



[12] 发明专利申请公开说明书

[21] 申请号 00817232.3

[43] 公开日 2003 年 4 月 16 日

[11] 公开号 CN 1411643A

[22] 申请日 2000.10.27 [21] 申请号 00817232.3
[30] 优先权
[32] 1999.12.15 [33] US [31] 09/464,363
[86] 国际申请 PCT/US00/29595 2000.10.27
[87] 国际公布 WO01/45317 英 2001.6.21
[85] 进入国家阶段日期 2002.6.14
[71] 申请人 艾利森公司
地址 美国北卡罗来纳州
[72] 发明人 D·R·欧文

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 陈 霁

权利要求书 9 页 说明书 15 页 附图 8 页

[54] 发明名称 用于选择性加密和解密点对多点消息的方法和设备

[57] 摘要

提供了方法和系统用于选择性地加密和解密在例如一个广播信道的通信网络的一个信道上传送的消息。为一个或多个使用该广播信道传送消息的服务提供组加密密钥。与一个特定服务相关的消息首先接收到一个错误校验值,例如由该未经加密的消息生成的循环冗余校验(CRC)值。然后使用该服务的组加密密钥对该消息进行加密,以及将该CRC添加到该加密后的消息并用该通信网络的广播地址传送出去。然后一个接收器接收到该消息以及判断该CRC指出了一个错误(因为这是从加密后的消息中生成而不是从未经加密的消息中生成)。然后该接收器使用该服务的组加密密钥对该消息进行解密(假定该接收器被授权接收该服务,即可访问该组加密密钥)并从该解密后的消息中生成一个CRC。如果该CRC与随该消息接收到的CRC匹配,那么该

接收器认为该消息与相应的服务有关并因此处理该消息。这里支持多服务以及该接收器具有相应的多个组加密密钥,可以测试每一个加密密钥直到提供了一个没有错误的CRC从而表明该消息是与之相关的服务。

I S S N 1 0 0 8 - 4 2 7 4

1. 一种选择性加密所传送消息的方法，包括的步骤有：
为一个未经加密的消息确定一个组加密密钥；
为该未经加密的消息生成一个错误校验值；
5 使用该组加密密钥对该未经加密的消息进行加密；以及
在一个通信网络的信道上将该加密后的消息和该错误校验值以一个相关的目的地址传送出去。

2. 按照权利要求 1 的方法，其中该相关的目的地址是该通信网络的一个广播地址以及其中该信道是该通信网络的一个广播信道。

10 3. 按照权利要求 2 的方法，其中为一个消息确定一个组加密密钥的步骤包括确定与该消息有关的服务以及选择与确定的服务有关的一个组加密密钥的步骤。

4. 按照权利要求 2 的方法，其中生成一个错误校验值的步骤包括计算该消息的冗余位的步骤。

15 5. 按照权利要求 4 的方法，其中传送的步骤还包括将加密后的消息与附加到该加密后的消息上的未经加密冗余位一起传送出去。

6. 按照权利要求 4 的方法，其中在确定一个组加密密钥的步骤之前是判断该未经加密的消息是否打算给具有相关组加密密钥的一个广播组的步骤，以及

20 其中如果该未经加密的消息并非打算给具有相关组加密密钥的一个广播组的话，则确定一个组加密密钥，生成一个错误校验值，对未经加密的消息进行加密和传送该加密后的消息的步骤并不执行。

7. 按照权利要求 6 的方法还包括以下步骤：

25 判断该未经加密的消息是否与一般广播或一个单独地址中的至少一个有关；

如果该未经加密的消息与一般广播有关的话，在该通信网络的广播信道上将该未经加密的消息以该通信网络的广播地址传送出去；以及

30 如果该未经加密的消息与一个单独地址有关的话，在通信网络上将该未经加密的消息以单独地址传送出去。

8. 按照权利要求 6 的方法还包括以下步骤：

判断该未经加密的消息是否与一般广播或一个单独地址中至少一

个有关;

如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话, 使用一个一般加密密钥对该未经加密的消息进行加密。

- 5 如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话, 基于该加密的消息生成一个错误校验值; 以及

如果该未经加密的消息与一个单独地址有关的话, 在通信网络上将该加密后的消息和基于该加密的消息的错误校验值以该单独地址传送出去, 以及如果该未经加密的消息与一般广播有关的话, 以该通信网络的广播地址传送。

- 10 9. 按照权利要求 2 的方法还包括以下步骤:

在该通信网络的广播信道上接收该加密后的消息和添加的错误校验值;

判断该接收到的消息是否送往该通信网络的广播地址;

为该接收到的消息生成一个错误校验值;

- 15 判断该错误校验值是否指出了—个错误;

如果该接收到的消息送往该通信网络的广播地址并且该错误校验值指出—个错误的话, 使用该组加密密钥对接收到的消息进行解密;

为该解密后的消息生成一个错误校验值; 以及

- 20 如果该解密后的消息的错误校验值指出没有错误的话, 将该接收到的消息指定给该与组加密密钥有关的一个组。

10. 按照权利要求 9 的方法, 其中为一个未经加密的消息确定一个组加密密钥的步骤包括确定多项服务中与该消息有关的一项, 以及选择多个组加密密钥中的一个作为该未经加密的消息的组加密密钥, 该选定的组加密密钥与该多项服务中该消息相关的、确定的一项服务有关。

- 25 11. 按照权利要求 10 的方法, 还包括的步骤有重复解密, 为解密后的消息生成错误校验值以及将接收到的消息指定给使用多个组加密密钥中选定的一些作为该组加密密钥的一个组的步骤, 直到该解密后的消息的至少一个错误校验值指出没有错误并且多个组加密密钥中选定的一些中的每一个密钥已经被当作组加密密钥使用过。

12. 按照权利要求 11 的方法, 还包括以下步骤:

接收用户对多个组加密密钥中的一个的请求;

将该用户和一个与多个组加密密钥中被请求的一密钥有关的服务相关联；以及

在该通信网络的广播信道上，以该用户的一个相关单独地址向用户传送该多个组加密密钥中被请求的密钥。

5 13. 按照权利要求 3 的方法，还包括以下步骤：

接收用户对组加密密钥的请求；

将该用户和与该组加密密钥有关的一项服务相关联；以及

在该通信网络的广播信道上，以该用户的一个相关单独地址向用户传送该组加密密钥。

10 14. 按照权利要求 13 的方法，其中该组加密密钥具有相关的持续时间以及其中为未经加密的消息确定一个组加密密钥的步骤还包括当先前的组加密密钥已经超过其相关的持续时间时，更新未经加密的消息的组加密密钥。

15 15. 按照权利要求 13 的方法，其中传送该组加密密钥的步骤之后的步骤有：

更新该组加密密钥；以及

使用与组加密密钥相关的服务有关的用户的相关单独地址将更新后的组加密密钥传送到与组加密密钥相关的服务有关的用户。

16. 按照权利要求 13 的方法，还包括以下步骤：

20 接收传送的组加密密钥；

在该通信网络的广播信道上接收加密的消息和添加的错误校验值；

判断接收到的消息是否送往该通信网络的广播地址；

为接收到的消息生成一个错误校验值；

25 判断该错误校验值是否指出了—个错误；

如果接收到的消息送往该通信网络的—个广播地址并且该错误校验值指出—个错误的话，使用该组加密密钥对接收到的消息进行解密；

为解密后的消息生成—个错误校验值；以及

30 如果解密后的消息的错误校验值指出没有错误的话，将接收到的消息指定给与该组加密密钥有关的组。

17. —种选择性解密所传送消息的方法，包括以下步骤：

在一个通信网络的一个信道上接收消息；
判断接收到的消息是否送往该通信网络的一个广播地址；
为接收到的消息生成一个错误校验值；
判断该错误校验值是否指出一个错误；

- 5 如果接收到的消息送往该通信网络的广播地址并且接收到消息的错误校验值指出一个错误的话，使用一个组加密密钥对接收到的消息进行解密；

为解密后的消息生成一个错误校验值；以及

- 10 如果解密后的消息的错误校验值指出没有错误的话，将接收到的消息指定给与该组加密密钥有关的组。

18. 按照权利要求 17 的方法，其中解密接收到的消息的步骤之前的步骤有：

为该组加密密钥传送一个请求；以及

在该通信网络的信道上接收组加密密钥。

- 15 19. 按照权利要求 17 的方法，还包括的步骤有重复解密，为解密后的消息生成错误校验值以及将接收到的消息指定给使用多个组加密密钥中的一些作为组加密密钥的一个组的步骤，直到该解密后的消息的其中至少一个错误校验值指出没有错误并且该多个组加密密钥中的一些中的每一个密钥已经被当作组加密密钥使用过。

- 20 20. 按照权利要求 17 的方法，其中为解密后的消息生成一个错误校验值的步骤包括：

为解密后的消息计算冗余位；以及

将计算的冗余位与接收到的消息中包含的冗余位相比较来判断是否为该解密后的消息指出了一个错误。

- 25 21. 按照权利要求 17 的方法，其中为解密后的消息生成一个错误校验值的步骤包括：

将一个纠错码应用到解密后的消息；以及

如果在将该纠错码应用到解密后的消息之后在解密后的消息中遗留任何错误的话，判定为该解密后的消息指出了一个错误。

- 30 22. 按照权利要求 17 的方法，还包括以下步骤：

判断接收到的消息是否送往接收该消息的一个接收设备的单独地址；以及

如果接收到的消息送往该单独地址的话,使用不同于该组加密密钥的一个一般加密密钥对接收到的消息进行解密。

23. 按照权利要求 22 的方法,还包括步骤有如果接收到的消息送往该通信网络的一个广播地址并且接收到的消息的错误校验值指出没有错误的话,使用该一般加密密钥对接收到的消息进行解密。

24. 一种选择性加密的系统包括:

一个使用一个组加密密钥对一个消息进行加密的加密电路;

基于该未经加密的消息生成一个错误校验值并将该错误校验值添加到该加密后的消息的错误校验值生成电路;

- 10 一个传送器,用于在通信网络的信道上将加密后的消息与添加的错误校验值一起传送出去;以及

一个加密密钥选择电路,基于与该消息有关的一项服务选择多个候选组加密密钥中的一个作为组加密密钥。

25. 按照权利要求 24 的系统,还包括:

- 15 一个接收器,用于接收对该组加密密钥的请求;以及

其中配置该传送器用以响应于接收组加密密钥请求而以请求设备的单独地址传送该组加密密钥;以及

其中该传送器将该加密后的消息以该通信网络的一个广播地址传送出去。

- 20 26. 一种选择性解密的系统,包括:

一个在通信网络的信道上接收消息的接收器;

一个使用组加密密钥解密该消息的解密电路;

一个为接收到的消息和解密后的消息生成一个错误校验值的错误校验值生成电路;

- 25 一个响应错误校验值生成电路的比较电路,用于判断是否为接收到的消息和解密后的消息指出一个错误;以及

一个响应该比较电路的选择电路,选择接收到的消息或解密后的消息中的一个作为要处理的消息。

27. 按照权利要求 26 的系统,还包括:

- 30 一个传送器,用于传送对组加密密钥的请求;以及

其中对该接收器进行配置用以接收该组加密密钥。

28. 一种选择性加密所传送消息的系统,包括:

- 用于为未经加密的消息确定一个组加密密钥的装置；
用于为该未经加密的消息生成一个错误校验值的装置；
用于使用该组加密密钥对未经加密的消息进行加密的装置；
用于将该错误校验值添加到该加密后的消息的装置；以及
- 5 用于在一个通信网络的一个信道上将加密后的消息和添加的错误校验值以相关的目的地址传送出去的装置。

29. 按照权利要求 28 的系统，其中该相关的目的地址是该通信网络的一个广播地址以及其中该信道是该通信网络的一个广播信道。

30. 按照权利要求 29 的系统，其中用于为一个消息确定一个组加密密钥的装置包括用于确定与该消息有关的一个服务以及选择与确定的服务有关的一个组加密密钥的装置。
- 10

31. 按照权利要求 29 的系统，其中用于生成一个错误校验值的装置包括为该消息计算冗余位的装置。

32. 按照权利要求 31 的系统还包括：

- 15 判断该未经加密的消息是否与一般广播或一个单独地址中的至少一个有关的装置；

如果该未经加密的消息与一般广播地址有关的话，在通信网络的广播信道上将该未经加密的消息以该通信网络的广播地址传送出去的装置；以及

- 20 如果该未经加密的消息与一个单独地址有关的话，在通信网络的广播信道上将该未经加密的消息以该单独地址传送出去的装置。

33. 按照权利要求 31 的系统还包括：

判断该未经加密的消息是否与一般广播或一个单独地址中至少一个有关的装置；

- 25 如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话，使用一个一般加密密钥对该未经加密的消息进行加密的装置；

如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话，基于该加密的消息生成一个错误校验值的装置；以及

- 30 如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话，将基于该加密的消息的错误校验值添加到加密后的消息的装置；以及

如果该未经加密的消息与一个单独地址有关的话，在通信网络的广播信道上将该加密后的消息和基于该加密的消息的附加错误校验值以该单独地址传送出去，以及如果该未经加密的消息与一般广播有关的话，以该通信网络的广播地址传送的装置。

5 34. 按照权利要求 30 的系统还包括：

用于接收用户对组加密密钥的请求的装置；

用于将用户和与该组加密密钥有关的服务相关联的装置；以及

用于在该通信网络的广播信道上，以该用户的一个相关单独地址向用户传送该组加密密钥的装置。

10 35. 按照权利要求 34 的系统，其中该组加密密钥具有相关的持续时间以及其中为该未经加密的消息确定一个组加密密钥的装置还包括当先前的组加密密钥已经超过其相关的持续时间时，用于为未经加密的消息更新组加密密钥的装置。

36. 按照权利要求 34 的系统还包括：

15 用于更新该组加密密钥的装置；以及

用于使用与组加密密钥相关的服务有关的用户的相关单独地址，将更新后的组加密密钥传送到与组加密密钥相关的服务有关的用户的装置。

37. 按照权利要求 34 的系统还包括：

20 用于接收传送的组加密密钥的装置；

用于在该通信网络的广播信道上接收加密的消息和添加的错误校验值的装置；

用于判断接收到的消息是否送往该通信网络的广播地址的装置；

用于为接收到的消息生成一个错误校验值的装置；

25 用于判断该错误校验值是否指出了错误的装置；

如果接收到的消息被送往该通信网络的一个广播地址并且该错误校验值指出一个错误的话，用于使用该组加密密钥对接收到的消息进行解密的装置；

用于为解密后的消息生成一个错误校验值的装置；以及

30 如果解密后的消息的错误校验值指出没有错误的话，用于将接收到的消息指定给与该组加密密钥有关的组的装置。

38. 一种选择性解密所传送消息的系统，包括：

- 用于在一个通信网络的一个信道上接收消息的装置；
用于判断接收到的消息是否送往该通信网络的一个广播地址的装置；
用于为接收到的消息生成一个错误校验值的装置；
5 用于判断该错误校验值是否指出一个错误的装置；
如果接收到的消息被送往该通信网络的广播地址并且接收到消息的错误校验值指出一个错误的话，用于使用一个组加密密钥对接收到的消息进行解密的装置。
- 10 用于为解密后的消息生成一个错误校验值的装置；以及
如果解密后的消息的错误校验值指出没有错误的话，用于将接收到的消息指定给与该组加密密钥有关的组的装置。
39. 按照权利要求 38 的系统，还包括：
用于传送对为该组加密密钥的请求的装置；以及
用于在该通信网络的信道上接收组加密密钥的装置。
- 15 40. 按照权利要求 38 的系统，还包括装置用于重复解密，为解密后的消息生成错误校验值以及将接收到的消息指定给使用多个组加密密钥中的一些作为组加密密钥的一个组的步骤，直到该解密后的消息的其中至少一个错误校验值指出没有错误并且该多个组加密密钥的一些中的每一个密钥已经被当作组加密密钥使用过。
- 20 41. 按照权利要求 38 的系统，其中为解密后的消息生成一个错误校验值的装置还包括：
用于为解密后的消息计算冗余位的装置；以及
用于将计算的冗余位与接收到的消息中包含的冗余位相比较来判断是否为该解密后的消息指出了一个错误的装置。
- 25 42. 按照权利要求 38 的系统，其中为解密后的消息生成一个错误校验值的装置还包括：
用于将一个纠错码应用到解密后的消息的装置；以及
用于如果在将一个纠错码应用到解密后的消息之后在解密的消息中遗留任何错误的话，判定为解密后的消息指出一个错误的装置。
- 30 43. 按照权利要求 38 的系统，还包括：
用于判断接收到的消息是否送往接收该消息的一个接收设备的单独地址的装置；以及

如果接收到的消息送往该单独地址的话，用于使用不同于该组加密密钥的一个一般加密密钥对接收到的消息进行解密的装置。

44. 按照权利要求 43 的系统，还包括装置用于如果接收到的消息送往该通信网络的一个广播地址并且接收到的消息的错误校验值指出
5 没有错误的话，使用该一般加密密钥对接收到的消息进行解密。

用于选择性加密和解密点对多点消息的方法和设备

发明背景

- 5 本发明涉及通信方法和设备，更特别地，涉及使用加密的通信方法和设备。

无线通信系统通常被用于向用户提供语音和数据通信。例如，模拟蜂窝无线电话系统，例如那些称为 AMPS, ETACS, NMT-450 和 NMT-900 的系统，长久以来在世界范围被成功应用。数字蜂窝无线电话系统如
10 那些遵照北美标准 IS-54 和欧洲标准 GSM 的系统自 20 世纪 90 年代初期以来便已投入服务。更近地，被广义标记为 PCS（个人通信服务）的广泛种类的无线数字服务已经被引进，包括遵照如 IS-136 和 IS-95 标准的高级数字蜂窝系统，如 DECT（数字增强式无绳电话）这样的低功率系统和如 CDPD（蜂窝数字分组数据）这样的数据通信服务。在 The
15 mobile Communications Handbook（移动通信手册）中对这些和其他的系统进行了描述，该手册由 Gibson 编辑并由 CRC 出版社（1996）出版。

图 1 说明了一种典型的陆地蜂窝无线电话通信系统 20。该蜂窝无线电话系统 20 可能包括一个或多个无线电话（移动终端）22；与多个
20 小区 24 的通信服务由基站 26 和一个移动电话交换局（MTSO）28 来提供。虽然图 1 中只显示了三个小区 24，一个典型的蜂窝网络可能包括上百个小区，可能包括一个以上 MTSO，并可能为成千个无线电话提供服务。

在该通信系统 20 中该小区 24 通常用作节点，从该小区出发经由
25 为该小区 24 服务的基站 26，建立了无线电话 22 和 MTSO28 之间的链路。典型地，每一个小区 24 已分配给它一个或多个专用控制信道和一个或多个业务信道。一个控制信道是一个用于传送小区标识和寻呼信息的专用信道。该业务信道承载了该语音和数据信息。通过该蜂窝网络 20，两个移动终端 22 之间或一个移动终端 22 和一个陆地线路电话
30 用户 32 之间的双工无线通信链路可能通过一个公共交换电话网络 34（PSTN）而实现。基站 26 的功能是处理一个小区 24 和移动终端 22 之间的无线通信。就这个能力而言，基站 26 充当数据和语音信号的中继

站。

正如图 2 所示, 可以使用卫星 42 例如向那些人口分布稀少或地形崎岖的服务区域, 执行与那些由传统的陆地基站执行的相似的功能, 这些地区使传统陆地线路电话或陆地蜂窝电话结构在技术上或经济上不可行。一个卫星无线电话系统 40 典型地包括一个或多个卫星 42, 卫星 42 担任一个或多个地面站 44 和终端 23 之间的中继或转发器。该卫星通过双工链路 46 向终端 23 和一个地面站 44 传送无线电话通信。该地面站 44 可以依次被连接到一个公共交换电话网络 34 上, 允许卫星无线电话之间的通信, 以及卫星无线电话与传统陆地蜂窝无线电话或陆地线路电话之间的通信。该卫星无线电话系统 40 可以使用一个单天线波束覆盖由该系统提供服务的整个区域, 或者, 正如所显示的, 该卫星可以经过设计以致于它生成多个重叠最小的波束 48, 每一波束服务于该系统服务区域的不同地理覆盖区域 50。该覆盖区域 50 提供与图 1 的陆地蜂窝系统 20 中的小区 24 相同的功能。

传统上使用几种不同类型的接入技术, 向例如图 1 和图 2 所示的无线系统的用户提供无线服务。传统的模拟蜂窝系统通常使用一个被称为频分多址 (FDMA) 的系统来创建多个通信信道, 其中离散的频段充当蜂窝终端与蜂窝基站通信的信道。典型地, 这些波段被重新用于地理上分离的小区以增加系统容量。现代数字无线系统典型地使用不同的多址技术例如时分多址 (TDMA) 和码分多址 (CDMA) 来提供提高的频谱效率。在 TDMA 系统中, 例如那些遵照 GSM 或 IS-136 标准的系统中, 载波被划分为顺续的时隙, 这些时隙被指定到多个信道以使多个信道可以被复用到单个载波上。CDMA 系统, 例如那些遵照 IS-95 标准的系统, 通过使用“扩展频谱”技术实现提高信道容量的目的, 其中通过由一个独一无二的扩展码调制一个数据调制的载波信号来定义一个信道, 该扩展码即在通信系统工作的频谱的很宽部分上扩展一个初始数据调制的载波的码。

在例如图 1 和图 2 的无线通信系统中的通信典型地利用不同的寻址模式, 用于将消息通过一个广播控制信道由基站发送出去。消息可能被传送到该通信系统的广播地址, 即, 寻址到由该系统提供服务的所有移动终端 (接收设备或接收器), 或发送到与一个特定移动终端相关的单独地址。当多于一个接收器对一个特定的消息感兴趣时, 广

播（点对多点）地址的使用可以避免过度的网络业务量。由这样的系统支持的接收器优选地被配置了一个广播地址和一个单独地址，因此它们可以访问到这两种类型的消息。这样的系统同样可以使用加密来为控制信道上的通信广播提供更多的保密性，该通信广播可能遭受预定的接收者以外的接收器的窃听。

这样的现有技术系统的一个问题是所有具有正确广播地址的移动终端可以访问具有该广播地址的所有消息广播。因此，方便地使用同一个信道来既发送打算被普遍接收的消息又传送那些打算只被潜在的接收器的子集接收的消息就存在问题。随着这样的通信网络上可得到的服务的扩展，包括引入额外付费服务，例如，股票报价或天气更新，这将更成问题了。服务供应商希望有一种方法为这样的额外付费服务控制记帐以及控制对这样的额外付费服务的访问。

以前被推荐的控制对额外付费服务的访问问题的一种方法是使用组地址。一个组地址可被描述为接收器子集所用的一个广播地址。在这样一个网络中，每一个接收器将具有一个广播地址，一个单独地址和，任选地，一个或多个组地址。然后可以使用与该额外付费服务有关的组地址将额外付费服务传送出去。控制访问额外付费服务的这种方法的缺点在于向组里增加或从中移走接收器引起的负担。它同样将这种负担施加到该地址管理系统上，而不是信道上。预防欺骗的担心可能会阻碍在例如蜂窝电话网络的网络中接收器地址的轻易改变。而且，使用组地址方法可能会遭受偷听，因此使该组地址遭受到那些想不付费就得到额外付费服务的人的窃听或侵犯其他用户的隐私和安全。因此，希望提供方法，使得能在一个安全、私密和其中可以容易地管理列入组或从中去除的广播信道上选择性地分发消息。

发明概述

本发明提供了方法和系统，用于选择性地加密和解密在通信网络的广播信道上传送的消息。为一个或多个使用该广播信道传输消息的服务提供组加密密钥。与一个特定服务相关的消息首先接收到一个错误校验值，例如循环冗余校验（CRC）值，由该未经加密的消息生成。然后使用该服务的组加密密钥对该消息进行加密以及将该CRC添加到该加密后的消息并用该通信网络的广播地址传送出去。然后一个接收

器接收到该消息以及判断该 CRC 指出了—个错误（因为这是从加密后的消息中生成而不是从未经加密的消息中生成）。然后该接收器使用该服务的组加密密钥对该消息进行解密（假定该接收器被授权接收该服务，即，可访问该组加密密钥）并从该解密后的消息中生成一个 CRC。

- 5 如果该 CRC 与随该消息接收到的 CRC 匹配，那么该接收器认为该消息与相应的服务有关并因此处理该消息。这里支持多服务以及该接收器具有相应的多个组加密密钥，可以测试每一个加密密钥直到提供了一个没有错误的 CRC 从而表明该消息是与之相关的服务。

- 10 在本发明的一个实施方案中，提供了一种方法用于选择性的加密所传送的消息。为一个未经加密的消息确定一个组加密密钥以及为该未经加密的消息确定一个错误校验值。使用该组加密密钥对该未经加密的消息进行加密。该加密后的消息和该错误校验值以一个相关的目的地址被在一个通信网络的一个广播信道上传送。优选地，该相关的目的地址是该通信网络的一个广播地址以及选择了一个与生成该消息
- 15 的一项服务有关的组加密密钥。该错误校验值可能是该消息的冗余位，例如 CRC，以及该未经加密的冗余位可能被附加到用于传送的加密后的消息中。

- 可以为接收到的未经加密的消息而非其他消息提供选择性的加密操作，该未经加密的消息打算传送到具有相关组加密密钥的一个广播
- 20 组。如果该未经加密的消息与一般广播有关的话，接收到的与一般广播或单独地址中至少一个相关的未经加密的消息可以以该通信网络的广播地址在该通信网络的广播信道上传送，如果该未经加密的消息与一个单独地址有关的话，则以该单独地址在该通信网络上传送。

- 在本发明的另一个实施方案中，如果该未经加密的消息与一般广
- 25 播或一个单独地址中至少一个有关的话，可以使用一个一般加密密钥对该未经加密的消息进行加密。如果该未经加密的消息与一般广播或一个单独地址中至少一个有关的话，可以基于该经加密的消息生成一个错误校验值。然后如果该未经加密的消息与一个单独地址有关的话，该加密后的消息和基于该经加密的消息的错误校验值可以以该单
- 30 独地址在通信网络上传送，以及如果该未经加密的消息与一般广播有关的话，以该通信网络的广播地址传送。

在本发明的另一个实施方案中，在该通信网络的广播信道上接收

到该加密后的消息和添加的错误校验值。该接收设备判断该接收到的消息是否被导向该通信网络的广播地址。为该接收到的消息生成一个错误校验值以及测试该值来判断该错误校验值是否指出了一个错误。如果该接收到的消息被导向该通信网络的广播地址以及该错误校验值指出一个错误的话，使用该组加密密钥对接收到的消息进行解密。为该解密后的消息生成一个错误校验值。如果该解密后的消息的错误校验值指出没有错误的话，将接收到的消息指定给与该组加密密钥有关的一个组。可以基于与该消息有关的多项服务中的一项确定该组加密密钥以及选择多个组加密密钥中的一个作为该未经加密的消息的组加密密钥，所述选定的组加密密钥与确定的、与该消息有关的多项服务中的一项服务有关。使用选定的多个组加密密钥中的一些作为组加密密钥来重复进行解密和错误校验操作，直到该解密后的消息的错误校验值指出没有错误或者选定的多个组加密密钥中一些密钥中的每一个已经被当作组加密密钥使用过。

在本发明的另一个实施方案中，从用户接收到对多个组加密密钥中的一个密钥的请求。该用户与多个组加密密钥中的一个请求的密钥相关的服务有关以及该多个组加密密钥中被请求的一个以该用户的一个相关单独地址在该通信网络的广播信道上被传送到该用户。该组加密密钥可能有相关的持续时间以及当先前的组加密密钥已经超过其相关的持续时间时，该组加密密钥可被更新。该组加密密钥同样可能基于周期的原理被更新以及更新后的加密密钥可以通过使用与组加密密钥有关的服务相关的用户的相关单独地址，被传送到与组加密密钥有关的服务相关的用户。

在本发明的另一个实施方案中，在该通信网络的广播信道上接收到传送的组加密密钥和加密的消息以及添加的错误校验值，以及该接收设备判断接收到的消息是否被导向该通信网络的广播地址。为接收到的消息生成一个错误校验值用以判断该错误校验值是否指出了一个错误。如果接收到的消息被送往该通信网络的广播地址并且该错误校验值指出一个错误的话，使用组加密密钥对接收到的消息进行解密。为解密后的消息生成一个错误校验值，以及如果解密后的消息的错误校验值指出没有错误的话，将接收到的消息指定给与该组加密密钥有关的组。

在本发明的另一个实施方案中，提供一种选择性解密所传送消息的方法，包括在通信网络的广播信道上接收一个消息并判断接收到的消息是否送往该通信网络的广播地址。为接收到的消息生成一个错误校验值用以判断该错误校验值是否指出错误。如果接收到的消息被送往该通信网络的广播地址并且该接收到消息的错误校验值指出一个错误的

5 的话，使用一个组加密密钥对接收到的消息进行解密。为解密后的消息生成一个错误校验值，以及如果解密后的消息的错误校验值指出没有错误的话，将接收到的消息指定给与该组加密密钥有关的组。可以为多个候选组加密密钥中的每一个密钥重复进行解密和错误校验操作，直到该解密后的消息的错误校验值指出没有错误或者该多个组加密密钥中的每一个已经被当作组加密密钥使用过。该解密后消息的错误校验值可以被当作解密后的消息的冗余位计算或通过将一个纠错码应用到解密后的消息计算，以及如果在将该纠错码应用到解密后的消息之后在解密后的消息中遗留任何错误的话，判定为解密后的消息指出一个错误。

10 15

在本发明的另一个方面，提供了一个选择性的加密系统，包括一个使用组加密密钥加密消息的加密电路和基于未经加密的消息生成一个错误校验值并将该错误校验值添加到加密后的消息的错误校验值生成电路。一个传送器将加密后的消息与添加的错误校验值一起广播到

20 通信网络的广播信道上以及加密密钥选择电路基于与该消息有关的服务选择多个候选组加密密钥中的一个作为组加密密钥。在一个实施方案中，提供一个请求组加密密钥的接收器以及配置该传送器用以响应于接收对组加密密钥的请求而以请求设备的单独地址传送该组加密密钥。

25 本发明的另一个方面，提供了一个选择性的解密系统，包括在通信网络的广播信道上接收消息的接收器和使用组加密密钥解密该消息的解密电路。错误校验值生成电路为接收到的消息和解密后的消息生成一个错误校验值。响应错误校验值生成电路的比较电路判断是否为接收到的消息和解密后的消息指出错误以及响应该比较电路的选择电路选择接收到的消息或解密后的消息中的一个作为将要处理的消息。

30

附图简述

图 1 是说明传统陆地蜂窝通信系统的示意图。

图 2 是说明传统基于卫星的无线通信系统的示意图。

图 3 是依据本发明的一个方面说明一个基站的示意图。

图 4 是依据本发明的一个方面说明一个移动终端的示意图。

5 图 5 是依据本发明的一个实施方案说明用于传送消息的示范性操作的流程图。

图 6 是依据本发明的另一个实施方案说明用于传送消息的示范性操作的流程图。

10 图 7 是依据本发明的另一个实施方案说明用于接收消息的示范性操作的流程图。

图 8 是依据本发明的另一个方面说明组地址管理的流程图。

详述

15 现在本发明将在下文中参照附图进行更充分地描述，附图中说明的是本发明的优选实施方案。不过，本发明可以用多种不同的形式来实现以及不应被认为局限于这里提出的实施方案，更确切地说，提供这些实施方案以便于这个公开内容将详尽而完整，以及充分地将本发明的范围传达给本领域的技术人员。在图中，相同的数字涉及的是相同的要素。

20 现在本发明将参照图 3 的示意框图进一步进行描述。图 3 说明了依据本发明的一个基站或其他选择性加密系统 200 的实施方案。该基站 200 包括一个收发器 205，用于在一个控制器 215 的控制之下通过一个天线 210 传送和接收 RF 通信信号。该控制器从例如移动交换中心（MSC）的外部信源接收消息，以及处理该消息以产生物理层脉冲串，
25 后者由收发器 205 通过天线 210 在物理信道上传送。基站 200 还包括一个使用组加密密钥加密一个消息的加密电路 220 和一个基于未经加密的消息生成一个错误校验值以及将该错误校验值添加到加密后的消息的错误校验值生成电路 230。加密密钥选择电路 240 基于与所要传送的消息有关的服务选择多个候选组加密密钥中的一个作为该组加密密
30 钥。寻址电路 250 判断该消息是否送往一个单独地址，用于一般广播或用于广播到与具有相应组加密密钥的服务有关的接收设备的有限组。该收发器 205 在该通信网络的广播信道上将该加密后的消息与添

加的错误校验值一起广播。该收发器 205 还可以从接收设备接收到组加密密钥的请求并将该组加密密钥以请求接收设备的单独地址传送。该加密电路 220, 错误校验值生成电路 230, 加密密钥选择电路 240 和寻址电路 250 可以作为控制器 215 上运行的代码来实现。

5 现在讨论图 4, 现在将进一步描述依据本发明的一个实施方案的一个移动终端(接收设备) 300 或其他选择性解密系统的实施方案。该移动终端 300 包括一个在控制器 315 的控制之下通过一个天线 310 传送和接收 RF 通信信号的收发器 305。该控制器 315, 例如微处理器, 微控制器或相似的处理设备, 可以执行移动终端 300 的存储器 380 中存储的程序指令, 例如动态随机存取存储器(DRAM), 电可擦除可编程只读存储器(EEPROM)或其他存储设备。该控制器 315 与移动终端 300 的用户接口组件例如显示器 360, 键盘 365, 扬声器 370, 和话筒 375 可操作地相关, 对本领域的技术人员而言, 其操作是众所周知的, 这里就不再作进一步的讨论。

15 移动终端 300 包括一个使用组加密密钥对接收到的消息进行解密的解密电路 320。可以由收发器 305 在一个通信网络的广播信道上接收该消息。移动终端 300 还包括为接收到的消息和由解密电路 320 生成的消息的解密版本生成一个错误校验值的错误校验值生成电路 330。一个比较电路 335 通过比较该错误校验值生成电路的输出与来自接收到的消息的接收到的错误校验值位来判断是否为接收到的消息或解密的消息指出了—个错误。选择电路 340 选择接收到的消息或解密后的消息中的一个作为响应比较电路 335 而处理的一个消息。选择操作将参照这里的流程图进行进一步的描述。收发器 305 还可能被配置以从例如参照图 3 描述的基站 200 这样的选择性加密设备中传送对组加密密钥的请求以及接收该组加密密钥。

25 应该理解, 图 3 和 4 中的模块说明的各种组件, 虽然被说明为独立的集成电路, 但可能使用各种硬件和软件来实现。例如, 收发器 205, 305 的一部分可以通过使用特定用途的硬件来实现, 例如一个特定用途集成电路(ASIC)和可编程逻辑器件例如门阵列, 和/或运行在计算设备例如微处理器, 微控制器或数字信号处理器(DSP)上的软件或固件。

30 同样应该理解, 虽然收发器 205, 305 的功能可能被集成到单个设备上, 例如单个 ASIC, 它们也可以被分布在多个设备之中。各种组件的功能,

例如寻址电路 250, 350, 加密电路 220, 解密电路 320, 错误校验值生成电路 230, 330, 比较电路 335 和加密密钥选择电路 240, 可以作为图 3 和 4 所示控制器 215, 315 上执行的代码来实现或也可以被结合在一个或多个设备中, 例如 ASIC 或 DSP。

- 5 尽管在上文中已经参照消息的加密和传送对基站 200 进行了一般的描述以及参照消息的解密和接收对移动终端 300 进行了一般的描述, 对应于点对多点通信, 需要理解的是本发明并不是局限于那样。基站 200 可以操作用来接收和解密例如, 与使用两路通信的服务有关的消息以及移动终端 300 也可以操作用来加密和传送消息。进一步可以理解的
- 10 组加密密钥的使用不必被用作从移动终端 300 到基站 200 的点对点 (而不是点对多点) 传送, 这是因为基站 200 可以使用移动终端 300 的单独地址来控制对服务的访问。

现在将参照图 5-8 对本发明进行进一步的描述。图 5-8 是流程图, 依据本发明的各方面说明用于选择性加密和解密打算给组的消息的示范性操作。应当理解的是图 5-8 的流程图中的模块, 以及流程图中模块的组合, 可以使用例如图 3 中的基站 200 和图 4 中的移动终端 300 这样的基站和无线终端中包括的电子电路来实现。同样可以理解的是图 5-8 的流程图

15 的模块, 以及流程图中模块的组合, 可以使用不同于图 3 和 4 所说明的那些组件来实现, 以及, 一般地, 图 5-8 的流程图

20 的模块, 以及流程图中模块的组合, 可以在特定用途的硬件如离散模拟和/或数字电路中实现, 例如集成电路组合或一个或多个特定用途集成电路 (ASIC), 以及通过装载在计算机或其他可编程数据处理设备中的计算机程序指令来产生一个机器, 因此在计算机或其他可编程数据处理设备上执行的指令为实现流程图模块中规定的功能而创建装置。

25 该计算机程序指令也可以被装载到一台计算机中或其他可编程数据处理设备中以引起一系列在计算机中或其他可编程设备上执行的操作步骤来产生一段计算机实现的进程, 因此在计算机中或其他可编程设备上执行的指令提供了实现流程图模块中规定的功能的步骤。

因此, 图 5-8 的流程图中的模块支持执行规定功能的电子电路和其他装置, 以及执行规定功能的步骤组合。应当理解的是图 5-8 的

30 流程图的每一个模块支持的电路和其他装置, 以及那里模块的组合, 可以通过专用硬件、在特定或一般用途数据处理器上操作的软件或固

件，或其组合来实现。

现在讨论图 5，当基站 200 接收到用于传送的消息时，在模块 500 中操作开始。该消息可能与一个特定的服务有关，例如额外付费服务，该服务正启动消息的传送。该消息也可能是一个送往特定单独接收站的消息或是打算向一个通信网络的广播地址进行一般分发。基站 200 判断接收到的消息是否是打算给一个单独的特定接收器地址（模块 505），如果是，选择希望的单独地址，以使用要传送的消息包含（模块 510）。

如果该消息不是打算传送到单独地址特定设备，基站 200 判断该消息是不是打算一般广播（模块 515），如果是，选择通信网络的广播地址用于与消息一起传送（模块 540）。如果该接收的消息既不是打算给单独地址接收器也不是打算一般广播，就处理消息以便作为现在将描述的组地址消息传送。优选地通过判断与消息有关的服务和选择多个候选组加密密钥中与确定的服务有关的一个作为组加密密钥（模块 520），来确定接收到的消息的组加密密钥。需要理解的是，如这里所使用的，称作未经加密的消息的、从模块 500 接收到的消息被只送往由基站设备 200 提供的加密。进一步需要理解的是该消息可能实际上以加密的形式提供给基站 200，这里由相关服务的供应商提供加密以及为预订相关服务的接收设备提供一个装置来解密这个服务供应商的加密，该加密是通过超出本发明范围之外的装置进行。因此，这种在与本发明无关的在服务供应商级别收到的加密保护的消息将被认为是未经加密的消息，正如在这里被使用的那个术语。

为接收到的消息（未经加密的消息）生成一个错误校验值（模块 525）。在一个实施方案中，冗余位，例如循环冗余校验（CRC），在模块 525 中计算用于未经加密接收到的消息。不过，需要理解的是依据本发明的各种实施方案，其他类型的检错码和进一步的纠错码可能会被用来生成错误校验值。

然后使用选定的组加密密钥对该未经加密接收到的消息进行加密（模块 530）。优选地，该消息不包括所计算的错误校验值符号（或位）和该广播地址，它依据该组加密密钥被加密。然后添加该错误校验值，例如，通过在传送之前将其附加到加密后的消息（模块 535）。然后将该通信网络的广播地址作为相关的目的地址添加（模块 540）以及加密

行类似于前面参照图 5 中模块 520 到 540 中的操作。因此，这里不再对这些模块中的操作进行进一步的描述。

现在将进一步参照图 7 从接收设备提供选择性解密的角度描述依据本发明的一个实施方案的操作。当一个移动终端（接收设备）300 在通信网络上接收到来自基站 200 的一个消息，在模块 700 中操作开始。然后该寻址电路 350 判断接收到的消息是否包括了移动终端 300 的单独地址（模块 705）。如果是，由错误校验值生成电路 330 生成一个错误校验值（模块 710）并由比较电路 335 将该值与接收到的消息中包含的错误校验值相比较（模块 715）。如果该错误校验值测试失败（模块 715），接收到的消息被假定包含了传输错误并被丢弃（模块 720）。如果该错误校验值测试通过（模块 715），则使用一个一般加密密钥解密该接收到的消息（模块 720）。请注意，对于图 7 所示的实施方案而言，或者使用一个一般密钥或者是例如，参照前面的图 6 所描述的一个组密钥对接收到的消息进行加密。然后进一步由接收移动终端 300 将该消息作为适合于接收到的消息的类型处理（模块 730）。

如果模块 700 中在通信网络的广播信道上接收到的消息没有携带一个单独地址的话（模块 705），移动终端 300 判断其是否携带了一个广播地址（模块 735）。如果该消息既不是送往该移动终端 300 的单独地址也不是一个广播地址，它会被丢弃（模块 720）。如果该消息与一个广播地址有关，操作转移到模块 740，为接收到的消息生成一个错误校验值，例如 CRC 值。如果生成的错误校验值指出没有错误的话（模块 745），使用一般加密密钥对该消息进行解密（模块 720）。

注意，对于组加密密钥加密的消息而言，基于类似前面参照图 5 和 6 所描述的未经加密的消息来生成 CRC。相反，正如参照图 6 所描述的，对于一般广播消息而言，基于加密后的消息生成该 CRC。因此，正如由模块 745 中的判决所说明的，这里当 CRC 在消息解密之前生成时，该 CRC 显示没有错误，希望该消息对应的是一般广播消息而不是选择性的组加密后的消息。不过，当 CRC 在解密指出一个故障之前检验接收到的消息时（模块 745），将接收到的消息作为一个选择性组加密后的消息进行处理。

使用组加密密钥对该消息进行解密（模块 750）。然后从该解密后的消息中生成一个错误校验值（模块 755）。如果模块 755 中生成的

后的消息和添加的错误校验值在该通信网络的一个广播信道上以相关的目的地址传送出去，优选地该地址是该通信网络的广播地址（模块545）。

5 进一步需要理解的是，正如这里所用到的，该通信网络的一个广播地址可能是由一个特定的通信网络所使用的多个广播地址中选定的一个。更一般地，这里的广播地址涉及与点对多点传送有关的一个地址，这里特定的服务可能希望传送到包含在广播地址组内的设备的子集。类似地，正如这里所用到的，术语“广播信道”指的是点对多点通信信道以及并不打算局限于在特定通信协议的语境下使用术语广播
10 信道所定义的任何特定信道，所述协议是例如为蜂窝无线电话所确定的那些协议。这样的协议可能包括多个点对多点信道，其中的一个或多个被称为广播控制信道，其中的另一些可以与不同的名字联系在一起，但是所有的信道依然是和这里所用那个术语一样的广播信道。而且，它并不局限于通过空中类型信道，其中多点接收器中的每一个基本上同时接收到信号，而是也包括其他类型的网络信道例如环类型计
15 算机网络上的通信连接，其中通过分组转发来实现广播信道，这里多点接收器中的第一个接收到一个广播地址，读取分组并将分组转发到计算机网络中的下一个多点接收器。

现在讨论图6，将描述依据本发明的选择性加密系统操作的另一个
20 实施方案。随着在基站200接收到要传送的消息，在模块600处操作开始。基站200判断未经加密接收到的消息是否与一般广播，单独地址或与到定义该广播地址子集的一组接收器的传送有关（模块605）。如果该未经加密接收到的消息与一般广播有关或与一个单独地址有关的话，在模块610处继续使用一个一般加密密钥对未经加密接收到的消息进行加密的操作。基于加密后的消息生成错误校验值（模块615）。
25 然后将基于加密后的消息的错误校验值添加到加密后的消息，优选地将其附加到加密后的消息（模块620）。如果该消息是打算为一般广播所用（模块625）则使通信网络的广播地址用于消息传送（模块655）。如果一个单独地址与一个消息有关，选择该单独地址与该消息一起传
30 送（模块630）。然后该消息以该相关的地址传送（模块660）。该加密后的消息随同基于加密后的消息生成的附加错误校验值一起传送。

对于打算给选定的广播组的消息，模块635到655中的操作的进

CRC 值对应于接收到的消息中所包含的 CRC 值（模块 758），指出没有错误，操作转移到模块 760 以及将接收到的消息指定给与模块 750 中使用的组加密密钥有关的服务组来生成一个成功的错误校验值。如果模块 755 中为解密后的消息生成的错误校验值指出一个错误以及所有

5 候选组加密密钥都已经经过测试的话（模块 765），则拒绝该消息（模块 775）。否则，选择候选组加密密钥中的下一个密钥（模块 770）以及操作返回到模块 750。为候选组加密密钥中的每一个持续进行该操作直到或者是解密后的消息的错误校验值指出没有错误或者是候选组加密密钥中的每一个都已经被测试过为止。

10 因此，本发明允许属于第一额外付费服务的消息与第一组加密密钥相关联以及属于第二额外付费服务的消息与第二组加密密钥相关联等等。实际上，特定服务组可以由其与特定组加密密钥的关联来标识，这与使用传送消息分组头所包含的组地址的现有技术方法相反。而且，可以为一般广播消息，单独地址消息和组加密后的消息提供加密，

15 同时，依然允许接收设备中迅速的接收和解密所有这样的消息。特别地，在加密之前为选择性组加密消息生成错误校验值以及在加密之后为一般广播和单独地址消息生成错误校验值，使得对消息类型的检测和参照图 7 描述的合适解密密钥的使用更为方便。

虽然一个一般的加密密钥已经被描述供一般广播和单独地址消息

20 使用，单独地址也可以被提供给与每一个地址有关的特定加密密钥。进一步需要理解的是，由于接收中的错误或是因为消息属于与接收器没有关联或接收器没有预订的额外付费服务组，消息可以被拒绝（模块 775）。而且，参照一个错误校验码例如 CRC 进行一般描述时，模块 710，740 和 755 中校验该错误校验值的操作，也可以使用其他检错码

25 或纠错码来提供。例如，在纠错码这种情况下，可以允许该纠错码来纠正其能力内的任何数目的传送错误，例如，在模块 755 的情况中对消息解密之后。一个成功的错误校验的检测接着可以对于由纠错码纠正后的消息版本进行。如果错误的数目在纠错码纠正错误的的能力内，该错误被纠正以及该错误校验值被认为已经通过了（例如模块 758 中的操作将转移到模块 760）。否则该错误校验值测试被认为已经指出了

30 一个错误。

现在将参照图 8 所示的实施方案描述涉及向移动终端设备 300 提

供组加密密钥的本发明的另一个方面。当预订与组加密密钥有关的额外付费服务的移动终端 300 向基站 200 发出对相关组加密密钥的请求时，在模块 800 中操作开始。然后基站 200 接收到对额外付费服务的、多个组加密密钥中相关的一个的请求（模块 805）。然后该发出请求的移动终端与该额外付费服务发生关联，该额外付费服务与多个组加密密钥中请求的那一个密钥有关（模块 810）。模块 810 中的操作可能包括对于请求组加密密钥的特别标识的用户得到付款授权或确认提供请求的相关额外付费服务的可用性。换句话说，模块 810 中将用户（移动终端）与一个特定服务相关联的操作，优选地是为得到授权做好一些准备和/或为发出请求用户提供对这样的服务的访问而付款。然后优选地，在通信网络的广播信道上以发出请求用户设备的相关单独地址将请求的组加密密钥传送到发出请求的用户设备（模块 815）。然后由发出请求的设备接收该组加密密钥（模块 820）。

对于图 8 说明的实施方案而言，该组加密密钥可能会周期性地发生变化，每一个得到授权的接收设备被通知该变化，优选地通过前面所描述的它们的单独地址。模块 825 中，如果前面使用的一个组加密密钥要求更新（例如，如果该密钥有相关的持续时间并已经超过了它的相关的持续时间），该组加密密钥被更新（模块 830）并且操作返回到模块 815 用于向得到授权的用户传送更新过的组加密密钥。在各种实施方案中，对于长时间持续的组，组加密密钥可以基于周期地变化，同时每一个接收器会被通知这种变化。可替换地，组加密密钥可能是按需求指定的以及只持续较短的一段时间，例如，为使用例如个人数字助理的设备作为一个移动终端 300 的离家旅行的投资者进行一天的股票价格值的监视。

虽然这里已经对选择性加密设备进行了一般描述并在此指基站 200，需要理解的是涉及选择性加密的能力不必在基站提供。例如，与一个通信网络有关的服务器设备或移动交换中心可以处理消息并为选择性加密及合适寻址和生成错误校验值作准备以及基站 200 可以简单地担当转发器用于在该通信网络的广播信道上传送消息。依据本发明的设备和操作也可以划分到多个设备，包括在基站执行一部分和在通信网络可以得到的移动交换中心或服务器设备上执行其他部分。而且，虽然参照无线网络进行了一般描述，需要理解的是本发明可

以适用于各种类型的网络，包括有线局域网（LAN），广域网（WAN）和城域网（MAN）并且并不局限于无线或蜂窝网络。

在附图和说明中，已经公开了本发明典型的优选实施方案以及，虽然使用了特定术语，但它们只是就一般的和描述的意义来使用，以及并非出于限制的目的，本发明的范围将在下面的权利要求书中提出。

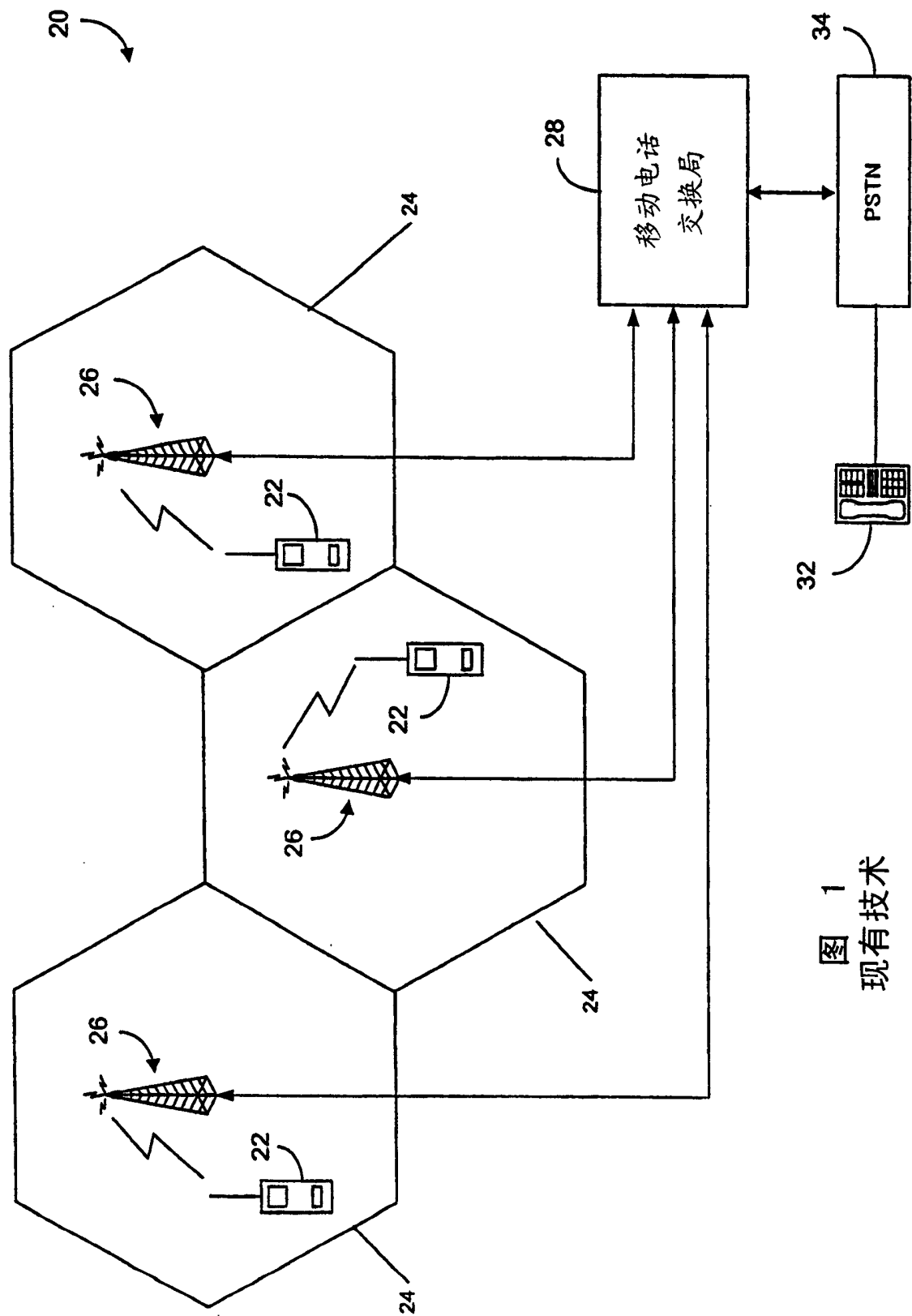


图 1
现有技术

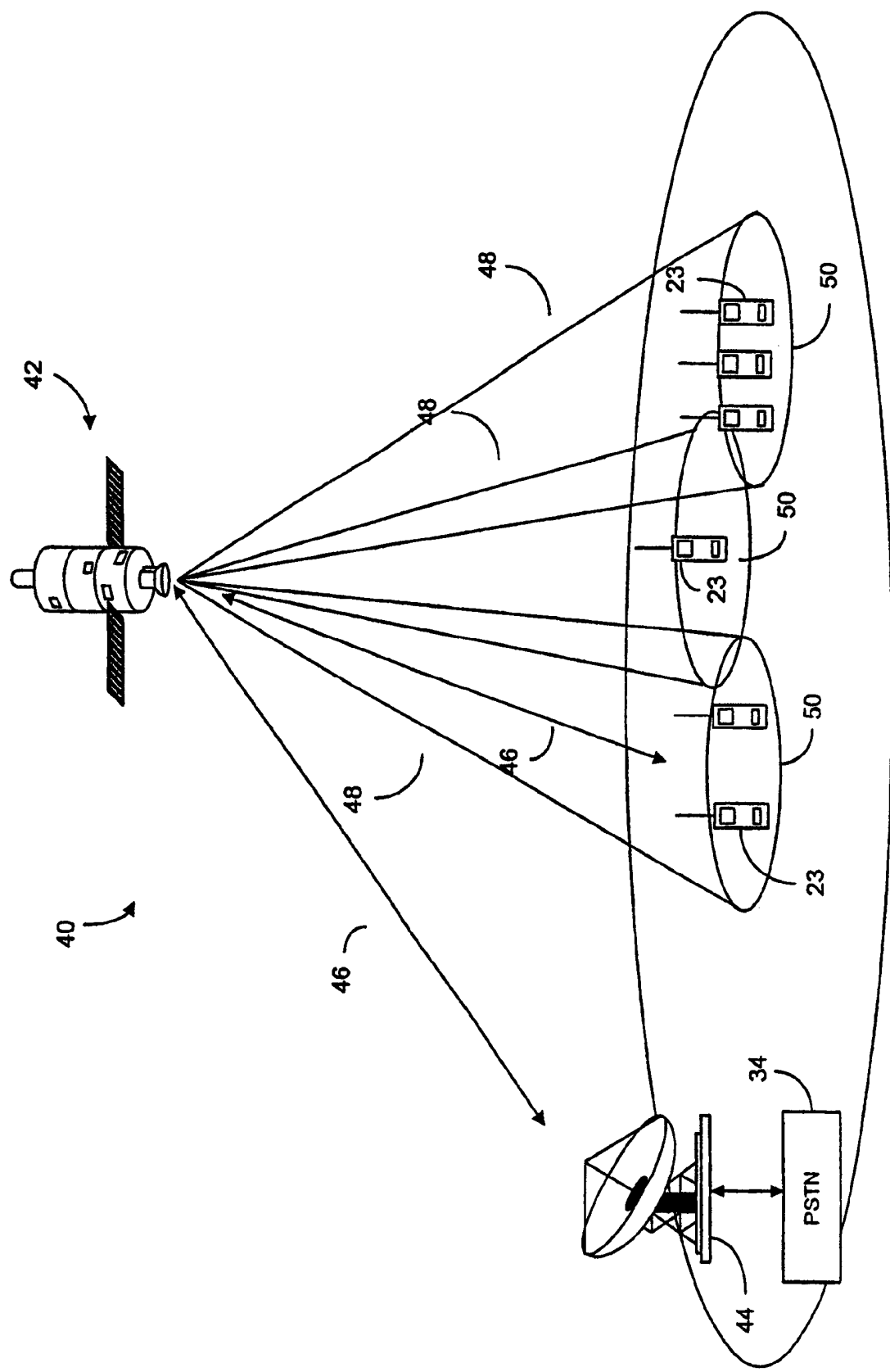


图 2
现有技术

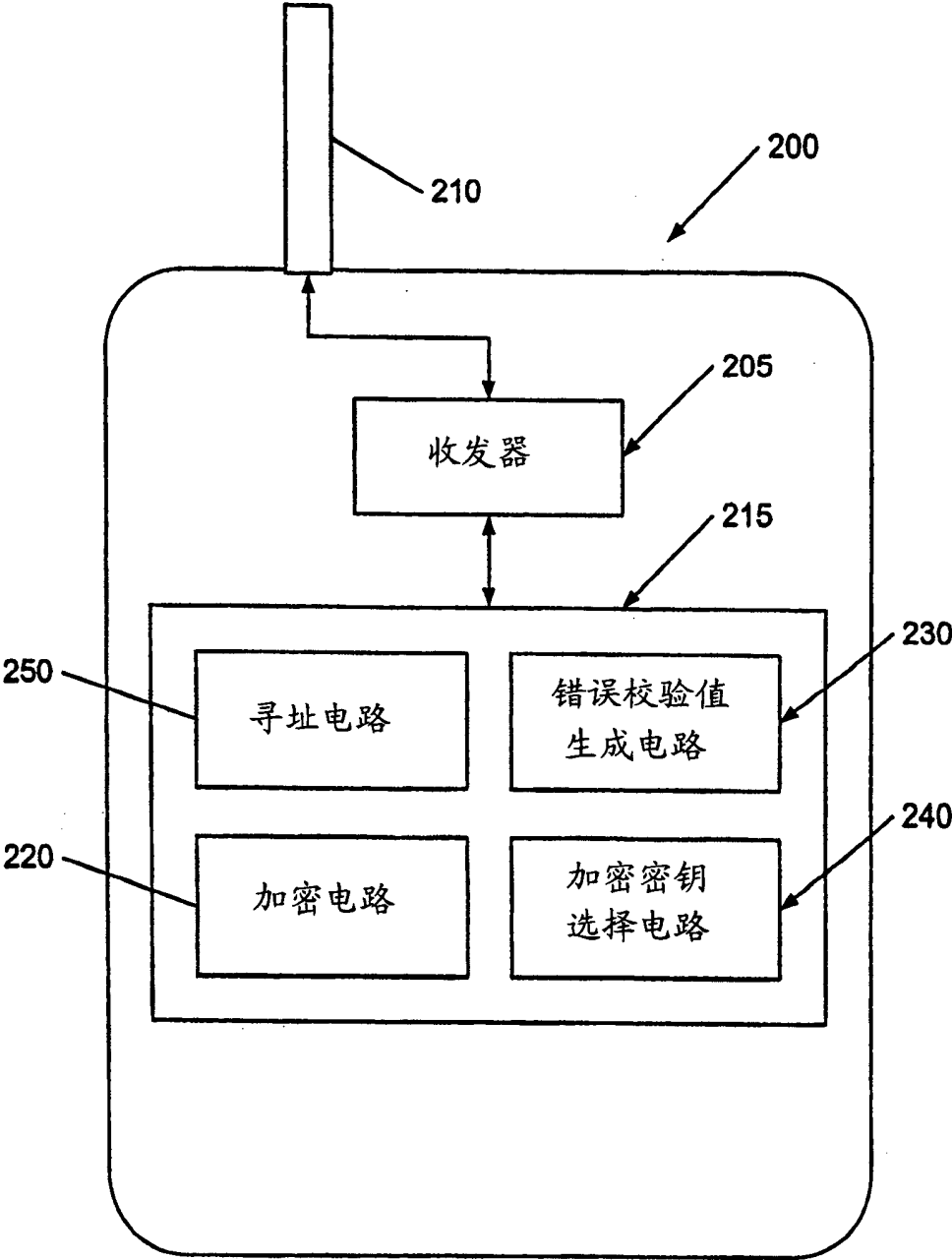


图 3

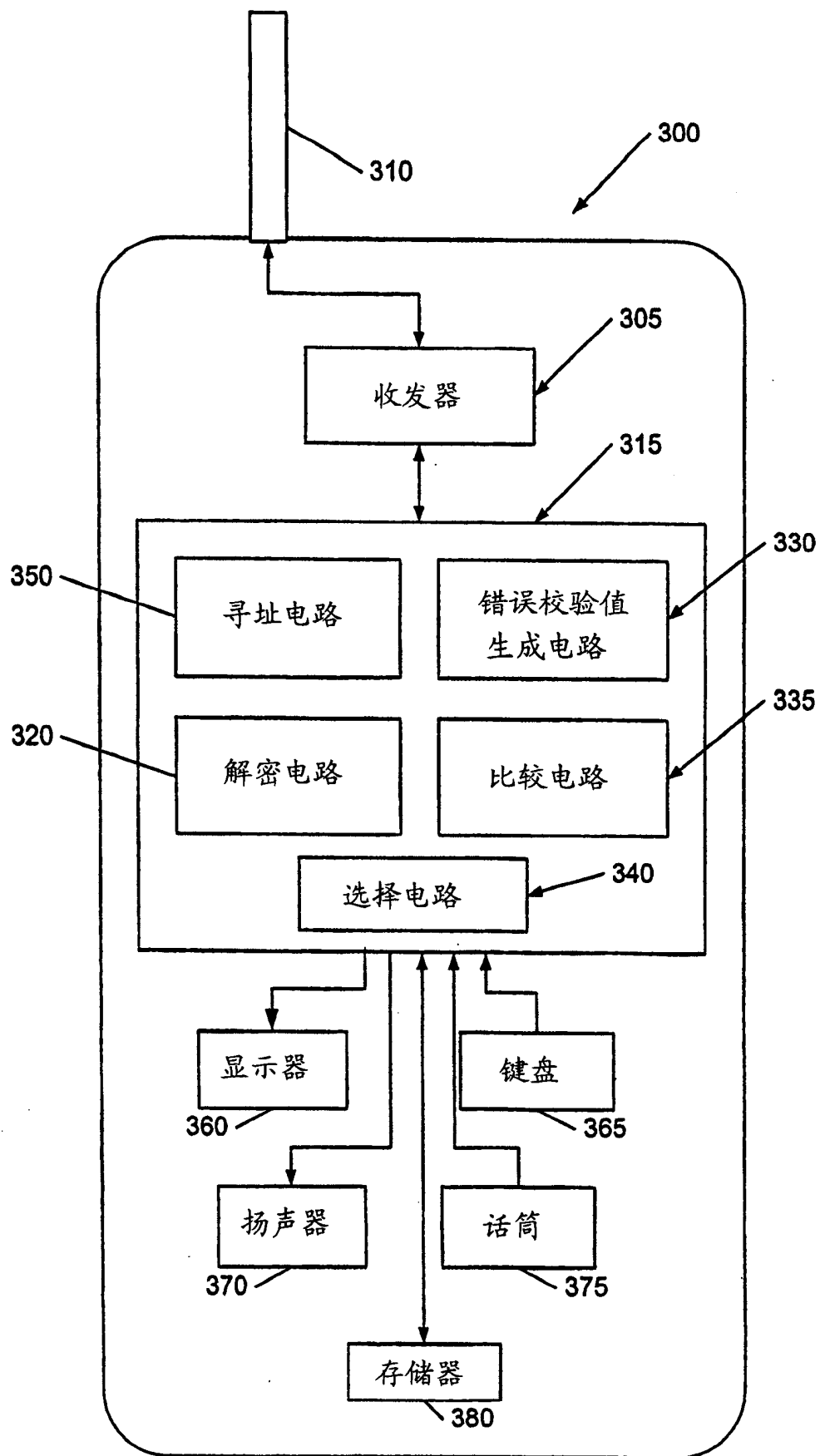


图 4

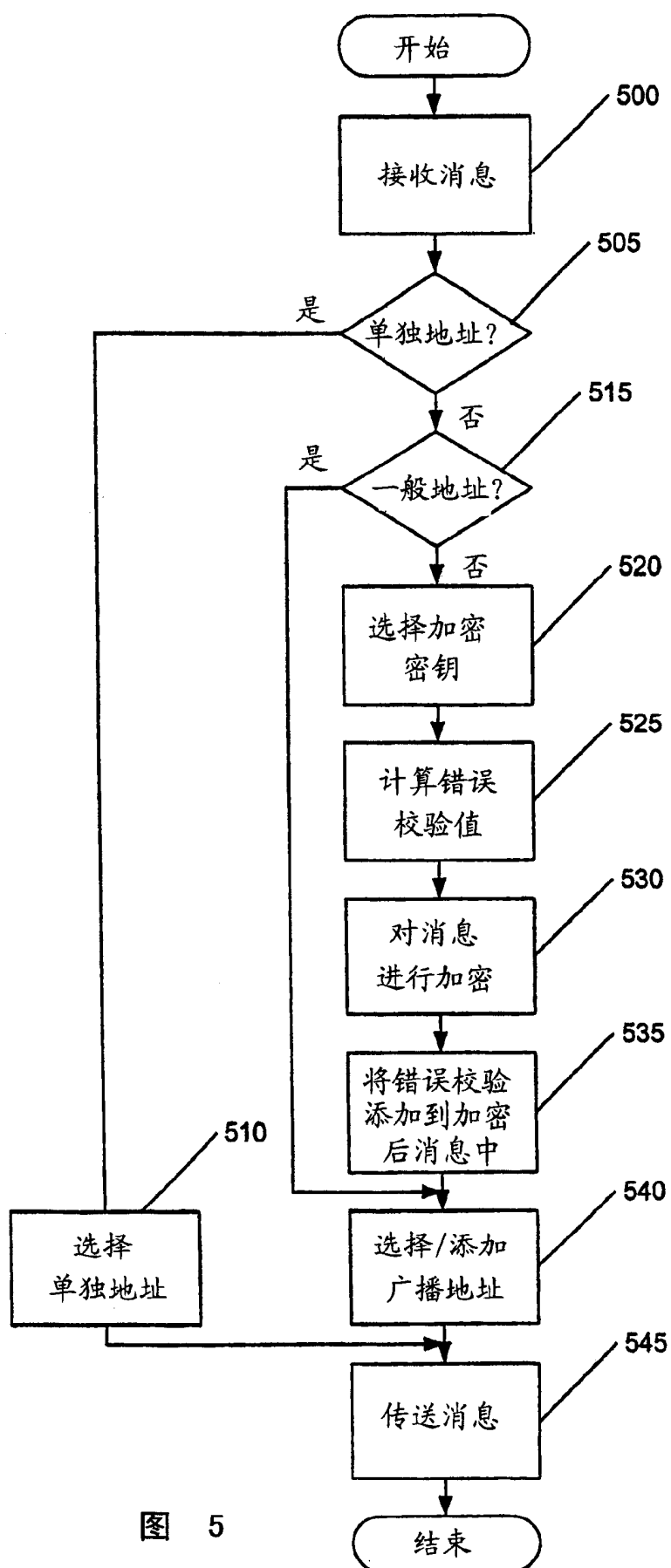


图 5

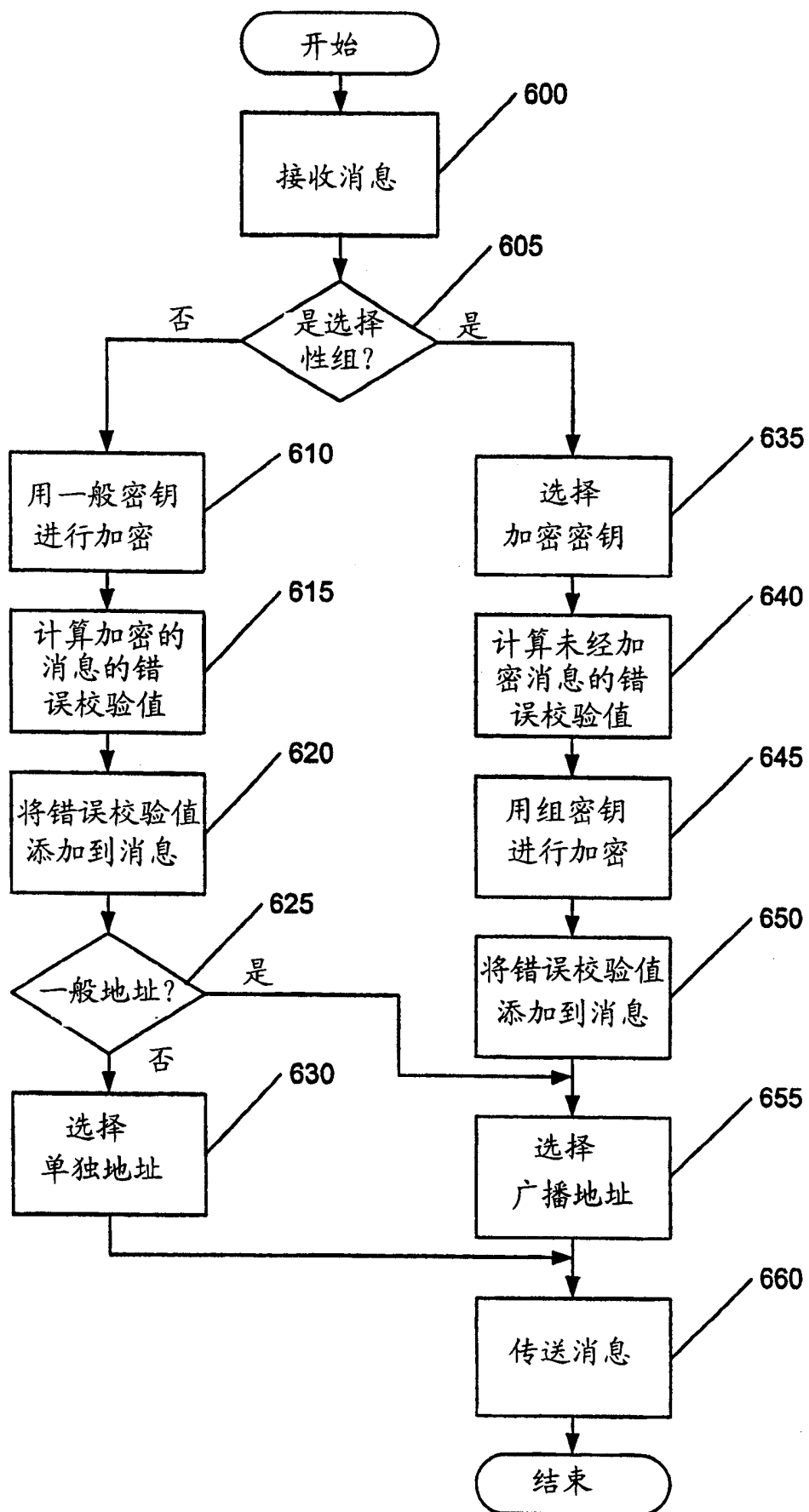


图 6

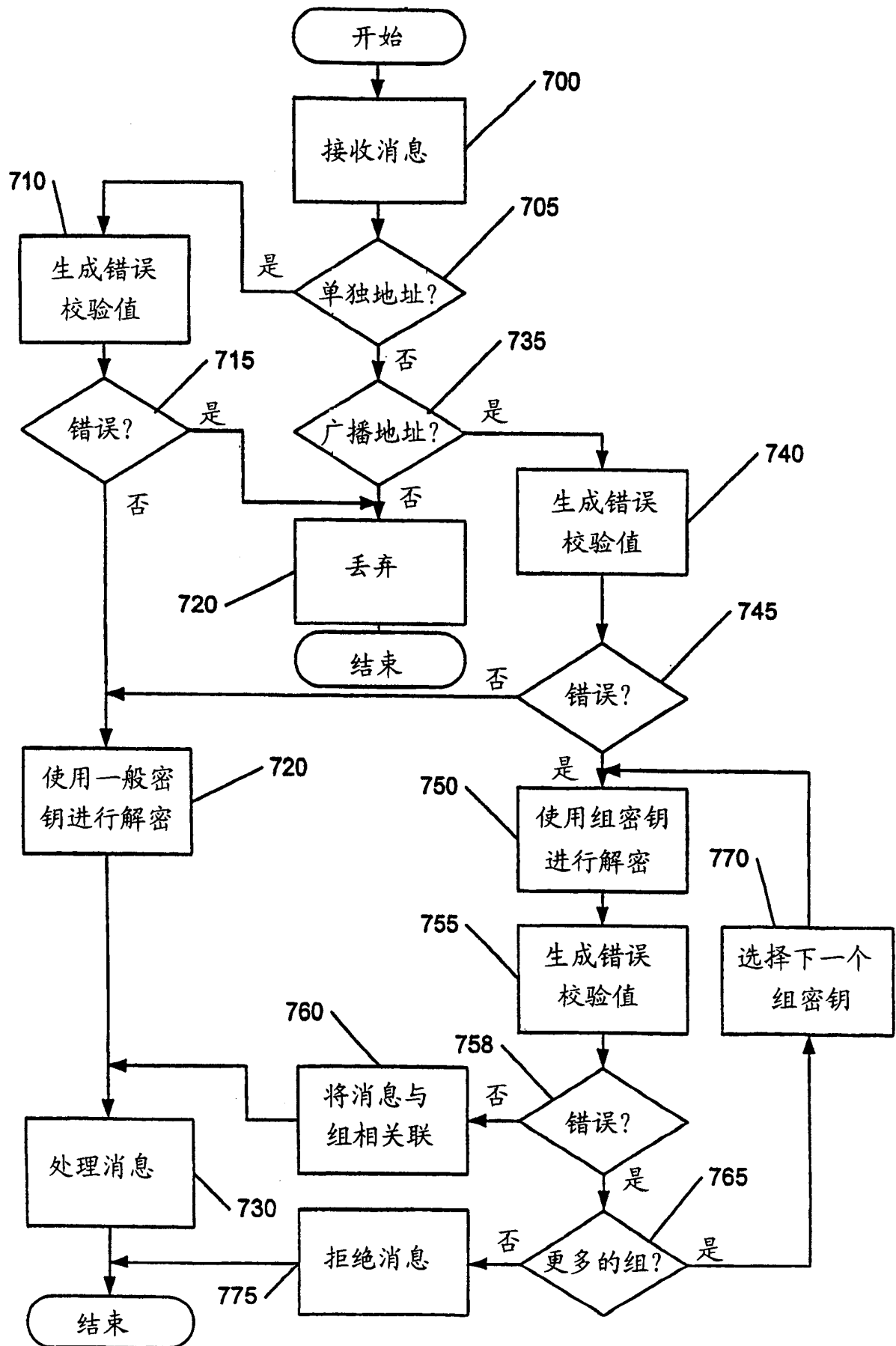


图 7

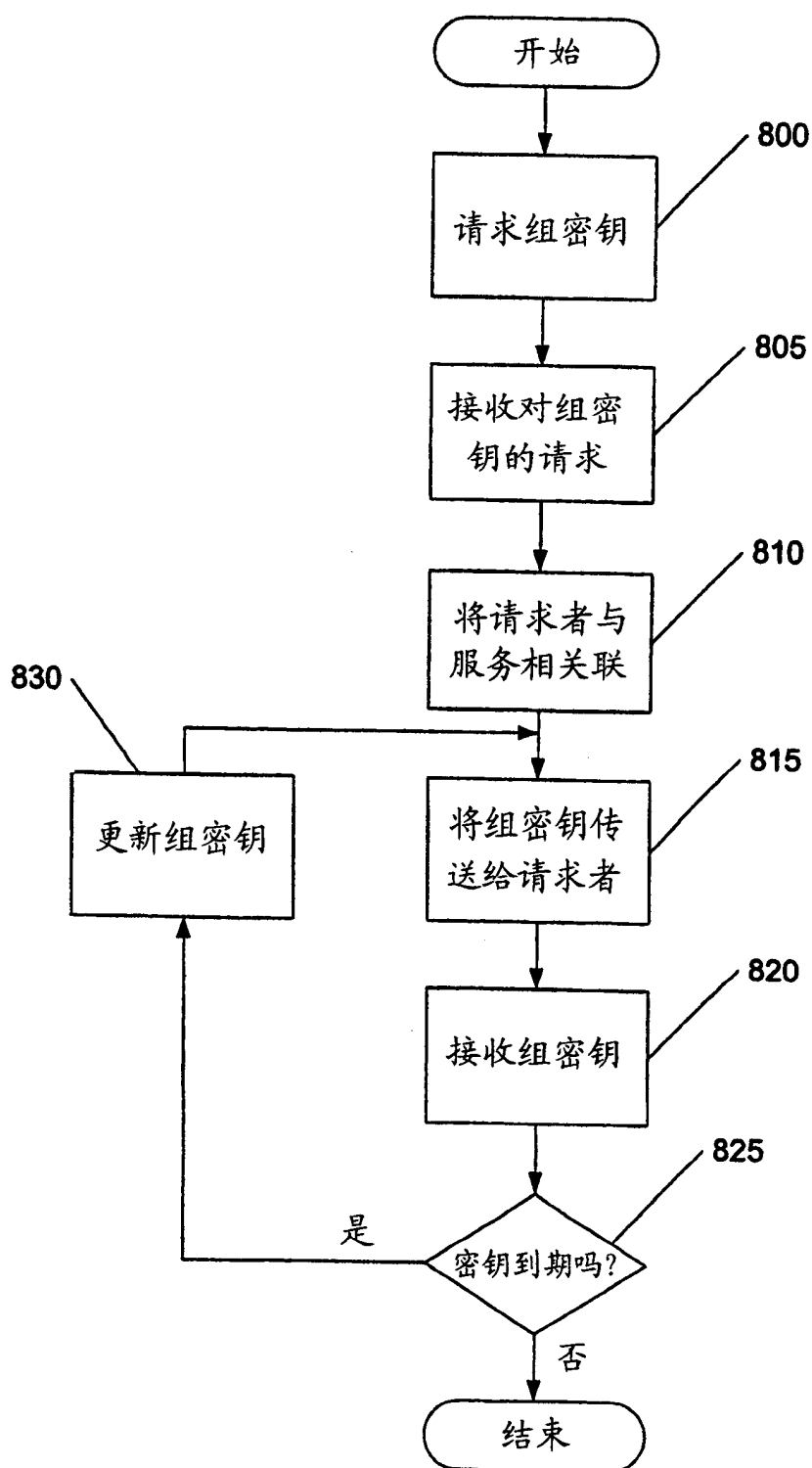


图 8