N-스크린 서비스가 제공되는 환경에서 효율적인 멀티 디바이스 지원을 위한 키 관리 기법*

김정훈[1], 이훈정[1], 김상진[2], 오희국[1†]
[1]한양대학교 컴퓨터공학과
[2]한국기술교육대학교 컴퓨터공학과
e-mail:jhkim@infosec.hanyang.ac.kr

The Scheme for Efficient Key Management for N-Screen Service in Multi Device Environment

Junghoon Kim[1†], Hoonjung Lee[1], Sangjin Kim[2], Heekuck Oh[1]
[1]Dept. of Computer Science and Engineering, Hanyang University
[2]Dept. of Computer Science and Engineering, Korea University of Technology and Education

요 약

단방향 서비스만을 제공하였던 기존의 케이블과 위성 방송은 인터넷을 활용하여 양방향 서비스를 제공하게 되었고, 이로 인해 사용자는 방송 시간에 구애받지 않고 원하는 콘텐츠를 시청할 수 있게 되었다. 현재는 더 나아가 사용자가 원하는 디바이스에서 자유롭게 콘텐츠를 이용할 수 있는 N-스크린 서비스를 제공하기 위한 노력을 기울이고 있다. 기존 방송 시스템에서 유료 콘텐츠를 보호하기 위해 사용한 접근제어 시스템에서는 암호키의 갱신 시간 때문에 사용자 소유가 아닌 디바이스에 일시적인 시청권한을 부여하는 N-스크린 서비스를 제공할 수 없지만 기존 환경에서 키 계층을 늘리는 방법을 통해 이러한 문제를 해결할 수 있다. 하지만 N-스크린 서비스가 제공되는 것은 사용자가 댁내의 TV 뿐만 아니라 다양한 모바일 디바이스를 사용하는 멀티 디바이스 환경을 요구하게 된다. 기존의 접근제어 시스템에서 여러 디바이스를 지원하려면 디바이스의 수 만큼 암호키를 분배하기 위한 메시지를 생성해야 되며, 이로 인해 메시지를 생성하기 위한 시간과 통신 대역폭에 오버헤드가 발생한다. 본 논문에서는 N-스크린 서비스를 제공하기 위해 키 계층을 늘린 접근제어 시스템에서 멀티 디바이스를 효율적으로 지원하기 위한 키 관리 기법을 제안한다.

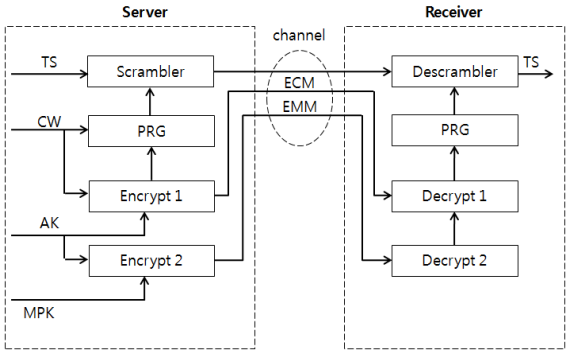
1. 서론

단방향 서비스만을 제공하였던 기존의 케이블과 위성 방송은 인터넷을 활용하여 양방향 서비스를 제공하게 되었고, 이로 인해 사용자는 시간에 구애받지 않고 원하는 콘텐츠를 시청할 수 있는 VoD와 같은 서비스를 제공 받을 수 있게 되었다. 현재는 더 나아가 사용자가 한정된 디바이스에서만 콘텐츠를 이용하지 않고 원하는 디바이스에서 자유롭게 콘텐츠를 이용할 수 있는 N-스크린 서비스를 제공하려 하고 있다[1][2]. N-스크린 서비스는 상황에 따라 사용자가 소유하지 않은 디바이스에서 유료 콘텐츠를 이용할 수 있는 상황이 발생할 수 있기 때문에 일시적인 시청권한의 위임이 필요하다. 그러나 기존 방송 시스템에서 유료 콘텐츠를 보호하기 위해 사용하는 접근제어 시스템(Conditional Access System, CAS)에서는 암호키의 갱신 시간 때문에 일시적으로 시청권한을 위임하기 어렵다. 하지만 키 갱신 시간을 유연하게 적용하기 위해 키 계층을 늘리면 일시적으로 시청권한을 위임할 수 있게 된다[3].

이때, N-스크린 서비스가 제공된다는 것은 사용자가 여러 디바이스를 사용하고 있는 멀티 디바이스 환경이라는 것을 뜻한다. 현재 방송 시스템에서 사용하는 CAS에서는 한명의 사용자가 여러 디바이스를 사용하는 경우와 여러 사람이 각각의 디바이스를 사용하는 것을 구별해서 다루지 않고 있으며, 서비스를 제공하기 위해 각각의 디바이스로 암호키를 분배하기 위한 메시지를 생성 및 브로드캐스팅 해야 한다. 이로 인해 메시지를 생성하기 위한 시간과 통신 대역폭에 오버헤드가 발생하며, 이는 서버에 큰 부담을 주게 된다. 따라서 각각의 디바이스를 중심으로 이루어지는 키 분배보다 해당 기기를 소유한 사용자를 중심으로 키 분배가 이루어지도록 콘텐츠 보호기법을 설계해야 하며, 안전성 또한 검증해야 한다.

본 논문에서는 N-스크린 서비스가 제공되는 환경에서 Secret Sharing을 활용하여 효율적으로 멀티 디바이스를 지원하는 키 관리 기법을 제안한다.

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1111 - 0010).
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2011-0000189).
† 교신저자, hkoh@hanyang.ac.kr



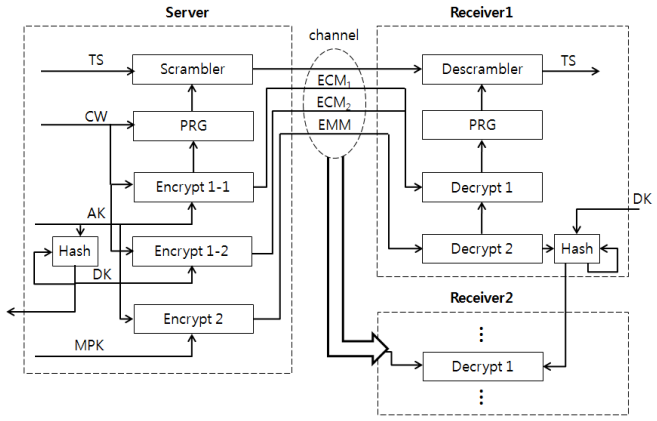
(그림 1) CAS의 구조

2. 관련연구

2.1 Conditional Access System(CAS)

CAS는 유료 방송에서 서비스 제공자들이 요금을 지불한 정당한 가입자에 대해서만 콘텐츠를 시청할 수 있도록 하기위해 사용하는 접근제어 기술이다[3][4][5]. CAS는 콘텐츠를 CSA(Common Scrambling Algorithms)에 의해 스크램블링하여 방송하고, 스크램블링에 사용된 키(Control Word, CW) 를 계층적으로 관리하여 권한이 있는 사용자만이 디스크램블링하여 정상적으로 방송을 시청할 수 있도록 한다. (그림 1)은 CAS의 구조를 나타낸다.

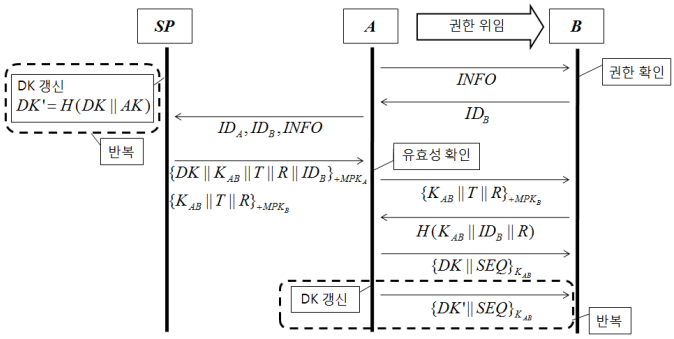
CAS는 스마트카드를 사용하여 키를 관리한다. 사업자는 CW(Control Word)를 대칭키 기반의 AK(Authorization Key)로 암호화하여 ECM(Entitlement Control Message)의 형태로 전송하고, AK는 공개키 기반의 MPK(Master Private Key)로 암호화되어 EMM(Entitlement Management Message)의 형태로 전송된다. 이때, 스크램블링은 안전성이 높지 않기 때문에 CW를 10초 정도의 짧은 주기 갱신하게 되며 그때마다 갱신된 CW를 전송하기 위해 ECM도 같이 변경되며, ECM은 특정 사용자를 위한 메시지가 아니므로 큰 부담이 되지 않는다. AK는 사용자가 탈퇴하는 경우 갱신되어야 하지만 갱신된 AK를 전달하기 위한 EMM은 각각의 사용자마다 모두 다르므로 메시지를 다시 생성하는데 큰 부담이 된다. 따라서 AK는 하루정도의 주기를 갖고 갱신되어 사용자의 탈퇴는 일괄적으로 처리된다.



(그림 2) 제안하는 기법의 구조

2.2 일시적 권한 위임

유료 콘텐츠에 대한 N-스크린 서비스를 지원하기 위해서는 일시적인 시청권한의 위임이 필요하다. 이때, 기존의 방송시스템에서는 권한이 있는 디바이스에서 권한이 없는 디바이스로 키를 전송해 줘야 하지만 CW를 전송할 경우 짧은 갱신주기로 인해 디바이스에 부담이 되고, AK를 전송할 경우 권한이 지속되는 시간이 너무 길어 사업자의 수익모델에 문제가 된다. 이러한 문제를 해결하기 위해서는 적당한 갱신 주기를 갖는 위임 키(Delegation Key, DK)를 추가적으로 운영함으로써 해결할 수 있다[]. (그림 #)는 우리가 제안했던 일시적 시청권한 위임 기법을 나타낸다. 우리가 제안했던 일시적 권한 위임 기법에서는 DK를 EMM처럼 전송하지 않고 권한 위임이 필요한 시점에 서버로부터 안전하게 전송받고, AK와 해쉬를 통해 자체 갱신하여 연산량과 대역폭에 부담을 줄이고 있다. (그림 3)은 일시적 권한위임이 이루어지는 프로토콜을 나타낸다.



(그림 3) 일시적 시청권한 위임 기법

2.3 Secret Sharing

Secret Sharing은 비밀정보를 여러 명의 사용자에게 분배한 뒤 일정 인원이 모이면 비밀 값을 복원할 수 있게 하는 기법이다[6]. Shamir가 제안한 Secret Sharing은 유한체 상의 t차 다항식 $f(x)$를 생성하여 $f(0)$을 비밀 값으로 사용하는 기법이다. $f(x)=y$일 때, 서로 다른 x,y를 사용자에게 분배 한 뒤 $t+1$명이 모이면 라그랑제 보간법을 이용해 $f(x)$를 구할 수 있게 되고, 따라서 비밀 값인 $f(0)$도 계산할 수 있게 된다.

$$f(x) = \sum_{k=1}^{t} y_k l_k(x)$$

$$l_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{x - x_i}{x_k - x_i}$$

3. 제안하는 기법

기존 유료 방송은 가정에 있는 TV에서 방송을 시청하는 환경 대상으로 하고 있으며, 실질적으로 한 가정을 대상으로 서비스되고 있다. 하지만 N-스크린 서비스가 제공되는 환경에서는 모바일 디바이스를 포함하여 한명의 사용자가 여러 디바이스를 사용하게 된다. 따라서 기존 환경보다 많은 디바이스를 서비스해야 되며, 디바이스가 증가되는 것에 비례하여 추가적으로 EMM을 생성해야 하는 오버헤드와 이를 전송해야 하는 오버헤드가 발생한다. 이러한 문제를 해결하기 위해서는 각각의 디바이스별로 EMM을 구성하지 않고 한명의 사용자를 위한 EMM을 만들어 여러 디바이스에서 사용할 수 있도록 해야 한다. 이때, Secret Sharing을 사용하면 사용자 단위로 EMM을 생성하지만 스마트카드에는 서로 다른 비밀 값이 저장되도록 할 수 있다. 본 논문에서는 Shamir가 제안한 기법을 사용하며 N-스크린 서비스가 제공되는 환경에서 효율적으로 멀티 디바이스를 지원하는 기법을 제안한다.

3.1 환경 정의

제안하는 기법은 우리가 제안했던 N-스크린 서비스를 지원하는 환경을 바탕으로 하고 있다. 따라서 모바일 디바이스를 포함한 모든 기기들은 같은 서비스 제공자의 서비스를 받고 있으며 각각의 디바이스들은 방송스트림을 수신할 수 있는 환경이라고 가정한다. 또한 키와 관련된 모든 연산은 스마트카드 내부에서 이루어지며, 계산된 내용이나 처음부터 저장된 비밀 값은 외부로 노출되지 않는다고 가정한다. 그리고 모든 디바이스는 근거리 통신 기능을 갖추고 있으며 인터넷을 통해 서비스 제공자와 양방향 통신을 사용할 수 있다고 가정한다.

3.2 초기화 단계

사용자가 최초 서비스에 가입하면 사용자는 자신의 공개키 $+MPK_u$를 서버에 전송하고 서버에서는 사용자를 위한 다항식 $f(x)=ax+b \bmod p$ 를 생성한 뒤 사용자의 디바이스에서 사용할 스마트카드에 비밀 값 $x_i, f(x_i)$를 분배한다. 또한, 서버에서는 발급한 스마트카드에서 다항식을 계산하기 위해 사용할 비밀 값 $x_s, f(x_s)$를 생성한 뒤 저장한다. 사용자는 발급한 스마트카드에 사용자 자신의 개인키 $-MPK_u$ 를 입력한다. 이때 서버에 저장하는 비밀 값과 스마트카드에 분배하는 비밀 값은 서로 같은 값이 되지 말아야 한다.

3.3 EMM 생성과 콘텐츠 재생

기존의 EMM은 사용자에게 발급된 스마트카드의 공개키로 AK를 암호화한 것이다. 그러나 멀티 디바이스 환경에서 기존의 방법을 그대로 사용하게 되면 EMM의 수가 늘어나 메시지를 생성하기 위한 연산 시간과 전달하기 위해 사용하는 통신 대역폭이 늘어난다. 제안하는 기법에서는 Secret Sharing을 사용하여 이 문제를 해결하기 위해 EMM을 다음과 같이 구성한다.

$$EMM = \left\{ x_s \| f(x_s) \| x_{AK} \| \{AK\}_{f(x_{AK})} \right\}_{+MPK_u}$$

제안하는 기법에서 EMM은 AK를 $f(x_{AK})$로 암호화한 뒤 서버에 저장된 비밀 값과 x_{AK}와 함께 다시 사용자의 공개키로 암호화한 형태이다. 이때, x_s와 x_{AK}가 서로 같은 경우 AK를 암호화하는데 사용한 키 값이 노출되므로 반드시 서로 다른 값을 사용해야 한다. 사용자의 디바이스에 장착된 스마트카드는 먼저 사용자의 개인키로 복호화 한 뒤, $x_s, f(x_s)$를 통해 다항식을 구하고, 그 다항식을 이용하여 $f(x_{AK})$를 구하게 된다. 따라서 AK역시 구하게 되므로 사용자는 ECM을 복호화 하여 CW를 얻고 콘텐츠를 재생할 수 있게 된다.

3.4 시청권한의 위임

기존에 우리가 제안했던 일시적 시청권한 위임 기법에서는 사용자가 발급한 스마트카드와 개인키를 바탕으로 하고 있었다. 하지만 제안하는 기법은 사용자의 개인키를 사용하고 있기 때문에 DK를 얻기 위한 프로토콜상의 메시지에서 악의적인 사용자에 의해 키가 노출될 수 있다. 따라서 프로토콜상의 메시지를 수정해야 하며, 제안하는 기법에서 EMM을 구성한 것과 같은 방법으로 다항식을 통해 계산된 값을 키로 사용하여 DK를 암호화 하는 과정을 추가한다. 이때, 스마트카드에서 DK를 요청하는 시점에는 이미 다항식을 계산한 시점이기 때문에 서버에 저장된 비밀 값은 전달하지 않는다. 프로토콜의 수행을 통해 DK를 얻은 디바이스에서는 기존과 동일한 방법으로 AK와 해쉬 연산을 통해 자체 갱신 하며 필요한 기간만큼 시청권한을 위임한다.

4. 분석

4.1 안전성 분석

제안하는 기법은 사용자의 개인키를 사용하여 메시지를 암호화 하고 있다. 따라서 악의적인 사용자에 의해 메시지의 내용이 노출될 수 있다. 하지만 서버에 저장된 비밀 값은 노출된다 하더라도 스마트카드에 저장된 다른 비밀 값이 없다면 보간법을 통해 다항식을 구할 수 없기 때문에 안전하다고 할 수 있다. 그리고 사용자마다 다항식이 다르기 때문에 노출된 다른 사용자의 비밀 값으로는 특정 사용자의 다항식을 구할 수 없다. 또한 스마트카드는 내부에 저장된 값에 사용자가 접근할 수 없다는 특징 때문에 비밀 값이 노출되지 않으므로 제안하는 기법은 안전하다고 할 수 있다.

4.2 효율성 분석

제안하는 기법에서는 멀티 디바이스 환경을 고려하여 EMM의 수를 줄여 연산시간 및 전송을 위한 대역폭을 효율적으로 사용하고 있다. 그러나 EMM을 구성하는 과정에서 기존의 보간법과 대칭키 연산을 더 요구하게 되었다. 대칭키 연산의 경우 일반적으로 공개키 연산보다 가벼운 것으로 알려져 있으며, 보간법 역시 실제 구현해서 테스트 해본 결과 시스템에 영향을 줄 만큼 크지 않아 스마트폰과 같은 모바일 디바이스에서 무리 없이 사용할 수 있는 수준이었다. (표 1)은 Intel Core i5 2.67GHz, 3GB 메인 메모리 환경과, 안드로이드 2.3 버전의 운영체제를 사용하는 삼성의 갤럭시S에서 비밀 값을 복원하는데 소요된 연산시간을 측정한 것이다. 따라서 각각의 디바이스를 위한 EMM을 생성하는 것보다 제안하는 기법이 연산량 측면에서 효율적이라고 할 수 있다. 대역폭 측면에서는 메시지의 길이가 한 블록을 초과하지 않으므로 전체적인 메시지의 크기에 변화가 없으며, EMM의 양이 줄어 기존 방법을 사용하는 것과 비교하여 제안하는 기법이 효율적이라고 할 수 있다.

(표 1) 비밀 값 복원 연산에 소요된 시간

비밀 값의 크기	PC(msec)	스마트폰(msec)
64bit	0.4	1.3
128bit	0.7	1.5
256bit	1.7	2.8
512bit	2.6	4.3
1024bit	5.1	9.6

5. 결론 및 향후과제

본 논문에서는 우리가 제안했던 일시적 시청권한 위임이 가능한 N-스크린 환경에서 멀티 디바이스를 효율적으로 지원하기 위한 키 관리 기법을 제안하였다. 제안하는 기법을 통해 기존 환경에서는 디바이스가 추가될수록 연산량과 통신량이 증가하는 오버헤드가 발생하였지만 제안하는 기법을 통해 사용자의 디바이스가 추가되더라도 추가적인 연산량과 통신량을 요구하지 않는 효율적인 환경을 제공하였으며, 스마트카드에 저장된 비밀 값은 절대 노출되지 않으므로 악의적인 사용자에 의해 키가 노출되지 않는다. 그러나 제안하는 기법은 전체적인 그림을 제시하고 있으며 세부 내용에 대해서는 아직 자세한 내용을 제시하지 않고 있기 때문에 지속적인 연구를 통해 좀 더 좋은 결과를 도출해 내야 하겠다.

참고문헌

[1] 김윤화, “3 스크린 플레이(3 Screen Play) 서비스 추진 현황,” 방송통신정책, Vol.21, No.11, pp.79-82, 2009

[2] 김윤화, “N 스크린 전략 및 추진 동향 분석,” 방송통신정책, Vol.22, No.20, pp.1-23, 2010

[3] 김정훈, 이훈정, 김상진, 오희국, “유료 콘텐츠의 N-스크린 서비스를 위한 일시적 시청권한 위임 기법,” 정보처리학회논문지 C, Vol.18, No.3, pp.135-142, 2011

[4] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review, Dec, 1995

[5] Herve Benoit, "Digital Television," Focal Press, 2002

[6] Adi Shamir, "How to Share a Secret," Communications of the ACM, vol.22, no.11, pp.612-613, 1979