한국산학기술학회논문지
Vol. 8, No. 5, pp. 1114-1121, 2007

홈 네트워크 기반의 안전한 콘텐츠 전송에 관한 연구

정용훈[1], 이창보[2], 이광형[3*], 전문석[4]

A Study on Secure Contents Transer Based on Home Network

Young-Hun Jung[1], Chang-Bo Lee[2], Kwang-Hyoung Lee[3*] and Moon-Seog Jun[4]

요 약 홈 네트워크는 가정 내의 가전기기들이 모여 하나의 네트워크를 이루는 것으로 가전기기들의 발전함에 따라 확장되어 가고 있으며, 또한 디지털 콘텐츠의 수도 꾸준히 증가하고 있다. 그러나 콘텐츠 가전기기 사이에 상호 운영성 부족으로 디지털 콘텐츠의 지속적인 저작권 보호가 힘들 뿐 아니라, 가전기기 간에 콘텐츠 이동을 위해서는 DRM 서버로부터 라이선스를 다시 재발급 받아야 한다. 따라서 본 논문에서는 홈 네트워크 안에서 디바이스 상호 인증을 통해 콘텐츠를 다른 디바이스로 자유롭게 이동 할 수 있는 프레임워크를 제안하며, DRM 서버의 라이선스 관리 부담을 줄이고 외부의 사용자가 홈 네트워크에 접근하더라도 사용자를 인증을 통해 콘텐츠 사용이 가능한 시스템을 제안한다.

Abstract Home networks is a network composed of devices in home and is being expanded by evolving devices. Also, The number of digital contents in home network has been increasing steadily. But it is difficult to continually protect the rights of digital contents due to lack of interoperability among contents devices. Besides, a license has to be re-issued by DRM sever for contents transfer between devices. Thus, this paper proposes framework which can freely transfer the contents to another device through mutual device authentication and a system that can decrease overload of license management of the DRM server and that enable users outside home network to use contents through user authentication.

Key Words : Home Network, DRM, Device authentication, user authentication

1. 서론

최근 컴퓨터 및 정보통신 기술의 발달과 함께 급속히 발전하는 인터넷 기술은 데이터 서비스, 인터넷 폰, 전자신문, 주문형 비디오, IPTV등 다양한 멀티미디어 서비스를 가능하게 하였으며, 이러한 인터넷의 발전은 가정 내의 정보화를 가속시키고 있다. 하지만 다양한 서비스를 통해 제공되는 수많은 콘텐츠 들은 디지털 저작권 관리 기술(DRM)에 의해 보호 받지 못하고 있거나, 저작권 보호 기술이 적용되어 있다 하더라도 DRM 업체별 독자적인 기술규격 사용으로 디지털 콘텐츠 및 디지털 기기의 상호호환성이 보장되지 않고 있다[1]. DRM의 상호 호환성 보장을 위해 MPEG-21(Moving Picture Experts Group-21), OMA(Open Mobile Alliance), DMP(Digital Media Project) 등 많은 국제표준단체에서 DRM 표준기술을 개발하고 있으나, 이들 단체 간에도 독자적인 기술규격 개발로 상호호환성이 보장되지 않고 있다. 만일 홈 네트워크 안에서 사용자가 소유하고 있는 여러 장치들 간에 DRM 기술의 상호 호환성이 보장되지 않는다면 콘텐츠를 이용하는 사용자는 불편함을 감수해야 하며, 뿐만 아니라, 현재는 사용자가 콘텐츠를 입수하더라도 인증된 사용자만이 콘텐츠의 라이선스를 받아 사용할 수 있는 Superdistribution 기술 때문에. 자신이 소유한 디바이스들 사이에서 콘텐츠가 이동할 때 마다 DRM 서버로부터 새로운 인증과 라이선스를 재발급 받아야 하는 문제점이 있다[2].

본 논문에서는 홈 네트워크 안에서의 가상의 라이선스 도메인을 생성하고, 도메인의 각각의 장치들은 콘텐츠를 이동하기 하기 전에 상호 인증을 통해 콘텐츠와 라이선스를 안전하게 이동함으로써, 서로 다른 디바이스들 간에 DRM기술의 상호호환과 콘텐츠 이동시 DRM 서버로부

본 연구는 서울시 산학연협력사업으로 구축된 서울 미래형콘텐츠컨버전스 클러스터 지원으로 수행되었습니다.
[1,2,4]숭실대학교 컴퓨터공학과
[3]서일대학 인터넷정보과
*교신저자: 이광형(dreamace@seoil.ac.kr)

터 새로이 라이선스를 발급받지 않아도 되기 때문에 DRM 서버의 부담을 줄일 수 있다. 또한 외부에 있는 클라이언트가 PDA와 같은 단말기로 홈 네트워크에 존재하는 콘텐츠를 사용할 때에, 안전한 사용자 인증을 통해 디지털 콘텐츠의 지속적인 저작권 보호기술이 가능한 구조를 제안한다. 본 논문의 구성은 홈 네트워크 구성 및 보안 기술요소 소개한 뒤에 제안하는 시스템의 구조를 기술하고, 기존의 DRM시스템과의 비교 및 안전성 평가 순으로 진행한다.

2. 홈 네트워크 구성 및 보안 기술

아래 [그림 1]은 홈 네트워크 시스템의 구성도를 보여주고 있으며 이러한 홈 네트워크 시스템은 크게 외부네트워크, 홈 게이트웨이, 내부 네트워크, 홈 미들웨어, 각종 디지털 정보 가전기기 그리고 다양한 응용서비스로 구성된다[3].

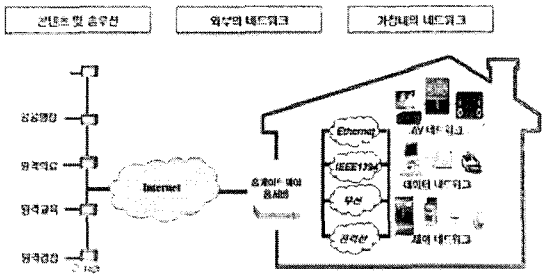

그림 1. 홈 네트워크 시스템 구성도

홈 네트워크 환경에서의 각종 디바이스들은 인터넷과 직접적으로 연결되어 있어 언제라도 외부 위협요소로부터 공격에 대상이 될 수 있으며, 디바이스의 다양성과 홈 디바이스의 자원 공유 등으로 인해 고려해야 할 보안요구 사항은 더욱더 복잡해지고 있다.

2.1 사용자 인증

홈 네트워크에서는 각 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증과정이 필요하다. 이를 위해 생체인식, 패스워드, 인증서, 스마트카드, RFID 등의 다양한 사용자 인증기술의 활용이 가능하며 사용자 인증기술은 외부에서 홈 네트워크에 대한 원격 접근과 댁내에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 이용하고자 할 때 해당 사용자가 정당한 사용자임을 증명하는 하기 위한 수단으로 사용된다[4].

2.2 접근 제어

사용자에 따라 제공받을 수 있는 홈서비스의 종류가 다르고 홈 네트워크 구성요소에 대한 제어 범위도 다르므로 각 사용자에게 부여된 권한에 맞는 기능만을 사용할 수 있게 하는 접근 제어 기술이 요구된다. 현재의 홈 네트워크 시스템의 구조를 고려할 때 접근제어를 위한 접근제어 목록은 각 단말기에 내장하고 있는 것이 효율적이다. 하지만 안정성 측면이나 사용자 측면과 같은 여러 요소들에 대해 일관된 보안정책을 적용해야 한다는 점에서 홈 게이트웨이에서 종합적으로 관리하는 것이 좀 더 효율적이다.

2.3 디바이스 인증

댁내 디바이스에 불법적인 사용을 방지하기 위해서는 홈 네트워크를 구성하고 있는 디바이스에 대한 인증이 선행되어야 한다. 현재 디바이스 인증은 미들웨어 레벨에서 제공되고 있으며 UPnP의 경우, 디바이스마다 부여된 Security ID를 이용하여 디바이스 등록시점에 인증이 이루어지며 HAVi의 경우는 디바이스마다 고유한 인증서를 발행하여 디바이스를 인증한다.

2.4 홈 미들웨어 보안

홈 게이트웨이와 서로 상이한 플랫폼을 가진 각각의 디바이스를 제어하기 위해서는 이들을 하나로 제어하고 관리할 수 미들웨어가 필요하다. 이러한 미들웨어 자체에서도 기본적인 보안 기능이 제공되고 있으며, 현재 미들웨어에서의 보안 요소를 표준으로 제정하여 사용하기 위한 연구가 계속적으로 진행되고 있다. [표 1]은 홈 네트워크에 사용되는 미들웨어에 따른 보안 기술들을 보여주고 있다[5].

표 1. 홈 네트워크 미들웨어에 따른 보안 기술

미들웨어	제공하는 보안기능
UPnP	•Ver 1.0에서는 보안기능이 정의되어 있지 않음 •Ver 2.0에서 보안기능이 추가 - 제품 인증 - 기기간 인증 - 접근제어를 위한 디바이스가 자체적인 ACL - 기밀성
Jini	•Ver 1.0에서는 Java Security에 의존 - 사용자 인증 - 기기간 인증 - 메시지 무결성 및 기밀성 - 접근제어 •Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성 등에 대한 기능 강화
HAVi	- HAVi인증서를 이용한 인증 - 접근제어

3. 제안하는 시스템

3.1 제안하는 시스템

제안하는 DRM 시스템의 구성요소는 다음과 같이 크게 3가지로 나뉘며 전체 구조는 [그림 2]와 같다.

- HADM(Home Authorized Domain Manager) : 홈 네트워크의 전체 도메인을 관리하는 장치로 새로운 디바이스를 도메인에 추가하거나, 혹은 디바이스를 제거한다. 홈 네트워크 안에서 홈 게이트웨이가 이 역할을 한다.
- Active 디바이스 : DRM 서버로부터 직접 콘텐츠를 다운로드 받을 수 있는 장치로, 라이선스를 재패키징 할 수 있는 모듈을 가지고 있으며, 비교적 높은 처리능력을 가진 PC, PDA와 같은 디바이스이다.
- Passive 디바이스 : DRM 서버로부터 직접 콘텐츠를 다운 받을 수 없으며, 비교적 제한된 처리능력을 가진 디바이스로 MP3 player, 자동차 오디오등이다.

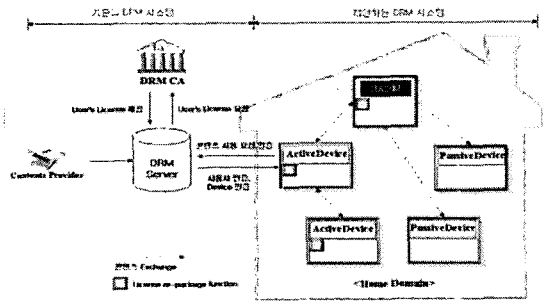

그림 2. 제안하는 시스템 전체구성

본 논문에서 제안하는 시스템에서는 홈 게이트웨이가 전체 디바이스를 관리하는 HADM로써의 역할을 수행한다. HADM을 통해 도메인을 생성한 뒤에 나머지 각각의 디바이스들을 차례로 도메인에 등록시킨다. 도메인 안에 Active 디바이스는 DRM 서버로부터 사용자 인증과 디바이스 인증 후에 콘텐츠 사용요청을 통하여, 콘텐츠와 라이선스를 다운로드 받아 콘텐츠를 사용할 수 있게 된다. 제안한 시스템의 특징은 디바이스 자신이 소유하고 있는 콘텐츠와 라이선스를 도메인 안에 존재하는 다른 디바이스들에게 전달해야 하는 경우가 발생하면, 디바이스는 같은 도메인에 속한 디바이스인지 자동으로 인증과정을 거쳐 이동하려는 디바이스의 환경에 맞게끔 라이선스를 재패키징 한다. 그리고 한번 라이선스의 이동이 발생하면 원래 라이선스를 가지고 있던 디바이스에는 라이선스가 더 이상 존재하지 않는다. 라이선스는 완전히 이동하게 되고 결국 홈 네트워크에 중복된 라이선스가 존재 하지 않으므로 라이선스 관리는 그만큼 쉬워지고, 또한 DRM 서버로부터 다시 라이선스를 발급 받아야 하는 불편함 또한 제거할 수 있다.

3.2 시스템 동작과정

제안하는 시스템의 동작과정은 도메인의 생성, 도메인으로 디바이스 등록, 그리고 디바이스 인증을 통한 콘텐츠 이동으로 구분되어지며, 도메인 안에 디바이스가 추가되거나 제거 되었을 때와, 라이선스 이동에 관하여 기술한다.

3.2.1 도메인 생성

사용자는 최초에, 자신이 소유하고 있는 디바이스들 중에 전체 도메인을 관리하기 위한 도메인 관리자인 HADM을 선택해야 한다[6]. HADM 장치는 키를 생성할 수 있고 DRM 서버와 온라인으로 연결되어 있어야 하며, 라이선스를 재패키징 할 수 있어야 한다. 사용자가 HADM이 될 장치를 선택하였다면, DRM 서버로부터 HADM을 수행하기 위한 HADM Agent를 다운로드 받아 설치한다. HADM Agent는 최초에 도메인 ID를 생성하는데, 도메인 ID는 디바이스 ID(DID)와 TimeStamp를 연접한 값을 해쉬 하여 얻는다(Domain ID = H(DID || TimeStamp)). 여기서 TimeStamp 값은 시간에 따라 항상 변하기 때문에 DID 값과 연접하여 해쉬를 하면 유일한 값이 보장된다. HADM은 자신에게 등록할 디바이스들이 사용할 Device Key를 미리 생성한다. 키의 개수는 DRM 서버와 사전에 미리 그 수를 정할 수 있지만, 집에서 사용하는 콘텐츠 사용이 가능한 디바이스 개수와 앞으로 도메인에 추가되거나 제거될 디바이스를 개수를 고려하여 AES 암호화 알고리즘으로 128bit Key를 20개 생성한다. 그리고 각 키마다 Domain Device Index(DDI)을 0~19를 부여하여 나머지 각각의 디바이스들이 HADM에 등록을 할 경우, 각 디바이스가 사용하게 될 Key의 DDI와 전체 Device Key Set을 전송한다. HADM은 등록되는 순서에 따라 차례대로 DDI값을 1씩 증가 시킨다.

각 디바이스들이 HADM에 자신을 등록과정을 마치면 HADM Agent는 각각의 디바이스 정보를 수집하여 DRM 서버에게 보고한다. 그리고 도메인 안에 디바이스들이 새로이 추가 되거나 제거되는 경우에도 DRM Agent는 수시로 DRM 서버에게 보고할 수 있다[7].

3.2.2 디바이스 등록

도메인을 생성한 뒤에 각각의 디바이스들은 도메인에 등록을 해야 하며, Active 디바이스와 Passive 디바이스가 HADM에 자신을 등록하는 과정은 [그림 3]과 같으며 세부과정은 다음과 같다.

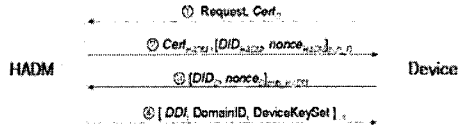

그림 3. 디바이스 등록 프로토콜

①,② 디바이스는 HADM에게 자신의 인증서 $Cert_D$와 함께 등록 요청 메시지를 보낸다. 그리고 HADM은 자신의 인증서 $Cert_{HADM}$와 함께 DID(Device ID), 난수 $nonce_{HADM}$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 연접하고 해쉬하여 비밀키 SK를 생성한다(Secret Key = H($nonce_{HADM}$||$nonce_D$)).

④ HADM은 디바이스에게 디바이스의 DDI(Domain Device Index)와 DomainID 그리고 Device Key Set를 비밀키 SK로 암호화 하여 전송한다.
디바이스의 모든 등록 과정을 마치게 되면 HADM에는 Domain ID와 각 장치에 해당하는 DID, DDI, DeviceKey가 저장되고, 최종적으로 DRM 서버에게 자신의 도메인 정보를 알린다.

3.2.3 디바이스 인증

DRM 서버로부터 콘텐츠를 다운로드 받은 디바이스가 도메인 안에 있는 다른 디바이스에게 콘텐츠를 전송하고자 할 때, 실제 자신의 도메인에 있는 디바이스인지 인증해야만 한다.

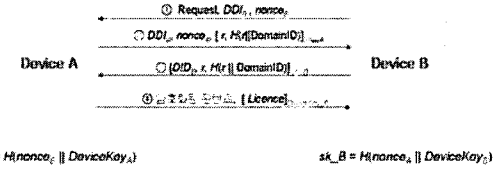

그림 4. 디바이스 인증 프로토콜

디바이스 A와 B가 상호 인증 과정은 [그림 4]와 같으며 세부 내용은 다음과 같다.

① 디바이스 B는 디바이스 A에게 콘텐츠를 요청 메시지와 자신의 Domain Device Index 번호 DDI_B 그리고 난수 $nonce_B$를 보낸다.

② 디바이스 A는 $nonce_B$와 자신의 Device Key를 연접하고 해쉬하여 비밀키 SK_A를 생성한다. 그리고 자신의 Domain Device Index 번호 DDI_A, 난수 $nonce_A$와 r, H(r||DomainID)을 비밀키 SK_A로 암호화 하여 디바이스 B에게 보낸다.

③ 디바이스 B는 [r, H(r||DomainID)]SK_A 를 복호화하여 디바이스 A가 같은 도메인 안에 있는 디바이스인지 검증을 한다. 만일 같은 도메인 안의 디바이스라면 $nonce_A$와 자신의 Device Key를 연접하고 해쉬하여 비밀키 SK_B를 생성한 후에 DID_B, r, H(r||DomainID)을 비밀키 SK_B로 암호화 하여 디바이스 A에게 보낸다.

④ 디바이스 A는 [DID_B, r, H(r||DomainID)]SK_B를 복호화하여 디바이스 B가 같은 도메인의 안에 있는 디바이스 인지 검증을 한다. 같은 도메인의 디바이스라면, 디바이스 사이에 상호인증 과정을 성공적으로 마치게 된다. 디바이스 A는 디바이스 B에게 DRM 서버로부터 받은 암호화된 콘텐츠와 디바이스 B의 DID정보에 맞게 재패키징된 라이선스를 디바이스 B의 Device Key로 암호화 하여 보낸다.

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

3.2.4 디바이스 추가

새로운 디바이스가 도메인 안에 추가되면 3.2.2절에서 기술한 등록 프로토콜을 통해 HADM에 등록한다. 새로운 디바이스가 추가 되어도 특별히 다른 디바이스에게 알릴 필요는 없다. 왜냐하면 도메인 생성 시 도메인의 구성하는 디바이스들에게 미리 Device Key Set를 알려 주었기 때문에, 추가된 디바이스는 등록 시 부여받은 DDI에 해당하는 키를 사용한다. 나머지 디바이스들도 추가적인 정보를 받지 않고 디바이스 인증 시 Device Key Set에 키를 사용한다. 만일 사용하지 않는 DDI의 키가 없는 경우에는 불가피하게 도메인을 재구

성해야 한다.

3.2.5 디바이스 제거

사용자는 디바이스가 다른 도메인으로 이동되거나 디바이스의 물리적인 손상, 도난, 해킹 등 여러가지 이유로 인하여 도메인에서 제거 될 시에 HADM Agent를 통해 DRM 서버에 제거된 장치를 보고하여야 한다. 그리고 장치가 도메인 안에서 제거되었다는 사실을 다른 디바이스에게도 알려야 하는데, 이것은 이미 제거된 장치에 다시 콘텐츠가 전송되는 것을 막기 위해서다. 각각의 디바이스에게 장치가 제거 되었다는 사실을 알리기 위해서 DRM 서버는 콘텐츠 안에다 ADL(Access Device List)라고 불리는 접근 가능한 디바이스 리스트를 함께 패키징 한다. 디바이스 DRM Agent는 자신이 가지고 있는 ADL과 콘텐츠 내에 포함된 ADL을 비교하여 도메인 내의 디바이스 변경 사항을 판단하고 최신의 ADL으로 갱신하다. 뿐만 아니라 HADM은 도메인에 가입된 디바이스들과 연결이 이루어질 때마다, ADL을 갱신하여 도메인 안의 구성원은 항상 최신의 ADL을 유지하여, 불법적인 디바이스에 콘텐츠가 전송되는 것을 막을 수 있다.

만일 HADM은 도메인을 구성하는 가장 핵심적인 장치로 새로운 디바이스로 교체되거나 공격자에 의해 시스템이 붕괴된 경우 DRM 서버에 이 사실을 알리고 3.2.1절 에서 기술한 도메인 생성과 3.2.2의 디바이스 등록과정을 거쳐 도메인을 재구성해야 한다.

3.3 사용자 인증

외부의 사용자가 홈게이트 웨이 서버를 통해 디바이스에 접근하거나, 혹은 접근한 디바이스의 콘텐츠를 전송받고자 할 경우, [그림 5]는 사용자 인증 과정을 보여주고 있으며 세부적인 설명은 ①~④와 같다[8][9].

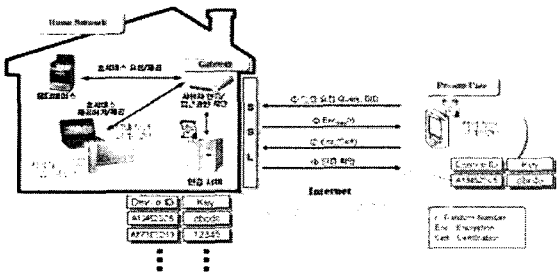

그림 5. 사용자 인증과정

① 클라이언트는 Query와 DID를 전송하고 사용자 인증을 요청한다.

② 홈 서버는 DID를 비교하고 난수 r을 생성한다. 그 후 클라이언트와 사전에 교환하여 가지고 있는 대칭키 k를 이용하여 난수 r을 암호화한 정보 $Enc_{key}(r)$을 클라이언트에게 전송한다.

③ 클라이언트는 대칭키 k로 전송받은 정보를 복호화하여 난수 r을 획득하고 획득한 난수r을 암호화키로 사용하여 자신의 인증서를 암호화하고 홈 서버에게 전송한다.

④ 홈 서버는 자신이 생성한 해당 클라이언트 난수 r을 이용하여 전송받은 정보를 복호화한 후 사용자 인증을 수행하며 수행 결과를 다시 클라이언트에게 전송한다.

4. 제안한 시스템의 분석 및 보안성 평가

4.1 기존의 DRM 시스템과 비교

MS사의 DRM인 WMRM과 Intertrust사의 DRM, 그리고 제안한 시스템의 프로토콜을 비교 분석 하면 [표 2]와 같다[10]. WMRM은 별도의 DRM 모듈의 필요 없이 윈도우 미디어 플레이가 DRM 기능을 지원한다. 그리고 제안한 시스템은 기존의 시스템과 마찬가지로 TRM(Temper Resistant Memory)을 지원하여 중요한 키 정보 및 인증 정보의 유출을 방지를 방지하고 있다. WMRM의 경우 라이선스 획득 시에만 인증을 하고 그 이후에는 사용자 장치에 저장되어 구동되므로, 라이선스 사용 규칙과 변경 등에서 제한적이나 Intertrust와 제안한 시스템은 언제든지 라이선스 서버와 연결만 가능하다면 실시간으로 사용 내역을 보고하거나 동적인 콘텐츠 권한 변경이 가능하다.

표 2. 기존의 DRM 시스템과의 특성 비교

	WMRM	InterTrust	제안 시스템
사용자 설치 모듈	N	Y	Y
저작권 보호	Y	Y	Y
동적권한변경	제한적임	Y	Y
네트워크 의존성	높음	매우 높음	낮음
라이선스 이동	N	N	Y

또한 기존의 DRM 시스템이 지속적인 콘텐츠 저작권 보호를 위해 항상 온라인으로 연결되어 있어야 하

나, HADM를 제외하고는 계속적인 온라인 연결을 필요로 하지 않으므로 네트워크 의존다가 다른 시스템에 비해 낮고, 라이선스의 이동성 측면에서도 라이선스에는 DID가 포함되어 라이선스의 이동 자체가 제한되어 있으나, 제안한 시스템은 라이선스 이동이 가능하다는 장점을 가지고 있다.

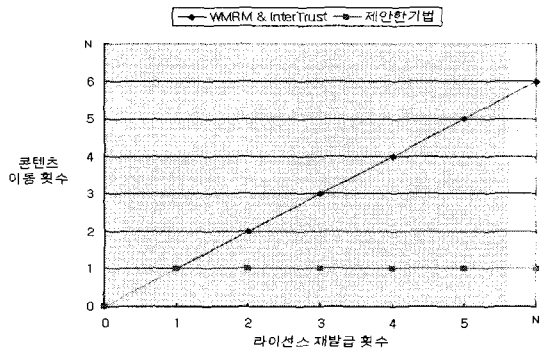

그림 6. 기존의 시스템과 제안한 시스템의 라이선스 재발급

[그림 6]은 콘텐츠 이동 회수에 따른 라이선스 재발급 회수를 나타내고 있다. 기존의 시스템들이 콘텐츠가 이동이 발생할 때마다 콘텐츠를 사용하기 위해 라이선스를 DRM 서버로부터 재발급 받아야 하지만 제안한 시스템은 DRM 서버로부터 한번 발급 받은 라이선스는 라이선스 권한 변경이 없는 한 다시 재발급 받지 않아도 된다. 라이선스 서버는 라이선스를 발급하는 부담을 덜어 과부하를 방지하고, 사용자는 라이선스로부터 새로이 인증 받아야 하는 불편함이 없어진다는 것을 확인할 수 있다.

4.2 안전성 평가

제안한 기법은 기존의 DRM 시스템이 제공하였던 라이선스의 분배권한을 사용자에게도 일부 넘겨주었다. 그러므로 그에 따르는 보안상에 문제점의 발생을 최소화 하고, 기존이 DRM 시스템이 제공한 콘텐츠 보호 기능을 제안한 시스템에서도 계속적으로 유지 할 수 있어야 한다. 제안한 기법에서는 디바이스의 인증을 위해 디바이스에 인증서를 탑재하였다. 이에 수반되는 문제가 없는지 분석해 보고, 악의적인 사용자들에 의한 스푸핑(Spoofing), 재전송(Replay Attack)등의 공격들에 대해서도 안전한지 평가하였다.

4.2.1 디바이스 인증

본 논문에서 제안한 시스템은 도메인에 디바이스 등록 시, 인증을 위해 디바이스 제조 과정부터 디바이스에 인증서의 탑재를 가정하고 있다. 인증서를 사용하는 이유는 불법적인 디바이스의 사용을 막고, 완벽하게 디바이스를 식별하기 위해서이다. 그리고 인증서를 사용한 공개키 암호화 방식은 현재까지 알려진 어떠한 공격에 대해서도 안전하며, 공개키와 개인키로 나누워져 있기 때문에 키 교환을 하는데 있어서도 편리하다. 3.2.3절에서 기술한 디바이스 등록 프로토콜 과정에서 HADM과 디바이스는 서로의 인증서를 교환한다. 인증서를 검증하는 과정은 실시간으로 이루어져야 하기 때문에 인증서를 검증할 처리 능력이 없는 Passive 디바이스에 경우에는 일부 제한이 따를 수 있다. 그러나 HADM은 도메인의 생성과정부터 사용자와 DRM 서버가 신뢰하는 장치이므로, 도메인에 가입하려는 디바이스가 HADM의 인증서를 검증하는 것은 반드시 필요한 과정은 아니며 보다 중요한 것은 도메인에 가입하려는 장치를 명확하게 식별하여 콘텐츠의 불법적인 도용을 막는 것이다.

4.2.2 스푸핑 및 재전송 공격에 대한 안전성

기존의 DRM 프로토콜의 경우에 데이터의 암호화로 인하여 스니핑 공격에는 강하나 스푸핑, 재전송 공격에는 매우 취약하다. 제안한 프로토콜은 스푸핑 및 재전송 공격으로부터 안전하기 위하여 디바이스 사이에 전송되는 데이터는 난수를 이용하여 불법적인 장치의 인증을 방지하고 있다. 3.2.3절에서 기술한 디바이스 인증 프로토콜에서 중요한 인증 정보인 Domain ID는 난수 r과 함께 연접하여 해쉬한 값으로 전송하기 때문에, 중간에서 메시지를 가로채더라도 실제 메시지의 내용을 알 수 없을 뿐 아니라 인증이 이루어질 때마다 값이 매번 변하기 때문에 값을 유추하는 것은 불가능하다. 그러므로 실제 Domain ID를 가지고 있지 않은 디바이스가 중간에 메시지를 가로채어 재전송 하여도 인증 받을 수 없다. 또한 외부의 사용자가 자신의 클라이언트 디바이스의 인증서를 이용하여 사용자 인증과 디바이스 접근제어를 수행한다. 또한 사용자 인증 데이터 정보는 항상 암호화 되어 전송되므로 불법적인 장치가 클라이언트의 개인키와 난수 r을 모르면 데이터의 정보가 노출될 위험이 없으며 홈 디바이스 제어 정보는 해쉬 한 값을 다시 암호화 하여 전송하기 때문에, 중간에서 메시지를 가로채더라도 메시지의 내용을 유추하는 것은 불가능 하다는 장점이 있다.

5. 결론

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 시간이나 공간에 구애를 받지 않고 다양한 홈서비스를 제공받을 수 있는 디지털 홈 구현을 위한 홈 네트워크에 대한 연구가 활발히 이루어지고 있다.

제안한 시스템의 특징은 기존의 DRM 시스템이 제공하였던 라이선스의 분배권한을 HADM 이라고 불리는 도메인 관리자에게 위임함으로써, 집에서 사용하는 가전제품들 사이에 콘텐츠 교환이 발생할 시, DRM 서버로부터 라이선스를 새로이 재발급 받지 않고 디바이스 상호 인증을 통해 라이선스를 재 패키징 한다. 이것은 기존의 DRM 시스템이 라이선스를 발급하고 관리하는데 들었던 비용을 분산 시킬 수 있으며, 사용자 입장에서도 DRM이 적용된 콘텐츠를 사용하는데 있어 아무런 방해 없이 콘텐츠를 집의 내부 혹은 외부에서 사용할 수 있다. 또한 안전성 평가를 통해 제안한 시스템이 기존의 시스템이 제공했던 안전성을 그대로 유지하는지도 확인하였다. 향후 연구로써 다양한 디바이스에 적용 가능한 DRM 모듈 및 미들웨어 개발이 필요하며 HADM과 DRM 서버 사이에 전송되는 도메인의 정보 및 사용자 정보를 노출을 막기 위한 안전한 프로토콜도 필요할 것이다.

참고문헌

[1] 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.

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

[3] 정재학, "홈 네트워크에서의 보안 요구사항 분석", 한국정보보호학회지 제14권 5호, pp.19-22, 2004.

[4] TTAS.KO-12.0030, "홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘", 한국정보통신기술협회, 2005.

[5] Car M. Ellison, "Home Network Security", Intel Technology Journal Vol 6, Issue 4, 2002.

[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] 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.

[8] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜", 한국정보과학회, Vol 30, pp.75-81, 2003.

[9] A. Freier, P. Karlton and P.C. Kocher, "The SSL Protocol, Version 3.0", Netscape Communications Corp. 1996.

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

정 용 훈(Young-Hun Jung) [정회원]

- 2004년 2월 : 숭실대학교 전자계산원 멀티미디어학과 (공학사)
- 2006년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2006년 ~ 현재 : 숭실대학교 컴퓨터공학과 (박사과정)

<관심분야>
멀티미디어 보안, DRM, RFID응용, 인증시스템

이 창 보(Chang-Bo Lee) [정회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 2007년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2007년 ~ 현재 : 숭실대학교 컴퓨터공학과 (박사과정)

<관심분야>
멀티미디어 보안, DRM, RFID응용, 인증시스템

이 광 형(Kwang-Hyoung Lee) [종신회원]

- 1998년 2월 : 광주대학교 전자계산학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 조교수

<관심분야>
멀티미디어 보안, 멀티미디어 데이터 검색, DRM, RFID 응용

전 문 석(Moon-Seog Jun) [정회원]

- 1981년 : 숭실대학교 전자계산학과 (공학사)
- 1986년 : University of Maryland Computer Science (공학석사)
- 1989년 : University of Maryland Computer Science (공학박사)
- 1989년 3월 ~ 7월 : Morgan State University 조교수
- 1989년 ~ 1991 : New Mexico State University Physical Science Lab 책임연구원
- 1991년 ~ 현재 : 숭실대학교 정교수