DigiPass IRD의 제한수신기능 설계 및 구현에 관한 연구

한용운*, 정덕진
인하대학교 공과대학 전자재료공학과

DigiPass IRD Fabrication and Verification of CAF

Yong-Woon Han, Duck-Jin Chung
Dept. of Electronic Materials & Device Engineering, INHA Univ.

요약 - 본 연구에서는 11.7GHz ~ 12.2GHz 주파수 대역의 무궁화 위성방송 송,수신기 정합표준 2.0과 디지털 위성방송 제한수신 정합 잠정표준을 만족하는 무궁화 위성방송 수신시스템 분야에 대한 연구를 수행하였다. 상위 표준에 의거하여 제한 수신모듈을 탑재한 디지털 위성방송 수신장치 개발에 따른 타당성과 신뢰성을 검증하고자 Subscribed and Per-Per-View 채널 디스크램블링 및 가입자 관리(Subscriber Management)에 필요한 데이터 ECM, EMM, RCM 등의 데이터 축출과 처리과정을 모델링하고 모의 실험 수신기(IRD : Integrated Receiver and Decoder)를 제작하여 한국 전자통신연구원에서 작성한 "제한 수신 시스템 신뢰성 검증시험절차서"에 따라 동작반응을 시험하였다.

1. 서 론

최근 들어 위성의 상업적 이용의 확대와 더불어 위성에 의한 직접위성방송(Direct Broadcastinf Satellite)이 도입되고 있으며, 음성 및 영상 신호 전송도 디지털로 가는 추세다. 종래의 지상파 방송 중심의 TV 방송은 위성방송이 디지털 전송 시스템으로 변화함에 따라 TV 신호를 디지털 처리 및 전송을 가능케 하여, 신호 전송의 높은 비화도를 가질 수 있고 영상 화질의 향상을 꾀할 수 있다. 또한 위성을 이용한 직접 위성방식은 수신료를 납부한 기입자만이 방송을 수신할 수 있는 가입자 개념으로 변환을 특징으로 한다. 위성방송은 누구나 시청할 수 있다는 전파상의 특성 때문에 조건부 접근 제어(Conditional Access Control : 이하 규격에 따라 제한 수신으로 명명함)기능의 역할에 대한 개념이 중요하게 대두되었다.

Pay-TV 시스템에서 제한 수신기능을 이용하여 위성방송에 가입자 개념을 추가하여 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하고, 전문 방송업자들에 의한 전문 방송 프로그램의 제작을 가능하게 하여 다양한 품질의 서비스를 제공할 수 있게 되었다. 가입자 개념을 가지는 상업 방송의 높은 부가가치성에 대한 인식으로 몇몇 선진국에서는 제한 수신에 대한 연구가 상당히 진척되고 있으며, 상용화에 성공하거나 검증단계에 있다. HDTV, DTTV, VOD, Digitla CAble Modem등 신호전송의 디지털화와 스크램블링 기술에 발맞추어 제한 수신 시스템의 중요도가 크게 부각되고 있다. 본 논문는 디지털 위성방송에서의 제한 수신 기능 및 KoreaSat DBS의 제한 수신 시스템인 DigiPass(Digital All Pass: Audio/Video/Data)시스템에 대해서 설명하고 11GHz ~ 12.2GHz 주파수 대역의 무궁화 위성방송 송,수신기 정합표준 2.0과 디지털 위성방송 제한 수신 정합 잠정표준을 만족하는 디지털 위성방송 수신기의 제한수신기능 구현 및 규격검증에 관한 연구를 수행하고자 한다.

2. DigiPass 시스템 분석

2.1 스크램블링/디스크램블링 기능

스크램블링(Scrambling)은 원 신호에 변형을 가하여 스크램블된 형태의 신호만으로는 수신권한이 없는 수신자는 시청할 수 없도록 하는 것으로 신호의 종류(영상,음성,데이터) 및 신호의 형태(아날로그,디지털)에 따라 스크램블링 방식이 달라진다. 디스크램블링은 스크램블된 프로그램을 원 신호대로 복원하는 과정을 말하며 결국 제어워드(Control Word : CW)라는 파라메터를 가진 수신기(IRD)들에서만 디스크램블된 프로그램의 시청이 가능하다. 신호의 질을 손상시키지 않고 스크램블링/디스크램블링(Scrambling /Decrambling)하는 과정은 아날로그 신호보다는 디지털에서 더 간단하며 스크램블링의 안전도는 결국 스크램블링을 위해 생성되는 의사 난수열의 안전도에 의존하므로 디지털 신호를 스크램블링하기 위해서 블록 암호화같은 방법이 사용된다.

2.2 자격 통제 기능

프로그램을 디스크램블하기 위해 필요한 권한과 관련 키들을 Entitlement라 한다.이 기능은 암호화된 Control Words와 프로그램을 Access해서 필요로한 요구조건들을 분배, 즉 난수 발생의 초기치인 제어워드(Conrol Word: CW)를 암호화하고 그 제어 워드를 자격통제 메시지(Entitlement Control Message)를 통해 전송한다.수신기(IRD)는 이 ECM을 받게 되면 암호화된 CW와 제어 조건들을 스마트 카드라고 하는 Security Device로 보내게 되어 먼저 합당한 데이터인지를 체크한 후에 CW를 복호화하고 디스크램블러로 보내게 되며 가입자는 디스크램블된 프로그램을 시청할 수 있다. ECM은 보통 한개의 패킷으로 구성되어 주기적으로 전송되며, 그때마다 새로운 CW가 암호화되어 전송된다.

2.3 자격 관리 기능

자격 관리 기능은 가입자들에게 자격(Entitlements)을 전달하는 기능으로 이 데이터는 EMM(Entitlement Management Message)라는 메시지에 실어서 보낸다. EMM은 수신기의 보안장치인 스마트 카드내에 자격을 부여하거나 갱신하는 기능을 지원하며, 각 수신기의 주소에 의한 인식 기능을 이용하여 수신자의 서비스 키를 바꾸거나 통제하는 통제 취득기능의 지원도 기능하다. 자격 관리 기능은 앞으로 시청할 프로그램의 수신자격에 대한 정보관리 기능이므로 Batch동작으로 실행된다.

따라서 전송할 프로그램과 동기화되어 전달될 필요는 없으며, EMM을 형성하여 특수 채널을 통해 방송되거나 우편등의 매체로도 전달될 수 있다. 위의 자격 통제 기능과 자격 관리 기능의 지원을 수행하기 위해 비밀

키와 암호화 알고리즘이 요구되고 사용되며 새로이 설계된 대부분의 제한 수신 시스템은 정보를 안정하게 저장하고 수행하기 위해 보통 스마트 카드를 사용하고 있다.

2.4 수신기 제어 기능

수신 제어 기능은 스마트카드 주소를 가진 수신기에게 개별적으로 명령을 내릴 수 있는 기능으로 RCM 메시지에 의해 전송된다. 현재 RCM 메시지는 2종류가 있는데 하나는 RSMS 센터의 PSTN 및 PSDN 전화번호를 알려주는 서비스 메시지이고 다른 하나는 스마트카드의 PPV 사용 기록을 업로드하도록 요청하는 명령 메시지이다. 수신기는 스마트카드의 기록 용량이 80%에 다다르면 RCM 서비스 메시지의 전화번호로 센터에 접속해 RCM 발송을 요청하도록 되어있다.

2.5 RSMS 데이터의 역다중화 방법

MPEG2 트랜스포트 스트림에 포함된 모든 데이터는 PSI 섹션 테이블에 의해 역다중화된다. 프로그램 서비스를 구성하는 ES의 PID들은 PMT에 나열되고, 각 채널마다의 PMT의 PID는 PAT에 나열되어 있다. PAT의 PID는 0으로 고정되어 있어서 어떤 역다중화 정보 없이도 추출해 낼 수 있다. 원래 DVB 규격에서는 PAT 외에도 대부분의 섹션 테이블들의 PID 값은 고정되어 있다. 그러나 국내 무궁화 위성방송 정합 표준은 이와 조금 상이하다. [그림 1]에서는 국내 정합규격에 의거하여 역다중화 참조방법을 도식화하였다. NIT/TDT/SDT가 모두 같은 PID를 가지고 있으며 PAT의 프로그램 0번 노드에서 지정된다. 이 테이블들의 종류를 구분하는 방법은 PID가 아닌 table_id 필드에 의해 식별해야 한다. PAT의 프로그램 1번 노드도 RCM의 PID를 위해 예약되어있다. 그러나 RCM의 PID는 CAT의 RCM descriptor내에 중복 기술되어 있으므로 둘 중에 어느 쪽을 택하여도 관계없다.

제한 수신 기능에 관련된 EMM과 RCM의 PID는 CAT 섹션의 CA descriptor에 지정되어 있다. CAT는 PID값이 1로 고정되어 있어서 PAT와 마찬가지로 역다중화 정보 없이도 추출해 낼 수 있는 PSI의 하나이다. ECM의 PID는 CAT 섹션이 아닌 PMT 섹션의 CA descriptor에 명시되어 있는데, 이는 CW가 각 채널마다 독립적으로 존재할 수 있기 때문이다. 수신기는 PMT 내에서 ECM PID의 존재 여부에 따라 채널의 스크램블 여부를 판단할 수도 있다.

3. DigiPass IRD 의 제한수신기능 설계

3.1. 하드웨어 구조

CAS 기능을 추가한 Digital Satellite IRD의 주된 구성요소는 [그림 2]와 같고 이러한 제한수신 기능의 구현을 위한 모듈로는 디스크램블러, 스마트 카드 인터페이스, 디이얼 백 모듈이 있다. 시스템은 Demux와 DVB 디스크램블러를 내장하고 있는 메인 CPU와 사용자 인터페이스를 주관하는 스탠바이 프로세서의 2개의 프로세서로 구성된다.

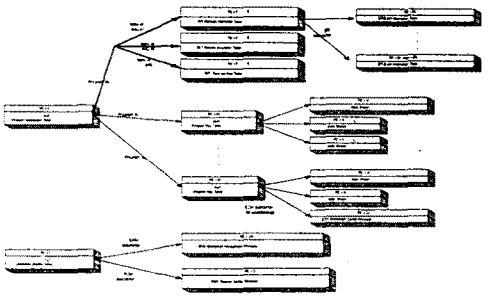

그림1 RSMS 데이터를 이용한 역다중화 계층도

디스크램블러의 모듈의 위치는 QPSK/FEC 출력단과 Demux 모듈의 입력단 사이에 존재한다. 국내 제한수신 시스템은 트랜스포트 패킷 단위의 스크램블 방식이기 때문에 Demux가 이루어지기 전에 패킷 헤더에 위치한 스크램블 여부 플래그를 조사하여 디스크램블을 먼저 수행해야 한다. 스마트카드 인터페이스는 메인 프로세서 내에 내장된 비동기 직렬 통신 모듈을 이용하여 구현되었다.

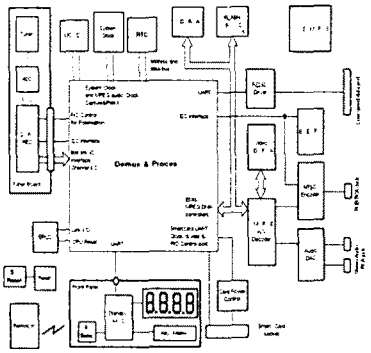

그림2 HW 모듈 블럭 다이어그램

3.2 디스크램블 및 메시지 처리

수신기 소프트웨어는 메인 프로세서인 ST20-TP2의 하드웨어-커널 멀티태스킹을 이용하여 약 30여개의 타스크로 구현되었다. [그림 3]은 메시지 처리 관련 주요 타스크들의 구조 및 데이터의 흐름을 보여준다. 타원으로 표시한 타스크들 사이의 데이터 교환은 링 모양으로 표시한 순환-큐를 통해 이루어질 수도 있고, 우체통 형태로 표시한 메일박스를 통해 이루어 진다. 메일박스를 통한 데이터 전송의 경우는 타스크 간의 동기가 자동으로 구현되지만 원형큐의 경우는 타스크 간의 데이터 전송의 동기를 맞추기 위해 깃발 모양으로 표시한 세마포를 사용하였다. ST20-TP2의 특징은 이러한 OS 커널의 기능들이 하드웨어적으로 지원되어 매우 효율적이라는 점이다. 튜너 및 QPSK/FEC 모듈로부터의 비트스트림 입력을 받아들이는 타스크가 그림의 최상단에 위치해 있다. 입력은 TS 패킷 단위로 이루어져 순환큐에 저장되며, 다음단의 디스크램블 타스크가 이 패킷의 헤더를 보고 필요에 따라 디스크램블한다. 디스크램블되어진 패킷은 큐의 원래의 자리로 되돌려지며, 다시 Demux 타스크의 입력이 된다. Demux는 기존에 구축된 SI 데이터베이스에 근간하여 TS 패킷들을 요구하는 Consumer 타스크들에게 분배하게 되고, 이 TS 패킷들은 각 Consumer 타스크들에 의해 PES 단위, 섹션 단

위, 메시지 단위로 조립된다. 그림의 우측에 위치한 섹션 핸들러 타스크는 모든 섹션에 관련되 TS 패킷을 받아서 필터링을 수행하여, 결과적으로 얻어진 섹션들을 다시 2차 Consumer 타스크들에게 섹션 단위로 전달한다. 이 섹션 Consumer 타스크들이 시스템 부팅시에 SI 데이터베이스를 구축하게되고 이것은 다시 Demux 타스크가 패킷들을 역다중화하는데 필요한 정보가 된다. 제한 수신 기능에 관련된 EMM, ECM, RCM 메시지는 RSMS 메시지 핸들러에 의해 일괄 처리되는데, 여기서는 스마트카드 어드레스에 의해 필터링이 행해진다. 이중 EMM과 ECM은 스마트카드 타스크에게 전송되고, 스마트카드 타스크는 실제 카드와 트랜잭션을 통해 CW를 얻어낸다. 이 CW는 초반부에 기술한 디스크램블러 타스크에게 전달되어 키값으로 사용된다. RCM 메시지는 USIF 타스크를 거쳐 다이얼백 타스크로 전달된다. 이는 RSMS 센터로 전화접속을 시도하여 스마트카드의 PPV 시청 기록을 업로드한다. 업로드가 완료되면 스마트카드의 메모리를 비우면서 RCM 명령 수행이 종료된다. 만약 스마트카드의 PPV 시청 기록용량이 80%에 다다를 때까지 RCM이 수신되지 않으면 다이얼백 타스크 측이 먼저 센터에 접속을 시도해 RCM 전송을 요청하게 된다.

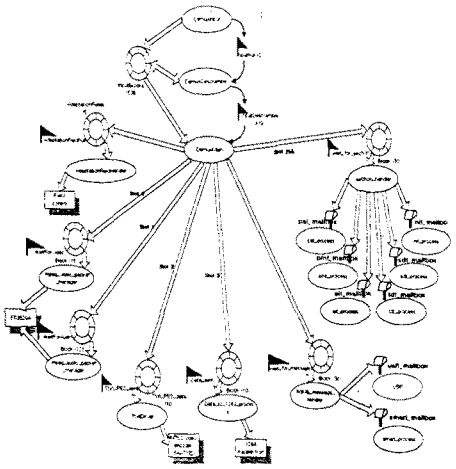

그림3 타스크 구조 및 데이타 흐름

3. 실 험 및 결 론

EMM 변경주기 측정결과는 실험 형상 데이터에서 600초(10분) 간격으로 CAM에서 전송하기로 한 제약조건과 같이 측정 데이터를 분석해 보면 10.0분 간격으로 검출됨을 알 수 있었다. EMM 전송주기 측정결과는 실험 형상데이터에서 15초 간격으로 CAM에서 전송하기로 한 제약조건과 같이 측정 데이터를 보면 15.0초를 기준으로 해서 0.2초 상회해서 검출됨을 알 수 있었다. EMM 처리시간은 0.34 ~ 0.35초에서 프로세싱됨을 알 수 있었고 EMM 처리시간의 0.01초(10mS)의 오차범위를 같는 이유는 EMM 메시지를 Smart Card까지의 물리적인 경로(Physical Path)가 시리얼 통신 구조라는 점과 메시지의 전달이 멀티타스크간의 신호처리의 Delay현상으로 분석되었다. 제안된 구조의 IRD의 EMM 메시지 처리시간이 평균 0.34x초 소요되므로 EMM 전송주기 15초인 형성데이터의 제약조건은 IRD가 처리하기에 문제가 없는 것으로 판단된다.

ECM 변경주기 측정결과는 실험 형상데이터에서 15초 간격으로 TAM에서 전송하기로 한 제약조건과는 같은 결과를 얻지 못했다. 데이터를 분석한 결과 ECM 메시지 변경시 3프레임으로 분산하여 메세지를 전송하며 첫 번째와 두 번째는 0.1초간 격으로 5회 반복전송하고 세 번째 프레임은 ECM 다음 변경주기 때까지 반복 전송됨을 알 수 있었다. ECM 변경주기는 첫 번째 프레임을 기준으로 할 때 변경주기가 14.5초와 15.5초를 반복적으로 전환됨을 알 수 있었다. ECM 전송주기 측정결과는 실험 형상데이터에서 0.1초 간격으로 TAM에서 전송하기로 한 제약조건과 같이 0.10x초 주기로 전송됨을 알 수 있으며 ECM 처리시간을 분석한 결과를 기준을 하면 ECM 메시지를 처리하는데 평균 0.4x초가 소요되므로 RSM 타스크에서 ECM 메시지를 축출(검출)했을 때 Control Word가 변경이 없다면 해당 ECM 메시지 프레임은 Skip해야 한다는 것을 알 수 있었다. ECM 처리시간은 0.41초 ~ 0.42초에서 처리됨을 알 수 있었고 처리시간정보는 ECM 메시지의 RSM 타스크 처리에 영향을 주는 것으로 분석되었다. RCM 메시지중 "사용량 레코드"전송의 처리시간은 다이얼 백 모뎀의 호 처리시간과 데이터 전송 시간을 합하여 약 평균 43초 걸리는 것으로 확인되었다.

표 1 항목별 실험 데이타

항목	1	2	3	4
EMM변경	10.064	10.065	10.066	10.062
EMM전송	15.167	15.175	15.163	15.153
EMM처리	0.343	0.342	0.342	0.343
ECM변경	0.5194	0.5114	0.5250	0.5151
ECM전송	0.1003	0.1039	0.1041	0.1005
ECM처리	0.412	0.411	0.413	0.412

제안된 제한 수신기능(CAF)구조은 해태전자 VT-2000K에 탑재되어 검증되었, 지역 실험 망과 한국통신 용인관제소 무궁화 위성망을 통해 한국 전자통신연구원에서 제작된 디지털 위성방송 유료서비스 시스템(DigiPass)의 CAS기능을 만족하고 있음을 디지털 위성방송 제한 수신시스템 검증절차서의 실험결과로서 알 수 있었다.

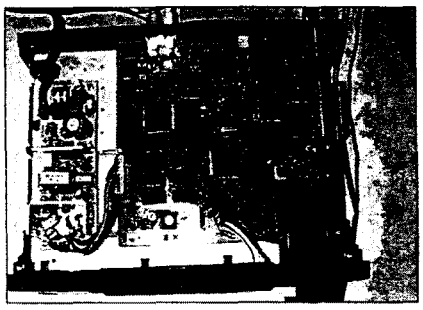

그림4 VT-2000K CAF IRD 내관

[참 고 문 헌]

[1] ISO/IEC 13818-1 MPEG-2 Systems Standard
[2] ISO/IEC 13818-2 MPEG-2 Video Standard
[3] ISO/IEC 13818-3 MPEG-2 Audio Standard
[4] ETSI/DVB Specification for Service Information in DVB, prETS 300 468 12/02/1996
[5] ETSI/DVB Digital broadcasting systems for television, ETR 211 12/02/1996
[6] 11.7GHz ~ 12.2GHz 주파수 대역의 위성방송 송수신 정합 표준(KICS.KO-07.0008), 정보통신부 고시 제 1997-17호,1997년 3월 21일
[7] 디지털 위성방송 제한수신 정합 잠정표준 (TTA.KO-07.0009) 제 1997년 8월 8일
[8]CCITT X.28,V.22bis
[9] ISO 7816 Standards for Smart Cards
[10] ST20-TP2 Programmable Transport IC for DVB Applications / SGS-THOMSON