Journal of Korea Multimedia Society Vol. 13, No. 2, February 2010(pp. 249-257)

SDCS: 유비쿼터스 환경의 안전한 콘텐츠 다운로드를 위한 안전한 D-CAS 시스템

여 상 수†

요 약

유비쿼터스 환경이 도래됨에 따라 IT 기술이 진보하고 있으며, 초고속 인터넷 보급으로 인한 다양한 콘텐츠가 생성 및 전파되고 있다. 콘텐츠란 인터넷이나 컴퓨터 통신망에서 사용하기 위하여 문자, 부호, 음성, 음향, 클라이언트, 영상 등을 디지털 방식으로 제작하여 처리 및 유통하는 각종 정보 또는 그 내용물을 통틀어 이르는 개념이다. 이러한 콘텐츠는 통신망을 통하여 공유되며 이로 인해 사용자 지식의 폭을 넓히고 표현의 자유를 얻을 수 있다. 이러한 이유로 사용자 참여가 점차 증대되고는 있지만 최근 저작권자의 동의 없이 무분별하게 콘텐츠가 유포되고 있어 콘텐츠 제작 과정에서 많은 문제점이 발생하고 있다. 이를 해결하기 위하여 콘텐츠 사용을 정당한 사용자로 제한하고, 콘텐츠 보호 및 안전한 다운로드를 제공하기 위한 많은 연구가 진행되고 있다. 따라서 본 논문에서는 콘텐츠를 다운로드 시 안전하게 다운로드 받을 수 있는 시스템(SDCS : Secure D-CAS System)을 제안하고자 한다.

SDCS: Secure D-CAS System for Secure Contents Download in Ubiquitous Environment

Sang-Soo Yeo†

ABSTRACT

The emerging ubiquitous environment is improving IT technologies and the popularization of broad-band Internet is encouraging creation and sharing of various contents. The contents include the concept of production and circulation of digital information/contents, in forms of characters, codes, voices, sounds, client and videos for being used on the Internet and networks. The contents are widely shared in networks and users can have a wide range of knowledge and gain the freedom of presentation from them. So now users' participations are augmented gradually. However, many contents without acquiring agree of copyright are sharing on the Internet, so many problems happen in the manufacturing process of digital contents. To solve this problem, many research projects to limit contents utilization onto legitimate users and to provide secure contents protection and download, are in progress. Therefore, in this paper, we propose a secure D-CAS system (SDCS) which provides security for contents downloading.

Key words: DRM(디지털저작권관리), Contents Protection(콘텐츠 보호), Secure Contents Download(안전한 콘텐츠 다운로드)

※ 교신저자(Corresponding Author) : 여상수, 주소 : 대전시 서구 도안동(302-318), 전화 : 042)829-7636, FAX : 042)822-8431, E-mail : ssyeo@msn.com
접수일 : 2009년 7월 21일, 수정일 : 2009년 10월 20일
완료일 : 2009년 10월 26일
† 정회원, 목원대학교 컴퓨터공학부 전임강사
※ 이 논문은 2009년 목원대학교 신임교원 정착연구 지원사업에 의하여 연구되었음.

1. 서 론

'유비쿼터스'란 '언제, 어디서나'라는 뜻의 라틴어에서 유래된 말로, 복사기 제조회사인 제록스의 '마크와이저'에 의하여 처음 사용되었다. 유비쿼터스 환경은 상황이 사용자를 인식하고 장소와 시간을 초월하여 서비스를 제공하는 환경을 의미한다. 마크와이저는 유비쿼터스 컴퓨팅을 메인프레임과 퍼스널컴퓨터에 이어 제 4의 정보혁명을 이끌 것이라고 주장하였고, 컴퓨터들이 단독으로 사용되지 않고 유비쿼터스 통신, 유비쿼터스 네트워크 등과 같은 형태의 컴퓨팅 네트워크 환경을 구축할 것이라 주장했다. 즉, 컴퓨터에 어떠한 기능을 추가하는 것이 아니라 자동차, 냉장고, 안경, 시계 등과 같이 사용자 주변에서 쉽게 볼 수 있는 사물에 컴퓨터를 접목하여 통신이 가능하도록 구축하는 정보기술 패러다임을 뜻하는 것이다. 이러한 유비쿼터스 환경에서는 사용자의 정보뿐만 아니라 서비스를 제공하기 위한 다양한 정보들이 사용되며, 신속한 서비스를 위하여 초고속 네트워크망이 구축되어 사용되고 있다. 초고속 네트워크망은 정보 전달의 속도가 빠른 망으로, 유비쿼터스 환경에서 사용하고 있는 이동성을 제공하는 디바이스 간에는 무선 통신망을 통해서도 정보들이 전달된다. 인터넷의 속도를 빠르게 하고, 이러한 초고속 인터넷의 보급은 초고속 네트워크망을 형성하는데 기반이 되고 있으며, 디지털 방송 시스템의 발전으로 인하여 다양한 콘텐츠가 개발되고 있다. 개발된 다양한 콘텐츠들은 초고속 네트워크망을 통하여 빠른 속도로 전파되어 사용자들에게 유용하게 사용되고 있다. 하지만 콘텐츠들이 저작권자의 동의 없이 무분별하게 유포되어 이를 해결하기 위한 연구가 진행되고 있다. 콘텐츠 보안과 관련된 기술로 DRM(Digital Rights Management: 디지털저작권관리) 기술과 CAS(Conditional Access System: 수신제한시스템) 기술이 있으며, 이 기술들을 이용하여 콘텐츠를 암호화하고 정당한 사용자만이 콘텐츠를 획득할 수 있도록 하고 있다. 특히 CAS에서는 STB(Set Top Box)에 케이블 카드(Cable Card)를 삽입하여 수신 제한 서비스를 제공하고 있으나, 키가 노출될 경우 시스템을 교체해야하므로 비용이 증가하고, 특정 업체의 STB에 종속되어 사용해야하는 단점이 존재한다. 따라서 본 논문에서는 안전하게 콘텐츠를 다운로드하여 사용하는 콘텐츠 보호 시스템(SDCS : Secure D-CAS System)과 그 접속 방법을 제안하고자 한다. 2장에서는 관련 기술에 관하여 서술하고, 3장에서는 유비쿼터스 환경과 디지털 콘텐츠에 관하여 설명한다. 4장에서는 제안 시스템에 관하여 설명하고, 마지막으로 5장에서 결론을 맺도록 한다.

2. 유비쿼터스 환경과 디지털 콘텐츠

유비쿼터스란 정보혁명에 이어 큰 혁명으로 불리고 있으며, 우리 사회를 변화시키는 하나의 물결이라고 할 수 있다. 미국 제록스사의 마크와이저는 처음으로 유비쿼터스라는 용어를 사용하였으며, 마크와이저가 바라보는 유비쿼터스 환경은 사용자가 네트워크나 컴퓨터를 의식하지 않고 시간 및 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경이다. 초기에는 단순히 네트워크망을 구성하여 모든 환경에 컴퓨팅 환경이 편재되어 있는 것을 의미하였으나, IT 기술의 발전의 가속화로 모바일 컴퓨팅 개념이 추가되어 이동하면서도 서비스를 제공받을 수 있는 환경으로 의미가 확장되고 있다.

'유비쿼터스'란 단어는 '언제, 어디서나'라는 뜻의 라틴어에서 유래된 용어이며, 컴퓨터들이 단독으로 사용되지 않고 유비쿼터스 통신, 유비쿼터스 네트워크 등과 같은 형태의 컴퓨팅 환경을 구축할 것이라고 말했다. 즉, 컴퓨터에 어떠한 기능을 추가하는 것이 아니라 자동차, 냉장고, 안경, 시계 등과 같이 어떤 기기나 사물에 컴퓨터를 접목하여 통신이 가능하도록 구축하는 정보기술 패러다임을 뜻하는 것이다.

유비쿼터스에 대해서는 우리나라뿐만 아니라 국외 여러 나라에서 다양한 연구를 진행하고 있다. 일본에서는 트론(TRON) 프로젝트를 주도하여 세계의 주목을 받았으며, 도쿄대 사카무라 켄 교수는 저서 '유비쿼터스 컴퓨팅 혁명'을 통해 '선진국의 경우 저성장 사회로의 이행이 가속화되고 있는데, 유비쿼터스 컴퓨팅은 지속적 성장이 가능한 순환형 시스템의 정착을 가능하게 해줄 것'이라고 전망하였다. 그는 저서에서 유비쿼터스 환경 하에서는 정보습득과 활용이 최적화되어 소모성 자원의 효율적인 사용이 가능해질 것이며, 유비쿼터스 컴퓨팅이 대량 생산의 획일적인 '하드와이어드' 사회를 개개인의 다양성에 적절하게 대응할 수 있는 사회로 탈바꿈시켜줄 것으로

전망하였다[1,2].

또한 세계 최대의 소프트웨어 업체인 마이크로소프트의 빌 게이츠 회장은 컴덱스 기조 연설에서 'SPOT(Smart Personal Object Technology)'을 새로운 화두로 제시했다. SPOT의 스마트 오브젝트는 인터넷 기능을 구현해 언제, 어디서나 온라인에 손쉽게 접속할 수 있도록 해주는 알람시계, 부엌용 전자기기, 스테레오 장비 등과 같은 소형 전자기기를 의미한다. 즉 유비쿼터스를 다르게 표현한 것으로 전 세계 IT 산업에 가장 큰 영향력을 행사하는 인물 중 하나인 빌게이츠가 유비쿼터스 시대의 본격적인 개막을 선언한 것이다.

이처럼 유비쿼터스는 전 세계적으로 최대 화두로 다뤄지고 있으며, 유비쿼터스의 실현으로 실세계의 각종 사물들과 물리적 환경 전반 즉, 물리공간에 걸쳐 컴퓨터들이 편재되어 있으나, 사용자에게는 겉모습이 드러나지 않도록 환경 내에 효과적으로 심어지고 통합되는 새로운 정보통신 환경의 구축을 예상하고 있다. 이러한 유비쿼터스의 개념을 바탕으로 구축된 환경이 유비쿼터스 컴퓨팅 환경이다. 이동 컴퓨팅과 지능적 환경이 함께 적용되면 유비쿼터스 컴퓨팅의 모든 기능이 실현된 것으로 예상되고 있다. 또한 유비쿼터스 컴퓨팅은 이동 컴퓨팅이나 지능적 환경만으로 비가시적 컴퓨팅이나 인간 중심의 인터페이스(Calm Technology)에 대한 시나리오 제시가 다음과 같이 가능하다[3].

- 비통합적 컴퓨팅 (Disaggregated Computing): 실내에 존재하는 스피커, 마이크, 디스플레이 등의 개별 사용자 인터페이스 장치들이 동적으로 재구성된다. 즉, 유비쿼터스 환경의 컴퓨터는 네트워크상 연결 혹은 근거리 무선통신 토폴로지 내에 존재하는 다양한 장치들의 가상 결합 그룹이다. 보통, 각각의 장치들은 소프트웨어적 장치인 프록시 소프트웨어를 가진다.
- 위치감지 컴퓨팅 (Location-Sensitive Computing): 예를 들어 걸어 다니는 관람자가 전시물을 관람하는 경우, 위치감지에 의하여 관람자와 가장 가까운 디스플레이 장치에 전시물에 대한 설명이 자동으로 표시된다. 이때 카메라에 의한 시각적 감시나 배지와 같은 태그를 이용하는 등의 사람 위치 파악 센서가 필요하다.
- 증강현실 (Augmented Reality): 위치감지 정보와 입는 컴퓨터가 결합될 때, 컴퓨터를 입고 있는 사람과 관련된 정보가 헬멧형 디스플레이상에 표시된다. 이는 단지 컴퓨터상에 생성되는 정보인 가상현실과는 반대되는 것으로 증강현실이라고 부른다.
- 객체감지 사용자 인터페이스와 필콘 (Object-Sensitive User Interfaces and Phicons): 임의 웹 페이지와 관련된 물리적 객체(전자적 사물), 즉 사람이 해당 웹 페이지와 관련된 객체에 사용자 이동 컴퓨터를 가져가면 사람은 해당 웹 페이지의 정보를 볼 수 있다.

위와 같이 유비쿼터스 환경에서는 유비쿼터스 컴퓨팅 환경 시나리오를 구축하기 위한 네트워크를 형성해 나가고 있다. 유비쿼터스 환경의 네트워크는 정보를 신속하고 정확하게 전송할 수 있어야 하며, 서비스가 지속적으로 제공될 수 있도록 네트워크의 질을 향상시켜야 한다. 이러한 환경은 초고속 인터넷을 기반으로 구축되고 있다. 초고속인터넷은 1995년부터 활성화되기 시작하여 컴퓨터를 통해 개방된 네트워크에 접속하여 다양한 사용자들이 정보 교류를 하는데 사용되었다.

인터넷 속도가 빠르기 때문에 다양한 콘텐츠들이 생성되어 초고속인터넷망을 통하여 전송되었으며, 사용자들의 콘텐츠 사용량이 증가하였다. 콘텐츠는 디지털 콘텐츠를 의미하며, 이는 유무선 전기 통신망에서 사용하기 위하여 문자, 부호, 음성, 음향, 클라이언트, 영상 등을 디지털 방식으로 제작해 처리 및 유통하는 각종 정보 또는 그 내용물을 통틀어 이르는 개념이다. 콘텐츠는 본래 문서·연설 등의 내용이나 목차, 요지를 뜻하는 말이었으나 IT 기술이 빠르게 발달하면서 각종 유무선 통신망을 통해 제공되는 디지털 정보나 그러한 내용물을 총칭하는 용어로 널리 쓰이게 되었다.

콘텐츠는 크게 디지털 콘텐츠와 멀티미디어 콘텐츠로 구분한다. 디지털 콘텐츠는 구입, 결제, 이용에 이르기까지 모두 네트워크와 PC를 통해 이루어지기 때문에 기존의 통신판매 범위를 훨씬 뛰어넘어 전자상거래의 새로운 형태로 확고한 자리를 잡았고, 갈수록 시장 수요도 확대되고 있다. 멀티미디어 콘텐츠는 콤팩트디스크, CD-ROM, 비디오테이프 등에 담긴 사진, 미술, 음악, 영화, 게임 등 읽기 전용의 다중매체 저작물과 광대역통신망이나 고속 데이터망을 통해 양방향으로 송수신되는 각종 정보 또는 내용물,

디지털화되어 정보기기를 통해 제작, 판매, 이용되는 정보 등을 말한다.

3. 관련 연구

안전하게 콘텐츠를 사용하기 위하여 콘텐츠 보안을 제공하는 기술은 DRM 기술과 CAS 기술이 있다. 최근에는 케이블 카드를 사용하는 CAS가 다운로드하여 사용할 수 있는 형태로 변화하여 유용성을 제공할 수 있도록 하고 있다. 이러한 기술들을 기반으로 본 장에서는 제안 시스템의 관련 기술들에 관하여 서술한다.

3.1 DRM

초고속 인터넷의 보급률이 증가함에 따라, 우리나라뿐만 아니라 각 나라에서 생성된 다양한 콘텐츠들이 초고속 인터넷망을 따라 빠른 속도로 전파되었다. 저작권과 관련되지 않은 콘텐츠들을 사용자들이 공유하고 유통시키는 것은 합법적인 것이지만, 저작권자의 허가 없이 콘텐츠를 유통하는 것은 위법이기 때문에, 저작권자의 권리 보호에 대한 요구가 증가하였다. 이러한 저작권자의 권리 보호하고 디지털 콘텐츠의 사용을 제한하여 콘텐츠 보호를 제공하는 기술이 DRM 기술이다[4].

DRM은 'Digital Rights Management'의 약어로 디지털 콘텐츠의 사용을 제어하고, 불법복제 및 유통을 방지하는 기술 및 서비스를 의미하여, '디지털 저작권 관리' 혹은 '디지털 권한 관리'로 표현되기도 한다[5,6]. 광의의 의미에서 디지털 콘텐츠의 지적재산권 보호를 위해 사용되는 보호기술(Protection)과 디지털 콘텐츠의 관리 효율화를 위해 사용되는 관리기술(Management), 그리고 디지털 콘텐츠의 투명하고 편리한 유통환경을 위해 사용되는 유통기술(Distribution)로 크게 구분되며, 능동적 보호기술의 사용 제어기술(Use Control)이 협의의 의미로서의 DRM 기술 범주에 해당된다. DRM이 적용된 콘텐츠를 사용하기 위해서는 콘텐츠를 사용하기 위한 라이센스가 필요하며, 이 라이센스는 저작권자가 콘텐츠를 사용을 허용하는 사용자에게 배포되는 키이다. 사용자는 라이센스를 획득한 후에 콘텐츠를 사용할 수 있으며, 라이센스가 없는 경우 DRM 기술로 콘텐츠를 사용할 수 없도록 통제하고 있다[7,8]. DRM 기술의 전체적인 범주는 그림 1과 같다.

3.2 CAS

CAS는 'Conditional Access System'의 약자로 방송 콘텐츠를 인증 받은 사용자에게 전송하여 수신할 수 있도록 콘텐츠 보안을 제공하는 기술이다. 인증 받은 사용자에게만 콘텐츠 수신을 허용하므로 '수신 제한 시스템'이라 표현되기도 한다. CAS는 수신 제한을 하기 위하여 스크램블링 기술과 키 관리 기술을 지원하고 있다. 또한 인증 받은 콘텐츠를 복사, 저장 및 배포할 수 없도록 다양한 보안 기술을 포함하고 있다. 이를 기반으로 수신 자격이 주어진 사용자만이 스크램블링 된 콘텐츠를 디스크램블링 하여 사용할 수 있도록 하는 것이다.

CAS의 전체적인 구성도는 그림 2와 같다. 하지만 디스크램블링에 사용되는 키를 케이블 카드에 저장하여 사용함으로써, 키가 노출될 경우 시스템을 변경하는데 비용이 증가하고, 특정 업체의 STB에 종속되어 있으므로 많은 문제점이 제기되었다. 이를 해결하기 위하여 소프트웨어를 다운로드하여 콘텐츠 보안을 제공하는 D-CAS (Downloadable-CAS)가 개발

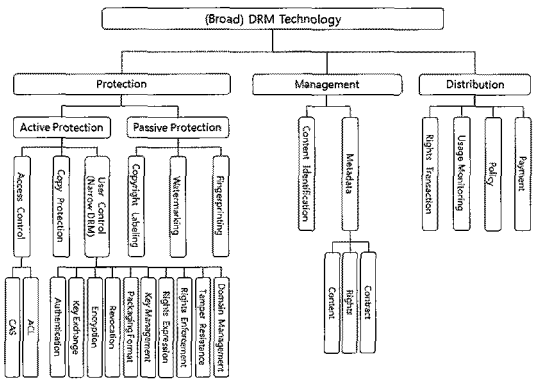

그림 1. DRM 기술 구성도

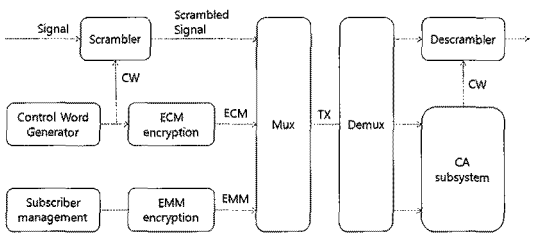

그림 2. CAS 시스템 구성도

되었다. D-CAS로 콘텐츠 보안을 제공하는 경우 특정 업체의 STB에 종속되지 않으며, 키 노출 시 해결 방안이 편리하고 비용이 적게 든다는 장점을 가지고 있어 D-CAS 형태의 콘텐츠 보안이 점차 증가하고 있다.

4. SDCS : Secure D-CAS System

초고속 인터넷 망을 통하여 다양한 콘텐츠가 개발되고, 개발된 콘텐츠들이 빠른 속도로 전파되고 있다. 다양한 콘텐츠로 인하여 사용자들은 많은 도움을 받고 있지만, 이러한 콘텐츠들이 무분별하게 유포되어 저작권자의 권리가 보호되지 못하고 있다. 이로 인한 피해가 속출하고 있으며, 이를 해결하기 위하여 DRM 및 CAS 기술을 콘텐츠에 적용하여 인가된 사용자만이 콘텐츠를 사용하여 저작권자의 권리를 보호하는 안전한 환경을 구축하고자 노력하고 있다. 하지만 기존에 사용하고 있는 CAS 기술은 케이블 카드를 통하여 인증 받는 방식으로 전체적인 시스템이 특정 개발 업체에 종속되어 있다는 문제점이 제기되고 있다. 이를 개선하여 개발된 기술이 D-CAS (Downloadable-CAS)이다. D-CAS란 CAS 기술을 사용하기 위한 환경을 다운로드를 통해 구축하므로, 문제 발생 시 해결하기가 쉽고, 유연성을 제공할 수 있다는 장점을 가지고 있다[9,10].

이러한 D-CAS는 콘텐츠 보안을 위한 기술로 자리 잡고 있으며, 비용적인 측면에서도 강점을 지니고 있다. 현재 DRM 및 CAS 기술을 사용하고 있는 시스템이 보급되어 있으나, D-CAS 기술이 점차 증가하고 있으며, 이러한 D-CAS의 장점을 이용하여 콘텐츠를 안전하게 다운로드하는 방안(SDCS : Secure D-CAS System)에 대하여 제안하고자 한다.

4.1 SDCS 구성

유비쿼터스 환경을 구축하기 위하여 네트워크 속도가 증가하고 있으며, 이에 따른 초고속 인터넷망에서 안전하게 콘텐츠를 사용하기 위하여 다양한 연구가 진행되고 있다. SDCS는 디지털 방송을 지원하는 환경의 콘텐츠 서버로부터 안전하게 콘텐츠를 다운로드하는 시스템으로, 콘텐츠 클라이언트 정보 및 서버 정보를 관리하고 배포하는 Policy & Schedule Server, Policy & Schedule Server로부터 배포된 정보를 기반으로 범용 보안 클라이언트를 생성/관리하는 Client Management Server, Client Management Server에 대한 인증 및 클라이언트 암호화를 처리하는 Authenticate Management Server, Policy & Schedule Server로부터 생성된 클라이언트 정보를 전송받는 Network Proxy로 구성된다.

- Policy & Schedule Server : 클라이언트 정보 및 호스트 정보를 관리하고 배포하는 서버로 호스트를 통하여 등록되는 호스트 정보 및 클라이언트 정보를 관리하고 클라이언트 배포 Policy & Schedule을 관리
- Client Management Server : Policy & Schedule 서버로부터 배포된 Policy & Schedule을 기반으로 클라이언트를 생성하는 서버로 CAS, DRM 등의 소프트웨어를 클라이언트화하여 범용 콘텐츠 보호호스트에게 제공하며, 다운로드할 클라이언트에 대한 암호화 및 전자서명을 처리
- Authenticate Management Server : Client Management Server에 대한 인증 및 클라이언트 암호화를 처리하는 서버로 범용콘텐츠 보호 호스트, Network Proxy , Client Management Server에 대한 인증처리를 수행하며, 클라이언트 암호화 처리를 위한 키 관리를 수행
- Network Proxy : Policy & Schedule Server로부터 생성된 클라이언트 정보를 전송받는 서버로 범용콘텐츠 보호 호스트, Client Management Server, Policy & Schedule Server, Authenticate Management Server, 운영 시스템 등과 직접 통신하며, 범용콘텐츠 보호 호스트와 메시지를 주고받는 프락시 역할과 인증을 수행

SDCS는 그림 3과 같이 구성되어 있으며, 네 가지 서버가 각각의 기능을 통하여 안전한 콘텐츠 다운로드 기능을 제공한다.

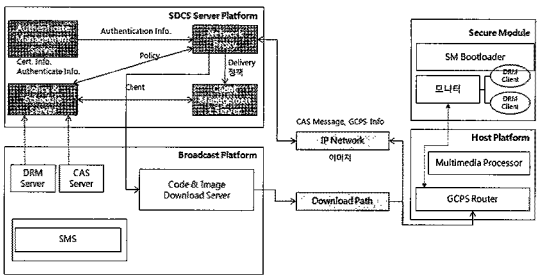

그림 3. SDCS 구성도

4.2 제안 시스템: SDCS

디지털 콘텐츠는 초고속 네트워크망을 통하여 무분별하게 전파되고 있다. 이로 인하여 디지털 콘텐츠를 생성한 저작권자의 권익이 보호되지 못하고 있으며, 현재 사용하고 있는 콘텐츠 보호 시스템은 케이블 카드를 인용한 방식으로 자체 발열과 고장, 셋톱박스의 가격 상승 등의 원인이 된다는 문제점이 있다. 또한 특정 벤더에 종속되어 서비스 업자나 사용자가 콘텐츠 보호 시스템을 유연하게 사용할 수 없다는 문제가 발생하므로, 이를 해결하기 위하여 디지털 콘텐츠 보호 기술이 필요하게 되었다[11,12].

SDCS는 Secure D-CAS System의 약어로 디지털 콘텐츠를 사용하는 환경에서 저작권자의 권익을 보호하며, 디지털 콘텐츠를 안전하게 다운로드 받아 사용하는 시스템이다. SDCS를 개발하는 이유는 케이블 카드를 사용하지 않아 기존의 케이블 카드에 종속적이지 않으며, 자체 발열과 고장, 가격 상승의 문제를 해결하는 디지털 방송 시스템에서의 다운로드 콘텐츠 보호 시스템 및 그 접속 방법이기 때문이다.

SDCS는 디지털 방송을 지원하는 환경의 범용콘텐츠 보호서버로부터 범용 콘텐츠 보호 호스트로 클라이언트를 다운로드 하는 다운로드 콘텐츠보호 시스템에 있어서, 클라이언트정보 및 호스트정보를 관리하고, 배포하는 Policy & Schedule Server, Policy & Schedule Server로부터 배포된 Policy & Schedule을 기반으로 클라이언트를 생성하는 Client Management Server, Client Management Server에 대한 인증 및 클라이언트 암호화를 처리하는 Authenticate Management Server, Policy & Schedule Server로부터 생성된 클라이언트정보를 전송받는 Network Proxy 로 구성되는 것을 특징으로 한다. 본 시스템은 디지털 방송을 지원하는 환경의 범용 콘텐츠 보호 서버로부터 범용콘텐츠 보호호스트로 클라이언트를 다운로드 하는 과정은 다음과 같은 절차를 통하여 이루어진다.

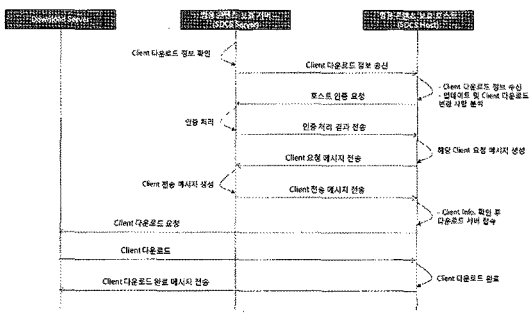

그림 4. SDCS 수행과정

(a) 범용콘텐츠 보호서버가 시스템정보를 생성하고, 범용콘텐츠 보호호스트에 전송하는 단계

(b) 범용콘텐츠 보호호스트가 인증을 요청하고 그 결과를 전송받는 단계

(c) 범용콘텐츠 보호호스트가 클라이언트 요청메시지를 생성하고 전송하는 단계

(d) 범용콘텐츠 보호호스트가 상기 클라이언트를 상기 범용콘텐츠 보호서버로부터 다운로드 받는 단계

(e) 단계(d)를 실시하고 범용콘텐츠 보호호스트가 범용콘텐츠 보호서버에 다운로드 완료메시지를 전송하는 단계

이외에 MSO Manager는 Policy & Schedule서버의 클라이언트로 MSO 관리자가 호스트 정보 및 클라이언트 정보를 관리하는 어플리케이션이다. MSO Manager는 클라이언트 배포에 대한 배포 정책 및 스케줄을 관리하며 이를 통해 등록된 소프트웨어 클라이언트와 Policy & Schedule은 Policy & Schedule 서버에 의해서 배포된다. 운영시스템은 SDCS의 환경 설정을 수행하고 서비스 처리 상태를 모니터링하여 관리자에게 보고한다. 또한 시스템 운영 과정을 감시하고 에러가 발생하면 관리자가 조치를 취할 수 있도록 에러 보고 기능을 수행한다.

범용콘텐츠 보호 호스트는 ESTB(embeded Set TOP Box)와 SM(Secure Module)로 구성된다. ESTB는 GCPS(General Content Protection System) Router를 포함하고, GCPS Router는 범용콘텐츠 보호서버로부터 범용 콘테츠 보호호스트로 전달한 범용 콘테츠 보호와 관련한 모든 메시지를 라우팅하며, SM 등과 주고받는 모든 범용 콘테츠 보호메시지를 라우팅(Routing), 필터링(Filtering), 큐잉(Queuing)하는 역할을 담당한다. SM은 SM Manager, SM bootloader, DRM Client, CAS Client 등을 포함하며, SM Manager는 SM에서 CAS Client가 동작하는 동안 GCPS 메시지를 모니터링하고, GCPS 메시지를 GCPS Router나 SM Bootloader로 라우팅한다. SM Bootloader는 SM의 논리적인 펌웨어의 하나로 SM을 부팅시키고, DRM Client, CAS Client를 램에 적재한 후, 이를 사용할 수 있게 로딩

한다. SM Bootloader의 다른 기능으로 SM Bootloader는 보안 다운로드기능을 포함한다.

보안 다운로더(Secure Downloader)는 다운로드된 클라이언트에 대한 검증절차를 거쳐 서명을 분리하고, 암호화된 클라이언트를 복호화하여 보안 램에 적재하는 역할을 수행하며, DRM Client는 다운로드 가능한 형태의 클라이언트파일로 보안 램에 적재될 수 있는 타입으로 전달되어야 한다. DRM Client는 DRM 메시지에 기반하여 로컬 라이센스(Local License)를 발급하고, 해당 콘텐츠의 라이센스의 유효성을 검사하여 콘텐츠에 대한 PVR(Personal Video Recorder) 및 재생할 수 있도록 한다. 예를 들어, DRM Client가 SM Manager로부터 DRM 메시지를 수신하여 이를 저장하고, PVR 시 해당 콘텐츠에 대한 로컬 라이센스를 발급하고, DRM Client는 라이센스 사용가능회수와 기간 등의 정보를 기준으로 재생 시 라이센스의 유효성을 검사하고 판단하며, 암호화 알고리즘에 따른 암호화 키를 생성하고 관리한다.

CAS Client클라이언트는 다운로드 가능한 형태의 클라이언트파일이 보안 램에 적재될 수 있는 타입으로 전달되어야 한다. 범용콘텐츠 보호시스템에서 사용하는 콘텐츠보호 솔루션클라이언트 파일의 구조에 있어 범용 콘테츠 보호시스템에서 다운로드되는 콘텐츠보호 솔루션클라이언트 파일은 다운로드되는 클라이언트에 대한 정보를 포함하는 클라이언트헤더 및 클라이언트의 내용인 클라이언트 데이터를 포함하고, 다운로드 되는 콘텐츠 클라이언트파일은 검증요구 시 필요한 서명데이터(Signature Data)를 더 포함한다. 구체적으로, 다운로드 콘텐츠보호 솔루션클라이언트는 기본적으로 하나의 콘텐츠보호 솔루션클라이언트를 포함하고 있지만, 최초의 다운로드의 경우에는 CAS, DRM 등 2개 이상의 클라이언트를 하나의 다운로드 콘텐츠보호 솔루션 클라이언트로 생성하여 전송할 수 있다. 그렇기 때문에 다운로드 클라이언트헤더에 클라이언트에 대한 정보를 포함한다. 예를 들어, 팩클라이언트갯수(Packed Image Number)는 다운로드 콘텐츠보호 솔루션클라이언트에 포함되어 있는 콘텐츠보호 솔루션의 클라이언트의 수이며, 전체 클라이언트길이(Total Image Length)는 다운로드 콘텐츠보호 솔루션클라이언트의 전체크기를 나타내고, Reserved는 추가정보를 의미하고, 이러한 정보는 클라이언트헤더에 포함된다.

범용콘텐츠 보호서버에서의 Client Management Server가 콘텐츠보호 솔루션클라이언트를 범용콘텐츠 보호호스트에 다운로드할 때, 다운로드 범용콘텐츠 보호클라이언트를 개방형으로 다운로드해주기 위한 단계는 범용콘텐츠 보호서버가 시스템정보를 생성하는 단계, 시스템정보를 범용콘텐츠 보호호스트로 전송하는 단계, 시스템정보가 새로운 시스템정보인지를 판단하는 단계, 인증을 요청하는 단계, 인증을 처리하는 단계, 처리된 인증결과를 전송하는 단계, 클라이언트요청 메시지생성단계, 범용콘텐츠 보호서버에 클라이언트 다운로드를 요청하는 클라이언트요청 메시지전송단계, 범용콘텐츠 보호서버에서 클라이언트를 생성하는 단계, 범용콘텐츠 보호호스트에 클라이언트 생성정보를 전송하는 단계, 범용콘텐츠 보호호스트에서 범용콘텐츠 보호서버에 접속하는 단계, 클라이언트를 다운로드하는 단계, 다운로드 받은 클라이언트를 검증하는 단계, 다운로드 완료메시지를 전송하는 단계로 이루어진다.

4.3 SDCS 효과

SDCS는 디지털 방송을 지원하는 환경의 범용콘텐츠 보호서버로부터 범용콘텐츠 보호호스트로 클라이언트를 다운로드 하는 다운로드 콘텐츠보호 시스템에 있어서, 클라이언트정보 및 호스트정보를 관리하고 배포하는 Policy & Schedule Server, Policy & Schedule Server로부터 배포된 배포 정책 및 스케줄을 기반으로 클라이언트를 생성하는 Client Management Server, Client Management Server에 대한 인증 및 클라이언트 암호화를 처리하는 Authenticate Management Server, Policy & Schedule Server로부터 생성된 클라이언트정보를 전송받는 Network Proxy로 구성되는 것을 특징으로 하는 다운로드 콘텐츠보호 시스템으로 다양한 효과를 제공한다.

SDCS에 따른 다운로드 콘텐츠보호 시스템 및 그 접속방법에 의하면 콘텐츠 보호에 대한 요소들을 다운로드 하여 사용하므로, 종래의 수신제한 시스템의 케이블카드 하드웨어의 종속성을 탈피할 수 있고, 다운로드 방식에 의해 STB당 소용되는 케이블카드의 비용절감을 할 수 있다는 효과가 얻어진다. 또한 디지털 케이블방송 시스템 외에 IPTV(Internet Protocol Television)시스템에도 적용을 할 수 있다는 효과가 얻어지며, 양방향 데이터처리가 가능하며, 사용자의 다운로드 이력관리가 기능이 제공될 수 있다.

5. 결 론

유비쿼터스 환경이 구축됨에 따라 유비쿼터스를 구축하는 다양한 디바이스 간의 통신이 중요한 이슈로 대두되고 있으며, 가장 기반이 되는 네트워크는 인터넷망이라고 할 수 있다. 사용자의 컴퓨터들이 인터넷망을 통하여 정보를 전송하는 것은 초고속 인터넷이 보급됨에 따라 더 활성화되고 있다. 초고속 인터넷망을 통하여 유통되는 것들 중 가장 많은 전송이 이루어지는 분야가 디지털 콘텐츠 분야이다. IT 기술의 발달로 일반 사용자들도 디지털 콘텐츠를 생성할 수 있는 능력이 충분하여, 사용자들로부터 생성된 디지털 콘텐츠의 양이 증가되고 있다. 유통하기 위하여 생성되는 디지털 콘텐츠도 존재하지만 저작권자의 허가 여부에 따라서 유통되어야 하는 디지털 콘텐츠도 존재한다. 그러나 초고속 네트워크망을 통하여 저작권자의 허가 없이 디지털 콘텐츠가 전파되고 있어 문제가 되고 있다. 이를 해결하기 위한 기술이 DRM 기술, CAS 기술 등으로 디지털 콘텐츠의 무분별한 유통을 막고, 저작권자의 권리를 보호해주는 기술이다.

앞으로는 현재보다 더 속도가 빠른 인터넷망을 구축하게 될 것이며, 컴퓨터뿐만 아니라 다양한 기기간의 네트워크망도 구축되어 지금보다 훨씬 넓은 범위의 초고속 네트워크가 구축될 것이다. 또한 IT 기술도 진보하여 일반 사용자들도 디지털 콘텐츠를 생성하고 이에 의하여 생성되는 디지털 콘텐츠의 양도 방대해질 것이다 이러한 환경에서 저작권자의 권익을 보호하고, 합당하게 디지털 콘텐츠를 사용하기 위해서는 DRM, CAS와 같이 콘텐츠 보호 기술에 대한 연구가 진행되어야 할 것이다.

이러한 콘텐츠 보호 시스템 및 기술들은 유비쿼터스 환경의 방대한 네트워크 상에 존재하는 콘텐츠에 대하여 올바른 사용자만이 획득할 수 있도록 인증을 제공하며, 안전하게 다운로드하여 사용할 수 있는 환경을 조성하는데 기여할 수 있으리라고 판단된다.

참 고 문 헌

[1] D. H. Wilson, A. C. Long, and C. Atkeson, "A Context-Aware Recognition Survey for Data Collection Using Ubiquitous Sensors in the Home," In Proc. of CHI 2005: Late Breaking Results, pp. 1865-1868, 2005.

[2] Bill Schilit, Norman Adams, and Roy Want, "Context-aware computing applications," *In* Proc. of IEEE Workshop on Mobile Computing Systems and Applications, pp. 85-90, Dec. 1994.

[3] R. Paradiso, G. Loriga, and N. Taccini, "Wearable Health Care System for Vital Signs Monitoring," In Proc. of MEDICON 2004, Italy, 2004.

[4] B. von Solms and D. Naccache, "On blind signatures and perfect crimes," *Computers and Security*, Vol.11, No.6, pp. 581-583, 1992.

[5] Mark Bauger, "Internet Digital Rights Management Taxonomy," IETF-51, Aug. 6, 2001.

[6] Paul England, John D. DeTreville, and Butler W. Lampson, "Digital Rights Management Operating System," United State Patent 6,330,670, Dec. 11, 2001.

[7] ISMA Report, "Internet Streaming Media Alliance DRM Task Force Report," IRTF-IDRM.52 IETF meeting, Oct. 2001.

[8] Kiyoshi Yamanaka, Hitoshi Shibagaki, Norihigo Sakurai, and Terunao Soneoka, "Trend of Digital Copyright Protection Technologies," *NTT R&D*, Vol.47, No.6, 1998.

[9] 여상수, 윤훈기, 김성권, "디지털 컨텐츠의 지적재산권 보호를 위한 익명 핑거프린팅의 연구동향," 한국정보보호학회지, 제11권, 제3호, pp. 90-99, 2001.

[10] 이덕규, 오형근, 이임영, "지불정보를 이용한 Hidden Agent 컨텐츠 불법 복사 방지에 관한 연구," 2002년 한국멀티미디어학회 춘계학술대회, pp. 947-950, 2002.

[11] 이덕규, 이임영, "Agent 기반 불법 복제 방지 DRM모델," 2001년 한국정보과학회 추계학술대회, 2001.

[12] 김영모, 고병수, "다운로드형 제한수신 시스템 기술 동향," 방송공학회지, 제13권, 제4호, pp. 54-63, 2008.

여 상 수

1993년 3월~1997년 2월 중앙대학교 컴퓨터공학과 공학사

1997년 3월~1999년 2월 중앙대학교 컴퓨터공학과 공학석사

2000년 3월~2005년 8월 중앙대학교 컴퓨터공학과 공학박사

2006년 3월~2007년 2월 단국대학교 정보컴퓨터학부 강의전임강사

2007년 2월~2008년 1월 일본 큐슈대학교 방문연구원

2008년 2월~2009년 2월 주식회사 비티웍스 연구개발본부 부장

2009년 3월~현재 목원대학교 컴퓨터공학부 전임강사

관심분야 : 정보보호, 멀티미디어, 임베디드, 정보시스템