P2P네트워크 환경을 위한 DRM 시스템 설계

이정기* · 김국세* · 이광** · 안성수***· 이 준*
*조선대학교, **청주과학대, ***동신대학교

Design of DRM System in P2P Network Environment

Jeong-Gi Lee* · Kuk-Se Kim* · Gwang Lee** · Seong-Soo Ahn*** · Joon Lee*
*Chosun University, **Chongju national College of Science & Technology, ***Dongshin University
E-mail : jk1004@chosun.ac.kr

요 약

P2P는 현재 활발히 진행되고 있는 비즈니스의 중요한 변화를 표현하는 함축적 용어라는 의미를 가진다. P2P 서비스는 인터넷상의 정보를 검색엔진을 거쳐 찾아야 하는 기존 방식과 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보를 제공받고 검색은 물론 내려 받기까지 할 수 있는 서비스이다. 이는 웹 사이트에 한정돼 있던 정보추출 경로를 개인이나 회사가 운영하는 데이터베이스로까지 확대할 수 있다. 즉 자신의 정보를 전국적 혹은 세계적으로 관리 운용하며, 회원 상호간의 다양한 정보 공유뿐만 아니라 동일한 정보를 공유하고자 하는 회원간의 커뮤니티 형성이 가능하며, 그룹웨어로서 역할을 통해 원격회의, 원격교육 등이 가능하다는 것이다.

ABSTRACT

The word P2P implies significant changes in current business dynamics. The P2P service enables individuals to be connected to the Internet for the direct provision of information and even downloads from one another without the conventional method of passing through search engines. This can be utilized to extend the path of retrieving information from limited web sites to personal and enterprise databases. That is, it is now possible for individuals to manage their own information on a national or global scope, share various information with other members, form communities of users interested in sharing homogeneous information, and utilize remote conference and remote education using groupware.

Ⅰ. 서 론

P2P 기술이 인터넷에 연결되어 있는 모든 컴퓨터를 네트워크화시킴으로써 방대한 콘텐츠 저장창고 역할을 하는 반면 그것은 역으로 그 만큼의 저작권 침해의 문제를 안고 있다.

디지털 콘텐츠가 네트웍을 통해 자유롭게 유통 되면서 불법복제로 인한 저작권 침해 방지하기위해 Microsoft, IntelTrust등의 업체가 DRM을 시도하고 있으나 초기시장을 형성하던 디지털 음악 및 전자문서 시장의 침체와 저작권자 위주의 DRM 기술에 대한 사용자의 불만 증대, 상이한 DRM 기술들 간의 상호호환성 결여 등의 이유로 제한된 범위에서만 사용되어 왔다. 콘텐츠의 표현 방식은 물론 제작 및 배포, 소비 구조 전송방식, 단말 방식 등이 모두 독립적으로 개발되고 있어 콘텐츠 제공자, 관리자, 사용자 등 모두에게 호환성 문제 또는 해결하는 과제로 남고 있다.

본 논문에서는 P2P 가장 큰 장점인 네트워크가 연결된 모든 컴퓨터에서 원하는 콘텐츠(음악, 동영상, 사진, 논문파일 등등)를 자유롭게 다운 받을수 있는 기술을 유지하며 현재 가장 이슈가 되고 있는 콘텐츠 저작권문제를 해결하는 방안으로 P2P상에서 디지털 콘텐츠 보호를 위한 DRM(Digital Rights Management)시스템을 설계 및 구현 하고자 한다.

Ⅱ. 본 론

1)P2P 및 DRM 기술

P2P 네트워크를 통하여 절달된 디지털콘텐츠에는 여전히 사용규칙이 첨부되어 있으며, 해당 콘텐츠를 수신한 사용자는 그 사용규칙에 따라서만 그 콘텐츠를 이용할 수 있다. 또한 사용자는 DRM에 의하여 보호받고 있는 콘텐츠를 DRM기술을 채택한 장치(s/w ,h/w)를 통하여만

이용할 수 있을 것이다. 이 경우에도 사용자는 clearinghouse를 통하여 대가를 지급한 경우에만 정해진 사용규칙에 따라 해당 콘텐츠를 이용할 수 있게 된다. 사용규칙은 매우 다양하여 콘텐츠의 복제횟수, 사용횟수, 배포조건 등을 자세히 정할 수 있다[1][2].

P2P서비스가 단순한 파일공유서비스에만 머무는 경우에는 공유되는 파일이 DRM기술에 의하여 보호되는 한, 앞으로 저작권침해문제는 크게 발생하지 않을 것이다. 그러나 P2P서비스가 지속적인 수익을 창출할 수 있는 하나의 비즈니스 모델로서 성공하기위해서는 결국 디지털콘텐츠의 권리자와 각 소비자들이 P2P기술을 통하여 전자상거래를 하는 방향으로 나아가야 할 것이다. 이 경우 디지털콘텐츠의 거래는 P2P를 기반으로 한 사이트의 중개로 이루어지고, 실제 거래 자체는 각 판매자와 구매자의 컴퓨터상에서 이루어지게 된다. 이 경우에는 특히 거래대상인 콘텐츠의 불법거래나 불법이용을 방지하기 위하여 보안기술이 필요하며, 여기서 DRM이 중요한 역할을 할 수 있다.

콘텐츠판매자는 DRM기술로 보호받는 콘텐츠를 P2P망을 통하여 직접 판매하고, 그렇게 판매된 콘텐츠의 사용자는 다시 clearinghouse를 통하여 사용료를 지급하고, 정해진 사용규칙에 따라 해당 콘텐츠를 사용하는 것이다. 그러나 종래의 DRM 기술은 일대다 와 한 권리자 대 다수의 이용자 의 이용 상황을 전제로 한 것이고, P2P서비스는 일대일의 상황을 전제로 한 것이다. 따라서 일반적인 저작물판매의 경우보다 P2P를 통한 전자상거래 환경 하에서 DRM기술을 접목시키는 것은 쉽지 않다. 현재 업계에서 P2P환경과 DRM 기술을 접목시키려는 노력을 하고 있으나, 이러한 유형의 비즈니스모델로 상용화된 것은 아직 보이지 않는다[3].

2)P2P에 적용 가능한 DRM 모델

그누텔라와 같은 P2P 구조는 피어들 간의 파일 공유를 직접 하기 때문에 서버를 사용하지 않고 피어들끼리 정보를 바로바로 교환할 수 있다. 따라서 서버를 거치는 경우보다 훨씬 빠른 최근의 정보를 찾을 수 있으며, 파일을 인덱스할 필요도 없다. 그러나 P2P를 통한 공유는 저작권 침해의 온상으로 저작권 관리 기술 및 여러 요구사항들이 반드시 필요하다. 라이선스 기법, 높은 분산 컴퓨팅 지원 그리고 콘텐츠를 발생하는데 있어서의 절차의 간소화 등 P2P 콘텐츠 전송에 적합한 DRM 기능을 고려해야 한다.

일반적으로 DRM 시스템은 다음 조건들을 만족해야 한다.

능동적 보안 : 콘텐츠 암호화, 사용 조건 검사(사용자 이름, 단말기, 사용횟수, 사용 시간, 지불 등), 복호화된 콘텐츠 파일의 저장 방지

수동적 보안 : 콘텐츠에 워터마크 삽입, 전송 및 사용 조건 추적

콘텐츠가 DRM 시스템에 등록될 때 콘텐츠는 암호화되고 삽입된 워터마크가 주어진다. 그리고 사용 조건과 분배를 위한 캡슐 제어 프로그램(capsule control program)과 더불어 암호화한다. P2P를 통해 콘텐츠를 공유할 경우 콘텐츠 자체가 서버를 통하지 않고 직접 한 사용자에서 다른 사용자에게 전송이 될 수 있으며 어떤 사용자는 콘텐츠를 암호화 시켜 저장할 수 있다.

3)기존 DRM 모델 한계

P2P 네트워크에 DRM을 적용하기 위해서는 안전성, 서버에대한 부담성, 빠르고 쉬운 다운로드 등을 고려하여야 한다. Pure 모델은 모든 DRM 처리는 서버에서 수행되는 반면 암호화된 콘텐츠는 P2P 모드로 전송된다. 사용자 피어(peer)들은 DRM 서버에 접근하여 수신된 콘텐츠를 복호화하기 위해 요청 (request) 기능을 장치에 가지게 된다[6] 리고 DRM 서버에 라이선스 발행을 요청하는 기능은 반드시 사용자 단말기에 설치되어야 한다. 이 방식에서 서버는 반드시 모든 사용자의 계정을 인증, 지불 및 정산을 통해 관리해야 한다. 암호화와 사용 제어 기능이 모두 DRM 서버에서 관리되며 사용자 인증을 한 서버 역시 센터에 위치하게 된다. 따라서 신뢰성과 안전성은 보장되지만 사용자 수가 증가할수록 서버엔 부담이 커지게 된다. Hybrid 시스템은 본 논문에서 제안하고자 하는 유료든 무료든 다운로드는 쉽고 빠르게 하며 유료일 경우 안정적이며 DRM서버에 무리를 주지 않는 가장 이상적인 모델로 Hybrid P2P 기반의 DRM이 적당하다. 그러나 Hybrid 시스템과 DRM기술을 다순 접목을 시키면 저작권자의 이익과 수익만을 보장하므로 P2P 가장 큰 장점인 정보공유에 문제점이 발생하며 또한 DRM 시스템의 목적인 보안 위협에 그대로 노출이 되므로 본 논문에서는 새로운 형태의 P2P 기반의 DRM 모델을 제안한다[3][4]

III. P2P 기반 DRM 시스템 설계

본 논문에서 제안하는 P2P 시스템에 DRM 기술을 효과적으로 적용하는 것이며 무엇보다 P2P상에서 Peer 들끼리의 수익성을 위해 superdistribution를 통해 유료컨텐츠의 수익만을 위한 모델이 아니다. 논문에서 제안하는 P2P 시스템은 분산컴퓨팅의 성능을 최대한 살리고 사용자 증가에 따른 엄청난 부하는 일어나지 않게 하며 정보 공유시 일어날 수 있는 모든 보안 위협 요소를 해결하고자 한다. Client/Server 기술 은 중앙 집중 방식을 지향하는 시스템 기술이며 중아서버가 존재한다. 제안하고자 하는 P2P 시스템은 분산처리 방식으로 중앙서버없이 Peer들 간의 쌍방향 통신이 가능하다. DRM의 경우는 라이선스 발급을 위한 클리어링하우스와

인증 서버 그리고 콘텐츠 암호화를 제공하는 패키저 등이 핵심 기술이다. 이런 요소들은 단순 접목의 P2P 시스템의 Peer들 간에 구현하기에는 곤란하다. 현 DRM 시스템이 인증과 과금 정보에 있어 중앙 서버를 따로 두는 경우처럼 P2P 네트워크에 적용하려면 서버/클라이언트 모델의 장점인 신뢰성과 안정성 및 중앙서버에 의한 시스템 전체 관리 가능 또한 중앙 서버의 다중화를 통해 Peer 장치간 동적 네트워크 구성이 가능하도록 하여 신뢰성을 향상시키도록 한다. 네트워크 관리 측면에서 보면 DRM은 콘텐츠 사용에 대한 라이선스 발행과 관리를 클리어링하우스에서 이행한다. 본 논문에서는 네트워크 환경에서 콘텐츠의 제공자, 저작권자, 배포자, 사용자 등의 권리를 보호하고, 안전하고 투명한 콘텐츠 사용을 지원하는 DRM 시스템을 설계하고자 한다.

<그림 1>은 DRM 유료관리 시스템의 P2P기반 DRM시스템 설계 한것이다. DRM Server는 크게 암복호 모듈, 라이선스 관리모듈, 키 관리모듈, 거래관리모듈 등으로 구성된다. DRM Client는 라이선스 키 관리 모듈, 복호화 모듈 등으로 구성된다. 그림 15에서 DRM Server는 S/W 암호개발자로부터 받은 파일을 암호화 처리하며, 라이선스 키 제작을 하고 온라인으로 유료 전송을 담당하여 Client 로부터 콘텐츠 요청이 있을 경우 결제를 통하여 승인 여부를 체크한 후 콘텐츠를 암호화모듈을 이용하여 암호화하게 되고 이정보를 DB에 기록하여 DRM Client 가 이 정보를 통하여 사용자 라이선스 체크여부를 결정할수 있게 하는 역할을 한다.

DRM Client는 DRM Server 측에서 다운 받은 암호화된 파일을 라이선스 획득 여부에 따라 복호화 시켜주며 복호화와 동시에 사용자 하드웨어 정보를 Server로 전송된다. 이 사용자 하드웨어 정보를 이용하여 사용 여부를 결정해 주며 계속적인 사용자 관리를 가능하게 한다.

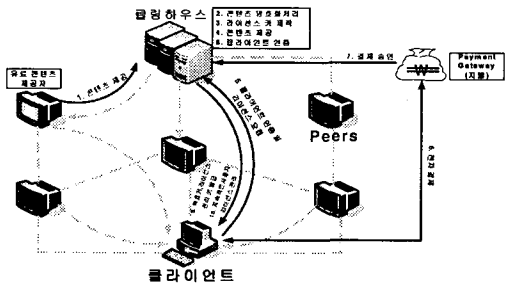

그림 4 P2P 기반 DRM 설계

1. Clearinghouse 설계

콘텐츠의 사용권한을 부여하고 이에 대한 지속적인 관리를 담당하는 시스템이 필요하게 되는데 이러한 역할을 담당하는 것이 Clearinghouse이다. Clearinghouse는 사용자의 콘텐츠 결제 처리를 담당하는 Financial Clearinghouse와 사용권한 정보가 담겨 있는 라이선스를 발급 및 관리하는 License Clearinghouse, 그리고 사용자의 콘텐츠 사용내역을 수집하여 이를 통계 처리하는 Usage Clearinghouse 로 크게 구분할수 있다. 본 논문에서 제안한 DRM 시스템은 그림 16과 같이 하나의 서버에서 콘텐츠 생성 관리, 일괄 처리 할 수 있도록 DRM Server 와 Packager, Retailer의 기능을 하나의 Clearinghouse에 포함 시켰다. 그러나 DRM Server 와 Packager, Retailer 는 독립적인 시스템으로 동작된다. 인증 모듈에서는 콘텐츠의 불법 사용을 방지하기 위하여 사용자의 인증 정보와 하드웨어 바인딩 기법으로 사용자의 하드웨어 정보를 이용하여 인증을 받는다. 본 논문은 사용자 단말기 네트워크 카드의 MAC Address를 해쉬함수에 적용한 값을 이용하여 사용 가능한 단말기를 제한하였다. 그리고 콘텐츠의 암호화와 패키징을 위하여 128 비트의 SEED 암호알고리즘과 128비트의 AES 암호 알고리즘을 사용하도록 설계하였다.

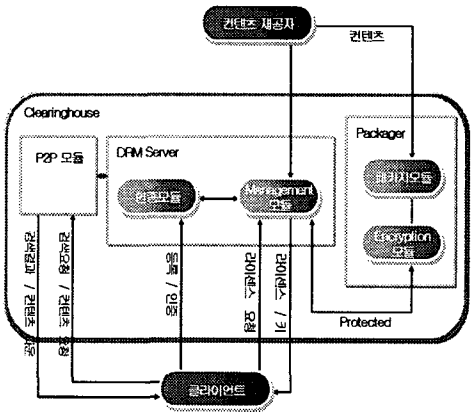

그림 5 Clearinghouse 설계

2). 인증 프로토콜

콘텐츠를 사용하기 위해서는 그림 17와 같이 사용자인증을 받아야 한다. 사용자인증은 회원가입을 통해 이루어지지만 본 논문에서는 하드웨어 바인딩 기법을 사용하기 때문에 회원 가입과 동시에 클라이언트 네트워크 카드 주소까지 함께 전송을 시켜 인증을 하도록 하였다. 콘텐츠를 다운 받은 사용자는 누구든지 회원에 가입할 수 있으며 이를 위해서 PKI기반의 인증서를 통한 로그인을 지원한다. ID와 암호기반의 로그인이나 인증서 기반의(Kb1=h(Binding_info)) 로

그인 과정을 통하여 사용자 인증을 받으면 서버는 인증서 Cert_u를 검증후 올바른 인증서이면 사용자 에게 인증이 성공적이라는 것을 알린다.

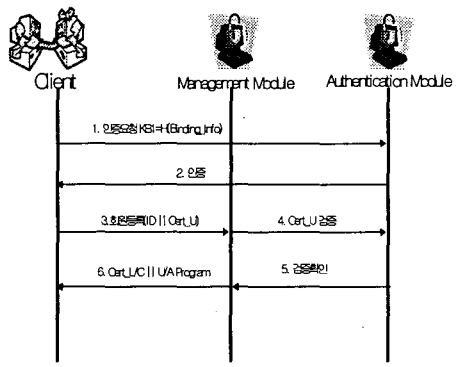

그림 6 인증 프로토콜

III. 결 론

P2P 기술이 인터넷에 연결되어 있는 모든 컴퓨터를 네트워크화시킴으로써 방대한 콘텐츠 저장창고 역할을 하는 반면 그것은 역으로 그 만큼의 저작권 침해의 문제를 안고 있다. 이에 따라 많은 콘텐츠 저작권자들이 P2P 솔루션을 기반으로 하는 온라인 서비스업체를 상대로 저작권 소송을 벌이고 있다 PC 통신이나 HTTP를 기반으로 하는 서비스 제공자의 경우 중앙에서 서버를 관리하고 통제함으로써 저작권 위반가능성이 있는 파일들에 대해 제재와 통제가 용이하지 않다. 또한 저작권문제 이전에 개개인의 컴퓨터를 통제하는 데서 오는 프라이버시 침해 문제 등의 유발 가능성이 있어 저작권관리는 쉽지 않을 전망이다. 그러나 P2P가 미래의 비즈니스 모델로서 기대됨에 따라 바이러스와 해킹 등의 보안 문제와 함께 저작권문제는 필연적으로 해결해야 할 사안이다.

사용자가 키를 노출했을 경우에는 심각한 보안 위협이 된다. 또 다른 기술적인 관심 사항 중에 하나는 키를 어디에 저장하느냐 하는 문제이다. 서버에 저장할 경우 키 관리의 문제를 단순하게 만들기는 하지만 사용자는 항상 서버와 온라인 상태를 유지해야 하는 단점이 있다. 사용자 컴퓨터에 두는 경우 키가 쉽게 복사되어도 안되며 쉽게 훼손되어서도 안 된다. 사용자 컴퓨터에 두었을 때 또 다른 문제점 중에 하나는 사용자가 당초 사용권한을 받은 컴퓨터가 아닌 다른 컴퓨터에서는 저작물을 사용할 수 없다는 점이다.

참고문헌

[1] Doraswamy, N., and Harkins, D. IPSec. Upper Saddle River, NJ: Prentice Hall, 1999.

[2] Drew, G. Using SET for Secure Electronic Commerce. Upper Saddle River, NJ: Prentice Hall, 1999.

[3] AAp, Digital Rights Management for Ebooks: Publisher equipments

[4] Chor, B., A. Fiat, and Naor, "Tracing Traitors", in Advances in Cryptology, Proceeding of CRYPTO '94, vol. 839 of Lecture Notes in Computer Science, Spinger_Verlag, PP 257-270, 1994.

[5] Jurgen Nutzel, "Matching Algorithms in Alternative File-Sharing Systems to Find New Users Having New Content", IICS 2003, LNCS 2877, PP. 180-188

[6] Akiko Seki, Wataru Kameyama, " A Proposal on Open DRM System Coping with Both Benefits of Rights_Holders and Users", IEEE GLOBECOM 2003, GC208