doi:10.3969/j.issn.1000-436x.2013.z1.005

云计算环境下基于评价可信度的动态信任评估模型

张琳[1,2,3]，饶凯莉[1]，王汝传[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：针对云用户如何选取可信的云服务提供商问题，提出了基于评价可信度的动态信任评估模型。该模型将云服务提供商的服务能力和云用户所需求的服务能力分别划分等级，有效地解决了云服务提供商服务能力动态变化对模型存在的潜在破坏问题。建立了信任度随时间窗变化的动态信任机制，在计算信誉度时，将用户的评价可信度作为其评价证据的可信权重，通过引入评价可信度和评价相似度提高了计算推荐行为可信度的准确率。仿真结果表明，该模型的评估结果更贴近云服务提供商的真实信任度，同时能有效抵御恶意云用户的攻击。

关键词：服务等级；时间窗；评价可信度；推荐可信度

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0031-07

Dynamic trust evaluation model based on evaluation credibility in cloud computing

ZHANG Lin[1,2,3], RAO Kai-li[1], WANG Ru-chuan[1,2,3]

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

Abstract: Considering the problem that cloud users will select a trusted cloud service provider, a dynamic trust evaluation model based on evaluation credibility was proposed.This model divides the ability of cloud service provider and the one of the user's requirments into many ranks, which can effectively solve the potential damage caused by the dynamic change in the ability of cloud service providers. A dynamic mechanism of trust changing about time-window was established. During the calculation of credibility, the user's evaluation credibility was used as the trust weight. The calculating accuracy of the recommended behavior credibility was improved by introducing the evaluation credibility and evaluation similarity. Simulation results show that the model results are closer to the cloud service provider's actual trust value, and can resist the attack of malicious cloud users effectively.

Key words: service rank; time-window; evaluation credibility; recommendation credibility

---

收稿日期：2013-06-26

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)；省属高校自然科学基金资助项目（13KJB520017）；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 (61170065, 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); The Natural Science Key Fund for Colleges and Universities of Jiangsu Province (12KJA520002); The Natural Science Fund for Colleges and Universities of Jiangsu Province(13KJB520017); The Science Foundation of Nanjing University of Posts and Telecommunications (NY212063); The Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions(PAPD) (yx002001)

1 引言

随着计算资源、软件资源、存储资源的融合，一种体现了“网络就是计算机”思想的新型计算模式——云计算应运而生[1]。云计算作为一种新资源使用，改变了服务的模式，但是却未颠覆传统的安全形式，云用户该怎样权衡云服务提供商的可靠性，以及如何从不断涌现出的云服务提供商中选择可靠的服务，引发了云用户对云服务提供商的信任问题。因此，面向云计算的信任模型的研究逐渐被提到日程上来，成为云计算安全机制领域中的研究热点。

目前，国内外学者已经基于不同的方法和数学工具提出了适应于各种网络环境下的多种信任模型。文献[2]基于模糊集合理论提出了一种可用于网格环境的信任评估模型，通过引入中间推荐节点的直接交互经验，体现出主观因素的重要性。文献[3]在信任云的基础上，提出了一种基于云模型的主观信任模型，通过信任变化云来刻画信任客体信任度的变化情况，对主观信任评价的研究起到了一定的推动作用。文献[4]在上下文感知的基础上提出一种CAT信任模型，该模型将上下文相似度和信任规则概念引入到直接信任值的计算中，使得直接信任值的计算更加精确。在推荐信任度的计算中过滤恶意和不可靠的推荐行为，确保推荐的准确性和可靠性。文献[5]提出了一种基于交互感知的动态自适应的信任评估模型，该模型引入了历史交互窗口、可信推荐数、实体熟悉度、评分相似度等概念，有效地克服了传统模型对交互证据感知不足的缺陷，提高了推荐的准确率，并有效地抵御了共谋实体的协同作弊。文献[6]提出了一种面向大规模P2P的全面和自适应的信任模型，该模型通过引入历史证据窗口（HEW），不仅减少风险、提高系统效率，同时也解决信任预测时直接证据不足的问题。在权重分配方面，通过引入置信因子和反馈因子动态地进行分配，克服了传统模型通过主观思想分配权重的不足。文献[7]提出了一种面向普适计算模型（FTM），本模型引入路径衰减方法和多级推荐协议进行推荐信任度的计算。

但现有模型仍存在一些问题。

1) 现有模型没有考虑到不同服务实体所能提供的服务能力是不同的，同时由于受到内外在因素的影响及其所具有的服务能力是动态变化的，因此可能出现要求很高的用户选择了信任度很高但服务能力很低的服务实体，不仅影响了服务实体交易信任度的计算，同时用户也没有得到期望的服务。

2) 虽然现有模型大多引入时间衰减函数[8]，解决了信任度随时间动态性变化的问题，但却没有考虑到信任度计算的时效性。

3) 有些模型对评价可信度不同的用户评价时，不加区分地计入信誉度的计算，没有考虑到用户实体的评价可信度对计算服务实体信誉度的影响,无法有效抵御恶意用户实体对信任模型的攻击。同时，也没有考虑评价可信度对推荐行为可信度的影响。

针对以上问题，本文将服务实体的服务能力和云用户所需求的服务能力进行等级划分；引入时间窗来控制信任度计算的时效性；同时通过计算用户的评价可信度来遏制恶意用户对信任度计算的影响。

2 基于评价可信度的信任评估模型

2.1 模型的相关定义

定义 1 设 $c_1,c_2,\cdots,c_n$ 为云计算应用系统中的 n 个用户实体，组成用户实体集合 $SC=\{c_1,c_2,\cdots,c_n\}$；$s_1,s_2,\cdots,s_m$ 为云计算应用系统中 m 个服务实体，组成服务提供实体集合 $SP=\{s_1,s_2,\cdots,s_n\}$，并且 $SP\cap SC=\varnothing$。

定义 2 设有 p 项服务属性度量指标，其集合表示为 $MR=\{Mr_1,Mr_2,\cdots,Mr_p\}$,其中，$Mr_i$ 表示服务效率、安全性、可维护性等服务属性度量指标。$Q_{s_j}^{t_k}(s_j,t_k)$ 表示服务实体 s_j 在 t_k 时刻宣称的自己所能提供的服务属性度量指标的质量集合，$Q_{s_j}^{t_k}(s_j,t_k)=\{Q_{s_j,Mr_1}^{t_k},\cdots,Q_{s_j,Mr_p}^{t_k}\}$，其中，$Q_{s_j,Mr_i}^{t_k}$ 表示服务实体 s_j 在 t_k 时刻宣称的关于第 i 个度量指标 Mr_i 的质量，并且 $0\leqslant Q_{s_j,Mr_1}^{t_k},\cdots,Q_{s_j,Mr_p}^{t_k}\leqslant 1$。为了便于等级划分，令 Cap_{s_j} 为综合能力，则

$$Cap_{s_j}=\sum_{i=1}^{p}w_iQ_{s_j,Mr_i} \tag{1}$$

其中，$w_1,w_2,\cdots,w_p$ 是服务属性度量指标的权重因子，满足 $\forall w_i\in(0,1),\sum_{i=1}^{p}w_i=1$。

对于特定的用户请求，在计算时重新设定 $w_1,w_2,\cdots,w_p$ 的值，使得用户偏好的相应服务属性度量指标权重因子相对较大。

本文根据 Cap_{s_j} 将服务实体集合 SP 划分成4个等级，相应 4 个等级集合为 $SP_1,\cdots,SP_4$。等级区间定义为[0,1]，划分方法如图 1 所示。

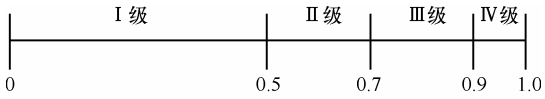

图 1　服务能力等级

定义 3　设 $CT_{c_i,s_j}^{t_r}$ 表示用户实体 c_i 在 t_r 时刻对服务实体 s_j 的综合信任度，令

$$CT_{c_i,s_j}^{t_r} = \omega_1 T_{c_i,s_j}^{t_r} + \omega_2 TD_{s_j}^{t_r} + \omega_3 RT_{c_i,s_j}^{t_r} \tag{2}$$

综合信任度的计算，涉及到 3 个信任度：用户实体根据与服务实体进行交互得到的直接交易信任度 T_{c_i,s_j}、所有与服务实体进行交易的用户实体对此服务实体的直接交易信任度聚合产生的信誉度 TD_{s_j} 和推荐用户实体的推荐信任度 RT_{c_i,s_j}。其中，ω_i（$i=1,2,3$）值的确定是动态变化的，随着交易次数 n_1 的增加，直接交易信任度权重 ω_1 越大；与其进行交易的用户数 n_2 越多，全局交易信任度权重 ω_2 也越大；同样，推荐用户数 n_3 越多，推荐信任度权重 ω_3 也越大。则

$$\omega_i = \frac{n_i}{n_1 + n_2 + n_3} \tag{3}$$

2.2　模型的架构图

云计算应用系统中存在 2 类实体：云用户实体和云服务实体。用户实体在可选服务实体等级集合中选择一个服务实体，并向信任评估中心请求此服务实体综合信任度，如若不小于信任度阈值，则选择此服务实体进行交互，反之，则重新选择另一个实体进行评估。交互完成后对服务实体提供的服务能力进行评价，随后评估中心更新相关信任度的信息。具体模型如图 2 所示。

针对 SP，涉及到 2 方面：所能提供的服务能力和提供服务的可信性。不同的服务实体所能提供的服务能力是不同的，或者由于受到内外在因素的影响，服务实体的服务能力是动态变化的，如果要求高的用户选择提供服务能力低的 SP，势必会导致此 SP 的信任度下降。所以应将 SP 的服务能力和 SC 的要求进行等级划分，确保 SC 在不小于自己等级的服务集合中进行服务选择，即等级低的 SC 可以向等级高的 SP 请求服务，但是等级高的 SC 不可以向等级低的 SP 请求服务。这样对双方都有一定的益处，SC 可以快速地选择合理的服务提供商，同时服务提供商不会受到恶意用户的攻击。为了防止服务提供商刻意夸大自己的服务能力，吸引更多的用户，本文采用一定的惩罚措施迫使服务提供商正确宣称自己所能提供的服务能力。具体流程如图 3 所示。

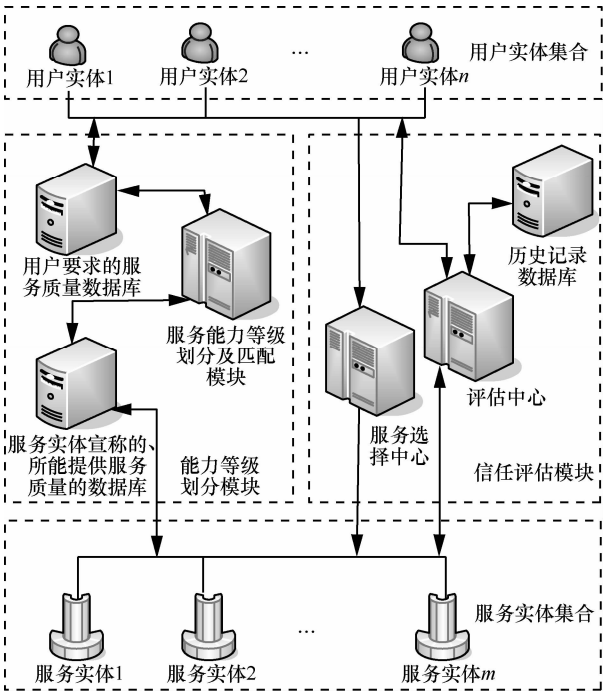

图 2　模型的架构

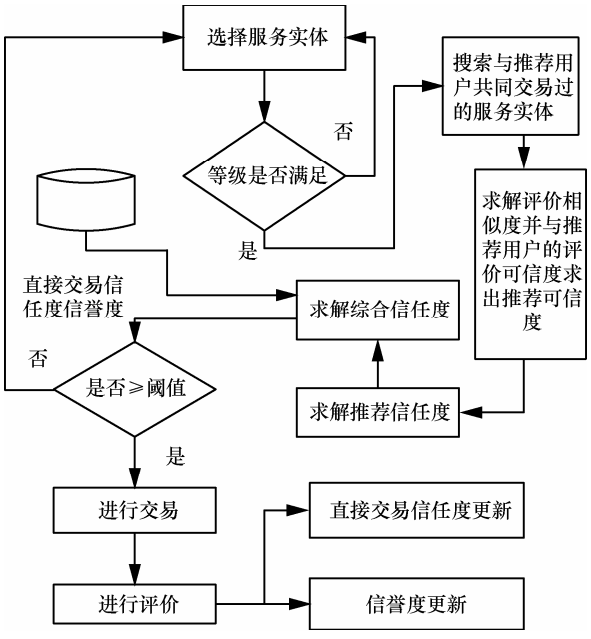

图 3　模型的工作流程

Step1　新加入云系统的服务提供商 s_i 会宣称自己所能提供的服务能力为 Q_{s_i}，能力等级划分中心会根据 Q_{s_i} 计算出 Cap_{s_i}，然后根据 Cap_{s_i} 将 s_i 划分到相应的等级集合中，s_i 根据今后的交易情况不断更新信任值，同时允许 s_i 根据自身的情况改变自己所

宣称的服务能力 Q_{s_i}，能力等级划分中心会根据 Q_{s_i} 的改变将 s_i 重新划分到相应的等级集合中。

Step2 用户 c_i 在提出服务请求前，会宣称自己的服务要求等级，进行服务选择时只能从不小于自己等级的等级服务集合中选择服务。为了防止恶意用户宣称虚假的服务请求等级，规定等级越高的服务，交易额就越高。信任评估中心向用户实体 c_i 提供直接交易信任度 T_{c_i,s_j}、信誉度 TD_{s_j} 和推荐信任度 RT_{c_i,s_j}，根据最终得到的综合信任度与用户 c_i 的信任度阈值进行比较，决定是否接受选择的 s_j 进行交易。

Step3 交易完成后，用户实体 c_i 根据服务提供者提供的服务能力给出评价，与服务提供者 s_j 宣称的服务能力进行比较，信任评估中心根据交易信任度计算公式对直接交易信任度和信誉度进行更新。同时计算出此时用户实体的评价可信度。

2.3 直接交易信任度计算模块

定义 4 设 $Q_{c_i\to s_j}^{t_k}(c_i,s_j,t_k)$ 表示用户实体 c_i 在 t_k 时刻接收到的服务实体 s_j 提供的服务属性度量指标的质量集合，t_k 表示第 k 次交易的时间，且 $Q_{c_i\to s_j}^{t_k}(c_i,s_j,t_k)=\{Q_{c_i\to s_j,Mr_1}^{t_k},\cdots,Q_{c_i\to s_j,Mr_p}^{t_k}\}$，其中，$Q_{c_i\to s_j,Mr_t}^{t_k}$ 表示用户实体 c_i 在 t_k 时刻接收到的服务实体 s_j 提供的第 t 个度量指标 Mr_t 的服务质量，并且 $0\leqslant Q_{c_i\to s_j,Mr_1}^{t_k},\cdots,Q_{c_i\to s_j,Mr_p}^{t_k}\leqslant 1$。

定义 5 交易满意度。用户实体 c_i 根据服务实体 s_j 提供给自己的服务能力与 s_j 自己宣称的服务能力进行比较，根据两者的差值计算满意度。用 $\eta(c_i,s_j,t_k)$ 表示用户实体 c_i 对服务实体 s_j 在 t_k 时刻提供服务能力的满意度，则

$$\eta(c_i,s_j,t_k)=\sum_{t=1}^{p}w_t\delta_{c_i\to s_j,Mr_t}^{t_k} \tag{4}$$

其中，$\delta_{c_i\to s_j,Mr_t}^{t_k}$ 是单服务属性度量指标的满意度，其计算方法如下。

$$\delta_{c_i\to s_j,Mr_t}^{t_k}=\begin{cases}1, Q_{c_i\to s_j,Mr_t}^{t_k}-Q_{s_j,Mr_t}^{t_k}\geqslant 0\\ \gamma^{\left|Q_{c_i\to s_j,Mr_t}^{t_k}-Q_{s_j,Mr_t}^{t_k}\right|}, Q_{c_i\to s_j,Mr_t}^{t_k}-Q_{s_j,Mr_t}^{t_k}<0\end{cases} \tag{5}$$

当 $Q_{c_i\to s_j,Mr_t}^{t_k}-Q_{s_j,Mr_t}^{t_k}\geqslant 0$ 时，表明服务实体满足了用户实体的服务请求，满意度为 1。当 $Q_{c_i\to s_j,Mr_t}^{t_k}-Q_{s_j,Mr_t}^{t_k}<0$ 时，表明服务实体提供的服务与用户实体的服务要求存在偏差，偏差越大，$\delta_{c_i\to s_j,Mr_t}^{t_k}$ 的值就越小，其中，$0<\gamma<1$。

为了保证计算的时效性，本文引入时间窗 win[9]，进行信任评估计算时只采用时间窗 win 内的记录，舍弃历史记录。时间窗的移动策略是每单位时间段（自行设定），时间窗 win 向前移动一个单位时间段的长度。时间窗如图 4 所示。

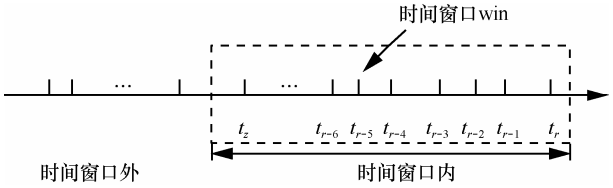

图 4 时间窗口 win

本文采用的方式是，根据迭代时间窗 win 内用户实体 c_i 对服务实体 s_j 的每次交易满意度，求出服务实体 s_j 的直接交易信任度。则

$$T_{c_i,s_j}^{t_r}=\frac{\psi(f_i^{t_r})\sum_{k=z}^{r}u(k)\eta(c_i,s_j,t_k)}{\sum_{k=z}^{r}u(k)} \tag{6}$$

其中，$z=\min\{k|t_k\subset \text{win}\}$，当前时刻 t_r，用户实体 c_i 在时间窗 win 内已交易的次数为 $f_{c_i}^{t_r}=r-z$；$\psi(f_{c_i}^{t_r})=\exp(-\frac{1}{f_{c_i}^{t_r}})$ 为交易次数函数，反应出在固定时间窗 win 内交易次数越多服务越可信；$u(k)$ 为时间衰减函数，令 $u(k)=\tau^{\frac{t_r-t_k}{\eta}}$，其中，$0<\tau<1$，$\eta$ 为协调因子，随着时间窗大小进行调节。

根据社会学，用户一般分为 2 类：一类是正常请求服务，根据交易情况给出可信评价；一类是恶意节点，真正目的是为了攻击敌对的服务实体,夸大共谋的服务实体。通过计算用户实体的评价可信度识别出恶意用户实体，保护信任评估模型。

同时，服务实体的信誉度由用户的评价证据决定，但是由于用户的不同，用户评价证据的权重亦不同，对此，本文采用用户的评价可信度作为评价证据的权重，提高了计算服务实体信誉度的准确率。同时，诚实度可以作为判断推荐行为可信度的一个参考因素。

定义 6 评价满意度。根据服务实体 s_j 的信誉度 TD_{s_j} 与用户实体 c_i 对 s_j 的评价产生的直接交易信任度 T_{c_i,s_j} 的差值计算评价满意度。用 ξ_{s_j,c_i} 表示服

务实体 s_j 对用户实体 c_i 给出的评价满意度。

设服务实体 s_j 距离当前时刻 t_r 最近一次更新的信誉度为 $TD_{s_j}^{t_{r-1}}$，则

$$\xi_{s_j,c_i}^{t_r}=\begin{cases}\beta^{\left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|}, \left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|\leqslant\theta\\ -\beta^{\left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|}, \left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|>\theta\end{cases} \tag{7}$$

其中，θ 为一个阈值，当 $\left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|\leqslant\theta$ 时，表明用户评价还是相对诚实的，差值越小，诚实度越高。当 $\left|T_{c_i,s_j}^{t_r}-TD_{s_j}^{t_{r-1}}\right|>\theta$ 时，表明用户评价是不诚实的，采取一定的惩罚措施，差值越大，惩罚力度越大，其中，$0<\beta<1$。

定义 7　评价可信度。用户实体给出的评价可信程度。

根据时间窗 win 内的多次评价满意度，用户实体 c_i 对服务实体 s_j 的评价可信度为

$$EH_{c_i,s_j}^{t_r}=\frac{\sum_{t_k\subset\text{win}}^{t_r}\xi_{s_j,c_i}^{t_r}}{f_{c_i}^{t_r}} \tag{8}$$

时间窗 win 内与用户实体 c_i 进行交易的服务实体集为：$P=\{s_1,\cdots,s_n\}$，则用户实体 c_i 的最终评价可信度为

$$EH_{c_i}^{t_r}=\frac{\sum_{t=1}^{n}EH_{c_i,s_t}^{t_r}}{|P|} \tag{9}$$

其中，$|P|$ 表示集合 P 中服务实体的数量。

2.4　信誉度计算模块

根据所有用户实体对服务实体的交易信任度得出此服务实体的信誉度，将 2.3 节中所求得的用户实体的评价可信度作为相应的权重。

在时间窗 win 内与服务实体 s_j 进行交易的用户实体集为 $C_1=\{c_1,\cdots,c_n\}$，则服务实体 s_j 的信誉度计算如下。

$$TD_{s_j}^{t_r}=\begin{cases}\dfrac{\sum_{i=1}^{n}EH_{c_i}^{t_r}T_{c_i,s_j}^{t_r}}{|C_1|}\cdot\lambda^{\frac{1}{|C_1|}}, |C_1|\neq 0\\ 0,\text{其他}\end{cases} \tag{10}$$

其中，$|C_1|$ 表示用户实体的数量；$\lambda\in(0,1)$，用来表示在时间窗 win 内与服务实体 s_j 进行交易的用户实体个数越多，则服务实体 s_j 越可信。

2.5　推荐信任度计算模块

根据社会心理学，人们更愿意相信与自己有相似行为同时评价可信度又高的用户的推荐信息，本文引入评价相似度的概念[10]。本文通过评价可信度和相似度求解推荐用户的推荐可信度。

定义 8　对于用户 c_i 可拥有的推荐用户集合为 $C_2=\{c_{j_1},\cdots,c_{j_n}\}$，在时间窗 win 内与用户实体 c_i 有过交易的服务实体集合为 A，与用户实体 c_{j_t} 有过交易的服务实体集合为 B_t，$A\cap B_t=\{p_1,\cdots,p_m\}$。

定义 9　设 $S_{c_i,c_{j_t}}^{t_r}$ 表示用户实体 c_i 与用户实体 c_{j_t} 在 t_r 时刻的评价相似度，则

$$S_{c_i,c_{j_t}}^{t_r}=\begin{cases}1-\sqrt{\sum_{k=1}^{m}(T_{c_i,p_k}^{t_r}-T_{c_{j_t},p_k}^{t_r})^2}\Big/|A\cap B_t|, A\cap B_t\neq\varnothing\\ 0,\text{其他}\end{cases} \tag{11}$$

其中，$|A\cap B_t|$ 表示集合中服务实体的个数。综合考虑，对于用户实体 c_i，推荐用户 c_{j_t} 的推荐可信度计算公式为

$$R_{c_i,c_{j_t}}^{t_r}=\partial\xi_{c_{j_t}}^{t_r}+(1-\partial)S_{c_i,c_{j_t}}^{t_r} \tag{12}$$

其中，$0\leqslant\partial<0.5$，因为用户更愿意相信跟自己评价相似的推荐用户实体，评价可信度可以作为一个参考。

用户实体 c_i 得到的关于服务实体 s_j 的推荐信任度为

$$RT_{c_i,s_j}^{t_r}=\frac{\sum_{c_{j_t}\in C_2\cap R_{c_i,c_{j_t}}^{t_r}\geqslant\alpha}R_{c_i,c_{j_t}}^{t_r}T_{c_{j_t},s_j}^{t_r}}{|C_2'|} \tag{13}$$

其中，C_2' 表示接受推荐的推荐用户集合，$|C_2'|$ 表示集合中的用户实体个数，并且 $|C_2'|\leqslant|C_2|$；α 为用户实体判定是否接受推荐的一个阈值，当 $R_{c_i,c_{j_t}}^{t_r}<\alpha$ 时，用户拒绝其推荐。

3　仿真实验分析

通过仿真实验来验证本文提出模型的有效性和抵御恶意节点攻击的能力，以文献[11]中提出的 CCIDTM 模型作为参考进行仿真实验。

云计算应用系统中涉及到 2 类实体：SC 用户实体和 SP 服务实体。仿真实验中，SC 和 SP 实体

又分为如下几类。

1) SC 用户实体类型

A 类：总是提供真实的服务评价；

B 类：随意给出服务评价，随着时间的变化，给出真实或虚假的评价；

C 类：恶意用户实体夸大共谋的服务实体，攻击敌对的服务实体。

2) SP 服务实体类型

A 类：提供真实的服务能力；

B 类：随意提供服务能力，随着时间的变化，给出真实或虚假的服务；

C 类：恶意服务实体提供虚假的服务能力，存在共谋的用户实体。

实验仿真参数设置如表 1 所示。

表 1　　仿真实验参数说明

参数	参数值	描述
w_i	服务属性权重	$\forall w_i \in (0,1), \sum w_i = 1$
γ	交易满意度影响因子	0.2
τ	时间影响因子	0.9
β	评价可信度影响因子	0.2
λ	交易实体数量影响因子	0.6
α	推荐可信度阈值	0.5

3.1　针对是否划分能力等级的仿真实验

实验设计了一个服务能力进行动态变化的服务实体，实验场景为服务实体提供了 80 次的服务，查询周期为 10。前 2 次查询周期服务实体的能力没有变化，后 6 次查询周期服务实体的能力不同程度地进行变化。为了突出本次仿真的重点，假设用户的评价是可信的并且云服务实体按宣称的能力提供服务。

从图 5 可以看出，本文提出的模型由于进行服务等级的划分，服务实体提供服务的云用户都是按服务等级进行服务请求的，所以即使服务实体能力在后 6 次查询周期进行了动态变化，服务实体的交易信任度一直保持在 1；对于未进行服务等级划分的 CCIDTM 模型[11]，前 2 次查询周期服务实体能力没有变化，所以其信任度为 1，但在随后的查询周期由于服务实体服务能力有了动态变化时，在进行第 3 次查询时信任值陡然下降，随后服务实体的信任度继续下降。这在人类社会中是不合理的，一个服务能力低的服务实体，其信任度不一定也低。因此本模型的提出有效地避免了这一问题。

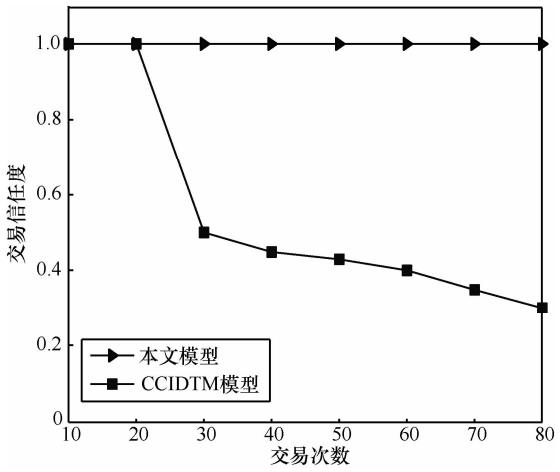

图 5　针对 3.1 节的仿真实验

3.2　针对用户实体 SC 评价可信度的仿真实验

从图 6 中可以看出，针对 A 类用户实体，由于一直提供真实的服务评价，所以其评价可信度一直维持在 1；针对 B 类用户实体，随意给出评价，时而真实时而虚假，所以其诚实度整体不高并呈锯齿状进行变化；针对 C 类用户实体，由于其一直提供虚假的服务评价，夸大共谋服务实体的评价值，攻击敌对服务实体的评价值，所以其评价可信度一直处于低值状态，随着交易次数的增加其值迅速减少。因此，该模型可以有效快速地识别出用户评价行为的真实或虚假。

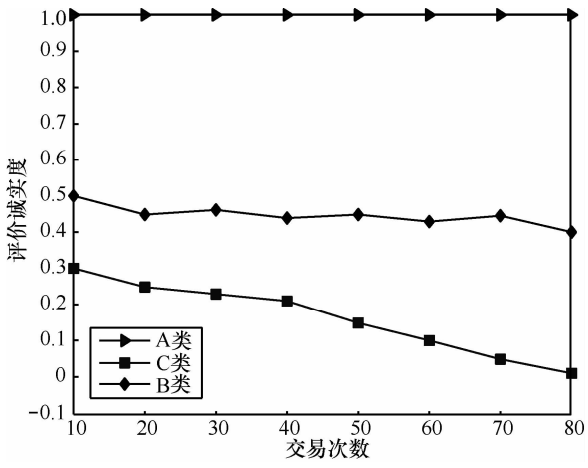

图 6　针对 3.2 节的仿真实验

3.3　针对抵御恶意用户攻击能力的仿真实验

为了验证本模型的有效性，本次仿真选取实体数量 10%~60%的恶意攻击实体。

根据图 7 可以看出，本文模型比文献[11]提出的模型更具顽健性，并且随着恶意用户实体比例的增加，其性能表现更加明显。原因在于虽然文献[11]

中引入评价相似度，大大提高了抵御恶意用户实体的能力，但是本文又引入了评价可信度，通过评价可信度和评价相似度使得推荐可信度更加准确，从而推荐信任值的计算更加准确；同时，诚实度越低的用户，其直接交易信任度对信誉度的影响越小，从而信誉度的计算越准确，最终得到的综合信任值越准确。因此对恶意用户起到更强的抵御作用。

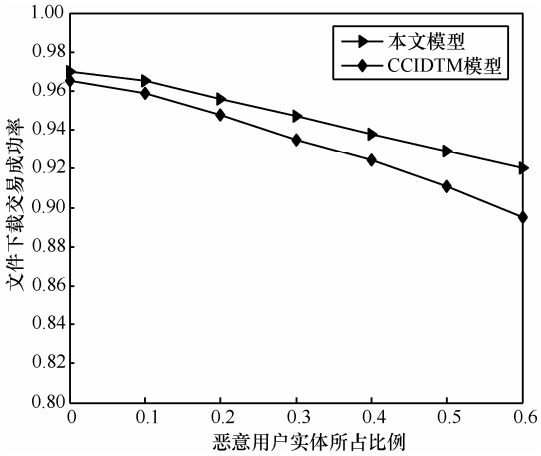

图 7　针对 3.3 节的仿真实验

4　结束语

本文提出了一种基于评价可信度的动态信任评估模型，将服务提供商的服务能力和云用户需求能力划分等级，有效地解决了因云服务提供商服务能力的动态变化对模型的潜在破坏。引入时间窗和时间衰减函数解决了信任度随时间的动态变化问题，体现了信任度的时效性；评价可信度和评价相似度的引入大大提高了判断推荐可信度的准确性，过滤了恶意推荐节点。同时，该模型综合考虑了直接交易信任度、信誉度和推荐信任度，得出综合信任度，使得用户能够选择到可靠、可信的实体进行交互。

参考文献：

[1] 冯登国, 张敏, 张妍等. 云计算安全研究[J].软件学报,2011,22(1):71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[2] 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.

[3] 王守信, 张莉, 李鹤松. 一种基于云模型的主观信任评价方法[J]. 计算机学报, 2010, 21(6):1341-1352.
WANG S X, ZHANG L, LI H S. Evaluation approach of subjectivetrust based on cloud model[J]. Journal of Software, 2010, 21(6):1341-1352.

[4] MOHAMMAD G U, MOHAMMAD Z, SHEIKH I A. CAT: a context aware trust model for open and dynamic systems[A]. Proceedings of the 23rd Annual ACM Symposium on Applied Computing, SAC'08[C]. Fortaleza, Ceara, Brazil, 2008. 2024-2029.

[5] 李峰, 申利民, 司亚利等. 基于交互感知的动态自适应的信任评估模型[J]. 通信学报, 2012, 33(10):60-70.
LI F, SHEN L M, SI Y L, *et al*. Dynamic adaptive trust evaluation modelbased on interaction-aware[J]. Journal on Communications, 2012, 33(10):60-70.

[6] LI X Y, GUI X L. A comprehensive and adaptive trust model for large-scale P2P networks[J]. Journal of Computer Science and Technology, 2009, 24(5):868-882.

[7] HAQUE M, AHAMED S. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments[J]. Journal of Systems and Software, 2009, 83(2):253-270.

[8] 李佳伦, 谷利泽, 杨义先. 一种具有时间衰减和主观预期的 P2P 网络信任管理模型[J]. 电子与信息学报, 2009, 31(11):2786-2790.
LI J L, GU L Z, YANG Y X. A new trust management model for P2P network with time self-decay andsubjective expect[J]. Journal of Electronics & Information Technology, 2009, 31(11):2786-2790.

[9] 石志国, 刘冀伟, 王志良. 基于时间窗反馈机制的动态P2P信任模型[J]. 通信学报, 2010,31(2):120-129.
SHI Z G, LIU J W, WANG Z L. Dynamic P2P trust model based on time-window feedback mechanism[J]. Journal on Communications, 2010, 31(2):120-129.

[10] 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):9-20.
MIAO G S, FENG D G, SU P R. Colluding clique detector based onactivity similarity in P2P trust model[J]. Journal on Communications, 2009, 30(8):9-20.

[11] 谢晓兰, 刘亮, 赵鹏.面向云计算基于双层激励和欺骗检测的信任模型[J]. 电子与信息学报, 2012, 34(4):812-817.
XIE X L, LIU L, ZHAO P. Trust model based on double incentive and deception detection for cloud computing[J]. Journal of Electronics and Information Technology, 2012, 34(4):812-817.

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，主要研究方向为云计算、网络安全、信任、可信计算等。

饶凯莉（1992-），女，江苏睢宁人，南京邮电大学硕士生，主要研究方向为云计算、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、移动代理等。