신기술논고

선 지불 메커니즘을 이용한 유료 방송 서비스

김신효, 조현숙
한국전자통신연구소

— 요 약 —

디지털 위성 방송 서비스의 시작으로 방송 사업자는 다채널 및 전문 채널의 활성화로 유료 방송 서비스에 많은 관심을 가지고 있다. 본 논문에서는 이 유료 방송 서비스의 송신 및 수신 시스템의 구조에 대해 언급하고 특히 선 지불 메커니즘을 따르는 유료 방송을 위해서 스마트 카드가 어떠한 관리 기능을 포함하여야 하는지를 기술하고, 그에 따른 선지불 기능 수행 과정을 송신측과 수신측으로 나뉘어 설명하여 선지불/후지불 메커니즘 각각의 장단점에 대해 논한다.

Ⅰ 서론

케이블 텔레비전과 디지털 위성 방송 서비스의 시작으로 방송 사업자는 다채널 및 전문 채널의 활성화로 기존 광고 수입에 의존하던 서비스를 탈피하여 가입자에게 양질의 방송 서비스를 제공하고 이들로부터 시청료를 징수하는 유료 방송 서비스를 제공하려 할 것이다. 이 유료 방송 서비스에서는 시청 요금을 지불한 가입자에게만 선별적으로 서비스를 제공하기 위한 제한 수신 시스템과 별도의 가입자 관리 시스템은 필수적이며, 이의 운용은 가입자들의 시청료가 주수입인 프로그램 제공자들에게는 프로그램 가격 이외의 또 다른 비용 부담을 안겨 줄 것이다. 그러므로 이들은 방대한 가입자 관리 시스템과 과금 처리 시스템의 운영보다는 선 지불 방식 서비스를 선호할 것이다.

본 논문에서는 프로세서 형의 스마크 카드를 이용한 유료 방송 서비스의 선지불(Pre-Paid) 방식에 대하여 논한다.

Ⅱ 유료 방송 서비스

유료 방송 서비스를 위해서는 다음과 같은 구성 요소를 필요로 한다.

- 송신장비
- 유료 방송 공급자
- 가입자 관리 시스템 (SMS:Subscriber Management System)
- 제한 수신 시스템 (CAS:Conditional Access System)
- 수신기(Set-top Box)
- 스마트 카드

1. 송신 시스템의 구성

유료 방송 송신 시스템은 제한 수신 시스템과 가입자 관리 시스템 및 스크램블로를 포함하는 일련의 송신 장비로 구성된다. 유료 방송에서 필수적인 제한 수신 시스템은 자격 관리/자격 제어 메세지 및 제어 단어를 생성한다. 스크램블러와 인터페이스를 갖고 유려 방송 프로그램 공급자들로부터의 비디오/오디오/데이터 소오스를 이미 생성한 제어 단어를 이용하여 스크램블링 하여 송신 장비를 거쳐서 수신기까지 전송된다.

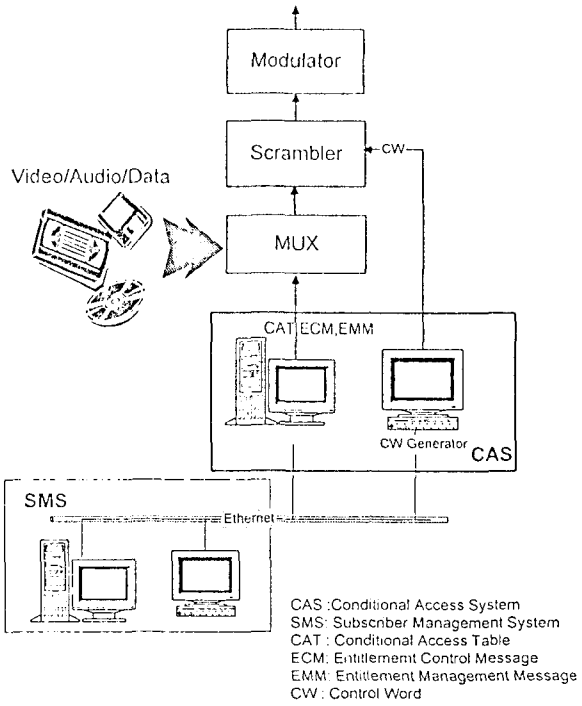

그림 1. 송신 시스템의 구성

2. 수신측의 구성

수신측은 디스크램블러를 포함하는 수신기와 가입자 권한 인증을 통해 제어 단어를 생산하는 스마트 카드로 이루어진다. 수신기는 제한 수신 메세지를 스마트 카드로 전달하며 스마트 카드로부터 정당한 가입자의 인증 후 복호화한 제어 단어를 리턴 받아서 디스램블링을 수행하고 원래의 신호로 텔레비전을 통해 가입자에게 보여 준다.

스마트 카드는 기존의 마그네틱 카드의 단점을 보완하여 프로세서 및 메모리를 내장한 카드이다. 스마트 카드의 가장 단순한 형태인 메모리 카드는 마이크로프로세서를 포함하지 않는 카드이며 이는 가격이 저렴한 반면 쉽게 읽히고 프로그램이 가능하여 보안에 취약한 약점으로 인하여 유료 방송 서비스에 이용하기에는 많은 취약점을 가진다[1].

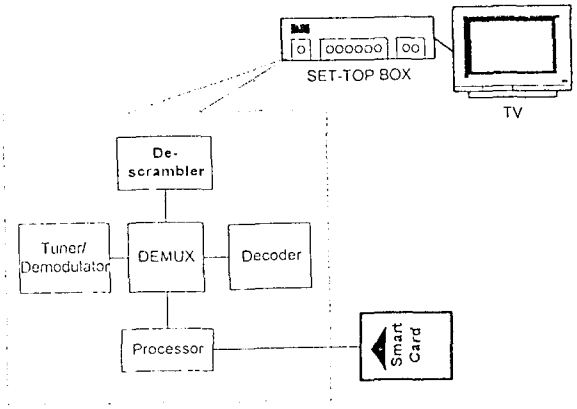

그림 2. 수신기의 구성

일반적인 스마트 카드는 응용 프로그램이 저장된 Masked ROM과 임시 데이터를 저장하는 RAM 및 가입과 관련된 정보를 저장하고 특수 복호화 알고리즘을 내장하는 EEPROM 영역과 이들 모두를 관리하는 8비트 마이크로 프로세서로 구성되어 있다.

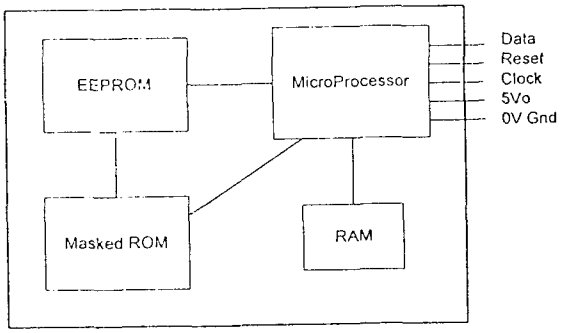

그림 3. 스마트 카드의 구조

위의 스마트 카드는 보안 관련, 사용량 기록 유지 및 토큰(Token) 관련 서비스 응용에 큰 역할을 담당할 것이다[2].

3. 유료 방송 서비스 시나리오

위의 구성을 갖는 유료 방송 시스템은 다음의 과정으로

가입자가 유료 방송을 시청할 수 있다.

먼저, 유료 방송 시청을 원하는 가입자는 가입자 관리 센터를 방문하여 가입 신청에 필요한 개인 정보를 알리고 자신의 스마트 카드를 발급 받는다.

이 스마트 카드는 가입 신청을 한 방송을 시청할 수 있는 권한이 저장되어 있다. 이 시청 권한 정보는 제한 수신 메세지 처리기를 통해 시청 권한을 가진 가입자 스마트 카드에서만 해독 가능한 자격 관리 메세지(EMM: Entitlement Management Message)형태로 암호화 과정을 거친 후 송신국으로 전송된다.

각 유료 방송 공급자는 송신국에 유료 방송 소오스를 제공함은 물론 유료 방송 정보를 제한 수신 시스템에 알린다. 여기에서는 유료 방송 스크램블에 이용할 제어 단어(CW:Control Word)를 생성하여 송신국으로 보내고 제어 단어는 암호화하여 자격 제어 메시지(ECM:Entitlement Control Message)로 만들어 송신국으로 보낸다. 송신국은 이를 이용해 유료 방송을 스크램블하고 제한 수신 메세지(EMM/ECM)와 함께 전송 매체를 이용하여 각 가정의 수신기로 보낸다.

각 가정의 수신기는 제한 수신 메세지를 가입자 스마트 카도로 보내어 복호화 하여 시청을 원하는 채널의 제어 단어를 획득하고 이를 이용하여 디스크램블 과정을 거쳐 텔레비전을 통해 시청하게 된다.

위의 유료 방송 서비스는 시청 권한의 획득 과정에 스마트 카드가 이용되었으며 유료 방송의 시청 대가인 시청료의 징수는 별도의 문제로 취급되어야 한다. 즉, 유료 방송 시청 내역을 스마트 카드의 내부에 저장하여 과금 정보로 활용할 수 있다. 시청 내역을 스마트 카드의 메모리에 저장하는 일은 카드 기술의 발전으로 가능한 일이 되었으나 주기적으로 카드의 시청 기록 내용을 중앙의 과금 처리기로 가져 오기 위해서는 별도의 return path을 이용하거나[3] 가입자가 직접 카드를 휴대하고 과금 장소를 방문하여야 한다. 이러한 이유로 과금을 위해서 카드 메모리에 시청 내용을 기록/유지하는 방식은 과금 처리 방식이 복잡성, 처리 비용부담 및 후지불로 인한 미납 가입자 처리 방안 등에 대한 신중한 고려가 필요하며 실제 서비스를 제공하는 방송 사업자들에게는 자금 압박을 가져다 줄 것이다〈4〉.

그러므로 과금 처리를 위한 부하를 줄이기 위해 집중적으로 관리하지 않는 별도의 메커니즘을 고려하여야 할 것이다. 이 새로운 메커니즘이란 유료 프로그램 시청을 원하는 가입자가 가입자 관리 센터를 방문하는 대신 지불한 비용 만큼의 유료 방송 서비스를 시청할 수 있는 권한(토큰)이 미리 입력되어 있는 카드를 구입하면 된다.

Ⅲ 선 지불 메커니즘에 따른 유료 방송 서비스

이러한 이유로 스마트 카드를 이용한 선 지불 유료 방송 서비스는 매우 유용하므로 이를 위해서 스마트 카드 내부에서 처리되어야 할 기능들과 이들을 이용한 서비스 시나리오에 대해 논하기로 한다.

먼저, 선 지불 스마트 카드의 구현을 위해서 송신측의 제한 수신 시스템은 다음의 두가지를 반드시 만족시켜주어야 한다.

1) 프로그램의 가격 정보를 스마트 카드에서 알아야 하므로 이 정보를 제어 단어와 함께 자격 제어 메세지 내에 포함하도록 하여야 한다.

2) 초기 토큰을 카드에 입력하기 위해 안전한 명령 체계가 존재하여야 한다.

1. 스마트 카드의 기능

선 지불 메커니즘을 수용하는 스마트 카드는 자신이 정당한 가입자임을 인증하기 위한 정보는 물론 카드내의 토큰 양에 대한 모니터링 및 프로그램 시청 시간만큼의 토큰을 감소해 나가는 간단한 알고리즘을 포함하고 있을 것이다.

그림 4.에서 도시한 바와 같이 선 지불 방식의 유료 방송 서비스를 위해서 스마트 카드는 다음의 기능 모듈을 포함하여야 한다.

- Input Message Filter
- EMM Manager
- ECM Manager
- Key Manager
- Token Monitor
- Output Message Generator

Input Message Filter는 수신기로부터의 데이터를 수신하여 해당 데이터의 유효성을 판단하여 적법한 입력이 아닌 경우에는 이에 대한 에러 메세지를 생성하거나 무시하도록 한다. 또 입력된 데이터가 ECM 또는 EMM일 경우에는 이들을 각 manager에게 전달한다.

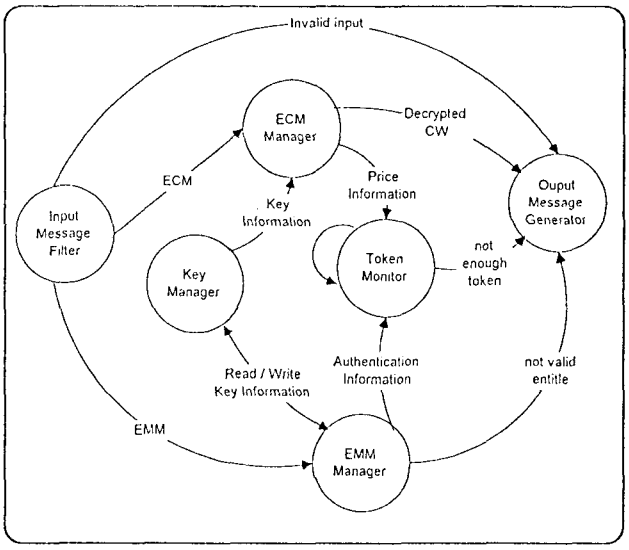

그림 4. 지불 스마트 카드의 기능 모듈

EMM Manager는 EMM을 Input Message Filter로부터 받아서 내부 암호화 알고리즘과 이미 발급 시에 저장한 암호 키를 이용하여 복호화하여 정당한 수신 권한임을 확인하는 절차를 수행한다. 즉, 정당한 가입자라면 ECM의 복호화에 이용할 암호 키를 생성하여 이를 Key Manager를 통해 저장하고 토큰에 대한 인증 확인을 주고 수신 권한이 없는 경우에는 수신 권한이 없음을 에러 메세지의 형태로 수신기에게 알린다.

ECM Manager는 Input Message Filter로부터 받은 ECM을 Key Manager가 제공하는 키로 복호하여 제어 단어를 생산하여 수신기로 리턴하는 한편 카드 내의 토큰 감소를 위한 유료 프로그램 가격 정보를 Token Monitor로 보낸다. 특히 제어 단어의 리턴은 충분한 토큰이 남아 있는지에 대한 결과를 Token Monitor로부터 받은 경우에만 수행되어야 한다.

Key Manager는 ECM/EMM의 복호 과정에서 필요한 암호 키를 관리한다. 이 암호 키는 카드 내의 안전한 공간에 저장되어야 하고 이의 액세스 또한 외부의 불순한 의도로부터 보호되어야 한다. 즉 주기적으로 키 값을 변경시키거나 키 저장 영역의 접근을 특별한 방법으로만 가능하도록 하는 방안도 고려되어야 할 것이다.

Token Monitor는 계속적으로 저장된 토큰 양을 살펴서 정당한 가입자의 인증을 받아야 하며 ECM Manager로부터의 가격 정보만큼의 토큰을 감소시키며 토큰 양이 0일 경우에는 더 이상의 선 지불 유료 방송 서비스가 불가함을 수신기로 알린다. 뿐만 아니라 가입자의 잦은 채널 변경으로 인해 이중으로 토큰양을 감소시키지 않도록 충분히 고려되어야 한다.

Output Message Generator는 스마트 카드는 카드 국제 표준 규격에 의해 한 라인의 contact point만을 가지므로 half-duplex통신 시에 필요한 포트 제어 및 output message를 외부로 보내는 역할을 수행한다[5]

2. 선 지불 유료 방송 서비스 시나리오

선 지불 유료 방송 서비스를 위해서는 먼저 가입자가 구입할 스마트 카드에 안전한 명령 체계에 의해 일정 양의 토큰을 미리 입력하여야 한다.

송신측의 제한 수신 시스템과 스크램블러는 그림 5에 도시한 바와 같이 다음의 과정을 수행한다.

1) 송신측에는 먼저 EMM과 ECM의 암호화에 이용할 키를 생성하고 이 값에 유효한 범위 내의 값인지를 확인한다.

2) 1)에서 생성한 키를 이용하여 가입자 별 그룹별 EMM을 생성하여 수신측의 스마트 카드로 보낸다.

3) 다음으로는 프로그램 가격과 제어 단어를 1)에서 생성한 키로 암호화하여 ECM을 생성하고 이를 수신측으로 송신 장비를 통해 전송한다. 이 메세지는 프로그램에 따라 시간에 따라 계속적으로 수신측으로 분배되어야 한다.

4) 유료 방송 프로그램들은 3)에서 만든 제어 단어로 수신 권한을 지닌 가입자만 볼 수 있는 형태로 스크램블 한 후 전송된다.

수신측에서의 선 지불 메커니즘에 의한 유료 방송의 시청 과정은 그림 6에 도시한 바와 같이 다음과 같다.

1) 수신기가 송신측으로부터 데이타를 받으면 이 중에서 시청 권한 부여와 관련된 데이타, 즉 EMM 및 ECM만을 선별하여 스마트 카드의 입력을 제공한다.

2) 스마트 카드는 EMM을 수신하여 카드 내의 키와 복호화 알고리즘을 이용하여 이를 해석하고 그 결과 값으로 유효한 가입자에 대한 판단 과정을 수행한다. 유효한 가입자가 아니라면 카드는 더 이상의 과정을 수행하지 않고 빠

져 나온다.

3) 2)의 첫번째 인증 과정을 거치면 EMM의 복호과정에서 획득한 키를 이용하여 ECM을 해석하고 스마트 카드 내부에 토큰이 남아 있는지를 확인하여 해당 프로그램의 가격 및 프로그램 시청 시간만큼 토큰을 감소한다.

4) 3)에서의 결과가 만족스러우면 스마트 카드는 수신기

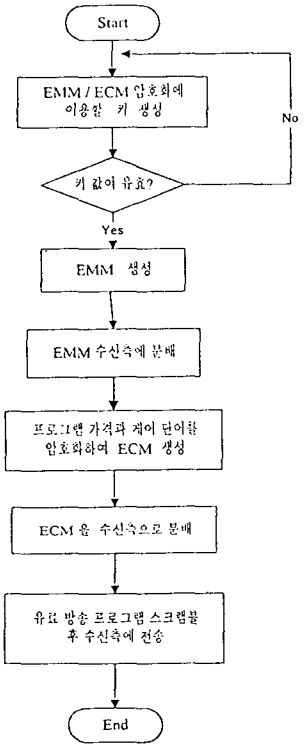

그림 5. 선 지불 서비스 시 송신측 시나리오

로 ECM의 해석 결과의 일부인 제어 단어로 스크램블된 유료 방송 프로그램을 풀어서 시청 가능한 신호로 변환하여 텔레비전으로 보낸다.

아래와 같이 동작하는 선 지불 방식의 유료 방송 서비스는 대량의 가입자 정보를 저장 및 과금을 위한 정보 변환 역시 불필요하므로 가입자 관리 시스템의 유지 보수 비용을 최소화 하는 효과가 있다.

한 번 발행한 스마트 카드는 입력된 토큰을 소비한 이후에는 계속적으로 유료 방송의 시청이 불가능하므로 메모리

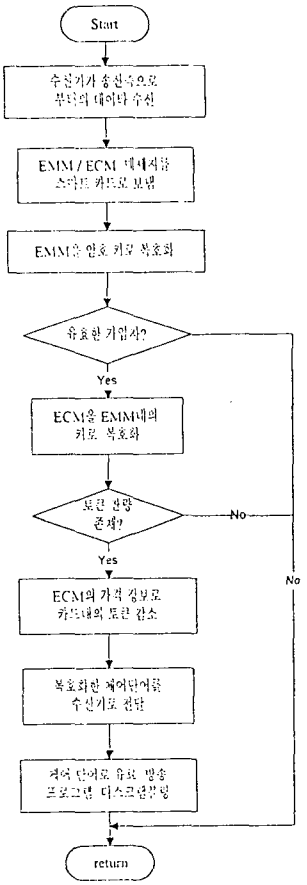

그림 6. 선 지불 서비스 시 수신측 시나리오

카드에 비해 상대적으로 가격이 비싼 스마트 카드를 토큰의 소비 이후에는 이를 회수하여 다시 사용할 수 있는 방법에 대한 고려가 필요할 것이다.

3. 선 지불과 후 지불 유료 방송 서비스

토큰을 이용한 선 지불 유료 방송 서비스는 다음의 특징을 가지고 있다.

- 가입자에게 과금 통지를 위해 필요한 가입자 정보의 보관과 과금 처리를 위한 시청 기록의 유지가 필요 없으므로 가입자 관리 시스템의 설계/구현이 비교적 간단하다.
- 토큰 서비스는 정해진 돈을 지불하고 구입한 카드 내

의 토큰이 0이 되면 자연히 유료 방송의 수신이 불가능하므로 중앙의 제한 수신 시스템 또는 가입자 관리 시스템이 가져야 할 수신 박탈과 관련된 동작 시나리오를 생략할 수 있다.

- 유료 방송 프로그램 공급자의 입장에서 보자면 서비스 선불료를 받을 수 있는 장점이 있다.
- 가입자의 잘못된 수신기 조작에 의해 카드의 토큰이 이중, 삼중으로 감소되지 않도록 스마트 카드 설계시 세심한 주의가 필요하다.

유료 방송 시청 내역을 기록하여 별도의 과금 정책에 의한 시청료를 징수하는 후 지불 서비스는 다음의 특징을 갖는다.

- 여러 유려 방송 서비스 제공자들 간의 가입자 시청료 수입의 분배시에 공정한 수입 분배를 위해 별도의 프로그램 선호도에 대한 조사를 수행하지 않고도 가입자들의 시청 내용을 파악할 수 잇으므로 시청료 분배의 공정성을 확보할 수 있을 것이다.
- 가입자 관리 시스템의 운용자가 가입자의 연체 방송 요금이 없는지를 수시로 확인하여 그 가입자의 자격 박탈 메세지를 스마트 카드로 전달하여 더 이상 유료 방송을 수신할 수 없도록 막아야 한다.

Ⅳ. 결론

토큰을 이용한 선 지불 유료 방송 서비스를 위해서는 중앙의 제한 수신 시스템과 가입자 관리시스템은 안전하게 토큰을 카드에 입력하기 위한 방안 및 데이타의 암/복호 키의 생성 과정의 설계에 대한 고려가 필요하다. 스마트 카드는 본 논문에서 기술한 카드 내의 기능 모듈에 대한 규현은 필수적이며 이를 위해서는 토큰 인증 알고리즘과 암호/복호 알고리즘에 대한 검증이 필요하다. 또 기존의 유료 방송 서비스의 자격 제어 메세지에 가격 정보를 실어 보냄으로 인하여 더 많은 양의 암호 데이타를 복호하기 위해 제한된 스마트 카드의 재원(메모리, 처리 속도)를 어떻게 활용할 것인지에 대한 고려를 포함하는 최적화된 알고리즘이 고려되어야 한다.

유료 방송 서비스를 선 지불 방식 지원 스마트 카드 또는 후 지불 방식인 시청 시간 저장 방식을 수용하는 서비스 중에 한가지만을 고집한다면 이 역시 가입자와 서비스 제공자 간의 이해 상충으로 인한 마찰도 우려되므로 서비스 시작시에 이 두 가지에 대한 서비스를 한 제한 시스템에서 모두 수용할 수 있는 방안에 대한 추후 연구가 필요하다.

참고문헌

[1] John McCormac, "European Scrambling Systems", Waterford University Press, 1996

[2] Roy Bright, "Smart Cards:Principles, Practice, Applications", Ellis Horwood Limited, 1988

[3] 김진철 외 1인, "디지털 위성방송 시스템에서의 사용량 데이터 업로드 스케쥴링 알고리즘 설계 및 구현 ", Proceedings of JCCI '96, pp. 932-935, 1996년 4월

[4] 김신효 외 1인, "유료 방송 서비스의 과금 정책에 따른 가입자 관리 센터의 구현", 한국 정보처리 학회 '96추계 학술발표, pp. 846-849

[5] ISO 7816:Identification Card., Part 1-6

[6] "Functional model of a conditional access system", EBU Technical Review Winter, 1995.

[7] 조현숙 외 1인, "Pay-TV 서비스를 위한 스마트 카드", 위성 통신과 우주산업, 제3권 제2호, pp. 58~65, 1995년 8월

필자소개

김 신 효

1990. 2. 전남대학교 전산통계 학사
1990. 3. 현재 한국전자통신연구원 근무

주관심분야
-Internet Security, Cryptography

조 현 숙

1980. 2. 전남대학교 수학 석사
1991. 8. 충북대학교 전산학 석사
1982. 3. 현재 한국전자통신연구원 근무
현재 지상 S/W 연구실

주관심분야-Cryptography,
Communication Security