

云计算环境下基于信任演化及集合的服务选择

胡春华^{1,2}, 刘济波¹, 刘建勋³

(1. 湖南商学院 计算机与电子工程学院, 湖南 长沙 410205; 2. 中南大学 商学院, 湖南 长沙 410083;

3. 湖南科技大学 计算机科学与工程学院, 湖南 湘潭 412201)

摘 要: 针对云计算环境中服务节点的可信度参差不齐常导致用户很难获得高质量组合服务的问题, 提出了一种基于信任生成树的云服务组织方法, 将服务提供者与请求者的交互行为经演化后形成信任关系, 使主体间可信程度达到相应级别, 形成对外提供相似服务功能的云服务集合, 将恶意、虚假的服务排除在信任生成树之外, 使服务组合在可信场景中进行; 在此基础上, 采用了基于信息熵的度量策略来对服务间的信任关系进行评估, 解决了现有研究中仅对可信参数进行简单加权分析的不足。实验分析表明, 该方法能有效抑制云计算环境下恶意节点的欺诈行为并保护真实节点的合法利益, 具有较好的服务选择质量。

关键词: 云计算; 信任推理; 信任生成树; 信息熵; 服务选择

中图分类号: TP393

文献标识码: A

文章编号: 1000-436X(2011)07-0071-09

Services selection based on trust evolution and union for cloud computing

HU Chun-hua^{1,2}, LIU Ji-bo¹, LIU Jian-xun³

(1. School of Computer and Electronic Engineering, Hunan University of Commerce, Changsha 410205, China;

2. School of Business, Central South University, Changsha 410083, China;

3. School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 412201, China)

Abstract: It was difficult for the service consumers to obtain high-quality composite services because of the existence of false or malicious service nodes in cloud computing environment. A novel cloud service-composition method based on the trust span tree was proposed. The trust relationship could be built after many times credible interaction between services requester and provider, and the trust union would be formed through the credible relationship evolution. So that the uncertain or malicious service should be excluded from the trust span tree, and the service composition would be carried out in a trust environment. At the same time, the measuring strategy of trust relationship among cloud services based on information entropy was designed, which could resolve the deficiencies of the trust parameter analysed by simply weighted angle in the previous studies. The experimental result shows that the method proposed in this paper is more superior in credibility and security, comparing to the traditional services selection methods.

Key words: cloud computing; trust reasoning; trust span tree; information entropy; services selection

收稿日期: 2011-02-16; 修回日期: 2011-06-20

基金项目: 国家自然科学基金资助项目(90818004); 湖南省自然科学基金资助项目(10JJ6110, 11JJ2033); 湖南省科技计划基金资助项目(2010JT4053); 国家教育部人文社会科学研究青年基金资助项目(10YJC630080)

Foundation Items: The National Natural Science Foundation of China (90818004); The Provincial Natural Science Foundation of Hunan (10JJ6110, 11JJ2033); The Science and Technology Program in Hunan Province (2010JT4053); The Society Science Foundation of Ministry of Education of China (10YJC630080)

1 引言

随着云计算和服务计算等相关技术的迅速发展,“网络就是计算机”的思想正变得越来越清晰。在该理念下 IT 资源服务化是其最重要的外部特征,能够将大量计算资源、存储资源与软件资源以服务(又称云服务,网格服务等)的形式链接在一起,形成巨大规模的共享虚拟 IT 资源池,为远程计算机用户提供“能力无限”的云服务资源,如云服务平台 Azure、blue cloud 等^[1,2]。由于单个云服务的功能有限,需要将云计算环境中多个服务组合成一个具有更大粒度的增值服务或系统,供其他远程用户使用。

在实际应用中,虽然云计算环境下服务资源非常丰富,但还存在动态变化、自治性强、安全难控等特征,使得用户要获得理想的组合服务还存在不少困难^[3,4]。主要原因如下。

1) 云计算环境下虽存在大量功能相同或相似,服务质量(QoS, quality of service)各异的云服务,但是网络中服务使用者(SC, services consumer)或服务提供者(SP, services provider)所宣称的 QoS 属性难以鉴别,用户选择的有效性受到限制,难选择高质量的组合服务。

2) 服务组合的各参与方可能存在恶意、欺诈或虚假的服务实体,提供了不完整、虚假甚至是恶意的服务注册信息,导致用户需经过多次请求才能获得真实服务,造成服务使用者感觉网络上的服务不可靠,容易出现真实服务被边缘化。

3) 缺乏公正且可操作强的评价机制,当前评价主要来自于使用者对服务的评价,而使用者反馈的质量信息又具有不同的可信值,例如宽容与苛刻的使用者对同一服务的评价结果将不同,恶意使用者还会给出虚假评价,同时现有评价机制对使用者和提供者共同欺骗等恶意行为缺乏深入考虑。

因此如何建立可信的服务评价机制使真实服务能获得较高的信任评价,而“恶意”服务的信任评价将会降低,并使其逐步边缘化,以保障服务使用者快速有效地获得所需服务,是一项值得深入研究的课题。

本文提出云计算环境下的服务资源通过可信服务演化机制,形成信任集合和集合体的有效策略,在基础上设计了一种基于信息熵的可信服务选取策略。通过研究服务提供者与使用者经可信交互

后形成的信任关系,将可信度高的 SP 和 SC 进行可信演化形成相应的信任集合,从而将恶意虚假的云服务排除在信任集合之外,实现服务调度在可信的环境中进行;同时采用基于信息熵的服务选取策略对服务间的信任关系进行度量,避免了以往研究中对多维可信指标简单加权的不足。经实验分析表明该方法能有效抑制网络中恶意节点的欺诈行为并保护真实节点的合法利益,具有良好的服务组织质量。

2 相关工作

云计算和服务计算环境下,关于服务组合中服务选择问题研究,国内外学者已开展了较深入地分析,提出了例如基因算法^[5]、PSO 算法^[6]、启发式算法^[7]、线性规则的方法^[8]、动态规则算法^[9]等有效方法。但这类方法都需具备以下前提条件:①选择算法的执行者对网络中的所有服务都是了解的;②这些服务所能够提供的服务质量也是清楚的;③服务所提供的信息都是真实可信的。显然,网络中服务常常动态产生,又随机消失,服务调度方法不可能对相关服务都能知晓,而且在纷繁复杂的互联网中假设所有的服务都真实是不现实的。

针对上述情况,提出服务选取的前提是要保证服务提供者信息的真实性,否则服务选取算法所依赖的基础就成问题。因此,有的研究人员提出了采用声誉机制的方法。文献[10]提出基于单声誉系统的方法,但过度依赖服务消费者(consumer)的回馈,不能处理消费者不汇报回馈的情况。文献[11]提出基于双层的声誉系统,但两层反馈的信息不一致时,难确定谁是真正的撒谎者。文献[12]提出了采用声誉机制的方法,让恶意的、虚假的服务其声誉就低,而真实的服务其声誉就高。文献[13]针对在线演化对服务评估高效性的要求,通过引入一个相关因子量化不同上下文中的推荐信任关系,得到信任可传递空间通过主体群内的信任传递与迭代计算,能有效确定具有高声誉值的推荐信息源。在服务组合时除了采用服务所宣称的服务质量进行组合外,再参考其声誉度,比只考虑服务所宣称的质量所得到的组合质量就会更理想,虽还未有较为成熟的方法,但显然是一个值得研究的方向。

文献[14]以服务主体对推荐者的信任关系为信息权重,经合并演算后得到服务的性能评估值。由于 Web 服务主体的表现存在个体差异,不同的度量

方式将得到不同的满意值，可能导致评估推荐信息时存在偏差。文献[15]提出了一种考虑 QoS 数据可信性的服务选择方法，通过依据服务实体的可信度对其 QoS 数据进行修正，包括对服务和使用者的 QoS 进行修正，得到的 QoS 属性较能够准确反映实体的真实情况，因而得到的服务组合质量相对较高。文献[16]对兴趣相近的服务使用者分配较高的信任值，寻求推荐信息时从相邻推荐者出发，推荐信息可信度随着链长衰减。文献[17]在此基础上利用服务本体模型描述了每个服务推荐者对于服务需求侧面的概念层次关系，并以此作为其推荐信息的参考权重，取得了较理想的实验效果。

此外，文献[18,19]在基于信任 QoS 以及信任推理的 Web 服务组合方面取得了一些研究成果，本文是在文献[19]的基础上进一步深入和跟踪研究。

3 可信服务演化机制研究

可信服务演化机制研究主要目标是对云服务间信任关系的发展进行合理度量和有效分析，实现真实服务主体能进行有效演化和自组织，而虚假服务主体常屏蔽在信任服务集合之外，从而提高云计算环境下服务选择的有效性。

3.1 服务主体的可信度量 and QoS 度量

假设云计算环境中存在 N 个服务主体 $X = \{x_1, x_2, \dots, x_N\}$ ，其中， $x_i (x_i \in X)$ 为第 i 个服务主体。根据担任角色的不同，主体分为服务提供者和服务使用者 2 种类型。

本文采用文献[5]给出的服务质量定义和主要属性，主要包括执行时间(T)、执行费用(C)、可信度(credibility)、声誉度(reputation)等性能指标。信任服务选择问题实际是一个服务消费者寻找可信度高的服务组合路径问题，显然可信度是其中最关键的指标，服务主体的声誉度只是为 SC 主观选择的参考。为了研究问题的简单，本文将可信度从 QoS 指标中独立出来研究，即以下的 QoS 指标中不含可信度等信任指标。

假设服务主体宣称的服务质量指标集合为 $Q^0 = \{Q_1^0, Q_2^0, \dots, Q_M^0\}$ ，而服务主体 x_i 对主体 x_j 实际交互时得到的服务质量指标分别表示为 $Q = \{Q_1(x_{ij}), Q_2(x_{ij}), \dots, Q_M(x_{ij})\}$ ，并设定其中的每个元素 $0 \leq Q_m(x_{ij}) \leq 1 (m = 1, 2, \dots, M)$ ，称为一个评价参数 (VP, value parameter)。

同时设 ϕ_m 为第 m 个 VP 相对于其他 VP 的重要性程度，且 ϕ_m 满足：

$$\sum_{m=1}^M \phi_m = 1, 0 \leq \phi_m \leq 1 \quad (1)$$

则称 ϕ_m 为 $Q_m(x_{ij}) (m = 1, 2, 3, \dots, M)$ 的权值。

定义 1 用 $f_{ij}^{(t)}$ 表示云服务 x_i 对 x_j 一次交互过程中的 QoS 评价。

$$f_{ij}^{(t)} = f(x_i, x_j, s, t) = \sum_{m=1}^M \phi_m Q_m(x_{ij}) \quad (2)$$

其中， s 是 x_i 提供的服务质量等级， t 是服务交互的时间片段，为了提高云计算环境中服务交互行为的信任评估能力，将交互中的时间段分为若干个小时片 t_i ， t_i 能反映该时刻服务主体的服务质量评价，并随时间变化且衰减^[19]。

定义 2 用 T_{ij} 表示服务主体 x_i 对 x_j 主体多次交互的 QoS 评价。

服务主体 x_i 与 x_j 在最近 d 次直接交互中得到 x_j 的性能评价为 $F_{ij} = \{f_{ij}^{(1)}, f_{ij}^{(2)}, \dots, f_{ij}^{(d)}\}$ ，其中， $0 \leq f_{ij}^{(k)} \leq 1, k \in [1, d], d \neq 0 < H$ ， F_{ij} 因子按照服务交互行为中的先后顺序进行排列， $f_{ij}^{(d)}$ 因子表示服务交互过程中最近的一次行为， $f_{ij}^{(1)}$ 则表示最久的一次交互行为， H 为服务交互中最大的交互次数。则 x_i 对 x_j 得到的服务质量为

$$T_{ij} = \sum_{k=1}^h \frac{1}{d} \mu(k) f_{ij}^{(k)} \quad (3)$$

其中， $\mu(k) \in [0, 1]$ 是衰减函数，用于表达不同时刻服务交互中信任信息的合理权值，根据现实生活中的行为习惯特征，可以对于最近发生的交互行为给予更高的权值，故其可表示为

$$\mu(k) = \begin{cases} 1, & k = d \\ \mu(k-1) = \mu(k) - 1/d, & 1 \leq k < d \end{cases} \quad (4)$$

定义 3 用 $C_m(x_i, x_j, s, t)$ 表示主体 x_i 对主体 x_j 多次交互的可信度评价。

令：

$$C_m(x_i, x_j, s, t) = \sum_{k=1}^h \frac{1}{d} \mu(k) C_{ij}^t \quad (5)$$

其中， $C_{ij}^t = \sum_{m=1}^M \phi_m (Q_m(x_{ij}) - Q_m^0)^2$ ，表示服务主体 x_i 对主体 x_j 一次交互的可信度，计算时将 C_{ij}^t 按照其

交互的时间顺序排列, 计算过程与定义 2 相似, $\mu(k) \in [0,1]$ 是衰减函数, 与定义 2 中的含义相同。

定义 4 用 $C_i(x_i, s, t)$ 表示服务主体 x_i 总的可信度。所有与主体 x_i 交互过的服务主体对其可信度的总体评价, 用加权平均表示。

$$C_i(x_i, s, t) = \sum_{j=1}^m \sum_{j=1}^n \eta_{ij} C_m(x_i, x_j, s, t) \quad (6)$$

其中, $\eta_{ij} = \frac{C_m(x_i, x_j, s, t)}{\sum_{i=1}^m \sum_{j=1}^n (1 - C_m(x_i, x_j, s, t))}$ 表示不同信任的

主体对其所作出的评价权重, 可信度高的主体所做的评价权重较大, 反之将较小^[19]。

可信度越高表示服务主体 x_i 所宣称的越真实;

反之, 表示其行为与其宣称的属性不符。

由此可以看出 SP 和 SC 的可信度含义稍有不同, 其中, SP 是表示其提供的服务与其宣称的是否相符, 而 SC 是表示其所做出的评价是否真实。

定义 5 用 Y_i 表示对服务主体 x_i 的总体服务质量评价。

$$Y_i = \sum_{j=1}^n \kappa_{ij} T_{ij} \quad (7)$$

其中, $\kappa_{ij} = \frac{(1 - C_i(x_i, x_j, s, t))}{\sum_{j=1}^n (1 - C_i(x_i, x_j, s, t))}$ 表示不同可信度的

服务主体对 Y_i 所作出的评价权重, 可信度高的主体所做的评价权重较大, 反之将较小; T_{ij} 为定义 2 中主体 x_j 对 x_i 做的服务质量评价, 与 x_i 交互的服务主体共有 n 个。

由上式可知服务主体 x_j 可信度 $C_i(x_j, s, t)$ 越高, 表示 x_j 的评价越真实, 因而所占权重越高, 反之, 所占的权重越小。

3.2 可信服务集合体的形成

服务经过可信演化后, 服务主体间可信程度达到相应等级, 形成对外提供相同(相似)服务功能的可信服务联盟, 称为信任集合。虽然信任集合中每个服务的可信度可由定义 4 得到, 但集合的总体可信度不能够用简单加权来完成。

3.2.1 信任集合的可信度计算

由于活跃的服务与外界交互的次数多, 使得服务使用者感觉该组织的可信度主要由这些活跃服务决定, 不活跃的服务对可信集合的信任度影响较

小。因此, 可信集合的总体可信度计算应以服务的活跃程度为权重, 服务间交互次数越多, 说明其活跃程度也就越高。由此可得:

$$A(x_i) = \beta(m_i) \quad (8)$$

其中, $A(x_i)$ 为第 i 个服务主体的活跃度, x_i 为第 i 个服务主体; $\beta(m) = 1 - \frac{1}{m + \alpha}$, α 为正常数, 用于影响服务可信度 $C_i(x_i, s, t)$ 趋于 1 的速度, m_i 为所有与服务 x_i 有交互行为的服务主体个数^[19]。

由式(8)可以看出 m_i 决定服务主体活跃度 $A(x_i)$, 与其交互的服务主体越多, $A(x_i)$ 值越大。所以服务主体 i 在集合中的权重值可以表示为

$$\delta_i = \frac{A(x_i)}{\sum_{j=1}^n A(x_j)} \quad (9)$$

从而可得信任集合的可信度为

$$C_U(u_i, s, t) = \sum_{j=1}^n \delta_j C_i(x_i, s, t) \quad (10)$$

3.2.2 信任集合体的形成

服务使用者依据服务组合的交互过程, 如果服务集合间因经常存在的服务组合行为, 而使“上游”与“下游”间服务交互达到了一定的信任级别, 这样将服务组合路径上的服务集合经过信任演化后形成更大的能提供部分完整组合服务功能的大服务集合称为信任集合体。这样不仅可以进行单个服务选择, 还可以对可信度高的服务路径进行选择, 提高服务选择的效率, 如图 1 所示。

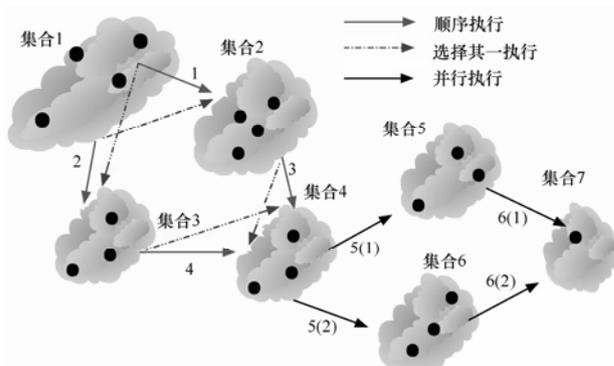


图 1 集合与信任集合体的关系

同样, 可以得到信任集合体的可信度, 其可信度与单个信任集合有所区别。具体计算方法与文献[20]的 Rep 类似, 只是将文献[20]单个服务的 Rep 用服务集合的可信度代替就可以。由于篇幅限

制，在此不再列出，具体可参见文献[20]。

多个服务组合形成一个组合服务，这时组合服务的服务质量指标的计算依据组合类型可分为4种^[5]，并分别给出了这4种类型的计算方法，例如串联模型的服务质量指标计算方法如下：

$$T_{uc} = \sum_{i=1}^n T_i, \quad C_{uc} = \sum_{i=1}^n C_i,$$

$$R_{uc} = \prod_{i=1}^n R_i, \quad \text{Re } p_{uc} = \sum_{i=1}^n \text{Re } p_i / n$$

3.3 可信服务的演化机制

上节主要论述了服务、信任集合、信任集合体的可信度计算方法以及主体的服务质量指标的度量方法。

本节将分析网络中可信服务主体随着交互行为可发展并更新形成信任集合的过程，信任集合采用定义6中信任生成树进行管理。

定义6 信任服务生成树 (CSST, credible services span tree)，简称为信任生成树，用无权无向图表示，即 $G=(V, E)$ ，其中 $V=n$ ，是树中服务节点的个数，每个服务的总体可信度可以表示为 $C_i(x_i, s, t)$ ， $E=m$ ，是树中边的个数，表示信任集合体的个数。

对应于网络中具有某类服务功能的信任集合 i 形成信任服务生成树 $CSST_i$ ，每棵树都由主、副2个令牌节点负责树中所有信息的维护，并和云计算的服务注册中心交互信息。信任集合的形成、演化和维护机制如下。

Step1 当 SP_i 申请加入某信任集合发出申请报文 (Join-Probe)，申请加入 $CSST_i$ 。

Step2 $CSST_i$ 根据 SP_i 的申请，核定该服务所具有的功能是否符合所需；若不符合将转向 Step7。

Step3 若功能符合所需，将赋予 SP_i 以候选服务的角色，只拥有服务组合等基本功能，不享有生成树内其他成员拥有的权利。

Step4 候选服务 SP_i 近期与其他服务交互次数达到了 k 次后，将进行可信度计算，由定义4计算其总体可信度。

Step5 如果可信度大于整个集合可信度的平均值 $C_i^a(u_i, s, t)$ ，且则将其转化为正式服务，该服务加入成功；否则转向 Step4。

Step6 通过对信任集合内所有云服务的交互行为进行信任计算，当云服务的可信度低于标准阈

值水平时，将其变为虚假服务，即非集合内服务。

Step7 退出 $CSST_i$ 。

显然，采用这种分布式自我维护的信任生成树来管理云服务的信任演化并聚集成信任集合的过程，具有以下优点。

1) 保证了服务的可信度。真实可信的服务将通过演化形成信任集合，用信任生成树进行管理，导致恶意或虚假的云服务无法加入该组织中，即使采取欺骗或伪装的方法加入集合中，如在交互中出现了不诚实行为，还容易被发现并踢出组织，保证了服务在可信的环境中进行。

2) 提高了服务的可用性。云计算环境下，采用生成树的形式来组织某类信任服务节点，有效减少其直接与注册中心的交互所带来的负载压力，这种组织结构虽内部服务动态性很大，但作为一个整体仍能有效对外提供服务，大大提高了服务的可用性。

4 基于信息熵的服务选择策略

在服务组合的实际中，服务选择代理如何在信任集合中为服务使用者选择合适的服务，是一项值得深入研究的内容。

云计算环境下的服务选择不仅与云服务的可信度有关还和其 QoS 值也有关联，例如某云服务主体的可信度为 70%，这表明其还有 30% 的不可信成分，而这不可信成分可使云服务组合过程中面临 30% 的风险。以往研究中有的仅考虑交互过程的可信度，其可信性指标以 QoS 的指标来代替；而有的仅从纯 QoS 选取角度来考虑，缺乏对服务可信度的深入分析。本文认为服务组合过程中可信与服务质量是相关的性能指标，仅考虑其中一个均不太合理。

信息熵是由香农(Shannon)将热力学熵引入信息论中用于度量信息量的一个概念，常被用于较粗略给出信息的不确定性度量值。信息熵在事件发生之前，它是结果不确定性的量度；在事件发生之后，它是从该事件中所得到的信息量度。因此，事件的信息熵既是一个事件信息量的量度，又可包含为事件本身中的相关信息^[21]。

由上述表示可得，服务质量 Y_i 所确定的信息熵为

$$H(Y_i) = -Y_i \text{lb} Y_i - (1 - Y_i) \text{lb}(1 - Y_i)$$

可信度 $C_i(x_i, s, t)$ 所确定的信息熵为

$$H(C_i(x_i, s, t)) = -C_i(x_i, s, t)\text{lb}C_i(x_i, s, t) - (1 - C_i(x_i, s, t))\text{lb}(1 - C_i(x_i, s, t))$$

服务质量所占的权重为

$$\delta_1 = \frac{H(C_i(x_i, s, t))}{H(Y_i) + H(C_i(x_i, s, t))}$$

可信度所占的权重为

$$\delta_2 = 1 - \delta_1$$

其中, $C_i(x_i, s, t)$ 意味着主体 i 可信度的高低, 而 $1 - C_i(x_i, s, t)$ 表示不可确定性成分 (不肯定的成份); Y_i 为主体 i 的服务质量评价, 而 $1 - Y_i$ 表示为其服务质量中的不确定性成分。

例如, 对于 2 个主体 i 和 j 的测量值分别为

$$\begin{bmatrix} Y_i & 1 - Y_i \\ 0.9 & 0.1 \end{bmatrix}, \begin{bmatrix} Y_j & 1 - Y_j \\ 0.7 & 0.3 \end{bmatrix}$$

则:

$$H(Y_i) = -0.9\text{lb}0.9 - 0.1\text{lb}0.1$$

$$H(Y_j) = -0.7\text{lb}0.7 - 0.3\text{lb}0.3$$

显然 $H(Y_j) > H(Y_i)$, 说明 $H(Y_j)$ 比 $H(Y_i)$ 的平均不确定性要大, 如果在服务交互动作发生之前, 两者是等概率事件, 难以预测下一步将要发生何种行为^[21]。因此, 云服务 QoS 熵值 $H(Y_i)$ 虽存在不确定的问题, 但可参考文献[21]大致预知 $H(Y_i)$ 出现的概率; 同时可根据信息熵来确定交互过程中可信度与其 QoS 在整个评价体系中所占的权重。例如某服务主体的(服务质量, 可信度)为(0.6, 0.8)。那么它们的信息熵分别计算为(0.970 8, 0.720 5), 因而给这 2 个评价指标的权重应该为(0.426, 0.574)。

表 1 信息熵及权重的计算

指标	服务质量	可信度
值	0.6	0.8
1-值	0.4	0.2
信息熵	0.970 8	0.720 5
权重 δ_i	0.426	0.574

根据信息熵计算出进行服务选择时的总体评价应为

$$\Delta(x_i, s, t) = \delta_1 Y_i + \delta_2 C_i(x_i, s, t) \quad (11)$$

当 SC 请求信任生成树提供服务时, 其选择思路如下: 当选择 Agent 接收到服务组合的请求后,

先在信任集合中进行选择, 选取可信度最高的服务集合 C_U^{\max} , 这时不考虑组合过程的服务质量, 因为该信任集合的信任生成树中有多个服务可供选择, 因此第 1 步选择最佳的信任集合。当相应的信任集合被选择后, 从该集合中选取可信度和 QoS 值均高的云服务, 并依据定义 4 计算得到该服务主体的可信度 $C_i(x_i, s, t)$, 利用定义 5 得到服务的总体服务质量 Y_i , 再依据式(9)计算得到其相应的权重。最后根据式(11)得到该云服务的总体评价 $\Delta(x_i, s, t)$, 返回 $\Delta(x_i, s, t)$ 值最大的一组云服务主体给服务消费者。

下面给出云计算环境中基于信任演化及集合的服务调度方法。

Step1 SP 中的服务选择 Agent 收到 SC 提出的服务组合请求。

Step2 Agent 根据 SC 的请求选取其中可信度高的信任集合 C_U^{\max} 或信任集合体, 其中信任集合的可信度由式(10)计算可得。

Step3 由该信任集合的信任生成树依据定义 4 计算获得可选服务的可信度 $C_i(x_i, s, t)$ 。

Step4 由定义 5 得到该信任生成树中可选服务的总体服务质量 Y_i 。

Step5 根据式(11)计算得到选择服务的总体评价 $\Delta(x_i, s, t)$ 。

Step6 返回一组具有最大 $\Delta(x_i, s, t)$ 的可选服务给 SC 进行服务组合。

5 实验与结果分析

为了更深入地阐述云计算环境下基于信任集合的服务调度策略的意义和作用, 将通过实验验证所提出的服务调度算法对服务组合效率的影响, 来证明该方法的有效性。

5.1 实验场景设置

实验运行在本课题组前期开发并升级形成的服务组合性能评价系统 SWES 中, 该实验系统由用户流程定制器、服务注册中心、调度算法库、实验日志组等部件构成。

在本模拟实验中, 设定服务提供者和服务消费者的身份相互独立, 且互不影响。同时将 SC 的类型分为以下 4 类。

- 1) A 类主体, 总能提供真实的服务评价。
- 2) B 类主体, 有时对交互主体给出扩大的评价 $C_{ij}^c + \eta(1 + \nu)$; 有时对其他主体作出缩小的评价

$$C_{ij}^t - \eta(1 + \nu)。$$

3) C 类主体，对与其交互的主体总给出相反的评价，但未与其他同类共谋。

4) D 类主体，是一类恶意主体，对共谋圈内的主体总是以正面的方面来进行评价，从而提高其共谋者的声誉，对共谋圈外的主体评价是随意变化的。

SP 所提供服务性能分为 3 种类型。

1) A 类主体，提供的服务真实可靠。

2) B 类主体，提供虚假服务，有共谋同伙，在共谋主体的虚假评价下拥有一定的声誉值，实际上是提供某类恶意或虚假的云服务。

3) C 类主体，随服务交互时间的不断变化，将不时提供某类真实或虚假服务给 SC。

在验证实验中，假定云计算环境下 SP 主体的个数为 1 000，SC 主体的个数为 100。向服务选择的方法输入参数 N 、 S 、 H 、 δ 说明见表 2。

表 2 模拟实验参数说明

参数	缺省值	描述
运行参数	N	1 100 主体总个数
	S	50 模拟次数
算法参数	H	20 有效最大历史记录数
	α	1 调节常数

5.2 实验结果分析

本实验的目的是对云计算环境下各种恶意或虚假服务的行为进行检测，验证本文提出的方法能否将真实可信的服务主体有效组织起来，形成信任集合，并探讨该服务选择方法对服务组合效率的影响，主要从服务组合的成功率和执行时间等性能指标检测。

实验 1 图 2 给出了 3 类服务提供者在服务主体交互过程中可信度的变化情况。从图中可以看出 A 类真实的 SP 随着交互次数的增多，其可信度也随着增长；B 类 SP 虽是虚假服务，但有共谋主体，因此其可信度随着交互次数的增加迅速下降，因有其他虚假服务的帮助，所以其下降幅度比 C 类 SP 要好些；C 类服务主体因随时间动态变化，不定期提供真实或虚假服务，其可信度随着交互次数的增加而变化不大；以上实验结果与利用定义 4 进行理论分析所得的结果较相符。

实验 2 图 3 表示云计算下服务主体随着交互次数的变化，可信服务能跟随交互场景逐渐形成信任集合，随着交互次数的增加，真实服务进入信任集合的数目也将增加，可信的服务经过演化终将被

组织进信任集合之中。而恶意或虚假的云服务主体在信任演化开始时，因部分服务选择过程由非 A 类 SP 主体参与完成，但随着服务信任演化及集合的形成，这些不诚实的服务交互行为将被逐步检测出来，其参与真实服务组合过程机会将逐步变小。

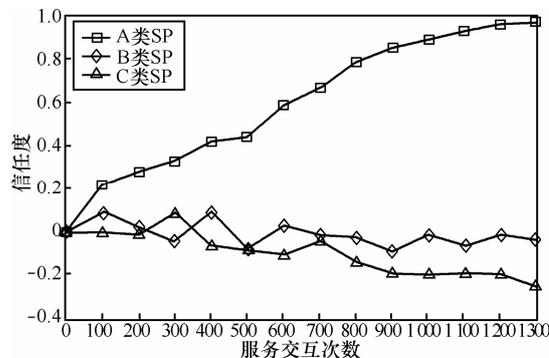


图 2 3 类 SP 随交互过程的可信度变化情况

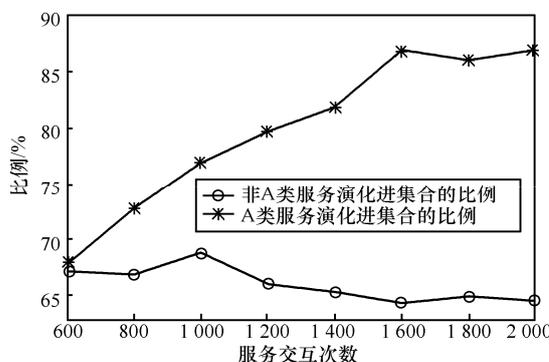


图 3 可信服务加入信任集合的比例

实验 3 图 4 表示了可信演化过程中，非诚实(虚假)的服务使用者 SC 在可信评价中所起的作用，从图中可以看出非诚实服务主体在整个可信演化与评价中所起的作用较弱，说明了本文提出的方法能够弱化恶意的 SP 与 SC，使这些恶意的 SP 和 SC 边缘化，从而使真实的服务主体化。

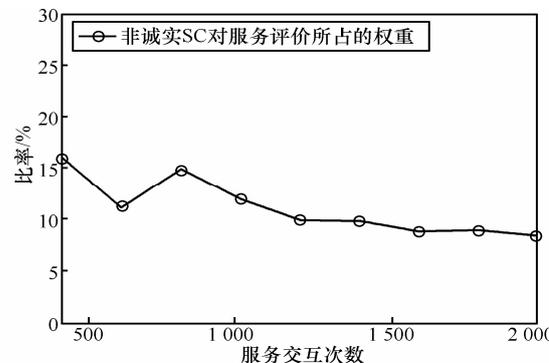


图 4 加入恶意服务的的服务组合比率

实验 4 图 5 表示服务组合过程是随着服务交互次数的增多,可信服务演化机制能对云服务进行了有效组织,形成将恶意或虚假服务进行有效限制的信任集合,从而使得整个服务组合过程的成功率越来越高,服务选择的效果越来越好。而无可信演化机制的服务选择方法,由于恶意、虚假的服务存在以及可信度不高的服务较多,导致其服务选择的成功率始终不高。

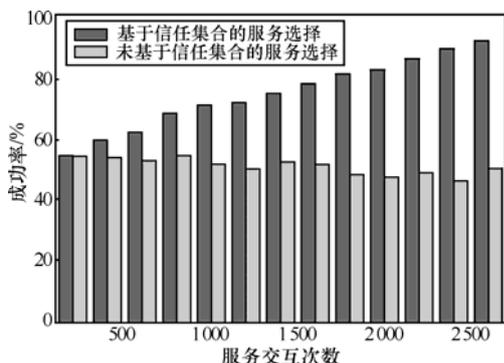


图 5 服务选择的成功率比较

实验 5 其目的是为了比较云计算环境下 2 种服务选择算法对服务组合执行时间的影响,服务组合执行时间可以用服务跳数 (hop) 来度量^[6]。从图 6 可以看出在服务组合执行初期,由于服务选择算法要寻找可靠性“最佳”的执行路径,需要花费一定时间,因而在开始阶段,基于信任集合的算法比一般算法在服务组合时间的开销上要大;但随着执行的开展,在信任集合形成后,尤其服务信任集合体形成后,基于信任集合的服务选择算法并不随着服务节点的增加而迅速增加执行时间,表明该算法能记忆执行成功的路径,达到了算法设计的要求。

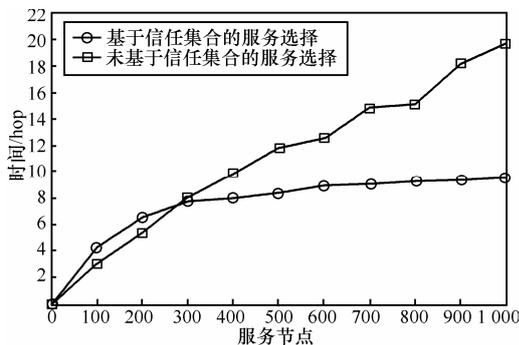


图 6 服务选择的时间比较

6 结束语

本文针对云计算环境下因服务资源的可信度

参差不齐常导致用户很难获得高质量的组合服务问题,提出了一种基于信任生成树的可信服务演化机制,使得虚假和恶意服务经演化后能排除在系统之外,实现了服务组合过程在可信的环境中进行;在此基础上,采用了基于信息熵的信任度量策略对可信服务进行选取,解决了现有研究中仅对可信参数进行简单加权分析的不足。经过实验分析表明该方法能有效抑制网络中恶意服务节点的欺诈行为并保护真实节点的合法利益,能较好地满足服务组合的相关要求。

参考文献:

- [1] ARMBRUST M, FOX A, GRIFFITH R, *et al.* A view of cloud computing[J]. Communications of the ACM, 2010, 53(4): 50-58.
- [2] 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.
- [3] ARDAGNA D, PERNICI B. Adaptive service composition in flexible processes[J]. IEEE Transactions on Software Engineering, 2007, 33(6): 369-384.
- [4] LIMAN N, BOUTABA R. Assessing software service quality and trustworthiness at selection time[J]. IEEE Transactions on Software Engineering, 2010, 36(4): 559-574.
- [5] 代钰, 杨雷, 张斌等. 支持组合服务选取的 QoS 模型及优化求解[J]. 计算机学报, 2006, 29(7): 1167-1178.
DAI Y, YANG L, ZHANG B, *et al.* QoS for composite Web services and optimizing[J]. Chinese Journal of Computers, 2006, 29(7): 1167-1178.
- [6] HU C H, WU M, LIU G P. QoS scheduling algorithm based on hybrid particle swarm optimization strategy for Web services workflow[A]. 6th International Conference on Grid and Cooperative Computing[C]. Piscataway: IEEE Computer Society, 2007. 330-337.
- [7] OH S C, LEE D W, KUMARA R T S. Effective Web service composition in diverse and largescale service networks[J]. IEEE Transactions on Services Computing, 2008, 1(1): 15-32.
- [8] ROSENBERG F, CELIKOVIC P, MICHLMAYR A, *et al.* An end-to-end approach for QoS-aware service composition[A]. 13th IEEE International Enterprise Distributed Object Computing Conference[C]. 2009. 151-160.
- [9] YANG X, SUSAN D U. The deltagrid service composition and recovery model[J]. International Journal of Web Services Research, 2009, 6(3): 35-66.
- [10] DAMIANI E, VIMERCATI D C, PARABOSCHI S. A reputation based approach for choosing reliable resources in peer-to-peer networks[A]. Proceedings of the 9th ACM Conference on Computer and Communications Security[C]. 2002. 18-22.

- [11] JURCA R., FALTINGSI B. Eliciting truthful feed-back for binary reputation mechanisms[A]. Proceedings of the 2004 IEEE/WIC/ ACM International Conference on Web Intelligence[C]. 2004. 214-220.
- [12] 陈志刚, 刘莉平, 刘安丰. 基于黑白板的信任敏感服务组合策略[J]. 通信学报, 2010, 31(6): 25-35.
CHEN Z G, LIU L P, LIU A F. Trust-sensitive Web service composition strategy based on black and white board[J]. Journal on Communications, 2010, 31(6): 25-35.
- [13] 潘静, 徐锋, 吕建. 面向可信服务选取的基于声誉的推荐者发现方法[J]. 软件学报, 2010, 21(2): 388-400.
PAN J, XU F, LV J. Reputation-based recommender discovery approach for service selection[J]. Chinese Journal of Software, 2010, 21(2): 388-400.
- [14] DAY J, DETERS R. Selecting the best Web service[A]. Proceedings of the 14th Annual IBM Centers for Advanced Studies Conference[C]. 2004. 293-307.
- [15] 李研, 周明辉, 李瑞超等. 一种考虑 QoS 数据可信性的服务选择方法[J]. 软件学报, 2008, 19(10): 2620-2627.
LI Y, ZHOU M H, LI R, *et al.* Service selection approach considering the trustworthiness of QoS data[J]. Chinese Journal of Software, 2008, 19(10): 2620-2627.
- [16] GOLBECK J. Generating predictive movie recommendations from trust in social networks[A]. Proceedings of the 4th International Conference on Trust Management[C]. 2006. 93-104.
- [17] SENSOY M, YOLUM P. Ontology-based service representation and selection[J]. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(8): 1102-1115.
- [18] 胡春华, 吴敏, 刘国平. Web 服务工作流中基于信任关系的 QoS 调度[J]. 计算机学报, 2009, 32(1): 42-53.
HU C H, WU M, LIU G P. QoS scheduling based on trust relationship in Web service workflow[J]. Chinese Journal of Computers, 2009, 32(1): 42-53.
- [19] 刘济波, 朱培栋. 面向信任演化与联盟的服务组合研究[J]. 计算机工程与应用, 2009, 45(13): 244-248.
LIU J B, ZHU P D. Research on composition based on credit evolution and alliance[J]. Computer Engineering and Application, 2009, 45(13): 244-248.
- [20] KUMAR S, MISHRA R B. A hybrid model for service selection in semantic Web service composition[J]. International Journal of Intelligent Information Technologies, 2008, 4(4): 55-69.
- [21] 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.

作者简介:



胡春华 (1973-), 男, 湖南新化人, 博士后, 湖南商学院副教授, 主要研究方向为服务计算、可信计算。



刘济波 (1962-), 男, 山东济南人, 湖南商学院教授, 主要研究方向为服务计算等。



刘建勋 (1970-), 男, 湖南衡阳人, 博士, 湖南科技大学教授, 主要研究方向为服务计算、可信计算等。