关于构造一种易于访问和安全管理网格的研究*)

姜正涛　衣鹏超　王育民
(西安电子科技大学 综合业务网国家重点实验室　西安 710071)

摘　要　灵活有效地使用计算资源，是网格期望达到的一个重要目标，现有的对于网格方面的讨论主要集中于各个相互独立个体之间的资源共享。本文从多个相对独立的团体资源共享方面考虑，探讨了关于如何构造可灵活扩展的树型逻辑网格的一种方法。这种形式的网格易于搭建，方便资源的查询、访问和权限动态管理，同时能够和目前通用的分布式 PKI 技术很好地结合，有利于实现全局安全策略向局部的映射。

关键词　网格，树型结构，网格组织，灵活扩展，动态管理，网格安全访问，PKI，CAS

Research on Constructing a Form of Grid Easy to Visit and Secure to Manage

JIANG Zheng-Tao　YI Peng-Chao　WANG Yu-Min
(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　One of the primary goals of the grid is to employ the computational source with efficiency and flexibility. Present investigations on the grid mainly focus on sharing resource among independent units. Considering sharing resource among relatively self-governed organization, we provide a kind of method for constructing tree-type logic grid, which is flexible to expand. This form of grid is easy to put up and facilitate to inquiry, visit and management of resources. At the same time, it can better combine with distributed PKI technology and is easy to realize mapping the global security strategy to local.

Keywords　Grid, Tree-type structure, Grid organization, Flexible expansion, Dynamic management, Grid secure visitation, PKI, CAS

1　引言

网格被认为是下一代的 Internet，网格的目标是基于目前比较成熟的技术，对网络上跨多个管理域的各种资源充分共享，并支持资源之间的互操作[1,2]。

目前对于网格的讨论多是集中在独立分散的资源之间。实际上，网格中的大部分结点（如小型计算机、超级计算机）并不是孤立的，而是隶属于某个组织（如企业、学校等）的。在组织内部（如局域网内部），这些接点之间的通信只需满足内部的安全协议，并不需要跨组织的安全策略，所以这些接点之间的通信可以比同组织外部结点的通信更频繁、更直接[3]。

目前最有影响的两个网格模型，一个是 Ian Foster 等人提出的以"协议"为中心的五层沙漏结构，另一个在以 IBM 为代表的工业界的影响下，在考虑到 WEB 技术的发展与影响后，Ian Foster 等人结合 Web Service 提出的以"服务"为中心的"服务结构"[2]。这两个结构主要是把网格作为中间件，对网格的协议和服务分层。

本文从网格的易于组织和动态安全管理方面，结合网格中的查询、访问、完全、管理等机制对树型组织（如企业、学校等）网格的构造做了探讨，在此基础上对网格的团体认证模型做进一步的研究，使得网格的资源提供方可以以更细的粒度为用户授权，动态地统计并管理用户以及该用户对应的团体的权限。而且这种形状的网格，能够很好地满足从小型网格到大型网格直至国家网格的搭建过程要求，能够与目前分布式 PKI 技术很好地结合，有利于实现全局安全策略向局部的映射和基于问题解决的互操作。

2　网格中的安全问题

网格可以看成是一个中间件，负责把动态的用户和资源安全地连接起来，更好为用户提供服务。

网格中需要解决的问题主要有以下几点：

1. 网格安全；2. 网格信息获取与发布；3. 网格资源管理；4. 网格数据传输。

网格的使用过程中涉及多方面的安全问题[3~5]，处于网格中的资源和用户是动态的，这些资源和用户可能分别属于不同的利益团体之间，它们的行为不仅影响着自己的可信程度，同时不良的行为也会给所处的团体带来不良的影响。对于这些不良行为的管理，也是网格需要解决的一个问题。

本文对不同于以往的以"协议"为中心的"沙漏结构"和"服务结构"，把网格需要解决的问题尝试以树型结构的模型来解决，使得网格的信息获取、发布、资源管理以及网格安全问题就如同多棵平行并且彼此充分融合的树。根据"小世界模型"理论，这样的逻辑分级查询要比"平级询问"的方法快得多[6,7]，并且资源的信息主要存储在当地的支点服务器或叶点服务器上，缓解了对信息注册和发布服务器的过分依赖，使其更能有效地为用户提供资源信息服务[8]。

*)基金项目：国家 863 资助项目（2002AA143021）、国家自然科学重点基金资助项目（69931010）。**姜正涛**　博士研究生，主要研究方向为网格安全及相关技术、密码算法理论的研究与分析、通信网的安全等；**王育民**　教授、博士生导师，主要从事编码理论、密码学、信息安全等领域的科研与教学工作。

3 一种易于动态管理团体和用户权限的网格安全管理机制

3.1 一种树型的网格服务机制

设 A 某个企业的服务器，A_1，A_2，…是 A 下属部门的服务器，A_{11}，A_{12}，A_{13}，…，A_{21}，A_{22}，…为分别属于部门 A_1，A_2 的资源(如个人主机或计算机群)，通常用户与团体有如图 1 所示的隶属关系。

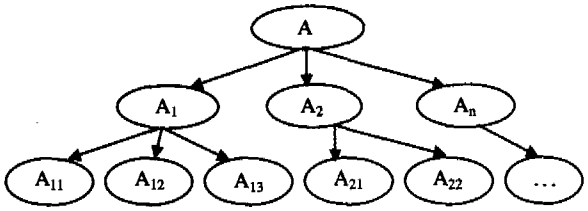

图 1 主体之间的逻辑关系

3.2 树型网格的信息发布与查询机制

当 A_{11} 正在进行计算工作时，就在 A_1 的任务列表中注明 A_{11} 的计算资源正在使用，并说明目前资源的使用或空余情况以及是否还可以同时运行其它任务。资源空置声明情况如表 1 所示。

表 1 资源空置声明

任务	计算	存储
主机	A_{11}，A_{13}	A_{12}
CPU 型号	Intel P4	Intel xeon
CPU 使用率	50%，30%	10%
内存空余	500M	3G
…	…	…

此外，A 拥有本组织资源的宏观描述，如表 2 所示。

表 2 组织 A 的资源

任务	计算	存储
主机	A_1	A_1，A_2
可使用资源数目	2	3
最大独立可使用资源(CPU)	70%	90%
最小独立可使用资源(CPU)	50%	30%
最大内存空余	500M	3G
最小内存空余	100M	200M
…	…	…

A 向外发布自己可提供的资源，如计算资源、存储资源等。

任务的分配过程如下：

(一)任务的提交过程：

1. 用户通过用户代理向网格提交自己的计算任务计划。

2. 网格服务器通过查询，得知组织 A 具有计算优势，就把任务交给 A。

3. 当 A 收到来自组织外部的计算任务时，便查询自己拥有的任务列表，根据计算任务的要求(如计算的速度等要求)，向具有计算优势的 A_1 或其它下属分发；如果任务包含多个子任务，A 就同时分发给下属部门，并修改自己目前的任务列表。

4. A_1 收到任务后，判断是大规模的计算还是一般计算。如果是大规模计算，就把任务交给性能较强的主机或机群；如果是一般的数学计算，就交给性能一般的主机。空闲的主机可以继续等待新任务的分发。

5. 在运行过程中，可能会需要一系列的中间结果，就通过 A_1(或 A_1，A)向其它主机索取。由于是在组织内部通信，不需要同外部通信那样严格地相互认证和协商密钥，提高了效率。

6. 如果在运行中，需要使用其它主机的计算或存储资源，就可以直接查询相临的主机或向 A_1 提出资源申请；如果 A_1 内资源不能满足要求，A_1 就代表申请的主机向 A 申请，A 通过自己拥有的任务列表及其下属部门找到 A_1 需要资源的并通知 A_1。

7. A_1 查询到或得到通知后就可以使用新发现的资源，并及时得到该资源的反馈信息或运算结果。

8. 待所有的计算结果完成后，组织 A 把整个组织所计算的结果返回给原用户，与组织 A 有关的整个计算完成。

以上步骤可用图 2 形式表示。

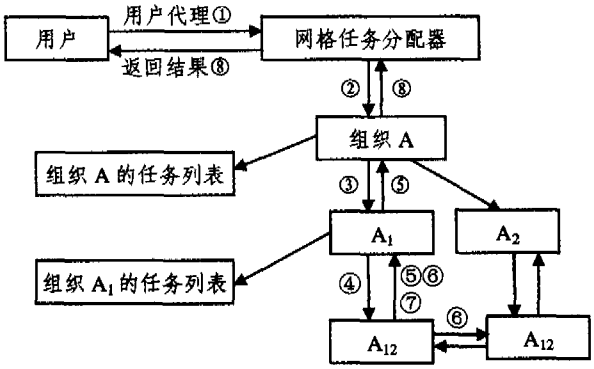

图 2 任务提交与计算过程

对于步骤 6，如果组织 A 范围内所有主机或机群目前都无法满足额外的资源要求，A 就可向邻近的组织或计算主体申请额外的资源或进程(注意该进程所拥有的权限不能升级，即应该是用户和该组织在要申请的资源的权限交集的一个子集)。如果 A 在一定的时间内还未找到所需要的资源，A 就向网格资源分配器申请，由任务分配器查询。找到后就可把需要的额外的计算任务转交给新找到的资源，最后该资源把运行后的结果返回给组织 A。所有任务完成后，由 A 把最终的结果通过网格服务器返回给提交该计算任务的主体用户。

3.3 树型网格的安全机制

以上仅考虑了树型网格的信息发布与查询机制。在任务实际执行之前还要相互身份认证，保证只有合法的用户才能提交任务，只有合法的资源才能提供服务。同时，在申请额外的进程资源时，还要保证进程的权限不能扩大，网格安全策略要服从本地安全策略。在组织 A 申请额外的资源时，同样和该资源进行相互身份认证，也要把提交任务用户的代理证书同时出示给该资源，由该资源决定是否处理来自组织 A 的关于某个用户的任务请求。额外资源的申请基本过程如图 3 所示。

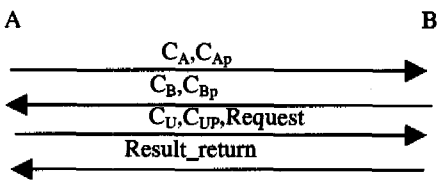

图 3 额外资源的申请过程

首先组织 A 同主体 B 出示各自的身份证书(C_A，如 X.

509 证书)和代理证书(C_{Ap}),通过 SSL 进行相互身份认证,双方鉴别各自的身份证书并验证代理证书是否合法。如果合法,就继续通信,否则中断通信;

认证通过后,组织 A 同时提交需要源任务申请用户的证书、代理证书以及需要 B 完成的任务,主体 B 根据本地的安全策略审查用户的(代理)证书在本地的权限,如果符合本地安全策略要求就执行该任务,否则中断通信;

最后,B 把完成的任务结果安全地返回给 A。

组织 A 不必是集中的计算资源,可以是为完成某项任务而通过 VPN 和 IPSec 组成的虚拟组织,在网格环境中我们把这样的网格称为虚拟专用网格(VPG)。

搭建虚拟专用网格的目的就是对资源更充分地共享,而且效率也更高。实际中的网格拓扑结构可大体上如图 4 所示。

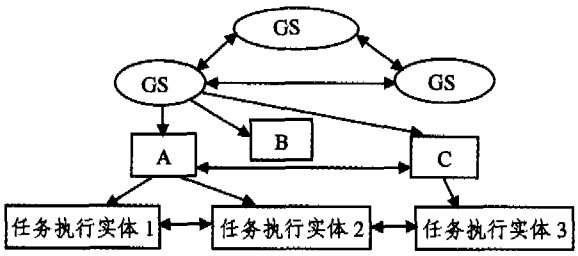

图 4 类树型网格的拓扑结构

以往 C/S 模式的 Internet 中通信和访问机制是固定的,在此基础上提出的 Web Service[7] 也依赖于处理从一台客户机发送到一台服务器上的请求。而网格架构同样依赖于相当基本的原理,即在多台客户机和多台服务器之间传送简单的请求。

目前网格存在两种主要的组件类型——服务器和客户机。网格的任务分配主要有两种模式:请求模式和分发模式。请求模式依赖于客户机请求工作,而分发模式依赖于代理直接给客户机提供工作。后者尽管不常用,但是如果某种环境中的工作是受到控制的,并可以仔细地分配到特定的执行单元,并分别监控,那么这种架构对于分发工作就是很实用的方法。

基于 Web 服务的机制还存在以下问题:

第一,代理需要确切知道哪些机器是网格的一部分,因为它需要能分别访问这些客户机;第二,分发的服务器需要直接和参与服务的所有计算机频繁地联系,这就消耗了服务器的性能,使其不能有效地处理其它请求;第三,不能有效地支持两个比较大的团体资源在一定条件下的相互使用,如合作中的两个企业有时候资源需要在一定程度上相互访问,但同时又要克服另一个团体对该资源的恶意访问、下载或上传有损该团体形象的电子内容。

在具体设计计算网格的安全系统时,必须结合计算网格中的其他管理系统,保证在计算网格的多个管理系统和层面上都有安全保障。除现有的技术措施以外,还需要进一步解决以下关键问题:

• 用户单点登录与信任管理。用户只需在一点登录,通过身份认证后就可以根据拥有的权限,访问计算网格中的各种合法资源。同时,根据用户对资源的使用情况,需要动态地为用户更新信任状态,以便下次访问时为该用户提高、维持或降低相应的权限。

• 根据其它团体的用户对该资源的访问统计情况(如是否恶意修改内容,是否进行了有损该资源利益的操作或企图),动态地为其他团体更新信任状态,以便为该团体中的成员下次访问资源时分配相应的权限。

• 对团体内成员信任的管理。团体内的某些成员可能习惯于对(本地发或外地的)资源进行恶意访问,团体为"管好"自己的成员,对它的可信程度进行动态的统计,及时更新成员的信任数据库,以便为该成员适时定义可拥有的合适权限,避免对本地资源的恶意使用或访问,同时也降低该成员恶意访问其他团体资源的能力,保证了对外维护该团体对于其他团体的形象与权限。

• 资源的动态性。在计算网格中,资源具有动态可变的特点,因此需要采用相应的管理机制,保证资源的适时安全性和可用性。

• 环境的异构性。在计算网格中,不同的节点可能采用不同的硬件或操作系统,从而给安全管理带来一定的困难。目前一般采用代理机制,并结合 Java 的跨平台特性来解决环境的异构性问题。

• 任务的多样性。在计算网格中,存在大量的并行任务,而每个并行任务一般都有多个进程或线程,并且可能分布在不同的网格节点上。如何对其进行安全管理,是一个甚少研究的问题。目前可选的解决方案是在每个网格节点建立任务代理,协调任务管理系统与安全传输通信体系,共同保证跨网格节点的任务安全。

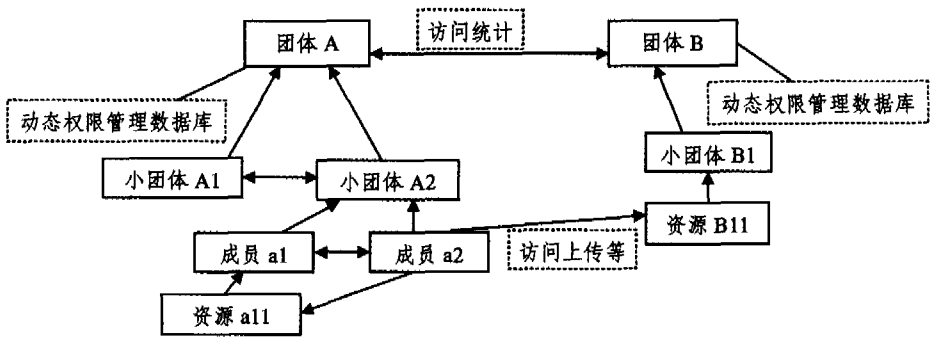

图 5 动态访问权限管理结构图

• 信任域的异构性。网格安全策略必须集成到一个局部可管理的用户和资源,形成异构集合,网格安全环境不能限制和影响局部的安全策略。这样,我们既不能代替局部安全策略,也不能够覆盖局部安全策略。因此,网格安全策略必须集中于管理域间相互作用和把网格安全策略映射为局部安全策略。

基于以上问题，结合本文关于类树型网格构造的讨论，给出对于团体、成员之间资源、信任以及权限的动态管理方法，该方法改进了以往一成不变的权限管理方法。根据本文的方法，在其他团体成员对本地资源的访问的权利映射过程中，不同的登录时间可能映射到不同的本地用户名，获得不同的访问权限，有利于灵活地解决权限分配问题。目前对该问题的解决还不成熟，不可能做到全面的解决，还需要做进一步的研究。

图5所示为通常的两团体及成员之间的访问权限管理。两个团体可以是两个站点，也可以是某团体内所属的两个小团体之间甚至可以是两个成员之间的相互访问权限的管理。两个团体A和B，它们各自都有自己的一个动态权限管理数据库，该数据库中存放的是对下属小团体或成员的相互访问的统计情况，同样保存着其他与其进行数据交换的团体用户访问情况的统计。通过对数据库的监测管理，不断更新用户或下属小团体的访问统计，并以此来及时更新成员的访问权限，确保系统不被过分地恶意侵害。而对于成员之间的访问控制也采取类似的方法，对于恶意访问或下载的用户权限进行限制，保证系统资源不被恶意侵害，维持系统的顺畅运行。

用户权限的大体控制如图6所示，3个圆分别代表不同的权限，用户权限是其在不同领域所拥有的权限的交集。这里的3个圆的面积随系统的统计情况随时变化。对3个圆的大小(权限)情况进行分析，就可以得到外部控制是如何根据统计情况调整圆的大小来调整用户的使用权限的。

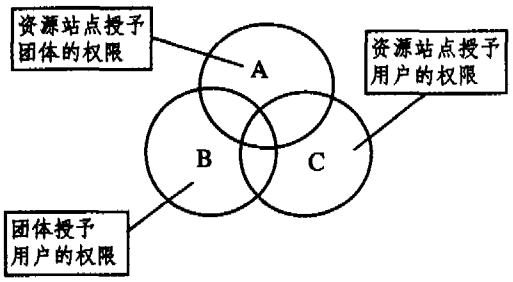

图6 用户权限构成图

在外部或内部的统计下，系统不断更新用户的访问权限，大体过程如下：

(1)如果用户对外界某个团体的资源恶意访问，那么首先圆C(资源站点授予用户的权限)会变小，而用户所在团体由于受到该用户(过多)恶意访问的影响，圆A(站点授予团体的权限)也会变小，进而该用户所在团体也会对它的权限进行控制，圆B(团体授予用户的权限)将变小。最后的结果可能是构成用户权限交集的3个圆都减小，最终导致用户的权限降低。

(2)团体内部对各用户之间的访问也存在统计，用户之间的相互访问也需要遵循一定原则。对于内部用户之间的恶意访问或恶意下载作出控制措施，控制用户的访问权限。如果成员对本团体内其他用户的站点进行了恶意访问，这些站点将该成员的恶意访问情况上报给用户权限管理部门。该团体通过修改该成员的权限，降低该成员的访问能力，此时表示团体授予用户的权限的圆B将减小，以此来防止该成员通过恶意访问本地或其他团体的资源，而给该团体带来损失。

(3)团体A可根据实际需要，通过询问其他团体(有资源共享关系的团体)或本地其他成员，适时地收集或调查下级成员的访问统计情况，及时确定该团体内成员的权限。

(4)另一种情况，如果团体对站点的资源使用进行了重新的付费购买，那么表示资源站点授予团体权限的圆A就会增大，同时用户对站点的使用权限也可能根据实际需要适当地提高。

(5)如果团体内用户所接受任务发生变化，则用户访问权限也是会发生变化。具体来说，团体授予用户的权限圆B将被拉动，以此来改变用户对站点的访问权限范围。

总之，以上所示的认证管理系统是一个随着统计情况动态适时更新用户权限的系统，它能够最大限度地避免系统资源被过分地恶意访问，灵活地处理网格系统中资源共享所面临的动态安全问题。

结束语 网格研究的一个重要目标就是灵活、动态的资源共享。在以往的网格研究中，很少考虑动态的安全问题。本文对于网格的逻辑搭建方式做了一点探讨，初步研究了一种方便团体资源和权限的动态管理形式，它在组成逻辑上类似一棵不规则的树，可以有效地动态统计某个团体及其成员的信任程度，便于及时更新该团体以及该团体成员可以访问本地资源或其它资源的权限，更细粒度地控制用户所拥有的权限，防止用户的恶意访问而造成巨大的损失，同时也为用户分配合适的访问权限。

动态适时的安全管理涉及很多方面，本文在这方面只是做了初步的探讨，很多问题需要进一步探讨。例如，用户的单点登录既要实现网格安全策略向本地安全策略的映射，又要动态地统计和管理该用户及其所属团体在本地的权限；团体在统计(调查)更新成员权限时，还要注意避免和处理不可信成员对它所相邻成员的不真实上报等。

参 考 文 献

1 Foster I, Kesselman C, Tsudik G, et al. A Security Architecture for Computational Grids[A]. In: Proc. 5th ACM Conference on Computer and Communications Security Conference, 1998. 83～92
2 Foster I, Kesselman C. The grid 2: blueprint for a new computing infrastructure. Boston: Elsevier Morgan Kaufmann, 2004
3 都志辉，陈渝，刘鹏. 网格计算[M]. 北京：清华大学出版社，2002
4 http://www.globus.org
5 Normile D. Beijing Genomics Institute: From Standing Start to Sequencing Superpower. Science, 2002, 296(5565): 36～38
6 Milgram S. The Small World problem. Psychology Today, 1967, 67(i): 60～67
7 Kleinberg J. The small-World phenomenon: An algorithm perspective. ACM Symp on Theory of Computing, 2000
8 W3C. Web Service 相关标准. http://www.w3c.org, 2003-06