计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(8): 1464-1472, 2011

基于交互式马尔可夫链的可信动态度量研究

庄 琭 蔡 勉 沈昌祥
(北京工业大学计算机学院 北京 100124)
(可信计算北京市重点实验室 北京 100124)
(zhuanglu686@yahoo.com.cn)

Trusted Dynamic Measurement Based on Interactive Markov Chains

Zhuang Lu, Cai Mian, and Shen Changxiang
(*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124)
(*Beijing Municipal Key Laboratory of Trusted Computing, Beijing* 100124)

Abstract Trusted computing ensures trustworthiness of a platform through extending the trust boundary from the root to the whole platform. Trusted measurement is invoked before the trust boundary is extended from one entity to including another. Static measurement, which takes place at startup, cannot ensure runtime trustworthiness, and therefore dynamic trusted measurement is indispensable to guarantee a computer platform to run dependably. According to dependability, availability and security of information and behavior, targets of trusted measurement are established. In present schemes of dynamic trusted measurement, the measurement of functionality is focused on, whereas dependability cannot be guaranteed without the measurement of performance. Based on interactive Markov chains (IMC), the measurement of performance feature besides function feature is introduced. In the expected behavior description, the function expectation is described through a model of transition system and the performance expectation is described through relating path probability indicating dependability to the time expectation in which a certain specific behavior function is achieved. By comparing the runtime evidence of a platform with a specific expectation, trusted verification on a combination of functionality and performance is achieved. The trusted dynamic measurement model based on IMC ensures dependability in the feature of performance besides function and guarantees trustworthiness of a platform across the board.

Key words trusted computing; trusted dynamic measurement; interactive Markov chains; functionality measurement; performance measurement

摘 要 可信动态度量为保障可信计算平台的可靠运行提供了重要支撑.根据系统的可靠性、可用性、信息和行为安全性,提出了可信度量要达到的目标.当前的可信度量集中在可信功能度量上,基于交互式马尔可夫链增加性能特征指标度量,即在预期行为描述模型中,运用变迁系统模型描述功能预期,通过将体现在可靠性上的路径概率与预期的关联,获取完成特定行为功能在时间特征上的预期,用于性能特征指标的度量.所构建的功能与性能特征预期用于对系统运行时证据实施相应的功能与性能上的可信性验证.基于交互式马尔可夫链的动态度量模型,从性能角度完善了对可靠性的保障,更全面地确保了系统的可信.

收稿日期:2011-04-07;**修回日期**:2011-06-09
基金项目:国家"九七三"重点基础研究发展计划基金项目(2007CB311100);国家"八六三"高技术研究发展计划基金项目(2009AA012437);"核高基"国家科技重大专项基金项目(2010ZX01037-001-001)

关键词　可信计算;可信动态度量;交互式马尔可夫链;功能度量;性能度量

中图法分类号　TP309

可信计算组织(Trusted Computing Group,TCG)推出以可信平台模块(TPM)[1]为核心的可信计算规范,标志着通过信任根扩展信任边界确保整个系统可信的可信计算平台的形成.信任边界的扩展过程即信任链的构建过程,通过一级度量一级,一级信任一级实现,所以信任扩展的依据是可信度量.TCG在信任链的构建中所采用的完整性度量是一种静态度量,完整性只能反映系统启动时的可信状态,尚不能反映系统运行时的可信状况,达不到TCG提出的"行为可预期"[2]的可信目标.因此,可信计算系统需要可信性动态度量的支持,软件的动态度量模型[3]的研究具有很强的现实意义.

可信动态度量是为了保障平台的运行时可信.自从动态可信提出以后,已有一些相关的研究进展.2004年至2006年间,IMA[4],PRIMA[5],BIND[6]等研究分别采用对运行时实体完整性、信息流完整性、实体的功能片段完整性度量方法,但没有从行为的角度准确地反映系统的可信.此后的研究更多地关注软件行为可信,BTAM[7]指出对系统的动态可信性度量只需关注与可信相关的行为,没有给出如何判断行为是否与可信相关及如何度量行为可信.一种基于软件行为的动态完整性度量模型[8-9]以及作者先前的工作[10]从实现行为可信功能的角度抽象预期,给出了度量行为动态可信的模型.

在性能检测方面,面向实时性、动态性的入侵检测技术提供了一些方法,如异常模型[11]中所使用的各种统计特性.阈值度量中,指定时间长度内少于m或多于n个事件发生即被视为异常,如系统登录时特定时间段内超过某一阈值的尝试则被视为恶意行为.IDES[12],Haystack[13]等统计动差模型中,通过计数值或时间间隔的统计特性检测异常,核心思想是度量值如果跌出了动差的期望间隔,则被视为异常.入侵检测技术为性能度量提供了一些方法,但当前的入侵检测技术仍存在如下缺陷:1)缺乏系统的描述模型,导致方法局限于特定场景下的特定问题;2)性能度量的同时牺牲了功能的度量,两者难以有效地结合.

功能即关注系统"做什么,怎么做",性能即关注系统"做得如何".当前的可信度量集中在功能度量上,尚未有相关研究对"做得如何"进行度量和评价,但随着并行性、分布性等特征的呈现,计算机系统的复杂程度不断增加,可信功能度量已不能全面描述和反映系统的可靠性,比如当引入行为时延时,就已超过了功能度量模型的表达能力.可信动态度量的功能度量验证应用软件行为是否可预期,反映了系统是否可靠,但系统的可靠性[3,14]如何,还需要由其他特征来描述.系统的可靠性通常用时间特征、概率特征等性能特征指标体现.本文基于交互式马尔可夫链(IMC)[15]构建细粒度的可信动态度量模型,在功能度量的基础上,引入性能特征指标的度量.对于IMC:一方面,它是一种描述系统功能和性能的混合模型,在系统功能刻画的基础上加入了性能指标,IMC常用于系统的功能验证和性能评价,如模型检验;另一方面,与其他模型相比,IMC在结合功能和性能时采用正交化的方式,有利于动态度量在同一个模型下引入性能特征指标的度量,如随机进程代数(SPA)在结合功能和性能时将两者合二为一,导致非确定性被随机分布所取代,以及针对同步的并发操作难以表示等缺陷,使得在这些模型下性能特征指标度量的引入将折损功能度量的效能.本文基于IMC构建度量模型,将IMC用于可信度量,即借助这种混合功能和性能的描述模型,在抽象行为的同时,引入与行为发生时延相关的状态转移概率,在此基础上可形成行为路径概率,将其与特定预期相关联即可获取预期路径时间,形成完成特定行为功能在时间特征上的预期,用于对平台运行时证据在系统性能特征指标上的度量,通过这种在度量模型中引入性能特征的描述,增强系统的可靠性.本文在IMC模型中运用变迁模型描述功能预期,对IMC模型中状态进行标记,表示从该状态出发的可信执行路径,以描述性能预期.在所构建的预期下通过对所获取的平台证据实施功能结合性能的可信性验证,实现对系统的可信度量.

1　交互式马尔可夫链

作为一种可组合化的并发系统分析框架,IMC采用正交的方式结合经典的功能模型——标记变迁系统(LTS)[16]和性能模型——连续时间马尔可夫链(CTMC),IMC定义如下:

定义1. 一个IMC是一个五元组$(S,Act,\rightarrow,\rightarrow,s_0)$,其中:

1) S 是一个非空的状态集合;

2) Act 是一个动作集合;

3) $\rightarrow \subseteq S \times Act \times S$ 是动作转移关系;

4) $\rightarrow \subseteq S \times \mathbb{R}_{\geqslant 0} \times S$ 是马尔可夫转移关系,满足 $\forall s_1, s_2 \in S, |(\rightarrow \cap (\{s_1\} \times \mathbb{R} \times \{s_2\}))| \leqslant 1$;

5) s_0 是初始状态.

定义中的 2 个转移关系分别是 LTS 中的动作转移与 CTMC 中的随机分布延迟转移(由指数分布的参数表示). 如图 1 所示,IMC 模型具有如下 2 个特点:

1) 系统在一个状态上可以执行多个可能的动作转移,如 S_1 可在动作 a,b 间进行选择. 由于动作转移与时间延迟是分离的,所以这些动作转移之间的选择保留了 LTS 的非确定性解释.

2) 在一个状态上若既可以执行动作转移,又可以执行马尔可夫转移,如 S_1,则采取最大前进假设:内部动作(用 τ 表示)的执行不允许时间延迟,即若有内部动作,则其执行是立即的,不允许其他延迟转移发生. 外部动作(集合以 Obs 表示,其中的动作以 $a,b,c,\cdots$ 表示)的执行依赖于环境,有可能被延迟,如对于 S_1,若在一定时间内系统没有执行动作(或与环境进行交互动作)a 或 b,那么系统可以选择执行马尔可夫转移.

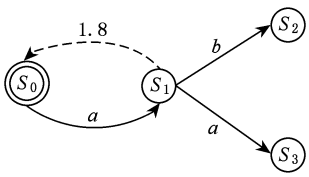

Fig. 1 IMC graph.

图 1 IMC 图示

2 基于交互式马尔可夫链的可信动态度量模型

可信动态度量包含以下 3 个步骤:1)行为预期描述;2)系统运行时证据获取;3)行为可信性验证. 下面依据该步骤阐述基于 IMC 的可信动态度量模型及构建方法.

2.1 行为预期描述

IMC 从功能和性能上描述了系统的特征,本节基于 IMC 从功能和性能角度实现对预期的描述,作为系统行为预期描述,用于可信动态度量. 首先介绍描述系统特征的 IMC 构建.

2.1.1 IMC 构建

本节重点阐述在功能描述的基础上结合系统性能特征构建 IMC 模型. 模型的构建基于作者先前基于软件行为学[17]理论对功能度量的研究工作[10]的成果.

文献[10]对软件行为学中描述行为主体在行为树上遍历、从事行为实际含义的行为信息基进行改造,形成行为度量信息基,用于可信动态度量. 事实上,行为度量信息基仅仅从功能角度描述了行为预期,即仅说明了软件应该"做什么",不涉及任何由时间、概率等体现的性能特征指标,即并未说明软件"做得怎么样". 本节以行为度量信息基作为功能描述,在此基础上结合系统性能特征生成 IMC 模型. 首先对行为度量信息基的结构进行说明,该结构通过行为树的 BNF(Backus-Naur form)定义形式简要描述如下(完整描述请参见文献[17]):

$root ::= root\_name:\{subject\_ide \quad APPLIES \ service\_ide:[EX\ condition]Action\_body\}$;

$node ::= node\_name:\{sercive\_ide:Action\_body\}$;

$Action\_body ::= \text{empty} \mid atom\_Action \mid compositive\_Action \mid Action\_body;Action\_body$.

行为树从树根开始定义根行为,树叶即原子行为,中间结点表示复合行为,可进入下一层次行为子树. 现定义相关操作以实现从行为度量信息基到 IMC 模型的构建.

定义 2. 操作 $extend(a)$,$del\_a(s_1,s_2)$,$create\_s(s)$,$create\_a(s_1,s_2,a)$,$create\_d(s_1,s_2,\lambda)$,$rel(node,a)$,$get\_node(a)$,$get\_prest(a)$,$get_poststs(a)$定义如下.

$extend(a)$:扩展当前 IMC 模型中的动作 a;

$del\_a(s_1,s_2)$:删除 IMC 模型中状态 s_1 和 s_2 间的动作;

$create\_s(s)$:生成状态 s;

$create\_a(s_1,s_2,a)$:生成状态 s_1 和 s_2 间的动作 a;

$create\_d(s_1,s_2,\lambda)$:生成状态 s_1 和 s_2 间的延迟,参数为 λ;

$rel(node,a)$:将 IMC 中的动作 a 关联到行为度量信息基中的行为结点 $node$;

$get\_node(a)$:获取与动作 a 关联的行为度量信息基中的行为结点;

$get\_prest(a)$:获取 IMC 模型中动作 a 的前驱状态;

get_poststt(*a*):获取 IMC 模型中动作 *a* 的后继状态.

扩展操作 *extend*(*a*)过程如图 2 所示:

```
s=get_prest(a);
t=get_poststt(a);
node=get_node(a);
del_a(s,t);
create_s(u);
if(node behavior is delayed) then
  create_s(v);
  create_d(s,v,λ);create_a(v,u,a);
else create_a(s,u,a);
if(node is an atom behavior) then
  combine u with t;
else for(every child c_node_i of node):
create_a(u,t,a_i);rel(c_node_i,a_i);extend(a_i);
```

Fig. 2　Flow of *extend* (*a*).

图 2　*extend*(*a*)流程

extend(*a*)是一个递归操作,通过扩展行为度量信息基中的行为实现到 IMC 模型的转化,对于一个行为度量信息基,其根结点为 *root_node*,则该信息基到 IMC 的转化过程如图 3 所述:

```
create_s(s);
create_s(t);
create_a(s,t,a);
rel(root_node,a);
extend(a);
```

Fig. 3　Construction of IMC model from behavior measurement information base.

图 3　从行为度量信息基构建 IMC 模型

至此,通过对行为度量信息基中行为结点的扩展完成了 IMC 的构造.

2.1.2　基于 IMC 模型的行为预期

2.1.2.1　功能预期

IMC 通过变迁模型中的动作转移实现了对功能预期的描述,即在单纯的功能模型中,通过在某一状态下可行的动作所触发的状态变迁描述功能预期.由于功能预期不是本文的重点,故不再进行展开.

2.1.2.2　性能预期

IMC 中的马尔可夫转移只是系统性能特征的刻画,而非性能预期的描述.性能预期即要在特定功能行为基础上对"做得如何"形成预期,如完成特定行为功能的时间.IMC 中通过路径表示特定的行为功能,但路径中已引入了性能指标.本文将路径概率关联预期,并通过路径概率获取路径时间,形成对完成特定功能行为在时间特征上的预期,作为性能指标的度量标准.实现方法即通过对 IMC 模型中的状态进行标记,表示从该状态出发的可信执行路径.首先对路径进行描述,并在此基础上刻画性能预期.

在 IMC 模型中,执行路径以如下方式表述:

$$\sigma(k)=s_0\xrightarrow{l_0}s_1\xrightarrow{l_1}\cdots s_{k-1}\xrightarrow{l_{k-1}}s_k,$$

$$s_i\in S,l_i=(a_i,t_i)\in(Act\cup\{*\})\times\mathbb{R}_{\geqslant 0},i\in\mathbb{N}.$$

l_i 为一个二元组,第 1 个分量表示系统在状态转移中执行的动作(若发生马尔可夫转移,则该分量表示为 $*$),第 2 个分量表示系统在执行状态转移前所延迟的时间.对可信执行路径的标记需要在路径概率测度定义的基础上.首先,IMC 的路径概率 Pr 可归纳定义如下:

$$Pr(\sigma(0))=1;$$

$$Pr(\sigma(k+1))=\begin{cases}Pr(\sigma(k))\displaystyle\int_{t_k}R(s_k,s_{k+1})\mathrm{e}^{-E(s_k)t}\mathrm{d}t,\\ \quad(s_k,R(s_k,s_{k+1}),s_{k+1})\in\rightarrow;\\ Pr(\sigma(k)),\ (s_k,a_k,s_{k+1})\in\rightarrow;\end{cases}\tag{1}$$

其中 $k\geqslant 0$,$R(s_k,s_{k+1})$ 是状态 s_k 到 s_{k+1} 的转移率,$E(s_k)=\sum_{s'\in S}R(s_k,s')$ 为 s_k 上的总转移率.IMC 中既存在概率转移,又存在非确定性动作转移,IMC 路径上的概率是定义在将非确定性动作转移确定下来之后的模型上的.事实上,

$$\int_{t_k}R(s_k,s_{k+1})\mathrm{e}^{-E(s_k)t}\mathrm{d}t=\int_{t_k}\frac{R(s_k,s_{k+1})}{E(s_k)}E(s_k)\mathrm{e}^{-E(s_k)t}\mathrm{d}t.$$

$E(s_k)\mathrm{e}^{-E(s_k)t}$ 是系统在状态 s_k 上停留时间 t 的概率密度,而 $\dfrac{R(s_k,s_{k+1})}{E(s_k)}$ 是系统从状态 s_k 转移到 s_{k+1} 的概率,因此上式积分表示系统在时间 t_k 内从状态 s_k 转移到 s_{k+1} 的概率.

对路径所应满足性质的描述需要基于动作的时序逻辑,文献[18]对连续随机逻辑(CSL)修改得到的时序逻辑系统 aCSL 满足了这样的需求,其中的路径公式由以下语法产生:

$$\varphi::=\Phi_{1A}\mathcal{U}^{<t}\Phi_2\mid\Phi_{1A}\mathcal{U}_B^{<t}\Phi_2,\quad t\in\mathbb{R}_{>0},A,B\subseteq Act,\tag{2}$$

其中,Φ_i 为状态公式.式(2)的具体含义为:到达 Φ_2 之前,路径所经状态都满足 Φ_1,同时状态转移只能执行 A 中动作,此外,到达 Φ_2 所经过的时间不超过 t.第 2 个公式与前者的不同在于必须执行到达 Φ_2 的转移,且执行的动作在集合 B 中.文献[18]还

论证了 aCSL 路径公式可以表示标准的线性时间和分支时间时序逻辑中 $\mathcal{U}, X, F$ 和 G 算子含义. 现用 $Path(s)$ 表示从 s 出发的所有路径的全体集合,用 $\models$ 定义在 IMC 状态和路径上的满足关系,用 $Prob(s,\varphi)$ 表示 $Path(s)$ 中所有满足 φ 的路径的概率测度,则有

$$Prob(s,\varphi)=Pr\{\sigma\in Path(s)\mid\sigma\models\varphi\}. \quad (3)$$

将在 IMC 模型上通过增加状态标记的方式完善性能预期描述,由此得到的行为度量信息基称作基于 IMC 的行为度量信息基,下面给出定义:

定义 3. 一个基于 IMC 的行为度量信息基为 (imc,L),其中:

1) imc 是一个交互式马尔可夫链;

2) L 是一个标记函数,$L:S\mapsto(\varphi(t),p,<>)$,其中:

$\varphi(t)$ 是一个以时间 t 为参数的路径公式;

p 是指定的概率测度,则预期路径时间 t_e 满足 $Prob(s,\varphi(t_e))=p$,s 为所标记的状态,这里记 $T(s,\varphi(t),p)=t_e$;$<>\in\{<,>\}$,$<$表示 t_e 为预期时间上限,$>$表示 t_e 为预期时间下限.

通过标记中的概率 p 可获取预期路径时间 t_e,下面的定理进一步揭示两者关系:

定理 1. $Prob(s,\varphi(t))=$

1) 1;

1.1 若 $\varphi(t)$ 形如式(2)前者,且 $s\models\Phi_2$;

1.2 若 $\varphi(t)$ 形如式(2)后者,且 $s\models\Phi_1\wedge(\exists s',s'\models\Phi_2)\wedge B$ 中动作执行;

2) $\sum\limits_{s'\in S}\int_0^{tm}R(s,s')\mathrm{e}^{-E(s)x}Prob(s',\varphi(t-x))\mathrm{d}x$;

从 s 出发执行马尔可夫转移,且:

2.1 若从 s 出发不存在动作转移,$tm=t$;

2.2 若从 s 出发存在动作转移,$tm=t_{\min}$,$t_{\min}$ 为最早动作发生所经历延迟;

3) $Prob(s',\varphi(t-t_{\min}))$;

从 s 出发执行动作转移,且 $s\xrightarrow{(a,t_{\min})}s'$;

4) 0;其他情况.

证明. 对于 1)4),显然成立. 2)3)分别对应马尔可夫转移和动作转移.

对于 2),由式(1)中的解释,$R(s,s')\mathrm{e}^{-E(s)x}$ 表示在时间 x 内从状态 s 转移到 s' 的概率密度,$Prob(s',\varphi(t-x))$ 表示从 s' 出发满足路径 $\varphi(t-x)$ 的概率测度,则 $\int_0^{tm}R(s,s')\mathrm{e}^{-E(s)x}Prob(s',\varphi(t-x))\mathrm{d}x$ 表示在 tm 时间内从 s 经 s' 且满足路径 $\varphi(t)$ 的概率,故 $\sum\limits_{s'\in S}\int_0^{tm}R(s,s')\mathrm{e}^{-E(s)x}Prob(s',\varphi(t-x))\mathrm{d}x$ 即从 s 出发的所有满足 $\varphi(t)$ 的路径概率.

对于 3),由式(1)可得,动作转移以概率 1 通过到达状态 s',则有 $Prob(s,\varphi(t))=Prob(s',\varphi(t-t_{\min}))$. 证毕.

基于 IMC 的行为度量信息基实现了在统一的模型下正交化的功能和性能预期描述.

2.2 运行时证据获取

构成可信动态度量平台证据的基本要素是行为及其属性(对于本文,行为属性应包括行为发生时的时间). 本文对一个基本行为的刻画采用软件行为学[17]中的描述方式:

定义 4. 一个行为定义为主体使用函数(过程)对客体进行操作:

$$ACT=\{(s)\mathrm{APPLIES}(f)\ \mathrm{TO}\ (obj)\mid s\in Subjects, f\in Functions, obj\in Objects\},$$

其中 APPLIES TO 为施用,$Subjects$ 为主体集,$Functions$ 为函数集(过程、服务),$Objects$ 为客体集.

可信计算平台需要获取定义 4 描述的行为支撑要素(即主体、客体以及施用). 获取方式通过可信操作系统中的引用监视器实现,引用监视器通常在系统的可信计算基(TCB)中. 其抗篡改、不可旁路、足够小以便分析测试的特性满足了这里的需求. 根据基于 IMC 的行为度量信息基,作为行为属性的行为发生时间应与行为本身一并进行日志记录,同时将记录摘要扩展至可信平台模块(TPM)中指定的 PCR[2](platform configuration register). PCR 是 TPM 中用于存储度量结果的存储单元,只能被清零和扩展操作修改,扩展操作计算当前 PCR 值和一个 160 b 的摘要 n 串接后的 SHA1 值并写入该 PCR,即 $PCR[i]\leftarrow SHA1(PCR[i]\|n)$,这样即使恶意行为出现,也无法修改其自身的度量值,有效防止记录的恶意篡改.

2.3 可信性验证

可信性验证的核心是通过对获取的运行时证据与行为预期的比较给出行为可信性的断言. 本文中,通过提取证据中的行为 $A=a_1\cdot a_2\cdot\cdots\cdot a_m$($a_i\in Act, i\in\mathbb{N}_+$),以及作为行为属性的行为发生时间 $t(a_i)$,在给定的基于 IMC 的行为度量信息基 $BMIB=(imc,L)$(即行为预期)下对行为可信性进行判定,若 $TW(A,BMIB)=\mathrm{T}$,则 A 对行为度量信息基 $BMIB$ 是可信的. 本文假设对于系统运行时的每一个马尔可夫转移→,在证据中引入一个特殊的内部

动作集 Z 中的动作(例如对应到实际系统中的中断)作为后继,标识马尔可夫转移的结束,显然内部动作的发生不存在延迟.则由行为序列 A 可导出一个 IMC 路径 $\sigma=s_0\xrightarrow{l_1}s_1\xrightarrow{l_2}\cdots\xrightarrow{l_m}s_m$,若 $a_i\in Z$ $(i=1,2,\cdots,m)$,则 $l_i=(*,t(a_i)-t(a_{i-1}))$,否则 $l_i=(a_i,t(a_i)-t(a_{i-1}))$,(设 $t(a_0)=0$),以下称 σ 为由 A 导出的 IMC 路径.下面给出基于 IMC 模型的行为可信性定义:

定义 5. 设行为序列 $A=a_1\cdot a_2\cdot\cdots\cdot a_m(a_i\in Act,i\in\mathbb{N}_+)$,其导出的 IMC 路径为 $\sigma=r_0\xrightarrow{l_1}r_1\xrightarrow{l_2}\cdots\xrightarrow{l_m}r_m$,行为度量信息基 $BMIB=(imc,L)$,其中 $imc=(S,Act,\rightarrow,\rightarrow,s_0)$,若 $TW(A,BMIB)=\mathrm{T}$,当且仅当在 imc 中存在一条路径 $\sigma'=s_0\sim^1 s_{k1}\sim^2\cdots\sim^n s_{kn}$ $(k_i\in\mathbb{N}_+,(s_{k(i-1)},\sim^i,s_{ki})\in\{\rightarrow,\rightarrow\})$,满足 $m=n$,且对 $\forall i\in\{1,2,\cdots,m\}$,若 $l_i.a=*$,则 $(s_{k(i-1)},\sim^i,s_{ki})\in\rightarrow$,否则 $(s_{k(i-1)},\sim^i,s_{ki})\in\rightarrow$,且以下 2 个条件同时成立:

1) 对 $\forall i\in\{1,2,\cdots,m\}$,若 $l_i.a\neq*$,则 $l_i.a=\sim^i$;

2) 对 $\forall i\in\{1,2,\cdots,n\}$,若 $L(s_{ki})=(\varphi(t),p,<>)\neq\varnothing$,且 $\exists j\in\mathbb{N}_+,i<j\leqslant n$,使得路径 $\sigma_T=r_i\xrightarrow{l_{i+1}}\cdots\xrightarrow{l_j}r_j\models\varphi(\infty)$,则 $\sum_{k=i+1}^{j}l_k.t<>T(s_{ki},\varphi(t),p)$.

上述可信性定义中,1)为功能可信性验证,2)为性能可信性验证,即 imc 中存在一条由动作转移形成的路径,与由 A 导出的 IMC 路径 σ 中由动作转移形成的路径相等,且该路径中若存在一个子行为序列在功能上满足序列起点对应的状态中所标记的路径,则该路径的执行时间应满足所标记的在概率测度 p 下的时间预期.

在上述可信性定义下,定理 2 说明基于 IMC 的可信动态度量模型与统计模型(一定概率水平下异常事件的检测)的兼容.

定理 2. 设行为序列 $A=a_1\cdot a_2\cdot\cdots\cdot a_m(a_i\in Act,i\in\mathbb{N}_+)$,其导出的 IMC 路径为 $\sigma=r_0\xrightarrow{l_1}r_1\xrightarrow{l_2}\cdots\xrightarrow{l_m}r_m$,行为度量信息基 $BMIB=(imc,L)$,其中 $imc=(S,Act,\rightarrow,\rightarrow,s_0)$,若 $TW(A,BMIB)=\mathrm{T}$,则对 $\forall s\in S$,若 $\exists 0\leqslant i<j\leqslant m$,使 $\sigma'=r_i\xrightarrow{l_{i+1}}\cdots\xrightarrow{l_j}r_j$ 满足 $\sigma'\in Path(s),\sigma'\models\varphi(\infty)$,则:

1) 当 $L(s)=(\varphi(t),\alpha,>)$ 时,$Prob(s,\varphi(\sum_{k=i+1}^{j}l_k.t))>\alpha$;

2) 当 $L(s)=(\varphi(t),1-\alpha,<)$ 时,$1-Prob(s,\varphi(\sum_{k=i+1}^{j}l_k.t))>\alpha$.

证明. 对于1),由于 $TW(A,BMIB)=\mathrm{T}$,且 $\sigma'\in Path(s)$,$\sigma'\models\varphi(\infty)$,依据定义 5 有 $\sum_{k=i+1}^{j}l_k.t>T(s,\varphi(t),\alpha)$,设 $T(s,\varphi(t),\alpha)=t_e$,则有 $Prob(s,\varphi(t_e))=\alpha$,由于 $\sum_{k=i+1}^{j}l_k.t>t_e$,且 $\varphi(t)=\Phi_{1A}\mathcal{U}^{<t}\Phi_2\mid\Phi_{1A}\mathcal{U}_B^{<t}\Phi_2$,所以有 $Prob(s,\varphi(\sum_{k=i+1}^{j}l_k.t))>Prob(s,\varphi(t_e))=\alpha$.

类似地,对于2)可得 $1-Prob(s,\varphi(\sum_{k=i+1}^{j}l_k.t))>\alpha$.

证毕.

定理 2 说明对 aCSL 路径概率测度的标记可检测某一概率水平 α 下的非预期,同时文献[18]论证了 aCSL 路径公式 φ 可以表示标准的线性时间和分支时间时序逻辑中 $\mathcal{U},X,F$ 和 G 算子的含义,因此本文基于 IMC 的动态度量模型通过对状态进行标记可以检测由 $\mathcal{U},X,F$ 以及 G 算子表达能力范围内的非预期,有效兼容了统计模型下的异常检测方法.需要强调的是由于度量模型是基于 IMC 的,所以度量平台系统应该满足马尔可夫性.

3　度量方法

本节针对服务多用户的集群系统给出实例,说明基于 IMC 动态度量模型的度量方法如何通过功能特征指标度量和性能特征指标度量保障系统的可信运行.

系统由一个主节点和若干个计算节点构成,主节点接受服务申请,向计算节点分发任务,获取计算结果并向用户反馈,计算节点根据主节点的任务分配完成计算任务并向主节点返回结果.现设置 3 个计算节点,承担平均每分钟 1 个用户的服务请求,每个计算节点平均 0.2 min 可完成对 1 个用户的服务计算.下面按步骤说明基于 IMC 模型的度量方法.

1) 构建 IMC

设 λ 为每个用户服务请求到达的指数分布延迟参数,根据条件有 $\lambda=1$,μ 为完成一个服务计算的延迟参数,根据每个节点服务时延 0.2 min,有 $\mu=5$,G 为主节点接到服务请求,D 为主节点向计算节点分派任务$(D\in\tau)$,设 $D_i\in D(i=0,1,2)$ 表示当前任务分配时已有 i 个计算节点被占用.E 为主节点接到 1 个计算节点返回计算结果,R 为主节点将结果反馈于相应用户$(R\in\tau)$,IMC 模型如图 4 所示:

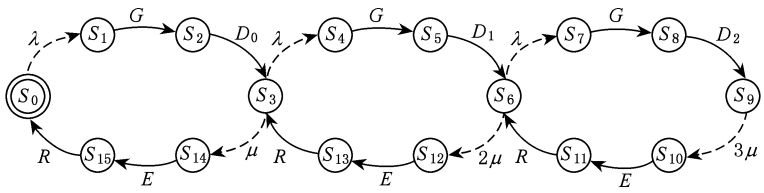

Fig. 4 IMC model of the instance.

图 4 实例的 IMC 模型

2) 构建基于 IMC 模型的行为度量信息基

构建基于 IMC 模型的行为度量信息基的主要工作是对 IMC 模型的状态进行 L 标记. 该系统在可靠性上要求从空闲态进入满负荷态前应能维持一段预期时间,即预期时间段内可保证用户得到即时的服务响应而不需要等待,故有基于 IMC 的行为度量信息基 $BMIB=(imc,L)$,其中 imc 为 1)中所建模型,标记函数 $L(S_0)=(\text{true}_{\overline{\{D_2\}}}\mathcal{U}^{\leqslant t}_{\{D_2\}}\text{true},0.1,>)$. 则 $Prob(S_0,\text{true}_{\overline{\{D_2\}}}\mathcal{U}^{\leqslant te}_{\{D_2\}}\text{true})=0.1$,根据定理 1,递归积分方程在 VC6.0 下通过数值方法求解,取积分区间 $h=0.01$,得到 $t_e=9.93$ min.

3) 运行时证据获取

在可信计算平台上获取如下 2 组运行时证据(为简化表达,$a(val)$ 表示 $t(a)=val$,单位为 min,$a\in Act$,同时,行为主体和客体明确,以下表述中略去):

① $A_1=z_1\cdot a_1\cdot z_2\cdot a_2\cdot z_3\cdot a_3$;

其中,$a_1=G(0.9)$,$a_2=G(2)$,$a_3=G(3.2)$,对 $\forall i\in\mathbb{N}_+$,$z_i\in Z$,且 $z_1(0.9)$,$z_2(2)$,$z_3(3.2)$.

② $A_2=z'_1\cdot b_1\cdot b_2\cdot z'_2\cdot b_3\cdot b_4\cdot z'_3\cdot b_5\cdot b_6\cdot z'_4\cdot b_7\cdot b_8\cdot z'_5\cdot b_9\cdot b_{10}\cdot z'_6\cdot b_{11}\cdot b_{12}\cdot z'_7\cdot b_{13}\cdot b_{14}\cdot z'_8\cdot b_{15}\cdot b_{16}\cdot z'_9\cdot b_{17}\cdot b_{18}\cdot z'_{10}\cdot b_{19}\cdot b_{20}\cdot z'_{11}\cdot b_{21}\cdot b_{22}\cdot z'_{12}\cdot b_{23}\cdot b_{24}\cdot z'_{13}\cdot b_{25}\cdot b_{26}$.

其中,$b_1=G(1.1)$,$b_2=D(1.1)$,$b_3=E(1.9)$,$b_4=R(1.9)$,$b_5=G(2)$,$b_6=D(2)$,$b_7=G(3.2)$,$b_8=D(3.2)$,$b_9=E(3.3)$,$b_{10}=R(3.3)$,$b_{11}=E(3.35)$,$b_{12}=R(3.35)$,$b_{13}=G(4.4)$,$b_{14}=D(4.4)$,$b_{15}=G(5.7)$,$b_{16}=D(5.7)$,$b_{17}=E(5.8)$,$b_{18}=R(5.8)$,$b_{19}=E(5.88)$,$b_{20}=R(5.88)$,$b_{21}=G(6.9)$,$b_{22}=D(6.9)$,$b_{23}=G(7.7)$,$b_{24}=D(7.7)$,$b_{25}=G(8.2)$,$b_{26}=D(8.2)$,对 $\forall i\in\mathbb{N}_+$,$z'_i\in Z$,且 $z'_1(1.1)$,$z'_2(1.9)$,$z'_3(2)$,$z'_4(3.2)$,$z'_5(3.3)$,$z'_6(3.35)$,$z'_7(4.4)$,$z'_8(5.7)$,$z'_9(5.8)$,$z'_{10}(5.88)$,$z'_{11}(6.9)$,$z'_{12}(7.7)$,$z'_{13}(8.2)$.

4) 可信性验证

① 功能特征指标验证

对于 A_1,其导出的 IMC 路径 $\sigma_1=r_0\xrightarrow{l_1}r_1\xrightarrow{l_2}\cdots\xrightarrow{l_6}r_6$,其中 $l_2=l_4=l_6=(G,0)$为动作转移,但在 imc 中,不存在 $\sigma'_1=S_0\sim^1S_{k1}\sim^2\cdots\sim^6S_{k6}$,满足 $\sim^2=\sim^4=\sim^6=G$,由定义 5 的 1),$TW(A_1,BMIB)=$F. 造成 A_1 未通过功能验证的原因在于主节点出现故障,即主节点收到服务请求后未分发计算任务.

对于 A_2,其导出的 IMC 路径 $\sigma_2=r_0\xrightarrow{l_1}r_1\xrightarrow{l_2}\cdots\xrightarrow{l_{39}}r_{39}$,其中对 $i\in I=\{2,3,5,6,8,9,11,12,14,15,17,18,20,21,23,24,26,27,29,30,32,33,35,36,38,39\}$,$l_i$ 为动作转移,在 imc 中,存在 $\sigma'_2=S_0\sim^1S_{k1}\sim^2\cdots\sim^{39}S_{k39}$,满足对 $\forall i\in I$,$\sim^i=l_i.a$,且对 $\forall i\in\{1,2,\cdots,39\}\backslash I$,$(S_{k(i-1)},\sim^i,S_{ki})\in\rightarrow$,由定义 5 中 1),$A_2$ 符合功能预期.

② 性能特征指标验证

对于 A_2,其导出的 IMC 路径中,对 $\forall i\in\{1,2,\cdots,39\}\backslash I$,$l_i$ 为马尔可夫转移,为清楚展现度量数据的性能特征,以表 1 方式显示度量值. 由于 $\sigma_2\models\varphi(\infty)$,但 $\sum_{k=1}^{39}l_k.t=8.2\text{ min}<t_e$,由定义 5 中 2),有 $TW(A_2,BMIB)=$F. 从表 1 节点 1 的服务时延可以看出,导致 A_2 未通过性能验证的原因是由于计算节点 1 的单任务服务时延显著超过了 0.2 min 的预期,造成了整个 IMC 路径的非预期.

Table 1 User Request and System Service Response

表 1 用户服务请求和系统服务提供情况

Time of Service Request/min	Time of Task Assignment/min	Service Delay/min	Number of Service Node	Covered States
1.1	1.1	0.8	1	S_3—S_0
2	2	1.3	1	S_3
3.2	3.2	0.15	2	S_6—S_3—S_0
4.4	4.4	1.4	1	S_3
5.7	5.7	0.18	2	S_6—S_3—S_0
6.9	6.9	1.4	1	S_3
7.7	7.7	0.53	2	S_6
8.2	8.2	0.2	3	S_9

本文度量方法在功能度量的同时实现了统一模型下的性能度量,对于 A_2 体现在性能指标上的非预期显然是文献[8-10]度量方法的盲点,但这种非预期又从根本上违背了行为可信性原则.所以本文的度量方法从功能、性能角度确保了系统行为的可预期,为可信计算平台的运行提供了有力支撑.

4 结　论

本文在理论上提出并论证了基于 IMC 的可信动态度量模型,并根据理论模型给出了实际的度量方法.在统一的模型下,有效实现了功能度量和性能度量的结合,且保持了结合的正交性,即两者的结合不会降低任何一方的度量效能,实现了在任一场景下对满足马尔可夫性的系统的可信动态度量,并给出了度量用例,该模型和方法能有效地对平台实施功能和性能的可信描述和度量,全面保障平台的可信运行.

参 考 文 献

[1] Trusted Computing Group. TPM Main, Part 1 Design Principles, Specification Version 1.2, Level 2 Revision 103 [EB/OL]. 2007. [2009-05-12]. https://www.trustedcomputinggroup.org/specs/TPM/mainP1DPrev103.zip

[2] Trusted Computing Group. TCG Specification Architecture Overview, Specification Revision 1.4.2 [EB/OL]. 2007. [2009-05-12]. https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf

[3] Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. Survey of information security [J]. Science in China: Series E, 2007, 37(2): 129-150 (in Chinese)
(沈昌祥,张焕国,冯登国,等. 信息安全综述[J]. 中国科学:E辑,2007,37(2):129-150)

[4] Sailer R, Zhang X, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture [C] //Proc of the 13th USENIX Security Symp. Berkeley, CA: USENIX, 2004: 223-238

[5] Jaeger T, Sailer R, Shankar U. PRIMA: Policy-reduced integrity measurement architecture [C] //Proc of the 11th ACM Symp on Access Control Models and Technologies. New York: ACM, 2006: 19-28

[6] Shi E, Perrig A, Doorn L V. BIND: A fine-grained attestation service for secure distributed systems [C] //Proc of the 2005 IEEE Symp on Security and Privacy. Washington DC: IEEE Computer Society, 2005: 154-168

[7] Li Xiaoyong, Zuo Xiaodong, Shen Changxiang. System behavior based trustworthiness attestation for computing platform [J]. Acta Electronica Sinica, 2007, 35(7): 1234-1239 (in Chinese)
(李晓勇,左晓栋,沈昌祥. 基于系统行为的计算平台可信证明[J]. 电子学报,2007,35(7):1234-1239)

[8] Peng Guojun, Pan Xuanchen, Fu Jianming, et al. Static extracting method of software indended behavior based on API functions invoking [J]. Wuhan University Journal of Natural Sciences, 2008, 13(5): 615-620

[9] Peng Guojun, Pan Xuanchen, Zhang Huanguo, et al. Dynamic trustiness authentication framework based on software behavior integrity [C] //Proc of the 9th Int Conf for Young Computer Scientists. Washington DC: IEEE Computer Society, 2008: 2283-2288

[10] Zhuang Lu, Cai Mian, Li Chen. Software behavior-based trusted dynamic measurement [J]. Journal of Wuhan University: Natural Science Edition, 2010, 56(2): 133-137 (in Chinese)
(庄琇,蔡勉,李晨. 基于软件行为的可信动态度量[J]. 武汉大学学报(理学版),2010,56(2):133-137)

[11] Denning D. An intrusion-detection model [J]. IEEE Trans on Software Engineering, 1987, 13(2): 222-232

[12] Lunt T, Jagannathan R. A prototype real-time intrusion-detection expert system [C] //Proc of the 1988 IEEE Symp on Security and Privacy. Washington DC: IEEE Computer Society, 1988: 2-10

[13] Smaha S. Haystack: An intrusion detection system [C] //Proc of the 4th Aerospace Computer Security Applications Conf. Austin, Texas: Tracor Applied Science Inc, 1988: 37-44

[14] Shen Changxiang, Zhang Huanguo, Wang Huaimin, et al. Research on trusted computing and its development [J]. Science in China: Information Sciences, 2010, 40(2): 139-166 (in Chinese)
(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] Hermanns H. Interactive marcov chains [D]. Erlangen & Nuremberg: Universität Erlangen-Nürnberg, 1998

[16] Tretmans J. Conformance testing with labelled transition systems: Implementation relations and testing generation [J]. Computer Networks and ISDN Systems, 1996, 29(1): 49-79

[17] Qu Yanwen. Software Behavior [M]. Beijing: Publishing House of Electronics Industry, 2004 (in Chinese)
(屈延文. 软件行为学[M]. 北京:电子工业出版社,2004)

[18] Wu Jinzhao, Wang Yongxiang, Qin Guangping. Interactive Markov Chains—Design, Verification and Evaluation of Concurrent Systems [M]. Beijing: Science Press, 2007 (in Chinese)
(吴尽昭,王永祥,覃广平. 交互式马尔可夫链——并发系统的设计、验证与评价[M]. 北京:科学出版社,2007)

Zhuang Lu, born in 1983. PhD candidate in Beijing University of Technology. His current research interests include information security and trusted computing (zhuanglu686@yahoo.com.cn)

Cai Mian, born in 1960. PhD. Professor of Beijing University of Technology. Her current research interests include information security and trusted computing (caim@bjut.edu.cn)

Shen Changxiang, born in 1940. Academician of Chinese Academy of Engineering. PhD supervisor of Beijing University of Technology. His research interests include computer information system, cryptography, information security architecture, system software security (secure operating systems and databases, etc.) and network security.

科学出版社期刊出版中心招聘启事

科学出版社期刊出版中心是专业化科技期刊出版服务机构,致力于打造中国科技期刊的集团军,做大做强科技期刊产业.现因业务发展需要,招聘以下岗位:

一、编辑人员 5 人,其中:

1.出版管理编辑 1 人;

2.医学专业编辑 3 人(医学中文编辑 2 人、医学英文编辑 1 人);

3. 工程技术专业编辑 1 人;

职位要求:

(1)硕士及以上学历,理工科或医学相关专业,年龄 35 岁以下;

(2)熟悉科技出版工作,有期刊工作经验者优先,在国内外专业刊物上发表过文章者优先;

(3)较好的语言、文字写作与审鉴能力,较强的沟通、组织协调及执行力;

(4)电脑操作熟练,工作认真,积极向上,具备较好的团队合作精神.

二、期刊业务拓展人员 2 人

职位要求:

(1)硕士及以上学历,具有专业学科背景,如地球科学、技术科学、生命科学等,年龄 35 岁以下;

(2)具有出版行业 3 年以上相关经历;熟悉期刊出版流程;

(3)较好的语言、文字表达能力,较强的公关、组织协调及执行力;

(4)电脑操作熟练,工作态度认真,思维活跃,具备团队合作精神.

三、计算机技术人员 1 人

职位要求:

(1)大学本科及以上学历,计算机与网络技术等相关专业,年龄 35 岁以下;

(2)有 2 年以上相关的计算机与网络技术工作经验;熟悉期刊出版流程和数字出版流程者优先;

(3)良好团队合作精神,时间观念强、讲求效率,对待工作认真负责.

应聘者请将简历发至 zhuwei@mail.sciencep.com,邮件主题请注明:"本人姓名+应聘职位".