

资源的数字权利保护机制研究^{*})

刘清堂 杨宗凯

(华中科技大学电子与信息工程系 武汉 430074)

摘要 数字权利保护机制是数字版权管理(DRM)研究的重要内容。数字权利描述语言为权利执行提供了权利描述信息。本文首先通过权利信息描述和资源的元数据描述的整合提出了教育资源的数字权利许可证基本模型。然后,文章探讨了教育资源的权利可执行性问题,并将可执行性依据归结为权利信息、技术支持和可信任的执行环境三个方面。接着,文章提出了教育资源的数字权利执行模型,并通过许可证的描述、执行机制的分析和探讨以及实例设计,研究了许可证执行的基本方法和策略。

关键词 数字权利,执行机制,许可证,模型

Research on Digital Rights Protection Mechanism of Learning Resources

LIU Qing-Tang YANG Zong-Kai

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)

Abstract Digital rights enforcement plays an important role on digital rights management. Digital rights expression language provides basic description information for rights enforcement. Firstly, the paper brings out license model of usage of learning resources by integrating learning object metadata specification with rights expression language. Secondly, it discusses probability of rights enforcement. The requirements of right enforcement lie in rights metadata, technology and "trusted" environment. Lastly, the paper probes into enforcement mechanism of learning resources to interpret, explain and implement their licenses.

Keywords Digital rights, Enforcement mechanism, License, Model

1 引言

数字版权管理(DRM)是基于信息安全技术的综合解决方案,它能有效地阻止对数字内容的非法使用和拷贝,以达到保护数字知识产权的目的。数字版权管理的主要内容包括对有形和无形资产的各种权利使用形式进行描述、认证、交易、保护、监控、记录和追踪等,也包括对权利拥有者之间关系的管理^[1]。数字版权管理是“权利的数字化管理”,而不是“数字化权利的管理”^[2,3]。数字版权管理依赖于信息安全,也包括复杂的问题,如法律条款、电子商务和系统可用性等。数字权利描述语言在数字权利执行和管理中扮演着重要的角色。它涉及资源的拥有者和使用者之间的权利使用管理,通常采用许可证形式描述资源使用权利的授予、需求条件和履行义务等之间的关系。

目前国内外许多组织正在探讨数字版权管理的标准化问题,如 OEBF (Open E-Book Forum)、MPEG、W3C、ODRL (Open Digital Rights Language)、ContentGuard、中国网络教育技术标准化委员会等^[6-8]。数字权利描述语言数字版权管理标准化的内容之一 MPEG21 定义了权利描述语言和数据字典对多媒体描述框架的知识产权管理进行权利描述。ODRL 通过描述资源、用户和权利三者关系建立数字权利描述信息模型。XrML (eXtensible Rights Markup Language) 采用权利,条款(terms)和条件表示权利关系。这些权利描述语

言已经被广泛地应用到多媒体、移动通信、电子出版等多个领域。如何结合已有的教育资源标准和权利描述语言设计许可证模型成为权利保护的首要问题。许可证描述的权利信息是否可执行?如何执行?以及针对教育的具体应用环境如何设计权利执行模型,许可证执行机制如何?如何解析、解释和验证许可证,并提供必要的控制信息是教育资源的数字版权管理考虑的主要问题。

2 数字权利语言与资源描述

权利描述语言信息模型包括三个基本的核心组件:权利、资源和用户,在教育资源的权利描述中需要的条件和履行的义务也是考虑的重要内容。数字权利语言应用于教育需要与已存在的网络教育技术标准整合使用。教育资源使用许可证的基本组件如下:

用户:资源提供商、资源的使用者和资源的贡献者等,通常使用学习技术标准如 LOM (Learning Object Model) 描述^[11-13];

权利:对资源的使用指定的权利,通常使用权利描述语言描述;

资源:需要指定权利的教育资源,通常采用教育技术标准描述,如 LOM 等;

条件:获取资源的使用权限时,需要遵循的条件,需要整合权利语言和教育技术标准进行描述;

^{*}项目来源:国家“十五”重大科技攻关项目“网络教育关键技术及示范工程”,教育资源描述组织与注册发现技术(专题编号,2001BA101A12)和教育部“标准化教育资源内容服务系统”(教技司[2004]104号)。刘清堂 讲师,博士,主要从事多媒体技术,远程教育,数字版权方向的研究工作。

义务:对应于一定的权利,主体必须履行一定的任务,通常采用权利描述语言描述;

教育资源的权利描述为资源的使用权利控制和管理提供了依据,同时也为资源的知识产权保护提出了新的要求:(1)资源的许可证执行可行性;(2)资源的版权保护体系;(3)资源的许可证描述和解析机制。

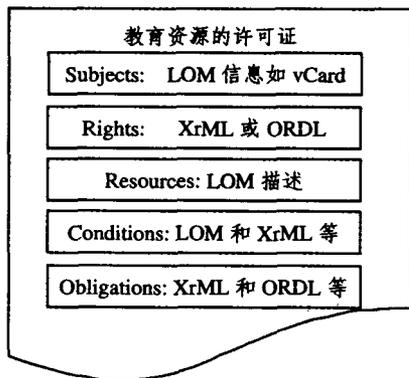


图 1 整合资源的元数据标准的许可证模型

3 权利的可执行性

权利的表达、使用和访问控制机制通常使用许可证形式描述。通过许可证,可以验证权利合理性并确定其可执行性。并不是所有的权利都可以采用数字权利描述语言表达。权利是否可被计算机执行可划分为^[9]:

非可执行的权利:指不依赖计算机技术和环境支持的使用权利,用于授予使用者对资源的使用权利,如法律授权书等;

潜在的可执行权利:指在一定的环境和计算机技术条件下,授予给使用者对资源的使用权利;

可执行的权利:能被计算机监视和观察的资源使用权利。权利执行的需求信息、技术支持和可信任的执行环境是权利可执行的基本条件。

权利执行的需求信息是权利执行的首要条件。需求信息必须能被权利执行系统记录和应用。如当消费者访问我们的网站后,就可以使用网站的学习资源。对权利执行系统而言,“当消费者访问我们的网站后”这个前提条件信息是难以被权利执行系统记录。

权利执行的技术支持是指相关的技术能支持、监视和控制资源的权利执行过程。如学习者能播放“计算机系统结构”课件一次。这个例子中包含了权利执行的相关信息,然而播放一次的控制就需要有能监视和控制执行过程的计算机支持。

可信任的执行环境是指为保证资源执行过程中的安全性。为防止盗版,权利的执行应在可信任的环境中。对于学习资源,资源的权利控制在服务器比在客户方的权利执行更容易和更具有可控性。

不同等级的权利执行分类中,非可执行的权利不能满足三个条件,潜在的可执行权利不能满足可信任执行环境的条件,而可执行的权利同时满足三个条件。

4 权利的执行

4.1 资源的数字权利执行模型

OpenDRM 项目定义一个 DRM 参考模型,包括内容服

务、许可证服务和客户端三个基本组件^[1~10]。其中,内容服务涉及内容保护的安全性;许可证服务总是与权利授予和一定的电子交易模式相关;客户端是权利执行的重要部件。数字资源的数字权利执行控制模型如图 2 所示。

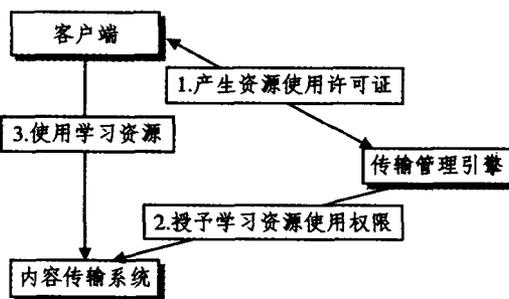


图 2 学习资源的传输与控制管理

该模型中,学习资源的描述与物理文件分开存储。学习资源的描述通过平台进行管理和存储,而学习资源通过内容提供者 and 传输系统传输。学习资源的传输与控制分为三个基本过程:许可证产生,授予学习资源的访问权利和访问学习资源。

许可证产生:客户端申请学习资源使用许可证。使用许可证可采用 XrML、ODRL 等权利描述语言以数字形式描述。相关的信息包括资源标识、用户标识等;

授予学习资源的访问权利:传输管理引擎初始化内容传输系统,依据资源的使用权限向学习者传输使用受控制的学习资源;

学习资源使用控制:学习者依据预定义的权利使用学习资源。资源的使用权利通过可信任的环境执行,如使用时间、次数的限制,打印、复制和浏览权利限制等。

4.2 许可证的描述

依据如图 1 所示教育资源的许可证模型,假设学习资源 music03. mp3 的使用有付费义务、具有播放权限,受到时间的限制等,其 XML 的权利描述格式如图 3 所示。其中 License 表示许可证,contract 表示授予权利,rightHolder 表示权利拥有者,play 表示授予权利(播放),audioResource 表示使用的资源,timeLimit 属于限制,而 payment 属于义务。

```

<license>
  <contract id = '001'>
    <rightHolder>.....</rightHolder>
    <play/>
    <audioResource id="music. mp3" url="urn: avs: musicCompa-
      ny">
      <dsig: DigestMethod Algorithm=
        "http:// www. w3. org/2000/09/ xmldsig# sha1"/>
      < dsig: Digest Value > 0kccZ4a3zFW9O
        PT1qElqSg==
      </dsig: Digest Value>
    </dsig: DigestMethod></audioResource>
    <timeLimit>
      <startTime>2003-01-01T00:00:00</startTime>
      <overTime> 2003 - 12-31T12: 59: 59 </overTime> </time-
        Limit>
    <payment>
      <amount> 20. 00 </amount>
      <currency> RMB <currenc><payment/>
    </contract>.....
</license/>
    
```

图 3 许可证的描述

4.3 数字权利执行机制

数字权利管理平台应该充分考虑系统的扩展性、系统间的互操作性。除了权利描述语言采用标准化的描述策略外,

系统的架构和运行机制之间应考虑普适性、灵活性和可扩展性。如图 4 所示是权利执行系统概念设计图。概念设计模型包括学习资源版权管理、内容管理传输和客户端三个部分。

学习资源版权管理包括传输管理引擎和权利执行接口。传输管理引擎通过权利执行接口为教育资源提供方和使用者提供权利信息支持。内容管理传输通过权利执行模块提供教育资源的访问权利控制,为客户端提供使用权利受控制的教育资源。客户端通过权利执行模块获取内容管理传输系统的受控学习资源,并依据使用控制信息进行学习资源的使用控制。

学习资源版权管理为客户端和内容管理传输提供了权利执行的接口,其主要作用在于通过许可证描述信息,为学习资源的访问控制和使用控制提供必要的信息。

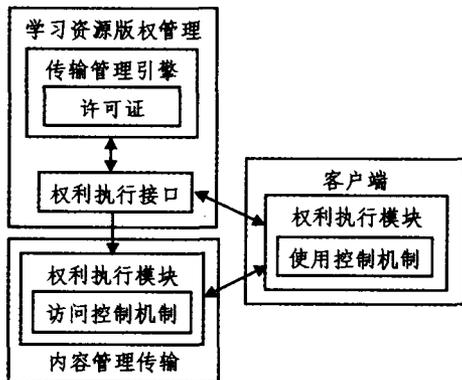


图 4 权利执行系统概念设计图

许可证标准化描述为学习资源的使用权利一次申请,不同平台可互操作提供了可能,并且权利的执行在访问和使用控制方面应具有独立性。教育资源的数字版权管理功能包括:

- (1)许可证应能够被版权管理平台的传输控制管理引擎解析和解释;
- (2)版权管理平台应包括权利执行接口,用于向传输服务器提供权利执行信息;权利执行接口能提供权利元数据用于表示权利使用信息;
- (3)权利执行接口能与内容传输服务器的权利执行模块之间进行通信,并传递权利执行信息;
- (4)权利执行模块能解释访问控制信息,并执行访问控制信息。传输服务器可使用不同的访问控制机制,如基于角色控制(RBAC)、访问控制列表(ACL)和 HTTP 访问控制等。
- (5)客户端权利执行模块能根据传输的学习资源的控制信息进行资源的使用控制。
- (6)传输管理引擎能通过许可证信息为不同的权利管理平台提供了互操作的机制。

4.4 许可证的执行

如图 5 所示是许可证执行过程图。它主要考虑了如何在许可证中抽取访问控制信息,检测和验证许可证保证其完整性、可鉴别性。主要的过程包括:

- (1)权利的使用者如客户端申请许可证,并请求服务;
- (2)传输管理引擎,用于执行许可证检测和解释许可证内容信息,生成访问控制信息;
- (3)访问控制服务。依据许可证控制信息,决定学习者对学习资源的使用控制和访问控制权利,授予相关的权利,履行

相关的义务。

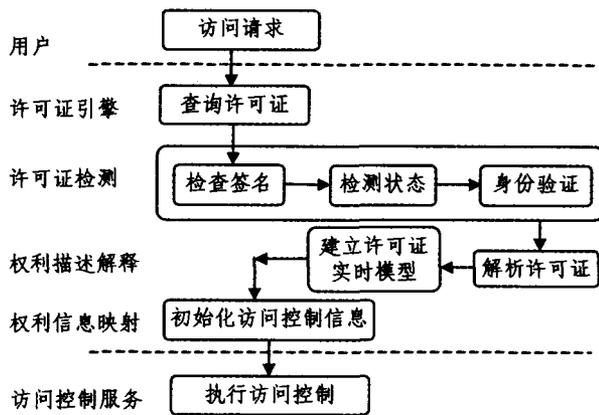


图 5 许可证的执行

用户的访问请求触发许可证的处理过程。一个访问请求表示一个对具体资源执行某项权利的要求。每个访问请求包括:

<主体、权利、资源、限制、义务、许可证标识号>

许可证执行引擎可以通过 HTTP 或 SOAP 服务绑定执行。当接收到一个访问请求,许可证引擎通过许可证号查找相关的许可证。当许可证被加载后,相关的操作被执行:

- (1)许可证签名检查:通过数字签名,验证许可证的完整性及来源。
- (2)许可证状态检测:验证许可证的可用状态,避免许可证的重复执行和超权限使用;
- (3)用户身份验证:用于验证用户的身份,通常采用 X.509 证书。

如果许可证成功通过检测,则是合法的。REL 解释器解析许可证,并抽取访问控制信息,建立一个实时的许可证对象模型,用于查询相关的许可证中对象属性如权利拥有者信息、使用者信息和内容标识信息等。

4.4 教育资源的权利执行

依据教育资源的权利执行概念设计图,我们设计了教育资源的版权管理系统的基本功能单元。权利持有者和使用者之间许可证发布的基本流程如图 6 所示。

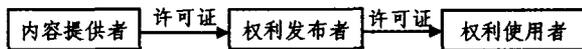


图 6 许可证的发布

内容提供者向权利发布者提供资源的使用许可证,并限定资源使用的权限范围,许可证发布者依据授予的权限范围和用户的需求向用户发布许可证。发放的许可证存储在许可证服务器上。如图 7 所示,当用户申请使用某种资源时,内容服务器查询该用户许可证;版权管理模块获取许可证并解析,获取控制信息;内容传输服务模块依据控制信息产生使用控制信息,并在教育资源中嵌入相关的使用管理信息;客户端获取该资源内容,并依据使用控制信息使用资源。

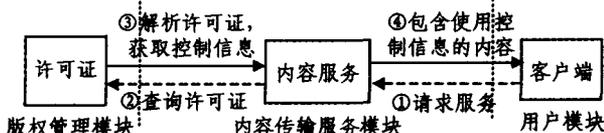


图 7 权利的执行与控制

小结 数字权利的保护机制依赖于权利描述语言和信息安全技术。权利描述语言为学习资源的权利保护提供必要的描述信息。教育资源的元数据描述信息和数字权利语言的整合使用为主体、资源、权利、条件和义务等若干要素的描述提供了可能。

权利的可执行性问题是数字版权管理的首要问题,它依赖于需求信息、技术支持和可信任的环境。由此权利又可进一步划分为非可执行的、潜在可执行的和可执行的权利。教育资源的数字权利执行模型为权利的可执行性提供了一种使用方案,为教育资源的数字版权管理提供了一种基本模型,该模型包括三个基本过程:许可证产生、访问权限的授予和学习资源的使用控制。许可证执行机制的概念设计图包括学习资源的版权管理、内容管理传输和客户端三个部分,许可证的管理、解析、检测和解释等是各部分的中心内容,权利执行接口和权利执行模块为学习资源的访问控制和权利使用控制提供了基础。

参考文献

- 1 Iannella R. Open Digital Rights Management. Position paper for the W3C DRM Workshop, 2000, Online. Available at: <http://www.iprsystems.com>
- 2 W3C Workshop on Digital Rights Management for the Web: Workshop Report, 2001

- 3 Iannella R. digital Rights Management Architectures. [Online] www.dlib.org/dlib/june01/iannella/06iannella.html
- 4 Erickson J S, Norwich V. OpenDRM: A Standard Framework for Digital Rights Expression, Messaging and Enforcement. [Online]. <http://personal.hpl.hp.com/joberi/opendrm-project.htm>
- 5 Liu Qiong, Safavi-Naini R, Sheppard N P. Digital Rights Management for Content Distribution. Australasian Information Security Workshop 2003 (AISW2003), Adelaide, Australia. Conferences in Research and Practice in Information Technology, Vol. 21. C., 2003
- 6 Iannella R. Open Digital Rights Language. 2000, Online. Available at: <http://odrl.net/odrl-08.pdf>
- 7 ContentsGuard Inc. XrML: Extensible rights Markup Language. 2000, Online. Available at: <http://www.xrml.org>
- 8 MPEG (Motion Picture Experts Group). (2001): MPEG-21 Working Documents (IPMP Part). <http://mpeg.telecomitalia.com/working-documents.htm>
- 9 Guth S, Koppen E. Electronic Rights Enforcement for learning media. Available at: <http://nm.wu-wien.ac.at/people/Guth/ical45.pdf>
- 10 Guth S, Koppen E, Strembeck M. Experiences with the Enforcement of Access Rights Extracted from ODRL-based Digital Contracts. ACM DRM'03. October 27, 2003, Washington, DC, USA
- 11 Abruf. IEEE Learning Technology Standards Committee (L.TSC). Learning Object Metadata - Draft Document v6. 0. <http://ltsc.ieee.org/doc/wg12/>, 2001
- 12 CELTSC. 学习对象元数据规范. 版本 1.6, CELTS-3.1
- 13 The SCORM Overview, SCORM version1. 2. <http://www.adlnet.org/ADLDOCS/Documents/SCORM-1.2-Overview.pdf>, 2001. 10. 01

(上接第 26 页)

an 进行逼近, 即: $V_{wopt}(n) \approx an$, 将其代入式(6), 可以将接入控制策略简化为:

$$W'_{opt}(r, c, n_0) = \begin{cases} 1, & (\frac{r}{c} \geq \frac{a}{2} \text{ AND } n \geq c) \\ 0, & (\frac{r}{c} < \frac{a}{2} \text{ OR } n < c) \end{cases} \quad (9)$$

如图 4 所示的 $V_{wopt}(n) \approx n$, 因此采用 *Accept if $r/c > 0.5$* 的“阈值准则”所能获得的平均总用户收益和最优接入控制策略所能获得的平均总用户收益是近似相等的。

根据这一观察, 我们可以对接入控制策略进行简化以使其实现复杂度大为降低, 同时又能获得近似最优的总用户收益期望值。具体做法是首先通过仿真的方法按照本文介绍的求解过程得出序列 $V_{wopt}(n)$, 然后寻找能逼近 $V_{wopt}(n)$ 的最优的线性函数 $a_{opt}n$ 。在找到 a_{opt} 后, 让每个 Sink 保留 a_{opt} 。在应用产生后, 按式(9)给出的“阈值准则”直接判断该应用是否接入即可。

结论 节省能量延长网络生命期是无线传感器网络研究的关键, 现有的研究工作主要从单应用的角度出发来进行研究。但实际的无线传感器网络往往需要支持多应用, 从而引入了新的节能及最大化网络价值的问题。本文从无线传感器网络中在多应用场景下的节能问题出发, 研究了针对多应用分布式接入控制策略。其目的为在网络能量耗尽之前获得的总用户收益期望值最大。在研究多应用接入控制的问题时, 我们发现问题的关键在于应用的发生是动态随机的, 而每一个应用的 Reward 和 Cost 在应用发生之前也是未知的。因此, 我们将多应用接入控制问题等效成为一个特殊的“动态随机背包问题”, 并根据相关理论对该问题进行了建模。为了求解这一模型, 我们还设计了估计应用 Reward 和 Cost 的联合概率分布 $P(r_i, c_i)$ 的方案。最后根据已有的求解类似模型的相关算法对该问题进行了求解, 并据此设计了相关的最优接入控制策略。经实验表明, 我们提出的多应用分布式接入控

制策略能在各种网络初始能量配置的情况下均获取显著的总用户收益值的提高。同时在实验最优接入控制策略的过程中, 发现可以采用一个最优阈值的“阈值准则”来获取次优解, 从而可以大大降低接入控制策略的复杂性。

参考文献

- 1 Min R, Furrer T, Chandrakasan A. Dynamic Voltage Scaling Techniques for Distributed Microsensor Networks. In: Proc. of the IEEE Computer Society Annual Workshop on VLSI (WVLSI'00), 2000
- 2 Ludwig J T, Nawab S H, Chandrakasan A. Low-Power Digital Filtering Using Approximate Processing. IEEE Journal of Solid-State Circuits, 1996, 31(3): 395~400
- 3 Schurgers C, Aberborne O, Srivastava M. Modulation scaling for energy-aware communication systems. In ISLPED, 2001. 96~99
- 4 Cui S, Goldsmith A J, Bahai A. Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks. IEEE Journal of Selected Areas in Communications, 2004, 22: 1089~1098
- 5 Park S, Srivastava M. Power aware routing in sensor networks using dynamic source routing. ACM MONET Special Issue on Energy Conserving Protocols in Wireless Networks, 1999
- 6 Schurgers C, Tsiatsis V, Ganeriwal S, Srivastava M. Topology management for sensor networks: exploiting latency and density, MobiHoc'02, 2002. 135~145
- 7 Vardhan S, Wilczvnski M, Portie G J, Kaiser W J. Wireless integrated network sensors (WINS): distributed in situ sensing for mission and flight systems, Aerospace Conference Proceedings, March 2000, 7: 18~25
- 8 Yuan Y, Chen W Q, He J. Convex Optimization Based Energy Efficient Transmission Scheme for Wireless Sensor Networks, submitted to IPSN 2005
- 9 Boulis A. Programmable Sensor Networks: Framework and Applications. [Ph. d. Dissertation]. University of California, Los Angeles, 2003
- 10 Boulis A, Srivastava M. Node-level Energy Management for Sensor Networks in the Presence of Multiple Applications. In: Proc of Percom'2003, March 2003. 41~49
- 11 Kleywegt A J, Papastavrou J D. The Dynamic and Stochastic Knapsack Problem, Operations Research, 1998, 46
- 12 Kleywegt A J, Papastavrou J D. The Dynamic and Stochastic Knapsack Problem With Random Sized Items, Operations Research, 2001, 49
- 13 PARSEC Project. Available at: <http://pcl.cs.ucla.edu/projects/parsec>