(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년12월08일
(11) 등록번호 10-0999653
(24) 등록일자 2010년12월02일

(51) Int. Cl.
H04W 12/08 (2009.01) *H04B 1/40* (2006.01)
(21) 출원번호 10-2008-0105249
(22) 출원일자 2008년10월27일
심사청구일자 2008년10월27일
(65) 공개번호 10-2010-0051889
(43) 공개일자 2010년05월19일
(56) 선행기술조사문헌
KR1020070099493 A
KR1020080025973 A
KR1020060064469 A
전체 청구항 수 : 총 11 항

(73) 특허권자
주식회사 케이티
경기 성남시 분당구 정자동 206
(72) 발명자
박재민
서울특별시 강남구 일원동 718 샘터마을 108-1305
김민정
서울특별시 관악구 봉천6동 현대홈타운 APT 302-131
(74) 대리인
특허법인이지

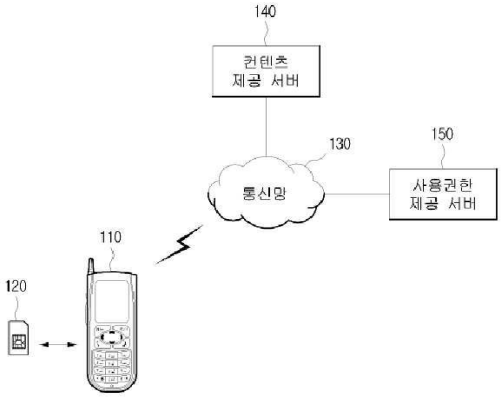
심사관 : 문성돈

(54) 스마트 카드를 포함하는 컨텐츠 재생 시스템 및 그 스마트 카드

(57) 요 약

본 발명의 일 측면에 따르면, 컨텐츠 재생 시스템이 개시된다. 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템은 스트리밍 방식으로 제공되는 컨텐츠의 N(자연수)번째 패킷에 적용된 DRM(Digital Right Management)을 해제하고, DRM이 해제된 N번째 원본 패킷을 컨텐츠 재생 단말로 전달하는 스마트 카드 및 스마트 카드로부터 N번째 원본 패킷을 전달받아 재생하고, 컨텐츠 제공 서버로 N+1번째 패킷을 요청하는 컨텐츠 재생 단말을 포함한다. 본 발명에 의하면, 기존의 스트리밍 서비스를 제공하는 서버와 제공받는 단말 간의 별도의 과정을 추가하지 않고도 DRM 기술을 적용하여, 더 두터운 컨텐츠 보호를 이룰 수 있으며, 스마트 카드 웹 서버 기능을 기반으로 하여 스트리밍 서비스에 DRM을 적용함으로써, OMA 표준에 정의되지 않는 영역을 보충하는 기술을 제시할 수 있는 장점이 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

스트리밍 방식으로 제공되는 컨텐츠를 재생하는 컨텐츠 재생 시스템에 있어서,

상기 컨텐츠의 제공 요청이 수신되면, 상기 제공 요청을 컨텐츠 재생 단말을 경유하여 컨텐츠 제공 서버로 전송하고,

상기 스트리밍 방식으로 제공되는 컨텐츠의 N(자연수)번째 패킷에 적용된 DRM(Digital Right Management)을 해제하고, 상기 DRM이 해제된 N번째 원본 패킷을 상기 컨텐츠 재생 단말로 전달하는 스마트 카드; 및

상기 스마트 카드로부터 상기 N번째 원본 패킷을 전달받아 재생하고, 상기 컨텐츠 제공 서버로 N+1번째 패킷을 요청하는 컨텐츠 재생 단말을 포함하는 컨텐츠 재생 시스템.

청구항 2

제1항에 있어서,

상기 컨텐츠 재생 단말은,

상기 스마트 카드로 상기 컨텐츠 제공 서버로의 접속을 요청하는 서비스 요청부;

상기 요청에 대응하여 상기 컨텐츠 제공 서버로부터 수신된 N번째 패킷에 DRM이 적용되었는지 판단하고, DRM이 적용된 경우에 상기 N번째 패킷을 상기 스마트 카드로 전달하는 판단부; 및

상기 N번째 원본 패킷을 상기 스마트 카드로부터 전달받는 경우, 상기 원본 패킷을 재생하는 재생부를 포함하는 것을 특징으로 하는 컨텐츠 재생 시스템.

청구항 3

제1항에 있어서,

상기 스마트 카드는,

상기 컨텐츠에 대응하는 사용권한을 다운로드 받아 보안 데이터 영역에 미리 저장하고, 상기 사용권한을 이용하여 상기 N번째 패킷에 적용된 DRM을 해제하는 것을 특징으로 하는 컨텐츠 재생 시스템.

청구항 4

제1항에 있어서,

상기 스마트 카드는,

USIM(UMTS Subscriber Identity Module), UIM(User Identity Module), R-UIM(Removable User Identity Module), SIM(Subscriber Identity Module) 및 UICC(Universal IC Card) 중 어느 하나인 것을 특징으로 하는 컨텐츠 재생 시스템.

청구항 5

컨텐츠 재생 단말에 장착되는 스마트 카드에 있어서,

상기 컨텐츠 재생 단말로부터 스트리밍 서비스를 제공하는 컨텐츠 제공 서버로의 접속 요청을 수신하고, 상기 접속 요청에 따라 상기 컨텐츠 재생 단말을 경유하여 상기 컨텐츠 제공 서버로 접속하는 스마트 카드 웹 서버 모듈; 및

상기 컨텐츠 재생 단말을 경유하여, 상기 컨텐츠 제공 서버로부터 스트리밍 방식으로 제공되는 컨텐츠의 N(자연수)번째 패킷에 적용된 DRM(Digital Right Management)을 해제하는 DRM 에이전트를 포함하되,

상기 DRM이 해제된 N번째 패킷은 상기 컨텐츠 재생 단말로 전달되어 재생되는 것을 특징으로 하는 스마트 카드.

청구항 6

제5항에 있어서,

상기 DRM 에이전트는,

상기 N번째 패킷으로부터 컨텐츠를 구별하는 식별정보를 추출하는 추출부;

상기 추출된 식별정보에 대응하는 사용권한을 선택하고, 선택된 사용권한으로부터 상기 DRM의 해제를 위한 복호키를 획득하는 키 관리부; 및

상기 복호키를 이용하여 상기 N번째 패킷에 적용된 DRM을 해제하고, 상기 스마트 카드 웹 서버 모듈을 통하여 상기 DRM이 해제된 N번째 원본 패킷을 상기 컨텐츠 재생 단말로 전달하는 복호화부를 포함하는 것을 특징으로 하는 스마트 카드.

청구항 7

제6항에 있어서,

상기 복호화부는,

상기 컨텐츠 재생 단말로부터 수신하는 N+1번째 패킷부터는 상기 N번째 패킷의 DRM 해제를 위한 획득된 복호화키를 이용하여 상기 N+1번째 패킷에 적용된 DRM을 해제하고, 상기 스마트 카드 웹 서버 모듈을 통하여 상기 DRM이 해제된 N+1번째 패킷을 상기 컨텐츠 재생 단말로 전달하는 것을 특징으로 하는 스마트 카드.

청구항 8

제7항에 있어서,

상기 복호화부는,

상기 획득된 복호화키에 미리 설정된 해쉬(hash) 함수를 적용하고, 상기 해쉬 함수가 적용된 복호화키로 상기 N+1번째 패킷에 적용된 DRM을 해제하는 것을 특징으로 하는 스마트 카드.

청구항 9

제7항에 있어서,

상기 복호화부는,

상기 획득된 복호화키와 상기 N+1번째 패킷과의 XOR 연산을 통하여 DRM을 해제하는 것을 특징으로 하는 스마트 카드.

청구항 10

제5항 또는 제6항에 있어서,

상기 스마트 카드 웹 서버 모듈은,

상기 DRM 에이전트에 의하여, 상기 컨텐츠에 대응하는 사용권한이 존재하지 않는 것을 판단되는 경우, 상기 컨텐츠 재생 단말을 경유하여, 사용권한 제공 서버에 접속하여 상기 사용권한을 다운로드 받는 것을 특징으로 하는 스마트 카드.

청구항 11

제5항 또는 제6항에 있어서,

상기 스마트 카드 웹 서버 모듈은,

상기 컨텐츠 재생 단말로부터 TCP/IP 또는 BIP에 의하여 상기 접속 요청을 수신하는 것을 특징으로 하는 스마트 카드.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 DRM이 적용된 컨텐츠를 스트리밍 방식으로 제공받아 재생하는 컨텐츠 재생 시스템에 관한 것으로, 상세하게는 컨텐츠 재생 단말에 장착된 스마트 카드에 저장된 사용권한을 이용하여 스트리밍 서비스 컨텐츠의 DRM을 해제하여 재생하는 컨텐츠 재생 시스템에 관한 것이다.

배 경 기 술

[0002] 인터넷 관련 기술의 발달로 인하여, 디지털로 제작된 컨텐츠의 유포가 활발해지고 있다. 그러나 이러한 디지털로 제작된 컨텐츠는 그 부당한 사용, 즉 불법 복사 및 유포를 제재하는데 어려움을 겪고 있다.

[0003] 이에 따라, 디지털 저작권 관리(Digital Rights Management, 이하, "DRM"이라 칭함) 기술이 이러한 문제점을 해결하기 위한 기술로 대두되었다.

[0004] 일반적으로 DRM은 디지털 컨텐츠에 대한 사용권한(Rights Object: RO)을 안전하게 보호하고 체계적으로 관리하기 위한 기술로서, 컨텐츠의 불법복제 방지 및 컨텐츠 사용권한의 획득, 컨텐츠의 생성 및 유통, 그리고 사용과정에 대한 일련의 보호 및 관리 체계를 제공한다.

[0005] DRM 기술은 접근 권한을 갖지 않은 사용자로부터 컨텐츠를 보호할 수 있다. 구체적으로, 컨텐츠 제공자는 특정 암호화 키를 사용해 보호된 컨텐츠를 제공하고, 사용자는 암호화된 컨텐츠를 복호하는데 필요한 사용권한을 발급받는다.

[0006] 한편으로는, 단말에 직접 컨텐츠를 저장하여 재생하는 형태로 제공하는 다운로드 방식이 아닌, 실시간 재생만 가능하고 재생 이후에 컨텐츠가 단말에 저장되지 않는 스트리밍 방식을 통하여 디지털 컨텐츠의 부당한 사용을 막는 방법도 대두되었다.

[0007] 그러나 종래에는 스트리밍 방식으로 컨텐츠를 제공하는 경우, 컨텐츠에 DRM을 적용하기 어려운 문제점이 있었다.

[0008] 한편, 스마트 카드는 3세대 이동 통신에서는 필수적인 구성으로 인식되고 있다. 다만, 통신 기술 및 집적 기술의 발달로 인하여 통신 단말에 장착되는 스마트 카드의 활용 가능성이 높아짐에도 불구하고, 그 활용 예는 기초적인 부분에 그치는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0009] 따라서 본 발명은 상술한 문제점을 해결하기 위하여 안출된 것으로서, DRM이 적용되어 스트리밍 방식으로 제공되는 컨텐츠를 제공받아 재생하는 컨텐츠 재생 시스템을 제공하는데 그 목적이 있다.

[0010] 또한, 본 발명의 또 다른 목적은 스마트 카드 웹 서버 기능을 수행하는 스마트 카드를 활용하여 스트리밍 서비스를 제공받고, 저장된 사용권한을 이용하여 스트리밍 서비스 컨텐츠에 적용된 DRM을 해제하여 컨텐츠를 재생하

는 컨텐츠 재생 시스템을 제공하는데 있다.

과제 해결수단

[0011] 본 발명의 일 측면에 따르면, 컨텐츠 재생 시스템이 개시된다.

[0012] 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템은 상기 스트리밍 방식으로 제공되는 컨텐츠의 N(자연수)번째 패킷에 적용된 DRM(Digital Right Management)을 해제하고, 상기 DRM이 해제된 N번째 원본 패킷을 컨텐츠 재생 단말로 전달하는 스마트 카드; 및 상기 스마트 카드로부터 상기 N번째 원본 패킷을 전달받아 재생하고, 상기 컨텐츠 제공 서버로 N+1번째 패킷을 요청하는 컨텐츠 재생 단말을 포함한다.

[0013] 본 발명의 다른 측면에 따르면, 스마트 카드가 개시된다.

[0014] 본 발명의 다른 실시예에 따른 스마트 카드는 상기 컨텐츠 재생 단말로부터 스트리밍 서비스를 제공하는 컨텐츠 제공 서버로의 접속 요청을 수신하고, 상기 접속 요청에 따라 상기 컨텐츠 재생 단말을 경유하여 상기 컨텐츠 제공 서버로 접속하는 스마트 카드 웹 서버 모듈; 및 상기 컨텐츠 재생 단말을 경유하여, 상기 컨텐츠 제공 서버로부터 스트리밍 방식으로 제공되는 컨텐츠의 N(자연수)번째 패킷에 적용된 DRM(Digital Right Management)을 해제하는 DRM 에이전트를 포함하되, 상기 DRM이 해제된 N번째 패킷은 상기 컨텐츠 재생 단말로 전달되어 재생되는 것을 특징으로 한다.

효 과

[0015] 따라서 본 발명은 기존의 스트리밍 서비스를 제공하는 서버와 제공받는 단말 간의 별도의 과정을 추가하지 않고도 DRM 기술을 적용하여 보다 나은 컨텐츠 보호의 효과가 있다.

[0016] 또한, 본 발명은 스마트 카드 웹 서버 기능을 기반으로 하여 스트리밍 서비스에 DRM을 적용함으로써, OMA 표준에 정의되지 않는 영역을 보충하는 기술을 제시하는 효과가 있다.

[0017] 또한, 본 발명은 스마트 카드에 사용권한을 저장하여, 스트리밍 서비스에서도 스마트 카드의 이동성을 활용할 수 있는 효과도 있다.

발명의 실시를 위한 구체적인 내용

[0018] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0019] 제2, 제1 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제2 구성요소는 제1 구성요소로 명명될 수 있고, 유사하게 제1 구성요소도 제2 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0020] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0021] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조

합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0022] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0023] 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다. 따라서, 본 명세서를 통해 설명되는 각 구성부들의 존재 여부는 기능적으로 해석 되어야 할 것이다.

[0024] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 대응하는 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0025] 도면에 대한 상세한 설명을 하기에 앞서, 본 발명의 컨텐츠 재생 단말과 스마트 카드(Smart Card)에 대하여 우선적으로 설명하기로 한다.

[0026] 컨텐츠 재생 단말은 PDA(Personal Digital Assistant), 셀룰러폰, PCS(Personal Communication Service)폰, WCDMA폰, CDMA-2000폰, MBS(Mobile Broad and System)폰, PC(Personal Computer), 핸드헬드 PC(Hand-Held PC) 및 노트북 PC(Notebook PC) 등과 같이 유무선 통신망(120)과 데이터를 송수신하는 통신 단말을 포함한다.

[0027] 이하, 컨텐츠 재생 단말은 스마트 카드를 장착하고, 통신망을 통하여 특정 서버와 패킷 통신을 수행하거나, 다른 통신 단말과 서킷 또는 패킷 통신을 수행하는 통신 단말로 구현되는 예를 대표적인 예로서 설명하기로 한다.

[0028] 스마트 카드는 WCDMA(Wideband Code Division Multiple Access) 기술에서 사용되는 USIM(UMTS Subscriber Identity Module), CDMA(Code Division Multiple Access) 기술에서 사용되는 UIM(User Identity Module) 또는 R-UIM(Removable User Identity Module), GSM(Global System for Mobile Communications) 기술에서 사용되는 SIM(Subscriber Identity Module) 및 3가지 모두의 기술을 포함하는 포괄적인 기술에서 사용되는 UICC(Universal IC Card)를 포함할 수 있는 명칭과 같이 다양한 명칭으로 사용될 수 있다.

[0029] 통신 단말은 스마트 카드를 이용하여 3세대 이동통신서비스를 제공받을 수 있다. 이는 통신 단말뿐만 아니라 노트북과 같은 휴대용 통신 단말에는 모두 적용될 수 있다.

[0030] 3세대에 접어든 이동통신 서비스뿐만이 아니라 Wibro(Wireless Broadband)로 대변될 수 있는 무선 휴대 인터넷 서비스의 경우에도 본 발명의 스마트 카드가 이용될 수 있다. 다만 이하에서는 스마트 카드가 통신 단말에 장착된 경우를 중심으로 설명하도록 한다.

[0031] 스마트 카드의 기능은 기본적으로 이동통신 서비스 또는 인터넷 서비스를 제공받는 경우, 가입자를 식별하고 인증하기 위한 가입자 정보(Subscriber's Information)을 저장하고, 통신 단말이 이를 독출하여 전송함으로써 통신망에서 가입자를 식별하고 인증할 수 있도록 한다. 따라서, 통신 서비스 가입자는 통신 단말에 의존적이지 않은 통신 서비스, 특히 이동통신 서비스를 제공받을 수 있다. 즉, 어떤 통신 단말이든 통신 서비스 가입자의 스마트 카드를 통신 단말에 연결시키면, 스마트 카드에 저장된 가입자 식별정보로 인하여 통신 서비스를 제공받을 수 있다

[0032] 그러나, 최근 집적회로 및 스마트 카드 제조기술의 발전으로 인하여 스마트 카드는 이러한 기본적인 기능 이외에도 연산처리 기능, 보조 연산처리 기능 및 대용량의 메모리가 추가되면서, 독립된 단말로서의 기능을 수행할 수 있는 수준에 이르고 있다.

[0033] 본 발명의 스마트 카드는 이러한 대용량의 메모리와 연산처리 기능을 가지는 프로세서가 탑재된 스마트 카드이다. 이러한 스마트 카드의 하드웨어적 기반을 바탕으로 스마트 카드 자체에서 다양한 어플리케이션을 실행하여

그 결과를 통신 단말로 전송함으로써 통신 단말에서 어플리케이션의 수행 결과를 오프라인으로 받아 볼 수 있게 된다.

[0034] 이 중에서도 스마트 카드의 어플리케이션의 수행 결과를 통신 단말에서 받아 볼 수 있는 수단적 개념으로 등장하는 것이 스마트 카드 웹 서버(SCWS: Smart Card Web Server)이다.

[0035] 스마트 카드는 OMA(Open Mobile Alliance) 표준에 정의된 바에 의하여 스마트 카드 웹 서버의 기능을 수행하며, 기본적으로 통신 단말의 브라우져(클라이언트)의 요청에 따라 웹 페이지 문서(Static or Dynamic HTML pages)를 통신 단말로 전달할 수 있다.

[0036] 이 경우 스마트 카드는 이동통신단말과 데이터를 교환하기 위한 환경이 필요하게 되는데 이는 BIP(Bearer Independence Protocol) 또는 USB 환경에 의한 TCP/IP 에 의하여 데이터 교환이 가능하다.

[0037] BIP는 통신 단말과 네트워크가 지원하는 패킷망(GPRS/UMTS packet bearer, Bluetooth, IrDA 등)을 이용하여 외부 노드와 통신 단말에 탑재된 스마트 카드 사이의 데이터 통신이 이루어지게 하는 프로토콜이다. BIP를 이용한 데이터 통신이 이루어 지기 위해서는 통신 단말, 스마트 카드 및 외부 노드는 모두 BIP를 지원해야 한다.

[0038] 그러나 본 발명의 스마트 카드는 OMA(Open Mobile Alliance) 표준에 정의된 바에 의하여 USB(Universal Serial Bus) 환경에서 TCP/IP 데이터 통신이 지원될 수 있으며, 이 경우 BIP에 비하여 향상된 속도로 데이터 통신을 수행할 수 있다.

[0039] 또한 스마트 카드는 외부 통신망의 원격관리 서버(Admin Server, 미도시)에 의하여 제어될 수도 있는데, 원격관리 서버는 HTTP 서버로서 스마트 카드에 포함되는 SCWS 모듈로 관리 명령(Admin Command)을 전송함으로써 SCWS 모듈을 관리할 수 있다. 예를 들어 SCWS의 설정 파라미터 설정 및 변경(Setting or changing configuration parameter of SCWS) 이나 HTML 페이지의 인스톨 또는 삭제 등을 수행할 수 있다.

[0040] 도 1은 본 발명의 일 실시예에 따른 스트리밍 서비스를 위한 시스템도이다.

[0041] 도 1을 참조하면, 스트리밍 서비스를 위한 시스템은 스마트 카드(120)가 장착된 컨텐츠 재생 단말(110), 통신망(130), 컨텐츠 제공 서버(140) 및 사용권한 제공 서버(140)를 포함할 수 있다.

[0042] 본 발명은 DRM(Digital Rights Management)이 적용된 스트리밍 서비스에 대한 것으로, 이하에서 스트리밍 서비스를 위한 시스템의 각 구성 요소의 동작을 중심으로 구체적으로 설명하기로 한다.

[0043] 컨텐츠 재생 단말(110)은 상술한 바와 같이, 통신망(130)을 통하여 패킷 서비스를 제공받을 수 있는 통신 단말이다. 본 발명의 컨텐츠 재생 단말(110)은 컨텐츠를 제공하는 서버에 접속하여, 스트리밍(streaming) 방식으로 컨텐츠를 제공받는다. 그리고 컨텐츠 재생 단말(110)은 해당 컨텐츠를, 즉 컨텐츠를 구성하는 패킷을 재생한다.

[0044] 상세하게는, 스트리밍 서비스의 컨텐츠에 DRM이 적용된 경우, 컨텐츠 재생 단말(110)은 해당 컨텐츠를 구성하는 패킷(DRM이 적용됨)을 스마트 카드(120)로 전달한다. 그리고 스마트 카드(120)는 전달된 패킷의 DRM을 해제하고, DRM이 해제된 패킷(이하, 원본 패킷이라 칭함)을 다시 컨텐츠 재생 단말(110)로 전달한다. 컨텐츠 재생 단말(110)은 전달된 원본 패킷을 재생하고, 다음 패킷의 전송을 요청한다.

[0045] 여기서, 스트리밍 방식으로 컨텐츠를 제공하는 것(즉, 스트리밍 서비스)는 컨텐츠를 제공받는 기기에 직접 데이터를 저장한 후 디코딩하여 재생하는 다운로드 방식과 달리, 컨텐츠를 제공받는 기기가 통신망(130)을 통하여 데이터 전송 받음과 동시에, 즉 실시간으로 컨텐츠의 재생이 가능한 전송 방식에 따른 서비스를 의미한다.

[0046] 실시간 전송 프로토콜/실시간 스트리밍 프로토콜(RTP/RSTP, 이하 RTP/RSTP로 표기)은 스트리밍 서비스의 표준 프로토콜이다. RSTP(Real Time Streaming Protocol)는 TCP/IP(Transport Control Protocol/Internet Protocol)를 통해 스트림 컨트롤에 대한 명령을 주고받는 역할을 하는 프로토콜이고, RTP(Real Time Protocol)는 UDP(User Datagram Protocol)를 통해 재생 오디오/비디오 데이터를 받는 프로토콜이다.

[0047] RSTP, RTP 모두 TCP, UDP 프로토콜 위에서 사용될 수 있지만, 대개의 경우 RTSP는 TCP 기반에서 이루어지고, RTP는 UDP 기반에서 이루어진다. 왜냐하면 TCP는 서버(server)와 클라이언트(client) 간의 전송을 보장하는 프로토콜이나 속도가 느리고, UDP는 전송을 보장하지 않는 대신 속도가 빠르기 때문이다.

[0048] 스트리밍 서비스의 구체적인 절차는 공지된 기술로서, 상세한 설명은 생략하기로 한다.

[0049] 통신망(130)은 CDMA나 WCDMA 뿐만 아니라, 통신 디바이스(110)로 컨텐츠 또는 어플리케이션을 제공할 수 있는

모든 유무선 통신망(130)을 포함한다.

[0050] 이하에서는WCDMA를 예로서 설명한다. WCDMA 망은 무선 기지국(Node B), 무선 제어국(RNC: Radio Network Controller), SGSN(Serving GPRS Support Node) 및 GGSN(Gateway GPRS Support Node)를 포함할 수 있다. WCDMA 망은 공지된 기술이므로, 본 발명의 요지를 명확하게 하기 위하여 상세한 설명은 생략한다.

[0051] 컨텐츠 제공 서버(140)는 통신망(130)을 통하여 컨텐츠 재생 단말(110)로 컨텐츠를 제공한다. 상세하게는, 컨텐츠 제공 서버(140)는 스트리밍 방식으로 컨텐츠를 제공하며, 해당 컨텐츠를 구성하는 패킷에 DRM을 적용하여 제공한다.

[0052] 사용권한 제공 서버(RI: Rights Issuer, 140)는 특정 컨텐츠에 대한 사용권한(Right Object)를 발급한다. 즉, 사용권한 제공 서버(140)는 컨텐츠 재생 단말(110)을 경유하여 스마트 카드(120)로 복호키(CEK: Content Encryption Key)를 획득할 수 있는 사용권한을 제공한다. 여기서, 복호키는 해당 컨텐츠에 적용된 DRM을 해제하기 위한, 즉 암호화된 컨텐츠를 복호할 수 있는 키이다.

[0053] 컨텐츠 제공 서버(140)와 사용권한 제공 서버(140)는 동일한 장치로 구현될 수 있다. 컨텐츠 제공 서버(140)와 사용권한 제공 서버(140)가 동일한 장치로 구현되는 경우, 서로 데이터베이스를 공유할 수 있으며, 미리 사용권한을 발급하고, 스트리밍 서비스 제공할 수 있다.

[0054] 지금까지, 도 1을 참조하여 본 발명의 일 실시예에 따른 스트리밍 서비스를 위한 시스템을 설명하였다. 이하, 도 2를 참조하여 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템에 대해서 상세히 설명하기로 한다.

[0055] 도 2는 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템의 구성도이다.

[0056] 도 2를 참조하면, 컨텐츠 재생 시스템은 스마트 카드(120)와 컨텐츠 재생 단말(110)을 포함한다.

[0057] 컨텐츠 재생 단말(110)은 DRM이 적용된 컨텐츠를 스트리밍 방식으로 제공받는다. 그리고 스마트 카드(120)에 의하여 DRM이 해제되면, 해당 컨텐츠를 재생한다.

[0058] 이하, 컨텐츠 재생 단말(110)의 구체적인 동작을 기능부로 구분하여 자세히 설명하도록 한다.

[0059] 통신부(240)는 통신망(130)을 통하여 컨텐츠 제공 서버(140)(또는 사용권한 제공 서버(140))와 스트리밍 서비스를 제공받기 위한 모든 데이터 및 신호를 송수신한다.

[0060] 입출력부(250)는 컨텐츠 재생 단말(110)의 제어를 위한 키패드, 터치 스크린, 마이크 등의 입력 장치와 음성 통화 서비스나 데이터 서비스 이용시 필요한 데이터를 사용자에게 제공하기 위한 스피커, LCD 창과 같은 출력 장치를 포함한다.

[0061] 단말 브라우저(260)는 서비스 요청부(262), 판단부(264) 및 재생부(266)를 포함한다.

[0062] 서비스 요청부(262)는 스마트 카드 웹 서버의 기능을 수행하는 스마트 카드(120)로 웹 페이지 문서의 제공을 요청한다. 여기서, 서비스 요청부(262)는 OMA 표준에 따라 USB 환경에서 TCP/IP 또는 BIP에 의하여 접속 요청을 전달한다.

[0063] 또한, 서비스 요청부(262)는 사용자에 의하여 입력된 제어 정보에 따라 스트리밍 서비스 대상 컨텐츠의 선택, 스트리밍 서비스의 개시, 재생된 패킷 이후의 다음 패킷 요청 등의 요청을 스마트 카드(120)로 전달한다. 이러한 요청은 스마트 카드(120)에 의하여 컨텐츠 재생 단말(110)을 경유하여 컨텐츠 제공 서버(140)로 전달된다.

[0064] 판단부(264)는 스트리밍 서비스에 따라 수신된 패킷에 DRM이 적용되었는지 여부를 판단한다. 그리고 판단부(264)는 해당 패킷을 DRM이 적용되지 않은 경우에는 재생부(266)로, DRM이 적용된 경우에는 스마트 카드(120)로 전달한다.

[0065] 재생부(266)는 스트리밍 서비스의 컨텐츠를 재생한다. 구체적으로, 재생부(266)는 DRM이 적용되지 않았거나, 스마트 카드(120)에 의하여 DRM이 해제된 패킷을 전달받아 재생한다.

[0066] 저장부(270)는 컨텐츠 재생 단말(110)의 전반적인 동작을 제어하는 소정의 프로그램 및 입출력되는 데이터 및 처리되는 각종 데이터를 저장한다. 또한, 저장부(270)는 스트리밍 서비스를 위하여, 수신된 패킷을 일시적으로 저장하는 버퍼(미도시)를 포함하여 구현될 수 있다.

[0067] 스마트 카드(120)는 컨텐츠 재생 단말(110)로부터 컨텐츠 제공 서버(140)로의 접속 요청이 있는 경우, 컨텐츠

재생 단말(110)을 경유하여 컨텐츠 제공 서버(140)로 접속한다. 그 후, 컨텐츠 제공 서버(140)로부터 수신된 웹 페이지 문서는 컨텐츠 재생 단말(110)의 표시 영역에 표시된다.

[0068] 또한, 스마트 카드(120)는 컨텐츠 제공 서버(140)로부터 스트리밍 서비스의 패킷에 적용된 DRM을 해제한다. 해제된 패킷은 컨텐츠 재생 단말(110)로 전달되어 재생된다.

[0069] 스마트 카드(120)는 내부에 CPU(Central Processing Unit), 비휘발성 메모리 및 활성메모리 영역(230)을 포함한다. 스마트 카드(120)는 메모리에 정보를 저장하고 그 정보를 가공하거나 정보를 이용하여 어떤 연산을 할 수 있는 능력이 있다.

[0070] 다만, 본 명세서는 설명과 이해의 편의를 위하여, 스마트 카드(120)의 구체적인 동작에 대해, 도 2를 참조하여 스마트 카드(120)의 기능에 기초한 기능부로 구분하여 설명하기로 한다.

[0071] 스마트 카드(120)는 스마트 카드 웹 서버 모듈, DRM 에이전트(220), 메모리 영역(230)을 포함할 수 있다.

[0072] 스마트 카드 웹 서버 모듈(이하, SCWS 모듈이라 칭함, 210)은 상술한 스마트 카드 웹 서버의 기능을 수행한다. 스마트 카드 웹 서버는 상술한 바와 같이, 컨텐츠 재생 단말(110)의 브라우져의 요청에 따라 웹 페이지 문서를 컨텐츠 재생 단말(110)로 전달하는 기능이다.

[0073] 구체적으로, SCWS 모듈(210)은 컨텐츠 재생 단말(110)로부터 컨텐츠 제공 서버(140)로의 접속 요청을 수신한다. 그리고 SCWS 모듈(210)은 해당 접속 요청에 응하여 컨텐츠 재생 단말(110)을 경유하여 컨텐츠 제공 서버(140)에 접속한다. 여기서, SCWS 모듈(210)은 컨텐츠 재생 단말(110)로부터 OMA 표준에 따라 USB 환경에서 TCP/IP 또는 BIP에 의하여 접속 요청을 수신할 수 있다.

[0074] SCWS 모듈(210)은 컨텐츠 재생 단말(110)과의 관계에서, 서버로서 웹 페이지 문서의 전송을 요청받고, 요청된 웹 페이지 문서를 컨텐츠 재생 단말(110)로 제공한다. 이와 같이, SCWS 모듈(210)과 컨텐츠 재생 단말(110)은 서버-클라이언트 관계와 유사하게 동작한다.

[0075] 본 발명의 SCWS 모듈(210)은 컨텐츠 재생 단말(110)을 경유하여 컨텐츠 제공 서버(140)에 접속하여 스트리밍 서비스의 제공을 요청한다.

[0076] 또한, SCWS 모듈(210)은 컨텐츠 재생 단말(110)을 경유하여 사용권한 제공 서버(140)에 접속할 수 있다. 스트리밍 방식으로 제공되는 컨텐츠의 사용권한이 존재하지 않는 경우에, 해당 컨텐츠의 사용권한을 발급받기 위함이다.

[0077] DRM 에이전트(220)는 스트리밍 방식으로 제공되는 컨텐츠에 DRM이 적용된 경우, 해당 DRM을 해제한다.

[0078] 이하, DRM 에이전트(220)의 동작은 기능부로 나누어 구체적으로 설명하기로 한다. DRM 에이전트(220)는 추출부(222), 키 관리부(224) 및 복호화부(226)를 포함할 수 있다.

[0079] 추출부(222)는 컨텐츠 재생 단말(110)이 스트리밍 서비스를 제공받는 경우, 해당 컨텐츠를 구성하는 패킷을 전달받는다. 추출부(222)는 전달된 패킷으로부터 컨텐츠의 식별정보를 추출한다.

[0080] 키 관리부(224)는 추출부(222)에 의하여 추출된 식별정보에 대응하는 사용권한을 선택한다. 그리고 키 관리부(224)는 선택한 사용권한으로부터 복호키를 획득한다.

[0081] 복호화부(226)는 키 관리부(224)에 의하여 획득된 복호키를 이용하여 컨텐츠 재생 단말(110)로부터 전달된 패킷을 복호한다. 즉, 복호화부(226)는 패킷에 적용된 DRM을 복호키를 이용하여 해제한다. 여기서, 복호화된 패킷을 원본 패킷이라 칭하기로 한다.

[0082] 또한, 복호화부(226)는 원본 패킷을 컨텐츠 재생 단말(110)로 전달한다. 이때, 원본 패킷은 SCWS 모듈(210)을 통하여 컨텐츠 재생 단말(110)로 전달될 수 있다.

[0083] 또한, 복호화부(226)는 스트리밍 서비스에 의하여 동일한 DRM이 적용된 패킷이 연속적으로 전달되는 경우, 기획득된 복호키를 이용하여 패킷의 복호를 수행한다. 즉, 상술한 추출부(222) 및 키 관리부(224)의 식별정보를 추출, 사용권한을 선택, 복호키를 획득하는 기능은 동일한 DRM이 적용된 패킷들에 대해서는 한번만 수행될 수도 있다.

[0084] 구체적으로, DRM 에이전트(220)는 스트리밍 서비스의 첫번째 패킷을 수신하는 경우, 상술한 식별정보 추출, 사용권한 선택, 복호키 획득을 수행하고, 획득된 복호키로 첫번째 패킷의 DRM을 해제한다. 여기서, 복호화부(226)는 AES(Advanced Encryption Stadard) 알고리즘을 이용하여 첫번째 패킷의 DRM을 해제한다. 여기서, AES 알

고리즘은 본 발명이 속하는 기술분야의 통상의 지식을 가진 자에게 공지의 기술로서 본 발명의 이해의 편의를 위하여 자세한 설명은 생략하기로 한다.

[0085] 본 발명의 일 실시예에 따르면, 복호화부(226)는 이후 연속적으로 수신되는 2번째, 3번째 패킷들에 대하여 기 획득된 복호키로 동일한 AES 알고리즘을 이용하여 DRM을 해제한다.

[0086] 본 발명의 다른 실시예에 따르면, 복호화부(226)는 2번째 패킷부터는 AES 알고리즘을 이용하지 않고, 2번째 패킷과, 특히 DRM이 적용된 데이터 영역과 XOR 연산을 수행한다. 물론, 본 실시예에서의 컨텐츠 제공 서버는 2번째 패킷부터는 복호키와의 XOR 연산만으로 원본 패킷이 생성될 수 있도록 패킷을 암호화하여야 한다. 본 실시예에 따르면, 스트리밍 서비스의 보안성은 다소 약해질 수 있으나, 스트리밍 서비스 자체의 실시간성을 높을 수 있는 효과가 있다.

[0087] 본 발명의 또 다른 실시예에 따르면, 복호화부(226)는 2번째 패킷은 기 획득된 복호키(CEK_1)에 미리 설정된 해쉬(hash) 함수를 적용하여 도출된 복호키(CEK_2)를 이용하여 2번째 패킷을 복호한다. 그리고 복호화부(226)는 3번째 패킷은 2번째 패킷의 복호를 위한 키, 즉 CEK_2에 다시 해쉬 함수를 적용하여 도출된 복호키(CEK_3)을 이용하여 3번째 패킷을 복호한다. 즉, 본 실시예에 따르면, 복호화부(226)는 N+1번째 패킷을 복호하기 위한 복호키(CEK_{N+1})를 하기의 수학식을 통하여 도출한다.

[0088] [수학식]

[0089] $(CEK_{N+1}) = hash(CEK_N)$

[0090] 여기서, CEK_N는 N번째 패킷을 복호하기 위한 복호키를 의미하고, hash()은 미리 설정된 해쉬 함수를 적용하는 것을 의미한다.

[0091] 본 실시예는 상술한 XOR 연산을 이용하는 실시예보다 보안성을 좀 더 강화하고, 모든 패킷에 대하여 AES 알고리즘을 수행하는 실시예보다는 실시간성을 강화하는 효과가 있다.

[0092] 본 발명의 메모리 영역(230)에는 컨텐츠의 재생을 위한 사용권한이 저장되어 있다. 저장된 사용권한은 요청에 의하여 DRM 에이전트(220)로 제공된다.

[0093] 메모리 영역(230)은 유저 데이터 영역과 보안 데이터 영역으로 구분될 수 있다. 유저 데이터 영역은 가입자 정보(예를 들어, IMSI(International Mobile Station Identity))를 저장한다. 상술한 사용권한은 외부로부터 허락되지 않은 접근(Reading/Writing)은 불가능한 메모리 영역(230)인 보안 데이터 영역에 저장될 수 있다.

[0094] 메모리 영역(230)에는 스마트 카드(120)의 전반적인 동작을 제어하는 소정의 프로그램 및 입출력되는 데이터 및 처리되는 각종 데이터를 저장할 수 있다.

[0095] 지금까지, 도 2를 참조하여 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템을 설명하였다. 이하, 도 3을 참조하여 본 발명의 일 실시예에 따른 컨텐츠 재생 방법에 대해서 상세히 설명하기로 한다.

[0096] 도 3 및 도 4는 본 발명의 실시예에 따른 컨텐츠 재생 방법에 대한 호 처리도이다.

[0097] 본 발명은 스마트 카드 웹 서버(SCWS)를 기반으로 하여, DRM이 적용된 스트리밍 서비스에 관한 것이다.

[0098] 도 3은 본 발명의 제1 실시예로서, 스마트 카드(120)가 미리 사용권한을 저장하고 있는 경우이며, 도 4는 본 발명의 제2 실시예로서, 스마트 카드(120)가 스트리밍 서비스를 위하여 사용권한을 다운로드 받아야 하는 경우이다.

[0099] 이하, 도 3을 참조하여, 본 발명의 제1 실시예에 대하여 설명하도록 한다.

[0100] 단계 S302에서, 컨텐츠 재생 단말(110)은 컨텐츠 제공 서버(140)로 스트리밍 서비스를 요청한다. 상세하게는, 컨텐츠 재생 단말(110)은 스마트 카드(120)의 SCWS 모듈(210)로 웹 페이지 문서의 제공을 요청하면, SCWS 모듈(210)은 컨텐츠 재생 단말(110)을 경유하여 컨텐츠 제공 서버(140)로 접속한다.

[0101] 그 후, SCWS 모듈(210)은 컨텐츠 재생 단말(110)로부터 전달된 요청에 따라, 컨텐츠 제공 서버(140)로 특정 컨텐츠의 스트리밍 서비스를 요청한다.

[0102] 이어서, 단계 S304 및 단계 S306에서, 컨텐츠 제공 서버(140)는 해당 컨텐츠의 패킷에 DRM을 적용한다(S304). 그리고 DRM이 적용된 패킷을 컨텐츠 재생 단말(110)로 전송한다(S306).

[0103] 여기서, 컨텐츠 제공 서버(140)는 컨텐츠를 구성하는 모든 패킷에 DRM을 적용할 수도 있고, 스트리밍 서비스에 따라 전송될 패킷에만 우선적으로 DRM을 적용하여 전송할 수도 있다.

[0104] 이하, 컨텐츠 제공 서버(140)가 스트리밍 서비스에 따라 N번째 패킷을 전송하는 경우를 구체적으로 설명한다.

[0105] 이어서, 단계 S308에서, 컨텐츠 재생 단말(110)은 단계 S306에서 수신된 N번째 패킷에 DRM이 적용되었는지 여부를 판단한다.

[0106] 판단 결과 DRM이 적용되지 않은 경우, 컨텐츠 재생 단말(110)은 단계 S320 및 단계 S322를 수행한다. 즉, 컨텐츠 재생 단말(110)은 단말 브라우저(260)를 통하여 N번째 패킷을 재생하고, N+1번째 패킷의 전송을 컨텐츠 제공 서버(140)로 요청한다.

[0107] 한편, 단계 S308에서 판단 결과, N번째 패킷에 DRM이 적용되어 있는 경우, 컨텐츠 재생 단말(110)은 N번째 패킷을 SCWS 모듈(210)(스마트 카드(120) 내에 포함)을 통하여 DRM 에이전트(220)(스마트 카드(120) 내에 포함)로 전달한다.

[0108] 이어서, 단계 S310에서, DRM 에이전트(220)는 N번째 패킷에서 식별정보를 추출한다. 여기서, 식별정보는 컨텐츠를 구별할 수 있는 컨텐츠 ID일 수 있다.

[0109] 이어서, 단계 S312에서, DRM 에이전트(220)는 추출된 식별정보에 대응하는 사용권한이 존재하는지 여부를 판단한다.

[0110] 본 실시예는 미리 사용권한을 발급받은 경우로 가정한 바, DRM 에이전트(220)는 사용권한이 있는 것으로 판단할 것이다. 한편, DRM 에이전트(220)가 사용권한이 없는 것으로 판단하는 경우는 본 발명의 제2 실시예이므로, 도 4의 설명에서 자세히 설명하도록 한다.

[0111] 이어서, 단계 S314에서, DRM 에이전트(220)는 저장된 사용권한을 추출하여, 사용권한으로부터 복호키(CEK: Content Encryption Key)를 획득한다. 복호키는 해당 컨텐츠에 적용된 DRM을 해제할 수 있는 키이다.

[0112] 이어서, 단계 S316에서, DRM 에이전트(220)는 복호키를 이용하여 전달된 N번째 패킷에 적용된 DRM을 복호한다.

[0113] DRM 에이전트(220)는N번째 패킷을 복호하여, N번째 패킷에 적용된 DRM이 해제된 N번째 원본 패킷을 생성한다.

[0114] 여기서, DRM이 적용된 패킷을 복호키로 복호하는 방법은 이미 당해 기술분야의 통상의 지식을 가진 자들에게 널리 알려진 기술(대칭키 암호화, 비대칭키 암호화, AES 알고리즘 등)이므로, 자세한 설명은 생략하기로 한다.

[0115] 이어서, 단계 S318 및 단계 S320에서, DRM 에이전트(220)는 생성된 N번째 원본 패킷을 SCWC 모듈을 통하여 컨텐츠 재생 단말(110)로 전달한다(S318). 그리고 컨텐츠 재생 단말(110)은 전달된 N번째 원본 패킷을 재생한다(S320).

[0116] 이로써, 컨텐츠 재생 단말(110)은 스트리밍 방식으로 제공된 DRM 적용 패킷을 재생할 수 있다.

[0117] 이후, 단계 S322에서, 컨텐츠 재생 단말(110)은 스마트 카드 웹 서버 기능을 이용하여 컨텐츠 제공 서버(140)로 N+1번째 패킷을 요청한다.

[0118] N+1번째 패킷에 대해서는 단계 S306 내지 단계 S320이 반복적으로 수행될 수 있다. 그리고 이와 같은 과정으 해당 컨텐츠를 구성하는 모든 패킷에 대하여 수행되면, 종국적으로 컨텐츠 재생 단말(110)은 DRM이 적용된 컨텐츠를 스트리밍 방식으로 제공받아 재생할 수 있다.

[0119] 또한, N+1번째 패킷에 대해서는 단계 S308의 일부(DRM 적용 여부 판단), 단계 S310 내지 단계 S314가 생략될 수도 있다. 본 발명은 스트리밍 서비스에 DRM 기술을 적용한 것으로 스트리밍 서비스의 실시간성과 DRM 기술의 보안성의 요구를 적절히 조화시킬 필요가 있다. 즉, 본 발명에서 보안성을 강화하면 실시간성이 약해지고, 실시간성을 강화하면 보안이 취약해질 우려가 있기 때문이다.

[0120] 이후, N번째 패킷을 해당 스트리밍 서비스의 1번째 패킷으로 가정하고 설명하기로 한다.

[0121] 1번째 패킷 이후에 연속적으로 수신한 패킷들에 대한 복호 방법으로, 그 첫번째는 보안성을 극대화하는 방법이다. 첫번째 방법에 의하면 스마트 카드(120)의 연산 능력이 일정치 이상인 경우에만 실시간성을 보장 받을 수

있다.

[0122] 첫번째 방법은 2번째 패킷을 수신한 경우에도 동일한 방법으로 DRM을 해제하는 방법이다. 즉, 2번째, 3번째 패킷에 대해서도 상술한 AES 알고리즘을 이용하여 DRM을 해제한다.

[0123] 두번째 방법은 보안성보다는 실시간성을 우선하는 방법이다. DRM 에이전트(220)는 1번째 패킷에 대응하여 이미 획득한 복호키와 2번째 패킷(특히, 데이터 영역)의 XOR 연산을 수행하여 2번째 패킷을 복호한다. 그리고 DRM 에이전트(220)는 3번째 패킷도 기 획득된 복호키와 XOR 연산을 수행하여 복호한다.

[0124] XOR 연산은 굉장히 간단한 연산이므로, 첫번째 방법에 비하여 보안성이 약해지기는 하나, 이로써 실시간성이 강화된다.

[0125] 세번째 방법은 XOR 연산을 이용하는 두번째 방법보다 보안성을 강화하는 방법으로, DRM 에이전트(220)는 2번째 패킷을 복호하기 위한 키(CEK_2)를 1번째 패킷을 복호하기 위하여 기 획득된 복호키(CEK_1)에 해쉬 함수를 적용하여 도출한다. 그리고 DRM 에이전트(220)는 도출된 CEK_2로 2번째 패킷의 DRM을 해제한다. 이어서, DRM 에이전트(220)는 3번째 패킷에 대응하는 복호키(CEK_3)를 CEK_2에 해쉬 함수를 적용하여 도출하고, 도출된 CEK_3으로 3번째 패킷을 복호한다.

[0126] 따라서 세번째 방법은 상술한 첫번째 방법에 비하여 실시간성을 강화할 수 있으며, 두번째 방법보다 보안성을 강화한 효과가 있다.

[0127] 이하, 도 4을 참조하여, 본 발명의 제2 실시예에 대하여 설명하도록 한다.

[0128] 본 발명의 제2 실시예는 컨텐츠 재생 단말(110)에 장착된 스마트 카드(120)에 사용권한이 미리 저장되지 않은 경우이다. 따라서 스마트 카드(120)는 수신된 패킷의 복호가 요청되면, 해당 컨텐츠의 사용권한을 다운로드 받을 필요가 있다. 즉, 제2 실시예는 상술한 제1 실시예의 단계 S312에서 DRM 에이전트(220)가 사용권한이 존재하지 않는 것으로 판단한 경우이다.

[0129] DRM 에이전트(220)는 단계 S312에서 사용권한이 존재하지 않는 것으로 판단되면, 단계 S410 내지 단계 S430을 수행한다.

[0130] 단계 S410에서, DRM 에이전트(220)는 SCWS 모듈(210)로 사용권한 요청을 전달한다. SCWS 모듈(210)은 스마트 카드 웹 서버 기능을 수행하여, 컨텐츠 재생 단말(110)을 경유하여 사용권한 제공 서버(140)로 사용권한 요청을 전송한다.

[0131] 즉, SCWS 모듈(210)은 DRM 에이전트(220)로부터 전달된 사용권한 요청을 OMA 표준에 따라 사용권한 제공 서버(140)로 전달한다. 물론, 사용권한 요청은 OMA 표준에 의하여 단순히 컨텐츠 재생 단말(110)을 경유할 뿐, 컨텐츠 재생 단말(110)의 제어에 의하여 전달되는 것은 아니다.

[0132] 한편, 사용권한 요청은 컨텐츠 식별정보 및 IMSI를 포함할 수 있다. 즉, 사용권한 요청은 컨텐츠의 정당한 사용을 인증하기 위해 필요한 정보로서, 컨텐츠를 구분할 수 있는 식별정보와 컨텐츠 사용을 요청하는 사용자를 인증할 수 있는 IMSI를 포함할 수 있다.

[0133] 이어서, 단계 S420 및 단계 S430에서, 사용권한 제공 서버(140)는 수신된 사용권한 요청에 대응하여 사용권한을 생성(혹은 저장된 사용권한 선택)한다(S420). 그리고 DRM 에이전트(220)는 사용권한 제공 서버(140)로부터 생성된 사용권한을 다운로드한다(S430). 즉, 사용권한 제공 서버(140)는 생성된 사용권한을 컨텐츠 재생 단말(110) 및 SCWS 모듈(210)을 경유하여 DRM 에이전트(220)로 전송한다. 이때, 사용권한 제공 서버(140)도 OMA 표준에 의하여 사용권한을 DRM 에이전트(220)로 전송할 수 있다.

[0134] 이후의 제2 실시예의 과정은 도 3의 설명에서 서술한 단계 S314 내지 단계 S322과 동일하다. 따라서 이후의 과정에 대해서는 생략하기로 한다.

[0135] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

[0136] 예를 들어, 컴퓨터가 읽을 수 있는 기록매체는 ROM, RAM, CD-ROM, 자기 테이프, 플라피디스크, 광데이터 저장장치 등을 포함할 수 있다.

[0137] 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함할 수 있다.

[0138] 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0139] 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0140] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0141] 도 1은 본 발명의 일 실시예에 따른 스트리밍 서비스를 위한 시스템도.

[0142] 도 2는 본 발명의 일 실시예에 따른 컨텐츠 재생 시스템의 구성도.

[0143] 도 3은 본 발명의 제1 실시예에 따른 컨텐츠 재생 방법에 대한 호 처리도.

[0144] 도 4는 본 발명의 제2 실시예에 따른 컨텐츠 재생 방법에 대한 호 처리도.

[0145] <도면의 주요부분에 대한 부호의 설명>

[0146] 110: 컨텐츠 재생 단말 120: 스마트 카드

[0147] 130: 통신망 140: 컨텐츠 제공 서버

[0148] 150: 사용권한 제공 서버 210: SCWS 모듈

[0149] 220: DRM 에이전트 222: 추출부

[0150] 224: 키 관리부 226: 복호화부

[0151] 230: 메모리 영역 240: 통신부

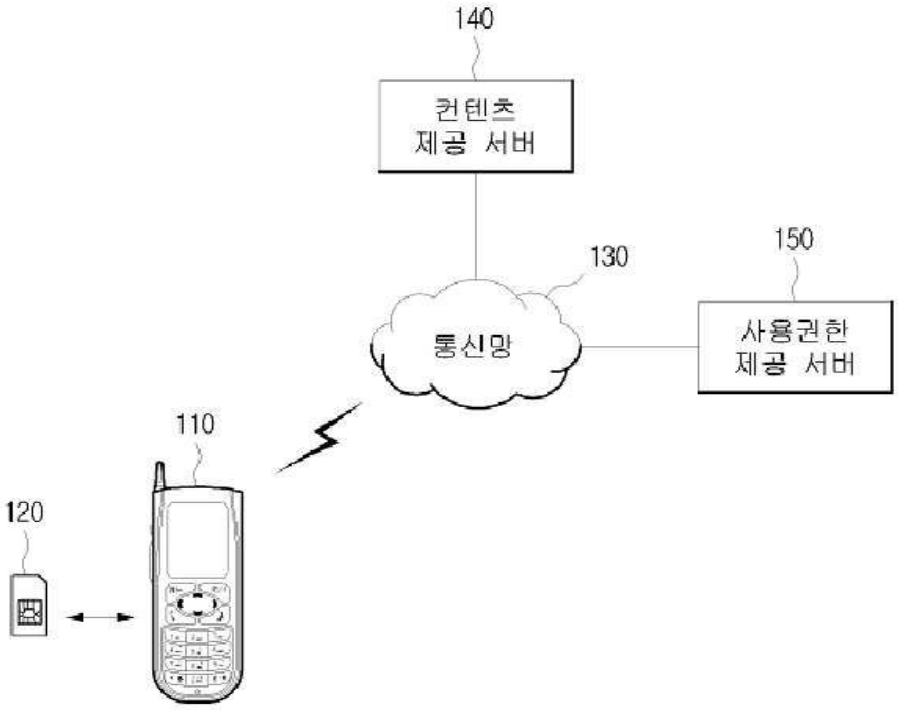
[0152] 250: 입출력부 260: 단말 브라우저

[0153] 262: 서비스 요청부 264: 판단부

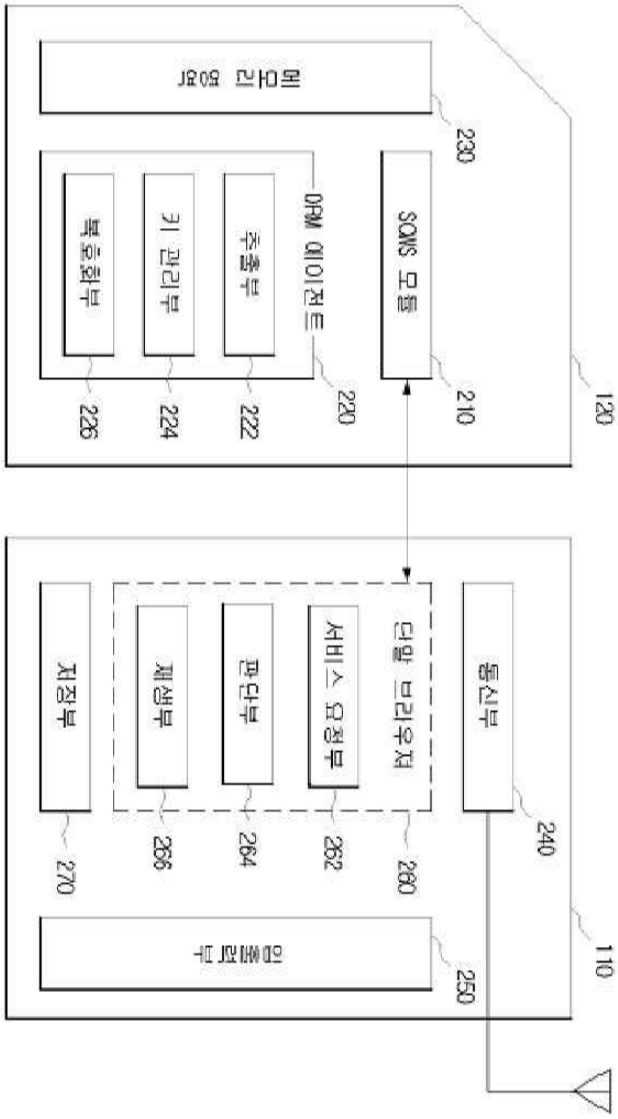
[0154] 266: 재생부 270: 저장부

도면

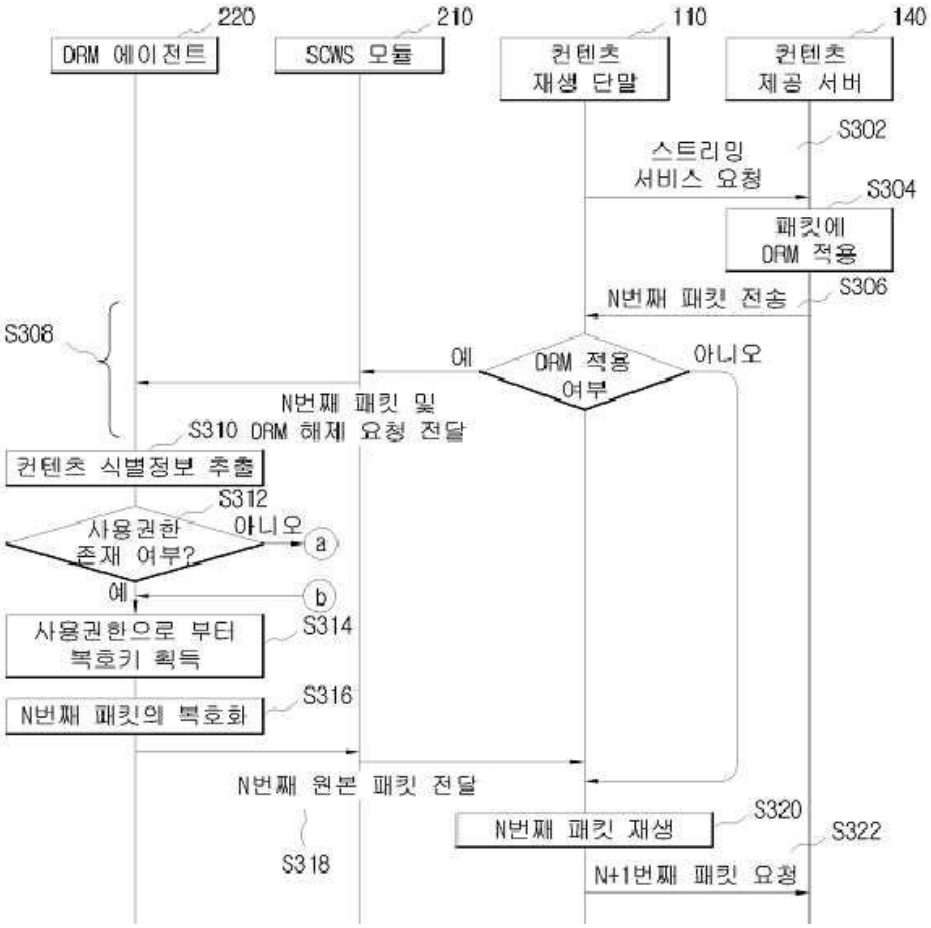
도면1



도면2


메모리 장치
230
SCWS 모듈
210
120
OFM 에이전트
220
추출부
222
키 관리부
224
복호화부
226
단말 브라우저
260
서비스 요청부
262
판단부
264
제생부
266
통신부
240
110
저장부
270
입출력 장치
250

도면3


220
DRM 에이전트
210
SCWS 모듈
110
컨텐츠 재생 단말
140
컨텐츠 제공 서버
S302
스트리밍 서비스 요청
S304
패킷에 DRM 적용
S306
N번째 패킷 전송
S308
예
DRM 적용 여부
아니오
N번째 패킷 및 S310 DRM 해제 요청 전달
컨텐츠 식별정보 추출
S312
사용권한 존재 여부?
아니오
a
예
b
사용권한으로 부터 복호키 획득
S314
N번째 패킷의 복호화
S316
N번째 원본 패킷 전달
S318
N번째 패킷 재생
S320
S322
N+1번째 패킷 요청

도면4


220
DRM 에이전트
210
SCWS 모듈
110
컨텐츠 재생 단말
150
사용권한 제공 서버
a
사용권한 요청
S410
S420
해당 컨텐츠의 사용권한 생성
사용권한 다운로드
b
S430