增强信息系统可生存性的应急响应模型

赵国生[1]，王健[2]，刘海龙[2]
（1. 哈尔滨师范大学 实验中心，黑龙江 哈尔滨 150001；2. 哈尔滨理工大学 计算机学院，黑龙江 哈尔滨 150001）

摘 要：提出一个基于监控-分析-响应三级渐进控制模式的生存应急响应模型，用以描述面向系统可生存性增强的自适应调整机制；以此为基础，建立了应急调度模型，能够依据关键服务可生存态势的变化，进行自主的应急协调及控制；进而提出面向生存性的服务降级策略，以保证关键服务在用户期望的截止时间内完成，整个应急配置过程对用户透明；仿真试验表明，提出的方法为关键服务的可生存性提供了保证，有效地提高了整个系统的可生存能力。

关键词：可生存性；应急响应；关键服务；应急调度
中图分类号：TP302 **文献标识码**：A **文章编号**：1000-436X(2010)9A-0150-05

Emergency response model for enhanced survivability of information system

ZHAO Guo-sheng[1], WANG Jian[2], LIU Hai-long[2]
(1. Center of Experimentation, Harbin Normal University, Harbin 150001, China;
2. School of Computer, Harbin University of Science and Technology, Harbin 150001,China)

Abstract: A survivable emergency response model based on three progressive control modes monitor-analysis-response was proposed which described the adaptive adjustment mechanism oriented to the improvement of system survivability. Based on that frame, an emergency scheduling model was proposed, which could autonomically coordinate and control emergent policies according to the survivable situation changes of critical services. Then a survivability-oriented services degraded strategy was presented. As a result, critical services could be finished farthest within its deadline expected by users. Moreover, the whole configuration process was transparent for users. The simulation results show that the proposed method can provide the guarantee of survivability for critical services and effectively improve the survivability of overall system.

Key words: survivability; emergency response; critical service; emergency scheduling

1 引言

可生存性研究是国际上新一代网络安全研究的热点，代表着网络安全的新方向。可生存性是指在遭受攻击、故障或意外事故时，系统能够及时地完成其关键服务的能力[1]。可生存性重点在提高应急响应和故障恢复方面的能力[2]，让系统对入侵和攻击具有弹性。面向生存性的应急响应技术是对动态的系统生存态势所进行的主动、有预见性地响应，是为了确保系统发生故障时关键

收稿日期：2010-08-10
基金项目：黑龙江省教育厅科学技术研究基金资助项目（11531237）；黑龙江省科技计划攻关基金资助项目（GZ09A09）
Foundation Items: Educational Commission of Heilongjiang Province (11531237); The Tackle Key Program of Heilongjiang Province (GZ09A09)

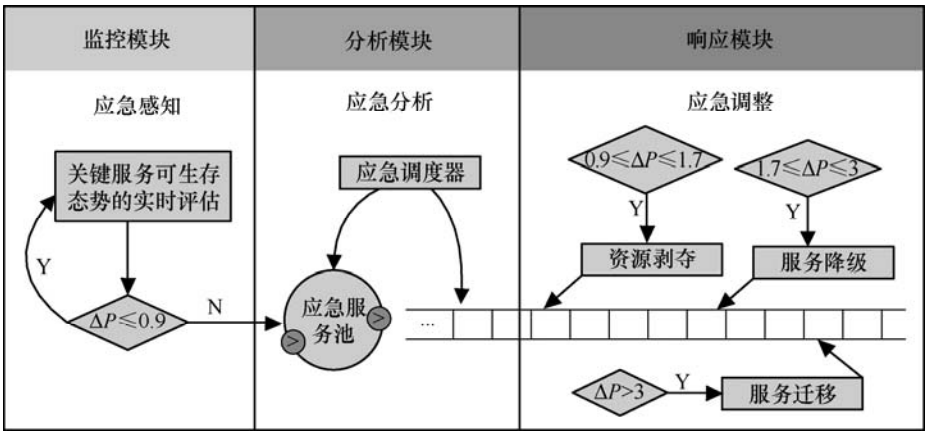

图 1　自适应的应急协调处理模型

服务仍可继续运作而预先制定和准备执行的一系列操作策略集，表现为一系列的资源协调、服务降级和服务迁移等步骤，它是整个系统生存性增强技术中的一个重要组成部分。美国国防部于 1989 年资助卡内基·梅隆大学建立了世界上第一个计算机应急响应/协调中心(CERT/CC)，目前其中一个重要的研究方向就是系统可生存能力技术[3,4]。由此可见，面向生存性的应急响应技术已经成为提高系统可生存能力的一个重要研究方向。第 2 节介绍了三级应急模型；第 3 节阐述应急响应模型实现的基本思路、关键技术和算法；第 4 节是性能分析；最后是结束语。

2　应急响应处理模型

本文将系统的生存应急响应能力进一步划分为应急感知能力、应急分析能力和应急调整能力。采取 monitor-analysis-response 的渐进控制模式来实现系统关键服务可生存性的自适应调整机制。

图 1 为本文提出的自适应的应急协调处理模型。该模型分监控、分析和响应 3 个模块，每一模块负责不同的应急策略。监控（monitor）模块负责对各关键服务的生存态势进行实时感知；分析（analysis）模块负责为多个需要应急的服务建立基于应急优先级的调度；响应（response）模块负责安排系统依据各关键服务当前不同的生存态势实施相应的调整措施。这样的应急策略基本上形成了一个完整的应急处理体系，每一阶段都有不同的动作策略执行。其中，ΔP 的值由文献[5]提出的生存态势实时感知方法获得。

3　三级应急策略的实现

3.1　服务生存态势的实时感知策略

如何及时地获得运行中的各关键服务的生存态势，是进行恰当应急响应、采取相适应的应急策略的前提。在文献[5]中，已经提出了一种衡量关键服务可生存态势的实时感知方法。

定义 1　假设评估前服务 S_j 的可生存性概率 P_1，评估后服务 S_j 的可生存性概率 P_2，则用“熵差” $\Delta P = -\mathrm{lb}(P_2 / P_1)$ 表示服务 S_j 可生存性态势的变化。

为了比较细致地刻画关键服务可生存性态势的变化，常采用表 1 的分级形式来描述。

表 1　　服务生存态势等级的分级描述

ΔP 范围	等级	服务性能下降
<0.1	较好	<3%
0.1~0.9	正常	3%~8%
0.9~1.7	稍差	8%~20%
1.7~3	较差	20%~50%
>3	瘫痪	>50%

若 $\Delta P \leqslant \sigma_0$ （σ_0 为小于 1 的常数,称为生存性阈值)表明系统可以正常提供该服务；若 $\Delta P > \sigma_0$ 表明系统不能正常提供该服务，一般取 $\sigma \leqslant 0.9$ 。ΔP 值越大,表明关键服务的可生存能力越差，或者说系统提供关键服务的能力下降。

3.2　应急调度策略

图 2 给出了一种综合截止期、松弛时间和关键度的三维动态优先级调度模型。其中，关键度序列是按照降序排列，即关键度越大，优先级越高；而

松弛时间、截止期序列是按照升序排列，即松弛时间和截止期越小，优先级越高。图 2 中处于同一斜剖面上的服务属于同一优先等级 P：

$$P = i + j + k \tag{1}$$

其中，i, j, k 分别表示服务在关键度、松弛时间、截止期序列中的位置。但同一优先等级上的服务，由于每个特征参数所占比重不同，使得不同服务具有不同的优先级，应急调度优先级可依照式(2)计算：

$$p = (P-1)(P-2)(P-3)/6 + (2P-i-2)(i-1)/2 + j \tag{2}$$

p 值越小，服务的优先级越高，且 3 个参数的重要程度由高到低依次为：关键度、松弛时间、截止期。

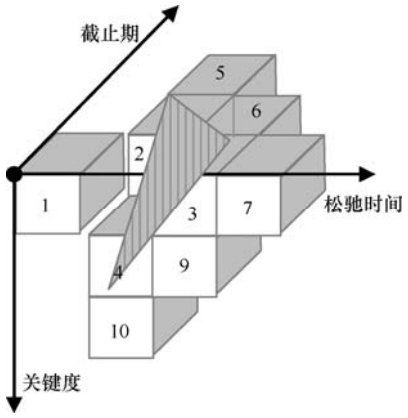

图 2　三维动态优先级调度模型

基于三维优先级设计的特点，关键度、松弛时间和截止期序列分别实现为基于关键度的服务链表 Q^v、基于松弛时间的服务链表 Q^c 和基于截止期的服务链表 Q^d。Q^v、Q^c 和 Q^d 都是带空闲头节点的双向循环链表，交错形成一个逻辑上的优先级分配队列。在系统运行过程中，当新的应急服务到达、服务完成或者服务失效时，都需要调整优先级队列，请参考先前提到的文献[6]。

3.3　服务降级策略

在该策略中，将每一个关键服务逻辑地划分为强制执行部分 M_i 和可选执行部分 O_i。M_i 必须在截止期到来前结束，以保证该服务的输出满足用户的最基本功能要求。O_i 有 $b-a$ 个（a 和 b 为用户可接受的服务等级范围，且 $a<b$）逻辑版本，不同逻辑版本具有不同的资源需求和运行时间，每一个逻辑版本都代表了该服务的一个服务等级。因此 O_i 的不同逻辑版本代表输出结果的不同精度，而 M_i 的输出已能满足用户的最低需要。

将这个降级策略记为函数 *degrade*(*s*)。其中，*s* 表示服务，而函数的返回值则为服务 *s* 被允许的实际服务等级。函数 *degrade*(*s*)的细节如下：

1) 令指针 *pa* 指向服务 *s* 节点;

2) if (*a*≤*pa*->*g*≤*b*) then {

pa->*g*−−;

//选择一个运行时间仅少于当前服务等级的逻辑版本;

3)重复 1)和 2)，直到 *s* 完成,或其服务等级已降至最低;}

4) else

s 迁移至另一服务器;

5) return(*pa*->*g*);

6) exit.

4　性能测试及分析

在仿真试验中，服务集由 200 个 $S_i(i=1,2,\cdots,200)$ 服务组成，服务的参数由下面的方法产生：

1) 服务的最坏情形执行时间 C_i 在 5～100 个时间单位之间随机选择，服从均匀分布；

2) 服务的到达时间 $T_i = NC_i/\rho$，其中，N 表示服务集中的总服务数，ρ 表示工作负载，且 $0<\rho<1$；

3) 服务 S_i 的截止期 $D_i = 2(C_i + T_i)$；

4) 由于服务的实际执行时间通常小于 C_i，因此令服务的实际平均执行时间为 $0.7C_i$；

5) 关键服务可选部分的逻辑版本数 g_i∈[a,b]，且 a, b 在 1～5 之间随机选择，服从均匀分布；

6）所有服务被随机划分到关键度不同的 $v(0 \leqslant v \leqslant 9)$ 个类别中，且令 $v=\{9,8,7\}$ 为关键服务集，$v=\{6,5,\cdots,0\}$ 为非关键服务集。

4.1　加权服务完成保证率

加权服务完成保证率（WGR, weighted guarantee ratio）是指不同关键度的服务在截止期内被按时完成的情况，它体现了应急生存策略的健壮性。当然，这个值也与使用的加权系数有关，这里利用公式 $WGR_v = 100\dfrac{w_v T_G^{\ v}}{w_v T_C^{\ v}}$，其中，$v$ 表示服务的关键度，$w_v = 2^v$ 表示不同关键度的服务权重，$T_G^{\ v}$ 表示在截止期内完成的第 v 类服务的总数，$T_C^{\ v}$ 表示提交的第 v 类服务的总数。

图 3 模拟了在不同系统负载情况下，不同关键度服务的完成率。当系统负载较小(≤0.4)时，关键度 v=9 和 v=8 的关键服务完成率超过或接近 0.95；当系统负载较大(≥0.8)时，关键度 v=9 和 v=8 的关键服务的完成率仍然维持在 0.85 左右，基本达到了服务可生存性保证；图中显示当系统负载值在 0.5～0.7 之间时，因系统中存在的空闲资源不足以满足完成关键服务所需的各类资源需求，发生了较多次的应急资源剥夺与重配，导致关键度 v=2 和 v=1 的非关键服务完成率呈线性下降，这说明该应急机制的引入也提高了非关键服务的失效率。

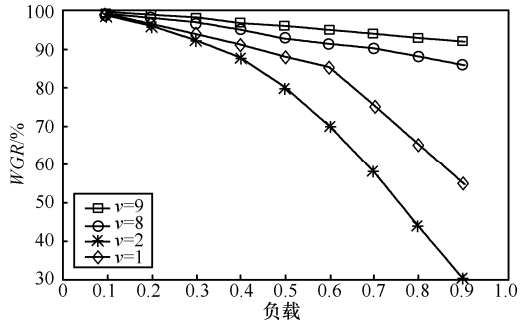

图 3　加权服务完成保证率

4.2　结果精度

结果精度（PR, precision in results）是指不同关键度的服务被降级完成后的近似结果。计算公式：

$$PR_v=\frac{\sum_{i=1}^{T_G^v}(g_i-a+1)}{(b-a+1)}}{T_G^v}$$

其中，v、T_G^v 的意义同上，g_i 表示第 v 类服务的第 i 个请求在截止期内被完成时的服务等级。

从图 4 中可以看出，对于关键度 v=1 和 v=2 的非关键服务，其结果精度随着负载的增加而急剧下降；而关键度 v=9 和 v=8 的关键服务由于运行时能够较优雅地降级服务，且又有强制服务部分的完成，其结果精度稳定维持在 0.8 以上。当负载超过 0.5 时，关键度 v=9 和 v=8 的关键服务的结果精度明显高于关键度 v=1 和 v=2 的非关键服务的结果精度，体现了应急模型对关键服务结果精度的保证。

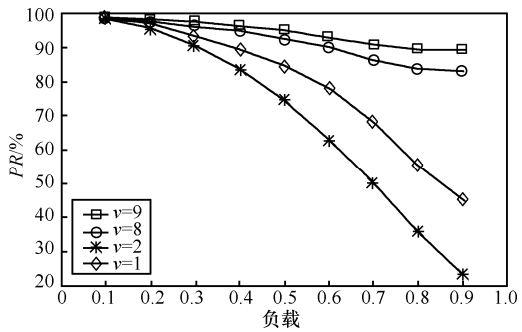

图 4　结果精度

4.3　截止期错过率

截止期错过率（MDR,missed deadline ratio）是指即使通过资源剥夺、服务降级也不能保证服务在其截止期内完成时的服务失效率。计算公式：$MDR_v=100\frac{w_vN_G^v}{w_vN_C^v}$，其中，$v$、$w_v$ 的意义同上，N_G^v 表示错过服务截止期的第 v 类服务数，N_C^v 表示第 v 类服务的请求总数。

图 5 模拟了在不同系统负载情况下，不同关键度服务 MDR 的变化趋势。对于关键度 v=1 和 v=2 的非关键服务来说，由于频繁的资源抢占所造成的截止期错失率随负载（超过 0.5 以后）的增大而急剧升高；而关键度 v=9 和 v=8 的关键服务由于能够通过资源剥夺以及较优雅地降级服务，其截止期错过率稳定控制在 0.15 期望值以下，这体现了应急模型对关键度高的关键服务截止期的保证。

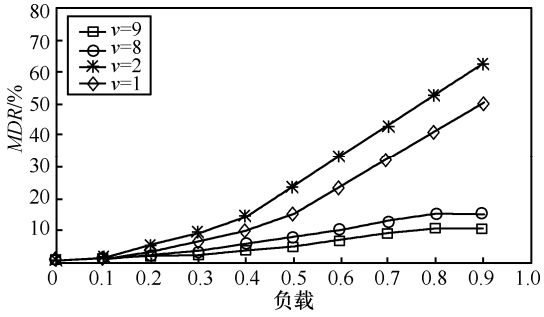

图 5　截止期错过率

5　结束语

可生存性研究是网络安全技术发展所处的一个新阶段，如何使用有效的技术来增强系统的可生存性是一个重要的研究内容。本文从应急响应的角度研究保证关键服务持续、可靠运行的可生存性增强策略。仿真试验表明所提出的方法为关键服务的可生存性提供了保证，有效地提高了整个系统的可生存能力。下一步的工作主要有 2 个方面：分析新增非关键服务的失效，制定出更合理的资源剥夺实施条件；对服务降级算法进行更深入的分析和改进。

参考文献：

[1] WESTMARK V R. A definition for information system survivability[A]. Proceedings of the 37th Hawaii Internal Conference on System Sciences[C]. Washington, 2004. 2086-2096.

[2] ELLISON R J, FISHER D A, LINGER R C, *et al*. Survivable Network Systems: an Emerging Discipline[R]. CMU/SEI, Technical Report, 1997.

[3] LIU P. Architectures for intrusion Tolerant database systems[A]. Proceedings of the Foundations of Intrusion Tolerant Systems[C]. Nevada, 2003. 3-13.

[4] TALLY G., WHITMORE B, SAMES D. Intrusion tolerant distributed object systems: project summary[A]. Proceedings of DARPA Information Survivability Conference and Exposition[C]. 2003. 149-151.

[5] 赵国生,王慧强,王健.基于灰色关联分析的网络可生存性态势评估研究[J].小型微型计算机系统,2006,27(10):1861-1864.
ZHAO G S, WANG H Q, WANG J. Study on situation evaluation for network survivability based on grey relation analysis [J]. Mini-Micro Systems, 2006, 27(10):1861-1864.

[6] 赵国生, 王慧强, 王健. CLDF:一种增强关键服务可生存性的应急调度算法[J]. 解放军理工大学学报, 2008, 9(5):528-531.
ZHAO G S, WANG H Q, WANG J. CLDF: an emergency scheduling algorithm for enhanced survivability of critical service [J]. Journal of PLA University of Science and Technology, 2008, 9(5):528-531.

作者简介：

赵国生（1977-），男，黑龙江勃利人，哈尔滨师范大学高级工程师，主要研究方向为可信计算、自律计算和认知网络。

王健（1979-），女，黑龙江哈尔滨人，哈尔滨理工大学讲师，主要研究方向为认知网络。

刘海龙（1976-），男，黑龙江哈尔滨人，哈尔滨理工大学博士生，主要研究方向为可信网络和认知网络。