실시간 멀티미디어 서비스의 DRM적용방법 설계

권순호, 김기영, 신용태
숭실대학교 컴퓨터학과
ksh1303@cherry.soongsil.ac.kr

A Design of adaptive method in realtime multimedia service

Soohung Kwon, Kyoung Kim, Youngtae Shin, / Jae-Chang Kwak
Dept. of Computing, Soongsil University, Dept. / Computer Science SeoKyung Univ.,

요약

인터넷 사용자의 복잡성 증가와 콘텐츠 제공업체의 양극은 지적재산권 보호에 관심을 갖게 하였습니다. 본 논문에서는 지적재산권을 보호할 수 있는 기법을 요용하여 기판리 시스템을 제안하고 실시간 멀티미디어 서비스를 보호할 수 있는 방안을 제안하였습니다. 또한 제안한 기법을 바탕으로 멀티미디어 데이터 서비스에 적용한 DRM시스템 모범을 제안하였습니다.

1. 소개

인터넷의 복잡성 증가와 각종 디지털 콘텐츠의 편리함으로 인해 지적재산권 보호 및 상품성이 강조되는 시대가 되었습니다. 이러한 디지털 콘텐츠는 인터넷을 통하여 배포되며 본 부가 가치가 부가되며 이용자에 의한 소비가 많아지며 이는 경제적 가치가 증가해버렸습니다. 이러한 디지털 콘텐츠의 보호를 위한 DRM(Digital Right Management) 기법이 발전되게 되었으며 국내 및 국외에서 지속적인 연구개발이 수행되고 있습니다.

국내에서도 본 논문에서는 이를 위한 보호를 위한 DRM(Digital Right Management) 기법이 발전되게 되었으며 국내 및 국외에서 지속적인 연구개발이 수행되고 있습니다.

2. 연구 배경

이 논문에서는 인터넷에 데이터를 실시간으로 주고받을 때에 이에 대한 저작권을 보호할 수 있는 방안에 대해 다루었습니다. 현재 마이크로소프트의 쿠키 및 AOL사의 리얼타임 서비스가 동영상에 대한 스토리밍 서비스를 하고 있습니다. 그러나 이러한 서비스는 URL의 출력 및 자료 스크립트 레코드에 의한 복제 및 배포가 이루어지지만, 이에 DRM을 적용하여 복제 및 배포를 막을 수 있는 방법으로 현재 마이크로소프트의 DRM(CM)이 보편화되고 있습니다. 하지만, 이는 현재로서 DRM이 제한된 멀티미디어 포맷에만 적용하고 있고, 그 외에는 별도의 DRM을 사용하는 서비스에 대한 DRM을 사용하지 않는다고 합니다.[7]

이 논문에서는 RTP를 사용하여 실시간으로 스토리밍 서비스를 제공하는 것과 MPEG2 포맷을 RTP 기반으로 전송할 경우 이를 보호할 수 있는 방법에 대해서 제시합니다. 또한 이는 이를 적용하고, 안전하게 보호할 수 있는 기판리에 대해 전반적으로 다루고자 합니다.

3. 관련 연구

이러한 소개 및 연구 배경에 필요한 용어를 제공하기 위해서는 전반적인 기판리 시스템, 영상포맷에 대한 이해, 그리고 스토리밍 서비스를 위한 RTP/RTCP에 대한 연구가 필요합니다.
한 DRM 출판의 전반적인 흐름에 대한 이해가 필요하다.

3.1. DRM 출판의 전반적인 흐름

위의 그림에서는 국내 및 과외에서 사용되는 DRM 출판의 기본적인 흐름을 표시하였다.

기본적으로 처음 사용자가 CP(Content Provider)에 등록을 하고, CP는 각종 엔터미디어 콘텐츠를 공급하는 회사의 서버를 지칭한다. 사용자가 CP에 등록하게 되면 CPE어서부터 입증서에 하이든스를 위한 사용자 등록을 하게된다. 하이든스를 여러 가지 필요를 채택해 입증서가 사용자측에 전달되면 여기에서는 토큰을 사용하여 전송하는 방식을 사용하였다. 사용자는 이 토큰을 CPE어서로부터 입증서와 콘텐츠를 복호화 할 경우에 사용하게 된다. 사용자는 CPE어서로부터 콘텐츠를 다운로드하고 토큰을 사용하여 콘텐츠를 복호화 할 수 있게 되었다.

3.2. MPEG2 포맷

MPEG2는 MPEG-1에서 시작하여 MPEG2까지 개발되었으며, MPEG-4 규격은 1999년 결정되었다. MPEG는 이제 멀티미디어에서 각각 중심적인 분야가 되었으며 나아가 그 응용분야가 확대되고 있다. MPEG-1과 MPEG2는 비디오 영상의 압축과 복호화 그리고 복호화에서 기능이 증가되어 있으며, MPEG-4는 이제도 영상처리, 회색조의 그래픽스, 내용기반 검색기술 등의 분야로 확대되었다. MPEG-7에는 매체 처리기능, 도트백트 통합처리 기능 등이 포괄되었다. MPEG-21은 인증 기능까지 포함하여 전자상거래분야까지 그 응용분야가 확대된 예정이다.

MPEG-2는 이론의 핵심은 DCT(Discrete Cosine Transform), DPCM(Differential Pulse Code Modulation), 음직임 예측(Motion Estimation)과 음직임 보상(Motion Compensation)이다. DCT의 이론적 원리는 Fourier Transform으로서 공간 압축을 수행한다. DPCM은 PCM 방식을 개선하기 위하여 개발된 부분과 방식으로 신호간의 차이만을 부호화하는 방식이며, MPEG-2 부분에 기본 구조는 DPCM방식으로 되어있다. 음직임 예측과 음직임 보상은 영상에 포함된 품질의 음직임을 부호화하여 시간에 따른 압축을 수행하기 위하여 개발된 방법이다. MPEG-2에서는 전 빠르 뒷쪽 매칭(full search block matching) 알고리즘을 사용하여 음직임 예측을 한다. 음직임 예측과 음직임 보상은 음직임 벡터를 이용하여 표현한다. [4]

3.3. RTP/RTCP

RTP는 오디오, 비디오 및 싱글레이어 데이터와 같은 실시간 대이동 컨테스트 또는 유니버스 네트워크 이용하여 전송하는 음성 서비스에 없었으나 단순·대량 네트워크 전송 기능을 제공한다. RTP는 서버 매출을 수신하지 않으며, 따라서 신호 전달과 같은 서비스 통신도 보장하지 않는다. RTP의 전송 기능은 제어 프로토콜에 의해 작동되며, RTCP의 플러시는 제어 프로토콜은 데이터 전달 채널을 감시하며, 최소한의 제어 기능과 메시지 기능을 제공한다. RTP와 RTCP는 하위의 전송 및 네트워크 계층에 활용하기 위해 설계되었다. RTP는 여러 독립 계층으로 구성되며 다음과 같은 특성 운용에서 요구되는 정보를 제공하여 프로토콜의 처리 과정을 통합시킬 수 있도록 설계되었다. 따라서 기존의 프로토콜들은 달리 RTP는 운용의 필요에 따라 데이터를 변형하거나 추가하여 운용에 있는 프로토콜이 될 수 있도록 하는 인증 및 압축용 프로토콜이다. [2, 3]

여기에서는 RTP에 MPEG2를 탑재 전송하여 실시간 서비스가 가능하도록 하고 있다. [1]

4. 제한 사항

제한하는 사항은 기본적인 DRM 기능을 수행하지만 멀티미디어 데이터의 실시간성 보장을 보장하는 실시간 전송방식과 인증된 사용자를 구분하여 기밀성을 제공할 수 있는 기능을 개선할 필요가 있다. 실시간성을 지원하기 위해서는 Mpeg2 데이터의 Intra Picture를 부분적 압축하여 제한과 RTP를 이용하여 전송함으로써 압축효과/복호화를 지속하는 실시간성을 보장하였다. Mpeg2 데이터의 Intra Picture 압축하는 다음과 같다.

4.1. MPEG-2의 압축과 복호화

MPEG에서는 압축의 가장 기본 단위가 되는 Picture라는 개념이 있다. 그리고 표시된 것은 intra picture에 압축화하여 시간적 압축기술을 사용하지 않고 공간적인 압축기술을 사용해서 압축된 압축량이다. 이 압축기는 주로 다른 픽셀들의 교차부에서 서로의 영향을 줄이며, 시간적인 압축을 사용하지 않기 때문에 주로 시간적에 별도로 복호화가 가능하다. 멀티미디어 콘텐츠는 압축화나 복호화가 불가능한 응용 분야에 많은 시간이 소비된다. 하지만 다른 분야를 제외고 이 Intra picture를 추출하여 압축효과 복호화를 수행하면 시간을 절약할 수 있으며, CPU의 부하를 줄여줄 수 있다. [4]

4.2. 채널화는 DRM 시스템의 흐름

제한하는 DRM 시스템은 기본적인 DRM의 흐름에 따른다. 또한 다른 DRM과 비교할 때 토큰이라는 것을 사용하여 일관적인 복식 방지 및 스크립트 헤더로부터의 복사를 방지한다.
1. Program Downloading

암호화된 스트림 인터페이스 콘텐츠는 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. 인증서명 등록

콘텐츠 서버(CP 서버)는 사용자를 구분할 수 있는 유일한 값을 (예: 주민등록번호) 인증서에 보낸다.

4. 사용자 키 전송

인증서는 콘텐츠 서버(CP 서버)로부터 전송 받을 값을 이용하여 사용자 키를 만든 후 CP 서버로 보낸다. 이 사용자 키는 CP 서버에서 멀티미디어 콘텐츠를 암호화 할 경우 사용되며다.

5. 하드웨어 정보 전송

다음의 프로그램에서의 키 전송은 시스템의 성능을 높이는 하드웨어 정보(당: 하드디스크, 시리얼버터, CPU, 시리얼, 파이선 시크로드 크기, 스타드 커드 시리얼번호 등)를 포함하여 보낸다.

6. 토큰다운로드

인증서에서는 사용자로부터 수신한 하드웨어 정보를 가공하여 내장된 토큰에 압축된 하드웨어 정보를 이용하여 가공 처리한 토큰을 압축해서 내장부로 있다. 이러한 하드웨어 정보는 복사방지에 사용된다.

4.3. 전체 키 관리시스템

\[ H : \text{해쉬 함수, MD5 사용} \]
\[ E : \text{암호화, Rijndael 대칭키 암호화 알고리즘 사용} \]
\[ D : \text{복호화, Rijndael 대칭키 암호화 알고리즘 사용} \]

\[ \text{CP(Content Provider) 서버에서의 키 관리 시스템} \]

\[ \text{UserKey} = H \text{[주민등록번호13] \& SeedKey(16)} \]
\[ \text{FKKey} = H \text{[UserKey(16) \& CP 서버 키(16)]} \]

CP서버는 사용자가 입력한 유일한 값인 주민등록번호와 인증서로부터 얻은 SeedKey 값을 해쉬함수를 이용하여 UserKey를 생성한다. 그 후 실제로 콘텐츠를 암호화할 FKKey는 생성한 UserKey와 CP서버로부터 생성한 토큰값을 이용하여 생성한다.

- 인증 서버에서의 키 관리 시스템

\[ \text{SeedKey} = H \text{[주민등록번호13]} \]
\[ \text{UserKey} = H \text{[주민등록번호13] \& SeedKey(16)} \]
\[ \text{EncUserKey} = E \text{[TempKey \& UserKey(16)} \]
\[ \text{TempKey} = H \text{[인증서 서버 키(16)] \& 하드웨어 정보(16)} \]

인증서에서는 CP서버로부터 얻은 값을 사용자 정보를 사용하여 SeedKey를 생성한다. 이 SeedKey는 CP서버에 전송하여 되어있는 인증서에서도 CP서비와 동일한 방법을 사용하여 UserKey를 생성한다. 그 후 콘텐츠로부터 토큰드로트 요구 시 요구 값을 전송하여 은 하드웨어 정보를 사용하여 EncUserKey를 생성한다. 토큰은 [인증서 서버 키(16)] EncUserKey(16) 레벨로 만들여 클라이언트에게 보내진다.

- 클라이언트측에서의 키 관리

\[ \text{UserKey} = D \text{[TempKey \& EncUserKey(16)]} \]
\[ \text{TempKey} = H \text{[인증서 서버 키(16)] \& 하드웨어 정보(16)} \]
\[ \text{FKKey} = H \text{[UserKey(16) \& CP 서버 키(16)]} \]

클라이언트에서는 토큰을 비트로 다른 스탠드와 같은 장소에 보관하고 있다가 콘텐츠 복호화 시 이를 사용하여 UserKey를 복호화 시킨다. 이후 콘텐츠를 암호화한 FKKey를 얻기 위해서 암호화된 콘텐츠의 해머에 담겨 있는 CP서버 키값과 EncUserKey로부터 복호화된 UserKey를 이용하여 콘텐츠 복호화에 필요한 FKKey를 얻는다.

5. 결론


6. 참조

[1] RTP Payload Format for MPEG1/MPEG2 Video (RFC 2250)
[3] RTP Profile for Audio and Video Conferences with Minimal Control (RFC 1889)
[4] "암호화된 MPEG-2" 애플리케이션, 김강준, 홍성공학대학교
[6] The MD5 Message-Digest Algorithm (RFC 1321)