적응성 있는 안전한 멀티미디어 데이터 전송 프레임워크에 관한 설계*

김일희**, 이길주**, 박용수**, 조성제***, 조유근****

**한양대학교 정보통신대학 컴퓨터전공

***단국대학교 자연과학대학 정보컴퓨터학부

****서울대학교 공과대학 전기컴퓨터공학부

Design of a Secure and Adaptive Transmission Framework for Multimedia Contents Distribution

Il-Hee Kim**, Gil-Ju Lee**, Yongsu Park**, Seungje Cho***, Yookun Cho****

**College of Information and Communications, Hanyang University,

***Department of Information and Computer Science, Dankook University,

****School of Electrical Engineering and Computer Science, Seoul National University.

요 약

인터넷의 발달로 네트워크를 통한 멀티미디어 데이터 서비스가 늘어나면서 유료 콘텐츠에 대한 저작권 관리와 보호 및 다양한 이기종의 단말 장치에 적합한 콘텐츠 적응(adaptation) 서비스에 대한 필요성이 높아지고 있다. 이를 위하여 현재까지 DRM, Scalable Coding, Progressive Encryption, ISMA, ARMS, Metadata Adaptation 등 다양한 연구가 진행되어 왔지만 요구사항을 포괄적으로 만족하는 멀티미디어 전송 프레임워크는 부재한 상태이다. 이에, 본 논문에서는 기존 기법을 분석하고 기능을 통합하여 안전하고 보다 여러 종류의 단말 장치에 서비스가 가능하며 다양한 서비스 형태를 가질 수 있는 프레임워크를 설계하였다. 이를 통해 멀티미디어 서비스가 보다 광범위하게 활용되고 확산 될 수 있으리라 기대된다.

I. 서론

멀티미디어 콘텐츠 증가와 멀티미디어 데이터의 재생 기기의 다양화로 인해 대두되는 두 큰 필요성을 낳게 되었다. 첫째는 유료 멀티미디어 콘텐츠에 대한 보호이고, 둘째는 이질적인 클라이언트 기기에 맞도록 멀티미디어 데이터를 변환하여 제공해야 하는 일이다.

멀티미디어 콘텐츠에 대한 보호 서비스를 세분화 하면 적합한 사용자 이외의 사용자가 유료의 콘텐츠를 이용하는 문제와 저작권에 의해 보호되어야 하는 콘텐츠를 불법적으로 위변조하는 문제, 그리고 end-to-end security 보장문제가 있을 수 있다.

멀티미디어 데이터 변환 서비스가 필요한 이유는 현재, 멀티미디어 데이터를 표현해주는 장치가 데스크탑 PC나 노트북과 같은 고해상도 및 다양한 데이터 포맷을 지원하는 장치에서부터 PDA나 휴대폰과 같은 저해상도의 데이터와 특정 포맷의 데이터만 플레이할 수 있는 기기까지 다양하게 존재한다. 그렇기 때문에 멀티미디어 콘텐츠가 이질적인 클라이언트 기기에 적합하게 표현될 수 있도록 해상도나 비트레이트, 파일 포맷 등을 변환해주어야 한다.

* 본 연구는 학술진흥재단 지원 2005년도 협동연구자지원사업과 2006년도 한국정보보호진흥원의 위탁과제 연구 결과로 수행되었습니다.

추가적으로 멀티미디어 데이터에는 광고나 로고 혹은 추가정보가 들어가는 경우가 많으며 이를 위해 이들 정보를 가지고 있는 메타데이터를 어댑테이션하는 기법이 필요하다.

본 연구에서는 위와 같은 멀티미디어 서비스의 요구사항들을 만족시키기 위하여, 기존의 연구 결과를 조사하고, 이를 토대로 적응성 있는 안전한 멀티미디어 데이터 전송 프레임워크를 설계하였다. 멀티미디어 서버와 사용자 단말장치 사이에 네트워크 트랜스코더를 두고 메타데이터 어댑테이션 기법을 이용하여 전송되는 데이터를 각 단말장치에 맞는 데이터로 변환하여 서비스해 준다. 아울러 메타데이터 어댑테이션 기법을 통해 광고 등의 부가서비스를 제공함으로써 멀티미디어 콘텐츠 서비스 형태를 좀 더 다양하게 제공할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. II장에서는 관련 연구에 대해 설명하고 III장에서는 II장의 관련 연구를 바탕으로 새롭게 설계된 적응성 있는 안전한 멀티미디어 데이터 전송 프레임워크를 설명하였다. 마지막으로 IV장에서는 결론을 맺는다.

II. 관련연구

1. Scalable Coding

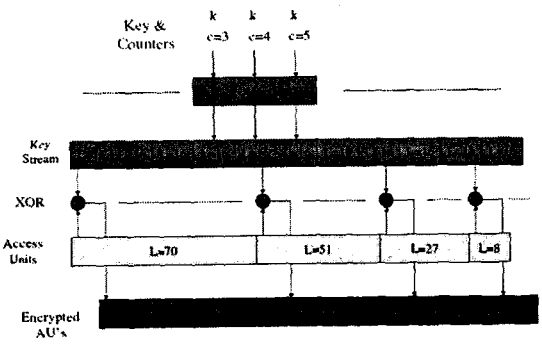
Scalable Coding은 스트림 데이터의 앞부분 만을 가지고도 복호화하여 서비스 할 수 있는 인코딩 기법으로 전송받는 스트림 데이터의 양에 따라서 화질이나 크기가 차이나는 특징이 있다. [3]

2. Progressive Encryption

Progressive Encryption은 Cipher block chains 기법과 Stream ciphers 기법이 있는데 Cipher block chains 기법은 우선 작은 평문을 암호화하고 이 암호화 된 암호문을 가지고 그 다음에 나오는 평문과 XOR 연산을 한다. 암호문과 평문을 XOR한 결과를 가지고 그 다음 블록을 암호화 해가는 방식이다. Stream ciphers 기법은 스트림 데이터를 bit단위로 암호화 하는데, 키스트림 생성기에서 만들어진 Running Key라고 하는 스트림데이터와 XOR연산을 하여 암호화하게 된다. 이 두 암호화의 특징은 앞의 일부분만으로도 순차적으로 복호화를 할 수 있다는 것이다. [3]

3. ISMA [5]

ISMA는 암호화 스트리밍 데이터 전송을 위해 대칭키 알고리즘을 사용하여 암호화 하고 전송을 위해 RTP 프로토콜을 UDP 위에서 적용한다. 대칭키 알고리즘으로 DES, 3DES, AES 등 다양한 알고리즘이 적용 가능하다. 이들 블록 암호화 알고리즘은 특정 길이의 블록만을 암호화 할 수 있기에 긴 미디어 데이터를 암호화하기 위해서 암호화 모드가 필요하다. ISMA에서 사용할 수 있는 여러 가지 암호화 모드 중에서 ARMS에 적합한 암호화 모드는 카운터 모드이다. 아래 그림은 AES 알고리즘을 카운터 모드를 이용하여 암호화 한 후 RTP 패킷을 만들기 위한 AU (Access Unit)을 만드는 과정을 보여주고 있다.



<그림1> AES 알고리즘과 카운터 모드를 이용한 RTP패킷 암호화 과정

이 그림에서 AES는 128비트 (16바이트) 단위로 동작하며 카운터 모드에 사용하는 카운터 c 값 역시 128비트를 갖는다. 카운터를 1씩 증가하면서 키 k를 이용하여 AES로 암호화 한 후, 생성된 키 스트림을 (각각 128비트 블록) 미디어 데이터의 Access Units (예: 비디오 프레임)에 XOR 연산을 수행하면 암호화된 Access

Unit이 생성된다.

그 후 암호화된 AU를 가지고 RTP 패킷을 생성하여 전송한다. 이 때, 각 RTP 패킷은 헤더가 있어 헤더에 카운터값을 넣게 되어 있다. 헤더에 들어가는 카운터 값은 c보다 4비트 큰데, 그 이유는 c는 RTP 패킷 내 첫 암호화 16 바이트 M을 풀기 위한 카운터 값을 의미하며, 4비트 정보는 암호화 시 M이 각 16 바이트 블록의 어느 부분부터 시작하는지를 의미한다.

매 RTP 패킷마다 132 비트 카운터를 넣는 것은 통신 오버헤드가 매우 크기 때문에 통상 이 중 LSB 16-24비트만을 넣게 된다. 그러면 수신자는 2^16 - 2^24비트 데이터가 손실이 생겨도 올바른 카운터 값을 추측할 수 있다.

4. ARMS [5]

우리가 대칭키의 counter 모드를 사용하여 암호화 작업을 수행 시 중요한 점이 카운터 값은 계속 증가해야하며 같은 키 K에 대해 이전에 사용한 카운터값을 재사용하면 보안상 허점이 생긴다는 것이다. 이에, ARMS는 하나의 미디어 콘텐츠에 대해 여러 개의 adaptation 된 스트림 데이터가 있어 이를 ISMA 상에서 적응력 있게 서비스 해 줄 경우, 카운터 값을 재사용하지 않으면서 가능한 RTP 헤더의 크기를 줄이고, 긴 패킷 손실을 견디는 방법을 제공한다.

5. Meta-data Adaptation [4]

멀티미디어 콘텐츠의 메타데이터에는 멀티미디어 데이터의 속성정보 - 화면 해상도, 비트레이트, 암호화된 미디어 데이터의 복호화를 위한 Right Object 정보가 포함되며 메타데이터는 통상 서비스 공급자와 사용자 단말간에 XML데이터 교환을 통해 처리된다.

메타데이터 어댑테이션은 서비스 공급자가 이미 생성된 미디어 콘텐츠에 광고 콘텐츠나 로고를 추후 삽입하거나 추가의 정보를 제공하기 위해 사용하는 기술이며, 사용자 인증을 위해 인증트리를 이용한다.

III. 제안 프레임워크

본 절에서는 서론에서의 요구조건을 만족시키는 제안 프레임워크를 설명한다.
그림2는 제안 프레임워크를 도식화 한 것이다.

<그림2> 적응성 있는 안전한 멀티미디어 데이터 전송 프레임워크

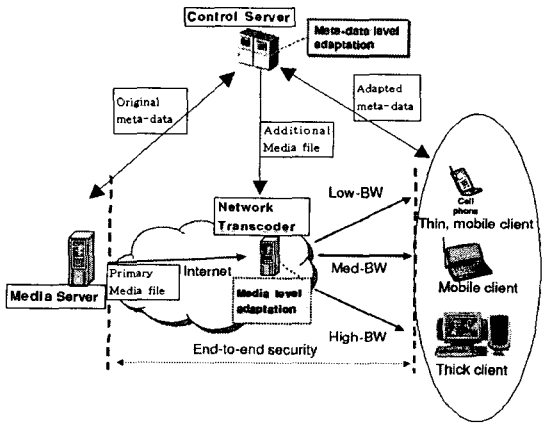


그림2의 좌측에 있는 Media Server가 멀티미디어 콘텐츠를 제공하는 서버이고 가운데 있는 Network Transcoder가 멀티미디어 데이터를 각 단말장치에 맞는 형태로 변형하여 서비스 해주는 서버이며 상단의 Control Server가 Media Server와 Network Transcoder 그리고 단말장치간의 통신을 통해 메타데이터를 주고받으며 적응성 있는 미디어 데이터 서비스를 관리해준다.
Control Server는 또한 사용자 인증 서버 및 광고 콘텐츠 제공 대행 서버의 역할도 수행한다.

서비스 시나리오는 다음과 같다.
① 각 단말 장치에서 Control Server에게 멀티미디어 콘텐츠를 요청하면 Control Server는 요청한 사용자가 적법한 사용자인지 인증과정을 수행한다.
② 그리고 Media Server에게 제공할 서비스의 메타데이터 (XML)를 받아서 복호화를 위한 Right Object를 추가한 후 단말장치에 보내준

다.

③ 단말 장치에서는 받은 메타데이터에 자신의 단말정보 (해상도나 처리능력등)를 포함하여 Network Transcoder에게 메타데이터를 전송하여 다시 콘텐츠를 요청한다.

④ Network Transcoder는 XML정보를 분석하여 Media Server와 Control Server에게 각각 미디어 데이터를 요청한다. Media Server로부터는 사용자가 요청한 원래의 미디어 콘텐츠이고, Control Server로부터 받은 데이터는 광고나 안내를 위한 미디어 데이터이다. 이 때 전달되는 미디어 데이터는 ISMA기법으로 Progressive Encryption하여 전송을 한다.

⑤ Network Transcoder에서는 각각의 서버로부터 받은 미디어 데이터를 메타데이터 안에 있는 단말정보를 가지고 해상도와 비트레이트를 변환하여 단말장치에게 보내주게 된다. Network Transcoder에서의 데이터 변환은 실시간으로 적용되며 동시에 여러 사용자의 요청을 처리해야 하기 때문에 변환에 드는 처리 비용을 최소화해야 한다. Media Server와 Control Server로부터 받는 미디어 데이터는 Scalable Coding과 Progressive Encryption을 하여 전송하기 때문에 Network Transcoder에서의 변환 작업은 많은 연산을 요구하는 것이 아니라 단지 받은 데이터의 특정 부분을 잘라 버리는 것만으로 필요한 해상도로의 변환이 가능하다. 그래서 변환에 드는 비용을 최소화 할 수 있게 된다. 아울러 전송되는 패킷은 Media Server에서부터 단말장치까지 모두 암호화된 패킷이 전송되고 중간에 복호화 과정이 없기 때문에 End-to-End Security를 보장할 수 있다.

⑥ 최종적으로 단말 장치에서는 받은 미디어 데이터를 메타데이터 안에 있는 Right Object를 이용해서 복호화 하여 콘텐츠를 볼 수 있게 된다.

IV. 결론

본 논문에서는 적응성 있는 안전한 멀티미디어 데이터 전송 프레임워크를 제안하였다. 이를 이용하면 이질적인 단말 장치에 맞는 미디어 서비스를 안전하게 제공할 수 있다. 뿐만 아니라 각종 부가 서비스도 가능하기 때문에 유료 콘텐츠를 비용 없이 보기를 원하는 사용자에게는 유료 콘텐츠 중간 중간에 광고가 나오도록 멀티미디어 콘텐츠를 매타데이터를 통해 변형하여 서비스 하는 새로운 서비스 방식을 시도해 볼 수 있다. 이 외에도 메타데이터를 활용하여 다양한 응용서비스도 고안할 수 있는 기반을 마련하였다고 할 수 있겠다.

[참고문헌]

[1] D. Holankar et al., Secure Streaming Media and DRM, in Proceedings of the 2004 Hawaii International Conference on Computer Science, Honolulu, Hawaii, January 2004.

[2] J. G. Apostolopoulos et al., Secure Media Streaming & Secure Adaptation for Non-Scalable Video, IEEE ICIP'2004.

[3] Susie Wee, Secure Scalable Streaming Enabling Transcoding without Decryption, 2001.

[4] T. Suzuki et al., A System for End-to-End Authentication of Adaptive Multimedia Content, in Proceedings of Int. Conf. on Comm. & Multimedia Security, 2004.

[5] C. Venkatramani et al., Securing Media for Adaptive Streaming, ACM MM'03, 2003.

[6] Susie Wee, John Apostolopoulos, Secure Scalable Streaming and Secure Transcoding with JPEG-2000, 2003.