P2P 기반 디지털 권한 관리 시스템 설계

김윤형° 김태형
한양대학교 컴퓨터 공학과
{yunhyung°, tkim}@cse.hanyang.ac.kr

Designing a P2P-based Digital Rights Management System

Yun-Hyung Kim° Tae-Hyung Kim
Dept. of Computer Science & Engineering, Hanyang University

요 약

P2P 네트워크의 발달과 DRM 기술의 발전에 힘입어 지적 재산권 소유자와 P2P 네트워크 사용자들에게 있어 P2P를 기반으로 하는 DRM에 대한 발전이 크게 대두되고 있다. 본 논문에서는 pure P2P를 기반으로 하는 DRM 시스템의 설계에 대해 제안한다. 이를 위해 기존에 제안되었던 P2P를 기반으로 하는 DRM 시스템과 라이센스 관리 기법들에 대해서도 아울러 설명함으로써, P2P를 기반으로 하는 DRM 시스템 모델과 효율적인 라이센스 관리 기법을 제시한다.

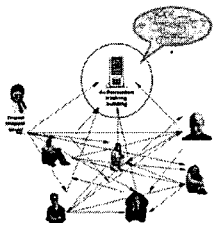
1. 서 론

전세계 사람들의 인터넷 사용에 힘입어 peer-to-peer network(이하 P2P 네트워크)의 사용이 증가하게 되었다. P2P 네트워크를 이용하는 사용자들은 인터넷을 통하여 원하는 contents(이하 컨텐츠)를 다운로드 하거나 자신이 공유하고자 하는 컨텐츠를 업로드 함으로써 원하는 컨텐츠를 빠른 시간 안에 얻을 수 있게 되었다. 그러나, P2P 네트워크를 이용함으로써 컨텐츠를 발행한 지적 재산권 소유자는 자신의 컨텐츠의 무분별한 배포에 있어서 익명성을 가진 P2P 네트워크의 특성으로 인해 해결점을 찾을 수 없는 상황 또한 발생하게 되었다. 지적 재산권 소유자의 이러한 문제점을 해결하기 위해 등장한 것이 DRM(Digital Rights Management)이라는 개념이다. DRM이란 컨텐츠에 DRM 속성을 집어넣어 해당 컨텐츠에 대한 라이센스가 있어야만 원하는 컨텐츠를 보거나, 듣거나 할 수 있는 권한을 주어지게 하는 것이다. DRM을 도입한다면 컨텐츠의 무분별한 배포를 막을 수 있어 지적 재산권 소유자에게는 이로울 수 있으나, 기존의 P2P 네트워크 사용자들에게는 컨텐츠의 공유 및 배포에 있어 걸림돌이 될 수도 있을 것이다. P2P 네트워크의 인터넷을 이용한 유연성과 주고 받는 컨텐츠에 대하여 누구에게 주고 받는지 모르는 익명성, 컨텐츠의 복제를 위해 소비되는 미디어(CD,DVD)등이 필요 없는 비용 절감 등의 특징은 지적 재산권 소유자가 자신의 컨텐츠를 배포하는 데 있어서도 필수 불가결한 요소이다. 그래서 우리는 이처럼 양 극단의 특징을 가진 P2P 네트워크와 DRM의 특징을 통합하여 P2P 네트워크 사용자와 지적 재산권 소유자에게도 장점이 될 수 있는 P2P 네트워크 기반 DRM 시스템을 설계하고자 한다.

2. 관련연구

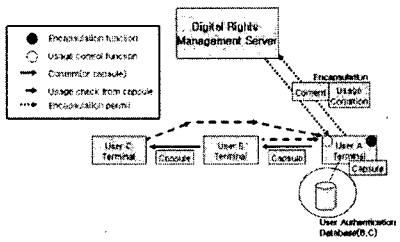
2.1 P2P 기반의 DRM 시스템

본 절에서는 P2P를 기반으로 하는 DRM 시스템에 대해 제안하고 있는 몇 몇 연구들을 살펴본다. Digital Containers[1]에서 제안하고 있는 시스템은 그림 1과 같다. 이 시스템은 사용자끼리 P2P 네트워크를 구성하고 각 네트워크마다 Digital Container라고 부르는 특별한 노드를 두어 그 노드에서 권한 및 인증을 처리하는 시스템으로 Hybrid 타입의 P2P 네트워크이다.



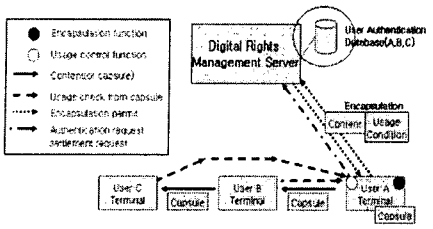
[그림 1. Digital Containers]

이 시스템의 경우에는 각 네트워크에서 특별한 노드라고 하는 Digital Container의 역할이 서버-클라이언트 구조에서의 서버의 역할과 동등한 역할을 수행하고 있어 Digital Container의 작동 중지나 문제점 발생의 경우 다른 사용자들도 권한 및 인증을 수행할 수 없는 문제점이 발생할 수 있다. 다음으로 이러한 문제점을 해결하기 위해 제안된 모델[2]을 살펴보자.



[그림 2.Distributed P2P-based DRM]

그림 2의 모델은 컨텐츠를 소유한 사용자에게 사용자 정보를 관리하는 방법을 제안한 모델이다. 그러나 사용자 권한 인증 작업을 수행하거나 데이터베이스를 관리하는 것은 보안에 관련된 사항이고 데이터베이스를 관리하는 사용자의 부주의로 인해 다른 사용자들에게 피해가 갈 우려가 있으므로 사용자 권한 인증과 같은 보안에 관련되고 주의 깊은 관리가 필요한 사항의 경우에는 권한 인증, 데이터베이스를 관리하는 서버가 불가피하다는 것을 수용하여 그림 3과 같은 모델로 수정하였다.



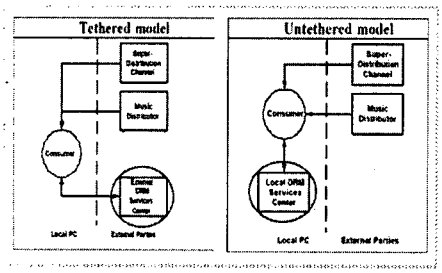
[그림 3. Semi-Distributed P2P-based DRM]

그림 3의 경우 Digital Rights Management Server를 두어 사용자 인증 데이터베이스를 관리하는 모델을 제안하고 있다. 결국, 특별한 노드가 서버의 역할을 담당하였던 모델에서 사용자 인증 데이터베이스만을 관리하는 믿을 만한 노드로 서버의 역할을 감소 시키는 결과를 만들었다.

2.2 라이센스 관리

본 절에서는 라이센스를 관리하기 위해 제안된 모델에 대해 살펴 보고자 한다.

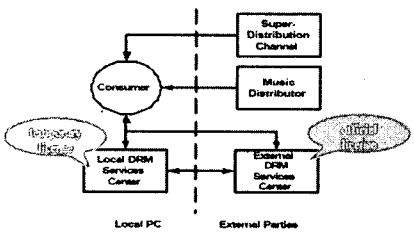
2.2.1 상용화 DRM 시스템에서의 모델[3]



[그림 4. Tethered and Untethered model]

그림 4의 왼쪽의 경우 라이센스 관리를 외부에 존재하는 External DRM Service Center에서 수행하는 모델이고 오른쪽의 경우 Local PC 상에서 라이센스를 관리하는 모델이다. Tethered Model의 경우에는 안정적인 권한 인증 및 권한 인증 데이터 베이스 관리를 수행할 수 있는 장점을 가진 반면에 중앙 서버에 크게 의존하는 서버-클라이언트 방식의 모델이고 오프라인의 경우에는 DRM 서비스를 제공 받을 수 없는 단점을 가지며, Untethered model의 경우에는 서버에 크게 의존하지 않고 권한 인증을 수행할 수 있고 오프라인의 경우에도 DRM 서비스를 제공받을 수 있는 장점이 있는 반면에, Local PC상에서 권한 인증 관리를 해야 하기 때문에 보안에 관계되거나 관리하는 데 있어 어려움이 있는 모델이다.

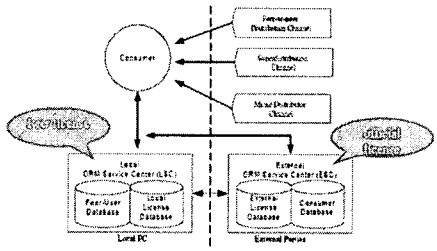
2.2.2 Enhanced license management model[3]



[그림5. Overview of the enhanced DRM model]

이 모델은 앞에서 제안하였던 두 모델의 장점을 통합하고 단점을 보완 하였다. 온라인일 경우에는 External DRM service center를 이용하여 DRM 서비스를 제공받고 오프라인일 경우에는 Local DRM service center를 이용하여 DRM 서비스를 제공받을 수 있는 모델이다. External DRM service center에서 지불 및 권한 인증을 거친 후에 충전 가능한 토큰 또는 쿠폰(그림에서의 temporary license)을 발급 받아 Local DRM service center에서 DRM 서비스를 제공받는 모델이다. 그러므로, 오프라인 상에서도 External DRM service center를 통하지 않고도 DRM 서비스를 제공 받을 수 있다.

2.2.3 The P2P enabled license management model[4]



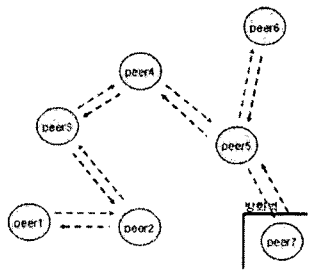
[그림6.The P2P enabled license management model]

그림 6의 모델은 Enhanced license management model을 기반으로 하면서 Local DRM Service Center가 관리하던 temporary license 대신에 peer license를 정의하여 임대 및 재배포의 용도에 따라 각각 peer-rental license,peer-redistribution license로 구분해 기존 모델을 개선하였다.

3. 제안하는 P2P 기반 DRM 모델

지금까지 P2P 네트워크를 기반으로 한 DRM에 대한 연구들을 보면 Hybrid타입의 P2P 기반 DRM이었다. 본 논문에서 우리는 Gnutella[5], Jxta[6]와 같은 pure P2P 네트워크를 기반으로 하는 DRM 모델을 제시하여 모든 피어가 동등한 입장에서 컨텐츠를 공유/교환할 수 있는 시스템을 제안하고자 한다.

3.1 Overview



[그림 7] P2P 네트워크 구성

[그림 8] peer의 구성

본 논문에서 제안하는 시스템 모델은 Gnutella[5]나 Jxta[6]와 같은 pure P2P 네트워크를 그림 7과 같이 구성하고 각 peer들마다 그림 8과 같은 라이센스를 캐쉬하는 LC(License Cache)와 라이센스를 해독, 생성 및 관리하는 MPEG REL SDK를 가진다.

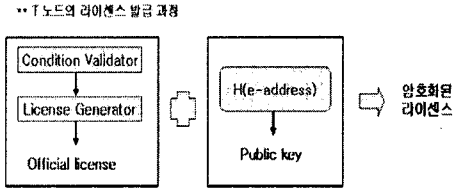
3.2 License

우리 시스템 모델에서는 2개의 라이센스를 정의하고 있다. 첫째는, 플레이어가 DRM 속성이 추가된 컨텐츠를 재생 하려고 하는 경우에 필요한 official license이고, 다른 하나는 지적 재산권 소유자에게 컨텐츠 사용에 대한 대금을 지불했을 경우에 받는 credential(Identity license)이다. official license는 MPEG-21[7] 표준에 따라 XrML 기반의 MPEG REL[8]로 작성된 라이센스를 정의할 것이고, credential은 지불한 컨텐츠에 대한

content ID, email-address, 지불한 대금에 맞는 권한(예를 들면, 읽기, 보기, 재배포), condition(예를 들면, 만료기간) 등으로 구성된다.

3.3 라이센스 획득 과정

본 논문에서 제안한 시스템 모델을 이용한 간단한 시나리오를 통해 라이센스 획득 과정을 살펴보자. 우리는 저작권자에게 라이센스 대금을 지불하는 지불 시스템은 고려하지 않으며, 플레이어는 DRM 속성을 가진 컨텐츠일 경우에 라이센스를 요청하는 시스템을 내장하고 있고, 컨텐츠의 다운로드는 인터넷이 연결되었을 경우에는 조건 없이 가능하며, 사용자는 자신의 개인키(private key)를 알고 있다는 가정을 두고 있다. 라이센스 대금 지불을 통해 credential을 획득한 P2P 네트워크를 구성하는 노드 중의 하나인 Consumer A는 자신의 플레이어로 컨텐츠를 재생하기 위해 official license를 획득하고자 한다. Consumer A는 자신이 원하는 라이센스를 찾기 위해 다른 이웃 노드들에게 질의 요청 메시지를 보낸다. 질의 요청 메시지는 content ID를 키 값으로 한다. 원하는 타겟 노드 T를 발견한 Consumer A 노드는 라이센스를 다운로드 받기를 원한다. 이 때, 타겟 노드 T는 ConsumerA에게 credential을 요청하고 ConsumerA 노드는 credential을 전송하고 credential을 받은 타겟 노드 T는 그림 9와 같이 credential에 명시되어 있는 권한에 맞는 라이센스를 생성, email-address에 Hash 함수를 적용시켜 public key 생성, 라이센스와 public key를 조합하여 암호화된 라이센스 생성하고 Consumer A에게 라이센스를 전송한다. Consumer A는 자신의 개인키를 이용하여 암호화된 라이센스를 복호화하고 원하는 라이센스를 획득한다.



[그림 9 T 노드의 라이센스 발급과정]

3.4 Jxta 기반 DRM Solution

P2P 네트워크를 기반으로 하는 DRM 모델에 대해 설명하였다. 우리가 제안한 모델을 실제 P2P 시스템에 적용하여 P2P 기반의 DRM Solution을 제안하고자 한다. 여기서 우리는 여러 가지 P2P 프로그램 중에 Jxta를 사용하여 제안하고자 한다. Jxta를 선택한 이유는 다음과 같다. Jxta는 메시지 전송에 있어서 XML 포맷을 사용하고 있다. 우리가 다루는 official license도 XrML(eXtensible right Markup Language)을 기반으로 하고 있어 메시지 전송 및 라이센스 관리 까지도 결국 XML 포맷 하나만으로 가능하고, Jxta에서 제공하는 Advertisement(광고)는 각 피어들이 자신이 소유한 자원에 대한 메타 데이터를 만들어 자신이 속한 네트워크 그룹에 광고함으로써 서로 자원을 공유/교환하는 것을 수월하게 해준다. 또한, Jxta를 구성하는 여러 프로토콜들과 서비스들이 메시지 전송 및 컨텐츠 검색, 다운로드 등을 용이하게 수행할 수 있도록 만들어져 있고, 각 피어 그룹마다 컨텐츠를 공유/교환하는 시스템인 cms(Content Manager Service)를 두어 컨텐츠의 효과적인 관리를 수행하고 있어 Jxta를 선택하였다.

3.4.1 Jxta의 cms(Content Manager Service)

Jxta는 각 피어그룹 마다 cms system을 이용하여 컨텐츠의 공유/교환 등과 같은 컨텐츠의 효율적인 관리를 수행하고 있다. 각 피어는 자신이 소유하고 있는 컨텐츠에 대해 컨텐츠의 메타 데이터를 content advertisement로 만들어 자신이 속한 피어 그룹에 광고를 한다. 컨텐츠를 찾기 원하는 피어는 content ID를 통해서 content advertisement를 확인하고, 컨텐츠를 소유한 피어와 통신을 통해 원하는 컨텐츠를 얻는다. 물론, 자신의 피어 그룹이 아닌 원격 피어 그룹에 존재하는 컨텐츠를 검색할 수도 있다. 일단, 다른 피어 그룹에 컨텐츠가 있음을 알게 되면, 컨텐츠를 다운로드 하려는 피어는 컨텐츠를 가지고 있는 피어 그룹에 조인을 하여 해당 피어그룹에서 제공하고 있는 cms 시스템을 이용하여 원하는 컨텐츠를 제공 받는다.

3.4.2 LMS(License Manager Service)

Jxta를 기반으로 하는 DRM solution에서는 cms와 유사한 방식으로 라이센스를 효율적으로 관리 해주는 LMS(License Manager Service)를 구축하여 기존의 Jxta 플랫폼에 새로운 서비스를 추가한다. cms와 lms가 서로 연관성을 가지는 것은 content ID를 키 값으로 하는 데 있다. cms와 마찬가지로 lms 또한 각 피어가 가지고 있는 라이센스의 메타 데이터를 이용하여 만든 license advertisement를 공유하고 있으며, 질의 요청을 위해 content ID를 키 값으로 하고 있다. 결국, content ID 하나를 가지고 원하는 컨텐츠와 라이센스를 동시에 제공 받을 수 있는 시스템이 된다. 컨텐츠와 라이센스를 제공받기 원하는 사용자는 content ID를 키 값으로 질의 요청 메시지를 보내고, 원하는 컨텐츠와 라이센스를 소유하고 있는 피어 그룹을 검색한다. 사용자는 피어 그룹에 조인을 하고, 원하는 컨텐츠를 다운로드 받거나, 라이센스 획득 과정(3.2절)을 거쳐 원하는 라이센스를 발급 받는다. 결국, Jxta의 각 피어 그룹들은 cms를 통한 컨텐츠의 효율적인 관리 뿐만 아니라 lms을 통한 라이센스의 효율적인 관리를 수행할 수 있게 된다.

4. 결론

본 논문에서는 P2P 네트워크를 기반으로 하는 디지털 권한 관리 시스템의 설계에 대해 제안하였다. pure P2P 네트워크를 구성하여 모든 노드들이 동등한 입장에서 역할을 수행하고 권한 인증을 수행하는 서버가 존재하지 않으며, 권한 인증 데이터베이스를 유지할 필요도 없으며, 온라인 혹은 오프라인에 상관없이 DRM 서비스를 제공 받을 수 있으며, MPEG REL을 이용한 라이센스 생성 및 관리로 MPEG-21 표준을 따르고 있다. 그리고, 신원 기반 암호화 기법을 이용한 라이센스 암호화를 통해 공인 인증 센터 없이도 보안 및 안정성에 있어서도 믿을 만한 시스템을 제안 하였다. 또한, 기존의 P2P 플랫폼인 Jxta를 이용한 solution을 설계함으로써 기존의 P2P 플랫폼과의 적합성 또한 보여주고 있다. 향후 Jxta와 연동한 Jxta 기반의 DRM 시스템을 구현할 예정이다. 현재는 MPEG REL에서 제안하고 있는 라이센스의 생성 및 관리에 대해 구체적인 연구 중이다.

5. 참고문헌

[1] Digital Containers
http://www.digitalcontainers.com/index.htm
[2] Iwata, T, Abe, T, Ueda, K, Sunaga, H; A DRM system suitable for P2P content delivery and the study on its implementation; APCC Sept 2003. Volume 2, 21-24
[3] Sai Ho Kwok, Digital rights management for the online music business, ACM SIGecom Exchanges, Volume 3 Issue 3 June 2002
[4] Kwok and S. M. Lui, S. H. (2001) A License Management Model to Support B2C and C2C Music Sharing. In Proceedings International WWW
Conference(10), Hong-Kong.
[5] Gnutella http://www.gnutella.com/
[6] Jxta http://www.jxta.org/
[7] MPEG-21
http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35366&ICS1=35
[8] MPEG REL
http://www.contentguard.com/MPEGREL_home.asp