

1. 一种有条件访问系统，包括：

用于生成多个授权信息的生成装置(3002)；

用于接收所述授权信息的接收装置(2020)；和

5 直接与所述生成装置相连接的通信服务器(3022)，所述生成装置适于通过所述通信服务器与所述接收装置通信；

其特征在于，所述生成装置适于根据从所述接收装置经过所述通信服务器与该生成装置通信的数据生成要发送给所述接收装置的授权信息。

10 2. 如权利要求 1 的有条件访问系统，其特征在于，根据来自所述接收装置的命令生成所述授权信息。

3. 如权利要求 2 的有条件访问系统，其特征在于，所述命令是选自包括节目订购命令、用户请求修改命令和父母关注码重置命令的一组命令中的至少一个命令。

15 4. 一种有条件访问用户的有条件访问系统，包括：

用户管理系统(3004)；

与该用户管理系统(3004)相连的用户授权系统(3002)；以及

通信服务器(3022)，所述服务器与用户授权系统直接相连，即，不经过用户管理系统；

20 其特征在于，所述用户授权系统适于根据经所述通信服务器接收的数据生成授权信息。

5. 如权利要求 4 的有条件访问系统，其特征在于，还包括用户的接收器/解码器(2020)，该接收器/解码器经调制解调器和电话线(4002)与所述通信服务器相连。

25 6. 如权利要求 5 的有条件访问系统，其特征在于，根据来自所述接收器/解码器的命令生成所述授权信息。

7. 如权利要求 6 的有条件访问系统，其特征在于，所述命令是选自包括节目订购命令、用户请求修改命令和父母关注码重置命令的一组命令中的至少一个命令。

30 8. 如权利要求 4 的有条件访问系统，其特征在于：

所述通信服务器(3022)与用户的接收器/解码器(2020)连接；

所述用户管理系统(3004)用于存储用户信息；以及

所述用户授权系统(3002)用于根据经通信服务器接收的命令生成

要发送给接收器/解码器的授权信息，并且还包括：

接到通信服务器上的订单集中服务器(3207)，用于从接收器/解码器上接收命令以及从用户管理系统接收信息；

5 接到订单集中服务器上的授权服务器(3202)，用于根据来自订单集中服务器的授权请求识别用户并确认用户身份；以及

接到订单集中服务器上的信息生成器(3210)，用于根据从订单集中服务器上接收的命令生成授权信息；

10 所述订单集中服务器适于根据从所述授权服务器和所述用户管理系统至少一个上接收的数据给信息生成器发出所述命令，并将所述授权信息通过通信服务器发送到接收器/解码器上。

广播和接收系统以及用于上述系
统的有条件访问系统

5 技术领域

本发明涉及一种广播和接收系统，具体讲，涉及一种大众传播数字交互卫星电视系统，以及一种对其有条件访问的系统。

具有但不排它地说，本发明涉及到大众传播的广播系统，它具有某些或全部下列最佳特征。

10 *是一种信息广播系统，最好是一种无线电广播和/或电视广播系统；

 *是一种卫星系统（尽管可应用于有线或地面传输）；

 *是一种最好是使用动画专家组（Moving Picture Expert Group）（MPEG）、更好是使用 MPEG-2 的数字系统，是用于数据/信号传输的压
15 缩系统；

 *能提供交互。

更加具体地讲，本发明涉及所谓的付费电视（或广播），用户/观众可选择已付费了的节目/电影/游戏，这种方式称作有偿收视（PPV）或在数据下载时的所谓有偿下载（PPF）。

20 背景技术

借助此已知的 PPV 或 PPF 系统，用户/观众为了得到所选的产品就要花大量的时间。

例如在一个已知的系统中，为了获得所选产品就要执行以下步骤：

25 I) 用户先给所谓的用户管理系统（SMS）打电话，在该已知系统中，SMS 包括多个人工接线员，这些接线员回答用户的来电并将用户要选的产品的必要信息以及用户的财务状况通知给用户授权系统（SAS），该系统中也包括或涉及到多个通信服务器。

 II) 在将通信服务器与用户的电视机接通之前，接线员要核
30 查用户的财务状况，这样，所要的东西才能传给用户供观看。

 *在另一种已知系统中，人工接线员被自动应答服务器替代，这样，当用户打电话给 SMS 后，就会听到录音，按录音与 I) 中步骤相同

送入相同信息。

第二种结构可以减少第一种结构中固有的延误，在有大量的用户在同一时间要预订时第一种结构的装置更易过载。

但尽管用了第二种装置，用户还要长串数字的信息，从而产生了出错的机会而且耗时。

第三种结构涉及的是用户采用法国的 MINITEL 和英国的 PRESTEL 的系统的屏幕，这种系统取代了与上述第二种结构有关的语音服务器。MINITEL 和 PRESTEL 系统在用户端使用了调制解调器。

在所有这些装置中，用户都要耗时并输入使系统能工作的信息，以将用户所选的节目送到用户的电视机上。

在使用卫星电视系统的情况下，在用户接收所选的节目时还有另外的延时。

在 PPV 和 PPF 系统中，控制用户对节目的访问的码元被称作授权管理信息 (EMM)，它需要注入到系统中以使用户能访问节目。具体讲，EMM 是一种机制，借此可使代表节目的加密数据能被特定的单个用户解密。

在已知的卫星电视系统中，EMM 以规则间隔的 MPEG-2 数据流经卫星链路发送到用户的电视上。对于特定用户的 EMM 来说，在用户的 EMM 发射到达用户的电视机之前可能要拖延几分钟。

这种发射延时是前述用户手动输入某些数据到系统中的固有延时之外的延时。这两个延时的累加效果就可能是用户为得到所选节目要花 5 分钟。

发明内容

本发明所涉及的就是为了克服此问题的一些事物。

第一方面，本发明提供了一种有条件访问系统，它包括：

用于生成多个（最好是有条件访问的）信息的装置；以及

用于接收此信息的装置，所述接收装置适于通过直接与所述生成装置相连的通信服务器与所述生成装置通信。

最好，信息是用于发给（例如通过广播）接收装置的授权信息，所述生成装置适于根据从所述接收装置接收的数据生成授权信息。

生成装置可通过所述通信服务器或卫星异频雷达收发机将数字数据分组的信息发送给所述接收装置。

接收装置可通过调制解调器或电话线与所述通信服务器相连。

在一个有关的方面，本发明提供一种将有条件访问授权提供给用户的有条件访问系统，它包括：

用户管理系统；

5 与该用户管理系统相连的用户授权系统；

通信服务器，所述服务器直接与用户授权系统相连。

该系统还可以包括用户的接收器/解码器，该接收器/解码器经调制解调器和电话线与所述通信服务器相连，进而连到所述用户授权系统。

10 在第二方面，本发明提供一种广播和接收系统，它包括如上所述的有条件访问系统。

在第三方面，本发明提供一种广播和接收系统，包括：

用于生成多个与广播节目有关的授权信息的装置；

用于从所述生成装置接收所述信息的装置；

15 用于将接收装置接到生成装置上以接收所述信息的装置，所述连接装置能专用于接收装置与生成装置间的连接。

这种专用连接通常为硬导线连接和/或调制解调连接，还可通过移动电话系统实现连接。换言之，专用连接就是能够形成一个（从点到点的）通信信道。这正与通过空中和环境介质广播信息的情况相反。

20 这种连接装置在接收装置中通常为调制解调器。

在其紧相关的一个方面，本发明提供了一种广播和接收系统，它包括：

用于生成多个与广播节目有关的授权信息的装置；

用于经一调制解调器从所述生成装置接收所述信息的装置；以及

25 用于将所述调制解调器接到所述生成装置和所述接收装置上的装置。

上述特征的优点是使用户能比以前任何方式更快地获得所需的观看授权（通过 EMM），这部分地得益于 SAS 用的计算机码少于 SMS 所用的计算机码，SAS 可更有效地工作（并在实时工作），部分地得益于
30 SAS 本身可直接产生所要的 EMM，还部分地得益于 EMM 可经过专用链路（通常带调制解调）与用户或订户相通。

最好，生成装置经通信服务器与所述调制解调器相连，该服务器

最好包括所述生成装置或与之相连。

接收装置还可适于通过卫星异频雷达收发机接收所述授权信息。

接收装置可以是接收器/解码器，它包括用于接收压缩的 MPEG 型信号的装置、用于对所接收的信号解码以提供一个电视信号的装置，
5 以及将电视信号加到电视上的装置。

接收装置最好适于经所述调制解调器和连接装置与所述生成装置相连。接收装置可包括对最终用户插入的聪明卡读卡的装置，一旦用户插入聪明卡，其上所存的数据就能将信息从所述接收装置自动地发到所述生成装置。

10 另外，系统还可包括语音线路，使广播和接收系统的末端用户与生成装置通信。

从以上描述可以明白，本发明提供了两种装置，借助此类装置，可缩短用户访问所要节目所用的时间，最好同时使用两个装置以达最大节约时间的效果，但这些装置也可单个地使用。

15 根据本发明的再另一方面，提供了一种广播和接收系统，在广播端包括：

包括用于广播回叫请求的装置的广播系统；

而在接收端包括：

包括根据回叫请求回叫广播系统的装置的接收机。

20 通过提供可要求接收机回叫的广播系统，可使广播系统能从接收机上获得关于接收机状态的信息。

用于回叫广播系统的装置最好包括可接在电话系统上的调制解调器。通过带调制解调器的回叫信道，可用简单方法使本发明起作用。

25 另外，用于回叫广播系统的装置最好设成能向广播系统发送与接收机有关的信息。该信息可包括剩余代币的数量、预订对话数目等等。

广播系统最好包括存储信息的装置，这样在需要时可在最后时段进行处理。

30 广播装置最好能广播回叫请求，该回叫请求包括在给定时刻所作的回叫命令，回叫广播系统的装置可响应所述命令。通过将回叫请求设成晚于实际请求，则在系统上可获得更大的灵活性。

广播装置可以广播作为用于广播的一个或多个授权信息。

广播系统最好包括用于产生校验信息（例如一个随机号码）并将

其加到接收器的装置，该接收器包括用于对校验信息加密并送到广播系统的装置，广播系统最好还包括用于对从接收机上接收的校验信息解密并将其与原校验信息相比较的装置。按此方式，可以验知接收器是真的。

5 上述特征可以任何适当组合来组合。它们也可以从方法上加以体现。

附图说明

以下参照附图以纯粹举例的方式说明本发明的最佳特征，在附图中：

10 图 1 示出了本发明最佳实施例的数字电视系统的总体结构；

图 2 示出了上述数字电视系统的有条件访问系统的结构；

图 3 示出了上述有条件访问系统中所使用的授权管理信息的结构；

15 图 4 是本发明一个最佳实施例的用户授权系统（SAS）的硬件的概略图；

图 5 是上述 SAS 的结构概略图；

图 6 是构成上述 SAS 一部分的用户技术管理（Subscriber Technical Management）服务器的概略图；

20 图 7 是如上述 SAS 所实现的用于自动地更新预订的过程的流程图；

图 8 是上述自动更新过程中所使用的组预订位图的概略图；

图 9 示出了上述自动更新过程中所使用的 EMM 的结构；

图 10 详细地示出了上述 EMM 的结构；

25 图 11 是一订单集中服务器在用于直接通过通信服务器接收命令时的概略图；

图 12 概略地说明了图 2 的一部分，它示出了本发明的一个实施例；

图 13 是一订单集中服务器在用于接收来自用户授权系统的命令以便请求回叫时的概略图；

30 图 14 是所述通信服务器的概略图；

图 15 示出了 EMM 发射周期率随 PPV 事件的时间而变的方式；

图 1 6 是用于发射 E M M 的信息发射器 (Message Emitter) 的概略图;

图 1 7 是显示将 E M M 存储到上述信息发射器内的方式的概略图;

5 图 1 8 是一聪明卡 (smartcard) 的概略图;

图 1 9 是上述聪明卡的存储器中存储区结构的概略图, 以及

图 2 0 是 P P V 事件描述的概略图。

具体实施方式

图 1 示出了本发明数字电视广播和接收系统 1 0 0 的概貌。本发明包括一通常的数字电视系统 2 0 0 0, 它使用周知的 M P E G—2 压缩系统来传送压缩后的数字信号。具体地说, 广播中心内的 M P E G—2 压缩器 2 0 0 2 接收数字信号流 (一般是视频信号流)。压缩器 2 0 0 2 通过线路 2 0 0 6 与一多路复用器和扰码器 2 0 0 4 相连。多路复用器 2 0 0 4 接收多个其它输入信号、汇集一个或多个传输流并将压缩后的数字信号通过线路 2 0 1 0 传给广播中心的发射器 2 0 0 8, 所说的线路当然可以呈包括电信线路在内的多种形式。发射器 2 0 0 8 通过上行线路 2 0 1 2 将电磁信号传给卫星收发器 2 0 1 4, 在该收发器中, 对所述电磁信号作电学处理并通过理论上的下行线路 2 0 1 6 将其广播给地面接收器 2 0 1 8, 所述地面接收器通常呈最终用户所拥有或租借的抛物面天线的形式。将接收器 2 0 1 8 所接收的信号传给最终用户所拥有或租借的并与最终用户的电视机 2 0 2 2 相连的集成接收器 / 解码器 2 0 2 0。接收器 / 解码器 2 0 2 0 将压缩后的 M P E G—2 信号解码成用于电视机 2 0 2 2 的电视信号。

25 有条件访问系统 3 0 0 0 与多路复用器 2 0 0 4 和接收器 / 解码器 2 0 2 0 相连并部分地位于广播中心内、部分地位于所述解码器内。有条件访问系统 3 0 0 0 能使得最终用户访问来自一个或多个广播提供商的数字电视广播。可将能对涉及到商业节目 (也就是说, 广播提供商所出售的一种或多种电视节目) 的信息进行解密的聪明卡插进接收器 / 解码器 2 0 2 0。最终用户可利用解码器 2 0 2 0 和聪明卡以预订模式方式或有偿收视服务模式购买节目事件。

交互系统 4 0 0 0 也与多路复用器 2 0 0 4 和接收器 / 解码器

2 0 2 0 相连并且也部分地位于广播中心内、部分地位于所述解码器内，而且能使得最终用户通过带调制解调器的反向信道 4 0 0 2 与多种应用相交互。

以下详细说明有条件访问系统 3 0 0 0。

- 5 参照图 2，从总体上说，有条件访问系统 3 0 0 0 包括一用户授权系统 (S A S) 3 0 0 2。S A S 3 0 0 2 通过相应的 T C P—I P 线路 3 0 0 6 (也可以使用其它类型的线路) 与一个或多个用户管理系统 (S M S) 3 0 0 4 相连，每个广播提供商均使用一个 S M S。另外，也可以在两个广播提供商之间共享一个 S M S，或者，一个提
10 供商使用两个 S M S，等等。

使用“母”聪明卡 3 0 1 0 的呈加密器 3 0 0 8 形式的第一加密装置通过线路 3 0 1 2 与 S A S 相连。使用母聪明卡 3 0 1 6 的也呈加密器 3 0 1 4 形式的第二加密装置通过线路 3 0 1 8 与多路调制器 2 0 0 4 相连。接收器/解码器 2 0 2 0 接收一“子”聪明卡 3 0 2
15 0。通信服务器 (Communication Server) 3 0 2 2 通过带调制解调器的反向信道 4 0 0 2 将接收器/解码器 2 0 2 0 直接连接于 S A S 3 0 0 2。S A S 还根据请求将预订授权发送给所说的子聪明卡。

所述聪明卡包含有一个或多个商业操作者的密码。所述“母”聪明卡对不同种类的信息进行加密，而“子”聪明卡则在有授权时对该
20 信息解密。

第一和第二加密器 3 0 0 8 和 3 0 1 4 分别包括一支架、一帶有存储在 E E P R O M 中的软件电子 V M E 卡、多达 2 0 个的电子卡以及聪明卡 3 0 1 0 和 3 0 1 6，对于每个电子卡来说，一个聪明卡 (聪明卡 3 0 1 6) 用于对 E C M 进行加密，一个聪明卡 (聪明卡 3
25 0 1 0) 用于对 E M M 进行加密。

以下参照电视系统 2 0 0 0 和有条件访问系统 3 0 0 0 的各种组件来详细说明数字电视系统的有条件访问系统 3 0 0 0 的操作。

多路复用器和扰码器

参照图 1 和图 2，在广播中心内，首先用 M P E G—2 压缩器 2
30 0 0 2 压缩 (或降低位速率) 数字视频信号。然后，通过线路 2 0 0 6 将压缩后的信号传给多路复用器和扰码器 2 0 0 4，以便将该信号与诸如其它压缩数据之类的其它数据复用。

所述扰码器生成一控制字，它在扰码过程中使用并且包括在多路复用器 2 0 0 4 中的 M P E G—2 数据流内。所述控制字是在内部生成的并且能使得最终用户的集成接收器 / 解码器 2 0 2 0 对节目进行解扰码。

- 5 将表示如何使节目商业化的访问标准也增加到 M P E G—2 数据流内。可按多种“预订”模式中的一种和 / 或多种“有偿收视服务”(P P V) 模式或事件中的一种来使节目商业化。在预订模式中，最终用户预订一种或多种商业节目或“节目集合”，从而获得观看所述集合内的每一个频道的授权。在上述最佳实施例中，可从频道集合中选出多达 9 6 0 种商业节目。在有偿收视服务中，最终用户可以按需购买节目。这可以通过事先预约节目(“预约模式”)或通过一进行广播就购买节目事件(“随机模式”)来加以实现。在上述最佳实施例中，不管用户是否是预订模式还是按 P P V 模式来观看，所有的用户都是订户，当然， P P V 的观看者不一定是订户。

- 15 所述控制字和访问标准用于形成授权控制信息 (Entitlement Control Message, ECM); 授权控制信息是一种按与扰码后的节目有关的方式所发送的信息。该信息包含有一控制字 (它使得能对节目进行解扰码) 以及广播节目的访问标准。通过线路 3 0 1 8 将所述访问标准和控制字传给第二加密器 3 0 1 4 。在该加密器中，生成一 E C M 并将其加密且传给多路复用器和扰码器 2 0 0 4 。

- 20 数据流中由广播提供商所提供的各个服务性广播节目均包括多种不同的成份，例如，电视节目包括视频成份、音频成份、字幕成份等等。对一种服务的这些成份中的每一种分别进行扰码和加密以便随后广播给收发器 2 0 1 4 。就所述服务的各个经扰码的成份而言，需要有一个独立的 E C M 。

节目发送

- 30 多路复用器 2 0 0 4 接收电信号，这些电信号包括来自 S A S 3 0 0 2 的加密 E M M 、来自第二加密器 3 0 1 4 的加密 E C M 以及来自压缩器 2 0 0 2 的压缩节目。多路复用器 2 0 0 4 对节目进行扰码并将扰码后的节目、加密的 E M M 和加密的 E C M 作为电信号通过线路 2 0 1 0 传给广播中心的发射器 2 0 0 8 。发射器 2 0 0 8 通过上行线路将电磁信号发送给卫星收发器 2 0 1 4 。

节目接收

卫星收发器 2 0 1 4 接收并处理发射器 2 0 0 8 所发射的电磁信号并将该信号通过下行线路 2 0 1 6 传给通常呈用户拥有或租用的抛物面天线形式的地面接收器 2 0 1 8。将接收器 2 0 1 8 所接收的信号传给最终用户拥有或租借的并与最终用户的电视机 2 0 2 2 相连的集成接收器 / 解码器 2 0 2 0。接收器 / 解码器 2 0 2 0 对信号进行多路复用以获得带有加密 EMM 和加密 ECM 的经过扰码的节目。

如果节目未被扰码, 也就是说, 未连同 MPEG-2 一道传送 ECM, 那么, 接收器 / 解码器 2 0 2 0 就对数据进行解压缩并将信号转换成视频信号以便传给电视机 2 0 2 2。

如果节目经过了扰码, 那么, 接收器 / 解码器 2 0 2 0 就从 MPEG-2 数据流中抽出相应的 ECM 并将该 ECM 传给最终用户的“子”聪明卡 3 0 2 0。“子”聪明卡 3 0 2 0 嵌在接收器 / 解码器 2 0 2 0 中的槽口内。子聪明卡 3 0 2 0 控制着最终用户是否有权对 ECM 进行解密并访问所说的节目。如果不是这样的话, 就将一否定的状态传给接收器 / 解码器 2 0 2 0 以指示不能对节目进行解扰码。如果最终用户有授权, 则对 ECM 进行解密并抽取出所说的控制字。然后, 解码器 2 0 2 0 用上述控制字对节目进行解扰码。对 MPEG-2 数据流进行解压缩并将其转换成视频信号以便转交给电视机 2 0 2 2。

用户管理系统 (SMS)

用户管理系统 (SMS) 3 0 0 4 包括一数据库 3 0 2 4, 它除其它工作以外还对所有最终用户文件、(诸如收费标准和宣传之类的) 商业数据、顶订情况、PPV 细节以及涉及到最终用户消费和授权的数据进行管理。SMS 在物理上可远离 SAS。

各个 SMS 3 0 0 4 通过相应的线路 3 0 0 6 将指示对要传给最终用户的授权管理信息 (EMM) 进行修改或创建的信息传给 SAS 3 0 0 2。

SMS 3 0 0 4 还将指示不修改或创建 EMM 而是仅指示最终用户状态变化 (涉及到在订购节目时授于最终用户的授权或者对最终用户的收费量) 的信息传给 SAS 3 0 0 2。

如下所述, SAS 3 0 0 2 将信息 (通常是诸如回叫信息或记帐

信息之类的请求信息)发送给SMS 3 0 0 4, 因此, 可以看出, 以上两者之间的通信是双向的。

授权管理信息 (EMM)

5 EMM是仅为个别最终用户 (订户) 或一组最终用户所专用的信息 (与ECM相反, ECM是仅为一个经扰码的节目所专用或者在一组经扰码的节目是同一商业节目的一部分的情况下为该组节目所专用的信息)。每一组最终用户可包含给定数量的最终用户。组织成组的目的在于使带宽达到最佳, 也就是说, 访问一组用户可以与若干最终用户进行联系。

10 在将本发明付诸实践时可使用多种特定类型的EMM。个别的EMM为个别的用户所专用并通常在提供有偿收视服务时使用, EMM包含分组标识以及用户在该组中的位置。所谓的“组 (Group)” 预订EMM为例如由2 5 6个用户构成的用户组所专用并通常在对某些预订服务进行管理时使用。这种EMM具有组标识和用户组位图。观众
15 EMM为所有观众所专用并且可例如为一特定的操作者所使用以提供某些免费服务。“观众”是用户的总称, 这些用户具有带相同操作者标识 (Operator Identifier OPI) 的聪明卡。最后, “唯一” (unique) EMM是指所述聪明卡的唯一标识。

以下参照图3说明典型的EMM的结构。实现为一系列数字数据
20 位的EMM基本上包括一头标3 0 6 0、EMM主体3 0 6 2以及一特征码3 0 6 4。头标3 0 6 0又包括: 一类型标识3 0 6 6, 它用于标识出所说的类型是个体、组、听众还是某种其它类型; 一长度标识3 0 6 8, 它给出了EMM的长度; 一用于EMM的可选地址3 0 7 0; 一操作者标识3 0 7 2; 以及, 一关键字标识3 0 7 4。当然,
25 EMM主体3 0 6 2可随EMM类型的不同而有很大变化。最后, 通常为8字节长的特征码3 0 6 4对EMM中其余数据的问题进行多种检验。

用户授权系统 (SAS)

30 将SMS 3 0 0 4所生成的信息通过线路3 0 0 6传给用户授权系统 (SAS) 3 0 0 2, SAS 3 0 0 2则又生成证实收到SMS 3 0 0 4所生成的信息的信息并将这些证实信息传给SMS 3 0 0 4。

如图 4 所示, 上述 S A S 在硬件层次上以周知的方式包括: 一主机 3 0 5 0 (在本实施例中, 该主机是 D E C 机), 它与一个或多个用于数据和命令输入的键盘 3 0 5 2 相连; 一个或多个视频显示装置 (V D U) 3 0 5 4, 它同于显示输出信息; 以及, 数据存储装置 3 0 5 6。还可在硬件上提供某些其它设备。

在本实施例中, 上述 S A S 在软件层次上运行于标准的开放式 V M S 操作系统, 以下将参照图 5 在总体上说明这套软件的结构, 应该认识到, 也可以用硬件来实现所说的软件。

从总体上说, 所述 S A S 包括: 一预订链接区 (Subscription Chain area) 3 1 0 0, 它可给出对预订模式的授权并每月自动地更新该授权; 一有偿收视链接区 (Pay Per View Chain area) 3 2 0 0, 它可给出对 P P V 事件的授权; 以及, 一 E M M 发射器 (EMM Injector) 3 3 0 0, 它用于将预订和 P P V 链接区所创建的 E M M 传给多路复用器和扰码器 2 0 0 4 从而给 M P E G 流加上 E M M。如果要授与诸如就将计算机软件下载到用户个人计算机而言的有偿文档 (Pay Per File, PPF) 授权之类的其它授权, 也可以设置其它类似的链接区。

S A S 3 0 0 2 的一个功能是根据商品化的不同模式 (预约模式、随机模式) 来管理对电视节目的访问授权, 所说的电视节目可以是预订模式中的商业节目或者是作为 P P V 事件而出售的。S A S 3 0 0 2 根据上述授权和接收自 S M S 3 0 0 4 的信息生成用于用户的 E M M。

预订链接区 3 1 0 0 包括一命令接口 (Command Interface, C I) 3 1 0 2、一用户技术管理 (S T M) 服务器 3 1 0 4、一信息生成器 (Message Generator, M G) 3 1 0 6 以及一加密器 (CIPHERING Unit) 3 0 0 8。

P P V 链接区 3 2 0 0 包括: 一授权服务器 (Authorisation Server, A S) 3 2 0 2; 一关系数据库 3 2 0 4, 它用于存储最终用户的相关详细资料; 一本地黑名单数据库 3 2 0 5; 用于上述数据库的数据库服务器 (Database Server) 3 2 0 6; 一订单集中服务器 (Order Centralized Server, O C S) 3 2 0 7; 一用于节目广播器的服务器 (Server for Programme Broadcaster, S P B) 3 2 0

8；一信息生成器（MG）3 2 1 0，其功能与用于上述预订链接区的功能基本上相同，以下不再予以说明；以及，加密器3 0 0 8。

EMM发射器3 3 0 0包括多个信息发射器（Message Emitter, ME）3 3 0 2、3 3 0 4、3 3 0 6和3 3 0 8以及软件多路复用器（Software Multiplexer, SMUX）3 3 1 0和3 3 1 2。在上述最佳实施例中，有两个用于信息生成器3 1 0 6的ME 3 3 0 2和3 3 0 4以及另外两个用于信息生成器3 2 1 0的ME 3 3 0 6和3 3 0 8。ME 3 3 0 2和3 3 0 6与SMUX 3 3 1 0相连，而ME 3 3 0 4和3 3 0 8则与SMUX 3 3 1 2相连。

10 以下对S A S的三个主要组成部分的每一个均作详细说明（预订链接区、P P V链接区和EMM发射器）。

预订链接区

首先说明预订链接区3 1 0 0，命令接口3 1 0 2主要用于将信息从SMS 3 0 0 4传给STM服务器3 1 0 4和OCS 3 2 0 6并将信息从OCS传给SMS。命令接口将直接命令或包含有命令的批文件当作来自SMS的输入。命令接口对来自STM服务器的信息进行句法分析并且能在信息出错（参数越界、缺少参数等）时发射准确的信息。命令接口跟踪一跟踪文件3 1 1 0中呈文本形式的输入命令而且还跟踪一重播文件3 1 1 2中呈二进制形式的输入命令，以便对一系列命令进行重播。可禁止跟踪并限制文件的大小。

20 以下具体参照图6详细说明STM服务器3 1 0 4。STM服务器是上述预订链接区的主引擎并能管理免费授权、创建新用户以及更新现有用户。如图6所示，将命令按一定的格式传给信息生成器3 1 0 6，所说的格式不同于将命令传给STM服务器时所用的格式。对每个命令来说，STM服务器都能仅在已成功地处理命令并将其发送给MG时将一确认信息发送给CI。

30 所述STM服务器包括一用户数据库3 1 2 0，其中存储有用户的相关参数（聪明卡号、商业数据、状态、组及在该组中的位置等等）。上述数据库对照该数据库的内容对CI 3 1 0 2所发送的命令进行语义检查并在命令有效时更新该数据库。

所述STM服务器还对STM服务器与MG之间的先进先出（FIFO）缓冲存储器3 1 2 2以及备份盘的FIFO 3 1 2 4进行管

理。上述 F I F O 的作用是在 M G 因任何原因而暂时不能进行响应时使来自 C I 的命令流平均化。上述 F I F O 还能确保在 S T M 服务器或 M G 崩溃的情况下不会丢失命令，这是因为，在重新启动时，所述 S T M 会将 F I F O 清空（也就是说发送给 M G ）。上述 F I F O 可实现为文件。

所述 S T M 服务器的核心包括一自动更新服务器 3 1 2 6，它可自动地进行更新并在操作者要求的情况下生成免费授权。在这种情况下，尽管应该认识到在 S M S 处初始化新授权的形成，但是，可将进行更新看作是包括第一次形成授权。正如会看到的那样，这两者可大致用相同的命令和 E M M 来加以处理。

使 S T M 分离于 S A S 并且使自动更新服务器位于 S A S 内而不是（像在周知系统中那样）位于 S M S 3 0 0 4 内是一项特别重要的特征，这是因为，它能显著地减少需要从 S M S 传给 S A S 的命令数（记住，S M S 和 S A S 可能处于不同的地点并由不同的操作者来控制）。事实上，自 S M S 所请求的两个主命令仅仅是应该开始一新的预订服务并（例如在未付费的情况下）中止一现有预订服务的命令。通过使 S M S 与 S A S 之间的命令交换减至最少，可以降低这两者之间的线路 3 0 0 6 中的命令传输故障的概率，而且，S M S 的结构一般也无需考虑有条件访问系统 3 0 0 0 的特点。

按图 7 的流程图所示的方式进行自动更新。为了降低带宽，假定非常高的更新百分比是标准的，那么，就在用户组中进行更新，在本最佳实施例中，每组有 2 5 6 个个别用户。所述流程图始于开始步骤 3 1 3 0 并前进至步骤 3 1 3 2，在该步骤中，按月启动更新功能（当然，应该注意，也可以有其它频率）。在按月频率的情况下，就如不进行更新授权就会到期的当前月份和所有以后月份而言，将授权赋给最终用户。

在步骤 3 1 3 4 中，就每一组以及该组中的个别用户访问用户数据库 3 1 2 0，以确定是否要更新特定个体的授权。

在步骤 3 1 3 6 中，根据上述用户数据库的内容形成如图 8 所示的组预订位图。该位图包括一组标识（在这种情况下是组 1 — “G 1”）3 1 3 8 以及 2 5 6 个个别用户存储区 3 1 4 0。根据特定用户是否要对其授权进行更新而将上述位图中的各个设置成 1 或 0。图

8 中示出了一组典型的二进制数据。

在步骤 3 1 4 2 中，将包括在组预订位图在内的适当命令传给信息生成器 3 1 0 6。在步骤 3 1 4 3 中，所述信息生成器设置一过期日期以向聪明卡指明这样的日期，超过该日期特定预约 EMM 将不再有效，一般将这一日期设是为下一个月的月末。

在步骤 3 1 4 4，所述信息生成器根据上述命令生成适当的组预订 EMM 并要求加密器 3 0 0 8 对 EMM 进行加密，然后，将加密后的 EMM 传给 EMM 发射器 3 3 0 0，在步骤 3 1 4 6 中，EMM 发射器 3 3 0 0 将 EMM 加进 M P E G - 2 数据流。

10 步骤 3 1 4 8 表明，对每一组重复上述过程。这一过程最后在结束步骤 3 1 5 0 结束。

事实上，以上参照图 7 所述的流程图具体涉及到对预订的更新。所述 S T M 还以相似的方式管理免费观众的授权以及新用户。

就用于特定电视节目或成组的这种节目的免费观众授权而言，可通过 S T M 将一命令传给信息生成器以生成带有过期日期即给定的天数（或周数）的适当观众 EMM（用于整个观众），从而可获得这种授权。M G 根据上述 S T M 命令来计算精确的过期日期。

就新用户而言，涉及到两个阶段。首先，购买时接收器 / 解码器 2 0 2 0 内的聪明卡能向用户提供一段给定时间（一般是几天）的免费授权（如果操作者希望的话）。这一点可通过生成用于用户的并且包括相关过期日期的位图来实现。然后，用户将其完整的书面材料交给（在 S M S）对用户进行管理的操作者。一旦对所述书面材料进行了处理，S M S 就向 S A S 提供一用于该特定用户的开始命令。一旦 S A S 接收到开始命令，S T M 就命令 M G 将一唯一地址赋给该新用户（包括特定的组号和在该组中的位置）并生成一特殊的所谓的“商业节目”预订 EMM（与通常的用于更新的“组”收费 EMM 相反）以向特定的用户提供授权直至下一个月月末。从这时开始，就如上所述那样自动地进行用户更新。利用上述两阶段的过程，可以向新用户授权直至 S M S 发出一中止命令。

30 应该注意，所述商业节目预订 EMM 用于新用户并用于重新启用现有用户。所述组预订 EMM 用于进行更新和挂起。

参照图 9，由上述过程生成的典型的预订 EMM 主体（也即忽略

了头标和特征码)包括下列主要部分即: 2 5 6 位预订(或用户组)位图 3 1 5 2; 用于对 EMM 加密的 1 2 8 位管理加密关键字 3 1 5 4; 6 4 位私用加密关键字 3 1 5 4, 它使得聪明卡 3 0 2 0 对控制字进行解密以访问广播节目; 以及, 1 6 位过期日期 3 1 5 8, 它指明了这样的日期, 超过该日期聪明卡就会忽略上述 EMM。事实上, 在上述最佳实施例, 设置在三组私用关键字, 一组用于当前月份, 一组用于下一个月、一组用于在系统出故障时进行恢复。

更具体地说, 除管理加密关键字 3 1 5 4 外, 所述组预订 EMM 主体具有所有的上述组成部分。所述商业节目预订 EMM 主体(它用于个别用户)包括代替整个用户组位图 3 1 5 2 的组 ID (标识)后面是在该组中的位置, 然后是管理加密关键字 3 1 5 4 和三组私用关键字 3 1 5 6, 随后是相关的到期日期 3 1 5 8。

信息生成器 3 1 0 6 用于将 S TM 服务器 3 1 0 4 发出的命令转换成 EMM 以便传给信息发射器 3 3 0 2。参照图 5, 首先, MG 生成 EMM 主体并将其传给加密器 3 0 0 8 以便相对管理和私用关键字进行加密。CU 将特征码 3 0 6 4 填加到 EMM 上并将该 EMM 传回给 MG, 在 MG 中加上头标 3 0 6 0。因此, 传给信息发射器的 EMM 是完整的 EMM。所述信息生成器还确定广播开始和结束的时间以及 EMM 的发射速率并将这些内容作为适当的指令连同 EMM 传给信息发射器。所述 MG 仅生成一给定的 EMM 一次, 这就是进行周期性传送的 ME。

参照图 5, 信息生成器包括自己的 EMM 数据库 3 1 6 0, 该数据库在相关 EMM 的生命周期内存储着该 EMM。一旦其发射期限已满, 就删除该 EMM。所述数据库用于确保 MG 与 ME 之间的一致性, 因此, 例如, 在将最终用户挂起时, ME 不会继续发送更新信号。在这方面, MG 计算相关的操作并将它们发送给 ME。

一旦生成了一 EMM, MG 就将一唯一的标识赋给该 EMM。当 MG 将该 EMM 传给 ME 时, 也就传递了上述 EMM 标识 (ID)。这就能在 MG 和 ME 处识别一特定的 EMM。

参照预订链接区, 信息生成器包括两个 FIFO 3 1 6 2 和 3 1 6 4, 一个用于 EMM 发射器 3 3 0 0 内的各个相关的信息发射器 3 3 0 2 和 3 3 0 4, 一个同于存储加密后的 EMM。由于预订链接区

和 EMM 发射器可分隔开显著的距离，故即使上述两者之间的线路 3 1 6 6 和 3 1 6 8 出现故障，使用 F I F O 也可使 EMM 的传送有完全的连续性。在有偿收视链接区内设置有相类似的 F I F O。

具体地说是信息生成器在总体上说是在条件访问系统的一个特征
5 涉及到通过将长度参数和标识参数混合起来从而减少 EMM 主体 3 0 6 2 的长度以节省空间这种方法。以下参照图 1 0 对此进行说明，图 1 0 说明了一个示例性的 EMM（事实上，它是一个 P P V EMM，这种 EMM 是最简单的 EMM）。在 P i d（数据包或“参数”标识）
10 3 1 7 0 中减少了长度。该 P i d 包括两部分即实际的 I D 3 1 7 2 以及用于数据包 3 1 7 4 的长度参数（此参数是必需的，以便能确认出下一个数据包的起点）。整个 P i d 为刚好一个字节的的信息，4 位供 I D 使用，4 位供长度参数使用。由于 4 位不足以按纯二进制的方式限定所说的长度，故使用了位与实际长度之间的对应关系，这种对应关系体现在一对对照表中，该对照表存储在信息生成器中的存储区 3 1
15 7 8 内（见图 5）。所述对应关系通常如下：

	0000=0
	0001=1
	0010=2
	0011=3
20	0100=4
	0101=5
	0110=6
	0111=7
	1000=8
25	1001=9
	1010=10
	1011=11
	1100=12
	1101=16
30	1110=24
	1111=32

可以看出，所述长度参数并不与数据包的实际长度成正比，它们

的关系部分地是平方关系而不是线性关系。这就使得数据包的长度有较大的范围。

有偿收视链接区

就有偿收视链接区 3 2 0 0 而言，参照图 5，具体地说，授权服务器 3 2 0 2 具有订单集中服务器 3 2 0 7 作为客户机，所述订单集中服务器请求有关与通信服务器 3 0 2 2 相连以购买 P P V 节目的各个用户的信息。

如果从 A S 3 2 0 2 中已知有用户，则可进行一组交易。如果就订单对用户进行了授权，则 A S 就会形成一帐单并将其发送给 O C S。否则，就将未对订单授权的信号发给 O C S。

如果已对至少一个交易进行了授权，那么，A S 仅在上述成组交易结束时通过数据库服务器 (D B A S) 3 2 0 6 来更新最终用户数据库 3 2 0 4，这就能使数据库访问的次数达到最优。

A S 授权进行购买所依据的标准存储在上述数据库中，可通过 D B A S 过程来加以存取。在一个实施例中，上述数据库与 S T M 所访问的数据库相同。

可根据客户的情况拒绝进行授权 (P P V - F o r b i d d e n , C a s i n o - F o r b i d d e n ...)。S T M 3 1 0 4 代表 S M S 3 0 0 4 对上述标准进行更新。

还要检查如 (用信用卡、自动付款或每天合法代币购买量等) 购买限制之类的其它参数。

就用信用卡付款而言，要对照存储在本地黑名单数据库 3 2 0 5 内的本地黑名单来检查卡号。

当所有的验证均成功时，所述 A S 就：

1、生成帐单并将其发送给 O C S，O C S 填写该帐单并将其存储到一个文件中，以后将此文件发送给 S M S 以便进行处理 (客户的实际的帐单)；以及

2、更新上述数据库以便主要地设置新的购买限制。

这种如果可以就检查并生成帐单的机制适用于各个命令，用户可在单个连接期间进行请求 (可在一次会话中预定例如 5 部电影)。

应该注意，与 S M S 所具有的信息量相比，A S 具有减少了的与用户有关的信息量。例如，A S 没有用户的姓名或地址。另一方面，

A S 具有用户的聪明卡号、用户消费级别（因此，可将不同的节目服务用于不同的用户）以及各种标志，这些标志例如是表示用户是赊购还是用户暂停还是聪明卡被盗的状态。使用减少了的信息量有助于减少对特定用户的请求进行授权所花费的时间。

- 5 D B A S 3 2 0 6 的主要目的是通过并行访问提高从 A S 来看的数据库效率（所以，仅用一个 D B A S 来限定一种结构实际上是没有意义的）。一个 A S 参数限定了应连接多少个 D B A S。一个给定的 D B A S 可仅与一个 A S 相连接。

10 O C S 2 3 0 7 主要处理 P P V 命令。该 O C S 按多种模式进行操作。

首先，O C S 处理 S M S 所发出的诸如节目更新（例如，如果 S M S 已存储了帐单，那么，O C S 就不生成帐单）、更新聪明卡 3 0 2 0 中的钱夹以及取消 / 更新会话之类的命令。

上述过程中的各个步骤是：

- 15 1、（用 A S 3 2 0 2 ）确认相关的用户；
2、如果有效，就向信息生成器生成适当的命令，收便发送一适当的 E M M。命令可以是：

20 节目订购，
更新钱夹，
会话删除。

请注意，上述操作并不意味着形成记帐信息，这是因为，业已从 S M S 周知有帐单。使这些操作与“免费节目”的购买相一致。

其次，O C S 处理经由通信服务器 3 0 2 2 接收自用户的命令。可通过与接收器 / 解码器 2 0 2 0 相连的调制解调器或通过用电话 4
25 0 0 1 的语音启动或通过用 M I N I T E L、P R E S T E L 或可用的类似系统来接收这些命令。

再次，O C S 处理 S M S 发出的回叫请求。以下详细说明后两种操作模式。

在上述第二种模式中，说明了 O C S 处理经由通信服务器 3 0 2
30 2 直接接收自最终用户（订户）的命令。这些命令包括（诸如用于特定 P P V 事件的）节目订购、用户所请求的预订修改以及对父母关注码的重置（父母关注码是这样的代码，父母可用该代码来限制对某些

节目或某类节目的观看授权)。

以下参照图 1 1 详细地说明处理上述命令的方式。

用户订购节目包括下列步骤:

- 1、利用 A S 确认通过 C S 3 0 2 2 进行呼叫以订购特定节目的
5 主叫用户;
- 2、用 A S 对主叫用户请求的有效性进行检查 (用接收器 / 解码器 2 0 2 0 将订单发到 A S , 可通过验证聪明卡 3 0 2 0 的详细资料来做到这一点);
- 3、确定购买的价格;
- 10 4、检查上述价格不会超过主叫用户的信用卡限额等;
- 5、从 A S 接收部分帐单;
- 6、填写帐单中的其它项目, 以形成一完整的帐单;
- 7、将上述完整的帐单增加到记帐信息存储文件 3 2 1 2 中以便进行后续处理; 以及,
- 15 8、将相应的命令发送给 P P V 信息生成器 3 2 1 0 以生成相关的 E M M。

如果用户用接收器 / 解码器 2 0 2 0 发出节目订单, 那么, 就在调制解调器线路 4 0 0 2 上发送所述 E M M (以下将详细说明其细节), 否则, 就广播上述 E M M。(在用户使用接收器 / 解码器 2 0 2
20 0 发出订单的情况下) 一个例外是调制解调器的连线有某种故障, 在这种情况下, 对 E M M 进行无线广播。

用户所请求的预订修改包括:

- 1、(用 A S) 确认主叫用户;
- 2、将信息发送给命令接口, 该 C I 又将该信息发送给 S M S ;
- 25 以及
- 3、(如果可以修改, 根据修改的费用) O C S 通过 C I 接收来自 S M S 的应答。

如果用接收器 / 解码器 2 0 2 0 请求修改, O C S 就向 S M S 生成一确认信息。否则, 例如就电话或 M i n i t e l 而言, 提醒用户
30 进行确认并通过 O C S 和 C I 将应答发送给 S M S 。

重置父母关注码包括:

- 1、(用 A S) 确认主叫用户; 以及

2、将一命令发送给MG以生成一带有适当重置口令的适当EMM。

就重置父母关注码而言，出于安全的原因不允许重置该代码的命令产生于接收器/解码器。只有SMS、电话和MINI TEL或类似的系统才能产生这种命令。所以，在这种特定的情况下，仅用无线的方式而不是用电话线来广播EMM。

从上述OCS的不同操作模式的实例中可以看出，用户可直接访问SAS特别是OCS和AS，因为，通信服务器直接与SAS特别是与OCS相连。这种重要的特征涉及到减少用户将其命令传给SAS的时间。

以下参照图12进一步说明上述特征，从图12中可以看出，最终用户的机顶盒(Set-Top-Box)特别是其接收器/解码器2020能够直接与通信服务器3022相通信，而通讯服务器3022则与SAS3002相联。从最终用户到SAS3002的通信服务器3022的连接不通过SMS3004，而是直接连到SAS3002上。

事实上，如上所述，提供了两种直接连接的方法。

第一种直接连接方法是通过电话4001的语言线路和适当的电话线(和/或通过MINI TEL或可用的类似连接方法)，在这种情况下，与经由SMS3004的通信相比，最终用户还必须要输入一系列语音命令或代码号，但能节省时间。

第二种直接连接方法源于接收器/解码器2020，通过最终用户插入他自己的子聪明卡3020来自动地输入数据，从而能减少最终用户必须输入相关数据的工作，这又能降低所花费的时间并减少输入时出错的可能性。

源于上述说明中的另一个特征是降低将最后的EMM传给最终用户所花费的时间，从而能鼓励选定节目的用户进行收视。

从广意上说，参照图12，可通过使最终用户的接收器/解码器2020具有直接与和SAS3002相联的通信服务器3022进行通信的能力来实现上述特征。

如前所述，集成接收器/解码器2020通过带调制解调器的反向信道4002直接与通信服务器3022相连，因此，可由SAS

3 0 0 2 处理来自解码器 2 0 2 0 的命令, 生成信息 (包括 EMM), 然后经由反向信道 4 0 0 2 将其直接送回至解码器 2 0 2 0。在 C S 3 0 2 2 与接收器 / 解码器 2 0 2 0 之间的通信过程中使用一种协议 (以下将予以说明), 因此, C S 对接收到相关 EMM 的确认信息进行接收, 从而将确定性增加给上述过程。

因此, 例如就预约模式而言, S A S 3 0 0 2 借助于聪明卡和解码器 2 0 2 0 的调制解调器以及电话线 4 0 0 2 接收来自最终用户的请求访问特定事件 / 节目的信息, 并将一适当的 EMM 通过电话线 4 0 0 2 和调制解调器返回给解码器 2 0 2 0, 所述调制解调器和解码器最好同时位于机顶盒 (S T B) 内。因此, 在不必经由多路复用器和扰码器 2 0 0 4、上行线路 2 0 1 2、卫星 2 0 1 4 和数据线路 2 0 1 6 来传送 M P E G - 2 数据流 2 0 0 2 中的 EMM 的情况下就能实现这一点, 从而能使得最终用户收视到所说的事件 / 节目。这就能显著地节省时间和带宽。实际确定性的前提条件如下: 用户一旦为其购买行为付了款, EMM 就会到达接收器 / 解码器 2 0 2 0。

在上述 O C S 3 2 0 7 的第三种操作模式中, O C S 处理 S A S 发出的回叫请求。参照图 1 3 说明了这一点。典型的回叫请求是为了确保接收器 / 解码器 2 0 2 0 通过带调制解调器的反向信道 4 0 0 2 用 S A S 所需要的接收器 / 解码器信息来回叫 S A S。

正如命令接口 3 1 0 2 所指令的那样, 预订链接区的信息生成器 3 1 0 6 生成一回叫 EMM 并将其发送给接收器 / 解码器 2 0 2 0。加密器 3 0 0 8 出于安全上的原因对该 EMM 进行加密。所述 EMM 在未被明确请求的情况下包含有接收器 / 解码器应该被唤醒并对自身进行回叫的时间 / 日期, 所述 EMM 一般还可包含有终端用户必须拨叫的电话号码、不成功拨叫之后的试拨次数以及两次拨叫之间的延迟时间。

所述接收器 / 解码器在接收到 EMM 或在指定的时间 - 日期与通信服务器 3 0 2 2 相连接。O C S 3 2 0 7 首先用 A S 3 2 0 2 确认主叫用户并验证诸如聪明卡操作者和用户详细资料之类的某些详细资料。然后, O C S 要求聪明卡 3 0 2 0 发送各种加密信息 (如相关会话号、何时监视会话、允许用户观查该会话几次、观查会话的方式、剩余的代币数、预约会话的次数等等)。P P V 链接区的生成器 3 2 1

0用加密器3008对这些信息解密。OCS将这些信息加进回叫信息存储文件3214以便以后进行处理并传给SMS3004。出于安全的原因对这些信息进行加密。重复上述整个的过程直至从聪明卡中不能读出更多的内容。

- 5 上述回叫功能的一个最佳特征是：在读取聪明卡之前（即刚好在如上所述那样用AS3202确认了主叫同户之后）由SAS3002检查接收器/解码器确实是真的而不是盗版或计算机伪造品。按下列方式进行上述检查。SAS生成一随机数，该随机数由接收器/解码器所接收、加密、然后返回给SAS。SAS对该随机数进行解密。
- 10 如果解密成功并检索到原始的随机数，就可得出结论说该接收器/解码器是真的，所述过程继续进行。否则，该过程就中止。

回叫过程中的其它功能是删除聪明卡上的过时会话或增加钱夹的钱数（以下在题为“聪明卡”一节中对后者加以说明）。

- 就PPV链接区3200而言，以下说明通信服务器3022。
- 15 在该最佳实施例，通信服务器3022在硬件层次上包括一有四个并行处理器的DEC机。参照图14，通信服务器在软件结构层次上的许多方面都是常规的通信处理器。与常规结构的一个具体差异是所述通信服务同时为接收器/解码器2020和用常规电话4001的语音通信进行服务并可以为MINITEL或类似系统服务。

- 20 看图时应该注意，图14中示出了两个订单集中服务器3207（为“OCS1”和“OCS2”），很自然，可以设置任何预定数量的订单集中服务器。

- 所述通信服务器包括两个主服务器（“CS1”和“CS2”）以及多个前端服务器（“Frontal1”和“Frontal2”），
- 25 图14中示出了两个前端服务器，一般地说，每个主服务器可配备10或12个前端服务器。的确，尽管业已示出了两个主服务器CS1和CS2以及两个前端服务器Frontal1和Frontal2，但可以使用任何数量的主服务器和两个前端服务器。通常应有某些富余。

- 30 CS1和CS2通过高层TCP/IP线路3230连接于OCS1和OCS2，而CS1和CS2则通过另一TCP/IP线路3232连接于Frontal1和Frontal2。

如前所述, C S 1和C S 2包括用于“S E N D R”(发送)、“R E C V R”(接收)、“V T X”(M I N I T E L、P R E S T E L或类似系统)、“V O X”(语音通信)以及“T R M”(与接收器/解码器相通信)的服务器。它们与“B U S”(总线)相连以便将信号传给
5 前端服务器。

C S 1和C S 2通过带调制解调器的反向信道4 0 0 2用X 2 5公用网络共用协议直接与接收器/解码器2 0 2 0相通信。在一个最佳实施例中, 通信服务器3 0 2 2与接收器/解码器2 0 2 0之间的较低层协议是以国际C C I T T的V 4 2标准协议为基础的, 该协议
10 通过错误检测和数据再传功能来保证可靠性并使用检查和(checksum)例程来检查再传输的完整性。还提供一种换码机制以防止传送不允许的字符。

另一方面, 通过前端通信服务器来进行语音电话通信, 每个前端通信服务器都能通过高速“T 2”(E 1)标准的电话I S D N线接收
15 如3 0个从连接器3 2 3 4到本地电话网的同步语音连接。

通信服务器的上述软件部分的三个特殊功能(它们当然可完全用硬件来加以实现)首先是将接收自接收器/解码器的较低层次的协议信息转换成输出给O C S的较高层次的协议信息, 第二是减少或控制同步连接的数量, 第三是在没有任何混淆的情况下提供若干同步信
20 道。在最后一个方面中, 通信服务器起多路调制器的作用, 并且, 一事实上在整个通信链路中都使用的给定会话I D(标识)限定了特定信道链路中的交互方式。

最后, 就有偿收视链接区3 2 0 0而言, 参照图5, 用于节目广播的服务器(S P B)3 2 0 8与一个或多个节目广播器3 2 5 0(它
25 一般都位于远离S A S的位置)以接收节目信息。S P B滤出与P P V事件(会话)相对应的信息以供使用。

一个重要的特征是S P B将滤出的节目事件信息传给M G, M G则依次向M E发出指令(控制命令)以便改变给定环境下的E M M的周期发射率, 通过M E用相关会话标识找出所有的E M M并改变分配
30 给该E M M的周期率来做到这一点。可将这一特征可看作是为特定的E M M动态地分配带宽。在以下涉及到E M M发射器的章节中详细地说明E M M的周期性发射。

以下参照图 1 5 说明改变周期率的环境，图 1 5 示出了在特定 P P V 事件之前直至事件结束时如何在短时间（例如 1 0 分钟）将周期率 3 2 5 2 从例如每隔 3 0 分钟的低周期率提高至例如每隔 3 0 秒至 1 分钟的高周期率，以便满足预定超级用户在这段时间对 P P V 事件的需求。通过这种方式，可根据预定用户的需求自动地分配带宽。这就有助于减少整个的带宽要求。

还可以改变其它 E M M 的周期率。例如，可通过多路复用器和扰码器 2 0 0 4 发送适当的位速率指令来改变预订 E M M 的周期率。

E M M 发射器

就 E M M 发射器 3 3 0 0 而言，以下参照图 1 6 说明信息发射器 3 3 0 2 至 3 3 0 8 的详细内容，信息发射器 3 3 0 2 至 3 3 0 8 构成了 E M M 发射器的一部分并起用于信息生成器的输出装置的作用。它们的功能是获取 E M M 并通过相应的线路 3 3 1 4 和 3 3 1 6 将 E M M（按轮转的方式）周期性地传给软件多路复用器 3 3 1 0 和 3 3 1 2 以及硬件多路复用器和扰码器 2 0 0 4。作为回答，软件多路复用器和扰码器 2 0 0 4 生成一控制整个周期率的全球位速率指令，为了做到这一点，M E 要考虑诸如周期时间、E M M 的大小等之类的多种参数。在图 1 6 中，E M M - X 和 E M M - Y 是用于操作者 X 和 Y 的组 E M M，而 E M M - Z 则是用于操作者 X 或操作者 Y 的其它 E M M。

以下对信息发射器的一个实例作进一步说明，应该注意，其余的 M E 以类似的方式操作。M E 在特别是传送开始和结束时间和发射速率以及若 E M M 是 P P V E M M 则还有会话号等来自 M G 的指令的控制下进行操作。就发射速率而言，在本最佳实施例中，所述相关指令可以取从很快到很慢的五种值中的一个。在指令中并不指定上述数字值，而是由 M E 将该指令映射成 S A S 的相关部分所提供的实际数字值。在本最佳实施例中，所述五种发射速率如下：

- 1、很快 每 3 0 秒
- 2、快 每分钟
- 3、中速 每 1 5 分钟
- 4、慢 每 3 0 分钟
- 5、很慢 每 3 0 分钟。

ME具有一第一和第二数据库3320和3322。第一数据库用于尚未获得广播日期的EMM，这些EMM存储在所述数据库中的一系列时序文件中。第二数据库用于立即进行广播的EMM。在系统崩溃的情况下，ME具有重新读取相关的存储文件并进行正确广播的能力。当MG希望保持输入指令之间的一致性并且EMM已被发送给ME时，就根据来自MG的请求更新所有存储在上述数据库中的文件。实际广播的EMM也存储在随机存取存储器3324内。

信息生成器中的FIFO3162和3164与信息发射器中的数据库3320和3322的组合是指如果这两者之间的线路3166临时中断，则它们能以独立的方式进行操作，ME仍能广播EMM。

软件多路复用器(SMUX)3310和3312提供了ME与硬件多路复用器2004之间的接口。在本最佳实施例中，尽管从总体上说不对可与一个SMUX相连的ME数量进行限制，但它们可各接收来自两个ME的EMM。SMUX将EMM集中起来然后根据EMM的类型将其传给适当的硬件多路复用器。这是必需的，因为，硬件多路复用器处理不同类型的EMM并将它们放到MP EG-2数据流中的不同位置。SMUX还将全球位速率指令从硬件多路复用器传给ME。

ME的一个特别重要的特征是它按随机的次序发射EMM。原因如下。信息发射器不能检测或控制将什么信息发射给了多路复用器。所以，信息发射器连续传送两个要由接收器/解码器2020所接收和解码的EMM。在这种情况下，如果EMM没有充分的间隔，则接收器/解码器和聪明卡就不能适当地检测出第二个EMM并对其解码。按随机的次序周期性地发射EMM可以解决这一问题。

以下参照图17说明随机化的方式，在这一实施例中，用ADA计算机语言实现必要的软件逻辑。随机化的一个特别重要的部分是将EMM正确地存储到数据库3320和3322（用于作备份）和RAM3324内。就具体的周期率和操作者而言，以二维阵列的方式按序列3330（例如从A至Z）以及该序列中的号码3332（从0至N）来存储EMM。将周期率3334加到第三维内，因此，有与周期率同样多的二维矩列。在这一最佳实施例中，有256种序列，每种序列中通常有200或300个EMM，有5种周期率。由不同

的操作者来增加所述矩阵的最后一维，有与操作者同样多的三维阵列。在MG要删除特定EMM的情况下，按这种方式存储数据能快速检索。

按“杂凑”(hash)算法(周知为“单向杂凑函数”)来存储EMM。这是靠取模方法来进行的，因此，在使用上述序列中的较大的号码之前填写连续的序列，并且，每个序列中的EMM的数量大致保持恒定。当MG向ME发送一带标识(ID)1的EMM时，将序列“1”分配给该EMM，并且，该EMM用序列3 3 3 0中的第一个号码3 3 3 2。将序列“2”分配给带有ID 2的EMM等等，直至序列2 5 6。(根据取模函数)将序列“1”分配给带有ID 2 5 7的EMM，该EMM占用第一序列中的第二个号码，等等。

例如在删除MG所请求的特定EMM时，用与以上相反的过程来检索特定的EMM。杂凑算法适用于EMM ID以获得听说的序列，此后，查找该序列中的号码。

在用随机化装置3 3 4 0根据周期性从RAM 3 3 2 4中检索出EMM时，就会进行实际的随机化，所说的随机化装置是用信息发射器的硬件和/或软件来实现的。所说的检索是随机的并且是基于上述杂凑算法的。首先，选定一随机数(在上述实例中，开始时在1至2 5 6的范围内)以形成一有意义的特定序列。第二，选定另一个随机数以形成上述序列中的特定号码。根据给定序列中的EMM的总数来选择所说的另一个随机数。一旦选定并广播了一给定的EMM，就用杂凑函数将其移至RAM 3 3 2 4中的第二个同样的存储区内。所以，在广播该EMM时，可按这样的程度减少第一存储区的大小即：一旦使用了整个的序列，就将其删除。一旦第一存储区完全变空，就在新一轮EMM广播之前用第二存储区代替第一存储区，反之亦然。

在上述方式中，在EMM的两个或三个周期之后，可在统计上忽略连续传送为同一最终用户指定的任何两个EMM的概率。

在存储EMM的同时，计算机3 0 5 0按规律的间隔计算存储的字节数并据此计算来自上述多路复用器和软件多路复用器的全球位速率指令所给出的发射位速率。

参照备份数据库3 3 2 0和3 3 2 2。事实上，在本实施例中，这些数据库是顺序文件存储器，它们具有RAM 3 3 2 4中内容的备

份。在信息发射器出故障并随后重新启动时，或更概括地说在无论因什么原因而重新启动M E时，就会在R A M与数据库之间形成链路，可在该链路上将存储的E M M上载至R A M。通过这种方式，可消除在出故障时丢失E M M的危险。

- 5 就预订E M M而言，可与以上所述相类似的方式存储P P V E M M，并且，所说的序列一般对应于给定的操作者且所述序列中的号码对应于会话号。

聪明卡

- 10 图1 8概略地示出了一子或“订户”聪明卡3 0 2 0，该卡包括一诸如Motorola 6 8 0 5微处理器之类的8位微处理器1 1 0，它具有一与一组标准触点1 2 0相连的输入/输出总线，所述触点在使用中与接收器/解码器2 0 2 0的读卡器中的相应一组触点相连接，所述读卡器具有常规的结构。微处理器1 1 0还与最佳的掩模R O M 1 3 0、R A M 1 4 0和E E P R O M 1 5 0作总线连接。所述聪明卡
- 15 符合I S O 7 8 1 6—1、7 8 1 6 2和7 8 1 6—3标准协议，这些协议分别决定了聪明卡的物理参数、触点在芯片上的位置以及外部系统（特别是接收器/解码器2 0 2 0）与聪明卡之间的特定通信，本文对这些协议不作进一步的说明。正如所说明的那样，微处理器1 1 0的一个功能是管理聪明卡中的存储器。

- 20 E E P R O M 1 5 0包含有某些动态创建的操作员存储区1 5 4、1 5 5、1 5 6和动态创建的数据区，以下参照图1 9对此进行说明。

- 25 参照图1 9，E E P R O M 1 5 0包括一8位的永久“卡I D”（或生产商）区1 5 1，该区包含有聪明卡3 0 2 0生产商所设置的永久用户聪明卡标识。

- 30 在重置聪明卡时，微处理器1 1 0发信号给接收器/解码器2020，所述信号包括一聪明卡所使用的有条件访问系统的标识以及根据存储在聪明卡中的包括卡I D在内的数据所生成的数据。接收器/解码器2 0 2 0存储上述信号并在以后用所存储的数据来检查该聪明卡是否与接收器/解码器2 0 2 0所使用的有条件访问系统相兼容。

 E E P R O M 1 5 0还包含有一永久的“随机数发生器”区1 5 2，该区包含有用于生成伪随机数的程序。所述随机数用于增加聪明

卡3020产生的并被送回至广播器的交易输出信号的种类。

在随机数发生器区152的下面设置有一144字节的永久“管理”区153。如下所述，永久管理区153是动态创建（和删除）区154、155、156中的ROM130中的程序所使用的特定
5 操作者区。永久管理区153包含有与聪明卡创建或删除存储区的授权有关的数据。

用于动态创建和删除区域的程序可响应特定的存储区创建（或删除）EMM，这些EMM由SAS3002所传送并被接收器/解码器2020所接收且被传给用户聪明卡3020。为了形成所说的E
10 MM，操作者需要上述管理区所专用的特定关键字。这就能防止一个操作者删除与另一操作者有关的存储区。

在管理区153的下方是一系列“操作者ID”区154、155、156，它们分别由于操作者1、2...N。通常将至少一个操作者ID区预装进用户聪明卡3020的EEPROM内，因此，最终
15 用户可通过该操作者对节目广播进行解密。但是，正如以下将说明的那样，最终用户（订户）可在以后用管理区域153响应其聪明卡3020所生成的交易输出信号来自动地创建另一个操作者ID区。

每个操作者区154、155、156均包含有聪明卡3020所属的组的标识以及聪明卡在该组中的位置。这一数据能使聪明卡（以及组中的其它聪明卡）响应一具有该组地址（不是聪明卡在该组的位置）的广播“组”预订EMM并响应仅发送给组内该聪明卡的“个别”
20 （或商业节目预订）EMM。每组可以有256个成员聪明卡，所以，这一特征可显著地降低广播EMM所需的带宽。

为了进一步减少广播“组”预订EMM所需的带宽，可连续地更新聪明卡3020及其它子聪明卡的EEPROM里的每个操作者区
25 154、155、156和所有相似的存储区中的组数据，从而使一特定的聪明卡改变在各组中的位置，以填补例如删除组成员所形成的空缺。正如在有一空缺表的STM服务器3104中那样，所说的空缺可由SAS3002来填补。

30 通过这种方式，可以减少碎片，并且将各组的成员数保持在或接近最多的256个成员。

每个操作者区154、155、156均与存储在EEPROM

1 5 0 内的一个或多个“操作者数据对象”相关联。如图 1 9 所示，一系列动态创建的“操作者数据”对象 1 5 7—1 6 5 位于操作者 I D 区的下方。这些对象中的每一个对象均标记有：

5 a) —“标识” 1、2、3 ... N，它们对应于相关的操作者 1、2、3 ... N，如图 1 9 中左面部分所示；

b) —“I D”，它指明了对象的类型；以及

10 c) —为数据保留的“数据”区，如图 1 9 中各相关操作者对象的右面部分所示。应该认识到，各个操作者均与一组类似的数据对象相关联，因此，以下对操作者 1 的数据对象中的数据类型的说明也适用于所有其它操作者的数据对象。还应注意，所述数据对象位于 E E P R O M 的相邻物理区内，它们的顺序并不重要。

删除数据对象会在聪明卡中形成一“空缺” 1 6 6，也就是说，被删除的对象先前占用的字节未被立即占用。因此，将“被闲置”的字节或“空缺”标记有：

15 a) —“标识” 0；以及

b) —“I D”，它指明上述字节是空的以接收一对象。

所创建的下一个数据对象填补标识 0 所标记的空缺。通过这种方式，能充分地利用 E E P R O M 1 5 0 的有限存储容量（4 千字节）。

20 以下参照与各操作者相关联的数据对象组来说明前述数据对象的实例。

数据对象 1 5 7 包含有 E M M 关键字，它用于对接收器 / 解码器 2 0 2 0 所接收的加密 E M M 进行解密。所述 E M M 关键字永久地存储在数据对象 1 5 7 内。可在发放聪明卡 3 0 2 0 之前创建数据对象 1 5 7，并且 / 或者，在创建一新操作者区（如前所述）时动态地创建数据对象 1 5 7。

30 数据对象 1 5 9 包含有 E C M 关键字，它们是由相关操作者（在本例中是操作者 1）所发送的，以便使最终用户能够对他所预订的特定节目组进行解密。一般每个月都发送新的 E C M 以及组预订（更新）E M M，这种 E M M 可对整个晚上都在观看来自操作者 1（在本例中）的广播的最终用户进行更新。使用独立的 E M M 和 E C M 关键字允许按不同方式（在本实施例中通过预订和个别（有偿收视服务）的方式）购买收视授权并且还能提高安全性。以下将说明有偿收视服务（P P

V) 模式。

由于周期性地发送新 ECM 关键字, 因此, 关键是防止用户例如通过关闭接收器 / 解码器或重置时钟以防旧的 ECM 到期从而越过接收器 / 解码器中的计时器来使用旧的 ECM 关键字。因此, 操作者区
5 1 5 4 包括这样的区域 (一般具有 2 字节的大小), 该区域包含有 ECM 关键字的到期日期。聪明卡 3 0 2 0 能将这一日期与包含在所接收到的 ECM 中的当前日期作比较并且若当前日期比前述到期日期晚就阻止进行解密。如上所述, 通过 EMM 来传送所说的到期日期。

数据对象 1 6 1 包含有一 6 4 位的预订位图, 它可精确地表示用
10 户所预定的广播操作者的节目。每一位都表示一个节目, 并且, 若节目已被预订, 则将该位设成 “1”, 若节目未被预订, 则将该位设成 “0”。

数据对象 1 6 3 包含有一定量的代币, 用户在 PPV 模式中可用该代币例如根据免费预告或其它广告来购买对即将到来的广播的收视
15 授权。数据对象 1 6 3 还包含有一限制值, 它可被设置为例如为负值以允许用户赊账。可例如用信用卡并通过带调制解调器的反向信道 4 0 0 2 或者用与信用卡相结合的语音服务器来购买代币。可将特定的节目事件收费为一个代币或多个代币。

数据对象 1 6 5 包含有对 PPV 事件的描述, 如图 2 0 的表 1 6
20 7 所示。

PPV 事件描述表 1 6 7 包含有: 一 “会话 ID” 1 6 8, 它标识出 (与节目以及广播时间和日期相对应的) 收视会话; 一 “会话模式” 1 6 9, 它指示如何购买收视授权 (例如按预约模式购买); 一 “会话下标” 1 7 0; 以及, 一 “会话收视服务” 1 7 1。

25 就按 PPV 模式接收节目而言, 接收器解码器 2 0 2 0 确定该节目是否是按 PPV 模式出售的节目。如果是这样的话, 解码器 2 0 2 0 就用存储在 PPV 事件描述表 1 6 7 中的项目来检查该节目的会话 ID 是否存入了描述表 1 6 7。如果描述表中已存入了会话 ID, 就从 ECM 中抽取出所说的控制字。

30 如果描述表中未存有会话 ID, 接收器 / 解码器 2 0 2 0 就通过一专门的应用程序将一信息显示给最终用户以指示该用户具有如从 ECM 中读出那样按例如 2 5 个代币的费用来收视会话的授权或者具有

与通信服务器 3 0 2 2 相连以购买节目事件的授权。在使用代币的情况下，如果最终用户（用遥控器 2 0 2 6（见图 2））回答“是”，则解码器 2 0 2 0 就将 ECM 发送给聪明卡，聪明卡将该卡 3 0 2 0 的钱夹中减去 2 5 个代币并将会话 ID 1 6 8、会话模式 1 6 9、会话下标 1 7 0 以及会话收视服务 1 7 1 写进 PPV 事件描述表 1 6 7 且从 ECM 中抽出所述控制字并对其解密。

在“预约”模式中，将一 EMM 传给聪明卡 3 0 2 0，因此，该聪明卡会用上述 EMM 将会话 ID 1 6 8、会话模式 1 6 9、会话下标 1 7 0 以及会话收视服务 1 7 1 写进 PPV 事件描述表 1 6 7。

10 可将会话下标 1 7 0 设置成使一个广播节目区别于另一个广播节目。这一特征允许对广播节目的一个子集例如五分之三的广播节目进行授权。一将带有与存储在 PPV 事件描述表 1 6 7 内的当前会话下标 1 7 0 不同的会话下标的 ECM 传给聪明卡，就将会话收视服务 1 7 1 减一。当会话收视服务达到零时，聪明卡就拒绝对带有与当前会话下标不同的会话下标的 ECM 进行解密。

会话收视服务的初始值仅取决于广播节目提供商希望限定所涉及到的节目事件的方式，用于相应节目事件的会话收视服务可取任何值。

聪明卡中的微处理器 1 1 0 执行一计数和比较程序以检测何时达到了对特定节目收视次数的限制。

20 可用前述“回叫”过程来从聪明卡中抽取出 PPV 事件描述表 1 6 7 中的所有会话 ID 1 6 8、会话模式 1 6 9、会话下标 1 7 0 和会话收视服务 1 7 1。

25 每个接收器/解码器 2 0 2 0 均包含有一标识，它可唯一地标识出上述接收器/解码器 2 0 2 0 或标识出该接收器/解码器的生产厂商或者可按某种其它方式对接收器/解码器进行分类，以使该接收器/解码器仅能同一种特定的聪明卡、由相同或相应生产厂商制造的特定类的聪明卡或者仅能供该类接收器/解码器使用的任何其它类的聪明卡一道工作。

30 通过这种方式，可防止由一个广播节目提供商所提供给用户的接收器/解码器 2 0 2 0 使用未经授权的子聪明卡 3 0 2 0。

除聪明卡与接收器之间“握手”以外，聪明卡 3 0 2 0 的 EEPOM 可包含有说明接收器/解码器 2 0 2 0 能发挥作用的类型的字

段或位图。这些类型是在生产所述聪明卡 3 0 2 0 的过程中或者由特定的 EMM 来指定的。

存储在聪明卡 3 0 2 0 中的位图一般包括多达 8 0 个接收器 / 解码器的列表，每个接收器 / 解码器均标识有一相应的接收器 / 解码器 I D，聪明卡可与该 I D 一道使用。与各接收器 / 解码器相关联的是状态“1”或“0”，它们分别指示聪明卡是否能与接收器 / 解码器一道使用。接收器 / 解码器的存储器 2 0 2 4 中的程序在存储于聪明卡内的位图中查找接收器 / 解码器的标识。如果找到该标识，且与该标识相关的值是“1”，则聪明卡“有效”，如果未找到该标识，则聪明卡不能与所述接收器 / 解码器一道使用。

此外，如果通常是因为操作者之间有协议而希望授权在特定的接收器 / 解码器中使用其它的聪明卡，则将一特定的 EMM 发送给这些聪明卡以通过收发器 2 0 1 4 改变聪明卡的位图。

各广播节目的提供商均根据某些特定的标准来区分它的用户。例如，可将某些用户分成“V I P”。因此，各广播节目提供商可将其用户分成多个子集，每个子集均包括任何数量的用户。

将特定用户所属的子集设定在 S M S 3 0 0 4 中。S A S 3 0 0 2 将 EMM 传给这样的用户，该用户将与他所属的子集有关的信息（一般长度为一个字节）写进聪明卡的 E E P R O M 的相关操作者数据区例如 1 5 4 内。当广播节目提供商广播节目事件时，就连同该事件传送一通常为 2 5 6 位的 E C M，以指示哪个子集的用户可以收视所说的事件，如果正如 E C M 所确定的那样依照存储在操作者区内的信息用户不具有收视前述事件的授权，则拒绝收视节目。

例如可利用这一功能在传送特定节目特别是与一特定地理区域内举行的运动会有关的节目期间关闭该地理区域内的所有给定操作者的聪明卡。通过这一方式，足球俱乐部或其它运动实体可以出售他们所在地之外的广播授权同时能防止地方支持者在电视中收视运动会。通过这种方式，可以鼓励地方支持者购票参加运动会。

与存储区 1 5 1 至 1 7 2 有关的各个特点均可看作是与动态创建存储区无关的独立发明。

应该认识到，以上完全是以举例的方式来说明本发明的，在本发明的范围内可对细节进行改进。

可独立地或以任何适当的组合形式来提供本说明书中公开的各个特征以及（在适当情况下）权利要求和附图。

在上述最佳实施例中，用计算机软件实现了本发明的某些特征。但是，对专家来说当然是很清楚，也可用硬件来实现这些特征中的任何一个。此外，应该认识到，可用电或类似的信号来实现用硬件、计
5 算机软件或类似手段所实现的功能。

交叉引用了我们共同未决的申请书，所有这些申请书有着相同的提交日期，题目为：“信号生成与广播”（代理人委托号 P C / A S B / 1 9 7 0 7 ），“供加密广播信号的接收器使用的聪明卡以及接收
10 器”（代理人委托号 P C / A S B / 1 9 7 0 8 ），“广播和接收系统以及用于上述系统的有条件访问系统（代理人委托号 P C / A S B / 1 9 7 0 1 0 ），“通过接收器 / 解码器将计算机文件从发射器下载到计算机上”（代理人委托号 P C / A S B / 1 9 7 1 1 ），“电视节目和其它数据的传送和接收”（代理人委托号 P C / A S B / 1 9 7 1
15 2 ），“下载数据”（代理人委托号 P C / A S B / 1 9 7 1 3 ），“计算机存储器组织”（代理人委托号 P C / A S B / 1 9 7 1 4 ），
“电视或无线电控制系统的开发”（代理人委托号 P C / A S B / 1 9 7 1 5 ），从传递的数据流中抽取数据部（代理人委托号 P C / A S B / 1 9 7 1 6 ），“访问控制系统”（代理人委托号 P C / A S B
20 / 1 9 7 1 7 ），“数据处理系统”（代理人委托号 P C / A S B / 1 9 7 1 8 ），“广播和接收系统以及用于该系统的接收器 / 解码器和遥控器”（代理人委托号 P C / A S B / 1 9 7 2 0 ）。本文引用了这些文件的内容。上述申请书清单包括了本申请书。

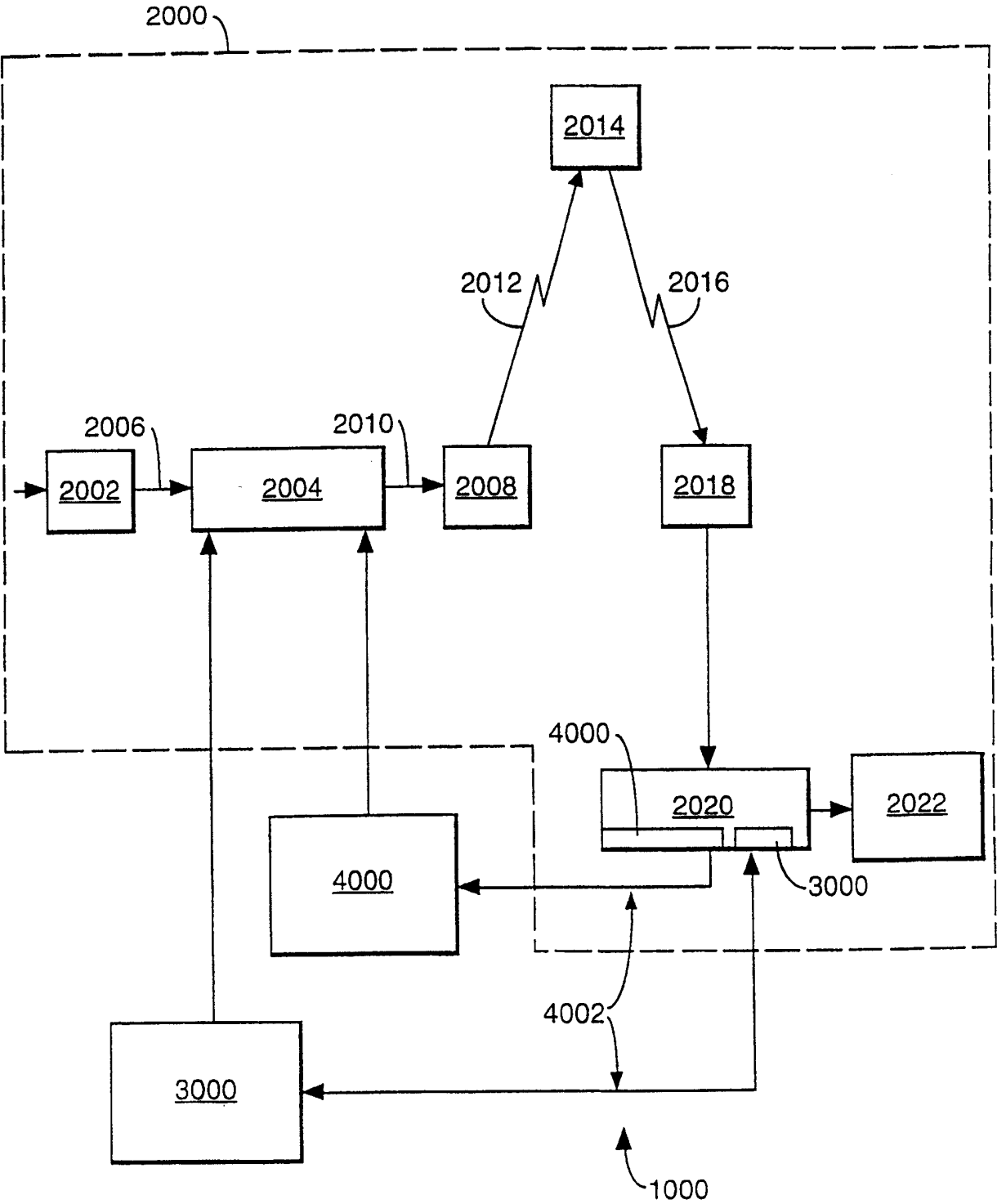
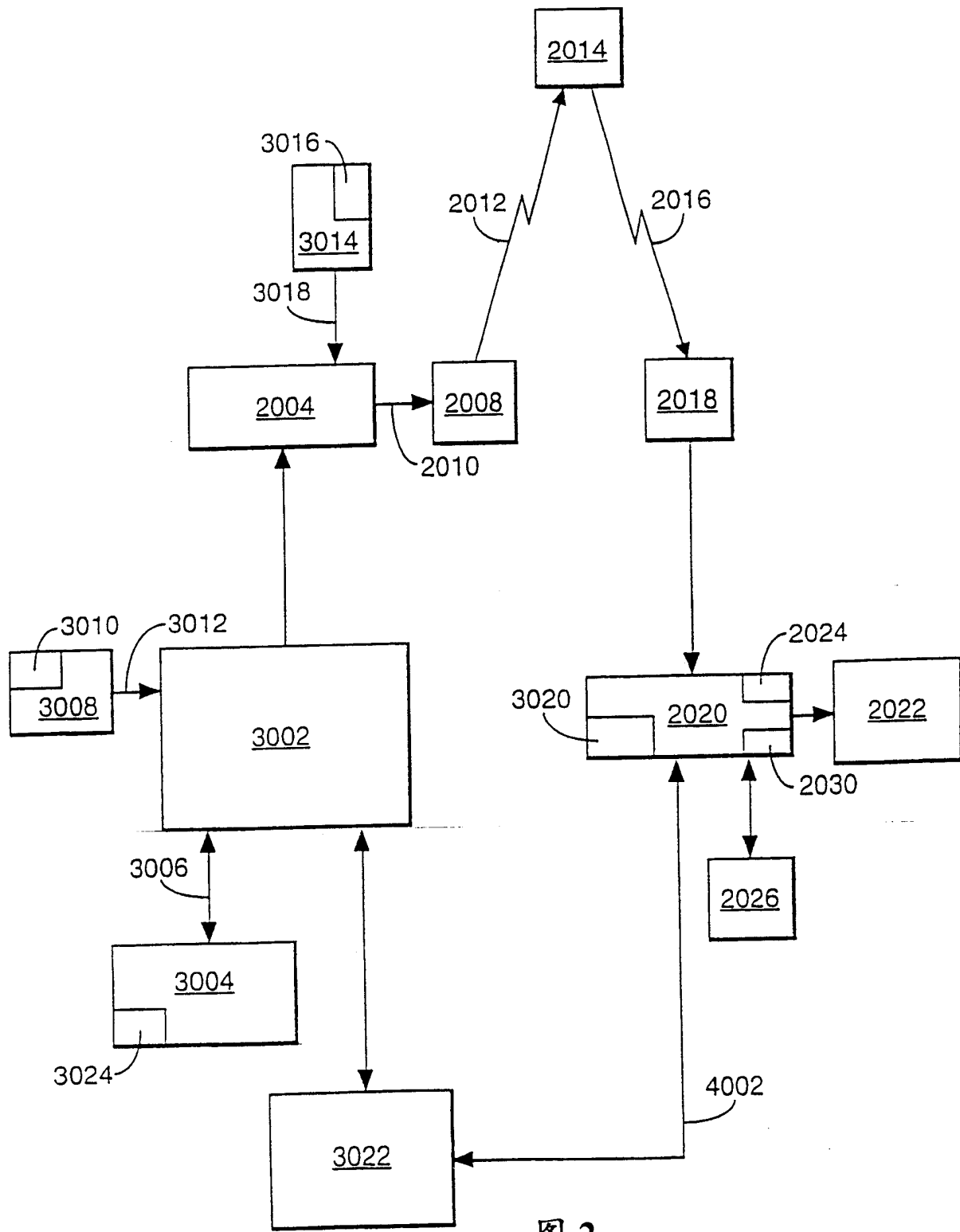


图 1



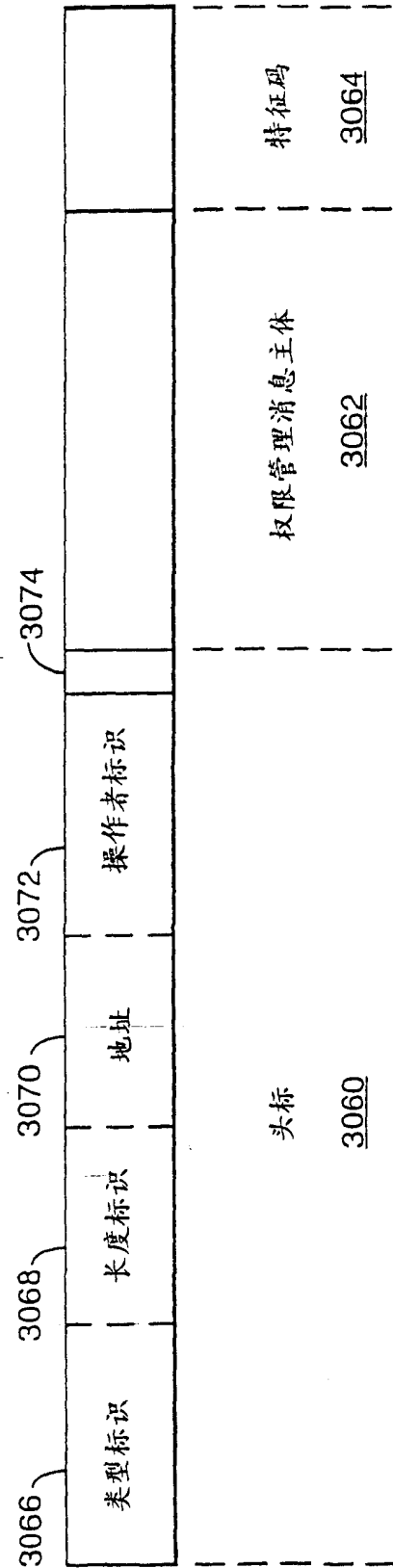


图 3

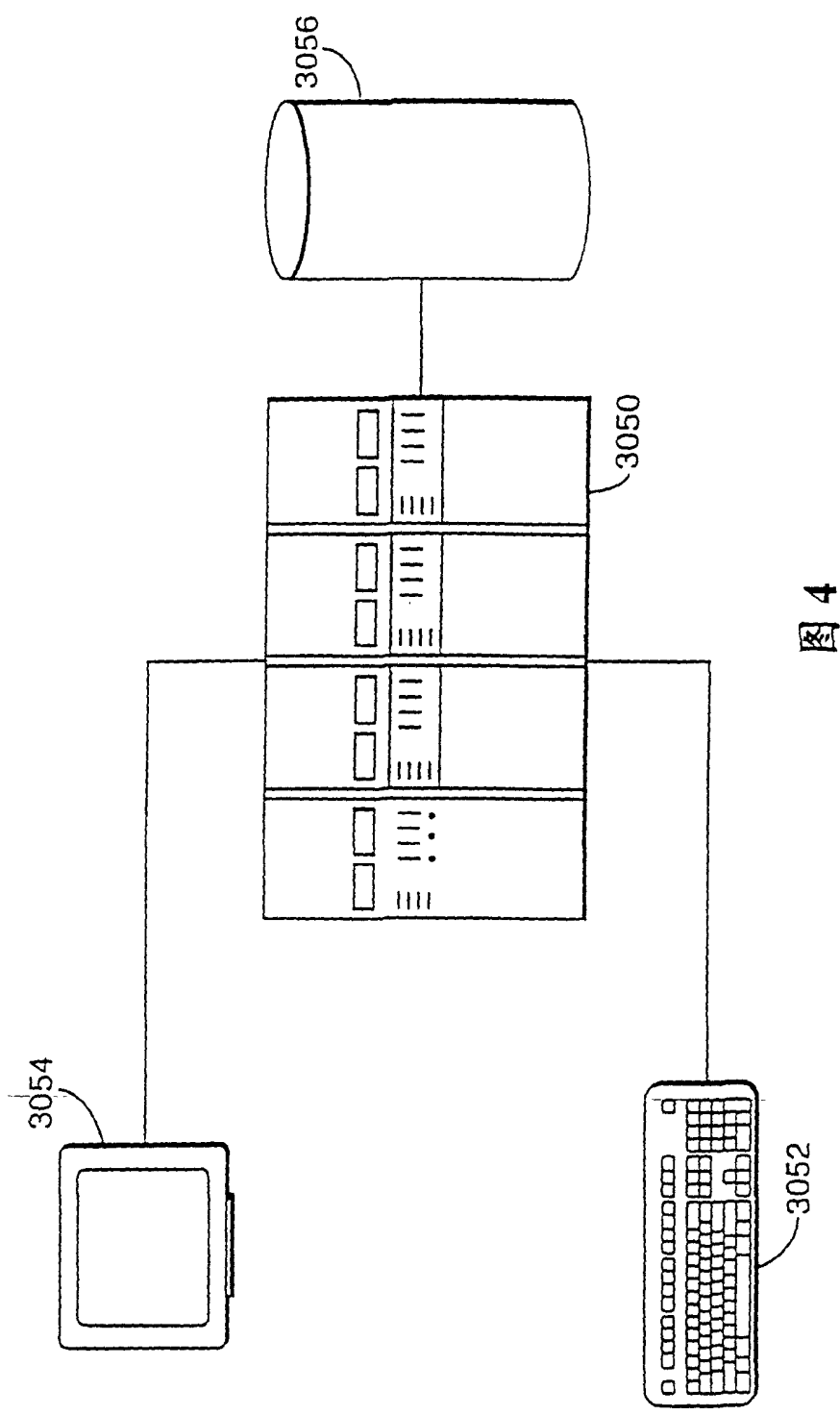


图 4

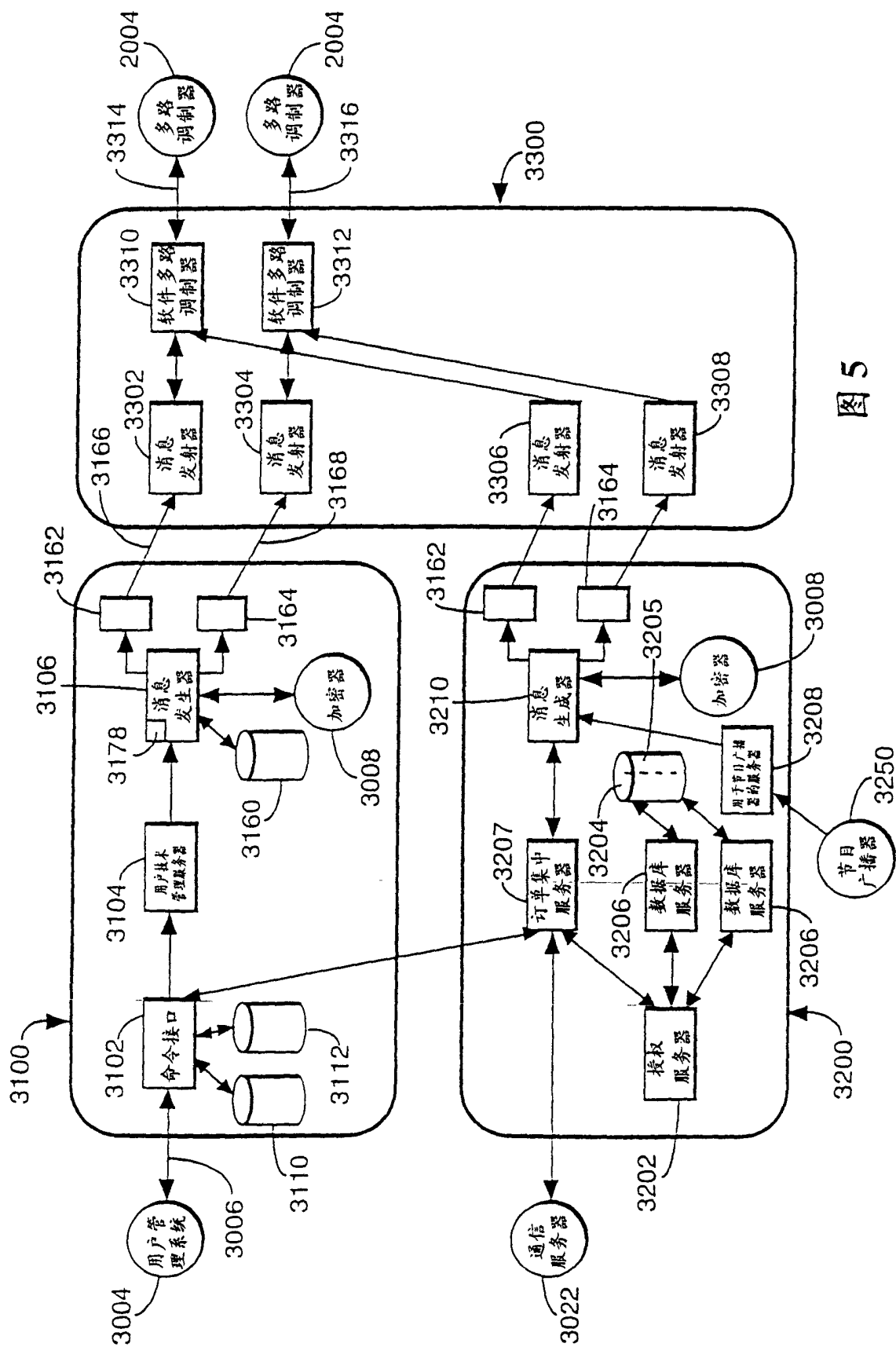


图 5

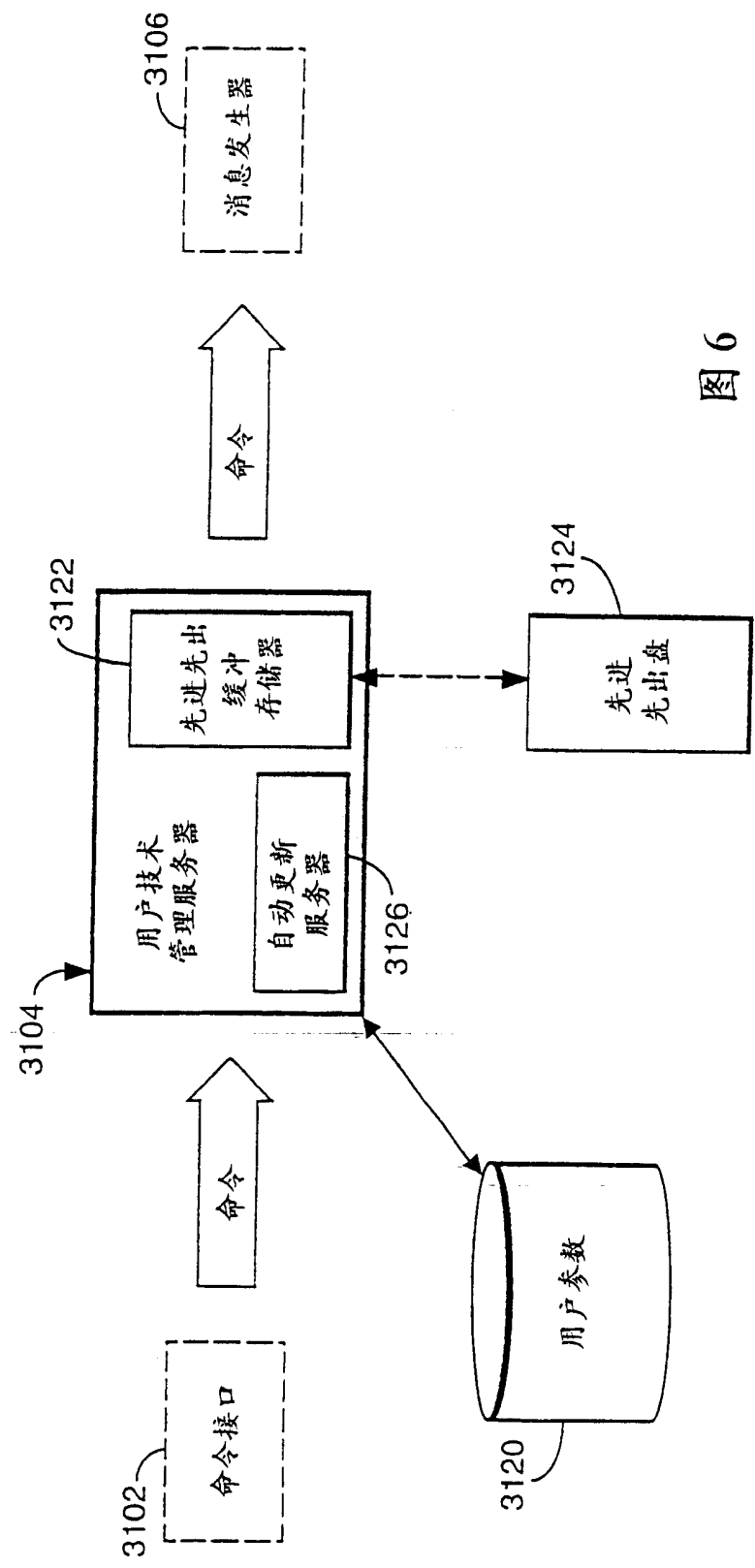
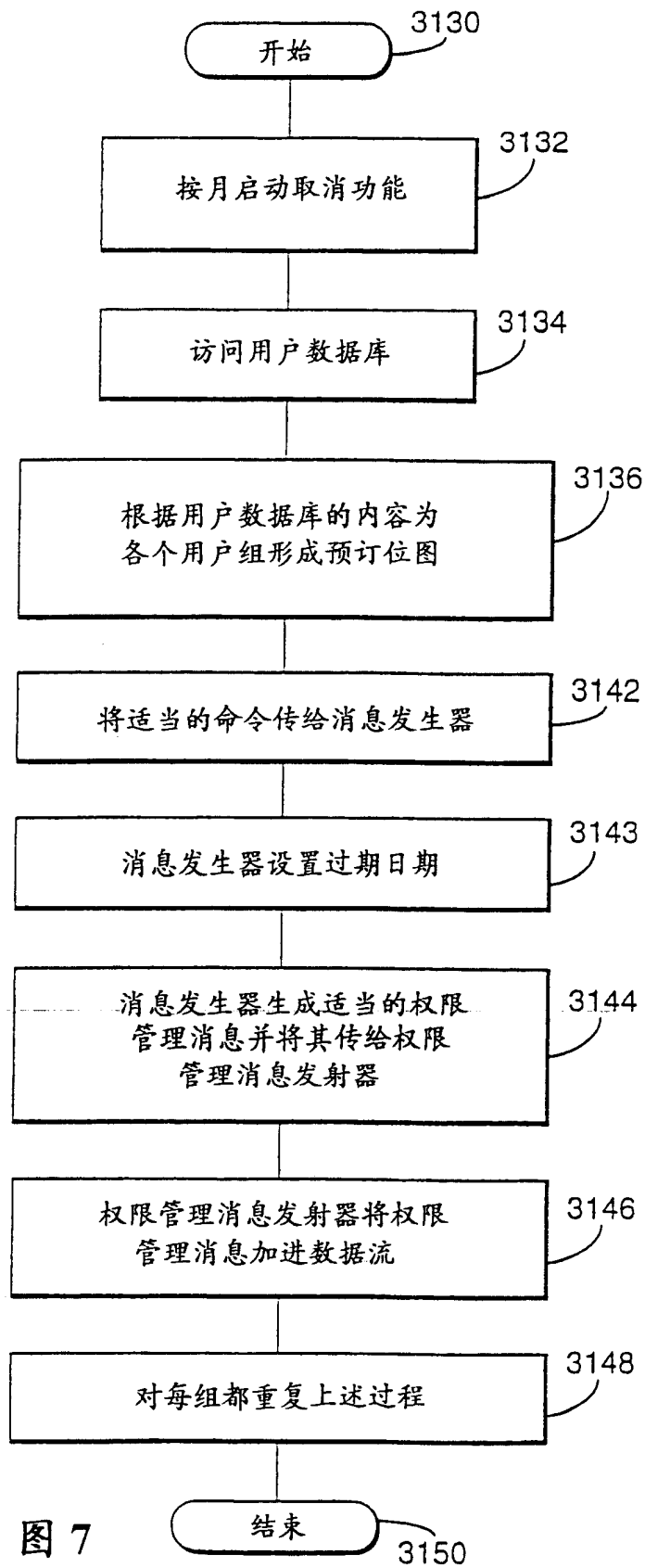


图 6



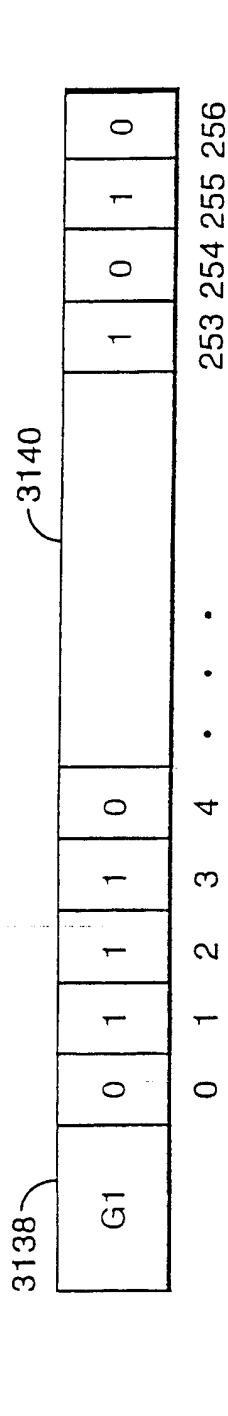


图 8

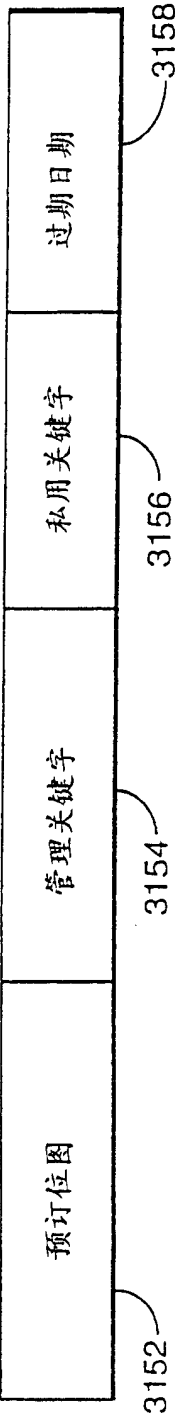
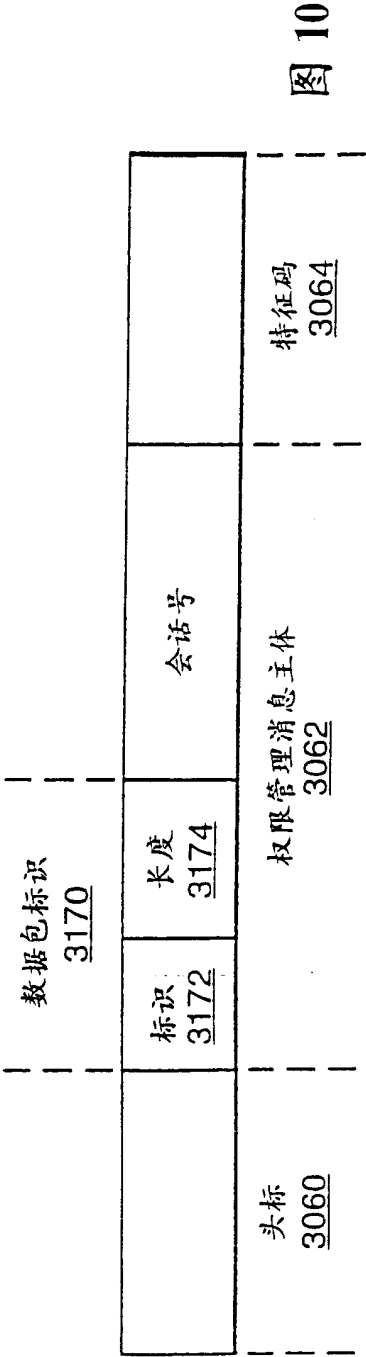


图 9



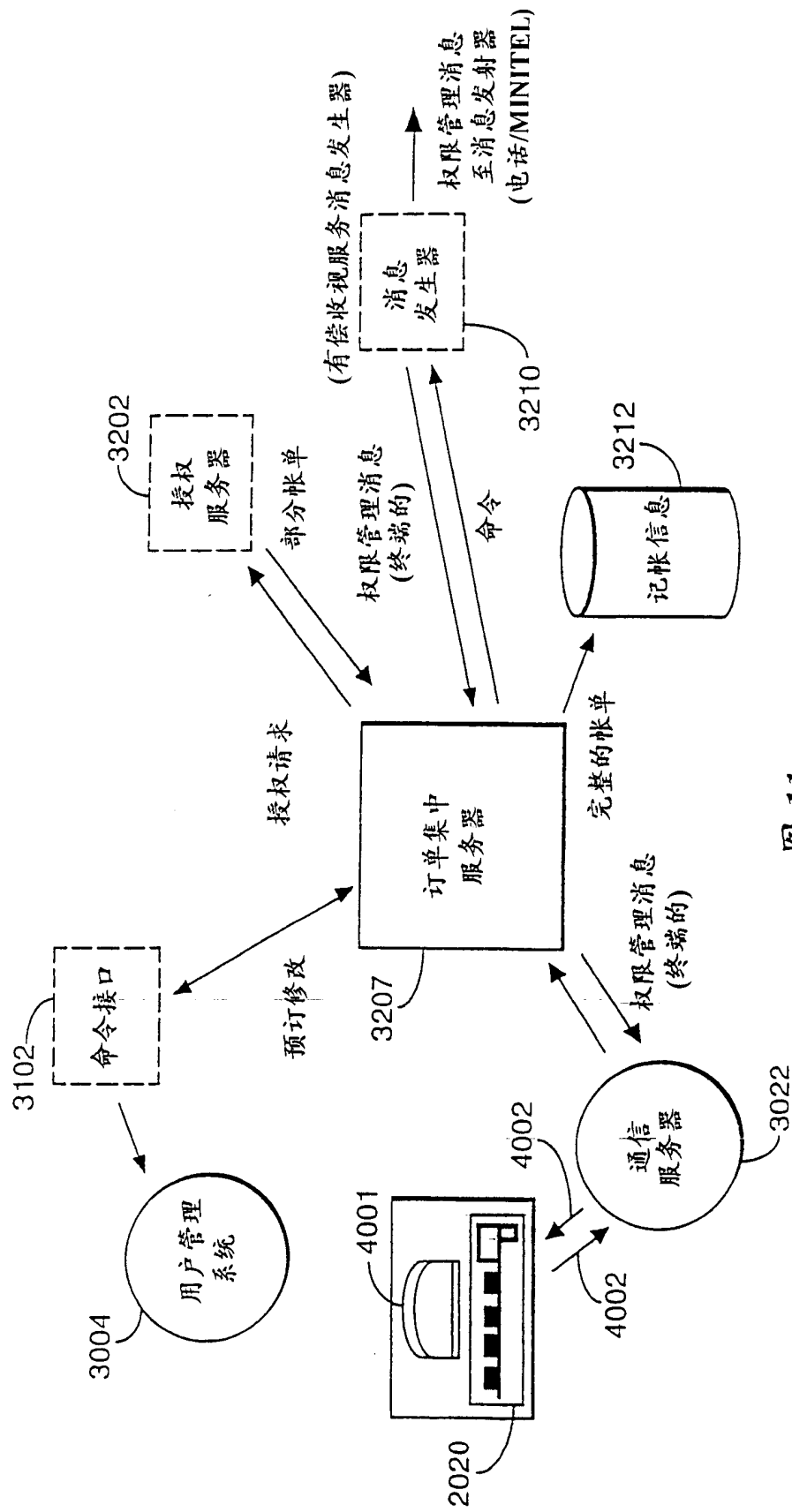


图 11

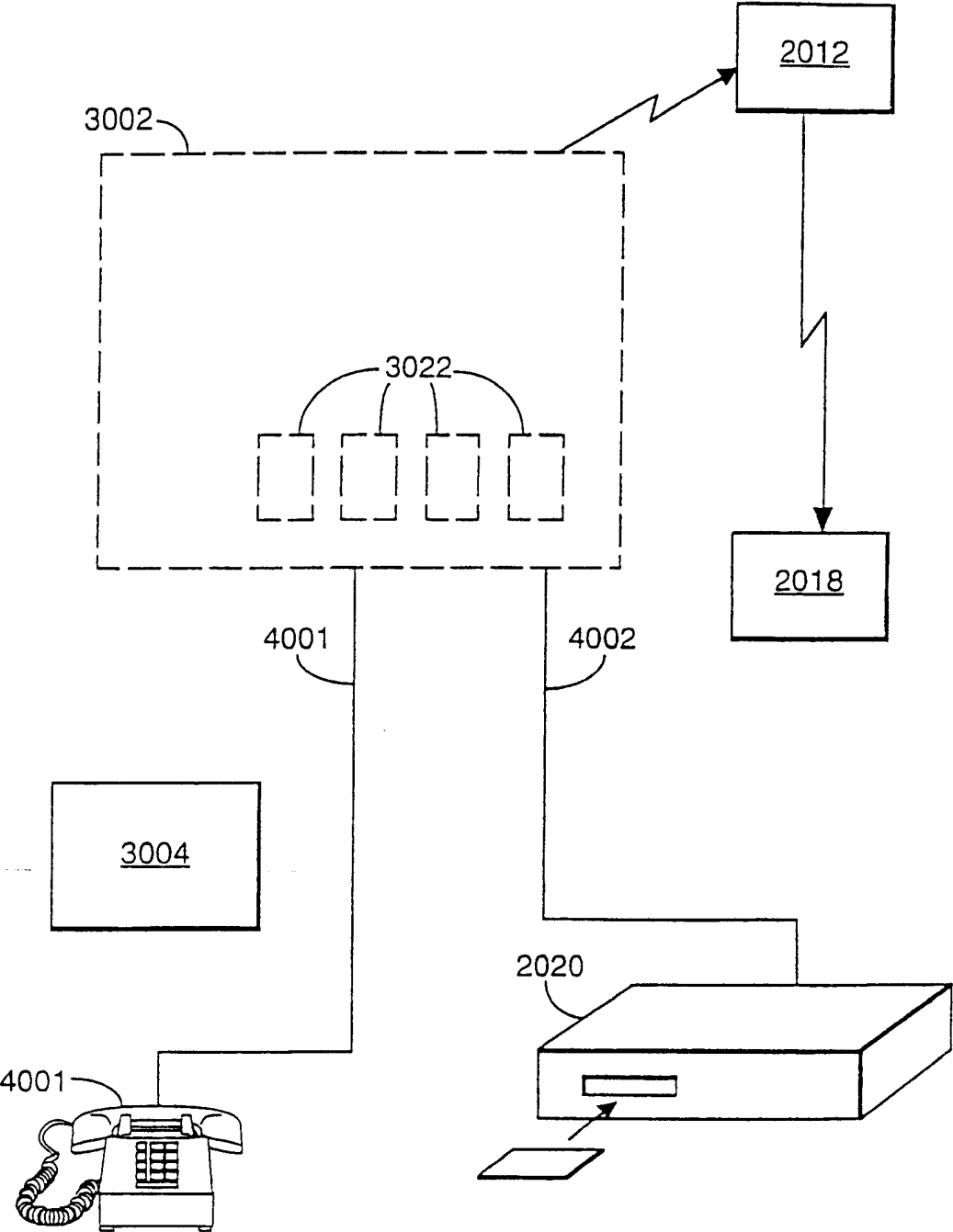


图 12

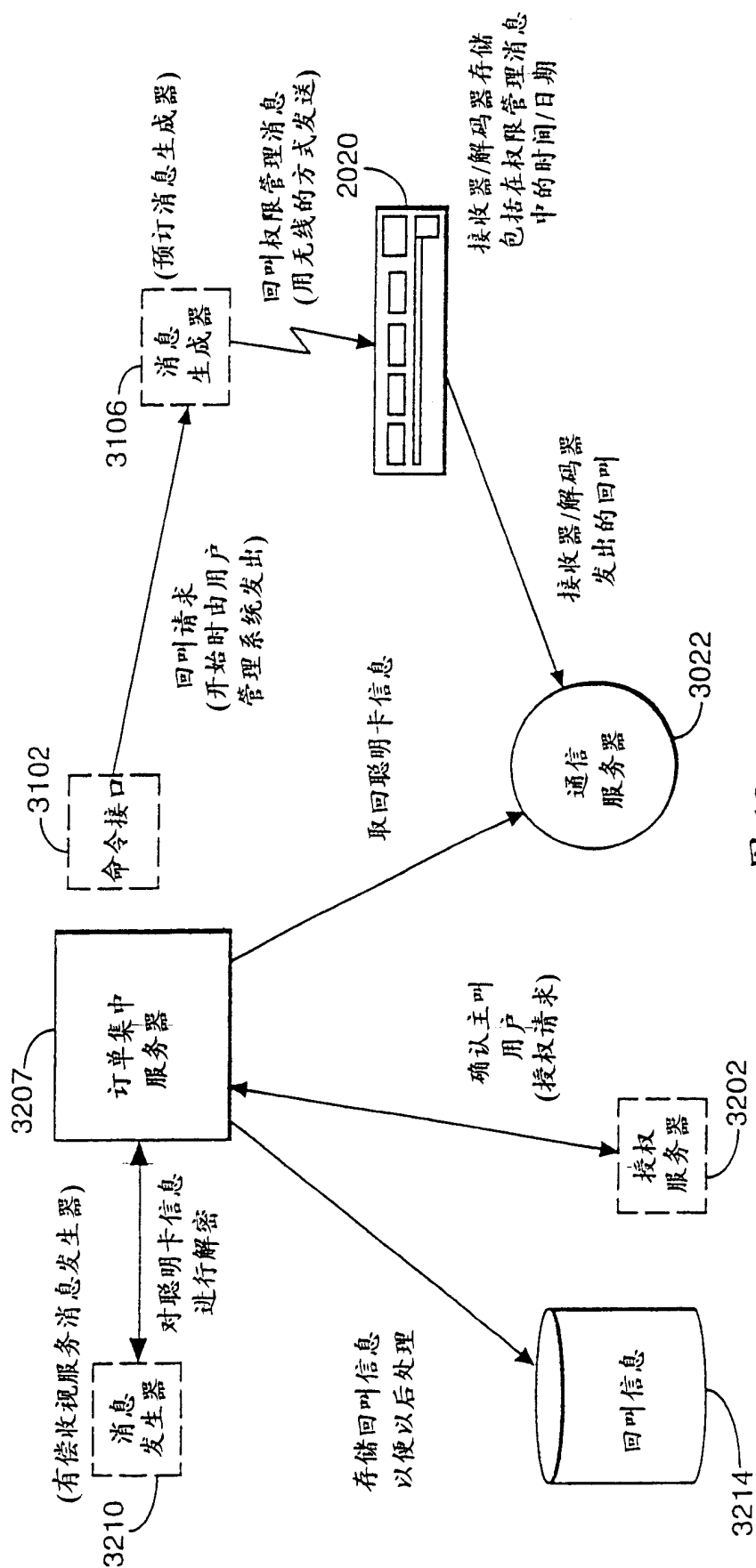
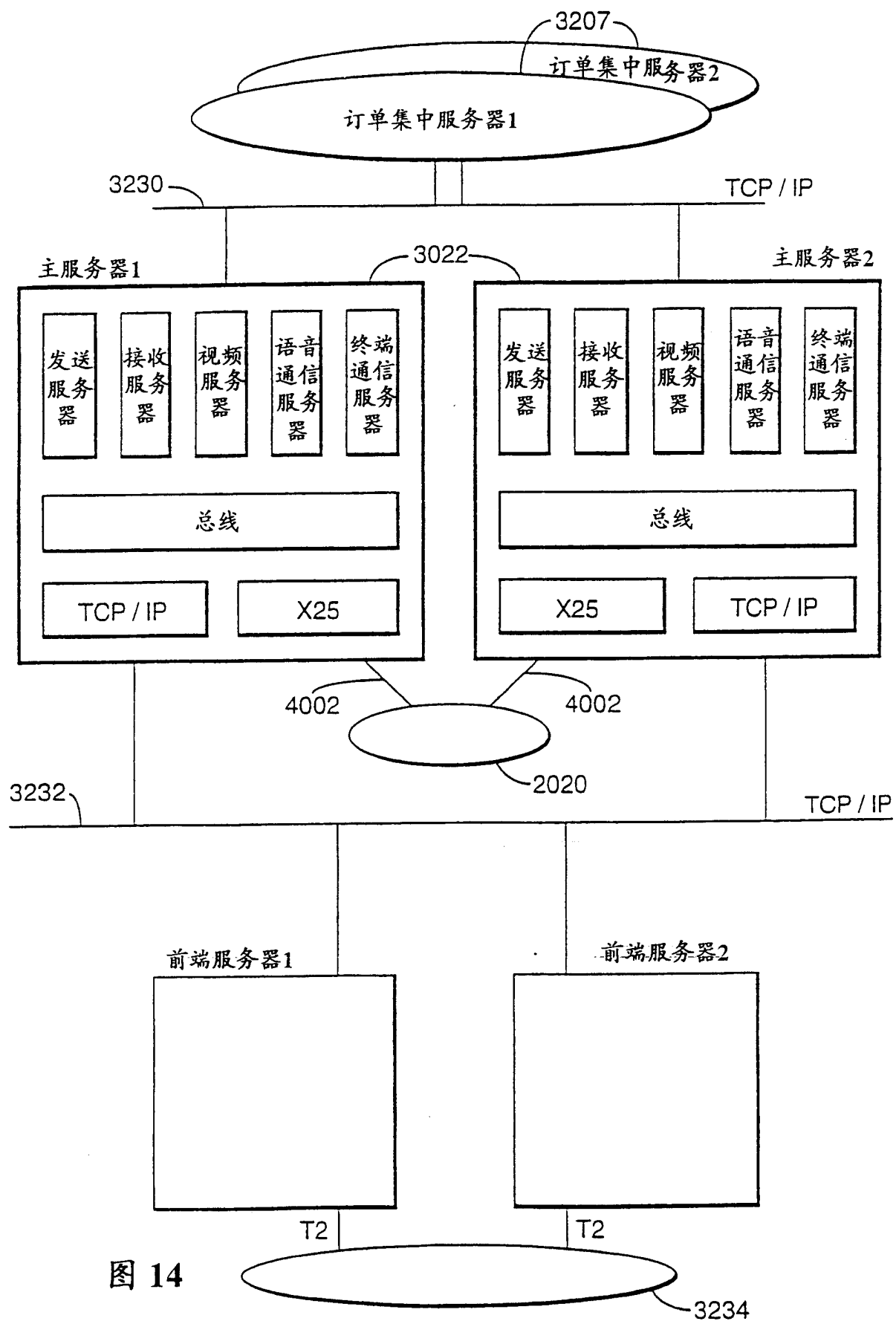


图 13



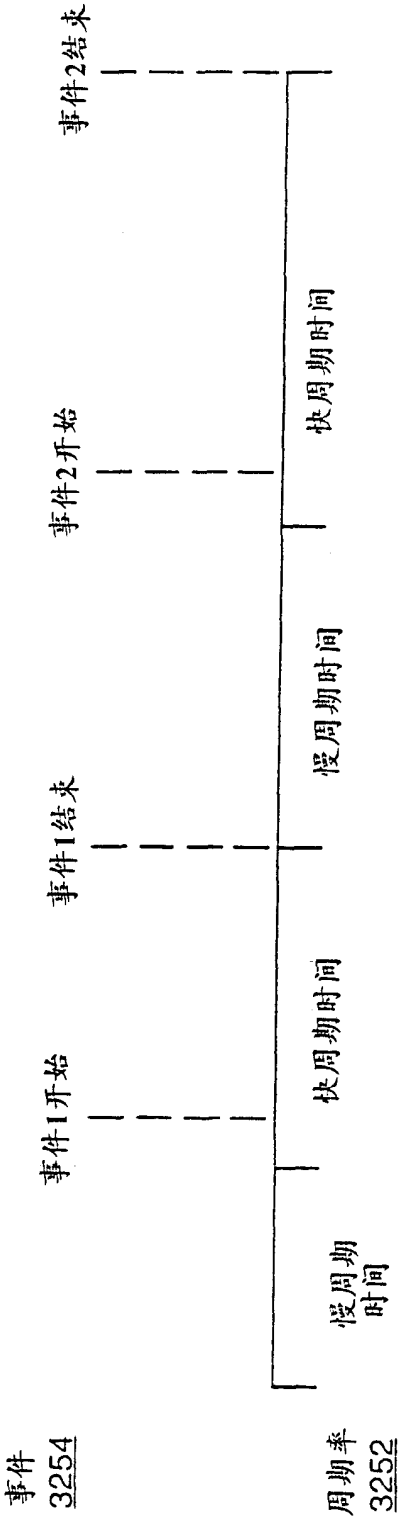


图 15

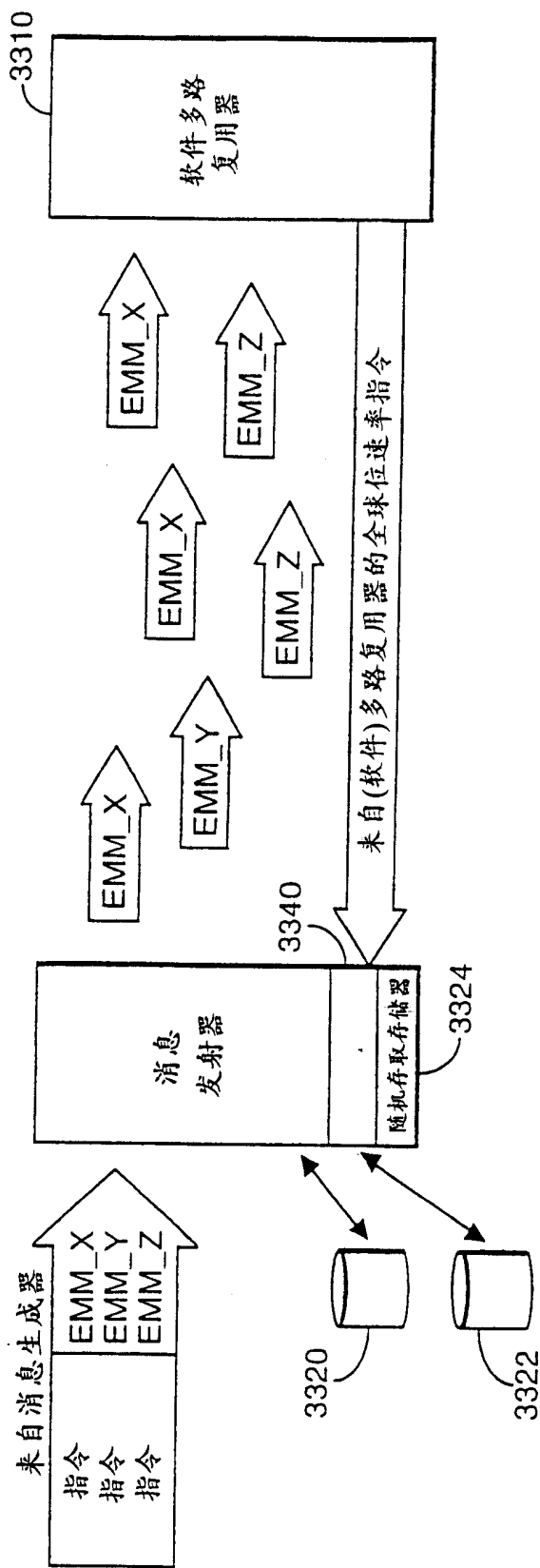


图 16

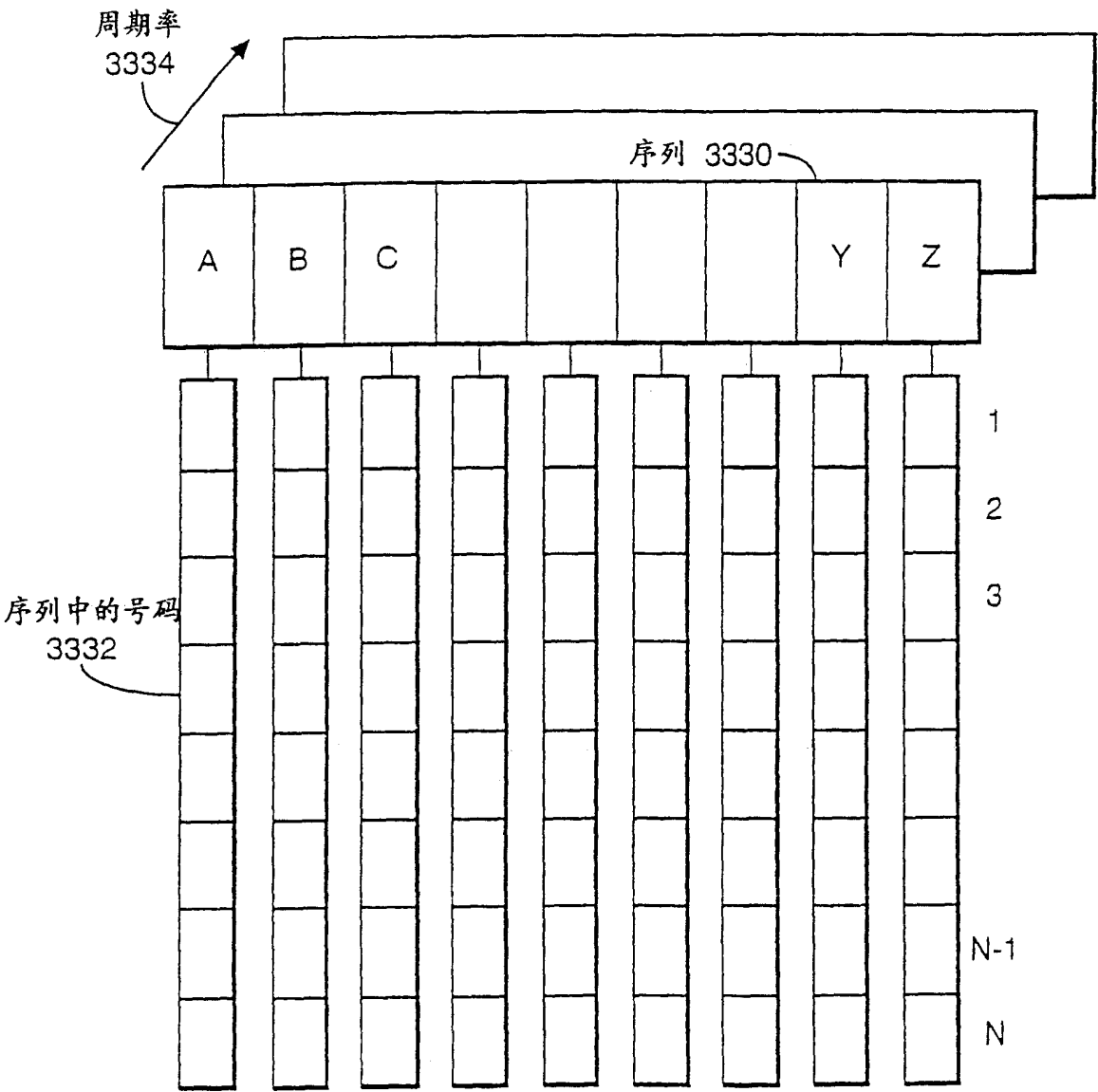


图 17

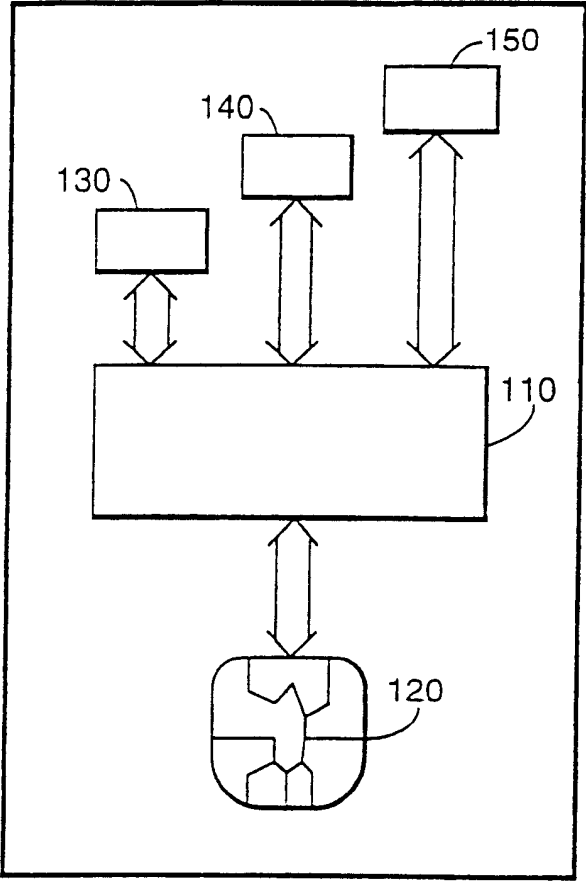


图 18

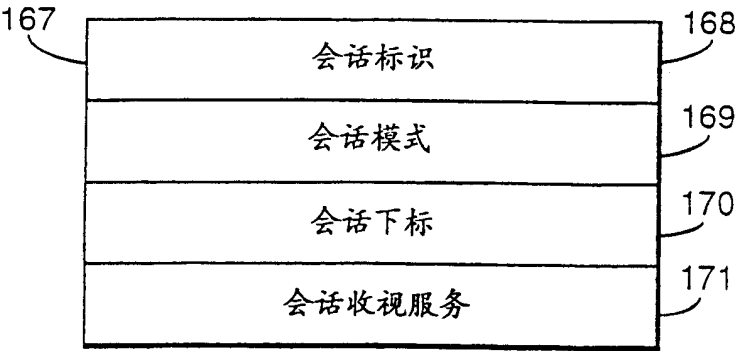


图 20

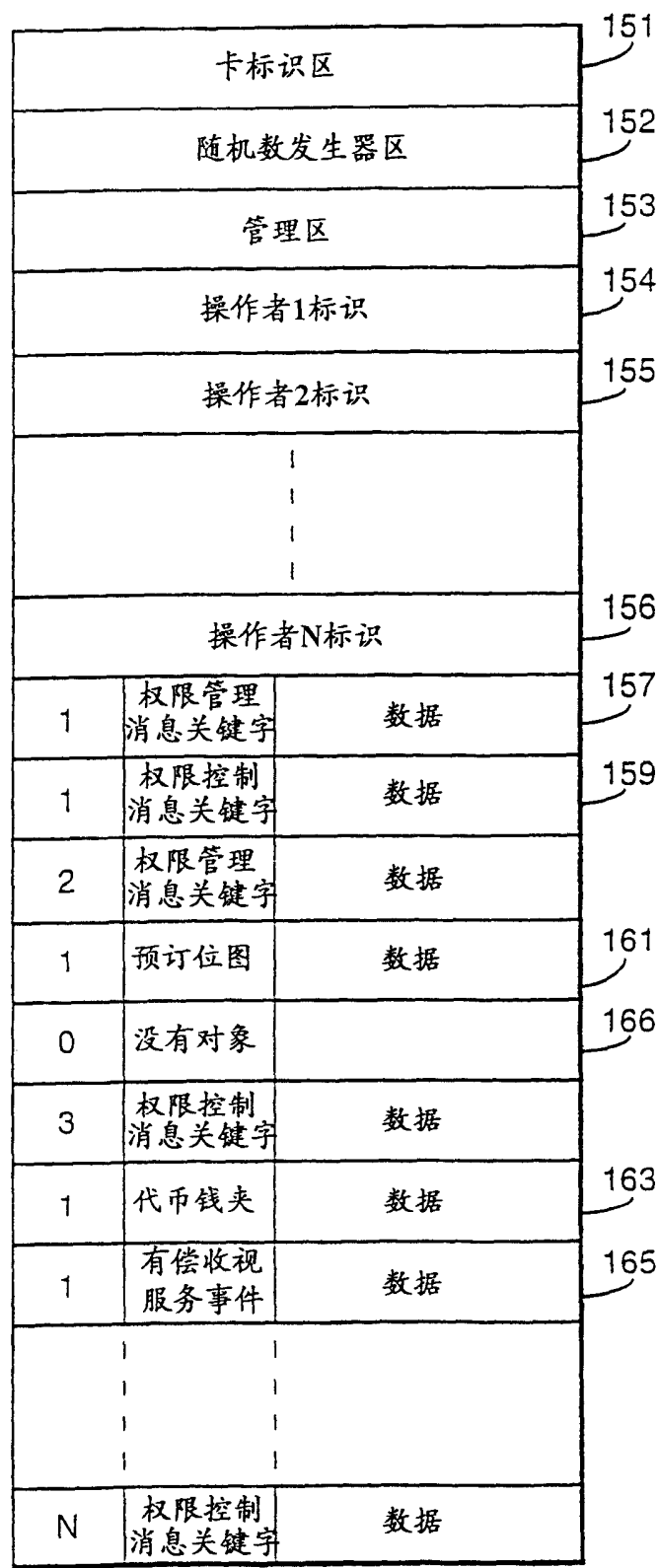


图 19