IPTV SVC환경에 알맞은 사용자 그룹 관리 방법1)

이정희2), 오희국3)
*한양대학교 컴퓨터공학과
e-mail:jachiman@naver.com, hkoh@hanyang.ac.kr

A Suitable User Group Management method for SVC(Scalable Video Coding) in IPTV

Jung-Hee Lee, Heekuck Oh
Department of Computer Engineering Hanyang Univ.

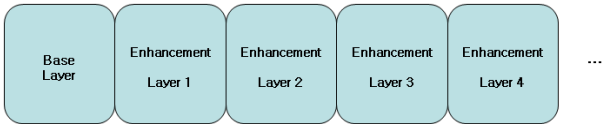
요 약

IPTV 환경에서는 콘텐츠를 수신하는 디바이스가 여러 종류가 있더라도 한번의 인코딩으로 콘텐츠 제공을 할 수 있는 Video Coding 기술인 SVC(Scalable Video Coding) 기술이 제공된다. SVC의 특징으로는 콘텐츠를 여러 계층으로 나뉘어 하나의 Base 계층과 여러 개의 Enhancement 계층을 가지게 되는데 상위계층은 하위 계층에 대해 더 추가적인 정보를 담고 있기 때문에 더 많은 계층이 전송될수록 데이터의 품질이 좋아지게 된다. 이러한 IPTV SVC환경의 그룹관리에 대해서 SVC의 특징인 계층간 순차적 관계를 적용한 안전한 사용자 그룹의 구성과 빈번한 가입과 탈퇴에 대해서 효율적인 그룹키 갱신에 대한 방법이 필요하다. 따라서 본 논문에서는 SVC의 특징인 계층간 순차적 관계를 지키는 사용자 그룹을 구성하고, 빈번한 가입/ 탈퇴에 대해서 효율적으로 처리하기 위한 일괄적인 그룹 키 갱신방법을 제안한다.

1. 서론

IPTV는 IP기반 서비스로 방송서비스와 통신서비스가 결합된 형태이다. IPTV의 가장 큰 특징은 여러 가지 단말을 통해 다양한 서비스를 제공한다는 점이다. 서버가 콘텐츠를 여러 디바이스로 제공할 때 각 디바이스에 맞게 콘텐츠를 맞춰서 제공해야 하는데, 지금까지의 방법으로는 서버가 각 디바이스에 맞게 콘텐츠를 각각 인코딩을 하여 제공해주는 방법을 사용하였다. 이 방법은 서버가 하나의 콘텐츠에 대해 각 디바이스에 맞는 인코딩을 어러번 해야 하므로, 모든 인코딩한 데이터를 다 서버가 보유하고 있어야 하는 오버헤드가 발생하게 된다.

이러한 문제를 해결하기 위한 대책으로는 SVC(Scalable Video Coding)을 들 수 있다[1]. SVC는 하나의 콘텐츠를 서비스 형태, 디바이스에 따라 가변적으로 사용할 수 있도록 포맷을 변환하는 방식으로 수신측의 성능을 고려하여 적합한 정도의 성능으로 콘텐츠를 제공하기 때문에 서버의 오버헤드를 줄이며, 서버의 능력을 효율적으로 관리할 수 있다. SVC의 특징으로는 콘텐츠를 여러 계층으로 나뉘어 하나의 Base 계층과 여러 개의 Enhancement 계층을 가지게 되는데(그림 1) 상위계층은 하위 계층에 대해 더 추가적인 정보를 담고 있기 때문에 더 많은 계층이 전송될수록 데이터의 품질이 좋아지게 된다. SVC에서는 이 특징을 이용하여 여러 가지 단말기에 효율적으로 알맞은 화면을 제공하게 되며, QoS(Quality of Service)를 지원해야 하는 IPTV 환경에 알맞다.



(그림 1) SVC를 구성하는 계층의 특징

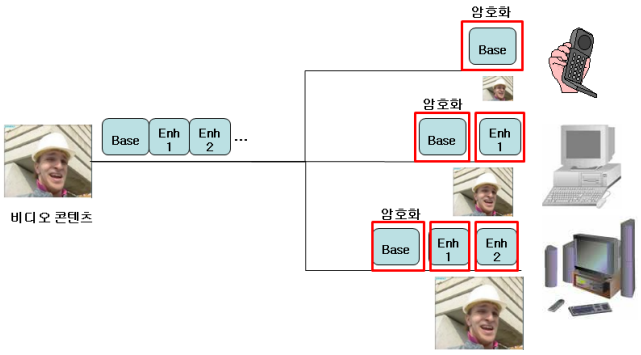
앞에 소개한 SVC가 적용된 IPTV환경의 사용자 그룹 관리 방법에서 사용자 그룹은 SVC의 특징인 계층간 순차적 관계를 깨뜨리지 않고 안전한 사용자 그룹이 구성되어야 하며, 또한, IPTV에서 부가 콘텐츠(유효기간동안 시청 가능한 부가 서비스)등을 이유로 사용자의 빈번한 가입과 탈퇴가 예상이 되는데 이에 대한 효율적인 그룹 관리 방법이 필요하다.

따라서, 본 논문에서는 IPTV환경에서 계층간 순차적 관계를 깨뜨리지 않으며 효율적인 그룹 관리 방법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 IPTV SVC환경의 구성과 사용자 그룹을 구성하는 데 고려해야 하는 보안 요구사항을 분석하고, 3장에서는 사용자 그룹 형성 방법과 사용자의 빈번한 가입, 탈퇴에 대해 효율적인 그룹 관리 방법으로 일괄적 키 갱신 기법을 제안한다. 그리고 마지막으로, 4장에서 결론을 맺는다.

1) 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2010-C1090 - 1011 - 0010)
2) 주저자, jachiman@naver.com
3) 교신저자, hkoh@hanyang.ac.kr

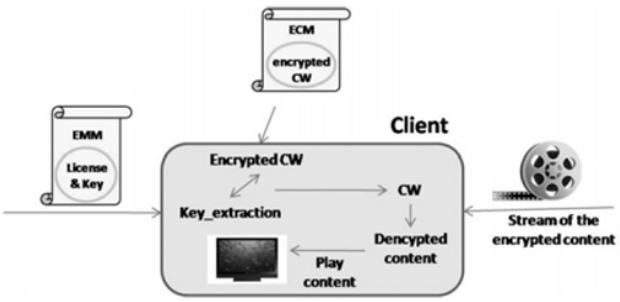
2. 환경 구성 및 보안 요구사항

[IPTV SVC 환경구성] IPTV SVC환경에서는 여러 장비에게 하나의 콘텐츠가 전송이 될 때, 우선 서버측에서 하나의 Base 계층과 여러개의 Enhancement 계층으로 나뉘어, 사용자의 서비스 형태, 디바이스에 따라 필요한 만큼의 계층만 사용자측에 전송을 해주게 된다.(그림 2)



(그림 2) IPTV SVC 환경

또한, IPTV에서는 콘텐츠를 안전하게 보호하기 위하여 계층적인 키 관리 방법을 사용하고 있는데, 이전의 키 계층적인 키 관리방법으로는 대표적으로 J. W. Lee 등[2], F. K. Tu등[3], Y. L. Huang등[4]이 있으며, (그림 3)과 같이 계층적인 키를 이용하여 콘텐츠를 암호화하게 된다. 본 논문에서의 키 관리방법은 Y. L. Huang등의 4단계 계층 키 방법(CW(Control Word), AK(Authorization Key), DK(Distribution Key), MK(Master Key))을 사용하고 있다.



(그림 3) 계층적인 키를 이용한 콘텐츠 보안 방법

[보안 요구사항] 다음은 IPTV SVC환경에서 안전한 사용자 그룹 구성을 위해서 필요한 보안 요구사항이다.

- 기밀성(Confidentiality): 부적합한 사용자에게 그룹키가 노출되지 않게 해야 한다.
- 전방향 안정성(Forward Secrecy): 그룹을 탈퇴한 멤버를 포함하여 이전 그룹키를 알고 있는 공격자는 새 그룹키를 알 수 없어야 한다.
- 후방향 안정성(Backward Secrecy): 그룹을 새롭게 가입한 멤버를 포함하여 현재 그룹키를 알고 있는 공격자는 이전 그룹키를 알 수 없어야 한다.

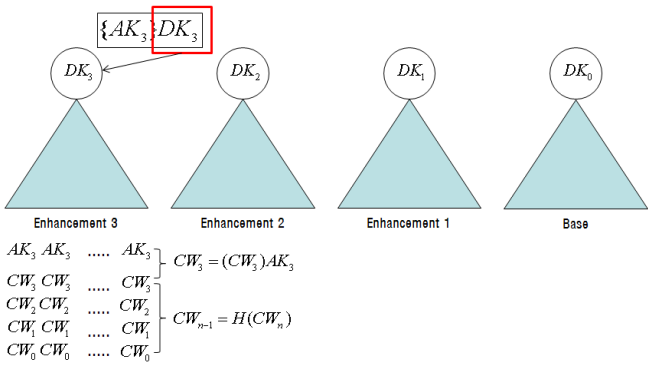
3. 제안하는 방법

본 논문에서는 사용자 그룹을 구성하는데 있어서, SVC의 계층간 순차적인 관계를 깨뜨리지 않는 사용자 그룹을 형성하고, 빈번한 가입/ 탈퇴에 대해서 일정한 주기에 한꺼번에 처리를 할 수 있게 하는 일괄 키 갱신 기법을 제안한다. 다음의 <표 1>은 표기법이다.

<표 1> 표기법

기호	내용
CW	콘텐츠를 암호화 할때 사용하는 키, AK에 의해 암/ 복호화됨
AK	사용자 자격을 위해 사용하는 키, DK에 의해 암/ 복호화됨
DK	그룹 키로 사용, MK(Master Key)에 의해 암/ 복호화됨
H(), h()	단방향 해쉬 함수
()K	키 K를 사용하여 대칭형 알고리즘으로 암호화
k	키 갱신을 하기 위해 키 서버에서 만드는 키
K_{11}	높이 1, 너비에 위치한 노드의 그룹 키
U_1	사용자1
⊕	XOR 연산

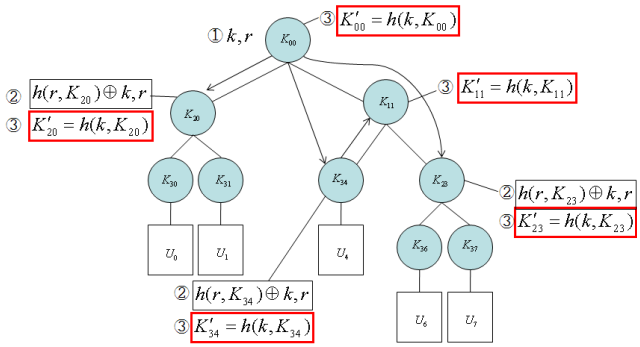
[사용자 그룹 형성] SVC환경에서는 사용자 그룹이 계층별로 구성이 된다. 그래서 콘텐츠의 품질에 따라 사용자 그룹이 구성되며, 높은 계층을 볼 수 있는 사용자는 선택된 그룹의 계층보다 낮은 계층을 모두 가지게 되어, 해당하는 품질의 계층을 보게 된다. 다음 (그림 4)는 사용자 그룹 형성방법을 나타내고 있으며, DK가 그룹의 루트 키로 되어 바로 하위 키인 AK를 암호화하여 해당되는 사용자에게 보내주게 되면, 이에 합당한 사용자만 AK를 얻게 되며, 이 AK를 통해 콘텐츠를 풀어 볼 수 있는 CW키를 얻게 된다. 또한 CW키 간의 단방향 해쉬함수관계 때문에 그 하위 계층의 CW를 모두 풀어볼 수 있게 된다.



(그림 4) IPTV SVC환경에 알맞은 사용자 그룹

[그룹 키 갱신 방법] 안전한 그룹을 이루기 위해서는 그룹의 기밀성, 전방향 안정성, 후방향 안정성을 위해 키 갱신 방법이 필요하다. 이에 대한 갱신 기법으로 개별 키 갱신 기법, 일괄 키 갱신 기법 등의 두 가지를 들 수 있다. 개별 키 갱신 기법은 사용자의 가입/ 탈퇴가 일어날 때마다 키 갱신을 해주는 방법이며, 일괄 키 갱신 기법은 일정기간 동안 발생된 가입/ 탈퇴를 한꺼번에 일괄적으로 처리하는 방법이다. IPTV환경에서는 부가서비스 등으로

인한 빈번한 가입, 탈퇴 등이 예상되므로, 효율적인 키 갱신 기법이 필요하다. 따라서, 가입/ 탈퇴시마다 키 갱신을 해주어 중복적인 연산을 수행하는 개별 키 갱신 기법[5],[6]보다 일정기간동안 가입/ 탈퇴내용을 수집한 후에 일괄적으로 갱신을 하는 일괄 키 갱신 기법이 더 효율적이다. 따라서, 본 논문에서는 일괄 키 갱신 기법을 사용하여 그룹 키 갱신을 한다. 키 갱신 주기는 가입/ 탈퇴시 바로 갱신하지 않더라도 부담이 없는 기간인 1일 단위로 갱신이 되는 사용자 자격인증 키인 AK에 맞춘다. 다음의 (그림 5)는 U_2, U_3, U_5가 탈퇴 시, 일괄 키 갱신 기법을 나타내고 있다. 갱신 방법은 탈퇴한 멤버를 제외한 균형 이진트리를 구성하고, 키 서버는 새로운 키 k와 랜덤 값 r을 만들어 서브트리들의 루트키를 각각 r과 해쉬하여 나온 값을 k와 XOR처리하여 r값과 보내주게 된다. 그러면, 각각의 서브트리는 자신의 루트키를 이용하여 k값을 구하고 k값과 자신의 루트키를 해쉬하여 키 갱신을 하게 된다. 다음의 동작만으로 앞에서 언급한 보안 요구사항인 기밀성, 전방향 안정성, 후방향 안정성을 만족하게 된다.



(그림 5) 제안하는 일괄 키 갱신 기법

4. 결론

본 논문은 IPTV SVC환경에 알맞은 사용자 그룹을 형성하고, 빈번한 가입, 탈퇴에 대해서 효율적인 일괄 키 갱신 기법을 제안하고 있다. 제안하는 방법은 SVC의 특징인 계층간 순차적인 관계를 깨뜨리지 않고 그룹을 형성하였으며, 빈번한 가입, 탈퇴등이 일어날 수 있는 IPTV환경을 고려하여 사용자 권한을 인증해주는 키인 AK키의 주기에 키 갱신 주기를 맞춤으로써 개별적인 키 갱신 기법에 비해 효율적인 갱신이 가능하며, 또한 갱신시 사용하는 암호화 비용도 해쉬 2번, XOR 연산 1번으로 적은 비용으로 안전한 그룹 관리가 가능하다.

참고문헌

[1] M. Dunte, and C. Ruland, “Construction and Usage of Time-limited Keys in Secure Multimedia Distribution,” in Proceedings of the 3th international conference on Communications and Networking(CHINACOM 2008), pp. 1270-1274, 2008.

[2] J. W. Lee, “Key distribution and management for conditional access system on DBS,” in Proceedings Int. Conf. Cryptology and Information Security, pp. 82-86, 1996.

[3] F. K. Tu, C. S. Laih, and S. H. Toung, “On key distribution management for condition access system on Pay-TV system,” in IEEE Int. Symp. Consumer Electronics (ISCE'98), vol. 45, Taipei, Taiwan, R.O.C., pp. 151-159, 1998.

[4] Y. L. Huang, S. Shieh, F.S. Ho, and J. C. Wang, “Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems,” in IEEE Transaction On Multimedia, Vol. 6, No. 5, pp. 760-769, 2004.

[5] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs, " In Proceedings of ACM SIGCOMM, 1998.

[6] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast : Issues and Architectures, " IETF RFC 2627, 1999.