



## [12] 发明专利申请公开说明书

[21] 申请号 01809910.6

[43] 公开日 2003 年 7 月 16 日

[11] 公开号 CN 1430858A

[22] 申请日 2001.5.18 [21] 申请号 01809910.6

[30] 优先权

[32] 2000.5.23 [33] FR [31] 00/06561

[86] 国际申请 PCT/FR01/01540 2001.5.18

[87] 国际公布 WO01/91501 法 2001.11.29

[85] 进入国家阶段日期 2002.11.22

[71] 申请人 诺泰网络有限公司

地址 加拿大魁北克

[72] 发明人 D·法寇尼耶 C·毛赛特

[74] 专利代理机构 上海专利商标事务所

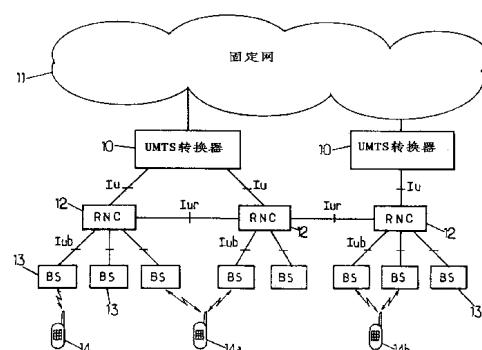
代理人 洪 玲

权利要求书 3 页 说明书 14 页 附图 6 页

[54] 发明名称 控制无线终端与蜂窝无线通信基础设施间的信道的方法

## [57] 摘要

所述基础设施包括核心网、链接至核心网的无线网络控制器及有无线接口且各自链接至一控制器的基站。加密信息通过第一通信路径以电路模式在核心网与终端间发送，经过第一主控制器，然而通过第二通信路径以电路模式在核心网与终端间发送，经过第二主控制器。第二路径建立在包括调整数据从第一主控制器向第二主控制器的传输及抑制第一路径的转移过程中。这些数据表示用来对该信息加密并以有规律的间隔得到递增的一序列号的当前值，还表示该序列号与第二控制器可用的一时间基准间的偏差。



1. 一种控制无线终端(14)与蜂窝无线通信基础设施间的电路模式通信逻辑信道的方法，所述基础设施包括至少一个核心网(30)、链接至核心网包括第一和第二控制器的无线网络控制器(40, 41; 60, 61)及有无线接口且这些接口都链接至一个无线网络控制器的基站(50, 51; 70, 71)，所述方法包括下列步骤：

建立核心网与终端间的至少一个第一通信路径，经过一基站(50; 70)及构成所述第一路径的主控制器的第一控制器(40; 60)；

沿第一通信路径发送有关所述逻辑信道的信息；

建立核心网与终端间的至少一个第二通信路径，经过一基站(51; 71)及构成所述第二路径的主控制器的第二控制器(41, 61)；以及

沿第二通信路径发送有关所述逻辑信道的信息，

其中，沿每个通信路径发送的信息是在从主控制器至无线终端的所述路径的一部分中加密的，加密作为包括一秘密密钥(CK)和与该密钥组合的一加密序列号(CSN)的参数函数来执行，借此主控制器和终端共同以经确定的持续时间的帧的速率递增加密序列号，以便具有同样的加密参数而能对所述信息解密，

并且其中。在包括从第一控制器向第二控制器发送调整数据及抑制每个第一路径的转移过程中建立第二路径，调整数据表示加密序列号的当前值及加密序列号与第二控制器可用的时间基准间的偏差的当前值。

2. 如权利要求 1 所述的方法，其特征在于，第二控制器(41; 61)处理从第一控制器(40; 60)接收的调整数据以把它递增的加密序列号对准由无线终端(14)自主递增的加密序列号。

3. 如权利要求 1 或 2 所述的方法，其特征在于，所述偏差( $\Delta_k$ )是由终端(14)根据从链接至第二控制器(41; 61)的基站接收并携带与所述时间基准相关的信息的无线信号而测量的。

4. 如权利要求 3 所述的方法，其特征在于，所述时间基站包括为一链接至第二控制器(41, 61)的基站维持的帧计数器。

5. 如权利要求 1 至 4 中任一所述的方法，其特征在于，所述转移过程包括：

一阶段，该阶段中，在核心网(30)和无线终端(14)间建立至少一第一附加路径，通过链接至第二控制器的基站(51)并通过除第一控制器外构成主控制器的第二控制器(41)，在该阶段期间至少一些表示所述偏差的调整数据从第一控制器发送至第二控制器；

一宏分集阶段，在该阶段期间同时沿包括所述第一附加路径的至少两个第一通信路径发送有关逻辑信道的信息；以及

一重定位阶段，在该阶段期间表示加密序列号的当前值的调整数据从第一控制器发送至第二控制器，在此之后每个第一路径由未通过第一控制器(40)的第二路径取代。

6. 如权利要求 5 所述的方法，其特征在于，重定位阶段是在抑制每个未通过第二控制器(41)的第一路径的一个阶段之后执行的。

7. 如权利要求 5 或 6 所述的方法，其特征在于，所述调整数据是通过无线网络控制器间提供的一接口而没有通过核心网(30)从第一控制器(40)发送至第二控制器(41)的。

8. 如权利要求 7 所述的方法，其特征在于，同以帧数表示的那样，所述偏差( $\Delta_k$ )用 p 个比特表示所述时间基准(8FN)用 Q 个比特表示，而加密序列号(CSN)用 M 个比特表示，M、P 和 Q 的整数且  $0 < P < Q < M$ 。

9. 如权利要求 8 所述的方法，其特征在于，重定位阶段期间第一控制器(40)在加密序列号(CSN)中的 p 个最低有效位是零的时候发送调整数据。

10. 如权利要求 5 或 6 所述的方法，其特征在于，在建立第 1 附加路径阶段期间发送的调整数据是通过无线网络控制器间提供的接口而没有通过核心网来发送的，而剩余的调整数据是在重定位阶段期间通过核心网(30)传发的。

11. 如权利要求 10 所述的方法，其特征在于，同以帧数表示一样，所述偏差( $\Delta_k$ )和所述时间基准(SFN)用 Q 比特表示，而加密序列号(CSN)用 M 比特表示，M 和 Q 是整数，且  $0 < Q < M$ 。

12. 如权利要求 1 至 4 中的任一所述的方法，其特征在于，第一和第二路径有分别由不同的接入资源支持的无线链路，且所述转移过程包括：

一旦链接至第二控制器的终端在第二路径的基站(71)的无线范围内，则从第一控制器(60)向第二控制器(61)发送调整数据；

同时发送由第一和第二路径的各自的基站(70, 71)加密的相同信息的无线信号的传输阶段；

---

将终端(14)从第一路径的无线链路切换至第二路径的无线链路；以及抑制第一路径，所述终端沿第二路径发送和接收加密的信息。

13. 如权利要求 12 所述的方法，其特征在于，调整数据是通过核心网(30)从第一控制器(60)发送至第二控制器(61)。

14. 如权利要求 13 所述的方法，其特征在于，同以帧数表示的那样，所述偏差( $\Delta_k$ )和所述时间基准(SFN)用 Q 个比特表示，而加密序列号(CSN)用 M 个比特表示，M 和 Q 是整数且  $0 < Q < M$ 。

15. 如权利要求 12 至 14 任一所述的方法，其特征在于，第一和第二路径的无线链路的不同接入资源包括不同的载频。

16. 如权利要求 12 至 15 任一所述的方法，其特征在于，第一和第二控制器(60, 61)属于不同的接入网。

17. 如权利要求 12 至 15 任一所述的方法，其特征在于，第一和第二控制器(60, 61)位于一公共网络结点上，并包括分离的、针对至少一些包括信息加密和解密函数的通信协议的有关第一和第二路径的电路，由此所述电路异步地彼此通信。

18. 蜂窝无线通信系统的接入网包括至少一个无线网络控制器，所述无线网络控制器配置为用来执行如前面的权利要求中的任一权利要求所述的方法。

## 控制无线终端与蜂窝无线通信基础设施间的信道的方法

本发明涉及无线通信领域，尤其涉及蜂窝网中使用的加密技术。

本发明尤其应用于使用码分多址(CDMA)技术的UMTS(通用移动通信系统)类型的第三代蜂窝网。

以下描述用于UMTS网络中的本发明，图1示出UMTS体系结构。

移动业务转换器10属于核心网(N)，它一方面链接至一个或多个固定网11，另一方面又通过所谓的Iu接口链接至控制设备12或RNC(无线网络控制器)。每个RNC12通过所谓的IUb接口链接至一个或多个基站13。基站13分布于网络覆盖的地域中，能通过无线电与称为UE(用户设备)的移动终端14、14a及14b通信。基站可以群分在一起形成称为节点B(nodeB)的节点。一些RNC12还可通过所谓Iur接口彼此通信。RNC与基站形成称之为UTRAN(UMTS陆地无线接入网)的接入网。

UTRAN包括OSI模型的层1和层2的元件以提供无线接口(称为Uu)上所需的链路以及属于层3的用来控制无线资源的一级15A(RRC，无线资源控制)，正如3GPP(第三代合作伙伴项目)于2000年3月发布的《Radio Interface Protocol》3.4.0版的技术规范3GTS 25.301中所述。从较高层看，UTRAN只是用作UE与CN间的中继。

图2示出RRC级15A、15B以及属于UTRAN及UE的较低层的各级。在每一侧，层2再细分为无线链路控制(RLC)级16A、16B及媒体接入控制(MAC)级17A、17B。层1包括编码和多路复用级18A、18B。无线级19A、19B提供来自级18A、18B提供的码元串的无线信号的发送的必要条件及在另一方向上所述信号的接收。

有多种将如图2的协议体系结构适合于图1的UTRAN的硬件体系结构的方法，一般根据信道类型可采用多种结构(见3GPP于2000年1月发布的《UTRAN Overall Description》版本3.1.0的技术规范3GTS 25.401的11.2部分)。RRC、RLC和MAC这三个级位于RNC12中。层1位于，例如，节点B中。然而该层的一部分可位于RNC12中。

当几个RNC参与与UE的通信时，通常有一称之为SRNC的所谓服务RNC

及至少一个称为 DRNC 的漂移 RNC，属于层 2 的模块 (RLC 和 MAC) 位于 SRNC 中，DRNC 链接至一基站，UE 与该基站在一无线链路中。合适的协议提供了这些 RNC 在 Iur 接口上的交换，例如 ATM(异步转移模式)和 AAL2(ATM 适配层 No. 2)。同样的协议亦可用于 Iub 接口上节点 B 与其 RNC 间的交换。

层 1 和层 2 都由 RRC 子层控制，由 3GPP 于 1999 年 10 月发布的《RRC Protocol Specification》版本 3.1.0 的技术规范 3GTS 25.331 描述了 RRC 子层的特点。RRC 级 15A、15B 监控无线接口。而且，与对应于由层 3 产生的用户数据的处理的“用户计划”形成对比的是，它按照“控制计划”处理要发送至远端站的流。

RLC 子层在由 3GPP 于 2000 年 3 月发布的《RLC Protocol Specification》版本 3.2.0 的技术规范 3GTS 25.322 中有描述。在发送方向，RLC 级 16A、16B 根据各自的逻辑信道接收包括由层 3 产生的业务数据单元 (RLC-SDU) 组成的数据流。级 16A、16B 的 RLC 模块与每个逻辑信道相关，这样尤其可把所述流的 RLC-SDU 单元分段成定址到 MAC 子层且包括任选 RLC 信头的协议数据单元 (RLC-PDU)。在接收方向，RLC 模块与之相反地对接收自 MAC 子层的数据单元的逻辑信道的 RLC-SDU 单元进行重新装配。

RLC 级 16A、16B 作为一操作，尤其是作为逻辑信道类型的函数，可有几种操作模式。由此在本描述中，将考虑 RLC 子层的透明模式，该模式适合涉及电路模式通信的逻辑信道。在所述透明模式中，当需要分段与装配操作时，RLC 模块便加以执行，且不向 RLC-POU 单元中引入信头。

MAC 子层在由 3GPP 于 2000 年 3 月发布的《MAC Protocol Specification》版本 3.3.0 的技术规范 3GTS 25.321 中有描述。它向一个或多个发送信道 TrCH 上移置一个或多个逻辑信道。在发送方向，MAC 级 17A、17B 可在一相同的发送信道中多路复用一或更多逻辑信道。在这样的一个发送信道上，MAC 级 17A、17B 递送连续发送块 TrBk，每个 TrBk 由一任选 MAC 信头和产生于相关逻辑信道的一 RLC-PDU 单元构成。

对于每个 TrCH，RRC 子层向 MAC 子层提供一组发送格式 (TFS，“发送格式组”)。发送格式包括等于 10、20、40 或 80 毫秒的传输时间间隔 (TTI)、发送块尺寸、发送块组尺寸以及定义将由层 1 用于 TrCH 中来检测并纠正发送差错的保护方案的参数。根据逻辑信道上或与 TrCH 相关的信道上的当前比特速率，MAC 级 17A、17B 从由 RRC 子层指配的 TFS 选择一发送格式，并且在把

该模式指示给层 1 的同时，在每个 TTI 中递送一组与所选格式相符的发送块。

层 1 可在一给定物理信道上多路复用多个 TrCH。在此情况下，RRC 子层向该物理信道指配一组发送格式组合(TFCS，“发送格式组合组集”), MAC 子层动态地从该 TFCS 集选择一发送格式组合，从而定义将用于多个被多路复用的 TrCH 中的发送格式。

UMTS 使用扩频 CDMA 技术，也就是说，发送的码元与由称为“码片”的样本构成的扩频码相乘，码片的速率(在 UMTS 情况下为 3.84 兆码片/秒)大于所发送的码元的速率。扩频码区分叠加在由一载频构成的同一传输资源上的多个物理信道(PhCH)。扩频码的自相关性和互相关性使接收机能分离 PhCH 并提取经发给它的码元。对于下行链路上 FDD 模式(“频分双工”)的 UMTS，每个基站被分派一个扰码，由互正交信道码(信道化码)区分所述基站使用的各个物理信道。基站亦可使用几个互正交扰码。在上行链路上，基站使用该扰码分离发送的 UE，且可能使用信道码来分离产生于一个和相同 UE 的物理信道。对于每个 PhCH，总扩频码是信道码与扰码的积。扩频因子(等于码片速率与码元速率的比)是 4 和 512 之间的 2 的幂。该因子被选为将在 PhCH 上发送的码元的比特速率的一函数。

在由基站使用的载频上以彼此相随的 10 毫秒帧组织成不同物理信道。每个帧再分成具有 15 个 666 微秒的多个时隙。每个时隙可承载一个或更多个物理信道的叠加形式，包括公共信道和 DPCH(“专用物理信道”)专用信道。每个 DPCH 用这些数据发送产生于 MAC 子层的发送格式组合指示符，使目的地端 MAC 模块能恢复 TrBk 的结构。

对同一通信而言，有可能建立对应于不同信道码的几个 DPCH，它们的扩频因子可以相等或不同。尤其是当一个 DPCH 不足以提供应用所需的传输比特速率时，遭遇到这种情况。而且，该通信可使用一个或更多发送信道。PhCH 上对产生于 TrCH 的信息码元流的编码和多路复用在由 3GPP 于 1999 年 10 月发布的《Multiplexing and Channel Coding (FDD)》版本 3.0.0 的技术规范 3GTS 25.212 中有详细描述。

就 RLC 子层的处理模块以透明模式操作的每个逻辑信道而言，MAC 级 17A、18B 在此之外还满足所发送信息的加密和所接收信息的解密的要求。在对应的发送信道上，涉及该逻辑信道的 TrBk 各自包含根据前述 3GTS 25.301 规范的第 8 章中所描述的机制加密的一 RLC-PDU 单元。

图 3 说明用于逻辑信道的 RNC 的/或 UE 的 MAC 级 17A、17B 的加密模块 20。通过异或操作(门 22)执行加密算法 21 以生成二进制掩码，该掩码与以透明模式从 RLC 接收的 RLC-PDU 单元的信息比特组合。同一模块可用于解密。算法 21 基于下列参数计算所述掩码：

- CK：M=32 位的保密加密密钥，定义于核心网与 UE 间的认证的前阶段；
- CSN：由 M=32 位构成的加密序列号；
- BEARER：逻辑信道标识符，用来生成各个逻辑信道的不同掩码；
- DIRECTION：指示传输方向(上行链路或下行链路)的比特，用来生成这两个方向的不同掩码；
- LENGTH：以比特数表示的掩码的长度，作为发送格式的一个函数由 RRC 级给出。

算法 21 对 M-比特号 CSN 和密钥 CK 进行组合以阻止同一掩码被用来对不同的块加密。号 CSN 以 10 毫秒无线帧的速率递增。图 3 示出提供参数 CSN 的 32 位计数器 23。随着逻辑信道的每个新块，计数器使号 CSN 以量 N 递增，N 是承载该逻辑信道的发送信道上每 TTI 的帧的数目(N=1, 2, 4 或 8)。计数器因此每 10 毫秒递增 1，每 20 毫秒递增 2，每 40 毫秒递增 4 或每 80 毫秒递增 8。一旦初始化加密的通信，RRC 级提供号 CSN 的初始值 CSN<sub>0</sub> 及计数器 23 的开始命令(START)。这些操作在执行 MAC 任务的 RNC 中及 UE 中都得到执行。

本发明考虑的问题是满足加密功能的 MAC 模块在网络基础设施中移位时 CSN 计数器的发送问题。这样的移动发生在含有无线接入资源的变化(切换)的转移过程的相关环境中。该转移过程可引起 SRNC 的改变，从而要求新 SRNC 的 CSN 计数器与前一 SRNC 的(及 UE 的)CSN 计数器同步，而提供给 RNC 用来彼此通信的 Iu 和/或 Iur 接口是异步的。如果同一 RNC 使用不同的电路来管理转移前后所用的接入资源，亦可面对这样的情况：MAC 模块的移动发生于同一 RNC 中。

转移过程的各种可能的情况在由 3GPP 于 1999 年 10 月发布的《Manifestations of Handover and SRNS Relocation》版本 3.0.0 的技术规范 3GTR 25.832 中有描述。一种情况区分了软切换(SHO)与硬切换(HHO)。一方面，SHO 使用宏分集模式并且可能跟有称为“重定位”的 SRNC 变化；另一方面，HHO 对应，例如，载频的变化(有或无 RNC 的变化)和/或对应不能通

过 Iur 接口彼此通信的两 RNC(同一接入网的或不同接入网的)间的切换。如果几个载频分配给 UTRAN 的操作员或如果该 URTAN 的所有 RNC 间未提供 Iur 接口，则在该 UTRAN 内会发生 HHO。HHO 亦可发生于两分离接入网间，例如，在两个 UTRAN 之间或一个 UTRAN 与一个不同类的基于相似的功能体系结构的系统间，该体系结构尤其使使用相同加密过程成为可能，诸如 GERAN 类型的系统(“GSM/EDGE 无线接入网”)。

在 FDD 模式中，UMTS 支持宏分集技术，宏分集技术包括做准备以使 UE 能同时与分离的基站通信：在下行链路中，UE 几次接收同样的信息，而在上行链路中，由 UE 发送的无线信号由基站接收以形成不同的估计值，这些估计值后来组合于 UTRAN 中。

宏分集提供接收增益，接收增益利用对信息的同一项的不同观察的组合改进系统性能。在 UE 移动时，宏分集亦使执行软小区间转移(SHO)成为可能。

在宏分集模式中，来自 UTRAN 或 UE 的多个传输的发送信道的路由选择及这些发送信道在接收中的组合是属于层 1 的选择和组合模块的责任的操作。该模块在与 MAC 子层的接口处，且位于服务所述 UE 的 RNC 中。如果涉及的基站依靠通过 Iur 接口通信的不同的 RNC，这些 RNC 中的一个充当 SRNC 而另一个充当 DRNC。

完成一 SHO 时，UE 与始发基站间的无线链路便断了。可以发生这样：UE 所在的基站范围内的基站没有在 SRNC 的相关性内的。

UTRAN 可很正常地继续以此方式支持通信。然而，这并非最优的，因为通过设法使得 DRNC 成为正在进行的通信的新的 SRNC 而省却出现在 Iur 接口上的交换并释放前一 SRNC 是可能的。这是由在前一 SRNC 的启动时触发的重定位过程的主题(《SRNS Relocation》，见前述 3GTS25.401 规范的 7.2.3.2 部分)。

该重定位过程包括从前一 SRNC 至前一 DRNC 的 RLC 和 MAC 实例的转移(以及如果保持宏分集则还有层 1 的选择和重组模块)转移。

由此产生的一个问题由加密算所用的 CSN 计数器以透明 RLC 方式的转移。尤其是，该计数器须与置于 UE 侧的 MAC 层中的计数器保持同步，而 RNC 间的链路(通过 Iu 接口及核心网或通过 IUr 接口)原则上是异步的。

32 位数 CSN 可分解为对应 P 个 CSN 的最低有效位(LSB)的连接帧数 CFN 及对应 32-p 个最高有效位(MSB)的超帧数 HFN(根据所述 3GTS 25.301 规范的第

8 章 P=8)。

监控每个由基站 13 服务的小区的 RNC 为该小区更新系统帧号 SFN, SFN 在 Q=12 个比特上编码并随每个新的 10 毫秒无线帧递增。所述号 SFN 由基站通过其公共控制信道广播。

UE 测量它从它的当前小区的相邻小区接收的信号与其自己的时钟间的时间偏差。在触发向目标小区的 SHO 之前, UE 向其 SRNC 提供它测量的该目标小区的偏差, 该偏差在  $2^P \times 10$  毫秒(即, 2.56 秒)的范围内对应在公共信道上获得的目标小区的 SFN 计数器与其自己的 CFN 计数器间的偏差。该偏差是根据检测同步模式以例如码元时间的数量级, 实际上小于 10 毫秒的时间精确度的。它用来时间上箝制新基站的发送, 这样在宏分集模式中, 由 UE 从多个站接收的信息项彼此不是太偏差, 这会要求过量的存储器以能组合观察。该偏差是通过 Iur 接口定址到新基站的。

由于该偏差的提供, 所以 DRNC 先验知道将用来加密解密的 CSN 计数器的 P 个最低有效位。然而, 这不提供最高有效位(HFN)。当前 3GPP 规范支持重定位过程包括由 SRNC 通过 Iu 接口发送消息“Relocation\_Required”, 在该消息插入 HFN 号, 这样 DRNC 能与它的加密序列计数器同步。一接收该消息, 核心网便执行将导致通信路由选择至 DRNC 的任务, 并向后者透明地重新发送 HFN。

这些安排不解决上述问题, 因为在 SRNC 发送 HFN 的值的时刻与 DRNC 接收它的时刻间, 已能使 UE 侧有效的 HFC 递增。每当 HFN 花不止 2.56 秒才能由 DRNC 接收就会出现这种情况。给定由异步核心网中的消息可遇到队列及由交换器 10 处理“Relocation\_Required”消息的时间情况下, 这难以有把握地避免。如果 HFN 花较少时间到达 DRNC 亦可出现差错: 例如, 如果是在 CFN 等于 255 时发送 HFN, 在 HFN 的值于 UE 处递增后它很可能由 DRNC 接收。

在不使用宏分集模式执行的 HHO 中更剧烈地遭遇以上问题。

在 HHO 中, 通常有一对广播阶段, 在此广播阶段期间在两个接入资源上同时发送同一下行链路信号项。这使 UE 一切换至第二接入资源便能无中断地接收发给它的信息。因此, 当要执行 HHO 时, 负责目标小区的 RNC 必须快速知道涉及 UE 的加密序列计数器 CSN。而且, 目标小区的 RNC 如果不同于先前的 SRNC 则一般预先不知道 CFN 计数器, 因为没有宏分集。由先前 SRNC 发送的值因此必须尽可能大地覆盖 CSN 的最低有效位的范围, 这样, 考虑到通过

异步网的路由选择时间，当它由目标小区的 RNC 接收时，它很可能过时。此缺陷在缺乏基站的同步时难以消除，这种同步对 UMTS 网络的操作不是必要的且不被标准所使用。

应注意的是，在 RLC 子层的非透明模式中，上面考虑的问题不存在。这些非透明模式是用于分组传输的，对分组传输而言切换期间或重定位过程期间短时中继传输通常没有损害，只要保证，例如通过确认机制，接收到正确的计数器值。而且，RLC 子层通过使用每个 RLC-PDU 单元的信头的序列号对含于该 RLC-PDU 单元中的数据加密来满足非透明模式的加密/解密功能的要求。该序列号是未经加密发送的，这样不必在两端对加密计数器进行同步。

在使用时分多址(TDMA)技术的第二代 GSM 系统(“全球移动通信系统”)中，加密只在空中接口上有效。密钥的递增是基于与 TDMA 超帧的同步，这种同步是在时分多路复用方案的帧结构中的无线链路的两侧上以非歧义的方式实现的。因此，以上问题亦不存在。

WO 98/09458 揭示一从 GSM 衍生的无线接入系统，该系统中只在空中接口上执行对通信的加密。该系统的一个限制是它要求基站在 TDMA 多帧的标度上的同步。而且，当基站间的交换所花时间多于多帧的相对短的持续时间(120 毫秒)时，加密计数器的同步便丢失。

本发明的一个目的是提供一种针对上述同步加密计数器问题的解决方案。

因而，本发明提供一种控制无线终端与蜂窝无线通信基础设施间的电路模式通信逻辑信道的方法。所述基础设施包括至少一核心网、链接至核心网并包括第一和第二控制器的无线网络控制器以及提供有无线接口且各个链接至一无线网络控制器的基站。该方法包括以下步骤：

- 在核心网与终端间建立至少一个第一通信路径，通过一基站并通过构成所述第一路径的主控制器的第一控制器；
- 沿第一通信路径发送逻辑信道的信息；
- 在核心网与终端间建立至少一个第二通信路径，通过一基站并通过构成所述第二路径的主控制器的第二控制器；
- 沿第二通信路径发送逻辑信道的信息。

沿每个通信路径发送的信息以从主控制器至无线终端的所述路径的一部分中加密。加密作为包括秘密密钥和与所述密钥结合的加密序列号的参数的

函数而被执行。主控制器与终端共同以具有确定持续时间的帧的速率递增加密序列号，以有相同的加密参数来允许解密信息。第二路径建立于转换过程中，该转换过程包括从第一控制器向第二控制器发送调整数据并抑制每个第一路径。所述调整数据表示加密序列号的及加密序列号与第二控制器可用的时间基准的偏差的当前值。

这使无线终端中加密序列号的递增保持连续性成为可能。第二控制器处理从第一控制器接收的调整数据以把它增加的加密序列号与由无线终端自主增加的加密序列号对准。因此，转换过程的执行对终端的 MAC 层可以是透明的。

加密序列号与第二控制器可用的时间基准间的偏差较佳地由终端根据无线信号测量，所述无线信号是从链接至第二控制器并携带涉及所述时间基准的信息的基站接收的。该时间基准有益地对应于为链接至第二控制器的一基站而保持的一帧计数器。

在 SH0 之后的重定位过程的情况下，该偏差已至少部分地提供给在建立通过一链接至该第二控制器的基站的一个新的通信路径的过程中的第二控制器。这样，在本方法的一实施例中，转换过程包括：

—— 一阶段，该阶段是在核心网与无线终端间建立至少一第一附加路径，通过一链接至第二控制器的基站并通过构成主控制器的第一控制器外还通过第二控制器，在此阶段至少一些表示所述偏差的调整数据从第一控制器发送至第二控制器；

—— 一宏分集阶段，在此阶段逻辑信道的信息同时沿包括所述第一附加路径的至少两个第一通信路径发送；以及

—— 一重定位阶段，在此阶段表示加密序列号的当前值的调整数据从第一控制器发送至第二控制器，在此之后每个第一路径由未通过第一控制器的第二路径取代。

为简化该过程，重定位阶段通常在抑制每个未通过第二控制器的第一路径的阶段之后执行。

当有宏分集阶段时，调整数据有益地通过一无线网络控制器间的接口而不通过核心网从第一控制器发送至第二控制器。这避免了需由核心网的转换器处理发送偏差数据的消息，从而使调整数据的传输持续时间最短，进而使它们迟到第二控制器的风险最小。

可选地，在建立第一附加路径阶段发送的调整数据可通过无线网络控制器间的接口而不通过核心网发送，而剩余的调整数据在重定位阶段通过核心网发送。尤其是当用比特数表示的偏差大于执行 SHO 所需的偏差时推荐这样做。通过核心网发送的调整数据的过时风险得以降低，因为这些数据只要不以大于偏差值的一个循环的时延到达第二控制器便有效。

在本方法的另一实施例中，第一和第二路径有分别由不同的接入资源，例如不同的载频(HHO 情况)，支持的无线链路。转移过程可以包括：

——一旦链接至第二控制器的终端在第二路径的基站的无线范围内，则从第一控制器向第二控制器发送调整数据；

——同时发送由第一和第二路径的各自的基站加密的相同信息的无线信号的传输阶段；

——将终端从第一路径的无线链路切换至第二路径的无线链路；以及

——抑制第一路径，终端沿第二路径发送和接收加密的信息。

在此情况中，调整数据通常通过核心网从第一控制器发送至第二控制器。

本发明的另一方面涉及包括至少一个安置为用来实现以上定义的方法的无线网络控制器的蜂窝无线通信系统的接入网。

下面参照附图对非限制性示例实施例的描述将使本发明的其他特点和优点变得明显，其中：

图 1 是 UMTS 网络的框图，此前对其作过评述；

图 2 是示出 UMTS 网络的无线接口所用的通信协议的分层构造的图，先前对其作过评述；

图 3 是用于 UMTS 网络的 MAC 层中的加密模块的示意图，先前对其作过评述；

图 4 是可使用本发明的 UMTS 网络的简图；

图 5 至图 8 是示出在各个通信实例中有效的链路的图 4 的网络的图；

图 9 和图 10 是分别由源 RNC 和目标 RNC 执行的重定位过程的步骤的流程图；

图 11 是本发明可用于其中的另一 UMTS 网络的简图；

图 12 至图 14 是示出在各个通信实例中有效的链路的图 11 的网络的图。

图 4 示出用来支持几个 SRNS 间的宏分集模式的 UMTS 网络基础设施。所给基础设施有一有意简化的配置以使本发明的说明明晰。核心网包括用于电

路模式的移动业务交换器(MSC, “移动业务交换中心”)30, 通过 Iu 接口链接至各有 RNC40 和 RNC41 的两无线网络子系统(SRNS)。两个 RNC40 和 41 通过 IUr 接口彼此通信并通过 IUb 接口分别监视基站 50 和 51(节点 B)。

图 5 至图 8 示出 UE14 移动时 UE14 与核心网间的有效通信路径。在图 5 的情况下, 第一路经已在 MSC 30 和 UE14 间通过充当 SRNC 40 和基站 50 以惯常方式建立。SRNC 40 和 UE 各有一 MAC 实例, 该 MAC 实例针对每个电路模式的专用逻辑信道和每个通信方向以参照图 3 所示的方式提供了在该第一路径上发送的信息的加宽和解密功能。模块 20 的静态参数(CK、BEARER、DIRECTION 和 LENGTH)及计数器 23 的初始化参数已由 RRC 级提供。

在图 6 的情况下, 另一路经已以宏分集模式通过 RNC 40、充当 DRNC 的 RNC41 及基站 51 在 MSC 30 和 UE 14 间建立。在建立这种其它路径前, UE14 已测量其自己的加密序列号 CSN 与由基站 51 在它的下行链路公共信道上广播的帧号 SFN 间的时间偏差 $\Delta$ 。该偏差 $\Delta$ 是以比 10 毫秒帧的分辨率更精细的分辨率测量的。其值由 UE 提交给 SRNC10 (RRC 层)且 SRNC40 在宏分集建立过程中通过 Iur 接口把它发送至 DRNC41, 这样, 基站 51 有一关于 UE14 的在码元时间数量级的标度上对准基站 50 的传输的传输。、

在这些规范的当前状态中, UE 的 RRC 层向其 SRNC 的 RRC 层发送 $\Delta$ 模的值  $2^P \times 10$  毫秒 = 2.56 秒。我们用  $\Delta_k = (\text{CSN} - \text{SFN}) \bmod 2^k$  表示由以 10 毫秒为单位表达的偏差 $\Delta$ 的整数部分的 k 个最低有效位表示的数 ( $1 \leq k \leq Q$ )。CSN 取 M=32 位而 SFN 取 Q=12 位时, 则 UE 测量  $\Delta_0 = \Delta_{12}$ 。然而, 它只通知 UTRAN 关于  $\Delta_p = \Delta_8$ 。

在图 6 的情况下, 逻辑信道是在两路经中的每一个上由置于 SRNC 40 的和 UE14 的 MAC 子层中的相同加密/解密模块加密的。一个选择组合模块已在层 1 中创建, 一方面在 SRNC 40 中, 另一方面在 UE 14 中。

在图 7 的情况下, 通过基站 50 的路经已得到抑制, 无线链路的质量不再是相当好。尽管 RNC40 不再有任何基站在与 UE 的无线链接中, RNC 40 仍充当 SRNC。相反地, 另一路经得到保持(当然, 仍会有以宏分集模式通过 DRNC 41 的其他路经; 而且, 先通过 DRNC 41 建立的路经可能已得到抑制。)

规范规定, 在这样的情况下, SRNC 40 可请求重定位, 这就导致图 8 所示的情况: 先前 DRNC 41 成为 MSC 30 向其转换通信的新的 SRNC。请求是在“Relocation Required”消息中进行的, 该消息是通过 Iu 接口发送至 MSC 的且含有预期从源 RNC 40 的 RRC 层透明的发送至目标 RNC 41 的 RRC 层的一

字段。根据当前规范，该字段含有当前 HFN，也就是说，由 RNC 40 和 UE 14 使用的加密序列号 CSN 的 M-P=24 最高有效位。核心网处理“Relocation\_Required”消息并将 HFN 值以透明方式发送至 RNC41，RNC41 能够用从目标小区的 SFN 计数器及先前接收的偏差 $\Delta_8$ 推断的 CFN 的当前值 ( $CFN = (SFN + \Delta_8) \bmod 2^8$ ) 补充它。这样补充的号 CSN 可由用于该逻辑信道的创建于 RNC41 中的新的 MAC 实例使用。然而，如果 HFN 在 RNC 40 与 41 之间的过渡期间 HFN 在 UE 级上已被修改，该 CSN 是出错的。

为避免这些错误，RNC 40 和 41 可运用能在 RRC 层中执行的图 9 和图 10 的重定位过程。

一旦已决定重定位(图 9 的步骤 100)，源 RNC 40 记录加密序列号 CSN 的当前值(CSNE)(步骤 101)并把它在一消息中发送至目标 RNC 41，该消息还可含有 $\Delta_k$ ( $k \leq Q$ )个比特中的全部或一些(步骤 102)，之后等待对该消息的确认(步骤 103)。

如果  $k \leq P$ ，则消息不必包括 $\Delta_k$ ，因为 RNC 41 已知 $\Delta_p$ 。

如果  $p < k \leq Q$ ，我们可把 $\Delta_k$ 包括进来或只包括它的  $k-p$  个最高有效位。这可通过修改由 UE 在 RRC 连接上向 SRNC 发送的测量报告，从而使报告包括 $\Delta_k$ ( $\Delta_k$  得到测量)而不仅仅是 $\Delta_p$ 来实现。

当目标 RNC 41 接收该消息(图 10 的步骤 110)时，便在步骤 111 中读取其中的值 CSNE 并在合适的时候读取偏差 $\Delta_k$ 的信息，然后在步骤 112 中根据以下计算两个帧指数  $TE_k$  和  $TR_k$ :

$$TE_k = (CSNE + \delta) \bmod 2^k$$

$$Tk_k = (SFN + \Delta_k) \bmod 2^k$$

其中，SFN 在目标小区的帧计数器的当前值，对应于该值的帧，将以值  $CSN_0$  初始化 RNC 41 的计数器 23。指数  $TE_k$  表示，在相对于 CSN 的倒计算数由 UE 定位的  $2^k$  个帧的循环中，预计消息开始在目标 RNC 处的时刻。正的或 0 整数  $\delta$  表示以 10 毫秒为单位的消息的路由选择的最小持续时间。如果没有有关该最小持续时间的先验的信息，我们取  $\delta=0$ 。指数  $TR_k$  表示，在同一循环中，UE 级的号 CSN 的  $k$  个最低有效位的当前值。向  $CSN_0$  的  $k$  个最低有效位指配  $TR_k$  是在步骤 113 中进行的，在步骤 113 中 CSNE 的  $M-k$  个最高有效位进一步指配给  $CSN_0$  的  $M-k$  个最高有效位。

如果指数  $TR_k$  小于指数  $TE_k$ (步骤 114)，则在消息的路由选择期间由 UE 保

持的 CSN 计数器的  $k$  个最低有效位中已存在溢出，这样必须更新最高有效位。为做到这一点，在步骤 115 中以模  $2^m$  递增  $2^k$  初始值  $CSN_0$ 。如果在步骤 114 中  $TR_k \geq TE_k$ ，则在步骤 113 中获得的初始化值  $CSN_0$  是正确的。

目标 RNC41 则可为正在进行的通信启动 MAC 实例，尤其是加密模块 20 及其相关计数器 23(步骤 116)。如果在目标 SRNS 中 UE 处于宏分集模式，目标 RNC 41 亦创建一个选择和组合模块。它随后向源 RNC 40 返回确认(步骤 117)以表示已完成重定位。

一接到该确认，源 RNC 便抑制它的涉及 UE14 的 MAC 实例，并且在适当的时候抑制它的选择/组合模块(步骤 104)。如果在规定时标内未收到确认，它可重复图 9 的过程或取消重定位请求。

只要用来从源 RNC 向目标 RNC 发送消息的时标不超过  $(2^k + \delta) \times 10$  毫秒，图 9 和图 10 的过程便正确地使目标 RNC 中的加密过程对准于 UE 中执行的加密过程。

该条件易于满足。例如取  $k=Q=12$  是可能的，这使得时标可多至至少 40 秒。为做到这一点，发送至准备宏分集的 DRNC 的偏差可拓宽至  $Q$  比特。可选地，向值 CSNE 提供丢失的  $Q-P$  个最高有效位是可能的。这样，图 9 和图 10 的消息可是通过核心网发送的“Relocation\_Required”消息、值 CSNE，并可能是置于以透明方式发送至目标 RNC 的 RRC 层的字段中的  $\Delta_0$  的  $Q-P$  个最高有效位。

通过 Iur 接口发送图 9 和图 10 的消息亦是可能的。该接口亦是异步的，但通常允许较短的路由选择时间，因为核心网不必处理这些消息。在此情况下，我们能够允许自己降低号  $k$ ，例如按  $k=p=8$ ，从而无需修改由 UE 发送回来的报告消息。

在有关 HHO 的关联环境中执行重定位的情况下，图 9 和图 10 的过程亦是可取的。这可出现于图 11 的图解配置中，除了在所涉及的两 RNC 60 和 61 之间没有 Iur 接口外。图 11 的图解配置类似于图 4 的图解配置。要注意的是，可以有一个这样的 Iur 接口，但不用于切换，例如因为后者在两不同的载频间。在另一实施例中，RNC 60 和 61 属于不同的接入网(例如 UTRAN 和 GERAN)。

HHO 的典型情况由图 12 和图 14 在图 11 的网络配置中进行说明。起初(图 12)，以惯常的方式在核心网的 MSC 30 与 UE14 间通过源 RNC60 和与之相关的基站 70 建立一个路径。UE 在其相邻小区的公共信道尤其是链接至图 12 所示

情况中的 RNC 61 的基站 71 的信道上执行规定的测量。当这些测量的分析显示向基站 71 的 HHO 是需要的时，SRNC 60 向其 MSC30 发送一条指定目标 RNC 61 的 HHO 请求消息（“Handover\_Prepares”）。

在触发切换时建立第二路径，始于下行链路（图 13）。逻辑信道的同一信息从 MSC 30（或几个 MSC）发送两次，通过 RNC60 及基站 70 发送一次，通过 RNC61 及基站 71 发送一次。在上行链路中，终端 14 保存第一路径的物理信道的参数直到它收到一要它切换至另一基站 71 的“Handover\_Command”消息。一收到该消息，UE14 便执行命令，一旦经同步的网络完成第二路径的建立便这样做。然后抑制第一路径（图 14）。

在图 13 所示的情况下，下行链路信息是在 RNC 与 UE 间的两路径上加密的。目标 RNC 61 的 MAC 实例已用一由图 9 和图 10 的过程提供的初始值  $CSN_0$  启动它的计数器 23。值  $CSNE$  和  $\Delta_k$  可由源 RNC 60 包括在“Handover\_Prepares”消息中并由核心网发送至目标 RNC 61。因此，UE 已测量  $\Delta_k$  并把它报告给其 SRNC 是必要的。我们将较佳地取  $k=Q=12$ 。

一转换至基站 71，UE 无需修改地使它的 CSN 号得到同步。它因此能立即接收下行链路信息并发送有正确的加密的上行链路消息。一旦基站 61 已获得同步，则完成第二路径。

在某些情况下，UD 在向目标 RNC 执行有载波改变的 HHO 之前可以已有在第一载频上源 RNC 与目标 RNC 间的微分集阶段。在这种情况下，目标 RNC 已有偏差  $\Delta_k$  或  $\Delta_p$ ，这样在 HHO 时重复它不是强制性的。

亦可发生另一 UE 已有源 RNC(SRNC) 与目标 RNC(DRNC) 间的宏分集阶段。当对 UE14 的 HHO 过程开始时，源 RNC60 无需从 UE14 接收偏差  $\Delta_k$  就能确定偏差  $\Delta_k$  的相关值：源 RNC 60 从两 UE 的 CFN 及由另一 UE 测量和显示的偏差推断该值。

应注意的是，根据本发明的一可选实施例，参照图 11 至图 14 以上述方式操作的控制器 60 和 61 可以是置于网络的给定结点的设备项的两个分离部件。该设备项可以是 UMTS 体系结构中的 RNC 类型的，且这两分离部件可以是分开的管理关于至少 MAC 层的两路径的电路，这些路径以异步方式彼此通信。这些电路例如由两不同的卡承载或装在 RNC 的两不同的机箱中。

还要注意的是，图 9 和图 10 的过程可采用各种等价形式。这样，发送给目标 RNC 的消息可含有使目标 RNC 能恢复这些参数的任一组合，而不是明显

地含有 CSNE 和  $\Delta_k$ 。

例如，在目标 RNC 已提供了偏差  $\Delta_p$  的 SH0 之后的重定位中，发送给目标 RNC 的消息可含有 HFN 的当前值 HFNE 及由目标小区的当前 SFN 的 k 个最低有效位表示的号  $SFNE_k (P < k \leq Q)$  亦即  $SFNE_k = (CSNE - \Delta_k) \bmod 2^k$ 。目标 RNC 则能如先前一样用  $\Delta_k = (HFNE \times 2^p - SFNE_k + \Delta_p) \bmod 2^k$  及  $CSNE = (HFNE \times 2^p + \Delta_p) \bmod 2^m$  操作。

在另一实施例中，尤其在 HHO 情况下可取的是，发送给目标 RNC 的消息含有 CSN 的当前值 CSNE 及前述的号  $SFNE_k (P < k \leq Q)$ 。目标 RNC 可以与用  $\Delta_k = (CSNE - SFNE_k) \bmod 2^k$  相同的方式操作。

而且，第二 RNC 41 或 61 可用的时间基准，相对于偏差  $\Delta_k$  或任一表示该偏差的有关量，可以与目标小区的 SFN 不同例如：

——链接至目标 RNC 的另一基站的 SFN，其公共控制信道已由 UE (或由由源 RNC 监控的另一 UE) 检测，从而允许这一其它站的偏差  $\Delta_k$  的测量。由于目标 RNC 知道它监控的基站的 SFN 间的区别，它因而能够恢复  $\Delta_k$  的正确值；

——任一基站的 SFN，尤其是源小区的 SFN，如果 RNC 知道各个小区间的 SFN 偏差，有时可用于用户位服务。

——对 RNC 公共的时间基准，例如通过 GPS 类型的接收机或类似之物接收由卫星星座发送的经同步的信号而获得。

在本发明的另一实施例中，源 RNC 只明显地发送 CSN 的最高有效位部分，例如 HFN，当剩余的最低有效位部分即 CFN 有一为目标 RNC 所知的经确定的值 (例如 0) 时也即隐含地提供该值时，源 RNC 强迫自己这样做。此种处理方式适合 SH0 之后的重定位的情况，因此用来执行这样的重定位的时标不是关键性的。

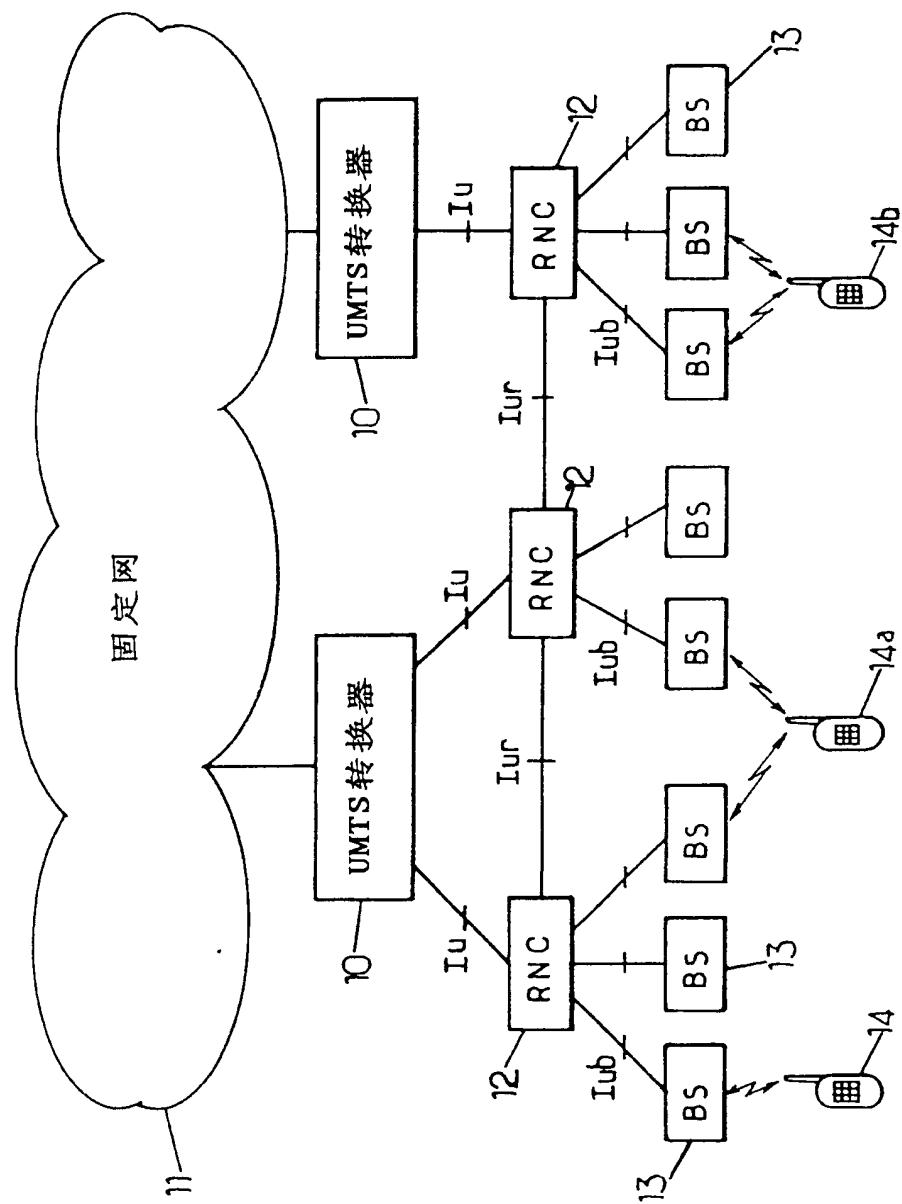


图 1

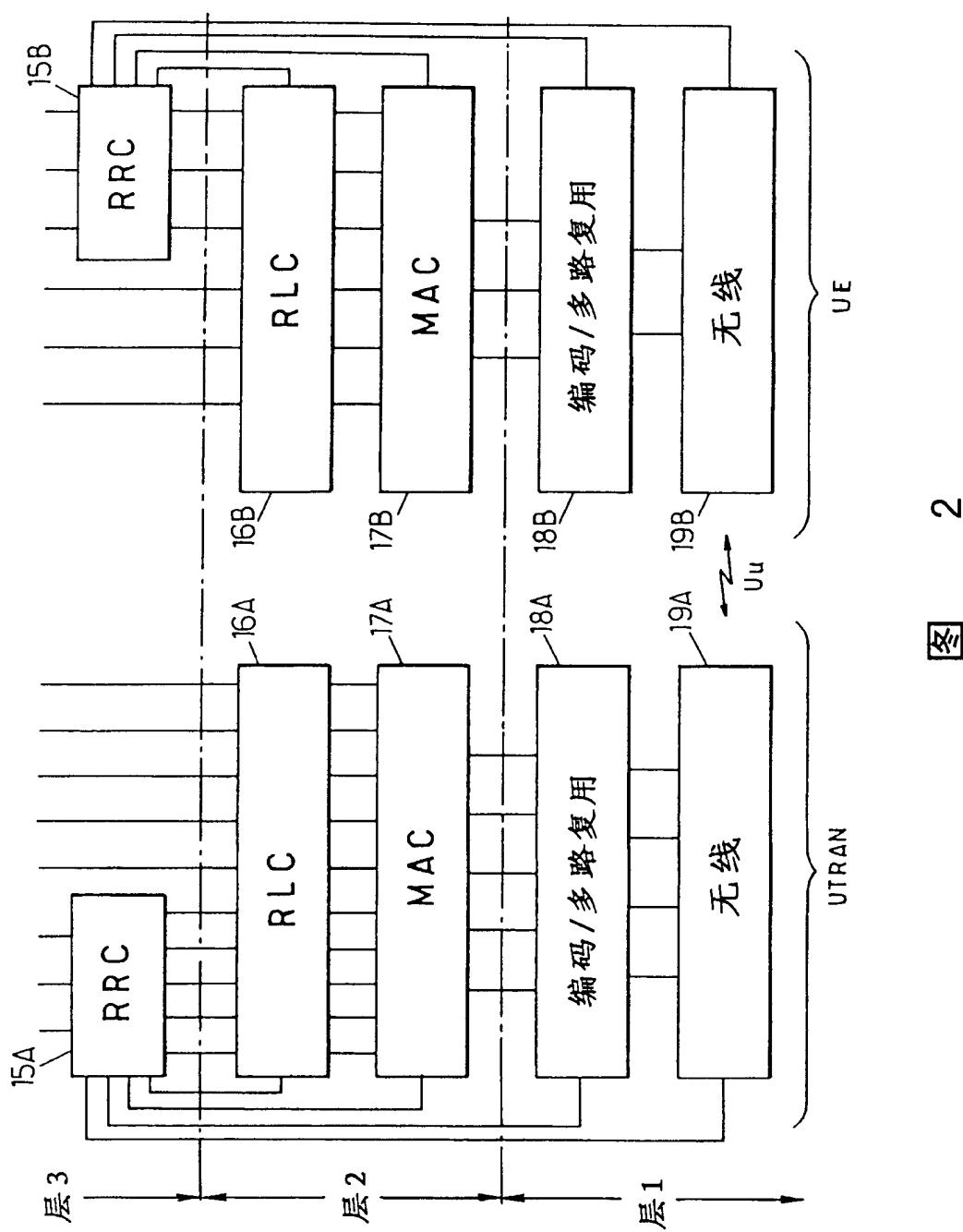


图 2

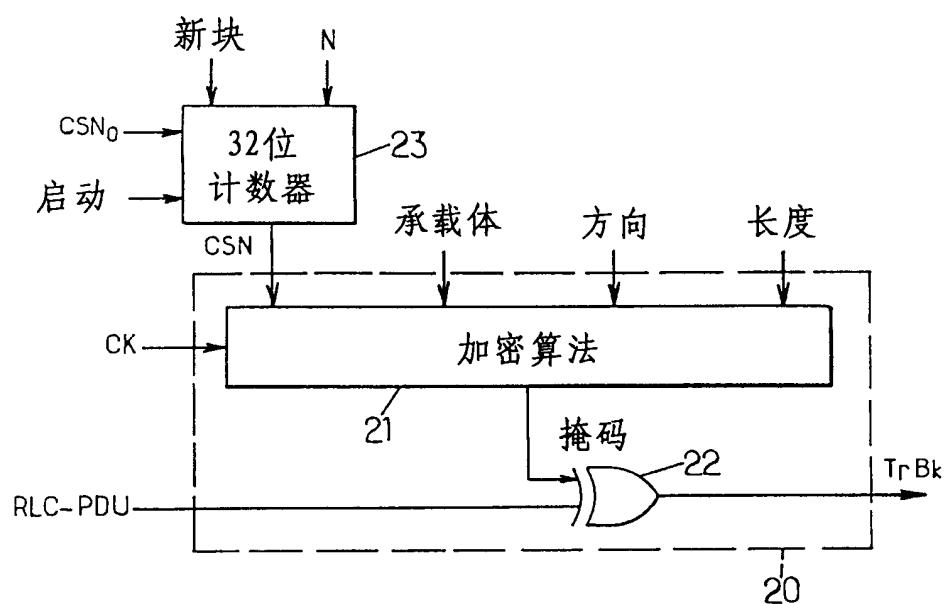


图 3

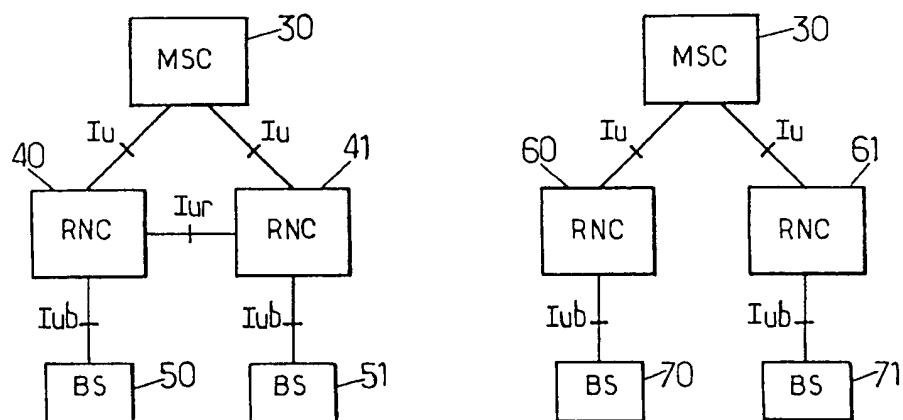


图 4

图 11

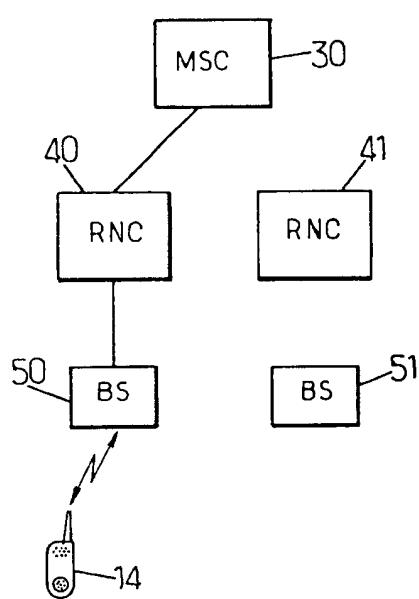


图 5

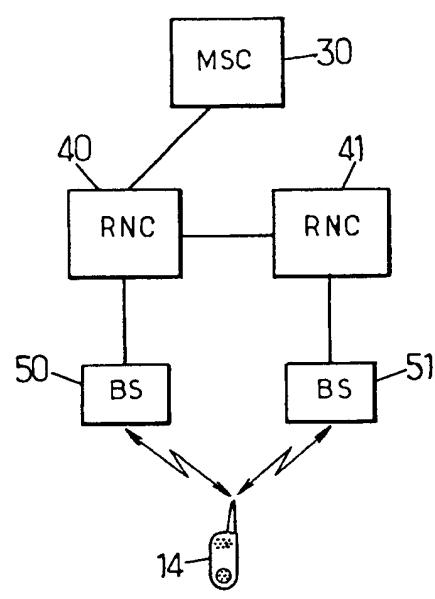


图 6

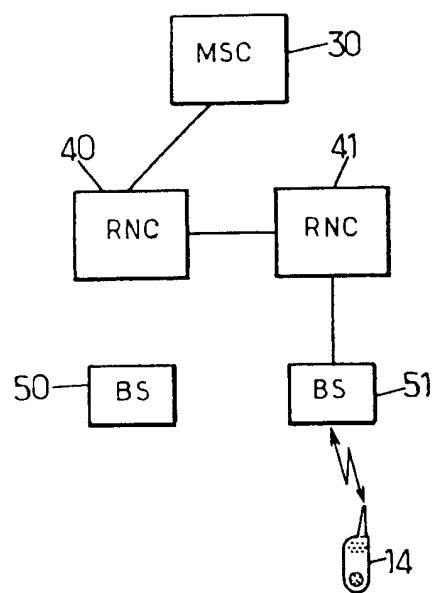


图 7

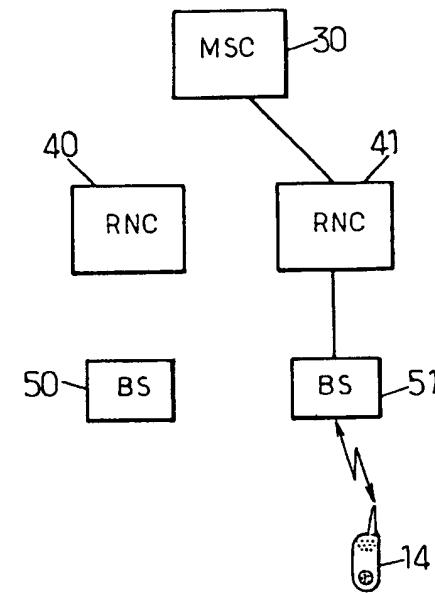
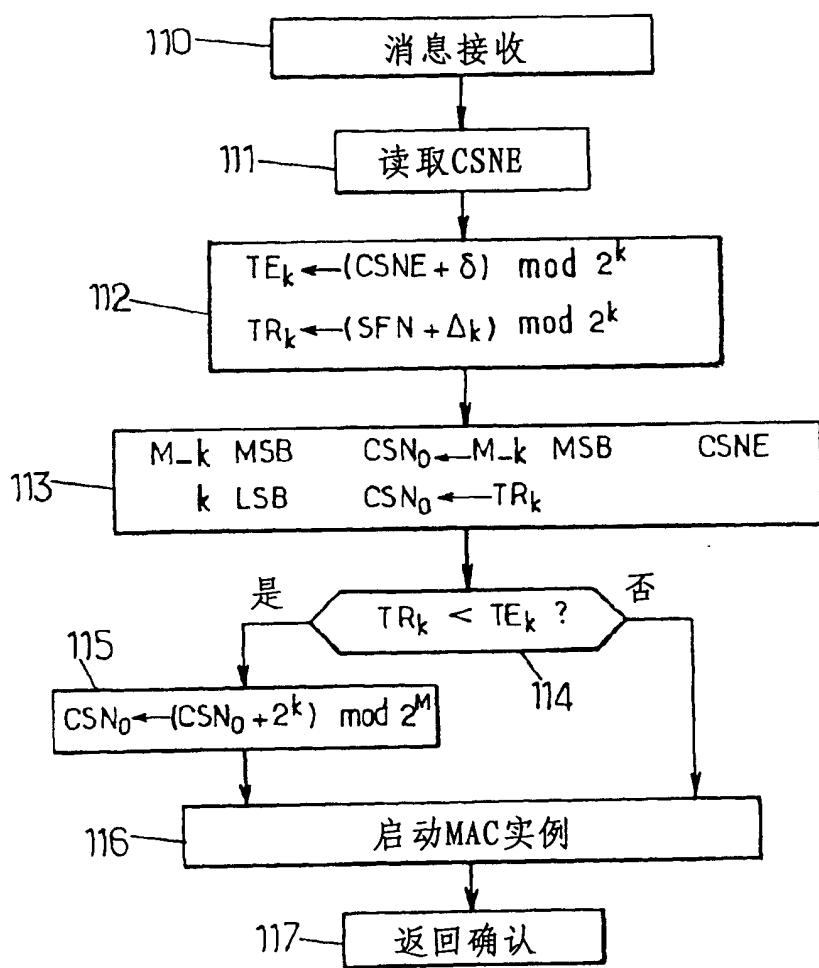
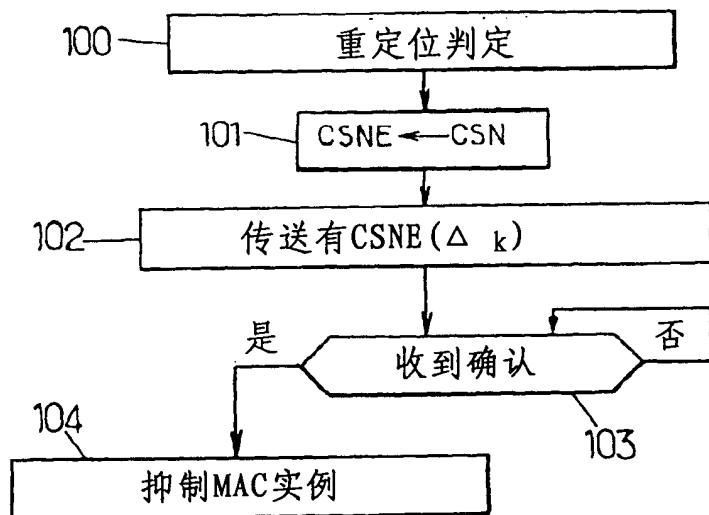


图 8



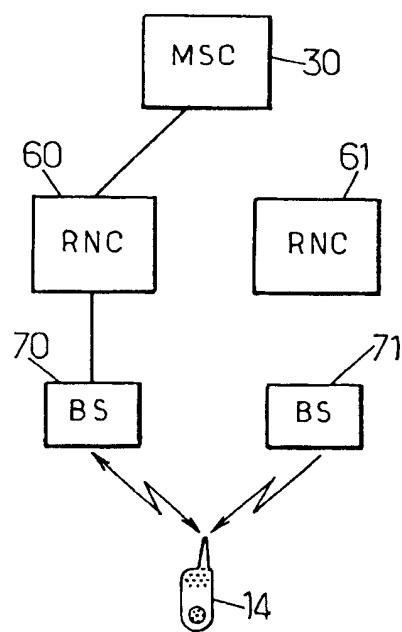


图 12

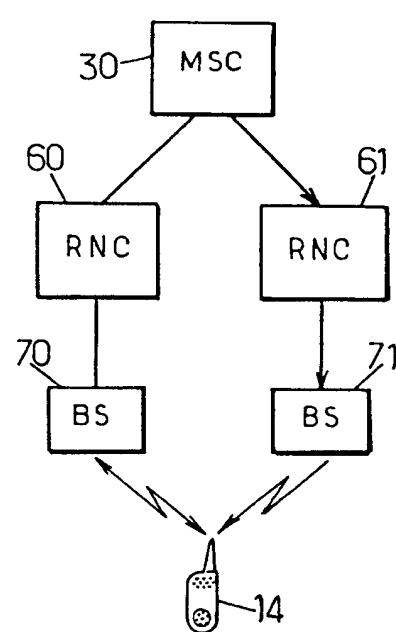


图 13

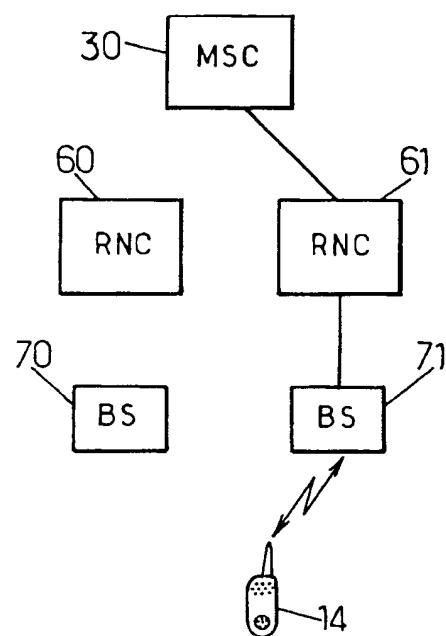


图 14