Journal of Korea Multimedia Society Vol. 8, No. 11, November 2005(pp. 1531-1542)

유비쿼터스 홈 환경에서의 사용자 중심 멀티미디어 서비스

박종혁[†], 이상진[††], 고병수[†††], 이상원[††††]

요 약

유비쿼터스 홈 환경(UHE: Ubiquitous Home Environment)에서의 멀티미디어 서비스에서는 사용자의 직접적인 명령 없이 자동적으로 실행되는 지능화된 서비스 와 각각의 사용자에 맞는 맞춤형 서비스, 사용자 편의성 및 투명성, 이종 디바이스간 멀티미디어 콘텐츠의 상호 호환성 등의 요구사항이 증가할 것이다. 또한, 이에 적합한 멀티미디어 보호·관리 및 인증·권한관리 방식 등이 필요 할 것이다. 본 논문에서는 UHE에 적합한 인증방식을 제안·적용하며, 이종 기기간 멀티미디어 상호 운용성을 보장하며, 센서모듈과 홈서버를 이용한 상황정보(사용자 취향 정보, 디바이스정보 등)를 지능적으로 처리하고, 투명하고 안전한 서비스를 제공할 수 있는 사용자 중심 멀티미디어 서비스 (UHMS: Ubiquitous Home Multimedia Service)를 제안한다.

User-Oriented Multimedia Service in the Ubiquitous Home Environment

Jong-Hyuk Park[†], Sang-Jin Lee[††], Byoung-Soo Koh[†††], Sang-Won Lee[††††]

ABSTRACT

In multimedia service of Ubiquitous Home Environment(UHE), the requirements such as intelligent service that is executed automatically without direct order of user and fitted service compatible for each user and comfortable of user, interoperabilityof multimedia contents between incompatible devices will increase. Multimedia protection and management, authentication and authority administration methods that are suitable for above demands are also required. In this paper, we suggest authentication method suited for UHE and propose user oriented multimedia service(UHMS: Ubiquitous Home Multimedia Service) that provides the interoperability of multimedia between incompatible devices, conducts intelligently the context information(preference information, device information etc.) using sensor module and home server, provides and secure services.

Key words: Ubiquitous(유비쿼터스), Multimedia Service(멀티미디어 서비스), USN(유비쿼터스 센서 네트워크), Context Awareness(상황인지), IPMP(지적재산권 보호), DIA(디지털 아이템 적응)

1. 서 론

유비쿼터스 컴퓨팅은 1998년 Xerox Palo Alto Research Center의 Mark Weiser에 의해 제시되었다. 일상 생활의 모든 사물 및 공간이 지능화되고 언제 어디서나 제한 없는 접속을 통해 사용자에게 인식

※ 교신저자(Corresponding Author) : 박종혁, 주소 : 서울특별시 중구 장교동 한화빌딩 19층 한화S&C(주)(100-797), 전화 : 02)729-5662, FAX : 02)729-4934
E-mail : hyuks00@hanwha.co.kr
접수일 : 2005년 3월 10일, 완료일 : 2005년 6월 30일
[†] 정회원, 한화에스앤씨(주) 기술연구소 선임연구원
[††] 고려대학교 정보보호대학원 부교수
(E-mail : sangjin@korea.ac.kr)
[†††] ㈜디지캡 연구기획팀 책임연구원
(E-mail : bskoh@digicaps.com)
[††††] 전자부품연구원 디지털미디어연구센터 선임연구원
(E-mail : leesw@keti.re.kr)
※ 본 연구는 *산업자원부 신성장동력과제 (HISP과제) 및 **정통부/정보통신연구진흥원의 대학 IT연구 센터 육성지원사업의 연구결과로 수행되었음.

되지 않는 다수의 컴퓨터간 상호작용으로 사용자에게 유용한 서비스를 제공한다. 또한 UHE에서의 멀티미디어 서비스에서는 사용자의 직접적인 명령 없이 자동적으로 실행되는 지능화된 서비스 와 각각의 사용자에 맞는 맞춤형 서비스, 사용자 편의성 및 투명성, 이종 디바이스간 멀티미디어 콘텐츠의 상호운용성 등 요구사항이 증가하고, 이 환경에 적합한 멀티미디어 보호 및 관리, 인증・권한관리 방식 등이 필요 할 것이다[1-5].

본 논문에서는 UHE에 적합한 인증방식을 제안・적용하며, 이종 기기간 멀티미디어 상호 운용성을 보장하며, 센서모듈과 홈서버를 이용한 상황정보(사용자 취향 정보, 디바이스정보 등)를 지능적으로 처리하고, 투명하고 안전한 서비스를 제공할 수 있는 사용자 중심 멀티미디어 서비스를 제안한다. 본 논문의 구성은 다음과 같다. I장 서론, II장 유비쿼터스 홈 환경에서의 시스템 요구사항, III장 제안 시스템의 구조, 설계, 시스템 주체별 프로토콜 및 분석, 끝으로 IV장에서는 제안 시스템에 대한 고찰 및 결론을 맺는다.

2. 관련 연구

본 장에서는 유비쿼터스 컴퓨팅 핵심 기술 및 멀티미디어 서비스를 위한 요소기술에 대해 살펴본 후, 홈에서의 멀티미디어 보안 연구 동향에 대해 살펴보도록 한다.

2.1 유비쿼터스 홈의 멀티미디어 DRM 핵심기술

유비쿼터스 컴퓨팅을 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[6]. 또한, 이러한 센서네트워크 모듈을 이용하여 인간과 컴퓨터간 상호 커뮤니케이션을 가능하게 하기위한 연구로 상황인지 컴퓨팅(CAC:Context Awareness Computing)에 대한 연구도 활발히 진행되고 있다[7-9].

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(transparency)과 이종 단말간의 상호운용성(inter- operability) 제공을 목표로 표준화 활동이 이루어지고 있다. MPEG-21 IPMP(Intellectual Property Management and Protection)는 이종 네트워크나 단말에서 모든 사용자가 그들의 저작권이나 디지털 아이템(DI: Digital Item)에 대한 동의를 표현하고, 지적 재산으로서 가치있는 멀티미디어 콘텐츠에 대한 저작권을 효율적, 체계적으로 보호 및 관리하는 표준이다[10,11]. 그리고, MPEG-21 DIA(Digital Item Adaptation)는 디지털 아이템을 사용자 특성, 환경정보, 네트워크나 터미널의 특성을 고려하여 다양한 멀티미디어 콘텐츠의 소비를 가능하게 하기 위한 일반적인 멀티미디어 접근을 제공하기 위해 세부정보를 체계적으로 기술하는 규격을 정의하고 있다. 또한 DIA 처리 과정은 사용자 특성, 사용 터미널 및 네트워크 환경 등의 사용자 환경 정보를 기술한 DIA 기술 도구(Description Tools)를 기반으로 입력된 디지털 아이템을 리소스 및 기술자 변환 과정을 거쳐 적응된 디지털 아이템(Adapted DI)으로 출력한다. 비디오 트랜스코딩 기술은 하나의 포맷으로 코딩된 비디오 스트림을 다른 포맷의 비디오 신호로 변환하는 기술로 적응된 디지털 아이템을 기반으로 비디오 콘텐츠를 이동통신 단말 등에서 재생하기 위해 사용되고 있다[12,13].

2.2 홈에서의 멀티미디어 보안 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 콘

텐츠에 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 운영할수 있었다. IBM의 xCP 클러스터 프로토콜은 브로트캐스트 암호화에 기반을 두고 있다. 홈에 있는 모든 장치들은 공통 미디어 키 블락과 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 미디어CPRM/CPPM)와 내부 장치 통신에 대한 네트워크 프로토콜 DTCP)에 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].

3. UHE에서의 멀티미디어 시스템 요구사항 [16-19]

- **사용자의 편리성 및 투명성**: 유비쿼터스 홈 환경에서는 사용자가 홈 디바이스를 최대한 쉽게 사용할 수 있어야 하며, 유무선 통신을 통한 멀티미디어의 정보들이 전달될 때 지능적으로 미디어가 처리되는 기술이 필요하다. 또한, 사용자의 개입이 최소화되고 사용의 투명성이 제공되어야 한다.

- **멀티미디어 상호 운용성**: 기존의 멀티미디어 서비스에서는 디바이스마다 해상도가 정해져 있으므로 서로다른 디바이스간 서비스를 위해서 여러 포맷의 리소스가 준비되어야 했다, 그러나 유비쿼터스 홈 환경에서는 이종 디바이스간 멀티미디어 콘텐츠에 대한 상호 운용성을 제공하기 위해서는 미디어 트랜스코딩을 위한 디지털 홈 미디어 서비스가 제공되어야 한다.

- **사용자 및 디바이스 인증** : 유비쿼터스 홈에서는 현재 인터넷에서 사용되고 있는 사용자 인증과 함께 유비쿼터스 홈 환경에서의 원활한 서비스를 위해 디바이스의 인증을 통한 미디어 서비스가 제공되어져야 한다. 본 논문에서는 이 문제를 해결하기 위해 사용자 인증과 디바이스 인증을 이용하여 인증서(Certificate)를 생성하고, 주기적으로 인증서를 관리함으로써 유비쿼터스 디바이스의 불법 복제 사용 및 미디어 서비스의 불법 사용 방지 서비스가 제공되어야 한다.

- **안전한 라이센스 관리 프로토콜** : 기존 시스템은 무결성에 대한 고려사항으로 전송중인 메시지와 디바이스내의 정보의 변경여부를 확인하는 것이 국한되었다. 그러나, 유비쿼터스 환경에서는 메시지보다 디바이스 자체의 무결성과 더불어 멀티미디어 서비스를 위한 라이센스 파일의 위변조를 불가능 하도록 관리하는 것이 중요하다.

- 기밀성 : 유비쿼터스 홈에서 기밀성에 대한 고려사항으로 전송 데이터간의 암호화 및 키 관리기법, 디바이스의 계산능력이 고려되어진 저전력 암호화 알고리즘 개발 등이 일반적이다. 또한 계산량을 줄이기 위한 대칭키 암호의 적절한 사용과 무선통신의 취약점을 고려하여 중요한 정보 및 중앙 서버의 정보는 꼭 암호화하여 저장 및 전송되어져야 한다.

- 가용성 : 무선 네트워크 환경에서 가용성에 대한 공격으로 신호방해 공격을 고려할 수 있으며, 유비쿼터스 홈 환경내의 디바이스들에 대한 서비스 거부공격, 악성코드 공격 등에 대해 고려 되어져야 한다.

4. 제안하는 UHMS 시스템

4.1 UHMS 시스템 구성

본 논문에서 제안하는 UHMS는 크게 두 부분으로 구성된다. 멀티미디어 콘텐츠를 생성, 가공하여 UHE에 전송하는 과정과 UHE에서 사용자가 멀티미디어 콘텐츠를 소비하는 과정으로 구성된다. 전자는 [20]에서 제안된 방식의 멀티미디어 콘텐츠 유통 모델을 따르며, 본 논문에서는 후자인 UHE에서의 멀티미디어 서비스에 대해 자세히 논의하도록 한다(그림 1 참조).

4.2 시스템 설계

본 논문에서 제안하는 시스템은 UHS, UHMA, USN Module, End User의 4개의 주체로 구성된다.

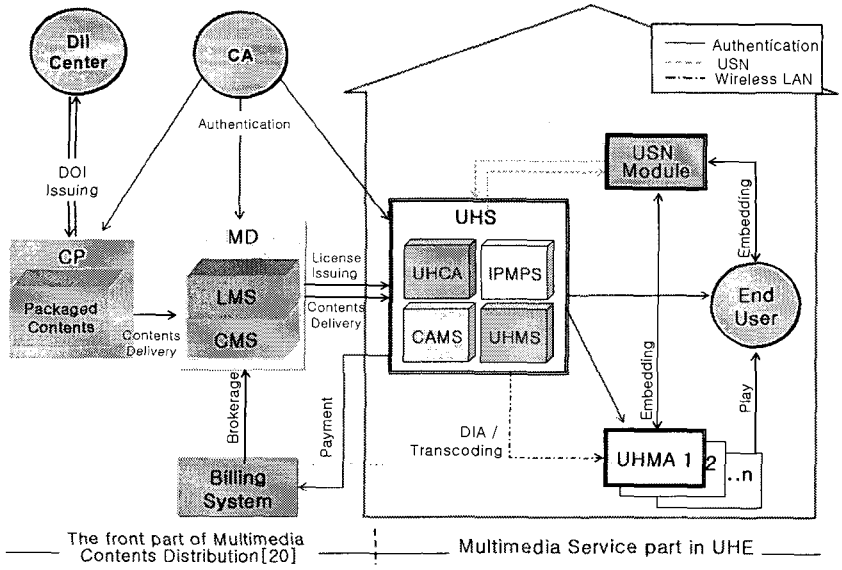


그림 1. UHSM 시스템 모델

① UHS (Ubiquitous Home Server) : UHE에서 시스템 구성의 핵심이며 UHCA, IPMPS, CAMS, UHMS로 구성된다.

그림 2는 UHS의 시스템 블록도를 나타내며, 네트워크 계층, 미들웨어 계층, 핵심 기능 계층과 사용자 인터페이스 계층으로 구성된다.

· UHCA(Ubiquitous Home Certificate Authority) : UHCA는 공인 인증기관에 의해 인증된 사설인증기관과 같이 UHE에서 사용자 및 UHMA에 대한 인증기능을 담당한다.

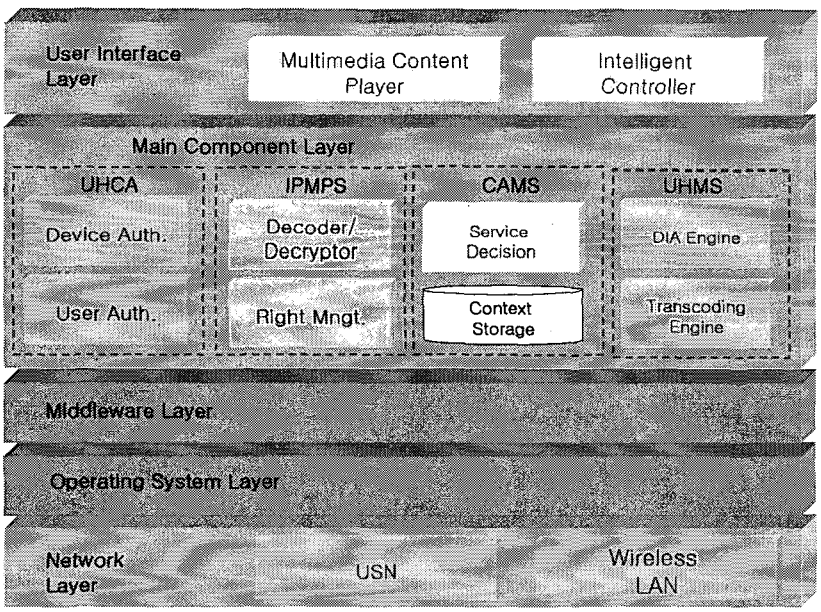


그림 2. UHS 블록 도

· IPMPS(Intellectual Property Management & Protection System) : IPMPS는 외부망를 통해 UHMS로 다운로드된 멀티미디어 콘텐츠에 대한 보안기능을 담당하는 부분으로, MPEG-21 IPMP 요구사항을 사용자에 대한 투명성(Transparency)이 보장될 수 있도록 UHE에 적합한 사용 권한설정, 위임, 관리 등 최소 보안 사항을 제공하는 역할을 한다. 표 1은 IPMPS에서 사용자의 권한 설정 및 위임 등을 위해 사용되는 사용권한 관리용 라이센스의 한부분이며, XML형태로 표현된다.

· CAMS(Context Awareness Management System) : CAMS는 USN Module이 유비쿼터스 센서 네트워크를 통해 수집된 상황정보(User location, User preference, User Multimedia starting/ ending Point 등)를 데이터베이스에 저장 및 관리하며, 현재 사용자의 상황정보를 수신받아 멀티미디어 서비스를 결정한다.

· UHMS(Ubiquitous Home Multimedia Server) : UHMS는 다운로드된 멀티미디어 콘텐츠를 각 UHMA 적합한 해상도 제공을 위해 MPEG-21 디지털 아이템 적응(DIA)과 실시간 비디오 트랜스 코딩을 적용하여 이종 멀티미디어 기기간 콘텐츠의 상호운용성을 제공한다.

② USN Module(Ubiquitous Sensor Network Module) : USN Module은 End User 및 UHMA에 부착되어 각 객체에 대한 상황정보(context) 수집 기능과 USN Module간 네트워크 통신을 담당한다. 그림 3은 USN Module 블록도를 나타내며, 4개의 계층으로 구성된다.

첫번째 계층인 Low Power Manager는 저전력 소비 관리 디바이스이며, 두번째 계층은 온도, 습도 등 일반적인 센서 외에 사용자의 위치정보 파악을 위한 움직임 감지 센서(motion sensor), 목소리 인지를 위한 음성센서(voice sensor), 밝기인지를 위한 밝기 센서(Brightness sensor), UHMA 상태점검을 위한 Device status check sensor 등을 포함하는 센서부분

표 1. 사용권한 설정 및 위임을 위한 라이센스의 일부분

```
<!usagerightsetting,management→
<grant><keyHolder licensePartID="hyuks"><info> <dsig:KeyValue>
    <dsig:RSAKeyValue><dsig:Modulus>... </keyHolder>
 <mx:play/><mx:diReference><mx:identifier>...</mx:identifier></mx:diReference>
 <trackQuery>
 <!--contentsusablecount→
 <notMoreThan>5</notMoreThan></trackQuery><fee><paymentFlat>
 <!contentsusabledate→
 <notBefore>2005-03-01T00:00:00</notBefore>...</validityInterval>
      <validityIntervalDurationPattern>
      <!usabledatefromissuingdate→
      <duration>P6D</duration></validityIntervalDurationPattern></grant>
 <issuer><timeOfIssue>2005-03-05T15:00:00</timeOfIssue></issuer>...
 <!rightauthorization→
 <entry>...<may-not-delegate/>
 <!usagerightauthorizationtoanotheruser→
 <using access>all}</using access>
 <valid><notBefore>2005-03-06T01:00:00</notBefore>
 <notAfter>2005-03-07T01:00:00</notAfter>
 <!validateduration→
 </entry><not-before>...</name></license>
 <!--XMLSignaturePart→
 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC
  -xml-c14n-20010315"/>...</Signature>
</Envelope>
```

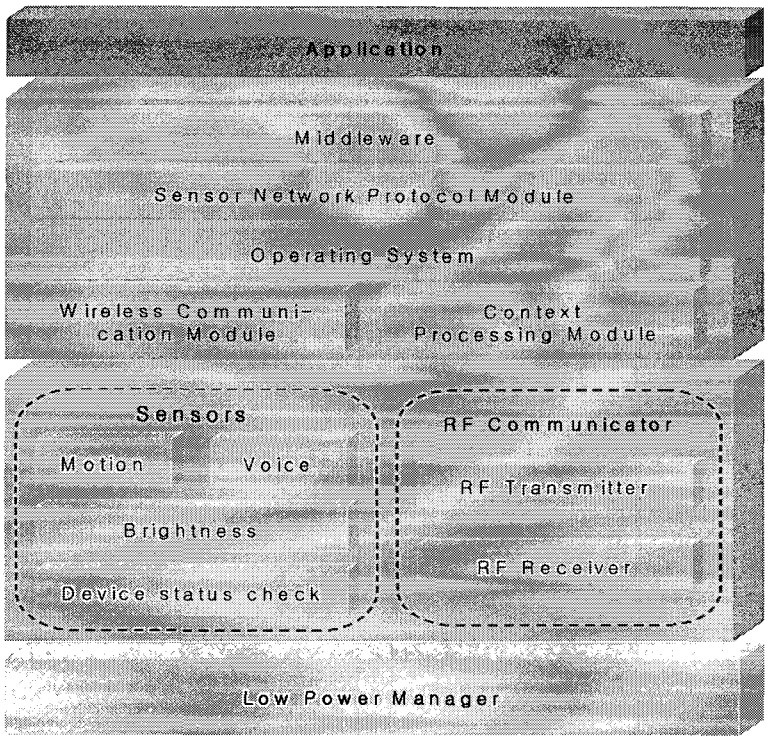


그림 3. USN Module 블록도

과 무선 통신 모듈 또는 Radio를 이용하여 900MHz / 2.4GHz로 데이터를 전송하는 RF Communicator로 구성된다. 세번째 계층은 운영체제, 무선 패킷전송 및 상황정보 처리를 위한 모듈, 센서 노드간 네트워크 구성을 지원하는 프로토콜 모듈, 전송된 미디어 메타데이터들을 이용하여 사용자 취향 데이터 결정 및 대상 단말의 동작 명령을 위한 미들웨어 부분으로 구성된다. 마지막 계층인 Application은 USN Module이 장착되는 주체(디바이스)에 필요한 서비스를 제공하기 위한 응용 프로그램이다(그림 3 참조).

③ UHMA (Ubiquitous Home Multimedia Appliance) : UHMA는 UHE에서 멀티미디어 콘텐츠를 디스플레이 해주는 장치로 PDA, PC, D-TV 등에 멀티미디어 서비스 기능이 강화되었으며, USN Module이 탑재되어 멀티미디어 디바이스의 상황정보를 유비쿼터스 센서 네트워크를 통해 전달하며, UHMS로부터 멀티미디어 콘텐츠를 재생할 디바이스에 적합하게 비디오 트랜스코딩된 미디어 서비스를 제공받는 주체이다.

④ End User : 음성, 지문 등의 생체인식을 통해 인증받은 정당한 사용자로 유비쿼터스 홈 내에서 멀티미디어 콘텐츠를 최종적으로 소비하는 주체이며, USN Module이 임베딩(embedding)된 디바이스(모바일 폰, 목거리, 시계 등)를 항상 휴대하고 있으며, 이를 통해 사용자의 위치정보 등 상황정보를 UHS로 실시간 전송할 수 있다.

4.3 시스템 동작 과정

제안하는 시스템의 동작 과정은 3개의 구간별 프로토콜로 구성되며, 구체적인 동작과정은 4.3.1~4.3.3에서 자세히 살펴본다.

표 2는 본 논문에서 사용되는 시스템 계수의 의미를 설명한다.

4.3.1 End User 및 UHMA와 UHS 간 인증 프로토콜

그림 4는 UHS의 UHCA, End User 및 UHMA 주체간 인증 과정을 나타내며, 각 Step은 다음과 같다.

STEP 1-3) User는 UHS의 인증서를 통해 UHS

표 2. 기호 설명

시스템계수	의 미
E , E′	서로 다른 대칭키 암호 알고리즘
SP	UHS의 공개키
k	USER, UHS가 세션마다 생성하여 사용하는 대칭키
r_1, r_2, r_3, r_4	Random Number
KEY	UHS와 UHMA간에 사전 약속된 대칭키
Certificate	인증서
E(Content)	패키징된 콘텐츠
Cont_Req	신규 콘텐츠 요청
Usr_Stat_Info	사용자 상황정보(사용자의 위치, 콘텐츠 재생 완료시점, 콘텐츠 관련 부가정보 등)
Updating_Cont_Adv	추가 신규 콘텐츠 정보를 알림(Advertising)
UA_Des_Info	UHMA의 서술(description) 정보
Adapted_Multi_Service	적응적 멀티미디어 서비스

를 인증하게 된다.

STEP 4-6) ⑦~⑨ 단계의 사용자 인증시 대칭키 암호를 사용하기 위해 User와 UHS간 세션키 생성 후 키를 공유한다.

STEP 7-9) UHS가 사용자를 인증한다.

STEP 10-12) UHS와 UHMA간 사전 공유된 대칭키를 통해 상호 인증(식별)을 하는 과정으로서 상호간의 안전성 및 기밀성 보장을 위해 두 개의 암호화 알고리즘을 이용한다.

4.3.2 UHS와 End User간 프로토콜

그림 5는 UHS의 UHCA, IPMPS, UHMS, CAMS와 End User사이의 프로토콜로 멀티미디어 콘텐츠를 소비하는 사용자가 인증후, UHS를 통해 원하는 콘텐츠를 다운로드받아 소비하기까지의 과정을 나타내며, 각 Step은 다음과 같다.

STEP 1) 위 4.3.1에서 살펴본 UHE에서의 사용자 및 UHMA 인증방식을 사용하여 인증한다.

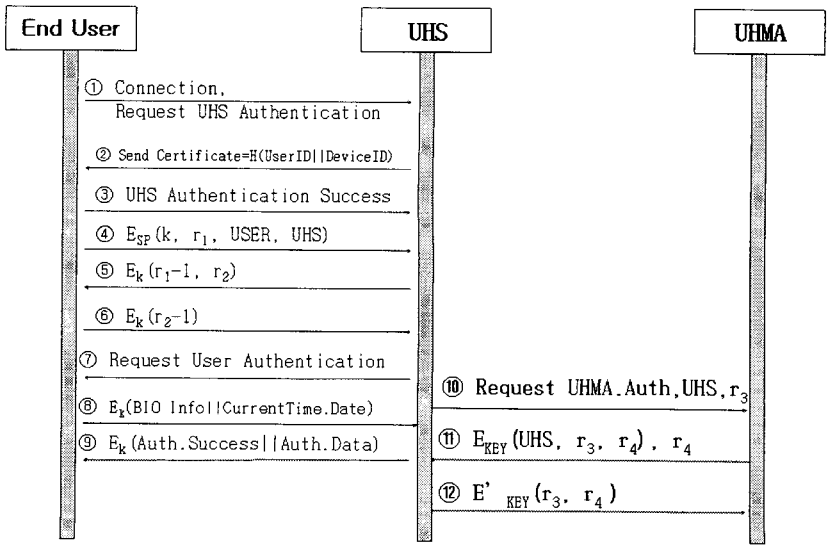


그림 4. End User 및 UHMA와 UHS 간 인증 프로토콜

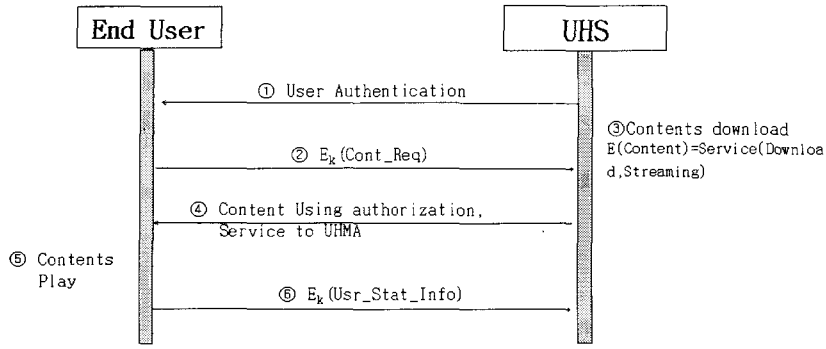


그림 5. UHS와 End User간 프로토콜

STEP 2-3) 인증된 사용자는 UHS를 통해 원하는 새로운 멀티미디어 콘텐츠를 UHS에 요청하며, 외부망을 통해 UHMS에 콘텐츠가 다운로드 및 멀티미디어 서비스가 지원 된다.

STEP 4-5) UHS의 IPMPS는 사용자에 대한 콘텐츠 사용권한 설정, 인가, 위임 등 권한 관리를 통해 사용권리를 통제하며, 사용조건이 만족할 때 콘텐츠를 재생 한다.

STEP 6) 콘텐츠를 재생하는 동시에 향후 사용자 중심 서비스를 위해 사용자 위치, UHMA 상태, 멀티미디어 콘텐츠 정보, 콘텐츠 재생 시작 / 종료 시점 등 상황정보를 UHS의 CAMS로 전송한다.

4.3.3 UHS와 USN Module 및 UHMA 간 프로토콜

그림 6은 UHS의 UHMS와 USN Module 및 UHMA간 프로토콜이며, 각 Step은 다음과 같다.

STEP 1) UHS는 사용자의 요청에 의해 다운로드된 신규 콘텐츠에 대한 갱신된 정보를 USN Module을 통해 UHMA에 알린다(Advertising).

STEP 2-3) CAMS는 현재 사용자의 위치정보 및 가장 근접된 UHMA의 Description 정보 수신 후, 사용자 상황정보를 고려하여 서비스를 결정한다.

STEP 4-6) CAMS는 UHMS로 DIA및 비디오 트랜스코딩기법을 적용하여 적응적 멀티미디어 서비스를 명령하며, UHMS는 UHMA로 고화질 미디어 서비스를 제공하여 콘텐츠를 재생하게 된다.

4.4 제안 시스템 분석

4.4.1 성능분석

본 절에서는 표 3에서 보는것과 같이 4가지 항목에 대해 기존 시스템과 제안 시스템에 대한 성능 비교분석에 대해 논하고자 한다.

· UHE 환경에 적합한 사용자 및 디바이스 인증방

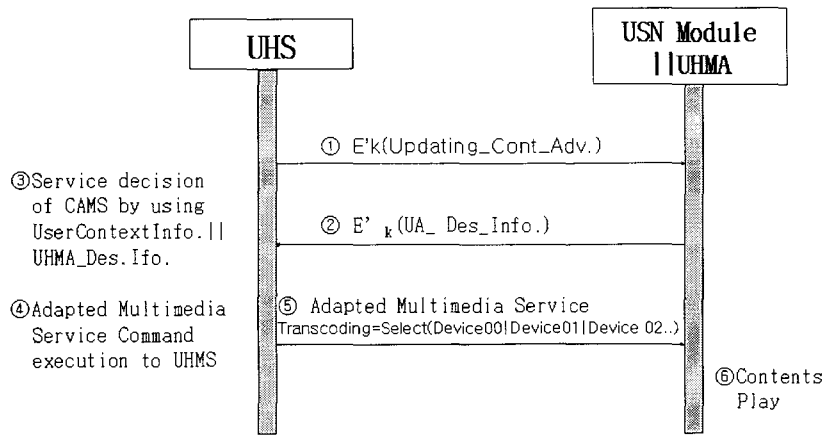


그림 6. UHS와 USN Module 및 UHMA간 프로토콜

표 3. 기존 시스템과 제안 시스템의 비교

내 용	기존 홈 네트워크 시스템 (KT/SKT 시범사업 등)	제안 UHMS 시스템
홈내 사용자, 디바이스 인증 방식의 안정성 및 효율성	단순한 인증 방식	고유한 사용자 아이디와 디바이스 아이디와의 조합 인증 지원
사용자 중심 멀티미디어 서비스	지원되지 않음	자작콘텐츠 및 유통등 제어 가능 저전력 위치 인지 기반의 멀티미디어 콘텐츠 제어 가능
홈내 멀티미디어 디바이스간의 멀티미디어의 상호 운용성 서비스	PC나 TV 디바이스에 국한	멀티미디어 실시간 트랜스코딩과 디바이스 인증을 통한 다양한 이종간 디바이스 지원
홈내 멀티미디어 콘텐츠 사용 권한관리의 효율성	XrML 기반 라이센스 방식	권한 위임 라이센스 방식

식: 기존 시스템에는 사용자 인증시 주로 PKI를 이용한 공인인증서 방식을 사용하며, 디바이스 인증은 ISP(Internet Service Provider) 등 서비스 사업자 별도 CA를 통해 디바이스를 인증한다. 이 방식에서 홈내 디바이스 인증시 매 세션마다 공개키 방식을 사용함에 따른 연산량 증가에 의한 속도 저하, 새로운 디바이스 추가시 ISP사업자의 CA를 통한 별도의 추가 인증 등 문제점들이 존재한다. 그러나, 제안 시스템에서는 사용자 및 디바이스 인증을 초기 셋팅시 상위 인증기관으로부터 인증된 하위 사설 인증기관 역할을 하는 UHS서버에서 담당하며, 디바이스 인증시 공개키 대신 사전 상호 공유된 대칭키 방식을 이용하여 속도면에서도 효율성을 도모한다. 4.3.1 인증 프로토콜은 콘텐츠의 도용을 방지하기 위해 사용자 인증 정보와 디바이스 정보를 동시에 인증하는 알고리즘을 사용하였다. 사용자의 아이디와 디지털 홈 네트워크 내의 각각의 디바이스들에 대한 고유한 아이디를 이용하여 인증 과정을 수행하므로 프라이버시 정보 유출 및 아이디 오용을 방지할 수 있다.

· 사용자 중심 멀티미디어 서비스: 기존 시스템은 CP가 제공하는 콘텐츠가 홈내에 다운로드/스트리밍 서비스되면 사용자가 선호 콘텐츠를 선택하고, 재생시킬 디바이스를 찾아 수동적으로 명령을 내린다. 즉 모든 액션에 사용자의 개입이 있어야 처리 됐으나, 제안 시스템에서는 사용자의 선호(취향) 정보, 위치 정보 등을 사용자의 수동적인 개입 없이 자동적으로 처리될 수 있는 UHE에 적합한 사용자 중심의 멀티미디어 서비스를 제공한다. 제안 시스템은 CP(Content Provider)와 관리(Management), 재분배(Super Distribution)등의 동시 처리가 가능하도록 구성되어 있으며, 다운로드 방식과 더불어 유니캐스트(Unicast)와 멀티캐스트(Multicast)와 같은 미디어 서비스를 제공함으로써 디지털 홈 기반의 사용자 중심 멀티미디어 서비스가 가능하도록 구성되었다.

· 멀티미디어 디바이스간 멀티미디어 상호 운용성: 기존 시스템에서는 홈 내의 이종 디바이스간에 멀티미디어 서비스가 각각 이루어 졌으며, 이를 위해 미리 각 디바이스에 적합한 콘텐츠가 준비 되어져 있어야 했다. 그러나, 제안 시스템에서는 적응적 디지털 아이템(Adapted Digital Item) 및 실시간 비디오 트랜스 코딩을 통해 하나의 콘텐츠로 이종 디바이스간에 서비스될 수 있는 멀티미디어 상호 운용성을 제공한다. 그리고 각각의 디바이스들은 사용자와 상호 인증이 가능하도록 설계하여, 한명의 사용자가 PC나 TV, PDA와 같은 여러 디바이스에서 하나의 콘텐츠를 시청할 수 있도록 하는 적응적 멀티미디어 서비스를 지원한다.

· 멀티미디어 콘텐츠 사용 권한관리의 효율성: 기존 시스템에서는 일반적인 온라인 콘텐츠 보호를 위한 사용 권한 관리를 위해 XrML기반 라이센스 방식을 사용했다. 이 방식은 사용자 A가 사용자 B로 사용 권한을 위임할 경우 다시 외부의 라이센스 관리 서버에 접속해야 하는 불편함이 있다. 그러나, 제안 시스템에서는 UHS의 IPMPS를 통해 권한위임 가능한 라이센스 방식을 사용하여 사용자의 편의성 및 권한 관리의 효율성을 증가할 수 있다.

4.4.2 안전성 분석

본 절에서는 UHE에서의 멀티미디어 서비스 시

고려되어져야 할 공격(반사공격, 라이센스 위·변조 공격, IP 스푸핑 공격)에 대한 제안 시스템의 안전성에 대해 논하고자 한다.

· 반사공격(Reflection Attack): 그림 4의 ⑩단계에서 UHS가 UHMA에게 난수 r3 전송, ⑪단계에서 UHMA가 UHS에게 E_{KEY}(r3)와 r4전송, ⑫단계에서 UHS가 UHMA에게 E_{KEY}(r4)를 보내는 방식으로 상호 개인식별을 할 경우, 1개 이상의 세션을 동시에 여는 것이 가능한 응용 환경하에서는 UHS를 가장한 공격자가 ⑪단계이후 두 번째 세션을 시작하여 UHMA에게 r4을 전송하면 이에 대해 UHMA는 E_{KEY}(r4)와 또 하나의 난수를 UHS에게 전송한다. 이때 두 번째 세션을 공격자가 일방적으로 종료 후 첫 번째 세션의 ⑫단계를 진행하기 위해 KEY를 몰라도 획득한 E_{KEY}(r4)을 전송함으로써 UHMA는 UHS를 정당한 사용자로 인식하게 된다.

본 시스템은 UHS와 UHMA간 인증시 동일 암호화 방식 사용에 의해 발생되는 이러한 반사공격[21]을 해결하고자 4.3.1에서 보는것과 같이 두 개의 대칭키 암호화 알고리즘을 사용함으로써 안전성을 확보할 수 있다.

· 라이센스 파일 위·변조 공격: 콘텐츠의 사용을 위해서는 권한이 정의 되어져 있는 라이센스 파일이 중요하다. 공격자가 라이센스 파일을 가로채어 위·변조하여 사용권한을 획득한다면 시스템의 안전성은 더 이상 보장될 수 없게 된다. 본 시스템은 표 1에서 보는것과 같이 XML 서명을 사용하여 라이센스 파일의 위·변조를 방지할 수 있다.

· IP 스푸핑(Spoofing) 공격: 홈 내에서 디바이스들 간의 상호 명령을 위해 무선통신 방식인 WLAN을 사용한다. 무선신호는 건물의 벽을 통과 할 수 있어 외부 공격자의 홈 내 시스템 접속이 가능하여 항상 도청의 위협이 존재한다. 본 시스템에서는 4.3 프로토콜들에서 보듯이 중요 정보 패킷에 대해서 대칭키 암호화 알고리즘을 사용하여 패킷 암호화를 적용 IP 스푸핑 공격을 방지할 수 있다.

· 서비스 거부 공격(DoS): 공격자는 UHS에 대량의 패킷을 보내거나 UHS 및 UHMA간 WLAN 통신을 방해하기 위해 Radio Wave를 보낼수 있다. 본 시스템에서는 UHS에 사용자 및 기기 인증 및 UHMA 통신에만 자원을 할당하여 DoS공격을 최소화할 수 있다.

5. 결 론

본 논문에서 제안한 UHMS 시스템은 기존 홈 네트워크에서 서비스 되는 일반적인 멀티미디어 서비스의 한세대 발전된 형태로 유비쿼터스 시대의 핵심 기술인 상황인지 정보를 유비쿼터스 센서 네트워크 기술과 접목하여 사용자 중심의 멀티미디어 서비스를 제공한다. 또한, 현재 홈내에서 이종 멀티미디어 디바이스간 상호 호환 서비스의 문제점을 해결하여 서로 다른 디바이스간 해상도를 적응적으로 파악하고, 그에 적합한 비디오 트랜스 코딩을 통하여 문제점을 해결한다. 마지막으로, 사용자 및 홈 디바이스간 인증의 안전성 및 효율성을 향상시킬 수 있는 방식을 제안·적용하였으며, 유비쿼터스 홈내의 멀티미디어 사용 권한 관리의 효율성을 증가시켰다.

향후, 본 논문에서 제안된 사용자 중심 멀티미디어 서비스에 사용자의 프라이버시 보호가 고려된 모델과 접목하여 보완 발전시킬 필요성이 있다.

참 고 문 헌

[1] Mark Weiser, "The Computer for the 21st Century," *Scientific American*, pp. 94-104, 1991.

[2] Mark Weiser, "Hot topic: Ubiquitous Computing," *IEEE Computer*, pp. 71-72, 1993.

[3] Muhlhauser, M, "Ubiquitous Computing and Its Influence on MSE," *Proceedings of International Symposium on Multimedia Software Engineering*, pp. 48-55, 2000.

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

[5] Jong Hyuk Park, Heung-Soo Park, Sangjin Lee, Jun Choi, and Deok-Gyu Lee, "Intelligent Multimedia Service System Based on Context Awareness in Smart Home," *KES'05*, pp. 1146-1152, 2005.

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

[7] Philip Robinson, "Context-Awareness in trust

management for Business Applications," *I-trust workshop*, 2003.

[8] A.K. Dey and G.D. Abowd, "Towards an understanding of context and context-awareness," *HUC99.*, 1999.

[9] Cliff Randell and Henk Muller, "Context Awareness by Analyzing Accelerometer Data," http://www.cs.bris.ac.uk/Tools/Reports, 2000.

[10] "MPEG-21 Part1: Vision, Technologies and Strategy," ISO/IEC JTC1/SC29/WG11 N4333, 2001.

[11] "MPEG-21 Overview v.5," ISO/IEC JTC1/SC29/WG11 N523, 2002.

[12] "MPEG-21 Digital Item Adaptation AM (v.5.0)," ISO/IEC JTC1/SC29/WG11 N5613, 2003.

[13] W. X. Guo, Z. W. Guo, and Ahmad, "MPEG-2 To MPEG-4 Trans-coding," *Proceeding of Workshop and Exhibition on MPEG-4*, pp. 83-86, 2002.

[14] EICTA: Content Protection Technologies, http://www.eicta.org/copyrightlevies/index.html.

[15] Bill Rosenblatt: Year In Review: DRM Standards, http://www.drmwatch.com/standards, DRM Watch(2004), 2005.

[16] Enyi Chen, Degan Zhang, Yuanchun Shi, and Guangyou Xu, "Seamless Mobile Service for Pervasive Multimedia," *PCM2004*, pp. 754-761. 2004.

[17] Frank Stajano, *Security for Ubiquitous Computing*, Wiley, 2002.

[18] Zhexuan Song, Ryusuke Masuoka, Jonathan Agre, and Yannis Labrou, "Task Computing for Ubiquitous Multimedia Services," *MUM2004*, pp. 27-29. 2004.

[19] Buxton, W., "Ubiquitous Media and the Active Office," http://www.billbuxton.com/ ubicomp.html

[20] Jong-Hyuk Park, Sung-Soo Kim, Jae-Won Han, and Sang-Jin Lee, "Implementation of the H-IPMP System Based on MPEG-21 for secure Multimedia Distribution Environment," *WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS*, Issue 5, Vol. 1, pp. 1301-1308, 2004.

[21] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, pp. 503, 1996.

박 종 혁

2001년 2월 순천향대학교 컴퓨터공학과 학사
2003년 2월 고려대학교 정보보호대학원 석사
2004년 3월 ~ 현재 고려대학교 정보보호대학원 박사과정
2002년 12월 ~ 현재 한화에스앤씨(주) 기술연구소 선임연구원
관심분야 : 유비쿼터스/홈네트워크 보안, 멀티미디어 콘텐츠 유통/보안, 접근제어

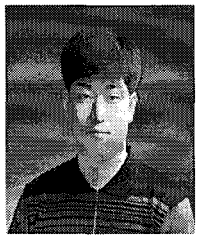
이 상 진

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

고 병 수

2000년 2월 호남대학교 컴퓨터공학과 석사
2004년 8월 대전대학교 컴퓨터공학과 박사
2004년 8월~현재 ㈜디지캡 연구기획팀 책임연구원

관심분야 : DRM, Computer Forensics, Digital Home



이 상 원

1995년 2월 시립 인천대학교 전자공학과 졸업
1995년 1월~1997년 10월 ㈜휴니드 테크놀러지스
1997년 11월~2000년 8월 ㈜이스텔시스템즈
2000년 10월~현재 전자부품연구원 디지털미디어연구센터 선임연구원

관심분야 : 유비쿼터스, 센서 네트워크, 센서 네트워크 하드웨어