지상파DMB 제한수신 시스템의 효율적인 설계 및 구현 방법

정회원 이 용 훈*, 이 진 환*, 이 광 순*, 이 수 인*, 김 남**

An Effective Method of Design and Implementation for Conditional Access System in Terrestrial-DMB

Yong-hoon Lee*, Jin-hwan Lee*, Gwang-soon Lee* ***Regular Members***,
Soo-in Lee*, Nam Kim** ***Regular Members***

요 약

본격적인 지상파DMB 서비스가 시작되면서 사업자별로 다양한 데이터 서비스를 준비하는 등 비즈니스 모델 개발에 주력하고 있다. 이에 따라 DMB에 적합한 제한수신 시스템의 필요성이 이슈화되면서 국내에서는 현재 표준화 작업이 활발히 진행되고 있다. 본 논문은 지상파DMB 방송환경에서의 적용을 목적으로 하는 지상파DMB 제한수신 서비스를 위한 앙상블 재다중화기와 수신 검증 플랫폼의 설계 및 구현 방법에 관해 제안한다. 또한 제안된 앙상블 재다중화기를 통하여 스크램블링된 앙상블 스트림을 송출하고, 수신검증 플랫폼을 통하여 적용된 스크램블 모드에 따라 디스크램블링 및 디코딩하여 이를 디스플레이함으로써 그 성능을 검증하였다.

Key Words : T-DMB, CAS, Ensemble Re-multiplexer

ABSTRACT

As the Terrestrial DMB(T-DMB) has been launched, service providers are focusing on finding a business model as well as preparing the variety of data services. So, the need for development of the CAS(Conditional Access system) is urgently required and its domestic standardization is also in progress. This Paper proposes design and implementation methods of an Ensemble Re-multiplexer and receiver platform for its verification that can be used for the CAS system in T-DMB. And, with transmitting ensemble stream scrambled by the proposed Ensemble Re-multiplexer, we verified their performance by de-scrambling and decoding according to scramble mode at the receiver platform.

Ⅰ. 서 론

디지털 데이터의 통합 방송에 있어서 송신측과 수신측 사이에 상호 보안성이 확립되지 않을 경우 방송의 상업적 구조가 무너지게 된다. 그리고 방송사업자는 다채널 및 전문 채널의 활성화로 기존 광고 수입에 의존하던 서비스를 탈피하여 가입자에게 양질의 방송 서비스를 제공하고 이들로부터 시청료를 징수하는 pay-TV, pay-per-view 등의 유료 방송 서비스를 제공하고자 하며, 또한 송출된 다양한 멀티미디어 데이터가 보호되어 정당한 수신권한이 있는 인증된 가입자만 수신할 수 있기를 바라는데 이

* 한국전자통신연구원 방송시스템연구그룹 ({lee.y.h, jinhwan, gslee, hyun, silee}@etri.re.kr)
** 충북대학교 전기전자공학부 교수 (namkim@chungbuk.ac.krm)
논문번호 : KICS2006-06-278, 접수일자 : 2005년 06월 20일, 최종논문접수일자 : 2006년 9월 25일

러한 문제를 해결하기 위해 개발된 것이 제한수신 시스템(CAS; Conditional Access System)이다.

국내DMB(Digital Multimedia Broadcasting)가 활성화됨에 따라 사용자들은 점점 더 이동환경에서의 멀티미디어 서비스에 익숙해져 가고 있으며, 비디오 서비스뿐만 아니라 다양한 콘텐츠를 휴대 단말을 이용하여 이동 중에도 서비스를 받고자 하는 요구가 증가하고 있다.

오디오나 비디오의 단순한 디지털화는 물론 다양한 멀티미디어 서비스가 주요한 응용 서비스인 지상파DMB는 각 응용 서비스에 따라서 서브채널, 데이터그룹, MOT라는 다양한 계층으로 제한수신할 수 있게 되어 있다. 따라서, 기존의 DTV보다 지상파DMB에서의 제한수신 규격은 다소 복잡하며, Eureka-147 DAB 제한수신 규격을 만족하는 다중화기나 CAS 장비의 상용화 제품이 아직 출시되고 있지 않은 상황이다. 우리나라에서 세계 최초로 서비스 표준을 정하고 상용화 서비스하고 있는 지상파DMB가 국내외에서 널리 보급되고 활성화되려면 유료화 서비스가 가능하여, 가입자에게는 차별화된 서비스를 제공함과 동시에 방송사업자에게는 수익을 보장할 수 있게 하여야 한다. 이를 위해서는 지상파DMB의 서비스와 기술 특성에 맞는 제한수신 장비가 출시되어야 하는데, 이를 위해서는 이에 맞는 제한수신 규격의 조속한 표준화가 필요하다[1, 2, 6].

현재 국내에서는 지상파DMB 제한수신과 관련하여 정합 표준화가 진행되고 있으며 그 내용들을 간단히 살펴보면 다음과 같다. 국내 지상파DMB 제한수신 규격은 지상파DMB의 근간이 되는 DAB의 제한수신 규격 초안인 draftETSI TS 102 367을 기초로 하여 차세대디지털방송표준 포럼 DMB분과위원회 제한수신 Adhoc그룹 을 통하여 표준(안)이 작성되었고 TTA(한국정보통신기술협회)에 제출되었으며, 제출된 표준 (안)을 토대로 현재 TTA DMB프로젝터그룹 산하 CAS실무반에서 표준화 제정을 진행중이다.[1]

이에 따라 국내에서는 일부 데이터 서비스에 대하여 유료화를 추진 중이며, 빠르면 2006년말 데이터 서비스를 실시할 예정이다. 그러나 현재 지상파DMB의 제한수신을 목적으로 한 헤드엔드 장비가 개발되지 않은 상황이기 때문에 제한수신 표준화와 병행하여 조기에 제한수신 장비를 국산화하지 않으면, 지상파DMB가 국내에서 주도해 나가는 기술임에도 불구하고 외국의 제한수신 업체의 기술에 종속될 우려가 매우 크며, 기존에 개발하거나 개발중인 송수신 시스템의 효용가치가 반감될 수 있다.

따라서 본 논문에서는 표준화가 진행중인 규격의 적용 및 검증을 목적으로 실제 DMB환경에서 제한수신 서비스의 가능 유무와 더불어 효율적인 제한수신 방법을 제안하며, 특히 제안한 방법을 토대로 현재 지상파DMB의 제한수신 서비스를 위해 필수적으로 개발되어야 하는 제한수신 서비스용 앙상블 재다중화기와 수신 검증 플랫폼의 설계 및 구현 방법에 관해 설명한다.

본 논문의 구성은 1장의 서론에 이어 2장에서는 지상파DMB 제한수신 시스템의 개요에 대해 설명하고, 3장에서는 제안하는 지상파DMB 제한수신 송수신 시스템에 대한 세부적인 내용을 언급한다. 또한 4장에서는 실제 설계한 제한수신 서비스용 앙상블 재다중화기와 수신 검증 플랫폼을 활용하여 구현 및 실험 결과를 제시한 후, 5장에서 결론을 맺는다.

Ⅱ. 지상파DMB 제한수신 시스템의 개요

일반적으로 디지털TV에서는 패킷화된 기초스트림 (PES; Packetized Elementary Stream)이나 전송스트림(TS; Transport Stream) 레벨에서 프로그램별로 스크램블링하도록 되어 있으며, 두 가지 레벨 중에서 단지 하나의 레벨만을 이용하여 스크램블링하여야 하며 두 가지 스크램블링 레벨을 섞어서 사용할 수 없도록 되어 있다[10]. 그러나 지상파DMB에서는 여러 프로그램 데이터들이 계층적으로 다중화되어 구성되며 최종적으로는 하나의 앙상블 데이터 형식으로 다중화되어 전송된다. 따라서 지상파DMB에서는 계층적이고 다양한 방식으로 스크램블링하여 제한수신을 적용하는게 필요하다.

지상파DMB에서는 여러 프로그램 데이터들이 계층적으로 다중화되어 구성되며 최종적 으로는 하나의 앙상블 데이터 형식으로 다중화되어 전송된다. 그림 1에서 알 수 있듯이 특정 프로그램에 제한수신을 적용하려면 해당 프로그램의 계층과 특성에 따라서 서브채널 모드, 데이터그룹 모드, 멀티미디어객체전송(MOT; Multimedia Object Transfer) 모드인 세가지 스크램블링 모드 중에서 한 가지 모드를 선택하여 제한수신을 적용할 수 있다.

서브채널 모드는 프로그램 관련 데이터(PAD; Program Associated Data)를 포함한 오디오 서브채널, 패킷모드 데이터 서브채널, DMB 비디오와 같은 스트림모드 데이터 서브채널 중에서 제한수신을

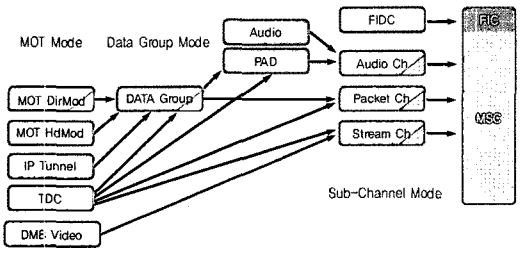


그림 1. 지상파DMB 제한수신 모드별 스크램블링 위치

표 1. 제한수신 모드 별 제한수신 파라미터의 위치

	Sub-channel CA			Data Group CA		MOT CA	
				Packet mode	PAD	Selected MOT Objects are scrambled	All MOT objects of an MOT Data Carousel are scrambled (see note)
CAId	FIG 0/2			FIG 0/2	-	FIG 0/2 / -	FIG 0/2 / -
CASysIdList	FIG 6			FIG 6	FIG 6	FIG 6	FIG 6
CA Indicat on	CAFlag in FIG 0/2			CAFlag in FIG 0/2	CAFlag in FIG 0/13	CAIndi: existence of MOT header parameter CAInfo in MOT directory	CAFlag in FIG0/2 / FIG 0/13
	Packet Ch	Stream Ch	Audio Ch				
CAOrg Indicat on	CAOrgFlag in FIG 0/3	CAOrgIndi: existence of FIG 0/4	CAOrgIndi: existence of FIG 0/4	CAOrgFlag in FIG 0/3	CAOrgFlag in FIG 0/13	CAOrgIndi: existence of MOT header parameter CAInfo in MOT directory	CAOrgFlag in FIG 0/3 / FIG0/13
CAOrg "permitte d CAMode"	FIG 0/3 "Sub-channel CA" or "Proprietary CA"	FIG 0/4 "Sub-channel CA" or "Proprietary CA"	FIG 0/4 "Sub-channel CA" or "Proprietary CA"	FIG 0/3 "Data Group CA" or "Proprietary CA"	FIG 0/13 "Data Group CA" or "Proprietary CA"	MOT header parameter CAInfo in MOT directory "MOT CA" or "Proprietary CA"	FIG 0/3 / FIG0/13 "MOT CA" or "Proprietary CA"
CASyncParam	SUBCAPrefix			DGCAPrefix		MOTCAPrefix	
CAIntMess	SUBCAPrefix			MSC Data Group type 1		MOT body or MSC Data Group type 1	

적용하려는 해당 서브채널 전체를 스크램블링하는 방식이다. 데이터그룹 모드는 IP 터널링, MOT, 투명데이터 채널(TDC; Trans-parent Data Channel) 서비스 등에 사용하는 프로그램 데이터를 주 서비스 채널(MSC; Main Service Channel) 데이터그룹화하여 사용하는 경우에 한 서비스 콤포넌트의 모든 데이터그룹 또는 일부 몇 개의 데이터그룹만을 스크램블링 할 수 있는 방식이다. 또한 MOT 모드의 경우는 헤더모드 MOT가 아닌 디렉토리모드 MOT를 사용하여 전송되는 파일에 대하여 MOT 레벨에서 스크램블링하는 방식이다.

스크램블링되거나 스크램블링되지 않은 프로그램 데이터는 제한수신 동기화 파라미터(CASync Param), 제한수신 내부메시지(CAIntMess)와 같이 MSC로 다중화되어서 전송된다. 또한, 제한수신에 필요한 파라미터인 제한수신 식별자(CAId), 제한수신 시스템 식별자 리스트(CASysIdList), 제한수신 모드(CAMode) 등은 제한수신 모드, 제한수신 시스템 종류, 제한수신 방식 등에 따라서 해당되는 고속 정보 그룹(FIG; Fast Information Group)에 실려서 고속 정보 채널(FIC; Fast Information Channel)로 다중화되어 전송된다.

표 1은 앙상블프레임 내에서 제한수신 모드에 따른 제한수신 파라미터와 제한수신 내부메시지 등의 위치를 나타낸 것이다. 그 내용을 간단히 살펴보면 다음과 같다.

- 제한수신 식별자(CA Identifier, CAId) : 서비스 내에서 적어도 하나의 콤포넌트가 스크램블링 된 경우에는 "111"로 설정하고 그렇지 않은 경우에는 "000"으로 설정한다.
- 제한수신 시스템 식별자 리스트(CA Sys-tem Identifier List, CASysIdList) : 현재 사용되고 있는 제한수신 시스템 식별자(CA System Identifier, CASysId), 단축 제한수신시스템 식별자(Short CA System Identifier, ShortCASysId), 제한수신 시스템 내부 특성(CA System Internal Characteristics, CAIntChar)을 포함하고 있다. CAIntChar는 각 CASysId에 해당되는 제한수신 시스템의 버전, 적용된 알고리즘, 시스템 규정 파라미터, 채널 ID, 길이 정보 등을 실을 수 있다. 각 CAIntChar의 길이는 최대 24바이트이며 그 구성 방법은 표준의 범위가 아니다. 제한수신 시스템의 내부 처리를 위하여 한시적으로 CASysId, ShortCASysId, CAIntChar는 서로 매핑되게 한다.
- 제한수신 지시(CA Indication) : 제한수신 지시는 서비스 콤포넌트별로 제한수신이 적용되었는지의 여부를 단말에서 판단할 수 있도록 한다. 해당 서비스 콤포넌트에서 제한수신플래그(CAFlag)가 "1"로 설정되었거나 제한수신지시자 필드(CA Indicator Field, CAIndi)가 존재하면 제한수신이 적용된 것으로 판정한다.
- 제한수신 구성(CA Organization, CAOrg) : CAOrg는 제한수신이 어떻게 적용되었는지를 가리키기 위하여 제한수신 모드(CAMode)와 공유 스크램블러 플래그(SharedFlag)를 포함한다. 제한수신 모드가 "000"이면 서브채널 모드, "001"이면 데이터그룹 모드, "010"이면 MOT 모드로 제한수신되었음을 가리킨다. 8비트로 구성된 SharedFlag는 해당 비트가 "1"로 설정되어 있으면, CASysIdList 내의 ShortCASysId에서 해당되는 제한수신 시스템을 이용하여 방송데이터를 디스크램블링할 수 있다는 것을 나타낸다. 예를들면, 공유 스크램블러 플래그가 "0001 1010"이라면 ShortCASysId가 "001", "011", "100"에 해당되는 제한수신 시스템들을

사용할 수 있다는 것을 나타낸다.

- 제한수신 동기화 파라미터(CA Synch-ronization Parameter, CASyncParam) : CASyncParam는 제어단어의 변경을 나타내기 위하여 최소한으로 토글 플래그가 사용되어야 하며 프레임 카운터, 초기화 변경자 등의 파라미터가 사용될 수 있다.
- 제한수신 시스템 내부메시지(CA System Internal Message, CAIntMess) : 이 메시지는 사용자의 자격과 암호화 키를 관리하기 위한 정보를 포함하고 있으며, 일반적으로 제한수신 시스템에서 말하는 ECM과 EMM이 이에 해당된다.

제한수신 시스템은 송신측 제한수신 컴포넌트와 수신측 컴포넌트로 나눌 수 있으며 그 구성도는 그림 2와 같이 나타낼 수 있다.

송신측 제한수신 시스템 컴포넌트는 제한수신 메시지 인코더, 제어단어 발생기, 동기화기 그리고 스크램블러로 구성되며, 내용은 아래와 같다.

- 제한수신 메시지 인코더(CA Message Encoder) : 제한수신 메시지 인코더는 사용자의 자격에 관련된 관리메시지(EMM; Entitlement Management Message) 또는 제어단어로 수신측 자격 체크를 활성화시키는 자격 제어메시지(ECM; Entitlement Control Message)를 발생한다. 이 메시지들과 메시지의 형식은 고유해서 제한수신 시스템마다 다르다. 이러한 메시지를 제한수신 내부메시지(CAIntMess; CA System Internal Message)라 부른다. 제한수신 내부메시지는 다중화 데이터의 한 부분이 된다.
- 제어단어 발생기(CW Generator) : 제어단어(CW; Control Word) 발생기는 제어단어를 제공하며, 이렇게 발생된 제어단어는 동기화기를 거쳐 제한수신 메시지 인코더와 스크램블러에 제공된다.
- 동기화기(Synchroniser) : 동기화기는 스크램블링과 제어단어 전달과정을동기화시키는데 필요하며, 이를 위해 제어단어는 동기화기를 거쳐 스크램블러와 제한수신메시지 인코더에 전달된다. 그 외에 제한수신 동기화 파라미터(CASyncParam)를 발생시켜 수신측으로 하여금 메시지를 디코딩하고 콘텐츠를 디스크램블링하는 과정을 동기화시킨다. 그리고 제한수신 동기화 파라미터도 다중화 데이터의 일부가 된다.

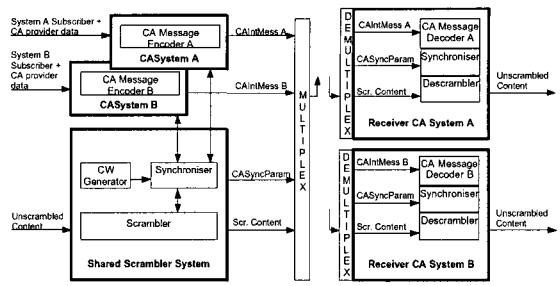


그림 2. 지상파DMB 제한수신 시스템의 개념도

- 스크램블러(Scrambler) : 스크램블러는 제공되는 제어단어로 컨텐츠를 스크램블링한다. 스크램블된 컨텐츠는 다중화 데이터의 한 부분이 된다.

수신측 제한수신 시스템 컴포넌트는 제한수신메시지 디코더, 동기화기 그리고 디스크램블러로 구성되며, 송신측에서 인코딩된 제한수신 메시지를 디코딩하고 스크램블링된 데이터를 디스크램블링한다[1].

Ⅲ. 제안하는 지상파DMB 제한수신 송수신 시스템

3.1. 제안하는 지상파DMB 제한수신 송신 시스템의 구성

현재 디지털 TV에서 사용되고 있는 제한수신 시스템은 TS에 실려 전송되는 여러가지의 서비스 중에서 일부의 수신 권한이 있는 가입자만이 제한적으로 수신할 수 있게 하는 시스템이다. 또한 기존의 디지털 TV 시스템에서는 제한수신 관련 메시지가 TS 패킷에 다중화되는 메커니즘은 MPEG-2 시스템을 사용하며, 제한수신 시스템으로부터 생성되는 메시지에 대하여 Table ID 값에 대한 정의를 추가하고 수신 모듈에서 다수의 제한수신 시스템을 구별하기 위해서 CA_descriptor를 정의하여 사용한다.[6]

그러나 이동 환경인 지상파DMB의 경우에서는 앞절의 설명에서 알 수 있듯이 기존의 디지털 TV에서와는 달리 서비스의 다중화 및 전송 메커니즘의 차이가 있으므로, 기존의 디지털TV에서의 제한수신 방식을 적용하기에는 문제가 있다. 즉, 일반적으로 DMB 비디오 서비스만을 제한수신 한다면 기존의 디지털 TV에서 사용한 방식을 사용해도 문제가 없겠지만, 오디오 및 다양한 데이터 서비스에 대해 각 레벨에 따른 단계적인 제한수신을 할 경우에는 큰 제약이 따른다. 이를 해소하기 위해 앞절의 설명과 같이 크게 3가지의 단계적인 레벨에 따른

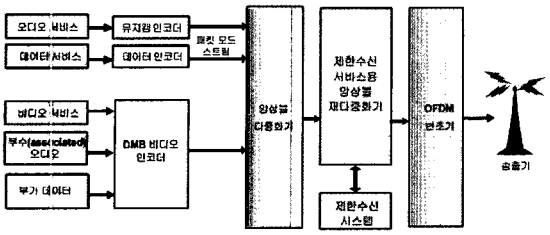


그림 3. 지상파DMB 제한수신 송신시스템 블록도

모드로 나누어서 제한수신을 적용하게끔 한 것이다.

일반적으로 스크램블러가 앙상블 다중화기 앞단에서 동작하는 경우 각 서비스 장치에 스크램블러를 설치하여야 하고, 또한 각각의 서비스에 따른 제한수신과 관련된 정보 및 동기정보를 각각 제어해야 하는 단점이 발생한다.

따라서 이러한 문제점을 해결하고, 모드에 따른 제한수신을 효과적으로 적용하기 위해서는 다중화된 서비스를 통합적으로 관리하여 제한수신을 적용하는 것이 필요하며, 본 논문에서는 그림 3과 같은 지상파DMB 제한수신 송신시스템을 제안한다.

그림 3에서 제안하는 제한수신 송신시스템은 기존 지상파DMB 시스템의 앙상블 다중화기 다음단에 제한수신 시스템과 연동되는 제한수신 앙상블 재다중화기를 포함한다. 여기서 제한수신 앙상블 재다중화기는 제한수신 모드가 결정되면 그 모드에 따라 스크램블링을 할 수 있도록 하는 기능이 포함되어 있다. 또한 제안하는 시스템은 제한수신 서비스용 앙상블 재다중화기가 제한수신 시스템과 연동하도록 함으로써 현재 입력되는 앙상블 정보를 분석하여 하나의 스크램블러를 통해 선택적으로 제한수신을 적용할 수 있다.

3.2. 제한수신 서비스용 앙상블 재다중화기의 설계 및 동작

제한수신 서비스용 앙상블 재다중화기는 스크램블되지 않은 서비스 스트림(앙상블 Ensemble)을 입력받아 선택된 서비스를 스크램블하기 위하여 제한수신 시스템과 연동하면서 새로운 앙상블 스트림으로 다중화하기 위해 필요한 장치이다. 따라서 본 논문에서 제안하는 제한수신 서비스용 앙상블 다중기의 구조는 그림 4와 같으며, 그 동작은 다음과 같다.

ETI(Ensemble Transport Interface) 입력부는 하드웨어적 인터페이스를 통해 스트림을 받아들이는 역할을 수행한다. 스크램블되지 않은 앙상블 스트림을 입력받으며, 입력받은 스트림을 다중화하기 위하여 입력단의 버퍼에 6144 바이트(1 프레임) 단위로 버퍼링을 하여 ETI 프레임의 계층 구조를 알아낸다. ETI 프레임 분석부에서는 저장된 ETI 스트림을 분석한 후 FIC, MSC를 파싱하여, FIG 분석부와 MSC 분석부로 전달하는 역할을 한다. ETI 프레임 분석부에서 분석된 각 필드별 데이터들은 프레임 단위로 버퍼에 저장되어 다중화시에 ETI 프레임을 구성하는데 필요한 데이터로 사용된다.

FIC 분석부에서는 다중화에 필요한 정보를 얻어내기 위하여 FIC의 각 필드들을 분석한다. ETI 프레임 분석부에서 FIC 및 MSC로 분리된 데이터에서 FIC 부분만을 분석하여 ETI 프레임의 계층적 구조를 파악한 후 파악된 앙상블 정보를 GUI (Graphical User Interface) 입력부에 넘겨준다. 이 정보는 GUI 환경에서 스크램블링 모드를 설정하기 위해 활용되며, 설정된 스크램블링 모드에 따라 FIG 생성부에서는 FIC 분석부에서 분석되어진 정보를 입력받아 FIG에서 제한수신과 관련 있는 FIG 0/2, FIG 0/3, FIG 0/4, FIG 0/13, FIG 6과 같은 FIG들을 편집 하거나 생성한다.

한편 MSC 분석부는 각각의 MSC 데이터를 서브채널 별로 나누어 처리한다. 만일 스트림모드일 경우 MSC 데이터를 각각의 채널별로 데이터를 나누는 역할 만을 수행하며, MSC 데이터가 패킷모드인 경우 MOT 계층에서 스크램블링하기 위해서 패킷, 데이터그룹, MOT 순으로 분석을 실시하여 분석된 계층 구조를 GUI에 표시하기 위해 GUI 입력부로 데이터를 보내게 되고, 스트림모드와 마찬가지로 채널별로 데이터를 분리한다. 이렇게 분리된 채

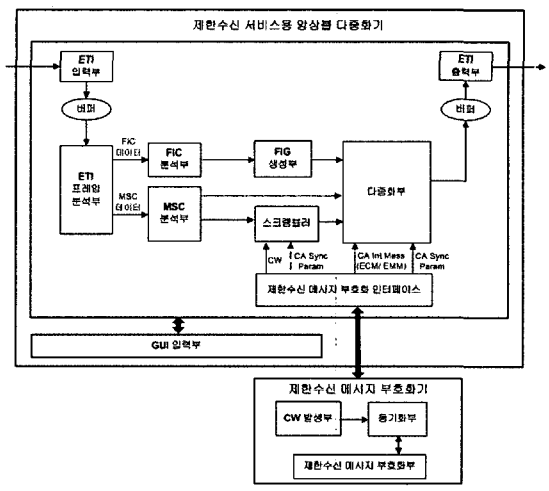


그림 4. 지상파DMB 제한수신용 앙상블 재다중화기 구조

널별 데이터는 선택된 제한수신 모드에 따라 스크램블러에서 스크램블링한다. 즉, 스크램블러를 통하여 스크램블링되지 않은 각 모드의 데이터를 입력받아 제한수신 시스템에서 받은 제어단어에 의하여 스크램블링을 실시하게 되며, 스크램블링시에 상호 동기는 CASyncParam에 의하여 맞추어 준다.

마지막으로 FIG 생성부, 스크램블러, MSC 분석부를 통해서 출력되는 모든 데이터는 다중화부에서 다중화된 후, ETI 출력부를 통하여 OFDM 변조기 및 송출장치를 통해 송출된다. 다중화부에서는 FIG 생성부에서 생성된 FIG, 스크램블러에서 스크램블링된 데이터, MSC 분석부에서 각 서브채널로 나뉘어진 스크램블링되지 않은 데이터 및 제한수신 시스템에서 생성된 CAIntMess가 다중화된다. 일반적으로 사용자의 자격과 전송키에 관한 관리 정보인 자격제어메시지(ECM; Entitlement Control Message), 자격관리메시지(EMM; Entitlement Management Message)등을 포함하고 있는 CAIntMess는 각각의 제한수신 모드에 따라서 삽입되는 위치가 변하게 되는데, 그 예를 살펴보면 다음과 같다.

i) 서브채널 모드일 경우 CAIntMess가 MSC 프레임 내에 삽입된다. 또한 삽입되는 형식은 그림 3에서와 같이 SUBCAPrefix에 Prefix의 Header와 CAIntMess의 형태로 삽입되는데, SUBCAPrefix와 스크램블된 프레임의 합은 8kbit/sec의 배수이어야 한다.

ii) 데이터그룹 모드일 경우에는 Session Header와 MCS Data Group data 필드를 스크램블링한다. 이때는 그림 6에서와 같이 데이터그룹타입 '1'에 CAIntMess가 수반된다.

iii) 마지막으로 MOT 모드에서는 CAIntMess가 3가지 중 한군데 삽입되게 된다. 콘텐츠와 무관한 CAIntMess일 경우에는 데이터그룹타입 '1'에 수반된다. 또한, 한 개 이상의 MOT Body를 참조하게 되면 해당하는 MOT의 Body 부분에 전송되며, 단지 한 개의 Body를 참조하게 되면 MOT CAPrefix의 형태로 CAIntMess가 전송된다[1].

또한, 제한수신 시스템과 제한수신 서비스용 앙상블 재다중화기 사이에 주고 받는 제한수신 메시지는 제한수신 데이터 인터페이스부에서 처리한다. 이는 제한수신 시스템에서 보낸 요청, 응답 메시지에 대한 처리 등이 해당한다. 메시지의 내용은 제한

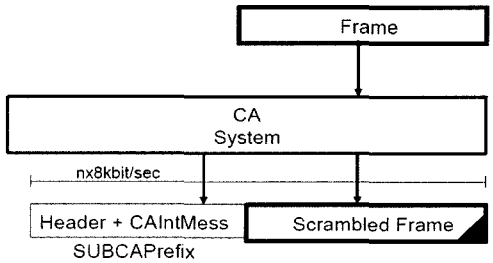


그림 5. 서브채널 모드에서의 콘텐츠와 CAIntMess의 전송

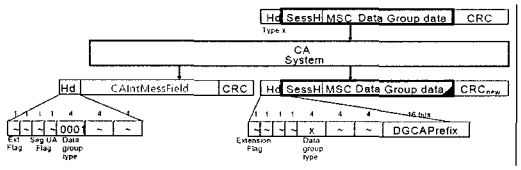


그림 6. 데이터그룹 모드에서의 콘텐츠와 CAIntMess의 전송

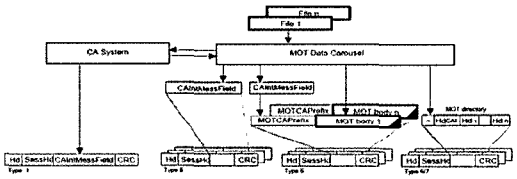


그림 7. MOT 모드에서의 콘텐츠와 CAIntMess의 전송

수신 메시지 부호화기와의 세션에 관련된 정보, 제한수신 파라미터에 관련된 CW, CA SyncParam, CAIntMess와 같은 정보를 상호 약속된 규약에 의하여 정의된 프로토콜에 의하여 통신을 하며, 그 내용에 관해서는 다음절에서 자세히 설명하겠다.

그림 8은 상기에서 설명하였던 제한수신용 앙상블 재다중화기에서 각 블록들 간의 신호 흐름을 전체적으로 나타낸 것이다.

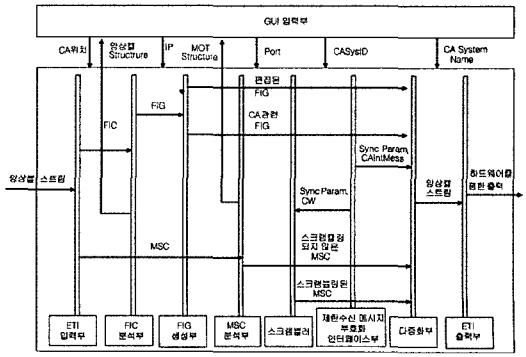


그림 8. 제한수신용 앙상블 재다중화기의 블록별 데이터 흐름도

3.3. 제한수신 데이터 인터페이스

본 논문에서 제안하는 지상파DMB 제한수신 시스템과 제한수신용 앙상블 재다중화기(EI/MUX/SCR)간의 인터페이스 구조는 다음과 같다.

물리계층에서의 물리적/전기적 특징은 IEEE 802.3/802.3u를 따르고 있다. 또한 제한수신용 앙상블 재다중화기는 그 기능에 따라 EI(Ensemble Information), MUX(Multiplexer) 및 SCR(Scrambler)로 나누어서 제한수신 시스템과 연동하여 통신한다. 일반적으로 MUX와 SCR은 그림 4의 다중화부와 스크램블러가 제한수신과 관련된 모든 데이터를 서로 통신할 수 있게 하는 기능을 수행하는 모듈을 말하며, EI는 제한수신용 앙상블 다중화기의 GUI 입력부로부터 스크램블할 앙상블에 대한 사용자의 요구사항을 입력받아 스크램블할 데이터를 제한수신 시스템에 전달하는 기능을 하는 모듈이다.

제한수신 시스템은 다중 연결이 가능한 TCP 서버로 구동된다. 제한수신용 앙상블 재다중화기의 각 모듈(EI/MUX/SCR)은 TCP 클라이언트가 되어야 하며, 각 모듈과 제한수신 시스템은 1개의 TCP 컨넥션을 열고 하나의 컨넥션은 다수의 로직 채널을 갖는다. 또한 로직 채널은 하나의 Service ID에 일대일 매칭된다.

제한수신 시스템과 제한수신용 앙상블 재다중화기간 주고받는 메시지는 응용 계층에서의 메시지로서, EI/MUX/SCR 모듈에 해당되는 제한수신 관련 메시지(CW, CA SyncParam, CAIntMess)와 제어명령에 관한 메시지를 포함하고 있으며 메시지 포맷은 그림 9와 같으며, 이의 정의는 표 2와 같다.

그림 10은 제한수신 시스템과 제한수신용 앙상블 재다중화기간의 제한수신 메시지의 흐름을 순차적으로 나타낸 것이며 그 절차는 다음과 같다.

먼저 제한수신용 앙상블 재다중화기가 EI, MUX, SCR에 대해 특정 Service ID에 대한 로직 채널을 열어(Open) 달라고 요구메시지(EI_OPEN_REQ, MUX_OPEN_ REQ, SCR_OPEN_ REQ)를 제한수신 시스템에 요청하면 제한수신 시스템은 요청받은 Service ID에 대한 로직 채널을 열고 이에 대한 응답메시지(EI_OPEN_RES, MUX_OPEN_RES, SCR_OPEN_RES)를 제한수신용 앙상블 재다중화기에 보낸다. 그러면, 제한수신용 앙상블 재다중화기에서는 제한수신 시스템에게 스크램블할 서비스의 ID를 리스트 형식으로 EI_UPDATE_REQ 메시지에 실어서 보내주면 제한수신 시스템은 응답 메시지로 EI_UPDATE_RES 메시지를 제한수신용 앙상블 재다중화기에 보낸다.

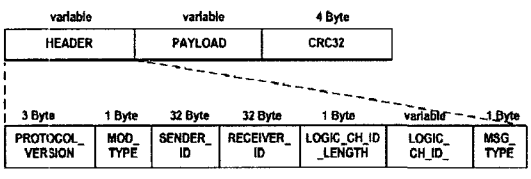


그림 9. 제한수신 메시지 포맷

표 2. 제한수신 메시지 정의

항목	크기(byte)	설명
PROTOCOL_VERSION	3	프로토콜 버전(1.0)
MOD_TYPE	1	모듈의 타입 0x00 : EI 0x01 : MUX 0x02 : SCR 0x03 ~ 0x10 Reserved
SENDER_ID	32	송신 장치 ID
RECEIVER_ID	32	수신 장치 ID
LOGIC_CH_ID_LENGTH	1	로직 채널 아이디(LOGIC_CH _ID)의 데이터 길이
LOGIC_CH_ID	Variable	로직 채널 아이디
MSG_TYPE	1	메시지 타입을 나타냄(각MOD_TYPE에 따라 달라짐)
PAYLOAD	Variable	전송 데이터
CRC	4	CRC32, 다항식

제한수신 시스템에서 CW를 생성한 후 SCR_CW_REQ 메시지를 통하여 제한수신용 앙상블 재다중화기에게 보내면, 제한수신 시스템에서는 ECM을 생성하여 MUX_INT_MESS_REQ 메시지를 통하여 제한수신용 앙상블 재다중화기에 보낸다. 제한수신 시스템이 제한수신용 앙상블 재다중화기에게 SYNC Parameter를 생성하여 MUX_SYNC_PARAM_REQ 메시지를 통하여 보낸다.

마지막으로 제한수신 파라미터에 관련된 CW, CA SyncParam, CAIntMess와 같은 정보를 모두 처리한 후, 로직 채널을 닫는 작업을 실시한다. 즉 제한수신용 앙상블 재다중화기가 EI, MUX, SCR 메시지에 대해 특정 Service ID에 대한 로직 채널의 닫기(Close)를 요청하면 제한수신 시스템은 요청받은 Service ID에 대한 로직 채널을 닫고 응답메시지로서 EI_CLOSE_RES, MUX_CLOSE_RES, SCR_CLOSE_RES 메시지를 제한수신용 앙상블 재다중화기에게 보내게 되면 한 싸이클의 동작이 완료된다.

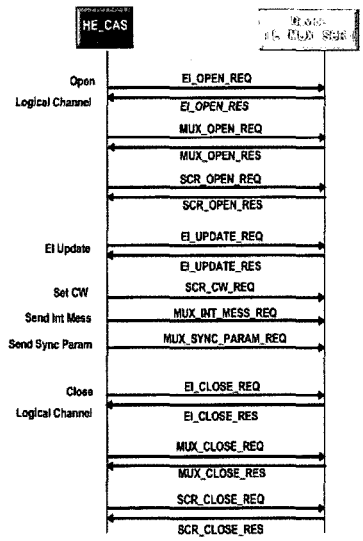


그림 10. 제한수신 시스템과 제한수신용 앙상블 재다중화기 간 메시지 흐름도

3.4. 제한수신 서비스용 수신 검증 플랫폼의 설계 및 동작

그림 11은 본 논문에서 제안하는 지상파DMB 제한수신 서비스용 수신 검증 플랫폼의 구조를 나타낸 것이며, 그 동작을 살펴 보면 다음과 같다.

DMB 수신 신호 처리기는 USB 인터페이스로 지상파DMB 제한수신 데이터 재생기와 접속 되며 수신된 데이터를 USB 인터페이스를 통해서 전송한다. 이 때 DMB 수신 신호처리기는 동기화를 위하여 수신되는 신호를 ETI 프레임 단위로 처리한다. 이렇게 처리된 ETI 데이터는 ETI 프레임 역다중화부에서 ETI 데이터를 프레임 단위로 버퍼에 저장하여 분석한 후 FIC 데이터, 서브 채널 MSC 데이터 및 동기화 파라미터와 제한수신 내부메시지를 파싱하여 FIG 분석부와 MSC 분석부 및 제한수신 메시지 복호화부에 전달한다.

한편, FIC 분석부에서는 입력되는 FIB(Fast Information Block)를 분석하여 채널에 관한 정보 및 설정된 스크램블링 모드 등을 분석하며, 분석된 FIG(Fast Information Group) 정보는 시스템 제어부를 통해 GUI 입력부와 연동하여 그 정보를 표시할 수 있게 한다.

MSC 분석부는 서브 채널별로 나눠 입력되는 MSC 데이터를 입력받아 데이터그룹 및 MOT 레벨로의 계층적인 분석을 실시한다. 제한수신이 적용된 경우 디스크램블러에서 제한수신 메시지 복호화기에서 받은 제어단어에 의하여 디스크램블링을 실시한

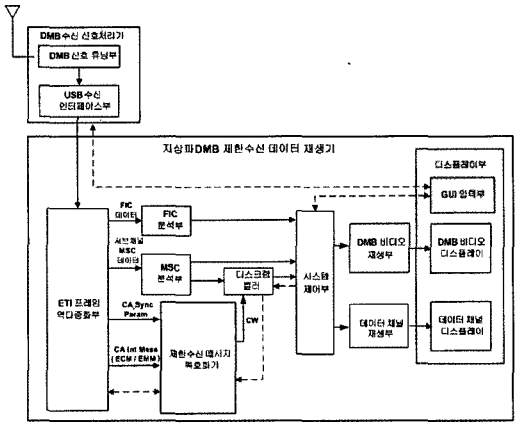


그림 11. 지상파DMB 제한수신 서비스용 수신 검증 플랫폼의 구조

다. 또한 디스크램블링은 시스템 제어부에서 컨트롤 신호에 의해 동작된다.

각 서비스별로 서비스를 재생하기 위한 응용 프로그램이 다르므로 시스템 제어부에서는 GUI 입력부에서 선택한 서비스를 타입별로 디스크램블링할 수 있도록 컨트롤하고, 디스크램블링된 서비스에 해당하는 데이터를 적당한 응용 프로그램과 연결해 주는 역할을 한다

한편, 제한수신 메시지 복호화기는 제한수신 파라미터에 관련된 CA SyncParam, CAIntMess 정보를 ETI 프레임 역다중화기로부터 입력받아 동기화를 고려하여 암호화된 CW를 추출하며, 추출된 CW는 디스크램블러의 요청이 있을 경우 디스크램블러로 보내는 역할을 수행한다.

그림 12는 서브채널 모드일 경우 DMB 스트림을 디스크램블링하는 과정을 나타낸 알고리즘 순서도이다.

그림 5의 전송 구조에서 SUBCAPrefix 데이터를 가져와 헤더 정보인 PrefixHeader를 분석하면 FF(First flag), LF(Last flag), CI(Continuity index), CWT(Control Word toggle) 등과 같은 패킷 식별자 및 위치에 대한 정보를 알 수 있다. FF와 LF의 경우 파라미터 설정에 따라 연속되는 패킷에서 특정한 패킷을 확인하는데 사용되며, CI는같은 패킷 식별자를 갖는 패킷에 대해 0~3까지 연속적으로 1씩 증가하는 카운터로 패킷의 손실을 식별하게 한다. 또한 CWT는 현재 사용된 제어 단어의 상태를 나타낸다. 따라서 이것의 토글링은 제어단어의 변화를 나타내므로 CA 동기화 파라미터 신호에 해당된다.

이러한 내용들을 바탕으로 서브채널 모드의 디스크램블링 과정을 살펴보면 다음과 같다. MSC에 해당하는 SUBCAPrefix 데이터를 가져와 Prefix-

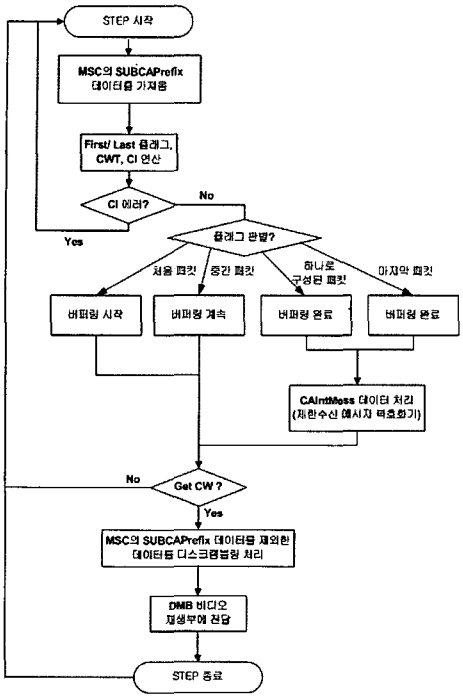


그림 12. 서브채널 모드의 디스크램블링 알고리즘 순서도

Header내의 해당되는 FF, LF, CWT, CI를 연산하고, CI의 에러가 없는 경우 FF와 LF를 분석하여 현재 패킷의 상태를 확인한 후 처리하는 과정을 거친다. 예를들어 SUBCAPrepix의 필드의 패킷의 길이가 24 바이트인 경우 프레임의 패킷 길이가 24 바이트를 초과할 경우 버퍼링을 하여 처리하게 된다. 버퍼링이 완료되면 CAIntMess 데이터를 제한수신 메시지 복호화기를 통해 복호화 처리를 한다. 또한 복호화 처리 과정에서 CW 데이터를 추출하고, 추출된 CW를 이용하여 스크램블링된 프레임 데이터를 디스크램블링하여 DMB 비디오 재생부에서 디코딩 처리된다[1].

Ⅳ. 구현 및 실험 결과

구현된 제한수신 서비스용 앙상블 재다중화기는 앙상블 다중화기에서 생성된 앙상블 스트림을 입력받아, 제한수신을 필요로 하는 서비스의 다중화 작업을 하기 위한 장치이다. 개발한 제한수신 서비스용 앙상블 재다중화기는 PC기반의 소프트웨어 형태로 구현하였으며, OS의 경우 윈도우 XP에 최적화되어 있다. 또한 이 장치는 앙상블 스트림의 입출력을 위해 ETI 인터페이스 카드를 PCI 타입으로 슬롯에 장착하여 사용하고 있으며, 제한수신 메시지

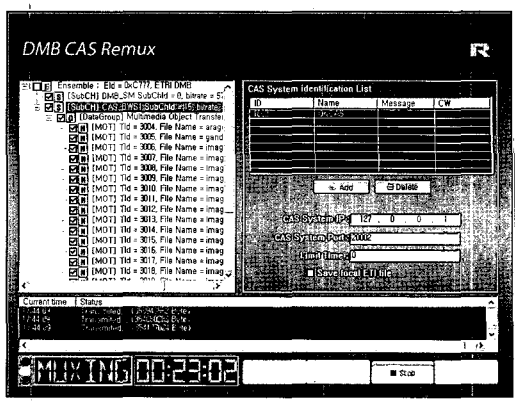


그림 13. 지상파DMB 제한수신 서비스용 앙상블 재다중화기의 GUI

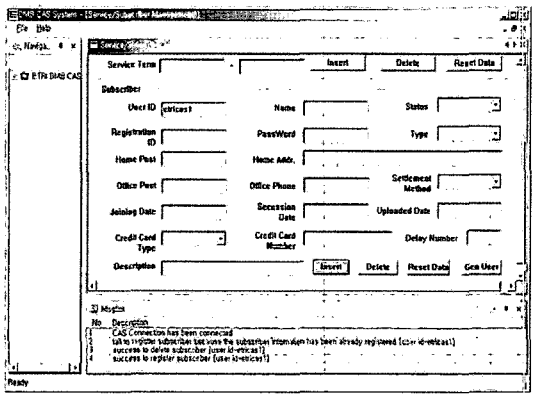


그림 14. 지상파DMB 가입자 관리 시스템 GUI

부호화기와의 인터페이스를 위해 TCP/IP를 사용하였다. 그림 14는 지상파DMB 제한수신 서비스용 앙상블 재다중화기의 GUI를 나타낸 것이다. 구현한 GUI를 통하여 제안한 지상파DMB 제한수신 서비스용 앙상블 다중화기의 전반적인 기능을 제어한다. 특히, 주요 기능으로는 3가지의 제한수신 모드에 대해 앙상블 트리에서 선택적으로 스크램블링하여 다중화할 수 있도록 하는 것을 특징으로 한다.

그림 14는 지상파DMB 가입자관리 시스템의 GUI를 나타낸 것이다. 지상파DMB 제한수신 시스템 GUI를 통하여단말의 인증, 가입자 및 서비스 등록에 대한의 절차가 이뤄지며, 앙상블 다중화기와 연동하여 가입자 및 서비스 관리에 대한 모든 절차를 제어한다.

또한 구현된 제한수신 서비스용 수신 검증 플랫폼은 수신기와 노트북 단말로 구성되어 있으며, 수신기와 노트북 단말은 USB 인터페이스를 사용하고 있다. 또한 제한수신 메시지 복호화기는 노트북 단말내에서 TCP/IP 인터페이스를 사용하여 통신하도

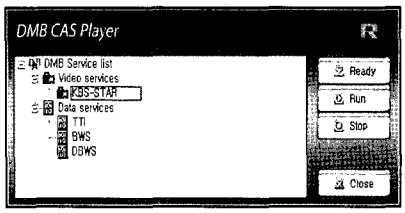


그림 15. DMB CAS 플레이어 GUI

록 구현하였다.

아래의 그림 15는 지상파DMB 제한수신 검증 플랫폼 플레이어의 GUI를 나타낸 것이다.

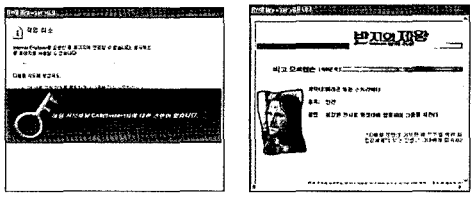
설정된 채널내의 앙상블의 구조를 서비스 트리 형태로 나타내며, 3가지의 제한수신 모드에 대해 앙상블의 서비스 트리에서 선택적으로 디스크램블링하여 선택된 서비스를 재생할 수 있게 하는 것을 특징으로 한다.

그림 16은 제한수신 서비스용 수신 검증 플랫폼을 통하여 서브채널 모드에서의 DMB 비디오 서비스를 디코딩하여 재생한 결과를 나타낸 것이며, 그림 17은 제한수신 서비스용 수신 검증 플랫폼을 통한 MOT 모드에서의 BWS(Broadcasting Website) 서비스를 디코딩하여 재생한 결과를 나타낸 것이다.

두 그림에서 알 수 있듯이 인증된 키를 이용하여 각 각의 서비스를 디스크램블링한 경우에는 정상적으로 디코딩되어 재생되는 것을 확인할 수 있으나,

(a) (b)

그림 16. 서브채널 모드에서의 DMB 비디오 서비스의 수신 화면 비교 : (a) 수신 권한이 없어 정상적으로 수신되지 않은 경우 (b) 수신 권한이 있어 인증된 키를 이용하여 정상적으로 수신한 경우



(a) (b)

그림 17. MOT 모드에서의 BWS 서비스의 수신 화면 비교 : (a) 수신 권한이 없어 정상적으로 수신 되지 않은 경우 (b) 수신 권한이 있어 인증된 키를 이용하여 정상적으로 수신한 경우

정상적으로 인증되지 않은 키를 이용하여 디코딩한 경우 서비스가 정상적으로 재생되지 않는 것을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 현재 국내에서 표준화 작업중인 지상파DMB 제한수신 규격을 토대로 효율적인 지상파DMB 제한수신 서비스를 위한 다중화 및 수신 검증 방법을 제시하였다. 특히 지상파DMB에서 제한수신을 필요로 하는 서비스의 다중화를 위해 지상파DMB 제한수신용 앙상블 재다중화기의 설계 방법을 제시하였고, 이와 더불어 수신 검증 플랫폼의 구현을 통해 그 성능을 검증하였다. 따라서 본 논문에서 제시된 방법을 통하여 국내 지상파DMB에 적합한 제한수신 방안을 결정하는데 필요한 검증 방법이 될 것이라 전망한다.

또한, 본 논문에서 사용된 방법을 응용하여 차후, 현재 사용되고 있는 3가지로 국한되어 있는 제한수신 모드외에 DMB 비디오 서비스에 포함되는 BIFS(Binary Format for Scene) 등과 같은 데이터 서비스에 대한 제한수신 방법에 대해서도 연구가 필요하다. 뿐만 아니라, 가입자수와 서비스의 이벤트가 늘어날 경우 증가되는 제한수신 내부 메시지의 데이터량을 대처하기 위한 효율적인 제한수신 알고리즘 개발 및 OOB(Out Of Band)를 통한 제한수신 데이터 전송 방법에 대한 연구가 추가적으로 필요하다.

참 고 문 헌

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

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

[3] ETSI ETS 300 174, "Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34-45 Mbps", Nov. 1992.

[4] ETSI ETS 300 799, "Digital audio broadcasting (DAB); Distribution interfaces; Ensemble transport interface (ETI)", Sept. 1997.

[5] 은성경, 김신효, 조현숙, "방송환경에서의 일반적

인 제한수신 구조," 방송공학회지, 제2권, 제1호, pp. 73-81, 1997년 3월
[6] 정준영, 구한승, 권은정, 권오형 "제한수신 기술 및 표준화 동향 분석," ITFIND 주간기술동향, 통권 1214호, pp. 1-14, 2005년 9월
[7] 배성수, 한종수, 김철묵, 최규태 "Digital Multimedia Broadcasting DMB 기술과 시스템", 세화, 2005년 6월
[8] ETSI TS 100 756, "Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34-45 Mbps", Nov. 1992.
[9] ATSC Standard A/70, Conditional Access System for Terrestrial Broadcast and Amendment No.1, http://www.atsc.org, 1999.
[10] ETR289, Digital Video Broadcasting (DVB):Support for use of scrambling and Conditional Access(CA) Within digital broadcast system, Oct., 1996
[11] Jean-Luc Giachetti, Vincent Lenoir, Andre Codet, David Cutts, John Sager "A COMMON CODITIONAL ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS", IEEE Transacions on Consumer Electronics, Vol 41, No 3, Aug. 1995.
[12] P.L. Clayson, N. S Dallard "SYSTEM ISSUES IN THE IMPLEMENTATION OF DVB SIMULCRYPT CONDITIONAL ACCESS", IEE International Broadcasing Convention, Conference Publication, No 447, Sept. 1997.

이 용 훈 (Yong-hoon Lee) 정회원

2005년 2월 한밭대학교 전자 공학과 학사
2005년 3월~현재 충북대학교 대학원 정보통신공학과 석사과정
2001년~현재 한국전자통연구원 디지털방송연구단 방송시스템 연구그룹
<관심분야> DMB, DTV 시스템, 영상신호처리

이 진 환 (Jin-hwan Lee) 정회원

1987년 2월 한국항공대학교 통신공학과 학사
2002년 2월 한국정보통신대학 통신공학과 석사
1989년~현재 한국전자통연구원 디지털방송연구단 선임연구원
<관심분야> DMB, DTV 시스템, 영상처리

이 광 순 (Gwang-soon Lee) 정회원

1993년 2월 경북대학교 전자공학과 학사
1995년 2월 경북대학교 전자공학과 석사
2004년 2월 경북대학교 전자공학과 박사
2001년~현재 한국전자통연구원 디지털방송연구단 선임연구원
<관심분야> DMB, DTV 시스템, 영상신호처리

이 수 인 (Soo-in Lee) 정회원

1987년 2월 경북대학교 전자공학과 학사
1989년 2월 경북대학교 대학원 전자공학과 석사
1996년 2월 경북대학교 대학원 전자공학과 박사
1990년~현재 한국전자통연구원 디지털방송연구단 방송시스템연구그룹장
<관심분야> DMB, DTV, CATV, 3DTV

김 남 (Nam Kim) 정회원

1981년 2월 연세대학교 전자공학과 공학사
1983년 2월 연세대학교 전자공학과 공학석사
1988년 8월 연세대학교 전자공학과 공학박사
1992년 8월~1993년 8월 미 Stanford 대학 방문교수
2000년 3월~2001년 2월 미 California Tech- nology Institute(Caltech) 방문교수
1989년~현재 충북대학교 전기전자공학부 교수, 컴퓨터 정보통신 연구소
<관심분야> 이동통신 및 전파전파, 마이크로파 전송선로 해석, EMI/EMC 및 전자파 인체보호 규격