主題

양방향 대화형방송 기술 개발 현황

KBS 강대갑, 삼성전자 이광기, LG전자 박석원, 대우일렉트로닉스 김용재

차 례

1. 서 론
2. 양방향 대화형방송 송수신 시스템 기술개발
3. 양방향 데이터방송 저작도구 및 표현미들웨어 기술 개발
4. 보안/인증을 적용한 송수신 상향채널 기술개발
5. 양방향 대화형 콘텐츠 개발
6. 양방향 대화형 표준안 작성 및 송수신 정합 실험 실시
7. 기술개발 결과 및 기대효과
8. 결 론

초 록

성공적인 양방향 대화형 방송 서비스를 위해서는 수신기 개발 뿐 만 아니라, 서비스 제공자와 함께 End-to-End 솔루션을 개발하는 것이 필수적이다. 본 기고에서는 최근의 기술 개발 현황을 대화형 서비스를 상용화하기 위한 미들웨어 기술의 안정화 및 서버와의 정합작업, 가입자관리, 대화형방송 편성/운행 시스템, 보안인증 기술의 개발, 서비스 개발 등을 중심으로 소개하고자 한다.

1. 서론

디지털방송은 기존 아날로그 방송과는 달리 고화질 및 고음질의 고품위 서비스를 제공할 뿐만 아니라 디지털 부호체계를 통한 시스템통합(integration)과 상호운용성(interoperability)을 바탕으로 다기능성을 제공한다. 다기능성이란, 멀티미디어 정보들을 방송매체를 통하여 제공하는 새로운 통합서비스를 의미한다. 이를 통하여 방송은 컴퓨터와 네트워크를 동원한 이른바 미디어 융합(media convergence)의 핵심이 될 수 있는 조건을 갖추게 되었는데, 대화형 기능(interactivity)이 가미되어 일방적이고 하향적이었던 방송영역을 새롭게 변화시키는 계기가 될 것이고, 방송서비스의 다양화 · 개인화 · 양방향화 · 네트워크화 등이 가능해 질 것이다. 이러한 방송과 통신의 융합에 따른 기술적/시대적 방송환경의 변화는 기본적인 오락기능과 가장 보편적인 정보전달의 임무를 수행해온 방송의 틀에서

벗어나 방송이 정보전달의 핵심적 기능을 수행하도록 요구하게 될 것이다. 이러한 서비스가 양방향 데이터방송 또는 대화형 방송이다.

대화형방송 기술은 다양한 고부가가치 수익모델을 제공, 디지털 방송의 조기 보급과 이를 통한 국내외 시장 선점에 크게 기여할 것이며, 누구나 쉽게 사용할 수 있는 TV라는 매체를 통해 방송과 관련된 부가 정보는 물론 전자상거래, 인터넷 서비스 등을 제공함으로써 국민들의 지역간, 계층간, 연령간의 정보격차를 해소시키는 데 크게 도움이 될 것이다. 이러한 상호작용성이 증가되고 발전된 형태의 방송서비스인 대화형 서비스는 지상파 방송, 케이블 TV, 위성방송 등 방송 및 관련 산업 전반에 걸쳐 큰 파급효과를 가져올 것이다. 대화형방송 기술은 단지 단말 산업에 국한되는 것이 아니라, 오히려 디지털 방송, 디지털 콘텐츠, 인터넷 산업, 더 나아가 가정 내의 타 디지털기기들과의 네트워크화에 이르기까지 새로운 분야의 산업을 이끌어가는 실질적인 견인차 역할을 담당할 것으로 분석되고 있다. 디지털방송 환경 하에서 차세대 응용 분야로 기대되는 대화형방송 서비스에 대한 지속적인 기술개발과 국제 동향 파악 및 표준화 연구는 국제 방송 시장에서 좀 더 우세한 경쟁력을 확보할 수 있는 중요한 사안이다.

본 기고에서는 양방향 대화형방송 국내 표준 및 송수신 서비스 가이드라인을 바탕으로 한 송수신 시스템 개발, End-to-End 시스템 개발 및 최근의 정합실험에 대하여 설명하고자 한다. 세부적인 내용은 다음과 같다.

- ㅇ 양방향 대화형 송수신 시스템 기술개발
  - ACAP 기반의 PSIP 기능보안
  - ATSC ACAP 송수신 프로토콜 개발(오브젝트 캐로셀, 데이터 캐로셀)
  - OTA S/W 다운로드 송수신 기술개발
  - 상향채널 통신을 위한 송수신 통신 프로토콜 개발
- ㅇ 양방향 대화형 저작도구 및 표현미들웨어 기술 개발
  - ACAP-J 및 ACAP-X 콘텐츠 저작을 위한 저작도구(CDK) 개발
  - 양방향 콘텐츠 처리를 위한 메타데이터 개발 기술 개발
  - 생성된 콘텐츠 관리를 위한 콘텐츠 관리 시스템 개발(CLM 개념적용)
  - 양방향 정보처리를 위한 가입자관리 시스템 개발(CRM 개념적용)
  - Java TV API 개발 및 정합 실험
  - Media Play Application 개발 및 정합 실험
  - HAVi UI 개발 및 정합 실험
  - 한글 입력 및 표시 기술 개발 및 정합 실험
- ㅇ 보안/인증을 적용한 송수신 상향채널 기술 개발(T-커머스 기술개발)
  - 패킷데이터 암호화 송수신 기능 개발
  - 인증서 및 인증서 폐기 목록 처리를 위한 송수신 기능 개발
  - 공개키 기반 인증처리를 위한 송수신 기술 개발
- ㅇ 양방향 대화형 콘텐츠 개발
  - ACAP 기반 시스템 검증 및 시연용 콘텐츠 개발
- ㅇ 양방향 대화형 표준안 작성 및 송수신 정합 실험 실시
  - 대화형방송 표준안 작성 및 송수신 서비스 가이드라인 작성
  - 가이드라인을 바탕으로 한 정합실험 실시(기능 개선 및 성능 향상)

2. 양방향 대화형방송 송수신 시스템 기술개발

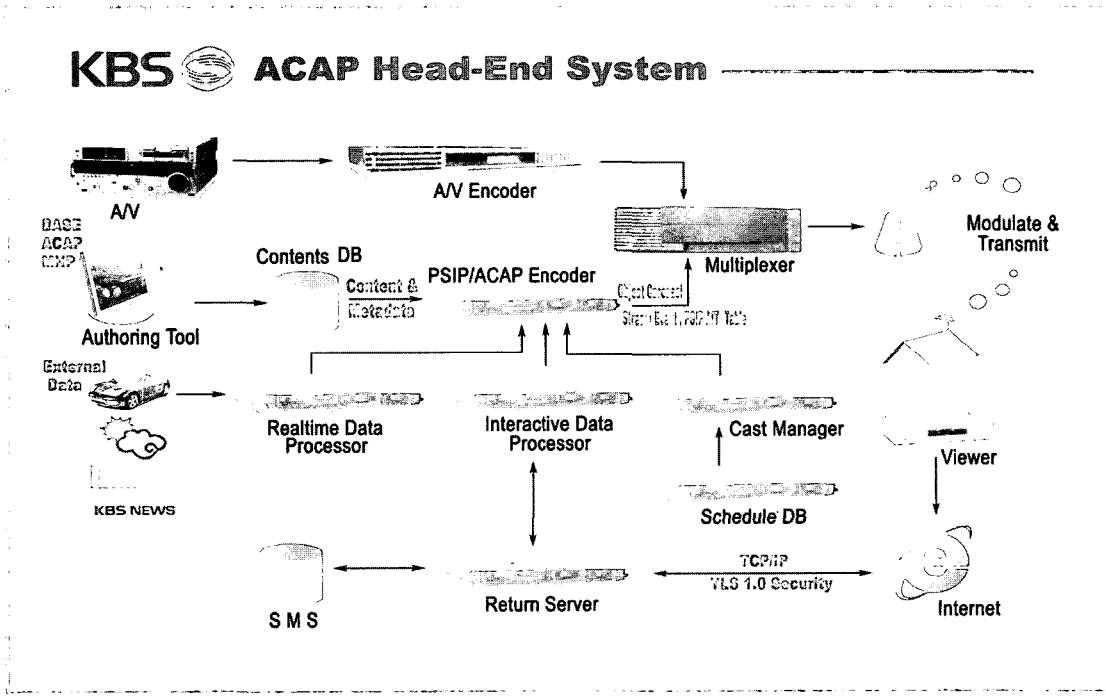
대화형방송 송수신시스템은 송출/운행 시스템, 리턴 채널시스템, 저작시스템, 정보처리시스템, 수신시스템으로 크게 나눌 수 있다. <그림 1>은 2004년 10월 현재, 온에어로 실험중인 KBS의 대화형방송 시스템이다. 구체적인 개발 내용은 다음과 같다.

1) PSI/PSIP(EPG) 부호화기

상안정성 확보는용 서비스를 위한 필수 전제조건이다. 송출되는 테이블 주기의 오차를 줄이고 장시간 운용했을 때의 메모리 누수 문제나 에러 누적 문제가 개선되었다. 또한 각 스트림의 송출 비트율을 보여주는 그래프의 응답속도를 높이고 안정성도 확보되었다. EPG 내용이 많을 때는 대역폭의 제한으로 인해 PSIP 테이블 전체가 송출되는 시간이 길어지게 되는데 이는 시청자로 하여금 필요한 정보를 얻는데 많은 시간을 기다리게 하여 불편을 겪게 할 수 있다. 따라서 PSIP 테이블을 중요도 순으로 송출주기를 조절할 수 있도록 기능이 보완되었다. 또한 새로 삽입되는 데이터 스트림에 대한 정보가 기존에 PMT에만 등록이 되는 것을 확장하여 VCT의 service location descriptor에도 충실히 등록하도록 하였고 VCT나 PMT등의 버전이 연속적으로 증가하여 STB가 오동작하는 현상도 제거하였다.

2) ACAP 데이터 송수신기 개발

데이터방송의 국제규격이 DASE에서 ACAP으



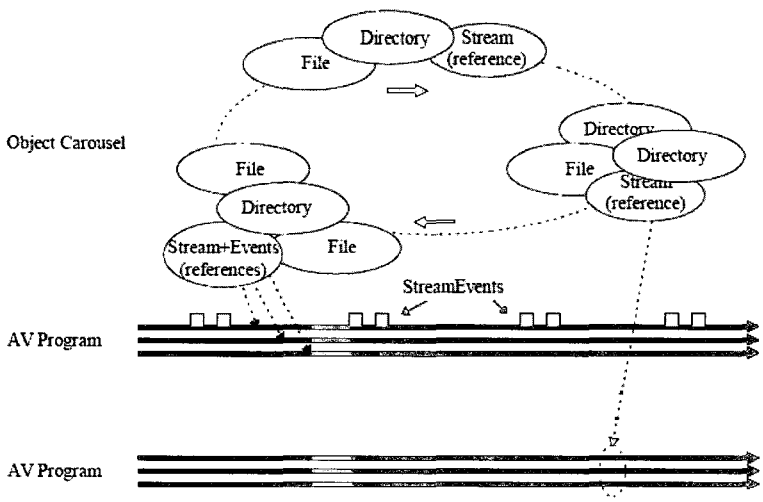
〔그림 1〕 ACAP 양방향 데이터방송 시스템 전체 구성도

로 전환되면서 송수신을 위한 프로토콜 방식도 변경되었다. ACAP 송수신 프로토콜 규격은 현재 ACAP Candidate Standard인 CS101A에 명시된 송출방식을 따르고 있고, 향후 확정될 국제표준을 바탕으로 국내 규격화도 진행 중이다. 기존의 간단한 Data Carousel 방식에서 Object Carousel이라는 좀더 구조적이면서 복잡한 구조를 갖는 방식으로 변모하였다. 이와 더불어 실시간 데이터를 전송하기 위해서 Object Carousel에서 정의하는 Stream Event Message를 Stream Event Descriptor를 포함하는 별도의 DSM-CC section으로 전송하는 방법을 채택하여 구현하였다.

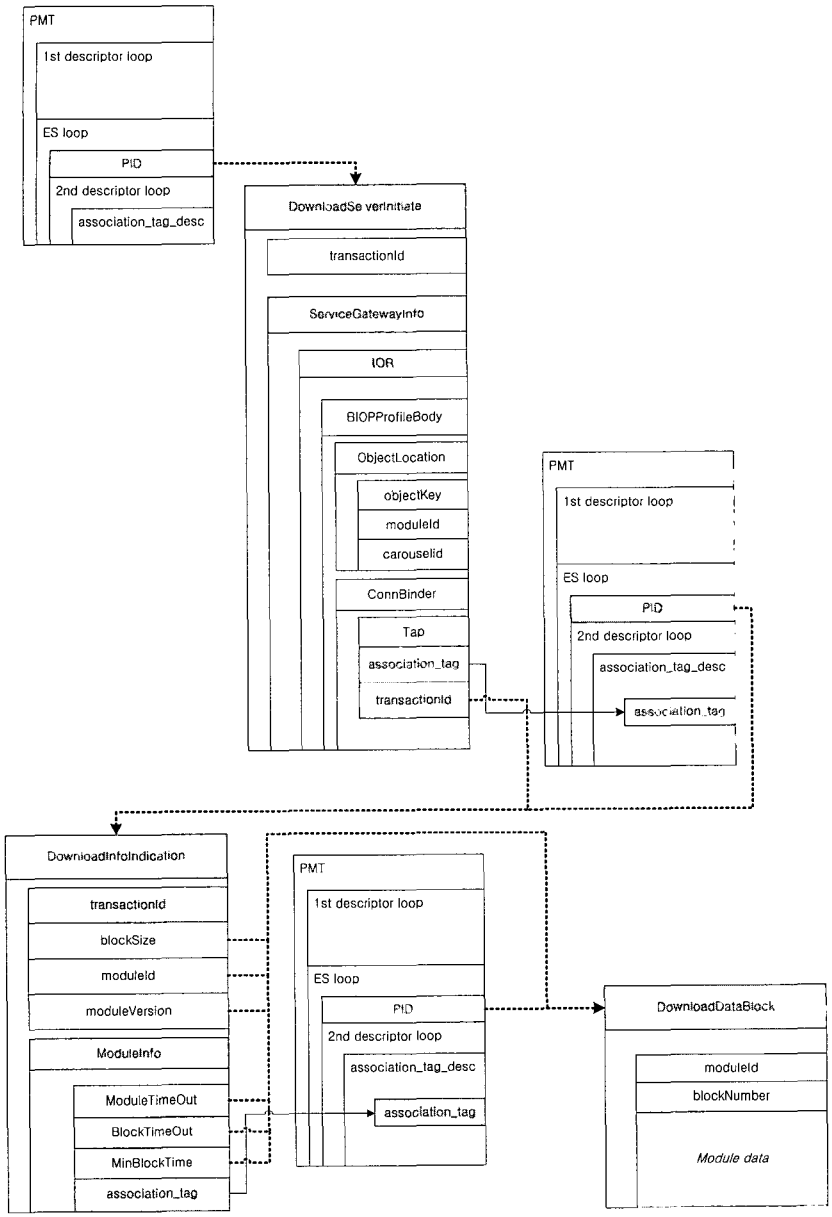
ACAP에서는 대화형방송과 시스템정보와의 바인딩을 위해서 필요한 애플리케이션 시그널링으로 AIT(Application Information Table)를 사용한다. 이를 위하여 ACAP에서 명시하고 있는 AIT에 반드시 포함되어야 디스크립터들로는 application descriptor, appliation name descriptor, transport protocol descriptor, ACAP-J application descriptor, ACAP-J application location descriptor가 있고 이러한 디스크립터 요소들을 포함시켜 AIT를 구현하였다.

또한, 애플리케이션 자체의 전송을 위하여 Object Carousel 프로토콜을 적용하여 구현하였고 이의 구성은 다음과 같이 하였다. 하나의 module단위는 10개의 object(file, directory)로 구성하였고, 10개의 module을 묶어서 하나의 group으로 바인딩하였다. 이러한 구성요소는 향후, object update정책과 연계하여 효율적 전송을 가능하도록 시나리오를 만들어 송수신 성능을 개선시킬 예정이다. DASE의 module update와 같은 방법으로 ACAP에서는 object update 기능을 추가하였다. 업데이트하는 단위가 module이 아니라 object 단위를 사용하도록 개발되었다.

이와 더불어, 실시간으로 데이터를 전송하기 위하여 Stream Event를 사용하여 인코딩하는 방법을 사용하였다. 실시간으로 전송할 요소의 데이터를 DSM-CC Stream Event descriptor 내에 넣고, 이것의 시그널링과 바인딩을 위해서 Object Carousel내에 Stream Event message를 만들어 전송하는 방법을 사용하였다. 이 밖에 애



〔그림 2〕 ACAP service 내의 Object Carousel



〔그림 3〕 수신기의 Object Carousel 분석 과정

플리케이션의 초기 맵핑을 위해서는 AIT내의 component_tag와 PMT내의 association_tag_descriptor내의 association_tag의 하위 바이트를 맵핑하도록 하였다. DVB-SI에서 정의하고 있는 stream_identifie_descriptor내의 component_tag는 사용하지 않았다.

Broadcast stream에서 전송되는 object를 처리하는 부분으로, carousel방식으로 들어오는 DSI, DII, DDB를 해석하고, IOR(Inter-Operable Object Reference)을 해석하여 object를 처리한

다. data carousel 방식으로 전송되는 데이터의 형식이 object의 집합인 경우 이 object를 해석하고 취득하며, 각각의 object는 file, directory, 그리고 stream object가 있다. <그림 2>은 object carousel의 예를 나타낸 그림이다.

Object Carousel에서 object를 얻는 방법은 IOR(Interoperable Object reference)를 이용한다. <그림 3>은 IOR을 이용하여 object를 찾아가는 것을 보여 주고 있다.

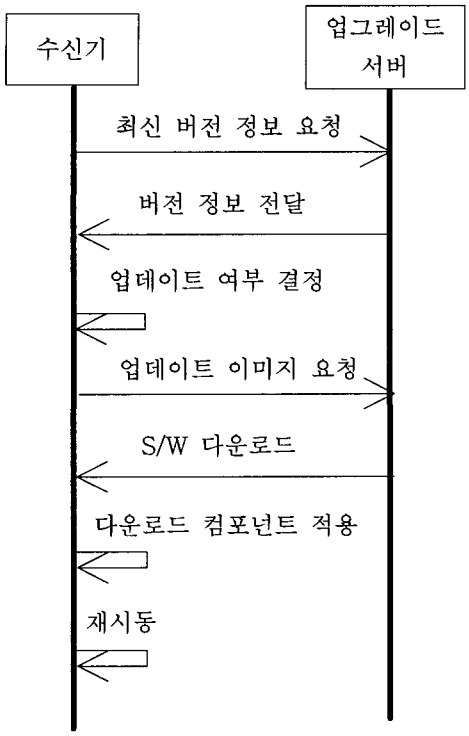
1. PMT로부터 DSI PID 획득
2. DSI 획득
3. DSI IOR 해석
4. IOR의 association_tag와 PMT의 association_tag를 비교하여 DII PID 획득
5. DII 획득
6. DII moduleInfo 해석
7. DII의 association_tag와 PMT의 association_tag를 비교하여 module PID 획득
8. Module 획득
9. Module내의 object 추출
10. 원하는 object가 존재하는 경우, object 획득
11. 원하는 object가 sub-directory에 존재하는 경우, sub-directory object의 IOR해석

3) 온에어 S/W 다운로드 송수신 기술 개발

소프트웨어 다운로드에 대한 방법으로 DVB, OCAP, ATSC 등에서 여러 가지 방법들이 제시되어 있으나, 국내에서는 향후 소프트웨어 다운로드에 대한 ATSC 규격이 완성되는대로 이 표준을 따르기로 국내 데이터방송 기술협의회에서 논의된 바 있다. 소프트웨어 다운로드와 관련하여, 현재 ATSC에서는 Candidate Standard인 CS/97을 내놓고 있다. 이에 따르면, 이전 버전의 스펙에서 1-layor, 2-layor Data Carousel을 검토하였으나 현재는 2-layor DSM-CC Data Carousel만 사용하도록 하였다. 또한, 스펙에서는 소프트웨어 다운로드의 시그널링을 위하여 VCT 내에 또 하나의 서비스 타입을 갖도록 하고 있어 별도의 virtual channel을 요구하고 있다. 향후, ATSC 표준 제정 일정과 연계하여 소프트웨어 다운로드 방식에 대한 구체적인 내용의 결정과 구현이 이루어질 것이다.

S/W다운로드는 온라인으로 소프트웨어를 업데이트 가능하도록 함으로써 수신기 문제 발생 혹은 새로운 서비스나 기능의 추가 시에 배포되어 있는 모든 수신기를 수거 또는 방문하여 A/S 해 줄 필요가 없이 온라인으로 바로 신속하게 업그레이드 할 수 있다. 이를 통해 off-line 업그레이드 시 발생하는 비용을 없앨 수 있으며, 변경사항 발생 시 신속히 대처할 수 있다. S/W 업데이트 모듈을 포함하고 있는 삼성 데이터 방송 수신기를 S/W 업데이트의 대상으로 한다. 업데이트 될 수 있는 대상은 ACAP/OCAP 데이터 방송 미들웨어, Firmware, Font ,기타 수신기 동작을 위해 필요한 소프트웨어 등이 될 수 있다.

업그레이드 시나리오에는 수동 업그레이드와 자동 업그레이드의 두 가지 방식이 있다. 수동업그레이드는 사용자가 직접 메뉴에서 업그레이드를 선택하는 것이며, 서버에 소프트웨어 업그레이드가 되었다는 정보를 인지하였거나 임의로 선택하여 수신기를 업데이트 할 수 있다. 자동업그레이드는 사용자가 수신기를 사용하지 않는 시간에 수신기가 스스로 업그레이드를 수행하는 방식이다. 수신기는 대기 모드인지를 검사한 후에 서버에 접속하여 서버의 버전이 수신기의 버전과 차이가 있는지를 확인한다. 만약 서버의 버전이 수신기의 버전과 다르면 업그레이드를 수행하고 다시 대기모드로 들어간다. 일반적인 경우에는 자동업그레이드가 수신기를 사용하지 않을 때 지



속적으로 업그레이드가 필요한 지를 검사하여 항상 최신 버전으로 유지할 수 있도록 업데이트 하게 된공동작업을 해야 할 때 새로 변경된 소프트웨어를 신다. 수동 업그레이드가 필요한 경우는 개발 단계에서 속히 적용할 때이며, 전시장과 같이 계속 수신기가 켜져 있어야 하는 경우에도 소프트웨어의 변경을 위하여 사용할 수 있다. 업그레이드를 하기 위한 프로토콜에는 TCP/IP, FTP, HTTP 등이 사용될 수 있으며, 전송되는 데이터에 오류를 검사할 수 있어야 한다. S/W 업데이트 flow는 다음과 같다.

a. 수신기에서 업그레이드 서버에 최신 버전에 대한 정보를 요청한다.
b. 서버로부터 버전 정보를 받아 수신기의 버전과 비교하여 업그레이드 여부를 판단한다.
c. 버전이 다른 컴포넌트가 있을 경우 업그레이드 하여야 할 이미지를 다운로드 받는다.
d. 다운로드가 완료되면 기존의 이미지를 새로 받은 이미지로 교체한다.
e. 수신기를 재시동하여 변경된 이미지가 적용되도록 한다.

4) 실시간/양방향 정보처리 시스템

실시간/양방향 정보처리 시스템은 DB와 리턴서버로부터 데이터를 읽어와서 애플리케이션에 적합하도록 정보처리를 한 후 데이터 인코더로 전송하는 기능을 수행한다. 실시간/양방향 정보처리 시스템은 실시간 데이터 처리기인 RDP (Real-time Data Processor), 양방향 데이터 처리기인 IDP(Interactive Data Processor), 송출수집 데이터 처리기인 GDP(Gathering Data Processor)로 구성된다.

RDP는 다양한 데이터 제공 업체와 통신하여 상대방 데이터 베이스로부터 데이터를 가져올 수 있고 자체 수동입력, 데이터 재처리 등이 가능하여 다양한 방법의 실시간 데이터방송 서비스가 가능하다. IDP는 리턴서버의 데이터 베이스와 접속하여 유효한 데이터를 실시간 제공받아 각 시나리오별 시작, 결과 데이터를 처리한다. IDP는 데이터 베이스 처리 관련 인터페이스를 일반화/고도화 하는 작업을 통해 다양한 DB환경에 능동적으로 대처하고 있다. GDP는 RDP와 IDP 출력을 입력으로 하여 전체를 취합하는 기능을 수행하는데 향후 멀티 애플리케이션 서비스를 위하여 새롭게 도입된 애플리케이션이다.

3. 양방향 데이터방송 저작도구 및 표현미들웨어 기술 개발

1) 저작도구 개발

ACAP 콘텐츠 저작 기능 개발, 양방향 콘텐츠

처리를 위한 메타데이터 구조 정의 및 생성부 개발, 양방향 모듈 자동화 및 CDK(Components Development Kits) 개념 도입 등을 목표로 하여 저작도구가 개발되고 있다.

국내 지상파 데이터방송 규격이 기존의 DASE 규격에서, 위성, 케이블 등 타매체와의 콘텐츠 호환성을 고려하여 MHP-GEM, OCAP 등을 수용한 ATSC-ACAP 방식으로의 변경이 진행 중이다. 이에 따라 향후 지상파 데이터방송 규격이 될 ACAP 방식의 콘텐츠 소스 코드를 생성하기 위한 ACAP-J 처리부를 추가 개발하였다. 또, 메타데이터 생성부는 양방향 처리용 정보 및 실시간 갱신 데이터 처리에 필요한 정보가 자동으로 생성되도록 개발되었고, 양방향 모듈 자동화 및 CDK 개념은 기존에 프로그래머가 저작도구의 코드에디터를 통하여 수동으로 프로그래밍하던 것을 자동화하기 위하여 도입하였는데, 현재 양방향 모듈 자동화를 위한 처리 구조 및 CDK 개념 도입을 위한 처리 구조를 정의한 상태이며, 양방향 모듈 중 일부에 대한 개발이 진행 중이다. 주요 개발 내용을 요약하면 아래와 같다.

- ACAP 처리부 개발
  - ACAP-J 코드 생성 모듈 추가, object carousel 처리부 개발
  - stream event 처리부 개발, MNG 대체 모듈 개발
- 메타데이터 생성부
  - 양방향 정보, ACAP-J용 정보 처리, ACAP-J 메타데이터용 DTD 개발
- CDK 기능 및 구조 정의 완료
  - CDK editor, CDK browser, CDK management engine, CDK presentation
  - CDK I/F, CDK 개발용 소스 패키지 구조, 모듈 간 상속 및 포함 관계 구조
- 양방향 처리 모듈 자동화
  - 리턴서버와의 통신 패킷 구조 정의 및 일부 모듈 자동화

2) 콘텐츠 관리 시스템 및 가입자 관리 시스템 개발

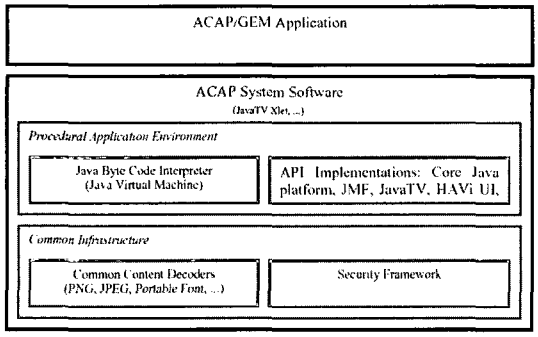
콘텐츠 관리 시스템은 생성된 콘텐츠를 효율적으로 저장/관리/공급하기 위하여 개발되었고, 가입자 관리 시스템은 가입자 정보를 효율적으로 관리하고 가입자에 관련된 양방향 정보처리를 효율적으로 수행하기 위하여 개발되었다. 이들은 현재 실험 서비스에 투입, 사용되어지고 있다. 개발된 기본적인 기능에 더하여, 올해부터는 콘텐츠 관리 시스템 및 가입자 관리 시스템에 CLM(Content Lifecycle Management), CRM(Customer Relationship Management) 개념 적용이라는 목표를 가지고 새로운 시스템 개발을 추진하고 있다.

CLM 개념을 적용함으로써, 서비스된 콘텐츠에 대한 시청자의 반응을 수집하여 콘텐츠 DB 시스템으로 관리하고 그 결과를 다양한 측정기준으로 분석하여 추후 콘텐츠 제작에 대한 기초자료를 제공할 수 있을 것이고, 가입자 관리 시스템에 CRM 개념을 도입함으로써, 가입자 정보 관리/가입자의 서비스 사용 현황과 같은 단순한 정보를 넘어선 서비스 형태 및 서비스 종료 등에 따른 보다 세부적인 데이터를 가공하여 제공하고, 차후 맞춤 고객관리와 같은 형태의 보다 나은 서비스를 고객에게 제공하고자 한다.

3) 표현 미들웨어 기술 개발

데이터 방송의 Contents가 TV Screen 상에서 제대로 실행이 되려면, 송신부에서는 Application의 Contents를 규격에 맞게 제작해야 하고, 수신부에서는 이를 해석하여 규격에 맞게 화면상에 표현해 주는 Application 동작환경을 제공해야 한다. 이 동작환경은 데이터방송 전용수신 단말기(STB)에 장착된 미들웨어(Middleware)가 담당

한다. 국내 지상파 데이터방송 잠정규격인 ACAP 규격에서는 Application 동작환경을 어떻게 명시하고 있는지 살펴보자. 아래 <그림 4>과 같이 ACAP-J System Architecture는 ACAP/GEM Application 과 이 Application을 구동하는 동작환경인 ACAP System Software (Procedural Application Environment, Common Infrastructure)로 나뉜다.



〔그림 4〕 ACAP-J System Architecture

다시 ACAP System Software는, ACAP-J Content의 제작 규격 및 보안 인증 기능을 정의하는 Common Infrastructure 와, 수신기에서 구현하여야 할 기능을 정의하는 Procedural Application Environment (절차적 어플리케이션 환경) 으로 나뉜다.

ACAP-J System Software를 구성하는 여러 요소는 크게 Common Contents 처리 모듈과 Procedural Application Environment (PAE)로 나눌 수 있는데 이를 살펴보면 다음과 같다.

가) Common contents 처리 모듈

Common contents 처리 모듈은 ACAP application을 구성하는 텍스트, 이미지, 영상, 음성 등 멀티미디어 resource 들을 처리하는 부분이다. 국내 데이터방송 표준은 ACAP 표준에서 정의하고 있는 Common contents 에 몇 가지를 더 추가하여 다음과 같은 MIME 타입을 지원하도록 하고 있다.

- ACAP-J Multimedia Contents
  - ▸ ACAP-J Application (Procedural) : Xlet(s)
- ACAP-J Monomedia Contents
  - ▸ Graphics : JPG, PNG, MPEG-I frame
  - ▸ Streaming Video/Audio MPEG-2 Transport Stream : MPEG-2 Video ES, AC-3 Audio ES
  - ▸ Non-Streaming Video / Audio MPEG-2 Video "Drip" Format, APEG-1 Audio Layers 1 and 2, audio/basic
- ACAP-J Other Contents
  - ▸ Online/Bitmap Font : TrueDoc PFR
  - ▸ Archives Format : ZIP
  - ▸ Security Metadata : application/acap-certificate, application/acap-digest, application/acap-permission, application/acap-signature
  - ▸ Text Format : dvb.utf8

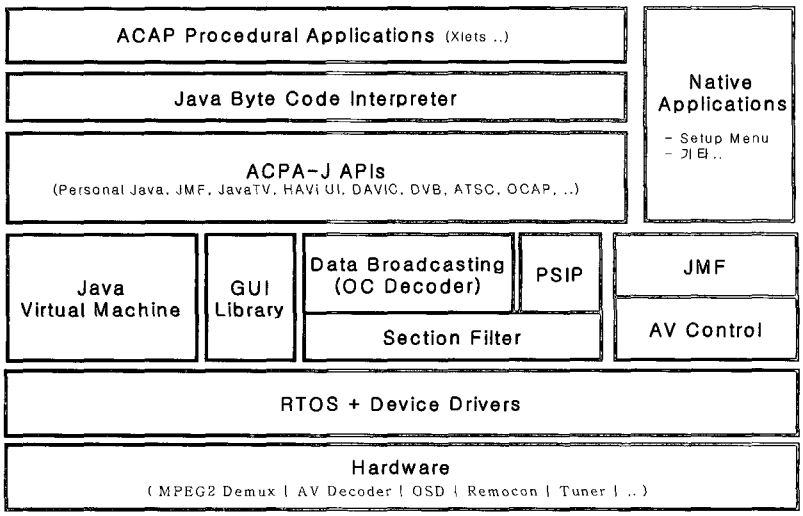
나) Procedural Application Environment (PAE)

PAE 는 Procedural Application(PA)를 구동하기 위해 수신단말 측에서 갖추어야 하는 환경이다. PA 는 pJava, JMF, JavaTV, HAVi 표준들에서 제공하는 기능들을 이용하여 application을 꾸미도록 되어 있으며 그 형태는 JavaTV 표준에서 정의하고 있는 JavaTV Xlet 의 형태를 띠고 있다. JavaTV Xlet 이란 Java application 을 방송 환경에서 사용하기 적합하도록 인터페이스를 정의한 것으로, Applet 이 Java application을 웹 환경에서 사용하기 적합하도록 개발된 것과

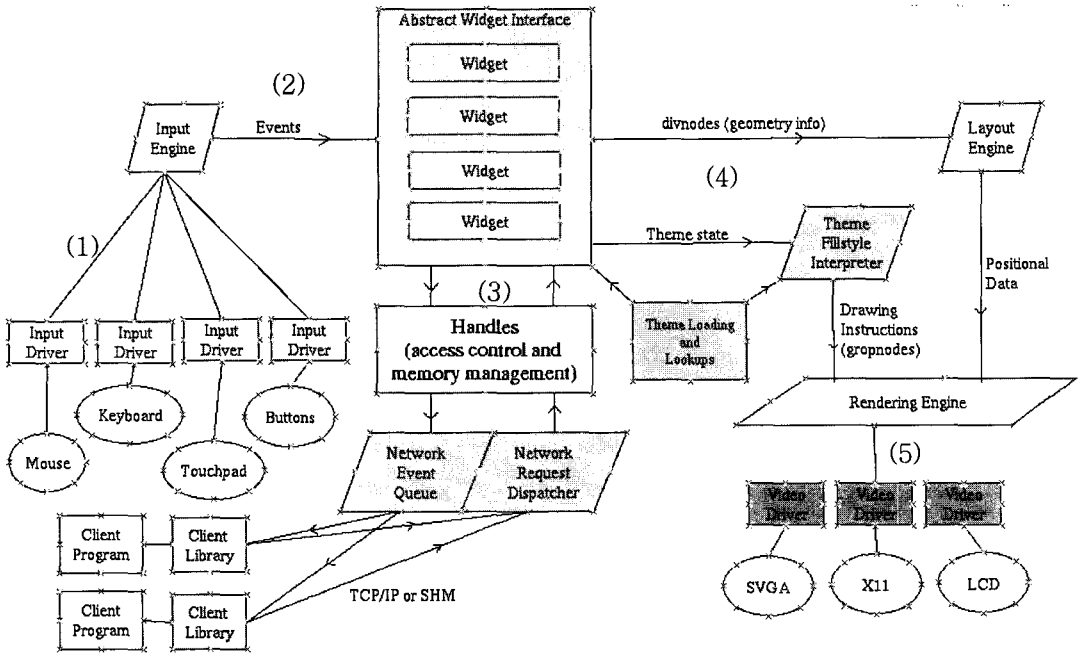
같은 이치이다. Xlet 이 일반 Java application처럼 Java Byte Code 의 형태로 방송국에서 전송되면, 이를 수신한 단말기에서는 시킬 PJava Spec.을 따르는 Java Virtual Machine 이 JavaTV API , Havi UI 등의 PAE 구성 요소들을 참조하여 Xlet 을 실행한다. 대화형 수신 단말기가 PAE(Procedural Application Environment) 를 구성하기 위해 갖추어야 할 API 들은 다음과 같다.

- Personal Java (PJAE 1.2A) : 임베디드 환경에서의 Java Virtual Machine 사양이다. Xlet 코드를 실질적으로 해석하고 실행한다.
- Java Media Framework (JMF 1.0) : 추상적으로 Media를 제어하는 틀을 java 언어로 작성한다.
- Java TV (JavaTV 1.0) : 일반적인 TV 및 STB 이 구현해야 할 Framework (틀) 을 SUN 사가 Java 언어를 이용하여 제안한 것이다. DASE Spec. 에서는 JavaTV API 라는 통일된 규격을 두어 각 STB 업체가 API 들을 자신들의 STB 환경에 맞게 구현하도록 하고 방송사들 역시 그 API 만을 사용하여 Content를 작성한다.
- HAVi Level 2 UI (HAVi L2 UI 1.0.1) : Application 이 사용하는 UI 역시 JavaTV API 의 경우와 마찬가지로 통일된 규격이 필요하다. HAVi 는 원래 홈 네트워크를 위한 표준인데 ACAP Spec. 에서는 이 중에서 UI 와 관련된 부분만을 사용하고 있다. HAVi UI 역시 Java 언어로 작성한다.
- DAVIC 1.4.1 Media/Resource Services
- ACAP Specific APIs

아래 <그림 5>은 ACAP-J 기반의 대화형 단말기의 소프트웨어 구성도이다. 이 그림에서 Hardware 부분과 Native Applications를 제외한 부분이 대화형 서비스를 지원하기 위한 실질적인 소프트웨어 모듈들이고 이들이 하드웨어 및 애플리케이션과 유기적으로 결합되어 있다. 소프트웨어 모듈은 그림 에서처럼 OS 및 디바이스 드라이버 모듈, 데이터 방송 및 PSIP 데이터를 관리하는 모듈, Graphic을 담당하는 GUI Library,



〔그림 5〕 ACAP-J 기반의 대화형 iMS 단말기의 소프트웨어 구조



〔그림 6〕 그래픽 라이브러리의 이벤트 처리

Java TV를 비롯한 ACAP-J API를 구현하기 위한 모듈, ACAP 애플리케이션을 수행하기 위한 JavaVM 등으로 구성된다.

ACAP-J 표현미들웨어란, Common Contents와 ACAP-J Applications을 해석하여 TV 화면에 표현해 주기 위한 소프트웨어라고 정의할 수 있다. 위 <그림 5>에서와 같이 ACAP-J 기반의 표현미들웨어와 관련한 소프트웨어 모듈은 크게 3영역으로 나눌 수 있다.

다) 그래픽 라이브러리 (GUI Library)

데이터방송 표준에서 그래픽 라이브러리에 대해서는 특별한 제한을 두고 있지는 않다. 그러나 기본적으로 그래픽 위젯(Widget)이 투명하게 그려질 수 있어야 하고, JPEG, PNG (단, MNG는 ACAP-X 영역이므로 제외)를 처리할 수 있어야 한다. 그래픽 라이브러리가 이벤트를 처리하는 과정은 <그림 6>과 같다.

(1) 입력 디바이스로부터 이벤트를 받아들인다.
(2) 이벤트를 해당 위젯(widget)에 전달한다.
(3) 이벤트를 처리하여 위젯(widget)의 상태를 변화시킨다.
(4) Layout이나 look에 변화가 있으면 Rendering Engine의 해당 함수를 호출함.
(5) 해당 그래픽 디바이스에 변화를 반영한다

라) Java Virtual Machine (JVM)

Xlet 애플리케이션을 구동하기 위해서는 Java VM(가상머신: Virtual Machine)이 필요하다. ACAP-J 규격에 따라 Personal Java를 사용한다. Java VM은 class loader, runtime data structures, execution engine으로 구성된다.

라) ACAP-J APIs

데이터 방송 및 PSIP 모듈에서 수신한 데이터

를 사용하여 JavaTV와 HAVi UI (User Interface) 등을 구현하는 모듈이다. JavaTV API는 일반적인 DTV STB이 갖추어야 할 기능들의 전체적인 구조와 함수 흐름을 제공하는 API로서, 크게 Xlet 애플리케이션을 처리하는 패키지, PSIP 데이터를 처리하는 패키지, 기타 유틸리티 패키지로 나눌 수 있다.

HAVi UI는 "TV-friendly" User-Interface의 틀을 제공하고 특별히 Consumer Electronic Device에 적합하도록 디자인된 사용자 인터페이스이다. 즉 HAVi User-Interface는 Java로 작성된 Application이 사용자로부터 입력을 받아들여 스크린에 표시할 수 있도록 해준다. HAVi UI의 API는 org.havi.ui, org.havi.ui.event package로 구성되어 있다. 본 대화형 iMS STB 상에서의 HAVi UI의 구현은 HAVi 1.1 spec의 HAVi Level 2 User Interface에 부합되도록 이루어졌다. ACAP-J 에 포함된 API들은 다음과 같다.

- JavaTV API 1.0
- JMF (Java Media Fr amework) 1.1
- HAVi(Home Audio Video interoperability) UI(User Interface) 1.0
- DAVIC(Digit al Audio VIsual Council) 1.4.1 Part9 (일부분)
- 기타 ATSC/ACAP-J 관련 특정 APIs

JavaTV는 방송 네트워크와 TV 수신기를 위한 네트워크 독립적인 응용 환경이며, JavaTV API는 Java 플랫폼 상에서 Java로 향상된 (enhanced) 양방향 콘텐츠를 위한 확장 표준이다. JMF는 표준 Java API의 일종으로 동영상, 음성과 같이 시간의 흐름에 연관되어 진행되는 정보의 표현을 제어하기 위한 API이다. HAVi UI는 홈 네트워크 상에 연결된 비디오, 오디오 기기들 간의 통신과 제어를 위한 규격의 이름이다. 이 표준에서는 DTV를 이용해서 다른 비디오, 오디오 기기를 제어하기 위한 사용자 인터페이스 화면을 시청자에게 보일 수 있도록 Java로 된 사용자 인터페이스 규격을 정하고 있다. 그 외 DAVIC 1.4의 일부분을 API로 사용하도록 되어 있으며, ATSC/ACAP-J 관련 특정 API는 JavaVM 위에서 정의되고 있으며, Personal Java 1.2의 일부분이기도 하다.

4. 보안/인증을 적용한 송수신 상향채널 기술개발

1) 리턴채널시스템

리턴채널 표준은 DASE와 ACAP 표준 변화에도 달라진 것이 없다. 두 가지 표준 모두 ATSC에서 표준으로 정하고 있는 A/96을 공통으로 채택하고 있기 때문이다. 리턴채널 시스템도 기존의 리턴데이터수집부, 리턴서버, SMS(가입자관리서버) 구성을 그대로 유지하며 구조적으로 크게 변화된 바는 없다. 하지만, 시범서비스에 사용된 T-commerce, T-mobile, T-poll 콘텐츠를 위해 기본 프로세서에 기능이 추가되었다.

채널보안 관련해서는 리턴서버는 TLS 1.0 프로토콜과 128비트 SEED 대칭키 암호화 알고리즘을 지원하고 있으며 수신기에서도 TLS1.0 표준 및 SEED를 위한 표준 JSSE provider 형태로 개발하고 있으며 개발된 내용은 상호 정합실험을 통해 맞춰가고 있다. SEED 암호화를 위한 cipher suite의 이름으로는 ACAP_RAS_WITH_SEED_CBC_SHA로 정의해서 사용하고 있으며 실제 헥사 값은 "0xff, 0x01"로 정의하였다. 채널보안을 수행하기 위해서는 방송국에서 데이터방송용 ACAP 콘텐츠를 온에어 채널로 내려보낼 때 루트인증서를 같이 내려보낸다. 이때 인증서 파일의 이름은 atsc.tls.organisation_id.application_id.x 와 같은

형태이다. 이때 organisation_id와 application_id는 AIT내의 해당 애플리케이션 루프에 들어있는 내용과 일치해야 한다. 셋톱박스에서는 이러한 루트인증서 파일을 확인하고 SSL 소켓통신을 시도할 때 미들웨어에서 TLS 1.0 프로토콜에 따라 서버로부터 서버 인증서를 요청하고 SEED 대칭키 암호화 알고리즘에 사용될 키를 RSA 프로토콜로 상호 공유한다. 이때 전자서명 값과 같이 다이제스트에 사용되는 알고리즘은 SHA 방식을 사용한다.

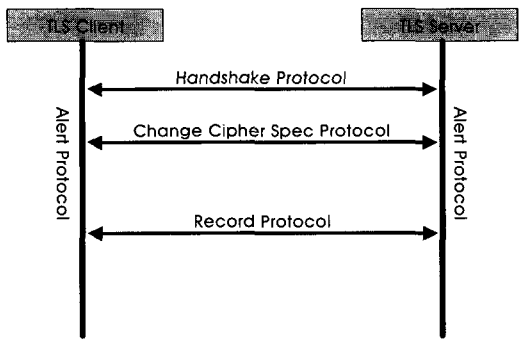
본 개발에서는 보안/인증을 적용한 상향채널 송신데이터처리 기술을 개발하였다. 데이터 방송 규격에 따라, 보안/인증 적용한 데이터 처리는 TLS 기반의 JSSE를 이용해서 처리된다. 따라서, 본 개발에서는 JSSE 스펙 1.0.2를 기반으로 정의된 API를 개발하고, 데이터 방송용 미들웨어 스펙에 따른 최적화와 커스터마이징을 수행하였다. 또한 국내 보안 규격에서 명시하는 국내 암호화 알고리즘 적용을 위해서, SEED 기반 cipher suite를 정의하고, 해당 cipher suite가 JSSE 내에서 지원될 수 있도록 하였다. 상세한 기술 개발 내용은 다음과 같다.

2) TLS 프로토콜

데이터 방송 리턴 채널 보안 메커니즘으로 규정되어 있는 JSSE는 IETF RFC 2246으로 표준화되어 있는 TLS(Transport Layer Security) 1.0 명세에 대한 자바 API 이다. 현재 TLS는 데이터 방송을 비롯하여 다양한 응용 분야의 채널 암호화에 널리 사용되는 표준 명세이다. TLS는 1994년 Netscape 사가 제안한 전송 계층 보안 프로토콜인 SSL(Secure Socket Layer)의 표준화 결과이며, TLS 버전 1.0은 SSL 버전 3.1과 동일한 동작 구조를 갖는다. TLS 구조의 주요 기능 및 설계 목표는 다음과 같이 요약된다.

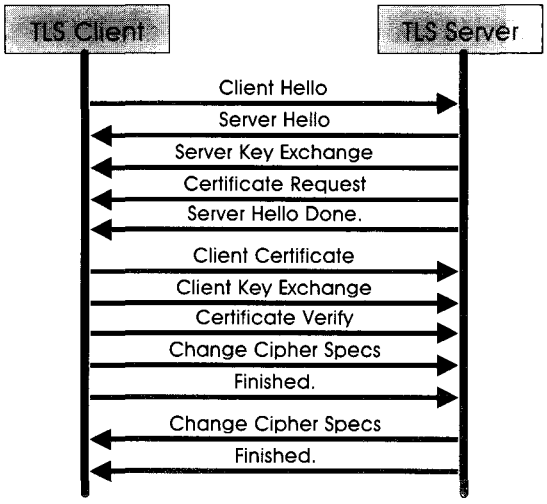
- ▶ 보안성 (Security) : 비밀성, 무결성, 강력한 인증 등 안전한 암호 통신을 위한 기본 조건을 기반으로 보안성을 제공한다.
- ▶ 상호운용성 (Interoperability) : 접속, 프로토콜 협상, 키관리 및 암호 통신에 대한 전반적인 프로토콜 표준화를 통하여 응용 프로그램 간의 상호 운용성을 제공한다.
- ▶ 확장성 (Extensibility) : 다양한 응용 환경에서의 요구사항을 수용하기 위하여 암호, 키관리 및 해쉬 알고리즘 등에 대한 확장성을 제공한다.
- ▶ 효율성 (Efficiency) : 응용 프로그램의 채널 사용 형태에 따른 효율적인 세션 처리 구조를 포함하여 상대적인 효율성을 제공한다.

TLS 표준 명세는 다음의 네가지 프로토콜로 요약될 수 있다. 각 단계별 진행은 <그림 7>과 같다.



〔그림 7〕 TLS 프로토콜 구성

- ▶ Handshake Protocol : 초기 협상 프로토콜
- ▶ Change Cipher Spec Protocol : 사용될 암호 알고리즘 변경 프로토콜
- ▶ Alert Protocol : 주요 이벤트 처리 프포로톨
- ▶ Record Protocol : 실제 메시지 암호 통신 프로토콜



〔그림 8〕 Handshake 프로토콜

TLS를 구성하는 프로토콜 중 실제 응용환경에 적용 시 고려 대상이 되는 프로토콜은 Handshake 프로토콜이다. Handshake 프토토콜의 수행 단계는 <그림 8>와 같다. Handshake 프로토콜은 초기 접속 과정, 인증서에 기반한 인증 과정, 가용한 암호 알고리즘 조합(Cipher Suite) 협상 과정등을 포함한다.

TLS Handshake 프로토콜이 제공하는 인증 방식은 응용 환경의 요구사항에 따라 다음의 세 가지 인증 모드(mode)으로 구분할 수 있다.

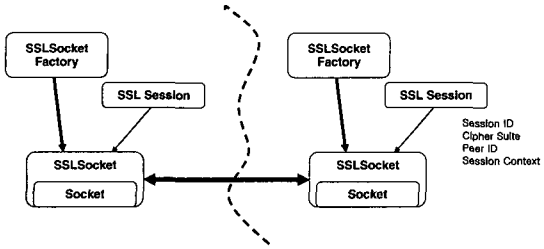
- 상호 인증 모드 (Mutual Authentication mode)
- 서버 인증 모드 (Server Authentication mode)
- 익명 모드 (Anonymous mode)

상호 인증 모드는 통신에 참가하는 쌍방이 서로 인증을 수행하는 방식이며, 이를 위하여 상호간에 인증을 위한 인증서를 제시한 후인증서를 통한 인증을 수행하는 방식이며, 이 경우 응용 프로그램은 전체적인 보안성을 TLS 모듈에 의존한다. 서버 인증 모드는 클라이언트에 대한 인증을 생략하고 서버 측에 대한 인증만을 수행하는 방식으로서, 서버에 대한 신뢰가 중요시되는 환경에 주로 적용된다. 서버 인증 모드의 사용 시 클라이언트의 신뢰가 요구되는 경우에는 별도의 클라이언트 인증 절차를 필요로 한다. 익명 모드는 별도의 인증 절차 없이 키교환 및 단순 채널 암호화만을 수행하기 위한 방식으로서, 클라이언트와 서버 간에 이미 상호 신뢰가 이루어진 경우, 또는 별도의 일방향/쌍방향 인증 방식을 응용 수준에서 제공하고 있는 경우 사용되며, TLS 표준 명세에서는 권하지 않는 방식이다. 데이터 방송 표준 명세에서는 TLS 통신 시 서버 인증 모드를 사용할 것을 명시하고 있다.

3) JSSE 1.0.2

데이터 방송 표준 명세 및 플랫폼은 자바 기반한 인터페이스를 명시하고 있으며, 리턴 채널 보안과 관련하여 MHP 1.0.2의 11.8.2절에서는 JSSE API를 제공할 것을 규정하고 있다. JSSE(Java Security Socket Extension)는 SSL 3.0 및 TLS 1.0을 제공하기 위한 자바 API로서 TLS가 규정하는 채널 보안기능을 제공한다. JSSE는 JCA(Java Cryptography Architecture)의 설계 규칙에 따라 사용하기 위한 API로서 그 구현이 독립되어 있으며 JCA처럼 Provider를 사용해 구현부를 지정하고 표준 API를 사용하여 SSL/TLS 통신을 수행할 수 있다. MHP 1.0.2 명세는 JSSE 1.0.2 명세를 따르도록 규정하고 있으며, JSSE 1.0.2 명세는 다음과 같이 요약될 수 있다.

JSSE 1.0.2는 PersonalJava 3.1과 128bit의 블록 암호화 알고리즘을 지원하며 javax.net, javax.net.ssl, javax.security.cert의 세가지 패키지로 구성되어 있다. 기존 Socket을 싸고 있는 SSLSocket을 이용하여 SSL/TLS 통신을 하게 되며, Socket Factory라는 클래스를 통해



〔그림 9〕 JSSE 동작 구조

SSLSocket을 생성하게 된다. SSLSocket은 SSLSession을 가지고 있으며 SSLSession에는 SSL/TLS 통신에 필요한 보안 정보가 들어가게 된다. JSSE 동작 구조는 <그림 9>와 같이 표현된다. 본 개발에서는 위에서 명시한 JSSE 스펙을 준수하는 JSSE API를 개발하였다. 단, 데이터 방송 규격에서 명시한 바, 서버쪽 기능에 대한 구현은 최적화 차원에서 삭제하도록 하였다. 구현된 JSSE API는 <표 1>과 같다.

4) 최적화

본 개발에서는 데이터 방송용 STB와 리턴 채널 서버 간에 보안에 민감한 정보를 안전하고 효율적으로 전달하기 위하여 리턴 채널 보안 모듈의 최적화를 수행하였다. 최적화 내용은 다음과 같다.

- ▶ 리턴 채널 보안 모듈의 최적화
- ▶ 기존 JSSE 모듈은 IETF RFC 2246에서 규정하는 TLS 1.0 표준에 명시된 모든 명세를 포함하기 때문에 데이터 방송 표준이

〈표 1〉 구현된 JSSE API

패키지	클래스
javax.net	
	SocketFactory
javax.net.ssl	
	HandshakeCompletedListener
	SSLSession
	SSLSessionBindingListener
	SSLSessionContext
	HandshakeCompletedEvent
	SSLSessionBindingEvent
	SSLSocket
	SSLSocketFactory
	SSLException
	SSLHandshakeException
	SSLKeyException
	SSLPeerUnverifiedException
	SSLProtocolException
javax.security.cert	
	Certificate
	X509Certificate
	CertificateEncodingException
	CertificateException
	CertificateExpiredException
	CertificateNotYetValidException
	CertificateParsingException

〈표 2〉 ACAP 요구 Cipher Suites

Cipher suite	키교환	암호화	해쉬
TLS_RSA_WITH_NULL_MD5	RSA	None	MD5
TLS_RSA_WITH_NULL_SHA	RSA	None	SHA-1
TLS_RSA_WITH_DES_CBC_SHA	RSA	DES CBC	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES(EDE) CBC	SHA-1

명시하는 구현 제외사항에 따른 최적화를 수행하였다.

- 성능 측면의 제약이 존재하는 STB 상에서 사용자 응답 시간을 보장할 수 있도록 JSSE 모듈의 최적화를 수행하였다.
- 데이터 방송 표준 명세가 제시하는 필수 Cipher Suite 만을 제공할 수 있도록 알고리즘 최적화를 수행하였다.
- 국내향 데이터 방송 표준 명세인 ACAP의 적용 시 국내 표준 블록 암호 알고리즘인 SEED가 사용될 수있도록 최적화를 수행하였다.

5) ACAP 및 MHP 표준 명세 수용

ACAP 표준 명세의 리턴 채널보안 내용은 MHP 표준 명세에서 기술하고 있는 리턴 채널 보안 관련 규정을 따른다. 따라서, 본 개발에서는 구체적인 Cipher Suite 요구사항을 제외한 JSSE 구현 요구사항은 MHP 1.0.2 표준 명세를 기반으로 최적화를 수행하였다.

MHP 1.0.2 명세의 12.10.1 절에서는 STB를 위한 클라이언트 모듈의 최적화를 위해 다음의 TLS 기능 모듈을 제외시킬 것을 명시하고 있다. 따라서, 본 개발에서는 다음의 제외 사항을 고려한 최적화를 수행하였다.

- TLS 프로토콜의 서버 동작 부분
- SSL 3.0 하위 호환 처리 부분
- TLS 클라이언트 인증 처리부분

데이터 방송 표준 명세에서는 각 표준에 따른 Cipher Suite들을 명시하고 있다. 각 표준 명세에서는 STB의 메모리 공간 제약 사항을 고려하여 최소한의 알고리즘들을 구현 조건으로 제시하고 있으며, 이를 통한 Cipher Suite 협상 간소화를 유도하고 있다. 본 연구에서 참조한 ACAP CS/96 표준 명세를 통하여 ACAP이 명시하는 필수 Cipher Suite은 <표 2>와 같다.

6) SEED 암호 알고리즘 적용

국내 보안 통신 환경에서는 메시지 암호화에 직접 적용되는 대칭키 방식의 블록 암호 알고리즘에 대하여 국내에서 설계된 알고리즘을 사용하도록 권고하고 있다. 특히, 금융 거래를 포함하는 전자상거래 환경에서는 금융감독원의 해당 규정에 의하여 SEED 암호 알고리즘을 사용하여야 하며, 본 개발에서 목적으로 하는 리턴 채널역시 전자상거래에 사용되기 위해서는 반드시 국내 국가기관에서 설계한 암호 알고리즘을 사용하여야만 한다. 그러나, IETF에서 권고하는 TLS 1.0 표준 명세에는 국제적으로 널리 사용되는 암호 알고리즘만을 조합하여 Cipher Suite을 제시하고 있으며, 국내에서만 사용되고 있는 SEED 알고리즘을 포함하는 Cipher Suite은 현재까지 표준화되어 있지 않다.

따라서, 향후 원활한 리턴 채널 이용을 위하여 국내 TLS 통신 환경을 위한 Cipher Suite의 표준화가 요구되며, SEED 알고리즘을 포함하는 TLS 표준 Cipher Suite의 제정을 통하여 데이터 방송 장비 제조사 간에 표준기반 SEED 통신을

수행할 수 있도록 해야만 한다. 본 개발에서는 한국향 데이터방송 표준으로 사용될 SEED 기반 cipher suite를 정의하였다. 이에 대한 논의는 데이터방송 기술 협의회를 통하여 이루어졌다. 확정된 SEED 기반 cipher suite의 정의는 ACAP_RSA_ WITH_SEED_CBC_SHA이다.

이 cipher suite는 블록 암호화 알고리즘으로 SEED를 사용하며, 해쉬 알고리즘으로는 SHA를, 키교환 알고리즘으로는 RSA를 이용한다. 해쉬 및 키교환 알고리즘의 경우, 국내향 알고리즘도 존재하나, 국내에서 조차도 일반적으로 사용되지 않으므로 가장 일반적인 알고리즘은 RSA와 SHA를 이용하도록 하였다. 해당 cipher suite에 대한 hex value는 0xff, 0x01로 결정하였다.

7) JSSE-미들웨어 간 연동

최적화 개발의 고려 대상이 되는 데이터 방송 표준 명세들은 기 정의된 보안 표준인 TLS(JSSE)를 근간으로 하는 리턴 채널 보안 방식을 제시하고 있다. 하지만, MHP 표준은 JSSE API가 고안된 배경인 웹 동작 환경과 상이한 데이터 방송 응용프로그램 운용 환경을 고려하여 별도의 서버 인증 메커니즘을 규정한다. 일반적인 웹 운용 환경에서의 JSSE는 클라이언트 플랫폼에 기 설치되어 있는 웹 브라우저라는 단일 응용 프로그램과 웹 서버와의 안전한 통신을 전제로 하며, 웹 브라우저가 신뢰하는 인증서(Trusted Anchor or Trusted Certificate)를 기반으로 하는 서버 인증을 수행한다.

그러나 데이터 방송 응용 프로그램 운용 환경에서는 다양한 종류의 응용 프로그램이 동적으로 전송되어 STB 상의 JSSE 모듈을 사용하게 되므로, 응용 프로그램마다 서로 다른 루트 인증서를 신뢰하는 다중 응용 환경을 가정한다. 따라서, 기존 JSSE 구현과 달리 응용 프로그램의 성격에 따른 신뢰 인증서 목록의 처리가 요구되며, 이때, 응용 프로그램의 서버 인증 방식을 파악하기 위해 미들웨어와의 연동 개발이 필요하다. 본 개발에서는 이를 위해서 다음과 기능을 개발하였다.

- ▶ JSSE-미들웨어 간 연동 기능
- ▶ TLS 초기 통신 시 수행되는 서버 인증절차 중 TLS 루트 인증서의 유무에 따른 인증 처리를 위한 미들웨어 연동 기능
- ▶ 데이터 방송 동작 환경을 고려하여 응용 프로그램에 종속된 TLS 루트 인증서의 처리를 위한 미들웨어 연동 기능

신뢰 인증서 목록의 처리와 관련하여 요구되는 리턴 채널 보안 모듈 및 미들웨어 준수 사항은 MHP 1.0.2 명세의 12.10.3 절에 언급되어 있으며, 해당 규정은 다음과 같이 요약된다.

(1) 응용 프로그램이 TLS 루트 인증서 없이 전송되었을 경우 :

- ▶ 표준 JSSE API를 이용한 TLS 프로토콜 수행
- ▶ JSSE 내에서 별도의 서버 인증을 수행하지 않음.
- ▶ 응용 프로그램이 별도의 방법을 통해 서버 공개키 및 서버 이름을 기반으로 인증 가능(JSSE 및 미들웨어 요구사항은 아님)

(2) 응용 프로그램이 TLS 루트 인증서들을 포함하여 전송되었을 경우 :

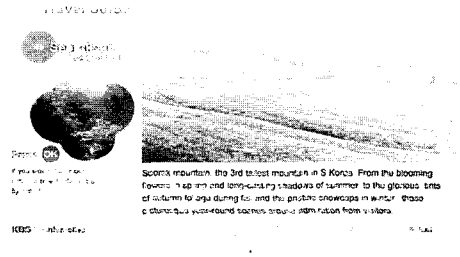
- ▶ 응용 프로그램이 제시한 TLS 루트인증서를 이용한 서버 인증서 검증 처리 수행

본 개발에서는 위의 규정을 만족시키도록 JSSE 수행 방식을 변경하였다.

5. 양방향 대화형 콘텐츠 개발

ACAP 기반 송출 시스템 및 리턴처리 시스템

을 검증하고, ACAP 수신기와의 정합 실험과 외부 전시를 위하여 실험용 콘텐츠 개발하였다. 개발된 콘텐츠를 이용하여 실제로 사용하기에 무리가 없도록 시스템 및 수신기를 실험하며 수 차례 개선과정을 거쳐, 양방향 실험 방송을 성공적으로 실시할 수 있었다. 실험용 콘텐츠로는 '뮤지션', '한국의 사계' 등의 방송프로그램에 해당하는 콘텐츠를 제작, NAB2004에 지상파 ACAP 콘텐츠로는 최초로 전시하였으며, KOBA2004에도 전시하여 많은 관심을 모았다. 이 콘텐츠는 DASE에서 ACAP으로 규격이 바뀌면서 변경된 소스코드를 전반적으로 실험하기 위하여, 실시간 처리, 리턴 처리 등이 포함된 다양한 기능들로 구성하였는데, 아래에서 개발된 '뮤지션', '한국의 사계' 콘텐츠에 대하여 간략하게 기술한다. 이러한 다양한 메뉴들을 통해 발생한 이슈들은 '지상파 데이터방송 정합가이드라인' 수정, 보강을 위한 기초자료로 사용된다. 아래 <그림 10>, <그림 11>은 실험 콘텐츠 화면이다.



〔그림 10〕 '한국의 사계' 화면

〔그림 11〕 '더 뮤지션' 화면

ㅇ 한국의 사계
- 대상 A/V: 다큐멘터리 '한국의 사계'
- '뮤지션' 메뉴: 스타 소개, 오늘의 프로그램, 앨범 소개
- '시청자 투표' 메뉴: 만나고 싶은 음악 장르에 대한 시청자 투표
- '메시지 존' 메뉴: 시청자 입력 메시지를 송출하는 주는 단문 서비스
- '뮤직 스토어' 메뉴: DVD 구매, 스타 소장품 경매

ㅇ 뮤지션
- 대상 A/V: 뮤직 '더 뮤지션' 윤희정 편
- '한국의 사계' 메뉴: 봄/여름/가을/겨울
- '한국의 미' 메뉴: 단청/고려청자/금관/하회탈/경회루
- '여행 가이드' 메뉴: 설악산/한라산/한려해상/지리산/경주 등 여행정보 받기
- '퀴즈 & 게임' 메뉴: 이벤트 퀴즈, 매칭 게임/사다리 게임

6. 양방향 대화형 표준안 작성 및 송수신 정합 실험 실시

현재 수행할 수 있는 양방향 대화형 서비스는 그 서비스 내용에 따라 독립형과 연동형으로 분류할 수 있고, 서비스의 리턴채널 사용 여부에 따라 단방향과 양방향으로 분류할 수 있다.

1) 연동형 서비스

연동형 서비스는 데이터방송 application 의 내용이 현재 방송 내용과 연동되어 있는 서비스를 의미한다. 이 서비스를 통해 사용자는 현재 방송 내용과 관련된 다양한 부가정보를 얻을 수 있고 리턴채널을 이용한 양방향 서비스인 경우에는 시

청자가 방송과 연계하여 실질적으로 인터랙티브하게 방송에 참여하거나, 경매, 옥션 등의 이벤트에 참여할 수도 있다.

〔그림 12〕 '한국의 사계' 화면

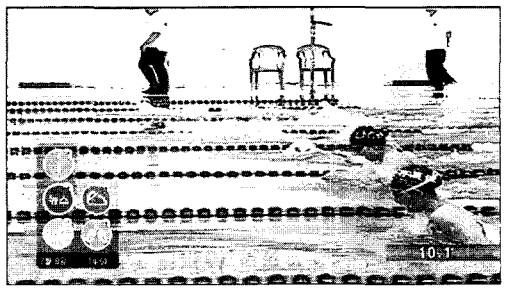
〔그림 13〕 '한국의 사계' 화면

위 화면들은 KBS에서 제작한 연동형 서비스를 데이터방송 수신 전용 셋탑박스(STB)에서 수신하여 ACAP-J 표현 미들웨어가 처리한 화면이다. 수신 셋탑박스에서 사용된 ACAP-J 표현미들웨어 관련 API들은 아래와 같다.

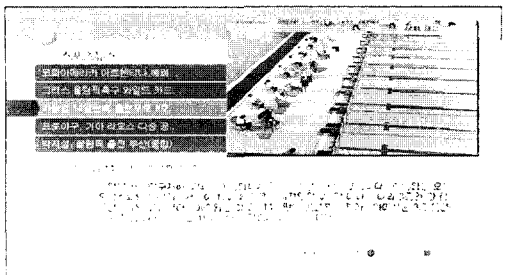
- Application lifecycle control APIs : org.dvb.application, javax.tv.xlet,
- Graphics APIs : org.havi.ui, org.havi.ui.HComponent,org.havi.ui. HContainer java.awt, java.awt.Imag, java.awt.Color, org.dvb.ui.DvbColor org.havi.ui.HScene, org.havi.ui.HVisible, javax.tv.graphics org.havi.ui.event ..
- User input event handling APIs : org.dvb.event, org.davic.resources.ResourceServer ..
- Java Media Framework (JMF) & Media control APIs : java.media, javax.media.Manager, javax.media.MediaLocator, org.davic.media.MediaLocator, javax.tv.locator.Locator ..
- JavaTV APIs : javax.tv.service.Service, javax.tv.locator.Locator, org.davic.mpeg, java.io.File, java.lang.String, Java.util.Vector, java.rmi.Naming ..

2) 독립형 서비스

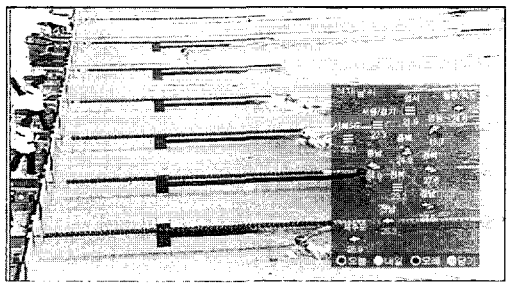
독립형 서비스는 데이터방송 application 의 내용이 현재 방송 내용과 관련 없는 서비스를 의미한다. 이 서비스에서 제공하는 정보는 주로 뉴스나 날씨, 교통, 온라인게임 등의 생활, 취미, 오락 정보로서 방송을 시청하면서도 언제든지 이런 정보들을 손쉽게 얻을 수 있다.



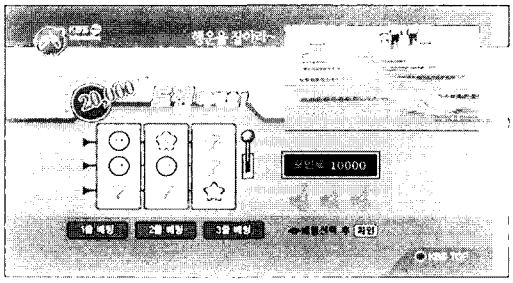
〔그림 14〕 독립정보 서비스 첫 화면



〔그림 15〕 독립정보 서비스 〈뉴스〉



〔그림 16〕 독립정보 서비스 〈날씨〉



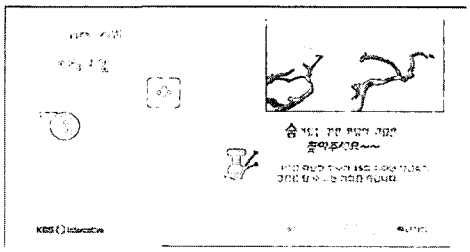
〔그림 17〕 독립정보 서비스 〈게임〉

수신 셋탑박스에서 사용된 ACAP-J 표현미들웨어 관련 API들은 아래와 같다.

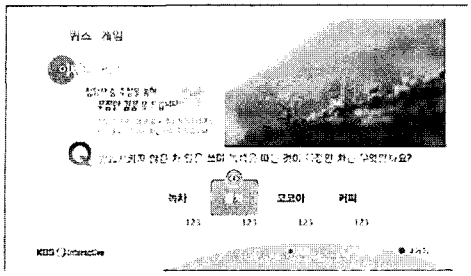
- Application lifecycle control APIs : org.dvb.application, javax.tv.xlet,
- Graphics APIs : org.havi.ui, org.havi.ui.HComponent, org.havi.ui.HContainer java.awt, java.awt.Imag, java.awt.Color, org.dvb.ui.DvbColor org.havi.ui.HScene, org.havi.ui.HVisible, javax.tv.graphics org.havi.ui.event ..
- User input event handling APIs : org.dvb.event, org.davic.resources.ResourceServer ..
- Java Media Framework (JMF) & Media control APIs : java.media, javax.media.Manager, javax.media.MediaLocator, org.davic.media.MediaLocator, javax.tv.locator.Locator ..
- JavaTV APIs : javax.tv.service.Service, javax.tv.locator.Locator, org.davic.mpeg, java.io.File, java.lang.String, Java.util.Vector, java.rmi.Naming ..

3) 양방향 서비스

양방향 서비스는 주로 연동형 서비스에서 사용자가 방송 사업자측과 인터랙티브하게 정보를 주고 받는 서비스를 의미한다. 이 서비스를 통해서 사용자는 방송 내용에 관해 자유로운 의견을 개진할 수도 있고 Quiz 나 투표 등에 직접 참가할 수도 있다. 사용자가 선택한 사항들은 실시간으로 방송 사업자에게 전송되며 방송 사업자는 이 정보들에 기반하여 실시간으로 방송 내용을 구성할 수 있다.



〔그림 18〕 양방향 서비스 〈게임〉



〔그림 19〕 양방향 서비스 〈게임〉

수신 셋탑박스에서 사용된 ACAP-J 표현미들웨어 관련 API들은 아래와 같다. 양방향의 경우에는 리턴채널 관련 API들이 추가로 사용된다.

- Return channel using APIs : org.dvb.net.rc, org.davic.resources, java.net.Inetaddress, java.net.URLConnection, java.net.Socket.
- Application lifecycle control APIs : org.dvb.application, javax.tv.xlet,
- Graphics APIs : org.havi.ui, org.havi.ui.HComponent, org.havi.ui.HContainer java.awt, java.awt.Imag, java.awt.Color, org.dvb.ui.DvbColor org.havi.ui.HScene, org.havi.ui.HVisible, javax.tv.graphics org.havi.ui.event ..
- User input event handling APIs : org.dvb.event, org.davic.resources.ResourceServer ..
- Java Media Framework (JMF) & Media control APIs : java.media,javax.media.Manager,javax.media.MediaLocator, org.davic.media.MediaLocator, javax.tv.locator.Locator ..
- JavaTV APIs : javax.tv.service.Service, javax.tv.locator.Locator, org.davic.mpeg, java.io.File, java.lang.String, Java.util.Vector, java.rmi.Naming ..

본 개발에서는 데이터방송 표준 명세인 ACAP에서 명시한, 리턴 채널 보안 기능을 개발하였다. 본 연구에서 중점적으로 고려 및 개발된 사항은 다음과 같다.

(1) 데이터 방송 스펙 및 JSSE 1.0.2 스펙을 기반으로 JSSE 1.0.2 API를 개발하였다.
(2) 임베디드 환경의 STB 성능 제약을 고려하여 응답시간을 최소화하였다.
(3) 국내 ACAP 환경의 필수 요구 조건인 국내 설계 블록 암호 알고리즘 SEED를 지원하는 리턴 채널 보안 모듈을 개발하였다.
(4) ACAP(MHP)이 명시하는 JSSE 상세 명세는 TLS 루트 인증서의 처리 기준이 IETF의 TLS 표준 스펙과 상이하므로 이를 보완할 수 있도록 미들웨어와 리턴 채널 보안 모듈 간에 인증서 처리를 위한 연동을 제공하였다.

7. 기술개발 결과 및 기대효과

가. 기술결과 결과

본 기고에서 소개된 기술들은 데이터방송 기술협의회를 통해 대화형방송(양방향 데이터방송) 송수신 정합실험을 실시하여 완성도를 높였고 이를 바탕으로 대화형방송(양방향 데이터방송) 송수신 실험방송을 실시하고 있다. 또한 개발된 기술의 홍보를 위해 NAB2004, KOBA2004 등 국내,외 전시회를 통해 성공적으로 전시하여 호평을 받으므로서 개발기술의 우수성을 입증하기도

하였다. 기술개발 결과는 다음과 같다.

- ㅇ 양방향 대화형 송수신 시스템 기술개발
- ㅇ 양방향 대화형 저작도구 및 표현미들웨어 기술 개발
- ㅇ 보안/인증을 적용한 송수신 상향채널 기술 개발
- ㅇ 양방향 대화형 콘텐츠 개발

나. 기대효과

본 기술 개발로 인하여 양방향 데이터방송(대화형방송) 서비스를 실시할 수 있는 제반 환경을 구축되었으며, 2005년에는 방송과 통신의 융합서비스인 대화형방송이 실시될 것이다. 이러한 서비스 실시는 단말기 산업의 대외 경쟁력 강화시켜 로열티 지불 부담 최소화하고 방송, 가전, 컨텐츠, 인터넷 산업을 동반 발전시킬 것이며, 이로 인하여 디지털방송 시장의 확대로 방송사, 단말 및 컨텐츠 업계 활성화에 기여할 것이다.

보다 양질의 디지털방송 서비스인 대화형방송 실시를 통해 계층간, 지역간, 세대간, 빈부간 등에서 오는 정보격차(디지털 디바이드(Divide))해소로 인하여 정보화시대를 구현될 것이다.즉, 디지털 TV 등 인터넷정보가전 제품을 이용한 언제 어디서나 막힘없이 정보를 얻을 수 있는 시대 구현될 것이다. 이러한 서비스는 지식정보 사회에서 능동적인 시민사회 기반 마련하여 수동적 시청자에서 능동적 참여자로 변화를 일으키게 될 것이며 새로운 수익 모델 창출(Interactive 광고, T-commerce, T-moll, T-Poll) 될 것으로 보인다. 또한 데이터방송에서의 보안 및 인증 관련 국내 기술의 확보로 신규 on-line 산업분야의 활성화에 기여하여 현재의 컴퓨터 시장에 버금가는 컨텐츠 등 S/W 시장이 형성될 것으로 기대된다.

8. 결 론

2003년 하반기부터 대화형방송 표준이 지상파와 케이블의 상호호환을 위해 지상파 표준인 DASE와 케이블 표준인 OCAP을 바탕으로 호환 표준인 ACAP이 새롭게 부각되어, 한국도 지상파 데이터방송 표준을 ACAP 표준을 준수하는 것으로 잠정 결정되었다. 이러한 추세에 맞춰 기 개발된 실험방송용 DASE 양방향 데이터방송 시스템의 기술을 바탕으로 성능을 개선, 추가, 변경하여 ACAP 표준을 만족하는 실험시스템을 개발 완성하였다.

이 외에 본방송에 대비하여 필요한 여러 가지 기능들과 안정성을 강화하기 위한 송수신 기능들이 추가되었으며, 내년 상반기 본방송을 목표로 운용의 편리성과 멀티애플리케이션 지원기능 등을 추가 개발할 예정이다.

또한 데이터방송 기술협의회를 통해 다양한 송수신 정합 가이드라인이 작성되었으며, 이를 바탕으로 ACAP 기반 송수신시스템(송출, 저작, 리턴, 수신 기능)이 개발되고 다양한 기능들에 대한 기본 검증이 완료되었다. 현재 ACAP 양방향 실험방송을 송수신할 수 있는 장비들이 개발되었으며, 2004년 6월부터 현재까지 ACAP 대화형방송 실험방송이 계속 실시하고 있다.

2005년 초로 예정되어 있는 양방향 대화형방송 본방송 실시를 위해서 다음과 같은 노력이 계속 진행될 예정이다.

- ㅇ 양방향 대화형 송수신 기술개발 완성 및 안정화
- ㅇ 양방향 대화형 저작도구 및 표현미들웨어 기술 개발 완성 및 안정화
- ㅇ 보안/인증을 적용한 송수신 상향채널 기술 개발 및 안정화

- ㅇ 양방향 대화형 표준안 작성 및 송수신 서비스 가이드라인 완성
- ㅇ 양방향 대화형 애플리케이션 개발

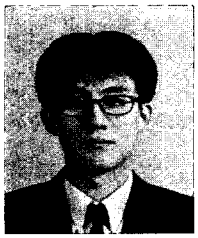
본 기고에서 소개한 기술 개발은 산자부 중기거점/차세대 신기술개발사업 과제인, 양방향 대화형방송 송수신 기술 개발 (Interactive Media Solution, IMS)를 통해 이루어졌음.

강 대 갑

1986년 : 부산대학교 전자공학과 졸업

1989년 : 한국과학기술원 대학원 졸업(석사)

1989년 ~ 현재 : KBS 방송기술연구팀 근무



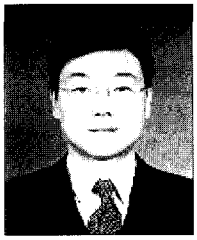
이 광 기

1993년 8월 : 연세대학교 공학 박사 (전자공학)

1993년 9월 ~ 1994년 2월 : 한국과학기술연구원(KIST) 초빙연구원

1994년 3월 ~ 1996년 8월 : 삼성 종합 기술원

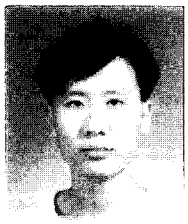
1996년 9월 ~ 현재 : 삼성 전자



박 석 원

1987년 : 명지대학교 전자공학과 학사

1987년 ~ 현재 : LG전자 DTV연구소/책임연구원



김 용 재

2000년 2월 : 연세대학교 공학 석사 (전기,컴퓨터공학)

2000년 2월 ~ 현재: 대우일렉트로닉스