디지털 위성방송 시스템에서 유료 TV방송 프로그램 접근제어

박 정 현[†] · 이 상 호[††]

요 약

본 논문에서는 디지털 위성 방송 시스템에서 유료 전문 채널/방송 프로그램 보호를 위한 접근제어 시스템을 정의 하였다. 접근제어 기능 구현을 위해 전송 레벨에서의 스트림 구조와 선택 기능을 분석하여 접근제어에 있어 가장 중요한 스크램블링/디스크램블링 기능을 정의하였고 접근제어 시스템 구조와 동작을 제시한 후, 자격 통제 메시지와 자격관리 메시지 구조를 각각 기술 하였다. 또한 접근제어의 일환으로 가입자 인증을 위해 스마트 카드 고유번호와 가입자 ID에 기초한 Fiat-Shamir 인증 방식과 Guillou-Quisquater 인증 방식을 제안 하였다. 제안된 인증 방식은 디스크램블러 고유번호나 가입자 ID에만 기초했을 때의 문제점을 해결할뿐 만 아니라 스마트 카드 이용 환경에 매우 효율적이며 안전성면에서도 매우 높다.

Access Control of Pay TV Program in Digital Satellite Broadcasting System

Jeong Hyun Park[†] · Sang Ho Lee[††]

ABSTRACT

In this paper, we describe access control system for protection of pay TV program in digital DBS (Direct Broadcast Satellite) system. We also propose a possible access control system and operation scenario for scrambling and descrambling which are important in access control system. Transport stream structure and option, entitlement checking message and entitlement management message for access control on digital broadcasting system are described in this paper. Especially, the authentication based on Fiat-Shamir and Guillou-Quisquater schemes required for verification of proper subscriber as access control is oriented to smart card number and subscriber ID(Identity). It has less restriction than scheme oriented to descrambler number.

1. 서 론

원래 다양한 형태의 방송서비스 제공, 난시청 지역의 TV 시청, 그리고 보다 화질 좋은 방송 프로그램의 보급 차원에서 시작된 위성 방송은 MPEG (Motion Picture Expert Group) 엔코딩/디코딩 기술의 발전으로 음성/영상/데이터의 디지털 전송이 가능케 되어 화질 좋고 다양한 전문 방송 채널의 출현과 함께 유료 TV 방송 보급의 큰 전환기를 갖도록 하고 있다. 그러나 유료 TV 방송 프로그램이 보다 일반화되고 상업적이면서 대중적인 오락 문화 보급으로 기여되기 위해서는 방송 프로그램 공급자에 의해 제작된 전문 방송 프로그램이 정당한 이용자에 한해서만 시청

† 정 회 원:한국전자통신연구원 이동관리연구실
†† 정 회 원:충북대학교 전자계산학과
논문접수:1997년 7월 15일, 심사완료:1997년 10월 27일

이 가능하고 비권한자의 시청을 막으면서 미가입자도 필요에 따라 언제든지 등록하여 전문채널/프로그램 시청이 가능하도록 디지털 위성 방송 시스템이 준비되어야 한다. 이를 위해 필요한 것이 유료 TV 방송 시스템에서 프로그램 보호를 위해 적용할 수 있는 접근제어 기술이다. 위성 방송 시스템에서 유료 방송 서비스/프로그램 보호를 위한 접근제어 기술은 매우 안전해야 하며 가입자의 가입과 이용이 쉽고 수신 품질에 손상을 주어서는 안 된다.

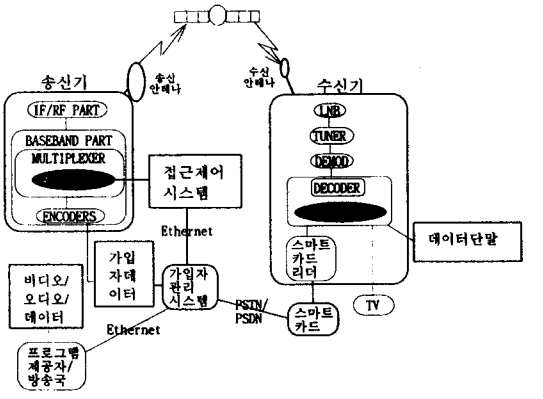
현재 미국, 유럽, 그리고 일본에서는 위성방송을 이용한 전문 방송 채널이 운영되고 있으며 유료 방송 전문 프로그램이 실용화되고 있다.

본 논문에서는 디지털 위성방송 시스템에서 유료 TV 방송 프로그램 보호를 위한 접근제어 시스템을 분석하고 필요한 동작 기술을 제시한다. 또 보호기능을 위한 트랜스포트 스트림을 분석 하고 자격관리에 필요한 메시지 구조를 정의 한다. 그 밖에 유료 TV 방송 프로그램 보호를 위한 접근제어 방법과 접근제어의 일환으로 정당한 가입자 검증을 위한 수신기와 스마트 카드간의 인증 방식을 제안 한다.

2. 디지털 위성방송시스템에서의 접근제어

본 소절에서는 송신기에서 스크램블되어 전송된 프로그램/데이터 신호를 수신측에서 수신 인가를 받은 가입자만이 소유한 디스크램블링 키로 프로그램을 복호화하여 시청할 수 있도록 하는 접근제어 시스템의 기본 구성과 동작 형태를 제시한다. (그림 1)은 접근제어 기능이 고려된 디지털 위성 방송 시스템의 기능적 블럭 다이어그램을 나타낸 것이다.

- 송신기:프로그램 및 데이터를 받아들여 엔코딩하고 MPEG 트랜스포트 스트림으로 만든 후 스크램블링하여 멀티플랙서로 보낸다. 이를 변조하여 신호 주파수대를 Ku 밴드로 전환하여 파워를 높여 위성으로 발사해 주는 기능을 한다. 입력으로는 아날로그 혹은 디지탈 프로그램 신호를 모두 받아들이고 데이터의 경우도 동기 및 비동기 경우를 모두 수용한다.
- 프로그램 제공자:프로그램을 직접 제작하거나 다른 제공자들로부터 프로그램을 구하여 제공한다. 접근제어 수신이 필요한 프로그램에 대해서는 접근 조건을 정의하여 프로그램 관련 정보를 가입자 관리시스템으로 보낸다.
- 가입자 관리시스템:프로그램 제공자의 요구와 가입자 관리시스템에서 정의한 관련 정보에 따라 권한키와 분배키, 그리고 제어문자를 생성하여 접근제어 시스템으로 보내고 가입자의 이용 상황을 관리한다. 또 접근제어 시스템과 통신하면서 자격관리 메시지와 자격통제 메시지를 받아들여 송신기 엔코더로 보낸다. 그밖에 가입자 관리에 필요한 정보를 수신자의 스마트 카드에 입력하여 프로그램 시청시 이용할 수 있도록 한다.
- 접근제어 시스템:가입자 관리시스템과 프로그램 제공자의 요구에 따라 자격관리메시지 (EMM)와 자격통제 메시지 (ECM)을 생성하여 가입자 관리 시스템으로 보낸다. 또 가입자 관리시스템에서 생성하여 보내 온 제어문자와 의사난수발생기를 통해 트랜스포트 스트림의 스크램블링 순서를 정하여 멀티플랙서로 보내 클럭에 맞추어 프로그램 데이터를 스크램블링하도록 한다.
- 스마트 카드:스마트 카드는 수신기로부터 암호화된 EMM과 ECM을 받아 가입자가 수신 자격을 갖고 있는지 확인하는 인증 기능과 EMM내의 키를 복호화하고 이 키를 이용하여 ECM으로부터 제어문자를 추출하는 기능을 갖고 있다. 추출된 제어문자를 수신기에 보내면 이를 이용해 송신기에서 전송되어 온 스크램블 된 프로그램 및 데이터를 디스



(그림 1) 디지털 위성방송 시스템의 기능적 다이어그램

(Fig. 1) Functional diagram of digital satellite broadcasting system

크램블링한다. 스마트 카드에는 가입자의 유료 TV 시청 이력 (채널 ID, 시작 시간, 끝 시간)과 가입자 정보 (가입자 ID, PIN), 암호 및 인증 알고리즘 (암호/해싱/인증), 그리고 가입자 자격 정보 (채널 ID, 자격 만료시기, 암호/인증키)등이 저장되어 있다.

2.1 접근제어 요구 조건

정당한 가입자만이 프로그램을 시청할 수 있게 하고 미 가입자의 불법 시청을 막을 수 있으면서 디스크램블링 키를 보호하는 접근제어 시스템의 기본적인 요구 조건은 다음과 같다.

- 품질:스크램블링/디스크램블링 과정이 수신된 영상/음성/데이터 신호에 크게 영향을 주어서는 안됨
- 시큐리티:미 가입자의 불법 시청을 막을 수 있는 스크램블링 방법 (비화성이 크면서 제어 문자 보호를 위한 적절한 암호 알고리즘과 키관리 방법)
- Universal conditional access:표준화된 스크램블링 알고리즘 (정당한 가입자면 어떤 수신기도 디스크램블링을 할 수 있어야 하며, 간단하고 저렴하며 융통성 있는 시스템이 되어야 함)
- End-to-end content protection:프로그램 발신지에서 수신기까지 전송되는 동안 영상/음성/데이터 신호는 프로그램별 혹은 서비스별 보호할 수 있어야 함
- 접근 모드:서비스 계약 기간, 서비스 이용 시간, 프로그램과 서비스 등급, 서비스 요금 등에 따라 다양한 제어가 되어야 함
- 시스템 표준화:시스템의 공통 기능은 표준화 되고 여러 가지 서비스 기능을 부가할 수 있도록 되어야 함 (수신기 구조는 구현하는데 융통성이 있어야 하며 회로 규모가 작고 부가 비용이 적게 들며 경제성 있고 유지/관리가 용이 하도록 만들 수 있어야 함)
- 접근 관리:권한부여 기능이 추가됨에 따른 관리나 전송상 오버 헤드가 재원의 비경제적 이용을 가져와서는 안됨
- 서비스 손상의 회피
  - 스크램블링/디스크램블링 과정에 따른 서비스 유용성에 손상이 있어서는 안됨
  - 접근제어 데이터의 잘못된 수신이나 수신 장애가 있어서는 안됨
- Interaction with digital processing:스크램블링 과정이 지나친 bit-rate reduction을 가져와서는 안됨
- Effect control:시스템은 마케팅 전략의 일환으로 프로그램 공급자에게 가능한 신호 범위를 허락할 수 있어야 함

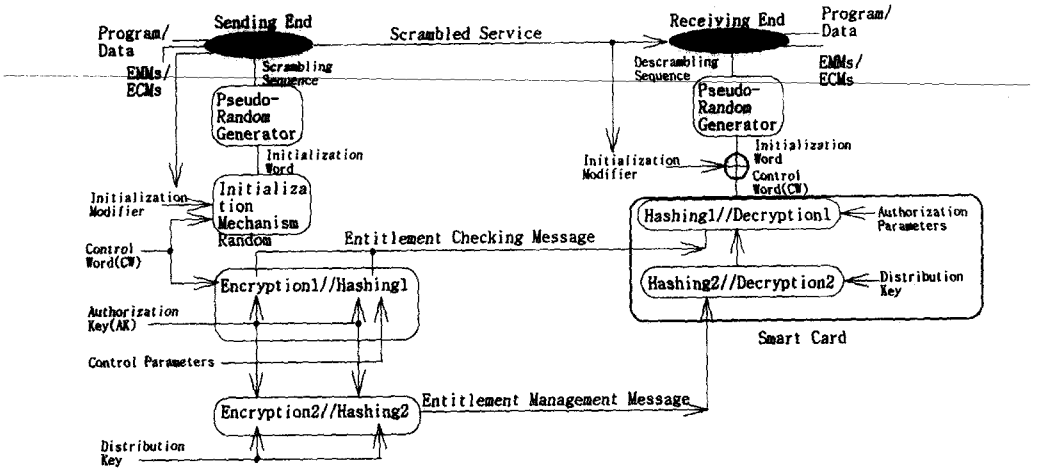
2.2 접근제어 기능

접근제어 시스템의 주요 기능은 프로그램과 데이터 신호 보호를 위한 스크램블링/디스크램블링 기능, 권한 받은 수신자에게만 시청이 가능하도록 프로그램 접근에 필요한 각종 정보를 부여하는 자격 관리 및 통제 기능이 있다.

- 스크램블 기능:송신측에서 접근제어 시스템의 제어하에 프로그램이나 데이터 내용의 특성을 변형하여 비인가 된 수신자에게는 서비스 내용이 가치가 없게 하는 것을 말하며 보통 디지털 데이터의 전송 속도와 비선형성을 고려하여 의사랜덤발생기에서 생성한 스트림과 데이터를 exclusive-OR하여 처리한다. 이를 스크램블이라 하며 디스크램블은 제어문자를 소유한 수신기에서 스크램블 된 신호를 원래의 신호로 복원하는 과정을 말한다.
- 자격통제기능 (Entitlement Checking Function):프로그램을 디스크램블하는데 필요한 권한키를 자격이라 한다. 이 자격을 난수발생기의 초기치 인 암호화된 제어문자와 프로그램을 접근하기 위해 필요한 요구 조건을 자격통제 메시지 (ECM:Entitlement Checking Message)를 통해 분배하여 부여 한다. 이를 자격 통제 기능이라 한다.
- 자격관리기능 (Entitlement Management Function):이 기능은 수신기에서 필요한 스마트 카드에 자격을 부여하거나 갱신하는 기능과 수신자의 서비스 키를 바꾸거나 통제하는 기능을 부여한다. 이를 자격 관리 기능이라 하며 이 자격 관리 기능은 수신자격에 관한 정보관리 기능으로서 자격관리 메시지 (EMM:Entitlement Management Message)를 통해 이루어지며 비정기적 전송 혹은 우편에 의해 전달 등 배치 동작으로 수행 가능하다.

2.3 접근제어 시스템 구성과 동작

접근제어 시스템은 크게 제어문자와 가입자 권한 키 등을 암호하고 해싱하는 내부 핵심 모듈, 멀티플

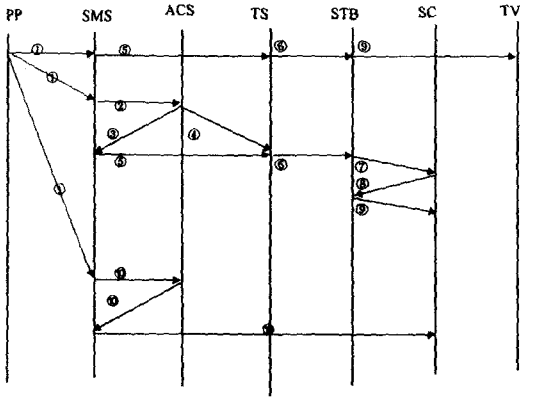


(그림 2) 접근제어 시스템의 기능적 블럭 다이어그램

(Fig. 2) Functional block diagram of conditional access system

랙서와 동기를 맞추기 위한 클럭과 제어문자를 통해 난수를 발생시키는 스크램블링 순서 발생부, 스크램블링 순서에 의해 멀티플랙서와 직접 결합하는 정합부, 가입자 관리시스템과의 정합부, 수신기 및 스마트 카드와의 정합부 등으로 구성된다. (그림 2)는 접근제어 시스템의 기본적인 블럭 다이어그램이다.

위 접근제어 시스템의 동작 순서를 살펴보면 다음과 같다.



PP (Program Provider: 프로그램 제공자/방송국)

SMS (Subscriber Management System: 가입자 관리시스템)

ACS (Access Control System: 접근제어 시스템), SC (Smart Card)

TS (Transmitter Station: 송신기), STB (Set-Top Box : 수신기), TV (Television)

① 프로그램 제공자는 프로그램과 접근제어 관련 정보를 가입자 관리 시스템과 송신기로 보낸다.

② 가입자 관리시스템에서는 내부DB에 있는 가입자 자격정보와 프로그램 제공자로 부터 받은 프로그램 접근 관련 정보를 접근제어 시스템으로 보낸다.

③ 가입자 관리시스템은 제어문자와 그밖에 EMM/ECM 생성을 위한 프로그램 및 채널 정보, 서비스 정보, 초기값, 분배키, 권한키 등을 생성하여 접근제어 시스템으로 보낸다.

④ 접근제어 시스템은 가입자 관리시스템에서 받은 정보를 이용해 EMM/ECM을 생성하고 이를 암호화하여 다시 가입자 관리시스템으로 보낸다. 또 제어문자와 멀티플랙서에서 받은 동기 클럭으로 난수 발생 순서를 정하여 멀티플랙서로 보내 송신기 엔코더에서 보내 온 트랜스포트 스트림과 exclusive-OR하여 프로그램 데이터를 스크램블한다.

⑤ 가입자 관리시스템에서는 접근제어 시스템에서 보내 온 ECM과EMM에 대해 기본 스트림을 형성해 멀티플랙서로 보내며, 이때 방송국에서 보내온 방송 프로그램은 엔코더를 통해 MPEG 스트림을 형성해 멀티플랙서로 보내진다.

⑥ 송신기는 스크램블된 프로그램정보, ECM 그리고 EMM을 위성을 통해 수신기로 보낸다.

⑦ ECM과 EMM 정보는 수신기에 준비된 스마트 카드와의 내부 통신을 통해 정당한 가입자 여부를 인

중하는데 이용되며 정당한 가입자의 경우 인증과 복호를 통해 가입자의 자격 관리 정보 및 원래 제어문자를 복원하게 된다.

⑧스마트 카드를 통해 복호화된 제어 문자는 다시 수신기로 보내져 스크램블된 프로그램을 디스크램블한다.

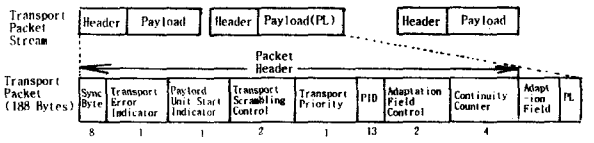
⑨이렇게 하므로 가입자는 디스크램블된 프로그램을 가입자 TV를 통해 정상적으로 시청할 수 있게 된다.

⑩또 가입자 관리시스템은 프로그램과 서비스 관련 정보, 자격 관련 정보, 이용자 ID, 복호와 해싱에 필요한 관련키, 관련 알고리즘 등을 스마트 카드에 주입하여 우편으로 혹은 동록시 발급해 주며 EMM의 비정기적인 송신을 통해 가입자의 자격관리를 조정 한다.

3. 접근제어를 위한 전송 스트림

3.1 접근제어를 위한 전송 스트림 구조

디지털 위성 방송 시스템의 MPEG-2 엔코더에서 발생하는 기본적인 전송 스트림과 스트림 내에서 접근제어 기능을 부가하기 위한 선택 기능은 다음과 같다.



트랜스포트 스트림 레벨에서 스크램블링하는 각 필드의 기능은 다음과 같다.

- Sync Byte:0100 0111 (0x47) 패턴
- Transport Error Indicator:1인 경우 트랜스 포트 스트림 패킷내에서 교정이 불가능한 에러가 발생했음을 의미
- Paylord Unit Start Indicator:PES (Packet Elementary Stream) 패킷이나 PSI (Program Specific Information)데이터를 운반하는 트랜스 포트 스트림이 정상적임을 의미('1')
- Transport Priority:같은 PID를 갖는 패킷중에서도 1인 경우 우선순위가 높음을 의미
- PID:패킷 페이로드에 저장된 데이터의 종류를 가르켜 줌
  - −PID값이 0x0000의 경우:Program Association Table
  - −PID값이 0x0001의 경우:Conditional Access Table
  - −PID값이 0x0002/0x000F의 경우:Reserved
  - −PID값이 0x00010/0x1FFE의 경우:Network PID, Program Map PID, Elementary PID등으로 할당
  - −PID값이 0x1FFF의 경우:Null Packet
- Transport Scrambling Control:스크램블링 모드를 나타냄
  - −00:Not Scrambled
  - −01:Reserved
  - −10:Even Word Scrambling
  - −11:Odd Word Scrambling
- Adaptation Field Control:트랜스 포트 스트림 패킷 헤더가 Adaptation Field나 Payload에 따라 오고 있음을 의미
  - −00:Reserved
  - −01:No Adaptation Field, Only Payload User Defined
  - −10:Adaptation Field Only, no Payload
  - −11:Adaptation Field followed by payload
- Adaptation Field는, 8 비트 Adaptation Field Length, 1비트 Discontinuity Indicator, 1비트 Random Access Indicator, 1비트 Elementary Stream Priority Indicator, 5비트 플래그, 선택적 필드, Stuffing Bytes 등으로 구성된다.
- PSI 정보는 다음과 같다.

구조 이름	스트림 형태	PID 번호	내 용
Program Association	MPEG	0x00	프로그램 번호와 Program Map Table PID 를 연관 시킴
Program Map Table	MPEG	PAT PID 로 할당	하나 이상의 프로그램 요소에 대한 PID 값 규정
Network Information Table	Private	Network PID 로 할당	물리적 네트워크 파라메터 (주파수, 트랜스 폰더수 등)
Conditional Access Table	MPEG	0x01	고유의 PID 값을 가진 하나 이상의 EMM 스트림

- 그밖에 트랜스 포트 스트림에 포함되는 Conditional Access Table의 내용은 다음과 같다.

```
CA_section( ) {
        Table_id                  8bits     uimsbf
        section_syntax_indicator  1bit      bslbf
        '0'                       1bit      bslbf
        reserved                  2bits     bslbf
        section_length            12bits    uimsbf
        reserved                  18bits    bslbf
        version_number            5bits     uimsbf
        current_next_indicator    1bit      bslbf
        section_number            8bits     uimsbf
        last_section_number       8bits     uimsbf
        for(i=0;i<N;i++){
            descriptor( )
        }
        CRC_32                    32bits    rpchof
        }
```

3.2 접근제어 메시지

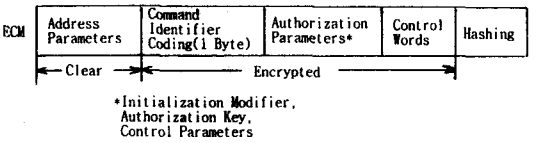
• ECM 메시지

ECM의 주요 역할은 암호화된 제어문자를 가입자 수신기로 안전하게 보내는 것이다. 따라서 가입자 통제 관련키 정보, 제어문자, 그리고 파레메터들이 암호화 및 해싱되어 보내지게 된다. ECM은 정보 운영 모드를 다음과 같이 나누기도 한다.

- No ECM at all (modes 0 and 1)
- One new ECM every block (mode 2)
- Several new ECMs every block (mode 3)

그리고 수신단에서는 디코더가 가입자가 선정한 프로그램에 대한 ECM을 찾아 수신자의 자격을 점검하고, 제어문자를 계산하기 위해서 그 메시지를 스마트 카드로 보낸다. 또 제어문자를 얻기 위해 전송 및 계산상의 지연을 고려하여 적어도 150 ms이전 수신자의 스마트 카드로 ECM이 보내져야 하며, 이러한 문제의 해결을 위해 실질적으로 두개의 ECMs (현재 제어문자, 다음 제어문자)을 사용하기도 한다. 그밖에 스트림을 구성하는 ECM의 메시지 구조를 보면 다음과 같다.

- 제어문자 인덱스
- 제어문자 변경 플래그 (액티브 제어문자 표에 따른 표시)
- 권한 지시기 (권한키 확인)
- 제어 파라메터 (유효기간, 가격 등 권한 파라메터)
- 암호화된 제어문자
- 데이터 필드 길이
- 알고리즘 종류
- 해싱 자료



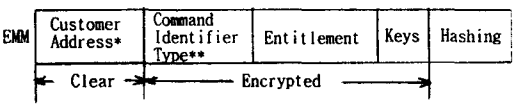
• EMM 메시지

가입자의 자격을 검증하고 관리하는 EMM은 비정기적으로 방송 혹은 우편 전달되며 크게 EMM-G (General), EMM-S(Shared), 그리고 EMM-U(Unique) 형태로 보내진다.

- 모든 이용자에게 EMM-G (어드레스 없이)
- 그룹 이용자에게 EMM-S (Shared address)
- 특정 가입자에게 EMM-U (Unique Address)

그밖에 EMM메시지를 구성하는 내용은 다음과 같다.

- 서비스 관련 정보
- 어드레스
- 데이터 필드 길이
- 최대 응답 길이
- 알고리즘 종류
- 권한 키
- 자격 정보
- 해싱 자료



* : 3-5 Bytes(24 bits for EMM-S, 40 bits for EMM-U)
** : 1 Byte(Crypto-Algorithm type등)

4. 접근제어를 위한 가입자 인증

4.1 접근제어 형태

정당한 가입자 여부를 확인하고 미등록 가입자에게는 프로그램을 시청 할 수 없도록 막아 주는 접근제어 기술은 제어 방식이 크게 스크램블/디스크램블 형태와 자격 통제/관리 메시지를 통해 이루어지며, 이를 뒷받침하기 위해 트랜스포트 스트림 구조에서의 선택 기능과 자격 통제/관리 메시지 구조를 정의한다. 그리고 운영 형태에 따라 EMM-U의 메시지 내에서 권한키 갱신, 프로그램 번호, 그리고 등록을 통한 접근제어 방법이 있다. 그리고 이용자는 ❶전문 프로그램을 수신기를 통한 등록 모드 설정, ❷예약을 통한 프로그램 번호에 의한 시청, ❸임펄스 Pay per view 신청에 따른 프로그램 번호에 의한 접근를 통해 시청할 수 있다. 이 3가지 모두는 수신된 ECM 메시지를 통해 수신기와 스마트 카드간의 인증과 복호 등의 과정을 거치게 된다. 따라서 유료 TV 방송 가입자는 기본적으로 ❶해싱을 통한 서명과 올바른 가입자 여부 확인, ❷권한키의 정당 여부를 확인하는 인증, ❸인증을 통해 얻은 암호화된 제어문자의 복호, ❹복호된 제어문자를 통한 디스크램블링 등의 내부적인 기술적 접근 과정을 거쳐 정당한 가입자로 검증 받은 후 전문 유료 TV 방송 프로그램을 시청하게 된다. 이와 같은 과정은 수신기와 스마트 카드를 통해 짧은 시간 안에 모두 처리 가능하다.

4.2 Fiat-Shamir(FS) 방식을 이용한 가입자 인증

접근제어 시스템에 적용하는 인증 방식은 가입자 ID기초한 Fiat-Shamir 인증 방식이나 디스크램블러 고유번호에 기초한 인증을 고려해 볼 수 있다. 그러나 디스크램블러 고유번호에 기초될 경우 유료 TV 시청시 자신의 수신기를 갖고 다녀야 하는 문제점을 갖게 되며 또 수신기의 도난 혹은 대여 시 유료 방송 프로그램의 불법 시청이 가능하게 된다. 또한 자신의 ID에 기초한 경우 스마트 카드 주입시 자신의 ID정보가 수신기에 로드 되어 이후부터는 ID의 추가 로드가 없을 경우 중고 수신기나 다른 집에서 사용했던 수신기를 사용하여 유료 방송 수신을 불법 시청할 수 있게 된다. 이런 경우를 고려하여 스마트 카드 고유번호에 기초한 인증 방식이나 혹은 기존의 ID에 기초한 방식에서 매 유료 TV시청시 마다 스마트 카드에서 수신기로 자신의 고유 ID를 로드 하도록 하는 방안이 있다. 그러나 앞으로 정보화 사회에서 스마트 카드의 역할은 현재의 신용카드 및 지불 카드 개념을 흡수하고 유료 TV 방송사에서 카드에 기초한 가입자 관리 개념의 도입이 가능하다고 볼 때, 스마트 카드 고유번호에 기초하면서 수신기에 스마트 카드 주입시 마다 자신의 ID가 로드 되는 방식이 효과적이라 본다. 이 경우 수신기와 스마트 카드간의 상호 인증 프로토콜은 다음과 같다.

과정 1: 유료 TV 방송 시청 가입 신청시 가입자는 자신이 구입한 스마트 카드를 갖고 등록을 하거나 가입자 관리시스템에서 미리 준비한 스마트 카드를 등록한다.

과정 2: 가입자 관리시스템에서는 큰 소수 p, q의 합성수 $n=pxq$와 일방향 함수 f를 준비하여 $V_j=f(I_s, j)$를 계산한다. 이때 함수 값 중 법 n상의 이차 잉여류가 되는 k개의 V_j만을 취하고 $V_j^{-1}(\text{mod } n)$의 가장 작은 자승근 S_j를 만들어 V_j, k개의 S_j값과 인덱스를 스마트 카드에 저장한다. 여기서 I_s는 자신의 ID와 해싱된 스마트 카드의 고유 번호이다.

과정 3: 또 스마트 카드에 복호 알고리즘, 인증 및 해싱 알고리즘, 난수 발생 알고리즘, 알고리즘 초기값, 권한키, 자격 정보, 그리고 서비스 관련 정보 등을 저장하여 가입자에게 전달한다.

이후 가입자는 유료 TV 시청시 다음과 같은 인증 과정을 거치게 된다.

과정 1: 스마트 카드는 랜덤 수 $R_i \in [0, n]$를 발생하여 $X_i=R_i^2 (\text{mod } n)$를 계산한 후 이를 수신기에 보낸다.

과정 2: 수신기는 랜덤한 이진 백터 $(e_{i1}, ..., e_{ik})$를 스마트 카드에 보낸다.

과정 3: 스마트 카드는 $Y_i=R_i \prod_{j=1,\ eij=1} S_j (\text{mod } n)$을 수신기로 보낸다.

과정 4: 수신기는 자신이 보관하고 있는 V_j로, $Y_i^2 \prod_{j=1,\ eij=1} V_j (\text{mod } n)=X_i$인지 확인한다. 스마트 카드는

위의 과정 4-7을 t번 통과되어야 정당한 가입자로 인증된다.

위의 인증 프로토콜은 사용자 A (수신자, 스마트 카드)가 자신의 비밀키에 대한 정보를 전혀 누출시키지 않고 사용자 B (송신국)에게 증명하는 과정으로 사용자 B는 위의 모든 과정을 올바르게 통과했을 때만 A의 신원을 인정한다. 이는 확인자 B가 증명자에게 임의의 질문을 하였을 때 증명자 A가 올바른 비밀키를 가지고 있을 때만 대답할 수 있도록 프로토콜을 구성하였기 때문이며 이와 같은 조건은 인증 프로토콜의 생명이라 할 수 있다. 위의 인증 프로토콜은 고정된 k와 임의의 t에 대해 영지식 프로토콜이라는 사실이 증명되었으며 비밀키를 모르는 제 3자가 인증 과정을 성공하려면 이진백터 $(e_{i1}, e_{i2},..., e_{ik})$를 미리 예측할 수 있어야 하므로 그 확률은 2^{-kt}가 될 것이다. 따라서 이 프로토콜의 안전성은 kt 값에 전적으로 의존하게 된다. 보통의 안전도를 요구하는 응용에서는 kt의 값이 30 정도이면 비밀키를 모르는 사람이 위 과정을 통과할 확률은 10^{-9}이므로 충분하다고 할 수 있다. 만약 t=1, k=30으로 둔다면 이때 증명자와 확인자는 단지 15번 정도의 모듈러 곱셈이 필요하다. 또 t=30, k=1로 둔 경우는 필요한 메모리는 512비트에 불과하지만 약 45번의 모듈러 곱셈과 30 k비트의 전송량이 필요하므로 비밀키의 크기와 전송량 사이는 서로 상충 관계가 성립함을 알 수 있다. 위 인증 방식의 안전성은 FS 인증 기반을 두기 때문에 매우 높으며[8], 효율성 측면은 기존의 디스크램블러에 기초한 방식이나 가입자 ID 기초한 방식의 장점만을 병행한 스마트 카드 고유 번호와 자신의 ID를 결합한 방식을 추구하므로 더 높다 할 수 있다.

4.3 Guillou-Quisquater(GQ) 방식을 이용한 가입자 인증

GQ방식은FS방식에 비해 요구되는 메모리도 적고 인증시 필요한 통신량도 적기 때문에 스마트 카드를 이용한 위성방송 서비스의 접근제어를 위한 가입자 인증에 적합한 모델이라 할 수 있다.

다음은 GQ방식을 이용한 위성방송서비스의 접근제어를 위한 인증 과정이다.

과정 1: 가입자 관리시스템은 먼저 두개의 큰 소수 p, q를 생성하여 n=pxq를 계산한다.

과정 2: 사용자가 등록시 이름, 은행구좌번호, 카드일련번호, 유효기간 등을 규정하는 자격물 ID_i를 가입자 관리시스템에 제출하고, 가입자 관리시스템은 ID_i로 부터 사용자의 J를 f함수를 이용해 계산한다 ($J=f(ID)$, $J=(ID_i//g(ID_i))$, g는 리던던시 생성 함수)

과정 3: 가입자 관리시스템은 $\gcd(v, \Phi(n))=1$을 만족하는 v를 선택한다. 여기서 $\Phi(n)=(p-1).(q-1)$이다.

과정 4: 가입자 관리시스템은 사용자 I의 비밀키로 $S_i=J_i^{-1/v} \bmod n$ ($S_i^v . J_i = \bmod n$)을 계산하여 스마트 카드에 저장하여 사용자 I에게 전달한다.

사용자 I는 다음 과정을 통해 인증을 받는다.

과정 1: 스마트 카드는 랜덤 수 R_i를 선택하여 $T=R_i^e \bmod n$계산 후 T와 I를 수신기에 보낸다.

과정 2: 수신기는 스마트 카드로 임의의 랜덤 수 d $(0<d<v-1)$를 보낸다.

과정 3: 스마트 카드는 $X_i=R_i.S_i^d \bmod n$을 계산하여 수신기에게 보낸다.

과정 4: 수신기는 T가 $J_i^d . X_i^v \bmod n$인 같은지를 통해 정당한 가입자 여부를 인증한다.

위 인증 방식에서 사용자의 비밀키를 모르는 사람이 인증 과정을 성공하려면 질문 d를 미리 예측할 수 있어야 하며 그 확률은 1/v이다. (d를 미리 예측할 수 있다면 임의의 X를 선택하여 인증 조건을 만족하는 T를 계산할 수 있을 것이다.) 따라서 시스템의 안전성은 v의 크기에 의존하게 된다.

5. 결 론

가속화되는 정보통신기술의 발달은 정보화사회의 촉진을 유도하면서 정보와 통신, 그리고 방송을 하나로 통합하는 형태로 발전시키고 있다. 더욱이 TV방송이 지상방송 (Terrestrial Broadcasting)에서 화질의 개선과 가입자 개념의 CATV (Cable TV)방송으로 발전되고, 최근에는 인공위성의 상업적 이용 확장으로

인공위성에 의한 디지털 직접 위성방송을 도입하고 있어 통신과 방송에 있어 전송 방식이나 전송 매체에 특별한 구분이 없어지는 실정이다. 이렇듯 통신 기술의 발전이 방송을 흡수하면서 디지털 TV 혹은 디지털 레디오와 같은 새로운 방송서비스의 출현을 가능케 하고 있다. 특히 디지털 위성방송은 난시청 지역을 해소할 뿐만 아니라 더욱 좋은 화질 방송을 제공해 줄 수 있어 다양하고 전문화된 방송 채널의 탄생을 가능케 하였고 이용자 입장에서도 각자의 기호에 맞는 품질 좋은 전문 방송 프로그램을 보다 폭 넓고 다양한 범위에서 선택하여 즐길 수 있게 하고 있다. 그러나 방송의 전문화와 품질의 고급화에 따라 유료 TV 방송 프로그램이 탄생되어 방송 프로그램의 가입자 개념을 도입하게 되었다. 유료 TV 방송 채널/프로그램이 발전 되면서 필요한 것이 정당한 가입자만이 시청할 수 있도록 하고 미가입자는 불법 시청할 수 없도록 하는 접근제어 기술이다. 이에 본 논문에서는 디지털 위성 방송 시스템에서 유료 전문 채널/방송 프로그램 보호를 위한 접근제어 시스템을 분석하였다. 접근제어에 있어 가장 중요한 스크램블링/디스크램블링 기능을 위한 시스템 구조와 동작 형태를 제안하였고, 접근제어 기능을 구현하기 위해 트랜스 포트 레벨에서의 스트림 구조와 기능을 분석하여 접근제어 메시지인 자격통제 메시지와 자격관리 메시지 구조를 기술하였다. 그리고 마지막으로 접근제어를 위해 스마트 카드 고유번호와 가입자 ID에 기초한 Fiat-Shamir 인증 방식과 Guillou-Quisquater 인증방식을 제안하였다. 제안된 인증 방식은 디스크램블러 고유번호나 가입자 ID에 기초한 단독 방식의 문제점을 해결할 뿐만 아니라 스마트 카드 이용 환경에 매우 효율적이며 안전성면에서도 매우 높다[8, 9]. 스마트 카드의 이용 범위가 날로 넓혀져 가고 반도체 기술의 발달로 향후 본 연구에서 제시한 가입자 인증은 매우 효과적이라 기대한다.

참 고 문 헌

[1] D. Angebaud and J. L. Giachetti, "SCRAMBLING AND CONTROLLING ACCESS TO AN ALL-DIGITAL BROADCAST PROGRAM," CCETT, France, 1993.

[2] ISO/IEC JTC1/SC29/WG11, "Coding of Moving Pictures and Associated Audio," November 1994.

[3] G. Monnin, "SMART CARDS EXCLUSIVE ADVANTAGES IN PAY-TV," Schlumberger Technologies, France, 1994.

[4] CCITT Recommendation X 810, "Conditional-Access Broadcasting Systems," 1992.

[5] CMTT-1/7-E, "Technical Methods for Ensuring Privacy in long-distance International Television Transmission," 1990.

[6] O. Hansrold, "Eurocrypts Smart Card for Mac/Packet Television," Proc. of First Int. Seminar on Conditional Access for Audiovisual Service, pp. 266-272, 1990.

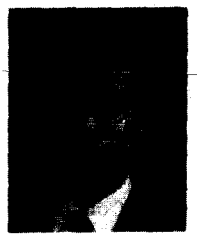
[7] J. Hashkes and M. Cohen, "Managing smart cards for pay television:the videoCrypt approach," Proc. of First Int. Seminar on Conditional Access for Audiovisual Services, pp. 214-224, France, 1990.

[8] M. Fiat and A. Shamir, "How to prove yourself: Practical Solution to Identification and Signature Problems," Proc. Crypto 86, Santa Babara, Springer-Verlag, LNCS vol. 263, pp. 186-199, 1986.

[9] L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors and Minizing Both Transmission and Memory," Eurocrypt88, Lecture notes in Computer Science, Vol. 330, pp. 123-128, 1988.

[10] Eiji Okamoto and Kazue Tanaka, "Key Distribution system based on identification information," IEEE Journal on selected areas in communications, Vol. 7, No. 4, pp. 481-485, May 1989.

[11] News Datacom, "Generic Digital TV system Description," August, 1993.



박 정 현

1982년 2월 숭실대학교 전자공학과 졸업(학사)
1985년 2월 숭실대학교 대학원 전자공학과 졸업(공학석사)
1997년 2월 충북대학교 대학원 전자계산학과 졸업(이학박사)
1982년 3월~현재 한국전자통신연구원 이동관리연구실 선임연구원
관심분야: 네트워크 시큐리티, 시큐리티 프로토콜, 이동 및 위성 통신 보안

이 상 호

1976년 숭실대학교 전자계산학과 졸업(학사)
1981년 숭실대학교 대학원 전자계산학과 졸업(공학석사)
1989년 숭실대학교 대학원 전자계산학과 졸업(공학박사)
1992년 9월~1993년 8월 Post-Doc. UBC in Canada
1981년~현재 충북대학교 전자계산학과 교수
관심분야: 프로토콜 설계, 컴퓨터 통신, 소프트웨어 엔지니어링, 암호학