(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년12월07일
(11) 등록번호 10-0782865
(24) 등록일자 2007년11월30일

(51) Int. Cl.
H04L 9/00 (2006.01)
(21) 출원번호 10-1999-0016936
(22) 출원일자 1999년05월12일
심사청구일자 2004년05월12일
(65) 공개번호 10-1999-0088222
(43) 공개일자 1999년12월27일
(30) 우선권주장
98-129214 1998년05월12일 일본(JP)
(56) 선행기술조사문헌
KR 1996-0015309 A(1996.05.22)
전체 청구항 수 : 총 19 항

(73) 특허권자
소니 가부시끼 가이샤
일본국 도쿄도 미나토쿠 코난 1-7-1
(72) 발명자
하라가즈히로
일본도쿄도시나가와구기다시나가와6-7-35소니가부시키가이샤내
(74) 대리인
이범래, 이병호, 장훈

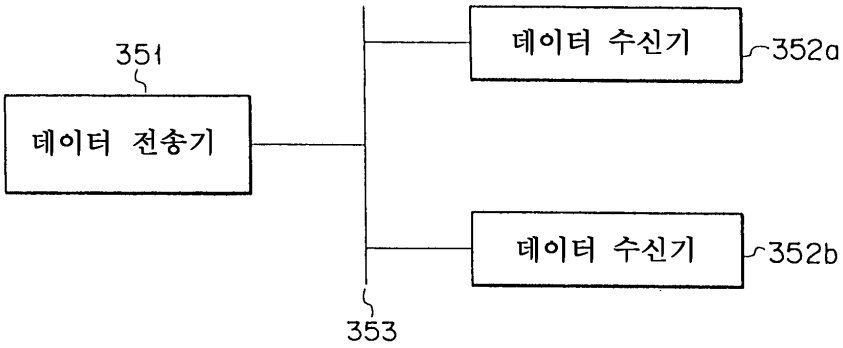
심사관 : 이준석

(54) 데이터 전송 제어 방법 및 데이터 전송 시스템

(57) 요 약

본 발명에 따른 데이터 전송 시스템은 데이터 전송기로부터 데이터 수신기 또는 수신기들로 안전하고 확실한 데이터 전송을 가능하게 한다. 시스템은 데이터를 암호화하여 암호화된 데이터를 전송하는 데이터 전송기와; 데이터 전송기로부터 암호화된 데이터를 수신하는 데이터 수신기와; 데이터 전송기로부터 데이터 수신기로의 데이터 전송에 사용되는 위성 링크와; 데이터 수신기들로부터 데이터 전송기로 데이터를 전송하는 데 사용되며, 위성 링크들보다 더 적은 데이터 전송 용량을 갖는 양방향 통신 채널을 포함한다. 위성 링크는 데이터 전송기로부터 암호화된 데이터를 데이터 수신기로 전송하는데 사용된다. 적어도 양방향 통신 채널은 데이터 전송기와 데이터 수신기 사이에서 제한 데이터 전송 제어 정보를 주고받는데 사용된다.

대표도 - 도1



특허청구의 범위

청구항 1

통신 채널들을 통한 데이터 전송 수단으로부터 데이터 수신 수단에의 데이터의 전송을 제어하는 데이터 전송 제어 방법에 있어서,

상기 데이터 전송 수단으로부터 상기 데이터 수신 수단에의 데이터의 전송을 위해 제공되는 제 1 통신 채널을 통하여, 상기 데이터 전송 수단에 의해 암호화된 데이터를 상기 데이터 수신 수단에 전송하는 단계; 및

상기 제 1 통신 채널보다 데이터 전송 용량이 작고, 상기 데이터 수신 수단으로부터 상기 데이터 전송 수단에의 데이터 전송에 또한 사용되는 적어도 제 2 통신 채널을 통하여, 특정한 데이터 수신 수단에 의해서만 상기 암호화된 데이터가 수신되도록 하기 위한 제한 데이터 전송 제어 정보(restrictive data transmission control information)를 상기 데이터 수신 수단에 전송하는 단계를 포함하는, 데이터 전송 제어 방법.

청구항 2

제 1항에 있어서, 상기 제 2 통신 채널은 상기 데이터 전송 수단과 상기 데이터 수신 수단 사이에서 양방향 통신을 허용하는 통신 채널인, 데이터 전송 제어 방법.

청구항 3

제 1항에 있어서, 상기 데이터 전송 수단은 암호화 키를 사용하여 데이터 암호화를 수행하고, 상기 데이터 전송 수단으로부터 상기 암호화된 데이터는 상기 데이터 암호화에 사용된 상기 암호화 키와 동일한 복호화 키를 이용하여 상기 데이터 수신 수단에 의해 복호화되는, 데이터 전송 제어 방법.

청구항 4

제 3항에 있어서, 상기 암호화 키 및 상기 복호화 키는 정보 및 데이터를 암호화 및 복호화하는 세션 키들인, 데이터 전송 제어 방법.

청구항 5

제 4항에 있어서, 상기 세션 키들은 미리 결정된 간격들로 갱신되는, 데이터 전송 제어 방법.

청구항 6

제 4항에 있어서, 상기 데이터 전송 수단 및 상기 데이터 수신 수단은 상기 데이터 수신 수단에 특정한 마스터 키를 가지며,

상기 데이터 전송 수단은 상기 마스터 키를 이용하여 상기 세션 키들을 암호화하여, 상기 암호화된 세션 키들을 상기 제 1 통신 채널 또는 상기 제 2 통신 채널을 통하여 상기 데이터 수신 수단에 전송하고,

상기 데이터 수신 수단은 상기 마스터 키를 이용하여 수신된 상기 암호화된 세션 키들을 복호화하는, 데이터 전송 제어 방법.

청구항 7

제 6항에 있어서, 상기 데이터 전송 수단은 특정한 정보 및 데이터의 수신이 허가되는 모든 데이터 수신 수단에 대응하는 상기 세션 키들을 가지며,

상기 데이터 전송 수단은 특정한 정보 및 데이터의 수신이 허가되는 상기 데이터 수신 수단에 상기 세션 키들을 미리 전송하는, 데이터 전송 제어 방법.

청구항 8

제 1항에 있어서, 상기 제 1 통신 채널은 상기 데이터 전송 수단으로부터 상기 데이터 수신 수단에의 단방향 통신을 허용하는 위성 링크이고,

상기 제 2 통신 채널은 상기 데이터 전송 수단과 상기 데이터 수신 수단 사이에서 양방향 통신을 허용하는 통신

채널인, 데이터 전송 제어 방법.

청구항 9

제 1항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되는, 데이터 전송 제어 방법.

청구항 10

제 1항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되는, 데이터 전송 제어 방법.

청구항 11

데이터 전송 시스템에 있어서,

데이터를 암호화하고 상기 암호화된 데이터를 전송하는 데이터 전송 수단;

상기 데이터 전송 수단으로부터 상기 암호화된 데이터를 수신하는 데이터 수신 수단;

상기 데이터 전송 수단으로부터 상기 데이터 수신 수단에의 데이터 전송에 사용되는 제 1 통신 채널; 및

데이터 수신 수단으로부터 상기 데이터 전송 수단에의 데이터 전송에 또한 사용되며, 상기 제 1 통신 채널보다 더 작은 데이터 전송 용량을 갖는 제 2 통신 채널;을 포함하고,

상기 제 1 통신 채널은 상기 암호화된 데이터를 전송하는데 사용되고,

적어도 상기 제 2 통신 채널은 특정한 데이터 수신 수단에 의해서만 상기 암호화된 데이터가 수신되도록 하기 위한 제한 데이터 전송 제어 정보를 전송하는데 사용되는, 데이터 전송 시스템.

청구항 12

제 11항에 있어서, 상기 데이터 전송 수단은 암호화 키를 사용하여 데이터 암호화를 수행하고, 상기 데이터 전송 수단으로부터의 상기 암호화된 데이터는 상기 데이터 암호화에 사용된 상기 암호화 키와 동일한 복호화 키를 사용하여 상기 데이터 수신 수단에 의해 복호화되는, 데이터 전송 시스템.

청구항 13

제 12항에 있어서, 상기 암호화 키 및 상기 복호화 키는 정보 및 데이터를 암호화 및 복호화하는 세션 키들인, 데이터 전송 시스템.

청구항 14

제 13항에 있어서, 상기 세션 키들은 미리 결정된 간격들로 갱신되는, 데이터 전송 시스템.

청구항 15

제 13항에 있어서, 상기 데이터 전송 수단 및 상기 데이터 수신 수단은 상기 데이터 수신 수단에 특정한 마스터 키를 가지며,

상기 데이터 전송 수단은 상기 마스터 키를 이용하여 상기 세션 키들을 암호화하여, 상기 암호화된 세션 키들을 상기 제 1 통신 채널 또는 상기 제 2 통신 채널을 통하여 상기 데이터 수신 수단에 전송하고,

상기 데이터 수신 수단은 상기 마스터 키를 이용하여 수신된 상기 암호화된 세션 키들을 복호화하는, 데이터 전송 시스템.

청구항 16

제 15항에 있어서, 상기 데이터 전송 수단은 특정한 정보 및 데이터의 수신이 허가되는 모든 데이터 수신 수단에 대응하는 상기 세션 키들을 가지며,

상기 데이터 전송 수단은 특정한 정보 및 데이터의 수신이 허가되는 상기 데이터 수신 수단에 상기 세션 키들을 미리 전송하는, 데이터 전송 시스템.

청구항 17

제 11항에 있어서, 상기 제 1 통신 채널은 상기 데이터 전송 수단으로부터 상기 데이터 수신 수단에의 단방향 통신을 허용하는 위성 링크인, 데이터 전송 시스템.

청구항 18

제 11항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되는, 데이터 전송 시스템.

청구항 19

제 11항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되는, 데이터 전송 시스템.

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<25> 본 발명은 데이터 전송기로부터 데이터 수신기로의 데이터 전송 제어를 위한 데이터 전송 제어 방법 및 데이터 전송 시스템에 관한 것이다. 보다 구체적으로, 데이터 전송기로부터 특정한 데이터 수신기로 전송된 데이터의 수신을 제한하는 데이터 전송 제어 방법 및 데이터 전송 시스템에 관한 것이다.

<26> 최근, 데이터 전송기로 하여금 데이터를 복수의 멀리 떨어져 위치하고 있는 데이터 수신기들로 전송하도록 허용하는 네트워크 타입의 데이터 전송 시스템들이 확립되었다. 예를 들면, 위성 텔레비전 방송이 위성 링크를 이용하는 방송 데이터 전송 시스템으로서 구현되어 영상 및 음성 정보를 복수의 데이터 수신기들에 분배한다.

<27> 방송 데이터 전송 시스템의 다른 예로는 로컬 에리어 네트워크(LAN)로서 설정되는 이더넷(Ethernet)이 있다. 도 1에 도시한 바와 같이, 이더넷 네트워크는 통상적으로 데이터를 전송하는 데이터 전송기(351) 및 데이터 전송기(351)로부터 네트워크(353)를 통하여 데이터를 수신하는 데이터 수신기(352a 및 352b)로 구성된다. 이더넷 상의 데이터 수신기들 사이의 최대 허용 거리는 수 킬로미터로 설정되어 있다.

<28> 데이터 전송 시스템에서 데이터 전송기(351)가 데이터 수신기(352a)에 데이터를 전송하는 경우, 데이터 전송기(351)는 네트워크(353) 상으로 데이터를 전송한다. 전송된 데이터에는 목적지 데이터 수신기(352a)를 식별하는 목적지 어드레스가 추가된다. 예를 들면, 대용량의 목적지 어드레스 정보를 표현하는데 48 비트가 사용된다.

<29> 데이터 전송기(351)에 의해 네트워크(353)로 전송된 데이터는 데이터 수신기들(352a 및 352b)에 의해 수신된다. 각 데이터 수신기는 수신된 데이터에 추가된 목적지 어드레스를 참조하여 어드레스가 자신의 어드레스와 대응하는지 확인한다. 이더넷에 의해 사용된 통상적인 프레임 포맷은 도 2에 도시된 바와 같이 구성된다. 이 포맷에서, 목적지 어드레스부(401)는 데이터를 수신하는 목적지 데이터 수신기의 어드레스를 나타낸다.

<30> 주어진 데이터 수신기가 수신된 어드레스가 자신의 어드레스가 아니라고 판정하면, 수신기는 전송된 데이터를 폐기한다. 즉, 데이터 수신기(352a)가 데이터에 추가된 어드레스가 자신의 어드레스라고 판정하면 전송된 데이터를 받아들이고, 데이터 수신기(352a)가 수신된 데이터에서 자신의 어드레스를 검출하지 못하면 그 데이터를 폐기하는 것이다. 이더넷 상에서의 데이터 수신기에 의한 데이터 수신 프로세스는 일반적으로 도 3의 흐름도를 구성하는 단계들에서 도시한 바와 같이 진행한다.

<31> 단계 S101에서, 데이터 수신기는 로컬 에리어 네트워크로부터 데이터를 포함하는 이더넷 프레임을 수신한다. 단계 S102에서, 데이터 수신기는 수신된 이더넷 프레임으로부터 목적지 어드레스를 추출한다. 단계 S103에서, 데이터 수신기는 목적지 어드레스가 자신의 어드레스(유니캐스트(unicast) 어드레스)인지 또는 자신이 속한 어드레스(멀티캐스트(multicast) 어드레스)인지 검사한다. 만약 목적지 어드레스가 수신기 그 자체의 어드레스(유니캐스트 어드레스) 또는 그것이 속한 어드레스(멀티캐스트 어드레스)인 것으로 판정되면, 데이터 수신기는

이더넷 프레임을 호스트 컴퓨터에 전송한다. 유니캐스트 어드레스는 개별적인 수신기를 지정하는 어드레스를 나타내고, 멀티캐스트 어드레스는 그 어드레스와 관련하여 전송된 데이터를 수신하는 복수의 데이터 수신기들(예를 들면, 데이터 수신기 그룹)를 허용하는 어드레스이다.

<32> 만약, 목적지 어드레스가 요구된 데이터 수신기를 지정하는 어드레스(유니캐스트 어드레스)도 데이터 수신기가 속한 어드레스(멀티캐스트 어드레스)도 아니라고 판정하면, 데이터 수신기는 이더넷 프레임을 폐기한다.

<33> 목적지 어드레스 기법에 기초한 데이터 전송 방법에 따르면, 데이터 수신기의 어드레스가 전송된 목적지 어드레스와 일치하지 않는 어떠한 데이터 수신기도 그 어드레스로 공급된 데이터를 수신할 수 없을 것이다. 그러나, 사실상 데이터 전송 방법에 의해 데이터 수신기가 자신의 어드레스를 가질 수도 있으며 다른 지정된 데이터 즉, 문제의 데이터 수신기를 식별하는 목적지 어드레스가 없는 데이터를 받아들이도록 부정하게 수정된 판정 특징을 가질 수도 있다. 이러한 가능성은 비밀 데이터가 특정한 데이터 수신기에 전송될 필요가 있는 경우에 보안상의 문제를 유발할 것이다.

<34> 이더넷 상에서, 동일 네트워크에 접속된 데이터 수신기들의 수는 제한되고, 접속된 수신기들 사이의 거리들도 제한된다. 이는 하나의 데이터 수신기로 전송된 데이터가 다른 데이터 수신기에 의해 불법으로 연결될 수도 있는 제한된 가능성이 있음을 의미한다. 예를 들면, 10BASE-5의 통상적인 이더넷 구조에서, 한 세그먼트에 대한 최대 케이블 길이는 500 미터로 제한되고 네트워크에 접속할 수 있는 트랜시버들(데이터 송수신기)의 수는 100까지로 설정된다.

<35> 반면에, 데이터 전송 네트워크가 위성 링크들을 이용하여 구성되면, 하나의 네트워크는 일본과 같은 한 국가 전체보다 더 넓은 영역을 커버할 수 있다. 이러한 네트워크 상에서, 홋카이도의 최북단 섬에 위치한 데이터 수신기로 전송된 데이터가 최남단의 오키나와 현에 위치한 데이터 수신기에 의해 도청될 수 있다. 즉, 다수의 데이터 수신기로 구성되는 임의의 위성 링크 기준 네트워크 상에서는, 예상치 못한 무리에 의해 불법으로 도청될 가능성이 증가한다.

<36> 위성 링크들과 같은 방송 타입 통신 채널들을 이용한 데이터 전송 설정에서는, 처리되지 않은 데이터가 의도한 데이터 수신기뿐만 아니라 문제의 데이터를 수신지 말아야 하는 수신기에 의해서도 수신될 수 있다. 통신 위성을 이용하는 오늘날의 디지털 데이터 방송 시스템들에 나타나는 이 문제에 대한 한가지 해결책은 위성 통신 링크들을 통하여 데이터를 전송하기 전에 데이터(즉, 영상 및 음성 정보)를 암호화하는 것이다. 데이터 수신기들은 원래의 데이터를 재구성하는 복호 기능을 가진다. 이러한 타입의 데이터 전송 시스템에서는, 데이터를 수신하도록 사전에 허가된 데이터 수신기들만 음성-영상물에 대한 전송을 복호할 수 있다. 하나의 그러한 시스템은 통신 기술 협회(일본)에 의한 보고서 제 74번에 기초한다. 시스템은 전송 포맷으로서 MPEG2(동화상 전문가 그룹 제 2단계) 전송 스트림 패킷들(TS 패킷들)을 이용한다. 예를 들면, 시스템은 암호화 키들을 사용하여 데이터 전송기로 하여금 데이터를 암호화하게 하고, 암호화 키에 대응하는 복호화 키를 사용하여 데이터 수신기로 하여금 암호화된 데이터를 복호화하게 한다. TS 패킷의 포맷은 도 4에 도시되어 있다. 포맷의 헤더에 있는 PID(패킷 식별)부(411) 및 스크램블 제어부(412)는 암호화 키를 결정한다. 일반적으로, 암호화 키들은 세션 키(Ks) 및 작업 키(Kw)를 포함한다. PID 부분(411)은 13 비트의 데이터로 구성되고 스크램블 제어부(412)는 2 비트 데이터로 구성된다.

<37> TS 패킷으로 데이터를 전송하도록 설정된 현재의 위성 텔레비전 방송에서의 데이터 전송 시스템은 도 5에 도시되어 있는 바와 같이 데이터 전송기(501) 및 데이터 수신기(511)를 포함한다. 데이터 전송기(501)는 다양한 암호화 키를 사용하여 데이터 암호화를 수행하는 암호 유닛(502, 503, 504)을 가진다. 데이터 수신기(511)는 다양한 암호화 키들을 사용하여 데이터 복호를 수행하는 복호 유닛(512, 513, 514) 및 허가 판단 유닛(515)을 가진다.

<38> 구조의 데이터 전송 시스템에서, 데이터 전송기(501)는 먼저 작업키(506)를 데이터 수신기(511)로 전송한다. 구체적으로, 데이터 전송기(501)는 PID 부분(411) 및 스크램블 제어부(412)에 대응하는 작업 키(Kw)(506)를 미리 준비한다. 그 다음에 데이터 전송기(501)는 마스터 키(Km)(507)를 이용하여 암호화 유닛(504)에 의해 암호화되는 작업 키(Kw)(506)를 얻는다. 암호화된 작업키(Kw)(506)는 데이터 수신기(511)로 전송된다. 마스터 키(Km)(507)는 데이터 수신기(511)에 특정한 마스터 키(복호화 키)(Km)(518)와 동일하다. 암호화된 작업키(Kw)(506)는 데이터 전송기(501)로부터 위성 링크를 통하여 데이터 수신기(511)로 전송된다.

<39> 마스터 키(Km)(507)로 암호화된 작업키(Kw)(506)를 수신 시, 데이터 수신기(511)는 자체의 마스터 키(Km)(518)를 이용하여 수신된 키를 복호화한다. 복호된 작업키(Kw)(517)는 PID 부분에 대응하는 데이터 수신기(511)에 의

해 보존된다. 작업키(Kw)(517)는 데이터 전송기(501)로부터 전송되는 암호화된 데이터를 복호화하는데 사용된다.

<40> 데이터 전송기(501)로부터 데이터 수신기(511)로의 데이터 전송시, 데이터 전송기(501)는 세션 키(Ks)(505)를 이용하여 암호화 유닛(502)에 의해 암호화된 TS 패킷에 데이터의 페이로드부(413)를 가진다. 동시에, 세션 키(Ks)(505)는 작업키(Kw)(506)를 이용하여 암호화 유닛(503)에 의해 암호화된다.

<41> 데이터 수신기(511)를 목적지로서 식별하는 PID 부분을 갖는 TS 패킷 수신시, 데이터 수신기(511)는 전송된 TS 패킷 내의 PID 부분(411)에 기초하여 사전에 보존된 작업키(Kw)(517)를 추출한다. 데이터 수신기(511)는 추출된 작업키(Kw)(517)를 이용하여 데이터 전송기(501)로부터의 데이터와 함께 전송된 암호화된 세션 키(Ks)(505)를 복호화한다. 따라서, 복호된 세션 키(Ks)(516)를 이용하여, 데이터 수신기(511)는 TS 패킷의 페이로드 부분(413)을 복호화하여 그로부터 데이터를 추출한다.

<42> 작업키(Kw)가 아직 이들 데이터 수신기들로 전송되지 않았기 때문에 허가되지 않은 데이터 수신기는 시청하고 싶은 PID 부분에 대응하는 적절한 작업키(Kw)를 가지고 있지 않다. 그러한 데이터 수신기는 데이터 전송기(501)가 작업키(Kw)를 이용한 그 다음 키 암호화에 이어 전송한 세션 키(Ks)를 복호할 수 없다. 복호되지 않은 세션 키(Ks)를 가지고는, 허가되지 않은 데이터 수신기들이 데이터 전송기(501)로부터 암호화된 데이터를 복호할 수 없다. 바꾸어 말하면, 허가되지 않은 데이터 수신기들은 암호화된 데이터만 수신할 수 있고 음성 영상물에 대한 데이터를 복호할 수는 없다.

<43> 위성 링크를 이용하는 방송 시스템은 전술한 바와 같이 통상적으로 제한 데이터 전송 제어(restrictive data transmission control)를 구현한다. 제한 데이터 전송 제어에 대한 많은 다른 방법들이 방송 시스템들뿐만 아니라 인터넷을 통하여서도 실행되고 있다.

<44> 인터넷 상에서는, 전자 메일을 암호화하여 부정한 무리들에 의한 도청 또는 위조를 방지하기 위해 PGP(Pretty Good Privacy) 및 PEM(Privacy Enhanced Mail)을 이용한다. 또한 인터넷 상에서는 HTTP(Hyper Text Transfer Protocol)에 기초한 전자 상거래에서 유통하는 신용카드 번호의 불법 도청을 막기 위해서 SSL(Secure Socket Layer)을 이용한다. 이들 기법들은 암호화 시스템을 이용하거나 또는 유연한 데이터 전송 제어를 채용하고 있다는 특징이 있다.

<45> IP(Internet Protocol) 데이터그램에 대한 보다 일반화된 데이터 전송 제어 방법들이 있다. 이러한 종류의 표준화된 방법들은 AH(Authentication Header) 및 일반적으로 IPSEC라고 하는 ESP(Encapsulating Security Payload)를 포함한다.

<46> 위성 링크를 이용하는 텔레비전 방송과 관련하여 다음의 문제점들이 일반적으로 나타나고 있다.

<47> 첫 번째 문제점은 허가된 데이터 수신기들의 수의 제한이다. 도 4에 도시된 바와 같이, 암호화 키들을 식별하는 PID 부분과 스크램블 제어부는 단지 13 비트들 및 2비트들만을 각각 포함한다. 이것은 15 비트가 2^{15}(=32,768)개 까지의 데이터 수신기들을 지정하는데 채용된다는 것을 의미한다.

<48> 두 번째 문제점은 사용중인 PID의 수가 증가함에 따라서 전송측에서의 비용이 증가한다는 것이다. 예를 들면, 데이터 수신기들은 PID들의 수에 거의 비례하는 개수의 MPEG2 인코더들을 필요로 한다. 따라서 PID 수가 증가함에 따라서 대규모의 설비들을 필요로 하는 데이터 전송측에 비용이 증가하게 된다.

<49> 세 번째 문제점은 위성 링크들을 통한 일방적인 데이터 전송에서 데이터 전송기는 정보가 목적지 데이터 수신기들로 정확하게 전송되었는지 알 수 없다는 것이다. 예를 들면, 데이터 전송기를 인식하지 못하면, 데이터 수신기들이 허가된 상태임에도 불구하고 실제로는 전송기로부터의 데이터를 수신할 수 없는 경우가 있을 수 있다. 그러나, 정보를 보다 신뢰성 있게 데이터 수신기에 전송하는 방법은 시간이 걸린다. 이것은 많은 자원의 낭비를 초래하며, 이 때문에 유연한 데이터 전송 제어에 대해 장애가 된다.

<50> 네 번째 문제점은 IP 데이터그램이 IP 목적지 어드레스로 조정된 PID를 가지고 데이터 전송기에 의해 전송되어야 하는 경우, 인터넷 프로토콜과 관련이 적다는 것이다. 구체적으로, IP 데이터그램의 목적지 어드레스는 13 비트 PID 부분에 대하여 조정하기 어려운 32 비트 어드레스 포맷을 가진다. 또한, 현재 인터넷 상에서 사용되는 전술한 방법은 다음과 같은 다섯 번째 문제점을 갖는다. 즉, PGP, PEM, SSL은 특정한 데이터 전송 제어를 위한 애플리케이션이며 인터넷 상의 모든 애플리케이션에 공통인 것은 아니다. 각 애플리케이션이 자체 제어 방법을 가질 필요가 있기 때문에, 새롭게 도입된 애플리케이션의 신속한 처리가 어렵게 된다.

<51> 여섯 번째 문제점은 인증 헤더(authentication header) 및 캡슐화 보안 페이로드가 애플리케이션과 무관하며, 인터넷 프로토콜의 현재 버전(예를 들면, IP v4)의 수준에서 이들 방법과 호환가능한 네트워크 장치들이 사실상 없다는 것이다. 인터넷 프로토콜의 다음 버전(예를 들면, IP v6)은 AH 및 ESP가 규격화된 형태로 인터넷 상에서 사용되도록 허용하고 있지만, 이들은 현재의 인터넷 상에서 실질적으로는 사용불가능한 것으로 생각된다.

발명이 이루고자 하는 기술적 과제

<52> 본 발명은 데이터 전송기들로부터 데이터 수신기들로의 데이터 전송에 있어서, 보다 더 안전하고 확실한 데이터 전송 제어 방법 및 데이터 전송 시스템을 제공한다.

<53> 본 발명의 일실시예에 따르면, 데이터 전송 수단에 의해 암호화된 데이터를 데이터 전송 수단으로부터 데이터 수신 수단에의 데이터 전송을 위해 제공된 제 1 통신 채널을 통하여 데이터 수신 수단에 전송하는 단계와, 암호화된 데이터가 적어도 제 2 통신 채널을 통하여 특정한 데이터 수신 수단에 의해서만 수신되도록 제한 데이터 전송 제어 정보를 데이터 수신 수단에 전송하는 단계를 포함하는 데이터 전송 제어 방법이 제공되고, 제 2 통신 채널은 제 1 통신 채널보다 더 적은 데이터 전송 용량을 가지며, 또한 데이터 수신 수단으로부터 데이터 전송 수단으로의 데이터 전송에 사용된다.

<54> 데이터 전송 제어 방법에 의하면, 데이터 전송 수단은 제 1 통신 채널을 통하여 데이터 수신 수단으로 데이터를 전송한다. 제한 데이터 전송 제어 정보는 데이터 전송 수단과 데이터 수신 수단 사이에서 적어도 제 2 통신 채널을 통하여 교환될 수도 있다.

위의 본 발명의 데이터 전송 방법에 의해, 데이터 전송 수단은 제 1 통신 채널 및 제 2 통신 채널을 통하여 데이터 수신 수단으로 제한 데이터 전송 제어 정보를 포함하는 데이터를 전송할 수 있다. 제 2 통신 채널을 통하여, 데이터 전송 수단과 특정한 데이터 수신 수단 사이의 데이터 교환에 대한 정보가 이들 사이에서 전송될 수도 있다.

<55> 예를 들면, 위의 본 발명의 방법은 데이터 전송 수단으로 하여금 특정한 데이터 수신 수단으로 전송된 데이터가 정확하게 수신되었는지 아는 것을 허용한다.

<56> 본 발명의 다른 실시예에 따르면, 데이터 전송 수단으로부터 데이터 수신 수단에의 데이터 전송에 사용된 제 1 통신 채널과; 데이터 전송 수단과 데이터 수신 수단 사이의 양방향 통신을 가능하게 하는 제 2 통신 채널을 포함하고; 제 1 통신 채널은 데이터 전송 수단으로부터 데이터 수신 수단으로 암호화된 데이터를 전송하는데 사용되고; 적어도 제 2 통신 채널은 데이터 전송 수단으로부터의 암호화된 데이터가 특정한 데이터 수신 수단에 의해서만 수신되도록 하는 제한 데이터 전송 제어 정보를 전송하는데 사용되는 데이터 전송 시스템이 제공된다.

<57> 구조의 데이터 전송 시스템에서, 데이터 전송 수단은 제 1 통신 채널을 통하여 데이터 수신 수단으로 데이터를 전송한다. 제한 데이터 전송 제어 정보는 데이터 전송 수단과 데이터 수신 수단 사이의 제 2 통신 채널을 통하여 교환되고, 제 2 통신 채널은 적어도 데이터 전송 수단으로부터 데이터 수신 수단에의 데이터 전송에 사용되며, 제 1 통신 채널보다 적은 데이터 전송 용량을 가진다.

<58> 본 발명의 데이터 전송 시스템에서, 데이터 전송 수단은 제한 데이터 전송 제어 정보를 포함하는 데이터를 제 1 및 제 2 통신 채널을 통하여 데이터 수신 수단에 전송할 수 있다. 제 2 통신 채널 상에서, 데이터 전송 수단과 특정한 데이터 수신 수단 사이의 데이터 교환에 대한 정보는 이들 사이에서 전송될 수도 있다.

<59> 예를 들어, 위의 본 발명의 시스템은 데이터 전송 수단으로 하여금 특정한 데이터 수신 수단으로 전송된 정보가 정확히 수신되었는지 아는 것을 허용한다.

<60> 본 발명의 다른 특징에 따라 복수의 프로토콜들에 따라서 데이터 전송 수단으로부터 데이터 수신 수단에 전송되는 데이터를 다중 방식으로 전송되도록 캡슐화하는 단계와; 캡슐화에 의한 데이터 캡슐들 중 적어도 하나를 암호화하는 단계를 포함하는 데이터 전송 제어 방법이 제공된다.

<61> 데이터 전송 제어 방법을 이용하면, 데이터 전송 수단으로부터 데이터 수신 수단에 전송되는 데이터가 복수의 프로토콜들에 맞추어 다중 방식으로 캡슐화된다.

<62> 위의 본 발명의 방법은, 데이터가 관련된 프로토콜 요청들과 함께 그대로 유지되어 전송되는 것을 허용한다. 이것은 데이터가 특정 프로토콜과 호환성을 가지면서 전송될 수도 있다는 것을 의미한다. 문제의 데이터를 저장하기 위한 공간을 확보하기 위해 프로토콜에 맞추어 데이터가 캡슐화되는 경우, 다양한 종류의 정보를 수용하는 데이터 공간이 제공된다. 캡슐화된 데이터를 암호화하면 한층 더 안전해진다.

<63> 예를 들면, 특정한 데이터를 수용할 수 있는 프로토콜에 따라서 데이터가 캡슐화될 수 있다. 캡슐화 프로세스는 목적지 어드레스들에 대한 암호화 키들과 같은 정보를 저장할 수 있는 충분한 공간을 제공한다. 목적지 어드레스 정보는 어드레스 정보가 PID 부분 및 스크램블 제어부에 기록되는 종래의 TS 패킷 기법에 비해서 상당히 증가된다. 이는 PID 부분을 확장할 필요를 없앤다.

<64> 또한, 각각의 애플리케이션이 자체 제어 방법이 제공될 필요가 없게 된다. 이것은 새롭게 도입된 애플리케이션들이 본 발명에 의해 신속히 처리될 수 있음을 의미한다. 또한, 인증 헤더(authentication header; AH) 및 캡슐화 보안 페이로드(encapsulating security payload; ESP)가 현재의 인터넷 상에서 사용될 수 있다.

<65> 본 발명의 다른 특징에 따르면, 암호화 키를 사용하여 데이터를 암호화하는 단계와; 암호화된 데이터에 문제의 데이터를 암호화하는데 사용된 암호화 키에 대한 암호화 키 정보를 부가하는 단계와; 암호화 키 정보와 함께 암호화된 데이터를 데이터 전송 수단으로부터 데이터 수신 수단에 전송하는 단계와; 데이터 수신 수단이 암호화된 데이터를 복호화하도록 하고 빈번히 갱신되는 복수의 복호화 키들 중 하나의 복호화 키를 이용하여 암호화된 데이터를 복호화하고, 상기 복호화 키들 중 하나는 암호화된 데이터에 부가된 암호화 키 정보에 따라서 선택되는 데이터 전송 제어 방법이 제공된다.

<66> 위의 본 발명의 방법에 의해, 암호화 키를 이용하여 데이터 암호화 단계에서 암호화된 데이터는 문제의 데이터를 암호화하는데 사용된 암호화 키에 대한 암호화 키 정보를 사용한다. 데이터 전송 단계에서, 암호화된 데이터는 데이터 전송 수단으로부터 데이터 수신 수단으로 암호화 키 정보와 함께 전송된다. 데이터 복호 단계에서, 암호화된 데이터는 데이터 수신 수단으로 하여금 암호화된 데이터를 복호화하는 것을 허용하고 빈번히 갱신되는 복수의 복호화 키들 중 하나의 키를 이용하여 복호되고, 복호화 키들 중 하나의 키는 암호화된 데이터에 부가된 암호화 키 정보에 따라서 선택된다.

<67> 위의 데이터 전송 제어 방법에 의해, 데이터 전송 수단은 암호화 키를 사용하여 데이터를 암호화한다. 데이터 수신 수단은 빈번히 갱신되는 복수의 복호화 키들 중 한 키를 이용하여 수신된 암호화된 데이터를 복호화한다. 하나의 복호화 키는 암호화된 데이터와 함께 전송된 암호화 키 정보에 기초하여 데이터 수신 수단에 의해 복수의 암호화 키들 가운데서 선택된다.

<68> 본 발명의 다른 목적들, 특징들 및 이점들은 첨부된 도면을 참조하여 보다 명확히 설명한다.

발명의 구성 및 작용

<69> 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예들을 상세히 기술할 것이다. 본 발명을 구현하는 하기의 데이터 전송 시스템은 데이터 전송기에 의해 위성 링크들을 통하여 전송된 데이터의 수신을 특정한 데이터 수신기로 한정하는 시스템이다.

<70> 도 6에 도시된 바와 같이, 본 발명의 데이터 전송 시스템은 데이터 전송기(2)로부터 위성 링크들(4a), 통신 채널 역할을 하는 전용선들(7) 및 전화선들(8), 양방향 통신 채널(9)을 통하여 데이터 수신기(3a, 3b, 3c)로의 데이터 전송을 제어한다. 시스템에서, 데이터 전송기(2)는 데이터를 암호화하여 이 암호화된 데이터를 통신 채널들을 통하여 데이터 수신기들(3a, 3b, 3c)로 전송한다.

<71> 데이터 전송 시스템(1)은 통신 위성(4)을 이용하여 데이터 전송기(2)로 하여금 데이터를 데이터 수신기(3a, 3b, 3c)로 전송하는 것을 허용하는 제 1 통신 채널로서의 역할을 하는 통신 채널(4a); 및 한쪽의 데이터 전송기(2)와 다른 쪽의 데이터 수신기들(3a, 3b, 3c) 사이에서 양방향 통신을 제공하는 제 2 통신 채널 역할을 하는 전용선(7), 전화선(8) 및 양방향 통신 채널(9)을 포함한다. 데이터 전송 시스템(1)은 데이터 전송기(2)로부터 데이터 수신기(3a, 3b, 3c)로 암호화된 데이터를 전송하기 위한 제 1 통신 채널을 사용하며, 데이터 전송기로부터 데이터 수신기들로 제한 데이터 전송 제어 정보를 전송하기 위한 제 2 통신 채널을 채용한다. 데이터 전송 시스템(1)은 인터넷에 접속된다.

<72> 제한 데이터 전송 제어 정보는 특정한 데이터 수신기 또는 수신기들로 하여금 데이터 전송기(2)로부터 전송된 데이터를 수신하는 것을 허용한다. 바꾸어 말하면, 제한 데이터 전송 제어 정보는 특정한 데이터 수신기 또는 수신기들이 소정의 전송된 관심 데이터를 수신하도록 인증한다.

<73> 전술한 통신 채널들을 이용하여, 데이터 전송기(2)는 다양한 데이터를 데이터 수신기(3a, 3b, 3c)로 전송한다. 데이터 수신기(3a, 3b, 3c)는 통신 채널들을 통하여 들어오는 데이터를 수신한다. 도 6에서는 단지 세 개의 데이터 수신기(3a, 3b, 3c)만 도시하였지만, 데이터 전송 시스템(1)은 실제로는 수백 내지 수십만개의 데이터 수

신기들을 포함할 수도 있다.

<74> 다음은 데이터 전송기(2)와 데이터 수신기(3a, 3b, 3c)(이하, 각각의 데이터 수신기(3a, 3b, 3c)를 서로 구별할 필요가 없으면 데이터 수신기(3)이라 한다) 사이의 데이터 교환들을 허용하는 통신 채널들에 대하여 설명한다.

<75> 위성 링크(4a)는 대역폭이 약 30Mbps인 Ku 대역 상의 단방향 회로이다. 위성 링크(4a)는 데이터 전송기(2)로 하여금 데이터를 예를 들어, 일본 전역에 걸쳐있는 데이터 전송기들로 동시에 전송하는 것을 허용한다.

<76> 양방향 통신 채널(9)은 데이터 전송기(2)와 데이터 수신기(3) 사이에 위성 링크(4a)와 무관하게 설치된다. 이들의 이름이 암시하는 바와 같이, 양방향 통신 채널(9)은 데이터 전송기(2)와 데이터 수신기(3) 사이에 양방향 통신을 가능하게 한다. 그리하여, 양방향 통신 채널(9)은 이하 인터넷 상에서의 통신에 사용하기 위한 범용 통신 채널들이라고 가정한다.

<77> 전용선(7)은 데이터 전송기(2)를 데이터 수신기(3)와 직접 연결하는 통신 수단이다.

<78> 인터넷(6)은 영상 및 음성 정보와 같은 다양한 종류의 정보를 제공한다. 인터넷 서비스 제공자(5)는 데이터 수신기(3)를 인터넷과 통신하도록 한다. 데이터 전송기(2)는 인터넷(6)에 접속된다고 가정한다.

<79> 데이터 전송기(2)와 데이터 수신기(3) 사이의 데이터 교환을 가능하게 하는 전용선(7), 전화선(8) 및 양방향 통신 채널(9)은 위성 링크(4a)보다 더 작은 대역 용량을 가진다. 일반적으로, 라인(7, 8, 9)은 수 Kbps로부터 수백 Kbps에 달하는 대역폭을 제공한다.

<80> 데이터 전송 시스템(1)은 또한 단지 특정한 데이터 수신기 또는 수신기들만 관심 데이터를 수신하도록 허용하는 제한 데이터 수신 시스템으로 구성된다. 따라서, 데이터 전송 시스템(1)은 데이터를 예를 들어, 데이터 수신기(3a)로만(유니캐스트형 데이터 분배) 전송하거나 데이터 수신기들(3a 및 3b)(멀티캐스트 데이터형 분배)로만 전송하거나 또는 모든 수신기들(3a, 3b, 3c)(방송 데이터형 분배)로 전송할 수 있다.

<81> 데이터 전송 시스템(1)에서, 데이터 전송기(2)는 데이터를 다음과 같이 데이터 수신기(3)로 전송한다. 즉, 데이터 전송기(2)로부터 데이터 수신기(3)로 전송될 데이터는 도 7a 내지 7g에 도시된 바와 같이 캡슐화된다. 캡슐화는 관심 데이터를 전송하는 데이터 전송기(2)에 의해 수행된다. 제 1 캡슐화 단계에서, 데이터 수신기(3)로 전송될 데이터는 제 1 프로토콜에 따라서 캡슐화된다. 제 2 캡슐화단계에서, 제 1 프로토콜에서 캡슐화된 데이터는 제 2 프로토콜에 따라서 또한 캡슐화된다. 캡슐화 프로세스는 처리되지 않은 데이터를 주어진 통신 프로토콜에 의해 규정된 전송 포맷에 기초하여 형성된 캡슐들(즉, 패킷들 또는 프레임들)로 주입하는 프로세스를 포함한다. 데이터를 이러한 캡슐들에 위치시켜서, 이들의 전송이 제어가능하게 된다.

<82> 제 1 캡슐화 단계에서, 데이터 수신기(3)로 전송될 전체 타겟 데이터를 문제의 실제 데이터부와 관련된 부가 정보부를 갖는 실제 데이터부 내로 위치시킴으로써 캡슐이 형성된다. 캡슐내 실제 데이터는 암호화된다. 이하 제 1 캡슐화 단계를 보다 상세히 설명한다.

<83> IP(인터넷 프로토콜) 데이터그램(101)은 도 7a에 도시된 바와 같이 인터넷 프로토콜에 기초한 데이터로 구성된다. IP 데이터그램(101)의 데이터는 데이터 전송기(2)로 전송된다. IP 데이터그램의 헤더는 예를 들면, 인터넷 상의 데이터그램의 목적지를 나타내는 목적지 어드레스를 포함한다.

<84> IP 데이터그램(101)은 인터넷 프로토콜에 기초하여서만 구성되는 것은 아니며, 이더넷 프로토콜에 따라서 구성될 수도 있다.

<85> 도 7b 내지 7d에서, 데이터 전송기(2)는 전술한 제 1 프로토콜에 따라서 데이터를 캡슐화한다. 예를 들면, DVB(Digital Video Broadcasting)를 위한 멀티 프로토콜 캡슐화가 제 1 프로토콜로 채용될 수도 있다.

<86> 도 7b에 도시된 바와 같이, 데이터 전송기(2)는 먼저 IP 데이터그램을 패딩함으로써(즉, 패딩부(102)를 추가) 제 1 프로토콜에 따라서 데이터 캡슐화를 수행하여 데이터부의 길이를 64 비트의 정수배로 한다. 예를 들면, 0 내지 63 비트의 패딩부가 IP 데이터그램(101)의 끝에 추가된다. 패딩부의 모든 비트는 각각 1이다. 패딩은, 데이터부의 길이가 64 비트의 정수배인 경우에 데이터부가 캡슐화에 보다 적합하기 때문에, 데이터그램을 미리 결정된 데이터 길이로 유지하기 위한 것이다. 제 1 프로토콜의 포맷에 위치한 데이터부는 이하 섹션이라 한다.

<87> 패딩(102)으로 보충된 섹션은 도 7c에 도시된 바와 같이 데이터 전송기(2)에 의해 암호화된다. 암호화는 암호화 키들을 이용하여 수행된다. 암호화 키들은 데이터 수신기(3)로 전송될 정보를 암호화하는데 사용되는 세션 키들(하기에 설명됨)이다. 여기서 적응된 암호화 방법은 트리플 DES와 같은 공통키 암호법(common key criptosystem)에 기초한 블록 암호화 방법이다. 트리플 DES 암호화는 현재 가장 강력한 공용키 암호법들

(public key criptosystems) 중 하나로서, 하드웨어 상에서 고속 암호화를 실현하기 쉽다. 암호화 프로세스는 대부분의 공용키 암호법들의 프로세스와는 달리, 30 Mbps 정도의 고속 전송률들을 갖는다.

<88> 도 7d에 나타낸 바와 같이, 데이터 전송기(2)는 암호화된 섹션 데이터부(104)에 섹션 헤더(103) 및 에러 검출을 위한 테일러(tailer; 105)를 보충한다.

<89> 암호화된 섹션 데이터부(104)는 MAC(Media Access Control) 프레임 구조를 채용한다. MAC 프레임 구성 프로세스에서, MAC 헤더가 데이터부에 부가된다. MAC 헤더를 참조하는 것은 프레임 내에 위치된 데이터의 목적지에 대한 제어를 용이하게 한다. 구체적으로, MAC 프레임은 프레임 내에 저장된 데이터의 수신이 허가되는 데이터 수신기의 목적지 어드레스를 수용한다.

<90> 섹션 헤더(103)는 48 비트 목적지 어드레스를 수용할 수 있을 만큼의 데이터 공간을 제공한다. 보다 구체적으로, 섹션 헤더(103)는 목적지 어드레스를 포함하도록 형성된 MAC 헤더를 가진다. 섹션 헤더(103) 내에 48 비트의 목적지 어드레스를 수용하는 데이터 공간의 제공은, 전술한 첫 번째 문제점, 즉, 데이터 수신기의 수적 제한 문제를 해결할 수 있다. 왜냐하면, 확장된 어드레스 공간이 암호화 키들을 식별하는 많은 정보를 수용하기 때문이다. 또한, 인터넷 프로토콜과의 약한 관련성에 대한 전술한 네 번째 문제점을 해결할 수 있고 이는 데이터그램 전송시에 IP 목적지 어드레스에 대한 IP 데이터그램(101)의 패킷 ID(하기에 설명됨)를 조정할 필요가 없기 때문이다.

<91> 테일러(105)는 CRC(Cyclic Redundancy Checking)에 따라 부호화된다. CRC는 MAC 프레임 내에 데이터를 수신하는 데이터 수신기(3)가 프레임이 위성 링크들을 통하여 정상적으로 전송되었는지를 확인하도록 설계된다. 예를 들면, CRC는 32비트로 부호화되어 있다.

<92> 지금까지 제 1 프로토콜에 따라서 전송될 데이터를 캡슐화하는 것에 대해 설명하였다. 다음은 제 1 프로토콜에 따라서 캡슐화된 데이터가 제 2 크로토콜에 따라서 캡슐화되는 방법에 대하여 설명한다.

<93> 제 2 프로토콜에 기초한 데이터 캡슐화는 제 1 프로토콜에 따라서 캡슐화된 데이터를 복수의 패킷들로 분할하는 단계를 포함한다. 제 2 프로토콜은 데이터의 캡슐화를 MPEG2(Moving Picture Experts Group Phase 2)에 기초한 TS(Transport Stream) 패킷들로 규정하는 프로토콜이다. TS 패킷들은 음성 및 영상 신호들 및 다른 데이터와 같은 다양한 종류의 데이터로 하여금 다중화되어 대용량 디지털 라인들을 통하여 전송되도록 허용한다. 제 2 프로토콜에 따르면, 데이터는 도 7e 내지 7g에 도시한 바와 같이 복수의 TS 패킷들(106, 107, 108)로 캡슐화된다. TS 패킷들(106, 107, 108)은 각각 TS 헤더(HTS) 및 TS 페이로드부(P)로 구성된다. TS 페이로드부(P)는 제 1 프로토콜에 따라서 분할되어 캡슐화된 데이터를 포함한다. 각 TS 패킷의 TS 헤더(HTS)는 도 4에 도시된 바와 같이 패킷 ID(PID) 부분과 스크램블 제어부를 포함한다. 통상적으로, 목적지 어드레스는 PID 부분 및 스크램블 제어부에 기록된다는 사실이 목적지 어드레스 정보의 범위를 한정하였다. 본 실시예에서는 목적지 어드레스가 섹션 헤더(103)에 기록되기 때문에 단점이 제거된다.

<94> 이상 제 2 프로토콜에 따른 데이터 캡슐화를 설명하였다. 전술한 바와 같이, 데이터 전송기(2)는 데이터를 캡슐화하여 제 1 및 제 2 프로토콜에 따라서 다중 방식으로 데이터 수신기(3)(IP 데이터그램)로 전송한다. 캡슐화된 데이터는 통신 위성(4)으로 진행한다.

<95> 제한 데이터 전송 제어는 두 레벨들, 즉, TS 패킷 레벨 및 섹션 레벨에서 개별적으로 이루어지기 때문에, 전술한 두 번째, 다섯 번째 및 여섯 번째 문제점이 해결된다.

<96> 보다 구체적으로, 두 번째 문제점, 즉, 사용중인 PID의 수가 증가함에 따른 전송 비용 증대의 문제점을 회피하면서, 많은 양의 정보가 암호화 키에 의해서 안전하게 될 수 있다.

<97> 다섯 번째 문제점, 즉, 각 애플리케이션이 스스로의 제어 방법을 가져야 하는 문제점이 더 이상 적용되지 않는다. 새롭게 도입된 애플리케이션들은 본 실시예에 의해 신속히 처리된다.

<98> 여섯 번째 문제점도 또한 본 실시예에 의해 해결된다. 즉, 인증 헤더(AH) 및 캡슐화 보안 페이로드(ESP)를 현재의 인터넷 상에서 사용할 수 있다.

<99> 전술한 IP 데이터그램의 캡슐화는 데이터그램이 위성 링크(4a)를 통하여 데이터 수신기(3)로 전송될 때 적용된다. 양방향 통신 채널(9)을 통하여, 특정화된 캡슐화없이 인터넷의 통상적인 프로세스들이 IP 데이터그램을 전송하는데 사용된다.

<100> 다음은 암호화 키를 이용하여 데이터가 데이터 전송기(2)에 의해 암호화되는 방법과, 암호화 키들을 이용하여

(복호화 키들을 이용하여) 데이터 수신기(3)에 의해 암호화된 데이터가 복호되는 방법을 설명한다. 도 8에 도시된 바와 같이 구성된 데이터 전송기(2) 및 데이터 수신기(3)는 도 6에 도시된 통신 채널을 통하여 상호접속된다. 데이터 전송기(2)는 (섹션을 사용하여) 제 1 프로토콜에 따라서 데이터를 데이터 수신기(3)로 전송한다. (TS 패킷을 사용하여) 제 2 프로토콜에 따른 데이터 전송은 위에서 도 5의 종래의 구성을 참조하여 설명하였다. 도 8의 본 발명의 장치와 도 5의 종래의 장치를 비교하여 보면, 실시예는 데이터 전송기 및 데이터 수신기에 의한 암호화 및 복호화를 위해 두 개의 키 레벨들, 즉, 세션 키(Ks)(24) 및 마스터 키(Km)(25) 상에서 동작하는 반면에, 종래의 구성은 세 개의 키 레벨 기법에 의존한다는 것을 알 수 있다. 본 실시예에 의하면 하나의 키 레벨을 절감할 수 있다.

<101> 세션 키(Ks)(24)는 공통키 암호 시스템 하에서 데이터 암호화 및 복호를 위한 데이터 전송기(2) 및 수신기(3)에 의해 포함된다. 구별을 위해, 데이터 수신기(3)에 포함된 세션 키(Ks)는 하기에 세션 키(Ks)(34)라 지칭한다.

<102> 세션 키(Ks)(24)를 사용하면, 데이터 전송기(2)는 특정한 데이터 수신기 또는 수신기들로 전송될 데이터를 암호화한다. 데이터 수신기(3)는 세션 키(Ks)(34)를 이용하여 수신된 암호화된 데이터를 복호화하고, 이에 따라 복호된 데이터로부터 중요한 정보를 추출한다.

<103> 세션 키(Ks)(24 및 34)는 규칙적인 간격, 예를 들면, 매일, 매시간 또는 매분마다 갱신된다. 도청자들이 소정 시간에 세션 키(Ks)(24)를 알게되더라도, 이들은 그 데이터를 키에 의해 인증된 제한된 시간 동안만 도청할 수 있다. 세션 키들을 갱신하는 것에 대해서는 하기에 보다 상세히 설명한다.

<104> 세션 키(Ks)(24)는 전술한 트리플 DES에 따라서 도 7c에 도시된 섹션 데이터부를 암호화하는데 사용된다.

<105> 섹션 키(Ks)(24)와 같이, 마스터 키(Km)(25)는 데이터 전송기(2) 및 데이터 수신기(3) 모두에 포함된다. 각각의 데이터 수신기(3A, 3B, 3C)는 그것의 고유한 마스터 키에 할당된다. 편의상, 데이터 수신기(3)에 포함된 마스터 키(Km)는 이하 마스터 키(Km)(35)라 지칭한다.

<106> 마스터 키(Ks)(25)는 데이터 전송기(2)와 데이터 수신기(3) 사이에서 전송되지 않는다. 어떠한 마스터 키도 통신 채널들 상에 제공되는 경우는 없다. 마스터 키는 그 사용자를 제외하고는 어떠한 수단에 의해서도 누구도 알 수 없다.

<107> 마스터 키(Km)는 세션 키(Ks)를 데이터 수신기(3)로 전송하기 전에 암호화하기 위해 데이터 전송기(2)에 의해 사용되고, 수신된 암호화된 세션 키(Ks)를 복호화하기 위해 데이터 수신기에 의해 사용된다. 보다 구체적으로, 데이터 전송기(2)는 마스터 키(Km)(25)를 이용하여 세션 키(Ks)(24)를 암호화하고, 암호화된 세션 키(Ks)(24)를 데이터 수신기(3)로 미리 전송한다. 암호화된 세션 키(Ks)(24)를 수신하면, 데이터 수신기(3)는 마스터 키(Km)를 이용하여 (세션 키(Ks)(34)를 추출하기 위해) 수신된 키를 복호화한다.

<108> 그 다음에 세션 키(Ks)는 마스터 키(Km)에 기초하여 암호화 및 복호를 거치며, 데이터 전송기(2)로부터 데이터 수신기(3)로의 전송 프로세스 동안 도청자들에 의한 도청으로부터 보호된다.

<109> 복호된 세션 키(Ks)를 이용하여, 데이터 수신기(3)는 문제의 세션 키(Ks)를 사용하여 암호화된 전송된 데이터를 복호화한다. 데이터 수신기(3)는 복호된 데이터로부터 의미있는 정보를 추출한다.

<110> 세션 키(Ks)는 트리플 DES에 따라서 마스터 키(Km)를 이용하여 암호화되고 복호된다. 대안적으로, 공용 암호 시스템이 채용될 수도 있다. 대안적인 시스템은 데이터의 암호화 및 복호화 프로세스들과는 다른 시스템에 의한 키들이 고속으로 수행될 필요가 없으며 이들이 또한 보안을 보장한다는 점에 있어서 이점을 가진다.

<111> 세션 키(Ks)(24)와는 달리 마스터 키(Km)(25)는 시간에 따라서 갱신되지 않는다.

<112> 이하, 세션 키(Ks)(24)가 갱신되는 방법을 설명한다. 세션 키(Ks)(24)를 갱신하는데 있어서는 데이터 전송기(2)가 능동적으로 사용된다. 마스터 키(Km)(25)를 이용하여 암호화된 세션 키(Ks)(24)(하기에는 암호화된 세션 키(Km(Ks))라 함)는 또한 데이터 전송기(2)에 의해 능동적으로 전송된다.

<113> 양방향 통신 채널들(9)을 이용하면, 데이터 수신기(3)는 세션 키(Ks)를 능동적으로 요청할 수 있다. 이런 방식으로, 각각의 데이터 수신기(3a, 3b, 3c)는 데이터 전송기(2)로부터 빠르고 확실하게 필요로 되는 세션 키들을 획득할 수 있다. 예를 들면, 새로운 데이터 수신기(3)가 데이터 전송 시스템(1)에 부가되는 경우, 장해에 의해 서비스를 받을 수 없는 데이터 수신기(3)가 장해로부터 회복되어 시스템(1)에 재접속되는 경우, 또는 데이터 수신기(3)가 세션 키(Ks)를 정확히 수신하지 못하는 경우, 데이터 수신기에 의해 키에 대한 능동적인 요청를 통하여 빠르고 확실한 세션 키(Ks)(24) 획득이 가능하다. 장해로부터의 회복 및 세션 키(Ks)의 갱신은 데이터 전송

기(2) 및 데이터 수신기(3)에 각각 결합된 CA(Conditional Access) 관리 유닛들(23 및 33)에 의해 관리된다. 두 유닛(23 및 33)은 서로 통신하여 이들 간에 제어 정보를 교환한다.

<114> 특징에 의해, 전술한 세 번째 문제점, 즉, 통신 채널들로서 위성 링크들에만 의존하는 데이터 전송 시스템에서, 정보가 정확히 목적지 데이터 수신기로 전송되었는지를 데이터 전송기가 알 수 없다는 문제점을 극복할 수 있다.

<115> 데이터 전송기(2)는 세션 키(Ks)를 단방향 위성 링크(4a) 또는 양방향 통신 채널(9)을 통하여 데이터 수신기(3)로 전송할 수도 있다.

<116> 세션 키(Ks)는 도 9에 도시된 흐름도를 구성하는 단계에서 갱신된다.

<117> 시간 상 주어진 시점에서, 데이터 수신기(3)는 두 개의 세션 키(Ks)(34), 즉, 세션 키(Ks_even) 및 세션 키(Ks_odd)를 갖는다. 데이터 수신기(3)는 데이터 전송기(2)로부터 전송된 정보 및 데이터를 복호화하는데 두 개의 세션 키들(Ks_even 및 Ks_odd) 중 하나의 키를 사용한다.

<118> 현재 사용되고 있는 두 개의 세션 키들(Ks) 중 어느 하나는 도 7d에 도시된 섹션 헤더(103)에 기록된 정보에 의해 식별된다. 예를 들면, 도 10에 도시된 바와 같이, 섹션 헤더(103)는 표 ID(table_id), MAC 어드레스부(MAC_address_1, MAC_address_2, MAC_address_3, MAC_address_4, MAC_address_5, MAC_address_6), 섹션 정보부(section_length, section_number, last_section_number), ssi(section_syntax_indicator), pi(private_indicator), rsvd(reserved), psc(payload_scramble_indicator)(111), asc(address_scramble_indicator), LSf(LLC_SNAP_flag), cni(current_next_indicator)을 포함한다. psc(111)는 두 개의 세션 키들(Ks) 중 어느 키가 현재 사용중인지를 나타낸다. psc(111)는 2 비트 정보로 이루어진다. 만약 psc의 상위 비트가 "0"이면, 이것은 세션 키(Ks_even)가 사용됨을 의미하고, 만약 psc의 상위 비트가 "1"이면, 이것은 세션 키(Ks_odd)가 현재 사용중임을 의미한다.

<119> 도 9의 단계 S1에서, 세션 키(Ks) 중 어느 키가 현재 사용되는지 검사된다. 단계 S2에서, 데이터 수신기(3)는 타이머에 의해 트리거되어 세션 키 갱신 프로세스를 개시한다.

<120> 단계 S3에서, 데이터 수신기(3)는 MAC 어드레스들이 세션 키(Ks)와 대응하여 포함되어 있는 대응표에서 찾아낸 현재의 세션 키(Ks)의 플래그를 갱신한다. 데이터 수신기(3)는 도 11에 도시되어 있는 바와 같은 MAC 어드레스와 세션 키 대응표를 갖는다. 현재 사용된 세션 키(Ks) 내의 플래그는 표에 대하여 갱신된다. 갱신 동작은 psc(111)의 상위 비트를 "0"으로 반전시킨다(invert).

<121> 단계 S4에서, 데이터 수신기(3)는 psc(111)에 기초하여 섹션에 포함된 IP 데이터그램을 복호화한다. 보다 구체적으로, psc 상위 비트가 "0"으로 설정되면, 데이터 수신기(3)는 현재의 세션 키(Ks_odd)(psc의 상위 비트가 "1"인 경우에 사용됨)의 사용을 중지하고, 복호를 위해 세션 키(Ks_even)로 전환한다. psc의 상위 비트가 "1"로 설정되면, 데이터 수신기(3)는 현재의 세션 키(Ks_even)(psc 상위 비트가 "0"인 경우에 사용됨)의 이용을 중단하고 복호를 위해 세션 키(Ks_odd)로 전환한다. 단계 S5에서 세션 키(Ks)가 새로 변경되기 전에, 데이터 전송기(2)는 마스터 키(Km)(24)를 이용하여 다음 세션 키(Ks)를 암호화하여 암호화된 키를 데이터 수신기(3)로 전송한다.

<122> 암호화된 세션 키(Km)(Ks)는 위성 링크(4a) 또는 양방향 통신 채널(9)을 통하여 전송된다. 전송에 이용된 프로토콜은 TCP/IP(Trasmission Control Protocol/Internet Protocol)와 같은 응답(acknowledgments)을 필요로 하는 프로토콜일 수 있다. 프로토콜에 의해 세션 키(Ks)는 데이터 전송기(2)로부터 데이터 수신기(3)로 확실히 전송될 수 있다.

<123> 단계 S6에서 세션 키 전송이 행해지고 있는 동안, 데이터 수신기(3)는 도 11에 도시된 MAC 어드레스와 세션 키 대응표를 갱신한다. 즉, 현재 사용된 세션 키(Ks)는 다음 세션 키(Ks)로 치환된다.

<124> 단계 S7에서, 데이터 수신기(3)는 다음 세션 키(Ks)가 현재 데이터 수신기(3)에 포함되어 있는지 확인한다. 단계 S8에서, 데이터 수신기(3)는 다음 세션 키(Ks)로 전환한다. 단계 S8 내지 S13은 psc의 상위 비트가 "1"로 설정되어 세션 키(Ks_odd)가 복호에 사용되는 프로세스를 구성한다. 이 프로세스는 단계 S7로부터 시작되거나, 데이터 수신기(3)가 현재의 세션 키(Ks)를 세션 키(Ks_even)(psc의 상위 비트: 0)라고 판단하면 단계 S1로부터 시작된다.

<125> 단계들을 수행함으로써, 데이터 전송기(2)는 데이터 수신기(3)에 확실하게 갱신되는 세션 키(Ks)를 제공한다. 데이터 수신기(3)는 두 개의 세션 키들(Ks)을 동시에 전환하므로 현재 유효한 세션 키(Ks)에 기초한 데이터 복

호가 중지되지 않는다. 세션 키(Ks)(24)의 갱신 빈도는 전송 처리 기간에 따라서 유연하게 변할 수도 있다. 세션 키(Ks)는 전술한 바와 같이 데이터 수신기 내에서 규칙적으로 갱신된다. 이렇게 갱신된 세션 키(Ks)를 사용하여, 데이터 수신기(3)는 키와 함께 전송된 정보 및 데이터를 복호화한다.

<126> 데이터를 전송하기 전에 데이터 전송기(2)에 의해 행해지는 단계들 및 데이터를 수신한 후에 데이터 수신기(3)에 의해 행해지는 단계들을 하기에 설명한다. 데이터 전송기(2)가 데이터를 전송하기 전에 수행하는 단계들은 도 12의 흐름도에 예시적으로 도시되어 있다. 데이터 수신시 데이터 수신기(3)에 의해 행해지는 단계들은 도 14의 흐름도에 예시적으로 도시되어 있다.

<127> 도 12의 단계(S21)에서, 데이터 전송기(2)는 전송기(2) 그 자체 또는 양방향 통신 채널(9)에 접속되어 있는 인터페이스로부터 데이터 수신기(3)로 전송될 IP 데이터그램을 수신한다. 데이터 전송기(2)는 또한 인터넷(6)으로부터의 액세스 정보에 기초하여 정보 센터로부터 정보를 수신한다.

<128> 단계 S22에서, 데이터 전송기(2)는 제 1 프로토콜에 기초한 목적지 어드레스를 알기 위해 IP 데이터그램의 목적지 어드레스부를 검사한다. 예를 들면, 데이터 전송기(2)는 도 13에 도시된 것과 같이 데이터 전송기(2)에 포함되어 있는 IP 어드레스와 MAC 어드레스 대응표를 참조하여 제 1 프로토콜에 따라서 데이터 수신기(3)의 목적지 어드레스를 찾아낸다.

<129> 이렇게 찾아낸 목적지 어드레스를 이용하여, 데이터 전송기(2)는 목적지 어드레스에 따라서 섹션을 생성한다. 여기서, 데이터 전송기(2)는 필요한 경우 데이터부에 비트 "1" 패딩을 제공하여서, 데이터부는 64 비트의 배수가 된다.

<130> 단계 S23에서, 데이터 전송기(2)는 도 11에 도시된 MAC 어드레스와 세션 키 대응표에서 키(Ks)의 플래그(112)를 검사함으로써 현재 사용된 세션 키(Ks)를 추출한다. 데이터 전송기(2)는 추출된 세션 키(Ks)를 이용하여 도 7c에 도시된 섹션의 데이터부를 암호화한다. 여기서, 데이터 전송기(2)는 현재의 세션 키(Ks)의 플래그를 검사하여 그 플래그의 내용을 도 11에 도시된 세션 헤더의 psc(111)의 상위 비트로 설정한다.

<131> 단계 S24에서, 도 7e 내지 7g에 도시된 바와 같이, 데이터 전송기(2)는 전체 섹션(109)을 TS 패킷들(106, 107, 108)의 페이로드 부분들(P)로 분할한다. TS 패킷(106, 107, 108)에는 미리 정해진 PID가 각각 부가된다. 페이로드(P)는 위성 링크(4a)로 출력되기 전에 제 2 프로토콜에 의해 필요로 되는 바와 같이 암호화된다.

<132> 이상 데이터 전송기(2)의 데이터 전송 전의 준비 단계를 설명하였다. 위성 링크(4a)를 통하여 수신된 데이터를 갖는 데이터 수신기(3)는 하기의 단계들을 수행한다.

<133> 도 14의 단계 S31에서, 데이터 수신기(3)는 위성 링크들(4a)를 통하여 수신한 TS 패킷들(106, 107, 108)을 복호화하여 전체 섹션(109)을 재구성한다.

<134> 단계 S32에서, 데이터 수신기(3)는 섹션의 목적지 어드레스(즉, MAC 어드레스)를 추출한다. 단계 S33에서, 데이터 수신기(3)는 MAC 어드레스가 도 15에 도시된 MAC 어드에스와 세션 키 대응표에 있는지 검사한다. 즉, 섹션이 데이터 수신기(3)가 수신하도록 인증된 데이터를 포함하는지의 여부가 검사된다. MAC 어드레스가 단계 S33에서 발견되지 않으면, 데이터 수신기(3)는 단계 S34로 진행하여 데이터를 폐기한다. MAC 어드레스가 검출되면, 데이터 수신기(3)는 도 10에 도시된 psc(111)가 섹션 헤더(103)로부터 추출되는 단계 S35로 진행한다. 데이터 수신기(3)는 psc(111)의 상위 비트를 검사하여 두 개의 세션 키(Ks)중 어느 키가 현재 유효한지 파악하여, 유효한 세션 키(Ks)를 선택한다.

<135> 단계 S36에서, 데이터 수신기(3)는 트리플 DES에 따라서 검색된 세션키(Ks)를 이용하여 섹션 데이터(104)를 복호화한다. 단계 S37에서, 데이터 수신기(3)는 복호된 데이터로부터 IP 데이터그램을 추출한다. 예를 들면, 데이터 수신기(3)는 복호된 데이터부 앞에 놓인 IP 헤더로부터 총 길이 필드(113)(도 16)를 판독하고, 그 필드(113)로부터 IP 데이터그램의 길이를 찾아내어 그에 따라서 계산된 전체 IP 데이터그램을 추출한다. 프로세스에서, 암호화시에 부가된 과도한 패딩이 제거되어 타겟 IP 데이터그램이 그대로 추출된다.

<136> 전술한 단계들을 수행함으로써, 데이터 전송기(2)는 데이터 전송 전에 필요한 프로세스를 수행하고, 데이터 수신기(3)는 수신된 데이터와 관련된 절차들을 행한다. 따라서 데이터 수신기(3)는 그 수신기로 어드레스된 정보 및 데이터를 받아들인다.

<137> 전술한 바와 같이 구성된 데이터 전송 시스템(1)은 앞에서 언급한 종래의 문제점들을 해결할 수 있다.

<138> 다양한 데이터 전송 시스템(1)은 대안으로 만들어질 수 있다. 도 17은 시스템(1)의 제 1 변형인 데이터 전송

시스템(201)이다. 데이터 전송 시스템(201)은 데이터 수신기(3)가 IP 라우터를 구비하고 있다는 것을 특징으로 한다.

<139> 데이터 전송 시스템(1)은 IP 데이터그램을 직접 수신하는 데이터 수신기(3a)를 가진다. 반면에 데이터 전송 시스템(201)은 IP 라우터로서 구성된 데이터 수신기(3a)를 가진다. 이 구성에 의해 위성 링크(4a)로부터 데이터 수신기(3a)에 의해 수신된 데이터는 위성 링크(4a)와 인터페이스되지 않는 컴퓨터(203a 및 203b)로 전송될 수 있으며, 컴퓨터(203a 및 203b)는 이더넷과 같은 로컬 에리어 네트워크(LAN)(202)를 통하여 데이터 수신기(3a)에 접속된다. 이 경우, 데이터 전송기(2) 및 데이터 수신기(3a)는 데이터 수신기(3a)뿐만 아니라 데이터 수신기(3a)에 접속된 로컬 에리어 네트워크(202) 상에 있는 모든 컴퓨터(203a 및 203b)를 통하여 제한 데이터 수신 제어를 제공할 수 있다. 보다 구체적으로, 데이터 전송기(2)의 IP 어드레스들이 섹션 목적지 어드레스들(MAC 어드레스들)과 대응하도록 설정되는 도 13의 대응표 내에서, 각각의 IP 어드레스들은 복수의 IP 어드레스들의 세트를 각각 나타내는 IP 네트워크 어드레스들과 치환된다. 한 측의 데이터 수신기(3a)와 다른 측의 컴퓨터(203a 및 203b) 사이의 제한 데이터 전송 제어를 행하는 것은 IP 프로토콜 또는 상위 애플리케이션의 레벨에서의 제한 데이터 전송 제어 방법이 요구된다. 이것은 데이터 전송 시스템(201)에서의 데이터 전송이 위성 링크(4a)를 통하여서만 행해지기 때문이다.

<140> 시스템(1)의 제 2 변형인 데이터 전송 시스템(301)이 도 18에 도시되어 있다. 데이터 전송 시스템(301)에서, 데이터 수신기(3a)는 IP 데이터그램을 포워딩하는데 있어서 프로토콜 변환을 전적으로 행하는 브리지(bridge)로서 구성된다. 데이터 전송 시스템(301)은 시스템(301)이 라우팅을 행하지 않는다는 점에 있어서 시스템(201)과 상이하다.

<141> 데이터 수신기(3a)는 위성 링크(4a)를 통하여 수신한 데이터를 복호화하여 IP 데이터그램을 추출한다. 추출된 IP 데이터그램은 이더넷 프레임에 위치되어 범용 라우터(302)로 전송된다. 차례대로 라우터(302)는 IP 데이터그램에 대하여 일반적인 프로세스를 행한다. 데이터 수신기(3a)는 자신에 대한 라우팅을 행할 필요없이 단순하게 구성되고 범용 라우터와 함께 사용된다.

<142> 본 발명의 정신 및 범주를 벗어나지 않고 본 발명에 대한 많은 다른 실시예들이 이루어질 수도 있으므로, 본 발명은 첨부한 청구범위에 정의된 것을 제외한 특정 실시예들에 한정되지 않음을 주지하라.

발명의 효과

<143> 이상과 같이 본 발명에 의하면 데이터 전송기로부터 데이터 수신기로의 데이터 전송에 있어서, 보다 더 안전하고 확실하게 데이터를 전송할 수 있다.

도면의 간단한 설명

<1> 도 1은 종래의 데이터 전송 시스템의 통상적인 구조의 개략도.

<2> 도 2는 종래의 데이터 전송 시스템에 사용되며 목적지(destination) 어드레스를 포함하는 이더넷(Ethernet) 프레임의 데이터 구조의 개략도.

<3> 도 3은 종래의 데이터 전송 시스템의 데이터 수신기가 이더넷을 통하여 수신한 이더넷 프레임이 수신기 자체의 목적지 어드레스를 포함하고 있는지의 여부를 검사하고, 목적지 어드레스 검사 다음의 프로세스를 수행하는 단계를 도시한 흐름도.

<4> 도 4는 TS 패킷에 대한 데이터 구조 포맷의 개략도.

<5> 도 5는 종래의 데이터 전송 시스템에서의 데이터 전송기 및 데이터 수신기 구조의 개략도.

<6> 도 6은 본 발명에 따른 데이터 전송 시스템의 개략도.

<7> 도 7a 내지 7g는 데이터 전송 시스템에서 데이터 전송기로부터 데이터 수신기로 전송되는, 다수의 프로토콜에 따라서 캡슐화 데이터의 개략도.

<8> 도 8은 데이터 전송 시스템에서 데이터 전송기 및 데이터 수신기의 블록도.

<9> 도 9는 데이터 전송기로부터 데이터 수신기로 전송되는 데이터를 암호화하는 세션 키를 갱신하는 단계의 흐름도.

<10> 도 10은 섹션 헤더의 데이터 구조의 개략도.

<11> 도 11은 MAC 어드레스들이 세션 키(Ks)의 플래그에 대응하여 설정되는 대응표.

<12> 도 12는 데이터 전송기가 데이터를 캡슐화하는 단계의 흐름도.

<13> 도 13은 IP 어드레스들이 MAC 어드레스들에 대응하여 설정되는 대응표.

<14> 도 14는 데이터 수신기가 세션 키(Ks)를 사용하여 수신된 데이터를 복호화하는 단계의 흐름도.

<15> 도 15는 MAC 어드레스들이 세션 키(Ks)에 대응하여 설정되는 대응표.

<16> 도 16은 IP 데이터그램(datagram)을 추출하는데 사용된 총 길이 필드를 보유하는 데이터 구조에 대한 복호 개략도.

<17> 도 17은 데이터 전송 시스템의 제 1 변형의 개략도.

<18> 도 18은 데이터 전송 시스템의 제 2 변형의 개략도.

<19> * 도면의 주요 부분에 대한 부호의 설명 *

<20> 1 : 데이터 전송 시스템 2 : 데이터 전송기

<21> 3 : 데이터 수신기 4 : 통신 위성

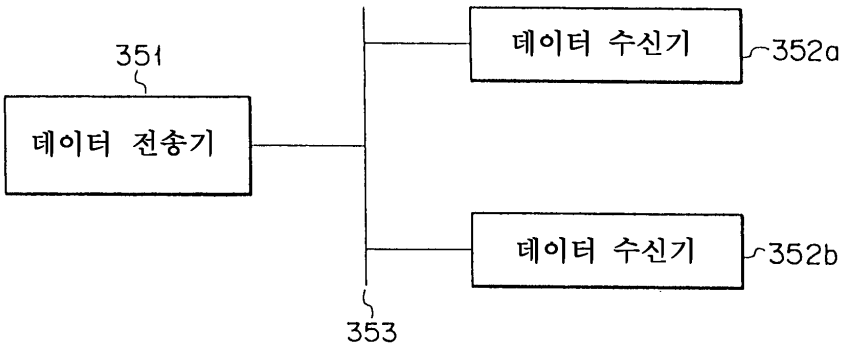
<22> 5 : 인터넷 서비스 제공업체 6 : 인터넷

<23> 7 : 전용선 8 : 전화선

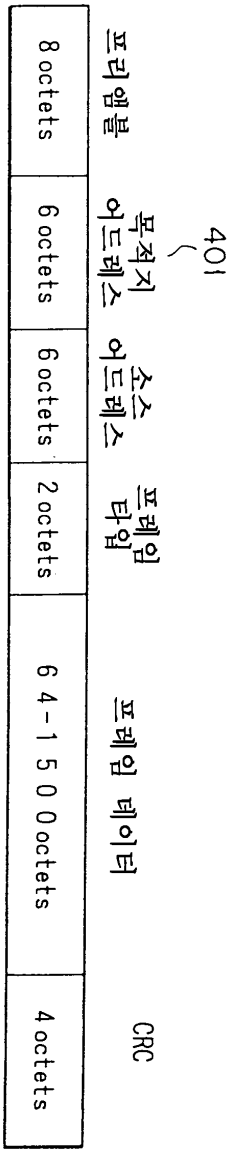
<24> 9 : 양방향 통신 채널

도면

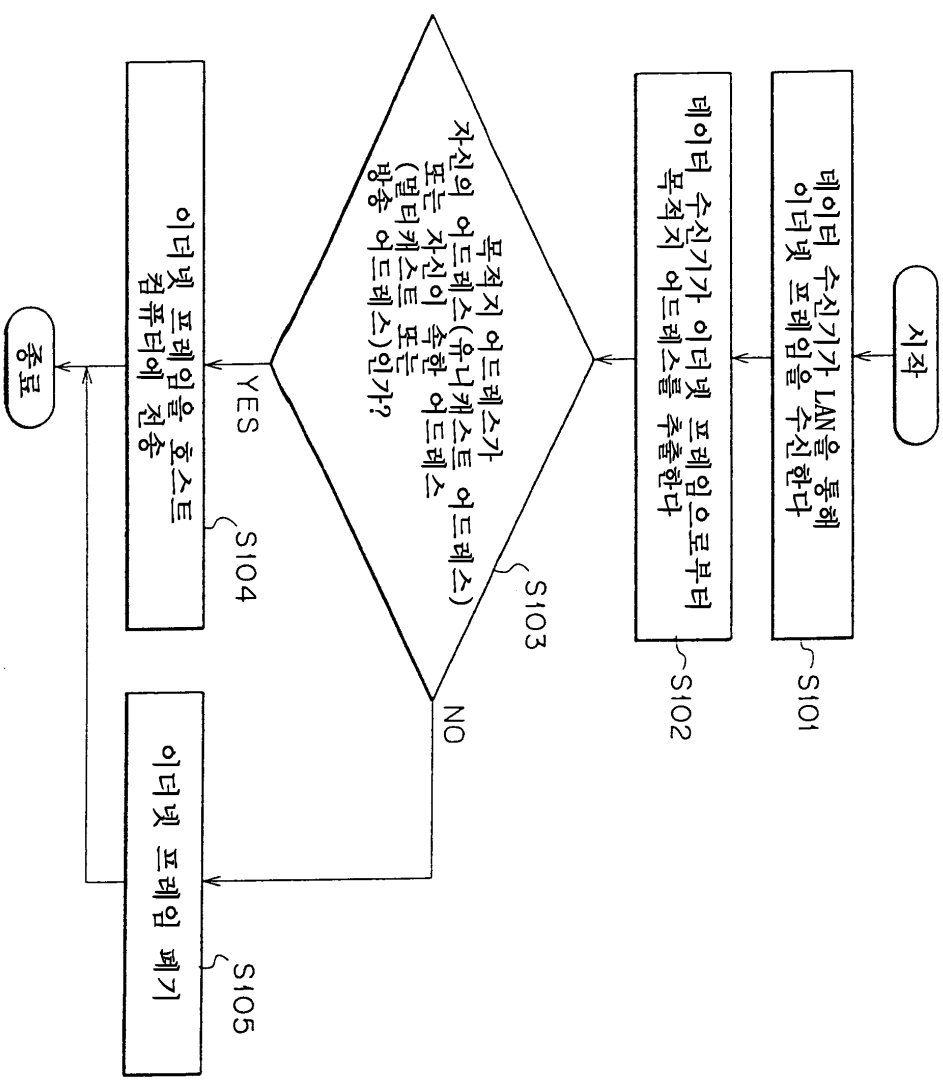
도면1



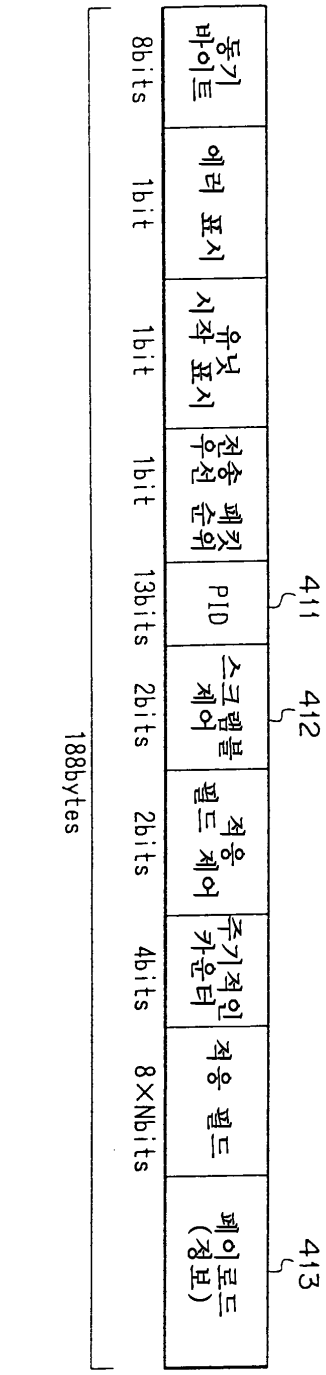
도면2


401
프리앰블
목적지 어드레스
소스 어드레스
프레임 타입
프레임 데이터
CRC
8 octets
6 octets
6 octets
2 octets
64-1500 octets
4 octets

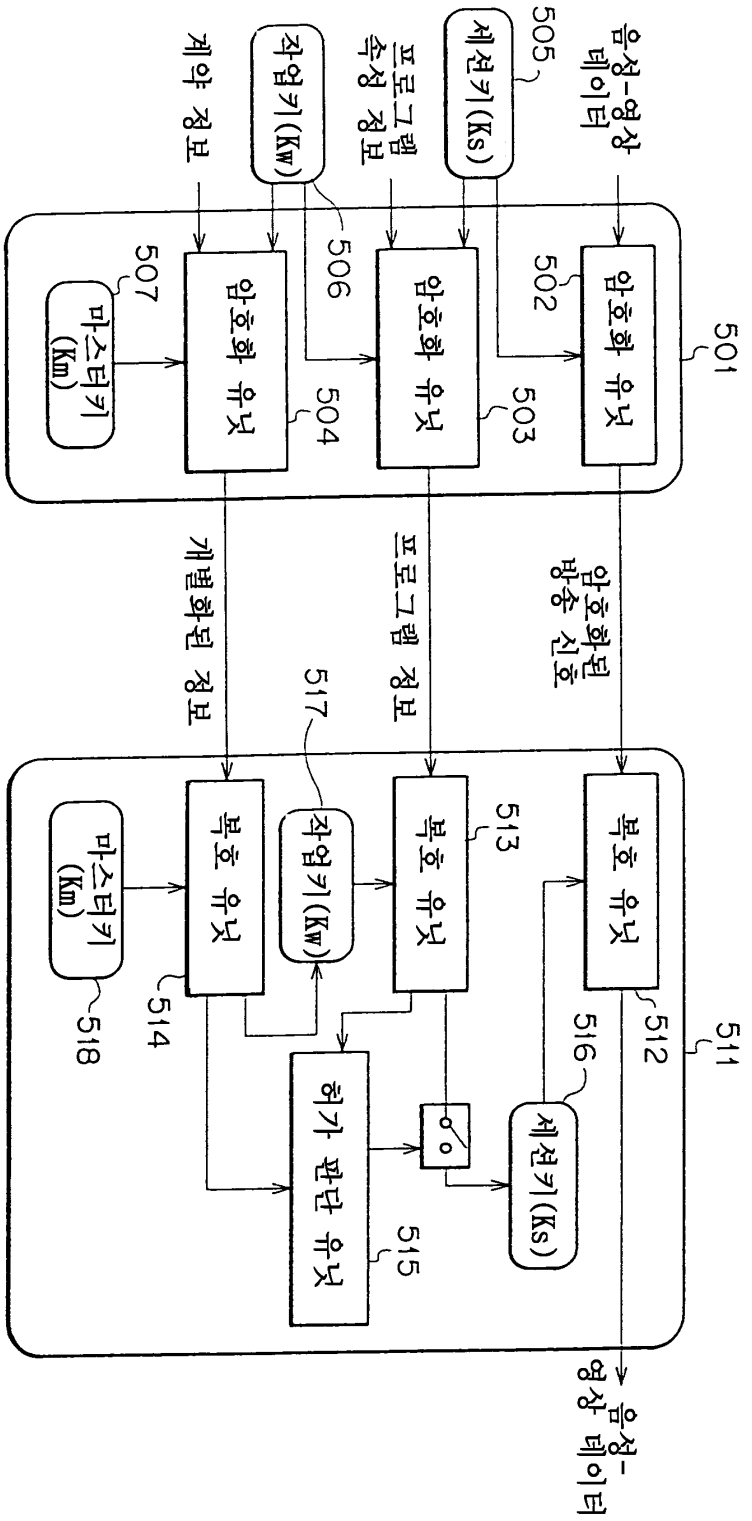
도면3


시작
데이터 수신기가 LAN을 통해 이더넷 프레임을 수신한다
S101
데이터 수신기가 이더넷 프레임으로부터 목적지 어드레스를 추출한다
S102
목적지 어드레스가 자신의 어드레스(유니캐스트 어드레스) 또는 자신이 속한 (멀티캐스트 또는 방송 어드레스)인가?
S103
YES
NO
이더넷 프레임을 호스트 컴퓨터에 전송
S104
이더넷 프레임 폐기
S105
종료

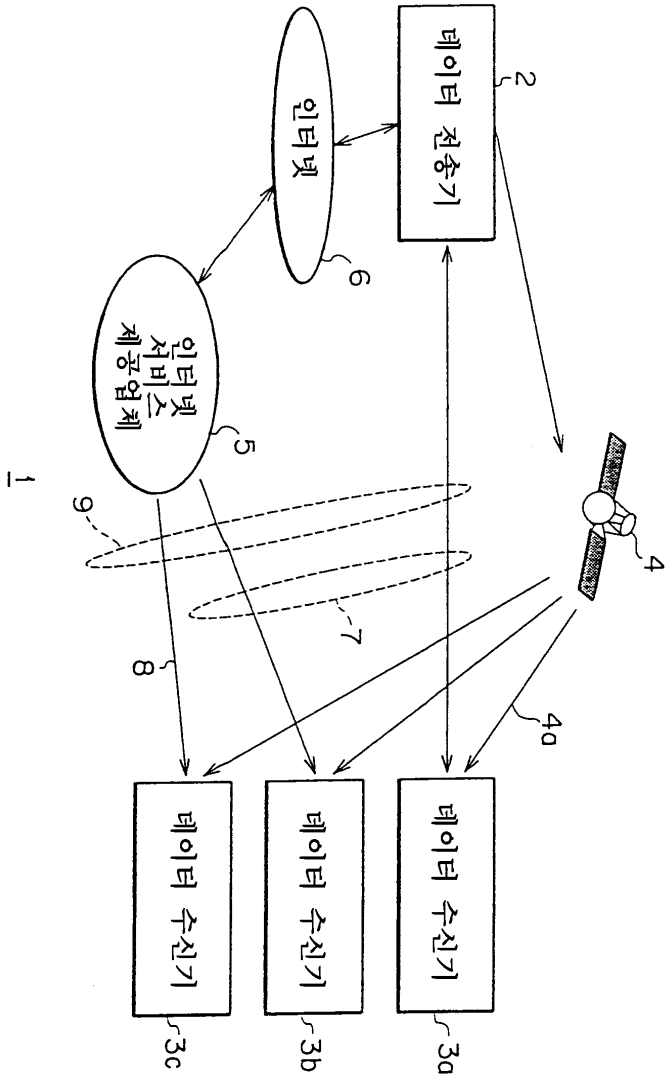
도면4


동기 바이트
8bits
에러 표시
1bit
유닛 시작 표시
1bit
전송 우선 패킷 순위
1bit
PID
13bits
411
스크램블 제어
2bits
412
적응 필드 제어
2bits
주기적인 카운터
4bits
적응 필드
8×Nbits
페이로드 (정보)
413
188bytes

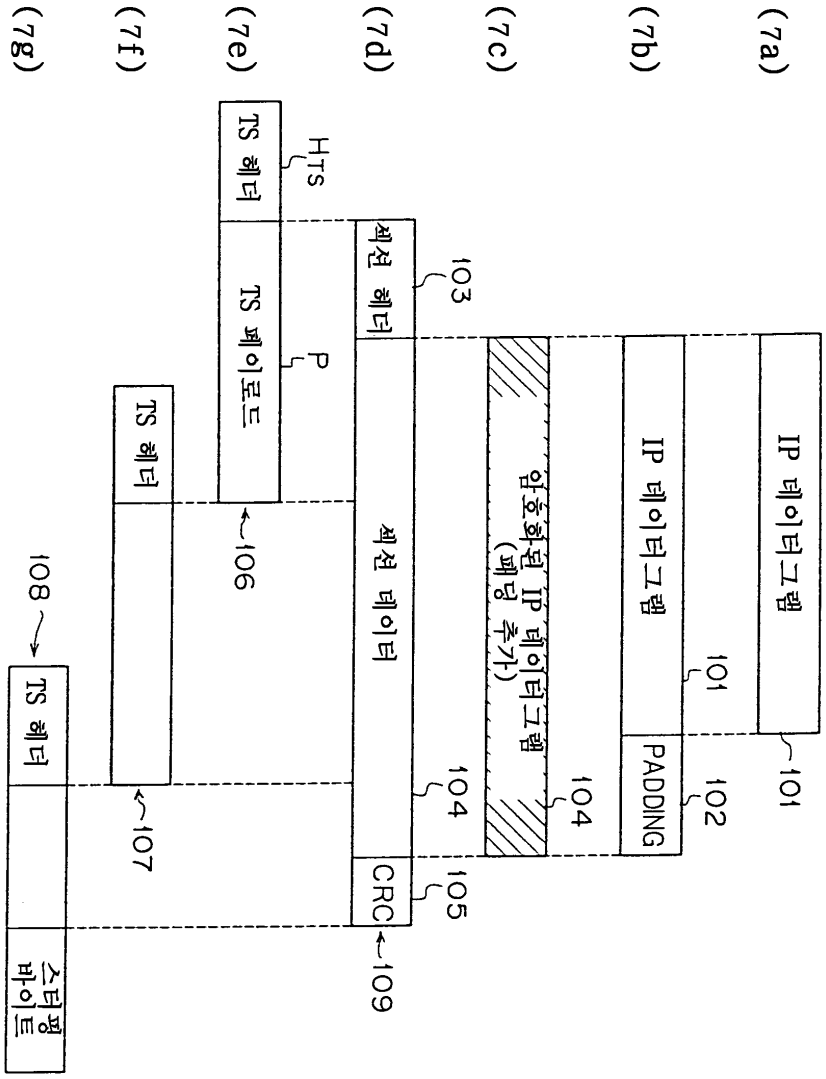
도면5


음성-영상 데이터
세션키(Ks)
505
작업키(Kw)
프로그램 속성 정보
계약 정보
501
암호화 유닛
502
암호화 유닛
503
암호화 유닛
504
506
마스터키 (Km)
507
암호화된 방송 신호
프로그램 정보
개별화된 정보
511
복호 유닛
512
516
세션키(Ks)
복호 유닛
513
517
작업키(Kw)
복호 유닛
514
마스터키 (Km)
518
허가 판단 유닛
515
영상 음성-데이터

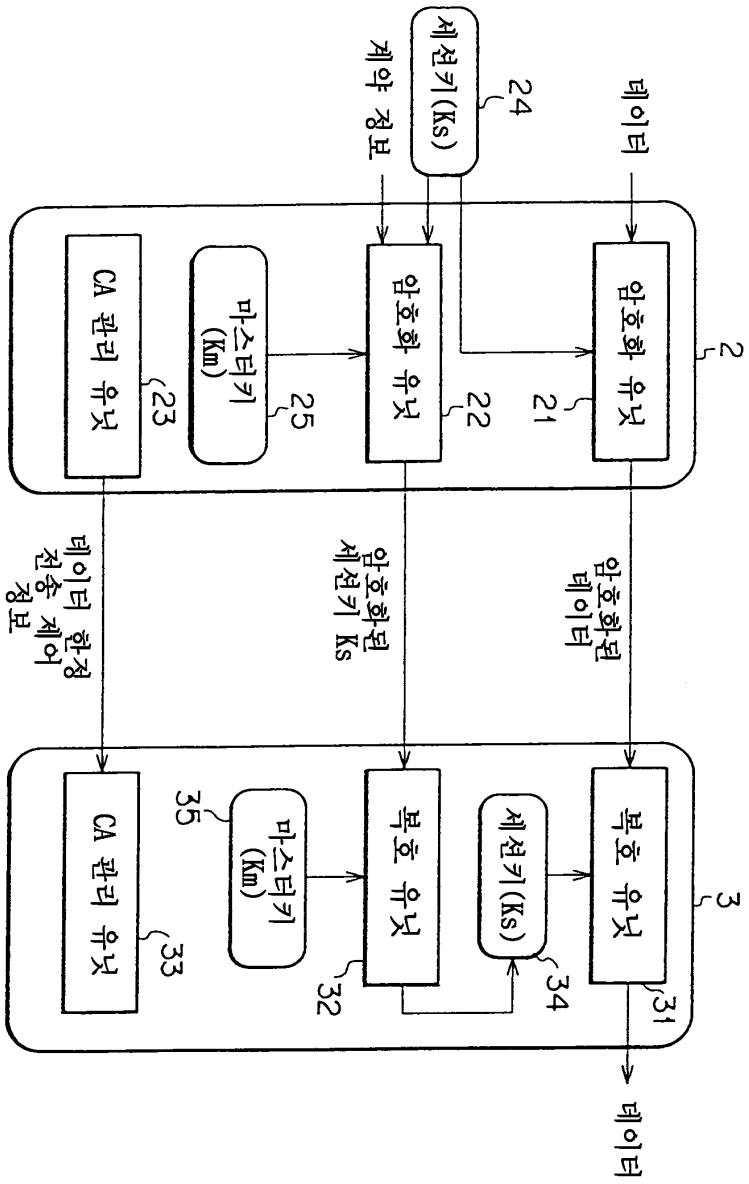
도면6


1
데이터 전송기
2
인터넷
6
인터넷 서비스 제공업체
5
9
7
8
4
4a
데이터 수신기
3c
데이터 수신기
3b
데이터 수신기
3a

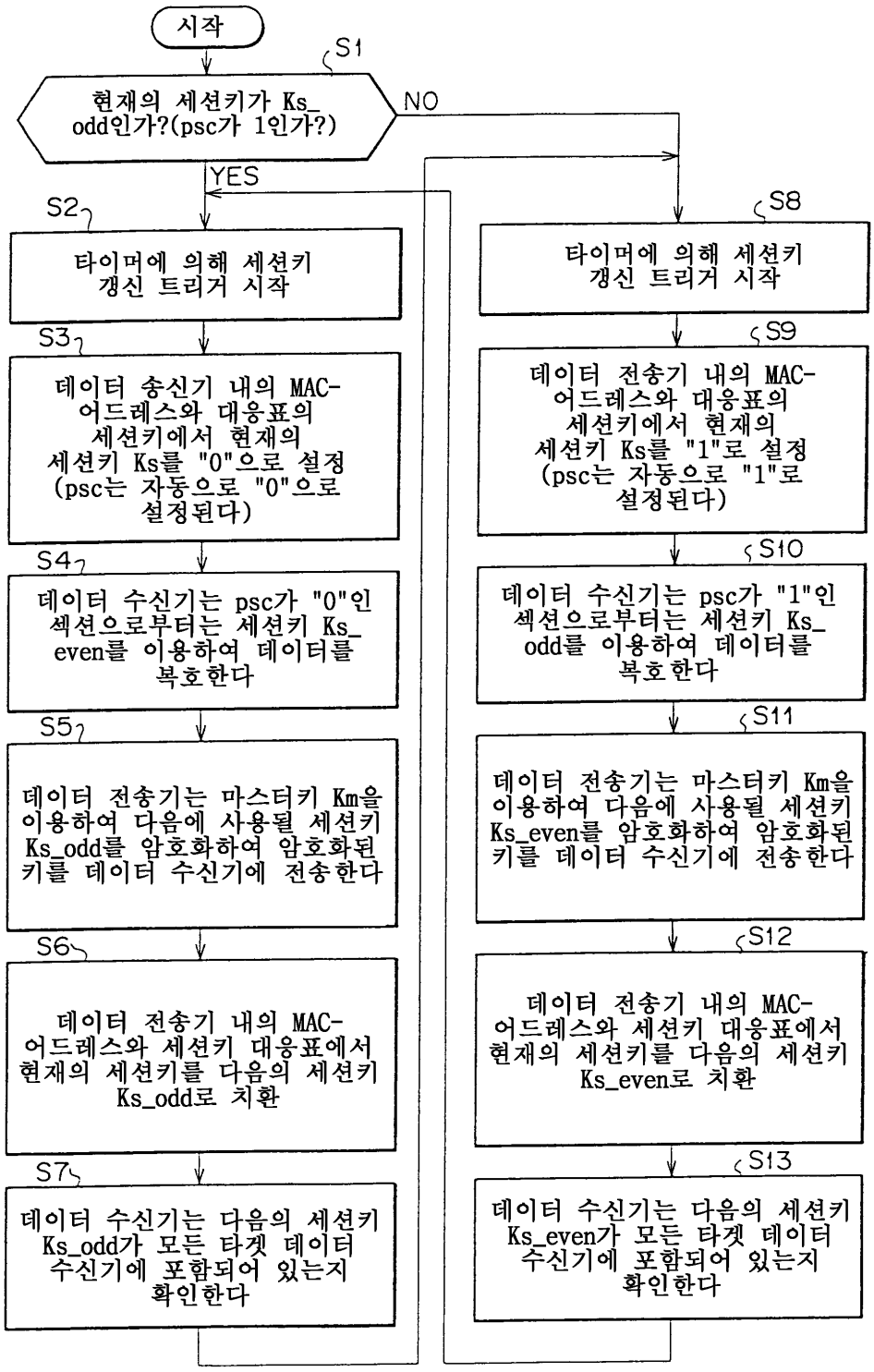
도면7


(7a)
IP 데이터그램
101
(7b)
IP 데이터그램
PADDING
101
102
(7c)
암호화된 IP 데이터그램
(패딩 추가)
104
(7d)
섹션 헤더
103
섹션 데이터
104
CRC
105
109
(7e)
TS 헤더
HTS
TS 페이로드
P
106
(7f)
TS 헤더
107
(7g)
TS 헤더
108
스터핑 바이트

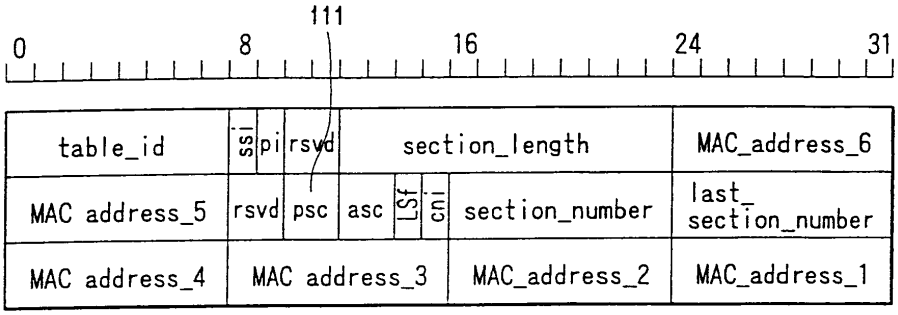
도면8


데이터
계약 정보
세션키(Ks)
24
암호화 유닛
2
21
22
CA 관리 유닛
23
마스터키(Km)
25
데이터 한정 전송 제어 정보
암호화된 세션키 Ks
암호화된 데이터
복호 유닛
3
31
세션키(Ks)
34
32
마스터키(Km)
35
CA 관리 유닛
33
데이터

도면9


시작
S1
현재의 세션키가 Ks_odd인가?(psc가 1인가?)
NO
YES
S2
타이머에 의해 세션키 갱신 트리거 시작
S3
데이터 송신기 내의 MAC-어드레스와 대응표의 세션키에서 현재의 세션키 Ks를 "0"으로 설정 (psc는 자동으로 "0"으로 설정된다)
S4
데이터 수신기는 psc가 "0"인 섹션으로부터는 세션키 Ks_even를 이용하여 데이터를 복호한다
S5
데이터 전송기는 마스터키 Km을 이용하여 다음에 사용될 세션키 Ks_odd를 암호화하여 암호화된 키를 데이터 수신기에 전송한다
S6
데이터 전송기 내의 MAC-어드레스와 세션키 대응표에서 현재의 세션키를 다음의 세션키 Ks_odd로 치환
S7
데이터 수신기는 다음의 세션키 Ks_odd가 모든 타겟 데이터 수신기에 포함되어 있는지 확인한다
S8
타이머에 의해 세션키 갱신 트리거 시작
S9
데이터 전송기 내의 MAC-어드레스와 대응표의 세션키에서 현재의 세션키 Ks를 "1"로 설정 (psc는 자동으로 "1"로 설정된다)
S10
데이터 수신기는 psc가 "1"인 섹션으로부터는 세션키 Ks_odd를 이용하여 데이터를 복호한다
S11
데이터 전송기는 마스터키 Km을 이용하여 다음에 사용될 세션키 Ks_even를 암호화하여 암호화된 키를 데이터 수신기에 전송한다
S12
데이터 전송기 내의 MAC-어드레스와 세션키 대응표에서 현재의 세션키를 다음의 세션키 Ks_even로 치환
S13
데이터 수신기는 다음의 세션키 Ks_even가 모든 타겟 데이터 수신기에 포함되어 있는지 확인한다

도면10



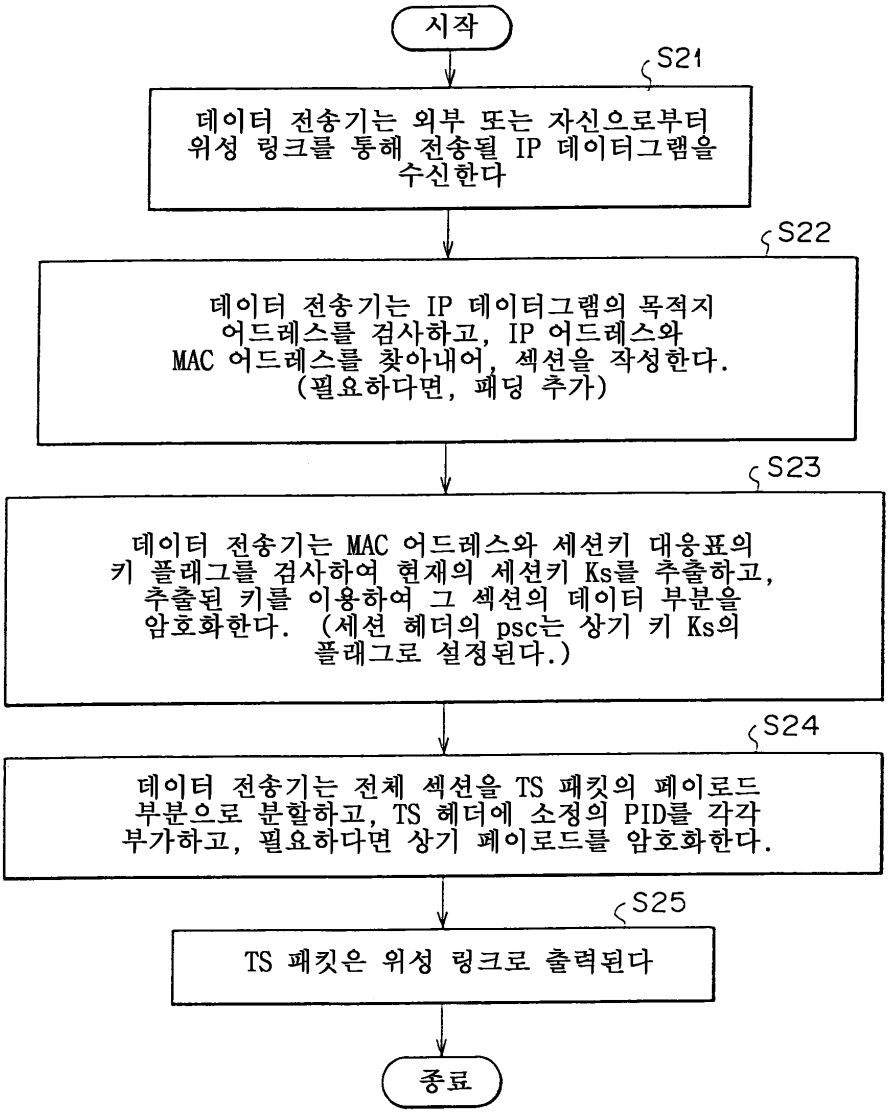
ssi : section_syntax_indicator
pi : private_indicator
rsvd : reserved
psc : payload_scramble_indicator
asc : address_scramble_indicator
LSf : LLC_SNAP_flag
cni : current_next_indicator

도면11

112

MAC 어드레스	Ks_even	Ks_odd	Ks 플래그
08:00:46:01:07:24	0×C08F...25	0×90B3...AF	0
08:00:45:01:07:09	0×26D2...61	0×BA02...3C	1
01:00:5e:16:0:0	0×461E...67	0×DC1A...22	0

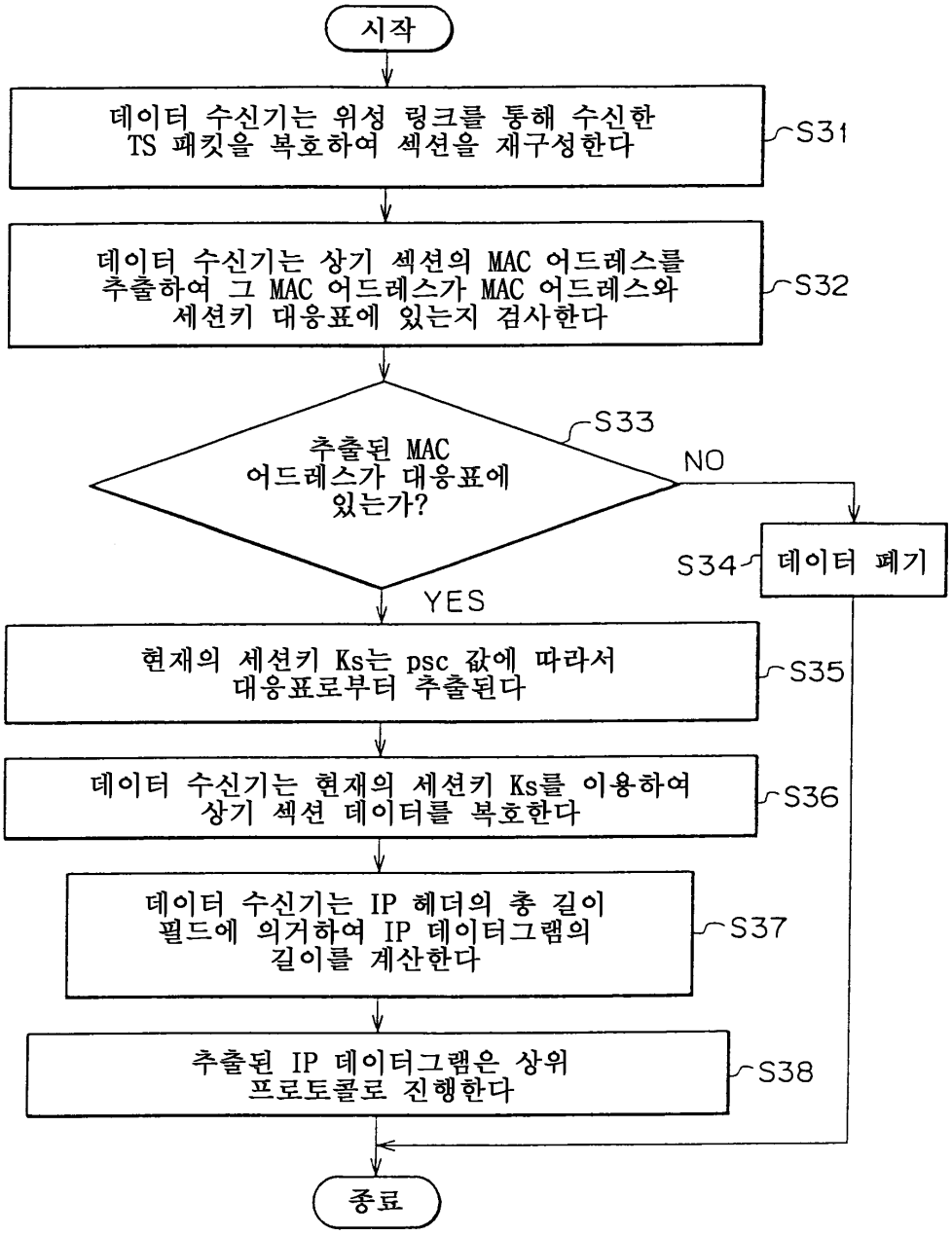
도면12



도면13

IP 어드레스	bitmask	MAC address
133.11.9.39	255.255.255.225	08:00:46:01:07:24
133.11.20.0	255.255.255.0	08:00:46:01:07:09
226.0.0.0	255.255.255.224	01:00:5e:16:0:0

도면14



도면15

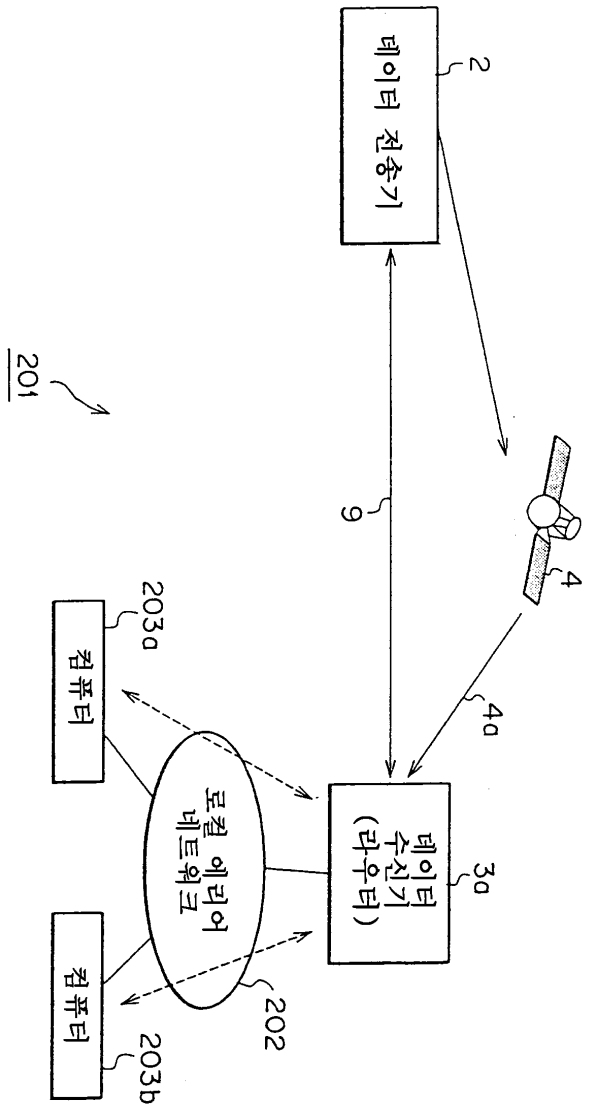
MAC 어드레스	Ks_even	Ks_odd
08:00:46:01:07:24	0×C08F...25	0×90B3...AF
01:00:5e:16:0:0	0×461E...67	0×DC1A...22

도면16

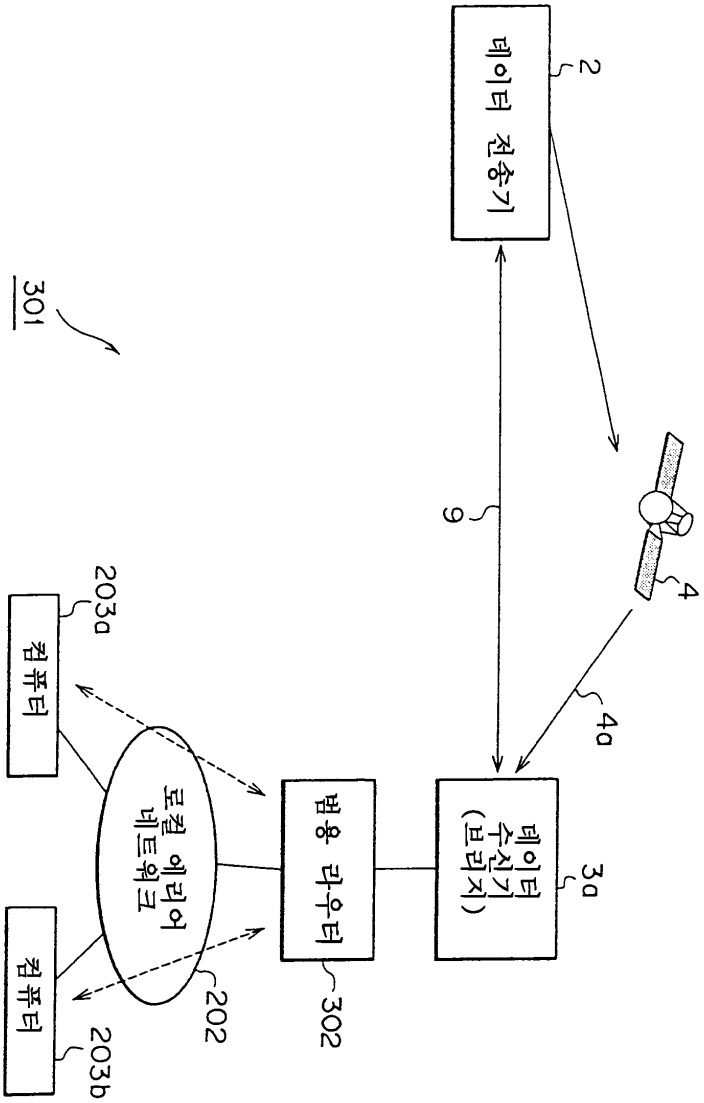
113

VERS	HLEN	SERVIE TYPE	TOTAL LENGTH
IDENTIFICAION		FLAGS	FRAGMENT OFFSET
TIME TO LIVE	PROTOCOL		HEADER CHECKSUM
SOURCE IP ADDRESS			
DESTINATION IP ADDRESS			
IP OPTIONS (IF ANY)			PADDING
DATA			
. . . . .			

도면17



도면18


데이터 전송기
2
9
4
4a
데이터 수신기 (브리지)
3a
범용 라우터
302
로컬 에리어 네트워크
202
컴퓨터
203a
컴퓨터
203b
301