第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·网络与通信· 文章编号：1000—3428(2007)12—0122—03 文献标识码：A 中图分类号：TP393

基于 P2P 模式的 DRM 系统体系和协议研究

徐海银，佘党恩，李 丹，董九山
(华中科技大学计算机科学与技术学院，武汉 430074)

摘 要：在分析了 P2P 网络模式和数字版权管理(DRM)技术体系的基础上，提出基于 P2P 模式的 DRM 系统体系，并对系统体系结构和传输协议进行了研究和探讨。基于体系的拓扑结构，提出了体系功能框架，并对其中内容管理、内容标识、付费机制和质量控制进行分析和设计。同时以数字内容的生命周期和价值链为依据，对体系的工作流程进行了深入的探讨。给出了体系的数字内容上传和下载协议，实现了 P2P 网络模式与 DRM 技术体系的有效集成。

关键词：数字内容；P2P 网络；数字版权管理(DRM)

Research on DRM System Architecture and Protocol Based on P2P

XU Haiyin, SHE Dang'en, LI Dan, DONG Jiushan
(School of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan 430074)

【Abstract】 This paper discusses a digital rights management（DRM）system applicable to P2P network, and advances its systematic architecture and basic protocol. The P2P-based DRM architecture includes topological structure, functional assignment and working flow, and focuses on the content management, content identification, royalty payment and quality control technologies. It puts forward its digital content uploading and downloading protocols, achieving an effective integration of P2P model and the DRM technologies.

【Key words】 Digital content; P2P network; Digital rights management(DRM)

与传统客户/服务器(C/S)模式的网络相比，P2P网络(P2P network)具有直接、快速、灵活的数字内容传输优势[1]。与此同时，P2P技术的发展也引发了一系列争议，主要集中在它对现有版权体系的巨大冲击以及它带来的信息控制上的困难等方面。1999 年，美国Napster版权案的出现成为P2P网络构成对数字内容版权侵犯的标志，直到今天，Napster公司仍然没有摆脱困境。

P2P网络技术的不断发展和广泛应用给开放式网络环境下数字内容的数字版权管理(digital rights management, DRM)带来更大的挑战。传统的DRM技术体系是基于C/S模式，面对P2P网络也有所力不从心[2]。直面P2P网络存在的数字内容版权问题，需集成DRM技术体系到P2P网络模式中，从而建立系统完整的P2P网络下数字内容版权管理体系[3]。

本文提出了系统可行的基于 P2P 模式的 DRM 系统体系，通过结合研究 P2P 网络模式以及 DRM 功能特性，在体系中实现了 P2P 网络模式与 DRM 技术体系的有效集成，从而形成完整可行的协同解决 P2P 网络下数字内容版权管理的解决方案。

1 基于 P2P 模式的 DRM 系统体系结构

根据目前P2P的发展，P2P网络可以划分为纯分布式P2P网络和混合式P2P网络两大类。纯分布式P2P网络中取消了服务器，链状的节点之间构成一个分散式网络；混合式P2P网络中各节点之间可以直接建立连接，但网络的构建需要服务器，通过集中认证，建立索引机制[1]。

本文提出的基于 P2P 模式的 DRM 系统体系是以混合式的 P2P 网络为基础，由可信中心服务器和 P2P 服务网络组成。其中，可信中心服务器是一个瘦服务器，提供可信的数字内容版权控制管理技术支持；P2P 服务网络是分布式的 P2P 网络，由基于点对点网状拓扑结构的若干节点主机组成，任意节点之间以对等方式进行通信。可信中心服务器与 P2P 服务网络中的节点主机建立普遍的通信链路，通过特定的传输协议实现对各节点的有效控制和管理。

1.1 功能框架

DRM技术体系的基本功能包括：数字内容加密，阻止非法内容注册，用户环境检测，用户行为监控，认证机制，付费机制和存储管理[2,4]。通过合理地分配DRM处理到体系的两端，形成系统的功能框架，如图 1 所示。

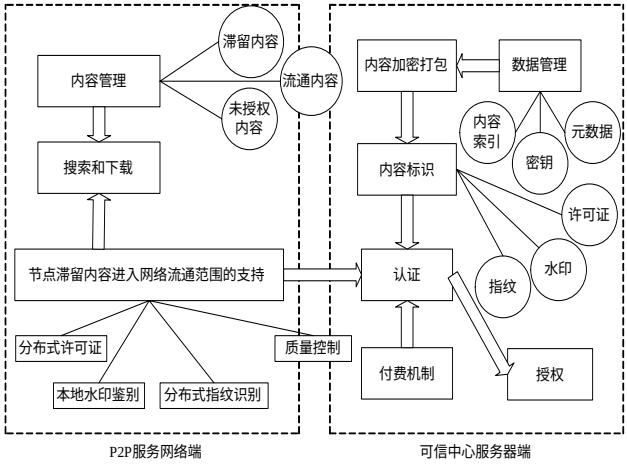

图 1 功能框架

基金项目：国家自然科学基金资助项目(50305007)
作者简介：徐海银(1968－)，男，博士、副教授，主研方向：数字媒体技术，信息安全；佘党恩，硕士；李 丹，博士；董九山，硕士
收稿日期：2006-07-08 **E-mail：**haiyinxu@mail.hust.edu.cn

在体系中，可信中心服务器提供基本的数字内容提供商版权的标识、发布、认证、授权以及付费机制的管理，同时提供秘密数据的管理机制，包括索引信息、密钥和元数据等；P2P 服务网络实现数字内容的分布式存储、搜索和下载以及节点滞留内容进入网络流通范围的支持(包括分布式许可证、本地水印鉴别、分布式指纹识别、质量控制等)，同时，协同可信中心服务器建立认证机制。

1.1.1 内容管理

在体系中，基本数字内容划分为 3 种类型：流通内容，滞留内容，未授权内容。流通内容是分布在整个网络体系中并在网络节点之间相互交易传输的一种数字内容。流通内容在网络中形成一个公有的大型分布式数据库，其基本数据元是经加密后形成的打包内容；滞留内容是存放在节点主机上的未加密的一类节点私有数字内容，节点滞留内容在用户主机上构成私有数据库；未授权内容是一类位于用户主机上从网络中下载但得不到可信认证授权的内容。恶意用户对数字内容进行非法下载和传播，这些内容就被划分为未授权内容。

网络流通内容、节点滞留内容、未授权内容构成整个体系中的基本数字内容，它们之间在一定的条件之下可以相互转换。节点主机从网络中下载流通内容，经过合法认证授权后解密、存储，成为滞留内容，节点滞留内容经过加密打包可以进入网络流通范围；流通内容下载到节点主机如果无法得到合法认证，则成为未授权内容，未授权内容经过再传播进入网络流通；一旦未授权内容重新获得合法认证和授权，经过解密可以存入节点私有数据库中，成为滞留内容，非法传播节点滞留内容使得内容进入未授权领域，成为未授权内容。

1.1.2 内容标识

当数字内容从公有数据库传输到节点私有数据库的时候，数字证书机制构成数字内容搜索和付费的重要手段。整个体系需要建立数字内容的标识以及关联这些标识机制到一个支持付费设施的认证许可系统。在该体系中，提出了 3 种数字内容的标识机制，即：

(1)授权上载标识

如果数字内容是由一个已授权服务器所提供，那么该服务器将关联此内容一个特征数字证书以保证数字内容的安全标识，同时也需要关联数字内容质量、许可证以及版权信息。

(2)数字水印标识

当数字内容未通过可信中心服务器认证授权而直接进入 P2P 网络，这时 P2P 网络可以通过检测内容中是否含有数字水印来尝试建立对数字内容的标识。如果检测到数字水印信息，P2P 服务网络则可以从可信中心服务器重新得到适当的许可信息。

(3)数字指纹标识

当用户私有数据库中的数字内容没有任何显式标识信息的时候，可以通过查询数字指纹数据库并从中提取可用于标识的数字指纹来实现内容标识。数字指纹的搜索是一个复杂集中化的过程，需要占用大量的资源，快速指纹搜索需要通过建立在分布式的数字指纹数据库上的并行处理算法完成。

1.1.3 质量控制

当读取的数字水印信息提供给可信中心服务器时，数字内容质量检测和控制是必需的，质量控制可以由可信中心服务器或者客户端通过直接的质量控制程序完成，在获得水印信息后对数字内容的质量进行检测和控制，但是一旦未授权内容过多，可信中心服务器的质量控制势必成为系统的瓶颈；为了减轻服务器端的负担，该体系采取的是在用户终端进行质量控制，可信中心服务器通过发送感知数据给客户端允许用户在终端对数字内容进行质量分析，分析结果直接反馈给可信中心服务器，这样既减轻服务器端的负担，又实现了数字内容质量分布式的管理和控制。

1.2 工作流程

数字内容从制作、发布、交易、使用直至销毁过程中完成了它的全生命周期，在数字内容的全生命周期中，内容本身因为创建、交换以及使用的过程使得它具备了基本的价值，随着生命的延续，数字内容在支撑环境中形成自身的价值链。通过对数字内容全生命周期和价值链的分析，可以得出数字社会中客体世界的运作规则和机制。

基于 P2P 模式的 DRM 系统体系是以数字内容在网络环境中的生命周期和价值链为依据，包括数字内容的创建、保存、管理与分发，以及数字版权和交易管理等多个环节。原始数据内容一经创建即进入生命周期过程，通过数字内容提供商对其进行安全保护处理之后进入网络发布，客户可以通过请求和付费后，由服务器认证授权发放许可后以不同的方式获得数字内容。整个流程中包含数字内容的交易和数字版权的控制管理，其工作流程如图 2 所示。

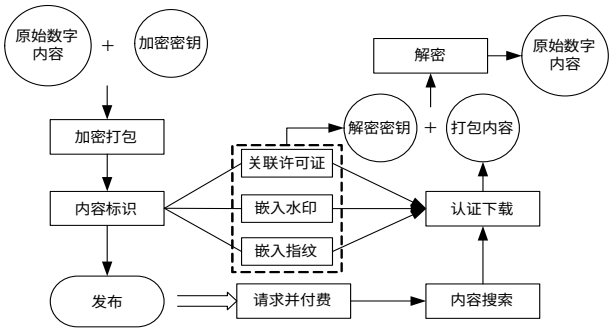

图 2 工作流程

在体系的工作流程中，由可信中心服务器提供用于加密打包的加密密钥，原始数字内容经过加密打包后成为打包内容，在网络发布之前需要经过内容标识以嵌入相关的版权维护信息，包括关联许可证、嵌入水印、嵌入指纹标识方法；网络客户通过请求并付费，再经过内容搜索可从网络发布内容中找到用户要求的数字内容，经过与内容标识对应的下载协议认证授权后，用户获得打包数字内容，并在内容标识中获得解密密钥，经过解密密钥解密打包内容即可获得原始数字内容。在以数字内容为中心的整个工作流程中，可信中心服务器和 P2P 服务网络分别承担各自的功能处理，通过两端之间的信息交互和网络通信协议控制了整个体系的有序工作。

2 基于 P2P 模式的 DRM 系统传输协议

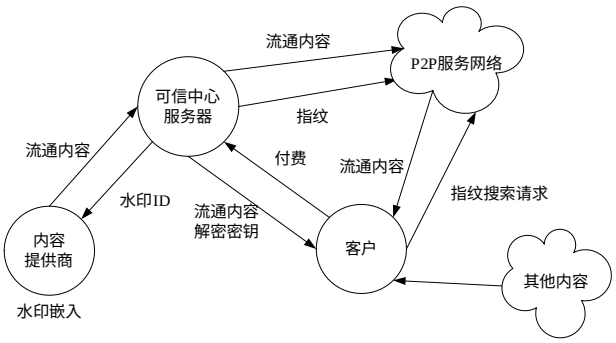

图 3 传输协议

在基于 P2P 模式的 DRM 系统传输协议中，数字社会下的主体对象是主要角色。通过对主体对象之间的数据流动和交易规则进行规范，保证整个体系的有序运作，如图 3 所示是体系传输协议的总体图解。数字内容的传输过程分为内容上传和内容下载两个部分，通过内容上传和内容下载协议实现了数字内容传输过程中版权的安全有效管理。

2.1 上传协议

内容提供商选取数字内容，并与可信中心服务器交涉，产生数字水印 ID，嵌入水印到原始数字内容并上传到可信中心服务器中。服务器接收内容，并分配唯一标识该内容的数字许可证与之相关联，许可证中含有相关的版权信息和元数据。同时，产生数字指纹来标识未授权的数字内容。服务器选择一个加密密钥对数字内容进行加密，解密密钥存放在数字许可证或者数字指纹中。适当的节点存储加密的打包数据内容和数字许可证，其余节点存储数字指纹和指向可信中心服务器上的关联许可证的指针。

2.2 下载协议

根据不同的内容版权标识方式，数字内容下载协议包含以下 3 种方式：

(1)直接下载

如果用户直接从信用卡或者安全的付费设备中获取了合法的授权许可，客户可以直接请求服务器获得内容的解密密钥，同时，客户可以直接从 P2P 网络中得到加密的打包内容，利用从服务器端授权发放的解密密钥解密打包内容，存入私有数据库中，即可得到原始的数字内容。

(2)水印请求下载

当客户从 P2P 网络中获得不带有数字许可证的数字内容，无法解密打包内容，这时可以读取数字内容的水印 ID 并请求提供给可信中心服务器，服务器经过对数字内容的质量检测，并权衡客户请求的内容质量，给出完整的符合客户请求的数字内容打包内容，客户于是可以通过付费获得授权许可得到原始数字内容。

(3)指纹请求下载

如果在水印请求下载中读取水印失败，则可通过读取数字指纹并发送请求到网络中获得标识信息，如果成功，则发送收到的 ID 至可信中心服务器获得经过质量检测的数字内容，通过认证授权即可获得数字内容。

3 结论

通过理论分析并结合相关实验验证，可以看出，该体系在用户行为监视、数据传输、服务器和用户终端载入、内容搜索和下载、安全可靠性、可扩展性等各方面性能都达到了较高标准，而且各种性能达到了协调，平均性能极佳。既克服了传统 C/S 模式下的服务器瓶颈，又实现了数字内容在 P2P 网络环境下的安全、快速、可信传输，是一种系统可行的 P2P 网络信息安全解决方案。

参考文献

1 Routsellis-Theotokis S, Spinellis D. A Survey of Peer-to-Peer Content Distribution Technologies[J]. ACM Computing Surveys, 2004, 36(4): 335-371.

2 Ku W, Chi Chihung. Survey on the Technological Aspects of Digital Rights Management[C]//Proc. of the 7th International Conference on Information Security, Palo Alto, CA, USA. 2004-09-27: 391-403.

3 Gu Guofei, Li Shipeng, Zhang Shiyong. PLI: A New Framework to Protect Digital Content for P2P Networks[C]//Proc. of Applied Cryptography and Network Security, Heidelberg. 2003: 206-216.

4 Iwata T, Abe' Kiyoshi T, Sunaga U H. A DRM System Suitable for P2P Content Delivery and the Study on Its Implementation[C]//Proc. of the 9th Asia-Pacific Conference on Communications. 2003-09-21: 806-811.

(上接第 118 页)

联网研发合作组织 CANARIE 和 CISCO 合作，提出并实现了 UCLP(User Controlled LightPath)。该项目使用 Web Service 和 Grid 技术，依靠软件的配置管理在互联网上构建了虚拟的面向联接的光纤网络，并且用户一定程度上可以选择信息穿越网络的路径，有一定的路由源端控制能力。UCLP 不是为源路由设计，但由于用户拥有一定的组网能力从而也同时拥有了路由控制能力。除此之外，Ad Hoc 领域较多的提到源路由概念，不过和互联网上要解决的问题相距较远。

源路由应用方面，也有为数不多的研究。多集中在网络管理和监控测量方面[6,7]，比如利用源路由得到网络拓扑、辅助网络诊断、排除网络故障等。

5 结论与展望

随着网络从技术转变为常识、网络环境的复杂化和用户需求的提升，人们对网络功能的期望也越来越高。用户深入参与到网络中，将是一个方展方向。源路由控制是用户参与网络的一种形式，而且已经有实际需求，源路由控制会逐渐引起研究者的重视。

致谢 在此，向为本文研究、开发和成果整理提供建议和帮助的同事，尤其是葛敬国博士、杨宏伟、王慧莉和徐浩表示由衷感谢。

参考文献

1 Postel J. Internet Protocol[Z]. USC/Information Sciences Institute. 1981.

2 Deering S, Hinden R. Internet Protocol, Version 6 Specification[S]. RFC2460, 1998.

3 Postel J. Transmission Control Protocol[S]. RFC 793, 1981.

4 Postel J. User Datagram Protocol[S]. RFC 768, 1980.

5 Estrin D, Li T. Source Demand Routing: Packet Format and Forwarding Specification[S]. RFC1940, 1996.

6 Brownlee N, Mills C. Traffic Flow Measurement: Architecture[S]. RFC2063, 1997.

7 The Cooperative Association for Internet Data Analysis[Z]. 2006-02-10. http://www.caida.org.