基于客观赋权法的嵌入式软件可信性评估方法研究*

谷海红，李苗在
（鹤壁职业技术学院 电子信息工程系，河南 鹤壁 458030）

摘　要：以基于证据推理方法的嵌入式软件可信性评估理论为基础，分析需求驱动的嵌入式软件可信性评估过程，并针对评估过程中存在的可信指标间相对权重难量化问题，提出一种基于可信证据熵的客观权重计算方法，用以改进传统方法中常用的主观判断方式。算例分析验证了该方法的合理性和有效性。

关键词：嵌入式软件；可信性；客观赋权；证据推理
中图分类号：TP311　　**文献标志码**：A　　**文章编号**：1001-3695(2012)05-1761-03
doi:10.3969/j.issn.1001-3695.2012.05.042

Objective weighting approach based embedded software trustworthiness evaluation method

GU Hai-hong, LI Miao-zai
(*Dept. of Electronic Engineering, Hebi College of Vocation & Technology, Hebi Henan* 458030, *China*)

Abstract: To discuss and explain the basic scientific problems in embedded software trustworthiness evaluation, the paper proposed a novel requirement-driven process model of software trustworthiness evaluation. Also, this paper set up a calculation method for indexing relative weight by trustworthy evidence entropy, which overcame the shortage of traditional method, in which the weight was set up by subjective manners. The experimental results show that the validity and rationality of the proposed model and it is suitable to embedded software.

Key words: embedded software; trustworthiness; objective weighting; evidential reasoning

纵观嵌入式软件的发展历史，由于软件系统失效或故障引起的重大安全事故屡见不鲜。1996 年 6 月，欧洲阿丽亚娜 5 型火箭因内部惯性参考系统软件的数据转换异常，导致其在发射 40 s 后爆炸；2003 年 8 月，因为控制系统软件问题导致美国和加拿大出现历史上最大规模的停电事故；2004 年 12 月，美国某空军实验基地的一架 F-22 战斗机，因软件发生故障在起飞过程中失控坠毁，进而导致该型战斗机的延迟交付。嵌入式软件的可信性问题已经成为人们关注的焦点。

与传统的软件质量度量技术不同，嵌入式软件的可信性评估问题既要反映出软件实体自身的客观实际，又要体现出用户对软件可信任程度的主观认识。可信性评估模型可以提供描述、量化及综合多种软件质量度量的功能，可以实现对复杂嵌入式软件系统可信性评估推理过程的一致性建模。Anne 等人[1]分析了开源构件部署时存在的构件质量难认证问题，有针对性地给出了开源构件的可信性评估和测试模型。Shi 等人[2]运用模糊理论建立了软件可信性评估模型，实现了对评估过程的不确定性建模。由于在不确定性度量方面具有较高的灵活性和更清晰的融合推理机制，且可以将精确数据与主观评价在统一识别框架下进行相容合成，证据推理（evidential reasoning, ER）方法也已经被应用于处理复杂的嵌入式软件可信性评估问题[3]。

可信指标间相对权重的合理估算对软件可信性评估模型的精确性具有直接影响。但在已有的可信性评估模型中，可信指标间相对权重的确定主要是采用专家群体决策的方式进行主观估计，专家评价的随意性和盲目性将会直接影响 ER 方法在嵌入式软件可信性评估过程中的实际应用效果。此外，可信性评估过程需要对多源可信证据进行多次合成，而每一次可信证据的合成皆需专家参与以确定相对权重，这也就限制了可信性评估模型的自适应求解能力。为此，本文以熵权法[4]和证据推理方法为理论基础，通过分析嵌入式软件的可信性评估过程提出一种新颖的客观赋权方法，利用可信证据熵和区分度综合度量隐藏在可信证据体内的客观信息。

1　嵌入式软件可信性评估过程

开放动态环境下，需求驱动的嵌入式软件可信性评估过程设计是可信性模型构建和失信因素分析的基础。而不同的嵌入式软件可能具有不同的可信需求，也即要求决策者建立满足不同应用需求的可信性评估指标系统，以实现对不同应用背景下嵌入式软件可信性的准确刻画。为此，从软件行为可信的角度，以基于 ER 理论的嵌入式软件可信性评估方法[3]为基础，给出如图 1 所示的嵌入式软件可信性评估过程抽象。

从图 1 不难看出，可信证据间权重的计算是保证评估结果准确性的关键。而传统的权重确定方法，通常是采取群决策的模式对专家给出的主观判断进行集结。人为因素的过分依赖将会造成权重的计算不够客观、准确，需要研究更为客观的可信指标赋权方法。

2　可信证据熵

在基于 ER 方法的嵌入式软件可信性评估过程中，通过定

收稿日期：2011-10-26；**修回日期**：2011-11-28　　**基金项目**：国家自然科学基金资助项目(90728140)

作者简介：谷海红(1975-)，男，副教授，主要研究方向为可信软件、云计算(dingshuai.hfut@gmail.com)；李苗在(1976-)，女，河南鹤壁人，讲师，硕士，主要研究方向为可信软件、软件工程.

量度量、主观评价、代码分析与测试等方式获得的原始评估数据都可以被统一转换为基本信度分配函数(basic probability assignment,BPA),又称做可信证据[5]。

定义 1 令 $\Omega=\{H_1,\cdots,H_N\}$ 是统一识别框架,$H_n(n=1,\cdots,N)$ 是一组完备的评价等级,β_n、β_Ω 分别是分配到单基焦元 H_n 和 Ω 上的信度,可信证据 m 被定义为 $m=\{(H_n,\beta_n),(\Omega,\beta_\Omega)\quad n=1,\cdots,N\}$,其中,$\beta_n\geqslant 0$ 且 $\beta_\Omega+\sum_n\beta_n=1$。

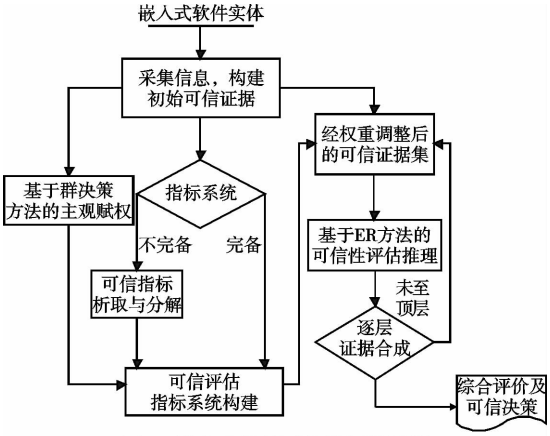

图1 嵌入式软件可信性评估过程

基于效用的定量或定性数据统一转换技术参见文献[5]。受篇幅限制,这里简要介绍定量数据到可信证据的转换过程。

例如,令 M 为待评嵌入式软件,$\Omega_M=\{H_1,\cdots,H_5\}$ 是统一识别框架,平均失效时间是 M 的一个定量评估指标,$v(H)=\{12\text{ h},72\text{ h},144\text{ h},296\text{ h},530\text{ h}\}$ 是由评估专家对该指标给出的效用等级函数,采取软件模型预测的方式,获得 M 在平均失效时间上的评估信息 $v_{\text{mttf}}=325$ h,则对应的可信证据 $m_{\text{mttf}}=\{(H_n,\beta_n),(\Omega,\beta_\Omega),n=1,\cdots,5\}$ 计算为

$$\beta_1=\beta_2=\beta_3=\beta_\Omega=0$$
$$\beta_4=(530-325)/(530-296)=0.8761$$
$$\beta_5=(325-296)/(530-296)=0.1239$$

即 $m_{\text{mttf}}=\{(H_4,0.8761),(H_5,0.1239)\}$。

在信息科学领域,熵被用做是信息的度量,表示平均信息量。如果熵最大,表明信源的不确定性最大,被传送的信号寄载的信息自然就最少。因此,给出可信证据信息熵(简称可信证据熵)的概念,用以度量可信证据的全局不确定性或隐含信息量。

定义 2 令 $m=\{(H_n,\beta_n),(\Omega,\beta_\Omega),n=1,\cdots,N\}$ 是统一识别框架 Ω 上的可信证据,则 m 的可信证据熵定义为

$$H(m)=-\beta_\Omega\log\beta_\Omega-\sum_{\beta_n\neq 0}\beta_n\log\beta_n \tag{1}$$

可信证据熵越大,表示该可信证据所呈现出的不确定性越大,其隐含的信息量就越少。例如,$m_1=\{(H_4,0.62),(H_5,0.26),(\Omega,0.12)\}$ 和 $m_2=\{(H_3,0.11),(H_4,0.46),(H_5,0.3),(\Omega,0.13)\}$ 是 Ω 下的两条可信证据,则可信证据熵 $H(m_1)=0.3913<H(m_2)=0.5326$,表明可信证据 m_1 比 m_2 的平均不确定性要大,即所包含的信息更多。虽然此时还无法量化在证据合成过程中二者的相对重要性程度,但由熵的定义易知,对合成的结果而言,m_1 将会比 m_2 贡献更大。

3 基于可信证据熵的客观赋权方法

与基于群决策的主观赋权方法不同,客观赋权方法更关注于从证据体内挖掘隐藏的信息,采取定量度量的方式发现不同证据间存在的客观差异,有利于克服决策专家的主观随意性。

嵌入式软件可信性评价的期望是相对权重可以唯一反映出可信证据的重要性程度,而可信证据熵函数在某些条件下并不满足单调性条件,也即意味着在定义域内可能存在非唯一解,这将会给决策者作出唯一判断造成障碍。依据可信证据中信度分配结构的不同,给出如下定理及其证明。

定理 1 若可信证据 m 中存在 $\beta_n=\beta_\Omega$ 且 $\beta_\Omega\neq 0$ 时,$H(m)$ 是非单调函数。

证明 设 $H(m)$ 是 m 的可信证据熵,且 $\beta_\Omega\neq 0$,则 $H(m)=-\beta_\Omega\log\beta_\Omega-\sum_{\beta_n\neq 0}\beta_n\log\beta_n$。令 $y=H(m)$,$x_i=\beta_n$,$1-\sum x_i=\beta_\Omega$ 得

$$y=-\sum x_i\log x_i-(1-\sum x_i)\log(1-\sum x_i) \tag{2}$$

由定义 1 及假设条件可知,$x_i\in[0,1)$,$1-\sum x_i\in(0,1]$。对 x_i 求偏导得

$$\frac{\partial y}{\partial x_i}=-\log x_i-1-\frac{\partial((1-\sum x_i)\log(1-\sum x_i))}{\partial x_i}=$$
$$-\log x_i-1+\log(1-\sum x_i)+1=$$
$$-\log\frac{x_i}{(1-\sum x_i)}$$

⇒当且仅当 $x_i=(1-\sum x_i)$ 时,$\partial y/\partial x_i=0$。

⇒式(2)所示函数为非单调函数⇔$\exists x_i$ 使 $x_i=(1-\sum x_i)$。

⇒若可信证据 m 中存在 $\beta_n=\beta_\Omega$ 且 $\beta_\Omega\neq 0$ 时,$H(m)$ 是非单调函数。证毕。

定理 2 若可信证据 m 中存在 $\beta_n=\mathrm{e}^{-1}$ 且 $\beta_\Omega=0$ 时,$H(m)$ 是非单调函数。

证明 设 $H(m)$ 是 m 上的可信证据熵,且 $\beta_\Omega=0$,则 $H(m)=-\sum_{\beta_n\neq 0}\beta_n\log\beta_n$。令 $y=H(m)$,$z_j=\beta_n$,得到

$$y=-\sum z_j\log z_j \tag{3}$$

由定义 1 及假设条件可知,$z_i\in[0,1]$。对 z_j 求偏导得

$$\frac{\partial y}{\partial z_j}=-\log z_j-1$$

⇒当且仅当 $z_j=\mathrm{e}^{-1}$ 时,$\partial y/\partial x_i=0$。

⇒式(3)所示函数为非单调函数⇔$\exists z_j$ 使得 $z_j=\mathrm{e}^{-1}$。

⇒若可信证据 m 中存在 $\beta_n=\mathrm{e}^{-1}$ 且 $\beta_\Omega=0$ 时,$H(m)$ 是非单调函数。证毕。

由上述两个定理易知,可信证据熵函数在某些条件下并不满足单调性,也就无法保证解的唯一性。因此,下面将给出区分度的概念对这一局限进行修正。

定义 3 令 $m=\{(H_n,\beta_n),(\Omega,\beta_\Omega),n=1,\cdots,N\}$ 是统一识别框架 Ω 上的可信证据,则 m 相对于其他可信证据的区分度定义为

$$Q(m)=\begin{cases}1-\dfrac{H(m)}{\log(n+2)} & \beta_n\leqslant\sigma\\ 0 & \beta_n>\sigma\end{cases} \tag{4}$$

其中:n 是可信证据 m 包含焦元的个数;σ 是容忍阈值,用于限定可信证据允许的最高未知程度,通常设为 0.5。若 β_n 高于该阈值,直接判定区分度为 0。在此基础上,对可信证据的区分度进行归一化处理,给出定义 4。

定义 4 设待评可信指标 e 上的可信证据集为 $\{m_i,i=1,\cdots,I\}$,可信证据 m_i 的区分度为 $Q(m_i)$,则合成过程中 m_i 的相对权重为

$$w_i=\frac{Q(m_i)}{\sum_{i=0}^{I}Q(m_i)} \tag{5}$$

显然有 $w_i\in[0,1]$,$\sum_{i=0}^{I}w_i=1$。

结合定义 3,若可信证据所包含的未知程度大于容忍阈值,即 $\beta_n>\sigma$,则可认定其客观权重为 0,这样就可以有效减少可信性评估系统的风险,提供系统抵御高不确定性风险带来的威胁。

在合成多源可信证据时,可信指标间客观权重是通过估算隐藏在证据体内的信息量而直接得到,不需要主观拟定。与传

统的方法相比,基于可信证据熵的权重计算改进了过去常用的主观判断方法,也可改善由于专家多次参与而导致的模型自适应性不强的问题。

4　案例分析

在前面的研究工作中,通过案例分析阐明了 ER 方法在解决嵌入式软件可信性评估问题时的计算过程[3]。为了验证所提出客观赋权方法的有效性,本文将继续以某自主研发的嵌入式软件系统为案例研究对象。该嵌入式软件是一种服务于金属模具铸造现场的质量控制软件,主要包括 RFID 读写控制、金属成分分析、模具质量管理、铸造智能决策等核心模块,可以实时采集工业现场数据、分析并预警可能发生的铸造事故,亦可通过人工干预或预定自修正方案的方式及时调整模具铸造计划,实现对金属模具铸造过程的全周期质量监管。

通过调查走访,建立如图 2 所示的可信性评估指标系统。

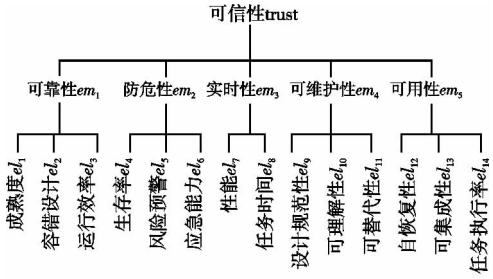

图2　可信性评估指标系统

设 $\Omega=\{H_1,\cdots,H_5\}$ 为统一识别框架,$U(H)=\{0,\ 0.25,\ 0.5,\ 0.75,\ 1\}$ 为决策专家给出的效用函数,经效用转换后的初始可信证据如图 3 所示。其中,$el_1 \sim el_{14}$ 为待评嵌入式软件的 14 个底层可信指标,β_3、β_4 和 β_5 为初始可信证据中底层可信指标在 Ω 上的信度分配。

以底层可信指标 el_9(设计规范性)为例,简要说明该嵌入式软件可信证据的获取过程。el_9 是一个定性评估指标,需要以专家主观决策的方式给出,规定的评价等级为 $\{A_1,\ A_2,\ A_3,\ A_4\}$,各等级效用为 $\{0,\ 0.33,\ 0.67,\ 1\}$。通过分析相关的需求分析文档、概要设计与详细设计文档、用户使用手册等,评估专家给出了该软件在 el_9 上的评价 $\{(A_3,\ 0.46),\ (A_4,\ 0.35)\}$。

运用文献[5]中提出的基于效用的定性数据转换技术,计算该软件在 el_9 上的可信证据 $m=\{(H_n,\beta_n),\ (\Omega,\ \beta_\Omega),\ n=1,\cdots,5\}$。其中:

$$\beta_1=\beta_2=0$$

$$\beta_3=0.46\times(0.75-0.67)/(0.75-0.5)=0.1472$$

$$\beta_4=0.46\times(0.67-0.5)/(0.75-0.5)=0.3128$$

$$\beta_5=0.35;\ \beta_\Omega=1-\beta_1-\beta_2-\beta_3-\beta_4-\beta_5=0.19$$

运用式(1)和(4)分别求解底层可信指标上可信证据熵 $H(m)$ 和区分度 $Q(m)$,如图 4 所示。对区分度进行归一化处理,计算出 $el_1 \sim el_{14}$ 上的客观权重 w_2,如图 5 所示。与文献[3]中基于群决策方法获得的主观权重 w_1 相比,客观赋权方法侧重于以可信证据体内隐含的信息量估计其在合成时的相对重要程度。

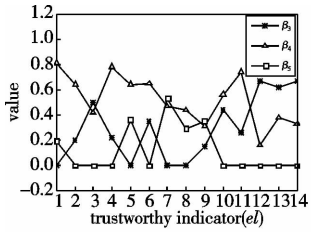

图3　初始可信证据

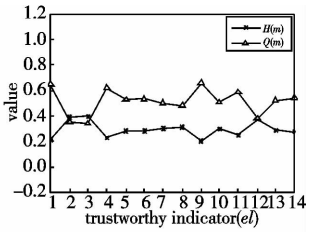

图4　可信证据熵和区分度

结合客观权重 w_2,使用 ER 算法对底层指标上可信证据进行一次合成,求得待评嵌入式软件在 $em_1 \sim em_5$ 上的可信证据;在此基础上,使用同样的方法估算 $em_1 \sim em_5$ 上的客观权重,并进行二次合成,获得软件的综合可信性评价;最后,使用式(6)的效用估算模型:

$$u(m)=\sum\nolimits_n \beta_n u(H_n)+\beta_\Omega u(\Omega)=\sum\nolimits_n \beta_n u(H_n)+\sum\nolimits_{\beta_n\neq 0}\frac{\beta_\Omega u(H_n)}{|m|} \tag{6}$$

对综合可信性评价及 $em_1 \sim em_5$ 上的可信证据进行量化,求得确定性综合评价结果 $u_2(m)$(图 6),其中综合可信性评估值为 $u_2(\text{trust})=0.7014$。

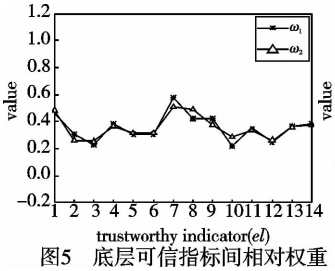

图5　底层可信指标间相对权重

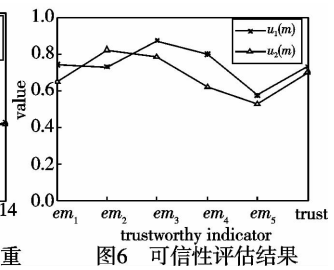

图6　可信性评估结果

相同实验条件下,采用基于主观赋权的 ER 方法进行可信性评估的仿真计算,对比实验结果如图 6 中的 $u_1(m)$。与 $u_1(m)$ 相比,基于可信证据熵的客观赋权方法的合理应用,保证了嵌入式软件可信性评估结果的准确性与客观性。

5　结束语

本文方法的提出有利于消除主观人为因素对可信指标权重及可信性评估推理过程的影响,对于增强可信性评估模型的自适应性也具有一定实际意义。在我国,于 2008 年启动的《可信软件基础研究》重大研究计划中,软件可信性的度量、建模与预测是一个核心科学问题,需要重点研究面向复杂软件,特别是嵌入式软件的多维可信属性的多尺度量化指标系统、度量和评估机制及软件在环境和自身演化下可信性的演化规律[6]。下一步笔者将结合已有的研究成果,重点研究软件演化或需求变更背景下的嵌入式软件可信性评估问题。

参考文献:

[1] ANNE I, MARKO P. Trustworthiness evaluation and testing of open source components[C] //Proc of the 7th International Conference on Quality Software. 2007:316-321.

[2] SHI Hui-ling, MA Jun, ZOU Feng-yi. Software dependability evaluation model based on fuzzy theory[C] //Proc of International Conference on Computer Science and Information Technology. 2008: 102-106.

[3] 李苗在. 基于证据推理的嵌入式软件可信性评估方法[J]. 计算机应用研究,2011,28(12):4604-4606.

[4] WANG T C, LEE H D. Developing a fuzzy TOPSIS approach based on subjective weights and objective weights[J]. Expert Systems with Applications,2010,37(2):1805-1807.

[5] YANG J B, WANG Y M, XU D L, *et al*. The evidential reasoning approach for MADA under both probabilistic and fuzzy uncertainties [J]. European Journal of Operational Research,2006,171(1): 309-343.

[6] 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.