韓國 컴퓨터情報學會 論文誌
第12卷 第3號, 2007. 7.

2007-12-3-1-7

홈 도메인에서의 콘텐츠 재배포를 위한 DRM 시스템 설계

문주영*, 이창보**, 김정재***, 전문석**

Design of DRM System for Contents Redistribution in Home Domain

Ju-Young Moon*, Chang-Bo Lee**, Jung-Jae Kim***, Moon-Seog Jun**

요 약

본 논문에서는 콘텐츠 재배포가 안전하게 이루어질 수 있는 홈 도메인 기반의 DRM 시스템을 제안하였다. 이 시스템은 사용자의 콘텐츠 사용상의 제약과 불편을 해소하면서 동시에 콘텐츠 제작자 및 제공자의 권익을 보호할 수 있는 홈 도메인 내의 콘텐츠 재배포를 위한 DRM 시스템이다. 가정의 디지털 장치를 이용하여 콘텐츠를 자유롭게 사용할 수 있도록 디바이스 상호간의 콘텐츠 재배포가 가능하도록 홈 도메인을 구축한다. 즉, 홈 도메인에 등록된 디바이스는 해당 도메인의 다른 디바이스에게 콘텐츠를 재배포 할 수 있고, 그의 재배포 내역을 DRM 서버에게 전송함으로써 콘텐츠 사용료에 대한 지불을 합리적으로 할 수 있다. 또한 이 시스템은 디바이스의 콘텐츠 재배포 권한을 도메인 내로 엄격히 제한함으로써 불법 재배포를 방지 할 수 있다.

Abstract

In this paper, we proposed the DRM(Digital Rights Management) system that allows to redistribute contents safely based on home domain. This DRM system for contents redistribution within home domain can solve the restriction and the inconvenience occuring in using contents and at the same time protect the right of contents producer and provider as well. To play contents using home digital device, we must build home domain for contents redistribution among devices. That is to say, devices that are registered with home domain can redistribute contents to other devices at same domain. The domain must send redistribution-specifics to DRM server, so that user can pay reasonable amount for using the contents. Futhermore, by restricting within domain the right of contents redistribution, one can strictly prohibit the illegal redistribution.

▸ Keyword : 저작권 보호(DRM), 홈 도메인(Home Domain), 디바이스 인증(Device Authentication), 콘텐츠 재배포 (Contents Redistribution), 라이선스 재패키징 (License Repackaging)

• 제1저자 : 문주영
• 접수일 : 2007.6.15, 심사일 : 2007.7.8, 심사완료일 : 2007. 7.20.
*부천대학 전산정보처리과
**숭실대학교 대학원 컴퓨터학과
***(주) RetailTech

Ⅰ. 서 론

최근 음악, 동영상, 이미지, 출판물 등 디지털 콘텐츠의 유통이 오프라인 환경에서 뿐 만 아니라 온라인 환경에서도 활발하게 이루어지고 있다. 이는 디지털 기술의 발전에 힘입어 고품질의 디지털 콘텐츠를 제작할 수 있게 되고, 초고속 인터넷, 무선 인터넷, 디지털 방송 등의 다양한 인프라의 형성에 기인한다. 이러한 디지털 유통의 환경 변화에 따라 사용자의 디지털 콘텐츠의 수요도 급격히 증가하고 있다. 이에 따라, 디지털 콘텐츠에 대한 제공자의 권리와 이익을 안전하게 보호하며 불법 복제와 유통을 막을 수 있는 방법이 필요하게 되었고, 암호화 기술을 기반으로 한 디지털 저작권 관리 (DRM : Digital Rights Management) 기술이 등장하였다[1]. DRM 기술은 콘텐츠의 불법 복제를 방지하고 사용 허가를 얻은 사용자에게 일정 범위 내에서 콘텐츠를 사용하게 하여 디지털 콘텐츠의 안전하고 투명한 유통을 가능하게 한다. 그러나 DRM 기술이 업체별 독자적인 기술 규격을 사용함에 따라 아직까지는 DRM 상호 호환성이 보장되지 못하고 있다[2]. 이로 인해 사용자가 자신이 소유하고 있는 여러 장치에서 콘텐츠를 사용하고자 할 때 불편함이 따를 수 밖 에 없다. 또한 미국의 InterTrust 사에서 제안한 Superdistribution 기술은 콘텐츠의 사용을 위하여 콘텐츠 뿐 아니라 콘텐츠의 라이선스를 함께 필요로 한다[3]. 이에 따라 사용자가 자신이 소유한 여러 장치에서 콘텐츠를 사용할 때 각 장치마다 별도로 라이선스 발급을 위한 인증 철차를 받아야 한다는 문제점이 발생한다.

본 논문에서는 불법 복제 및 유통으로부터 디지털 콘텐츠를 보호하면서, 사용자의 콘텐츠 사용을 위한 편의성을 높일 수 있는 프레임 워크를 제안하였다. 이는 홈 도메인을 생성하여 각 장치를 도메인에 등록한 후, 장치 상호간에 상호 인증을 거쳐 콘텐츠를 재배포하여 사용할 수 있도록 한다. 이때 콘텐츠의 재배포 범위를 도메인 내로 철저히 제한하여 불법 재배포를 방지하고, DRM 서버가 도메인 내의 재배포 내역을 보고 받아 도메인의 콘텐츠 사용료 지불을 요청하게 된다.

Ⅱ. 관련 연구

본 장에서는 라이선스와 콘텐츠의 분배를 분리하여 서로 다른 채널을 통해 전달하는 방식을 적용한 DRM 시스템의 구조, 라이선스 구조, 그리고 홈 도메인 내의 콘텐츠 전송 시스템에 대하여 살펴본다.

2.1 DRM 시스템의 구성

콘텐츠를 라이선스와 서로 다른 채널을 통해 전달하는 방식을 적용한 시스템으로, 라이선스 인증 및 분배를 위한 DRM 시스템은 〈그림1〉과 같다. 디지털 콘텐츠 보호와 사용 규칙 관리 및 사용료 체계 관리 구조로 구성된다.

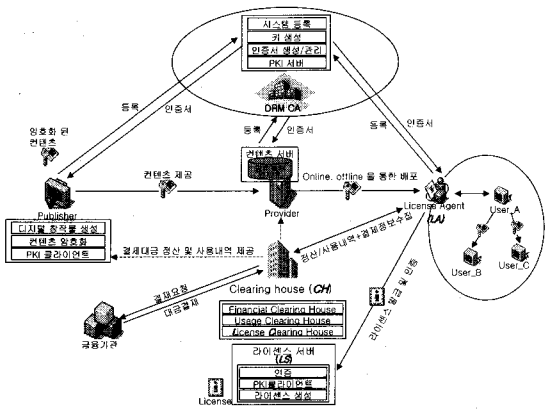

그림 1. DRM 시스템 구성도
Fig 1. Schematic diagram of DRM system

각 DRM 시스템의 참여자 즉 콘텐츠 출판업자, 콘텐츠 제공자, 사용자는 DRM CA에 공개키를 등록하고 인증서를 발급받는다. 콘텐츠 출판업자는 콘텐츠 제공자에게 콘텐츠를 암호화하여 전송하고, 콘텐츠 제공자는 암호화된 콘텐츠를 온라인 또는 오프라인을 통하여 사용자에게 배포한다. 한편 사용자는 라이선스 없이 콘텐츠를 사용할 수는 없으므로, 라이선스 에이전트를 통해 라이선스 서버로부터 라이선스를 발급받아 콘텐츠를 사용하게 된다[4][5].

2.2 라이선스 구조

라이선스는 라이선스 일련번호 sn, 라이선스의 하드웨어 바인딩 정보 KID=H(DID‖LSID), 라이선스 발행 시간 date, 사용규칙 Usage rule 그리고 기타 정보인 Other_data를 포함한다. KID를 구성하는 DID는 사용자의 하드웨어 장치 ID, LSID는 라이선스 서버의 ID로서, 라이선스가 지정된 디바이스에서만 유효하도록 하기 위함이다. 또한, 라이선스의 파라미터를 라이선스 서버가 전자서명 하여 전달함으로써 라이선스의 무결성, 부인방지의 안전성을 확보한다[5].

$$License = \{sn,\ KID,\ date,\ c,\ Other\_data,\ SigLS(H(sn,\ KID,\ date,\ Usage\ rule,\ Other\_data))\}$$

2.3 홈 도메인 기반의 DRM 시스템의 기존 연구

홈 도메인 기반의 DRM 시스템은 가정에서 콘텐츠 이용이 가능한 각종 디바이스를 하나의 홈 도메인으로 구성한다[6]. 하나의 홈 도메인으로 등록된 디바이스들은 상호간의 인증과정을 거쳐 콘텐츠와 재패키징한 라이선스를 주고 받음으로써 홈 도메인내에서의 콘텐츠 배포가 가능하다[7].

2.3.1 시스템의 구성요소

홈 도메인을 위한 DRM 시스템의 구성요소는 크게 3가지로 나뉘며 전체 구조는 <그림2>와 같다.

HADM(Home Authorized Domain Manager)

: 홈 디바이스를 관리하는 장치이며, 홈 도메인 내에 새로운 디바이스를 추가하거나 특정 디바이스를 제거한다.

Active 디바이스

: DRM 서버로부터 직접 콘텐츠를 다운로드 받을 수 있는 디바이스로서, 라이선스를 재패키징할 수 있는 모듈을 가지고 있다.

Passive 디바이스

: DRM 서버로부터 직접 콘텐츠를 다운로드 받을 수 없으며, 비교적 제한된 처리능력을 가진 디바이스로 MP3 플레이어, 자동차 오디오가 이에 속한다.

2.3.2 도메인 생성

먼저, 홈 도메인을 관리하기 위한 HADM을 선택한다. HADM은 디바이스 키를 생성할 수 있고 라이선스를 재패키징할 수 있는 능력을 갖춘 디바이스이어야 한다.

HADM Agent에 의하여 도메인 ID를 생성한다.

도메인에 등록될 디바이스를 위한 Device Key를 최대 등록 가능한 디바이스 수만큼 미리 생성하여 Device Key Set을 구한다. 이때 Device Key는 AES 암호화 알고리즘으로 128bit Key로 생성한다. 그리고 각 Device Key마다 Domain Device Index(DDI)를 부여하고, 새로 등록된 디바이스에게 DDI와 Device Key Set을 전송한다.

도메인 내에서 디바이스의 추가, 삭제 등의 변경사항이 발생할 때마다 HADM은 DRM 서버에게 보고한다.

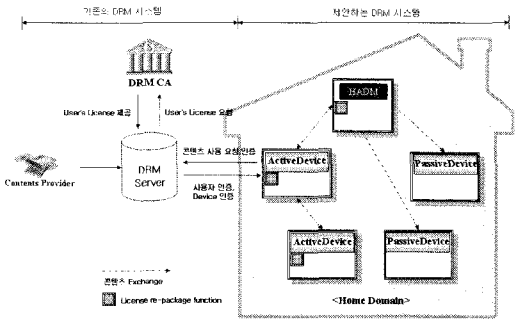

그림 2. 홈 도메인 기반의 DRM 시스템 구성도
Fig 2. Block diagram of DRM system based on home domain

2.3.3 디바이스 등록

도메인의 생성 후, 각 디바이스를 도메인에 등록한다. 디바이스 등록 세부과정은 <그림3>과 같다.

HADM은 등록할 Device로부터 Device ID(DID)를 전달받고, 디바이스에게 부여할 DDI와 미리 생성해놓은 Device Key Set을 비밀키 SK (H(noceHADM ‖ nonceD)로 암호화하여 전송한다.

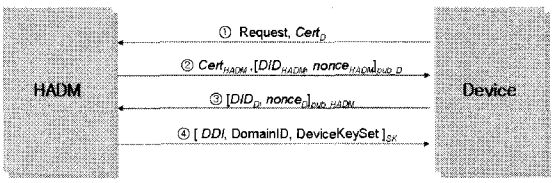

그림 3. 디바이스 등록 프로토콜
Fig 3. Protocol process for device registration

이러한 등록과정을 마치면, HADM에는 등록된 디바이스에 대한 DDI와 DID가 저장되고 등록된 디바이스에는 Domain ID, 자신의 DID, Device Key Set이 저장된다. 디바이스의 모든 등록 과정을 마치면, HADM은 DRM 서버에게 도메인 정보를 알린다.

2.3.4 디바이스 인증

디바이스가 DRM 서버로부터 다운로드받은 콘텐츠를 도메인내의 다른 디바이스에게 콘텐츠를 전송하고자 할 때, 디바이스 상호간의 인증 절차가 필요하다.

디바이스의 상호 인증 과정은 <그림4>와 같다. Device A가 Device B에게 콘텐츠를 전송하고자 할 때 Device A는 Device B와 같은 도메인 내에 속하는지 확인하기 위하여

Device B의 Domain ID를 받는다. Device A는 Device B가 자신과 같은 도메인에 속해 있음을 확인하고, Device B에게 Device B의 DID 정보에 맞게 재패키징된 라이선스와 콘텐츠를 보낸다.
상호인증을 마친 Device B는 Device A로부터 받은 콘텐츠를 사용할 수 있게 된다.

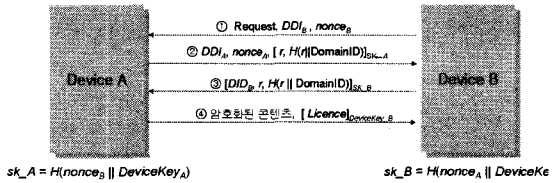

그림 4. 디바이스 인증 프로토콜
Fig 4. Protocol process for device authentication

III. 제안 시스템

II장에서 소개한 홈 도메인 기반의 DRM 시스템은 사용자의 편의성 측면에 중점을 둔 시스템으로서, 본 연구에서는 사용자 뿐 아니라 콘텐츠 제공자의 입장이 충분히 고려된, 즉 콘텐츠 제공에 대한 정당한 대가가 보장될 수 있는 홈 도메인상의 DRM 시스템을 제안하고자 한다.
또한, DRM 시스템의 도메인 관리 기능을 강화함으로써 콘텐츠 재배포에 대한 안전성을 높일 수 있는 시스템을 제안한다.

3.1 시스템 요구사항

본 논문에서 제안하는 시스템에 필요한 요구사항은 다음과 같다.
각 디바이스는 디바이스 인증기관으로부터 발급받은 디바이스 인증서와 개인키를 디바이스에 탑재한다[8].
홈 도메인 서버로 사용될 디바이스는 DRM 서버로부터 다운로드한 HADM Agent가 설치되어 있다.
각 디바이스는 DRM 서버로부터 다운로드한 DRM Agent가 설치되어 있다.
각 디바이스에는 고유한 디바이스 ID가 부여되어 있다.
인증서 및 키는 TRS(Temper Resistant Memory)로 보호하여 물리적인 공격으로 인한 인증서 및 키 유출을 방지하도록 한다.
제안하는 시스템은 홈도메인 서버로 사용될 디바이스를 제외한 모든 디바이스가 온라인으로 연결되어 있지는 않다고 가정한다.

3.2 시스템 모델

본 논문에서 제안하는 DRM 시스템은 II장에서 소개한 홈 도메인 기반의 DRM 시스템에서 몇 가지 기능을 개선한 모델로서, DRM 시스템 구성도는 <그림5>와 같다.

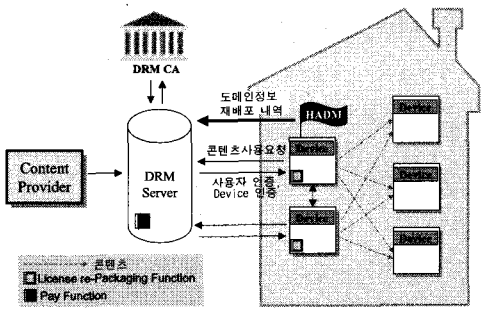

그림 5. DRM 시스템 구성도
Fig 5. Schematic diagram of DRM system

DRM 시스템의 주요 구성 요소는 다음과 같다.
HADM(Home Authorized Domain Manager)
: 홈 디바이스를 관리하는 장치로서[7], 홈 도메인 내에 새로운 디바이스를 추가하거나 특정 디바이스를 제거하고, 도메인 내의 유효한 디바이스 리스트를 관리한다. 또한 DRM 서버와 온라인으로 연결되어 있어 도메인 정보와 도메인 내의 디바이스 간 콘텐츠 재배포 내역 RDS(Re-Distribution Specifics)를 DRM 서버에게 전달한다.
디바이스
: 도메인 내에 속하며 직접 DRM 서버로부터 콘텐츠와 라이선스를 받거나, 도메인 내의 다른 디바이스로부터 받을 수 있다. 또한, 디바이스의 성능에 따라 콘텐츠 배포를 위한 라이선스 재패키징 모듈을 가지고 있어 다른 디바이스에게 콘텐츠를 재배포 할 수 있다.
DRM 서버
: DRM 서버는 콘텐츠 제공업자로부터 공급된 콘텐츠와 DRM 인증기관에서 발급한 콘텐츠의 라이선스를 사용자에게 배포한다. 또한 해당 도메인의 콘텐츠 재배포 내역을 HADM으로부터 보고받아 정산하여 도메인에게 결재를 요청할 수 있다.

3.3 시스템 동작

3.3.1 도메인 내에서의 콘텐츠 재배포

홈 도메인에 등록된 디바이스간의 콘텐츠 재배포 과정은 〈그림6〉과 같으며, 디바이스 상호 인증을 통하여 동일한 도메인 안에 있음을 확인하고 콘텐츠와 함께 재패키징된 라이선스를 요청한 디바이스에게 전달한다.

이때, 콘텐츠 사용료 지불 방식에 있어서 기존 시스템은 도메인에 등록할 수 있는 최대 디바이스 수에 따라 사용 금액을 책정하는 방식이었으나, 본 시스템에서는 도메인 내의 디바이스 상호간 콘텐츠 재배포 내역 RDS에 따라 사용 금액을 정산할 수 있도록 하였다. 이는 콘텐츠 제공자나 사용자 모두에게 있어서 합리적 지불 방식이기 때문이다.

따라서, 디바이스 B가 디바이스 A에게 콘텐츠 전송을 요청할 경우, 먼저 디바이스 B의 콘텐츠 재배포 내역 RDSB를 디바이스 A에게 보고해야만 콘텐츠를 전송받을 수 있도록 설계하였다. 이때 디바이스 A는 자신의 재배포 내역 RDSA에 디바이스 B로부터 받은 콘텐츠 재배포 내역 RDSB를 추가하여 갱신한다. 이를 통해 도메인 내에 있는 디바이스의 재배포 내역 RDS는 상위 디바이스에 집중되고, 상위 디바이스가 최종적으로 DRM 서버로부터 직접 콘텐츠를 전송받고자 할 때 수집된 도메인의 콘텐츠 재배포 내역 RDS를 DRM 서버에게 보고한다. 즉, 디바이스의 콘텐츠 재배포 내역 RDS는 〈그림7〉과 같이 상위 디바이스를 통하여 DRM 서버에게로 보고되고, DRM 서버는 Pay Function을 이용하여 해당 도메인의 사용 내역을 정산한다.

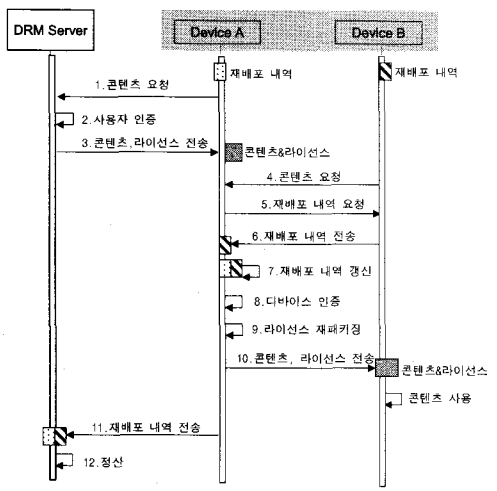

그림 6. 도메인에서의 콘텐츠 재배포 과정
Fig 6. Redistribution process of contents in domain

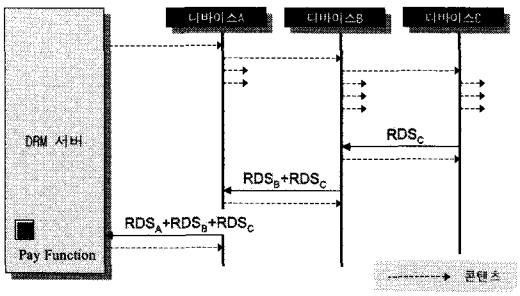

그림 7. 콘텐츠와 재배포내역 흐름도
Fig 7. Flowchart of contents and redistribution specifics

한편, 디바이스 상호 인증 세부 과정은 다음과 같다.

(1) $D_B \rightarrow D_A$: request content, DDI_B, $nonce_B$
(2) $D_A \rightarrow D_B$: DDI_A, $nonce_A$, $[r, H(r \| DomainID)]_{SK\_A}$
(3) $D_B \rightarrow D_A$: $[DID_B, r, H(r \| DomainID)]_{SK\_B}$
(4) $D_A \rightarrow D_B$: Request RDS_B
(5) $D_B \rightarrow D_A$: $[RDS_B, r, H(r \| RDSB)]_{DeviceKey\_A}$
(6) $D_A \rightarrow D_B$: 암호화된 콘텐츠, $[License]_{DeviceKey\_B}$

3.3.2 디바이스의 콘텐츠 불법 재배포 제한

홈 도메인 기반의 DRM 시스템에서 콘텐츠의 불법 재배포를 위협하는 요인을 지적하고 대안을 제시하고자 한다.

만일, 도메인 내의 다른 디바이스로부터 콘텐츠를 재배포 받아 사용하던 디바이스 A가 다른 도메인으로 이동하였을 경우, 디바이스 A는 새로운 도메인 내의 디바이스들에게 이전 도메인의 콘텐츠를 재배포할 수 있게 된다(〈그림8〉). 이는 불법 재배포에 해당되므로 이를 방지하기 위한 방안이 필요하다.

따라서 본 연구에서 제안하는 DRM 시스템에서는 라이선스 재패키징 과정을 보완하였다. 라이선스 재패키징은 콘텐츠를 재배포 받을 디바이스 정보에 맞게 처리하는 작업으로서, 이 과정에서 라이선스에 도메인 ID 정보를 추가하여 포함시키도록 한다. 도메인 내에서의 콘텐츠 재배포 시, 콘텐츠의 라이선스에 포함된 도메인 ID와 재배포받을 디바이스의 도메인 ID가 불일치하는 경우에는 콘텐츠의 재배포가 불가능하도록 처리한다.

이러한 방법으로, 도메인을 이동한 디바이스는 이전의 도메인에서 배포 받은 콘텐츠를 새로운 도메인내의 다른 디바이스에게 재배포할 수 없도록 한다.

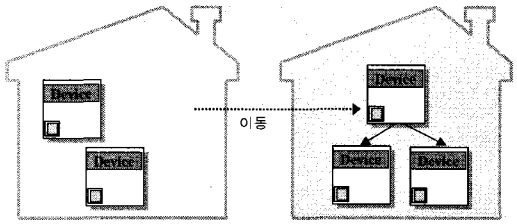

그림 8. 디바이스의 불법 재배포
Fig 8. Illegal contents redistribution of device

3.3.3 유효 디바이스 리스트 ADL (Accessible Device List)

도메인 내의 디바이스가 추가되거나 제거되면 디바이스 내의 다른 디바이스가 그 사실을 알아야 한다. 즉, 새로운 디바이스가 도메인 안에 추가된 경우, 새 디바이스에게 콘텐츠를 재배포 할 수 있어야 한다. 또한 디바이스의 물리적인 손상, 도난, 해킹, 이동 등의 여러 가지 이유로 인하여 도메인에서 디바이스가 제거 되었을 경우, 이미 제거된 디바이스에게 다시 콘텐츠를 재배포하는 일이 없도록 해야 한다.

따라서 도메인의 디바이스 구성이 변경되면 다른 디바이스들이 변경 내용을 알아야 하는데, 이는 유효 디바이스 리스트 ADL (Accessible Device List)의 관리로써 가능하게 된다. ADL은 HAMD에 의하여 갱신되며 수시로 DRM 서버에게 보고된다. 각 디바이스는 콘텐츠를 DRM 서버로부터 배포받거나, 도메인 내의 다른 디바이스로부터 재배포 받을 때, 최신 ADL을 전달받아 자신의 ADL을 갱신한다.

IV. 제안 시스템 평가

기존의 홈 도메인 기반의 DRM 시스템과 본 논문에서 제안한 시스템의 특성을 비교 분석하면 〈표1〉과 같다[7].

기존 시스템은 도메인을 이동한 디바이스의 불법 배포에 대한 고려를 하고 있지 않다. 이에 반해, 제안 시스템은 라이선스를 재패키징하는 과정에서 재배포 가능한 도메인 ID 정보를 포함시킴으로써 도메인 밖으로의 불법 재배포를 허용하지 않도록 하였다.

또한 기존 시스템은 콘텐츠의 사용료를 정산하는 방법에 있어서 도메인 구성 초기에 최대 몇 개의 디바이스로 구성할 것인가에 따라 콘텐츠의 사용료를 지불하도록 하고 있으나, 이는 콘텐츠 제공자나 사용자 모두에게 있어 합리적이지 못하다. 따라서 제안 시스템에서는 콘텐츠 재배포 내역 RDS에 따라 콘텐츠 사용료를 지불하도록 하는 방안을 도입하였다.

표 1. 기존 시스템과의 특성 비교
Table 1. The comparison of specific characters between DRM systems

	기존 시스템	제안 시스템
사용자 설치 모듈	Y	Y
라이선스 이동	Y	Y
저작권 보호	Y	Y
불법 배포 대책	N	Y
콘텐츠 사용료 지불 정책	도메인의 최대 가능한 디바이스 수	콘텐츠 재배포 건수

V. 결론

본 논문에서는 가정에서 사용하는 디지털 장치간의 콘텐츠 공유가 가능한 홈 도메인 내에서 콘텐츠 재배포를 위한 프레임 워크를 제안하였다. 특히 도메인 기반 시스템에서도 지속적으로 콘텐츠 저작권 보호가 이루어질 수 있도록 콘텐츠의 불법 배포를 방지할 수 있는 시스템을 제안하였으며, 또한 콘텐츠에 대한 사용 대가를 타당성 있게 지불할 수 있는 시스템을 제안하였다.

향후 과제로는 HADM이 디바이스 간의 상호 작용에 관한 정보를 체계적으로 관리하고 활용할 수 있는 방안이 필요하며, 도메인 간의 공모(Compromise)에 대한 검토가 필요하다.

참고문헌

[1] Joshua Duhl, "Digital Rights Management : A Definition," IDC 2001.

[2] Carlos Serrão, Victor Torres, Jaime Delgado, Miguel Dias, "Interoperability Mechanisms for registration and authentication on different Open DRM platform", IJCSNS International Journal of Computer Science and Network Security, VOL. 6 NO.12, Dec 2006

[3] Brad Cox, Superdistribution: Objects As

Property on the Electronic Frontier, Addision-Wesley, May, 1996.

[4] 김정재, 박재표, 전문석, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지 C, VOL. 12-C NO. 02 pp. 0183~0190 2005.04.

[5] 박복녕, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜," 한국정보과학회논문지 VOL.30 NO 02, pp 189~198, 2003.04.

[6] Natali. Helberger, Nicole, Dufft, Margreet Groenenboom, Kristóf Kerényi, Carsten, Orwat, Ulrich Riehm, "Digital rights management and consumer acceptability," A multi-disciplinary discussion of consumer concerns and expectations, State-of-the-art report, Amsterdam, pp.104 et seq..., 2004.

[7] 이창보, 김정재, 문주영, 이경석, 전문석, "홈 도메인에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계", 한국정보처리학회 논문지 C, VOL. 14-C NO. 03, 2007. 04

[8] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J. Kamperman, Andrew S. Tanenbaum "A DRM Security Architecture for Home Networks," Proc. 4th ACM Workshop on DRM, pp. 1-10, 2004.

저 자 소 개

문 주 영

1995년 : 동경농공대학교 전자정보공학과 공학석사
2000~ 현재 : 부천대학 전산정보처리과 조교수

이 창 보

2007년 : 숭실대학교 대학원 컴퓨터학과 공학석사
2007 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정

김 정 재

2005년 : 숭실대학교 컴퓨터학과 공학박사
2006 ~ 현재 : (주) RetailTech 수석 연구원

전 문 석

1989년 : University of Maryland Computer Science 공학박사
1991~ 현재 : 숭실대학교 교수