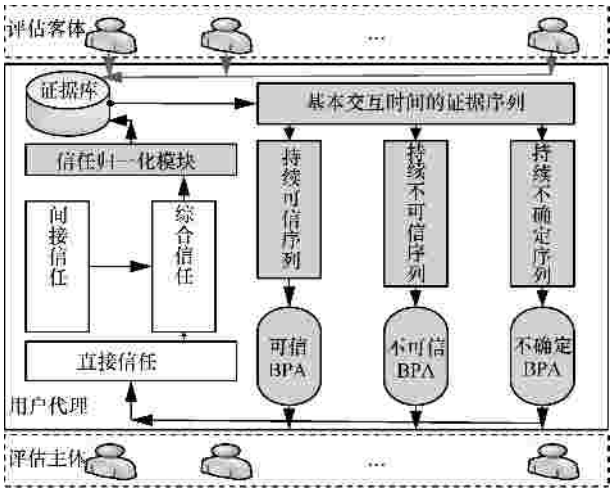

图 1 基于改进的 D-S 证据理论的信任模型

在图 1 的模型中，UA 可以从证据库中获得关于节点 j 的基于交互时间的证据序列，该证据序列按时间顺序记录了每次交互节点 j 提供的服务是否可信。根据该证据序列，通过持续序列提取算法，将其中连续可信服务、连续不可信服务和连续不确定服务的证据子序列取出，分别形成持续可信序列、持续不可信序列和持续不确定序列。

为了奖励持续提供真实可靠服务的节点并且惩罚恶意节点，本文利用已知的持续序列设计出具有奖惩效果的基本可信度函数。根据基本可信度函数计算出节点的直接信任。将直接信任和通过推荐者推荐得到的间接信任通过 D-S 证据理论合理地融合后，得到综合信任。由于 D-S 证据理论得到综合信任是一个三元组的形式，为了对信任值进行较为准确地评估，本文提出了一种基于评估函数的信任值归一化方法。

3 基于持续序列因子的基本可信度函数

在分布式网络中，存在着很多恶意节点，而信任模型的一个重要责任就是防止恶意服务的蔓延，这就要求它准确、及时地反映节点是否为恶意节点。因此，本文根据恶意节点的一个行为特征，即恶意节点会持续提供不可信服务，通过改进基本可信函数来提高抵制恶意节点的效率。所以本文提出了基于持续序列因子的基本可信度函数。

以下是持续序列因子的相关概念。由于基本可信度函数及其相关概念在文献[8]中已有提及，本文

不再赘述。

3.1　持续序列因子

用户 i 与实体 j 交互 n 次，且每次得到的服务质量为 $S_{ij}=\{S_{ij}^{t_1},S_{ij}^{t_2},\text{L},S_{ij}^{t_n}\}$。第 k 次交互的服务质量为 $S_{ij}^{t_k}$，其中，$1\le k\le n$，并采用可信门限值 a_i 和 b_i，满足 $0\le a_i\le b_i\le 1$。当 $b_i\le S_{ij}^{t_k}\le 1$ 时，这次服务为可信服务 $\{T\}$；当 $0\le S_{ij}^{t_k}\le a_i$ 时，服务为不可信服务 $\{-T\}$；否则，为不确定服务 $\{T,-T\}$。

定义 1　基于交互时间的证据序列是从证据库中得到的按时间排列的关于服务的质量序列，表示为 $S_{ij}=\{s_{ij}^{t_1},s_{ij}^{t_2},\text{L},s_{ij}^{t_n}\}$，并且 $0\le n\le H$，H 描述了用户代理最多存储的关于服务 j 的证据序列长度。

定义 2　持续可信（不可信/不确定）服务子序列是从基于交互时间的证据序列中获取的包含一个或一个以上可信（不可信/不确定）服务的序列。

$$CTS_{ij}=\left\{\begin{array}{l} ts_{t_{a_1}}^{t_{a_1+length_1-1}}(length_1)_{ij},ts_{t_{a_2}}^{t_{a_2+length_2-1}}(length_2)_{ij},\\ \ldots,ts_{t_{a_m}}^{t_{a_m+length_m-1}}(length_m)_{ij} \end{array}\right\}$$

上式表示若干持续可信子序列组成的持续可信序列，且 $1\le length\le n$。其中，$ts_{t_{a_k}}^{t_{a_k+length_k-1}}(length_k)_{ij}$ 表示第 k 个持续可信服务子序列，且 t_{a_k} 和 $t_{a_k+length_k-1}$ 分别表示该子序列中第一个服务的时间与最后一个服务的时间。持续不可信服务序列和子序列分别用 CFS_{ij} 和 $fs_{t_{b_k}}^{t_{b_k+length_k-1}}(lenght_k)_{ij}$ 表示，并且持续不确定序列和子序列为 CPS_{ij} 和 $ps_{t_{g_k}}^{t_{g_k+length_k-1}}(lenght_k)_{ij}$。

本文从证据序列中提取持续服务可信子序列，持续不可信子序列和持续不确定子序列提取算法相似。以下是持续服务成功子序列提取算法。

输入：$\{s_1,s_2,\ldots,s_n\}$

输出：若干持续可信子序列

```
while(1≤i≤n)
//i 表示 s 的下标；n 表示服务总次数
{
if (rf[i] ==服务可信)
{
/*创建一个新的序列，用来存储持续服务可信子序列*/
new vector ts;
for ( j = i; j < n; j++)
    {
//将符合质量的服务添加到子序列
if ( s[ j] = =服务可信)
            ts . Add( s[ j] );
        else
            { i = j ;break;}
    }
 }
else i++;
//输出若干持续服务可信子序列
ts . output;
}
```

3.2　改进的基本可信度函数

根据社会学原理，人们更相信与自己有持续可信交互的对象，而不愿相信持续不可信的对象，并且对行为不稳定的对象也没有好感。例如，在 2 个球队具有相同胜率的时候，人们更愿意相信一个连续获胜的球队而不愿意相信连续失败或胜利失败间隔产生的球队。因此，本文针对这种情况，提出了基于基本可信度函数的直接信任。

由于用户更相信距离当前时间较近的持续序列以及长度较长的持续序列，所以在计算信任值时，必须考虑时间及持续序列长度(即持续可信服务数量)对信任的影响。为了防止恶意节点的攻击，并激励节点持续提供真实可靠的服务，用以下函数将时间和持续可信服务的数量映射到可信 BPA 函数中。

$$\left\{\begin{array}{l} m\{T\}_{ij}=\dfrac{\sum_{k=1}^{m}fade_{k,ts}\times length_{k,ts}}{N}\\ fade_{k,ts}=r^{\,t-t_{a_k+length_k-1}} \end{array}\right. \tag{1}$$

其中，$fade_{k,ts}$ 为第 k 个持续可信子序列的基于时间和序列的衰减函数，并且 $fade_{k,ts}$ 中的 $0<r<1$。当序列为持续可信子序列时，将子序列中距离当前时间 t 最近的最后一次服务时间 $t_{a+length-1}$ 作为该子序列的衰减时间。这样奖励了持续可信服务次数多的服务，并且激励了服务持续与用户交互可信，其中，N 为基于时间和持续序列的总服务次数。

有预谋的恶意节点一般有以下特点：节点提供服务的质量多次变换，更有可能出现持续不可信服务序列或持续不确定服务序列。针对该类恶意节点，如式(2)所示的不可信 BPA 函数利用时间衰减函数的倒数和持续不可信服务长度来惩罚持续不可信服务和多次变换可信度服务。

$$m\{-T\}_{ij}=\frac{\sum_{k=1}^{z}1/\sqrt{fade_{k,fs}\times punish}\times length_{k,fs}}{N} \quad (2)$$

其中，$fade_{k,fs}$ 为第 k 个持续不可信服务子序列的基于时间和序列的衰减因子，$length_{k,fs}$ 为第 k 个持续不可信服务子序列的长度，$punish$ 为基于可信间断点的惩罚因子。

$$fade_{k,fs}=r^{\,t-t_{b_k}} \quad (3)$$

其中，$fade_{k,fs}$ 衰减因子具有对服务不可信行为的惩罚作用，体现为在衰减时，将子序列中距离当前时间 t 最远的第一次服务时间 t_{b_k} 作为该子序列的衰减时间。

另外，除了衰减因子对恶意行为的惩罚外，还有一个惩罚因子 $punish$ 也具有惩罚作用，有

$$punish=\frac{v\ \tan(c_j-v\ )+v\ \tan v}{\mathrm{p}/2+v\ \tan v} \quad (4)$$

其中，c_j 为服务 j 从服务可信变换为服务非可信（包括服务不确定及服务不可信）的概率，v 是一个控制惩罚因子速度的参数，并且 v 可以根据用户对恶意节点的容忍度来适当调节，来区分善意失误节点和恶意节点。当 c_j 大于 v 时，惩罚因子 $punish$ 增长较快，惩罚力度越大；反之，则其增长较慢。

$$c_j=\begin{cases}(m-1)/n, & \text{当} t_n=t_{a_m+length_m-1}\text{，且} length_m\geq 2\text{时}\\ m/n, & \text{否则}\end{cases} \quad (5)$$

m 为持续可信子序列的个数，n 为证据序列的长度。

为了惩罚持续不确定服务，本文关于不确定 BPA 函数为

$$m\{T,-T\}_{ij}=\frac{\sum_{k=1}^{n-m-z}1/\ fade_{k,ps}\times length_{k,ps}}{N} \quad (6)$$

其中，衰减函数 $fade_{k,ps}$ 与式(3)相似。

上文中提及的基于时间和持续序列的总服务次数，又称为积极服务数量 N 为

$$N=\sum_{k=1}^{m}fade_{k,ts}\times length_{k,ts}+\sum_{k=1}^{z}1/\sqrt{fade_{k,fs}\times punish}\times length_{k,fs}+\sum_{k=1}^{n-m-z}1/\ fade_{k,ps}\times length_{k,ps} \quad (7)$$

因此，本文提出的基于持续序列的基本可信度函数通过持续可信序列来奖励节点持续提供真实可信的服务，并且通过持续不可信（不确定）序列和时间衰减函数惩罚节点的恶意行为或不确定行为。

4 基于评估函数的信任值归一化算法

在以往的证据模型中，信任关系是用一个三元组来表示，但对信任度的归一化方法很少涉及，即使提及也仅仅是将其 BPA 函数中关于可信部分的分配函数值作为信任值而忽略不可信部分[8]，或者考虑到不可信部分但是只是定性地给出节点是否可信，而忽略可信的程度[11]。本文针对以上问题，提出了一种基于评估函数的信任值归一化方法。

4.1 信任值计算方法

信任值的归一化算法是评估模型之后的一步工作，以便评估结果更加可观。在这之前必须计算出节点的综合信任值，本文基于 3.2 节提出的改进基本可信度函数可以计算出实体 i 对实体 j 的直接信任度：$DT_{ij}=\langle DT_{ij}\_m\{T\},DT_{ij}\_m\{-T\},DT_{ij}\_m\{T,-T\}\rangle$，并基于项目组前期的工作[13]得到间接信任度为 $IT_{ij}=\langle IT_{ij}\_m\{T\},IT_{ij}\_m\{-T\},IT_{ij}\_m\{T,-T\}\rangle$。

最后用 D-S 证据理论将直接信任值和间接信任值融合可得综合信任值为 $T_{ij}=<m\{T\},m\{-T\},m\{T,-T\}>$。

4.2 D-S 证据理论相关知识

在 D-S 证据理论中，利用信任函数和似然函数得到的类概率函数，既可以将它作为知识的非精确性度量，又可以描绘出知识的估计信任度。因此，本文以下部分称其为评估函数。其定义和性质[14]如下。

定义 3 (评估函数) 设 $X=\{t_1,t_2,\mathrm{L},t_n\}$ 为有限识别框架，对任何命题 $A\subseteq X$，命题 A 的评估函数为

$$f(A)=Bel(A)+\frac{|A|}{|X|}\times[Pl(A)-Bel(A)] \quad (8)$$

其中，$Bel(A)$ 表示为对命题 A 为真的信任度，$Pl(A)$ 表示为对命题 A 非假信任度，而 $Pl(A)-Bel(A)$ 为对命题 A 的不确定程度。$|A|$ 和 $|X|$ 分别表示 A 和 X 中元素的个数。

性质（评估函数的性质） 评估函数有以下性质，在文献[14]中给出了相关证明。

1) $\sum_{i=1}^{n}f(\{t_i\})=1$；

2) 对任何 $A \subseteq X$，有 $Bel(A) \le f(A) \le Pl(A)$；

3) 对任何 $A \subseteq X$，有 $f(-A) = 1 - f(A)$。

推论 (评估函数的推论) 在 D-S 证据理论中，利用信任函数和似然函数的数学性质和关系，容易得到关于评估函数的如下推论。

1) $f(f) = 0$；

2) $f(X) = 1$；

3) 对任何 $A \subseteq X$，有 $0 \le f(A) \le 1$。

4.3 基于评估函数的信任归一化算法

由评估函数性质及推论可知，评估函数既表现出信任证据中的可信部分，又体现了不可信部分，本文将评估函数作为信任值归一化的数学工具。

已知本模型的知识框架为 $X = \{T, -T\}$，表示综合信任关系的三元组为 $\langle m\{T\}, m\{-T\}, m\{T,-T\}\rangle$。因为“不知道 $\{T,-T\}$”部分只可能是知识框架中出现的事件，所以当将属于 $\{T,-T\}$ 的基本可信度值分配给可信事件和不可信事件时，应该基于可信事件和不可信事件发生的概率分配权值。因此，归一化后的综合评估信任值为

$$f'_{ij}(\{T\}) = \frac{p(\{T\})}{P(\{T\}) + P(\{-T\})}[Pl_{ij}(\{T\}) - Bel_{ij}(\{T\})] + Bel_{ij}(\{T\}) \tag{9}$$

其中，$\{T\}$ 为服务可信集合。由式(9)可知，可信事件发生的概率越大，越容易得到不知道集合的认同，那么分配给它的基本概率分配值就越大。

如上文所述，有可信门限值 a_i 和 b_i，满足 $0 \le a_i \le b_i \le 1$。当 $b_i \le s_{ij}^{t_k} \le 1$ 时，这次服务为可信服务 $\{T\}$；当 $0 \le s_{ij}^{t_k} \le a_i$ 为时，服务为不可信服务 $\{-T\}$；否则，为不确定服务 $\{T,-T\}$。因此，在本模型中可信事件的概率应该以几何概率模型来计算，其计算公式为

$$p(\{T\}) = \frac{1 - b_i}{1 - b_i + a_i} \tag{10}$$

从式(9)、式(10)可以看出改进后的评估函数仍然符合评估函数的性质，这样将评估值 $f'_{ij}(\{T\})$ 当作三元组 $\langle m\{T\}, m\{-T\}, m\{T,-T\}\rangle$ 归一化后的信任值，既考虑了可信、不可信、不确定的情况，又考虑其权重问题，所以评估后的信任值较以往模型更贴近真实值。

5 仿真实验分析

本文通过实验来评价新模型抵御恶意攻击的能力，为了方便比较，同时实现了文献[8]和文献[11]中的信任证据模型。

5.1 针对防恶意攻击能力的仿真

有一种恶意攻击节点会为了吸引用户而有目的地将其伪装为可信服务节点，以取得用户的信任，当其可信值积累到较高时，就会对用户进行恶意攻击。为了考察本模型对这种攻击的敏感程度，本模型与文献[8]和文献[11]中的模型分别进行了比较。前者是利用事件概率作为基本可信度函数，而后者是基于时间衰减函数的。

实验设计了一个欺骗节点，模拟了它的 2 种攻击行为：1)该欺骗节点先建立信任值，再进行恶意攻击；2)恶意节点在建立信任值和恶意攻击之间振荡。

针对前者，3 种模型共同的实验场景为：该恶意节点与用户进行了 10 次交互，前 3 次均为可信交互，后 7 次均为不可信交互。参数设置如下：$H = 20$，$r = 0.8$，$v = 0.5$，且 $a_i = b_i$，则 3 种模型对滥用信任的敏感程度如图 2 所示。

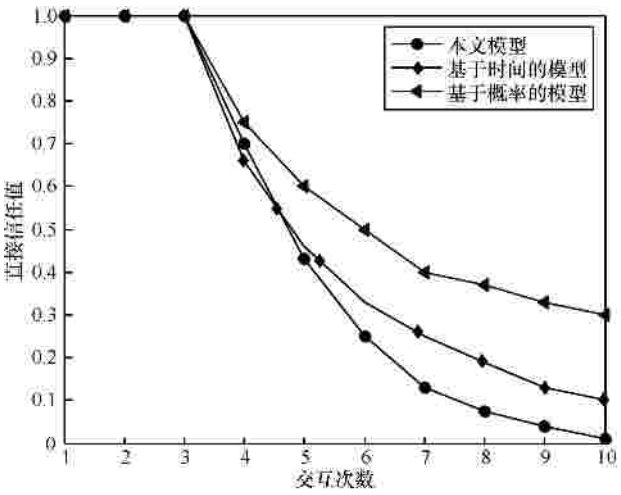

图 2　针对第 1 种行为的实验分析

图 2 显示了当恶意节点通过一段时间的成功交互并积累一定的信任评价后，进行不合作时信任值的变化曲线。如图所示，这 3 种模型最终都导致信任值的降低，本文提出的基于持续序列因子的基本分配函数的 D-S 信任证据模型对节点行为的改变更加敏感，当节点改变合作行为时，信任值迅速下降，能够更快地检测出节点的恶意行为。

针对后一种行为，3 种模型共同的实验场景为：

该恶意节点与用户进行了 10 个交互次数，前 3 次均为可信交互，后 7 次出现间歇式不可信交互，参数与上相同。则 3 种模型对振荡信任的敏感程度如图 3 所示。

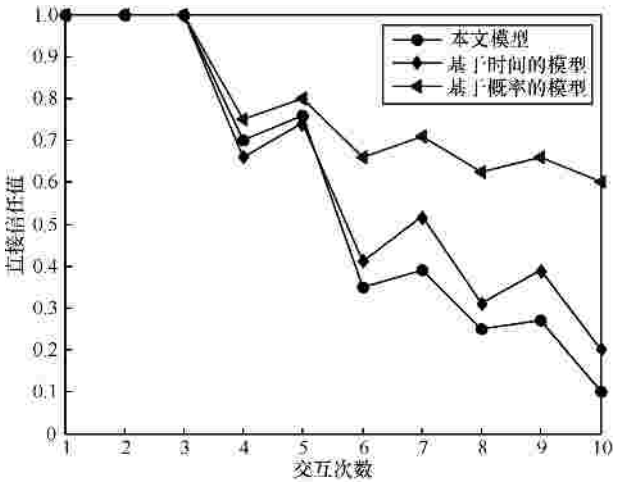

图 3 针对第 2 种行为的实验分析

图 3 显示了当恶意节点在建立和滥用声誉之间摇摆时，一个评价主体对聚集信任攻击节点的信任值变化曲线。同样，本文模型能够迅速发现节点的恶意行为，并延迟恢复信用值。

5.2 节点信任值的动态变化分析

为分析不同类型节点的综合信任值的动态变化，本文对长期诚实节点、长期欺骗节点、偶尔失误善意节点和动荡欺骗恶意节点这 4 种节点的信任值随其行为动态变化进行分析和研究。

假设长期诚实节点在本实验中的 10 次交互没有欺骗行为；长期欺骗节点在首次诚实交互后一直进行欺骗；偶尔失误善意节点只在第 2、第 6 次存在欺骗行为；动荡欺骗恶意节点每隔一次诚实服务都会再次欺骗。在该实验中 $H=20$，$r=0.8$，$v=0.5$，且 $a_i=b_i$，则 3 种节点欺骗行为的持续性对信任值的动态变化如图 4 所示。

从图 4 中可以看出，在交互初期，各种节点的可信度相差不大，但是随着欺骗行为的发生，根据各欺骗行为连续程度不同，其信任值也出现不同程度的变化。其中，长期诚实节点的直接信任由于持续诚实交互而一直维持在 1；长期欺骗节点随着恶意欺骗的持续增加其信任值迅速减少；偶尔失误善意节点的信任值变化虽然同动荡欺骗恶意节点的信任值曲线一样呈锯齿状但是偶尔失误节点整体变化是呈上升趋势而非恶意节点的下降趋势。因此，该模型可以根据节点的恶意欺骗行为特征体现在信任值的动态变化，并且可以较为清晰地显示出善意偶尔欺骗节点与恶意节点之间的区别。

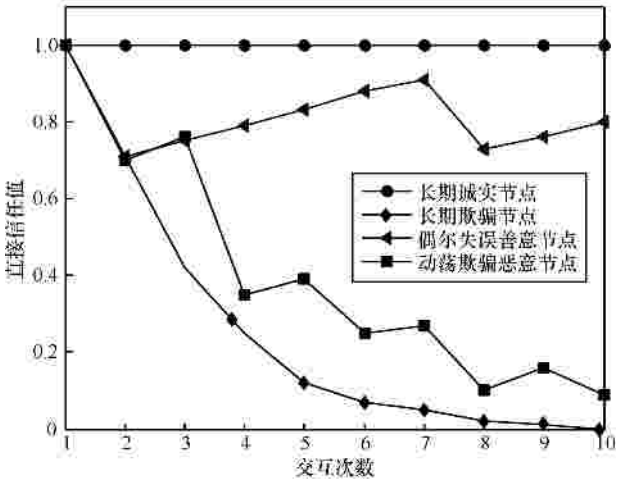

图 4 节点随节点行为特点动态变化的实验分析

6 结束语

基于 Dempster-Shafer 证据理论的基本概率分配函数和类概率函数，本文提出了一种基于改进 D-S 证据理论的信任评估模型。本文考虑了持续序列对诚实节点持续提供真实可信服务的奖励作用和对恶意节点连续恶意行为的惩罚作用，并将持续序列引入到可信度评估的基本概率分配函数中，从而使得新方案的可信度较准确地反映了节点的行为方式，并且为更准确地度量信任值，本文提出了基于改进评估函数的信任评估方法。最后，通过仿真实验分析了新方案对可信度的评估效果。

将来的工作是使本文能够有效地抵制多种恶意攻击，进一步讨论相关方法，同时研究更加实用和灵活的可信度评估模型，比如在保护推荐信息提供者的私有数据不会泄漏的条件下实现可信度评估的保护隐私的可信度评估模型以及在较小的计算复杂度下实现高效的恶意节点抵御功能等。

参考文献：

[1] DENKO M K, SUN T, WOUNGANG I. Trust management in ubiquitous computing: a Bayesian approach[J]. Computer Communications, 2011, 34(3):398-406.

[2] 孙玉星, 黄松华, 陈力军等. 基于贝叶斯决策的自组网推荐信任度修正模型[J]. 软件学报, 2009, 20(9):2574-2586.
SUN Y X, HUANG S H, CHEN L J, *et al*. Bayesian decision-making based recommendation trust revision model in ad hoc networks[J]. Journal of Software, 2009, 20(9):2574-2586.

[3] CAI H Y, LI Z, TIAN J F. A new trust evaluation model based on cloud theory in e-commerce environment[A]. Proceedings of the 2011

2nd International Symposium on Intelligence Information Processing and Trusted Computing[C]. 2011.139-142.

[4] **黄海生，王汝传. 基于隶属云理论的主观信任评估模型研究**[J]. **通信学报**, 2008, 29(4):13-19.
HUANG H S, WANG R C. Subjective trust evaluation model ba d on membership cloud theory[J]. Journal on Communication, 2008, 29(4): 13-19.

[5] **李致远，王汝传**. P2P **电子商务环境下的动态安全信任管理模型**[J]. **通信学报**, 2011, 32(3):50-59.
LI Z Y, WANG R C. Dynamic secure trust management model for P2P e-commerce environments[J]. Journal on Communications, 2011, 32(3): 50-59.

[6] MA S N, HE J S, GAO F. A trust quantification method based on grey fuzzy theory[A]. International Conference on Security of Information and Networks[C]. 2010.27-31.

[7] **陈超，王汝传，张琳. 一种基于开放式网络环境的模糊主观信任模型研究**[J]. **电子学报**, 2010, 38(11):2505-2509.
CHEN C, WANG R C, ZHANG L. The research of subjective ust model based on fuzzy theory in open networks[J]. Acta lectronica Sinica, 2010, 38(11):2505-2509.

[8] **朱友文，黄刘生，陈国良等. 分布式计算环境下的动态可信度评估模型**[J]. **计算机学报**, 2011, 34(1):55-64.
ZHU Y W, HUANG L S, CHEN G L, *et al*. Dynamic trust evaluation model under distributed computing environment[J]. Chinese Journal of Computers, 2011, 34(1):55-64.

[9] **蒋黎明，张宏，张琨. 开放系统中一种基于模糊修正的证据信任模型**[J]. **电子与信息学报**, 2011, 33(8):1930-1936.
JIANG L M, ZHANG H, ZHANG K. An evidential trust model with fuzzy adjustment method for open systems[J]. Journal of Electronics & Information Technology, 2011, 33(8):1930-1936.

[10] **杨凯，马建峰，杨超. 无线网状网中基于** D-S **证据理论的可信路由**[J]. **通信学报**, 2011, 32(5):89-96.
YANG K, MA J F, YANG C. Trusted routing based on D-S evidence theory in wireless mesh network[J]. Journal on Communications, 2011, 32(5):89-96.

[11] **田春岐，邹仕洪，王文东. 一种新的基于改进型** D-S **证据理论的** P2P **信任模型**[J]. **电子与信息学报**, 2008, 30(6):1480-1484.
TIAN C Q, ZOU S H, WANG W D. A new trust model based on advanced D-S evidence theory for P2P networks[J]. Journal of Electronics & Information Technology, 2008, 30(6):1480-1484.

[12] JIANG L, XU J, ZHANG K. A new evidential trust model for open distributed systems[A]. Expert Systems with Applications[C]. 2012. 3772-3782.

[13] **张琳，王汝传，张永平. 一种基于模糊集合的可用于网格环境的信任评估模型**[J]. **电子学报**, 2008, 36(5):862-868.
ZHANG L, WANG R C, ZHANG Y P. A trust evaluation model based on fuzzy set for grid environment[J]. Acta Electronica Sinica, 2008, 36(5):862-868.

[14] **王万森. 人工智能原理及其应用**[M]. **北京: 电子工业出版社**, 2006.
WANG W S. Artificial Intelligence Principle and Application[M]. Beijing: Electronic Industry Press, 2006.

作者简介:

张琳（1980-），女，江苏丰县人，博士后，南京邮电大学副教授、硕士生导师，主要研究方向为网格计算、网络安全、信任、可信计算等。

刘婧文（1989-），女，江苏连云港人，南京邮电大学硕士生，主要研究方向为服务计算、信息安全、信任、可信计算等。

王汝传（1943-），男，安徽合肥人，南京邮电大学教授、博士生导师，主要研究方向为计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

王海艳（1974-），女，江苏盐城人，南京邮电大学教授、硕士生导师，主要研究方向为信息安全、计算机软件、可信计算等。

（上接第 166 **页）**

[20] CAO J, WU Z A, WU J J, *et al*. SAIL: summation-based incremental learning for information-theoretic text clustering[J]. IEEE Trans on Cybernetics, 2013, 43(2):570-584.

[21] WU J J, XIONG H, CHEN J. COG: local decomposition for rare class analysis[J]. Data Mining and Knowledge Discovery, 2010, 20(2): 191-220.

作者简介：

刘文杰（1988-），男，湖北黄石人，南京大学硕士生，主要研究方向为数据挖掘、多媒体技术。

伍之昂[通信作者]（1982-），男，江苏宜兴人，博士，南京财经大学副教授，主要研究方向为网络计算、数据挖掘和推荐系统。E-mail: zawuster@gmail.com。

曹杰（1969-），男，江苏姜堰人，博士，南京财经大学教授、博士生导师，主要研究方向为商务智能和数据挖掘。

潘金贵（1952-），男，江苏南京人，博士，南京大学教授、博士生导师，主要研究方向为多媒体技术。