网格多级委托授权模型及其应用

黄 琛，李忠献，杨义先

(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 海淀区 100876)

【摘要】多级委托授权符合现实中组织的分级管理架构，是授权中的一种重要的策略。目前织女星网格授权模型并没有对多级委托的情况进行深入讨论，使得该模型的应用受到一定限制。该文给出了基于织女星网格的多级委托授权模型，并形式化地定义了权威集及隶属关系，主体集及多级委托划分关系，资源操作集及授权关系。同时还给出了实现该模型的数据结构与查找算法，量化地分析它的性能。该模型在通用性和易用性要求的前提下实现了多级委托，完善了织女星网格的授权模型。

关 键 词 访问控制； 授权； 委托； 网格计算
中图分类号 TN393.08 **文献标识码** A

A Model of Grid Multi-Level Delegation Authorization with Applications

HUANG Chen, LI Zhong-xian, and YANG Yi-xian

(Info. Sec. Center of State Key Lab of Networking & Switching Tech., BJ University of Post & Telcom Haidian Beijing 100876)

Abstract Multi-level delegation mechanism that meets management structure in most of organizations is an important strategy of authorization. Present Vega grid model has not discussed it deeply, and then the application is subject to certain restrictions because of lack of it. An authorization model with delegation based on Vega grid is proposed, meanwhile, authorities' collection and affiliation, subjects' collection and multi-level segmentation, resources-operation collection and authoritative relationship are formally defined. In addition, not only are search algorithm and data structure that implement the model also proposed, also quantitative analysis of its performance is done. The model supports multi-level delegation under the premise of generalization and ease of use, which extends Vega grid model to fit practical applications better.

Key words access control; authorization; delegation; grid computing

在本质上是分布式系统的网格环境中，授权要求自主控制的不同管理域之间的广泛协同[1]。网格内部的各管理域结成一个基于合约的联盟，在该联盟内，各成员会同时拥有一些潜在的合作知识和约定，去解析在整个网格中通用和共享的授权语义。进一步理解为，每个跨越两个或多个管理域的授权策略都能够被网格的参与成员正确地生成、接受和理解。这要求在协议、语法和语义上对网格中共享的授权策略有共同的约定。文献[2-3]用主体、资源和操作三个正交的实体概念来描述了在织女星网格操作系统[4]中的授权模型，将授权策略描述为映射在这个三维空间上的点，主体、资源和操作分别被标记为S、R、T，这个映射被记为$F:S\times R\times T\rightarrow\{0,1\}$。这种方法有别于传统的RBAC[5-6]模型，在解决网格授权系统的工程化研究方面，提出了一个新的视角。权威是授权模型中经常存在的重要实体，它是能够可信地发放、验证和撤销授权策略的管理者，能够自己进行授权操作，也能够将自己所管理的域内的主体、资源和操作委托给下级权威进行管理，以减少自己的管理负担。多级委托的方式[7]如果能够被引入到网格授权系统当中，将在实际应用中起到非常重要的作用。然而，采用文献[2-3]的方法所描述的授权策略与模型中，并没有将多级委托的因素考虑在内，这大大限制了该方法的应用。

基于文献[2-3]的视角，结合文献[7]所考虑的多级委托授权情况，本文将讨论如何建立一种支持网格多级委托的授权模型。由于网格系统通常是异构的，模型的通用性和互操作性就显得尤为重要，一个形式化描述简单和易于多方理解的授权模型在这种场合下就是非常合适的。本文第2节提出并形式化

收稿时间：2007 – 12 – 15；修回日期：2008 – 04 – 28
作者简介：黄 琛(1982 –)，男，博士生，主要从事网络信息安全方面的研究.

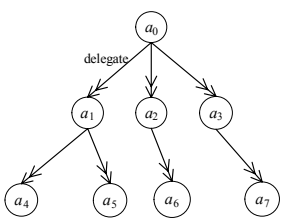
描述一种具备较好通用性和互操作性的多级委托网格授权模型，包含权威、主体、资源和操作四种实体。第3节将介绍一种能够实现该模型的数据结构和访问控制算法，并量化分析该算法的性能，包括空间复杂度、时间复杂度和平均查找长度。

1　网格多级委托授权模型

基于文献[2-3]的视角，授权模型包含主体(S)、资源(R)和操作(T)三个集合。主体可以代表单独的用户，也可以代表组织的成员。资源代表系统中的部件，这个部件用一个三元组($Z(r)$,$Q(r)$,$D(r)$)表示，其中$Z(r)$是r的记号；$Q(r)$是r的参数集；$D(r)$是r的描述集。操作代表用户行为的基本单位。并且还定义了一个三维空间(S,R,T)，其坐标原点为在上述三个集合均不取值的点，表示为(Φ,Φ,Φ)。授权策略用这个空间的任意子集$D=\{(s,r,t)|s\in S,r\in R,t\in T$，且用$F(s,r,t)=1\}$来表述。

1.1　权威

研究多级委托的情况时，就需要引入权威(A)这个元素。多级委托实际上是权威将自己对主体授权的权力委托给下级权威的过程，权力可以一级一级向下委托，权威之间实际上形成了一个树形的结构。如图1所描述的示例，a_0为顶级权威，a_1～a_3为2级权威，a_4～a_7为3级权威，图中的树形结构表示了a_0～a_7之间的隶属关系。



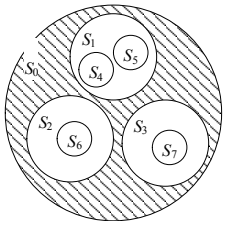


图1　权威的隶属关系　图2　分级委托下的主体划分

定义 1　权威集合。设所讨论的权威集合为A。该集合包含n个权威成员$a_0,a_1,\cdots,a_{n-1}$，记权威集合为$A=\{a_0,a_1,\cdots,a_n\}$。

定义 2　权威隶属关系。设R_A是一个在集合A上的二元关系，$R_A=\{(a_i,a_j)|a_i,a_j\in A$，且$a_i$是$a_j$的上级，$0\leqslant i,j\leqslant n\}$。权威隶属关系即为$R_A$所代表的二元关系，显然，此关系具有传递性、反对称性，但不具备反身性、对称性。

1.2　主体

因为授权的权力被分级下放，所以，主体集合也被划分成多个子集，由多个权威管理。对应图1的示例，给出如图2的主体划分，S_0代表顶级权威a_0所管理的主体集合，S_1代表2级权威a_1所管理的主体，以此类推。S_0仅为图中的阴影部分所代表的面积，不是整个集合。当一个主体子集S_1被委托给了下级权威，那么，该权威也同时失去对S_1的管理权力，由下级权威继承对该主体子集的权力。这种规定可以避免现实情况中权责不分的情况，每一个授权决策都可以找到责任权威人。

定义 3　主体集合。记所讨论的主体集合为S，$S=\{s_0,s_1,\cdots,s_n\}$，集合中的成员为系统中的主体。

定义 4　主体划分。设R_S是一个在集合S上的二元关系，$R_S=\{(s_i,s_j)|\ s_i,s_j\in S$且$s_i$和$s_j$的管理权威相同，$0\leqslant i,j\leqslant n\}$。

证明R_S为一个等价关系，$\vee s_i,s_j\in S$。

(1) 因为 s_i 仅有一个管理权威，所以$(s_i,s_i)\in R_S$;

(2) 如果 $s_iR_Ss_j$，表明 s_i 与 s_j 的管理权威相同并唯一，所以 $s_jR_Ss_i$;

(3) 如果 $s_iR_Ss_j$，$s_jR_Ss_k$，还是由于管理权威的唯一性，s_i、s_j 和 s_k 具有同一个管理权威，也就是 $s_iR_Ss_k$。

因此证明R_S是S上的等价关系。

主体划分是集合S的一系列非空子集，它们是满足R_S关系的一系列等价类，记为$P=\{S_0,S_1,\cdots,S_k\}$，它们满足下列两个性质。

性质 1　$S=S_0\cup S_1\cup\cdots\cup S_k$;

性质 2　当$i\neq j$时，$S_i\cap S_j=\Phi$。

1.3　资源与权限

在文献[2-3]中，资源集R和操作集T是分别定义的。资源和操作实际上是关系非常密切的两个集合，资源和操作联系在一起才有意义。为了更清楚地表达授权粒度，本文将这两个集合组成的二维空间压缩成为一维空间。

定义 5　资源操作集。设集合R与集合T的笛卡尔积为资源操作集，记为$RT=R\times T=\{(r_1,t_1),(r_1,t_2),\cdots,(r_i,t_j),\cdots,(r_n,t_m)|0\leqslant i\leqslant n,\ 0\leqslant j\leqslant m,\ r_i\in R,t_j\in T\}=\{rt_1,rt_2,\cdots,rt_{n\times m}\}$。

定义 6　权限策略集。设SRT为集合S与集合RT的笛卡尔积，记$SRT=S\times R\times T$。SRT为权限策略集。

定义 7　权限集。管理权威将资源授予给主体的操作，实际上就是在集合SRT上建立一个等价二元关系$\{(s_i,rt_i),(s_i,rt_j)|(s_i,rt_i),(s_i,rt_j)\in SRT,\ s_i$拥有对$rt_i$和$rt_j$的权限$\}$。权限集是$SRT$上根据这个等价关系的确定的等价类，记为$(s_i)_{SRT}$。

图3示例了主体s_1的权限集，$a,b,c,d,e\in R$表示不同的资源，$r,w,x,z\in T$表示不同的操作。从图中可以看出，该主体在a资源上具有r操作的权限，SRT上的

成员 (s_1,a+r)可以表示这样一个授权。

2 访问控制

访问控制对于一个授权模型来讲无疑是重要的，衡量一个模型的实用与否，很大程度取决于基于该模型的访问控制是否易于实现，是否具有很高的效率。当然，对于一种授权模型，可以有多种方法来设计访问控制，每一个方法可能会有不同的侧重点和优势。本文给出一个具体的方法，重点关注空间复杂度和平均查找长度。空间复杂度较小表示算法所占用的资源较少，平均查找长度较短表示权限查找的效率较高，也就是访问控制效率较高。下面将详细描述该方法所涉及的数据结构和算法，并分析和评价该算法的性能。

	r	*w*	*x*	*Z*
a	√			√
b		√		
c	√			
d			√	
e				√

图3 主体的授权集

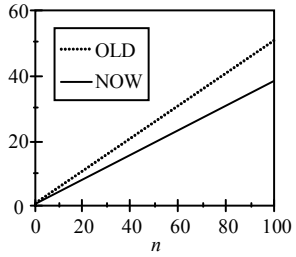


图4 平均查找长度比较图

2.1 数据结构

数据结构均基于网格实体不能排序的前提下，并且考虑通用性和易用性而设计的。一个主体的RT权限集由单链表存储结构表示：

```
typedef struct RT Node{
    RT      rt;
    BOOL    own;
    int     hits;
    struct RT Node  * next;
}RT Node, * RT List;
```

*rt*域取值于*RT*集。如果一个*RT* List里存在着一个*rt*，own域的值取true声明有权限，own域的值取false声明无权限；hits域代表该*rt*的查找命中次数。

一个权威的*S*集由单链表存储结构表示：

```
typedef struct S Node{
    SUBJECT     s;
    RT List     r;
    int         hits
    struct S Node       * next;
}SNode, * S List;
```

*s*域为*S*集内的某个成员；*r*表示该*s*的所拥有的*RT*集；hits域代表该*s*的查找命中次数；*S Node*表示就是权限集的等价类(s_i)*SRT*。

树形结构的权威集由树的二叉链表存储表示：

```
typedef struct A Node{
    Authority   a;
    S List      ss;
    struct A Node  * firstchild, * nextsibling;
}A Node, * A Tree;
```

*a*域为*A*集内的某个成员；*ss*是*S*集的等价类*P*，代表该权威所能管理的主体子集。另外，树的上下级关系表示权威的上下级关系，上级权威可以收回和下放自己所管理的主体子集。

2.2 查找算法

查找算法是访问控制的核心，如何快速检索到一个主体是否具备某个权限就是查找算法所要解决的问题。对于单链表的存储结构，成员的位置对于查找成功率非常有帮助。在实际系统中，由于任务轻重不同，每个主体访问的频次不尽相同，那么频次越高的在查找表中位置越靠前越容易被命中；由于角色不同，每个主体访问的资源也不同，越和主体的角色契合的资源越靠前越容易被命中。所以，下面所描述查找算法会根据命中次数调整节点在链表中的位置。

算法 1 带命中权重的单链表查找算法

该算法找到目标节点后，同时将该节点的命中权重加1，并且将节点在链表中的位置提前，使用该算法查找的单链表，其节点是按命中权重的大小排序的。

```
ET * SearchWithWeight(ElemtList& SL, ElemType s){
    //在这个主体集中找到s，并将s根据命中数，放置在合适的位置
    ET * light, * pre, * current;
    light=pre=current=SL;
    if(!current||EQ(current → s,s)){current → hits++; return current; }
    while(current=current→next){
      if(EQ(current→s,s)){
          current→hits++;
          将current根据hits移位到正确的位置
          return current;
       }else  if(pre → hits>current → hits){light=pre; pre=current;}
    }    return current; }
```

算法 2 先序遍历查找权威树算法

当某权威的主体管理子集中含有目标*s*时，该算法返回目标ret节点的指针。

```
Status PreOrderSearch(A Tree AT, SUBJECT s, S Node * & ret){
  if(AT){ret= SearchWithWeight (AT→ss, s);
    if(ret==NULL)
      if(PreOrderSearch(AT→firstchild, s, ret))
       if(PreOrderSearch(AT→nextsibling, s, ret)) return OK;
   return ERROR;
}else return OK;}
```

算法 3　多级委托授权模型的权限查找算法

当主体拥有目标*rt*的权限时，本算法返回true，否则返回false；

```
BOOL Search(A Tree AT, SUBJECT s, RT  rt){
    //首先在ATree中找到拥有目标s管理权力的权威a的节点和ret节点
    S Node*ret=NULL;
    if(PreOrderSearch(AT,s,ret) ){
        RT  Node*r  Node=SearchWithWeight(s→r, rt);
        return r Node→own;
    }   return false;}
```

2.3　性能分析

由定义6和7可知，查找算法占用空间包括树型的*A*集的占用空间和*P*集与*RT*集的笛卡尔积的占用空间之和，授权策略为在该笛卡尔积上建立二元关系。从空间占用最大量来看，*A*集占用空间n；笛卡尔积占用空间n^2。因此，查找算法的空间复杂度为$O(n+n^2)$，比一般用三维空间{*A*,*P*,*RT*}需要的$O(n^3)$空间略优。

单链表的查找时间复杂度是$O(n)$，虽然算法1除了查找以外，调整了命中节点的位置，但是算法的规模仍控制在$O(n)$上。二叉树遍历的时间为$O(n)$，算法2在遍历的过程中执行了算法1，综合之后，算法2时间复杂度为$O(n^2)$。算法3为算法1与算法2之和，因此时间复杂度为$O(n+n^2)$，该规模也比$O(n^3)$略优。

不事先排序的查找算法的$\mathrm{ASL}_{SS}=(\frac{n+1}{2})$。算法3的ASL在平均概率(假设$n$阶的单链表的命中权重是公差为1的递减数列)的假设下，计算公式为：

$$\mathrm{ASL}_{(1)}=\frac{n\times 1}{n(n+1)/2}+\frac{(n-1)\times 2}{n(n+1)/2}+\cdots+\frac{1\times n}{n(n+1)/2}=\frac{n+2}{3}$$

$$\mathrm{ASL}_{(2)}=(\mathrm{ASL}_{(1)}+\mathrm{ASL}_{SS})/2=\frac{5n+7}{12}$$

$$\mathrm{ASL}_{(3)}=(\mathrm{ASL}_{(1)}+\mathrm{ASL}_{(2)})/2=\frac{3n+5}{8}$$

从图4可知，随着n值变大，算法3与原算法的差距随n线性增大。n=1 000时，ASL缩短了约125，因此，算法3的ASL较优。

3　结 束 语

本文扩展了文献[2-3]中的基础授权模型，给出了基于织女星网格的多级委托授权模型，并形式化地定义了权威集及隶属关系，主体集及多级委托划分关系，资源操作集及授权关系。另外，出于工程应用的考虑，还给出了实现该模型的数据结构与查找算法，同时还量化地分析它的性能。该模型在通用性和易用性要求的前提下实现多级委托，完善了织女星网格的授权模型，更加契合网格的实际应用。

目前，本模型是没有区分委托的深度的，实际上，委托的深度越深，信任传播的越远，信任度就应该越低[8]，解决这方面的问题是将来的工作之一。

参　考　文　献

[1] FOSTER I, KESSELMAN C, TUECKE S. The anatomy of the grid: Enabling scalable virtual organizations[J]. International Journal of Supercomputer Applications, 2001, 15(3): 200-222.

[2] 徐京京, 代红雷, 查　礼, 等. 基于社区的服务网格多粒度授权与访问控制研究[J]. 计算机应用研究, 2006, 23(7): 199-203.

[3] 李　伟, 徐志伟. 一种网格资源空间模型及其应用[J]. 计算机研究与发展, 2003, 40(12): 1756-1762.

[4] 徐志伟, 李　伟. 织女星网格的体系结构研究[J]. 计算机研究与发展, 2002, 39(8): 923-929.

[5] DAMIANI M, BERTINO E, CATANIA B, et al. GEO-RBAC: a spatially aware RBAC. ACM transactions on in-formation and system security (TISSEC), 10(1), 2007.

[6] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[7] LI N H, WINSBOROUGH W H, MITCHELL J C. Distributed credential chain discovery in trust management (full version)[C]//In: Proceedings of the 8th ACM Conf on Computer and Communications Security. New York: ACM Press, 2001: 156-165.

[8] 翟征德, 冯登国, 徐　震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报, 2007, 18(8): 2002-2015.

编　辑　熊思亮