一种基于多维属性的CPS软件可信性评估方法

戎 玫
(暨南大学深圳旅游学院 深圳 518053)
(中国科学院软件研究所计算机科学国家重点实验室 北京 100190)

摘 要 信息物理融合系统(CPS)是一种融合了物理过程和计算进程的新型系统,在信息物理融合系统中,存在多种软件且每个软件的运行环境是动态变化的。如何有效保证软件在动态环境下的正确性、安全性、可靠性等属性是值得关注的问题,而可信评估可为软件质量的控制和管理提供有力依据。提出了一种基于多维属性的CPS软件可信性评估方法。首先提出一种基于多维属性的可信指标系统,在此基础上提出一种具有时效性的可信属性评价方法,用以评价CPS软件的可信性;然后,设计可信性结果决策规则集,根据软件间的交互结构,计算出软件系统的可信性,并根据决策规则集评价软件系统可信性;最后通过一个实例进一步说明了所提方法的有效性。

关键词 多维属性,信息物理融合系统,可信证据时效性,软件可信性评估
中图法分类号 TP311 **文献标识码** A

Trustworthiness Evaluation Method for CPS Software Based on Multi-attributes

RONG Mei
(Shenzhen Tourism College, Jinan University, Shenzhen 518053, China)
(State Key Laboratory of Computer Sciences, Chinese Academy of Sciences, Beijing 100190, China)

Abstract Cyber-Physical System(CPS) is a kind of new system by combining physical world with computation. There are many kinds of software in Cyber-physical System, and each of them is running dynamically. It's hard to ensure the properties such as correctness, safety, reliability with the dynamical environment. And trustworthiness evaluation can provide evidence for software quality management. So we proposed a method for CPS software's trustworthiness evaluation based on multi-attri-butes. Firstly, we proposed a trustworthiness evaluation indicator system based on multi-attributes, secondly brought forward a method for software trustworthiness evaluation by considering the aging of trustworthiness evidences. After that, a set of decision rules was designed to explain the evaluation result. Then based on the interaction logic of software, the trustworthiness level of CPS software system was evaluated. At last, an example was used to explain the effectiveness of the framework.

Keywords Multi-attributes, Cyber-physical system, Aging of trustworthiness evidences, Software trustworthiness evaluation

信息物理融合系统(Cyber-Physical System,CPS)是一个综合了计算过程和物理环境的多维复杂系统[1],可感知现实世界的动态变化,并做出反馈。CPS通常部署在一些关键基础设施及可信性要求很高的领域。可信性是在安全性、可靠性及可用性等概念上建立起来的一个新概念,是客观对象的诸多属性在人们心中的一个综合反映[2]。因此,如何保证CPS的可信性是一个值得研究的方向。而在一个CPS中,软件负责系统的数据处理、通讯控制、决策支持等,故软件可信与否直接关系到CPS的可信性。目前对于CPS的研究工作主要有CPS体系结构分析[3]、CPS传感器网络[4]、CPS应用实例[5]和CPS软件设计[6,7]等。而CPS可信性评估的研究工作都是对传感器网络的可信性评估[8,9],关于CPS软件可信性评估的研究较少。

软件可信性评估是指基于合理的证据或经验对软件实体的所有非功能性属性(又称为可信属性)是否遵从预定规则集的评价,基于多维可信属性的软件可信性评估技术是实施可信性过程控制和开展可信性管理的核心基础,是可信软件发展亟待解决的问题之一。已有的研究提出了许多不同的评估方法。文献[10]中描述了一种采用软件分级模型对可信性进行评估的方法;文献[11]采用了度量和提高软件过程可信性的方法来保障软件可信,构建了可信过程管理框架TPMF;文献[12]建立了基于验证的可信证据模型,并在此基础上给出了一种反映人对软件认知深入程度的可信评估方法;文献[13]中针对开源构件可信性进行了评估。分析上述研究成果发现,现有的评估方法主要存在的问题包括:(1)度量属性单一,如文献[13]只考虑了可靠性,未考虑其他属性;(2)未考虑可信证据的时效性,即可信证据与软件可信性的关系会随时间发生变化;(3)面向特定的阶段,如文献[11]对软件过程进

到稿日期:2013-01-24 返修日期:2013-04-30 本文受江苏省自然科学基金(BK2011281),苏州市应用基础研究计划(SYG201241)资助。
戎 玫(1966—),女,博士,副教授,CCF高级会员,主要研究方向为网络软件工程与形式化方法、物联网(CPS)与可信计算。

行评估。

为了判断软件的可信状态，迫切需要研究软件可信性评估技术，基于多维可信属性的多尺度量化指标系统、度量和评估机制已经成为软件可信性评估领域的研究热点[2]。在软件可信性评估过程中主要存在的问题有：可信度量指标的选取、指标的合理量化、多量纲信息融合以及复杂的评估推理逻辑等。基于此，本文首先通过考虑多维可信属性，建立一组可信属性评估指标系统和评估结果决策规则集；接着，引入可信证据时效性概念，并利用可信属性评估指标系统评价软件可信性；最后，根据评估结果决策规则集对可信性评估推理结果进行具体阐释。

1 CPS 软件的可信性评估方法

软件的可信属性表达了软件的一种与可信相关的客观能力，若软件具有相关可信属性，那么该软件可以达到预期目标[10]，建立一个可操作性强的可信属性量化指标系统是开展可信软件评估的基础。而不同的软件具有不同的可信需求，甚至同一软件在不同时段也可能具有不同的需求，所以迫切需要研究一种可信软件评估指标系统的动态构造模型。文献[10]将软件的可信属性表达为树形结构，分别是可用性、可靠性、安全性、实时性、可维护性、可生存性。本文在文献[10]的基础上采用树形结构建立可信属性评估指标系统，并细化可信属性之间的关系。

评估指标系统通常满足树型逻辑结构，这里简称为可信指标树。树中的每一个节点都是可信属性，其中根节点是可信性，其他节点都是对可信性的细化；可信属性可嵌套，子属性是对父属性更详细的描述。在可信指标树属性模型中，每个叶节点都是可以直接度量的单元，可以通过评估指标计算出相应的评估结果。在建立了可信指标树后，需要求出各层可信属性之间的权重分配。作为一种多属性决策问题，这里可以采用 AHP 方法求解各属性的权重。

在建立了可信指标树后，遵循决策独立性条件制定符合用户要求的可信决策规则集，可信性决策规则集通常是对软件可信性评估推理结果的具体阐释，可为专家最终决策提供有效支持。

在建立了可信指标树和评估结果决策规则集后，就可以对 CPS 软件的可信性进行评估。首先，需要采集可信证据，可信证据的来源包括软件测试或代码分析、软件模型预测、专家定性评价或系统运行记录等；然后，对采集到的数据进行转换，并利用可信指标树对各可直接度量的可信属性进行评估。由于 CPS 软件运行环境的动态性，使得可信证据的可信性随时间变化，即具有时效性特征。因此在评价可信属性时，需要引入时间衰减函数 ρ 来表示可信证据的时效性，这里认为时间衰减函数 $\rho=e^{\beta(t-\sigma)}$，下面通过一个定理来说明该函数的正确性。

定理 1 设 ρ 为时间衰减函数，t 为时间变量，σ 为当前时刻，β 表示衰减速率，则 $\rho=e^{\beta(t-\sigma)}$，且 β 越大衰减越快。

证明：用 $f(t)$ 表示当前可信性程度，用 $\overline{f(t,\omega)}$ 表示经过时间 ω 可信性的平均改变率，则 $\overline{f(t,\omega)}=\dfrac{f(t+\omega)-f(t)}{\omega}$，从统计学意义上看，近期的活动相对于久远的活动而言具有更高的可信任度，则 $f(t)$ 随着 t 的增加而增大。假定每一个时刻可信性的改变率用 β 表示，则定义 $\beta=\dfrac{\dfrac{f(t+\omega)-f(t)}{\omega}}{f(t)}$，为了求得 $f(t)$，将 $f(t)$ 看作连续函数，则 $\beta=\dfrac{\lim\limits_{\omega\to 0}\dfrac{f(t+\omega)-f(t)}{\omega}}{f(t)}=\dfrac{f'(t)}{f(t)}$，解得 $f(t)=e^{\beta t+c}$，又由于 $0\leqslant f(t)\leqslant 1$，则 $t\leqslant -\dfrac{c}{\beta}$，令 $\sigma=-\dfrac{c}{\beta}$，那么 $f(t)=e^{\beta(t-\sigma)}$，即 $\rho=e^{\beta(t-\sigma)}$。

在证明了引入的衰减函数的正确性后，就可以利用度量方法对可直接度量的软件可信属性进行综合评价，具体如下，设可直接度量的软件可信属性集为 TA。

$\theta_j^i(\sigma)$ 是软件 i 的某一可直接度量的可信属性 j 在过去时间内度量结果的综合体现，设 $d_j^i(t)$ 为软件 i 的可信属性 j 在过去某时刻 t 的度量结果，则可信属性综合评价方法如下：

$$\theta_j^i(\sigma)=\frac{\sum_{t\leqslant\sigma}\rho d_j^i(t)}{m},(t\leqslant\sigma,0\leqslant\rho\leqslant 1,m\neq 0,j\in TA)$$

式中，σ 为当前时刻，m 为某一可信属性过去度量结果的数目。

接着，在得出可直接度量的软件可信属性综合评价结果后，根据可信指标树中各层可信属性的权重，利用可信指标树评估 CPS 软件可信性，具体的软件可信性评估方法如下。

根据构造的可信指标树，从底层向上逐层推导。设 w_j 为某一可信属性所占的权重，$\theta_j^i(\sigma)$ 为该可信属性的综合评价结果，$\delta^i(\sigma)$ 为其父结点，那么推导方法为：

$$\delta^i(\sigma)=\sum w_j\theta_j^i(\sigma),\sum w_j=1$$

反复利用上式，最后可计算出顶点结点值，即软件 i 的可信性。在计算出软件可信性后，就可以利用决策规则集来评估软件的可信等级，从而判断软件的运行是否满足要求。

由于 CPS 是一个网络化的开放系统，故单个软件的可信并不一定能保证整个软件系统运行的可信性[15]。因此，需要对 CPS 软件系统的可信性进行评估，下面介绍基于交互结构的 CPS 软件系统可信性评估方法。

2 基于多维属性的 CPS 软件可信性评估方法

CPS 软件系统是由各软件通过网络交互组合而成，因此，CPS 软件系统可信性由软件系统中各软件可信性及各软件间交互结构的可信性决定，这里认为网络完全可信，故不考虑网络的可信性对 CPS 软件系统可信性的影响。在大多数网络化的系统中，顺序、循环、并发和选择是其基本的交互结构[16]。因此，可以采用这 4 种结构作为 CPS 软件系统交互结构的组成基础，并通过计算每一种结构的可信性得到 CPS 软件系统的可信性，下面给出这 4 种结构的可信性评估方法。

CPS 软件系统由顺序、循环、并发和选择 4 种交互结构组成，每种结构的可信性评估方法如下：

(1)顺序：顺序结构如图 1 所示，设 $\delta^i(\sigma)$ 为软件的可信性，$\Delta(\sigma)$ 为软件系统的可信性，那么 $\Delta(\sigma)=\prod_{i=1}^{n}\delta^i(\sigma)$，$i$ 为软件个数；

(2)循环：循环结构如图 2 所示，设 $\delta^i(\sigma)$ 为软件的可信性，$\Delta(\sigma)$ 为软件系统的可信性，p 为循环的概率，那么 $\Delta(\sigma)=\dfrac{(1-p)\delta^i(\sigma)[1+\sum_{m=1}^{\infty}(p\delta^i(\sigma))^m]}{m+1}$，$i$ 为软件个数，m 为循环次

数；

(3)并发：并发结构如图 3 所示，设 $\delta^{s}(\sigma)$ 为软件的可信性，$\Delta(\sigma)$ 为软件系统的可信性，那么 $\Delta(\sigma)=\min\{\delta^{s1}(\sigma),\delta^{s2}(\sigma),\cdots,\delta^{sn}(\sigma)\}$，$n$ 为软件个数；

(4)选择：选择结构如图 4 所示，设 $\Gamma_i(\sigma)$ 为由软件组成的第 m 个模块的可信性，$\Delta(\sigma)$ 为软件系统的可信性，p_m 为第 m 个分支执行的概率，那么 $\Delta(\sigma)=\dfrac{\sum_{m=1}^{\infty}(p_m\Gamma_m(\sigma))^m}{m}$。

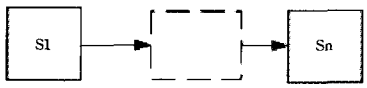

图 1　顺序结构

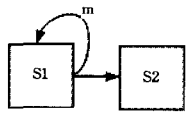

图 2　循环结构

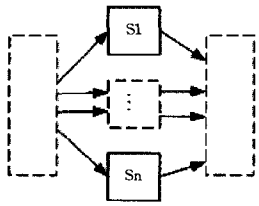

图 3　并发结构

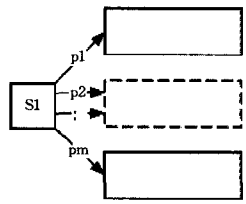

图 4　选择结构

根据交互结构可信性评估方法，通过分析 CPS 软件系统的交互结构，可以计算出 CPS 软件系统的可信性，接着利用评估结果决策规则集评估 CPS 软件系统的可信性等级。

3　实例分析

随着城市的发展，现有的交通基础设施已经不能满足要求，交通拥挤现象严重。在这种背景下，从 CPS 的观点出发，把车辆和道路结合起来考虑，便产生了解决交通问题的思想，这就是智能交通系统(Intelligent Transportation System，ITS)。ITS 以区域为单位组织汽车，每个区域内部有一定数量的汽车，每辆车都配有不同的软件，并且区域中汽车数目动态变化。

为了便于分析，本文仅以 ITS 中一个区域内的两辆车之间的交互作为实例。在 ITS 中，一辆车至少配有传感器软件 s、执行器软件 a 以及控制软件 c，这些软件之间存在交互，而在不同的车辆之间也存在通信。假设汽车 1 与汽车 2 要根据各自的状态调整汽车的运行参数，首先 $c1$ 要求 $s1$ 获取汽车 1 的运行状态信息，然后将信息传送给 $c2$，$c2$ 再要求 $s2$ 获取汽车 2 的运行状态信息，将信息返回给 $c1$，最后 $a2$ 和 $a1$ 根据汽车 1 和汽车 2 的运行状态对汽车的运行参数进行调整，做出软件系统的交互结构图，如图 5 所示。

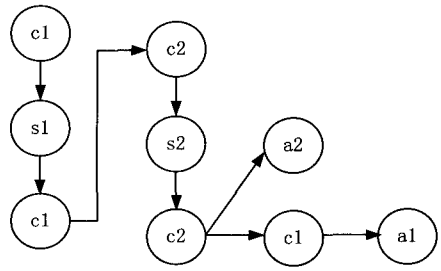

图 5　软件系统交互结构图

通过分析需求，可直接度量的可信属性为可用性、可靠性、机密性、完整性、实时性、可维护性和可生存性，建立可信指标树，如图 6 所示，其中每个叶子结点即为可直接度量的可信属性。对文献[10]中的可信属性进行扩展，定义可直接度量的可信属性的度量方法，如表 1 所列。

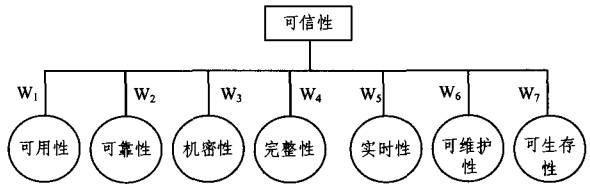

图 6　可信指标树图

表 1　可信属性度量方法

可信属性名称	度量方法
可用性	$d_U(t)=\dfrac{UFN}{FN}$，UFN 表示不可用功能数，FN 表示功能总数
可靠性	$d_R(t)=1-\dfrac{Failed\_Time}{t}$，Failed_Time 表示失效时间，t 为执行时间
机密性	$d_S(t)=1-\dfrac{Ill\_Act}{Act}$，Ill_Act 为非法操作数据次数，Act 为总操作次数
完整性	$d_I(t)=1-\dfrac{Incon\_Data}{Data}$，Incon_Data 为不一致数据，Data 为总数据
实时性	If aTime<eTime then $d_{RT}(t)=e^{aTime-eTime}$，else $d_{RT}(t)=1$，aTime 表示预期时间，eTime 表示执行时间
可维护性	$d_M(t)=\dfrac{MCN}{CN}$，MCN 表示修改代码行数，CN 表示代码总行数
可生存性	$d_L(t)=\dfrac{ARN+RN}{AN}$，ARN 为抗攻击次数，RN 为受攻击恢复次数，AN 为受攻击总次数

设有多位专家为软件的可信属性进行权重评价，利用 AHP 方法求解可信属性权重分配，这里限于篇幅，不给出具体计算过程，软件的可信属性权重分配结果如表 2 所列。

表 2　软件的可信属性权重分配

软件名称	可用性	可靠性	机密性	完整性	实时性	可维护性	可生存性
传感器软件	0.1	0.2	0.1	0.1	0.2	0.1	0.2
执行器软件	0.1	0.2	0.1	0.1	0.2	0.1	0.2
控制软件	0.2	0.2	0.1	0.2	0.1	0.1	0.1

在建立了可信指标树后，遵循决策独立性条件制定符合用户要求的可信决策规则集。可信性决策规则集通常是对软件可信性评估推理结果的具体阐释，可为专家最终决策提供有效支持。下面给出一个可信决策规则集，如表 3 所列，其中 v 表示综合评估值，$l=d(v)$ 表示可信性等级函数，$r(d(v))$ 表示决策规则函数。

表 3　可信决策规则集

v	l=d(v)	r(d(v))
[0,0.25)	Poor	不可信,使用风险大
[0.25,0.5)	Low	可信度低,使用风险较大
[0.5,0.75)	Medium	可信度适中,使用风险适中
[0.75,1]	High	可信度高,使用风险小

利用本文定义的可信属性评价方法,可以对系统的各可信属性进行评价,限于篇幅,这里不具体给出计算过程,各可信属性综合评价结果如表 4 所列。

表 4　可信属性综合评价结果(β=1)

软件名称		可用性	可靠性	机密性	完整性	实时性	可维护性	可生存性
汽车 1	传感器软件 s1	0.84	0.82	0.95	0.96	0.91	0.95	0.87
	执行器软件 a1	0.92	0.87	0.86	0.95	0.85	0.89	0.93
	控制软件 c1	0.81	0.93	0.87	0.88	0.83	0.87	0.95
汽车 2	传感器软件 s2	0.93	0.91	0.91	0.85	0.93	0.93	0.89
	执行器软件 a2	0.89	0.86	0.83	0.88	0.91	0.85	0.85
	控制软件 c2	0.87	0.87	0.87	0.93	0.93	0.93	0.97

根据表 4 给出的软件可信属性综合评价结果及表 2 给出的可信属性权重分配,可以计算出软件的可信性,结果如表 5 所列。

根据图 1 及定义 4,可以得出该软件系统的可信性为 $\Delta(t)=0.396$,再根据决策规则集对软件系统的可信性等级进行评估,结果为低可信性,说明使用该系统具有较大风险。该实例中各软件的可信性都较高,但是经过交互组合后,整个系统的可信性大幅下降,因此软件间的交互和系统状态的转移会对整个系统的可信性产生影响,需要对软件的交互结构进行调整。因此在实际的系统设计中,需要加强软件间交互结构的管理。

表 5　软件可信性

	汽车 1			汽车 2		
软件名称	传感器软件 s1	执行器软件 a1	控制软件 c1	传感器软件 s2	执行器软件 a2	控制软件 c2
可信性	0.89	0.892	0.876	0.908	0.869	0.904

结束语　由于 CPS 通常部署在可信性要求很高的领域,故 CPS 的可信性保障是一个重要的研究方向。而在 CPS 中,软件扮演者协调、控制整个系统的角色,因此软件的可信性保障尤其重要。但是由于组成 CPS 软件系统的软件种类繁多,导致用户需求复杂,而不同领域、不同软件的用户对软件可信性要求具有很大区别,目前的可信性评估方法存在着评估属性单一、针对特定的评估对象、未考虑可信证据的时效性等问题。考虑到可信性是多种可信属性的综合反映,通过对可信属性的分类来描述和评价软件的可信性。基于此,本文对已有的支持可信评估的框架进行了扩展和改进,提出了一种基于多维属性的 CPS 软件可信性评估方法,并详细分析了应用该方法进行可信评估的过程,给出了具体的案例分析,说明了该方法的有效性。

本文提出的可信评估方法假定获取的证据都是可信的,因此没有采取措施保障证据的可信性,在后续工作中将针对证据的可信度做进一步的研究;此外,本文也没有考虑需求改变时的应对方法,因此下一步研究工作还将考虑当需求发生变化时评估方法的动态演化问题。

参 考 文 献

[1] Poovendran R. Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds [J]. Proceedings of the IEEE, 2010, 98(8): 1362-1366

[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] 王中杰,谢陆路. 信息物理系统研究综述[J]. 自动化学报, 2011, 37(10): 1157-1166

[4] Ehyaei A, Tovar E, Pereira N, et al. Scalable Data Acquisition for Densely Instrumented Cyber-Physical Systems[C]// 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems(ICCPS). Los Alamitos: IEEE Computer Society, 2011: 174-183

[5] Marija D I, Xie L, Khan U A. Modeling of Future Cyber-Physical Energy Systems for Distributed Sensing and Control [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2010, 40(4): 825-838

[6] Bak S, Manamcheri K, Mitra S, et al. Sandboxing Controllers for Cyber-Physical Systems[C]// 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems (ICCPS). Los Alamitos: IEEE Computer Society, 2011: 3-12

[7] Duggirala P S, Mitra S. Abstraction Refinement for Stability[C]// 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems(ICCPS). Los Alamitos: IEEE Computer Society, 2011: 22-31

[8] Zhang F, DiSanto W, Ren J, et al. A Novel CPS System for Evaluating a Neural-Machine Interface for Artificial Legs[C]// 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems(ICCPS). Los Alamitos: IEEE Computer Society, 2011: 67-76

[9] Tang L, Yu X, Kim S, et al. Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems[C]// 2010 IEEE International Conference on Data Mining. Los Alamitos: IEEE Computer Society, 2010: 1079-1084

[10] 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

[11] Yang Y, Wang Q, Li M S. Process trustworthiness as a capability indicator for measuring and improving software trustworthiness [C]// Lecture Notes in Computer Science 5543: Proceedings of the International Conference on Software Process. Berlin Heidelberg: Springer-Verlag, 2009: 389-401

[12] 丁学雷,王怀民,王元元,等. 面向验证的软件可信证据与可信评估[J]. 计算机科学与探索, 2010, 4(1): 46-48

[13] Uzma R, Marietta J T. Defining and Evaluating a Measure of Open Source Project Survivability[J]. IEEE Transactions On Software Engineering, 2012, 38(1): 163-174

[14] 沈昌祥,张焕国,王怀民,等. 可信计算的研究与发展[J]. 中国科学:信息科学, 2010, 40(2): 139-166

[15] 吕建,徐锋,王远. 开放环境下基于信任管理的软件可信保障[J]. 中国计算机学会通讯, 2007, 3(11): 14-24

[16] Lee E A. Cyber physical systems: Design challenges[C]// 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC). Los Alamitos: IEEE Computer Society, 2008: 363-369