文章编号:1003 - 207(2009)06 - 0163 - 07

考虑信息源相关的软件可信性评估模型

杨善林,丁 帅,付 超

(合肥工业大学计算机网络系统研究所,安徽 合肥 230009)

摘 要:本文研究了信息源相关背景下的软件可信性评估问题。首先提出了一种改进的 Denoeux 谨慎连接规则,给出了面向多证据合并的水平合成算法;其次,定义了一个综合折扣和相对权重的联合系数用于指标集结或群体意见集结;最后,在分析评估过程中客观存在的信息不确定性和信息源相关等问题的基础上,给出了一个基于证据理论的软件可信性评估模型。典型算例验证了该模型的合理性和有效性。

关键词:软件可信性;信息源相关;证据理论;评估模型

中图分类号:TP311 **文献标识码**:A

1 引言

随着软件规模和设计复杂性的急剧增长,软件系统的高可信要求给我们提出了新的更高的挑战[1]。为了对软件生产实施高效的可信控制,必须先对软件实体的可信状态进行客观的判断,因此软件可信性评估技术已经成为当前可信软件研究领域中的一个核心科学问题。

在软件范畴中,可信性的定义有很多,尚未得到统一[2],而不同的定义可能会导致可信性评估方法的不同,所以在研究评估方法之前,需要深刻把握软件可信性的内在本质,给出一个合理规范的定义。软件可信性是一个用来反映软件实体多维质量特征的综合属性,是在传统可靠性、防危性、可用性和可维护性等软件非功能性属性的基础上提出的[3]。由此,我们认为可信性是一个基于合理的证据或经验对软件实体的所有非功能性属性(又可称为可信属性)是否遵从预定规则集的综合评价体系。

目前,已有学者在软件可信性评估研究方面进行了一些尝试性的工作。文献[4]提出了一种面向嵌入式构件软件的可信性模型,讨论了质量剖面子模型和可信性剖面子模型的内部结构和运行模式,定义了一个可信性评估函数 TEF,用三元组〈compliance, benignity, stability〉较为全面的展现了软件的可信性状况。文献[5]提出了一种基于 Markov 模型的软件可信性评估方法,通过对 risk、safety、reliability 三个相关因素的预测与分析,分别建立了静态和动态两个模型。文献[6]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。遗憾的是,上述模型都存在对评估信息源的相关性及可靠性考虑不足的问题,未能从根本上保证模型推理的合理性,且由于这些模型所考察的可信属性较少,导致模型本身普适性较差,只适用于特定的情境中。

与硬件可信性相比,软件可信性评估技术还很落后,众多国内外知名研究机构都将软件可信性评估技术作为可信软件领域未来几年的研究重点。正在执行的 TrustSoft 计划以构件技术为基础,通过验证软件的多个质量属性来全面研究软件可信性预测与评估机制[3]。在我国,于 2008 年启动的《可信软件基础研究》重大研究计划中,复杂软件,特别是网络和嵌入式软件的多维可信属性的多尺度量化指标系统、度量和评估机制及测评体系是一个核心科学问题[7]。

受限于专家的有限理性与软件预测模型的非完全可靠,软件可信性评估存在难以避免的不确定性。运用证据理论开展软件可信性评估问题的建模与求解,将有效解决评估推理过程中存在的信息不确定性问题。在传统的证据理论中,Dempster 合成规则和非规范化的 TBM(Transferable Belief Model,可传递信度模型)连接规则长期扮演着核心角色。使用这些方法进行证据合并时,都要求待合并元素满

收稿日期:2008 - 12 - 22;**修订日期**:2009 - 09 - 08

基金项目:国家自然科学基金资助项目(70631003, 90718037);教育部博士点基金(200803590007);合肥工业大学校发展基金(081104F)

作者简介:杨善林(1948 -),男(汉族),安徽怀宁人,合肥工业大学计算机网络系统研究所教授,博导,研究方向:决策科学与技术、可信软件.

足证据独立性条件,即要求形成证据的信息源之间不能有交叉。而文献[8]以案例分析的方式阐述了可信属性间客观存在的两种基本关联类型:内在联系(Intrinsic relationships)和外在联系(Extrinsic relationships)。Denoux 在文献[9]中也指出:若两位专家共享若干知识或经验背景,则他们的决策将不满足独立性要求。因此,在复杂的软件可信性评估过程中,信息源相关是一个需要考虑的关键因素。

针对以上问题,本文研究建立一种考虑信息源相关的软件可信性评估模型,以证据理论进行不确定型软件可信性评估模型的构建与求解,以改进的 Denoux 谨慎连接规则解决评估信息源相关背景下的信息融合问题,最后通过一个算例验证了模型的合理性和有效性。对比软件可信性评估的已有工作,本文构建的模型从根本上保证了模型推理的合理性,具有较好的普适性。

2 考虑信息源相关的软件可信性评估模型

软件可信性评估的目的在于对软件实体的可信状态有较为全面的主观认知,并结合评估结果找出导致软件失信的因素,最终给出改进方案。基础数据的可靠性与评估模型的合理性是确保软件可信性评估正确性的关键。而传统的软件可信性评估模型都未曾考虑信息源的相关性[4-6],特别是可信属性之间的交互关系及可能产生的涌现特征,包括多属性/单属性的局部/全局相容与匹配等。日趋复杂的软件可信性评估需求将进一步限制这些模型的精确度。为此,我们提出了一个考虑信息源相关的软件可信性评估模型,其整体框架如图 1 所示。

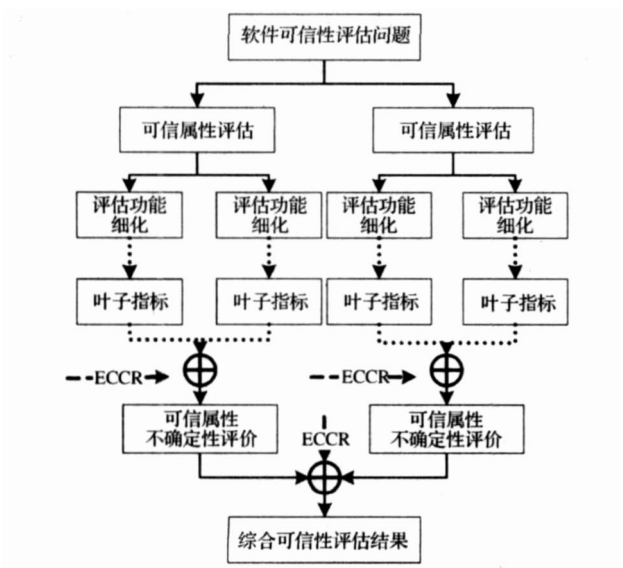

图 1 软件可信性评估推理模型

在获得经联合系数调整的初始证据后,结合指标系统的复杂层次性,逐级开展证据合成,并将指标上的不确定性评价反馈给用户,直至得到顶层指标 e_r 上的信度分配为止,最后结合效用量化所有指标评价。

模型的实现逻辑是采用分布式评估框架的思想,将复杂的评估问题进行逐层划分,形成一组规模较小可直接操作的软件度量问题,再利用一种改进的谨慎连接规则(extended cautious conjunctive rule, ECCR)逐层向上推理,最终定量的给出待评软件实体的可信性评估结果。模型中的核心部件将在下文中逐一讨论。

3 改进的 Denoeux 谨慎连接规则

3.1 基本概念[9-12]

为了便于阐述 ECCR 的证据合成机理,有必要简要介绍谨慎连接规则的相关基础。

定义 1 设 Ω 为识别框架,S 为 Ω 上的证据源,则 S 的 BBA(basic belief assignment,基本信度分配)定义为函数 $m:2^{\Omega}\to[0,1]$,满足 $\sum_{A\subseteq\Omega}m(A)=1$。

BBA 不要求 $m(\varnothing)=0$,区别于 BPA(basic probability assignment)。

定义 2 若子集 $A\subseteq\Omega$,且有 $m(A)>0$,则称 A 为 m 的焦元(Focal Element)。

依据焦元类型的不同,m 可以将称为:

正规 BBA。若 $\varnothing$ 不是一个焦元;

亚正规 BBA。若 $\varnothing$ 是一个焦元;

教条 BBA。若 Ω 不是一个焦元;

简单 BBA。若焦元不超过 2 个,且当焦元数为 2 时,Ω 必定是其中的一个焦元;

绝对 BBA。若只包含一个焦元;

贝叶斯 BBA。若焦元 A 都是单基焦元。

定义 3 设 m 为识别框架 Ω 上的 BBA,$\forall_{A\subseteq\Omega}q(A)=\sum_{B\subseteq\Omega_A}m(B)$ 称为公共函数(commonality function)。

基于 Shafer 原著[11]中非教条 BBA 的标准分解定义。对于一个可分解的非教条 BBA m,可将其定义为若干简单 BBA 的标准组合,即:

$$m=\oplus_{\varnothing\neq A\subset\Omega}A^{w(A)},$$

其中,$\forall A\subset\Omega, A\neq\varnothing, w(A)\in[0,1]$,称为权重函数(与相对权重无关),$\oplus$ 表示 Dempster 合成算子。

扩展上述分解,Denoeux 认为一个亚正规 BBA 可非标准分解为:

$$m = \bigoplus_{A\subset\Omega} A^{w(A)},$$

其中, $\forall A \subset \Omega, w(A) \in [0,1]$。

以上分解限定 $w(A) \in [0,1]$。文[11]中, Smets 将权重函数扩展到[0, + ∞],将满足 $w(A) > 1$ 的简单 BBA 称为逆(inverse)简单 BBA,从而实现任意非教条 BBA 的分解。扩展后的 $w(A)$ 定义为:

$$w(A) = \prod_{B\supseteq A} q(B)^{(-1)^{|B|-|A|+1}} = \begin{cases} \dfrac{\prod_{B\supseteq A, |B|\notin 2\mathbb{N}} q(B)}{\prod_{B\supseteq A, |B|\in 2\mathbb{N}} q(B)}, & |A| \in 2\mathbb{N}, \\ \dfrac{\prod_{B\supseteq A, |B|\in 2\mathbb{N}} q(B)}{\prod_{B\supseteq A, |B|\notin 2\mathbb{N}} q(B)}, & |A| \notin 2\mathbb{N}, \end{cases}$$

其中, $2N$ 表示偶自然数集, $|A|$ 为焦元 A 的基数。

对于软件可信性评估问题而言,经一致性转换后得到的评估基本信息皆为贝叶斯 BBA,权重函数 $w(A)$ 的求解过程即可简化为:

$$w(A) = \begin{cases} \dfrac{m(\Omega)}{m(h_p) + m(\Omega)}, & A = h_p \\ m(\Omega)\prod_{p=1}^{P}\left(1 + \dfrac{m(h_p)}{m(\Omega)}\right), & A = \varnothing \\ 1, & otherwise。 \end{cases} \quad (1)$$

基于权重函数,遵循最小许诺原理(Least Commitment Principle,LCP),Denoeux 给出相关信念合成规则。

定义 4　令 m_1 和 m_2 为两个信息源非独立的 BBA, $w_{1\wedge 2}(A) = \min(w_1(A), w_2(A))$ 为联合权重函数,Denoux 谨慎连接规则(Cautious Conjunctive Rule)定义为:

$$m_{1\wedge 2} = m_1 \wedge m_2 = \bigoplus_{\varnothing\neq A\subset\Omega} A^{w_{1\wedge 2}(A)},$$

其中,算子 ∧满足可交互性、可连接性和幂等性。

3.2　ECCR

谨慎连接规则较好地解决了信息源非独立情况下的证据合成问题,但规则中未能区别考虑由"相对权重或折扣"与"信息不完整"引起的无知,也就无法将非原始信息中的无知剔除,导致合并结果的不合理。为此,我们有必要对谨慎连接规则中的无知进行分化处理,并给出一个改进的合成规则。

定理 2.1　设 $\Omega = \{h_p, p = 1, \cdots, P\}$, m 为 Ω 上的 BBA, $m(\Omega)$ 和 $m(\tilde{\Omega})$ 分别表示由"相对权重或折扣"和"信息不完整"引起的无知, Ω 上的权重函数为

$$w(\bar{\Omega}) = \frac{m(\tilde{\Omega})}{m(\bar{\Omega}) + m(\tilde{\Omega})}。$$

证明 $m(\Omega) = m(\bar{\Omega}) + m(\tilde{\Omega})$。则有

$$q(A) = \begin{cases} m(\bar{\Omega}), & A = \Omega \\ m(\tilde{\Omega}), & A = \tilde{\Omega} \end{cases}$$

所以, m 可表示为如下 q 的函数:

$$m(\Omega) = q(\Omega) = q(\bar{\Omega}) + q(\tilde{\Omega}),$$
$$m(\tilde{\Omega}) = q(\tilde{\Omega}),$$
$$m(\bar{\Omega}) = q(\Omega) - q(\tilde{\Omega}).$$

对上式,使用 $\ln w$ 替代 m, $-\ln q$ 替代 q,

$$\ln w(\bar{\Omega}) = -\ln q(\Omega) + \ln q(\tilde{\Omega}),$$
$$= \ln\frac{q(\tilde{\Omega})}{q(\Omega)} = \ln\frac{m(\tilde{\Omega})}{m(\bar{\Omega}) + m(\tilde{\Omega})},$$

整理得: $w(\bar{\Omega}) = \dfrac{m(\tilde{\Omega})}{m(\bar{\Omega}) + m(\tilde{\Omega})}$。证毕。

定义 5　令 m_1 和 m_2 为两个信息源非独立的 BBA,联合权重函数 $w_{1\wedge^* 2}(A) = \min(w_1(A), w_2(A))$ 为

$$w_{1\wedge^* 2}(A) = \begin{cases} \min(w_1(h_p), w_2(h_p)), & A = h_p, p = 1, \cdots, P \\ \min(w_1(\varnothing), w_2(\varnothing)), & A = \varnothing, \\ \min(w_1(\bar{\Omega}), w_2(\bar{\Omega})), & A = \bar{\Omega}, \end{cases}$$

则改进的 Denoux 谨慎连接规则定义为:

$$m_{1\wedge^* 2} = m_1 \wedge^* m_2 = \bigoplus_{\varnothing\neq A\subset\Omega} A^{w_{1\wedge^* 2}(A)},$$

其中,标准化系数为 $\xi = [(1 - m(\varnothing))(1 - m(\tilde{\Omega}))]^{-1}$。

ECCR 不仅适用于软件可信性评估的模型求解过程,也可广泛应用于证据不独立背景下的不确定性信息融合问题。

3.3　水平合成算法

基于改进的 Denoux 谨慎连接规则,进一步给出面向多 BBA 合并的水平合成算法。

算法 1.　基于改进 Denoux 谨慎连接规则的水平合成算法:

Step1.　令 $\Omega = \{h_p, p = 1, \cdots, P\}$ 为识别框架, $m_t (t = 1, \cdots, I)$ 为 Ω 上的一组信息源相关的 BBA,初始化 $j = 1, i = 2$;

Step2.　按照式(1)和定理 2.1 分别计算 m_j, m_i 的权重函数 $w_j(A)$, $w_i(A)$;

Step3.　执行改进的 Denoux 谨慎连接规则进行合并,更新 $m_j \leftarrow m_j \wedge^* m_i$,标准化系数 $\xi = (1 - m$

$(\varnothing)^{-1}$;

Step4 如果 $i = I + 1$,则 $i \leftarrow i + 1$,转 **Step2**;否则向下执行;

Step5 剔除合成结果中由"相对权重与折扣"引起的无知,输出 m^*。

$$m^* = m/(1 - m(\overline{\Omega})) \tag{2}$$

m^* 即为 $m_1, \cdots, m_I$ 的标准化合成结果。

4 软件可信性评估模型推理过程抽象

4.1 指标系统模型

基于多维可信属性的多尺度量化指标系统(Trustworthiness evaluation index system, TEIS)的建立是进行软件可信性评估模型研究不可或缺的基础。而应用背景的多样性、用户需求的持续变化及外部环境的动态演变等,都会导致软件需要满足不同的可信需求,从而进一步要求评估专家针对性地构建具有不同逻辑结构的 TEIS。因此,为了便于阐述软件可信性评估的逻辑推理过程,首先给出 TEIS 的形式化定义。

定义 6 软件可信性评估指标系统是一个六元组, $TEIS = (X_e, X_m, X_w, subelem, indeva, weis)$:

$X_e = \{e_r, X_{em}, X_{el}\}$ 是指标系统中所有指标的集合,其中:e_r 是根指标,即软件可信性的综合评价指标; X_{em} 是中间指标集合,包括了软件的可信属性和子可信属性; X_{el} 是叶子指标集合,叶子指标又称为度量元,用于原始信息采集,依据评价方式的不同,又可分为定性和定量叶子指标;

X_m 是指标上 BBA 的集合,如果存在 $m_t \in X_m$,那么 m_t 表示待评软件在指标 e_t 上的可信状况;

X_w 是指标相对权重的集合,并满足同一指标下的所有子指标权重归一化;

$subelem$ 是一个二元关系, $subelem \subseteq X_e \times X_e$,如果 e_1 和 e_2 都是 X_e 中的成员,那么 $(e_1, e_2) \in subelem$ 表示 e_1 是 e_2 的子指标;

$indeva$ 是一个二元关系, $indeva \subseteq X_m \times X_e$,如果 m_1 是 X_m 中的成员, e_1 是 X_e 中的成员,那么 $(m_1, e_2) \in indeva$ 表示 m_1 是指标 e_1 在 Ω 上的 BBA;

$weis$ 也是一个二元关系, $weis \subseteq X_w \times X_e$,如果 w_1 是 X_w 中的成员, e_1 是 X_e 中的成员,那么 $(w_1, e_2) \in weis$ 表示 w_1 是 e_1 的相对权重。

以上定义利用 3 个二元关系将软件可信性评估指标系统中的指标、BBA 和相对权重联系成一个整体。当然,必须在这些二元关系上增加一些限制,才能满足特定应用背景下的软件可信性评估需求。这里,我们不讨论这些限制的详细内容,只是说明软件可信性评估指标系统都能被这个模型所描述。

4.2 联合系数

进行软件可信性评估问题的建模与求解时,需要将 TEIS 中的指标由下至上集结、传递。叶子指标上基本评估信息采集的合理性与准确性是保证模型推理结果能够准确反映软件实体客观现状的基础。而专家评价的随意性及预测模型的不精确性都会导致信息源的不可靠,也就进一步造成原始信息的不可靠,需要使用折扣进行调整。折扣因素估计方法详见文献[14]。

而相对权重也是指标集结过程中不可或缺的因素。因此,集结 TEIS 中的指标需同时考虑信息源的可靠性和指标间的相对权重。和相对权重类似,折扣引起的无知不属于原始信息,也应该在合成过程中予以剔除。对同一证据而言,二者语义不同,但对原始证据的调整策略完全一致,所以本文将采用如下的方法对指标上的 BBA 进行处理:

令 $X_m = \{m_i, i = 1, \cdots, I\}$ 为 $\Omega = \{h_p, p = 1, \cdots, P\}$ 上待合并的 BBA, k_i 为 m_i 的折扣估计值, w_i 为相对权重。合并折扣和相对权重并归一化,得联合系数 π_i:

$$\pi_i = \begin{cases} 1 - k_i, & w_i = 1, \\ \dfrac{w_i(1 - k_i)}{\sum_i w_i(1 - k_i)}, & w_i \neq 1, k_i \neq 0, \\ w_i, & k_i = 0。 \end{cases} \tag{3}$$

使用系数 π_i,对 m_i 做如下调整:

$$\begin{aligned} m_i^{\pi} &= \pi_i m_i = \pi_i m_i(h_p), \ p = 1, \cdots, P, \\ m_i^{\pi}(\Omega) &= 1 - \pi_i \sum_p m_i(h_p) \\ \overline{m}_i^{\pi}(\Omega) &= 1 - \pi_i, \\ \overleftarrow{m}_i^{\pi}(\Omega) &= \pi_i(1 - \sum_p m_i(h_p)). \end{aligned} \tag{4}$$

其中, $\sum_i \pi_i = 1$。由此得到经折扣和权重联合调整后的 BBA m_i^{π},作为初始证据进行叶结点层合并。此外,软件可信性评估是一个递阶过程,需要进行多层合并,直至 e_r。不失一般性,令过程中折扣 $k = 0$,则 $\pi = w$。

4.3 推理过程抽象

运用基于 ECCR 的水平合成算法,对模型的推理过程进行如下抽象:

Step 1 令 $\Omega = \{h_s, 1 \leq s \leq S\}$ 为待评软件的可信性评估统一识别框架,各评价等级的效用为 $V =$

$\{v_s, (1 \leq s \leq S)\}$,评估指标系统 $TEIS = (X_e, X_m, X_w, subelem, indeva, weis)$,其中:$X_e = \{e_r, X_{em}, X_{el}\}$,$e_r$ 是软件可信性综合评价指标,$X_{em} = \{em_1, \cdots, em_n\}$,$X_{el} = \{\{el_p\}, \{el_q\}\}(p, q \in [1, m])$,$el_p$ 和 el_q 分别表示定量和定性叶子指标。$EM = \{em_x\}(1 \leq x \leq X)$ 为参与定性叶子指标评价的专家集合,专家权重为 $\{w_{em_x}\}(1 \leq x \leq X)$;

Step 2　对每个指标层级 $H_t(1 \leq t \leq N)$,求得指标的相对权重,定义为 $X_w = \{\{w_{em_i}\}, \{w_{el_k}\}\}(1 \leq i \leq n, 1 \leq k \leq m)$;同时,采集原始评估信息,运用基于效用的信息转换技术[15]分别求得定量和定性叶子指标在 Ω 上的 BBA,定义为 $X_m = \{\{m_{el_p}\}, \{m^x_{el_q}\}\}, (p, q \in [1, m])$;

Step 3　求得联合系数 π,使用式(4)计算叶子指标上经相对权重和折扣联合调整后的 BBA $X^{\pi}_m = \{\{m^{\pi}_{el_p}\}, \{m^{\pi, x}_{el_q}\}\}$;

Step 4　执行群体意见集结。对定性叶子指标 el_q,使用水平合成算法集结专家意见,求得定性叶子指标上的合成评价 $\{m_{el_q}\}(q \in [1, m])$;结合相对权重 $\{w_{el_q}\}$,求得调整后待合并的 BBA $\{m^{\pi}_{el_q}\}(\pi = w_{el_q})$;

Step 5　对层级 H_N 指标上的 BBA 进行合成,求得层级 H_{N-1} 上指标的 BBA $\{m_{em_i}\}(i \in [1, n])$;再结合指标上的相对权重 $\{w_{em_i}\}$,求得调整后 BBA $\{m^{\pi}_{em_i}\}(\pi = w_{em_i})$;

Step 6　如果 N > 1,则 N = N - 1,转 **Step 5**;否则,向下执行;

Step 7　执行最后一次证据合成,求得待评软件的可信性综合评价 m_{e_r};

Step 8　量化评价,提供更为直观的定量评估数据。依据统一评价等级 h_s 的效用值,使用下式计算所有指标的评价值 $V = \{v_{e_r}, \{v_{em_i}\}^n_{i=1}, \{v_{el_k}\}^m_{k=1}\}$。

$$v_{e_r} = \sum_{s=1}^{S} m_{e_r}(h_s)\, v(h_s)$$

$$v_{em_i} = \sum_{s=1}^{S} m_{em_i}(h_s)\, v(h_s), i = 1, \cdots, n$$

$$v_{el_k} = \sum_{s=1}^{S} m_{el_k}(h_s)\, v(h_s), k = 1, \cdots, m \quad (5)$$

模型最终以指标上的 BBA 和量值两种方式给出软件的可信性评估结果,"不确定性"因素的深入理解保证了推理过程的合理性及评估结果的准确性。

5　算例

随着我国工业化信息化进程的不断推进,大规模工业检测软件(industrial inspection software, IIS)已经被广泛应用于多种工业现场检测系统中[16],对于提升产品质量,提高企业竞争力具有较高的实际意义。本文就以该类软件为研究背景,设计典型算例验证文中提出的模型。

IIS 是一类运行于工业现场的智能软件,必须严格控制危险事故的发生,所以防危性(safety)是其最需考察的可信性质。其次,尽量降低软件失效的发生(可靠性, reliability)、提高工作效率(可用性, availability)和知识产权保护问题(安全性, security)也是需要关注的。由此,设计如图 2 所示 TEIS。

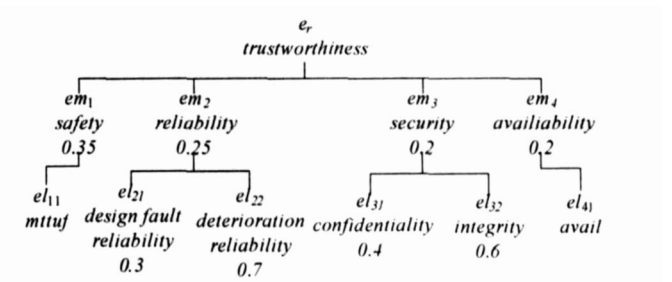

图 2　典型 IIS 软件的可信性评估指标系统

令 $\Omega = \{h_p, p = 1, \cdots, 5\}$ 为统一识别框架,各等级的效用为 $v_h = \{0.1, 0.3, 0.5, 0.7, 0.9\}$,DM = {DM1, DM2, DM3}为参与定性评价的专家集合,专家权重 $w_{DM} = \{0.3, 0.3, 0.4\}$。经一致性转换后的实验数据即为叶子指标在 Ω 上的信度分配 $X_m = \{\{m_{el_p}\}, \{m^x_{el_q}\}\}(1 \leq x \leq 3, p = \{11, 31, 32, 41\}, q = \{21, 22\})$,$el_p$ 和 el_q 分别表示定量和定性叶子指标。

结合折扣估计 k 和相对权重系数 w,利用式(3)计算联合系数 π,并进一步计算联合调整后的 BBA $X^{\pi}_m = \{\{m^{\pi}_{el_p}\}, \{m^{\pi, x}_{el_q}\}^3_{x=1}\}$。表 1 和表 2 分别表示指标系统中定量和定性叶子指标上的原始数据(BBA)及系数调整后 BBA。

基于前文定义的模型,首先在定性叶子指标 el_q 上对专家意见进行集结,计算 el_{21} 和 el_{22} 上的合成评价,表 3 给出了合成结果及经系数调整后 BBA $m^{\pi}_{el_{21}}, m^{\pi}_{el_{22}}$。

对具有相同父结点的叶子指标开展集结,求得第 2 层指标上的 BBA,再结合相对权重进行调整,结果如表 4。最后,在第 2 层指标上开展指标集结,得到顶层指标 e_r 在 Ω 上的信度分配,即 $m_{e_r} = \{(h_4, 0.3233), (h_5, 0.5541)\}$,并利用式(5)该软件的可信性量化评估值 $v_{e_r} = 0.725$。

开展软件可信性评估的最终目的是为了保证决策专家和软件开发人员对该软件的质量状况有全面深刻的主观认识,以便进一步开展软件应用的风险

评价和制定有针对性的改进策略。所以,为了便于决策专家的可信判定,结合项目开发经验和软件的实际应用背景,制定如表(5)所示的可信等级评定及决策表。其中:v 表示利用模型求得的量化评估值。对可信性而言,利用本文模型求得的量化评估值 v_{e_r} = 0.725。依据表 5,决策专家获得了该软件的可信性等级为"较可信,质量一般,应用风险较高,深度改进后部署"。

同时,若不考虑客观存在的评估信息源相关性问题,我们再利用证据推理(evidential reasoning, ER)方法[15]中的解析合成算法进行可信证据的融合,求得在 Ω 上的信度分配为 $m = \{(h_4, 0.397), (h_5, 0.528)\}$,并进一步求得可信性评估值 v = 0.7531,获得可信性评价为"基本可信,质量较好,应用无风险,简易改进后部署或直接部署"。

对比实验结果表明,若不考虑信息源的相关性,采取 ER 方法推算出的量化可信性评估值 $v > v_{e_r}$,这是由于计算过程中未能将由信息源相关引起的重叠计算部分进行有效去除,导致结果偏离事实,且会对专家的后期决策造成重大影响。由此易知,采用本文定义的模型可以获得更为准确、合理的可信性评估结果。

表 1 定性叶子指标上的 BBA 及联合调整结果

el	k	w_{el}	m_{el}	π	m_{el}^{π}
el_{11}	0.15	1	$\{(h_4, 0.25), (h_5, 0.75)\}$	/	$\{(h_4, 0.2125), (h_5, 0.6375), (\bar{\Omega}, 0.15), (\hat{\Omega}, 0)\}$
el_{31}	0.25	0.4	$\{(h_4, 0.62), (h_5, 0.38)\}$	0.4098	$\{(h_4, 0.2541), (h_5, 0.1557), (\bar{\Omega}, 0.5902), (\hat{\Omega}, 0)\}$
el_{32}	0.28	0.6	$\{(h_4, 0.71), (h_5, 0.29)\}$	0.5902	$\{(h_4, 0.419), (h_5, 0.1712), (\bar{\Omega}, 0.4098), (\hat{\Omega}, 0)\}$
el_{41}	0.31	1	$\{(h_4, 0.16), (h_5, 0.84)\}$	/	$\{(h_4, 0.1104), (h_5, 0.5796), (\bar{\Omega}, 0.31), (\hat{\Omega}, 0)\}$

表 2 定性叶子指标上的 BBA 及联合调整结果

DM	w_{DM}	el	k	m_{el}^{x}	π	$m_{el}^{\pi, x}$
DM1	0.3	el_{21}	0.05	$\{(h_4, 0.2), (h_5, 0.7)\}$	0.3523	$\{(h_4, 0.0707), (h_5, 0.2473), (\bar{\Omega}, 0.6467), (\hat{\Omega}, 0.0353)\}$
		el_{22}	0.2	$\{(h_4, 0.6), (h_5, 0.4)\}$	0.2824	$\{(h_4, 0.1694), (h_5, 0.113), (\bar{\Omega}, 0.7176), (\hat{\Omega}, 0)\}$
DM2	0.3	el_{21}	0.32	$\{(h_4, 0.2), (h_5, 0.8)\}$	0.2522	$\{(h_4, 0.0504), (h_5, 0.2018), (\bar{\Omega}, 0.7478), (\hat{\Omega}, 0)\}$
		el_{22}	0.1	$\{(h_4, 0.6), (h_5, 0.3)\}$	0.3176	$\{(h_4, 0.1906), (h_5, 0.0953), (\bar{\Omega}, 0.6824), (\hat{\Omega}, 0.0318)\}$
DM3	0.4	el_{21}	0.2	$\{(h_4, 0.3), (h_5, 0.5)\}$	0.3955	$\{(h_4, 0.1187), (h_5, 0.1978), (\bar{\Omega}, 0.6045), (\hat{\Omega}, 0.0791)\}$
		el_{22}	0.15	$\{(h_4, 0.6), (h_5, 0.4)\}$	0.4	$\{(h_4, 0.24), (h_5, 0.16), (\bar{\Omega}, 0.6), (\hat{\Omega}, 0)\}$

表 3 el_{21} 和 el_{22} 上的合成评价

el	w_{el}	m_{el}	m_{el}^{π}
el_{21}	0.3	$\{(h_4, 0.2297), (h_5, 0.5996)\}$	$\{(h_4, 0.0689), (h_5, 0.1799), (\bar{\Omega}, 0.7), (\hat{\Omega}, 0.0512)\}$
el_{22}	0.7	$\{(h_4, 0.5774), (h_5, 0.3265)\}$	$\{(h_4, 0.4042), (h_5, 0.2285), (\bar{\Omega}, 0.3), (\hat{\Omega}, 0.0673)\}$

表 4 待评软件的可信性综合评价

	w_{em}	m_{em}	m_{em}^{π}	v
em_1	0.35	$\{(h_4, 0.2125), (h_5, 0.6375)\}$	$\{(h_4, 0.0744), (h_5, 0.1881), (\bar{\Omega}, 0.65), (\hat{\Omega}, 0.0875)\}$	0.7225
em_2	0.25	$\{(h_4, 0.2042), (h_5, 0.7175)\}$	$\{(h_4, 0.0511), (h_5, 0.1794), (\bar{\Omega}, 0.75), (\hat{\Omega}, 0.0196)\}$	0.7887
em_3	0.2	$\{(h_4, 0.1495), (h_5, 0.6065)\}$	$\{(h_4, 0.0299), (h_5, 0.1213), (\bar{\Omega}, 0.8), (\hat{\Omega}, 0.0488)\}$	0.6505
em_4	0.2	$\{(h_4, 0.1104), (h_5, 0.5796)\}$	$\{(h_4, 0.0221), (h_5, 0.1159), (\bar{\Omega}, 0.8), (\hat{\Omega}, 0.062)\}$	0.5989
e_r	/	$\{(h_4, 0.3233), (h_5, 0.5541)\}$	/	0.725

表 5 可信等级评定及决策表

v	可信等级	决策意见
$0 \leq v \leq 0.5$	不可信	质量较差,应用风险极高,不能部署
$0.5 < v \leq 0.75$	较可信	质量一般,应用风险较高,深度改进后部署
$0.75 < v \leq 0.9$	基本可信	质量较好,应用无风险,简易改进后部署或直接部署
$0.9 < v \leq 1$	非常可信	质量极好,应用无风险,直接部署

6 结语

保障软件可信是应对由软件失效引起重大事故甚至引发社会危机的有效途径,本文从管理科学的角度,分析和研究了信息源相关背景下软件可信性评估模型的构建方法。提出一种改进的谨慎连接规则,将合并过程中由相对权重引起的未知从结果中剔除,提高了合成精度;给出了软件可信性评估指标系统的形式化定义,并在此基础上建立一种普适性的软件可信性评估模型。与传统的软件可信性评估模型相比,该模型主要具备以下两个特点:

(1)准确性:采用不确定性推理方法,并首次考虑了软件可信性评估过程中客观存在的评估信息源

相关性问题,从源头上保证了评估结果的准确性。因此,与传统的软件可信性评估方法相比,评估结果的准确性得到较大的提升。

(2) 普适性:给出了软件可信性评估指标系统的抽象化定义,由此建立的推理模型可广泛适用于评估过程独立、可信需求确定的单体软件可信性评估过程中,而传统的方法往往只能解决某一类甚至某一特定应用软件的可信性评估问题。

互联网环境下,软件可信性正面临许多新的挑战和问题,这就要求我们不仅要从传统的安全、可靠、可用等角度提高软件个体的可信性,还要从软件群体行为可信的角度对软件的协同行为进行约束,下一步我们将研究群体软件的可信性评估问题,重点关注群体行为下可能出现的涌现特征。

参考文献:

[1] Avizienis, A., Laprie, J. C., Randell, B., et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11 - 33.

[2] 王怀民,唐扬斌,尹刚,李磊. 互联网软件的可信机理[J]. 中国科学 E 辑, 2006, 36(10): 1156 - 1169.

[3] Steffen, B., Wilhelm, H., Alexandra, P., et al. Trustworthy software systems: a discussion of basic concepts and terminology[C]. ACM SIGSOFT Software Engineering Notes archive, 2006, 31(6): 1 - 18.

[4] Gabriele, L., Andrew, T.. Managing trustworthiness in component-based embedded systems[J]. Electronic Notes in Theoretical Computer Science, 2007, 179: 143 - 155.

[5] Water, J. G.. Software dependability evaluation based on markov usage models[J]. Performance evaluation, 2000, 40: 199 - 222.

[6] Shi, H. L., Ma, J., Zou, F. Y.. Software dependability evaluation model based on fuzzy theory[C]. In International Conference on Computer Science and Information Technology, 2008: 102 - 106.

[7] 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.

[8] Hasselbring, W., Reussner, R.. Toward trustworthy software systems [J]. IEEE Computer, 2006, 39(4): 91 - 92.

[9] Denoux, T.. Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence [J]. Artificial Intelligence, 2008, 172: 234 - 264.

[10] 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: 309 - 343.

[11] 王雪荣. 一种基于证据理论的动态综合绩效评价实用方法[J]. 中国管理科学, 2006, 14(4): 121 - 127.

[12] Smets, Ph. The canonical decomposition of a weighted belief[C]. In Int. Joint Conf. on Artificial Intelligence, Morgan Kaufman, SanMateo, CA, 1995: 1896 - 1901.

[13] Shafer, G.. A Mathematical Theory of Evidence [M]. Princeton University Press, Princeton, NJ, 1976.

[14] Elouedi, Z., Mellouli, K., Smets, P.. Assessing sensor reliability for mulTEISensor data fusion within the transferable belief model [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part B: cybernetics, 2004, 34(1): 782 - 787.

[15] Yang, J. B.. Rule and utility based evidential reasoning approach for multiattribute decision analysis under uncertainties [J]. European Journal of Operational Research, 2001, 131: 31 - 61.

[16] 詹辉,张其才. 铸铁材质参数液态在线智能检测和质量控制系统[J]. 中国科技奖励, 2007, 3: 38 - 41.

A Software Trustworthiness Evaluation Model Considering Correlation of Information Sources

YANG Shan-lin, DING Shuai, FU Chao

(Institute of Computer Network System, Hefei University of Technology, Hefei 230009, China)

Abstract: This paper studies a software trustworthiness evaluation model, considering the correlation of information sources. Firstly, an improved Denoeux cautious conjunctive rule and a horizontal evidence combination algorithm are introduced. Secondly, an association coefficient is defined to the index or group opinion aggregation. Finally, on the analysis of objective problems, such as information uncertainty and correlation of information sources in the process of evaluation, a software trustworthiness evaluation model based on evidence theory is proposed. Experimental results show the rationality and validity of the model.

Key words: software trustworthiness; correlation of information sources; evidence theory; evaluation model