doi: 10.3969/j.issn.1006-1576.2012.07.017

基于云计算理念的分布式仿真容错系统

范希辉，刘萍，崔逊学，吴海兵
（陆军军官学院二系，合肥 230031）

摘要：为提高分布式仿真系统的容错性，满足广域网环境下大规模作战仿真的需要。分析了云计算中的节点失效常态化理念，提出了基于多服务器的分布式仿真容错网络模型，重点对其中的错误恢复策略进行了研究，包括基于租约的客户端错误恢复、基于心跳的数据服务器错误恢复以及基于日志的主控服务器错误恢复。设计并实现了分布式仿真容错原型系统。测试结果表明：该系统能有效提高分布式仿真系统的容错性，对于实现云计算与高层体系结构的结合，提高仿真系统的鲁棒性具有一定的参考价值。

关键词：云计算；分布式；仿真；容错；高层体系结构
中图分类号：TJ02　　**文献标志码**：A

Distributed Simulation Fault Tolerance System Based on Concept of Cloud Computing

Fan Xihui, Liu Ping, Cui Xunxue, Wu Haibing
(*No*. 2 *Department*, *Army Officer Academy*, *Hefei* 230031, *China*)

Abstract: For improving the fault tolerance of distributed simulation systems and meeting the need for large-scale combat simulation under (wide area network) WAN. analyzed the concept of cloud computing node failure normalization, the distributed simulation fault tolerance network model based on multi-server was presented, focused on the error recovery strategy especially, including the lease-based client error recovery, the heartbeat-based data server error recovery, and the log-based master server error recovery. Designed and implemented a prototype fault-tolerant system of distributed simulation, results show that the system can improve the fault tolerance of distributed simulation system effectively. This research has a certain reference value to achieve the combination of cloud computing and high level architecture (HLA), and can improve the robustness of simulation system.

Key words: cloud computing; distributed; simulation; fault tolerance; HLA

0　引言

基于网络的分布式作战仿真，已成为训练模拟系统发展的趋势。随着仿真成员的增加和仿真规模的扩大，特别是当高层体系结构(high level architecture，HLA)扩展到广域网应用之后，仿真系统出现故障的概率也越来越高。在仿真系统运行过程中，如果某个关键仿真进程/仿真节点崩溃，将会导致整个仿真系统停止运行，而仅仅重新启动崩溃的仿真进程/节点又会导致系统状态不一致，这时唯一的方法就是重启整个仿真系统，这会对人力、物力资源造成极大浪费并可能引发严重后果[1]。在大规模的分布式作战仿真中，数据传输错误、服务器瘫痪、网络故障等意外情况很多，如何对这些情况进行及时有效的处理，提高系统的容错性，是大规模分布式仿真系统必须解决的关键问题。云计算将节点失效视为常态，并采用多种方法，从多个角度，使用不同的容错措施，以不被信任的服务器为用户提供值得信任的服务[2]。因此，笔者借鉴云计算的容错理念，对分布式仿真系统的容错机制进行了设计，给出了一个初步的解决方案。

1　分布式仿真容错研究现状

目前，分布式仿真多采用 HLA 规范，但现有的 HLA 规范除了预定义的异常处理机制能提供一定程度上的可检测性之外，并没有涉及到正式的失败处理模型和容错技术。新一代的 HLA Evolved 标准[3-6]在接口规范描述中增加了容错相关的通知服务，发生异常的联邦成员可以被移出联邦，其他已加入成员将会收到相应的通知，从而产生可以预期的仿真结果，如图 1 所示。但是这些都还停留在理论工作和标准制定的层次上，还未看到其具体的应用。当前主流的 RTI 软件(如 DMSO RTI，pRTI，MAK RTI 等)都没有提供容错技术支持。

从容错逻辑实现上来看，容错系统与仿真系统存在独立、完全融合、部分融合关系[7]，从已有的

收稿日期：2012-02-01；**修回日期**：2012-02-28
基金项目：国家自然科学基金“远场声源定位的短基线传感器网络关键问题研究”(61170252)
作者简介：范希辉(1979—)，男，山东人，博士研究生，讲师，从事网络化仿真、传感器网络、网络安全研究。

研究看，通常采用部分融合模型，即在基于 HLA 的分布式仿真系统的基础上，进行容错处理。从设计角度看，容错系统通常包括状态监控、数据保存和错误恢复 3 个模块[1,8]，如图 2 所示。

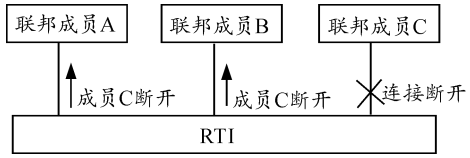

图 1 HLA Evolved 容错处理

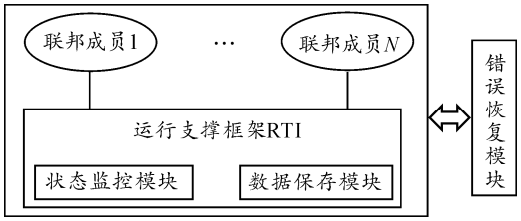

图 2 带容错功能的分布式仿真系统设计

从关键技术方面看，容错研究所涉及到的关键技术主要包括故障检测、冗余备份和错误恢复等，其中错误恢复是容错研究的难点，并且一直没有得到很好地解决[7]，特别是对于大规模的分布式仿真来说，意外情况很多，错误恢复研究尤为重要。

2 云计算节点失效常态化理念

云计算是并行计算(parallel computing)、分布式计算(distributed computing)和网格计算(grid computing)的发展，具有超大规模、高可靠性、通用性、高可扩展性和按需服务等特点，使得用户能够通过网络按需获取计算力、存储空间和信息服务。由于云计算平台中服务器数量规模巨大，出现某个节点失效的概率非常大。云计算主要创新之一就是将服务器作为一种不稳定系统对待，在系统架构时就将节点失效考虑进去，服务器的失效被作为是系统的一个常态，而不是异常，云计算能以不被信任的服务器为用户提供值得信任的服务[9]。如 Google 就采用大量低档服务器代替价格昂贵的高档服务器，既降低了服务器成本，又通过解决节点失效问题保证了服务的质量。云计算提供了完善的冗余备份和故障恢复机制，采用了副本存放、文件分割、错误恢复、数据完整性检测、快照等策略，通过对所有节点进行有效监控和协调，及时对节点失效故障做出迅速的报警，并将故障的详细情况向管理节点汇报，做出相应的数据和计算迁移操作，保证系统的连续运行，确保了在故障情况下数据存储的可靠性[2]。将云计算的节点失效常态化理念应用于分布式仿真系统，将有效提高仿真系统的容错性。

3 基于云计算理念的分布式仿真容错设计

云计算是分布式计算的一种，与分布式仿真在网络架构、资源管理等方面存在很多共同之处。笔者借鉴云计算的理念，重点从错误恢复策略方面对分布式仿真系统进行容错设计。

3.1 基于多服务器的容错网络模型

分布式仿真系统采用的网络模型主要有分布式、集中式和多服务器结构，多服务器结构集合了分布式和集中式的特点，具有集中控制的优点，并且将整个系统的负载分配到多台服务器，由多台服务器通力合作为客户端提供服务，具备更好的可扩展性和负载能力。

在分布式仿真系统的容错设计中，笔者借鉴云计算的容错理念，采用基于多服务器的网络模型，并按功能将服务器划分为主控服务器、数据服务器和备用主控服务器。其结构如图 3 所示。

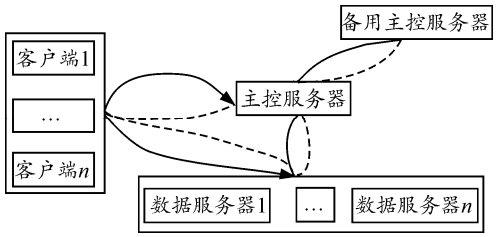

图 3 基于多服务器的容错网络模型

从图 3 可以看出，多服务器采用主从结构的体系。其中，主控服务器负责管理仿真系统的元数据，维护系统的命名空间并协调客户端对文件的访问，记录命名空间内的任何改动或命名空间本身的属性改动。数据服务器用于存储实际的数据，负责它们所在的物理节点上的存储管理，处理客户的读写请求，并依照主控服务器的命令，执行数据块的创建、复制、删除等工作。客户端联系主控服务器以获取组成文件的数据块的位置列表，而真正的文件 I/O 操作是直接和数据服务器进行交互的，主控服务器不参与文件的传输。容错系统典型的部署是在一台专门的机器上运行主控服务器，集群中的其他机器各运行一个数据服务器；也可以在运行主控服务器的机器上同时运行数据服务器，或者一台机器上运行多个数据服务器。为防止主控服务器出现意外，容错系统还设置有备用主控服务器。基于多服务器的容错网络模型具有良好的可扩展性，可满足大规模分布式仿真系统的需要，并且由于主流的 RTI 也是采用基于多服务器的网络模型，因此这样的容错

设计能很容易与现有的分布式仿真系统相结合。

3.2　基于多服务器网络模型的错误恢复策略

在基于多服务器的容错网络模型中，客户端、数据服务器、主控服务器都有可能失效，对于它们的失效应采取不同的错误恢复策略。

3.2.1　基于租约的客户端错误恢复

客户端出现故障通常影响不大，但当客户端在写文件的时候，一旦出现故障，如果主控服务器不能得知，就无法将这个文件的享用权分配给其他客户端。可采用基于租约的策略来解决这个问题。所谓租约，就是当客户端需要占用某文件的时候，与主控服务器签订一个短期合同。这个合同有一个期限，在这个期限内，客户端可延长合同期限，一旦超过期限，主控服务器会强行终止此租约，将这个文件的享用权，分配给其他客户端。当客户端需要写文件的时候，它需要申请一个租约。主控服务器负责记录哪个文件上有租约，租约的客户是谁，是否有租约到期等。客户端会定时轮询续签租约，主控服务器会轮询检查所有租约，查看是否有到期未续的租约。如果正常，该客户端完成写操作，会关闭文件，停止租约，一旦有所意外，如文件被删除，客户端瘫痪，主控服务器会停止此租约，以此来避免由于客户端停机带来的资源被长期霸占的问题。

3.2.2　基于心跳的数据服务器错误恢复

相比客户端，数据服务器是一个更不稳定的因素。一旦某数据服务器瘫痪，并且主控服务器不能得知，主控服务器就会变相地欺骗客户端，给它们无法连接的读写服务器列表，导致它们无法工作。因此，为了仿真系统的稳定，数据服务器必须时刻向主控服务器汇报，保持主控服务器对它们的完全了解。解决这个问题，可采用基于心跳消息的策略。

主控服务器周期性地从集群中的每个数据服务器接收心跳包，收到心跳包说明该数据服务器工作正常。在心跳包中，数据服务器会将其整体运行状况告知主控服务器，比如：有多少可用空间、用了多大的空间等。主控服务器会记住此数据服务器的运行状况，以作为新的数据块分配或是负载均衡的依据。主控服务器会标记最近没有心跳的数据服务器为死机，不会发给它们新的 I/O 请求。任何存储在死机的数据服务器的数据将不再有效，数据服务器的死机会造成一些数据块的副本数下降并低于指定值。主控服务器会不断检测这些需要复制的数据块，并在需要的时候重新复制。重新复制的引发可能有多种原因：数据服务器不可用、数据副本的损坏、数据服务器上的磁盘错误或者复制因子增大等。

3.2.3　基于日志的主控服务器错误恢复

作为整个系统的核心和单点，主控服务器一旦出现故障，整个分布式系统将彻底瘫痪。如何在主控服务器出现故障后，启用新的主控服务器并迅速使其进入工作角色，就成了系统必须考虑的问题。可以采用基于日志的策略来解决这个问题。

在主控服务器上，所有对文件目录操作的关键步骤都会被写入日志。另外，主控服务器会在某些时刻，将当下的文件目录完整的序列化到本地，称为镜像。一旦存有镜像，镜像前期所写的日志和其他镜像，已不再需要。事务日志和映像文件是系统的核心数据结构，都存储在主控服务器的本地文件系统。主控服务器启动时，它将从磁盘中读取映像文件和事务日志，把事务日志的事务都应用到内存中的映像文件上，然后将新的元数据刷新到本地磁盘的新的映像文件中，这样可以截去旧的事务日志，这个过程称为检查点。一旦主控服务器出现故障，或者是停机修整结束，并重新启动后，主控服务器会根据最近的镜像与镜像之后的所有日志，重建整个文件目录，迅速将服务能力恢复到之前的水准。对于数据服务器而言，需要通过一些手段，迅速得知主控服务器的更迭消息，并立刻到新的主控服务器进行注册，开始向其发送心跳消息，这个机制，通常用分布式协同服务来实现。备用主控服务器作为主控服务器的替补，主要功能是辅助主控服务器处理映像文件和事务日志。主控服务器只有在启动阶段才合并映像文件和事务日志，备用主控服务器将定期从主控服务器上复制映像文件和事务日志到临时目录，合并生成新的映像文件后再重新上传到主控服务器，主控服务器更新映像文件并清理事务日志，使得事务日志的大小始终控制在某个特定的限度下。当主控服务器出现故障的时候，运行备用主控服务器的服务器会立刻来代替，在其上启动主控服务，利用其日志和镜像，恢复文件目录，并逐步接收各数据服务器的注册，最终取代主控服务器向外提供稳定的服务。

值得一提的是，在日志的保存策略上，也可在本地保存的同时书写网络日志，在备用服务器上生成同样的日志，这样就确保了备用主控服务器的状态与主控服务器完全同步，缩短了间歇期，但执行效率有所降低，实现起来难度更大。 （下转第 71 页）