基于DS理论的多源证据融合云安全信任模型

束 柬 梁昌勇

（合肥工业大学管理学院 合肥 230009）（过程优化与智能决策教育部重点实验室 合肥 230009）

摘 要 云计算技术在带来信息更大范围共享、成本更低等便捷的同时，也面临着隐私泄露、信息丢失等新的安全问题。如何在海量分布式的云系统中识别和管理节点的可信度成为云安全问题研究的重要方向之一。本模型考虑云计算分布式体系架构，结合DS证据理论和信任机制，构建云环境下基于DS理论的信任模型，为云安全问题提供了新思路。该模型在主客观信任值的基础上合成综合信任值，进行可信度判断；并讨论模型中的关键问题，包括信任值初始化和更新、恶意节点惩罚、负载均衡；再通过仿真实验从有效性、均衡性和鲁棒性等方面对模型进行验证；最后进行总结并对下一步研究进行展望。

关键词 云计算，信息安全，信任机制，DS证据理论

中图法分类号 C931.6 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.8.022

Dynamic Trust Model Based on DS Evidence Theory under Cloud Computing Environment

SHU Jian LIANG Chang-yong

(School of Management, Hefei University of Technology, Hefei 230009, China)

(Key Laboratory of Process Optimization and Intelligent Decision-making, Ministry of Education, Hefei 230009, China)

Abstract Cloud computing technology faces the new security problems of privacy disclosure and information lost. How to identify and manage the trust degree of nodes in cloud system becomes a important research area of cloud security. Then the trust model can provide a new idea to solve it. Considering that the architecture of cloud computing is a distributed system, combining with the DS evidence theory and trust mechanism, a dynamic trust model based on DS theory was built under the cloud environment. In the model, subjective and objective trust values are merged into a integrated trust-value to describe the safety and credibility of the cloud nodes. The problems of trust value initialization and updating, malicious nodes punishment and load balancing were discussed. Simulation experiment proves the effectiveness, balance and robustness of the model. Finally, the summary and the prospects for future research were put forward.

Keywords Cloud computing, Information security, Trust mechanism, DS evidence theory

1 引言

随着硬件技术的升级和信息技术的更新，云计算技术作为一项全新的计算服务交互模式，给企业生产经营和人们的工作和生活都带来了翻天覆地的变化。云计算跨平台能力实现了海量异构数据分步式的存取和利用，大大加速了信息技术的发展，降低了信息成本，提高了效率。然而，新机遇总是伴随着新的挑战，云计算技术在提供便利的同时也带来了新的安全隐患，大大拓宽了传统信息安全边界，故其面临着更高、更全面的安全需求[1]，云安全问题已经成为桎梏云计算发展的关键问题。而描述云中用户和服务节点可信关系的信任模型，为云安全问题的解决提供了关键而有效的支持[2]。

基于DS理论的云计算安全服务信任模型将云计算服务中的用户作为安全保护对象，将云中恶意服务节点作为安全防范对象。其信任值的衡量是以云用户与云服务节点之间的历史交互信息作为直接信任值评估的基础，结合DS证据理论对多个云节点的推荐信任证据组合得到多源推荐信任值，并合成综合信任值。最终通过比较不同服务安全等级的信任阈值来判断是否允许服务交互，从而保障服务的可信性和安全性。模型的基本思路如图1所示，结合云计算虚拟化和分布式计算的特征，将云计算中心看成一个服务网络形式，各节点在提供服务时是彼此独立的。

本文旨在借助分布式系统中的信任模型，建立基于DS理论的云计算安全模型。第2节介绍了相关工作和理论基础；第3节给出云环境下基于DS理论的动态信任模型；第4节列举分析了模型中的关键问题；第5节给出了仿真实验的结果和分析；最后总结全文，并指出了下一步的工作方向。

到稿日期：2015-07-07 返修日期：2015-08-29 本文受国家自然科学基金项目（71331002，71271072），高等学校博士点基金项目（20110111110006）资助。

束 柬（1989－），男，博士生，主要研究领域为云计算、信息安全、信任机制，E-mail：shujian7@163.com（通信作者）；梁昌勇（1965－），男，教授，博士生导师，主要研究领域为信息管理与信息系统、决策分析与决策支持系统、企业管理及其信息化。

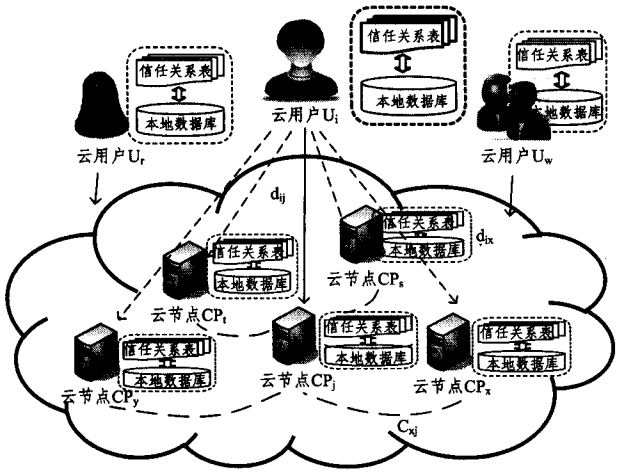

图 1　信任模型中的信任关系

2　国内外研究现状

云服务部署在分布式的互联网环境中，且云用户和云服务提供商的行为都具有动态性和不确定性，因此给云计算的安全管理带来了很大的考验[3]。近年来，传统基于攻防角度的硬安全策略（“硬安全”）逐渐难以全面覆盖云计算的安全边界[4]；而近年学术界和企业界更多地关注云计算的“软安全”问题，信任和信誉评估等都归为“软安全”的范畴。基于信任的安全模型作为云安全策略的主要手段，对其进行研究具有重要意义。

2.1　云计算环境下信任管理研究热点

目前云计算服务中的信任评估问题主要集中在以下 3 个方面。

（1）信任管理系统框架的研究，是基于某种系统结构，以某种方式进行用户的信任反馈过程，以及如何存储和发布信任信息等，目前主要的信任管理系统结构包括集中式和分布式两种。Zacharia[5] 针对 eBay 系统可能受到恶意评价攻击的问题，提出了一种迭代的集中式信任模型 Sporas。集中式信任模型出现较早，然而其存在系统负载过大、单点失效和健壮性等问题。李小勇等[6] 进行了大规模分布式环境下信任模型的研究，总结了几种典型的信任模型，如 EigenTrust 模型[7] 和 PowerTrust 模型[8]。

（2）信任评估模型的研究，是指根据收集到的实体的历史行为和其他反馈信息，经过分析、处理和计算，得到一个较为准确客观的反映实体可信度和可靠度的信任值。Jaiganesh 等[9] 提出了一种基于用户行为信任的模糊 ART 模型，其通过信任机制保护云中每个虚拟机节点中数据和资源的安全性。部分学者虽提出了基于证据理论的云计算信任模型，但这些模型仅有信任的传递和聚合两种方式，没有充分考虑信任值的更新、惩罚机制和负载均衡等。

（3）基于信任评估的服务推荐和选择的研究，是指使得用户能够自由选择或由第三方推荐满足其个性化需求且信任值高的云服务商，从而提高服务质量，降低风险[10]。朱锐等[11] 研究了基于偏好推荐的可信服务选择问题，指出基于信任的云服务推荐系统必将成为云服务选择的重要实现手段之一。Moghaddam 等[12] 提出 AgeTrust 模型，该模型将基于信任的协同过滤推荐模型与随机游走模型结合，提高了推荐可信度。

2.2　信任管理在云计算技术中的主要难点

总结目前国内外研究现状，云计算环境下信任管理的主要挑战主要体现在以下几个方面[13]：

（1）云环境下如何刻画和度量云中主体间的信任值没有得到统一定义，虽可参照分布式系统中给出的信任模型框架，但云计算系统有其特殊性，信任问题的刻画不能照搬硬套；

（2）云中各实体都有自己的既定目标，具有自治性，这就意味着各实体都追逐自身利益最大化，具有不确定性，有时会破坏整体的安全环境，如实体的欺骗行为等；

（3）云中资源分配、服务部署到实体行为都具有高度动态性，使得云中信任值的变化也始终处于动态变化中，故所建立的信任模型需动态实时捕捉云中实体可信度的变化，并在不同的上下文环境中挑战信任管理策略。

2.3　Dempster-Shafer 证据理论

Dempster-Shafer（DS）证据理论源自 20 世纪 60 年代。Dempster[14] 提出了集值映射的概念，并诱导和定义了上、下概率。随后，Shafer[15] 用信度函数对上、下概率重新进行诠释，创立了“证据的数学理论”。20 世纪七八十年代，DS 证据理论被引入人工智能领域，许多相关的理论和应用研究随之涌现。我国从 20 世纪 80 年代也逐步开展了证据理论的研究工作，出版的多部信息融合专著都对证据理论做了专门介绍[16]。证据理论作为一种不确定性推理方法，为决策级不确定信息的表征与融合提供了强有力的工具，在信息融合、模式识别和决策分析等领域得到了广泛应用[17]，是未来研究随机集的重要方法和途径之一。

故本文提出了一种基于 DS 理论的多源证据信任模型，该模型借鉴以 EigenTrust 为代表的全局推荐思想，结合基于主观评价的直接信任和基于 DS 理论融合的客观推荐信任，提出了云计算环境下的动态信任模型，并对模型中信任值的初始化、信任值的更新、恶意节点的惩罚以及节点的均衡性等关键问题进行了探讨，最后通过仿真实验加以验证。

3　云环境下基于 DS 理论的多源证据融合信任模型

3.1　主观直接信任值

主观直接信任是指用户与节点单点之间根据直接交互历史信息而产生的信任情况，表示云用户对节点的主观信任程度。本文用 d_{ij} 表示云用户 U_i 对云节点 CP_j 的主观直接信任值，设 N_{ij} 为云用户 U_i 与云节点 CP_j 在最近某个固定时间 τ 内的实际交互总次数；T_{ij} 为在云用户 U_i 看来服务可信的次数；F_{ij} 为在云用户 U_i 看来服务不可信的次数；$N_{ij}-T_{ij}-F_{ij}$ 为在云用户 U_i 看来可信度难以判断的交易次数。

当 $N_{ij}=0$ 时，则表示云用户 U_i 与云节点 CP_j 在最近某个固定时间内没有交互行为，此时云用户 U_i 与云节点 CP_j 的直接信任是不确定的，系统设置一个缺省的初始信任值 θ_1 和 θ_2。直接信任值的计算见过程算法 1。

算法 1　直接可信度评估过程及其初始化

FOR j=1:n

　IF $N_{ij}\neq 0$://U_i 与 CP_j 有历史交互

　　$d_{ij}^1=d_{ij}(\{T\})=T_{ij}/N_{ij}$

　　$d_{ij}^2=d_{ij}(\{-T\})=F_{ij}/N_{ij}$

　ELSE://历史交互总次数为 0

　　$d_{ij}^1=\theta_1$

$d_{ij}^2=\theta_2$

//θ_1,θ_2 为可信度初始值,$0<\sigma<0.5$

$d_{ij}^0=d_{ij}(\{T,-T\})=1-d_{ij}^1-d_{ij}^2$

云服务中,每个云用户都需要存储和管理一张用于信任决择的数据结构:云服务直接信任值表,如表 1 所列。该表对应附着于每个用户的账户下,用于记录节点间的历史交互情况。表中可信服务次数和不可信服务次数分别代表用户受到该节点服务中成功服务和恶意服务的次数,表中数据按照可信度的大小降序排列。

表 1 直接信任表

Node No.	Trusted service number	Fault service number	Total service number	Trusted degree
CP_1	T_{11}	F_{11}	N_{11}	T_{11}/N_{11}
CP_2	T_{12}	F_{12}	N_{12}	T_{12}/N_{12}
…	…	…	…	…

3.2 客观推荐信任值及其组合

除主观直接信任值外,还需获取虚拟节点之间的客观推荐信任值。该信任值是云节点之间对彼此客观信任程度的刻画,在每次服务交互完成后根据服务质量更新节点之间的客观推荐信任值。客观推荐信任值的管理和更新用云服务推荐信任表来表示,该表分布式存储于各个云服务节点中,记录的是该节点对其他节点的推荐信任值。考虑云计算服务中拥有海量分布式的虚拟节点,该表应尽量精简,以保证计算的收敛性和减少通信传输量。表 2 为某节点推荐信任表的示例。

表 2 推荐信任表

Node No.	Recommend trusted level	Recommend untrusted level
CP_1	c_{11}^1	c_{f1}^2
CP_2	c_{12}^1	c_{f2}^2
…	…	…

在信任评估时,本模型综合考虑多个节点的推荐信任值,结合 DS 理论的 Dempster 组合规则,将多源推荐证据融合成客观推荐信任,以刻画某云节点的客观可信度。假设某次云服务中用户 U_i 请求访问云服务节点 CP_j,该次服务的安全等级所需的推荐信任节点数为 n。根据 U_i 的直接信任表查询有过直接交互的前 n 个云节点,查询$[CP_1,CP_2,\cdots,CP_n]$对 CP_j 的推荐信任$[c_t^1,c_t^2,c_t^0]$,并合成一个 $3\times n$ 阶矩阵,用 $M_{s(n)}$ 来表示:

$$M_{s(n)}=\begin{bmatrix} c_1^1 & c_1^2 & c_1^0 \\ c_2^1 & c_2^2 & c_2^0 \\ c_t^1 & c_t^2 & c_t^0 \\ \cdots & \cdots & \cdots \\ c_n^1 & c_n^2 & c_n^0 \end{bmatrix}$$

其中,第 $t(t=1,\cdots,n)$行表示云节点 CP_t 对 CP_j 的推荐基本信任值函数,$s(n)$表示推荐节点的合集$[CP_1,\cdots,CP_n]$。

本模型考虑多个推荐节点间彼此独立,且可信证据的焦元一致。故可结合 DS 理论,采用 Dempster 规则[18,19]对矩阵 $M_{s(n)}$ 中的 n 个推荐信任值函数进行组合,得到组合推荐信度函数 $m_{s(n)}$。现给出两个推荐信任值函数的合成规则,设$n=2,s(2)=[CP_1,CP_2]$,c_1 和 c_2 分别为云节点 CP_1 和 CP_2 对某节点的推荐信任值函数,经 Dempster 组合得到其组合推荐信任值 $m_{s(2)}$。具体过程如下:

$$m_{s(2)}^1=(c_1^1\times c_2^1+c_1^1\times c_2^0+c_1^0\times c_2^1)/(1-k_{s(2)})$$

$$m_{s(2)}^2=(c_1^2\times c_2^2+c_1^2\times c_2^0+c_1^0\times c_2^2)/(1-k_{s(2)})$$

$$m_{s(2)}^0=(c_1^0\times c_2^0)/(1-k_{s(2)})$$

$$k_{s(2)}=c_1^1\times c_2^2+c_1^2\times c_2^1$$

由上得到了两个云节点的组合推荐信任值函数 $m_{s(2)}$。由此类推,可以得到 n 个推荐节点的组合推荐信任值计算公式。本模型结合 Dempster 算法的一个线性时间算法[20],给出其过程,如算法 2 所示。

算法 2 Dempster 规则合成综合推荐信任值的过程

$m_{s(1)}^1=c_{1j}(\{T\}|CP_j)$//给 $m_{s(1)}$ 初始化赋值

$m_{s(1)}^2=c_{1j}(\{-T\}|CP_j)$

$m_{s(1)}^0=c_{1j}(\{T,-T\}|CP_j)$

FOR $k=2:n\&k\neq j\&c_{kj}(\{T,-T\})\neq 1$

$t=1-c_k^1\times m_{s(k-1)}^2+m_{s(k-1)}^1\times c_k^2$

$p=c_k^1\times m_{s(k-1)}^1+c_k^1\times m_{s(k-1)}^0+c_k^1\times m_{s(k-1)}^0$

$q=c_k^2\times m_{s(k-1)}^2+c_k^2\times m_{s(k-1)}^0+c_k^0\times m_{s(k-1)}^2$

$r=c_k^0\times m_{s(k-1)}^0$

$m_{s(k)}^1=m_{s(k)}(\{T\}|CP_j)=p/t$

$m_{s(k)}^2=m_{s(k)}(\{-T\}|CP_j)=q/t$

$m_{s(k)}^0=m_{s(k)}(\{T,-T\}|CP_j)\}=r/t$

3.3 综合信任值

本文在主观直接信任值和组合的客观推荐信任值的基础上,将两者融合得到综合信任值来判断节点的可信度。设融合权重分别为 ε_1 和 ε_2,考虑直接信任值权重应大于间接信任值,要求 $\varepsilon_1\geqslant\varepsilon_2$,$\varepsilon_1+\varepsilon_2=1$。

定义 8 云用户 U_i 对云节点 CP_j 的综合信任值函数为

$$z_{ij}^1=z_{ij}(\{T\}|CP_j)=\varepsilon_1*d_{ij}^1+\varepsilon_2*m_j^1$$

$$z_{ij}^2=z_{ij}(\{-T\}|CP_j)=\varepsilon_1*d_{ij}^2+\varepsilon_2*m_j{}^2$$

$$z_{ij}^0=z_{ij}(\{T,-T\}|CP_j)=1-(z_{ij}^1+z_{ij}^2)$$

在某次云服务交互前,用户根据所需服务类型的不同,确定相应的信任阈值,通过比较综合信任值与信任阈值的大小,就可以判断该节点是否达到该项云服务所需的安全等级,并选择是否继续访问,接受节点的服务。

4 模型中的关键问题

4.1 信任值初始化

云服务来自云计算中心的海量服务节点,而节点又在时刻变化着,老的节点"死去",新的节点"出生",故云节点信任值的初始化是保证云安全模型正常运行的基础。一个新的节点首先需在云计算信任中心进行注册,获得唯一标示身份后才能以云服务节点身份提供云服务。

节点的初始化包括直接信任值初始化 θ 和推荐信任值初始化 σ。一方面,过小的初始信任值会使得新进入的服务节点达不到用户访问的信任阈值,从而使其始终得不到访问;另一方面,过大的初始信任值使得节点失去维系信任值的动力,部分恶意节点在其信任值低于阈值后,只需在云信任中心重新注册就能继续提供恶意服务,会大大降低该信任机制的有效性和敏捷性。

4.2 信任值的更新

本模型信任值的更新问题分为两部分:直接信任值的更新和推荐信任值的更新。信任值的更新都发生在每次服务交互之后,云用户会根据服务的质量和安全性反馈服务评价结果。结合 DS 理论,在识别框架 $U=\{T,-T\}$ 下,本文将反馈

结果分为:“可信”、“不可信”和“不确定”3类。具体云服务更新机制如算法3所示。

算法3 云安全信任模型信任更新机制算法

```
a,α,β// a为服务反馈结果,α,β为推荐信任更新常数
IF a=1 // a为用户的反馈结果,a=1代表可信
   T_ij=T_ij+1 and N_ij=N_ij+1
   FOR t=1:n & t≠j
      c_ij=c_ij+α
ELSEIF a=2 // 若反馈不可信
   F_ij=F_ij+1 and N_ij=N_ij+1
   FOR t=1:n & t≠j
      c_ij=c_ij-β
ELSE:
   N_ij=N_ij+1// 若反馈不确定
```

其中,a 为云服务的反馈结果,假设云用户是理性的和可信的,其反馈结果是对该次服务的客观描述。

4.3 恶意节点惩罚机制

对服务中不可信行为的惩罚机制是安全模型中剔除恶意节点的重要保证。假设某恶意节点先伪装成正常节点,提供一段时间的正常服务,其信任值将达到较高的程度,此后其提供一次恶意云服务,再提供一次正常服务。若缺乏相应的惩罚机制,该节点的信任值将始终维持在一个较高的程度,其欺骗行为无法被安全模型识别。故本模型信任惩罚机制的设置原则为:信任值易大量降低,却只能少量上升。在信任值的更新中,本模型修改信任函数,定义如下:

$$\beta=\alpha\times(1+\rho)$$

$$d_{ij}^1=\frac{T_{ij}}{N_{ij}+\rho F_{ij}},d_{ij}^2=\frac{\rho F_{ij}}{N_{ij}+\rho F_{ij}}$$

其中,ρ 为惩罚系数且 $\rho\geqslant 0$,当 $\rho=0$ 时,仍为原来的定义;而当 $\rho>0$ 时,β 大于 α,使得推荐信任值的下降幅度大于上升幅度;且在直接信任值 d_{ij} 中增加不可信服务次数 F_{ij} 所占权重。

4.4 负载均衡,避免服务热点

云计算是一种分布式计算方法,故在云服务中既要保证每个可靠节点都被充分利用,避免资源闲置浪费,也要避免因某些信任值过高的节点的访问量过大而出现服务热点的情况。一个完备的安全机制不能因为安全性的要求就牺牲其系统的可用性,应充分保障负载均衡和整体资源利用率最大化。本模型采用如下方法解决:云用户在请求服务之前,有若干个满足服务需求类型的云节点[CP_1,…,CP_n],若每次都选择访问信任值最高的节点,则会出现服务热点现象,使得部分节点一直处于被访问的状态,而其他符合服务条件的节点则分不到计算任务。因此,在本安全模型中采用随机队列抽取的方法,在[CP_1,…,CP_n]中选取信任值大于信任阈值的 m 个节点组成备选集,并从中随机选择云节点进行服务,从而避免负载均衡的问题。

5 仿真实验结果与性能分析

在理论研究的基础上,本文进行相应的仿真实验以对模型中所提出的关键问题进行实践检验,其中有效性检验保证了信任值初始化和更新的问题;鲁棒性检验保证了恶意节点惩罚机制问题;均衡性检验保证了负载均衡,避免服务热点的问题。仿真实验中,假设云计算服务都是理想的,即云中的服务都是由单个节点提供给单个用户,假定用户行为较为简单,即若对某虚拟节点的综合信任值大于信任阈值,则接受服务;反之则更换节点并重新计算信任值。在每次服务交互完成后,会更新直接信任值表和间接推荐信任值表。

5.1 云安全模型有效性检验

本组实验假设共有100个用户{U_1,U_2,…,U_{100}},每个用户 U_i 随机从500个节点{CP_1,CP_2,…,CP_{500}}中选择某个云节点 CP_j 进行服务请求,若对该节点 CP_j 的综合信任值大于信任阈值,则完成一次服务交互。假设每个用户都请求完成1000次服务交互,在理想的状态下,即无恶意节点,成功的交互次数为 10^5。本节实验列举了恶意节点数量在10%~50%之间时云服务中的交互成功总数,实验结果如图2所示。从中可看出,本模型对云计算服务中的恶意节点具有一定的遏制作用,即使在恶意节点占总服务节点一半的情况下,成功交互次数仍达80046。

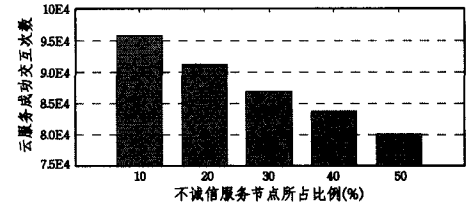

图2 不同恶意节点比例情况下云计算服务交互情况

5.2 云安全模型均衡性检验

在本组仿真实验中,为了简化,选取10个云节点对10个用户进行服务,假设每个用户请求1000次云服务。设定 CP_1 到 CP_8 为可信节点,提供正常服务;CP_9 和 CP_{10} 为不可信节点,提供恶意服务。实验结果如图3所示。

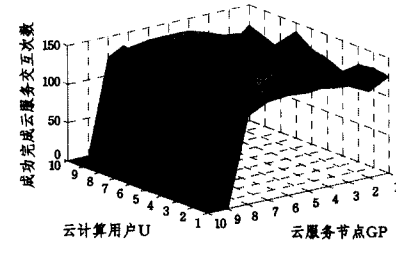

图3 云服务中用户与节点交互负载均衡情况

由于 CP_9 和 CP_{10} 为不可信节点,对其请求服务的次数极少,而 CP_1 到 CP_8 这8个云节点提供的云服务次数基本维持在100~130之间。实验证明在该安全模型的保障下,一方面,用户可以避开不可信节点,选择可信节点进行安全的交互;另一方面,云计算中心的可信节点所提供的服务次数较为平均,没有出现单个节点服务量很大的现象,有效地消除了服务热点问题,保证了负载均衡。

5.3 云安全模型鲁棒性检验

在实际环境中,恶意节点一般会伪装成正常的节点,在提供一定比例的正常服务中混杂着不可信服务;而正常节点在进行服务交互时,由于传输的延迟和网络堵塞等原因,提供的服务也有可能没有达到用户满意的程度 。因此,本节仿真实验设定,10个云节点对10个用户进行服务,假设每个用户请求完成100次服务,CP_8 为恶意节点,以33%的概率提供正常服务,以67%的概率提供不可信服务;其他9个节点为正常节点,以95%的概率提供正常服务,5%的概率提供质量较差的服务。假设用户是行为简单的,将正常服务视为合格的服务,将不可信服务和质量较差的服务都视为不合格服务。

图4示出经1000次交互后各节点对目标节点 CP_j 的推荐值对比。可见经多次交互后，正常节点 CP_3 获得高于阈值 ϕ_1 的可信推荐值和低于信任阈值 ϕ_2 的不可信推荐值，而对恶意节点 CP_8 的结果正好相反。故可证明该模型对恶意节点的伪装和隐藏有较好的甄别机制，且对正常节点的失误服务也有一定的容错性。仿真结果表明该模型具备一定的鲁棒性。

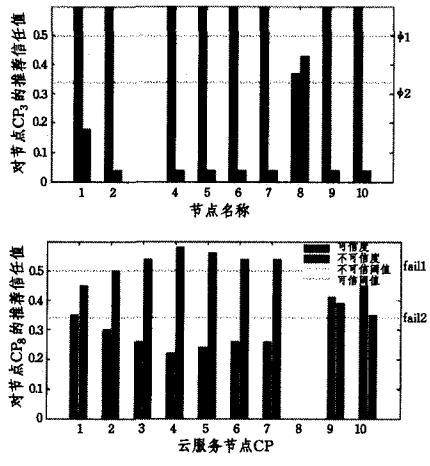

图4　恶意节点和正常节点所获得推荐信任值的对比

结束语　基于Dempster-Shafer证据理论和信任理论，提出了云计算环境下的安全服务信任模型，实现了其相应算法并展示了仿真结果。本文结合用户与云节点在交互中的服务特征，从直接信任值和推荐信任值两个维度来刻画节点的可信程度，并通过Dempster规则将多个推荐信任值组合，最终合成综合信任值，从而使得新模型的综合可信度较准确地反映了节点的行为方式。最后，通过仿真实验验证了新模型在云计算环境下的有效性、均衡性和鲁棒性等问题。将来的工作是将本文的安全模型应用到实际的云计算系统中，对本模型进一步提炼和总结，增加安全模型的维度。目前只讨论了节点对用户的安全性，信任只是单向地从用户传向云节点，下一步将研究用户同服务节点间的双向信任传递和更新机制，并结合云计算中不同的服务类别和不同的访问行为来探究不同安全等级下的信任安全机制。

参考文献

[1] Lin C, Su W B, Meng K, et al. Cloud Computing Security: Architecture Mechanism and Modeling [J]. Chinese Journal of Computer, 2013, 36(9): 1765-1784(in Chinese)
林闯，苏文博，孟坤，等. 云计算安全：架构，机制与模型评价[J]. 计算机学报，2013，36(9)：1765-1784

[2] Kirthica S, Sridhar R. Solution for Traversal Vulnerability and an Encryption-Based Security Solution for an Inter-cloud Environment [M]// Computational Intelligence in Data Mining. Volume 2, Springer India, 2015: 283-291

[3] Yu Neng-hai, et al. Review of cloud computing security[J]. Acta Electronica Sinica, 2013, 41(2): 371-381(in Chinese)
俞能海，等. 云安全研究进展综述[J]. 电子学报，2013，41(2)：371-381

[4] Feng Chao-sheng, et al. Key Techniques of Access Control for Cloud Computing[J]. Acta Electronica Sinica, 2015, 43(2): 312-319(in Chinese)
冯朝胜，等. 云计算环境下访问控制关键技术[J]. 电子学报，2015，43(2)：312-319

[5] Zacharia G, Moukas A, Maes P. Collaborative reputation mechanisms for electronic market places[J]. Decision Support Systems, 2000, 29(4): 371-388

[6] Li Xiao-yong, Gui Xiao-lin. Research on Dynamic Trust Model for Large Scale Distributed Environment[J]. Journal of Software, 2007(6): 1510-1521(in Chinese)
李小勇，桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报，2007(6)：1510-1521

[7] Blaze M, et al. Decentralized Trust Management[C]// Proceedings of 1996 IEEE Symposium on Security and Privacy. IEEE, 1996: 164-173

[8] Yang M H, Wang Z P, Yao J J. Research on a new cloud trust model and its defense abilities [J]. Manufacturing and Engineering Technology, 2014, 1(1): 399-405

[9] Jaiganesh M, Aarthi M, Kumar A V A. Fuzzy ART-Based User Behavior Trust in Cloud Computing[M]// Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, 2015: 341-348

[10] Kumar T S, Pandey S. Customization of Recommendation System Using Collaborative Filtering Algorithm on Cloud Using Mahout[M]// Intelligent Distributed Computing. Springer International Publishing, 2015: 1-10

[11] Zhu Rui, Wang Huai-min, Feng Da-wei. Trustworthy Services Selection Based on Preference Recommendation[J]. Journal of Software, 2011(5): 852-864(in Chinese)
朱锐，王怀民，冯大为. 基于偏好推荐的可信服务选择[J]. 软件学报，2011(5)：852-864

[12] Moghaddam M G, Mustapha N. AgeTrust: A New Temporal Trust-Based Collaborative Filtering Approach[C]// Preceedings of 2014 International Conference on Information Science and Applications(ICISA). 2014: 1-4

[13] Song Guo-feng, Liang Chang-yong. A cloud security access control model based on user behavior trust[C]// The 15th China Management Science Academic Essays. 2013(in Chinese)
宋国峰，梁昌勇. 一种基于用户行为信任的云安全访问控制模型[C]//第十五届中国管理科学学术年会论文集（下）. 2013

[14] Dempster A P. Upper and lower probabilities induced by a multiple valued mapping[J]. The Annals of Mathematical Statistics, 1967, 38(2): 325-339

[15] Shafer G. A mathematical theory of evidence[M]. Princeton: Princeton University Press, 1976

[16] 段新生. 证据理论与决策、人工智能[M]. 北京：中国人民大学出版社，1990：13-35

[17] Sevastianov P, Dymova L, Bartosiewicz P. A framework for rule-base evidential reasoning in the interval setting applied to diagnosing type 2 diabetes[J]. Expert Systems with Applications, 2012, 39(4): 4190-4200

[18] Dempster A. Upper and Lower Probabilities Induced by Multivalued Mapping [J]. Annalys of Mathematical Statistics, 1967, 38(2): 325-339

[19] Shafer G. A mathematical theory of evidence[M]. Princeton: Princeton university press, 1976

[20] Zhu Jun-mao, et al. A Grid & P2P trust model based on recommendation evidence reasoning. Journal of Computer Research and Development, 2005, 42(5): 797-803(in Chinese)
朱峻茂，等. Grid与P2P混合计算环境下基于推荐证据推理的信任模型[J]. 计算机研究与发展，2005，42(5)：797-803