Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1111

다중기기 시청환경을 지원하기 위한 SVC와 CAS 결합 기법*

손 정 갑,[1†] 오 희 국,[1] 김 상 진[2‡]
[1]한양대학교, [2]한국기술교육대학교

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

Junggab Son,[1†] Heekuck Oh,[1] SangJin Kim[2‡]
[1]Hanyang University, [2]Korea University of Technology and Education

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 적용하기 위해 고려해야할 점들에 대해 살펴보고 CAS를 통해 암호화된 SVC 콘텐츠를 전송하는 모듈을 제안한다. 제안하는 기법을 적용하면 단일 스트림을 사용하는 CAS 에서도 다중기기를 이용하여 콘텐츠를 시청할 수 있으며, 사용자에게 시청 화질에 따른 과금 부과가 가능하다. 제안하는 기법의 안전성은 CAS와 단방향 해시 함수의 안전성에 기반한다. 또한, 실험 결과 10%미만의 적은 오버헤드로 스트리밍 서비스 되는 SVC 콘텐츠를 안전하게 보호할 수 있다는 장점이 있다.

ABSTRACT

CAS used in IPTV or DTV has an environment of sending single type of contents through single streaming. But it can be improved to support users' various video applications through single streaming by combining with SVC. For such an environment, efficiency should be firstly considered, and hierarchical key management methods for billing policy by service levels should be applied. This study aims to look into considerations to apply SVC to CAS and propose SVC encryption in CAS environment. The security of the proposed scheme is based on the safety of CAS and oneway hash function. If the proposed scheme is applied, scalability can be efficiently provided even in the encrypted contents and it is possible to bill users according to picture quality. In addition, the test results show that SVC contents given by streaming service with the average less than 10%overhead can be safely protected against illegal uses.

Keywords: IPTV, CAS, SVC, streaming service

접수일(2013년 7월 8일), 수정일(2013년 10월 8일), 게재확정일(2013년 11월 12일)
* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (no. 2012-R1A2A2A01046986).
* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임 (no. 2012-R1A1A2009152).
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0301-13-1002)
† 주저자, jgson@infosec.hanyang.ac.kr
‡ 교신저자, sangjin@kut.ac.kr(Corresponding author)

I. 서 론

IPTV나 DTV 등 사용자에게 유료 서비스를 제공하는 방송환경에서는 합법적인 사용자만 서비스에 접근할 수 있도록 하기 위하여 접근제한시스템(Conditional Access System, CAS)를 사용한다[1], [2]. 기존 접근제한시스템은 하나의 스트림을 통해 한 형태의 콘텐츠만을 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 환경을 지원하기 위하여 접근제한시스템을 다양한 기기를 사용하는 환경에 적합하도록 개선하는 것이 필요하다.

실시간 스트리밍 서비스는 국내에서 KT가 글로벌 온라인 방송 플랫폼 업체 유스트림과 협력해 유스트림 코리아를 설립하였으며, 해외에서는 영국BBC월드와 이드가 미국의 동영상 실시간 재생서비스 플랫폼 제공업체인 ViKi에 투자하는 등 관심이 날로 높아지고 있다[3]. 이러한 실시간 서비스는 사용자의 다중기기 시청환경을 반영하여 제공될 것이며 이를 위한 적절한 콘텐츠 보호기법이 필요하게 될 것이다. 콘텐츠 보호기법은 사용자의 다양한 기기를 통한 시청환경을 지원할 수 있어야 한다.

사용자의 다양한 시청환경은 콘텐츠가 여러 형태로 인코딩 되어야 함을 의미하며, 다중 스트림을 사용하기 힘든 방송 시스템에서 SVC(Scalable Video Coding)는 상당히 매력적인 기술이다. SVC는 계층적 코딩 방식을 사용하며 하나의 스트림으로 HD TV용 콘텐츠와 Mobile 기기용 콘텐츠를 모두 지원할 수 있다[4].

본 논문에서는 기존 방송환경에서 실시간 방송을 보호하기 위해 사용하였던 CAS에 SVC기법을 결합하여 CAS를 통해 SVC 인코딩 된 콘텐츠를 전송하는 방법으로 다중기기 시청환경을 지원하는 기법을 제안한다. CAS와 SVC 결합 환경에서 고려해야 할 점은 다중기기 시청 환경에서도 등록된 기기에서만 콘텐츠 재생이 가능해야 하며, SVC의 계층적 구조에 적합한 암호기법이 필요하다. 또한, 다양한 시청 환경을 보장하기 위하여 암호기법의 효율성을 보장하여야 하며, 현재의 시스템과의 호환성을 위하여 가급적이면 변경이 적은 편이 유리하다. 논문에서는 제안하는 모듈을 실제 구현하여 CAS를 통해 SVC 콘텐츠를 전송할 수 있음을 보인다.

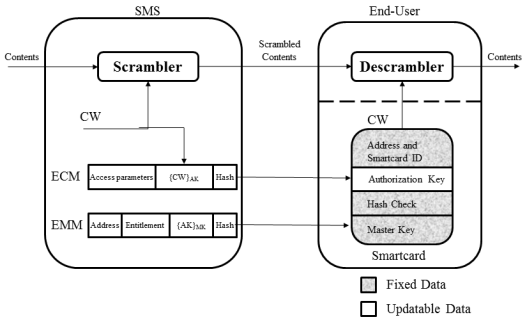

Fig.1. CAS Overview

논문의 구성은 다음과 같다. 2장에서 관련연구에 대해 살펴보고 3장에서 제안하는 기법에 대해 서술한다. 4장에서 제안하는 기법을 안전성과 효율성 측면에서 분석하고 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1 접근제한시스템

접근제한시스템(Conditional Access System, 이하 CAS)은 사용자의 조건에 따라 접근을 제한하는 시스템으로 유료 TV 시스템에서 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 솔루션이다[1], [2]. 하드웨어와 소프트웨어의 결합 즉, 스마트카드와 스크램블링의 결합을 통하여 콘텐츠의 안전성을 보장한다. 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. Fig. 1. 은 CAS의 구성도이다. SMS (Subscriber Management 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. 생성된 EMM, ECM은 스크램블링된 콘텐츠 스트림에 포함되어 TS(Transport Stream)으로 전송되게 된다.

수신측에는 송신측과 반대의 과정을 수행하게 되는데 TS로부터 EMM/ECM을 추출하여 스마트카드로 전송하면 스마트카드는 MPK로 EMM의 $E_{MPK}\{AK\}$를 복호화하여 자신의 스마트카드에 저장되어 있는 AK를 갱신하고, ECM의 $E_{AK}\{CW\}$를 복호화한 후, CW를 디스크램블러로 전송한다. CW를 전송받은 디스크램블러는 이를 이용해 콘텐츠를 디스크램블링하여 시청 할 수 있게 된다.

최근에는 DCAS (Downloadable CAS), iCAS (Interchangeable CAS), XCAS (eXchangeable CAS) 등 새로운 형태의 CAS 가 많이 개발되었다[3], [4]. 기본적인 동작 원리는 기존 CAS와 유사하므로 본 논문에서는 CAS를 기반으로 제안하는 기법을 설계한다.

2.2 SVC

SVC (Scalable Video Coding)는 temporal scalability, spatial scalability, quality scalability를 통해 높은 코딩 효율성을 제공하며, SVC를 통해 여러 계층의 영상을 하나의 비트스트림으로 제공할 수 있다[5], [6]. SVC는 H.264/AVC (Advanced Video Coding)과 호환성을 유지하는 Base Layer (BL)와 BL과의 결합을 통해 보다 향상된 품질의 영상을 제공할 수 있는 다수의 Enhancement Layer (EL)로 구성된다. BL은 가장 낮은 품질의 원본 비디오가 포함되어 있다. EL은 BL에 추가되어 보다 높은 품질의 영상을 얻을 수 있도록 설계되었으며, 모든 EL이 BL에 결합되었을 때, 스트림이 가지는 가장 고화질의 영상을 획득할 수 있다[7]. 이를 통해 temporal, spatial, quality 측면에서의 다양한 scalability와 H.264/AVC 수준의 효율을 제공한다. H.264/AVC와 비교하여 SVC의 주된 이점은 단일 스트림에 서로 다른 품질의 여러 스트림을 포함할 수 있다는 것이다. 따라서 SVC 비트스트림은 목적지의 요구에 맞게 대응할 수 있다. 이러한 특징은 한번의 인코딩으로 필요한 모든 비트스트림을 생성할 수 있기 때문에 인코딩 비용 측면에서도 장점이 된다[8].

2.2.1 Temporal scalability

Temporal scalability는 화면주사율(frame rate)에 관여하며, 움직임 보상 예측을 위한 참조 영상(reference picture)를 보다 낮은 계층의 picture로 제한함으로써 제공한다. 기존의 MPEG-1/2, MPEG-4 visual 등에서도 Temporal scalability가 제공되지만, SVC에서는 참조 영상 메모리 제어를 통해 보다 유연한 Temporal scalability를 제공한다. MMOC(Memory Management Control Operation)은 복호된 영상을 저장할 수 있는 DPB(Decoded Picture Buffer)를 적절히 제어한다. DPB에 저장된 영상들은 RPLR(Reference Picture List Reordering)을 사용하여 임의적으로 참조 영상 선택이 가능하다. 이러한 특징으로 인해 임의 순서 부호화 및 참조 영상 선택을 가능하게 하며, 이를 기반으로 Hierarchical B Picture 구조의 시간적 스케일러빌리티를 지원한다.[9]

2.2.2 Spatial scalability

Spatial scalability는 이미지의 해상도에 관여하며, layered coding을 통해 제공한다. 해상도에 따라 계층을 구성하고 각 계층 부호화기로 해당 해상도의 비디오를 부호화하는 다계층 부호화 구조를 가진다. 각 계층은 독립적 부호화가 가능하지만 하위 계층의 부호화 결과인 pixel value, motion vector, residual and syntax element를 상위 계층에서 이용하는 inter-layer prediction으로 부호화 효율을 높인다. 부호화 효율의 개선과 동시에 단일 루프 복호를 지원하기 위해 화면간 또는 동일 화면내 예측뿐만 아니라, 계층간 예측 알고리즘을 기본으로 채용하고 있다. 계층간 예측방법의 기본은 EL의 rate-distortion 계산을 위해 하위계층 정보의 활용을 극대화 한 것이다. 이와 같은 계층간 예측은 inter-layer motion prediction, inter-layer residual prediction, inter-layer intra prediction의 3가지 종류가 있다[8].

2.2.3 Quality scalability

Quality scalability (SNR scalability로도 표기됨)는 특별한 형태의 spatial scalability로써, CGS (Coarse Grained Scalability)와 MGS (Medium Grain Scalability)의 2가지 모드를 지원한다. CGS는 각 계층이 동일한 해상도를 갖는 경우에는 계층별로 양자화 계수(Quantization Parameter, QP)만을 변경한다. 즉, 상위 계층으로 갈수

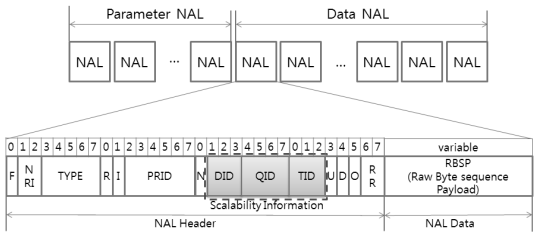

Fig.2. Structure of NAL

록 작은 값의 QP를 사용하여 화질을 향상시키는 방법이다. MGS는 양자화 오류에 대한 점진적 부호화 기법을 사용한다. 즉, 첫 번째 화질 계층은 큰 양자화 간격(step size)으로 양자화한 후, 상위 화질계층으로 갈수록 양자화 간격을 세밀하게 줄여 보다 좋은 화질 계층을 얻는다[10], [11]. Spatial EL은 화질향상을 위해 Quality EL을 포함하며, 이는 하나의 NALU으로 구성된다.

2.2.1 NALU

다양한 전송 환경에서 SVC를 전송하기 위해서, 일반적으로 SVC 비트스트림은 temporal, spatial, quality scalability를 구성하는 각 계층이 하나의 NALU (NAL Unit)를 구성하고 NALU는 RTP (Real-time Transport Protocol)로 패킷화되어 IP망으로 전송된다[12], [13]. NALU의 크기는 가변적으로 구성할 수 있다. Fig. 2. 는 NAL의 구성을 나타낸다. NAL header는 scalability 정보가 포함되며, NAL 데이터는 인코딩 된 비디오 데이터가 들어있다. NALU간에는 부호화 시 참조에 의한 높은 의존관계가 존재한다. NAL header에 포함된 DID (Dependency ID), QID (Quality ID), TID (Temporal ID)를 통해 참조관계 및 scalability 정보를 표현하며, 이를 통해 NALU가 어느 스케일러블 계층에 해당되는지를 파악할 수 있다. 따라서 NAL header의 확인만으로 NALU의 수용 혹은 제거를 결정할 수 있다.

Scalability 정보는 NAL Header 내에 들어있기 때문에 SVC를 암호화할 때에는 반드시 NAL unit 단위로 암호화하여야 한다.

2.3 SVC 암호화 기법

SVC는 보다 고화질의 영상을 얻기 위하여 BL에 EL이 계층적으로 결합되는 구조이다. 따라서 일반적인 데이터 암호화 기법을 사용하여 인코딩된 모든 비트스트림을 데이터처럼 암호화 하게 되면 SVC의 scalability를 효과적으로 사용할 수 없게 된다. 또한, 일반적으로 IPTV와 같은 스트리밍 서비스에서는 고화질의 영상을 시청하기 위하여 추가적으로 과금이 필요한 경우가 많다. 이러한 특성을 만족하기 위하여 하위 레벨의 접근권한을 가진 사용자는 상위 레벨에 접근할 수 없어야 한다. 따라서, 계층적 구조를 유지하면서 콘텐츠를 암호화하는 기법이 필요하다. 이를 위해 많은 연구가 진행되었다.

2009년 Li 등은 SVC 콘텐츠를 위한 계층적 암호기법을 제안하였다 [33]. 제안하는 기법은 BL과 EL로 구성되는 SVC의 특징에 따라, 2계층 키 배열을 생성하고 스트림 암호방식인 LEX (Leak Extraction)를 사용하여 콘텐츠를 암호화한다. 이 기법은 SVC 콘텐츠를 BL과 EL로만 구분하여 암호화한다. 이 방식은 BL과 EL을 구분하기 위한 별도의 어플리케이션이 필요하므로 암/복호화에 비용이 많이 드는 편이다.

2010년 T. Cho 등은 SVC의 계층적 특징을 지원하면서 CW의 주기적인 갱신과 가입 및 탈퇴를 효율적으로 처리할 수 있는 키 관리 기법을 제안하였다 [34]. CAS는 실시간 스트리밍을 위한 접근제어 기법이다. 사용자의 가입 탈퇴는 AK를 통해 처리된다. SVC 암호화 기법이 사용자의 가입과 탈퇴까지 고려할 필요는 없다.

2012년 Diaz-Sanchez 등이 SVC 콘텐츠 암호화를 위한 flexible key stream 기법을 제안하였다 [35]. 이 기법은 MHT (Merkel Hash Tree)를 기반으로 SVC 콘텐츠의 계층 정보에 따라 Hash DAG (Directed Acyclic Graph)를 생성한다. 제안하는 기법을 통해 PPQ (Pay-Per-Quality)를 지원할 수 있다.

이와 같이 SVC 콘텐츠들에 대한 많은 연구가 진행되었지만 여전히 CAS에 실제로 적용할 수 있는지 여부는 알 수 없다. 특히, 이전 기법들의 경우, SVC의 Header까지는 고려하지 않고 있기 때문에 실제 구현에서는 효율성이 떨어질 수 있다. 추가적으로, SVC의 Quality Layer는 특별한 형태의 spatial EL로써 이와 같은 NALU로 구성된다. 관련연구에서는 이러한 SVC 콘텐츠의 특징을 고려하지 않고 있다.

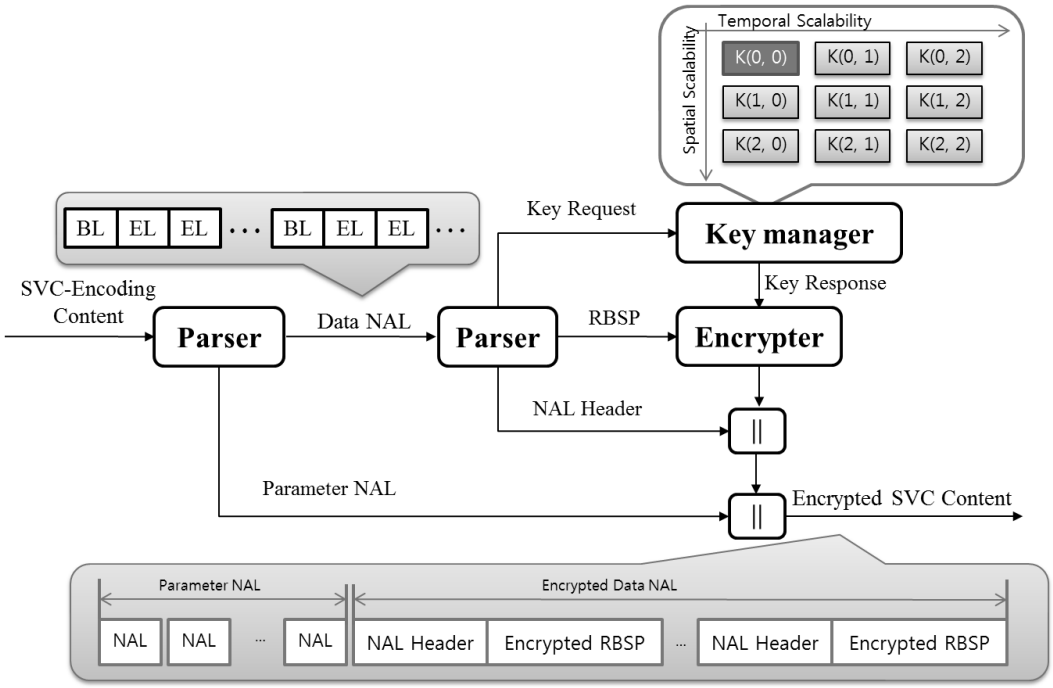

Fig.3. Proposed Encrypted Module for Combining CAS and SVC

III. 제안하는 기법

본 논문에서는 CAS로 SVC콘텐츠를 전송함에 있어 필요한 암호화 모듈을 제안하고, CAS를 이에 맞게 수정한다.

제안하는 기법에서는 Quality EL을 위한 키를 생성하지 않고 Spatial EL과 같은 키를 사용한다. Quality Scalability의 적용은 복호화 과정을 거친 후 디코딩 과정에서 이루어진다고 가정한다. 본 논문에서는 Temporal scalability, spatial scalability를 위해 2차원 키 배열을 생성한다. 많은 관련 연구에서 해쉬 체인을 사용하여 3차원 키 배열을 생성하는 방식을 사용한다[33]. 제안하는 기법에서는 이를 2차원 배열로 축소시켜 키 배열을 생성한다.

Fig. 3. 은 논문에서 제안하는 암호화 모듈을 나타낸다. 암호화 모듈은 *Parser, Key manager, Encrypter, Concatenator*의 네 가지 주요 함수로 구성된다. 논문에서는 우선 CAS를 위한 SVC 암호화 모듈을 먼저 설명한다. 이후에 암호화된 SVC 콘텐츠를 전송하기 위해 CAS를 수정한다. 일반적으로 CAS는 암호화-전송-복호화-재생의 단계를 거치기 때문에 암호화와 복호화 단계를 중점적으로 설명한다.

3.1 암호화 단계

제안하는 기법을 통해 서비스제공자가 수행하는 암호화 과정은 Parser, Key manager, Encrypter, Concatenator의 네가지 기능으로 이루어진다.

• **Parser**: SVC-Encoded Content를 입력받아 Parameter NAL과 Data NAL을 분리하고,

Table. 1. Key array

	j	$j-1$	...	$j-n_s$
i	$i=r_i, j=r_j$	$i, H(j)$	...	$i, H(j-n_s-1)$
$i-1$	$H(i), j$	$H(i), H(j)$	...	$H(i), H(j-n_s-1)$
⋮	⋮	⋮		⋮
$i-n_t$	$H(i-n_t-1), j$	$H(i-n_t-1), H(j)$	...	$H(i-n_t-1), H(j-n_s-1)$

n_t: Temporal EL의 수, n_s: Spatial EL의 수

Data NAL을 다시 NAL Header과 RBSP으로 분리한다. Parameter NAL로부터 scalability정보를 얻어 key manager에게 전송한다. Parameter NAL과 NAL Header를 Concatenator에게, RBSP를 Encrypter에게 전송한다. 또한, Encrypter에게 암호화키, 암호알고리즘 정보 등 RBSP 암호화에 필요한 제어 메시지를 함께 전송한다.

• **Key manager**: Parser로부터 scalability 정보를 받아 이에 해당하는 Key matrix를 생성한다. 키 생성과정은 다음과 같다. $H()$는 cryptographic hash function을 나타낸다.

1. r_i와 r_j를 랜덤하게 생성한다.
2. 해쉬 체인을 이용하여 Table. 1. 과 같이 키 배열을 생성한다.
3. 생성된 키 배열을 Encrypter에게 전송한다.

• **Encrypter**: Parser로부터 RBSP와 제어메시지를, Key manager로부터 키 테이블을 전송받아 RBSP를 암호화한다. 이때 사용되는 암호 알고리즘은 Parser에 의해 결정될 수 있다.

• **Concatenator**: 암호화된 RBSP와 이에 해당하는 NAL Header를 결합하여 NALU를 복원한다. 모든 NALU를 복원한 후 Parameter NAL을 결합하여 암호화된 SVC Content를 생성한다.

3.2 복호화 단계

CAS를 통해 제안하는 기법으로 암호화된 SVC content를 전송받으면, Parameter NAL과 NAL Header를 분석하여 원하는 품질의 영상만을 수용할 수 있다. 먼저 사용자의 기기는 AK대신 $i||j$를 획득하게 되고, 이를 통해 원하는 품질만큼의 EL을 획득할 수 있는 Key matrix를 얻을 수 있다. 이후, encryption phase와 동일한 과정을 거쳐 복호화된 SVC콘텐츠를 획득하게 된다.

3.3 CAS 변경

SVC 콘텐츠를 전송하기 위해 CAS의 ECM, EMM, 그리고 스마트카드에 AK가 저장되는 메모리 부분이 수정되어야 한다.

CAS에서 콘텐츠 전송을 위해 서비스제공자는 사용자가 원하는 품질에 맞는 (i,j)를 선택하여 CAS의 AK 대신 포함하여 전달한다. 사용자가 base layer만 시청할 경우, AK=$K(0,0)$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 Fig. 4. 와 같이 표현된다.

CAS에서 사용하는 스마트카드에는 데이터 업데이트가 가능한 메모리가 사용되는데, 주로 AK를 저장하고 유지하기 위해 사용된다. 제안하는 기법에서는 이를 2차원 키 배열을 저장하도록 수정한다.

제안하는 암호화 모듈을 통해 SVC 콘텐츠를 전송하기 위해서 추가적으로 하드웨어 설치를 필요로 하지 않으며, 소프트웨어 변경만으로 SVC 콘텐츠를 전송할 수 있다.

IV. 분석

분석에서는 제안하는 기법을 안전성과 효율성 측면에서 분석하며, 특히 CAS로 SVC 콘텐츠를 전송할 때 발생하는 오버헤드와, 이러한 기법이 실제로 적용가능한지 여부에 대해 분석한다.

4.1 안전성

CAS에서 AK는 주로 프로그램 단위 혹은 채널 단위(채널 단위일 경우 보통 하루)의 비교적 긴 갱신주기를 가지며, CSA를 이용하여 콘텐츠를 스크램블링한다. CSA는 DES를 기반으로 하는 암호화 알고리즘이며, brute-force 공격 등을 통하여 쉽게 키를 획득할 수 있다는 문제점이 발견되었다[14]-[19]. 이러한 문제점에 대응하기 위해 CW는 보통 10~25초의 짧은 갱신주기를 가진다[20]. 제안하는 기법에서는 $k(0,0)$가 CAS에서의 AK에 해당하며, CW역시 동일한 갱신주기를 가지므로 기존 CAS와 동일한 보호기법을 적용하여 콘텐츠를 보호한다.

기존 CAS에서는 2001년 W.Kanjanarin et al.

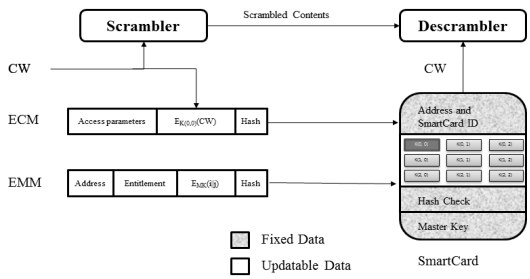

Fig.4. Combining CAS and SVC

에 의 해 스마트카드 복제공격이나 McCormac Hack 공격을 통한 불법시청이 가능하다는 문제점이 발견되었다[21]. 이러한 공격에 대응하기 위하여 스마트카드와 STB간 안전한 채널을 형성하는 연구가 진행되었으며[22]-[26], 최근에는 chipset-pairing 기반의 CAS가 등장하였다[27]. 따라서 적절한 보호 기법의 적용을 통해 기존 CAS가 가지는 문제점들을 해결할 수 있다. 최근 사용되는 다양한 종류의 DCAS, XCAS등은 이러한 공격을 방어하도록 설계되었다[4].

제안하는 기법에서는 하위 품질영상의 시청권한을 가진 사용자가 상위 품질영상의 시청이 불가능하다. 이를 위해 one-way hash function을 사용하여 하위 계층의 키로 상위 계층의 키를 복호화 할 수 없도록 설계하였다. 그러므로 제안하는 기법의 안전성은 기반으로 사용되는 CAS의 안전성과 단방향 해시 함수의 안전성에 근거한다.

4.2 효율성

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. 본 절에서는 제안하는 SVC암호화기법을 적용하였을 때 발생하는 delay를 측정하고 기존 기법과 비교하여 효율성을 분석한다.

encoding과 decoding은 SVC reference codec[28], [29]을 이용하여 수행하였다. Table. 2. 는 실험에 사용된 encoding parameter을 나타낸다[30]. SVC로 인코딩된 콘텐츠를 CAS를 통해 전송하여 사용자 단말에서 수신한 후, 콘텐츠 복호화 및 디코딩 시간을 측정하였다. 제안하는 기법과 데이터를 하나의 키(CW)로 디스크램블링하는 기존의 방식에 대해 delay를 측정하여 제안하는 기법의 오버헤드를 분석하였다. 콘텐츠 스트리밍 환경에서는 성능 비교의 척도로 zapping time을 사용한다. Zapping time은 서비스 요청으로부터 영상이 재생되기까지의 시간을 의미하며 이에 영향을 미치는 수많은 요소가 존재한다[31], [32]. 따라서 zapping time으로는 제안하는 기법의 정확한 오버헤드 측정이 힘들다. 본 실험에서는 콘텐츠가 버퍼에 저장된 후부터 복호화와 SVC 디코딩을 통해 실제 영상이 재생되기까지의 delay를 측정한다. Table. 3. 은 실험 결과를 보여준다. 실험은 STB에서 수행하지는 못하였기 때문에 실제 환경과는 차이가 있을 수 있다. 따라서 제안하는 기법을 적용하지 않은 CAS에서의 스트림 전송 시간을 비교 대상으로 제시한다.

Table. 2. Experimental Environment

	Temporal Scalability	spatial scalability
Base layer	15fps	352×288(CIF)
Enhancement layer	30fps	704×576(4CIF)
	50fps	1280×720(HDTV)

Table. 3. Experimental Result (ms)

		15fps	30fps	50fps
CIF	CAS	103	115	120
	Proposed Scheme	110	123	129
4CIF	CAS	127	173	243
	Proposed Scheme	136	186	261
HDTV	CAS	223	282	427
	Proposed Scheme	241	305	463

실험 결과, 제안하는 기법을 적용하였을 때, 대략적으로 평균 6.98%의 오버헤드가 발생한다. 보다 고화질로 갈수록 많은 오버헤드가 발생하며, 실험 환경의 최고화질 영상에서는 7.73%의 오버헤드가 발생하였다. 시간으로는 약 0.04초의 추가 delay가 발생하는 것으로, 이는 사람이 느끼기 힘든 정도이다. 뿐만 아니라 scalability를 효과적으로 제공하면서 스트리밍 콘텐츠를 보호할 수 있다는 점에서 충분히 감수할 만한 결과를 보여준다.

V. 결 론

본 논문에서는 CAS와 SVC 결합 환경을 위한 암호화 모듈을 제안하였으며, 이를 바탕으로 CAS를 수정하여 재설계하였다. 제안하는 암호화 모듈은 2차원 키 배열을 이용하여 SVC 콘텐츠를 계층적으로 암호화한다. Header부분을 제외한 실제 데이터 부분만 암호화 하여 사용자가 자신에게 맞는 콘텐츠만 전송받을 수 있게 설계하였다. 제안하는 기법을 CAS를 통해 전송하기 위해 기존 CAS의 AK 대신 계층적으로 키를 관리할 수 있는 비밀값을 전달하여 사용자가 원

하는 품질 수준의 서비스를 이용할 수 있도록 수정하였다. 실험 결과 6.98%의 적은 오버헤드로 SVC콘텐츠를 CAS를 통해 전송할 수 있음을 보였다.

References

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

[2] F.K. Tu, C.S. Laih, and H.H. Tung, "On key distribution management for conditional access system on pay-TV system," IEEE Transactions on Consumer Electronics, vo1.45, pp. 151-158, Feb. 1999.

[3] F. Kamperman and B.V. Rijnsoever, "Conditional access system ineteroperability through software downloading," IEEE Transaction on Consumer Electronics, vol. 47, no. 1, pp 47-53, 2001.

[4] Y. Jeong, S. Kim, H. Kim, H. Koo, and E. Kwon, "A novel protocol for downloadable CAS," IEEE Transactions on Consumer Electronics, vol. 54, no. 3, pp. 1236-1243, 2008.

[5] ISO/IEC JTC 1/SC 29/WG 11 N8750: Joint Scalable Video Model(JSVM), Marrakech, Morocco, Jan. 2007.

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

[7] J.R. Ohm, "Advances in scalable video coding," Proceedings of the IEEE, vol. 93, issue. 1, pp. 42-56, Jan. 2005.

[8] H. Schwarz, D. Marpe, and T. 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, 2007.

[9] H. Schwarz, D. Marpe, and T. Wiegand, "Analysis of hierarchical B pictures and MCTF," IEEE International Conference on Multimedia and Expo, pp. 1929-1932, July 2006.

[10] T.C. Thang, J.W. Kang, J.J. Yoo, and J.G. Kim, "Multilayer adaptation for MGS-based SVC bitstream," The 16th ACM Conference on Multimedia, pp. 689-692, Oct. 2008,

[11] T.C. Thang, J.G. Kim, J.W. Kang, and J.J. Yoo, "SVC adaptation: standard tools and supporting methods," EURASIP Signal Process: Image Communication, vol. 24, pp. 214-228, 2009.

[12] T. Stockhammer, M.M. Hannuksela, and S. Wenger "H.26L/JVT coding network abstraction layer and ip-based transport," IEEE ICIP, vol.2, pp. 485-488, 2002.

[13] A. Ellefthériadis and S. Wenger, "System and transport internet of SVC," IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 9, pp. 1149-1163, Sept. 2007.

[14] W. Li and D. Gu, "Security analysis of DVB common scrambling algorithm," The 1st International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007), pp. 271-273, Nov. 2007.

[15] R.P. Weinmann and K. Wirt. "Analysis of the DVB Common Scrambling Algorithm", The 8th IFIP TC - 6 TC - 11 Conference on Communications and Multimedia Security, pp. 195-207, Sept. 2007.

[16] K. Wirt. "Fault attack on the DVB common scrambling algorithm", Computational Science and Its Applications, pp.577 - 584, May 2005.

[17] D. Boneh, R.A. DeMillo, and R.J. Lipton. "On the importance of checking cryptographic protocols for faults", EUROCRYPT '97, LNCS 1233, Springer-Verlag, Berlin, pp. 37 - 51, 1997.

[18] E. Biham and A. Shamir. "Differential fault analysis of secret key cryptosystems", Crypto 1997, LNCS 1294, Springer-Verlag Berlin, pp.513 - 525, 1997.

[19] P. Kocher, J. Jaffe, and B. Jun. "Differential power analysis," CRYPTO'99, LNCS 1666, Springer-Verlag, Berlin, pp. 388 - 397, 1999.

[20] 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, Nov. 2006.

[21] W. Kanjanarin and T. Amornraksa, "Scrambling and key distribution scheme for digital television", IEEE International Conference on Networks, pp. 140-145, Oct. 2001.

[22] E. Yoon and K. Yoo, "A new secure key exchange protocol between STB and smart card in DTV broadcasting", Workshop on Intelligence and Security Informatics (WISI 2006), LNCS 3917, pp. 165-166. 2006.

[23] E. Yoon and K. Yoo, "Robust key exchange protocol between set-top box and smart card in DTV broadcasting", INFORMATICA, vol. 20, no. 1, pp. 139-150, 2009.

[24] T. Hou, J. Lai, and C. Yeh, "Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting", TENCON 2007, IEEE Region 10 Conference, pp. 1-5, Oct. 2007.

[25] H. Kim, "Secure communication in digital TV broadcasting", International Journal of Computer Science and Network Security (IJCSNS), vol. 8, no. 9, pp. 1-5, 2008.

[26] T. Jiang, Y. Hou, and S. Zheng, "Secure communication between set-top box and smart card in DTV broadcasting", IEEE Transaction on Consumer Electronics, vol. 50, no. 3, pp. 882-886, 2004.

[27] J. Son, H. Lee, and H. Oh, "PVR: a novel PVR scheme for content protection," IEEE Transactions on Consumer Electronics, vol. 57, no. 1, pp. 173-177, 2011.

[28] Joint Video Team (JVT) of ISO/IEC MPEG&ITU-T VCEG, "Draft reference software for SVC," Soc. JVT-AB203, MPEG/ITU-T, Technical Report, July 2008.

[29] G.V. Wallendael, W.V. Lancker, J.D. Cock, P. Lambert, J.F. Macq, and R.V. Walle, "Fast channel switching based on SVC in IPTV environments," IEEE Transactions on Broadcasting, vol. 58, no. 1, 2012.

[30] Y. Lee, J. Lee, I. Kim, and H. Shin, "Reducing IPTV channel switching time using H.264 scalable video coding," IEEE Transactions on Consumer Electronics, vol. 54, no. 2, pp. 912-919, 2008.

[31] S. Siddarth and A. Chattopadhyay, "To zap or not to zap: a study of the determinants of channel switching during Commercials," Marketing Science, vol.17, no. 2, pp. 124-138, 1998.

[32] H. Brosius, M. Wober, and G. Weinmann, "The loyalty of television viewing: how consistent is TV viewing behavior?," Journal of Broadcasting and Electronic Media, vol.36, no. 3, pp. 321-335, 1992.

[33] C. Li, C. Yuan, and Y. Zhong, "Layered encryption for scalable video coding," International Congress on Image and Signal Processing, pp. 1-4, Oct. 2009.

[34] T. Cho and S. Yong, "Access Control Method and Key Management Method for H.264/SVC," The KIPS Transactions, Part C vol. 17C, no. 5, pp. 415-426, 2010.

[35] D. Diaz-Sanchez, R.S. Guerrero, A.M. Lopez, F. Almenares, and P. Arias, "A H.264 SVC distributed content protection system with flexible key stream generation," IEEE Interantional Conference on Consumer Electronics - berlin (ICCE-Berlin), pp. 66-70, Sept. 2012.

〈저 자 소 개〉

손 정 갑 (Junggab Son) 학생회원
2009년 2월: 한양대학교 컴퓨터공학부 학사
2011년 2월: 한양대학교 컴퓨터공학부 석사
2011년 3월~현재: 한양대학교 컴퓨터공학과 박사과정
〈관심분야〉 암호기술 응용, 클라우드 컴퓨팅 보안

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과 학사
1989년: 아이오와주립대학 전자계산학과 석사
1992년: 아이오와주립대학 전자계산학과 박사
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안

김 상 진 (SangJin Kim) 종신회원
1995년: 한양대학교 컴퓨터공학과 학사
1997년: 한양대학교 컴퓨터공학과 석사
2002년: 한양대학교 컴퓨터공학과 박사
2003년 3월~현재: 한국기술교육대학교 컴퓨터공학부 부교수
〈관심분야〉 프라이버시 보호, 애드혹 네트워크 보안, 클라우드 컴퓨팅 보안