(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 104737569 B
(45)授权公告日 2019.07.26

(21)申请号 201380054484.1

(22)申请日 2013.10.18

(65)同一申请的已公布的文献号
申请公布号 CN 104737569 A

(43)申请公布日 2015.06.24

(30)优先权数据
13/656,112 2012.10.19 US

(85)PCT国际申请进入国家阶段日
2015.04.17

(86)PCT国际申请的申请数据
PCT/US2013/065735 2013.10.18

(87)PCT国际申请的公布数据
WO2014/063088 EN 2014.04.24

(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 A·E·埃斯科特 M·范德韦恩 A·W·登特

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 袁逸

(51)Int.Cl.
H04W 12/02(2006.01)
H04W 12/04(2006.01)
H04W 92/18(2006.01)

(56)对比文件
US 2008137853 A1,2008.06.12,
EP 1858193 A1,2007.11.21,
US 2010316223 A1,2010.12.16,

审查员 罗丽

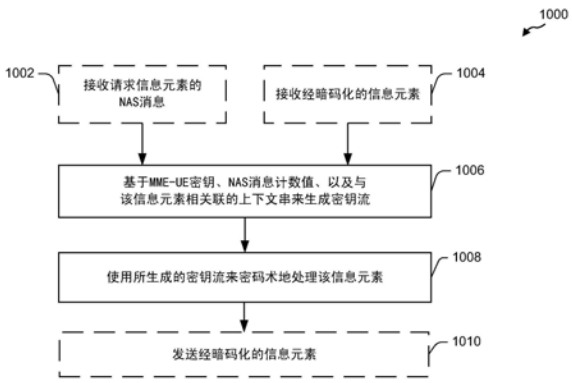
权利要求书4页 说明书12页 附图12页

(54)发明名称

用于为敏感信息的通信提供附加安全性的方法和装置

(57)摘要

提供了与为基于LTE的WWAN内敏感信息的通信提供附加安全性有关的无线通信方法、装置以及计算机程序产品。在一个示例中,通信设备被装备成基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上下文串、和上下文信息来生成密钥流,并且使用所生成的密钥流来密码术地处理该信息元素。在此类示例中,该通信设备可以是UE、MME,等等。



CN 104737569 B

1.一种无线通信的方法,包括:

基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上下文字符串来生成密钥流;并且

使用所生成的密钥流来密码术地处理所述信息元素,其中所述密码术地处理包括使用所生成的密钥流来暗码化所述信息元素、或使用所生成的密钥流来译解所述信息元素。

2.如权利要求1所述的方法,其特征在于,进一步包括:

发送经暗码化的信息元素。

3.如权利要求1所述的方法,其特征在于,进一步包括接收所述信息元素。

4.如权利要求1所述的方法,其特征在于,所述MME-UE密钥包括接入安全性管理实体(ASME)密钥(K_ASME)。

5.如权利要求2所述的方法,其特征在于,所述NAS消息计数值包括与用来传送所述经暗码化的信息元素的NAS消息相关联的NAS消息计数。

6.如权利要求2所述的方法,其特征在于,进一步包括接收触发所述密钥流的生成的NAS消息,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数值。

7.如权利要求3所述的方法,其特征在于,所述接收包括使用NAS消息来接收所述信息元素,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数。

8.如权利要求1所述的方法,其特征在于,所述上下文字符串包括与要在所述信息元素中传送的数据的类型相关联的信息。

9.如权利要求1所述的方法,其特征在于,所述上下文字符串包括与以下至少一者相关联的标识信息:发送所述信息元素的实体,或者接收所述信息元素的实体。

10.如权利要求1所述的方法,其特征在于,所述信息元素包括以下至少一者:无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符、第一UE密钥、第二UE密钥、或者最终UE密钥。

11.如权利要求2所述的方法,其特征在于,所述暗码化包括将所述密钥流直接与所述信息元素进行异或。

12.如权利要求1所述的方法,其特征在于,所生成的密钥流的长度是基于以下至少一者的:所述信息元素的长度、或者常量值。

13.如权利要求1所述的方法,其特征在于,所生成的密钥流的一部分被用作暗码化过程中的密钥。

14.如权利要求2所述的方法,其特征在于,所述发送进一步包括使用LTE NAS安全性规程来发送经暗码化的信息元素。

15.如权利要求1所述的方法,其特征在于,所述生成和处理是由UE或者MME中的至少一者执行的。

16.一种用于无线通信的设备,包括:

用于基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上下文字符串来生成密钥流的装置;以及

用于使用所生成的密钥流来密码术地处理所述信息元素的装置,其中所述密码术地处理包括使用所生成的密钥流来暗码化所述信息元素、或使用所生成的密钥流来译解所述信息元素。

17.如权利要求16所述的设备，其特征在于，进一步包括用于发送经暗码化的信息元素的装置。

18.如权利要求16所述的设备，其特征在于，进一步包括用于接收所述信息元素的装置。

19.如权利要求16所述的设备，其特征在于，所述MME-UE密钥包括接入安全性管理实体(ASME)密钥(K_ASME)。

20.如权利要求17所述的设备，其特征在于，所述NAS消息计数值包括与用来传送所述经暗码化的信息元素的NAS消息相关联的NAS消息计数。

21.如权利要求17所述的设备，其特征在于，进一步包括用于接收触发所述密钥流的生成的NAS消息的装置，并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数值。

22.如权利要求18所述的设备，其特征在于，所述用于接收的装置配置成使用NAS消息来接收所述信息元素，并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数。

23.如权利要求16所述的设备，其特征在于，所述上下文字符串包括与要在所述信息元素中传送的数据的类型相关联的信息。

24.如权利要求16所述的设备，其特征在于，所述上下文字符串包括与以下至少一者相关联的标识信息：发送所述信息元素的实体，或者接收所述信息元素的实体。

25.如权利要求16所述的设备，其特征在于，所述信息元素包括以下至少一者：无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符、第一UE密钥、第二UE密钥、或者最终UE密钥。

26.如权利要求17所述的设备，其特征在于，所述暗码化包括将所述密钥流直接与所述信息元素进行异或。

27.如权利要求16所述的设备，其特征在于，所生成的密钥流的长度是基于以下至少一者的：所述信息元素的长度、或者常量值。

28.如权利要求16所述的设备，其特征在于，所生成的密钥流的一部分被用作暗码化过程中的密钥。

29.如权利要求17所述的设备，其特征在于，所述用于发送的装置配置成使用LTE NAS安全性规程来发送经暗码化的信息元素。

30.如权利要求16所述的设备，其特征在于，所述用于生成的装置和用于处理的装置是由UE或者MME中的至少一者执行的。

31.一种用于无线通信的装置，包括：

处理系统，所述处理系统被配置成：

基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上下文字符串来生成密钥流；并且

使用所生成的密钥流来密码术地处理所述信息元素，其中所述密码术地处理包括使用所生成的密钥流来暗码化所述信息元素、或使用所生成的密钥流来译解所述信息元素。

32.如权利要求31所述的装置，其特征在于，所述处理系统被进一步配置成：

发送经暗码化的信息元素。

33.如权利要求31所述的装置,其特征在于,所述处理系统被进一步配置成:

接收所述信息元素。

34.如权利要求31所述的装置,其特征在于,所述MME-UE密钥包括接入安全性管理实体(ASME)密钥(K_ASME)。

35.如权利要求32所述的装置,其特征在于,所述NAS消息计数值包括与用来传送所述经暗码化的信息元素的NAS消息相关联的NAS消息计数。

36.如权利要求32所述的装置,其特征在于,所述处理系统进一步配置成接收触发所述密钥流的生成的NAS消息,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数值。

37.如权利要求33所述的装置,其特征在于,所述接收包括使用NAS消息来接收所述信息元素,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数。

38.如权利要求31所述的装置,其特征在于,所述上下文字符串包括与要在所述信息元素中传送的数据的类型相关联的信息。

39.如权利要求31所述的装置,其特征在于,所述上下文字符串包括与以下至少一者相关联的标识信息:发送所述信息元素的实体,或者接收所述信息元素的实体。

40.如权利要求31所述的装置,其特征在于,所述信息元素包括以下至少一者:无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符、第一UE密钥、第二UE密钥、或者最终UE密钥。

41.如权利要求32所述的装置,其特征在于,所述处理系统进一步配置成将所述密钥流直接与所述信息元素进行异或。

42.如权利要求31所述的装置,其特征在于,所生成的密钥流的长度是基于以下至少一者的:所述信息元素的长度、或者常量值。

43.如权利要求31所述的装置,其特征在于,所生成的密钥流的一部分被用作暗码化过程中的密钥。

44.如权利要求32所述的装置,其特征在于,所述处理系统进一步配置成使用LTE NAS安全性规程来发送经暗码化的信息元素。

45.如权利要求31所述的装置,其特征在于,所述装置是UE或者MME中的至少一者。

46.一种计算机可读介质,其存储用于执行以下操作的代码:

基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上下文字符串来生成密钥流;并且

使用所生成的密钥流来密码术地处理所述信息元素,其中所述密码术地处理包括使用所生成的密钥流来暗码化所述信息元素、或使用所生成的密钥流来译解所述信息元素。

47.如权利要求46所述的计算机可读介质,其特征在于,进一步存储用于执行以下动作的代码:

发送经暗码化的信息元素。

48.如权利要求46所述的计算机可读介质,其特征在于,进一步存储用于执行以下动作的代码:

接收所述信息元素。

49.如权利要求46所述的计算机可读介质,其特征在于,所述MME-UE密钥包括接入安全

性管理实体(ASME)密钥(K_ASME)。

50.如权利要求47所述的计算机可读介质,其特征在于,所述NAS消息计数值包括与用来传送所述经暗码化的信息元素的NAS消息相关联的NAS消息计数。

51.如权利要求47所述的计算机可读介质,其特征在于,进一步存储用于接收触发所述密钥流的生成的NAS消息的代码,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数值。

52.如权利要求48所述的计算机可读介质,其特征在于,进一步存储用于使用NAS消息来接收所述信息元素的代码,并且其中所述NAS消息计数值包括与接收到的NAS消息相关联的NAS消息计数。

53.如权利要求46所述的计算机可读介质,其特征在于,所述上下文字符串包括与要在所述信息元素中传送的数据的类型相关联的信息。

54.如权利要求46所述的计算机可读介质,其特征在于,所述上下文字符串包括与以下至少一者相关联的标识信息:发送所述信息元素的实体,或者接收所述信息元素的实体。

55.如权利要求46所述的计算机可读介质,其特征在于,所述信息元素包括以下至少一者:无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符、第一UE密钥、第二UE密钥、或者最终UE密钥。

56.如权利要求47所述的计算机可读介质,其特征在于,进一步存储用于将所述密钥流直接与所述信息元素进行异或的代码。

57.如权利要求46所述的计算机可读介质,其特征在于,所生成的密钥流的长度是基于以下至少一者的:所述信息元素的长度、或者常量值。

58.如权利要求46所述的计算机可读介质,其特征在于,所生成的密钥流的一部分被用作暗码化过程中的密钥。

59.如权利要求47所述的计算机可读介质,其特征在于,进一步存储用于使用LTE NAS安全性规程来发送经暗码化的信息元素的代码。

60.如权利要求46所述的计算机可读介质,其特征在于,所述用于生成的代码和用于处理的代码是由UE或者MME中的至少一者执行的。

用于为敏感信息的通信提供附加安全性的方法和装置

背景技术

[0001] 领域

[0002] 本公开一般涉及通信系统，并且尤其涉及提供用于基于长期演进(LTE)的无线广域网(WWAN)中敏感信息(诸如密钥)的通信的安全结构。。

[0003] 背景

[0004] 无线通信系统被广泛部署以提供诸如电话、视频、数据、消息收发、和广播等各种电信服务。典型的无线通信系统可采用能够通过共享可用的系统资源(例如，带宽、发射功率)来支持与多用户通信的多址技术。这类多址技术的示例包括码分多址(CDMA)系统、时分多址(TDMA)系统、频分多址(FDMA)系统、正交频分多址(OFDMA)系统、单载波频分多址(SC-FDMA)系统、和时分同步码分多址(TD-SCDMA)系统。

[0005] 这些多址技术已在各种电信标准中被采纳以提供使不同的无线设备能够在城市、国家、地区、以及甚至全球级别上进行通信的共同协议。电信标准的一示例是长期演进(LTE)。LTE是对由第三代伙伴项目(3GPP)颁布的通用移动电信系统(UMTS)移动标准的增强集。LTE被设计成通过提高频谱效率、降低成本、改善服务、利用新频谱、以及与在下行链路(DL)上使用OFDMA、在上行链路(UL)上使用SC-FDMA以及使用多输入多输出(MIMO)天线技术的其他开放标准更好地整合来更好地支持移动宽带因特网接入。LTE可支持直接设备对设备(D2D)(对等)通信。

[0006] 许多设备可以是能在蜂窝网络中操作的。当第一设备检测到另一设备时，第一设备可以尝试与此感兴趣的设备直接通信。服务移动性管理实体(MME)可以被用来建立设备间的D2D通信链路。WWAN内不存在允许附连至LET网络的两个设备在没有共有密钥的场合执行安全D2D通信的功能性。另外，目前的LTE NAS安全性规程允许在安全性上下文建立之后，使用具有32位MAC并具有任选的暗码化(例如，对于所有消息而言，暗码化可以被任选地设置成开启或关闭)的完好性保护。即使在当暗码化选项被选择时，初始消息(即，UE在脱离空闲时所发送的第一条消息)也仅仅是具有完好性地被发送。尽管LTE NAS安全性规程可以为涉及网络接入的消息和数据提供合适的保护，但是该规程可能并非强壮到足以保护其他类型的数据(例如，用来为安全D2D通信生成密钥的密钥或者机密材料)。

[0007] 随着对D2D通信的需求有所增加，存在对为LTE内敏感信息的通信提供附加安全性而同时使得对WWAN资源的使用最小化的方法/装置的需要。

[0008] 概述

[0009] 以下给出一个或多个方面的简要概述以提供对这些方面的基本理解。此概述不是所有构想到的方面的详尽综览，并且既非旨在标识出所有方面的关键性或决定性要素亦非试图界定任何或所有方面的范围。其唯一的目的是要以简化形式给出一个或多个方面的一些概念以作为稍后给出的更加详细的描述之序。

[0010] 根据一个或多个方面及其对应公开，来描述与为基于LTE的WWAN内敏感信息的通信提供附加的安全性有关的各种方面。在一个示例中，通信设备被装备成基于移动性管理实体-用户装备(MME-UE)密钥、非接入阶层(NAS)消息计数值、以及与信息元素相关联的上

下文串、和上下文信息来生成密钥流，并且使用所生成的密钥流来密码术地处理该信息元素。在此类示例中，该通信设备可以是UE、MME，等等。

[0011] 根据相关方面，提供了用于为基于LTE的WWAN内敏感信息的通信提供附加安全性的方法。该方法可以包括基于MME-UE密钥、NAS消息计数值、以及与信息元素相关联的上下文串生成密钥流。此外，该方法可以包括使用所生成的密钥流来密码术地处理该信息元素。

[0012] 另一方面涉及配置成为基于LTE的WWAN内敏感信息的通信提供附加安全性的通信装置。该通信装置可以包括用于基于MME-UE密钥、NAS消息计数值、以及与信息元素相关联的上下文串生成密钥流的装置。此外，该通信装置可包括用于使用所生成的密钥流来密码术地处理该信息元素的装置。

[0013] 另一方面涉及一种通信装置。该装置可包括配置成基于MME-UE密钥、NAS消息计数值、以及与信息元素相关联的上下文串来生成密钥流的处理系统。此外，该处理系统可进一步配置成使用所生成的密钥流来密码术地处理该信息元素。

[0014] 还有一方面涉及计算机程序产品，其可以具有包括用于基于MME-UE密钥、NAS消息计数值、和与信息元素相关联的上下文串生成密钥流的代码。此外，该计算机可读介质可包括用于使用所生成的密钥流来密码术地处理该信息元素的代码。

[0015] 为了能达成前述及相关目的，这一个或多个方面包括在下文中充分描述并在所附权利要求中特别指出的特征。以下描述和附图详细阐述了这一个或多个方面的某些解说性特征。但是，这些特征仅仅是指示了可采用各种方面的原理的各种方式中的若干种，并且本描述旨在涵盖所有此类方面及其等效方案。

[0016] 附图简述

[0017] 图1是解说网络架构的示例的示图。

[0018] 图2是解说接入网的示例的示图。

[0019] 图3是解说LTE中的DL帧结构的示例的示图。

[0020] 图4是解说LTE中的UL帧结构的示例的示图。

[0021] 图5是解说用于用户面和控制面的无线电协议架构的示例的示图。

[0022] 图6是解说接入网中的演进型B节点和用户装备的示例的示图。

[0023] 图7是解说设备对设备通信网络的示图。

[0024] 图8是解说用于保护网络中的设备对设备通信的第一方法的呼叫流图。

[0025] 图9是解说用于保护网络中的设备对设备通信的第二方法的呼叫流图。

[0026] 图10是第一无线通信方法的流程图。

[0027] 图11是解说示例性设备中的不同模块/装置/组件之间的数据流的概念性数据流图。

[0028] 图12是解说采用处理系统的装置的硬件实现的示例的示图。

[0029] 详细描述

[0030] 以下结合附图阐述的详细描述旨在作为各种配置的描述，而无意表示可实践本文所描述的概念的仅有配置。本详细描述包括具体细节来提供对各种概念的透彻理解。然而，对于本领域技术人员将显而易见的是，没有这些具体细节也可实践这些概念。在一些实例中，以框图形式示出众所周知的结构和组件以便避免淡化此类概念。

[0031] 现在将参照各种装置和方法给出电信系统的若干方面。这些装置和方法将在以下

详细描述中进行描述并在附图中由各种框、模块、组件、电路、步骤、过程、算法等(统称为“元素”)来解说。这些元素可使用电子硬件、计算机软件或其任何组合来实现。此类元素是实现成硬件还是软件取决于具体应用和加诸于整体系统上的设计约束。

[0032] 作为示例,元素、或元素的任何部分、或者元素的任何组合可用包括一个或多个处理器的“处理系统”来实现。处理器的示例包括:微处理器、微控制器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编程逻辑器件(PLD)、状态机、门控逻辑、分立的硬件电路以及其他配置成执行本公开中通篇描述的各种功能性的合适硬件。处理系统中的一个或多个处理器可以执行软件。软件应当被宽泛地解释成意为指令、指令集、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行件、执行的线程、规程、函数等,无论其是用软件、固件、中间件、微代码、硬件描述语言、还是其他术语来述及皆是如此。

[0033] 相应地,在一个或多个示例性实施例中,所描述的功能可被实现在硬件、软件、固件,或其任何组合中。如果被实现在软件中,那么这些功能可作为一条或多条指令或代码被存储或编码在计算机可读介质上。计算机可读介质包括计算机存储介质。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限制,此类计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储、磁盘存储或其他磁存储设备、或能被用来携带或存储指令或数据结构形式的期望程序代码且能被计算机访问的任何其他介质。如本文中所使用的盘(disk)和碟(disc)包括压缩碟(CD)、激光碟、光碟、数字多用碟(DVD)、软盘和蓝光碟,其中盘常常磁性地再现数据,而碟用激光来光学地再现数据。上述的组合也应被包括在计算机可读介质的范围内。

[0034] 图1是解说LTE网络架构100的示图。LTE网络架构100可被称为演进型分组系统(EPS)100。EPS 100可包括一个或多个用户装备(UE)102、演进型UMTS地面无线电接入网(E-UTRAN)104、演进型分组核心(EPC)110、归属订户服务器(HSS)120以及运营商的IP服务122。EPS可与其他接入网互连,但出于简化起见,那些实体/接口并未示出。如图所示,EPS提供分组交换服务,然而,如本领域技术人员将容易领会的,本公开中通篇给出的各种概念可被扩展到提供电路交换服务的网络。

[0035] E-UTRAN包括演进型B节点(eNB)106和其他eNB 108。eNB 106提供朝向UE 102的用户面和控制面的协议终接。eNB 106可经由回程(例如,X2接口)连接到其他eNB 108。eNB 106也可称为基站、基收发机站、无线电基站、无线电收发机、收发机功能、基本服务集(BSS)、扩展服务集(ESS)、或其他某个合适的术语。eNB 106为UE 102提供去往EPC 110的接入点。UE102的示例包括蜂窝电话、智能电话、会话发起协议(SIP)电话、膝上型设备、个人数字助理(PDA)、卫星无线电、全球定位系统、多媒体设备、视频设备、数字音频播放器(例如,MP3播放器)、相机、游戏控制台、或任何其他类似的功能设备。UE 102也可被本领域技术人员称为移动站、订户站、移动单元、订户单元、无线单元、远程单元、移动设备、无线设备、无线通信设备、远程设备、移动订户站、接入终端、移动终端、无线终端、远程终端、手持机、用户代理、移动客户端、客户端、或其他某个合适的术语。

[0036] eNB 106通过S1接口连接到EPC 110。EPC 110包括移动性管理实体(MME)112、其他MME 114、服务网关116、以及分组数据网络(PDN)网关118。MME 112是处理UE 102与EPC 110之间的信令的控制节点。一般而言,MME 112提供承载和连接管理。所有用户IP分组通过服

务网关116来传递，服务网关116自身连接到PDN网关118。PDN网关118提供UE IP地址分配以及其他功能。PDN网关118连接到运营商的IP服务122。运营商的IP服务122可包括因特网、内联网、IP多媒体子系统(IMS)、以及PS流送服务(PSS)。

[0037] 图2是解说LTE网络架构中的接入网200的示例的示图。在这一示例中，接入网200被划分成数个蜂窝区划(蜂窝小区)202。一个或多个较低功率类eNB 208可具有与这些蜂窝小区202中的一个或多个蜂窝小区交叠的蜂窝区划210。较低功率类eNB 208可以是毫微微蜂窝小区(例如，家用eNB(HeNB))、微微蜂窝小区、微蜂窝小区或远程无线电头端(RRH)。宏eNB 204各自被指派给相应各个蜂窝小区202并且被配置成为蜂窝小区202中的所有UE 206、212提供去往EPC 110的接入点。UE 212中的一些可以处于设备对设备通信中。在接入网200的这一示例中，没有集中式控制器，但是在替换性配置中可以使用集中式控制器。eNB 204负责所有与无线电有关的功能，包括无线电承载控制、准入控制、移动性控制、调度、安全性、以及与服务网关116的连通性。

[0038] 接入网200所采用的调制和多址方案可以取决于正部署的特定电信标准而变化。在LTE应用中，在DL上使用OFDM并且在UL上使用SC-FDMA以支持频分双工(FDD)和时分双工(TDD)两者。如本领域技术人员将容易地从以下详细描述中领会的，本文给出的各种概念良好地适用于LTE应用。然而，这些概念可以容易地扩展到采用其他调制和多址技术的其他电信标准。作为示例，这些概念可被扩展到演进数据最优化(EV-DO)或超移动宽带(UMB)。EV-DO和UMB是由第三代伙伴项目2(3GPP2)颁布的作为CDMA2000标准族的一部分的空中接口标准，并且采用CDMA向移动站提供宽带因特网接入。这些概念还可被扩展到采用宽带CDMA(W-CDMA)和其他CDMA变体(诸如TD-SCDMA)的通用地面无线电接入(UTRA)；采用TDMA的全球移动通信系统(GSM)；以及采用OFDMA的演进型UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20和Flash-OFDM。UTRA、E-UTRA、UMTS、LTE和GSM在来自3GPP组织的文献中描述。CDMA2000和UMB在来自3GPP2组织的文献中描述。所采用的实际无线通信标准和多址技术将取决于具体应用以及加诸于系统的整体设计约束。

[0039] 图3是解说LTE中的DL帧结构的示例的示图300。帧(10ms)可被划分成10个相等大小的子帧。每个子帧可包括2个连贯的时隙。可使用资源网格来表示2个时隙，每个时隙包括资源块(RB)。该资源网格被划分成多个资源元素。在LTE中，资源块包含频域中的12个连贯副载波，并且对于每个OFDM码元中的正常循环前缀而言，包含时域中的7个连贯OFDM码元，或即包含84个资源元素。对于扩展循环前缀而言，资源块包含时域中的6个连贯OFDM码元，并具有72个资源元素。物理DL控制信道(PDCCH)、物理DL共享信道(PDSCH)以及其他信道可被映射到各资源元素。

[0040] 图4是解说LTE中的UL帧结构的示例的示图400。用于UL的可用资源块可分割成数据区段和控制区段。该控制区段可形成在系统带宽的2个边缘处并且可具有可配置大小。该控制区段中的这些资源块可被指派给UE用于控制信息的传输。该数据区段可包括所有不被包括在控制区段中的资源块。该UL帧结构导致该数据区段包括毗连的副载波，这可允许单个UE被指派该数据区段中的所有毗连副载波。

[0041] UE可被指派控制区段中的资源块410a、410b以向eNB传送控制信息。该UE还可被指派数据区段中的资源块420a、420b以向eNB传送数据。该UE可在该控制区段中获指派的资源块上在物理UL控制信道(PUCCH)中传送控制信息。该UE可在该数据区段中获指派的资源块

上在物理UL共享信道(PUSCH)中仅传送数据或传送数据和控制信息两者。UL传输可横跨子帧的这两个时时隙并且可跨频率跳跃。

[0042] 资源块集合可被用于在物理随机接入信道(PRACH)430中执行初始系统接入并达成UL同步。PRACH 430携带随机序列并且不能携带任何UL数据/信令。每个随机接入前置码占用与6个连贯资源块相对应的带宽。起始频率由网络来指定。即,随机接入前置码的传输被限制于某些时频资源。对于PRACH不存在跳频。PRACH尝试被携带在单个子帧(1ms)中或在数个毗连子帧的序列中,并且UE每帧(10ms)可仅作出单次PRACH尝试。

[0043] 图5是解说LTE中用于用户面和控制面的无线电协议架构的示例的示图500。用于UE 502和eNB的无线电协议架构被示为具有三层:层1、层2和层3。数据/信令的通信522可以跨这三个层在UE 502与eNB之间进行。层1(L1层)是最低层并实现各种物理层信号处理功能。L1层将在本文中被称为物理层506。层2(L2层)508在物理层506之上并且负责UE与eNB之间在物理层506之上的链路。

[0044] 在用户面中,L2层508包括媒体接入控制(MAC)子层510、无线电链路控制(RLC)子层512、以及分组数据汇聚协议(PDCP)514子层,它们在网络侧上终接于eNB处。尽管未示出,但是UE在L2层508上方可具有若干个上层,包括在网络侧终接于PDN网关118处的网络层(例如,IP层)、以及终接于连接的另一端(例如,远端UE、服务器等)处的应用层。

[0045] PDCP子层514提供不同无线电承载与逻辑信道之间的复用。PDCP子层514还提供对上层数据分组的报头压缩以减少无线电传输开销,通过将数据分组暗码化来提供安全性,以及提供对UE在各eNB之间的切换支持。RLC子层512提供对上层数据分组的分段和重装、对丢失数据分组的重传、以及对数据分组的重排序以补偿由于混合自动重复请求(HARQ)引起的脱序接收。MAC子层510提供逻辑信道与传输信道之间的复用。MAC子层510还负责在各UE间分配一个蜂窝小区中的各种无线电资源(例如,资源块)。MAC子层510还负责HARQ操作。

[0046] 在控制面中,用于UE和eNB的无线电协议架构对于物理层506和L2层508而言基本相同,区别在于对控制面而言没有头部压缩功能。控制面还包括层3(L3层)中的无线电资源控制(RRC)子层516和NAS子层522。RRC子层516负责获得无线电资源(即,无线电承载)以及负责使用eNB与UE 502之间的RRC信令来配置各下层。NAS子层522负责支持会话管理规程以为UE502建立和维护IP连通性,并且支持UE 502与MME之间在无线电接口处的控制面通信。NAS子层522提供支持UE 502与分组数据网络网关(PDN GW)之间的移动性的协议。NAS子层522协议可以被用来执行EPS承载管理、验证、EPS连接管理(ECM)空闲移动性处置、ECM空闲中的寻呼始发、安全性控制等。

[0047] 用户面还包括网际协议(IP)子层518和应用层520。IP子层518和应用子层520负责支持eNB 504与UE 502之间的应用数据通信。

[0048] 图6是接入网中WAN实体(例如,eNB、MME等)610与UE 650处于通信的框图。在DL中,来自核心网的上层分组被提供给控制器/处理器675。控制器/处理器675实现L2层的功能性。在DL中,控制器/处理器675提供报头压缩、暗码化、分组分段和重排序、逻辑信道与传输信道之间的复用、以及基于各种优先级度量对UE 650的无线电资源分配。控制器/处理器675还负责HARQ操作、丢失分组的重传、以及对UE 650的信令。

[0049] 发射(TX)处理器616实现用于L1层(即,物理层)的各种信号处理功能。这些信号处理功能包括编码和交织以促成UE 650处的前向纠错(FEC)以及基于各种调制方案(例如,二

进制相移键控(BPSK)、正交相移键控(QPSK)、M相移键控(M-PSK)、M正交振幅调制(M-QAM))向信号星座进行的映射。随后,经编码和调制的码元被拆分成并行流。每个流随后被映射到OFDM副载波、在时域和/或频域中与参考信号(例如,导频)复用、并且随后使用快速傅里叶逆变换(IFFT)组合到一起以产生携带时域OFDM码元流的物理信道。该OFDM流被空间预编码以产生多个空间流。来自信道估计器674的信道估计可被用来确定编码和调制方案以及用于空间处理。该信道估计可以从由UE 650传送的参考信号和/或信道状况反馈推导出来。每个空间流随后经由分开的发射机618TX被提供给一不同的天线620。每个发射机618TX用各自的空间流来调制RF载波以供传输。

[0050] 在UE 650处,每个接收机654RX通过其各自相应的天线652来接收信号。每个接收机654RX恢复出调制到RF载波上的信息并将该信息提供给接收(RX)处理器656。RX处理器656实现L1层的各种信号处理功能。RX处理器656对该信息执行空间处理以恢复出以UE 650为目的地的任何空间流。如果有多个空间流以UE 650为目的地,那么它们可由RX处理器656组合成单个OFDM码元流。RX处理器656随后使用快速傅里叶变换(FFT)将该OFDM码元流从时域转换到频域。该频域信号对该OFDM信号的每个副载波包括单独的OFDM码元流。通过确定最有可能由WAN实体610传送了的信号星座点来恢复和解调每个副载波上的码元、以及参考信号。这些软判决可以基于由信道估计器658计算出的信道估计。这些软判决随后被解码和解交织以恢复出原始由WAN实体610在物理信道上传输的数据和控制信号。这些数据和控制信号随后被提供给控制器/处理器659。

[0051] 控制器/处理器659实现L2层。控制器/处理器可以与存储程序代码和数据的存储器660相关联。存储器660可称为计算机可读介质。在UL中,控制器/处理器659提供传输信道与逻辑信道之间的分用、分组重装、去暗码化、报头解压缩、控制信号处理以恢复出来自核心网的上层分组。这些上层分组随后被提供给数据阱662,数据阱662代表L2层之上的所有协议层。各种控制信号也可被提供给数据阱662以进行L3处理。控制器/处理器659还负责使用确收(ACK)和/或否定确收(NACK)协议进行检错以支持HARQ操作。

[0052] 在UL中,数据源667被用来将上层分组提供给控制器/处理器659。数据源667代表L2层之上的所有协议层。类似于结合由WAN实体610进行的DL传输所描述的功能性,控制器/处理器659通过提供头部压缩、暗码化、分组分段和重排序、以及基于由网络实体610进行的无线电资源分配在逻辑信道与传输信道之间进行复用,来实现用户面和控制面的L2层。控制器/处理器659还负责HARQ操作、丢失分组的重传、以及向WAN实体610的信令。

[0053] 由信道估计器658从由WAN实体610所传送的参考信号或者反馈推导出的信道估计可由TX处理器668用来选择恰适的编码和调制方案以及促成空间处理。由TX处理器668生成的诸空间流经由分开的发射机654TX提供给不同的天线652。每个发射机654TX用各自的空间流来调制RF载波以供传送。

[0054] 在WAN实体610处以与结合UE 650处的接收机功能所描述的方式相类似的方式来处理UL传输。每个接收机618RX通过其相应各个天线620来接收信号。每个接收机618RX恢复出被调制到RF载波上的信息并将该信息提供给RX处理器670。RX处理器670可实现L1层。

[0055] 控制器/处理器675实现L2层。控制器/处理器675可以与存储程序代码和数据的存储器676相关联。存储器676可称为计算机可读介质。在UL中,控制/处理器675提供传输信道与逻辑信道之间的分用、分组重组、去暗码化、头部解压缩、控制信号处理以恢复出来自UE

650的上层分组。来自控制器/处理器675的上层分组可被提供给核心网。控制器/处理器675还负责使用ACK和/或NACK协议进行检错以支持HARQ操作。

[0056] 图7是设备对设备通信系统700的示图。设备对设备通信系统700包括多个无线设备704、706、708、710，一个或多个基站(eNodeB 702、712)以及一个或多个MME(714、716)。

[0057] 设备对设备通信系统700可与蜂窝通信系统(诸如举例而言，无线广域网(WWAN))相交叠。无线设备704、706、708、710中的一些可以使用DL/ULWWAN频谱以设备对设备通信的形式来一起通信，一些可与基站702和/或基站712通信，而一些可以这两种通信皆进行。在另一方面，WWAN可包括多个基站(702、712)，该多个基站(702、712)可通过经由一个或多个网络实体(例如，MME 714、716)提供的连通性来提供协调式通信环境。

[0058] 例如，如图7中所示，无线设备708、710处于设备对设备通信中，而无线设备704、706处于设备对设备通信中。无线设备704、706还正与基站702通信。

[0059] 在一操作性方面，设备704和设备706可以使用通过来自MME 714和/或MME 716的协助而生成的密钥来执行安全D2D通信。

[0060] 图8和9解说了呼叫流图，这些呼叫流图解说其中一个或多个MME可以协助UE进行密钥生成的各种配置。图8和9所给出的呼叫流图是作为示例实现来提供的，并且本领域技术人员将会理解本文中所描述的主题内容并不限于在这些附图中所阐述的具体示例。

[0061] 图8是包括第一UE 802(UE(1))、服务第一UE的MME 804(MME(1))、服务第二UE的MME 806(MME(2))和第二UE 808(UE(2))的通信网络800的呼叫流图。虽然通信网络800中示出了两个MME，但是本领域普通技术人员将会认识到，该呼叫流图中所描述的方法可由任何数目的MME(独自或者联合)执行。如进一步参照图10所描述的，包括在本文中所描述的一个或多个NAS消息中的信息元素可以使用密钥流来被密码术地处理(加密/解密)。在此类方面，可以基于MME-UE密钥、NAS消息计数值、以及与信息元素相关联的上下文串来生成该密钥流。

[0062] 在动作810，UE(1)802和UE(2)808可以决定要尝试建立安全D2D通信链路。在动作812，UE(1)802可以向MME(1)804发送NAS消息，该NAS消息指示要与UE(2)808建立共享密钥的意图。该NAS消息可以包括第一UE密钥。在另一方面，在动作814，MME(1)804可以从MME(1)804和UE(1)802已知的值来计算第一UE密钥，并且在动作816，UE(1)802可以从相同值计算第一UE密钥。

[0063] 类似地，在动作818，UE(2)808可以向MME(2)806发送NAS消息，该NAS消息指示要与UE(1)802建立共享密钥的意图。该NAS消息可以包含第二UE密钥。在另一方面，在动作820，MME(2)可以从MME(2)806和UE(2)808已知的值来计算第二UE密钥，并且在动作822，UE(2)808可以从相同值计算第二UE密钥。

[0064] 在动作824，在如于所描绘的呼叫流图中所描述的那样有多个MME的场合，MME(1)可以向MME(2)提供第一UE密钥和UE(1)802的标识符。进一步，MME(2)可以向MME(1)提供第二UE密钥和UE(2)808的标识符。

[0065] 方框826中描述了一任选方面。在动作828，MME(1)804可以从第一UE密钥和第二UE密钥计算最终UE密钥。进一步，在动作830，MME(2)806可以从第一UE密钥和第二UE密钥计算最终UE密钥。在另一方面，MME(804、806)之一可以计算最终UE密钥并且将该最终UE密钥发送给另一MME。

[0066] 在动作832，MME(1)804可以至少发送第二UE(2)808被联系上了的确认。在一方面，MME(1)804可以向第一UE(1)802发送第二UE密钥。在另一方面，MME(1)804可以向第一UE发送最终UE密钥。类似地，在动作834，MME(2)806可以向第二UE(2)808发送第一UE密钥。在一方面，MME(2)806可以向第二UE(2)808发送最终UE密钥。在敏感信息(例如，第一UE密钥、第二UE密钥、最终UE密钥等)被传送的方面，可以实现附加的安全性规程。此类规程的进一步讨论参考图10来提供。

[0067] 方框836中描述了另一任选的方面。在动作838，UE(1)802可以至少基于第一UE密钥来计算最终UE密钥。在另一方面，UE(1)802可以基于第一UE密钥和第二UE密钥来计算最终UE密钥。类似地，在动作840，UE(2)808可以基于第一UE密钥和第二UE密钥来计算最终UE密钥。

[0068] 此后，在动作842，UE(1)802和UE(2)808可以执行安全D2D通信。

[0069] 图9是包括第一UE 902(UE(1))、服务第一UE的MME 904(MME(1))、服务第二UE的MME 906(MME(2))和第二UE 908(UE(2))的通信网络900的另一呼叫流图。虽然通信网络900中示出了两个MME，但是本领域普通技术人员将会认识到，该呼叫流图中所描述的方法可由任何数目的MME(独自或者联合)执行。如进一步参照图10所描述的，在本文中所描述的一个或多个NAS消息中所包括的信息元素可以使用密钥流来被密码术地处理(加密/解密)。在此类方面，可以基于MME-UE密钥、NAS消息计数值、以及与该信息元素相关联的上下文串来生成密钥流。

[0070] 在动作910，UE(1)902可以检测UE(2)908的存在，并且可以决定要尝试建立与UE(2)908的安全D2D通信链路。在动作912，UE(1)902可以向MME(1)904发送NAS消息，该NAS消息指示要与UE(2)908建立共享密钥的意图。该消息可以包括第一UE密钥。在另一方面，在动作914，MME(1)904可以从MME(1)904和UE(1)902已知的值来计算第一UE密钥，并且在动作916，UE(1)902可以从相同值计算第一UE密钥。

[0071] 在动作918，MME(1)904可以向MME(2)提供第一UE密钥和第二UE(2)908标识符。在动作920，MME(2)906可以寻呼UE(2)908，并且在动作922，UE(2)可以响应该寻呼。在一方面，UE(2)908可以用包含第二UE密钥的NAS消息作出响应。

[0072] 在另一方面，在动作924，MME(2)906可以从MME(2)906和UE(2)908已知的值计算第二UE密钥。在动作926，可以将第二UE密钥从MME(2)906发送到MME(1)904。

[0073] 方框928中描述了一任选的方面。在动作930，MME(1)904可以从第一UE密钥和第二UE密钥计算最终UE密钥。进一步，在动作932，MME(2)906可以从第一UE密钥和第二UE密钥计算最终UE密钥。在另一方面，MME(904、906)之一可以计算最终UE密钥并且将该最终UE密钥发送给另一MME。

[0074] 在动作934，MME(1)904可以至少发送第二UE(2)908被联系上了的确认。在一方面，MME(1)904可以向第一UE(1)902发送第二UE密钥。在另一方面，MME(1)904可以向第一UE发送最终UE密钥。类似地，在动作936，MME(2)906可以向第二UE(2)908发送第一UE密钥。在一方面，MME(2)906可以向第二UE(2)908发送最终UE密钥。在敏感信息(例如，第一UE密钥、第二UE密钥、最终UE密钥等)被传送的方面，可以实现附加的安全性规程。此类规程的进一步讨论参考图10来提供。

[0075] 方框938中描述了另一任选的方面。在动作940，UE(2)908可以从MME(2)906和UE

(2)908已知的值计算第二UE密钥。在动作940,UE(1)902可以至少基于第一UE密钥来计算最终UE密钥。在另一方面,UE(1)902可以基于第一UE密钥和第二UE密钥来计算最终UE密钥。类似地,在动作944,UE(2)908可以基于第一UE密钥和第二UE密钥来计算最终UE密钥。

[0076] 在此之后,在动作946,UE(1)902和UE(2)908可以执行安全D2D通信。

[0077] 图10解说了根据所给出的主题内容的各种方面的各种方法体系。尽管为使解释简单化将这些方法体系图示并描述为一系列动作或序列步骤,但是应当理解并领会,所要求保护的主题内容不受动作的次序所限,因为一些动作可按不同于本文中图示和描述的次序出现和/或与其他动作并发地出现。例如,本领域技术人员将理解和领会,方法体系可被替换地表示为一系列相互关联的状态或事件,诸如在状态图中那样。不仅如此,并非所有解说了的动作都是实现根据所要求保护的主题内容的方法体系所必需的。另外还应该领会,下文以及贯穿本说明书所公开的方法体系能够被存储在制品上以便将此类方法体系传输和传递给计算机。如本文中所使用的术语“制品”意在涵盖可从任何计算机可读设备、载体、或介质访问的计算机程序。

[0078] 图10是第一无线通信方法的流程图1000。该方法可由UE来执行。在另一方面,该方法可以由MME执行。

[0079] 在另一方面,上下文信息也可以包括第二UE的无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符等等。在任选的方面,在框1002,实体可以接收指示已请求了信息元素的NAS消息。在一方面,该信息元素可以是密钥,诸如第一UE密钥、第二UE密钥、最终UE密钥等。

[0080] 在另一任选方面,在框1004,在实体处可以从另一实体(例如,UE、MME等)接收信息元素。在一方面,该信息元素可以由传送实体来暗码化。在另一方面,可以使用NAS消息来接收该信息元素。在此类方面,该NAS消息可以指示计数值。当接收实体是UE时,该计数值可以是下行链路计数值。当接收实体是MME时,该计数值可以是上行链路计数值。

[0081] 在框1006,该实体可以生成密钥流以用作该信息元素的暗码。在一方面,可以基于MME-UE密钥、NAS消息计数值、以及与该信息元素相关联的上下文流来生成该密钥流。在此类方面,如在LTE环境中所定义的,MME-UE密钥可以是接入安全性管理实体(ASME)密钥(K_ASME)。进一步,在此类方面,NAS消息计数值可以是与接收到的NAS消息相关联的NAS消息计数值、与要被用来传送信息元素的NAS消息相关联的NAS消息计数值等。更进一步,上下文串可以包括与传送信息元素的实体、接收信息元素的实体、传送和接收实体所已知的第三实体等等相关联的信息。在此类方面,信息元素可以包括实体标识符,诸如但不限于无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符等,或者其任何组合。在另一方面,上下文串可以包括与该信息元素中所包括的数据的类型相关联的信息。例如,数据类型可以是密钥、用户信息等。在一方面,所生成的密钥流的长度可以基于该信息元素的长度。在另一方面,所生成的密钥流的长度可以是可配置的常量值。

[0082] 在框1008,该实体可以使用所生成的密钥流来密码术地处理该信息元素。在接收到经暗码化的信息元素的方面,该实体可以使用所生成的密钥流来译解该信息元素。在一方面,此暗码化可以包括将该密钥流直接与该信息元素进行异或。在该实体将该信息元素暗码化以用于传输的方面,所生成的密钥流的一部分可以被用作此暗码化过程中的密钥。

[0083] 在任选的方面,在框1010,该信息元素可以使用NAS消息来发送。在该信息元素被

请求的方面，接着，该信息元素可以被发送到请求实体和/或请求实体所指示的第三实体。在另一方面，该信息元素可以使用通过LTE NAS规程可用的加密来发送。

[0084] 如此，该实体可以使用具有增加的安全性的信息元素而不是使用新的信息元素来传达数据。

[0085] 图11是解说示例性设备1102中的不同模块/装置/组件之间的数据流的概念性数据流图1100。该设备可以是UE。在另一方面，该设备可以是MME。

[0086] 设备1102包括可以从另一实体(例如，UE 704、eNodeB 702、MME 714等)接收消息1112的接收模块1104。在一方面，消息1112可以指示NAS消息计数值1116、信息元素1114、对信息元素的请求等等。在设备1102是UE 702的方面，该NAS消息计数值可以是下行链路计数值。在设备1102是MME的方面，该NAS消息计数值1116可以是上行链路计数值。

[0087] 设备1102可以进一步包括安全通信模块1106和密钥流生成模块1108。在一方面，安全通信模块可以向密钥流生成模块1108提供NAS消息计数值1116以用于密码术处理。密钥流生成模块1108可以基于MME-第一UE密钥、NAS消息计数值116、以及与信息元素相关联的上下文串来生成密钥流1118。在一方面，用于密钥流118生成的NAS消息计数值可以与接收到的消息1112相关联和/或与用来传送经暗码化的信息元素的NAS消息1120相关联。该上下文串可以包括与传送该信息元素的实体、接收该信息元素的实体、传送和接收实体所已知的第三实体等等相关联的信息。在此类方面，信息元素1114可以包括实体标识符，诸如但不限于无线电网络临时标识符(RNTI)、表达标识符、服务标识符、事务标识符、MME标识符等，或者其任何组合。在另一方面，上下文串可以包括与该信息元素中所包括的数据的类型相关联的信息。例如，数据类型可以是密钥、用户信息等。在一方面，密钥流1118的长度可以基于该信息元素的长度。在另一方面，密钥流1118的长度可以是可配置的常量值。

[0088] 安全通信模块1106可以使用该密钥流来密码术地处理该信息元素。在接收到的消息1112包括了经暗码化的信息元素的方面，安全通信1106可以使用该密钥流来译解接收到的经暗码化的信息元素。在接收到的消息1112包括了对信息元素的请求的方面，安全通信模块1106可以获取所请求的信息元素，并且使用密钥流1118对其进行暗码化以生成经暗码化的信息元素1120，以用于由传输模块1110进行传输。

[0089] 该设备可包括执行图10的前述流程图中的算法的每个步骤的附加模块。如此，图10的前述流程图中的每个步骤可由一模块执行且该设备可包括这些模块中的一个或多个模块。各模块可以是专门配置成实施所述过程/算法的一个或多个硬件组件、由配置成执行所述过程/算法的处理器实现、存储在计算机可读介质中以供由处理器实现、或其某个组合。

[0090] 图12是解说采用处理系统1214的设备1102'的硬件实现的示例的示图1200。处理系统1214可实现成具有由总线1224一般化地表示的总线架构。取决于处理系统1214的具体应用和整体设计约束，总线1224可包括任何数目的互连总线和桥接器。总线1224将包括一个或多个处理器和/或硬件模块(由处理器1204、模块1104、1106、1108、1110和计算机可读介质1206表示)的各种电路链接在一起。总线1224还可链接各种其它电路，诸如定时源、外围设备、稳压器和功率管理电路，这些电路在本领域中是众所周知的，并且因此将不再进一步描述。

[0091] 处理系统1214可耦合至收发机1210。收发机1210被耦合至一个或多个天线1220。

收发机1210提供用于通过传输介质与各种其它装置通信的手段。处理系统1214包括耦合至计算机可读介质1206的处理器1204。处理器1204负责一般性处理，包括执行存储在计算机可读介质1206上的软件。该软件在由处理器1204执行时使处理系统1214执行上文针对任何特定装置描述的各种功能。计算机可读介质1206还可被用于存储由处理器1204在执行软件时操纵的数据。处理系统进一步包括模块1104、1106、1108、和1110中的至少一个模块。各模块可以是在处理器1204中运行的软件模块、驻留/存储在计算机可读介质1206中的软件模块、耦合至处理器1204的一个或多个硬件模块、或其某种组合。处理系统1214可以是UE 650的组件且可包括存储器660和/或TX处理器668、RX处理器670、和控制器/处理器659中的至少一者。在另一方面，处理系统1214可以是WAN实体610(例如，MME)的组件且可包括存储器676和/或包括TX处理器616、RX处理器670、和控制器/处理器675中的至少一者。

[0092] 在一个配置中，用于无线通信的设备1102/1102'包括用于基于MME-UE密钥、NAS消息计数值、以及与信息元素相关联的上下文串生成密钥流的装置，以及用于使用所生成的密钥流来密码术地处理该信息元素的装置。在一方面，用于处理的装置可以配置成使用所生成的密钥流来暗码化该信息元素。在此类方面，设备1202/1202'可以进一步包括用于发送经暗码化的信息元素的装置。在一方面，用于发送的装置可以进一步配置成使用LTE NAS安全规程来发送经暗码化的信息元素。在另一方面，设备1202/1202'可进一步包括用于接收信息元素的装置。在此类方面，用于处理的装置可以进一步配置成使用所生成的密钥流来译解该信息元素。在另一方面，用于接收的装置可以配置成接收触发密钥流的生成的NAS消息。

[0093] 前述装置可以是设备1102和/或装置1102'的处理系统1214中被配置成执行由前述装置叙述的功能的前述模块中的一者或多者。如前文所述，处理系统1314可包括TX处理器668、RX处理器656、以及控制器/处理器659。如此，在一种配置中，前述装置可以是被配置成执行由前述装置所述的功能的TX处理器668、RX处理器656、以及控制器/处理器659。在另一方面，如前文所述，处理系统1214可包括TX处理器616、RX处理器670、以及控制器/处理器675。如此，在一种配置中，前述装置可以是被配置成执行由前述装置所述的功能的TX处理器616、RX处理器670、和/或控制器/处理器675。

[0094] 应理解，所公开的过程中各步骤的具体次序或层次是示例性办法的解说。应理解，基于设计偏好，可以重新编排这些过程中各步骤的具体次序或层次。此外，一些步骤可被组合或被略去。所附方法权利要求以示例次序呈现各种步骤的要素，且并不意味着被限定于所呈现的具体次序或层次。

[0095] 提供之前的描述是为了使本领域任何技术人员均能够实践本文中所描述的各种方面。对这些方面的各种改动将容易为本领域技术人员所明白，并且在本文中所定义的普适原理可被应用于其他方面。因此，权利要求并非旨在被限定于本文中所示出的方面，而是应被授予与语言上的权利要求相一致的全部范围，其中对要素的单数形式的引述除非特别声明，否则并非旨在表示“有且仅有一个”，而是“一个或多个”。除非特别另外声明，否则术语“一些/某个”指的是一个或多个。本公开通篇描述的各种方面的要素为本领域普通技术人员当前或今后所知的所有结构上和功能上的等效方案通过引述被明确纳入于此，且旨在被权利要求所涵盖。此外，本文中所公开的任何内容都并非旨在贡献给公众，无论这样的公开是否在权利要求书中被显式地叙述。没有任何权利要求元素应被解释为装置加功能，除

非该元素是使用短语“用于……的装置”来明确叙述的。

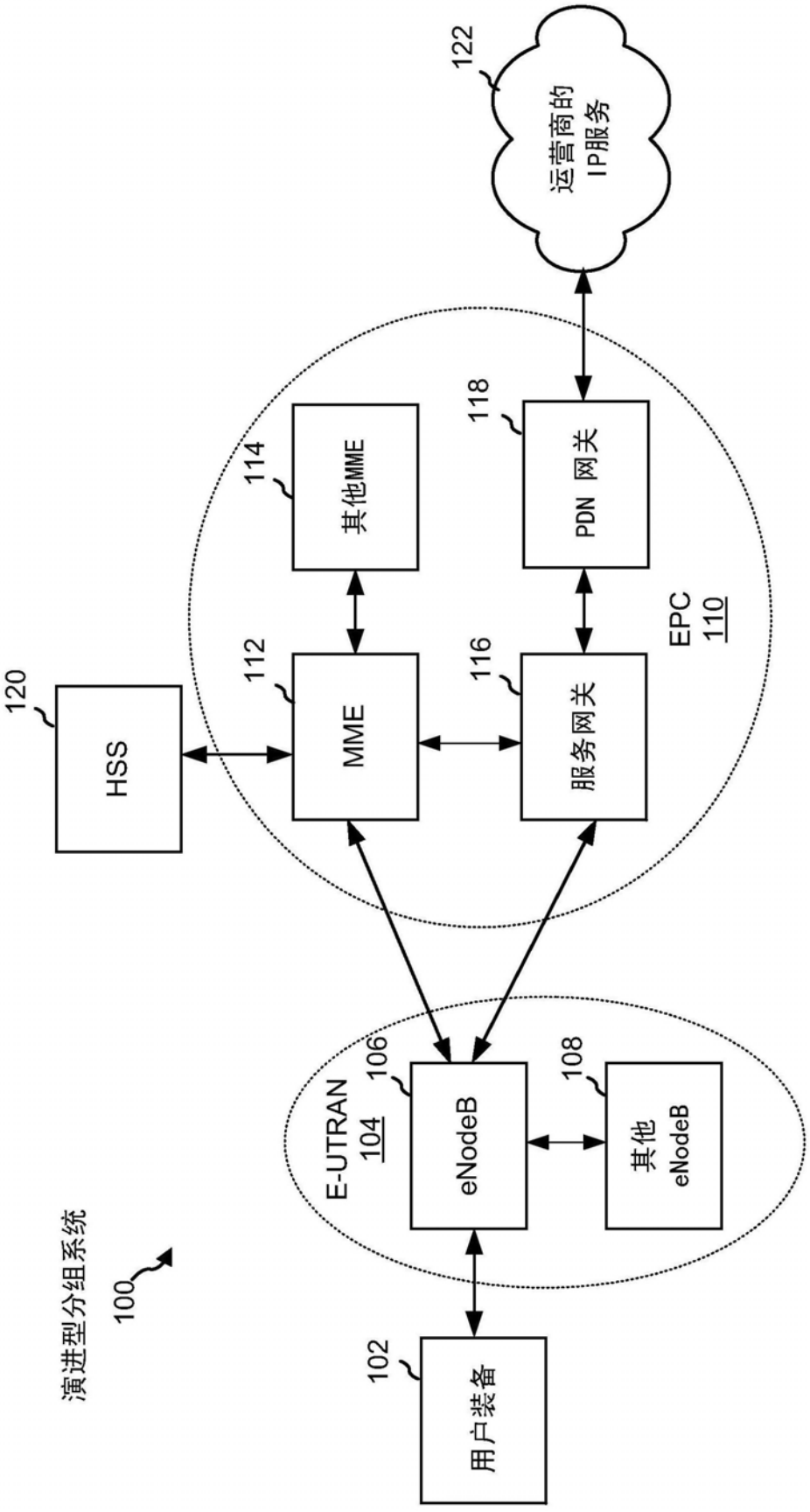

演进型分组系统
100
用户装备
102
E-UTRAN
104
eNodeB
106
其他
eNodeB
108
HSS
120
MME
112
服务网关
116
其他MME
114
PDN 网关
118
EPC
110
运营商的
IP服务
122

图1

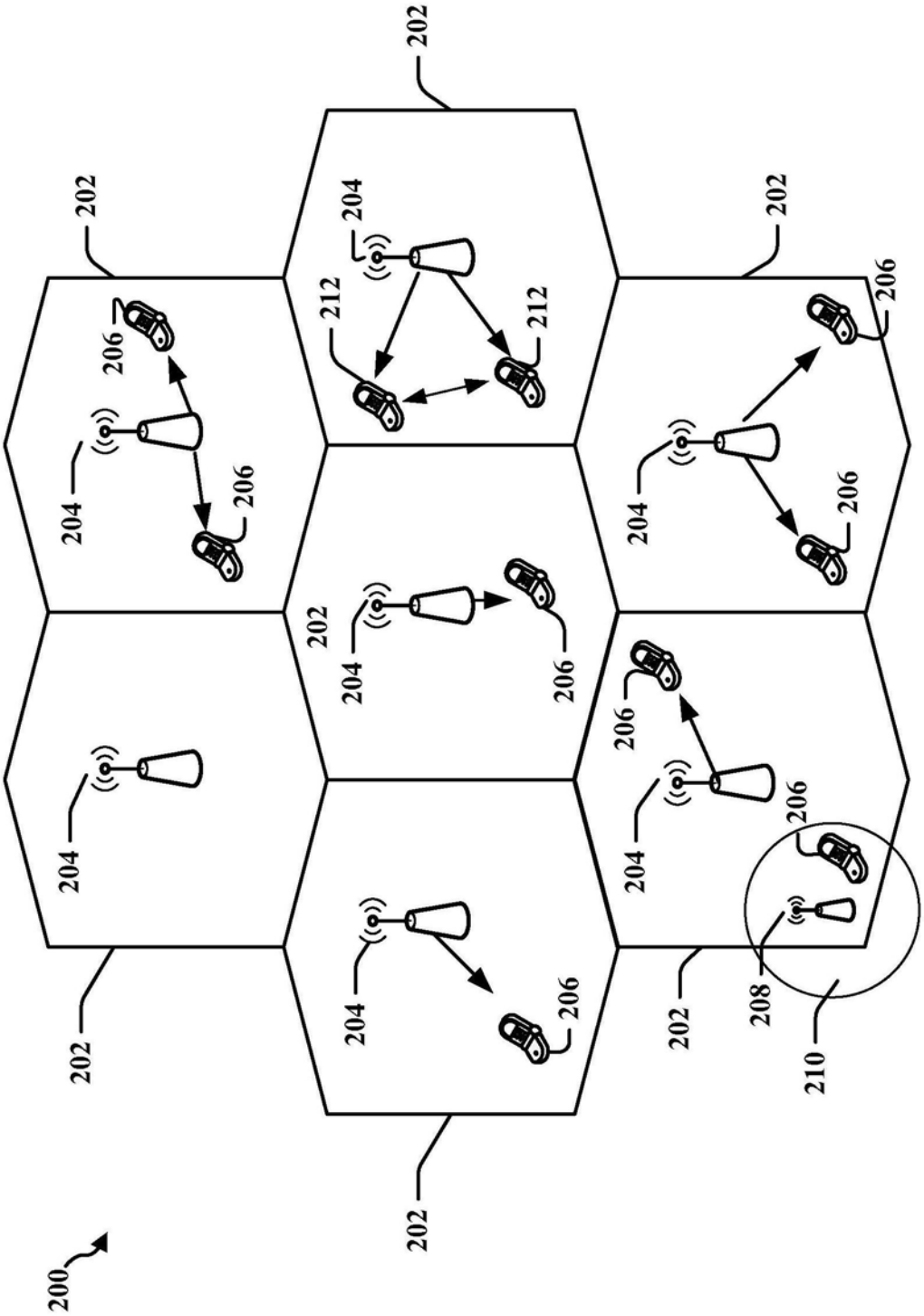


图2

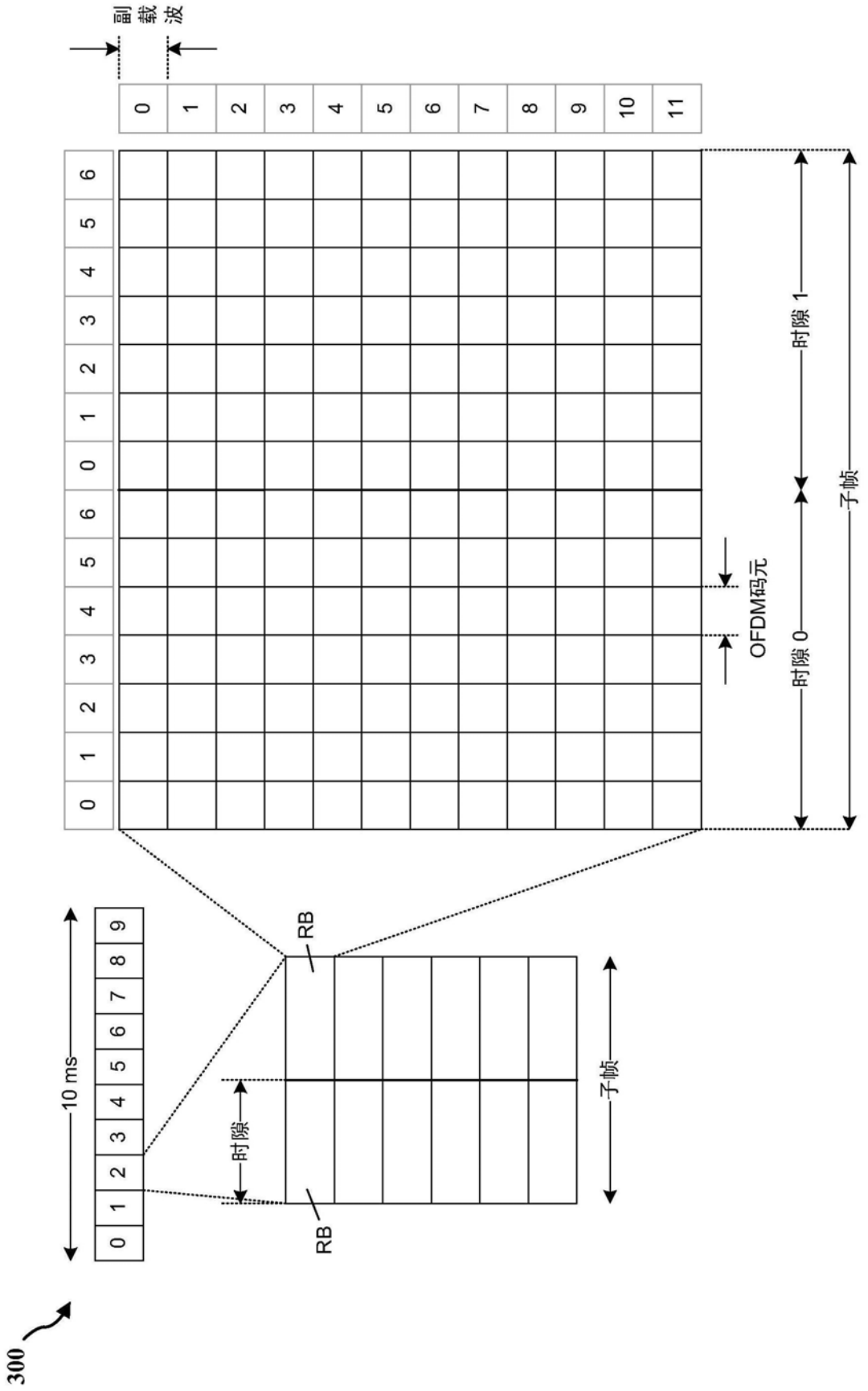

副载波
0
1
2
3
4
5
6
7
8
9
10
11
0
1
2
3
4
5
6
0
1
2
3
4
5
6
时隙 1
时隙 0
子帧
OFDM码元
10 ms
0
1
2
3
4
5
6
7
8
9
RB
RB
时隙
子帧
300

图3

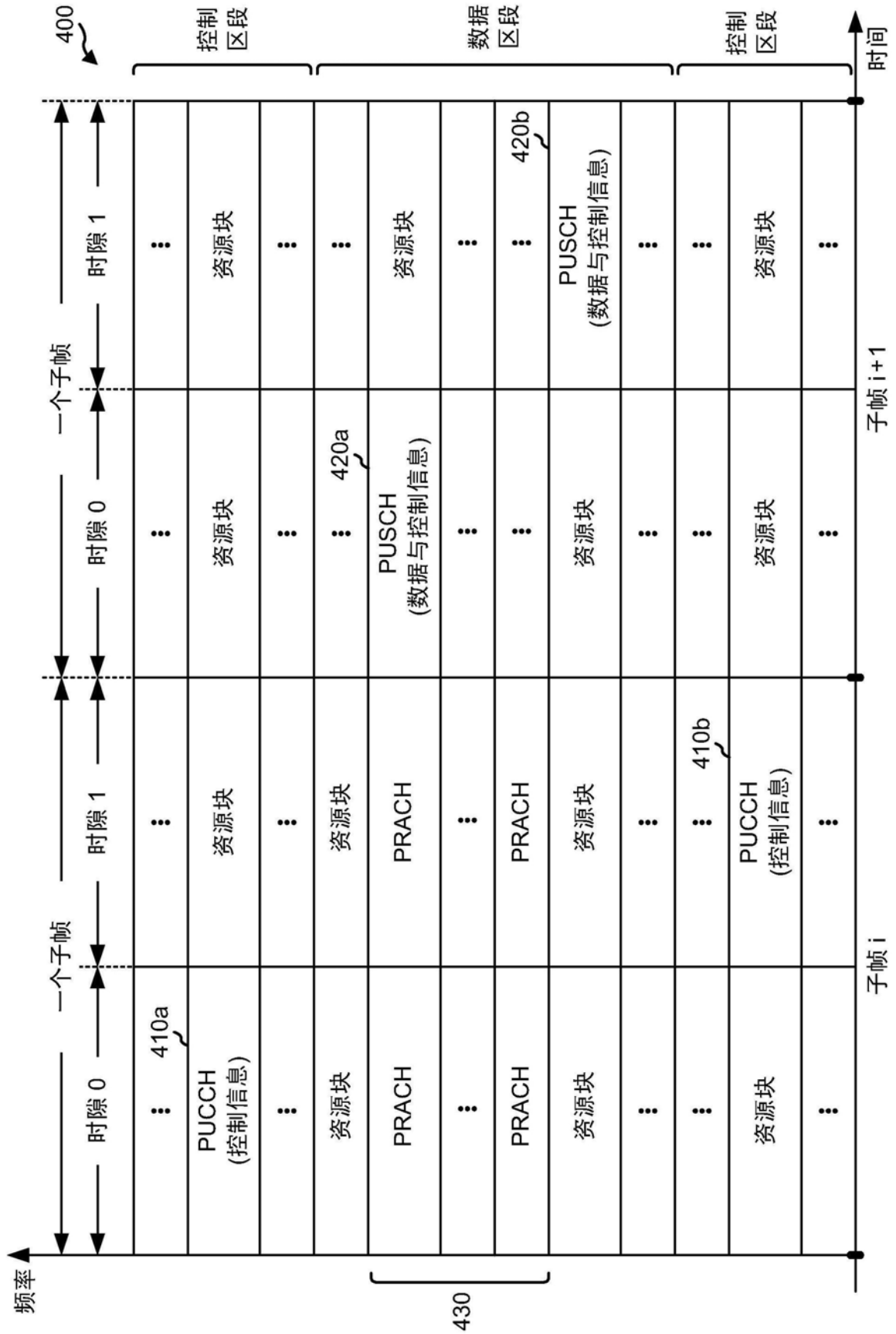

400
控制区段
数据区段
控制区段
时间
频率
一个子帧
一个子帧
时隙 0
时隙 1
时隙 0
时隙 1
410a
PUCCH
(控制信息)
资源块
420a
PUSCH
(数据与控制信息)
420b
410b
PRACH
PUCCH
(控制信息)
子帧 i
子帧 i+1
430

图4

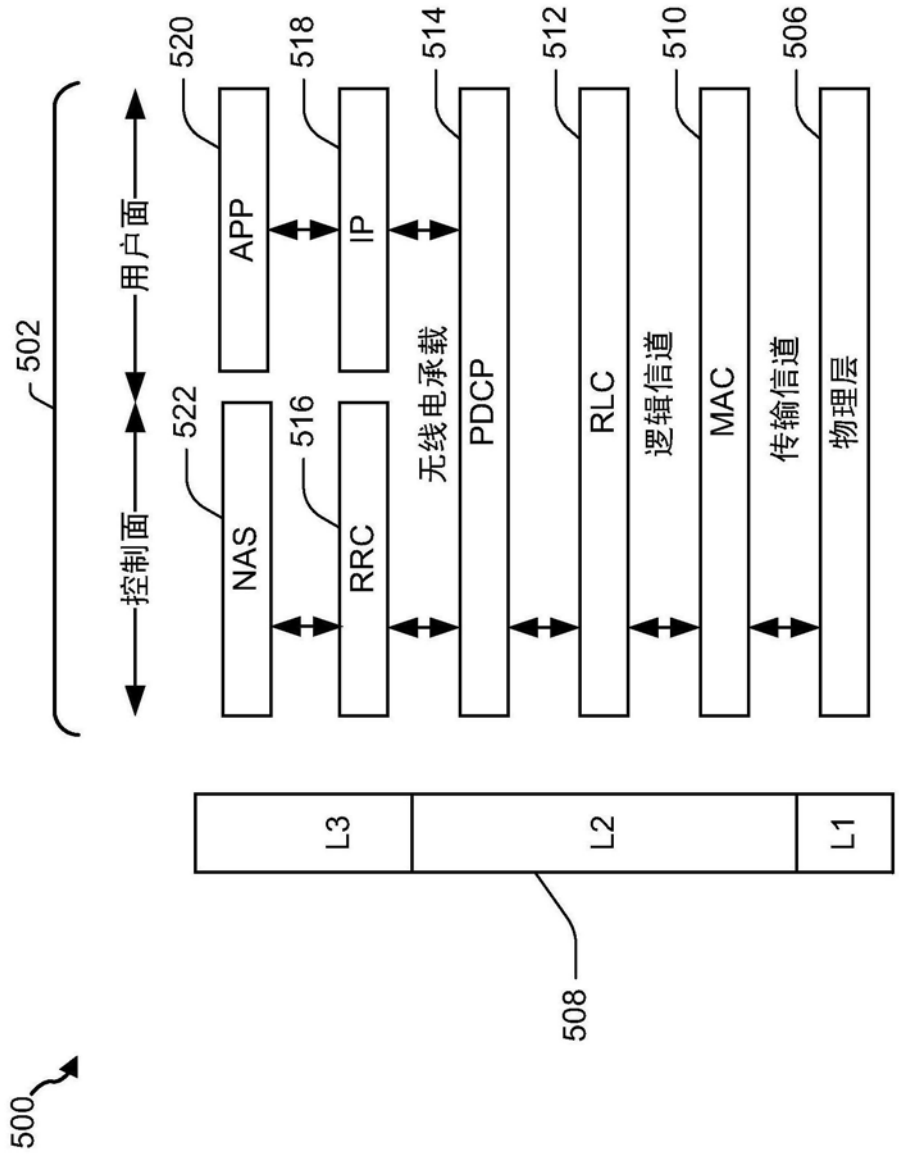

500
502
用户面
控制面
520
518
514
512
510
506
522
516
APP
IP
NAS
RRC
无线电承载
PDCP
RLC
逻辑信道
MAC
传输信道
物理层
L3
L2
L1
508

图5

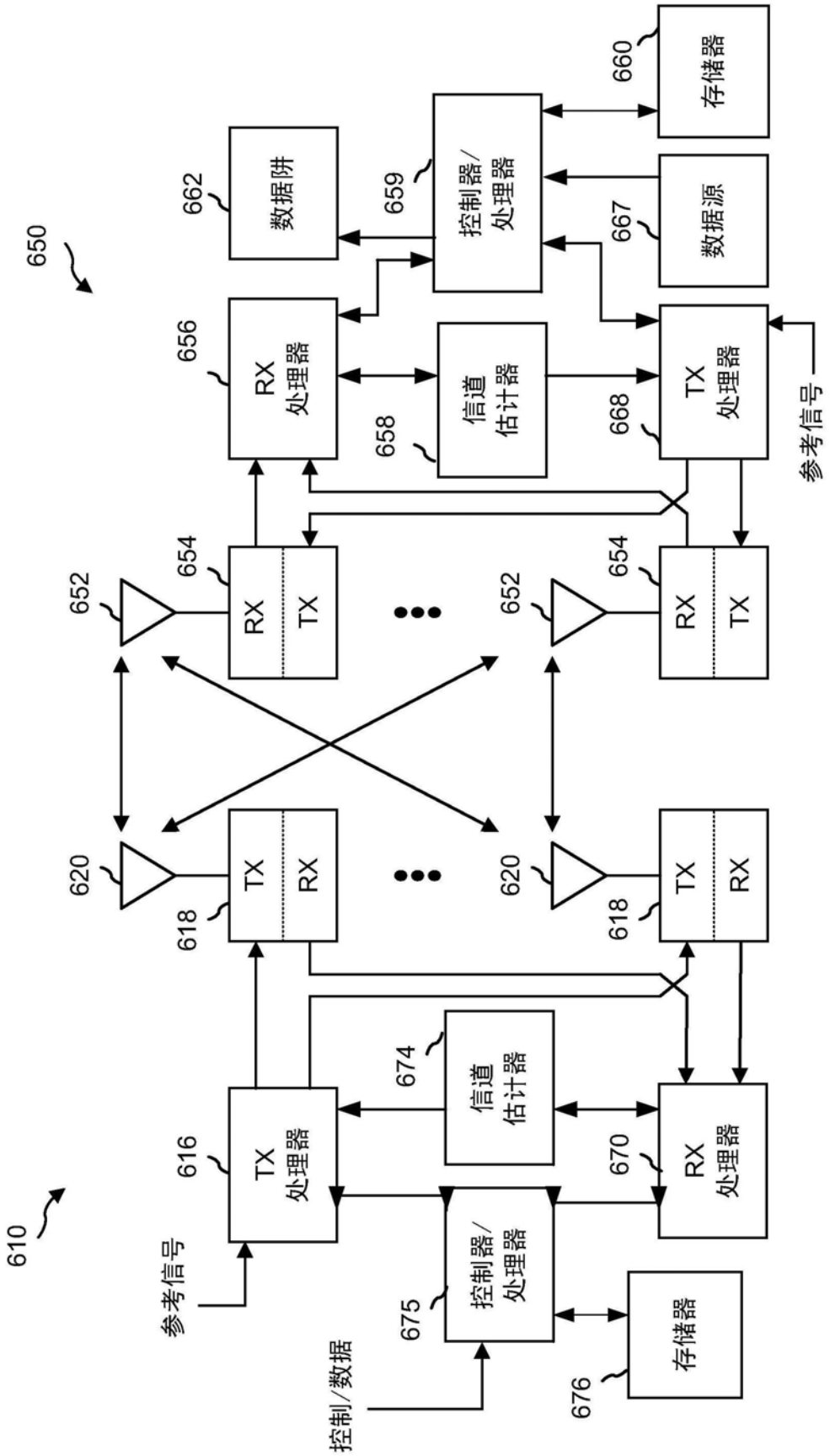

650
662
数据阱
659
控制器/
处理器
660
存储器
667
数据源
656
RX
处理器
658
信道
估计器
668
TX
处理器
参考信号
654
RX
TX
652
620
618
610
616
TX
处理器
674
信道
估计器
670
RX
处理器
675
控制器/
处理器
676
存储器
参考信号
控制/数据

图6

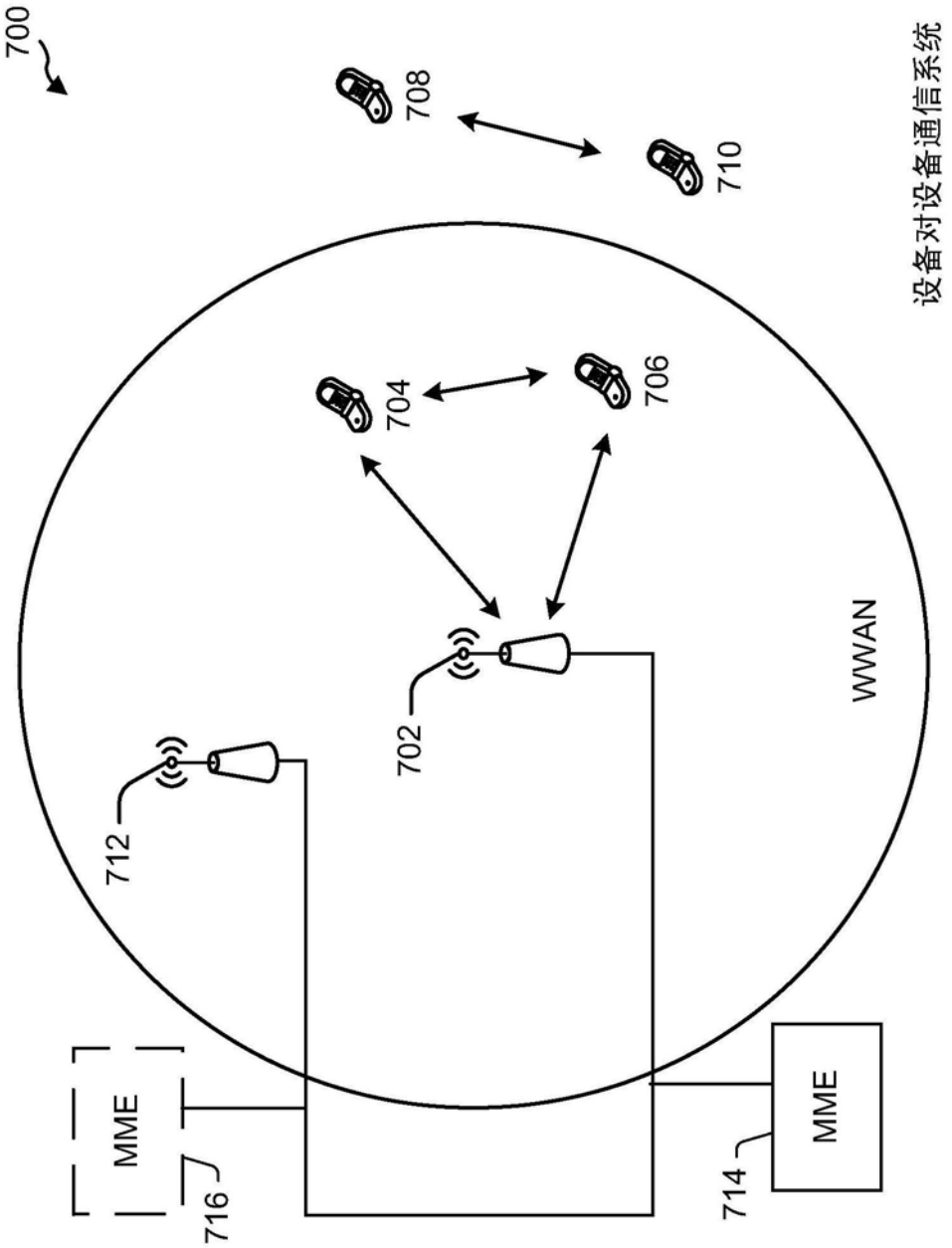


图7

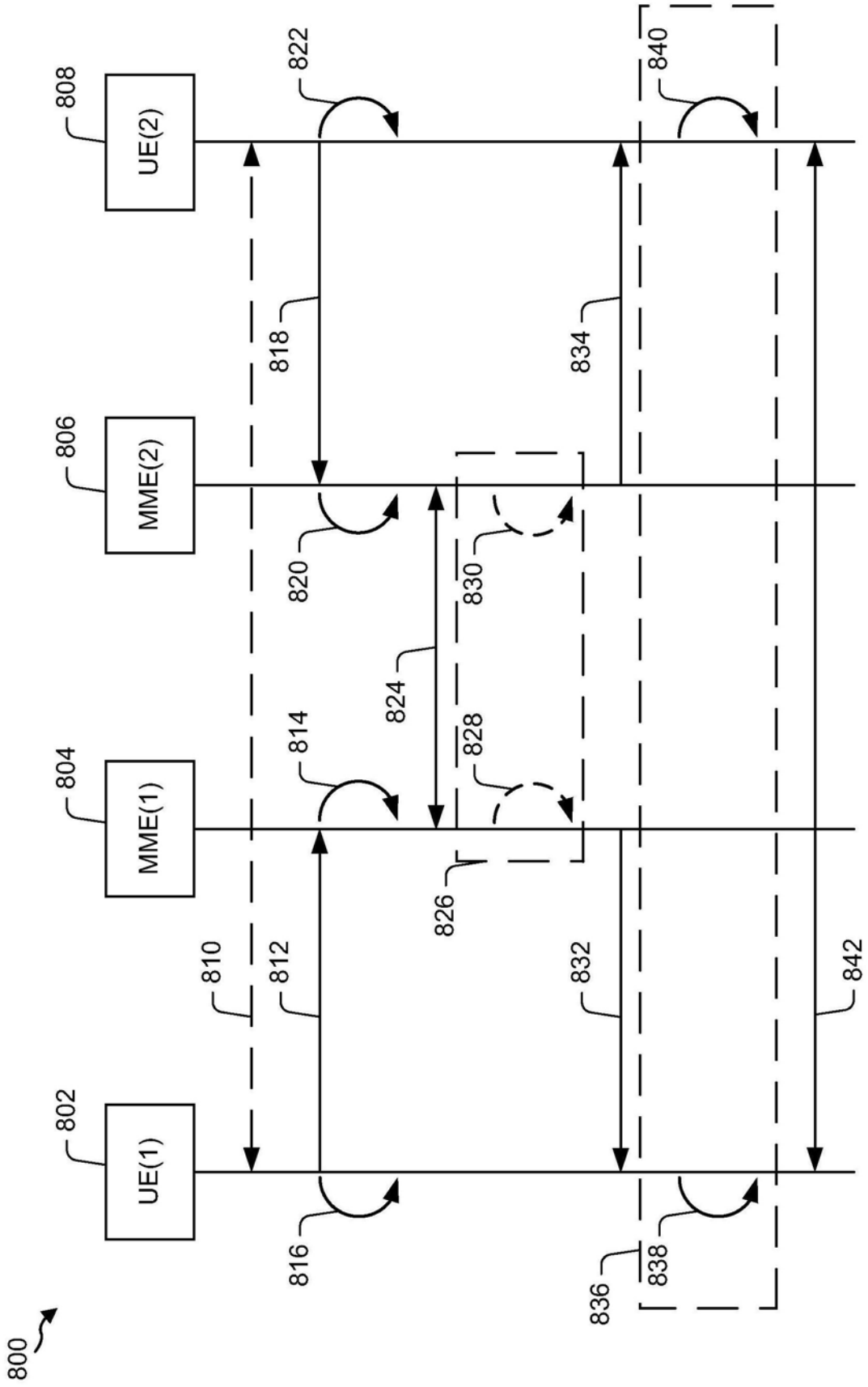

800
802
UE(1)
804
MME(1)
806
MME(2)
808
UE(2)
810
812
814
816
818
820
822
824
826
828
830
832
834
836
838
840
842

图8

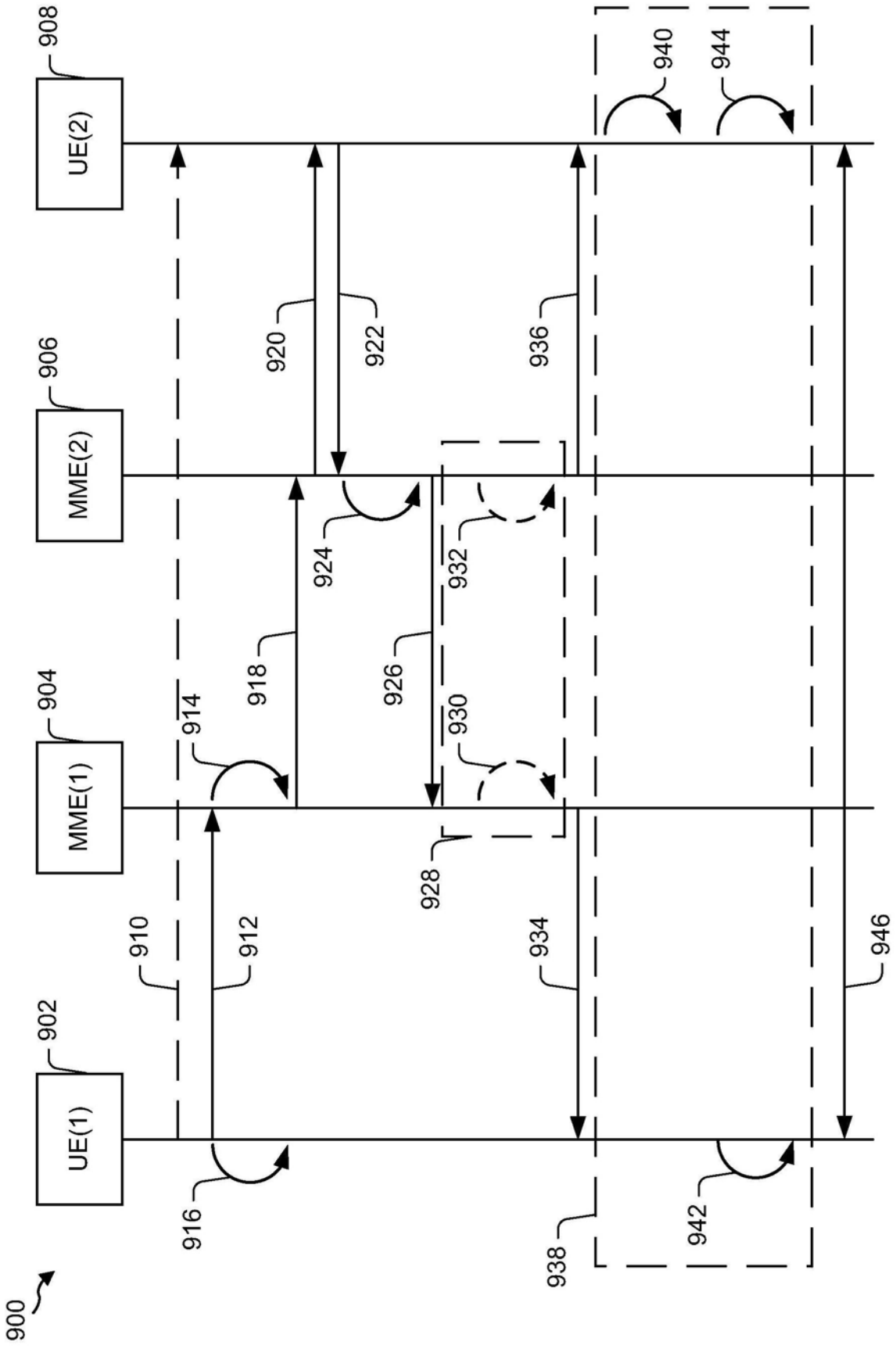

900
UE(1)
902
MME(1)
904
MME(2)
906
UE(2)
908
910
912
914
916
918
920
922
924
926
928
930
932
934
936
938
940
942
944
946

图9

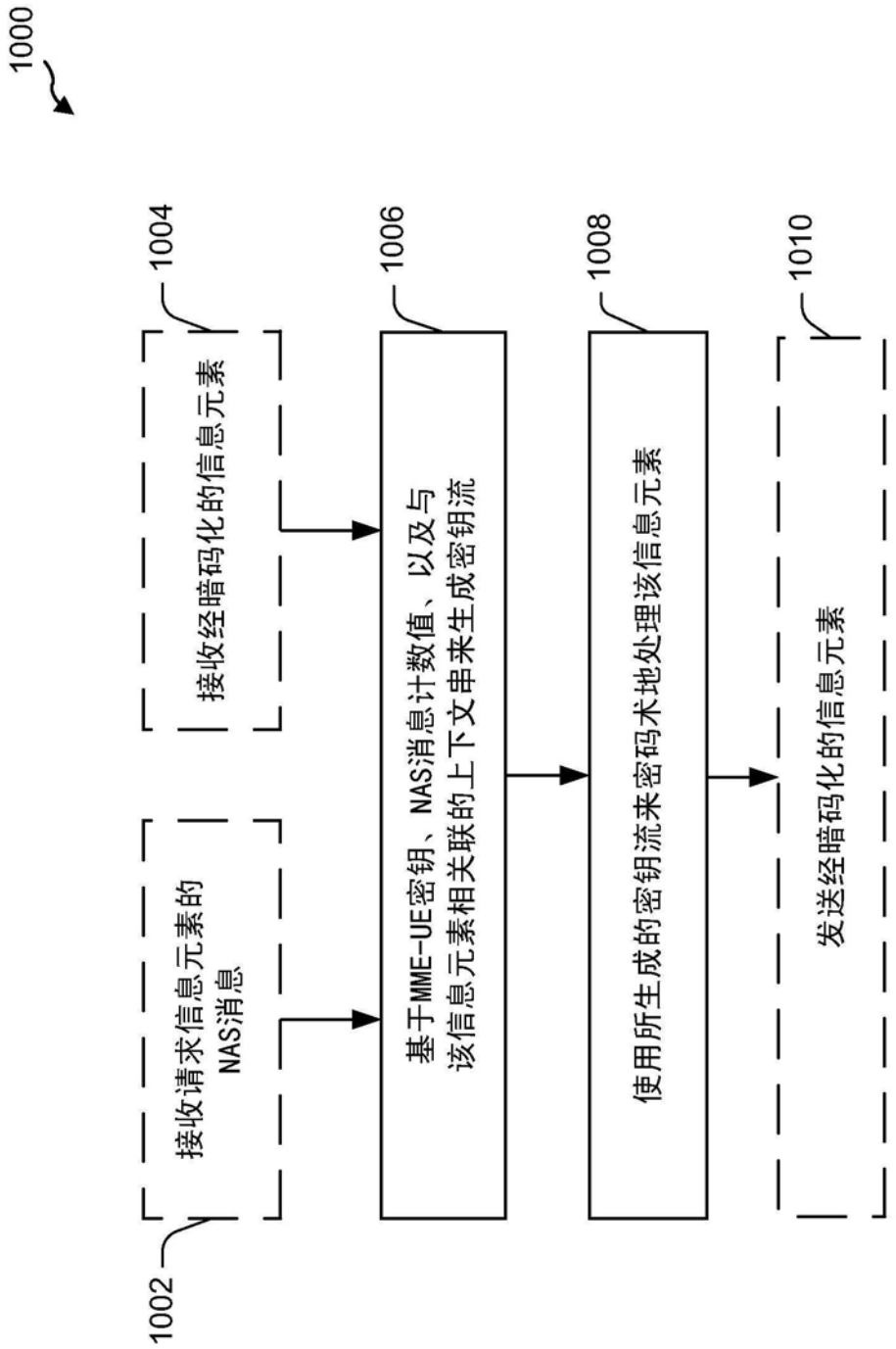

1000
1002
接收请求信息元素的NAS消息
1004
接收经暗码化的信息元素
1006
基于MME-UE密钥、NAS消息计数值、以及与该信息元素相关联的上下文串来生成密钥流
1008
使用所生成的密钥流来密码术地处理该信息元素
1010
发送经暗码化的信息元素

图10

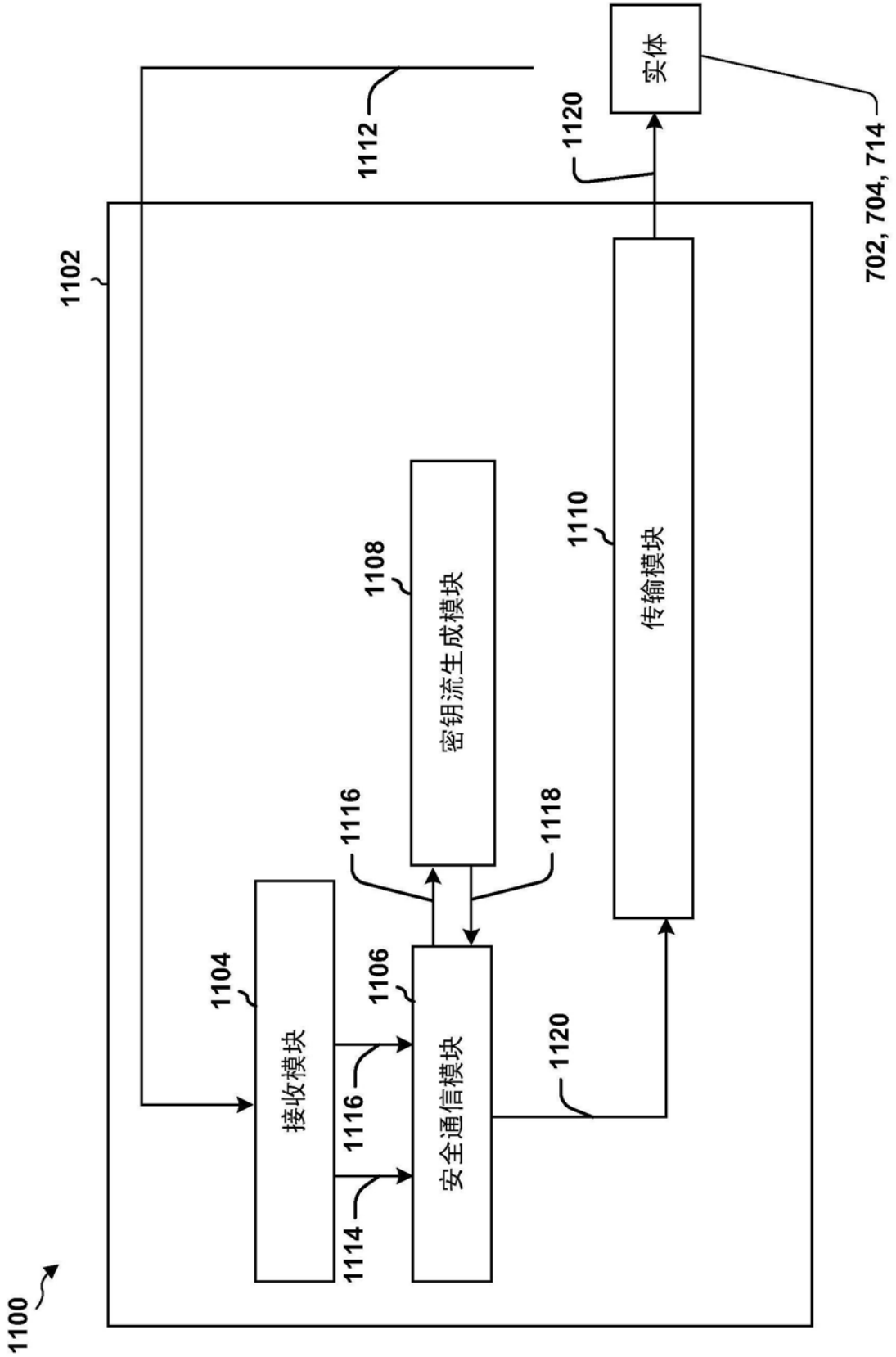

1100
1102
1104
接收模块
1106
安全通信模块
1108
密钥流生成模块
1110
传输模块
1112
1114
1116
1116
1118
1120
1120
实体
702, 704, 714

图11

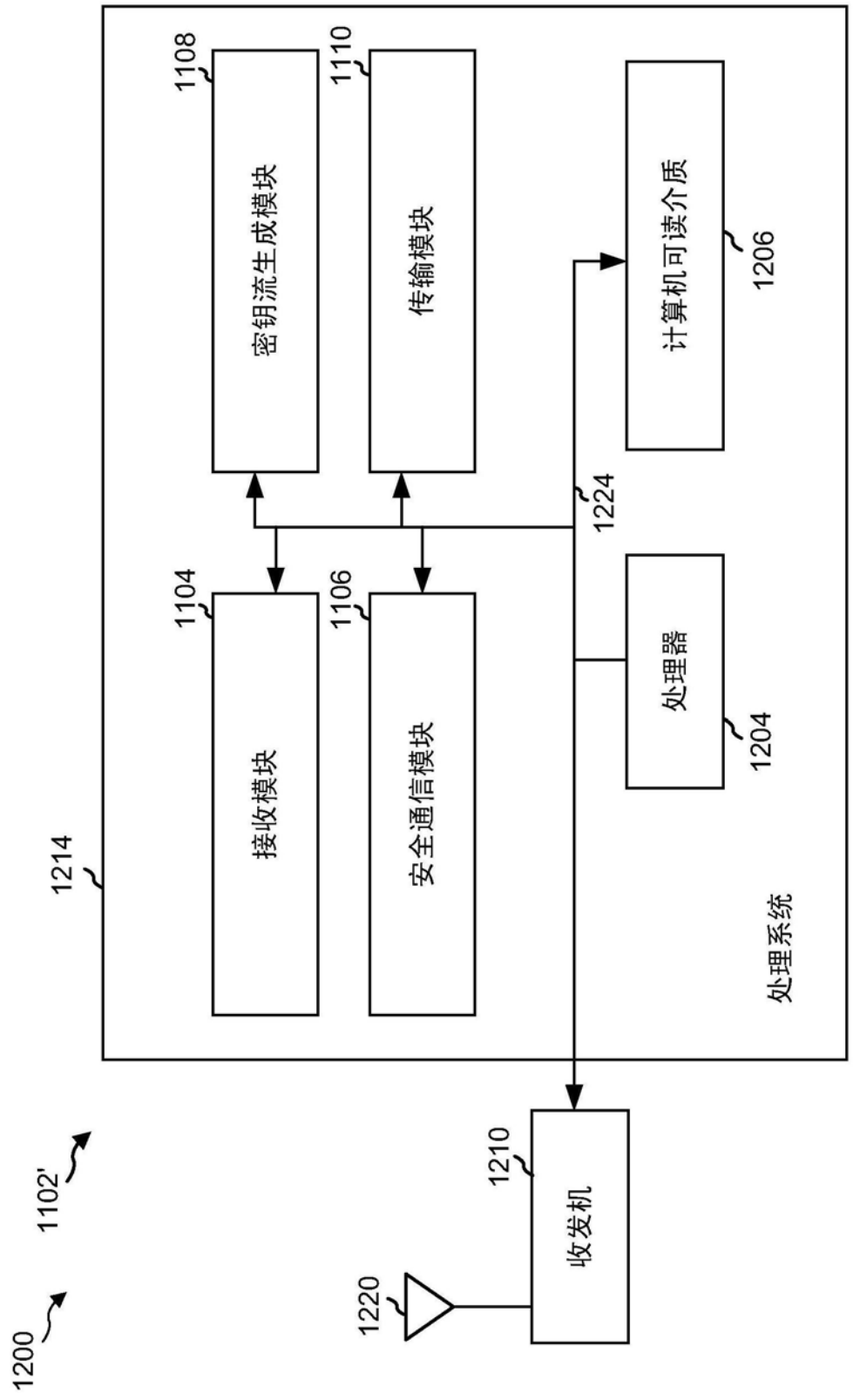

1200
1102'
1214
1108
密钥流生成模块
1110
传输模块
1104
接收模块
1106
安全通信模块
1224
计算机可读介质
1206
处理器
1204
处理系统
1210
收发机
1220

图12