面向信息系统的生存性恢复机制

夏秦，王志文，邹华峰，冯博琴
（西安交通大学电子与信息工程学院，710049，西安）

摘要：为了克服现有信息系统生存性恢复手段单一、执行顺序固化以及恢复过程缓慢等不足，提出了一种以功能部件作为基本修复单位的生存性恢复机制.该机制根据关键功能部件的失效程度将信息系统提供的服务区分成完整服务、可接受服务以及中断服务3种类型，并以功能部件的可用性定义服务和信息系统的生存性.根据失效功能部件对服务的影响程度将恢复过程分为2个阶段，先通过修复关键功能部件恢复中断服务，然后再通过修复非关键功能部件完善可接受服务.应用新的恢复机制对一个网络教学系统进行生存性恢复实验，结果表明该机制能够依据信息系统的生存性态势确定恢复行为和执行顺序，与串行恢复机制相比，恢复行为的执行次数由9减少到3.

关键词：信息系统；生存性；恢复；服务
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2010)04-0018-05

A Recovery Mechanism of Survivability for Information System

XIA Qin, WANG Zhiwen, ZOU Huafeng, FENG Boqin
(School of Electronics and Information Engineering, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: A recovery mechanism of survivability with components being basic fixed units is presented for information systems to overcome the deficiencies appeared in existing approaches on survivability recovery, such as undiversified method, solidified executing sequence and delayed recovery process. Services provided by a information system are classified into complete services, acceptable services and interrupted services according to the disabled extent of critical components, and the survivability models of services and the information system are built separately with availability of components. According to the affecting degree of disabled components on services, the recovery procedure is divided into two phases, recovering interrupted services by repairing critical components and improving acceptable services by repairing non-critical components. A survivability recovery experiment in a network teaching system shows that the proposed mechanism can determine the recovering actions and executing sequences depending on the survivability state of information systems. A comparison with the mechanism using serial recovery actions shows that the number of actions performed by the proposed mechanism is reduced from 9 to 3.

Keywords: information system; survivability; recovery; service

信息系统生存性恢复是当前研究可信系统所面临的一项富有挑战性的任务，其目标在于当系统遭受攻击、软硬件故障等事故时，仍然能够及时向用户提供基本服务[1].目前针对生存性恢复方面开展的研究工作可以分为两类，一类采用服务迁移技术[2-5]，另一类采用软件抗衰技术[6].前者只能使用确定性冗余资源，启动时序固化，后者主要使用微重启技术，手段单一.因此，本文根据功能部件的可用性将服务分为完整服务、可接受服务以及中断服务3种类型，通过恢复中断服务和完善可接受服务2

收稿日期：2009-10-20. 作者简介：夏秦(1973—)，女，讲师，博士生. 基金项目：国家自然科学基金资助项目(60970121)；国家科技人员服务企业行动计划资助项目(2009GJG00025)；西安交通大学科研基金.

个过程,实现了信息系统生存性恢复的多样化,实验表明该机制能够有效地提高信息系统的生存性.

1　信息系统生存性模型

1.1　信息系统服务类型

在一个信息系统中,系统、服务与功能部件之间存在着固有的依赖关系,即系统依赖于多种服务构成,而每个服务又依赖于不同的功能部件组合,其中功能部件是信息系统中实现特定功效的原子模块,在运行中只能处于正常或失效状态. 由于功能部件处于依赖关系的最低环节,因此其失效将直接影响到相关服务的质量,进而波及到系统的生存性. 不过,各功能部件的失效对相关服务的影响程度不同,有的只是降低服务的质量,而有的则会导致服务中断.

根据服务依赖的功能部件的运行状况,可以将服务划分成 3 种类型,而关联这些不同类型服务的核心则是关键功能部件(服务所必需的功能部件).

(1)完整服务:给定一个服务,若其依赖的功能部件都能正常运行则称该服务是完整的.

(2)可接受服务:给定一个服务,若其依赖的全部关键功能部件都能正常运行,则称该服务是可接受的,而完整服务就是可接受服务的一种特殊形式.

(3)中断服务:给定一个服务,若其依赖的功能部件存在关键功能部件失效,则称该服务是中断的.

1.2　信息系统定义

对信息系统 I,定义

$$I=(S,C,F,R,\Omega,\Psi,\Lambda,\Gamma) \tag{1}$$

式中:S 是信息系统向外提供的完整服务集;C 是支撑信息系统运行的功能部件集;F 是引发信息系统功能部件失效的故障事件集;R 是信息系统功能部件失效时所对应的恢复行为集;Ω 是服务重要性映射函数,反映信息系统对于各服务的依赖程度

$$\alpha_i=\Omega(s_i),s_i\in S,\ \alpha_i\in(0,1)\ \wedge\ \sum_{i=1}^{|S|}\alpha_i=1 \tag{2}$$

其中 α_i 由信息系统管理员确定,s_i 服务在整个信息系统中越重要,则 α_i 的取值越接近 1,否则越接近 0;Ψ 是服务规范函数,反映系统在提供一个完整形式服务时需要使用的功能部件集合

$$C_i=\Psi(s_i),\ s_i\in S,\ C_i\subset C \tag{3}$$

若将一个完整服务所要求的关键功能部件表示为 $C_{i,C}$,则由 Ψ 可知,$C_{i,C}\subseteq C_i$,根据可接受服务和中断服务的定义可知它们分别满足条件 $\forall c_j\in C_{i,C}\rightarrow c_j\in C_{i,A}$($C_{i,A}$ 表示可接受服务对应的功能部件集合)和 $\exists c_j\in C_{i,C}\wedge c_j\notin C_{i,I}$($C_{i,I}$ 表示中断服务对应的功能部件集合)的约束;Λ 是功能部件对服务支撑的重要性映射函数,反映一个服务对各功能部件的依赖程度

$$\beta_{j,i}=\Lambda(c_j,s_i),c_j\in C,\ s_i\in S,\ \beta_{j,i}\in[0,+\infty) \tag{4}$$

其中 $\beta_{j,i}$ 由信息系统管理员确定,当 $c_j\notin C_i$ 时,$\beta_{j,i}=0$;当 $c_j\in C_{i,C}$ 时,$\beta_{j,i}=+\infty$;Γ 是恢复行为映射函数,反映了信息系统在故障事件下各失效功能部件对应的各种可能修复行为

$$\lambda_{j,k}=\Gamma(c_j,f_k),c_j\in C,\ f_k\in F,\ \lambda_{j,k}\subset R \tag{5}$$

若 $\lambda_{j,k}=\varnothing$,则故障事件 f_k 对功能部件 c_j 无影响.

1.3　信息系统生存性度量

信息系统在任何时刻总是处于某种运行状态,在该状态下,支撑信息系统的众多功能部件将呈现不同的功能特征,有的继续处于正常工作状态,能够实现信息系统要求的功能,而有的则可能因各种故障事件而导致功能失效,无法满足原来的功能需求. 另外,由于信息系统向外提供的服务对于内部的支撑功能部件有着不同的依赖关系,使得一个功能部件的失效对不同的服务产生不同的效果:有的服务不受影响,继续以完整形式提供;有的服务没有受到致命影响,能够以可接受形式继续提供;那些以该失效功能部件作为关键的服务则无法继续提供.

根据功能部件对服务的影响程度以及信息系统当前的运行状态,将服务 s_i 的生存性量化为

$$\eta_i=\begin{cases}\dfrac{\sum_{j=1}^{|C_{i,A}|}\beta_{j,i}\ \Big|\ c_j\in C_{i,A}\ \wedge\ c_j\notin C_{i,C}}{\sum_{j=1}^{|C_i|}\beta_{j,i}\ \Big|\ c_j\in C_i\ \wedge\ c_j\notin C_{i,C}} \\ 0,\ \exists c_j\rightarrow c_j\in C_{i,C}\ \wedge\ c_j\notin C_{i,A}\end{cases}$$
$$\eta_i\in[0,1] \tag{6}$$

根据信息系统模型可知,一个信息系统的生存性可表示为

$$\eta=\sum_{i=1}^{|S|}(\alpha_i\times\eta_i),\ \eta\in[0,1] \tag{7}$$

2　生存性恢复

信息系统生存性量化计算仅仅是生存性恢复的第一步,计算结果只是反映了信息系统在当前运行状态下的一种生存性态势. 当信息系统发生故障时,一些功能部件会失效,导致与之相关的服务中断,严重降低了系统的生存性. 为此,必须在故障事件产生

后尽快修复失效的功能部件，进而恢复中断的服务以改善系统的生存性，图1描述了信息系统服务的状态变化过程，图中标注的各状态迁移主要是受功能部件工作状态所决定，而功能部件的工作状态又依赖于故障事件是否产生以及相应的恢复行为是否启用这2个前提.

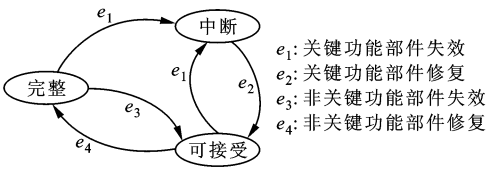

图1 信息系统服务状态迁移

实际上，故障事件的产生具有很强的随机性，且单个故障事件经常会导致多个功能部件失效，同时每个失效功能部件又对应着多种恢复行为，这将导致信息系统的生存性恢复存在着多种选择. 因此，选择合适的修复行为及其执行顺序对于服务修复以及整个系统的生存性提升都有着重要影响.

为了更快、更有效地提升信息系统的生存性，将生存性恢复分为2个阶段，即恢复中断服务和完善可接受服务. 前者是通过对关键功能部件的修复以便能够快速恢复中断服务，而后者则是通过对非关键功能部件的修复以便能够完善可接受服务，使之趋于完整.

2.1 恢复中断服务

服务中断是由于服务所依赖的关键功能部件发生失效而导致服务无法继续使用，不仅对系统的服务提供造成巨大的负面影响，而且导致信息系统的生存性急剧下降. 鉴于此，恢复中断服务首要关注的就是实时性，需要在最短的时间内做出恢复决策并启动相应的恢复行为. 针对该需求，本文提出了专门的恢复控制策略：首先是优先恢复失效的共享功能部件，即那些同时充当多个服务的关键功能部件，它的失效直接导致多个服务中断，对信息系统的生存性影响更为严重；其次是在选取恢复行为时尽量减少执行系统生存性的计算次数，以便将修复时间降至最低. 基于上述策略，中断服务恢复过程包括如下5个步骤.

(1)当信息系统发生故障事件 f_k 时，构建失效的关键功能部件集 ε 和初始化恢复行为集 λ_E

$$\varepsilon_k := \{c_j \mid \exists \beta_{j,i} = +\infty \wedge \lambda_{j,k} \neq \varnothing, j = 1,2,\cdots, |C_i|, i = 1,2,\cdots, |S|\}$$
$$\lambda_E := \varnothing \tag{8}$$

(2)构建所有失效关键功能部件对应的恢复行为集

$$R_C := \bigcup_{i=1}^{|S|} R_{i,C},\ i = 1,2,\cdots, |S| \tag{9}$$

式中：$R_{i,C} = \{\lambda_{j,k} \mid c_j \in \varepsilon_k,\ j = 1,2,\cdots, |C_i|\}$ 表示服务 s_i 失效时，关键功能部件对应的恢复行为子集. 若 $R_C = \varnothing$ 则结束当前阶段修复过程，否则对集合中任一恢复行为统计其在子集 $R_{i,C}$ 中出现的频次，将频次最高的恢复行为合并成集 R_f.

(3)若 $|R_f| = 1$，则启用其中唯一的恢复行为；否则，对 R_f 中的每个恢复行为 r_m 估算与之对应的系统生存性 η_m，并启用能获得最大生存性的恢复行为，设被启用的恢复行为标记为 r，更新被启用的恢复行为集 $\lambda_E := \lambda_E + \{r\}$.

(4)构建恢复行为 r 修复的关键功能部件集

$$P_k := \{c_j \mid c_j \in \varepsilon_k \wedge r \in \lambda_{j,k}\} \tag{10}$$

(5)更新失效的关键功能部件集 $\varepsilon_k := \varepsilon_k - P_k$，若 $\varepsilon_k = \varnothing$ 则结束当前阶段修复过程，否则转向步骤(2).

2.2 完善可接受服务

故障事件除了导致信息系统服务的关键功能部件失效之外，也会导致非关键功能部件的失效. 根据图1所示的服务状态迁移可以发现，关键功能部件的修复可以将中断服务转变为可接受服务，使之能够继续使用，但这些可接受服务仍然存在失效的功能部件，为了能够对外提供更加优良的服务，进一步提升信息系统的生存性，需要对剩余的失效功能部件进行修复.

由于可接受服务已经是可以使用的服务，此时对失效功能部件的修复实际上就是对可接受服务的完善，在实时性需求上没有恢复中断服务那么强烈. 另外，某些非关键功能部件对应的恢复行为可能与关键功能部件对应的修复行为存在重叠，这使得在恢复中断服务的同时已经修复了部分失效的非关键功能部件. 因此，该阶段的生存性恢复控制策略变得相对简单，具体流程如下.

(1)当信息系统发生故障事件 f_k 时，构建失效的非关键功能部件集

$$\bar{\varepsilon}_k := \{c_j \mid \exists \beta_{j,i} \in (0, +\infty) \wedge \lambda_{j,k} \neq \varnothing \wedge \lambda_{j,k} \notin \lambda_E, i = 1,2,\cdots, |S|\} \tag{11}$$

(2)构建所有失效非关键功能部件对应的恢复行为集

$$\bar{R}_C := \bigcup_{i=1}^{|S|} \bigcup_{j=1}^{|s_i|} \lambda_{j,k} \wedge c_j \in \bar{\varepsilon}_k \tag{12}$$

(3)对于集合$\overline{R}_C$中的每个恢复行为，估算系统的生存性，并启用能获得最大生存性的恢复行为$\tilde{r}$.

(4)构建恢复行为$\tilde{r}$修复的非关键功能部件集

$$\overline{P}_k := \{c_j \mid c_j \in \bar{\varepsilon}_k \wedge r \in \lambda_{j,k}\} \quad (13)$$

(5)更新失效的非关键功能部件集$\bar{\varepsilon}_k := \bar{\varepsilon}_k - \overline{P}_k$.

(6)重复步骤(2)～步骤(5)，直到$\overline{P}_k = \varnothing$或$\overline{R}_k = \varnothing$为止.

3　实验测试

为了更好地描述和说明信息系统生存性恢复机制，本文选择了网络教学系统这一实际应用来详细说明信息系统生存性的恢复过程.

3.1　教学系统配置

图 2 描述了某学校网络教学系统的网络结构，该系统通过互联网为师生提供远程教学、学习以及管理等服务. 教学系统的客户通过多种 Internet 访问方式连接到系统服务端，服务器采用保护主机的防火墙部署方式，使得服务资源能够得到有效的安全保护. 教学系统服务的基本工作流程是：远端客户首先经过身份认证，然后执行对应的应用功能，并根据服务需求进行业务数据库服务器的访问.

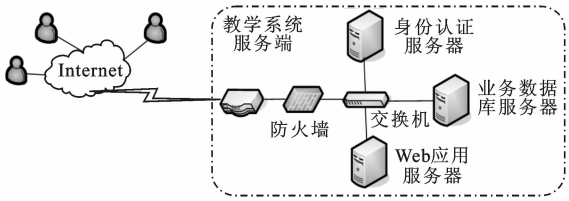

图 2　教学系统网络结构

网络教学系统的模型定义如下.

(1)教学系统提供的服务集 $S=\{s_1, s_2, s_3\}$，其中 s_1 是学生查看课程成绩，s_2 是课程教师登记/修改课程成绩，s_3 是学生给课程教师留言.

(2)支撑教学系统运行的功能部件集 $C=\{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$，其中 c_1 是验证客户身份，c_2 是加载业务数据库，c_3 是验证成绩，c_4 是成绩入库，c_5 是发送留言，c_6 是生成访问日志，c_7 是访问日志入库.

(3)引发教学系统功能部件失效的故障事件集 $F=\{f_1\}$，其中 f_1 是数据库服务器与网络交换机之间的通信电缆出现断连.

(4)教学系统功能部件失效所对应的恢复行为集合 $R=\{r_1, r_2, r_3\}$，其中 r_1 是功能部件以离线方式工作，r_2 是将数据库服务器的网络通信切换至 Wi-Fi 无线方式，r_3 是启用应用服务器的本地应急功能.

(5)服务重要性映射 Ω 使得 $\alpha_1=\Omega(s_1)=0.2$，$\alpha_2=\Omega(s_2)=0.5$，$\alpha_3=\Omega(s_3)=0.3$.

(6)服务规范函数 Ψ 使得 $C_1=\{c_1, c_2, c_6, c_7\}$，$C_2=\{c_1, c_2, c_3, c_4, c_6, c_7\}$，$C_3=\{c_1, c_2, c_5, c_6, c_7\}$.

(7)功能部件 c_j 对服务 s_i 支撑的重要性映射函数 Λ 决定了 $\beta_{j,i}$，如表 1 所示.

(8)恢复行为映射函数 Γ 反映了功能部件 c_j 对于故障 f_k 产生的恢复行为 $\lambda_{j,k}$，如表 1 所示.

表 1　功能部件对服务的依赖程度及对故障的恢复行为关系

c_j	$\beta_{j,1}$	$\beta_{j,2}$	$\beta_{j,3}$	$\lambda_{j,k}$
c_1	3	$+\infty$	4	$\{r_1\}$
c_2	$+\infty$	$+\infty$	$+\infty$	$\{r_2\}$
c_3	0	5	0	$\varnothing$
c_4	0	3	0	$\{r_2\}$
c_5	0	0	3	$\{r_3\}$
c_6	1	$+\infty$	$+\infty$	$\{r_1\} \vee \{r_3\}$
c_7	2	1	1	$\{r_3\}$

注：$\beta_{j,1}$、$\beta_{j,2}$、$\beta_{j,3}$ 分别为服务 s_1、s_2、s_3 对功能部件 c_j 的依赖程度.

3.2　教学系统生存性修复

如果教学系统在运行过程中发生故障事件 f_1，其生存性修复过程如下.

(1)恢复中断服务：①由 $C_{i,C}$ 构建 $\varepsilon_k=\{c_1, c_2, c_6\}$，$\lambda_E=\varnothing$；②由 $\lambda_{j,k}$ 分别构建 $R_{1,C}=\{r_2\}$，$R_{2,C}=\{r_1, r_2, r_3\}$，$R_{3,C}=\{r_1, r_2, r_3\}$，所以 $R_C=\{r_1, r_2, r_3\}$；③由于 r_1、r_2、r_3 在各服务恢复行为中出现的频次分别是 2、3、2，所以 $R_f=\{r_2\}$；④启用 r_2，更新 $\lambda_E=\{r_2\}$；⑤由 $P_k=\{c_2\}$，更新 $\varepsilon_k=\{c_1, c_6\}$，继续下一轮；⑥由于 $R_{1,C}=\varnothing$，$R_{2,C}=\{r_1, r_3\}$，$R_{3,C}=\{r_1, r_3\}$，所以 $R_C=\{r_1, r_3\}$；⑦由于 r_1、r_3 在各服务恢复行为中出现的频次分别是 2、2，所以 $R_f=\{r_1, r_3\}$；⑧由 $\beta_{j,i}$ 分别计算启用 r_2 后与恢复行为 r_1、r_3 对应的教学系统生存性是 $\eta_1=0.887\ 5$，$\eta_3=0.25$；⑨因此启用 r_1，更新 $\lambda_E=\{r_2, r_1\}$；⑩ 由 $P_k=\{c_1, c_6\}$，更新 $\varepsilon_k=\varnothing$，结束当前恢复过程.

(2)完善可接受服务：①由 $C_{i,C}$ 和 C_i 构建 $\bar{\varepsilon}_k=\{c_5\}$，其中 c_4、c_7 由于启用 r_2 已被修复；②由 $\lambda_{j,k}$ 构建 $\overline{R}_C=\{r_3\}$；③启用 r_3，$\overline{P}_k=\{c_5\}$；④更新 $\bar{\varepsilon}_k=\varnothing$，结束恢复过程.

3.3 教学系统生存性态势

针对教学系统出现的通信链路断连故障事件，生存性恢复需要执行恢复行为 r_2、r_1、r_3 才能将系统提供的服务修复完整. 在此期间，各服务受故障事件及恢复行为启用次序影响而处于不同的工作状态，图3描述了各服务的状态迁移过程. 所有服务在初始阶段都是完整的，但故障事件 f_1 发生时，由于它影响了所有服务共同依赖的关键功能部件，所以3个服务均处于中断状态. 根据修复控制策略，恢复行为 r_2 最先启用，它修复了服务 s_1 依赖的关键功能部件使得其进入可接受状态，而 s_2、s_3 因仍存在失效关键功能部件而继续处于中断状态. 随后执行的恢复行为 r_1 在修复 s_2、s_3 依赖的关键功能部件的同时，还修复了 s_1 与 s_2 的非关键功能部件，因此 s_1 和 s_2 都被恢复成完整状态，但 s_3 因非功能部件 c_5 未能修复而停留于可接受状态. 最后执行的恢复行为 r_3 修复了 c_5，使得 s_3 恢复到完整状态.

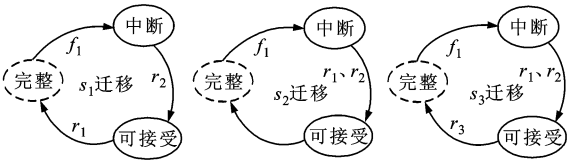

图3 教学系统各服务状态迁移过程

根据各恢复行为对服务的修复程度，教学系统的生存性在不同时刻具有不同的结果，图4给出了该系统的生存性态势分布. 初始时刻 T_0 的生存性为1，由于故障事件 f_1 中断了所有的服务，在 T_1 时刻的生存性突降为0，接着因恢复行为 r_2、r_1、r_3 的启用使得服务依赖的功能部件逐步得以修复，系统的生存性在 T_2、T_3 和 T_4 时刻分别有不同程度的提升，由0变成0.066 7、0.887 5直至最后的1. 由此可以看出，教学系统在生存性修复过程中启用的每一个恢复行为都能够提升其生存性，反映了生存性恢复机制的有效性.

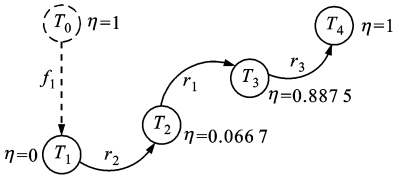

图4 教学系统生存性态势

4 小 结

针对现有信息系统生存性恢复方法的不足，本文提出了一种以功能部件作为基本修复单位的生存性恢复机制. 该机制通过3次恢复行为的执行，实现了系统的生存性恢复. 串行恢复机制由于 s_1、s_2、s_3 的恢复行为均包含 r_1、r_2、r_3，需要执行9次才能实现系统的生存性恢复，因此进一步证明了本文机制的有效性. 鉴于故障事件产生的偶然性，本文的后续研究需要关注功能部件对于系统生存性的不确定性影响，并提出相应的恢复方案.

参考文献：

[1] WILLIAM Y, DAVID D, HANS K. Survivability-over-security: providing whole system assurance [C]// Proceedings of IEEE/CMU/SEI Third Information Survivability Workshop, ISW-2000. Piscataway, NJ, USA: IEEE, 2000:201-204.

[2] LU Tunlu, GU Ning. Survivability-aware configuration management of service-oriented system based on service dependency [C]// First Joint IEEE/IFIP Symposium on Theoretical Aspects of Software Engineering, TASE'07. Piscataway, NJ, USA: IEEE, 2007: 421-432.

[3] THEIN T, POKHAREL M, CHI S D, et al. A recovery model for survivable distributed systems through the use of virtualization [C]// Proceeding-4th International Conference on Networked Computing and Advanced Information Management, NCM. Piscataway, NJ, USA: IEEE, 2008:79-84.

[4] AYARA A, NAJJAR F. A formal specification model for survivability in pervasive systems [C]// Proceedings of the 2009 International Symposium on Parallel and Distributed Processing with Applications, ISPA 2008. Piscataway, NJ, USA: IEEE, 2008: 444-451.

[5] WANG Jian, WANG Huiqiang, ZHAO Guoshen. ERAS-an emergency response algorithm for survivability of critical services [C]// First International Multi-Symposiums on Computer and Computational Sciences, IMSCCS'06. Piscataway, NJ, USA: IEEE, 2006:97-100.

[6] HUANG Gang, MEI Hong, YANG Fuqing. Runtime recovery and manipulation of software architecture of component-based systems [J]. International Journal of Automated Software Engineering, 2006, 13 (2): 251-278.

（编辑 刘杨）