콘텐츠 보호를 위한 DRM이 적용된 P2P 모델

성 재 연[†] · 정 연 정[††] · 윤 기 송[†††]

요 약

P2P(Peer to Peer)는 오늘날 가장 주목 받는 파일 공유 시스템으로 현재 네트워크 트래픽의 50% 가량을 점유하고 있을 정도로 많은 콘텐츠의 유통경로가 되고 있다. 이처럼 P2P는 가장 큰 콘텐츠 유통 경로로 활용되기도 하지만 콘텐츠의 가장 큰 불법 유통 경로로 활용되기도 하며 최근에 들어 음악산업뿐만 아니라 영상산업 전반으로 불법 유통을 야기시키고 있으나 현재 이를 방지하면서 P2P의 장점을 최대한 살릴 수 있는 DRM(Digital Right Management)이 적용된 P2P모델이 제시되지 못하고 있다.

이에 본 논문에서는 기존 DRM기능들을 변형하여 기존에 P2P모델에 적합한 형태로 적용함으로써 기존의 P2P 모델구조를 변형시키지 않고 P2P의 높은 확장성(Scalability)과 분산 처리 성능을 지원할 수 있는 콘텐츠 보호를 위한 DRM이 적용된 P2P 모델을 제안한다.

키워드 : 콘텐츠, 저작권 보호, DRM, P2P, FastTrack, 라이센스

DRM Enabled P2P Model for Contents Protection

JaeYoun Sung[†] · Yeonjeong Jeong[††] · Kisong Yoon[†††]

ABSTRACT

P2P(Peer To Peer) system, a most attractive file sharing system, is the largest channel of contents distribution and it takes 50% of network traffic. But P2P systems are infamous for used to illegal contents distribution channel not only in music industry, but also in movie industry. But, DRM(Digital Right Management) enabled P2P models are not suggested until now that interrupting illegal contents distribution and keeping advantage of P2P. So in this paper, we suggest a DRM enabled P2P model that can support distributed processing ability and high scalability with no modification in exist P2P model or architecture.

Key Words : Content, Digital Rights Management, DRM, Peer To Peer, p2p, License

1. 서 론

P2P는 오늘날 가장 주목 받고 파일 공유 시스템으로 사용자의 기호에 적합하여 빠른 발전이 이루어 지고 있으며, Napster[1]를 시작으로 Gnutella[2], KaZaA[3]와 같은 많은 P2P 시스템들이 개발되어 사용되고 있다. P2P는 FastTrack[4]과 같은 프로토콜을 이용한 높은 분산처리 능력을 기반으로 빠른 파일 전송을 제공하며, P2P 구조가 가지는 높은 확장성(Scalability)때문에 안정된 파일 공유능력을 제공한다.

P2P는 콘텐츠 자체를 직관적으로 검색하므로 콘텐츠를 얻기 위해 특정 콘텐츠 포탈사이트를 미리 검색할 필요가 없으므로 사용자 측면에서 사용이 용이하고 공유된 콘텐츠는 네트워크상의 사용자에 의해 능동적이고 빠르게 확산되므로 콘텐츠 유통채널로써 강점을 지닌다. 실제로 현재 네트워크 트래픽의 50% 가량을 P2P가 점유하고 있을 정도로 많은 콘텐츠의 유통경로가 되고 있다.

그러나, P2P는 위에 명시된 바와 같은 풍부한 장점에도 불구하고 현재 콘텐츠의 가장 큰 불법 유통 경로로 이용되어, 최근 들어 음악 콘텐츠에서 기승을 부리던 불법유통 문제가 영상 콘텐츠 전반으로 확산되면서 그 피해 규모가 더욱 커지고 있다. 이에 따라 각국에서 P2P상의 불법 콘텐츠 공유를 금지하는 법률안이 잇따라 세워지고 있어 P2P자체의 존폐위기에 직면해 있기도 하다.

이를 극복하기 위해 P2P에 DRM 기술을 접목하여 불법적인 콘텐츠 유통을 막을수 있으면서도 확장성이나 분산처리능력(Distributed Processing)과같은 P2P 특유의 장점을 유지할 수 있는 방안이 필요하다.

현재 콘텐츠에 대한 보호 방안으로서 크게 DRM(Digital Rights Management)과 워터마크(Watermark)를 이용하는 방안이 제시되고 있다. DRM의 경우 일반적으로 서버- 클라이언트 구조를 기반으로 해서 연구가 이루어 지고 있는 상

† 정 회 원 : 과학기술연합대학원대학교
†† 준 회 원 : 한국전자통신연구원 선임연구원
††† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2005년 11월 14일, 심사완료 : 2006년 6월 14일

태이며[5~7] 아직까지는 P2P 구조에 적합한 방안이 제시되지 못하고 있다. 이에 본 논문에서는 콘텐츠 보호를 위해 서버-클라이언트 구조가 아닌 P2P 구조에서 콘텐츠 패키징, 콘텐츠 배포, 라이센스 발급 등의 DRM 기능이 가능한 DRM이 적용된 P2P 모델을 제안한다.

본 논문에서는 먼저 DRM과 P2P간의 융합이 시도된 기존의 연구내용을 크게 3가지로 나누어 살펴보고 장점과 한계를 알아본 뒤, P2P 상에서 콘텐츠 보호를 지원하기 위해 DRM이 적용된 P2P 모델을 제안한다. 제안하는 모델은 기존의 P2P가 가지는 FastTrack과 같은 프로토콜을 통한 높은 분산처리 능력과 P2P 구조가 가지는 높은 확장성능을 저하 시키지 않으면서 콘텐츠 보호를 위한 라이센스 발급 가능하다.

2. 관련 연구

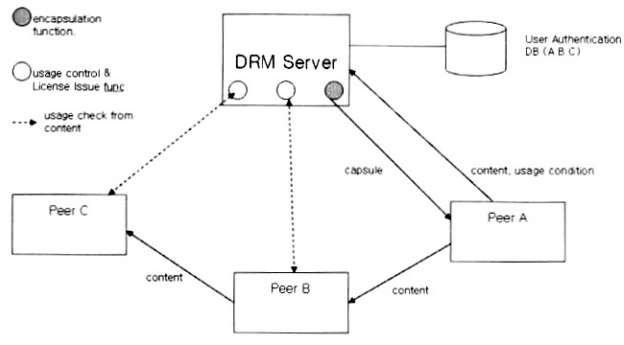
본 장에서는기존에 연구된 DRM이 적용된 P2P 모델들을 3가지 유형으로 나눠서 설명한뒤 각 모델에 대한 장, 단점을 비교하여 문제점을 알아본뒤 새로이 제안하는 P2P 환경에서 콘텐츠 보호를 위한 DRM이 적용된 P2P 모델의 필요성과 장점을 설명한다.

기존에 연구된 사례는 크게 3가지 형태로 나눌 수 있는데[5], 첫째로 DRM 기능을 수행하기 위해서는 기존의 서버-클라이언트 구조의 DRM 시스템을 그대로 이용하고, 단지 콘텐츠의 전달 채널로만 P2P 시스템을 이용하는 기존의 서버-클라이언트 기반 모델(Existing Server-Client based Model)이 있고, 둘째로 대부분의 DRM 기능은 Peer 노드에서 수행되지만 고정적인 DRM 서버를 두고 있는 분산 P2P 모델(Distributed P2P Model)이 있으며, 셋째로 분산 P2P 모델과 유사한 구조를 가지지만 사용자인증 기능을 Peer 노드가 아닌 DRM 서버에서 수행하도록 한 반 분산 P2P 모델(Semi-distributed P2P Model)이 있다.

2.1 기존의 서버 클라이언트 기반 모델 (Existing Server-Client based Model)

이 모델은 기존의 DRM 시스템을 그대로 이용하고, 콘텐츠를 배포하기 위한 채널로써 기존의 P2P 시스템을 이용하는 모델이다. DRM과 관련된 모든 기능들은 DRM 서버와 DRM 클라이언트에서 수행된다. DRM 서버는 콘텐츠를 안전한 형태로 배포할 수 있도록 패키징하여 보호된 콘텐츠(Protected-content)를 생성하고, 배포된 보호된 콘텐츠에 대한 사용을 통제할 수 있도록 사용권한을 가지는 라이센스를 Peer 노드로 발급한다. Peer 노드내의 DRM 클라이언트는 DRM 서버로부터 발급받은 라이센스에 접근하여 허가된 사용권한 범위 내에서 콘텐츠를 이용할 수 있도록 한다. 이때, P2P 시스템은 DRM 서버가 생성한 보호된 콘텐츠가 Peer 노드로 전달되는 과정에서 보호된 콘텐츠의 전달 채널로서 사용되게 된다.

이 모델은 DRM 시스템과 P2P 시스템이 별개의 시스템



(그림 1) 서버 클라이언트 기반 모델

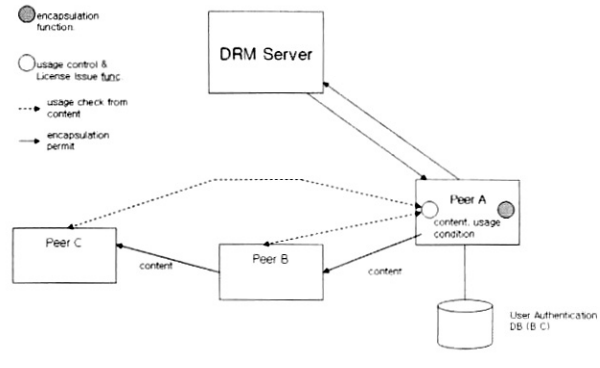
으로서 존재하는 형태이며 DRM 시스템을 P2P 시스템에 알맞도록 최적화하여 적용한 것이 아니며 두 시스템간에 유기적인 결합 관계가 존재하지 않으므로 P2P가 가지는 분산처리나 확장성과 같은 장점을 라이센스 발행 능력면에 있어서는 전혀 이용하지 못하기 때문에 P2P 네트워크에 새로운 Peer 노드가 추가되어 네트워크가 확장할 때 마다 DRM 서버의 부하는 점점 커지게 된다. 그래서 DRM 서버시설의 추가 증강없이는 성능이 저하될 수 있으며 콘텐츠 자체의 공유 외에는 P2P 모델의 이점을 전혀 이용하지 못한다.

또한 P2P 측면에서는 DRM 기능이 P2P 내에서 지원되지 않아 P2P 자체적으로 파일에 대한 통제나 보호를 지원할 수 없다.

2.2 분산 P2P 모델(Distributed P2P Model)

(그림 2)의 분산 P2P 모델은 Peer 노드에 사용자 인증과 사용권한 제어를 위한 DRM 클라이언트 모듈과 콘텐츠 패키징과 라이센스 발급을 위한 DRM 서버 모듈이 존재하고, 라이센스 자체는 Peer 노드에서 발행되지만 Peer 노드와는 별개의 DRM 서버가 존재하여 모든 Peer 노드에서의 라이센스 발급을 제어한다.

원본 콘텐츠를 가진 Peer 노드는 이를 패키징하여 보호된 콘텐츠로 만들고 P2P의 파일 공유기능을 통해 배포한다. 배포된 보호된 콘텐츠에 대한 라이센스 발급은 이를 패키징한 Peer 노드에서 수행하는데, 패키징한 Peer 노드에서 다른 Peer 노드로 라이센스를 발급하기 위해서는 DRM 서버에 콘텐츠에 대한 라이센스 발급 허가를 받은 후 라이센스를



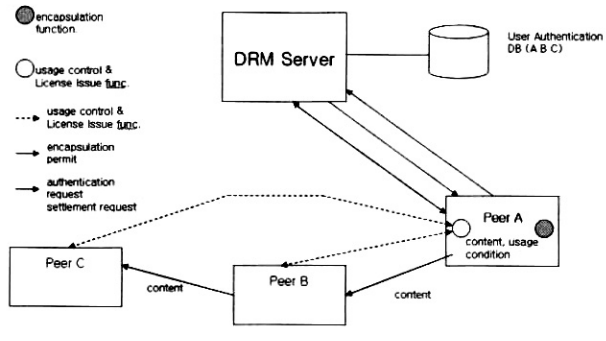
(그림 2) 분산 P2P 모델

만들어 다른 Peer 노드에게 전달한다.

이 방식의 경우 콘텐츠 발급은 여러 Peer 노드에서 분산처리가 제공되지만, 여전히 DRM 서버가 존재하여 모든 라이센스 발급에 관여하게 되므로 확장성이 제공되지 않으며 유지비용이 발생하게 될 가능성이 존재한다. 또한 구조의 한계상 콘텐츠를 패키징한 Peer 노드에서만 라이센스 발급이 가능하기 때문에 안정적인 라이센스 발급을 보장할 수 없을 뿐만 아니라 라이센스 발급을 위한 분산처리에도 한계를 가진다.

2.3 반 분산 P2P 모델(Semi-distributed P2P Model)

(그림 3)의 반 분산 P2P 모델은 기본적으로 분산 P2P 모델과 동일하지만 라이센스를 발급하는 Peer 노드에서 사용자 인증이 수행되지 않고 DRM 서버에서 수행된다. 그로 인해 보안성은 높일 수 있지만, 기본적으로 분산 P2P 모델과 같은 문제점을 가지고 있다.



(그림 3) 반 분산 P2P 모델

2.4 결 론

위에서 살펴본 바와 같이 기존의 연구에서는 모두 P2P 구조와는 별개의 DRM 서버를 유지하고 있으며 이 서버는 라이센스 발행 능력면에서 확장성과 분산처리능력 같은 P2P 본연의 장점을 살릴 수 없으며 유지 비용을 발생시키게 된다. 그러므로 서비스해야 할 Peer 노드 수가 증가할수록 라이센스 발급 Peer 노드의 부하는 커지게 되고, 특정 보호된 콘텐츠에 대한 라이센스 발급은 이를 패키징한 하나의 Peer 노드에서만 가능함으로 안정적인 서비스를 제공할 수 없다. 따라서, 콘텐츠 보호를 위해 DRM 기능을 지원하면서 P2P가 가지는 높은 분산처리와 확장용이성을 이용할 수 있는 방안이 필요하다.

이에 본 논문에서는 P2P 구조 상에서 DRM 기능이 지원되면서도 기존의 P2P 구조를 전혀 바꾸지 않고 P2P 시스템의 높은 확장성과 분산 처리 성능을 지원할 수 있는 방안을 제안한다. 제안된 시스템은 고정적인 DRM서버가 존재하지 않아 추가적인 시설의 증강없이 높은 확장성를 제공할 수 있고, 하나의 보호된 콘텐츠에 대해 여러 Peer 노드들이 라이센스 발급 서버의 역할을 수행할 수 있도록 하여 P2P의 높은 분산 처리 성능과 안정적인 DRM 서비스를 지원할 수 있다.

3. 제안하는 DRM이 적용된 P2P 모델

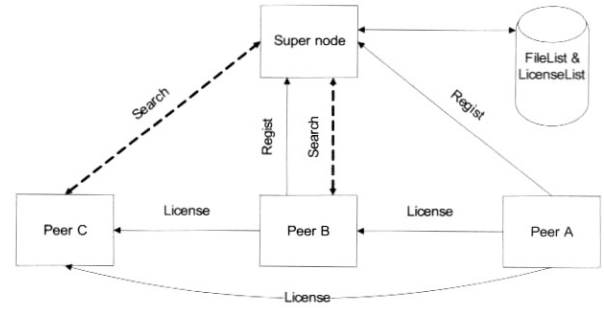
본 장에서는 별개의 DRM 서버가 존재하지 않고 각 Peer 노드에서 모든 DRM 기능을 수행할 수 있는 콘텐츠 보호를 위한 DRM이 적용된 P2P 모델을 제안한다.

제안하는 모델은 Super 노드가 각 Peer 노드들의 발행가능 한 라이센스 리스트를 유지하여 라이센스 검색과 발행이 가능하다. (그림 4)에서 볼 수 있듯이 라이센스 발급시에 Peer 노드는 기존의 콘텐츠 검색과 동일한 방법으로 라이센스를 검색하게 되고 Peer 노드는 검색결과 내에서 사용가능한 라이센스를 선택하여 다운로드 하게 된다. 제안하는 DRM이 적용된 P2P 모델은 콘텐츠 발급뿐 아니라 라이센스 발급 시에도 높은 분산처리 능력을 보여주게 된다.

(그림 4)는 제안하는 모델에서 라이센스를 검색하고 발급하는 모습을 보여준다.

모든 P2P상의 Peer 노드는 자신이 발급가능한 라이센스를 Super 노드에 등록(Regist)한다. 모든 P2P상의 Peer 노드는 콘텐츠를 검색하듯이 라이센스를 검색할수 있고 Super 노드는 자신의 라이센스 리스트에 있는 정보를 결과로 Peer 노드들에게 전달할수 있다. 검색 결과로 Peer 노드는 자신이 원하는 라이센스를 발행할수 있는 Peer 노드 군을 얻게 되어 선택하여 라이센스를 발급받을 수 있다.

제안하는 모델에서 가장 큰 역할을 하는 것은 라이센스 리스트 유지기능과 라이센스 검색질의에 대한 결과를 전달 기능을 가진 Super 노드이다. 이 Super 노드가 라이센스를 발행할수 있는 Peer 노드를 찾아주는 역할을 함으로써 DRM 서버를 유지하지 않고 DRM 기능을 P2P상에 유기적으로 결합시킬수 있다.



(그림 4) DRM이 적용된 P2P 모델

3.1 제안하는 DRM이 적용된 P2P모델의 구조

본 논문에서 제안하는 콘텐츠 보호를 위한 DRM이 적용된 P2P 모델의 구조는 (그림 5)와 같다. 기본 구조는 기존의 2세대의 P2P 구조를 그대로 따르고 있으며 다른 점은 각 Peer노드에서 DRM 기능을 수행하기 위한 DRM 수행모듈(DRM Agent)이 존재하며 Super 노드에서 라이센스 발급이 가능한 Peer노드에 대한 리스트를 유지한다는 것이다.

제안된 DRM이 적용된 P2P 모델의 Peer 노드는 기존의 P2P기능 모듈에 더불어 인증서와 DRM 수행모듈로 구성된

다. DRM수행모듈은 원본 콘텐츠를 콘텐츠 암호화 키(Content Encryption Key: CEK)로 암호화하고 콘텐츠 메타데이터 등과 함께 패키징하여 보호된 콘텐츠로 만드는 패키저와 CEK를 저장하는 안전한 데이터베이스(Secure DB), 그리고 라이센스를 발급하거나 라이센스에서 CEK를 추출하여 보호된 콘텐츠를 사용할 수 있게 하는 라이센스 핸들러(License Handler)로 구성된다.

Super 노드 역시 동일한 모듈로 구성되나 특정조건을 만족할 시에 P2P 모듈 내부의 Super 노드 기능이 활성화 되어 Super 노드로서의 기능도 수행하게 된다.

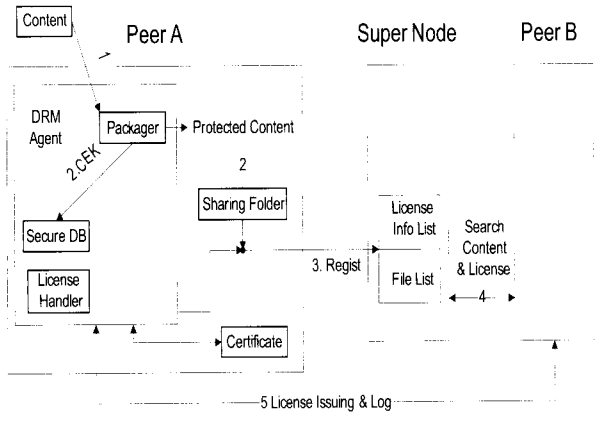
기존의 P2P에서는 Peer 노드가 P2P에 접속할시에 Super 노드로 자신의 공유파일 리스트를 전송한다. 이때 제안하는 모델에서는 파일리스트뿐만 아니라, 자신이 발행할 수 있는 라이센스에 대한 정보인 라이센스 발급 정보를 전송한다.

라이센스 발급 정보에는 Peer 노드에서 라이센스에 대한 검색이 용이하도록 해당 콘텐츠의 해시값과 Peer 노드가 발행할 수 있는 사용권한 정보가 포함된다.

기존의 FastTrack 프로토콜에서 DHT(Distributed Hash Table)를 사용하여 동일 콘텐츠를 검색하여 전송하는 것처럼, 이 콘텐츠의 해시값을 이용한 기능을 라이센스 발행에 적용하여 해당 콘텐츠에 대한 라이센스 발급이 가능한 Peer 노드를 검색하고 라이센스 획득이 가능하게 한다.

콘텐츠 발급과 동시에 라이센스가 발급되지 않아도 되므로 콘텐츠 획득과 라이센스의 획득은 동시에 수행될 필요가 없으며, 콘텐츠 제공 Peer 노드와 라이센스 발행 Peer 노드가 동일할 필요도 없어 높은 분산처리 능력과 안정된 파일 공유 능력을 가진다.

또한 Super 노드는 DRM 서버와 같이 기존의 P2P 모델에서 이질적인 존재가 아니라 본래 P2P 모델안에 존재하는 객체이며 이는 P2P 네트워크 상에 고정된 것이 아니라 동적으로 생성 소멸된다. DRM 서버는 DRM 기능을 대부분 수행하지만 본 논문에서의 Super 노드는 Peer 노드에서 요구하는 라이센스를 기존의 콘텐츠 검색과 같은 방법으로 검색하여 결과를 돌려주는 역할을 하며 Super 노드 자신에게 연결된 Peer 노드들의 라이센스 발급 정보 리스트를 유지하는 핵심적인 기능을 수행한다.



(그림 5) 제안하는 DRM 이 적용된 P2P 구조

3.2 서비스 시나리오

제안된 DRM이 적용된 P2P 모델에서 DRM 서비스는 (그림 5)에 표기된 번호와 같은 순서의 시나리오로 표현할 수 있다. (그림 5)의 1, 2번 과정에서 수행되는 패키징은 다른 Peer 노드에서 동일 콘텐츠를 배포할 시에 수행되지 않으며 보호된 콘텐츠는 공유 폴더에 저장된다.

① 콘텐츠 패키징

(그림 5)에 나타난 1번과 2번에 해당하는 과정으로써 Peer 노드에서 원본 콘텐츠를 패키징하여 그 결과물로 보호된 콘텐츠와 콘텐츠를 암호화 하는데 사용한 CEK가 생성된다. CEK는 Peer 노드에서 안전하게 안전한 데이터베이스(Secure DB)에 보존되며, 보호된 콘텐츠는 P2P 네트워크에 공유된다.

② 콘텐츠 등록

(그림 5)에서 3번의 과정으로써 Peer 노드에서 Super 노드로 파일리스트를 전송할 시에 파일리스트내에는 파일 이름과 파일에 대한 해시 값뿐만 아니라 그 Peer 노드에서 라이센스를 발행할 수 있는 파일에 대한 라이센스 발급 정보(발행가능 라이센스에 대한 정보)가 포함된다. 라이센스 발급 정보는 해당 콘텐츠의 해시 값과 사용 가능한 사용권한 정보를 포함한다.

③ 콘텐츠 검색 및 다운로드

(그림 5)에서 4번에 수행되는 과정으로써 콘텐츠 검색과 검색된 파일의 다운로드는 기존의 P2P 에서 사용되는 방식을 그대로 사용한다. Peer 노드는 Super 노드에서 원하는 콘텐츠를 검색하고 검색된 파일을 가지고 있는 Peer 노드들로부터 FastTrack과 같은 P2P 분산처리 프로토콜에 따라 다운로드 받는다.

④ 라이센스 발행 가능 Peer 노드 검색 및 라이센스 발급

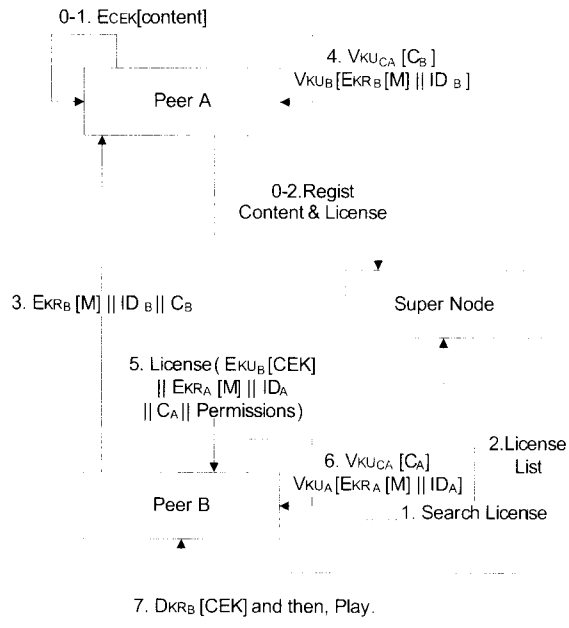
(그림 5)에서 4번과 5번에 해당하는 과정으로써 Peer 노드가 콘텐츠에 대한 라이센스를 발급받기 위해서는 라이센스 발급이 가능한 Peer 노드를 검색해야 하는데, 이를 위해 Super 노드는 자신의 파일 리스트 내에서 파일과 동일한 해시 값을 데이터로 가지는 라이센스 발급 정보를 검색하여 라이센스 발급 가능 Peer 노드를 알려준다. Peer 노드는 이들 노드 중 하나를 선택하여 라이센스 발급을 요청하게 되고, 라이센스 발급 가능 Peer 노드는 발급요청을 한 Peer 노드에 대한 인증 과정을 거친 후 라이센스를 발급한다.

⑤ 콘텐츠 사용

Peer 노드는 발급받은 라이센스에 명시된 사용권한 범위 내에서 보호된 콘텐츠를 사용 또는 재생할 수 있다

3.3 키 관리 방안

제안된 모델에서 콘텐츠를 대칭키로 암호화한 후 이 콘텐



(그림 6) 키 관리 방안

츠를 암호화하는데 사용된 대칭키(CEK: Content Encryption Key)를 Peer 노드간에 (그림 6)의 키 관리 방안을 이용하여 전송함으로써 안전하게 라이센스를 Peer 노드로 전송할 수 있다.

키 관리방안은 참고문헌 [9]의 표기법을 사용하여 표현하였다.

범례

CEK: Content Encryption Key (콘텐츠를 암호화 하는데 쓰이는 키)

V: Verify (검증)

E: Encryption (암호화)

D: Decryption (복호화)

C: Certificated (인증서)

KU: Public Key (공개키)

KR: Private Key (개인키)

M: Message (검증시 확인을위한 약속된 메시지)

ID: 아이디

Permissions: 콘텐츠에 접근할수 있는 권한을 라이센스내에 약속된 언어로 표현한 것

키 관리 방안은 패키징과 키 분배의 두 가지로 나누어 설명할 수 있으며, 패키징 과정은 원본 콘텐츠를 로컬에서 생성한 대칭키인 CEK(Content Encryption Key)로 암호화하여 보호된 콘텐츠를 생성한 후, 해당 콘텐츠에 대한 파일리스트와 라이센스 발급정보를 Super 노드에 등록하는 과정에서 수행되는 키 관리 방안이며 Step 0-1 과 Step 0-2로 패키징 과정을 표현하였다.

키 분배 과정은 인증된 Peer 노드에게 보호된 콘텐츠에 접근할 수 있도록 Peer 노드들 간에 상호 인증하는 과정과 라이센스를 통해 수신자의 공개키로 암호화된 CEK를 전달하는 과정에서 수행되는 키 관리 방안이며 Step 1에서 Step 7과 같다.

(그림 6)은 본 논문에서 제안된 모델에서 인증서와 공개키 기반 암복호화 알고리즘이 어떻게 쓰여지는지 보여주는 예이며 일반적인 형태의 구조이며 [8]의 키 관리 방안을 참고하였다. 보호된 콘텐츠 자체는 대칭키(Secret Key)로 암호화 되지만, 보호된 콘텐츠에 접근할수 있게 하는 CEK를 포함한 라이센스는 라이센스를 구매한 사용자의 공개키로 암호화되므로 사용자의 개인키(Private Key)를 이용해서만이 접근할 수 있다.

Step 0-1: (Peer A) E_{CEK}[content]

네트워크 상의 모든 Peer 노드는 CA로부터 인증서를 미리 발급받은 상태이다.

Peer A는 CEK를 생성하여 원본 콘텐츠를 AES (Advanced Encryption Standard)와 같은 대칭키 알고리즘으로 암호화한 후 보호된 콘텐츠를 생성한 후 공유폴더에 저장하고 CEK는 로컬의 Secure DB 영역에 저장한다.

Step 0-2: (Peer A → Super Node) Regist Content & License

기존의 P2P시스템에서는 Peer 노드가 Super 노드에 접속시 자신의 공유 콘텐츠 리스트만 전송하여 Super 노드에 등록하였지만, 제안하는 모델에서는 라이센스의 검색을 위한 라이센스 리스트도 Super 노드에서 유지되게 해야 하므로 Peer A는 Super 노드에 접속하거나 갱신이 필요할 때 자신의 콘텐츠 파일의 해시값과 함께 Peer A 자신이 발행 가능한 라이센스에 관한 메타정보나 결제정보, 권한정보 등을 Super 노드에 전송하여 등록한다.

Step 1: (Peer B → Super Node) Search License

이때 Peer B는 이미 P2P를 통하여 콘텐츠를 획득한 상태이다.

Peer B가 Super 노드를 통하여 특정 콘텐츠에 대한 라이센스를 검색한다. 이때 검색은 미리 다운로드 받은 콘텐츠의 해시값을 사용하여 동일 해시값을 가진 라이센스 발급정보를 검색함으로써 이루어진다.

Step 2: (Super Node → Peer B) License List

Super 노드는 Peer B에게 라이센스 검색질의에 대한 결과값인 라이센스 목록을 건네주고 Peer B는 이들중 Peer A를 선택한다.

Step 3: (Peer B → Peer A) EKR_B [M] || ID $_B$ || C_B

Peer B는 자신이 라이센스를 발급받을 권한이 있는 사용자임을 알리기위해 자신의 시스템환경에 대한 메타데이터를 담고 있는 M과같이 자신의 전자서명(EKR_B||ID_B)과 전자인증서를 함께 Peer A로 전송한다.

이때 M에는 Peer B에 대한 간단한 성능정보와 어떠한 사용권한을 지원하는지 여부가 DRM 수행모듈에서 작성되어 첨부된다. 전자서명은 자신의 비대칭키쌍 중에 개인키(Private key)를 사용하여 약속된 메시지등을 암호화한후 자신의 ID를 붙여서 만들어진다.

Step 4: (Peer A) VKU_{CA} [C_B], VKU_B [EKR_B [M] || ID_B]

Peer A는 Peer B의 인증서를 CA(Certificate Authority)의 비대칭키쌍중에 공개키(Public Key)를 이용하여 검증한 후 Peer B의 전자서명을 검증하여 확인한다.

검증과정은, 먼저 CA의 공개키로 Peer B의 인증서(Certificate)를 복호화 한다. 만일 CA가 발행한 인증서라면 Peer A는 Peer B의 인증서를 열어서 Peer B의 공개키에 접근할수 있게되고, 같이 전송된 Peer B의 개인키(Private Key)로 암호화된 메시지를 해독하여 검증하게 된다.

Step 5: (Peer A → Peer B) License (EKU_B [CEK] || EKR_A [M] || ID_A|| C_A || Permissions)

Peer A는 CEK를 Peer B의 공개키로 암호화하고 사용권한(Permission)을 설정한 후 권한 기술언어(REL: Rights Expression Language)로 라이센스를 생성하여 Peer B에게 자신의 전자서명과 인증서를 넣어서 라이센스를 발행하며 전자서명의 작성과정은 Step 3과 동일하다.

권한 기술언어는 주로 XML을 이용한 문서로 작성되며 각 사용권한은 문서내에 엘리먼트로 표현되며 실제 구현단계에서 비즈니스 모델에 따라 XrML[10] 이나 ODRL[11] 같은 상용 권한 기술언어를 사용 할 수도 있고 좀더 최적화되거나 간소한 형태의 전용 권한 기술언어를 작성하여 사용할 수도 있다.

사용권한에 대해서는 다음 3.4 단락에서 자세히 살펴본다. 이때 Peer B는 라이센스에 대해 적절한 지불을 마쳤다고 가정한다. 지불 방법은 비즈니스 모델에 따라 다양할수 있다.

Step 6: (Peer B) VKU_{CA} [C_A], VKU_A [EKR_A [M] || ID_A]

Peer B는 Peer A의 인증서를 CA의 공개키를 이용하여 검증한 후 Peer B의 전자서명을 검증하여 확인한다.

검증과정은 Step 4에서 설명한 바와 같다.

Step 7: (Peer B) DKR_B [CEK] and then, Play.

Peer B는 Step 4와 동일한 방법으로 검증과정을 거치고, 자신의 개인키(Private Key)를 이용하여 CEK와 사용권한(Permission)을 복호화한 후 Local DB에 저장한다. Peer A는 사용권한 범위 내에서 콘텐츠를 사용할 수 있으며 이 라이센스는 자신의 공개키로 암호화되어 로컬의 안전한 데이터베이스(Secure DB)에 저장되므로 권한이 없는 사용자는 접근할 수가 없다.

3.4 P2P 환경에서의 사용권한 정책

P2P상에는 다양한 시스템환경의 사용자가 존재하므로 인해 시스템환경에 따라 사용권한의 적용이 불가능하게 될 경우도 있다. 예를들어, 라이센스 내에 부여되는 콘텐츠에 대한 사용권한은 일반적으로 사용횟수(Count), 사용기한(Date), 사용시간(Interval)등과 라이센스를 다른 기기로 전송하기 위한 라이센스 전송(Export)등이 있는데 P2P상의 Peer 노드들의 상이한 시스템환경으로 인해 특정 Peer 노드에서 시스템환경내에 사용시간과 사용기한을 체크하는데 참조하는 신뢰할수 있는 시스템 시간이 존재하지 않는다거나 라이센스전송을 위한 USB나 네트워크등의 인터페이스를 갖추지 않고 있을 수 있다.

이 때문에 라이센스를 발행하는 Peer 노드에서 P2P상의 다양한 시스템환경을 고려할수 있어야 하며 이를위해 본 논문의 (그림 6)의 Peer A는 Step0-2의 과정에서 Super 노드에 라이센스를 등록할 때 하나의 콘텐츠에 대하여 사용권한 설정이 각기다른 하나 이상의 라이센스를 설정하여 등록함으로써 P2P상의 다양한 시스템환경을 지원하도록 할수있다.

예를들어 Peer A가 사용횟수와 사용시간을 사용권한으로 가지는 라이센스를 작성할수 있는 Peer 노드라면 사용횟수가 3인 라이센스 1과 사용시간이 2일로 설정된 라이센스 2를 Super 노드에 등록한다.

이때 각 라이센스는 동일 콘텐츠 해시값으로 검색되므로 검색하는 Peer 노드 입장에서는 두 라이센스 모두 검색이 가능하게 된다. 이후 Peer B는 자신이 사용할 수 있는 라이센스 1을 선택하여 구매를 하게 될 것이다.

다만, Peer B에서 라이센스 2에 대하여 구매는 물론이고 발행도 할수 없게 해야 하므로 만일 Peer B가 구매를 시도할 경우 Step 3의 과정에 포함되는 메시지인 M에 구매자의 간단한 시스템 프로파일이 포함됨으로써 Step 4의 검증과정에서 라이센스 발행 거부가 일어나게 되고 Peer B의 구매를 막게 된다.

또한 라이센스를 여러 Peer 노드에서 발행하게 하여 본 모델의 이점을 극대화 하기 위해서는 위에서 언급한 일반적인 사용권한뿐만 아니라 라이센스 자체를 발행할수 있는 사용권한 역시 라이센스내에 포함될 수 있어야 한다. 이는 과금정책과 비즈니스 모델에 영향을 많이 받는 사용권한이므로 라이센스내에 특정필드를 두어 라이센스가 발급될 때 마다 추적정보를 기록하여 과금이 일어날 때 참조하여 수익금을 분배하게 할 수 있다.

4. 비 교

<표 1>은 기존의 연구된 DRM 이 적용된 P2P 모델과 본 논문에서 제안하는 DRM이 적용된 P2P 모델을 여러 관점에서 각각의 P2P모델 구조의 특징에 따라 비교한 결과를 나타낸다.

순수한 P2P는 모든 P2P상의 기능들이 Peer 노드들로 구성되고 수행되지만 기존의 DRM이 적용된 P2P모델인 서버-클라이언트 기반모델, 분산모델, 반분산 모델에서는 라이센스 발행기능과 라이센스 검색 기능을 포함한 DRM기능을

〈표 1〉 P2P 모델 성능 비교 평가

평가항목	서버 클라이언트 기반 모델	분산 모델	반 분산 모델	제안하는 DRM이 적용된 P2P모델
서버 부하	Poor	Rather Good	Fair	None
보안성	Good	Fair	Rather Good	Rather Good
라이센스 발급분산처리능력	Poor	Rather Good	Fair	Good
확장성	Poor	Rather Good	Fair	Good

지원하기 위하여 P2P상에 독립된 개체인 서버를 추가하였다. 특히 라이센스 발행에 관한 모든 기능들은 서버에서 관리하였으므로 수천에서 수백만의 Peer 노드에게 이러한 서비스를 수행하기 위해서 서버는 걸리는 부하는 클수밖에 없다.

P2P의 특성상 짧은 시간 이내에 전체 네트워크 규모가 수배로 커지는 경우가 허다하므로 서버의 용량이 크고 개개의 통신부하량이 작다고 하더라도 서버는 지속적인 서비스를 하지못할 가능성이 높아진다.

하지만 본 모델은 기존의 모델과는 달리 서버의 기능중 라이센스 발행기능을 Peer 노드에 추가하고 라이센스 검색기능을 Super 노드가 된 Peer 노드가 수행하게 함으로써 기존의 서비스를 유지하면서도 서버를 없앨수 있다. 물론 이 경우 각 Peer 노드는 라이센스 발행기능을 갖추어야 하며 Super 노드가 되었을경우 라이센스 검색 기능도 제공해야 하므로 Peer 노드내의 DRM 수행모듈의 크기는 현재보다 비교적 커지게 될것이다.

특히 Super 노드 기능이 활성화 되었을 시에 기존에 콘텐츠 리스트와 더불어 라이센스 리스트도 유지해야 하므로 2배 이상의 리스트 저장공간이 필요하게 될 것이고 콘텐츠 검색질의와 라이센스 검색질의가 거의 비슷한 빈도로 발생한다면 2배의 검색서비스에 대한 부하량을 가지게 될 것이다.

하지만 P2P상에서 콘텐츠 검색과 같은 부분은 실제 아주 작은 비율의 통신부하량이며 실제로는 작게는 메가바이트에서 크게는 기가바이트의 용량에 이르는 콘텐츠 자체의 전송에 대부분의 통신부하가 발생하므로 전체적으로 Peer 노드에 걸리게 되는 부하량은 미미한 수준이다.

즉, DRM 기능의 추가로 인해 부가되는 부하량을 기존의 P2P에서와 같이 모든 Peer 노드에 분산시키면서 서버자체가 존재하지 않으므로 서버 부하 측면에서 가장 우수하다.

보안성 관점에서 서버-클라이언트 기반 모델은 모든 DRM 기능을 서버에서 수행하므로 높은 가장 높은 보안성을 가지게 된다. 분산 모델은 모든 DRM 기능을 Peer 노드에서 수행하나 안전한 키 관리 방안이 제시되지 않았으므로 낮은 보안성을 가지며 반 분산 모델은 사용자 인증을 DRM 서버에 맡기므로 비교적 높은 보안성을 가진다. 본 논문에서 제안하는 모델은 라이센스의 발급과 전송시에 제안한 키 관리 방안을 사용함으로써 비교적 높은 보안성을 지닌다.

라이센스 발급 분산처리 능력 관점에서 서버-클라이언트 기반 모델은 모든 라이센스를 서버가 발행하므로 서버의 장애나 오류시 라이센스를 발급 받을 수 없으며 라이센스 발급 요청에 대해 서버의 처리능력이 따라가지 못할 수 있다. 분산 모델은 최초 콘텐츠를 패키징한 Peer만이 라이센스를 발행할 수 있으며 네트워크 전체의 라이센스 발행을 제어하기 위한 DRM 서버가 존재 하므로 서버-클라이언트 기반 모델과 같은 이유로 안정적인 라이센스 발급능력을 제공할 수 없다. 반 분산 모델도 분산 모델과 동일한 문제점을 가지며 사용자 인증 기능을 DRM 서버에 둠으로서 보안성은 향상 시킬 수 있으나 라이센스 발급처리 능력에 있어서는 더욱 서버의 부하를 가중시킨다. 본 논문에서 제안하는 모델은 DRM 서버가 존재하지 않으면서도 FastTrack 프로토콜을 수정하여 라이센스를 검색한 후 Peer 노드간의 라이센스 발급이 가능하고, 라이센스 발급가능한 Peer 노드를 여러 개 검색하여 찾을 수 있으면 라이센스 자체도 여러 Peer 노드들 중에서 발급받을 수 있으므로 가장 높은 라이센스 발급분산 처리능력을 나타낸다.

확장성 측면에서 앞서 말한 분산처리 성능과 관련하여 본 논문에서 제안하는 모델은 새로운 시스템이 P2P 네트워크 상에 추가되면 전체적인 성능이 향상된다고 볼 수 있고, 일부 라이센스 발급 Peer 노드가 라이센스 발급능력에 장애를 입는다 하더라도 다른 Peer 노드에서 계속 라이센스 발급이 가능하므로 P2P 본연의 장점을 그대로 살릴 수 있어 P2P 네트워크의 확장이 용이하다. 이와는 달리 다른 모델들은 DRM 서버의 존재로 인하여 P2P 네트워크가 커질수록 DRM 서버의 병목현상이 우려되고 라이센스 발급 Peer 노드의 장애나 DRM 서버의 장애로 인해 라이센스 발급 장애가 발생할 가능성이 높아진다.

5. 결 론

P2P는 가장 큰 콘텐츠 유통 경로로 활용되기도 하지만 콘텐츠의 가장 큰 불법 유통 경로로 활용되어 콘텐츠 불법 유통을 야기시키고 있다. 이러한 문제점을 해결하기 위해 기존의 연구에서는 P2P 구조와는 별개의 DRM 서버를 유지하는 서버-클라이언트 기반 구조의 DRM을 채택하고 있으며 이는 P2P 구조에 적합하지 않을 뿐만 아니라 P2P 본연의 장점을 전혀 이용할수 없게하며 DRM 서버의 유지비용을 발생시킨다

이에 본 논문은 기존의 P2P시스템에서 기존구조에 변화를 주지않고 DRM을 지원할 수 있는 P2P 환경에서 콘텐츠 보호를 위한 DRM이 적용된 P2P 모델을 제안한다. 제안된 방안은 콘텐츠 보호를 라이센스 발행을 통하여 지원하며 DRM 시스템에서 요구하는 기능을 기존의 P2P 구조에 맞도록 적용하였으므로 P2P의 높은 확장성과 분산 처리 성능을 지원할 수 있다. 제안된 방안은 콘텐츠 배포 시 FastTrack과 FastTrack 호환, 계열 프로토콜의 분산처리 능력을 전혀 저하시키지 않으며, 라이센스 발급 시 P2P 환경의 분산 처

리를 활용하여 여러 Peer 노드가 라이센스 발급 서버 역할을 수행함으로써 높은 라이센스 발급 분산 처리를 제공한다. 본 논문에서 제안하는 DRM이 적용된 P2P 모델은 보다 다양한 비즈니스 모델과 결합하여 사용 될수 있으며 또한 다른 모델들은 DRM 서버와 같은 새로운 장비의 추가가 필요하지만 제안하는 모델은 기존의 구조를 그대로 사용하고 실제 소프트웨어의 업그레이드 만으로 구현할 수 있는등 이점이 있다.

향후 DRM 수행모듈의 신뢰도 향상 방법과 사용권한 제어와 콘텐츠 흐름 추적 등에 대해서 더욱 연구가 필요하다.

참 고 문 헌

[1] "Napster" http://www.napster.com

[2] "Gnutella" http://www.gnutella.com

[3] "KaZaA" http://www.kazza.com

[4] "FastTrack" http://en.wikipedia.org/wiki/Fasttrack

[5] Iwata, T.; Abe, T.; Ueda, K.; Sunaga, H.; "A DRM system suitable for P2P content delivery and the study on its implementation" APCC 2003. The 9th Asia-Pacific Conference on Vol.2, pp.806~812, 2003.

[6] Kwok and S. M. Lui, S. H. "A License Management Model to Support B2C and C2C Music Sharing" In Proceedings International WWW Conference (10), Hong-Kong. 2002.

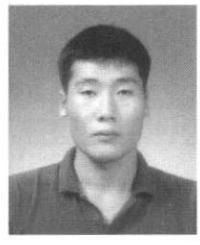
[7] Ton Kalker, Dick HJ Epema, Pieter H. Hartel, Reginald L. Lagendijk, M. Vansteen "Music2Share-Copyright-Compliant Music Sharing in P2P Systems" In Proceedings of the IEEE. Vol.92, pp.962-970, 2004.

[8] "OMA(Open Mobile Alliance)DRM" http://www.openmobilealliance.org

[9] William Stallings, Cryptography and Network Security: Principles and Practice (2nd Edition), Prentice-Hall, pp. 341-349, 1999.

[10] "XrML" http://www.xrml.org

[11] "ODRL" http://www.w3.org/TR/odrl/



성 재 연

e-mail : sjy64387@etri.re.kr

2005년 안동대학교 컴퓨터공학과(학사)

2005년~현재 과학기술연합대학원대학교 (석사)

관심분야 : 정보보호, DRM

정 연 정

e-mail : yjjeong@etri.re.kr

1994년 부산대학교 전자계산학과(학사)

1996년 부산대학교 전자계산학과(석사)

2005년 충남대학교 컴퓨터과학과(박사)

1996년~현재 한국전자통신연구원 선임연구원

관심분야 : 정보보호, DRM

윤 기 송

e-mail : ksyoon@etri.re.kr

1994년 부산대학교 조선공학과(학사)

1988년 City University of New York 전산학과(석사)

1993년 City University of New York 전산학과(박사)

1993년~현재 한국전자통신연구원책임 연구원

관심분야 : 정보보호, 저작권 보호, 분산처리