종단 사용자 디바이스간 도메인 기반 권한 정보 관리 기법

장경아° 이병래
삼성전자 시스템연구소
{kachang, byungrae.lee}@samsung.com

Rights Management Scheme for Domain Usage between the End-User's Devices

Kyung-Ah Chang° Byung-Rae Lee
System R&D Laboratories, Samsung Electronics

요 약

최근 논의되고 있는 디지털 홈 네트워크는 유무선 통신 프레임워크를 기반으로 사용자 디바이스간 다양한 정보 공유 및 멀티미디어 컨텐츠 교환의 활성화가 예상되며, 대부분의 사용자는 자신이 구입한 권한 정보를 가족 또는 친구 등과 공유 가능하게 할 수 있는 형태의 유연한 서비스를 요구하고 있다.

본 연구에서는 이러한 홈 네트워크 환경에 대해 사용자 소유의 디바이스로 구성된 도메인에서의 권한 정보 관리 기법을 제안한다. 제안한 기법은 정당한 사용자 도메인의 디바이스에 대해 보유하고 있는 권한 정보 한도 내에서 DRM 포맷에 독립적으로 해당 디바이스를 위한 권한 정보를 생성 및 기존 권한 정보의 상태 정보에 대한 업데이트를 수행하며, 이때, 사용자 디바이스의 성능을 고려하도록 하였다.

1. 서론

멀티미디어 기능이 강화된 사용자 디바이스(Device)의 보급이 일반화 되면서 벨 소리, 사진 및 그림, 동영상 등에 대한 유료 서비스가 확산되고 있으며, 이러한 서비스는 초기 복제 방지 기술을 기반으로 수행되었으나 현재 사용자의 권한 정보(Rights Object; RO)에 대한 유연성 및 편리성을 기반으로한 DRM (Digital Rights Management) 기술로 전환되었다.

DRM은 기본적으로 사용자간 암호화된 컨텐츠(Content)의 분배는 자유롭게 허용하며 해당 컨텐츠의 실행은 반드시 권한 정보를 구입한 이후 가능하도록 제어하고 있다. 이때, 암호화된 컨텐츠를 수신한 각 사용자는 자신의 권한 정보를 구입하여야 한다.

그러나, 최근 논의되고 있는 디지털 홈 네트워크(Home Network)는 유무선 통신 프레임워크를 기반으로 사용자 디바이스간 다양한 정보 공유 및 멀티미디어 컨텐츠 교환의 활성화가 예상되며, 대부분의 사용자는 자신이 구입한 권한 정보를 가족 또는 친구 등과 공유 가능한 형태의 유연한 서비스를 요구하고 있다.

본 연구에서는 이러한 홈 네트워크 환경에 대해 DRM 관련 OMA (Open Mobile Alliance) [1,2] 차기 표준안을 기반으로 확장하여 사용자 소유의 디바이스들로 구성된 도메인(Domain) [2,3]에서의 권한 정보 관리 기법을 제안한다.

제안한 기법은 정당한 사용자 도메인의 디바이스에 대해 보유하고 있는 권한 정보 한도 (Constraints) 내에서 DRM 포맷(Format)에 독립적으로 해당 디바이스를 위한 RO를 생성 및 기존 RO 상태 정보의 업데이트를 수행하며, 이때, 사용자 디바이스의 성능을 고려하도록 하였다.

2. 관련 연구

2.1 기존 DRM 서비스

일반적으로 DRM 기술[2]에 있어서 자유로운 분배가 가능한 암호화된 컨텐츠와는 달리 RO는 매번 암호화된 컨텐츠의 실행 시 요청되어 해당 서비스 제공자로부터

구입해야 하며 대부분 사용자의 디바이스에 바인딩(Binding) 되도록 한다.

이때, 사용자는 자신이 기 보유하고 있는 RO의 전달이 불가능하며, 정의된 권한 한도의 잔여 분에 접근이 불가능하여 사용자 소유의 다른 디바이스에서 컨텐츠 실행 시 이용할 수 없을 뿐만 아니라, 서비스 제공자에 대해 각 디바이스는 사용자의 기 보유하고 있는 RO에 해당하는 동일 컨텐츠의 실행을 위해서는 매번 새로운 등록 과정을 수행 및 RO 구입 과정을 진행해야 하는 등 제한적이다.

2.2 도메인(Domain) 메커니즘

현재 OMA DRM WG에서 정의된 표준안[2]에는 기본적으로 무선 환경에서의 DRM 지원을 위한 다양한 기술안과 더불어서 사용자가 보유하고 있는 다수의 멀티미디어 디바이스를 고려한 도메인 메커니즘을 정의하고 있다.

도메인 메커니즘[2,3,4]은 등록된 디바이스에 대해 도메인 키를 공유하고 컨텐츠와 함께 Domain RO를 다운로드하여 이후 도메인 정보를 보유하고 있는 디바이스에 대해 추가적인 다운로드 없이 컨텐츠를 사용하도록 한다. 이때 모든 멀티미디어 디바이스는 서비스 제공자와 사전 등록 프로세스를 완료한 상태이며, 새로운 디바이스의 추가 또는 등록 정보의 만료 시 해당 디바이스는 표준 등록 프로토콜을 수행하여야 Domain RO의 실행이 가능하다.

그러나, 이러한 도메인 메커니즘 역시 기존 DRM 시스템과 마찬가지로 서비스 제공자의 DRM 포맷과 이종의 DRM 솔루션이 설치된 사용자 디바이스의 서비스 참여 또는 해당 컨텐츠의 실행이 불가능하다.

3. 도메인 기반 권한 정보 관리 기법

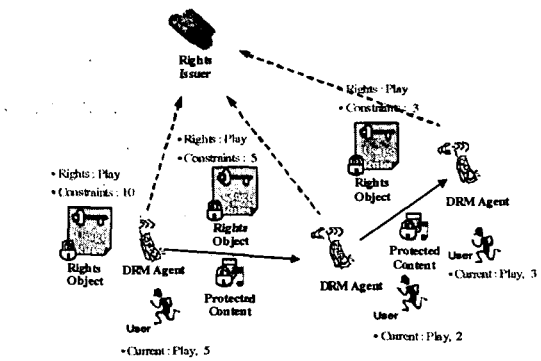
3.1 도메인 권한 정보 관리 기법

제안한 도메인 기반 권한 정보 관리 기법은 사용자가 다수의 멀티미디어 디바이스를 보유하고 있으며, 해당 디바이스는 고유의 DRM 솔루션 (DRM Agent)를 통해 Domain RO의 유효성을 검증한 후 컨텐츠 실행이 가능함을 가정하고 있다. 또한 도메인 서비스 수행 시 서비스 제공자 (Rights Issuer; RI)와의 등록 프로토콜 진행 및 이종의 DRM 솔루션이 설치된 디바이스에 대한 확장을 위해 NS (Network Storage)를 통한 Cross-domain 메커니즘을 구성하도록 하였다. 해당 도메인 권한 정보 공유 기법은 아래와 같이 동작한다.

사용자의 디바이스 A는 디바이스 B에게 DRM 보호된 컨텐츠와 A의 RO 저작 정보를 송부하는 것으로 서비스는 초기화 된다. 디바이스 B는 디바이스 A에게 컨텐츠 전송 허가 응답 및 자신의 공개키를 도메인 키로 암호화하여 전송하게 된다.

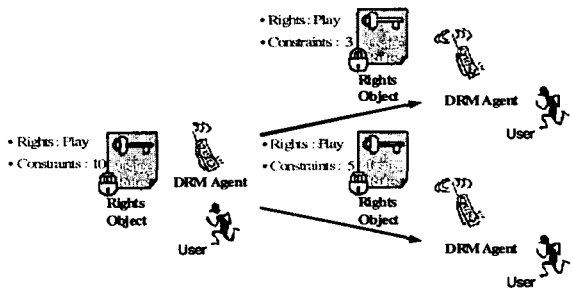
디바이스 A는 디바이스 B에게 암호화된 컨텐츠와 디바이스 A의 RO를 사용자가 원하는 형태로 저작하여 해당 결과를 서명하여 전송한다.

디바이스 B는 전송 받은 컨텐츠 및 서명을 검증하고 디바이스 A에게 응답을 전송한다 디바이스 A는 응답 메시지를 받은 후 디바이스 B가 해당 RO의 권한 한도 내에서 컨텐츠를 실행할 수 있다는 것을 파악할 수 있다.



<그림 1> 사용자의 도메인 권한 정보 공유 예시

사용자의 디바이스 전체에 대해 동일한 DRM 포맷으로 제어가 가능할 경우 아래의 과정이 수행된다.



<그림 2> 도메인 기반 권한 정보 공유 기법

[표 1] 프로토콜 기호 정의

기호	정의
E(K, D)	암호키 K로 데이터 D를 암호화
D_K	도메인 키(Domain Key)
SK_A	디바이스 A의 개인키
RO_B	A가 B를 위해 저작한 RO
RO_{state}	RO 현황 정보
information	기타 부가 정보

동일한 DRM 포맷을 지원하는 디바이스 A, B의 경우 권한 정보 공유 프로토콜은 <그림 3>에 기술되어 있다.

1. $B \rightarrow A: E(D_K, PK_B)$
2. $A \rightarrow B: Content \| E(SK_A, RO_B)$
3. $A \rightarrow RI: : PK_B \| RO_{state} \| information$
4. $A,B \rightarrow RI: RO_{state}$

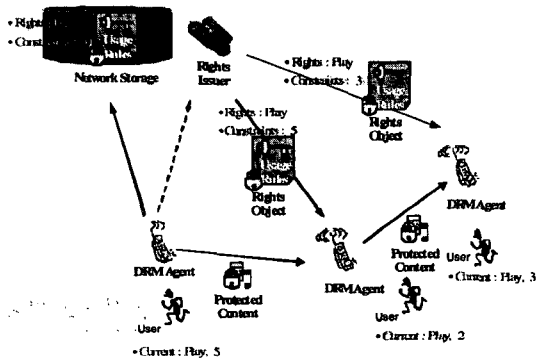
<그림 3> 도메인 기반 권한 정보 공유 프로토콜

1. 디바이스 A는 저장되어 있는 RO의 정의된 권한 한도 내에서 디바이스 B를 위한 RO를 생성한다. 이에 대해 디바이스 B는 자신의 공개키를 도메인 키로 암호화하여 전송한다.
2. 디바이스 A는 저작된 RO를 서명하여 암호화된 컨텐츠와 함께 전송한다.
3. 디바이스 A는 디바이스 B의 공개키와 RO 저작 수행 여부 및 자신의 현재 잔여 RO 정보를 서비스 제공자 RI에게 전송하도록 한다.
4. 서비스 제공자 RI는 디바이스 A와 디바이스 B로부터 보유하고 있는 RO 현황에 대해 주기적으로 업데이트 정보를 수신한다.

3.2. 도메인 권한 정보 확장 시나리오

본 연구에서는 동일 DRM 포맷뿐만 아니라 이종의 DRM 솔루션이 설치된 사용자 디바이스와의 도메인 권한 정보 관리를 위한 확장 시나리오를 제안하며 이는 서비스 제공자 RI의 지원을 기반으로 진행 된다.

1. 디바이스 A는 서비스 제공자 RI에 등록된 Network Storage에 접속하여 RO의 권한 한도 내에서 이종의 DRM 포맷으로 구성된 디바이스 B를 위한 새로운 RO를 생성하고 서비스 제공자 RI는 DRM 포맷 B에 적합한 형태로 변환한다.
2. 디바이스 B는 자신의 공개키를 전송하고, 이를 수신한 디바이스 A는 해당 공개키를 Network Storage로 전달하여 변환된 RO를 서명한 후 암호화된 컨텐츠와 함께 또는 저장된 Network Storage의 주소를 전송한다.
3. 서비스 제공자 RI는 디바이스 A와 디바이스 B로부터 보유하고 있는 RO 현황에 대해 주기적으로 업데이트 정보를 수신하여 관리하게 된다. 이종의 DRM 솔루션이 설치된 디바이스 B 또한 로컬에 저장된 잔여 RO 정보를 RI에게 전송하도록 한다.



<그림 4> 도메인 확장 시나리오

4. 결론 및 향후 과제

본 논문에서는 홈 네트워크 환경에 대해 사용자 소유의 디바이스로 구성된 도메인에서의 권한 정보 관리 기법을 제안하였다. 제안한 기법은 정당한 사용자 도메인의 디바이스에 대해 보유하고 있는 권한 정보 한도(Constraints) 내에서 DRM 포맷에 독립적으로 해당 디바이스를 위한 RO를 생성 및 기존 RO 상태 정보의 업데이트를 수행한다.

향후 다양한 이종의 DRM 포맷과의 확장 및 다양한 컨텐츠 공유 프로토콜 최적화에 대한 연구와 분석이 진행되어야 할 것이다.

참고 문헌

[1] Open Mobile Alliance, OMA, http://www.openmobilealliance.org

[2] OMA DRM v.2.0 Draft (OMA-DRM-DRM-V2_0-20040716), OMA Download+DRM WG

[3] A. Fiat and M. Naor, "Broadcast Encryption", *Advances in Cryptology - CRYPTO '93*, Springer, LNCS Vol. 773, pp. 480-491, 1994

[4] W. Trappe, J. Song, R. Poovendran and K. Liu, "Key Distribution for Secure Multimedia Multicasts via Data Embedding", *Proc. of Acoustics, Speech, and Signal*, IEEE, Vol. 3, pp. 1449-1452, 2001