



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0058840
(43) 공개일자 2010년06월04일

(51) Int. Cl.

H04N 7/16 (2006.01)

(21) 출원번호 10-2008-0117399

(22) 출원일자 2008년11월25일

심사청구일자 2008년11월25일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 공동 220번지 충남대학교

(72) 발명자

류재철

대전 유성구 어은동 한빛아파트 1032-801

이중후

대전 유성구 관평동 대덕테크노밸리아파트
504-301

김민영

충남 천안시 서북구 입장면 하장리 초원아파트
105-605

(74) 대리인

김원준

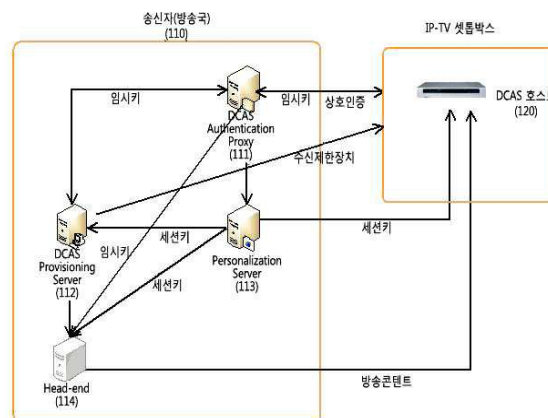
전체 청구항 수 : 총 5 항

(54) 디지털 방송용 제한수신장치를 다운로드하는 방법

(57) 요약

본 발명은, 송신자측에 DCAS 인증프록시(AP), 개인화서버, DCAS 제공서버 및 헤드엔드를 포함하는 방송 시스템과, 수신자측에 DCAS 호스트를 포함하는 셋톱박스로 이루어진 디지털방송 시스템에서 제한수신장치를 다운로드하는 방법으로서, (A) ① 셋톱박스에 입력된 라이선스 번호로부터 공유키를 생성하는 단계와, ② 상기 공유키를 이용하여 DCAS AP와 DCAS 호스트가 상호인증하는 단계와, ③ 상호인증되면 DCAS AP가 임시키(TK)를 생성하여 DCAS 호스트와 개인화서버에게 배포하는 단계로 이루어지는 DCAS AP와 DCAS 호스트간의 상호인증 및 키 분배 과정; (B) ① 상기 임시키를 이용해서 개인화서버와 DCAS 호스트가 상호인증하는 단계와, ② 상호인증되면 개인화서버가 세션키(SK)를 생성하여 DCAS 호스트와 DCAS 제공서버에게 배포하는 단계로 이루어지는 DCAS 개인화서버와 DCAS 호스트간의 상호인증 및 키 분배 과정; (C) ① DCAS 제공서버가 상기 세션키(SK)로 제한수신장치 소프트웨어를 암호화하여 DCAS 호스트로 전송하는 단계와, ② DCAS 호스트가 상기 세션키(SK)를 이용하여 제한수신장치 소프트웨어를 복호화하고 이를 설치하는 단계로 이루어지는 DCAS 제공서버와 DCAS 호스트간의 상호인증 및 키 분배 과정;을 포함하는 디지털 방송용 제한수신장치를 다운로드하는 방법에 관한 것이다.

대표도 - 도1



특허청구의 범위

청구항 1

송신자측에 DCAS 인증프록시(AP), 개인화서버, DCAS 제공서버 및 헤드엔드를 포함하는 방송 시스템과, 수신자측에 DCAS 호스트를 포함하는 셋톱박스로 이루어진 디지털방송 시스템에서 제한수신장치를 다운로드하는 방법으로서,

(A) ① 셋톱박스에 입력된 라이선스 번호로부터 공유키를 생성하는 단계와, ② 상기 공유키를 이용하여 DCAS AP와 DCAS 호스트가 상호인증하는 단계와, ③ 상호인증되면 DCAS AP가 임시키(TK)를 생성하여 DCAS 호스트와 개인화서버에게 배포하는 단계로 이루어지는 DCAS AP와 DCAS 호스트간의 상호인증 및 키 분배 과정;

(B) ① 상기 임시키를 이용해서 개인화서버와 DCAS 호스트가 상호인증하는 단계와, ② 상호인증되면 개인화서버가 세션키(SK)를 생성하여 DCAS 호스트와 DCAS 제공서버에게 배포하는 단계로 이루어지는 DCAS 개인화서버와 DCAS 호스트간의 상호인증 및 키 분배 과정;

(C) ① DCAS 제공서버가 상기 세션키(SK)로 제한수신장치 소프트웨어를 암호화하여 DCAS 호스트로 전송하는 단계와, ② DCAS 호스트가 상기 세션키(SK)를 이용하여 제한수신장치 소프트웨어를 복호화하고 이를 설치하는 단계로 이루어지는 DCAS 제공서버와 DCAS 호스트간의 상호인증 및 키 분배 과정을

포함하는 것을 특징으로 하는 디지털 방송용 제한수신장치를 다운로드하는 방법.

청구항 2

제 1 항에 있어서,

상기 (A) DCAS 인증프록시와 DCAS 호스트간의 상호인증과정은,

① 입력된 라이선스 번호의 해쉬값을 구하고, 이를 두 개로 분리하여 각각 송신용공유키와 수신용공유키로 저장하는 단계;

② 상기 라이선스 번호에 대한 송신용공유키 및 수신용공유키를 사전에 저장하고 있는 DCAS AP가, 제 1 임의값 a1을 생성하여 DCAS 호스트에게 전송하는 단계;

③ DCAS 호스트가 DCAS AP로부터 수신한 임의값 a1을 송신용공유키로 암호화하여 임의값 a2과 함께 DCAS AP로 전송하는 단계;

④ DCAS AP가 수신용공유키로 복호화하여 상기 임의값 a1을 확인한 후, DCAS 호스트가 전송한 임의값 a2 및 임시키(TK)를 송신용공유키로 암호화하여 DCAS 호스트에 전송하는 단계;

⑤ DCAS 호스트가 수신용공유키로 복호화하여 상기 임의값 a2를 확인한 후, 수신용공유키로 상기 임시키(TK)를 추출하는 단계;

⑥ DCAS AP가 임시키(TK)를 개인화서버에 전송하는 단계;로 이루어진 것을 특징으로 하는 디지털 방송용 제한수신장치를 다운로드하는 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 (B) DCAS 개인화서버와 DCAS 호스트간의 상호인증과정은,

① 개인화서버가 소정의 메시지와 세션키(SK)를 상기 임시키(TK)로 암호화하여 임의값 a3과 함께 DCAS 호스트로 전송하는 단계;

② DCAS 호스트가 상기 임시키(TK)로 복호화하여 소정의 메시지를 확인하고 세션키(SK)를 추출하는 단계;

③ DCAS 호스트가, 상기 임의값 a3을 세션키(SK)로 암호화하여 개인화서버로 전송하는 단계;

④ 개인화 서버가 세션키(SK)로 복호화하여 상기 임의값 a3을 확인한 후, 동일한 세션키(SK)를 DCAS 제공서버에게 전달하는 단계;로 이루어진 것을 특징으로 하는 디지털 방송용 제한수신장치를 다운로드하는 방법.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 (C) DCAS 제공서버와 DCAS 호스트간의 상호인증과정은,

- ① DCAS 제공서버가, 제한수신장치 소프트웨어와 제한수신장치 소프트웨어의 해쉬값을 세션키(SK)로 암호화하여 DCAS 호스트로 전송하는 단계;
- ② DCAS 호스트가 DCAS 제공서버로부터 수신한 정보를 상기 세션키(SK)로 복호화하여 제한수신장치 소프트웨어를 획득하고, 동시에 함께 전송된 해쉬값과 비교하여 다운로드 과정에서 변경되지 않았음을 확인하는 단계;
- ③ DCAS 호스트가 복호화된 제한수신장치 소프트웨어를 설치하는 단계;로 이루어진 것을 특징으로 하는 디지털 방송용 제한수신장치를 다운로드하는 방법.

청구항 5

제 1 항 또는 제 2 항에 의한 방법에 의한 디지털방송 시스템에서,

- (A) 상기 DCAS AP와 개인화서버가 각각 상기 임시키(TK)와 세션키(SK)를 디지털방송용 헤드엔드로 전송하는 단계;
- (B) 상기 헤드엔드가 H(임시키||세션키)를 분배키로 삼아 인증키를 암호화하여 배포하고, 다시 인증키로 제어단어를 암호화하여 배포한 뒤에 제어단어를 이용해서 방송 콘텐츠를 스�크램블링하여 셋톱박스로 전송하는 단계;
- (C) 상기 DCAS 호스트에 설치된 제한수신장치가 H(임시키||세션키)를 분배키로 삼아 인증키를 복호화하고, 복호화된 인증키를 이용해서 제어단어를 복호화 한 뒤에 제어단어를 이용해서 상기 방송 콘텐츠를 디스크램블링하는 단계;를

포함하는 것을 특징으로 하는 디지털 방송 송수신방법.

명세서

발명의 상세한 설명

기술분야

[0001] 본 발명은 디지털 방송에 적용되는 제한수신장치를 안전하게 다운로드하는 방법 및 디지털 방송의 콘텐츠 송수신 방법에 관한 것이다.

배경기술

[0002] 제한수신장치(CAS : Conditional Access System)는 디지털 방송 콘텐츠 보호를 위해 방송시스템에 가입자(subscriber)의 개념을 도입하여 수신자격이 있는 시청자만이 시청이 가능하도록 한 시스템이다. CAS는 송신부(방송국)에서 방송 콘텐츠를 암호화하고 가입자(수신기)를 인증하는 장비, 가입자(수신기) 측에 가입자 정보를 저장한 장치 및 방송 콘텐츠를 복호화하는 장치 등으로 구성되며 스�크램블링/디스크램블링, 자격 제어, 자격 관리 등의 기능을 가지고 있다.

[0003] ① 스�크램블링/디스크램블링(Scrambling/Descrambling) : 수신자격이 없는 수신자는 시청이 불가능하도록 데이터를 스�크램블링한다. 방송 콘텐츠는 제어단어(CW: Control Word)를 이용하여 암호화 및 복호화 처리된다. 제어단어는 암호화되어 스�크램블링된 방송 데이터와 함께 전송되며 수신자는 암호화된 제어단어를 복호화하고 이

를 이용해서 방송 데이터의 디스크램블링을 수행한다.

- [0004] ② 자격 제어(Entitlement Control) : 제어단어를 인증키(AK: Authentication Key)로 암호화하고, 이를 ECM(Entitlement Control Message)에 포함시켜 수신자에게 전송한다. ECM은 'E_{AK}[CW, 제어변수]'와 같은 구조로 되어 있다. 새롭게 생성되고 암호화된 제어단어는 주기적으로 전송된다. ECM에는 암호화된 제어단어 외에 제어변수가 포함된다. 수신기가 제어단어를 해독하고, 이를 이용하여 수신된 방송 데이터를 디스크램블링한다.
- [0005] ③ 자격 관리(Entitlement Management) : 수신기에 자격을 부여·갱신·관리하는 기능을 하며, 인증키를 분배키(DK: Distribution Key)로 암호화하여 EMM (Entitlement Management Message)을 생성하고 수신자에게 전송한다. EMM은 'E_{DK}[AK, 자격정보]'와 같은 구조로 되어 있다. 따라서 송신자와 수신자는 반드시 같은 비밀키인 분배키(DK)를 공유하여야 하며, 이러한 비밀키를 공유하는 과정에서 보안성을 높이기 위해 스마트 카드 등의 하드웨어를 이용하는 것이 일반적이다.
- [0006] 현재 우리나라의 케이블 방송은 미국식 표준인 오픈케이블(Opne Cable) 방식을 따르고 있는데, 오픈케이블 방식은 가입자 정보를 별도의 케이블카드(제한수신 모듈)에 담아 셋톱박스(가입자 단말장치)로부터 분리/장착할 수 있도록 하는 하드웨어적 방식이다. 또 다른 하드웨어적 방식으로는 CAS 모듈을 셋톱박스에 내장하는 임베디드 CAS가 있다. 그러나 이와 같이 하드웨어적으로 제한수신 클라이언트를 구현하는 경우에 호환성 부족, 연동성 부족, 안전성 미흡 등의 단점이 있다.
- [0007] ① 호환성 : 하드웨어로 구현된 제한 수신 시스템의 경우에는 한 제조업체에서 구현한 시스템과 다른 제조업체에서 구현한 시스템 간의 호환성 확보에 어려움이 있다.
- [0008] ② 다른 서비스와의 연동 : 최근 지적재산권의 중요성이 강조되면서 디지털저작권관리(DRM : Digital Right Management) 등에 대한 관심이 높아지고 있는 가운데, 하드웨어로 구현된 제한 수신 시스템은 DRM 등 다른 서비스와의 연동이 어렵다.
- [0009] ③ 안전성 : 하드웨어로 구현된 제한수신장치가 키 정보의 보호 등에 있어서 안전성이 높은 것은 사실이나, 제한수신장치에 내장된 암호 알고리즘이 크랙되거나 키 정보가 누출된 경우에는 이의 대체가 쉽지 않다. 즉, 하드웨어의 교체 이외에는 보안사고에 대처할 방법이 없다.
- [0010] 이러한 하드웨어적 방식에서의 문제점들을 해결하기 위해서 최근에는 제한수신 클라이언트를 소프트웨어로 구현하는 방식으로, 셋톱박스 내에서 물리적인 하드웨어 대신에 소프트웨어적으로 가입자 정보 등을 처리하는 '소프트웨어 CAS'와, '다운로드형 CAS(DCAS : Downlaodable CAS)'가 개발된 바 있다. DCAS는 셋톱박스에 사업자가 제공하는 CAS가 미리 설치돼 있는 것이 아니라 네트워크에 연결시 서버로부터 CAS를 보안이 보장되는 칩(Secure Micro)에 다운로드하는 방식이다. 이때 CAS뿐 아니라 DRM이나 ASD(Authorized Service Domain)과 같은 다른 보안모듈도 함께 내려받을 수 있다.
- [0011] 종래의 DCAS는 다음과 같이 동작한다.
- [0012] (1) DCAS AP (Authentication Proxy)와 DCAS 호스트는 미리 공유된 키를 소지하고 있다.
- [0013] (2) CAS 클라이언트 프로그램을 다운로드 해야 할 때, 이를 위해서 DCAS AP는 우선 DCAS 호스트를 발견하기 위한 메시지를 브로드캐스트한다.
- [0014] (3) DCAS 호스트가 (1)의 메시지에 응답함으로써 DCAS AP는 셋톱박스를 식별할 수 있다.
- [0015] (4) DCAS AP는 다운로드 될 CAS 클라이언트 프로그램을 암호화하는데 사용될 암호키를 DCA 호스트에게 전송한다. 이 때, 암호키를 암호화하는 데는 미리 공유된 키가 사용된다.
- [0016] (5) AP는 (3)에서 전달된 암호키로 CAS 클라이언트 프로그램을 암호화하여 DCAS 호스트에게 다운로드 한다. 이후 DCAS 호스트 내에서 CAS 클라이언트가 정상적으로 동작하게 된다.
- [0017] (6) 방송 시스템은 방송 콘텐츠를 스캔블하는데 사용되는 키(제어단어)를 DCAS 호스트에게 전송한다.
- [0018] (7) 방송 시스템은 스캔블된 방송 콘텐츠를 DCAS 호스트에게 전송한다.

[0019] 이러한 종래의 방법은 DCAS AP가 DCAS 호스트를 발견하는 과정에서 상호인증이 이루어지지 않으며, 제한수신장치를 암호화하는데 사용되는 암호키를 보호하기 위한 공유키의 분배 과정이 명확하지 않다.

[0020] 제한수신장치를 소프트웨어적으로 구현하는 것이 하드웨어로 구현하는 것에 비해서 여러 가지 장점을 갖지만, 이 방법 역시 몇 가지 문제점을 가지고 있는 것 또한 사실이다. 예를 들면, 현재 인터넷에서는 여러 가지 악성 소프트웨어로 인한 피해가 확산되고 있는데, 이와 같은 문제가 디지털 방송에서도 그대로 재현될 수 있다. 즉, 제한수신 서버로 가장한 공격자가 시스템이나 네트워크에 문제를 일으키는 악성 코드를 제한수신 클라이언트에 게 다운로드 함으로써 사용자나 방송 시스템 운영자에게 서비스 장애, 경제적 손실 등의 피해를 줄 수 있다. 특히 제한수신장치는 방송 콘텐츠를 디스크램블링 하는 가장 핵심 기능을 수행하기 때문에 제한수신장치 프로그램이 다운로드 되는 동안 위/변조 될 경우에는 전체 방송 서비스에 피해를 줄 수 있다.

발명의 내용

해결 하고자하는 과제

[0021] 본 발명은 종래의 방법에서 발생할 수 있는 보안 문제점을 해결하고 전체 시스템의 보안성을 개선하는 것을 목적으로 한다.

[0022] 또한 본 발명은, IP-TV 방송 시스템으로부터 방송을 다운로드 받아 시청하는데 있어서 스크램블링 된 방송 콘텐츠를 디스크램블링하는 역할을 하는 제한수신장치를 보호하는 방법을 제공하는 것을 목적으로 한다.

과제 해결수단

[0023] 전술한 과제를 해결하기 위한 본 발명은, 송신자측에 DCAS 인증프로시(AP), 개인화서버, DCAS 제공서버 및 헤드엔드를 포함하는 방송 시스템과, 수신자측에 DCAS 호스트를 포함하는 셋톱박스로 이루어진 디지털방송 시스템에서 제한수신장치를 다운로드하는 방법으로서, (A) ① 셋톱박스에 입력된 라이선스 번호로부터 공유키를 생성하는 단계와, ② 상기 공유키를 이용하여 DCAS AP와 DCAS 호스트가 상호인증하는 단계와, ③ 상호인증되면 DCAS AP가 임시키(TK)를 생성하여 DCAS 호스트와 개인화서버에게 배포하는 단계로 이루어지는 DCAS AP와 DCAS 호스트간의 상호인증 및 키 분배 과정; (B) ① 상기 임시키를 이용해서 개인화서버와 DCAS 호스트가 상호인증하는 단계와, ② 상호인증되면 개인화서버가 세션키(SK)를 생성하여 DCAS 호스트와 DCAS 제공서버에게 배포하는 단계로 이루어지는 DCAS 개인화서버와 DCAS 호스트간의 상호인증 및 키 분배 과정; (C) ① DCAS 제공서버가 상기 세션키(SK)로 제한수신장치 소프트웨어를 암호화하여 DCAS 호스트로 전송하는 단계와, ② DCAS 호스트가 상기 세션키(SK)를 이용하여 제한수신장치 소프트웨어를 복호화하고 이를 설치하는 단계로 이루어지는 DCAS 제공서버와 DCAS 호스트간의 상호인증 및 키 분배 과정;을 포함하는 디지털 방송용 제한수신장치를 다운로드하는 방법에 관한 것이다.

[0024] 본 발명에서 상기 (A) DCAS AP와 DCAS 호스트간의 상호인증과정은, ① 입력된 라이선스 번호의 해쉬값을 구하고, 이를 두 개로 분리하여 각각 송신용공유키와 수신용공유키로 저장하는 단계; ② 상기 라이선스 번호에 대한 송신용공유키 및 수신용공유키를 사전에 저장하고 있는 DCAS AP가, 제 1 임의값 a1을 생성하여 DCAS 호스트에게 전송하는 단계; ③ DCAS 호스트가 DCAS AP로부터 수신한 임의값 a1을 송신용공유키로 암호화 a1'하여 임의값 a2과 함께 DCAS AP로 전송하는 단계; ④ DCAS AP가 수신용공유키로 복호화하여 상기 임의값a1을 확인한 후, DCAS 호스트가 전송한 임의값 a2 및 임시키(TK)를 송신용공유키로 암호화하여 DCAS 호스트에 전송하는 단계; ⑤ DCAS 호스트가 수신용공유키로 복호화하여 상기 임의값 a2를 확인한 후, 수신용공유키로 상기 임시키(TK)를 추출하는 단계; 및 ⑥ DCAS AP가 임시키(TK)를 개인화서버에 전송하는 단계;로 이루어질 수 있다.

[0025] 본 발명에서 상기 (B) DCAS 개인화서버와 DCAS 호스트간의 상호인증과정은, ① 개인화서버가 소정의 메시지와 세션키(SK)를 상기 임시키(TK)로 암호화하여 임의값 a3과 함께 DCAS 호스트로 전송하는 단계; ② DCAS 호스트가 상기 임시키(TK)로 복호화하여 소정의 메시지를 확인하고 세션키(SK)를 추출하는 단계; ③ DCAS 호스트가, 상기

임의값 a3을 세션키(SK)로 암호화하여 개인화서버로 전송하는 단계; 및 ④ 개인화서버가 세션키(SK)로 복호화하여 상기 임의값 a3을 확인한 후, 동일한 세션키(SK)를 DCAS 제공서버에게 전달하는 단계;로 이루어질 수 있다.

[0026] 본 발명에서 상기 (C) DCAS 제공서버와 DCAS 호스트간의 상호인증과정은, ① DCAS 제공서버가, 제한수신장치 소프트웨어와 제한수신장치 소프트웨어의 해쉬값을 세션키(SK)로 암호화하여 DCAS 호스트로 전송하는 단계; ② DCAS 호스트가 DCAS 제공서버로부터 수신한 정보를 상기 세션키(SK)로 복호화하여 제한수신장치 소프트웨어를 획득하고, 동시에 함께 전송된 해쉬값과 비교하여 다운로드 과정에서 변경되지 않았음을 확인하는 단계; 및 ③ DCAS 호스트가 복호화된 제한수신장치 소프트웨어를 설치하는 단계;로 이루어질 수 있다.

[0027] 또한 본 발명은, 전술한 방법에 의한 디지털방송 시스템에서, (A) 상기 DCAS AP와 개인화서버가 각각 상기 임시 키(TK)와 세션키(SK)를 디지털방송용 헤드엔드로 전송하는 단계; (B) 상기 헤드엔드가 H(임시키||세션키)를 분배키로 삼아 인증키를 암호화하여 배포하고, 다시 인증키로 제어단어를 암호화하여 배포한 뒤에 제어단어를 이용해서 방송 콘텐츠를 스�크램블링하여 셋톱박스로 전송하는 단계; 및 (C) 상기 DCAS 호스트에 설치된 제한수신장치가 H(임시키||세션키)를 분배키로 삼아 인증키를 복호화하고, 복호화된 인증키를 이용해서 제어단어를 복호화한 뒤에 제어단어를 이용해서 상기 방송 콘텐츠를 디스크램블링하는 단계;를 포함하는 디지털 방송 송수신방법에 관한 것이다.

효 과

[0028] 종래의 다운로드 가능한 제한수신장치가 적용된 IP-TV 시스템은 방송 시스템과 IP-TV 셋톱박스 간의 인증 방법이 취약하고, 다운로드 되는 제한수신장치 소프트웨어의 암호화에 사용되는 암호키의 관리 방법이 취약하다. 이에 따라 공격자가 방송 시스템(DCAS AP)로 위장하여 악성코드를 가입자에게 다운로드 하거나, 비인가 사용자가 제한수신장치 소프트웨어를 다운로드 받아 불법적으로 방송 콘텐츠를 시청하는 공격이 가능하다.

[0029] 본 발명에 의하면 DCAS AP와 DCAS 호스트는 도전-응답 방식에 기반한 상호인증 절차를 수행하기 때문에 DCAS AP로 위장하여 공격자가 개설한 사이트로 DCAS 호스트의 연결을 유도하는 공격을 차단할 수 있다.

[0030] 본 발명에 의하면 개인화서버와 DCAS 호스트는 도전-응답 방식에 기반한 상호인증 절차를 수행하기 때문에 개인화서버로 위장하여 DCAS 호스트가 악성코드를 다운로드 받도록 유도하는 공격을 차단할 수 있다.

[0031] 본 발명에 의하면 DCAS 제공서버(Provisioning Server)에서 DCAS 호스트로 다운로드 하는 제한수신장치 소프트웨어를 암호화함으로써 암호화에 사용되는 암호키를 모르는 비인가 사용자가 제한수신장치 소프트웨어를 다운로드 받아 불법적으로 방송 콘텐츠를 시청하는 공격을 차단할 수 있다.

[0032] 본 발명에 의하면 방송 콘텐츠를 스�크램블링 하는데 사용되는 키가 제한수신장치 소프트웨어가 다운로드 되는 과정에 함께 배포되도록 함으로써 비인가 사용자가 불법적으로 방송 콘텐츠를 시청하는 공격을 차단할 수 있다.

[0033] 본 발명에 의하면 방송 사업자는 소프트웨어적으로 구현된 제한수신장치를 가입자에게 제공함으로써 유지/보수 등에 소요되는 비용을 줄임과 동시에 비인가 사용자에게 의한 불법 시청을 차단함으로써 이익을 극대화 할 수 있다.

[0034] 또한 본 발명에 의하면 IP-TV를 시청하는 가입자는 소프트웨어적으로 구현된 제한수신장치를 통해 최신의 제한수신장치를 사용하는데 종래의 시스템이 가지고 있는 불편함을 제거할 수 있으며, 악성코드 유입 등의 외부 침해로부터 안전한 방식으로 IP-TV 서비스를 제공받을 수 있다.

발명의 실시를 위한 구체적인 내용

[0035] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 그러나 이러한 도면 및 그에 대한 서술은 본 발명의 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 본 발명의 기술적 범위가 한정되거나 변경되는 것은 아니다. 또한 이러한 예시에 기초하여 본 발명의 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 당업자에게는 당연할 것이다.

- [0036] 도 1은 안전한 다운로드 가능한 제한수신 시스템을 구성하는 일반적인 도면이다. 도 1의 예에서 방송 시스템(110)은 DCAS AP(111), DCAS 제공서버(112), 개인화서버(113), 헤드엔드(114)로 구성된다. 이 때, 헤드엔드 시스템은 여러 개의 하위 구성요소로 좀 더 복잡하게 구성되나, 본 발명의 설명에서는 단순화한다.
- [0037] 방송 사업자는 DCAS AP(111)를 통해서 가입자의 IP-TV 셋톱박스(120)를 발견하고, 셋톱박스에 설치된 DCAS 호스트와의 상호인증을 통해서 정당한 가입자인지 확인한다. 상호인증 과정에서는 이후 제한수신장치를 다운로드 받기 위해서 DCAS 호스트가 개인화서버와 연결할 때 개인화서버를 인증하는데 사용되는 키가 교환된다. 개인화서버는 DCAS 호스트와 상호인증을 수행하면서 이후 제한수신 클라이언트를 암호화할 때 사용될 암호키를 배포한다. DCAS 제공서버는 개인화서버와 DCAS 호스트의 상호인증 과정에서 배포된 암호키를 이용해서 제한수신 장치 소프트웨어를 암호화하여 DCAS 호스트에게 전송한다.
- [0038] 도 2는 DCAS AP(111)과 DCAS 호스트(120)가 상호인증을 수행하는 절차를 나타내는 예시이다. (210)과 (220)은 IP-TV 셋톱박스가 최초로 설치될 때 배포되는 키 정보이다. IP-TV 셋톱박스가 설치될 때 함께 배포되는 소프트웨어와 함께 인쇄된 형태로 배포되는 라이선스 키의 해쉬값과 동일하다. 따라서 (210)과 (220)은 서로 동일한 값이다. 도 2의 상호인증 과정이 시작되면 (210)과 (220)은 각각 (211), (212)와 (221), (222)로 분리된다. 이는 전송 방향에 따라 사용되는 키를 달리 함으로써 보안성을 향상시키기 위함이다.
- [0039] (단계 230)에서 CAS AP는 DCAS 호스트에게 Challenge 값 Rand1을 전송한다.
- [0040] (단계 231)에서 DCAS 호스트는 Epsk1[Rand1]과 같이 Response 값을 생성한다. Response 값과 함께 DCAS AP 인증을 위해서 Challenge 값 Rand 2를 전송한다.
- [0041] (단계 232)에서 DCAS AP는 Epsk1[Rand1]를 계산하여 DCAS 호스트가 전송한 값과 일치하는지 여부를 확인함으로써 DCAS 호스트를 인증한다. 그리고 DCAS 호스트가 전송한 Challenge 값에 대하여 Epsk2[Rand2 + TK]와 같이 Response 값을 생성하여 DCAS 호스트에게 전송한다. 이 때, TK는 DCAS PS에게 전달될 임시키이다.
- [0042] (단계 232) 이후에 DCAS 호스트는 Epsk2[Rand2 + TK]를 복호화하여 그 결과에 자신이 전송한 Rand2가 포함되어 있으면, 정당한 DCAS AP로 간주하고 인증을 완료하며 TK를 저장한다. 또한 DCAS AP는 자신이 생성한 TK를 개인화서버에게 전달한다.
- [0043] 도 3은 방송 시스템(110) 내의 개인화서버(113)와 DCAS 호스트(120)가 상호인증을 수행하는 절차를 나타내는 예시이다.
- [0044] (단계 310)에서 개인화서버는 DCAS AP로부터 전달 받은 TK를 이용해서 제한수신장치 소프트웨어를 암호화하는데 사용될 키(SK)와 약속된 메시지(SUCCESS)를 암호화하여 DCAS 호스트에게 전송한다. 이 때, DCAS 호스트 인증을 위한 Challenge 값인 Rand3이 함께 전송된다.
- [0045] (단계 311)에서 DCAS Host는 개인화서버가 전송한 메시지를 복호화하여 약속된 메시지(SUCCESS)가 포함되어 있으면 TK를 소지하고 있는 정당한 개인화서버로 간주한다. 이후 획득한 Rand3과 SK를 이용해서 Response를 생성해 개인화서버에게 전달한다.
- [0046] (단계 311) 이후에 개인화서버는 DCAS 호스트가 전송한 메시지를 확인함으로써 인증을 완료하고, SK를 DCAS 제공서버에게 전달한다.
- [0047] 도 4는 DCAS AP와 DCAS 호스트, 개인화서버와 DCAS 호스트 간의 상호인증이 각각 완료된 이후에, DCAS 제공서버로부터 DCAS 호스트로 제한수신장치 소프트웨어가 안전하게 다운로드 되는 절차를 나타내는 예시이다.
- [0048] (단계 410)에서 DCAS 제공서버는 앞서 개인화서버와 DCAS 호스트 간의 상호인증 과정에서 개인화서버로부터 전달 받은 SK를 이용해서 E_{SK}[제한수신장치 소프트웨어]와 같이 DCAS 클라이언트 프로그램을 암호화하여 DCAS 호스트에게 전달한다. 이 때, 제한수신장치 소프트웨어의 해쉬값을 함께 전송함으로써 DCAS 호스트가 제한수신장치 소프트웨어가 다운로드 도중에 변경되었는지 여부를 확인할 수 있도록 한다.

[0049] 도 4에 예시된 과정까지 완료된 이후에 방송시스템의 헤드엔드 시스템에서 방송 콘텐츠를 스크램블링하여 DCAS 호스트로 전송하는 과정은 종래의 방법과 동일하다. 이 때, 분배키는 앞서 배포된 임시키(TK)와 세션키(SK)를 합친 뒤에 해쉬연산을 수행한 결과($DK = H(TK || SK)$)로 한다. 즉, 제한수신장치 소프트웨어를 다운로드 하는 과정에서 방송콘텐츠를 스크램블링 하는데 사용된 키 값이 배포된다.

도면의 간단한 설명

[0050] 도 1은 본 발명이 적용되는 제한수신장치의 보호를 위한 방송 시스템의 구성을 나타내는 개념도.

[0051] 도 2 내지 도 4는 본 발명에 의한 방법에서 상호인증과정을 예시적으로 보여주는 개념도.

[0052] <도면의 주요 부분에 대한 부호 설명>

[0053] 110: 송신자(방송국)

[0054] 111: DCAS AP

[0055] 112: DCAS 제공서버

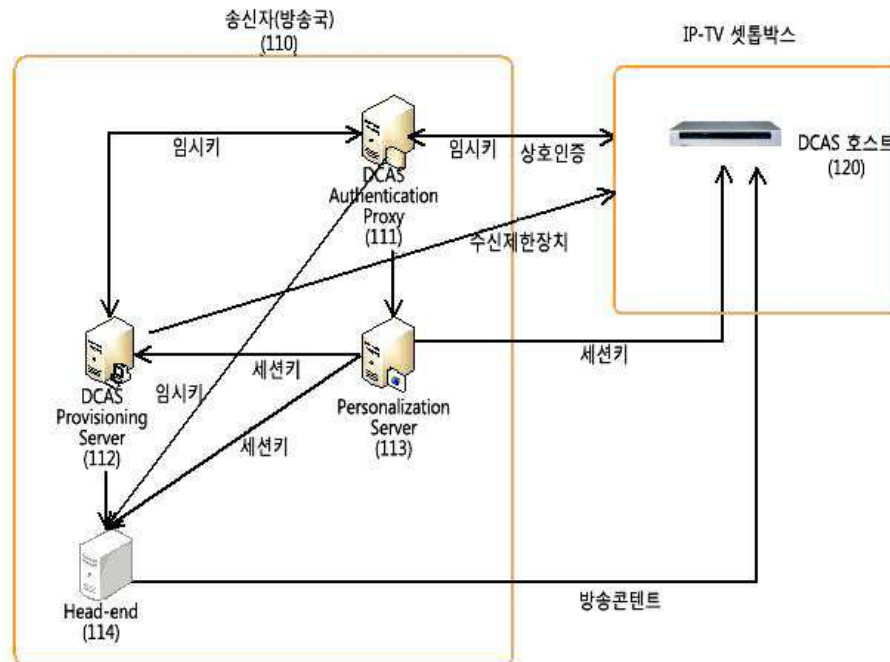
[0056] 113: 개인화서버

[0057] 114: 헤드엔드

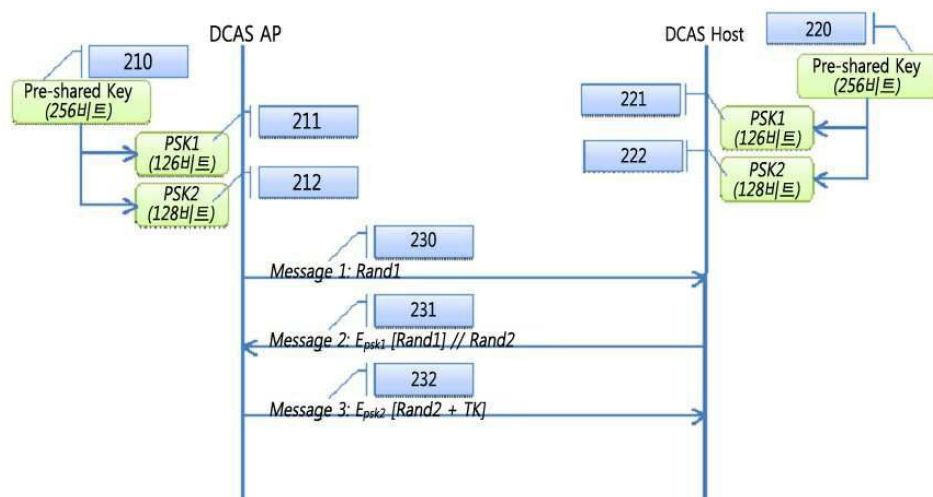
[0058] 120: IP-TV 셋톱박스 (DCAS 호스트 및 제한수신장치 탑재)

도면

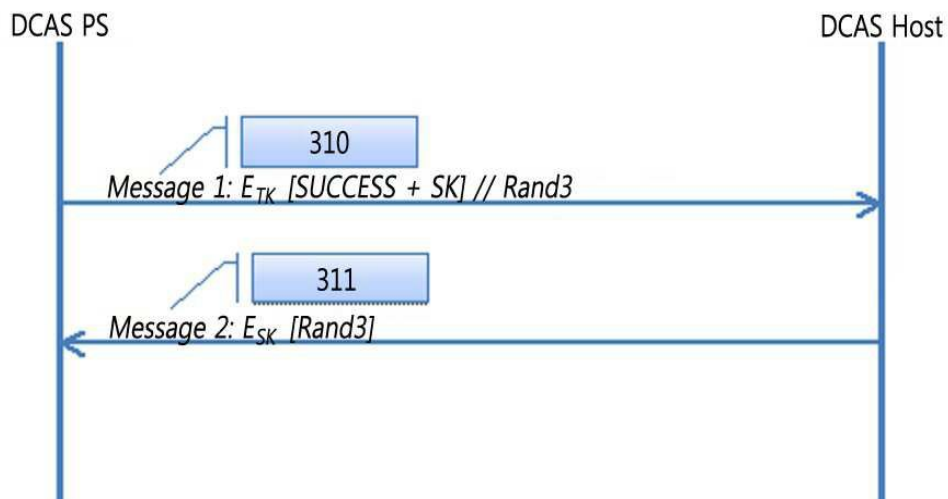
도면1



도면2



도면3



도면4

