

# T-DMB 제한수신시스템에서 제한 수신 메시지 다중화 기법 연구

김동현\* · 서형윤\* · 배병준\*\* · 김종덕\*<sup>o</sup>

\*부산대학교 · \*\*전자통신연구원

## A Study on Conditional Access Message Multiplexing Method in T-DMB Conditional Access System

Dong-Hyun Kim\* · Hyung-Yoon Seo\* · Byung-Jun Bae\*\* · Jong-deok Kim\*<sup>o</sup>

\*Pusan National University · \*\*Electronics and Telecommunication Research Inst

E-mail : dhkim1106@pusan.ac.kr

### 요 약

제한수신 시스템은 케이블 및 고정형 위성 방송 시스템에서 서비스 유료화를 위해 개발되었고 기술 및 시장 성숙도가 높다. 그러나 이러한 평가는 고정형 방송 시스템에서의 제한수신 기술로 한정된다. 지상파 DMB와 같은 디지털 이동 방송의 경우는 사용 형태 및 기술 특성으로 인해 기존 고정형 방송 시스템의 제한수신 기술을 그대로 적용하기 어렵다. 특히 제한된 리소스를 사용하는 T-DMB의 경우 각 서비스 채널마다 전송해야하는 제한수신 메시지는 방송 서비스에 문제를 발생시킨다. 각 서비스채널로 전송되는 제한수신 메시지를 논리적인 제한수신용 채널을 통해 전송하는 것이 바람직한데 이럴 경우 각 서비스 채널에서 사용되는 제한수신 메시지를 하나의 전용채널로 다중화 할 수 있는 기법이 필요하다. 본 논문에서는 전용채널 구성시 필요한 제한수신 메시지 다중화 기법을 설계하였다.

### ABSTRACT

CAS(Conditional Access System) was developed for paid-for service in cable and fixed satellite broadcast system and technology and market maturity are high. However, these assessment is limited by CAS in fixed broadcasting system. In case of digital mobile broadcast such as T-DMB is difficult to apply CAS technology of fixed broadcasting system because of a use method and technology characteristic. Expecially, in case T-DMB using limited resources, a CAS message which must transmit in each service channel can cause problems. It is desirable that system transmits the CAS message which transmitted by each service channel through logical CAS message-only channel. In order to make a logical CAS message channel, we need a multiplexing techniques for CAS message using in each channel. In this paper, we design the CAS message multiplexing techniques for composition of CAS message-only channel.

### 키워드

T-DMB, CAS(Conditional Access System), CAS Message, ECM, EMM

### 1. 서 론

T-DMB(Terrestrial-Digital

Multimedia

\* "이 논문 또는 저서는 2010년 교육과학기술부로부터 지원받아 수행된 연구임 "(지역거점연구단 육성사업/차세대물류IT기술연구사업단)

\*o 교신저자

Broadcasting)는 대한민국에서 개발된 디지털 영상 및 오디오 방송 전송 기술로써, 휴대 전화와 같은 기기에 텔레비전, 라디오와 같은 다중 매체를 전달하고 데이터 방송을 하기 위한 디지털 방송 서비스 기술이다[1]. 무료 서비스 기반의 T-DMB를 유료화 하기 위해서는 제한수신 기술이 필요하다. 제한수신 기술이란 유료화 서비스 중인 특정 방

송 프로그램에 대한 수신 가능 여부를 사용자의 디지털 방송 수신기가 결정하도록 하는 것이다. 정당한 수신료를 지불하는 사람만이 해당 프로그램을 시청할 수 있도록 하기 위한 것으로 디지털 방송 상업화의 기본 필수 기술이다. 제한수신 시스템은 암호화된 방송 프로그램을 위성/케이블/지상파/IP망과 같은 방송망을 통해서 전송하고 특정 가입자들만이 암호화된 방송 프로그램을 시청할 수 있도록 하는 방송 보안 시스템이다.

이러한 제한수신 시스템에서 제한수신을 하기 위해 사용하는 메시지는 ECM(Entitlement Control Message)과 EMM(Entitlement Manager Message)이 있다. ECM은 보통 제한수신 시스템이 보호하고자 하는 방송 채널마다, 제한수신 시스템마다 하나씩 존재한다. EMM은 가입자 관리를 목적으로 생성, 전달되는 메시지로서 방송 채널과는 직접적인 관련은 없고 가입자 관리의 다양성에 의해 여러 형태의 EMM들이 존재한다. 주파수의 효율성이 떨어지는 T-DMB의 경우 이러한 제한수신 메시지들을 각 서비스 채널을 통해 전송하게 되면 가입자의 증가에 따라 방송서비스에 영향을 미칠수 있기 때문에 전용채널의 구성을 생각할 수 있다. 이러한 전용채널을 이용하여 각 서비스채널에서 사용하는 제한수신메시지를 사용하기 위해서는 각 제한수신메시지의 다중화 방법이 필요하고 본 논문에서는 전용채널을 이용한 제한수신 메시지 다중화 방법을 설계하겠다.

## II. 제한수신 메시지 다중화 기법

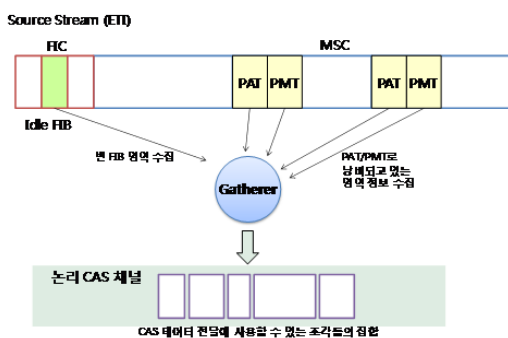


그림 1. 전용채널 구성을 위한 자원 조합 개념도

그림1은 제한수신 재다중화에 포함될 기능 모듈의 하나로 낭비 자원을 수집 결합하여 논리적 채널을 만들기 위한 Gatherer의 기능 개념도에 해

당한다.

우리가 제안하는 다중화 기법은 다음과 같다. 모든 제한수신 메시지를 T-L-V(형식-길이-값, Type-Length-Value)의 공통 구조를 가지게 한다. 헤더에 해당하는 T-L의 길이를 부하 절감을 위해 최소한의 자원만을 할당한다. 실제 우리는 Type에 4 bits, Length에 4 bits를 할당하는 방법을 제안한다. 길이 값을 위한 4 bits는 15까지만 표현할 수 있으므로 그 자체가 값을 의미하게 하는 것은 바람직하지 않다. 자주 사용되는 길이 값 집합을 미리 지정하고 그에 대한 인덱스로 활용한다.

Type은 기본적으로 제한수신 메시지를 분류하기 위해 활용하지만 또 다른 중요 기능은 조각 나눔 기능을 지원하는 것이다. 조각 나눔이라 메시지의 길이가 길어 한 번의 전송 기회에서 모두 처리하기 곤란할 때 이를 여러 개의 조각으로 나누어 전달하는 것을 의미한다. 조각 나눔을 통해 메시지를 전달할 때는 해당 조각이 메시지의 처음인지, 중간인지, 마지막인지 나아가 조각 중 몇 번째에 해당하는지 등의 정보를 담아 보내는 것이 바람직하다. 표1은 이것을 고려하여 임시로 지정한 제한수신 메시지 구분자를 정리한 것이다.

표1. 제한수신 메시지 구분자

Type	메시지
0000	Null, Padding
0001	ECM
0010	EMM-D
0011	EMM-A
0100	EMM-S
.....	.....
1110	Intermediate Chunk
1111	Final Chunk

예를 들어, 그림1의 Gatherer가 13bytes, 160bytes, 160bytes의 길이를 가지는 전용 채널을 구성하는 3개의 자원 조각을 수집하였다고 하고, 제한수신 시스템에서 그 시점에 전달하기를 원하는 메시지가 8bytes길이의 ECM, 256bytes길이의 EMM-S, 16bytes길이의 EMM-D라고 하자. 우리는 각 자원 조각의 제일 앞에 0xCA라는 값을 부여하여 해당 자원이 제한수신 메시지 전송용으로 쓰이고 있음을 표시하였다. 마치 MPEG2-TS 헤더

의 Ox47과 유사하다.

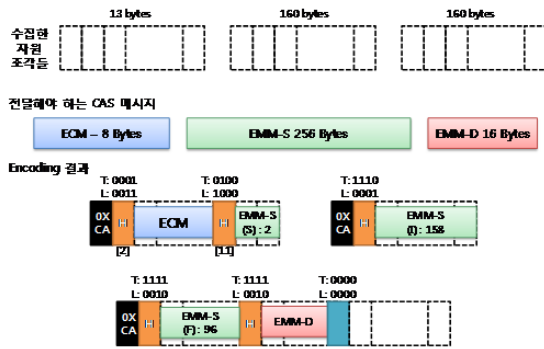


그림 2. 제안하는 제한수신 메시지 다중화 예

ECM 메시지에는 그림2와 같이 적절한 Type 및 Length 값을 부여하여 전달용 메시지를 구성한다. T-L 헤더를 추가하더라도 ECM 메시지의 길이는 9bytes이므로 0xCA 구분자를 포함하더라도 첫 번째 조각에는 여전히 3 bytes의 전송 공간이 남는다. 우리는 256 bytes 길이의 EMM-S 메시지를 이 공간을 이용하여 바로 이어 보낸다. 단 하나의 자원 조각에 메시지 전체를 보낼 수 없으므로 나머지는 이어지는 자원 조각에서 조각 나뉘어 전송된다. 두 번째 자원 조각으로 전달되는 EMM-S 메시지 조각의 Type 값을 살펴보면 조각 나눔에 의한 중간 조각임을 1110을 통해 나타내고 있고 길이 값 필드에는 길이가 아닌 조각 내 순서 번호에 해당하는 0001을 부여하고 있다. 두 번째 자원 조각을 통해서도 EMM-S 전송을 완료할 수 없기 때문에 이어지는 세 번째 조각에도 EMM-S 메시지 조각 일부가 포함되어 있음을 볼 수 있다. 마지막 조각이므로 그에 해당하는 Type 값을 부여하여 처리하고 있음을 확인할 수 있다. 예제를 통해 기존 방법과 달리 자원을 낭비하지 않고 제한수신 메시지를 전달할 수 있음을 확인할 수 있다.

### V. 결론 및 향후 연구 계획

T-DMB 서비스는 주로 광고 수익을 통해 운영을 해 왔으나 고품질, 다채널, 전문 채널 서비스 제공 등 양질의 서비스를 시청자에게 제공하기 위해서는 기존 광고 수익 구조에서 탈피하여 가입자에게 서비스에 대한 시청료를 징수할 수 있는 시스템이 필요하다. T-DMB의 유료화를 위해 제한수신 시스템을 사용할 수 있으며 고정형의 제

한수신 시스템 방식을 T-DMB에서 사용하기에는 제한점이 많다. 특히 제한된 대역폭은 각 서비스 채널을 통해 전송해야 하는 제한수신메시지에 의해 특이할 만한 문제점이 될 것이다. 이러한 문제점은 전용채널 구성을 통해 극복할 수 있을 것이다. 각각 전송되는 제한수신 메시지를 하나의 전용채널을 통해 전송하기 위해서는 각각의 메시지를 하나의 전용채널로 전송하기 위한 다중화 기법이 필요하다. 그래서 본 논문에서는 제한수신 메시지를 다중화 할 수 있는 다중화 기법을 설계하였다. 제한수신 메시지 구분자를 이용하여, 메시지의 종류를 구분하였고, 조각 나눔기능을 이용하여 메시지의 위치 및 순서를 구분하는 것이 우리가 설계한 다중화 기법의 특징이다. 여러 다중화 기법과 비교하여 제안한 기법의 성능을 평가하고 우수성을 검증하기 위한 시스템 개발이 필요하다.

### 참고문헌

- [1] <http://www.wikipedia.org>.
- [2] TTAS.KO-07.0043, 지상파 디지털 멀티미디어방송(DMB)제한수신 정합표준, 2006. 10.20.
- [3] 김용환, "지상파DMB 기술및표준현황", 한국통신학회지, Vol. 21 No. 11, pp. 35-45, 2004. 11.
- [4] 신용태, 오성훈, "제한수신기술", 방송공학회지, 제13권제4호, pp.4-13, 2008. 12
- [5] 황희상, 김대웅, 은종원, 박성열, 조혜정, "지상파 DMB수신제한 솔루션 적용 사례", 방송공학회지, 제13권제4호, pp.25-36, 2008. 12
- [6] ETSI: EN 300 401, 3<sup>rd</sup>EditionRadiobroadcastingsystems:DigitalAudio Broadcasting(DAB)tomobile,portableandfixedreceivers,2001.