碩士學位請求論文

디지털 콘텐츠의 안전한 유통을 위한 DRM 시스템의 연구

濟州大學校 大學院

電氣電子工學科

梁 東 赫

2006年 12月

디지털 콘텐츠의 안전한 유통을 위한 DRM 시스템의 연구

指導敎授　都 良 會

梁 東 赫

이 論文을 工學 碩士學位 論文으로 提出함

2006年 12月

梁東赫의 工學 碩士學位 論文을 認准함

審査委員長＿＿＿＿＿＿＿＿印

委　　員＿＿＿＿＿＿＿＿印

委　　員＿＿＿＿＿＿＿＿印

濟州大學校 大學院

2006 年　12 月

A Study on Digital Rights Management System for safety Distributions of Digital Contents

Dong-Hyuk Yang

(Supervised by professor Yang-Hoi Doh)

A thesis submitted in partial fulfillment of the requirement for the degree of Master of Engineering

2006. 12.

This thesis has been examined and approved.

Thesis director, Sung-taek Ko, Prof. of Elec. Eng.

Thesis director, Jeong-woo Jwa, Prof. of Telecom. Eng.

Thesis director, Yang-hoi Doh, Prof. of Elec. Eng.

(Name and signature)

2006. 12. 12

Date

DEPARTMENT OF ELECTRONICS ENGINEERING
GRADUATE SCHOOL
CHEJU NATIONAL UNIVERSITY

목 차

Abbreviations

3GPP	3rd Generation Partnership Project
CEK	Content Encryption Key
DCF	DRM Content Format
DRM	Digital Rights Management
ISO	International Organization for Standardization
LAN	Local Area Network
MMS	Multimedia Messaging Service
MPEG	Motion Picture Expert Group
MP3	MPEG audio layer 3;
OMA	Open Mobile Alliance
OS	Operating System
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
REL	Rights Expression Language
REK	Rights Encryption Key
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
SMS	Short Messaging Service
UI	User Interface
URI	Uniform Resource Indicator
XML	eXtensible Markup Language

Definitions

Combined Delivery	DRM 콘텐츠를 전달하기 위한 방법으로 전달되는 콘텐츠 안에 사용권한 객체가 포함되어 있는 형태
Content	하나 이상의 미디어 객체들을 의미
Content Issuer	DRM 콘텐츠를 공급하는 공급기
Content Provider	콘텐츠 발급기와 권한 발급기를 보유하여 콘텐츠와 권한을 발급하는 공급자
Device	DRM Agent를 통하여 DRM으로 보호되는 콘텐츠를 재생할 수 있는 하드웨어나 소프트웨어
Domain	권한 발급기(RI)에 의해 정이된 장치나 사용자의 그룹
DRM Agent	Device에서 미디어 객체와 사용권한 객체의 사용과 유지 보수 및 관리를 담당하는 요소
DRM Message	사용권한 객체와 미디어 객체가 담겨있는 메시지
Forward Lock	수신자는 미디어 객체를 수신 받은 장치에서만 사용이 가능하고, 다른 장치로 전달이 불가능한 전송방법
Media Object	디지털로 작업된 콘텐츠 객체
DRM Content	DRM으로 보호되는 콘텐츠. 보안공격으로부터 보호를 위해 암호화 과정을 거쳐 사용자에게 전달
Rights Issuer	사용권한 발급기
Rights Object	DRM 콘텐츠를 사용하기 위한 사용 권한, 규칙, 암호화 키 등이 담겨 있는 객체
Separate Delivery	암호화된 미디어 객체와 그에 필요한 사용권한이 다른 경로로 전달되는 전송 방법. 암호화된 미디어 객체는 여러 가지 방법으로 전달될 수 있으나, 사용권한은 오로지 콘텐츠 공급자만 발급할 수 있다.
Superdistribution	Separate Delivery를 이용하여 암호화된 미디어 객체는 사용자에 의해 복사 및 전달이 가능한 형태로 폭발적인 유포를 유도하고, 사용권한의 발급은 콘텐츠 공급자가 제어하는 DRM의 특징적인 콘텐츠 배포방법.
User	DRM 콘텐츠를 이용하는 사용자

Summary

A Digital Rights Management (DRM) system has a reproduction control (copy control) function doing functional encryption (encryption) fixed user who encrypts copyright of digital contents for the purpose of protection so as not to be able to know contents of contents only so that functional, access restriction permitting (conditional access) cannot reproduce illegally access and identification and a tracing (identification & tracing) function chase the contents reproduced when contents were reproduced, and to confirm. The existing DRM system tends to limit convenience or flexible business model because DRM system emphasizes protecting content. This is causing inconvenience on user using DRM contents.

This paper presents three types of DRM systems. The first is the DRM system that it is possible for especially support flexible business model through re-issue Rights Object (RO), and the second is the DRM system that can protect copyright about user manufacture contents, the last is the DRM systems that application is possible to Multimedia Messaging Service (MMS). A user makes various free use possible compare with the existing DRM system to use DRM contents through suggested DRM systems, and make copyright protection possible about own direct contents that made. In entrances of contents supplier do compare with the existing DRM so as to be able to establish price policy of more various forms or a sales policy, and can expect so that acceleration to apply DRM at multimedia contents of further a lot of forms through this becomes. Finally, copyright protection about the contents which contents supplier provides to MMS becomes possible, and to develop to MMS of various forms will contribute.

Ⅰ. 서론

21세기 정보화 사회의 급속한 발전으로 예전의 아날로그화 된 콘텐츠들이 급속히 디지털화된 콘텐츠로 전환되었다. 또한 인터넷의 힘을 빌려 디지털 콘텐츠는 빠른 속도로 전파되고 이용되고 있다. 이러한 디지털 콘텐츠는 원본과 사본이 완전하게 동일하고, 사용자가 임의로 재편집이 가능하며, 해당 콘텐츠를 다른 사용자에게 전달하고 사용하는데 아무런 제한이 없다. 또한 네트워크 기술의 발달과 인터넷 전송속도의 향상으로 인하여 인터넷을 통한 정보의 공유가 확산됨에 따라 디지털 콘텐츠의 저작권 및 라이선스를 무시한 채 디지털 콘텐츠들이 무분별하게 불법 유포되고 있다. 이러한 디지털 콘텐츠의 저작권 보호를 위해 디지털 저작권 보호기술(Digital Rights Management, 이하 DRM)이 나타나게 되었다[1]. 기존 아날로그 콘텐츠에서 사용되었던 콘텐츠의 저작권 보호 방법에는 두 가지가 있다. 하나는 유통되는 모든 콘텐츠에 복사방지 장치를 만드는 것이고, 다른 하나는 콘텐츠에 특정한 코드나 유형 등을 삽입하여 콘텐츠의 소유자가 누구인지 명시한 후 유통하는 방법이다. 전자를 복제 방지 기술, 후자를 워터마킹이라고 부른다. 복제 방지 기술은 유통되는 콘텐츠가 많아질수록 해당 기술을 적용하는데 비용이 추가될 수 있고, 이 기술에 사용된 방법이 유출되거나 해킹 등에 의해 깨어지게 되면 저작권 보호가 불가능해진다는 단점이 있다. 이에 비하여 주로 영상이나 이미지에 주로 적용되는 워터마킹은 사용자가 콘텐츠를 사용하는 데는 전혀 지장을 주지 않으면서도 원본의 출처나 복제 경로를 찾아내는 데는 아주 효과적이다. 하지만 이 기술은 특정 디지털 콘텐츠에서만 적용이 되며 수많은 개인 사용자들의 불법적인 콘텐츠 사용을 모두 방지하지 못하는 단점이 있다. 무엇보다 아날로그 콘텐츠가 디지털 콘텐츠로 바뀌게 되면서, 워터마킹 또한 해킹으로부터 안전하지 못하게 되었다. 아날로그 시대에서 디지털 시대로 넘어오면서 기존 복제 방지 기술이나 워터마킹이 가지는 문제점들을 해결하기 위하여 수많은 연구자들이 노력하고 있지만, 이 기술만으로는 지금의 수많은 종류와 다양한 형태의 디지털 콘텐츠를 전부 보호할 수는 없는 약점을 가지고 있다. 무엇보다 최근 인터넷을 통해

블로그와 개인 홈페이지에서 확산되고 있는 사용자 제작 콘텐츠(User Created Contents, 이하 UCC)는 개인 사용자들이 복제 방지 기술이나 워터마킹을 직접 적용하기에는 시간과 비용, 그리고 기술적적인 측면에서 불가능한 경우가 많다. 이러한 수많은 종류와 형태의 디지털 콘텐츠의 저작권을 안전하게 보호하기 위해서는 콘텐츠의 내용을 알 수 없게 암호화하는 암호화(Encryption) 기능과 정해진 사용자만 접근을 허가하는 접근제한(Conditional Access) 기능, 불법적으로 복제를 하지 못하게 하는 복제 제어(Copy Control) 기능, 그리고 콘텐츠가 복제되었을 때 그 복제된 콘텐츠를 추적하고 확인하는 식별 및 추적(Identification & Tracing) 기능이 필요하다[2]. 이런 요구를 모두 충족시키면서 디지털 콘텐츠의 저작권을 보호할 수 있는 기술이 바로 DRM이다. 일반적으로 DRM은 디지털 콘텐츠에 암호화 기술을 적용하여 적법한 사용자만이 해당 디지털 콘텐츠를 사용하게 함으로써 콘텐츠 저작권 관련 당사자의 권리와 이익을 지속적으로 보호하고 관리하는 기술을 말한다. DRM으로 보호되는 디지털 콘텐츠는 먼저 저작권자가 지정한 절차에 의한 패키징 과정을 거쳐 암호화된 콘텐츠로 변환이 되서 배포가 된다. 배포된 암호화된 콘텐츠를 이용하고자 하는 사용자는 DRM에 의해 지정된 절차를 만족해야만 이를 사용할 수 있다. 현재 DRM은 수많은 기관과 단체에서 표준 규격을 연구하고 있거나 이미 개발하여 사용되고 있으며, 그 중에서도 본 논문에서는 Open Mobile Alliance(OMA)에서 연구한 표준 규격을 준수하는 DRM을 연구하였다. OMA에서 연구하고 있는 DRM은 OMA Digital Rights Management V2.0까지 Release되어 있다[3]. OMA DRM 표준에서는 원본 콘텐츠를 패키징을 통해 DRM으로 보호되는 콘텐츠(DRM Content Format, 이하 DCF)로 변환하여 악의적인 공격으로부터 콘텐츠를 보호하는 방법[4], 여러 가지 경로를 통하여 사용자에게 배포되는 DCF를 사용하기 위해서 사용자는 콘텐츠 공급자로부터 사용권한 객체(Rights Object, 이하 RO)를 발급하는 방법[5], RO에 사용 규칙(Usage Rule)을 명세하는 방법[6]을 통해 콘텐츠의 암호화하여 배포하고 사용자의 사용제어를 통해 배포되는 콘텐츠의 저작권을 보호한다. 여기에서 살펴보면, OMA DRM 표준에서는 콘텐츠를 암호화하여 배포하는 방법과, 배포된 콘텐츠의 사용을 위해 사용권한 객체의 발급을 통한 콘텐츠의 사용 제어가 핵심이 된다. 이는 기존 아날로그 콘텐츠에 있어서 콘텐츠를 구입한 사람은 적법한 범위 내에서 자유

롭게 콘텐츠를 사용할 수 있었지만, DRM으로 보호되는 콘텐츠에 있어서 콘텐츠 공급자는 사용자가 콘텐츠를 어떻게 사용할 수 있는지에 대해서도 제한을 둘 수가 있다는 것을 의미한다. 즉, OMA DRM에서는 DRM으로 보호되는 암호화된 콘텐츠의 배포는 모든 경우에 있어서 자유롭게 허용이 되지만, 암호화된 콘텐츠를 사용하기 위한 사용권한은 오로지 콘텐츠 공급자만이 발급 가능하도록 되어 있다. 콘텐츠 공급자 관점에서 보면, DRM은 콘텐츠 사용 제어 측면에서 강력한 통제력을 갖게 된다. 하지만, 많은 사용자들은 콘텐츠를 사용하는데 있어서 '콘텐츠 사용권'을 구입하는 것보다는 '콘텐츠 자체'를 구입하는 것을 원한다. 완전한 '콘텐츠에 대한 사용 권리'가 포함된 콘텐츠를 구입하여 자기 소유의 다른 장치들을 통해 콘텐츠를 공유하려 하고 자신의 친구들에게 자신의 구입한 콘텐츠를 자랑하거나 선물하고 싶어 한다. 현재의 OMA DRM 시스템에서 이 문제를 해결하기 위해서는 사용자들이 사용권한에 발급에 관여를 하여, 그들의 원하는 대로 '콘텐츠 자체'인 '사용권한'을 다른 장치나 사람들에게 전달이 가능하도록 콘텐츠 공급자의 사용권한에 대한 통제력을 약화시키던지, 이러한 사용자의 모든 요청을 콘텐츠 공급자가 처리를 해야만 할 것이다. 하지만 콘텐츠의 안전한 보호를 위해서는 이러한 요청은 실현되기가 힘들다. 사용권한에 발급에 대한 사용자의 간섭은 사용권한의 유출이나 악용에 심각한 문제를 가져올 수가 있기 때문이다. DRM은 사용자의 편의를 위한 것이기 보단, 저작권 보호를 위한 측면이 강조되어 사용자의 편의를 어느 정도 침범하는 것이 사실이다. 하지만, 사용하기 불편한 DRM은 사용자들로부터 외면당하여, 결국 가치는 있으나 사용되지 않는 기술로 전락되기 마련이다.

본 논문에서는 OMA DRM 시스템을 기반으로 하여, 사용자와 사용자 사이에서 DRM으로 보호되는 콘텐츠와 그에 대한 사용권한을 좀 더 자유롭게 전달할 수 있는 DRM 시스템을 제안한다. DRM을 저작권 보호의 측면에서 보다 디지털 콘텐츠 유통을 위한 저작권 보호 시스템의 측면에서, 융통성 있게 사용권한의 발급과 분배를 해결하고자 한다. 또한 디지털 콘텐츠의 적극적인 마케팅을 위하여 사용자가 유통과정에 직접 참여할 수 있는 DRM 시스템을 연구하였다. 더 나아가, 사용자가 DRM 시스템에 있어서 단순한 사용자로서 콘텐츠를 사용하는 것이 아닌, 사용자가 직접 DRM 시스템이 주체가 되어 사용자 제작 콘텐츠에 대한 저작

권 보호가 가능하도록 연구하였다. 마지막으로 멀티미디어 메시징 서비스(Multimedia Messaging Service, 이하 MMS)를 통해 첨부되어 전송되는 멀티미디어 콘텐츠에 대해서 저작권 보호를 하기 위해 MMS를 위한 DRM 시스템을 연구하였다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 DRM에 대한 시스템 구조와 필요 요소들을 기술하였고, 본 본문에서 제안하는 DRM 시스템을 설계할 때 고려한 사항에 대해서 기술한다. Ⅲ장에서는 기존 DRM 시스템이 가지고 있는 RO의 재발급에 대한 문제를 해결하는 DRM 시스템과 사용자 제작 콘텐츠를 위한 DRM 시스템, 그리고 MMS에 첨부되는 멀티미디어 콘텐츠의 저작권을 보호할 수 있는 DRM 시스템에 대하여 기술한다. Ⅳ장에서는 제안된 DRM 시스템과 OMA DRM 시스템과의 성능을 Use Case 분석을 통해 비교·평가하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

본 절에서는 Open Mobile Alliance에서 표준 규격으로 연구 중인 OMA Digital Rights Management V2.0 Approved Enabler를 기반으로 DRM 시스템의 구조와 해당 시스템 구조에서 발생할 수 있는 문제에 대해서 설명한다.

1. OMA Digital Rights Management

OMA DRM에서는 원본 콘텐츠의 암호화와 사용 규칙을 통한 사용제어라는 2가지 방법으로 콘텐츠의 저작권을 보호한다. 원본 콘텐츠를 암호화하기 위해서 DRM으로 보호되는 콘텐츠 포맷(DRM Content Format, 이하 DCF)으로 패키징하는 과정이 필요하며, OMA DRM Content Format v2.0에서 이를 정의하고 있다. 패키징을 통해 변환된 DCF는 누구나 콘텐츠를 자유롭게 배포를 하거나 복제할 수 있는 Super-Distribution이라는 유통 방법을 통하여 콘텐츠 공급자에서 사용자에게로 전달이 된다. 사용자는 DCF를 사용하기 위해서 먼저 DCF를 해석하여 원래의 콘텐츠로 변환을 시켜야 할 필요가 있다. 이 복호화 과정에서 필요한 콘텐츠 암호화 키(Contents Encryption Key, 이하 CEK)는 사용권한 객체(Rights Object, 이하 RO)로서 콘텐츠 공급자로부터 발급받아 사용하게 된다. 사용자가 콘텐츠 공급자로부터 RO를 발급받기 위해서는 사용자의 식별자, 발급을 원하는 DCF의 식별자, 사용자에 대한 인증 등 여러 가지 종류의 사용자 정보를 콘텐츠 공급자로 전달되어야 한다. 또한 개인 사용자인지, 단체 사용자들 혹은 장치들인지에 따라 다른 형태의 RO가 발급되어야 한다. 이러한 RO의 발급방법과 사용자 그룹(Domain)에 대한 내용을 OMA DRM Specification v2.0에서 정의하고 있다. 요약하자면, OMA DRM 시스템을 구성하고 있는 주요한 요소는 콘텐츠의 암호화를 담당하는 DRM Packager, RO의 발급을 담당하는 DRM Server, 사용자측에서 DCF와 RO를 제어하고 관리하는 DRM Agent이다. DRM Packager란 CEK를 생

성하여 원본 콘텐츠를 DCF로 변환하고 CEK를 한 번 더 암호화 하여 Rights Encryption Key(REK)를 만드는 요소이다, DRM Server는 사용권한 발급기(Rights Issuer, 이하 RI)를 통하여 CEK와 REK, 그리고 사용 규칙(Usage Rule)이 명세된 RO를 사용자에게 발급하기 위한 요소이다. 마지막으로 DRM Agent는RO에 담긴 CEK와 REK로 DCF를 해석하고, 동시에 RO에 명세된 사용 규칙에 의거하여 사용자가 DCF를 사용하는 것을 제어하고 관리하는 요소이다. 아래의 fig. 1은 OMA DRM의 시스템 구조와 구성 요소들을 보여준다.

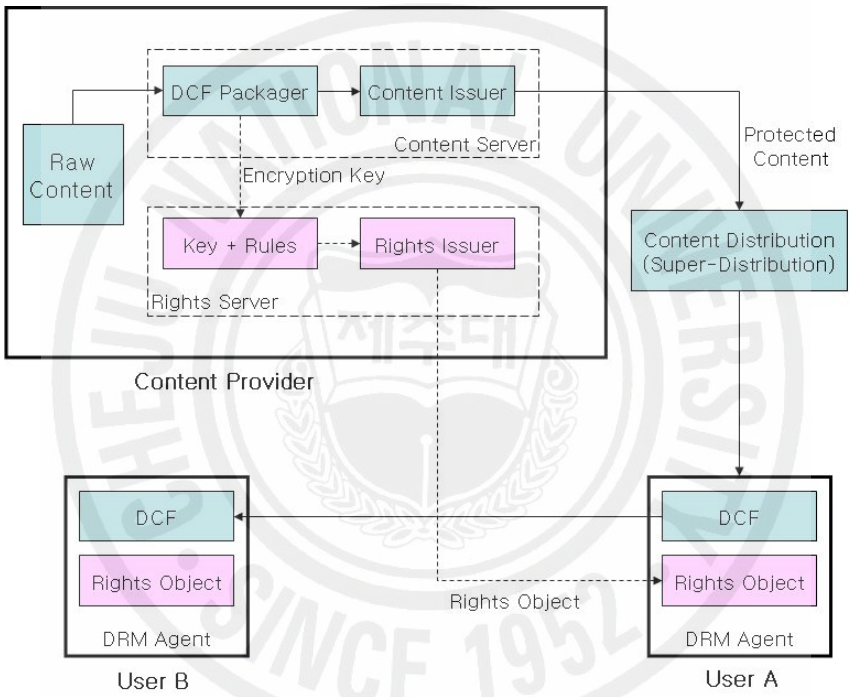

Figure 1. System Architecture of OMA DRM

OMA DRM의 시스템 구조에서 표현된 각각의 요소는 다음과 같다.

1) Raw Content : 원본 콘텐츠

2) Content Provider : 콘텐츠 공급자. 저작자로부터 콘텐츠의 저작권을 위임받아 콘텐츠 공급과 판매를 담당. 원본 콘텐츠를 암호화 하는 DCF Packager와, RO를 발급하는 RI 보유

3) Super-Distribution : 암호화된 콘텐츠인 DCF의 복사와 배포는 자유롭게 가능하고, 사용자가 이 DCF를 사용하기 위해서 콘텐츠 공급자로부터 RO를 발급받아서 사용하게 되는 콘텐츠 유통/배포 방식

4) User : DCF와 RO를 다운로드 받아 후, Agent를 통하여 CEK를 추출하고 RO에 명세된 사용 규칙에 따라 콘텐츠를 사용

OMA DRM 시스템에서는 다음 fig. 2에 보이는 순서로 콘텐츠 공급자가 원본 콘텐츠를 암호화한 후 DCF 형태로 패키징한 후 배포를 하고, 사용자는 DRM Agent의 관리 하에서 다운로드 받은 DCF와 RO를 이용하여 콘텐츠를 사용하게 된다.

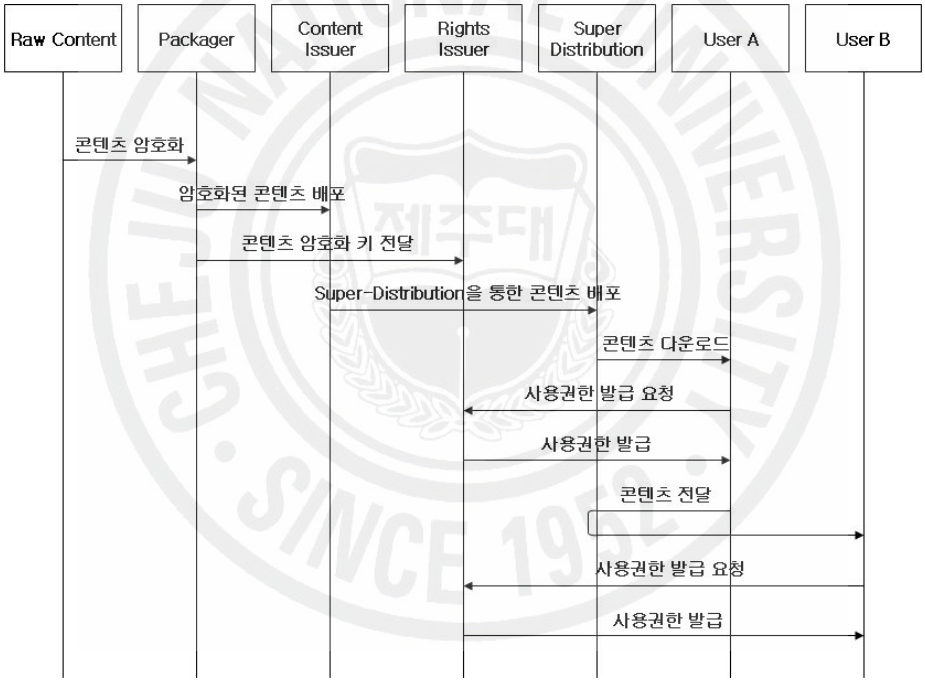

Figure 2. Event Flow Diagram

1) 콘텐츠 저작자는 콘텐츠 공급자에게 원본 콘텐츠를 전달

2) 콘텐츠 공급자는 원본 콘텐츠를 패키징하여 DCF로 변환

3) 패키징 과정에서 생성한 CEK와 원본 콘텐츠에 대한 정보가 RI로 전달

4) DCF로 변형된 멀티미디어 콘텐츠는 사용자들에게 Super-Distribution을 통

해 자유롭게 배포

5) DCF를 다운로드한 사용자는 콘텐츠를 사용하기 위해 콘텐츠 공급자에게 RO를 요청

6) RI는 CEK와 사용 규칙을 명세한 RO를 사용자에게 발급 및 전달

7) 사용자는 DRM Agent를 통해 RO에 담긴 CEK로 DCF를 해독하고 사용 규칙에 의거하여 콘텐츠를 사용

2. OMA DRM Contents Format

OMA DRM의 DCF는 원본 콘텐츠를 안전하게 보호하기 위하여 콘텐츠 정보(콘텐츠 이름, 콘텐츠 경로, 콘텐츠 타입, 콘텐츠 ID, RI 경로, 암호화 방법 등)가 저장된 DCF Header에 AES-128 알고리즘을 이용한 암호화 과정을 거친 원본 콘텐츠 객체가 있는 DCF Body를 삽입하여 생성된다. DCF 패키징 과정 중에 만들어진 CEK와 REK는 DRM Server의 RI로 전달되어 사용자의 RO 발급 요청 시 CEK와 REK가 RO에 포함되어 사용자에게로 전달이 된다. OMA DRM의 DCF 구조는 아래 fig 3.과 같은 형태로 구성되어 있다.

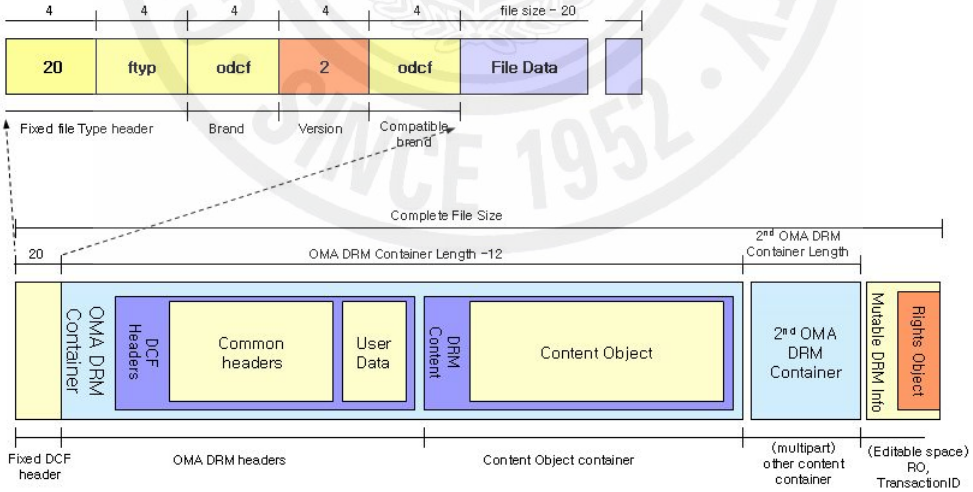

Figure 3. DCF Structure

3. OMA Rights Expression Language

OMA DRM에서 DCF를 사용하는데 필요한 RO는 XML(eXtensible Markup Language)을 기반으로 한 REL(Rights Expression Language)로 표현된다. REL은 Foundation Model, Context Model, Agreement Model, Inheritance Model, Security Model, Permission Model, Constraint Model의 7가지 Model로 구성되어 있다. OMA REL의 구조는 다음 fig. 4에 보인다.

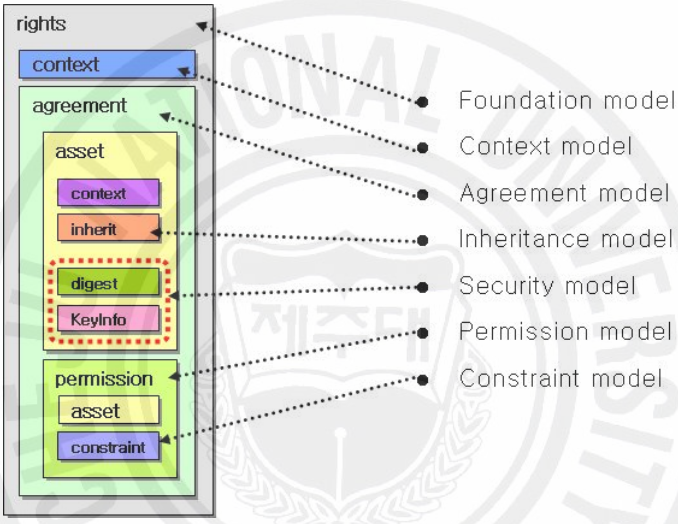

Figure 4. REL Structure

Foundation Model은 RO의 기본이 되는 것으로 나머지 6개 Model들의 부모 요소(Parent Element)가 된다. Context Model은 권한에 대한 META Information을 보여주고, Agreement Model은 DCF에 대한 사용자의 권리를 표시한다. Inheritance Model은 RO의 상속을 명세하고, Security Model은 DCF를 해독하기 위해 필요한 CEK와 암호화 정보를 표시한다. 그리고 Permission Model은 사용자의 가능한 권한(재생, 출력, 실행 등)을 명세하고, Constraint Model은 DCF를 사용하는 데 필요한 사용 규칙(사용 횟수, 사용 시간, 사용 가능한 기간 등)을 명세한다.

4. OMA Rights Object Acquisition Protocol

ROAP(Rights Object Acquisition Protocol)는 OMA DRM에서 사용자가 콘텐츠 공급자로부터 RO를 발급받기 위한 통신 프로토콜이다. OMA DRM에서는 4-Pass Registration Protocol, 2-Pass RO Acquisition Protocol, 1-Pass RO Acquisition Protocol, 2-Pass Join Domain Protocol, 2-Pass Leave Domain Protocol이 있고, 이러한 Protocol를 통하여 RO 발급을 관리한다. 아래의 fig 5.에서 보이는 4-Pass Registration Protocol은 사용자와 콘텐츠 공급자가 서로 통신하기 전에 반드시 사용하여 상호 등록을 하는 프로토콜이다. 앞으로 ROAP에 사용하게 될 프로토콜의 버전, 알고리즘, 인증서 정보, 기타 확장 기능에 대한 정보가 사용자의 장치와 콘텐츠 공급자의 RI에 저장된다. 사용자는 Device Hello를 콘텐츠 공급자에게 전달하고, 콘텐츠 공급자는 RI Hello를 통해 응답한다. 이후 사용자는 RegistrationRequest를 통하여 사용자와 콘텐츠 공급자간의 상호 등록을 요청하고, 콘텐츠 공급자는 OCSP(Online Certificate Status Protocol)를 통해 사용자에 대한 확인을 요청할 수 있고, RegistrationResponse를 통해 상호 등록 결과를 사용자에게 전송한다.

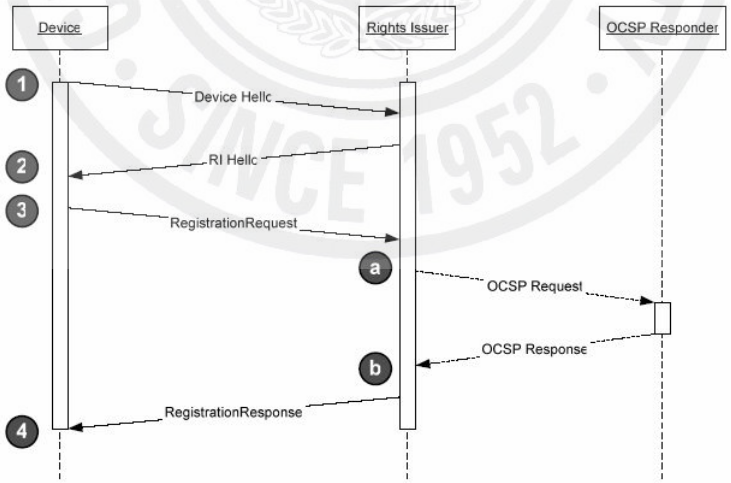

Figure 5. 4-Pass Registration Protocol

아래의 fig 6.에서 보이는 2-Pass RO Acquisition Protocol은 사용자와 콘텐츠 공급자에게 RO를 요청하고, 콘텐츠는 요청받은 RO를 전달하는 프로토콜이다. 사용자는 RO Request를 통해 콘텐츠 공급자에게 RO를 요청하고, 콘텐츠 공급자는 OCSP(Online Certificate Status Protocol)를 통해 사용자에 대한 확인을 요청할 수 있고, RO Response를 통해 RO를 사용자에게 전달한다.

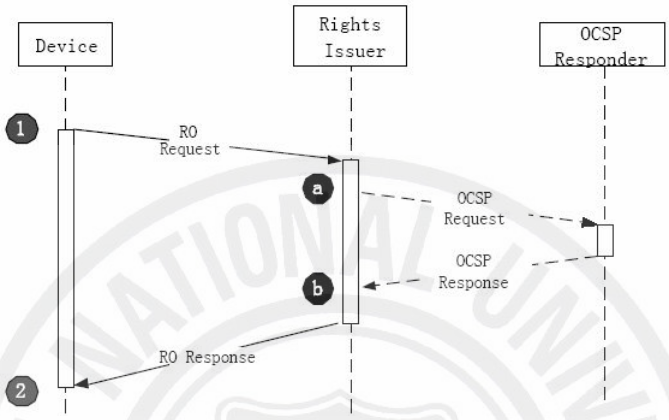

Figure 6. 2-Pass RO Acquisition Protocol

아래의 fig 7.에서 보이는 1-Pass RO Acquisition Protocol은 사용자의 RO 발급 요청 없이 콘텐츠 공급자가 직접 사용자에게 RO를 전달(Push)하는 프로토콜이다. 정기적으로 발급되는 RO의 경우 혹은 다른 사용자에 의하여 RO가 구입(선물)이 되고 전달이 되는 경우, 콘텐츠 공급자는 RO를 RO Response에 담아 사용자에게 전달한다.

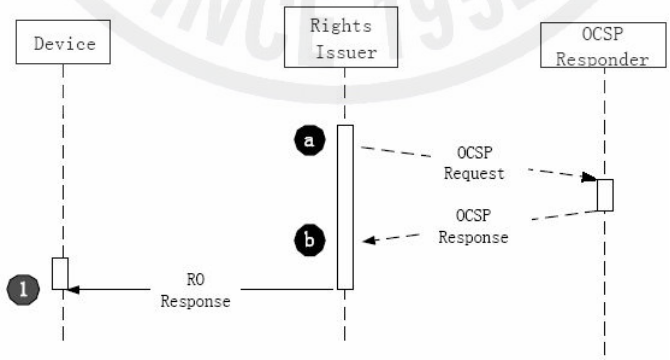

Figure 7. 1-Pass RO Acquisition Protocol

아래의 fig 8.에서 보이는 2-Pass Join Domain Protocol은 사용자가 특정 Domain에 가입을 하기 위한 프로토콜이다. 사용자는 JoinDomain Request를 통해 콘텐츠 공급자에게 Domain 가입 요청을 하고, 콘텐츠 공급자는 이에 대한 응답을 JoinDomain Response를 통해 사용자에게 전달한다.

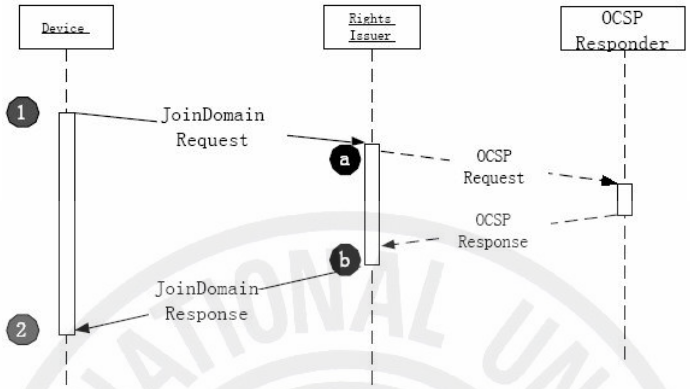

Figure 8. 2-Pass Join Domain Protocol

아래의 fig 9.에서 보이는 2-Pass Leave Domain Protocol은 사용자가 Domain 탈퇴를 위한 프로토콜이다. 사용자는 LeaveDomain Request를 통해 콘텐츠 공급자에게 Domain 탈퇴 요청을 하고, 콘텐츠 공급자는 이에 대한 응답을 LeaveDomain Response를 통해 사용자에게 전달한다.

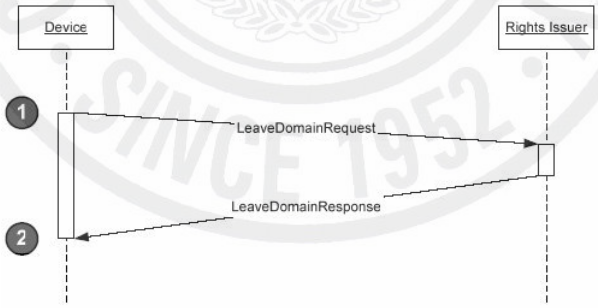

Figure 9. 2-Pass Leave Domain Protocol

위에서 나타난 바와 같이 OMA DRM에서는 ROAP를 통해 사용자의 RO 발급 요청이나 도메인 가입/탈퇴 요청을 처리한다. 만약 사용자 소유의 어떤 장치가 콘텐츠 공급자에게 연결이 될 수 없는 경우(Unconnected Device to Contents

Provider)에는 다음과 같은 형태로 ROAP를 수행하여 RO의 발급 요청이나 도메인 가입/탈퇴 요청을 처리할 수 있다.

1) 사용자의 Unconnected Device(이하 UD)는 Connected Device(이하 CD)를 통해 콘텐츠 공급자에게 DeviceHello를 전달한다.
2) 콘텐츠 공급자가 RI Hello를 CD로 전송하면, CD는 이를 그대로 UD에게 전달한다.
3) UD는 상호등록 요청인 RegistrationRequest를 CD를 거쳐 콘텐츠 공급자에게 보내고, 이에 대한 응답인 RegistrationResponse가 콘텐츠 공급자에서 CD를 거쳐 UD로 전달된다.
4) 마찬가지로 도메인 등록 요청인 JoinDomainRequest도 CD를 거쳐 콘텐츠 공급자에게 보내지고, 이에 대한 응답인 JoinDomainResponse가 콘텐츠 공급자에서 CD를 거쳐 UD로 전달된다.

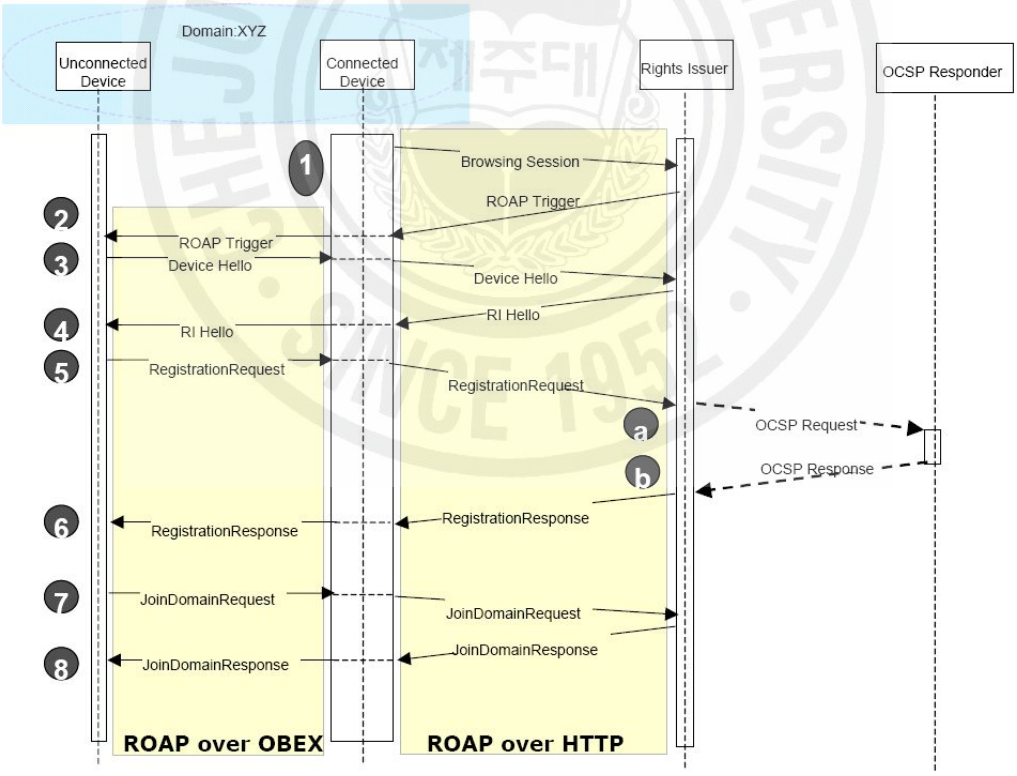

Figure 10. Unconnected Device Registration and Domain Establishment

5. OMA DRM에 대한 고찰

OMA DRM은 콘텐츠의 내용을 알 수 없게 암호화하는 암호화(Encryption) 기능과 아무나 접근할 수 없게 하는 접근제한(Conditional Access) 기능, 불법적으로 복제를 하지 못하게 하는 복제 제어(Copy Control), 그리고 복제되었을 때 그 복제된 콘텐츠를 추적하고 확인하는 식별 및 추적(Identification & Tracing) 기능으로 구성되어 있다. 위와 같은 기능을 통하여 OMA DRM은 사용 규칙을 정의하고 그 범위 내에서만 콘텐츠가 동작하도록 제어하는 암호화 기술을 이용하여 사용권한을 만족하는 사용자에게만 디지털 콘텐츠를 사용할 수 있게 한다. 이를 위하여 OMA DRM에서는 RO의 발급은 오로지 콘텐츠 공급자만이 가능하도록 되어 있다. 따라서 사용자가 실제 DCF를 사용하는데 필요한 RO를 발급받기 위해 사용자는 반드시 콘텐츠 공급자에 접속해야할 필요가 있다. 이것은 사용자와 콘텐츠 공급자는 항상 온라인으로 연결이 되어 있어야 함을 의미하고, 반대로 온라인으로 연결이 불가능한 사용자의 경우에는 DRM이 적용될 수 없음을 의미하게 된다. 또한 OMA DRM에서는 한명의 사용자나 하나의 멀티미디어 콘텐츠 재생장치(Multimedia Contents Player, 이하 MCP)에 대하여 하나의 DCF에 대한 하나의 RO만을 허용한다. 혹은, Domain으로 묶인 사용자들이나 MCP는 Domain RO를 통하여 DCF를 사용할 수 있다. 이것은 사용자가 정당한 방법으로 획득한 RO가 있더라도, 자기 소유의 다른 MCP에서 RO를 사용하기 위해서는 해당 MCP을 위한 새로운 RO를 발급받아야 하고, Domain RO의 경우에도 Domain을 벗어난 사용자나 MCP 역시 새로운 RO를 발급받아야 함을 의미한다. RO의 발급제한은 유효한 RO를 보장하기 위함과 RO에 대한 악의적인 공격이나 접근을 차단하기 위함이지만, 이로 인하여 사용자는 기존에 한번 구입하면 자유롭게 사용이 가능했던 아날로그 콘텐츠에 비하여 한번 구입을 해도 자유롭게 사용이 불가능한 DRM으로 보호되는 디지털 콘텐츠의 사용에 대한 불편을 초래할 수가 있고, 이러한 불편으로 인하여 사용자는 DRM을 콘텐츠 저작권을 위한 필수적인 보호 기술로 인식하지 않고, 사용자의 권한을 제한하고 차단하는 기술로 바라볼 위험을 가지고 있다.

Ⅲ. 안전한 콘텐츠 유통을 위한 DRM 시스템

OMA DRM을 포함한 기존 DRM에서는 일반적으로 하나의 RO는 하나의 콘텐츠에 대해서만 연결된다. RO는 내부에 RO의 대상이 되는 콘텐츠와 사용자 혹은 장치에 대한 식별자가 존재한다. 해당 식별자와 일치하지 않는 사용자나 콘텐츠는 비록 RO를 보유하고 있다하더라도 그 RO로 사용자가 원하는 콘텐츠를 재생하는데 쓰일 수 없다. 이것은 콘텐츠 공급자 입장에서 생각해본다면, RO의 무결성을 보장함과 동시에 사용자의 부적절한 RO의 사용을 완전히 차단할 수 있는 장점이 있다. 반면에 콘텐츠 사용자 입장에서는 자신이 구입한 콘텐츠일지라도 RO에 명세된 사용 규칙 내에서만 콘텐츠 이용이 가능하게 된다. 사용자에게 있어서, 이러한 제한은 지금까지 사용자가 아날로그 콘텐츠를 이용하면서 당연시하고 있었던 콘텐츠의 자유로운 사용(콘텐츠 개조, 변형, 복제, 선물 등)을 콘텐츠 공급자가 간섭한다고 볼 수 있다. 무엇보다 DRM 기술은 콘텐츠의 이용을 제한하여 저작권을 보호하는 기술이지 사용자에게 불편함이나 제한된 사용을 강요함은, 아직 DRM 존재 의의에 대해 사람들의 인식이 긍정적이지 않은 지금에서는 오로지 콘텐츠 공급자만을 위한 보호 기술로 인식되고 DRM이 적용된 콘텐츠의 사용을 꺼리게 될 우려가 있다. 그리고 지금까지의 DRM은 콘텐츠 제작자를 포함한 콘텐츠 공급자가 배포하는 디지털 콘텐츠의 저작권을 보호하고 사용을 제어하기 위해 개발되고 연구되어 왔다. 이때까지의 콘텐츠는 주로 전문적인 제작자에 의하여 배포되고 해당 제작자가 인정한(유통 계약을 체결한) 콘텐츠 공급자에 의해서 배포되는 콘텐츠만이 합법적인 콘텐츠로 인정을 받고 보호를 받는다. 하지만 개인용 컴퓨터의 발달은 동시에 개인용 멀티미디어 저작도구의 발전을 이끌었고, 인터넷의 출현으로 이러한 개인이 작성한 콘텐츠가 일반 대중들에게도 널리 퍼지게 될 환경이 마련되었다. 그리고 포털 사이트 등을 통해서 사용자들이 직접 작성한 콘텐츠에 대한 관심이 커지게 되었고, 일부 사용자들은 그들과 같이 직접 콘텐츠를 제작하게 되었다. 이러한 현상이 반복되어 지금에 이르러는 수많은 종류와 형태의 사용자 제작 콘텐츠(User Create Content, 이하 UCC)들이 출현하게 되었고, 모바일 기기

의 컨버전스 융합과 제공되는 서비스의 다양화로 사용자가 원하는 즉시 하나의 콘텐츠가 완성이 되고, 해당 콘텐츠는 모바일을 통해 자신이 미리 정해둔 곳으로 등록이 되고, 다른 사용자들은 그 콘텐츠를 확인할 수 있는 서비스가 출현하였다. 이러한 UCC들은 개인 사용자들의 콘텐츠 제작 욕구는 충족시켜주었고, 이를 통해 만족을 얻는 사용자들을이 점점 증가함에 따라 지금은 하나의 문화 트렌드로 자리잡게 되었다. 하지만 이러한 UCC들은 주로 멀티미디어 저작 도구에 의한 자동적으로 생성된 콘텐츠가 대부분이고, 다른 콘텐츠를 무단으로 복제한 후 수정을 하는 경우가 많으며, 막상 유통되었을 때 이 UCC를 보호하기 위한 장치가 전혀 없는 문제점을 가지고 있다. 따라서 이러한 UCC들을 통합적으로 관리하고 보호하는데 가장 적합한 보호 장치는 DRM이지만, 현재까지의 DRM은 오로지 콘텐츠 공급자를 기준으로 시스템이 개발되어 UCC를 보호하기에는 여러 가지 문제점을 가지고 있다. 무엇보다 많은 개인 사용자들은 자신의 UCC를 보호하기 위해 고비용이 들어갈 수 있는 DRM을 적용하려고 하지 않을 것이다.

본 장에서는 사용자가 DRM이 적용된 콘텐츠를 사용하는데 있어, 기존 아날로그 콘텐츠를 사용한 것처럼 적법한 사용범위 내에서는 콘텐츠, 특히 RO에 대하여 사용자가 관여할 수 있는 시스템에 대해 설명한다. 제안하는 DRM 시스템은 OMA DRM 시스템을 기본으로 하여 RO의 발급과 전달에 있어서 사용자가 그 역할을 일정부분 담당을 하게 된다. 동시에 RO의 무결성을 보장하기 위해서 사용자가 직접 RO를 수정하거나 접근할 수 없도록 콘텐츠를 보호하는 것은 여전히 필요할 것이다. 또한 개인 사용자들에 의해 제작된 UCC에 대해 통합적으로 관리가 가능한 DRM 시스템에 대해서도 설명한다. 그리고 이러한 콘텐츠들을 전달하기 위해 사용될 수 있는 MMS에 대해서도 DRM을 적용시킬 방안에 대해서도 설명한다. 본 논문은 사용자에게 발급된 RO를 사용자가 다시 재발급 할 수 있는 DRM 시스템, 사용자 제작 콘텐츠에 대해서도 적용 가능한 DRM 시스템, 멀티미디어 메시지에 첨부되는 멀티미디어 콘텐츠를 보호하기 위한 DRM 시스템을 제안하고 있다.

1. 사용권한 재발급이 가능한 DRM 시스템

본 절에서는 RO의 재발급을 가능하게 하는 DRM 시스템에 대해 설명한다. 제안하는 DRM 시스템에서는 RO의 발급은 콘텐츠 공급자가 담당하는 것에는 변함이 없지만, 발급받은 RO에 대해서 사용자가 재발급을 할 수 있도록 허용한다. 이러한 DRM 시스템에서는 사용자가 단순히 콘텐츠를 사용하기 위해 RO가 발급받는 것이 아닌, 콘텐츠 공급자의 마케팅 정책과 맞물려 사용자들이 적극적으로 DRM으로 보호되는 콘텐츠를 사용하는데 유도하기 위해서 사용될 수 있다.

1) 다단계 판매 방식(multi-level marketing plan)

다단계 판매 방식은 다계층 판매방식 또는 피라미드 판매(pyramid selling)라고도 한다. 이것은 상점에서 물건을 파는 보통의 판매방법과는 다른 특수판매의 일종으로 이 방식에서는 fig. 11에서처럼 본부 회사(최상위 판매자)와 독립된 가입자(판매자)가 연쇄적으로 다른 판매자를 판매조직에 가입시켜 차례로 조직 내의 상위 그룹으로 승진함으로써 조직을 확대해 나간다[7].

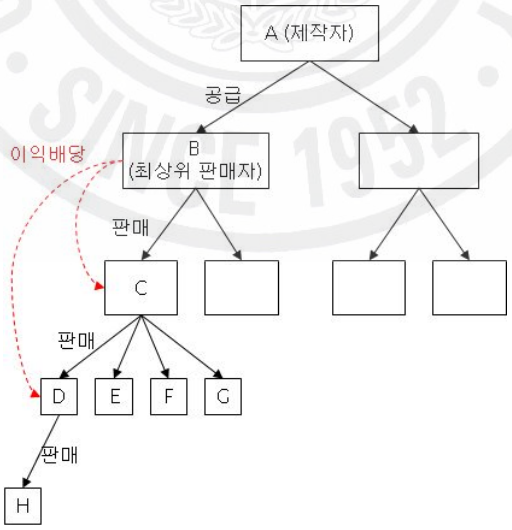

Figure 11. Multi-level Marketing Plan

이 확대의 추진력으로서 새 가입자가 내는 가입금의 일부 또는 전부, 또는 가입자의 상품 매입으로 인한 도매 이익을, 권유에 성공하거나 승진한 기가입자에게 배분한다. 상품의 판매와 새로운 판매원의 획득으로 이익이 얻어지는 것을 미끼로 판매원을 모집하여 권리금을 받고, 모집된 판매원도 그러한 방식을 되풀이하여 판매원을 늘리고 판매량도 늘리려는 시장 개발 방법이다. 그러나 이와 같은 판매 방식은 상품의 판매 상황과 관계없이 조직이 확대되고 말단 판매원에게 재고가 누적되는 등 가입자와 소비자에게 주는 피해가 적지 않다. 이에 따라 부당한 피해를 줄이기 위해 적절한 입법으로 이를 규제하고 있다. 하지만 DRM 시스템에서 RO에 판매에 대한 일정 부분의 이익을 사용자에게 되돌려준다고 한다면, 콘텐츠 공급자는 RO를 통해 콘텐츠의 사용을 제어하는 것만이 아니라, 사용자로 하여금 RO의 판매에 직접 참여하도록 유도할 수 있게 된다. 현재 수많은 곳에서 사용되고 있는 물건 구입이나 회원 유치 시 지급되는 포인트 제도나 Cash Back 제도를 보면, 사용자는 제품을 구입하는데 있어서, 혹은 보험이나 금융 상품에 가입을 하는데 있어서 포인트 지급이나 Cash Back이 가능한 제품을 선택하고 있음을 알 수 있다. 다른 사용자들은 이러한 포인트를 적극적으로 지급받기 위해 지인들에게 부탁을 하거나 요청을 하여 특정 상품을 구매하는데 영향을 끼치기도 한다. 본 절의 DRM 시스템은 위에서 언급한 사용자의 욕구를 다단계 판매 방식을 도입하여 해결한다. 이를 통하여 DRM으로 보호되는 콘텐츠가 널리 유통되도록 유도하고, 더 나아가 DRM 시스템이 사용자들의 거부감이 없이 정착될 수 있게 할 것이다.

2) 다단계 판매 방식을 적용한 DRM 시스템

DRM 시스템에서는 그 어떠한 경우에 있어서도 암호화된 콘텐츠와 RO에 대해서는 무결성이 보장되어야 한다. 따라서 일반적인 다단계 판매 시스템에서 하위 판매자들이 물건을 직접 주고받으면서 이익을 발생시키지만, 본 절의 DRM에서는 사용자들은 RO를 주고받게 된다. 여전히 암호화된 콘텐츠는 2장에서 설명한 Super-Distribution을 통하여 언제 누구나 자유로운 방법으로 전달이 될 수 있기 때문에 판매자들이 RO의 발급을 수행하는 것으로 다단계 시스템에서 물건을 판매하는 것과 동일하게 된다. 이를 위해서는 판매자들이 RO를 발급할 수 있어야 한

다. 하지만 DRM의 시스템 구조상 RO는 오직 콘텐츠 공급자만이 발급할 수 있도록 되어 있다. 인증되지 않은 판매자들이 발급하는 RO는 콘텐츠 유통과 사용에 있어 적법한 절차를 무시하고 유통과정의 투명성에 대해 혼란을 야기할 우려가 있다. 따라서 다단계 판매 방식에서 물건의 판매가 이루어질 때 판매자들이 물건 그 자체에 대해서는 관심이 없듯이, DRM 시스템에서도 판매자들이 RO에 대해 관심을 두지 않도록 RO의 무결성은 여전히 보장되어야 한다. 판매자들은 단지 RO의 전달만을 허용하도록 되어 있다. 본 절에서 제안하는 DRM 시스템은 fig. 12에 보이는 것처럼 ROAP와 Rights Issuer에 의한 두 가지 형태의 RO 재발급 방법을 제한하고, 이를 통하여 RO의 다단계 판매 방식을 지원하고 있다.

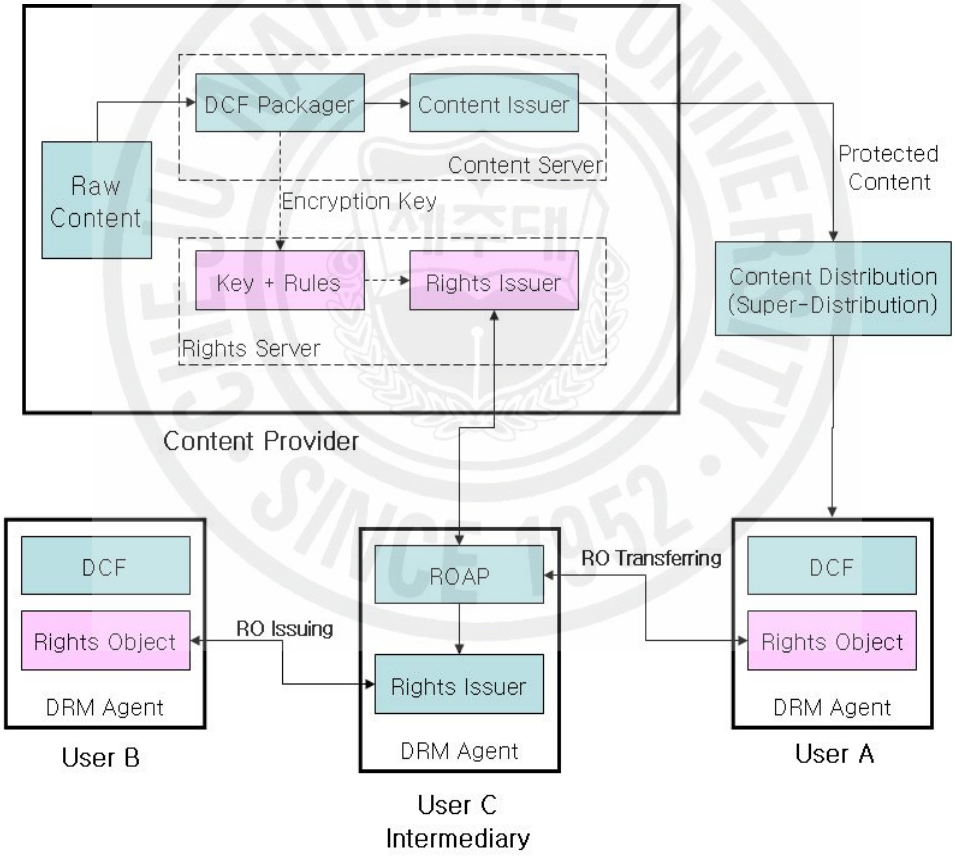

Figure 12. System Architecture of Suggested-DRM

fig. 12는 2장의 OMA DRM 시스템 구조에서 ROAP와 Rights Issuer를 가지는 사용자(혹은 중개자)가 추가되었다. 일반적으로 RO의 전달만을 수행하는 경우는 ROAP를 통하여, 사용권한이 발급이 필요할 때는 Rights Issuer를 통하여 발급할 수 있는 사용자이다. 제안된 DRM 시스템에서는 모든 사용자는 ROAP를 통하여 사용자가 소유한 RO를 다른 사람들에게 전할 수 있지만, 모든 사용자가 Rights Issuer를 갖고 있지는 않다. Rights Issuer를 가질 수 있는 사용자(혹은 중개자)는 콘텐츠 판매자로부터 RO 발급에 대하여 인증을 받은 사용자(혹은 중개자)만이 가능하다. 제안된 DRM 시스템은 콘텐츠 공급자가 원본 콘텐츠를 DCF로 패키징하여 Super-Distribution을 통해 배포하고, 사용자(혹은 중개자)는 ROAP와 Rights Issuer를 통해 RO를 다른 사용자에게 전달하거나 발급하며, 콘텐츠 공급자는 RO의 전달/발급에 관여한 사용자에 대한 정보를 수집한 후, 마케팅 목적에 맞게 이익의 일부를 되돌려 줄 수 있도록 한다.

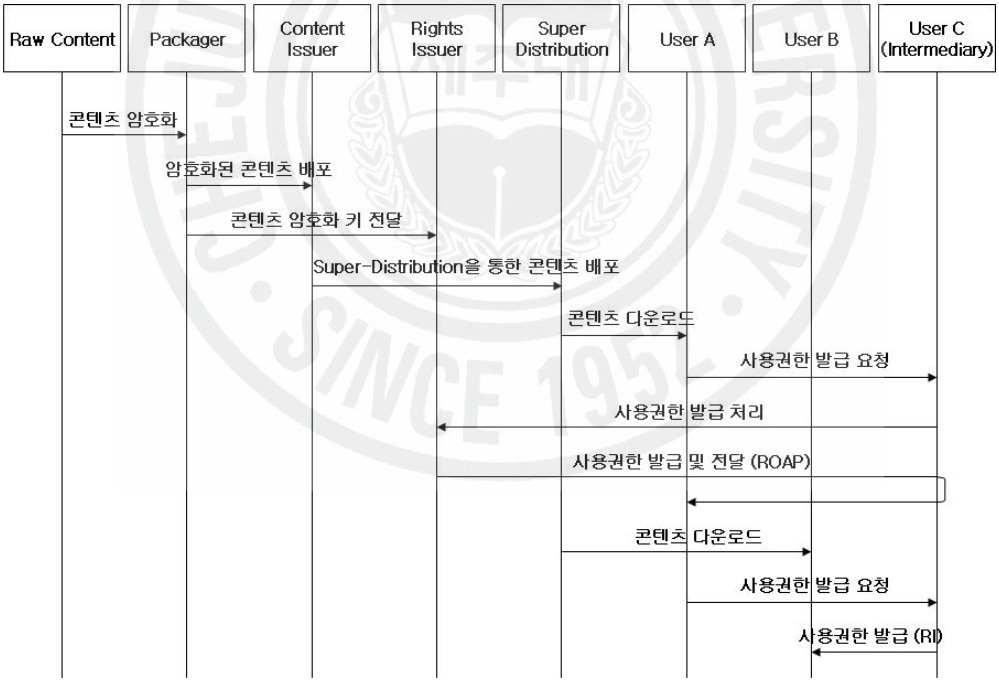

Figure 13. Event Flow Diagram

위의 fig. 13에서 보이는 것처럼 콘텐츠 공급자를 대신하여 RO를 판매하고 이에 대한 이익을 되돌려 받는 중개자는 사용자 중 그 누구나가 가능하다. 그 이유는 RO를 콘텐츠 공급자로부터 발급받기 위한 ROAP는 DRM 시스템의 사용자라면 그 누구나 기본적으로 가지고 있기 때문이다. 하지만, RO의 무결성을 위하여 그 어떤 사용자도 RO를 수정하거나 복사하는 것은 금지된다. ROAP는 판매를 위하여 사용될 수 있는 부분은 오로지 다른 사용자를 위하여 RO 발급을 대신 요청하고, 이를 통하여 콘텐츠 공급자는 대신 발급 요청하는 사용자에 대한 정보를 획득할 수 있고, 발급된 RO 또한 ROAP를 통하여 RO의 내부를 직접 접근하는 것 없이 다른 사용자에게로 전달하는데 있다. 마찬가지로 인증된 사용자(혹은 중개자)가 보유할 수 있는 Rights Issuer 또한 RO의 무결성을 보장하기 위해 그 기능이 제한된다. 사용자(혹은 중개자)의 Rights Issuer는 콘텐츠 공급자로부터 미리 판매 정책이 정해진 RO들을 저장해 두었다가 다른 사용자들의 발급 요청이 있을 때, 판매 정책이 정해진 RO들 중 하나를 선택하여 복사하고 사용자에게 그대로 발급하게 된다. 위의 fig. 13에서 나타난 바와 같이 제안된 DRM 시스템은 다음과 같은 순서로 다단계 판매 방식을 위한 RO의 재발급을 수행한다.

1) 콘텐츠 저작자는 콘텐츠 공급자에게 원본 콘텐츠를 전달
2) 콘텐츠 공급자는 원본 콘텐츠를 패키징하여 DCF로 변환
3) 패키징 과정에서 생성한 CEK와 원본 콘텐츠에 대한 정보가 RI로 전달
4) DCF로 변형된 멀티미디어 콘텐츠는 사용자들에게 Super-Distribution을 통해 자유롭게 배포
5) DCF를 다운로드한 사용자(혹은 중개자)는 콘텐츠를 사용하기 위해 콘텐츠 공급자에게 RO를 요청
6) RI는 CEK와 사용 규칙을 명세한 RO를 사용자(혹은 중개자)에게 발급 및 전달
7) 사용자(혹은 중개자)는 DRM Agent를 통해 RO에 담긴 CEK로 DCF를 해독하고 사용 규칙에 의거하여 콘텐츠를 사용
8) 사용자(혹은 중개자)는 콘텐츠 공급자의 마케팅 정책에 의해 콘텐츠를 다른 사용자에게 소개
9) 다른 사용자는 사용자(혹은 중개자)의 홍보에 의하여 콘텐츠의 구입을 결정

10) 사용자(혹은 중개자)는 다른 사용자를 위한 RO를 ROAP를 통하여 콘텐츠 공급자에게 대신 요청하고 발급받은 후 이를 다른 사용자에게 전달

11) 만약 사용자(혹은 중개자)가 콘텐츠 공급자로부터 인증이 되어있고, Rights Issuer를 지급받았다면, 사용자(혹은 중개자)가 직접 RO를 발급하여 다른 사용자에게 전달

그러므로 제안된 DRM 시스템은 크게 두 가지 형태의 RO 전달/발급이 가능하다. 첫째로 그 어떤 사용자라도 ROAP를 통해 RO의 전달에 참여하고, 그에 대한 이익을 기대할 수 있고, 둘째로 RO 중개를 전문으로 하려는 사용자는 콘텐츠 공급자로부터 전달받은 Rights Issuer를 통해 RO 발급을 직접 담당하면서 좀 더 적극적으로 다른 사용자들에게 RO를 판매할 수 있다.

2. 사용자 제작 콘텐츠를 위한 DRM 시스템

본 절에서는 사용자 제작 콘텐츠를 보호하기 위한 DRM 시스템에 대해 설명한다. 제안하는 DRM 시스템에서는 수많은 사용자들이 제작한 콘텐츠를 보호하고 관리하기 위하여 개인 DRM Packager와 개인 DRM Server를 제공한다. 개인 DRM Packager는 사용자 제작 콘텐츠를 암호화하기 위한 것이고, 개인 DRM Server는 암호화된 콘텐츠를 사용하기 위한 사용권한의 발급을 위한 것이다. 사용자들이 각기 다른 DRM Packager나 DRM Server를 사용한다면, 다시 말해 DCF의 규격과 RO의 규격이 각기 다르다면, 다른 형태로 암호화된 DCF나 다른 형태로 발급된 RO는 서로 연결될 수 없고, 사용될 수 없다. 또한 사용자 모두가 DRM Packager나 DRM Server를 가져야만 사용자가 제작한 콘텐츠를 DRM으로 보호할 수 있는 것은 여러 가지 불편을 초래할 것이다. 이러한 문제를 해결하기 위해 본 절에서는 사용자가 DRM Packager가 포함되어 있는 가상 DRM Server에 접속하여 사용자 제작 콘텐츠를 암호화하여 배포하고, 사용권한을 발급할 수 있는 DRM 시스템을 제안한다.

1) 제안된 DRM 시스템의 필요 요소

사용자가 제작한 콘텐츠를 다른 사용자에게 전달하고 싶지만, 이것을 전달받은 다른 사용자가 콘텐츠를 제작한 사용자의 의도와는 다른 용도로 사용될 우려가 존재하게 된다. 이를 방지하기 위해 DRM 시스템을 생각해볼 수 있겠지만, 개인 사용자가 DRM 시스템을 구성하고 운영하는 것은 무리가 있다. 개인 사용자가 직접 DRM 시스템을 구성하고 운영하기 위해서는 개인 사용자를 위한 DRM Server와 DRM Packager가 필요하고, 무엇보다 암호화된 콘텐츠와 사용권한을 제어할 수 있는 DRM Agent를 개인 제작 콘텐츠를 사용하는 모든 사용자들에게 전달을 하고 설치를 하여야만 할 것이다. 만약 한명의 사용자가 이러한 DRM 시스템을 구성하고 운영을 한다고 할 때, 다른 개인 사용자들이 그 사용자처럼 DRM 시스템을 구성하고 운영을 하게 된다면, 이는 수많은 다른 형태의 DRM 시스템이 혼재하게 되는 것을 의미한다. 따라서 각기 다른 사용자들이 제작한 콘텐츠를 이용하는데 공통적으로 적용될 수 있도록 DRM 서비스를 제공하는 사업자가 존재하여 해당 서비스에 가입된 사용자들에게 DRM 서비스를 제공하고, 공통적인 DRM Packager와 DRM Agent를 사용하게 하여야 한다.

2) 가상 DRM Server를 통한 사용자 제작 콘텐츠를 위한 DRM 시스템

본 절에서 제안하는 DRM 시스템은 위와 같은 문제를 해결하기 위해 사용자 제작 콘텐츠를 위한 DRM Packager와 콘텐츠를 제작한 사용자가 직접 RO 발급이 가능한 Rights Issuer가 포함된 DRM Server, 다른 수많은 개인 제작자들의 암호화된 콘텐츠와 RO를 공통적으로 관리할 수 있는 DRM Packager를 필요로 한다. 예를 들어, 사용자들은 개인 제작 콘텐츠에 대한 DRM 서비스를 하고 있는 포털 사이트에 가입을 하고, 해당 사이트에서 제공하는 DRM Packager를 통하여 콘텐츠를 암호화하고, 마찬가지로 포털 사이트의 여러 가지 서비스나 기능을 통해 다른 사용자에게 홍보하거나 전달할 수 있게 된다. 포털 사이트를 통해 개인 제작 콘텐츠를 접하게 된 다른 사용자들은 그 콘텐츠에 대하여 권한 발급을 포털 사이트를 통해 제작한 사용자에게 요청할 수 있고, 콘텐츠를 제작한 사용자는 마찬가

지로 포털 사이트의 기능을 이용하여 콘텐츠 구입을 원하는 사용자에게 RO의를 발급할 수 있을 것이다. RO를 전달받은 사용자는 포털 사이트에서 제공하는 DRM Agent를 다운로드 받아 개인 제작 콘텐츠를 사용할 수 있을 것이다. 이를 위한 DRM 시스템의 구조도는 다음 fig. 14에 나타나있다.

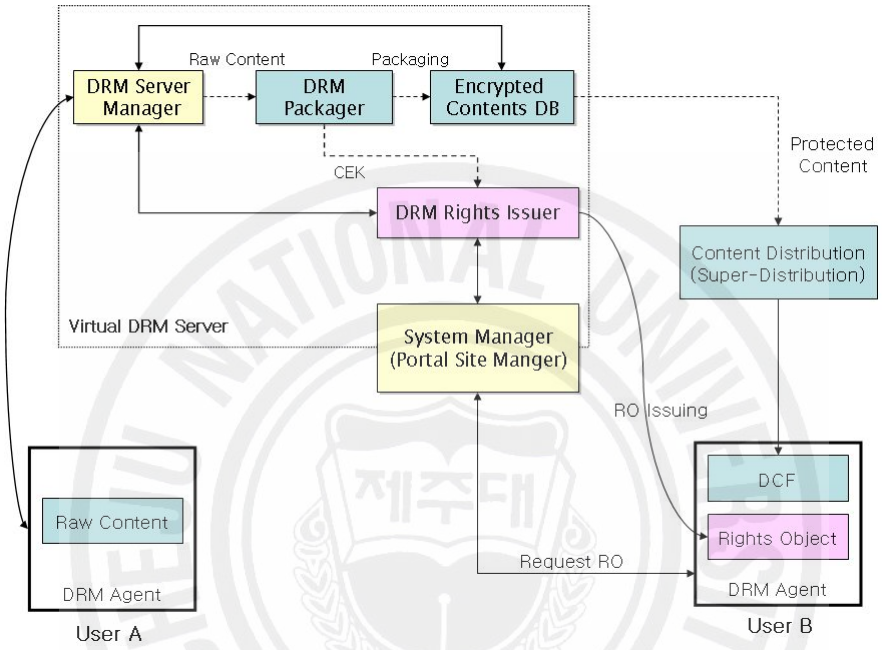

Figure 14. System Architecture of Suggested-DRM

가상 DRM Server는 일반적으로 웹 페이지나 모바일 같은 온라인 서비스를 통해 제공된다. 사용자는 개인 제작 콘텐츠에 대한 DRM 서비스를 하고 있는 웹 페이지나 모바일 서비스에 접속을 하여 언제든지 자신이 제작한 콘텐츠를 해당 서비스에 등록할 수 있다. DRM 서비스 제공자는 개인 콘텐츠 제작자를 위하여 암호화된 콘텐츠로 패키징을 할 수 있는 DRM Packager를 제공하고, 이를 저장할 수 있는 DB도 제공한다. 이 DB를 통하여 DRM 서비스 제공자는 사용자 제작 콘텐츠에 대한 검색 엔진 기능을 제공할 수 있고, 이를 통한 콘텐츠 배포도 이루어진다. 사용자 제작 콘텐츠를 다운로드 웹 페이지나 모바일 서비스로부터 직접 다운로드 받은 다른 사용자는 DRM 서비스 제공자에 의해 콘텐츠를 제작한 사용자에

게 해당 콘텐츠에 대한 사용권한의 발급을 요청할 수 있고, 콘텐츠를 제작한 사용자는 직접 사용권한을 발급하거나 DRM 서비스 제공자에 의해 정의된 여러 가지 방법 중의 하나를 선택하여 자동적으로 발급할 수 있을 것이다. 제안된 DRM 시스템은 다음의 fig. 15의 순서로 사용자 제작 콘텐츠에 대하여 암호화를 수행하고 사용권한을 발급하게 된다.

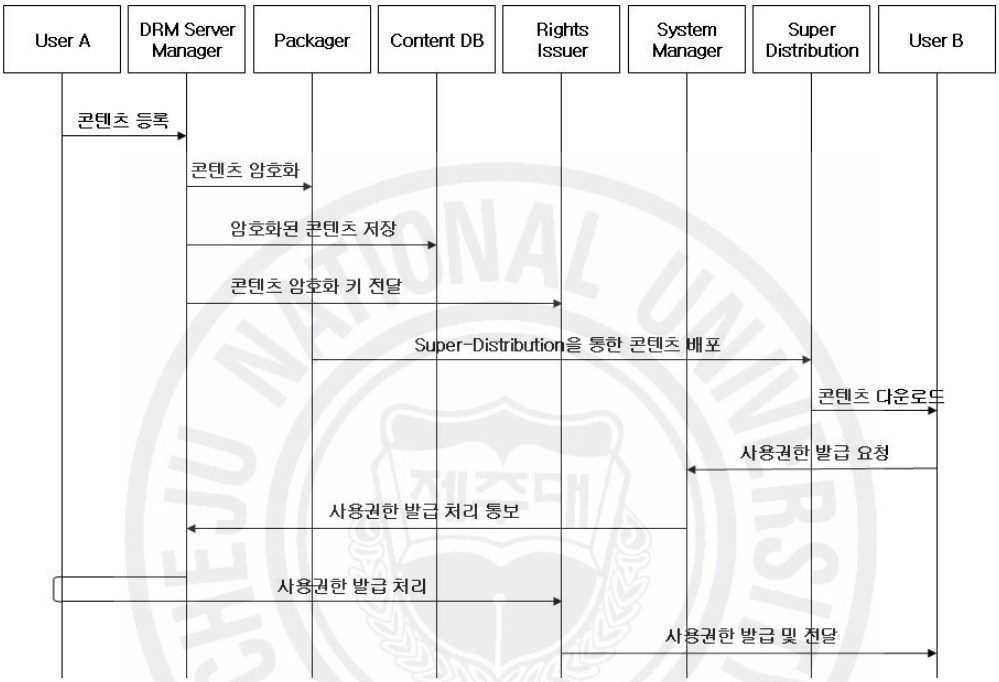

Figure 15. Event Flow Diagram

1) 콘텐츠 제작자는 사용자 제작 콘텐츠를 가상 DRM 서버에 등록
2) 등록된 원본 콘텐츠는 자동으로 패키징 되어 DB에 저장
3) DRM 서비스 제공자의 검색 서비스 등에 의해 콘텐츠가 배포
4) 콘텐츠를 다운로드 받은 사용자는 RO 발급을 DRM 서비스 제공자에게 요청
5) DRM 서비스 제공자는 원본 콘텐츠 제작자에게 이를 통보하고 RO 발급 처리를 요청
6) 원본 콘텐츠 제작자는 가상 DRM 서버에 접속하고 Rights Issuer를 통해 RO 발급을 처리
7) 사용자는 발급 받은 RO를 이용하여 콘텐츠를 사용

3. MMS를 위한 DRM 시스템

본 절에서는 멀티미디어 메시징 서비스(Multimedia Messaging Service, 이하 MMS)에서 적용 가능한 DRM 시스템에 대해 설명한다. 제안하는 DRM 시스템에서는 기존 MMS 시스템의 변경을 최소로 하는 DRM 요소만을 추가하는 형태로, MMS에서 사용가능한 DRM 시스템을 연구하였다. DRM이 적용된 MMS는 첨부되어 전송되는 멀티미디어 콘텐츠에 대한 저작권 보호를 가능하게 한다.

1) 기존 MMS의 구성

단문 메시지 서비스(Short Message Service)와는 달리 멀티미디어 콘텐츠의 전송을 위한 MMS 시스템을 구성하는 주요 요소들은 아래의 fig. 16 보이는 것처럼 멀티미디어 콘텐츠를 제작하여 사용자들에게 제공하는 콘텐츠 공급자(Content Provider), 첨부되는 멀티미디어 메시지에 음악, 영상, 이미지 등의 부가서비스를 제공하는 부가 서비스 공급자(Value Added Service Provider), 멀티미디어 메시지의 저장과 보관을 담당하는 MMS Server, 멀티미디어 메시지의 송신과 수신을 담당하는 MMS Relay/Server, 전달되는 수신기에 사용이 가능한 형태로 멀티미디어 콘텐츠를 변환하기 위한 Transcoder, 멀티미디어 메시지를 전송한 송신자와 수신자를 인증하는 인증 서버, 멀티미디어 메시지 전송에 따른 과금을 처리하기 위한 과금 서버로 구성되어 있다[8]. MMS를 사용하는 일반적인 시나리오는 다음과 같다. MMS의 전송을 원하는 사용자는 콘텐츠 공급자로부터 제공되는 다양한 종류의 멀티미디어 콘텐츠를 선택하고 자신이 전달하기 원하는 메시지를 작성한 후 사용자의 요구사항에 맞는 부가서비스를 추가하여 전송을 하게 된다. 전송된 메시지는 MMS Relay/Server에서 사용자와 수신자의 정보를 확인하여 수신자에게 사용이 가능한 형태로 멀티미디어 메시지를 변형하고 멀티미디어 메시지 전송에 대한 과금 처리를 수행한 후에 수신자에게 전송을 한다.

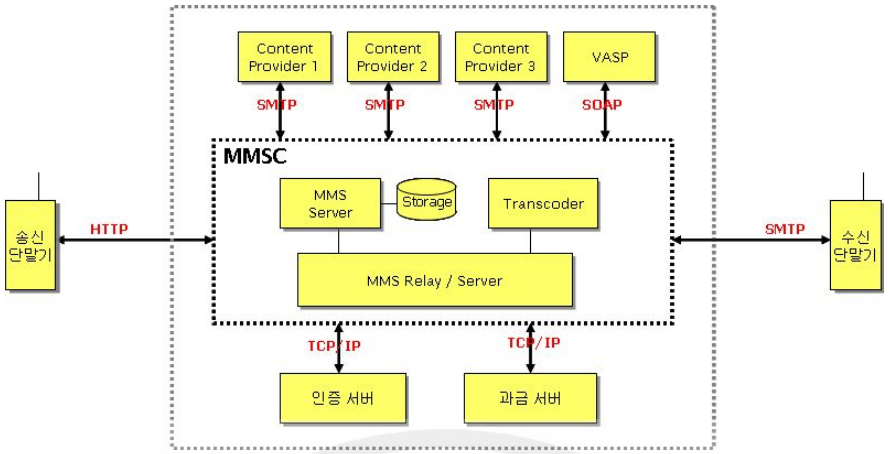

Figure 16. System Architecture of MMS

MMS 시스템 구성 요소들과 MMS 시스템에 연결되는 외부 구성 요소들 사이의 Interface는 MM1 ~ MM10으로 정의한다.

1) MM1 : MMS User Agent와 MMS Relay/Server 사이의 인터페이스. 전송 규격은 WAP이나 기타 플랫폼 및 프로토콜에 따라 각각 정의될 수 있음
2) MM2 : MMS Relay/Server와 MMS Server 사이의 인터페이스
3) MM3 : MMS Relay/Server와 External Messaging System 간 인터페이스
4) MM4 : MMS Relay/Server와 타 MMS Relay/Server 사이의 인터페이스. SMTP(Simple Mail Transfer Protocol)를 이용하여 메시지 전송
5) MM5 : MMS Relay/Server와 Home Location Register 사이의 인터페이스. 기존의 MAP 기능을 사용함 (예 : 모바일 위치를 측정하기 위한 절차, 단문 메시지 서비스 센터와 연동하기 위한 절차)
6) MM6 : MMS Relay/Server와 MMS User Databases 사이의 인터페이스
7) MM7 : MMS Relay/Server와 MMS VAS Application 사이의 인터페이스. HTTP 전송계층을 사용하는 SOAP(Simple Object Access Protocol)가 기반
8) MM8 : MMS Relay/Server와 Post-processing System 사이의 인터페이스
9) MM9 : MMS Relay/Server와 Online Charging System 사이의 인터페이스
10) MM10 : MMS Relay/Server와 Messaging Service Control Function 사이의 인터페이스

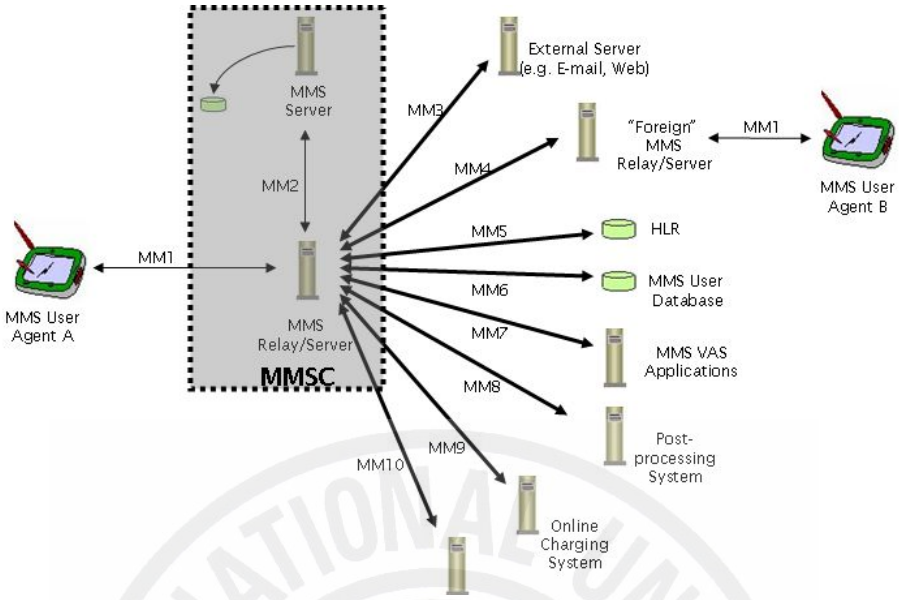

Figure 17. 3GPP TS 23.140 Reference Architecture[9]

2) MMS DRM 시스템

1992년 12월 당시 아날로그 방식이었던 무선전화통신망을 디지털 기술로 전환하기 위한 GSM Phase 1 이동통신 표준 테스트를 위해, Sema PLC 회사에서 PC를 이용해 영국의 통신기업 보다폰에 메시지를 보낸 것이 최초의 메시지 전송으로 알려져 있다. 그로부터 10여년이 지난 오늘날 단문 메시징 서비스(Short Messaging Service, SMS)는 이동통신사업자들의 이동통신망을 개방한 이후 다양한 서비스 방식과 마케팅을 통해 대중화되었다. 인터넷 등장 이후 멀티미디어 서비스가 일반화되어 텍스트 위주의 SMS로는 더 이상 사용자의 욕구를 충족할 수 없게 되었다. 이동통신망의 진화에 따라 전전송속도가 증가하고 멀티미디어 솔루션을 지원하는 다기능 단말기가 보급됨에 따라 멀티미디어 메세징 서비스(MMS : Multimedia Messaging Service)가 개발되었다[10]. MMS 표준규격에는 첨부되는 멀티미디어 콘텐츠에 대한 저작권 보호 방법이 규정되어 있지 않다. 따라서 본 논문에서는 MMS 시스템에 DRM 시스템을 적용하였다. MMS DRM 시스템은 DRM이 적용된 MMS 시스템을 의미한다. MMS DRM을 위해서 원본 콘텐츠를 암호화 하는

DRM Packager와 사용권한 발급을 관리하는 DRM Rights Issuer가 MMSC에, 사용자의 암호화된 콘텐츠 사용을 제어하는 DRM Agent가 사용자 단말기에 추가되었다. DRM의 요소와 MMS의 요소를 결합하여 구성한 MMS DRM 시스템의 전체 구조는 다음 fig. 18과 같다.

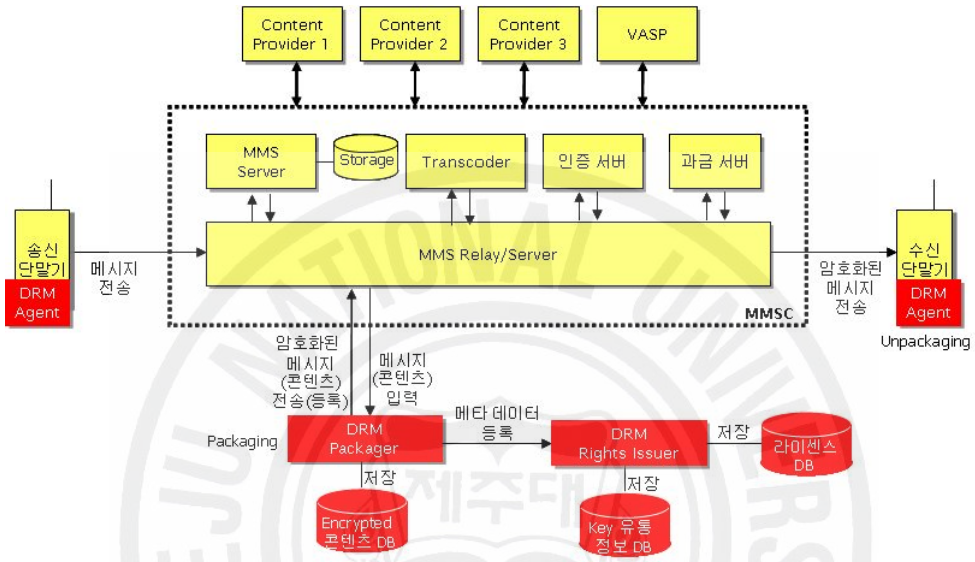

Figure 18. MMS DRM Architecture

가) MMS DRM Packager

MMS DRM Packager는 원본 콘텐츠를 DRM으로 보호되는 암호화된 콘텐츠인 DCF로 변환을 담당하는 요소이다. 콘텐츠 공급자가 원본 콘텐츠를 DRM Packager를 통해서 암호화를 하고 이를 MMS Server에 저장한다. 사용자는 MMS Server에 접속하여 첨부할 콘텐츠를 검색하고 선택하여 MMS에 첨부하고 전송하게 된다. 본 논문에서 MMS에 적용된 DRM Packager는 원본 콘텐츠를 OMA DRM Content Format 규격에 준하여 패키징하게 된다. 패키징된 결과를 콘텐츠 공급자에게 통보하고 콘텐츠 공급자는 콘텐츠 식별자를 통해 암호화된 콘텐츠를 확인할 수 있다. 또한 DRM Packager는 콘텐츠의 메타 정보와 콘텐츠 정보, 암호화 정보 등을 암호화된 콘텐츠의 헤더에 저장하고 이를 통해 콘텐츠의 저작권 정보를 보관하게 된다.

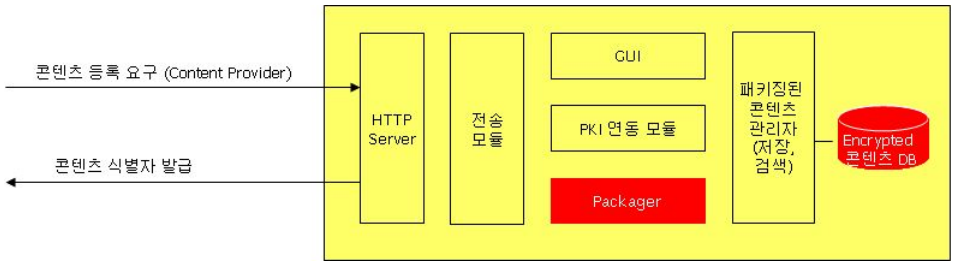

Figure 19. MMS DRM Packager Architecture

나) MMS DRM Server

MMS DRM Server는 사용권한의 발급과 발급된 사용권한의 사후 관리를 담당하는 요소이다. 또한 DRM Packager로부터 암호화된 콘텐츠의 정보를 받아 암호화된 콘텐츠를 복호화하는데 필요한 콘텐츠 암호화 키의 발급도 관리한다. MMS DRM Server는 Rights Issuer를 통해 사용자에게 전달할 Rights Object를 OMA DRM REL 규격에 따라 생성하는 기능, DRM Content 정보 및 콘텐츠 메타 데이터를 DRM Server에 등록하는 기능, Right Holder를 통한 저작권 관리(삭제/중지/재개/검색/통계 정보 제공 등) 기능, 구입을 원하는 사용권한에 대한 List 페이지 제공 기능, OMA DRM 의 Download 규격에 따른 Right Agreement 전달 기능, 가격 정책 및 마케팅 정책에 따른 사용권한 발급 및 관리 기능, 콘텐츠 공급자와 DRM Server 사이에 PKI 암호화 기술을 기반의 공개키에 대한 인증서 발급을 통한 사용자 인증 기능, 과금 서버 및 인증 서버 연동을 통한 과금 처리 및 인증 처리 기능을 수행한다.

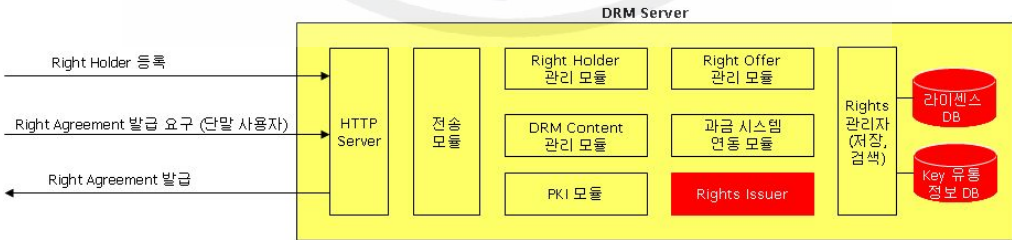

Figure 20. MMS DRM Server Architecture

다) MMS DRM Agent

MMS DRM Agent는 사용자가 암호화된 콘텐츠를 사용권한에 명세된 사용규칙에 맞게 사용될 수 있도록 관리하는 요소이다. 따라서 MMS DRM Agent는 사용권한의 검색 및 관리(전송/삭제/백업/복구)를 지원하는 기능, DRM Content를 이용하는 Content Application과 Interface 기능, 사용권한을 설치하는 Discovering Application / Download Agent / Push Agent와 Interface하는 기능, DRM Content와 사용권한의 무결성을 검사하는 기능, DRM Content를 사용권한에 명세된 내용에 따라 콘텐츠의 이용을 제어하는 기능을 수행한다.

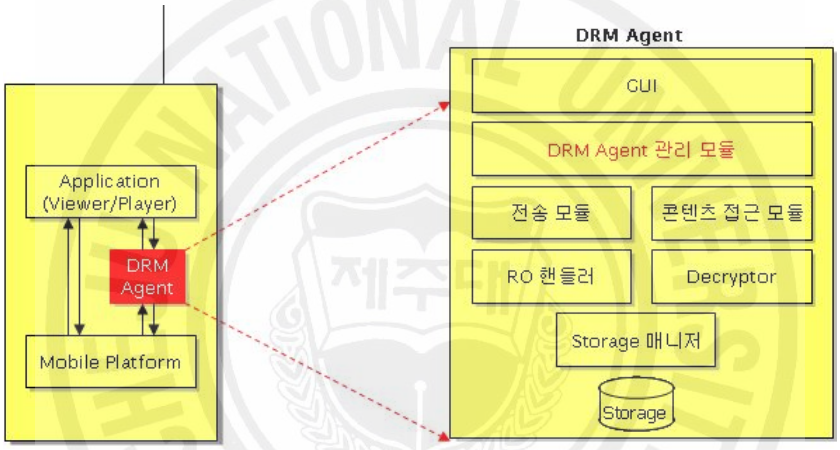

Figure 21. MMS DRM Agent Architecture

라) Event Flow Diagram

본 논문에서 연구한 MMS DRM 시스템은 다음의 순서를 통하여 MMS를 작성한 사용자와 MMS를 전송받는 사용자에게 전달이 된다. 여기서는 DRM을 필요로 하는 콘텐츠 공급자로부터 제공되는 멀티미디어 콘텐츠의 MMS 전송에 대하여 고려하였다.

1) Content Provider는 사용자에게 멀티미디어 콘텐츠를 제공하기 위해 DRM Packager를 통하여 원본 콘텐츠를 암호화 함
2) 암호화된 콘텐츠에 대한 암호화키를 RI로 전달하고, RI는 이를 DB에 보관함
3) MM 작성을 원하는 사용자는 Content Provider가 제공하는 멀티미디어 콘텐

츠 중 하나를 선택하고 자신의 메시지를 입력한 후, 작성이 완료된 MM을 수신측 사용자에게 전달

4) MMSC는 송신측 사용자의 MM과 수신측 사용자의 정보(단말기 번호) 전달받음

5) MMSC는 인증 서비스를 이용하여 수신측 사용자의 단말기 성능을 확인하고, MM의 변환이 필요하다면 Transcoder를 사용하여 MM을 변환

6) 변환이 완료된 MM을 수신측 사용자에게 전달

7) 수신측 사용자는 전달받은 MM을 사용하기 위하여 MMSC로 RO의 구입을 요청

8) RO에 대한 과금처리

9) Rights Issuer는 수신측 사용자에게 MMSC를 통해 RO 전달

10) 수신측 사용자는 발급된 RO를 이용하여 DRM Agent를 통해 MM을 재생

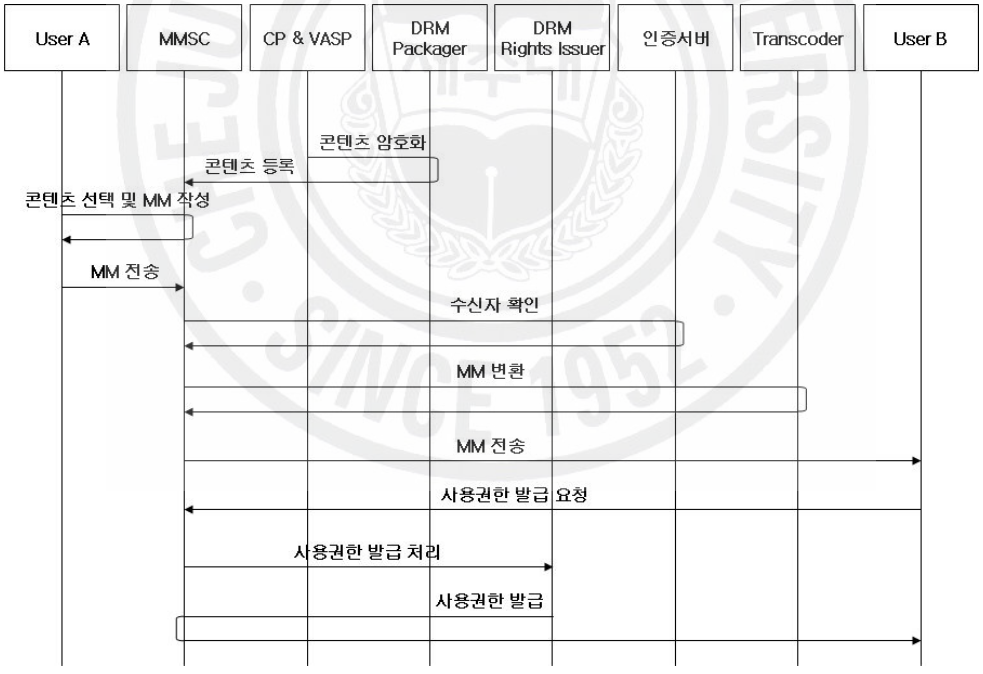

Figure 22. MMS DRM Event Flow Diagram

Ⅳ. Use Cases

인터넷 기술이 발전함에 따라 인터넷은 가장 강력한 정보의 생성 및 유통 매개물인 동시에 가장 효과적인 정보의 재생산(Reproduction) 장소가 되었다. 이러한 특성으로 인해 '디지털 딜레마(Digital Dilemma)'에 빠지기 시작하였는데, 영화나 음악, 책과 같은 멀티미디어 콘텐츠가 인터넷을 통해 빠르고 쉽게 유통되는 것과는 반대로 해당 콘텐츠의 불법적인 사용에 대한 문제점이 제기되기 시작한 것이다. 이러한 디지털 콘텐츠의 저작권에 대한 논쟁이 가열되면서, 콘텐츠의 불법사용 방지 및 저작권 보호를 위한 DRM(Digital Right Management)이 주목을 받고 있다. DRM은 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호함으로써 콘텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템으로 정의할 수 있다. 더 나아가 DRM은 디지털 콘텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포괄하는 개념이다. 본 논문에서는 안전한 콘텐츠 유통을 위한 3가지 형태의 DRM 시스템을 제안하였다. 다양한 가격 정책 및 마케팅 정책을 기대할 수 있는 사용권한의 재발급이 가능한 DRM 시스템, 사용자 제작 콘텐츠의 저작권 보호를 위한 DRM 시스템, MMS에 첨부되는 멀티미디어 콘텐츠를 보호하기 위한 DRM 시스템은 목적에 따라서 하나의 시스템으로 통합되어 동작하거나 별개의 시스템으로서 동작을 하게 된다. 제안된 3가지 DRM 시스템은 기존 DRM 시스템이 가지고 있었던 여러 가지 문제를 보완한다. 본 절에서는 기존 DRM 시스템의 성능과 제안하는 DRM 시스템의 Use Case를 비교 분석하여 제안하는 DRM의 기능과 성능을 평가하였다.

1. OMA DRM

2000년도 초, 인터넷의 급속한 확산과 온라인 음악 및 e-Book의 전자상거래가 새로운 디지털 콘텐츠 산업의 수익원으로 부상하게 되자 많은 DRM 제품이 시장

에 출시되게 되었다. 그러나 DRM 업체들은 각각 고유한 기술을 이용하여 제품을 내놓았기 때문에 제품의 호환성이 제공되지 않았다. DRM 제품 간의 상호호환성이 갖추어 지지 않고서는 시장의 활성화가 어렵다고 판단되어 DRM 표준화를 위해 많은 국제적 표준화 단체들이 설립되었다. 대표적인 곳이 MPEG-21, OMA(Open Mobile Alliance), OeBF(Open e-Book Forum), SDMI(Secure Digital Music Initiative) 등이 있다. 여러 표준화 단체들 중에서 DRM 표준기술 사양의 개발을 위해 현재 OMA와 MPEG-21이 가장 활발한 활동을 보이고 있으며, 그 중 OMA에서는 OMA에서는 모바일 플랫폼을 기준으로 유통되는 무선 콘텐츠의 저작권 보호를 위해 3GPP에서 개발해 온 DRM 관련 기술 사양을 인수받아 2002년 6월 OMA DRM v1.0의 Candidate로 발표하였고, 현재 OMA DRM v2.0의 Candidate로 업데이트 되어있다[11]. 본 논문에서 제안하는 DRM 시스템과 비교분석 하기 위한 OMA DRM의 주요 기술적 요소로는 콘텐츠를 전달하기 위한 “Delivery Mechanism", 콘텐츠 암호화를 위한 "Content Format", 콘텐츠 사용권한을 명세한 "Right Express Language", 그리고 콘텐츠의 다운로드를 명세한 “Download"로 이다. OMA에서는 Forward-Lock, Combined Delivery, Separate Delivery라는 3가지 형태의 전송 방법을 지원하고 있다. Forward-Lock은 콘텐츠가 DRM 객체로 변환되어 전송되면, 해당 DRM 객체는 다른 곳으로 전송될 수 없다. Combined Delivery는 DRM 객체를 권리 객체와 미디어 객체로 분리하여 전송하는 방법이다. 하지만 DRM의 권리 객체는 다른 곳으로 재전송될 수 없다. Separate Delivery는 DRM 객체의 미디어 객체와 권리 객체가 별도의 방법으로 전송될 수 있다. 특히 미디어 객체는 다른 곳으로 제한 없이 재배포가 가능하다. 단, 콘텐츠의 사용을 위해 콘텐츠 공급자로부터 권리 객체를 다운로드 받아야만 한다. OMA에서는 기본적으로 Separate Delivery를 통해 미디어 객체와 사용권한 객체를 전송하고 있기 때문에, 미디어 객체를 암호화하기 위해 DRM Content Format(DCF)를 규정하고 있다. 이 DCF는 콘텐츠의 정보를 담고 있는 헤더부분과 원본 콘텐츠가 암호화된 보디부분으로 구성된다. 사용권한 객체를 명세하기 위해서 OMA에서는 Rights Expression Language)를 통해 명시한다. DRM 콘텐츠는 REL를 통해 명세된 권리 정보에 따라 이용되기 때문에, 권리 객체는 수정이 가능하거나 다른 곳으로 재배포가 되는 것을 차단하고 있다. 또한 단순성과 효율성을

위해, 하나의 권리 객체는 하나의 콘텐츠를 참조하도록 제한되고 있다. 복합 객체를 위해서는 권리 객체가 각각의 개별 요소들에 대하여 직접적으로 명세한 경우에서만 적용될 수 있다.

2. Use Cases

본 절에서는 사용자 시나리오를 이용하여 소비자들이 넓은 범위의 콘텐츠에 접근하는 형태의 서비스를 설명하고 이를 OMA DRM v2.0과 제안하는 DRM에 적용하고 비교를 한다. 주어진 예들은 특정한 콘텐츠 공급자나 사용자들과 관계되어 있지 않으며, 앞으로 사용자가 DRM으로 보호되는 콘텐츠를 이용하는데 실제적으로 도움이 되는 방법을 제공하기 위함이다. 어떤 Use Case는 특정한 비즈니스 모델에 국한될 수 있고, 다른 어떤 Use Case는 확장된 비즈니스 솔류선이 반영된 시나리오로 이끌 수 있을 것이다. 즉 본 절에서는 OMA DRM v2.0과 제안한 DRM이 제공하는 기능에 대해 더 나은 이해를 제공하고, 그 성능을 비교·분석하는데 있다.

가) Use Case : OMA DRM v2.0[12]

OMA DRM v2.0의 Use Case는 사용자 시나리오를 이용하여 콘텐츠 소비자들이 넓은 범위의 콘텐츠에 접근하는 형태의 서비스를 설명하고 있다. OMA DRM v2.0 Use Case에서 주어진 예들은 특정한 무선 사업자, 콘텐츠 제공자 또는 단말 제조업자와 관계되어 있지 않으며, 앞으로 사용자가 배포된 콘텐츠를 다루는데 실제적으로 도움이 되는 방법을 제공하는데 그 목적이 있다. 어떤 사용 예는 너무 어려울 것이고, 또는 특정한 비즈니스 모델에 국한될 수도 있으나 이것은 이전 솔루션 또는 확장된 비즈니스 솔루션이 반영된 시나리오로 이끌 것을 기대할 수 있다. 간단하게 이 부분의 목표는 첫째로 OMA DRM v2.0 에 제공되는 기능에 대해 더 나은 이해를 제공하기 위해서이고, 둘째로 OMA DRM v2.0의 공식적인 요구사항에서 요구되는 OMA 시나리오의 높은 레벨의 기술을 제공하기 위해서이며, 마

지막으로. OMA DRM v2.0이 무엇인지 설명하는 데 도움이 되는 공식적인 문서가 되기 위해서이다.

OMA DRM Use Case에 등장하는 조는 활동적인 10대로, 그녀는 실제 삶과 가상 현실 상에서 많은 친구들을 가지고 있고 그녀는 몇 개의 가상 커뮤니티에 속하며 그들과 경험을 나누기를 좋아한다. 실제 삶에서 그녀의 친구들과 같이 사회적으로 서로 즐거운 시간을 보내지만, 이메일이나 실시간 메시지 또는 단문메시지 같은 메시징 기술을 이용하여 만날 때 그들은 실제로 대화를 나눌 수는 없다. 그리고 조는 디지털 카메라를 포함한 다양한 형태의 멀티미디어 저작 도구를 가지고 있고, 이를 이용하여 정지 영상이나 동영상을 제작할 수 있다. 그녀는 그녀 자신이 콘텐츠 제공자가 되어 그녀의 친구에게 제작한 콘텐츠를 보내거나 인터넷 홈페이지에 등록하길 원한다. 또한 그녀는 현재 사용 중인 멀티미디어 콘텐츠가 있으며, 이는 서로 다른 콘텐츠 공급자로부터 구입한 것이다.

1) Scenario 1 : 다양한 장치에서 콘텐츠 사용하기

조는 DRM 적용된 MP3를 그녀의 모바일 폰을 통해 구입하고 다운로드 한다. 또한 MP3를 자신의 DRM 호환 포터블 뮤직 플레이어로 복사한다. 그녀는 MP3를 구입할 때 다른 멀티미디어 재생 장치에서도 사용할 수 있는 권한을 포함하여 구입하였을 때에만 다양한 장치에서 MP3를 사용할 수 있다. 그리고 DRM 호환 여부 및 구매 조건에 따라 한 순간에 단 하나의 재생 장치에서만 MP3를 사용할 수 있거나, 여러 재생 장치에서 동시에 MP3를 사용할 수 있다.

2) Scenario 2 : 다른 사용자를 위한 RO 구입

조는 좋은 MP3를 사용하고 나서 이것을 자신의 어머니에게 보내기를 원한다. 그녀는 MP3를 배포한 콘텐츠 공급자로부터 사용권한(RO)를 구입한다. 그녀의 어머니는 콘텐츠 공급자로부터 MP3와 RO를 함께 전달받고 사용한다.

3) Scenario 3 : RO와 콘텐츠의 재 발급

조는 사고로 DRM이 적용된 MP3를 구입한 그녀의 모바일 단말기를 떨어뜨렸고, 그녀는 모바일 단말기를 교체하는 과정에 있다. 그리고 그녀의 모바일 단말기 및 MP3에 대한 보증 기간이 남아 있다. 모바일 단말기에서 그녀의 인증 정보 및 사용권한 정보는 안전한 장소 (Smart Card 등)에 저장되어 있으므로 인증 정보 및 사용권한 정보는 손상되지 않았고, 이를 새로운 단말기로 옮긴후 기존에 구입한 MP3와 이에 대한 사용권한을 다시 사용할 수 있다.

4) Scenario 4 : 서비스 제공자로부터 DRM 콘텐츠와 RO를 백업

조는 여러 개의 DRM 콘텐츠와 관련 사용권한이 있는 그녀의 무선 단말기를 분실하였고, 새로운 단말기를 구입하였다. 그리고 그녀의 DRM 콘텐츠에 대한 보증 기간이 남아 있다. 새로운 단말기에는 그녀에 대한 새로운 정보만 설정이 되지만, 콘텐츠 공급자는 그녀에게 제공한 콘텐츠 발급 기록을 유지하고 있기 때문에 그녀는 콘텐츠 공급자를 통하여 이전에 구입했던 DRM 콘텐츠와 이에 대한 사용권한을 다운로드 할 수 있다. 하지만 단말기 외부에서 내부의 사용권한 상태 정보를 저장할 수 있는 특별한 방법이 없기 때문에, 콘텐츠 공급자는 부정한 수단으로 사용할 가능성이 있는 분실된 단말기에 대한 인증을 취소할 수 있다.

5) Scenario 5 : 콘텐츠와 RO의 사용자 백업

조는 외부 저장소와 연결이 가능한 모바일 단말기를 보유하고 있다. 그녀는 구입한 DRM 콘텐츠와 이에 대한 사용권한을 외부 저장소에 백업을 한다. 그 후, 그녀는 자신의 모바일 단말기가 고장이 나서 새로운 단말기로 교체를 한다. DRM 콘텐츠와 이에 대한 사용권한의 보증 기간이 남아 있어 백업한 저장소로부터 DRM 콘텐츠와 사용권한을 복원한다. 이전 단말기에 사용했던 사용권한에 대한 정보를 확인할 수 없기 때문에 그녀는 새로운 사용권한을 발급 받고, 부정한 수단으로 사용할 가능성이 있는 기존 단말기에 대한 인증을 취소한다.

6) Scenario 6 : 사용자가 만든 콘텐츠의 보호

조는 직접 콘텐츠(사진, 동영상 등)를 작성하고 그것을 친구에게 보내려고 한다. 그러나 그녀는 친구 외에 다른 누군가에게 자신이 제작한 콘텐츠가 유포되는 것을 원하지 않는다. 그녀의 단말기는 콘텐츠에 "forward lock"으로 패키징하여 전송할 수 있는 기능을 제공한다. 콘텐츠 전송은 구체적이진 않지만 여기서는 MMS가 될 수 있다.

7) Scenario 7 : DRM 콘텐츠와 사용권한을 다른 DRM 시스템으로 전송

조는 OMA DRM 적용된 MP3를 구입하고, 그녀의 모바일 단말기에 다운로드하여 사용 중이다. 그리고 나서 다른 DRM 시스템이 적용된 MP3 재생 장치를 통해 이 MP3를 사용하고자 한다. 조는 이를 위해 다음과 같은 과정을 거칠 수 있다. 그녀는 다른 DRM 시스템이 적용된 MP3 재생장치에서 사용하기 위해 MP3와 이에 대한 사용권한을 복사 방지가 적용된 스트리밍 저장소로 옮긴다. 이제 조는 자신의 소유한 무선 재생장치를 통해 스트리밍 저장소로부터 MP3를 실시간 스트리밍을 통해 재생할 수 있다. 이러한 무선 재생장치의 예는 블루투스가 적용된 헤드폰이 된다.

8) Scenario 8 : 복합 콘텐츠 시나리오

조는 인기 있는 음악을 다운로드하기 위해 뮤직 서비스에 가입하고 음악, 가사, 이미지와 관련 링크가 포함된 패키지를 전송받는다. 그녀는 자신의 재생 장치로 이 패키지를 재생할 수 있다. 이 패키지를 위한 단일 사용권한은 각 개별 요소를 위해 다른 사용조건을 제공할 수 있다. 콘텐츠 공급자는 음악 시장 활성화를 원하기 때문에 가사, 이미지, 그리고 다른 정보는 무료로 사용할 수 있도록 할 것이며, 조는 이러한 정책을 통해 친구들과 공유할 수 있다. 구체적이진 않지만 패키지의 전송은 MMS가 될 수 있고, 패키지는 몇 가지의 콘텐츠를 포함하지만, 조는 오직 콘텐츠 패키지와 관련된 단일 사용권한을 가진다.

9) Scenario 9 : 기본 다운로드

조는 콘텐츠 공급자의 포탈 사이트에서 다운로드할 콘텐츠 결정하고 결재를 완료한 후, 콘텐츠를 다운로드 받고 이에 대한 사용권한을 다운로드 받는다. 이 후 그녀는 콘텐츠를 사용할 수 있으며, 콘텐츠 공급자에 의해 정의된 사용권한에서 벗어나는 콘텐츠에 대한 접근은 차단된다. 일반적으로 그녀가 사용할 수 있는 것은, 콘텐츠를 특정한 날짜까지 사용할 수 있는 사용 기간, 할당(누적)된 시간이나 횟수만큼 콘텐츠를 사용할 수 있는 사용 횟수/시간 이다.

10) Scenario 10 : 서비스 가입

조는 인터넷 음악 서비스 가입하고 음악 재생 기능과 저장 기능이 있는 자신의 모바일 단말기를 통해 접속한다. 조가 이용가능한 서비스는 음악 재생(정지, 다시 시작 등) 스트리밍 서비스와 음악 다운로드 서비스이다. 다운로드 서비스의 경우 모바일 단말기가 인터넷 연결 여부와 관계없이 서비스 가입이 가능하고, 다운로드 된 음악은 언제든지 사용이 가능하다.

11) Scenario 11 - 기본 스트리밍(실시간 재생)

조는 콘텐츠 공급자의 포털 사이트에 접속하고, 실시간 재생 방식으로 지원되는 뮤지션 그룹의 실황 콘서트의 재생을 원한다. 그녀는 실황 콘서트에 대한 콘텐츠 선택 및 요금 결재 과정을 완료하고 실시간 재생에 대한 정보와 이에 대한 사용권한을 모바일 단말기로 다운로드 한다. 여기서 사용권한은 전송되는 실시간 재생에 관련된 정보와 재생되는 콘텐츠에 대한 사용규칙(실행 횟수, 실행 시간 등)을 담고 있다. 이 후 그녀는 원하는 실황 콘서트를 자신의 모바일 단말기를 통해 관람할 수 있다.

12) Scenario 12 - 가입을 통한 멀티캐스트 스트리밍

조는 자신의 모바일 단말기를 통해 인터넷 라디오 서비스를 신청하고 이를 청취한다. 그녀는 여러 개의 멀티캐스트 라디오 채널을 선택할 수 있고, 그 채널에서 라디오 방송을 들을 수 있다.

13) Scenario 13 - 기존 DRM 시스템과의 호환성

조는 여러 콘텐츠 공급자들로부터 다양한 형태의 콘텐츠를 모바일 단말기로 다운로드 한다. 콘텐츠 공급자로부터 다운로드 받은 콘텐츠가 OMA DRM v1.0으로 보호된다면, 그녀의 모바일 단말기는 어떠한 문제도 없이 OMA DRM v1.0에 적용된 사용규칙에 따라 콘텐츠를 사용할 수 있다.

14) Scenario 14 - 미리보기 사용권한

Super-distribution를 통해 조는 처음으로 듣게 되는 뮤지션의 음악을 다운로드 받는다. 조는 미리보기 사용권한을 통해 그 음악을 한번 또는 일부분만 재생할 수 있다. 그 음악이 스트리밍 서비스를 지원할 경우, 음악 콘텐츠를 다운로드 함과 동시에 미리보기를 할 수 있다.

15) Scenario 15 - Super-distribution

조는 그녀의 모바일 단말기와 직접 연결이 가능한 방법(블루투스, IrDA, 케이블 연결 등)을 통해 그녀 친구의 모바일 단말기로 부터 DRM 콘텐츠를 다운로드 한다. DRM 콘텐츠 내부에는 이 콘텐츠에 대한 정보와 사용권한 발급 방법에 대한 정보가 있어, 이를 통해 그녀는 새로운 사용권한을 발급받을 수 있다. 이를 위하여, 다운로드 된 DRM 콘텐츠의 무결성을 확인해야 하고, 그녀의 단말기에서 사용가능한 DRM 콘텐츠인지 판단해야 한다.

16) Scenario 16 - 단말기 취소

콘텐츠 공급자는 조가 예전에 불법적인 방법으로 그녀의 친구들과 콘텐츠를 공유했었기 때문에 그녀가 새로운 콘텐츠를 얻는 것에 대한 제제를 원한다. 콘텐츠 공급자는 가입된 조의 단말기를 취소하여 더 이상의 DRM 콘텐츠나 사용권한을 제공하지 않는다.

17) Scenario 17 - 사용권한과 사용자 신원증명서의 묶기

조는 두 개의 모바일 단말기를 가지고 있으나 가입자 확인 모듈(Subscriber Identity Module, SIM)은 오직 하나의 폰에만 존재할 수 있기 때문에 그녀는 사용

을 원하는 폰에 SIM을 넣는다. 그 후 조는 두 개의 단말기에서 게임을 실행하고 싶지만, 같은 게임을 두 번 사는 것을 원하지 않는다. 그래서 조는 두 개의 단말기에 사용권한을 발급받고, SIM이 존재하는 단말기에서 게임을 실행할 수 있다. 만약 다른 사람의 SIM을 그녀의 단말기에 담았을 때에는 사용권한은 무시된다.

18) Scenario 18 - 자동적으로 갱신되는 사용권한

조의 모바일 단말기에서 사용권한이 만기가 되었다. 조는 이 사실을 모르고 그 사용권한을 통해 DRM 콘텐츠를 사용하고자 한다. 단말기의 DRM 관리모듈은 사용권한 만기를 그녀에게 통보하기 전 콘텐츠 공급자에게 이를 알리고 갱신을 요청한다. 콘텐츠 공급자가 이 갱신요청을 거절할 경우, DRM 관리모듈은 사용권한 만기와 새로운 사용권한의 구입을 통보한다.

19) Scenario 19 - 다른 콘텐츠 공급자로의 연결

조의 사용권한이 만기가 되었다. 그녀의 모바일 단말기는 콘텐츠 공급자를 통해 사용권한을 발급 받으려고 한다. 하지만, 콘텐츠 공급자는 이를 거절하고, 다른 콘텐츠 공급자의 연결 방법을 대신 통보한다. 조는 이 연결 방법을 통해 다른 콘텐츠 공급자와의 연결을 시도하고 새로운 사용권한을 발급받는다.

20) Scenario 20 - 깨진 DRM 솔루션

OMA DRM 솔루션은 DRM 표준으로 아주 널리 사용되고 있어서 보안상 해킹을 당하기 쉽다.. 콘텐츠 공급자는 모바일 단말기의 인증을 확인하고 DRM 콘텐츠 다운로드 시 블랙 리스트 작성을 위한 단말기 인증 정보(DRM 버전 정보,단말기 정보 등)를 추가함

21) Scenario 21 -다양한 암호화 방법에 관련한 동작

조는 OMA DRM에서 정의되지 않은 암호화 방식이 적용된 단말기를 사용한다. 콘텐츠 공급자는 암호화된 콘텐츠를 그녀에게 전달하기 전, 어떤 암호화 방식이 조의 단말기에서 사용될 수 있는지 알아낼 수 있다.

나) Use Case : 사용권한 재발급이 가능한 DRM 시스템

사용권한 재발급이 가능한 DRM 시스템에 대한 Use Case는 사용자 시나리오를 이용하여 OMA DRM에서 사용이 불가능한 서비스를 설명하기 위함이다. OMA DRM의 Use Case를 살펴보면 모든 사용권한은 콘텐츠 공급자가 발급하고 있다. 만약 콘텐츠 공급자가 사용권한을 발급할 수 없는 경우, 다른 콘텐츠 공급자를 통하여 사용권한을 발급하도록 되어 있다. 이는 소비자인 사용자와 콘텐츠 공급자 사이에 직접적으로 연결이 되어 있음을 의미하고, 이를 통하여 콘텐츠 공급자가 발급되는 사용권한에 대한 악의적인 접근 방지를 가능하게 하지만 사용자와 콘텐츠 공급자만이 연결되는 단순한 유통 모델만을 가능하게 하는 단점이 있게 된다. 좀 더 다양한 형태의 유통 모델을 지원할 수 있도록 하고, 사용자가 이 유통과정에 직접 참여가 가능하도록 하여 사용자 중심의 적극적인 콘텐츠 유통을 가능하게 하는 예를 보이는 것이 이 Use Case가 설명하기 위한 주된 목적이다.

OMA DRM의 Use Case와 마찬가지로, 사용자는 많은 친구들과 자주 연락을 주고받으며, 인터넷을 통해 다양한 멀티미디어 콘텐츠를 살펴보는 것을 좋아한다. 또한 그는 자신의 친구들이 자기가 좋아하는 것에 대해서 보여주는 것을 좋아한다. 그리고, 콘텐츠 공급자는 사진, 동영상, 음악, 게임, e-book 등 여러 가지 다양한 멀티미디어 콘텐츠를 제공하고 있다. 콘텐츠 공급자는 제공하는 콘텐츠에 대해서 좀 더 많이 팔릴 수 있는 방법을 연구하고 있다. 이를 위해 콘텐츠를 콘텐츠 공급자를 대신해서 판매하게 되면 그 판매에 대한 이익의 일부를 대신 판매한 사람에게 제공할 것을 결정하였다. 사용자는 이 사실을 알고 콘텐츠 공급자가 제공하는 콘텐츠들의 일부를 구입하여 자신의 친구들에게 직접 판매하고 이에 대한 이익을 콘텐츠 공급자로부터 분배받을 것을 기대한다.

1) OMA DRM Use Case에서 적용 가능한 시나리오

OMA DRM에서 사용자가 다른 사용자에게 DRM 콘텐츠나 사용권한을 전달할 수 있는 Use Case는 Scenario 2 : 다른 사용자를 위한 RO 구입이다. 하지만 이 Use Case의 경우에는 사용자가 콘텐츠와 해당 사용권한을 구입하여 콘텐츠 공급자로 하여금 다른 사용자에게 전달할 뿐이다.

2) Scenario 1 - 사용자가 사용권한을 콘텐츠 공급자를 통해 판매하는 경우

사용자는 판매에 대한 이익이 보장된 콘텐츠와 사용권한을 구입한다. 그리고 사용자의 친구들에게 Super-distribution을 통해 콘텐츠를 전달하고, 이에 대한 사용권한을 구입할 것을 홍보할 수 있다. 구입을 결정한 친구들의 사용권한 발급을 위해 사용자는 콘텐츠 공급자로 접속을 하고 구입을 결정한 친구의 정보(단말기 번호 등)를 전달하고 사용권한 발급을 요청한다. 콘텐츠 공급자는 사용자와 사용자 친구의 정보를 확인한 후 사용권한을 발급하고, 사용자에 대한 판매실적 정보를 보관한 후 이를 근거로 판매에 대학 이익을 분배한다.

3) Scenario 2 - 사용자가 사용권한을 직접 발급하여 판매하는 경우

사용자는 콘텐츠 공급자로부터 허가된 권한발급기를 자신의 단말기에 설치할 수 있다. 이 권한발급기를 통하여 사용자가 보유한 재발급이 허가된 사용권한을 복사하여 다른 사용자나 친구들에게 발급할 수 있다. 사용자에 설치된 권한발급기는 사용자가 권한발급을 시작할 때 콘텐츠 공급자로 발급정보를 전달하고. 이 정보를 근거로 하여 콘텐츠 공급자는 사용자에 대한 판매 이익을 분배하게 된다.

다) Use Case : 사용자 제작 콘텐츠를 위한 DRM 시스템

사용자 제작 콘텐츠를 위한 DRM 시스템에 대한 Use Case는 사용자 시나리오를 이용하여 OMA DRM에서 사용이 불가능한 서비스를 설명하기 위함이다. OMA DRM은 콘텐츠 공급자를 위한 DRM 시스템이며, 이를 위해 콘텐츠 공급자의 관점으로 DRM 시스템이 구성되어 있다. OMA DRM이 연구가 시작된 시기에는 특정한 콘텐츠 제작자가 제작한 콘텐츠는 특정한 콘텐츠 공급자만이 배포하고 판매를 하였다. 여기에서 벗어난 콘텐츠 배포는 모두 불법적인 콘텐츠 배포로 간주되었다. 하지만 인터넷의 발달과 멀티미디어 콘텐츠 저작도구들의 발달로 이제는 사용자가 직접 콘텐츠를 제작하고, 이를 배포하는 시기가 도래하였다. 기존의 OMA DRM에서는 이러한 사용자들이 제작한 콘텐츠에 대해서 저작권을 보호할 방법이 전무하다. 무엇보다 개인 사용자들을 위해서 콘텐츠를 암호화하여 배포하

거나 암호화된 콘텐츠에 대한 사용권한을 발급할 방법이 존재하지 않는다. 이제부터 설명하는 Use Case는 사용자 제작 콘텐츠를 위한 DRM 시스템이 어떠한 방법으로 콘텐츠를 암호화하고, 이를 배포하며, 이에 대한 사용권한을 발급하는지 보여준다. 이 Use Case를 통해 사용자가 제작한 콘텐츠에 대해서도 저작권을 보호하며, 무엇보다 DRM 시스템이 사용자의 사용을 제한하여 콘텐츠 공급자의 이익을 보장하는 것이 아닌, 사용자와 콘텐츠 공급자 모두를 위한 저작권 보호 시스템임을 보여주는데 그 목적이 있다.

OMA DRM의 Use Case와 마찬가지로, 사용자는 많은 친구들과 자주 연락을 주고받으며, 인터넷을 통해 다양한 멀티미디어 콘텐츠를 살펴보는 것을 좋아한다. 또한 그는 자신이 소유한 멀티미디어 저작도구를 이용하여 자기가 직접 사진을 찍고, 동영상을 만들며, 음악을 작곡하는 것을 좋아한다. 그리고 자신의 작품을 친구들에게 보여주는 것을 좋아하나, 모르는 사람들에게 배포가 되는 것을 원하지 않는다. 또한 특정 작품에 대해서는 그것에 대한 가치를 인정받길 원하고 이에 대한 증거로서 자신이 직접 해당 작품에 대해서 판매를 하기를 원한다. 콘텐츠 공급자는 이러한 사용자들의 욕구를 만족시키기 위해 사용자 제작 콘텐츠를 위한 서버를 구축하고 서버에 사용자들의 콘텐츠를 보관하고, 관리하며, 콘텐츠의 배포 및 판매를 도와줄 수 있도록 한다.

1) OMA DRM Use Case에서 적용 가능한 시나리오

OMA DRM에서 사용자가 제작한 콘텐츠에 대해 DRM을 적용시킬 수 있는 Use Case는 Scenario 6 : 사용자가 만든 콘텐츠의 보호의 경우이다. 여기서는 사용자의 단말기에 “foward lock” 기능이 담겨있어 사용자가 만든 콘텐츠를 암호화하고 암호화 정보를 같이 원하는 상대방에게 전달할 수 있다.

2) Scenario 1 – 사용자 제작 콘텐츠 암호화

사용자 제작 콘텐츠를 제작한 제작자는 콘텐츠 공급자가 제공하는 DRM 포탈 사이트에 가입을 하고 접속을 한다. 제작자는 사이트에서 제공하는 DRM Packager를 통해 콘텐츠를 암호화 할 수 있다. 암호화된 콘텐츠는 제작자가 원하는 상대방에게 e-mail이나 MMS를 통해 전달될 수 있다.

3) Scenario 2 - 사용자 제작 콘텐츠 서버에 등록 및 검색

제작자는 제작한 콘텐츠를 DRM 포털 사이트에 접속하여 암호화를 하고 이를 보관할 수 있다. 보관된 콘텐츠는 제작가 원할 때 다른 사용자에게 전달될 수 있으며, 포털 사이트 자체적으로 지원하는 검색 엔진을 통해 다른 사용자에게 검색 결과로 제공될 수 있다.

4) Scenario 3 - 사용자 제작 콘텐츠의 배포

사용자 제작한 콘텐츠의 배포를 원하는 제작자는 DRM 포털 사이트에 접속하여 암호화를 한 후 이를 판매 리스트에 등록한다. 등록된 콘텐츠는 인터넷 커뮤니티 게시판이나 포털 사이트에서 제공하는 검색엔진 등 여러 가지 방법을 통하여 다른 사용자에게 제공될 수 있다. Super-distribution을 통해 암호화된 콘텐츠는 자유롭게 배포가 가능하다.

5) Scenario 4 - 사용권한의 판매 및 발급

사용권한이 필요한 콘텐츠를 다운로드한 다른 사용자는 이를 사용하기 위해 DRM 포탈 사이트를 통해 사용권한의 발급을 요청하게 된다. DRM 포탈 사이트는 사용권한 발급이 필요한 콘텐츠의 정보를 확인하고 이에 대한 발급요청을 제작자에게 통보한다. 제작자는 DRM 포탈 사이트로 접속하여 사용권한을 직접 발급할 수 있다. 일련의 과정을 자동적으로 처리하기 위해 DRM 포탈 사이트는 미리 정의된 형태의 사용권한 발급정보를 저장한 후 이를 판매 리스트 형태로 사용자에게 제공할 수 있고, 사용자는 이 중 한가지를 선택하고 사용권한을 즉시 발급받을 수 있다.

6) Scenario 5 - 복합적인 시나리오

사용자 제작 콘텐츠를 위한 DRM 포탈 사이트가 사용권한의 발급에 다른 사용자의 참여를 허가하고 이에 대한 이익을 보장해 준다면, 사용권한 재발급이 가능한 DRM 시스템과 융합하여 다양한 형태의 유통·마케팅 모델을 적용할 수 있을 것이다.

라) Use Case : MMS를 위한 DRM 시스템

MMS를 위한 DRM 시스템에 대한 Use Case는 사용자 시나리오를 이용하여 MMS에 DRM이 필요한 이유를 설명하고 이에 대한 사용 예를 보여, 궁극적으로는 첨부되는 멀티미디어 콘텐츠에 대한 저작권 보호를 통하여 좀 더 다양한 형태의 멀티미디어 메시징 서비스가 가능하도록 하는데 있다. 3GPP에서 시작하여 현재 OMA에서 개발 중인 MMS는 첨부되는 멀티미디어 콘텐츠의 저작권 보호를 위하여 OMA DRM v1.0의 “forward lock", "combined delivery", "separate delivery"의 3가지 형태의 전달방법을 지원할 뿐이다. 이제부터 설명하는 Use Case는 MMS를 통해 콘텐츠를 배포하는 콘텐츠 공급자와 이를 사용하는 사용자 사이의 사용 예를 통하여 어떠한 방법으로 MMS에 첨부되는 멀티미디어 메시지의 저작권을 보호하는 지 보여준다.

사용자는 많은 친구들과 자주 연락을 주고받으며, 독특한 내용의 메시지를 작성하여 친구들에게 전달하고 그 반응을 살펴보는 것을 좋아한다. 그는 자신이 소유한 멀티미디어 저작도구를 이용하여 여러 가지 콘텐츠를 직접 만들어서 전송하곤 하지만, 전문적인 콘텐츠 제작자가 만든 콘텐츠를 자주 이용하고 있다. 콘텐츠 공급자는 MMS를 통하여 다수의 사용자를 위한 멀티미디어 콘텐츠를 제공하고 있다. 기본적으로 사용자는 모바일 단말기 내부로 직접적으로 접근하여 내용을 확인하는 것이 불가능하지만 여러 가지 방법을 통하여 불법적인 접근이 이루어지고 있고, 콘텐츠 공급자는 이러한 경우를 통해 자신의 멀티미디어 콘텐츠가 무단으로 사용되는 것을 원하지 않는다.

1) Scenario 1 - 콘텐츠의 등록 및 검색

콘텐츠 공급자는 MMS에 첨부 가능한 다양한 종류의 멀티미디어 콘텐츠를 제작하고 이를 MMS 서버에 등록을 한다. 콘텐츠의 저작권 보호를 위해 서버 등록 과정에서 콘텐츠는 암호화를 거쳐 보관이 된다. 등록된 콘텐츠는 사용자가 원할 때 다양한 방법으로 그 목록이 제공될 수 있다. 사용자는 주로 인터넷이나 모바일 단말기를 통해 MMS 서버에 접속하여 등록된 콘텐츠를 검색할 수 있고, 멀티미디어 메시지 작성에 이를 사용할 수 있다.

2) Scenario 2 - 멀티미디어 메시지의 작성

사용자는 첨부를 원하는 멀티미디어 콘텐츠를 선택하고 문자 메시지를 추가하여 멀티미디어 메시지를 완성한다. 작성이 완료되면, 전송을 원하는 상대방을 선택하여 MMS를 통해 작성한 멀티미디어 메시지의 전송을 시작한다.

.

3) Scenario 3 - 상대방 확인 및 콘텐츠 변환

MMS 서버는 사용자로부터 멀티미디어 메시지를 받고 상대방의 정보를 확인한다. 만약 상대방이 사용자가 작성한 멀티미디어 메시지의 재생이 불가능한 모바일 단말기를 보유한 경우, 상대방 모바일 단말기에서 재생이 가능한 형태로 멀티미디어 메시지의 변환을 시작한다. 변환이 완료되면 MMS 서버는 상대방에게 멀티미디어 메시지의 도착을 알리는 단문 메시지를 통해 수신 확인을 수행한다.

4) Scenario 4 - 멀티미디어 메시지의 수신 및 사용권한 발급

사용자 제작한 콘텐츠의 배포를 원하는 제작자는 DRM 포털 사이트에 접속하여 암호화를 한 후 이를 판매 리스트에 등록한다. 등록된 콘텐츠는 인터넷 커뮤니티 게시판이나 포털 사이트에서 제공하는 검색엔진 등 여러 가지 방법을 통하여 다른 사용자에게 제공될 수 있다. Super-distribution을 통해 암호화된 콘텐츠는 자유롭게 배포가 가능하다.

5) Scenario 5 - 사용권한의 판매 및 발급

멀티미디어 메시지를 수신한 상대방은 멀티미디어 메시지를 확인하기 위하여 다음과 같은 두 가지 방법을 선택할 수 있다. 상대방은 MMS 서버에 접속하여 멀티미디어 메시지 재생에 필요한 사용권한을 발급받는다. 혹은, 상대방은 멀티미디어 메시지가 도착함과 동시에 함께 첨부된 사용권한을 이용하여 즉시 재생이 가능하다. 전자의 경우 멀티미디어 메시지의 재생을 위한 사용권한은 상대방이 구입을 해야 하고 후자의 경우는 사용자가 멀티미디어 콘텐츠를 선택할 때, 이에 대한 사용권한을 함께 구입하여 전달하는 경우이다.

5) Scenario 6 - 응용 가능한 MMS 서비스

정기 구독이 가능한 멀티미디어 콘텐츠나, 모바일 매거진, 모바일 신문 등 콘텐츠 공급자에 의해 서비스가 제공되고 사용자가 이를 받아보는 단방향 서비스의 경우 사용자는 두 가지 방법으로 이 서비스를 제공받을 수 있다. 사용자는 서비스에 가입하고 이에 대한 결재를 수행하고 서비스를 제공받는다. 암호화된 멀티미디어 콘텐츠를 사용하는데 필요한 사용권한은 멀티미디어 메시지에 같이 첨부되어 전달이 된다. 혹은 사용자는 서비스에 가입을 하였지만 결재를 수행하지 않았다. 콘텐츠 공급자는 멀티미디어 콘텐츠를 제공하고 사용자는 이를 확인할 수 있지만 그 내용을 완전히 확인하기 위해서 사용자는 콘텐츠 공급자로부터 사용권한을 발급받아야 한다.

6) Scenario 7 - 복합적인 시나리오

MMS를 위한 DRM 시스템이 사용자 제작 콘텐츠를 위한 DRM 포탈 사이트에서 콘텐츠 전송을 위해 사용된다면, 콘텐츠를 배포하고, 이에 대한 사용권한을 전달하는데 좀 더 다양한 형태의 배포·마케팅 모델을 적용할 수 있을 것이다.

3. 고찰

제안된 DRM 시스템은 OMA DRM 시스템을 근본으로 하여 OMA DRM에서 예측할 수 있는 여러 가지 문제점을 보안하고, 현재 엄청난 속도로 확산되고 있는 사용자 제작 콘텐츠에 대하여 저작권을 보호할 수 있는 방안을 제안하였으며, 이러한 콘텐츠들이 전송될 때 사용될 수 있는 MMS에 대해서도 DRM을 적용하여 MMS에 첨부되는 멀티미디어 콘텐츠에 대해서도 저작권 보호를 가능하게 한다. 특히 MMS에 대한 DRM은 사용자들이 직접 제작한 콘텐츠에 대한 DRM이 아닌 MMS 서비스를 통하여 수익을 얻으려는 멀티미디어 콘텐츠 공급자를 위한 DRM으로서, 기존 MMS 시스템의 변경을 최소로 하고 DRM을 적용시키는데 그 중점을 두었다. 이에 대한 성능을 확인하기 위해 기존 OMA DRM v2.0에서 제공하는

Use Case를 분석하고, 제안하는 DRM 시스템에 적용 가능한 Use Case를 확인하였다. 이를 통해 OMA DRM v2.0에서 직접적으로 다루기 어려운 여러 가지 부분들을 제안하는 DRM 시스템들을 통해 보완이 가능한 것을 확인할 수 있었다. 하지만 제안하는 DRM 시스템들이 완전한 DRM 시스템으로 완성하기 위해서는 부족한 점이 많이 보인다. 무엇보다 콘텐츠에 대한 보호 방법, 사용권한 작성 및 발급에 대한 방법, 콘텐츠와 사용권한의 전달 방법 등에서 보완해야할 점이 나타나 있다. 이러한 점을 최소로 하기 위해, 본 연구에서는 기본적으로 OMA DRM의 규격을 준수하는 형태로 연구를 진행하였고 OMA 규격을 벗어나는 부분에 대해서는 각 장에서 자세하게 정리를 하였다. 이를 통하여 3가지 형태의 서로 다른 DRM 시스템이 제안되었고, 사용 목적에 따라 별개의 DRM 시스템으로 혹은 두 가지 시스템이 융합된 컨버전스 형태의 DRM 시스템으로 구현이 가능할 것이다. 본 논문에서 목표로 삼는 DRM 시스템은 다양한 비즈니스 모델과 다양한 형태의 사용권한 요구를 충족시킬 수 있는 DRM 시스템이다. 또한 개인 사용자에 대한 DRM이 요구가 되고 있는 시점에서 제안한 DRM은 하나의 길잡이가 될 것이라 기대한다.

Ⅴ. 결론

DRM 시스템은 콘텐츠의 저작권 보호를 가능하게 하는 시스템이다. 이를 위해서 콘텐츠를 암호화하여 안전하게 보호하고, 암호화된 콘텐츠를 사용하기 위해서 사용 규칙이 담긴 객체를 콘텐츠 공급자가 발급하고 사용자가 이를 받아 사용하도록 되어 있다. 암호화된 콘텐츠는 자유롭게 배포될 수 있고, 보안 공격으로부터 버틸 수 있도록 강인성을 갖고 있다. 사용 권한에 담겨있는 다양한 사용규칙을 통하여 콘텐츠 공급자는 하나의 콘텐츠에 대한 여러 개의 각기 다른 가격정책을 결정할 수 있고, 조금 더 나아가 사용자가 직접 가격을 결정하고, 결정된 가격에 맞는 사용권한을 발급받을 수도 있게 된다. 또한 자기가 가지고 있는 다른 콘텐츠 재생 장치에도 사용권한의 변경 없이 그대로 사용할 수 있게 되고, 가족이나 친구처럼 같은 Domain으로 구성되어 있는 경우 내가 보유한 콘텐츠를 다른 사람에게, 다른 사람이 보유한 콘텐츠를 내가 사용하는데 제약 없이 가능하다. 본 논문은 이러한 DRM의 기본 기능 외에 다양한 비즈니스 모델 적용을 위하여 사용권한이 재발급이 가능하도록 DRM 시스템을 설계하였고, 사용자게 제작한 콘텐츠에 대한 저작권 보호를 위하여 일괄적으로 이를 보호할 수 있는 DRM 시스템과 차세대 메시징 서비스로 떠오르는 MMS에 대해서도 DRM을 적용시킬 수 있는 방안에 대하여 연구하였다. 제안한 DRM 시스템은 사용권한을 재발급 할 수 있도록, 사용자가 사용권한 요청을 대신 할 수 있는 ROAP를 제안하였고, 콘텐츠 공급자로부터 인증된 사용자에 대해서는 사용권한을 발급할 수 있는 Rights Issuer에 대하여 연구하였다. 이를 통하여 사용자는 다른 사용자에게 콘텐츠를 판매할 수 있고, 이에 대한 수익을 기대할 수 있으며, 좀 더 전문적으로 콘텐츠를 팔려고 하는 사용자는 콘텐츠 공급자로부터 인증 받은 Right Issuer를 통하여 자신이 직접 콘텐츠에 대한 사용권한을 발급할 수 있게 된다. 콘텐츠 공급자만이 아니고 일반 사용자에 대해서도 가상 DRM 서버를 통한 사용자 제작 콘텐츠를 보호하는 DRM 시스템에 대해 연구하였고, 이를 통합적으로 관리하는 관리자 시스템을 통하여 사용자 제작 콘텐츠에 대한 등록, 검색, 사용 권한 발급 등이 효율적으로 관리될 수 있도록 연구하

였다. 또한 기존 MMS 시스템의 변경을 최소로 하면서 동시에 DRM이 가능한 MMS DRM 시스템을 위하여 DRM의 필수 요소인 DRM Server, DRM Packager, DRM Agent를 통해 콘텐츠 공급자로부터 제공되는 MMS에 첨부되는 멀티미디어 콘텐츠에 대한 저작권 보호를 가능하게 한다.

본 논문은 기존 DRM이 가지고 있는 제한적인 유통 시스템과 사용 규칙을 보다 다양하고 자연스럽게 바꾸는데 그 목표를 두고 연구를 하였다. 사용자에 의해 사용권한의 재발급이 가능한 DRM 시스템, 가상 DRM 서버, MMS DRM을 통하여 기존 DRM의 약점을 보완할 수 있기를 기대하고 있고 향후, 유비쿼터스 시대에서 사용가능한 그리고 적용 가능한 DRM 시스템 연구를 위하여, 또한 아날로그 콘텐츠를 이용하는 것과 동일한 디지털 콘텐츠의 이용을 보장하기 위한 DRM 시스템에 대한 연구에 중점을 두고 진행할 것이다.

참 고 문 헌

· 논문에 직접 인용한 문헌
· [1] DRM Working Group, http://www.digicaps.co.kr
· [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] Open Mobile Alliance, 2006.3, "Enabler Release Definition for DRM V2.0 Approved Version 2.0", http://www.openmobilealliance.org
· [4] Open Mobile Alliance, 2006.3, "DRM Content Format Approved Version 2.0", http://www.openmobilealliance.org
· [5] Open Mobile Alliance, 2006.3, "DRM Specification Approved Version 2.0", http://www.openmobilealliance.org
· [6] Open Mobile Alliance, 2006.3, "DRM Rights Expression Language Approved Version 2.0", http://www.openmobilealliance.org
· [7] AllExperts: Multi-level marketing: Encyclopedia. http://experts.about.com/e/m/mu/Multi-level_marketing.htm
· [8] Open Mobile Alliance, 2005.10, "MMS Architecture Candidate Version 1.3", http://www.openmobilealliance.org
· [9] 3rd Generation Partnership Project, 2005.3, "3GPP TS 22.140 V6.7.0; Technical Specification Group Services and System Aspects; Multimedia Messaging Service (MMS); Stage 1 (Release 6)", http://www.3gpp.org
· [10] 위윤희 "SMS에서 MMS로 가는 길", 한국콘텐츠학회논문지, Micro Software, http://www.imaso.co.kr/?doc=bbs/gnuboard_pdf.php&bo_table=article&page=3&wr_id=735&publishdate=20030701
· [11] 한국정보처리학회, 2004.2, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구"
· [12] Open Mobile Alliance, 2006.3, "OMA DRM Requirements Approved Version 2.0", http://www.openmobilealliance.org

· 논문을 작성하는데 참고한 문헌

· Open Mobile Alliance, 2006.3, “Enabler Release Definition for DRM V2.0 Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2006.3, “DRM Architecture Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2006.3, “OMA DRM Requirements Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2006.3, “DRM Rights Expression Language Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2006.3, “DRM Specification Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2006.3, “DRM Content Format Approved Version 2.0“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, Enabler Release Definition for MMS Candidate Version 1.3“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, “MMS Architecture Candidate Version 1.3“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, “MMS Requirements Candidate Version 1.3“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, “Multimedia Messaging Service Client Transactions Candidate Version 1.3“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, “MMS Conformance Document Candidate Version 1.3“, http://www.openmobilealliance.org
· Open Mobile Alliance, 2005.10, “MMS Message Template Specification Candidate Version 1.3“, http://www.openmobilealliance.org
· 3rd Generation Partnership Project, 2005.3, "3GPP TS 22.140 V6.7.0; Technical Specification Group Services and System Aspects; Multimedia Messaging Service (MMS); Stage 1 (Release 6)", http://www.3gpp.org
· 3rd Generation Partnership Project, 2005.6, "3GPP TS 23.140 V6.10.0; Technical Specification Group Core Network and Terminals; Multimedia Messaging Service (MMS); Functional description; Stage 2 (Release 6)", http://www.3gpp.org
· 3rd Generation Partnership Project, 2005.3, "3GPP TS 26.140 V6.2.0; Technical Specification Group Services and System Aspects; Multimedia Messaging Service (MMS); Media formats and codecs (Release 6)", http://www.3gpp.org

- Nair, S.K., Popescu, B.C., Gamage, C., Cripso, B., Tanenbaum, A.S., 2005, " Enabling DRM-preserving Digital Content Redistribution", Proceedings of 7th International IEEE Confer-ence on E-Commerce Technology 2005, Munich Germany (2005)
- Hartung, F., Ramme, F., 2000.11, "Digital Rights Management and Watermarking of Multimedia content for M-commerce Applications", IEEE Com. Magazine
- M. Gilbert, 2001.11, "What's Cool, What's Hot : Content Technology Hype Cylce", Gartner
- M. Gilbert, 2001.9, "Emerging Technologies for Managing Content", Gartner
- Susan Feldman, 2001.8, "Document and Content Technologies Market Forecast and Analysis Summary 2000-2005", IDC
- Eric F. Goodness, 2001.10, "Content Delivery Networks : Planning a Professional Servicess Portfolio", Gartner
- Radha Vichare, 2002.4, "Content Networking : Content Caching Forecast and Analyiss, 2001-2006", IDC
- Whitepaper, 2001.4 "An Overview of Digital Rights Enforcement and MediaRightsTM Technology", Elisar Software Corporation
- Ant Allan, 2001.11, "Digital Rights Management Software : Perspective", Gartner
- Joshua Dahl, 2001.6, "The DRM Landscape : Technologies, Vendors, and Market", IDC
- A. Wientraub, 2001.7, "Content Management Providers : Timetable Toward DRM", Gartner
- 강호갑, 2006.02, "[표준기술동향] DRM(Digital Rights Management)", TTA 저널 제103호
- 강호갑, 2001.3 "DRM을 이용한 컨텐츠 불법사용방지시스템 구축 방안", KIEC, 정기간행물2001년 3월호(통권28호)
- 이창열, 2002.07, "DRM(Digital Rights Management)", TTA저널 제82호
- 이승제, 2005.04, "[표준기술동향] OMA 표준화 동향 - OMA DRM", TTA 저널 제98호
- 지경용, 조은진, 고중걸, 2000.12, "CDN의 현재와 미래", ETRI, 기술경영연구시리즈 00-10
- 한국정보처리학회, 2004.2, "DRM 최신 국제표준 기술사양 분석 및 세계 유명 제품 동향과 전망에 관한 연구"

URL :

- AllExperts: Multi-level marketing: Encyclopedia. http://experts.about.com/e/m/mu/Multi-level_marketing.htm
- 위윤희, “SMS에서 MMS로 가는 길”, 한국콘텐츠학회논문지, Micro Software, http://www.imaso.co.kr/?doc=bbs/gnuboard_pdf.php&bo_table=article&page=3&wr_id=735&publishdate=20030701
- 홍승표, 정현수, “컨텐츠(Content) 기술 및 시장 동향”, http://kidbs.itfind.or.kr/ITWRD/ITWorld/et3-7.htm*

감사의 글

이 학위 논문이 결실을 맺기까지 많은 분들의 도움이 있었습니다. 이 논문을 위하여 저에게 부족한 점과 나아가야할 방향을 제시해 주시고 논문이 마무리 될 때까지 꾸준한 관심을 가져주신 도양회 교수님께 제일 먼저 감사함을 전하고 싶습니다. 그리고 이 논문을 완성할 수 있도록 아낌없는 지원과 배려를 해주셨던 고성택 교수님, 제주디지털콘텐츠협동연구센터를 통해 DRM에 대한 공동 과제를 수행하면서 처음 뵙게 된 이후 저에게 여러 가지를 가르쳐주시고 잘못된 부분을 지적해 주셨던 좌정우 교수님, 제가 제주대학교 대학원에 들어올 수 있게 되었고, 그 이후에도 꾸준히 저에게 관심을 가져주시고 보아주신 이광만 교수님, 실험 수업 조교라는 인연으로 저에게 많은 시간을 같이 해주셨던 김경연 교수님과 강민제 교수님, 수치해석 부분에서 많은 것을 가르쳐 주셨던 김경식 교수님, 신호와 시스템 관련된 많은 지식을 강의해 주신 고석준 교수님, 제가 고민하는 부분을 언제나 쉽게 해결할 수 있도록 도움을 주셨던 김호찬 교수님, DRM과제를 수행하면서 언제나 저의 의지가 되었던 부창진 선배님, 같은 연구실에서 매일 얼굴을 마주보며 언제나 내 말을 잘 따라주었던 형찬이와 혁이, 마지막으로 제가 집에 없음에도 언제나 저를 믿고 제가 건강하기를 매일 기도하고 계신 어머님, 부족한 나를 언제나 믿고 따라주었던 동생들, 힘들때면 언제나 나의 말벗이 되어주었던 나의 친구 왕석이, 나에게 언제나 배려를 해주며 양보해주었던 나의 친구 운용이, 이 자리에서 모두 이야기를 할 수 없지만 언제나 저를 잊지 않는 여러 친척분들과 나의 절친한 친구들, 이 모든 분들이 있었기에 지금의 제가 있을 수 있었고, 부족한 저이지만 이렇게 논문을 완성하게 되었습니다. 이 분들에게 감사히 마음을 전하고자 합니다.

이에 만족하지 않고 언제나 노력하는 모습으로 언젠가는 저를 지켜주었던 모든 분들에게 제가 받았던 것 이상을 다시 되돌려 드릴 것을 다짐하면서 논문의 마지막을 마무리 하겠습니다.

2006. 12.

양 동 혁 드림