云环境下基于协同推荐的信任评估与服务选择

游 静 冯 辉 孙玉强
(常州大学信息科学与工程学院 常州 213164)

摘 要 "模糊、自治"的云计算环境中,服务品类繁多、质量参差不齐,用户主体难以进行可信赖的服务选择。在用户交互经验的基础上,结合现实人际交易模式,提出了一种基于协同推荐的综合信任量化评估模型。模型引入了时间衰减、权重两类动态因子,设计了多元化混合协同推荐算法来实现用户之间的有效协作,帮助用户正确选择可信云服务。为了验证模型的可行性,设计出一个分布式的原型系统,对模型的用户满意度和服务选择质量进行仿真实验。仿真结果表明,该模型能够更快地提高平均服务满意度,更有效地抑制恶意服务,而且随着交互次数的增长,服务选择质量也会不断提高。

关键词 信任评估,服务选择,信任模型,协同推荐,云计算
中图法分类号 TP319 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.5.026

Trust Evaluation and Service Selection Based on Collaborative Recommendation for Cloud Environment

YOU Jing FENG Hui SUN Yu-qiang
(Faculty of Information Science & Engineering, Changzhou University, Changzhou 213164, China)

Abstract In the "fuzzy and autonomy" cloud computing environment, the service category is numerous and the quality is uneven, so it is difficult for the users to carry out a trusted service selection. On the basis of the user interaction experience and the real interpersonal interaction model, a comprehensive trust evaluation model based on collaborative recommendation was proposed. In the model, two kinds of dynamic factors, the time decay and the weights, are introduced and a multivariate hybrid collaborative recommendation algorithm is designed to achieve effective collaboration among users, which can help users select the trusted cloud services. In order to verify the feasibility of the model, a distributed prototype system was designed, and the simulation experiments were carried out on the user satisfaction and service quality of the model. Simulation results show that the model can faster increase the average service satisfaction and more effectively inhibit malicious service, and with the growth of the number of interactions, the service selection quality will also continue to improve.

Keywords Trust evaluation, Service selection, Trust model, Collaborative recommendation, Cloud computing

1 概述

自2007年"云计算"概念诞生至今,互联网中服务化观念逐步普及,大量基础设施资源、平台资源和软件资源通过互联网以服务(又称云服务)的方式整合起来,向外提供功能齐全的服务。然而互联网的随机性、开放性和不可预测性等不确定性因素[1],导致服务缺乏有效的验证机制,无法准确度量服务的可靠性,出现了恶意实体提供虚假信息、传播病毒和蠕虫等欺骗行为,使得用户节点进行服务选择存在极大的风险。因此,制定有效的服务信任评估机制来抑制恶意行为,帮助用户选择可信赖服务,是云计算环境下服务安全可信的保障。

当前国内外学者已对服务信任评估机制进行了一些理论研究,将用户对服务的信任源分为自身的直接信任和他人的推荐信任。S. D. Kamvar等人[2]提出的EigenTrust信任评估模型虽然综合了服务的直接信任源和推荐信任源,然而其推荐信任源选择全部与服务有交互的高信任值的信任实体,这些信任实体的推荐信息相对用户节点并不一定可信;王晋东等人[3]在研究云模型理论的基础上,提出一种基于加权多属性云的服务信任评估方法,其通过用户评价的相似度确定推荐信任源,服务评估具备可信性,有参考意义;R2Trust[4]是一个基于声誉和风险的信任评估管理模型,通过风险因子抑制恶意行为,从可信实体获取推荐信任源。从上述文献研究发现,信任评估机制是在交互记录基础上,通过协同推荐机制选择推荐信任源,对服务进行信任评估。因此,推荐信息源的选择是影响服务评估准确度的关键因素,需要有相应的方法对推荐者进行过滤,定位可靠的推荐信息源。

针对如何选择可靠推荐信任源问题,本文提出了一种多元化混合协作推荐机制,该机制综合了高可靠的熟人推荐信任源与服务自荐信任源,提供理想的推荐信任源。本文第2节给出了信任模型中信任、时间衰减因子、权重等相关概念的

到稿日期:2015-04-24 返修日期:2015-08-03 本文受江苏省自然科学基金(BK2009535),江苏省高校自然科学基金(07KJB520022)资助。
游 静(1975-),女,博士,副教授,主要研究方向为服务信任评估模型、软件抗衰与自愈,E-mail:498219012@qq.com;冯 辉(1991-),男,硕士,主要研究方向为服务信任评估模型;孙玉强(1963-),教授,主要研究方向为并行计算。

定义和计算公式，并介绍了多元化混合协作推荐机制的详细内容。为了验证模型的可行性，本文参照张明清等人[5]提出的基于 Agent 的分布式系统设计方案，完成了信任模型分布式仿真原型系统的架构设计；第 3 节详细介绍了分布式仿真原型系统的架构体系；第 4 节通过几组实验验证了模型的可行性；最后对全文工作进行了总结归纳，并对未来的工作进行了展望。

2 基于协同推荐的信任模型

云环境下，服务选择是基于信任关系的一种决策行为。如何从众多服务中辨别出可信赖的服务，依赖于准确的信任评估。现实社会中，信任是维系人际关系的基础，是一种很难具体定量表示的抽象心理认知[6]。普遍情况下，实体之间的信任关系是模糊不清的，存在“未知”关系，实体间很难进行精确的信任评估[7]，且随着实体间行为上下文的动态变化，信任关系也会发生改变，此外还需要考虑到各种动态因子，如时间衰减、组成权重、地点等，因此信任评估是一种动态的描述过程[8]。

本文参考上述对现实社会信任的描述，提出了一种基于协同推荐的信任服务评估模型，将信任定义为主体通过客体的交互行为记录，结合自身记录、他人推荐与客体自荐建立的一种对客体信赖度的动态预测，帮助用户进行正确的服务决策。这其中他人推荐与客体自荐信任源由协同推荐机制给出。

2.1 协同推荐机制

传统的基于推荐的信任机制主要分为以下两类。

(1)全局的推荐机制[9-11]。系统中需要设定一个集中的服务中心用于存储每个主客体之间的交易记录，当主体需要客体评估信息时，由服务中心提供推荐数据。

(2)基于熟人的推荐机制[12-14]。熟人推荐机制下，主体通过有交互记录的熟识节点集获取相关服务的推荐信任数据。

上述两种传统协同推荐机制虽然都能对服务进行信任评估，但对于开放、动态的云计算环境，都存在明显的缺陷。云环境下数据存储量已经从 TB 级别升至 PB 级别，因此对于全局的推荐机制下设置集中的服务中心，其存储性能和安全性值得商榷；而由于云环境下数据分散，部分节点会出现交互集信息匮乏的情况，使得基于熟人的推荐机制下获得的推荐数据源不够全面，难以进行有效的信任评估。

本文提出一种多元化混合协同推荐机制，即结合熟人的协同推荐机制，将熟人的推荐信任源作为一种信任来源，并引入服务对用户的信任度概念，由服务自主向用户推荐可信赖的用户集，作为另一种信任来源。这种推荐机制通过服务的自荐信任弥补了熟人机制信任匮乏的缺陷，也不需要集中的服务中心即可向用户提供可信赖的推荐信任源，在开放、动态的云环境下能对服务进行有效的信任评估。

2.2 协同推荐信任的相关概念

给定用户集 US、服务商集 AS 和服务集 Sa，若 $u,v\in US$，主体 u 对客体 v 的信任关系描述为 $u\rightarrow v$；若 $u\in US, a\in AS$，a 的服务 $s\in Sa$，主体 u 对客体 a 就 a 可以提供的服务 s 建立的信任关系描述为 $u\xrightarrow{s}a$。

定义 1(信任度) 信任度是对信任的定量表示，是主体在某个时刻得出的对客体提供的服务或行为的可靠程度的评价，取值范围为[0,1]。若 $u,v\in US$，主体 u 对客体 v 在时刻 tl 的信任度为 $T(u\xrightarrow[tl]{}v)$；若 $u\in US, a\in AS$，a 的服务 $s\in Sa$，u 对 a 就服务 s 在时刻 tl 的信任度描述为 $T(u\xrightarrow[tl]{s}a)$。该值存储在主体的信任度表中，并按表 1 进行信任等级分类。

表 1 信任等级

信任等级	可信度	取值范围
1	完全失信	[0,0.2]
2	不太可信	(0.2,0.5]
3	基本可信	(0.5,0.7]
4	比较可信	(0.7,0.9]
5	完全可信	(0.9,1]

信任等级是主体对客体提供的服务或行为的信任分级。在参考现实社会信任级别分类的基础上，将信任度合理划分成 5 个等级，为用户节点提供直观的判断依据。

定义 2(信任类别) 云环境下主体对客体的信任数据源由主体的直接信任源和他人推荐信任源构成，且由于推荐信任源是分散的，需要从第三方筛选获取信息，因此模型将信任分为 3 类，如图 1 所示(U_a 表示用户主体，S 表示服务，$U_1\cdots U_n$ 表示 U_a 熟识用户集，$U_1\cdots U_m$ 表示 S 信任用户集)。

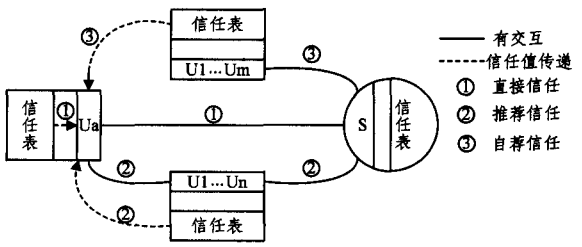

图 1 信任类别

直接信任：在给定的上下文环境中，用户主体 U_a 通过以往的直接交互经验得到的服务客体 s 的信任信息，具有最高的可靠性，是对现实社会中“认识或了解”的抽象，与其相对应的量化表示为直接信任度 DT。

推荐信任：用户主体 U_a 选取可信赖的交互用户集$\{U_1\cdots U_n\}$，且用户集$\{U_1\cdots U_n\}$与服务 s 都有过交互，通过用户集$\{U_1\cdots U_n\}$推荐获得有关服务 s 的信任信息，是对现实中“介绍”的抽象。与其相对应的量化表示为推荐(传递)信任度 RT。

自荐信任：服务 s 选取可信赖的交互用户集$\{U_1\cdots U_m\}$，通过用户集对服务 s 的信任度向用户主体 U_a 提供自荐信任数据，是对现实中“据说”的抽象。与其相对应的量化表示为自荐信任度 ST。

主体 U_a 综合考虑对客体 s 的 3 类信任值，结合时间衰减、权重等动态因子，得出对客体 B 的综合信任评价。与其相对应的量化表示为综合信任度 GT。

定义 3(动态因子) 现实社会中，主客体间信任关系不是静态的，会随着时间流逝、主客体间的行为上下文而动态变化，因此在模型中考虑了时间衰减和权重 2 类动态因子，其相关定义如下。

时间衰减因子：主客体间信任关系会随着时间的推移而

减小，即相隔时间越久的信任度对现在的影响越小，时间越近的信任值越可靠，故定义时间衰减因子如下：

$$\delta(t)=\begin{cases}-\dfrac{\Delta t^{\frac{5}{2}}}{12964181}+1, & 0\leqslant\Delta t\leqslant 700\\ 0, & \Delta t>700\end{cases}$$

其中，$\Delta t=(t-tl)$，t 为当前时间，tl 为信任主客体最后一次交互的时间，Δt 取天为单位。图 2 表示了时间因子的衰减函数曲线图。

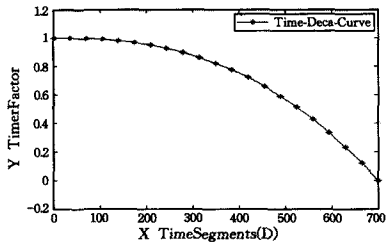

图 2　时间因子的衰减函数曲线图

如图 2 所示，横轴表示时间段，单位为天数；纵轴则是相对应的时间衰减因子值。从图中可以明显看出，随着时间的增加，时间衰减因子逐渐变小，第一年内的信任相对可靠，时间衰减平缓，直至第 2 年趋向于 0，评价完全失效。

权重因子：为了平衡直接信任、推荐信任和自荐信任在综合信任中的比例，在信任模型中引入权重因子，ω_1、ω_2、ω_3 分别表示直接信任权重、推荐信任权重、自荐信任权重，在[0,1]之间取值。3 类权重定义如下：

$$\omega_1=1-\frac{1}{\sqrt[3]{1+k}},\omega_2=\frac{2}{3}(1-\omega_1),\omega_3=\frac{1}{3}(1-\omega_1)$$

k 表示节点间共发生 k 次直接交易，且 $\omega_1+\omega_2+\omega_3=1$。

图 3 为权重因子 ω_1、ω_2、ω_3 随交互次数增加而变化的曲线图。

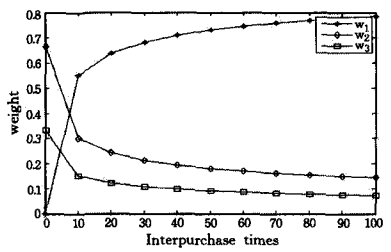

图 3　权重随交互次数增加的曲线图

图 3 中横轴表示交互次数，纵轴表示权重值。从图中可以明显看出，交易初期，两节点之间的交易次数较少时，模型以推荐信任和自荐信任为主，随着直接交互次数的增加，节点间活跃度越来越高，直接信任的权重明显增大，从而该信任度值在综合信任度中的比例也在相应上升，符合现实社会信任权重的变化情况。

2.3　协同推荐信任度计算

2.3.1　直接信任度

节点间直接信任度分为 3 种情况：

(1)节点 u，a 都不提供服务；

(2)节点 u 与节点 a 提供的某一服务 s 有交互；

(3)节点 u 与节点 a 提供的服务 s 无交互，但与 a 提供的其他服务有过交互。

考虑到历史经验和时间衰减的影响，具体公式如下：

$$DT(u\xrightarrow[t]{s}a)=$$

$$\begin{cases}0, & u,a\in US\\ \delta(t)T(u\xrightarrow[tl]{s}a), & u\in US,a\in AS,\exists u\xrightarrow{s}a\\ \dfrac{1}{k}\sum\limits_{s'\in Su}\delta(t)T(u\xrightarrow[tl]{s'}a), & u\in US,a\in AS,\exists u\xrightarrow{s'}a\&\&s'\neq s\end{cases}$$

其中，k 表示主体 u 使用过的客体 a 的服务的数量。

2.3.2　推荐信任度

若 $u\in US$，$a\in AS$，且 u 有交互用户实体 w，$\exists w\xrightarrow{s}a$，则推荐信任度

$$RT(u\xrightarrow[t]{s}a)=DT(u\xrightarrow[t]{}w)\cdot DT(w\xrightarrow[t]{s}a)$$

其中

$$DT(u\xrightarrow[t]{}w)=$$

$$\begin{cases}\delta(t)T(u\xrightarrow[tl]{}w), & u,w\in US,\exists u\to w\\ \dfrac{1}{k}\sum\limits_{s'\in Sw}\delta(t)T(u\xrightarrow[tl]{s'}w), & u,w\in US,\exists u\xrightarrow{s'}w\\ 0, & u\in US,w\in AS\end{cases}$$

为了有效避免某些实体的欺诈行为，本文选取 n 个用户实体作为中间实体，将其传递信任度加权平均得出两个实体之间的传递信任度：

$$RT(u\xrightarrow[t]{s}a)=\frac{1}{n}\sum_{w\in W}DT(u\xrightarrow[t]{}w)\cdot DT(w\xrightarrow[t]{s}a)$$

附加条件：$DT(u\xrightarrow[t]{}w)\geqslant 0.6$。其中 w 是与 u 和 a 均有信任关系的实体集合，实体集 w 是将直接信任度 $DT(u\xrightarrow[t]{}w)$ 从高到低排序后选取的前 n 个值大于 0.6 的实体。

2.3.3　自荐信任度

服务商 a 提供的服务 s 存在交互用户集 US，即 $\forall v\in US$，有 $v\xrightarrow{s}a$，由服务 s 将交互集的可信度 $DT(a\xrightarrow{s}v)$ 从高到低排序后，选取前 m 个实体作为可信赖用户集为用户实体 u 提供服务 s 的推荐信任数据源，综合得到自荐信任度：

$$ST(u\xrightarrow[tl]{s}a)=\frac{1}{m}\sum_{v\in US}DT(u\xrightarrow[tl]{}v)\cdot DT(v\xrightarrow[tl]{s}a)$$

若主体 u 与客体 v 不存在交互记录，取 $DT(u\xrightarrow[tl]{}v)=0.5$。

上述计算中，服务 s 对用户 v 的可信度 $DT(a\xrightarrow{s}v)$ 是由系统根据用户使用次数自动给定，计算公式如下：

$$DT(a\xrightarrow{s}v)=$$

$$\begin{cases}0.5\delta(t), & 1\leqslant n\leqslant f\\ (0.5+\dfrac{1}{\pi}\arctan(n-f))\delta(t), & n>f\end{cases}$$

为了有效区分服务对用户的信任程度，本文取 $f=5$，即与服务 s 交互次数超过 5 的用户将设定更高的信任值，且信任值受时间衰减动态因子影响。

2.3.4　综合信任度

综合信任度综合直接、推荐和自荐信任，以及时间衰减、权重动态因子，得出：

$$GT(u\xrightarrow[t]{s}a)=\omega_1\cdot T(u\xrightarrow[t]{s}a)+\omega_2\cdot RT(u\xrightarrow[t]{s}a)+\omega_3\cdot ST(u\xrightarrow[t]{s}a)$$

3 仿真环境

3.1 分布式信任管理原型系统的框架

通过上述对信任模型的概念分析，发现不同用户在各种因素影响下对相同服务的信任评估是有区别的，带有一定的主观因素，因此信任管理系统中信任评估、信任管理、信任决策等功能都交由用户端自己完成，信任数据源通过本地数据、熟识用户和服务自荐用户来获取。实现上述功能的分布式仿真实验环境如图 4 所示。

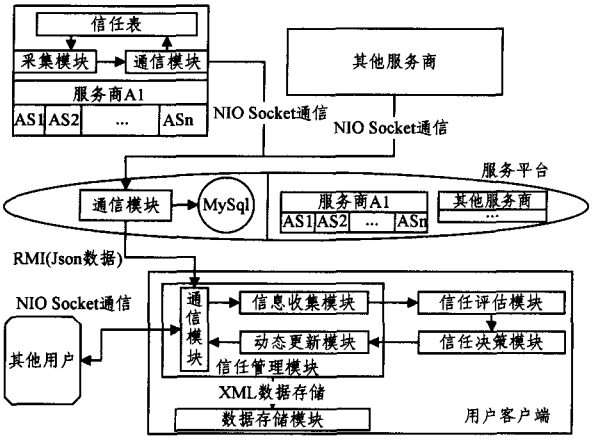

图 4 仿真环境

整个仿真环境主要分为 3 部分：服务商端、服务平台和用户客户端，它们分别运行在不同的 JVM(Java 虚拟机)下。

(1)服务商端各自独立，提供相应服务，在各自本地信任表中存储服务-用户交互记录，由采集模块从信任表中根据自荐推荐算法提取相应数据到通信模块，最后由通信模块完成与服务平台的信息交互。界面开发采用 Swing 技术，利用 NIO Socket 技术完成通信功能。

(2)服务平台基于 Linux 平台架构，运行在高访问量的环境中，承担服务器职责，通过 EJB 一种 JavaEE 服务器端组件模型，实现 RMI(远程接口调用)功能的封装，完成分布式体系结构服务端业务逻辑功能，再通过 Jboss(EJB 容器)发布，向用户客户端提供接口服务。服务平台承载服务的显示及信息传输功能，为了减轻平台性能压力，平台上并不存储节点交互信息，MySql 数据库中只需存储用户节点和服务商节点的 ip、port 信息以及服务商服务的相关描述信息，由通信模块完成信息交互功能。

(3)用户客户端为了完全反映仿真环境的分布性特征，互相之间都是对等的，各客户端自主选择合作对象协同完成任务。开发方面采用 Swing 技术，由于 Java 语言具备跨平台性，客户端可以在任意系统环境下运行。客户端在使用过程中通过 Java 命名和目录接口(Java Naming and Directory Interface，JNDI)来借用代理服务中心 EJB 容器对象池中的对象，调用业务逻辑，完成客户端功能模块开发。由图 4 可知，用户客户端主要由 4 部分组成：

1)信任管理模块：由通信模块、信息收集模块、动态更新模块 3 个小模块组成。通信模块负责与 EJB 容器和其他用户的交互，与 EJB 容器之间通过 RMI(远程方法接口)技术完成 Json 格式数据的传输，与其他用户间使用 NIO(New I/O)技术完成异步非阻塞通信；信息收集模块负责收集通信模块从服务平台中转和熟识用户处获取的数据，并将 Json 格式数据转换成 Bean 对象；动态更新模块负责根据信任决策传递的数据更新本地数据，并通过服务平台更新服务商端数据。

2)信任评估模块：该模块对信息收集模块所提供的信息进行筛选，结合上述信任评估算法进行综合计算，得到被评价对象的综合信任度评价值。

3)信任决策模块：决策模块主要完成两个功能，第一个功能是依据评估模块传递的综合信任值，决定是否执行服务选择；第二个功能是服务使用完毕后，将服务的评价结果返回到信任管理模块的动态更新模块，更新本地数据和服务商端数据。

4)数据存储模块：用户的数据都采用 XML 格式存储在各自客户端中，由用户自己维护，其他用户端只能通过信任度验证来请求查询数据，而不能修改他人数据，这种机制的安全性很高。

4 实验

4.1 仿真设计

实验根据图 4 所示的仿真环境搭建分布式系统、模拟交互、监控数据变化。硬件设备配置 1 台服务商 PC 端(10 个服务商，每个提供 100 个服务)、1 台服务器 PC 端、5 台客户 PC 端(100 个用户端)；服务器 PC 端在 Linux 环境下运行一个 EJB 服务端，配置 JBOSS 服务器。系统硬件配置如表 2 所列。

表 2 实验环境硬件配置

	服务 PC 端	服务商、客户 PC 端
操作系统	CentOS 7	Windows 8.1
内存	DRR3 16G	DRR3 32G
处理器	Intel 酷睿 i5 4460 @ 3.2GHz	Intel 酷睿 i7 4710MQ @2.5GHz

为了得到预期仿真结果，结合前面给出的信任模型和分布式系统的设计框架，对仿真配置环境进行如下设置。

(1)服务分布

系统中服务类别分为诚实服务(Honest Service)和恶意服务(Malicious Service)。诚实服务是真实、可信的且让用户使用满意的服务。反之，恶意服务提供的是虚假、失信、低效的服务。在仿真实验中两类服务的比例是影响仿真结果的重要因素，参考真实市场中商品平均良品率为 75%，在本仿真环境设计中诚实服务占 75%，恶意服务占 25%。

(2)初始信任分布

初始信任规定了系统服务的初始信任值情况。初始信任值的设定有均匀分布、正态分布、幂率分布和 U 型分布等 4 种分布，这里采用常见的正态分布。

(3)阈值

设定阈值是对用户的一种验证机制，用户节点会对访问者的信任进行核实，只有信任值大于阈值时，才会进行交互。阈值的大小会影响用户间的交互，阈值太小会导致用户管理太松懈，恶意用户节点会推荐虚假信息；阈值太大又会使得用户管理过于苛刻，节点间可以相互交互的用户集太小，导致推荐信息不够全面。综合考虑，本仿真实验取折中值，设定阈值为 0.5。

(4)仿真参数选择

通过以上分析，确定仿真运行的参数及其取值如表 3 所列。

表 3　仿真运行参数

参数	参数说明	初始值
N_u	用户客户端	100 个
N_p	服务提供商	10 个
N_s	云服务	每个 N_p 提供 100 个
ρ	服务良品率	75%
$\delta(t)$	时间衰减因子	1
ω_1	直接信任权重	0
ω_2	推荐信任权重	2/3
ω_3	自荐信任权重	1/3
T_0	初始信任值	正态分布
β	满意度阈值	0.5
M	交易次数	100
GT	综合信任值	0

4.2　仿真实验与分析

本文进行了 3 组实验。第一组实验对比传统静态信任评估方法与本文模型(My Trust)，观测随着交互次数增多服务满意度的变化情况；第二组实验对比本文模型(My Trust)与 R^2Trust、EigenTrust 模型，观测对恶意实体的抑制能力；第三组实验观测一组用户在本文信任模型基础上服务选择的质量情况。通过 3 组实验显示本文信任评估模型在用户服务满意度及奖惩机制方面的效率，验证其能否帮助用户选择可信赖的服务。

实验 1　服务满意度是用户与服务交互结束后对服务质量的评断，取值范围为[0,1]，是评判信任模型好坏的一个重要参考指标。服务满意度不低于 0.7，表明本次交易成功；服务满意度低于 0.7，表明本次交易失败。本实验比较传统静态信任评估方法(不考虑时间衰减、权重)和本文提出的综合信任评估方法，分别观测随着交互次数的增长各自平均服务满意度的变化情况，如图 5 所示。

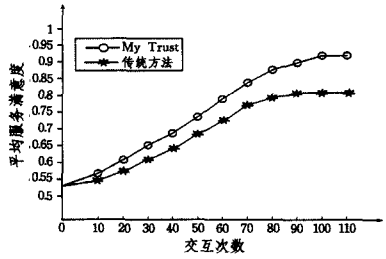

图 5　2 类模型服务满意度随交互次数的变化情况

从图 5 可以明显看出，随着交易次数增多，采用 My Trust 模型比传统静态评估方法能更快地提高服务满意度，因为本文模型在推荐数据源选择方面是由可靠的熟人推荐及服务信赖推荐源构成的，并考虑到了时间衰减和权重两类动态因子的影响，对服务的评估准确且可信。图中曲线可以反映本文提出的信任评估模型适用于分布式的仿真环境，对云环境下的服务信任评估更高效。

实验 2　本实验为了验证本文 My Trust 模型对恶意实体的抑制能力，模拟恶意实体比例增长的仿真环境，与 R^2Trust 及 EigenTrust 模型做对比实验来观测一组用户相应的平均服务满意度的变化情况。本实验设定 10 个用户作为观测对象，实验结果如图 6 所示。

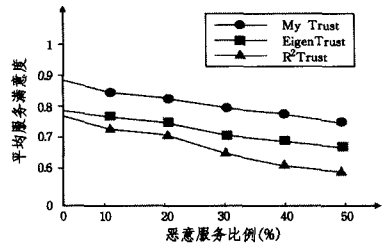

图 6　3 类模型随恶意服务比例增加平均服务满意度的变化情况

从图 6 可以看出本文提出的 My Trust 模型在没有恶意服务存在时，相比另外两种模型初始满意度更高一些，约为 0.9。随着恶意服务比例增多，3 类模型下用户的平均服务满意度都有明显下降，本文模型在恶意服务比例达到 50%时，平均服务满意度仍能保持在 0.7 以上，表明本文提出的综合信任评估模型具备良好的奖惩机制，能够有效抑制恶意服务。

实验 3　服务信任评估模型的目的是让用户可以选择可信的服务。本实验通过选取一组用户集作为实验源，观测随着交互次数增多用户集中诚实服务与恶意服务的比重变化情况，验证本文信任评估模型对用户选择能否提供有效依据，实验结果如图 7 所示。

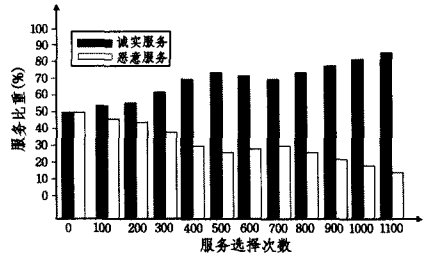

图 7　2 类服务所占比重随服务选择次数增多的变化情况

图 7 显示，随着服务选择次数的增多，用户服务选择总数中诚实服务所占的比重逐渐上升，恶意服务所占比重不断降低，说明用户的服务选择质量逐步提升。实验结果表明，本文提出的综合信任模型能够帮助用户进行正确的服务选择，提高服务的选择成功率。

结束语　在复杂开放的云计算环境中，如何帮助用户选择值得信赖的服务，是当前云计算相关技术的研究热点。因此本文针对云环境中服务的随机性、模糊性和不可预测性等不确定性因素，引入时间衰减、权重等动态因子，结合多元化混合协作推荐算法，综合考虑用户的主观因素，提出了基于交互记录的综合信任量化评估模型。为了验证综合信任模型的可行性，本文参考 Agent 建模方法，设计出了分布式的信任管理原型系统，自底向上对信任模型进行建模仿真，充分考虑系统的各方面指标，进而完善分布式架构。该仿真方法为信任模型仿真的规范化提供了参考。最后通过 3 组仿真实验，证明云环境下综合信任模型能够帮助用户进行正确的服务选择，抑制了市场中的恶意服务，更加真实地反映了云计算环境中服务信任情况，为用户的服务选择提供了可靠的安全决策。

参 考 文 献

[1] Zhang Shi-bin, He Da-ke, Endo Homare. Research of fuzzy autonomous trust establishment strategy[J]. Journal of Electronics&InformationTechnology, 2006, 28(8): 1492-1496

[2] Kamvar S D, Schlsser M T, Carcia-Molinah. The EigenTrust Al-

gorithm for Reputation Managementin P2P Networks[C]//Proceedings of the International Conference on WWW. Budapest, Hungary, 2003

[3] Wang Jin-dong, Wei Bo, Zhang Heng-wei, et al. Research on Service Trust Evaluation Approach under Cloud Computing Environment[J]. Computer Science, 2014, 41(12): 38-42(in Chinese)
王晋东,卫波,张恒巍,等. 云计算环境下服务信任评估方法研究[J]. 计算机科学,2014,41(12):38-42

[4] Tian Chun-qi, Yang Bai-jian. R^2 Trust, a Reputation and Risk Based Trust Management Framework For Large-Scale, Fully Decentralized Overlay Networks[J]. Future Generation Computer Systems, 2011, 27(8): 1135-1141

[5] Zhang Ming-qing, Fan Tao, Tang Jun, et al. Agent-based simulation of trust model in distributed system[J]. Computer Engineering & Design, 2014, 35(9): 3202-3206(in Chinese)
张明清,范涛,唐俊,等. 基于 Agent 的分布式系统信任模型仿真[J]. 计算机工程与设计,2014,35(9):3202-3206

[6] Tian Jun-feng, Cai Hong-yun. Actuality and Development of Trust Model[J]. Journal of Hebei University(Natural Science Edition), 2011, 31(5): 555-560(in Chinese)
田俊峰,蔡红云. 信任模型现状及进展[J]. 河北大学学报(自然科学版),2011,31(5):555-560

[7] Chang E, Thomson P, Dilion, et al. The Fuzzy and Dynamic Nature of Trust[M]//Trust, Privacy, and Security in Digital Business(LNCS 3592). Berlin: Springer-Verlag, 2005: 161-174

[8] Li Xiao-yong, Gui Xiao-lin. Trust Quantitative Model with Multiple Decision Factors in Trusted Network[J]. Chinese Journal of Computers, 2009, 32(3): 405-416(in Chinese)
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

[9] Vu L H, Hauswirth M, Aberer K. QoS-Based service selection and ranking with trust and reputation management[C]//Meersman R, Tari Z, eds. Proc. of the OTM 2005(LNCS 3760). 2005: 466-483

[10] Ali A S, Ludwig S A, Rana O F. A cognitive trust-based approach for Web service discovery and selection[C]//Proc. of the 3rd European Conf. on Web Services. 2005: 38-49

[11] Day J, Deters R. Selecting the best Web service[C]//Proc. of the 14th Annual IBM Centers for Advanced Studies Conf.. 2004: 293-307

[12] Billhardt H, Hermoso R, Ossowski S, et al. Trust-Based service provider selection in open environments[C]//Proc. of the 22nd Annual ACM Symp. on Applied Computing. New York: ACM Press, 2007: 1375-1380

[13] Page L, Brin S, Motwani R, et al. The PageRank citation ranking: Bringing order to the Web[R/OL]. Stanford Digital Library Technologies Project, 1998. http://ilpubs.stanford.edu:8090/422/

[14] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks[C]//Proc. of the 3rd Int'l Conf. on Peer-to-Peer Computing. IEEE Computer Society Press, 2003: 150-157

(上接第 131 页)

[7] Moreno Y, Nekovee M, Vespignani A. Efficiency and Reliability of Epidemic Data Dissemination in Complex Networks[J]. American Physical Sciety, 2004, 69(5): 343-358

[8] Newman M E J. Spread of Epidemic Disease on Networks[J]. Physical Review E Statistical Nonlinear & Soft, Matter Physics, 2002, 66(1): 016128

[9] Pastor-Satorras R, Vespignani A. Epidemic Spreading in Scale-Free Networks[J]. Physical Review Letters, 2001, 86(14): 3200-3203

[10] Khayam S A, Radha H. A Topologically-Aware Worm Propagation Model for Wireless Sensor Networks[C]//25th IEEE International Conference on Distributed Computing Systems Workshops, 2005. IEEE, 2005: 210-216

[11] Song Y, Jiang G P. Model and Dynamic Behavior of Malware Propagation over Wireless Sensor Networks[M]//Complex Sciences. Springer Berlin Heidelberg, 2009: 487-502

[12] Guo W, Zhai L, Guo L, et al. Worm Propagation Control based on Spatial Correlation in Wireless Sensor Network[M]//Web Technologies and Applications. Springer Berlin Heidelberg, 2012: 68-77

[13] Tang S, Myers D, Yuan J. Modified SIS Epidemic Model for Analysis of Virus Spread in Wireless Sensor Networks[J]. International Journal of Wireless and Mobile Computing, 2013, 6(2): 99-108

[14] Peng S, Wang G, Yu S. Modeling the Dynamics of Worm Propagation Using Two-Dimensional Cellular Automata in Smartphones[J]. Journal of Computer and System Sciences, 2013, 79(5): 586-595

[15] Mishra B K, Tyagi I. Defending against Malicious Threats in Wireless Sensor Network: A Mathematical Model[J]. International Journal of Information Technology and Computer Science (IJITCS), 2014, 6(3): 12-19

[16] Hu L, Evans D. Using Directional Antennas to Prevent Wormhole Attacks[C]//NDSS. 2004: 241-245

[17] Panyim K, Krishnamurthy P, Le A. Secure Connectivity through Key Predistribution with Directional Antennas to Cope with Jamming in Sensor Networks[C]//2013 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS). IEEE, 2013: 471-475

[18] Mickens J W, Noble B D. Modeling Epidemic Spreading in Mobile Environments[C]//Proceedings of the 4th ACM Workshop on Wireless Security. ACM, 2005: 77-86

[19] Pantazis N A, Vergados D J, Vergados D D, et al. Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling[J]. Ad Hoc Networks, 2009, 7(2): 322-343

[20] Ai J, Abouzeid A A. Coverage by Directional Sensors in Randomly Deployed Wireless Sensor Networks[J]. Journal of Combinatorial Optimization, 2006, 11(1): 21-41