지상파 디지털 방송을 위한 CAS 설계

[0]이강석*, 김상필*, 김락현*, 어 윤**, 염흥열*

순천향대학교 전기전자공학부*, 한국전자통신연구원**

Design of CAS for Digital Terrestrial Broadcasting

[0]Gang-Seog Lee*, Sang-Phil Kim*, Rack-Hyun Kim*, Yoon Uh**, Heung-Youl Youm*

Dept. of Electrical and Electronic Eng., Soonchunhyang Univ.*,
Electronics & Telecommunications Research Institute**
E-mail : hyyoum@asan.sch.ac.kr*

요약문

본 논문에서는 기존의 방송망에서의 다양한 한정 액세스 방식들을 살펴보고, ETSI 표준 한정 액세스 방식을 분석한다. 또한 스마트 카드 활용이 가능하고 다중 송신자 구조를 갖는 ECM(Entitlement Control Message) 과 EMM(Entitlement Management Message) 등의 메시지 분배를 위한 암호키 분배 방식을 살펴보고, 지상파 디지털 방송에 적용할수 있는 공개키 알고리듬과 키된 MAC 를 이용한 자격 메시지 분배 기법을 제안한다.

제1장 서론

스크램블링/디스크램블링 기능, 인증을 위한 가입자 신분 확인(Authentication) 기능, 그리고 접근 제어(Access Control) 기능은 유료 방송시스템을 실현하기 위한 핵심 기능 중의 하나이다. 한정 수신 시스템은 시청료를 지불한 시청자 만이 수신측에서 스크램블된 형태로 전달된 신호를 디스크램블하여 원하는 프로그램을 시청할 수 있게 하는 시스템이다. 한정 액세스 시스템은 허가된 시청자 만이 프로그램을 시청할 수 있어야 하며 여타 시청자들에 의한 불법 시청을 막을 수 있도록 구성되어야 한다. 한정 수신 시스템을 실현하기 위해서는 스크램블링의 강도가 어느 정도 높아야 하고, 스크램블링 및 디스크램블링을 위한 관련 파라메터들은 암호학적으로 안전한 알고리듬을 사용하여 수신단으로 안전하게 전달되어야 한다. 방송망에 적용 가능한 한정 액세스는 크게 스크램블러의 비밀키인 제어워드(CW: Control Word)를 분배하는 기능과 CW를 암호화하여 전달하는데 이용되는 인증키(AK)를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현될 수 있다.

본 고에서는 기존의 한정 액세스 방식을 분석하고, 이를 바탕으로 CW를 암호화하여 전달

하기 위한 ECM 메시지 전달 방법과 EMM 메시지 전달 방식을 제시한다. ECM 은 키된 MAC 기법을 적용하여 전달되며, EMM은 CW를 암호하여 전달하기 위해 요구되는 인증 키인 (AK)를 전달하기 위한 자격 관리 메시지이므로 분배 주기가 길어서 공개키 암호 방식을 채용하여 전달한다. 제안 방식은 비밀키 암호 방식을 이용할 경우의 복잡한 암호키 관리 문제를 해결할 수 있다.

제2장 ETSI 한정 수신 시스템과 스크램블링

유럽표준화기구(ETSI: European Telecommunication Standard Institute)에서는 DVB(Digital Video Broadcasting) 를 위하여 MPEG-2 규격에 한정 액세스 요소를 부가한 한정 액세스 규격을 제시하였다[1]. 한정 액세스 시스템은 매우 민감한 부분이므로 서로 다른 CAS 시스템간에 최대 호환성을 달성하기 위한 최소 기능만을 표준화하였다. 디지털 방송의 공통의 CA 요소는 사용자 수신기에 내장되어 동작되도록 하였다.

가. DVB 스크램블링 알고리듬

스크램블링 알고리듬은 오랜 시간동안 공격 가능성을 최소화하기 위해 고안되었다. 스크램블링 알고리듬의 기술적인 세부 사항은 담당 기관의 엄격한 심사를 거쳐서 비공개를 원칙으로 진실된 사용자들에게만 분배된다.

MPEG-2 스트림은 TS(Transport Stream) 레벨과 PES(Packtized Elementary Stream) 레벨에서 스크램블링 된다. MPEG-2 TS 레벨 스크램블링은 TS 패킷 페이로드에 적용되고, PES 레벨 스크램블링은 PES 레벨 패킷에 적용된다[2].

PES 레벨 스크램블링의 경우, PES 패킷 헤더는 스크램블되지 않는다. TS 패킷은 분할된 PES 패킷의 마지막 패킷을 포함하는 경우만을 제외하면 적응 필드(AF : Adaptation Field)를 갖지 않는다. 그림 1에서와 같이 PES 패킷은 PES 헤더와 페이로드 부로 구성되며, 스크램블링은 PES 페이로드에 적용된다. PES 패킷은 184 바이트로 구성된 TS 패킷 내로 사상된다. PES 패킷 헤더는 183 바이트 이하므로 여러 TS 패킷 들로 분할되지 않는다. TS 패킷의 맨 마지막 부분은 적당한 크기의 적응 필드(AF)가 삽입되며, 나머지는 PES 데이터와 결합된다. 그림 2는 스크램블된 PES 패킷들이 TS 패킷들로 사상되는 방법을 나타낸다.

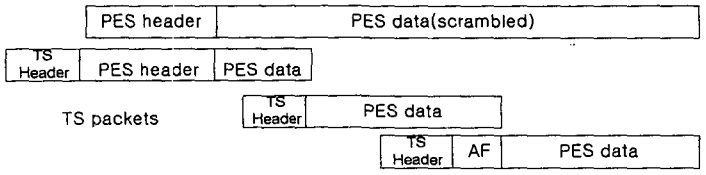

그림 1 PES 레벨 스크램블링 다이어그램

PES 레벨 스크램블링은 디스크램블링 과정을 용이하게 하기 위해 PES 패킷과 TS 패킷에 제약점을 부가하였다. 삽입된 적응 필드는 약간의 비트 속도 증가를 초래한다. 스크램블링 알고리듬은 스크램블러의 복잡도 대가로 디스크램블러의 메모리 양을 최소화하도록 고안되

었다.

나. MPEG-2 환경에서 스크램블링 알고리듬의 사용

여기서는 스크램블링 알고리듬을 효율적으로 사용하기 위한 MPEG-2 비트 스트림의 구문 정의와 운용 관련 권고안을 기술한다. MPEG-2 규격은 TS 패킷 헤더와 PES 패킷 헤더에 두 비트의 스크램블링 제어 서브 필드를 포함한다. 표 1은 TS 헤더에 포함된 스크램블링 제어 비트들을 나타낸다.

표 1 Transport_scrambling_control values

Bit values	Description
00	No scrambling of TS packet payload
01	Reserved for future DVB use
10	TS packet scrambled with Even Key
11	TS packet scrambled with Odd Key

표 2는 PES 패킷 헤더들에 스크램블링 제어 비트들을 나타낸다.

표 2 PES_scrambling_control values

Bit values	Description
00	No scrambling of PES packet payload
01	Reserved for future DVB use
10	PES packet scrambled with Even Key
11	PES packet scrambled with Odd Key

스크램블링 제어 비트(scrambling_control) 의 첫 비트는 페이로드가 스크램블됐는지 여부를 나타낸다. 두 번째 비트는 홀수 또는 짝수 제어워드의 사용을 나타낸다. 만일 TS 레벨에서 스크램블되지 않았으면, 데이터 스크램블링은 PES 레벨에서 수행된다.

PES 레벨 스크램블링은 방송 하부구조 운용에 최대한의 융통성을 부여하기 위하여 요구된다. 다음과 같은 세 가지 권고가 스크램블된 PES 패킷들에 적용된다. 스크램블링은 한 레벨(TS또는 PES) 에서만 실행되어야 하고, 스크램블된 PES 패킷 헤더는 184 바이트를 초과하지 않아야 하며, 스크램블된 PES 패킷의 한 부분을 운반하는 TS 패킷들은 PES 패킷의 끝을 포함하고, PES 패킷의 끝을 정열하기 위한 Adaptation 필드를 포함한다.

다. 분배 매체 경계에서의 제어 전이 문제

PSI(Program Specific Information)는 CA(Conditional Access) 시스템 정보를 찾기 위한 구문 요소들을 포함한다. CAT 와 PMT(Program Map Table) 에는 EMM 과 ECM 정보 등의 CA 정보를 전달하는 TS 패킷의 PID 값들을 참조하는 CA_PID 필드를 포함한다. 또한 분배 매체 경계에서 CA 정보를 운반하는 TS 패킷들을 또다른 매체의 CA 데이터로 융통성 있게 대체하는 것이 바람직하다. 이를 위하여 다음과 같은 권고안을 표준화하였다. CA_descriptor 에 주어진 CA_PID 값과 동일한 PID 값들을 갖는 모든 TS 패킷들은 오직 CA System 정보만을 포함한다. 따라서 그 외의 다른 어떤 정보 요소도 CA 정보를 포함하지 않는다. 두 개의 다른 CA 공급자들은 동일한 CA_PID 값들을 갖지 않아야 한다. 이들

권고안은 기존의 CA 정보를 새로운 CA 정보로 대체하고, 수신단에서 CA 데이터의 용이한 필터링을 위해 방송 전달 매체 경계에서의 효율적인 CA 정보의 전이를 허용한다.

라. Conditional Access(CA) 데이터

여기서는 ECM과 EMM 등과 같은 CA 정보의 전송을 위한 섹션 메커니즘을 분석한다. CA 정보의 구조는 각각의 CA 시스템 식별자에 의해 명시된다. 표 3은 CA 메시지 세션의 구문을 나타내고, 표 4는 구체적인 table_ID 값을 나타내고 있다. CA_message_section은 TS로 삽입될 때 ISO/IEC 13818-1 private_sections 으로 취급된다. 표 3과 같은 CA 메시지 섹션은 최대 256 바이트의 길이를 갖는다.

표 3 CA Message Table(CMT)을 위한 구문

Syntax	비트 번호	Identifier
CA_message_section(){		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
DVB_reserved	1	bslbf
ISO_reserved	2	bslbf
CA_section_length	12	uimsbf
for(i=0; 1<N; i++){		
CA_data_byte	8	bslbf
}		
}		

section_syntax_indicator 는 항상 "0"으로 세트되는 한-비트 표시자이고, DVB_reserved 는 미래 DVB 응용들을 위해 사용될 것이다. CA_section_length 는 section_length 필드 다음에 오는 바이트들의 수를 나타낸다. CA_data_byte는 private CA 정보를 운반하는 8비트 필드로서, 첫 9 바이트는 CA_data_byte 들의 주소 필터링을 위해 사용된다.

표 4 Table identifiers의 할당

table_id 값	설명
0x00 - 0x02	MPEG specified
0x03 - 0x3F	MPEG specified
0x40 - 0x72	V2-SI specified
0x73 - 0x7F	DVB_reserved
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82 - 0x8F	CA_message_section, CA System private
0x90 - 0xFE	private
0xFF	ISO_reserved

16개의 table_id 값이 여러 다른 한정액세스 정보를 전달하기 위해 설정되었다. 0x80과 0x81의 두 가지 table_id 필드는 ECM 데이터를 전송하기 위하여 설정되었고, 두 table_id 값이 변화하면 ECM 내용들이 변화되었음을 나타낸다. 이 값이 변화하면 수신자는 변화된 CA 정보를 필터링해야 한다.

제3장 한정 액세스 방식

기존의 케이블망용 한정 액세스 시스템은 케이블에 연결되어 있는 사용자만이 비디오/오디오 신호를 수신할 수 있고, 별도의 블랙 박스(Set top box)를 부가하여 특정 프로그램의 액세스를 제한하며, 사용자의 액세스 빈도를 저장하는 계수기를 포함하여 과금을 처리하며, 교환기가 사용자의 요구에 응하여 선택적으로 프로그램을 분배한다는 원칙하에 설계되었다.

방송 환경에서는 반드시 스크램블링 기법이 요구되며, 여러 가지 다양한 스크램블링 기법이 적용될 수 있다. 적용되어야 할 스크램블링 기법은 안전성이 높아야 하며, 스크램블링의 도입으로 인하여 서비스 신호의 질을 저하하지 않도록 설계되어야 한다.

스크램블러에 이용될 수 있는 PRBS(Pseudo Random Binary Sequence) 생성기는 주기가 될 수 있는 한 길어야 하고, 출력 비트간의 상관(Correlation)이 작아야 하며, 난수 계열의 일부분으로부터 스크램블러의 비밀 정보인 초기치(Initial Value) 를 유도할 수 없어야 한다는 특성을 가져야 한다. 가장 간단한 한정 액세스 방법은 그림 2와 같이 구축될 수 있다. 여기서, CW(Control Word) 는 스크램블러의 비밀키를 생성하는데 이용된다.

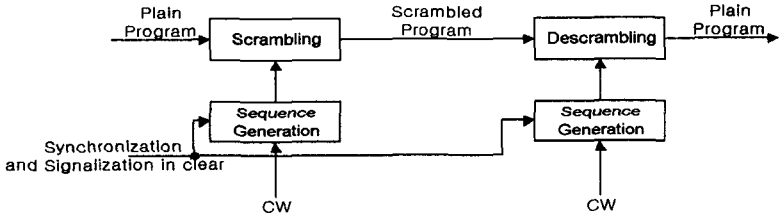

그림 2 스크램블러와 디스크램블러를 위한 구성 요소

이 방식에서는 CW에 대한 액세스가 곧 프로그램에 대한 액세스가 된다. 따라서 CW의 안전한 분배가 서비스에 대한 액세스로 종속된다.

그림 3과 같은 방식은 그림 2의 인증 방식에 관리 기능을 추가한 방법으로 CW를 각 사용자의 비밀키로 암호화한 관리 메시지를 매 달마다 우편을 통해 분배한다.

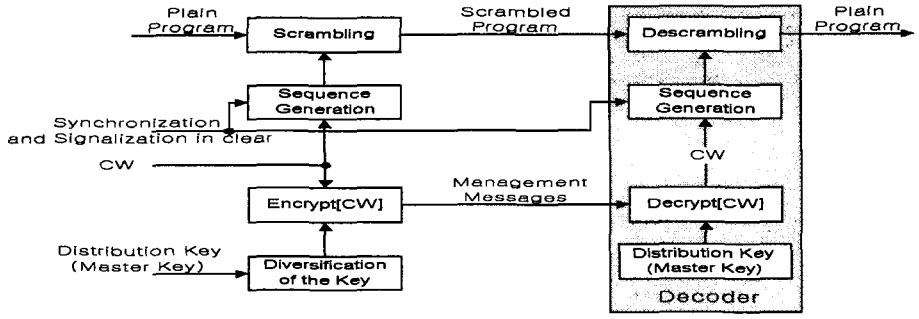

그림 3 CW 를 분배하기 위한 분배 모델

이 방식은 디코더가 고유의 분배키를 비밀리에 저장할 수 있음을 전제한다. 각 사용자는

매달마다 우편으로 사용자의 분배키(distribution key)로 CW를 암호화한 데이터를 전달받아 디코더에 입력한다. 입력된 내용으로부터 디코더는 자신의 분배키를 이용하여 CW를 복구한다. 각 디코더는 자신의 고유한 개별화된 분배키를 비밀리에 간직해야 한다. 이 방식의 특징은 다음과 같다.

1) 디코더의 물리적 안전성이 시스템의 전체 안전성에 상당한 영향을 미친다. 디코더는 등록되어 사용되며, 고유의 ID를 갖는다. 디코더는 시스템 관리자의 소유이며, 시스템 관리자는 디코더를 제작하고 서비스를 제공하는 동안 유지 보수해야 한다. 디코더는 TV 내에 포함될 수 있다.
2) 디코더는 특정 서비스에만 적용되며, 다른 서비스와 연동되어 사용될 수 없다. 그러므로 각 서비스마다 별도의 디코더를 만들어 사용자로 제공해야 한다.
3) 디코더는 가입자가 서비스 제공자로 등록될 때 임대된다.
4) 매달마다 변경되는 암호문의 수는 사용자가 충분히 쉽게 입력할 수 있도록 해야 한다.

그림 4는 내포된 ECM 채널을 통해 인증의 분배가 가능한 방식이다. 이 방식은 방송신호의 동기 표시 신호(프레임 카운터) 와 일방향 함수를 이용하여 CW를 생성하거나 서버로부터 별도의 ECM을 수신하여 CW를 생성한다. CW는 256 프레임 (약 10sec) 마다 갱신되며, 기존의 장치와 호환성을 위하여 지역적으로 입력된 제어 워드의 이용도 가능토록 구성된다.

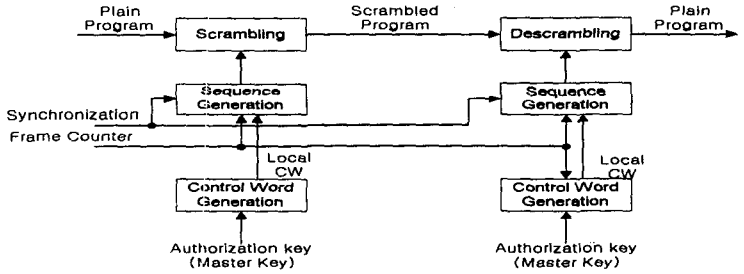

그림 4 내재적인 인증의 분배가 가능한 분배 방식

일반적으로 CW 는 식 (1)과 같다.

$$CW = E_{Bts}(F2) \tag{1}$$

여기서 F2는 비트의 프레임 워드이고, t 는 시간을, s 는 특정 서비스를 의미한다. 각 사용자는 자신의 비밀키 Di 를 비밀리에 보관한다. 한편 CW는 서버로부터 식 (2)와 같은 암호문 형태로 각 가입자로 전달된다. CW의 길이는 64 비트이다.

$$E_{Sgts}(CW) = E_{Sgts}(E_{Bts}(F2)) \tag{2}$$

이를 수신한 사용자는 비밀리에 보관하고 있는 S_{gts} 를 이용하여 CW를 복구한다. S_{gts}, B_{gts} 를 각 사용자로 분배하기 위한 EMM은 식 (3)과 같다.

$$E_{D_i}(M, S_{gts}),\ E_{D_i}(M, B_{gts}) \qquad (3)$$

여기서, Di 는 각 사용자마다 다르다. 각 사용자는 자신의 비밀키를 이용하여 식 (3)과 같은 암호문을 이용하여 비밀정보 S_{gts}, B_{gts} 를 복구한다.

각 사용자로 전달되는 EMM의 갯수는 사용자를 그룹화 함으로서 감소시킬 수 있다. EMM은 특정 사용자에만 전송되는 EMM-U, 특정 그룹에만 전송되는 EMM-S, 그리고 모든 사용자로 전달되는 EMM-G 가 있다. CW의 길이는 충분히 길어야 하고, 수명은 짧아야 한다. 그림 5는 디코더 대신에 스마트카드를 이용한 방식이다.

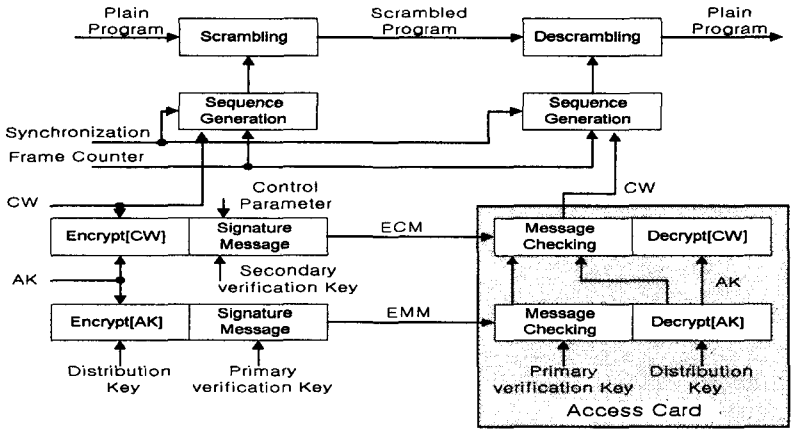

그림 5 인증의 분배를 갖는 방식

이 방식은 CW를 분배하기 위한 ECM과 CW를 암호화하는데 이용되는 인증키를 분배하기 위한 EMM에 바탕을 두고 있으며, EMM은 서버와 각 사용자의 액세스 카드가 공유하고 있는 가입자의 분배키와 서명문을 위한 일차 검증키를 이용하여 생성된다. 가입자측 IC 카드는 ECM 및 EMM 으로부터 해당 정보를 도출한다.

CW는 ECM 형태로 암호화되어 가입자에 전달된다. ECM은 CW를 인증키로 암호화한 암호문과 이에 대한 서명문을 쇄상한 구조를 갖는다. 각 가입자는 ECM으로부터 CW를 복구하고 제어 메시지의 정당성을 서명 알고리듬과 무결성 알고리듬으로 검사한 후, 메시지가 정당하면 CW 를 디스크램블러로 전달한다. 인증키의 분배는 EMM를 통해 전달되며, EMM은 각 사용자의 분배키로 인증키를 암호화한 암호문과 사용자의 자격을 나타내는 자격 정보를 사용자의 일차 검증키(Primary Verification Key)로 서명한 서명문으로 생성된다. 각 사용자의 액세스카드는 분배키를 이용하여 인증키를 복구하고 자격 메시지를 검사하며, 인증키를 ECM 제어부로 전달한다. 이 방식은 서버와 사용자가 비밀리에 분배키와 서명용 일차 검증키를 공유하고 있다고 가정한다.

그림 6에서 나타난 방식은 그림 5의 방식과 거의 유사하나, 서버측의 안전성을 향상하기 위하여 ECM 생성용 제어 카드와 EMM 생성용 관리 카드를 도입하였다. 일정 초마다 새로운 인증키가 자격 관리 메시지를 통해 각 사용자 또는 그룹에 전달된다. 서비스 제공자가 $E_{Di}(AK)$를 각 사용자에 전송하지 않으면 각 사용자는 절대로 인증키를 복구할 수 없다.

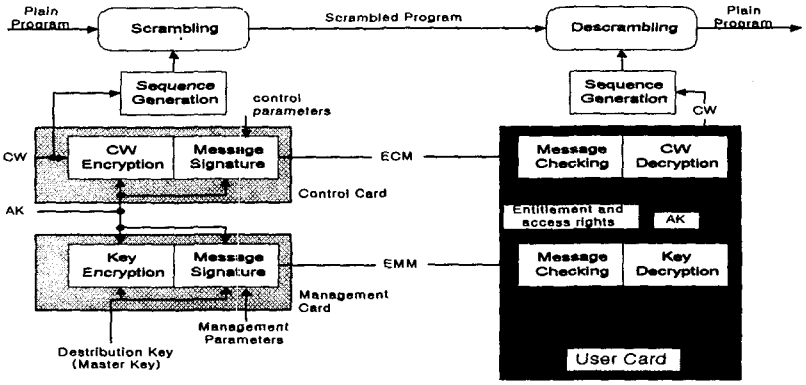

그림 6 인증 분배를 갖는 향상된 방식

자격(entitlement)이 키 자체냐 아니면 키를 사용할 수 있는 권한이냐는 문제는 매우 중요하다. 자격이 인증키인 경우, 동일한 인증키를 갖는 모든 사용자는 동일한 권한을 갖는다. 따라서 사용자의 권한을 바꾸기 위해서는 모든 사용자의 인증키를 변경해야 한다. 인증키가 공중망을 통해 분배되는 경우, 진품 장치와 위조 장치를 동시에 소지하고 있는 불법 사용자에게도 전달될 수 있다. 따라서 인증키를 자주 변동한다 해도 시스템의 안전성의 향상에는 도움이 되지 않는다.

자격이 인증키의 사용을 제한하는 조건인 경우, 자격은 카드에서 개인 별로 관리된다. 사용자 자격의 변동은 각 사용자의 보안 장치에서 해당 인증키와 연관되는 자격 조건을 변동하는 것으로 충분하다. 따라서 나머지 가입자의 조건은 변동이 없어도 된다. 각 사용자의 보안 장치에서 인증키와 관련된 조건을 관리하기 위하여 방송망 주소 기법을 사용하여 정보를 전송할 수 있다. 조건의 예는 가입 기간(t), 미리 예약된 프로그램(s), 그리고 충동 액세스(Impulsive Access) 에 대한 신용도 등이다.

자격 관리는 보안 장치 내에서의 비밀 정보의 관리 문제이다. 인증키와 관련된 자격 관리는 무결성 서비스와 인증 서비스를 요구한다.

보안 장치가 디코더와 일체형인가 분리형인가 결정하는 것 또한 매우 중요하다. 보안 장치는 시스템 관리자의 소유이며, 보안 장치가 디코더 내에 존재하는 경우, 디코더는 시스템 관리자의 소유이므로 하나의 디코더가 여러 개의 유료 TV 운용자와 연동할 수 없게 된다. 따라서 다양한 서비스 제공자에 대한 여러 종류의 디코더를 요구하게 된다.

분리형인 경우, 디코더는 공용으로 사용되고, 디코더의 제조, 분배, 그리고 판매는 자유롭다. 그러나 분리형의 보안 장치는 엄격히 관리되어야 한다. 디코더는 TV에 일체화될 수 있고, 이를 위해서는 디코더와 보안 장치 간의 인터페이스를 위한 일련의 표준안과 ECM과 EMM의 전송에 관한 표준안의 설정이 요구된다. 분리형 장치는 암호 알고리듬의 자유로운 진화를 가능케 하고, 멀티미디어 서비스의 사업화를 촉진하며, 지금까지의 실리콘 기술을 이용할 수 있는 장점이 있다.

인터페이스를 어떻게 어느 위치에 정의하느냐에 따라 한정 액세스 시스템는 큰 영향을 받는다. DAVIC에서는 한정 액세스를 위하여 두 종류의 인터페이스를 정의하고 있다. DAVIC STU 는 둘 중 최소한 하나의 인터페이스를 지원해야 하며, 이는 그림 7과 같이 CA0와

CA1 인터페이스이다[3]. CA0 인터페이스는 고속 디스크램블링기능을 포함하는 CA 기능 전체를 포함토록 하는 인터페이스이며, CA1은 저가의 저속 암호 처리를 사용하는 스마트카드로 인터페이스 한다. 암호 처리 기능은 스마트카드에서 실현된다[4][5]. CA1 인터페이스는 스크램블링 협상 기능을 포함해야 한다.

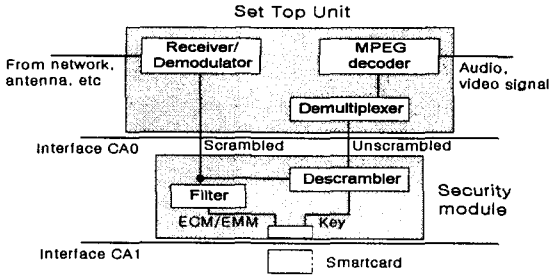

그림 7 CA1 인터페이스와 CA0 인터페이스

CA0는 스크램블링된 신호를 수신하여 디스크램블링된 신호를 보낸다. 보안 모듈은 고속 디스크램블링과 고속 필터링 기능을 포함한다. 이들 기능들은 스마트 카드 형태로 구현되는 저속 키 관리 기능과 상호 동작한다. 저속 키 관리 기능은 고속 보안 모듈 내에 포함되거나, 별도의 보조 물리 모듈 내에 실현된다. CA0 인터페이스를 채용한 STU 구조는 전체 한정 수신 기능을 통째로 바꿀 수 있다는 특징이 있다. CA0 인터페이스는 상대적으로 복잡한 모듈로 성취되는 약점이 있으나, 특정 STU와 다른 서비스 제공자들간에 최대한의 상호 동작 능력을 제공한다. STU는 하나 이상의 CA0 인터페이스를 포함할 수 있다. CA0 인터페이스를 채용한 장치는 공격이 성공했을 경우 CAS의 설계가 용이한 장점이 있다.

CA1 인터페이스는 저속의 보안 관리 기능만을 수행하는 복잡도가 낮고 좀더 개인적인 보안 모듈과 CA0 인터페이스를 갖는 보안 모듈간을 접속한다. DAVIC 공통 필터링 기능을 채택하고 특정 STU와 서비스 제공자들 간에 공통의 스크램블링 알고리듬의 사용을 전제하면 CA1 인터페이스는 최대한 호환성을 제공한다.

CA1 인터페이스는 몇 가지 중요한 장점이 있다. 첫째, 물리적인 인터페이스(ISO-7816 Part 1-6)의 복잡성이 CA0 에서 정의된 PC 카드 인터페이스의 복잡도보다 낮다. 둘째, CA1 인터페이스만이 실현되었을 경우 STU의 CA1 인터페이스측에 디스크램블링, 디코딩, 디멀티클랙싱을 단일 칩으로 집적화할 수 있어서 CA1 인터페이스의 복잡도를 현저하게 감소시킬 수 있다는 것이다. 셋째, 분리 가능한 모듈 자체의 복잡도는 최소한 보안 공격의 침해, 새 서비스들의 기능 부가, 새 서비스 제공자들을 위한 액세스를 위해 모듈을 대체할 수 있기 때문에 최소화되어야 한다는 것이다.

물리 인터페이스 복잡도의 감소 및 요구되는 기능 감소 측면으로 보면 스마트 카드를 이용하는 방법이 전체 보안 모듈을 이용하는 방법보다 단순하다. CA0 인터페이스는 다중화되어 있는 디스크램블링된 내용을 인터페이스를 통해 전달한다. CA1 인터페이스는 디지털 내용을 더욱 안전하게 보호할 수 있다. CA1 접근은 디지털 내용이 STU 안에서 전달된다. 이는 가정 사용자(home user)에 의한 내용의 기록을 더욱 어렵게 한다. 디스크램블링과 디코딩이 단일 칩상에서 집적화된다면, 디지털 내용은 더욱 안전하게 보호될 것이다.

제4장 다중 송신자를 갖는 효율적인 한정 액세스 시스템 설계

정보 데이터를 암호하는 암호 기술이 한정 액세스 제어를 실현하기 위하여 사용되어야 한다. 여기서 복호화를 위한 키가 정당한 수신자에게만 분배되도록 구성되는 것이 매우 중요하다. 만일 정보 데이터 암호 기법이 안전하다면 한정 액세스 제어 시스템의 보안 문제는 복호화키의 분배 방식에 의존하게 되기 때문이다.[6][7]

가. 한정 액세스 제어를 위한 키 분배 방식

한정 액세스 제어 방식은 송신자가 그림 8과 같이 데이터를 암호한 후 전송을 하고 오직 인증된 수신자만이 복호 키를 분배받아 방송을 수신하도록 하는 시스템이다. 따라서 인가된 수신자에게만 복호 키를 분배하는 것은 매우 중요하다.

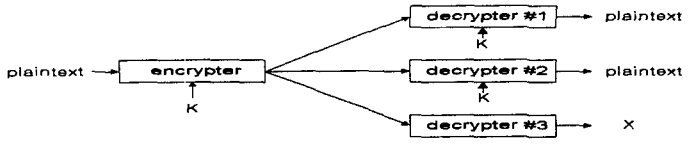

그림 8 CAS를 포함하는 데이터 방송

한정 액세스 제어를 이용하는 정보 데이터 방송에는 두 가지 키 분배 방식이 있는데, 첫 번째 방식은 암호 채널을 사용하여 복호화키를 전송하는 것이고, 두 번째 방식은 비밀 해쉬 함수와 해쉬 함수의 공통 입력을 이용하여 복호키를 생성하는 방식이다.

첫 번째 방법은 암호 채널을 통해 복호화키를 전송한다. 사용될 암호시스템은 비밀키 암호시스템 또는 공개키 암호 시스템이다. 비밀키 암호 시스템이 사용될 경우, 송신자와 수신자간에 공유된 암호키로 암호 채널을 형성한다. 공개키 암호시스템이 사용될 경우, 채널의 암호화는 수신자의 공개키를 사용하여 수행되고, 공개키에 대응되는 비밀키는 복호 키를 얻는데 사용된다. 비밀키 암호시스템의 장점은 고속 동작이 가능하고 복잡도가 낮은 점이다. 공개키 암호시스템의 이점은 공개키 암호시스템의 관리가 수신단에서 필요하지 않다는 것이다.

해쉬 함수 방법의 경우, 해쉬 함수 입력 데이터는 보통 모든 수신자에게 전송된다. 그 데이터는 해쉬 함수로 입력되고, 해쉬 함수 출력이 수신자 복호 키로 사용된다. 해쉬 함수는 IC 카드에 적재되고, IC 카드는 오직 인증된 수신자에게만 교부된다. IC 카드는 부정행위에 대해 안전한 장치로 인정되고, 해쉬 함수는 공격자에 의해 읽혀지지 않는다.

비밀키 암호시스템에 기반을 둔 키 분배 방식이 한정 액세스 제어를 갖는 정보 데이터 방송 시스템에 널리 적용되고 있다.

나. 다중 송신자 제공 서비스에서의 암호시스템

다중 송신자 지불-TV 시스템에서의 수신자는 특정 시간에 한 송신자를 선택하여 데이터 분배 서비스를 수신한다. 다중 송신자가 제공하는 서비스의 복호화 키는 암호화된 채널을 통

해 전송되어야 한다. 송신자의 장비에 저장된 수신자의 비밀 정보는 해당 송신자의 서비스를 이용할 수 있도록 한다. 그리고 특정 송신자가 또 다른 송신자를 가장해서는 않된다. 또한 기지 평문 공격(Known-plain Text Attack)에 강해야 한다. 이 방식은 송신자의 장비에 있는 수신자의 비밀 정보의 관리 허점이 전체 시스템의 안전성을 침해할 수 있는 단점이 있다. 상기 요구조건을 만족하면서, 기지 평문 공격을 피할 수 있는 두 가지 방법들을 제시한다.

첫 번째 방법은 그림 9에서 도시된 바와 같이 각 수신자는 각 송신자에 대응되는 수신자키를 유지한다. 여기서, K_{ij}는 송신자 #i 에 대한 수신자 #j 의 수신자 키이다. 수신자 #j 는 각 송신자에 대응되는 수신자 키 K_{Ai}, K_{Bi}, K_{Ci}, ... 를 유지하며, 송신자 A 는 수신자 키 K_{A1}, K_{A2}, K_{A3}, ..., K_{An} 을 유지해야 한다.

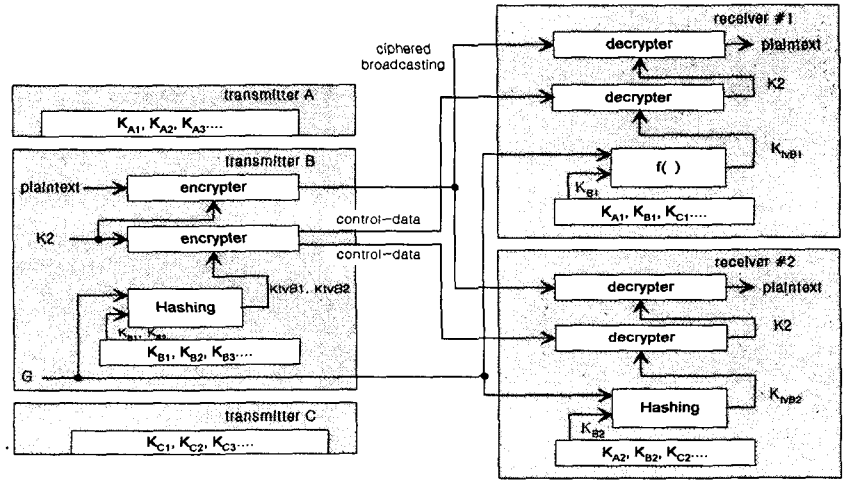

그림 9 비밀키 방식에 기초한 두 계층으로 구성된 키 분배 방식

송신자 i 는 자신의 키-생성-데이터(G_i)를 생성하고, 이를 수신자에 송신하며, K_{ij}, G_i를 해쉬한 결과 값인 수신자 #j 와의 시간-변형 개별-키(K_{tvij})를 공유한다.

송신자와 수신자간에 공유되는 시간-변형 개별-키는 키 분배를 위한 기본-계층-암호키로 사용된다. 이 방식에서는 각 수신자가 각 송신자에 대해 하나의 수신자-키를 가져야만 하므로 송신자의 수를 증가시키는 것이 용이치 않다는 단점이 있다.

두 번째 방법은 키-분배를 위해 공개키 암호 시스템을 채용하는 것이다. 모든 송신자는 수신자의 공개키(K_{pi})를 갖고 각 수신자는 자신의 공개키(K_{pi})에 대응하는 유일한 비밀 키(K_{si})를 갖는다. 이 방법에서 모든 인증된 수신자들에게 공통인 비밀 제어 정보는 수신자의 공개-키(K_{pi})로 암호화되어 각 수신자에게 송신된다. 수신된 정보는 수신자의 비밀키(K_{si})로 복호화된다. 그림 10은 두 계층으로 구성된 키-분배를 제공하는 공개키 암호시스템의 예를 보여준다.

두 번째 방법에서는 송신자의 수를 쉽게 증가시킬 수 있다. 그러나 제어-데이터의 크기가 첫 번째 방법의 그것보다 더 크다. 만일 공개키 암호시스템을 위해 RSA 암호가 사용된다면

암호화된 데이터의 크기는 충분한 안전을 위해 512비트 보다 더 커야 한다.

RSA 암호의 암호화 속도가 비밀키 암호 시스템인 DES에 비해 근사적으로 1000배 정도 느리기 때문에 첫 번째 방법에 비해 접근 제어 데이터를 생성하기 위한 계산적 부담이 크다는 점이다[8]. 계산의 부담 적인 측면에서는 첫 번째 방법이 우수한 반면, 송신자를 변화시키기 위한 시스템 융통성의 측면에서는 두 번째 방법이 우수하다.

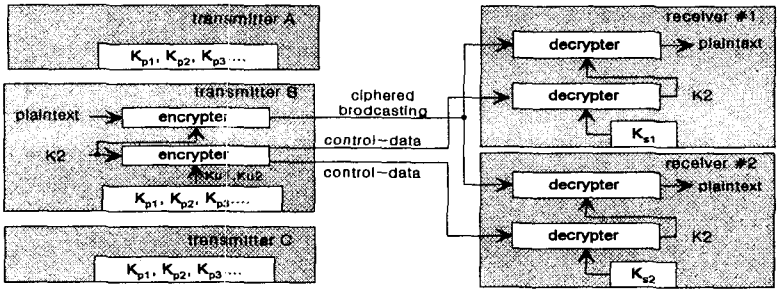

그림 10 공개키 방식에 기초한 두 계층으로 구성된 키 분배 방식

제5장 제안된 ECM과 EMM에서의 키된 MAC 와 공개키 기법 제안

가. ECM에서의 키된 MAC 기법 제안

기존의 ECM에서 해쉬 부분을 키된 MAC로 제안한다. 그림 11은 해쉬 함수 대신에 키된 MAC 구조를 가진 ECM의 구조를 나타낸다.

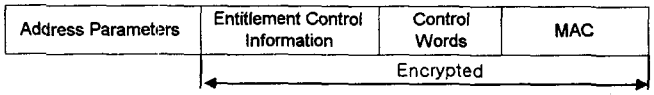

그림 11 ECM(Entitlement Control Message)

MAC는 제어 파라메터, 제어 워드를 일방향 함수로 해쉬한 결과 값이다. 해쉬 함수는 보통 MD5(Message Digest 5) 또는 SHA(Secure Hash Algorithm) 를 사용한다. MAC 값을 수신한 수신기는 AK 로 제어 워드를 해독한 후 송신단에서 MAC를 생성한 것과 같이 수신단에서 MAC를 계산하여 올바른 메시지임을 검증한다.

나. EMM에서의 공개키 기법 제안

EMM을 전송하는 방식에는 비밀키 암호 시스템을 사용하는 방법과 공개키 암호 시스템을 사용하는 방법이 사용될 수 있는데, 고속 S/W의 등장은 공개키 암호 알고리듬을 사용해도 처리 속도면에서 큰 지장을 초래되지 않는다. EMM의 전송은 공개키 암호 시스템을 이용하여 정보를 전송한다. 그림 12는 공개키 암호 시스템 방식을 이용한 EMM의 구조를 나타낸다.

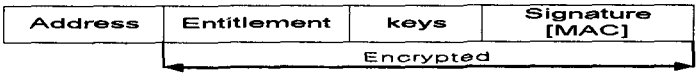

그림 12 EMM(Entitlement Management Messages)

자격 메시지와 AK는 고객의 공개키로 암호되고 서명문은 주소와 자격 메시지 그리고 AK를 MAC한 값을 방송국의 비밀키로 서명한 값이다.

다. 제안된 기법을 이용한 CAS의 구성도

위의 제안된 ECM과 EMM을 이용한 CAS의 전체 구성도는 그림 13과 같다.

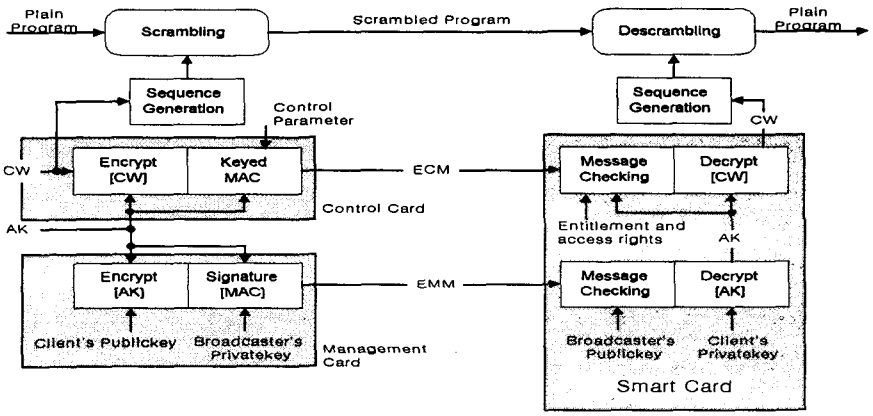

그림 13 키된 MAC와 공개키 암호방식을 이용한 CAS 구성도

가입자의 공개키와 서비스 제공자의 서명용 공개키는 각각 송신국과 고객의 스마트 카드에 저장되어 있다. 송신국은 AK를 고객의 공개키로 암호한 값과 이에 대한 자신의 서명문을 EMM을 통해 전송한다. 수신자는 서명문을 방송국의 공개키로 복호하여 메시지의 정당성을 검증한다. 정당한 방송국에서 왔음을 확인한 수신자는 EMM을 스마트 카드로 전달하여 새 AK를 전달받는다.

64-비트 CW 를 초기치로 한 계열 생성기로 스크램블된 프로그램은 고객으로 전송된다. CW는 AK로 암호화되고, 주소 파라메터와 암호화된 제어워드, 그리고 프로그램의 자격 제어 정보를 MAC한 결과를 구한다. 그리고 그림 11과 같은 ECM 채널로 고객으로 전송된다. 수신자의 디코더는 고객이 선정한 프로그램에 대한 ECM을 찾아 MAC 계산 결과를 통해 수신자의 자격을 검사한 후 암호화된 CW를 스마트 카드로 전송한다. 스마트 카드는 EMM으로부터 구한 AK로 암호화된 CW를 복호하여, 평문의 CW를 디지털 디스크램블러로 전송한다. 최종적으로 디스크램블러는 암호화된 프로그램을 디스크램블링한다.

스크램블링 방식은 DVB에서 권고한 계열 생성 방식을 사용할 수 있고, CW 를 암호하기 위한 비밀키 알고리듬은 IDEA를 사용하며, MAC 계산을 위한 해쉬 함수는 MD5 를 사용한다. EMM에 사용되는 공개키 암호 방식은 RSA 를 사용한다. 본 논문에서는 상기의 구체적인 암호 메카니듬을 적용하여 CAS 시스템을 실현하였다. 키된 MAC 는 인증과 무결성을

동시에 채용한 방식으로써 채용되었고, EMM 을 전송하기 위한 공개키 암호 방식은 비밀키 암호시스템이 갖는 복잡한 키 관리 문제를 해결하기 위해 채용되었다. 공개키 암호시스템이 비밀키 암호시스템에 비해 속도가 느리긴 하지만 고속 멱승 알고리듬의 소프트웨어 및 하드웨어의 실현으로 인해 속도 문제는 충분히 극복되리라 예측된다.

제6장 결 론

한정수신 시스템의 가장 핵심은 안전한 스크램블링 기법과 자격메시지를 안전하게 분배할 암호알고리듬 이다. 본 고에서는 방송 서비스에 적용될 수 있는 여러 가지 한정 액세스 방식들을 살펴보고, DAVIC에서의 CAS 인터페이스와 CAS(한정 수신 시스템)표준(ETSI) 스크램블링을 살펴보았다. 그리고 스마트카드를 이용한 CAS에서 자격(Entitlement)메시지인 ECM과 EMM의 분배에 있어 키 분배방식을 살펴보고, 공개키 암호 시스템과 키된 MAC를 이용한 자격 메시지 분배를 제안했다. 키된 MAC로 인해 좀더 확실한 인증이 요구되며, 공개키 암호 시스템을 이용하여 비밀키 암호 시스템에서 발생할 수 있는 문제점을 해결할 수 있었다.

이를 실현하여 검증한 결과 만족할 만한 결과를 얻을 수 있었다. 여기에 적용된 비대칭 암호알고리듬인 RSA의 속도는 팬티엄 100에서 0.3초를 얻는 멱승 알고리듬을 사용하였다[9].

-참고문헌-

[1] ETSI, "DVB Support for Use of Scrambling and CA within Digital Broadcasting Systems," ETR289, 1996.

[2] ISO/IEC 13818-1, Information Technology - generic Coding of Moving Pictures and Associated Audio Information: System, ISO/IEC JTC1/SC29, 1996., Seoul.

[3] 염흥열, 이종형, "DAVIC 에서의 액세스 제어 방식," 한국통신정보보호학회 학회지, 제7권 제1호, 1997.3.

[4] 조진만, 은성경, 조현숙, "위성방송의 제한수신 서비스를 이한 스마트카드 기술," JCCI'96, 1996.

[5] 김경신, 김승주, 원동호, "스마트카드를 이용한 유료 방송 한정수신 시스템," JCCI'96, 1996.

[6] CCIR "Conditional-Access Broadcasting System," Recommendation 810, 1992.

[7] General Characteristics of a Conditional Access Broadcasting System-Report CCIR 107-1.

[8] Bruce Schneier, "Applied Cryptography," Wiley, 1996.

[9] 윤호선, 백종현, 김락현, 염흥열, "공개키 암호시스템을 위한 효율적인 승산 및 멱승 연산 알고리듬의 실현", '97 대한전자공학회 호서지부 춘계학술 발표회, 1997.4.