

# 수신 제한된 방송 서비스 제공 시스템 설계 및 구현

論 文
8-2-4

## Design and Implementation of Providing Conditional Access Broadcasting Service System

김동옥\*, 신익룡\*\*  
Dong-Ok Kim, Ik-Ryong Shin

### Abstract

In this paper, This thesis is cell phone for make CAS service be for hand joining broadcasting Create a way CAS Chip. PerSam issue card inside use Seed Key and algorithm make CID Key and record CAS Chip. PerSam member Card inside use Seed Key and algorithm make Subscriber Key after include Subscriber. Key CAS Chip for record CID Key register EMM. make CAS CHIP in accordance with issue CAS Chip. broadcast service entry be for hand treatment so make low bandwidth for joining message and make increase a member.

**Keyword** : CAS, DMB, CW(Control Word) ECM(Entitlement Control Message)

### I. 서 론

IPTV를 통하여 전송되는 콘텐츠 저작권 보호는 필수적인 사항으로 기존의 케이블방송 및 위성 DMB와 같은 방송 시스템에 적용되어 온 CAS(Conditional Access System) 기술을 이용한 유료 서비스에 필요한 기술이다. IPTV는 이러한 방송 채널을 보호할 뿐 아니라 사용자가 IPTV 콘텐츠를 저장하여 다양한 용도로 재사용 및 재배포 할 수 있다. 콘텐츠를 서비스할 때 필요한 보호기술과 콘텐츠의 저장 및 사용에 필요한 보호방식이 각각 필요하다.

이러한 두 가지 보호기술은 현재 다양한 기술, 제품, 표준이 존재하고 있으며 서비스형태, 사업자의 정책에 따라 다양한 형태로 결합하여 사용될 수 있다.

디지털 멀티미디어 방송 서비스(DMB)는 가입자들이 옥외에서 또는 이동 중에도 수신안테나를 장착한 개인 휴대용 또는 차량용 이동 단말을 통해 비디오, 오디오 및 데이터 등 다양한 멀티미디어 방송을 다채널로 시청하거나 청취할 수 있는 방송 서비스를 말한다.

지금까지 서비스는 종전의 아날로그 방송 형태를 디지털화함으로써 고품질 CD 수준의 음질, 다양한 데이터 서비스, 양방향성, 우수한 이동수신 품질 등을 제공하게 되고 기존의 보고 듣는 방송 개념을 보고 듣고 참여하는 방송으로 확장시켰으며, 데이터 방송을 통해 음악방송 외에도 뉴스, 교통정보, 기상정보, 지리위치정보, 동영상 정보 등과 같은 다양한 멀티미디어 정보를 문자와 그래픽으로 전송할 수 있게 되었다.[1]

한편으로는, DMB 서비스는 일반적으로 유료 서비스이므로 가입자의 수신제한을 위하여 CAS(Conditional Access System)를 적용한다. 이러한 CAS는 각 이동단말기에 내장된 DMB 칩을 통해 시청등급을 설정함으로써 수신제한 기능을 수행하며, 상기 DMB칩의 불법사용을 통한 DMB 시

접수일자 : 2009년 4월 24일  
최종완료 : 2009년 6월 22일  
\*김동옥 : 한국정보통신기술대학교 이동통신설비과  
교신저자, E-mail : dokim@icpc.ac.kr  
\*\*신익룡 : 캐스톤(주)

청을 방지하는 보안기능을 수행한다.

단말기에 삽입 또는 내장되어 동작하는 CAS 칩은 암호화된 방송 콘텐츠를 복호화 하는데 필요한 CW(Control Word)를 ECM(Entitlement Control Message)으로부터 생성하고, 가입 메시지, 수신권한 정보 등을 EMM(Entitlement Management Message)으로부터 추출하는 역할을 한다.

이러한 CAS 칩이 정상적으로 특정 프로그램을 시청할 수 있도록 지원하기 위해서는 가입 절차가 필요하고, 이러한 가입 절차는 가입 메시지를 수신함으로써 이루어진다.[2]

따라서 본 논문에서 제시한 방법은 CAS 칩 발급 시 미리 방송 서비스 가입 처리를 수행토록 하여 가입 메시지로 인한 대역폭을 줄이고, 그로 인한 가입자 수를 늘릴 수 있는 수신 제한된 방송 서비스 제공 시스템 및 방법을 제공하는데 있다.

또한, 이동 단말기를 구매한 후, 별도의 가입 절차를 밟지 않아도 수신 제한된 방송 서비스를 제공받을 수 있는 수신 제한된 방송 서비스 제공 시스템 및 방법을 제공하는데 있다.

그리고 CAS 칩 발급 시 가입 메시지와 함께 상품 권한 정보가 포함하도록 하여 상품에 대한 구매 절차를 거치지 않고 바로 해당 프로그램을 시청할 수 있도록 하는 수신 제한된 방송 서비스 제공이 가능하도록 하는 시스템이다.

## II. CAS Module 및 시스템

### 1. CAS Module

그림 1은 종래의 CAS(Conditional Access System) 정보 송수신 모듈에 관한 것으로, 방송 시청을 가능하게 하는 CAS 정보를 이용하는 셋탑박스 메인처리부에 연결된 CAS 정보 송수신 모듈에 있어서, 상기 셋탑박스 메인 처리부로부터의 CAS 정보를 포함하는 TX 데이터를 변조하여 입력단과 출력단중 적어도 하나를 통해 출력하는 TX 변조기 및 입력단 또는 출력단을 통해 수신되는 CAS 정보를 포함하는 RX 신호를 복조하여 셋탑박스 메인 처리부로 전달하는 RX 판별기를 포함하고 있다

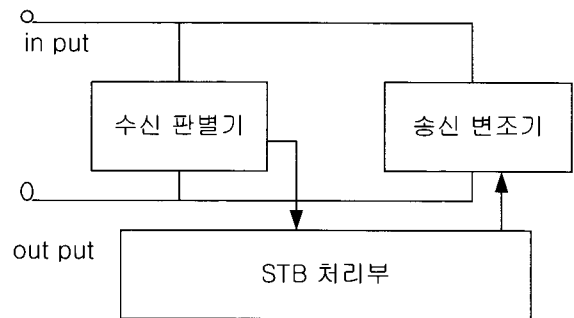


그림 1. CAS Module 구성도

CAS 정보 송수신 모듈은, 상기 셋탑박스 메인 처리부로부터의 송신 제어에 따라 상기 TX 변조기가 송신 경로를 선택하도록 제어하는 I/O 제어기를 더 포함하는 것으로 구성 되어 있다.[3][4]

TX 변조기는, I/O 제어기의 송신 경로 선택제어에 따라 상기 입력단과 출력단 중 하나의 송신경로를 선택하고, 선택된 송신 경로를 통해 CAS 정보를 포함하는 TX 신호를 출력하는 형태로 되어있다.

또한, 기존의 CAS 정보 송수신 모듈의 특징은, 방송 시청을 가능하게 하는 CAS 정보를 이용하는 셋탑박스 메인 처리부에 연결된 CAS 정보 송수신 모듈에 있어서, 상기 셋탑박스 메인 처리부로부터의 CAS 정보를 포함하는 TX 데이터를 변조하여 입력단과 출력단중 적어도 하나를 통해 출력하는 TX 변조기 입력단 및 출력단을 통해 수신되는 CAS 정보를 포함하는 RX 신호를 복조하여 셋탑박스 메인 처리부로 전달하는 RX 판별기 입력단과 출력단중 적어도 하나의 DC 공급경로를 통해 DC 전원을 출력하는 DC 전원부를 포함하고 있으며, 모듈은, 셋탑박스 메인 처리부로부터의 제어에 따라, DC 전원부가 입력단과 출력단중에서 적어도 하나의 DC 공급경로를 선택하도록 제어하는 I/O 제어기를 더 포함하는 것이 특징이다.

### 2. CAS 기존 방법의 원리

그림 2는 현재 셋탑박스를 이용한 방송 수신시스템은 하나의 안테나에 연결된 제1 셋탑박스(STB1) 및 제2 셋탑박스(STB2) 각각이 제1 룸(Room1) 및 제2 룸(Room2)에 설치되어 있고, 제1 셋탑박스(STB1) 및 제2 셋탑박스(STB2) 각각에는 텔레비전이 연결되어 있다.

이 때, 각 룸에서는 TV 방송을 시청하기 위해서는 각 셋탑박스에 이용할 CAS 카드가 필요하다.

그런데, 이와 같은 하나의 셋탑박스는 각각의

CAS 정보가 내장된 카드키(Card-Key)가 삽입되어야 하며, 이 CAS 카드키(CAS Card-Key)는 사용자 하나의 셋탑박스에서만 동작하므로 별도의 두 번째 방(2nd Room)에서도 동일한 고가의 셋탑박스를 구입하여야 하는 문제점이 있다.

즉, 셋탑박스를 두 대 이상을 사용하고자 할 경우에는 두개 이상의 CAS 카드를 구매해야 하는 문제점이 있으며, 또한 하나의 셋탑박스를 이용하여 2개의 다른 장소에서 텔레비전 방송을 시청 및 제어할 수 없다는 문제점이 있다.[5][6]

이러한 문제점은, 셋탑박스에 CAS 정보를 공유하는 기능이 없다는 것이다.

그림 3은 현재의 CAS(Conditional Access System)칩 발급에서부터 이동 단말기가 방송 서비스를 이용하는 방법을 설명하기 위한 개념도이다. 그림 3에서 PerSAM 카드 발급사는 단말기 제조사로부터 CAS 칩 발급 주문이 요청되면, CAS 칩에 중요 정보를 발급할 때 사용되는 발급용 PerSAM 카드를 발급하고, 각 CAS 칩에 저장될 CSID 리스트를 생성하여 발급용 PerSAM 카드와 함께 CAS 칩 발급사에 제공한다.

CAS 칩 발급사는 PerSAM 카드 발급사로부터 제공받은 발급용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 CAS 칩에 내장될 CID Key를 생성하고 그것을 CAS 칩에 입력한다.

그러면, CAS 칩의 생성이 완료되고 CAS 칩 발급사는 생성된 CAS 칩을 단말기 제조사에 전송한다.

단말기 제조사는 이동 단말기에 CAS 칩을 탑재하고, 그 결과를 고객 관리 서버에 전송하고 고객 관리 서버는 이동 단말기에 탑재된 CAS 칩의 CSID 정보를 CAS 서버에 전송한다.

이와 같은 과정에 의해 CAS 칩이 탑재된 이동 단말기 생성된다. 생성된 이동 단말기를 이용하여 방송 서비스를 이용하기 위하여 사용자는 고객

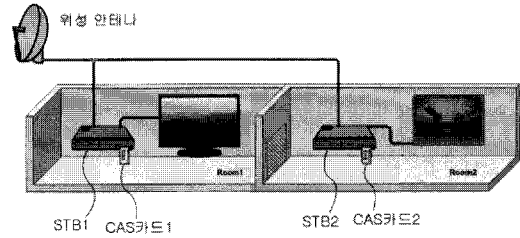


그림 2. 셋탑박스를 이용한 방송 수신 시스템 구성도

관리 서버에 방송 서비스 가입을 요청하는 방송 서비스 가입 요청 메시지를 전송한다. 방송 서비스 가입 요청 메시지는 이동 단말기에 탑재된 CAS 칩의 CSID 정보를 포함한다.

고객 관리 서버는 방송 서비스 가입 요청 메시지를 CAS 서버에 전송하고 서버는 방송 서비스 가입 요청 메시지에 포함된 CSID에 대해 가입 승인을 수행하여 이동 단말기에 가입 메시지를 전송한다. 이동 단말기는 방송 서비스를 이용할 수 있게 된다.

이와 같이 종래의 CAS 칩이 탑재된 이동 단말기를 이용하여 특정 프로그램을 시청하기 위해서는 별도의 가입절차를 거쳐야 하는 불편함이 있었다.

또한, 방송 서비스 가입 절차에 의한 가입 메시지를 전송하는데 있어서 상당량의 대역폭이 필요한 단점이 있다.

그리고 방송 서비스를 제공받기 위해서 단말기를 구매한 후 별도의 가입 절차를 밟아야 하므로 방송 서비스를 제공받기 위한 절차가 복잡한 단점이 있다.

### III. 제안된 시스템 설계

#### 1. 본 논문의 구성

본 논문에서 제시하는 방법 및 시스템은 이동 단말기가 수신 제한된 방송 서비스를 제공받을 수 있도록 미리 방송 서비스 가입 처리가 수행된 선가입 CAS 칩을 생성하는 방법에 있어서 발급용 PerSAM카드 내부의 seed key 및 알고리즘을 이용하여 CID key를 생성하고 생성된 CID key를 CAS 칩에 등록하는 단계 가입용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 Subscriber Key를 생성하고 생성된 Subscriber Key를 가입 EMM에 포함시킨 후 CID key가 등록된 CAS 칩에 가입 EMM를 등록하여 CAS 칩

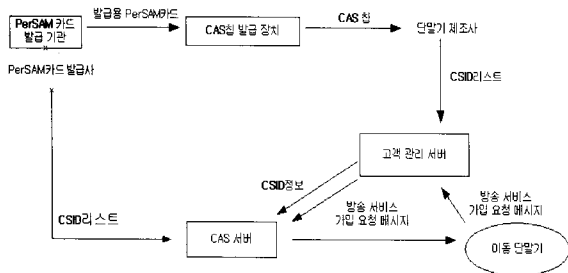


그림 3. 시스템 구성도

을 생성하는 단계를 포함하는 것을 특징으로 하는 수신 제한된 방송 서비스 제공을 위한 CAS 칩 생성 방법과 이동 단말기가 수신 제한된 방송 서비스를 제공받을 수 있도록 미리 방송 서비스 가입 처리가 수행된 CAS 칩을 생성하는 방법에 있어서 카드 인증 및 키 값 로딩을 위한 키 저장 장치인 PerSAM 카드를 발급하는 PerSAM 카드 발급 장치가 CSID 리스트를 생성하여 CAS 서버와 CAS 칩 발급 장치에 제공하는 단계 CAS 서버가 CSID 리스트별 가입 EMM을 생성하여 CAS 칩 가입 장치에 제공하는 단계로 칩 발급 장치가 발급용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 CID key를 생성하고 생성된 CID key를 CAS 칩에 등록하는 단계 및 상기 CAS 칩 가입 장치가 가입용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 Subscriber Key를 생성하고 생성된 Subscriber Key를 CAS 서버로부터 제공된 가입 EMM에 포함시킨 후 CAS 칩 발급 장치에서 발급 완료된 CAS 칩에 가입 EMM를 등록하여 가입 완료된 CAS 칩을 생성하는 단계를 포함하는 것을 특징으로 하는 수신 제한된 방송 서비스 제공을 위한 CAS 칩 생성 방법이 제공된다.

그리고, 가입자 정보가 저장된 고객 관리 서버와 CAS 서버를 통해 이동 단말기가 방송 서비스를 제공받는 방법에 있어서 임의 채널에 대한 방송 서비스 수신에 요청되면 탑재된 CAS 칩의 가입 EMM를 분석하여 해당 채널의 방송 서비스 수신에 가능한지를 판단결과 해당 채널의 방송 서비스 수신에 가능하지 않으면 해당 채널의 방송 서비스 수신을 위한 시청 권한 요청 여부 질의 메시지를 출력하여 출력된 시청 권한 요청 여부 질의 메시지를 통해 요청 명령이 선택되면 고객 관리 서버를 통해서 CAS 서버에 시청 권한 요청 메시지를 전송하여 시청 권한 부여 메시지가 수신되면, 해당 채널의 방송 서비스를 제공받는 단계를 포함하는 것을 특징으로 하는 수신제한된 방송 서비스 제공 방법이 제공된다.

첫 번째 단계는 CAS 칩의 가입 EMM의 채널 시청 자격 및 유료 채널에 대한 시청 등급에 관한 정보를 확인하여 해당 채널의 방송 서비스 수신에 가능한지를 판단하는 것을 말한다.

3단계 이후부터는 CAS 서버는 이동 단말기를 해당 채널의 방송 서비스에 가입시킨 후 이동단

말기에 시청 권한 부여 메시지를 전송한다.

또한 CID key 및 가입 EMM이 등록된 CAS 칩이 탑재되어 있고, 방송 서비스 수신을 위한 채널이 선택되면 가입 EMM을 이용하여 해당 채널의 방송 서비스 수신에 가능한지의 여부를 판단하고 해당 채널의 방송 서비스 수신에 불가능하면 시청 권한 요청 여부 질의 메시지를 출력하는 이동 단말기 CAS 칩 발급 시 미리 방송 서비스 가입 처리가 수행된 CSID 리스트를 포함하는 가입자 정보를 관리하고 이동 단말기로부터 시청 권한 요청 메시지가 수신되면 상기 시청 권한 요청 메시지를 전송하는 고객 관리 서버 및 상기 고객 관리 서버로부터 시청 권한 요청 메시지가 수신되면 메시지에 포함된 채널의 방송 서비스에 가입시킨 후 시청 권한 부여 메시지를 이동 단말기에 전송하는 CAS 서버를 포함하는 것을 특징으로 하는 수신 제한된 방송 서비스 제공 시스템이 제공될 수 있다.

이동 단말기는 시청 권한 요청 여부 질의 메시지를 통해 요청 명령이 선택되면, 이동 단말기 식별 정보 및 해당 채널 정보를 포함하는 시청 권한 요청 메시지를 생성하여 고객 관리 서버에 전송한다.

CAS 칩 발급 및 수신 제한된 방송 서비스 제공 시스템은 각 CAS 칩에 저장할 CSID(Called Subscriber Identification) 리스트를 생성하는 PerSAM 카드 발급 장치 PerSAM 카드 발급 장치에서 생성한 CSID 리스트별 가입 EMM을 생성하는 서버 PerSAM 카드 발급 기관에서 발급된 발급용 PerSAM 카드를 이용하여 CID Key를 생성하고 그림 4는 CAS 칩에 입력하는 CAS 칩 발급 장치 CAS 칩 발급 장치에서 발급 완료된 CAS 칩에 서버에서 생성된 가입 EMM을 등록하여 가입 완료된 CAS 칩을 생성하는 CAS 칩 가입 장치 가입 완료된 CAS 칩을 이동 단말기에 탑재하고 그 CSID 리스트를 고객 관리 서버에 제공

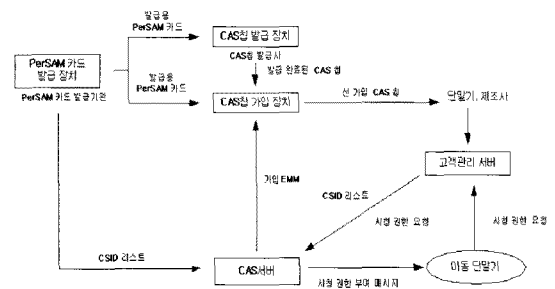


그림 4. CAS칩 발급 및 수신 제한된 방송 서비스 제공 시스템

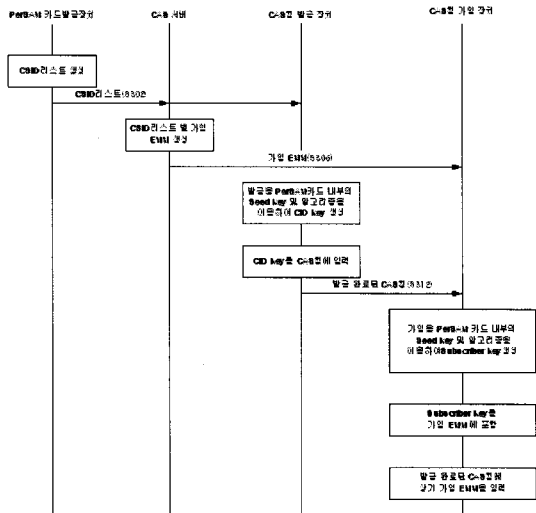


그림 5. 이동 단말기를 이용한 방송 서비스 제공 방법 흐름도  
하는 단말기 제조사 이동 단말기로부터 특정 채널의 시청권한이 요청되면 서버에 시청 권한 요청 메시지를 전송하는 고객 관리 서버를 포함한다.

PerSAM 카드 발급 기관은 발급용 PerSAM 카드와 방송 서비스 처리에 사용되는 가입용 PerSAM 카드를 발급하여 발급용 PerSAM 카드는 CAS 칩 발급 장치에 제공하고 가입용 PerSAM 카드는 CAS 칩 가입 장치에 제공한다.

또한, PerSAM 카드 발급 장치는 CAS 칩에 저장할 CSID 리스트를 생성하여 CAS 칩 발급 장치와 CAS 서버에 전송한다.

CAS 서버는 PerSAM 카드 발급 기관으로부터 CSID 리스트가 수신되면, CSID별 가입 EMM을 생성하여 CAS 칩 가입 장치에 전송한다. 가입 EMM은 이동 단말기 사용자의 채널 시청 자격 및 유료 채널에 대한 시청 등급에 관한 정보를 포함한다.

CAS 칩 발급 장치는 발급용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 CID Key를 생성하고 그것을 CAS 칩에 등록하여 CAS칩의 발급을 완료한다. 그러면, CAS 칩 발급사는 발급 완료된 CAS 칩을 CAS 칩 가입 장치에 제공한다.

상기와 같은 과정에 의해 생성된 CAS 칩이 내장된 이동 단말기를 구매한 사용자는 별도의 가입 절차를 밟지 않아도 수신 제한된 방송 서비스를 제공받을 수 있다. 즉, 생성된 CAS 칩이 내장된 이동 단말기는 별도의 가입 절차를 거치지 않아도 해당 가입 EMM에 등록된 채널 시청 자격

및 유료 채널에 대한 시청 등급에 관한 정보에 따라 해당하는 채널의 방송 서비스를 제공받을 수 있다.

그림 5는 본 논문에서 제시에 따른 가입 완료된 CAS 칩이 탑재된 이동 단말기를 이용한 방송 서비스 제공 방법을 나타낸 흐름도이다.

이동 단말기 사용자가 메뉴를 이용하여 임의 채널에 대한 방송 서비스 수신을 요청하면 이동 단말기는 내장된 CAS 칩의 가입 EMM를 분석하여 해당 채널의 방송 서비스 수신이 가능한지를

판단한다. 이동 단말기는 방송 서비스 시청 요청 명령이 입력되면, CAS 칩의 가입 EMM의 채널 시청 자격 및 유료채널에 대한 시청 등급에 관한 정보를 확인하여 해당 채널의 방송 서비스 수신이 가능한지를 판단한다.

해당 채널의 방송 서비스 수신이 가능하지 않으면 이동 단말기는 해당 채널의 방송수신을 위한 시청 권한 요청 여부 질의 메시지를 출력한다.

출력된 시청 권한 요청 여부 질의 메시지를 확인한 사용자가 해당 채널의 방송 수신을 위하여 요청 명령을 선택하면 이동 단말기는 고객 관리 서버를 통해서 CAS 서버에 시청 권한 요청 메시지를 전송한다

여기서, 시청 권한 요청 메시지는 이동 단말기 식별정보, 방송 서비스 수신을 원하는 채널 정보 등을 포함한다.

상기 CAS 서버는 상기 이동 단말기를 해당 채널의 방송 서비스에 가입시킨 후, 상기 이동 단말기에 시청 권한 부여 메시지를 전송한다

그러면, 이동 단말기는 해당 채널의 방송 서비스를 수신할 수 있다.

만약, 판단결과 해당 채널의 방송 서비스 수신 이 가능하면 이동 단말기는 해당 채널의 방송 서비스를 제공받는다.

이와 같이, 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다.

본 논문은 이동 단말기가 수신 제한된 방송 서비스를 제공받을 수 있도록 미리 방송 서비스 가입 처리가 수행된 선가입 CAS 칩을 생성하는 방법에 있어서 발급용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 CID key를 생성하고

생성된 CID key를 CAS 칩에 등록하고 가입용 PerSAM 카드 내부의 seed key 및 알고리즘을 이용하여 Subscriber Key를 생성하고 상기 생성된 Subscriber Key를 가입 EMM에 포함시킨 후 CID key가 등록된 CAS 칩에 상기 가입 EMM를 등록하여 선가입 CAS 칩을 생성하는 것으로서, CAS 칩 발급시 미리 방송 서비스 가입 처리를 수행하도록 하여 가입 메시지로 인한 대역폭을 줄이고, 그로 인한 가입자 수를 늘릴 수 있다.

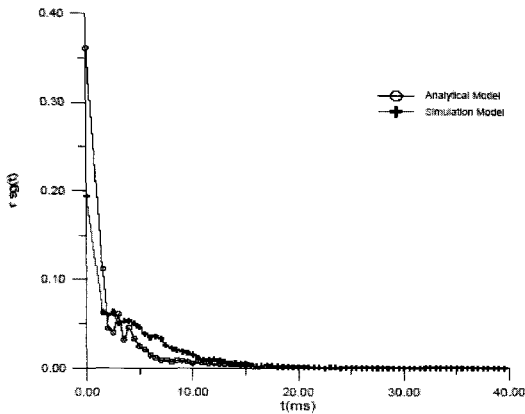


그림 8. U=0.7인 경우의 ATRT의 분포

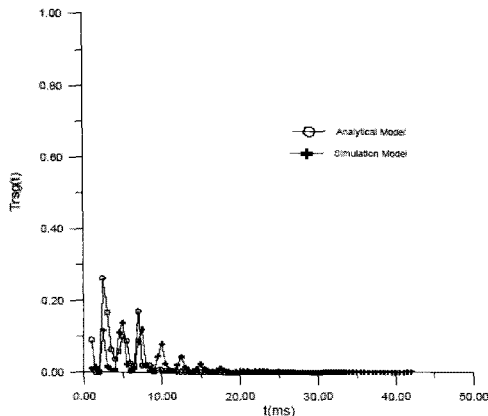


그림 9. U=0.7인 경우의 Residual Time의 분포

## V. 시스템 시뮬레이션 결과

도출한 식을 일반적인 시스템인 30개의 노드를 갖는 FOUNDATION Fieldbus에 적용시킨 예에 대하여 기술한다. 각 노드는 주기적 데이터 전송 큐, 산발적 실시간 데이터 전송 큐, 비 실시간 데이터 전송 큐를 갖는다. 시스템의 트래픽은 0.7, 0.5, 0.3의 3가지 경우에 대하여 시뮬레이션 하였

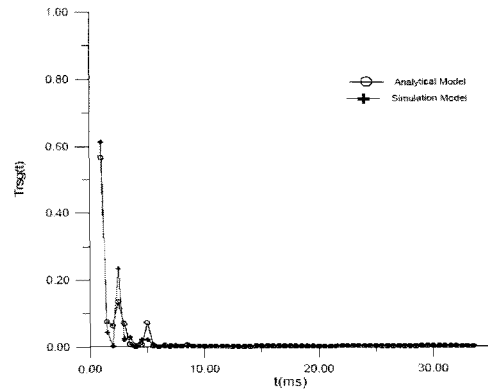


그림 6. U=0.3인 경우의 ATRT의 분포

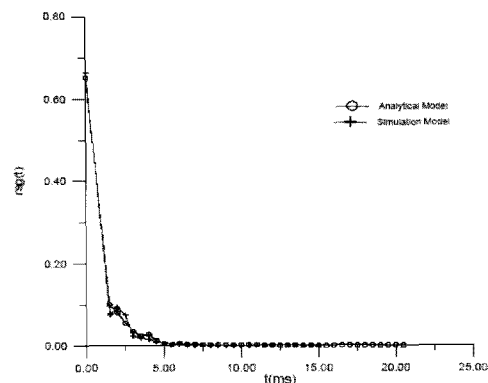


그림 7. U=0.3인 경우의 Residual Time의 분포

다. 본 논문에서는 통신망 시스템의 트래픽이 주기적 데이터가 60%, 산발적 실시간 데이터가 10%, 비실시간 데이터가 30%로 구성되는 경우에 대하여 분석하였다. 주기적 데이터는 전체 30개 노드에서 모두 생성하고, 비실시간 데이터와 산발적 실시간 데이터는 각각 15개의 노드에서만 생성한다고 가정한다. 주기적 데이터의 데이터 생성 주기는 기술한 윈도우 스케줄링 기법을 이용하여 도출하였고, 산발적 실시간 데이터와 비실시간 데이터는 전체 트래픽을 고려하여 데이터의 도착빈도를 도출하였다. 각 통신망의 데이터의 전송 없이 각 노드를 방문하는데 걸리는 시간인  $R=1.2ms$ 이다. 물리계층의 전송속도는 2Mbps를 사용하였다.

그림 6과 그림 7은 트래픽 U=0.3인 경우 수학적 모델과 시뮬레이션 모델의 ATRT의 분포와 Residual Time의 분포를 비교한 그래프이다.

그림 8과 그림 9은 트래픽 U=0.7인 경우 수학적 모델과 시뮬레이션 모델의 ATRT의 분포와 Residual Time의 분포를 비교한 그래프이다.

그림 8와 그림 9는 트래픽이 높은 U=0.7인 경우는 U=0.3 이나 U=0.5인 경우보다는 오차가 있으나 거의 일치함을 보여준다.

D =20ms로 설정하고, Pa=0.0022로 설정했을 때  $pf < Pa$ 를 만족하는 TTRT는 14.48 ms 이다. 위의 조건으로 시뮬레이션을 했을 때의 결과는  $pf=0.0018$ 로 본 논문 설계의 요구사항을 만족한다. 주기적 데이터의 최대 전송 지연 시간은 14.252ms로 모든 주기적 데이터에 대하여 전송지연 시간의 최대 허용값인  $\Phi_i (i = 1\sim 30)$ 을 초과하지 않는다. 비실시간 데이터 패킷의 평균 전송지연 시간은 5.2060ms로 만족할만한 결과를 보여준다.

## V. 결 론

본 논문에서 제시한 시스템은 CAS 칩 발급 시 미리 방송 서비스 가입 처리를 수행토록 하여 가입 메시지로 인한 대역폭을 줄이고 그로 인한 가입자 수를 늘릴 수 있는 수신 제한된 방송 서비스 제공 시스템 및 방법을 제공할 수 있다.

또한, 이동 단말기를 구매한 후 별도의 가입 절차를 밟지 않아도 수신 제한된 방송 서비스를 제공할 수 있는 수신 제한된 방송 서비스 제공 시스템 및 방법을 제공할 수 있고 CAS 칩 발급 시 가입 메시지와 함께 상품 권한 정보가 포함하도록 하여 상품에 대한 구매 절차를 거치지 않고 바로 해당 프로그램을 시청할 수 있도록 하는 수신 제한된 방송 서비스 제공 시스템 및 방법을 효율적으로 제공할 수 있다.

산업이용 가능성은 이상과 같이 수신 제한된 방송 서비스 제공 시스템 및 방법은 CAS 칩 발급 시 미리 방송 서비스 가입 처리가 수행된 선가입 CAS 칩이 탑재된 이동 단말기를 이용하여 방송 서비스 초기 이용할 때 별도의 가입절차를 밟지 않고 수신 제한된 방송 서비스를 받을 수 있다.

본 논문에서 제시하는 대역폭 할당 기법을 이용하면 통신망 시스템의 성능을 미리 예측할 수 있고 통신망 시스템의 전송 지연시간의 요구사항을 만족시키기 위해서 어떤 인자를 어떻게 조절해야 하는가를 결정할 수 있다.

추후 연구과제로는 더 많은 시뮬레이션을 수행

하여 다양한 환경에서 수학적 모델의 타당성 검증과 통신망 매개변수의 증감에 따른 pf값의 변화의 관찰을 진행할 예정이다.

### 감사의 글

본 논문은 중소기업청에서 지원하여 연구하였습니다.

### [ 참고 문헌 ]

- [1] E. H. Armstrong, "A some recent developments of regenerative circuits," in *Proceeding of the Institute of Radio Engineers*, vol. 10, pp. 244-260, Aug., 1922.
- [2] S. Cavalieri, A. D. Stefano, and O. Mirabella, "Optimization of acyclic Bandwidth allocation exploiting the priority mechanism in the fieldbus data link layer," *IEEE Transactions on Industrial Electronics*, vol. 40, no. 3, pp. 297-306, June, 1993
- [3] *Data Link Protocol Specification*, ISA/SP50-1996-360M (Draft Standard).
- [4] K. G. Shin and C. Chou, "Design and evaluation of real-time communication for fieldbus-based manufacturing systems," *IEEE Transaction on Robotics and Automation*, vol. 12, no. 3, pp. 357-367, June, 1996.
- [5] 위성방송용 송수신기 정합 규격(TTA.KO-07.0008, 2004-12-20)
- [6] [http://www.francetelecom.com/ps/ps\\_vaad](http://www.francetelecom.com/ps/ps_vaad)
- [7] Functional model of a conditional access system(EBU)

## Biography



### 김 동 옥

1988년 서울산업대학교 전자통신과 졸업  
1996년 광운대학교 전자통신과(공학석사)  
2001년 한국항공대학교 정보통신과(공학박사)  
2003년 2월~현재 한국정보통신기술대학 이동통신과  
교수

<관심분야> Digital Communication Network, UWB, MIMO,  
OFDM.

<e-mail> dokim@icpc.ac.kr



### 신 익 룡

1985년 철도대학 신호처리과(공학사)  
1990년 한국방송통신대학교 전자계산학과 졸업  
2000년 2월~현재 (주) 캐스톤 대표이사  
<관심분야> 정보보호, CAS, DSB, 정보보완  
시스템 최적화, 신호처리, 오류정정부호

<e-mail> irshin@castone.co.kr