CDN 환경에서 콘텐츠 보안 방법 연구*

김점구** · 김태은***

요 약

인터넷 사용자의 폭발적 증거와 전자상거래를 통한 디지털 컨텐츠 유통 시장의 성장 등으로 인해 급격히 증가하는 네트워크 트래픽을 수용하고 처리하기 위해 다양한 연구들이 진행되고 있다. 본 논문은 새로운 네트워크 서비스의 중심으로 등장할 CDN 시스템 환경에서 디지털 컨텐츠와 저작권을 보호하기 위한 방안으로 CDN 기반의 분산 DRM 시스템을 설계한다. 이를 위해 분산 저장되어 있는 컨텐츠에 보다 강한 보안성을 제공하는 DRM 패키지 형식이 정의되었으며, 기존의 CDN 시스템과 상호 운용하기 위한 분산 DRM 시스템의 동작 절차를 제시한다.

A Study on Contents Security Method Based on a Content Delivery Network

Jeom Goo Kim** · Tae Eun Kim***

ABSTRACT

Is caused by with growth etc. of the digital contents circulation market which leads suddenly accommodates in order to control the network traffic which increases and the researches which are various are being advanced the explosive evidence and a electronic transaction of the Internet user. The present paper protects a digital contents and a copyright from CDN system environments which will appear the center of new network service with the plan for the dispersive DRM system of CDN bases plans. Respect this dispersion DRM package formats which provide a stronger security characteristic in the contents which is stored the operational process of the dispersive DRM system for to be defined, CDN system and of existing interoperability they present.

Key words : Contents, Security

* 본 논문은 문화관광부 한국문화콘텐츠진흥원및 충남디지털문화산업진흥원의 지원에 의해 수행되었음.
** 남서울대학교 컴퓨터학과
*** 남서울대학교 멀티미디어학과

1. 서 론

최근 인터넷 정보통신 기술의 발전으로 인한 인터넷 사용자의 폭발적 증거와 전자상거래를 통한 디지털 컨텐츠 유통 시장의 성장 등으로 인해 급격히 증가하는 네트워크 트래픽을 수용하고 처리하기 위해 다양한 연구들이 진행되고 있다. CDN 서비스는 기존의 네트워크 구조, 설비를 변경없이 사용하면서 컨텐츠 캐싱 기술을 이용해 네트워크 간의 트래픽을 효과적으로 감소시킬 수 있으며 서비스의 품질을 향상시키는 방법을 제시하고 있어 새로운 네트워크 서비스의 주축으로 성장할 것이다.

그러나 분산되어 있는 디지털 컨텐츠는 저작권 보호나 보안에 더 많은 취약성을 가지고 있고, 분산 저장된 컨텐츠를 서비스하기 위한 CDN 시스템의 동작절차는 기존의 단일 서버 시스템에서의 서비스와 다른 동작절차를 보여주고 있다. 이러한 CDN 시스템에서 디지털 컨텐츠의 저작권 관리를 위해서 분산 환경에 적용될 수 있는 새로운 DRM (Digital Right Management) 시스템이 요구된다.

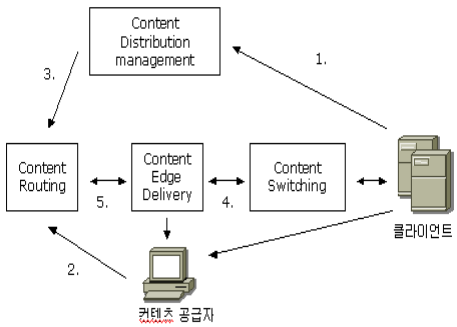
DRM은 디지털 컨텐츠를 암호화하여 인터넷상에서의 거래를 안전하게 보장하며, 저작권자의 권리를 보호하는 기술이다. 다른 표현으로 신뢰성 있는 라이센스, 안전한 저작권과 허가, 신뢰성 있는 환경과 인프라를 가능하게 하는 H/W, S/W를 포함하는 디지털 저작권 관리를 위한 넓은 의미의 기술, 절차, 처리, 알고리즘이라고 한다.

본 논문은 분산 환경에서 더욱 강한 보안성을 가지며, 유연하게 관리될 수 있는 분산 DRM 패키지를 정의하고, CDN 시스템 서비스의 각 동작절차에서 분산 DRM 패키지가 처리되는 과정들을 기술한다. 또한 CDN 시스템과 상호 동작하기 위하여 요구되는 분산 DRM의 추가 메시지들과 동작절차를 기술하여 분산 DRM 시스템 모델을 설계한다.

2. 관련 연구

2.1 CDN(Contents Delivery Network)

CDN은 네트워크의 주요지점에 전략적으로 설치된 시스템을 통해 사용자의 가장 가까운 지점에서 컨텐츠를 전송함으로써 네트워크 상에서 발생하는 병목현상 및 데이터 손실을 줄여 사용자에게 보다 빠르고 안정적으로 컨텐츠를 배포하는 서비스이다. 이와 같은 CDN의 동작 방식은 (그림 1)과 같다.



(그림 1) CDN의 동작 방식

Content Distribution and Management 요소는 제작된컨텐츠를 지역 네트워크의 로컬 캐시 서버로 분배하는 기능, 분배된 컨텐츠에 대한 복구, 갱신 및 동기화와 같은 기능, 그리고 분산 서버들에 대해 실시간으로 다양한 정보를 수집하는 기능을 하며, Content Edge Delivery 요소는 지역 네트워크의 로컬 캐시 상에 저장된 컨텐츠에 대한 사용자 서비스를 제공하고 컨텐츠 분배 및 관리 시스템과 연계하기 위한 서버의 다양한 성능정보를 수집하여 제공하는 기능을 하며, Content Routing 요소는 사용자의 컨텐츠 요청에 대해 사용자에게 가장 효과적인 서비스를 제공할 수 있는 로컬 캐시 시스템을 찾는 기능을 하고, Content Switching 요소는 컨텐츠 라우팅에 의해 선택된 캐시 시

스템에서 Load balancing, 서버 장애 등 다양한 상황을 고려하여 최상의 서버를 찾는 기능을 한다.

(그림 1)의 동작방식에서 먼저 클라이언트는 content distribution 요소에 컨텐츠를 요청한다. 컨텐츠 공급자는 미리 2의 과정을 통해 컨텐츠를 분배한다. content routing 요소에 의해 최적의 사이트를 찾게 되모 Content edge delivery를 통해 최적의 서버로부터 컨텐츠를 클라이언트에게 제공하게 된다.

CDN 시스템에서 미들-마일 구간을 통과하는 트래픽의 양을 감소하기 위해 사용하는 핵심기술은 캐싱(Caching) 기술, Load balancing 기술, 스트리밍(Streaming) 기술로 구성된다.

2.2 DRM(Digital Right Management)

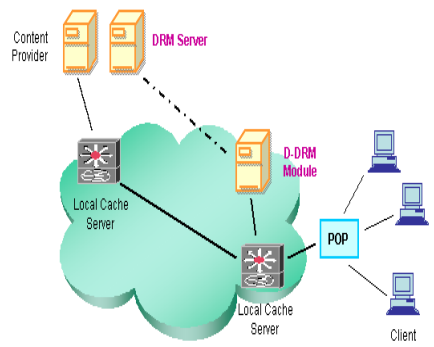
DRM은 디지털 컨텐츠를 암호화하여 인터넷상에서의 거래를 안전하게 보장하며, 저작권자의 권리를 보호하는 기술이다. 다른 표현으로 신뢰성 있는 라이센스, 안전한 저작권과 허가, 신뢰성 있는 환경과 인프라를 가능하게 하는 H/W, S/W를 포함하는 디지털 저작권 관리를 위한 넓은 의미의 기술, 절차, 처리, 알고리즘이라고 한다.

이러한 디지털 컨텐츠의 저작권자 권리를 보호하며 디지털 컨텐츠를 보안하는 방법 중 적극적인 방법으로는 DRM과 소극적인 방법인 워터마크(Watermark) 기술이 있다.

3. 분산 DRM 설계

본 논문에서 기반으로 하는 컨텐츠 유통 네트워크 모델은 CDN 시스템이 구성되어 각 지역 네트워크의 로컬 캐싱 서버에 컨텐츠가 분산 저장되어 있는 구조이다.

분산 DRM 시스템은 CDN 시스템의 각 구성 요소들이 기본이 되고, DRM 서비스를 제공하기 위해 하나의 DRM 서버와 각 로컬 캐시 서버 당 하나의 D-DRM 모듈(Distributed DRM module)이 추가된다. DRM 서버는 각 컨텐츠에 대한 비밀키와 사용자에 대한 정보를 관리하며, 컨텐츠에 대한 비밀키를 사용자 정보로 가공하여 D-DRM 모듈에 전달하는 역할을 한다. D-DRM 모듈은 인증된 사용자의 컨텐츠 요청에 대해 DRM 서버에 비밀키를 요청하며, 가공된 비밀키를 수신 받아 DRM 패키지의 해당 위치에 삽입시키는 역할을 한다.

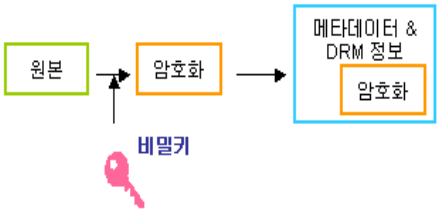


(그림 2) 컨텐츠 유통 네트워크 모델

분산 DRM 시스템은 컨텐츠의 안전한 유통과 보호를 위해서 컨텐츠가 컨텐츠 제공자로부터 지역 네트워크의 로컬 캐시 서버로 배포되는 과정과 로컬 캐시 서버에 저장되어 있는 시기, 최종 사용자에게 전송되는 과정과 사용자가 컨텐츠를 소유하고 있는 시기 등에 컨텐츠에 대한 보호가 이루어져야 한다.

본 논문에서 제안하는 디지털 컨텐츠는 일차적으로 컨텐츠의 원본이 DRM 패키징 과정 거쳐 가공되고, 패키징 된 컨텐츠가 CDN의 분배 시스템을 통하여 분배 된다. 컨텐츠 원본의 패키징 과정은 (그림 3)과 같다.

DRM 컨텐츠 패키징 과정은 최초의 디지털 원본 컨텐츠를 비밀키 암호화 알고리즘을 사용하여 컨텐츠를 암호화 한다. 각 컨텐츠는 고유한 암호

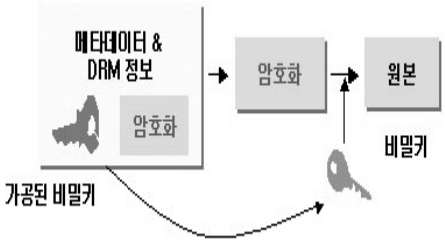


(그림 3) 컨텐츠 원본의 패키징 과정

화 비밀키를 가지게 되며, 각 컨텐츠에 대한 비밀키들은 DRM 서버에 저장되고 관리되어야 한다.

암호화된 컨텐츠는 메타데이터와 기본적인 DRM 정보에 의해 다시 포장되어 패키징 과정이 일차 완료되며, CDN의 분배 시스템을 통해 각 네트워크의 로컬 캐시 서버로 분배되어 진다.

인증 또는 지불 절차를 거친 사용자가 컨텐츠를 요청하게 되면, D-DRM 모듈은 컨텐츠 ID 정보와 사용자 정보를 DRM 서버에게 전송한다. DRM 서버는 사용자의 정보를 이용하여 해당 컨텐츠의 비밀키를 가공하여 D-DRM 모듈에 전달하고, D-DRM 모듈은 DRM 패키지의 Contents Key 필드에 가공된 비밀키를 삽입된 후 DRM 패키지를 사용자에게 전송한다.



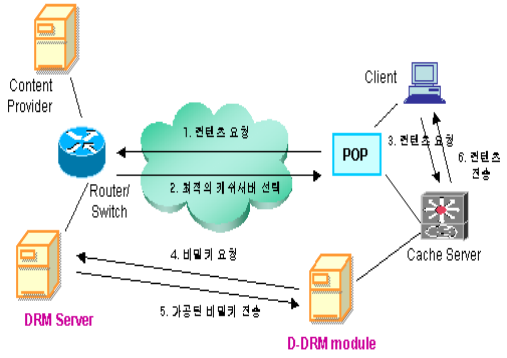
(그림 4) 분산 DRM의 컨텐츠 사용

사용자의 DRM 클라이언트 모듈은 수신 받은 패키지 내에서 가공된 비밀키를 추출하여 자신의 정보를 이용하여 비밀키를 유출하며, 이 비밀키로 암호화된 컨텐츠를 (그림 4)와 같이 복호화 하여 사용하게 된다.

4. CDN 기반의 분산 DRM의 동작 절차

본 논문에서 제안하는 분산 DRM 시스템은 CDN 시스템에 기반을 두므로 CDN 시스템의 동작 절차와 매우 유사하다.

최초의 원본 디지털 컨텐츠는 컨텐츠 제공자에 의해서 분산 DRM 패키지로 변형된다. 즉, 컨텐츠는 고유한 비밀키로 암호화되며 헤더와 메타데이터 정보가 삽입된다. 다음 과정으로 제작된 분산 DRM 패키지는 CDN의 분배 시스템에 의해 각 지역 네트워크의 로컬 캐시 서버로 분배된다. 분배가 완료된 후에는 사용자의 요청을 대기하는 상태가 된다.



(그림 5) CDN 기반의 분산 DRM의 동작 절차

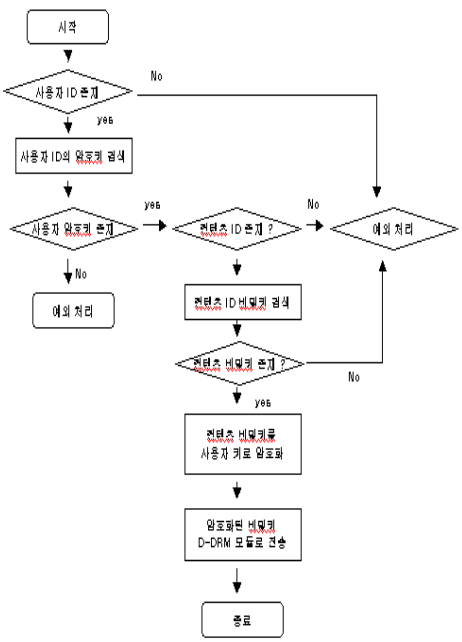
1) 사용자가 컨텐츠를 요청
2) 컨텐츠 라우팅을 통해 최적의 캐쉬 서버 검색
3) 사용자는 해당 캐수 서버에 컨텐츠 재요청
4) 컨텐츠 요청을 받은 D-DRM 모듈은 해당 컨텐츠의 비밀키를 얻기 위해 DRM 서버로 비밀키 요청
5) DRM 서버는 D-DRM 모듈로부터 정보를 수신하고, 비밀키 관리 시스템으로부터 컨텐츠

ID에 해당하는 비밀키를 검색하고, 검색된 결과인 비밀키를 사용자 정보를 사용하여 가공하여 D-DRM 모듈로 전송

6) 해당 컨텐츠의 분산 DRM 패키지 헤더에 있는 Content Key 필드를 가공된 비밀키로 갱신하고, 컨텐츠를 요청한 사용자에게 분산 DRM 패키지를 전송

5. 분산 DRM 시스템의 동작 알고리즘

분산 DRM 시스템의 동작 알고리즘은 (그림 6)과 같다.



(그림 6) 분산 DRM 시스템의 동작 알고리즘

1) 원본 컨텐츠를 고유의 비밀키로 암호화한 메타데이터와 헤더를 삽입하여 DRM 패키지를 생성하고, 컨텐츠의 비밀키를 DRM 서버에 등록한다.
2) CDN의 분배 시스템을 이용하여 지역 네트워크의 로컬 캐시 서버로 DRM 패키지를 분배하고, 한다.
3) 컨텐츠 서버는 사용자의 요청을 기다린다.
4) 사용자의 컨텐츠 요청이 발생하면, CDN 시스템의 Content Routing, Content Switching을 사용하여 최적의 로컬 캐시 서버를 찾아 요청을 redirect 시킨다.
5) 컨텐츠 요청을 받은 D-DRM 모듈은 컨텐츠 ID와 사용자 정보를 가지고 DRM 서버에 비밀키를 요청하고, DRM 서버의 응답을 기다린다. D-DRM 모듈이 사용자 정보를 획득할 수 없을 경우 동작을 중단한다.
6) 비밀키 요청을 받은 DRM 서버는 해당 컨텐츠 ID와 사용자 정보를 검색하고 컨텐츠의 비밀키를 사용자 정보로 가공하고, D-DRM 모듈로 전송한다. 컨텐츠 ID에 해당하는 비밀키나 사용자 정보를 찾을 수 없는 경우 동작을 중단한다.
7) D-DRM 모듈은 가공된 비밀키를 수신하고, DRM 패키지 내의 컨텐츠 키 필드에 삽입한다. 지정된 시간동안 DRM 서버로부터 비밀키를 수신하지 못하면 동작을 중단한다.
8) 로컬 캐시 서버는 DRM 패키지를 사용자에게 전송하고 동작을 종료한다.

6. 결론 및 향후 연구 방향

본 논문에서는 새로운 네트워크 서비스의 중심으로 등장할 CDN 시스템 환경에서 디지털 컨텐츠와 저작권을 보호하기 위한 방안으로 CDN 기반의 분산 DRM 시스템을 설계하였다. 이를 위해 분산 저장되어 있는 컨텐츠에 보다 강한 보안성을 제공하는 DRM 패키지 형식이 정의되었으며, 기존의 CDN 시스템과 상호 운용하기 위한 분산 DRM 시스템의 동작 절차가 제시되었다.

제안된 분산 DRM 패키지는 더욱 신뢰성 있는 비밀키 관리와 지불 시스템이 지원된다면, Peer-to-Peer 네트워크 환경을 통해 사용자간에 발생하는 디지털 컨텐츠 유통 시스템도 지원 가능하고, 미래에 나타날 새로운 디지털 컨텐츠 유통 환경에서도 융통성 있게 적응하며 높은 보안성을 제공할 것으로 기대된다.

참 고 문 헌

[1] 이창열, MPEG-21 기반 방송 컨텐츠 유통 프로토타입 시스템 개발, 한국전자통신연구원, 연구결과보고서, 2000년 12월.

[2] AAP, DigitalRightsManagemnet for Ebooks : Publisher Requirements version 1.0, 2000.

[3] ContentGuard, ContentGuard DRM Solution overview, October 2000.

[4] Joshua Duhl, and Susan Kevorkian, Understanding DRM Systems ; An IDC White Paper, 2001.

[5] MPEG-21 Overview v3.0, N4511, December 2001.

[6] Paul, John D. and ButlerW., Digital Rights Management Operating System, United State Patent6, 330, 670, December 11, 2001.

[7] Thomas Hardjono and Mark Baugher, IDRM Directions and Work Items, IETF-51 August 6, 2001.

[8] Carpenter, B., “Architecture Principles of the Internet”, RFC 1958, June 1996.

김 태 은

중앙대학교 전기공학과(공학사)
중앙대학교 전자공학과(공학석사)
중앙대학교 전자공학과(공학박사)
한국재단참여연구원
삼성전자 휴먼테크논문 대상
은상수상
현재 남서울대학교 멀티미디어학과 교수
관심분야 : 멀티미디어시스템, 영상인식, 증강현실, 웹3D처리기술

김 점 구

광운대학교 전자계산학과(이학사)
광운대학교 전자계산학과(이학석사)
한남대학교 컴퓨터공학과(공학박사)
(주)제성프로젝트 연구원
(주)시사컴퓨토피아 인터넷사업
본부장
현재 남서울대학교 컴퓨터학과 교수
관심분야 : 정보보호, 컴퓨터 네트워크, 무선통신