

服务计算环境下的信任评估模型^{*}

张永胜^{1a,2}, 吴明峰^{1a,2}, 郑志华^{1a,2}, 李园园^{1a,2}, 傅孟霞^{1b}

(1. 山东师范大学 a. 信息科学与工程学院; b. 传媒学院 济南 250014; 2. 山东省分布式计算机软件新技术重点实验室, 济南 250014)

摘要: 分析了传统信任评估模型, 论述了基于信任的扩展 SOA 模型和信任建模方法, 根据第三方代理的推荐信誉看法和团体信誉看法, 提出了一种新的服务计算信任评估安全模型(SOC-TrustSM)。SOC-TrustSM 在传统信任评估模型的基础上, 引入了第一手、第二手、第三手的推荐信誉看法及团体信誉看法, 能够较准确地获得服务计算环境下获信代理的信任值, 可以有效地抵御代理间的恶意推荐行为。

关键词: 服务计算; Web 服务; 访问控制; 团体信誉; 可信度

中图分类号: TP393.04 **文献标志码:** A **文章编号:** 1001-3695(2012)07-2693-03

doi:10.3969/j.issn.1001-3695.2012.07.080

Trust evaluation model in services computing

ZHANG Yong-sheng^{1a,2}, WU Ming-feng^{1a,2}, ZHENG Zhi-hua^{1a,2}, LI Yuan-yuan^{1a,2}, FU Meng-xia^{1b}

(1. a. School of Information Science & Engineering, b. School of Communication, Shandong Normal University, Jinan 250014, China; 2. Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250014, China)

Abstract: On the basis of analysis of the traditional trust evaluation model's advantages and disadvantages, trust concept and trust calculation methods, according to the third party agent reputation and group recommended opinions, this paper proposed a new trust evaluation security model in the environment of service computing (SOC-TrustSM). On the basis of traditional trust evaluation model, SOC-TrustSM introduced the thought of first or second or third-hand view and group credit view. SOC-TrustSM can effectively evaluate the agency credibility of both sides in the environment of service computing, and resist malicious recommendation behavior of agency effectively.

Key words: services computing; Web services; access control; group credit; trust level

服务计算(services computing, SC)利用服务作为基本组件来开发应用系统。Web 服务是 SC 的核心支撑技术,它是一种新型的分布式计算模式,凭借其动态性、松散耦合、语言与平台无关等特性而成为企业异构平台应用集成的最佳选择。随着 Web 服务应用规模的不断扩大,涉及的 Web 服务提供者、Web 服务请求者的数目也在不断增加,系统并不能保证每个实体都是可信的,尤其是出于某种不正当的竞争关系,第三方可能会提供一些虚假甚至恶意的服务注册信息,使得服务请求者难以获得符合自己需要的高质量 Web 服务,致使 Web 服务使用风险增加,从而制约了基于 SOA 架构的服务计算的发展。通过构建有效的信任评估机制来完善服务计算环境下的访问控制已经成为迫切需要解决的问题。本文分析了传统信任评估模型,在此基础上提出了一种新的服务计算信任评估安全模型(SOC-TrustSM)。

1 信任评估模型研究现状

在大规模的分布式计算环境下,为了准确地反映代理间的信任关系,学术界和工业界针对不同的研究和应用领域提出了许多信任评估模型,如 Beth 信任评估模型^[1]、Schillo 信任评估模型^[2]、JΦsang 信任评估模型^[3]等。这些模型都给出了信任

的表述、信任度量的方法和综合信任值的计算公式,但却无法满足代理间信任关系的动态性和不确定性的要求。当有多个推荐信任时,综合信任值往往只是通过简单的均值来获取,这些方法很难反映代理间真实的信任关系。

文献[4]提出了一种在网格环境下基于向量的信任评估模型。在该模型中引入了自信、信任的历史查询、时间衰减因子等来适应信任的不确定性和动态性,对 Web 服务中的恶意代理有较强的抵御能力^[5]。不足之处有:a)该模型没有考虑代理的信誉,在计算推荐信任值时只相信邻居节点,所以不能够准确反映信任关系的真实情况;b)该模型假定已经建立信任关系的代理不会提供虚假的推荐信息,因此不能解决代理之间的欺骗行为。

文献[6]提出了一种开放网络环境下的云信任模型。在该模型中使用推荐信任值进行综合信任值计算,能够得到一个比较合理的信任值。不足之处有:a)没有讨论代理在未建立信任关系时信任值的初始化问题;b)没有区分对推荐信誉是基于第一手还是第二手的推荐,模型过于简单化。

文献[7]提出了一种在 Web 服务环境下基于模糊理论的信任评估模型。模型包括信任的定义、信任实体使用基于模糊逻辑的信任模型进行信任评估、调整代理的信任值三项内容。使用模糊推理系统进行信任评估,能适应 Web 服务环境的动

收稿日期: 2011-11-05; **修回日期:** 2011-12-25 **基金项目:** 山东省自然科学基金资助项目(ZR2011FM019)

作者简介: 张永胜(1962-),男,山东潍坊人,教授,主要研究方向为软件工程环境、Internet/Intranet 工程、网络信息安全;吴明峰(1985-),男,硕士研究生,主要研究方向为 Web 服务安全(wumingfeng310@126.com);郑志华(1962-),女,副教授,主要研究方向为信息安全;李园园(1986-),女,硕士研究生,主要研究方向为访问控制安全模型;傅孟霞(1985-),女,硕士研究生,主要研究方向为计算机教育应用。

态性,在实体交互后及时进行信任值的调整,对恶意代理有较好的抵御能力。不足之处有:a)在计算综合信任值时对时间因素考虑较少,未涉及信任值随时间变化的问题,所以模型的适应能力需要改进;b)只使用代理的直接信任值进行计算,并没有考虑代理的信誉。

Sun 等人^[8]提出了一种基于熵理论的信任评估模型,它能够实现代理之间信任值的动态更新,具有良好的动态适应能力。不足之处在于:模型的计算收敛性较慢,可扩展性较差。

文献[9]提出了一种基于模糊 Petri 网的 Web 服务信任评估模型。该模型考虑了推荐代理在信任评估中的权重、推荐代理阈值和推荐信任规则等要素,采用矩阵运算能够在 Web 服务信任评估中得到一个比较准确、有效的获信代理的信任值,从而降低风险,保证 Web 服务交互的成功率。不足之处有:a)信任评估时对相应的时间因素和背景因素考虑较少;b)没有考虑对诚实交互的激励机制和对恶意交互的惩罚机制。

文献[10]提出了一种能力属性增强的 Web 服务信任评估模型(ServTrust)。ServTrust 是基于多代理器的解决方案,在模型中定义了属性增强因子及强、中、弱、无和不可知五种信任关系,利用 PKI 中基于 CA 的信任机制来保证 Web 服务的可信性和完整性,在一定程度上可以防止恶意代理的欺骗行为。不足之处在于不能有效地识别哪些行为是恶意行为。

2 SOC-TrustSM

2.1 基于信任的扩展 SOA 模型

服务计算建立在面向服务的体系架构(SOA)这种新型的分布式计算技术基础上。SOA 由三种角色和三种行为构成。三种角色分别是服务提供者、服务请求者和注册中心;三种行为分别为发布、查找和绑定。在此基础上通过增加可信的第三方代理来扩展 SOA 模型。信任代理根据代理之间交互记录来计算获信代理的直接信任值,并提供更新、查询功能。由于 SOA 模型中的服务请求者是动态变化的,同一时间信任代理作出评价的数量可能非常大,要求信任代理具有较高的计算能力。扩展的 SOA 模型如图 1 所示。

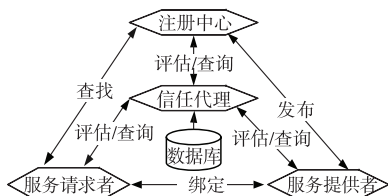


图1 基于信任的扩展SOA模型

2.2 信任评估模型的相关概念

参考现有的信任评估模型,给出与信任模型相关的信任关系的定义^[11]。

定义1 求信代理。在给定的背景和时段下,对另一个代理有忠诚或信念的一个代理。

定义2 获信代理。在给定的背景和时段下,被另一个代理寄托忠诚或信念的一个代理。

定义3 信任。在给定的背景和时段下,直接信任值、第三方代理的推荐信任值、第三方代理的推荐信誉值及团体信誉值不同权重的组合。用四元组 $SOC-TrustSM(dT, iT, C, G)$ 表示,其中 dT 表示直接信任值; iT 表示推荐信任值; C 表示基于第一手、第二手、第三手的推荐信誉值(或者说是看法); G 表示团体信誉值(或者说是看法)。

定义4 直接信任。求信代理 A 对获信代理 B 的直接信任值是指从 A 和 B 的历史交互记录中得到 A 对 B 可信度的评价。

定义5 推荐信任。求信代理 A 和获信代理 B 没有历史交互记录,可以通过第三方代理的介绍而建立的一种信任关系。

定义6 信任关系。在推荐信任关系中存在求信代理对第三方代理的信任以及第三方代理对获信代理的推荐信任。

定义7 信誉。所有来自第三方推荐代理关于获信代理的推荐信誉值的聚合。根据第三方信誉推荐者是直接推荐、间接推荐还是二次间接推荐,对应地可分为第一手、第二手和第三手推荐信誉看法,即推荐信誉值(为减少信任值计算的复杂度,本文规定:信誉看法考虑到第三手的看法,超过第三手的看法则当做第三手看法来计算)。第一手信誉看法即第三方推荐代理的直接信誉看法;第二手信誉看法即第三方推荐代理的间接信誉看法;第三手信誉看法即第三方推荐代理的二次间接信誉看法。

定义8 团体信誉。在服务计算环境中由信誉值高的第三方代理组成一个专家团,通过亲身体验来对其他代理或者服务作出的评价。

2.3 信任值的计算

1)直接信任值 正如社会生活中的一对好朋友如果较长时间不联系会变得疏远一样,求信代理和获信代理之间长时间没有交往,它们彼此之间的信任值会降低,即信任值随时间衰减。另外信任值还应与特定的背景相关联。根据求信代理和获信代理的历史交互经验(历史交互记录表),直接信任值 $dT_d^{(m)}(x, y, n', b')$ 的计算公式为

$$\begin{cases} dT_d^{(m)}(x, y, n', b') = s_i(x, y, n', b') \times w_i \times f_i & \delta = 1 \\ dT_d^{(m)}(x, y, n', b') = \theta & \delta = 0 \end{cases} \quad (1)$$

其中: $s_i(x, y, n', b')$ 表示在时段 n' 、背景 b' 下求信代理 x 给出获信代理 y 的信任值; w_i 为背景相似度的影响变量, $w_i \in (0, 1)$,若当前背景和上一次交互的背景越相似,其值越靠近 1,反之越接近 0; δ 表示代理双方是否发生过历史交互,即是否有历史交互记录表; f_i 表示获信代理最后一次交往的时间所确定的看法的重要程度的时间影响因子; θ 表示代理双方未建立信任关系时的初始值(本文设置为 0.5)。 f_i 的定义如下:

$$f_i(n) = e^{-\frac{(T_p - T_n)}{N}} \quad (2)$$

其中: T_p 为最近一次交往的时间或时段; T_n 为现在交往时间; N 为时间衰减因子, N 越小,衰减的速率越大。

2)推荐信任值 推荐信任值的计算,需要从三方面来考虑:a)求信代理对第三方代理的信任强度;b)第三方推荐代理对获信代理的信任强度;c)相关的背景和时间。假如求信代理 x 有 n 个第三方信任代理 $\{y_1, y_2, \dots, y_n\}$,则 x 的推荐信任值 $iT_d^{(m)}(x, y_i, n', b')$ 定义如下:

$$iT_d^{(m)}(x, y_i, n', b') = \frac{\sum_{i=1}^n s_i(x, y_i, n', b') dT_d^{(m)}(x, y_i, n', b') + s_i(y_i, y, n', b') dT_d^{(m)}(y_i, y, n', b')}{n} \quad (3)$$

其中: y_i 为第 i 个第三方推荐代理; n 为第三方推荐者代理的数目。在推荐信任中引入信任强度能够抑制恶意推荐代理对信任评估带来的影响并尽可能准确地反映出推荐信任值。

3)推荐信誉值 推荐信誉值的计算是根据时间和背景,从若干个第三方代理中得到获信代理信誉的聚合。在信誉系统里,并不是每个代理的信誉推荐看法都是同等重要的,为了更精确地评估推荐信誉值,把看法分为第一手、第二手和第三

手信誉看法。信誉度量包括以下三个方面:a)提供信誉看法的推荐代理本身的信任值;b)时间影响因子;c)区分是基于第一手、第二手还是第三手的推荐信誉。推荐信誉值 $C_d^{(m)}(x, y, n', b')$ 的定义如下:

$$C_d^{(m)}(x, y, n', b') = \mu \sum_{i=1}^m s_i(y_i, n', b') F_{\text{view}}(y_i, y) f_i + \alpha \sum_{i=1}^n s_i(y_i, n', b') S_{\text{view}}(y_i, y) f_i + \eta \sum_{i=1}^n s_i(y_i, n', b') T_{\text{view}}(y_i, y) f_i \quad (4)$$

其中: μ 、 α 、 η 分别指第一手、第二手和第三手看法的权重因子^[12],求信代理根据自身评价标准来设置权重因子 μ 、 α 、 η 从而可以得到一个更全面、更客观的推荐信誉值; $s_i(y_i, n', b')$ 为第三方推荐代理提供的信誉值; $F_{\text{view}}(y_i, y)$ 表示推荐信誉代理 y_i 对获信代理 y 的第一手看法; $S_{\text{view}}(y_i, y)$ 表示推荐信誉代理 y_i 对获信代理 y 的第二手看法; $T_{\text{view}}(y_i, y)$ 表示推荐信誉代理 y_i 对获信代理 y 的第三手看法。

4) 团体信誉值 由信誉高的第三方代理组成一个专家团队,通过亲身体验来对其他代理或者服务作出评价。把具有一定权威性的团体信誉看法聚合得到团体信誉值。加入时间衰减因子来确保离目前最近的团体信誉看法的影响力最大。通过加强团体信誉看法的权重因子可以有效地减小服务计算环境中恶意代理的非法操作造成的危害。团体信誉值 $G_d^{(m)}(x, y, n', b')$ 定义为

$$G_d^{(m)}(x, y, n', b') = \sum_{i=1}^m G_i(g_i, n', b') R_g(g_i, y) f_i \quad (5)$$

其中: m 为允许出现的团体个数; $G_i(g_i, n', b')$ 为第 i 个团体提供的获信代理信誉值; $R_g(g_i, y)$ 为第 i 个团体的可信度。

5) 综合信任值 在给定的时间和背景下,信任值的计算由四部分组成:直接信任值、推荐信任值、推荐信誉值和团体信誉值。不同的求信代理对每一部分的重视程度不同,本文给出信任评估模型 SOC-TrustSM 可通过设置不同的影响因子来体现对各个部分的影响程度,综合信任值 SOC-TrustSM(dT, iT, C, G) 可由如下公式求得:

$$\text{SOC-TrustSM}(dT, iT, C, G) = a_1 \times dT_d^{(m)}(x, y, n', b') + a_2 \times iT_d^{(m)}(x, y, n', b') + a_3 \times C_d^{(m)}(x, y, n', b') + a_4 \times G_d^{(m)}(x, y, n', b') \quad (6)$$

其中: a_1 、 a_2 、 a_3 、 a_4 表示直接信任、推荐信任、推荐信誉和团体信誉的权重因子,其取值都在(0,1)之间,且 $a_1 + a_2 + a_3 + a_4 = 1$ 。

6) 综合信任值的动态更新 求信代理和获信代理之间的信任关系在动态变化^[13]。根据第三方代理给出的信任值与在历史记录表里查到的信任值,得出修改后的第三方代理的信任值。给出信任值更新 TC 的计算公式如下:

$$TC = \begin{cases} \eta \text{SOC-TrustSM}(x, y, n', b') + \delta \times \frac{1}{1+e^{-k}} & \text{诚实交互} \\ \alpha \text{SOC-TrustSM}(x, y, n', b') - \beta \times \frac{1}{1+e^{-k}} & \text{不诚实交互} \end{cases} \quad (7)$$

其中: $\delta + \eta = 1$; $\alpha + \beta = 1$ 。设当前评估的信任值为 $T_a(z, n', b')$,上一次历史交互信任值为 $T_{\text{actual}}(z, n', b')$,那么 $E_i = |T_a(z, n', b') - T_{\text{actual}}(z, n', b')|$ 表示信任值更新误差,若 E_i 大于信任值更新误差阈值 ε 则为不诚实交互,反之则为诚实交互。如果代理间是诚信交往,则正向加强获信代理的信任值;如果代理间交往是不诚实交互,则负向加强获信代理的信任值。同时信任评估模型要能保证不诚信交往的负向加强大于诚信交往时的正向加强的幅度^[14]。

3 模拟实验结果及其分析

通过模拟实验来比较 SOC-TrustSM 与 JΦsang 信任评估模

型在以下三个方面的性能:a)欺诈行为对代理信任值调整幅度的影响;b)代理的综合信任值随时间的变化;c)不诚实代理不断增加时的交互成功率。

实验运行环境为 Pentium® Duan-Core 2.1GHz CPU, 2 GB 内存, 250 G 硬盘和 Windows 7 旗舰版操作系统。所有 Web Services 皆使用 C# 语言编写, VS2008 (/GL, /O2 优化) 编译通过。

实验参数设定:直接信任权重因子 $a_1 = 0.3$, 推荐信任权重因子 $a_2 = 0.2$, 推荐信誉权重因子 $a_3 = 0.2$, 团体信誉权重因子 $a_4 = 0.3$ 。假定在初始状态下,所有获信代理的初始信任值为 0.5,信任值更新误差阈值 $\varepsilon = 0.2$ 。实验数据分析软件环境为 MATLAB 7.11。

实验 1 如图 2 所示,在 JΦsang 信任评估模型中,获信代理的综合信任值随恶意推荐代理数量的增加,降低的速度非常缓慢,不能有效防止推荐代理和获信代理之间的合谋行为。在 SOC-TrustSM 中通过设置信任值更新误差阈值 ε 来发现模型中的恶意推荐代理。根据信任值更新式(7),设置不诚信交互行为的惩罚因子 α 和 β ,使第三方推荐代理的信任值迅速降低,从而可以实现对恶意代理和获信代理之间合谋行为的惩罚。

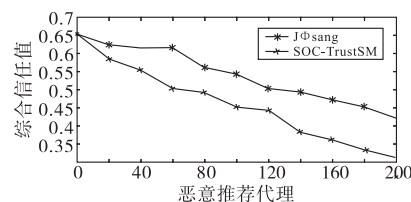


图2 恶意推荐数目增加信任度下降趋势

实验 2 如图 3 所示,在 JΦsang 信任评估模型中,获信代理通过较少次数的诚信交互就可以获得一个比较高的综合信任值。此模型对获信代理获得高信任值后进行恶意推荐不能起到有效的预防。在 SOC-TrustSM 中通过设置式(7)中的激励因子 δ 和 η 使代理信任值上升的速度比较缓慢,必须要经过长时间提供正确的看法才能获得较高的信任值,即获信代理要付出昂贵的代价才能获取一个较高的信任值。这样可以有效地防止代理轻松获得高信任值后进行非法或者恶意操作。

实验 3 图 4 给出的实验结果表明, SOC-TrustSM 和 JΦsang 模型在恶意推荐代理的比例不断增加时,代理间的 Web 服务交互成功率变化幅度较小,说明这两种模型对恶意代理之间的共犯行为有一定的抵御能力。但是当恶意推荐代理所占的比例达到 35% 时, JΦsang 中的 Web 服务交互成功率呈现明显下降趋势。在 SOC-TrustSM 中通过设置 ε 来发现并抑制恶意交互行为,使得 Web 服务交互成功率保持在一定的范围内。这说明在 SOC-TrustSM 能够抑制服务计算环境下恶意代理之间的欺诈行为,具有良好的健壮性。

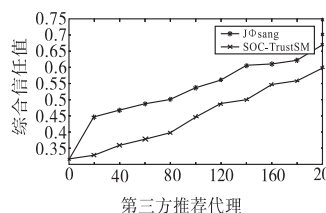


图3 诚信推荐数目增加信任度上升趋势

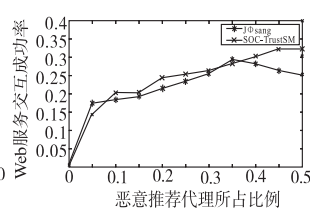


图4 Web服务交互成功率

4 结束语

本文在分析传统信任评估模型的基础上,提出了一种服务计算信任评估安全模型 SOC-TrustSM。在模型(下转第 2707 页)

(上接第2695页)中引入了直接信任看法、推荐信任看法、推荐信誉看法(区分为基于第一手、第二手和第三手的看法)和团体信誉看法,将普通代理与权威代理的评价进行区分,可以削弱多代理之间恶意信任评价对信任值评估的影响,使评价机制更为合理。

参考文献:

- [1] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks[C]//Lecture Notes in Computer Science, vol 875. Berlin: Springer, 1994: 1-18.
- [2] SCHILLO M, FUNK P, ROVATSOS M. Using trust for detecting deceitful agents in artificial societies [J]. **Applied Artificial Intelligence**, 2000, 14(8): 825-849.
- [3] JΦSANG A. Prospective for modeling trust in information security [C]//Proc of Australasian Conference on Information Security and Privacy. [S. l.]: Springer, 1997: 79-92.
- [4] JAMEEL H, HUNG L X, KALIM U, *et al.* A trust model for ubiquitous systems based on vectors of trust values [C]//Proc of the 7th IEEE International Symposium on Multimedia. Washington DC: IEEE Computer Society, 2005: 674-679.
- [5] 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, 18(6): 1510-1521.
- [6] 李德毅, 孟海军, 史雪梅. 隶属云和隶属云发生器[J]. 计算机研究与发展, 1995, 32(6): 15-20.
- [7] DUMA C, SHAHMEHRI N. Dynamic trust metrics for peer-to-peer system [C]//Proc of the 16th International Workshop on Database and Expert Systems Applications. Washington DC: IEEE Computer Society, 2005: 776-781.
- [8] SUN Y, YU W, HAN Z, *et al.* Trust modeling and evaluation in Ad hoc networks [C]//Proc of Global Telecommunications Conference. Washington DC: IEEE Computer Society, 2005: 1-10.
- [9] 李季, 朱小勇. 模糊 Petri 网及其在 Web 服务信任评估中的应用 [J]. 计算机应用研究, 2010, 27(2): 573-576.
- [10] 李海华, 杜小勇, 田莹. 一种能力属性增强的 Web 服务信任评估模型 [J]. 计算机学报, 2008, 31(8): 1471-1476.
- [11] 陈德人, 郑小林, 于红华. 服务信任与信誉 [M]. 杭州: 浙江大学出版社, 2008: 227-279.
- [12] 王莹, 张永胜, 张永强, 等. 一种信任增强的 Web 服务综合评估模型 [J]. 计算机工程与应用, 2010, 46(29): 89-92.
- [13] 朱小勇. Web 服务环境下的信任评估模型研究 [D]. 重庆: 重庆大学, 2010.
- [14] 陈书义, 闻英友, 赵宏. 基于模糊集合的可信计算信任模型评估 [J]. 计算机科学, 2008, 35(11): 39-41.