情報保護學會論文誌
第20卷 第1號, 2010. 2

도메인 키 기반의 효율적인 스케일러블 콘텐츠 재분배 메커니즘

박 수 완,† 신 상 욱‡
부경대학교 일반대학원 정보보호학과

Domain Key Based Efficient Redistribution Mechanism of Scalable Contents

Su-Wan Park,† Sang Uk Shin‡
Dept. Information Security, Graduate School, Pukyong National University

요 약

본 논문에서는 홈 네트워크 내 차별적인 성능을 가지는 장치들이 장치 성능에 적응적으로 콘텐츠를 재분배하는 메커니즘을 제안한다. 제안 시스템은 최근에 표준화 된 H.264/SVC 스케일러블 코딩 기법에 의해 압축 암호화된 콘텐츠를 각 장치 성능에 적합한 수준(level)으로 제공하는 DRM 시스템의 콘텐츠 재분배 메커니즘이다. 본 논문은 SVC 콘텐츠를 효율적으로 재분배하기 위해 제시된 3가지 요구사항을 티켓을 사용하여 해결하고, 도메인 키를 사용하여 도메인 내의 장치들이 콘텐츠를 효율적으로 사용할 수 있도록 한다.

ABSTRACT

In this paper, we propose a redistribution mechanism of the content that is adapted to devices, which may have different display size and computing capabilities, in home network. The proposed system introduces a mechanism that the encrypted content compressed by H.264/SVC(Scalable Video Coding) scheme which has been standardized recently is provided to the device into a level of content suitable to each device capability. To efficiently superdistribute SVC content, this paper defines three requirements and proposes redistribution mechanism which satisfies these requirements using another licence that it is called 'Ticket'. Our system allows devices to redistribute the content freely in the domain using domain key.

Keywords: DRM, SVC, authorized domain, content redistribution

I. 서 론

초기 DRM(Digital Rights Management)은 콘텐츠 소유권자에 의해서만 분배되는 소유권자 의존형 콘텐츠 분배 모델이었으나 콘텐츠 분배 서버의 부하가 커지고 소비자들끼리 콘텐츠를 자유롭게 재분배하고자 하는 요구와 소비자가 소유한 다수의 홈 장치들 사이에서 콘텐츠를 제한없이 사용하고자하는 요구가 추가되면서 보다 진화된 DRM 기술이 요구되었다. 이를 위해 개인이 소유한 장치들을 인증된 도메인(Authorized Domain)으로 정의하고 AD 내에서의 콘텐츠 배포와 권리 배포를 가능하게 하는 메커니즘들[1-3]이 제안되었다. 하지만 DRM 콘텐츠를 효율적으로 재분배하기 위해서는 도메인 관리만으로는 부족하다. 실제로, 홈 네트워크 내의 서로 다른 장치들은 개별적인 성능과 채널 능력을 가지므로, 장치들에게 적응적인 콘텐츠와 라이센스를 제공하는 DRM 기법들[4-5]을 요구한다.

재생 장치들에게 적응적인 콘텐츠를 분배하기 위해서는 미디어 이동성을 위한 트랜스코딩(trans-

접수일(2009년 9월 10일), 수정일(2009년 10월 23일), 게재확정일(2009년 11월 12일)
† 주저자, music016@pknu.ac.kr
‡ 교신저자, shinsu@pknu.ac.kr

coding) 기술을 제공해야 한다. 하지만 DRM 보호된 콘텐츠의 적응(adaptation)은 다양한 보안 위협에 노출되기 쉬울 뿐 아니라 콘텐츠에 따른 라이센스도 변경되어야 하므로 비효율적이다. 이 문제는 최근에 주목을 받고 있는 스케일러블 코딩 기법에 의해 해결될 수 있다. 특히, H.264/SVC (Scalable Video Coding)[6]는 콘텐츠의 확장성을 제공하는 가장 최근에 표준화 된 비디오 부호화 기술로서, 원본 비디오 스트림을 하나의 기본 계층(Base Layer)과 여러 개의 강화 계층(Enhancement Layer)으로 나눠 처리한다. 기본 계층은 H.264/AVC[7] 코딩 기법을 기반으로 하여 대부분의 중요한 코딩 정보를 담고 있으며 이 부분만으로도 기본적인 비디오의 재현이 가능하다. 반면 강화 계층은 더욱 향상된 비디오 화질을 위한 추가 정보를 담고 있다. 비디오 제공자는 사용자의 환경에 적합하게 기본 계층과 강화 계층들을 선택하여 제공함으로서 사용자의 범용 미디어 접근을 지원한다. 이때, 계층적 부호화는 공간적, 시간적 그리고 SNR 확장성을 통해 이루어진다. H.264/SVC는 확장성을 제공하기 위해 각 레이어의 비트스트림을 NAL 단위로 제공하고 일부의 레이어들을 사용자에게 전송함으로써 사용자 장치나 채널에 적합한 콘텐츠를 제공한다.

본 논문에서는 홈 네트워크 안에 있는 각 장치들이 서로에게 적응적인 콘텐츠를 제공할 수 있도록 하기 위하여 최근에 표준화 된 H.264/SVC의 스케일러블 코딩 기법에 의해 압축 암호화된 콘텐츠를 이용하는 재배포 메커니즘을 제안한다.

II. 스케일러블 콘텐츠의 재배포 메커니즘

본 논문에서 제안하는 SVC DRM은 사용자가 구입한 콘텐츠를 사용자 소유의 장치들 간에 자유롭게 재분배 할 때 개별적인 성능과 동적인 채널 능력을 가지는 각 장치들에게 알맞은 수준으로 콘텐츠를 제공하도록 하는 일반적인 DRM의 확장된 개념이다. 제안된 SVC DRM 메커니즘은 홈 도메인 내의 장치들 간에 스케일러블한 콘텐츠와 콘텐츠의 사용 권한을 효율적으로 제공하기 위해 H.264/SVC 기술에 의해 스케일러블하게 압축되고, 이전에 제안된 암호화 기법[8]에 의해 보호된 콘텐츠를 사용한다.

2.1 SVC DRM 시스템의 개요

2.1.1 SVC DRM 시스템의 요구사항

본 논문에서 제안하는 시스템의 기본 가정들은 다음과 같다

- 각 장치는 인증기관으로부터 발급받은 개인키와 공개키 인증서를 장치에 탑재한다.
- 각 장치가 안전하게 소유한 인증서와 키 정보들을 저장하고 콘텐츠 사용 규칙들을 수행하기 위해 신뢰된 DRM 에이전트(agent)를 DRM 서버로부터 다운로드 받는다.
- 각 장치는 위조방지 모듈(tamper-resistant module)을 제공하는 TP(trusted platforms) 기반을 가정한다.
- 각 장치는 차별적인 성능을 가진 장치들에게 적합한 수준의 콘텐츠를 제공하기 위해서 SVC 헤더 파싱(Parsing) 기능과 H.264/SVC 추출기(Extractor) 기능을 가진다.

홈 네트워크 내에서 서로 다른 능력을 가진 장치들에게 각 장치에 적응적인 콘텐츠를 제공하기 위해서는 다음의 요구사항들을 만족해야 한다.

[요구사항 1] 상위 수준의 장치가 그에 따른 콘텐츠를 구입하고 라이센스를 발급 받았을 경우, 하위 수준의 장치에게 그것들을 효율적으로 재분배할 수 있어야 한다. 예를 들면, PC가 콘텐츠를 구입한 후, PMP에게 콘텐츠를 재분배 할 경우에 해당한다.

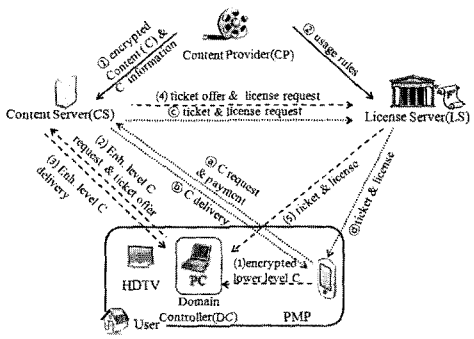
[요구사항 2] 하위 수준의 장치가 그에 따른 콘텐츠를 구입하고 라이센스를 발급 받았을 경우, 상위 수준의 장치에게 그것들을 효율적으로 재분배할 수 있어야 한다. 예를 들면, PMP가 콘텐츠를 구입한 후, PC에게 콘텐츠를 재분배 할 경우에 해당한다.

[요구사항 3] 사용자가 콘텐츠를 구입한 이후 홈 네트워크 내 상위 수준의 장치에서의 콘텐츠 사용을 고려하여 현재 요청하는 장치 보다 상위 수준의 콘텐츠를 구입한다면, 콘텐츠 서버는 현재 요청 장치에게는 장치에 적합한 콘텐츠와 라이센스를 제공하되, 사용자가 상위 수준 장치를 사용할 경우에는 콘텐츠의 재구매 과정이 생략된 상위 레이어 콘텐츠의 사용을 가능하게 한다. 예를 들면, 현재 PMP를 가지고 있는 사용자가 몇 시간 후 PC에서 콘텐츠를 보기 위해 PC 수준의 콘텐츠를 구입하였다면, 서버는 우선 PMP에게 맞는 콘텐츠와 라이센스를 제공하고 이후 PC 사용에서는 지불절차 없이 상위 레이어 콘텐츠를 손쉽게 제공해야 한다.

2.1.2 SVC DRM 시스템의 구조 및 구성요소

제안 시스템의 기본적인 구조는 그림 1과 같으며,

참여 개체들의 대략적인 기능과 동작은 다음과 같다.



〔그림 1〕 제안 DRM 시스템의 구조

- Content Provider(CP): 콘텐츠 제작자로부터 콘텐츠를 받아서 키 생성, 암호화, 헤더 생성, 패키징 등의 기능을 수행한다. ①콘텐츠 관련 정보와 패키징 된 콘텐츠를 CS에게 전송하고 ②콘텐츠에 대한 사용 규칙 정보와 콘텐츠 암호화 키를 LS에게 전송한다.
- Content Server(CS): 콘텐츠에 대한 가격 및 결제 처리 방법 등을 정한 후 DB에 저장하고, 웹 서비스와 같은 어플리케이션을 통해 콘텐츠 정보들을 제공한다. ⓐ사용자가 콘텐츠를 선택하고 지불을 완료하면, ⓑCS는 패키징 된 콘텐츠를 사용자에게 제공하고 ⓒ티켓과 라이센스 발급 요청을 위해 LS에게 구입한 콘텐츠 정보와 사용자 정보를 전송한다.
- License Server(LS): 콘텐츠 사용자에게 정책에 따른 사용 권한을 부여하고, 권한에 따른 라이센스 발급 및 관리를 수행한다. ⓓ제안 시스템의 LS는 티켓과 라이센스를 발급하고 관리한다.
- Domain Controller(DC): 도메인 내의 모든 장치들을 관리하고, 도메인에 장치를 추가하거나 제거하는 작업을 수행한다.

2.1.1절의 요구사항들을 살펴보면, 요구사항 1은 장치들 간의 통신만으로 콘텐츠와 라이센스 교환할 수 있지만, 요구사항 2와 3은 상위 레이어 콘텐츠를 얻기 위해서 CS와의 통신이 필요하다. 제안 기법은 사용자가 구입한 콘텐츠에 대한 정보를 티켓을 통해 CS에게 전달함으로써 문제를 해결한다. 티켓은 도메인 내 장치들이 구입한 콘텐츠를 장치 성능에 맞게 사용할 수 있도록 돕는 반면, 라이센스는 암호화 된 콘텐츠를 사용하는데 필요한 사용자의 사용 권한과 콘텐츠의 복호화 키를 제공한다. 티켓은 별도의 정보로 전달 될 수도 있지만, 기존의 라이센스를 확장하여 티켓 필드를 추가 정의함으로써 전달 될 수도 있다. 조건2의 경우, (1)홈 네트워크 안의 하위 수준 장치는 상위 수준 장치에게 하위 수준의 콘텐츠와 해당 티켓을 전송한다. (2)상위 수준 장치가 장치 정보와 티켓을 이용하여 CS에게 하위 장치로부터 받은 콘텐츠에 부가될 상위 레이어들을 요청하면, CS는 그에 대한 비용을 책정한다. (3)수신 장치로부터 지불이 완료되면, CS는 장치에게는 콘텐츠를 제공하고 (4)LS에게는 티켓을 전송하여 라이센스를 요청한다. 마지막으로, (5)LS는 티켓 정보를 이용해 사용자 권한에 맞는 라이센스를 발급한다. 조건 3의 경우는 조건 2와 동일하나 상위 레이어들에 대한 선 지불이 이루어지므로 지불 과정이 생략된다.

도메인 생성/등록은 도메인 내에 포함될 장치 중 성능이 가장 좋은 장치 하나를 도메인 서버인 DC로서 선택하고, 필요한 정보들을 설정하여 LS에게 전송하고 도메인 내 공유 비밀키인 도메인 키 KD 수신함으로서 이루어진다. 이후 도메인에 등록을 요청하는 장치들은 등록과 동시에 DC를 통해 도메인 키 KD를 얻게 되고, 도메인 내에서 콘텐츠를 사용할 때 KD를 사용하게 된다. 본 논문에서는 도메인 생성/등록과 장치의 등록이 안전하게 수행되었다고 가정한다. 이러한 도메인 생성/등록, 장치 등록의 과정들은 Abbadi에 의해 제안된 기법[3]과 같이 기존의 도메인 DRM 메커니즘들을 이용하여 처리될 수 있으며, 본 논문에서는 콘텐츠 분배과정에 초점을 맞추어 제안한다.

2.2 도메인 내에서의 스케일러블 콘텐츠 재배포

2.2.1 콘텐츠 서버(CS)로부터 콘텐츠 전송

도메인 내 장치 D_A가 CS와 LS로부터 콘텐츠와 라이센스 및 티켓을 전송받는 과정은 다음과 같다.

1) D_A는 콘텐츠 요청을 위해 D_A의 인증서($Cert_A$), 도메인 ID(Domain_ID), 콘텐츠 ID(CID), D_A의 수준(D_level_A), 사용자가 구입을 원하는 콘텐츠의 수준(C_level), nonce 값(N_A) 그리고 KD를 이용한 메시지 인증 MAC 값을 포함하는 Content_Request 메시지를 CS에게 전송한다.
2) CS는 LS와 안전한 세션이 미리 설정되었다는 가정 하에서, 수신된 Domain_ID를 LS에게 전송하여 도메인 키 K_D를 얻은 후, D_A로부터 수신된 MAC값을 검증한다.

3) CS는 지불 요청을 위해 $Cert_{CS}$, CS의 nonce 값인 N_{CS}, D_A로부터 수신한 N_A 그리고 서명 값 SignCS를 포함하는 지불 요청 메시지인 Pay_Req_Info 메시지를 D_A에게 전송한다.

4) D_A는 지불 정보인 Pay_Info를 CS의 공개키로 암호화하여 $E_{Pu_{CS}}$(Pay_Info, DIDA, Domain_ID, N_A, N_{CS}, $Sign_A$(Pay_Info, DIDA, Domain_ID, N_A, N_{CS})) 형태로 CS에게 전송한다.

5) CS는 CS의 개인키를 사용하여 수신된 정보를 복호화하고, 얻어진 정보를 이용해서 서명 값 $Sign_A$을 검증한다. 검증이 성공적으로 이루어지면, CS는 사용자가 구입을 원하는 콘텐츠의 수준 C_level와 콘텐츠를 요청한 장치의 수준 D_level_A와 비교하여 다음과 같이 장치 D_A가 수신할 콘텐츠의 수준 $Level_A'$을 결정한다.

$$Level_A' = \begin{cases} D\_Level_A, & \text{if}(C\_Level \geq D\_Level_A), \\ C\_Level, & \text{otherwise.} \end{cases} \quad (1)$$

CS는 콘텐츠 암호화 키(KC)에 의해 암호화 된 콘텐츠 $E_{K_C}(C)$ 중에서 장치 DA에게 적합한 수준$Level_A'$에 해당하는 일부의 레이어들로 구성된 콘텐츠 $E_{K_C^n}(C_A)$을 DA에게 전송한다. 이때, 암호화는 [8]의 기법과 같이 계층적으로 암호화되며, K_C^n는 DA가 수신할 콘텐츠 수준의 암/복호화 키를 의미한다.

6) 동시에 CS는 D_A를 위한 티켓과 라이센스를 요청하기 위해 $Cert_A$, Domain_ID, CID, C_level, DID_A, $Level_A'$, $H(C_A)$, N_A, N_{CS}을 LS에게 전송한다.

7) LS는 콘텐츠 복호화 키 K_C를 해쉬 함수를 이용해 $Level_A'$에 대응하는 키로 생성한다. 다시 말해, 콘텐츠의 가장 상위 수준 h의 키가 K_C일때, $Level_A'$를 위한 키는 n(=h-$Level_A'$)번 암호학적 해쉬함수가 적용된 $K_C^n = H^n(K_C)$이 된다. 생성된 콘텐츠의 복호화 키 K_C^n를 포함하는 라이센스(L)와 사용자가 구입한 콘텐츠의 수준 정보를 포함하는 티켓(T)은 식 (2)와 (3)과 같이 구성된다. 이후, LS는 DA의 공개키로 암호화 된 T와 L, CertLS 그리고 서명 값을 DA에게 전송한다.

$$T = (C\_ID \| C\_Level \| DID_A \| Level_A' \| Domain\_ID \| Sign_{LS}(C\_ID \| C\_Level \| DID_A \| Level_A' \| Domain\_ID)) \quad (2)$$

$$L = (E_{K_D}(usage\ rules \| K_C^n) \| H(C)) \| C\_ID \| C\_Level \| Domain\_ID \| Sign_{LS}(E_{K_D}(usage\ rules \| K_C^n) \| H(C)) \| C\_ID \| C\_Level \| Domain\_ID)) \quad (3)$$

8) D_A는 서명 값을 검증하고, 개인키를 사용하여 암호화 된 T와 L을 복호화 한다. 그리고 T와 L은 DRM 을 통해 안전하게 저장된다. 콘텐츠 실행 시, 각 장치의 DRM 은 라이센스에 포함된 복호화 키 K_C^n를 $Level_A'$(=h-n)번 해쉬 함수를 적용하여 각 레이어 키들은 구하고, 구해진 각 레이어 키 $K_C^h, K_C^{h-1}, \cdots, K_C^n$은 각 수준 $Level_0, Level_1, \cdots, Level_A'$의 레이어들을 복호화하기 위해 사용된다.

2.2.2 도메인 내 장치 간의 콘텐츠 재배포

다음은 2.1.1절에 제시된 요구사항들에 따른 도메인 내 SVC 콘텐츠의 재분배 기법을 기술한다.

[요구사항 1] 상위 수준의 장치 DA가 콘텐츠를 구입한 후, 하위 수준의 장치 DB에서 콘텐츠를 재사용할 경우 콘텐츠 재분배 과정은 다음과 같다.

1) D_B는 $Cert_B$, Domain_ID, CID, D_level_B, 사용자가 새롭게 원하는 콘텐츠의 수준 $C\_level_B^*$ 그리고 KD를 이용한 MAC 값을 포함하는 Content_Request 메시지를 D_A에게 전송한다.

2) D_A는 소유하고 있는 K_D을 이용하여 MAC값을 검증한 후, ($Level_A'$ ≥ C_level*)를 만족하는지 확인하고, D_B에게 전송할 콘텐츠의 수준을 다음과 같이 결정한다.

$$Level_B' = \begin{cases} D\_Level_B, & \text{if}(C\_Level^* \geq D\_Level_B), \\ C\_Level^*, & \text{otherwise.} \end{cases} \quad (4)$$

이후, DA는 H.264/SVC extractor 기능을 이용해 $Level_B'$에 적합한 복호화 키 $K_C^{n'}$ ($n' = h - Level_B'$)를 가지는 콘텐츠 $E_{K_C^{n'}}(C_B)$을 콘텐츠 $E_{K_C^n}(C_A)$로부터 추출하여 생성한다. 그리고 재구성된 콘텐츠 $E_{K_C^{n'}}(C_B)$는 $Cert_A$, $E_{K_D}(T \| L)$ 그리고 이들 MAC 값과 함께 D_B에게 전송된다.

3) D_B는 K_D을 이용하여 MAC 값을 검증하고 수신된 라이센스와 티켓을 복호화 한다.

[요구사항 2] 하위 수준의 장치 D_A가 콘텐츠를 구입한 후, 상위 수준의 장치 D_B에서 콘텐츠를 재사용할

경우와 [요구사항 3] 하위 수준의 장치 D_A가 상위 수준의 콘텐츠를 구입한 후, 상위 수준의 장치 D_B에서 티켓을 이용해 콘텐츠의 상위 레이어들을 추가적으로 사용하고자 할 경우의 콘텐츠 분배 과정은 다음과 같다.

1) D_B는 $Cert_B$, Domain_ID, CID, D_level_B, C_level* 그리고 이들의 MAC 값을 포함하는 Content_Request 메시지를 D_A에게 전송한다.
2) D_A는 K_D을 이용하여 MAC값을 검증한다. 검증이 성공적으로 이루어지면, D_A는 ($Level_A' <$ C_level*)을 확인하고 $E_{K_C^a}(C_A)$, $E_{K_D}(L\|T)$, $Cert_A$, MAC 값을 D_B에게 전송한다.
3) DB는 DB에 적합한 해상도와 화질을 가지는 콘텐츠를 얻기 위해서 $Cert_B$, Domain_ID, D_level_B, C_level*, N_B, $E_{K_D}(T\|L)$, MAC 값을 Enhancement_Layers_Request 메시지에 포함시켜 CS에게 전송한다.
4) CS는 LS와 안전한 세션이 미리 설정되었다는 가정 하에서, 수신된 Domain_ID를 LS에게 전송하여 도메인 키 KD를 얻은 후, DB로부터 수신된 MAC값을 검증한다.
5) CS는 사용자가 새롭게 원하는 콘텐츠 수준 C_level*와 티켓에 포함되어 있는 구입된 콘텐츠의 수준 C_level 그리고 장치의 수준 D_levelB을 비교하여 D_B에게 전송할 콘텐츠의 수준을 다음과 같이 결정한다.

if C_Level* > C_Level (∵요구사항2)

$$Level_B' = \begin{cases} D\_Level_B, & \text{if}(C\_Level^* \geq D\_Level_B), \\ C\_Level^*, & \text{otherwise}, \end{cases} \quad (5)$$

else (∵요구사항3)

$$Level_B' = \begin{cases} D\_Level_B, & \text{if}(C\_Level \geq D\_Level_B), \\ C\_Level, & \text{otherwise}. \end{cases} \quad (6)$$

요구사항 2에 해당하는 수식 (5)는 이전에 구입한 콘텐츠 수준보다 상위 수준을 요구하므로 CS는 C_Level*−C_Level의 차익에 대한 지불 요청 Pay_Req_Info을 $Cert_{CS}$, N_{CS}, $Sign_{CS}$과 함께 D_B에게 전송한다. 반q_I요구사항 3에 해당하는 수식(6)은 지불 요청이 생략된다.

6) D_B는 암호화된 지불 정보 $E_{Puc_{CS}}$(Pay_Info, DID_B, N_B, N_{CS}, $Sign_B$(Pay_Info, DID_B, N_B, N_{CS}))을 CS에게 전송한다.
7) CS는 지불 확인 후 티켓으로부터 DA에 사용된 콘텐츠 수준을 얻어 $Level_B'-Level_A'$을 구하고, 그에 따른 암호화 된 콘텐츠의 상위 레이어들(Enhancement Layers)을 DB에게 전송한다.
8) 동시에 CS는 $Cert_B$, Domain_ID, C_level*, $Level_B'$, T, N_B, N_{CS}과 H(Enh.layerC)를 LS에게 전송하여 $Level_B'$에 대응하는 콘텐츠 복호화 키를 요청한다.
9) LS는 $Level_B'$에 대응하는 키를 포함한 라이센스를 생성하고 티켓을 다음과 같이 업데이트한다. 이때, T의 C_Level은 C_level* 값으로 업데이트된다. 그리고 이들을 D_B의 공개키로 암호화 한 후, $Cert_{LS}$, 서명 값과 함께 D_B에게 전송한다.

$$T = (C\_ID\|C\_Level\|DID_B\|Level_B'\|Domain\_ID\| Sign_{LS}(C\_ID\|C\_Level\|DID_B\|Level_B'\| Domain\_ID)) \quad (7)$$

10) DB는 서명값 $Sign_{LS}$을 검증한 후, 라이센스와 티켓을 D_B의 개인키로 복호화하여 사용한다.

III. 제안 기법 분석

제안된 SVC DRM의 가장 큰 특징은 개별적인 성능과 동적인 채널 능력을 가지는 각 장치에게 적응적으로 콘텐츠를 제공한다는 것이다. 따라서 제안 기법의 특징은 다음과 같다.

- 제안 시스템은 SVC DRM에서 콘텐츠를 장치에 적응적으로 제공하기 위한 세 가지 요구사항을 제시하였으며, 요구사항들을 만족하는 DRM을 설계하기 위해 티켓을 사용하였다. LS는 도메인 내 장치가 구입한 콘텐츠 수준에 대한 정보를 티켓에 포함시켜 라이센스와 함께 장치에게 제공함으로서, 도메인 내 다른 장치들은 콘텐츠를 구입한 장치에게 적합한 수준의 콘텐츠가 아닌 수신할 장치에 적합한 수준의 콘텐츠를 얻을 수 있다.
- 제안 시스템의 각 장치는 차별적인 성능을 가진 다른 장치들에게 적합한 수준의 콘텐츠를 재분배하기 위해서 SVC 헤더 파싱 기능과 H.264 /SVC 추출기 기능을 가진다. 각 장치에 이와 같은 기능들을 부가적으로 적재시키는 것은 서버가 아닌 클라이언트에게 추가적인 비용을 부과하지만, 어플리케이션이 단순하여 구축이나 운용상의 어려움을 갖지 않고, 최근 클라이언트 성능의 발전 속도를 고려하면 이는 충분히 수용가능한 문제이다.
- 제안 시스템은 같은 도메인 내에 있는 장치들이 콘텐츠를 자유롭게 사용할 수 있도록 하기 위해 도메인 키를 사용하였다. DC는 도메인 생성/등록 과

정에서 LS로부터 수신된 도메인 키는 도메인에 등록된 장치들에게만 분배되고, 같은 도메인에 등록된 장치들은 도메인 키를 이용하여 복잡한 절차 없이 라이센스와 티켓을 공유할 수 있다.

제안된 SVC DRM 기법은 일반적인 DRM 기법들과 마찬가지로 물리적 또는 디지털적인 방법들을 사용하여 허가되지 않은 사용자들이 콘텐츠에 접근하지 못하도록 보호하는 것이 중요한 목표이다. 제안 기법에서는 다음과 같은 안전성을 제공한다.

- 각 장치는 위조방지 모듈을 제공하는 TP 기반을 가정한다. 이것은 장치 인증서, 도메인 키, 티켓, 라이센스, 그리고 암호화 된 콘텐츠를 사용하고 저장하는 동안에 기밀성과 무결성을 제공한다. 또한, 티켓과 라이센스는 수신하는 장치의 공개키 또는 도메인 키 KD로 암호화되어 전송되므로 복호화 과정은 수신한 개체의 개인키 또는 도메인 키를 요구하게 되고, 그 과정은 DRM을 통해서만 수행되므로 안전성을 보장하게 된다.
- 같은 도메인에 속한 장치들은 라이센스와 티켓을 공유하기 위해 도메인 키인 KD를 사용한다. KD는 모든 장치들의 TP 모듈에 바인딩되어 수행되고, DC에 등록되어 KD를 얻은 장치들만이 콘텐츠를 사용할 수 있다. 또한, KD와 nonce 기반 challenge-response 프로토콜을 사용하여 안전성을 보장한다.
- 제안 기법에서는 라이센스 안에 Domain_ID를 포함시켜, 콘텐츠를 사용할 때 장치에 저장된 Domain_ID와 동일한지를 확인하다. 이를 통해 콘텐츠의 불법적인 사용과 재배포를 방지한다. 또한 손상되거나 위조된 장치들이 도메인에 등록되거나 불법적으로 콘텐츠를 사용하는 것을 방지하기 위해, 이들 장치들의 리스트를 관리하는 것이 필요하다. 이를 위해 LS가 취소된 장치 리스트를 주기적으로 DC에게 발행할 수 있으며, 또는 DC의 도메인 등록 또는 도메인 키 갱신과 같은 단계에서 전달될 수도 있다.

IV. 결 론

본 논문에서는 홈 네트워크 내 개별적인 성능과 동적인 채널 능력을 가지는 각 장치에게 적응적으로 콘텐츠를 제공하는 SVC DRM의 재분배 메커니즘을 제안하였다. 제안 시스템에서 같은 도메인에 등록된 장치들은 서로의 장치에게 알맞은 수준의 콘텐츠를 제공할 수 있어야 한다. 이를 위해, SVC 콘텐츠를 효율적으로 재분배하기 위한 세 가지 요구사항을 제시하였으며, 티켓을 사용하여 이 요구사항들을 해결하는 재분배 메커니즘을 제안하였다. 향후 단일 도메인의 제안 기법은 다중 도메인 간 분배에서도 적용될 수 있도록 확장되어야 하며, 콘텐츠와 라이센스 등을 관리하는 DC의 역할 및 향상된 도메인 관리 기법은 SVC DRM 모델에서 명확하게 제시해야 한다. 더불어, 실제 서비스 방안에서 장치들 간의 콘텐츠 공유(share), 전송(transfer), 임대(loan) 등의 다양한 서비스 시나리오가 연구되어야 한다.

참 고 문 헌

[1] 왕보현, "DRM에서 디바이스 식별자를 이용한 재배포 관리 메커니즘에 관한 연구," 박사학위논문, 경원대학교 전자계산학과, 2008년 2월.

[2] 문주영, "Home Domain 기반의 콘텐츠 재배포를 위한 DRM System 설계," 박사학위논문, 숭실대학교 컴퓨터학과, 2008년 2월.

[3] I. Abbadi, "Digital rights management for personal networks," RHUL-MA-2008-17, Royal Holloway, University of London, 2008.

[4] H.G. Kim, "Scalable DRM System for Media Portability," ASIAN 2007, LNCS 4846, pp. 78-85, 2007.

[5] B. Valer and F.C. Mihai, "Scalable and Secure Architecture for Digital Content Distribution," SoftCOM2006, pp. 182-187, Sep. 2006.

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

[7] W. Weigand, G.J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC Video Coding Standard," IEEE Trans. on Circuits and System for Video Technology, vol. 13, no. 7, pp. 560-576, July 2003.

[8] S.W. Park and S.U. Shin, "An Efficient Encryption and Key Management Scheme for Layered Access Control of H.264/Scalable Video Coding," IEICE Trans. on information and systems, vol. E92-D, no. 5, pp. 851-858, May 2009.