개인 정보 네트워크에서의 권한 정보 공유를 위한 동적 디바이스 관리 기법

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

Dynamic Device Management Scheme for Rights Object Sharing in the Personal Private Networks

Kyung-Ah Chang° Byung-Rae Lee
Software Center, Samsung Electronics

요 약

개인 정보 네트워크는 근거리 무선 통신을 기반으로 구성된 디바이스간 정보 공유 및 무선 인터넷의 확장으로 디지털 컨텐츠 교환의 활성화가 예상되고 있다. 본 논문에서는 무선 및 휴대용 디바이스의 한계적 계산 능력과 불안정한 대역폭 및 기존 네트워크 환경과의 확장을 고려한 표준화 논의 내용을 기반으로 DRM 관련 권한 정보 공유를 위한 개인 정보 네트워크 내의 동적 디바이스 관리 기법을 제안하였다.

제안한 기법은 개인 정보 네트워크를 구성하는 사용자 디바이스의 성능을 고려하여 Proxy를 통한 Store/ Forward 서비스 구조를 기반으로 기존 유무선 네트워크의 컨텐츠 제공자 및 권한 제공자와의 서비스를 수행하도록 하였으며, Proxy에 그룹 키 관리 기능을 구성하여 개인 정보 네트워크 내의 권한 정보 공유를 위한 디바이스의 참가 및 탈퇴를 관리하도록 하였다.

1. 서론

개인 정보 네트워크는 근거리 무선 통신을 기반으로 홈 네트워크 또는 오피스 네트워크에서 디바이스간 정보 공유 및 각 디바이스의 고유의 기능을 단일 형태로 통합이 가능하며, 무선 인터넷으로 장소와 시간에 독립적인 디지털 컨텐츠 교환 및 사용을 가능하게 할 것으로 예상된다.

이와 관련하여 DRM (Digital Rights Management)은 음악, 영화, 게임과 같은 멀티미디어 포맷에 대해 뗇ne-Source Multi-Use? 떴omposite Media Mix? 등 유형의 가공을 통한 다양한 디지털 컨텐츠의 효용성을 제어할 수 있어야 한다.

본 연구에서는 OMA (Open Mobile Alliance) 표준안에서 진행되고 있는, 무선 디바이스의 한계적 계산 능력과 불안정한 대역폭 및 기존 네트워크 환경과의 확장을 고려한 OMA DRM Phase2의 논의 내용을 기반으로 개인 정보 네트워크의 동적 디바이스 관리 기법을 제안하였다.

제안한 기법은 무선 또는 CE 디바이스의 성능을 고려하여 Proxy를 통한 Store/ Forward 서비스 구조를 기반으로 기존 유무선 네트워크의 컨텐츠 제공자(CI, Contents Issuer) 및 권한 제공자(RI, Rights Issuer)와의 서비스를 수행하도록 하였으며, 해당 Proxy에 그룹 키 관리 기능을 구성하여 개인 정보 네트워크 내의 권한 정보 공유를 위한 디바이스의 참가 및 탈퇴를 관리하도록 하였다.

2. 관련 연구

2.1 Proxy 기반 Store/ Forward 서비스

무선 디바이스에 대한 DRM은 WAP (Wireless Application Protocol) 포럼 이후 차세대 주요 서비스 중 하나로 OMA에서 활발한 표준안 제정 작업이 진행 중이다.

이러한 OMA DRM Phase2 표준안에는 기본적으로 무선 환경에서의 DRM 지원을 위한 다양한 기술안 뿐만 아니라 무선 디바이스의 한계적 성능을 고려한 사용자 시나리오에 대해 Proxy 기반 Store/ Forward 메커니즘을 정의하고 있다.

Store/ Forward 메커니즘은 Proxy를 통해 CI에 대한 네트워크 연결 및 해당 디바이스를 대행하여 디지털 컨텐

츠 구입이 가능하다. 이때 사용자 디바이스 관련 정보는 디지털 컨텐츠 및 권한 정보 프로세스 진행시 CI에게 제공하도록 한다.

이러한 메커니즘을 통해 다운로드된 컨텐츠 및 권한 정보는 Proxy에 저장 및 관리하도록 하며 이후 해당 디바이스로 이동시키게 된다.

이 때, Proxy는 권한 정보를 획득하기 위해 해당 디바이스를 대행하여 RI와의 인증 및 권한 정보 획득 프로토콜을 수행한다.

2.2 공유 그룹 관리 기법

DRM 서비스는 정당한 사용자 그룹에 대해 한정적으로 암호화된 디지털 컨텐츠를 복호화하여 서비스 이용이 가능하도록 보장하기 위해 다양한 암호학적 그룹 키 관리 메커니즘을 요구하고 있다.

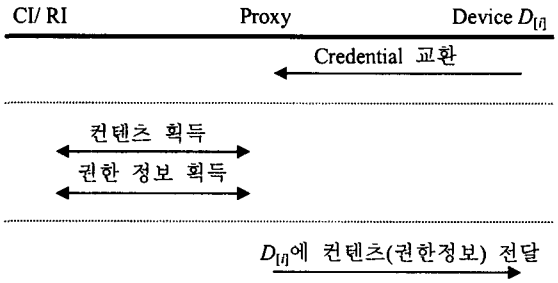
이에 대해 Broadcast Encryption은 데이터 수신 그룹의 동적 변화를 효과적으로 브로드캐스트하는 기법을 제시하고 있으며 Fiat, Naor의 연구를 시작으로 논리적 키 계층 구조 (logical-tree-hierarchy, LKH) 방식, 단향향 함수 트리 (One-way Function Trees, OFT) 방식 등의 다양한 연구가 진행 중이다.

LKH는 멀티캐스트 그룹의 안전성을 보장하기 위해 키재발급 애플리케이션을 제시하기 위해 그룹의 참가 및 탈퇴 발생시 사용자는 대부분의 경우 네트워크에 연결되어 있음을 가정하고 있으며 이로 인한 LKH의 통신 오버헤드를 개선하기 위한 연구가 진행 중이며, OFT는 키 트리 구조를 구성하여 Leaf부터 Root에 이르는 모든 노드에 대한 키재발급 브로드캐스트의 연산량을 감소 시켰다.

3. 권한 정보 공유 지원 동적 디바이스 관리 기법

3.1 Proxy 기반 권한 정보 공유 구조

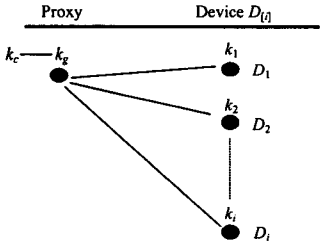
개인 정보 네트워크는 기존 네트워크의 CI와 RI와의 프로세스를 담당하는 Proxy를 기반으로 n 개의 디바이스로 구성된 그룹 g로 정의할 수 있으며 모든 디바이스 D_i 는 Proxy에 의해 유용한 그룹 키 k_g 를 공유하여 그룹 내의 권한 정보 공유가 가능하게 된다. Proxy는 권한 정보 공유 목적으로 그룹에 참가하고자 하는 디바이스 고유의 키 k_i 포함하는 인증서 발급 등 내부 네트워크 그룹 관리 및 k_g 를 이용하여 권한 정보를 공유하도록 한다.



<그림 1> Proxy 기반 DRM 서비스 단계

Proxy 기반 개인 정보 네트워크에서의 DRM 서비스는 다음과 같이 구성된다.

- 초기화 단계 : DRM 관련 정보 권한 공유 서비스를 이용하고자 하는 디바이스 D_i 는 Proxy에 관련 정보를 등록하도록 하여 디바이스 인증서 발급 및 그룹 키 공유가 가능하게 된다.



<그림 2> 디바이스 관련 키 할당

- Store 단계 : Proxy는 등록한 디바이스들을 대행하여 기존 네트워크의 CI와 RI와의 DRM 서비스 프로토콜 수행하여 디지털 컨텐츠 및 권한 정보를 획득하여 다운 로드 또는 로컬에 저장한다. 이때 개인 정보 네트워크 내부의 디바이스 그룹에 대한 권한 정보 공유 목적으로 서비스 세션 키 k_c와 그룹 키 k_g를 이용한 변환 과정이 수행된다.
- Forward 단계 : 디바이스의 참가 및 탈퇴에 대한 상태 정보 업데이트로 동적 그룹 관리 기법을 통해 디지털 컨텐츠 및 권한 정보 공유 및

Usage Clearing을 수행하게 된다.

3.2. 제안한 동적 디바이스 관리 기법

본 연구에서 개인 정보 네트워크는 n 개의 디바이스와 Proxy로 구성된 단일 도메인에 대한 멀티캐스트 모델에 대한 트리 구조 기반 키 분배 기법을 기반으로 한다.

제안한 동적 디바이스 관리 기법에서 유무선 디바이스 D_i는 2개의 키 암호화용 키 k_i 와 k_g 및 권한 정보 공유를 위한 서비스 세션 키 k_c 를 보유하게 된다. 서비스 세션 키 k_c 는 Proxy를 통해 전달되는 권한 정보 암호화를 위해 사용되며, 그룹 키 k_g 는 k_c 의 업데이트 메시지를 암호화하는데 사용된다. $k_1, k_2, ?, k_n$ 들은 k_g 의 업데이트 메시지를 위한 키 암호화용 키로 사용된다.

또한 Proxy는 2β bit 열을 β bit로 전환 가능한 단방향 해쉬 함수 $f(x, y)$를 보유하고 있다고 가정한다.

- 등록 단계 : 디바이스 등록은 각 디바이스의 정보를 기반으로 Proxy에서 디바이스에 대한 인증서를 할당, 디바이스 D_i는 키 암호화용 키 k_i를 획득하게 된다.

  또한 t ? 1 시간 간격으로 보유하고 있는 키의 사용 만료에 대한 유용성을 점검하며, 이때 $k_g(t) = k_g(t ? 1)$ 요구되지 않으나 권한 정보 공유를 위한 서비스 세션 키가 $k_c(t ? 1)$에서 $k_c(t)$로의 변경에 대해 Proxy에서는 상태 정보 업데이트 메시지 $m_c(t) = E_{Kg(t)}(k_c(t))$를 생성하여 개인 정보 네트워크 내의 디바이스들에게 브로드캐스트 한다.
- 참가 단계 : 이미 개인 정보 네트워크 내의 n ? 1 디바이스들이 t ? 2 시점에 그룹 키를 공유하고 있는 상황에서 새로운 디바이스가 참가하고자 할 때, t ? 1 시점에서 기존 n ? 1 디바이스들에게 키 재발급 정보를 분배하도록 한다. 이 때, 이전 서비스로부터의 악의적인 접근을 방지하기 위해 k_c 와 k_g는 모두 새로이 발급되어야 한다.

  이를 위해 그룹 키를 $k_g(t ? 1)$에서 $k_g(t)$로 업데이트 하여 개인 정보 네트워크 내의 디바이스들에게 $m_g(t) = E_{Kg(t)}(k_c(t))$ 형태의 메시지를 서명 후 브로드캐스트 하도록 하며 이후 서비스 세션 키를 $k_c(t)$로 업데이트 한다.
- 탈퇴 단계 : t ? 2 시점에 임의의 디바이스가 개인 정보 네트워크를 탈퇴하고자 한다면 $k_g(t ? 1)$와 $k_c(t ? 1)$는 업데이트 되어야 한다. 참가 단계와 마찬가지로 그룹키 k_g를 우선적으로 업데이트 하여 새로운 서비스 세션 키를 암호화하는데 사용하도록 한다. $k_g(t ? 1)$를 업데이트 하기 위해 Proxy는 임의 난수 $\beta(t)$를 이용하여 $k_g(t)$와 함께 키 재발급 메시지 $m_g(t)$를 다음과 같이 생성하여 서명 후 전송하도록 한다.

$$m_g(t) = k_g(t) + \prod_{i=1}^{n-1} f(d_i, \beta(t))$$

  정당한 디바이스 D_i 는 해당 메시지를 통해 $m_g(t)(\mathrm{mod}\ f(d_i, \beta(t)))$ 를 연산 후 $k_g(t)$를 얻기 위해 $m_g(t)$를 저장하게 된다. 이후 서비스 세션 키는 업데이트 되어 메시지 $m_c(t) = E_{Kg(t)}(k_c(t))$에 서명 후 브로드캐스트 한다.

4. 결론 및 향후 과제

본 논문에서는 Proxy를 기반으로 개인 정보 네트워크 내의 유무선 디바이스에 대한 DRM 관련 Store/ Forward 서비스를 제시하였으며 권한 정보 공유를 위한 무선 및 휴대용 디바이스의 동적 참가 및 탈퇴에 대한 그룹 키 관리 기법을 제안하였다.

향후 다양한 DRM 시스템으로 확장 및 프로토콜 최적에 대한 연구와 분석이 진행되어야 할 것이다.

참고 문헌

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

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

[3] OMA DRM v.2.0 Draft (OMA-DRM-DRM-V2_0-20030810), OMA DLDRM WG

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