第 33 卷 第 5 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.5 Computer Engineering March 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)05—0283—03 文献标识码：A 中图分类号：TP302.8

双机容错系统中最佳检查点间隔的分析

鄢喜爱[1,2]，杨金民[1]，田 华[2]
(1. 湖南大学软件学院，长沙 410082；2. 湖南公安高等专科学校，长沙 410138)

摘 要：设置检查点是容错计算机系统进行故障恢复的重要手段。因为检查点间隔选择过大或过小都将使系统性能受到影响，所以检查点间隔的适当选定是系统性能优化的一个重要指标。该文针对双机容错系统，采用检查点设置与回卷恢复的方法提出了一种系统模型，利用马尔科夫链得到了最佳检查点间隔的求解等式，通过实验证实了求解等式的正确性。

关键词：双机容错；回卷恢复；检查点间隔

Analysis of Best Checkpoint Interval of Duplicated Fault Tolerance System

YAN Xiai[1,2], YANG Jinmin[1], TIAN Hua[2]
(1. Software College, Hunan University, Changsha 410082; 2. Hunan Public Security College, Changsha 410138)

【Abstract】 Checkpointing is one of the most important method for fault tolerant computer to recover from faults. Too big or too small checkpoint interval maybe degrade the performance of system, so proper determination of checkpoint interval can make system performance optimized. This paper presents a duplicated fault tolerance system with the methods of setting checkpoints and rollback recovery, and achieves an equation about the best checkpoint interval through the Markov chain. In the end, the correctness of this conclusion through experiment is testified.

【Key words】 Duplicated fault tolerance; Rollback recovery; Checkpoint interval

回卷恢复技术是实现容错计算，提高系统可靠性的有效途径[1]。评价回卷恢复协议性能的一个重要指标是协议的容错开销。容错开销是指系统在有故障情况下计算任务的期望完成时间与无故障无容错情况下计算任务完成时间的差值。容错开销包括两个方面:无故障时开销和故障恢复开销。 无故障时开销是指系统在无故障执行时，增加容错策略时所导致的程序执行时间增加。故障恢复开销是指发生故障时，系统状态恢复到故障点时刻状态所花费的时间。目前，回卷恢复主要采用基于检查点的回卷恢复技术。检查点的回卷恢复技术是在进程正常运行的适当时刻设置检查点，保存进程状态，当出现故障时，进程卷回到检查点状态，通过重试，进行故障恢复，从而避免从头开始执行，减少计算损失。检查点时间间隔的设置直接影响检查点协议的容错开销，因为当检查点间隔大时，检查点频率小，无故障时开销小，但故障恢复开销大，如果检查点间隔小，则故障恢复开销小，无故障时开销大[2]。

本文分析研究的是双机容错系统中最佳检查点间隔的设置策略。文献[3]讨论了双机系统中检查点设置周期的选择，但未考虑进行卷回时也有可能发生故障的状态。本文利用马尔科夫链对系统的各种状态迁移进行了分析，从理论上求出最佳检查点间隔；并通过实验证实了求解等式的正确性。

1 系统模型及假设

双机容错系统的主要功能是确保系统的不间断运行。主机和副机可以通过网络、串口、SCSI 等通道相互监视各自的运行情况，一旦某台机器发生故障，另一台机器将迅速自动接管它的全部资源，从而保证了系统的不间断性，也保证了系统数据的完整性[4]。

本文采用的双机容错系统是一种同构型的双工系统，如图 1 所示。两个处理结点之间由专用的高速网相连，进行系统内部及外部的通信。两个处理结点同时加电和工作，并周期性地设置检查点。一个任务同时输送给两个处理机，两个处理机按检查点的时间间隔对中间结果(中间状态)进行比较，一旦结果(状态)相同，说明系统正常，保存程序执行的中间状态。否则，就说明其中有一个处理机在程序执行中出现故障，于是两处理机同时卷回到最近一个检查点，拷贝检查点所保存的数据，重新执行[3]。

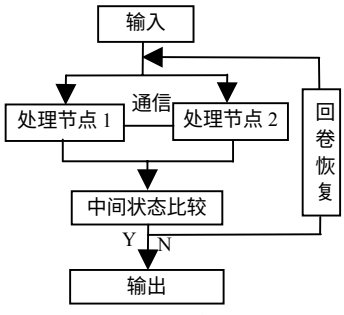

图 1 双机容错系统模型

此系统仅考虑由硬件不稳定及断电等造成的处理机停止响应或崩溃等这类硬件故障，假定软件及网络是无错的，系统的平均无故障时间(MTBF)比检查点间隔周期要长，每个处理机中发生的故障的次数服从泊松过程，每个处理机故障率为 λ。

基金项目：国家自然科学基金资助项目(NSFC 60473031)；湖南省自然科学基金资助项目(05JJ30116)

作者简介：鄢喜爱(1972－)，男，硕士生，主研方向：故障恢复与系统容错；杨金民，博士、副教授；田 华，馆员

收稿日期：2006-09-04 **E-mail：**yanxiai222@yahoo.com.cn

2 系统中最佳检查点间隔的理论分析

2.1 系统参数的设定

假定检查点无故障时开销为 C(做检查点时保存和比较进程状态的开销)，故障恢复开销为 R，并设 C、R 都是常量。

假设检查点间隔为 T；任务运行有效时间(不采用容错措施且运行过程中无故障发生时，任务的理论运行时间)为 W，同一任务 W 为常量，可通过不采用容错措施时测出；完成该任务所需要的实际运行时间(包括容错开销时间)为 S(T)。

设 U= ⌈ W/ T ⌉，任务的运行时间便大约被分为 U 个检查点间隔。如果能计算出每个检查点间隔的实际运行时间 t，则 S(T)为

$$S(T)=U*t \tag{1}$$

系统利用率 A 等于系统的有效时间除以系统的实际运行时间，即 A=W/S(T)。

2.2 系统中的状态迁移

一个检查点间隔的过程中，系统进程状态的转换过程可用三态离散马尔科夫链来表示，如图 2 所示。

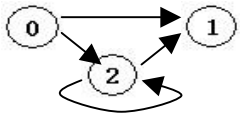

图 2 3 个状态的马尔科夫链

图中状态 0 为一个检查点间隔开始执行的初始状态，状态 1 为一个检查点间隔完成后的结束状态，状态 2 为故障恢复态。进程在初始状态 0，如果经过一个检查点间隔时间后没有出现故障，则迁移到状态 1，否则迁移到状态 2；进程在状态 2，如果经过故障恢复后没有出现故障，则迁移到状态 1，否则返到回状态 2，仍利用原检查点文件进行故障恢复[5]。

2.3 系统中最佳检查点间隔的求解

一个检查点间隔的实际完成时间可利用三态离散马尔科夫链来求解。设从状态X 到Y 的迁移概率为PXY，相应的权重为WXY。其中PXY表示这种迁移的可能性，WXY表示在状态迁移到Y之前处于X的持续时间[6]。

从状态 0 到状态 1：根据系统模型，单个处理机不发生故障的概率为 $e^{-\lambda(T+C)}$，(T+C)是在无故障时完成一个检查点间隔所需要的时间，则 2 个处理机都不发生故障的概率 $e^{-2\lambda(T+C)}$，权重为W_{01} = T + C。

从状态 0 到状态 2：系统中发生故障的概率P_{02}= 1–P_{01}；发生故障的概率密度为 $2\lambda e^{-2\lambda t}$，则对应的权重为

$$W_{02}=\int_0^{T+C} t\frac{2\lambda e^{-2\lambda t}}{1-2\lambda e^{-2\lambda t}}dt=\frac{1}{2\lambda}-\frac{T+C}{e^{2\lambda(T+C)}-1}$$

从状态 2 到状态 1：当状态迁移到 2 后，由于需要首先进行故障恢复，因此完成该间隔一共所需时间为T+C+R。在恢复期间及随后的检查点间隔内 2 台处理机都不发生故障的概率为$P_{21}=e^{-2\lambda(T+C+R)}$，相应权重为$W_{21}$ = T+C+R。

从状态 2 到状态 2：发生该种状态转移，说明在故障恢复期间又发生故障。此故障概率P_{22}=1–P_{21}；类似于W_{02}，有

$$W_{22}=\frac{1}{2\lambda}-\frac{T+C+R}{e^{2\lambda(T+C+R)}-1}$$

根据文献[7]完成一个检查点间隔所需要的时间就是

$$t = P_{01}W_{01} + P_{02}[W_{02} + W_{22}P_{22}/(1 - P_{22}) + W_{21}] \tag{2}$$

将相应的值代入式(2)，则可得到完成一个检查点间隔所需要的时间为

$$t=\frac{1}{2\lambda}(e^{2\lambda(T+C+R)}-e^{2\lambda R}) \tag{3}$$

将式(3)代入式(1)，则可得

$$S(T)=\lceil\frac{W}{T}\rceil*\frac{1}{2\lambda}(e^{2\lambda(T+C+R)}-e^{2\lambda R})=\frac{We^{2\lambda R}}{2\lambda}(\frac{e^{2\lambda(T+C)}-1}{T})$$

以 T 为变量，对 S(T)求导，并设

$$\frac{\partial S(T)}{\partial T}=0$$

则可求出最优的检查点设置周期：

$$\frac{\partial S(T)}{\partial T}=\frac{We^{2\lambda R}}{2\lambda}(\frac{T2\lambda e^{2\lambda(T+C)}-(e^{2\lambda(T+C)}-1)}{T^2})$$

在上式中，

$$\frac{We^{2\lambda R}}{2\lambda}$$

为常量，T^2为分母不能为 0，所以得出

$$e^{2\lambda(T+C)}(2\lambda T-1)+1=0 \tag{4}$$

上式直接计算出 T 的表达式比较复杂，我们采用科学计算程序包 Matlab 编程进行数值分析得如图 3 所示的结果。图 3 说明：当故障率一定时，最佳检查点的间隔随着检查点开销的增加而增大；当检查点的开销一定时，最佳检查点的间隔随着系统处理机的故障率升高而减小。

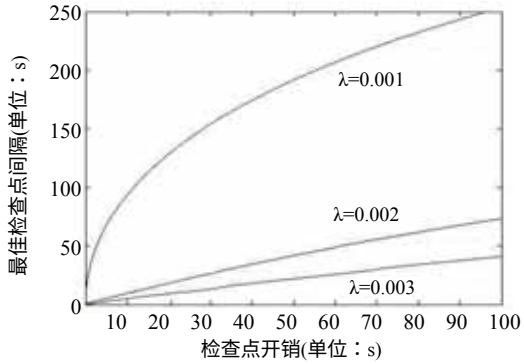

图 3 最佳检查点间隔数值分析

3 实验、计算结果分析比较

该实验使用联想扬天 A4800C 品牌机，CPU 为 Pentium 4 521，内存 512MB。作为稳定存储器的硬盘容量为 160GB。运行的操作系统为 Win2000。

应用程序选择了 RSA 加密算法中模为 1 024 位的密钥求解。选择它为应用程序的主要原因是既可以获得比较长的运行时间，又可以获得比较大的数据量，以防止偶然性因素带来的影响。对于每种测量数据，文章采用 10 次的平均值。表 1 为实验的采用的数据。

表 1 实验所采用的数据

λ	检查点大小	W	C	R
0.001	2 336KB	5 736s	5s	5s

实验通过取不同的检查点时间间隔测试任务的实际运行时间 S(T)，然后计算系统的利用率，显然，当系统的利用率最大时，对应的检查点间隔就是最佳检查点间隔。实验结果如图 4 所示。

实验测得当 T 约为 68s 时，系统利用率最高，即检查点最佳时间间隔为 68s；实验结果分析图同时说明存在一个最佳检查点间隔。取实验所采用的参数，用科学计算程序包 Matlab 对式(4)编程进行数值分析，分析结果如图 5 所示，检查点最佳时间间隔也是约为 68s；另外，将 T=68s 代入式(4)进行数学计算也近似成立，从而验证了式(4)的正确性。

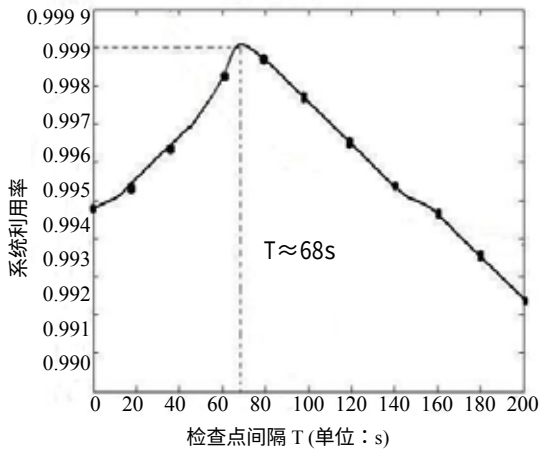

图 4 系统利用率与检查点间隔的关系

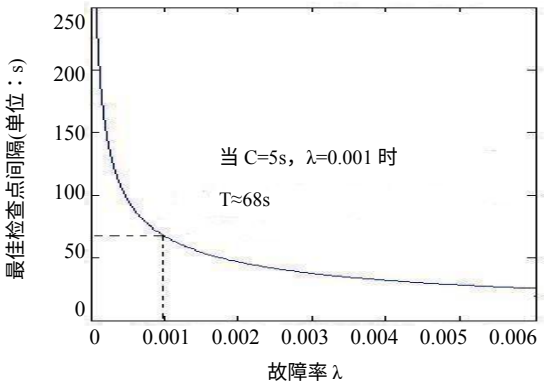

图 5 实验环境下等式的数值分析求解结果

4 结论

确定检查点最佳间隔，可以有效地减小检查点的开销，提高系统的利用率。本文通过对双机容错系统中各个可能的状态进行分析，得出了一种确定检查点最佳间隔的求解等式，并通过科学计算程序包 Matlab 编程对其进行了准确的数值分析。实验结果验证了求解等式的正确性，并表明了选择不同的检查点间隔将直接影响系统的利用率，而且存在一个最佳的检查点间隔。

在分析中假定检查点无故障时开销为常量，而在实际的系统中，检查点时刻进程状态的大小可能会发生变化，这可能会影响到分析的精度。如何通过数学建模获知进程状态大小的变化来确定动态的最佳检查点间隔是我们今后研究的重点。

参考文献

1 Manetho E. A Survey of Rollback Recovery Protocols in Message Passing Systems[J]. ACM Computing Surveys, 2002, 33(3): 375-408.

2 杨金民, 张大方. 基于分块消息日志的回卷恢复策略[J]. 电子学报, 2004, 32(5): 857-859.

3 谢宝湘, 金士尧. 实进双机系统中检查点设置周期的选择[J]. 计算机工程与科学, 2001, 23(1): 90-92.

4 吴　娟, 马永强. 一种基于主备机快速切换的双机容错系统[J]. 计算机应用, 2005, 25(8): 1948-1950.

5 Vaidya N H. A Case for Two-level Recovery Schemes[J]. IEEE Transactions on Computers, 1998, 47(6): 656-666.

6 刘云生, 张传富. 基于 Markov 链的分布式仿真系统最佳检查点间隔研究[J]. 国防科技大学学报, 2005, 27(5): 73-77.

7 Trivedi K S. Probability and Statistics with Reliablility, Queueing and Computer Science Applications[M]. Prentice Hall, 1988.

（上接第 282 页）

且管理员需要维持多台设备之间密码的一致性，当后台认证使用 Radius 时，可以集中解决用户的认证问题。由于当前基本上每台网络设备都能很好地支持 Radius 服务，而基本不支持 LDAP 服务，要实现网络设备的统一认证就必须在 Radius 服务器上进行开发，这相对于更改各个网络设备公司的网络操作系统要显得简单。为实现此目的，网络中心同深圳华为公司北京研究所进行磋商后，华为公司在其综合接入管理服务器(CAMS)中增加了到 LDAP 的接口，这样，网络设备的认证信息能够顺利从 Radius 服务器进行中转，到 LDAP 服务器进行最终的用户认证。

网络设备的认证实现后，对全校无线网络进行了改造，对每一个无线 AP 设置双 SSID，其中一个为 Public，另一个为 Private，Public 的 SSID 对无线接入用户提供 Portal 认证，这个 Portal 认证同前面城市热点的 Portal 页面一样，不同的是城市热点的 Portal 是有线网络用户访问校外时才弹出，而无线网络的 Portal 当用户走出本段的网关时就必须弹出，这种方式简单易操作，不需要增加客户端，对用户端的操作系统也无特殊的需求，但安全性相对较差，在用户的手持笔记本与无线基站之间无法对数据进行加密，对无线用户来说存在一定的安全隐患。如果用户需要获得较高的安全性，只需要选择 Private 的 SSID，就可以采用 802.1x 的方式进行认证，这样用户的移动站同基站之间的数据就进行了加密处理，保护了用户数据的安全。802.1x 的方式实际上是通过华为的 Cams 中提供的 Radius 进行认证，只是经过修改后的 Radius 服务器在收到用户的用户名与密码后是到 Ldap 认证中心进行认证，而对用户的计费等还是在本地 Radius 服务器中进行。

3.2 安全性讨论

以上系统到 LDAP 认证中心的认证基本上都是明文方式进行，如果需要获得进一步的安全性，在各应用系统认证接口上采用 SSL/TLS 即可以实现加密的认证，但倘若并发认证的用户数量较大，加密这些信息可能会占用一定的系统资源。

4 总结

通过以上的实现方式，已经基本上建立了全校的统一身份认证体系，网络用户只需要维护一套用户名与密码就可以使用学校的各个系统，方便了用户的使用。用户丢失密码后，只需要到网络信息中心更改密码即可，而不需像原先一样，用户往往说不清楚修改什么密码，造成密码修改错误。目前，正在同相关移动运营商进行磋商，将用户的手机号同用户名进行绑定，如果用户忘记密码，只需向学校的特服号码发送一条特定的短消息就可以完成密码的重新初始化。

参考文献

1 Tanenbaum A S. 计算机网络[M]. 3 版. 北京: 清华大学出版社, 1998-07.

2 Sun Microsystems Inc.. iPlanet Directory Server Access Management Edition Installation and Configuration Guide(Copyright 2002)[Z]. http://docs.sun.com/source/816-5626-10/01intro.html.

3 吴晓斌, 张月琳. 基于 LDAP 的校园网统一身份认证系统设计[J]. 华中科技大学学报(自然科学版), 2003, 31(增刊): 332.