비인가 무선접속 모드를 이용한 디지털 멀티미디어 방송의 제한 수신시스템의 인증 제안

The Proposed UMA Mode in DMB CAS Authentication Process

오세갑*, 강희조*

Se-Kab Oh*, Heau-Jo Kang*

요 약

본 논문은 방송과 통신이 결합한 디지털 멀티미디어 휴대 이동 통신 단말기에 관한 연구로, 디지털 멀티미디어 방송을 수신할 수 있는 휴대 단말기에 유무선 통합 솔루션을 제공할 수 있는 UMA(Unlicensed Mobile Access)기능을 포함시키고 UMA 망을 위한 UNC(Universal Naming Convention)에서 CAS(Conditional Access System) 시스템을 지원할 경우, 단말기가 AP를 통해 CAS 인증을 받고 방송 신호를 수신하는 방법으로 단말기 사용자는 본인이 원하는 콘텐츠에 대한 원하는 시간만큼의 시청을 하고 이에 대한 요금만을 부과할 수 있는 시스템 인증을 제안한다.

Abstract

In this paper refer to the digital multimedia mobile phone with the combination of broadcasting and the communication the unity of wire and wireless solution that can provide the UMA(Unlicensed Mobile Access) function is added. In UNC(Universal Naming Convention) in the case of CAS(Conditional Access System) is supported, the device(mobile phone) is authenticated through AP and then following the method of broadcasting signal the user can view the wanted contents as long as they want and for this matter the service charge system are proposed.

Keyword : Unlicensed Mobile Access, CAS, DMB, Universal Naming Convention, Authentication

I. 서 론

DMB는 차량용 소형TV, 노트북, PDA, 휴대폰 등과 같은 소형 단말을 이용하여 장소와 시간에 구애받지 않고 고속 이동 중에도 동영상 및 CD(Compact Disc) 수준의 오디오는 물론 다양한 멀티미디어 데이터 서비스에 대하여 안정적으로 수신이 가능한 이동 멀티미디어 방송으로서 세계 최초로 국내에서 서비스 표준을 정하고 상용화 서비스를 하고 있다[1].

그러나 디지털 데이터의 통합 방송에 있어서 송신측과 수신측 사이에 상호 보안성이 확립되지 않을 경우 방송의 상업적 구조가 무너지게 된다. 그리고 방송사업자는 가입자에게 양질의 방송 서비스를 제공하기 위하여 시청료를 징수하는 유료 방송 서비스를 제공하며, 송출된 다양한 멀티미디어 데이터가 보호되어 정당한 수신권한이 있는 인증된 가입자만 수신할 수 있기를 바르는데 이러한 문제를 해결하기 위해 개발된 것이 CAS(제한수신시스템)이다[2].

* 목원대학교 대학원 IT공학과 (Dept. of Information Technology Eng., Graduate School, Mokwon University)
· 교신저자(Corresponding Author) : 강희조
· 접수일자 : 2008년 5월 13일

본 논문은 디지털 멀티미디어 방송을 수신할 수 있는 휴대 단말기에 유무선 통합 솔루션을 제공할 수 있는 UMA기능을 포함시키고 UMA 망을 위한 UNC에서 CAS 시스템을 지원할 경우, 단말기가 AP를 통해 CAS 인증을 받고 방송 신호를 수신하는 방법으로 단말기 사용자는 본인이 원하는 콘텐츠에 대한 원하는 시간만큼의 시청을 하고 이에 대한 요금만을 부과할 수 있는 방법과 장치에 관하여 제안한다.

Ⅱ. 기존 기술 분석

2-1 기존 기술의 문제점

CAS(Conditional Access System)란 DMB 수신장치 내부에 저장된 코드를 통해 인증이 된 코드이면 방송 수신이 가능하고 인증이 되지 않는 코드이면 방송 수신을 할 수 없게 하는 장치이다. 이 장치를 통해 사업자는 사용자들에게 요금 징수가 가능하다. 그러나 DMB 수신 장치 내부에 저장된 코드로만 인증을 하게 된다면 사용자는 방송 시청 여부를 떠나 DMB 방송을 수신하기 위해서는 항상 사업자 측에서 정해놓은 일정액을 지불해야만 하는 단점이 있다. 그러나 본 논문에서 제안하는 AP를 통한 CAS 인증은 휴대 단말기 사용자가 AP가 있는 곳이라면 언제든 UMA 망에 접속하여 CAS 인증을 받고, 원하는 콘텐츠에 대해서 원하는 시간만큼의 방송 시청을 요구할 수가 있고, 이에 대한 요금만을 부과하면 되는 것으로 요금 부과 시스템에서의 보다 융통성 있고 효율적인 방법을 제공하게 된다.

2-2 문제점 해결 방안

본 논문에서 WLAN을 통해 AP에 ACCESS 될 수 있는 부분과 DMB 수신 부분 및 휴대폰 부분으로 구성된 유비쿼터스 휴대 단말장치의 CAS 인증에 관한 것이다. WLAN을 통한 AP 접속 부분이 UMA 폰을 구성하는 영역으로 궁극적으로 UNC 서버까지 접속이 되어 IP를 통한 통화를 제공해준다. 그러나 이 영역은 통화의 기능 뿐만 아니라 최대 54Mbps의 속도로 서버에 접속이 가능한 영역으로써 고속의 데이터 전송이 가능하다. 이러한 특징적 기능을 CAS 인증에 적용하는 것이 제안된 시스템의 특징이다. 기존에는 단일 요금제를 통해 저장된 CAS CODE가 인증되는 경우에 DMB 시청이 가능하였다. 그러나 제안된 방법과 같이 UNC 서버에 저장된 인증 CAS CODE를 갖고 와서 DMB를 시청하게 됨으로써 UNC 망 업체는 DMB 부가 서비스를 제공하는 권한을 가질 수 있고 사용자는 DMB 지원 사업자에게 일률적인 요금 체계에서 벗어나 원하는 콘텐츠에 대한 원하는 시간만큼의 방송 시청을 요구하여 보다 저렴하고 체계적인 요금 방법으로 방송을 수신할 수 있는 장점을 갖는다.

이러한 체계적 요금 지불은 WLAN의 고속 데이터 전송 특징과 양방향 통신이므로 가능하다.

2-3 기존 기술과의 차이점

기존의 기술에서는 방송의 단방향 통신으로 인해 CAS 인증을 통한 일률적 요금체계로 진행될 수밖에 없다. 그러나 본 논문에서 제안한 방식으로 단말이 구성된다면 WLAN의 고속 데이터 전송 특징과 양방향성을 이용하여 필요한 콘텐츠에 대한 요금 정산 요청이 가능하며, 사용자는 또한 방송 시청 시간에 따른 유연한 요금 체계 형성이 가능하다. 이러한 요금 정산을 위해서는 UNC 서버를 관리하는 사업자 측에서 방송 서비스를 대처할 수 있는 인프라가 구성되어 있어야 한다.

Ⅲ. 제안하는 UMA 모드를 이용한 DMB의 CAS 인증절차

그림 1은 블록 다이어그램으로써, 디지털 멀티미디어 방송 수신 부분과 IP 통신이 가능한 UMA 기능의 복합형을 나타내고 있다. 그림 1에서 특별히 제시되고 있는 방법은 휴대 이동 통신 단말기에 유무선 통합 솔루션을 제공할 수 있는 UMA 기능으로 종래의 단말기에 저장된 CAS CODE De-scramble 기능을 이용한 방송 수신인가를 하는 방법과 단말기가 AP의 Hotspot에 있는 경우 UMA 망을 이용하여 UNC 서버

에 접속 후 UNC에서 제공되는 CAS CODE De-Scramble을 통해 방송 신호 수신인가를 하고 방송 수신을 할 수 있도록 하는 방법을 나타낸다.

본 논문에서 제안하는 휴대 이동 통신 단말기는 Mobile Phone 장치와 WLAN 장치, 그리고 DMB 모듈을 지원하는 DMB 수신 장치가 장착된 Mobile Phone (①)이 필요하다.

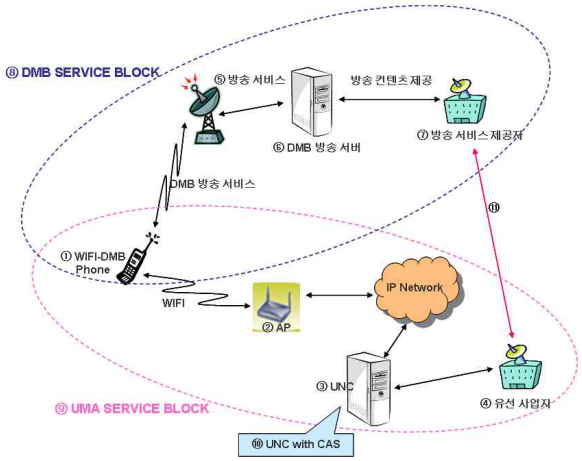

그림 1. UMA 기능의 복합형 블록 다이어그램
Fig. 1. Complex block diagram of UMA function

① : WLAN, DMB가 내장된 GSM Handset
② : GSM Handset과 IP Network과 연결하기 위한 무선접속장치
③ : UMA (Unlicensed Mobile Access)와 GSM간의 Switching을 위한 UMA Network Control System
④ : UNC Server를 관장하는 사업자
⑤ : DMB 방송 서비스를 송수신하기 위한 기지국
⑥ : 방송 서비스 사업자로부터 제공받은 방송 컨텐츠를 제어하는 시스템
⑦ : 방송 서비스 사업자
⑧ : DMB 서비스를 제공 할 수 있는 기본 요소의 모음
⑨ : UMA 서비스를 제공 할 수 있는 기본 요소의 모음
⑩ : CAS (Conditional Access System)은 방송에 가입자 개념을 도입하여 정당한 시청 권한을 가진 가입자만이 특정프로그램을 수신할 수 있게 하는 시스템

그림 1에서는 이와 관련된 내용을 모두 포함 시키고 있다. UMA SERVICE BLOCK (⑨)과 DMB SERVICE BLOCK (⑧)으로 나누어 확인해 본다.

UMA SERVICE BLOCK (① ~ ④)에서 UMA CALL이란 유럽의 몇몇 업체에서 서비스 될 예정인 것으로 UMA망과 GSM망과의 핸드오버가 가능하고 AP(②)가 있는 위치에서는 AP Hotspot에 접속되어 보다 저렴한 통화 요금으로 전화가 가능하며, 뿐만 아니라 고속의 데이터 서비스 또한 받을 수 있는 장점 있는 시스템이다. 기본적으로 양방향 통신이 가능하며, 실시간 데이터 처리가 가능하고 최고 속도 54Mbps까지 지원하다.

DMB SERVICE BLOCK (⑤ ~ ⑦)에서는 방송국(⑤)을 통해 방송 신호를 수신하는 것이지만 요금 처리를 위해서 CAS라는 인증 절차를 갖고 있다. 현재는 기본적으로 단방향 통신만이 가능하기 때문에 단말기 내부에 저장되어 있는 CAS 인증 코드를 이용하여 방송국간의 인증 처리로 방송을 듣고, 보고, 받을 수 있다.

두 개의 시스템이 합쳐지는 유무선 통합 유비쿼터스 시스템에서는 서로의 장점과 단점을 결합하고 가장 이상적인 시스템 구성이 가능하게 되는데 본 논문의 요지는 여기에 있다. DMB SERVICE BLOCK에서 CAS 인증을 단말기에 저장된 HARD CODE를 이용하게 되면 사용자는 방송 수신 시간과 관계없이 일정 기간에 똑같은 요금을 정산하게 된다. 하지만 만약 사용자가 방송 시청 시에만 혹은 원하는 데이터 서비스를 받는 경우에만 요금 정산이 이루어지게 된다면, 사용자는 보다 저렴하게 방송 수신이 가능하며, 사업자(⑦)는 보다 많은 고객을 확보할 수 있게 되는 장점이 있다. 이러한 기능을 위해서 본 논문에서 제시되는 방법은 DMB SERVICE BLOCK에서 필요한 CAS CODE를 UMA SERVICE BLOCK에 있는 UNC 서버(③) 내부의 CAS 코드(⑩)를 이용하는 것이다. 이렇게 함으로 인해 UNC 서버를 관장하는 유선 사업자 업체(④)는 DMB 서비스를 제공하는 권한을 갖게 되고 사용자는 원하는 시간에 원하는 콘텐츠에 한에서만 요금을 지불을 하게 되어 보다 체계적인 요금체제 구축이 가능하며, CAS HARD CODE를 이용할 때와 같이 콘텐츠 이용에 상관없이 일정 금액을 지불하는

폐단을 막을 수 있게 된다.

CAS 코드는 DMB의 실시간 데이터를 De-Scramble에 적용하여 사용되는 코드로 실시간 처리가 가능해야 하지만, 기술적으로 UMA 영역에서의 높은 데이터 처리율로 이러한 문제점 또한 해결이 가능하다.

본 기능이 내재되어 있는 이런 복합형 단말기는 기술적으로 현재 충분히 보급이 가능한 형태의 단말기이다. 하지만 이러한 기능을 추구하기 위한 인프라 구성은 보다 더 많은 진전이 필요하다 특히, UNC 서버를 관장하는 유선 사업자 측과 DMB 방송 사업자 간의 협의(⑪)는 반드시 필요한 것에 해당된다. 협의되어야 할 내용으로는 요금 정산 체계와 CAS CODE 동기 등이 해당된다.

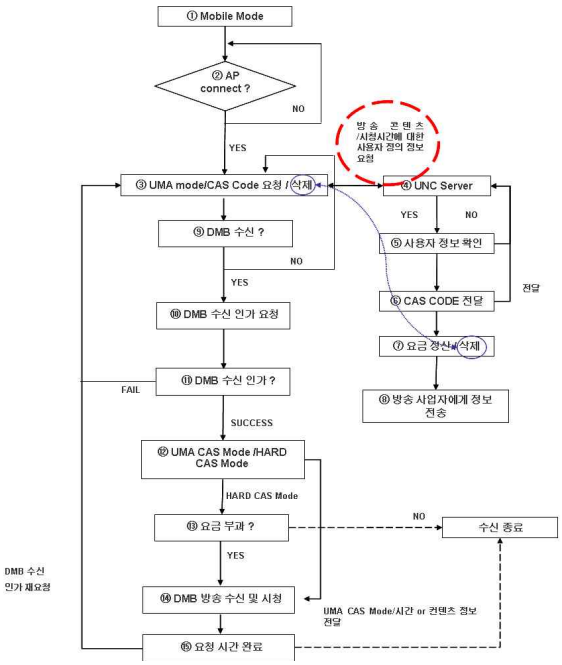

그림 2. UMA 망을 이용한 디지털 멀티미디어 방송 시청에 대한 요금 부과 프로세스 블록도

Fig. 2. DMB using UMA for the service payment process algorithm

그림 2는 UMA 망을 이용한 디지털 멀티미디어 방송 시청에 대한 요금 부과 프로세스 블록도를 모드 전개에 따른 흐름을 나타내고 있다.

초기 Mobile Mode(①)에서는 GSP망에만 붙은 상태로 순수 폰 상태를 유지하면서 AP가 있는지를 주기적으로 체크하면서 AP Connect(②)되면 UMA Mode (③)상태로 변형된다.

UMA Mode 상태란 Handset이 AP의 Hotspot에 있음을 의미하며 방송 서비스를 받기 전에 사용자는 UNC 서버(④)에게 “어떤 콘텐츠를 수신하겠다.” 혹은 “어떤 데이터 서비스를 DMB를 통해서 받겠다.”, “얼마의 시간 동안 방송을 수신하겠다.”라는 방송 콘텐츠/시청시간에 대한 사용자 정의 정보를 CAS CODE 요청(③)시 하게 된다.

이러한 정보를 서버는 확인하며 우선, 어떤 사용자(⑤)인지를 확인한 후 UNC 서버를 통한 CAS CODE선택이 가능한지 확인하고 가능한 경우에 CAS CODE (⑥)를 단말기에게 전달시키게 되며, 이와 동시에 요금을 정산(⑦)시키며, 이에 관한 정보를 방송 사업자에게 정보를 전달(⑧)시키게 된다. 만약, 사용자가 CAS CODE 요청이 불가능한 경우에는 CAS CODE 전달은 이루어지지 못하게 된다.

CAS CODE를 받은 단말기는 DMB 수신(⑨)을 하게 된다. RF 수신 감도가 낮거나 혹은 어떤 특별한 경우로 인해 방송 수신이 되지 못하는 경우에는 CAS CODE 삭제 모드로 돌아가 요금 정산 삭제 요청(③, ⑦)을 하게 된다. DMB 수신 인가 요청이 일정 RF 수신 감도 레벨 이상을 충족하여 수신 인가 요청(⑩)을 받아들이게 되면 단말기는 UNC 서버로 부터 받은 CAS CODE를 통해 다시 DMB 수신인가(⑪)가 정확히 이루어지는지를 확인하게 된다. 만약 단말기와 AP간의 무선 채널 특성으로 인해 잘못된 데이터를 받아 들여져서 수신 인가가 이루어 지지 못하게 된다면 다시 CAS Code 요청 모드로 돌아가 다시 코드를 받아 다음 단계를 진행시키게 되며, 성공 시에는 CAS CODE Mode를 체크(⑫)하게 된다.

만약 단말기가 저장된 HARD CAS CODE를 통해 DMB 수신을 하는 경우에는 CAS CODE 요청으로 CODE를 받아 처리하지 않고 방송 서비스 업체를 통해 요금 부과(⑬)가 이루어지게 되며 UMA CAS Mode인 경우에는 “시간 혹은 어떤 콘텐츠를 이용하겠다.”라는 정보를 갖고 방송 수신 및 시청(⑭)이 이루어지게 된다. 시청 중 콘텐츠가 완료되거나 요청된 시간이 초과하게 되면 방송 수신은 정지(⑮)하게 되며, 사용자의 요청에 따라 DMB 수신 인가 재요청을 하게 된다.

그림 1에서 DMB SERVICE BLOCK(⑧)에 해당되

는 부분은 그림 2에서 (⑨ ~ ⑮)에 해당되는 부분이며, UMA SERVICE BLCOK에 해당되는 부분은 (④ ~ ⑧)에 해당되는 부분이다.

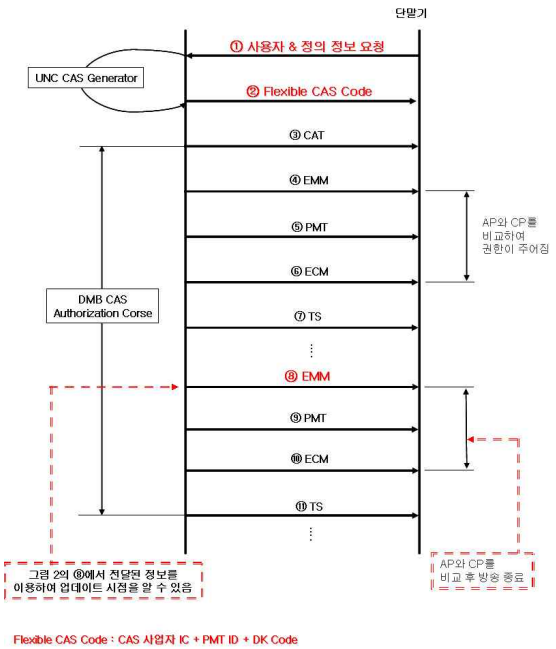

그림 3. UNC 서버를 통해 획득한 Flexible CAS CODE 인증 과정

Fig. 3. The gain of flexible CAS CODE through UNC service

표 1. 전송되는 신호의 구성요소

Table 1. Transmitted signal parameters

CAT	CAS 사업자 ID + EMM Packet ID
EMM	AK (encrypted by DK) + AP
PMT	Channel [audio/video/data]별 Packet ID + ECM Packet ID
ECM	CW (encrypted by AK) + CP
TS	Encrypted by CW

그림 3은 그림 2에서 적색 굵은 파선으로 표시된 부분과 '⑫'부분을 상세하게 표시된 부분으로 CAS 인증 절차 과정이다. 본 논문에서 제시하고 있는 UNC 서버에서 CAS 코드를 송출 받아서 방송 신호를 복원하여 보고 CAS CODE가 완료되는 과정을 확인할 수 있다.

단말기 사용자는 WLAN 연결됨을 확인된 상태에서 CAS 코드를 요청할 수 있게 된다. 요청된 내용 전달(①)은 "어떤 콘텐츠를 수신하겠다." 혹은 "어떤 데이터 서비스를 DMB를 통해서 받겠다.", "얼마의 시간 동안 방송을 수신하겠다."라는 내용이다.

UNC 서버는 우선 사용자 등록을 확인하고 전달된 사용자 요청에 맞는 코드를 생성하기 위해 CAS Generator를 통화시켜 생성된 CAS CODE를 단말기에 전달(②)시킨다. 전달되는 CAS CODE에는 Flexible CAT(Conditional Access Table) ID, PMT(Program Map Table) ID 및 DK(Distribution Key)가 포함되어 있다.

단말기는 CAS CODE가 전달되면 DMB 수신을 위한 모드로 전환되어 청취모드로 동작되면서 처음으로 갖고 있는 Flexible CAT ID와 맞는 CAT 신호를 모니터링하고 맞는 CAT 신호(③)가 들어오게 되면 EMM(Entitlement Management Message) Packet ID를 이 과정에서 획득하게 된다. 이러한 획득과정에 단말기는 다음에 들어오는 자신에게 맞는 EMM 신호를 Searching 할 수 있게 되며, EMM 신호(④)에서 단말기는 처음 UNC 서버에서 전달받은 DK 신호를 이용하여 EMM 신호에서 AK(Authorization Key)를 획득하게 된다. EMM 신호는 표 1에서 볼 수 있듯이 부호화된 AK 신호와 AP(Authorization Parameter) 신호로 구성되어 있는데, 부호화된 AK 신호는 DK 코드로 Decryption을 할 수 있으므로 AK 신호를 얻을 수 있게 되는 것이다. 또한 단말기는 AP 신호를 자신의 메모리 공간 안에 저장하여 DMB 서비스 동안 자신의 DMB 청취 파라미터로서 이용하게 된다. AP 신호는 사용자수신 권한 정보를 포함하고 있는 것으로 어떤 방송과 어떤 서비스를 이용할 수 있는지를 포함하고 있는 것이다.

그 후 단말기는 또다시 PMT 신호(⑤)를 찾게 되며, 이 신호에서 ECM(Entitlement Control Message) Packet ID 정보를 단말기는 획득하게 된다. 이 ID를 이용하여 ECM 신호(⑥)를 찾게 되는데, ECM 신호는 표 1에서 표현되어 있듯이 AK 신호에 의해 부호화된 CW(Control Word)와 CP(Control Parameter)로 구성되어 있는데 단말기는 전 과정에서 얻은 AK를 이용하여 CW신호를 구하게 되며, 차후에 CW신호를 TS(Transport Stream) 신호를 Decryption 하는데 사용하게 된다. 단말기는 사용자 수신 권한 정보 AP와 획득된 CP가 동일하면, TS 신호(⑦)를 받아들일 수 있는 권한이 주어지게 되며, CW에 의해 부호화된 방송

TS 신호는 전 과정에서 구해진 CW로 방송을 청취할 수 있게 되는 것이다.

그림 2의 '⑧'에서 UNC 서버는 방송사업자에게 정보를 전달하기 때문에 방송국에서는 이 정보와 맞는 시점에 EMM 신호 업데이트를 통해 방송 청취를 중단 시킬 수 있는데 이 과정은 '⑧ ~ ⑪'에서 확인할 수 있다.

방송사업자는 사용자의 권한을 해지하기 위해서 전달되는 EMM 신호(⑧)의 AP를 변경하여 보내게 되며, 단말기는 자신의 메모리 공간 내에 저장된 AP 정보를 업데이트하게 된다. 일률적인 과정(⑨ ~ ⑩)이 지난 후 TS 신호를 받기 이전에 AP 정보와 CP 정보를 비교하는 과정에서 AP 정보 업데이트가 이전에 이루어 졌기 때문에 비교과정 차이로 더 이상 이 사용자에게는 방송을 청취할 수 있는 권한이 없어지게 되는 것이다.

모든 과정은 일반적 CAS 인증과정과 동일하지만, 적색으로 표시된 부분은 본 논문에서 새롭게 제안된 과정이다.

Ⅳ. 결 론

기존의 기술은 요금 체계가 획일적이고 다른 매체 즉, 전화통화, 인터넷을 이용하여 DMB를 신청되어야 하기 때문에 콘텐츠별 시청을 하기 위한 접근이 어렵다. 그러나 제안된 시스템에서는 CAS 코드 저장 매체가 휴대전화기내에서 사라지고 콘텐츠별 시청을 위한 접근 방법이 용의하기 때문에 DMB의 시청이 자유로워진다. 또한 요금 체계의 변화로 체계적인 콘텐츠 접근이 가능하며 All-IP망이 형성되는 4G발전 방향에 부합될 것이다.

UMA 모드를 이용한 DMB의 CAS는 과도기적인 통신에 탄생될 수 있는 방법이기도 하다. UMA, DMB/DVB-H 등의 인프라 구축이 되어 있어 본 논문에서 제안된 시스템의 개발 접근이 용이해질 것이다.

참 고 문 헌

[1] 이진환, 이용훈, "지상파DMB 제한수신 기술 및 표준화", *한국방송공학회 학회지*, 11권 3호, pp. 20~30, 2006. 9.

[2] 이용훈 외. "지상파DMB 제한수신 시스템의 효율적인 설계 및 구현 방법", *한국통신학회논문지*, 31권 10A호, pp.1020~1030, 2006. 10.

[3] ETSI TS 102 367, "Digital audio broadcasting (DAB); Conditional access", v.1.2.1, Jan. 2006.

[4] ETSI EN 300 401, "Radio broadcasting systems; Digital audio broadcasting (DAB) to mobile, portable and fixed receivers", v.1.3.3, May 2005.

[5] 김용만, "디지털 방송을 위한 CAS(Conditional Access System) 개발", *대한전자공학회* 학회지, 26권 6호, pp. 72~78, 1999. 6.

오 세 갑 (吳世甲)

1999. 8. : 한국항공대학교 항공통신정보공학과(공학석사)
1999. 8. ~ 2001. 3. : (주)세영통신 전파기술연구소 연구원
2001. 3. ~ 2006. 5. : (주)벨웨이브 통신연구소 책임연구원
2006. 5. ~ 현재 : 대전테크노파크 고주파센터 대리
2007. 3. ~ 현재 : 목원대학교 IT 공학과 박사과정
관심분야 : 무선멀티미디어통신, 무선통신, 이동통신, WAVE, IT기반 융합기술 등

강 희 조 (姜熙照)

1994년 : 한국항공대학교 대학원 항공전자공학과 (공학박사)
1996년 ~ 1997년 : 일본 오사카대학교 공학부 통신공학과 객원교수
1990년 ~ 2003년 : 2월 동신대학교 전자정보통신공학부 교수
2003년 ~ 현 재 : 목원대학교 컴퓨터공학부 교수
관심분야 : 멀티미디어통신, 유비쿼터스, 무선이동통신, 가시광통신, 모바일 컴퓨터, 환경전자공학, RFID, 인지적무선통신, 기술정책