

用于 Web 服务的分布式信任和声誉模型

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: 为了提高以 Web 服务为基础的电子商务的安全性, 提出了分布式信任和声誉模型. 实施此模型只需对普通 Web 服务体系结构做功能扩充. 通过改进信任和声誉初值的方法, 使好的新注册 Web 服务获得机会. 根据 Web 服务的服务情况, 在不同阶段信任和声誉取值来源重点各不相同. 在其他用户推荐时, 考虑交易金额和时间因素, 可以有效地抵御共谋团体的欺诈行为. 仿真测试表明提出的信任和声誉模型能达到设计目的.

关键词: Web 服务; 恶意推荐; 共谋团体; 声誉; 信任

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)08-0208-04

Distributed Trust and Reputation Model for Web Services

LIU Bin, ZHANG Ren-jin

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

Abstract: To improve the safety of e-commerce based on web service, a decentralized trust and reputation model is proposed. Only function expansion is to be done for implementing this model on general web service architecture. A new well registered web service can obtain opportunities by improving the initial approach of the trust and reputation value. According to the transaction condition of the web service, the trust and reputation values mainly come from different key sources in different stages. Considering the transaction amount and the time factor in other user recommending can resist collusion group's fraud behavior. Simulation results show that the proposed trust and reputation model can meet the design purpose.

Key words: web service; malicious recommendation; collusion group; reputation; trust

1 引言

随着计算机技术和网络技术的发展, Web 服务作为一种开放式的软件获得了广泛的应用. 在这种分布式系统中, 传统的技术如授权、访问控制、信息安全服务等确定性安全措施对多个实体协作欺诈无能为力, 信任和声誉作为一种以交互历史为基础的预测机制能比较有效地防御这种行为^[1]. 根据 Web 服务的体系结构, 一些研究人员把 Web 服务的信任和声誉按集中式管理^[2,3], 即以 Web 服务注册中心为基础添加一个管理信任和声誉的机构. 这种全局式方法的好处就是实现简单, 但这种集中式的管理存在着以下问题: 第一, 当规模比较大时, 需要具有

很强计算能力的计算机或集群才能满足全局信任和声誉实时评估的需求, 影响系统的扩充; 第二, 所有 Web 服务被选择的机会几乎完全受控于这个管理机构, 如果它是完全可信的当然不会有问题, 但这种假设是无法保证, 一旦信任和声誉管理机构凭借它的垄断地位谋利, 将会使服务使用者和服务提供者的利益受损, 与采用信任和声誉机制的初衷背道而驰; 第三, 集中式信任和声誉管理易于被攻击, 一旦管理中心所受的可用性攻击得逞, 所有与之相关的 Web 服务都会出问题^[4]. 因此, 现在更多的研究是把 Web 服务的信任机制按分布式管理^[5], 他们提出了一种基于本体的社区式 Web 服务体系结构, 把服务使用者同服务提供者交互的实际数据以及服务使

收稿日期: 2011-06-01; 修回日期: 2011-06-29

基金项目: 贵州省科学技术基金项目(黔科合 J 字[2010]2102 号, [2008]2124 号)

用户对服务提供者的评价保留在服务使用者处,新的服务使用者对服务提供者进行信任评估时需要从使用过此服务的用户收集相关信息后进行评估,但他们采用的 Web 服务体系结构并不符合目前 Web 服务的一般结构,按他们的结构,Web 服务应用需要重建,这种代价太大.另外,他们使用的措施对多用户团队欺诈行为起到的作用有限.我们提出一种新的用于 Web 服务的信任和声誉模型,采用现有的 Web 服务系统结构,只需对功能进行一些扩充,因此更容易实施,主要工作包括:

(1)提出了一种新的 Web 服务信任和声誉模型;

(2)改进了新服务信任和声誉初始值设定,不是采用缺省值的形式;

(3)加强信任和声誉值对共谋团体的抵抗能力.

2 支持分布式信任和声誉的 Web 服务

2.1 Web 服务系统结构

我们采用的 Web 服务系统结构仍和基本的 Web 服务系统结构相同,并没有增加任何专门的信任和声誉管理机构,如图 1 所示,系统中仍然只包含三方:注册中心、服务提供者、服务使用者.

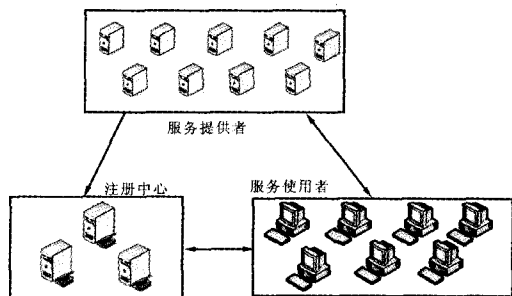


图 1 系统结构

为了在普通的系统结构中实施信任和声誉管理,需要增强系统中三方的功能:

(1)注册中心包含 Web 服务描述的信息以及 Web 服务交易历史信息,但不包含用户的反馈(用户使用 Web 服务后对 Web 服务的评价);

(2)服务提供者是 Web 服务的拥有者,Web 服务是统一资源标识(Uniform Resource Identifier, URI)标识的软件,在我们的模型中 Web 服务代表电子商务中的卖方,每次交易结束后,Web 服务应向注册中心提交交易的时间和金额,以备验证;

(3)服务使用者是应用 Web 服务的实体,服务使用者从注册中心查找服务时应申明是否同意共享对此服务的评价,完成交易后在本地保留交易完成

情况及对服务的评价的信息.

2.2 交易过程

交易过程如图 2 所示,共分为八个阶段:

(1)服务使用者向注册中心查询需要使用的 Web 服务;

(2)注册中心向服务使用者返回满足服务使用者要求的 Web 服务的相关信息,包括 Web 服务注册信息以及与此 Web 服务进行交易的一些相关信息(愿意共享评价的使用者做出的交易信息);

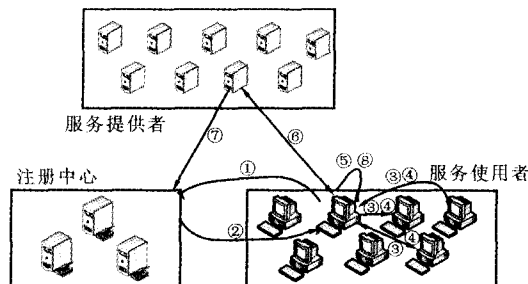


图 2 交易过程示意图

(3)服务使用者向其他使用过这些 Web 服务的使用者请求提供同这些服务的交易信息及评价信息;

(4)其他服务使用者返回相关交易信息及评价信息;

(5)根据其他使用者提供的信息、注册中心提供的信息以及自己的历史记录计算出每个 Web 服务的信任和声誉值(计算方法见第 3 节),其他使用者提供的交易记录需要与注册中心记录的交易时间和交易金额进行验证,防止其他客户或病毒篡改数据,如果发生篡改则要删除相应记录.完成所有计算后 Web 服务使用者选择一个最合适的 Web 服务进行交易;

(6)使用者与被选择的 Web 服务进行交易;

(7)执行交易的 Web 服务向注册中心提交交易记录;

(8)使用者对此次交易的 Web 服务进行评价,并把对此服务的评价记录在本地档案中.

3 信任和声誉模型

信任和声誉是个复杂的问题,每个人对其理解都有不同,目前也没有一个统一的说法,针对 Web 服务,我们认为一个好的信任和声誉模型应能满足以下要求:

(1)初始值的问题,许多研究者提出的模型都用某个缺省值作初始值,如果新进入的 Web 服务的信

信任值设置得太低,它将无法与其他已经早已存在的 Web 服务竞争(除非这些 Web 服务无法提升它们的信任值),这对于新的 Web 服务非常不利,即使它能提供更好的服务但因初始信任和声誉值低而无法获得机会,Web 服务使用者由于不知道有更好的服务也没有机会选择更好的 Web 服务^[6];如果新进入的 Web 服务的信任值设置得太高^[7],这对已经存在并提供良好服务的 Web 服务不利,服务提供者可通过提供新的 Web 服务进行欺诈行为而不必担心信任和声誉值下降;

(2) Web 服务的信任和声誉应是主观因素和客观因素、直接经验和间接经验的合成^[8]. 主观因素是使用者根据与 Web 服务交易后对 Web 服务的评价. 客观因素是 Web 服务使用者根据与 Web 服务交易时的客观度量,如 Web 服务金额. 直接经验是指使用者自己与 Web 服务交易的历史经验. 间接经验是指提供共享的使用者与 Web 服务交易的历史经验.

(3) 使用者对 Web 服务的 QoS 有偏向性,因此 Web 服务信任和声誉应考虑的服务质量的各个方面以及用户对这些方面的偏好,不同的使用者对同一个 Web 服务进行信任和声誉评估时得到的值可能不同;

(4) 使用者要从其他使用者获取他们对 Web 服务的评价,但这些对 Web 服务作出评价的使用者并不都是可信的,因此要考虑其他使用者的可信性;

(5) 电子商务中的欺诈行为都是以赚钱为目的,无论是以个体还是以团队的形式,因此需要考虑交易额.

因此,在我们提出的模型中信任和声誉值来源于三个方面:服务提供商的注册信息,使用者的直接经验,其他使用者的间接经验. 与大部分计算方法相同,我们也采用连续型值度量信任和声誉值,并采用规格化后的值,即 $[0, 1]$,值越大代表越值得信任. 由于 Web 服务的 QoS 具有多样性,有些是负属性(取值越大,性能越低,如服务价格),有些是正属性(取值越大,性能越高,如可用性),所以需要进行转换. 假设需要进行评估的 Web 服务一共有 m 个,每个 Web 服务包含 n 个 QoS 属性,则 Web 服务 i 的 QoS 属性可表示为 $\{q_{i1}, q_{i2}, \dots, q_{in}\}$, $i \in \{1, 2, \dots, m\}$, 若 q_{ij} ($j \in \{1, 2, \dots, n\}$) 为正属性,则按式(1)进行转换,若为负属性,则按式(2)进行转换,其中 $q_{j,\min}$ 为所有需要转化服务的第 j 个 QoS 属性中的最小值, $q_{j,\max}$ 为所有需要转化服务的第 j 个 QoS 属性中的最

大值.

$$v_{ij} = \begin{cases} \frac{q_{ij} - q_{j,\min}}{q_{j,\max} - q_{j,\min}} & \text{if } q_{j,\max} - q_{j,\min} \neq 0 \\ 1 & \text{if } q_{j,\max} - q_{j,\min} = 0 \end{cases} \quad (1)$$

$$v_{ij} = \begin{cases} \frac{q_{j,\max} - q_{ij}}{q_{j,\max} - q_{j,\min}} & \text{if } q_{j,\max} - q_{j,\min} \neq 0 \\ 1 & \text{if } q_{j,\max} - q_{j,\min} = 0 \end{cases} \quad (2)$$

用户对服务 i 的信任和声誉评估值可通过式(3)计算得出,其中 $T_p(i)$ 是通过服务 i 注册时宣称具备的性能计算得出的信任值, $T_e(i)$ 是从与服务 i 交易历史计算得出的信任值, n 为与服务 i 交易的次数, N 为一个正的自然数, $\alpha \in [0, 1]$, 其取值与服务 i 所属公司有关,公司信誉好则取值大,反之亦然. 在没有任何交易历史时,服务的信任和声誉值完全由 $T_p(i)$ 和所属公司声誉确定,随着交易次数的增加, $T_p(i)$ 在服务信任值中所占的比重逐渐减少, $T_e(i)$ 所占的比重逐渐增加.

$$T(i) = \alpha e^{-n/N} T_p(i) + (1 - e^{-n/N}) T_e(i) \quad (3)$$

3.1 Web 服务初始信任和声誉的计算

新注册的 Web 服务没有与任何使用者交易的历史,故无法采用历史经验评估其信任和声誉值,许多模型都是给所有的新注册的 Web 服务一个缺省值. 文献[2]把初始值设为 1,但这很容易导致欺诈行为,当信任度降到一定程度后,重新注册一个新的身份又可以继续进行欺诈活动了. 更多的研究者是把初始值设为中间值,即 0.5,但这种方法会导致一个问题,即使某个新 Web 服务能提供很好的服务,但因为缺省值比较低而无法获得用户的认可,这不仅不利于新注册 Web 服务的发展,而且也减少了用户获得优质服务的机会. 我们的方法是根据服务提供商注册时提供的 QoS 计算 $T_p(i)$,从式(3)可以看出最终值会乘以一个系数 α ,这也符合人们的实际心理,对于一贯声誉好的公司提供的新产品也会认为比较可信,而对于名不经传的公司提供的产品也不会很有信心. $T_p(i)$ 按式(4)计算得出,其中 v_{ij} ($j \in \{1, 2, \dots, n\}$) 是 Web 服务 i 的第 j 个质量属性 q_{ij} 按式(1)、(2)转换后的值, $w_j \in \{1, 2, 3, 4\}$ 表示用户对第 j 个质量属性的偏好程度,值越大代表用户关心此质量属性的性能.

$$T_p(i) = \sum_{j=1}^n v_{ij} w_j (\sum_{j=1}^n w_j)^{-1} \quad (4)$$

3.2 从经验获得信任和声誉的计算

经验包括自身经验和推荐经验(其他使用者的),其值由式(5)计算得出, M 为正自然数, m 为用

户自己同 Web 服务 i 的交易次数,从式(5)可以看出,随着自己的交易次数增加,直接经验的比重也会增加。

$$T_e(i) = e^{-m/M} T_d(i) + (1 - e^{-m/M}) T_r(i) \quad (5)$$

与信任和声誉值初始值获取方法不同,从经验获取信任和声誉值是根据使用者每次用完服务后针对服务的 QoS 评价值,假设评价分为四个等级,如{差,一般,好,优秀},可数值化为{0,1/3,2/3,1}。

3.2.1 直接经验

假设使用者与 Web 服务 i 的直接交易次数为 K 次,对第 j 个属性的评价值为 c_{kj}^i ,用户对第 j 个 QoS 属性为 w_j ,第 k 次交易时间为 t_k ,当前时间为 t , T 为正常数,则第 i 次直接经验由式(6)计算,所有交易的直接经验 $T_d(i)$ 由式(7)计算。

$$T_{kd}(i) = \sum_{j=1}^n c_{kj}^i w_j (\sum_{j=1}^n w_j)^{-1} \quad (6)$$

$$T_d(i) = \sum_{k=1}^K T_{kd}(i) e^{-\frac{t-t_k}{T}} (\sum_{k=1}^K e^{-\frac{t-t_k}{T}})^{-1} \quad (7)$$

3.2.2 推荐经验

文献[4]中为了预防共谋,将所有用户的反馈信息按 k 聚类算法找出给定评价值相对集中的主用户群体,最终的评估值受主用户群体给出的评价影响大,而其他用户给出的评价影响要小。他们的这种方法在共谋团体不大时比较有效,但当共谋团体比较大反而加强了共谋的效果。这种方法是以前交易次数来评估信任和声誉,往往都是用小的金额去换信任和声誉,得到信任后进行大金额欺诈,考虑到共谋团体实际是为了从中获利,因此我们以金额作为信任和声誉的权重,即使用很多小金额次数进行恶意评价也不能对信任和声誉值产生很大的影响。另外我们加入了时间衰减,如果要对信任和声誉值产生持久且大的影响,就必须长期投入比较大的金额,这让共谋团体或个体的恶意行为很难获利了。假设其他使用者与 Web 服务 i 的交易次数为 K 次,对第 j 个属性的评价值为 c_{kj}^i ,用户对第 j 个 QoS 属性为 w_j , a_k 代表第 k 次交易的金额,第 k 次交易时间为 t_k ,当前时间为 t , T 为正常数,则第 i 次推荐经验由式(8)计算,所有交易的直接经验 $T_r(i)$ 由式(9)计算。

$$T_{kr}(i) = \sum_{j=1}^n c_{kj}^i w_j (\sum_{j=1}^n w_j)^{-1} \quad (8)$$

$$T_r(i) = \sum_{k=1}^K T_{kr}(i) e^{-\frac{t-t_k}{T}} a_k (\sum_{k=1}^K e^{-\frac{t-t_k}{T}} a_k)^{-1} \quad (9)$$

4 仿真测试及分析

因为篇幅,只做了两个重要的测试,第一个测试是小金额共谋团体恶意诋毁服务,第二个是单个用户大金额恶意诋毁服务。如图 3 所示,共做了 40 次服务,其中●表示无恶意诋毁的情况,★表示小金额共谋团体恶意诋毁服务,我们试验的是第 6 次开始,其他用户都恶意评价用户,从图 3 可以看出,用户计算出服务的信任和声誉有明显的下降,但幅度并不是特别大,到第 20 次服务时,恶意评价已经基本没有影响,这是因为,当用户直接经验比较多后,其他用户的影响已经很小了。◆表示大金额恶意诋毁服务,从图中看出第 6 次服务时,信任和声誉下降了很多,但随着时间推移,到第 12 次服务时影响已经很小了,这是因为在我们的模型中引入了时间衰减,时间隔久后,恶意评价的影响已经很小了。综合两个测试可知,恶意诋毁只有在用户自身经验比较少时才能起作用,而且需要比较大的金额,所以其他用户想通过恶意诋毁而获得利益比较难达到目的,说明我们设计的模型能达到预期效果。

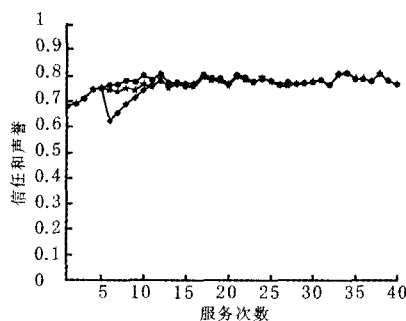


图 3 仿真测试

5 结束语

提出的用于电子商务情形下 Web 服务体系结构的分布式信任和声誉模型,只需对普通的 Web 服务体系结构做功能扩充即可使用,能方便应用于现有的 Web 服务应用系统。通过改进初始信任和声誉的初值计算方法,在不同阶段数据来源重点不同,考虑交易金额和时间因素等多种手段使 Web 服务使用者可以计算出更接近于实际的信任和声誉值,能比较好地保护使用者和 Web 服务的利益。

参考文献:

- [1] Damjan Kova, Denis Trek. Qualitative trust modeling in (下转第 215 页)

指标定位测试点. 另一个需要面对的问题是在共享资源的访问测试中如何建立触发竞争条件所需的精确时序序列,这就要求我们针对同一指标进行高频度重复测试以达到目的. 我们的目标是通过日志分析实时嵌入式系统 TOPPERS/ASP 的实践,并且进一步扩充测试案例,增加测评指标,更加规范化该方法.

5 结束语

本文通过深入分析 RTOS 的执行流程和 TOPPERS/ASP 系统完备的日志系统功能,并采用完善的日志 log 功能对 TOPPERS/ASP 的几个因素进行分析测试,对实时嵌入式系统的测试新方式做出了有益的探索.

参考文献:

- [1] 胡军,张岩,于笑丰,等. 嵌入式软件建模、实现与验证: 研究与发展[J]. 计算机科学,2005 32(1):16-23.
- [2] 汪泓澄. 嵌入式系统的性能基准程序及任务时限违背率 [D]. 上海:同济大学,2006.
- [3] 程国达,彭澄廉. 嵌入式系统描述与验证环境的实现 [J]. 计算机辅助设计与图形学报,2004(1):109-115.
- [4] 周炎森. SmartOSEK IDE3.0 及其模型检查和协同工作 [D]. 杭州:浙江大学,2007.
- [5] 蔡俊良,孙晓明. 一种基于 Linux 的车用实时操作系统 [J]. 清华大学学报:自然科学版,2004,44(1):78-84.
- [6] 赵立业,张激,游夏. 实时操作系统的性能分析和评估 [J]. 计算机工程,2008,4(1):283-286.
- [7] Sharygina N, Model checking of software control systems, PhD thesis[D]. Austin: The University of Texas, 2002.
- [8] Xie F, Yang G, Song X. Component-based hardware/software co-verification for building trustworthy embedded systems[J]. Journal of Systems and Software, 2007,80(5):643-654.
- [9] Sangiovanni-Vincentelli A L. Quo vadis sld: Reasoning about trends and challenges of system-level design[J]. Proceedings of the IEEE,2007,95(3):467-506.
- [1] 胡军,张岩,于笑丰,等. 嵌入式软件建模、实现与验证: 研究与发展[J]. 计算机科学,2005 32(1):16-23.
- [2] 汪泓澄. 嵌入式系统的性能基准程序及任务时限违背率 [D]. 上海:同济大学,2006.
- [3] 程国达,彭澄廉. 嵌入式系统描述与验证环境的实现 [J]. 计算机辅助设计与图形学报,2004(1):109-115.
- [4] 周炎森. SmartOSEK IDE3.0 及其模型检查和协同工作 [D]. 杭州:浙江大学,2007.
- [5] 蔡俊良,孙晓明. 一种基于 Linux 的车用实时操作系统 [J]. 清华大学学报:自然科学版,2004,44(1):78-84.
- [6] 赵立业,张激,游夏. 实时操作系统的性能分析和评估 [J]. 计算机工程,2008,4(1):283-286.
- [7] Sharygina N, Model checking of software control systems, PhD thesis[D]. Austin: The University of Texas, 2002.
- [8] Xie F, Yang G, Song X. Component-based hardware/software co-verification for building trustworthy embedded systems[J]. Journal of Systems and Software, 2007,80(5):643-654.
- [9] Sangiovanni-Vincentelli A L. Quo vadis sld: Reasoning about trends and challenges of system-level design[J]. Proceedings of the IEEE,2007,95(3):467-506.

作者简介:

魏先民 男,(1969-),硕士,副教授. 研究方向为分布式数据库、人工智能.

(上接第 211 页)

- SOA[J]. Journal of Systems Architecture, 2009, 55(4): 255-263.
- [2] 李海华,杜小勇,田萱. 一种能力属性的 Web 服务信任评估模型[J]. 计算机学报,2008,31(8):1471-1477.
- [3] 刘彬,张仁津. 一种基于 Web 服务的信任评估模型[J]. 微电子学与计算机, 2010,27(8):168-172.
- [4] Kevin Hoffman, David Zage, Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation Systems [J]. ACM Computing Surveys, 2009, 42(1): 1-31.
- [5] Zaki Malik, Athman Bouguettaya. RATEWeb: reputation assessment for trust establishment among web services[J]. The VLDB Journal, 2009, 18(4): 885-911.
- [6] Zaki Malik, Athman bouguettaya. Reputation Bootstrapping for trust establishment among web services[J]. Internet Computing, 2009, 13(1):40-47.
- [7] 吴鹏,吴国新,方群. 一种基于概率统计方法的 P2P 系统信任评模型[J]. 计算机研究与发展,2008, 45(3): 408-416.
- [8] Hien Trang Nguyen, Weiliang Zhao, Jian Yang. A Trust and Reputation Model Based on Bayesian Network for Web Services[C]//2010 IEEE International Conference on Web Services. Miami: IEEE computer society, 2010:251- 258.

作者简介:

刘彬 男,(1973-),硕士,副教授. 研究方向为网络计算、计算机图形学.

张仁津 男,(1963-),硕士,教授. 研究方向为软件方法学,组件技术,对象技术.