디지털 유료 방송시스템에 적합한 키 관리 모델에 관한 연구

정회원 양 형 규*

A Study on Efficient Key Management Model for Digital Pay-TV System

Hyung-kyu Yang* *Regular Member*

요 약

최근 들어, 정보통신 기술의 발달과 함께 디지털 방송 기술이 주목을 받으면서 제공되는 컨텐츠들에 대한 보호의 중요성이 증대되고 있다. 하지만, 이러한 여러 가지 디지털 방송 서비스의 활성화를 위해서는 방송 컨텐츠의 보호, 송수신자간의 상호 인증 등 여러 가지 보안 서비스가 제공되어야 한다. 그러므로 본 논문에서는 기존의 디지털 방송 시스템의 안전성 및 효율성을 분석하고, 디지털 유료 방송 시스템에 적합한 키 관리 모델을 제안한다.

Key Words : Key management, pay-tv, group key

ABSTRACT

Recently, with the development of information and communication technology, digital pay-TV technology is paid attention. So the protection of the provided contents is becoming more important. However, in order to encourage an active based on digital TV, the contents and information sent and received respectively by the broadcaster and the subscriber must be protected. Therefore, in this paper, I analyze the requirements to protect the digital contents, the security and efficiency of the previous digital pay-TV system model. Then I proposed a key management model for digital pay-TV system.

Ⅰ. 서 론

최근 정보통신기술의 발달과 함께 디지털 TV의 서비스 영역이 다양한 분야로 확대되면서 시청자들과 방송사 사이에 다양한 요구가 증가하고 있다. 특히 이러한 서비스 분야의 확대는 주문형 비디오(VOD), TV 상거래, 실시간 여론조사 등과 같은 시청자의 참여가 가능한 서비스의 형태로 이어질 것으로 기대된다. 하지만, 다양한 디지털 TV 서비스의 활성화를 위해서는 방송 콘텐츠의 보호, 송수신자간의 상호 인증 등 여러 가지 보안 서비스가 반드시 제공되어야 한다. 정보 보안이 제대로 이루어지지 않을 경우 서비스의 가용성을 침해당하거나 비인가된 사용자에게 기밀 정보가 노출될 수 있고 금융·경제적인 혹은 다른 정보들의 신뢰도가 감소될 위험이 존재하기 때문이다. 예를 들면, 일정한 회비를 지불해야만 서비스를 받을 수 있는 VOD 서비스는 암호키를 발급 받지 못한 비회원은 영상 서비스를 받을 수 없도록 하는 조처가 있어야 하며, 주식 시세 정보와 같은 응용에서는 투자자는 정보 제공자에

※본 논문은 2005년도 강남대학교 교내 연구비 지원에 의한 것임.
* 강남대학교 컴퓨터미디어공학부 (hkyang@kangnam.ac.kr)
논문번호 : KICS2005-11-458, 접수일자 : 2005년 11월 15일

대한 신원을 확신할 수 있어야만 수신된 시세정보의 신뢰성을 확보할 수 있다.

정보의 기밀성, 데이터의 무결성, 사용자 인증 등과 같은 보안 서비스는 PKI 기술과 키 교환 프로토콜의 결합을 통하여 효율적으로 이루어질 수 있다. 특히, 전송되는 방송 콘텐츠의 보호를 위해서는 단일 송신자와 다수의 수신자사이에 효율적으로 방송내용을 암호화하고 복호화 할 수 있는 메커니즘이 필수적으로 요구된다. 하지만 전송되는 콘텐츠의 암·복호화에 이용되는 비밀 암호키를 설정하기 위해 현재 가장 널리 사용되는 Diffie-Hellman (DH) 키 합의 프로토콜은 이러한 방송 시스템에는 적합하지 않다. DH 키 합의 프로토콜은 통신 당사자들이 키를 공유하기 위해 제안된 프로토콜이므로 이 프로토콜을 이용하게 되면 송신자는 각 수신자별로 별도의 암·복호화 키를 설정해야 하는 문제를 가지고 있다. 이 경우 송신자는 같은 방송 내용에 대해 수신자의 수만큼 암호화 과정을 반복 수행하게 되므로 효율적이지 못하다 할 수 있다.

그러므로, 안전하고 효율적인 데이터방송 시스템을 구축하기 위해서는 위와 같은 문제점의 해결이 선행되어야 하며, 이를 위해 송신자와 수신자의 안전한 통신을 위한 키 관리 문제가 선결되어야 한다. 그러므로 본 논문에서는, 방송 단말(셋톱박스)과 방송국에서의 안전성 요구사항을 분석하여 이를 바탕으로 유료방송시스템에 적합한 키 관리 모델을 제안한다.

Ⅱ. 디지털 유료 방송시스템 모델의 안전성 및 효율성 요구사항

디지털 유료 방송시스템의 기본적인 안전성 요구사항은, 시청료를 지불하지 않은 비인가자는 방송내용을 시청할 수 없어야 한다는 것이다. 이는 방송사의 수익과도 밀접한 관련이 있는 부분이며 시청자 또한 정당하게 시청료를 지불하고 방송시스템을 이용하였을 경우, 정당하지 않은 비인가자로부터의 불이익을 방지하기 위한 필수적인 요구사항이라 할 수 있다.

2.1 Perfect Forward Secrecy(PFS)

방송국 또는 시청자의 장기 비밀 값이 노출되더라도 공격자는 과거의 암호화된 방송내용을 복호화하여 시청할 수 없어야 한다.

2.2 Known Key Security(KKS)

방송국과 시청자 사이의 과거의 세션키가 노출되더라도 현재 또는 미래의 암호화된 방송 내용을 볼 수 없어야 한다.

2.3 Memory Dump Attack(MDA)

트로이 목마와 같은 바이러스가 방송국의 서버와 시청자의 셋톱 박스에 설치되어 메모리의 모든 정보가 노출되더라도 공격자는 과거나 미래의 암호화된 방송 내용을 볼 수 없어야 한다.

2.4 방송사와 시청자의 연산량 최소화

방송 시청자들이 사용하는 저 CPU, 저 메모리의 셋톱박스(STB : Set-Top Box)는 제한된 연산 능력을 가지고 있다. 따라서, 시청자들은 키 설정 시의 연산을 최소화하여야 하며, 암호화된 방송내용을 최소한의 연산으로 복호화 할 수 있어야 한다.

유료방송시스템은 다수의 시청자를 대상으로 많은 양의 방송내용을 전송하여야 한다. 따라서 방송국은 방송내용을 최소한의 연산으로 암호화 할 수 있어야 한다.

2.5 안전하고 효율적인 키 관리

방송국과 시청자는 효율적으로 암·복호화를 하기 위해 필연적으로 비밀키를 사용하게 되며 따라서 이러한 암·복호화 키의 효율적인 관리가 중요하다.

Ⅲ. 관련 연구

본 장에서는 기존의 디지털 유료 방송시스템을 위해 제안된 키 관리 모델의 효율성과 안전성을 분석하고, 이를 바탕으로 디지털 유료 방송시스템에서의 안전성과 효율성 요구사항을 3장에서 분석한다. 본 논문에서는, 기존의 모델에 대한 분석을 위해 하나의 방송국과 3명의 시청자들로 구성되었다고 가정하고 설명한다.

3.1 기존 디지털 유료 방송시스템

[파라미터 및 용어의 정의]

- U_4 : 방송국
- U_1, U_2, U_3 : 시청자
- C : 방송내용
- PK_X : X의 공개키
- SK_X : X의 개인키
- K : 공통의 세션키
- GK : 공통의 그룹키

- $E_K()$: K를 이용한 암호화
- $D_K()$: K를 이용한 복호화
- r_i : i 번째 사용자가 선택하는 비밀 랜덤 수
- p : 큰 소수
- g : Z_p에서 위수 q를 갖는 원시원소

3.1.1 공개키 암호화 방식 기반 키 관리 모델

공개키 암호화 방식에 기반한 디지털 유료 방송 시스템에서의 키 관리 모델에서는, 방송국은 시청자들의 공개키를 이용하여 방송내용을 암호화하고 시청자들에게 전송해 주는 방식이며, 이때 방송내용의 암호화에 사용되는 방식은 RSA 암호 방식과 같은 공개키 암호화 방식이다.

3.1.1.1 방송 데이터 송·수신 과정

(1) 방송국은 수신료를 지불한 시청자들의 공개키를 이용하여 방송내용을 암호화한 후 시청자들에게 브로드캐스트 한다.

(2) 시청자들은 방송국으로부터 전송 받은 암호화된 방송내용을 자신의 개인키로 복호화하여 방송내용을 시청한다.

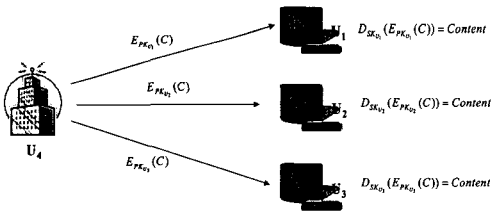

그림 1. 공개키 암호방식 기반 방송 데이터 송·수신 과정

본 모델에서는 방송국은 같은 방송내용을 서로 다른 시청자의 공개키로 각각 암호화하여야 하므로 방송국의 연산량이 증가하게 된다. 그러므로 시청자가 n명으로 확장되게 되면 방송국은 n번의 암호화 연산을 수행하여야 하며, 방송데이터 사이즈 또한 n으로 증가하게 된다. 또한 방송국의 관리해야 하는 암호화키의 수도 n으로 증가하게 된다. 또한 본 모델에서는 PFS와 MDA가 제공되지 않는다.

3.1.2 키 전송 방식 기반 키 관리 모델

키 전송 방식을 기반으로 하는 키 관리 모델의 경우, 방송국은 세션키를 생성하여 정당한 시청자들에게 키 전송 방식으로 키를 분해한 후 방송국은 자신이 생성한 세션키를 이용하여 방송내용을 암호화하여 시청자들에게 전송해 주는 방식이다. 본 모델에서 사용하는 암호화 방식은 AES, SEED 등과 같은 대칭키 암호 방식이다.

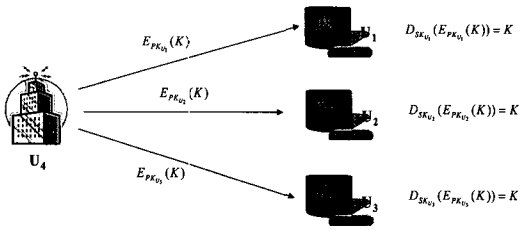

그림 2. 세션키 송수신 과정

(1) 방송국은 하나의 세션키를 생성하여, 수신료를 지불한 시청자들의 공개키를 이용하여 세션키를 암호화하고 시청자들에게 전송한다.

(2) 시청자들은 방송국으로부터 전송받은 암호화된 세션키를 복호화하여 세션키를 저장해둔다.

3.1.2.1 방송 데이터 송·수신 과정

(1) 방송국은 키 설정 단계에서 생성한 공통의 세션키 K로 방송내용을 암호화하고 시청자들에게 전송한다.

(2) 방송국으로부터 전송 받은 $E_K(content)$을 각 시청자들은 방송국으로부터 전송 받은 세션키로 복호화 하여 방송을 시청한다.

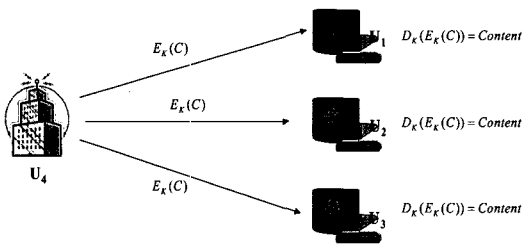

그림 3. 키 전송 방식 기반 데이터 송수신 과정

본 모델에서는 방송국이 세션키 K를 생성하고, 세션키 K를 이용하여 방송내용을 암호화한다. 이로써 방송국에서의 암호화 과정은 시청자의 증가와 상관없이 한 번에 이루어진다. 또한 본 모델은 매우 효율적이라 할 수 있지만, PFS와 MDA을 제공하지 않는다는 단점을 가지고 있다. 다시 말하면, 장기 비밀 값이 노출되었을 경우, 과거나 미래의 방송내용의 안전성이 보장되지 않는다. 또한 악의적인 공격자에 의해 방송국 서버 또는 셋톱박스 메모리의 정보가 노출될 경우 과거 방송내용의 안전성이 보장되지 않는다는 단점을 가지고 있다.

3.2 키 합의 방식 기반 키 관리 모델

키 합의 방식에 기반한 키 관리 모델에서는, 방송국은 Diffie-Hellman 키 합의 방식으로 시청자들의 세션키를 생성한 후 방송국은 이 세션키를 이용하여 방송내용을 암호화 하고 시청자들에게 전송해 주는 방식이다.

3.2.1 키 합의 단계

(1) 방송국과 시청자들은 방송내용을 암호화할 때 사용할 세션키를 Diffie-Hellman 방식으로 생성하여 서로 공유한다.

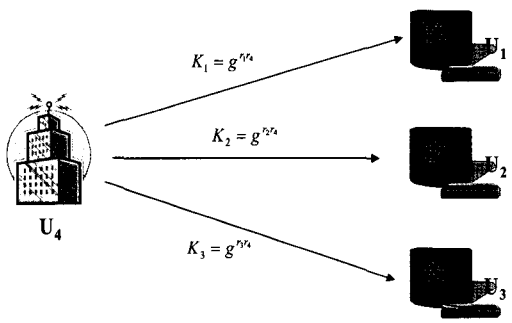

그림 4. 디피-헬만 방식을 이용한 키 합위 과정

나. 방송 데이터 송·수신 과정

(1) 방송국은 키 설정 단계에서 생성한 각각의 세션키로 방송내용을 암호화하고 시청자들에게 브로드캐스트 한다.

(2) 방송국으로부터 전송 받은 암호화된 방송내용을 각 시청자들은 방송국과 공유한 각각의 세션키로 복호화 하여 방송을 시청한다.

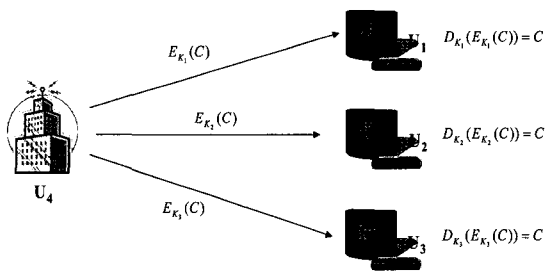

그림 5. 키 합의 방식 기반 데이터 송수신 과정

본 모델에서는 방송국과 시청자들이 각각 Diffie-Hellman 방식으로 세션키를 공유한다. 그러나 이러한 세션키 공유 방법은 시청자의 수가 증가함에 따라 세션키의 수도 비례하여 증가하게 된다. 그러므로 시청자가 n명일 경우 방송국의 암호화 과정, 암호화키의 수, 방송데이터의 사이즈 모두 n이 된다.

3.3 브로드캐스팅 암호화 방식 기반 키 관리 모델

브로드캐스팅 암호 방식에 기반한 키 관리 모델에서는 기존에 잘 알려진 브로드캐스팅 암호화 방식을 이용하여 키를 관리하는 모델이다. 이러한 브로드캐스팅 암호화 기법을 이용한 모델은 실제 디지털 유료 방송시스템과 가장 가까운 모델이라 할 수 있다.

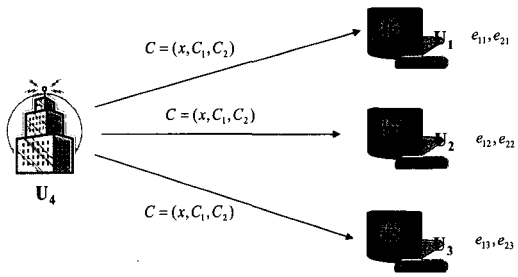

그림 6. 브로드캐스팅 기반 데이터 송수신 과정

[파라미터]

- p, q : 큰 소수
- N : 서로 다른 큰 소수 p, q의 곱
- d_1, d_2 : 개인키
- e_{1n}, e_{2n} : n번째 시청자의 비밀키 쌍
- X: 서로소인 값
- G: Z_n^*상에서 랜덤하게 선택된 이차잉여
- M: 방송내용
- N은 공개정보이며 p, q, d_1, d_2는 비밀 정보이다.

3.3.1 방송 데이터 송·수신 과정

(1) 방송국은 x, g을 선택하여 방송내용을 다음과 같이 생성한 후 $C = (x, C_1, C_2)$ 메시지를 시청자들에게 브로드캐스트 해준다.

(2) 방송국으로부터 전송 받은 메시지를 각 시청자들은 자신의 비밀키 쌍을 이용하여 복호화 한 후 방송 시청을 한다.

본 모델에서는 방송국은 브로드캐스팅 암호화 기법을 이용하여 방송내용을 암호화하여 전송해주며, 각 시청자들은 비밀키쌍을 이용하여 방송내용을 시청할 수 있는 방식이다. 암호방식이 비대칭 알고리즘(RSA 암호화 방식)를 사용함으로써 대칭키 암호 알고리즘에 비해서는 계산 효율성이 떨어진다. 또한 브로드캐스트 암호화 기법을 사용함으로써 방송국에서의 암호화 과정, 방송데이터 사이즈, 암호화키의

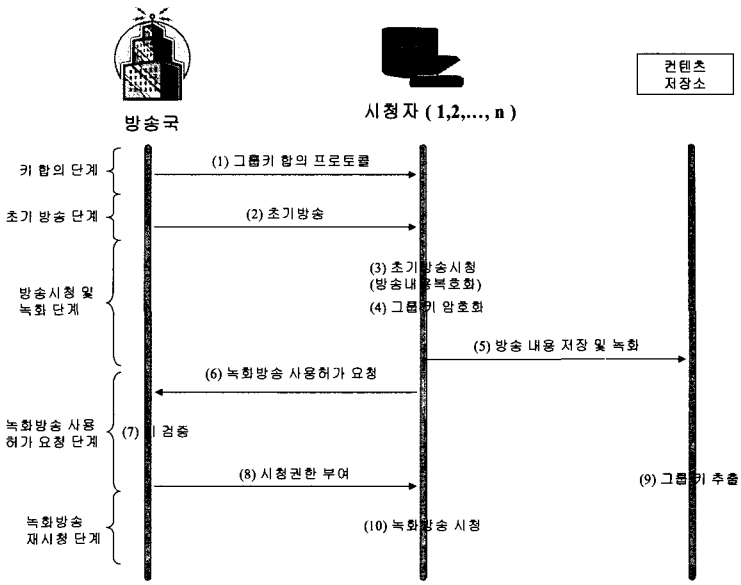

그림 7. 제안하는 유료 방송시스템에서의 키 관리 모델

표 1. 기존 키 관리 모델 비교·분석

	공개키암호화 방식기반	키전송방식 기반	키합의방식 기반	브로드캐스팅 암호화방식기반
키 교환 방식	없음	있음(키 전송)	있음(키 합의)	없음
방송국의 암호화	n	1	n	1
암호 알고리즘	비대칭 알고리즘	대칭 알고리즘	대칭 알고리즘	비대칭 알고리즘
암호화 키의 수	n	1	n	1
데이터 사이즈	n	2	n	1
PFS	X	x	o	x
KKS	N/A	o	o	N/A
MDA	X	x	o	x

수에서 효율적이다. 하지만, PFS, MDA가 모두 제공되지 않는 단점을 가지고 있다. 즉, 장기 비밀 값이 노출되었을 경우, 과거나 미래의 방송내용의 안전성이 보장되지 않는다.

3.4 기존 디지털 유료 방송시스템 모델들의 안전성 및 효율성 비교·분석

다음의 표 3은 기존 디지털 유료 방송시스템 모델들에 대한 안전성 및 효율성에 대하여 비교 분석한 것이다.

Ⅳ. 제안하는 키 관리 모델

본 장에서는 2장과 3장을 통해 분석하고 도출한 디지털 유료 방송시스템에서의 안전성과 효율성 요구사항을 만족시키기 위한 키 관리 모델을 제안한다.

본 모델은 유료시청자만이 방송국으로부터의 초기 송출 방송을 시청할 수 있으며, 시청자가 방송을 녹화한 후 녹화된 방송을 시청하기 위해서는 지정된 요금을 지불해야 하는 모델이다.

[키 합의 단계]

(1) 방송국은 정당한 시청자들과 그룹키 합의 프로토콜을 이용하여 암호 통신에 사용할 공통의 세션키를 설정한다.

가. 그룹키 합의 프로토콜

그룹키의 개념을 이해하기 위하여 그룹 내의 한 멤버가 나머지 그룹 멤버들 모두에게 비밀 메시지를 전송한다고 가정하자. 이 때 그룹의 모든 멤버들이 하나의 그룹키를 공유하게 되면, 송신자는 그룹키를 사용하여 메시지를 한 번만 암호화해서 전송

해도 그룹 내의 모든 수신자들은 송신자가 암호화 시 사용한 그룹키와 같은 키를 가지고 있으므로 이를 사용하여 수신한 메시지를 안전하게 복호화할 수 있게 된다. 방송시스템과 같이 공개된 네트워크 상에서 안전하게 그룹 통신을 하기 위해서는 그룹 구성원간에 그룹키를 안전하고 효율적으로 공유할 수 있는 방법이 필요하며, 이러한 목적으로 설계되는 프로토콜을 그룹키 합의 프로토콜이라고 한다. 제안하는 그룹키 합의 프로토콜에서 파라미터의 정의는 다음과 같다.

- $\{U_1, U_2, \cdots, U_n\}$: 그룹 구성원의 집합
- $\{U_n\}$: 방송국
- $U_1, U_2, \cdots, U_{n-1}$: 시청자
- $p = k \cdot q + 1$(k: 정수, q: 소수) : 큰 소수
- g: 모듈러 p상에서 위수 q를 갖는 순환 부분군의 원시 원소
- K_i: 그룹 구성원 U_i의 비밀 서명키
- PK_i: 그룹 구성원 U_i의 서명 검증키
- Sig: 서명 알고리즘
- $Verify$: 검증 알고리즘
- $H()$: 일방향 해쉬 함수
- SK: 그룹 구성원 사이에 공유된 세션키

· 제안한 그룹키 설정 프로토콜의 동작과정

공개 파라미터 p, g가 모든 프로토콜 참가자에게 알려져 있다고 가정한다. 그룹 구성원의 집합 U는 클라이언트$\{U_i | i = 1, 2, \cdots, n-1\}$와 서버 $\{U_n\}$의 합집합이고, 제안한 프로토콜의 자세한 실행 과정은 다음과 같다.

① 1 라운드에서, 각각의 시청자 $U_i \neq U_n$는 임의의 $r_i \in_R Z_q$를 뽑아, $z_i = g^{r_i}$을 계산한 다음 각각의 비밀 키 K_i로 서명하여 $s_i Sig_{K_i}(Z_i)$를 얻는다. 그런 다음, 서버 U_n에게 메시지 $m_i = (Z_i, S_i)$를 전송한다. 또한 서버는 임의의 $r, r_n \in_R Z_q$을 뽑아 $z = g^r$, $x_n = z^{r_n} (= g^{r r_n})$을 계산한다.

② 2 라운드에서, 방송국 U_n은 z_i의 서명 s_i를 검증한 다음, 서명 값이 모두 옳다면 $x_i = z_i^r$을 계산한다. 그런 다음, 일회용(nonce)의 l비트, $\delta \in \{0,1\}^l$ (여기서, l은 안전성 파라미터)를 뽑아 $X = \oplus_{i=1}^{n} H(\delta \| x_i)$를 계산한다. X_i의 집합을 $Y = \{X_i | 1 \leq i \leq n-1\}$로 놓고, 비밀 키 K_n으로 $(\delta \| z \| Y)$를 서명하여 $s_n = Sig(\delta \| z \| Y)$를 얻는다. 이때, $X_i = X \oplus H(\delta \| x_i)$이다. 이제 메시지 $m_n(\delta, z, Y, S_n)$을 전체 그룹 구성원에게 브로드캐스트 한다.

③ 공통키를 계산하는 단계로, 방송국 U_n으로부터 브로드캐스트 메시지를 받은 후, 각각의 시청자 $U_i \neq U_n$는 서명 s_n을 검증한 다음, U_i는 다음과 같이 $X_i = X \oplus H(\delta \| x_i), x_i = z^{r_i}$를 복구할 수 있다. 이제 서버 U_n을 포함한 모든 시청자는 공통의 세션키 $SK = H(X, Y)$를 계산할 수 있다. 여기서 H는 일방향 해쉬함수이다.

제안하는 프로토콜은 $n-1$번의 유니캐스트와 한 번의 브로드캐스트 통신을 필요로 하고, 2라운드 만에 암호 통신에 사용할 세션키를 나눠 갖게 된다. 따라서, 본 프로토콜은 하나의 방송국과 다수의 시청자들로 구성된 유료방송시스템에서 효율적으로 세션키를 공유할 수 있다.

[방송국에서의 초기방송]

(2) 방송국은 키 설정과정을 통해 생성한 그룹키를 이용하여 시청자들에게 전송할 방송내용을 암호화한 후 브로드캐스팅 한다. 이때, 방송국은 방송내용을 각각의 송신자들에게 전송하기 위하여 각각 암호화 과정을 수행하지 않아도 되며, 방송내용을 한번만 암호화하여 송신자들에게 전송하기 때문에, 암호화의 수행에 따른 효율성 측면에서 기존의 방식들에 비해 장점을 가지고 있다.

[초기방송 시청 및 녹화과정]

(3) 수신료를 지불한 정당한 시청자들은 방송국으로부터 유료방송 시청을 위한 스마트카드를 발급받았으며, 이 스마트카드 내에 공통의 그룹키가 저장되어 있다. 그러므로 방송을 시청하려는 시청자는 방송국으로부터 수신한 암호화된 방송내용을 복호화하여 초기 방송을 시청할 수 있다.

(4) 각 시청자들의 스마트카드내에 저장되어 있는 그룹키는 방송국의 공개키를 이용하여 암호화된다.

(5) 각 시청자들은 전송 받은 암호화된 방송내용을 저장하고 (4)번 과정에서 암호화된 그룹키를 스마트카드에 저장한다.

[녹화방송 사용허가 요청]

(6) 시청자가 저장해둔 방송내용을 다시 시청하기 위해서는, 사용자의 스마트카드에 저장되어 있는 방송국의 공개키를 이용하게 된다. 이 경우, 스마트카드는 시청자의 스마트카드에 저장되어 있는 방송국의 공개키로 암호화되어 있는 그룹키를 방송국에 전송하게 된다. 이 과정은, 저장해둔 방송내용을 다시 시청하기 위해 방송국에 허가를 요청하는 과정이라 할 수 있다.

(7) 방송국은 시청자로부터 전송받은 암호화된 자신의 그룹키를 방송국의 개인키를 이용하여 복호화 과정을 수행한다. 복호화 과정을 수행한 후 전송받은 그룹키의 값을 검증하게 된다.

(8) 전송받은 그룹키의 검증이 이상없이 이루어지면, 다시 시청을 원하는 시청자의 공개키로 다시 암호화 한 뒤 전송해 준다. 이 과정은, 방송국이 방송의 재 시청을 원하는 시청자에게 저장된 방송내용의 시청 권한을 부여하는 과정이다.

[녹화방송 시청 단계]

(9) 방송국은 정당하게 시청료를 지불한 시청자들과 본 논문에서 제안하고 있는 효율적이고 안전한 그룹키 설정 프로토콜을 이용하여 공통의 세션키를 설정한다.

(10) 녹화방송을 다시 시청하고자 하는 시청자는 방송국과의 통신을 통해 획득한 그룹키를 사용하여 암호화된 방송내용을 복호화하고 이 방송내용을 다시 시청할 수 있게 된다.

■ 시청자 : $D_{K_{group}}(E_{K_{group}}(C)) = C$

제안하는 키 관리 모델은, 방송국에서의 초기방송은 유료시청자만이 시청할 수 있으며, 시청자가 방송을 녹화한 후 녹화된 방송의 시청을 원할 경우, 재 시청에 관한 요금을 지불하는 모델로서 perfect forward secrecy와 known key security를 만족하며, memory dump attack에 안전한 모델이라 할 수 있다. 또한, 방송데이터를 그룹키 방식에 기반하여 암호화를 수행함으로써 암호 알고리즘에 사용되는 암·복호화 키의 사용을 최소화 하여, 효율적인 키 관리가 이루어질 수 있다는 장점이 있다.

또한, 제안하는 키 관리 모델에서는 암호화와 복호화 키를 송신자와 수신자간에 수행하는 키 분배 방식이 아닌 그룹키 설정 방식을 이용함으로써 시청자의 증가에 따른 키 분배 문제를 해결할 수 있으며, 시청자의 증가와 상관없이 방송국과 시청자들 사이에서 안전하고 효율적으로 암호화와 복호화 키가 분배될 수 있는 모델이라 할 수 있다.

V. 결 론

본 논문에서는 지금까지 제안된 디지털 방송 시스템들에 대한 분석을 통해 안전성과 효율성에 대한 비교 분석을 수행하였다. 본 논문에서는 각 방식들의 효율성 비교를 위해 방송국의 암호화와 방송데이터 사이즈, 그리고 암호화 키 수에 대한 비교·분석을 수행하였으며, 그 결과 공개키 암호방식과 D-H를 이용한 방식의 경우 모두 n번의 계산량을 필요로 하지만 세션키를 이용하는 방식의 경우 방송국의 암호화와 데이터 사이즈, 그리고 암호화 키 수가 모두 1번이므로, 다른 방식들에 비해 효율적임을 알 수 있다. 각 방식들의 안전성 측면에서는 공개키 암호 방식을 이용하는 경우 PFS와 MDA에 안전하지 못하며, 세션키 방식을 이용하는 경우 KKS에는 안전하나 PFS와 MDA에는 안전하지 못함을 알 수 있었다.

지금까지의 디지털 방송 시스템은 일반적으로 PKI(Public Key Infrastructure)기반을 이용하거나, 브로드캐스트 암호화 기법을 이용하여 구축하였으나, 두 시스템 모두 perfect forward secrecy를 제공하지 못하는 큰 단점을 가지고 있음이 밝혀졌다. 따라서, 본 논문에서는 안전하고 효율적인 유료방송시스템 키 관리를 설계하기 위하여 perfect forward secrecy를 제공하는 그룹키 합의 프로토콜을 제안하였으며, 이를 이용하여 안전하고 효율적인 유료방송 시스템 키 관리 모델을 제안하였다. 본 논문에서 제안하는 키 관리 모델은, 향후 디지털 유료 방송시스템에서의 안정성과 효율성을 위해 효과적으로 사용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Arvind Narayanan, C. Paudu Pangan, Kwangjo Kim: Practical Pay-TVSchemes. ACISP 2003, LNCS 2727, pp.192-203, 2003.

[2] A.K Lenstra and E.R. Verheul: Selecting Cryptographic Keys, Journal of Cryptology, 1999.

[3] T.Matthews, Suggestions for Random Number Generation in Software RSA Laboratories'

Bulletin no.1, 1996.

[4] M. Burmester and Y. Desmedt: A secure and efficient conference key distribution system. Eurocrypt'94, LNCS 950, pp.275-286, 1994.

[5] C. Blundo and A. Cresti: Space requirements for broadcast encryption. In Advances in Cryptology, Eurocrypt' 94 LNCS 950, pp.287- 298, 1994.

[6] D.A. Agarwal, O. Chevassut, M.R. Thompson, and G. Tsudik: An Integrated Solution for Secure Group Communication in Wide-Area Networks. In Proc. of 6th IEEE Symposium on Computers and Communications, pp.22-28, 2001.

[7] Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik: On the Performance of Group Key Agreement Protocols. In Proc. of 22nd IEEE International Conference on Distributed Computing Systems, pp.463-464, 2002.

[8] G. Ateniese, M. Steiner, and G. Tsudik: New multiparty authentication services and key agreement protocols. IEEE Journal on Selected Areas in Communications, vol.18, no.4, pp.628-639, April 2000.

[9] K. Becker, and U. Wille: Communication complexity of group key distribution. In Proc. of 5th ACM Conf. on Computer and Communications Security, pp.1-6, 1998.

[10] M. Bellare, D. Pointcheval, and P. Rogaway: Authenticated key exchange secure against dictionary attacks, Eurocrypt'00, LNCS1807, pp.139-155, 2000.

[11] M. Bellare and P. Rogaway: Entity authentication and key distribution. Advances in Cryptology, Crypto'93, LNCS 773, pp.232-249, 1993.

[12] M. Bellare and P. Rogaway: Random oracles are practical: A paradigm for designing efficient protocols. In Proc. of 1st ACM Conf. on Computer and Communications Security (CCS'93), pp.62-73, 1993.

[13] M. Bellare and P. Rogaway: Provably secure session key distribution the three party case. In Proc. of 27th ACM Symposium on the Theory of Computing (STOC), pp.57-66, 1995.

[14] E. Biham, D. Boneh, and O. Reingold: Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring. Information Processing Letters (IPL), vol.70, no.2, pp.83-87, 1999.

[15] C. Boyd and J.M.G. Nieto: Round-optimal contributory conference key agreement. PKC 2003, LNCS 2567, pp.161-174, 2003.

[16] E. Bresson and D. Catalano: Constant round authenticated group key agreement via distributed computation. Proc. 7th International Workshop on Practice and Theory in Public Key Cryptography (PKC'04), LNCS 2947, pp.115-129, 2004.

[17] E. Bresson, O. Chevassut, and D. Pointcheval: Provably authenticated group DiffieHellman key exchange the dynamic case. Asiacrypt'01, LNCS 2248, pp.290-309, 2001.

[18] E. Bresson, O. Chevassut, and D. Pointcheval: Dynamic group Diffie-Hellman key exchange under standard assumptions. Eurocrypt'02, LNCS 2332, pp.321-336, 2002.

[19] E. Bresson, O. Chevassut, and D. Pointcheval: Group Diffie-Hellman key exchange secure against dictionary attacks. Asiacrypt'02, LNCS 2501, pp.497-514, 2002.

[20] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater: Provably authenticated group Diffie-Hellman key exchange. In Proc. of 8th ACM Conf. on Computer and Communications Security, pp.255-264, 2001.

[21] O. Pereira and J.-J. Quisquater: A security analysis of the Cliques protocols suites. Proc. 14th IEEE Computer Security Foundations Workshop, pp.73-81, June 2001.

[22] M. Steiner, G. Tsudik, and M. Waidner: Diffie-Hellman key distribution extended to group communication. Proc. of 3rd ACM Conf. on Computer and Communications Security (CCS'96), pp.31-37, 1996.

양 형 규(Hyung-kyu Yang) 정회원

한국 통신학회 논문지 2005년 1월호 참조

현재 강남대학교 컴퓨터미디어공학부 부교수