다중기기 시청 환경을 지원하기 위한 SVC와 CAS 결합 기법*

손정갑, 이훈정, 오희국
한양대학교 컴퓨터공학과
e-mail: jgson@infosec.hanyang.ac.kr

SVC and CAS Combining Scheme for Support Multi-Device watching Environment*

Junggab Son, Hoonjung Lee, Heekuck Oh
Dept of Computer Science and Engineering, Hanyang University

요 약

IPTV나 DTV에서 사용하는 CAS는 하나의 스트리밍으로 하나의 콘텐츠만을 전송하는 환경이지만 SVC와의 결합을 통해 사용자의 다양한 비디오 어플리케이션을 단일 스트리밍으로 지원하도록 개선할 수 있다. 이러한 환경에서는 효율성을 우선적으로 설계하여야 하며, 서비스 등급별 과금 정책을 위해 계층적 키 관리 기법의 적용이 필요하다. 본 논문에서는 CAS에 SVC를 적용함에 있어 발생할 수 있는 문제점들에 대해 살펴보고 CAS환경에서의 SVC 암호화기법에 대해 제안한다. 제안하는 기법의 안전성은 기존 CAS와 단방향 해시 함수의 안전성에 기반하며, 기존 CAS에 비교적 적은 오버헤드로 적용이 가능하다는 장점이 있다.

1. 서론

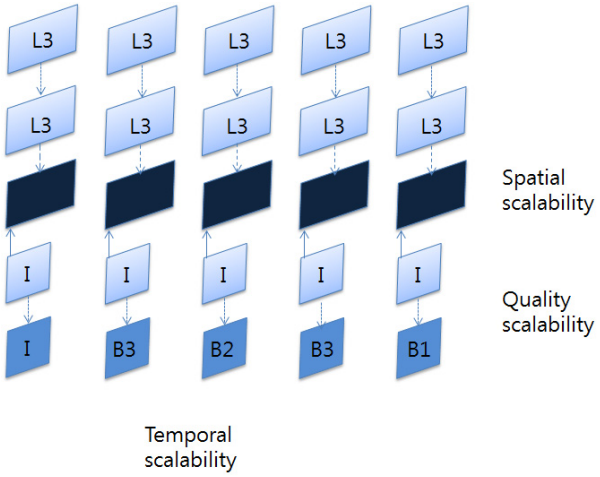
IPTV나 DTV 등 사용자에게 유료 서비스를 제공하는 방송환경에서는 합법적인 사용자만 서비스에 접근할 수 있도록 하기 위하여 접근제한시스템(Conditional Access System, CAS)를 사용한다. 기존 접근제한시스템은 하나의 스트림을 통해 한 형태의 콘텐츠를 사용자에게 전달하도록 설계되었다. 하지만 비디오 코딩 기술과 장비의 발달로 인해 다양한 비디오 어플리케이션이 생겨나고 콘텐츠를 시청할 수 있는 기기가 다양해짐에 따라 사용자의 편의를 위해 여러 단말에서 서비스를 이용하고자 하는 사용자의 욕구가 증가하고 있다. 이러한 사용자의 욕구를 만족시키기 위하여 접근제한시스템을 다양한 기기를 사용하는 환경에 적합하도록 개선하는 것이 필요하다.

사용자의 다양한 시청환경은 콘텐츠가 여러 형태로 코딩 되어야 됨을 의미하며, 하나의 스트리밍을 사용하는 방송 시스템의 전송 구조에서 SVC(Scalable Video Coding)은 상당히 매력적인 기술이다. SVC는 하나의 콘텐츠를 서비스 형태에 따라 가변적으로 사용할 수 있도록 포맷을 변환하는 방식으로, 계층적 코딩 방식을 사용하기 때문에 HD TV 용으로 제작된 콘텐츠를 별다른 인코딩 없이 Mobile 기기에서 시청할 수 있다는 장점이 있다.

일반적으로 방송환경에서는 화질에 따라 요금이 달라진다. 일반 방송과 HD방송의 가격이 다른 것이 그 예이다. 따라서, SVC를 적용함에 있어 계층적 키 관리를 통하여 서비스의 품질에 따라 서비스의 등급을 구분할 수 있어야 하며, 사용자가 선택한 서비스 품질에 맞는 콘텐츠만 수신할 수 있도록 제한적 서비스 수신이 가능하여야 한다. 또한, HD TV부터 모바일 단말까지 다양한 시청 환경을 보장하기 위하여 암호화 기법의 효율성을 보장하는 것이 중요하다.

본 논문에서는 접근제한시스템과 SVC의 연동에 대해 발생하는 문제들에 대해 살펴보고 효율적인 계층 관리를 위한 키 관리 시스템에 대해 제안한다.

* "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2011- C1090 - 1111 - 0010)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No.2011-0000189).



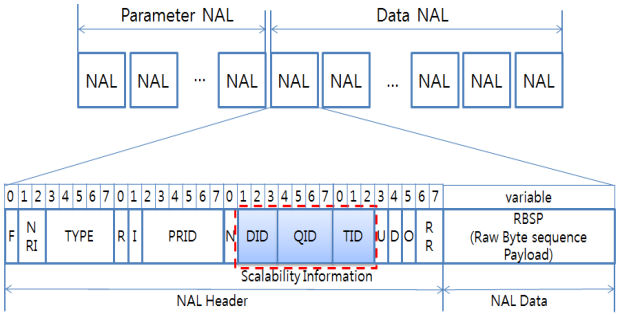
(그림 1) SVC의 개념도

논문의 구성은 다음과 같다. 2장에서 SVC구조에 대해 살펴보고 3장에서 SVC 암호화 기법과 이를 CAS에 적용해 본 후 4장에서 결론을 맺는다.

2. H.264/ SVC

일반 사용자에게 보다 편리한 사용자 인터페이스 환경을 제공하기 위해서는 현재의 윈도우즈의 기반 사용자 인터페이스의 차원을 넘어서 사용자의 작업을 대행해 줄 수 있는 에이전트 시스템이 제공되어야 한다. 또한 에이전트 시스템서비스 확장과 사용보급을 위하여 응용을 위한 미들웨어 플랫폼에 대한 연구개발이 이루어져야 한다. SVC는 spatial, temporal, quality scalability를 통해 높은 코딩 효율성을 제공한다. spatial scalability는 layered coding을 통해 제공하며, 이미지의 해상도를 조절한다. temporal scalability는 계층적 구조를 통해 제공하며, 프레임 수를 결정한다. quality scalability는 특별한 형태의 spatial scalability로 볼 수 있으며, base layer와 enhancement의 크기를 결정한다. SVC는 하나의 base layer와 다수의 enhancement layer로 구성되어 있으며, base layer는 가장 낮은 품질의 원본 비디오가 포함되어 있다. Enhancement layer는 base layer에 추가되어 보다 높은 품질의 영상을 얻을 수 있도록 설계되었으며, 모든 enhancement layer가 base layer에 결합되었을 때, 스트림이 가지는 가장 고화질의 영상을 획득할 수 있다[3]. (그림 1)은 SVC의 구조를 나타낸다.

다양한 전송 환경에서 SVC를 전송하기 위해서, VCL(Video Coding Layer)과 NAL(Network Abstract layer)를 분리하였다. NAL은 VCL 데이터

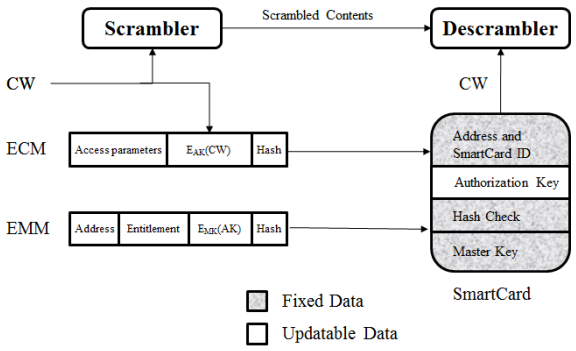


(그림 2) SVC NAL의 구조

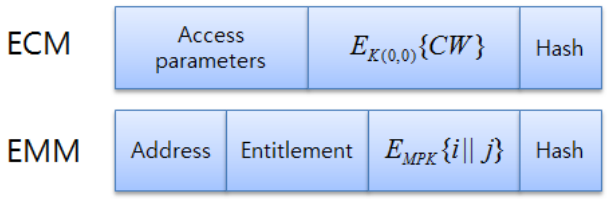
의 대략적인 전송정보를 제공한다. SVC는 NAL unit 단위로 구성되어 있으며, NAL의 크기는 가변적으로 구성할 수 있다. (그림 2)는 NAL의 구성을 나타낸다. NAL Header는 scalability 정보가 포함되며, NAL 데이터는 인코딩 된 비디오 데이터가 들어있다. DID(Dependency ID), QID(Quality ID), TID(Temporal ID)를 통해 scalability 정보를 표현하며, Scalability 정보는 NAL Header 내에 들어기 때문에 SVC를 암호화할 때에는 반드시 NAL unit 단위로 암호화하여야 한다. SVC에 관한 자세한 내용은 표준화 문서[4]를 통해 알 수 있다.

3. 접근제한시스템

CAS는 사용자의 조건에 따라 접근을 제한하는 시스템으로 유료 TV 시스템에서 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 솔루션이다[1-2]. CAS는 크게 두 가지 기능을 수행한다. 첫째는 CSA(Common Scrambling Algorithms)라는 스크램블링 알고리즘을 사용하여 콘텐츠를 스크램블링/디스크램블링 하는 기능이고, 두 번째는 스크램블링/디스크램블링에 필요한 여러 키들을 계층적으로 관리하는 기능이다. (그림 3)은 CAS의 구성도이다. SMS (Subscriber Management



(그림 3) CAS의 개념도



(그림 4) 제안하는 기법을 통해 전송되는 EMM/ECM

System)는 CW (Control Word)를 생성하고 생성된 제어 단어를 이용해 방송 콘텐츠를 스크램블링하여 전송한다. 이때 생성된 CW는 AK (Authorization Key)로 암호화되어 ECM (Entitlement Control Message)을 통해 전송되고, AK는 각 사용자의 스마트카드에 저장되어 있는 MPK (Master Private Key)로 암호화 되어 EMM (Entitlement Management Message)을 통해 전송된다. 수신측에는 송신측과 반대의 과정을 수행하게 되는데 EMM의 EMPK{AK}를 복호화하여 자신의 스마트카드에 저장되어 있는 AK를 갱신하고, ECM의 EAK{CW}를 복호화한 후, 제어 단어를 이용해 콘텐츠를 디스크램블링하여 시청 할 수 있게 된다.

최근에는 DCAS, iCAS 등 새로운 형태의 CAS가 많이 개발되었지만 기본적인 동작 원리는 기존 CAS와 동일하므로 본 논문에서는 CAS를 기반으로 제안하는 기법을 설계한다.

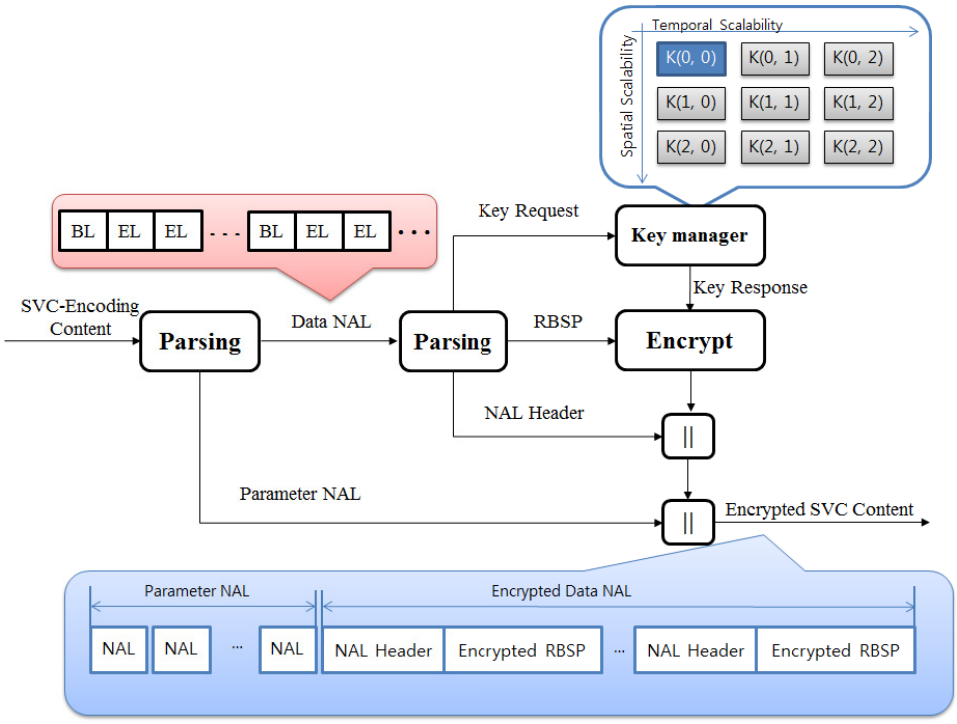
3. 제안하는 기법

본 논문에서는 CAS와 SVC 결합 환경을 위한 암호화 기법에 대해 제안한다. SVC에서 보다 고화질의 영상을 얻기 위하여 base layer에 enhancement layer가 계층적으로 결합되는 구조에서는 단일 계층의 키를 사용할 경우 상위 layer에 대해 원치 않는 노출이 발생할 수 있기 때문에 바람직하지 않다. 또한, Quality layer는 특별한 형태의 Spatial layer로써 화면 크기를 조절하기 위해 사용되므로 효율성을 위해 같은 서비스 등급의 Spatial layer에 적용된 키와 동일한 키를 사용한다.

서비스제공자는 (그림 5)와 같은 2차원 키 배열을 생성하여 SVC를 NAL unit 단위로 암호화 한다. 키 생성 과정은 다음과 같다.

1. i와 j를 랜덤하게 생성한다.
2. i-1=H(i), j-1=H(j)를 i~0, j~0까지 계산한다.
3. K(i, j)=i||j 식을 적용하여 (그림 5)와 같은 키 배열을 생성한다.

위와 같이 키 배열을 생성한 후, 서비스제공자는 SVC로 인코딩된 콘텐츠를 암호화한다. 먼저 콘텐츠가 암호화 모듈에 입력되면 첫 번째 parser는



(그림 5) 제안하는 기법의 블록 다이어그램

Parameter NAL 과 Data NAL을 분리하여 Data NAL을 두 번째 parser에게 전달한다. 두 번째 parser는 NAL unit으로부터 NAL header와 RBSP를 분리하여 RBSP를 Encrypter에게 전달하고 Key manager에게 scalability정보를 전달하면 key manager는 그에 맞는 key를 encrypter에게 전달한다. encrypter를 통해 암호화된 RBSP는 NAL Header와 결합하여 NAL unit의 형태로 생성되게 되며, 생성된 NAL unit들은 parameter NAL 과 결합하여 초기의 SVC와 동일한 형태가 된다.

CAS에서 콘텐츠 전송을 위해 서비스제공자는 사용자가 원하는 품질에 맞는 (i, j)를 선택하여 CAS의 AK 대신 포함하여 전달한다. 사용자가 base layer만 시청할 경우, AK=(0 ,0)이 된다. base layer를 얻지 못하면 영상을 디코딩할 수 없으며, (i, j)를 통해 항상 K(0, 0)을 획득할 수 있으므로, CW는 K(0, 0)으로 암호화하여 전송한다. 이를 CAS에 적용하면 EMM과 ECM은 [그림 3]과 같이 표현된다.

4. 분석

CAS에서 AK는 주로 프로그램 단위 혹은 채널 단위(채널 단위일 경우 보통 하루)의 비교적 긴 갱신주기를 가지며, CW는 보통 10~25초의 짧은 갱신주기를 가진다[5]. SMS로부터 (i, j)를 전송받은 사용자 기기는 자신이 선택한 품질 수준의 2차원 키 배열을 생성한 후, 이것을 콘텐츠 복호화에 사용한다. 2차원 배열은 프로그램 시청시작 시 혹은 갱신 시 한번만 생성하면 되므로 비교적 오버헤드는 작은 편이지만, 계층별로 복호화하는 과정에서 추가적인 오버헤드가 발생한다. 갱신되는 CW를 처리하는 부분에서는 기존 CAS와 동일한 오버헤드를 가진다. 제안하는 기법의 안전성은 주기적으로 CW가 갱신되는 CAS의 안전성과 단방향 해시 함수의 안전성에 기반한다.

5. Conclusion

본 논문에서는 CAS와 SVC 결합 환경을 위한 암호화 기법을 제안하였다. 제안하는 기법은 기존 CAS의 AK 대신 계층적으로 키를 관리할 수 있는 비밀값을 전달하여 사용자가 원하는 품질 수준의 서비스를 이용할 수 있도록 하였다. 제안하는 기법은 2차원 배열의 키 생성을 시청 초기단계로 국한시켜 SVC 적용에 따른 오버헤드를 최소화하였다.

참고문헌

[1] EBU Project Group B/CA, Functional model of a conditional access system, EBU Technical Review, Winter 1995.

[2] ETSI Technical Report 289: Support for use of scrambling and Conditional Access within digital broadcasting system, 1996.

[3] Heiko Schwarz, Detlev marpe, Thomas Wiegand, “Overview of the Scalable Video Coding Extension of the H.264/AVC Standard,” IEEE Transactions on circuits and systems for video technology, vol.17, no.9, SEP 2007.

[4] Advanced Video Coding for Generic Audiovisual Services, ITU-T Rec. H.264 Version 8 (including SVC extension): Consented in July 2007.

[5] M. Zhu, M. Zhang, X. Chen, D. Zhang and Z. Huang. “Hierarchical key distribution scheme for conditional access system in DTV broadcasting,” International Conference on Computational Intelligence and Security, pp.1532 - 1535, 2006.