DOI: 10.3745/KIPSTC.2011.18C.3.135

유료 콘텐츠의 N-스크린 서비스를 위한 일시적 시청권한 위임 기법

김 정 훈[†] · 이 훈 정[††] · 김 상 진[†††] · 오 희 국[††††]

요 약

최근, 통신기술의 급속한 발전으로 인해 때와 장소에 구애받지 않고 콘텐츠를 소비하고자 하는 사용자의 욕구와 새로운 비즈니스 모델을 찾고자 하는 사업자의 바람이 맞물려 N-스크린 서비스 전략이 주목 받고 있다. N-스크린은 TV, 컴퓨터, 휴대용 단말 등 다양한 기기에서 끊김 없이 콘텐츠를 공유, 소비할 수 있도록 지원하는 스크린 확장 개념의 서비스로서 미국의 통신회사인 AT&T에서 처음 제안했던 3-스크린 서비스 전략이 발전된 형태이다. 유료 콘텐츠에 대한 N-스크린 서비스에서 유료 콘텐츠에 대한 끊김없는 스크린 전환을 지원하기 위해서는 스크린을 전환하고자 하는 기기로 일시적인 시청권한을 부여해야 한다. 하지만 접근제어 시스템을 사용하고 있는 현재의 방송환경에서는 일시적으로 권한을 부여하는 것이 불가능하다. 본 논문에서는 현재 방송환경에서 유료콘텐츠에 사용하고 있는 접근제어 기법에 대해 살펴보고 일시적인 권한 부여를 할 수 없는 이유에 대해서 살펴본 뒤 현재 사용 중인 접근제어 기법을 기반으로 추가적인 키를 사용해 시청권한 문제를 해결하는 방법을 제안한다.

키워드 : N-스크린, 접근제어시스템, 권한 위임, IPTV

The Scheme for Delegation of Temporary Right to Watching Pay-TV in N-Screen Service

Junghoon Kim[†] · Hoonjung Lee[††] · Sangjin Kim[†††] · Heekuck Oh[††††]

ABSTRACT

Recently, the strategy for N-screen service is in the spotlight along with the consumer's need to use contents regardless of time and place due to the rapid development of communication technology, which is meshing with the desire of service providers seeking a new business model. N-screen, as a screen-extension-concept service which enables consumers to continuously share and use contents in various equipments such as TV, computer and portable terminals, is an advanced type of 3-screen service strategy initially proposed by AT&T, an American telecommunication company. In the N-screen service for pay-contents, in order to support continuous screen changes to and from various equipments, temporary watching right should be given to the equipment intended for screen change. However, it is impossible to give the temporary watching right in the present broadcasting environment, adopting an access-control system. In this paper, the access-control technology being used for pay-contents in the present broadcasting environment and the reason for not being able to give temporary watching right, will be examined. After the examination, the solution for delegation of watching right by using an additional key on the basis of currently used access-control technology, will be proposed.

Keywords : N-Screen, Conditional Access System(CAS), Right Delegation, IPTV

1. 서 론

최근, 통신기술의 급속한 발전으로 인해 때와 장소에 구애받지 않고 콘텐츠를 소비하고자 하는 사용자의 욕구가 증대되고 있다. 이러한 사용자의 욕구와 새로운 비즈니스 모델을 찾고자 하는 사업자의 바람이 맞물려 N-스크린 서비스 전략이 주목받고 있다. N-스크린은 미국의 통신회사인 AT&T에서 처음 제안했던 서비스 전략인 3-스크린[1]이 발

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음(NIPA-2011-C1090-1111-0010).
※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No.2011-0000189).
† 준 회 원 : 한양대학교 컴퓨터공학과 석사과정
†† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정
††† 종신회원 : 한국기술교육대학교 컴퓨터공학과 부교수
†††† 종신회원 : 한양대학교 컴퓨터공학과 교수
논문접수 : 2011년 1월 28일
수 정 일 : 1차 2011년 3월 28일
심사완료 : 2011년 4월 1일

전한 형태로 TV, 컴퓨터, 휴대용 단말 등 다양한 기기에서 끊김없이 콘텐츠를 공유, 소비할 수 있도록 지원하는 스크린 확장 개념의 서비스이다[2]. N-스크린 서비스는 시청중인 콘텐츠를 사용자의 현재 상황에 맞는 스크린을 통해 콘텐츠를 이어서 볼 수 있는 기능을 제공한다. 예를 들어 집에서 TV를 통해 시청하고 있던 방송을 출근하면서 모바일 단말을 통해 이어서 시청하고, 사무실에 도착해서는 컴퓨터로 방송을 계속 보는 것을 가능하게 한다. 현재 대표적으로 AT&T의 'AT&T Video Share'[3], 애플의 '모바일미'[4], 마이크로소프트의 '라이브 메쉬'[5] 등이 서비스 되고 있다. 그러나 현재 실용화된 서비스는 유료 콘텐츠에 대한 서비스를 지원하지 않고 있으며, 콘텐츠를 다양한 기기에 전달해 주는 것이 가능할 뿐, 끊김없는 스크린 전환을 하며 콘텐츠를 소비하는 진정한 N-스크린 서비스는 제공되지 않고 있다[6][7].

N-스크린 서비스를 제공함에 있어서 유료 콘텐츠를 시청권한이 없는 다른 기기의 스크린으로 전환하고자 한다면 시청권한도 함께 넘겨줘야 하는데 현재 서비스 제공자들이 콘텐츠 보호를 위해 사용하는 접근제어 기술로는 이를 구현하는데 문제점이 있다. 본 논문에서는 이러한 시청권한 문제를 해결하기 위해 현재 사용되고 있는 접근제어 기술을 변형하여 유료 콘텐츠의 끊김없는 스크린 전환을 위한 일시적 권한 위임 기법을 제안한다.

이어지는 논문의 구성은 다음과 같다. 2장에서는 방송 시스템에서 콘텐츠 보호를 위해 사용하는 접근제어 기술과 N-스크린을 구현함에 있어 발생하는 시청권한 문제를 살펴보고 3장에서는 시청권한 문제를 해결하기 위한 미디어 서버에 의해 권한을 위임하는 중앙 집중형 방식의 접근 방법과, 단말에서 직접 권한을 위임하는 분산형 방식의 접근방법에 대해 알아본다. 4장에서는 본 논문에서 제안하는 시청권한 문제를 해결하기 위한 기법에 대해서 설명하고 5장에서는 제안하는 기법의 분석, 6장에서는 결론을 짓는다.

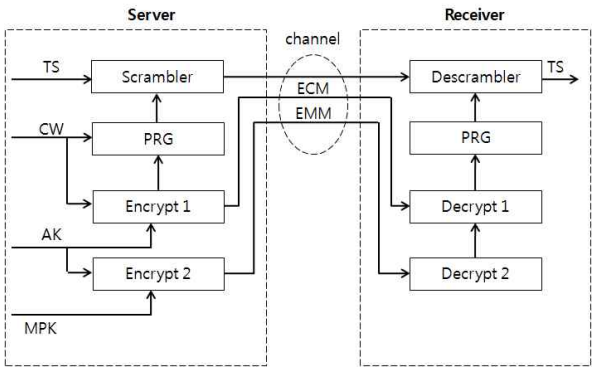
2. 연구배경

이 장에서는 유료 방송에서 콘텐츠 보호를 위해 사용하는 접근제어 기술을 살펴보고, 유료 콘텐츠의 스크린 전환을 위해 해결해야 하는 시청권한 문제에 대해 알아본다.

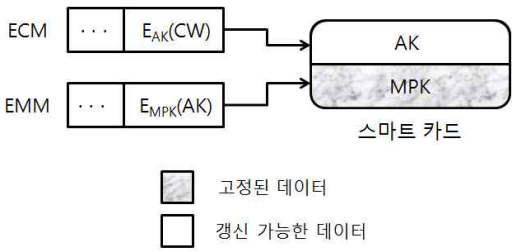
2.1 접근제어시스템(Conditional Access System, CAS)

(그림 1)은 CAS의 구조를 나타낸다. CAS는 서비스 제공자들이 요금을 지불한 정당한 가입자에 대해서만 콘텐츠를 시청할 수 있도록 하기위해 사용하는 접근제어 기술로 유료 디지털 방송에서 DRM(Digital Rights Management)과 함께 필수적으로 사용되는 기술이다. 대표적인 기능으로는 CSA (Common Scrambling Algorithms)에 의해 콘텐츠를 스크램블링/디스크램블링 하는 기능과 이때 사용하는 여러 키들을 계층적으로 관리하는 기능이 있다[8][9].

(그림 2)는 CAS 메시지와 키의 관계를 나타낸다. CAS에서 사용되는 키들을 계층적으로 관리하는 기능은 사용자의



(그림 1) CAS의 구조



(그림 2) CAS 메시지와 키의 관계

셋톱박스에 내장된 스마트카드를 바탕으로 이루어진다. 스마트카드는 서비스 제공자가 발급하는 것으로 권한이 있는 사용자라면 스마트카드에 저장된 공개키 기반의 MPK (Master Private Key)를 통해 스크램블링에 사용되는 키를 얻어낼 수 있다. 스크램블링에 사용되는 8바이트의 키는 CW(Control Word)라 하며 대칭키 기반의 AK(Authorization Key)를 통해 암호화 되어 ECM(Entitlement Control Message)의 형태로 전송된다. AK는 사용자의 스마트카드에 내장된 MPK를 통해 암호화 되어 EMM(Entitlement Management Message)의 형태로 전송된다. 따라서 권한이 있는 사용자는 스마트카드의 내장된 MPK를 통해 EMM을 복호화 하여 AK를 얻고, AK를 통해 ECM을 복호화 하여 CW를 얻을 수 있게 된다. 이때 EMM과 ECM은 콘텐츠의 비디오, 오디오 정보들과 함께 TS(Transport Stream)에 실려 사용자에게 전달된다. 이때 사용되는 키들은 모두 스마트카드 내부에서만 사용되며 외부로 노출되지 않는다. 또한 CAS에서 사용되는 키는 스마트카드를 소유하고 있는 사용자도 알 수 없다. 만약 스마트카드에 저장된 MPK가 노출되어 유포된다면 노출된 키를 통해 AK와 CW를 얻어, 정당하지 않은 방법으로 방송을 시청할 수 있게 되는 문제가 발생한다. 따라서 CAS의 안전성은 스마트카드에 의존한다고 할 수 있다.

2.2 시청권한 문제

N-스크린 서비스에서 끊김없는 스크린 전환은 현재 시청중인 콘텐츠에 대한 정보를 Zigbee[10], Bluetooth[11] 같은 근거리 무선통신 기술을 활용해 다른 기기로 전송하면, 전

송받은 정보를 토대로 이전 기기에서 시청하고 있었던 콘텐츠를 바로 재생하는 형태로 구현할 수 있다. 시청중인 콘텐츠가 무료라면 위와 같은 방법으로 간단하게 스크린 전환을 할 수 있다. 하지만 유료 콘텐츠의 경우, 스크린 전환을 하는 두 기기간의 시청권한이 다르다면 문제가 될 수 있다. 서비스 제공자가 전송하는 유료 콘텐츠는 CAS에 의해 보호되고 있으며, 기존에 콘텐츠를 시청하고 있는 기기는 시청권한이 있지만 이어서 시청할 기기에 시청권한이 없는 경우라며 CW를 얻지 못해 암호화된 콘텐츠를 복호화 할 수 없는 문제가 있다.

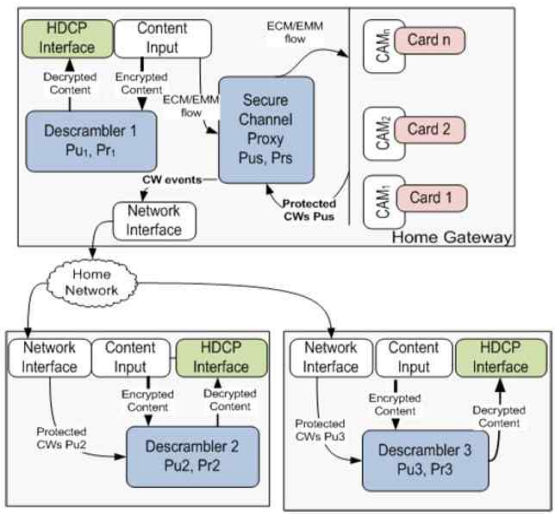
현재 시스템에서 시청권한을 부여하는 것은 서비스 제공자가 시청권한을 부여하려는 기기의 스마트카드에서 복호화 할 수 있는 EMM을 전송해줌으로써 이루어진다. EMM을 복호화 할 수 있게 되면 AK를 얻을 수 있고, CW를 얻어 스크램블된 콘텐츠를 정상적으로 시청할 수 있게 된다. 그러나 N-스크린 서비스를 위해 서비스 제공자가 시청권한을 새롭게 부여하는 것은 시청권한이 지속되는 시간이 필요 이상으로 길기 때문에 문제가 된다. 위와 같은 방법으로 시청권한이 부여된다면 AK가 갱신될 때 까지 시청권한이 지속된다. 그런데 AK를 갱신하는 것은 EMM 또한 갱신해야 되는 것을 의미하며 이는 시청권한이 지속 되어야 하는 사용자의 수만큼 공개키 암호연산을 해야 한다는 것을 의미한다. 현재 시스템에서는 연산의 부담을 줄이기 위해 AK의 갱신을 하루에 한번 하고 있어, 한번 부여한 시청권한은 쉽게 회수할 수 없다. 한번 부여된 시청권한이 장시간 지속된다면 모바일 단말이 이동하면서 여러 기기에 시청권한을 부여해 주는 오남용이 발생할 수 있으며 이는 서비스 제공자의 수익모델을 해치는 것이다. 따라서 유료콘텐츠에 대한 N-스크린 서비스를 지원하기 위해서는 일시적인 시청권한이 가능해야 한다.

3. 관련 연구

N-스크린 서비스에서 끊김없는 스크린 전환은 모바일 단말의 참여가 필수적이다. 스크린 전환은 모바일 단말에서 컴퓨터와 TV같은 고정된 단말로, 혹은 그 반대로 이루어지는데, 시청권한 문제를 해결하는 방법은 모바일 단말을 어떤 방법으로 운영하는지에 따라 중앙 집중형과 분산형으로 나눌 수 있다. 모바일 단말이 홈 미디어 서버를 통해 콘텐츠 시청을 지원 받는 형태의 환경이라면 시청권한도 홈 미디어 서버에서 부여하는 형태가 되고, 홈 미디어 서버 없이 모바일 단말에서 독자적인 시청권한으로 방송을 시청하는 환경이라면 시청권한도 모바일 단말에서 자체적으로 부여하는 형태가 된다.

3.1 중앙 집중형 N-스크린 구현

홈 미디어 서버를 통해 모바일 단말을 구현하는 환경이라면 콘텐츠의 시청권한 문제도 홈 미디어 서버를 통해 이루어진다. 홈 미디어 서버를 통해 시청권한을 부여하는 것은



(그림 3) HKMS의 구조

2002년 Heuvel 등이 제안한 기법[12]과 2006년 Pei 등이 제안한 기법[13]이 있으며 대표적으로는 2009년 Sanchez 등이 제안한 HKMS(Home Key Management System)[14]가 있다. HKMS는 CAS에서 키를 관리하는 CAM(Conditional Access Module)을 홈 미디어 서버에 배치하고 스크린과의 안전한 채널을 형성한 뒤 CW를 전송해주는 형태로 권한을 부여하고 있다. 제안된 기법은 댁내에서 활용하는 것을 목적으로 하여 모바일 단말에 대한 내용을 직접적으로 언급하진 않았지만, 홈 미디어 서버와 통신하는 채널을 무선 상에서 생성한다면 모바일 단말을 지원할 수 있다. 스크린 전환을 하려는 기기에 대해서도 모바일 단말을 지원하는 형태처럼 안전한 채널을 형성해 CW를 전송해 줌으로써 시청권한을 부여 해 줄 수 있다.

그러나 중앙 집중형 방식으로 스크린 전환을 지원하는 것은 단순한 콘텐츠 공유에 가까울 수 있다. 스크린 전환을 위한 시청권한의 부여는 콘텐츠에 대한 시청권한을 갖고 있는 사용자가 스크린을 사용하고 있는 상황에 대해서만 이루어 저야 하는데 제안된 기법을 통해서는 이를 확인 할 수 없으며, 이로 인해 권한을 갖고 있는 사용자가 스크린을 사용하고 있지 않는 상황에서도 시청권한을 계속 부여함으로써 서비스 제공자의 수익모델을 해치는 콘텐츠 공유가 될 가능성이 있다. 따라서 중앙 집중형 방식으로 N-스크린을 지원하기 위해서는 스크린이 전환되는 상황에 대해서만 제한적으로 시청권한을 부여해 주는 제약을 추가적으로 구현해야 한다.

3.2 분산형 N-스크린 구현

홈 미디어 서버 없이 독자적으로 모바일 단말이 방송을 시청하는 환경에서는 스크린전환을 위해 시청권한을 다른 기기로 부여하는 것을 모바일 단말 중심으로 해야 한다. N-스크린 서비스에서 발생하는 시청권한 문제는 아직까지 뚜렷한 연구결과가 없다. 따라서 이번 소단원에서는 일반적으로 생각할 수 있는 방법에 대해서 논한다.

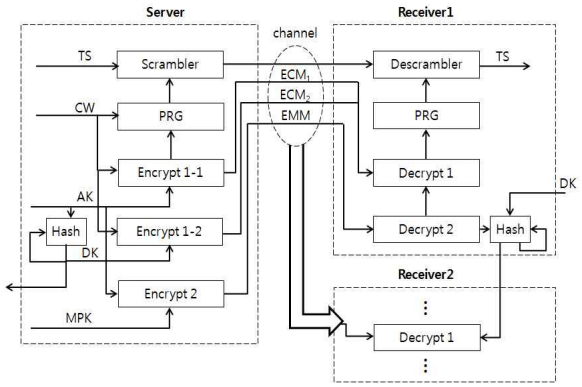
〈표 1〉 N-스크린 구현 유형별 장단점

유형	방법	장점	단점
중앙 집중형	홈 미디어 서버에서 권한 부여	스크린 전환 시 모바일 단말에서 처리하는 작업이 거의 없음	무분별한 시청권한 부여를 제약하는 추가적인 작업이 필요함
분산형	모바일 단말에서 권한 부여	무분별한 시청권한 부여가 불가능함	모바일 단말에서 발생하는 베터리 소모량이 많음

모바일 단말에서 시청권한을 부여하는 방법으로는 AK를 전송해 주는 것과 CW를 전송해 주는 방법이 있다. 먼저 AK를 전송해 주는 방법은 AK의 갱신 주기가 길어서 한번 부여한 권한이 필요 이상으로 지속되는 문제가 있으며, 일시적인 시청권한 부여를 위해 AK의 갱신주기를 짧게 하는 것 또한 현재 시스템에서는 불가능하다. AK를 갱신하는 것은 시청권한을 회수하는 것을 의미한다. AK를 갱신하면 시청권한이 지속 되어야 하는 사용자에게 AK를 전달하기 위해 EMM을 다시 생성해야 하는데, 이는 시청권한이 지속되는 사용자의 수만큼 스마트카드에 저장된 MPK로 AK를 암호화 하는 것을 의미한다. 또한 AK는 채널마다 다르기 때문에 EMM을 생성하기 위한 연산은 더욱 커진다. 이러한 연산의 부담을 최소화 하기 위해 AK의 갱신주기를 보통 24시간 정도로 길게 설정하고 있다. 따라서 모바일 단말에서 AK를 전송하는 것으로는 일시적인 시청권한 부여를 할 수 없다. 반대로 CW는 갱신주기가 너무 짧아서 문제가 된다. CW는 사업자의 설정에 의해 달라지지만 보통 10초 정도를 갱신주기로 갖는다. 따라서 모바일 단말에서는 시청권한을 위임받을 기기로 갱신된 CW를 10초마다 전송해 주어야 하는데 이것은 모바일 단말의 전원을 고려하면 매우 비효율적인 방법이다. 또한 모바일 단말의 전원 문제를 해결하기 위해 CW의 갱신주기를 길게 하는 것은 안전성에 문제가 있다. 현재 방송 시스템에서 사용하는 스크램블링 알고리즘은 실시간 방송에 대한 빠른 처리를 위해 안전성을 낮추는 대신 갱신주기를 매우 짧게 하는 방법을 사용하고 있다. 따라서 CW의 갱신주기를 길게 하는 방법은 피해야 한다. 그러나 분산형 N-스크린 구현은 모바일 단말에서 근거리 무선통신을 통해 시청권한을 부여하므로 물리적으로 일정 거리 안의 기기에 대해서만 시청권한을 부여할 수 있다는 제약이 자연스럽게 발생한다는 장점이 있다.

4. 제안하는 기법

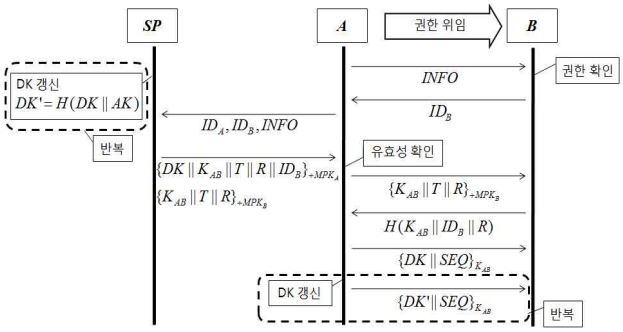
이 장에서는 CAS가 적용된 유료 콘텐츠에 대해 N-스크린 서비스를 지원하기 위한 일시적인 권한 위임 기법을 제안한다. (그림 4)는 기존의 CAS를 변형한, 제안하는 기법의 구조를 나타낸다. 제안하는 기법은 분산형 N-스크린 환경을 바탕으로 AK와 CW를 직접 전송해 주는 방법의 키 갱신 주기 문제를 해결하기 위해 기존의 AK와 같은 역할을 하는 위임 키(Delegation Key, DK)를 추가적으로 도입하였다. DK는 CW를 얻기 위해 사용하는 키 이며, 이를 위해 서비스 제공자 측에서는 DK로 암호화된 CW를 추가적으로 전송한다. 암호화된 CW는 ECM이라 할 수 있으며, 기존의 AK로 암호화된 CW와 구별하기 위해 AK로 암호화된 CW는 ECM_1, DK로 암호화된 CW는 ECM_2로 구별한다. DK를 전달하는 것은 AK가 EMM을 통해 전달하는 것과 같이 특정 메시지를 통해 전달하지 않는다. 이는 서버에서 메시지를 구성하는데 필요한 연산을 줄이고 방송에 사용하는 스트림의 대역폭을 낭비 하지 않기 위해서 이다. DK는 AK와의 해쉬 연산을 통해 갱신되며, 스크린 전환으로 인한 일시적 권한 위임이 필요할 때 별도의 통신채널을 통해 권한이 있는 기기(Receiver1)로 한번 전송한다. 권한이 있는 기기(Receiver1)에서는 AK와의 해쉬 연산을 통해 스크린 전환이 지속되는 동안 DK를 자체갱신하면서 권한이 없는 기기(Receiver2)로 DK를 전송하여 시청권한을 위임한다. 이때 기기간의 안전한 통신채널을 구성하기 위해 사용되는 세션 키 또한 서비스 제공자로부터 받게 된다.



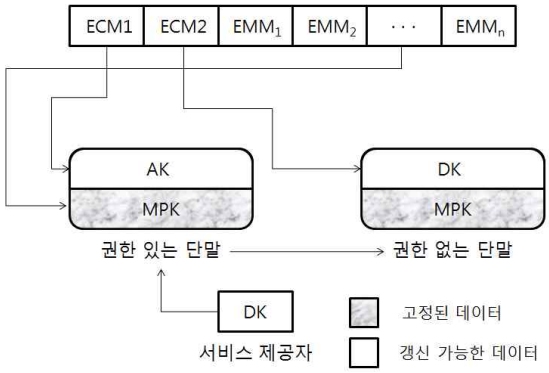
(그림 4) 제안하는 기법의 구조

4.1 환경 정의

제안하는 기법은 모바일 단말을 중심으로 수행 된다. 모바일 단말을 포함한 방송을 수신하는 모든 기기들은 같은 서비스 제공자의 서비스를 받고 있으며 각각의 기기는 방송 스트림을 수신할 수 있는 환경이 마련되어 있다고 가정한다. 기본적으로 CAS와 같이 서비스 제공자가 제공하는 스마트카드는 내부에서 일어나는 계산이 스마트카드 외부로 노출되지 않으며, 사용되는 스마트카드에 저장된 키는 사용자도 알지 못한다. 또한 참여하는 모든 기기들은 근거리 통신 기능이 갖춰져 있고, 모바일 단말은 인터넷을 통해 서비스 제공자와 양방향 통신이 가능하다고 가정한다.



(그림 5) 일시적 시청권한 위임 기법



(그림 6) 제안하는 기법의 키와 메시지의 관계

4.2 일시적 시청권한 위임 기법

(그림 5)는 제안하는 기법에서 DK를 안전하게 전송하기 위한 프로토콜을 나타낸다. 제안하는 기법의 프로토콜은 서비스 제공자로부터 DK를 받아 권한을 위임받을 기기로 이를 전송하는 일련의 과정이며 시작 단계, 세션 키 확립 단계, DK 전달 단계, 3가지의 단계로 구성되어 있다. 본 논문에서 사용하는 표기법은 <표 2>와 같다.

〈표 2〉 표기법

표기	설명
A	시청 권한이 있는 기기
B	시청 권한이 없는 기기
SP	서비스 제공자
INFO	시청중인 콘텐츠의 정보
ID_X	X의 스마트카드 ID
$+MPK_X$	X의 공개키
K_{XY}	X와 Y의 세션 키
DK	위임 키
T	SP가 메시지를 생성한 시간, 타임스탬프
R	랜덤값
SEQ	메시지 Sequence

4.2.1 시작 단계

시작 단계는 모바일 단말 *A*에서 다른 기기 *B*로 시청권한을 위임하기 위한 첫 번째 단계이다. 이 단계에서는 스크린 전환을 하면서 시청권한의 위임이 필요한지 확인하는 작업을 한다. 모바일 단말 *A*를 통해 콘텐츠를 시청하던 사용자가 다른 기기 *B*로 스크린을 전환하려고 하면 근거리 무선 통신을 이용해 현재 어떤 콘텐츠를 시청하고 있는지와 어느 부분을 시청하고 있는지에 대한 내용을 포함하고 있는 *INFO*를 *B*에게 전송한다. *B*는 *A*로부터 받은 *INFO*를 확인하여 시청권한이 있는지 여부를 확인한다. 시청권한이 있다면 프로토콜이 종료 되고 스크린 전환이 이루어지지만, 시청권한이 없으면 *A*에게 ID_B를 전송하여 프로토콜을 계속 진행한다.

4.2.2 키 확립 단계

키 확립 단계는 *DK*가 전송되는 기기간의 통신 채널을 보호하기 위해 사용할 세션 키를 *SP*에 의해 확립하는 단계이다. ID_B를 전송받은 *A*는 *SP*에게 ID_A,ID_B,*INFO*를 전송함으로써 세션 키와 *DK*를 요청한다. 사용자의 스마트카드에 저장된 MPK는 서비스 제공자가 제공하는 것이므로 별도의 인증과정을 거치지 않는다. *SP*는 *A*의 요청에 대한 응답으로 $\{DK||K_{AB}||T||R||ID_B\}+MPK_A$, $\{K_{AB}||T||R\}+MPK_B$를 *A*에게 전송한다. *A*는 먼저 $\{DK||K_{AB}||T||R||ID_B\}+MPK_A$를 복호화 하여 *DK*와 K_{AB}를 얻는다. 그리고 서비스 제공자가 메시지를 생성할 당시의 시간을 나타내는 타임스탬프 *T*와 *A*가 서비스를 요청한 시간을 비교하여 현재 세션의 유효성을 확인한다. *T*는 DK가 갱신되는 주기의 동기화를 위해 필요한 정보이기도 하다. 또한 ID_B를 확인하여 *SP*로부터 받은 세션 키가 어떤 기기와 통신하기 위한 세션 키 인지 확인한다. 다음으로 *A*는 *SP*로부터 받은 $\{K_{AB}||T||R\}+MPK_B$를 *B*에게 전송한다. B역시 A에게 자신의 ID를 전송한 시간과 *T*를 비교하여 현재 세션에 대한 메시지인지 확인하고 *A*에게 $H(K_{AB}||ID_B||R)$ 전송한다. A는 B로부터 받은 메시지와 직접 계산한 $H(K_{AB}||ID_B||R)$를 비교하여 B와 세션 키 확립이 오류 없이 되었다는 것을 확인한다.

4.2.3 DK 전달 및 콘텐츠 재생 단계

세션 키를 확립한 뒤 *A*는 *B*에게 $\{DK||SEQ\}K_{AB}$를 전송한다. *B*는 *A*로부터 받은 메시지를 복호화 하여 DK와 *SEQ*를 얻고 프로토콜과는 별개로 서비스 제공자가 전송하는 방송 스트림에서 ECM_2를 얻는다. ECM_2는 $\{CW\}_{DK}$로 구성된 메시지이므로 *DK*를 이용해 복호화 하여 *CW*를 얻을 수 있다. *CW*를 얻은 *B*는 콘텐츠를 디스크램블링할 수 있게 되어 정상적으로 방송을 시청할 수 있게 된다. 이때 *DK*는 *SP*가 정책적으로 결정한 시간마다 AK와의 해쉬 연산을 통해 자체 갱신되므로, 그 때마다 *A*는 *DK*를 $DK'=H(DK||AK)$로 갱신하고 이를 *B*에게 전송한다. 단말 *A*가 *B*에게 부여한 시청권한을 다시 회수하는 과정은 별도의 프로토콜을 통해 이루어지지 않는다. 단말 *A*가 이동을 하여 더 이상 *DK*를 전송해 주지 않는다면 *B*는 *DK*가 갱신될 때까지 시청권한이 유지되다가 갱신되고 난 후 갱신된 *DK'*을 계산할 수 없어 자연스럽게 권한이 소멸된다. *SEQ*는 *A*와 *B*사이에서 *DK*의 동기화를 확인하기 위해 사용된다. (그림 6)은 제안하는 기법의 키와 메시지의 관계를 나타낸다.

5. 분 석

이 장에서는 제안하는 기법의 안전성과 효율성에 대해 분석한다. 안전성 분석에 앞서 제안하는 기법이 만족해야 하는 보안 요구사항들에 대해 살펴본 후 이러한 요구사항을 만족하는지에 대해 휴리스틱하게 논의한다. 효율성에 대한 분석은 3장에서 제시한 분산형 N-스크린의 AK를 전송하는 방법과 CW를 전송하는 방법의 연산량과 무선통신량을 비교하여 분석한다.

5.1 보안 요구사항

제안하는 기법은 공개키 암호방식을 사용하였으며 DK를 추가적으로 사용하였다. 따라서 제안하는 기법이 만족해야 하는 보안 요구사항은 다음과 같다.

- 메시지 위조 공격: 통신에 사용되고 있는 두 당사자 사이에 오고 가는 메시지를 위조하여 공격자가 원하는 결과를 얻는 공격이다.
- 재전송 공격: 프로토콜상에서 유효 메시지를 복사한 후 나중에 재전송함으로써 정당한 사용자로 가장하는 공격이다.
- 알려진 키 안전성: 공격자가 이전 세션에 생성된 세션키를 알아냈다 하더라도 그것을 이용하여 그 이전에 생성된 세션키나 앞으로 생성될 세션키를 알아내는 것이 계산적으로 어려워야 한다.
- 전방향·후방향 안전성: 자체 갱신되는 비밀값이 노출되었다고 가정했을 때, 노출된 비밀값으로 갱신되기 이전의 비밀값을 계산해 내지 못해야 하며, 앞으로 갱신될 비밀값을 계산해 내지 못해야 한다.

5.2 안전성 분석

- 메시지 위조 공격: 제안하는 기법의 프로토콜은 시작단계에서 참여하는 기기의 스마트카드 ID를 평문으로 전송한다. 이 과정에서 공격자는 ID를 조작해서 SP에게 공격자가 프로토콜에 참여하는 것으로 속이고 DK를 얻으려고 한다. 이때 공격자는 A와 SP 사이, A와 B 사이에서 전송되는 ID 정보를 조작할 수 있다. 먼저 공격자는 A에서 SP에게 전송하는 메시지 ID_A, ID_B, $INFO$를 차단하고 ID_A, ID_M, $INFO$를 SP에게 전송한다. SP는 이에 대한 응답으로 A에게 $\{DK||K_{AM}||T||R||ID_M\}+MPK_A$, $\{K_{AM}||T||R\}+MPK_M$을 전송한다. 이때 SP로부터 받은 메시지에는 현재 어느 기기와 통신을 하려는 지에 대한 정보가 담겨 있어 사용자의 기기에서는 공격을 감지할 수 있다. 또한 A와 B사이에서 이러한 메시지를 위조하여 처음부터 공격자와 통신하는 것으로 A를 속이는 경우 프로토콜 상에서 공격을 감지할 수는 없다. 그러나 A는 시청권한을 주고 있지만 B는 이를 받지 못하고 있으므로 공격을 감지할 수 있다. 이 경우 공격자는 최초 한번 DK를 얻을 수 있지만 공격자의 ID가 서버로 전송되기 때문에 쉽게 추적할 수 있다. 또한 A와 B사이는 근거리 통신에 의한 것이므로 공격자 역시 근거리에 있어야 한다. 따라서 A와 B사이에서 ID를 위조하는 것은 현실적인 측면에서 실행할 가치가 없는 공격이라고 할 수 있다. 따라서 제안하는 기법은 위와 같은 상황에서 발생하는 메시지 위조 공격에 안전하다.
- 재전송 공격: 공격자는 A와 B사이의 세션 키를 확립하는 과정에서 사용된 메시지를 수집하여 재전송 공격을 하려 한다. 키 확립 단계에서 사용되는 메시지에는 $\{DK||K_{AB}||T|R|||ID_B\}+MPK_A$, $\{K_{AB}||T||R\}+MPK_B$, $H(K_{AB}||ID_B||R)$가 있다. 모든 메시지에는 SP에서 메시지를 생성할 당시의 시간을 나타내는 타임스탬프 T가 포함되어 있어 사용자는 실제 서비스를 요청한 시간과 T를 비교하여 현재 세션에 대한 메시지인지 확인할 수 있다. 따라서 공격자가 위의 메시지를 재전송 한다 하더라도 사용자는 이를 판별할 수 있다. 그러므로 제안하는 기법은 위와 같은 상황에서 발생하는 재전송 공격에 안전하다.
- 알려진 키 안전성: 공격자가 이전 세션에 사용했던 세션 키를 알고 있다고 가정하는 상황에서 공격자는 이젠 세션, 혹은 이후의 세션에 사용될 키를 계산하려 한다. 제안하는 기법의 세션 키는 서비스 제공자가 전송해 주는 세션 키를 그대로 사용하는 키 확립 프로토콜을 사용한다. 따라서 이전 세션에서 사용했던 세션 키와 그 이전, 이후의 세션 키와의 상관관계가 없어 이를 계산을 할 수가 없다. 따라서 제안하는 기법은 알려진 키에 안전성을 갖는다.
- 전방향·후방향 안전성: DK는 랜덤값이 아닌 연산을 통해 갱신하는 키이다. 공격자가 DK를 알고 있다고 가정했을 때 DK를 통해 갱신 이전, 이후의 DK를 계산하려 한다. DK는 AK와의 해쉬 연산을 통해 계산한다. 따라서 DK가 노출되었다고 가정했을 때, 갱신 이전의 DK를 구하는 것은 계산적으로 어렵다. 또한 AK를 알지 못하면 갱신될 DK를 계산하지 못한다. 만약 공격자가 AK도 알고 있다고 가정하면 갱신된 후의 DK를 계산할 수 있지만 AK를 알고 있다는 것은 DK를 계산해 내는 것 보다 좀 더 포괄적인 범주에서 공격에 성공한 결과라고 할 수 있어 AK를 알고있는 상황에서 DK를 계산해 내는 것은 의미가 없다고 할 수 있다. 따라서 제안하는 기법은 DK에 대한 전방향·후방향 안전성을 갖는다.

5.3 효율성 분석

제안하는 기법은 CAS를 바탕으로 추가적인 요소가 더해진 형태이며, 기존의 CAS와 호환성을 갖고 있는 장점이 있다. 연산량 측면에서 서비스 제공자측 서버에서는 사업자가 결정한 주기마다 DK의 갱신을 위한 해쉬 연산을 해야 하는 것과 CW를 DK로 암호화한 ECM_2를 만들어 내는 연산이 추가 되었다. 또한 시청권한을 위임하면서 서버와 기기, 기기와 기기간의 DK를 안전하게 전달하기 위해 발생하는 암/복호화 연산이 추가되었으며 휴대용 단말에서 DK를 갱신하기 위한 해쉬 연산이 추가되었다. 서버와 휴대용 단말에서 갱신한 DK의 동기화 문제는 현재 사용하고 있는 CAS에서

〈표 3〉 분산형 N-스크린 환경에서의 연산량 비교

구분	CW 전송		AK 전송		제안하는 기법	
	서버	모바일 단말	서버	모바일 단말	서버	모바일 단말
대칭키 암호연산	·	360번	6번	6번	360×c번	6번
공개키 암호연산	·	·	6(n×c)번	·	·	·
무선 통신 회수		360번		6번		6번

이미 해결되어 있기 때문에 고려하지 않아도 된다. 만약 동기화가 되어 있지 않다면 10초마다 갱신되는 CW를 이용해 콘텐츠를 복호화 할 수 없다. 추가된 연산중에서 가장 큰 연산은 ECM_2를 만들어 내는 것이지만, 이는 기존의 ECM을 생성하는 연산을 한 번 더 하는 것으로, 추가된 연산은 상수시간 내에 계산할 수 있어 AK를 갱신할 때 발생하는 것처럼 많은 연산을 요구하지 않아 효율적이다.

<표 3>은 CW를 지속적으로 전송하는 방법, AK의 갱신주기를 10분으로 줄이고 전송해 주는 방법, 그리고 기존 환경에서 제안하는 기법을 적용한 뒤 DK의 갱신주기를 10분으로 가정한 것을 바탕으로 1시간 동안 추가된 연산량과 통신량을 나타낸 것이다. 기기간의 통신채널을 보호하기 위한 세션 키 확립과정은 제안하는 기법의 프로토콜을 사용한다고 가정하며, 이 과정에서 시작단계, 키 확립단계에서 발생하는 통신과 연산은 3가지 경우 모두 공통적으로 발생하는 부분이므로 <표 3>에서는 생략하였다. CW를 전송할 경우 한 시간 동안 권한위임을 하기 위해서는 CW의 갱신주기를 10초라고 가정했을 때 360번의 무선 통신을 하게 되는데 전원이 제한적인 모바일 단말의 특성을 고려하면 매우 비효율적인 방법임을 알 수 있다. AK를 10분 간격으로 갱신했을 경우 서버에서는 10분마다 가입자의 수(n) × 채널의 수(c) 만큼 공개키 암호연산을 해야 하는데, 이는 방송의 가입자 수를 고려하였을 때 너무 많은 연산량을 요구하게 된다. 제안하는 기법을 사용했을 때 발생하는 가장 큰 연산량의 증가는 10초마다 CW가 갱신될 때 ECM_2 메시지를 생성하는 것이다. 그러나 서버측에서 1시간동안 360 × 채널의 수(c) 만큼의 대칭키 연산이 증가하는 것은 AK를 갱신하는 것에 비해 큰 부담이 되지 않는다. 따라서 제안하는 기법이 모바일 단말의 전원과, 서버의 연산량을 고려해 봤을 때 가장 효율적이다. 3장에서 언급한 중앙 집중형으로 구현하는 경우에도 키를 전송하는 주체만 달라지기 때문에, 권한을 주기위해 CW를 이용하거나 AK를 이용하는 것은 같은 문제이며 이로 인해 증가되는 연산의 양은 중앙 집중형으로 구현하는 것과 크게 다르지 않다.

제안하는 기법은 기존 CAS를 사용하는 방송환경에 큰 영향을 주지 않는 범위 안에서 설계되었다. 기존에 CAS와 관련된 연구에서는 EMM 메시지의 크기를 줄여 대역폭 손실을 줄이고 유연한 과금 모델을 적용하기 위해 4계층 키 구조를 사용하는 기법이 제안되었다[15][16][17]. 제안된 기법들은 4계층의 키가 수직적인 구조를 형성하고 있어 상위 계층의 키를 알아야 CW를 얻고 방송을 시청할 수 있는 구조이다. 그러나 제안하는 기법은 4개의 키를 사용하고 있지만 수직적인 계층 구조를 갖고 있지 않아 3계층 키 구조를 사용하는 현재 방송 시스템과 호환되어 사용할 수 있다. 즉, 제안하는 기법을 도입하여도 현재 사용 중인 CAS를 전부 교체하지 않고 그대로 사용할 수 있어 효율적이라고 할 수 있다.

6. 결론 및 향후 과제

본 논문에서는 CAS를 사용하는 방송환경에서 유료 콘텐츠에 대한 N-스크린 서비스를 지원하기 위한 일시적 권한 위임 기법을 제안하였다. 또한 N-스크린 서비스를 지원하기 위해 해결해야 하는 시청권한 문제를 처음으로 제시하였다. 제안하는 기법은 기존 CAS에서 N-스크린 서비스를 지원하도록 할 경우 발생하는 권한이 지속되는 문제를 해결하기 위해 DK를 추가적으로 운영하여 일시적인 권한 위임이 가능하도록 하였다. DK를 추가적으로 운영함으로써 발생할 수 있는 키의 노출이 발생하지 않도록 프로토콜을 설계하였고, 만약 DK가 노출된다 하더라도 지속적으로 갱신되므로 안전하다고 할 수 있다. 연산량 측면에서는 ECM을 계산하는 연산량이 증가하지만, 상수 배 증가하였기에 감당할 수 있는 정도이다. 제안하는 기법은 기존 CAS를 사용하는 방송환경에 큰 영향을 주지 않는 범위 안에서 설계되었다. 따라서 제안하는 기법을 실제 도입한다 해도 기존의 기기들이 서비스 받는데 어떠한 문제도 발생하지 않는다는 장점이 있다.

현재의 방송 환경은 하나의 서비스 제공자와 하나의 기기를 지원하는 일대일 환경이지만 N-스크린 서비스를 지원하는 것은 하나의 서비스 제공자가 여러 기기를 지원하는 일대다 환경을 의미한다. 향후 개방형 IPTV등과 같은 여러 서비스 제공자가 하나의 기기를 지원하는 다대일 환경과 개방형에 N-스크린 서비스가 더해져 여러 서비스 제공자가 여러 기기를 지원을 통해 다대다 환경까지 확장할 수 있도록 지속적인 연구가 필요하다.

참 고 문 헌

[1] AT&T Delivering the Digital Lifestyle- From Three Screen , http://www.att.com/Common/files/pdf/AT&T -3_ScreensFactSheet_0530.pdf

[2] 김병균, "컨버전스 시대의 N-Screen 방향," *멀티 무선 컨버전스 서비스 포럼 2010*

[3] AT&T Video Share - Wireless from AT&T - , http://www.wireless.att.com/messaging-internet/media-entertainment/attvideoshare.jsp

[4] Apple - MobileMe -, http://www.apple.com/mobileme/

[5] Live Mesh Beta, https://www.mesh.com/welcom/default.aspx

[6] 김윤화, "3 스크린 플레이(3 Screen Play) 서비스 추진현황," 방송통신정책, Vol.21, No.11, pp.79-82, 2009

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

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

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

[10] ZigBee Alliance Document, ZigBee Specification Pro/2007, 2007.

[11] Specification of the Bluetooth System, http:// www. bluetooth.com/Specification%20Documents/ Core_V40.zip, 2010.

[12] S.A.F.A. van den Heuvel, W. Jonker, F.L.A.J. Kamperman and P.J. Lenoir, "Secure Content Management in Authorised Domains," International Broadcasting Convention, 2002.

[13] Qingqi Pei, Kefeng Fan, Jianfeng Ma and Jinxiu Dai, "An Intelligent Digital Content Protection Framework between Home Network Receiver Devices," International Conference on Computational Intelligence and Security, 2006.

[14] Daniel Diaz-Sanchez, Andres Marin, Florina Almenarez and Alberto Cortes, "Sharing Conditional Access Modules through the Home Network for Pay TV Access," IEEE Transactions on Consumer Electronics, Vol.55, No.1, Feb., 2009

[15] F. K. Tu, C. S. Laih and S. H. Toung, "On Key Distribution Management for Conditional Access System on Pay-TV System," IEEE Transactions on Consumer Electronics, Vol.45, No.1, pp.151-158, 1999.

[16] Y. L. Huang and Sh. Shieh, "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems," IEEE Transactions on Multimedia, Vol.6, No.5, pp.760-769, 2004.

[17] Shyh-Yih Wang and Chi-Sung Laih, "Efficient Key Distribution for Access Control in Pay-TV Systems," IEEE Transactions on Multimedia, Vol.10, No.3, pp.480-492, 2008.

김 정 훈

e-mail : jhkim@infosec.hanyang.ac.kr
2010년 한양대학교 컴퓨터공학과(학사)
2010년～현 재 한양대학교 컴퓨터공학과 석사과정
관심분야 : 암호기술 응용, IPTV 보안

이 훈 정

e-maill : hjlee@infosec.hanyang.ac.kr
2003년 단국대학교 전자컴퓨터학부(학사)
2005년 한양대학교 컴퓨터공학과(석사)
2005년～2009년 (주)한단정보통신 전임연구원
2009년～현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 암호기술 응용, 키 관리

김 상 진

e-mail : sangjin@kut.ac.kr
1995년 한양대학교 전자계산학과(학사)
1997년 한양대학교 전자계산학과(석사)
2002년 한양대학교 전자계산학과(박사)
2003년～현 재 한국기술교육대학교 컴퓨터공학과 부교수
관심분야 : 암호기술 응용

오 희 국

e-mail : hkoh@hanyang.ac.kr
1983년 한양대학교 전자공학과(학사)
1989년 아이오와주립대학 전자계산학과 (석사)
1992년 아이오와주립대학 전자계산학과 (박사)
1993년～1994년 한국전자통신연구원 선임연구원
1995년～현 재 한양대학교 컴퓨터공학과 교수
관심분야 : 암호프로토콜, 네트워크 보안