[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04Q 7/22

[12] 发明专利说明书

[21] ZL 专利号 97197207.9

[45] 授权公告日 2003 年 12 月 24 日

[11] 授权公告号 CN 1132376C

[22] 申请日 1997.6.6 [21] 申请号 97197207.9
[30] 优先权
[32] 1996.6.14 [33] US [31] 08/664,571
[86] 国际申请 PCT/SE97/01000 1997.6.6
[87] 国际公布 WO97/48208 英 1997.12.18
[85] 进入国家阶段日期 1999.2.10
[71] 专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72] 发明人 L·A·比尔斯特伦
审查员 李 明

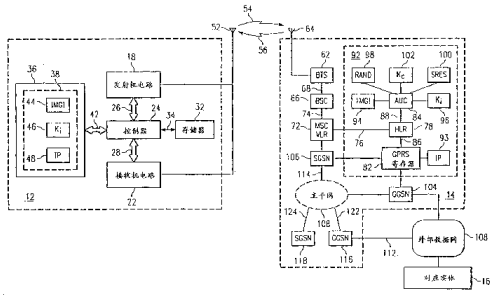
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 栾本国 李亚非

权利要求书 6 页 说明书 13 页 附图 2 页

[54] 发明名称 在通信系统中提供匿名数据传送的方法与装置

[57] 摘要

向通信台(12)提供匿名接入通信网(14)以便在其中通信的方法及相关装置。只在验证了通信台授权在网络(14)中通信之后才将接入提供给通信台(12)，但接入是在无须单个地用对该通信台唯一的永久性标识符向网络(14)标识通信台(12)下提供的。



ISSN1008-4274

1.一种用于提供匿名数据传送业务给移动电信系统中至少一组移动台以允许该至少一组移动台的一个移动台与对应的实体之间取道电信网的匿名数据传送的方法，所述方法包括下述步骤:

构成至少一组移动台，用一个组身份及一个相关的组用户验证密钥定义该至少一个组;

将该组身份与验证密钥的拷贝提供给该至少一组的各移动台;

起动附加过程，该附加过程包含该组的一个移动台发送给电信网的附加请求，该附加请求包含在所述提供步骤中提供给该至少一个组的各移动台的组身份;

响应该附加请求将网络生成的随机数分配给该移动台;

至少部分地根据验证密钥及网络生成的随机数，在移动台上计算移动台生成的带符号的响应值;

发送该移动台生成的带符号的应答给电信网;

也至少部分地根据验证密钥及网络生成的随机数在电信网上计算一个网络生成的带符号的计算的应答;

比较移动台生成的带符号应答与网络生成的带符号应答;

如果在所述比较步骤中执行的比较具有选择的值，分配给该移动台一个单独的临时移动台标识符;

通过网络在移动台与对应实体之间传送数据；以及

执行位置管理程序.

2.根据权利要求 1 的方法，其中所述构成步骤还包括至少将一个要从属于该组的移动台传送数据给它的授权的目的地地址与该组身份关联；及其中所述传送数据步骤包括将数据传送给该至少一个授权的目的地地址。

3.根据权利要求 1 的方法，其中该匿名数据传送包括分组数据传送，其中该临时移动台标识符包括临时逻辑链路身份，其中所述起动附加过程的步骤还包括在与电信网信号交换中在移动台上选择一个随机临时逻辑链路身份来跨越共享分组数据信道临时、唯一地标识该移动台，直到网络分配给该移动台一个网络生成的临时逻辑链路身份为止；以及其中该网络用该随机的临时逻辑链路身份跨越该共享的分组数据信号标识该移动台，直到生成了网络生成的临时逻辑链路为止。

4.根据权利要求 1 的方法，还包括下述步骤：在移动台与网络两者上从验证密钥与网络生成的随机数计算出加密密钥，及存储该加密密钥，及其中分配给移动台单独的临时移动台标识符、传送数据及执行位置管理过程的步骤包括按照它加密与解密传输。

5.根据权利要求 1 的方法，其中所述分配网络生成的随机数的步骤还包括为了为组身份组中的各单个移动台提供唯一的加密密钥，分配网络生成的随机数。

6.根据权利要求 1 的方法，其中所述将单独的临时移动台标识符分配给移动台的步骤还包括分配给移动台临时网络层身份及其中在所述传送数据步骤中执行的数据传送及在所述执行位置管理过程步骤中执行的位置管理过程还包括以允许移动台与对应实体之间的双向通信的方式执行从对应实体到移动台的数据传送及相关位置管理过程。

7.根据权利要求 1 的方法，其中所述将临时移动台标识符分配给移动台的步骤还包括由网络分配给移动台一个临时国际移动用户身份的步骤，以便能够在网络中按非匿名移动用户类似地处理。

8.根据权利要求 1 的方法，其中的匿名数据传送包括传送分组数据，及其中所述执行位置管理过程的步骤在移动台与对应实体之间的分组交换序列永远由移动台起动时，包括下述步骤：

只在活跃的分组交换序列的时段中，由移动台执行位置更新；

在活跃的分组交换序列之间的时段中，在网络上拒绝试图传送分组给移动台；以及

以明显的或隐含的位置更新在移动台上起动新的分组交换序列。

9.根据权利要求 1 的方法，还包括在端对端应用层上向对应的实体标识移动台的步骤。

10.根据权利要求 1 的方法，还包括在端对端应用层上在移动台与对应实体之间提供加密的步骤。

11.根据权利要求 1 的方法，还包括在所述根据组身份的传送步骤中提供对数据传送收费的步骤。

12.根据权利要求 1 的方法，其中的匿名数据传送包括传送电路交换的数据，及其中所述传送数据的步骤包括在移动台上始发电路交换的数据呼叫。

13.根据权利要求 12 的方法，其中所述执行位置管理过程的步骤

包括下述步骤:

在移动台上起动新的数据呼叫之前，移动台只是周期性地并根据需要执行位置更新；及

在电信网上拒绝试图建立终接在移动台上的呼叫.

14.根据权利要求1的方法，还包括下述步骤：在所述分配给该移动台单独的临时移动台标识符的步骤之前，如果在所述比较步骤中所执行的比较具有选择的值，在移动台与网络之间交换至少一个加密密钥.

15.根据权利要求14的方法，其中在所述分配给移动台单独的临时移动台标识符的步骤期间，移动台与网络之间的通信、传送数据及执行位置管理过程是用在所述交换步骤中交换的至少一个加密密钥加密的.

16.根据权利要求1的方法，其中所述起动附加过程的步骤包括作为其第一步骤，在移动台与网络之间交换至少一个加密密钥的步骤.

17.根据权利要求16的方法，在其中将组身份发送给电信网的附加过程的起动步骤的一部分中及在所述分配给移动台一个网络生成的随机数的步骤中的移动台与网络之间的通信发送移动生成的带符号应答，分配给移动台单独的临时移动台标识符，传送数据及执行位置管理过程是用在所述交换步骤中交换的至少一个加密密钥加密的.

18.一种在具有用于在至少第一通信台与对应实体之间实行通信的通信网的通信系统中起动数据传输的方法，该第一通信台为一组用组标识的通信台中的一个用组标识的通信台，该组中的各用组标识的通信台用组标识符标识，所述方法包括下述步骤:

提供组标识符信号给通信网，该组标识符信号具有至少表示该组标识符的值;

至少部分地响应在所述提供步骤中提供给通信网的对应于该组标识符信号的值，访问至少第一网络编码的信号及第二网络编码的信号;

将在所述访问步骤中访问的第二网络编码的信号发送给第一通信台;

响应在所述发送步骤中发送的第二网络编码的信号的接收，在第一通信台上构成第一台编码的信号;

比较第一网络编码的信号与第一台编码的信号；以及

响应在所述比较步骤中所执行的比较，授权起动第一通信台与对应实体之间的数据传输。

19.根据权利要求 18 的方法，其中的提供步骤包括将组标识符信号从第一通信台传输到通信网。

20.根据权利要求 18 的方法，其中在所述访问步骤中访问的第一网络编码的信号是通过用与该组标识符关联的验证码改变第二网络编码的信号而构成的。

21.根据权利要求 18 的方法，其中在所述构成步骤中所构成的第一台编码的信号是通过用与组标识符关联的验证码改变在所述发送步骤中所发送的第二网络编码的信号而构成的。

22.根据权利要求 18 的方法，还包括将在所述构成步骤中构成的第一台编码的信号传输给通信网的中间步骤，及其中所述比较步骤是在通信网上执行的。

23.根据权利要求 18 的方法，其中在所述授权步骤中授权起动的传输是在第一网络编码的信号实际上与第一台编码的信号对应时授权的。

24.根据权利要求 18 的方法，其中在所述授权步骤中授权的数据传输包括从第一通信台到对应实体的数据传输。

25.根据权利要求 18 的方法，其中该数据包括分组数据，及其中在所述授权步骤中授权起动其传输的分组数据是按照无线协议格式化的。

26.根据权利要求 18 的方法，包括将与组标识符关联的验证码存储在通信网的存储单元中的进一步的引导步骤。

27.根据权利要求 26 的方法，其中所述存储步骤还包括存储与组标识符关联的目的地地址，该目的地地址标识要向其传输数据的对应实体。

28.根据权利要求 18 的方法，包括将第一网络编码的信号及第二网络编码的信号存储在通信网的存储单元中的进一步引导步骤。

29.根据权利要求 18 的方法，其中提供给通信网的组标识符信号进一步具有临时唯一地标识第一通信台的值。

30.在具有用于实行至少一个第一通信台与对应实体之间的通信

的通信网的通信系统中，该第一通信台为一组用组标识的通信台中的一个用组标识的通信台，该组中的各用组标识的通信台用组标识符标识，一种用于起动数据传输的改进装置，无须单个地标识第一通信台便能起动数据传输，所述装置包括：

位于第一通信台上的组标识符信号发生器，所述组标识符信号发生器用于生成具有至少表示该组标识符的值的组标识符信号，及用于将该组标识符信号传输到通信网；

位于该通信网上的网络编码的信号访问器及发射器，所述网络编码的信号访问器及发射器用于至少部分地响应由所述组标识符信号发生器传输给通信网的组标识符信号，访问至少第一网络编码的信号及第二网络编码的信号，及用于发射第二网络编码的信号给第一通信台；

位于第一通信台上的台编码的信号发生器，所述台编码的信号发生器用于响应在第一通信台上第二网络编码的信号的接收，构成第一台编码的信号；

耦合成接收第一网络编码的信号及第一台编码的信号的指示的比较器，所述比较器用于比较第一网络编码的信号与第一台编码的信号的值，及用于响应在它们上面执行的比较有选择地授权起动第一通信台与对应实体之间的数据传输。

31.在具有用于实行通信的通信网的通信系统中，第一通信台的改进，所述第一通信台用于与通信网通信并且是一组用组标识的通信台中的一个用组标识的通信台，该组中各用组标识的通信台用一个组标识符标识，所述第一通信台包括：

组标识符信号发生器，用于生成至少表示该组标识符的值的组标识符信号，及用于将该组标识符信号传输到通信网；

接收机，用于接收通信网响应所述组标识符信号发生器传输给通信网的组标识符信号而生成的通信网生成的应答信号；以及

台编码的信号发生器，耦合成接收通信网生成的应答的指示，所述台编码信号发生器用于响应在第一通信台上接收的第二网络编码的信号，构成第一台编码的信号。

32.在至少第一通信台与对应实体之间实行通信的通信网装置，第一通信台为一组用组标识的通信台中的一个用组标识的通信台，该组

中的各用组标识的通信台用组标识符标识，所述通信网装置包括:

接收机，耦合成接收第一通信台生成的通信台生成的信号，该通信台生成的信号包含至少一个组标识符信号及一个第一台编码的信号，组标识符信号具有至少表示该组标识符的值;

网络编码的信号访问器及发射机，用于至少部分地响应所述接收机接收的组标识符信号，访问至少第一网络编码的信号及第二网络编码的信号，及用于发送该第二网络编码的信号到第一通信台；以及

比较器，耦合成接收第一网络编码的信号及第一台编码的信号的指示，所述比较器用于比较第一网络编码的信号与第一台编码的信号的值及用于响应在它们上面执行的比较，有选择地授权起动第一通信台与对应实体之间的数据通信.

在通信系统中提供匿名数据传送的方法与装置

本发明一般涉及数据传输，诸如在提供分组无线电业务的通信系统中传输的分组数据或在提供电路交换通信的通信系统中传输的电路交换数据。更具体地，本发明涉及用于给通信台提供到构成通信系统的一部分的通信网的匿名接入的方法及实现该方法的相关装置。虽然提供了对网络的匿名接入，但只有在验证了该通信台被授权与网络通信之后才许可这种接入。一旦提供了该匿名接入，便允许在通信台与对应实体之间的数据通信，而无须用永久性唯一的标识符对通信网标识该通信台。

由于提供了通信台对网络的匿名接入，便可实行往来于通信台的数据通信，而无须用该通信台唯一的永久性标识符来唯一地标识该通信台。特定通信台及其用户是保持匿名的。本发明可用来向移动台提供匿名接入到分组无线电业务，诸如新建议的在移动通信全球系统（GSM）电信系统标准中标准化的通用分组无线电业务（GPRS）。执行验证来保证移动台是授权与该网络通信的。

电子学与通信领域中的进展已允许引入与商业化许多新型的通信系统。信息能以以前不可能或无法提供的方式传递给地点。

蜂窝式电话便是由于这些进展而已成为可能的通信系统的范例。由于在发送台与接收台之间不需要固定的有线连接在它们之间就可实现通信故按照蜂窝式电话或其它无线电通信系统的通信是有利的。当使用固定的或硬接线的连接来实行通信不方便或不能现实时，用蜂窝式电话或其它无线电电信系统实行通信特别有利。按照蜂窝式通信系统的一些传统通信有时称作电路交换通信，由于数据是在信道上和在通信期间专用的电路路径传输到特定的发送与接收台对。

蜂窝式电话以及其它类型的无线电电信领域中的继续进展已允许对已装机的蜂窝式及其它无线电电信网引入新的业务及新的通信方式。

例如，已提出建议向现有的蜂窝式及其它通信网提供传递分组数据的能力，诸如上述通用分组无线电业务（GPRS）。将要在发送与接

收台之间传输的信息构成离散的数据分组。可在通信信道上将单个的分组从发送台发送到接收台。由于信息是利用离散的分组传递的，发送台只在发送离散的分组所需的时段中利用信道。因此，信道通常是多个发送台使用的共享信道。

由于这种共享信道的共享性质，有可能必须将要由发送台传输的数据分组排队直到成为能利用共享的信道。然而，由于共享信道是共享的，不需要分配专用通信信道给发送台来实行分组通信，在共享信道上传输数据的费用可由许多用户分担。通过因特网进行的通信及涉及寻呼网的通信也是利用分组数据的数据传输的通信系统的范例。

上述GSM数字蜂窝式通信网为已建议引入GPRS及已公布建议的标准的蜂窝式通信系统的范例。对应于这些标准构成的GSM移动台能通过GSM网传递分组数据。

在提供GSM移动台接入GSM网在其中通信之前执行验证过程。标准验证过程是在GSM标准中公布的。例如在转让给本发明的受让人的美国专利号5,282,250中描述了示范性验证过程。这里通过引用将其内容结合在此。

执行验证过程来保证移动台是授权在系统中通信的。为了类似的原因，其它蜂窝式电话及其它无线电电信系统利用类似的验证过程。

作为GSM通信系统中的验证过程的一部分，将永久与唯一地标识移动台或至少要向其收取提供的网络通信费用的一方的国际移动用户身份（IMSI）提供给网络。响应这一提供的身份，验证过程验证该移动台是授权通过网络通信的。通过提供IMSI给网络，将必要的用户身份提供给网络。

已提出了利用按照GSM网提供的GPRS的通信应用的若干建议。这些应用也可能类似地按照其它类型的蜂窝或其它通信系统提供。这些建议能在也允许传统的电路交换（如传统的话音电话）通信的GSM移动台，或者在只提供分组数据通信的移动台中的某些建议的应用中实现。取决于移动台可在其中工作的通信系统，移动台一词用来指只允许电路交换的通信、只允许GPRS通信、或至少GPRS通信与电路交换通信两者的设备而言。

在准许移动台接入通信网之前使用的现有验证过程要求将IMSI或其它永久的唯一标识符提供给网络。这一用其IMSI或其它永久的唯

一标识符来识别终端的要求会禁止实现某些建议的应用。在若干这些建议的应用中，会不利地影响移动台的用户的隐私权。

已建议的示范性应用为交通遥测应用，在其中，车载移动台发送位置、方向及速度信息给交通控制中心。根据多个车载移动台向交通控制中心传送的这些信息，便能在必要时实现交通控制操作来缓解交通堵塞。

已建议的另一示范性应用为自动收费应用，在其中，将通过自动收费门或收费点的自动运输工具提供给收费控制中心。当通过自动收费门时，车载移动台发射信号给收费控制中心。

为了允许实现这些应用以及其它应用而并没有不利地影响移动台的用户的隐私权，要求移动台匿名接入网络。但是，仍需要验证移动台以防止网络的非授权使用。

因此，所需要的是用来向移动台提供匿名接入通信系统的通信网的方式，借此允许移动台在通信系统中传递数据，同时在提供移动台这种匿名接入系统之前还提供用来验证该移动台的方式。

鉴于关于数据通信的这一背景信息，演变出了本发明的重大改进。

本发明有利地提供了向通信台提供匿名接入通信系统的通信网以便在该通信系统中传递数据的方法及实现该方法的有关装置。接入是只在验证了该通信台是授权在网络中通信之后才提供给通信台的，但接入是在不用对该通信台的唯一永久性标识符单独地标识该通信台的情况下提供的。

在本发明的一个方面中，通信台包括可在通信系统中工作的移动台，该通信系统提供诸如 GPRS 等分组无线电业务，允许在移动台与对应实体之间传送分组数据。向移动台提供对通信网的匿名接入。在准许移动台接入网络之前，验证该移动台为允许利用通信网的一组移动台的一个成员。借此，移动台得到验证，而无须使用移动台的永久性唯一标识符来验证移动台。

可将本发明的教导有利地用来提供对作为 GSM 数字蜂窝式通信系统的一部分提出的广义分组无线电业务的匿名接入。移动台对 GSM 网的接入，并借此向移动台提供广义分组无线电业务，是在不要求移动台向网络提供该移动台的国际移动用户身份（IMSI）的情况下提供的。

作为替代，移动台向 GSM 网提供国际移动组身份（IMGI）。借此便能验证该移动台为授权提供分组无线电业务的一组匿名移动台的成员。借此向移动台提供服务而无须移动台向网络提供其 IMSI。

在本发明的另一方面中，向移动台提供对通信网的匿名接入以允许其通过它传送电路交换数据。

在一个实施例中，只允许向移动台提供分组无线电业务。在另一实施例中，该移动台构成允许诸如在传统蜂窝式通信系统中所提供的电路交换电信的移动台的一部分。在另一实施例中，移动台既允许电路交换通信又允许分组数据通信。

利用匿名移动台身份来进行 GPRS 匿名接入包含操作员特定的组身份及随机数来提供已在 ETSI Tdoc SMG3 95 G096 中提出的唯一身份。然而，在文件中未提出提供匿名接入业务的解决方法。

在一个示范性实现中，利用本发明来起动交通遥测应用中的分组数据传输，例如向交通控制中心提供车辆交通信息。在这一应用中，为了隐私原因要求匿名通信。移动台位于车辆上并发送表示关于这些移动台所在的车辆的位置上的位置、方向与速度信息的分组数据。根据这些信息，便能实行诸如红绿灯控制操作等交通控制操作来缓解交通堵塞。由于授于移动台的匿名接入，便能保持移动台所在的车辆的用户或所有人的隐私。

在另一示范性应用中，在自动收费应用中利用本发明。在通过自动收费门时车载移动台发射信号。将这些信号的指示用诸如 GSM 通信网提交给收费控制中心。这便允许用诸如根据编码智能卡等电子方式支付收费。准许移动台匿名接入网络使得移动台的身份对于网络是匿名的。取决于支付方法，可以有选择地将移动台的永久性身份的指示提供给收费控制中心，但是以对通信网透明的方式进行。即保持通信网不知道移动台的永久性身份。

其它交通遥测应用以及其它应用也能类似地实施本发明的教导来提供通信台对通信网的匿名接入，同时还验证通信台来保证该通信台是授权与通信系统通信的。

因此，还可将本发明的教导有利地用在通信系统中来提供匿名接入以允许电路交换数据的通信。

因此，在这些与其它方面，公开了用于在通信系统中起动数据传

输的方法及其相关的装置。通信网实现至少第一通信台与对应实体之间的通信。该第一通信台为一组组标识的通信台的一个组识别通信台。该组中的各个组识别通信台是用组标识符识别的。数据传输的起动无须用对第一通信台唯一的永久性标识符来单个地识别第一通信台。将组标识符信号提供给通信网。该组标识符信号具有至少表示该组标识符的值。至少部分地响应提供给通信网的组标识符信号构成至少第一网络编码信号及第二网络编码信号。然后将第二网络编码信号发送给第一通信台。第一通信台响应第二网络编码信号的接收构成第一台编码信号。然后将第一网络编码信号与第一台编码信号比较。然后根据这些比较授权起动第一通信台与通信网之间的数据传输。

从下面简述的附图、下面对本发明的最佳实施例的详细描述及所附权利要求书中将获得对本发明及其范围的更完整的理解。

图 1 示出示范性通信系统的功能框图，其中本发明的实施例可进行操作来构成其一部分。

图 2 示出部分功能框，部分地示意性说明利用本发明的实施例来向控制中心提供车辆交通信息的示范性应用。

图 3 示出部分功能框，部分地示意性说明利用本发明的实施例在车辆收费门上自动收取车辆交通通行费的另一示范性应用。

图 4 示出列出本发明的实施例的方法步骤的流程图。

首先参见图 1，示范性通信系统提供移动台 12 对通信网 14 的匿名接入。这里的通信系统构成 GSM 通信系统，移动台 12 构成 GSM 移动台，而通信网包含 GSM 基础结构网。

在本发明的实施例的操作期间提供给移动台 12 的匿名接入允许移动台 12 取道通信网 14 与这里为对应实体 16 的远程定位的设备通信，而无须用唯一地标识该移动台的永久性标识符标识该移动台 12。虽然为了示例的目的，只示出了单个移动台 12，但多个移动台能取道通信网 14 通信。移动台 12 为一组移动台之一，该组中各移动台用一个组标识符公共标识。

在本发明的一个实施例中，移动台 12 允许电路交换数据的通信。而在本发明的另一实施例中，移动台 12 至少允许分组数据及电路交换数据两者的通信。在图中所示的示范性实施例中，移动台 12 可取道这里构成 GPRS 通信网的通信网 14 进行操作来传递分组数据。

移动台 12 包含发射机电路 18 与接收机电路 22 等。发射机电路 18 与接收机电路 22 的操作受这里标识为控制器 24 的处理电路的控制。控制器 24 分别取道线路 26 与 28 耦合在发射机与接收机电路 18 与 22 上。控制器还取道线路 34 耦合在存储装置 32 上。在其中的通信系统包括 GSM 通信系统的示范性实施例中，发射机与接收机电路分别进行操作以发射及接收 TDMK、GMSK 调制的信号。在其它实施例中，移动台 12 的电路当然可进行操作来生成与接收以其它方式调制及其它通信方式中的其它类型的通信信号。

用户身份模块（SIM）卡 36 位于移动台 12 上并包含存储器元件 38。SIM 卡 36 以传统方式耦合在移动台 12 的电路上，这里表示为用线路 42 连接 SIM 卡 36 与控制器 24。

存储器元件 38 包含用于存储国际移动组身份（IMGI）44、验证密钥（Ki）46 及可选用的一个或多个目的地地址的存储单元。这里示出了单一的因特网协议地址（IP）48。在一个实施例中，SIM 卡 36 的存储元件 38 可进一步包含附加的存储单元，用于存储其它信息，诸如传统上在按照通过移动台 12 的传统电信的验证过程中使用的国际移动用户身份（IMSI）及相关验证密钥 Ki。在移动台 12 的工作期间生成的上行信号是由发射机电路 18 形成并由天线 52 变送的。传输给移动台 12 的信号是由天线 52 检测并在其上换能及作用在接收机电路 22 上的，全部以传统方式。

通信网 14 接收移动台 12 生成的上行信号 54 并将下行信号 56 发射到移动台 12。通信网 14 包含可以传统方式操作来利用天线换能器 64 收发上行与下行信号 54 与 56 的基地台（BTS）62 等。基地台收发机 62 以传统方式取道线路 68 耦合在基地台控制器（BSC）66 上，而基地台控制器 66 又取道线路 74 耦合在移动业务交换中心（MSC）72 上。访问者位置寄存器（VLR）位于移动业务交换中心上，这里一起作为 MSC/VLR 参照。移动交换中心 72 及位于其上的 VLR 以传统方式用线路 76 耦合在基地位置寄存器（HLR）78 上。

HLR78 分别取道线路 86 与 88 耦合在通用分组无线电业务(GPRS)寄存器 82 及验证中心（AUC）84 上。在本发明的一个实施例中，GPRS 寄存器 82 及 AUC84 与 HLR78 位于一起；这一实施例用虚线示出的框 92 表示。耦合在 GPRS 寄存器 82 上的存储单元 93 存储类似于 IP 地址

48 的 IP 地址值。

验证中心 84 包含用于存储包含对应于存储在移动台 12 上的 SIM 卡 38 上的 IMGI44 及 Ki46 的国际移动组身份（IMGI）94 及验证密钥（Ki）96 的组身份。AUC84 的处理电路生成随机数 RAND98。将 RAND98 的值存储在通信网的存储单元中。在 GPRS 上下文中，RAND98 是存储在 GPRS 寄存器或任何适当地方的。AUC84 的处理电路可进行操作执行根据 RAND98 与 Ki96 的值构成用 SRES100 指示的带符号的响应（SEES）值的算法。还根据 RAND98 与 Ki96 的值用一种算法计算密钥（Kc）102。

通信网进一步示出为包含国际 GPRS 支持节点（GGSN）104 及服务 GPRS 支持节点（SGSN）106。GGSN104 与 SGSN106 为逻辑实体。GGSN104 提供对外部数据网的接口，这里为外部数据网 108。GGSN104 可进行操作，诸如翻译数据格式，发出协议与地址信息信号，以便允许不同网络之间的通信。GGSN104 可进一步进行操作来选择路由到 SGSN 上，诸如 SGSN104，来执行协议转换及查询来自 GPRS 寄存器 82 的数据。

SGSN106 提供诸如去往及来自节点 106 的服务区的分组数据的分组路由选择，信令与 MSC/VLR72 及 GPRS82 的交换，以及关于诸如移动台 12 等分组数据移动台的控制、监视及参数存储功能。如图中所示，服务节点 104 与 106 是用主干网 108 耦合在一起的，这种耦合用延伸到主干网 108 的线路 112 与 114 表示。进一步示出诸如 GGSN116 与 SGSN118 等附加支持节点为耦合在主干网 108 上的，这种耦合分别用线路 122 与 124 表示。附加服务节点能额外表示及类似地耦合在一起，也构成通信网 14 的部分。

下面主要相对于分组数据的匿名传送描述本发明的实施例的示范性操作，例如相对于 GPRS 阶段 1 服务描述、GSM02.60，b1.3.0，5.4.4 节描述的。这种描述定义允许将匿名的移动台始发的（MO）分组传送到预定的目的地地址的匿名接入（AA）业务的要求。当然应理解可对下面的电路交换数据而不是分组数据的通信及其它通信系统中的数据通信的操作的描述作出适当的修改。

虽然移动台 12 的接入允许在移动台 12 与对应实体 16 之间匿名与透明地进行数据通信，但必须验证移动台 12 来保证移动台 12 应是准许这种接入来用通信网 14 通信的。本发明的操作，在允许移动台匿名接入用通信网 14 的通信的同时，保证该移动台是授权在其中通信的。

在本发明的一个实施例中，进一步准许移动台 12 与对应实体 16 之间的双向通信，全都同时保持移动台在通信网 14 中的匿名性。

为了提供以类似于传统 GPRS 点对点传输中所利用的操作的方式进行跨越空中接口的可靠传输，采用了公认的逻辑链路操作。在示范性实施例中，假定 GPRS 业务是基于构成网络层协议的因特网协议（IP）的。在其它实施例中能够支持诸如传统的 CLNP 或 X.25 协议等其它协议。这些假定仅仅是为了描述图 1 的示范性实施例而作出的。在其它实施例中，能利用其它类型的操作及其它类型的协议作为替代。

当要在移动台 12 与对应实体 16 之间传递数据时，便实现附加/激活过程，即注册过程。

移动台 12 必须向通信网 14 标识自己。为了这样做，移动台 12 将组标识符信号发送给网络。该组标识符信号具有表示 IMGI44 的值。在一个实施例中，组标识符信号进一步包含目的地地址 48。为了立即在共享的分组数据信道上进行通信的目的而唯一地标识移动台 12，随机标识符，这里为随机临时逻辑链路身份（TLLI），也构成该组标识符信号的一部分。该随机 TLLI 是例如存储在存储器元件 32 的存储单元中或者由控制器 24 以某种方式生成的。对于特定的通信，随机 TLLI 的传输允许单个地识别移动台 12 直到由 SGSN 分配给该移动台一个 TLLI 为止，但该随机 TLLI 并不向通信网 14 提供移动台 12 的永久性身份。

如果附加/激活过程采用传统的专用 GSM 信号信道，随机 TLLI 是不需要的。

已在 ETSI GPRS SMG2/3 特定的 95G087 及 Tdoc 132/96 中建议了在共享分组数据信道上的 GPRS 附加与路由选择区更新的初始部分中使用基于 IMSI 的移动台的随机 TLLI。这些文件还讨论了随机 TLLI 碰撞的内在危险的处理。

首先，通过为随机 TLLI 分配足够大的位数（对于所述文件中所建议的随机部分为 22 位，但必要时可分配更多的位），便能使在使用随机 TLLI 的非常短的时段（几秒钟）中，同一 SGSN 区中两个或更多移动台选择同一随机 TLLI 的概率极低。

在随机 TLLI 碰撞的罕见事件中，可使用 Tdoc132/96 中建议的碰

撞解决规则。如果在报文序列的给定点上或在给定的上下文中所接收的报文不与期望的报文对应，这些规则基于中止及用新的随机 TLLI 重新启动信号报文序列。

然而，在匿名接入的情况中，由于不能使用对各移动台独一无二的与 IMSI 相关的信息，解决基于上下文的碰撞的措施更为有限。在本发明的一个实施例中，移动台以加密的形式（在已经建立了加密密钥的附加过程的后期）提供国际移动台设备身份（IMEI）作为基于上下文的碰撞解决措施。在本发明的又另一实施例中，采用下述补充方法。SGSN 监视接收的与当前在 SGSN 上使用的随机 TLLI（在当前正在进行的匿名附加过程的短的初始部期间）。如果接收到当前已在使用的随机 TLLI，该 SGSN 便以中止报文应答从其接收该随机 TLLI 的单元。这导致接收该中止报文的移动台用新的随机 TLLI 进行新的尝试。

将在基地台 62 上接收的组标识符信号的指示以传统方式提交给 SGSN106（或适当的 MSC/VLR72）。

SGSN106（或适当的 MSC/VLR72）取出三元组。这些三元组为 RAND98、加密密钥 Kc102 及 SRES100 的值。RAND98 的值是以在 IMGI94 所标识的移动台组中独一无二的方式分配的。而如上所述，包括第一网络编码信号的 SRES100 是根据 RAND98 与 Ki96 的值计算的。

一旦取出，SGSN106 便取道基地台 62 将检索到的 RAND98 作为第二网络编码的信号的一部分传输给移动台 12。第二网络编码的信号是通过网络 14 的各元件的操作生成的。控制器 24 还以用来计算 SRES100 与 Kc102 相同的方式的算法计算 SRES 与加密密钥 Kc 的值。可是，这里在移动台 12 上计算的值是根据传输给移动台的 RAND98 的值及存储在存储器元件 38 中的 Ki46 的值计算的。

一旦在移动台上计算出了 SRES 的值，便生成指示该 SRES 的第一移动台编码的信号并将其传输回通信网 14。将这一信号的指示提供给 SGSN106，并将其与前面所述的以前在 AUC84 计算与存储并作为三元组取出的 SRES100 进行比较，即与第一网络编码信号进行比较。

如果移动台计算的 SRES 的值与 SRES100 的值对应，便验证了移动台 12 并向其提供对通信网 14 的接入。此后，必要时利用在移动台 12 上计算的加密密钥与从验证中心取出的加密密钥 102 的取出值加密移动台与通信网之间的另外的通信。

在用 Kc 的加密下，SGSW（从动态存储池）分配给 MS 单个 TLLI 及单个临时 IP 地址，或更一般地，临时网络层身份。

此外，为了方便在网络中与单个 IMSI 用户类似地处理，可分配临时的 IMSI。

以类似于在 GPRS 系统中为单个的其于 IMSI 的用户传统地建立与维护 SGSN 与 GGSN 上下文的方式，为包含移动台 12 在内的移动台建立与维护 SGSN 与 GGSN 上下文。在图 1 中所示的示范性实施例中，SGSN 上下文包含用户数据等，其中包含 IMGI、可选用的目的地的预定义 IP 地址、临时 IP 地址、TLLI、Kc、移动台状态及单元/路由选择区位置。SGSN 与 GGSN 上下文允许定位在通信网 14 所包含的区内的任何位置上的移动台通过通信网传递数据。

此后，便能执行移动台 12 与对应实体 16 之间取道通信网 14 的数据通信。当在移动台 12 上生成要按照通信网 14 所提供的 GPRS 传输的分组数据时，便允许以传统方式按照选择的分组数据协议取道通信网 14 对对应实体 16 的传输。分配临时网络层身份及建立与维护 SGSN 与 GGSN 路由选择上下文允许在移动台 12 与对应实体 16 之间的双向通信。在 IP 协议的情况中，这包含可靠的传输控制协议（TCP）通信。对于道路收费及其它涉及电子支付的应用，可靠的双向通信应是特别有用的。

如果 IMGI 组预约包含一个或多个预定的目的地地址（图 1 中的 IP 地址 48 与 93），在移动台（IP 地址 48）或者在网络（IP 地址 93）之一中，相对于预定义的目的地地址掩护移动台 12 所启动的数据传送。

提供给移动台 12 的接入不需要用对该移动台唯一的永久性标识符验证该移动台。作为替代，根据只将移动台 12 标识为一组移动台的成员的 IMGI44 向移动台 12 提供匿名接入。对于通信网，移动台 12 的实际或永久性身份是不知道的。取决于特定的应用，移动台 12 提供给对应的实体 16 的数据可以向对应的实体 16 唯一地标识移动台 12。然而，这一标识是按照对通信网透明的端对端应用层的。为了安全的目的，也能在这一端对端应用层上执行移动台与对应的实体之间的数据加密。

以类似于在 GPRS 通信网中所允许的方式允许移动台 12 在通信网

14 所包含的整个区域中到处移动，并且通信网 14 的部件可进行操作以类似的方式响应这种移动．类似地，SGSN 内部及 SGSN 之间的单元/路由区更新过程类似于用于更新传统的基于 IMSI 的 GPRS 点对点业务用户的对应过程。

在上述过程中，一旦提供给了移动台 12 接入取道通信网 14 的通信，便能由移动台 12 或对应实体 16 起动数据通信．然而，如果移动台与对应实体之间的以分组交换序列形式的数据通信总是由移动台起动的话，便能简化对通信网要求的移动管理．例如，当分组交换序列结束而移动台 12 返回到备用状态时，例如当活跃状态定时器过时时，可认为移动台 12 对终接在移动台(MT)上的通信为不能接入的．因此，随后的 MT 分组被 SGSN 拒绝．然后在移动台在备用状态中时，不需要路由选择区更新或寻呼．在以后起动新的分组交换序列之前，移动台 12 必须首先执行路由选择区更新．在 SGSN 之间的路由选择区更新的事件中，然后执行重新建立 SGSN 与 GGSN 上下文的正常过程．这一简化的移动管理过程可以是匿名接入业务的固有部分，或者作为替代也可以是预约选择项．

如在上面的过程中所述，既在要求验证移动台 12 为授权取道通信网通信的组的成员的验证要求，又在移动台与通信网之间传递的数据的加密中提供了安全性．在验证过程中，如上所述，利用了属于用 IMGI44 与 94 标识的组的移动台 12 的组公用的单一验证密钥 Ki．并且进一步利用了该组中的各移动台 12 的单独的 RAND98 的值及加密密钥 Kc．例如可以结合路由选择区的更新而更新与之相关的 RANP98 的值与 Kc．这一过程提供与传统 GPRS 通信系统中对抗缺乏对验证密钥 Ki 的值的知识的第三方所利用的相同级别的保护。通过在应用级上提供移动台 12 与对应实体 16 之间的附加端对端加密便能提供例如同一移动台的 IMGI 组的单个成员之间的附加安全保护．

本发明也能采用诸如在 CDPD 系统说明书版本 1.1 中所描述的蜂窝式数字分组数据系统中所使用的其它加密方法．在一个实施例中，网络接收 SRES 之后，即验证之后，替代使用基于 RAND 及 Ki 的加密密钥 Kc，在网络与移动台之间交换一个或多个加密密钥．在另一实施例中，作为匿名附加过程的第一部分在网络与移动台之间交换加密密钥．再者，一旦交换了加密密钥，以后在移动台与网络之间的交换是根据需

要以用这些加密密钥加密的形式的。在后一实施例中，这意味着，随后包含传输 IMGI 与 RAND 的验证过程可以以加密方式执行。

这两个替代加密实施例可在属于同一 IMGI 组的不同移动台之间提供增强的安全性。

图 2 示出一般性地示出在 152 上的交通遥测系统。利用本发明的一个实施例取道通信网 14 将装在车辆 156 上的车载移动台 12 所生成的数据传递给交通控制中心 158。移动台 12 所提供的数据包含诸如这些移动台所在的车辆 156 的有关位置、方向与速度信息。根据这一信息，交通控制中心实现交通控制操作。例如，能使交通控制中心 158 有选择地改变沿道路的交通灯的定序与运转，借此缓解交通堵塞。由于准许移动台 12 并从而这些移动台所在的车辆的用户或所有人的匿名接入，确保了这些车辆的用户或所有人的隐私。

图 3 示出一般性地示出在 172 上的另一交通遥测应用。同样，车载移动台 12 是安装在车辆 156 中的(图中示出了一个这种车载移动台 12 及一辆这种车辆 156)。当装有移动台 12 的车辆 156 通过收费点时，通信网 14 检测到移动台 12 生成的信号。将这一接收的指示提供给收费控制中心 176。移动台 12 所生成的信号的信息内容允许根据智能卡的编码电子地支付费用。取决于支付方法，可在对通信网透明的端对端应用层上有选择地将移动台的永久性身份的指示提供给收费控制中心。借此保持移动台对通信网的匿名性，同时利用上面描述的过程，用诸如上述 IMGI 等组标识符验证该移动台 12。

图 4 示出一般性地示出在 182 上的本发明的实施例的方法。该方法起动在诸如移动台 12 等至少第一通信台与诸如对应实体 16（示出在图 1 中）等对应实体之间在具有用于实现通信的通信网的通信系统中的数据传输。该第一通信台是用组标识的一组通信台中的通信台。该组中的各用组标识的通信台是用组标识符标识的。下面相对于图 1 中所示的示范性实施例描述方法步骤。类似地描述与展示类似实施例。

首先，如用框 184 所示，将 IMGI44 提供给通信网 14。然后，如用框 186 所示，访问网络生成的 SRES100 及 RAND98 的值。这些值是在图 1 的实施例中根据 IMGI94 及 Ki102 的值形成的，并且在本发明的一个实施例中能预先计算、预先存储。

此后，如用框 188 所示，将网络生成的 RAND 发送到移动台 12。在移动台上响应 RAND98 的接收，构成移动台生成的 SRES 值。比较网络与移动台生成的 SRES 值，如用框 194 所示。然后，如用判定框 196 所示，判定这两个值是否基本上相同。如果否，拒绝对通信网的接入，如用框 198 所示。如果这两个值基本上相同，便采取从判定框 196 到框 202 的“是”分支，并接入移动台以便提供取道通信网 14 的通信。此后，如用框 204 所示，适当时传送数据。

在本发明的另一实施例中，类似于上面概述的匿名接入 GPRS 的原理，提供匿名接入传统的电路交换的 GSM（或类似的蜂窝式系统）数据业务。提供的业务是匿名的移动台始发的（MO）数据呼叫业务。在本实施例中，以传统的方式分配给用组标识的移动台一个临时移动台身份（TMSI），而不是 GPRS 例中的 TLLI。在呼叫建立时的验证可根据组用户验证密钥。由于只支持 MO 呼叫，与传统上用于基于 IMSI 的移动台的过程相比，可以简化移动管理过程。从而移动台只须在起动数据呼叫前根据需要定期执行位置更新。

本发明的实施例的操作向诸如移动台 12 等通信台提供匿名接入诸如通信网 14 等通信网，以便在其中传递数据。只在验证授权在网络中传递通信时才提供通信台接入，但接入是不必用对该通信台唯一的永久性标识符向网络单个地标识该通信台来提供的。

上面所描述的是用于实现本发明的最佳实施例，本发明的范围不应受这种描述的限制。本发明的范围是用下面的权利要求书定义的。

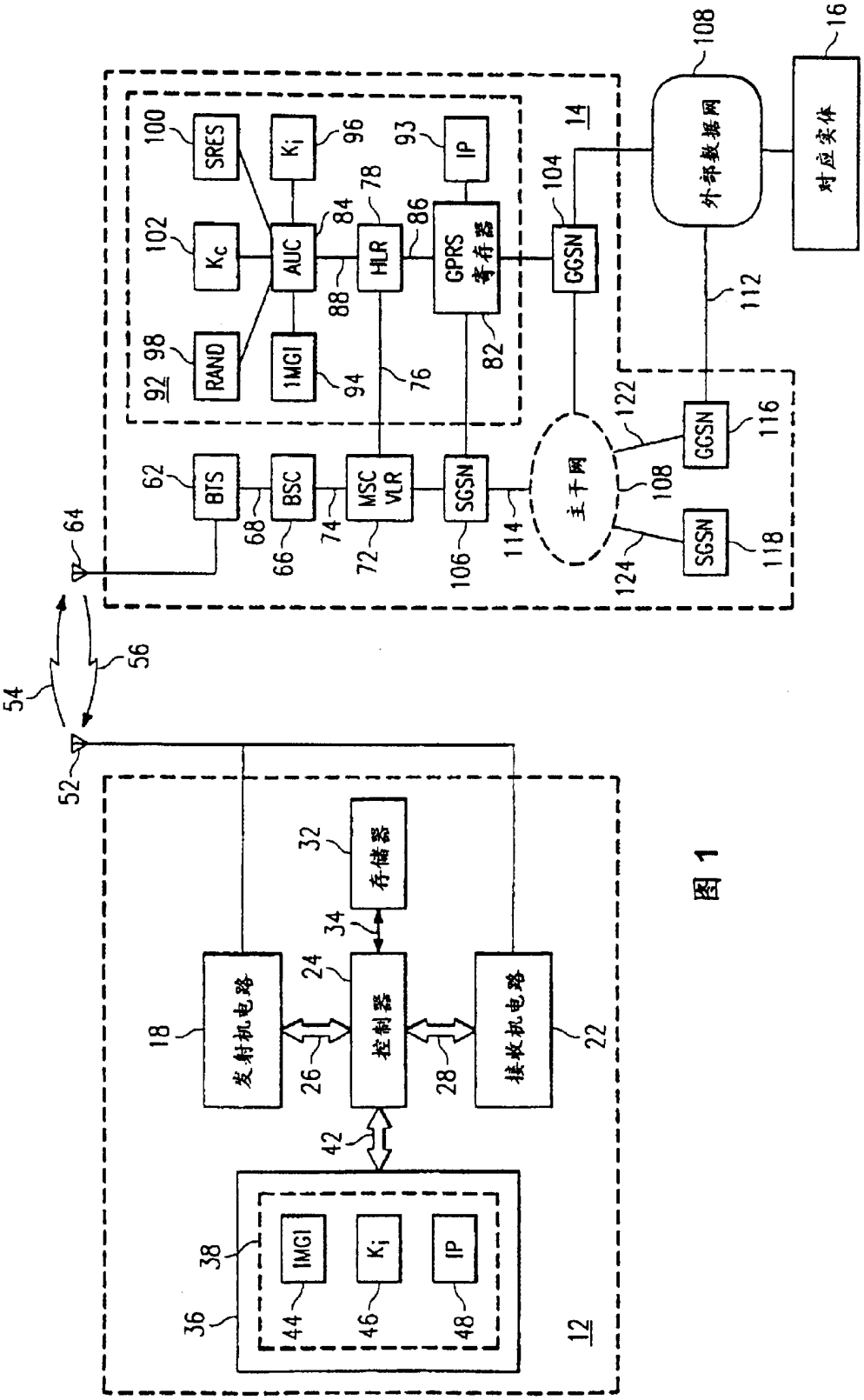

SRES
Ki
IP
Kc
AUC
HLR
GPRS 寄存器
GGSN
外部数据网
对应实体
RAND
IMGI
BTS
BSC
MSC VLR
SGSN
主干网
GGSN
SGSN
存储器
发射机电路
控制器
接收机电路
IMGI
Ki
IP

图 1

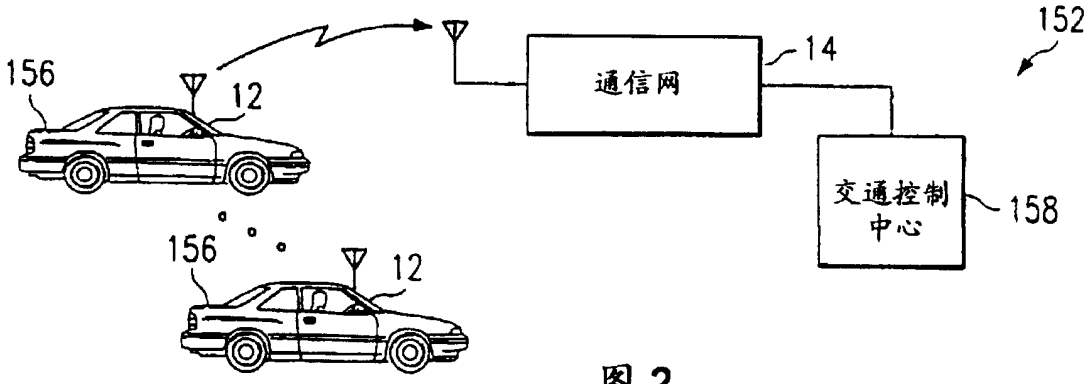

152
156
12
通信网
14
交通控制中心
158
156
12

图 2

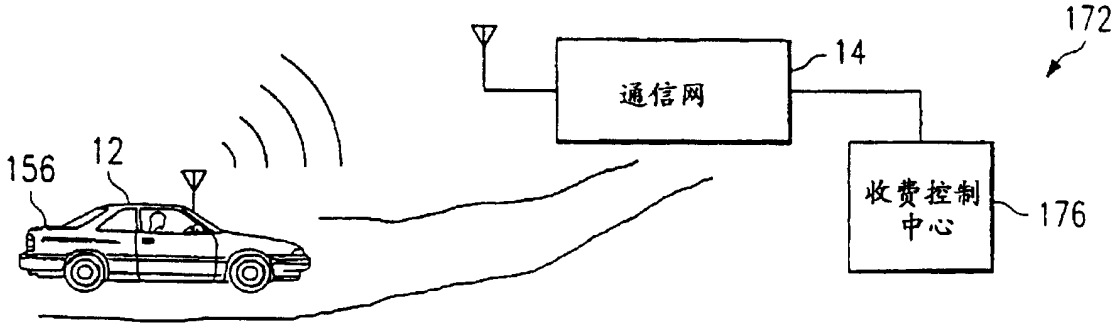

172
通信网
14
156
12
收费控制中心
176

图 3

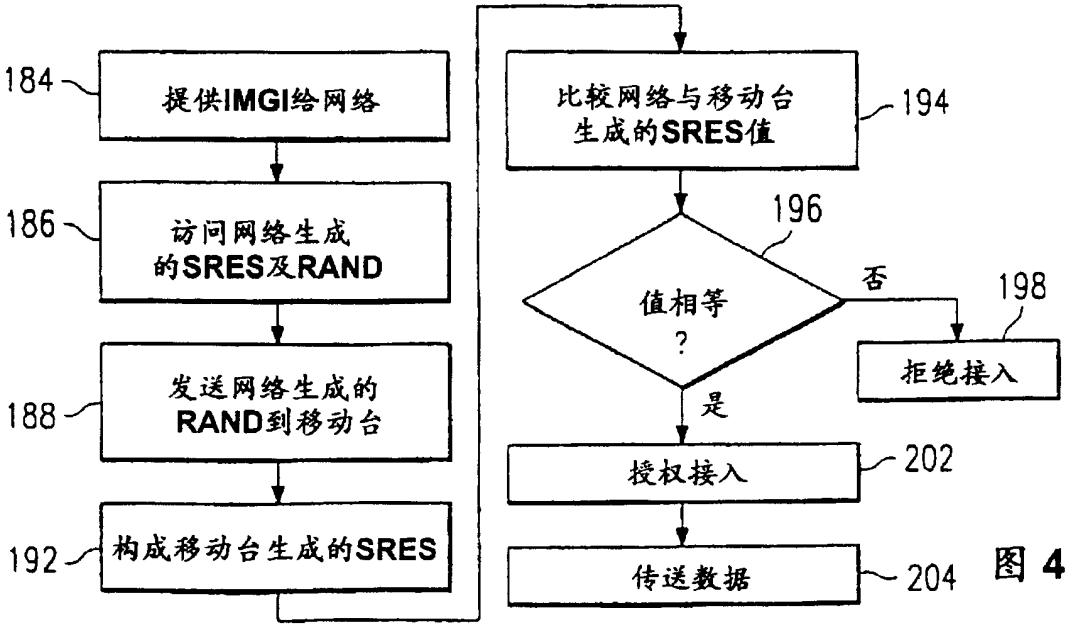

184
提供IMGI给网络
186
访问网络生成的SRES及RAND
188
发送网络生成的RAND到移动台
192
构成移动台生成的SRES
比较网络与移动台生成的SRES值
194
196
值相等?
否
198
拒绝接入
是
授权接入
202
传送数据
204

图 4