[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/20 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 02106237.4

[45] 授权公告日 2008 年 7 月 9 日

[11] 授权公告号 CN 100401792C

[22] 申请日 2002.4.5 [21] 申请号 02106237.4

[30] 优先权

[32] 2001. 4. 7 [33] KR [31] 18519/2001

[73] 专利权人 LG 电子株式会社

地址 韩国首尔

[72] 发明人 李承俊

[56] 参考文献

WO0054456 2000.9.14

审查员 冯晓明

[74] 专利代理机构 中原信达知识产权代理有限责任公司

代理人 张天舒 袁炳泽

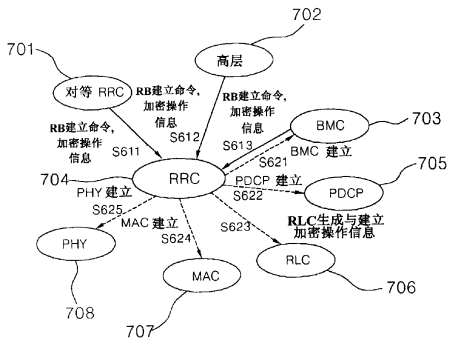
权利要求书 3 页 说明书 15 页 附图 6 页

[54] 发明名称

在移动通信系统中建立无线电载体的方法

[57] 摘要

本发明涉及在移动通信系统的无线电接口协议中建立无线电载体的方法，特别是涉及选择性地对每个无线电载体进行加密处理的方法。 本发明根据每当无线电载体建立时从高层传来的加密操作信息对要提供的服务进行数据加密处理，从而能够选择性地对每个无线电载体进行加密。



1. 一种在无线电接口中通过无线电载体发送数据，以便选择性地在每个无线电载体上进行加密处理的方法，包括：

将每个无线电载体的加密操作信息从指定层（701，702，703）传输到无线电资源控制 RRC 层（704），所述加密操作信息指示是否执行加密处理；

将每个无线电载体的加密操作信息从 RRC 层（704）传输到无线电链路控制 RLC 层（706）；以及

根据所述加密操作信息在 RLC 层（706）中选择性地对每个无线电载体的数据进行加密。

2. 根据权利要求 1 所述的方法，还包括：

将无线电载体建立信息从所述指定层（701，702，703）传输到 RRC 层（704）；以及

根据所述无线电载体建立信息在 RRC 层（704）建立低层（705，706，707，708）的无线电载体。

3. 根据权利要求 1 所述的方法，其中，所述指定层（701，702，703）是高层（702）、广播/多点传输 BMC 层（703）、或对等 RRC 层（701）。

4. 根据权利要求 1 所述的方法，其中，利用非访问层 NAS 消息将加密操作信息传输给高层（702）。

5. 根据权利要求 1 所述的方法，其中，在无线电载体建立时生成 RLC 层（706）。

6. 根据权利要求 1 所述的方法，其中，可以使用所建立的无线电载体，在提供数据服务时，，改变所述加密操作信息。

7. 根据权利要求 6 所述的方法，其中，可以通过改变从所述指定层（701，702，703）传来的加密标识符而实现加密操作信息的改变。

8. 根据前面任意一项权利要求所述的方法，其中：

接收到无线电载体建立请求后，从所述指定层（701，702，703）向无线电资源控制 RRC 层（704）传输加密操作信息和无线电载体建立信息；

根据所述无线电载体建立信息，在 RRC 层（704）建立低层（705 至 708）的无线电载体；以及

响应于所述无线电载体建立请求，生成无线电链路控制 RLC 层（706）。

9. 根据权利要求 8 所述的方法，其中，对于接收到的每个无线电载体建立请求，选择性地进行加密处理。

10. 根据前面任意一项权利要求所述的方法，其中，所述的加密操作信息是加密标识符。

11. 根据权利要求 8 所述的方法，用于改变加密操作，包括：

根据从所述指定层（701，702，703）传来的加密操作信息，在无线电链路控制层（706）选择性地对数据进行加密处理；

在所述指定层（701，702，703）中更新加密操作信息；

将更新了的加密操作信息传输给 RLC 层（706）；以及

根据更新了的加密操作信息选择性地对数据进行加密处理。

12. 根据权利要求 1 所述的方法，用于在移动通信收发机中对数据进行加密，包括：

在无线电资源控制层（704）建立无线电链路控制层（706）和无线电载体，以满足数据服务请求。

13. 根据权利要求 12 所述的方法，其中，将数据服务请求从所述指定层（701，702，703）传输到 RRC 层（704）。

14. 根据权利要求 12 或 13 所述的方法，其中，将无线电载体建立信息从所述指定层（701，702，703）传输到 RRC（704）层。

15. 根据权利要求 12 所述的方法，其中，可以在提供使用所建立的无线电载体的数据服务的过程中改变加密操作信息。

16. 根据权利要求 1 所述的方法，用于在无线电载体协议中建立无线电载体，包括：

（a）从所述指定层（701，702，703）向无线电链路控制层（706）传输加密操作信息；和

（b）根据加密操作信息，在 RLC 层（706）选择性地对通过无线电载体传送的数据进行加密。

17. 根据权利要求 16 所述的方法，其中：

为多个无线电载体中的每一个执行（a）和（b）；以及

对应无线电载体中每一个的加密操作信息指示通过各自无线电载体传送的信息是否在各自 RLC 层（706）被加密。

在移动通信系统中建立无线电载体的方法

发明领域

本发明涉及移动通信系统。具体而言，本发明涉及在无线电资源控制（下文中缩写为 RRC）层指定了无线电载体的情况下设定是否进行加密处理和改变每个无线电载体的加密设置的方法。

背景技术

在第 3 代合作项目（3GPP）中，用于这个第 3 代的网络和无线电接入系统，尤其是 RRC 层，是一个控制每个层的协议层。RRC 层属于开放式系统互连（OSI）参考模型的 3 个低层中的第 3 层。每个层包括分组数据集中协议（packet data convergence protocol，PDCP）层，广播/多点传输控制（BMC）层，无线电链路控制（RLC）层，媒体访问控制（MAC）层，以及物理（PHY）层。这里，PHY 层属于第 1 层，其它层，即 PDCP 层，BMC 层，RLC 层和 MAC 层均属于第 2 层。

图 1 是显示 3GPP 中无线电接口协议配置的示意图。

参照图 1，无线电接口协议包括控制每个层的 RRC 层 10，传输分组数据的 PDCP 层 21，传输广播和多点传输数据的 BMC 层 22，作为数据链路层而负责流量控制的 RLC 层 23，利用逻辑信道和传输信道之间的适当映射关系而传输（或承载）RLC 层 23 提供的数据的 MAC 层 24，以及通过将数据载入实际物理信道而将数据传输到无线电部分的 PHY 层 30。

仅在控制平面上定义 RRC 层 10，其负责与无线电载体（radio bearer，RB）的建立、重设和释放相关的传输信道和物理信道控制。

特别地，建立无线电载体意味着定义提供特定服务所需的协议层和信道特征，以及指定每个具体参数和操作方法。

PDCP 21 位于 RLC 层的上部，使得通过网络协议（如 IPv4 或 IPv6）传输的数据可以通过空中接口传输。

BMC 层 22 通过空中接口传输来自小区广播中心（CBC）的消息。更明确地说，BMC 层 22 在实际传输消息之前对通过终端传输的小区广播消息进行调度。通常，BMC 层 22 通过以无应答方式（unacknowledged mode，UM）操作的 RLC 层 23 传输数据。

RLC 层 23 对将要传输的适当的 RLC 协议数据单元（PDU）进行配置，以进行更好的 RLC 服务数据单元（SDU，是从高层传来的）分段和拼接功能，并进行自动重复请求功能（ARQ，承担传输过程中丢失的 RLC PDU 的重传）。按照如何处理来自高层的 RLC PDU，RLC 层 23 分为透明模式（TM）、应答模式（acknowledged mode，AM）、和无应答模式（UM），并且具有储存 RLC SDU 或 RLD PDU 的 RLC 缓存器。

另一方面，在 RLC 层 23 和 MAC 层 24 之间访问逻辑信道（L_CH）。为了使用频分双工（FDD），现有的 3GPP 使用 6 个逻辑信道，包括 DTCH，DCCH，CTCH，CCCH，BCCH 和 PCCH。

DTCH（专用业务信道）是用于传输特定用户设备（UE）的专用数据的信道，DCCH（专用控制信道）是用于传输特定用户设备的专用控制信息的信道。

CTCH（公用业务信道）是用于将公用数据传输给多个用户设备的信道，而 CCCH（公用控制信道）是用于将公用控制信息传输给多个用户设备的信道。

另外，BCCH（广播控制信道）是用于传输广播信息的信道，PCCH（寻呼控制信道）是用于传输寻呼信息的信道。

同时，在 MAC 层 24 和 PHY 层 30 之间访问传输信道（T_CH）。在这种情况下，为 FDD 共使用了 7 个传输信道，包括 DCH，BCH，FACH，PCH，RACH，CPCH 和 DSCH。

首先，DCH（专用信道）是用于传输特定用户设备的专用数据的信道，而 BCH（广播信道）是用于传输广播信息的信道。

FACH（前向访问信道）是用于传输前向（下行）数据的信道，PCH（寻呼信道）是用于传输寻呼信息的信道。

RACH（随机访问信道）是用于传输反向数据的信道，CPCH（公用分组信道）是用于传输小分组数据的信道，而 DSCH（下行链路共享信道）是用于在前向方向上传输大量数据的信道。

另外，可以复用多个逻辑信道（L_CH）以形成单个的传输信道（T_CH），并且同样，可以复用多个传输信道（T_CH）以形成单个的物理信道。

因此，配置好的无线电接口协议进行无线电载体（RB）建立过程，以定义或指定提供特定服务所需的层和信道的特征。图 2 描述了无线电载体建立过程。

具体而言，图 2 解释了在现有技术的无线电接口协议中建立无线电载体的方法。如图所示，为了建立 RB，RRC 层 204 首先分别从一个或每个层（包括对等 RRC 201、高层 202 和 BMC 层 203）接收无线电载体建立命令（S211 至 S213）。然后，RRC 层 204 将无线电载体

建立命令传给低层（如，BMC 层、PDCP 层、RLC 层、MAC 层、或 PHY 层），以便为数据服务建立适当的层（S221 至 S225）。因此，通过无线电载体建立过程，可以决定是否使用 PDCP 层 205 和 BMC 层 203，以及在几种 RLC 模式中，即在应答模式（AM）、无应答模式（UM）或透明模式（TM）中应该采用哪种模式。而且，当生成 RLC 实体时，决定在 RLC 层和 MAC 层之间应该使用哪个逻辑信道，以及在 PHY 层内使用哪个物理信道。总之，通过指定参数和建立其操作方法而建立无线电载体。

这里，RLC 层不象其它层那样一直可用。实际上，只有当建立了 RB 时它才生成，并且在提供相关服务后丢弃。

根据现行的 3GPP 标准，一个 RB 毫无例外地必须使用一个 RLC 实体。同样，用户设备能一次容纳最多 32 个无线电载体，并且不象其它层那样，多个 RLC 实体能同时存在。

如前所述，RLC 实体主要分为不能附带 RLC 报头的透明模式（TM）和能附带 RLC 报头的不透明模式。其中，不透明模式能进一步分为有应答信号的应答模式（AM）和没有应答信号的无应答模式（UM）。

以下参照图 3 解释 RLC AM 实体的结构。如图所示，为了由从高层传下来的服务数据产生固定大小的协议数据单元，发送侧的 AM 实体进行分段/拼接处理（S301），并且包括进具有序号（SN）的报头（S302）。

包含报头的 PDU 存储在重发缓存器内，以备稍后需要重传（S305）。

同时，包含报头的 PUD 由复用器进行复用（S304），并且为了

数据安全而进行加密（S305）。

然后，加密的 PDU 暂时储存在发送缓存器中，并被传输到设定字段模块（S306）。通过设定字段模块，除 RLC 报头序号之外的其它字段（D/C 和轮询字段（poll field））被设定为适当的值并且传输到低层（S307）。

特别地，载有来自高层的数据信息的 PDU 被称为 AMD（AM 数据）PDU，它的结构如图 4 所示。如图所示，RLC 层包含两种不同格式的协议数据单元。其中一种是 UMD PDU（无应答数据 PDU），它特别用于发送侧需要无应答信号的时候；而另外一种是 AMD PDU（应答数据 PDU），它用于发送侧需要应答信号时。如图 4 所示，AMD PDU 包含报头、长度指示符组、数据，PDA（填充）或捎带（piggyback）型 PDU。

仅对 AMD PDU 进行加密。这时，报头组，特别是前两个八位字节（包含序号的组），将不被加密，只有报头组后面的组被加密。

另一方面，接收侧的 AM 实体分离从低层传来的协议数据单元（S308），并且将分离出的协议数据单元暂时储存在接收缓存器中（S309）。一旦全部接收到构成一个完整 SDU 的协议数据单元，AM 实体将这些协议数据单元解密（S310），去除 RLC 报头（S311），将解密的协议数据单元重组为 SDU，最后将它们传输到高层（S312）。

同时，图 5 显示了 RLC UM 实体。参照图 5，发送侧的 UM 实体进行分段/拼接处理，将从高层传来的服务数据单元变成固定大小的 PDU（S511）；并且为了数据安全而对 PDU 进行加密（S512）。然后，RLC UM 实体通过包含进具有序号的报头而构造 UMD 协议数据单元（S513），将 UMD 协议数据单元储存在发送缓存器内，最后通过低层将它们传输到无线电部分（S514）。

图 6 显示了 UMD PDU 结构。参照图 6，UMD PDU 包括报头、长度指示符组、数据和 PAD（填充）。如图所示，UMD PDU 格式中的第一个八位字节指示了含有序号的报头。这里，这个报头组不进行加密，只有其它的组进行加密。

同时，接收侧的 UM 实体接收 UMD PDU 并暂时储存在接收缓存器内（S521）。当通过接收侧接收到用于构造一个完整 SDU 的全部协议数据单元时，从协议数据单元中去除 RLC 报头（S522）。然后，接收侧的 UM 实体对协议数据单元进行解密（S523），将解密的协议数据单元重组为 SDU，最后将它们传输高层（S524）。

因此，3GPP 进行加密处理以确保用户数据的安全。根据 RLC 模式，涉及 AM 和 UM 时加密处理特别地在 RLC 层内进行，而涉及到 TM 时在 MAC 层进行。值得注意的是，并不是所有数据都被加密。也就是说，在 AM 和 UM 情况下，仅对传输到逻辑信道中的 DTCH 或 DCCH 的数据进行加密处理。在 TM 的情况下，仅对传输到传输信道中的 DCH 的数据进行加密处理。这个加密处理不是对每个无线电载体都可用，而是总体地决定是否对所有的无线电载体进行加密处理。

通常，当加密数据从发送侧传输到接收侧时，接收侧通过解密处理重新构建数据。此时，为了更精确地收发数据，发送侧和接收侧应该使用相同的算法和加密参数。这可以参照图 3 和图 5 而更好地理解。

然而，现有方法的一个问题是，因为所有的无线电载体都进行或都不进行加密处理，所以不能对单个无线电载体进行单独的加密处理。换句话说，如果用户希望只对特定的无线电载体进行加密处理，而不管其它的无线电载体，那么现有的建立无线电载体的方法就未必是正确选择。

例如，目前使用的 BMC 数据采用了 RLC UM 实体，并且传输给逻辑信道中的 CTCH，因此，不对其进行加密处理。事情就是，BMC 数据内存在不须加密的数据，但是同样存在须加密的数据。因此，加密处理必须在无线电载体上选择地进行。例如，BMC 服务包括 SMS-CB（短消息服务-小区广播）、SMS-PP（短消息服务-点对点）、IP 多点传输服务等等。在 SMS-CB 服务的情况下，由于存在用于小区内所有用户设备的信息，因此不须进行加密处理。

相反，对于 SMS-PP 服务，因为一个特定用户设备具有仅用于另外一个特定用户设备的信息，所以需要加密处理。类似，在 IP 多点传输服务的情况下，信息要发送给特定组中的用户设备，因此也需要进行加密处理。然而，根据现有的建立无线电载体的方法，当涉及 SMS-PP 服务或 IP 多点传输服务时，对设备来说只有两种选择，即全部加密或全部不加密。因此，不可能进行有鉴别的加密服务，并且 SMS-CB 服务和 SMS-PP 服务不管怎样都不能同时进行。

此外，如果提供了特定的服务同时对该服务进行加密，然后又在需要的时候在某一点决定不对该服务进行加密，现有的建立无线电载体的方法不能改变对该特定无线电载体的加密，而是需要重新建立所有的无线电载体。

另外，为了建立所有的无线电载体，必须收集关于每个层的信息，这时，将产生大量的信令开销，甚至更糟，仅仅为了改变和应用是否对特定无线电载体进行加密就耽搁了大量的时间。

发明内容

因此，本发明的一个目的是提供一种在无线电接口协议中建立无线电载体的方法，以通过在建立无线电载体的同时设定是否进行加密处理而选择性地对每个无线电载体进行加密处理。

本发明的另一个目的是提供一种在使用建立的无线电载体或对数据进行加密而提供数据服务的过程中改变加密操作信息的方法。

为了实现以上目的，提供了一种在无线电接口协议中建立无线电载体的方法，该方法包括以下步骤：从指定的层将加密操作信息传输给无线电资源控制（RRC）层；将加密操作信息从 RRC 层传到无线电链路控制（RLC）层；以及根据加密操作信息在 RLC 层上对数据进行加密。

指定层包括高层、广播/多点传输（BMC）层、或/和对等 RRC 层。

当无线电载体建立时生成无线电链路控制层（RLC）。

加密操作信息可以在使用所建立的无线电载体而提供数据服务的过程中改变，并且通过改变从指定层传来的加密标识符实现加密操作信息的改变。

在本发明的另一方面，提供了一种在无线电接口协议中进行加密处理的方法，该方法包括以下步骤：接收到无线电载体建立请求之后，从指定层将加密操作信息和无线电载体建立信息传输到无线电资源控制（RRC）层；根据无线电载体建立信息在 RRC 层建立低层无线电载体；响应于无线电载体建立请求生成无线电链路控制（RLC）层；以及根据加密操作信息在 RLC 层对数据进行加密。

每次生成无线电载体建立请求，由新生成的 RLC 层进行加密处理。

本发明还有另一个方面，提供了一种改变加密的方法，这种方法包括以下步骤：根据从指定层传来的加密操作信息，在无线电链路控

制（RLC）层对数据进行加密处理；在指定层中更新加密操作信息；将更新了的加密操作信息传输给 RLC 层；以及根据更新了的加密操作信息对数据进行加密处理。

本发明还有一个方面，提供了一种在移动通信收发机中加密数据的方法，该方法包括以下步骤：在无线电资源控制（RRC）层建立无线电链路控制（RLC）层和无线电载体，以满足数据服务请求；将无线电载体上的加密操作信息从 RRC 层传输到 RLC 层；以及根据加密操作信息对通过无线电载体从 RLC 层传来的数据进行加密。

无线电载体建立信息是从指定层传输到 RRC 层的。

附图说明

由以下的详细说明，结合附图，可以更清楚地理解本发明上述的目的、特征和优点。附图中：

图 1 是一个示意图，显示了第 3 代合作项目（3GPP）中的无线电接口协议结构；

图 2 显示了根据现有技术的在无线电接口协议中建立无线电载体的方法；

图 3 显示了无线电链路控制应答模式（RLC AM）实体的结构；

图 4 显示了图 3 中无线电链路控制 AM 数据协议数据单元（RLC AMD PDU）的格式结构；

图 5 显示了无线电链路控制无应答模式（RLC UM）实体的结构；

图 6 显示了图 5 中无线电链路控制 UM 数据 PDU（RLC UMD PDU）的格式结构；

图 7 显示了根据本发明的在无线电接口协议中建立无线电载体的方法；

图 8 显示了根据本发明的无线电资源控制服务访问点（RRC SAP）。

优选实施例说明

以下参照附图对本发明的优选实例进行说明。在以下的说明中，即使在不同的图中也对相同的部件使用相同的标号。说明书中所限定的内容只是为了帮助更好地理解本发明。因此，很明显，没有那些所限定的内容也可以实施本发明。另外，不对公知的功能或结构做详细描述，因为不必要的细节会使得本发明不清晰。

图 7 示意地显示了根据本发明的在无线电接口协议中建立无线电载体的方法。本发明的建立无线电载体的方法能够传输关于是否进行加密处理的信息，尤其当高层、对等 RRC（无线电资源控制）层、或 BMC（广播/多点传输控制）层中的至少一个层请求 RRC 层的无线电载体建立时，其中 RRC 层根据请求在低层建立无线电载体，同时将关于是否进行加密处理的信息传输给 RLC（无线电链路控制）层，RLC 层随后确定数据的加密。同时，应注意到每次建立无线电载体时生成前述的 RLC 层。

参照图 7，当无线电载体建立命令分别从对等 RRC 层 701、高层 702 和 BMC 层 703 传输到 RRC 层 704，以向特定用户设备（UE）提供不同种类的服务时，同时也传输加密操作信息（S611 至 S613）。这里，加密操作信息指示了是否进行加密处理，优选地，它是加密指示符（ciphering indicator）。以下详细说明对不同层应用这个过程。

1)如果无线电载体建立命令和加密操作信息是从高层传输到 RRC 层（S612）

如果从高层 702 向低层提供特定的服务，高层 702 首先给它的低层 RRC 层 704 发出无线电载体建立命令，以在该低层中建立无线电载体（S612）。这称做 NAS（Non Access Stratum，非访问层；AS 的上组）消息。NAS 消息位于控制平面，并能通过 RRC SAP（无线电资源控制服务访问点）从 NAS 传输到 AS（Access Stratum，访问层：一个包括 RRC 层、BMC 层、PDCP 层、RLC 层、MAC 层、PHY 层

等的组）（参照图 8）。这里，RRC SAP 包括三个不同种类的服务访问点，例如，GC（总控制）SAP、NT（通知）SAP、和 DC（专用控制）SAP。因此，当使用 NAS 消息将无线电载体建立命令传输给 RRC 层 704 时，NAS 消息中可以包含加密指示符。为了将要提供给其低层（即 BMC 层 703、PDCP 层 705、RLC 层 706、MAC 层 707 和 PHY 层 708）的服务，接收到 NAS 消息的 RRC 层 704 建立适当的无线电载体（S621 至 S625）。另外，RRC 层 704 将加密指示符传输给 RLC 层 706。然后，RLC 层 706 根据加密指示符进行数据加密。这时，根据服务种类决定使用或不使用 BMC 层和 PDCP 层。

2)如果无线电载体建立命令和加密操作信息是从对等 RRC 层传输到 RRC 层（S611）

对等 RRC 层的无线电载体建立过程是高层无线电载体建立过程的一部分。因此，如果提供了来自高层 702 的特定服务，则该高层建立它的低层和它自己的对等实体。这样，须传输的数据被发往对等 RRC 层 701。为此，从高层 702 接收到无线电载体建立命令的 RRC 层 704 通过信息单元（information element）把无线电载体建立命令传给其对等 RRC 层 701。对等 RRC 层 701 也建立它的低层（S611）。同时，通过在信息单元内插入加密指示符以通知是否进行加密处理，RLC 层 706 可以进行数据加密。这里，高层 702 和 RRC 层 701 相互区分的原因是，从一个 RRC 层 704 的角度来说，无线电载体建立命令可以传输到 NAS 或对等 RRC 层。

3）如果无线电载体建立命令和加密操作信息是从 BMC 层传输到 RRC 层（S613）

广播/多点传输服务功能在 CBC（小区广播中心）内进行，CBC 位于 CN（核心网络）内。传输广播信息时，CBS 给 BMC 层 703 发出无线电载体建立命令，BMC 层 703 通过基元（primitive）将无线电载体建立命令转给 RRC 层 704（S613）。这时，加密指示符被插入到该基元中以进行传输，收到该基元的 RRC 层 704 建立它的低层，同

时通知给其它方的 RRC 层，使得也建立其它方的低层。另外，BMC 层 703 将加密指示符传输给 RLC 层 706，以对数据进行加密（S621 至 S625）。

另一方面，由于从高层 702、对等 RRC 层 701、BMC 层 703 传来的信息是给出控制信息的信号消息，而不是用户数据，所以它没有象 PDU 或 SDU 那样的具体形式，只有名称可以定义。特别地，无线电载体建立命令和加密指示符在高层 702 的情况下通过 NAS 消息，在对等 RRC 层 701 的情况下通过信息单元，在 BMC 层 703 的情况下通过基元而传输。

如上所述，当 RRC 层 704 接收到关于无线电载体建立命令和是否进行加密处理的请求时，RRC 层 704 通过基元把命令转给它的低层。

通常，加密可在 RLC 层和 MAC 层进行。特别地，由于所有的无线电载体共同地使用 MAC 层，所以加密处理不必在每个无线电载体上进行。然而，当涉及 RLC 层时，由于为每个无线电载体单独地生成层，所以可以选择性地加密。

例如，在 RLC 层的情况下，对每个无线电载体的加密处理只在 AM 和 UM 中进行，而不是在 TM 中。这是因为 TM 中的加密是在 MAC 层中进行，因此，无需对每个无线电载体进行单独的加密处理。

并且，RLC AM 和 UM 接收来自 RRC 层的无线电载体建立命令，建立其它参数，同时决定是否进行加密处理。如果决定进行加密处理，则 RLC AM 或 UM 对数据进行加密，并将加密数据传给 MAC 层 707。相反，如不进行加密处理，则 RLC AM 或 UM 将数据直接传给 MAC 层 707，不进行加密处理。

因此，如果 RRC 层 704 建立 BMC 层 703，则 RRC 层 704 利用

CBMC-CONFIG-REG 把 CTCH 环境（配置）建立命令传给 BMC 层 703（S621）。

另外，如果 RRC 层 704 建立 PDCP 层 705，则 RRC 层 704 利用 CPDCP-CONFIG-REG 把报头压缩信息、RLC-SAP 信息（即，在 AM/UM/TM 中应使用哪个 RLC）、以及关于是否对 PDCP 序号进行同步的信息传给 PDCP 层 705。

而且，如果 RRC 层 704 建立 RLC 层 706，则 RRC 层 704 利用 CRLC-CONFIG-REG 给 RLC 层 706 发出信息，包括 RLC AM、UM 或 TM 中所需模式的选择，RLC 实体生成，加密元素（即，加密码、密匙值和加密所需的 RLC HFN（超帧数目，Hyper Frame Number）值，要加密的 PDU 的 SN-AM 和 UM）和每种模式所需的其它参数（S623）。更明确地说，在 AM 的情况下，参数包括 PDU 大小、按序发布指示、定时器值、协议参数值、轮询触发器、状态触发器、SDU 抛弃模式等。另一方面，在 UM 的情况下，参数可以是定时器值，而在 TM 的情况下，参数可以包含定时器值和分段指示。

通过使用 CMAC-CONFIG-REQ 传输用户设备信息（也就是，S-RNTI，C-RNTI，SRNC 本体（identity），激活时间），RB 信息（也就是，传输信道本体，逻辑信道本体，MAC 逻辑信道优先级），传输信道信息（也就是，传输格式组合组），以及加密元素（只有当 RLC 处于 TM 加密模式时使用，密匙值和 MAC HFN 值），RRC 层 704 可以建立 MAC 层 707（S624）。

RRC 层 704 还将 CPHY-TrCH-CONFIG-REG 或 CPHY-RL-Setup-REG 传给 PHY 层 708（S625）。

如上所述，RRC 层 704 使用基元将无线电载体建立命令传给每个层，并为无线电载体建立合适的环境。

同时，在无线电载体建立过程中任何时间，基元可以重设。也就是说，如果用户希望改变某一参数，通过把包含有要改变的参数的基元再次发送给 RRC 层，他或她就能改变相关的参数。

当对每个无线电载体进行选择性加密时，称做“加密标识符（ciphering identifier）”的附加参数被添加在从 RRC 层到 RLC 层的 CRLC-CONFIG-REG 基元上。

而且，是否进行加密处理的决定在 RLC AM 实体或 UM 实体内是可调整的。换句话说，虽然相关的 RLC 实体要通过 CRLC-CONFOG-REQ 基元来通知是否进行加密处理，但是可以再次通过 CRLC-CONFOG-REQ 基元来改变这个决定，尤其是在加密处理的过程中用户又不希望加密数据时。

而且，对于无线电载体，即使在使用过程中，也可以通过上述 3 个信令随时改变加密操作信息，并且 RRC 层可以根据这个加密操作信息对 RLC 层中的数据进行加密。例如，如果起先数据根据主要功能是加密数据的加密操作信息进行加密，有可能通过改变加密操作信息而不对数据进行加密，从而没有数据被加密。

同时，因为对等 RRC 层 701、高层 702 和 BMC 层提供了互不相同的服务，所以 RRC 层可以从包括对等 RRC 层、高层和 BMC 层的这些层中的至少一个层接收无线电载体建立命令。即使在这种情况下，是否进行加密处理的决定最终也是通过上述信令传给 RRC 层。然后 RRC 层建立其低层，并给低层发出加密操作信息。

总之，根据本发明的建立无线电载体的方法，可以选择性地对每个无线电载体进行加密处理，从而使 3GPP 能够同时提供多种服务。

另外，本发明的建立无线电载体的方法可以在提供使用所建立的无线电载体的数据服务的过程中改变加密操作信息，从而防止时间延迟和更迅速地提供服务。

虽然参照特定的优选实施例显示并叙述了本发明，但是本领域技术人员可以理解，在不脱离所附权利要求所限定的精神和范围的情况下，可以对本发明进行形式和细节上的多种变化。

图1

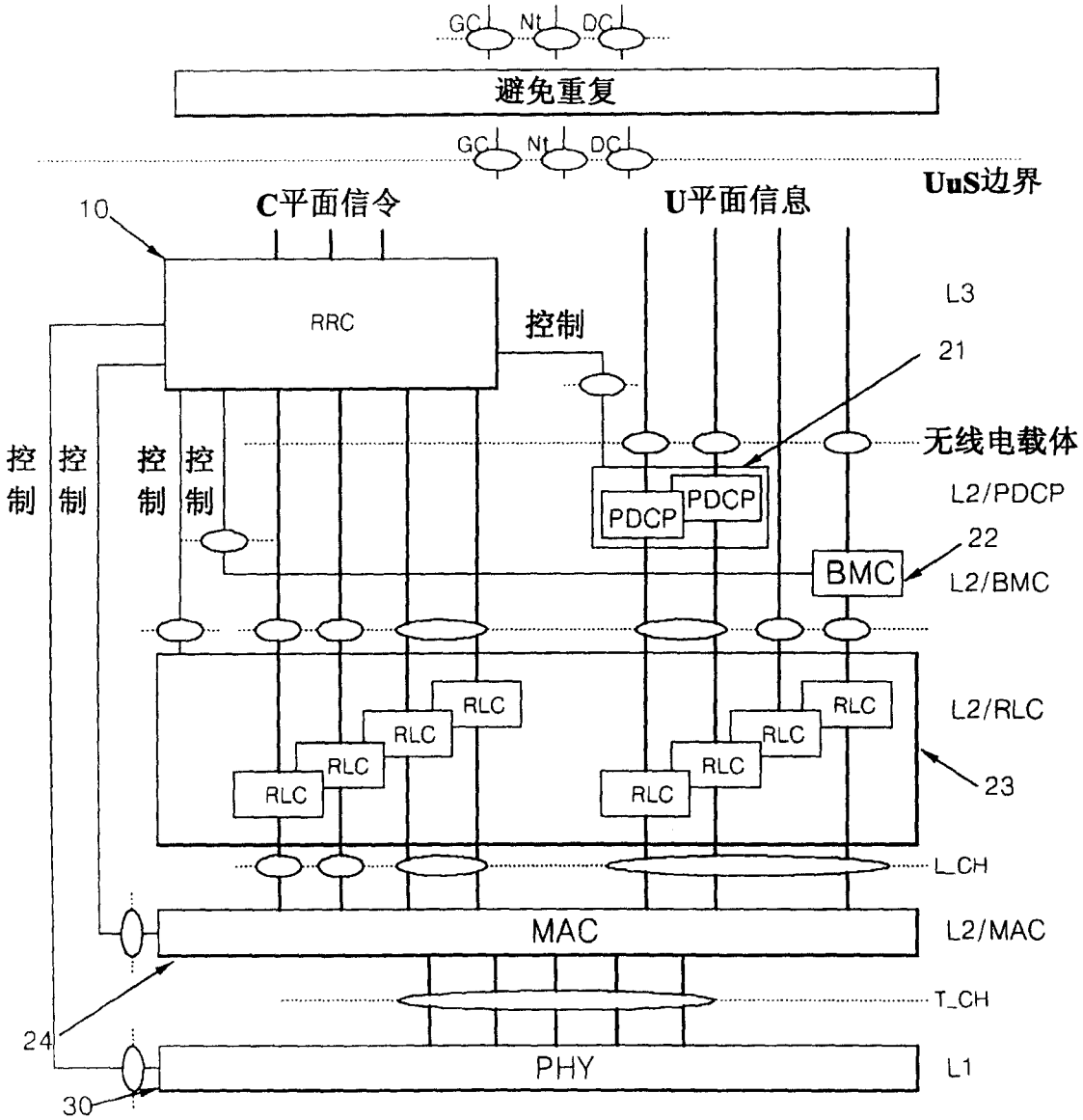

GC
NT
DC
避免重复
GC
NT
DC
UuS边界
10
C平面信令
U平面信息
RRC
控制
L3
21
无线电载体
控制
控制
控制
控制
PDCP
PDCP
L2/PDCP
22
BMC
L2/BMC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
L2/RLC
23
L_CH
MAC
L2/MAC
T_CH
24
PHY
L1
30

图2

(现有技术)

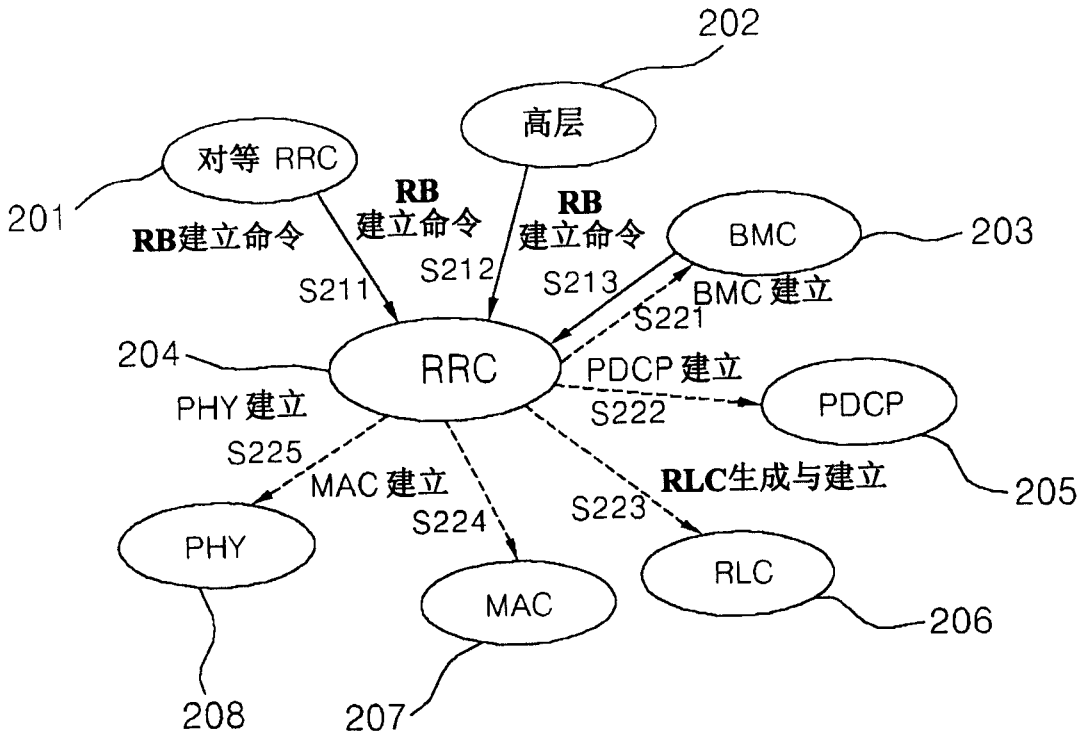

202
高层
对等 RRC
201
RB建立命令
RB
建立命令
S211
S212
RB
建立命令
S213
BMC
203
BMC 建立
S221
204
RRC
PDCP 建立
S222
PDCP
205
PHY 建立
S225
MAC 建立
S224
S223
RLC生成与建立
PHY
MAC
RLC
206
208
207

图3

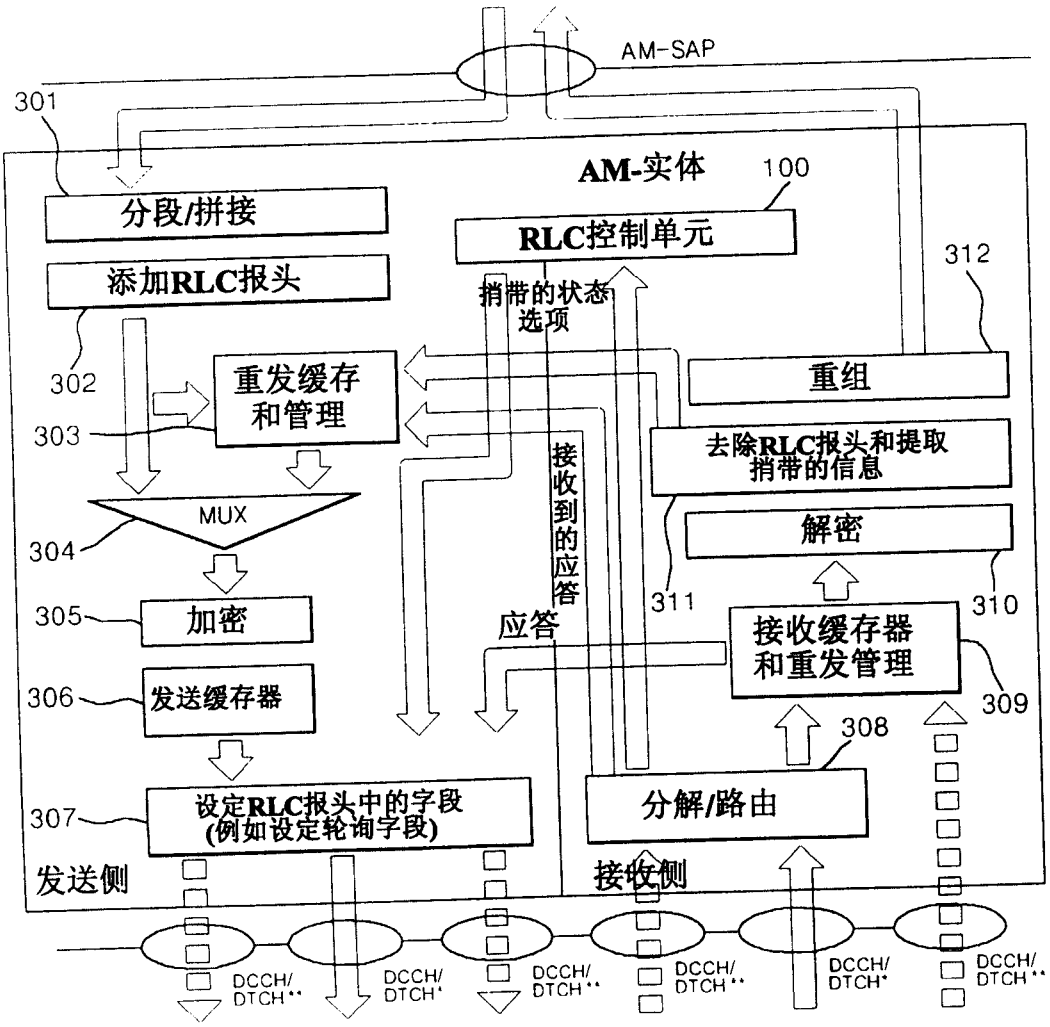

AM-SAP
301
AM-实体
100
分段/拼接
RLC控制单元
添加RLC报头
捎带的状态选项
312
302
重发缓存和管理
重组
303
去除RLC报头和提取捎带的信息
接收到的应答
MUX
解密
304
311
310
305
加密
应答
接收缓存器和重发管理
306
发送缓存器
309
308
307
设定RLC报头中的字段(例如设定轮询字段)
分解/路由
发送侧
接收侧
DCCH/DTCH*
DCCH/DTCH**
DCCH/DTCH*
DCCH/DTCH**
DCCH/DTCH**
DCCH/DTCH*
DCCH/DTCH**

图4

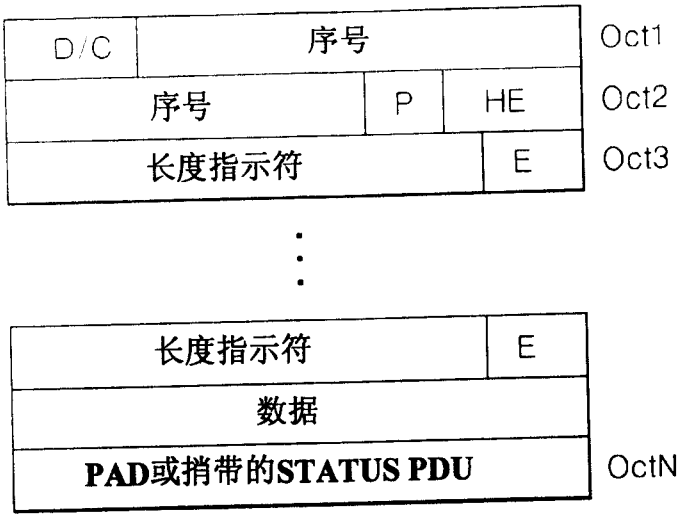

D/C
序号
Oct1
序号
P
HE
Oct2
长度指示符
E
Oct3
长度指示符
E
数据
PAD或捎带的STATUS PDU
OctN

图5

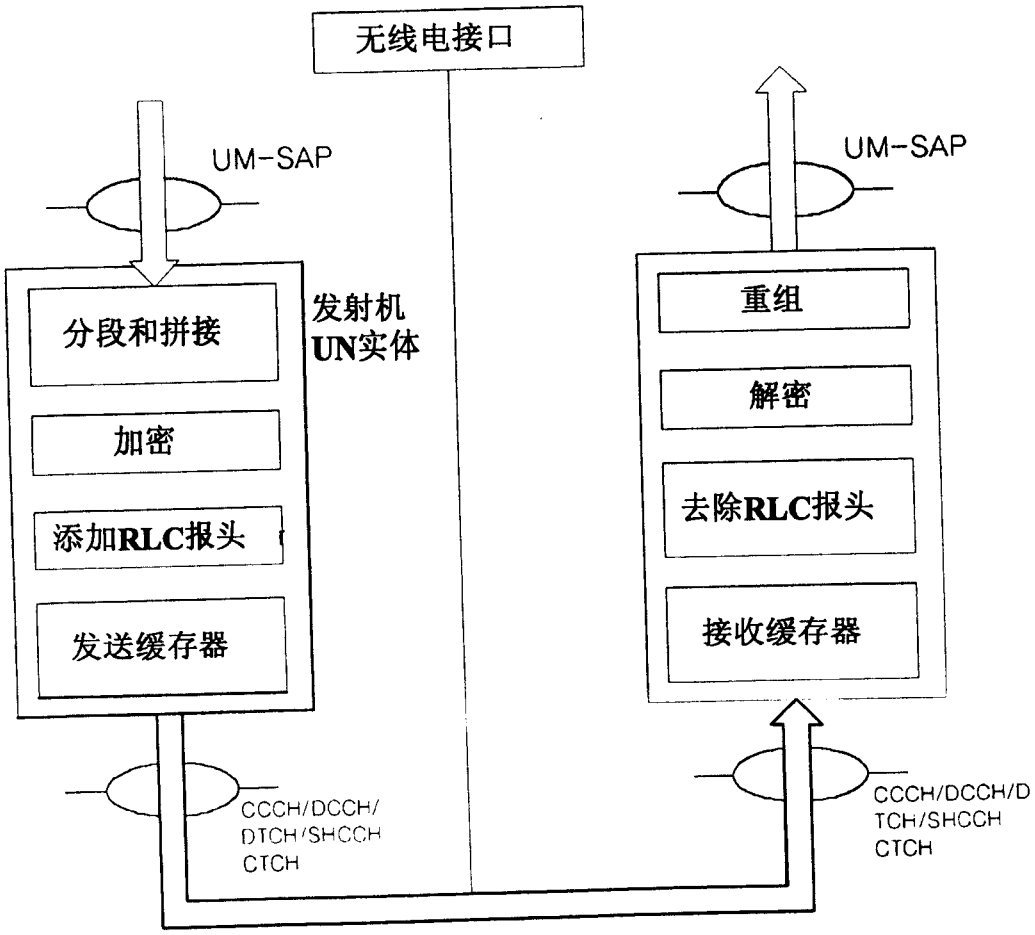

无线电接口
UM-SAP
UM-SAP
分段和拼接
发射机
UN实体
加密
添加RLC报头
发送缓存器
重组
解密
去除RLC报头
接收缓存器
CCCH/DCCH/
DTCH/SHCCH
CTCH
CCCH/DCCH/D
TCH/SHCCH
CTCH

图6

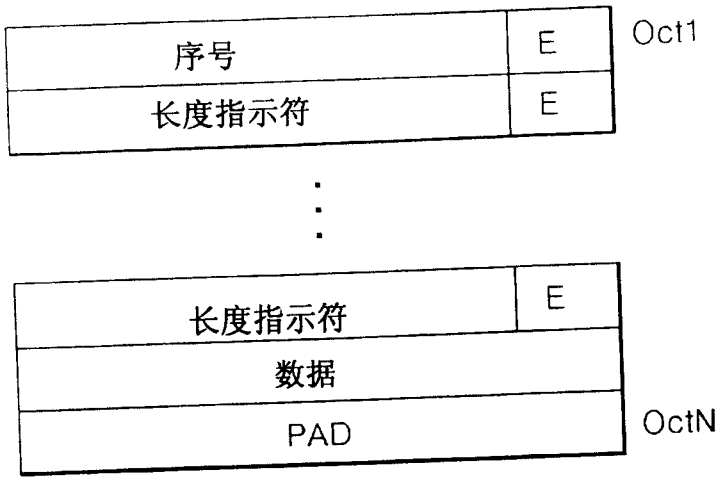

序号
E
Oct1
长度指示符
E
长度指示符
E
数据
PAD
OctN

图7

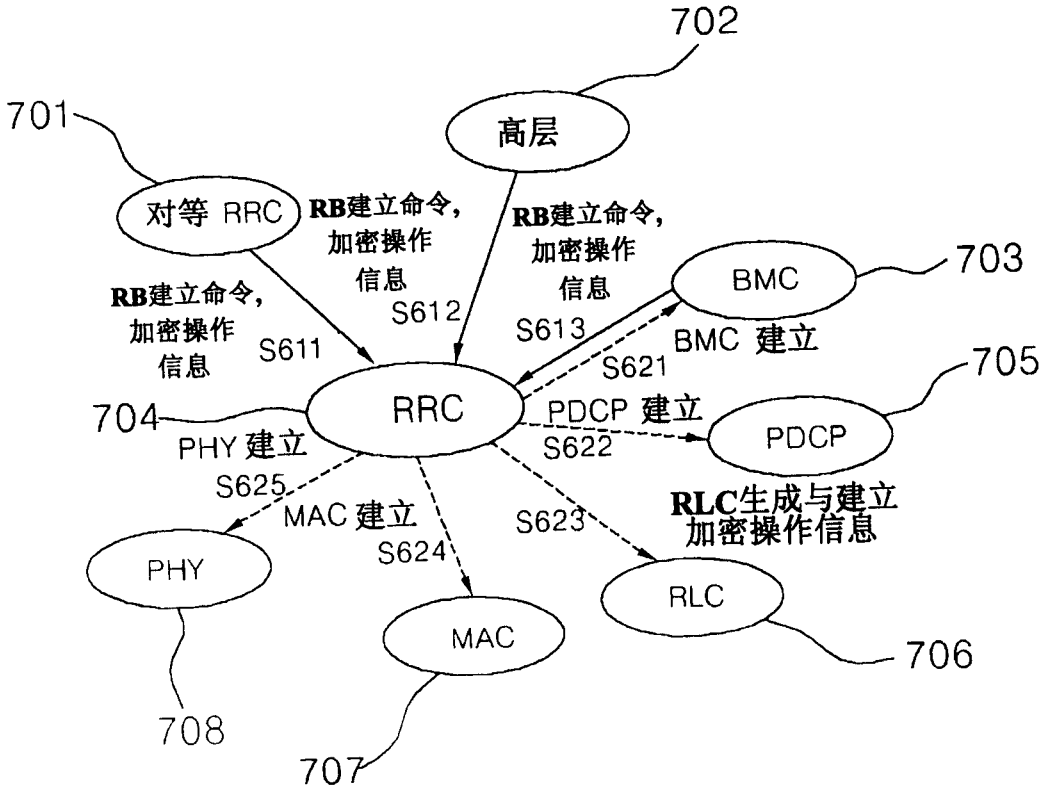
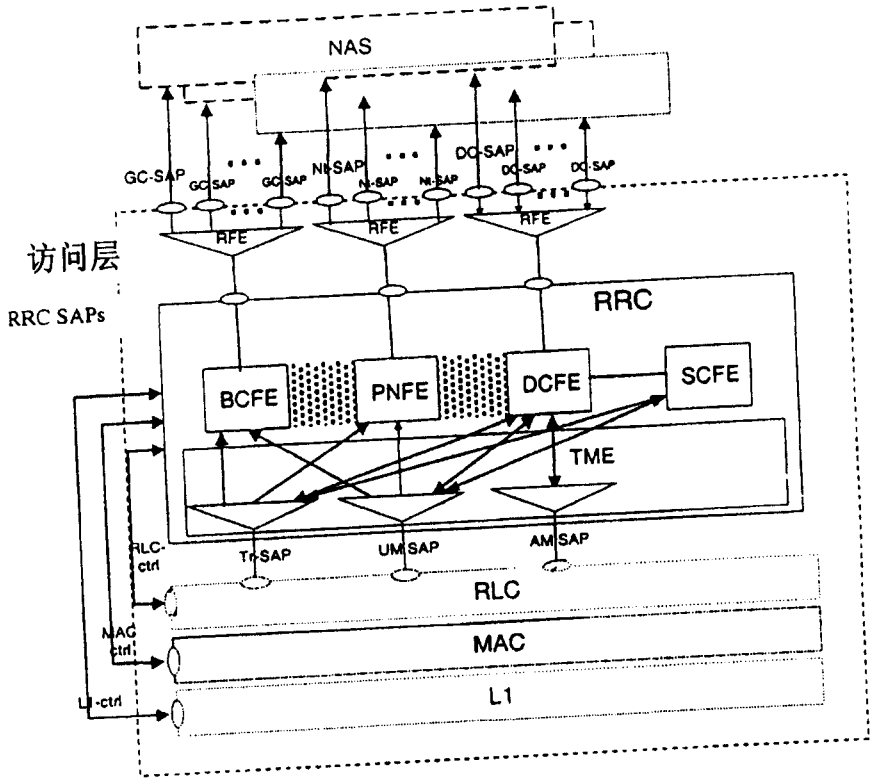

702
701
高层
对等 RRC
RB建立命令，加密操作信息
S612
RB建立命令，加密操作信息
RB建立命令，加密操作信息
S611
S613
BMC
703
BMC 建立
S621
705
704
RRC
PDCP 建立
S622
PDCP
PHY 建立
S625
MAC 建立
S624
S623
RLC生成与建立加密操作信息
PHY
MAC
RLC
706
708
707

图8


NAS
GC-SAP
NI-SAP
DC-SAP
RFE
访问层
RRC SAPs
RRC
BCFE
PNFE
DCFE
SCFE
TME
RLC-ctrl
TM-SAP
UM-SAP
AM-SAP
RLC
MAC-ctrl
MAC
L1-ctrl
L1