计算机科学2003Vol.30№.9

网格监控系统研究

黄达明　李国东　张德富
（南京大学计算机软件新技术国家重点实验室　南京210093）

Research on Monitoring System for Grid

HUANG Da-Ming　LI Guo-Dong　ZHANG De-Fu
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

Abstract The monitoring system is very critical for complex and large high-performance distributed system such as a Grid. With the help of a monitoring system the users and developers of a Grid can perform tasks such as fault-detection and diagnosis, performance analysis and tuning and performance prediction. And a good monitoring system can give useful data to the scheduling module of the Grid. This paper gives a detailed presentation and analysis of the key techniques of a grid monitoring system, and points out the research directions of the grid monitoring system based on current research around the world.

Keywords Grid, Monitoring, GMA, MDS

1. 引言

网格是以资源共享为目的，支持对可计算资源的远程和并发访问，用高速网络连接的地理上分布的可计算资源所组成的一个具有单一系统映像的高性能计算和信息服务环境。网格系统具有可扩展性、异构性、多级管理域、动态性等特征。这是由于网格是由分布在不同地理位置的不同管理域的资源组成，资源可能随时加入，也可能随时因失效或自愿等原因退出。

网格的用户和开发人员经常需要监控系统的运行状态以发现未知的性能问题，从而及时发现故障的根源，分析系统性能瓶颈，在最短时间内恢复或调整系统。但是对于网格这样复杂的高性能分布式系统，跟踪发现性能问题的根源是非常困难的。这是由于在网格中分布式系统组件之间的交互是复杂，而且常常是间接的。瓶颈和性能问题可以发生在数据流经的途径的任何一个组件上，可以是应用、中间件软件、操作系统、设备驱动程序、网卡或者网络设备如路由器和交换机等，更有一些问题牵涉到组件之间的交互，而这些交互是不可预知、难以捕捉和难以重复的。

因此监控系统对于网格来说是非常重要的：网格的监控数据可以用来判定性能问题的根源从而可以调整系统和应用以达到更好的性能；错误检测和恢复机制也需要监控数据来判断是否一项服务已经崩溃以及是否需要将用户请求导向备用系统；性能预测服务也要使用监控历史数据来调整预测服务，为网格的动态负载平衡策略提供可靠的依据。

现有的集群系统的监控系统并不能适应网格系统的需要，因为集群系统往往是属于某一个管理域，在地理上比较集中的。而现有的一些中大规模的网络监控系统也是不适应网格系统需要的，因为网络监控只是网格监控的一个部分，它们并不能监控网格复杂的其它组件。所以开发专门的网格监控系统是近几年来网格研究的热点之一[1~20]，有不少网格系统项目已经开发出了相应的监控系统或相应的监控基础设施[2~13,16,17]，还有一些组织在进行网格监控的标准化工作[19,20]，这些都将在下面一一介绍。

2. 网格监控系统

一个网格监控系统必须是安全、可扩展的，可以在最小消耗系统资源情况下收集监控数据，高带宽低延迟地传输监控数据，以及有效地利用监控数据[1]，下面我们将从技术上对网格监控系统的各个方面做出阐述，包括监控对象、事件和数据格式，体系结构，监控数据的传输，监控数据的分析利用以及网络时间。由于监控对象、事件和数据格式是基础，因此先进行阐述，而由于体系结构的重要性，将进行重点阐述。

2.1 监控对象、事件及数据格式

在网格中性能问题可能发生在网格的任一个组件上，如应用、操作系统、网卡、网络设备等，要发现问题就要对这些组件进行监控，获取必需的监控数据。这样，网格中需要掌握必需的运行状态信息的组件就叫做监控对象。监控对象可以按计算机体系结构分为三类，即(1)系统类，主要指CPU利用率、主机负载等主机硬件资源；(2)网络类，主要指网络带宽、路由情况等网络资源；(3)应用类，指在网格中运行的应用，包括各种类型的服务器，客户程序等[12]。

要了解监控对象的状态信息，就要在这些对象运行的关键时刻或者这些对象状态发生变化的时候发出通知，或者按照一定的时间间隔报告这些对象的状态，这就是事件。一般来说，对系统类对象，可以通过在系统中安装一些本地的传感器程序来监视这些对象，当这些对象的状态发生监控系统感兴趣的变化，或者超过一些预定的阈值的时候，这些传感器程序就产生相应的事件；对于网络类对象，可以通过一些网络管理工具或者在网络设备上运行的一些特定的传感器程序来监视它们，在发生变化或者异常的时候产生相应的事件，或者按照一定时间间隔执行网络中端到端的测试，产生网络监控对象

黄达明　硕士研究生，主要研究方向为并行计算与分布式系统。李国东　硕士，主要研究方向为并行计算和分布式系统。张德富　教授，博士生导师，主要研究方向为并行处理技术和分布式系统。

的性能信息，比如端到端的带宽、延迟等；而对于应用类对象，通过传感器程序无法进行有效的监控，一般都是通过在这些应用的关键运行点嵌入一些产生事件的 API，比如在一个读或者写操作开始和结束的时刻，这些 API 一般通过库的形式提供，和应用编译链接起来。需要指出的是，对于需要按照定时产生的事件，这个时间间隔是可以改变的，在系统运行平稳的时候，可以周期长一些；而系统运行状态变化较大时，可以频率高一些。这方面的研究见文[2,3,5～7,9～11]。

事件要传送到相应的地方供监控系统分析利用，这需要一个数据格式。这方面大多数系统都采用了 IETF 的通用日志消息格式 ULM(Universal Logger Message Format)。这是一个 ASCII 文本格式，易于分析处理，也易于第三方软件的利用，从而提高了互操作性。但由于这是文本格式的，因此产生的数据量比较大，这增加了系统负荷，降低了网络传输效率，所以有些系统进行了使用二进制事件格式的研究，如采用 SDDF(Self-Defining Data Format)，这样可以在降低系统负荷，增加网络传输效率的基础上提供更好的监控粒度，当然，在分析和处理时效率就差一些。

2.2 体系结构

目前网格监控系统体系结构方面主要有两种选择，一个是 Globus 项目中所使用的监控和发现服务 MDS(Monitoring and Discovery Service)[2]，另一个是全球网格论坛 GGF(Global Grid Forum)提倡并致力于标准化的网格监控体系结构 GMA(Grid Monitoring Architecture)[1]。

2.2.1 MDS MDS 体系结构主要是用于发现、刻画和监控网格中的资源、服务和计算等，提供有关资源的一切信息，包括资源的静态信息和动态信息，是 Globus 项目的三大支柱技术之一。

MDS 主要由可配置的信息提供者组件 GRIS(Grid Resource Information Service)、可配置的聚合目录组件 GIIS(Grid Index Information Service)以及网格信息协议 GRIP(GRid Information Protocol)、网格注册协议 GRRP(GRid Registration Protocol)组成，如图1所示。

GRIS 可以提供关于网格中一个或多个资源实体的信息，它通过一个良好定义的 API 与更本地的信息提供者如传感器等通信，获取资源信息。一个 GRIS 可以通过 GRRP 协议向一个或多个 GIIS 表示它的存在，即注册，一个 GIIS 在获知一个 GRIS 存在的情况下，也可以通过 GRRP 协议邀请这个 GRIS 加入。一个 GIIS 可以向更上层的 GIIS 注册，从而构成层次型的结构，这与网格是由一个个机构、团体或者说虚拟组织 VO(Virtual Organization)组成是一致的。GRIS 协议用来发现资源和查询资源的情况。

在用于监控系统时，监控数据可以通过向 GRIS 或者 GIIS 查询或者订阅得到。在从 GRIS 获取资源监控数据时，GRIS 可以分析并分解查询给各个本地信息提供者，由本地信息提供者直接提供监控数据，也可以通过 GRIS 的综合过滤后再返回监控数据。从效率考虑，GRIS 会缓存所代理的资源的信息数据，只要商量好的生命期未过，就认为这些数据是有效的，从而可以大大提高查询的效率。GIIS 可以提供一个资源的特殊的视图，通过它和底层 GIIS 及 GRIS 的商量(通过 GRRP)，它可以提供有关资源某一方面的信息，与 GRIS 一样，GIIS 可以分解查询由底层组件返回资源信息，也可以综合信息后返回，从效率考虑，GIIS 也会缓存信息数据。

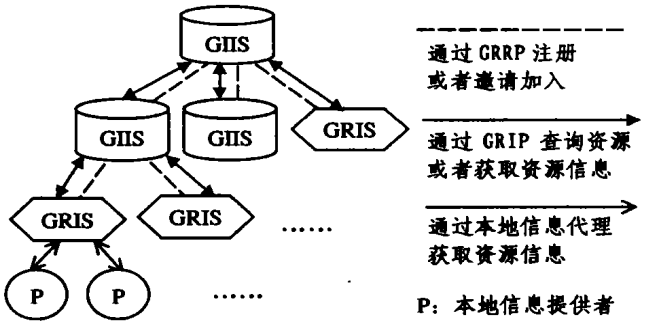

图1 MDS 体系结构

目前比较典型的采用 MDS 的监控系统是英国 Portsmouth 大学正在开发和试验的网格监控系统 GridRM 的原型系统，见文[16]。

2.2.2 GMA GMA 体系结构只有三个组件：生产者、消费者和目录服务，如图2所示。

在 GMA 中，最基本的监控数据叫做事件，一个事件是一个命名的、带时间戳的可能包含一个或多个数据项的结构。构成事件的数据可能是从多个源收集来的，比如硬件或软件传感器所测量采样的性能数据，面向应用的数据以及对历史数据的查询等。

一个生产者提供监控事件数据。它响应消费者的请求并发送监控事件数据给消费者。生产者通常在目录服务中注册它所能提供的监控事件数据。为了发现需要它能提供的事件数据的消费者，生产者也可以搜索目录服务来发现相应的消费者，然后传送相应的监控事件数据。一个消费者请求生产者并接收监控事件数据。为了发现能提供自己所需事件数据的生产者，消费者可以搜索目录服务。一个被动的接收事件数据的消费者也可以向目录服务注册自己所需要的事件数据，这样相应的生产者可以通过搜索目录服务发现它并向它提供数据。目录服务提供信息发布和发现，出于性能考虑，目录服务仅仅包含监控事件的元数据以及这些数据相关联的生产者和消费者的映射，并不存储监控事件数据本身。

GMA 体系结构支持生产者和消费者之间的三种交互模式：发布/订阅、查询/响应以及通知。在发布/订阅模式中，初始发起者(可能是生产者也可能是消费者)和对方联系指明感兴趣的事件，然后生产者通过一条持久稳固的通道向消费者发送性能事件数据，直到生产者或者消费者中某一方终止订阅为止。在查询/响应模式中，初始发起者只能是消费者，它向生产者请求感兴趣的事件，然后生产者在一个单独的回答中传送所有的性能事件数据给消费者。在通知模式中，发起者是生产者，生产者在一个单独的通知中向相应的消费者传送所有的性能事件数据。

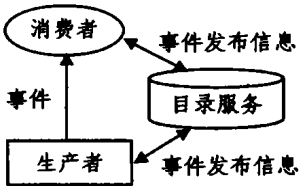

图2 GMA 体系结构

生产者和消费者可以组合起来构成一个生产者/消费者管道，如图3所示。这可以用来过滤或者聚合数据。比如，一个

消费者可以从多个生产者收集数据，然后使用这些数据产生新的派生的数据类型，再发送给其它的消费者使用。也可能一个消费者只对大量性能事件中的某一些感兴趣，比如某项性能超过某个阈值的事件，这也可以通过生产者/消费者管道实现。

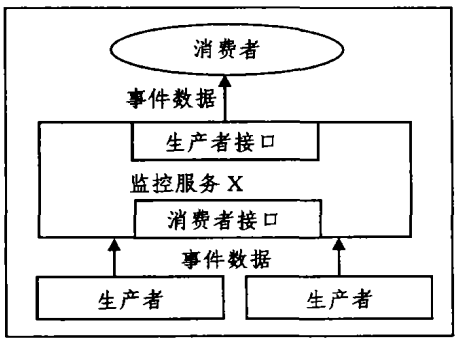

图3 生产者/消费者管道

GMA 体系结构通过将数据发现和数据传输分离，使得生产者和消费者之间通过需求协商可以做到匹配，系统中传输的数据可以精确地和本地模式的控制，还允许事件数据的复制和精简，从而达到网格监控系统所要求的监控数据传输的低延迟、高传输率、低负载和安全性，也使得网格监控系统非常易于扩展。

目前有不少监控系统已经采用了或在工作中融入了 GMA 模式，见文[3,4]，及正在使用 GMA 模式[17]。

2.2.3 *两者的结合* 由于 Globus 工具集被众多的网格项目采用作为基础，已经成为事实上的工业标准，因此 MDS 也获得了广泛的应用，更被 GGF 采纳作为网格信息服务 GIS(Grid Information Service)的基础设施之一而标准化，又称为元计算目录服务 MDS (Metacomputing Directory Service)。GMA 是对构筑一个可扩展的监控系统的组件的抽象描述，并没有规定具体的实现细节，它是在许多工作的基础上发展而来的，当然也包括 MDS。MDS 与 GMA 在信息的发现和监控数据的传输方面有不同的地方，而一些专家(如 Ian Foster 等)认为可以使用 MDS 获取相对静态的信息而使用 GMA 来获取高度动态的信息，当前的网格监控系统，有可能采用两者的结合，即在 MDS 的基础上构筑 GMA 模式的监控系统。

2.3 监控数据传输和存储

为了对网格进行有效的监控，随时都可能会有大量的监控数据产生，对这些数据进行有效安全可靠的传输和利于处理的存储是非常重要的。

由于网络的状况随时可能变化，因此要求将监控数据及时地送给即时分析工具或者历史数据库有时是办不到的；而监控的特殊性质使得监控数据可能突然性地暴涨，这样发送端和接收端的速度匹配也是一个重要的问题。现行系统的一般做法是使用缓存。在监控事件的产生地，将监控数据先收集并存储到本地磁盘上，然后由专门的程序负责从磁盘中读取数据发往网络上的目的地；在网络的另一边，由专门的程序负责从网络接收数据，同样也存储到本地磁盘，然后再从磁盘中读出监控数据传给分析工具或者存入监控数据历史数据库。这样，通过在网络两边磁盘上的缓存，可以做到速度匹配，后来的数据不会淹没前面没有来得及发送或处理的数据；而由于网络状态不理想没来得及发送的数据也不会丢失，由于数据带有时间戳，因此即使有延迟也不会影响正确性。为了容错，在网络或目的地系统出现问题的时候，可以将监控数据发往一个备份目的地，当原来系统恢复后，再将数据重新发往那里，而备份系统中的数据也可以有选择地复制给主目的地系统。这方面具有代表性的工作有文[4,6,7,9]。

对监控数据的存储，目前大多数系统采用的是 LDAP 目录服务。但是，取决于要分析的应用和系统，可能需要即时的、几天的甚至几个月的历史数据。性能的突然变化可能与其它变化有关，也可能在过去周期性地出现。为了发现问题，用户需要能够从各个不同的角度来观察整个历史数据集合。而 LDAP 不支持"jion"操作，这样就不能对监控数据进行有效的分析和利用。现在不少系统都倾向于使用关系型数据库来构造监控系统的数据存储库。这方面具有代表性的工作有文[4,9]。

2.4 监控数据分析和利用

要发现系统的性能问题，就要对监控数据进行及时有效的分析；而要对系统的性能作出评价和预测，还要对大量的监控历史数据进行有效的分析。所以分析工具起着十分关键的作用。

目前对监控数据的可视化分析工具主要通过对监控数据的分析，提供下面几种图形来描绘一个网格系统应用的运行：(1)生命线，表示一个数据对象或计算对象在分布式系统中各个组件上所花的时间，从而可以看出时间主要是花在哪个组件上了；(2)负载图，可以有效地看出系统监控对象的负载情况，比如 CPU 利用率、网络带宽等；(3)点图，可以看出一个事件的发生频率或者数据传输率等。现在一些工作提供了可视化分析工具如 NetLogger[6,7]，visPerf[11]，PROVE[10]。

除此之外，美国 Argonne 国家实验室还开发了 GridMapper 工具[8]，可以在一幅电子地图上有效地展示一个 Grid 系统的资源和网络连接情况，清晰地观察数据在网络中的传输过程，从而可以直观地看出系统中性能问题的发生地。

除了供发现性能问题和恢复错误外，监控数据还被用来进行性能预测，从而可以供某些调度策略使用。可以将监控数据集输入多种预测模型，产生不同的预测数据，然后结合实际使用，采纳最优和最准确的预测模型和预测结果，如 NWS[9]。

2.5 网络时间

网格是一个大规模、地理上分布很广的分布式系统，监控数据的传输可能会有很大的延迟，所以需要给事件数据加上时间戳来保证数据的有效性。为了分析从网格中各个组件获取的带有时间戳的事件数据，需要有比较精确的同步时钟。目前比较好的也是比较普遍的做法是在网格中每个子网里安装基于 GPS 的网络时间协议(NTP)服务器，在子网的每台主机或设备里运行支持 NTP 协议的工具，比如 xntpd 守护进程。采用这种方法，每个子网里主机的时钟可以同步到0.25ms 之内，如果主机或设备离时间源比较远，比如有几个 IP 路有跳跃，那么时钟同步精度会有所下降，但是对绝大多数的分析工作而言，1ms 的同步精度已经是足够用了。

3. 相关工作

目前有很多网格项目在实验和部署之中，其中有很多都开发了网格监控系统或者网格监控工具。比较具有代表性的有以下一些。

(1) 美国 Lawrence 国家实验室 LBNL 开发的网格监控系统。在事件的产生，收集，传送、存储和分析结果方面都做得

非常好。这个系统是基于 GMA 和 NetLogger 工具集[6,7]的，包括四个组件：一个应用监视组件，产生监控事件数据；一个监控激活服务，用来触发监控服务、收集和传送事件数据；一个监控事件接收组件，接收网上传来的事件数据；一个数据库伺服器，将事件数据转换成 SQL 记录并存入数据档案库，这是一个关系型的数据库。具体工作可以见文[3,4]。而 LBNL 在产生事件的传感器系统设计方面也作了很好的研究，具体工作请见 JAMM(Java Agents for Monitoring and Management)系统[5]。

(2) 美国 Argonne 国家实验室的 GridMapper 工具。这个网格监控工具在大规模分布式系统的工作状态和资源状态的可视化方面做得非常好，不但可以直观地显示和应用关联的网络交通情况，还可以显示和应用关联的计算活动状态及资源状态。它的最独到之处是可以按实际的地理位置显示系统活动和状态图。具体工作请参见文[8]。

(3) 美国加州大学 San Diego 分校和田纳西大学等单位联合开发的网络天气服务 NWS(Network Weather Service)。在监控数据产生、收集方面有自己的一套，最具特色的贡献就是使用监控数据进行了性能预测，为调度等工作提供了有力的支持。具体工作请见文[9]。

(4) 在欧洲最大的网格项目 DataGrid 项目中进行的使用 GRM 和 PROVE(PROtotype Validation Exercise)工具组成网格监控基础设施的研究。GRM 和 PROVE 原来是 P-GRADE 图形化并行程序开发环境的组成部分。P-GRADE 在并行程序的监控和调试方面作了很多工作。现在改进 GRM 和 PROVE 来进行网格监控也取得了一定的成绩。GRM 是监控信息采集和传送工具，而 PROVE 是分析和可视化工具。使用 GRM 和 PROVE 在数据缓存、数据传输效率、扩展性以及错误定位精度方面都比 NetLogger 工具集有一定优势，具体工作请见文[10]。

(5) 美国田纳西大学和韩国 Kwangju 科技研究所共同开发的 VisPerf 监控工具，在传感器程序、监控数据采集和传输以及可视化分析方面都做了自己独到的工作，还在监控数据穿越防火墙方面做了一定的研究，具体工作请见文[11]。

(6) 由中科院计算所和北京理工大学等单位合作开发的 GridMon 网格监控系统，建立了网格的树状基本结构，实现了全局监控和局部监控的分离，是中国网格监控研究的代表。具体工作请见文[12]。

(7) 英国 Portsmouth 大学的 GridRM 项目，在原型阶段采用了 MDS 模式[16]，后期扩展为 GMA 模式，具体工作见文[17]。

4. 未来工作

目前国际上主要有两大组织在进行网格监控系统的标准化工作，一个是 GGF 的性能工作组，另一个是欧洲 DataGrid 项目的 WP3小组。GMA 体系结构是未来网格监控系统的必然选择，但是由于具体实现的不同，因此监控系统之间的或操作性是研究的方向之一。互操作性问题必然牵涉到数据格式问题，目前广泛采用的 ASCII 格式是 ULM，虽然有些单位开发了自己的二进制格式，但是并没有得到广泛的使用；使用 XML 也是选择之一，但是 XML 表示的冗繁使得效率是个问题，这方面需要更多的研究。增加关系数据模式和在监控系统中使用关系数据库也是必然的趋势，这方面的研究可以参见 R-GMA[14,15]。随着 Web 服务的普及，Web 方式使用网格监控系统也是趋势之一，使监控服务以 Web 服务的方式出现的研究已有一些工作在做，包括使用 SOAP 做为控制流等。网格监控和网格信息服务是分不开的，在存取控制、认证等安全方面仍有很多工作要做。还有就是更高效率地采集监控数据，如何在尽可能小的影响系统的基础上提供更高粒度的监控始终是研究的方向。

结论 监控系统对于网格来说是非常重要的，通过监控系统可以进行错误监测和分析，性能分析和调整，性能调整以及为调度提供有力的依据。本文对网格监控的目的、目标和要求做了介绍，从技术角度对网格监控系统的各个方面进行了阐述，并对目前网格监控研究的现状做了介绍，最后提出了网格监控系统未来研究的方向。

参 考 文 献

1 Tierney B, Aydt R, Gunter D, et al. A Grid Monitoring Architecture. In: Performance Working Group of Global Grid Forum, 2002. http://www-didc.lbl.gov/GGF-PERF/GMA-WG/papers/GWD-GP-16-3.pdf

2 Czajkowski K, Fitzgerald S, Foster I, Kesselman C. Grid Information Services for Distributed Resource Sharing. In: Proc. of the 10th IEEE Intl. Symposium on High Performance Distributed Computing(HPDC-10), IEEE Press, 2001

3 Gunter D, Tierney B, Jackson K, Lee J, Stoufer M. Dynamic Monitoring of High-Performance Distributed Applications. In: Proc. of the 11th IEEE Symposium on High Performance Distributed Computing, July 2002

4 Lee J, Gunter D, Stoufer M, Tierney B. Monitoring Data Archives for Grid Environment. In: Proc. of IEEE Supercomputing 2002 Conf. LBNL-50216, 2002

5 Tierney B, Crowley B, Gunter D, Lee J, Thompson M. A Monitoring Sensor Management System for Grid Environments. In: Proc. of the IEEE High Performance Distributed Computing Conf. (HPDC-9), Aug. 2000

6 Tierney B, et al. The NetLogger Methodology for High Performance Distributed Systems Performance Analysis. In: Proc. of IEEE High Performance Distributed Computing, July 1998. 28～31

7 Gunter D, Tierney B, Holding M, Lee L. NetLogger: A Toolkit for Distributed System Performance Analysis. In: 8th Intl. Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, Francisco, California, 2000. 267

8 Allcock W, et al. GridMapper: A Tool for Visualizing the Behavior of Large-Scale Distributed Systems. In: 11 th IEEE Intl. Symposium on High Performance Distributed Computing HPDC-11 20002 (HPDC'02) P. 179

9 Wolski R, Spring N T. Hayes J. The Network Weather Service: A Distributed Resource Performance Forecasting Service for Metacomputing. Future Generation Computing Systems, 1999. http://nws.npaci.edu/.

10 Balaton Z, Kacsuk P, Podhorszki N. From Cluster Monitoring to Grid Monitoring Based on GRM and PROVE. Euro-Par, 2001. 874～881

11 Lee D W, Dongarra J J, Ramakrishna R S. VisPerf: Monitoroing Tool for Grid Computing. Workshop on Grid Computing (submitted), Baltimore, MD, Nov. 2002

12 ZHA Li, XU Zhi-Wei, LIN Guo-Zhang, LIU Yu-Shu, LIU Dong-Hua, LI Wei. A LDAP Monitoring System for Grid. Journal of Computer Research and Development, 2002, 39(8)

13 Waheed A, Smith W, George J, Yan J. An Infrastructure for Monitoring and Management in computational Grids. In: Proc. of the 2000 Conf. on Languages, Compilers, and Runtime Systems, 2000

(下转第151页)

〈T,TIME〉,这里 TIME 等于初始化该表格时的系统时间。事务的排列次序是任意的。

2) 当事务 T_i 被执行后,运用〈T_i,new_time〉去替换旧的〈T_i,TIME〉,并且将这条记录插到事务队列的最前面,这里 new_ time 代表事务 T_i 的执行时间。

3) 设置该表的有效值 V=0,检查该表格的所有事务,如果(系统的当前时间)-(〈T_i,TIME〉中的 TIME)≤168小时(i=1,2,3,…),则 V=V+1;(这里168小时不是一个固定的值,我们需要根据具体情况调整这个值,在 EH_GRBAC 我们认为168小时内没有操作的事务是很少执行的事务)。

4) 当另一个事务执行后,重复步骤2) 和3)。

我们能够通过图3来表达知识库中表格的结构。

当一个请求通过了授权子系统,知识子系统将判断该请求是否属于相应的正常集,如果它属于正常集,该请求通过访问控制,反之,系统要求进一步的口令,如果用户能够提供正确的进一步口令,请求将通过访问控制,否则被拒绝。

5 相关工作

以下我们将介绍一些相关工作,并且将它们和基于知识的访问控制进行比较。

GRBAC:我们已经在第2节讨论了 GRBAC。GRBAC 通过三种角色的组合能够表达很多情况。但是在这种模式中,访问控制过程完全依赖于认证过程的结果。GRBAC 和基于知识的访问控制相结合能够克服单独运用 GRBAC 的缺点,为系统提供一定的安全容错功能。

上下文感知的访问控制:在文[4]中,Covington 讨论了上下文感知的访问控制,它主要是基于环境角色。而基于知识的访问控制是基于知识和规律。环境角色能够表达各种环境状态,但是知识具有更加广泛的含义,它不仅可以包含各种环境信息,而且包含各种从系统运行中总结出来的带有一定规律性的知识。

自适应安全模式:在文[5]中,Covington 通过参数化认证过程设计了一种能够提供自适应安全级别的模型。这个模型根据传感器的信息提供自适应的认证过程。这个模型和 EH_GRBAC 之间主要存在三个区别:首先,在 Convington 模型中,传感器提供的信息主要包括:用户生理信息、口令和识别卡等等,但是基于知识的访问控制策略中,知识不仅可以包括这些信息,而且包括诸如:用户习惯和访问趋势等动态信息。这些知识需要从以前的访问控制过程中进行发掘。特别地,convington 的模型在认证过程中引入了历史信息,但这种信息是指用户操作的上下文以及以前的认证请求。EH_GRBAC 中的历史知识是指从历史信息中总结出来的知识,例如:用户习惯、访问倾向等等。其次,在 Covington 的模型中,认证和访问控制是两个前后过程,但是,在基于知识的访问控制中,我们在访问控制中融入了认证过程。因此,基于知识的访问控制过程能够意识到通过了认证过程的假冒者的进攻,提供一定的安全容错性。第三,在基于知识的访问控制中,基于知识的认证功能不可以在认证阶段完成,因为用户的行为和访问倾向只能在访问控制的过程中才能表现出来。

小结 本文提出了一种新的访问控制策略:基于知识的访问控制策略。在遍在计算的环境中,因为个人的兴趣、行为习惯和工作内容,用户对资源的访问会表现出一定的规律。基于知识的访问控制策略正是利用这些知识和规律,在访问控制的过程中增加额外的认证功能。这种模式相对于传统的访问控制模式具有一些独特的优势:诸如个人兴趣、行为习惯等信息不容易被假冒者模仿,所以系统能够使用这些知识来提供安全容错功能。但是基于知识的访问控制模式不是一个完整的访问控制模式,它需要和传统的访问控制模式相结合来提供一个完善的安全系统。

参 考 文 献

1 张向刚,刘锦德. 多密钥 KDC 的安全容错性及其性能分析. 电子科技大学学报,2001,30(6): 596~599

2 Ferraiolo D,Kuhn R. Role-Based Access Control. In:Proc. of 15th National Computer Security Conf. 1992

3 Moyer M J,Ahamad M. Generalized Role Based Access Control. In:Proc. of the 2001 Intl. Conf. on Distributed Computing Systems (ICDCS), Oct. 2001

4 Covington M J,et al. Securing Context-Aware Application Using Environment Roles. In:Proc. of SACMAT, May 2001

5 Covington M J,Ahamad M,Venkateswaran H. Providing Adaptive Security through Parameterized Authentication. In:2002 IEEE Symposium on security and privacy, May 2002

(上接第147页)

14 Fisher S. Relational Grid Monitoring Architecture. http://hep-unx.rl.ac.uk/grid/wp3/release.html

15 Fisher S. Relational model for information and monitoring. GGF International Draft GWD-GP-7-1. http://www.gridforum.org/1_GIS/RDIS.htm

16 Baker M,Ong H,Smith G. A Prototype Grid-site Monitoring System. http://homer.csm.port.ac.uk/publications/technical/reports/grid/DSGmonitoring.pdf

17 GridRM Project. University of Portsmouths , U.K. http://homer.csm.port.ac.uk/projects/research/grid/grid-monitoring/

18 MDS 2.2 User's Guide. http://www.globus.org/mds/mdsusers-guide.pdf

19 Global Grid Forum Information Systems and Performance Area. http://www.gridforum.org/1_GIS/GIS.htm

20 European DataGrid wp3(Grid Monitoring Services) http://hep-unx.rl.ac.uk/edg/wp3/

21 查礼,徐志伟,林国瑾,刘玉树,刘东华,李伟. 基于 LDAP 的网格监控系统. 计算机研究与发展,2002,39(8)