(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년07월03일
(11) 등록번호 10-1281928
(24) 등록일자 2013년06월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/18 (2006.01) *H04N 7/167* (2011.01)
H04L 12/18 (2006.01)
(21) 출원번호 10-2009-0121881
(22) 출원일자 2009년12월09일
심사청구일자 2009년12월09일
(65) 공개번호 10-2010-0102032
(43) 공개일자 2010년09월20일
(30) 우선권주장
1020090020127 2009년03월10일 대한민국(KR)
(56) 선행기술조사문헌
US20080177998 A1
US20080098212 A1
Jeong et al., "A novel protocol for downloadable CAS," IEEE Transactions on Consumer Electronics, Vol. 54, No. 3, P 1236-1243.
전체 청구항 수 : 총 18 항

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
권은정
대전광역시 서구 대덕대로 415, 102동 603호 (만년동, 상아아파트)
구한승
대전광역시 서구 둔산북로 215, 10동 1302호 (둔산동, 가람아파트)
(뒷면에 계속)
(74) 대리인
특허법인무한

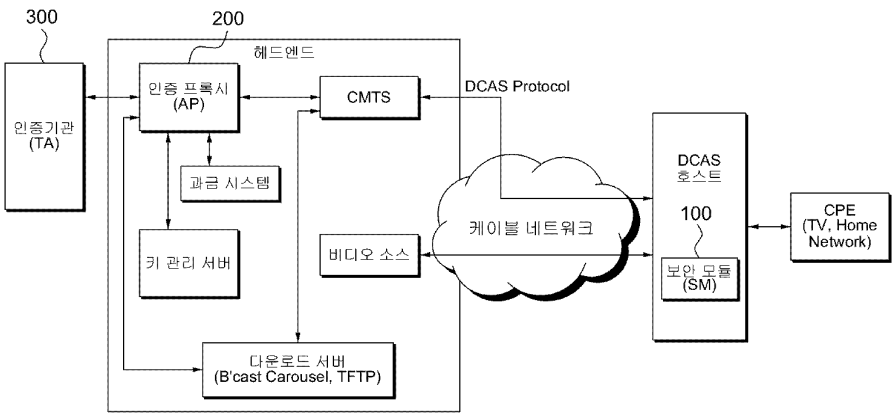
심사관 : 이형일

(54) 발명의 명칭 **다운로더블 제한 수신 시스템에서의 상호 인증 장치 및 방법**

(57) 요 약

본 발명의 다운로더블 제한 수신 시스템에서의 상호 인증 장치는 인증 프록시(AP: Authentication Proxy)를 이용하여 보안 알림(SecurityAnnounce) 정보를 인증하여 보안 모듈(SM: Secure Micro)로 전송하는 알림 프로토콜(Announce Protocol) 처리부, 상기 인증 기관 및 상기 보안 모듈 간의 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보 및 키 응답(KeyResponse) 정보를 중계하는 키 프로토콜(Keying Protocol) 처리부, 상기 보안 모듈을 이용하여 상기 키 응답 정보를 복호화 하는 복호화부, 상기 키 응답 정보에 대한 제1 암호화 키와 상기 인증 프록시에서 생성한 제2 암호화 키와 동일한지 여부를 판단하는 인증 프로토콜(Authentication Protocol) 처리부 및 상기 보안 모듈이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를 상기 인증 프록시로부터 상기 보안 모듈로 전송하는 다운로드 프로토콜(Download Protocol) 처리부를 포함한다.

대 표 도



(72) 발명자

김순철

대전광역시 유성구 반석동로 33, 양지마을5단지아파트 503동 1101호 (반석동)

김희정

대전광역시 유성구 은구비남로 34, 열매마을아파트 802동 1101호 (노은동)

정영호

대전시 유성구 용산동 우림필유아파트 1107동 1204호

권오형

대전광역시 유성구 어은로 57, 107동 1103호 (어은동, 한빛아파트)

이수인

대전광역시 서구 둔산로 155, 크로바아파트 106동 606호 (둔산동)

이 발명을 지원한 국가연구개발사업

과제고유번호	2007-S-007-03
부처명	방송통신위원회
연구사업명	IT성장동력기술개발
연구과제명	Downloadable 제한수신 시스템 개발
주관기관	한국전자통신연구원
연구기간	2007. 03. 01 ~ 2010. 02. 28

특허청구의 범위

청구항 1

인증 프록시(AP: Authentication Proxy)가 보안 알림(SecurityAnnounce) 정보를 인증하여 보안 모듈(SM: Secure Micro)로 전송하도록 제어하는 알림 프로토콜(Announce Protocol) 처리부;

인증 기관 및 상기 보안 모듈 간의 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보 및 키 응답(KeyResponse) 정보를 중계하는 키 프로토콜(Keying Protocol) 처리부;

상기 보안 모듈이 상기 키 응답 정보를 복호화하도록 제어하는 복호화부;

상기 키 응답 정보에 대한 제1 암호화 키와 상기 인증 프록시에서 생성한 제2 암호화 키와 동일한지 여부를 판단하는 인증 프로토콜(Authentication Protocol) 처리부; 및

상기 보안 모듈이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를, 상기 인증 프록시로부터 상기 보안 모듈로 전송하도록 제어하는 다운로드 프로토콜(Download Protocol) 처리부

를 포함하고,

상기 복호화부는,

상기 보안 모듈이 버진 스테이트(Virgin State)인 경우 또는 인증 프록시 지역(AP Zone)을 이동한 경우, 최신 공용키(CHK: Common Hash Key)를 추출하여 공용키를 업데이트시키도록 제어하는 업데이트부; 및

상기 보안 모듈이 버진 스테이트가 아닌 경우 또는 인증 프록시 지역을 이동하지 않은 경우, 상기 보안 모듈에 보유된 공용키(CHK)를 통해 HMAC 메시지 인증을 수행하도록 제어하는 인증부

를 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 2

제1항에 있어서,

상기 키 프로토콜 처리부는,

상기 보안 모듈이 상기 인증 프록시로부터 상기 보안 알림 정보에 포함된 공용키(CHK: Common Hash Key)를 수신하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 3

제1항에 있어서,

상기 키 프로토콜 처리부는,

상기 보안 모듈이 상기 보안 모듈의 개인키로 전자 서명된 상기 키 요구 정보를 상기 인증 프록시로 전송하도록 제어하고, 상기 인증 프록시가 상기 키 요구 정보로부터 추출한 키 페어링 식별자(Key Paring ID) 및 인증 프록시 식별자(AP ID)를 기반으로 재생성된 상기 키 요구 정보를 상기 인증 기관으로 전송하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 4

제3항에 있어서,

상기 키 프로토콜 처리부는,

상기 인증 기관이 상기 키 페어링 식별자를 통하여 보안 모듈 인증서를 조회하여 상기 보안 모듈을 인증하도록 제어하고, 상기 인증 기관이 상기 보안 모듈의 인증 결과를 상기 키 응답 정보에 정의하여 상기 인증 프록시로 전송하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 5

제4항에 있어서,

상기 키 프로토콜 처리부는,

상기 인증 프록시가 인증 프록시 인증서를 상기 키 응답 정보에 정의하여 상기 보안 모듈로 전송하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 6

제5항에 있어서,

상기 복호화부는,

상기 보안 모듈이 상기 인증 프록시 인증서를 기반으로 상기 키 응답 정보에 포함된 정보 중 어느 하나 이상을 복호화하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 7

삭제

청구항 8

제1항에 있어서,

상기 제1 암호화 키는 상기 보안 모듈을 통하여 상기 키 응답 정보를 기반으로 생성된 제1 메시지 암호화 키(Message Encryption Key) 및 제1 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함하고,

상기 제2 암호화 키는 상기 인증 프록시를 통하여 생성된 제2 메시지 암호화 키(Message Encryption Key) 및 제2 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 9

제8항에 있어서,

상기 각 제1, 2 메시지 암호화 키는 상기 보안 모듈과 상기 인증 프록시 간에 전송되는 메시지를 암호화 하는데 사용되는 대칭키이며,

상기 각 제1, 2 보안 모듈 클라이언트 이미지 암호화 키는 상기 보안 모듈 클라이언트 이미지 정보를 암호화 하기 위하여 사용되는 대칭키인 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 10

제9항에 있어서,

상기 각 제1, 2 메시지 암호화 키 및 상기 각 제1, 2 보안 모듈 클라이언트 이미지 암호화 키는 마스터 키(MK)에 Pseudo Random Number Generator(PRNG)을 입력하여 생성되는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 11

제1항에 있어서,

상기 인증 프로토콜 처리부는,

상기 제1 암호화 키가 상기 인증 프록시에서 생성한 제2 암호화 키와 동일하지 않은 경우, 상기 인증 프록시가 상기 보안 모듈로 상기 제1 암호화 키와 상기 제2 암호화 키의 불일치 여부를 알리는 불일치 정보를 전송하도록 제어하는 다운로더블 제한 수신 시스템에서의 상호 인증 장치.

청구항 12

알림 프로토콜 처리부, 키 프로토콜 처리부, 복호화부, 인증 프로토콜 처리부, 다운로드 프로토콜 처리부를 포함하는 상호 인증 장치를 이용하여 상호 인증을 수행하는 방법에 있어서,

상기 키 프로토콜 처리부가 인증 프록시(AP: Authentication Proxy)가 보안 알림(SecurityAnnounce) 정보를 인증하도록 제어하고, 상기 인증된 보안 알림 정보를 상기 인증 프록시로부터 보안 모듈(SM: Secure Micro)로 전송하도록 제어하는 단계;

상기 키 프로토콜 처리부가 인증 기관 및 상기 보안 모듈 간의 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보 및 키 응답(KeyResponse) 정보를 중계하는 단계;

상기 복호화부가 상기 보안 모듈이 상기 키 응답 정보를 복호화 하도록 제어하는 단계;

상기 복호화부가 상기 보안 모듈이 버진 스테이트(Virgin State)인 경우 또는 인증 프록시 지역(AP Zone)을 이동한 경우, 최신 공용키(CHK: Common Hash Key)를 추출하여 공용키를 업데이트시키도록 제어하는 단계;

상기 복호화부가 상기 보안 모듈이 버진 스테이트가 아닌 경우 또는 인증 프록시 지역을 이동하지 않은 경우 상기 보안 모듈에 보유된 공용키(CHK)를 통해 HMAC 메시지 인증을 수행하도록 제어하는 단계

상기 인증 프로토콜 처리부가 상기 키 응답 정보에 대한 제1 암호화 키와 상기 인증 프록시에서 생성한 제2 암호화 키와 동일한지 여부를 판단하는 단계; 및

상기 다운로드 프로토콜 처리부가 상기 보안 모듈이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를 상기 인증 프록시로부터 상기 보안 모듈로 전송하도록 제어하는 단계

를 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 13

제12항에 있어서,

상기 키 프로토콜 처리부가 상기 보안 모듈이 상기 인증 프록시로부터 상기 보안 알림 정보에 포함된 공용키(CHK: Common Hash Key)를 수신하도록 제어하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 14

제12항에 있어서,

상기 키 프로토콜 처리부가 상기 보안 모듈이 상기 보안 모듈의 개인키로 전자 서명된 상기 키 요구 정보를 상기 인증 프록시로 전송하도록 제어하는 단계; 및

상기 키 프로토콜 처리부가 상기 인증 프록시가 상기 키 요구 정보로부터 추출한 키 페어링 식별자(Key Paring ID) 및 인증 프록시 식별자(AP ID)를 기반으로 재생성된 상기 키 요구 정보를 상기 인증 기관으로 전송하도록 제어하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 15

제14항에 있어서,

상기 키 프로토콜 처리부가 상기 인증 기관이 상기 키 페어링 식별자를 통하여 보안 모듈 인증서를 조회하여 상기 보안 모듈을 인증하도록 제어하는 단계; 및

상기 키 프로토콜 처리부가 상기 보안 모듈의 인증 결과를 상기 키 응답 정보에 정의하여 상기 인증 프록시로 전송하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 16

제15항에 있어서,

상기 키 프로토콜 처리부가 상기 인증 프록시가 인증 프록시 인증서를 상기 키 응답 정보에 정의하여 상기 보안 모듈로 전송하도록 제어하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 17

제16항에 있어서,

상기 복호화부가 상기 보안 모듈이 상기 인증 프록시 인증서를 기반으로 상기 키 응답 정보에 포함된 정보 중 어느 하나 이상을 복호화하도록 제어하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 18

삭제

청구항 19

제12항에 있어서,

상기 제1 암호화 키는 상기 보안 모듈을 통하여 상기 키 응답 정보를 기반으로 생성된 제1 메시지 암호화 키(Message Encryption Key) 및 제1 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함하고,

상기 제2 암호화 키는 상기 인증 프록시를 통하여 생성된 제2 메시지 암호화 키(Message Encryption Key) 및 제2 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

청구항 20

제12항에 있어서,

상기 제1 암호화 키가 상기 인증 프록시에서 생성한 제2 암호화 키와 동일하지 않은 경우, 상기 인증 프로토콜 처리부가 상기 인증 프록시가 상기 보안 모듈로 상기 제1 암호화 키와 상기 제2 암호화 키의 불일치 여부를 알리는 불일치 정보를 전송하도록 제어하는 단계

를 더 포함하는 다운로더블 제한 수신 시스템에서의 상호 인증 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명의 실시예들은 다운로더블 제한 수신 시스템에서의 상호 인증 장치 및 방법에 관한 것이다.

[0002] 본 발명은 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발지원사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2007-S-007-03, 과제명: Downloadable 제한 수신 시스템 개발].

배 경 기 술

[0003] 제한수신시스템은 방송 프로그램에 암호를 삽입하여 시청이 허가된 가입자들만 유료방송을 시청할 수 있는 권한을 부여해주는 시스템으로, 유료 방송 서비스를 제공하기 위해서는 CA(Conditional Access) 응용의 구현 형태에 따라 대부분 스마트 카드 또는 PCMCIA 카드 형태의 케이블카드를 이용하고 있다.

[0004] 최근 들어서는 양방향 통신 네트워크를 기반으로 다운로더블 제한수신 시스템(DCAS: Downloadable Conditional Access System) 기술 개발이 이슈가 되고 있는 바, 다운로더블 제한 수신 시스템이란, 셋탑박스에 CAS S/W가 설치될 수 있는 보안모듈을 탑재하여 양방향 통신 네트워크를 통해 CAS S/W의 결함 발생이나 CAS S/W의 버전 업데

이트 등과 같은 상황에서 용이하게 CAS S/W를 갱신할 수 있도록 하는 기술이다.

[0005] 다운로더블 제한 수신 시스템은 인증되지 않은 상태의 가입자의 셋탑박스로 CAS S/W를 전송할 경우 가입자는 불법적으로 유료방송 서비스의 시청이 가능하거나 예측하지 못한 상황을 발생시킬 수 있기 때문에 인증 서버와 셋탑박스에 탑재될 보안모듈간의 상호인증이 수행되어야 한다.

[0006] 또한, 셋탑박스에 탑재될 보안모듈이 헤드엔드에 위치한 인증 프록시를 인증하지 않을 경우 인증 프록시를 가장한 제 3의 서버로부터 다양한 공격을 받을 수가 있다.

[0007] 따라서, 전술한 바와 같은 다운로드 가능한 제한수신 시스템에서 보안상의 문제점을 해결하기 위한 효과적인 상호인증 방법이 요구되고 있다.

발명의 내용

해결 하고자하는 과제

[0008] 본 발명의 일실시예는 인증 프록시와 보안 모듈 간의 상호 인증 프로토콜을 제공하는 것을 목적으로 한다.

[0009] 또한, 본 발명의 일실시예는 하드웨어 기반의 실체 인증이 불필요해 뿐만 아니라, 이에 따른 운용비용의 절감, 결함이 발생 시 빠른 시스템 갱신이 가능한 상호 인증 장치를 제공하는 것을 목적으로 한다.

[0010] 또한, 본 발명의 일실시예는 다운로더블 제한 수신 시스템에서 소프트웨어를 전송하기 위한 과정에서 발생하는 트래픽 데이터 암호화/복호화, 메시지 인증, 장치 인증 등과 같은 다양한 보안의 세부기능들을 수행할 수 있는 효과적인 인증 프로토콜을 제공하는 것을 목적으로 한다.

과제 해결수단

[0011] 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 장치는 인증 프록시(AP: Authentication Proxy)를 이용하여 보안 알림(SecurityAnnounce) 정보를 인증하여 보안 모듈(SM: Secure Micro)로 전송하는 알림 프로토콜(Announce Protocol) 처리부, 상기 인증 기관 및 상기 보안 모듈 간의 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보 및 키 응답(KeyResponse) 정보를 중계하는 키 프로토콜(Keying Protocol) 처리부, 상기 보안 모듈을 이용하여 상기 키 응답 정보를 복호화 하는 복호화부, 상기 키 응답 정보에 대한 제1 암호화 키와 상기 인증 프록시에서 생성한 제2 암호화 키와 동일한지 여부를 판단하는 인증 프로토콜(Authentication Protocol) 처리부 및 상기 보안 모듈이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를 상기 인증 프록시로부터 상기 보안 모듈로 전송하는 다운로드 프로토콜(Download Protocol) 처리부를 포함한다.

[0012] 또한, 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 방법은 인증 프록시(AP: Authentication Proxy)를 이용하여 보안 알림(SecurityAnnounce) 정보를 인증하여 보안 모듈(SM: Secure Micro)로 전송하는 단계, 상기 인증 기관 및 상기 보안 모듈 간의 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보 및 키 응답(KeyResponse) 정보를 중계하는 단계, 상기 보안 모듈을 이용하여 상기 키 응답 정보를 복호화 하는 단계, 상기 키 응답 정보에 대한 제1 암호화 키와 상기 인증 프록시에서 생성한 제2 암호화 키와 동일한지 여부를 판단하는 단계 및 상기 보안 모듈이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를 상기 인증 프록시로부터 상기 보안 모듈로 전송하는 단계를 포함한다.

효 과

[0013] 본 발명의 일실시예에 따르면 인증 프록시와 보안 모듈 간의 상호 인증 프로토콜을 제공할 수 있다.

[0014] 또한, 본 발명의 일실시예에 따르면 하드웨어 기반의 실체 인증이 불필요해 뿐만 아니라, 이에 따른 운용비용의 절감, 결함이 발생 시 빠른 시스템 갱신이 가능한 상호 인증 장치를 제공할 수 있다.

[0015] 또한, 본 발명의 일실시예에 따르면 다운로더블 제한 수신 시스템에서 소프트웨어를 전송하기 위한 과정에서 발생하는 트래픽 데이터 암호화/복호화, 메시지 인증, 장치 인증 등과 같은 다양한 보안의 세부기능들을 수행할 수 있는 효과적인 인증 프로토콜을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

[0016] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예에 의해 제한되거나 한정되는 것은 아니다.

[0017] 한편, 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0018] 도 1은 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템의 구성을 도시한 블록도이다.

[0019] 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템은 전술한 바와 같이 보안 모듈(SM: Secure Micro)(100)과 인증 프록시(AP: Authentication Proxy)(200) 간의 상호 인증 방법을 제공한다.

[0020] 본 발명의 일실시예에 따른 상호 인증 장치는, DCAS 호스트 보안 모듈(100), 헤드엔드의 인증 프록시(200) 및 인증 프록시(200)와 연결된 인증 기관(TA: Truxted Authority)(300)를 포함한다.

[0021] 본 발명의 일실시예에 따른 인증 프록시(200)와 보안 모듈(100)은 도 1에 도시된 바와 같이, 케이블 네트워크를 통해 양방향 통신이 가능하다.

[0022] 본 발명의 일실시예에 따른 인증 프록시(200)와 보안 모듈(100)은 인증에 필요한 정보를 관리하기 위해 케이블 사업자가 아닌 제 3의 인증 기관(300)을 활용하며, 인증 기관(300)은 인증 프록시(200)을 통하여 인증에 필요한 각종 중요한 정보를 제공한다.

[0023] 본 발명의 일실시예에 따른 인증 프록시(200)는 인증 기관(300)으로부터 전송 받은 인증에 필요한 정보를 보안 모듈(100)로 전송하기 위하여 CMTS를 경유하며, 인증 과정에서 발생하는 모든 키 정보는 키 관리 서버에서 관리되고, 인증이 정상적으로 완료된 후에는 제한 수신 시스템(CAS: Conditional Access System) 소프트웨어가 다운로드 서버 및 CMTS를 거쳐 보안 모듈(100)로 전송된다.

[0024] 본 발명의 일실시예에 따른 보안 모듈(100)은 제한 수신 시스템(CAS: Conditional Access System) 소프트웨어를 다운로드 함으로써, 스크램블되어 전송되는 방송 신호에 대한 시청 허가를 획득하여 가입자에게 TV와 같은 CPE(Customer Premises Equipment)를 통해 유료방송 서비스를 제공할 수 있다.

[0025] 본 발명의 일실시예에 따른 보안 모듈(100), 인증 프록시(200) 및 인증 기관(300) 간에 송수신 되는 메시지에 대한 규약 및 절차에 관한 통신 메커니즘을 DCAS 프로토콜 이라고 정의하고, DCAS 프로토콜을 통하여 보안 모듈(100), 인증 프록시(200), 인증 기관(300) 사이에 송수신되는 메시지에 대한 보안 및 이들간의 인증 기능을 수행하게 된다.

[0026] 도 2는 본 발명의 일실시예에 따른 케이블 네트워크 상의 통신 메커니즘 계층도를 도시한 도면이다.

[0027] 이때, 본 발명의 일실시예에 따르면 DCAS 프로토콜이 동작하는 계층은 도 2에 도시된 바와 같이 케이블 네트워크를 통한 DOCSIS계층, IP계층, TCP/UDP계층과는 독립적으로 동작되도록 제어된다.

[0028] 본 발명의 일실시예에 따른 DCAS 프로토콜의 주요기능 중 하나는 제한 수신 시스템 소프트웨어를 보안 모듈(100)로 안전하게 전송하기 위하여 사전에 인증 프록시(200)와 보안 모듈(100) 간의 상호 인증을 수행 과정이 포함되어야 한다.

[0029] 따라서, 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 보안 모듈(100)과 인증 프록시(200) 간의 상호 인증 방법을 도 3 및 도 4를 참조하여 상세히 설명하도록 한다.

[0030] 도 3은 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 장치의 구성을 도시한 블록도이고, 도 4는 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 방법을 도시한 흐름도이다.

[0031] 이때, 본 발명의 일실시예에 따른 보안 모듈(100), 인증 프록시(200) 및 인증 기관(300)는 네트워크 프로토콜 동작 전에 다음과 같은 정보를 보유하고 있음을 가정하여 설명하기로 한다.

[0032] 한편, 본 발명의 다른 실시예에 따르면, 인증 기관(300)을 헤드엔드 내로 이동시킬 경우 LKS(Local Key Server)가 인증 기관(300)의 기능을 대체할 수도 있다.

[0033] 본 발명의 일실시예에 따른 보안 모듈(100)은 인증 기관 인증서(TA X.509 인증서), 보안 모듈 인증서(SM 인증서), Ki 값 및 3 * OP(Operation Variant Algorithm Configuration Field) 등의 값을 보유하고 있음을 가정한다.

[0034] 또한, 본 발명의 일실시예에 따른 인증 프록시(200)는 인증 기관 인증서(TA X.509 인증서) 및 인증 프록시(AP X.509 인증서) 등의 값을 보유하고 있음을 가정한다.

[0035] 또한, 본 발명의 일실시예에 따른 인증 기관은 인증 기관 인증서(TA X.509 인증서), 인증 프록시 인증서(AP X.509 인증서), 보안 모듈 인증서(SM 인증서), 3 * OP, Ki 값 및 키 페어링 식별자 정보(Key Paring ID) 등의 값을 보유하고 있음을 가정한다.

[0036] 상기와 같은 가정 하에 본 발명의 일실시예에 따른 상호 인증 장치는 알림 프로토콜(Announce Protocol) 처리부(310), 키 프로토콜(Keying Protocol) 처리부(320), 인증 프로토콜(Authentication Protocol) 처리부(340) 및 다운로드 프로토콜(Download Protocol) 처리부(350)로 구성된다.

[0037] 본 발명의 일실시예에 따른 알림 프로토콜 처리부(310)는 인증 프록시(200)를 이용하여 보안 알림(SecurityAnnounce) 정보를 보안 모듈(100)로 전송하도록 제어한다(401).

[0038] 이때, 본 발명의 일실시예에 따른 알림 프로토콜 처리부(310)는, 인증 프록시(200)를 이용하여 상기 보안 알림 정보를 HMAC(Hashed Message Authentication Code) 방식으로 인증하여 멀티캐스트(multicast) 방식으로 보안 모듈(100)로 전송한다.

[0039] 한편, 본 발명의 일실시예에 따른 보안 모듈(100)은 공용키(CHK: Common Hash Key)를 이용하여 상기 HMAC 메시지 인증을 수행한다. 이에, 본 발명의 일실시예에 따른 보안 모듈(100)은 인증 프록시(200)로부터 수신된 상기 보안 알림 정보에 대한 인증을 수행하기 위하여 다음과 같은 키 프로토콜 과정을 수행한다.

[0040] 이때, 본 발명의 일실시예에 따른 보안 모듈(100)은 인증 프록시(200)가 보유한 공용키와 동일한 공용키를 보유하지 않은 경우, 인증 프록시 지역(AP Zone)을 이동한 경우 또는 공용키를 보유하고 있지 않은 버진 스테이트(Virgin State)인 경우 인증 프록시(200)로부터 상기 보안 알림 정보에 포함된 공용키를 수신한다.

[0041] 본 발명의 일실시예에 따른 키 프로토콜 처리부(320)는 인증 프록시(200)를 이용하여 보안 모듈(100)로부터 상기 보안 알림 정보에 대한 키 요구(KeyRequest) 정보를 수신하여 인증 기관(300)으로 전송하고, 상기 전송한 키 요구 정보에 대한 키 응답(KeyResponse) 정보를 인증 기관(300)으로부터 수신하여 보안 모듈(100)로 전송한다(402~405).

[0042] 본 발명의 일실시예에 따른 키 프로토콜 처리부(320)는, 보안 모듈(100)을 이용하여 보안 모듈(100)의 개인키로 전자 서명된 상기 키 요구 정보를 인증 프록시(200)로 전송하도록 제어한다(402).

[0043] 본 발명의 일실시예에 다른 키 프로토콜 처리부(320)는 인증 프록시(200)를 이용하여 상기 키 요구 정보에 대한 RSA 전자 서명 검증하고, 상기 키 요구 정보로부터 추출한 키 페어링 식별자(Key Paring ID) 및 인증 프록시 식별자(AP ID)를 기반으로 재생성된 상기 키 요구 정보를 인증 기관(300)으로 전송한다(403).

[0044] 본 발명의 일실시예에 따른 키 프로토콜 처리부(320)는, 인증 기관(300)을 이용하여 상기 키 페어링 식별자를 통하여 보안 모듈 인증서(SM 인증서)를 조회하여 보안 모듈(100)을 인증하고, 보안 모듈(100)의 인증 결과를 상기 키 응답 정보에 정의하여 인증 프록시(200)로 전송한다(404).

[0045] 이때, 본 발명의 일실시예에 따른 인증 기관(300)은 보안 모듈(100)이 버진 스테이트(Virgin State)인 경우 티피 페어링(TP_Paring) 기능을 수행하거나, 보안 모듈(100)이 버진 스테이트가 아닌 경우 초기 페어링(Paring) 값과 비교확인 기능을 수행한다.

[0046] 본 발명의 일실시예에 따른 키 프로토콜 처리부(320)는, 인증 프록시(200)를 이용하여 인증 프록시 인증서(AP 인증서)를 상기 키 응답 정보에 정의하여 보안 모듈(100)로 전송한다(405).

[0047] 이때, 본 발명의 일실시에에 따른 인증 프록시(200)는 상기 키 응답 정보의 Auth_Rst의 값이 참이면, 해쉬 키(Hash Key) 생성 절차에 따라 공용키(CHK) 및 개인키(IHK: Individual Hash Key))를 생성하여 상기 인증 프록시 인증서와 함께 키 응답 정보 에 추가하여, 인증 프록시(200)의 개인키로 전자 서명하고 일부 인자에 대해서는 보안 모듈(100)의 공개키로 암호화 하여 보안 모듈로 상기 키 응답 정보를 전송한다.

[0048] 본 발명의 일실시예에 따른 복호화부(330)는 보안 모듈(100)을 이용하여 상기 키 응답 정보를 복호화 한다

(406).

[0049] 이때, 본 발명의 일실시예에 따른 복호화부(330)는 보안 모듈(100)을 이용하여 상기 인증 프록시 인증서를 기반으로 상기 키 응답 정보에 포함된 정보 중 어느 하나 이상을 복호화한다.

[0050] 예를 들어, 본 발명의 일실시예에 따른 복호화부(330)는 업데이트부 및 인증부 등으로 구성될 수 있는 바, 도 5를 참조하여 복호화 및 인증 과정을 설명하면 다음과 같다.

[0051] 도 5는 본 발명의 일실시예에 따른 복호화 및 인증 과정을 도시한 흐름도이다.

[0052] 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 보안 알림 정보를 수신하여 이를 분석하고(510), 버진 스테이트인지 여부를 판단한다(520).

[0053] 이때, 본 발명의 일실시예에 따른 업데이트부는 보안 모듈(100)을 이용하여 버진 스테이트(Virgin State)인 경우 또는 인증 프록시 지역(AP Zone)을 이동한 경우, 최신 공용키(CHK: Common Hash Key)를 추출하여 공용키를 업데이트시킨다(530).

[0054] 또한, 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 보안 알림 정보에 포함된 인증 프록시 식별자(AP_ID)가 보안 모듈(100) 내부에 보유한 인증 프록시 식별자와 동일한지 여부를 판단하고(540), 동일한 식별자를 보유하지 않은 경우 단계(530)을 수행한다.

[0055] 그러나, 본 발명의 일실시예에 따른 인증부는 보안 모듈(100)을 이용하여 버진 스테이트가 아닌 경우 또는 인증 프록시 지역을 이동하지 않은 경우 보안 모듈(100)에 보유된 공용키(CHK)를 통해 HMAC 메시지 인증을 수행한다(550).

[0056] 또한, 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 보안 알림 정보 인증을 성공하였는지 여부를 판단하고(560), 성공하지 못 한 경우 상기 단계(530)을 수행한다.

[0057] 그러나, 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 보안 알림 정보 인증을 성공한 경우 상기 키 요구 정보를 인증 프록시(200)로 전송하고 상기 키 응답 정보로부터 공용키, 개인키 및 암호화 키 등을 추출한다(570).

[0058] 본 발명의 일실시예에 따른 인증 프로토콜 처리부(340)는 보안 모듈(100)로부터 상기 키 응답 정보에 대한 제1 암호화 키를 포함하는 클라이언트 서명(ClientSignOn) 정보를 인증 프록시(200)로 전송하고, 인증 프록시(200)를 이용하여 상기 제1 암호화 키가 인증 프록시(200)에서 생성한 제2 암호화 키와 동일한지 여부를 판단하여 동일한 경우, 상기 클라이언트 서명 정보에 대한 클라이언트 서명 확인(ClientSignOnConfirm) 정보를 보안 모듈(100)로 전송하도록 제어한다(407~409).

[0059] 이때, 본 발명의 일실시예에 따른 상기 제1 암호화 키는 상기 보안 모듈을 통하여 상기 키 응답 정보를 기반으로 생성된 제1 메시지 암호화 키(Message Encryption Key) 및 제1 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함하고, 상기 제2 암호화 키는 상기 인증 프록시를 통하여 생성된 제2 메시지 암호화 키(Message Encryption Key) 및 제2 보안 모듈 클라이언트 이미지 암호화 키(SM Client Image Encryption Key)를 포함한다.

[0060] 예를 들어, 본 발명의 일실시예에 따른 보안 모듈(100)는 상기 키 응답 정보에 정의된 값을 이용하여 상기 제1 메시지 암호화 키 및 상기 제1 보안 모듈 클라이언트 이미지 암호화 키를 생성한다.

[0061] 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 제1 메시지 암호화 키 및 제1 보안 모듈 클라이언트 이미지 암호화 키가 인증 프록시(200)에서도 생성될 수 있도록 상기 클라이언트 서명 정보를 생성한다.

[0062] 이때, 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 제1 메시지 암호화 키와 상기 제1 보안 모듈 클라이언트 이미지 암호화 키 값에 대한 해쉬(Hash) 값도 상기 클라이언트 서명 정보에 추가하며, 상기 키 응답 정보에 정의된 개인키를 이용하여 HMAC을 적용한 후 인증 프록시(200)로 전송한다(407).

[0063] 본 발명의 일실시예에 따른 인증 프록시(200)는 상기 클라이언트 서명 정보를 수신하여 인증 프록시(200)의 개인키를 이용하여 HMAC 메시지 인증을 수행한다.

[0064] 본 발명의 일실시예에 따른 인증 프록시(200)는 상기 클라이언트 서명 정보에 해쉬(Hash)된 상기 제1 메시지 암호화 키 및 상기 제1 보안 모듈 클라이언트 이미지 암호화 키 값이 인증 프록시(200)가 생성한 제2 메시지 암호화 키 및 제2 보안 모듈 클라이언트 이미지 암호화 키 값과 동일한지 비교하여 다음과 같은 과정을 수행한다.

[0065] 예를 들어, 본 발명의 일실시예에 따른 인증 프록시(200)는 제1 메시지 암호화 키 및 상기 제1 보안 모듈 클라이언트 이미지 암호화 키가 상기 제2 메시지 암호화 키 및 상기 제2 보안 모듈 클라이언트 이미지 암호화 키가 상이한 경우, 불일치 여부를 알리는 불일치 정보를 보안 모듈(100)로 전송한다.

[0066] 또한, 본 발명의 일실시예에 따른 인증 프록시(200)는 제1 메시지 암호화 키 및 상기 제1 보안 모듈 클라이언트 이미지 암호화 키가 상기 제2 메시지 암호화 키 및 상기 제2 보안 모듈 클라이언트 이미지 암호화 키가 동일한 경우 클라이언트 서명 확인 정보를 상기 보안 모듈(100)로 전송한다(409).

[0067] 이때, 상기 클라이언트 서명 확인 정보는 상기 암호화 키 및 IV 값을 입력으로 하는 AES(Advanced Encryption Standard) 알고리즘을 이용하여 암호화 하여 전송된다.

[0068] 본 발명의 일실시예에 따른 다운로드 프로토콜 처리부(350)는 보안 모듈(100)이 보안 모듈 클라이언트 이미지(SM Client Image) 정보를 다운로드하도록 허여하는 다운로드 제공 정보(DownloadInfo)를 인증 프록시(200)로부터 보안 모듈(100)로 전송하도록 제어한다(410).

[0069] 이때, 상기 다운로드 제공 정보는 개인키를 이용하여 HMAC 메시지 인증을 수행하고 상기 암호화 키 및 IV 입력의 AES 알고리즘을 이용하여 메시지를 암호화 한 후 보안 모듈(100)로 전송된다.

[0070] 본 발명의 일실시예에 따른 보안 모듈(100)은 상기 다운로드 제공 정보를 수신하여 메시지 인증 및 복호화 과정을 정상적으로 수행하고, 보안 모듈 클라이언트 이미지 정보가 저장된 서버로부터 상기 보안 모듈 클라이언트 이미지 정보를 다운로드 한다.

[0071] 이때, 상기 보안 모듈 클라이언트 이미지 정보는 상기 암호화 키 및 IV를 이용하여 AES 로 암호화 되어 있으므로, 보안 모듈(100)은 이를 복호화 하기 위하여 상기 암호화 키 및 IV를 이용하여 상기 보안 모듈 클라이언트 이미지 정보를 복호화 하여 이를 수행할 수 있게 된다.

[0072] 또한, 본 발명의 일실시예에 따른 다운로드 프로토콜 처리부(350)는 상기 다운로드 제공 정보에 대한 다운로드 확인(DownloadConfirm) 정보를 보안 모듈(100)로부터 인증 프록시(200)로 전송하도록 제어한다(411).

[0073] 또한, 본 발명의 일실시예에 따른 보안 모듈은 상기 다운로드 제공 정보에 구매 리포트 요구 정보(PurchaseReport_REQ)가 정의된 경우, 개인키를 이용하여 구매 리포트 정보(PurchaseReportMessage)에 HMAC을 적용하고 상기 암호화 키로 암호화하여 인증 프록시(200)로 전송한다(412).

[0074] 본 발명의 일실시예에 따른 상호 인증 장치의 보안 모듈(100)과 인증 프록시(200) 간의 DCAS 인증 프로토콜을 수행에서 메시지 인증에 필요한 해쉬 키(Hash Key)인 공용키(CHK)와 개인키(IHK) 생성 절차는 다음과 같다.

[0075] 본 발명의 일실시예에 따른 개인키와 공용키는 아래와 같이 SHA(Secure Hash Algorithm)1 해쉬 함수를 이용해 생성될 수 있다. 이때, 난수 RANDIHK와 RANDCHK는 하드웨어 기반 또는 소프트웨어 기반 중 하나로 생성 될 수 있다.

[0076] 예를 들어, 본 발명의 일실시예에 따른 개인키와 공용키는 하드웨어로 생성하는 경우 FIPS 140-2 section 4.7.1 방식으로, 소프트웨어로 생성하는 경우 FIPS 186-2 appendix 3.3 방식으로 구현될 수 있다. 이때, 상기 개인키와 공용키는 소프트웨어로 구현될 경우 난수 생성기의 시드(seed) 값은 유일한 유닛(unit-unique)에 대한 비밀(secret) 값이어야 한다.

[0077] 또한, 본 발명의 일실시예에 따른 보안 모듈(100)과 인증 프록시(200) 간의 DCAS 인증 프로토콜을 수행에서 메시지 암호화 및 상기 보안 모듈 클라이언트 이미지 정보 암호화에 필요한 상기 각 제1, 2 메시지 암호화 키 및 상기 각 제1, 2 보안 모듈 클라이언트 이미지 암호화 키 생성 절차는 다음과 같다.

[0078] 이때, 상기 메시지 암호화 키는 DCAS 네트워크 프로토콜에서 보안 모듈(100)과 인증 프록시(200) 간에 전송되는 메시지를 암호화 하는데 사용되는 대칭키이다. 또한, 상기 보안 모듈 클라이언트 이미지 암호화 키는 상기 보안 모듈 클라이언트 이미지 정보를 암호화 하기 위하여 사용되는 대칭키이다.

[0079] 도 6은 본 발명의 일실시예에 따른 메시지 암호화 키 및 보안 모듈 이미지 암호화 키 생성 방법을 도시한 흐름도이다.

[0080] 예를 들어, 상기 메시지 암호화 키 및 상기 보안 모듈 클라이언트 암호화 키는 128 bits 길이를 가지며, 도 6에 도시된 바와 같이 마스터 키(MK)를 Pseudo Random Number Generator (PRNG)의 입력으로 취해 생성할 수 있다.

[0081] 본 발명의 일실시예에 따르면 도 6에 도시된 SHA1의 입력 값들 중 n*Kc에서 n이 3이라는 것은 인증 프록시로부

터 수신한 RAND_TA 내 3개의 RAND 값들로 생성된 3개의 Kc의 연속으로 붙여진 값을 의미한다.

[0082] 본 발명의 일실시예에 따르면 핑(PRNG)은 FIPS 186-2 내에 규정된 알고리즘 1(Algorithm 1)의 변형을 사용하며, RFC4186 의 Appendix B에 기술된 알고리즘을 따를 수 있다.

[0083] 본 발명에 따른 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(Floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0084] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면의 간단한 설명

[0085] 도 1은 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템의 구성을 도시한 블록도이다.

[0086] 도 2는 본 발명의 일실시예에 따른 케이블 네트워크 상의 통신 메커니즘 계층도를 도시한 도면이다.

[0087] 도 3은 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 장치의 구성을 도시한 블록도이다.

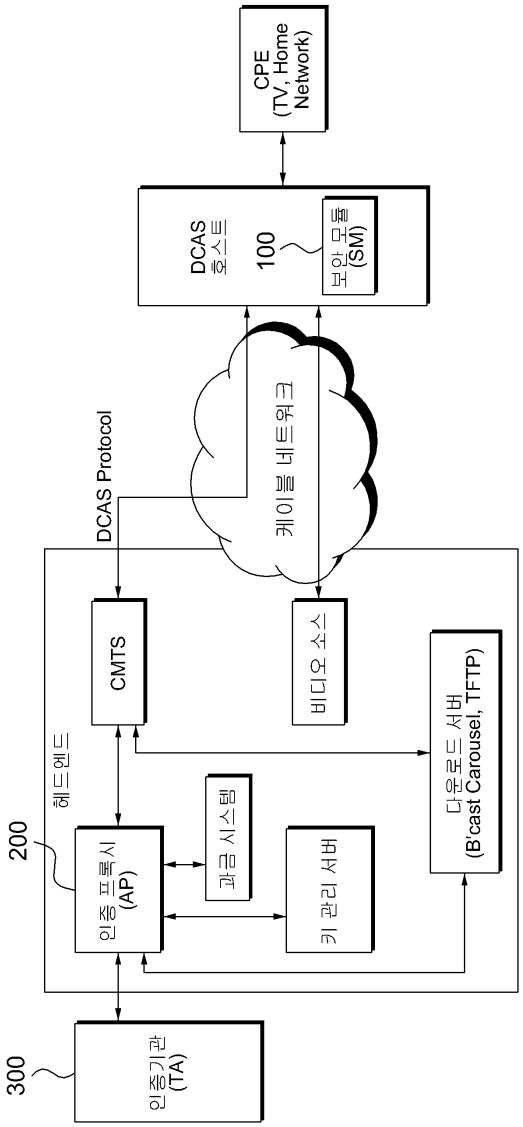
[0088] 도 4는 본 발명의 일실시예에 따른 다운로더블 제한 수신 시스템에서의 상호 인증 방법을 도시한 흐름도이다.

[0089] 도 5는 본 발명의 일실시예에 따른 복호화 및 인증 과정을 도시한 흐름도이다.

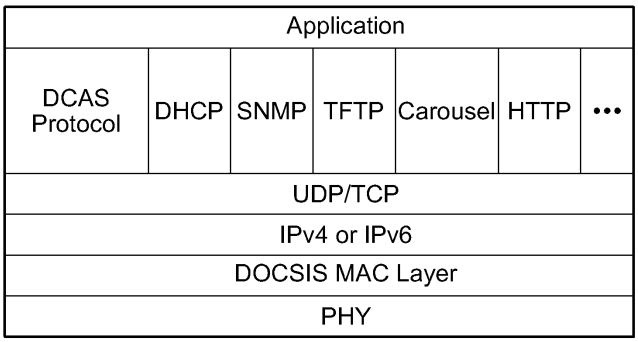
[0090] 도 6은 본 발명의 일실시예에 따른 메시지 암호화 키 및 보안 모듈 이미지 암호화 키 생성 방법을 도시한 흐름도이다.

도면

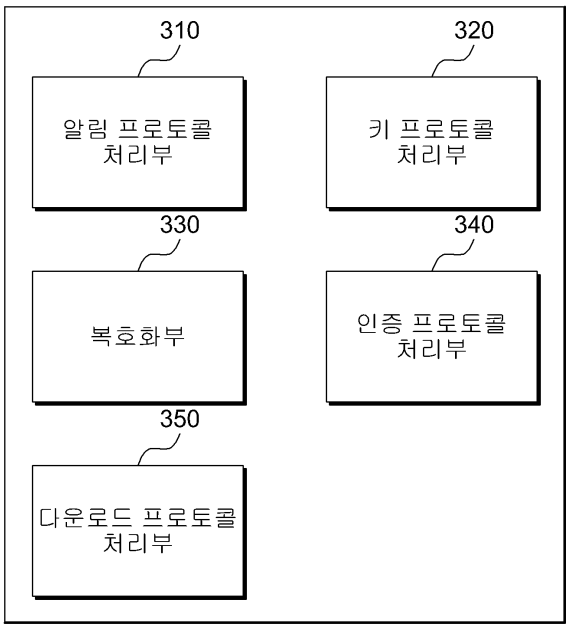
도면1


CPE
(TV, Home Network)
DCAS 호스트
100
보안 모듈 (SM)
케이블 네트워크
DCAS Protocol
CMTS
비디오 소스
다운로드 서버
(B'cast Carousel, TFTP)
헤드엔드
200
인증 프록시 (AP)
과금 시스템
키 관리 서버
300
인증기관 (TA)

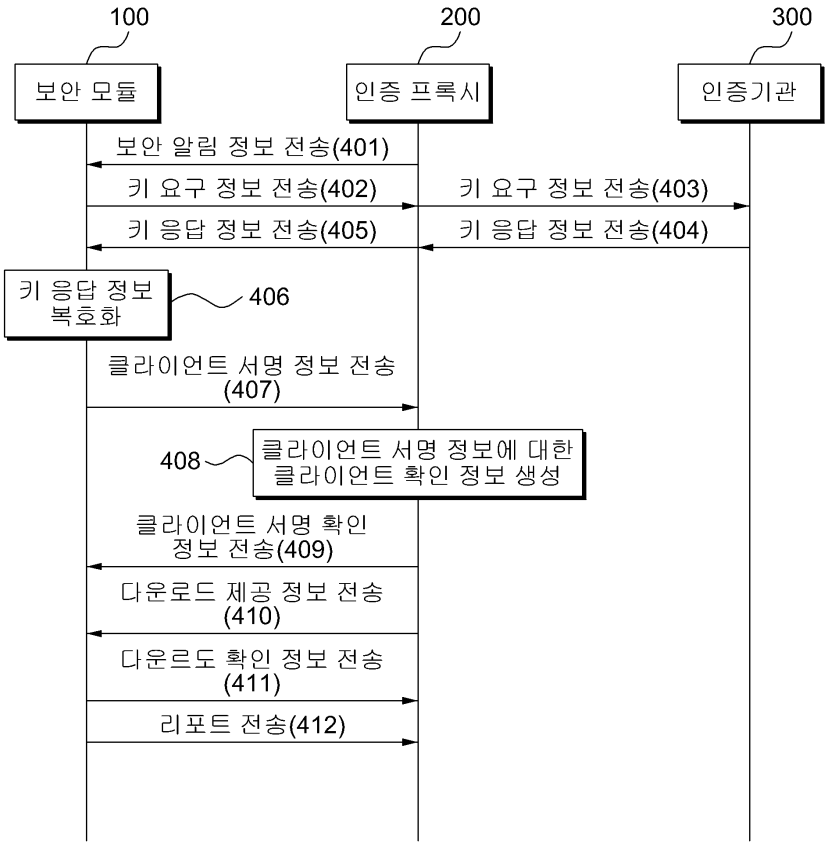
도면2


Application
DCAS Protocol
DHCP
SNMP
TFTP
Carousel
HTTP
•••
UDP/TCP
IPv4 or IPv6
DOCSIS MAC Layer
PHY

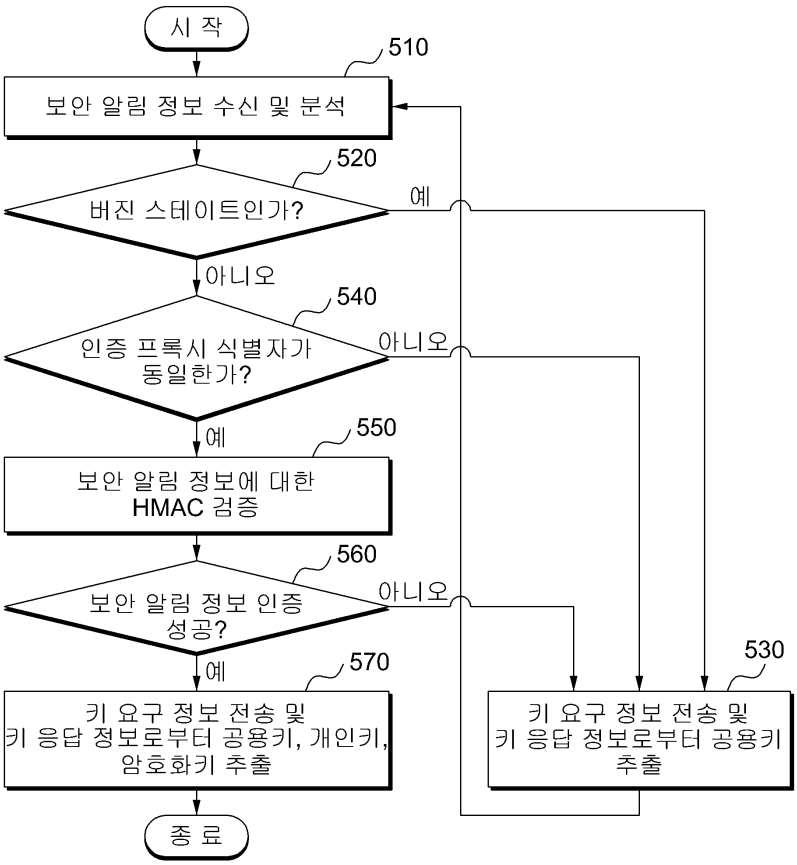
도면3


310
320
알림 프로토콜 처리부
키 프로토콜 처리부
330
340
복호화부
인증 프로토콜 처리부
350
다운로드 프로토콜 처리부

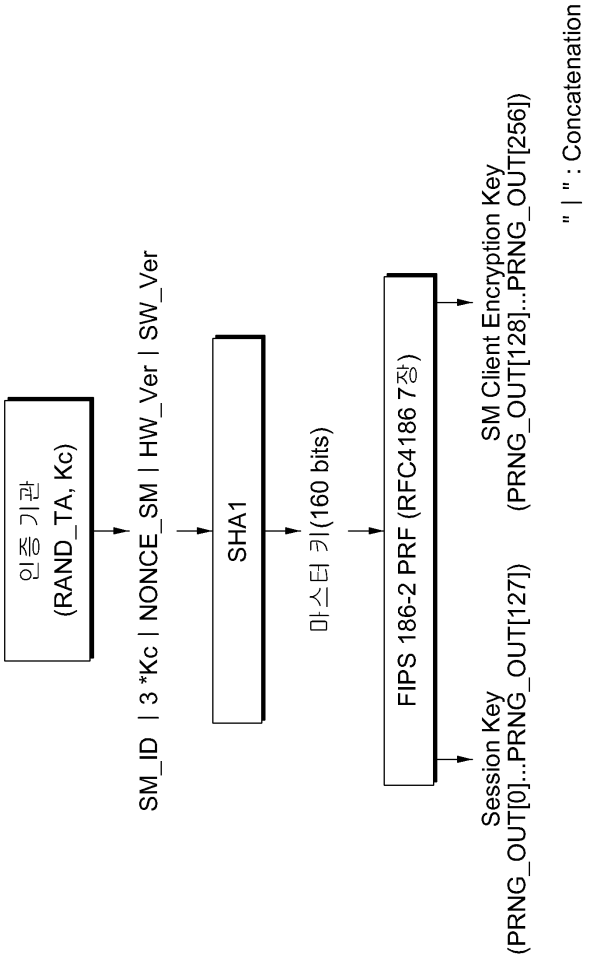
도면4


100
200
300
보안 모듈
인증 프록시
인증기관
보안 알림 정보 전송(401)
키 요구 정보 전송(402)
키 요구 정보 전송(403)
키 응답 정보 전송(405)
키 응답 정보 전송(404)
키 응답 정보 복호화
406
클라이언트 서명 정보 전송 (407)
408
클라이언트 서명 정보에 대한 클라이언트 확인 정보 생성
클라이언트 서명 확인 정보 전송(409)
다운로드 제공 정보 전송 (410)
다운르도 확인 정보 전송 (411)
리포트 전송(412)

도면5


시 작
510
보안 알림 정보 수신 및 분석
520
버진 스테이트인가?
예
아니오
540
인증 프록시 식별자가 동일한가?
아니오
예
550
보안 알림 정보에 대한 HMAC 검증
560
보안 알림 정보 인증 성공?
아니오
예
570
키 요구 정보 전송 및 키 응답 정보로부터 공용키, 개인키, 암호화키 추출
530
키 요구 정보 전송 및 키 응답 정보로부터 공용키 추출
종 료

도면6


인증 기관
(RAND_TA, Kc)
SM_ID | 3 *Kc | NONCE_SM | HW_Ver | SW_Ver
SHA1
마스터 키(160 bits)
FIPS 186-2 PRF (RFC4186 7장)
Session Key
(PRNG_OUT[0]...PRNG_OUT[127])
SM Client Encryption Key
(PRNG_OUT[128]...PRNG_OUT[256])
" | " : Concatenation