情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

공모에 대비한 홈 네트워크의 정보보호 관리

문주영*, 이창보**, 김정재***, 전문석**

요 약

본 논문에서는 사용자의 디지털 장치로 구성되어 있는 홈 네트워크에서 적용할 수 있는 DRM 시스템을 제안한다. 제안 시스템은 사용자의 편의성을 고려하면서 콘텐츠 소유자의 권익을 안전하게 보호하기 위한 DRM 모델로서, 특히 도메인 내의 디지털 장치의 공모(compromise)에 대비한 안전한 시스템을 제안하였다. 가정 내에서 사용할 수 있는 각 디지털 장치를 하나의 도메인에 등록시킴으로써, 도메인에 속한 장치 상호간에 디지털 콘텐츠를 전송하여 공유할 수 있다. 물론, 도메인 내에서 디지털 콘텐츠의 사용 내역을 수집하여 정당한 사용대가를 지불하게 된다. 본 논문에서는 도메인 외부로의 콘텐츠 불법 전송, 도메인에 등록되지 않은 장치의 위장 행위 그리고 도메인 내의 장치들의 공모 등의 안전성을 위협하는 요소에 대한 대응 방법을 제시함으로써 장치의 콘텐츠 전송 권한을 도메인 내의 합법적인 디바이스만 가지도록 엄격히 제한할 수 있도록 하였다.

Ⅰ. 서 론

최근 초고속 인프라가 보편화되면서 다양한 형태의 멀티미디어 콘텐츠의 유통이 급속히 활성화되고 있다. 영화, 음악, 도서 등 많은 주요 문화 콘텐츠와 정보 자산, 도서관, 지리 정보 등 다양한 생활 콘텐츠들이 디지털 형태로 서비스되는 디지털 콘텐츠 시대가 열렸다. 그러나 이러한 디지털 콘텐츠는 무한히 반복하여 사용해도 품질의 저하가 발생하지 않고 수정과 복사가 용이하며 통신망을 통해 대용량의 콘텐츠를 순식간에 전송할 수 있는 기술적 특성을 가지고 있다. 이러한 특성은 디지털 콘텐츠의 배포가 용이하여 손쉽게 콘텐츠를 이용할 수 있는 순기능을 제공하지만, 콘텐츠의 불법 복제로 인한 저작권 소유자들의 권익을 심각하게 위협하는 역기능을 야기하기도 한다. 이에 따라 디지털 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법 복제와 불법 유통을 막을 수 있고 체계적으로 콘텐츠를 관리할 수 있는 메커니즘이 필요하게 되었으며, 이를 위한 것이 암호화 기술을 기반으로 한 디지털 저작권 관리 (DRM: Digital Rights Management) 기술이다[1]. DRM은 전자책, 음악, 비디오, 게임 소프트웨어, 이미지 등의 각종 디지털 콘텐츠를 불법 복제로부터 보호하고 요금을 부가하여 저작권 소유자에게 발생하는 이익을 관리하는 메커니즘이며, 이제는 단순 보안 기술에서 보다 포괄적인 개념으로서의 저작권 승인과 집행을 위한 프로그램과 보안 기술, 지불, 결제 등의 포괄적 기능을 포함한다.

그러나 이러한 DRM 기술이 아직까지는 서비스별, 기기별, 업체별로 상이한 기술 규격을 사용함에 따라 다양한 표준들이 혼재되어 있으며, 디지털 콘텐츠의 이용이 서비스 종류, 기기, 또는 서비스 업체와 무관하게 투명성을 보장받을 수 있도록 DRM 상호 호환성을 위한 표준화 활동이 활발하게 이루어지고 있다[2]. 본 논문에서는 콘텐츠의 분리형 전달 방식을 적용한 DRM 시스템에 기반을 두고, 미국의 Intertrust 사에서 제안한 Superdistribution 기술[3]을 실현하는데 궁극적인 목표를 두고 있다.

본 제안 시스템은 도메인을 생성하여 각 장치를 도메인에 등록한 후 장치 상호간에 콘텐츠를 전송할 수 있는 구조를 가지며, 도메인내의 장치들은 상호 인증 프로토콜에 의하여 동일한 도메인에 속해 있음을 검증하는 절차가 포함된다. 또한 다른 장치에 콘텐츠를 전송하는 장치는 라이선스를 재패키징하여 콘텐츠와 함께 전송한

* 부천대학 전산정보처리과 (jym@bc.ac.kr)
** 숭실대학교 대학원 컴퓨터학과 (onsmile79@nate.com, mjun@computing.ssu.ac.kr)
*** (주) RetailTech (argniss@nate.com)

다. 이로써 도메인 내의 여러 장치가 동일한 콘텐츠를 사용하기 위하여 각 장치마다 별도로 라이선스 발급 절차를 밟는 불편을 해소할 수 있게 된다.

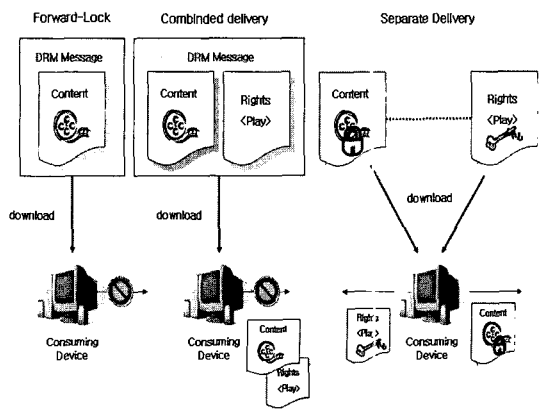
따라서 본 논문에서는 불법 복제 및 불법 유통으로부터 디지털 콘텐츠를 보호하면서, 사용자의 콘텐츠 사용을 위한 편의성을 높일 수 있는 프레임워크를 제안하고자 한다. 본 논문의 2장에서는 제안 시스템을 위한 기반 기술을 소개하고, 3장에서는 제안 시스템의 구조를 소개한다. 그리고 4장에서는 제안 시스템의 안전성을 분석하고, 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관련 연구

2.1. 콘텐츠 전달 방식

콘텐츠 전달 방식에는 〔그림 1〕과 같이 3가지 방법이 있다[4].

- 지정 전달(Forward-lock) : 디바이스에 전달된 콘텐츠가 다른 디바이스로 전송되지 않도록 하는 방식이다. Rights가 존재하지 않으며 사용자는 기본 사용 방침에 따라 콘텐츠를 이용한다.
- 혼합 전달(Combined delivery) : Rights object와 원본 콘텐츠가 함께 DRM Message의 형태로 패키징 된다. Rights object는 사용 권한에 대해 정의하며 CP/SP(Contents Provider/Service Provider)는 play, display, print, execute의 권한을 설정할 수 있다. 다운로드 된 콘텐츠 및 Rights object는 다른 디바이스에 전달될 수 없으며 최종 사용자는 DRM Content의 저장, 설치, 삭제 등을 할 수 있어야 한다.
- 분리형 전달(Separate delivery) : 콘텐츠와 Rights object가 서로 다른 채널을 통해 디바이스에 전달된다. 암호화된 콘텐츠는 다른 디바이스로 전달될 수 있지만, Rights의 전달은 불가능하며 콘텐츠를 전달받은 다른 디바이스의 사용자는 새로운 Rights를 발급받아야 한다. Separate delivery 방식은 콘텐츠를 구입한 사용자가 해당 콘텐츠를 제 3자에게 자유롭게 배포할 수 있게 함으로써 다양한 유통 채널을 제공하는 Superdistribution 기술을 가능하게 한다. PC 기반의 DRM 기술과는 달리 무선 단말기 플랫폼과 같은 폐쇄된 환경에서는 지정 전달 방식과 혼합 전달 방식만으로도 콘텐츠의 외부 유출로 인한 불법복제를 방지할 수 있었으나, 전체적인 디바이스의 성능 향상과 디바이스 간 통신이 가능해짐에 따라 분리형 전달 방식을 통해 콘텐츠의 기밀성을 증가시키려는 요구가 점차 증가하고 있다.



〔그림 1〕 콘텐츠 전달 방식

2.2. 라이선스 구조

라이선스는 라이선스 일련 번호 sn, 라이선스 발행시간 date, 사용규칙 Usage rule, 라이선스 하드웨어 바인딩 정보인 KID = H(DID||LSID)와 기타 필요한 정보를 포함한 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 전자 서명하여 전달함으로써 라이선스의 무결성, 부인방지를 확보한다[5][6].

License = {sn, KID, date, Usage rule, Other_data, SigLS(H(sn, KID,date, Usage rule, Other_data))}

Ⅲ. 제안 시스템 구조

본 장에서는 시스템 모델과 시스템 요구 사항에 대하여 소개한다. 그리고 본 시스템에서의 가능한 여러 공격

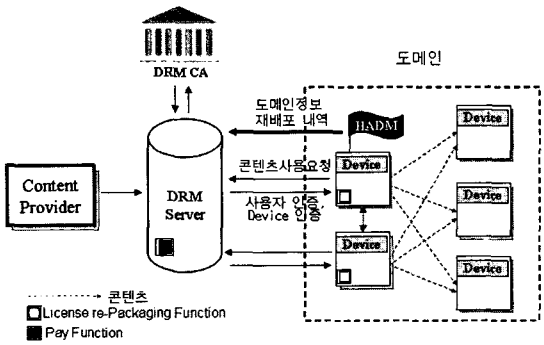
시나리오에 대하여 분석하여 그에 대한 안전한 시스템을 제안한다.

3.1. 시스템 모델

먼저 여러 디바이스를 사용하는 가정이나 소집단의 사용자는 도메인을 설정한다[7]. 등록된 디바이스는 도메인 내의 다른 디바이스에게 콘텐츠를 재패키징된 라이선스와 함께 보내줄 수 있다. 이는 디바이스 상호 인증 과정이 선행된다.

도메인을 위한 DRM 시스템의 구성 요소는 [그림 2]와 같이 크게 3가지로 구분된다.

- HADM(Home Authorized Domain Manager) : 디바이스를 관리하는 도메인 서버의 역할을 담당하는 장치로서, 도메인 내에 새로운 디바이스를 추가하거나 특정 디바이스를 제거한다. DRM 서버와 항상 온라인으로 연결되어 디바이스 추가, 제거 등의 변경 사항을 보고하고, 그 밖의 도메인 정보를 송신한다.
- 디바이스 : DRM 서버로부터 직접 콘텐츠를 다운로드 받거나, 도메인 내의 다른 디바이스와 콘텐츠를 주고 받을 수 있다. 특히 다른 디바이스에게 콘텐츠를 전송하기 위하여 라이선스 재패키징 모듈을 가지고 있다.
- DRM 서버 : DRM 서버는 콘텐츠 제공업자로부터 공급된 콘텐츠와 DRM 인증기관에서 발급한 콘텐츠의 라이선스를 사용자에게 배포한다. 또한 해당 도메인의 콘텐츠 전송내역 RDS(Redistribution Specifics)를 HADM으로부터 보고받아 정산하여 해당 도메인에게 결재를 요청한다.



[그림 2] 제안한 시스템 모델

3.2. 시스템 요구 사항

제안 시스템에 필요한 요구사항은 다음과 같다.

- 각 디바이스는 디바이스 인증기관으로부터 발급받은 디바이스 인증서와 개인키를 탑재한다[8].
- 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.
- 도메인 서버로 사용될 디바이스를 제외한 나머지 디바이스는 온라인으로 연결되지 않을 수 있다고 가정한다.

3.3. 시스템에 대한 위협 및 대책

3.3.1. 무효한 디바이스의 위장 행위

특정 디바이스가 도난, 해킹, 이동 등의 여러 가지 이유로 인하여 도메인으로부터 제거된 경우, 여전히 해당 도메인의 유효한 디바이스처럼 악의적인 행동을 할 수 있다. 이는 디바이스가 도메인에서 제거된 후에도 다음과 같은 정보를 가지기 때문이다.

- 자신이 속해 있던 도메인 ID
- HADM에 의하여 부여받은 고유한 디바이스 ID
- 도메인 내의 다른 디바이스와의 콘텐츠 전송을 위하여 사용했던 비밀키

또한, 제거된 디바이스가 유효한 다른 디바이스의 ID를 이용하여 상호 인증 과정에서 유효한 디바이스로 위장하여 행동할 수 있다.

따라서 제안 시스템에서는 다음과 같이 방어한다.

- 제거된 디바이스와 공유한 다른 디바이스의 비밀키를 갱신한다.
- 콘텐츠 전송을 위한 디바이스 상호 인증 과정에서 디바이스의 ID를 검증한다.
- HADM에 의하여 유효 디바이스 리스트 ADL (Accessible Device List)을 관리한다. ADL은 디

바이스의 제거 뿐 아니라 추가의 경우에도 갱신되어야 하며, DRM 서버에게 보고되고 각 디바이스에게 배포된다. 각 디바이스는 콘텐츠를 DRM 서버로부터 배포받거나, 도메인 내의 다른 디바이스로부터 콘텐츠를 전송받을 때 최신 ADL을 전달받아 자신의 ADL을 갱신한다.

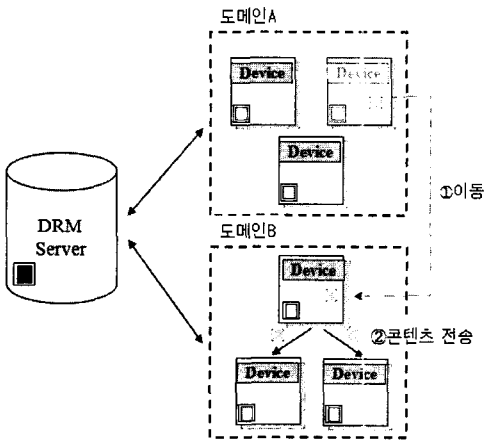
3.3.2. 다른 도메인으로 이동한 디바이스의 불법 전송

만일, 도메인 내의 다른 디바이스로부터 콘텐츠를 전송받아 사용하던 디바이스가 [그림 3]과 같이 다른 도메인으로 이동한 후, 새로운 도메인 내의 디바이스들에게 이전 도메인의 콘텐츠를 전송하려 할 수 있다. 이는 콘텐츠의 전송을 허가받지 않은 도메인에서 발생하는 콘텐츠의 불법 전송에 해당된다.

제안 시스템에서는 이에 대응하여 라이선스 재패키징 과정에서 도메인 ID 정보를 추가하여 라이선스에 포함시킴으로써, 라이선스의 도메인 ID가 전송받을 디바이스의 도메인 ID와 불일치하는 경우에 콘텐츠의 전송을 불가능하게 한다.

3.4. 안전한 시스템 구조

제안 시스템의 동작 과정은 도메인의 생성, 도메인의 디바이스 등록 그리고 디바이스 인증을 통한 콘텐츠 전송으로 구성되며, 도메인 내의 디바이스 구성 변경에 관하여 기술한다.



[그림 3] 다른 도메인으로 이동한 디바이스의 불법 전송

3.4.1. 도메인의 생성

도메인 생성 과정은 다음과 같다.

① 도메인을 관리하기 위한 HADM을 선택한다. HADM은 다수의 비밀키를 생성하고, 디바이스 정보의 암호화 작업을 위한 모듈을 가지며 라이선스를 재패키징할 수 있는 능력을 갖춘 디바이스를 선택해야 한다.

② HADM Agent에 의하여 도메인 ID를 생성한다.

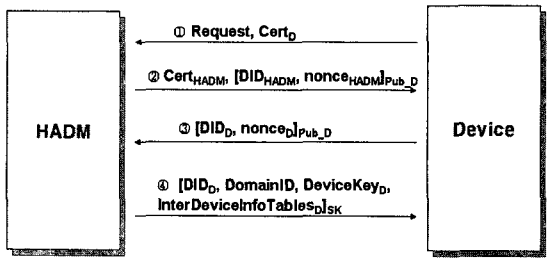
③ 각 디바이스에게 송신할 키 집합을 생성한다. 즉, HADM과 디바이스간의 통신을 위한 비밀키 DeviceKey, 도메인 내의 두 디바이스간의 통신을 위한 비밀키 집합 InterDeviceKeySet을 최대 등록 가능한 디바이스의 수만큼 미리 생성한다. 이때 DeviceKey와 InterDeviceKeySet은 AES 암호화 알고리즘의 128bit Key로 생성한다. 그리고 각 DeviceKey와 InterDeviceKeySet마다 Domain Device Index(DDI)를 부여하고, 새로 등록된 디바이스에게 DDI와 함께 DeviceKey와 InterDeviceKeySet을 전송한다.

3.4.2. 도메인 내에 디바이스 등록

도메인의 생성 후, 디바이스를 등록한다. 디바이스 D의 등록 과정은 [그림 4]와 같다.

①, ② 디바이스는 HADM에게 자신의 인증서 CertD와 함께 등록 요청 메시지를 보낸다. 그리고 HADM은 자신의 인증서 $Cert_{HADM}$와 함께 DID (Device ID), 난수 $Cert_{HADM}$를 디바이스의 공개키 pub_D로 암호화 하여 보낸다.

③ 디바이스는 자신의 DID와 난수 $nonce_D$를 HADM의 공개키 pub_HADM으로 암호화하여 보낸다. HADM과 디바이스는 $nonce_{HADM}$와 $nonce_D$를 연



[그림 4] 디바이스 등록 프로토콜

접하고 해쉬하여 비밀키 SK를 생성한다($SK=(H(nonce_{HADM} \| nonce_D)$).

④ HADM은 디바이스에게 부여할 DDI(Domain Device Index), DomainID, DeviceKey 그리고 미리 생성해 놓은 InterDeviceInfoTables를 비밀키 SK($=H(nonce_{HADM} \| nonce_D)$)로 암호화하여 전송한다. 이때, InterDeviceInfoTables는 InterDeviceKeySet과 EncryptedDeviceInfoSet으로 구성된다. InterDeviceKeySet은 디바이스가 도메인 내의 다른 디바이스와의 상호 인증을 위한 비밀키로서 통신을 위한 세션키를 생성하는데 사용된다. 또한 EncryptedDeviceInfoSet은 디바이스의 DDI (Domain Device Index), DID(Device ID)를 각각의 다른 디바이스의 DeviceKey로 암호화 한 데이터 집합으로서, 해당 디바이스가 다른 디바이스와의 상호 인증 과정에서 자신의 DDI를 검증받을 때 필요로 한다.

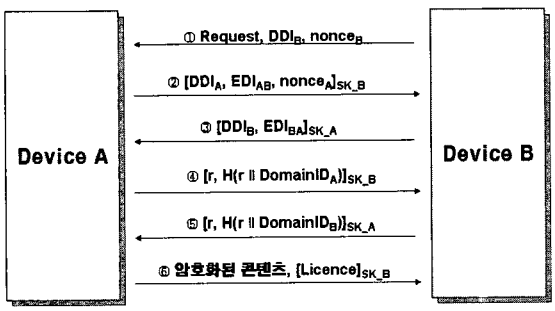
디바이스의 모든 등록 과정을 마치게 되면 HADM에는 Domain ID와 각 장치에 해당하는 DID, DDI, DeviceKey, InterDeviceInfoTables가 저장되고, 최종적으로 DRM 서버에게 자신의 도메인 정보를 알린다.

3.4.3. 디바이스 인증을 통한 콘텐츠 전송

DRM 서버로부터 콘텐츠를 다운로드받은 디바이스가 도메인 내의 다른 디바이스에게 콘텐츠를 전송하고자 할 때, 두 디바이스가 동일한 도메인에 속하는지 검증해야 한다.

이를 위한 디바이스 A와 B의 상호 인증 과정은 〔그림 5〕와 같으며 세부 내용은 다음과 같다.

① 디바이스 B는 디바이스 A에게 콘텐츠 요청 메시지와 함께 DDI_B(B의 Domain Device Index) 와 난수 $nonce_B$를 보낸다.



〔그림 5〕 디바이스 인증 프로토콜

② 디바이스 A는 디바이스 B에게 DDI_A, 난수 $nonce_A$ 그리고 EDI_{AB} (EncryptedDeviceInfo$_{AB}$: 디바이스 B의 DeviceKey로 암호화된 DDI_A와 DID_A)를 SK_B($=H(InterDeviceKey_{BA} \| nonce_B)$)로 암호화하여 전달한다.

③ 디바이스 B는 DID_B와 EDI_{BA}를 SK_A ($=H(InterDeviceKey_{AB} \| nonce_A)$)로 암호화하여 전달한다. 여기서 디바이스의 DDI를 검증한다.

④ 디바이스 A는 디바이스 B에게 r과 $H(r \| DomainID_A)$를 암호화하여 보낸다.

⑤ 디바이스 B는 $[r, H(r \| DomainID_A)]_{SK\_B}$ 를 복호화하여 디바이스 A가 같은 도메인 내의 디바이스인지 검증한다.

⑥ 디바이스 A 역시 디바이스 B로부터 전달받은 $[r, H(r \| DomainIDB)]_{SK_A}$를 복호화하여 디바이스 B가 같은 도메인에 속하는지를 검증한다.

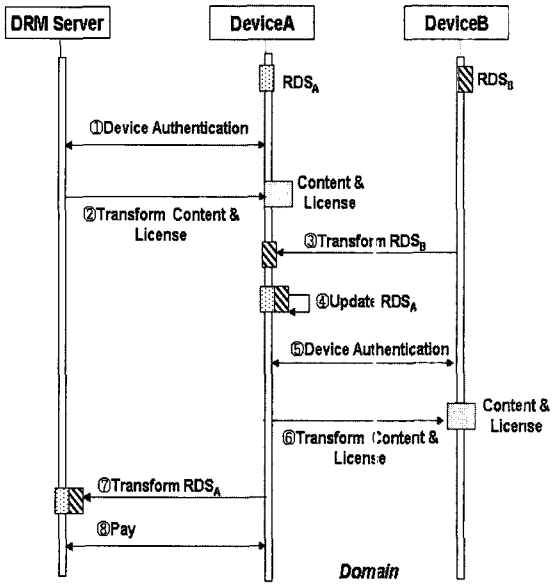
⑦ 디바이스 간에 상호 인증 과정을 성공적으로 마치게 된다. 디바이스 A는 디바이스 B에게 DRM 서버로부터 받은 암호화된 콘텐츠와 디바이스 B의 DID정보에 맞게 재패키징된 라이선스를 암호화하여 보낸다[9].

상호 인증 과정을 마친 후에 디바이스 B는 디바이스 A로부터 받은 콘텐츠와 라이선스로 콘텐츠를 사용할 수 있다.

3.4.4. 전송 내역 (RDS)

디바이스 간의 콘텐츠 전송 과정에서 〔그림 6〕과 같이 콘텐츠 전송 내역 RDS(Redistribution Specifics)를 전달한다. 이는 도메인 내에서의 콘텐츠 전송 내역이 최종적으로 DRM 서버에게 보고되어 해당 도메인의 콘텐츠 사용료를 정산하기 위함이다.

도메인 내에 있는 디바이스 간의 콘텐츠 전송이 이루어질 때마다 〔그림 6〕과 같이 RDS가 상위 디바이스에 집중되고, 상위 디바이스가 최종적으로 DRM 서버로부터 직접 콘텐츠를 전송받고자 할 때 수집된 도메인의 RDS를 DRM 서버에게 보고하게 된다. 디바이스 B가 디바이스 A에게 콘텐츠 전송을 요청할 경우, 먼저 디바이스 B의 RDSB를 디바이스 A에게 보고해야만 콘텐츠를 전송받을 수 있다. 이때 디바이스 A는 RDSA에 디



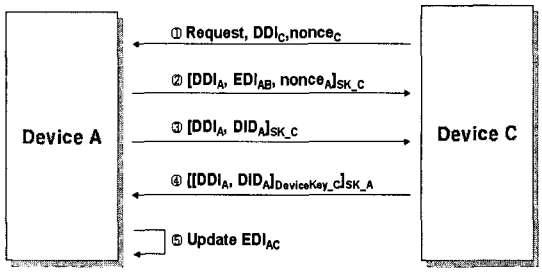
〔그림 6〕 콘텐츠 전송에 따른 전송내역(RDS)의 흐름

바이스 B로부터 받은 RDSB를 추가하여 RDSA를 갱신한다.

3.4.5. 도메인 내의 디바이스 추가 및 제거

도메인에 디바이스가 추가되거나 제거되면 디바이스 내의 다른 디바이스가 그 사실을 알아야 한다. 즉, 새로운 디바이스가 도메인에 추가된 경우, 새 디바이스에게 콘텐츠를 전송할 수 있어야 한다. 또한 디바이스의 물리적인 손상, 도난, 해킹, 이동 등의 여러 가지 이유로 인하여 도메인에서 디바이스가 제거되었을 경우, 이미 제거된 디바이스에게 콘텐츠를 전송하는 일이 없도록 해야 한다. 따라서 도메인의 디바이스 구성이 변경되면 다른 디바이스들이 변경 내용을 알아야 하며, 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 배포 받거나, 도메인 내의 다른 디바이스로부터 전송받을 때, 최신 ADL을 전달받아 자신의 ADL을 갱신한다.

또한, 디바이스의 추가 작업에서는 새롭게 등록된 디바이스의 DeviceKey가 갱신되기 때문에 도메인 내의 다른 디바이스 내에 저장되어 있는 새 디바이스의 EDI를 갱신된 DeviceKey로 재 암호화해야 하는 경우가 있다. 이는 제거된 디바이스의 DDI를 재사용 할 수 있지만 DeviceKey는 새로 생성하여 부여하는 데 기인하며, 새 디바이스가 제거된 디바이스의 DDI를 재사용할 때 발생한다. 이에 따라 갱신된 DeviceKey로의 재 암호화 작업이 필요하며, 이는 새롭게 추가된 디바이스가 다른 디바이스와의 첫 번째 상호 인증 과정에서 실행한다.



〔그림 7〕 새 디바이스의 EDI 갱신

제거된 디바이스 B의 DDI를 인계한 새 디바이스 C의 EDI가 디바이스 A에서 갱신되는 과정은 〔그림 7〕과 같으며 세부 내용은 다음과 같다.

① 디바이스 C는 디바이스 A에게 콘텐츠 요청 메시지와 함께 DDI_C와 난수 $nonce_C$를 보낸다. 이때, DDI_C는 제거된 디바이스 B와 동일한 DDI를 사용한 것으로 가정한다.
② 디바이스 C가 EDI_{AB}(제거된 디바이스 B의 비밀키로 암호화)의 복호화에 실패하면, ③에서 디바이스 C는 디바이스 A로부터 DID_A, DDI_A를 전달받는다.
④ 디바이스 C로 DeviceKey로 암호화하여 디바이스 A에게 전달한다.
⑤ 디바이스 A는 EDI_{AC}를 갱신한다.

Ⅳ. 시스템 분석 및 평가

4.1. 기존의 도메인 기반의 DRM 시스템과의 비교 분석

본 절에서는 기존의 도메인 기반의 DRM 시스템과 본 논문에서 제안한 시스템의 특성을 비교한다[10].

4.1.1. 타 도메인으로의 불법 전송 방지

기존 시스템에서는 디바이스가 악의적으로 타 도메인으로 불법 전송을 할 수 있다. 이는 특정 도메인에서

제거된 디바이스가 타 도메인으로 이동한 후 이전 도메인에서 전송받은 콘텐츠를 현재 디바이스에게 전송하게 되면 이는 불법 전송에 해당된다. 한편, 제안 시스템은 라이선스를 재패키징할 때 도메인 ID 정보를 라이선스 정보에 포함시킨다. 라이선스의 도메인 ID가 전송받을 디바이스의 도메인 ID와 불일치하는 경우에 콘텐츠의 전송이 불가능하도록 하였다. 이러한 방법으로 도메인을 이동한 디바이스가 다른 도메인 내의 디바이스에게 콘텐츠를 불법적으로 전송하는 것을 막을 수 있다.

4.1.2. 디바이스의 위장 행위 방어

기존 시스템은 각 디바이스의 비밀키 DeviceKey를 도메인 내의 다른 모든 디바이스에게 배포함으로써, 도메인에서 제거된 디바이스가 다른 유효한 디바이스로의 위장이 용이하였다. 이는 결국 콘텐츠의 불법 전송을 초래할 수 있다. 한편, 제안 시스템은 디바이스 상호 인증 과정에서 상대 디바이스에게 자신의 EDI를 보냄으로써 자신의 DDI를 검증받도록 하였으며, 이를 통하여 도메인으로부터 제거된 디바이스가 유효한 디바이스처럼 위장 행위 하는 것을 방지할 수 있다.

4.1.3. 콘텐츠 사용료 지불 방식

기존 시스템은 도메인 구성 초기에 최대 몇 개의 디바이스로 구성할 것인가에 따라 콘텐츠의 사용료를 지불하도록 하고 있으나, 제안 시스템에서는 콘텐츠 전송 내역 RDS에 따라 콘텐츠 사용료를 지불하도록 하는 방안을 도입하여 콘텐츠 제공자와 사용자 모두에게 합리적인 지불방안을 적용할 수 있다.

4.2. 시스템의 안전성 분석

제안 시스템은 제거된 디바이스의 위장 행위를 차단하고 다른 도메인으로 이동한 디바이스의 콘텐츠 불법 전송에 대한 방어를 함으로써 안전성을 확보하였다. 이는 도메인 내의 디바이스들의 악의적인 행동을 위한 공모에 대한 여러 가지 시나리오에 대하여 충분한 방어가 가능할 것으로 평가한다.

V. 결 론

본 논문에서는 가정에서 사용하는 디지털 장치간의 콘텐츠 공유가 가능한 도메인 내에서 콘텐츠 전송을 위한 프레임워크를 제안하였다. 특히 도메인 기반 시스템에서도 지속적으로 콘텐츠 저작권 보호가 이루어질 수 있도록 콘텐츠의 불법 전송을 방지할 수 있는 시스템을 제안하였으며, 특히 디바이스 간의 악의적인 공모(Compromise)에 의한 콘텐츠의 불법 전송에 대응할 수 있도록 하였다. 또한 콘텐츠에 대한 사용 대가를 타당성 있게 지불할 수 있는 시스템을 제안하였다.

향후 과제로는 HADM의 디바이스 간의 상호 작용에 관한 정보를 체계적으로 관리하고 활용할 수 있는 방안에 대한 연구이다.

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, pp.291-303, Dec 2006.

[3] Brad Cox, "Superdistribution: Objects As Property on the Electronic Frontier," Addision-Wesley, May 1996.

[4] Kevin Mowry, "*Digital Rights Management*", 5th Annual Wireless Java Conference, 2004.

[5] 김정재, 박재표, 전문석, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," *한국정보처리학회 논문지 C*, VOL.12-C, NO.02, pp.0183-0190, April 2005.

[6] 박복녕, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜," *한국정보과학회논문지*, VOL.30, NO.02, pp.189-198, April 2003.

[7] Natali Helberger, Nicole Dufft, Margreet Groenenboom, Kristóf Kerényi, Carsten Orwat, Ulrich Riehm, "Digital rights management and consumer acceptability," *A multi-disciplinary di-*

scussion of consumer concerns and expectations, State-of-the-art report, Amsterdam, pp.104 et seq..., 2004.

〔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.

〔9〕 Iwata. T, Abe. T, Ueda. K, Sunaga. H, "A DRM system suitable for P2P content delivery and the study on its implementation," Proceeding of the 9th Asia-Pacific Conference on Communications (APCC 2003), VOL.2, pp.806-811, 2003.

〔10〕 이창보, 김정재, 문주영, 이경석, 전문석, "홈 도메인에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계," *한국정보처리학회논문지 C*, VOL.14-C, NO.03, pp.221-228, June 2007.

〈著者紹介〉

문 주 영 (Ju-Young Moon)
정회원
1989년 2월 : 경희대학교 물리학과 졸업
1995년 3월 : 동경농공대학교 전자정보공학과 석사
2000년 8월 ~ 현재 : 부천대학 전산정보처리과 조교수
관심분야 : 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID

이 창 보 (Chang-Bo Lee)
학생회원
2005년 2월 : 숭실대학교 컴퓨터학과 졸업
2007년 2월 : 숭실대학교 대학원 컴퓨터학과 석사
2007 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정
관심분야 : DRM, RFID, 네트워크 보안

김 정 재 (Jung-Jae Kim)
정회원
1995년 2월 : 영동대학교 컴퓨터공학과 공학사
1999년 2월 : 숭실대학교 컴퓨터공학과 석사
2005년 2월 : 숭실대학교 컴퓨터학과 박사
2006년 ~ 현재 : (주) RetailTech 수석 연구원
관심분야 : 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID

전 문 석 (Moon-Seog Jun)
종신회원
1989년 : University of Maryland Computer Science 공학박사
1991년 ~ 현재 : 숭실대학교 교수
관심분야 : 전자상거래 보안멀티미디어 보안, 인증시스템