특집 제한수신기술

지상파DMB 제한수신 기술 표준

□ 이진환, 이용훈 / 한국전자통신연구원 방송시스템연구부

Ⅰ. 서 론

지상파DMB(Terrestrial Digital Multimedia Broadcasting, T-DMB)는 차량용 소형TV, 노트북 컴퓨터, 내비게이션, PDA(Personal Digital Assistant), 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 이동멀티미디어 방송으로서 세계 최초로 국내에서 서비스 표준을 정하고 상용화 서비스를 하고 있다.

또한, 국내에서는 교통 및 여행자정보 (Traffic & Traveler Information, TTI), 미들웨어, 방송웹사이트(Broadcast Website Service, BWS), 슬라이드 쇼 등 다양한 종류의 데이터 서비스를 위한 표준들을 제정하였으며, 관련 기술을 개발하여 몇몇 방송사에서는 일부 기술에 대하여 서비스를 실시하고 있다.

무료 보편 서비스를 추구하는 국내 지상파DMB는 대부분의 수입원을 방송광고에 의지하고 있으나, 중국, 독일, 인도네시아, 가나 등 해외의 여러 나라에서는 유료화를 추진 중이다.

국내 수도권 지상파DMB 6개 사업자의 공동협의체인 지상파DMB 특별위원회에서는 DMB비디오와 기본 오디오를 제외한 일부 데이터 서비스의 유료화에 대비하여 공동 제한수신 시스템 (Conditional Access System, CAS)을 공급할 우선협상 대상자를 선정하여 CAS와 DRM(Digital Rights Management) 솔루션 개발을 추진 중이며, 이동통신사와 협력을 통한 양방향 데이터 서비스 등의 수익모델 발굴에 노력하고 있다.[1] [2]

지상파DMB에서의 유료서비스를 위하여 ETSI (European Telecommunications Standards Institute)에서는 Eureka-147 방식의 DAB(Digital

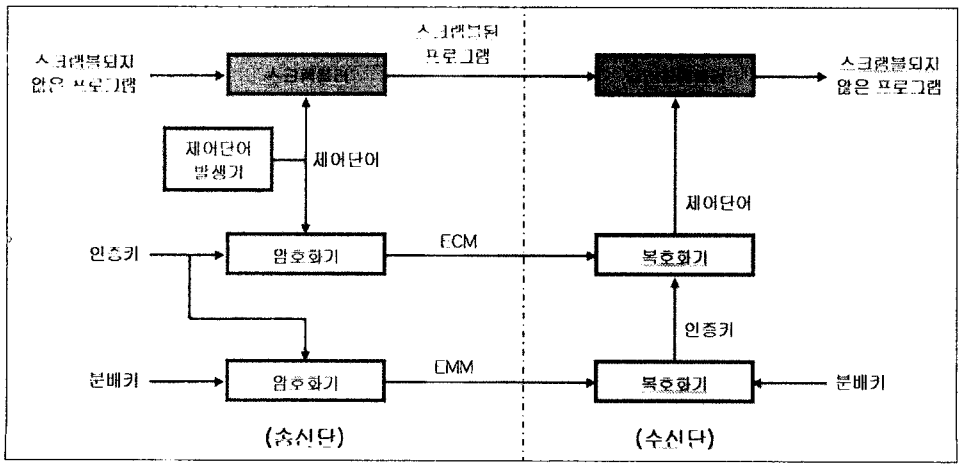
Audio Broadcasting) 제한수신 표준을 2006년 1월에 개정 공표하였으며, 국내에서도 TTA(한국정보통신기술협회; Telecommunications Technology Association) 내 DMB프로젝트그룹에서는 Eureka-147 DAB 제한수신 표준을 기반으로 표준화 작업을 진행하였다.

본 고에서는 지상파DMB 제한수신 기술 표준에 대하여 소개한다. 이를 위해 1장 서론에 이어 2장에서는 일반적인 디지털 방송에서의 제한수신 기술에 관하여 기술하고, 3장에서는 지상파DMB 제한수신 기술의 기본이 되는 Eureka-147 DAB 제한수신 표준에 대하여 소개한다. 4장에서는 국내에서 진행한 지상파DMB 제한수신 기술 표준에 대하여 기술하고, 5장에서 결론을 맺는다.

II. 일반적인 제한수신 기술

제한수신 시스템이란 유료화 서비스 중인 특정 방송 프로그램에 대한 수신 가능 여부를 사용자의 디지털방송 수신기가 결정하도록 하는 장치이다. 정당한 수신료를 지불하는 사람만이 해당 프로그램을 시청할 수 있도록 하기 위한 것으로 디지털 방송 상업화의 기본 필수 기능이다. [3]

제한수신 시스템이 갖추어야 할 기본적인 기능 요건은 인증받지 않은 수신자로부터 콘텐츠의 접근을 보호하기 위해 음성, 비디오 등의 방송데이터를 뒤섞는 스크램블링 기능, 인증 기능과 접근 제어 기능을 갖추어야 한다. 일반적인 제한수신 시스템의 구성은 <그림 1>에서 보는 바와 같이 송신단에서 방송데이터를 스크램블링하는 과정과 스크램블링에 사용되는 제어단어를 인증키로 암호화하는 과정 그리고 인증키를 분배키로 암호화하는 과정으로 나누어진다. 수신단에서는 송신단과 동일한 구성을 가지며 역의 과정을 통해 인증키를 분배키로 복호화하고 복호화된 인증키로 다시 제어단어를 획득하며, 획득한 제어단어를 통해 방송데이터를 디스크램블링하여 시청 가능한 형태의 신호를 출력하게 된다. 제한수신 시스템의 주요 기능은 다음과 같다.[4]



<그림 1> 제한수신 시스템의 블록도

1. 스크램블링/디스크램블링

스크램블링이란 수신자격이 없는 수신자는 시청이 불가능하도록 방송데이터를 뒤섞어서 변형시키는 기술로서 제어단어를 이용하여 스크램블링 처리한다. 즉, 제어단어는 방송데이터를 스크램블링하고 디스크램블링하는 일종의 키로 작용하므로, 디스크램블링 키인 제어단어를 복원하여 가질 수 있는 수신기에서만 디스크램블링을 처리할 수 있으며 정상적인 시청이 가능하다. 제어단어는 암호화기에 의해 보호되어 스크램블링된 방송데이터와 함께 전송되며, 수신기에서는 암호화된 제어단어를 복호화하여 방송데이터를 디스크램블링한다. 이를 위해 송신단과 수신단에는 같은 비밀키를 공유하여야 하며 이러한 비밀키를 공유하는 과정에서 보안성을 높이기 위해 스마트카드 등을 사용하여 사용자에게 전달한다.

2. 자격 제어

제어단어를 인증키로 암호화하고, 이를 ECM (Entitlement Control Message)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 수신자로 판단될 경우에만 제어단어를 해독하고, 이를 이용하여 수신된 프로그램을 디스크램블링할 수 있다. 이 ECM은 프로그램 마다 다르게 전송된다.

3. 자격 관리

수신기에 자격을 부여 · 갱신 · 관리하는 기능을 하며, 인증키를 분배키로 암호화하여 EMM(Entitlement Management Message)을 생성하고 암호화하여 수신자에게 전송한다. EMM은 수신기의 제한수신 모듈에 자격을 부여하거나 또는 갱신하는 기능을 한다. 송신부에서는 가입신청을 한 정당한 수신자에게 해당 프로그램의 인증키와 수신자격을 전송한다. 인증키는 해당 수신자의 고유한 비밀키를 이용하여 암호화된 다음 인증변수와 함께 EMM에 포함되고 메시지의 변조 방지를 위해 전자서명 등이 추가되어 전송된다.

앞에서 설명한 제어단어를 보호하기 위한 암호화 알고리즘, 암호화 키들을 관리하기 위한 보안 방법, ECM과 EMM의 구조 등은 제한수신 솔루션 회사와 각 제한수신 알고리즘에 따라서 각기 다른 방식을 사용하며, 이러한 것들은 제한수신 솔루션 회사의 고유한 권한이며 비밀에 해당되므로 제한수신 표준의 범위에 해당되지 않는다.

III. Eureka-147 DAB 제한수신 기술 표준

원래 Eureka-147 DAB 제한수신 표준은 지상파 DAB 전송 표준인 ETSI EN 300 401 V1.3.3의 9장에 실려 있었으나, 구현하기에 복잡하고 MOT (Multimedia Object Transfer) 레벨에서 제한수신이 지원되지 않는 점 등의 단점 때문에 새로운 별도의 표준인 ETSI TS 102 367 V1.2.1이 제정되었다. 새로운 제한수신 표준은 기존의 제한수신 표준과 호환되지 않으며, ETSI EN 300 401 V1.3.1에 실린 전송 표준과도 일부 호환되지 않으며 2006년 6월에 개정 공표된 전송 표준인 ETSI EN 300 401 V1.4.1과 호환된다. 새로운 제한수신 표준은 독일의 연구기관인

프라운호퍼가 제안하여 WorldDAB 포럼 (2007년에 WorldDMB 포럼으로 명칭 변경)에서 표준화 작업을 거친 후 ETSI를 통하여 2006년 1월에 공표되었다.

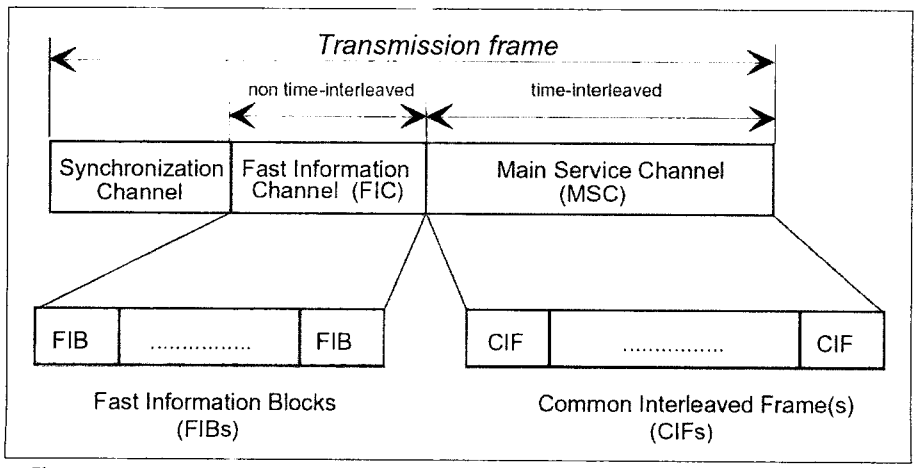
제한수신 표준은 단지, 앙상블 프레임 내에서 제한수신 파라미터 설정 방법, 제한수신 내부메시지(ECM, EMM)의 위치 등 제한수신 시그널링과 전송메커니즘에 관해서만 정해져 있으며, 이 장에서는 이 새로운 제한수신 표준인 ETSI TS 102 367 V1.2.1에 대하여 기술한다.[5]

DAB 제한수신 표준을 이해하기 쉽도록 Eureka-147 DAB 전송프레임의 구조에 대하여 우선 설명한다. Eureka-147 DAB 전송프레임은 <그림 2>와 같이 동기화 채널(Synchronization Channel), 고속정보 채널(Fast Information Channel, FIC), 주서비스 채널(Main Service Channel, MSC)로 구성되어 있다. 단말기가 방송정보를 빠르게 접근할 수 있도록 하기 위하여 사용하는 FIC는 다중화 구성 정보, 서비스 정보 등을 포함하고 있다. 또한, FIC는 여러 개의 FIB(Fast Information Block)로 구성되어 있으며, 이 FIB는 여러 개의 FIG(Fast Information Group)로 구성되어 있다. 제한수신과 관련된 파라미터 설정 등의 시그널링은 주로 이 FIG 필드값의 설정을 통하여 이루어진다. FIG 유형들을 <표 1>에 나타내었으며, 이 중에서 제한수신과 관련된 FIG의 유형을 회색으로 칠하여 나타내었다.[6] [7]

<표 1> FIG 유형 목록

FIG type number	FIG type	FIG application
0	000	MCI and part of the SI
1	001	Labels, etc. (part of the SI)
2	010	Labels, etc. (part of the SI)
3	011	Reserved
4	100	Reserved
5	101	FIC Data Channel (FIDC)
6	110	Conditional Access (CA)
7	111	Reserved (except for Length 31)

FIG Type/Ext	Description
FIG 0/0	ENSEMBLE INFORMATION
FIG 0/1	SUB-CHANNEL ORGANIZATION
FIG 0/2	SERVICE ORGANIZATION
FIG 0/3	SERVICE COMPONENT IN PACKET MODE
FIG 0/4	SERVICE COMPONENT IN STREAM MODE OR FIC WITH CA
FIG 0/5	SERVICE COMPONENT LANGUAGE
FIG 0/6	SERVICE LINKING INFORMATION
FIG 0/7	DATA SERVICE COMPONENT TYPE EXTENSION
FIG 0/8	SERVICE COMPONENT GLOBAL DEFINITION
FIG 0/9	COUNTRY, LTO & INTERNATIONAL TABLE
FIG 0/10	DATE & TIME
FIG 0/11	REGION DEFINITION
FIG 0/12	PROGRAMME TYPE PREVIEW
FIG 0/13	USER APPLICATION INFORMATION

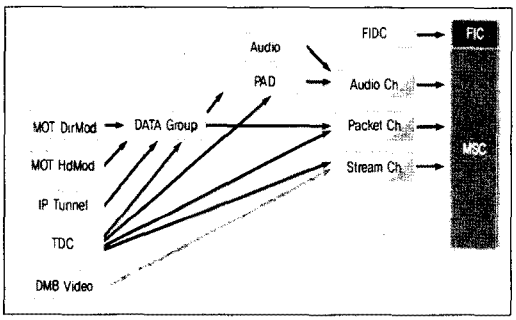


<그림 2> Eureka-147 DAB 전송프레임의 구조

1. 제한수신 모드

DTV에서는 방송데이터를 TS(Transport Stream)나 PES(Packetised Elementary Stream) 레벨에서 스크램블링하도록 표준에 정해져 있으며, 이 두 가지 레벨 중에서 단지 하나의 레벨만을 이용하여 스크램블링하여야 하며 두 가지 스크램블링 레벨을 섞어서 사용할 수 없도록 정해져 있다.[8]

그러나, 지상파DMB에서 방송데이터는 <그림 3>에서와 같이 프로그램 특성에 따라서 계층적으로 다중화되어 구성되며 최종적으로는 하나의 앙상블프레임 형식으로 다중화되어 전송된다. 또한, 제한수신 표준에서도 <그림 3>에서와 같이 해당 프로그램의 계층과 특성에 따라서 서브채널 모드, 데이터그룹 모드, 멀티미디어 객체전송(Multimedia Object Transfer, MOT) 모드인 세 가지 스크램블링 모드 중에서 하나의 방식을 선택하여 제한수신을 적용할 수 있게 되어 있다.



<그림 3> 지상파DMB에서 제한수신 모드

i) 서브채널 제한수신 : 해당 서브채널 전체를 스크램블링하는 방식이다. PAD(Programme Associated Data)를 포함한 오디오 서브채널, 패킷모드 서브채널 및 스트림모드 서브채널이 서브채널 제한수신 모드의 대상이다. DMB비디오 프로그램을 스크램블링하려면 이 서브채널 모드로 스크램블링하여야 한다.

ii) 데이터그룹 제한수신 : IP(Internet Protocol) 터널링, MOT 및 투명 데이터 채널(Transparent Data Channel, TDC)과 같이 MSC 데이터그룹을 사용하는 모든 종류의 DMB 데이터 전송 프로토콜에 대하여 제한수신을 적용할 수 있다. 데이터그룹 모드는 한 서비스 컴포넌트의 데이터그룹 전체를 스크램블링할 수 있다. 이는 MOT 관리 데이터(MOT 디렉토리, MOT 헤더)를 포함하는 데이터그룹도 모두 스크램블링함을 의미한다. 또한, 데이터그룹 제한수신은 한 서비스 컴포넌트의 일부 몇 개의 데이터그룹만을 스크램블링할 수 있다. 이 경우에는 제한수신을 지원하지 않는 수신기에서도 해당 서비스 컴포넌트 중 스크램블링되지 않은 데이터그룹은 제공받을 수 있다. 예를 들어, IP 서비스로 이미지와 사운드를 전송할 경우, 이미지만 스크램블링하고, 사운드는 스크램블링하지 않을 수 있다.

iii) MOT 제한수신 : MOT 디렉토리 모드를 사용하여 전달되는 파일에 대하여 제한수신을 적용할 수 있다. 예를 들어 MOT 디렉토리 모드가 적용되는 BWS에 링크된 객체들이 이의 대상이 될 수 있다. MOT 모드는 디렉토리 구조 내에서 일부 또는 전체 파일들을 스크램블링할 수 있다. 제한수신을 지원하지 않는 수신기도 MOT 객체 중 스크램블링되지 않는 객체를 처리할 수 있다. 예를 들어 방송웹사이트의 경우, 특정 서비스에 가입하는 방법 등의 정보, 일부 광고 데이터 또는 방송웹사이트 애플리케이션의 초기화면 등은 무료로 서비스할 수 있

다. MOT 디렉토리는 해당 파일들의 스크램블링 여부에 관한 정보를 가지고 있으며, MOT 디렉토리 자체는 스크램블링되지 않는다.

2. 공유 스크램블러

동일한 서비스에 대하여 여러 개의 제한수신 솔루션 제공자가 존재하는 경우에 방송데이터는 공통 스크램블링 알고리즘에 의하여 스크램블링되며 각기 다른 제한수신 시스템에 의하여 발생된 제한수신 내부메시지(ECM, EMM)는 동기화되어야 한다. 수신기에서 제한수신 내부메시지를 복호화하려면, 해당 서비스에 대하여 제공하고 있는 제한수신 솔루션 중에서 한 가지 솔루션은 탑재하고 있어야 하며, 모든 수신기에는 방송 데이터를 디스크램블링하기 위한 공통 디스크램블러가 탑재되어야 한다.

공유 스크램블러 시스템은 하나의 제한수신 시스템 내에서 업데이트가 계획되고 구버전과 신버전이 특정 기간 동안 동시에 사용하여야 할 경우에도 적용될 수 있으며, 이 공유 스크램블러 개념은 방송사가 특정 제한수신 업체의 기술에 종속되는 것을 피할 수 있다.

3. 제한수신 파라미터

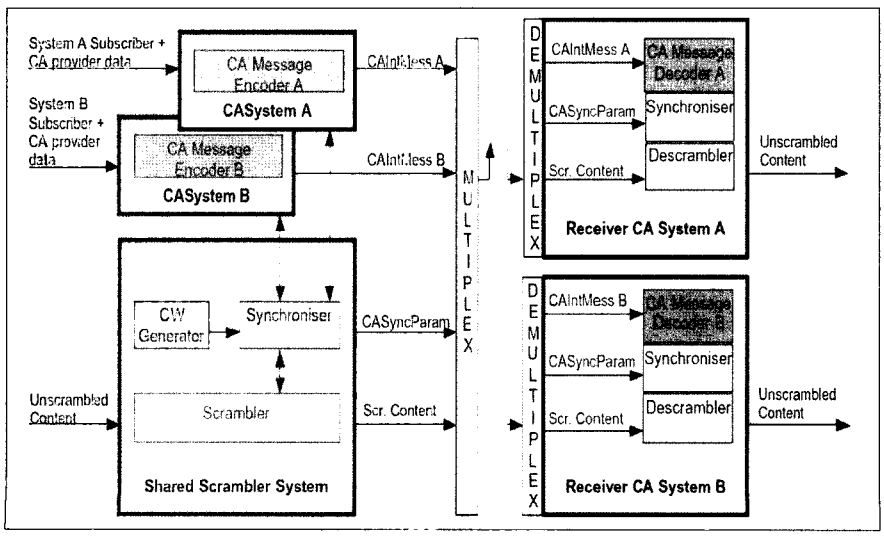
<표 2>에는 앙상블프레임 내에서 제한수신 모드에 따른 제한수신 파라미터와 제한수신 내부메시지 등의 위치를 나타내었다.

1) 제한수신 식별자 (CA Identifier, CAId)

서비스 내에서 적어도 하나의 컴포넌트가 스크램블링된 경우에는 "111"로 설정하고 그렇지 않은 경우에는 "000"으로 설정한다.

2) 제한수신 시스템 식별자 리스트 (CA System Identifier List, CASysIdList)

현재 사용되고 있는 제한수신 시스템 식별자 (CA System Identifier, CASysId), 단축 제한수신 시스템



<그림 4> 공유 스크램블러의 개념

<표 2> 제한수신 모드 별 제한수신 파라미터의 위치

<table>
<tr><th></th><th colspan="3">Sub-channel CA</th><th colspan="2">Data Group CA</th><th colspan="2">MOT CA</th></tr>
<tr><th></th><th colspan="3"></th><th>Packet mode</th><th>PAD</th><th>Selected MOT Objects are scrambled</th><th>All MOT objects of an MOT Data Carousel are scrambled (see note)</th></tr>
<tr><td>CAId</td><td colspan="3">FIG 0/2</td><td>FIG 0/2</td><td>-</td><td>FIG 0/2 / -</td><td>FIG 0/2 / -</td></tr>
<tr><td>CASysIdList</td><td colspan="3">FIG 6</td><td>FIG 6</td><td>FIG 6</td><td>FIG 6</td><td>FIG 6</td></tr>
<tr><td rowspan="2">CA Indication</td><td colspan="3">CAFlag in FIG 0/2</td><td rowspan="2">CAFlag in FIG 0/2</td><td rowspan="2">CAFlag in FIG 0/13</td><td colspan="2">CAIndi. existence of MOT header parameter CAInfo in MOT directory</td></tr>
<tr><td>Packet Ch</td><td>Stream Ch</td><td>Audio Ch</td><td>CAFlag in FIG0/2 / FIG 0/13</td></tr>
<tr><td>CAOrg Indication</td><td>CAOrgFlag in FIG 0/3</td><td>CAOrgIndi. existence of FIG 0/4</td><td>CAOrgIndi. existence of FIG 0/4</td><td>CAOrgFlag in FIG 0/3</td><td>CAOrgFlag in FIG 0/13</td><td colspan="2">CAOrgIndi. existence of MOT header parameter CAInfo in MOT directory
CAOrgFlag in FIG 0/3 / FIG0/13</td></tr>
<tr><td>CAOrg
"permitted CAMode"</td><td>FIG 0/3
"Sub-channel CA" or "Proprietary CA"</td><td>FIG 0/4
"Sub-channel CA" or "Proprietary CA"</td><td>FIG 0/4
"Sub-channel CA" or "Proprietary CA"</td><td>FIG 0/3
"Data Group CA" or "Proprietary CA"</td><td>FIG 0/13
"Data Group CA" or "Proprietary CA"</td><td colspan="2">MOT header parameter CAInfo in MOT directory "MOT CA" or "Proprietary CA"
FIG 0/3 / FIG0/13 "MOT CA" or "Proprietary CA"</td></tr>
<tr><td>CASyncParam</td><td colspan="3">SUBCAPrefix</td><td colspan="2">DGCAPrefix</td><td colspan="2">MOTCAPrefix</td></tr>
<tr><td>CAIntMess</td><td colspan="3">SUBCAPrefix</td><td colspan="2">MSC Data Group type 1</td><td colspan="2">MOT body or MSC Data Group type 1</td></tr>
</table>

식별자 (Short CA System Identifier, Short-CASysId), 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, Short-CASysId, CAIntChar는 서로 매핑되게 한다.

3) 제한수신 지시 (CA Indication)

제한수신 지시는 서비스 컴포넌트별로 제한수신이 적용되었는지의 여부를 단말에서 판단할 수 있도록 한다. 해당 서비스 컴포넌트에서 제한수신 플래그(CAFlag)가 "1"로 설정되었거나 제한수신 지시자 필드(CA Indicator Field, CAIndi)가 존재하면 제한수신이 적용된 것으로 판정한다.

4) 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.

예를 들면, 공유 스크램블러 플래그가 "0001 1010" 이라면 ShortCASysId가 "001", "011", "100"에 해당되는 제한수신 시스템들을 사용할 수 있다는 것을 나타낸다.

5) 제한수신 동기화 파라미터 (CA Synchronization Parameter, CASyncParam)

디스크램블러에서 동기화를 위하여 사용되는 CASyncParam은 제어단어의 변경을 나타내기 위하여 최소한으로 토글 플래그가 사용되어야 하며 프레임 카운터, 초기화 변경자 등의 파라미터가 사용될 수 있다.

6) 제한수신 시스템 내부메시지 (CA System Internal Message, CAIntMess)

이 메시지는 사용자의 자격과 암호화 키를 관리하기 위한 정보를 포함하고 있으며, 제한수신 시스템에서 일반적으로 말하는 ECM과 EMM이 이에 해당된다.

IV. 국내 지상파DMB 제한수신 표준화

국내에서는 2004년 10월경부터 2005년 7월경까지 차세대 디지털방송 표준포럼 (차방포럼)의 DMB분과위에서 제한수신 애드혹그룹을 통하여 Eureka-147 DAB의 새로운 제한수신 표준인 ETSI TS 102 367 초안을 기본 내용으로 국내 지상파 DMB 제한수신 정합표준(안)을 작성하였다. 차방포럼에서 작성한 표준(안)을 TTA에 제안하였으며, TTA의 DMB 프로젝트그룹에서는 CAS실무반을 구성하여 2006년 2월경부터 표준화 작업을 진행하였다.

TTA에서는 차방포럼에서 작성한 제한수신 표준 요구사항과 지상파DMB방송사의 요구사항을 취합하고 검토하여 표준을 작성하는데 필요한 요구사항을 결정하였으며, 이 요구사항에 맞도록 표준화 작업을 추진하였다.

지역별로 각 MSO(복수 종합유선방송사업자, Multiple System Operator)나 SO가 방송 송출을 관리하는 CATV 또는 단지 하나의 방송 사업자가 존재하는 위성DMB나 위성 DTV와는 달리 지상파 DMB는 여러 개의 방송 사업자가 존재한다. 현재는 수도권 지역에서 6개 사업자, 비수도권 지역에서는 13개 사업자가 서비스를 실시하고 있으나, 아날로그TV 채널(7~13번)에서 지상파DMB 채널로의 전환 등을 고려하면 훨씬 많은 수의 지상파 DMB 사업자가 등장할 것으로 예상된다. 따라서, 방송사들마다 다른 CAS 솔루션을 채택할 가능성도 배제할 수 없으며, 방송사가 CAS 솔루션 회사를 교체하거나 CAS 장비를 업데이트할 수 있게 하려면, 공유 스크램블러 개념을 이용하여 서비스할 수 있어야 한다.

따라서, TTA에서는 Eureka-147 DAB의 제한수신 표준을 기본으로 하되 실제로 공유 스크램블러 시스템을 이용한 제한수신 서비스가 가능하도록 추가로 필요한 사항들에 대하여 표준화를 진행하였으며, 이를 <표 3>에 정리하였다.

이를 위하여 첫번째로 필요한 사항은 공통 스크램블러 알고리즘의 선정이다. 따라서, TTA에서는 Eureka-147 DAB의 제한수신 표준의 내용에 공통 스크램블러에 관한 내용을 추가하여 "지상파 DMB 제한수신 정합표준"을 작성하여 2006년 10월에 제정 공표하였다. 최근에 개발된 스크램블러 중에서 보안성에 강한 AES(Advanced Encryption Standard)를 국내 지상파DMB CAS의 공통 스크램

블러로 선정하였으며, 제어단어 길이는 128비트만을 사용할 수 있도록 하였다. AES 스크램블링 알고리즘에는 크게 Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR) 모드 등 다섯 가지 모드가 존재한다. TTA의 제한수신 표준에서는 AES-128 중에서도 디스크램블링한 이후에 전송 에러가 확산되지 않으며, 스크램블링할 메시지의 길이가 제어단어 길이의 배수가 아니더라도 패딩 데이터를 추가할 필요가 없는 CNT 모드를 권고하고 있으며, CNT 모드로 동작시키는 데 필요한 카운터 블록값을 처리하는 방법도 표준에서 제시하였다.[9] [10] [12]

두번째로는 지상파DMB 헤드엔드 장비와 CAS 장비 간의 인터페이스를 위하여 "지상파 DMB 공유 스크램블러 시스템을 위한 송신장비 정합표준"을 작성하였다. 이 표준은 DVB(Digital Video Broadcasting)의 SimulCrypt 표준인 ETSI TS 103 197에 실려있는 내용 중에서 일부를 발췌하였으며 지상파 DMB에서 새롭게 규정할 필요가 있는 부분을 추가하여 작성하였다. [11] [13]

이 표준에서는 "ECM 생성기와 동기화기 간의 인터페이스", "EMM 생성기와 다중화기 간의 인터페이스", "동기화기와 다중화기 간의 인터페이스", "동기화기와 스크램블러 간의 인터페이스"에 대하여 장비 간의 송수신 메시지 구조 및 타이밍 관계 등을 정의하였다. 장비 간의 물리적인 인터페이스는 IP기반의 TCP를 사용하기로 정하였으며, 물리적으로 별도로 구성되는 장비 간의 정합시에만 이 표준을 준수할 의무가 있다.

이러한 내용을 표준으로 정해 놓으면, 헤드엔드 장비사와 CAS 솔루션 제공사가 각기 독립적으로 이 표준에 맞추어 각자의 장비를 개발할 수 있으며, 방송사에서는 이 표준에 맞게 개발된 다중화기와 CAS장비 중에서 방송사의 요구 조건에 맞는 장비를 선택할 수 있는 장점을 갖게 된다.

V. 맺음말

본 고에서는 지상파DMB 제한수신 표준의 기본이 되는 Eureka-147 DAB 제한수신 표준에 대하여 주로 소개하였으며, 이와 더불어 TTA에서 진행되어온 지상파DMB 제한수신 기술 표준에 대하

〈표 3〉 국내 지상파DMB 제한수신 표준

표준명(표준번호)	주요내용
지상파DMB 제한수신 정합표준 (TTAS.KO-07.0043)	Eureka-147 DAB 제한수신 표준 (ETSI TS 102 367) 준수 - 제한수신 파라미터 설정 방법 - 제한수신 내부메시지의 위치 - 제한수신 시그널링과 전송 메커니즘 정의
	공통 스크램블러 선정 - 128비트 AES 알고리즘 채택 - 카운터 모드 권고 및 카운터 블록값 처리 방법 제시
지상파DMB 공유 스크램블러 시스템을 위한 송신장비 정합표준 (TTAS.KO-07.0044)	DVB의 SimulCrypt 표준 (ETSI TS 103 197) 참조 - 장비 간의 송수신 메시지 구조 및 타이밍 관계 정의 - 장비 간의 물리적인 인터페이스: IP기반 TCP

여 소개하였다. 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. TTA에서는 Eureka-147 DAB 제한수신 표준의 내용을 기본으로 작성하되, 공통 스크램블러 알고리즘을 표준으로 정하였으며, 헤드엔드와 CAS 장비 간의 인터페이스를 표준으로 정함에 따라서, 이 표준을 만족하는 다중화기나 CAS 장비의 상용화 제품이 많이 출시될 수 있을 것으로 기대한다. 이에 따라서, 우리나라에서 세계 최초로 서비스 표준을 정하고 상용화 서비스하고 있는 지상파DMB가 국내외에서 널리 보급되고 활성화될 수 있는 발판으로 작용되기를 기대한다.

참 고 문 헌

[1] 전자신문, http://www.etnews.co.kr/news/detail. html?id=200712100171

[2] 전자신문, http://www.etnews.co.kr/news/detail. html?id=200808050141

[3] TTA용어사전, http://word.tta.or.kr/terms/terms.jsp

[4] 정준영, 구한승, 권은정, 권오형, "제한수신 기술 및 표준화 동향 분석," 정보통신연구진흥원: 정보통신 기술, 정책 및 산업 주간기술 동향," 2005. 9.

[5] ETSI TS 102 367 V1.2.1, "Digital Audio Broadcasting (DAB); Conditional access," 2006. 1.

[6] ETSI EN 300 401 V1.4.1, "Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers," 2006. 6.

[7] ETSI TR 101 496-2 v1.1.2, "Digital Audio Broadcasting (DAB); Guidelines and rules for implementation and operation; Part 2: System features," 2001. 5.

[8] ETR 289, "Digital Video Broadcasting (DVB); Support for Use of Scrambling and Conditional Access (CA) within Digital Broadcasting Systems," 1996. 10.

[9] Federal Information Processing Standards Publication 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001. 11.

[10] NIST Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation Methods and Techniques," 2001. 12.

[11] ETSI TS 103 197 V1.4.1, "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt," 2004. 9.

[12] 정보통신단체표준 TTAS.KO-07.0043, "지상파 디지털 멀티미디어 방송 (DMB) 제한수신 정합표준," 2006.10. 20.

[13] 정보통신단체표준 TTAS.KO-07.0044, "지상파 디지털 멀티미디어 방송 (DMB) 공유 스크램블러 시스템을 위한 송신 장비 정합표준," 2006.10. 20.

필 자 소 개

이 진 환

- 1987년 : 한국항공대학교 통신공학과 졸업
- 2002년 : 한국정보통신대학교 통신공학과 졸업(석사)
- 1989년 ~ 현재 : 한국전자통연구원 방송시스템연구부 책임연구원
- 주관심분야 : 디지털방송 시스템, 제한수신 시스템

이 용 훈

- 2005년 : 한밭대학교 전자공학과 졸업
- 2007년 : 충북대학교 정보통신공학과 졸업(석사)
- 2001년 ~ 현재 : 한국전자통신연구원 방송시스템연구부
- 주관심분야 : 디지털방송 시스템, 제한수신 시스템