# 지상파 이동 멀티미디어 방송용 제한 수신 시스템 분석

## Analysis of Conditional Access System(CAS) for Terrestrial Digital Multimedia Broadcasting(T-DMB)

정근일, 최성종
Geun il Jung, Seong jong Choi

Abstract - 본 논문에서는 현재 무료로 본 방송이 진행 중인 T-DMB 제한 수신을 위한 시스템 분석에 대해 기술하였다. T-DMB 방송사업자들은 별도의 수신료를 징수하지 않고 광고 수입에 의존하게 되는데, 막대한 제작 비용이 소모되는 데이터 서비스를 위한 콘텐츠들을 무료로 서비스하게 된다면 수익 구조상 데이터 서비스에 매우 소극적이 될 것이다. 이런 이유로 일부 데이터 서비스들에 대한 유료화 필요성이 대두되면서 제한 수신 시스템의 도입이 추진되고 있다. 현재 제한 수신 시스템을 T-DMB에 적용하기 위한 방법으로 서브 채널 제한 수신, 데이터 그룹 제한 수신, MOT 제한 수신 등의 세 가지 모드가 있다. 분석 결과, T-DMB에 제한 수신 시스템을 적용할 시에, 많은 가입자 수에 따른 대역폭 부족의 문제, AV와 함께 전송되는 BIFS만 따로 스크램블링 할 수 없다는 문제, 복수의 제한 수신 사업자들의 헤드 엔드 장비간 공통 인터페이스 작성, 다양한 수신 단말기들이 공통 인터페이스 작성 등의 문제점들에 대해서 기술하였다.

**Key Words** 지상파 이동 멀티미디어 방송, :T-DMB, 제한 수신 시스템, CAS

### 1. 서론

이동 중에도 선명한 화질의 비디오 서비스, 고음질의 오디오 서비스, 그리고 각종 부가 데이터 서비스를 수신할 수 있는 지상파 이동 멀티미디어 방송(Terrestrial Digital Multimedia Broadcasting : T-DMB, 이하 T-DMB)이 현재 본 방송을 서비스하고 있다. T-DMB는 기본적으로 비디오 서비스, 오디오 서비스, 각종 데이터 서비스 등의 멀티미디어 서비스를 무료로 제공한다. 즉, 별도의 수신료를 징수하지 않고, 광고 수입에 의존하는 비즈니스 모델을 갖는다. 데이터 서비스를 위한 콘텐츠를 제작하는 데에는 막대한 제작 비용이 소요되는데, 이것을 무료로 서비스하게 된다면, 방송사업자 입장에서는 수익 구조상 데이터 서비스에 매우 소극적이 될 것이다. 이러한 이유로 일부 데이터 서비스들에 대한 유료화 필요성이 대두되면서, 요금을 지불한 사용자만이 허가된 서비스에 접근 할 수 있는 제한 수신 시스템(Conditional Access System : CAS)의 접목이 필요하다.

이에 본 고에서는, T-DMB의 시스템 구조와 함께 T-DMB에 적용할 수 있는 제한 수신 시스템을 분석하였다.

### 2. 지상파 이동 멀티미디어 방송(T-DMB)

#### 2.1 지상파 이동 멀티미디어 방송 기술 개요

T-DMB는 상대적으로 적은 투자를 통하여 이동 수신이 가능한 내 손안의 디지털 TV라는 목표로, 무료 멀티미디어 서비스, 무료 대용량 데이터 서비스, CD급 음질의 오디오 전용 방송 등을 제공한다.

T-DMB는 유럽의 디지털 오디오 방송(Digital Audio Broadcasting : DAB) 방식인 Eureka-147 시스템을 기반으로 국내에서 MPEG-4 기반의 비디오 서비스와 대화형 방송 기능을 추가한 방식을 사용하므로, 사용하는 주파수 대역이 동일할 경우 DAB와 T-DMB는 완벽한 호환성을 갖는다.

T-DMB는 7인치 정도의 LCD 화면에 비디오 CD급 화질의 비디오 서비스를 제공하며, CD급 음질의 오디오 전용 방송도 가능하다. 또한 T-DMB는 대화형 데이터 방송을 위한 데이터 서비스, 오디오 서비스와 함께 제공되는 앨범의 재킷 사진이나 음악 방송의 스튜디오 사진, 방송 웹사이트(Broadcast Web site : BWS), 교통 정보(TPEG) 등의 다양한 데이터 서비스들을 무료 혹은 유료로 제공한다.

#### 2.2 지상파 이동 멀티미디어 방송 표준 및 시스템 구조

T-DMB 표준은 기본적으로 EUREKA-147이라 불리는 DAB 표준[1]을 기반으로 하고 있다. EUREKA-147 표준은 MPEG-1 오디오 레이어 II 표준을 중심으로 오디오와 밀접히 연관된 데이터 서비스 및 이와 별도의 스트림 형태 또는 패킷 형태의 데이터 서비스가 가능하도록 구성되어 있다. 여러 개의 오디오 압축 스트림 및 여러 종류의 데이터는 각기 채널부호화를 거친 후 시스템 제어 데이터와 함께 하나의 비트스트림으로 다중화되는데, 이렇게 다중화된 결과를 앙상블(emsemble)이라 부르며, OFDM 방식으로 변조된 후 고출력 증폭을 거쳐 송신된다. T-DMB는 압축된 비디오 서비스 정보를 EUREKA-147 시스템의 스트림 모드로 전송한다[2].

T-DMB 전송 프레임은 주서비스채널(Main Service Channel : MSC)과 고속정보채널(Fast Information Channel : FIC)의 정보를 다중화함으로써 구성된다. MSC는 미디어 데

저자 소개
* 정근일 : 서울시립대학교 전자전기컴퓨터공학부 석사과정
** 최성종: 서울시립대학교 전자전기컴퓨터공학부 부교수

FIC)의 정보를 다중화함으로써 구성된다. MSC는 미디어 데이터를 다중화하여 전송하는 채널이고, FIC는 MSC 다중화 제어 정보, 시스템 정보 등 미디어 데이터에 앞서 수신기에 전달되어야 하는 중요한 데이터를 전송하는 채널이다. FIC의 경우, 길쌈부호화 이후에 등장하는 시간 인터리버를 사용하지 않음으로써, 미디어 데이터가 겪는 처리 지연 시간을 피할 수 있도록 하였다. MSC는 여러 개의 서브 채널로 구성된다. 주 서비스다중화기는 미디어 데이터를 다중화하여 MSC 데이터를 출력하는 다중화기로서, 각 미디어 데이터는 하나의 서브 채널로 대응된다. 단, 패킷 모드 데이터의 경우, 패킷 다중화 구성기에 의해 일차적으로 다중화된 후, 그 결과가 하나의 서브 채널로 대응될 수 있다. T-DMB에서 추가된 비디오 서비스의 경우, 하나의 비디오 프로그램이 하나의 서브 채널에 대응된다. 서브 채널의 전송 용량은 동적으로 제어될 수 있으며, 각 서브 채널별 전송 용량은 FIC 정보 중 다중화 제어 정보(Multiplex Control Information : MCI)에 의해 수신기로 전달된다.

## 3. 제한 수신 시스템

### 3.1 제한 수신 시스템 개요

제한 수신 시스템은 수신자격(Entitlement)이 있는 사용자만이 서비스 또는 서비스 컴포넌트에 접근할 수 있도록 허용하는 시스템을 말한다.

제한 수신 시스템은 스크램블과 암호화의 조합으로 이루어진다[3]. 스크램블은 소리, 영상, 데이트를 알아볼 수 없도록 처리하는 것을 말하며, 암호화는 스크램블된 신호를 디스크램블 하기 위해 제어단어(Control Word : CW)를 암호화하는 것을 말한다.

### 3.2 스크램블링/디스크램블링

수신자격이 없는 수신자는 시청이 불가능하도록 데이터를 일정한 규칙에 의해 변형 및 복원한다. 이 때 사용되는 것이 제어단어로 데이터를 변형하고 복원하는데 일종의 키로 작용한다. 이 제어단어는 다시 암호화기(Encryptor)에 의해 보호되어 스크램블링된 방송 데이터와 함께 전송되며 수신기의 복호화기(Decryptor)에서 암호화된 제어단어를 복호화하여 방송 데이터 디스크램블링을 수행한다.

### 3.3 자격 제어 메시지

제어단어를 인증키로 암호화하고, 이를 자격 제어 메시지(Entitlement Control Message : ECM)에 실어서 수신자에게 전송한다. 보안을 위해 제어단어는 주기적으로 전송되며, 그 때마다 제어단어가 새롭게 생성되고 암호화된다. ECM에는 암호화된 제어단어 외에 제어변수가 포함되며, 수신기는 전송된 ECM을 수신할 수는 있지만 수신된 제어변수와 수신기의 인증변수를 비교하여 정당한 사용자로 판단될 경우에만 제어단어를 해독하고, 이를 이용하여 수신된 프로그램을 디스크램블링 한다.

### 3.4 자격 관리 메시지

수신기에 자격을 부여·갱신·관리하는 기능을 하며, 인증키를 분배키로 암호화하여 자격 관리 메시지(Entitlement Management Message : EMM)을 생성하고 암호화하여 수신자에게 전송한다. EMM은 수신기의 제한수신 모듈에 자격을 부여하거나 또는 갱신하는 기능을 한다. 송신부에서는 가입 신청을 한 정당한 수신자에게 해당 프로그램의 인증키와 수신자격을 전송한다. 인증키는 해당 수신자 고유의 비밀키를 이용하여 암호화한 다음 인증변수와 함께 EMM에 포함되며 메시지 변조 방지를 위해 전자서명 등이 추가되어 전송된다.

## 4. 지상파 이동 멀티미디어 방송에의 제한 수신 시스템 적용

### 4.1 지상파 이동 멀티미디어 방송에서의 스크램블링 모델

제한 수신 시스템은 T-DMB에의 적용을 위해 서브 채널, 데이터 그룹, MOT 등의 세 가지 레벨중 하나의 모드로 스크램블링이 가능하다[4]. 서브 채널 제한 수신은 완전한 하나의 서브 채널을 스크램블링한다. 예를 들어, PAD를 포함한 오디오 서브 채널이나, 패킷 모드 서브 채널, 스트림 모드 서브 채널을 각각 하나의 채널 별로 스크램블링 할 수 있다. 데이터 그룹 제한 수신은 IP 터널링이나, MOT, TDC 등과 같이 MSC 데이터 그룹을 사용하는 DAB 데이터 전송 프로토콜 모두를 스크램블링한다. MOT 제한 수신은 MOT 디렉토리 모드를 사용하여 전송되는 파일들을 스크램블링한다.

세 가지 모드에 관한 개념이 아래 그림 1에 나타나 있다.

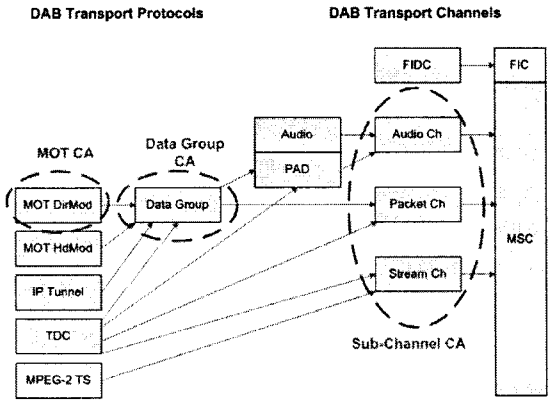


그림 1 세 가지 스크램블링 모드

### 4.2 Sub-channel CA

서브 채널 제한 수신은 많은 어플리케이션들을 만족시킬 수 있는 가장 보편적인 스크램블링 모드를 제공한다. 서브 채널 제한 수신은 전송 레벨에 위치하기 때문에 완전한 MSC의 서브 채널 하나를 스크램블한다. 그러므로 서브 채널 제한 수신 모드에서는 오디오 프로그램을 스크램블 하지 않고 그에 따른 PAD만을 스크램블 할 수 없다. PAD만을 스크램블 하고자 한다면 아래에 설명할 데이터 그룹 제한 수신을 이용해야 한다. 서브 채널 제한 수신에서는 PAD를 포함한 오디오 서브 채널, 패킷 모드로 데이터 서비스를 전송하는 패킷 모드 서브 채널, 스트림 모드 데이터를 전송하는 스트림 모드 서브 채널 등이 입력 스트림이 된다.

### 4.3 Data Group CA

데이터 그룹은 패킷 모드 서브 채널을 통해 전송된다. 데이터 그룹 제한 수신은 서비스 컴포넌트의 모든 데이터 그룹

이나 혹은 일부의 데이터 그룹을 스크램블 할 수 있다. 제한 수신 자격이 없는 수신기는 모든 데이터 그룹을 스크램블 할 경우 해당 서비스 컴포넌트로부터 어떤 정보도 처리 할 수 없고, 일부의 데이터 그룹을 스크램블 할 경우에는 스크램블 되지 않은 데이터 그룹은 처리 할 수 있다.

### 4.4 MOT CA

MOT 제한 수신은 MOT 디렉토리 모드와 관련이 있으며, 디렉토리 구조에 있는 MOT 객체들의 일부 혹은 모두를 스크램블한다. 제한 수신 자격이 없는 수신기는 스크램블 되지 않은 객체들을 처리 할 수 있다. 어떤 객체들이 스크램블 되었는지에 대한 정보는 MOT 디렉토리에 포함되어 있다. 따라서 MOT 디렉토리는 스크램블하지 않는다.

그림 2는 각각의 제한 수신에서 제한 수신 시스템의 의치를 나타낸다.

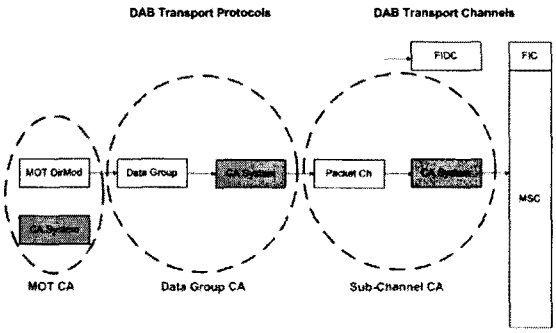


그림 2 세 가지 모드의 제한 수신에 따른 각각의 제한 수신 시스템의 위치

### 4.5 문제점

복수의 제한 수신 시스템을 동시에 송신단에 적용하는 것을 simulcrypt라 한다. 이 기술은 여러 제한수신 공급자를 수용하기 위하여 송신단과 가입자의 수신기에서 스크램블링과 제어단어 암호화 처리를 담당하는 부분을 모듈로 분리한 방식이다. 또한 모듈에서 동작하는 디스크램블링과 제어단어 암호화 기능을 분리하여 스크램블링 방식은 공통 스크램블링 알고리즘을 사용해야 한다. 제어단어 암호화 방법은 각 제한 수신 시스템마다 다르게 사용하도록 하여 가입자 수신기는 서로 다른 제한 수신 시스템을 갖는 보안 모듈을 수용할 수 있도록 하였다. 따라서, 다양한 제한 수신 공급자들의 헤드엔드 장비간의 simulcrypt를 위한 공통 인터페이스 작성이 필요하며, 현재 이 부분은 표준에 포함되어 있지 않다.

T-DMB는 AV와 연동된 데이터 방송을 위해 선택 사항인 BIFS (Binary Format for Scenes)를 채택하였고, 이를 사용할 경우 대화형 데이터 방송이 가능하므로 부가 데이터 서비스에 의한 여러 가지 비즈니스 모델이 가능하다. AV와 BIFS 데이터들은 MPEG-4 SL 및 MPEG-2 TS 패킷화 과정으로 다중화 되어 MSC의 스트림 모드로 전송이 된다. 현 제한 수신 시스템에서는 AV와 BIFS의 데이터들이 MPEG-2 TS로 패킷화 되어 전송되는 스트림 채널 전체를 스크램블링 할 수는 있으나, AV 정보를 제외한 BIFS 관련 데이터만을 스크램블링 하기는 불가능하므로, BIFS 정보만을 스크램블링 할 수 있는 방법 또한 모색되어야 할 것이다.

또 한 가지 고려해야 할 사항으로 제한 수신을 위한 T-DMB의 대역폭을 들 수 있다. 제한 수신을 위한 각종 파라미터 및 ECM, EMM 등을 FIC 채널을 통해 전송할 수 있는데, 가입자가 많아지면 제한된 FIC 채널의 대역폭이 문제가 될 수 있다.

## 5. 결론

본 고에서는 이동 중에도 선명한 화질의 비디오 서비스, 고음질의 오디오 서비스, 그리고 각종 부가 데이터 서비스를 수신할 수 있는 T-DMB 시스템과 T-DMB의 일부 데이터 서비스에 적용할 수 있는 제한 수신 시스템에 대해 간략하게 살펴보았다. 또한 현재의 T-DMB 시스템에 적용 시에 나타날 수 있는 여러 가지 문제점들에 대해서도 알아보았다.

현재 한국정보통신기술협회(TTA)에서 실무반을 구성하여 T-DMB에 제한 수신 시스템을 적용하기 위한 요구사항을 분석하고 이를 만족하는 표준안을 재정 중에 있다. 표준화가 완료되는 시점에는 시장 및 산업계의 요구사항이 충분히 반영되어 합당한 비즈니스 모델이 수립된 표준이 될 것으로 생각된다.

## 참고문헌


[1] ETSI EN 300 401(V1.4.1): "Radio Broadcasting System; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers,", ETSI, Jan. 2006.

[2] 정보통신단체표준 TTAS.KO-07.0024, "초단파 디지털라디오방송 송수신 정합 표준", 2003년 10월 24일.

[3] EBU Project Group B/CA "Functional Model of a Conditional Access System" EBU Technical Review Winter 1995.

[4] ETSI TS 102 367(V1.2.1): "Digital Audio Broadcasting(DAB); Conditional access", ETSI, Jan, 2006