韓國 컴퓨터情報學會 論文誌
第10卷 第2號, 2005. 5.

2005-10-2-2-6

위성 DMB에서의 효율적인 유료시청권한 제어에 관한 연구

김 현 주*, 김 숭 주*, 원 동 호*, 한 우 철**

A Study the Control of Conditional Access to Pay-TV in Satellite digital Multimedia Broadcasting

Hyun-jue Kim*, Seung-joo Kim*, Dongho Won*, Woo-chul Han**

요 약

제한수신 시스템이란 송신기에서 스크램블된 신호를 수신측의 수신권한을 받은 가입자만이 방송 프로그램을 시청할 수 있도록 하는 시스템으로 운영의 많은 부분을 가입자들의 시청료에 의존하는 유료 방송에서 필수적으로 사용되는 기술이다. 방송 프로그램과 정당한 가입자를 보호하기 위하여 도입한 제한수신 시스템에서 가장 기본적이자 가장 중요한 사항은 안전하게 키를 관리하고 분배하는 것이다. 본 논문에서는 최근 주목받고 있는 유료 방송 시스템인 위성 DMB에 적합한 효율적인 키 관리 프로토콜을 제안하고, 이를 기존의 제한수신 시스템 모델에 적용하여 위성 DMB에서의 유료시청 권한 제어 시스템을 설계한다.

Abstract

The Conditional Access System is a complete system for ensuring that broadcasting services be accessible to only those who are entitled to receive them. Secure key management and efficient delivery mechanism are very important design factors to this system. In this paper, we propose secure and efficient protocols which would be well fitted to a Pay TV system including the satellite DMB. Further, by applying our protocol to the existing conditional access system, we propose a new system that properly enables the control of conditional access to the Pay TV in satellite DMB environment..

▸ Keyword : Satellite DMB, Conditional Access System, Key Management

• 제1저자 : 김현주
• 접수일 : 2005.04.12, 심사완료일 : 2005.05.18
* 성균관대학교 정보통신공학부,** 대림대학 산업시스템경영과
※본 연구는 정보통신부 지원 대학 IT 연구센터 육성지원사업(C1090-0403-0005)으로 수행되었음

Ⅰ. 서 론

네위성 DMB 서비스는 고품질의 음성과 영상서비스를 이동하면서도 즐길 수 있는 이동 멀티미디어 방송 서비스로, 특히 이동통신망을 리턴 패스로 이용할 경우 양방향 서비스도 가능한 방송·통신 융합 서비스로써 차세대 핵심 산업의 하나로 크게 주목받고 있다. 위성 DMB는 현재 이동성이라는 강력한 경쟁력을 기반으로 기존의 방송 시장에 성공적으로 진입하고 있다. 그리고 이와 함께 방송국 호스트가 위성 DMB용 수신 단말기에게 방송하는 멀티미디어 콘텐츠의 보호도 점차 그 중요성을 더해가고 있다[1~3].

위성 DMB는 지상파 DMB와는 달리 위성체를 이용해 방송을 하며 수신률이 낮은 도심지역은 갭필러라는 일종의 중계기를 활용해 수신을 하는 방식이다. 그리고 지상파 DMB에서 서비스하지 않는 보다 특화된 서비스를 제공하고, 이에 따른 위성사용료, 방송콘텐츠 이용료 또는 정보이용료로 운영이 되는 유료 방송 시스템이다. 운영의 많은 부분을 가입자들의 시청료에 의존하는 유료 방송 시스템을 유지하기 위해서는 비가입자나 시청료를 내지 않은 사용자들은 정상적인 방송 신호를 수신할 수 없도록 하는 제한수신 시스템의 도입이 필수적이다[4,5]. 방송 프로그램과 정당한 가입자를 보호하기 위하여 도입한 제한수신 시스템에서 가장 기본적이자 가장 중요한 사항은 안전하게 키를 관리하는 것이다. 암/복호화에 사용되는 키가 노출되면 유료 방송 시스템내의 모든 보안 서비스가 공격당하게 되므로 키의 안전성을 위한 키관리 메커니즘은 그 어느 무엇보다도 중요하다. 또한 유료 방송 서비스에서는 사용자들의 가입과 탈퇴를 보장해야 하기 때문에, 새로운 가입자의 추가나 기존 가입자의 삭제를 용이하게 하고 가입자 증가에 따른 메시지의 증가를 최소화해야 한다는 점에서도 키관리 메커니즘의 중요성이 부각된다. 이를 위해서는 서비스 및 과금 형태에 따라 그룹을 형성하고 이에 대한 그룹키(group key)를 공유해야 한다[6~8].

본 논문에서는 유료방송에 적합한 그룹키 관리 프로토콜을 제안하고, 이를 이용하여 위성 DMB에서의 유료시청권한 제어 시스템을 설계한다.

본 논문의 구성은 다음과 같다. 1장의 서론을 시작으로 2장에서는 제한수신시스템의 구조에 대하여 살펴보고 3장에서는 위성 DMB에 적합한 그룹키 관리 프로토콜을 제안한다. 그리고 4장에서는 3장의 프로토콜을 기존의 제한수신 시스템 모델에 적용함으로써 위성 통신을 이용한 그룹키 관리 프로토콜 기반의 새로운 유료시청권한 제어 시스템을 제안하고 시스템의 효율성을 분석한다. 그리고 끝으로 4장에서 결론을 맺는다.

Ⅱ. 제한수신 시스템

디지털 위성 방송에서의 제한수신 시스템 도입의 정당성은 다음과 같은 두 가지 특성에서 찾아볼 수 있다.

- 광역성(Wide Area): 위성으로부터 지상을 향해 발사한 전파는 넓은 지역에 미치기 때문에 넓은 지역을 통신의 대상으로 할 수 있다. 이로 인하여 제한된 지역을 넘어 방송 전파가 도달하는 전파 월경의 문제가 발생할 수 있다. 예를 들어, 지역 또는 가입자 그룹에 문화적, 인구학적 사유로 인한 프로그램과 광고에 대해 방송을 규제해야하는 상황이 발생할 수 있다.
- 동보성(Broadcasting): 위성 방송은 한 지점으로부터 여러 곳에 흩어져 있는 다수의 수신 대상 설비로 동시에 동일 내용의 정보를 전송하는 동보통신이기 때문에 가입자와 미가입자가 모두 같은 전파를 수신한다.

이러한 위성 방송의 특성으로부터 발생되는 문제는 제한수신 시스템(conditional access system)을 도입함으로써 해결할 수 있다. 제한수신 시스템이란 송신측에서 송출한 스크램블링(scrambling)된 신호를 수신측의 수신인가를 받은 정당한 가입자만이 디스크램블링(descrambling)하여 프로그램을 시청할 수 있도록 하는 시스템이다. 디지털 위성 방송에서의 제한수신 시스템의 기본 요구조건은 다음과 같다.

첫째, 프로그램 및 데이터는 스크램블링되고, 통신링크상에서 미가입자의 불법 도/시청을 막을 수 있도록 보호되어야 한다.

둘째, 시청료를 지불할 정당한 가입자만이 프로그램을 시청할 수 있도록 가입자 신분확인(authentication) 기능과 접근제어(access control) 기능이 있어야 한다.

언급된 위의 두 가지 조건은 결국 방송 프로그램과 가입자 보호를 위한 것으로, 방송 프로그램의 보호 메커니즘으로는 스크램블링/디스크램블링이 있고, 가입자 보호 메커니즘으로는 인가된 가입자들에게 해당 시청 자격(entitlement)을 주는 기술이 있다. 여기서의 자격이란 프로그램을 디스크램블링하는데 필요한 관련키와 수신자의 시청 권리를 말하며, 방송 프로그램의 스크램블링에 사용한 키와 프로그램 취득 조건(access parameter)을 자격 통제 메시지(ECM: Entitlement Control Message) 내에 포함시켜 전송하는 자격 통제 기능(ECF: Entitlement Control Function)과 자격의 유효 기간 등을 자격 관리 메시지(EMM: Entitlement Management Message) 내에 포함하여 전송하는 자격 관리 기능(EMF: Entitlement Management Function)으로 구분할 수 있다.

스크램블링 및 디스크램블링 기능, 인증 기술을 이용한 가입자 신분 확인 기능 그리고 접근 제어 기능들은 제한수신 시스템을 실현하기 위한 핵심 기술들이다. 제한수신 시스템을 실현하기 위해서 ECM 및 EMM내에는 스크램블링 및 디스크램블링에 필요한 관련키가 적당한 암호화 알고리즘에 의해 암호화되어 각 수신자에게 전송된다. 이러한 기능 블록을 포함한 제한수신 시스템의 일반적인 구조는 (그림 1)과 같다. 우선 방송국에서는 전송될 프로그램(영상 및 음성 신호)를 제작하고 제작된 신호를 의사난수 발생기에서 발생된 난수로 스크램블링한다. 이때 사용된 난수 발생 초기치(CW: Control Word)는 가입자관리서버에서 제공되며 역시 서버에서 제공된 암/복호화키(authorization key)로 암호화된 후, ECM에 넣어져 스크램블링된 프로그램과 함께 방송국으로부터 위성을 통해 각 수상기에 전달된다.

방송국의 가입자관리시스템에서는 CW를 발생하고 해당 CW 암호화시 사용되는 암/복호화키는 수신측 디스크램블러와 연결된 스마트카드라고 하는 접근제어장치에 안전하게 보관되어있는 가입자 고유키(distribution key)로 다시 암호화된 후 EMM에 넣어져 별도 통신 채널을 통해 각 디스크램블러에 직접 전달된다.

각 가입자 컨버터에서는 스크램블링된 영상 및 음성 신호와 함께 ECM을 수신하여 그 중에 암호화된 CW를 스마트카드에 전달하고, 스마트카드에서는 EMM을 통해 수신받은 암/복호화키를 스마트카드 내부에 안전하게 저장되어 있는 가입자 고유키를 사용하여 복호화하고, 복호화된 암/복화화키는 다시 현재의 CW를 복호화하여 스크램블링에 사용된 것과 동일한 CW를 디스크램블러에 보냄으로써 수신된 신호를 디스크램블링할 수 있도록 한다.

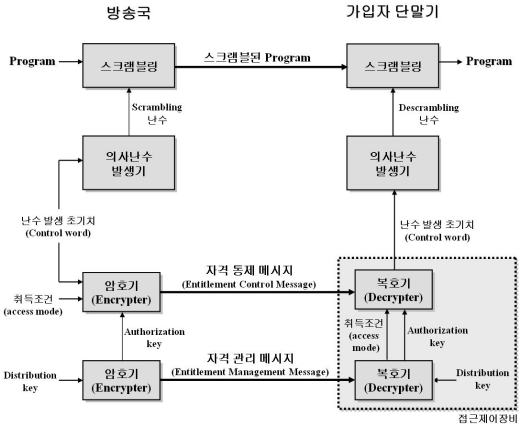

그림 1. 제한수신 시스템 구조
Fig 1. Conditional Access System for Broadcasting

일반적으로 송신측의 스크램블링은 하드웨어 장비로 실현되며 디스크램블링 기능은 STB와 같은 수신기 내의 하나의 칩으로 구현된다. 그리고 자격 통제와 자격 관리는 송신측에서는 제한 수신 엔진과 수신측에서는 스마트카드와 같은 보안장치가 각각 그 기능을 수행하게 된다. 이때 스마트카드와 수신기의 디스크램블러는 서로 통신하여 합법적인 상대임을 확인하는 상호 인증 과정을 거치게 된다. 만약 스마트카드를 이용하지 않는 한정 수신 시스템인 경우에는 가입자별로 고유한 복호화 키가 디스크램블러내에 저장되며, 이를 이용한 CW의 복호화가 디스크램블러에서 수행된다.

III. 제한수신 시스템의 키관리

방송 프로그램과 정당한 가입자를 보호하기 위하여 도입한 제한수신 시스템에서 가장 기본적이자 가장 중요한 사항은 안전하게 키를 관리하는 것이다. 암/복호화에 사용되는 키가 노출되면 유료 방송 시스템내의 모든 보안 서비스가 공격당하게 되므로 키의 안전성을 위한 키관리 메커니즘은 그 어느 무엇보다도 중요하다. 또한 유료 방송 서비스에서는 사용자들의 가입과 탈퇴를 보장해야 하기 때문에, 새로운 가입자의 추가나 기존 가입자의 삭제를 용이하게 하고 가입자 증가에 따른 메시지의 증가를 최소화해야 한다는 점

에서도 키관리 메커니즘의 중요성이 부각된다. 이를 위해서는 서비스 및 과금 형태에 따라 그룹을 형성하고 키를 공유해야 한다. 따라서 공유되는 그룹키의 갱신 및 그룹내에서 특정 가입자의 삭제는 문제시 될 수 있다[9,10].

본 장에서는 그룹 구성원의 가입이나 탈퇴와 같은 동적인 그룹 이벤트에 대처할 수 있는 그룹키 관리 프로토콜을 제안한다. 제안하는 그룹키 관리 프로토콜은 초기의 그룹키 교환 프로토콜 IKEP와 그룹 내에서 탈퇴(leave) / 가입(join) 등의 이유로 그룹 멤버의 변화가 일어날 때 그룹키를 효율적으로 갱신하는 프로토콜 SLP / SJP의 세 개로 구성되어 있다. 각 프로토콜들의 자세한 동작과정은 다음과 같다.

① IKEP(Initial Key Exchange Protocol):

$MG=\{U_1, U_2, \cdots, U_n\}$는 프로토콜에 참가하는 n명의 사용자 U_i ($i=[1,n]$)들로 이루어진 그룹으로, U_n은 방송국이며 $U_1, U_2, \cdots, U_{n-1}$은 가입자들이다.

▸ 초기화단계: 시스템 파라미터는 $\langle G_1, G_2, e, p, P, H, H_Q \rangle$ 이다. 여기서 G_1과 G_2는 위수가 임의의 k-bit의 큰 소수 p인 순환군으로, G_1은 타원곡선 $E(F_p)$위의 점들로 이루어진 덧셈군이고, G_2는 F_{p^2}의 부분군으로 곱셈군이다. 이때 k는 안전성 파라미터이다. 그리고 P는 G_1의 생성원이며, 함수 $e: G_1 \times G_1 \rightarrow G_2$는 Pairing이다. 그리고 $H: \{0,1\}^* \rightarrow Z_p^*$와 $H_Q: \{0,1\}^* \rightarrow G_1$는 암호 해쉬 함수들이다.

▸ 키 추출. 프로토콜의 초기 단계에서, 각 사용자 $U_i \in MG$들은 키 생성 알고리즘에 의해 각자의 개인 식별정보 ID_i에 대응되는 공개키와 비밀키 쌍 ($Q_i = H_Q(ID_i)$, $D_i = wQ_i$)을 얻는다. 여기서 $w \in {}_R Z_p^*$는 마스터키이고, $P_{pub} = wP$는 키 발급 기관의 공개키이다.

▸ 그룹키 설정 단계:

‣방송국 U_n은 임의의 정수 $s, v \in {}_R Z_p^*$를 선택하고, $P_S = sP$와 $P_V = vP$를 계산한다. 여기서 s와 v는 방송국이 비밀로 간직한다. $n-1$명의 가입자 $U_i \neq U_n$는 임의의 정수 $r_i \in {}_R Z_p^*$를 선택하여 부분키 $P_i = r_i P$를 생성한다. 그리고 자신의 공개키 Q_i와 비밀키 D_i를 사용하여

$O_i = H(P_i) D_i + r_i Q_i$를 계산하고

$M_i = U_i \| P_i \| O_i$를 방송국 U_n에게 전송한다. 여기서 r_i는 각 가입자가 비밀로 간직한다. ‣ $n-1$개의 메시지 M_i를 모두 전달받은 방송국은 가입자들로부터 전달받은 P_i가 정당한지를 확인하기 위하여 다음 방정식이 성립하는지를 체크한다.

$$\prod_{i=1}^{n-1} e(O_i, P) = \prod_{i=1}^{n-1} e(Q_i, H(P_i)P_{pub} + P_i)$$

만약 위의 방정식이 성립하지 않는다면 방송국은 P_i를 거부한다. P_i의 정당성 유무를 모두 확인한 후, 방송국은 임의의 정수 $z \in {}_R Z_p^*$를 선택하고, 각 가입자들이 그룹키 K를 생성하도록 하기 위하여, 방송국 U_n은 $T_i = z \cdot e(P_i, -svP)$를 계산하여 집합 $T = \{T_i \mid i \in [1, n-1]\}$를 생성하고 $g = e(P, svP)$를 계산한다. 그리고 $M_n = g \| T$를 그룹내의 모든 가입자 U_i에게 브로드캐스트를 한다. 방송국으로부터 메시지 M_n를 전달받은 각 가입자 $U_i \neq U_n$는 $z = T_i \cdot g^{r_i}$를 계산하고, 그룹 MG의 모든 구성원들은 이를 사용하여 그룹키 $K = H(z \| T)$를 생성한다.

② SLP(Subscribe Leave Protocol): MG_L는 사용자 집합 L이 그룹 MG를 탈퇴하여 새롭게 형성된 그룹이다.

▸ 그룹키 갱신 과정:

‣방송국 U_n은 새로운 임의의 정수 $s', v', z' \in {}_R Z_p^*$를 선택하고, $P_S' = s'P$와 $P_V' = v'P$를 계산한 후, IKEP 프로토콜을 그대로 수행하여 T'를 계산하여 새로운 그룹 MG_L의 그룹키 $K = H(z' \| T')$를 생성한다. 그리고 방송국 U_n은 각 가입자 $U_i \in MG_L \setminus \{U_n\}$들이 그룹키를 갱신하도록 하기 위하여 $M_n' = T' \| g'$를 새로운 그룹 MG_L내의 모든 가입자에게 브로드캐스트

한다. 이때, $g' = e(P, s'v'P)$이다.

각 가입자 $U_i \in MG_L \setminus \{U_n\}$는 IKEP 프로토콜을 그대로 수행하여 $z' = T'_i \cdot g'^{r_i}$ ($i = [1, n-1] \setminus \{L\}$)를 계산한 후, 새롭게 형성된 멀티캐스트 그룹 MG_L에 대한 그룹키 $K = H(z' \| T')$를 생성한다.

③ SJP(Subscribe Join Protocol): MG_J는 사용자 집합 J가 그룹 MG에 새롭게 가입하여 생성된 그룹이다.

▸그룹키 갱신 과정:

‣새롭게 그룹에 가입하는 가입자 $U_j \in J$들은 임의의 정수 $r_j \in Z_p$를 선택하여 부분키 $P_j = r_j P$를 계산한다. 그리고 IKEP 프로토콜에서와 같이 $O_j = H(P_j) D_j + r_j Q_j$를 계산하고 $M_j = U_j \| P_j \| O_j$를 방송국 U_n에게 전송하여 자신을 인증한다.

‣방송국 U_n는 IKEP 프로토콜과 동일한 방법으로 가입자 $U_j \in J$로부터 전달받은 P_j가 정당한지를 확인한 후, 새로운 임의의 정수 s'', v'', $z'' \in {}_R Z^*_p$를 선택하고, $P_S'' = s''P$와 $P_V'' = v''P$를 계산한 후, IKEP 프로토콜을 그대로 수행하여 T''를 계산하여 새로운 그룹 MG_J의 그룹키를 생성한다. 그리고 방송국 U_n는 각 가입자 $U_i \in MG_J \setminus \{U_n\}$들이 그룹키를 갱신하도록 하기 위하여 $M_n'' = T'' \| g''$를 새로운 그룹 MG_J내의 모든 가입자에게 브로드캐스트 한다. 이때, $g'' = e(P, s''v''P)$이다.

각 가입자 $U_i \in MG_J \setminus \{U_n\}$는 IKEP 프로토콜을 그대로 수행하여 $z'' = T''_i \cdot g''^{r_i}$ ($i = [1, n-1] \cup \{J\}$)를 계산한 후, 새롭게 형성된 멀티캐스트 그룹 MG_J에 대한 그룹키 $K = H(z'' \| T'')$를 생성한다.

IV. 제안하는 위성 DMB에서의 유료시청권한 제어 시스템

유료위성방송을 위한 시청권한 제어란 트래픽제어시스템(TCS: Traffic Control System)에서 생성된 상품 및 서비스(통상 채널의 패키지 또는 프로그램 등) 정보를 기준으로 가입자 관리 시스템(SMS: Subscriber Management System)에서 유료가입자를 모집하여 가입자를 생성하고 가입자가 선택한 상품 서비스 및 기타 마케팅정보를 제한수신 시스템을 통하여 전송하며 이 정보를 스트림서버에서 출력되는 방송스트림 정보에 포함하여 위성으로 암호화하여 전송하면, 수신 이동 단말기에서 이 스트림정보에 포함되어 있는 명령과 키정보를 단말기에 저장되어 있는 보안알고리즘 체계에 의해 해당되는 제어 명령이나 시청권한정보를 기록하고, 암호화되어 전송된 채널의 출력스트림이 자신의 시청권한과 일치 할 경우 제한수신 시스템의 보안 메커니즘에 따라 복호화를 행하고 해당 가입자의 단말기 화면에 표시되도록 하는 각종 명령 규칙을 말한다.

본 장에서는 유료 위성 DMB를 위한 시청권한 제어 시스템을 설계한다. 제안하는 시스템은 3장에서 제안한 개인식별정보에 기반한 안전한 그룹키 관리 프로토콜을 이용하여 가입자와 가입자 관리 시스템간의 인증 및 정상적인 방송 시청을 위해 가장 중요한 암/복호화키(group key)를 분배하도록 한 새로운 시스템이다.

본 시스템은 송신측, 위성 DMB 방송망, 수신측 등 크게 세 부분으로 구성되며, 송신측은 방송국과 가입자 관리 시스템으로 구성된다. (그림 2)는 시스템의 구성과 필요한 모듈들을 나타낸다. 본 시스템에서, 제작된 방송 **AV**은 CW라는 키 값을 사용하여 스크램블링/디스크램블링하기 때문에, 송신측과 수신측은 CW를 공유하고 있어야 한다. 일반적으로 CW는 불법도청의 공격을 막기 위해 주기적으로 변하도록 설계를 하고 자격통제메시지(ECM)에 암호화된 형태로 저장되어 수신측에 전송된다. 여기에 사용되는 암호키가 K이며, K는 IKEP 프로토콜 실행으로 생성된다. (그림 3)은 본 시스템의 전반적인 동작과정을 나타낸 것이다.

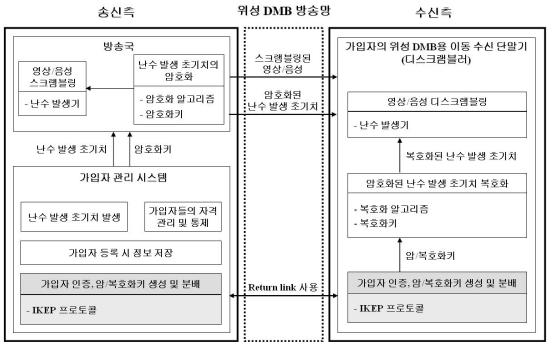

그림 2. 제안하는 시스템의 전체적 구성
Fig 2. Structure of Our System

송신측	위성 방송망	수신측
AV 제작 CW 생성 I=PRNG(CW) J=SCR$_I$(**AV**) K 생성 (by IKEP) F=E_K(CW)	K 생성정보, J, F →	K 생성 (by IKEP) CW=D_K(F) I=PRNG(CW) **AV**=SCR$_I^{-1}$(J)

그림 3. 제안하는 시스템의 동작 과정
Fig 3. Execution of Our System

4.1 제안 시스템

제안하는 위성 DMB에서의 유료시청권한 제어 시스템의 동작과정을 좀 더 세부적으로 살펴보면 다음과 같다.

4.1.1 시스템 파라미터

제안하는 위성 DMB에서의 유료시청권한 제어 시스템에서 사용하는 시스템 파라미터의 정의는 다음과 같다.

- **U**: 위성 DMB 방송국(Broadcasting station)에 가입한 모든 가입자들의 집합
- **AV**: 제작된 상품(채널의 패키지, 프로그램 및 서비스 등)들의 집합
- $G_{content}$ = { $U_1, U_2, \cdots, U_n$ } $\subseteq$ **U**: 같은 상품 $content \in$ **AV**을 신청한 가입자들 $U_1, U_2, \cdots, U_{n-1}$과 방송국 U_n으로 구성된 그룹
- K: $G_{content}$의 그룹키 즉, CW에 대한 암/복호화키
- ID: 가입자 U_i가 구매한 이동 단말기의 고유식별정보(serial number)
- CW: 난수 발생 초기치인 컨트롤 워드(Control Word)
- PRNG: 의사난수발생기(Pseudo Random Number Generator)
- I = PRNG(CW): CW를 초기치(seed)로 하여 의사난수발생기를 통해 발생시킨 의사난수열(pseudo random bit sequences)
- SCR$_I$(x): x를 I로 스크램블링한 값
- SCR$_I^{-1}$(y): y를 I로 디스크램블링한 값
- E_K(CW): K를 키로 하여 CW를 암호화한 값
- D_K(F): K를 키로 하여 F를 복호화한 값

4.1.2 시스템 동작 과정

[가입자 등록 과정]

① 가입을 원하는 사용자 U_i가 방송국의 가입자 관리 시스템에게 유료 가입 신청을 하면, 가입자 관리 시스템은 가입자 U_i의 위성 DMB용 이동 단말기의 고유식별정보 ID_i에 대한 공개키와 비밀키를 생성하고, 이를 안전한 통신 채널을 이용하여 가입자 U_i에게 발급한다. 이때, 공개키 Q_i와 비밀키 D_i는 3장에서 제안된 IKEP 프로토콜의 실행에 따른다.

$Q_i = H_Q(ID_i)$, $D_i = wQ_i$

방송국		가입자 $U_i \in$ **U**
$Q_i = H_Q(ID_i)$ $D_i = wQ_i$ (by IKEP)	가입자 정보 ← Q_i, D_i → (안전한 통신 채널)	가입신청

그림 4. 제안하는 시스템의 가입자 등록 과정
Fig 4. Registration of a Subscriber under Our System

[가입자의 상품 선택/등록 과정]

② 가입자 U_i는 판매되는 프로그램 정보를 보고 이용할 상품 $content \in$ **AV**을 선택한다.

③ 가입자 U_i는 IKEP 프로토콜의 실행에 따라, 임의의 정수 $r_i \in Z_p$를 선택하고, P_i와 O_i를 계산한다.

$P_i = r_i P$, $O_i = H(P_i)D_i + r_i Q_i$

④ 가입자 U_i는 이동통신망을 리턴 링크(Return Link)로

이용하여, M_i를 방송국의 가입자 관리 시스템으로 전송한다.

$M_i = Inf_{content} \| U_i \| P_i \| O_i$

여기서 $Inf_{content}$는 가입자 U_i가 선택한 상품 $content$에 대한 정보이다.

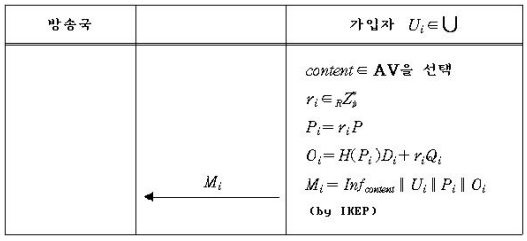

그림 5. 제안하는 시스템의 가입자의 상품선택/등록 과정
Fig 5. Choice Content and its Registration by subscriber under our System

[각 상품별 그룹 생성 과정]

⑤ 가입자 관리 시스템은 가입자들이 선택한 상품을 기준으로 가입자들을 분류하여 각 그룹들을 생성한다. 즉, 하나의 그룹은 같은 상품을 선택한 사용자들과 방송국으로 구성된다.

$G_{content} = \{ U_1, U_2, \cdots, U_n \} \subseteq \bigcup$ 를

$content \in$ **AV**을 신청한 가입자

$U_1, U_2, \cdots, U_{n-1}$와 방송국 U_n으로 구성된 그룹이라고 하자.

[그룹 $G_{content}$에 대한 유료시청권한 제어 과정]

⑥ 가입자 관리 시스템은 IKEP 프로토콜을 실행하여, P_i ($i \in [1, n-1]$)의 정당성 유무를 모두 확인하고, 그리고 이들을 사용하여 $G_{content}$의 그룹키 K를 생성하고, g와 T를 계산한다.

$K = H(z \| T)$

$g = e(P, svP)$

$T = \{ T_i \mid i \in [1, n-1] \}$

여기서 $T_i = z \cdot e(P_i, -svP)$ 이다.

⑦ 방송국은 K로 CW를 암호화한 값 F를 계산한다.

$F = E_K(CW)$

⑧ 방송국은 CW를 사용하여 난수 I를 발생시킨다.

$I = PRNG(CW)$

⑨ 방송국은 $content$를 I로 스크램블링한 값 J를 생성한다.

$J = SCR_I(content)$

⑩ 방송국은 위성 방송망을 통하여 g, T, J와 F (여기서 F는 자격통제메시지(ECM)내에 담겨 있음)를 브로드캐스팅하고, 가입자 U_i ($i \in [1, n-1]$)의 단말기들은 이것을 수신한다.

⑪ 위성으로부터 g, T, J와 F를 수신한 가입자 U_i ($i \in [1, n-1]$)의 단말기는 IKEP프로토콜을 실행하여, 그룹 $G_{content}$의 그룹키 K를 생성한다.

$K = T_i \cdot g^{r_i}$

⑫ 가입자 U_i ($i \in [1, n-1]$)의 단말기는 F를 K로 복호화하여 CW를 계산한다.

$CW = D_K(F)$

⑬ 단말기의 디스크램블러는 CW를 사용하여 난수 I를 얻는다.

$I = PRNG(CW)$

⑭ 단말기의 디스크램블러는 I를 이용하여 위성 수신한 J를 디스크램블링하여 가입자 U_i ($i \in [1, n-1]$)가 선택한 상품 $content$을 얻는다. 그리고 $content$는 해독되어 가입자 U_i ($i \in [1, n-1]$)의 단말기 화면에 나타난다.

$content = SCR_I^{-1}(J)$

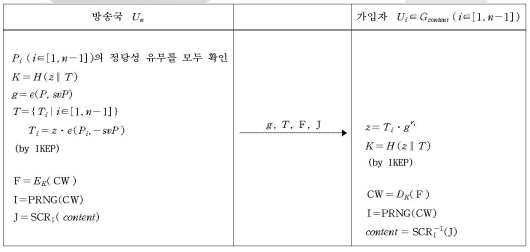

그림 6. 제안하는 시스템의 그룹 $G_{content}$에 대한 유료시청권한 제어 과정
Fig 6. Control of Conditional Access of Group $G_{content}$ to Pay-TV Program under Our System

4.2 제안 시스템의 장점

과거의 제한수신 시스템은 TV와 연결된 셋탑 박스(Set-top box)에 복호화 알고리즘과 비밀키가 저장되어 있는 구조로 도/시청의 발생 가능성을 내포하고 있었다. 도/시청의 가장 널리 알려진 방법으로 TV 셋탑 박스 자체를 하드웨

어 복제하는 것을 예로 들 수 있다. 이러한 도/시청을 막는 방법 중 하나는 각 가입자 TV의 셋탑 박스를 정기적으로 교체하여 복호화 알고리즘이나 비밀키를 갱신하는 것이다. 그러나 이는 비경제적인 해결책으로, 대신 디스크램블러와 분리가능한 스마트카드를 발급하여 모든 복호화 알고리즘과 비밀키를 스마트카드 내에 저장하는 시스템이 일반화되었다[11].

그러나 이러한 스마트카드를 이용하는 제한수신 시스템의 경우, 가입자는 카드 리더기(card adaptive device)를 구비해야 하고, 스마트카드 내의 복호화 알고리즘이나 비밀키를 주기적으로 갱신해주어야 한다. 또한 대부분 디스크램블러와 스마트카드가 일체화되어 있는 형태이므로, 지신의 TV 셋탑 박스가 설치되어있지 않은 다른 장소에서는 시청을 할 수 없고, 셋탑 박스를 타인에게 양도시 자격 갱신과 관련된 복잡한 절차를 필요로 하는 등 사용상 많은 제한을 받게 된다.

본 논문에서 제안하는 유료시청권한 제어 시스템은 스마트카드 대신 안전한 그룹키 관리 프로토콜을 이용하는 새로운 위성 제한수신 시스템이다. 제안하는 새로운 유료시청권한 제어 시스템은 안전한 그룹키 관리 프로토콜을 이용하여 가입자와 가입자관리시스템간의 인증 및 정상적인 방송 시청을 위해 가장 중요한 암/복호화키를 다운로딩한다. 본 논문에서 제안한 시스템이 갖는 장점은 다음과 같다.

① 시청시마다 스마트카드를 휴대할 필요가 없다.

② 스마트카드 리더기를 TV 셋탑 박스내에 내장할 필요가 없어 비용 절감의 효과가 있다.

③ 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러와 가입자간의 독립성이 유지되므로 장소에 구애받지 않고 원하는 방송을 시청할 수 있다.

④ 컨트롤 워드에 대한 암/복호화키를 스마트카드등의 수신측 보안 모듈(user security module)에 저장하는 것이 아니라 가입자가 시청 요구를 할 때마다 전송하므로 갱신 주기를 방송국 사정에 따라 자유자재로 조정할 수 있다.

⑤ 기존의 제한수신 시스템과 비교하여 방송국의 가입자 관리 시스템의 암/복호화키의 암호화 모듈을 제거하였고, 수신측의 암호화된 컨트롤 워드 복호화 과정도 간략화 하여 계산량을 줄였다.

⑥ 개인식별정보에 기반하는 방식을 사용함으로써, 가입자 관리 시스템에서의 키 관리가 용이하다.

⑦ 사용자들의 가입이나 기존 가입자들의 탈퇴 또는 규약 위반 등에 의해 퇴출될 경우가 발생할 때, 이에 따른 암/복호화키의 갱신이 가능하며, 그리고 새롭게 가입한 가입자들이 가입 이전의 통신에 대해 정보를 얻을 수 없으며 탈퇴·퇴출된 가입자들이 탈퇴·퇴출 이후의 통신에 대해 정보를 얻을 수 없다.

⑧ 송신측에서 일방적으로 수신측으로 프로그램을 송출하는 형태의 기존의 일방향 제한수신 시스템과는 달리 가입자의 요구사항을 방송국에서 접수하고 그에 대한 적절한 데이터를 전송하는 형태의 양방향 한정수신 시스템 모두 적용이 가능하다.

V. 결 론

본 논문에서는 그룹키 관리 프로토콜 기반의 유료시청권한 제어 시스템을 제안하였다. 제안한 시스템은 IKEP 프로토콜을 이용하여 가입자와 가입자 관리 시스템간의 인증 및 키를 분배하도록 한 새로운 시스템으로, 특히, 가입자가 단 한 번의 지수승 연산만으로 암/복호화키를 생성할 수 있기 때문에 단말기의 소형화 경향으로 인해 제한된 시스템 자원을 보유한 가입자들로 구성된 위성 DMB 등에 적용될 수 있는 효율적인 방식이다.

본 논문에서 제안한 그룹키 관리 프로토콜이나 이를 기반으로 하는 유료시청권한 제어 시스템 모델을 활용한 방송 시스템이 보편화 될 경우, 국내 위성 DMB 방송 관련 사업의 활성화가 이루어져 양방향 이동 멀티미디어 서비스 사회의 현실화가 한층 가속되리라 기대된다. 그리고 더 나아가 다양한 양방향 서비스 개발을 위하여 보다 진보된 위성 DMB 시스템 모델을 만들어 내는데 이바지 할 수 있으며, 이것을 통하여 새롭게 시작되는 위성 DMB 방송의 비즈니스 접근 방법이 더욱 구체화되고 구현 가능성이 높은 비즈니스 수익모델을 만들어 낼 수 있을 것이라 생각한다. 아울러 인터넷 시장의 주류를 이루고 있는 E-Commerce와 M-Commerce에 이어 T-Commerce 활성화에 활용될 수 있을 것이다.

참고문헌

[1] Vendela Paxal, telenor R&D, "DVB with Return Channel via Satellite", DVB-RCS200, 2000.

[2] ETSI, "Digital Audio Broadcasting(DAB) to Mobile, Portable and Fixed Receivers", EN 300 401 V1.3.3, 2001.

[3] Document TM 2465, "The Convergence of Broadcast & Telecomms Platforms, Executive Summary", Ad hoc Group DVB-UMTS of the DVB Project, 2001.

[4] ETSI, "Digital Video Broadcasting(DVB): Support for Use of Scrambling and Conditional Access(CA) within Digital Broadcasting Systems", ETR 289 V1, 1996.

[5] ETSI, "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications", ETSI EN 50221 V1, 1997.

[6] S. Berkovits, "How To Broadcast A Secret", Advances in Cryptology-Eurocrypt'91, LNCS 547, pp. 535~541, Springer- Verlag, 1991.

[7] B.-M. Macq and J.-J. Quisquater, "Cryptology for Digital TV Broadcasting", Proc. of the IEEE, 83(6):944-57, 1995.

[8] S. Tranter, "An Overview of Digital Broadcasting", NDS Ltd. 2001.

[9] A. Wool, "Key Management for Encrypted Broadcast", Proc. of the 5th ACM conference on Computer and Communications Security, pp. 7-16, Springer -Verlag, 1998.

[10] A. Narayanan, C.P. Rangan, and K. Kim, "Practical Pay TV schemes", Proc. of the 9th Australasian Conference on Information Security and Privacy, LNCS 2727, pp. 192-203, Springer -Verlag, 2003.

[11] 은성경, 조현숙, "유료방송 해킹 방지 기법", NETSEC -KR'99, 1999.

저 자 소 개

김 현 주

1995년 세명대학교 수학과(이학사)
1997년 서강대학교 대학원 수학과 (이학석사)
2005년 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
현재 성균관대학교 정보통신공학부 연구전임강사
<관심분야> 암호이론, 이동통신보안

김 승 주

1994년 성균관대학교 정보공학과 (공학사)
1996년 성균관대학교 대학원 정보공학과(공학석사)
1999년 성균관대학교 대학원 정보공학과(공학박사)
현재 한국정보보호학회 논문지 편집위원
현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
현재 성균관대학교 정보통신공학부 교수
현재 한국정보과학회 논문지 편집위원
<관심분야> 암호이론, 정보보호제품 및 스마트카드 보안성평가

원 동 호

성균관대학교 전자공학과(학사, 석사, 박사)
1988년~1999년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2003년~2004년 성균관대학교 연구처장
1982년~현재 성균관대학교 정보통신공학부 교수
2000년~현재 정보보호인증기술연구소장
<관심분야> 암호이론, 정보시스템보안 등

한 우 철

건국대학교 대학원 산업공학과(공학박사)
현재 대림대학 산업시스템 경영과 교수
<관심분야> 의사결정지원시스템 경영정보시스템