

一种基于 Web 服务的信任评估模型

刘 彬, 张仁津

(贵州师范大学 数学与计算机科学学院, 贵州 贵阳 550001)

摘 要: 处于开放网络环境中的 Web 服务, 时刻面临着遭遇恶意欺诈行为的风险, 因此在 Web 服务体系中构建安全可靠的信任管理机制成为必然趋势. 根据 Web 服务的特点, 提出了一种新的信任评估模型, 把对 Web 服务的信任度量归纳为业绩信任度和用户评价信任度两种情况. 在实施信任度评估时, 重点考虑服务时间、服务结果、恶意行为对信任度的影响, 并按新的信任评估模型设计了 Web 服务的体系结构, 说明了新体系结构下 Web 服务的应用过程. 仿真结果表明提出的信任评估模型能较好地辨别 Web 服务应用中的恶意欺诈行为.

关键词: Web 服务; 业绩信任度; 用户评价信任度; 信任评估模型

中图分类号: TP302

文献标识码: A

文章编号: 1000-7180(2010)08-0168-05

A Trust Evaluation Model Based on Web Services

LIU Bin, ZHANG Ren-jing

(School of Mathematic and Computer Science, Guizhou Normal University, Guiyang 550001, China)

Abstract: Huge risk exists in web service because of many cheatings and malicious acts in the open environment of internet with web services. So it's a trend to build an effective trust mechanism based on web services. According to the characteristic of web service, a new trust evaluation model is proposed. In this trust model for web services reduces to trust degree of business and trust degree of customer evaluation. During implementing trust degree evaluation, it is necessary to think about the influence of service time, service result and malicious behavior to trust degree as pivot, and it designs a new web services architecture grounded on the new trust evaluation model, and explains the application of web services under the new architecture also. Simulation experimental results show the new trust evaluation model can distinguish the cheating and malicious act in web services.

Key words: web services; trust degree of business; trust degree of customer evaluation; trust evaluation model

1 引言

随着 Internet 技术的飞速发展, Web 服务技术得到广泛应用, 为各组织之间, 组织与用户之间建立灵活多样的协作关系创造了可能. 以前的许多研究都认为服务提供者、使用者提供的信息是真实可靠的, 但从实际情况来看, 在这种开放的 Web 服务环境中, 欺骗性和不确定性是广泛存在的. 因此, 如何降低 Web 服务交易双方的风险, 如何构建有效的信任管理机制是当前 Web 服务应用的一个重要课题.

早前, Web 服务体系结构中主要关注服务质量

(Quality of Service, QoS)以及安全方面的扩展^[1-3], 但这些方法主要适合解决服务质量和访问权限等, 对恶意欺诈行为几乎没有作用. 现在越来越多的学者研究 Web 服务的信任问题. William Conner^[4]等人根据多个不同实体的反馈信息合成基于声誉的信任管理框架. 苏锦钊^[5]等人提出的是基于信任和声誉的评估模型. 胡旭东^[6]等人提出了一种由 Web 服务质量, 服务信誉等多种属性决策的 Web 服务发现模型. 李海华^[7]等人提出了一种采用多代理的解决策略的能力属性的 Web 服务评估模型. 文中提出了一种新的 Web 服务评估模型, 依据 Web 服务在真

实环境中存在的问题,综合考虑服务时间、服务结果、恶意行为多种因素.在其他的信任评估模型中都把评估值进行了规格化(信任度的值在 $[0,1]$ 之间),但这种规格化的值是在很小的范围内变化,所以区分度不是很好.在本信任评估模型中并没有把信任度值进行规格化,而是直接以实数值表示.因为在本信任评估模型中信任度的值受到时间衰减因子的影响,所以信任度的值能设计到一个比较合理的范围内.

2 信任评估模型

2.1 安全问题

Web服务相关的行为可以分为正常行为和恶意行为.对于正常行为来讲,其提供的服务和为其他服务给予的评价都是真实可靠的.恶意行为通常都不会提供真实的服务,或者在开始阶段为了获得较高的信任度而提供真实的服务,当信任值达到一定程度后就进行欺诈活动.另外还有一类比较难于识别的团伙恶意行为,它们经常对其它真实的服务提供恶意的评价,而对自己团伙给予高的评价.这些恶意行为对Web服务的信任体系有很大的危害,所以在Web信任评估中必须要能有效地识别出这些恶意行为.

2.2 信任评估

信任评估主要基于博弈^[8],概率统计^[9],模糊集合^[10],主观逻辑^[11],实体行为^[12]等方法.根据Web服务的特点,文中设计一种基于Web服务信任评估模型,在这个信任评估模型中我们把对Web服务的信任度量设计为两个方面的信任度量:业绩信任度和用户评价信任度.

业绩信任度表示服务在某个时刻能提供有效服务的信任值,初始值为0.假设服务每提供一次服务就能得到一份业绩信任度.如果一个服务被使用得越多,则认为该服务的业绩信任度越高.为了防止一些服务在获得比较高的业绩信任度后就变坏,因此,我们在业绩信任评估度计算公式中加入了受服务时间影响信任值的时间衰减系数,可以认为近期服务对业绩信任度的影响比远期服务对业绩信任度的影响要大一些.为了让服务提供商重视每一次交易,我们在业绩信任度的计算中加强失败服务对业绩信任值影响的失败罚因子.假设服务 s 在 T 时间内(可以设为一个月或二个月等时间间隔)提供服务 m 次,那么此服务的业绩信任度公式:

$$e_s(m) = e_s(0) + \sum_{k=1}^m g(k) \alpha^{t_c - t_k} \beta(k) \quad (1)$$

其中, $e_s(0)$ 是 T 时间之前此服务所获得的折合业绩信任度,此参数是为了避免计算量过大而影响服务选择性能. $g(k)$ 是此服务第 k 次服务获得的信任值,取值原则是服务成功 $g(k) = 1$,服务失败则 $g(k) = -1$. $\alpha \in (0,1)$ 为时间衰减系数, t_c 为当前时刻, t_k 为第 k 次服务的时刻. $\beta(k)$ 为第 k 次服务的罚因子,其取值为 $\{1, q\}$.如果第 k 次服务成功, $\beta(k) = 1$,如果第 k 次服务失败,则 $\beta(k) = q (q > 1)$,这使得服务失败比服务成功对信任度的影响更大.

用户评价信任度表示被服务对象给服务的评价值,初始值为0.每次服务完成后,用户给服务一个评价,用户好评越多,服务获得的评价信任度越高.假设服务 s 在 T 时间内(可以设为一个月或二个月等时间间隔)提供服务 m 次,那么此服务的用户评价信任度公式:

$$c_s(m) = c_s(0) + \sum_{k=1}^m f(k) \alpha^{t_c - t_k} \sigma(m) \beta(k) \gamma(k) \quad (2)$$

其中, $c_s(0)$ 是 T 时间之前服务 s 所获得的用户评价折合用户评价信任度,此参数是为了避免计算量过大而影响服务选择性能. $f(k)$ 的取值为 $\{-2, -1, 0, 1, 2\}$ 中的一个(服务成功评价为正值,服务失败评价为负值),考虑到这种评价有滞后性,可以在服务完成之后由系统取缺省值0,被服务者提供评价时再修改为实际的评价值. $\alpha \in (0,1)$ 为时间衰减系数, t_c 为当前时刻, t_k 为第 k 次服务的时刻. $\sigma(m)$ 由式(3)确定,其主要作用是保证当服务的业绩信任度高时获得的用户评价信任度也高,反之亦然,用0.1钳位是避免业绩信任度为负数时会出现助长恶意行为的情况:

$$\sigma(m) = \max(e_s(m), 0.1) \quad (3)$$

$e_s(m)$ 是服务 s 提供 m 个服务后的业绩信任度. $\beta(k)$ 同式(1),代表服务失败罚因子. $\gamma(k)$ 是第 k 个服务中的被服务对象 i 对 s 的防恶意评价系数,其值为:

$$\gamma(k) = \lambda / \xi^p \quad (4)$$

其中, ξ 为 m 个评价中 i 对 s 评价次数, λ, p 用于抑制恶意评价, i 对 s 过多的评价并不能带来高的评价信任度.

3 体系结构

为了实现对Web服务提供者的信任评估,需要

有专门的机构对它们收集信息,文献[7]采用多代理器的解决方案,以信任代理服务器为核心,此服务器不仅完成信息收集及服务选择等功能,而且把服务使用者和服务提供者隔离开,在信任代理服务器建立服务使用者和提供者的代理器,这种解决方案存在的一个问题是信任代理服务器要完成绝大部分的功能,在服务量少的情况下不存在问题,一旦服务种类多,服务量大的情况下就难胜任工作了.因此,文中提出另外一种解决方案(如图1所示),在这个模型中,具体的交易是由服务使用者与服务提供者之间完成,大大地减轻了信任管理服务器的负载.

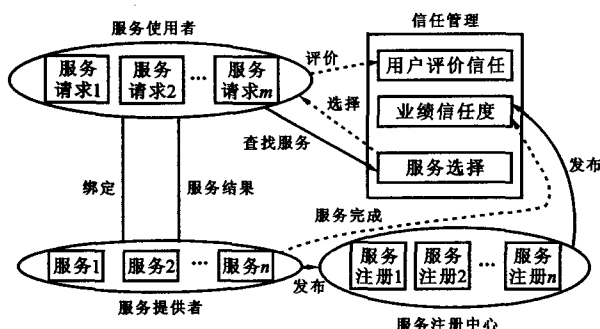


图1 基于信任的Web服务体系结构

基于信任的服务发布过程如下:

- (1) 服务提供商向服务注册中心发布服务;
- (2) 服务注册中心向信任管理中心提交服务.

基于信任的服务请求及服务过程如下:

- (1) 使用者向信任管理中心提交请求信息(如功能,服务价格,业绩信任度,用户评价信任度);
- (2) 信任管理中心根据用户的请求,把满足用户要求的所有服务用户的要求排序;
- (3) 用户根据信任管理中心返回的服务相关信息向服务提供者提出绑定请求,绑定后向服务提供者提供相关的处理数据;
- (4) 服务提供者完成后把服务结果返回给用户和信任管理中心;
- (5) 用户对服务提供者进行评价.

4 仿真实验及分析

仿真实验的主要目的:根据设计的信任评估模型,考察相关参数取值对业绩信任度和用户评价信任度的影响,看能否达到预期的效果.

4.1 不同参数的比较

仿真实验的初始条件设置:设服务的初始折合约绩信任度 $e_s(0)$ 和初始折合评价信任度 $c_s(0)$ 为0,在实际应用时可根据服务提供商的情况设置不同的值.在仿真中模拟了30次服务的情况: {1,1,1,

2}, {1,2,2,2}, {1,2,3,2}, {1,3,4,1}, {1,3,4,1}, {1,4,3,2}, {1,4,2,2}, {1,4,2,2}, {-1,4,4,-2}, {1,5,1,1}, {1,5,1,2}, {1,5,1,2}, {1,6,2,2}, {1,7,2,2}, {1,8,1,2}, {-1,9,1,-2}, {1,10,1,2}, {1,10,1,2}, {-1,11,1,-1}, {-1,11,2,-1}, {-1,12,2,-2}, {-1,13,2,-2}, {-1,14,1,-1}, {-1,14,1,-1}, {-1,15,2,-1}, {1,16,3,1}, {1,17,3,1}, {1,18,4,2}, {1,19,4,2}, {1,20,4,1}. 大括号中的第一项代表服务结果,1表示成功,-1表示失败;第二项代表服务时间(这里假设以天为单位);第3项代表被服务的对象;第4项代表被服务对象的对服务的评价值.

图2比较了 α 和 q 的取值对业绩信任度的影响.可以看出,当提供的服务有失败服务时业绩信任度会迅速下降(第9次服务,第19次至第25次服务).当服务下降很多后(第19次至第25次服务),随后即使提供成功的服务(第26次至第30次服务),业绩信任度也上升得很慢.这可以有效地防止服务的恶意行为,在实际应用中效果会更好,从前面的服务选择可以知道,当服务的业绩信任度比较低时,被选中提供服务的机率也会低.

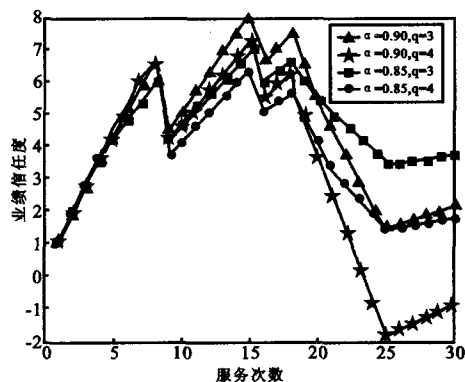


图2 α 和 q 对业绩信任度影响的比较

图3比较了 λ 和 p 的取值对用户评价信任度的影响.可以看出 λ 的取值不能太小.当 $p = 1.4$ 时, λ 的取值控制了用户评价信任度的变化率,取值适当即可.从图中的整体可以看出,同业绩信任度有相同的效果,当服务失败后用户评价信任度会迅速下降(第9次服务,第19次至第25次服务),当业绩信任度下降很多后(第19次至第25次服务),随后即使提供成功的服务,用户评价信任度上升得很慢(第26次至第30次服务).

图4给出的是防止自己或团伙恶意评价的比较.这仿效的是部分恶意服务提供商为了获得高的信任度值而采取自己或团伙欺骗的方式,从图4中

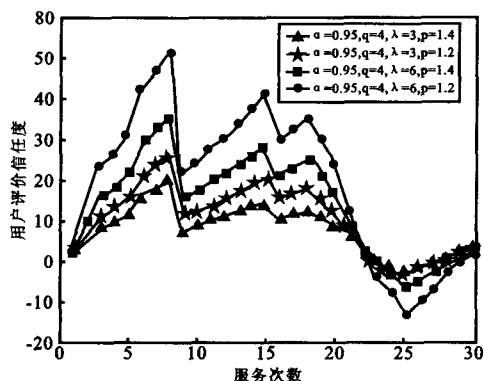
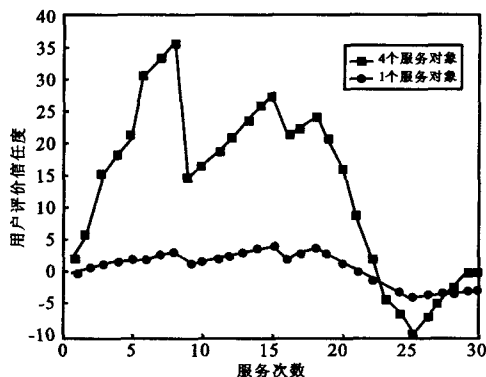
图3 λ 和 p 对用户评价信任度影响的比较

图4 多次评价对用户评价信任度影响的比较

可以看出,这种欺诈行为在我们的信任评估模型中并没有因同一个对象频繁评价而获得明显的用户评价信任度的提升。

4.2 对欺诈行为敏感程度的比较

为了能与其他方法进行比较,本文的信任模型获得的信任值需要作一定的修改,即把信任值进行规格化。因为本文的规格化仅仅是为了与其他方法进行比较,所以是在全局进行规格化,即最小值规格化为0,最大值规格化为1。依据文献[9]比较了两种获得并积累一定的信任后的欺诈行为:(1)突然进行不合作;(2)以一次不合作、一次合作等时间间隔和周期性摇摆。实际上文献[9]中的方法、平均模型和 EigenRep 模型给出的都是初始信任值为最大值1,不需要积累信任就获得了最大的信任度,这为恶意欺诈提供了很好的条件。但在模型中初始值是一个很小的值,必须通过提供诚信的服务才能获得信任度的增加,这无形中增加了欺诈行为的成本。

因为篇幅,文中只对业绩信任度进行了比较。第一个仿真比较是比较突然进行不合作的欺诈行为对业绩信任值的影响。仍以4.1节中30次服务作一定修改,取前20次服务进行测试,前10次都改为服务成功,后10次都改为服务失败。与概率统计模型、平均模型和 EigenRep 模型比较如图5所示。

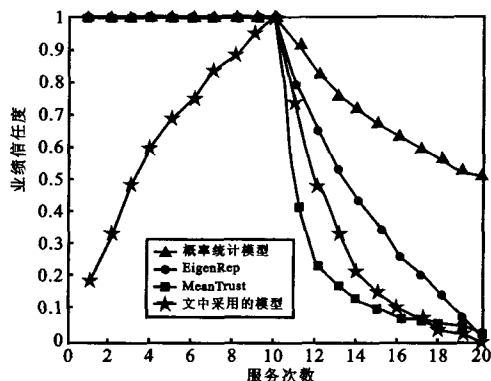


图5 突然不合作欺诈行为引起的业绩信任值变化

依据人的思维习惯,服务成功后信任值应该增加,但从图5中可以看出,概率统计模型、平均模型和 EigenRep 模型在开始一直维持在最大值1。而文中模型每次服务成功都能使信任值获得提升,这就鼓励服务提供商多提供服务。当服务失败后信任值都在下降,文中的模型下降的速度介于概率统计模型和 EigenRep 模型之间。在服务失败时让信任度降得过快未必有利,因为有部分服务失败并非完全是服务提供商的责任。

第二个仿真比较的是周期性摇摆欺诈行为对业绩信任值的影响。这个仿真中模型的条件仍是4.1节中30个服务,把服务前10个都改为成功,后20个周期性地以一个失败一个成功的形式出现,与概率统计模型、平均模型和 EigenRep 模型比较如图6所示。在这个比较测试中除了有前一个比较中有的特点,另一个特别突出的特点是概率统计模型、平均模型和 EigenRep 模型在信任值下降后,每提供一个成功服务都会获得等量或者近似等量的信任值增加。文中模型当信任值降得越低时,服务成功获得信任值提升的量越小,这样就能让服务提供商更加珍惜它的信任值,一旦它的信任值过低就很难再把信任值提升起来。

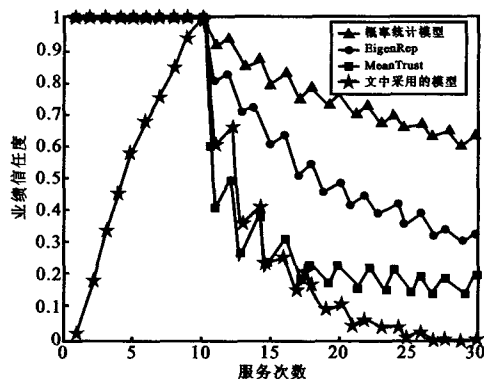


图6 周期性摇摆欺诈行为引起的业绩信任值变化

5 结束语

文中提出了一种基于 Web 服务的信任评估模型,针对这种模型设计了 Web 服务的体系结构并说明了服务流程.该信任评估模型能对 Web 服务提供商做出真实的评价,能有效防止服务提供商恶意提高自己的信任度,降低他人信任度的恶意行为,保护了服务使用者的利益.

参考文献:

- [1] 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.
- [2] 肖道举,杨剑,陈晓苏.Web 服务安全保障机制研究[J].华中科技大学学报:自然科学版,2004,32(4):50-52.
- [3] George Spanoudakis, Stephane LoPresti. Web service trust: towards a dynamic assessment framework[C]// the Proceedings of the 4th International Conference on Availability, Reliability and Security. New York: ACM, California: IEEE Computer Society Press, 2009.
- [4] William Conner, Arun Lyengar. A trust management framework for service-oriented environments[C]// 18th International World Wide Web Conference. New York: ACM, 2009.
- [5] 苏锦钿,郭荷清,刘森.Web 服务中的信任和声誉评估模型[J].计算机工程与应用,2006,42(21):127-130.
- [6] 胡旭东,曾国荪,陈波.一种基于非功能属性决策的可信 Web 服务发现模型[J].计算机科学,2009,36(2):95-98.
- [7] 李海华,杜小勇,田萱.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):1471-1477.
- [8] 罗俊海,范明钰.基于博弈的 MANETs 信任模型研究[J].计算机研究与发展,2008,45(10):1704-1710.
- [9] 吴鹏,吴国新,方群.一种基于概率统计方法的 P2P 系统信任评估模型[J].计算机研究与发展,2008,45(3):408-416.
- [10] 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.
- [11] 林剑柠,吴慧中.基于主观逻辑理念的网络信任模型分析[J].计算机研究与发展,2007,44(8):1365-1370.
- [12] 刘莉平,葛志辉.Grid 环境下基于实体行为的信任评估模型[J].计算机科学,2008,25(7):2020-2022.

作者简介:

刘彬男,(1973-),副教授.研究方向为网络计算、计算机图形学.
张仁津男,(1963-),教授.研究方向为软件方法学、组件技术、对象技术.

(上接第 167 页)

程的基础上,提出了一种基于响应时间的任务调度策略(STSRT),并对其进行了仿真验证.下一步的工作主要包括:在真实的应用环境中对任务调度策略进行进一步优化、大规模网络信息发送原型系统的实现.

参考文献:

- [1] 刘伯红,蔡丽.短信群发系统的设计与实现[J].微型电脑应用,2004,20(9):22-23.
- [2] 陈慧玲,帅立国,姜昌金.基于 http 协议的论坛群发技术的研究[J].计算机技术与发展,2007,17(3):38-43.
- [3] An Youngbae, Park Daeyeon. Scalable web server cluster system using content-aware packet filtering[C]// International Conference on Parallel and Distributed Processing Techniques and Applications. San Jose, 2003:721-727.
- [4] Hantian Wei, Xiaomei Xiong. The research and implement of an efficient load balancing algorithm[C]// Internet Conference on Services Science, Management and Engineering. Hong Kong, 2009:416-419.
- [5] Shailendra S Aote, Kharat M U. A game-theoretic model for dynamic load balancing in distributed systems[C]// International Conference on Advances in Computing, Communication and Control. Thailand, 2009:235-238.
- [6] Umit V Catalyurek, Erik G Boman, Karen D Devine, et al. A repartitioning hypergraph model for dynamic load balancing[J]. Parallel and Distributed Computing, 2009, 69(8):711-724.

作者简介:

董海量男,(1984-),硕士研究生.研究方向为网络安全、密码学.
胡华平男,(1967-),博士后,教授,博士生导师.研究方向为信息安全与密码学.
刘建锋男,(1984-),硕士研究生.研究方向为网络安全、密码学.
虞欣平男,(1963-),高级工程师.研究方向为网络工程与保障.