[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04K 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02827523.3

[45] 授权公告日 2009 年 3 月 25 日

[11] 授权公告号 CN 100473000C

[22] 申请日 2002.12.5 [21] 申请号 02827523.3

[30] 优先权

[32] 2001.12.7 [33] US [31] 60/340,172

[32] 2002.1.17 [33] US [31] 60/350,401

[32] 2002.2.14 [33] US [31] 10/077,651

[32] 2002.2.19 [33] US [31] 60/358,471

[86] 国际申请 PCT/US2002/039208 2002.12.5

[87] 国际公布 WO2003/050995 英 2003.6.19

[85] 进入国家阶段日期 2004.7.26

[73] 专利权人 高通股份有限公司

地址 美国加利福尼亚州

[72] 发明人 Y·里蒙尼 A·R·霍尔克曼

M·格林 N·简恩 A·T·亨特

[56] 参考文献

CN1171026A 1998.1.21

US5915021A 1999.6.22

US5850444A 1998.12.15

审查员 庄 湧

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 陈 炜

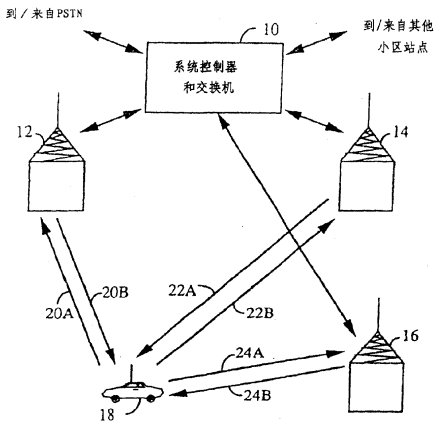
权利要求书 2 页 说明书 13 页 附图 5 页

[54] 发明名称

在混合通信网络中的认证

[57] 摘要

描述了一种方法，认证一移动站从由第一移动交换控制站控制的第一蜂窝通信系统内的第一基站到第二移动交换控站控制下的不同蜂窝系统内的第二基站。 该方法包括包括：对分配给第二蜂窝通信系统的移动站的私有密钥以及第二蜂窝通信系统生成的随机数应用一算法，按结果在第二蜂窝通信系统处生成一认证码。 按对私有密钥和随机数应用一算法的结果在第一蜂窝通信系统处生成一认证码。将在第一蜂窝通信系统处生成的认证码在数据分组内发送到移动站，自此将认证码发送到第二蜂窝通信系统。 将第一蜂窝通信系统处生成的认证码与在第二蜂窝通信系统处生成的认证码比较。



1．在具有从第一基站到第二基站的移动站的系统内的一种认证方法，其中所述第一基站在由第一移动交换控制站控制的第一蜂窝通信系统内，而所述第二基站在由第二移动交换控制站控制的不同的第二蜂窝通信系统内，所述方法包括：

在所述第二蜂窝通信系统生成认证码，作为对分配给所述第二蜂窝通信系统的移动站的私钥和由所述第二蜂窝通信系统生成的随机数应用算法的结果；

在所述第一蜂窝通信系统生成认证码，作为对所述私钥和所述随机数应用算法的结果；

将在所述第一蜂窝通信系统处生成的认证码在数据分组内发送到移动站；

将在所述第一蜂窝通信系统处生成的认证码从所述移动站发送到所述第二蜂窝通信系统；

将在所述第一蜂窝通信系统生成的认证码与在所述第二蜂窝通信系统生成的认证码进行比较。

2．如权利要求 1 所述的方法，其特征在于：

所述第一蜂窝通信系统包括 CDMA 系统；以及

所述数据分组包括 ADDS 消息。

3．如权利要求 1 所述的方法，其特征在于，在不同的数据分组中将认证码发送到所述第二蜂窝通信系统。

4．如权利要求 3 所述的方法，其特征在于，所述第二蜂窝通信系统包括 GSM 系统。

5．如权利要求 1 所述的方法，其特征在于，所述第一蜂窝通信系统包括由第一移动交换控制站控制的第一基站，而所述第二蜂窝通信系统包括由第二移动交换控制站控制的第二基站，所述方法包括：

在移动站测量由所述第一基站发送的信号参数；

在移动站测量由所述第二基站发送的信号参数；

当两种参数到达预定条件时，通过所述第一基站将信号质量消息从移动站发送到所述第一移动交换控制站；

在所述第一移动交换控制站为所述第二移动交换控制站生成用于信道请求消息的信息；

从所述第一移动交换控制站将所述信息发送到所述移动站；

在所述移动站从来自所述第一移动交换控制站的信息生成用于所述第二移动交换控制站的信道请求消息；以及

将所述信道请求消息从所述移动站发送到所述第二移动交换控制站。

6．如权利要求 5 所述的方法，还包括在所述第二移动交换控制站生成标识所述第二蜂窝通信系统内用于所述移动站的信道的信道信息。

7．如权利要求 6 所述的方法，还包括在所述移动站和所标识的信道内的所述第二基站之间建立通信。

8．如权利要求 7 所述的方法，还包括中断所述移动站和所述第一基站之间的通信。

9．如权利要求 5 所述的方法，其特征在于，所述两种参数对应于信号强度。

10．在具有从第一基站到第二基站的移动站的系统内的一种认证装置，其中所述第一基站在由第一移动交换控制站控制的第一蜂窝通信系统内，而所述第二基站在由第二移动交换控制站控制的不同的第二蜂窝通信系统内，所述装置包括：

用于在所述第二蜂窝通信系统生成认证码，作为对分配给上第二蜂窝通信系统的移动站的私钥和由所述第二蜂窝通信系统生成的随机数应用算法的结果的装置；

用于在所述第一蜂窝通信系统生成认证码，作为对所述私钥和所述随机数应用算法的结果的装置；

用于将在所述第一蜂窝通信系统处生成的认证码在数据分组内发送到移动站的装置；

用于将在所述第一蜂窝通信系统处生成的认证码从移动站发送到所述第二蜂窝通信系统的装置；

用于将所述第一蜂窝通信系统处生成的认证码与在所述第二蜂窝通信系统处生成的认证码进行比较的装置。

11．如权利要求 10 所述的装置，其特征在于：

所述第一蜂窝通信系统包括 CDMA 系统；以及

所述数据分组包括 ADDS 消息。

12．如权利要求 10 所述的装置，其特征在于，在不同数据分组中将认证码发送到所述第二蜂窝通信系统。

13．如权利要求 12 所述的装置，其特征在于，所述第二蜂窝通信系统包括 GSM 系统。

在混合通信网络中的认证

相关申请

本申请对于美国临时专利申请序列号 60/340172 有优先权，后者题为“Method and Apparatus for Effecting Handoff Between Different Cellular Communications Systems”，提交于 2001 年 11 月 7 日；且本申请还对代理人号 020045 有优先权，后者题为“Method and Apparatus For Effecting Handoff Between Different Cellular Communications Systems”，提交于 2002 年 2 月 14 日；本申请还对于美国临时专利申请序利号 60/350401 有优先权，后者题为“GSM Authentication,Encryption and Other Feature Support in a CDMA 1x Network Using a GSM-1x MSC”，提交于 2002 年 1 月 17 日。

技术领域

本发明一般涉及在不同蜂窝通信系统内用于认证的方法和装置。

背景技术

所谓的码分多址（CDMA）调制技术是进行有大量系统用户的通信的几种技术之一。虽然其他技术诸如时分多址（TDMA）、频分多址（FDMA）和诸如幅度压缩扩展单边频带的 AM 调制方案可用，但 CDMA 有优于其他这些调制技术的重要优势。在多址通信系统内使用 CDMA 技术在美国专利号 4901307 内有揭示，题为“Spread Spectrum Multiple Access Communication System Using Satellite Or Terrestrial Repeaters”，被转让给本发明的受让人，在此引入作为参考。

在美国专利号 4901307 内，描述了一种多址技术，其中大量移动电话系统用户，每个有一个收发机，使用码分多址（CDMA）扩频通信信号通过卫星中继器或陆地基站（又被称为小区基站或小区站点）通信。使用 CDMA 通信，则频谱可以被重复使用多次，从而能增加系统用户容量。使用 CDMA 技术比起其他多址技术有更高的频谱效率。

在常规的蜂窝电话系统内，可用的频带被分成一般为 30 KHz 带宽的信道，

而使用模拟 FM 调制技术。系统服务区域在地域上被分成不同大小的小区。可用的频率信道被分成集合，每个集合一般包括相等数量的信道。频率集合被分配给小区的方式是为了最小化同信道干扰可能。例如，考虑一个系统，其中有七个频率集合，且小区为等大小的六边形。用于一个小区的频率集合不能在该小区的六个最近或周围邻域内被使用。更进一步，则在一个小区内使用的频率集合不能在该小区的十二个最近的邻域内使用。

在常规的蜂窝系统中，实现的切换方案用于使得呼叫或其他类型的连接（例如数据链路）能在移动站跨越两个小区边界时保持连续。从一个小区到另一小区的切换是在小区基站内处理呼叫或连接的接收机注意到来自移动站的接收到信号强度落到预定阀值以下时开始。较低的信号强度指示意味着移动站可能接近小区边界。当信号电平落到预定阀值之下，则基站要求系统控制器确定相邻基站是否以优于当前基站的信号强度接收移动站信号。

响应当前基站查询的系统控制器用切换请求将消息发送到相邻基站。接近与当前基站邻近的基站使用特定的扫描接收机，它们寻找在特定信道上的来自移动站的信号。如果其中一个相邻基站向系统控制器汇报足够的信号电平，则尝试切换。

切换然后在选择了用于新基站的信道集合的空闲信道时开始。控制消息被发送到移动站，命令它从当前信道切换到新的信道。在相同时刻，系统控制器将呼叫从第一基站切换到第二基站。

在常规系统中，如果到新基站的切换不成功，则呼叫会被中断。切换失败的发生有许多原因。如果在相邻小区内没有可用的空闲信道用于该呼叫通信，则切换会失败。如果另一基站报告听到了从该移动站，而实际上该基站听到的是在完全不同的另一小区内使用相同信道的不同移动站，则切换会失败。该报告差错会使得呼叫被切换到错误的小区，一般是一个信号强度不足以维持通信的小区。另外，如果移动站不能接听到命令以切换信道，切换会失败。实际操作经验表明切换失败发生频繁会导致系统不可靠性。

常规电话系统内的另一经常的问题是当移动站接近两个小区的边界时。在该情况下，信号电平在两个基站处波动。该信号电平波动导致“乒乓”情况，即在两个基站间来回地进行切换呼叫的重复请求。该种附加的不需要的切换请求增加了移动站不正确地接听信道切换命令或完全不能接听到命令的概率。另外，如果不幸地被转到一所有信道都被使用而没有可以接受切换的可用信道的

小区内，则乒乓情况增加了呼叫被中断的概率。

在美国专利号 5101501 内，题为“Method and System For Providing A Soft Handoff In Communications In a CDMA Cellular Telephone System”，被转让给本发明的受让人，并在此引入作参考，揭示了一种方法和系统，用于向在切换时通过多于一个小区基站的移动站提供通信。在该环境中，蜂窝系统内的通信不受从第一基站到第二基站的实际切换而中断，第一基站对应移动站要退出的基站，而第二基站对应移动站要进入的基站。该类型的切换可以被认为是小区基站和移动站间通信的“软”切换，其中两个或多个基站或基站的扇区并发地向移动站发送。使用该种“软”切换技术可以大大减少乒乓情况的发生概率，该情况指在一对基站间进行重复的切换请求。

在美国专利号 5267261 内揭示了改善的软切换技术，题为“Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System”，转让给本发明的受让人，在此引入作为参考。软切换技术通过在移动站处测量系统内每个基站发送的“导频”信号强度而得到改善。这些导频强度测量在软切换过程中通过方便可用基站切换候选而起到辅助作用。

改善的软切换技术要求移动站监控来自相邻基站的导频的信号强度。当测量的信号强度超过给定阀值时，移动站通过基站向系统控制器发送信号强度消息，移动站通过该基站通信。来自系统控制器到新基站和到移动站的命令消息建立新的和当前基站间的临时通信。当移动站检测到对应至少一个基站的导频的信号强度落到预定电平以下时，其中移动站通过该基站通信，移动站通过正进行通信的基站将指示对应基站的测得的信号强度报告给系统控制器。来自系统控制器到经标识的基站和移动站的命令消息中止通过对应基站的通信，而通过其它基站的通信则继续。

虽然以上的技术合适于相同蜂窝系统内的小区间的呼叫转移，但当移动站进入由来自另一蜂窝系统的基站服务的小区时会有更困难的情况。在该种“系统间”切换的复杂因子为相邻蜂窝系统经常有不同的特征。例如，相邻的蜂窝系统经常以不同频率操作，且可能维持基站输出功率或导频强度的不同电平。这些差异有效地防止了移动站实现导频强度的比较及现存的移动辅助软切换技术要考虑的其它类似方面。

当没有资源可供进行软系统间切换时，如果要维持服务不中断，则从一个系统到另一的呼叫或连接的切换定时很关键。即系统间切换必须在最能导致系

统间呼叫或连接成功转移的时刻进行。在该种切换中，这里被称为硬切换，移动站和一个系统间的通信必须在移动站和其它系统间的通信开始前中止。切换只在当例如以下情况下被尝试：

（i） 在新小区内有可用的空闲信道

（ii） 但在移动站失去了与当前基站的联系之前移动站实际上已处在新小区基站范围内，以及

（iii） 移动站所处于的位置保证它能接收到切换信道的命令

理想情况下，每个该种硬系统间切换会以一种方式进行，以最小化不同系统的基站间的潜在的“乒乓”切换请求。然而，现存的切换过程在下述识别失败时使得这更加困难，即要识别何时且通过哪个基站，移动站应被提供新频率和信道信息并被指示转移现存呼叫和连接。

现存系统间切换技术的这些和那些缺点损害了蜂窝通信的质量，且可能会在蜂窝系统进一步扩展时恶化性能。相应地，需要一种系统间切换技术，能可靠地引导不同蜂窝通信系统的基站间的呼叫或连接的切换。

美国专利号 5697055 描述了一种方法和系统，用于实现第一和第二蜂窝系统的基站间的移动站通信的系统间切换，题为“Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System”，被转让给本发明的受让人且在此引入作为参考。在移动站处，测量由第二系统的第二基站发送的信号的可定量化参数。当测量的可定量化参数值超过第一预定水平，则移动站通过第一系统的第一基站将信号质量消息传递给第一移动切换控制站。

信道请求消息然后从第一移动交换控制站传递到第二系统内的第二移动切换控制站。在第二基站处，测量从移动站接收到的信号的可定量化参数。当可定量化的参数的测量值超过预定水平，第二基站建立与移动站的通信。或者，第一基站发送的第一导频信号的信号强度在移动站处被测量。当第一导频信号的测量的信号强度变得少于第二预定水平时，切换请求消息然后被发送到第二基站，从而建立移动站通信。提供移动切换控制站间的语音链路使得能在第一和第二蜂窝系统间转发存在的连接，并使得能进行软系统间切换。

虽然该方式对于两个系统都基于 CDMA 从而两者能实现软切换的情况适用，但仍存在一问题即如何处理一个或多个系统不能实现该种软切换时的系统间切换的问题。例如，所谓的 GSM 标准没有软切换机制。因此，在处理将使用空中接口从 CDMA 网络到 GSM 网络的呼叫切换中存在问题。另外，GSM 认

证不能被完成，因为 CDMA 2000 机制不能传递 GSM 进行认证所需要的数据。GSM 内的加密也不同于 CDMA 2000 内的加密。

一种处理该问题的方式是修改 GSM，使得它能实现到诸如 CDMA 系统的非 GSM 系统的切换。然而，GSM 已经存在很久了，相对而言，操作者不会很情愿耗费巨资以对现存的设备进行修改以适应相邻的不兼容系统。如果在支持双模式移动站的空中接口中加入新的消息，则必须要进行修改以支持这些新消息。很明显，从操作者的角度这是不期望的。

CDMA 系统和 GSM 系统间的切换的另一问题在于 CDMA 和 GSM 认证使用两种不同的方法和密钥。GSM 和 CDMA 1X 内的认证方法基本相同，但密钥大小不同。CDMA 1X 有附加处理，诸如唯一的询间应答和计数方法，这分别防止信道劫持和重播攻击。

发明内容

本发明解决以上问题。

根据本发明的一方面，提供了在具有从第一基站到第二基站的移动站系统内的一种认证方法，其中所述第一基站在由第一移动交换控制站控制的第一蜂窝通信系统内，而所述第二基站在由第二移动交换控制站控制的不同的第二蜂窝通信系统内，所述方法包括：在所述第二蜂窝通信系统生成认证码，作为对分配给所述第二蜂窝通信系统的移动站的私钥和由所述第二蜂窝通信系统生成的随机数应用算法的结果；在所述第一蜂窝通信系统生成认证码，作为对所述私钥和所述随机数应用算法的结果；将在所述第一蜂窝通信系统处生成的认证码在数据分组内发送到移动站；将在所述第一蜂窝通信系统处生成的认证码从所述移动站发送到所述第二蜂窝通信系统；将在所述第一蜂窝通信系统生成的认证码与在所述第二蜂窝通信系统生成的认证码进行比较。

本发明还提供了与该方法对应的装置。

以上本发明的特征在所述的权利要求书内提出，且其优点会随着本发明的示例实施例参考附图的以下详细描述中变得明显。

附图说明

在附图中：

图 1 是蜂窝系统的示意图；

图 2 是两个蜂窝系统间的边界示意表示；

图 3 是双模式移动站的示意图；

图 4 是 GSM 系统内的数据交换的示意表示；以及

图 5 是单模式移动站的示意表示。

具体实施方式

图 1 是示例蜂窝电话系统的示意说明。说明的系统可以使用任何一种多址调制技术以方便大量系统移动站或移动电话和基站间的通信。该种多址通信系统技术包括：时分多址（TDMA）、频分多址（FDMA）、码分多址（CDMA）以及诸如幅度压缩扩展单边频带的 AM 调制方案。CDMA 的扩频调制技术在上述的美国专利号 4901307 内揭示，它有许多优于其它多址通信系统的调制技术的显著优点，因而是较佳的。

在一般 CDMA 系统中，每个基站发送唯一的导频信号，这包括在对应的导频信道上发送“导频载波”。导频信号是在所有时间使用公共伪随机噪声（PN）扩展码由每个基站发送的未经调制的、直接序列、扩频信号。除了提供用于切换确定的相干解调的相位基准和信号强度测量的基准外，导频信号使得移动站能获得初始系统同步，即定时同步。由每个基站发送导频信号

在图 1 示出的系统内，系统控制器和交换机 10 还被称为移动交换中心（MSC），一般包括接口和处理电路（未示出），用于向多个基站 12、14 和 16 提供系统控制。控制器 10 还控制从公共交换电话网络（PSTN）到合适基站的电话呼叫用于传输到合适移动站的路由。控制器 10 还控制通过至少一个基站从移动站到 PSTN 的路由。控制器 10 还引导通过合适基站在移动用户间的直接呼叫，因为该种移动站一般相互间不直接通信。

控制器 10 还通过各种方式诸如专用电话线路、光纤连路或通过微波通信链路耦合到基站。在图 1 内，说明三个该种示例基站 12、14 和 16 以及示例移动站 18，该移动站包括蜂窝电话。箭头 20a 和 20b 定义基站 12 和移动站 18 间可能的通信链路。箭头 22a 和 22b 定义基站 14 和移动站 18 间可能的通信链路。相同地，箭头 24a 和 24b 定义基站 16 和移动站 18 间的可能通信链路。

基站服务区域或小区的地理形状的设计使得移动站一般能最接近一个基站。当移动站处于空闲时，即没有进行呼叫，移动站一直监控来自每个相邻基站的导频信号传输。如图 1 内说明的，导频信号由基站 12、14 和 16 分别在通信链路 20b、

22b 和 24b 上被发送到移动站。移动站然后通过比较从这些特定基站发送的导频信号强度而确定它在哪个小区。

在图 1 说明的示例中，移动站 18 可以被认为最接近基站 16。当移动站 18 开始一呼叫，则控制消息被发送到最近的基站，此处为基站 16。基站 16 在接收到呼叫请求消息时，发送信令到系统控制器 10 并传送该呼叫号码。系统控制器 10 然后通过 PSTN 将呼叫连到目标接收者。

如果在 PSTN 内开始呼叫，则控制器 10 发送呼叫信息到区域内所有的基站。基站接着将寻呼消息发送到目标接收移动站。当移动站接听到寻呼消息，它以发送到最近基站的控制消息进行响应。该控制消息发送信令到系统控制器，即该特定基站在与移动站通信。控制器 10 然后通过最近基站将呼叫路由到移动站。

如果移动站 18 移出初始基站即基站 16 的覆盖区域，则尝试通过将呼叫路由通过另一基站而继续该呼叫。在切换过程中，有不同的开始呼叫的切换或通过另一基站路由的方法。

在基站初始切换的方法中，初始基站即基站 16 注意到移动站 18 发送的信号已经低于一定的阀值电平。基站 16 然后发送切换请求到系统控制器 10，它将请求中继到基站 16 的所有的相邻基站 12、14。控制器发送的请求包括与信道相关的信息，包括移动站 18 使用的 PN 码序列。基站 12 和 14 将接收机调谐到移动站使用的信道，并测量信号强度，这一般使用数字技术。如果基站 12 和 14 接收机报告一个比初始基站报告的信号强度更强的信号，则对该基站进行切换。

或者，移动站本身可以开始所谓的移动站辅助切换。基站每个发送导频信号，这些信号连同其他东西标识基站。移动站配备了搜索接收机，除了实行其他功能外，它用于扫描相邻基站 12 和 14 的导频信号传输。如果发现相邻基站 12 和 14 的一个的导频信号强于给定阀值，则移动站 18 发送该消息到当前基站 16。

移动站和基站间的交互过程允许移动站通过一个或多个基站 12、14 和 16 通信。在该过程中，移动站标识并测量它接收的导频信号的信号强度。该信息通过与移动站通信的基站传递到 MSC。MSC 在接收到该信息时，开始或终止移动站和基站间的连接，从而影响移动站辅助的切换。

以上过程还可以被认为是“软”切换，因为移动站同时通过多于一个基站同时通信。在软切换期间，MSC 在从每个基站接收到的信号间组合或选择，移动单元在不同小区间移动时与这些基站通信。以相同的方式 MSC 可以将来自 PSTN 的信号中继到每个移动单元与之通信的基站。如果移动站正好位于两个或多个基站的覆

盖区域内而不是在同一蜂窝系统内即不为相同的 MSC 所控制，移动站辅助的切换会更复杂。

一种实现在不同系统内的基站间切换的方法参考图 2 描述，这以示意图示出在 CDMA 移动交换中心 MSC 的蜂窝通信网络 30 和 GSM 移动交换中心 MSCg 控制下的 GSM 蜂窝系统，该网络包括 CDMA 蜂窝系统（例如 IS-95 1X）。在图 2 中，说明性地示出五个该种示例基站 B1A 到 B5A，分别位于 CDMA 系统的小区 C1A 到 C5A，且五个基站 B1B 到 B5B 分别位于 GSM 系统的小区 C1B 到 C5B。虽然为了说明方便，小区 C1A 到 C5A 和 C1B 到 C5B 被示出为圆形，但可以理解小区一般设计成其他形状，且实际上其形状取决于它所处的区域的地形和拓扑。在以下说明中，小区 C1A 到 C3A 和 C1B 到 C3B 可以被称为“边界”小区，因为这些小区接近第一和第二蜂窝系统之间的边界。该命名使得每个系统内其余的小区可以被方便地称为“内部”小区。

以下将参考一移动站给出描述，该移动站能接收并对 CDMA 和 GSM 蜂窝系统内的基站来的信号作出反应。然而可以考虑使用任何类型的通信系统，诸如 CDMA 一、CDMA 2000、CDMA 2000 1x、CDMA 2000 3x、高数据速率原理（HDR）、CDMA 1xEV、CDMA 1xEVDO、TDMA、TDSCDMA、W-CDMA、GPRS 以及其他。为了该目的，移动站用带有接收链的双频带收发机经配置，该收发机调到两个蜂窝系统的不同的工作频率。在图 3 的附图内给出该种移动站的示意图。如在此示出的，移动站 40 包括通过天线共用器 44 连接到 CDMA 传输和接收链 46 和 GSM 传输和接收链 48 连接的天线 42。传输/接收链 46、48 对相应的 CDMA 和 GSM 系统是常规的。链输出经合适解调并将数据转换到常规的基带电路 50，并从基带电路 40 接收用于传输的数据。传输/接收链 46、48 由控制器 52 控制，控制器响应于来自 CDMA 和 GSM 系统的命令信号还要在两个链间切换。因此，在本实施例中，两个链不是同时活动的。在另一实施例中，两个链可能同时为活动的。

在另一实施例中，移动站用单个收发机配置，该收发机有可以调谐到两个蜂窝系统之一的一个接收链。图 5 的附图给出该种移动站的示意图。如在此示出的，移动站 53 包括天线 54。天线共用器 55 连到 CDMA 传输和接收链 56（如果它是 CDMA 手机）。否则，移动站 53 连到 GSM 传输和接收链 57。传输/接收链 56、57 对于它们各自的 CDMA 和 GSM 系统是常规的。链输出经合适解调并将数据转换到常规基带电路 58，并从基带电路 58 接收传输数据。传输/接收链或是链 56 或是链 57 由控制器 59 控制。

回到图 2，CDMA 移动交换中心（MSCc）控制从公共交换电话网络（PSTN）到合适基站 B1A 到 B5A 的电话呼叫的路由以传输到指定的移动站。CDMA 移动交换中心 MSCc 还控制从第一蜂窝系统的覆盖区域内的移动站通过至少一个基站到 PSTN 的呼叫路由。GSM 移动交换中心 MSCg 以类似的方式进行操作以控制基站 B1B 到 B5B 的操作，并路由 PSTN 和 GSM 蜂窝系统间的呼叫。控制消息等在系统间数据链路 34 上在 MSCc 和 MSCg 间传递。

当移动站位于 CDMA 系统的内部小区中时，移动站一般经编程以监视从邻近（即内部和/或边界）的基站的导频信号传输。移动站然后通过比较来自周围基站发送的导频信号强度而确定它在哪个内部小区内。当移动站接近内部小区的边界时，可以以例如美国专利号 5267261 内描述的方式开始移动站辅助切换。

当移动站位于边界小区 C1A 到 C3A 或 C1B 到 C3B 的一个之内时，存在不同的情况。作为一例，考虑一种情况，移动站位于小区 C2A 内，但正逼近小区 C2B。在这一情况下，移动站可以开始从基站 B2B 接收可用信号电平，该电平然后可以被报告给基站 B2B 以及移动站当前与之通信的任何其他基站。可用信号电平正被移动站或基站接收的时间可以通过测量接收到信号的一个或多个可定量化的参数（例如信号强度、信噪比、帧擦除率、比特差错率和/或相对时间延时）而确定。该机制类似于上述标识的美国专利号 5697055 内描述的。

如果两个系统均为 CDMA 系统，则美国专利号 5697055 内描述的切换机制可以用于实行小区 C2A 和 C2B 间的切换。然而有一个问题，因为当前没有机制用于使用从 CDMA 网络到 GSM 网路的空中接口进行切换一呼叫的机制。GSM 认证不能完成，因为 CDMA 机制不能传输进行 GSM 认证需要的数据。GSM 内的加密不同于 CDMA 内的加密。如果为了支持双模式移动站，向空中接口加入新消息，则必须进行修改以支持这些新消息。这是不希望的。

该问题的解是使用一通用消息，该通用消息包括使得移动站从 CDMA 网络转移到 GSM 网络的指令。该通用消息必须能传递实现 GSM 认证和加密必要的数据。最好，通用消息还可以支持 GSM 内的其他辅助特征。换而言之，建立的 GSM 协议必须保持不动，以最小化现存 GSM 系统内的任何改变。切换操作的部分包括建立订户身份，且一旦实现了切换，必须维持信令和物理连接的数据机密性（加密）。订户身份认证的定义和操作要求在 GSM 02.09 内给出。

认证过程还用于设定加密密钥。因此，认证过程在网络建立了订户身份后并在信道经加密前实现。两个网络功能为了实现该点是必须的，两个功能即为认证过

程本身以及系统内的认证和加密密钥的管理。

这样，使用任何时候可用的通道机制（在切换情况和非切换情况下），且可以是单向或双向的。一种类型的通道机制是在 CDMA 系统 GSM 参数内进行透明传递的所谓的 ADDS（应用数据传递服务）消息和短数据突发消息，这些参数一般不由 GSM 基站控制器 BSC 检查，而是为双模式移动站需要。与数据突发一起使用 ADDS 消息使得能在网络的移动服务交换中心（MSC）或网络其他元件间发送类有效负荷（诸如 SMS、位置定位服务器、OTASP）。系统利用该点以在网络和移动站之间端到端地传递 GSM 信息，而不需要对 CDMA BSC 或 BTS 有任何改变。

在图 2 示出的网络安排内，用于传递 GSM 切换数据的 ADDS 消息，诸如从 MSC 通过 BSC 到移动站的定时信息和认证数据。移动站然后使用所谓的 MAP（移动应用协议）消息以传递切换数据到 GSM 网络内的 MSCg。这只需要对 MSCg 进行较小的改变，以使得它能解释 MAP 消息内的数据，并相应地控制移动站。当然其他的传输该数据的方法也是可以的。

当移动站在 CDMA 和 GSM 系统的边界时（例如在小区 C2A 内并接近小区 C2B），移动站通过将消息送回 MSCc 而开始切换过程，该消息通知 MSCc 这样的情况，移动应被切换到 GSM 系统。

小区数据库（未示出）可以用作切换过程的一部分。该数据库用于在 GSM 网络上将必要的信息提供给移动站，从而它能实现 CDMA MSC 和 GSM 间的切换，如需要的。

在 GSM 系统内，有两种类型的切换可供使用，即同步的和异步的。为了实现简单，更偏向于异步切换。移动站因此被告知切换对于 GSM 会是异步切换。在移动站接收了切换命令后，移动首先发送几个接入突发数据到 GSM 基站控制器 BSCg，直到它接收回 MAP 切换消息，该消息被送回 CDMA MSC，以使得能生成 GSM 认证数据并被提供给移动站。GSM 有异步切换的过程，数据突发能帮 BSCg 获得移动站的定时。ADDS 消息因此包括'行动时间'消息，指明切换发生的特定时间。只有一旦该数据被接收了，移动站才会开始正常的传输。

CDMA 和 GSM 间切换的另一问题是 CDMA 和 GSM 认证使用两种不同的方法和密钥。GSM 和 CDMA 1X 内的认证方法基本相同，但密钥大小不同。CDMA 1X 有附加的过程，诸如唯一询问应答和计数方法，这相应地防止了信息劫持和重播攻击。对于要在 GSM 系统内使用的 CDMA 物理层，GSM 认证方法可以在 CDMA 物理层上使用而不需要做出重大修改。这提供给了系统不必要支持两种不同类型的

认证中心、两种类型的 SIM 卡的好处。

认证过程包括一系列在系统和移动站间的交换。系统发送不可预测数 RAND 到移动站。下一步，移动站计算结果 SRES，又被称为 RAND 数的签名，使用的算法被称为 A3 算法。A3 算法使用 RAND 和单个订户认证密钥 Ki 以计算 SRES。订户认证密钥 Ki 在用户首次预订服务时被分配，且被存储在 SIM（订户身份模块）卡内以及系统的本地位置寄存器（HLR）内。Ki 是加密中的私有密钥，因此不在网络上被发送。最终，移动站发送签名 SRES 到系统，在此它经有效性测试。

值得注意的是加密密钥的使用和认证过程独立于切换过程。附图的图 4 说明认证如何在 GSM MSC 中实现。GSM 内的认证密钥被称为 Ki，且是 128 比特长。网络生成随机数（RAND），它的长度也是 128 比特。RAND 和 Ki 被输入到 A3 算法，该算法从输入数据计算 32 比特结果（SRES）。RAND 数还在空中消息上被发送到移动站。在 GSM 系统中，每个移动站包括智能卡，即所谓的 SIM（订户身份模块）卡。认证的标准 SIM 命令在 GSM 11.11 内规定。这些命令只在它们不与 GSM 应用的正确功能干扰时才被执行。如果 SIM 在呼叫期间从移动站被移去，则呼叫被立即中止，如 GSM 11.11 定义的。

移动站内的 SIM 还通过对接收到的 RAND 数和本地存储的 Ki 的副本应用 A3 算法。计算的结果同样是 SRES，且应与网络计算的 SRES 相同。结果 SRES 因此由移动站发送到网络，在网络处与网络计算的 SRES 值比较 。如果两个 SRES 值相同，则移动站鉴定为真实的。在图 2 的系统中，RAND 数在空中接口上使用 ADDS 消息被发送，且结果 SRES 被送回。

SRES 的值还被用于称为 A8 的算法中以计算 64 比特加密或加密密钥 Kc。移动站内的 SIM 的 GSM 认证和加密算法应用到 CDMA 物理层，以替代一般使用 CDMA CAVE 算法生成的私有长码掩码。64 比特的 Kc 密钥唯一地映射到 42 比特私有长码上，且因此作为“私有长码掩码”的基础以提供语音保密。私有长码掩码通过 CDMA 消息被传递，且对其的解释与它从 CAVE 算法生成没有不同。使用对语音保密的这一方法使得系统能在混合 CDMA/GSM 网络中保持唯一的认证中心和唯一的 SIM 类型。

GSM 在帧级实现加密。每个帧使用帧号和 64 比特 Kc 密钥进行加密，该密钥如参考图 4 讨论的导出。该帧号和 Kc 掩码对每个帧应用，在 CDMA 1X 系统中，加密使用 42 比特私有长码实现。在图 2 的混合系统中，Kc 密钥用于导出 42 比特私有长码掩码，一映射算法在 Kc 和私有长码间实现映射。该映射在 MSCc 内实现，

MSC 简单地告诉 BSC 使用哪个长码。

ADDS 操作使得能在陆地网络单元（例如 MSC、SMS、PDC）和移动站间进行透明服务传输。该系统使用这一操作传输认证信息 RAND 到 MS 并将 SRES 传输回 MSC。ADDS 消息操作是从 MSCc 到 BSCc，并允许数据在寻呼信道上被发送回移动站。ADDS 传输操作是从 BSCc 到 MSCc，且允许数据从移动站在接入信道上发送到网络。ADDS 传递器操作是从 MSCc 到 BSCc，或 BSCc 到 MSCc，并允许数据在移动站和网络间在话务信道上被发送。ADDS 参数被定义为“ADDS 用户部分”，这包括 6 比特的“数据突发类型”，该 6 比特指明应用数据消息的格式。ADDS 操作使用 ADDS 用户部分参数以包含服务专用数据。认证操作使用 ADDS 用户部分以携带认证数据。描述的系统使用新的数据突发类型，名为“GSM-MAP 认证”，它相应地由移动站解释。

值得注意的是，示例实施例可以在当在接收端存在存储属于认证过程的信息的数据库或该数据库可以在接收端访问时实现。示例实施例的处理器可以被用于与一方实现一加密方案，与另一方实现另一加密方案。示例实施例的基本实现可以不需要到中间资源的物理连接而实现，因为与分开方的通信通过无线媒质而发送。

本领域的技术人员还可以理解，这里揭示的结合这里描述的实施例所描述的各种说明性的逻辑块、模块、电路和算法步骤可以用电子硬件、计算机软件或两者的组合来实现。为清楚地说明硬件和软件的可互换性，各种说明性的组件、方框、模块、电路和步骤一般按照其功能性进行阐述。这些功能性究竟作为硬件或软件来实现取决于整个系统所采用的特定的应用和设计约束。技术人员可以知道在这些情况下硬件和软件的可交换性。作为一例，各种用在此的说明性实施例揭示性的逻辑块、流程图、窗口以及步骤的实现或执行可以在硬件或软件内实现或实行，使用以下列举的以实现在此描述的功能，包括：应用专用集成电路(ASIC)、可编程逻辑器件、离散门或晶体管逻辑、离散硬件组件诸如 FIFO 内的寄存器、执行固件指令集和的处理器、任何常规可编程软件和处理器、现场可编程门阵列(FPGA)或其它可编程逻辑器件或任何以上的组合。通用处理器最好是微处理器，然而或者，处理器可以是任何常规的处理器、控制器、微控制器或状态机。软件模块可以驻留于 RAM 存储器、快闪(flash)存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动盘、CD-ROM、DVD-ROM、寄存器或任意其它的磁性或光存储介质。本领域内的技术人员可以理解信息和信号可能使用各种不同的科技和技术表示。例如，上

述说明中可能涉及的数据、指令、命令、信息、信号、比特、码元和码片最好由电压、电路、电磁波、磁场或其粒子、光场或其粒子、或它们的任意组合来表示。

上述优选实施例的描述使本领域的技术人员能制造或使用本发明。这些实施例的各种修改对于本领域的技术人员来说是显而易见的，这里定义的一般原理可以被应用于其它实施例中而不使用创造能力。因此，本发明并不限于这里示出的实施例，而要符合与这里揭示的原理和新颖特征一致的最宽泛的范围。

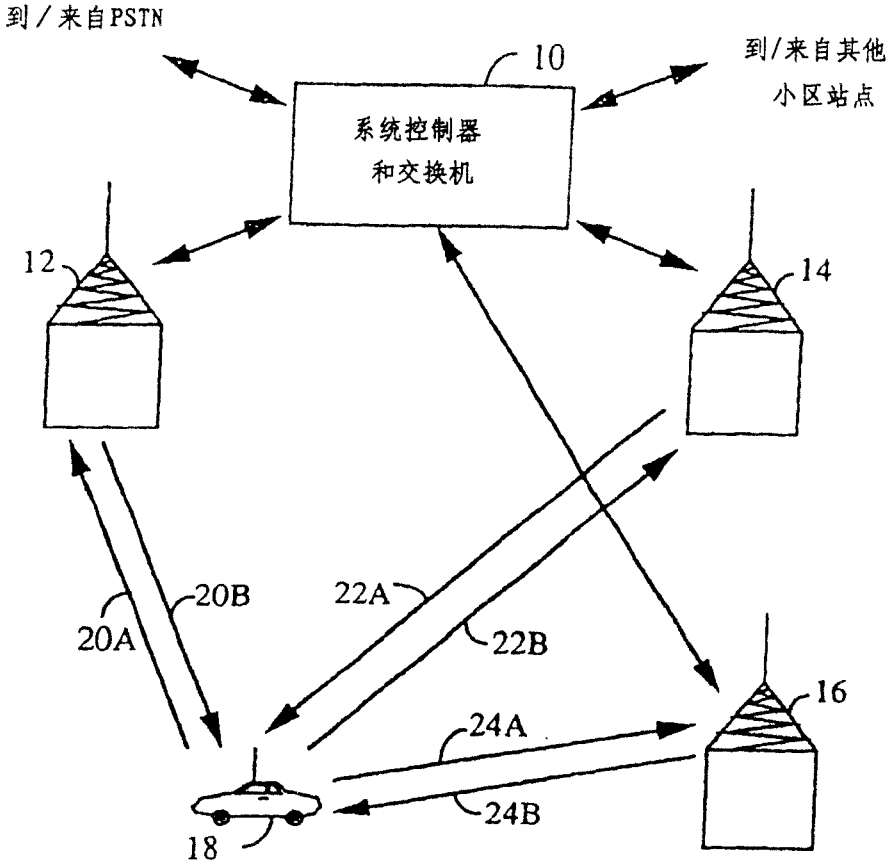

到／来自PSTN
10
到/来自其他
小区站点
系统控制器
和交换机
12
14
20B
20A
22A
22B
16
24A
24B
18

图 1

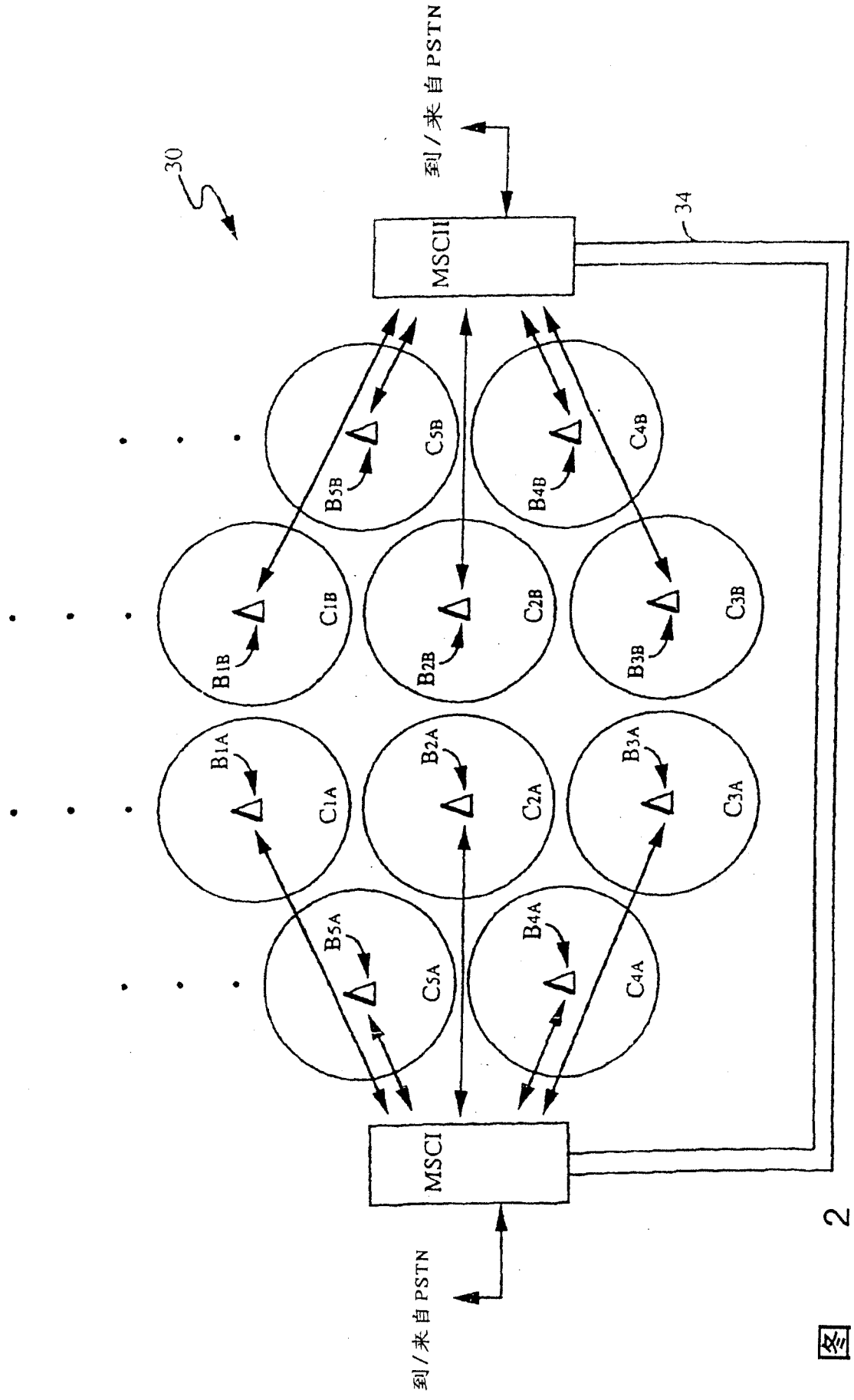

30
到/来自 PSTN
MSCII
34
B5B
C5B
B4B
C4B
B1B
C1B
B2B
C2B
B3B
C3B
B1A
C1A
B2A
C2A
B3A
C3A
B5A
C5A
B4A
C4A
MSCI
到/来自 PSTN

图 2

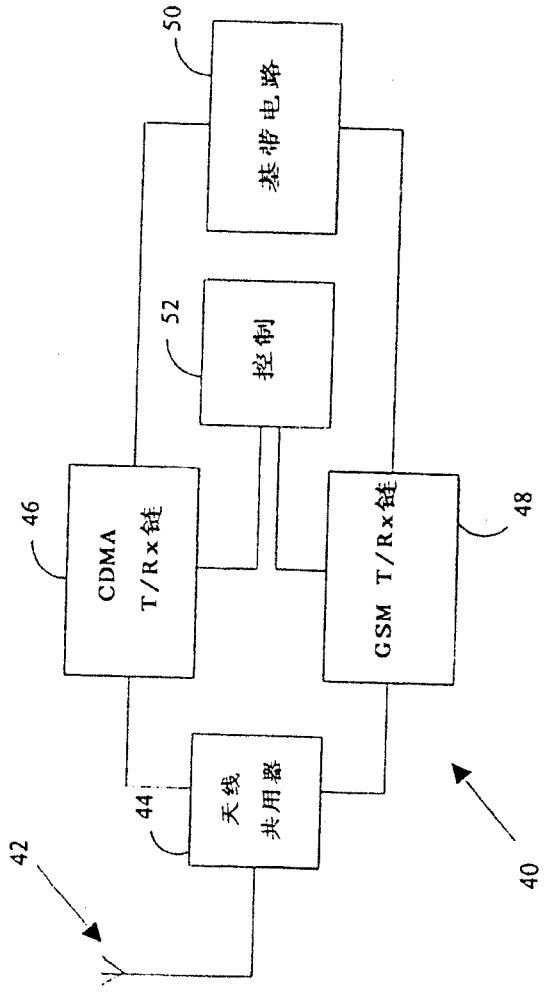


图 3

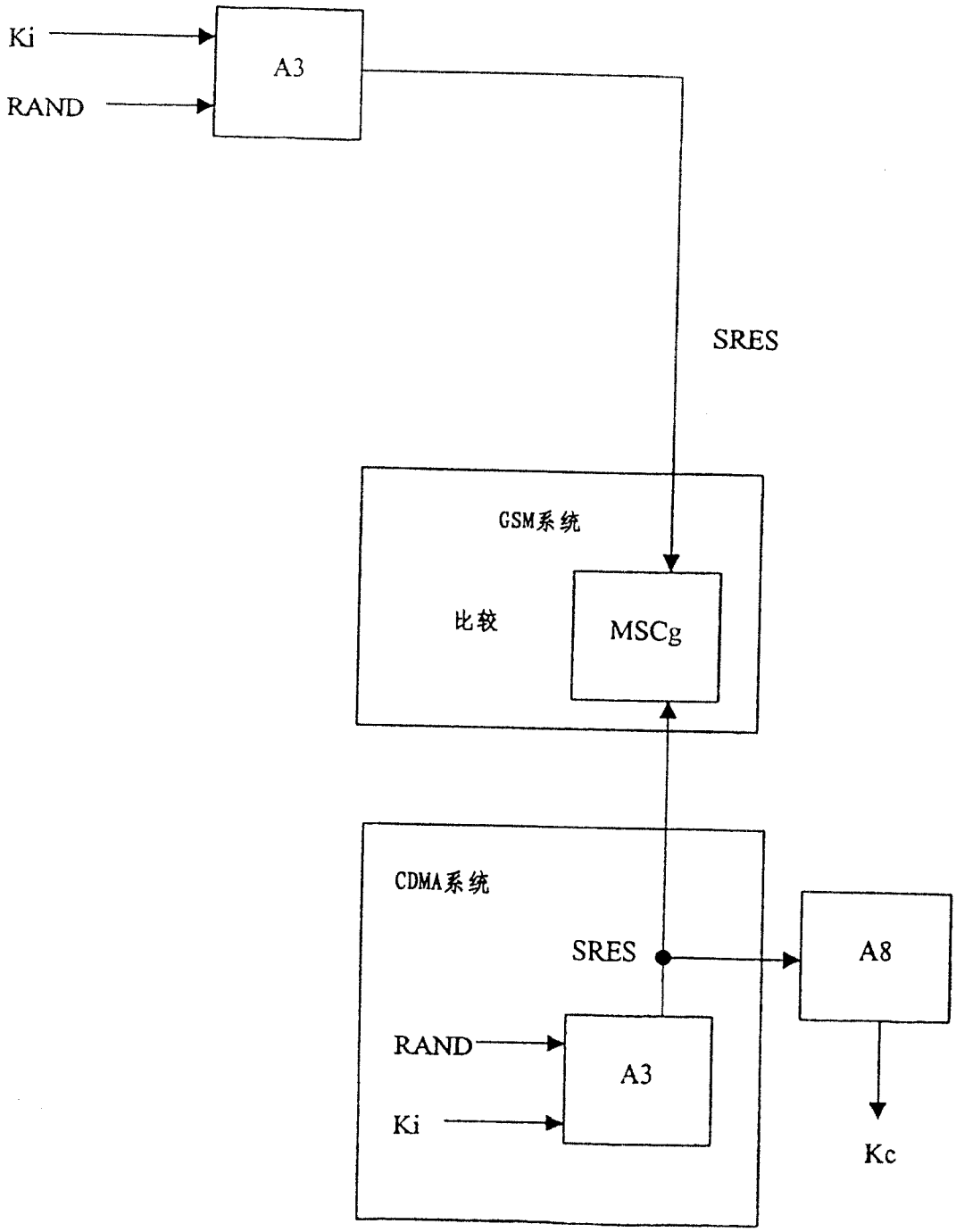


图 4

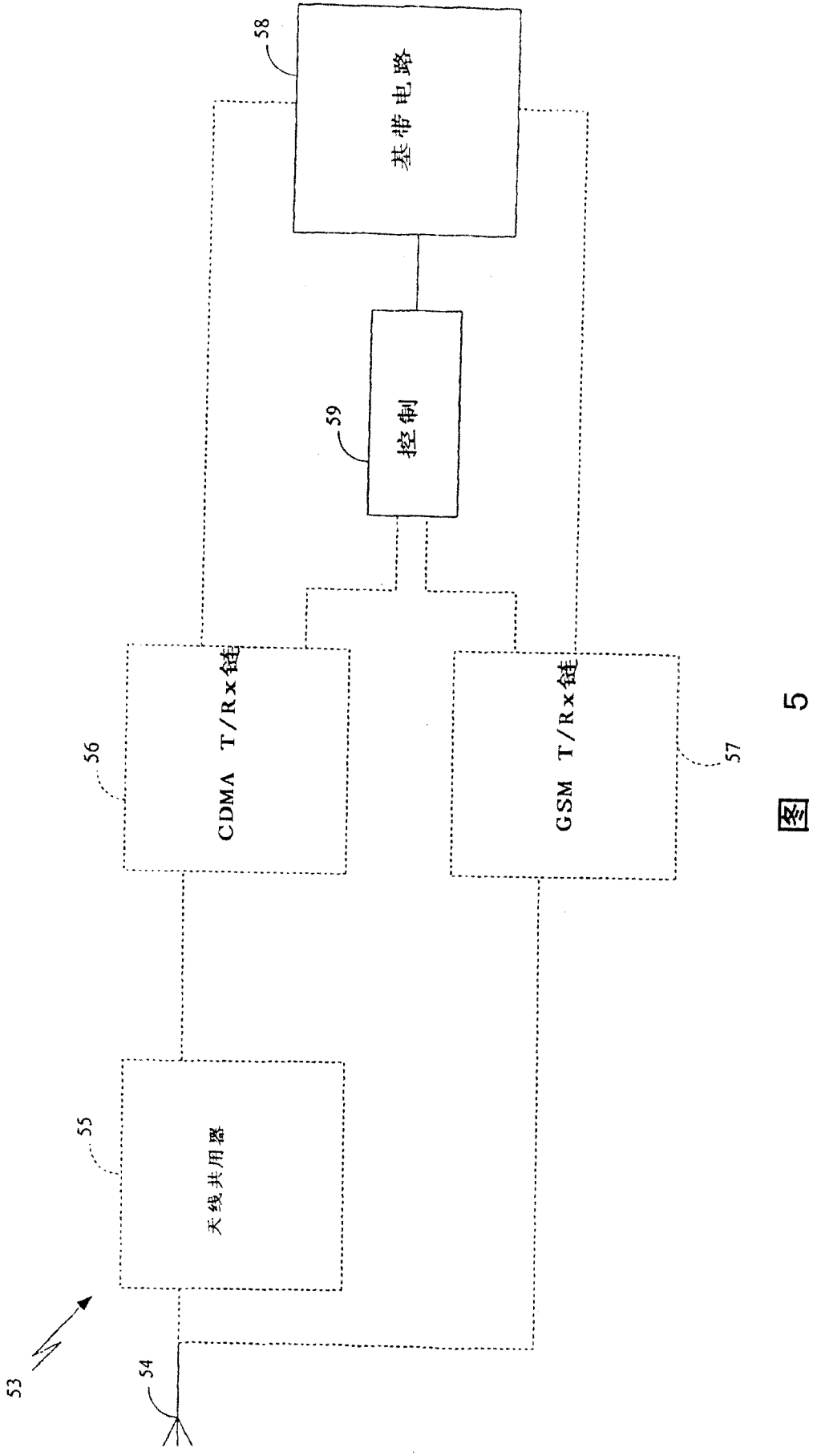


图 5