文章编号:1671-4598(2019)03-0231-04 DOI:10.16526/j.cnki.11—4762/tp.2019.03.047 中图分类号:TP311.1 文献标识码:A

一种多策略双机热备方法

罗贵舟，王锦杰，杨旭斌，蒋兰兰，巩远航
（南瑞集团有限公司（国网电力科学研究院有限公司），南京 210003）

摘要：随着电网监控系统对实时性要求的不断提高，为避免由于网络环境、程序故障等原因导致的服务中断，保障实时应用服务不间断运行，提出了一种多策略双机热备方法；通过利用主备节点之间 HeartBeat 协议以及借助与数据库的时间同步机制实现对运行状态的双重心跳检测，避免裂脑问题；再利用节点 IP 多重校验完成服务接管，并实现主备间的平滑切换；该方法处理机制简单高效，无需任何额外系统配置，并在实际应用中验证了其稳定的性能。

关键词：双机热备；多策略；裂脑问题；HeartBeat；IP 接管

A Multi Strategy hot standby method

Luo Guizhou, Wang Jinjie, Yang Xubin, Jiang Lanlan, Gong Yuanhang
(NARI Group Corporation/State Grid Electric Power Research Institute, Nanjing 210003, China)

Abstract: With the continuous improvement of real-time requirement of power grid monitoring system, a multi-strategy dual-machine hot standby method is proposed to avoid service interruption caused by network environment and program faults and ensure the uninterrupted operation of real-time application services. By using HeartBeat protocol between master and standby nodes and time synchronization mechanism with database, the dual heartbeat detection of running state can be realized to avoid the problem of split-brain. Then the service takeover can be completed by using IP multiple checks of nodes, and the smooth switching between master and standby can be realized. This method is simple and efficient without any additional system configuration, and its stable performance is verified in practical application.

Keywords: hot standby; multi strategy; split-brain; HeartBeat; IP address takeover

0 引言

在电网监控系统中，随着核心业务的不断增加，系统对应用服务的实时性和稳定性都提出了严格要求[1]，既要保证服务的全天候执行，也要保证内存资源的高度一致，而物理链路、网络故障、程序异常等都会导致服务中断，甚至系统瘫痪，因此系统的高可用性或容错性能一直作为监控领域重要指标之一。高可用解决方案有多种，如高端容错主机、集群（cluster）、双机热备（Hot standby）等。其中高端容错主机完全基于硬件，成本极高，适用于对容错有很高要求的应用；集群技术是利用网络将一组相互独立的服务器互联，并以单一系统的模式加以管理以提供系统高可用性的服务，集群技术偏重于解决负载均衡、并行计算等问题，部署相对复杂，且易造成内存数据的不一致；双机热备系统作为高可用集群的最小单元，是将主服务器部署成互为备份的两台服务器，当其中运行着的一台服务器出现故障无法启动时，另一台备份服务器会迅速的自动切换，接管服务，从而达到程序和数据的备份，系统投资小、部署简单，适用于实时处理系统中。可见双机热备是电网监控中保持系统实时性、稳定性的优选方案。

双机热备主要分为两类：基于共享存储的方式以及纯软件方式[2]，前者是利用磁盘阵列保障数据的连续完整，后者是利用镜像软件实现数据以及程序的复制备份从而保障系统安全，它们虽保证系统稳定的方式不一样，但故障判断方式基本一致，通常采用心跳检测。本文主要对目前热备方案中的心跳以及切换机制存在的缺点进行研究，并给出优化方案。采用服务间 HeartBeat 协议以及与数据库时间同步相结合方法取代单一心跳所带来的诊断不确定性，避免“裂脑”（split-brain）问题的出现[3]；利用 IP 校验与布尔值权限标识取代虚拟 IP（VIP），完成服务接管。该方法无需配置任何系统参数，部署简单，故障判断准确，实现无缝切换。

1 传统双机热备机制

目前，双机热备作为一种提高系统高可用性方法，已拥有较多产品，根据不同应用可划分 3 种工作模式：双机主从模式（active/standby）、双机互备模式、双机双工模式（active/active），双机主从模式指主服务器处于服务状态，而备服务器处于侦测准备状态；双机互备模式是指部分服务运行于主机，部分服务运行于备机；双机双工模式是指系统两台服务器同时运行，实现负载均衡。很多热备开源软件都是基于经典热备协议 VRRP[4]、HSRP[5] 进行开发，比如 Linux-HA[6]。传统双机热备是通过主备节点服务器间心跳机制（HeartBeat）检测彼此状态，若备节点服务器

收稿日期:2018-09-10； 修回日期:2018-10-12。
基金项目:国家自然科学基金项目(61573319),浙江省自然科学基金重点项目(LZ15F030003)。
作者简介:罗贵舟(1990-),男,江苏淮安人,初级工程师,研究生,主要从事电力系统及其自动化方向的研究。

认定主节点异常，就会接管主节点全部功能并对外提供服务[7-8]。在热备中，心跳协议以及相关算法一直是热备研究的热门领域，现已有较多研究成果以及应用。在文献［9］中，描述了利用心跳机制解决了异构集群中节点超时设置的公平性，缩短了 Hadoop 实时处理系统在短作业下的容错时间；在文献［10－11］中，采用虚拟化心跳算法监测网络，实现了数据中心虚拟化系统的网络状态监测；在文献［12］中，采用心跳包实现了 CAN 工业总线的高可用。这些应用表明目前心跳技术已趋于成熟，但也体现出绝大部分还停留在对协议本身的研究，没有从运行架构上对热备方法进行优化。

根据以上应用分析，可以看出传统的双机热备机制心跳链路单一，输出结果可靠性较低，无法有效判断是网络故障还是服务故障，易出现服务竞争风险。虽 Fencing 和 Quorum 机制可有效防止这一风险，但是这两种方法可能会引入新的节点故障问题，另外他们对网络设备的双机热备不通用[3]。

2 多策略双机热备框架

为了解决传统双机热备方案中潜在的“裂脑”问题以及保证主备服务切换准确无误，多决策双机热备方法不再完全依赖于节点间单一心跳链路检测，而是通过第三方决策介质－数据库，实现多重“心跳”判断，交叉检测，再利用 IP 双向校验实现服务接管，该方法可部署于电网监控系统常用架构中，不增加任何额外物理资源以及不使用任何第三方辅助软件，由内置的低耦合线程完成全部热备服务流程。图 1 为多策略热备架构图，它由 3 个决策实体组成：主节点应用服务器、备节点应用服务器和数据库。主备服务器采用 Linux 操作系统，数据库采用 ORACLE，程序对服务器配置无依赖。

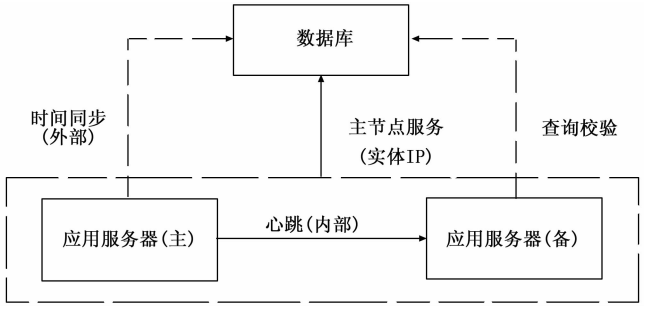

图 1 多策略热备架构图

由图可知，多策略热备架构中，同时部署运行 2 台应用服务器，工作于双机主从模式，主备服务器之间建立心跳链路，根据心跳协议定时发送 Heartbeat 报文，与此同时，数据库作为中间辅助介质，默认主节点会按一定时间间隔向其同步相关信息，包括节点号、IP 地址以及同步时间，内部心跳故障后，备节点会主动查询数据库同步时间，该过程完成报文应答和时间超时校验的交叉检测，即多策略心跳侦测机制。若主节点因某种原因宕机，备节点将主动获得数据库使用权，并更新数据库时间，且根据布尔输出值获得本节点对外服务权，备节点无缝切换成“主”节点，该过程形成多策略 IP 接管机制。

在上述架构中，服务节点均以实体 IP 对外提供服务，优化了传统虚拟 IP 切换所带来的对不同脚本的维护缺点。主备服务器中应用程序同时运行，资源数据和性能数据互为备份，主备机具有相同的内部资源交换以及接收外部服务、请求功能，但只有主机能够对外提供服务，包括读写数据库，向 WEB 端发送数据等。

3 关键技术

3.1 定时器设计

定时器作为一种时钟装置，对软件中断服务至关重要，衡量其性能的指标包括：启停时间，处理 Tick 时间以及超时事件处理时间。对于少量定时器创建，一般操作系统能够较好解决，但程序中有大量定时器创建、删除时，系统定时器的可靠性将很难控制。传统的定时器数据结构通常采用链表方式，按照时间先后顺序存储相应事件，时间复杂度为 $O_{(n)}$，算法执行时间较长。多策略机制中的双重心跳检测以及接管服务状态切换需要高性能的定时装置，定时器的精度成为保证心跳报文定时发送以及状态机跳转的关键。为保证双机热备性能，提高时钟管理效率，重点研究了一种提高定时精度的数据结构，它由定时器信息块、定时器资源池以及忙定时器三部分组成。

定时器信息块（Timer Information Block，TMIB）存储所创建的定时器信息，对应数据结构为：TMIB＝｛use，arrived，type，que，pno，totoal _ 100m，timer _ no，que10，que100，prev，next｝，其中 prev 指向前一个定时器信息块，next 指向下一个定时器信息块。

定时器资源池（Timer Resource Pool，TMRP）记录所创建定时器数目，以及允许使用的定时器起始和终点，对应数据结构为：TMRP ＝ ｛total，head，end，tm［NUM］｝，其中 total 记录程序中可用定时器数目，初始值为 NUM，随着定时器不断被创建，total 不断递减，而随着定时器到期，该值又不断递增；head 记录可使用定时器队列的起始位置，这样保证定时器始终在该值处开始创建；end 为闲置定时器结束位置，当定时器到期释放时，定时器信息块为 TMRP－＞tm［TMRP－＞end］，这样可保证定时器资源池的循环使用；tm［NUM］存储定时器信息，该信息块是循环结构，从 TMRP－＞head 开始，到 TMRP－＞end 结束，在这之间的所有定时器都可被分配使用。

忙定时器（Busy timer，BTM）是以队列形式记录正在使用的定时器，与定时器资源池结构相类似，BTM 结构体中也包含 haed、end 成员，从而保证忙定时器资源的循序利用。图 2 为定时器创建使用时，TMRP 与 TMIB 成员以及数据对应关系。

图 2 中展示了定时器被创建过程（灰色表示忙定时器，白色表示空闲定时器）。定时器初始化时，NUM 全为可用定时器，随着定时器的创建和使用，head 成员不断改变指

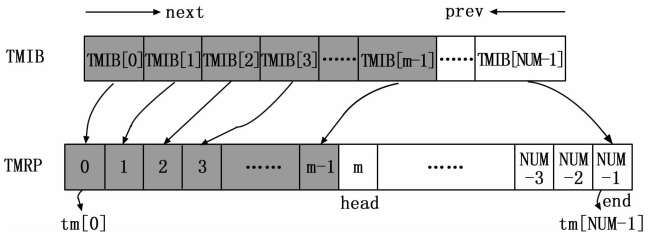

图 2　TMRP 与 TMIB 对应关系图

向位置，但始终指向空闲定时控制队列头，同时 total 成员的数量逐步递减，图中创建了 m 个定时器后（m＜NUM），可用闲置定时队列数量 total 减少为 NUM－m，head 指向 m 位置。

图 3 展示了定时器继续被创建以及有定时器被释放过程。若继续创建了两个定时器，他们启用 TMRP［tm［m］］和 TMRP［tm［m＋1］］两个闲置定时器位置，此时，TMRP 中的 head 成员将指向定时器资源池的 tm 数组第 m＋2 个定时器信息块位置。与此同时，若有两个定时器到到期后需退出，假设释放出 TMIB［1］和 TMIB［3］两个定时器控制块。那么，资源池将接管这两个控制块使用权，即从 TMRP－＞end 位置开始，将这两个已闲置的信息块保存到 TMRP 的 tm 数组成员中。如图所示，TMIB［1］和 TMIB［3］将插入到 TMRP［tm［0］］和 TMRP［tm［1］］的队列中，并将 TMRP－＞end 的位置往后移两位。可见，无论 TMIB 中的定时器如何改变，TMRP 结构体中将始终保持闲置的定时器控制队列（白色部分）和已经被使用定时控制队列（灰色部分）两个区域连续。

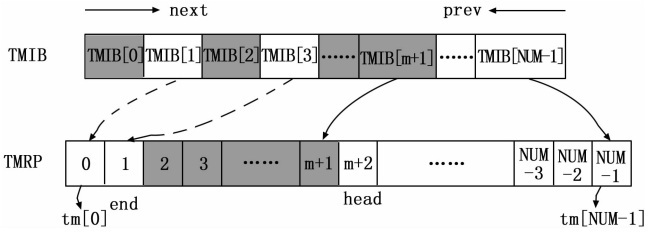

图 3　定时器创建与释放示意图

以上数据结构使定时器的精度、数目变得灵活，可满足同步延时、相对定时、以及绝对定时等定时器的需要，提高了定时服务性能，为多策略双机热备程序中链路心跳、时间同步以及状态定时跳转提供了精准的时钟管理服务。

3.2　双重心跳机制

在双机热备中，故障检测是软件程序的基本功能，其检测点的多少直接关系到热备的性能，对于实时应用系统的热备需求，用户需要一种性能稳定可靠，部署简单且廉价的方案，而传统双机热备，通常采用单一心跳检测作为判断服务故障状态依据，在实际应用中容易出现服务竞争，造成“裂脑问题”，进而使数据库产生大量垃圾数据，甚至导致数据的严重不一致，这在电网系统中是绝对避免的。双重心跳机制优化了单一心跳缺点，采用多点交叉检测，检测逻辑强相关，与应用程序耦合性低，避免了“裂脑”发生，实现故障的精准自判断。图 4 为双重心跳逻辑示意图。

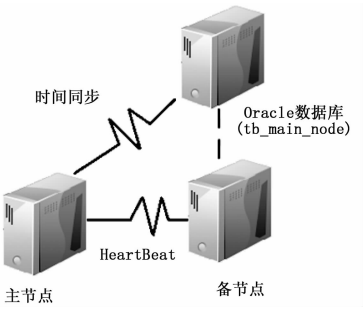

图 4　双重心跳逻辑示意图

如图 4 所示，2 台应用服务器间采用 HeartBeat 协议，备节点主动发送 hello 心跳报包到主节点，每 5 秒发送一次，若连续 20 次没收到主节点响应，则可确定主备之间心跳链路异常，以此作为第一次心跳检测，此时无法判断主节点服务确切状态，服务此时未发生切换。随后，备节点检查数据库，进入第二次“心跳”检测即时间同步机制。

在 oracle 数据库中建立 tb _ main _ node（node，ip _ addr，latest _ update _ time）服务节点表，如下表所示。

表 1　服务节点表

NODE	IP_ADDR	LATEST_UPDATE_TIME
1	192.168.91.101	2018－1－6 10:51

其中 node 为主备节点标识（逻辑标识，代表不同 IP 地址），这在主备程序配置文件中人为定义，ip _ addr 为节点 ip 地址，node 与 ip _ addr 一一对应，latest _ update _ time 为节点与数据库的同步时间，格式为“年－月－日 时：分”。主节点应用程序每分钟调用 OCI 接口更新服务节点表中的索引 latest _ update _ time 值，实现应用程序节点时间与数据库的同步。当第一次心跳检测异常后，备节点开始查询 tb _ main _ node 中的 latest _ update _ time 值，若检测到 latest _ update _ time 延时于备机时间 60 s，则可以确切判断主机节点服务宕机，输出布尔结果值；反之，则主备节点服务正常，只是心跳链路异常。主服务宕机后，备节点用自身信息更新服务节点表，进入服务接管流程。以上可以看出，服务节点表只会保留“主”节点信息。

设计中，心跳协议以及同步时间可根据用户需要进行灵活配置，用户只需在配置文件录入性能指标具体值即可，定时装置可满足毫秒级侦测要求。

3.3　IP 接管机制

在电网监控领域，通常为保证内存实时数据以及性能资源的一致性，需同时启动 2 台主备应用程序，只是仅有主节点才有权限向数据库或 WEB 端写入数据。本文设计中，采用内嵌到应用程序的轻量级软件服务实现 IP 接管，利用实体 IP 校验以及布尔权限标志取代传统虚拟 IP 切换，无需运行 IP 切换脚本，以及不考虑任何服务器参数。根据程序接管流程给出如下定义：

定义 1：节点逻辑号（module）：用于区分主备 IP 地址，在程序配置文件中设置，与服务节点表 node 类似。

定义 2：布尔权限标识（g _ MainNode）：用以识别主备节点服务状态，取值为：TRUE/FALSE。TRUE 表明程序处于全激活状态，可对外提供服务，FALSE 表明程序只能内部交互，对外服务关闭。

IP 接管同样借助服务节点表实现。双节点服务初次启动后，默认的主节点会自动将信息更新到表中，随后在每次同步时间之前，会查询节点表中的 node 值是否与自身节点逻辑号一致，若相同，则表明此时节点对应的 IP 为主节点，否则说明该服务器已变成备节点。在查询中，为了防止服务节点表同时被主备节点访问，设计中，利用存储过程访问数据，先 select for update 进行锁住，然后再进行查询，从而保证事务的一致性。

故障发生后，IP 校验以及切换具体流程为：

步骤一：利用 ORACLE 调用接口（OCI）访问数据库，查询 tb _ main _ node 的 node 值；

步骤二：判断 node 与 module 不等，用自身（备）信息更新 tb _ main _ node 内容，g _ MainNode 此时为 FALSE；

步骤三：tb _ main _ node 进入时间同步流程，并进入步骤一；

步骤四：判断 node 与 module 相同，g _ MainNode 值变为 TRUE。

步骤五：备机成为新的主节点，以 tb _ main _ node 中的 ip _ addr 实体地址对外提供服务。

多策略双机热备方案在故障点检测和服务接管两方面逻辑依赖性强，不增加新的节点故障，与其他业务功能耦合性低，程序设计中，根据功能特点独立出可裁剪、可配置的线程进行部署，图 5 为多策略双机热备软件流程图。

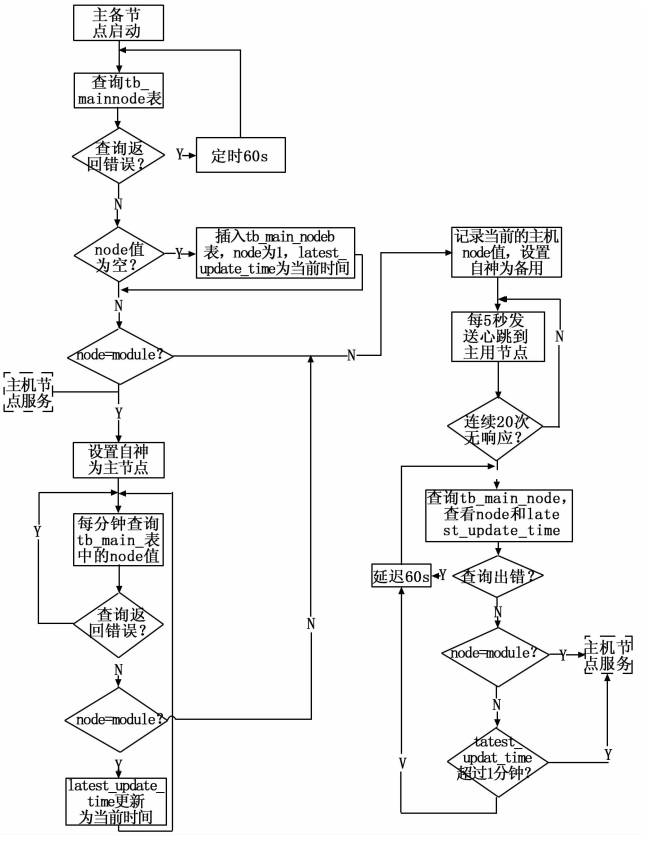

图 5 多策略双机热备软件流程图

4 测试与应用

要测试多策略双机热备方法是否可靠，须验证系统故障后，服务能否及时接管，以及是否存在主备节点同时争夺对外提供服务的情况，即备节点试图接管服务时，主节点是否还继续提供服务；如果存在争夺服务的情况，那么就可以判定该方法存在“裂脑”问题。测试中，监控系统由 4 台服务器组成，如图 6 所示，其中 192.168.91.100 为数据转发服务器，用于向主备应用服务器转发实时数据；192.168.91.101、192.168.91.102 为主备应用服务器，用于处理实时数据和资源信息，并向数据库写历史数据以及与 WEB 前台交互；192.168.91.103 服务器中部署 WEB 以及 ORACLE 服务，101、102、103 为热备决策实体。系统运行时，ORACLE 中 tb _ main _ node 默认值为 { ‘1’, ‘192.168.91.101’, ‘2018－1－6 10：51’’}，则 101 服务器为主节点，系统服务正常，随后将 101 中的处理进程强制关闭或主服务器关机，2 分钟后，tb _ main _ node 值自动更新为 { ‘2’, ‘192.168.91.102’, ‘’2018－1－6 10：53’’}，102 成为新的主节点，接管 101 对外一切服务，WEB 前台和数据库数据连续更新，系统无缝切换，系统平稳运行。

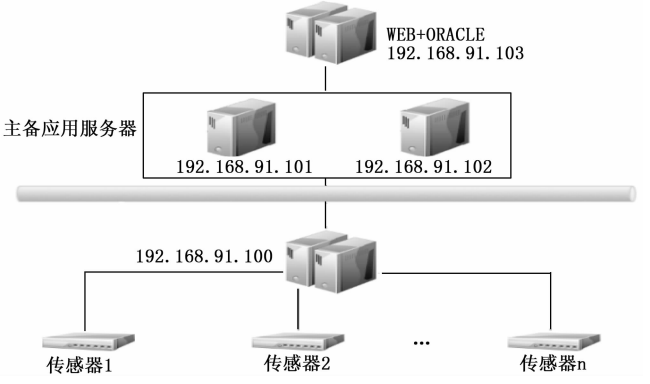

图 6 应用服务测试部署图

目前，多策略双机热备方法已在机房综合监控系统得到应用，并部署到了江苏、福建、青海等省公司用于处理全省机房数据，以提高通信机房无人值守能力。以某省为例，在系统全面上线后，主节点应用服务器先后出现过因内存溢出、服务器宕机、进程启动不了等故障，双机热备程序均及时做出判断，并及时（小于 2 分钟）无缝切换到备机，而且备节点内存中的性能信息以及实时数据与宕机主机保持完全一致。系统中实时处理服务在热备方案的支持下健壮运行，该机制经过了专家论证和现场考验，得到了用户肯定。

（下转第 239 页）