# 具有角色特性的 UCON 属性管理研究*

蔡伟鸿，王高举，陈华华
（汕头大学 计算机系，广东 汕头 515063）

**摘 要**：属性作为 UCON 模型的核心元素，缺乏灵活简洁的管理机制。针对该问题，通过分析核心 UCON 模型属性的特征，提出了一种具有角色特性的属性管理结构（MASUR）。该结构依据创建属性的能力将主体划分为系统管理主体、属主主体和一般主体，扩展了核心 UCON 模型的中心化管理方式，具备了区分各主体的职责能力；然后将属性分为系统属性、自主属性和受控属性，提出属主的概念，明确地限定属性的更新主体；最后借鉴成熟的 RBAC 成果，引入属性角色与操作角色，以适用于现代大规模系统的属性分类和管理。MASUR 为现代系统提供了一种对属性更宽泛、更细粒度的灵活控制方法。

**关键词**：属性管理；属性角色；操作角色；属主；UCON；MASUR
**中图分类号**：TP315；TP309 **文献标志码**：A **文章编号**：1001-3695(2014)05-1463-04
doi:10.3969/j.issn.1001-3695.2014.05.043

## Research of attributes management of UCON with role properties

CAI Wei-hong, WANG Gao-ju, CHEN Hua-hua
(*Dept. of Computer Science & Technology, Shantou University, Shantou Guangdong* 515063, *China*)

**Abstract**: Attributes as the core element of UCON model, are short of a brief and flexible administrative pattern. To solve this problem, this paper analyzed the properties of attributes of core UCON model and proposed a managed attributes structure of UCON model with role properties(MASUR). MASUR was sorted into system administrative subjects, owner subjects and general subjects by the ability of creating attributes. Thus, it expanded the centric-administration mode of core UCON model and owned the ability to clarify the duties of subjects. Moreover, MASUR had three attribute types: system attributes, discretionary attributes and other-controlled attributes, and gave a new concept "owner" to clearly restrict the subjects to updating attribute's value. Considered the mature theory result of RBAC, the structure involved the attributes role and operator role, which was more convenient to the attributes classifies in modern large-scale systems. MASUR gave a wider and fine-grained flexible controlling attributes method in modern systems.

**Key words**: attributes management; attributes role; operator role; owner; UCON; MASUR

UCON(usage control)自 2002 年被提出，包含了传统的访问控制模型、信任管理、数字版权管理等内容，定义了授权、义务和条件三个决定条件，具有属性易变性和决策连续性两个重要特征，为访问控制提供了一个高度抽象的统一的模型，以解决开放式网络环境下用户权限的灵活管理（访问者不必通过特定的标志来判断访问权限）、细粒度的授权过程和大规模用户的授权问题。但是 UCON 大部分工作仍停留在理论研究上，如 Jin 等人[1]正式定义了 ABAC 的统一模型、Pretschner 等人[2]阐述了 UCON 的机制等，UCON 属性和策略管理复杂的问题更加突出。Chen 等人[3]提出了基于 UCON 的云服务访问控制；基于角色的访问控制（RBAC）能够很好地解决封闭式环境下权限的分配与回收[4]，将角色与属性结合成为了一个研究热点。结合属性的易变性、开放性和角色的相对稳定性和管理的便利，将属性加入到 RBAC[5~7]，提高了模型的应用性和可操作性，很好地支持了分布式管理[8,9]。熊智等人[10]提出了基于角色和规则引擎的 UCON 应用模型，灵活地应用于云存储场景中；Jin 等人[11]提出了权限过滤策略，以限制角色的最大权限；谢辉等人[12]把角色加入到 UCON 系统中，有效地实现了动态授权机制，并且降低了授权管理的规模，但是角色作为用户的一种属性，不区分属性的类别容易造成角色数量的激增，而且文献[11,12]均没有对属性的变化作出阐述；Jin 等人[13]又通过 RBAC97 模型来管理属性，以解决用户和属性间的授权关系，但是仍限制了用户对资源的控制。传统的 UCON 模型中主体属性、客体属性是相对静态的，只能够由管理行为进行修改，仅适用于传统的访问控制策略。现代信息系统中，更加复杂的、动态的决策要求主客体属性的修改作为对数字资源访问的边际效应[14]。此外，系统能够允许用户参与策略的制定与修改，使属性的分类与管理成了 UCON 的一个重要的、必要的研究课题。

本文对属性的类别进行了详细的分析与划分，汲取 RBAC 中角色的重要意义，避免了传统 UCON 复杂、不易于管理的缺点，使得改进后的 UCON 系统更适用于现代的信息系统。

## 1 基础元素

### 1.1 背景简介

文献[7]中对属性进行了分析和分类，同时也分析了属性

**收稿日期**：2013-08-01；**修回日期**：2013-09-23 **基金项目**：广东省自然科学基金资助项目(S2011010004197)；广东高校工程技术研究中心建设项目(GCZX-A1306)；汕头市科技计划资助项目(2011-134-149)；汕头大学创新团队资助项目(ITC12001)

**作者简介**：蔡伟鸿(1963-)，男，广东潮州人，教授，博士，主要研究方向为网络与通信、信息安全(whcai@stu.edu.cn)；王高举(1989-)，男，硕士研究生，主要研究方向为信息安全；陈华华(1987-)，男，硕士研究生，主要研究方向为信息安全.

管理的重要意义。Park 给出的分类属性管理结构图如图 1 所示。

文中根据属性是否由系统自动执行,将属性划分为系统属性(易变属性,由系统自动执行)和管理属性(非易变属性,由管理行为对属性进行修改),管理属性中根据行为的操作者划分为安全管理员控制和用户控制(包括自己控制和非自己控制)。易变的属性不需要管理行为就可对属性进行修改,是 UCON 核心模型中的一个重要特性。管理员控制和系统控制刻画了安全管理员、用户和系统对属性更改的能力。通过对属性的分类,明确了 UCON 系统中对属性操作的能力和职责范围,为 UCON 系统的管理提供了清晰的权限区域原则。这种属性分类的方式是建立在 UCON 管理集中在系统端的基础上,大大限制了用户对于权限、策略和属性的管理需求,在数字资源的管理系统中,用户需要对数字资源进行更加详细的控制与决策。图 1 中的分类方式稍显力不从心。

本文通过对属性更加广泛的分析与研究,将属性划分为系统属性、自主属性和受控属性,提出了一种更宽泛的属性管理方式。

### 1.2 相关元素

在数字保护系统中,用户需要对数字资源进行更加细粒度的限制与控制,传统 UCON 系统的权限控制是集中在管理员层次,限制了用户的控制粒度,并且加大了管理员的负担。按照属性的创建主体可以将主体分成系统管理主体、属主主体和一般主体三类。系统管理主体维护系统的策略与属性规则,创建属主主体,并且对属主主体的创建能力与权限进行控制,防止属主主体的非法操作和对资源的不合理限定;属主主体在系统规则的允许范围内创建属性与策略;一般主体是核心 UCON 模型中的主体,该类主体不具有创建属性的能力,只包含有系统属性和受控属性。例如在数字资源管理系统中,用户发布的资源可以由用户自身对资源请求者的权限进行控制,并且能够为请求者创建某些属性,以判断请求者是否满足请求的内容要求。根据属性创建者的不同将属性分为系统属性、属主属性和受控属性。

**定义 1** 主体根据创建或更新属性、决策的能力分为系统管理主体、属主主体、一般主体。

a) 系统管理主体(system administrative subjects, SAS)。UCON 系统中的核心组成部分,具有最高的管理级别,承担系统核心策略与属性规则的制定与修改,称为系统管理主体。

b) 属主主体(owner subjects, OS):符合系统管理主体定义的规则与策略,允许进行定制属性与策略的主体集合称为属主主体,是 UCON 系统的重要组成部分。

c) 一般主体(general subjects, GS)。UCON 系统中,除系统管理主体外,不具有定制策略与属性能力的主体集合称为一般主体;

**定义 2** 属主(owner)。UCON 系统中,对于策略,主体属性或客体属性的任一对象 $o$,如果存在主体 $s$ 拥有修改属性或策略的权利,那么称主体 $s$ 是对象 $o$ 的属主。

**定义 3** UCON 系统的属性分为系统属性、自主属性和受控属性。

a) 系统属性(system attributes, SA)。属性管理系统中,经系统管理主体定义和决策,允许由系统自动更新属性值,或者由其属主的行为进行修改的属性称为系统属性。

b) 自主属性(discretionary attribute, DA)。属性管理系统中,如果一个属性的属主主体或属主是其自身,那么称这样的属性为自主属性。

c) 受控属性(other-controlled attributes, OA)。属性管理系统中,对某一属性,如果满足:a) 由属主主体进行定义和决策;b) 含有该属性的对象是主体的一种,且不是其属主主体或属主;c) 若含有该属性的对象是客体,则该属性只能由属主或者属主主体进行修改,称该类属性为受控属性。

属性的结构如图 2 所示。系统管理主体拥有的属性仅包含系统属性;属主主体和一般主体拥有的属性包含由系统管理主体创建的系统属性。属主主体创建的受控属性和自主属性,而客体仅拥有系统属性与受控属性。属性对象至少包含属主主体对象与属主两个信息。图 2 与 Park 给出的分类方法不同的是:该图中系统属性、自主属性和受控属性均有易变属性与不易变属性,由属主进行属性的控制。下面均不再区分易变性,但是仍然支持属性的易变性。

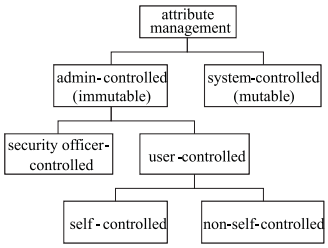


图1 属性管理分类

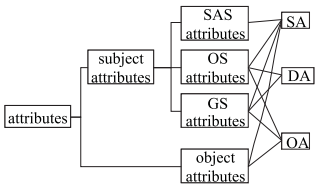


图2 属性的结构图

另一方面,UCON 数量庞大的策略对本身的管理带来了极大的不便。本文加入了角色的特性,期望能够降低策略制定的基数。例如在电子商务网络中,用户一般具有姓名、昵称、注册时间等相对稳定的属性、还有阅读章节、阅读次数等动态产生的属性,假设有 4 个静态属性、6 个动态属性,则在核心 UCON 模型中需要产生 $2^{10}=1024$ 条策略;将静态属性作为角色时,需要 $2^4+2^6=80$ 条策略和 4 个角色。由此可以看出,采用角色的方式可以极大地降低策略的复杂性和数量。

**定义 4** UCON 中的角色分为属性角色(attribute roles, AR)和操作角色(operator roles, OR)。

a) 属性角色(AR),由一组相关的主体/客体属性组成。

c) 操作角色(OR),由一组相关的操作组成。

属性角色—属性映射关系为

$$ARA \subseteq AR \times 2^{SA \cup DA \cup OA}$$

操作角色—权限映射关系为

$$ORA \subseteq OR \times 2^{permissions}$$

角色间的继承关系为

$$RH\psi \subseteq \varphi(Roles) \times \varphi(Roles)$$

$$\varphi(Roles)=\begin{cases} ARA & \text{if } \psi \in AR \\ ORA & \text{if } \psi \in OR \end{cases}$$

表示角色间的偏序关系记为$\geqslant$。若角色 $r_1$ 和 $r_2$ 间有关系 $r_1 \geqslant r_2$,则 $r_1$ 继承 $r_2$ 中所有的属性或权限。

主体与角色关系是:属性角色作为主体长期存在的属性,是主体属性的一种静态属性;由于 UCON 是基于请求的,故操作角色作为主体的一种动态属性,请求结束后,动态角色不再是主体的属性,但是由于其生命周期较长,在主体撤销动态角色的属性时,动态角色仍存在于系统当中,而操作角色的删除由属主主体进行。

## 2 具有角色特性的 UCON 属性管理结构 MASUR

MASUR 是以属主为中心的属性管理结构,通过确定属性的属主明确地限定了更改属性的操作主体,在更新属性值或创

建属性对象时根据属性的类别来防止非法的行为。MASUR 的结构如图 3 所示。

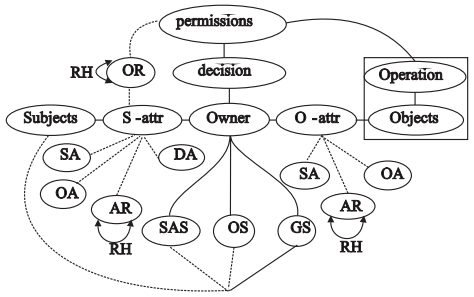


**图3 MASUR结构**

**定义 5**　MASUR 结构中,Subjects、Objects、S-attr、O-attr、SA、DA、OA、Permissions、Roles 分别表示主体、客体、主体属性、客体属性、系统属性、自主属性、受控属性、权限和角色集合。其中,Subjects 包含了 SAS、OS、GS 三种主体,属性对象 $o$ 含有信息属主主体和属主两种信息,记为 $o$:{os,owner-set},若 owner-set = null,则由系统自动执行,主体不能更改其属性值;S-attr 包含属性角色与操作角色,O-attr 包含属性角色,分别记为 subject〈[{sa: SA}][{da: DA}],[{oa: OA}],[{ar: AR}],[{or: OR}]〉,object〈〈{sa:SA}〉,[{oa:OA}],[{ar:AR}]〉;PERMISSIONS 是对客体的行为操作,记为 permission〈object,operation〉。

**定义 6**　UCON 中主体与属性间的关系。

a)系统管理主体—属性(属性角色)分配 SASAA(SASARA)

$SASAA \subseteq SAS \times 2^{SA}$

$SASARA \subseteq SAS \times 2^{AR} \times 2^{OR}$

b)属主主体—属性(属性角色)分配 OSAA(OSARA)

$OSAA \subseteq OS \times 2^{SA} \times 2^{OA} \times 2^{DA}$

$OSARA \subseteq OS \times 2^{AR} \times 2^{OR}$

c)一般主体—属性(属性角色)分配 GSAA(GSARA)

$GSAA \subseteq GS \times 2^{SA} \times 2^{OA} \times 2^{DA}$

$GSARA \subseteq GS \times 2^{AR} \times 2^{OR}$

d)客体—属性(属性角色)分配 OAA(OARA)

$OAA \subseteq Objects \times 2^{SA} \times 2^{OA}$

$OARA \subseteq Objects \times 2^{AR}$

e)决策—属主分配关系 DOWA

$DOWA \subseteq Decision \times Subjects$

**定义 7**　相关函数定义:

a)每一个会话仅属于一个主体,而一个主体在同一时刻可以有多个会话。

$session\_users(se:SESSIONS) \rightarrow s:SUBJECTS$

b)当前会话与激活的操作角色是 1 对 $n$ 的关系。

$activated\_roles(se:SESSIONS) \rightarrow or:OR$

主体拥有的角色集合映射。

$assigned\_subject\_roles(u:SUBJECTS) = \{r: r \in AR, (u,r) \in SASARA \mid OSARA \mid GSARA = r \vee OR, \forall se:SESSIONS, session\_users(se) = u \Rightarrow r \in activated\_roles(se)\}$

$assigned\_object\_roles(o:OBJECTS) = \{r:r \in AR, (o,r) \in OAA\}$

d)使用前预先授权基于主客体属性,从而对客体的访问权限进行决策。

$allowed\_permissions_{pre}(s:SUBJECTS, o:OBJECTS, p:PERMISSIONS) \Rightarrow preA(SA,DA,OA,AR,p)$

e)使用中授权需要判断义务与条件是否符合要求。

$allowed\_permissions_{on}(s:SUBJECTS,o:OBJECTS,p:PERMISSIONS) \Rightarrow act(oBligations) \wedge constraints(conditions) \wedge (onA(SA,DA,OA,AR,p) \vee \exists or, or' \in OR,\ or \geqslant or' \wedge (or',p) \in ORA \wedge (s,or) \in GS \cup OS \cup SAS \Rightarrow onA(SA,DA,OA,AR,p))$

f)在授权过程中,当环境或主体属性或客体属性发生变化时,若不再满足要求的条件,则立即撤销对主体的授权。

$stoped(s,o,p)(constraints(conditions) \wedge onA(SA,DA,OA,AR)$

g)属性的修改是由属性的属主对象进行操作。

$update\_attributes(s:SUBJECTS,o:OBJECTS \mid SUBJECTS, attr:O\text{-}ATTR):s \in o.attr.owner \Rightarrow update(o.attr)$

h)属性的创建语义。

$create\_attribute:PFR(s:SUBJECTS \subseteq SAS \cup DS) \cup \Rightarrow atom(OBJECTS.attr = \{s,\{\langle[null,[DS,[OS]]]\rangle\}\},action(add\_attributes))$

其中 atom 表示原子操作。

**定义 8**　权限过滤规则(permissions filtered rules,PFR)形式描述如下:

```
PFR({oo:S-Attr|O-ATTR|SUBJECTS|OBJECTS| ROLES})
{
  filter: = true;
  condition1:filter⇐filter∧predicate_function1;
  condition2:filter⇐filter∧predicate_function2;
  ...
  conditionN:filter⇐filter∧predicate_functionN.
  return filter;
}
```

## 3　MASUR 的应用

带有角色特性的属性管理具有极大的可扩展性和适应性。一方面,便于实现传统访问控制;另一方面,能够兼容核心 UCON 模型,而且弥补了核心 UCON 模型在对用户属性控制上的缺陷。

### 3.1　RBAC 的模型描述

RBAC 可以表示 DAC 和 MAC 的策略模型,因此若属性管理可以表示 RBAC 模型,则属性管理同样适用于 DAC 和 MAC 模型。由于 RBAC 中角色一方面是用户的集合,另一方面是权限的集合,而 MASUR 中的角色意义已发生了改变,角色仅作为用户的一个属性参与策略谓词的判定,属性角色在很大程度上替代了用户的集合;UCON 基于请求和属性的方式避免了 RBAC 中角色的永久权限。属性管理中通过以下关系进行迁移:

a)角色—权限关系直接由关系 ORA 代替。

$PA \subseteq P \times R \mapsto ORA$

b)用户—角色关系由关系 SASRA、OSRA 和 GSRA 分类替代。

$UA \subseteq U \times R \mapsto SASRA\&OSRA\&GSRA$

角色继承的偏序关系 RH 仍保持不变,互斥角色通过 PFR 来实现。

$PFR(SUBJECTS,ROLES)$

$\{\forall u \in SUBJECTS, (\exists r \in AR, (u,r) \in [SASRA \mid OSRA \mid GSRA] \Rightarrow \forall r' \in ROLES, r' \neq r, (u,r) \notin [SASARA \mid OSARA \mid GSARA] \vee \forall r \in OR, r \in u.activated\_roles(SESSION) \Rightarrow \forall r' \in ROLES,\ r' \neq r, r' \notin u.activated\_roles(SESSION))\}$

d)权限基数限制规则。

$PFR(SUBJECTS):$

$\{\forall u \in SUBJECTS, |\{r: \exists r \in OR \cup AR, (u,r) \in ORA \cup ARA\}| < max\_num\}$

e)先决条件角色,若拥有角色 $r_1$,必已拥有角色 $r_2$。

$PFR(u:SUBECTS, r_1, r_2:ROLES):$

$\{r1 \in assigned\_subject\_roles(u) \Rightarrow r2 \in assigned\_subject\_roles(u)\}$

f)时间频度限制。

PFR($u$:SUBJECTS,duration)

{exits_attribute($u$. last_access_time) ∧ $u$. access_time − $u$. last_access_time < duration}

g)运行时互斥。

PFR(SUBJECTS,ROLES):

{∀$u$ ∈ SUBJECTS,$r_1$ ∈ ROLES,$r_2$ ∈ ROLES,($u$, $r_1$) ∈ UA,($u$,$r_2$) ∈ UA,is_active($u$. $r_1$) ⇒¬ is_active($u$. $r_2$) ∧is_active($u$. $r_2$) ⇒¬ is_active($u$. $r_1$)}

### 3.2 数字资源管理中属性的管理应用

在数字资源管理中,数字资源的发布者在某种程度上也可以承担部分管理任务,对发布的资源进行细粒度的控制。此外,在数字资源的买卖中,电子资源来源相对较广,需要提供独立的个性服务吸引更多的买家,这就需要卖家对资源作出更多的权限管理,而不仅仅是系统平台提供的权限与服务。

例如,卖家创建用户的本月在店内消费金额属性 month_consume,如果用户在店内再次购买额超过了一定值,那么允许用户优惠购买其他产品。

a)用户 $s$ 购买电子书 ebook1 后的策略。

if exist month_consume ∈ $s$. OA and month_consume. creation_month = this_month

then month_consume + = consume

else then clear(month_consume),add_attribute($s$. month_consume), month_consume = consume

b)用户 $s$ 再购买电子书 ebook2 时的策略。

if exist month_consume ∈ $s$. OA and month_consume. creation_month = this_month

decrease(month_consume),discount(price)

## 4 结束语

通过对 UCON 属性的分析与分类,构建了具有角色特性的 UCON 属性结构(MASUR),能够很好地适应开放式环境下对用户的属性定制需求,允许用户自定义相关属性,对用户的数字资料进行细粒度的控制与决策。核心是根据属性的创建者进行分类从而达到属性管理的目的。该方法可以扩展传统的 RBAC 模型,并保持了属性的可变性和决策的连续性,同时避免了 RBAC 的缺陷。本文中没有考虑对用户的信任机制,而用户的信任问题在合作网络中有重要的作用;此外,本文也并没有对过程前、过程中、过程后三个阶段进行正式的描述与分析。正式描述这三个阶段将是本文接下来要进行的工作和研究内容。

**参考文献:**


[1] JIN Xin, KRISHNAN R, SANDHU R. A unifed attribute-based access control model covering DAC MAC and RBAC[C]//Proc of the 26th IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy. Berlin: Springer-Verlag,2012:41-55.

[2] PRETSCHNER A, HILTY M, BASIN D,*et al*. Mechanisms for usage control[C]//Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press,2008:240-244.

[3] CHEN Dan-wei, HUANG Xiu-li, REN Xun-yi. Access control of cloud service based on UCON[C]//Proc of the 1st International Conference on Cloud Computing. Berlin: Springer-Verlag, 2009: 559-564.

[4] FUCHS L, PERNUL G, SANDHU R. Roles in information security: a survey and classification of the research area[J]. Computers and Security, 2011,30(8):748-769.

[5] KUHN D R, COYNE E J, WEIL T R. Adding attributes to role-based access control[J]. Computer, 2010,43(6): 79-81.

[6] HUANG Jing-wei, DAVID M N, BOBBA R,*et al*. A framework integrating attribute-based policies into RBAC[C]//Proc of the 17th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2012:187-196.

[7] 符湘萍, 吴振强, 杨蓓. 一种基于可信度和属性的 RBAC 授权模型[J]. 计算机应用研究, 2011,28(2):742-745.

[8] BASIN D, HARVAN M, KLAEDTKE F, *et al*. Monitoring usage-control policies in distributed systems[C]//Proc of the 18th International Symposium on Temporal Representation and Reasoning. Berlin: Springer-Verlag,2011:88-95.

[9] JIANG Ze-tao, HU Shuo, GAN Sheng-ke, *et al*. Research on an UCON model supporting distributed management[C] //Proc of IEEE International Conference on Information and Automation. 2008:1520-1524.

[10] 熊智, 徐江燕, 王高举,等. 基于角色和规则引擎的 UCON 应用模型[J]. 计算机工程与设计, 2013,34(3):831-836.

[11] JIN Xin, SANDHU R, KRISHNAM R. RABAC: role-centric attribute-based access control[C]//Proc of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security. Berlin: Springer-Verlag,2012: 84-96.

[12] 谢辉, 张斌, 张红旗. 一种基于角色的使用控制授权模型[J]. 微电子学与计算机, 2010,27(6):137-141.

[13] JIN Xin, KRISHNAM R, SANDHU R. A role-based administration model for attributes[C]//Proc of the 1st International Workshop on Secure and Resilient Architectures and Systems. New York: ACM Press,2012:7-12.

[14] PARK J, ZHANG Xin-wen, SANDHU R. Attribute mutability in usage control[C]//Proc of the 18th IFIP TC11/WG11.3 Annual Conference on Data and Applications Security. Berlin: Springer-Verlag, 2004:15-29.