(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1645865 B
(45)授权公告日 2010.06.16

(21)申请号 200510054449.7

(22)申请日 1999.05.12

(30)优先权数据
129214/98 1998.05.12 JP

(62)分案原申请数据
99106605.7 1999.05.12

(73)专利权人 索尼公司
地址 日本东京都

(72)发明人 原和弘

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 黄小临 王志森

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
WO 97/50249 A1,1997.12.31, 全文.
CN 1169806 A,1998.01.07, 说明书第6页倒数第1行-第8页第8行及附图1-2.
US 5652795 A,1997.07.29, 全文.
CN 1122979 A,1996.05.22, 全文.
EP 0179612 A2,1986.04.30, 全文.
CN 1173954 A,1998.02.18, 全文.

审查员 阎岩

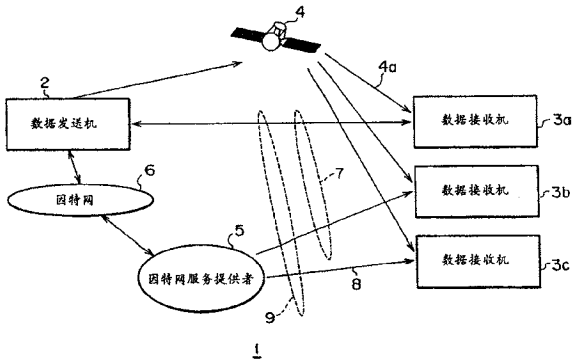
权利要求书 1 页 说明书 13 页 附图 15 页

(54)发明名称

数据传输控制方法和数据传输系统

(57)摘要

一种把数据从数据发送机发送到一个或多个数据接收机的数据传输系统,包括:数据发送机,对数据加密和发送加密数据;数据接收机,接收加密数据;卫星链路,把数据从数据发送机传输到数据接收机;和双向通信信道,把数据从数据接收机传输到数据发送机,且具有比卫星链路小的数据传输容量。卫星链路把加密数据从数据发送机传输到数据接收机。至少双向通信信道用于在数据发送机和数据接收机之间传送限制性数据传输控制信息。



CN 1645865 B

1. 一种数据传输控制方法，用于控制通过通信信道从数据发送装置到数据接收装置的数据的传输，并且用于使所述数据发送装置对数据进行加密，和通过所述通信信道把该加密数据传送到所述数据接收装置，所述数据传输控制方法包括以下步骤：

根据多个协议、以多路复用的方式、对要发送的数据进行封装；并且

对至少一个由封装产生的数据囊进行加密，

其中，数据封装的步骤包括：

第一封装步骤，用于根据第一协议、对要发送到所述数据接收装置的数据进行封装；以及

第二封装步骤，用于根据第二协议、对来自所述第一封装步骤的封装的数据进行进一步的封装；

其中，所述第一封装步骤向包括要发送到所述数据接收装置的所述数据的实数据部分补充与所述实数据部分相关联的附加的信息部分，所述第一封装步骤进一步对所述实数据部分进行加密；以及

其中，所述附加的信息部分包括目的地址信息，该目的地址信息识别授权接收包含在所述实数据部分中的数据的数据接收装置。

2. 如权利要求 1 所述的数据传输控制方法，其中，所述目的地址信息是单个的或是成组的目的地址信息。

3. 如权利要求 1 所述的数据传输控制方法，其中，所述数据发送装置拥有与所述目的地址信息对应的会话密钥，所述会话密钥被所述数据发送装置用来对信息和数据进行加密，并且被所述接收装置用来对收到的加密的信息和数据进行解密；并且

其中，所述数据发送装置预先根据所述目的地址信息、把所述会话密钥发送到授权接收该发送的信息和数据的数据接收装置。

4. 如权利要求 3 所述的数据传输控制方法，其中，所述会话密钥以预定的时间间隔被更新。

5. 如权利要求 3 所述的数据传输控制方法，其中，所述会话密钥通过允许从所述数据发送装置到所述数据接收装置的单向通信的、或是其间的双向通信的通信信道进行发送。

6. 如权利要求 1 所述的数据传输控制方法，其中，所述第一封装步骤唯一地决定附加到所述实数据部分上的所述目的地址信息如何被存储到所述附加信息部分，所述第一封装步骤使用与所述目的地址信息对应的数据接收装置专用的主密钥、进一步对所述实数据部分进行加密。

7. 如权利要求 1 所述的数据传输控制方法，其中，所述附加的信息部分提供容纳所述目的地址信息的 48 比特的空间。

8. 如权利要求 1 所述的数据传输控制方法，其中，所述第一封装步骤根据网际协议、或以太网协议，对要发送到所述数据接收装置的数据进行封装。

9. 如权利要求 1 所述的数据传输控制方法，其中，所述数据接收装置用作 I P 路由器。

10. 如权利要求 1 所述的数据传输控制方法，其中，所述数据接收装置用作网桥。

数据传输控制方法和数据传输系统

[0001] 本申请是如下专利申请的分案申请：申请号：99106605.7，申请日：1999.5.12，发明名称：数据传输控制方法和数据传输系统。

技术领域

[0002] 本发明涉及一种用于控制从数据发送机到数据接收机的数据的传输的、数据传输控制方法和数据传输系统。本发明特别涉及一种用于限制从数据发送机到特定数据接收机的发送数据的接收的、数据传输控制方法和数据传输系统。

背景技术

[0003] 近几年，允许数据发送机将数据发送到多个远程数据接收机的、网络型数据传输系统已经建立起来了。例如，作为利用卫星链路把视频和音频信息分配给多个数据接收机的广播数据传输系统、实现了卫星电视广播。

[0004] 该广播数据传输系统的另一个例子是作为局域网 (LAN) 建立的以太网。如图 1 所示，以太网网络典型地由用于发送数据的数据发送机 351、以及用于通过网络 353 接收来自数据发送机 351 的数据的数据接收机 352a 和 352b 构成。以太网上的多个数据接收机之间的最大允许距离设定为几公里。

[0005] 在期望上述数据传输系统中的数据发送机 351 把数据发送到数据接收机 352a 时，数据发送机 351 把数据放到网络 353 上。对发送的数据添加标识目的数据接收机 352a 的目的地址。示例性地，用 48 比特表示大量的目的地址信息。

[0006] 由数据发送机 351 放到网络 353 上的数据被数据接收机 352a 和 352b 接收。每个数据接收机参照附加在接收数据上的目的地址，看该地址是否与其自己的地址相符。由以太网使用的典型的帧格式如图 2 所示。在该格式中，目的地址部分 401 指定应该接收该数据的目的数据接收机的地址。

[0007] 如果一个给定的数据接收机判定接收的地址不是其自己的，则该接收机丢弃该发送的数据。换言之，判定附加在数据上的地址是其自己的地址的数据接收机 352a 接受该发送的数据，而在接收的数据中未能检测到其自己的地址的数据接收机 352a 丢弃该数据。在以太网上，数据接收机的数据接收处理典型地按图 3 中的流程图的步骤进行。

[0008] 在步骤 S101 中，数据接收机从局域网接收包含数据的以太网帧。在步骤 S102 中，数据接收机从接收的以太网帧中提取目的地址。在步骤 S103 中，数据接收机进行检查，看目的地址是否是其自己的地址（单点广播 (unicast) 地址）、或是其所属的地址（多点广播 (multicast) 地址）。如果目的地址的结果是该数据接收机自己的地址（单点广播地址）、或是其所属的地址（多点广播地址），则该数据接收机把该以太网帧传输到主机。单点广播地址表示指向单个接收机的地址，而多点广播地址是允许多个数据接收机（例如，一个数据接收机组）接收与该地址一起发送的数据的地址。

[0009] 如果目的地址的结果既不是指向所述的数据接收机的地址（单点广播地址），也不是该数据接收机所属的地址（多点广播地址），那么该数据接收机丢弃该以太网帧。

[0010] 按照上述的、基于目的地址方案的数据传输的方法，任何地址与发送的目的地址不匹配的数据接收机、都应该不能接收与该地址一起提供的数据。然而，实际上，对于该数据传输方法，数据接收机的地址和判定特性可能被任意修改，从而接收其他指向的数据，即，没有标识所述数据接收机的目的地址的数据。当需要把机密数据传输到特定的数据接收机时，上述可能性就引出了安全性的问题。

[0011] 在以太网上，连接到同一个网络的数据接收机的数目是有限的，并且，被连接的接收机之间的距离也是有限的。这意味着，发送给一个数据接收机的数据被另一数据接收机非法窃听的可能性是有限的。示例性地，在典型的 10BASE-5 以太网的方案下，用于一个段 (segment) 的电缆的最大长度被限制在 500 米，而且，可连接到网络的收发机（数据发送－接收机）的数目设定为最多 100。

[0012] 同时，如果用卫星链路构成数据传输网络，则一个网络就可覆盖比整个象日本这样的国家还广泛的区域。在这样的网络上，发送给最北方的北海道岛上的一个数据接收机的数据，可能会被最南方的冲绳县里的一个数据接收机窃听。换言之，在任何配有大量数据接收机的、基于卫星链路的网络上，数据被不希望的各方非法窃听的可能性增加了。

[0013] 在利用广播型通信信道，例如卫星链路，的数据传输体制中，未处理的数据不但能被不希望的数据接收机接收，而且还能被那些不应该接收所述数据的接收机接收。对于今天的、使用通信卫星的数字数据广播系统，上述问题的一个解决方案就是数据（即，主要是视频和音频信息）在通过卫星通信链路发送之前进行加密。对数据接收机来说，具有重建原始数据的解密功能。在上述类型的数据传输系统中，只有那些预先授权接收数据的数据接收机才能够解密该传输用于视听消费。一个这样的系统基于日本电气通信技术审议会 74 号报告。该系统使用 MPEG2(Moving Picture ExpertsGroup Phase 2，运动图象专家组阶段 2) 传输流包 (TS packets，TS 包）作为其传输格式。示例性地，该系统让其数据发送机使用加密密钥对数据进行加密，并让其数据接收机使用与加密密钥对应的解密密钥对加密数据进行解密。TS 包的格式示于图 4。格式的首标中的 PID(packet identification，包标识符）部分 411 和加扰控制部分 412 确定了加密密钥。典型地，加密密钥包括会话密钥 (Session key)Ks 和工作密钥 (Work key)Kw。PID 部分 411 构成 13 比特的数据，而加扰控制部分 412 构成 2 比特的数据。

[0014] 如图 5 所示，在现有的、用 TS 包传输数据的卫星电视广播体制中，数据传输系统典型地包括数据发送机 501 和数据接收机 511。数据发送机 501 具有使用多种加密密钥执行数据加密的加密单元 502、503 和 504。数据接收机 511 具有使用多种解密密钥执行数据解密的解密单元 512、513 和 514、以及授权判断单元 515。

[0015] 在上述结构的数据传输系统中，数据发送机 501 首先把工作密钥 Kw 506 发送到数据接收机 511。具体地说，数据发送机 501 预先准备与 PID 部分 411 和加扰控制部分 412 相对应的工作密钥 Kw 506。数据发送机 501 然后得到由加密单元 504、用主密钥 (master key) Km 507 加密的工作密钥 Kw 506。加密后的工作密钥 Kw 506 被发送到数据接收机 511。主密钥 Km 507 与数据接收机 511 特有的主密钥（解密密钥）Km 518 相同。加密后的工作密钥 Kw 506 通过卫星链路从数据发送机 501 发送到数据接收机 511。

[0016] 一收到用主密钥 Km 507 加密的工作密钥 Kw 506，数据接收机 511 就用其自己的主密钥 Km 518 对接收的密钥进行解密。数据接收机 511 与 PID 部分对应地保存解密后的工

作密钥 Kw 517。工作密钥 Kw 517 用于对来自数据发送机 501 的加密数据进行解密。

[0017] 在从数据发送机 501 给数据接收机 511 发送数据的时候，数据发送机 501 由加密单元 502 使用会话密钥 Ks 505 加密 TS 包中的数据的净荷部分 413。同时，加密单元 503 使用工作密钥 Kw 506 对会话密钥 Ks 505 进行加密。

[0018] 在接收到 TS 包，且其 PID 部分标识数据接收机 511 作为目的以后，数据接收机 511 根据发送的 TS 包中的 PID 部分 411、提取预先保存的工作密钥 Kw 517。数据接收机 511 使用提取出来的工作密钥 Kw 517、对加密的、与数据一起从数据发送机 501 被发送的会话密钥 Ks 505 进行解密。通过使用经如此解密的会话密钥 Ks 516，数据接收机 511 对 TS 包中的净荷部分 413 进行解密，以便从中提取数据。

[0019] 因为没有向未经授权的数据接收机发送工作密钥 Kw，所以这些数据接收机不具有适当的、与所关心的 PID 部分相对应的工作密钥 Kw。这些数据接收机不能使用工作密钥 Kw、对数据发送机 501 在密钥加密之后紧跟着发送的会话密钥 Ks 进行解密。由于会话密钥 Ks 没有解密，未经授权的接收机就不能够对来自数据发送机 501 的、加密的数据进行解密。换句话说，未经同意的数据接收机能够收到加密数据，但不能解密该数据用于视听消费。

[0020] 如上所述，使用卫星链路的上述广播系统典型地实现了限制性数据传输控制。限制性数据传输控制的各种其他的方法也不仅通过广播系统来实施，还通过，比方说，因特网来实施。

[0021] 在因特网上，PGP(Pretty Good Privacy，相当好的加密性）和 PEM(Privacy Enhanced Mail，增强的私密邮件）被示例性地用来加密电子邮件，以防御被不希望的各方窃听或篡改。在因特网上还使用 SSL(SecureSocket Layer，加密套接字协议层），它是为阻止非法窃听在基于 HTTP(HyperText Transfer Protocol，超文本传输协议）的电子商务中传输的信誉卡号码而设计的。这些方案的特点是使用加密系统或采用灵活的数据传输控制。

[0022] 对 IP(Internet Protocol，网际协议）数据报，存在更加通用的数据传输控制方法。这一类的标准化的方法包括 AH(Authentication Header，鉴定首标）和 ESP(Encapsulating Security Payload，安全封装的净荷），总体称之为 IPSEC。

[0023] 总体上，在使用卫星链路的电视广播方面，碰到了以下几个问题：

[0024] 第一个问题是，授权的数据接收机的数目有限。如图 4 所示，用于标识加密密钥的 PID 部分、和加扰控制部分分别只包括 13 比特和 2 比特。这意味着用 15 比特只能指定不超过 2^{15}（＝ 32,768）个数据接收机。

[0025] 第二个问题是，随着使用的 PID 的数目增长，在发送端的花费也增加。示例性地，数据接收机需要的 MPEG 2 编码器几乎与 PID 的数目成正比。因此，随着 PID 数量的增加，使需要安装大规模设备的数据发送机端的花费也增加。

[0026] 第三个问题是，在通过卫星链路的单向 (one-way) 数据传输中，数据发送机不能够知道信息是否已被正确地传输到目的数据接收机。例如，可能存在这样的情况，不通知数据发送机，数据接收机实际上不能从那里接收数据，尽管其为已被授权的状态。然而，试图将信息更可靠地传输到数据接收机则花费时间。这可能涉及大量资源的浪费，这使得该可靠但耗时的方案成为灵活的数据传输控制的阻碍。

[0027] 第四个问题是当 IP 数据包必须与由数据发送机调整为 IP 目的地址的 PID 一起发

送时，与网际协议的亲和性差。更具体地说，IP 数据报的目的地址具有 32 比特的地址格式，这对于 13 比特的 PID 部分来说调整起来很困难。而且，目前因特网上使用的上述方法具有第五个问题：PGP、PEM 和 SSL 是应用专用 (application-specific) 数据传输控制，并且不为因特网上的所有应用所共有。向每个应用提供其自己的控制方法的必要、使得迅速处理新引进的应用很困难。

[0028] 第六个问题是，虽然鉴定首标和安全封装的净荷是应用无关的 (application-independent)，但是在网际协议的目前版本 (例如，IP v4) 的水平上，实际上没有与这些方法兼容的网络设备。尽管网际协议的下一个版本 (例如，IP v6) 允许在因特网上以标准的方式使用 AH 和 ESP，但他们被认为几乎不能在现有的因特网上使用。

发明内容

[0029] 本发明提供了一种数据传输控制方法和数据传输系统，从而，可以以比以前更加安全和更加可靠的方式执行从数据发送机到数据接收机的数据传输。

[0030] 根据本发明的一个方面，提供了一种数据传输控制方法，包括以下步骤：通过为从数据发送装置到数据接收装置的数据传输而设的第一通信信道、把由数据发送装置加密的数据发送到数据接收装置；以及至少通过第二通信信道把限制性数据传输控制信息发送到数据接收装置，该信息用于使来自数据发送装置的加密数据只单独地被特定的数据接收装置接收，该第二通信信道具有比第一通信信道小的数据传输容量，并且也可用于从数据接收装置到数据发送装置的数据传输。

[0031] 在使用该数据传输控制方法时，数据发送装置通过第一通信信道把数据发送到数据接收装置。至少通过第二通信信道、可在数据发送装置和数据接收装置之间交换限制性数据传输控制信息。

[0032] 用上述发明的数据传输控制方法，数据发送装置可以通过第一通信信道和第二通信信道把包含限制性数据传输控制信息的数据发送到数据接收装置。关于在数据发送装置和特定的数据接收装置之间的数据交换的信息、可通过第二通信信道在其间发送。

[0033] 示例性地，上述发明的方法使数据发送装置能够知道、向特定的数据接收装置发送的数据是否已被其正确地接收。

[0034] 根据本发明的另一情况，提供了一种数据传输系统，包括：第一通信信道，用于从数据发送装置到数据接收装置的数据传输；以及第二通信信道，允许在数据发送装置和数据接收装置之间进行双向通信；其中，第一通信信道用于把加密数据从数据发送装置传输到数据接收装置；并且其中，至少第二通信信道用于传输限制性数据传输控制信息，该信息用于使来自数据发送装置的加密数据只单独地被特定的数据接收装置所接收。

[0035] 在上述结构的数据传输系统中，数据发送装置通过第一通信信道把数据发送到数据接收装置。限制性数据传输控制信息通过第二通信信道、在数据发送装置和数据接收装置之间进行交换，第二通信信道至少用于从数据发送装置到数据接收装置的数据传输，并且具有比第一通信信道小的数据传输容量。

[0036] 在上述发明的数据传输系统中，数据发送装置可通过第一和第二通信信道、把包含限制性数据传输控制信息的数据发送到数据接收装置。关于在数据发送装置和特定的数据接收装置之间的数据交换的信息，可通过第二通信信道在其间传输。

[0037] 示例性地，上述发明的系统使数据发送装置能够知道、向特定的数据接收装置发送的信息是否已被正确地接收。

[0038] 根据本发明的进一步的情况，提供了一种数据传输控制方法，包括以下步骤：根据多个协议、以多路复用的方式、对要从数据发送装置发送到数据接收装置的数据进行封装；以及对至少一个由封装产生的数据囊 (capsule) 进行加密。

[0039] 在使用上述的数据传输控制方法时，根据多个协议、以多路复用的方式对要从数据发送装置发送到数据接收装置的数据进行封装。

[0040] 上述发明的方法使数据能在保持相关协议要求不变的情况下被传输。这意味着数据可以被传输，同时保持了它们与特定协议的兼容性。当根据协议封装数据，以便保护存储所述数据的空间时，这里提供了容纳各种信息的数据空间。加密封装的数据进一步保证了安全性。

[0041] 示例性地，可以根据能够容纳特定数据的协议对数据进行封装。封装处理提供了足够的空间，用来存储象加密密钥这种的关于目的地址的信息。在常规的 TS 包方案下，地址信息被写到 PID 部分和加扰控制部分，与此相比，上述目的地址信息有了显著的增加。这样就不必再扩展 PID 部分了。

[0042] 此外，不必为每个应用提供其自己的控制方法。这意味着，用本发明的方法可立即处理新引进的应用。而且，允许鉴定首标 (AH) 和安全封装的净荷 (ESP) 在现有的因特网上使用。

[0043] 根据本发明另一方面，提供了一种数据传输控制方法，包括以下步骤：使用加密密钥对数据进行加密；向加密数据中补充关于用于加密所述数据的加密密钥的加密密钥信息；把加密数据与加密密钥信息一起从数据发送装置传输到数据接收装置；以及使用使数据接收装置能够解密该加密数据的、并且经常更新的多个解密密钥中的一个、对加密数据进行解密，这一个解密密钥是根据附加在加密数据上的加密密钥信息进行选择的。

[0044] 用上述发明的方法，向在数据加密步骤中、用加密密钥进行加密的数据，提供关于用于加密所述数据的加密密钥的加密密钥信息。在数据传输步骤中，加密数据与加密密钥信息被一起从数据发送装置传输到数据接收装置。在数据解密步骤中，通过使用使数据接收装置能够解密该加密数据的、并且经常更新的多个解密密钥中的一个、对加密数据进行解密，这一个解密密钥是根据附加在加密数据上的加密密钥信息来进行选择的。

[0045] 用上述发明的数据传输控制方法，数据发送装置用加密密钥对数据进行加密。数据接收装置使用经常更新的多个解密密钥中的一个对接收的加密数据进行解密。这一个解密密钥是根据与加密数据一起传输的加密密钥信息，由数据接收装置从多个解密密钥中选出的。

附图说明

[0046] 通过阅读下面的描述和附图，本发明的其他目的、特性和优点将会变得更加清楚，其中，

[0047] 图 1 是常规数据传输系统的典型结构的示意图；

[0048] 图 2 是说明一个以太网帧的数据结构的示意图，该以太网帧被常规数据传输系统用于传输数据，并且该以太网帧包含目的地址；

[0049] 图 3 是一些步骤的流程图，在这些步骤中，常规数据传输系统的数据接收机进行检查，看通过以太网接收的一个以太网帧是否包含该接收机自己的目的地址，并且在这些步骤中，数据接收机在目的地址检查之后执行处理；

[0050] 图 4 是用于 TS 包的数据结构格式的示意图；

[0051] 图 5 是说明如何在常规数据传输系统中建立数据发送机和数据接收机的示意图；

[0052] 图 6 是具体实现本发明的一个数据传输系统的示意图；

[0053] 图 7A 至 7G 是在该数据传输系统中要从数据发送机发送到数据接收机、并且根据多个协议进行封装的数据的示意图；

[0054] 图 8 是该数据传输系统中的数据发送机和数据接收机的方框图；

[0055] 图 9 是对会话密钥进行更新的步骤的流程图，该会话密钥用于对要从数据发送机发送到数据接收机的数据进行加密；

[0056] 图 10 是节 (section) 首标的数据结构的示意图；

[0057] 图 11 是根据会话密钥 Ks 的标志设置 MAC 地址的对应表；

[0058] 图 12 是数据发送机封装数据的步骤的流程图；

[0059] 图 13 是根据 MAC 地址设置 IP 地址的对应表；

[0060] 图 14 是数据接收机用会话密钥 Ks 解密接收数据的步骤的流程图；

[0061] 图 15 是 MAC 地址与会话密钥 Ks 的对应表；

[0062] 图 16 是拥有用于提取 IP 数据报的 TOALLENGTH（总长度）字段的数据结构的示意图；

[0063] 图 17 是该数据传输系统的第一变形的示意图；以及

[0064] 图 18 是该数据传输系统的第二变形的示意图；

具体实施方式

[0065] 下面将参照附图详细地描述本发明的优选实施例。下面所述的、具体实现本发明的数据传输系统、仅限于特定的数据接收机接收由数据发送机通过卫星链路发送的数据。

[0066] 如图 6 所示，该发明的数据传输系统对通过用作通信信道的卫星链路 4a、专线 7 和电话线 8、以及通过双向通信信道 9 的、从数据发送机 2 到数据接收机 3a、3b 和 3c 的数据的传输进行控制。在该系统中，数据发送机 2 对数据进行加密，并通过通信信道将加密数据发送到数据接收机 3a、3b 和 3c。

[0067] 数据传输系统 1 包括：通信信道 4a，它使用了通信卫星 4，该通信信道用作使数据发送机 2 能够将数据发送到数据接收机 3a、3b 和 3c 的第一通信信道；以及专线 7、电话线 8 和双向通信信道 9，用作在作为一方的数据发送机 2 和作为另一方的数据接收机 3a、3b 和 3c 之间提供双向通信的第二通信信道。数据传输系统 1 将第一通信信道用于从数据发送机 2 到数据接收机 3a、3b 和 3c 的加密数据的传输，同时将第二通信信道用于从数据发送机到数据接收机的限制性数据传输控制信息的传输。数据传输系统 1 被连接到了因特网。

[0068] 限制性数据传输控制信息是允许一个特定的数据接收机或多个接收机接收从数据发送机 2 发送的数据的信息。换句话说，限制性数据传输控制信息授权一个特定的数据接收机或多个接收机接收所关心的发送数据。

[0069] 通过使用上述的通信信道，数据发送机 2 把各种数据发送到数据接收机 3a、3b 和

3c。数据接收机 3a、3b 和 3c 接收通过这些通信信道传过来的数据。虽然图 6 的体制只示出了三个数据接收机 3a、3b 和 3c，但是数据传输系统 1 实际上包括从几百到几十万个数据接收机。

[0070] 下面描述允许在数据发送机 2 和数据接收机 3a、3b 和 3c 之间进行数据交换的通信信道（在下文中，如果没有具体的、区分单个数据接收机 3a、3b 和 3c 的必要，则一般性地称之为数据接收机 3）。

[0071] 卫星链路 4a 是在具有大约 30Mbps 的带宽的 Ku 波段上的单向电路。卫星链路 4a 使数据发送机 2 能够同时把数据发送到，比方说，遍及日本分布的多个数据发送机。

[0072] 在数据发送机 2 和数据接收机 3 之间、建立与卫星链路 4a 无关的双向通信信道 9。就象其名字的含义，双向通信信道 9 允许在数据发送机 2 和数据接收机 3 之间进行双向通信。因此，在下文中，双向通信信道 9 假定为用于通过因特网通信的通用通信信道。

[0073] 专线 7 是直接把数据发送机 2 和数据接收机 3 连接起来的通信装置。

[0074] 因特网 6 提供多种信息，如视频和音频信息。因特网服务提供者 (Internet service provider)5 在通信上将数据接收机 3 连接到因特网。假定数据发送机 2 连接到了因特网 6 上。

[0075] 允许在数据发送机 2 和数据接收机 3 之间进行数据交换的专线 7、电话线 8、以及双向通信信道 9 具有比卫星链路 4a 小的频带容量。通常，线路 7、8 和 9 提供几到几百 Kbps 的带宽。

[0076] 数据传输系统 1 还作为所谓的限制性数据接收系统被建立，该系统只允许一个特定的数据接收机或多个接收机接收所关心的数据。因此，数据传输系统 1 可将数据比方说只传送到数据接收机 3a（单点广播数据分配），仅传送到一组数据接收机 3a 和 3b（多点广播数据分配），或传送到所有的数据接收机 3a、3b 和 3c（广播数据分配）。

[0077] 在数据传输系统 1 中，数据发送机 2 到数据接收机 3 的数据发送如下所述：如图 7A 至 7G 所示，对要从数据发送机 2 发送到数据接收机 3 的数据进行封装。封装是由发送所关心的数据的数据发送机 2 执行的一个过程。在第一封装步骤中，根据第一协议对要发送到数据接收机 3 的数据进行封装。在第二封装步骤中，根据第二协议对根据第一协议封装的数据进一步封装。封装过程就是将未处理的数据放到、根据由给定的通信协议所规定的传输格式、而形成的囊 (capsules)（例如，包或帧）中。随着数据被放到这样的囊中，它们的传输就变得可控制。

[0078] 在第一封装步骤中，通过将整个要被发送到数据接收机 3 的目标数据放到实际数据部分中来形成囊，该实际数据部分备有与该所述实际数据部分相关的附加信息部分。对囊中的实际数据部分进行加密。下文是对第一封装步骤的更加详细的描述。

[0079] 如图 7A 所示，IP（网际协议）数据报 101 由基于网际协议的数据构成。IP 数据报 101 中的数据是为数据接收机 3 指定的。IP 数据报的首标包括在，比方说，因特网上，标识该数据报的目的的目的地址。

[0080] IP 数据报 101 并不限于根据网际协议来建立；可替换地，它可根据以太网协议来建立。

[0081] 如图 7B 至 7D 所示，数据发送机 2 根据上述的第一协议对数据进行封装。示例性地，可采用用于DVB(Digital Video Broadcasting,数字视频广播）的多协议封装作为第一

协议。

[0082] 如图 7B 所示，数据发送机 2 根据第一协议执行数据封装，首先对 IP 数据报进行填充（例如，增加填充部分 102），以使该数据部分的长度为 64 比特的整数倍。例如，将 0 至 63 比特的填充部分附在 IP 数据报 101 的后头。填充部分中的所有比特都为“1”。因为当数据部分的长度为 64 比特的整数倍时，该数据部分更适于加密，所以用填充来使数据报保持为预定的数据长度。按第一协议的格式放置的数据部分在下文称之为节 (section)。

[0083] 如图 7C 所示，添加了填充 102 的节然后被数据发送机 2 加密。加密通过使用加密密钥来执行。该加密密钥是用于对要发送到数据接收机 3 的信息进行加密的会话密钥（稍后描述）。这里采用的加密方法是基于通用密钥密码系统，例如，Triple-DES 的块加密方法。Triple-DES 加密是当今最坚固的公共密钥密码系统之一，并且容易在硬件的基础上实现高速加密。与大多数公共密钥密码系统不同，该加密过程很快，足以跟上以 30Mbps 这样高的速率进行的传输。

[0084] 如图 7D 所示，数据发送机 2 向加密的节数据部分 104 添加了一个节首标 103 和一个用于检错的尾标 105。

[0085] 加密的节数据部分 104 采取 MAC(Media Access Control，媒体访问控制）帧结构。在建立 MAC 帧的过程中，向该数据部分添加 MAC 首标。参照 MAC 首标使得对放置在该帧中的数据的目的地址控制更加容易。具体地说，MAC 帧中有授权接收该帧中存储的数据的、数据接收机的目的地址。

[0086] 节首标 103 提供了足够容纳 48 比特的目的地址宽的数据空间。更具体地说，节首标 103 具有在其中形成的 MAC 首标，以便保存目的地址。在节首标 103 中提供拥有 48 比特的目的地址的数据空间、这解决了前面所述的第一问题，即，对可配置的数据接收机数目的限制。这是因为扩展的地址空间可容纳大量的用于标识加密密钥的信息。此外，因为在数据报传输时，不必根据 IP 目的地址对 IP 数据报 101 的包 ID（稍后描述）进行调整，所以解决了上述关于与网际协议亲和性差的第四个问题。

[0087] 尾标 105 被编码用于 CRC(Cyclic Redundancy Checking，循环冗余校验）。CRC 是为接收 MAC 帧中的数据的数据接收机 3 而设计的，以便检验该帧是否被通过卫星链路正常地传输。示例性地，CRC 涉及在 32 比特中的编码。

[0088] 至此，描述了根据第一协议对要发送的数据进行的封装。下面将描述如何根据第二协议对根据第一协议封装的数据进行进一步的封装。

[0089] 根据第二协议的数据封装就是将根据第一协议封装的数据分割成多个包。第二协议是规定了根据 MPEG 2 将数据封装到 TS（传输流）包中的协议。TS 包允许通过大容量的数字线路、多路复用和传输各种数据，例如音频和视频信号、以及其他数据。如图 7E 至 7G 所示，数据被根据第二协议封装到多个 TS 包 106、107 和 108 中。TS 包 106、107 和 108 每个都由 TS 首标 HTS 和 TS 净荷部分 P 组成。TS 净荷部分 P 包含已经根据第一协议被分割的、并且被封装了的数据。每个 TS 包的 TS 首标 HTS 由如图 4 所示的包 ID(PID) 部分和加扰控制部分构成。按照惯例，把目的地址写到 PID 部分和加扰控制部分的事实、限制了目的地址信息的范围。在本实施例中，由于把目的地址写到了节首标 103，所以消除了该缺点。

[0090] 以上描述说明了根据第二协议的数据的封装。如上所述，数据发送机 2 根据第一和第二协议、以多路复用的方式、对要发送到数据接收机 3 的数据（IP 数据报）进行封装。

该封装的数据被发送到通信卫星 4。

[0091] 因为限制性数据传输控制是在两个级 (levels) 上，例如在 TS 包级上和在节级上，独立地实行的，所以前面描述的第二、第五和第六个问题也得到了解决。

[0092] 更具体地说，保证了大量的关于加密密钥的信息，同时又绕过了第二个问题，即，随着使用的 PID 数目增加而剧增的传输费用。

[0093] 第五个问题，即，需要向每个应用提供其自己的控制方法的问题已不再存在。新引进的应用能被本实施例迅速地处理。

[0094] 第六个问题也被该实施例绕开了，即，允许在现有的因特网上使用鉴定首标 (AH) 和安全封装的净荷 (ESP)。

[0095] 上述的 IP 数据报的封装适用于通过卫星链路 4a 把数据报传送到数据接收机 3 时的情况。在双向通信信道 9 上，使用普通的因特网方法来传输 IP 数据报，而不依靠专门的封装。

[0096] 下面将描述数据发送机 2 如何使用加密密钥对数据进行加密，以及数据接收机 3 如何使用该加密密钥（用作解密密钥）对加密数据进行解密。图 8 中建立的数据发送机 2 和数据接收机 3、通过图 6 所示的通信信道进行互连．数据发送机 2 根据第一协议（使用节）把数据发送到数据接收机 3。在上文，已经参照图 5 的传统的构成对根据第二协议（使用 TS 包）的数据传输进行了说明。对比图 8 中的本发明的组成、和图 5 中的传统的构成可以看出，本实施例用两个密钥级来操作，即，用于数据发送机和数据接收机进行加密和解密的会话密钥 Ks 24 和主密钥 Km 25，而传统的构成依靠三个密钥级的方案。本实施例节省了一个密钥级。

[0097] 在众所周知的通用密钥密码系统下，数据发送机 2 和数据接收机 3 具有会话密钥 Ks 24，用于对数据加密和解密。为了区别起见，数据接收机 3 拥有的会话密钥 Ks 在下文称之为会话密钥 Ks 34。

[0098] 数据发送机 2 使用会话密钥 Ks 24、对要发送到一个特定的数据接收机或多个接收机的数据进行加密。数据接收机 3 使用会话密钥 Ks 34、对收到的加密数据进行解密，从而从解密的数据中提取出有意义的信息。

[0099] 定期对会话密钥 Ks 24 和 34 进行更新，例如，每天，按小时或按分钟。即使窃听者碰巧在在某一时间点上知道了会话密钥 Ks 24，他们也只能在密钥授权的有限的时间范围内窃听数据。会话密钥 Ks 的更新将在后面详细讨论。

[0100] 根据上边提到的 Tripe-DES、会话密钥 Ks 24 被用来对图 7C 所示的节数据部分进行加密。

[0101] 主密钥 Km 25，象会话密钥 Ks 24 一样，被数据发送机 2 和数据接收机 3 二者拥有。每个数据接收机 (3A，3B，3C) 被分配了各自唯一的主密钥。为了区分起见，数据接收机 3 拥有的主密钥 Km 在下文称之为主密钥 Km 35。

[0102] 主密钥 Ks 25 永远不会在数据发送机 2 和数据接收机 3 之间发送。任何主密钥也不会被放到通信信道上。主密钥是一种在任何情况都不应该被除了它的拥有者之外的任何一方所获悉的加密密钥。

[0103] 数据发送机 2 在把会话密钥 Ks 发送到数据接收机 3 之前、使用主密钥 Km 对其进行加密；并且，数据接收机 3 使用主密钥 Km、对接收的加密的会话密钥 Ks 进行解密。更具

体地说，数据发送机 2 使用主密钥 Km 25 预先将会话密钥 Ks 24 加密，并把该加密的会话密钥 Ks 24 发送到数据接收机 3。一收到加密的会话密钥 Ks 24，数据接收机 3 就使用它自己的主密钥 Km 对接收的密钥进行解密（以便提取会话密钥 Ks 34）。

[0104] 会话密钥 Ks，经历了根据主密钥 Km 的加密、和然后解密的过程，可以防止在从数据发送机 2 到数据接收机 3 的数据传输的过程中、被潜在的窃听者肆意窃听。

[0105] 数据接收机 3 使用解密的会话密钥 Ks、对已经使用所述会话密钥 Ks 加密了的发送数据进行解密。数据接收机 3 从解密的数据中提取有意义的信息。

[0106] 根据 Triple-DES，用主密钥 Km 对会话密钥 Ks 进行加密和解密。另一种方法，可以采用一种公共密钥密码系统。该可替换的系统的优点在于，不象数据的加密和解密过程，该系统的那些密钥不必被高速执行，它们也确保了安全性。

[0107] 与会话密钥 Ks 24 不同，主密钥 Km 25 不随时间更新。

[0108] 下面描述如何对会话密钥 Ks 24 进行更新。是数据发送机 2 主动更新会话密钥 Ks 24 的。使用主密钥 Km 25 加密的会话密钥 Ks 24（以下称之为加密的会话密钥 Km(Ks)）、也是由数据发送机 2 主动发送的。

[0109] 双向通信信道 9 的使用使数据接收机 3 能够主动地请求会话密钥 Ks。如此，各个数据接收机 3a、3b 和 3c 便能从数据发送机 2 快速而可靠地获得他们需要的会话密钥。示例性地，通过数据接收机在下述情况中对密钥的主动请求，使快速可靠地获得会话密钥 Ks 24 成为可能：一个新的数据接收机 3 加入到数据传输系统 1 中；已经停止工作且又从故障中恢复的数据接收机 3 再加入到系统 1 中；或数据接收机 3 未能正确地接收会话密钥 Ks。从故障中的恢复和会话密钥 Ks 的更新、由分别包括在数据发送机 2 和数据接收机 3 中的 CA(Conditional Access，条件存取）管理单元 23 和 33 来管理。这两个单元 23 和 33 彼此之间相互通信，以便交换其间的控制信息。

[0110] 上述特性使克服前面提到的第三个问题成为可能，即，在一个仅仅依靠卫星链路作为通信信道的数据传输系统中，数据发送机不能知道信息是否已经被正确地发送到目的数据接收机。

[0111] 数据发送机 2 既可通过单向的卫星链路 4a、也可通过双向的通信信道 9、把会话密钥 Ks 发送到数据接收机 3。

[0112] 会话密钥 Ks 的更新步骤如图 9 的流程图所示。

[0113] 在某一时间点上，数据接收机 3 拥有两个会话密钥 Ks 34，即，会话密钥 Ks_even（偶）和会话密钥 Ks_odd（奇）。数据接收机 3 使用这两个会话密钥 Ks_even 和 Ks_odd 中的一个、对从数据发送机 2 发送的信息和数据进行解密。

[0114] 由写在图 7D 所示的节首标 103 中的信息、标识当前使用的会话密钥是两个中的那一个。例如，如图 10 所示，节首标 103 包括：表 ID(table_id)，MAC 地址部分 (MAC_address_1，MAC_address_2，MAC_address_3，MAC_address_4，MAC_address_5，MAC_address_6)，节信息部分 (section_length（节长度），section_number（节号），last_section_number（最终节号）)，ssi(section_syntax_indicator（节句法指示符）)，pi(private_indicator（私有指示符）)，rsvd(resverd（保留的）)，psc(payload_scramble_indicator（净荷加扰指示符）)111，asc(address_scramble_indicator（地址加扰指示符）)，LSf(LLC_SNAP_flag（标志）)，和 cni(current_next_indicator（当前下一个

指示符))。psc 111 指示当前使用的会话密钥是两个中的哪一个。示例性地，psc 111 由两比特信息构成。如果 psc 的高位是“0”，就意味着会话密钥 Ks_even 正被使用；如果 psc 的高位是“1”，就意味着会话密钥 Ks_odd 正被使用。

[0115] 在图 9 的步骤 S1 中，检查看当前使用的是哪一个会话密钥 Ks。在步骤 S2 中，数据接收机 3 被计时器触发，启动会话密钥的更新处理。

[0116] 在步骤 S3 中，数据接收机 3 更新在一个对应表中找到的当前会话密钥 Ks 的标志，在该对应表中，MAC 地址与会话密钥 Ks 相对应。示例性地，如图 11 所示，数据接收机 3 拥有一个 MAC 地址与会话密钥 (MAC-address-to-session-key) 对应表。当前被使用的会话密钥 Ks 的标志根据该表进行更新。更新操作把 psc 111 的高位转换成，比方说，“0”。

[0117] 在步骤 S4 中，数据接收机 3 根据 psc 111、对包含在节中的 IP 数据报进行解密。更具体地说，如果 psc 的高位设成“0”，则数据接收机 3 停止使用当前的会话密钥 Ks_odd（当 psc 高位是“1”时使用的），并转换到会话密钥 Ks_even 用于解密。如果 psc 的高位设成“1”，则数据接收机 3 停止使用当前的会话密钥 Ks_even（当 psc 高位是“0”时使用的），并转换到会话密钥 Ks_odd 用于解密。

[0118] 在步骤 S5 中、且在会话密钥 Ks 再次改变之前，数据发送机 2 使用主密钥 Km 24 对下一个会话密钥 Ks 进行加密，并把该加密的密钥发送到数据接收机 3。

[0119] 加密的会话密钥 Km(Ks) 通过卫星链路 4a 或通过双向通信信道 9 发送。用于传输的协议应该是一种要求确认的协议，例如，TCP/IP（传输控制协议 / 网际协议）。该协议能使会话密钥 Ks 可靠地从数据发送机 2 传输到数据接收机 3。

[0120] 在步骤 S6 中、且当会话密钥的传输正在进行时，数据接收机 3 更新图 11 所示的 Mac 地址与会话密钥对应表。就是说，当前使用的会话密钥 Ks 被下一个会话密钥 Ks 代替。

[0121] 在步骤 S7 中，数据接收机 3 核实下一个会话密钥 Ks 现在已被数据接收机 3 持有。在步骤 S8 中，数据接收机 3 切换到下一个会话密钥 Ks。步骤 S8 至 S13 构成将 psc 的高位设成“1”，从而使会话密钥 Ks_odd 用于解密的过程。该过程从步骤 S7 开始；或者，如果数据接收机 3 发现当前的会话密钥 Ks 是会话密钥 Ks_even(psc 的高位 :0)，则从步骤 S1 开始。

[0122] 通过执行以上步骤，数据发送机 2 给数据接收机 3 传送已可靠地更新的会话密钥 Ks。数据接收机 3 立即切换它的两个会话密钥，从而不间断地根据当前有效的会话密钥 Ks 解密数据。会话密钥 Ks 24 的更新频率可依据传输处理的持续时间而灵活地改变。

[0123] 如上所述，会话密钥 Ks 在数据接收机 3 内部定期更新。数据接收机 3 使用如此更新的会话密钥 Ks、对与密钥一起发送的信息和数据进行解密。

[0124] 下面描述数据发送机 2 在发送数据之前执行的步骤，以及数据接收机 3 在收到数据之后执行的步骤。数据发送机 2 在发送数据之前执行的步骤示例性地示于图 12 的流程图中。数据接收机 3 在收到数据之后执行的步骤示例性地示于图 14 的流程图中。

[0125] 在图 12 中的步骤 S21 中，数据发送机 2 接收要从发送机 2 本身、或从连接到双向通信信道 9 的接口被发送到数据接收机 3 的 IP 数据报。数据发送机 2 还根据来自因特网 6 的存取信息、从信息中心接收信息。

[0126] 在步骤 S22 中，数据发送机 2 检查 IP 数据报的目的地址部分，以便知道基于第一协议的目的地址。例如，数据发送机 2 参照象图 13 所示的这样一个 IP 地址与 MAC 地址对应表，根据第一协议，找出数据接收机 3 的目的地址，该表由数据发送机 2 保留。

[0127] 找到目的地址以后，数据发送机 2 根据该目的地址创建一个节。此时，数据发送机 2 向数据部分提供所需要的比特“1”填充，以便使数据部分成为 64 比特的倍数。

[0128] 在步骤 S23 中，数据发送机 2 通过检查象图 11 所示的这样一个 Mac 地址与会话密钥对应表中的、当前使用的会话密钥 Ks 24 的标志 112，来提取那个密钥 Ks。数据发送机 2 使用如此提取出的会话密钥 Ks、对图 7C 所示的节的数据部分进行加密。此时，数据发送机 2 检查当前的会话密钥 Ks 的标志，并把该标志内容设成图 11 所示的节首标中的 psc 111 的高位。

[0129] 在步骤 S24 中，数据发送机 2 把整个节 109 分割成图 7E 至 7G 所示的、TS 包 106、107 和 108 的净荷部分 P。对每个 TS 包 106、107 和 108 补充预定的 PID。如第二协议所要求的那样，在把净荷 P 输出到卫星链路 4a 上之前，对其进行加密。

[0130] 前面的描述已经说明了数据发送机 2 在数据发送之前的、准备工作的步骤。通过卫星链路 4a 收到数据的数据接收机 3 执行以下步骤。

[0131] 在图 14 的步骤 S31 中，数据接收机 3 对通过卫星链路 4a 收到的 TS 包 106、107 和 108 进行解密，以便从其中重建整个节 109。

[0132] 在步骤 S32 中，数据接收机 3 提取节的目的地址（即，MAC 地址）。在步骤 S33 中，数据接收机 3 进行检查，看是否在图 15 所示的 Mac 地址与会话密钥对应表中找到了 MAC 地址。就是说，执行一项检查，看该节是否包含了授权数据接收机 3 接收的数据。如果在步骤 S33 中没有找到 MAC 地址，数据接收机 3 就转到步骤 S34、并丢弃该数据。如果检测到了 MAC 地址，数据接收机 3 便到达步骤 S35，在该步骤中，从节首标 103 中提取图 10 所示的 psc 111。数据接收机 3 检查 psc 111 的高位比特，以便看两个会话密钥 Ks 中的哪一个为当前有效的，选中该有效的会话密钥 Ks。

[0133] 在步骤 S36 中，数据接收机 3 根据 Tripe_DES、用检索的会话密钥 Ks 对节数据 104 进行解密。在步骤 S37 中，数据接收机 3 从解密数据中提取 IP 数据报。示例性地，数据接收机 3 从加在解密的数据部分前的 IP 首标中、读取总长度字段 113（图 16 中），从字段 113 中找出 IP 数据报的长度，并且提取经过相应计算的整个 IP 数据报。在该过程中，除去了加密时被附加的额外的填充，以便原样提取目标 IP 数据报。

[0134] 通过执行上述步骤，数据发送机 2 在数据发送之前、执行必要的处理，并且数据接收机 3 执行与收到的数据相关联的过程。数据接收机 3 因此接受已经寻址到那里的信息和数据。

[0135] 上述构成的数据传输系统 1 能够解决前边提到的按常规碰到的问题。

[0136] 可以对数据传输系统 1 进行变形。图 17 所示的数据传输系统 201 是系统 1 的第一变形。数据传输系统 201 的特点在于数据接收机 3 作为 IP 路由器提供。

[0137] 数据传输系统 1 让数据接收机 3a 直接接收 IP 数据报。与之相反，数据传输系统 201 让它的数据接收机 3a 用作 IP 路由器。该体制使得数据接收机 3a 从卫星链路 4a 接收的数据、能够传送到没有与卫星链路 4a 接口的计算机 203a 和 203b，计算机 203a 和 203b 通过局域网 (LAN)202，例如以太网，连接到数据接收机 3a。这样，数据发送机 2 和数据接收机 3a 不仅可以通过数据接收机 3a，还可以通过连接到数据接收机 3a 的局域网 202 上的所有计算机 203a 和 203b，来提供限制性数据接收控制。更具体地说，在图 13 的数据发送机 2 的 IP 地址与节的目的地址 (MAC 地址）的对应表内，用每一个都代表了一组多个 IP 地址的 IP

网络地址、来替换单个的 IP 地址。为实现在数据接收机 3a 这方、与计算机 203a 和 203b 那方之间的限制性数据传输控制，要求数据传输控制方法或在 IP 协议级上执行、或在更高级的应用级上执行。这是因为数据传输系统 201 中的数据传输仅通过卫星链路 4a 执行。

[0138] 数据传输系统 301 是系统 1 的第二变形，其简要示于图 18 中。在数据传输系统 301 中，数据接收机 3a 用作在传送 IP 数据报中仅执行协议转换的网桥。数据传输系统 301 与系统 201 的不同点在于、系统 301 不执行路由选择。

[0139] 数据接收机 3a 对通过卫星链路 4a 接收的数据进行解密，以便从其中提取 IP 数据报。提取出的 IP 数据报被放到一个以太网帧中，并被传输到通用路由器 302。路由器 302 对 IP 数据报执行常规处理。因为没有必要其本身实行路由选择，所以，数据接收机 3a 结构简单，并与通用路由器一起使用。

[0140] 因为在不脱离其精神和范围的情况下，本发明可以有很多明显不同的实施例，所以，应该理解的是，除所附的权利要求中所限定的之外，本发明并不局限于其特定的几个实施例。

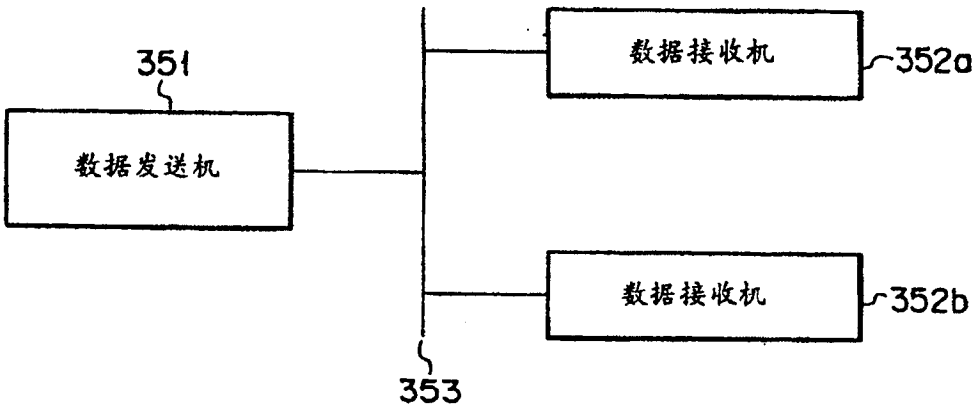


图 1

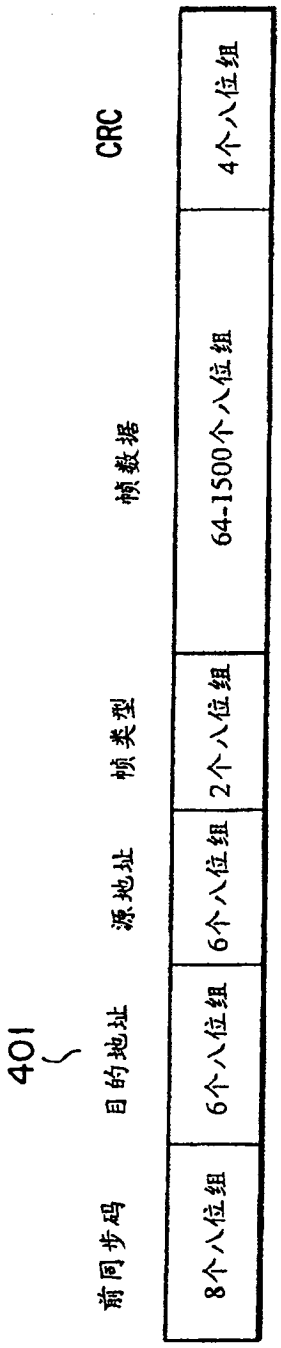

401
前同步码
目的地址
源地址
帧类型
帧数据
CRC
8个八位组
6个八位组
6个八位组
2个八位组
64-1500个八位组
4个八位组

图 2

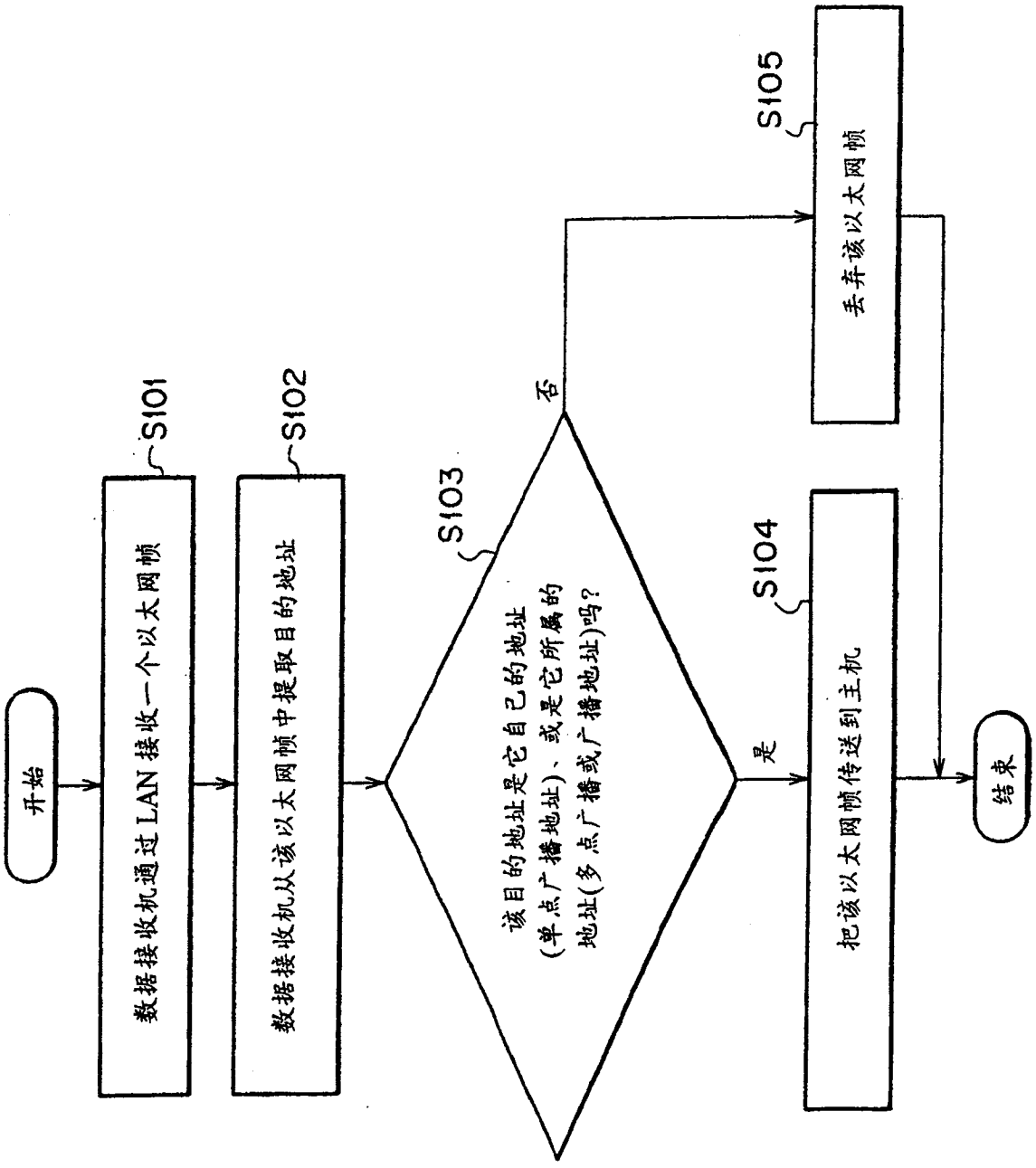

开始
S101
数据接收机通过LAN接收一个以太网帧
S102
数据接收机从该以太网帧中提取目的地址
S103
该目的地址是它自己的地址
(单点广播地址)、或是它所属的
地址(多点广播或广播地址)吗?
否
是
S104
把该以太网帧传送到主机
S105
丢弃该以太网帧
结束

图 3

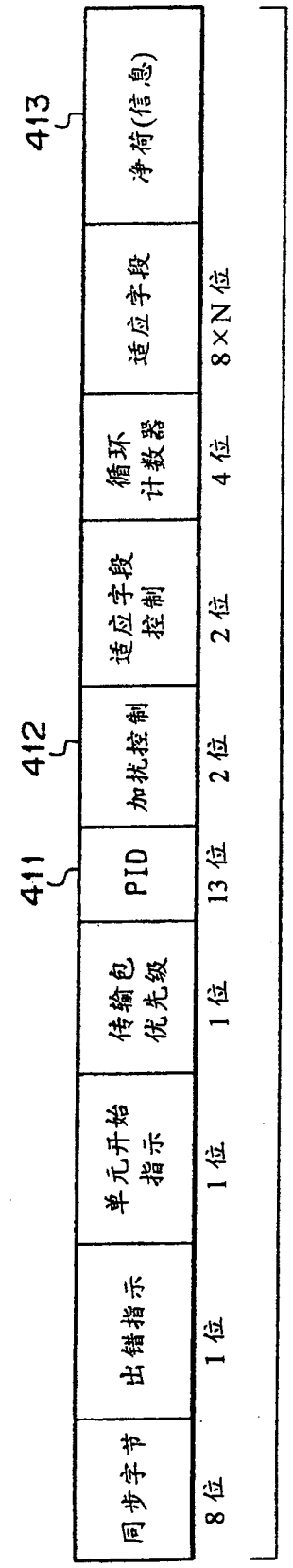

同步字节
出错指示
单元开始指示
传输包优先级
PID
加扰控制
适应字段控制
循环计数器
适应字段
净荷(信息)
411
412
413
8 位
1 位
1 位
1 位
13 位
2 位
2 位
4 位
8×N 位
188 字节

图 4

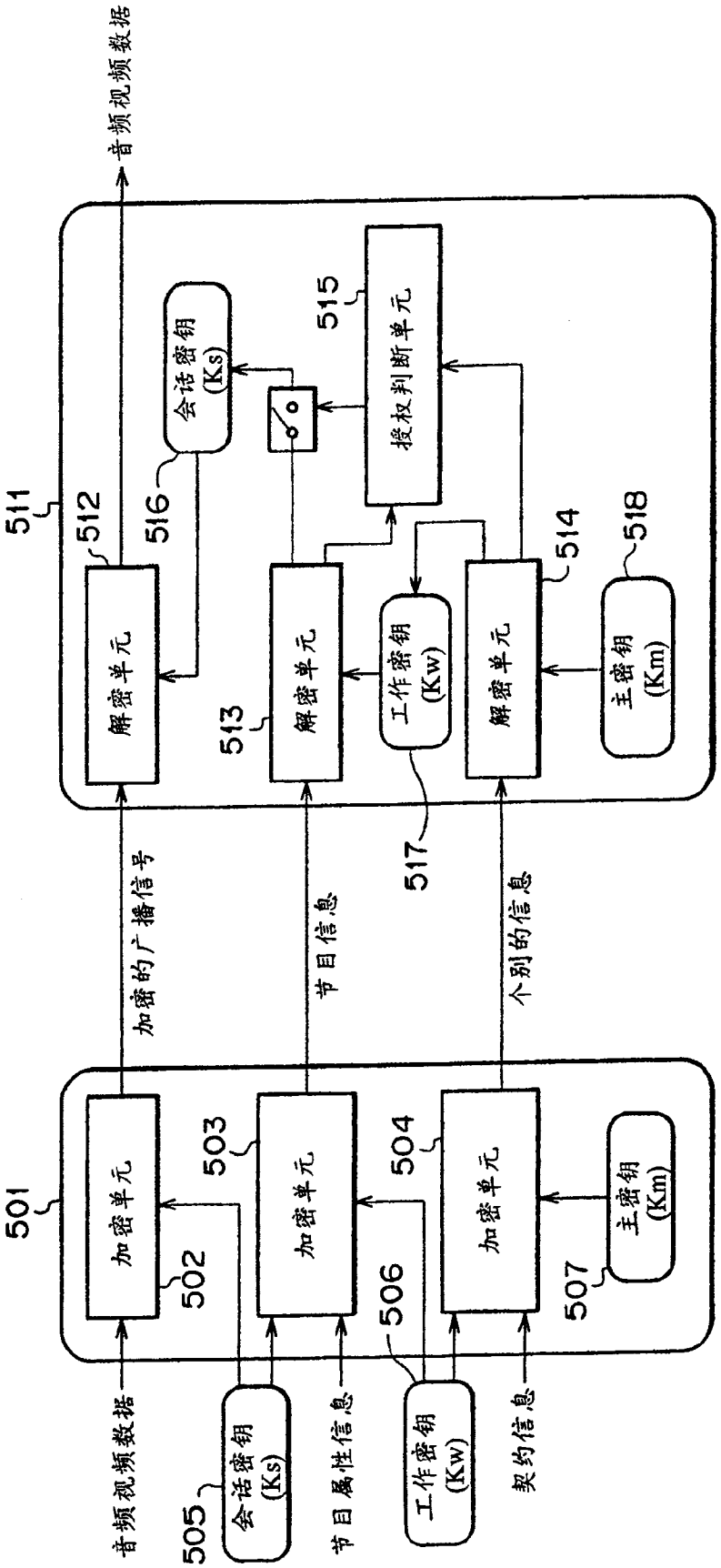

音频视频数据
节目属性信息
契约信息
会话密钥 (Ks)
工作密钥 (Kw)
主密钥 (Km)
加密单元
加密单元
加密单元
501
502
503
504
505
506
507
加密的广播信号
节目信息
个别的信息
517
511
512
513
514
515
516
518
解密单元
解密单元
解密单元
会话密钥 (Ks)
授权判断单元
工作密钥 (Kw)
主密钥 (Km)
音频视频数据

图 5

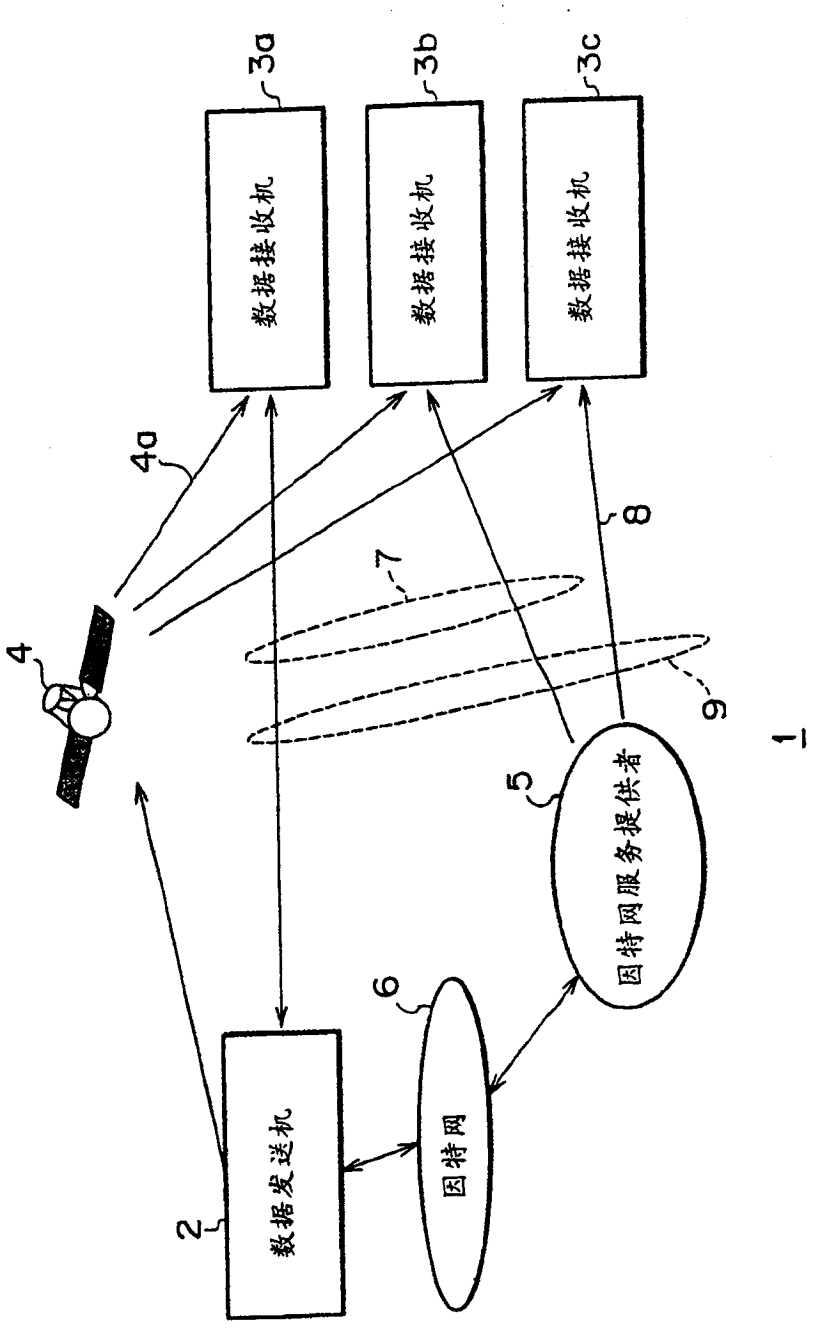


图 6

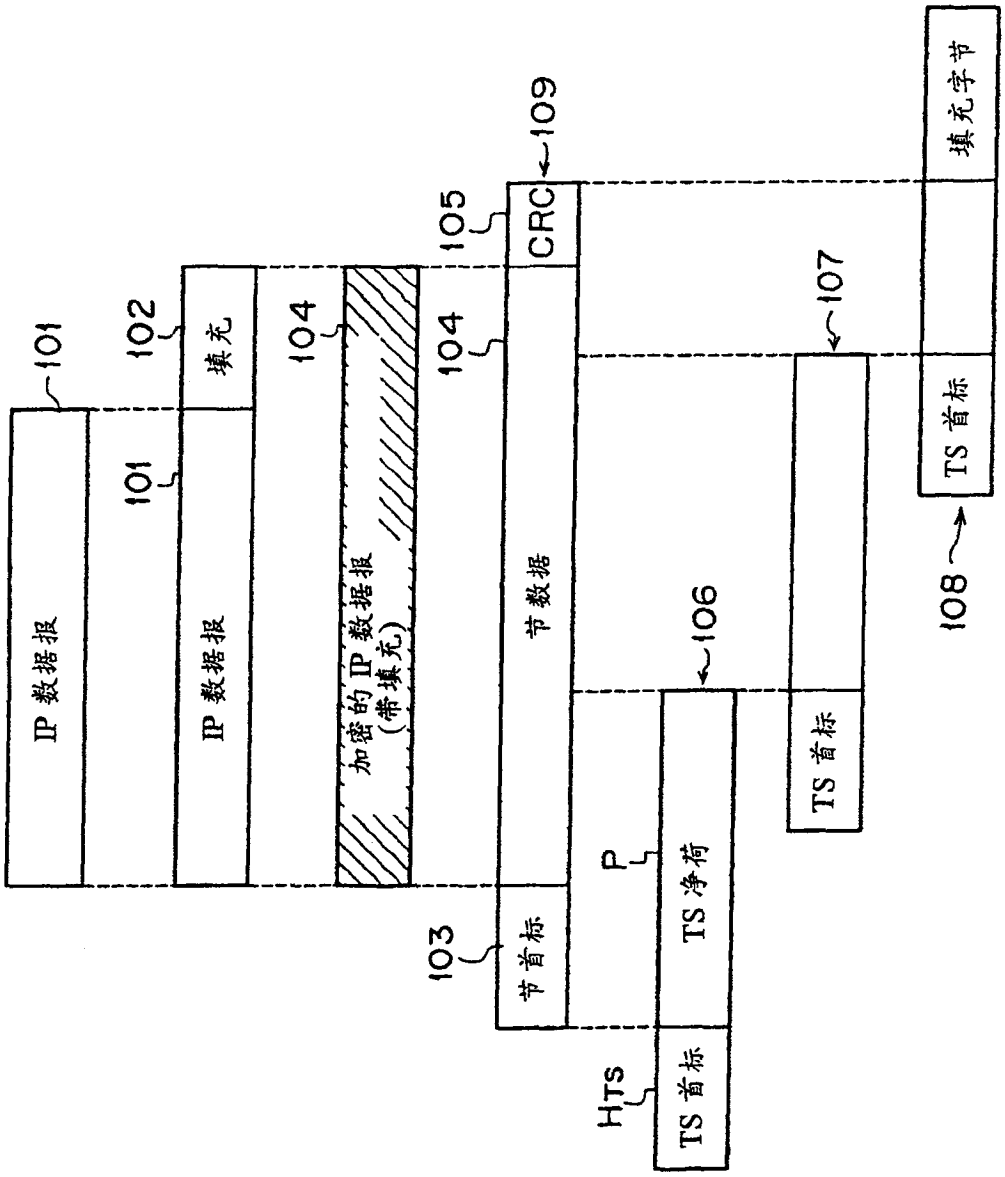


图 7A 图 7B 图 7C 图 7D 图 7E 图 7F 图 7G

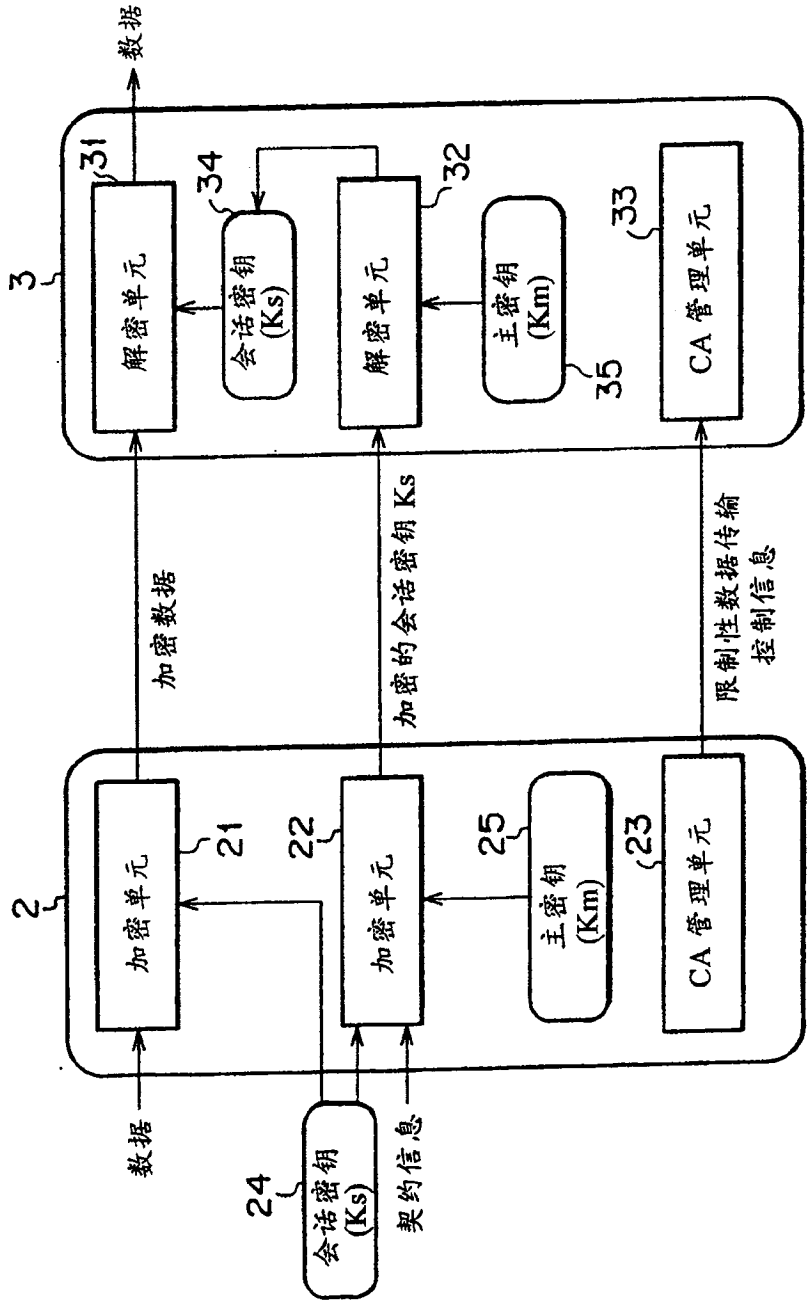

数据
3
31
解密单元
34
会话密钥 (Ks)
32
解密单元
主密钥 (Km)
35
33
CA 管理单元
加密数据
加密的会话密钥 Ks
限制性数据传输控制信息
2
加密单元
21
22
加密单元
25
主密钥 (Km)
23
CA 管理单元
数据
24
会话密钥 (Ks)
契约信息

图 8

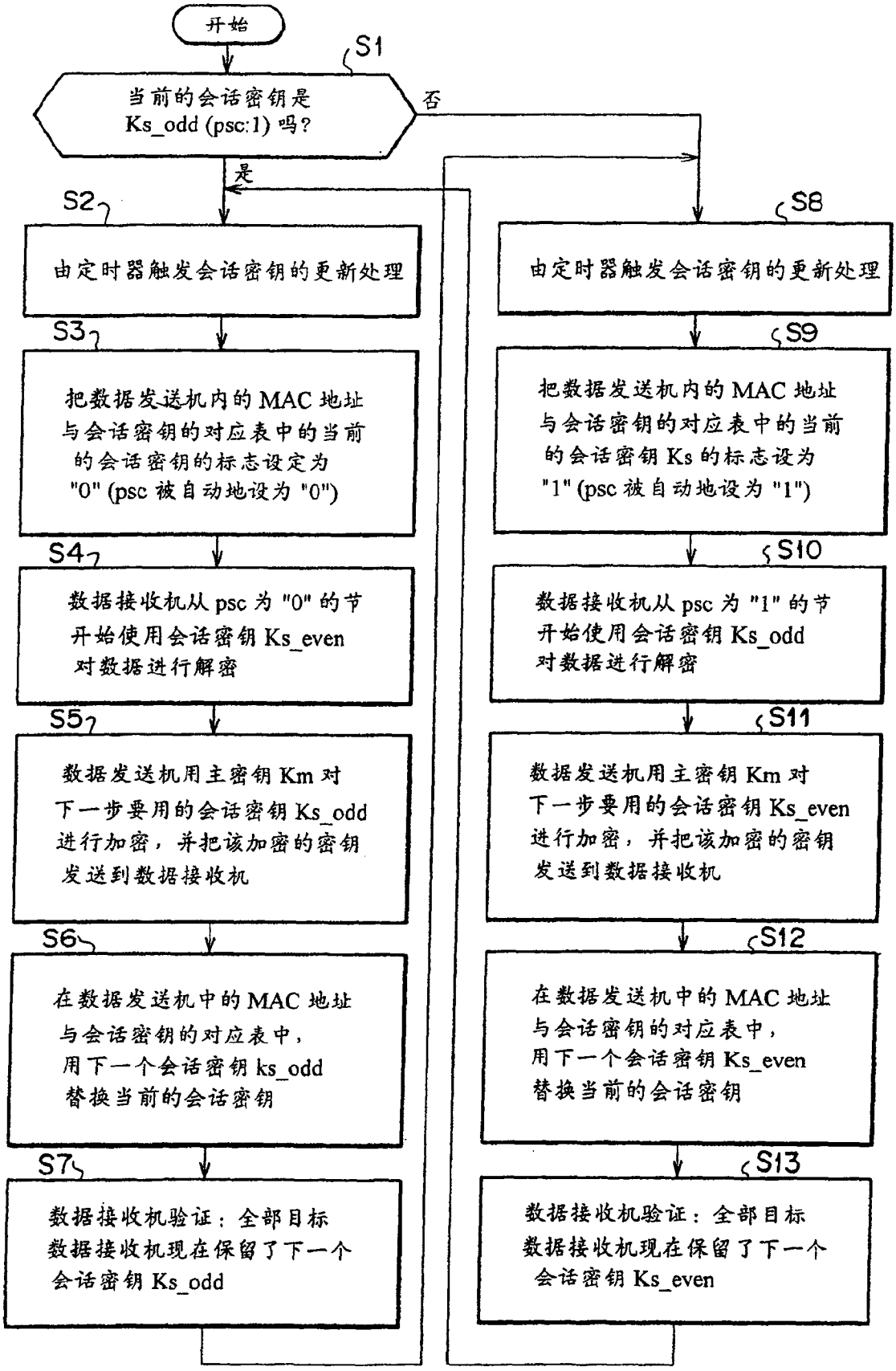
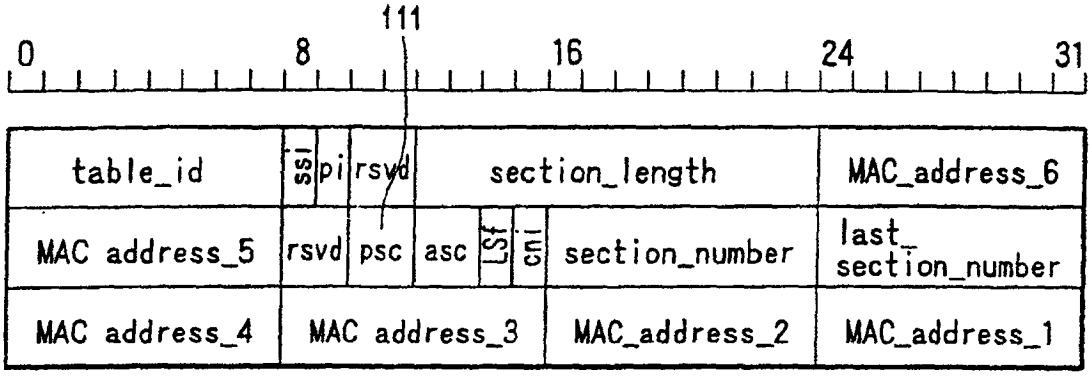

开始
S1
当前的会话密钥是 Ks_odd (psc:1) 吗?
否
是
S2
由定时器触发会话密钥的更新处理
S3
把数据发送机内的 MAC 地址与会话密钥的对应表中的当前的会话密钥的标志设定为 "0" (psc 被自动地设为 "0")
S4
数据接收机从 psc 为 "0" 的节开始使用会话密钥 Ks_even 对数据进行解密
S5
数据发送机用主密钥 Km 对下一步要用的会话密钥 Ks_odd 进行加密，并把该加密的密钥发送到数据接收机
S6
在数据发送机中的 MAC 地址与会话密钥的对应表中，用下一个会话密钥 ks_odd 替换当前的会话密钥
S7
数据接收机验证：全部目标数据接收机现在保留了下一个会话密钥 Ks_odd
S8
由定时器触发会话密钥的更新处理
S9
把数据发送机内的 MAC 地址与会话密钥的对应表中的当前的会话密钥 Ks 的标志设为 "1" (psc 被自动地设为 "1")
S10
数据接收机从 psc 为 "1" 的节开始使用会话密钥 Ks_odd 对数据进行解密
S11
数据发送机用主密钥 Km 对下一步要用的会话密钥 Ks_even 进行加密，并把该加密的密钥发送到数据接收机
S12
在数据发送机中的 MAC 地址与会话密钥的对应表中，用下一个会话密钥 Ks_even 替换当前的会话密钥
S13
数据接收机验证：全部目标数据接收机现在保留了下一个会话密钥 Ks_even

图 9



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

图 10

112

MAC 地址	Ks_even	Ks_odd	Ks 标志
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

图 11

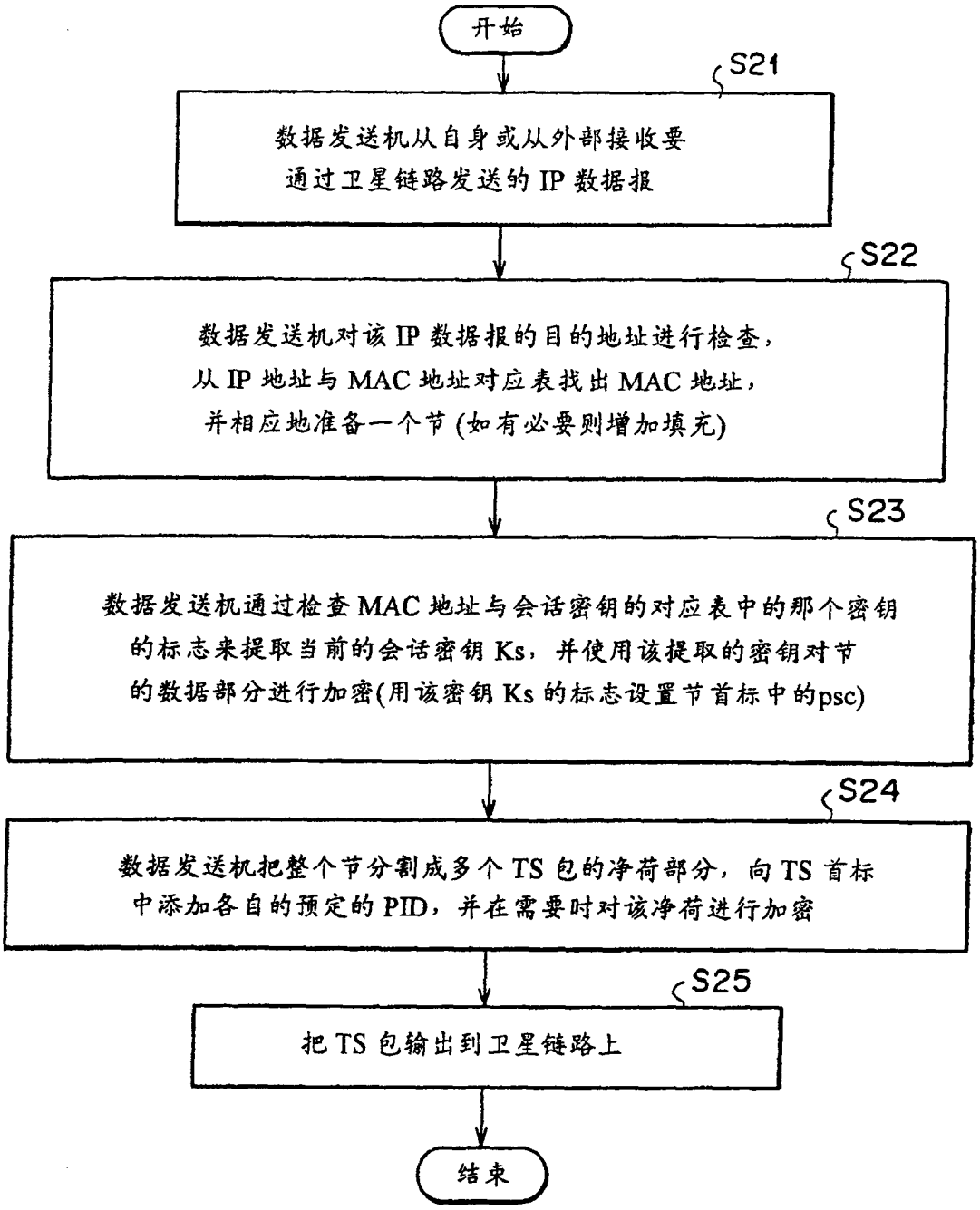

开始
S21
数据发送机从自身或从外部接收要
通过卫星链路发送的 IP 数据报
S22
数据发送机对该 IP 数据报的目的地址进行检查，
从 IP 地址与 MAC 地址对应表找出 MAC 地址，
并相应地准备一个节 (如有必要则增加填充)
S23
数据发送机通过检查 MAC 地址与会话密钥的对应表中的那个密钥
的标志来提取当前的会话密钥 Ks，并使用该提取的密钥对节
的数据部分进行加密(用该密钥 Ks 的标志设置节首标中的psc)
S24
数据发送机把整个节分割成多个 TS 包的净荷部分，向 TS 首标
中添加各自的预定的 PID，并在需要时对该净荷进行加密
S25
把 TS 包输出到卫星链路上
结束

图 12

IP 地址	位掩码	MAC 地址
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

图 13

MAC 地址	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

图 15

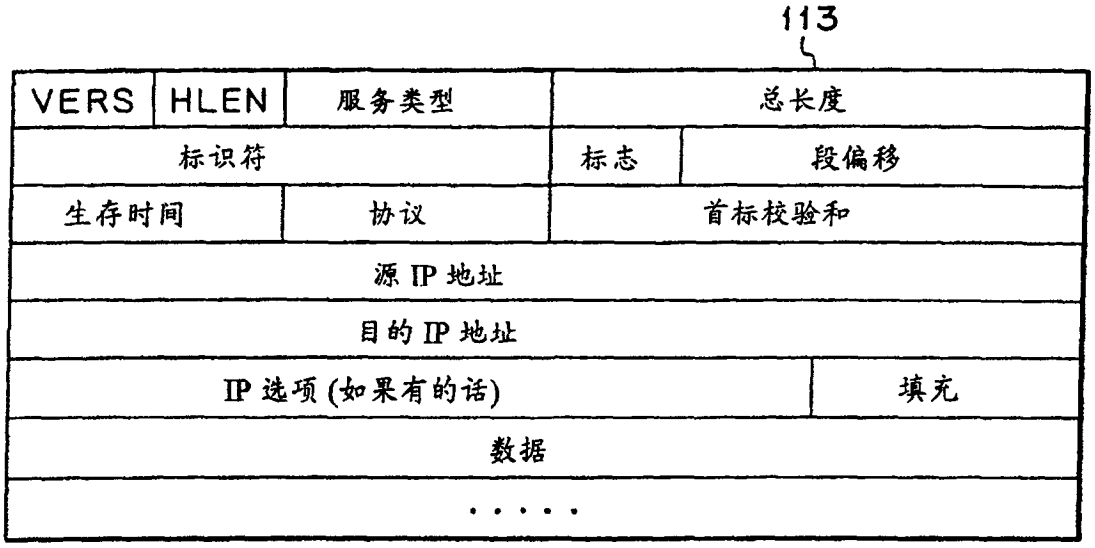


图 16

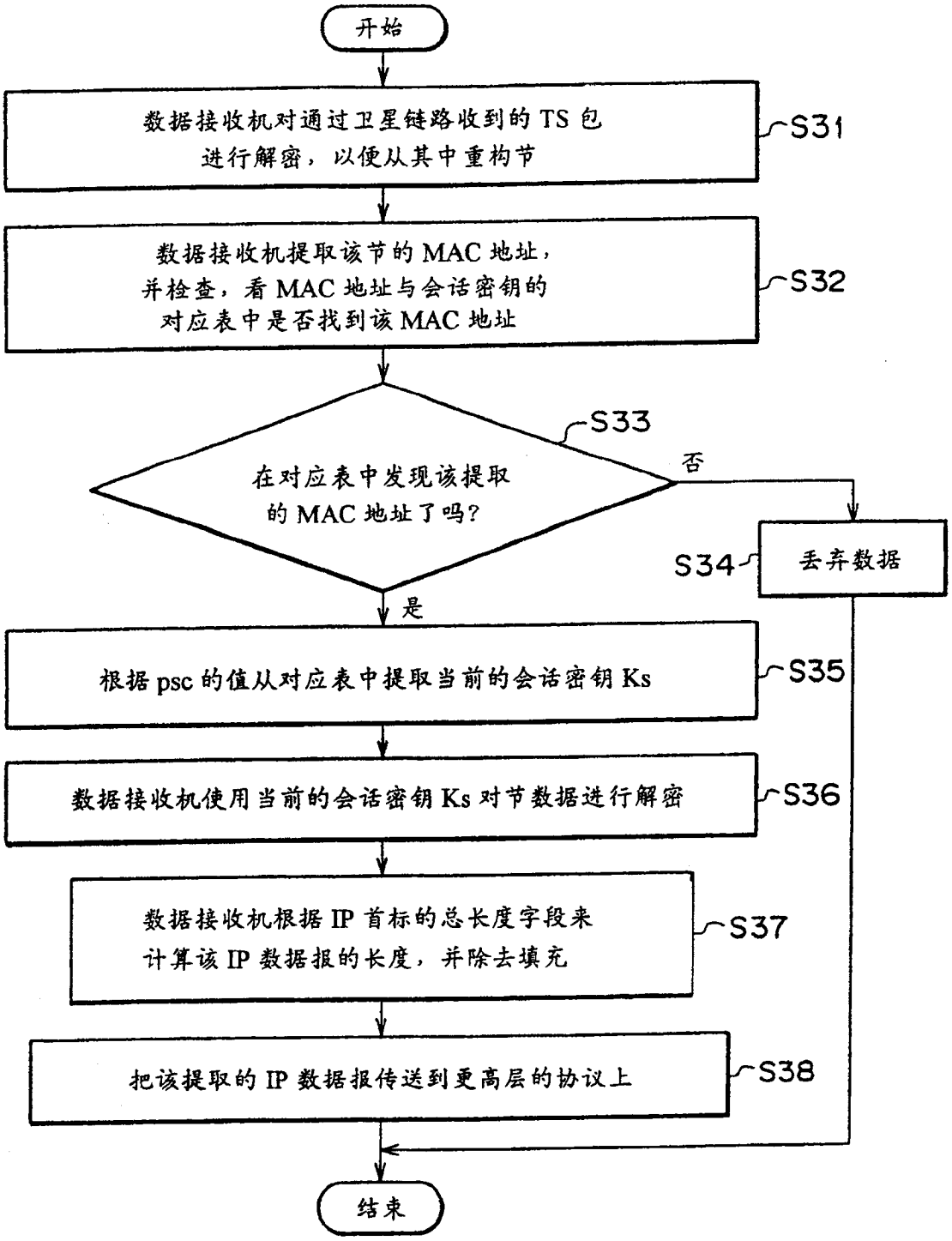

开始
数据接收机对通过卫星链路收到的 TS 包进行解密，以便从其中重构节
S31
数据接收机提取该节的 MAC 地址，并检查，看 MAC 地址与会话密钥的对应表中是否找到该 MAC 地址
S32
S33
在对应表中发现该提取的 MAC 地址了吗？
否
S34
丢弃数据
是
根据 psc 的值从对应表中提取当前的会话密钥 Ks
S35
数据接收机使用当前的会话密钥 Ks 对节数据进行解密
S36
数据接收机根据 IP 首标的总长度字段来计算该 IP 数据报的长度，并除去填充
S37
把该提取的 IP 数据报传送到更高层的协议上
S38
结束

图 14

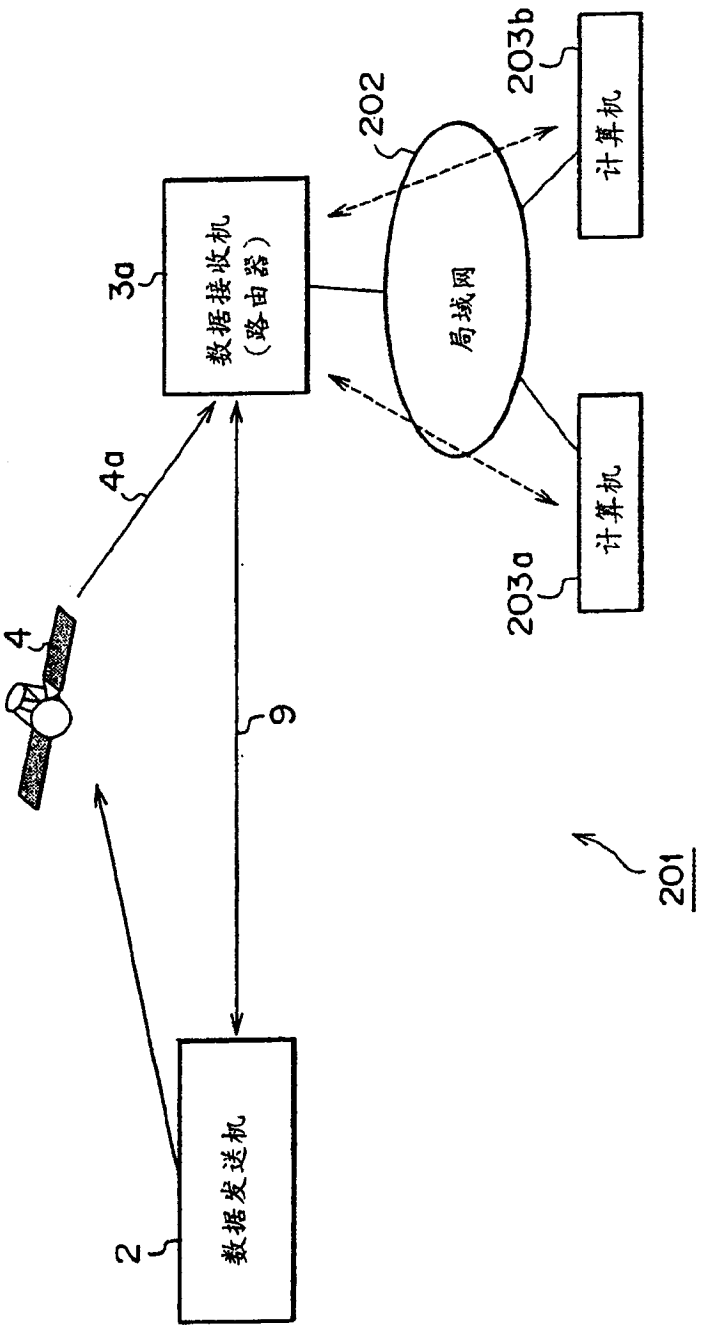


图 17

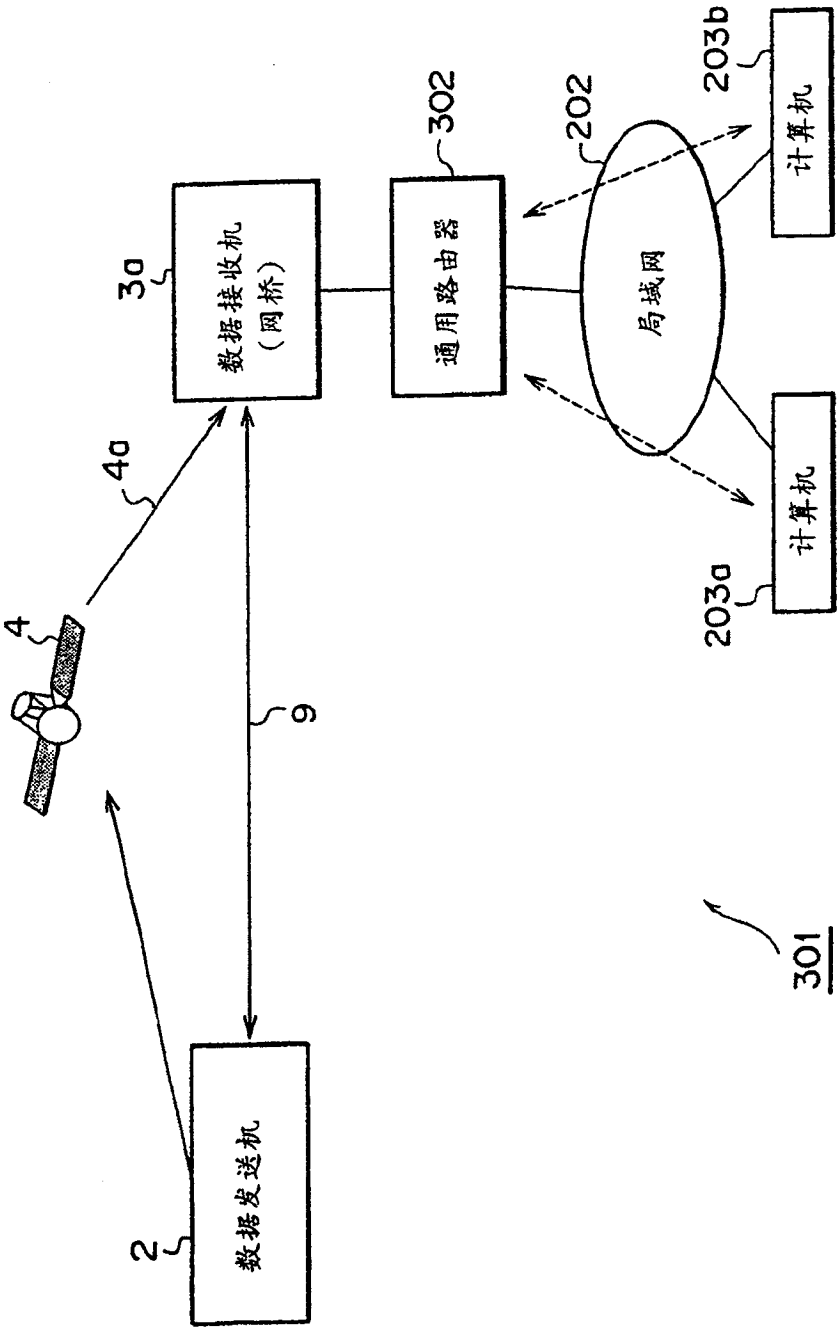

数据发送机
2
数据接收机
（网桥）
3a
通用路由器
302
局域网
202
计算机
203b
计算机
203a
301
4
4a
9

图 18