한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호 (2010. 7)

IPTV에서 확장성 있는 콘텐츠의 보호 방법

용승림*, 조태남°
*인하공학전문대학 컴퓨터시스템학과
°우석대학교 정보보안학과
e-mail: slyong@inhatc.ac.kr, tncho@ws.ac.kr

An Efficient Protection Method for Scalable Content in IPTV

Seung-Lim Yong*, Taenam Cho°
*Dept. of Computer Systems & Engineering, Inha Technical College
°Dept. of Information Security, Woosuk University

● 요 약 ●

PTV에서는 제공되는 컨텐츠에 대해 정당한 사용자만이 접근할 수 있도록 CAS를 사용한다. 사용자들의 네트워크 환경이 다양해지고 소유한 단말기도 성능과 규격이 다양화됨에 따라 사용자의 환경에 따라 수신할 수 있는 확장성 있는 비디오 코딩 방법들이 제시되고 있다. 이러한 방법으로 코딩된 컨텐츠를 CAS를 이용한 IPTV 환경에서 보호하기 위해서는 적절한 보호 기법이 요구된다. 본 논문에서는 최근 각광받고 있는 IPTV에서 확장성 있는 컨텐츠에 대한 수신 제한 기법을 제안하고자 한다.

키워드: IPTV, CAS(수신제한시스템), H.264/SVC, Key Management(키관리)

I. 서론

IPTV는 멀티미디어 콘텐츠의 확산과 광대역 IP 네트워크의 발전을 바탕으로 한 기술로서, 초고속 인터넷 망을 이용하여 방송채널, 주문형 서비스(VoD: Video on Demand), 양방향 데이터 서비스 등을 하나의 단말로 제공하는 융합 서비스이다. 이 서비스에 대한 접근 제한을 위해 수신 제한 시스템 (CAS: Conditional Access System)이 사용된다. CAS 시스템에서는 스크램블링(scrambling) 알고리즘을 이용하여 컨텐츠를 보호한다. 수신 권한이 있는 정당한 사용자만이 디스크램블링(descrambling)할 수 있는 코드를 얻을 수 있다. 이 코드는 주기적으로 변경되는데, 이 변경되는 코드를 안전하게 사용자에게 전달하기 위해서 암호화된 통신 메커니즘을 제공한다.

이러한 서비스의 사용자들은 처리 용량, 스크린 크기 등 다양하고 서로 다른 특성을 가진 단말기를 가질 수 있다. SVC(Scalable Video Coding)은 비디오 통신 시스템의 다양성 문제를 해결하는 효과적인 방법 중의 하나이다. H.264/AVC에 대한 SVC 표준(H.264/SVC)은 비디오의 세 가지 요소(공간적, 시간적, 화질적 요소)에 대해 확장성을 제공한다. 즉, 사용자의 기기와 네트워크 환경에 적합하도록 비디오를 다시 인코딩(encoding)하거나 코드를 수정하지 않도록 한다. 비디오의 세 가지 요소에 대하여 각각 계층 구조로 코딩을 하여 네트워크나 사용자 기기의 환경에 따라 선별적으로 디코딩하는 방식이다. PPV(Pay Per View)에서는 사용자의 선택(지불한 요금)에 따라 컨텐츠의 품질을 달리할 수 있다. 이를 위해서는 사용자가 지불한 서비스 품질에 맞는 컨텐츠만 수신할 수 있도록 제한하는 방법이 필요하므로, 각 계층별로 다른 키(key)로 암호화하여 전송하고, 각 사용자는 요금을 지불한 계층의 복호화키를 소유하여 복호화할 수 있도록 할 수 있다.

H.264/SVC에서 세 가지 각 요소의 계층이 여러 개이기 때문에 사용자의 편의에 따른 세 요소를 선택할 경우 매우 다양한 종류의 컨텐츠 품질이 있을 수 있다. CAS를 이용하는 IPTV 시스템에서는 컨텐츠의 보호를 위해 하나의 CW가 사용되고 있으며 사용권한이 있는 모든 사용자에게 브로드캐스트로 전송된다. 그러나 H.264/SVC 컨텐츠에 대한 수신제한을 하기 위해서는 사용자마다 서로 다른 복호화키 집합을 유니캐스트로 전송하여야 한다는 문제가 발생한다. 본 논문에서는 CAS를 이용한 IPTV 시스템에서 H.264/SVC 컨텐츠에 대한 효율적 수신제한 방법을 제시한다.

II. 관련 연구

1. 수신제한 시스템(CAS)

먼저 사용자 U_i는 오프라인으로 서버(SP: Service Provider)와의 비밀키인 MPK_i(Master Private Key)를 공유한다. 이 키는 스마트 카드에 저장되고 사용자 STB(Set-Top Box)에 장착된다. 브로드캐스트 혹은 멀티캐스트로 전송되는 컨텐츠는 CW(CodeWord)를 이용하여 스크램블되어 있으며 이 값은 매우 짧은 주기로 갱신된다. 사용자가 컨텐츠를 수신하여 디스크램블하기 할

수 있도록 CW가 서버로부터 사용자들에게 전달된다. 그림 1에서 보는 바와 같이 CW는 사용자 모두가 공유한 비밀키 AK로 암호화 되어 컨텐츠 전달 이전에 ECM(Entitlement Control Message)이라는 메시지를 통해 전송된다.

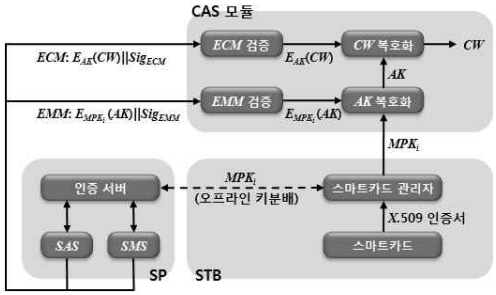

그림 1. CAS 구조
Fig. 1. CAS Architecture

AK는 모든 사용자가 공유하는 그룹키(group key)로서 사용자가 가입하거나 탈퇴할 때마다 새로운 값으로 갱신되어야 한다. 그렇지 않다면 사용자가 탈퇴한 이후에도 CW를 복호화할 수 있고, 새로 가입한 사용자는 가입 이전에 수신하여 저장한 ECM을 가입 후 알게 된 AK로 복호화하여 CW를 알 수 있게 되므로 이전의 컨텐츠를 디스크램블할 수 있기 때문이다. 갱신된 AK는 그림 1에서와 같이 각 사용자와 서버만이 공유한 MPK_i로 암호화하여 EMM이라는 메시지를 통해 전달된다.

2. H.264/SVC 및 접근제어 기법

H.264/SVC는 다양한 네트워크 환경 및 사용자 단말에 적합하도록 다양한 이미지 크기(spatial), 프레임 수(temporal)와 품질(quality)을 선택적으로 사용할 수 있는 구조를 제공한다[1]. 이 세 가지 속성의 다양성을 제공하기 위하여 이미지에 대한 비트 스트림을 계층적으로 구성한다. 그림 2에서와 같이 베이스 계층(base layer)은 기본적인 해상도와 가장 낮은 품질에 대한 비트 스트림이다. 증강 계층(enhancement layer)에서는 베이스 계층의 해상도와 품질을 높이는데 필요한 데이터로 구성된다. 증강 계층은 여러 개일 수 있다. 각 계층은 서로 다른 종류의 슬라이스들로 구성되는데(그림 3에서 서로 다른 색의 사각형) 이들 슬라이스들이 상호 참조함으로써 동적 이미지를 표현한다. 이 상호 참조의 정도를 조정함으로써 프레임 수를 조정할 수 있다[2].

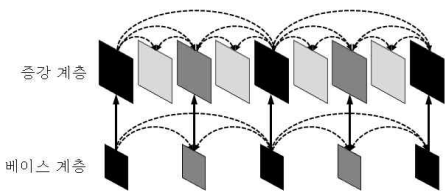

그림 3. H.264/SVC의 계층 구조
Fig. 3. Hierarchical Structure of H.264/SVC

[3]에서 Bin 등은 H.264/SVC에 대한 사용자의 접근제한 기법을 제안하였다. 이 방법의 핵심 아이디어는 각 계층별로 키를 할당하고, 각 사용자는 자신이 정당하게 수신할 수 있는 계층에 대한 키만 소유하도록 하는 것이다. 사용자가 필요로 하는 모든 계층에 대한 키를 소유한다면 많은 키를 소유해야 한다. 상위 계층을 수신할 수 있는 사용자는 그 계층의 모든 하위 계층 정보를 수신할 수 있어야 한다는 점에 착안하여, 사용자는 자신이 수신할 수 있는 최상위 계층에 대한 키만 소유하도록 하고 하위 계층의 키는 상위 계층으로부터 유도될 수 있도록 설계하였다. 응용에 따라 서비스 제공자는 H.264/SVC가 제공하는 3개의 확장 가능한 속성 중에서 일부를 사용자가 선택할 수 있도록 할 수 있을 것이다. 하나의 콘텐츠에는 하나의 마스터 키 MK가 대응된다. 만약 3개의 속성에 대해 사용자가 선택하도록 할 경우라면, 그림 4에서와 같이 MK에 속성 번호 i를 접합하여 해시함수 $H()$를 적용함으로써 각 속성 대한 타입키 K_i를 생성한다. 이 타입키로부터 모든 계층키를 유도해낸다. i번째 속성의 j번째 계층키(K_i^j)는 $K_i^j = H(K_i^{j+1}) = H^{n_i+1-j}(K_i)$로 정의된다. 해시함수의 특성상 상위 계층 키로부터 하위 계층 키는 계산할 수 있지만 하위 계층 키로부터 상위 계층 키는 알아낼 수 없기 때문에, 사용자는 정당하게 수신할 수 있는 계층의 키만을 알 수 있다. 그림 3에서 음영 처리된 키는 사용자가 각 속성에서 선택한 최상위 레벨의 키이다.

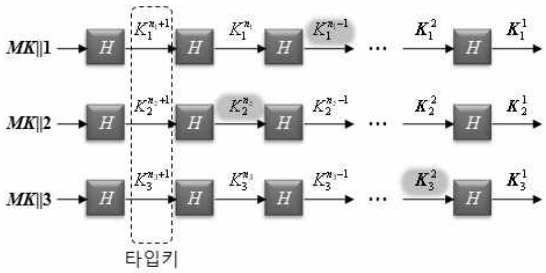

그림 3. H.264/SVC 키관리 구조
Fig. 3. Key Management Structure of H.264/SVC

컨텐츠를 전송할 때, 전송단위에 포함된 데이터는 여러 속성의 여러 계층에 포함될 수 있다. 이 데이터에 관련된 계층의 키들의 곱을 K라 할 때, α^K로 암호화한다(α는 환형 그룹의 생성자).

3. 계층적 그룹키 관리 기법

1절에서 기술한 바와 같이 이 그룹키는 사용자의 가입이나 탈퇴가 일어날 때마다 갱신되어야 하는데, 사용자의 수가 많고 사용자의 그룹 가입 및 탈퇴가 빈번한 경우에 그룹키의 효율적 갱신 방법이 중요하다. Wong 등은 [4]에서 키트리(key-tree)를 이용하여 키 갱신을 $O(\log n_U)$(n_U는 사용자 수)에 수행할 수 있는 LKH(Logical Key Hierarchy)를 제안하였다.

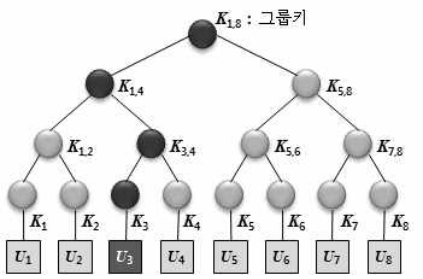

그림 4. 계층적 키관리 구조
Fig. 4. Hierarchical Key Management Architecture

사용자 U_i는 서버와 비밀키 K_i를 공유한다. 서버는 사용자들과 공유한 비밀키들을 단말노드로 하여 이진 트리를 구성하고, 각 내부노드에 키를 할당한다. 각 사용자는 자신의 비밀키로부터 루트에 이르는 경로상의 키를 소유한다. 루트키는 모든 사용자가 공유하므로 그룹키가 된다. 그림 4는 8명의 사용자에 대한 키트리이다. 사용자가 탈퇴할 경우, 그 사용자가 소유하던 키들을 모두 갱신하고 갱신된 키는 그 키의 갱신되지 않은 자식 노드키로 암호화하여 브로드캐스트한다. 사용자가 가입하는 경우에도 유사한 방법으로 갱신할 수 있다.

4. 누적형 키분배 기법

[5]에서 저자들은 H.264/SVC을 사용할 경우 하위 계층만을 필요로 하는 모든 사용자들도 모든 계층을 수신해야 하기 때문에 대역폭을 낭비한다고 지적하고, 수신자가 필요한 계층만을 추출하여 전송하는 방법을 제안하였다. 각 계층은 에는 서로 다른 키를 사용하므로, 각 계층마다 키트리 $T_i(i \leq n_a$, n_a는 계층 수)를 유지한다. 사용자가 i번째 계층의 품질을 원한다면 $T_j(1 \leq j \leq i)$의 키트리에 삽입되어야 한다. 이 방법은 하나의 속성에 대해 기술하고 있으므로, 여러 개의 속성을 감안할 때, 서버가 유지해야 하는 키트리의 개수와 사용자가 선택할 수 있는 계층의 조합의 수는 $n_K = \prod_{i=1}^{n_A} n_i$($n_A$는 속성의 수)이다. 서버는 동일한 콘텐츠에 대해 n_K개의 서로 다른 전송 스트림을 형성해야 함을 의미한다.

III. 제안 방법

[5]의 방법을 CAS 구조에 적용한다면, 각 사용자는 최대(사용자가 각 속성의 최고 계층을 선택했을 때) $O(n_K \times \log n_U)$개의 키를 소유해야 한다. 각 트리의 최대 단말 노드 수는 사용자 수인 n_U이기 때문이다. 사용자의 가입과 탈퇴시 변경되는 키의 수는 사용자가 소유한 키의 수와 같으므로 $O(n_K \times \log n_U)$개이다. 데이터의 스크램블링 킷값을 변경하고자 한다면 기존의 계층별 그룹키로 암호화해서 보내야 하므로 n_K개의 키가 전송되어야 한다.

Bin의 방법을 CAS 구조에 적용할 경우에도 각 속성별 계층 키를 보내주어야 한다. 또한 정당한 사용자만이 계층키를 수신할 수 있도록 하기 위해서 각 계층마다 LKH를 유지한다면, 사용자의 가입이나 탈퇴마다 $O(n_A \times \log n_U)$개의 키 갱신이 일어나며 이를 전송해야 한다.

컨텐츠 보호에 사용되는 *CW*나 계층키는 *ECM*을 통해 암호화되어 전달되어야 하며, 사용자의 가입과 탈퇴로 인한 그룹키나 계층키의 갱신은 *EMM*을 통해 전달된다. 현재 국내 IPTV에서 *CW*의 갱신 주기는 약 0.1초로서 매우 짧다[6]. 본 논문에서는 전송량 및 암복호화의 횟수를 줄이기 위해 ECM를 통해 전달되는 키의 개수를 줄이기 위한 방법을 제안하고자 한다.

1. 제안 1

[5]의 방법과 같이 서버는 각 속성의 계층별로 키트리를 유지하면서, 사용자가 가입하면 각 속성에 대해 수신하고자 하는 계층부터 이하 계층의 모든 트리에 추가한다. i번째 속성의 j번째 계층의 키트리의 루트 LK_i^j는 계층키 생성에 사용된다. 컨텐츠마다 하나의 MK가 할당되고, 계층키는 해시함수를 이용하여 $K_i^j = H_2(MK \| LK_i^k)$와 같이 생성한다. MK는 CAS의 CW 대신 ECM을 통하여 암호화없이 전송하되 서버가 서명하도록한다. 사용자의 가입과 탈퇴가 일어나면, EMM을 통해 관련된 키트리의 갱신된 키를 전송한다. 전송방법은 키트리의 갱신 방법을 사용한다. 따라서 갱신되는 키의 수는 $O(n_K \times \log n_U)$이다.

2. 제안 2

제안 1에서 각 사용자는 최대 n_K개의 키트리에 가입되어야 한다. 두 번째 제안에서는 각 속성별로 하나의 키트리에 가입하는 방법을 제안한다.

제안 1에서와 같이 CW 대신 MK를 사용하고, 계층키는 $K_i^j = H_2(MK \| LK_i^k)$와 같이 생성한다. 단, LK_i^j는 [3]의 방법과 같이 서버가 하나의 비밀값 s로부터 생성한다. 즉, $LK_i = H(s \| i)$이고, $LK_i^j = H(LK_i^{j+1}) = H^{n_i+1-j}(LK_i)$이다. 서버는 제안 1에서와 같이 각 계층마다 키트리를 유지하지만, 각 사용자는 각 속성마다 수신할 최상위 계층의 트리에만 가입한다. 사용자는 가입한 키트리의 $O(\log n_U)$개 키와 LK_i^j를 소유한다. 사용자의 가입과 탈퇴가 일어나면 해당 키트리와 s를 갱신한다. 키트리의 갱신 방법은 기존의 방법을 이용하고, s로부터 갱신된 LK'^j_i를 키트리의 루트로 암호화하여 전송한다. 사용자는 갱신된 키트리 루트 키로부터 LK'^j_i를 수신하고 하위 계층 키인 $LK'^k_i (k < j)$를 계산한다.

IV. 분석 및 결론

[5]의 방법과 [3]의 방법을 CAS 구조에 적용했을 대와 제안한 기법에 대해 ECM, EMM 및 각 사용자가 소유해야 하는 키의 개수를 표 1에 요약하였다.

코딩에 사용되는 속성의 최대 개수는 3개이나 크기와 화질은 코딩 구조상 하나의 속성으로 처리할 수 있다. 각 속성의 계층의 개수는 이론상 매우 많을 수 있으나 사실상 사용자가 선택할 수 있는 종류는 많지 않을 것으로 예상된다. 구체적인 수는 응용에 따라 달라질 수 있을 것이나 현재 IPTV의 가입자 수가 백만을 넘어선 것을 감안하면 아래와 같은 관계가 성립된다.

$$n_A < \sum_{i=1}^{n_A} n_i < \prod_{i=1}^{n_A} n_i \,,\ \log(n_U) \ll n_U \approx 2{,}000{,}000$$

표 1. 효율성 비교

Table 1. Comparison of Efficiencies

	ECM	*EMM* 과 U_i
[5]의 방법	$\prod_{i=1}^{n_A} n_i$	$O(\prod_{i=1}^{n_A} n_i \times \log n_U)$
[3]의 방법	$\prod_{i=1}^{n_A} n_i$	$O(n_A \times \log n_U)$
제안 1	1	$O(\prod_{i=1}^{n_A} n_i \times \log n_U)$
제안 2	1	$O(n_A \times \log n_U) + \sum_{i=1}^{n_A} n_i$

표 1에서 보는 바와 같이 제안한 방법은 가장 빈번하게 전송되는 ECM의 크기를 줄임으로써 메시지의 크기 및 암복호화 시간을 절약하였다. 대신 [3]의 방법에 비하여 EMM의 크기가 늘어났으나, EMM은 ECM에 비해 빈도가 낮을 뿐 아니라 줄어든 ECM 크기에 비해 늘어난 EMM의 크기가 작으므로 효율성이 증대된 것으로 분석된다.

참고문헌

[1] Heiko Schward, Mathias Wien, “The Scalable Video Coding Extension of the H.264/AVC Standard,” IEEE Signal Processing Magazine, 2008. 3.

[2] Heiko Schwarz, Detlev Marpe, and Thomas Wiegand, “Overview of the Salable Video Coding Extensions of the H.264/AVC Standard,” IEEE transactions on circuits and systems for video technology, vol 17, no 9, september 2007.

[3] Wong C.K, Gouda M, and Lam S.S, “Secure Group Communications using key graphs,” ACM SIGCOMM 98.

[4] Bin B.Zhu, Shipeng Li, Ming Feng, “A Framework of Scalable Layered Access Control for Multimedia”, IEEE International Symposium, 2005.

[5] 이정희, 오희국, “IPTV환경에서 누적형 계층 비디오 멀티캐스트를 위한 키 분배 방법”, 한국정보보호학회 하계학술대회 논문집 Vol.19, No.1.

[6] 신기은, 최형기, “해쉬 트리 기반의 효율적인 IPTV 소스 인증 프로토콜”, 정보처리학회논문지 C 제16-C권 제 1호, 2009.2.