第 34 卷 第 5 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.5 Computer Engineering March 2008
·网络与通信· 文章编号：1000—3428(2008)05—0107—03 文献标识码：A 中图分类号：TP393

基于多级单向哈希链的网格代理证书管理

刘 颖[1]，余侃民[1]，魏 军[1]，姬正洲[2]
(1. 空军工程大学电讯工程学院，西安 710077；2. 空军工程大学理学院，西安 710051)

摘 要：代理证书是网格安全基础设施(GSI)中关键机制之一，用户需要通过代理证书访问网格服务，但目前的 GSI 方案中缺乏有效的代理证书管理机制。针对代理证书的生命周期控制不灵活、证书容易受到攻击等问题，该文提出一种基于多级单向哈希链的网格代理证书管理方案。多级单向哈希链由 2 层或 2 层以上哈希链构成，每个代理证书都由一个哈希值保护，其有效时间能够得到自适应控制，增强了网格代理证书管理的安全性和任务成功率。实验表明网格环境下该方案计算和通信开销较小。
关键词：网格安全基础设施；代理证书；多级单向哈希链；哈希值

Grid Proxy Certificates Management Scheme Based on Hierarchical One-way Hash Chains

LIU Ying[1], YU Kan-min[1], WEI Jun[1], JI Zheng-zhou[2]
(1. Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077;
2. Science Institute, Air Force Engineering University, Xi'an 710051)

【Abstract】 Proxy Certificates(PCs) is one of key mechanisms in Grid Security Infrastructure(GSI). Users need PCs to access grid services. But there is no effective mechanism to manage the PCs in GSI. An adaptive proxy certificates management scheme based on hierarchical one-way hash chains in grids is presented to solve the problem that PCs' lifetime does not be controlled neatly and PCs would be attacked easily. A hierarchical one-way chain consists of two or more levels of chains, where values of a first-level chain act as roots of a set of second-level chains and each PC is protected by a hash value, so the PCs' available time can be controlled adaptively. Results show that the security of PCs management and success rate of tasks are improved. Experiments indicate computation and communication costs much lower in grid environments.
【Key words】 Grid Security Infrastructure(GSI); Proxy Certificates(PCs); hierarchical one-way hash chains; hash value

1 概述

网格计算通过新的组织方式将广域网上的各种计算资源、信息资源、设备资源等集成起来，以统一的方式向用户提供服务，是当前网络计算领域的研究热点。与传统网络环境不同，网格中计算资源，用户都是动态分布的，网格环境中虚拟信任关系需要动态的创建和消亡，它需要突破地理位置的限制，突破传统共享及协作能力的限制，突破各独立域上安全机制对计算资源的限制，形成一个全新的、更自由的、更方便的资源共享，解决传统网络技术无法解决的问题。因此，网格安全问题是网格计算中的一个核心问题。在保证网格计算安全性的同时，还必须要尽量方便用户和各种服务的交互与使用。在设计网格安全机制时特别要考虑网格计算环境的动态主体特征及复杂性。要保证网格计算环境中不同主体之间的相互鉴别和各主体间通信的保密性和完整性。在网格环境中，客户机位于不同的地理空间和组织，为保证网格实体(用户、资源和程序)之间的通信安全、防止篡改、实现组织中安全机制方面的互操作性。网格安全基础设施(Grid Security Infrastructure, GSI)正是解决网格计算中安全问题的一个集成方案。

GSI是Globus Toolkit[1-2]的重要组件，用于提供支持网格的基础安全服务。代理证书(Proxy Certificate, PC)是GSI的关键技术之一。代理证书是一种基于X.509 证书[3-4]的会话证书，它的生命周期很短(一般几个小时)或是有限的，网格用户和他们创建的任务需要通过证书访问安全网格服务。但目前的GSI方案中缺乏有效的代理证书管理机制。因此，本文提出了一种新型的自适应代理证书管理方案。该方案基于笔者所提出的多级单向哈希链，每个代理证书都由一个哈希值保护，其有效时间能够得到安全的自适应控制。

2 GSI中的代理证书机制

在 GSI 中，一个代理包含一个新的证书即代理证书。代理证书是一种会话证书，是由用户而不是认证中心来签署，证书中有新的公钥和私钥、用户的标示和时间戳，时间戳表示在一定范围内，这个代理是有效的。由于代理的有效性有时间限制，因此代理证书没有用户的私钥那样安全。通常是把代理证书的私钥保存在本地的文件系统中，对私钥不进行加密，不允许其他用户对其进行访问。一旦代理被创建并存储，则用户可以使用代理证书和使用用户代理进行相互鉴别，并且不需要输入口令。当采用代理进行相互鉴别时，鉴别过程与用户和代理之间的鉴别过程有所不同，被请求方将会收到用户的证书和代理的证书(由用户签署)。因为在鉴别过程中，用户证书中用户的公钥用来确认代理证书中数字签名的

基金项目：国家自然科学基金资助项目(60573040)；陕西省自然科学基金资助项目(2004F14)
作者简介：刘 颖(1980－)，女，博士研究生，主研方向：网格计算；余侃民，副教授；魏 军，讲师；姬正洲，硕士研究生
收稿日期：2007-03-10 **E-mail：**yying_liu@126.com

合法性，这样实际上形成了一个“认证中心—用户—代理”的信任链。现有的代理证书机制可以实现网格环境中的单一登录(在本地机器上创建代理证书)和远程委托(在远程主机上创建代理证书，形成证书授权链)，但仍缺乏安全有效的代理证书管理机制。首先 GSI 代理证书由本地文件访问授权机制保护，虽然代理证书有生命周期限制，但其安全性还是远远不够的；其次，当用户在不同的网格节点系统登录时，如果每次都需要用户证书，那么证书的副本很可能留在某些易受攻击的系统中；另外，为了能让任务有效地运行，可能需要给这些任务颁发长效证书(长生命周期)，当动态网格任务的运行时间无法预测时，如果代理证书生命周期过长，则容易导致证书被攻击；如果时间过短，则可能导致任务失败，或者需要用户再次提供代理证书。

3 网格代理证书管理方案

在本节提出了一种自适应代理证书管理方案，将网格代理证书的最大生命周期划分为若干时间段。证书可以在任何一个时间段结束时失效，是否失效可以由证书的所有者或者其管理者控制。证书验证者不需要从 CA 获取撤销信息就能验证证书的有效性。因此，这种撤销机制简单且安全。该方案基于笔者提出的多级单向哈希链概念。在许多安全应用中，单向哈希链的应用很重要。哈希链基于一个公开的函数 H，该函数在现有的计算环境下很容易进行正向计算但几乎不可能进行反向计算。如果单向函数的输入是定长的，这就是单向哈希函数(OWHF)。文献[4]给出了单向哈希函数的定义。

3.1 多级单向哈希链

本文所提出的多级单向哈希链由 2 层或 2 层以上哈希链构成。第 1 条哈希链是主哈希链，它的值作为副哈希链的根。主链的第i个值对应第i条副链的根。在第i+1 条副链的任何一个值释放之前，第i条副链的值已经被全部释放，包括主链的值H_i。如图 1 所示，要建立多极单向哈希链，先选取一个随机数H_0，再计算出主链$H_0(r), H_1(r), \cdots, H_n(r)$，然后选取作为种子分别产生$n$条哈希链。

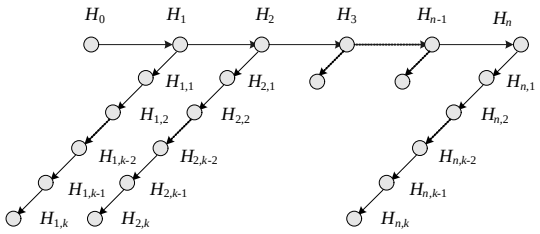

图 1 多级单向哈希链

3.2 自适应代理证书

对于代理证书生成，分 2 种情况来讨论。第 1 种情况是该网格用户所在的节点本身同时具有较强的计算和通信能力，比如个人计算机、小型工作站等。第 2 种情况是网格节点本身的计算或者通信能力较弱，不能保证代理证书产生和管理所带来的额外开销，如小型手持设备、无线设备。从实际的网格环境来看，这种分类是有必要的。对于第 1 种情况，代理证书的所有操作都在本地节点完成。带有扩展数据的代理证书通过以下的方法产生：

(1)估算代理证书路径的合适长度n，并产生主哈希链$H_0(r), H_1(r), \cdots, H_n(r)$，其中，$H_0(r)=r$是一个只有用户自己知道的随机值。

(2)产生首条代理证书链：

1)产生一对秘钥：SK_P——私钥，PK_P——公钥。

2)定义代理证书参数

T——最大生命期(在传统的方案中最常用的代理证书有效期是 12 h，在本文的方案中，由于可以随时对代理证书进行撤消，因此其最大生命可根据网格应用的需要设为足够长)；D——初始时间；L——代理证书有效性更新周期。

假设$k = T/L$是一个整数，更新点可以分别定义为$D_1 = D+L, D_2 = D+2L, \cdots, D_k = D+kL$。

3)产生第n条证书链的首个代理证书$PC = SIGN_U(U, PK_P, D, H_{n,k}(r), k, L)$，用户$U$使用自己的私钥签署该证书。

4)产生该证书链的其他的代理证书。过程与第 1 个代理证书类似，但其他代理证书不是由用户而是由上一级的代理进行签署。

5)发布哈希值。在该证书链的第j个代理证书的初始时间D，用户U释放哈希值$H_{j,k-1}(r)$初始化该证书，在这里$D = D_j + L$。假设下一个更新点是D_e，则用户U将释放$H_{ji}(r)$，其中 $i = k - (D_e-D)/L$。每个代理证书中T, D和L的值可以相同，也可以根据需要取不同的值。在该方案中，假设它们都是取相同的值。接下来，根据需要在每个更新点，释放对应的哈希值。

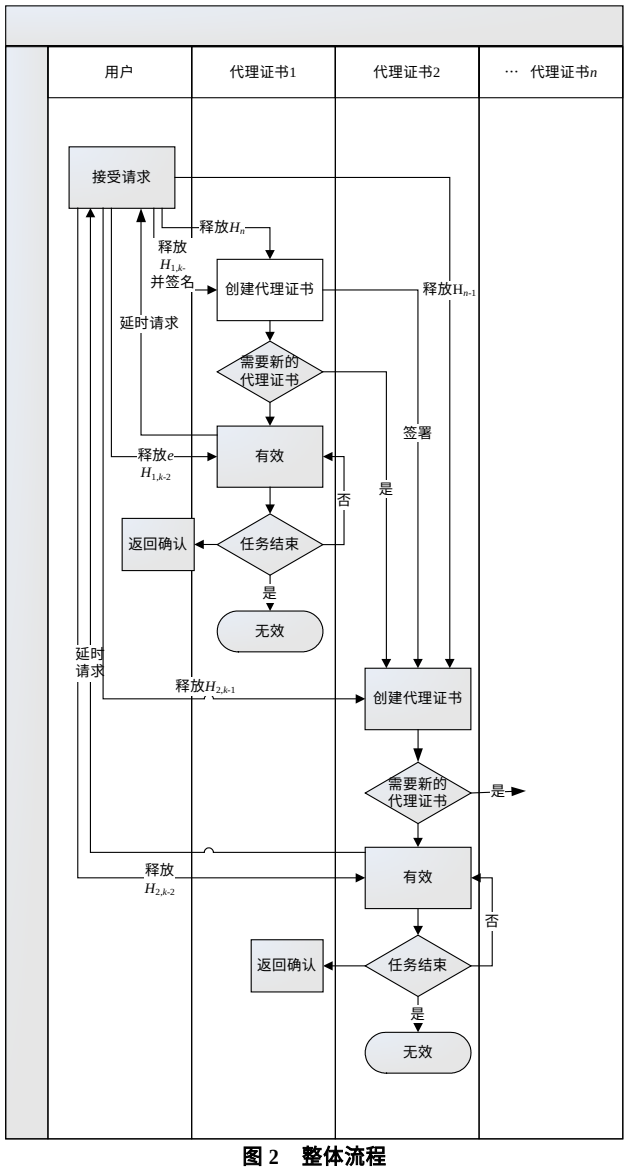

图 2 整体流程

(3)根据网格任务的需要产生其他的代理证书链，过程与(2)类似，全部网格任务完成后，返回一个确认，所有的代理证书全部自动失效。

(4)代理证书验证。当某个资源或用户V需要验证该代理证书的状态时，可以采用以下步骤：1)V首先验证用户U在$(U, PK_P, D, H_{jk}(r), k, L)$上的签名，如果签名有效，$V$就可以确认该代理证书的的公钥是$PK_P$，初始时间为$D$，最大生命期为$T = kL$，更新周期为$L$，单向哈希链中第$j$个代理证书的哈希值为$H_{jk}(r)$。2)$V$验证是否满足$0 \le i < k$并且$H_{j,k-i}(H_{ji}(r)) = H_{jk}(r)$，如果满足，$V$就可以认为$H_j(r)$是一个以$H_{jk}(r)$结尾的单向哈希链中的有效值。3)$V$验证是否满足$D \le D + (k-i)L$，如果满足，$V$将认定该代理证书有效，并且在$D = D + (k-i)L$时间内都将有效。

这样，U就可以通过释放对应的$H_{ji}(r)$来控制代理证书是否有效，整个过程如图 2 所示。

对于上述的第 2 种情况，必须在网格中设置代理证书服务器，该服务器的功能是接受网格节点的请求并代替该节点进行上述的代理证书的操作，包括代理证书和单向哈希链的产生以及哈希值的发布，如图 3 所示。

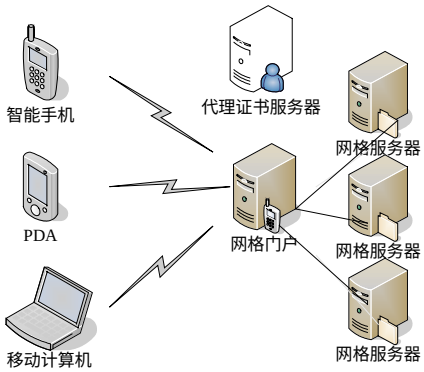

图 3　代理证书服务器

3.3　哈希链根的保护

对于第 1 种情况，用户U是依靠哈希链根r来控制代理证书是否有效的。这样做的优点是可以通过一个独立的密钥r来保护私钥SK_p。只要r或者SK_p没有泄露，系统就是安全的。如果SK_p泄露，用户U可以通过销毁r来使代理证书在下一个更新点很快失效。同样，如果r泄露了，用户可以销毁SK_p并且停止使用该私钥。但是如果r和SK_p存储在同一台计算机上，一旦系统被侵入，r和SK_p同时泄露的话，还是会带来安全隐患。因此，为提高安全性，需要将r和SK_p分开保存在不同的系统中，或者将r的值记住以后，将其销毁。

对于设置有代理证书服务器的情况，由于所有代理证书的操作都由服务器完成，因此该服务器的安全显得非常重要。该服务器应该由可信任的第三方来进行管理，并和使用该服务器的用户有安全上的约定。

4　实验分析和结论

使用本文的方案可以提高代理证书的安全性和网格任务完成的成功率。

(1)安全性方面。由于传统的 GSI 方案中，没有对代理证书加以保护，攻击者很有可能通过非法获取网格用户产生的代理证书，来冒充该用户的某些操作。本文的方案通过添加一个独立的密钥来保护代理证书，安全性显然能得到有效的提高。

(2)提高网格任务完成成功率方面。传统方案中代理证书的最大生命周期一经设定就不可更改，但本文提出的方案中，代理证书的有效期是可根据需要随时中止的，因此在运行一些复杂的、需要时间较长的网格任务时，可以将代理证书的生命周期设置为足够长，而不会带来安全上的问题。

(3)系统代价方面。只需要在网格任务开始时，运行哈希函数，在网格任务运行期间，不需要耗费额外的计算资源。而且，每次释放的哈希值是一个固定长度 128 位的值，因此占用的通信资源也非常少。

为了评估本方案的计算和通信开销，笔者在实验室环境下，按照本文提出的方案，配置了自适应的代理证书管理方案。实验环境如下：

硬件环境：联想 E3 个人计算机 100 台。Intel P4 2.8 GHz 处理器，512 MB内存，100 Mb/s网卡，按IP地址的顺序分别记为p1～p100。IBM X455 服务器 2 台。Intel Itanium 2 处理器 1.5 GHz×4，56 GB内存，1000 Mb/s网卡，记为I_1, I_2。联想T630 服务器 3 台。Intel Xeon处理器 2.0 GHz×2，10 GB内存，1000 Mb/s网卡，记为L_1, L_2, L_3。

网络环境：100 Mb/s 交换机，100 Mb/s 网线。

软件环境：PC 机为 Windows XP，网格中间件为 Globus Toolkit 4.0.3。服务器为 Windows 2003 Server，网格中间件为 Globus Toolkit 4.0.3。

为了监控网络流量的变化，在每台服务器和其中 10 台 PC 上安装了网络流量监控软件 OnlineEye Pro V1.6.0 版。

在 5 台服务器中分别存储 5 门不同课程的全校学生成绩。需要完成的网格任务是在任一台作为网格节点的计算机上查询某班学生的所有成绩，并记录每完成一次完整操作的所需时间。设定网格代理证书链最大长度为 200，代理证书最大生命周期为 1 h，更新周期为 1 min。实验选取了 2 种最极端的特例，一种是通过任意一台PC分别访问服务器I_1, I_2, L_1, L_2, L_3。另一种是在序号为p_1的计算机上依次通过代理访问p_2, p_3, p_4, …, p_{100}直至服务器I_1, I_2, L_1, L_2, L_3。实验结果表明，在第 1 种情况下，系统能正常运行，网络流量无明显变化，完成一次操作的时间为 0.01 s。在第 2 种情况下，系统也正常运行，网络流量稍有增加，但变化不明显，完成一次操作的时间为 2.17 s，考虑参与操作节点数量的增加和网络延时的关系，表明提出的方案在较简单的网格任务中，计算和通信开销可以忽略。由于实验条件所限，本方案在大型复杂网格任务中的性能评估，还需在以后的工作中进一步研究。

参考文献

[1] Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure[M]. San Francisco: Morgan Kaufmann Publishers, 1999.

[2] Housley R, Polk W, Ford W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile[S]. IETF, RFC 3280, 2002.

[3] IETF Public-key Infrastructure (X.509) (PKIX)[EB/OL]. (2004-01-12). http://www.ietf.org/html.charters/ kix-charter.html.

[4] Berson T A, Gong L, Lomas T M A. Secure: Keyed, and Collisionful Hash Functions[R]. SRI International, Tech Rep: SRI-CSL-94-08, 1994.

[5] Foster I, Kesselman C. Globus: A Metacomputing Infrastructure Toolkit[J]. International Journal of Supercomputer Applications, 1997, 11(2): 115-128.