(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102474717 B
(45)授权公告日 2014.03.12

(21)申请号 201080031950.0
(22)申请日 2010.07.02
(30)优先权数据
2009-168130 2009.07.16 JP
(85)PCT国际申请进入国家阶段日
2012.01.16
(86)PCT国际申请的申请数据
PCT/JP2010/061352 2010.07.02
(87)PCT国际申请的公布数据
WO2011/007686 JA 2011.01.20
(73)专利权人 株式会社NTT都科摩
地址 日本东京都
(72)发明人 岩村干生 W.A.哈普萨里
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 于小宁
(51)Int.Cl.
H04W 12/04(2006.01)

审查员 傅颖

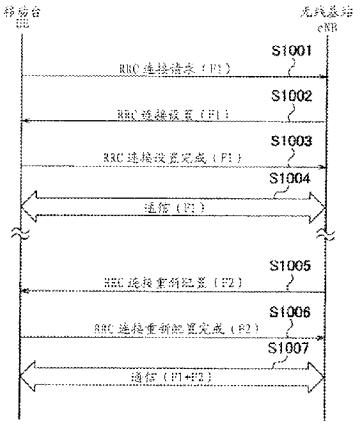
权利要求书1页 说明书5页 附图4页

(54)发明名称

移动通信系统、移动台以及无线基站

(57)摘要

本发明的移动通信系统是移动台(UE)在与无线基站(eNB)之间同时利用多个频率载波进行通信的移动通信系统，移动台(UE)对全部的多个频率载波应用(apply)相同的密钥(KeNB)进行通信的安全性处理。



CN 102474717 B

1. 一种移动通信系统，移动台在与无线基站之间，利用多个频率载波进行通信，其特征在于，

所述移动台对所述多个频率载波的全部应用相同的密钥进行通信的安全性处理，

所述移动台基于所述多个频率载波中的其中一个频率载波的物理小区 ID 以及频率码，生成所述密钥。

2. 如权利要求 1 所述的移动通信系统，其特征在于，

对所述多个频率载波的全部应用相同的安全性处理的算法。

3. 如权利要求 1 所述的移动通信系统，其特征在于，

所述多个频率载波中的其中一个频率载波是由所述无线基站指定的锚载波。

4. 如权利要求 3 所述的移动通信系统，其特征在于，

在所述锚载波被所述无线基站变更的情况下，所述移动台基于变更后的所述锚载波的物理小区 ID 以及频率码，生成所述密钥。

5. 一种移动台，其特征在于，

具有在与无线基站之间同时利用多个频率载波进行通信的通信单元，

所述通信单元对所述多个频率载波的全部应用相同的密钥进行通信的安全性处理，

所述移动台具有密钥生成单元，基于所述多个频率载波中的其中一个频率载波的物理小区 ID 以及频率码，生成所述密钥。

6. 如权利要求 5 所述的移动台，其特征在于，

所述通信单元对所述多个频率载波的全部利用相同的安全性处理的算法。

7. 如权利要求 5 所述的移动台，其特征在于，

所述多个频率载波中的其中一个频率载波是由所述无线基站指定的锚载波。

8. 如权利要求 7 所述的移动台，其特征在于，

在所述锚载波被所述无线基站变更的情况下，所述密钥生成单元基于变更后的所述锚载波的物理小区 ID 以及频率码，生成所述密钥。

9. 一种无线基站，其特征在于，

包括在与移动台之间同时利用多个频率载波进行通信的通信单元，

所述通信单元对所述多个频率载波的全部应用相同的密钥进行通信的安全性处理，

所述无线基站具有密钥生成单元，基于所述多个频率载波中的其中一个频率载波的物理小区 ID 以及频率码，生成所述密钥。

10. 如权利要求 9 所述的无线基站，其特征在于，

所述通信单元对所述多个频率载波的全部利用相同的安全性处理的算法。

11. 如权利要求 9 所述的无线基站，其特征在于，

所述多个频率载波中的其中一个频率载波是被所述无线基站指定的锚载波。

12. 如权利要求 11 所述的无线基站，其特征在于，

在所述锚载波被变更的情况下，所述密钥生成单元基于变更后的所述锚载波的物理小区 ID 以及频率码，生成所述密钥。

移动通信系统、移动台以及无线基站

技术领域

[0001] 本发明涉及移动通信系统、移动台以及无线基站。

背景技术

[0002] 在LTE(长期演进)方式的后续的通信方式即高级LTE方式的移动通信系统中,利用以下的被称为“载波聚合(Carrier Aggregation)”的技术:移动台UE在与无线基站eNB之间,同时利用多个频率载波进行通信。

[0003] 构成“载波聚合”的频率载波被称为“分量载波”。

[0004] 各“分量载波”有时还作为独立的LTE方式的小区起作用。即,也可以将利用不同的频率载波的LTE方式的小区作为“元素载波”,进行“载波聚合”。

[0005] 从而,在高级LTE方式中,通过“载波聚合”,能够同时利用多个LTE方式的小区进行通信,其中所述多个LTE方式的小区利用不同的频率载波。

[0006] 这里,在LTE方式中,用于无线安全性处理的密钥KeNB依赖于正在通信的小区的“PCI(Physical Cell Identity,物理小区ID)”以及“E-ARFCN(E-UTRA绝对无线频率信道号码(Absolute Radio Frequency Channel Number),频率码)”这两者。

[0007] 这是因为在生成密钥KeNB时,使用将PCI以及E-ARFCN作为参数的密钥生成函数KDF(密钥导出函数(Key Derivation Function))。

[0008] 此外,该密钥KeNB根据对每个移动台UE不同的母密钥KASME而生成。从而,在LTE方式中,该密钥KeNB是小区固有(Cell specific)且移动台UE固有(UE specific)。

发明内容

[0009] 发明要解决的课题

[0010] 但是,在该高级LTE方式的移动通信系统中,存在并未规定“载波聚合”中的无线安全性处理的问题。

[0011] 因此,本发明鉴于上述的问题而完成,其目的在于提供能够适当地实现“载波聚合”中的无线安全性处理的移动通信系统、移动台以及无线基站。

[0012] 用于解决课题的手段

[0013] 本发明的第1特征是移动通信系统,移动台在与无线基站之间,同时利用多个频率载波进行通信,其要旨在于,所述移动台对所述多个频率载波的每一个应用相同的密钥进行通信。

[0014] 本发明的第2特征是移动台,其要旨在于,具有在与无线基站之间同时利用多个频率载波进行通信的通信单元,所述通信单元对所述多个频率载波的每一个应用相同的密钥进行通信的安全性处理。

[0015] 本发明的第3特征是无线基站,其要旨在于,包括在与移动台之间同时利用多个频率载波进行通信的通信单元,所述通信单元对所述多个频率载波的每一个应用相同的密钥进行通信的安全性处理。

[0016] 发明的效果

[0017] 如上说明那样，根据本发明，能够提供能够适当地实现“载波聚合”中的无线安全性处理的移动通信系统、移动台以及无线基站。

附图说明

[0018] 图 1 是本发明的第 1 实施方式的移动通信系统的整体结构图。

[0019] 图 2 是本发明的第 1 实施方式的移动通信系统的协议栈图。

[0020] 图 3 是用于说明在本发明的第 1 实施方式的移动通信系统中发送三个 PDCP-SDU 时的例子的图。

[0021] 图 4 是本发明的第 1 实施方式的移动台的功能方框图。

[0022] 图 5 是本发明的第 1 实施方式的无线基站的功能方框图。

[0023] 图 6 是表示本发明的第 1 实施方式的移动通信系统的动作的时序图。

具体实施方式

[0024] （本发明的第 1 实施方式的移动通信系统）

[0025] 参照图 1 至图 3，说明本发明的第 1 实施方式的移动通信系统。

[0026] 本实施方式的移动通信系统是高级 LTE 方式的移动通信系统，在该移动通信系统中，移动台 UE 在与无线基站 eNB 之间，能够同时利用多个频率载波进行通信，即可利用“载波聚合”。

[0027] 如图 1 所示，在本实施方式中，移动台 UE 能够同时利用根据“PCI（物理小区 ID）＝1”而确定的小区 #1 中的频率载波 F1、根据“PCI ＝ 2”而确定的小区 #2 中的频率载波 F2、根据“PCI ＝ 3”而确定的小区 #3 中的频率载波 F3 进行通信。

[0028] 这里，设小区 #1 至小区 #3 均为无线基站 eNB 下属的小区。另外，小区 #1 至小区 #3 也可以是分别独立的 LTE 方式的小区。

[0029] 如图 2 所示，在本实施方式的移动通信系统中，移动台 UE 以及无线基站 eNB 具有物理 (PHY) 层功能、MAC（媒体接入控制）层功能、RLC（无线链路控制）层功能、PDCP（分组数据汇聚协议）层功能。

[0030] PDCP 层功能进行移动台 UE 与无线基站 eNB 之间的通信中的无线安全性处理。

[0031] 此外，RLC 层功能进行 RLC 层中的重发控制，MAC 层功能进行 HARQ 重发控制。

[0032] 图 3 表示发送三个 PDCP-SDU#1 ～ #3 时的例子。

[0033] 如图 3 所示，第一，PDCP 层功能对 U- 面的 PDCP-SDU#1 ～ #3 实施加密 (Ciphering) 处理，从而生成 PDCP-PDU#1 ～ #3 后，将其交给 RLC 层功能。

[0034] 另一方面，PDCP 层功能除了对 C- 面的 PDCP-SDU#1 ～ #3 实施加密 (Ciphering) 处理之外，还附加篡改保护 (Integrity Protection) 处理用的 MAC-I，从而生成 PDCP-PDU#1 ～ #3 后，将其交给 RLC 层功能。

[0035] 第二，RLC 层功能实施分割处理 (Segmentation) 或连结处理 (Concatenation)，以便生成由调度器指定的 TBS（传输块尺寸）的 RLC-PDU#1 ～ #4，并附加 RLC 报头。

[0036] 另外，在以 AM 模式启动的情况下，RLC 层功能进行 RLC 层中的重发控制。

[0037] 第三，RLC 层功能将生成的 RLC-PDU#1 ～ #4 交给 MAC 层功能。

[0038] 第四，MAC 层功能对 RLC-PDU#1 ～ #4 附加 MAC 报头，从而生成 MAC-PDU#1 ～ #4，并利用 HARQ 重发控制，将其发送给物理层功能。

[0039] 如图 4 所示，移动台 UE 包括取得单元 11、密钥生成单元 12、通信单元 13。

[0040] 取得单元 11 从无线基站 eNB 取得用于确定该无线基站 eNB 下属的各小区的“PCI”以及用于确定在各小区中使用的频率载波的“E-ARFCN(E-UTRA Absolute Radio Frequency Channel Number)”。

[0041] 密钥生成单元 12 基于由取得单元 11 取得的“PCI”以及“E-ARFCN”，生成密钥 KeNB。

[0042] 例如，密钥生成单元 12 也可以根据密钥生成函数 KDF(PCI，E-ARFCN) 生成密钥 KeNB。

[0043] 这里，密钥 KeNB 是用于生成在 PDCP 层功能中的无线安全性处理中使用的密钥 (KUPenc、KRRCenc、KRRCint) 的密钥。

[0044] KUPenc 是 U- 面的加密处理用的密钥，KRRCenc 是 C- 面的加密处理用的密钥，KRRCint 是 C- 面的篡改保护处理用的密钥，这些均根据密钥 KeNB 而生成。

[0045] 另外，在使用“载波聚合”的情况下，密钥生成单元 12 生成对多个频率载波均应用的一个密钥 KeNB。

[0046] 此外，在使用“载波聚合”的情况下，密钥生成单元 12 对于在 PDCP 层功能中的无线安全性处理中使用的密钥 (KUPenc、KRRCenc、KRRCint)，也生成对多个频率载波均应用的一组密钥 (KUPenc、KRRCenc、KRRCint)。

[0047] 即，在使用“载波聚合”的情况下，密钥生成单元 12 基于多个频率载波中的其中一个的“PCI”以及“E-ARFCN”，具体来说基于“锚载波 (Anchor Carrier)”的“PCI”以及“E-ARFCN”，生成该密钥 KeNB。

[0048] 这里，从构成“载波聚合”的多个频率载波中，决定一个“锚载波”。

[0049] 例如，在“连接设置 (Connection Setup)”时、“安全模式命令 (Security Mode Command)”时、“重新配置 (Reconfiguration)”时、“RAT 内切换”时、“RAT 间切换”时、“重建立 (Re-establishment)”时等，从无线基站 eNB 对移动台 UE 设定“锚载波”。

[0050] 或者，“锚载波”也可以决定为移动台 UE 最初确立了 RRC 连接的频率载波。

[0051] 另外，当“锚载波”变更时，密钥生成单元 12 也可以再次基于变更后的“锚载波”的“PCI”以及“E-ARFCN”生成上述的密钥 KeNB。

[0052] 在“锚载波”变更时，也可以从无线基站 eNB 启动 eNB 内切换 (Intra-eNB handover)。在指示了 eNB 内切换的情况下，移动台 UE 也可以在变更“锚载波”的同时还更新密钥 KeNB，并与 LTE 方式的切换同样地，进行 PHY、MAC、RLC 的各层的重置处理。

[0053] 通信单元 13 由上述的物理 (PHY) 层功能、MAC 层功能、RLC 层功能、PDCP 层功能构成，并在与无线基站 eNB 之间，同时利用多个频率载波进行通信。

[0054] 另外，对于在 PDCP 层中使用的加密处理以及篡改保护处理的算法，也在多个频率载波的每一个中相同。

[0055] 在“安全模式命令”时、“重新配置”时、“RAT 内切换”时、“RAT 间切换”时、“重建立”时等，从无线基站 eNB 对移动台 UE 设定要使用的算法。

[0056] 如图 5 所示，无线基站 eNB 包括密钥生成单元 21、通信单元 22。这里，密钥生成单

元 21 具有与图 4 所示的密钥生成单元 12 相同的功能，通信单元 22 具有与图 4 所示的通信单元 13 相同的功能。

[0057] 以下，参照图 6，说明本实施方式的移动通信系统的动作。

[0058] 如图 6 所示，在步骤 S1001 中，移动台 UE 对无线基站 eNB 发送用于请求在与小区 #1 之间确立通信（RRC（无线资源控制）连接）的“RRC 连接请求”。

[0059] 在步骤 S1002 中，无线基站 eNB 对移动台 UE 发送对于在步骤 S1001 中接收到的“RRC 连接请求”的“RRC 连接设置”。

[0060] 在步骤 S1003 中，移动台 UE 对无线基站 eNB 发送“RRC 连接设置完成”。

[0061] 其结果，在步骤 S1004 中，在移动台 UE 与无线基站 eNB 之间，确立利用了频率载波 F1 的 RRC 连接，且开始经由该 RRC 连接的通信。

[0062] 此后，在步骤 S1005 中，无线基站 eNB 对移动台 UE 发送有关使用频率载波 F1 而确立的 RRC 连接的“RRC 连接重新配置”。

[0063] 该“RRC 连接重新配置”设定作为用于通信的无线资源而追加频率载波 F2。

[0064] 在步骤 S1006 中，移动台 UE 对无线基站 eNB 发送“RRC 连接重新配置完成”。

[0065] 其结果，在步骤 S1007 中，在移动台 UE 与无线基站 eNB 之间开始同时利用了频率载波 F1 以及频率载波 F2 的通信。

[0066] 同样，还能够追加其他的频率载波，并进行同时利用了三个以上的频率载波的通信。此外，还可以在通信过程中释放一部分频率载波，并变更频率载波数。

[0067] 一般来说，在高级 LTE 方式的移动通信系统中，当 HARQ 重发控制中存在残留错误的情况下，进行 RLC 层中的重发控制。

[0068] 这里，在 RLC 层中的重发中，有时通过与最初发送时不同的“分量载波 (compoment carrier)”重发 RLC-PDU。

[0069] 但是，在 RLC-PDU 中包含一个以上的加密处理后的 PDCP-PDU。从而，在依照 LTE 方式而利用依赖于各频率载波的密钥 KeNB 的情况下，存在以下的遗憾之处。

[0070] • 假设当想要利用与初次发送时不同的“分量载波”重发 RLC-PDU 的情况下，暂时释放 PDCP 层的加密，从而再次进行配合用于重发的“分量载波”的加密处理，从而必须要重新生成 RLC-PDU。

[0071] • 此外，假设在该高级 LTE 方式的移动通信系统中，当通过利用了不同的“分量载波”的连接来发送 PDCP-PDU 的每一段 (segment) 的情况下，在接收侧，接收到的 PDCP-PDU 的每一段的用于加密处理的密钥不同，PDCP-PDU 的解码处理变得非常困难。

[0072] 但是，根据本实施方式的移动通信系统，由于对用于形成 RRC 连接的多个“分量载波”使用一个密钥 KeNB，因此能够避免上述的缺陷。

[0073] 以上所述的本实施方式的特征也可以如下表现。

[0074] 本实施方式的第 1 特征是移动通信系统，该移动通信系统构成为，移动台 UE 在与无线基站 eNB 之间，通过同时利用多个频率载波进行通信，其要旨在于，移动台 UE 对全部的该频率载波应用相同的密钥 KeNB 进行通信的安全性处理。

[0075] 在本实施方式的第 1 特征中，移动台 UE 也可以基于“锚载波（多个频率载波中的其中一个）”的“PCI（物理小区 ID）”以及“E-ARFCN（频率码）”，生成该密钥 KeNB。

[0076] 在本实施方式的第 1 特征中，可以对全部的上述频率载波利用相同的安全性处理

（加密处理以及篡改防止处理）的算法。

[0077] 在本实施方式的第 1 特征中，“锚载波 (Anchor Carrier)”可以由所述无线基站来指定。

[0078] 在本实施方式的第 1 特征中，也可以在“锚载波”被无线基站 eNB 变更的情况下，移动台 UE 基于变更后的“锚载波”的“PCI”以及“E-ARFCN”，生成上述的密钥 KeNB。

[0079] 本实施方式的第 2 特征是移动台，其要旨在于，具有在与无线基站 eNB 的之间同时使用多个频率载波进行通信的通信单元 13，通信单元 13 对全部的该频率载波应用相同的密钥 KeNB 进行通信的安全性处理。

[0080] 在本实施方式的第 2 特征中，也可以包括密钥生成单元 12，其基于“锚载波”的“PCI”以及“E-ARFCN”，生成该密钥 KeNB。

[0081] 在本实施方式的第 2 特征中，通信单元 13 还可以对全部的上述频率载波使用相同的安全性处理（加密处理以及篡改防止处理）的算法。

[0082] 在本实施方式的第 2 特征中，可以由无线基站 eNB 指定“锚载波”。

[0083] 在本实施方式的第 2 特征中，也可以在“锚载波”被无线基站 eNB 变更的情况下，密钥生成单元 12 基于变更后的“锚载波”的“PCI”以及“E-ARFCN”，生成上述的密钥 eNB。

[0084] 本实施方式的第 3 特征是无线基站 eNB，其要旨在于，具有在与移动台 UE 之间，同时利用多个频率载波进行通信的通信单元 22，通信单元 22 对全部的该频率载波应用相同的密钥 KeNB 进行通信的安全性处理。

[0085] 在本实施方式的第 3 特征中，也可以包括密钥生成单元 21，其基于“锚载波”的“PCI”以及“E-ARFCN”，生成该密钥 KeNB。

[0086] 在本实施方式的第 3 特征中，通信单元 22 可以对全部的上述频率载波利用相同安全性处理（加密处理以及篡改防止处理）的算法。

[0087] 在本实施方式的第 3 特征中，也可以在“锚载波”被变更的情况下，密钥生成单元 21 基于变更后的“锚载波”的“PCI”以及“E-ARFCN”，生成上述的密钥 KeNB。

[0088] 另外，上述的无线基站 eNB 和移动台 UE 的动作可以通过硬件来实施，也可以通过由处理器执行的软件模块来实施，也可以通过两者的组合来实施。

[0089] 软件模块可以设置在 RAM（随机存取存储器）、闪存、ROM（只读存储器）、EPROM（可擦可编程只读存储器）、EEPROM（电可擦可编程只读存储器）、寄存器、硬盘、移动盘、CD-ROM 这样的任意形式的存储介质内。

[0090] 该存储介质连接到处理器，以便该处理器能够对该存储介质读写信息。此外，该存储介质也可以集成到处理器中。此外，该存储介质和处理器也可以设置在 ASIC 内。该 ASIC 可以设置在无线基站 eNB 和移动台 UE 内。此外，该存储介质以及处理器也可以作为分立部件而设置在无线基站 eNB 以及移动台 UE 内。

[0091] 以上，利用上述的实施方式详细说明了本发明，但对于本领域技术人员来说，应该明白本发明并不限定于在本说明书中说明的实施方式。本发明能够作为修正和变更方式来实施而不脱离由权利要求书的记载所决定的本发明的宗旨和范围。从而，本说明书的记载以例示说明为目的，对本发明无任何限制的意思。

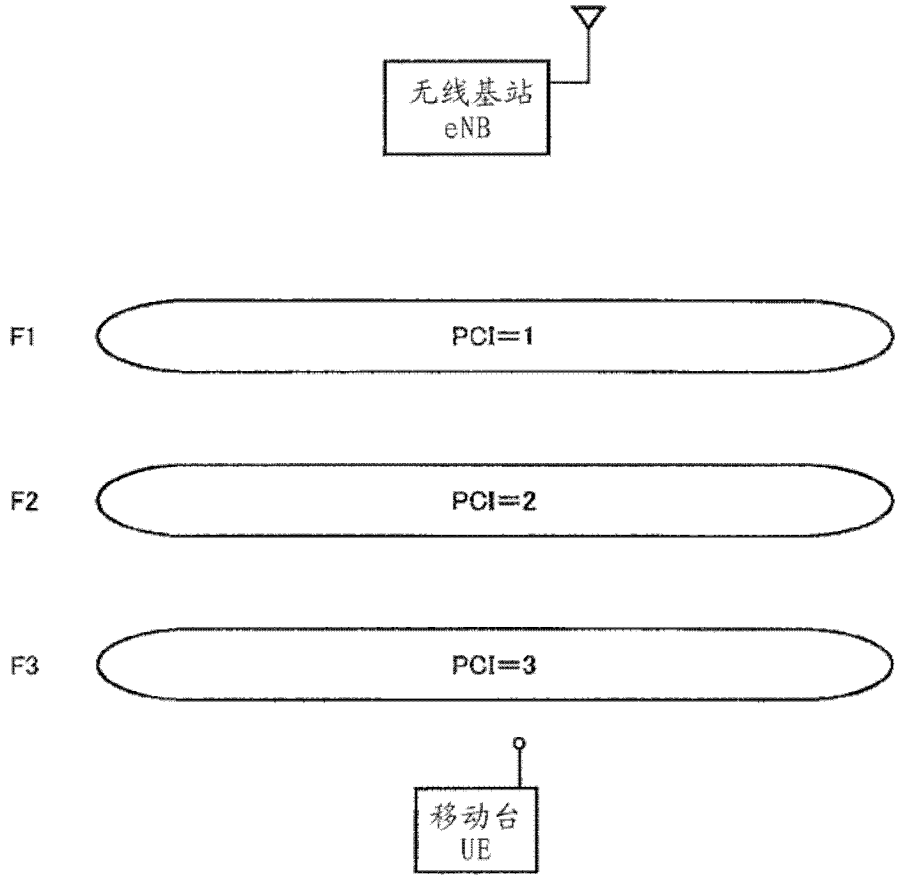

无线基站
eNB
F1
PCI=1
F2
PCI=2
F3
PCI=3
移动台
UE

图 1

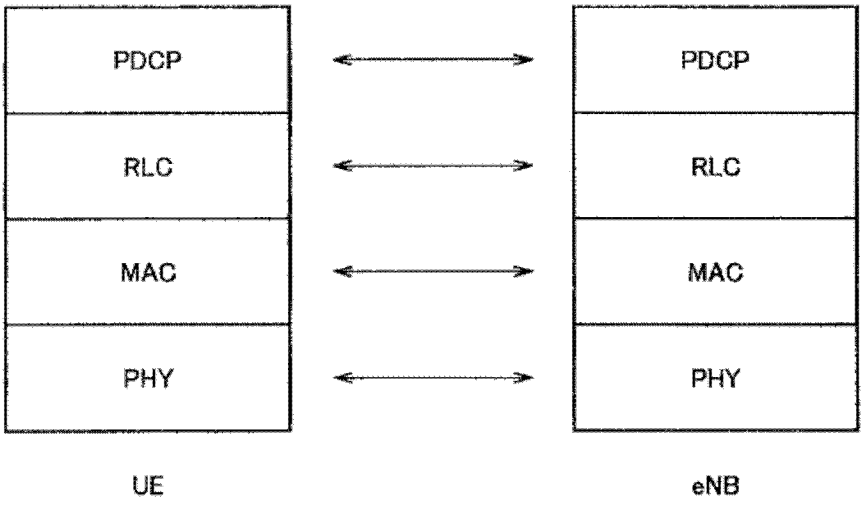

PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
UE
eNB

图 2

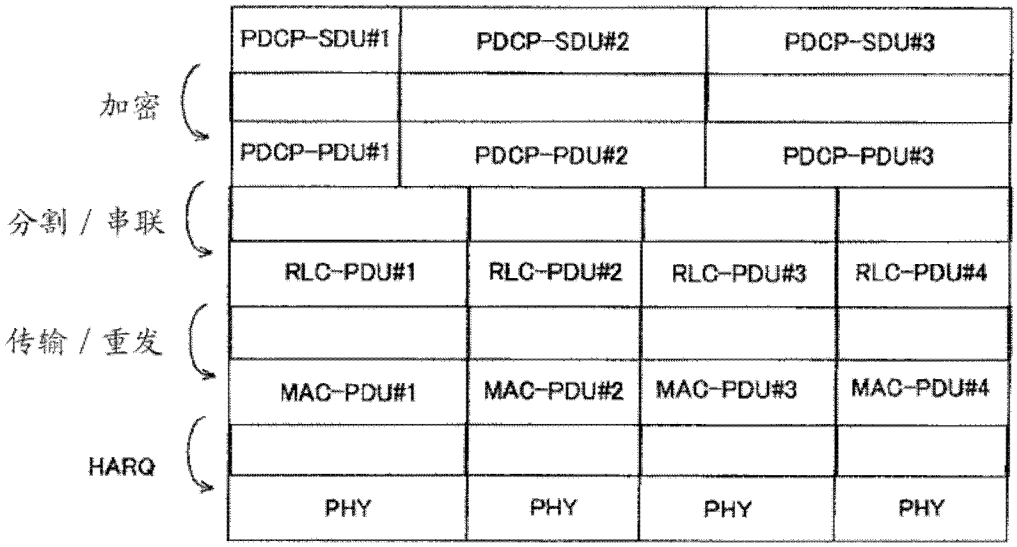

PDCP-SDU#1
PDCP-SDU#2
PDCP-SDU#3
加密
PDCP-PDU#1
PDCP-PDU#2
PDCP-PDU#3
分割 / 串联
RLC-PDU#1
RLC-PDU#2
RLC-PDU#3
RLC-PDU#4
传输 / 重发
MAC-PDU#1
MAC-PDU#2
MAC-PDU#3
MAC-PDU#4
HARQ
PHY
PHY
PHY
PHY

图 3

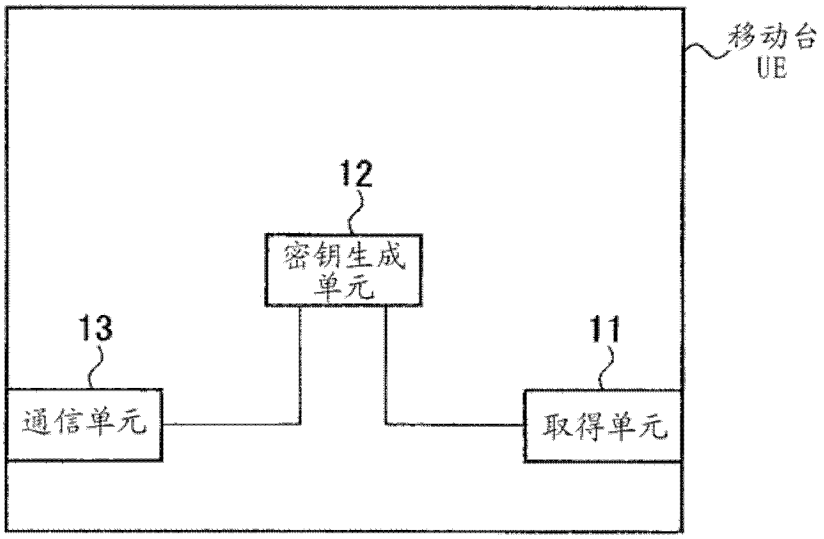

移动台
UE
12
密钥生成
单元
13
11
通信单元
取得单元

图 4

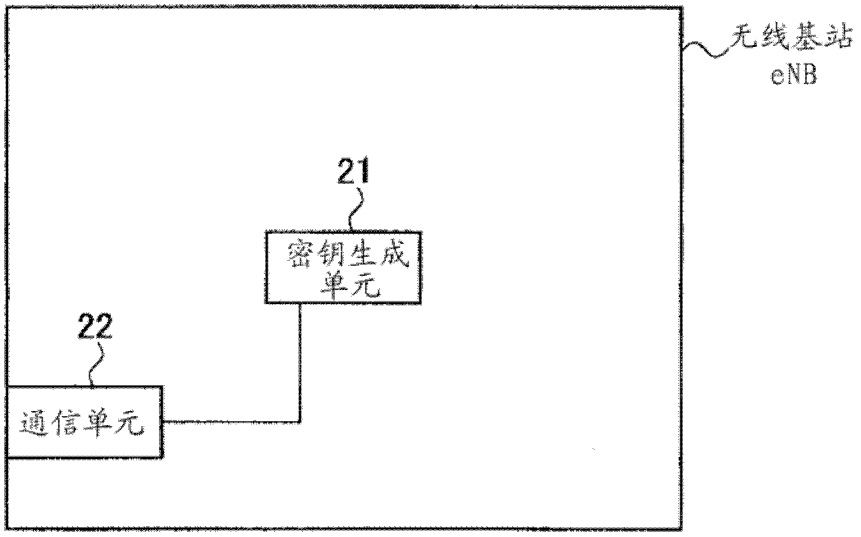


图 5

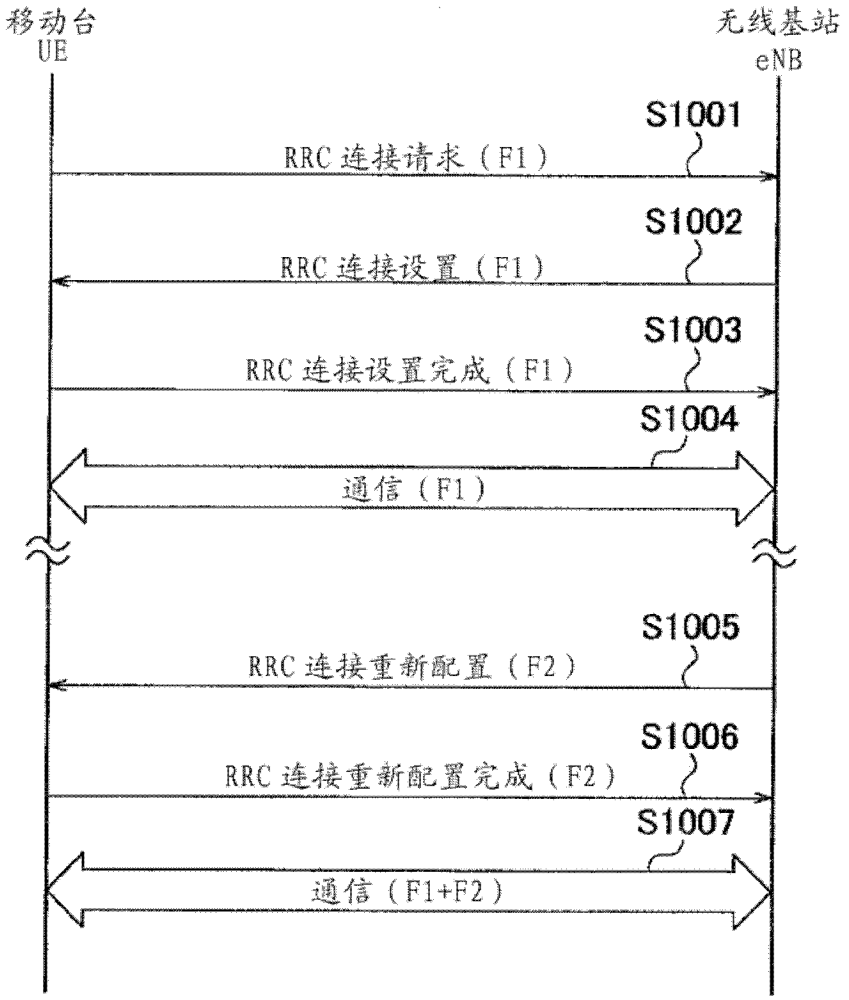

移动台
UE
无线基站
eNB
S1001
RRC 连接请求（F1）
S1002
RRC 连接设置（F1）
S1003
RRC 连接设置完成（F1）
S1004
通信（F1）
S1005
RRC 连接重新配置（F2）
S1006
RRC 连接重新配置完成（F2）
S1007
通信（F1+F2）

图 6