ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.4, April 2006, pp.682−690
DOI: 10.1360/jos170682
© 2006 by *Journal of Software*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一个适用于网构软件的信任度量及演化模型*

王 远[1,2+], 吕 建[1,2], 徐 锋[1,2], 张 林[1,2]

[1](计算机软件新技术国家重点实验室(南京大学),江苏 南京 210093)

[2](南京大学 计算机软件研究所,江苏 南京 210093)

A Trust Measurement and Evolution Model for Internetware

WANG Yuan[1,2+], LÜ Jian[1,2], XU Feng[1,2], ZHANG Lin[1,2]

[1](State Key Laboratory for Novel Software Technology (Nanjing University), Nanjing 210093, China)

[2](Institute of Computer Software, Nanjing University, Nanjing 210093, China)

+ Corresponding author: Phn: +86-013951822067, Fax: +86-25-83593283, E-mail: wangyuan@ics.nju.edu.cn, http://moon.nju.edu.cn

Wang Y, Lü J, Xu F, Zhang L. A trust measurement and evolution model for internetware. *Journal of Software*, 2006,17(4):682−690. http://www.jos.org.cn/1000-9825/17/682.htm

Abstract: Internetware is built upon the coordination of the heterogeneous, autonomous software entities in the open coordination environment. But it is very difficult to select the honest coordination software entities with dependable quality of services to build the trusted Internetware because of the openness and dynamic of the Internet. Trust relationships among software entities will provide important information about the selections of trusted coordination entities. The trust relationships are always changing along with the co-operations of software entities. However, the existing trust models cannot support the automatic formation and update of the trust relationships among entities, and cannot reflect the dynamic attribute of the trust relationships. This paper presents a trust measurement and evolution model for the Internetware. The model abstracts the process of the trust measurement, transfer and combination rationally and provides a reasonable approach to form and update trust relationships automatically. This model is helpful to solve the problem of the trustworthiness of the Internetware.

Key words: internetware; trust; software coordination; evolution; software service

摘 要: 网构软件的构建依赖于对开放协同环境中各种异构的、自治的软件服务实体间的有效协同.Internet的开放性与动态性,使得对于诚实的、具有可靠服务质量协同实体的选择难度较大,难以确保网构软件的可信性.软件实体间的信任关系对于保障网构软件的可信性具有重要的指导意义.软件实体间的信任关系通常随协作的进行而不断变化,但现有的信任模型缺乏对实体间信任关系的自动形成与更新的支持,从而无法刻画信任关系的动态性.针对该问题,提出了一个适用于网构软件的信任度量及演化模型.该模型不仅对信任关系度量过程和信任信息传递及合并过程进行了合理抽象,而且还提供了一种合理的方法,用于促进协同实体间信任关系的自动形成与更新.该模型有助于解决开放环境下网构软件的可信性问题.

* Supported by the National Natural Science Foundation of China under Grant Nos.60233010, 60273034, 60403014 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.2002CB312002 (国家重点基础研究发展规划(973)); the National High-Tech Research and Development Plan of China under Grant Nos.2005AA113160, 2004AA112090 (国家高技术研究发展计划(863))

Received 2005-05-11; Accepted 2005-12-14

© 中国科学院软件研究所 http://www.jos.org.cn

关键词: 网构软件;信任;软件协同;演化;软件服务
中图法分类号: TP311 文献标识码: A

网构软件[1]的构建依赖于 Internet 间异构的、自治的软件服务实体间的有效协同.传统的软件可信[2]保障技术在开发网构软件时遇到若干挑战:(1) 网构软件开发过程是一个基于丰富软件资源平台的软件实体组合过程[2],在构建过程中涉及到大量的移动实体与匿名实体,开发者无法直接管理参与协同的软件实体;(2) 网构软件在提交运行后,其结构依然具有动态演化性[2]:参与协同的实体可能动态地离开或加入系统,或根据用户需求及环境变化系统对实体进行重配置与替换[3];(3) 网构软件拥有开放、多样的用户群体[2],不同用户需求不相同;同一用户在不同环境、时段的需求也不同.网构软件可信需求与传统的软件系统相比,具有一种“柔性”特点[4,5];(4) Internet 中不存在绝对可信的第三方能够识别所有参与协同的软件实体,并对其可信程度作出担保.综上所述,网构软件需要一种动态演化的、相对的、“柔性”的可信保障机制.

信任可用于解决网构软件可信性问题:实体选取信任度高的实体进行协作,并只允许信任度较高的实体访问自身提供的服务.信任度量可为网构软件提供一种“柔性”、相对的软件度量机制,并且信任关系的动态变化为网构软件可信需求的动态变化提供支持.当前,为处理 Internet 中实体间信任关系提出了多个信任模型,如 Jøsang 模型[6]、TEM 模型[7]、Abdul-Rahman 模型[8]、Beth 模型[9]等.这些模型提供了描述、量化、传递信任信息以及综合多方信任信息的功能,并且对信任信息的操作均以实体间的推荐信任关系为基础.但是,上述模型就如何自主地适应信任关系的动态变化而展开的研究还不是很充分,无法有效支持信任关系,尤其是推荐信任关系的自动形成与更新,并且缺乏抵御恶意推荐信息的能力,因此不能较好地适用于网构软件.在开放软件协同环境下,为每一个软件实体的潜在协作实体及其推荐者人工静态地指定合适的信任值是极其困难的.网构软件要求软件实体应具有自主形成信任关系的能力,因此需要新的信任模型来支持信任的形成与更新.本文提出了一个适用于网构软件的信任度量及演化模型.模型对实体间信任关系的量化、传递及合并过程进行了合理的抽象,并提出了一种基于自治实体的请求-推荐模式来处理较为复杂的信任信息综合过程.模型重点强调对信任关系演化的支持,提出一种“反馈学习”的方法以支持推荐信任关系的形成与更新,同时考虑了减低恶意推荐信息对最终信任关系量化的影响.为解决网构软件可信性提供了依据.

1 信任、信任关系与信任信息

关于信任,目前尚未有一个广泛可以接受的定义[8−10].基于文献[10],本文给出适用于该模型的信任定义.

定义 **1**. 信任是软件实体关于其他实体或实体集团具有完成某一特定任务能力可能性的主观判断,其程度依赖于实体对于信任对象的直接经验和推荐信息.

若实体 A 信任实体 B,则 A 与 B 之间存在信任关系.信任关系表明评估实体确信评估对象能够以一定的概率正确地、非破坏性地进行某类协作活动,判断的依据为此前该实体所观察到的评估对象的行为及相关推荐信息.信任关系通常分为两类:直接信任关系与推荐信任关系(以下简称直接信任与推荐信任).直接信任是指实体与协作者之间的信任关系,可用 $t=\frac{N}{M}$ 进行量化.其中,M 为评估实体与协作者之间的总协作次数;N 为其中成功的次数;$t\in[0,1]$.直接信任表明实体认为协作者成功参与下次协作的概率为 t,预测的依据为此前实体所获得的直接经验;推荐信任是指实体与推荐者之间的信任关系,体现了实体认为其所提供信任信息为真的程度.推荐信任无法采用简单的方法进行量化,本模型采用[0,1]之间的实数来量化推荐信任,其大小反映了推荐信息的可信度,本文将在第 3 节给出确定其具体数值的方法.信任信息是指形成实体间信任关系的相关信息,在模型中也分为两类:一类为实体的直接经验;另一类为推荐信息.模型中,信任关系采用二元组 $R=\langle t,d\rangle$ 描述,其中:t 表示可信度,d 表示不可信度,且 $t+d=1$.直接经验采用二元组 $\langle s,f\rangle$ 描述,其中:s 为成功协作的次数,f 为失败的次数.模型中,推荐信息为推荐者与目标对象间的信任关系(记为 $R_{I:O}^{A\leftarrow C}=\langle t_{I:O}^{A\leftarrow C},d_{I:O}^{A\leftarrow C}\rangle$,表示实体 C 提供给 A 的关于实体 O 的推荐信息).

© 中国科学院软件研究所 http://www.jos.org.cn

2 信任度量及演化模型

模型基于信任网络的思想对实体间信任关系进行抽象.推荐信息与直接经验是评价实体间信任关系的基础,推荐信息的可信度由推荐者的可信度决定.实体通过收集推荐信息评估目标,推荐信息依靠信任网络进行传递.同时,实体对于推荐信息的评价受直接经验的影响:通常,与直接经验一致或相似的推荐信息更为可信.信任网络中的信任关系随着实体间的协作而不断发生变化.因此,一个完整的信任模型应该支持信任信息的传递与合并以及信任关系的形成与更新.模型将软件实体分为评估者、推荐者和评估对象,并假设每一个评估者均存在一个相对熟识的推荐者集合 $S.S$ 中,实体的推荐信息可作为评估者进行信任度量的依据.

2.1 信任信息的传递

信任信息的传递是将来自推荐者的推荐信息传递给评估者.接收信息取决于:(1) 评估者对推荐者的推荐信任 $R^A_{r:B}$;(2) 推荐者的直接信任 $R^B_{d:C}$.因此,接收信息可信度可表现为 $R^A_{r:B}$ 可信度与 $R^B_{d:C}$ 可信度的乘积.如图 1 所示.

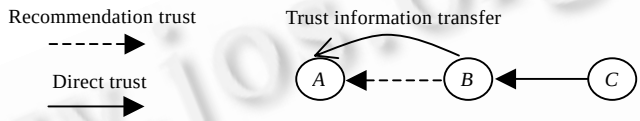


Fig.1 A simple process of trust information transfer

图 1 简单信任信息传递过程

定义 **2**(传递算子⊗). 实体 A 为评估者,实体 C 为评估对象,实体 B 为 A 的一个推荐者.设 $R^A_{r:B}=\langle t^A_{r:B},d^A_{r:B}\rangle$ 为 A 对于 B 的推荐信任, $R^B_{d:C}=\langle t^B_{d:C},d^B_{d:C}\rangle$ 为 B 对于 C 的直接信任(与具体上下文相关).

$$R^{A\leftarrow B}_{I:C}=R^A_{r:B}\otimes R^B_{d:C}=\langle t^{A\leftarrow B}_{I:C},d^{A\leftarrow B}_{I:C}\rangle,\text{其中 } t^{A\leftarrow B}_{I:C}=t^A_{r:B}\times t^B_{d:C},\ d^{A\leftarrow B}_{I:C}=t^A_{r:B}\times d^B_{d:C}+d^A_{r:B}\times t^B_{d:C}+d^A_{r:B}\times d^B_{d:C}.$$

⊗可描述复杂信任信息传递过程.如图 2 所示,信任信息从 D 到 C,再从 C 到 B,最后从 B 到 A,计算过程如下:

$$R^{A\leftarrow B}_{I:E}=R^A_{r:B}\otimes R^{B\leftarrow C}_{I:E},\ R^{B\leftarrow C}_{I:E}=R^B_{r:C}\otimes R^{C\leftarrow D}_{I:E},\ R^{C\leftarrow D}_{I:E}=R^C_{r:D}\otimes R^D_{d:E}.$$

"$A\leftarrow B\leftarrow\ldots\leftarrow D$"构成了一条信任链.理论上,信任信息可以通过任意长度的信任链进行传播.但实际应用中,信任随着信任链的增长而衰减直至消亡.⊗体现了推荐信息信任度随着信任链增长而衰减的特点.如图 2 所示.

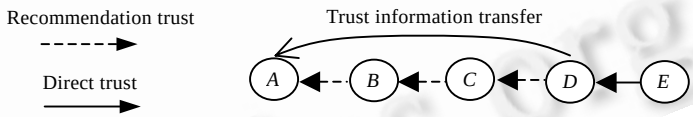


Fig.2 The process of trust information transfer

图 2 信任信息传递过程

2.2 信任信息的合并

评估者需要将不同推荐者所提供的推荐信息合并.如图 3 所示,评估者 A;评估对象 F;B,C,D 和 E 为 A 的推荐者.A 获得关于 F 的推荐信息,然后进行合并,合并信任的可信度应大于单个或部分推荐信任可信度.

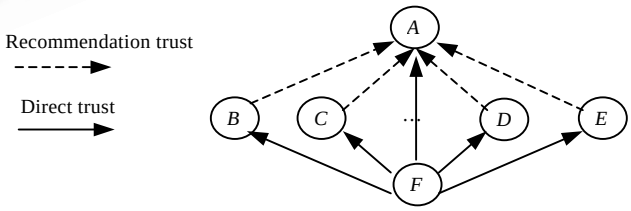


Fig.3 The process of trust information combination

图 3 信任信息合并过程

设 A 形成的合并信任为 $R^A_{c:F}=\langle t^A_{c:F},d^A_{c:F}\rangle$, $R^{A\leftarrow Oi}_{I:F}=\langle t^{A\leftarrow Oi}_{I:F},d^{A\leftarrow Oi}_{I:F}\rangle$ ($1\le i\le n$,n 为 A 的推荐者个数)为 A 从实体 O_i

© 中国科学院软件研究所 http://www.jos.org.cn

处获得的推荐信任值,则 $t_{c:F}^{A}\in[0,1]$,并满足如下条件:

若对于 $\forall i,1\le i\le n$,$\exists j,k$,使得 $t_{I:F}^{A\leftarrow Oj}\ge t_{I:F}^{A\leftarrow Oi}$, $t_{I:F}^{A\leftarrow Ok}\le t_{I:F}^{A\leftarrow Oi}$;则 $t_{I:F}^{A\leftarrow Ok}\le t_{c:F}^{A}\le t_{I:F}^{A\leftarrow Oj}$.

定义 **3**(算子⊕). 评估者 A,A 的推荐者集合 RS,$r_i\in RS$, $R_{r:r_i}^{A}=\langle t_{r:r_i}^{A},d_{r:r_i}^{A}\rangle$ 为 A 对 r_i 的推荐信任,r_i 所提供的推荐信息记 $R_{I:o}^{r_i}=\langle t_{I:O}^{r_i},d_{I:O}^{r_i}\rangle$,评估对象 O.$|RS|$为集合中元素的个数. $R_{c:O}^{A}$ 为 A 关于 O 的合并信任.

$$R_{c:O}^{A}=R_{I:O}^{A\leftarrow r_1}\oplus R_{I:O}^{A\leftarrow r_2}\oplus\ldots\oplus R_{I:O}^{A\leftarrow r_n}=\langle t_{c:O}^{A},d_{c:O}^{A}\rangle .$$

其中

$$n=|RS|,\ R_{I:O}^{A\leftarrow r_i}=R_{r:r_i}^{A}\otimes R_{I:O}^{r_i}=\langle t_{I:O}^{A\leftarrow r_i},d_{I:O}^{A\leftarrow r_i}\rangle,\ t_{c:O}^{A}=\sum_{i=1}^{n}\left(t_{I:O}^{A\leftarrow r_i}\times t_{r:r_i}^{A}\Big/\sum_{j=1}^{n}t_{r:r_j}^{A}\right),\ d_{c:O}^{A}=1-t_{c:O}^{A}.$$

⊕的定义满足既定需求.由于直接信任与所收集到的推荐信息描述方式相同,因此可以方便地进行综合.模型规定:实体可作为自身的推荐者,其推荐信任可信度为 1.即对于任意实体 A,A 持有如下推荐信任:

$$R_{r:A}^{A}=\langle t_{r:A}^{A},d_{r:A}^{A}\rangle \text{ ,其中 } t_{r:A}^{A}=1,\ d_{r:A}^{A}=0 .$$

根据该规定,将实体的直接信任与所收集到的推荐信息统一处理如下:

$$R_{s:O}^{A}=R_{I:O}^{A\leftarrow A}\oplus R_{I:O}^{A\leftarrow r_1}\oplus\ldots\oplus R_{I:O}^{A\leftarrow r_n}=\langle t_{s:O}^{A},d_{s:O}^{A}\rangle ,$$

其中 $R_{I:O}^{A\leftarrow A}=R_{r:A}^{A}\otimes R_{d:O}^{A}$,其他同定义 3.

2.3 基于自治实体的请求-推荐模式

基于自治实体的请求-推荐模式用于处理复杂信任网络中的信任信息.模式规定如下:(1) 当评估者向其推荐者发送请求时,推荐者才将相关信任信息传递给请求者.请求中包含深度信息;(2) 推荐者传递的是经过自身处理的信任信息;(3) 评估者只意识到最近推荐者的存在;(4) 推荐者只接受来自“高层”的推荐请求.图 4 为一个较为复杂的信任网络,设所有的信任关系均为$\langle 0.9,0.1\rangle$.A 设定请求深度为 2;B,E 和 F 收到请求后将请求深度减 1,继续向下层传递;当深度为 0 时,则不再传递.

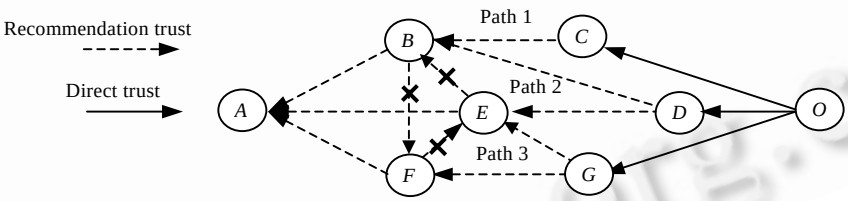


Fig.4 A complex trust network

图 4 复杂信任网络

实体 A 所得到的最终关于实体 O 的信任评价 $R_{s:O}^{A}$ 的计算过程如下:

(1) 依次计算 3 条推荐路径的综合推荐信息 $R_{c1:O}^{A}$, $R_{c2:O}^{A}$, $R_{c2:O}^{A}$;

Path 1: $R_{c1:O}^{A}=R_{r:B}^{A}\otimes R_{s:O}^{B}$, $R_{s:O}^{B}=R_{I:O}^{B\leftarrow C}\oplus R_{I:O}^{B\leftarrow D}$, $R_{I:O}^{B\leftarrow C}=R_{r:C}^{B}\otimes R_{d:O}^{C}$, $R_{I:O}^{B\leftarrow D}=R_{r:D}^{B}\otimes R_{d:O}^{D}$;

Path 2: $R_{c2:O}^{A}=R_{r:E}^{A}\otimes R_{s:O}^{E}$, $R_{s:O}^{E}=R_{I:O}^{E\leftarrow G}\oplus R_{I:O}^{E\leftarrow D}$, $R_{I:O}^{E\leftarrow D}=R_{r:D}^{E}\otimes R_{d:O}^{D}$, $R_{I:O}^{E\leftarrow G}=R_{r:G}^{E}\otimes R_{d:O}^{G}$;

Path 3: $R_{c3:O}^{A}=R_{r:F}^{A}\otimes R_{I:O}^{F\leftarrow G}$, $R_{I:O}^{F\leftarrow G}=R_{r:G}^{F}\otimes R_{d:O}^{G}$.

(2) 将所获得的推荐信息 $R_{c1:O}^{A}$, $R_{c2:O}^{A}$, $R_{c2:O}^{A}$ 进行综合.

$$R_{s:O}^{A}=R_{c1:O}^{A}\oplus R_{c2:O}^{A}\oplus R_{c3:O}^{A}=\langle t_{s:O}^{A},d_{s:O}^{A}\rangle=\langle 0.729,0.271\rangle .$$

$R_{s:O}^{A}$ 综合了所有的路径信息与推荐信息.B,E 和 F 间的推荐信任关系在此次评估过程中构成了“环路”,造成实体间循环等待推荐信息,出现“死锁”.上面的规定 4 可破除“死锁”,解决信任网络中的“环路”问题. $R_{s:O}^{A}$ 的生成过程还表明,模式使用了“路径”压缩技术.A 获得的推荐信息经过推荐者处理后不再含有“路径”信息.“路径”压缩技术的优点如下:(1) 信息隐藏.开放协同环境中传递的信息越少,则系统越安全.该模式下,即使攻击者捕获了某一段特殊的消息,他也只能获得某一实体关于一个特定评估对象推荐的信息,而无法从中推出消息的全局视

© 中国科学院软件研究所 http://www.jos.org.cn

图,从而保证了整个系统的安全性;(2) 增强了灵活性.实体可以自主地处理所获得的信息并再传递,而不影响传递路径上的其他实体;(3) 增强可操作性.简化了评估实体对于推荐信息的处理过程;(4) 负载平衡.推荐信息的处理过程有效地分布到了路径中的各个实体之上,不会形成处理的"瓶颈".

评估实体在获得对于评估对象的最终信任之后需要对其进行评估.该模型采用的方法是为每一个实体设定一个可信度阈值 t.对于经过合并运算获得的信任 $R^A_{s:O}$:若 $t^A_{s:O}>t$,则实体认为评估对象符合协同需求,可以参与协作活动;否则,实体将拒绝评估对象进行协同.可信度阈值大小反映了软件实体对于协同对象可信性需求的严格程度.在 Internet 软件协同环境中,软件实体必须具有感知环境的能力和对协同操作作出评价的能力.当一个软件实体由于可信度阈值过低而受到威胁时,必须及时提高阈值;反之,如果阈值过高,软件实体拒绝了大部分实体的协同请求,则应该相应下调阈值,尽可能地使合法的协同请求者能够调用服务.t 值的大小与软件实体参与协同的意愿成反比.t 越小,实体越容易参与协同,同时其可信性保障越低;反之亦然.选取合适的阈值是软件实体正常工作的重要因素之一.阈值与具体的应用相关,需视具体情况而定.

2.4 信任关系的演化

信任关系演化是指信任关系随着协作的进行自动形成与更新的过程.直接信任关系的变化可依据评估实体与评估对象协同过程中 M 和 N 值进行调整.但对推荐信任关系却很难采用相同的方式,原因在于很难确定推荐者推荐行为的好坏,即很难获得类似于直接信任信息中的 M 和 N 值.为了刻画推荐信任关系的变化,引入"反馈学习"的方法来评价推荐信任关系:在每次协同之后,评估者先更新自身的直接信任,然后根据直接信任评价推荐信息.依据对推荐信息的评价,对于"善意"推荐者,提高其可信度;反之,降低其可信度.

一个正常的、非恶意的软件实体在一定的时间和环境中,应该以一种相对稳定的概率参与某类协作活动.该场景符合贝努里(Bernoulli)概率模型.贝努里概率模型定义了一类随机实验模型:(1) 实验在相同条件下独立进行 M 次;(2) 每次实验只有两个可能结果:A 与 A'.评估对象每一次参与某类协作活动,均可看成贝努里概率模型的一次随机实验.M 次协同可看成评估对象以相对固定的频率完成 M 重贝努里实验.根据贝努里大数定律[11],在 M 次协同中,评估对象成功进行某类协作活动的观测频率,将随着 M 的增大依概率收敛于评估对象的固有成功协作概率.根据该原理,我们通过假设检验来判定评估者的观测频率(直接信任)是否服从推荐信息所指定的概率分布,若检验通过,说明推荐信息正确反映了评估对象进行相关协作活动的概率.设 $R^A_{d:O}=\langle t^A_{d:O},d^A_{d:O}\rangle$ 为 M 次协作后实体 A 对实体 O 的直接信任,B 为 A 的推荐者,$R^{A\leftarrow B}_{I:O}=\langle t^{A\leftarrow B}_{I:O},d^{A\leftarrow B}_{I:O}\rangle$ 为 B 提供给 A 的当前推荐信息.$t^A_{d:O}$ 反映了 A 与 O 成功协作次数在总协作次数中所占的比重.$t^{A\leftarrow B}_{I:O}$ 反映了 B 认为 O 会成功操作的概率.判断 $R^{A\leftarrow B}_{I:O}$ 是否准确的过程就是判断在某个显著水平 $\alpha(\alpha\in[0,1])$下,根据 $t^A_{d:O}$ 判断 O 的协作概率是否为 $t^{A\leftarrow B}_{I:O}$.其步骤如下:

(1) 设定假设 H_0:O 按照概率 $t^{A\leftarrow B}_{I:O}$ 进行协作.选取合适的显著水平 α;

(2) 根据中心极限定理[11]设定统计量 $U=\dfrac{M\cdot|t^A_{d:O}-t^{A\leftarrow B}_{I:O}|}{\sqrt{M\cdot t^{A\leftarrow B}_{I:O}\cdot(1-t^{A\leftarrow B}_{I:O})}}$,随着 M 的递增,U 服从正态分布 $\Phi(0,1)$;

(3) 根据公式 $P\{U\geq k|H_0\}=\alpha$,得到 $k=\int_{-\infty}^{1-\frac{\alpha}{2}}\frac{e^{-x^2/2}}{\sqrt{2\pi}}dx$.若 $U\geq K$,则不接受 H_0;反之接受.

上述操作中,H_0 成立且 $U\geq k$ 的概率为 α.当 α 足够小时,$U\geq K$ 为小概率事件,很难发生;一旦发生,则 H_0 不再成立的概率相当大.但是,虽然当 α 足够小时,可以将 $U\geq K$ 时 H_0 不成立的概率保持在较高的水平,但是会增加"存伪"误判的比例.即在 H_0 不成立且 $U<K$ 时,认为 H_0 成立.增大 α,虽然可以减少"存伪"误判,但是会导致"弃真"误判,将一部分 H_0 成立且 $U\geq K$ 的情况排除在外."存伪"与"弃真"两类误判互为消长,在 M 确定的情况下,无法同时降低两类误判的比例.为了解决此类问题,模型引入了接受显著水平 α_0 和拒绝显著水平 α_1,对应的 k 值为 k_0 和 k_1,且 $\alpha_0>\alpha_1$,$k_0>k_1$.当 $U<k_0$ 时,则认为 H_0 成立;当 $k_0<U<k_1$ 时,评估实体对推荐信息持保留意见,不作任何判断;$k_1<U$ 时,则拒绝 H_0.同时使用 α_0 与 α_1,则评估者对推荐信息的评价不再是二值的(满意或不满意),允许不确定情形的存在避免了评估者在直接经验不足的情况下,对信任关系的"盲目"更新.模型采用 3 个值记录评估者的意见:{*satisfied*,*unknown*,*unsatisfied*},记为 v^A_B,依次对应 U 的 3 种取值情况.其中 A 为评估者,B 为推荐者.

© 中国科学院软件研究所 http://www.jos.org.cn

评估者对推荐信息作出评估后,需要调整相应的推荐信任.模型基于信息论的基本理论给出了更新推荐信任的方法.信息论认为:已发生事件所蕴涵的信息量与事件发生的概率相关联.事件发生的概率越小,一旦发生,其所蕴涵的信息量就越大;反之,对于概率为 1 的事件,则认为是常识,其所蕴涵的信息量为 0.本文认为:若一个"善意"推荐者提供了"恶意"信息,将引起评估者的关注;反之亦然.据此,该模型给出了实体推荐信息量的定义.

定义 **4**(实体推荐信息量). 实体推荐信息量记为 I_B^A,评估者 A,推荐者 B, $R_{r:B}^A=\langle t_{r:B}^A, d_{r:B}^A\rangle$ 为 A 对 B 的推荐信任;当 $v_B^A=satisfied$ 时, $p=t_{r:B}^A$;当 $v_B^A=unsatisfied$ 时, $p=d_{r:B}^A$;其余情况 $p=1$.

$$I_B^A=-\lg p\ .$$

更新推荐信任,不能仅依赖于推荐者在当前协作活动中所提供的信息,对推荐者进行推荐活动的历史信息也应当加以使用.不同的历史信息对于推荐信任更新过程所产生的影响是不同的,越近的历史信息所产生的影响应该越大.模型通过影响因子 θ来反映历史信息的重要程度,越重要的历史信息其影响因子越大.某一特定历史信息的影响因子,应随着协作活动的不断深入而衰减,当 θ衰减到一定程度时,所代表的历史信息对于推荐者的评估将失去指导意义.此时,应当抛弃该历史信息.模型使用滑动窗口来模拟该过程.实体为某类协作过程 ω中的每一个推荐者引入一个滑动窗口来记录最近 n 次 ω类协作过程中其提供推荐信息的情况.

图 5 为一个 n 次滑动窗口,从右至左编号为 $n,n-1,\ldots,1$,记录了最近 n 次评估者关于推荐者的评价,其内容记为 C_i,C_i="+"表示对推荐信息满意; C_i="/"时,表示无法确定;C_i="−"表示不满意.滑动窗口是一个 FIFO 队列,窗口 i 被赋予了权值 θ_i,代表了所记录历史信息的影响因子,其中 $\theta_i=i$.当一次新的协作完成之后,在调整推荐信任之前,推荐信息的评估结果从右侧进入滑动窗口,原有的记录依次左移,最左端记录被移出窗口队列并被丢弃.滑动窗口模拟了历史信息的衰减过程,保证了最近发生的历史信息具有较大的影响因子.滑动窗口个数 n 体现了评估者对于历史信息的重视程度,n 越大说明评估者对于历史信息越看重;但 n 过大,将会导致评估者对于推荐信任的更新效果不明显.本文第 3 节将结合模拟实验讨论 n 的选择.

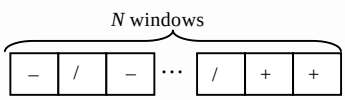


Fig.5 n slide windows

图 5 n 次滑动窗口

当一次协作结束后,实体利用该次实体推荐信息量来更新推荐信任,演化过程如下:设演化之前的信任为 $R_{r:B}^A=\langle t_{r:B}^A, d_{r:B}^A\rangle$,$A$ 为评估者,B 为推荐者, $new\_R_{r:B}^A$ 为更新后的信任.β为同类推荐信息在历史经验中所占的比重,λ为常数,称为幅度调整因子,令$\lambda=InN$,N 为滑动窗口的个数.

(1) 当 $v_B^A=satisfied$ 时,令 $p=t_{r:B}^A$,则 $p'=\beta(1-p)\dfrac{I_B^A}{\lambda+I_B^A}+p$, $new\_R_{r:B}^A=\langle p', 1-p'\rangle$,其中 $\beta=\sum_{Cj="+"}\theta_j \Big/ \sum_{i=1}^{n}\theta_i$;

(2) 当 $v_B^A=unsatisfied$ 时,令 $p=d_{r:B}^A$,则 $p'=\beta(1-p)\dfrac{I_B^A}{\lambda+I_B^A}+p$, $new\_R_{r:B}^A=\langle 1-p', p'\rangle$,其中 $\beta=\sum_{Cj="-"}\theta_j \Big/ \sum_{i=1}^{n}\theta_i$;

(3) 当 $v_B^A=unknown$ 时, 令 $new\_R_{r:B}^A=R_{r:B}^A$.

利用 $new\_R_{r:B}^A$ 替换原来的 $R_{r:B}^A$,就完成了整个信任演化过程.评估者在协作结束之后,依上述步骤更新所有推荐者的推荐信任,即完成了推荐信任的更新过程.

"反馈学习"法对推荐信任的更新依赖于具体客观的协作信息,同时结合评估实体的"主观"判断,是一种较为合理的分布式的信任更新方法.该模型所采用的信任更新方法与实体推荐信息量紧密相关,信息量越大,则调整的幅度越大.但是,单纯地依赖信息量来调整推荐信任具有局限性.因为对于非推荐实体相关属性发生转变而导致的小概率事件的发生,若进行信任更新,会导致后继评估的误差.例如,一个信任度极高的推荐者偶然给出了一个错误信息(由于网络传输造成的数据错误),但其在随后的操作中所提供的信息均极为准确.如果根据仅有的一次错误操作就降低推荐者的信任度,会影响后继操作中评估者的判断.因此在信任度的更新过程中,要尽量减少信任度的大规模"波动".本模型通过利用历史信息使得评估者对于偶然发生的小概率事件所造成的推荐信任较大调整具有较强的抵御能力.另外,对于经常提供恶意信息的推荐者,该方法可以大幅度地降低其可信度,减少其推荐信息对于合并信任的影响,使模型具有抵御恶意推荐信息的能力.

© 中国科学院软件研究所 http://www.jos.org.cn

3 模拟实验与分析

模拟实验初步验证了模型形成与更新推荐信任的合理性,并分析了滑动窗口的作用以及显著水平的选择.

3.1 实验初始场景

模拟实验初始场景如图 6 所示:评估者有 5 个推荐者,相关推荐信息可信度分量依次为 0.5,0.6,0.7,0.8,0.9.评估对象真实信任度为 0.7,即评估对象以 0.7 的概率进行协作活动.评估对象真实信任度对于评估者是不可见的,评估者通过协作获得关于评估对象的直接经验(观测频率),然后利用直接经验评价推荐信息并更新推荐信任.由于模型不承认存在绝对可信的推荐者,因此,实验为信任定义了两个边界值:MAX_*VALUE*=0.999, MIN_*VALUE*=0.001.当可信度大于 MAX_*VALUE* 时,则不再提升;反之,当小于 MIN_*VALUE* 时,则不再将其下调.在学习之前,将每个推荐者的推荐信任设为 *init _op* .事实上,可以将推荐信任设为[MAX_*VALUE*,MIN_*VALUE*]间的任意二元组,初始推荐信任的设定,不会影响学习的结果.

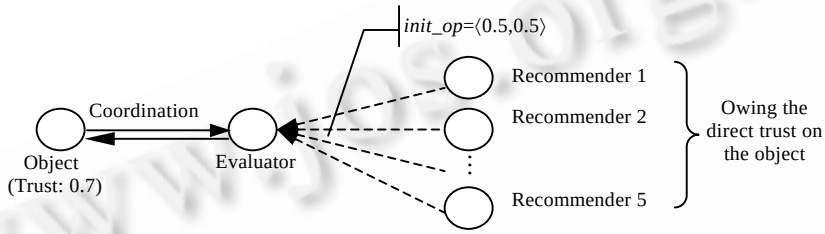
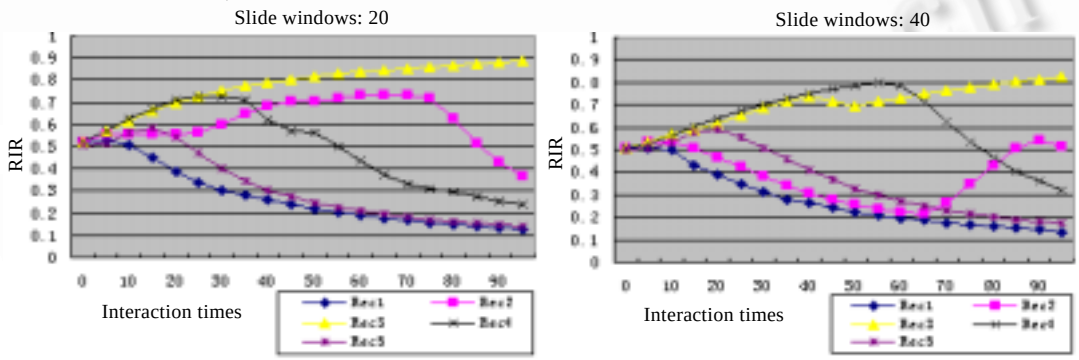


Fig.6 The initial experiment scenario

图 6 实验初始场景

3.2 实验结果与分析

图 7(a)使用了 20 个滑动窗口;图 7(b)使用了 40 个滑动窗口.均采用相同α_0和α_1,分别为 0.2 和 0.05.评估者与评估对象进行 100 次协作,每次协作后,评估者调整每个推荐者的推荐信任,纵坐标标记了推荐信任可信度(RTR)分量.最终,推荐者 3 的信任度是最高的:推荐者 3 的推荐信息与评估对象的真实可信度一致.而推荐者 1 和推荐者 5 的信任度最低,这也与其推荐信息与评估对象差距较大相一致.



(a) (b)

Fig.7 Experimental results (1)

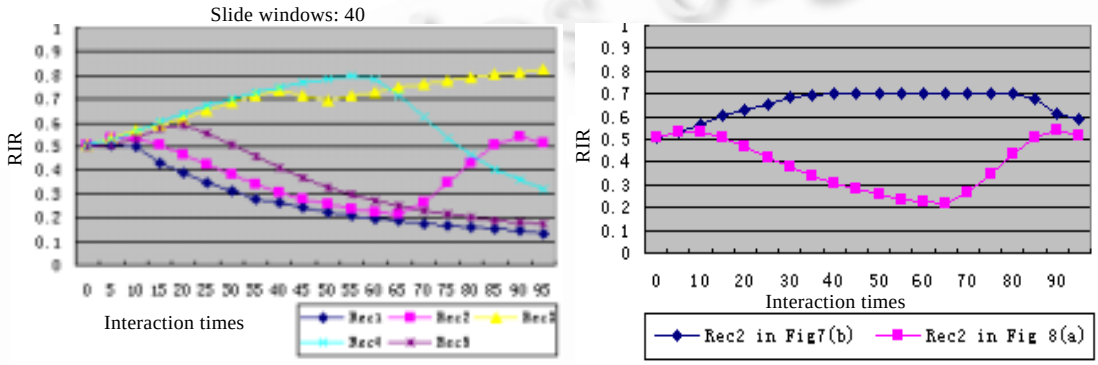
图 7 实验结果(1)

实验显示:大约进行了 20 次协作后,推荐者的推荐信任已有了较大的不同,并且分类比较准确,这表明模型具有较强的分辨能力.比较两组结果:图 7(b)的波动较为平缓;图 7(a)相对而言波动较大.这是由滑动窗口的数量导致的.滑动窗口的数量体现评估实体对于历史信息的看重程度.在图 7(b)中,评估实体较多地看重推荐者的历史信息,即使推荐者有少量的不良推荐行为(例如网络造成数据传输错误),也不会造成推荐信任度的大幅下降.推荐信任关系一旦形成,就会在一个相对稳定的范围内进行“微调”;除非推荐者的信息确实与评估对象有较大差别,否则实体间的推荐关系不会有较大的变化,保持了信任关系的稳定.但过多地看重历史信息会产生一些

© 中国科学院软件研究所 http://www.jos.org.cn

“犹豫”实体,面对恶意推荐者,不能通过较少的协作降低其可信度.实验显示:滑动窗口在 30~40 时可以满足大多数应用的需求.

图 8 采用了 40 个滑动窗口且α_0=α_1=0.12.与图 7(b)相比,图 8(a)中的推荐者 1、推荐者 5 与推荐者 3 的曲线并未发生很大变化,这表明:对于推荐信息不准确或准确的实体来说,使用一个显著水平与使用两个显著水平所造成的推荐度的最终差别并不明显,模型在两种情形下均能显著地降低或提高其可信度.但是,使用两个显著水平还是一个显著水平,会对推荐信息准确度较为模糊的推荐者的信任度产生较大影响.图 8(a)与图 7(b)相比,推荐者 2 与推荐者 4 的推荐信任度曲线均发生了较大的变化.图 8(b)以推荐者 2 为例对比了两种情形下信任曲线的变化情况.使用不同的接受显著水平与拒绝显著水平,使得评估实体在直接经验不充分的情况下,不急于调整相关推荐者的推荐信任度,而是将其维持在现有水平,待直接经验增长到能对推荐信息作出判断的程度时,再对其进行相应的提升或降低.而使用一个显著水平,造成评估者在每次协作之后都会调整推荐信任,当直接经验缺乏时,这种调整是盲目的,造成了推荐度的较大波动.虽然模型在两种情形下最终都能够使得推荐者的信任度趋于稳定,但是就整个信任更新过程来看,同时使用接受显著水平和拒绝显著水平可加大对推荐信息的利用程度.



(a) (b)

Fig.8 Experimental result (2)

图 8 实验结果(2)

4 相关工作

Abdul-Rahman 在 1997 年提出了一个信任模型[8].模型强调实体间信任关系的有条件传递,给出单条路径推荐信任度的公式和综合多条路径的公式;缺点为过于简单,不适用于 Internet 环境.Beth 信任模型[9]采用经验来表述和度量信任关系,并基于经验给出信任度推导和综合公式.不足之处在于:Beth 模型仅仅采用肯定经验对直接信任度度量,信任动态变化机制过于简单;无法抵御恶意推荐所带来的影响.Jøsang 模型[6]引入证据空间和观念空间的概念对信任进行描述和度量,并且基于一套主观逻辑算子给出了信任的传递与合并机制.Jøsang 模型考虑了信任的不确定性,通过综合推荐信息来降低信任的不确定性;不足之处在于:它没有考虑对于恶意信息的处理情况,不具备抵御恶意推荐的能力.TEM 模型[7]利用实体间的交互经验来量化信任关系,提供了信任的量化、传递以及合并多条推荐信息的机制,能够有效处理同源信息经过多条路径传递的情形;不足之处在于:不支持信任的动态变化.本文提出的模型涵盖了上述模型的主要工作:支持信任度量、传递与合并.重大改进在于:增加了信任自动形成与更新功能,支持信任关系动态变化尤其是推荐信任关系的调整,较大程度地减少了人工干预.模型能够降低恶意推荐者的可信度,具有抵御恶意推荐的能力.模型还提出一种基于自治实体的请求推荐模式来处理实体传递合并信任信息的行为,该模式安全、高效、易实现.

5 总 结

本文给出了一种适用于构建网构软件的信任度量及演化模型.主要工作如下:(1) 利用实体间的信任关系来解决软件实体协同过程中的可信性问题;(2) 提供了相关的公式与算子以及一种基于自治实体的请求-推荐

© 中国科学院软件研究所 http://www.jos.org.cn

模式来支持信任信息的传递与合并;(3) 基于贝努里概率模型和假设检验的思想,给出了评价推荐信息的相关机制;(4) 在评价推荐信息的基础上,利用信息论的基本思想来提供相关公式以支持实体间信任关系的演化.该模型可解决以下问题:(1) 支持可信实体的选取;(2) 支持软件实体动态地加入或退出网构软件系统,实体间信任关系可自动形成与更新.模型着重给出了一种动态形成实体间推荐信任关系的合理方法;(3) 利用信任度量支持一种适用于网构软件的"柔性"可信评估机制,可信性的变化通过信任关系的变化体现;(4) 支持相对信任信息的获取.此外,实验证明,该模型具有抵御"恶意"推荐信息的能力.该模型为保障网构软件系统的可信性提供了有效的解决方案.

References:

[1] Yang FQ. Thinking on the development of software engineering technology. Journal of Software, 2005,16(1):1−7 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1.htm

[2] Yang FQ, Mei H, Lü J, Jin Z. Some discussion on the development of software technology. ACTA ELECTRONICA, 2002, 30(12A):1901−1906 (in Chinese with English abstract).

[3] Poladian V, Sousa JP, Garlan D, Shaw M. Dynamic configuration of resource-aware services. In: Proc. of the 26th Int'l Conf. on Software Engineering (ICSE). Edinburgh, 2004. 604−613.

[4] Shaw M. Everyday dependability for everyday needs. In: Proc. of the 13th Int'l Symp. on Software Reliability Engineering. IEEE Computer Society, 2002. 7−11.

[5] Shaw M. Self-Healing: Softening precision to avoid brittleness. In: Proc. of the 1st ACM SIGSOFT Workshop on Self-Healing Systems. 2002. 111−113.

[6] Jøsang A. An algebra for assessing trust in certificate chains. The Internet Society Symp. on Network and Distributed System Security. San Diego, 1999. http://www.idi.ntnu.no/~ajos/papers/algcert.ps

[7] Xu F, Lü J, Zheng W, Cao C. Design of a trust valuation model in software service coordination. Journal of Software, 2003,14(6):1043−1051 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1043.htm

[8] Abdul-Rahman A, Hailes S. A distributed trust model. In: Proc. of the '97 New Security Paradigms Workshop. Cumbria: ACM, 1997. 48−60. http://www.ib.hu-berlin.de/~kuhlen/VERT01/abdul-rahman-trust-model1997.pdf

[9] Beth T, Borcherding M, Klein B. Valuation of trust in open network. In: Gollmann D, ed. Proc. of the European Symp. on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3−18.

[10] Gambetta D. Can we trust trust? In: Gambetta D, ed. Trust: Making and Breaking Cooperative Relations. Blackwell: Oxford Press, 1990. 213−237.

[11] Gao ZX, Chen HJ. Probability and Statistics. Nanjing: Nanjing University Press, 1995 (in Chinese).

附中文参考文献:

[1] 杨芙清.软件工程技术发展思索.软件学报,2005,16(1):1−7. http://www.jos.org.cn/1000-9825/16/1.htm

[2] 杨芙清,梅宏,吕建,金芝.浅论软件技术发展,电子学报,2002,30(12A):1901−1906.

[7] 徐锋,吕建,郑玮,曹春.一个软件服务协同中信任评估模型的设计.软件学报,2003,14(6):1043−1051. http://www.jos.org.cn/1000-9825/14/1043.htm

[11] 高祖新,陈华钧.概率论与数理统计.南京:南京大学出版社,1995.

王远(1980－),男,山东青岛人,博士生,主要研究领域为分布对象技术,可信计算,Web 服务技术.

徐锋(1975－),男,博士,副教授,主要研究领域为可信计算,电子商务安全.

吕建(1960－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为中间件技术,Agent 技术,分布式对象技术.

张林(1982－),男,硕士生,主要研究领域为信任管理,可信计算.

© 中国科学院软件研究所 http://www.jos.org.cn