韓國컴퓨터情報學會 論文誌
第15卷 第11號, 2010. 11.

2010-15-11-2-1

TTA.KO-07.0079 XCAS 프로토콜 A.1의 CAS 서비스 분리를 통한 CAS Client 개인화 메커니즘

김 영 모*, 장 은 겸**, 최 용 락***

A Mechanism of CAS Client Personalization through separating CAS Service of Protocol A.1 on TTA.KO-07.0079 XCAS

Young-Mo Kim*, Eun-Gyeom Jang**, Yong-Rak Choi***

요 약

CAS Client 개인화는 CAS Client의 식별을 위해서 CAS Client에 CAS ID나 Key를 발급하는 것으로 CAS 운영을 위해 중요한 기술이다. TTA.KO-07.0079 XCAS에서 프로토콜 A.1은 XCAS Server에서 CAS Server 로부터 전달 받은 CAS Client 개인화 데이터를 미리 저장해 놓고, XCAS HOST의 요청에 따라 개인화 데이터를 전송하여 CAS Client 개인화를 수행한다. 하지만, 이러한 방법은 CAS의 서비스 영역을 XCAS에서 수행하게 하여 XCAS Server에 CAS Client 이미지 관리와 네트워크 트래픽을 가중시키는 단점이 있다. 본 논문에서는 TTA XCAS A.1의 이러한 단점을 보완하기 위하여 XCAS Server에서 CAS의 서비스 영역을 분리하고, CAS Client 개인화를 CAS Server에서 이루어지게 하여 XCAS Server의 이미지관리 및 네트워크 트래픽을 분산시켰다.

Abstract

CAS Client personalization means to issue CAS ID or Key for CAS service, which is Core Technology for CAS operation. Protocol A.1 on TTA.KR-07.0079 XCAS, stores CAS Client personalization data from CAS server in XCAS server, and transmits the personalization data by request of XCAS HOST for CAS Client personalization. However, this may increase Network Traffic and CAS Client image management in XCAS server. In this thesis, to complement this, CAS Client personalization is executed on CAS Server by separating CAS service field. Therefore this can distribute Image management and Network Traffic of XCAS server.

• 제1저자 : 김영모 교신저자 : 장은겸
• 투고일 : 2010. 08. 17, 심사일 : 2010. 08. 25, 게재확정일 : 2010. 09. 02.
* 대전대학교 컴퓨터공학과 박사과정 ** 대전대학교 컴퓨터공학과 겸임교수 *** 대전대학교 컴퓨터공학과 교수

▸ Keyword : 제한수신시스템(CAS: Conditional Access System), 다운로드형 제한수신시스템 (Downloadable CAS), XCAS(eXchangeable CAS), CAS 개인화(CAS Personalization)

Ⅰ. 서 론

케이블 방송 및 위성방송 등에 있어서 유료방송의 불법시청을 막기 위한 기술로 CAS(Conditional Access System)와 DCAS(Downloadable CAS)가 있다. 이 기술은 유료방송 서비스에서 사업의 성패를 결정하는 매우 중요한 기술이다[1][2].

CAS 기술은 SMS(Subscriber Management System)와 함께 유료방송 서비스를 위한 필수적인 구성 시스템으로 가입자에게 원하는 프로그램을 제공하고, PPV(Pay Per View) 및 VoD(Video on Demand) 등과 같은 다양한 부가서비스로서 방송 사업자가 방송 콘텐츠에 스크램블(Scramble)을 걸어 케이블, 위성, 지상파, 인터넷, 휴대이동 방송망을 통해 시청자에게 전송하면 CAS Client가 유료 가입자인지, 어떤 서비스에 가입했는지 등을 확인하여 방송 콘텐츠를 디스크램블링(Descrambling)하여 시청하게 하는 기술이다. 이러한 CAS 기술은 방송 사업자에게 무자격자의 불법 시청을 방지할 수 있게 하고, 가입자의 시청 성향 등 마케팅 자료를 제공함과 동시에 타깃 마케팅 등의 다양한 마케팅을 가능하게 하는 효과가 있다[3]. 반면에 DCAS 기술은 네트워크를 통해 가입자의 셋톱박스나 일체형 TV에 하드웨어 형태의 제한수신 모듈을 별도로 두지 않고, 사업자가 소프트웨어 제한수신 모듈을 가입자 단말에 바로 다운로드 시켜 유료케이블방송 서비스를 제공하는 기술로서, 유료방송 서비스 사업자에게 운영상의 유연성을 제공하는 기술이다[4,5]. 국내에서는 TTA에서 XCAS(eXchangeable CAS)[6]로 재명명하여 표준화하였다.

TTA-07.0079 XCAS는 단말에서 제한수신모듈을 분리함으로써 케이블카드와 동일한 단말 표준화의 이점을 갖는 동시에 케이블카드의 관리 비용 절감과 케이블방송 사업자에게 CAS업체에 대한 종속성을 탈피하고, CAS의 결함이 발생하거나 업그레이드가 필요한 경우 즉시 대처할 수 있는 유연성을 확보할 수 있다. 이와 더불어 소비자는 단말 제조업체 간의 가격 경쟁을 통한 다양한 고품질 단말들을 저렴하게 구매할 수 있는 기회를 가질 수 있다[1][6].

CAS Client 개인화는 CAS 사업자가 CAS 서비스를 위하여 가입자별로 각각의 식별자를 부여하는 것을 말하며 기존에는 오프라인환경에서 스마트카드나 CableCARD등에 CAS 사업자가 직접 포팅하여 수행하였지만 XCAS에서는 STB(Set-Top-BOX)의 SM(Secure Module)에 어떤 CAS vender의 Client가 설치될지 모르기 때문에 기존의 경우와 다르게 온라인을 통하여 개인화해야 한다[7]. 그러나 현재, CAS 개인화에 대한 연구는 TTA.KO-07.0079 XCAS A.1 프로토콜의 개인화가 전부이다. XCAS A.1의 문제는 XCAS Server에서 CAS개인화 데이터를 전송하는 것으로, 이는 CAS Server에서 이루어져야 할 이미지 관리와 네트워크 트래픽이 XCAS Server의 이미지 관리 및 네트워크 트래픽에 부하를 가져온다는 것이다.

따라서 본 논문에서는 XCAS A.1의 개인화에 대한 문제점을 보완하는 CAS Client 개인화 프로토콜을 제안한다. 먼저 Ⅱ장에서는 관련연구로 DCAS를 소개하고 XCAS A.1의 문제점을 살펴본다. Ⅲ장에서는 Ⅱ장에서의 문제점을 바탕으로 요구사항을 정의하고, 정의된 요구사항을 바탕으로 XCAS 환경에서 개선된 CAS Client 개인화를 위한 프로토콜을 제안한다. Ⅳ장에서는 제안 프로토콜을 검증하며, Ⅴ장에서는 결론을 서술한다.

Ⅱ. 관련 연구

2.1 DCAS 시스템

북미 MSO(Multiple Service Operator)들로 하여금 네트워크를 통해 제한수신 소프트웨어를 안전하게 다운로드 시킬 수 있게 제안된 DCAS 기술은 STB에 CAS Client가 미리 설치되어 있는 것이 아니라, 서비스 가입자의 STB이 사업자 네트워크 연결시 DCAS Server로부터 CAS Client 이미지를 안전하게 DCAS HOST의 SM에 다운로드하고, 설치한 후 스크램블 된 방송을 디스크램블하여 시청할 수 있도록 하는 기술[8][9]로서, 다운로드 받은 CAS[9], DRM(Digital Rights Management)[10], ASD(Authorized Service Domain)등의 콘텐츠 보호 모듈이 잘 구동되어 서비스 될 수 있도록 지원하는 플랫폼 기술이라 할 수 있다[1][4]. 그림 1은 DCAS 구성도를 보여준다.

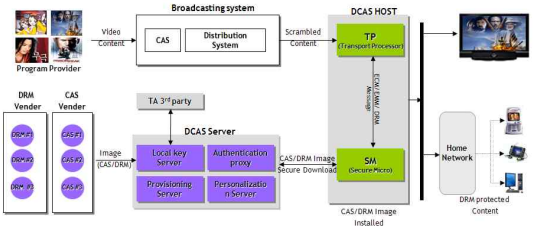

그림 1. DCAS 구성도
Fig. 1. DCAS configuration

DCAS 시스템은 크게 DCAS Server, DCAS HOST 그리고 3rd party에서 SM, TP(Transport Processor) 인증서를 관리하는 TA(Trusts Authority)로 구성될 수 있다. DCAS 서버는 CAS Client 다운로드 프로토콜(Download Protocol) 및 전송 요구사항을 관리하는 AP(Authentication Proxy), TA와 연동하여 키 관리를 수행하는 LKS(Local Key Server), DCAS에서 다운로드 정책과 스케줄을 관리하는 DPS(DCAS Provisioning Server), 이미지 생성 및 이미지를 다운로드 해주는 PS(Personalization Server)로 구성된다. DCAS HOST는 기존의 제한수신 방식들이 동작할 수 있는 호환성을 제공하며, 다수의 제한수신 방식을 지원하기 위한 멀티 디스크램블러 칩(TP)과 CA 어플리케이션의 다운로드 및 구동을 위한 보안 칩(SM) 을 내장한다. TA시스템은 SM, TP 인증서 발행 및 인증서 관리를 수행한다[4].

2.2 TTA.KO-07.0079 XCAS A.1 프로토콜

TTA의 XCAS 송수신정합 표준에서는 교환가능형 제한수신시스템(XCAS: eXchangeable CAS)을 통해 디지털유선방송서비스 제공을 위한 헤드엔드장비, 가입자단말기, 가입자 외부장치 및 제한수신모듈을 대상으로 하며, 케이블네트워크 정합, 가입자단말기와 제한수신 모듈간의 정합 및 가입자 단말기와 외부장치 정합에 관한 규격을 포함한다. 그림 2는 XCAS 송수신 정합표준의 시스템 구조이다[6].

그림 2. 교환가능형 제한수신 시스템 구조
Fig. 2. XCAS Architecture

TA Server는 XCAS 인증을 위한 X.509 인증서를 발급하여 보안모듈 인증에 필요한 정보를 XCAS 헤드엔드에 제공해야 하고, XCAS 헤드엔드 Server는 CAS Client 이미지를 관리하고, 다운로드 및 갱신과 관련된 정보들을 XCAS 인증 Server에 제공해야 한다. 그리고 XCAS 가입자 단말기는 표준의 "부록 A." 에서 정한 프로토콜 중 하나에 따라 XCAS 헤드엔드로부터 CAS Client 이미지를 안전하게 다운로드 받아 설치하고 이를 이용하여 제한수신 서비스를 제공해야 한다. XCAS 표준에서 A.1, A.2, A.3는 CAS Client 이미지 다운로드 프로토콜이다.

보안모듈과 XCAS 헤드엔드 간 보안 프로토콜은 그림 3에서 보는 바와 같이 크게 Announcement 프로토콜, Keying 프로토콜, Authentication 프로토콜 그리고 Download 프로토콜의 4개의 서브 프로토콜로 구성된다. 이때, 프로토콜메시지 처리 주체 중 하나인 TA는 시스템 구성에 따라 XCAS 헤드엔드 내에서 수행됨을 알 수 있다[6].

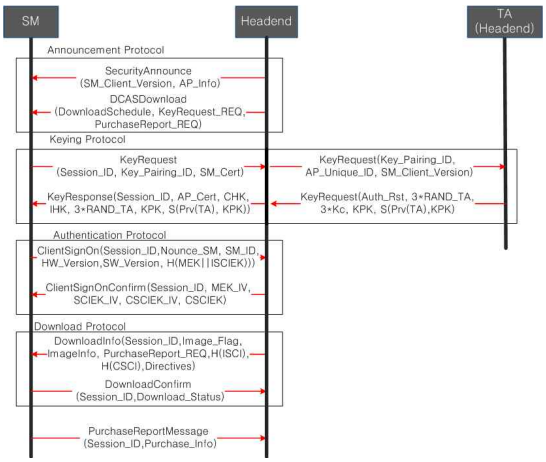

그림 3. 보안모듈과 XCAS 헤드엔드간에 보안 프로토콜
Fig. 3. Secure Protocol of between XCAS headend and Secure Module

특히, Keying 프로토콜, Authentication 프로토콜, 그리고 Download 프로토콜에서는 CAS Client 이미지 다운로드와 CAS Client 개별화와 관련된 프로토콜을 기술하고 있다.

Keying 프로토콜은 "KeyRequest" 및 "KeyResponse" 메시지 처리 단계를 포함한다. "SecurityAnnounce" 메시지를 수신한 보안모듈은 보유한 CHK(Common HMAC Key)를 이용하여 HMAC-SHA1 메시지 인증을 수행한다. XCAS 헤드엔드 Server는 HMAC-SHA1처리에 필요한 CHK, IHK (Individual HMAC Key)를 생성하여 헤드엔드 Server 인증

서와 함께 “KeyResponse” 메시지에 추가한 후, 키 관련 인자에 대해서는 보안 모듈의 공개키로 암호화하고 헤드엔드 Server의 개인키로 서명하여 보안 모듈로 “KeyResponse” 메시지를 전송한다. Authentication 프로토콜은 “ClientSignOn”과 “ClientSignOnConfirm” 메시지 처리 단계를 포함하며, 보안모듈은 “KeyResponse” 메시지에 포함된 키 생성에 필요한 인자 값을 이용하여 메시지 암호화 키 및 Individual 보안 모듈 Client 이미지 암호화 키를 생성한다. 이 암호화키는 XCAS 헤드엔드 Server에서도 생성한다. XCAS 헤드엔드 Server가 생성해 낸 메시지 암호화 키 및 Individual 보안 모듈, Client 이미지 암호화 키가 보안모듈이 생성한 키들과 동일하다면, 헤드엔드 Server는 “ClientSignOnConfirm”메시지를 보안 모듈로 전송한다. 이때 전송되는 “ClientSignOnConfirm”메시지는 IHK를 이용하여 HMAC-SHA1 메시지 인증을 수행하고, AES 알고리즘을 이용하여 암호화한 Common 보안모듈 Client 이미지 암호화키, Individual 보안모듈 Client 이미지 암호화 키 IV(Initial Vector) 그리고 Common 보안모듈 Client 이미지 암호화 키 IV와 암호화 되지 않은 Session_ID, 메시지 암호화 키 IV 값들을 보안 모듈로 전송한다[6].

이처럼 TTA XCAS A.1 프로토콜에서는 XCAS Server를 통하여 Individual 보안모듈 Client 이미지를 전송 하는 것을 CAS Client 개인화방법으로 선택하였다. 이는 두 가지 측면에서 문제점이 발생한다. 첫째는 CAS Server의 CAS Client 이미지 관리를 XCAS Server에서도 관리해야 하는 것으로 CAS Client 이미지를 이중으로 관리해야 하며, 나머지 다른 하나는 이미지 관리 기능과 CAS Server의 개인화에 필요한 트래픽을 XCAS Server에 전가하여 네트워크 트래픽을 증가시키는 문제점이 있다.

III. XCAS 환경에서 CAS Client 개인화 프로토콜

3.1 XCAS 환경에서 CAS Client 개인화 프로토콜 요구사항

XCAS 의 CAS Client 개인화는 기존의 방식과 다르게 특정 CAS vender가 아닌 임의의 다른 CAS vender들도 보안모듈에 CAS Client를 설치 가능해야하기 때문에 기존 방식으로는 불가능하다. 따라서 온라인 기반의 CAS Client 개인화가 필요하며, 현재, 온라인 방식으로 개인화 하는 XCAS A.1의 문제점을 보완한 XCAS 기반의 CAS Client 개인화 요구사항을 도출해보면 다음과 같다.

첫째, XCAS 기반의 방송시스템 환경에서 CAS vender가 바뀌면 CAS 개인키도 변경되어야 한다.

둘째, 온라인 방식으로 CAS Client 개인화가 이루어져야 한다. XCAS 환경에서의 CAS Client 개인화는 특정 CAS vender가 아닌 임의의 CAS vender가 설치 가능해야 하기 때문에 기존방식대로 포팅하여 제공하는 것은 사실상 불가능하다.

셋째, XCAS와 CAS는 서비스에 있어서 상호독립적으로 운영되야 한다. XCAS의 고유서비스는 콘텐츠서비스보호 솔루션을 다운로드 시켜주는 서비스이고, CAS는 유료방송서비스를 가능하게해주는 서비스이기 때문에 서비스간 종속성이 없어야 한다.

넷째, CAS 개인키는 CAS Client 이미지와 분리하여 제공되어야 한다. 개인키는 CAS Server를 통하여 제공받을 수 있지만, 하나의 이미지로 제공받을 경우 XCAS 서버의 이미지 관리 문제와 네트워크 트래픽 증가, 실시간성이 떨어지는 문제점이 있다.

다섯째, CAS Server는 CAS Client가 설치되어있는 HOST 인증을 위하여 XCAS Server와 통신해야 한다. 이는 임의의 불법적인 요청에 대한 방어수단으로, 각각의 vender와 불특정 다수의 요청에 대한 것이다. 인증시 X.509방식을 통하여 상호인증을 수행해야 한다.

여섯째, CAS는 XCAS Server에서 인증한 HOST에 대해서만 인증하고, CAS 개인키를 제공한다. CAS Server는 XCAS Server에서 인증한 HOST에 대해서만 개인키를 내려주고 그렇지 않은 경우는 개인화키를 내려주지 않는다. 또한, 인증서 폐지 목록에 등록해 두어 다음 요청시 XCAS Server에 앞서 미리 차단한다.

3.2 XCAS 환경에서 CAS Client 개인화를 위한 시스템 구성도

본 논문의 XCAS 환경에서 CAS Client 개인화를 위한 시스템 구성도는 그림 4와 같다. 먼저 Head-End구성으로는 CAS Client 개인화를 위한 서비스 가입 여부를 전송해 주는 SMS, CAS ID발급과 CAS 개인화 키를 생성하고 전송하기 위한 A vender의 CAS Server와 B vender의 CAS Server 그리고 CAS Client 이미지를 전송해 주는 XCAS Sever로 구성된다.

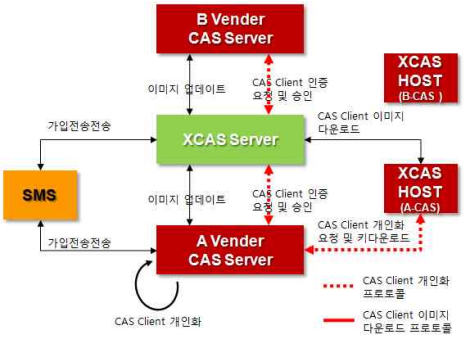

그림 4. XCAS환경에서의 CAS Client 개인화를 위한 시스템 구성도
Fig. 4. Configuration of system for CAS Client Personalization based on XCAS

단말에는 XCAS 서버로부터 CAS Client 이미지를 다운로드 하고, 이를 설치하고, 로딩하여 CAS 서비스를 하는 SM과 TP가 구성된다. 이렇게 구성된 헤드엔드와 단말간에는 CAS Client 이미지를 다운로드하는 프로토콜과 CAS Client를 개인화하는 프로토콜로 구성되며, 초기 CAS Client 이미지 다운로드 이후에만 CAS Client 개인화를 수행하고, 업데이트시에는 CAS Client 개인화를 수행하지 않는다.

3.3 CAS Client 개인화 프로토콜

XCAS환경에서 CAS 개인화를 위한 제안 프로토콜은 크게 2가지로 나뉜다. 첫째는 CAS Client 다운로드 프로토콜이고, 다른 하나는 CAS Sever와 SM 모듈간의 CAS 개인화 프로토콜이다. 본 논문에서는 첫 번째 프로토콜을 TTA XCAS A.3의 초기 이미지 다운로드 프로토콜과 업데이트 이미지 다운로드 프로토콜을 이용한다. 이는 A.3 프로토콜이 CAS Client 이미지 다운로드로 한정되기 때문에 본 논문 3.1절의 요구사항을 만족하기 때문이다.

3.3.1 초기 이미지 다운로드 프로토콜

초기 상태의 보안모듈, MSO 이동, SO 이동 시에도 초기 다운로드 프로토콜을 수행하게 된다. 또한 해지 된 단말기가 다른 시청자에게 재사용이 될 경우에도 초기 다운로드 프로토콜이 수행 될 수 있다[6].

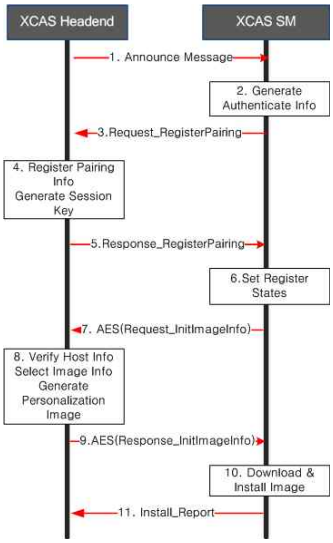

그림 5. 초기 다운로드 프로토콜
Fig. 5. Initial download protocol

부팅 후 초기 상태를 확인 한 보안모듈은 SM_ID와 TP_ID를 이용하여 Pairing 정보를 Server에 등록요청을 한다. 이때 SM_ID와 TP_ID를 서명한 정보를 함께 보내 XCAS 헤드엔드가 해당 보안모듈의 인증을 수행할 수 있도록 한다. 보안모듈의 등록이 완료되면 XCAS 헤드엔드는 이미지 다운로드 메시지 전달에 사용할 세션키를 생성하여 함께 전송을 하며, 또한 다운로드 이미지 인증을 위해 SO 인증서를 함께 전송 한다. 보안 모듈 등록이 완료되면 보안 모듈은 동일한 세션에서 다운로드 할 초기 이미지 정보를 Server에 다시 요청한다. 이때부터는 XCAS 헤드엔드로 부터 전달받은 세션키를 사용하여 메시지의 본문을 AES 암호화를 한다.

XCAS Server는 보안모듈의 정보와 다운로드 정책에 의하여 다운로드 될 이미지 정보를 결정하고, 이미지 정보와 이미지 암호화 키를 보안모듈의 공개키로 RSA 암호화하여 전달한다. 이미지 정보를 전달받은 보안 모듈은 이미지 다운로드 및 설치를 시도하게 되고, 이미지 설치가 성공적으로 완료되면 설치 정보를 다시 Server에게 통보한다.

3.3.2 업데이트 다운로드 프로토콜

이미지 설치가 완료되어 사용 중인 단말기 보안 모듈은 Server로부터 전달되는 "Announce 메시지 (AM)"에 의해서 이미지의 업데이트 또는 변경이 가능하다[6].

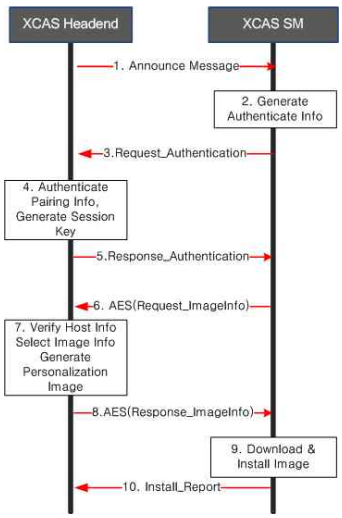

그림 6. 업데이트 다운로드 프로토콜
Fig. 6. Update download protocol

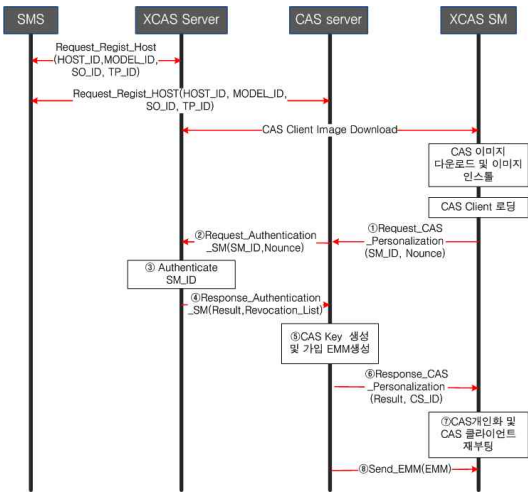

그림 7. XCAS 환경에서 CAS Client 개인화 프로토콜
Fig. 7. CAS Client Personalization based on XCAS

이 프로토콜에 의해서 다운로드 되는 이미지는 단순 업데이트 이미지가 될 수도 있으며, 경우에 따라서는 초기 다운로드 이미지가 될 수도 있다. 이는 전적으로 단말기의 상태에 따른 다운로드 정책에 의해서 결정이 된다. 업데이트 이미지 다운로드 프로토콜은 기본적으로 초기 다운로드 프로토콜과 크게 다른점은 없으며, 단지 처음에 SM-TP 페어링 정보를 등록하는 대신에 확인 및 인증만 하는 것이 다르다. 즉, AM에서 업데이트 정보를 확인 한 SM은 SM_ID와 TP_ID를 이용하여 Server에게 인증을 요청 한다. SM에 대한 인증이 완료되면 XCAS 헤드엔드는 이미지 다운로드 메시지에 사용한 세션키를 생성하여 함께 전송을 한다. SM 인증이 완료되면, SM은 동일한 세션에서 이미지 정보를 Server에 다시 요청한다. 이때부터는 XCAS 헤드엔드로부터 전달받은 세션키를 사용하여 메시지의 본문을 AES로 암호화를 한다. Server는 SM의 정보와 다운로드 정책에 의하여 다운로드 될 이미지 정보를 결정하고, 이미지 정보와 이미지 암호화 키를 SM의 공개키로 RSA 암호화하여 전달한다. 이미지 정보를 전달받은 SM은 이미지 다운로드 및 설치를 시도하게 되고, 이미지 설치가 성공적으로 완료되면 설치 정보를 다시 Server에게 통보한다.

3.3.3 XCAS를 위한 CAS Client 개인화 프로토콜

보안모듈이 CAS Client를 다운로드하고 설치한 이후 로딩된 CAS Client는 유료방송서비스를 위하여 CAS Client 개별화를 해야 하며, 이를 위한 제안 프로토콜은 그림 7과 같다.

① Request_CAS_Peraonalization(SM_ID, Nounce): SM_ID는 SM을 식별할 수 있는 ID로 SM에 포팅된 인증서 식별자이다. TTA XCAS 표준에 의하면, 16byte를 사용한다. Nounce는 CAS Server와 XCAS HOST간 보안통신을 위하여 난수이다.

② Request_Authencation_SM(SM_ID, Nounce): 메시지에서 Nounce는 XCAS Server와 CAS Server간의 보안통신을 위하여 난수이다.

③ Authenticating SM: XCAS Server는 SM_ID를 기반으로 하여 SM을 인증을 수행한다.

④ Response_Authencation_SM(Result, Revocation_List): Result는 인증에 대한 결과 값이고, Revocation_List는 인증에 실패한 SM 인증서의 목록들이다.

⑤ Generating CAS Key, Subcriber EMM: CAS Server는 인증이 수행된 CAS Client에게 CAS 개인화 키와 서비스 가입을 위한 가입 EMM을 생성해야 하며, CAS key 필드와 EMM 필드는 key 길이와 EMM 형식이 업체마다 다른기 때문에 가변길이로 설정해야 한다.

⑥ Response_CAS_Peraonalization(Result, CS_ID): Result는 개인화에 대한결과 값이고, CS_ID는 개인화에 성공하였을 경우 CAS 서버에서 발급하는 CAS ID이다.

⑦ Rebooting CAS Client: CAS ID를 발급받으면 CAS Client는 리부팅을 요청하고 EMM(Entitlement Management Message)을 수신대기 모드로 전환한다.

⑧ Send_EMM: Server에서는 브로드케스팅으로 EMM을 전송한다.

SMS는 콜센터나 고객의 요청에 의하여 가입신청요청을 XCAS Server나 CAS Server에 호스트 정보등록을 통하여 전달한다. XCAS Server와 CAS Server는 전달된 내용을 등록하고 가입자 STB에서 이미지 전송 요청과 CAS 서비스 요청이 왔을 때 제안프로토콜에 의하여 이미지를 내려주고, CAS를 개별화한다. 이후, 관련 상품 EMM을 전송하여 가입자 Server가 유료방송서비스를 시청할 수 있게 한다.

IV. 제안프로토콜의 평가

4.1 요구사항 만족도 평가

3.1절의 요구사항에 대한 제안프로토콜의 만족도를 확인하면 "XCAS 환경에서 CAS vender가 바뀌면 CAS 개인키도 변경되어야 한다."와 "XCAS 환경에서는 온라인 방식으로 CAS Client 개인화가 이루어져야한다."의 요구사항을 본 논문에서는 온라인 방식으로 CAS Client 개인화를 수행하는 제안 프로토콜에 의하여 만족한다. 또한, "상호 시스템간의 서비스에 영향을 미치지 않기 위하여 독립적인 운영이 보장", "HOST에 이미지 제공시 CAS 이미지를 분리하여 제공" 요구사항에 대해서는 제안프로토콜에서 CAS의 공통이미지는 XCAS Server에서 전송하고, CAS Client 개인화를 CAS Server에서 이루어지게 하여 이 또한 만족한다. "CAS Server는 CAS Client가 탑재되어 구동될 HOST의 인증을 위하여 XCAS Server와 안전하게 통신해야 한다"는 요구사항도 만족하며 "CAS는 XCAS Server에서 인증한 HOST에 대해서만 키를 전달해야한다"라는 요구사항도 제안프로토콜에 의하여 만족하는 것을 확인할 수 있다.

4.2 제안프로토콜과 XCAS A.1과의 비교 평가

본 절에서는 본 논문에서 제안하는 프로토콜과 XCAS A.1에서 제안하는 프로토콜을 다음과 같은 2개의 시나리오에 의하여 이미지 관리와 네트워크 트래픽에 대한 비교 평가를 한다. 제안 프로토콜을 위한 시스템 구조에 의하면, XCAS에서 m개의 CAS vender가 제공하는 공통이미지를 다운로드 해주는 경우, m은 CAS vender의 수를 나타내며, k는 업데이트 되는 이미지로 공통이미지를 나타낸다.

먼저, XCAS Server에서 관리하는 공통이미지 개수는 식(1)과 같으며, 관리하는 용량은 식(2)와 같이 나타낼 수 있다. m은 CAS Vender수를 나타내며, I는 초기 등록되는 이미지수, k는 업데이트 되는 이미지 수, v는 이미지 크기를 나타낸다.

$$m(I+k) \quad \cdots\cdots (1)$$

$$\sum_{i=1}^{m}(I+k)\times v_i \quad \cdots\cdots (2)$$

CAS Server에서 관리하는 공통이미지와 개인화데이터를 포함한 이미지 수는 식(3)과 같으며, 식(3)에서 I와 k는 보안사고와 같은 특정한 사건이 발생하지 않는 한 증가하지 아니하며, 개인화 데이터를 포함한 이미지 수는 가입자 n만큼 증가한다. 전체 이미지 용량은 다음 식(4)와 같이 공통이미지에 대한 v와 개인화 데이터 이미지 용량을 곱하여 나타낼 수 있다. I는 초기 등록되는 이미지 수이고, k는 업데이트 되는 수, v는 이미지 크기를 나타낸다. n은 가입자 수이고, ts는 전체 가입자 수이다. p는 개인화데이터이미지 용량이다.

$$(I+k)+\sum_{n=1}^{ts}n-\sum_{n=1}^{ts-1}n \quad \cdots\cdots (3)$$

$$v(1+k)+\sum_{n=1}^{ts}n\times p-\sum_{n=1}^{ts-1}n\times p \quad \cdots\cdots (4)$$

네트워크 트래픽에 대해서는 다음과 같은 트래픽을 예상할 수 있다. "CAS Server가 보안사고 및 보안정책으로 인하여 Client 이미지를 업데이트한다."와 신규가입자는 일정하게 정해져 있다."고 가정하면, XCAS Server에 발생하는 네트워크 트래픽은 다음과 같은 식(5),(6),(7)로 나타낼 수 있다. 네트워크 트래픽은 이미지 다운로드시에 생기는 트래픽과 일반적인 메시지 통신을 할 때 생기는 트래픽으로 나눌 수 있다. 본 논문에서는 P를 메시지 통신시 생기는 트래픽이라 가정한다.

신규가입자에 대한 네트워크 트래픽은 식(5)와 같으며, N은 신규가입자 수이다. $(\sum_{i=1}^{m}(I+k))\times v_i$는 신규가입자가 초기 이미지 다운로드시 발생하는 공통이미지에 대한 트래픽이고, 여기에 메시지 통신시 발생하는 P를 더하면 가입자 1명당 발생하는 트래픽이 된다.

$$N\times((\sum_{i=1}^{m}(I+k))\times v_i+p) \quad \cdots\cdots (5)$$

기존 가입자들에 대한 트래픽은 식(6)과 같으며, 여기서 ct는 전체 가입자 수이다. 기존가입자들의 경우는 이미지 업데이트시 일어나며 공통이미지에 발생하는 네트워크 값과 이미지 업데이트시에 발생하는 P를 더한 값에 가입자 수를 곱하여 구할 수 있다.

$$\sum_{n=1}^{ts} n(v+P) - \sum_{n=1}^{ts-1} n(v+P) \quad \cdots\cdots (6)$$

따라서 어떤 특정한 날에 XCAS Server 네트워크트래픽은 식(7)과 같이 나타낼 수 있다. 이는 식(5)와 식(6)에 각 CAS Vender별 이미지 용량 크기 vi, Pi을 대입하여 구할 수 있다.

$$N(\sum_{i=1}^{m}(I+k)\times v_i + P_i) + \sum_{n=1}^{ts} n \times \sum_{i=1}^{m}(v_i + P_i) - \sum_{v=1}^{ts-1} n \times \sum_{i=1}^{m}(v_i + P_i)$$

$$\cdots\cdots (7)$$

그리고 개인화에 따른 CAS Server의 트래픽은 식(8)과 같다. CAS Client 개인화는 신규회원의 가입에 따라 이루어진다. TN은 하루에 가입하는 신규 회원의 총수이다. 개인화 이미지 데이터 용량과 메시지 통신시 발생하는 P에 신규가입자 수를 곱하여 구할 수 있다.

$$\sum_{N=1}^{TN} N(p+P) - \sum_{N=1}^{TN-1} N(p+P) \quad \cdots\cdots (8)$$

따라서 시나리오 1.과 시나리오 2에 도출된 식을 적용하여 제안프로토콜과 XCAS A.1의 이미지관리와 네트워크트래픽에 대한 비교 평가를 한다.

- ***시나리오1.*** *SO는 10명의 가입자를 보유하고 있으며, 1개의 CAS 시스템을 운영한다. 하루 평균 가입자는 2명이라고 가정한다. i는 초기 등록된 이미지 개수로 1이지만, XCAS 서버는 보안정책에 의하여 가입자 50명 증가시마다 공통이미지 업데이트를 한다. 공통이미지 용량 v는 500kb이며, p는 500kb이다. 이미지 다운로드시에 필요한 프로세스 트래픽 P는 100kbps이다. 개인화시 필요한 트래픽은 300kbps이다.*
- ***시나리오2.*** *SO는 5명의 가입자를 보유하고 있으며, 2개의 CAS 시스템을 운영한다. 하루 평균 신규가입자는 2명이고, 1명은 A CAS vender 이고, 1명은 B CAS vender이다. 초기 등록된 이미지 개수로 1이다. XCAS 서버는 보안정책에 의하여 각 vender별로 가입자가 50명 증가시 마다 공통이미지를 업데이트 한다. A vender의 공통이미지 용량 v는 500kb이며, p는 500kb이다. 또한, 이미지 다운로드시와 개인화시에 필요한 프로세스 트래픽 P는 100kbps이다. B vender의 공통이미지 용량 v는 700kb이며, p는 600kb이다. B vender에 대한 이미지 다운로드시 필요한 트래픽과 개인화시에 필요한 트래픽 P는 100kbps이다.*

시나리오1.의 이미지 관리와 네트워크 트래픽은 다음과 같다. 이미지 관리 부분에 있어서, 제안프로토콜의 경우 식(1)과 (2)에 의하여 계산할 수 있으며 XCAS A.1의 경우는 XCAS Server에서 CAS Server의 이미지 관리를 똑같이 수행해야 하기 때문에 식(3),(4)와 같이 계산할 수 있다. 그림 8은 시나리오 1.에 따른 XCAS Server에서 관리해야 하는 이미지 수를 나타낸다.

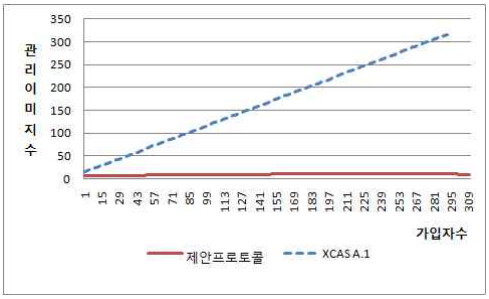

그림 8. 제안프로토콜과 XCAS A.1의 XCAS Server에서 관리하는 이미지 수 비교
Fig. 8. Image count Comparison for managing Proposed Protocol and XCAS A.1

제안프로토콜은 이미지 관리수가 가입자 수와 상관없이 일정하지만, XCAS A.1의 경우는 가입자 수에 따라 늘어나는 것을 확인할 수 있다. 네트워크 트래픽부분에 있어서, 제안프로토콜의 경우 식(7)에 의하여 계산할 수 있으며, XCAS A.1의 경우는 XCAS Server의 트래픽에 CAS Server의 CAS Client 개인화시의 네트워크 트래픽을 더하면 전체 네트워크 트래픽을 계산할 수 있다. 그림9는 시나리오 1.에 따라 서비스 운영날짜별 네트워크 트래픽을 나타낸 것으로, 보안정책에 의해 가입자가 50명 늘어날 때, 업데이트로 인한 트래픽이 증가하는 것을 확인할 수 있고, 제안프로토콜이 XCAS A.1 보다 네트워크 트래픽이 신규가입자 수만큼의 트래픽이 적음을 확인할 수 있다.

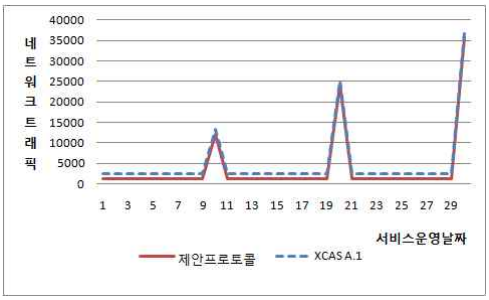

그림 9. XCAS Server에서 발생하는 네트워크 트래픽 비교
Fig. 9. Network Traffic Comparison of XCAS Server

시나리오2.의 이미지 관리와 네트워크 트래픽은 다음과 같다. 이미지 관리 부분에 있어서, 제안 프로토콜의 경우 식(1)과 식(2)에 의하여 계산할 수 있으며, XCAS A.1의 경우는 XCAS Server에서 CAS Server의 이미지 관리를 똑같이 수행해야 하기 때문에 식(3), 식(4)와 같이 계산할 수 있다. 그림 10은 시나리오 2.에 따른 제안프로토콜과 XCAS A.1의 XCAS Server에서 관리해야 하는 이미지 수이다.

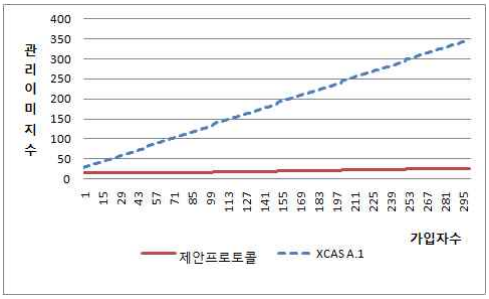

그림 10. 제안프로토콜과 XCAS A.1의 XCAS Server에서 관리하는 이미지 수 비교
Fig. 10. Image count Comparison for managing Proposed Protocol and XCAS A.1

제안프로토콜이 이미지 관리수가 일정한 반면, XCAS A.1의 경우 가입자 수에 따라 늘어나는 것을 확인할 수 있으며, CAS Vender의 수에 따라 제안프로토콜과 XCAS A.1의 이미지 관리수가 배수로 늘어나는 것을 확인할 수 있었다.

네트워크 트래픽부분에 있어서, 제안 프로토콜의 경우 식(7)에 의하여 계산할 수 있으며, TTA의 경우는 XCAS Server의 트래픽에 각 CAS vender Server의 CAS Client 개인화시 트래픽을 더하면 트래픽을 계산할 수 있다. 그림 11은 시나리오 2.에 따른 네트워크 트래픽을 나타낸 것으로, 제안프로토콜이 XCAS A.1 보다. 네트워크 트래픽이 신규가입자와 CAS vender의 이미지 용량에 따른 계산량 만큼 적음을 확인할 수 있다.

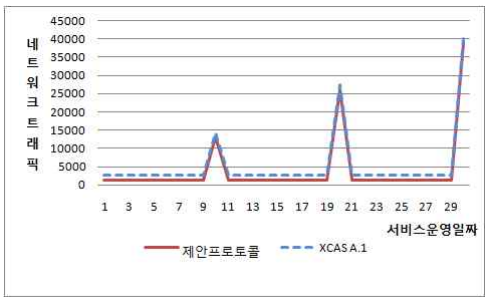

그림 11. XCAS Server에서 발생하는 네트워크 트래픽 비교
Fig. 11. Network Traffic Comparison of XCAS Server

따라서, 시나리오 1.과 시나리오 2.에 따른 검증을 통하여 제한프로토콜을 사용하면, XCAS Server의 이미지 관리에 있어서 이미지 관리 대상 개수 및 용량이 줄어들며, XCAS Sever의 네트워크의 트래픽을 CAS Server에서 분산하기 때문에 XCAS A.1보다 네트워크 트래픽이 줄어드는 효과를 얻었다.

V. 결론

지금까지 최근 디지털 방송기술 분야에서 관심사항이 되고 있는 TTA.KO-07.0079 XCAS 기술에 대하여 살펴보았으며, XCAS 기술에 있어서 CAS 서비스를 위한 CAS Client 개인화 기술이 중요하지만, 지금까지 연구가 미흡하며, 현재 XCAS A.1에서 CAS Client 이미지 다운로드 시에 개인화 데이터를 전송하는 개인화 방법이 XCAS Server의 네트워크 트래픽과 이미지 관리의 문제점이 있음을 확인하였다. 또한, XCAS A.1의 문제점을 바탕으로 XCAS CAS Client 개인화 요구사항을 정의하였고, 이를 바탕으로 XCAS를 위한 CAS Client 개인화를 위한 시스템 구성과 프로토콜을 제안하였다. 본 논문의 프로토콜의 검증을 위하여 정의된 요구사항을 바탕으로 요구사항 만족도와 수식을 통하여 주어진 시나리오를 검증하였다. 검증결과 네트워크 트래픽과 이미지 관리부분에 있어서, 제안하는 방법이 XCAS A.1보다 우수한 것을 확인 할 수 있었으나, 네트워크 트래픽과 관련하여 서버시스템과 네트워크 상의 여러 고려사항을 반영하지 못한 아쉬움이 있다. 향후 XCAS 기술과 IPTV의 CAS 기술에서도 제안된 CAS 개인화방법이 상용화와 서비스 확대를 위해서 필요할 것이며, 기술의 이를 위해서 완전성 및 안정성이 보장되어야 할 것이다.

참고문헌

[1] 김영모,“다운로드형 제한수신 시스템 기술 동향,” 방송공학회, 제 13권, 제 14호, 1-10쪽, 2008년 12월.

[2] EBU Project Group B/CA, "Functional Model of a Conditional Access System," EBU Technical Review Winter, 1995.

[3] 정서현, “Open IPTV 환경에서 재암호화 과정 없는 댁내 컨텐츠 분배를 위한 키관리 기법,” 한국컴퓨터정보학회논문지, 제 15권, 제 7호, 57~66쪽, 2008년 1월.

[4] Cable Television Laboratories, Inc., “DCAS System Overview Technical Report,” OC-TR-DCAS-D02-060912, September 2006.

[5] 정영호, “다운로더블 제한수신 시스템 기술,” 전자공학회, 제 35권, 제 292호, 15-24쪽, 2008년 9월.
[6] 한국정보통신기술협회,“교환가능형 제한수신시스템송수신 정합표준,“ TTAK.KO-07.0079, 2010년 6월.
[7] 대한민국특허청, “다운로드 기반의 수신제한 시스템에서 카스 Client의 개인화 방법,” KR 10-0886901, 2009년 3월.
[8] “NGNA Plan: Integrated Multimedia Architecture,” NGNA LLC, July 2004.
[9] US FCC, “CS Docket No. 97-80: Report of the National Cable & Telecommunications Association on Downloadable Security”
[10] 박종현, “디지털 방송을 위한 Set-Top Box기반 TV-Anytime 메타데이터 관리 시스템,” 한국컴퓨터정보학회논문지, 제 13권, 제 4호, 71-78 쪽, 2008년 10월.

저 자 소 개

김 영 모

2005 : 대전대학교 공학석사
1996-현재 : 대전대학교 컴퓨터공학과 박사과정
관심분야 : 컴퓨터 포렌식스, CAS, DRM, e-Learninig

장 은 겸

2007 : 대전대학교 공학박사
2008-현재 : (주)엠투엠코리아 부설 기술연구소장
2009-현재 : 대전대학교 컴퓨터공학과 겸임교수
관심분야 : DRM, 컴퓨터 포렌식스, 스마트 그리드, 모바일 보안

최 용 락

1982-1986 : 한국전자통신연구원 선임연구원
1986-현재 : 대전대학교 컴퓨터공학부 교수
1997-1999 : 한국정보보호학회 충청지부 지부장
학회활동 : 한국통신정보보호학회, 한국정보과학회, 한국정보처리학회, 한국인터넷정보학회 종신회원
관심분야 : 컴퓨터통신보안