[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04Q 7/26

[12] 发明专利申请公开说明书

[21] 申请号 00816178.X

[43] 公开日 2003 年 2 月 26 日

[11] 公开号 CN 1399857A

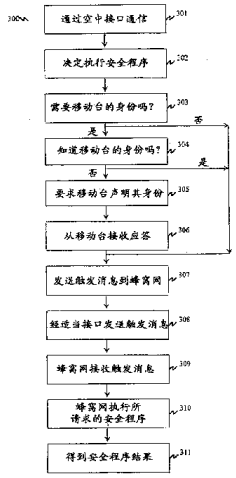
[22] 申请日 2000.11.24 [21] 申请号 00816178.X
[30] 优先权
[32] 1999.11.26 [33] FI [31] 19992530
[86] 国际申请 PCT/FI00/01024 2000.11.24
[87] 国际公布 WO01/39536 英 2001.5.31
[85] 进入国家阶段日期 2002.5.24
[71] 申请人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 汉努·弘卡拉 马库·劳蒂沃拉
塔皮奥·斯克 皮特里·沃苏凯宁
蒂莫·汉尼宁 罗伊·米克斯
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李德山

权利要求书 4 页 说明书 14 页 附图 5 页

[54] 发明名称 在混合蜂窝电信系统中执行涉及移动台的安全程序的方法和设备

[57] 摘要

一种用移动台执行安全程序的方法(300)，其中混合蜂窝电信系统与移动台(301)通信，而且该混合蜂窝电信系统与蜂窝网(308)通信。该方法的特征在于，蜂窝网用移动台执行安全程序，涉及安全程序的数据借助该混合蜂窝电信系统在该蜂窝网和移动台之间传送，以及触发蜂窝网的安全程序的决定是在蜂窝网(309)外部做出的。本发明还涉及一种混合蜂窝电信系统(100、200)中的单元(510)，它触发安全程序，以及涉及一种蜂窝网中的网络单元(500)，它在接收到触发信号后执行安全程序。



ISSN1008-4274

权　利　要　求　书

1. 一种用移动台执行安全程序的方法（300），其中

- 混合蜂窝电信系统与移动台（301）通信，
- 该混合蜂窝电信系统与蜂窝网（308）通信，

其特征在于

- 蜂窝网用移动台执行安全程序，
- 涉及安全程序的数据借助该混合蜂窝电信系统，在该蜂窝网和移动台之间传送，以及
- 触发蜂窝网的安全程序的决定是在蜂窝网（309）外部做出的。

2. 根据权利要求 1 的方法（300），其特征在于，有关触发安全程序的决定在混合蜂窝电信系统（302）中做出，而且蜂窝网的安全程序由该混合蜂窝电信系统触发。

3. 根据权利要求 2 的方法（300），其特征在于，安全程序由将蜂窝分系统连接到该混合蜂窝电信系统的网关单元（202）触发。

4. 根据权利要求 2 的方法（300），其特征在于，安全程序由属于该混合蜂窝电信系统的网闸（203）触发。

5. 根据权利要求 2 的方法（300），其特征在于，安全程序由属于该混合蜂窝电信系统的基站收发信台（201）触发。

6. 根据权利要求 2 的方法（300），其特征在于，移动台的身份由混合蜂窝电信系统请求（305）。

7. 根据权利要求 1 的方法（300），其特征在于，有关触发安全

程序的决定由所述移动台（302）做出，而且蜂窝网的安全程序由所述移动台触发。

8. 根据权利要求 1 的方法（300），其特征在于，通过经适当的接口（307、308）发送触发消息到蜂窝网以触发安全程序。

9. 根据权利要求 8 的方法（300），其特征在于，通过发送具有请求的安全程序指示的移动性管理消息（406、407）来触发安全程序。

10. 根据权利要求 1 的方法（300），其特征在于，混合蜂窝电信系统的固定网的某一部分是利用网际协议网和 H.323 标准实现的。

11. 一种用于在混合蜂窝电信系统（100、200）中用移动台（140）执行安全程序的设备（511），该系统具有用以与移动台（140）通信的装置（105、201、202、203、204）及用以与蜂窝网（130）通信的装置（125、206、207），其特征在于，该设备包括用以从所述混合电信系统（100、200）发送触发信号到所述蜂窝网（130）的装置（512、513、514）。

12. 根据权利要求 11 的设备，其特征在于，所述触发信号为移动性管理消息，其中分配一个适当的参数值用于指示请求的安全程序。

13. 根据权利要求 11 的设备，其特征在于，所述蜂窝网（130）为 GSM 网络，而该混合蜂窝电信系统的至少部分非蜂窝分系统为基于分组的网络。

14. 根据权利要求 11 的设备，其特征在于，所述蜂窝网（130）为 UMTS 网络，而该混合蜂窝电信系统的至少部分非蜂窝分系统为基于分组的网络。

15. 一种混合蜂窝电信系统（100、200）的单元（510），该系统具有用以与移动台（140）通信的装置（105、201）及用以与蜂窝网（130）通信的装置（125、206、207），其特征在于，该单元包括设备（511），该设备具有用以发送安全程序触发信号到蜂窝网（130）的装置（512、513、514）。

16. 根据权利要求 15 的单元（510），其特征在于，所述触发信号为具有所请求的安全程序指示的移动性管理消息。

17. 根据权利要求 15 的单元（510），其特征在于，该单元为基站收发信台（201）。

18. 根据权利要求 15 的单元（510），其特征在于，该单元为网关（202），它将蜂窝分系统连接到该混合蜂窝电信系统。

19. 根据权利要求 15 的单元（510），其特征在于，该单元为网闸（203）。

20. 一种蜂窝网（130）的单元（500），它具有用移动台（140）执行安全程序的装置，其特征在于，该单元包括用以接收安全程序触发信号的装置（502、503、504）。

21. 根据权利要求 20 的单元（500），其特征在于，所述单元（500）具有用于根据接收的触发信号初始化安全程序的装置（502、503、504）。

22. 根据权利要求 20 的单元（500），其特征在于，所述触发信号为移动性管理消息，其中分配一个适当的参数值用于指示所请求的安全程序。

23. 根据权利要求 20 的单元（500），其特征在于，所述单元为移动交换中心。

24. 根据权利要求 20 的单元（500），其特征在于，所述单元为 GSM 网络的单元。

25. 根据权利要求 20 的单元（500），其特征在于，所述单元为 UMTS 网络的单元。

说　　明　　书

在混合蜂窝电信系统中执行涉及移动台的安全程序的方法和设备

技术领域

本发明一般涉及在组合蜂窝电信网与其它网络的电信系统中执行安全程序。本发明尤其涉及有关移动台的安全程序。

背景技术

传统的独立网络已经用于传送数据和话音。目前数据主要在基于分组的网络中传送，尤其是在网际协议（IP）网络中传送。这些网络可以是例如，简单的局域网（LAN）或复杂的互连公司（corporate）网。话音呼叫传统地在电路交换网中传输。然而近些年，在使用类似因特网的基于分组的网络作为传输媒介的实时数据应用上发展极为迅速。这些实时应用可支持话音和可视电话，而且例如，IP 电话预期要比传统的固定或移动网络电话便宜。

国际电信联盟（ITU）已经创建了 H.323 规范，用于定义通过不提供服务质量（QoS）保证的网络进行音频、视频及数据通信的标准框架结构。例如，基于分组的网络可以是这些网络。H.323 规范旨在允许出自不同制造商的多媒体产品和应用互操作。H.323 规范为呼叫控制、多媒体管理和带宽管理以及网络之间的对接定义了功能。H.323 规范为基于网络的通信系统定义了 4 种主要组成部分：终端、网关、网闸（gatekeeper）及多点控制设备。下面将简要描述 H.323 终端、网关及网闸。对于存在至少 3 个参与者的会议电话需要多点控制设备。

终端为网络中的客户设备。它典型地为用户提供实时、双向通信。所有 H.323 终端必须支持话音通信，它们也可支持视频和数据通信。终端可以利用个人计算机实现，或终端可以是独立设备，如常规电话。终端的其它例子有因特网电话、音频会议电话终端、以及可视会议电话终端。

网关用于连接 H.323 网络与其它类型的网络和/或终端类型。网关可例如，转换网络之间的信息传输格式或协议。可能分布的 H.323 网关也可参与呼叫建立及网络之间的其它程序。

网闸用作 H.323 网络的一个给定地域，即 H.323 区域的控制设备。网闸为注册的端点，例如 H.323 终端或网关，提供呼叫控制业务。此外，网闸执行于终端的局域网别名和网关之间的地址转换为 IP 或其它网络地址。网闸也可执行带宽管理，即传输资源控制。注册、地址转换及带宽管理应用注册、许可及状态（RAS）信令。

网闸也可用于路由 H.323 呼叫，在此情况下呼叫受网闸的控制。这使得能以简单方式提供多种多样的服务和业务管理功能。虽然网闸的概念在逻辑上独立于网关或多点控制设备的概念，但网闸也可在同一物理设备实现为网关或多点控制设备。

通常，涉及移动台的呼叫在连接的某一点通过固定线路传送，固定线路可以是蜂窝网的一部分或传统的公众交换电话网（PSTN）的一部分。最近已经开发了使用其它固定网络，尤其是基于分组的网络，用于传送至少一些移动台始呼或移动台被呼的呼叫的系统。这些系统在此称为混合蜂窝电信系统，它们中的例子有多呼叫平台。

混合蜂窝电信系统的例子在图 1 示出。系统 100 包括蜂窝分系统 101-104，它应用支持与移动台 140 通信的蜂窝技术。每个蜂窝分系统包含至少一个基站或对应的网络单元，作为例子，图 1 示出了在蜂窝分系统 102 中的基站 105。系统 100 的其余部分可以利用其它网络技术实现，例如 IP 网络和 H.323 标准。该混合蜂窝电信系统的非蜂窝部分 110 包括两个本地非蜂窝分系统 111 和 112，以及借助例如因特网与该非蜂窝分系统相连的公共非蜂窝部分 113。

本地非蜂窝分系统 111 和 112 可以位于公司的两个不同房屋内，而且它们用于借助蜂窝分系统发送呼叫和连接到移动台。本地非蜂窝分系统需要具备路由呼叫的实体（对应 H.323 网闸）以及数据库，在该数据库中存储有关借助蜂窝分系统可到达的终端的信息。在图 1 中这些单元已经用本地网闸 115 和 117 及本地数据库 114 和 116 表示。

蜂窝网关 121-124 连接蜂窝分系统到本地非蜂窝分系统，而且它们负责进行例如必要的协议转换。网关在此称为蜂窝网关，只不过是为了将它们区别于在混合蜂窝电信系统中可能涉及的其它网关。

当混合蜂窝电信系统的蜂窝分系统例如覆盖公司的所有办公室和建筑物时，从一个办公室到另一个办公室的移动呼叫可以利用该系统的非蜂窝部分作为固定传输媒介进行。呼叫无需通过公众蜂窝或固定电话网，即无需通过公众网关 125。尤其是如果该公司在世界各地都有办公室时，这可以使电话费用大为节省。

混合蜂窝电信系统 100 经公众网关 125 连接到公众蜂窝网 130。公众蜂窝网 130 典型地由蜂窝网络运营商拥有、管理及维护，而蜂窝分系统（在图 1 中，例如蜂窝分系统 101-104）可以由蜂窝网络运营商或蜂窝分系统所处房屋的公司运作。

呼叫和信令信息均可通过公众网关 125 传递。另一端点不在该混合蜂窝电信系统内的呼叫通过图 1 所示例子中的公众蜂窝网 130 路由。与网关 125 相连的公共非蜂窝部分 113 可以位于蜂窝网络运营商的房屋内。有关经允许使用该混合蜂窝电信系统的移动台和用户的信息需存储于该系统中，例如存储于用户数据库 118 中。

从某种意义上讲，混合蜂窝电信系统是公众蜂窝网 130 的延伸。混合蜂窝电信系统可依赖于得接入由公众蜂窝网 130 提供的某一业务。例如，必要的用户信息可以取自公众蜂窝网。需要通知公众蜂窝网能通过该混合蜂窝电信系统到达的移动台。否则它无法例如，正确地路由呼入。

多呼叫平台（RCP），它组合某一蜂窝系统的部分和分系统和固定网络技术，在此用作混合蜂窝电信系统的更有形的例子。图 2 提供了一个 RCP 系统 200 的原理图，它应用全球移动通信系统（GSM）作为蜂窝系统，而且组合 H.323 标准和 IP 网络用于通过固定网传输部分呼叫。部分 RCP 系统位于公司房屋 220a 内。这个部分包括局域网 209a 及至少一个蜂窝分系统，在局域网 209a 中，呼叫和与呼叫相关的信息以 H.323 格式表示。LAN 209a 经基于 IP 的网络 230 连接到另

一 LAN 209b，209b 由蜂窝网运营商 220b 运作，而且通常位于蜂窝网运营商的房屋内。只要 LAN 209a 和 209b 都连接到相同 IP 网 230，它们就不必位于相同房屋内。

位于公司房屋 220a 内的每个蜂窝分系统包括一个或多个基站收发信台（BTS）201 以及与这些基站收发信台相连的分系统控制器（SSC）202。在 RCP 系统中，分系统控制器通常称为 IMC（内联网移动性群集）。SSC 提供给 BTS 与 BSC 相同的接口，但是实际功能典型地在不同 RCP 实体之间分配。SSC 也用作其控制的蜂窝分系统之间的网关，以及 RCP 系统的 H.323 部分。SSC 202 连接到办公室 220a 的局域网 209a。

网闸（WGK）203 为 H.323 网闸，其中已经添加了一些 GSM 功能。其涉及 RCP 系统中的信令。它用作其区域内所有呼叫的中心点并提供呼叫控制和管理服务，如网络拓扑信息，RCP 用户信息的更新，呼叫建立期间的地址转换，许可控制及带宽控制。网闸也以多种方式用作虚拟开关。因此网闸有时候也称为移动电话服务器（MTS），每个 RCP 区域可以由一个网闸管理。

RCP 系统 200 的蜂窝分系统 210 和非蜂窝分系统 211 由图 2 中的虚线示出。网闸 203 的 203a 部分构成 RCP 系统 200 的蜂窝网关（例如对应图 1 中的蜂窝网关 121）。

有关在 RCP 系统中出现的每个移动台和 H.323 兼容终端 205 的信息存储于端点数据库（EPD）204，该数据库或连接到网闸 203，或成为该网闸的一部分。利用在 EPD 204 中存储的信息，网闸 203 可确定呼叫的目的地地址是否在其控制区内。当在 RCP 系统中建立呼叫时需要这个信息。

在第二 LAN 209b，有一个 A-接口网关（AGW）206 和内联网位置寄存器（ILR）207。A-接口网关 206 处理 RCP 系统 200 和公众蜂窝网 130 之间经 A-ter 型接口 241 的通信。A-ter 接口为在 GSM 网络中，在码型变换器子复用器（TCSM）和基站控制器之间通常存在的接口。因此，RCP 系统 200 和公众蜂窝网 130 之间的通信可以像基站

分系统和公众蜂窝网 130 之间的正常通信那样处理，从公众蜂窝网 130 的观点看，RCP 系统 200 用作普通的基站分系统。AGW 负责在公众蜂窝网和 RCP 系统的 H.323 部分之间转换语音和数据流及信令。如果 RCP 系统采用其它一些蜂窝网标准而非 GSM，那么 AGW（或具有不同名称的对应网关）的功能由相关蜂窝网标准确定。

ILR 数据库 207 的主要功能是存储使用 RCP 系统 200 的用户的移动性管理信息。对于有权使用 RCP 系统的所有用户来说，在 ILR 有一个永久入口。ILR 包含 RCP 特定信息（如移动台当前所处区域的控制网闸的 IP 地址）和 GSM 特定信息（尤其是在来访位置寄存器（VLR）中存储的相同信息）。网闸 203 负责更新 ILR 中的 RCP 特定信息，而且 ILR 207 和公众蜂窝网 130 之间的通信借助 MAP-接口 242 处理。MAP 接口是在归属位置寄存器（HLR）和移动业务交换中心（MSC）之间通常存在的标准 GSM 接口。因此从蜂窝系统 130 的观点来看，来自 RCP 系统 200 的移动性管理信息就象普通 GSM 用户的移动性管理信息那样处理。

当移动台 140 用在存在 RCP 系统 200 的办公室 220a 时，呼叫由 BTS 201 接收，就像在普通蜂窝网络中一样。SSC 202 变换它从移动台 140 接收并由上行链路无线电连接传输的数据为根据 H.323 标准的 IP 分组。它还发送这些分组到局域网 209a。当数据从局域网 209a 经 BTS 201 传送到移动台 140 时，SSC 202 将接收的 H.323 信息转换为 BTS 201 能理解的适当蜂窝网标准格式。

网闸 203 负责在建立呼叫时涉及的信令。如果目的地地址在网闸的控制区内而且目的地为 H.323 终端 205，那么就与 H.323 终端 205 直接建立连接。如果目的地为网闸 203 控制区内的移动台 140，那么呼叫经 SSC 202 被传送到 BTS 201 再到移动台 140。如果呼叫是从移动台 140 到另一 RCP 区域，那么呼叫被送入控制该另一 RCP 区域的网闸。如果目的地为移动台，则通知由此移动台可到达的两个 SSC 建立该呼叫。

当呼叫是从 RCP 系统 200 到一个目的地，该目的地是通过公众蜂

窝网 130 可到达的移动电话(任一移动台所有者为 RCP 系统覆盖区外部的 RCP 用户，或根本不是 RCP 用户）时，网闸 203 借助类似因特网的分组交换网传送呼叫到 A-接口网关 206。如上所述，AGW 206 通过 A-接口 241 与公众蜂窝网 130 通信。因此，公众蜂窝网 130 像 MSC 接收的任何普通移动台呼叫那样处理该呼叫，并利用已知的特定网络方法和系统连接该呼叫。

如果该呼叫是从 H.323 终端 205 到 PSTN 232 或到公众蜂窝网 130，那么该通信由 ISDN 网关（IGW）208 处理。因此从类似 PBX（专用小交换机）的公众蜂窝网 130 的观点来看， IGW 208 借助 DSS.1 接口 243 与公众蜂窝网 130 通信。这使得 H.323 终端 205 能利用公众蜂窝网 130 与除 RCP 系统内的移动台之外的其它移动台通信。IGW 还处理 RCP 系统 200 和 PSTN 网络 232 之间的通信，这使得 H.323 终端能与 PSTN 网络 232 通信。从移动台 140 至 PSTN 网络 232 的呼叫可以借助 AGW 206 利用公众蜂窝网 130 中的系统处理以连接该呼叫到 PSTN 网络 232，或利用 IGW 208 该呼叫可连接到 PSTN 网络 232。

在 RCP 系统 200 中，移动台之间的呼叫使用 GSM 语音编码。如果移动台始呼的呼叫是通过公众蜂窝网路由到固定电话，那么公众蜂窝网将负责解码语音。如果呼叫的一个端点为 RCP 系统 200 中的移动台，而另一个端点为 H.323 终端，那么在 GSM 编码和 H.323 标准定义的编码方法之间可能需要解码和重新编码该语音。

加密 GSM 系统中 BTS 和移动台之间的通信是标准空中接口的部分功能。由于 RCP 系统 200 使用相同标准接口用于 BTS 201 和移动台 140 之间的通信，因此利用与正常 GSM 系统相同的程序执行加密。GSM 程序应用常规密钥加密技术，其中密钥必须为加密方和解密方知晓。对 RCP 系统内的那些移动台 GSM 加密密钥 Kc 存储于 ILR。在 GSM 中，网络决定何时鉴权移动台或何时生成新的加密密钥。生成和使用新的加密密钥对确保加密难以破解，即防止窃密是必要的。不应用单个加密密钥加密太多的信息。

当呼叫是借助 GSM 网在 RCP 外部进行时，GSM 网络负责必要

的密钥生成和鉴权程序。其中的问题在于，当呼叫是在RCP内部进行时，蜂窝网络无法察觉它们。因此，无法负责必要的生成程序。

另一方面，鉴权验证移动台的身份，或实际上是移动台中SIM卡的身份。这使得例如，网络能生成与正确的SIM身份相关的计费信息。此外，根据用户或SIM卡的身份可以限制接入某些业务。另一问题在于，在某些情况下，RCP系统不知道使用其资源的移动台的身份。例如，如果切换是从GSM网到RCP系统进行的，有关加密密钥的必要信息是在GSM网络的原BSC和RCP系统的新BSC之间发送。只有有关加密密钥的信息才被发送，不接收有关移动台身份的信息。只有在移动台发送位置更新消息以通知系统其当前位置后（使得呼入路由到正确的小区），移动台才被蜂窝网鉴权而且移动台的身份才会为蜂窝网和RCP系统知晓。

因此，RCP系统或其它混合蜂窝电信系统必须在某些情况下自己确定何时鉴权移动台以及何时改变加密密钥。如果不改变在混合蜂窝电信系统中使用的所有移动台，系统将无法鉴权移动台或生成新加密密钥。移动台所支持的方法只在蜂窝系统中使用，而且使用的许多程序为蜂窝网络运营商的专有信息。

有可能为混合电信系统，例如为RCP系统，设计和创建独立的鉴权和密钥管理系统。在此问题在于，这种系统将需要在RCP系统中使用的所有移动台具备某一特殊设备，这种设备能存储RCP特定的秘密信息以及能基于这个信息进行计算。此外，该秘密信息应仅为移动台知晓，而如果使用的是常规对称密钥加密技术，应仅为RCP系统知晓。SIM卡可能可以用于这种目的，但它只能解决一半问题。对于将在RCP系统使用的每个移动台来说，在ILR中应有一个记录，例如，描述其密钥（常规加密）或公共密钥（公共密钥加密）。系统的构成和管理将冗长乏味，而且偶尔的来访者无法使用RCP系统。

发明内容

本发明的一个目的是提供一种用于在混合蜂窝电信系统中提供安全服务的新方法。安全服务包括鉴权及生成和交换加密密钥。该方法

甚至可用在移动台仅与该混合蜂窝电信系统内的终端通信时。

本发明的另一目的是提供一种用于在混合蜂窝通信中提供安全服务的新设备。这种设备对现有网络单元很容易实现，因此能经济地解决现有技术的上述问题。

本发明的再一目的是提供新网络单元，它包括用于在混合蜂窝电信系统中提供安全性的设备。利用使转换更容易和经济可行的软件修改，当前网络单元可转换为根据本发明的网络单元。

本发明的上述这些和另外目的是通过令蜂窝网的正常安全程序在外部触发实现的。

根据本发明用移动台执行安全程序的方法，其中：

- 混合蜂窝电信系统与该移动台通信，以及
- 该混合蜂窝电信系统与蜂窝网通信，

该方法的特征在于：

- 蜂窝网用移动台执行安全程序，
- 涉及安全程序的数据在该蜂窝网和移动台之间借助该混合蜂窝电信系统传送，以及
- 用以触发蜂窝网的安全程序的决定是在蜂窝网外部做出的。

根据本发明用于在混合蜂窝电信系统中用移动台执行安全程序的一种设备，混合蜂窝电信系统具备用以与移动台通信的装置及用以与蜂窝网通信的装置，特征在于该设备包括用于从所述混合电信系统发送触发信号到所述蜂窝网的装置。

根据本发明的混合电信系统的一种单元，混合蜂窝电信系统具备用以与移动台通信的装置及用以与蜂窝网通信的装置，特征在于该单元包括一个设备，其具备用以发送安全程序触发信号到蜂窝网的装置。

根据本发明的蜂窝网的一种单元，具备用移动台执行安全程序的装置，特征在于该单元包括用以接收安全程序触发信号的装置。

在根据本发明的方法中，移动台借助混合蜂窝电信系统与其它终端通信。该混合蜂窝电信系统具备使移动电话经该电信系统建立呼叫

或连接的装置，即至少一个蜂窝分系统。

在根据本发明的方法中，当需要运行安全程序时，从外部触发蜂窝网的正常安全程序，而且涉及安全程序的数据或消息借助该混合蜂窝电信系统在蜂窝网和移动台之间传送。当蜂窝网接收到触发请求时，它执行所请求的安全程序。当前只有蜂窝网能确定何时运行安全程序，因此该方法的实现需要对某些蜂窝网络单元作小的改变。

安全程序包括鉴权及生成和交换加密密钥。在一些蜂窝网中，例如在 GSM 中，同一程序负责上述这些操作。但是在蜂窝网中，这些程序能独立执行，因此可以请求任何一个程序。

本发明并不拘泥于如何确定需要安全操作或谁确定。例如，可以是移动台请求新加密密钥。或混合蜂窝电信系统可确定需要鉴权移动台，并发送触发请求到蜂窝网。

如果混合蜂窝电信系统不知道移动台的身份，它必须首先询问移动台其身份码，接着要求蜂窝网鉴权该特定移动台。另一方案是，混合蜂窝电信系统发送最初的触发请求到移动台。这个移动台被修改以便在它接收到初始触发请求后发送包含其身份码的鉴权触发请求。这个方案需要对移动台作修改，因此如果存在询问移动台身份的办法，那么第一个方案更为可行。

根据本发明的方法只需要对混合蜂窝电信系统或蜂窝网中的网络单元作小的修改，因此实现更为经济和容易。安全程序初始化请求可以按需要的频度发送到蜂窝网。这使得不会危及空中接口的安全标准就能使用混合蜂窝电信系统。

附图说明

现在通过举例参照优选实施例和附图详细描述本发明，其中：

图 1 是混合蜂窝电信系统的原理图；

图 2 是 RCP 系统的原理图；

图 3 是根据本发明的方法的第一个优选实施例的流程图；

图 4 是根据本发明的方法的第二个优选实施例的流程图；

图 5 是根据本发明的单元和设备的原理图。

具体实现方式

上面参考图 1 和图 2 描述了现有技术。

图 3 是本发明的第一个优选实施例的流程图。在方法 300 中，混合蜂窝电信系统决定用移动台执行安全程序。蜂窝网实际上运行该安全程序。

在步骤 301 执行移动台和电信系统之间的正常通信。该通信典型地通过标准空中接口在属于该混合蜂窝电信系统的移动台和BTS之间处理。通常在步骤 301 的通信为涉及呼叫初始化的通信，但也可使用任何其他类型的通信。

在步骤 302，决定用移动台执行安全程序。这个决定可基于各种参数。为执行安全程序，例如它可以是有关每个呼叫初始化程序的自动判决，或它可以固定间隔周期性做出。特别是在从普通蜂窝网的切换到混合蜂窝电信系统后，可能需要鉴权。该决定可由混合蜂窝电信系统或由移动台本身做出。

在步骤 303，混合蜂窝电信系统决定是否必须执行安全程序以使蜂窝网了解移动台的相关身份。这个决定取决于将执行哪个安全程序以及在蜂窝网中如何实现该程序。例如，不用知道另一方的身份就可能生成加密密钥，只要有另一方的地址就够了。在这种情况下，身份必须在后一步骤中鉴权。例如，有可能混合蜂窝电信系统知道移动台的 H.323 名称的事实就足以用蜂窝网执行某些安全程序。

如果必须知道移动台的身份，在步骤 304 混合蜂窝电信系统检测是否已经知道该身份。如果它不知道，则在步骤 305 要求移动台自己识别。之后它等待移动台应答（步骤 306）。如果移动台拒绝发送应答，那么它和混合蜂窝电信系统之间的通信将被中断。在步骤 307，混合蜂窝电信系统发送触发请求到蜂窝网。这个触发请求指示需要哪个安全程序以及可能的话在该程序中涉及的移动台身份。请求的安全程序可以由例如，该消息中的正确参数值指示。如果不需要移动台的身份，从步骤 303，或如果已经知道其身份，从步骤 304，在流程图中转到步骤 307。

触发消息通过适当的接口在步骤 308 发送到蜂窝网。之后蜂窝网接收触发消息（步骤 309）并用移动台执行所请求的安全程序（步骤 310）。在安全程序已经运行后，在步骤 311 混合蜂窝电信系统就能得到该程序的结果。例如结果可以是对成功鉴权的确认或新加密密钥。

当描述本发明的第三个优选实施例时，应用 GSM 和 H.323 标准的 RCP 系统用作混合蜂窝电信网络的例子，而 GSM 网络用作蜂窝系统的例子。这些例子被选择用于使优选实施例的描述更为有形；但它们决不限制本发明的范围。

图 4 是本发明第二个优选实施例的流程图。图 4 所示的方法 400 在 RCP 系统中可用于鉴权移动台以及生成新加密密钥。在 GSM 网络中，同一程序负责这两个功能。

在步骤 401，执行移动台和 RCP 系统之间的正常通信。该通信典型地通过标准空中接口在移动台和 BTS 之间处理。通常在步骤 401 的通信为涉及呼叫初始化的通信，但也可使用任何其他类型的通信。

在步骤 402，RCP 决定鉴权移动台或生成新加密密钥。在步骤 403，RCP 系统检测其是否知道移动台的身份，实际上是移动用户的身份。实际上它指的是 GSM 用户的临时移动用户标识符（TMSI）或国际移动用户标识符（IMSI）码。为执行应用常规密钥加密的 GSM 安全程序，必须知道移动台的相关 TMSI 或 IMSI。

如果 RCP 系统不知道移动台身份，它必须首先询问（图 4 的步骤 404）。这可以利用例如图 4 建议的 IDENTIFY_REQUEST 消息执行。这个消息通常在移动台的鉴权失败后由 MSC 在 GSM 网中发送。失败原因之一是 MSC 用于从 VLR 获得鉴权的 TMSI 码不正确，MSC 要求移动台给予其 IMSI 码。这就需要从 HLR 取出正确的鉴权信息。移动台例如用 IDENTIFY_RESPONSE 消息应答该身份请求（图 4 的步骤 405）。

一旦知道了移动台的身份，或实际上移动用户的身份，RCP 系统在步骤 406 发送触发消息给蜂窝网。这个消息通过适当的接口在步骤 407 传送到 GSM 网。如果 MSC 负责鉴权移动台，那么鉴权请求经

MAP 接口发送。触发消息例如可以是移动性管理消息。具体说，它可以是 CM_SERVICE_REQUEST 消息，这个消息通常由移动台发送到蜂窝网。一个新值，其名称为例如“所需的鉴权”，可以分配给发送的移动性管理消息中的参数。在 CM_SERVICE_REQUEST 消息中，这个参数可以是例如 CM_SERVICE_TYPE 参数。CM_SERVICE_REQUEST 通过 MAP 接口发送到 MSC。

在蜂窝网一侧，执行鉴权的部分必须了解新参数的意义。如果只添加一个额外的参数值到消息说明中，那么消息格式就不改变。因此转发消息的网络单元应不需要任何修改。

CM_SERVICE_REQUEST 消息包含移动电话的身份码。这个消息通常由移动电话本身发送，而且在这些情况下它能填充必要的身份信息。当 RCP 系统用这个消息触发蜂窝网的鉴权程序时，它必须填充移动台的身份码。

在步骤 408 蜂窝网接收鉴权请求，而在步骤 409 执行鉴权。在 GSM 网络中，通常是 MSC 涉及移动台的鉴权，而且要求 HLR 发送鉴权三元组。这个鉴权三元组包含随机数 RAND，HLR 将它与移动用户密钥 Ki 一起使用，来计算鉴权响应 SRES 和新加密密钥 Kc。在鉴权程序期间，移动台还计算 SRES，它发送 SRES 到 MSC 用于验证。

在步骤 410，RCP 系统已经得到鉴权结果。新鉴权三元组从 GSM 取出给 ILR。作为 GSM 鉴权程序的一部分，移动台生成密钥 Kc，而且利用已知的 GSM 程序，在完成步骤 410 后 BTS 和移动台以同步方式使新密钥生效。

图 5 是 RCP 系统 200 的原理图，它带有网络单元 510，其中包括用以触发涉及本发明的移动台 140 的安全程序的系统 511。例如，网闸 203 可包括用以触发安全程序的系统 511。系统 511 也可在例如 SSC 或 BTS 实现。

图 5 还示出了蜂窝电信网 130，它带有网络单元 500，其中包括用以根据本发明执行安全程序的系统 501。网络单元 500 可以是例如，该蜂窝网内的移动交换中心。图 5 还示出了标准 GSM 接口 241、242

和 244，通过这些接口能处理从 RCP 系统 200 到移动台 140 以及到蜂窝网 130 的通信。

在图 5 中，在 RCP 网络单元 510 中的系统 511 具备 I/O 端口 512，例如利用图 1 所示的 LAN 109a 用以与 RCP 系统 200 的其他部分通信。使用在存储器 514 中存储的程序的处理器 513 用于控制安全程序请求。例如，每当呼叫被初始化或以固定间隔周期性拨打时，可发送该请求。

当希望需要安全程序时，由存储器 514 中存储的程序控制的处理器 513 利用 I/O 端口 512 发送安全程序触发信号到 RCP 系统 200。在本发明的第四个优选实施例中，这个触发信号为正常移动性管理消息，其某一参数已赋予一个新值。触发信号利用已知的方法和装置经与蜂窝电信网 130 的适当接口 241、242 处理。

在蜂窝网 130 中，触发信号最好由控制安全程序的单元接收。在 GSM 系统中这个单元通常为 MSC。单元 500 包括用于初始化安全程序的系统 501。触发信号由 I/O 端口 502 接收并由受存储器 504 中存储的程序控制的处理器 503 检测。当检测到触发信号时，在触发信号中所陈述的正常安全程序被初始化，并利用已知的装置和方法由控制该安全程序的网络单元 500 执行。

给定功能实体，例如基站控制器的名称，通常在不同电信系统语境中不同。例如在通用移动通信系统（UMTS）中，对应基站控制器（BSC）的功能实体为无线网络控制器（RNC）。因此，用于表示在这个说明书中的各种功能实体的特定术语只是相应于 GSM 和 RCP 系统的例子，而无论如何不限制根据本发明的方法或网络单元。

特别是 UMTS 和 UMTS 网络单元可用于未来的混合蜂窝电信系统中，而且根据本发明的方法和网络单元可以利用 UMTS 和 UMTS 网络单元实现。

H.323 标准和 IP 网络的组合已用作非蜂窝电话网的例子。它们并不限制在混合蜂窝电信系统的非蜂窝部分能使用的方法和技术。因此根据本发明的方法和网络单元并不局限于应用 H.323 标准或 IP 技术的方法或网络单元。

混合蜂窝电信系统在此被提出作为组合蜂窝网络技术和既非蜂窝又非传统固定电话技术的技术的电信系统的例子。将这种电信系统划分为蜂窝和非蜂窝分系统在此已用来更有形地解释该系统。它并不局限根据本发明的方法和网络单元使用的系统于具备在此描述的所有不同分系统的这些系统。

鉴于前面的描述，本领域的技术人员知道在本发明的范围内可进行各种修改。虽然已经详细描述了本发明的实施例，但应理解对其进行多种修改和变化都是可能的，所有这些都落入本发明的真正精神和范围内。

说 明 书 附 图

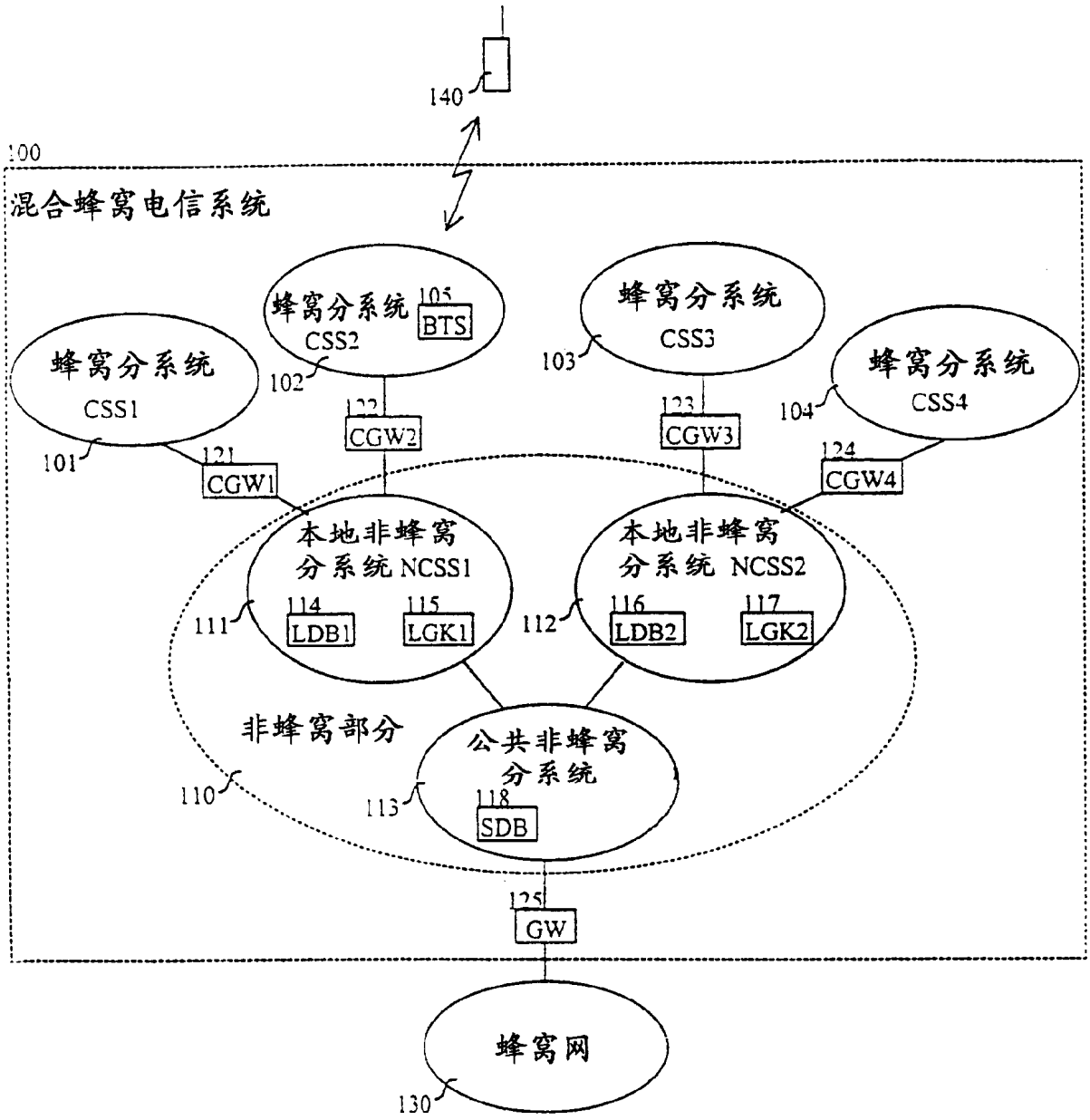


图1
现有技术

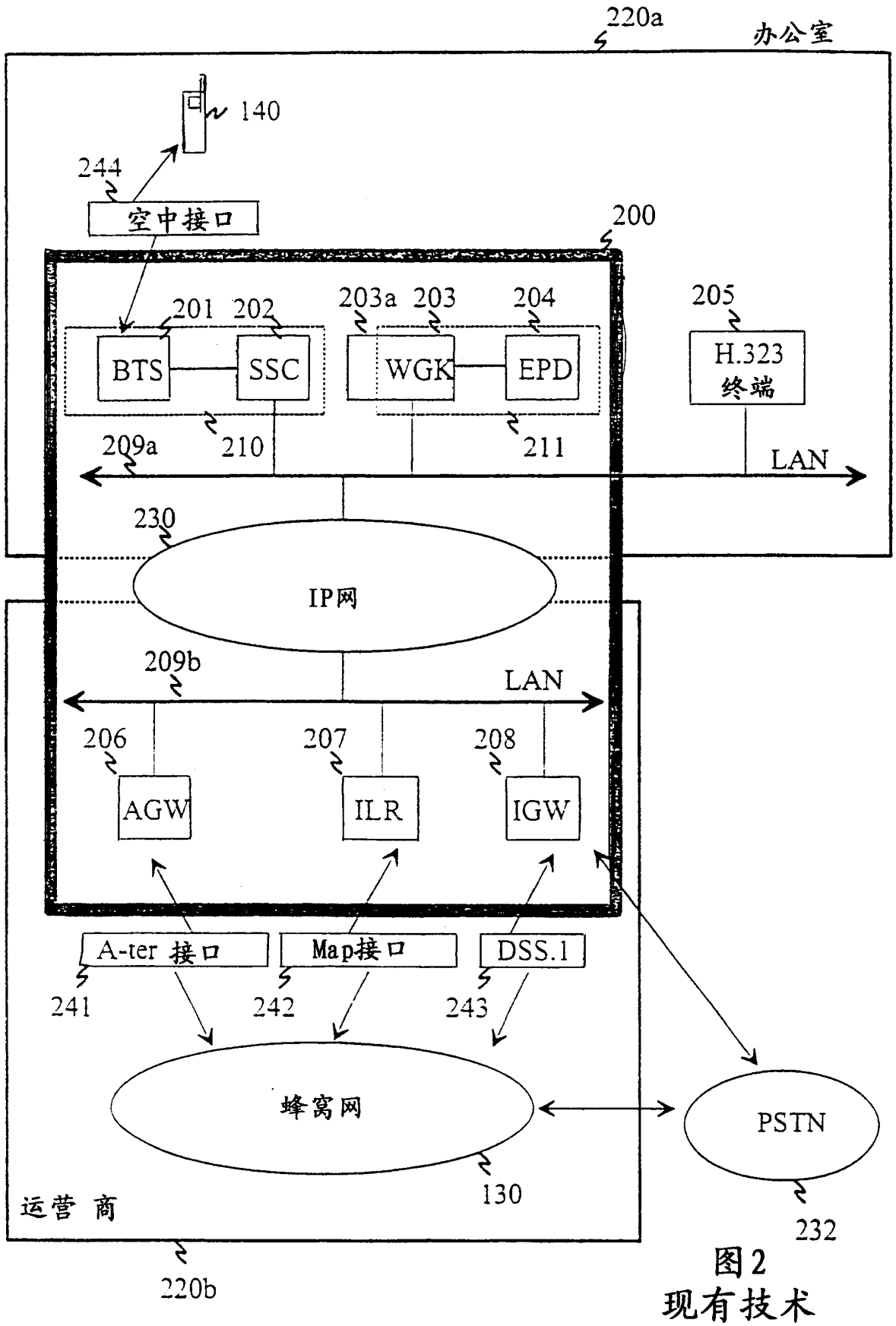


图2
现有技术

IIE021139

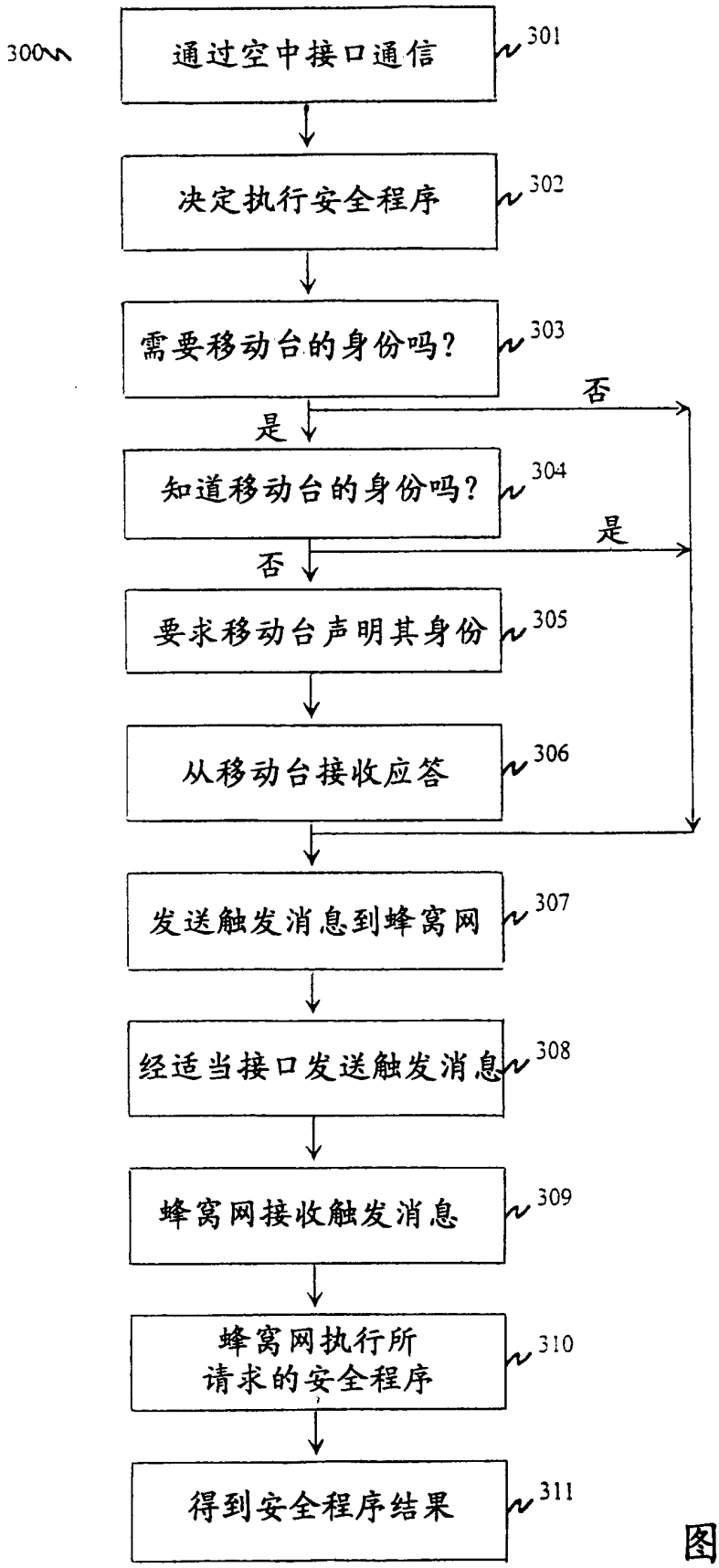

300
通过空中接口通信
301
决定执行安全程序
302
需要移动台的身份吗?
303
否
是
知道移动台的身份吗?
304
是
否
要求移动台声明其身份
305
从移动台接收应答
306
发送触发消息到蜂窝网
307
经适当接口发送触发消息
308
蜂窝网接收触发消息
309
蜂窝网执行所
请求的安全程序
310
得到安全程序结果
311

图3

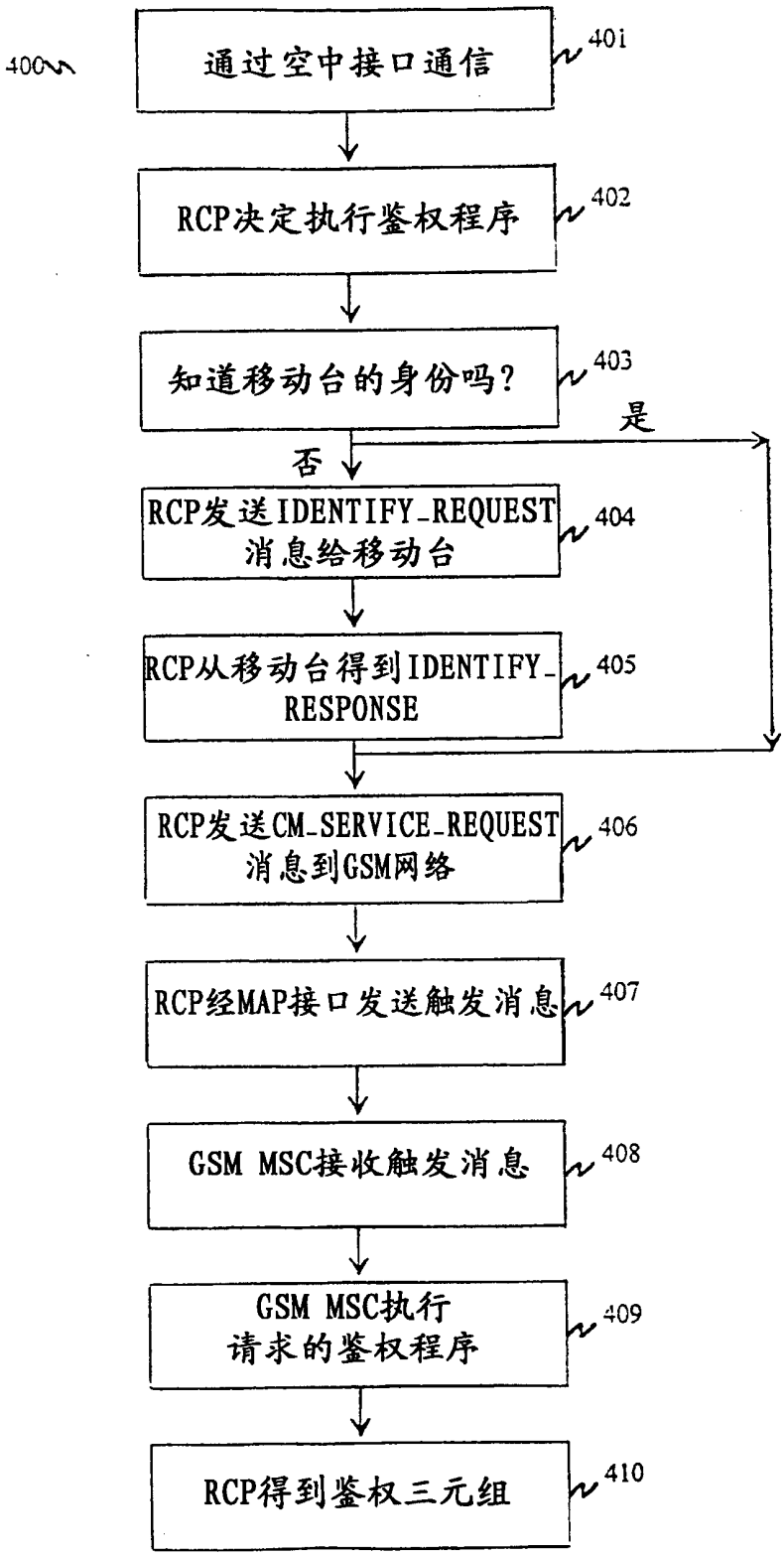

400
通过空中接口通信
401
RCP决定执行鉴权程序
402
知道移动台的身份吗?
403
是
否
RCP发送IDENTIFY_REQUEST消息给移动台
404
RCP从移动台得到IDENTIFY_RESPONSE
405
RCP发送CM_SERVICE_REQUEST消息到GSM网络
406
RCP经MAP接口发送触发消息
407
GSM MSC接收触发消息
408
GSM MSC执行请求的鉴权程序
409
RCP得到鉴权三元组
410

图4

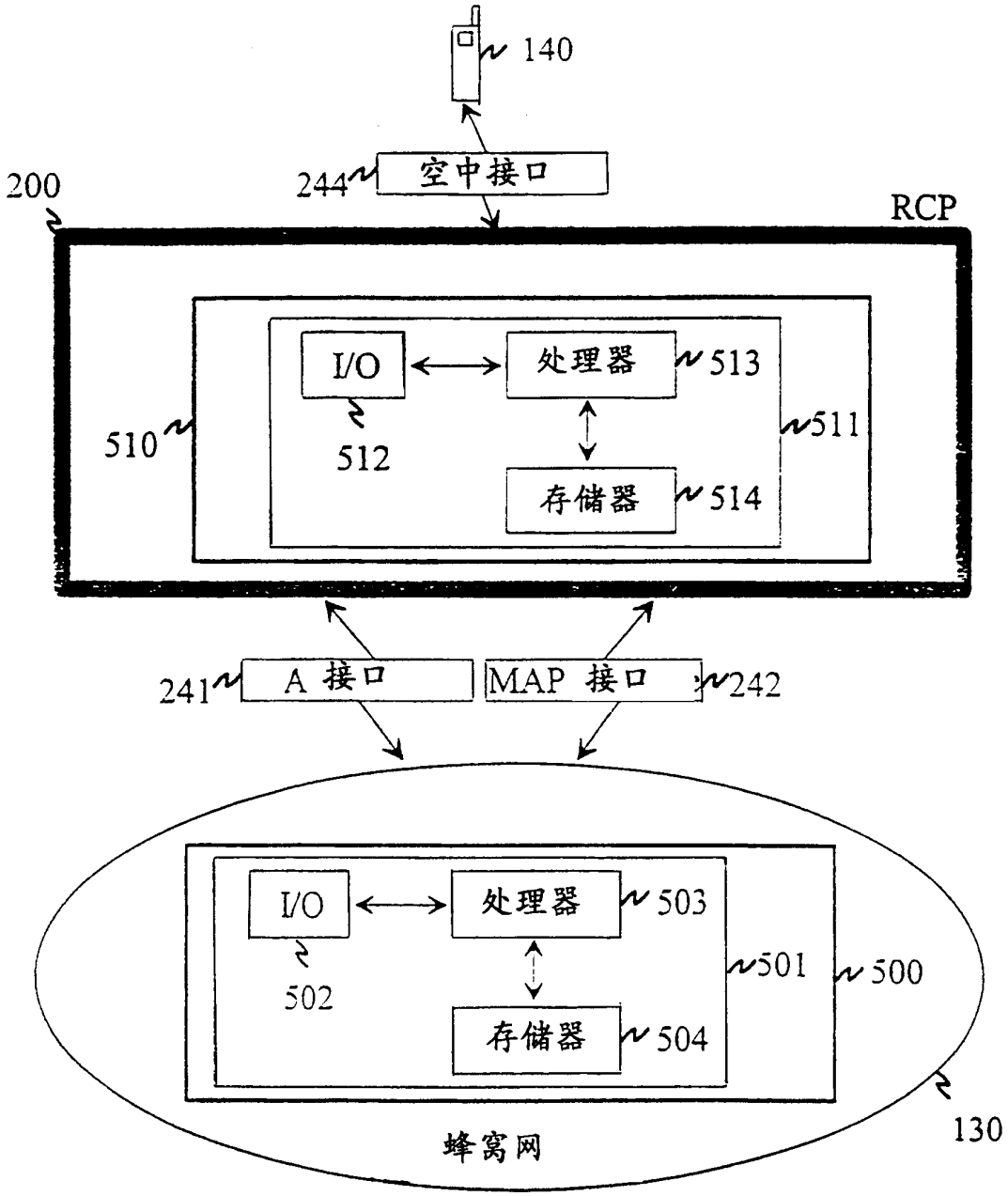

140
空中接口
244
200
RCP
I/O
处理器
513
512
510
511
存储器
514
241
A 接口
MAP 接口
242
I/O
处理器
503
502
501
500
存储器
504
130
蜂窝网

图5