다운로드형 제한수신 시스템의 성능 검증

*조용성 **권오형 ***최동준 ****허남호

한국전자통신연구원

*yscho73@etri.re.kr

Performance Evaluation of Downloadable Conditional Access System

*Cho, Yong Seong **Kwon, O-Hyeong ***Choi, Dong-Joon **** Her, Namho

Electronics and Telecommunications Research Institute (ETRI)

요약

최근 유료 방송 서비스를 위한 제한수신 시스템의 적용에 있어 지적되었던 여러 문제들을 해결할 수 있는 DCAS(Downloadable Conditional Access System) 기술이 소개되었다. 또한, OpenCable과 DCAS를 기반으로 국내 디지털 케이블 방송 시스템을 위한 교환가능형 제한수신 시스템(eXchangeable CAS: XCAS) 표준이 재정되었다. 본 논문에서는 DCAS와 국내 XCAS 표준 규격을 기반으로 개발된 다운로드형 제한수신 시스템을 소개하고, 개발된 시스템의 성능 검증 결과를 제시하여 상용 유료방송 시스템에 적용하는 방안에 대해 논하고자 한다.

1. 서론

제한수신 시스템은 케이블, 위성 및 IPTV 등과 같은 유료 방송 시스템에서 가입자에게 전송되는 방송 프로그램을 보호하고 유료 서비스에 가입된 정당한 가입자에게만 방송 시청 권한을 부여하기 위해 사용되고 있는 시스템이다 [1]. 초기 유료 방송 시스템에서는 각 방송 사업자별로 고유한 제한수신 시스템 방식을 적용한 하드웨어가 내장된 방송 수신기를 제공하는 형태의 서비스가 일반적이었다. 그러나, 제한수신 내장형 시스템에서는 시스템에 대한 해킹 또는 새로운 서비스의 추가 등의 이유로 방송 사업자가 제한수신 시스템을 변경하고자 하는 경우에 가입자에게 제공한 모든 셋톱박스를 교체해야 하는 문제가 발생하였다. 이후, 제한수신 내장형 시스템의 문제점을 해결하기 위하여 셋톱박스로부터 제한수신 관련 기능을 분리한 케이블카드라고 하는 하드웨어 보안 모듈을 사용하는 방식이 제안되기도 하였으나, 카드 발급에 따른 비용 문제, 동작 과정에서 발열에 의한 오작동 등과 같은 문제로 인해 시장의 외면을 받고 있는 실정이다 [2].

최근, 유료 방송 서비스를 위한 제한수신 시스템의 적용에 있어 지적되었던 여러 문제점을 해결할 수 있는 DCAS(Downloadable Conditional Access System) 기술이 소개되었다. DCAS는 디지털 케이블 망에서 제한수신 클라이언트 프로그램을 안전하게 다운로드 할 수 있는 보안 시스템 구조를 정의하고 있다. 이를 통해, 종래의 기술에서 제한수신 시스템 변경을 위해 셋톱박스 또는 케이블카드를 교체해야 하는 시간적, 금전적 손실을 최소화할 수 있고, 해킹이 발생한 경우나 새로운 서비스를 추가해야 하는 경우에도 빠르고 안전하게 제한수신 시스템을 변경할 수 있다.

국내에서는 OpenCable과 DCAS 표준을 기반으로 디지털 케이블 방송 시스템을 위한 교환가능형 제한수신 시스템(XCAS) 표준이 재정되었으며, 국내 표준 규격을 기반으로 한 상용화가 진행되고 있다.

본 논문에서는 DCAS 표준 규격과 국내 XCAS 표준 규격을 기반으로 설계되고 구현된 시스템을 소개하고, 개발된 시스템을 개선하고 상용 시스템에 적용할 수 있는 방안에 대한 논의를 위해 시스템 성능 검증 결과를 제시한다.

2. 개요

다운로드형 제한수신 시스템은 디지털 케이블 방송 시스템에서 HFC망을 통해 제한수신 시스템을 효과적으로 설치하고 변경할 수 있는 진보된 기술이다. 이를 위해, 제한수신 클라이언트 프로그램을 3자 인증을 기반으로 한 보안채널을 통해 방송 사업자의 헤드엔드로부터 가입자의 셋톱박스로 전송하고, 전송된 제한수신 클라이언트를 안전하게 구동시킬 수 있도록 하는 보안 시스템 구조를 정의하고 있다.

다운로드형 제한수신 시스템의 구조는 그림 1과 같다.

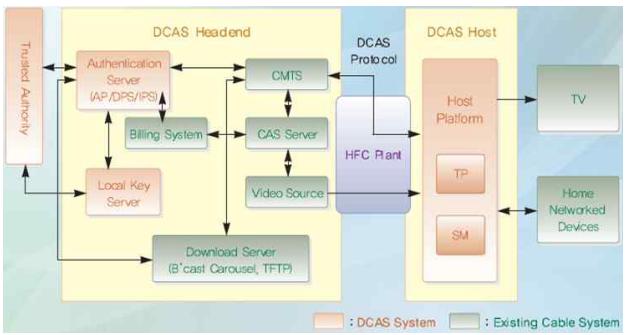


그림 1. 다운로드형 제한수신 시스템 구조

TA(Trusted Authority)는 방송 사업자의 헤드엔드와 가입자의 셋톱박스간의 상호 인증을 위한 3자 인증 기능을 제공하고, 헤드엔드와 셋톱박스 사이의 보안채널 형성을 위한 암호화 키 공유를 지원한다. 다운로드형 제한수신 시스템 헤드엔드는 방송 수신기의 인증, 다운로

드 클라이언트 및 다운로드 정책 관리 등의 기능을 담당하는 AP (Authentication Proxy), DPS(DCAS Provisioning Server), IPS (Integrated Personalization Server)와 보안을 위한 키를 관리하는 LKS(Local Key Server)로 구성된다. DCAS 방송수신기는 DES, TDES, DVB-CSA, AES 등 복수의 스크램블 방식을 지원하는 멀티 디스크램블러와 DCAS 보안을 위한 인증 프로토콜을 지원하고 다운로드 된 제한수신 시스템을 안전하게 관리하고 구동시키는 하드웨어 기반의 전용 보안칩인 보안모듈로 구성된다.

3. 설계 및 구현

가. 헤드엔드 인증시스템

앞서 언급한 바와 같이, 다운로드형 제한수신 시스템은 디지털 케이블 방송 시스템의 HFC망을 통해 제한수신 시스템을 변경하고 갱신할 수 있는 시스템 기술이다. 그러므로, 헤드엔드와 셋톱박스가 상호 교환하는 인증 메시지와 HFC망을 통해 다운로드되는 제한수신 클라이언트 프로그램의 보안을 유지하는 것이 무엇보다 중요하다. 제한수신 시스템이 다양한 해킹의 위협에 노출되어 제한수신 클라이언트 프로그램이 유출되면, 제한수신 시스템을 기반으로 한 유료 방송 시스템에 심각한 문제를 가져올 수 있기 때문이다.

본 시스템에서는 다운로드형 제한수신 시스템을 위한 헤드엔드 서버와 보안 인증 프로토콜이 개발되었다. 다운로드형 제한수신 시스템 인증 프로토콜은 상호 인증, 세션키 공유와 보안채널을 통한 안전한 다운로드를 지원하는 일련의 메시지들로 구성된다. 또한, 헤드엔드 인증시스템과 셋톱박스 사이에 교환되는 모든 메시지와 데이터는 암호화되고, 메시지 검증을 위한 서명을 포함하고 있다. 다운로드형 제한수신 시스템을 위한 인증 프로토콜의 인증 절차는 그림 2와 같다 [4].

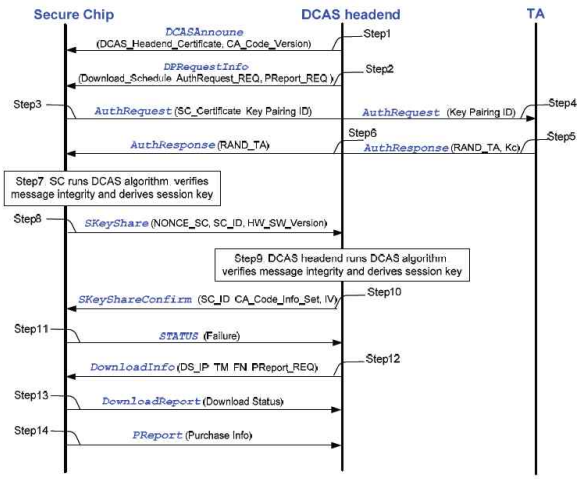


그림 2. 다운로드형 제한수신 시스템 인증 프로토콜 절차

헤드엔드 인증시스템은 다운로드형 제한수신 시스템 인증 프로토콜에 따라 가입자의 방송수신기와의 통신을 지원하는 AP, DPS, IPS로 구성되는 인증 서버와 키 정보를 관리하는 LKS로 구성되며, 시스템과 망의 보안을 위해 다음과 같은 기능을 제공한다.

- 제한수신 클라이언트 프로그램의 안전한 다운로드
- 다운로드 정책 관리 및 배포
- 제한수신 클라이언트 프로그램의 관리
- 다운로드형 제한수신 시스템 인증 프로토콜 처리
- 인증 관련 키 정보 관리

그림 3 다운로드형 제한수신 시스템 헤드엔드 서버

나. 다운로드형 제한수신 시스템 셋톱박스

다운로드형 제한수신 시스템을 지원하는 셋톱박스는 하드웨어 칩 기반의 멀티 디스크램블러와 보안모듈을 포함하는 구조로 설계되어 구현되었다.

멀티 디스크램블러는 다양한 방식의 제한수신 시스템을 지원할 수 있도록 DES, TDES, AES와 DVB-CSA 방식의 디스크램블러를 모두 포함하고 있으며, 보안모듈로부터 전달되는 제어단어를 이용하여 스크램블 된 방송 프로그램을 디스크램블하는 기능을 담당한다.

보안모듈은 다운로드 된 제한수신 클라이언트 프로그램이 안전하게 설치되어 구동될 수 있는 보안 환경을 제공한다. 또한, 헤드엔드 인증시스템과의 상호 인증, 세션키 공유를 위한 암호화 알고리즘을 포함하고 있으며, 물리적인 공격으로부터 보안모듈내의 보안 정보를 보호할 수 있는 보안 기능을 제공할 수 있다.

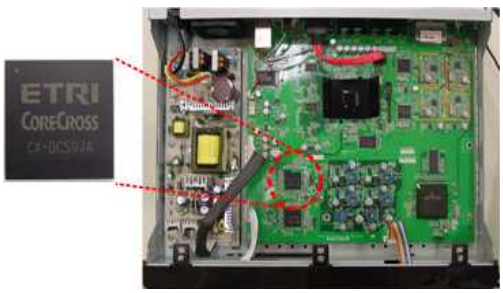


그림 4 다운로드형 제한수신 시스템 셋톱박스

4. 성능 검증

개발된 시스템의 성능을 검증하기 위하여 셋톱박스에 최초로 제한수신 시스템을 설치하는 경우와 방송 가입자의 거주지 변경 등으로 새로운 방송사업자의 제한수신 시스템으로 제한수신 시스템이 변경되는 두 가지 예상되는 경우를 가정한 시험을 통해 검증되었다.

- 시험 시나리오 1 : 어떤 제한수신 시스템도 설치되지 않은 셋톱박스가 최초로 기기에 대한 인증을 요청하는 경우를 가정한다. 헤드엔드 인증시스템은 셋톱박스의 등록여부를 확인하고 다운로드형 제한수신 시스템 인증 프로토콜에 따라 셋톱박스와의 보안 인증 절차를 진행한다. 보안 인증 절차를 통해 셋톱

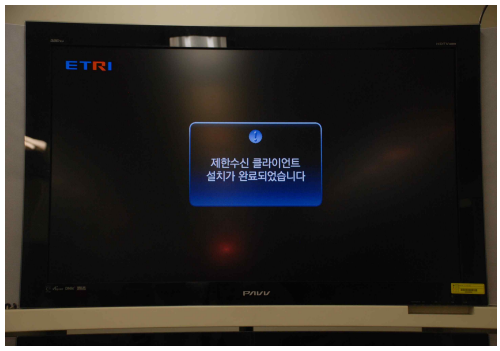
박스의 인증이 확인된 경우, HFC망을 통해 제한수신 클라이언트 프로그램이 다운로드 되어 설치된다. 이후, 셋톱박스의 보안모듈에 설치된 제한수신 클라이언트가 정상적으로 동작하면 유료 방송 시청이 가능하게 된다.

- 시험 시나리오 2 : 방송 가입자의 거주지 변경 등의 이유로 방송사업자의 변경이 발생한 경우를 가정한다. 이전과 다른 방송사업자의 망에 접속한 셋톱박스는 보안 인증 프로토콜에 따라 헤드엔드 인증시스템과 등록 확인과 기기 인증 과정을 진행한다. 헤드엔드 인증시스템은 셋톱박스를 인증하고, 인증된 셋톱박스로 제한수신 클라이언트 프로그램에 대한 다운로드 정보를 제공한다. 셋톱박스에 다운로드 된 제한수신 시스템이 설치되면 새로운 방송사업자의 제한수신 시스템과 연동하여 제공되는 유료방송을 시청할 수 있게 된다.
- 시험 시나리오 3 : 방송 사업자가 제한수신 시스템을 갱신하는 경우를 가정한다. 시험 시나리오 2와 동일한 절차에 따라 제한수신 시스템 클라이언트를 갱신된 후, 정상적으로 유료방송을 시청할 수 있게 된다.
- 시험 시나리오 4 : 방송 사업자가 기존의 제한수신 시스템을 다른 시스템으로 변경하는 경우를 가정한다. 시험 시나이로 2와 동일한 절차에 따라 제한수신 시스템이 변경된 후, 정상적으로 유료방송을 시청할 수 있게 된다.

그림 5는 개발된 시스템 상에서 시험 시나리오에 따라 셋톱박스를 인증하고, 제한수신 클라이언트 프로그램을 다운로드하여 제한수신 시스템을 설치 또는 변경한 후, 유료방송을 시청하는 과정을 시험한 결과의 예시한 것으로, 셋톱박스의 제한수신 시스템 정보 확인, 보안 인증 프로토콜을 통한 제한수신 시스템 클라이언트 다운로드, 제한수신 시스템 클라이언트 설치 및 정상적인 유료방송 시청까지의 과정을 살펴볼 수 있다.

a) 셋톱박스 및 제한수신 시스템 정보 교환

b) 인증된 셋톱박스의 제한수신 클라이언트 다운로드



c) 제한수신 클라이언트 설치

d) 클라이언트 설치 후 유료방송 시청

그림 5 다운로드형 제한수신 시스템 시험 결과

5. 결론

본 논문에서는 국내외 표준을 기반으로 설계되고 구현된 다운로드형 제한수신 시스템을 소개하였다. 또한, 구현된 시스템을 HFC망에서 다양한 경우를 가정한 시험 시나리오를 통해 검증함으로써, 유료방송을 위한 제한수신 시스템을 하드웨어 장치의 변경없이 유선을 통해 안전하고 빠르게 설치하고 변경할 수 있음을 확인하였다.

본 논문에서 소개한 다운로드형 제한수신 시스템은 방송 매체별 특성을 고려한 수정을 통해 다양한 유료방송 시스템 환경에 적용할 수 있을 것으로 기대된다.

참고문헌

[1] EBU Project Group B/CA, “Functional Model of a Conditional Access System,” EBU Technical Review, pp.64-77, Winter 1995
[2] Y. Cho et al., “Design and Implementation of Security Module for Downloadable Conditional Access System”, ICHIT 2010
[3] OpenCable™ Technical Reports: DCAS System Overview Technical Report, CableLabs, OC-TR-DCAS-D02-060912, 2006
[4] Y. Jeong, et al., “ A Noble Protocol for Downloadable CAS,” IEEE Trans. Consumer Electronics, vol.54, no.3, pp.1236-1243, Aug. 2008