

통방송합환경에서의 상호운용적 DRM 툴 기술

최범석, 변영배, 남제호
한국전자통신연구원(ETRI) 방통융합콘텐츠보호연구팀

Interoperable DRM Tool Technology for communication and broadcasting conversions environment

B. S. Choi, Y. B. Byun, and J. Nam
ETRI Broadcasting Media Research Group

요 약

DRM 기술의 호환성 부재는 콘텐츠 소비 활성화에 큰 장애물로 부각되고 있다. 현재 상호운용적인 DRM 기술 개발을 위하여 다양한 산업체와 기관들이 DRM 기술에 대한 표준화 단체를 구성하고 이 문제를 해결하기 위해 노력하고 있다. 본 논문에서는 툴 개념을 기반으로 서로 다른 DRM 간의 상호운용성(interoperability)을 지원하는 방법에 대하여 설명한다.

1. 서론

다양한 네트워크와 사용자 단말이 혼재되어 사용되는 방송통신 융합 환경에서 멀티미디어 서비스가 효율적으로 제공되어지기 위해서는 ‘상호운용성(interoperability)’이 매우 중요한 문제로 대두된다. 특별히 DRM(Digital Rights Management) 기술에 있어서 상호운용성 문제는 디지털 콘텐츠 소비의 활성화를 막고 있는 큰 장애물로 인식되고 있다. 국제표준화 기구인 ISO/IEC 산하 MPEG 그룹에서는 DRM 기술의 상호운용성 문제를 해결하고자 MPEG IPMP(Intellectual Property Management and Protection) 기술을 표준화 하고 있다. MPEG IPMP 기술은 보호 기능(인증, 암호화, 워터마킹)을 모듈화(이하 DRM 툴)하고 이러한 DRM 툴과 함께 툴에 대한 정보 및 API

를 공개하므로 툴에 대한 상호운용성과 재사용을 허용하는 방식으로 상호운용성을 지원한다. 그러나 대부분의 서비스 제공자들은 그들만이 주로 사용하는 DRM 툴들을 개발하여 사용하고 있으며, 자신들이 사용하는 툴에 대한 정보(툴의 기능, 툴 API 등)가 외부에 공개되는 것을 극히 꺼리고 있다. 본 논문에서는 이러한 툴의 보안성을 최대한 보장하면서 툴에 대한 상호운용성을 지원하기 위한 툴팩(ToolPack) 기술에 대하여 설명한다.

2. 툴팩 기술

일반적으로 콘텐츠 제공자들은 자신들이 사용하는 고유한 툴들을 소유하고 있다. 툴팩의 개념은 이러한 툴들을 개별적으로 제공하기 보다는 툴그룹

(ToolGroup)으로 함께 제공하고 각기 고유한 툴그룹을 작동시키기 위한 툴에이전트(ToolAgent)를 두어 툴그룹과 툴에이전트를 툴팩으로 묶어 제공하는 개념이다

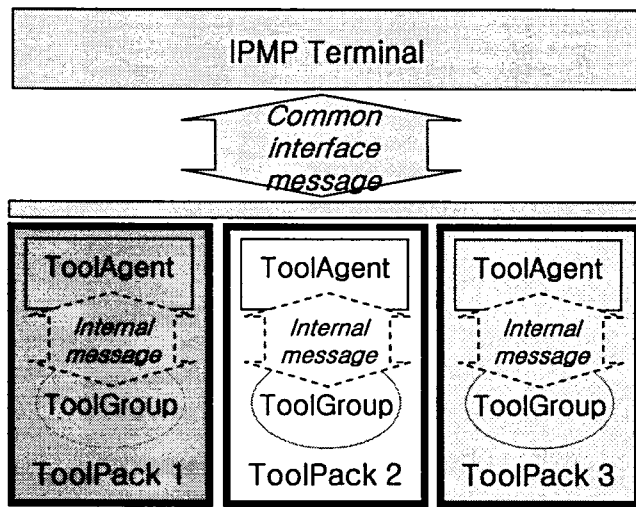


그림 2. 툴팩 핵심 개념

툴그룹의 개개의 툴과 툴에이전트는 내부 인터페이스를 사용하여 작동하며, IPMP 터미널과 같은 외부 모듈과의 동작은 그림 2에서 보여지듯이 공통 인터페이스를 통하여 작동하도록 한다. 따라서 개별툴에 의존적인 메시지를 정의할 필요가 없게되며 공통 인터페이스 메시지가 간략화된다. 즉, 새로운 툴팩이 적용되더라도 새로운 인터페이스 메시지를 정의할 필요가 없어지므로 툴에 대한 확장성이 증대된다. 또한 툴에 대한 개별적인 정보가 IPMP 터미널까지 전달되지 않으므로 툴에 대한 보안성이 높아진다고 할 수 있다.

3. 통방융합환경과 툴팩

본 장에서는 툴팩의 개념을 통방융합서비스 환경에 적용할 경우 필요한 처리 과정에 대하여 설명한다.

3.1 툴팩 등록

방송사는 서비스에 적용될 툴팩을 먼저 툴등록 서버에 등록할 필요가 있다. 방송사가 사용할 툴그룹

과 툴에이전트를 관련 정보와 함께 툴등록서버에 등록요청하면, 툴등록서버는 툴그룹과 툴에이전트에 대한 해쉬값을 생성하고 툴팩을 유일하게 구별시켜 줄 툴팩ID를 발급한다. 툴등록서버는 방송사가 제공할 툴팩정보와 툴팩ID를 생성하고 이를 툴등록서버의 개인키를 사용하여 서명한다. 마지막으로 툴등록서버는 툴팩헤더, 툴그룹, 툴에이전트를 툴팩스키마로 묶고 이를 방송사에게 전달하므로 툴팩 등록절차를 마치게 된다.

3.2 툴 업로드

툴 등록절차를 마친 툴팩은 툴관리서버에 업로드하여 다른 디바이스에서 사용할 수 있도록 해야 한다. 툴관리서버는 툴팩에 대한 업로드 요청을 받으면 툴팩 헤더정보와 바이너리 툴팩을 DB형태로 관리하게 된다.

3.3 서비스 신청

사용자가 최초로 서비스 요청을 하게되면 방송사는 사용자 인증 후, 사용자 단말에 툴관리서버의 위치와 툴팩ID를 알려준다. 단말은 툴관리서버에 필요한 툴팩을 요청하고, 툴관리서버는 요청한 툴팩을 검색하여 사용자의 단말로 전송하게 된다.

3.4 방송스트림 입력

IPMP 터미널은 방송스트림으로부터 방송 콘텐츠 소비에 필요한 툴팩정보(툴팩ID, 버전 등)를 추출하여 해석하고 필요한 툴팩을 로딩한 후 툴에이전트를 호출하게 된다[그림 3 참조]. 툴에이전트가 호출되면 IPMP 터미널은 툴들을 초기화하기 위한 정보를 담고 있는 툴팩데이터와 단말에서 가용한 콘트롤 포인트의 리스트를 툴에이전트에 넘겨주게 된다. 만일 사용자가 하나 이상의 서로 다른 서비스 채널에 대하여 동시에 다른 기능을 선택하게 되면, 각 서비스 채널에 대한 툴팩의 툴에이전트를 모두 호출하게 된다. 예를 들어 ETRI 서비스 채널은 일반 시청을 선택하고 동시에 KBS 채널은 녹화를 선택하였다면, ETRI 서비스 채널에 대한 툴에이전트와 KBS 서비스 채널에 대한 툴에이전트가 동시에 호출되어 사용자가 선택

The diagram illustrates the system architecture. On the left, an 'AV' input (MPEG-2 TS) is received. This signal is processed by a 'DEMUX' block, which splits it into 'Audio DB' and 'Video DB' paths. These paths lead to 'Audio Decode' and 'Video Decode' blocks, respectively. The decoded signals are then combined in a 'Multiplexer' block, which also receives input from a 'Content Storage' (콘텐츠 저장소). The output of the Multiplexer is sent to a 'Renderer' block. A 'Control Point' (● Control Point) is shown at the bottom, which manages the system by interacting with the 'Content Storage' and a set of 'Tools' (Tool1, Tool2, ..., ToolN). The 'Tools' are represented by a cluster of circles, and the 'Content Storage' is represented by a cylinder.

3.5 톨 초기화 및 연결

3.6 미싱(missing) 툴 처리

3.7 튜블 갱신

갱신되는 경우에는 방송스트림과 함께 ToolPack update message 또는 Tool update message가 전송되며 IPMP 터미널은 본 메시지를 통하여 툴 갱신을 수행하게 된다. 만일 툴 갱신 메시지 안에 바이너리 툴팩 또는 툴이 존재한다면, 바로 툴 갱신이 이루어지지만, 바이너리 툴팩 또는 툴 없이 툴팩 또는 툴에 대한 정보만 존재한다면, IPMP 터미널은 툴관리서버에 접속하여 해당 툴팩 또는 툴을 요청하여 다운로드 한다.

4. 주요 요소 기술

4.1 컨트롤 포인트

| Control Point | Description |
|---------------|-------------|
| 0x00 | 사용 안함 |
| 0x01 | 역 다중화 전 |
| 0x02 | 오디오 디코딩 전 |
| 0x03 | 오디오 디코딩 후 |
| 0x04 | 비디오 디코딩 전 |
| 0x05 | 비디오 디코딩 후 |
| 0x06 | 저장 전 |
| 0x07 | 재생 전 |
| 0x08 | 전송 전 |
| 0x09 ~ 0x30 | 예비 콘트롤 포인트 |

표 1. 컨트롤 포인트 리스트

4.2 톨팩 스키마

227

트와 툤팡 데이터를 포함하는 ToolPackDataInfo 파트, 그리고 서명(signature)으로 구성된다. 툤팡은 IPMP 터미널에 의하여 파싱된다. 툤팡의 XML 스키마 구조는 다음과 같다.

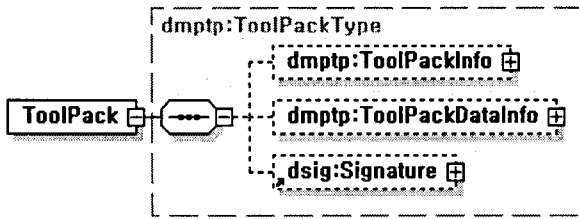


그림 4. 툤팡 스키마 구조

ToolPackInfo 엘리먼트에는 툤팡 ID와 팩, 그리고 서명을 포함한다. 다음은 ToolPackInfo 엘리먼트의 스키마 구조를 나타낸다.

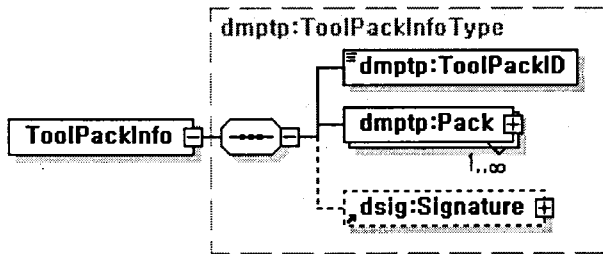


그림 5. ToolPackInfo 스키마 구조

Pack 엘리먼트는 툰에이전트와 툰그룹, 그리고 툰에이전트와 툰그룹이 작동할 수 있는 타겟 플랫폼에 대한 정보를 포함한다. 다음은 Pack 엘리먼트의 스키마 구조를 나타낸다

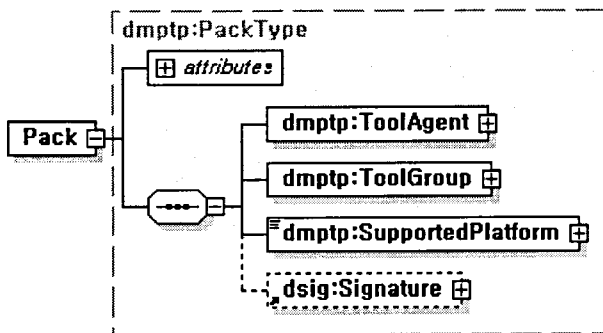


그림 6. Pack 스키마 구조

4.3 인터페이스 메시지

툴팩을 초기화 하고 툰팩을 작동시키기 위하여 IPMP 터미널과 툰에이전트 사이에 공통으로 사용할 수 있는 메시지를 정의한다. 주요 메시지는 표 2와

같다.

| 메시지 이름 | 기능 |
|---------------------------|--------------|
| InitAuthentication_msg | 툴 인증 초기화 |
| MutualAuthentication_msg | 상호 인증 |
| GetToolGroupInstance_msg | 툴 그룹 요청 |
| SendToolGroupInstance_msg | 툴 그룹 전달 |
| GetToolInstances_msg | 개별 툰 요청 |
| SendToolInstances_msg | 개별 툰 전달 |
| GetToolPackData_msg | 툴팩 데이터 요청 |
| SendToolPackData_msg | 툴팩 데이터 전달 |
| GetControlPointList_msg | 컨트롤포인트리스트 요청 |
| ConnectToolPack_msg | 컨트롤포인트리스트 전달 |
| NotifyToolPackEvent_msg | 툴 이벤트 전달 |
| DisconnectToolPack_msg | 툴 연결 해제 |

표 2. 인터페이스 메시지

5. 결론

본 논문에서는 상호운용성을 지원하는 툰 기반 DRM 기술에 대하여 소개하였다. 툰팩의 특징은 서비스 제공자 입장에서는 개별 툰에 대한 API 및 툰 정보를 공개할 필요가 없으므로 툰을 보다 안전하게 제공할 수 있도록 하며, 사용자 입장에서는 하나의 단말 디바이스에서 다양한 서비스 제공자들의 콘텐츠를 변환없이 소비할 수 있도록하므로 콘텐츠 사용에 대한 편리성을 제공할 수 있다. 또한 단말 디바이스 제조자 입장에서는 하나의 단말 플랫폼으로 디바이스를 제작할 수 있으므로 단말의 제조 단가를 낮출 수 있다.

향후 연구계획으로는 다양한 플랫폼을 고려한 툰 운용 방법, 콘텐츠와 함께 툰을 제공하는 방법, 단말에 저장되는 툰을 보호하기 위한 방법이 있다.

[참고문헌]

- [1] ISO/IEC 13818-1, MPEG-2 systems.
- [2] Information technology – Generic coding of moving pictures and associated audio information – Part 11: IPMP on MPEG-2 systems.
- [3] ISO/IEC 14496-1:2000/AMD.3-IPMPX.