基于任务链的实时多任务软件可靠性建模

雷 航

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出了以实时多任务系统中的任务链为组件，任务链运行时间比例作为组件的权重系数，建立实时多任务软件的可靠性建模方法。该方法符合实时多任务系统应用软件运行的实时情况，拓展了实时系统可靠性建模的思路，其可靠性模型可以给出单个任务链的可靠性参数，且建模方法还可以根据不同任务链的重要程度，进行可靠性分配并决定软件测试和投放时间。

关 键 词 实时系统; 多任务; 任务链; 可靠性模型

中图分类号 TP311.1 文献标识码 A

Reliability Modeling for Real-Time Multi-Task Software Based on Lansaction

Lei Hang

(School of Computer Science and Enginering, UEST of China Chengdu 610054)

Abstract Taking lansaction as component in real-time multi-task system, and executeing time rate as the quotiety of lansaction, the paper present a method of reliability modeling based on lansaction for real-time multi-task software. The method tally with the actual situation of programm executing of real-time multi-task. The model can submit evaluation results of single lansaction, so, the reliability modeling is convenient for reliability assigning and determine test time according to importance of the lansaction.

Key words real-time system; multitasking; lansaction; reliability modeling

软件系统对整个计算机系统可靠性的影响已十分突出，故软件可靠性评价已受到广泛重视。 国内外已提出100多种软件可靠性评价模型，其中以J-M模型、G-O模型、Musa执行时间模型、L-V模型和Seeding模型等为典型代表。但因没有建立起成熟的软件可靠性理论，故对各种不同模型的优劣评价存在很大争议，仅有一点已达成共识，即可靠性模型中所需参数要易于分析和测试，否则即使模型在理论上作得十分完善，而所需参数不易得到即失去现实意义。另外，实时多任务系统是一种模块化程度很高的软件系统，B.Littlewood在70年代末期提出了按结构化、模块化的方式进行软件可靠性建模[1]，该模型在理论上比较严谨，但十分复杂，对于非多任务实时系统，其模块之间的转换方式和转换概率也很难确定，而当时实时多任务系统还没有发展起来，使这一建模思想未能得到充分发展。对于实时多任务系统，任务和任务链由外部事件和时钟触发，任务间的转换方式和转换概率相对较容易确定。

1 实时多任务链的引入

对于实时多任务软件，文献[2]提出了按任务模块进行可靠性建模，并按运行时间比例对可靠性进行加

收稿日期：2003 – 05 – 20
基金项目：国防科工委“十五”预研基金资助项目
作者简介：雷 航(1961 –)，男，博士，副教授，主要从事嵌入式实时系统可靠性测试及评价，系统性能分析和实时软件工程方面的研究.

权处理，假设任务间相互独立，但在实际系统中，任务间往往相互关联。完成一个系统响应过程是由单个任务或多个有数据传递关系的任务构成的任务链来完成，单个任务完成系统响应过程的情况非常简单，在一个实际系统中也较为少见，本文讨论任务链的情况。按照任务链中有无公共任务，可将系统任务链的构成分为以下两种情况：

1) 如果系统中的任何一个任务只属于某一个任务链，各个不同的任务链之间无共同任务，链之间没有联系，对任务链i(标识为L_i)，假设该任务链上有k_i个任务，则分别表示为$L_i(1), L_i(2),\cdots, L_i(k_i)$，则系统结构如图1所示。从图中可以看出，对任意一条任务链，都是一个串联结构。如果各任务的可靠度分别为$R_i(t)$，则一条任务链可靠度为$R(t)=\prod_{i=1}^{k_i} R_i(t)$。

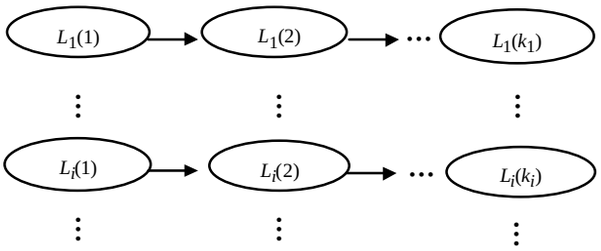

图1　无公共任务的系统结构

2) 如果系统中某些任务属于多个链(≥2)，即至少存在两个链，这两个链之间有公共任务，因此，任务链之间存在联系和制约。假设两条链L_i和L_j有公共任务，其中$L(g1)$、$L(g2)$和$L(g3)$是三个公共任务，其结构如图2所示。图中，链L_i的执行路径是$L_i(1)\rightarrow L(g1)\rightarrow L(g2)\rightarrow L_i(2)\rightarrow L(g3)\rightarrow L_i(3)$，链$L_j$的执行路径是$L_j(1)\rightarrow L(g1)\rightarrow L(g2)\rightarrow L_j(2)\rightarrow L(g3)\rightarrow L_j(3)$。

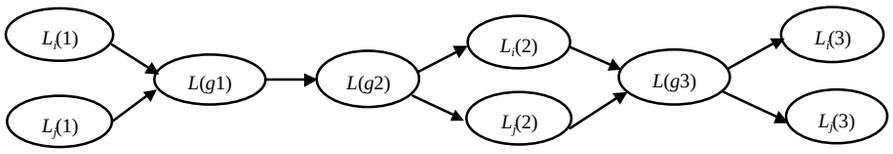

图 2　有公共任务的系统结构

由于两条执行路径的执行是由于不同的外部事件或时钟来驱动，不同任务链不可能同时启动，即使多个外部事件同时产生，按照基于优先级的任务调度方式，或相同优先级按时间片调度，不同的任务链也是串行执行。因此，也可以将有公共任务的系统结构的执行过程转换成类似串联系统结构，如图3所示。

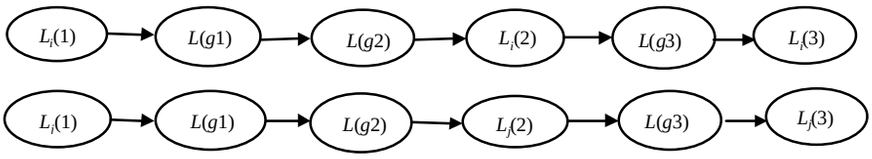

图 3　具有公共任务的任务链等价结构

从图3可知，可将实时系统对外部事件(或时钟)的响应过程看成是若干任务链的执行过程。需要说明的是，图3中任务链的形式上仅类似于串并联结构，但由于该结构并非容错系统结构，因此其可靠性分析还不能按传统串并联系统的可靠性分析方法来进行。

在实时多任务系统中，特别是嵌入式多任务实时系统，以任务模块作为基本的评价单元较合理。在嵌入式系统中，软件测试环境与实际运行环境具有不一致性[2]，同时，多任务执行时，不同任务占有系统的时间具有不平等性。前者说明了如果在模型中不考虑任务的实际运行时间占系统总运行时间的比例，会造成在软件投放后对其进行的可靠性估计有较大的误差；后者则说明了不同任务(模块)对软件系统可靠性的影响可能会有很大差异。另外，由于各个任务的重要性不同，因此需要区别对待各个任务模块，以便对各个任务模块分别进行可靠性分配和可靠性评价。

由于不同任务链是由不同的外部事件(或时钟)来驱动，因驱动频率可能有很大的差异，因此不同任务链

执行的频率不同，并且不同任务链的执行时间也不同，使得不同任务对系统可靠性的影响也会有较大差异，因此需要分析不同任务链被驱动的概率和执行时间，利用该概率(该概率值也决定了不同执行路径占系统运行时间的比例)对模型进行加权处理。

2 用于可靠性建模的任务链参数

任务链的执行频率取决于外部事件的频率或驱动任务链所用时钟的频率。前者一般为非周期性，后者为周期性。对于由时钟驱动的任务链，其执行频率是该时钟的频率，而由事件驱动任务链的执行频率则取决于系统的调度方式。由事件驱动的任务的调度方式通常有以下两种：1) 系统设计时，指定事件对应任务(或任务链)的优先级，一旦某一事件到达系统，如果该事件所对应的任务(或任务链)的优先级高于当前任务的优先级，则剥夺当前任务的运行，其优点是能够尽可能地满足高优先级任务的运行，但由于事件的随机性，使系统的时间确定性较差；2) 安排一个周期任务(由时间驱动)来处理外部事件，即周期性地处理非周期事件，优点是时间确定性较好，但可能会出现高优先级任务的响应时间得不到满足。对于采用哪一种方式，由系统设计者根据系统的特性(如实时性要求、吞吐量要求等)来决定。

在进行时间特性分析时，如果按第2)种方式，则可将整个系统中的任务都看作是周期性任务；如果按第1)种方式，则根据随机过程理论，任务的到达服从参数为l的泊松分布，取平均周期$T=1/l$，则可以同样按照周期任务时间分析的方法分析，由此可将周期任务和非周期任务的执行时间分析统一起来。假设系统中共有N个任务链；第i条链上的j个任务标识为T_{ij}；触发各任务链的事件的周期分别为d_1，d_2，…，d_N；第1条任务链上有k_1个任务，即$L_1(1)$，$L_1(2)$，…，$L_1(k_1)$；第2条任务链上有k_2个任务，即$L_2(1)$，$L_2(2)$，…，$L_2(k_2)$，…；第N条任务链上有k_N个任务，即$L_N(1)$，$L_N(2)$，…，$L_N(k_N)$；第i条任务链上的第j个任务的运行时间为C_{ij}；任务链L_i的运行时间为F_i；任务链L_i运行时间占系统运行时间的比例为P_i；任务模块的可靠性为$R_{ij}(t)$。

在实际的系统中，任务链的运行时间应该包括各任务的运行时间，以及调度这些任务所需要的系统时间开销，但系统运行时间开销属于系统软件开销，与这里所讨论的应用任务的可靠性无关，所以在计算任务链运行时间时，采用任务链L_i的运行时间为各个任务运行时间之和，即$F_i=\sum_{j=1}^{K_i} C_{ij}$。

再考虑任务链的运行时间占系统运行时间的比例，影响任务运行时间的主要因素有任务链的周期、计算时间、中断响应时间、任务调度时间、关调度或priority ceiling协议以及任务同步引起的任务等待时间等，但上述因素仅推迟了任务的运行，并不影响任务运行时间比例。

根据文献[3]提出的对多任务系统单个任务的时间性能分析方法，本文将该方法扩展到任务链，从时刻0～t，任务链L_i占系统运行时间比例为

$$P_i=\frac{\left(\frac{t}{d_i}F_i\right)}{t}=\frac{F_i}{d_i}=\sum_{j=1}^{K_i}\frac{C_{ij}}{d_i}$$

3 基于任务链的可靠性模型

按照G-O NHPP模型[4]，结合前面的说明，假设每一故障的暴露率(被检测的概率)均等，其值为b_{ij}到任一时刻t，发生的累计故障数$N_{ij}(t)$服从均值为$m_{ij}(t)$的Poisson分布，均值$m_{ij}(t)$使得很小时间段(t，$t+\Delta t$)内，任务模块发生故障的次数与t时刻模块中残留的故障数成正比；$m_{ij}(t)$是一个有界的非减函数，且$m_{ij}(0)=0$，$m_{ij}(\infty)=a_{ij}$，a_{ij}表示当$t\to\infty$时在任务模块T_i中查出的期望故障数。

任务模块的故障强度函数为

$$l_{ij}(t)=\frac{b_{ij}(a_{ij}-m_{ij}(t))\Delta t}{\Delta t}=b_{ij}(a_{ij}-m_{ij}(t))=a_{ij}b_{ij}\,\mathrm{e}^{-b_{ij}t}$$

用极大似然函数模型可以计算出参数a_{ij}和b_{ij}，并由此得到任务模块的故障强度函数$l_{ij}(t)$。

在不考虑运行时间比例的情况下，任务链L_i的总故障强度函数为$\sum_{j=1}^{K_i} l_{ij}(t)$。当引入任务链运行时间比例，

将该比例对任务链故障强度函数加权，则任务链L_i的总故障强度函数为

$$l_{sumi}(t)=P_i\sum_{j=1}^{K_i}l_{ij}(t)=\sum_{j=1}^{K_i}C_{ij}/d_i\sum_{j=1}^{K_i}l_{ij}(t)$$

根据故障强度函数与可靠性之间的关系，可得任务链L_i的可靠性为

$$R_i(t)=\prod_{j=1}^{K_i}\exp\{-P_i\int_0^t l_{ij}(t)\mathrm{d}t\}=\exp\{\int_0^t -l_{sumi}(t)\mathrm{d}t\}$$

式中　$R_i(t)$仅是一条任务链的可靠性，而系统中由多条任务链构成，对整个多任务应用系统的可靠性而言，与传统串并系统可靠性分析不同的是，在串并系统中多条链并行，只要有一条链能够工作，系统即可正常工作，但在实时多系统运行过程中，多条链是分时工作，任何一条任务链发生故障，则视为软件系统故障。在时间$[0,t]$内，除了系统时间开销和系统空闲时间，就有一条任务链处于运行状态,并且各任务链之间相互独立，因此，对于由多条链构成的实时多任务链，其可靠性可以采用求均值的方式进行，即

$$R_{sys}=(\sum_{i=1}^{N}R_i(t))/N=\sum_{i=1}^{N}\exp\{\int_0^t -l_{sumi}(t)\mathrm{d}t\}/N$$

在系统可靠性R_{sys}的计算函数中，直接采用求均值的方法，而没有再考虑任务链的运行时间比例权值，这只因为在$l_{sumi}(t)$函数中，已经引入了时间比例P_i。假设有三个任务链，其可靠性分别是R_1=0.98，R_2=0.97 R_3=0.95，则应用任务系统的可靠性R_{sys}=(0.98+0.97+0.95)/3=0.966。如果系统中各任务链可靠性相等$R_1=R_2=\cdots R_N=R$，则$R_{sys}=R$，即任何一条任务链处于运行状态，应用软件系统的可靠性均为R。

4　模型合理性说明

在实时多任务系统的运行过程中，在时间$[0,t]$内，整个系统的时间开销主要包括以下三部分：1) 应用任务运行所占用的时间(用t_A表示)；2) 系统任务运行的时间(如操作进行的系统资源管理、中断处理等，用t_S表示)；3) 系统空闲时间，即在一个时间段Δt内，没有任务链被触发，则时间Δt为系统空闲时间(用t_I表示)，所以$\sum_{i=1}^{N}P_i<1$。由于本模型针对多任务应用软件，因此假设在系统任务运行的时间段和系统空闲时间段内，其可靠性为1，这意味着在时间段t_S+t_I内，软件系统不发生故障，只有在时间t_A内，软件系统才可能发生故障。如果按照日常时钟时间，而不考虑任务链的运行时间占整个系统运行时间的比例，则估计的可靠性会低于系统运行时实际的可靠性。

按照任务链建立可靠性评价模型，符合实时多任务系统的实际运行过程，还可以根据不同任务链的重要程度进行可靠性分配并决定测试和投放时间，这对于系统中存在完成重要事件处理的关键路径非常重要。

参　考　文　献

[1] Littlewood. Software reliability model for modular program structure[J]. IEEE Trans.on Reliability, 1979, R-28(3): 241-246

[2] 雷　航, 熊光泽, 刘锦德. 一种多任务实时软件可靠性模型[J]. 应用科学学报, 1998, VOL-16(1): 1-6

[3] Michael G H, Mark H K, John P L. Timing analysis for fixed-priority scheduling of hard real-tinme system[J]. IEEE Trans on Softw.Eng. 1994, SE-20(1): 13-28

[4] Goel A L, Okumoto K Time dependent error detection rate model for software reliability and other performance measures[J]. IEEE Trans. Reliability, 1979, 28(3): 206-211

编　辑　徐培红