Ubi-Home에서의 지능적 멀티미디어 스트리밍을 지원하는 DRM 설계 및 구현

정회원 박 종 혁*, 이 상 진*, 홍 인 화**, 안 태 원**, 이 덕 규***

Design and Implementation of the DRM Supporting Smart Multimedia Streaming in Ubi-Home

Jong Hyuk Park*, Sang-Jin Lee*, In-Hwa Hong**,
Tae-Won Ahn**, Deok-Gyu Lee*** ***Regular Members***

요 약

본 논문에서는 Ubi-Home에서의 지능적 멀티미디어 스트리밍을 지원하는 콘텐츠 보호 및 관리 시스템(UHSMS-DRM: Ubi-Home Smart Multimedia Streaming-Digital Right Manaagement)을 설계 및 구현하였다. 제안 시스템은 Ubi-Home에서 디지털 콘텐츠의 저작권 보호 및 관리를 위한 유연한 유통 플랫폼을 제공하며, PC, STB, PDA, Portable device 등 다양한 디바이스의 인증을 통해 정당한 사용자에게 Multimedia Steaming Service를 제공한다. 그리고, 도메인 인증개념을 적용하여 Ubi-Home의 모든 디바이스에 대한 라이센스 관리의 효율성을 높인다. 또한, Ubi-Home에서 intelligent Service를 위해 사용자의 위치를 인지하기 위한 알고리즘을 제안 및 적용한다.

Key Words : Ubi-Home, DRM, Ubiquitous Sensor Network, User Location Recognition, Multimedia Service

ABSTRACT

In this paper, we design and implement the UHSNS-DRM(Ubi-Home Smart Multimedia Streaming-Digital Right Management) in Ubi-Home. The proposed system support flexible distribution platform for digital content copyright protection and management in Ubi-Home. This system also can provide multimedia streaming service to authorized users who are using PC, STB, PDA, and Portable Device, etc. Furthermore, we adopt concept of domain authentication and it help to improve the efficiency of license management for all devices in Ubi-Home. We design user's location recognition algorithm in order to provide intelligent services. Of course, this algorithm is applied for the proposed system. Start after striking space key 2 times.

Ⅰ. 서 론

컴퓨팅 파워의 급속한 발달은 도구에서 환경으로, 수백, 수천 개의 기기가 네트워크에 접속하며, 사람과 사람의 통신에서 사람과 머신, 사물과 사물간의 통신으로 통신 패러다임의 변화인 유비쿼터스 시대를 도래 시켰다. 유비쿼터스 컴퓨팅은 1998년 Xerox PARC의 Mark Weiser에 의해 제창되었으며, 일상생활의 모든 사물 및 공간이 지능화되고 언제 어디서나 제한 없는 접속을 통해 사용자에게 인식되지 않는 다수의 컴퓨터간 상호작용으로 사용자에게 유용한 서비스를 제공한다. 또한, 가정에서도 Ubi-Home환경이 조성되면서 윤택하고, 편리한 댁내 보안, 건강 모니터링, 전자상거래 등 다양한 서비스가

* 고려대학교 정보보호대학원 ({hyuks00, sjlee}@korea.ac.kr) ** 전자부품연구원 디지털미디어센터 (hongih@keti.re.kr),
*** 순천향대학교 정보기술공학부(hbrhcdbr@sch.ac.kr)
접수번호 : KICS2005-07-290, 접수일자 : 2005년 7월 15일, 최종논문접수일자 : 2006년 3월 13일

이루어 질 것이다[1-3].

그러나, 멀티미디어 서비스 측면을 고려해 보면, 현재 멀티미디어 서비스 환경은 멀티미디어 콘텐츠의 전달과 소비를 위한 다양한 프레임워크 및 요소들이 존재하고 있지만, 이러한 이종 요소간 상호운용적으로 멀티미디어 콘텐츠가 유통 가능한 프레임워크가 아직 존재하지 않는다. 따라서 Ubi-Home환경에 적합한 지능적이고 안전한 멀티미디어 서비스가 이루어질 수 있도록 체계적이고 효율적인 콘텐츠 보호 및 관리 시스템이 필요하다.

본 논문에서는 Ubi-Home에서의 디지털 콘텐츠의 저작권 보호 및 관리를 위한 유연한 유통 플랫폼을 제안하며, IP를 보유한 PC, IP-STB, 디지털 가전 등 다양한 디바이스 상에서 디지털 방송 콘텐츠인 MPEG-2/4 TS format 콘텐츠를 VOD와 Live 스트리밍 서비스를 통해 안전하게 수신할 수 있는 Ubi-Home에서의 DRM을 제안한다. 또한, 기존의 무선 네트워크 환경에서 제공하지 않는 위치 인식 알고리즘을 구현하여 지능적인 서비스를 지원하도록 하였다.

본 논문의 구성은 다음과 같다. II장에서는 Ubi-Home에서의 DRM 관련 기술 및 연구동향에 대해 살펴보며, III장에서는 Ubi-Home에서의 멀티미디어 DRM 요구사항에 대해 설명한다. IV장에서는 제안 시스템인 UHSMS-DRM의 설계, 프로토콜, 구현 및 분석에 대해 설명하고, V장에서는 향후 연구방향 및 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 Ubi-Home을 실현시키는 유비쿼터스 핵심 기술 및 DRM 관련 기술에 설명한 후, 홈에서의 DRM 연구 동향에 대해 살펴보도록 한다.

2.1 Ubi-Home의 멀티미디어 DRM 핵심기술

Ubi-Home 환경을 실현시키는 핵심기술인 유비쿼터스 센서 네트워크(USN: Ubiquitous Sensor Network)는 어떤 사건·현상내부나 그 주변에 조밀하게 배치된 마이크로 컨트롤러를 내장한 소형 컴퓨터 시스템인 센서노드들로 이루어지며, 그 내부는 센싱, 데이터 처리, 통신 모듈 등으로 구성된다[4]. 또한, 이러한 센서네트워크 모듈을 이용하여 인간과 컴퓨터간 상호 커뮤니케이션을 가능하게 하기위한 연구로 상황인지 컴퓨팅(CAC:Context Awareness Computing)에 대한 연구도 활발히 진행되고 있다. 여기에 사용되는 상황(Context) 정보에는 사용자 신체, 공간, 환경, 컴퓨팅 시스템 정보 등이 포함될 수 있다[5, 6].

멀티미디어 콘텐츠 응용분야에서 사용하는 모든 유형과 유통환경을 구성하는 표준 프레임워크인 MPEG-21(Moving Picture Experts Group)에서는 다양한 멀티미디어를 생성, 분배, 전송하는 사용자에 대한 투명성(transparent)과 이종 단말간의 상호운용성(interoperability) 제공을 목표로 표준화 활동이 이루어지고 있다. MPEG21-IPMP(Intellectual Property Management and Protection)는 이종 네트워크나 단말에서 모든 사용자가 그들의 저작권이나 디지털 아이템(DI: Digital Item, 콘텐츠)에 대한 동의를 표현하고, 지적 재산으로서 가치 있는 멀티미디어 콘텐츠에 대한 저작권을 효율적, 체계적으로 보호 및 관리하는 표준이다[7, 8].

2.2 홈에서의 DRM 연구 동향

홈 네트워크에서의 멀티미디어 보안(DRM) 연구 동향에 대해 살펴보면, 최근 적어도 두 표준기관인 디지털 비디오 방송과 TV Anytime은 홈 네트워크에서 콘텐츠 보호에 대해 주의를 돌리고 있다. Thomson의 SmartRight, Cisco의 OCCAM, IBM의 xCP Cluster Protocol에 의해 검토중인 세가지 제안들이 있다. Thomson의 SmartRight는 모든 장치에서 스마트 카드에 기반을 두고 있다. 이 스마트 마트는 공개키 인증서를 포함하고 있으며, 장치는 홈 네트워크에서 스마트 카드가 인증서를 교환하고 키를 설정하는 것을 도와준다. 스마트 카드는 콘텐츠 자체의 암호화와 복호화를 수행하게 된다. Cisco의 OCCAM(Open Conditional Content Access Management)시스템은 홈에 있는 각각의 장치들이 각 콘텐츠에 대해 유일한 "티켓"을 필요 하도록 하며, 이 티켓은 장치의 공개키에서 콘텐츠 키를 암호화 한다. 각각의 콘텐츠 소유자들은 티켓을 받기 위해 홈에 있는 인터넷에 접속된 모든 장치들을 가지고 자신의 티켓 발행 센터를 운영할 수 있었다. IBM의 xCP 클러스터 프로토콜은 브로트캐스트 암호화에 기반을 두고 있다. 홈에 있는 모든 장치들은 공통 미디어 키블락과 다른홈과 구별할 수 있는 유일한 ID를 설정하기 위해 협력한다. 홈에서의 콘텐츠는 암호학적으로 미디어 키와 아이디에 의해 제한된다. 보호된 콘텐츠는 자유롭게 홈에서 움직일 수 있지만 홈에서 다른 홈으로 이동하기 위해서 보조장치를 필요로 한다[14].

기타 표준화 동향을 살펴보면, 콘텐츠 미디어 스토리지 표준인 4C, 5C Consumer Electronics

Consortia는 각각 콘텐츠 저장 미디어-CPRM/CPPM와 내부 장치 통신에 대한 네트워크 프로토콜-DTCP에 관련된 표준들을 정의하고 있다. 4C 주체의 멤버 중 하나인 도시바는 작년 CPRM-compliant DVD를 소개했고, 이러한 스펙들은 홈 엔터테인먼트 네트워크 "솔루션"이 아니라 홈 디지털 엔터테인먼트 네트워크의 필수적인 기초라는 모두가 동의하는 것을 적용한다[15].

Ⅲ. Ubi-Home에서의 DRM 요구사항[11-14]

Ubi-Home에서 멀티미디어 콘텐츠 보호 및 유통을 위해서는 다음과 같은 요구사항들이 고려되어져야 한다.

· 콘텐츠 보호 및 유통: 콘텐츠 유통에서의 불법적인 접근에 의한 변조를 방지하기위해서, 콘텐츠는 암호화 되거나 스크램블 되어져야 한다. 일반적으로 DRM 제공자는 암호화 과정 및 알고리즘 등을 신뢰성 있게 유지해야 한다.

· 유연한 콘텐츠 및 디바이스 인증: Ubi-Home내의 각각의 디바이스들은 해당 콘텐츠와 비교되어 접근 권한을 제어하거나 미디어 콘텐츠를 시청하거나, 삭제 혹은 편집할 수 있는 유영한 인증 구조를 갖추어야 한다.

· 사용규칙 관리 및 콘텐츠 재분배: 콘텐츠 생성자와 배포자 사이의 계약관계에 따른 사용 규칙을 설정 및 관리할 수 있어야 하며, 분산환경에서의 유통을 고려하여 콘텐츠의 재분배가 가능해야 한다.

· 사용자 위치 인지: Ubi-Home에서의 지능적인 서비스를 위해 사용자의 위치를 인식하여 사용자 중심의 서비스를 제공할 수 있어야 한다.

· 저전력 무선 네트워크: 무선 센서를 이용하여 Ubi-Home네트워크를 구현하고, 궁극적으로 Ubi-Home보안 시스템에 필요한 유비쿼터스 센서 네트워크로 발전하기 위해서는 저전력 무선 네트워크 구조가 필요하다.

· Interoperability: 콘텐츠의 암호화 및 scrambling을 위해 표준 알고리즘 및 그와 관련된 키 알고리즘, license format 등이 서비스간이나 이종 디바이스간에 상호 호환될 수 있어야 한다.

Ⅳ. UHSMS-DRM

4.1 UHSMS-DRM 설계

우리의 제안 시스템은 [그림 1]과 같이 MPEG-2/4를 지원하는 VOD와 Real-time 스트리밍 서비스를 제공하는 DRM 부분과 사용자 중심의 미디어 서비스를 제공하기 위한 위치인지 시스템 부분으로 구성된다.

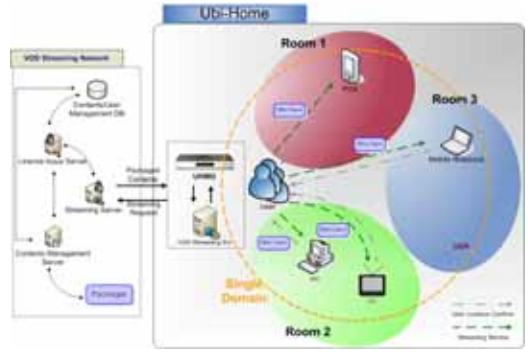

그림 1. UHSMS-DRM 구성도

4.1.1 Ubi-Home에서의 DRM 부분

[그림 2]는 Ubi-Home에서의 DRM 부분 상세 구성도를 나타내며 UHMG(Ubi-Home Multimedia Gateway)를 중심으로 스트리밍 서비스 전송 부분과 수신 부분으로 분류된다. 전송 부분은 VOD와 멀티캐스트 Live 스트리밍 서비스를 제공하는 스트리밍 서버, 디지털콘텐츠의 유통 전반에 대한 저작권 보호 기능을 수행하기 위한 콘텐츠 패키저와 라이센스 서버, 콘텐츠와 라이센스의 사용 로그에 대한 통계 및 모니터링 서비스를 제공하는 콘텐츠 관리 서버로 구성된다. UHMG를 통하여 스트리밍 서비스를 수신하는 부분은 Ubi-Home의디바이스로 구성되며 Ubi-Home은 하나의 Domain으로 지정된다. 즉, 사용자가 요청한 디바이스는 해당 Domain에 소속되고 그 디바이스들은 콘텐츠와 라이센스의 공유 및 사용이 가능해진다.

본 절에서는 일반적인 DRM의 구성요소인 패키져, 콘텐츠 관리 서버, 라이센스 관리서버에 대한

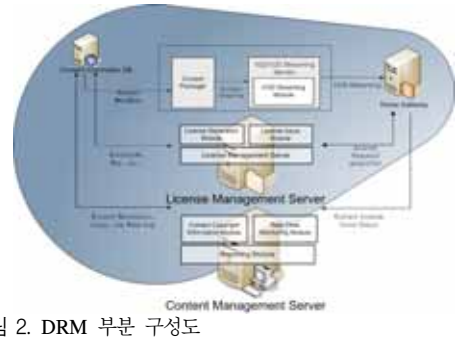

그림 2. DRM 부분 구성도

설명은 생략하며, 핵심개념인 도메인 및 사용자 identity monitoring에 대해 자세히 살펴보도록 한다.

−**UHSMS-DRM의 Domain**: Domain은 동일한 콘텐츠와 라이센스를 공유하는 디바이스들의 집합 개념으로 생각할 수 있으며, Ubi-Home내의 디바이스 간 디지털 콘텐츠와 라이센스의 자유로운 공유 및 유통을 관리하기 위하여 OMA DRM[12]의 Domain 개념을 확장·응용한다. UHSMS-DRM Domain에서는 하나의 Ubi-Home을 하나의 도메인으로 가정하며, Private Domain Key를 도메인 내의 장치들이 공유한다. 또한, 하나의 Domain은 한 개 이상의 도메인 키를 가지며, 디바이스들은 여러 도메인에 등록될 수 있다.

[그림 3]은 Domain의 등록 및 탈퇴에 대한 시나오를 나타낸다. Domain-00에는 4개의 디바이스가 등록되어 있으며, 디바이스 3과 4가 탈퇴함으로써 Domain Generation이 증가된다. Domain 3과 4는 도메인 키를 계속 보유하고 있으며 이미 구입한 콘텐츠를 이용할 수 있다. Domain-01에 속한 디바이스들은 Domain-01 및 Domain-00의 Key를 모두 가지고 있으므로 양쪽의 모든 콘텐츠를 이용할 수 있다. Domain 이동에 따른 콘텐츠의 사용은 콘텐츠별 라이센스 정책을 따른다. Domain-00에 속한 디바이스 A를 들고 Domain-01로 이동했을 경우 라이센스 정책은 다음과 같이 고려될 수 있다: 디바이스 A는 Domain-00에서 구입한 콘텐츠를 이용할 수 있으나, Domain-01에 속한 디바이스의 콘텐츠는 이용 및 재생이 불가능하다. 또한, 디바이스 A는 Domain-00에서 구입한 콘텐츠를 이용할 수 있으며, Domain-01에 속한 디바이스의 콘텐츠도 이용 및 재생이 가능하다.

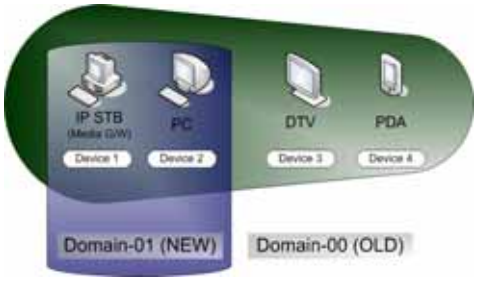

그림 3. Device의 Domain 등록/탈퇴

−사용자 **Identity** 모니터링: 사용자에게 맞춤형 서비스를 제공하기 위해서는 사용자의 Identity를 정확히 파악하는 것이 중요하다. 현재 사용자를 파악하기 위한 여러 방법이 있으나 서비스 구현이 가장 효율적인 방법은 센서 네트워크 노드에 해당 사용자 ID를 저장하고 사용하는 방법이 적합하다. 현재는 단말을 사용하는 사용자는 유일하다고 가정하며, 단말이 사용자를 자동으로 인식해서 어떤 사용자가 단말을 사용하고 있는지를 파악하는 것은 다른 기술적 문제이다. 미디어 파라미터와 같이 XML 형식으로 <user> 태그를 사용하여 사용자의 이름을 영문으로 기록하여 모바일 단말의 사용자를 구별한다.

4.1.2 Ubi-Home에서의 사용자 위치인지 부분

무선 네트워크 환경에서는 노드들이 무작위로 배치되며 노드들은 능동적으로 주변상황에 대응하여 정보를 전달한다. 이런 정보 전달을 위해서는 신뢰성 있은 위치 정보와 데이터의 전송이 중요하며 기존의 무선 네트워크 환경에서는 위치 인식 및 능동적인 주변 상황에 대응한 정보 전달 기능을 지원하지 않는다. 제안 시스템에서는 그리드 형태로 배치된 무선 네트워크를 기반으로 RSSI(Received Signal Strength Indicator)를 측정하여 무작위로 배치된 이동 노드들에 대한 위치 인식 알고리즘을 제안 및 구현한다.

위치인식 알고리즘은 [그림 4]와 같이 RSSI측정과 RSSI값을 이용한 삼각측량, 삼각 측량 값과 이동 노드의 움직임 평균속도에 의한 거리측정, 마지막으로 이 두 값의 비교 부분으로 구성되며, RSSI Sampling --> Location calculation --> Error compensation --> Estimate의 의 과정을 거쳐 위치를 인식하게 된다. 삼각측량 방식을 사용한 이유는 거리에 따른 RSSI의 상관 공식을 이용하여 거리로 환산할 수

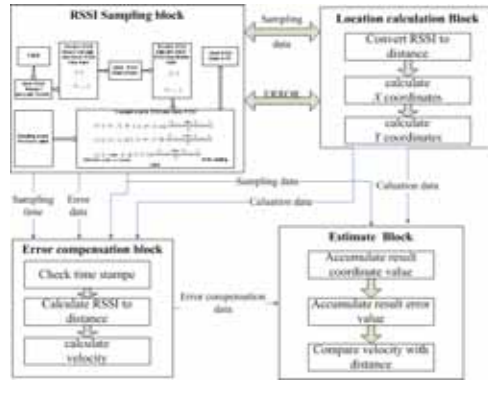

그림 4. 위치인지 알고리즘

있으며 각 노드의 거리를 알면 삼각측량으로 위치를 파악할 수 있어 최소한의 계산으로 비교적 정확한 위치 인식할 수 있기 때문이다.

RSSI를 측정하기 위해서 RSSI Request Message와 RSSI Reply Message로 구성된 메시지 포맷화 과정이 필요하며 버클리 대학에서 제공하는 TinyOS의 MAC[16]을 사용한다. RSSI는 주기적으로 RSSI Request Message 전송과 RSSI Reply Message의 수신, 측정된 RSSI값과 오차 값을 10회 누적 연산하였으며 PC로 데이터를 전송하기 위해서는 메시지 포맷화의 과정을 거치며 비교 과정에서 오차를 벗어난 값은 제거 한다. 노드에서 측정된 RSSI값을 식(1)을 이용하여 [그림 7]과 같은 테스트환경의 거리 a, b, c로 환산하며, 식(2), (3)을 이용하여 x, y 좌표를 환산한다. 또한, error compensation에서 측정된 RSSI값, sample time를 이용 이동 노드의 평균속도, 이동거리를 환산하여 Estimation block에서 값을 비교하여 위치를 인식한다.

$$\frac{\text{측정}RSSI\text{값} * \text{기준거리}}{\text{기준거리}RSSI\text{값}} \qquad \text{식(1) 거리 환산공식}$$

$$x = \frac{a^2 + b^2 - c^2}{2a} \qquad \text{식(2)} \qquad \text{x좌표}$$

$$y = \sqrt{b^2 - x^2} \qquad \text{식(3)} \qquad \text{y좌표}$$

4.2 프로토콜 설계

<표 1>은 본 논문에서 사용되어지는 시스템 계수를 설명 한다.

표 1. 본 논문에서 표현되어지는 시스템 계수

시스템 계수	의 미
ContentID	콘텐츠의 식별을 위한 고유 값
UserID	사용자 고유 값
DeviceID	디바이스 식별을 위한 고유값
EKey	콘텐츠 패키징에 사용되는 키
License	전자서명 되어진 라이센스
AUS	인증 서버
UHMG	Ubi-Home 멀티미디어 게이트웨이
CMS	콘텐츠 관리 서버
VSS	VOD 스트리밍 서버
CertificateX.509v3	X,509v3 포맷의 인증서
A	멀티미디어 서브스에 사용되는 콘텐츠 A
E(A)	콘텐츠 A를 패키징 함
DRMClient	콘텐츠 디패키징 및 콘텐츠 관련 권한을 부여하는 등의 DRM Client의 일련작업
Auth( )	사용자, 디바이스 인증
H( )	해쉬 함수
Cert( )	인증서 데이터

<라이센스 발급 프로토콜>

기본적인 라이센스는 다음과 같이 구성되어 있다.

$$License = (ContentID, DeviceID, Ekey, Certificatelicense)$$

ContentID는 유통되는 콘텐츠의 유일한 저작권 코드로 디지털 콘텐츠의 저작권을 명확하게 나타내며, 각 콘텐츠의 공통적인 검색키로 사용될 수 있다. DeviceID는 사용자의 특정 Device의 ID로 사용자와 그가 이용하는 하드웨어에 바인딩하기 위해 생성된 값을 가진다. 본 논문에서 DeviceID는 사용자 Device에 대한 고유한 값과 사용자 ID로 구성되며, 이 값은 안전한 스트리밍 서비스를 위해 Sequence number를 재생성하고, 클라이언트에서 다시 재 조합하여 정상적인 스트림 데이터로 변경하는데 이용된다. Rights는 콘텐츠의 중요도에 따라 다양한 등급으로 적용할 수 있으며, 등급에 따라 콘텐츠의 사용 횟수, 사용 기간, Device의 등록 수등을 제한할 수 있으며, 기본적인 DeviceID는 다음과 같이 구성되어 있다.

$$DeviceID = H(UserID \| DeviceID)$$

사용자는 라이센스 획득을 통해 콘텐츠에 대한 정당한 사용 권한을 부여받는다. 클라이언트의 관리 모듈은 사용자가 플레이어를 실행할 때, DRM 서버에 사용정보를 전달하여 콘텐츠 및 라이센스의 불법 사용을 방지한다.

멀티미디어 서비스에 대한 라이센스를 요청하고 획득하는 단계를 간단히 나타내면 다음과 같다.

Step 1. 콘텐츠의 사용 권한을 획득하기 위해 라이센스 발급 요청

$$User \rightarrow AUS:$$
$$Data(UserID \| DeviceID \| ContentID)_{Request}$$

Step 2. 인증서버는 사용자의 아이디 및 디바이스 아이디를 확인

$$AUS \rightarrow User:$$
$$H(ContentID \| License \| Certificate_{X.509v3})$$

Step 3. 사용자의 공개키를 이용하여 라이센스를 암호화하고 클라이언트에게 전송

$$AUS \rightarrow Auth(UserID, DeviceID)$$

Step 4. 클라이언트는 라이센스를 받고, 사용내역을 CMS에게 전송

$$User \rightarrow CMS:$$
$$License(UserID \| ContentID \| Certificateuser)$$

위 라이센스 획득 프로토콜을 선 요구사항으로 가정하고 본 논문에서 제안한 유비쿼터스 홈 환경에서의 Smart Multimedia Service를 위한 DRM의 전체적인 프로토콜은 다음과 같다([그림 5] 참고).

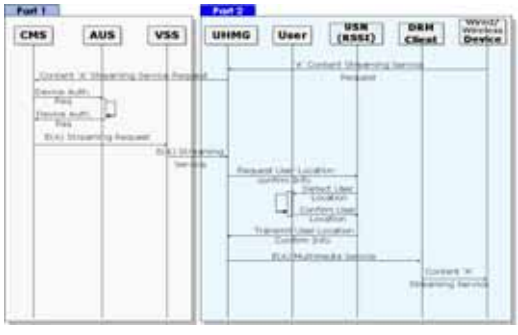

그림 5. UHSMS-DRM 프로토콜

<Part 1>

1. 디바이스는 자신의 UserID를 UHMG에 전송한 후, 콘텐츠 'A'의 스트리밍 서비스를 요청한다..

$$Device \rightarrow UHMG: A_{Request}$$
$$(UserID \| DeviceID \| ContentID)$$

2. UHMG는 CMS에 디바이스로부터 받은 정보를 전송한 후, 콘텐츠 'A'의 스트리밍 서비스를 요청한다.

$$UHMG \rightarrow CMS: A_{Request}$$
$$(UserID \| DeviceID \| ContentID)_{Request}$$

3. CMS는 AUS에 인증을 요청한다.

$$CMS \rightarrow AUS: Auth_{Request}$$
$$(UserID \| DeviceID \| ContentID)$$

4. AUS는 CMS에 인증정보를 전송한다.

$$AUS \rightarrow CMS: Cert$$
$$(DeviceID, UserID, Ekey, \cdots)$$

5. CMS는 인증정보를 받은 후, VSS에 콘텐츠 A에 대한 스트리밍 서비스를 요청한다.

$$CMS \rightarrow VSS: Request_{E(A)}$$

6. VSS는 패키징된 콘텐츠 A에 대한 스트리밍 서비스를 위해 UHMG에 이를 보낸다.

$$VSS \rightarrow UHMG: Streaming_{E(A)}$$

<Part 2>

7. UHMG는 USN module에 사용자 위치 정보를 요청한다.

$$UHMG \rightarrow USNmodule: Request_{Msg}$$

8. USN module은 UHMG에 사용자 위치정보에 대한 응답패킷을 전송한다.

$$USNmodule \rightarrow ? UHMG: Reply_{packet}$$

9. UHMG는 사용자 위치정보에 기반하여 DRM Client로 패키징된 콘텐츠 A를 전송한다.

$$UHMG \rightarrow DRM_{Client}: E(A)$$

10. DRM client는 콘텐츠 A를 디패키징한 후, 멀티미디어 스트리밍 서비스를 실시한다.

$$DRM_{Client} \rightarrow Device: A_{Content}(Straming)$$

4.3 UHSMS-DRM 시스템 구현

본 절에서는 DRM 부분과 위치인지 부분의 단계별 테스트 결과를 간단히 살펴보도록 한다. [그림 6]은 구현되어진 정당한 라이센스를 발급받아 콘텐츠가 재생되는 화면과 위치인지를 위해 구현되어진 USN module을 보여준다.

<표 2>는 제안 시스템의 유연한 Ubi-Home에서의 라이센스의 권한을 표현하는 REL의 일부분이다. MPEG-21 REL의 유통 메커니즘과 OMA DRM의 Super-distribution, Domain Mechanism을 보완 확장하며, 유무선 환경의 멀티미디어 device간의 호환성 있는 라이센스 포맷을 지원한다.

사용자 위치 인지 네트워크 구성을 위해 [그림 7]과 같이 환경을 구성하고 그리드 형태로 배치된 무선 네트워크를 기반으로 RSSI를 측정하여 무작위로 배치된 이동 노드들의 위치 인식을 측정한 결과 <표 3>과 같은 결과를 도출하였다.

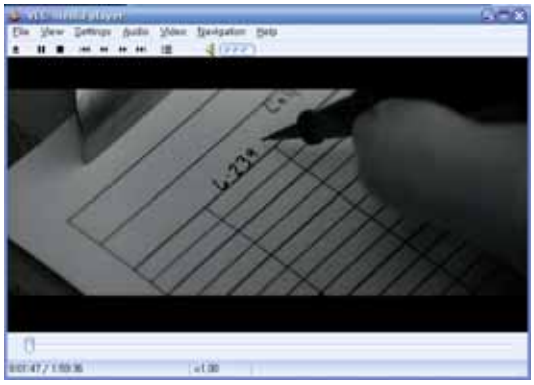

그림 6. 콘텐츠 재생 화면과 USN Module

표 2. 유연성있는 UHSN-DRM REL의 일부분

```
    // field where multimedia parameter is handled for location confirmation.
<Nodes>
      <Node id="6400">
            <BaseId>7e00</BaseId>
            <Computing>
                  <Codec>mpeg4,mpeg2</Codec>
              <Network>wlan,bt</Network>
                  <IP>192.168.1.10</IP>
                  <Resolution>1024x768</Resolution>
            </Computing>
        <Foraging>
            <Genre>movie,drama,sports,news,documentary</Genre>
            <Keyword>ring,band,brothers</Keyword>
             <Device>tv,radio,pc,pda,fridge</Device>
    </Foraging>
  </Node>
</Nodes>

// Domain structure for flexible content and device certification
<Domain>
    <DeviceID>12345</DeviceID>
    <DeviceID>67890</DeviceID>
</Domain>

// Granting certification key value on content ID concerned.
<asset>
     <context>
         <uid> cid:12345  </uid>
     </context>
     <KeyInfo>
          <KeyValue>vUEwR8LzEJoeiC+dgT1mgg==</KeyValue>
     </KeyInfo>
</asset>

//Restricting frequency and period for granting authority of media service.
<DigestValue>WgCxegWxrpb2kBOSttmf2P8ZFLI=</DigestValue>
<SignatureValue>
Ir+M11rC9vjXp79HHkTDTIGHj8pnh1mBC9PdgWDiH3qFnRFQhdhixmhttN
5HXuZUtNJRv5JrclsX7PeybEt1rCioctkQU7vCuaBdGJ1hdOxaWRLNceSstA
LhrDYizjeRcLu44ULv8Mm+YdkpisfOvAIyLR+emQu9UHmnnnnQ/bNQ=
</SignatureValue>
// limit counts and duration for authorization of multimedia service.
<permission>
     <play>
         <constraint>
              <count>5</count>
         </constraint>
    </play>   ....
```

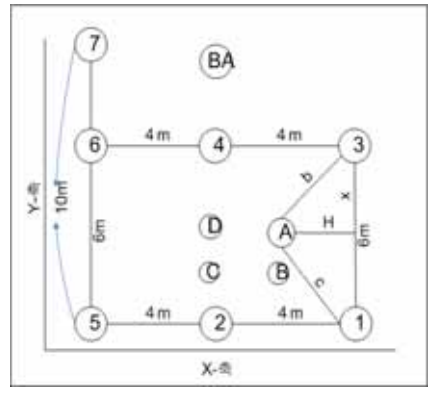

그림 7. 사용자 위치인지 테스트 환경

표 3. 실험 결과

Node 3 기준	실제좌표		계산값		RSSI 값		오차	
	X	Y	X	Y	노드1	노드3	X	Y
A지점	2	3	1.6	2.9	85	80	0.4	0.1
B지점	2	4	2.8	5.1	92	145	0.8	1.1
C지점	4	4	3.8	4.5	117	147	0.2	0.5
D지점	4	3	4.9	3.3	141	148	0.9	0.3

3.4 UHSMS-DRM 시스템 분석

<표 4>는 기존 DRM 시스템과 제안된 시스템과의 비교 분석을 보여준다. 제안시스템은 특정 디바이스 뿐만아니라 여러 디바이스나 콘텐츠도 병행 인증이 가능하고 디바이스 아이디에 따라 유연한 라이센스를 지원할 수 있다. 또한, 라이센스 포멧이 기존 시스템에서는 디바이스에 의존적이었으나, 제안 시스템에서는 고정 디바이스 및 이동형 디바이스간에 상호 호환적인 유연한 라이센스 포멧을 지원한다. 또한, Domain과 X.509 Device Certificate를 이용한 디바이스 인증방식을 적용하여 Domain에 소속된 디바이스 간 정책에 따른 디지털콘텐츠

표 4. 기존 DRM 시스템과 제안된 UHSMS-DRM 시스템의 비교

항목 / 비교 시스템	콘텐츠 재분배	유연한 라이센스 형식 지원	위치인지 기반 지능형 서비스	도메인 인증 기능 지원	디바이스 및 콘텐츠 병행인증
MS-DRM	O	△	X	X	△
Intertrust DRM	X	X	X	X	X
제안 시스템	O	O	O	O	O

(O: 양호, △: 보통, X: 미흡)

와 라이센스의 자유로운 공유 및 유통이 가능하도록 했다.

다음은 Ubi-Home에서 고려되어지는 공격들에 대한 제안 시스템의 안전성에 대해 설명한다.

－라이센스 변조 및 복제 방지: AUS를 통하여 사용자와 콘텐츠의 권한을 일정 기간동안 관리함으로써 라이센스의 검증을 하고 <표 2>와 같이 라이센스 내 전자서명을 통해 라이센스 횟수 조작 및 권한 변조등의 공격으로부터 라이센스 무결성을 보장한다. Base64로 엔코딩된 DigestValue를 컨텐츠 prvkey로 암호화시킨후 다시 베이스 64로 엔코딩 시켜 Signature로 사용하고, 클라이언트쪽에서는 위의 DigestValue를 1차 확인한후, 다시 Signature Value를 확인함으로써 라이센스의 변조 유무를 확인할 수 있다.

－불법 수신 공격 방지: 미디어 서비스를 받는 클라이언트는 UserID와 DeviceID를 이용하여 스크램블링 한 후 스트리밍 서버로 전송되므로 4.2절과 같이 해당 UserID나 DeviceID로 인증되지 않은 사용자에 대한 불법 수신 공격으로부터 콘텐츠를 보호한다.

－악의적인 네트워크 공격 방지: 네트워크상에 전송되는 모든 패킷들은 네트워크 성능에 따라 128비트 이상의 대칭키 암호화를 통하여 안전하게 전달함으로써 네트워크를 통한 악의적인 공격으로부터 기밀성 서비스를 방지한다. 디지털 홈 내의 스트리밍 서비스와 관련된 네트워크 환경은 ISMA등과 같은 보안성이 보장된 네트워크를 이용하였다.

－Device 복제 공격 방지: 각각각의Device들은 사용자 및 디바이스의 고유한 일련번호를 조합하여 라이센스를 부여하므로, Device가 복제되더라도 사용자 ID와 디바이스 ID, 그리고 전자서명 값이 일치하지 않으면 라이센스 발급을 중단하여 불법 사용자로부터 Device의 복제를 방지한다.

－사용자 위장 공격 방지: 사용자나 디바이스, 도메인(Domain) 인증은 X.509v3 인증서를 통하여 정당한 권한을 갖는 객체인지를 구분하고 해당 사용자의 등록된 DeviceID를 확인함으로써 위장 공격으로부터 인증 및 부인봉쇄 서비스를 제공한다.

Ⅴ. 결 론

본 논문에서는 Ubi-Home에서의 지능적 멀티미디어 서비스를 제공하는 콘텐츠 보호 및 관리 시스템을 제안한다. 그리고, Ubi-Home에서 디지털 콘텐츠의 저작권 보호 및 관리를 위한 유연한 유통 플랫폼을과 PC, STB, PDA, Portable device 등 다양한 디바이스의 인증을 통해 정당한 사용자에게 멀티미디어 스트리밍 서비스를 제공한다. 또한 도메인 인증개념을 적용하여 Ubi-Home의 모든 디바이스에 대한 라이센스 관리의 효율성을 증가 시킨다. 그리고, 기존의 무선 네트워크 환경에서 제공하지 않는 위치 인식 알고리즘을 구현하여 Ubi-Home에서의 지능적 서비스를 통하여 사용자 중심 서비스를 실현 한다.

향후, Ubi-Home에서의 멀티미디어 디바이스의 특성을 파악하여, 그에 적합한 해상도로 실시간 트랜스 코딩하여 최적화된 서비스를 제공할 수 있는 시스템에 대한 연구가 더 필요하며, 제안 시스템과 사용자의 프라이버시 보호가 고려된 모델과 접목하여 발전시킬 필요성이 있다.

참 고 문 헌

[1] Mark Weiser: Hot topic: Ubiquitous Computing, *IEEE Compute* (1993)

[2] Mark Weiser: The Computer for the 21st Century, *Scientific American* (1991)

[3] Zhexuan Song, Ryusuke Masuoka, Jonathan Agre, and Yannis Labrou: Task Computing for Ubiquitous Multimedia Services, *MUM '04* (2004)

[4] M. Satya: *IEEE Pervasive Computing Magazine*, http://www.computer.org/ pervasive

[5] A.K. Dey and G.D. Abowd: Towards an understanding of context and context awareness, *HUC99* (1999)

[6] Philip Robinson: Context-Awareness in trust management for Business Applications, *I-trust workshop* (2003)
[7] MPEG-21 Part1: Vision, Technologies and Strategy, *ISO/IEC JTC1/SC29/WG11 N4333* (2001)
[8] MPEG-21 Overview v.5, *ISO/IEC JTC1/SC29/WG11 N523* (2002)
[9] EICTA: *Content Protection Technologies*, http://www.eicta.org/copyrightlevies/index.html
[10] Bill Rosenblatt: *Year In Review: DRM Standards*, http://www.drmwatch. com/standards, DRM Watch(2004), 2005
[11] DMP: TIRAMISU *IST-2003-506983 DRM Requirements* (2004)
[12] http://www.openmobilealliance.org, OMA-DRM-REQ-v2_0-20030515-C.pdf(2003)
[13] MPEG-21 Overview v.5, *ISO/IEC JTC1/SC29/WG11 N5231*, Shanghai (2002)
[14] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard: Digital rights management for content distribution, *AISW2003* (2003)
[15] Tiny OS Community Forum, http://www.tinyos.net

박 종 혁 (Jong-Hyuk Park) 정회원

2001년 2월 순천향대학교 컴퓨터공학과 학사
2003년 2월 고려대학교 정보보호대학원 석사
2006년 2월 고려대학교 정보보호대학원 박사과정 수료
2002년 12월~현재 한화에스앤씨(주) 기술연구소 선임연구원
<관심분야> 유비쿼터스/홈네트워크 보안, 멀티미디어 콘텐츠 유통/보안, 접근제어

이 상 진 (Sang-Jin Lee) 정회원

1987년 2월 고려대학교 수학과 학사
1989년 2월 고려대학교 수학과 석사
1994년 2월 고려대학교 수학과 박사
1999년 3월~현재 고려대학교 정보보호대학원 부교수
<관심분야> 정보은닉이론, 블록암호 및 스트림 암호 분석과 설계, 암호 프로토콜, 컴퓨터 포렌식

홍 인 화 (In-Hwa Hong) 정회원

1992년 7월 서울산업대학교 전자공학과 학사
1995년 8월 숭실대학교 전자공학과 석사
1991년 10월~현재 전자부품 연구원 디지털미디어 연구센터 책임연구원
<관심분야> 디지털 방송, 방송통신 융합 Security, 홈 미디어 서버, USN기반 지능형 미디어검색

안 태 원 (Tae-Won Ahn) 정회원

2003년 2월 단국대학교 전자공학과 학사
2003년 7월~현재 한양대학교 정보통신 대학원 미디어 통신공학 석사과정
<관심분야> 임베디드 시스템, 센서네트워크, 라우팅

이 덕 규 (Deok-Gyu Lee) 정회원

2001년 2월 순천향대학교 컴퓨터공학사
2003년 2월 순천향대학교 전산학과 석사
2006년 2월 순천향대학교 전산학과 박사
<관심분야> Broadcast Encryption, DRM, EKE