(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0073485
(43) 공개일자 2009년07월03일

(51) Int. Cl.
H04N 7/167 (2006.01) *H04N 5/44* (2006.01)
(21) 출원번호 10-2007-0141446
(22) 출원일자 2007년12월31일
심사청구일자 2007년12월31일

(71) 출원인
주식회사 드리머아이
서울특별시 금천구 가산동 345-30
(72) 발명자
이주화
경기도 성남시 중원구 상대원동 279-1
선경상대원2차 APT116동 1106호
김점곤
서울특별시 송파구 석촌동 259-15번지 401호
(74) 대리인
김영철, 김 순 영

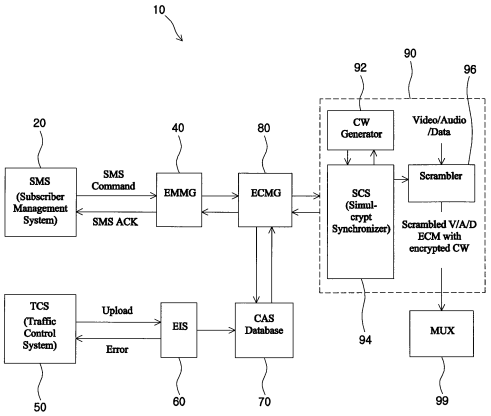
전체 청구항 수 : 총 5 항

(54) 디지털 데이터 방송용 수신제한시스템

(57) 요 약

본 발명은 디지털 데이터 방송 시스템에 관한 것으로서, 특히 디지털 데이터 방송의 수신제한시스템에 관한 것이다. 본 발명에 의하면, EMM 데이터를 생성하는 EMM 생성기와, ECM 데이터를 생성하는 ECM 생성기와, 제어 워드(CW)를 생성하는 CW 생성기와, 방송 데이터를 스크램블하는 스크램블러를 포함하며, 상기 EMM 생성기는 EMM 데이터를 상기 ECM 생성기로 전달하며, 상기 ECM 생성기는 상기 EMM 데이터를 ECM 데이터 내에 삽입하여 상기 스크램블러로 전달하는 디지털 데이터 방송용 수신제한시스템가 제공된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

EMM 데이터를 생성하는 EMM 생성기와,

ECM 데이터를 생성하는 ECM 생성기와,

제어 워드(CW)를 생성하는 CW 생성기와,

방송 데이터를 스크램블하는 스크램블러를 포함하며,

상기 EMM 생성기는 EMM 데이터를 상기 ECM 생성기로 전달하며,

상기 ECM 생성기는 상기 EMM 데이터를 ECM 데이터 내에 삽입하여 상기 스크램블러로 전달하는 디지털 데이터 방송용 수신제한시스템.

청구항 2

제1항의 수신제한시스템에 있어서, 상기 ECMG 및 EMMG는 제어 정보용 TCP/IP 프로토콜 및 데이터 정보용 UDP 프로토콜을 따르는 동일한 모듈로 형성되는 디지털 데이터 방송용 수신제한시스템.

청구항 3

제1항의 수신제한시스템에 있어서, 상기 ECMG 및 EMMG는 제어 및 데이터 정보용 TCP/IP 프로토콜을 따르는 분리된 모듈로 형성되는 디지털 데이터 방송용 수신제한시스템.

청구항 4

제1항의 수신제한시스템에 있어서, 상기 제어 워드는 비대칭 암호화 알고리즘에 의해 암호화된 제어 워드인 디지털 데이터 방송용 수신제한시스템.

청구항 5

제1항 내지 제4항 중 어느 하나의 청구항의 수신제한시스템에 있어서, 상기 제어 워드는 모든 가입자를 위한 동일한 개인 키에 의해 해독되는 디지털 데이터 방송용 수신제한시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 디지털 데이터 방송 시스템에 관한 것으로서, 특히 디지털 데이터 방송의 수신제한시스템에 관한 것이다.

배 경 기 술

<2> 최근 방송의 디지털화가 진행되면서, 디지털 비디오 방송(DVB, Digital Video Broadcasting)과 디지털 오디오 방송(Digital Audio Broadcasting)과 같은 디지털 데이터 방송 서비스가 각광받고 있다. 디지털 데이터 방송 서비스에서 핵심이 되는 기술은 수신제한시스템(CAS, Conditional Access System)이다. CAS는 권한을 가진 가입자만이 방송 서비스를 이용할 수 있게 하는 시스템으로서, 수신가능 여부를 각각의 디지털 방송 수신기가 결정하도록 하는 일련의 과정을 의미한다. 수신제한시스템은 가입자가 서비스, 프로그램 및 이벤트에 접근할 수 있도록 제어한다. 방송 시스템에서 서비스, 프로그램 및 이벤트는 비디오, 오디오 및 데이터의 3가지 요소로 이루어진다. 이들 3가지 요소가 결합되어 이벤트를 형성한다. 방송장치의 제어하에 하나 이상의 이벤트의 결합이 프로그램을 형성한다. 서비스는 방송장치의 제어하에 스케줄에 따라 방송되는 일련의 프로그램이다.

<3> CAS는 신호를 암호화하여 송신하는 송신측(CAS 서버, 'Head-End'라고도 함)와, 암호화된 신호를 수신하여 해독하는 수신측(CAS 클라이언트)으로 이루어진다. CAS 서버는 비디오, 오디오 및 데이터의 3가지 요소를 적절한 암호화 알고리즘으로 엔코딩하여 다중송신한다. 일반적으로 CAS 서버는 ECMG(ECM Generator), EMMG(EMM

Generator), SMS(Subscriber Management System), TCS(Traffic Control System), MUX를 포함한다. ECMG는 ECM(Entitlement Control Message, 자격 제어 메시지) 섹션(section)을 생성하고, CW(Control Word, 제어 워드)를 ECM 섹션으로 운반한다. SMS는 모든 가입자에 대한 상세한 정보를 저장하며, EMMG를 통해 EMM(Entitlement Management Message, 자격 관리 메시지) 생성을 초기화한다. SCS(SimulCrypto Synchronizer)로부터의 요청에 따라, EMMG는 EMM 섹션(section)을 생성하고 이것을 MUX로 전달한다. EMM는 CW의 암호화에 사용되는 서비스 키(Service Key)를 포함한다. EMMG와 ECMG의 출력 데이터는 암호화된다. CW로 스크램블된 A/V 방송 스트림은 EMM 및 ECM과 함께 클라이언트로 전송된다. 클라이언트는 스마트 카드를 이용하여 EMM을 해독하여 서비스 키를 추출한다. 추출된 서비스 키를 이용하여 ECM은 해독되고 ECM 내의 CW가 추출된다. CW를 이용하여 방송 데이터가 해독된다.

<4> 종래에는 EMM 내의 서비스 키를 보낼 때, EMM은 많은 대역폭(bandwidth)을 차지하는 각 개인의 가입자에게 보내져야 한다. EMM 대역폭의 요구량은 가입자의 수에 비례하므로, 가입자 수가 증가함에 따라 보다 많은 대역폭이 요구되는데, 이는 송신측의 큰 부담으로 작용한다.

발명의 내용

해결 하고자하는 과제

<5> 본 발명의 목적은 EMM에 따른 대역폭을 최소화하는 디지털 데이터 방송의 수신제한시스템을 제공하는 것이다.

과제 해결수단

<6> 상기와 같은 목적을 달성하기 위하여, 본 발명은 ECM 내에 EMM을 삽입한다. 본 발명은 ECM과 EMM을 암호화하는 대신에 CW를 암호화한다.

<7> 본 발명의 일측면에 따르면, EMM 데이터를 생성하는 EMM 생성기와, ECM 데이터를 생성하는 ECM 생성기와, 제어 워드(CW)를 생성하는 CW 생성기와, 방송 데이터를 스크램블하는 스크램블러를 포함하며, 상기 EMM 생성기는 EMM 데이터를 상기 ECM 생성기로 전달하며, 상기 ECM 생성기는 상기 EMM 데이터를 ECM 데이터 내에 삽입하여 상기 스크램블러로 전달하는 디지털 데이터 방송용 수신제한시스템가 제공된다.

<8> 상기 수신제한시스템에 있어서, 상기 ECMG 및 EMMG는 제어 정보용 TCP/IP 프로토콜 및 데이터 정보용 UDP 프로토콜을 따르는 동일한 모듈로 형성될 수 있다.

<9> 상기 수신제한시스템에 있어서, 상기 ECMG 및 EMMG는 제어 및 데이터 정보용 TCP/IP 프로토콜을 따르는 분리된 모듈로 형성될 수 있다.

<10> 상기 수신제한시스템에 있어서, 상기 제어 워드는 비대칭 암호화 알고리즘에 의해 암호화될 수 있다.

<11> 상기 수신제한시스템에 있어서, 상기 제어 워드는 모든 가입자를 위한 동일한 개인 키에 의해 해독될 수 있다.

효 과

<12> 본 발명의 구성을 따르면 앞서서 기재한 본 발명의 목적을 모두 달성할 수 있다. 구체적으로는 ECM 데이터가 EMM 데이터를 포함하는 구조이므로, 데이터 송신의 부담을 현저하게 감소시킬 수 있다.

발명의 실시를 위한 구체적인 내용

<13> 이하, 도면을 참조하여 본 발명의 일실시예를 상세히 설명한다.

<14> 도1을 참조하면, 수신제한시스템(10)은 유료 방송 시스템을 위한 것으로서, SMS(Subscriber Management System)(20), TCS(Traffic Control System)(50), ECMG(Entitlement Control Message Generator)(80), EMMG(Entitlement Management Message Generator)(40), EIS(Event Information Scheduler)(60), CAS 데이터베이스(70), 멀티플렉서(Multiplexer)(99), 스크램블러 모듈(90)을 구비한다. 스크램블러 모듈(90)은 CW 생성기(92), 사이멀크립트 동기장치(SCS, SimulCrypt Synchronizer)(94)와, 스크램블러(scramber)(96)를 구비한다.

<15> SMS(20)는 가입자 등록 정보 및 청구 정보와 같은 가입자 관리 정보를 감독하기 위한 시스템이다. SMS(20)는 가입, 계산 및 청구의 기능을 갖는 유료 방송 시스템에서 중심 시스템이다. 추가적으로, SMS(20)는 그룹 관리, 텍스트 메시지 명령 및 보안 명령과 같은 다른 기능도 갖는다. SMS(20)는 클라이언트이고 EMMG(40)은 서버이다. SMS(20)로부터 명령어 메시지가 EMMG(40)로 전달되고, EMMG(40)로부터는 확인 메시지가 SMS(20)로 전달된다.

<16> EMMG(40)는 SMS 명령에 따라 EMM 섹션을 생성하는 장치이다. EMMG(40)의 출력은 EMM 블록(Block)의 형태가 된다. EMM 블록 유니크(unique)한 태그(tag)를 갖는다. EMMG(40)는 수신제한시스템의 한명의 가입자 또는 그룹 또는 모든 가입자를 지정할 수 있다.

<17> TCS(50)는 방송 시스템의 방송 스케줄을 관리하는 시스템이다. TCS(50)는 각 서비스 채널을 정해진 시간을 갖는 이벤트로 정의하고, 이벤트에 대한 작동 수단을 결정한다. TCS(50)는 각 이벤트의 정해진 시간 동안 접근 기준(access criteria)을 포함하는 ECM을 만들기 위해 각 서비스의 CAS 관련 이벤트 스케줄을 CAS 서버로 전달해야 한다. CAS 관련 이벤트 스케줄 정보는 CAS 제어 정보(접근 기준), PPV(Pay Per View) 정보, 및 특정 이벤트의 자녀 보호(Parental Control)이다. TCS(50)는 CAS 관련 이벤트 정보를 SIF(Schedule Information Format) 형식으로 조직한다.

<18> EIS(60)는 TCS(50)와 CAS 데이터베이스(70) 사이를 연결하는 장치이다. EIS(60)는 SIF 형성 파일을 파스하고, 그 데이터를 CAS 데이터베이스(70)에 저장한다.

<19> ECMG(80)는 스크램블러 모듈(90)의 요청에 따라 특정 서비스에 대하여 ECM을 생성하는 장치이다. ECMG(80)는 이벤트 스케줄 정보를 포함하는 CAS 데이터베이스(70)로부터 현 시점에 해당하는 서비스 이벤트를 검색한 후, 해당 이벤트를 위한 접근 기준을 생성한다. 전달된 CW 및 생성된 접근 기준과 함께, ECMG(80)는 ECM을 생성한 후 스크램블러 모듈(90)로 전달한다.

<20> 스크램블러 모듈(90)은 비디오/오디오/데이터 입력을 스크램블하여 보호하는 장치이다. 스크램블러 모듈(90)는 비디오, 오디오 및 데이터의 다양한 콘텐츠 형태를 지원하며 다양한 엔코딩 시스템과 멀티플렉서를 통합하고 협력하는 것이 가능하다. 스크램블러 모듈(90)은 CW 생성기(92), 동기장치(94)와, 스크램블러(96)를 구비한다. 또한 스크램블러 모듈(90)은 DVB 사이멀크립트 표준을 따르는 공유 스크램블러 기능을 제공하여, 하나 이상의 CAS로 통합함으로써 스크램블된 비디오, 오디오 데이터를 갖는 각 CAS의 ECM 및 EMM을 보내고 받는다.

<21> 이제, 도1 내지 도5를 참조하여 상기 실시예의 작용을 상세히 설명한다.

<22> SMS(20)는 XML 형식의 명령을 만들고, 이를 HTTP 요청을 통해 EMMG(40)로 전달한다. EMMG(40)은 요청을 처리하고 결과를 XML 형식으로 HTTP 응답을 통해 SMS(20)로 보낸다.

<23> TCS(50)는 CAS 관련 이벤트 스케줄 정보를 SIF 형식으로 조직한다. EIS(60)는 SIF 파일을 다운로드하고 업로드하기 위한 내부 버퍼(buffer)를 포함한다. EIS(60)는 업로드된 파일을 계속 체크하며, 성공적으로 수행되었을 때 EIS(60)는 SIF 정보를 CAS 데이터베이스(70)의 이벤트 스케쥴 정보로서 기록한다. 만일 받은 파일에 대한 체크 중에 에러가 발생할 경우, EIS(60)는 에러 로그 파일을 만들고 이를 에러 폴더에 저장한다.

<24> ECMG(80)와 스크램블러 모듈(90) 사이의 인터페이스(interface)는 DVB 사이멀크립트 포로토콜에 기반한다.

<25> 클라이언트인 EMMG(40)와 서버인 ECMG(80)는 도2에 도시한 바와 같이 연결 지향(connection-oriented) TLV 프로토콜을 사용한다. TCP 프로토콜은 DVB 사이멀크립트 표준에서 사용되는 바와 같이 데이터 제공 및 제어를 위해 사용된다.

<26> SMS 요청이 EMMG(40)에 전달되면, EMMG(40)는 EMM 섹션을 생성하고, 이를 제어 데이터 프로토콜를 이용하여 ECMG(80)로 전달한다. EMMG(40)의 데이터를 수신하면, ECMG(80)는 EMM 섹션을 큐 버퍼(queue buffer)에 저장하고, 도4에 도시된 바와 같이 SCS(94)의 요청에 따라 최초 수신 EMM 블록(150)을 ECM 섹션에 삽입한다. 만일 ECM 큐 버퍼에 둘 이상의 EMM 블록이 있다면, ECMG(80)는 도5에 도시된 바와 같이 EMM 블록(150a)을 ECM 센션 내에 가능한 크기로 삽입한다. ECMG(80)는 각 EMM의 발송/미발송 상태를 유지한다. SCS(94)의 다음 요청이 있으면, ECMG(80)는 큐 버퍼로부터 발송 EMM 메시지를 삭제하고, ECM 섹션의 미발송 EMM 메시지를 발송한다. 에러 메시지를 접수하면, ECMG(80)는 이미 발송한 메시지의 상태를 토글(toggle)한다.

<27> ECMG(80)와 EMMG(40)는 동일한 모듈 또는 분리된 모듈로 형성될 수 있는데, 동일한 모듈로 형성될 경우 제어 정보를 위한 TCP/IP 프로토콜 및 데이터 정보를 위한 UDP 프로토콜을 따르며, 분리된 모듈로 형성될 경우에는 제어 및 데이터 정보를 위해 TCP/IP 프로토콜을 따른다.

<28> 본 발명은 EMM 및 ECM 섹션을 암호화하는 대신에 제어 워드(CW)를 암호화하고자 한다. 이를 지원하고자, EMM 블록은 어떠한 키(Key) 섹션도 포함하지 않으며, EMM 블록이 유니크한 태그에 의해 식별됨을 의미하는 TLV 형식을 따른다. EMM 블록은 주로 2가지 섹션을 포함하는데, 첫째는 타겟(target) 상세부이고, 둘째는 메시지 상세부에 관한 것이다. 도3에 도시된 바와 같이 다른 구조가 ECM 섹션에 삽입될 때, EMM 섹션은 도4 및 도5에 도시된 바와 같이 각각의 태그를 갖는 ECM 섹션 안으로 삽입될 수 있다. EMM 블록이 없는 경우, ECM 섹션은 도3에 도시된

바와 같이 ECM 정보 블록 만을 포함한다.

<29> 제어 워드를 암호화하기 위하여 비대칭 암호화 방법이 사용된다. 각 가입자는 암호화된 제어 워드를 해독하는 동일한 개인 키를 갖는다. 본 실시예의 CAS는 비대칭 암호화 알고리즘으로서 NTRU 암호화, RSA 및 EIGamal을 사용한다.

<30> 본 발명은 DVB 및 DAB 표준에 따라 데이터를 제어하고 관리하고 방송하는 디지털 방송 시스템에 이용할 수 있다.

<31> 이상 본 발명을 상기 실시예를 들어 설명하였으나, 본 발명은 이에 제한되는 것이 아니다. 당업자라면, 본 발명의 취지 및 범위를 벗어나지 않고 수정, 변경을 할 수 있으며 이러한 수정과 변경 또한 본 발명에 속하는 것임을 알 수 있을 것이다.

도면의 간단한 설명

<32> 도1은 본 발명의 일실시예에 다른 수신제한시스템의 구조를 도시한 블록도이다.

<33> 도2는 도1의 EMMG와 ECMG 사이의 포로토콜 인터페이스를 도시한 도면이다.

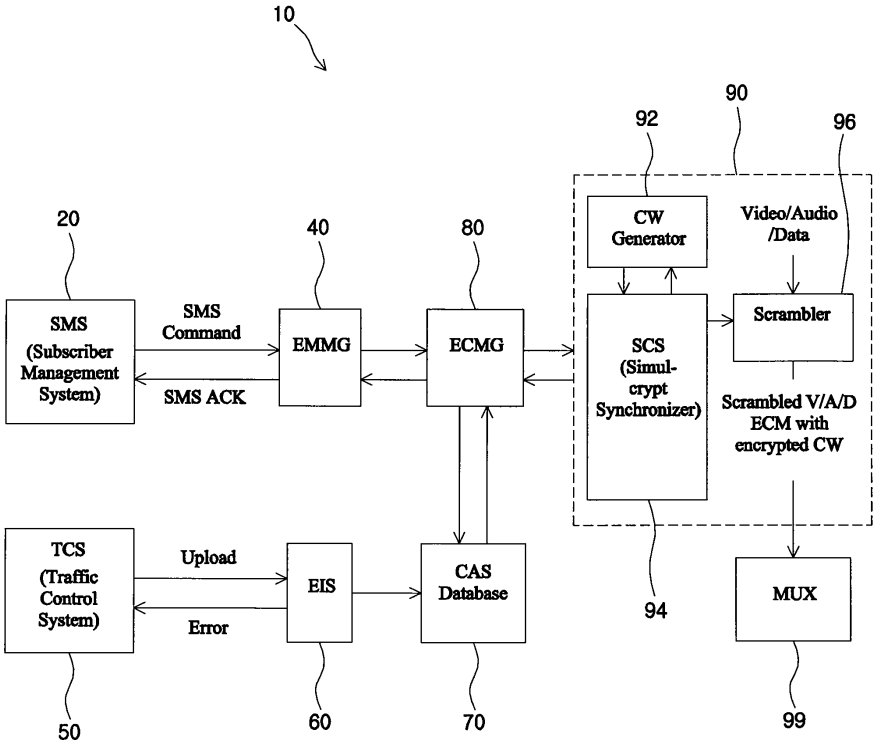
<34> 도3은 일반적은 ECM의 데이터 구조를 도시한 도면이다.

<35> 도4는 EMM을 갖는 ECM의 데이터 구조를 도시한 도면이다.

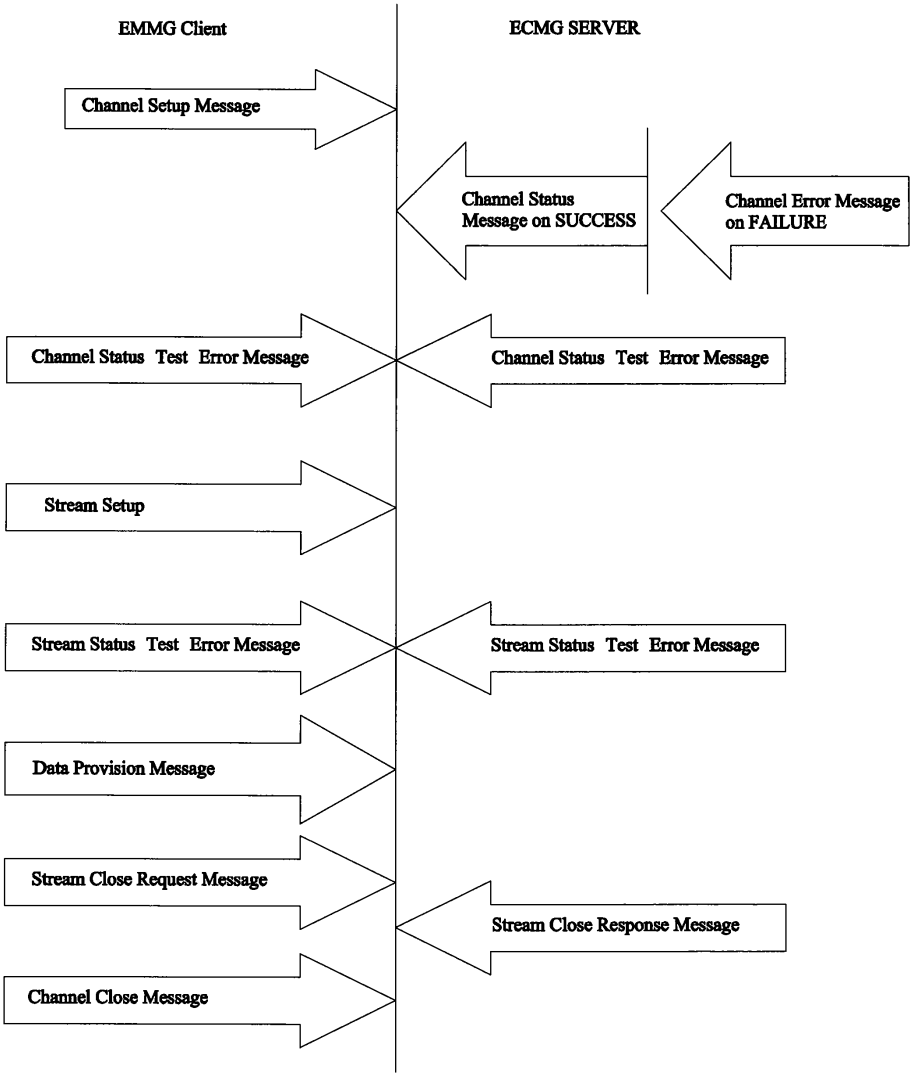
<36> 도5는 다중의 EMM을 갖는 ECM의 데이터 구조를 도시한 도면이다.

도면

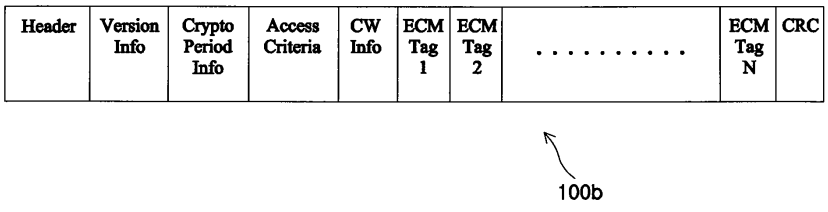
도면1



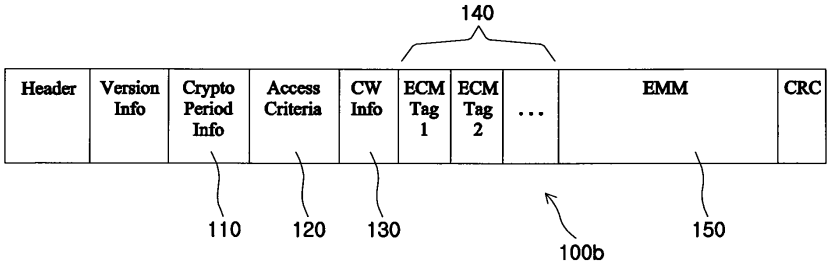
도면2


EMMG Client
ECMG SERVER
Channel Setup Message
Channel Status Message on SUCCESS
Channel Error Message on FAILURE
Channel Status Test Error Message
Channel Status Test Error Message
Stream Setup
Stream Status Test Error Message
Stream Status Test Error Message
Data Provision Message
Stream Close Request Message
Stream Close Response Message
Channel Close Message

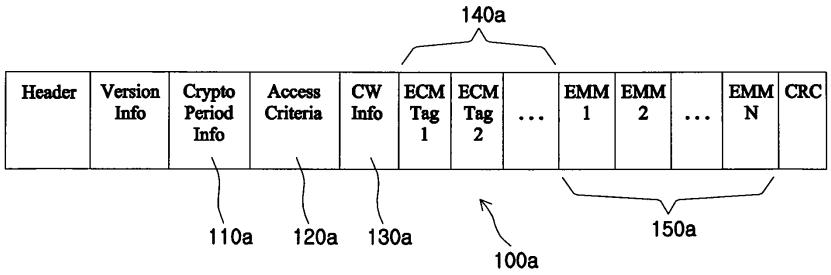
도면3


Header
Version Info
Crypto Period Info
Access Criteria
CW Info
ECM Tag 1
ECM Tag 2
. . . . . .
ECM Tag N
CRC
100b

도면4


140
Header
Version Info
Crypto Period Info
Access Criteria
CW Info
ECM Tag 1
ECM Tag 2
...
EMM
CRC
110
120
130
100b
150

도면5


140a
Header
Version Info
Crypto Period Info
Access Criteria
CW Info
ECM Tag 1
ECM Tag 2
...
EMM 1
EMM 2
...
EMM N
CRC
110a
120a
130a
100a
150a