组件化软件系统的可信度量模型

黄杜娟[1],马艳芳[1],潘海玉[2]
(1. 淮北师范大学 计算机科学与技术学院,安徽 淮北 235000;2. 桂林电子科技大学 计算机与信息安全学院,广西 桂林 541004)

摘 要:软件可信性是保证软件质量的重要因素. 文章以研究组件化软件系统的可信性为目的,以组件自身的属性作为出发点,结合组件的权重和不同组合模式,建立相应的软件系统可信度量模型. 根据组件自身的各种属性,建立单个组件的可信性度量. 结合组件的权重和组件的各种组合方式,分别建立相应系统的可信性度量模型. 通过理论验证,这些模型满足单调性、非负性、凝聚性、敏感性和替代性等代数性质,更有利于开发人员及用户对软件可信性进行分析和度量. 列举相关案例对可信性度量模型进行验证.

关键词:软件可信性;组件;权重;可信性度量模型
中图分类号:TP 311 **文献标识码**:A **文章编号**:2095-0691(2019)02-0043-11

0 引言

软件是信息基础设施的灵魂,在信息化社会占据着越来越重要的地位. 但是在软件的实际应用过程中,常出现一些软件失效的事件,给人们的工作和生活带来不利的影响,甚至造成巨大损失[1]. 软件并不总是值得信任的,所以软件的可信性问题越来越受到人们的关注[2]. 关于软件可信性的研究有很多,如何对软件可信性进行评估和度量,一直是软件可信性研究中的一个重要方面.

目前,国内外学者在软件可信性评估、度量与分配等方面的研究取得很多成果,如陶红伟提出基于属性的软件可信性度量模型,利用属性之间的关系,计算软件系统的可信性[3]. Algirdas[4]提出可信计算的概念,并提出传统软件的可信性主要包括安全性和可靠性. 王怀民等[5]分析云计算的特点以及可能存在的安全威胁,并提出可信云服务的定义. 汤永新等[6]介绍软件可信性认识的演变过程以及软件可信性度量模型的发展变化,总结已有的软件可信性描述性概念和观点. 张俊[7]为确定可信度量中的属性权重,在分析软件属性之间的相互影响及重要性的基础上,提出属性的权重分配方法,对软件可信属性的权重进行预测与分配. 白川等[8]利用经济学的方法来衡量选择可信软件非功能需求策略的方法,提出经济学和需求工程相结合的可信软件非功能需求策略选择框架.

随着软件的复杂性越来越高,传统的开发方法已经不能满足目前软件市场的需要. 近年来,组件开发方法越来越得到广泛应用. 基于组件开发模式所得到软件系统的可靠性、安全性等问题也越来越被研究者重视. 如郑晓东[9]提出利用petri网和组件的思想对软件可靠性进行评估,利用petri网对组件化软件系统进行动态分析和模拟,使软件可靠性的分析结果更加准确. Elshaafi等[10]提出一种新方法,用于推断出分布式环境下复合服务下的单个组件的可信度. Elshaafi等[11]预测由组件组装的服务的可信性. 韩强等[12]针对面向业务流程重组的应用服务器(BPRAS,business process re-engineering oriented application server)在可信性度量方面的不足,给出BPRAS的业务流程建模与可信性度量协助框架,并从构件之间的运算角度建立BPRAS代数模型.

基于组件的开发方法中的代码重用范围可以是某一个特定领域,所以组件技术在很大程度上可以提

收稿日期:2018-09-12
基金项目:国家自然科学基金项目(61672023);安徽省自然科学基金项目(1508085MA14,1708085MF159);安徽高校自然科学研究项目(KJ2017A375)
作者简介:黄杜娟(1994—),女,安徽淮南人,硕士生,研究方向为软件可信性度量模型. **通信作者**:马艳芳(1978—),女,黑龙江大庆人,博士,教授,研究方向为形式化方法、可信计算.

高软件开发的效率和质量. 但是由于组件可以由第三方开发,在一个系统中所用到的组件有可能是用不同的语言编写的,其与已有组件或旧系统之间是否相容、是否匹配,以及组件本身是否灵活等问题. 可能会使新系统产生不可靠、不安全等问题,基于组件的软件允许对其中使用的某个组件进行动态升级,这对系统的测试充分性带来难度[13]. 由此可知组件对软件可信性及软件质量产生很大的影响. 本文从组件本身所拥有的属性为出发点,先研究单个组件的可信性,再与组件的组合模式相结合,建立各个子系统的可信性度量模型,进而求得整个软件系统的可信性度量.

1 预备知识

1.1 软件可信性的定义

要度量软件的可信性,首先要确定软件可信性的概念. 目前,关于软件可信性的定义还没有一个统一的说法. ISO/IEC 15408标准关于可信性的描述:参与计算的组件,其操作或过程在任意操作条件下是可以预测的,并能够抵抗病毒以及一定的物理干扰[14]. 可信计算机组织认为,一个实体总是遵循其设定目标所期望的方式运行,则这个实体是可信的[15]. 美国国家研究委员会(NRC)提出,一个软件可信的条件是即使在环境发生崩溃、操作人员发生失误或者遭遇外来攻击时,该软件仍然可以按照人们的预期运行[16]. 刘克等[2]认为,可信性是一个综合性的概念,是对诸多属性的一个综合反映,是在正确性、可靠性、安全性和时效性等众多概念的基础上建立的,认为软件的可信是指软件系统的动态行为及其结果总是符合人们的预期,并在受到干扰时仍然能够提供连续的服务. 这里所说的干扰主要包括操作错误、环境影响、外部攻击等. 本文所采用的可信性定义为文献[3]中所提出的定义,软件可信性是指软件的行为和结果符合用户期望,并在受到干扰时仍能提供连续服务的能力.

关于软件可信性的定义没有一个较为明确的说法,但可信性通常被看作是一个综合概念,可以通过属性来刻画[3]. Steffen认为软件可信性应该由其包含的可信属性进行描述,这里的可信属性包括正确性、私密性、安全性、防危性、服务质量,其中,服务质量又包括可用性、可靠性和性能[17-18]. 在文献[3]中也从属性的角度对软件可信性进行度量,给出基于分层和权重的软件可信性度量模型的构造准则,即一个软件的可信性度量模型若满足非负性、单调性、凝聚性、敏感性和替代性5个性质,这个度量模型就是合理的.

1.2 组件的可信度量模型

组件是具有一定功能,能够独立工作或同其他组件协调工作的程序体[9]. 组件是对数据和方法的简单封装,只有接口是可见的,通过接口与外界交互. 组件本身拥有很多可信属性,每一个单个组件都可看作是一个小型的软件体系结构. 它的可信属性如正确性、安全性和可靠性等性质决定这个组件本身的质量,故通过分析文献[3]中给出的软件可信性度量模型,可以建立单个组件的可信性度量模型:假设 $y_1,y_2,\cdots,y_i\cdots,y_m$ 为某个组件的 m 个属性值,且 $0<y_i\leqslant 1\ (1\leqslant i\leqslant m)$, $\alpha_1,\alpha_2,\cdots,\alpha_m$ 为第 i 种属性在所有属性中所占权重,且 $0<\alpha_i\leqslant 1$, $\sum_{i=1}^{m}\alpha_i=1$, T 表示单个组件的可信度. 对文献[3]中有关公式进行简化,得到关于单个组件的可信性度量模型:

$$T_C=y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_i^{\alpha_i}\cdots y_m^{\alpha_m}. \tag{1}$$

由文献[3]可知,该模型满足非负性、单调性、凝聚性、敏感性和替代性这5种性质,据此可提出定理1.

定理1 (1) T_C 关于每个属性值 $y_i\ (1\leqslant i\leqslant m)$ 是单调递增函数.

(2) $0<T_C\leqslant 1$.

(3) T_C 满足凝聚性准则,即对于所有的 $1\leqslant i\leqslant m$,有 $\dfrac{\partial^2 T_C}{\partial y_i^2}\leqslant 0$.

(4) T_C 对所有属性都敏感.

(5)在 T_C 中各属性之间具有替代性.

证明　(1)因为 $\frac{\partial T_C}{\partial y_i}=\alpha_i y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_i^{\alpha_i-1}\cdots y_m^{\alpha_m}\ (1\leqslant i\leqslant m)$，可知 $\frac{\partial T}{\partial y_i}>0\ (1\leqslant i\leqslant m)$，即 T_C 关于每个 y_i $(1\leqslant i\leqslant m)$ 单调递增. 也就是说,对于单个组件来说,如果提升组件中某个属性的属性值,则整个组件的可信性值也会有所提升.

(2)由上可知 T_C 关于每一个 $y_i(1\leqslant i\leqslant m)$ 单调递增,又因为 $0<y_i\leqslant 1$ 且 $1\leqslant i\leqslant m$，所以 $0<T_C\leqslant 1$. 即组件的可信性属于 $(0,1]$,符合可信性的一般规律.

(3)对于 T_C 关于每一个 y_i 求二阶导数可得，$\frac{\partial^2 T_C}{\partial y_i^2}=\alpha_i(\alpha_i-1)y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_i^{\alpha_i-2}\cdots y_m^{\alpha_m}$，因为当 $1\leqslant i\leqslant m$ 时，有 $0<\alpha_i\leqslant 1$，所以 $\frac{\partial^2 T_C}{\partial y_i^2}\leqslant 0$. 即对于所有的 $1\leqslant i\leqslant m$，T_C 都满足凝聚性准则. 也就是说,对于单个组件来说,提高某个属性的属性值,组件的可信性值会增加,但是当属性值提升到某一程度时,组件的可信性值将增加缓慢,甚至难以增加. 这也说明一味地增加属性值有时候可能对组件可信性值提升的效果并不明显.

(4)模型 T_C 关于每个属性的灵敏性为 $\frac{\partial T_C}{\partial y_i}\cdot\frac{y_i}{T_C}=\frac{\alpha_i y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_i^{\alpha_i}\cdots y_m^{\alpha_m}}{T_C}=\alpha_i$，$1\leqslant i\leqslant m$. 故 T_C 关于属性的灵敏性与 α_i（$1\leqslant i\leqslant m$）相关. 也就是说,任何一个属性所占权重发生变动都会影响组件的可信性,即组件的可信性应该与每一个属性所占的权重相关.

(5)由计算可得 $h_{ij}=-\frac{\partial T/\partial y_j}{\partial T/\partial y_i}=-\frac{\alpha_j}{\alpha_i}\cdot\frac{y_i}{y_j}$，$1\leqslant i,j\leqslant m$，$\sigma_{ij}=\frac{\mathrm{d}\left(\frac{y_i}{y_j}\right)}{\mathrm{d}(h_{ij})}\frac{h_{ij}}{\frac{y_i}{y_j}}=\frac{\mathrm{d}\left(\frac{y_i}{y_j}\right)}{-\frac{\alpha_j}{\alpha_i}\mathrm{d}\left(\frac{y_i}{y_j}\right)}\left(-\frac{\alpha_j}{\alpha_i}\right)=1$. 所以,在该模型中,各属性之间可以发生替代性. 即只增加或减少其中一对属性值 y_i 和 y_j，并保持其他属性值不变,可以保持组件的可信性不变.

综上,该模型满足单调性、非负性、凝聚性、灵敏性和替代性5种性质.

2　系统的可信度量模型

软件系统是通过自底向上的方式逐层构建的,每一层的构造方式都比较简单,都是由几种典型的模型构成,可以按照软件系统的构造方式来逐层计算系统的可信性[19]. 将整个软件系统划分为若干个子系统,每个子系统由多个组件构成,组件之间通过顺序、分支、并行和循环结构构成. 首先,分别讨论这4种典型的构造方式,并计算出各种构造方式所对应的子系统的可信性度量. 然后,再根据子系统的可信性度量模型计算出整个系统的可信性.

通过上面对单个组件可信性度量模型的分析,本节将从组件的角度出发,在得到组件可信性度量模型的基础上,建立软件可信性度量模型,并对其进行理论验证. 假设 $C_1,C_2,\cdots,C_n$ 为构成子系统的组件，δ_i 为第 $i\ (1\leqslant i\leqslant n)$ 个组件在子系统中所占的权重,其反映第 i 个组件的重要程度，$0<\delta_i\leqslant 1$ 且 $\sum_{i=1}^{n}\delta_i=1$. 利用公式(1)可以计算出软件系统中单个组件的可信度,假设第 i 个组件的可信度为 T_{C_i}，且 $0<T_{C_i}\leqslant 1$.

对于一个简单的软件子系统,通常可以由组件通过顺序、分支、并行和循环等结构组成. 下面对于这4种情况组成的子系统进行建模与验证.

2.1 组件通过顺序结构构成的子系统

若组件之间是通过顺序结构构成的子系统,则可假设子系统 S 由组件 $C_1, C_2, \cdots, C_n$ 顺序组成. 如图1所示:

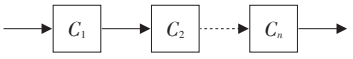

图1 顺序结构框图

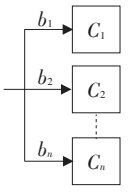

图2 分支结构框图

则该子系统的可信性度量模型为:

$$T_S = T_{C_1}^{\delta_1} T_{C_2}^{\delta_2} \cdots T_{C_n}^{\delta_n}. \tag{2}$$

由于式(2)与式(1)结构相同,所以类似于定理1的证明可得:T_S 满足单调性、非负性、凝聚性、灵敏性和替代性5点性质,此处不再证明.

2.2 组件通过分支结构构成的子系统

分支结构是一种常见的组件组合结构. 在分支结构中,程序每次运行都会以一定的概率选择一个分支去运行[19]. 由于组件的重要程度可通过组件权重的高低来反映,这里假设用每个组件被选中的概率来表示这个组件的权重. 若该分支结构由组件 $C_1, C_2, \cdots, C_n$ 组成,分支结构如图2所示,当满足不同的条件时,子系统选择不同的组件执行.

则该子系统的可信性度量模型为

$$T_B = \frac{\sum_{i=1}^{n} (T_{C_i}^{\delta_i})}{n}. \tag{3}$$

该模型满足非负性、单调性、凝聚性、敏感性和替代性5种性质,据此可提出定理2.

定理2 (1) T_B 关于每个组件的可信度 T_{C_i} $(1 \leqslant i \leqslant n)$ 是单调递增函数.

(2) $0 < T_B \leqslant 1$.

(3) T_B 满足凝聚性准则,即对于所有的 $1 \leqslant i \leqslant n$,有 $\frac{\partial^2 T_B}{\partial T_{C_i}^2} \leqslant 0$.

(4) T_B 对所有组件都敏感.

(5)在 T_B 中各组件之间具有替代性.

证明 (1)由 $\frac{\partial T_B}{\partial T_{C_i}} = \frac{1}{n}\delta_i T_{C_i}^{\delta_i - 1}$,且 $0 < \delta_i \leqslant 1$, $1 \leqslant i \leqslant n$, $0 < T_{C_i} \leqslant 1$,所以 $\frac{\partial T_B}{\partial T_{C_i}} > 0$,即 T_B 关于每个组件的可信度 T_{C_i} $(1 \leqslant i \leqslant n)$ 是单调递增函数. 也就是说在分支结构中,增加组件的可信度 T_{C_i} ,会使整个子系统的可信性得到提升.

(2)因为 $0 < T_{C_i} \leqslant 1$, $0 < \delta_i \leqslant 1$,所以 $T_B > 0$,且当 $T_{C_i} = 1$ 时, $T_B = 1$. 又因为 T_B 关于每个组件的可信度 T_{C_i} 是单调递增函数,所以 $T_B \leqslant 1$,即 $0 < T_B \leqslant 1$.

(3)由于 $\frac{\partial^2 T_B}{\partial T_{C_i}^2} = \frac{1}{n}\delta_i(\delta_i - 1) T_{C_i}^{\delta_i - 2}$,且 $0 < \delta_i \leqslant 1$,所以 $\frac{\partial^2 T_B}{\partial T_{C_i}^2} \leqslant 0$,即 T_B 满足凝聚性准则. 对于子系统来说,并不是一味地增加组件的可信度就能使整个子系统的可信性有很好的提升,当组件的可信度增加到某个高度时,该组件对子系统可信性的影响会逐渐变小.

(4) T_B 关于每个组件的灵敏性为 $\frac{\partial T_B}{\partial T_{C_i}} \cdot \frac{T_{C_i}}{T_B} = \frac{\delta_i . T_{C_i}^{\delta_i - 1} T_{C_i}}{n T_B} = \frac{\delta_i . T_{C_i}^{\delta_i}}{n T_B}, 1 \leqslant i \leqslant n$,故 T_B 关于组件的灵敏性与 δ_i $(1 \leqslant i \leqslant n)$ 相关. 即 T_B 对所有组件都敏感,任何一个组件的权重对子系统可信性的影响都很大.

(5)由计算可得

$$h_{ij}=-\frac{\partial T_B/\partial T_{C_j}}{\partial T_B/\partial T_{C_i}}=-\frac{\delta_j}{\delta_i}\frac{T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i-1}},1\leqslant i,j\leqslant n\ ,$$

$$\sigma_{ij}=\frac{\mathrm{d}\left(\frac{T_{C_i}}{T_{C_j}}\right)}{\mathrm{d}\left(h_{ij}\right)}\frac{h_{ij}}{\frac{T_{C_i}}{T_{C_j}}}=\left(-\frac{\delta_j}{\delta_i}\frac{T_{C_j}^{\delta_j}}{T_{C_i}^{\delta_i}}\right)\frac{\frac{1}{T_{C_j}}\mathrm{d}\left(T_{C_i}\right)-\frac{T_{C_i}}{T_{C_j}^2}\mathrm{d}\left(T_{C_j}\right)}{-\frac{\delta_j}{\delta_i}\left(\frac{(\delta_j-1)T_{C_j}^{\delta_j-2}}{T_{C_i}^{\delta_i-1}}\mathrm{d}\left(T_{C_j}\right)-\frac{\left(\delta_i-1\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}}\mathrm{d}(T_{C_i})\right)}$$

$$=\frac{\frac{1}{T_{C_j}}-\frac{T_{C_i}}{T_{C_j}^{\ 2}}\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}}{-\frac{\left(\delta_i-1\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}}+\frac{(\delta_j-1)T_{C_j}^{\delta_j-2}}{T_{C_i}^{\delta_i-1}}\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}}\frac{T_{C_j}^{\delta_j}}{T_{C_i}^{\delta_i}}.$$

又因为 $\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}=-\frac{\partial T_B/\partial T_{C_i}}{\partial T_B/\partial T_{C_j}}=-\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i-1}}{T_{C_j}^{\delta_j-1}}$，所以

$$\sigma_{ij}=\frac{\frac{1}{T_{C_j}}+\frac{T_{C_i}}{T_{C_j}^2}\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i-1}}{T_{C_j}^{\delta_j-1}}}{-\frac{\left(\delta_i-1\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}}-\frac{(\delta_j-1)T_{C_j}^{\delta_j-2}}{T_{C_i}^{\delta_i-1}}\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i-1}}{T_{C_j}^{\delta_j-1}}}\frac{T_{C_j}^{\delta_j}}{T_{C_i}^{\delta_i}}=\frac{T_{C_j}^{\delta_j-1}+\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i}}{T_{C_j}}}{\left(1-\delta_i\right)T_{C_j}^{\delta_j-1}+\frac{\delta_i}{\delta_j}\frac{(1-\delta_j)T_{C_i}^{\delta_i}}{T_{C_j}}}.$$

所以，在模型 T_B 中，各组件之间可以发生替代，其替代性为

$$\sigma_{ij}=\frac{T_{C_j}^{\delta_j-1}+\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i}}{T_{C_j}}}{\left(1-\delta_i\right)T_{C_j}^{\delta_j-1}+\frac{\delta_i}{\delta_j}\frac{(1-\delta_j)T_{C_i}^{\delta_i}}{T_{C_j}}},\ 1\leqslant i,j\leqslant n\ .$$

由上可知，T_B 满足单调性、非负性、凝聚性、灵敏性和替代性这5点性质.

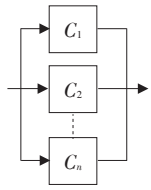

图3　并行结构框图

2.3　组件通过并行结构构成的子系统

对于并行结构并没有明确的定义，分为如下2种基本情况进行讨论. 第1种是与并行，即只有当并行结构的所有组件都能成功运行时，才可以称这个并行结构是成功的[19]. 对于可信性的度量方法等同于顺序结构中的求法，此处不再证明.

第2种是或并行，即有一个组件运行成功即可. 假设并行结构由组件 $C_1,C_2,\cdots,C_n$ 组成（如图3所示），则该子系统的可信度量模型为：

$$T_P=1-\prod_{i=1}^{n}(1-T_{C_i}^{\ \delta_i}).\tag{4}$$

该模型满足非负性、单调性、凝聚性、敏感性、替代性这5种性质，据此可提出定理3.

定理3　(1) T_P 关于每个组件的可信度 T_{C_i} $(1\leqslant i\leqslant n)$ 是单调递增函数.

(2) $0<T_P\leqslant 1$.

(3) T_P 满足凝聚性准则，即对于所有的 $(1\leqslant i\leqslant n)$，有 $\frac{\partial^2 T_P}{\partial T_{C_i}^2}\leqslant 0$.

(4) T_P 对所有组件都敏感.

(5)在 T_P 中各组件之间具有替代性.

证明 (1)由于 $\frac{\partial T_P}{\partial T_{C_i}}=\delta_i T_{C_i}^{\delta_i-1}\prod_{j=1,j\neq i}^{n}(1-T_{C_j}^{\delta_j})$,且 $0<\delta_i\leqslant 1$,$0<T_{C_i}\leqslant 1$,所以 $\frac{\partial T_P}{\partial T_{C_i}}>0$. 故该模型关于 T_{C_i} 为单调递增函数.

(2)由 $T_P=1-\prod_{i=1}^{n}(1-T_{C_i}^{\delta_i})$ 且 $0<\delta_i\leqslant 1$,$0<T_{C_i}\leqslant 1$,所以 $0\leqslant 1-T_{C_i}^{\delta_i}<1$,故 $0\leqslant\prod_{i=1}^{n}(1-T_{C_i}^{\delta_i})<1$,即 $0<T_P\leqslant 1$.

(3)由 $\frac{\partial^2 T_P}{\partial T_{C_i}^{\ 2}}=\delta_i(\delta_i-1)T_{C_i}^{\delta_i-2}\prod_{j=1,j\neq i}^{n}(1-T_{C_j}^{\delta_j})$ 且 $0<\delta_i\leqslant 1, 0<T_{C_i}\leqslant 1$,所以 $\frac{\partial^2 T_P}{\partial T_{C_i}^{\ 2}}\leqslant 0$.即 T_P 满足凝聚性准则.

(4)模型 T_P 关于每个组件的灵敏性为 $\frac{\partial T_P}{\partial T_{C_i}}\frac{T_{C_i}}{T_P}=\frac{\delta_i T_{C_i}^{\delta_i}\prod_{j=1,j\neq i}^{n}(1-T_{C_j}^{\delta_j})}{T_P}$,$1\leqslant i,j\leqslant n$,故 T_P 关于所有组件都敏感.

(5)由计算可得 $h_{ij}=-\frac{\partial T_P/\partial T_{C_j}}{\partial T_P/\partial T_{C_i}}=\frac{\delta_j}{\delta_i}\frac{T_{C_j}^{\delta_j-1}\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i-1}\left(1-T_{C_j}^{\delta_j}\right)}$,$1\leqslant i,j\leqslant n$,所以

$$\sigma_{ij}=\frac{\mathrm{d}\left(\frac{T_{C_i}}{T_{C_j}}\right)}{\mathrm{d}\left(h_{ij}\right)}\frac{h_{ij}}{\frac{T_{C_i}}{T_{C_j}}}$$

$$=\frac{\delta_j}{\delta_i}\frac{T_{C_j}^{\delta_j}\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}\frac{\frac{1}{T_{C_j}}\mathrm{d}\left(T_{C_i}\right)-\frac{T_{C_i}}{T_{C_j}^{\ 2}}\mathrm{d}\left(T_{C_j}\right)}{\frac{\delta_j}{\delta_i}\left(\frac{\left(1-T_{C_i}^{\delta_i}-\delta_i\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}\mathrm{d}\left(T_{C_i}\right)+\frac{\left(\left(\delta_j-1\right)T_{C_j}^{\delta_j-2}+T_{C_j}^{2\delta_j-2}\right)\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i-1}\left(1-T_{C_j}^{\delta_j}\right)^2}\mathrm{d}\left(T_{C_j}\right)\right)}$$

$$=\frac{\frac{1}{T_{C_j}}-\frac{T_{C_i}}{T_{C_j}^2}\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}}{\frac{\left(1-T_{C_i}^{\delta_i}-\delta_i\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}+\frac{\left(\left(\delta_j-1\right)T_{C_j}^{\delta_j-2}+T_{C_j}^{2\delta_j-2}\right)\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i-1}\left(1-T_{C_j}^{\delta_j}\right)^2}\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}}\frac{T_{C_j}^{\delta_j}\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}.$$

因为

$$\frac{\mathrm{d}\left(T_{C_j}\right)}{\mathrm{d}\left(T_{C_i}\right)}=-\frac{\partial T_P/\partial T_{C_i}}{\partial T_P/\partial T_{C_j}}=\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i-1}\left(1-T_{C_j}^{\delta_j}\right)}{T_{C_j}^{\delta_j-1}\left(1-T_{C_i}^{\delta_i}\right)},$$

所以

$$\sigma_{ij}=\frac{\frac{1}{T_{C_j}}-\frac{\delta_i}{\delta_j}\frac{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}{T_{C_j}^{\delta_j+1}\left(1-T_{C_i}^{\delta_i}\right)}}{\frac{\left(1-T_{C_i}^{\delta_i}-\delta_i\right)T_{C_j}^{\delta_j-1}}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}+\frac{\left(\delta_j-1\right)+T_{C_j}^{\delta_j}}{T_{C_j}\left(1-T_{C_j}^{\delta_j}\right)}\frac{\delta_i}{\delta_j}}\frac{T_{C_j}^{\delta_j}\left(1-T_{C_i}^{\delta_i}\right)}{T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}$$

$$=\frac{T_{C_j}^{\delta_j-1}\left(1-T_{C_i}^{\delta_i}\right)-\frac{\delta_i}{\delta_j}T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}{\left(1-T_{C_i}^{\delta_i}-\delta_i\right)T_{C_j}^{\delta_j-2}+\left(\left(\delta_j-1\right)+T_{C_j}^{\delta_j}\right)T_{C_j}^2T_{C_i}^{\delta_i-1}\frac{\delta_i}{\delta_j}}.$$

所以组件之间的替代性为

$$\sigma_{ij}=\frac{T_{C_j}^{\delta_j-1}\left(1-T_{C_i}^{\delta_i}\right)-\frac{\delta_i}{\delta_j}T_{C_i}^{\delta_i}\left(1-T_{C_j}^{\delta_j}\right)}{\left(1-T_{C_i}^{\delta_i}-\delta_i\right)T_{C_j}^{\delta_j-2}+\left(\left(\delta_j-1\right)+T_{C_j}^{\delta_j}\right)T_{C_j}^{2}T_{C_i}^{\delta_i-1}\frac{\delta_i}{\delta_j}}.$$

综上可知,模型 T_P 满足单调性、非负性、凝聚性、灵敏性和替代性这5点性质.

2.4　组件之间通过循环结构构成的子系统

循环结构也是软件系统中最常出现的结构,系统中某个或多个组件被重复执行多次,则构成循环结构. 假设循环体为 A ,当满足一定条件时,执行 t 次循环,当不满足条件时跳出循环.

若循环体由组件 $C_1,C_2,\cdots,C_n$ 组成,循环次数 $t\geqslant 1$. 用 T_A 来表示循环体 A 的可信度,组件通过循环结构组成的子系统框图如图4所示. 则该循环结构的可信性模型为:

$$T_L=T_A^{\,t}. \tag{5}$$

如果,循环体 A 为顺序结构,则 $T_A=T_S$;如果循环体 A 为分支结构,则 $T_A=T_B$;如果循环体 A 为并行结构,则 $T_A=T_P$. 当 $t=1$ 时,式(5)可化为式(2)~(5),均满足单调性、非负性、凝聚性、敏感性和替代性. 下面验证当 $t>1$ 时,这5条性质的满足情况.

当循环体 A 为顺序结构时,该循环结构满足定理4.

定理4

(1) T_L 关于每个组件的可信度 $T_{C_i}(1\leqslant i\leqslant n)$ 是单调递增函数.

(2) $0<T_L\leqslant 1$.

(3) T_L 在一定条件下满足凝聚性准则,即在 $t\leqslant\left\lfloor\frac{1}{\delta_i}\right\rfloor$ 时,有 $\frac{\partial^2 T_L}{\partial T_{C_i}^2}\leqslant 0$.

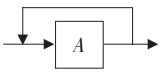

图4　循环结构框图

(4) T_L 对所有循环组件是敏感的.

(5)在 T_L 中各组件之间具有替代性.

证明　(1)由 $T_L=T_{C_1}^{t\delta_1}T_{C_2}^{t\delta_2}\cdots T_{C_n}^{t\delta_n}$ 得, $\frac{\partial T_L}{\partial T_{C_i}}=t\delta_i T_{C_1}^{t\delta_1}T_{C_2}^{t\delta_2}\cdots T_{C_i}^{t\delta_i-1}\cdots T_{C_n}^{t\delta_n}$,其中 $0<\delta_i\leqslant 1$, $0<T_{C_i}\leqslant 1$,所以, $\frac{\partial T_L}{\partial T_{C_i}}>0(1\leqslant i\leqslant n)$,即 T_L 关于每个组件的可信度单调递增. 对于由顺序结构组成的循环系统,增加每个组件的可信度 T_{C_i} ,都会使整个子系统的可信性得到提升.

(2)因为 T_L 关于每一个 $T_{C_i}(1\leqslant i\leqslant n)$ 单调递增,且 $0<T_{C_i}\leqslant 1$, $0<\delta_i\leqslant 1$, $t>1$,所以 $0<T_L\leqslant 1$,即模型 T_L 的可信性属于 $(0,1]$.

(3)对于 T_L 关于每一个 T_{C_i} 求二阶导数可以得到 $\frac{\partial^2 T_L}{\partial T_{C_i}^2}=t\delta_i\left(t\delta_i-1\right)T_{C_1}^{t\delta_1}T_{C_2}^{t\delta_2}\cdots T_{C_i}^{t\delta_i-2}\cdots T_{C_n}^{t\delta_n}$,因为 $0<T_{C_i}\leqslant 1$, $0<\delta_i\leqslant 1$, $t>1$. 所以 $t\delta_i T_{C_1}^{t\delta_1}T_{C_2}^{t\delta_2}\cdots T_{C_i}^{t\delta_i-2}\cdots T_{C_n}^{t\delta_n}>0$,当 $t\delta_i-1\leqslant 0$,即 $t\leqslant\frac{1}{\delta_i}$ 时,取 $t\leqslant\left\lfloor\frac{1}{\delta_i}\right\rfloor$,有 $\frac{\partial^2 T_L}{\partial T_{C_i}^2}\leqslant 0$,故在该条件下满足凝聚性准则. 当 $t>\frac{1}{\delta_i}$ 时, $\frac{\partial^2 T_L}{\partial T_{C_i}^2}>0$,在这个条件下,模型 T_L 不满足凝聚性准则. 即对于由顺序结构构成的循环系统来说,只有当 $t\leqslant\left\lfloor\frac{1}{\delta_i}\right\rfloor$ 时,该模型才会满足凝聚性准则,在其他条件下,都不满足凝聚性准则的.

(4)模型 T_L 关于每个组件的灵敏性为 $\frac{\partial T_L}{\partial T_{C_i}}\frac{T_{C_i}}{T_L}=\frac{t\delta_i T_{C_1}^{t\delta_1}T_{C_2}^{t\delta_2}\cdots T_{C_i}^{t\delta_i-1}\cdots T_{C_n}^{t\delta_n}T_{C_i}}{T_L}=t\delta_i$, 故 T_L 对该组件是敏感的,且关于每个组件的灵敏性与 $t\delta_i$ 相关,即在该循环系统中,每个组件所占权重以及它循环的次数对整个子系统的可信性都是有影响的,当各个组件所占权重或循环次数发生变动都会影响子系统的可信性.

(5)若该模型中循环体为单个组件,则不存在替代性. 此处考虑的组件个数大于1.

由计算可得 $h_{ij}=-\dfrac{\partial T'_L/\partial T_{C_j}}{\partial T'_L/\partial T_{C_i}}=-\dfrac{\delta_j}{\delta_i}\dfrac{T_{C_i}}{T_{C_j}}$,$1\leqslant i,j\leqslant n$. 所以 $\sigma_{ij}=\dfrac{\mathrm{d}\left(\dfrac{T_{C_i}}{T_{C_j}}\right)}{\mathrm{d}\left(h_{ij}\right)}\dfrac{h_{ij}}{\dfrac{T_{C_i}}{T_{C_j}}}=\dfrac{\mathrm{d}\left(\dfrac{T_{C_i}}{T_{C_j}}\right)}{-\dfrac{\delta_j}{\delta_i}\mathrm{d}\left(\dfrac{T_{C_i}}{T_{C_j}}\right)}\left(-\dfrac{\delta_j}{\delta_i}\right)=1$. 所以各组件之间可以发生替代,替代性为 $\sigma_{ij}=1$. 故可以根据用户的需求,对各个组件作出相应调整,以此来更好地满足用户需求.

综上可知,当循环体为顺序结构时,模型 T_L 满足单调性、非负性、灵敏性以及替代性,并且在一定条件下可满足凝聚性.

当循环体 A 为分支结构时,采用数学归纳法进行证明. 当 $t=1$ 时,式(5)可化为式(3),此时是满足5条性质的. 假设当 $t=d$ 时同样满足这5条性质,现在证明当 $t=d+1$ 时是否满足这5条性质.

当 $t=1$ 时,有 $T_L=T_B=\dfrac{\sum_{i=1}^{n}(T_{C_i}^{\delta_i})}{n}$ (①);当 $t=d$ 时,有 $T_L^{(d)}=T_B{}^d=(\dfrac{\sum_{i=1}^{n}(T_{C_i}^{\delta_i})}{n})^d$ (②);那么当 $t=d+1$ 时,有 $T_L^{(d+1)}=T_L^{(d)}T_B$ 且 $\dfrac{\partial T_L^{(d+1)}}{\partial T_{C_i}}=\dfrac{\partial T_L^{(d)}}{\partial T_{C_i}}T_B+T_L^{(d)}\dfrac{\partial T_B}{\partial T_{C_i}}$.

很容易验证该模型满足单调性、非负性和凝聚性. 接下来,考察该情况下此模型是否满足敏感性和替代性.

首先看敏感性:$\dfrac{\partial T_L^{(d+1)}}{\partial T_{C_i}}\dfrac{\partial T_{C_i}}{\partial T_L^{(d+1)}}=\dfrac{\partial T_L^{(d)}}{\partial T_{C_i}}\dfrac{T_{C_i}}{T_L^{(d)}}+\dfrac{\partial T_B}{\partial T_{C_i}}\dfrac{T_{C_i}}{T_B}$,由于①②式满足敏感性,所以,当 $t=d+1$ 时,也满足敏感性.

接下来,看替代性:通过计算,可以得到

$$h_{ij}^{(d)}=-\frac{\partial T_L^{(d)}/\partial T_{C_j}}{\partial T_L^{(d)}/\partial T_{C_i}}=-\frac{\mathrm{d}T_B^{d-1}\partial T_B/\partial T_{C_j}}{\mathrm{d}T_B^{d-1}\partial T_B/\partial T_{C_i}}=h_{ij}^{(B)};$$

$$h_{ij}^{(d+1)}=-\frac{\partial T_L^{(d+1)}/\partial T_{C_j}}{\partial T_L^{(d+1)}/\partial T_{C_i}}=-\frac{\dfrac{\partial T_L^{(d)}}{\partial T_{C_j}}T_B+T_L^{(d)}\dfrac{\partial T_B}{\partial T_{C_j}}}{\dfrac{\partial T_L^{(d)}}{\partial T_{C_i}}T_B+T_L^{(d)}\dfrac{\partial T_B}{\partial T_{C_i}}}=-\frac{\mathrm{d}T_B^{d-1}\dfrac{\partial T_B}{\partial T_{C_j}}T_B+T_L^{(d)}\dfrac{\partial T_B}{\partial T_{C_j}}}{\mathrm{d}T_B^{d-1}\dfrac{\partial T_B}{\partial T_{C_i}}T_B+T_L^{(d)}\dfrac{\partial T_B}{\partial T_{C_i}}}=\frac{\mathrm{d}T_B^{d-1}h_{ij}^{(B)}T_B+T_L^{(d)}h_{ij}^{(B)}}{\mathrm{d}T_B^{d-1}T_B+T_L^{(d)}}=h_{ij}^{(B)},$$

所以,该模型满足替代性.

当循环体 A 为并行结构时,通过数学归纳法同样可以证明满足这5大性质,具体过程不再赘述.

2.5 整个系统的可信性

对于一个复杂系统来说,它可以分解成若干个子系统,假设为 $S_1,S_2,\cdots,S_N$,而通过式(2)~(5)可以得到每个子系统的可信度量值. 假设每个子系统的重要性都是相同的,且 $0<T_{S_i}\leqslant 1$,那么整个系统的可信性度量可以通过下面的公式计算:

$$T_{WS}=\frac{\sum_{i=1}^{n}(T_{S_i})}{N} \tag{6}$$

由分析可知,该模型同样满足非负性、单调性、凝聚性、敏感性、替代性,据此得出定理5.

定理5 (1) T_{WS} 关于每个子系统的可信度 $T_{S_i}(1\leqslant i\leqslant N)$ 是单调递增函数.

(2) $0<T_{WS}\leqslant 1$.

(3) T_{WS} 满足凝聚性准则,即对于所有的 $1\leqslant i\leqslant N$,有 $\dfrac{\partial^2 T_{WS}}{\partial T_{S_i}^2}\leqslant 0$.

(4) T_{WS} 对所有组件都敏感.

(5)在 T_{WS} 中各组件之间具有替代性.

由于式(6)与式(3)相类似,定理5的证明类似于定理2,所以很容易证明该模型满足单调性、非负性、凝聚性、敏感性和替代性. 此处不再证明.

3　实验与分析

本文选取点餐网站来验证所述方法的正确性. 这个订餐网主要包含:登录、选餐、付款和订单是否完成这几个部分,该系统可以简化为登录、选餐和付款3个子系统. 其中,选餐模块又包括选择早餐、正餐、下午茶、夜宵等,可抽象为各个不同的组件. 当用户需要订餐时,先登录该网站,然后选择订餐种类,再进入店铺中进行选餐. 选餐完成后即可预订订单并完成付款,待订餐送达后,订单即完成.

本网站系统中组件之间的可信性框图可抽象为图5. 其中,组件 C_2~C_5 之间是分支结构,根据用户自己的需求进行选择. 组件 C_6~C_9 之间是或并行结构,进行选择其中之一后根据用户的需求可以选择执行循环的次数. 选餐完成后提交订单完成付款,整个订餐操作完成. 关于各个组件的属性及权重数据由软件专业人员提供,如表1所示.

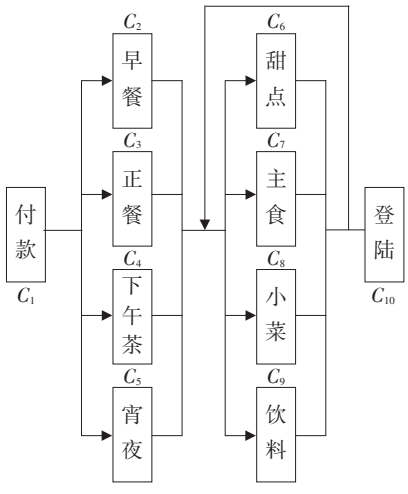

图5　订餐系统的组件可信性框图

表1　组件属性及权重

组件	可靠性/权重	正确性/权重	安全性/权重	可用性/权重
C_1	0.7/0.2	0.9/0.2	0.9/0.5	0.8/0.1
C_2	0.7/0.1	0.8/0.2	0.7/0.6	0.6/0.1
C_3	0.8/0.2	0.7/0.1	0.9/0.6	0.7/0.1
C_4	0.9/0.3	0.7/0.1	0.9/0.5	0.8/0.1
C_5	0.8/0.2	0.6/0.2	0.8/0.5	0.7/0.1
C_6	0.65/0.1	0.6/0.1	0.95/0.6	0.6/0.2
C_7	0.7/0.1	0.5/0.1	0.8/0.7	0.7/0.1
C_8	0.8/0.2	0.5/0.1	0.8/0.6	0.65/0.1
C_9	0.9/0.3	0.8/0.25	0.8/0.3	0.7/0.15
C_{10}	0.95/0.3	0.85/0.2	0.9/0.3	0.8/0.2

先计算各组件的可信性:

$T_{C_1}=0.7^{0.2}0.9^{0.2}0.9^{0.5}0.8^{0.1}=0.845\,9$;$T_{C_2}=0.7^{0.1}0.8^{0.2}0.7^{0.6}0.6^{0.1}=0.707\,9$;

$T_{C_3}=0.8^{0.2}0.7^{0.1}0.9^{0.6}0.7^{0.1}=0.836\,0$;$T_{C_4}=0.9^{0.3}0.7^{0.1}0.9^{0.5}0.8^{0.1}=0.867\,4$;

$T_{C_5}=0.8^{0.2}0.6^{0.2}0.8^{0.5}0.7^{0.1}=0.745\,3$;$T_{C_6}=0.65^{0.1}0.6^{0.1}0.95^{0.6}0.6^{0.2}=0.796\,8$;

$T_{C_7}=0.7^{0.1}0.5^{0.1}0.8^{0.7}0.7^{0.1}=0.743\,2$；$T_{C_8}=0.8^{0.2}0.5^{0.1}0.8^{0.6}0.65^{0.1}=0.747\,6$；

$T_{C_9}=0.9^{0.3}0.8^{0.25}0.8^{0.3}0.7^{0.15}=0.812\,3$；$T_{C_{10}}=0.95^{0.3}0.85^{0.2}0.9^{0.3}0.8^{0.2}=0.883\,3$.

将整个订餐系统分为以下几个子系统：组件C_1组成子系统T_{S_1}；组件C_2~C_5组成子系统T_{S_2}，其中，组件C_2在该子系统中所占的权重为0.2，组件C_3在该子系统中所占的权重为0.3，组件C_4在该子系统中所占的权重为0.2，组件C_5在该子系统中所占的权重为0.3；组件C_6~C_9组成子系统T_{S_3}，假设循环3次，其中，组件C_6在该子系统中所占的权重为0.2，组件C_7在该子系统中所占的权重为0.3，组件C_8在该子系统中所占的权重为0.3，组件C_9在该子系统中所占的权重为0.2；组件C_{10}组成子系统T_{S_4}. 根据式(2)~(6)，计算可得：

$$T_{S_1}=T_{C_1}=0.845\,9;\ T_{S_2}=T_B=\frac{T_{C_2}^{0.2}+T_{C_3}^{0.3}+T_{C_4}^{0.2}+T_{C_5}^{0.3}}{4}=0.942\,1;$$

$$T_{S_3}=T_A^t=T_P^t=\left[1-\prod_{i=1}^{n}\left(1-T_{C_i}^{\delta_i}\right)\right]^t=\left[1-\left(1-T_{C_6}^{\delta_6}\right)\left(1-T_{C_7}^{\delta_7}\right)\left(1-T_{C_8}^{\delta_8}\right)\left(1-T_{C_9}^{\delta_9}\right)\right]^t=0.999\,8;$$

$$T_{S_4}=T_{C_{10}}=0.883\,3;$$

那么，整个订餐系统的可信性为：$T_{WS}=\frac{T_{S_1}+T_{S_2}+T_{S_3}+T_{S_4}}{4}=0.917\,8$.

4 结语

软件在现代社会应用广泛，软件是否可信成为人们关注的重点. 为提高软件质量与复用率，越来越多的软件开发人员利用组件的思想设计软件，所以，对软件可信性的研究归根结底可看作是对组件的可信性研究. 组件可信性的度量对整个软件系统可信性的度量有很重要的影响，从组件的角度研究软件可信性有着重要的意义. 本文从组件的角度出发，分析软件的可信属性以及组件的几种常见组合模式，分别从顺序、分支、并行、循环这4种组合模式上建立相应的可信度量模型，并通过理论验证这些度量模型满足单调性、非负性、凝聚性、敏感性、替代性等代数性质. 在求得简单子系统可信性的基础上，计算出整个系统的可信性，为从组件的角度研究软件的可信性提出一个新的方向.

在今后的工作中，将通过更多的实践去验证所建立的模型，并且不断将其完善和补充. 接下来将研究关键组件与非关键组件对软件可信性的影响.

参考文献：

[1] 郎波，刘旭东，王怀民，等. 一种软件可信分级模型[J]. 计算机科学与探索，2010，4(3)：231-239.

[2] 刘克，单志广，王戟，等. “可信软件基础研究”重大研究计划综述[J]. 中国科学基金，2008，22(3)：145-151.

[3] 陶红伟. 基于属性的软件可信性度量模型研究[D]. 上海：华东师范大学，2011.

[4] ALGIRDAS A，LAPRIE J C，BRIAN R，et al.Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Trans Dependable Secure，2004，1(1)：11-33.

[5] 丁滟，王怀民，史佩昌，等. 可信云服务[J]. 计算机学报，2015，38(1)：133-149.

[6] 汤永新，刘增良. 软件可信性度量模型研究进展[J]. 计算机工程与应用，2010，46(27)：12-16.

[7] 张俊. 基于多维分层属性的软件可信性度量模型的研究与工具实现[D]. 上海：华东师范大学，2016.

[8] 白川，张璇，王旭，等. 可信软件非功能需求可满足性经济学方法分析[J]. 计算机工程与应用，2017，53(22)：249-257.

[9] 郑晓东. 基于Petri网的组件化软件系统可靠性研究[D]. 苏州：苏州大学，2008.

[10] ELSHAAFI H，BOTVICH D.Trustworthiness Inference of multi-tenant component services in service compositions[C]// Proc Ftra International Conference on Computer Science and ITS Applications，2012(203)：301-312.

[11] ELSHAAFI H，MCGIBNEY J，BOTVICH D.Aggregation and optimisation of trustworthiness of composite services[M]. Secure and Trustworthy Service Composition.Springer International Publishing，2014：150-172.

[12] 韩强，袁玉宇. 构件化业务流程重组应用服务器可信性度量方法研究[J]. 通信学报，2014(3)：47-57.

[13] 梅琳. 基于组件的软件可信性评价模型研究[D]. 南京:南京大学,2003.
[14] ISO/IEC 15408-1-2005.Information technology-security techniques-evaluation criteria for IT security,part 1:Introduction and general model[S]. 2005.
[15] Trusted Computing Group.TCG architecture overview specification revision 1.2,28 April 2004.
[16] SCHNEIDER F.B.Trust in cyberspace[M]. National Academy Press,1998.
[17] HASSELBRING W,REUSSNER R.Toward trustworthy software systems[J]. Computer,2006,39(4):91-92.
[18] BECKER S,HASSELBRING W,PAUL A,et al.Trustworthy software systems:a discussion of basic concepts and terminology[J]. Acm Sigsoft Software Engineering Notes,2006,31(6):1-18.
[19] 陆文,徐锋,吕建. 一种开放环境下的软件可靠性评估方法[J]. 计算机学报,2010,33(3):452-462.

The Trustworthiness Measure Model for Componented-based Software System

HUANG Dujuan[1],MA Yanfang[1],PAN Haiyu[2]
(1.*School of Computer Science and Technology,Huaibei Normal University,235000,Huaibei,Anhui,China*;
2.*School of Computer and Information Security,Guilin University of Electronic Technology,541004,Guilin,Guangxi,China*)

Abstract: Software trustworthiness is an important factor to ensure software quality.The component design method has great influence on software trustworthiness and software quality.In this paper,based on the attributes of the components,and combining the weight and different combination modes of components,the software system trustworthiness measurement models were established.First,according to the various attributes of the component,the trustworthiness of a single component was computed.Then,combining the weight of component and various combinations of components,the trustworthiness measurement models of the system were proposed.It is proved that these models meet the algebraic properties of monotonicity,non-negativity,acceleration,sensitivity,and substitution,which are more conducive to the developers and users to analyze and measure the trustworthiness of the software.Finally,some cases are listed to verify the reasonability of trustworthiness measurement model.

Key words: software trustworthiness; component; weight; trustworthiness measurement model