主 題

디지털 위성방송의 유료서비스를 위한 제한수신시스템

ETRI 무선방송연구소 방송SW개발팀장 조 현 숙

차 례

Ⅰ. 서 론
Ⅱ. CAS(Conditional Access System)
Ⅲ. 제한수신에서의 키관리
Ⅳ. SimulCrypt와 MultiCrypt 비교
Ⅴ. 결 론

Ⅰ. 서 론

위성을 이용한 디지털 방송의 다채널 시대에 가입자는 개별화된 전문 채널 서비스를 받을 수 있고, 한편 방송사업자는 기존 지상파에서 광고료 수입에만 의존하던 방송 서비스 운영을 TV 방송에 가입자 개념을 추가하여 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하고, 전문 방송 사업자들에 의한 전문 방송 프로그램의 제작을 가능케 하여 다양한 기능의 서비스를 제공할 수 있게 되었다.

이렇듯, 다채널 방송 시대의 방송 사업자는 광고료 수입에만 의존하던 경영 방식을 탈피하여 가입자의 시청료에 의해 운영함으로써, 가입자는 전문화된 채널 및 개인별로 차등화된 보다 양질의 서비스를 받을 수 있는 장점들을 가지고 있다. 이러한 조건부 제한수신 서비스를 만족할 수 있는 시스템 즉, 제한수신시스템(CAS : Conditional Access System)이란 송신기에서 스크램블된 신호를 수신측의 수신 인가를 받은 가입자만이 디스크램블하여 프로그램을 시청할 수 있도록 하는 시스템으로, 이 시스템이 갖추어야 하는 기본적인 요건은 프로그램 및 데이타는 스크램블링되고 통신 링크상에서 보호되어야 하며, 인증을 위한 가입자 신분확인(Authentication)기능과 접근 제어(Access Control) 기능을 갖추어야 한다.

위의 두 가지 요건은 결국 자원(프로그램 및 데이터)과 가입자 보호를 위한 것으로, 자원의 보호 메카니즘으로는 스크램블링/디스크램블링이 있고, 가입자 보호메카니즘으로는 인가된 가입자들에게 해당 시청 권한을 주는 기술이다.

결국, Pay-TV 시스템에서의 안전성은 스크램블링 부분과 암호화 부분에서 좌우된다고 할 수 있는데, 보통 안전성 시스템에 문제가 되는 것은 스크램블링 시스템, 암호화 시스템, 혹은 두 시스템 모두에 피해를 당하는 경우이다.

본 논문에서는 유료 서비스를 위한 제한수신시스템에 대한 기능, 제한수신시스템에서 제기되는 보호 메커니즘 중 키관리에 대해서 살펴보고, 마지

막으로 DVB(Digital Video Broadcasting)에서 제안한 CAS 방식SimulCrypt, MultiCrypt)에 대해서 고찰하고 있다.

II. Conditional Access System

2.1 시스템 요구사항

제한수신 시스템은 크게 스크램블링/디스크램블링, Entitlement Control/Management Function과 같은 3가지 요구사항을 만족하여야 하며, 이러한 기능들은 보다 안전하고 효율적인 운용을 위해 암호화 기법이 요구된다. 자격(Entitlement)은 프로그램 및 데이터의 스크램블링에 필요한 관련 키와 수신자의 시청 권리를 말하며 자격통제와 자격관리로 대별할 수 있다.

- Scrambling/Descrambling Functions

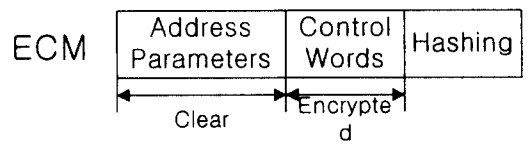
스크램블링은 비 인가된 수신자는 시청할 수 없도록 원래의 TV 신호 형태를 변형시키는 것으로 TV 프로그램 형태(오디오/비디오/데이터)와 신호형태(아날로그/디지털)에 따라 그 방식이 다르다. 디스크램블링은 디스크램블링 Key인 CW(control word)를가질수 있는 수신기에서만 수행된다. DVB 프로젝트에서, EP-DVB 응용에 적용되는 스크램블링 방식은 장기간 외부 공격의 가능성을 최소화하기 위해서 설계해 왔다. 따라서, 스크램블링 방식은 고도의 암호 메커니즘으로 구성된다.

- Entitlement Control Function

Entitlement Control 기능은 Entitlement Control Message(ECM)을 전송하는 기능을 가지며, ECM은 암호화된 CW와 Control Parameter로 구성되고 주기적으로 재생성되어 전송된다. 수신기는 ECM을 스마트 카드로 보내어 스마트 카드내의 마이크로 프로세서는 스마트 카드 내에 있는 Authorization Parameter와 전송 받은 Control Parameter 비교하게 된다. 그 결과가 같으면, 그때 그 수신기는 인증이 되고, 인증된 스마트 카드 내에 있는 Service Key를 가지고 CW를 복호화한다.

이 CW 값은 프로그램마다 다른 값을 가진다. current CW/next CW, control parameters:current date,pay per time/pay per event

ECM(Entitlement Control Messages) 구조



- Entitlement Management Function

Entitlement Management 기능은 권한을 가입자에게 시청 권한(access rights)을 주고, 수신측을 위한 authorization key를 update한다. Entitlement Management 기능은 프로그램의 정보를 관리하고 EMM을 생성한다. EMM addressing 방식은 다음과 같이 3가지 방식을 사용한다.

- EMM-G : 모든 수신기에 접근할 수 있는EMM을 보낼때
- EMM-S : 수신기를 몇몇 그룹으로 나뉘어 EMM을 보낼때
- EMM-U : 수신기에 따라 다른 EMM을 줄때

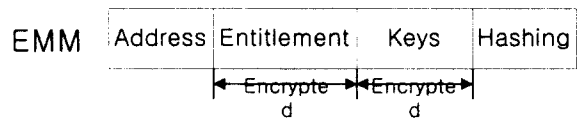
2.2 Pay-TV 서비스

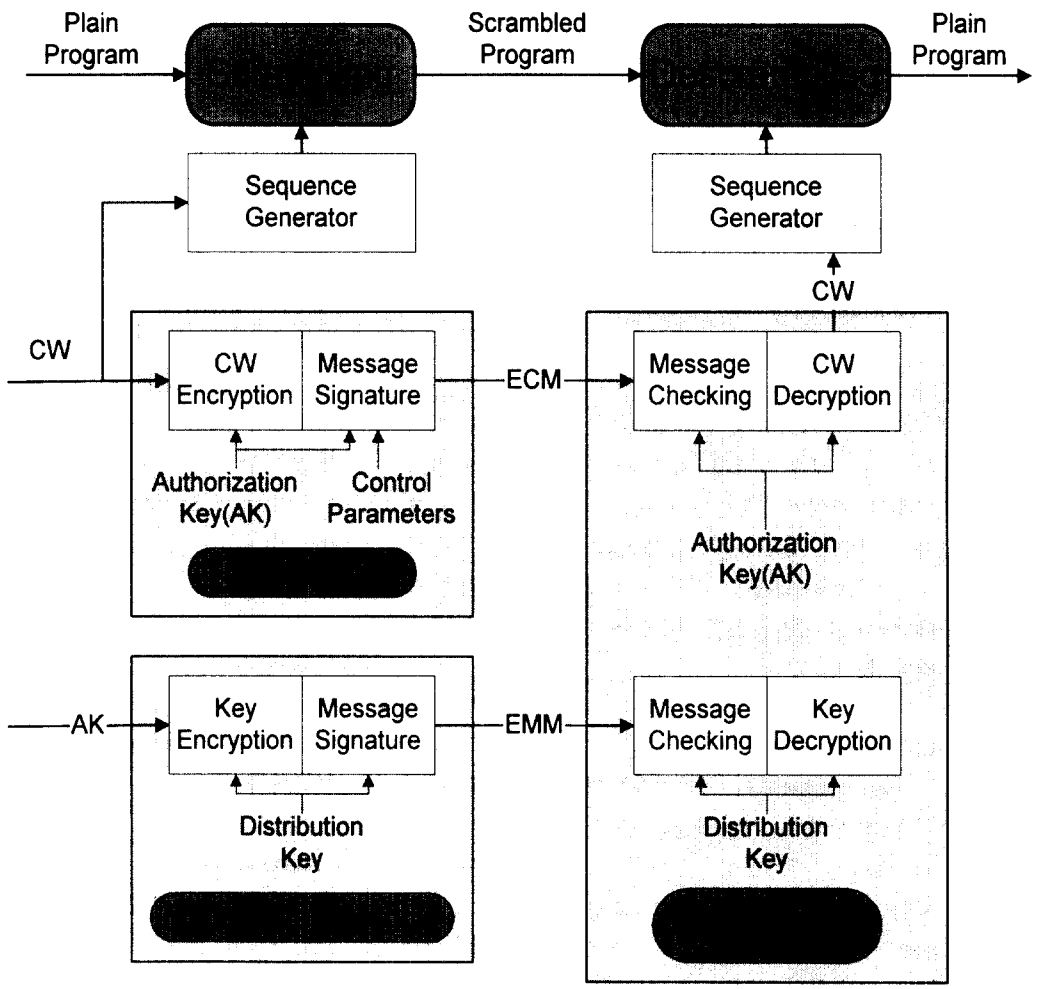
제한수신시스템이 유료방송을 위해 제공할 수 있는 서비스는 아래와 같다.

- Pay-Per-View : 과금 방식이 프로그램 단위로 이루지는 방식으로 Pre-booked 방식, Impulse PPV, Impulse with polling 방식 등이 있다.
- Grouping of entitlements: 여러 개의 채널을 그룹화 하여 서비스
- Over-the-Air Addressing : Entitlement를 Over-the-air로 전송하여 시청권한이 없는 가입자의 시청을 방지하거나 새로운 Entitlement를 부여할 수 있는 방법
- Subscription : 특정 채널 또는 특정 채널 그룹에

EMM(Entitlement Management Messages)구조

(그림 1) CAS 구성도





속해 있는 모든 프로그램의 시청을 가능하도록 하는 시청 권한 부여 서비스

- Thematic selection : 여러 채널에서 특정한 프로그램 주제(스포츠, 드라마, 월드컵 축구,...)에 대한 수신 권한 부여 서비스
- Geographic Limitation: 특정 지역에 대해서만 제공하도록 하여 다른 언어/문화권에 특정 서비스를 제공할 수 있는 기능
- Free Time : Pay-Per-View 프로그램에 대해서 처음 부분을 스크램블 없이 전송하여 비용 지불 없이 시청 가능하도록 하는 서비스
- Date Limits : 가입자가 자신의 entitlement를 가질 수 있는 기간을 정할 수 있도록 하는 서비스
- Over-the-air S/W download : 수신기에서 구동 가능한 게임 등의 S/W를 가입자에게 다운로드 하여 이용할 수 있도록 하는 서비스

- Dial-Back connection : 가입자의 스마트 카드에 저장되어 있는 과금 정보를 전화망을 통해 upload하기 위한 서비스

위의 서비스 중에서 date limits 서비스는 일정 시간 또는 특정 프로그램에 한해서 시청할 수 있는 스마트 카드를 발급하여 서비스 제공자가 선전용으로 제공할 수 있도록 하는 Single event (throwaway card) 서비스로도 이용 가능하다.

2.3 Considerations

• Considerations for viewers

가. 편리성

제한수신시스템은 서비스 처리 시 수신이 인가된 시청자에게 부담을 최소화해야 한다. 특히 채널 변경시 가입자에게는 특별한 조치를 요구하지 말아야 하며, "zapping"시(zapping시 상한 시간은 1초) 음성이나 화면의 지연 현상을 발생시키지 말아야 한다. 더구나, 장비, 비용 및 노력의 면을 고려해야 한다.

나. 수신기 시장

Open market에서 제조업자들이 경쟁적으로 수신기를 생산하여, 시청자들은 디지털 수신기나 Set-Top Box를 다각도로 선정할 수 있는 시장이 형성되어야 한다. 그런 시장은 적법한 기관에서 출판한 open standard를 완전히 수용하는 디지털 방송시스템을 요구한다. 물론 CA 시스템도 포함한다. 표준에 포함된 IPR에 대한 licensing 항은 적절한 표준기관에 의해 규제되어야 한다

다. 서비스 시장의 공개

서비스 제공자의 규제하에 발급된 관련 CA entitlement를 가진자와 관련 표준을 수용하는 IRD를 가진 시청자들은 인증된 프로그램 서비스를 access할 수 있어야 한다.

• 시스템 설계시 고려 사항

가. CW 처리

CW는 스크램블링/디스크램블링 시퀀시를 생성하기 위한 initialization word로서, PRBS를 초기화하기 위한 초기화 시간을 요구하게 된다. 송신측과 수신측 사이의 동기화 때문에 Current/Next CW의 전송은 동시에 발효된다. CW생성 주기는 channel hopping 시간과 ECM의 전송량 사이의 trade-off 관계가 있다. CW의 주기가 클수록 ECM의 양은 감소되나, 다음 CW의 수신 시간 때문에 channel hopping 시간은 증가하게 된다. 반대로, CW 주기 counter가 짧을수록 channel hopping 시간은 감소하게 되나, ECM의 양과 전송주기는 증가하게 된다. 단지 ECM은 overhead 데이터이기 때문에 ECM 전송 양의 증가는 실제 프로그램 데이터(오디오/비디오/데이터)는 감소하게 된다.ECM 전송량 뿐 아니라 Channel Hopping 시간을 줄이는 방법은 소스 clock 정보를 사용하는 PRBS를 초기화하는 것이 될 것이다.

나. Security

제한수신시스템은 불법 시청을 막는데 효율성을 가져야 하므로 다음과 같은 사항을 설계시 고려하여야 한다

A. Addressability

- CA시스템은 유일한 ID와 address를 갖는 장치들을 가져야 한다
- Security 장치들은 인증 메시지들에 대해 address 되어야 한다
- 효율적인 addressing 방법은 보다 강한 security와 가입자에게는 보다 편리하고, 운용면에서는 가격이 낮아야 한다.

B. 불법 시청에 대한 안전성(Security against piracy)

- 시스템 설계는 모든 메시지를 안전하게 전달하도록 되어야 한다.
- 안전성(Security) 암호 설계 및 운용 그리고

secrets을 어떻게 유지하는가에 달려 있다.

C. 비밀 유지

Security processor는 비밀 데이터를 보호해야 한다.

Return Path

PPV와 impulse PPV는 시청자에서부터 CA시스템 운용자에게 return path의 설비를 요구한다. 많은 시스템에서 Return path는 수신기에 부착된 모뎀과 전화선을 사용하여 구현되고 있다. Return Path는 시청 내역을 기록하기 위해 사용될 수 있으며, 또한 프로그램 권한을 발급할 때 고려되어야 하는 사항이다.

III. 제한수신에서의 키 관리

3.1 개요

일반적으로 두 곳 이상에서 통신하고자 할 때 안전한 채널을 확립하기 위해서 사용되는 암호화 시스템에서 대화 키의 생성, 분배 및 정보의 관리 등이 키 관리 문제이다. 이는 암호 시스템, 채널 및 통신의 특성과 깊은 연관을 가지며 시스템의 운용 상황을 고려한 적합한 키 관리 방식을 채택해야만 시스템의 안정성과 효율성을 얻을 수 있다. 일반적으로 암호화 시스템은 암호화 및 복호화 시 동일 키를 사용하는 관용 키 암호화 시스템과 암호화 및 복호화시 상이한 키를 사용하는 공개키 암호화 시스템으로 구분된다.

관용 키 암호화 시스템은 두 통신 당사자가 통신할 때 대화 키를 공유하기 위해서 대화 키를 포함한 전문을 새로운 비밀 키로 암호화 하여야 한다. 이와 같은 관용 키를 이용한 방식에는 중앙 집중식 키 관리와 계층적 키 관리가 있다. 중앙 집중식 키 관리는 통신망 내에 키 센터를 두고 키 분배 문제를 해결하는 방식이다. 어떤 사용자가 다른 사용자와 안전한 채널을 확립하여 안전한 통신을 할 필요가 있을 경우 먼저 키 센타에 대화키를 요구하면 키 센터는 임의의 대화키를 생성하여 두 사용자와의 각 비밀키로 암호화한 동일한 대화키에 대한 두 개의 다른 암호문을 요구한 사용자에게 전송하여 준다. 이를 받은 사용자는 통신하고자 하는 상대방에게 상대방과 키 센터사이의 비밀키로 암호화된 대화키의 암호문을 전송하여 대화 키 분배가 수행된다. 이 방식은 소규모 네트워크에서는 효율적이나 네트워크의 사용자가 많을 경우 키 센터에 대한 트래픽 혼잡 문제와 키 센터에 문제가 있을 때 어떤 채널도 확립할 수 없다는 문제가 있으며, 계층적 키 관리 방식은 이런 문제를 해결하기 위해서 개선된 방식이다. 계층적 키 관리 방식은 각각의 지역에 중앙 키 센터를 두고 이 센터들을 영역, 전역의 순으로 트리 구조 형태의 계층적으로 구성하는 방식이다. 이 방식은 다수의 키 센터를 유지 함으로서 중앙 집중식 키 관리 방식의 문제점은 해결할 수 있으나 사용자가 매 통신 시마다 키 센터와 통신하여야 한다는 문제점은 여전히 존재한다.

공개 키 암호화 시스템은 암호화와 복호화에 서로 다른 키를 사용하며 이 시스템은 공개된 암호화 키로 전문을 암호화하여 송신하면 지정된 수신자만이 복호화 키를 이용해서 전문을 해독할 수 있으므로 관용 키 시스템에서의 비밀 키 유지 문제는 해결된다. 그러나, 키 관리가 적절히 수행되지 않는다면 네트워크상의 모든 사용자의 공개 키를 스스로 관리해야 한다. 이로 인해서 관용 키 시스템에서와 같은 문제를 가지며 이의 해결을 위해서 키 센터를 이용할 수 있으나 이것 또한 관용 키 시스템에서와 같은 문제가 있다. 그래서 공개 디렉토리의 계층적 구조와 분산 특성을 고려해서 인증표를 이용하는 키 관리 방식이 있다. 인증표는 인증하고자 하는 공개키를 CA (Certificate Authority)의 비밀키로 암호화하여 서명함으로써 인증표가 지니는 공개키의 유효성을 증명한다. 사용자들은 CA의 공개키로 인증표의 서명을 복호화 함으로써 인증표의 부정 여부를 판단하고 인증표가 지니는 공개키를 신뢰할 수 있게 된다. 인증표는 정보를 계층적이고 분산적으로 관리해서 시스템의 저하를 가져

오지 않고 누구나 쉽게 접근할 수 있는 공개 디렉토리에 저장된다. 이와 같은 키 관리 시스템에서의 과정은 우선 통신을 원하는 사용자가 통신하고자 하는 상대방의 인증표를 공개 디렉토리로부터 얻는다. 그리고 사용자는 인증표가 지니는 CA의 디지탈 서명을 검증하여 공개키의 유효성을 판단한다. 만약 공개키가 유효하다면 전문을 공개키로 암호화하여 상대방과 통신함으로서 안전한 채널을 확립 할 수 있다.

공개키 암호화 시스템은 키 관리 측면에서 관용키 암호화 시스템에 비해서 많은 장점을 가지나 암호화 및 복호화에 많은 부하를 가져오는 단점이 있다. 그래서 이런 단점을 보완하기 위해서 두 시스템을 혼용해서 사용할 수 있다. 우선 공개키 암호화 시스템을 이용하여 안전한 채널을 확립한 후 대화키를 생성하여 확립된 안전한 채널을 경유하여 전송함으로서 관용키를 이용한 안전한 채널을 확립하는 방법이다. 즉, 대화키의 암호화는 공개키 시스템을 이용하고 전문의 암호화에는 관용키 암호화 시스템을 사용하는 것이다.

3.2 제한수신 시스템의 키 관리 특성

키 관리 방식은 사용되는 암호화 시스템 이외에 사용되는 통신 채널의 특성과도 밀접한 연관이 있기 때문에 통신 환경의 보안 서비스 제공을 위해 키 관리 방식을 선택하기 위해서는 사용되는 통신 채널의 특성을 고려해야 한다. 제한 수신 시스템에 적용되는 방송 환경은 방송측에서 수신측에 일방적으로 정보를 송신하는 단방향 채널이며 하나의 송신자가 다수의 시청자에게 동일한 정보를 송신하는 일대다 채널이다. 이런 방송 채널의 특성은 일반적인 네트워크상에서의 키 관리와는 다음과 같은 차이점이 있다.

- 일반적인 네트워크상에서는 통신자간의 신뢰성이 보장 되지 않았지만 제한 수신 시스템에서는 시청자는 방송자를 절대 신뢰 해야 한다는 가정 아래 방송측이 키 서버 역할을 수행 할 수 있다.
- 일반적인 네트워크 환경에서 사용되는 기존의 키 관리 방식은 상호 인증 과정이 포함되는 handshaking이 필요하나 제한 수신 시스템에서는 단 방향 채널을 사용하기 때문에 handshaking이 불가능 하다.

3.3 제한 수신 시스템의 키 관리 방안

키 관리 방안에는 여러 가지가 있을 수 있으나 방송 환경에서 키를 분배하기 가장 용이한 방법은 송신될 모든 정보를 하나의 키로 암호화하여 방송하는 것으로서 실제적으로 키 분배가 존재하지 않으며 구현이 매우 간단하다. 그러나 하나의 키를 사용 함으로서 보안상의 문제점이 있으며 가입자의 추가나 삭제를 위해서 별도의 절차가 필요하다.

두번째 방안은 방송하고자 하는 정보를 각 사용자의 비밀키로 암호화 한 뒤에 연결하여 방송하는 방법으로 구현이 용이한 편이며 가입자의 추가 및 삭제 또한 용이하다. 그러나 가입자의 증가에 따른 방송 정보의 크기가 선형적으로 증가 함으로서 현실에 적합하지 못하다.

제한 수신 시스템에서 키 관리 설계시 중점을 두는 점은 새로운 가입자의 추가나 기존 가입자의 삭제를 용이하게 하고 가입자 증가에 따른 메시지의 증가를 최소화하는 것이다.

이를 위해서는 서비스 및 과금 형태에 따라 그룹을 형성하고 키를 공유해야 한다. 따라서 공유되는 그룹 키의 갱신 및 그룹내에서 특정 가입자의 삭제는 문제시 될 수 있다. 가입자의 추가 및 삭제의 용이함을 위해서 키의 체계를 계층적 단계를 두고 분배 하는 것이 효율적이다. 즉 실제 서비스 요소는 각 그룹별로 Group Key로 암호화하고 자격을 가진 가입자들에게 해당 Group Key를 각 가입자의 고유한 Private Key를 이용하여 암호화하여 전달하는 것이다. 가입자의 추가시에는 새로운 가입자에게만 그룹 키를 전달하면 되므로 메시지 증가의 부담이 크게 감소한다. 특정 그룹에서 가입자의

삭제는 그룹이 공유하는 Group Key를 갱신 함으로서 용이하게 해결할 수 있다.

키 분배시 사용되는 알고리즘은 관용키 알고리즘과 공개키 알고리즘 모두 사용될 수 있으며 관용키 알고리즘을 사용할 경우에는 가입자는 자신이 가입한 모든 방송국과의 secret key를 유지 해야 하며 이는 새로운 방송국에 가입하고자 할 때 스마트 카드에 새로운 정보를 입력해야 한다. 모든 방송국이 가입자의 Master Key를 공유할 수 있으나 보안상 취약할 수 있으므로 방송국의 안전성이 요구된다. Public Key를 사용할 경우에는 사용자는 자신의 스마트 카드에 단지 자신의 비밀키만을 보관하고 방송국들에게는 사용자의 가입 여부에 따라 사용자의 공개키를 유지하여 마스터키로서 사용하면 된다.

3.4 제한 수신 시스템의 키 계층 구조

키 관리 시스템은 4개의 계층으로 구성되며 상위 계층부터 제어 단어(Control Word), 세션 키(Session Key), 분배 키(Distribution Key), 마스터 키(Master Key)의 순으로 구성 된다. 각 키는 자신의 상위 키를 암호화하여 분배 하는데 사용되며 역활 및 특성은 다음과 같다.

가. 제어 단어(Control Word)

제어 단어는 방송 프로그램을 스크램블링 하기 위하여 사용되며 서비스 채널별로 고유하다. 높은 안전성을 얻기 위해서 제어 단어는 자격 제어 메세지를 이용해 메세지 전송시 짧은 주기(10초이내)로 매번 갱신 되어야 한다.

나. 세션 키(Session Key)

세션 키는 제어 단어의 암호화에 사용되며 가입자의 그룹 형성에 따라 각 가입자에게 고유하거나 각 그룹에 고유하다. 이 키는 사용자에게는 비밀로 유지되며 자격 관리 메세지를 이용해서 약 한달 주기로 갱신된다.

다. 분배 키(Distribution Key)

분배 키는 세션 키의 암호화에 사용되며 가입자의 그룹 형성에 따라 개인 키(Private Key) 와 그룹 키(Group Key)로 구분된다. 개인 키는 가입자 주소로 식별되는 각 가입자에게 고유하며 그룹 키는 그룹 주소로 식별되는 개별 그룹에 고유하다. 키는 스마트 카드내에 저장되며 가입자에게 공개되어서는 않되며 필요시 자격 관리 메세지를 이용해서 갱신 될수 있다.

라. 마스터 키(Master Key)

마스터 키는 분배 키의 암호화에 사용되며 가입자 주소로 식별되는 각 가입자에 고유하다. 키는 스마트 카드내에 저장되며 사용자에게 공개 되어서는 안되며 스마트 카드의 라이프 싸이클 동안 변경 되지 않는다.

3.5 제한 수신 시스템 키 분배 절차

키 분배 절차는 마스터 키의 발급, 분배 키 분배, 세션 키 분배 그리고 제어 단어 분배의 절차로 행해진다.

1) 마스터 키 발급

가입자가 스마트 카드를 발급 받으면 스마트 카드 내에는 라이프 싸이클 동안 변하지 않는 마스터 키가 저장되어 있으며 가입자가 등록한 방송국은 이와 동일한 마스터 키를 관리 해야 한다. 마스터 키는 분배 키의 분배 및 갱신과 송금 및 과금 정보의 보호에 사용된다.

2) 분배 키 분배

분배 키는 그룹 키와 개인 키로 구분되며 세션 키의 암호화에 사용된다. 가입자가 처음 가입시 EMM-S(MK[GK,H]) 나 EMM-U(MK[PK,H])를 이용하여 획득하며 그룹내의 가입자 변동시 EMM-S를 이용하여 갱신되며 보안을 위해서 EMM-S 나 EMM-U 를 통해서 약 한달 주기로

갱신된다. EMM-S 와 EMM-U 메세지내의 H 값은 메세지의 무결성을 위한 단방향 해쉬 함수 값이다. 가입자는 방송된 EMM 메세지를 수신하여 자신의 마스터 키 MK로 메세지를 복호화 하고 해쉬 함수로 H를 생성하여 전송되어온 H 값과 비교한 후 분배 키를 획득한다.

3) 세션 키 분배

세션 키는 제어 단어의 보호를 위해 사용되며 서비스 채널별로 고유하다. 프로그램 방송시 개별 가입자 또는 가입자 그룹에 대하여 분배 키로 암호화되어 EMM 메세지에 실려 방송된다. 가입자는 EMM 메세지를 수신하면 이미 획득된 자신의 분배 키로 메세지를 복호화 하고 H 값을 생성하여 수신된 H 값과 비교하여 검증한 후 세션 키를 획득한다.

4) 제어 단어 분배

제어 단어는 실제 방송 프로그램을 스크램블링하는데 사용되며 서비스 채널 별로 고유하고 방송시 ECM 메세지에 실려 방송된다. 가입자들은 이미 분배된 세션 키로 이 메세지를 복호화 한 후 제어 단어를 획득하여 스크램블된 프로그램을 디스크램블 하는데 사용한다.

IV. SimulCrypt와 MultiCrypt 비교

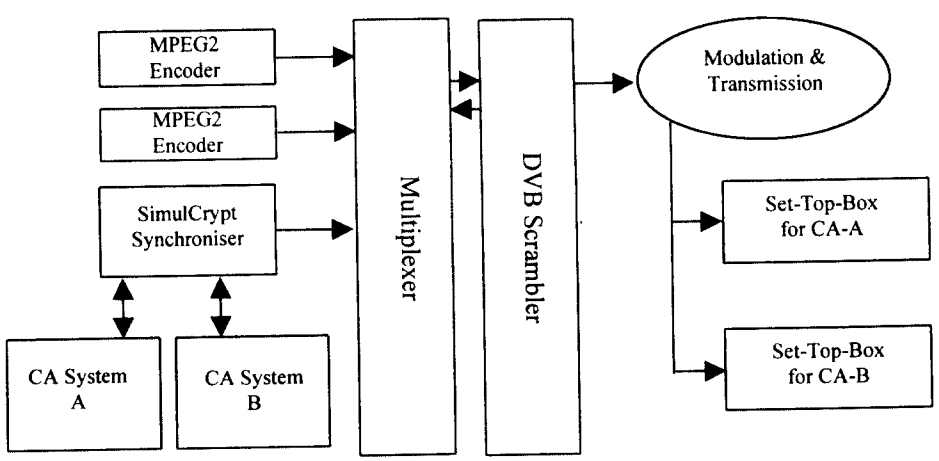
DVB(Digital Video Broadcasting)에서는 디지털 방송에서 표준화 되지 않은 부분이 제한수신시스템(Conditional Access System)임을 인식하고 많은 논의가 있었으나, 결국에는 시스템의 보안성, 서비스방식의 다양화, 시장 경쟁원리 등을 고려하여 하나의 시스템으로 표준화하지 않고, SimulCrypt와 MultiCrypt라는 두 가지 방식을 제안하였다.

4.1 SimulCrypt

SimulCrypt는 Scrambling으로 DVB Common Scrambling Algorithm을 사용하고, 제한수신메시지(ECM, EMM등)의 전송시 기본구조 및 사용 PID(Packet IDentification)를 명시한 방식이다.

SimulCrypt방식의 구조는 아래의 그림과 같다. 같은 Scrambling방식을 사용하므로 하드웨어적으로는 어느정도 통일을 기할 수 있다. 동일 스트림내에 각기 서로 다른 제한수신 시스템을 운용하는 것도 가능하므로, 광대역 서비스 제공 시 동일한 스트림을 이용하여 각 지역에 맞는 제한수신 시스템을 사용할 수 있다. 또한 제한수신시스템이 해킹 되어 새로운 시스템으로 이전할 경우 서비스 중단 없이 이전할 수 있는 방법으로써도 이용될 수 있다.

(그림 2) SimulCrypt



SimulCrypt방식은 News Digital Systems사의 주도로 1997년 초에 유럽 각국의 정부관계자, 방송관계자를 대상으로 시연을 한바 있다. 이 시연에서는 Canal+, News Datacom, Irdeto의 3개 제한 수신시스템이 사용되었고, DMV 송신장비와 Intelsat 위성을 사용하여 영국, 네덜란드, 프랑스에서 진행되었다. 또한 미국에서 열린 NAB'97에도 News Digital Systems와 Canal+가 전시를 한바있다.

4.2 MultiCrypt

MultiCrypt방식은 제한수신모듈(수신기내에 장착 또는 수신기와 연결될 수 있는 제한수신 관련 부분)과 수신기의 인터페이스를 표준화(Common Interface) 함으로써, 수신기는 제한수신시스템과 관계없이 공통화를 이룰 수 있도록하는 방식이다.

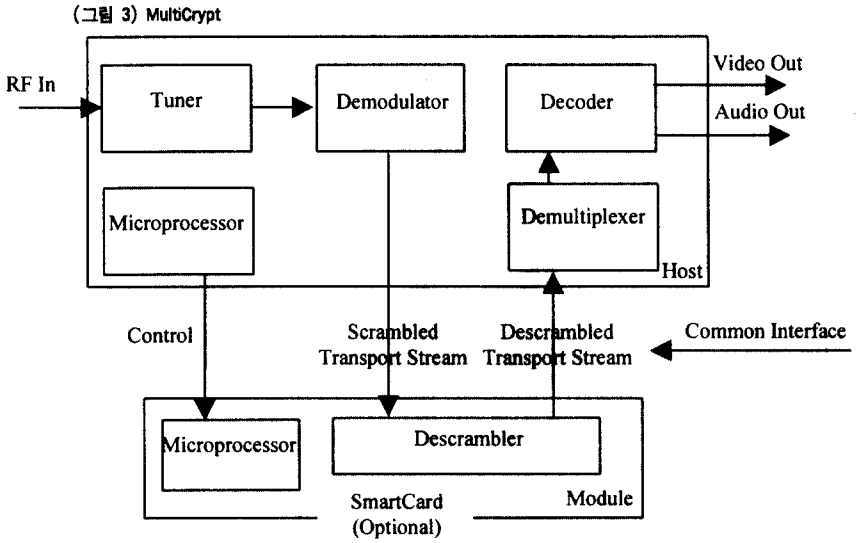
표준 인터페이스로는 PCMCIA가 사용되며, 제한수신모듈내에는 일반적으로 Control Processor와 Descrambler 그리고 option으로 SmartCard 인터페이스가 있을 수 있다. Descrambler와 Control Processor가 내장되어 있으므로 스크램블링 알고리즘과 제한수신 메시지 처리방식은 독자적인 것을 사용할 수 있다. 아래 그림은 인터페이스 부분과 간략한 신호흐름을 보여준다.

MultiCrypt방식을 이용할 경우 스크램블링 방식과 메시지 처리 방식등이 외부에 알려지지 않음으로써 SimulCrypt방식보다는 보안성이 높다고 할 수 있는 반면, PCMCIA모듈이 추가 됨으로써 서비스 사업자의 부담이 증가하는 단점이 있다.

PCMCIA moudle을 공급하는 것으로 DVB에 보고된 업체는 1997년 말 현재 Gemplus, Matra, SCM Microelectronics등이 있다.

(그림 4) PCMCIA Module

(그림 3) MultiCrypt



4.3 비교

SimulCrypt든 MultiCrypt든 강제적인 표준은 아니며, 어느 방식이 보다 우월하다고 볼 수 없다. 방송여건 및 사업방향에 따라 원하는 것을 선택할 수 있다.

한 예로, 방송신호가 서로 다른 매체를 이용하여 재전송되는 경우(예를 들면, 위성에서 케이블로)를 가정하면, SimulCrypt에서는 중계 장비에서 스트림을 descramble/rescramble할 필요없이 제한수신 메시지만 추가 혹은 변경해주면 되지만, 제한수신 사업자간의 Control Word등의 정보를 공유해야 함으로써 보안문제를 야기할 수 있다. MultiCrypt에서는 관련정보를 서로 공유하지 않으므로써 좀더 안전한 방식이라고 할 수 있는 반면, 중계 장비에서 스트림을 descramble/rescramble해야 하는 부담이 있다.

V. 결 론

지금까지 살펴 본 CAS 시스템은 위성을 이용한 디지털 위성방송에서 뿐만 아니라 CATV(Cable TV)에도 적용할 수 있다. 최근 방송 추세는 채널마다 전문성을 지니며 다른 방송과 구별이 되는 전문 방송채널의 확대 및 방송 사업자의 수입을 광고료에 의존하지 않고 가입자의 시청료에 의존하여 방송 내용의 질적 차별화를 추구하고 있다.

또한, 데이타의 전송 방식에 있어서도 기존의 아날로그 방식에서 탈피해 디지털화로 나아가고 있으며, HDTV등 보다 나은 화질과 음질등 고 품질의 서비스 제공을 추구하고 있다. 이런 추세에 직접위성방송과 CATV 같은 방송 기술 및 제한 수신 기능의 지원을 위한 기술은 필수적이며 잠재적으로 매우 높은 부가 가치를 지니고 있다.

그러나 이와 관계된 기술은 유럽을 비롯한 선진국들의 점유물로 되어 있어 기술 보유국들의 기술에 대한 횡포 또한 만만하지 않은 상황이고, CAS 시스템이 가지는 시스템 특성상 기술 도입시 막대한 기술료와 매월 지불 해야만 하는 security fee는 국민 경제에 막대한 영향 뿐 아니라 유료 방송 실시에 있어 초기 시스템 도입에 따라 기술의 종속성은 영영 탈피하기 어려운 상황이 예상되었다.

CAS시스템은 끊임없이 외부로부터 해킹의 가능성에 대비하여야 한다.

국내에서도 디지털 위성방송에서의 유료 방송을 위한 CAS 시스템인 DigiPass가 개발된 상태이며, 국내 유료 서비스를 대비하여 표준화가 시급한 상황이다.

[참고 문헌]

1. The DVB Conditional Access Package, http://www.dvb.org/dvb_standard/dvb_dvbca.htm

2. Functional model of a conditional access system, EBU Technical Review No.266, Winter 1995/6.

3. Technical Specification of DVB SimulCrypt, DVB Document A028, May 1997.

4. Common Interface Specification for conditional access and other digital video broadcasting decoder applications, DVB Document A017, May 1996.

5. H.S.Cho "Conditional Access System for digital multimedia DBS" APSCC'96 Nov. 5-8

6. 조현숙,임춘식,"DigiPass : KoreaSat DBS의 Conditional Access System" 전자공학회지, VOL. 22 NO.7, 1995

조 현 숙

• 1976년 전남대학교 수학과 졸업
• 1991년 충북대학교 전산학과 석사
• 1982년 ~ 현재 ETRI 무선방송연구소 방송기술연구부 책임연구원