基于 UCON 的无线阅读 DRM 系统①

吴志浩，范冰冰，黄兴平

(华南师范大学 计算机学院，广州 510631)

摘 要：针对现有无线阅读 DRM 技术缺乏真正分布式网络环境下动态授权决策机制的问题，提出一套基于 UCON 的无线阅读 DRM 系统方案，阐述系统的模型及其关键技术。实验结果表明系统能有效进行阅读用户进行动态授权并具有良好的可用性。

关键词：UCON；DRM；无线阅读；动态授权；使用控制

UCON-Based Wireless Reading DRM System

WU Zhi-Hao, FAN Bing-Bing, HUANG Xing-Ping

(School of Computer, South China Normal University, Guangzhou 510631, China)

Abstract: Current DRM technology of Wireless Reading System in network environment cannot effectively give the dynamic authorization and decision. To solve the problem, this paper presents a Mobile Wireless Reading DRM system based on Usage Control model, explaining the system model and the core technology. Experimental results show that the system can dynamically authorize users with good availability.

Key words: UCON; DRM; Wireless Reading; dynamic authorization; usage control

1 引文

无线阅读是一种为无线终端用户提供在线或离线阅读漫画、小说、杂志等数字资源的移动增值业务。无线阅读数字资源的使用控制问题一般由移动 DRM(Digital Rights Management)技术来解决。目前，DRM 技术中对数字资源的使用控制有两种方案：一是使用传统访问控制模型。二是使用当前成熟的技术标准，如当前移动 DRM 领域最权威的 OMA DRM[1]标准。而以上两者在无线阅读领域均存在一定的不足。传统访问控制模型使用授权数据集合(访问控制矩阵、等级、角色)为客体分配权限，是一种使用前预先授权机制[2]，在无线网络环境下缺乏对终端的控制能力，无法根据用权进行动态授权决策。而 OMA DRM 即使具备一定终端控制能力，但由于其自身缺乏明确终端动态授权机制及其核心权限描述语言所基于的 ODRL (Open Digital Rights Language)未能将责任机制与访问控制机制分离[3]，导致 OMA DRM 缺乏完整使用控制描述能力。事实上，随着无线阅读业务的普及和发展，阅读业务愈趋复杂，终端对数字资源的使用决策将不再仅仅依靠服务器简单预授权完成，而需更多考虑即时和动态等因素，现有 DRM 技术中单一的授权概念无法全面表达整个数字资源使用控制过程。

鉴于此，针对无线阅读的特点，本文引入 UCON 模型，结合一种集中管理、分散控制的授权控制机制，设计并实现一套无线阅读 DRM 系统。

2 UCON模型

为统一传统访问控制模型（包括 MAC、DAC 等）和信任管理等概念， Jaehong Park 等提出 UCON (Usage Control)[2]理论。UCONABC 模型是 UCON 理论的核心模型，主要由主体、主体属性、客体、客体属性、权利、授权、责任、条件八个要素构成[4]。

与传统模型不同的是，UCONABC 是基于属性的决策模型，它使用泛化观点把身份、访问控制列表、

① 基金项目:国家自然科学基金(60703094);广州市科技支撑计划(2009Z2-D261)
收稿时间:2011-01-16;收到修改稿时间:2011-02-25

安全等级、角色、信任度[2]等因素统一到主客体属性中，并在传统授权的基础上，引入责任、条件两个概念来分别表示使用者使用决策时的主观因素和环境因素。授权是指判定用权主体是否允许使用客体特定权利的控制规则集合。责任是系统要求主体使用客体特定权利前或过程中责任主体必须完成的行为集合，如用户阅读电子书时必须打开某个广告窗口。条件是指用权主体使用客体特定权利前或过程中必须满足的系统或环境的强制约束条件，如系统负载，工作时间限制。

3 无线阅读DRM系统

3.1 系统访问控制模型

UCONABC 模型的授权策略可通过 16 个基本模型来表达，如表 1 所示。其中，0，1，2，3 分别表示主体或客体属性不需要更新、在用权前更新、在用权中更新和用权以后更新；“pre”表示使用前执行，“on”表示使用过程中执行； “Y”和“N”分别表示是否存在该基本模型。本无线阅读系统主要考虑单次点播、包月、计时三种业务，系统要求用户在使用阅读业务时要履行一定的广告阅读责任，同时系统能够限定用户在工作时间内访问。系统采用表 1 中 preA0、onA2、onB2、onC0 四种组合模型。

表 1　UCONABC 基础模型

	0(immutable)	1(pre-update)	2(onging-update)	3(post-update)
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

系统的形式化描述如下：

S 为无线阅读用户； O 为用户真实能阅读的数字内容，数字书籍的最小计费单位，可能是书包、书、章、节。其中书包是一或多本书的集合； P 表示数字资源产品，唯一对应用户与数字内容之间的订购关系(单次点播、包月)，每个产品只有唯一订购类型。例如，P 可能是包月专区的书包，也可能是单次点播购买的章节。 P 与是多对多映射。 $R:\{read,copy,write,print\}$，表示权利集合； T ，表示时间集合，精确到日； AT ，表示剩余可使用时间，精确到秒； M ，表示货币价值量的集合，结算货币是人民币； $TYPE:\{0,1,2\}$，表示业务类别，0 为点播业务，1 为包月业务,2 为计时业务；

$productInfo:P\to O\times TYPE$ ，一对多映射；

$monthProductList:S\to P\times R\times T$ ，负责记录用户的包月产品列表，多对多映射， T 表示包月截止日期；

$ownerList:P\to S\times R$ ，负责记录产品单次点播的用户列表，在单次点播业务中，用户一旦点播某个产品以后不能退订，订购关系不再发生变化；

$OBS:S$ ，表示责任主体；

$OBO:\{ad\_link\}$ ；

$OB:\{clickAd\}$ ；

$OBT:\{once\}$ ；

$credit:S\to M$ ；

$value:P\times R\to M$ ；

$avTime:S\to AT$ ；

主客体属性：

$ATT(S):\{credit,\ monthProductList\}$ ；

$ATT(P):\{value,\ ownerlist,\ productInfo\}$；

系统属性：

$WORKINGTIME$ ，表示系统的工作时间区间；

$SYSTEMTIME$ ，表示当前系统时间；

职责描述如下：

$getOnOBL(s,o,r)=\{(s,o,clickAd,once)\}$ ；

条件策略描述如下：

$getOnCon(s,o,r)=SYSTEMTIME\in WORKINGTIME;$

访问控制函数：

$Allowed(s,o,r)\Rightarrow buy(s,o,r)\vee baoyue(s,o,r)$ ；

$Stoped(s,o,r)\Rightarrow\neg timecount(s,o,r)\wedge$ ；

$\neg onFullfilled(getOnOBL(s,o,r))\wedge$

$\neg onConChecked(getOnCon(s,o,r))$ ；

$buy(s,o,r)\Rightarrow BY\neq\phi,$

$BY=\{(s,r),\exists(s,r)\in ownerList(p)\ \ ,where\ p=$

$\{p',\exists(o,type)\in productInfo(p')\}\}$ ；

$baoyue(s,o,r)\Rightarrow(PRD\neq\varphi)\wedge(t\geq SYSTEMTIME),$

$PRD=\{(o,type),(o,type)\in productInfo(p)\},$

$p=\{p',(p',r,t)\in monthProductList(s)\}$ ；

$timecount(s,o,r)\Leftarrow avTime(s)>0$ ；

属性更新函数：

$if\ type=2\ \ onUpdate(avTime(s))$: 根据使用时间不断自减更新 $avTime(s)$ ；

3.2 系统架构

本文的无线阅读 DRM 系统是无线阅读平台的其中一部分。图 1 展示了 DRM 系统交互数据流。无线阅读 DRM 系统主要由 DRM 服务器和 DRM 终端两部分组成：

(1) UCON DRM 服务器：包括电子书打包、密钥管理、UCON 访问控制、UCON 许可证生成以及传统计费服务器的部分认证、授权功能。

(2) UCON DRM 终端：基于 UCON 的 DRM 终端具有使用控制决策、许可证认证、解密和解析，电子书解密和阅读等功能。由于 UCON 终端拥有部分使用控制决策功能，终端底层系统使用可信计算技术，防止终端被非法攻击，限于篇幅在此不作深究。

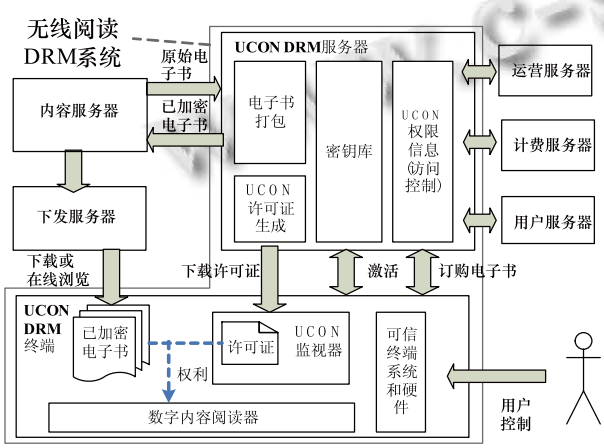

图 1 无线阅读 DRM 系统

3.3 系统关键技术

DRM 系统采用集中管理，分散控制的策略，服务器负责集中管理授权规则，计算授权结果，把授权结果缓存于 UCON 许可证并下发到终端。终端解析该许可证，结合实际用权情况进行即时使用决策。

3.3.1 UCON 许可证定义

本系统使用 XML 定义 UCON 许可证。许可证是一种将服务端授权策略或结果保存在终端以便控制资源使用的文件。UCON 许可证分为两类，其中一类是用户专属许可证，每个用户有且仅有一个用户专属许可证，负责记录用户相关控制策略，如计时订购决策策略。另一类是电子书专属许可证。每个用户对于任一电子书都有一个电子书专属许可证，负责记录用户对该电子书的使用策略和结果，如点播产品策略、包月产品策略。许可证由策略 policy 组成。policy 包括 subject、object、rights、decision、update 五棵子树，前两者描述决策所需要的主客体属性和客体密钥信息，rights 子树描述使用权利，decision 子树包括 Authorization、Obligation、Condition 三个子节点，分别表达授权策略、责任策略和条件策略。Update 子节点表达更新主客体属性的操作。

举例而言，对于策略“用户订购了计时业务，只有在系统服务时间内，阅读电子书期间履行了点击广告窗口的责任，才可对客体执行 read 操作”，用户专属许可证的 xml 代码描述如下：

```
<Policy>
<Subject>
<name>alice</name>
<SubjectAttribute id="saId">
<model><constraint id="timecountId" type="timecount">
<AttributeValue id="tcount" DataType="&xml;int">999999
</AttributeValue><FunctionFunctionId="&function;greater-than-or-equal"
/><AttributeValueDataType="&xml;int">0</AttributeValue>
</constraint></model>
</SubjectAttribute>
</Subject>
<Rights><right id="readId"><AttributeValue DataType="&xml;string">read</AttributeValue></right></Rights>
<Decision permissionRightId="readId">
<Authorization><SubjectAttributeDesignator ref="saId"></SubjectAttributeDesignator></Authorization><Obligation><Function
FunctionId="&function;click-advertisement-once"
/></Obligation>
<Condition>
<AttributeDesignator DataType="&xml;time" AttributeId="CURRENTTIME" /><Function FunctionId="&function;belongsto"
/><AttributeDesignator DataType="&xml;time" AttributeId="WORKINGTIME" />
</Condition>
```

```
</Decision>
<Update>
<Function FunctionId="&function:sub-everytime" type=”on”>
<AttributeDesignator AttributeId="tcount" DataType="&xml;int" />
</Function>
</Update>
</Policy>
```

3.3.2 UCON 终端的决策模型

UCON 监视器是 UCON 终端核心模块。其结构如图 2 所示。UCON 监视器包括 UEF(使用控制实施模块)和 UDF(使用控制决策模块)两部分。UEF 负责使用控制的实际执行，UDF 提供决策结果。UEF 分为安全模块、主控模块、更新模块。安全模块负责认证许可证、解密、解析许可证；更新模块负责即时更新主客体属性。主控模块负责调用 UDF 获取决策结果、监控用权情况作出即时控制。UDF 分为授权模块、责任模块、条件模块三部分，通过分析加载于内存中的 UCON 许可证 dom 树进行决策，决策结果返回 UEF。

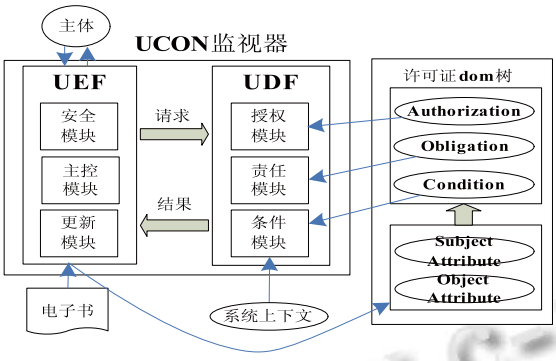

图 2　UCON 监视器

UDF 访问控制决策流程如图 3 所示。UDF 接到 UEF 发出的决策请求，查找许可证索引表，分别得到用户专属许可则和电子书专属许可证，利用服务器公钥验证许可证签名，若认证成功，则信任许可证，并查看许可证版本，若许可证非最新则更新许可证，然后使用用户私钥解密许可证。系统把解密好的许可证载入内存，生成 dom 树解析，依据权限、授权、条件、责任四个节点进行决策判定。决策过程中反复验证责任是否被履行。如果四节点判定皆为“permit”，则根据情况执行属性更新，最后返回 permit。否则返回 deny。

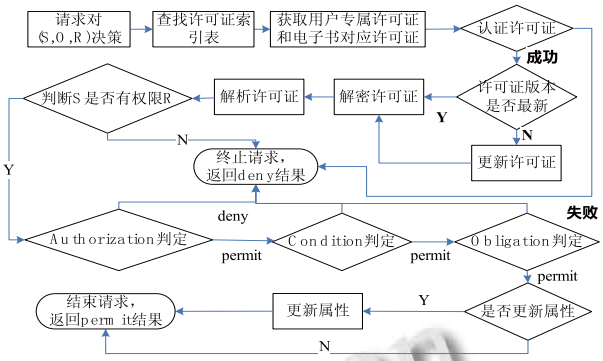

图 3　UDF 访问控制决策流程

4　系统测试

为测试本无线阅读 DRM 系统的有效性，配置测试环境如下：服务器是 Dell PowerEdge 2850，操作系统是 Linux AS 4，UCON DRM 服务端使用 EJB 3.0 技术实现，部署在 JBoss 4.2.3 上；DRM 终端环境为 Symbian s60，UCON 监视器采用 J2ME 实现。访问控制决策模块分别使用两套方案，方案一为基于 UCON 的 DRM 系统，方案二沿用传统 OMA DRM[1]标准实现。服务器和终端通过 wifi 技术进行网络链接。DRM 终端分别模拟单次点播、包月、计时三种业务分别进行 100 次测试，分别记录从终端发出阅读请求到认证、解密、解析许可证，再到使用控制决策成功返回决策请求的平均时间。由测试结果(图 4)可知，使用 UCON 方案的 DRM 系统决策性能上与传统 OMA DRM 方案相近，说明本系统具有较好的可用性。

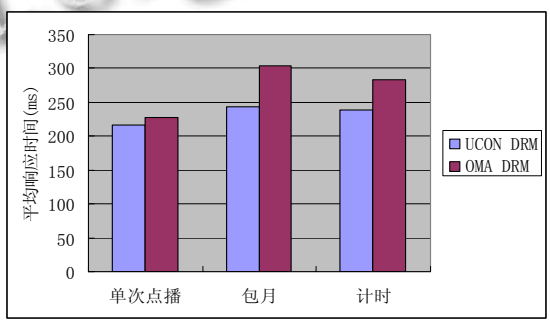

图 4　测试结果

在阅读电子书期间，用户需浏览至少一次广告，如没有履行该责任，系统会弹出对话框询问用户是否执行浏览动作(图 5)，如用户选择“取消”，系统将回收用户阅读权限。系统具有良好的动态授权控制能力。

(下转第 77 页)

表 3 GA、QGA 和 IQGA 计算结果对比

问题规模	GA			QGA			IQGA		
（M×N）	最好解	平均解	平均收敛代数	最好解	平均解	平均收敛代数	最好解	平均解	平均收敛代数
3×7	0.888737	0.861924	44.81	0.888737	0.86235	58.81	0.888737	0.864903	57.81
5×10	0.951167	0.927218	102.12	0.951622	0.932738	97.7	0.951622	0.934298	81.3
7×15	0.79348	0.74523	101	0.79348	0.76672	70.76	0.79348	0.766804	71.25
9×20	0.90459	0.84725	126.35	0.907194	0.862426	116.25	0.907194	0.875632	108

5 结语

本文提出的改进的量子遗传算法能有效地求解模糊交货期多机并行调度问题，解决了传统量子遗传算法更新操作依赖于二进制位、满意度和最优解的缺陷，克服了传统量子遗传算法在量子位观测值与最优解无直接联系时容易陷入局部最优解的缺点。

参考文献

1 吴悦,汪定伟.用遗传算法解模糊交货期下 low-shop 调度问题.系统工程理论与实践,2002:108–112.

2 Han KH, Kim JH. Quantum-inspired evolutionary algorithms with a new termination criterion, H8 gate, and two-phase scheme. IEEE Trans. on Evolutionary Computation, 2004, 8(2):156–169.

3 张葛祥,李娜,金炜东,胡来招.一种新量子遗传算法及其应用.电子学报,2004,32(3): 0372–2112.

4 黄德才,郭海东.基于 JIT 的非等同并行多机调度问题的混合遗传算法.计算机集成制造,2004,10(3):1006–5911.

5 杨淑媛,刘芳,焦李成.一种基于量子染色体的遗传算法.西安电子科技大学学报,2004,31(1):76–81.

6 熊焰,陈欢欢.一种解决组合优化问题的量子遗传算法 QGA.电子学报,2004,32(11): 0372–2112.

7 王万良,吴启迪.生产调度智能算法及其应用.北京:科学出版社,2007.

8 王宇平,李英华.求解 TSP 的量子遗传法.计算机学报, 2007, 30(5):748–755.

9 李士勇,李盼池.量子计算与量子优化算法.哈尔滨:哈尔滨工业大学出版社,2009.

(上接第 34 页)

图 5 终端界面

5 结语

本文提出的基于 UCON 无线阅读 DRM 系统具有以下优点：1）系统确切地表达了责任、条件、授权三个决策因素，逻辑清晰，具有较强的动态授权控制能力。2）系统的性能与传统 OMA DRM 系统相比性能相近，表明系统具有较好的可用性。3）系统采用 UCON 模型，该模型能够统一传统访问控制模型，具有良好的可扩展性。下一步我们将在 UCON 基础上完善权利描述语言 REL。

参考文献

1 Open Mobile Alliance. DRM Specification Approved Version 2.1.1 – 06 Avr 2010.

2 Park J, Sandhu R. Usage control: A vision for next generation access control. International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, 2003,2(1):17–31.

3 钟勇,秦小麟,刘凤玉.一种面向 DRM 的责任授权模型及其实施框架.软件学报,21(8):2060–2061.

4 Park J, Sandhu R. The UCONABC Usage Control Model. ACM Trans. on Information and System Security(TISSEC), Feb 2004.