실시간 멀티미디어 서비스의 DRM적용방법 설계

권순홍[0], 김기영, 신용태
숭실대학교 컴퓨터학과
ksh1303@cherry.soongsil.ac.kr

A Design of adaptive method in realtime multimedia service

Soonhong Kwon[0], Kiyoung Kim, Yongtae Shin, / Jae-Chang Kwak
Dept. of Computing, Soongsil University, Dept / Computer Science SeoKyeong Univ.,

요 약

인터넷 사용자의 폭발적 증가와 콘텐츠 제공업체의 범람은 지적재산권 보호에 관심을 갖게 하였다. 본 논문에서는 지적재산권을 보호할 수 있는 기밀성을 보장하는 키관리 시스템을 제안하고 실시간 데이터의 특성을 수용하여 효율적인 멀티미디어 전송을 보장할 수 있는 암호화 기법인 선택적 암호화 기법을 제안한다. 또한 제안한 기법을 바탕으로 멀티미디어 데이터 서비스에 적합한 DRM시스템 모델을 제안한다.

1.소 개

인터넷의 폭발적인 증가와 각종 디지털 콘텐츠의 범람으로 이에 대한 저작권 보호 및 상품성이 강조되는 시대가 되었다. 하지만 이러한 디지털 콘텐츠는 인터넷을 통하여 배포나 복제가 너무나 손쉽게 이루어져 이를 상품으로 제공하는 업체나 저자들은 뜻하지 않은 피해를 입는 경우가 늘어나게 되었다. 이에 따라 각종 디지털 콘텐츠에 저작권을 표기하는 워터마킹이나 불법복제가 이루어지지 않도록 방지하는 DRM(Digital Right Management) 기술이 발전되게 되었고 국내 및 국외에서 지속적인 연구개발이 수행되고 있다.

국내에도 벤처 열풍에 힘입어 각종 디지털 콘텐츠를 제공하는 업체들이 많이 생기게 되었고, 각 업체의 상품을 효율적으로 관리하기 위해서는 판매와 더불어 불법복제 방지 시스템이 필요하다는 것을 점차 인식하게 되었다. 따라서 본 논문에서는 디지털 콘텐츠를 보호할 수 있는 방안에 대한 전체 시스템 설계 및 키 관리 시스템에 대해 다루고자 한다.

2.연구 배경

이 논문에서는 멀티미디어 데이터를 실시간으로 주고받을 때에 이에 대한 저작권을 보호할 수 있는 방안에 대해서 다룬다. 현재 마이크로 소프트의 플레어 및 AOL사의 리얼플레이어가 동영상에 대한 스트리밍 서비스를 하고 있다. 그러나 이러한 스트리밍 서비스는 URL의 노출 및 각종 스트리밍 레코더에 의해서 불법 복제 및 배포가 이루어지고 있다. 이에 DRM을 적용하여 불법 복제를 막을 수 있는 방법으로 현재 마이크로 소프트의 DRM솔루션이 나와있다. 하지만 이는 마이크로 소프트가 제작한 멀티미디어 포맷에만 적용되고 있고, 그 외에는 별다른 스트리밍 서비스에 대한 DRM솔루션이 언급되지 않고 있다.[7]

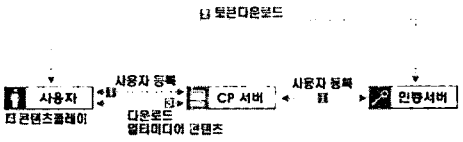
이 논문에서는 RTP를 사용하여 실시간으로 스트리밍 서비스를 제공하는 것과 MPEG2 포맷을 RTP 기반으로 전송할 경우 이를 암호화할 수 있는 방법에 대해서 제시한다. 뿐만 아니라, 이를 효율적이고 안전하게 보호할 수 있는 키 관리에 대해 전반적으로 다루고자 한다.

3.관련 연구

위의 소개 및 연구 배경에 필요한 솔루션을 제공하기 위해서는 전반적인 키 관리 시스템, 영상포맷에 대한 이해, 그리고 스트리밍 서비스를 위한 RTP/RTCP에 대한 연구가 필요하다. 또

한 DRM 솔루션의 전반적인 흐름에 대한 이해가 필요하다.

3.1.DRM 솔루션의 전반적인 흐름



위의 그림에서는 국내 및 국외에서 사용되는 DRM 솔루션의 기본적인 흐름을 표시하였다.

기본적으로 처음 사용자가 CP(Content Provider)에 등록을 하게 된다. CP는 각종 멀티미디어 콘텐츠를 공급하는 회사쪽의 서버를 지칭한다. 사용자가 CP에 등록을 하면 CP서버에서는 인증서버에 라이센스를 위한 사용자 등록을 하게된다. 이 라이센스를 여러 가지 포맷을 사용하여 인증서버가 사용자측에 전송하는데 여기서는 토큰을 사용하여 전송하는 방식을 사용하였다. 사용자는 이 토큰을 CP서버로부터 암호화된 콘텐츠를 복호화 할 경우 사용하게 된다. 사용자는 CP서버로부터 콘텐츠를 다운로드하고 토큰을 사용하여 콘텐츠를 복호화 한 후 재생하게 된다.

3.2.MPEG2 포맷

MPEG은 MPEG-1에서 시작하여 MPEG2까지 개발되었으며, MPEG-4 규격은 1999년 결정되었다. MPEG은 이제 멀티미디어에서 가장 중심적인 분야가 되었으며 나날이 그 응용분야가 확대되고 있다. MPEG-1과 MPEG2는 비디오 영상의 압축과 부호화 그리고 복호화에만 기능이 집중되어 있으나, MPEG-4는 이외에도 영상처리, 컴퓨터 그래픽스, 내용기반 검색기능 등의 분야로 확대되었다. MPEG-7은 여기에 텍스처 처리기능, 도큐먼트 통합처리 기능 등이 포함되었다. MPEG-21은 인증 기능까지 포함하여 전자상거래분야까지 그 응용분야가 확대될 예정이다.

MPEG-2 이론의 핵심은 DCT(Discrete Cosine Transform), DPCM(Differential Pulse Code Modulation), 움직임 예측(Motion Estimation)과 움직임 보상(Motion Compensation)이다. DCT의 이론적인 원천은 Fourier Transform으로서 공간 압축을 수행한다. DPCM은 PCM 방식을 개선하기 위하여 개발된 부호화 방식으로 신호간의 차이만을 부호화하는 방식이며 MPEG-2 부호기의 기본 구조는 DPCM방식으로 되어있다. 움직임 예측과 움직임 보상은 영상에 포함된 물체의 움직임을 부호화하여 시간 축에 따른 압축을 수행하기 위하여 개발된 방법이다. MPEG-2에서는 전 탐색 블록 매칭(full search block matching) 알고리즘을 사용하여 움직임 예측을 한다. 움직임 예측과 움직임 보상은 움직임 벡터를 이용하여 표현한다.[4]

3.3.RTP/RTCP

RTP는 오디오, 비디오 및 시뮬레이션 데이터와 같은 실시간 데이터를 멀티캐스트 또는 유니캐스트 네트웍을 이용해서 전송하는 응용 서비스에 알맞은 단말-대-단말 네트웍 전송 기능을 제공한다. RTP는 자원 예약을 수행하지 않으며, 따라서 적시 전달, 순차 전달과 같은 서비스 품질도 보장하지 않는다. RTP 데이터 전송 기능은 제어 프로토콜에 의해 확장되는데, RTCP라 불리우는 이 제어 프로토콜은 데이터의 전달 상황을 감시하며, 최소한의 제어 기능과 매체 식별 기능을 제공한다. RTP와 RTCP는 하위의 전송 및 네트웍 계층에 무관하게 설계되었다. RTP는 별개의 독립 계층으로 구현되기보다는 특정 응용에서 요구되는 정보를 제공하여 프로토콜의 처리가 응용의 처리 과정으로 통합될 수 있도록 설계되었다. 따라서 기존의 프로토콜들과는 달리 RTP는 응용의 필요에 따라 헤더를 변경하거나 추가하여 응용에 맞는 프로토콜이 될 수 있도록 하는 일종의 맞춤형 프로토콜이다. [2,3]

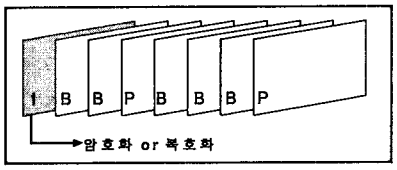
여기서는 RTP에 MPEG을 담아 전송하여 실시간 서비스가 가능하도록 하고 있다. [1]

4.제안 시스템

제안하는 시스템은 기본적인 DRM의 기능을 수용하지만 멀티미디어 데이터의 실시간성을 보장하는 실시간 전송방식과 인증된 사용자를 구별하여 기밀성을 제공할 수 있는 키 관리를 기법을 추가하였다.

실시간성을 지원하기 위해서 MPEG2 데이터의 Intra Picturer를 부분적 암호화한 패킷을 RTP를 이용하여 전송함으로써 암호화/복호화 시 발생되는 지연시간을 대폭 감소시켜 실시간성을 보장하였다. MPEG2 데이터의 Intra Picture 암호하는 다음과 같다.

4.1. MPEG-2의 암호화 및 복호화



MPEG에서는 압축의 가장 기본 단위가 되는 Picture라는 개념이 있다. I라고 표시된 것은 Intra picture의 약칭으로 시간적 압축기술을 사용하지 않고 공간적인 압축기술만을 사용해서 압축한 픽처이다. 이 I픽처는 주로 다른 픽처들의 참조픽처로서의 역할을 하며, 시간적인 압축을 사용하지 않기 때문에 독립적으로 복호화가 가능하다. 멀티미디어 콘텐츠는 암호화나 복호화시 거대한 용량 때문에 많은 시간이 소비된다. 하지만 다른 부분을 제외하고 이 Intra picture만 추출하여 암호화, 복호화를 수행하면 시간을 절약할 수 있으며, CPU의 점유율 또한 낮출 수 가 있다.[4]

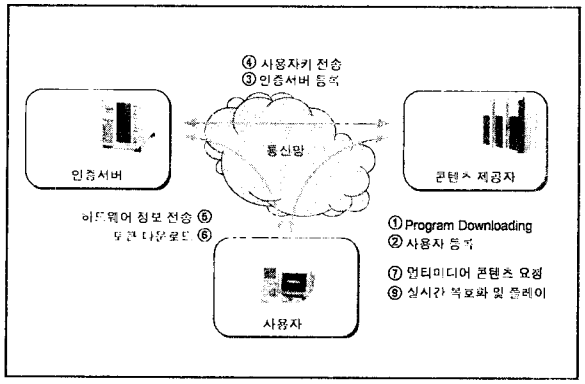
4.2.제안하는 DRM 시스템의 흐름

제안하는 DRM 시스템은 기본적인 DRM의 흐름을 따른다.

또한 다른 DRM과 비교해볼 때 토큰이라는 것을 사용하여 일반적인 복사 방지 및 스트리밍 레코더로부터의 복사를 방지한다.

1.Program Downloading

암호화된 스트리밍 멀티미디어 콘텐츠를 복호화 할 수 있게 하고 토큰이 다운로드 되어있지 않으면 토큰을 수신할 수 있는 프로그램을 다운로드 한다.



2.사용자 등록

사용자는 사용자 등록을 하면서 각종 정보를 콘텐츠 제공자에게 제공한다.

3.인증서버 등록

콘텐츠 서버(CP 서버)는 사용자를 구분할 수 있는 유일한 값을 (예:주민등록 번호) 인증서버에 보낸다.

4.사용자키 전송

인증서버는 콘텐츠 서버(CP 서버)로부터 전송된 값을 이용하여 사용자키를 만든 후 CP 서버로 보낸다. 이 사용자키는 CP 서버에서 멀티미디어 콘텐츠를 암호화 할 경우 사용되어진다.

5.하드웨어 정보 전송

다운로드 한 프로그램에서 처음 토큰을 신청할 시 이는 하드웨어 정보(예 : 하드디스크 시리얼넘버, CPU 시리얼, 파이션 세그먼트 크기, 스마트 카드 시리얼번호 등)를 포함하여 보낸다

6.토큰다운로드

인증서버에서는 사용자로부터 수신한 하드웨어 정보를 가공하여 내려보내고 토큰에 담겨진 하드웨어 정보를 이용하여 가공 처리한 후 토큰에 담아서 내려보낸다. 이러한 하드웨어 정보는 복사방지에 사용된다.

4.3.전체 키 관리시스템

H : 해쉬 함수,MD5를 사용[6]

E : 암호화, Rijndael 대칭키 암호화알고리즘을 사용[5]

D : 복호화, Rijndael 대칭키 암호화알고리즘을 사용[5]

-CP(Content Provider) 서버에서의 키관리 시스템

UserKey = H [주민등록번호(13) || SeedKey(16)]
FKey = H [UserKey(16) || CP서버 랜덤(16)]

CP서버는 사용자가 입력한 유일한 값인 주민등록번호와 인증서버로부터 받은 SeedKey값을 해쉬함수를 사용하여 UserKey를 생성한다. 그후 실제로 콘텐츠를 암호화할 FKey는 생성한 UserKey와 CP서버로부터 생성한 랜덤값을 ||시킨후 해쉬함수를 통과시켜 생성한다.

- 인증 서버에서의 키 관리 시스템

SeedKey = H [주민등록번호(13)]
UserKey = H [주민등록번호(13) || SeedKey(16)]
EncUserKey = $E_{TempKey}$ [UserKey(16)]
↳TempKey = H [인증서버 랜덤(16) || 하드웨어정보(16)]

인증서버에서는 CP서버로부터 넘겨받은 사용자 정보를 사용하여 SeedKey를 생성한다. 이 SeedKey는 CP서버에 전송하게 되어있고 인증서버에서도 CP서버와 동일한 방법을 사용하여 UserKey를 생성한다. 그 후 클라이언트로부터 토큰다운로드 요구 시 요구와 같이 전송되어 온 하드웨어 정보를 사용하여 EncUserKey를 생성한다. 토큰은 [인증서버 랜덤(16) || EncUserKey(16)]형태로 만들어 클라이언트에게 보내진다.

- 클라이언트측면에서의 키 관리

UserKey = $D_{TempKey}$ [EncUserKey(16)]
↳TempKey = H [인증서버 랜덤(16) || 하드웨어정보(16)]
FKey = H [UserKey(16) || CP서버 랜덤(16)]

클라이언트에서는 토큰을 윈도의 레지스트리와 같은 장소에 보관하고 있다가 콘텐츠 복호화 시 이를 사용하여 UserKey를 복호화 시킨다. 이후 콘텐츠를 암호화한 FKey를 얻기 위해서 암호화된 콘텐츠의 헤더에 담겨온 CP서버 랜덤값과 EncUserKey로부터 복호화된 UserKey를 이용하여 콘텐츠 복호화에 필요한 FKey를 얻는다.

5.결 론

현재 제안된 시스템은 구현중에 있다. 전체적인 암호화 및 복호화 시스템은 Rijndael 블록 암호화 알고리즘[5]을 사용한다. 또한 인증절차에도 블록 암호화 알고리즘을 사용하여 전체적인 인증절차를 수행하고 있는 것이 제안된 시스템의 특징중 하나이다. 실시간 전송에 대한 처리는 RTP 프로토콜의 Payload에 MPEG2를 얻어 보낼 계획이다.[1]

6.참 조

[1] RTP Payload Format for MPEG1/MPEG2 Video (RFC 2250)
[2] RTP: A Transport Protocol for Real-Time Applications (RFC 1889)
[3] RTP Profile for Audio and Video Conferences with Minimal Control (RFC 1890)
[4] "알기쉬운 MPEG-2" 이호석,김준기 홍릉과학출판사
[5] http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
[6] The MD5 Message-Digest Algorithm(RFC 1321)
[7] http://www.microsoft.com/windows/windowsmedia/drm.asp