情報保護學會論文誌
第13券 第4號, 2003. 8

컨텐츠 스트리밍을 위한 안전한 DRM 시스템 설계 및 구현*

이 진 흥**, 김 태 정**, 박 지 환**

Design and Implementation of Secure DRM System for Contents Streaming

Jin-Heung Lee**, Tea-Jung Kim**, Ji-Hwan Park**

요 약

DRM(Digital Rights Management)은 인터넷상에서 디지털 컨텐츠의 안전한 유통과 저작권을 관리하는 기술이다. 기존의 DRM 시스템은 암호화된 컨텐츠를 다운로드 한 후에 간단한 인증 절차를 거쳐 사용을 허가하는 형태가 일반적이다. 본 논문에서는 종단간의 실시간 데이터 전송을 위해 RTP(Real-time Transport Protocol)를 이용한다. 그리고 주기적인 사용자 인증을 통해 컨텐츠의 안전한 유통 및 저작권 보호를 가능한 시스템을 설계하고, 그것을 기반으로 하는 DRM 시스템을 구현하였다. 제안된 시스템은 인증된 사용자만이 라이센스에 대한 접근 권한을 부여 받음으로써 네트워크 상에서 컨텐츠의 불법 유통 및 불법 복제가 불가능하도록 하였다.

ABSTRACT

DRM(Digital Rights Management) is a technology that manages secure distributions and copyrights of digital contents on the Internet. It is general giving the rights to use the encrypted contents that are downloaded by a simple authorization process in the existing DRM system. Once this is done you are allowed to access. In this paper, we use RTP(Real-time Transport Protocol) for end-to-end real-time data transmission. And the system is designed to make it possible to protect copyrights and to distribute contents with safety through periodic authentication. We implemented DRM system to stand this basis. The proposed system vests only authorized users with authority to access the license. Hence it prevents contents to be distributed and copied illegally on networks.

keyword : *DRM(Digital Rights Management), 저작권보호, RTP/RTCP, 스트리밍 서비스*

Ⅰ. 서 론

인터넷 및 정보통신 기술의 발전으로 다양한 컨텐츠가 개발되어 이용되고 있다. 디지털 정보의 편리성으로 디지털 컨텐츠에 대한 수요가 증가하고, 제작 및 유통이 용이함으로 디지털 컨텐츠 제작은 더욱 증가될 것이다. 이러한 컨텐츠 유통의 증가는 전자상거래, 컨텐츠 제작업체, 지불업체 등 다양한 분야의 산업 활성화를 가져오게 될 것이다.

그러나 디지털 정보는 복제, 변형, 불법 유통 등이 용이함으로 저작권자 및 유통업체의 피해를 가져오고, 수익창출의 어려움으로 컨텐츠 산업의 심각한 문제가 되고 있다. 또한, 인터넷으로 컨텐츠의 유통 및 지불이 이루어지므로 보안상의 문제가 심각하게 대두되고 있다. 따라서, 무분별한 불법 유통을 막고, 저작권자 및 유통업체의 수익 분배를 위한 관리 시스

* 본 논문은 2003년도 영남지부 학술대회 우수논문임.
** 부경대학교 대학원 정보보호학과(jhlee@pknu.ac.kr, tjkim@dreamwiz.com, jpark@pknu.ac.kr)

템이 필요하다. DRM 시스템은 디지털 컨텐츠를 인가된 사용자에게만 안전하게 전달 및 사용 가능하게 하는 시스템으로 디지털 컨텐츠의 문제점들의 해결 방안으로 제시되고 있는 기술이다.[1]

디지털 저작권 관리는 사용자와 저작권자와의 계약에 의해 디지털 컨텐츠(소프트웨어, 음악, 비디오, e-books 등)를 안전하게 사용할 수 있도록 해야 한다. 이러한 계약은 컨텐츠에 접근하는 사용자 인증과 실행 결과에 대한 저작권 사용을 승인한다. DRM 시스템은 일반적으로 서버로부터 컨텐츠를 넘겨받아 클라이언트에서 분배되며, 어플리케이션에서 승인된 컨텐츠의 접근을 수행한다. 이러한 DRM 시스템은 전체 시스템을 모니터 할 수 있어야 하며, 시스템과 독립적으로 설계되어야 한다. 또한, 사용자들의 권한을 확인하고, 그들을 모니터링 하는 기능을 가져야 한다.[2]

본 논문에서는 인터넷 방송과 같은 컨텐츠 스트리밍을 위한 DRM 시스템을 설계 및 구현하였다. 논문의 구성은 2장에서 DRM에 관한 관련연구를 기술하고, 3장에서 제안된 DRM 시스템의 구성 및 특징에 대하여 서술하며, 4장에서 전체 시스템의 구현에 대하여 기술한다. 끝으로 5장에서 결론 및 향후 연구 과제를 제시한다.

II. DRM 관련 기술

2.1 저작권 관리를 위한 기술

저작권 관리 기술은 온라인 환경에서 일어나는 저작권자 및 제공자에 대한 저작권을 지속적으로 관리하는 기술을 말한다. 이러한 저작권 관리 기술에는 디지털 컨텐츠를 식별하는 기술과 컨텐츠에 대한 권리를 명세 하는 기술이 있다. 전자에는 도서에 부여되는 ISBN과 같이 모든 디지털 컨텐츠를 식별 가능한 번호 체계를 부여함으로써 저작권 정보를 등록하고 관리하는 컨텐츠 저작권 등록 관리기술(DOI, Digital Object Identifier)이 있다.[3] 그리고 권리 명세를 위한 기술로는 저작권 보호 및 관리 시스템을 효과적으로 구축 가능한 XrML(eXtensible Rights Markup Language) 등이 있다.[4] XrML은 XML로 정의된 명확한 구문 규칙을 기반으로 정의된다. 현재 저작권 관리를 위한 기술은 저작권에 대한 내용을 명시하기 위해 XrML 기반으로 표준화가 진행되고 있으며, 식별자 부여를 위해서 DOI 기술을 적극 활용하는 추세이다.

2.2 저작권 보호를 위한 기술

저작권자 및 컨텐츠 제공자는 저작권 보호를 위해 컨텐츠를 허가되지 않은 사용자로부터 안전하게 보호되어야 한다. 저작권 보호를 위한 기술은 암호화 기술을 중심으로 발전되어왔으나, 그 이외에도 디지털 워터마킹 기술, 접근제어 기술 등의 다양한 기술들이 이용된다.

2.2.1 암호화 기술(encryption techniques)

암호화 기술을 이용한 컨텐츠의 보안 강도는 암호화를 위해 사용된 알고리즘의 강인성과 암호화의 키 길이, 그리고 이러한 암호 알고리즘을 처리하는 프로세스의 강인성 정도에 따라 달라진다. 국내 표준으로 제정된 SEED 알고리즘과 DES 알고리즘을 대체하기 위해 개발되고 NIST에서 차세대 블록암호로 선정된 AES(Advanced Encryption Standard) 알고리즘은 이러한 강인성을 유지하면서 보다 효율적이고 안전하게 설계되어 졌다.[5,6] SEED와 AES 알고리즘은 알려진 여러 가지 해독 공격에 강하고, 여러 플랫폼에서 빠르게 동작되며, 구조가 단순하게 되어있어 보다 효율적이고 안전하게 사용될 수 있다. 그러나 암호화 기술은 일단 암호화된 데이터의 평문을 얻은 사용자는 원래의 소유권자와 동일한 능력을 갖게 되어 데이터의 저작권과 소유권을 알 수 없기 때문에 이를 무단 복사하여 배포하는 것을 막을 수 없는 단점이 있다.

2.2.2 디지털 워터마킹 기술(digital watermarking techniques)

디지털 워터마킹 기술은 컨텐츠의 원 소유자를 주장할 수 있는 워터마크 정보를 삽입하여 저작권에 대한 분쟁이 발생할 경우 삽입된 워터마크 정보를 추출하여 저작권을 주장하는 기술이다. 최근 컨텐츠의 활용 증가에 의해 문서의 불법유통 방지, 신분증 위·변조 방지, 디지털 방송, DVD Player, Potable Device 등 다양한 분야로 확대되고 있다. 디지털 워터마킹 기술은 다양한 신호처리 공격 및 고의적인 공격에 대한 강인성(robustness)과 워터마크 정보의 삽입에 따른 비가시성(invisibility), 확실한 소유권 증명이 가능하도록 하는 신뢰성(reliability) 그리고, 기본 플랫폼에 대해서 구현 가능한 효율성(efficiency) 등이 요구된다.[7]

디지털 워터마킹 기술은 지적 재산권 보호를 위한 기술일 뿐만 아니라 응용분야에 따라 불법 유통을

추적할 수 있는 핑거프린팅(fingerprinting), 데이터 인증 및 무결성 검증 등과 같은 다양한 분야에 응용 가능하다.

2.2.3 접근 제어 기술(access control techniques)

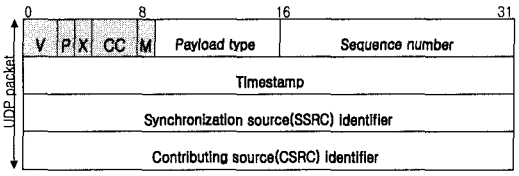
접근 제어 기술은 제한적인 권리에 따라 이용 횟수나 시간 등을 한정시키기 위한 기술로서 허가되지 않은 접근을 방지하는 기술이다. 접근 제어 기술은 정보보호 서비스에 직접적인 관계를 가지며, 각 서비스에 대한 권한 할당을 위한 수단이 된다.

컨텐츠의 저작권 보호를 위한 접근 제어 기술은 컨텐츠 자체에 대한 접근 방지 기술과 사용자의 권리에 따른 접근 제어 기술로 구분될 수 있다. 일반적인 뉴스, 스포츠 소식, 이미지 서비스 등은 사용자 식별을 통하여 인가된 사용자에게만 접근 권한이 부여되도록 구성해야 한다. 그러나 무선 환경에서의 벨소리 다운로드 및 바탕화면 서비스 등은 컨텐츠와 그 컨텐츠에 대한 사용 권리를 분리시켜 다운로딩 등에 대한 접근 권한 제한적으로 가능하게 해야 한다. 이와 같이 이용자 간의 컨텐츠 이동을 'Superdistribution'이라고 한다.[8] 이 경우, 이용자가 유통의 한 부분을 담당하게 되고, 컨텐츠를 전송하는 과정에서 컨텐츠 판매업자, 광고주들의 훌륭한 마케팅 효과를 거둘 수 있는 장점을 가진다. 그러나 이러한 접근 통제 방식은 암호화 기술과 같이 저작권 및 소유권을 제공하지는 않기 때문에 저작권 문제의 근본적인 해결책은 되지 못한다.

2.3 스트리밍 서비스를 위한 프로토콜

RTP(Real-time Transport Protocol)[9]는 오디오, 비디오 등의 실시간 데이터를 멀티 캐스트 또는 유니 캐스트 네트워크를 이용한 단말-대-단말 네트워크 전송 서비스에 알맞은 프로토콜이다. RTP 데이터 전송 기능은 제어 프로토콜인 RTCP(RTP Control Protocol)에 의해 확장된다. RTCP는 데이터의 전달 상황을 감시하고, 최소한의 제어 기능과 매체 식별 기능을 제공한다.

RTP는 별개의 독립 계층으로 구현되기보다는 특정 응용에서 요구되는 정보를 제공하여 프로토콜의 처리가 응용 처리 과정으로 통합될 수 있도록 설계되었다. 따라서 기존의 프로토콜들과는 달리 RTP는 응용의 필요에 따라 헤더를 변경하거나 추가하여 응용에 맞는 프로토콜이 될 수 있도록 하는 일종의



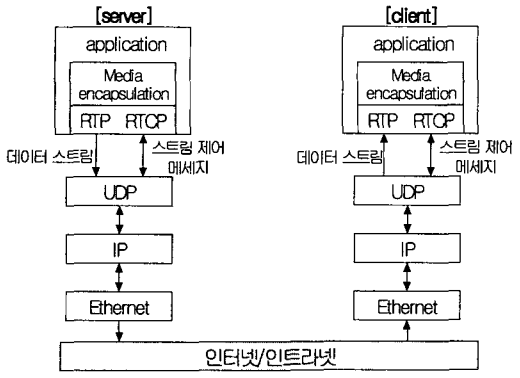
〔그림 1〕 RTP Header

맞춤형 프로토콜이다.

TCP나 UDP와 같이 코드량이 많고 수행시간이 긴 프로토콜에 비해 RTP는 간략화된 프로토콜에 의해 수행시간이 적기때문에 실시간 응용프로그램에 알맞다. 이러한 실시간 전송을 위해서 RTP는 [그림 1]과 같이 헤더 내에 일련번호를 제공하여 데이터를 순차적으로 처리할 수 있게 하며, 데이터가 생성된 시각 정보에 의해 처리되어야할 시각을 알려줌으로써 다른 스트리밍 데이터와 동기를 맞출 수 있게 된다.

다시 말하면, 모든 RTP 패킷은 timestamp를 가지며, 클라이언트(client)의 플레이어(player) 내에서 발생하는 동기신호 사이의 매핑을 수행한다. 또한, timestamp는 다양한 데이터 소스로부터 제공되는 미디어들을 통합하는 기능을 가지고 있다. 전송되는 각각의 패킷은 Sequence number와 timestamp를 가지며, Sequence number는 각 패킷마다 유일한 번호로서 패킷 손실에 대한 검출과 복구에 이용된다. Timestamp는 동일한 번호를 지님으로서 특정한 시간에 전송되어진 데이터를 복호화 하게 된다. RTP는 UDP 기반의 프로토콜이며, 수신단에서 수신된 데이터 패킷이 일정한 순서로 전송되었는지 보장할 수 없다. 그러므로 수신단에서는 패킷의 Sequence number를 이용하여 패킷을 재정렬해야만 한다.

RTCP는 스트리밍 서비스를 받는 모든 사용자에게 RTP와 동일한 전달 메커니즘을 이용하여 주기적으로 제어 패킷을 전송하여 세션(session)에 관한 정보를 서로 전달한다. RTCP의 제어 메시지로는 SDES Source DEScription), SR(Sender Report), RR(Receiver Report) 및 BYE(good BYE) 등의 메시지가 있다. SDES는 한 사용자가 회의에 참가할 때 자신의 정보를 다른 모든 참가자에게 보내기 위해 사용된다. SR과 RR은 각각 송신자와 수신자의 상태 정보를 전송하며, 데이터 분배의 품질에 대한 피드백을 제공하는 기능을 수행한다. BYE는 현재의 세션을 종료할 때 사용한다. RTCP는 어플리케이션으로 하여금 서버로부터 데이터를 요청하거나, 멀티미디어 회의에 실시간 연결이 가능하게 한다. UDP와 같이 RTCP도 비 연결지향



〔그림 2〕 RTP/RTCP의 동작 원리

프로토콜이며, 각각의 스트림은 세션 ID에 의해 서로 구별된다.

RTP를 이용한 스트리밍 서비스는 RTP 서버와 클라이언트로 구성된다. RTP 서버는 멀티미디어 컨텐츠를 스트리밍 파일 포맷으로 부호화하고, 하나 이상의 연결된 RTP 세션에 보내진다. 클라이언트는 서버와 연결된 RTP세션으로부터 미디어 스트림을 받아서 패킷을 재정렬하고, 플레이어 및 파일 저장이 가능하게 된다. [그림 2]는 이러한 RTP/RTCP의 동작 원리를 나타낸다.

Ⅲ. 제안된 DRM 시스템의 구성 및 특징

기존의 다운로딩 방식의 DRM 시스템은 CD 복제 소프트웨어, 캡쳐보드 등을 이용한 불법 복제 및 불법 유통을 제어하기에는 많은 문제점을 갖고 있다. 즉, 저작권 보호를 수행하는 장치의 통제권을 벗어난 부분에서 이루어지는 저작권 침해는 현재의 시스템에서 방지하기 어렵다. 특히, 컨텐츠 다운로딩 방식은 사용자의 PC 어딘가에 컨텐츠가 저장된다. 이것은 PC의 하드웨어 접근이 용이한 현 상황에서 저작권 관리의 근원적인 위험이 내포됨을 의미한다.

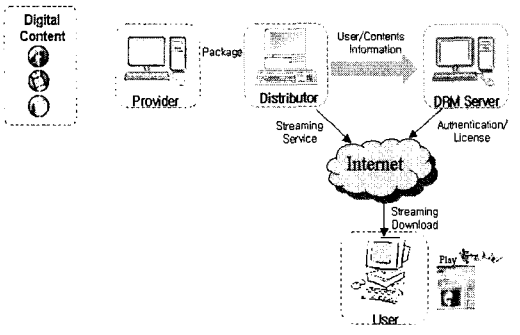
본 논문에서는 컨텐츠 유통 시스템을 그림3과 같이 스트리밍 서비스를 대상으로 구성한다. 컨텐츠 제공자는 실시간 방송, 비디오, 오디오, 교육용 컨텐츠를 서버 모듈에서 암호화한 후, 온라인으로 유통한다. 유통되는 컨텐츠는 DRM 서버에서 사용자 인증 절차를 거친 정당한 사용자에게만 스트리밍 서비스가 이루어진다.

3.1 DRM 서버 구조

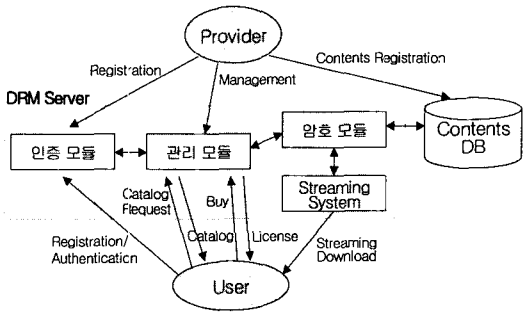
DRM 서버는 컨텐츠의 안전한 유통을 위해 컨텐츠를 암호 알고리즘으로 패키징 하는 암호 모듈과 온라인 상의 각 사용자를 인증하는 인증 모듈, 인증 및 암호와 관련된 정보들을 관리하는 관리 모듈, 그리고, 실시간 스트리밍 서비스가 가능한 스트리밍 모듈로 구분된다. 각 모듈은 독립적이며 상호 연동되어 동작된다. 특히 암호 모듈과 스트리밍 모듈은 계층적 구조로 이루어져 있으며, 사용자의 요구에 의해 컨텐츠를 스트리밍되기 전 단계에서 사용자 정보에 의해 암호 모듈이 동작된다.

제안 DRM 시스템은 두 가지 유형으로 구성될 수 있다. 대형 컨텐츠 제공업자와 같이 컨텐츠 생성, 관리, 유통을 일괄 처리하는 경우, DRM 서버는 [그림 4]와 같이 하나의 시스템 내에 모든 모듈이 포함되어 상호 연동되어 동작될 수 있다. 그리고 소규모의 컨텐츠 제공업자들은 컨텐츠 생성과 유통을 자체 시스템에서 암호 모듈과 스트리밍 모듈로서 제공되고, 컨텐츠 관리 및 라이센스 부여는 독립적인 DRM 시스템으로 제공할 수 있다.

인증 모듈에서는 컨텐츠의 도용을 방지하기 위해 사용자 인증 정보와 사용자의 하드웨어 정보를 함께



〔그림 3〕 제안 DRM 시스템 구성도



〔그림 4〕 DRM 서버 동작 절차

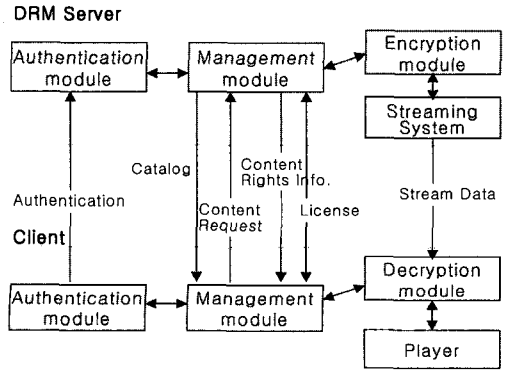
인증 받게 된다. 본 논문에서는 사용자 PC의 MAC 어드레스를 이용하여 사용 가능한 PC를 제한하였다. 그리고 이 정보를 전송되는 패킷에 적용하여 네트워크 상의 불법 사용자로부터 컨텐츠를 안전하게 하였다. 인증된 사용자는 관리 모듈을 통하여 판매자의 모든 컨텐츠 목록과 사용자들의 판매 현황 등을 확인 할 수 있다.[10]

DRM 서버 내의 지불 처리는 DRM 시스템과 독립적인 지불 시스템을 사용한다. 지불 처리 루틴에 의해 구입한 컨텐츠의 비용을 지급하고, 지급된 비용에 대하여 판매자와 저작권자에 대한 비용 분배는 DRM 서버의 관리 모듈에서 이루어진다.

암호 모듈에서는 전송될 스트리밍 패킷에 대하여 사용자 하드웨어 정보를 이용한 Sequence number에 의해 재조합과 대칭키를 이용한 암호화가 이루어진다. 본 논문에서는 128비트 SEED 암호 알고리즘을 이용하였고, 확장성을 고려하여 차세대 표준 암호인 128비트 AES 암호 알고리즘 처리가 가능하도록 구현하였다.

3.2 클라이언트 구조

클라이언트는 스트리밍으로 전송된 컨텐츠를 어플리케이션 영역에서 복호화하고, 플레이어로 실행한다. 클라이언트 장치들은 PC, 셋탑 박스(*set-top* box), 게임 콘솔, PDA, 모바일 폰(mobile phone) 등과 같이 매우 다양하다. 클라이언트는 사용자 단말기에서 동작되므로 DRM 시스템에 손상을 가할 수 있다. 따라서 적절한 보안 레벨을 제공해서 클라이언트 환경을 안전하게 하고, 시스템을 손상시키려는 의도를 어렵게 해야 한다.[11]



〔그림 5〕 클라이언트 구조

제안 DRM 시스템의 클라이언트는 [그림 5]와 같이 구성된다. 임의의 공격자로부터 클라이언트 모듈 내에 저장된 값들을 보호하기 위해 클라이언트 모듈에 저장되는 데이터는 모두 암호화된다. 클라이언트는 DRM 서버와 같이 인증 모듈, 관리 모듈, 암호 모듈 및 스트리밍 전송되어진 컨텐츠를 실행하는 플레이어가 포함된다. 사용자는 실제 DRM 서버로부터 컨텐츠를 실행할 때, 컨텐츠에 대한 사용 규칙을 확인하고, 사용 권한에 대한 라이센스를 획득한다.

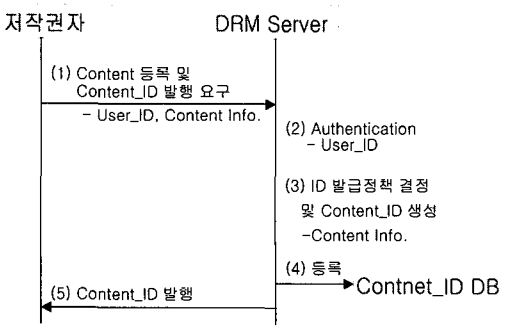
3.3 라이센스(license)

라이센스는 컨텐츠 사용을 위한 컨텐츠 복호키와 사용 규칙 등을 포함한다. 일반적으로 사용자는 컨텐츠를 다운로드 또는 스트리밍 서비스 등을 정당하게 사용하기 위해서 해당 컨텐츠의 사용 권한을 할당받아야 한다. 라이센스 발급은 플레이어 동작 시, 해당 컨텐츠의 라이센스를 확인하고 라이센스가 없거나 기간이 만료된 라이센스를 가지고 있으면 DRM 서버로부터 재발급 받아야 한다.

제안된 시스템의 라이센스는 다음과 같은 정보들로 구성된다. [그림 6]의 절차에 의해 발행된 컨텐츠 식별 ID(Content _ID), 라이센스를 특정 사용자의 컴퓨터에 한정시키기 위한 정보(Binding_info), 해당 컨텐츠에 대한 사용 규칙을 정의한 권한(Rights), 암호화된 패킷을 복호하기 위한 키(Key) 그리고, 앞의 모든 정보에 대한 DRM 서버의 전자 서명값(Certificate $_{License}$)으로 구성되어 있다.

$License$={Content_ID, Binding_info, Key, Rights, $Certificate_{License}$}

Content_ID는 유통되는 컨텐츠의 유일한 저작권



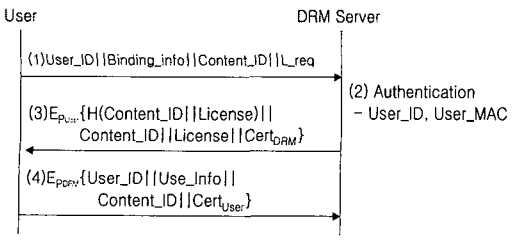
〔그림 6〕 Content_ID 발행절차

코드로 디지털 컨텐츠의 저작권을 명확하게 나타내며, 각 컨텐츠의 공통적인 검색키로 사용될 수 있다. 또한, 바코드와 같이 컨텐츠 분배 기록들을 쉽게 관리할 수 있다.[12,13] Binding_info는 사용자의 특정 장치 ID로 사용자와 그가 이용하는 하드웨어에 바인딩하기 위해 생성된 값을 가진다. 구현된 시스템의 Binding_info는 사용자 PC에 대한 MAC 어드레스와 User_ID의 해쉬 값으로 이루어지고, 이 값은 안전한 스트리밍 서비스를 위해 Sequence number를 재생성하고, 클라이언트에서 다시 재 조합하여 정상적인 스트림 데이터로 변경하는데 이용된다. Rights는 사이트 또는 컨텐츠의 중요도에 따라 다양한 등급으로 적용할 수 있으며, 등급에 따라 컨텐츠의 사용 횟수, 사용 기간, PC의 등록 수 등을 제한 할 수 있다.

Binding_info = H(User_ID||User_MAC)

사용자는 라이센스 획득을 통해 컨텐츠에 대한 정당한 사용 권한을 부여받는다. 클라이언트의 관리 모듈은 사용자가 플레이어를 실행할 때, DRM 서버에 사용정보를 전달하여 컨텐츠 및 라이센스의 불법 사용을 방지한다. [그림 7]은 스트리밍 컨텐츠에 대한 라이센스를 요청하고 획득하는 단계를 나타내고 있다.

(1) 사용자는 카탈로그에서 컨텐츠를 선택하고, 선택된 컨텐츠의 사용 권한을 얻기 위해 DRM 서버에 자신의 ID와 하드웨어 바인딩 정보, 그리고 라이센스를 발급하고자 하는 컨텐츠의 ID와 함께 라이센스 발급을 요청한다.
(2) DRM 서버는 라이센스 발급을 요청한 사용자의 정보를 확인하고, 등록된 User_ID와 User_MAC에 의해 라이센스를 요청한 사용자의 하드웨어를 확인한다.
(3) 사용자 공개키를 이용하여 발급된 라이센스를 암호화하고, 요청한 클라이언트에게 전송한다.
(4) 클라이언트는 전송된 라이센스로부터 정당한 사용 권한을 할당받아 컨텐츠를 실행시키고 그 사용내역(Use_Info)을 다시 서버에게 전송하게 된다.



[그림 7] 라이센스 발급 프로토콜

전송 받은 사용내역은 DRM 서버의 관리 모듈에서 등록, 관리함으로서 라이센스의 불법사용을 방지할 수 있다. 또한 라이센스는 Binding_info에 의해서 다른 PC로 옮겨졌을 때, 컨텐츠에 대한 사용권한을 통제할 수 있다. 컨텐츠의 off-line 분배 시, 사용자들은 DRM 서버로부터 라이센스 발급 절차를 통해 컨텐츠의 사용 권한을 획득할 수 있다.

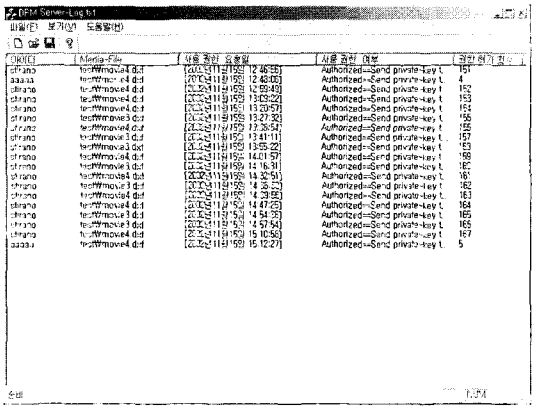
Ⅳ. 시스템 구현 및 분석

4.1 시스템 구현

본 논문에서 구현된 DRM 시스템은 크게 서버와 클라이언트로 구성된다. 서버와 클라이언트의 각 모듈들은 C언어로 구현하였다. DRM 서버의 운영체제로는 Windows 2000 Server 환경에서 MY-SQL을 사용하고, 클라이언트는 Windows 2000 Professional 환경에서 구현하였다.

[그림 8]은 구현된 DRM 서버 화면을 나타낸다. DRM 서버는 인증된 사용자에 대한 컨텐츠의 사용 권한을 관리한다. 구입한 컨텐츠에 대하여 사용자 권한 여부와 사용 횟수를 주기적으로 관리함으로써 저작권 관리 및 불법 유통을 방지할 수 있다. 인증된 사용자가 컨텐츠에 대한 접근을 시도할 때, 서버의 관리 모듈은 라이센스 검증 및 사용 횟수를 증가시켜 부정한 조작을 방지한다.

클라이언트가 식별되어지면 서버는 암호 모듈을 통하여 패킷을 암호화하고, 패킷 헤더의 Sequence number를 Binding_info에 의해 변경시킨 뒤, 스트리밍 시스템으로 전송되어진다. Binding_info에 의한 Sequence number 변경은 패킷 전송에는 아무런 영향을 미치지 않는다. 다만, 수신측의 클라이언트에서 식별된 사용자의 User_ID와 클라이언트 모듈의 MAC 어드레스를 이용하여 처음 상태의 Sequence number로 복구하는 과정이 추가된다. 전송되는 RTP 패킷은 변경된 Sequence number에 의해 스크램블 되어 인가되지 않은 사용자에 의한 불법수신을 제한한다. 또한, 악의적인 공격자에 대한 안전성을 보장하기 위해 네트워크 상에 전송되는 패킷은 128 비트 대칭키 암호



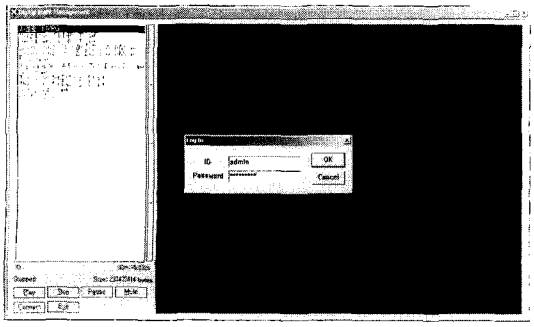
〔그림 8〕 컨텐츠에 대한 사용권한을 관리하는 DRM Server 화면

화하여 패킷을 전송한다.

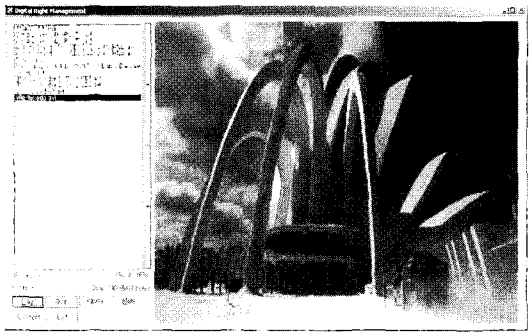
구현된 DRM 시스템은 사용자 및 클라이언트의 MAC 어드레스를 식별하고, 식별된 장치 내에서 스트리밍 컨텐츠에 대한 실행 권한을 부여받는다. 실행 권한은 라이센스에 명시되어 있으며, 정당한 라이센스 발급을 통하여 스트리밍 컨텐츠에 대한 접근 권한을 가지게 된다. 따라서 기존의 다운로딩 방식의 DRM 시스템이 가지는 컨텐츠 및 라이센스의 부정 복제를 방지함으로써 보다 안전한 컨텐츠 유통 구조를 만들 수 있다.

[그림 9]는 데스크탑 환경의 클라이언트에서 DRM 서버에 접속하기 위한 인증 과정을 나타낸다. 클라이언트의 인증 모듈은 서버로부터 정당한 사용자를 확인하고, 등록된 정보에 의해 Binding_info를 생성하여 하드웨어를 확인한다.

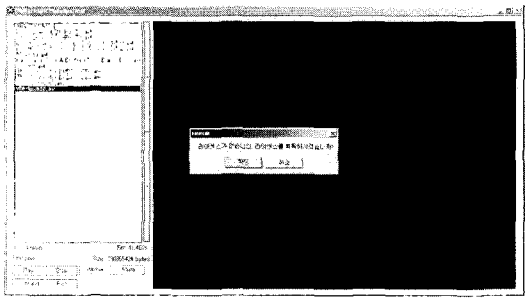
사용 권한이 확인된 컨텐츠는 스트리밍 데이터로 전송되어 실행된다. [그림 10]은 구현된 DRM 클라이언트로서 전용 플레이어 형식의 클라이언트 모듈이다. 스트리밍 데이터 실행 시, 사용자의 하드웨어 정



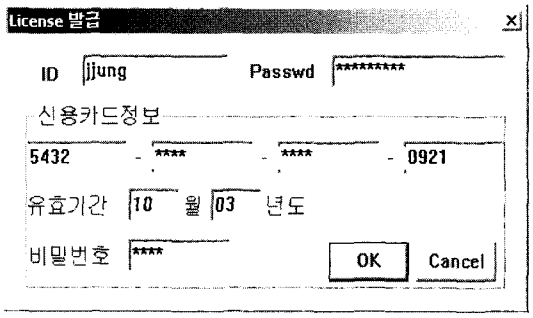
〔그림 9〕 사용자 인증 화면



〔그림 10〕 구현된 Player 실행 화면



〔그림 11〕 라이센스에 의한 접근 거부 화면



〔그림 12〕 라이센스 발급 요청 화면

보를 호출하여, 전송된 패킷 헤더의 Sequence number를 재구성한다. 재구성된 Sequence number는 전송된 스트림 데이터를 정확한 순서로 재구성해서 실행 가능한 스트림으로 변경하게 된다.

컨텐츠에 대한 사용 권한을 가지지 않은 사용자가 컨텐츠에 접근하면 클라이언트는 [그림 11]과 같이 에러 메시지를 띄우고 모든 접근 시도를 중단시킨다. 모든 실행이 중단되면 [그림 12]와 같이 클라이언트의 관리 모듈에서 사용 권한 획득을 위해 대상 컨텐츠의 라이센스 발급을 요청하게 된다. 사용자는 컨텐츠에 대한 정당한 지불 절차를 거친 뒤에 비로소 컨텐츠에 대한 접근 권한을 부여받게 된다.

정상적인 절차를 거치지 않고 부정한 방법으로 컨텐츠를 획득하였을 때, 그 컨텐츠는 블록 암호화와 패킷 재구성에 의해 랜덤한 비트열의 정보만 얻게 된다. 또한, 라이센스의 도용 시, 등록된 하드웨어 정보에 의한 비트열의 재구성이 불가능하므로 정상적인 컨텐츠를 획득할 수 없게 된다.

4.2 시스템 분석

스트리밍을 위한 DRM 시스템의 설계 및 구현을 통하여 기존의 다운로드 방식의 DRM 시스템이 가지는 복제 소프트웨어, 캡쳐보드 등을 이용한 불법 복제 방지의 어려움과 유통 중인 컨텐츠에 대한 지속적인 저작권 관리 문제의 어려움 등을 해결 할 수 있음을 보였다. [표 1]은 제안된 DRM 시스템과 기존의 DRM 시스템과의 비교를 나타낸다.[14]

기존의 DRM 시스템은 주로 암호화와 워터마킹 기술을 활용하여 감시 및 추적 기능을 제공하지만 제한적인 저작권 관리만이 가능하다. 그러나 다양한 컨텐츠 저작과 유통을 위해 저작물에 대한 접근 제어 기술, 실시간 감시 및 추적 기술, 컨텐츠 스트리밍 기술 등을 필요로 한다. 본 논문은 스트리밍 다운로딩 기술을 기반으로 하고, 디지털 컨텐츠 유통 과정에서 암호화 기술과 전자서명 기술을 활용하여 안전성 및 보안성을 제공한다. 또한, DRM 서버에서 컨텐츠 이용 시 실시간 감시와 추적이 가능하도록 구성하여 다양한 컨텐츠 산업에 적용 가능하다.

V. 결 론

본 논문에서는 스트리밍 서비스를 기반으로 한 DRM 시스템을 설계 및 구현하였다. 구현된 시스템은 크게 서버와 클라이언트로 구성되며, 허가된 사용자의 특정 하드웨어 장치에서 컨텐츠 접근이 가능하도록 하였다. 이를 위해, 사용자 인증 단계에서 개인 식별과 함께 하드웨어 장치에 대한 식별을 포함한다. 또한, 라이센스 내에 이러한 정보를 포함하여 불법적인 라이센스 도용 및 컨텐츠의 불법 복제를 방지하였다. 구현된 DRM 시스템은 주기적으로 컨텐츠와 라이센스를 관리함으로써 유통업체 및 저작권자의 저작권 관리 및 불법유통 감시, 수익 구조 개선이 가능할 것이다.

구현된 시스템은 초기 등록 단계에서 사용자 정보 및 하드웨어 정보가 안전한 채널을 통하여 서버에 전달되었음을 가정한다. 이후, 사용자 인증은 개인 ID 및 사용자 하드웨어의 고유 정보만으로 간단하게 인증할 수 있다. 또한, 네트워크 상의 전송 패킷은 인증된 사용자에 바인딩되므로 유통되는 컨텐츠에

〔표 1〕 DRM 시스템의 비교

	MicroSoft	Adobe	ContentGuard	제안한 DRM 시스템
라이센스에 대한 보안	· 다른 PC로 복제 방지 · 기간/횟수 조작방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작방지 · Tampering 방지
Super Distribution	지원	미지원	미지원	지원(스트리밍 데이터에 대한 다운로드 서비스시)
암호화된 컨텐츠 구성	암호화 + 메타정보(URL)	암호화 + 라이센스	암호화 + 라이센스	암호화 + 라이센스
암호화 키 관리	서버 + 암호화된 컨텐츠 파일 내 속성	서버	별도파일(Rights-Label)	서버
복호화 키 관리	라이센스 내에 포함	라이센스 내에 포함	라이센스 내에 포함	라이센스 내에 포함
메타데이터 저장 위치	암호화된 컨텐츠 파일 내 속성	라이센스 내에 포함(암호화된 컨텐츠와 독립)	라이센스 내에 포함(암호화된 컨텐츠와 독립)	라이센스 내에 포함(암호화된 컨텐츠와 독립)
라이센스 관리	· 한 파일로 관리 · plain text · key 만 암호화	· 한 파일로 관리 · plain text · key 만 암호화	· 라이센스마다 다른 파일 · plain text · key 만 암호화	· 라이센스마다 다른 파일 · plain text · key 만 암호화 · 전자서명 데이터 이용
서비스 방법	다운로딩	다운로딩	다운로딩	스트리밍 + 다운로딩
지원 타입	Audio, Video	PDF, EBX	HTML, XML, ASCII, PDF, MS Office 등	Multimedia contents

대한 불법 복사 및 도용을 억제할 수 있다. 또한, 현재 많은 개발이 이루어지고 있는 디지털 방송과 같은 실시간 컨텐츠 서비스 등에 DRM 시스템이 저작권 보호 및 안전한 유통을 위해 활용될 수 있을 것이다. 향후, 본 시스템은 PDA와 모바일 폰 등에 적합한 모듈 설계 및 Kernel 레벨에서 컨텐츠에 대한 라이센스 관리 등의 개발이 이루어져야 할 것이다.

참 고 문 헌

[1] Joshua Duhl, Susan Devorkian, "Understanding DRM Systems", IDC White Paper, 2001, http://www.intertrust.com/main/research/whitepapers/IDCUnderstandingDRMSystems.pdf.

[2] F. Hartung, F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-commerce Applications" IEEE Com. Magazine, Vol. 38, pp.78~84, Nov. 2000.

[3] http://www.doi.org

[4] http://www.xrml.org

[5] 박성준, 이인수, 박형선, 김병천, 김승주, "128비트 블록 암호알고리즘 표준", 한국정보통신기술협회, 1999.

[6] NIST, "Announcing the Advanced Encryption Standard(AES)", FIPS Publication 197, 2001.

[7] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, pp.1673~1687, 1997.

[8] Nokia Connecting People, Digital Rights Management and Superdistribution of Mobile Content, Nokia White Paper, 2001.

[9] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", Network Working Group Request for Comments 1889, Jan. 1996.

[10] Park. Jaehong, Ravi Sandhu, "Towards Usage Control Models: Beyond Traditional Access Control", Proc. of the 7th ACM Symposium on Access Control Models and Technologies, 2002.

[11] William Shapiro, Radek Vingralek, "How to Manage Persistent State in DRM Systems", Proc. of the ACM Workshop on Security and Privacy in Digital Rights Management, Nov. 2001.

[12] The Content ID Forum, "CIDF Specification Ver. 1.0", May, 2000.

[13] ISO/IEC JTC1/SC29/WG11, M6953, Digital Item Identification and Description based on Content ID Technology, March, 2001.

[14] DRM 포럼 운영, 정보통신표준화전략포럼 최종 연구보고서, Dec, 2002.

〈著者紹介〉

이 진 흥 (Jin-heung Lee)
1998년 2월 : 동서대학교 정보통신공학과 졸업
2000년 2월 : 부경대학교 전자계산학과 석사
2000년 7월~2001년 9월 : (주)실트로닉테크놀로지 팀장
2002년 3월~현재 : 부경대학교 대학원 정보보호학과 박사과정
<관심분야> DRM(Digital Rights Management), 저작권보호, 정보보호 및 암호학

김 태 정 (Tea-jung Kim)
1999년 2월 : 경성대학교 컴퓨터공학과 졸업
1999년 12월~현재 : 한국정보통신교육원 강사
2002년 3월~현재 : 부경대학교 대학원 정보보호학과 석사과정
<관심분야> 데이터베이스, 정보보호 및 암호학

박 지 환 (Ji-hwan Park) 정회원
1984년 2월 : 경희대학교 전자공학과 졸업(공학사)
1987년 3월 : 일본 국립전기통신대학 정보공학과 졸업(공학석사)
1990년 3월 : 일본 요코하마국립대학 전자정보공학과 졸업(공학박사)
1996년 4월~현재 : 동경대학 생산기술연구소 협력연구원
1990년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 교수
1997년 3월~현재 : 한국정보보호학회 이사
2002년 3월~현재 : 한국정보보호학회 영남지부장 및 논문지 편집위원
1998년 12월~현재 : 한국멀티미디어학회 운영위원 논문지 편집위원
1999년 3월~현재 : 한국정보처리학회 논문지 편집위원
<관심분야> 멀티미디어 컨텐츠 보호 및 응용, 암호학