(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 104854594 B
(45)授权公告日 2019.01.08

(21)申请号 201380063786.5
(22)申请日 2013.12.06
(65)同一申请的已公布的文献号
申请公布号 CN 104854594 A
(43)申请公布日 2015.08.19
(30)优先权数据
13/706,849 2012.12.06 US
(85)PCT国际申请进入国家阶段日
2015.06.05
(86)PCT国际申请的申请数据
PCT/US2013/073522 2013.12.06
(87)PCT国际申请的公布数据
WO2014/089403 EN 2014.06.12
(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 M·范德韦恩 V·D·帕克 G·茨瑞特西斯
(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.
G06F 21/12(2013.01)
G06F 21/33(2013.01)
H04W 12/06(2009.01)
(56)对比文件
US 2012/0064828 A1,2012.03.15,
CN 1746872 A,2006.03.15,
CN 102460388 A,2012.05.16,
CN 101512516 A,2009.08.19,
US 2012/0300938 A1,2012.11.29,
US 2012/0015629 A1,2012.01.19,
US 2010/0043061 A1,2010.02.18,
US 2008/0002698 A1,2008.01.03,
审查员 张峰

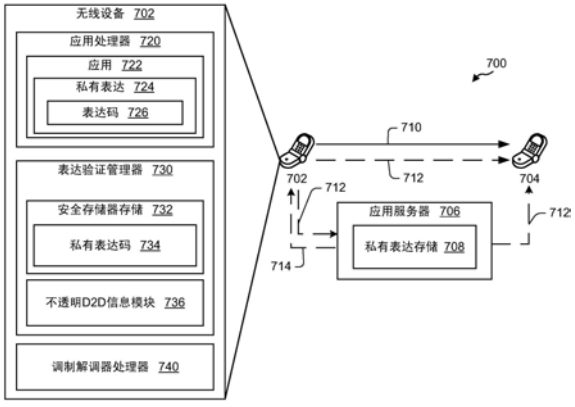
权利要求书5页 说明书11页 附图10页

(54)发明名称

用于提供对抗冒充风险的私有表达保护的方法和装置

(57)摘要

提供了与在无线通信网络中提供私有表达保护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,UE被装备成内部地接收要宣告私有表达和/或至少对与该私有表达相关联的表达码的引用的请求(例如,从在该UE上运行的应用接收该请求),并且确定对该表达码的引用和/或该表达码是否与存储着的该表达码的实例匹配。在一方面,该UE可被装备成在存储着的该表达码的实例对应于随该请求一起接收到的表达码时,宣告该私有表达或该表达码中的至少一者。在另一方面,该UE可被装备成在存储着的表达码不对应于随该请求一起接收到的表达码时,禁止任何与该私有表达相关联的信息的宣告。



CN 104854594 B

1.一种用户装备UE进行无线通信的方法,包括:

由该UE的表达验证管理器EVM作为要由所述UE的处理器执行的应用的配置过程的一部分而生成表达码的实例,其中该EVM与所述UE的调制解调器相关联;

将所述表达码的所述实例存储在安全存储器存储中;

在所述UE的处理器处从所述应用接收要在设备到设备通信信道上宣告私有表达的请求,其中所述请求包括至少对与所述私有表达和所述应用相关联的表达码的引用;

由所述EVM确定所述至少对所述表达码的引用是否对应于之前生成并存储着的与所述应用相关联的所述表达码的实例;

一旦确定所述至少对所述表达码的引用对应于存储着的所述表达码的实例,就使用基于长期演进LTE的无线广域网WWAN频谱或无执照频谱来在所述设备到设备通信信道上向一个或多个其他经授权的对等方设备宣告与所述私有表达和所述应用相关联的所述表达码;以及

一旦确定所述至少对所述表达码的引用不对应于存储着的所述表达码的实例,就禁止宣告与所述私有表达相关联的信息。

2.如权利要求1所述的方法,其特征在于,所述安全存储器存储是与用户装备UE相关联的非易失性存储器NVM。

3.如权利要求1所述的方法,其特征在于,进一步包括:

传送与所述表达码相关联的不透明设备对设备D2D信息。

4.如权利要求3所述的方法,其特征在于,所述不透明D2D信息被安全地传送给一个或多个获授权的设备。

5.如权利要求3所述的方法,其特征在于,所述不透明D2D信息被传送给与所述应用相关联的应用服务器。

6.如权利要求3所述的方法,其特征在于,所述不透明D2D信息包括以下至少一者:

所述私有表达、所述表达码、所述应用的名称、计数器、生成时间、之前生成的表达码、过期日期或者宣告方用户装备UE的证书。

7.如权利要求3所述的方法,其特征在于,进一步包括:

生成指示所述不透明D2D信息的真实性的数字签名,并且其中所述不透明D2D信息是随所生成的数字签名一起传送的。

8.如权利要求7所述的方法,其特征在于,所述数字签名还能包括以下至少一者:

经运营商签名的密钥、临时设备指示符或生存时间TTL值。

9.如权利要求1所述的方法,其特征在于,获得所述表达码的所述实例包括:

从受信任的服务器安全地获得所述表达码的所述实例。

10.如权利要求1所述的方法,其特征在于,所述EVM被配置为所述UE的应用接口与调制解调器接口之间的中间层。

11.如权利要求10所述的方法,其特征在于,所述EVM的第一部分与所述UE的调制解调器相关联,并且其中所述EVM的第二部分配置为所述UE的所述应用接口与所述调制解调器接口之间的所述中间层。

12.一种用于无线通信的用户装备UE,包括:

用于由该UE的表达验证管理器EVM作为要由所述UE的处理器执行的应用的配置过程的

一部分而生成表达码的实例的装置，其中该EVM与所述UE的调制解调器相关联；

用于将所述表达码的所述实例存储在安全存储器存储中的装置；

用于在所述UE的处理器处从所述应用接收要在设备到设备通信信道上宣告私有表达的请求的装置，其中所述请求包括至少对与所述私有表达和所述应用相关联的表达码的引用；

用于由所述EVM确定所述至少对所述表达码的引用是否对应于之前生成并存储着的与所述应用相关联的所述表达码的实例的装置；

用于一旦确定所述至少对所述表达码的引用对应于存储着的所述表达码的实例，就使用基于长期演进LTE的无线广域网WWAN频谱或无执照频谱来在所述设备到设备通信信道上向一个或多个其他经授权的对等方设备宣告与所述私有表达和所述应用相关联的所述表达码的装置；以及

用于一旦确定所述至少对所述表达码的引用不对应于存储着的所述表达码的实例，就禁止宣告与所述私有表达相关联的信息的装置。

13.如权利要求12所述的UE，其特征在于，所述安全存储器存储是与所述UE相关联的非易失性存储器NVM。

14.如权利要求12所述的UE，其特征在于，所述用于宣告的装置进一步配置成：

传送与所述表达码相关联的不透明设备对设备D2D信息。

15.如权利要求14所述的UE，其特征在于，所述不透明D2D信息被安全地传送给一个或多个获授权的设备。

16.如权利要求14所述的UE，其特征在于，所述不透明D2D信息被传送给与所述应用相关联的应用服务器，所述应用服务器将私有表达码分发给在所述一个或多个其他经授权的对等方设备上的应用。

17.如权利要求14所述的UE，其特征在于，所述不透明D2D信息包括以下至少一者：

所述私有表达、所述表达码、所述应用的名称、计数器、生成时间、之前生成的表达码、过期日期或者宣告方UE的证书。

18.如权利要求14所述的UE，其特征在于，所述用于确定的装置进一步配置成：

生成指示所述不透明D2D信息的真实性的数字签名，并且其中所述不透明D2D信息是随所生成的数字签名一起传送的。

19.如权利要求18所述的UE，其特征在于，所述数字签名还能包括以下至少一者：经运营商签名的密钥、临时设备指示符或生存时间TTL值。

20.如权利要求12所述的UE，其特征在于，所述用于获得所述表达码的所述实例的装置被配置成从受信任的服务器安全地获得所述表达码的所述实例。

21.如权利要求12所述的UE，其特征在于，所述EVM配置为所述UE的应用接口与调制解调器接口之间的中间层。

22.如权利要求21所述的UE，其特征在于，所述EVM的第一部分与所述UE的所述调制解调器相关联，并且其中所述EVM的第二部分配置为所述UE的所述应用接口与所述调制解调器接口之间的所述中间层。

23.一种用于无线通信的用户装备UE，包括：

存储器；以及

耦合到所述存储器的至少一个处理器，所述处理器被配置成：

由该UE的表达验证管理器EVM作为要由所述UE的处理器执行的应用的配置过程的一部分而生成表达码的实例，其中该EVM与所述UE的调制解调器相关联；

将所述表达码的所述实例存储在安全存储器存储中；

在所述UE的所述至少一个处理器处从所述应用接收要在设备到设备通信信道上宣告私有表达的请求，其中所述请求包括至少对与所述私有表达和所述应用相关联的表达码的引用；

由所述EVM确定所述至少对所述表达码的引用是否对应于之前生成并存储着的与所述应用相关联的所述表达码的实例；

一旦确定所述至少对所述表达码的引用对应于存储着的所述表达码的实例，就使用基于长期演进LTE的无线广域网WWAN频谱或无执照频谱来在所述设备到设备通信信道上向一个或多个其他经授权的对等方设备宣告与所述私有表达和所述应用相关联的所述表达码；以及

一旦确定所述至少对所述表达码的引用不对应于存储着的所述表达码的实例，就禁止宣告与所述私有表达相关联的信息。

24.如权利要求23所述的UE，其特征在于，所述安全存储器存储是与所述UE相关联的非易失性存储器NVM。

25.如权利要求23所述的UE，其特征在于，所述至少一个处理器被进一步配置成：

传送与所述表达码相关联的不透明设备对设备D2D信息。

26.如权利要求25所述的UE，其特征在于，所述不透明D2D信息被安全地传送给一个或多个获授权的设备。

27.如权利要求25所述的UE，其特征在于，所述不透明D2D信息被传送给与所述应用相关联的应用服务器。

28.如权利要求25所述的UE，其特征在于，所述不透明D2D信息包括以下至少一者：

所述私有表达、所述表达码、所述应用的名称、计数器、生成时间、之前生成的表达码、过期日期或者宣告方UE的证书。

29.如权利要求25所述的UE，其特征在于，所述至少一个处理器被进一步配置成：

生成指示所述不透明D2D信息的真实性的数字签名，并且其中所述不透明D2D信息是随所生成的数字签名一起传送的。

30.如权利要求29所述的UE，其特征在于，所述数字签名包括以下至少一者：

经运营商签名的密钥、临时设备指示符或生存时间TTL值。

31.如权利要求23所述的UE，其特征在于，所述至少一个处理器被进一步配置成：

从受信任的服务器安全地获取所述表达码的所述实例。

32.如权利要求23所述的UE，其特征在于，所述EVM配置为所述UE的应用接口与调制解调器接口之间的中间层。

33.如权利要求32所述的UE，其特征在于，所述EVM的第一部分与所述UE的调制解调器相关联，并且其中所述EVM的第二部分配置为所述UE的所述应用接口与所述调制解调器接口之间的所述中间层。

34.一种非瞬态计算机可读介质，所述非瞬态计算机可读介质存储用于无线通信的计

算机可执行代码，包括用于实现以下操作的代码：

由用户装备UE的表达验证管理器EVM作为要由所述UE的处理器执行的应用的配置过程的一部分而生成表达码的实例，其中该EVM与所述UE的调制解调器相关联；

将所述表达码的所述实例存储在安全存储器存储中；

在所述UE的处理器处从所述应用接收要在设备到设备通信信道上宣告私有表达的请求，其中所述请求包括至少对与所述私有表达和所述应用相关联的表达码的引用；

由所述EVM确定所述至少对所述表达码的引用是否对应于之前生成并存储着的所述表达码的实例；

一旦确定所述至少对所述表达码的引用对应于存储着的所述表达码的实例，就使用基于长期演进LTE的无线广域网WWAN频谱或无执照频谱来在所述设备到设备通信信道上向一个或多个其他经授权的对等方设备宣告与所述私有表达和所述应用相关联的所述表达码；以及

一旦确定所述至少对所述表达码的引用不对应于存储着的所述表达码的实例，就禁止宣告与所述私有表达相关联的信息。

35.如权利要求34所述的非瞬态计算机可读介质，其特征在于，所述安全存储器存储是与所述UE相关联的非易失性存储器NVM。

36.如权利要求34所述的非瞬态计算机可读介质，其特征在于，进一步包括用于执行以下操作的代码：

传送与所述表达码相关联的不透明设备对设备D2D信息。

37.如权利要求36所述的非瞬态计算机可读介质，其特征在于，所述不透明D2D信息被安全地传送给一个或多个获授权的设备。

38.如权利要求36所述的非瞬态计算机可读介质，其特征在于，所述不透明D2D信息被传送给与所述应用相关联的应用服务器。

39.如权利要求36所述的非瞬态计算机可读介质，其特征在于，所述不透明D2D信息包括以下至少一者：

所述私有表达、所述表达码、所述应用的名称、计数器、生成时间、之前生成的表达码、过期日期或者宣告方用户装备UE的证书。

40.如权利要求36所述的非瞬态计算机可读介质，其特征在于，进一步包括用于执行以下操作的代码：

生成指示所述不透明D2D信息的真实性的数字签名，并且其中所述不透明D2D信息是随所生成的数字签名一起传送的。

41.如权利要求40所述的非瞬态计算机可读介质，其特征在于，所述数字签名还能包括以下至少一者：

经运营商签名的密钥、临时设备指示符或生存时间TTL值。

42.如权利要求34所述的非瞬态计算机可读介质，其特征在于，所述用于获得所述表达码的实例的代码包括

用于从受信任的服务器安全地获取所述表达码的所述实例的代码。

43.如权利要求34所述的非瞬态计算机可读介质，其特征在于，所述EVM配置为所述UE的应用接口与调制解调器接口之间的中间层。

44.如权利要求43所述的非瞬态计算机可读介质，其特征在于，所述EVM的第一部分与所述UE的所述调制解调器相关联，并且其中所述EVM的第二部分配置为所述UE的所述应用接口与所述调制解调器接口之间的所述中间层。

用于提供对抗冒充风险的私有表达保护的方法和装置

[0001] 领域

[0002] 本公开一般涉及通信系统，并且尤其涉及在基于无线通信的网络中的设备对设备(D2D)通信中使用私有表达。

背景技术

[0003] 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。

[0004] 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来更好地支持移动宽带因特网接入、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。LTE可支持直接设备到设备(对等)通信。

[0005] 当前，许多设备(例如，用户装备(UE))可以是可在蜂窝网络中操作的。D2D LTE协议可提供处于直接通信射程内的UE之间的通信。UE可如由邻域知悉式应用所驱动地使用表达来宣告各种属性(用户或服务身份、应用特征、地点等)。表达可以是公开的——在其对于宣告方UE的射程内的任何UE都是可访问时，或者可以是私有的——当访问被仅限于事先被授权的特定UE时。当使用私有表达时，宣告方UE可已向已被授予在处于邻域中时访问/解码所宣告的表达的许可的一个或多个监视方UE提供了(例如经由线下过程)对应的表达码。

[0006] 然而，可能因私有表达冒充风险产生用户安全性漏洞。例如，在第一用户知道与第二用户相关联的表达码的场合，第一用户可以通过使用应用生成第一用户的设备以第二用户的表达码来宣告私有表达的请求来冒充第二用户。由此，其他人可能被骗，认为第二用户在场。

[0007] 随着对D2D通信的需求增加，存在对于用于在基于无线通信的网络中保护私有表达标识符的方法/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，描述了与在基于LTE的WWAN中提供私有表达保护有关的各种方面。在一个示例中，UE被装备成内部地接收要宣告私有表达和/或至少对

与该私有表达相关联的表达码的引用的请求(例如,从在该UE上运行的应用接收该请求),并且确定对该表达码的引用和/或该表达码是否与存储着的该表达码的实例匹配。在一方面,该UE可被装备成在存储着的该表达码的实例对应于随该请求一起接收到的表达码时,宣告该私有表达或者该表达码中的至少一者。在另一方面,UE可被装备成在存储着的表达码不对应于随该请求一起接收到的表达码时,禁止任何与该私有表达相关联的信息的宣告。

[0011] 根据相关方面,提供了一种用于在无线通信网络中提供私有表达保护的方法。该方法可包括接收至少对要宣告私有表达的请求的引用。在一方面,该请求可包括与该私有表达相关联的表达码。进一步,该方法可包括,由表达验证管理器(EVM)确定此至少对该表达码的引用是否对应于之前获得并存储着的该表达码的实例。在一方面,该方法可包括一旦确定该表达码对应于存储着的该表达码的实例,就宣告该私有表达或该表达码中的至少一者。附加地或替换地,在一方面,该方法可包括一旦确定该表达码不对应于存储着的该表达码的实例,就禁止宣告与该私有表达相关联的信息。

[0012] 另一方面涉及一种配置成在基于LTE的无线通信网络中提供私有表达保护的通信设备。该通信设备可包括用于接收要宣告至少对私有表达的引用的请求的装置。在一方面,该请求可包括与该私有表达相关联的表达码。进一步,该通信设备可包括用于由表达验证管理器(EVM)确定此至少对该表达码的引用是否对应于之前获得并存储着的该表达码的实例的装置。在一方面,该通信设备可包括用于一旦确定该表达码对应于存储着的该表达码的实例,就宣告该私有表达或该表达码中的至少一者的装置。附加地或替换地,在一方面,该通信设备可包括用于一旦确定该表达码不对应于存储着的该表达码的实例,就禁止宣告与该私有表达相关联的信息的装置。

[0013] 另一方面涉及一种通信装置。该装置可包括配置成接收要宣告私有表达的请求的处理系统。在一方面,该请求可包括至少对与该私有表达相关联的表达码的引用。进一步,该处理系统可被配置成,由表达验证管理器(EVM)确定此至少对该表达码的引用是否对应于之前获得并存储着的该表达码的实例。在一方面,该处理系统可进一步被配置成一旦确定该表达码对应于存储着的该表达码的实例,则宣告该私有表达或该表达码中的至少一者。附加地或替换地,在一方面,该处理系统可进一步被配置成一旦确定该表达码不对应于存储着的该表达码的实例,就禁止宣告与该私有表达相关联的信息。

[0014] 又一方面涉及一种计算机程序产品,其可具有计算机可读介质,该计算机可读介质包括用于接收要宣告私有表达的请求的代码。在一方面,该请求可包括至少对与该私有表达相关联的表达码的引用。进一步,该计算机可读介质可包括,用于由表达验证管理器(EVM)确定此至少对该表达码的引用是否对应于之前获得并存储着的该表达码的实例的代码。在一方面,该计算机可读介质可包括用于一旦确定该表达码对应于存储着的该表达码的实例,就宣告该私有表达或该表达码中的至少一者的代码。附加地或替换地,在一方面,该计算机可读介质可包括用于一旦确定该表达码不对应于存储着的该表达码的实例,就禁止宣告与该私有表达相关联的信息的代码。

[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是无线通信方法的流程图。

[0025] 图9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。

[0026] 图10是解说采用处理系统的装置的硬件实现的示例的示图。

[0027] 详细描述

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 相应地，在一个或多个示例性实施例中，所描述的功能可以在硬件、软件、固件、或其任何组合中实现。如果在软件中实现，则各功能可作为一条或多条指令或代码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。作为示例而非限定，这样的计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储、磁盘存储或其它磁存储设备、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它介质。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。上述的组合应当也被包括在计算机可读介质的范围内。

[0032] 图1是解说LTE网络架构100的图示。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。

[0033] 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也可被称为基站、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。UE 102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。

[0034] 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)。

[0035] 图2是解说LTE网络架构中的接入网200的示例的示图。在此示例中，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到设备通信中。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。

[0036] 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。

[0037] 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。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。

[0038] 图4是解说LTE中的UL帧结构的示例的示图400。UL可用的资源块可被划分成数据区段和控制区段。控制区段可形成在系统带宽的两个边缘处并且可具有可配置的大小。控制区段中的资源块可被指派给UE以用于传输控制信息。数据区段可包括所有未被包括在控制区段中的资源块。该UL帧结构导致数据区段包括毗连副载波,这可允许单个UE被指派数据区段中的所有毗连副载波。

[0039] UE可被指派有控制区段中的资源块410a、410b以用于向eNB传送控制信息。UE也可被指派有数据区段中的资源块420a、420b以用于向eNB传送数据。UE可在控制区段中的获指派资源块上在物理UL控制信道(PUCCH)中传送控制信息。UE可在数据区段中的获指派资源块上在物理UL共享信道(PUSCH)中仅传送数据或者传送数据和控制信息两者。UL传输可横跨子帧的这两个时隙,并可跨频率跳跃。

[0040] 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。

[0041] 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和eNB的无线电协议架构502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。

[0042] 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之上可具有若干个上层,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)的应用层。

[0043] 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。

[0044] 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。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之间的RRC信令来配置各下层。用户面还包括网际协议(IP)子层518和应用(APP)子层520。IP子层518和应用子层520负责支持eNB与UE之间的应用数据通信。

[0045] 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。

[0046] 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。随后经编码和经调制的码元被拆分成并行流。每个流随后被映射到OFDM子载波、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。

[0047] 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信号的每个子载波包括单独的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。

[0048] 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可被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。

[0049] 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WAN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。

[0050] 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。

[0051] 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。

[0052] 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可被称为计算机可读介质。在UL中，控制器/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、报头解压缩、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。

[0053] 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702、704。在任选的方面，设备对设备通信系统700还可包括可操作以与无线设备702、704中的一个或多个无线设备通信的应用服务器706。

[0054] 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702、704中的一些可以使用DL/UL WWAN频谱和/或无执照频谱(例如，WiFi)按设备对设备通信的方式来一起通信，一些可与基站通信，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，该多个基站可通过经由一个或多个网络实体(例如，MME等)提供的连通性来提供协作式通信环境。

[0055] 无线设备702可包括应用处理器720、表达验证管理器730和调制解调器处理器及其他组件等。在一方面，应用处理器可被配置成启用一个或多个应用722。在此类方面，应用722可包括用于向一个或多个其他获授权的对等方设备(例如，无线设备704)宣告的私有表达724。如图7中所描绘的，每个私有表达可具有相关联的表达码726。表达码726可由接收方无线设备截取并使用，以辅助访问私有表达724。进一步，表达码726可被用以辅助私有表达724自验证(例如，确认请求方应用722与生成/存储了该表达码的设备相关联)。

[0056] 表达验证管理器730可包括安全存储器存储732(例如，安全非易失性存储器)。在一方面，表达验证管理器730可作为应用722配置/重配置过程的一部分地来生成私有表达码。例如，作为应用722安装的一部分，表达验证管理器730可生成私有表达码。在一示例中，表达验证管理器730在应用722被重配置以改变与私有表达相关联的访问特征(例如，哪些对等方设备704被允许访问该私有表达)时可生成经更新的私有表达码。在一方面，表达验证管理器730可生成与每个应用722相关联的多个私有表达码。在另一方面，安全存储器存储732可安全地存储所生成的私有表达码。虽然图7将表达验证管理器730描绘为与应用处理器720和调制解调器处理器740分开的模块，但是表达验证管理器730也可驻留在应用处理器720、调制解调器740、或其任何组合中。进一步，在一方面，表达验证管理器730可作为

应用处理器720与调制解调器处理器740之间的接口。在另一方面，表达验证管理器730的第一部分可与调制解调器处理器740相关联，并且表达验证管理器730的第二部分可被配置为应用处理器720与调制解调器处理器740之间的中间层。在另一方面，安全存储器存储732可存储来自其他设备704的信息(例如，不透明D2D信息712)。在此类方面，接收到的信息可具有生存时间(TTL)值。在另一方面，TTL值可以是本地生成的。调制解调器处理器740可配置成使用一个或多个无线电接入技术(RAT)来接收和传送信息。

[0057] 应用服务器706可被配置成存储与私有表达通信相关联的信息。在一方面，应用服务器706可在将私有表达码726分发给无线设备(例如，702、704)上的应用722时遵守用户选定的关系。在一方面，受信任应用服务器706可生成要被存储在安全存储器存储732中的表达码714。

[0058] 在一操作方面，作为应用722配置/重配置过程的一部分，不透明D2D信息模块736可辅助无线设备702生成不透明D2D信息712。在一方面，不透明D2D信息712可被直接传送给获授权的无线设备704。在另一方面，不透明D2D信息712可被传达给应用服务器706，用于存储在私有表达存储708中并传达给一个或多个获授权的无线设备704。在一方面，不透明D2D信息712可包括私有表达724、表达码726、应用722的名称、计数器、生成时间、之前生成的表达码、过期日期、宣告方无线设备702的证书等等。在另一方面，不透明D2D信息712可用指示此不透明D2D信息712的真实性的数字签名来签名。在此类方面，该数字签名可包括经运营商签名的密钥、临时设备标识符、TTL值等。

[0059] 在另一操作方面，与无线设备702相关联的应用722可请求私有表达724被宣告。在此类方面，应用722可将此请求随私有表达724和相关联的表达码726一起发送给表达验证管理器730。表达验证管理器730可被配置成将接收到的表达码726与存储在安全存储器存储732中的私有表达码734进行比较。若表达码726匹配于存储着的私有表达码734，那么表达验证管理器730允许调制解调器处理器740宣告710私有表达724。与之形成对比的是，若表达码726不匹配于存储着的私有表达码734，那么表达验证管理器730禁止调制解调器处理器740宣告710私有表达724。

[0060] 无线设备可替换地被本领域技术人员称为用户装备(UE)、移动站、订户站、移动单元、订户单元、无线单元、无线节点、远程单元、移动设备、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、或某个其它合适术语。

[0061] 下文中讨论的示例性方法和装置适用于各种无线设备对设备通信系统中的任一种，诸如举例而言基于FlashLinQ、WiMedia、蓝牙、ZigBee或以IEEE802.11标准为基础的Wi-Fi的无线设备对设备通信系统。为了简化讨论，在LTE的上下文内讨论了示例性的方法和装置。然而，本领域普通技术人员将理解，这些示例性方法和装置更一般地可适用于各种其它无线设备到设备通信系统。

[0062] 图8和图11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。

[0063] 图8是第二无线通信方法的流程图800。该方法可由UE来执行。

[0064] 在任选的方面，在框802，UE可作为对应用和相关联的私有表达的配置过程的一部分地来生成表达码。在一方面，该表达码可被用于访问控制，例如，用于过滤哪些人被允许访问对应的私有表达。例如，在启用D2D的应用首次被安装时(和/或发生解除好友关系时，例如，撤销私有表达访问授权)，UE可生成私有表达和与该私有表达相关联的表达码二者。在一方面，当该表达码在越空使用时，UE可重新生成该表达码而不生成私有表达。

[0065] 附加地或替换地，在任选的方面，在框814，UE可从受信任的服务器安全地接收表达码。

[0066] 在一方面，在框804，UE可存储所生成的表达码。在一方面，该表达码可被存储在密钥存储中。在此类方面，密钥存储可包括用于数据和代码的受保护的非易失性物理存储器。密钥存储可维护用于所宣告的私有表达的本地密钥(例如，码)。在另一任选方面，密钥存储维护并且任选地验证用于所监视的私有表达的远程密钥。在此类方面，对远程密钥的验证包括检查远程UE已授权本UE监视该表达，例如通过采用签名验证来进行此检查。

[0067] 在任选的方面，UE也可传送与该表达码相关联的不透明D2D信息。在此类方面，不透明D2D信息可被传送给另一UE和/或受信任应用服务器。进一步，在此类方面，此不透明D2D信息可包括私有表达、表达码、应用的名称、计数器、生成时间、之前生成的表达码、过期日期、宣告方UE的证书等等。在另一方面，不透明D2D信息可以用指示该不透明D2D信息的真实性的数字签名来签名。在此类方面，该数字签名可包括经运营商签名的密钥、临时设备标识符、存活时间(TTL)值等。

[0068] 在框808，UE可从应用接收请求，该请求包括表达码(和/或对该表达码的引用)并且请求对相关联的私有表达的宣告。

[0069] 在框810，UE可确定随该宣告请求一起包括的表达码是否匹配于所存储的此请求方应用的表达码。在一方面，与UE相关联的表达验证管理器(EVM)可执行该确定。在此类方面，EVM可以是驻留在UE应用处理器(当其为高级别操作系统(HLOS)“服务”的一部分时)中、调制解调器处理器中、或其任何组合中的受信任实体。进一步，在一方面，EVM可作为应用与该UE的调制解调器处理器之间的接口。在另一方面，EVM的第一部分可与UE的调制解调器相关联，并且EVM的第二部分可被配置为应用层与UE的调制解调器之间的中间层。

[0070] 若在框810，UE确定随宣告请求一起包括的表达码匹配于存储着的该请求方应用的表达码，那么在框812，UE可宣告该私有表达。

[0071] 与之形成对比的是，若在框810，UE确定随宣告请求一起包括的表达码不匹配于存储着的该请求方应用的表达码，那么在框814，UE可禁止宣告该私有表达。

[0072] 图9是解说示例性设备900中的不同模块/装置/组件之间的数据流的概念性数据流图902。该设备可以是UE。

[0073] 设备902包括可从应用接收要宣告私有表达922的请求920的应用处理模块910。在一方面，请求920可包括表达码916和/或对表达码916的引用。在一方面，表达码916可由应

用配置模块906生成并且存储在安全存储器模块908中。在任选的方面，表达码916可使用接收模块904来从受信任应用服务器706接收。设备902可进一步包括私有表达验证模块912，其可被配置成将随请求920一起接收到的表达码916和/或对表达码916的引用与存储在安全存储器模块908中的表达码916进行比较。在一方面，私有表达验证模块912可被实现为如针对表达验证管理器730所描述的。在表达码916匹配的场合，私有表达验证模块912提示传送模块914宣告私有表达922。与之形成对比的是，在表达码916不匹配的场合，私有表达验证模块912禁止传送模块914宣告私有表达922。在另一方面，应用配置模块906可生成与该表达码相关联的不透明D2D信息918以用于使用传送模块914来传送。在此类方面，不透明D2D信息918可被传送给另一UE(例如，UE 704)和/或受信任应用服务器706。进一步，在此类方面，不透明D2D信息918可包括私有表达、表达码、应用的名称、计数器、生成时间、之前生成的表达码、过期日、宣告方UE的证书等等。在另一方面，不透明D2D信息918可用指示该不透明D2D信息的真实性的数字签名来签名。

[0074] 该设备可包括执行图8的前述流程图中的算法的每个步骤的附加模块。如此，图8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。

[0075] 图10是解说采用处理系统1014的设备902'的硬件实现的示例的示图1000。处理系统1014可实现成具有由总线1024一般化地表示的总线架构。取决于处理系统1014的具体应用和整体设计约束，总线1024可包括任何数目的互连总线和桥接器。总线1024将包括一个或多个处理器和/或硬件模块(由处理器1004、模块804、806、808、810和计算机可读介质1006表示)的各种电路链接在一起。总线1024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，且因此将不再进一步描述。

[0076] 处理系统1014可耦合至收发机1010。收发机1010被耦合至一个或多个天线1020。收发机1010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1014包括耦合至计算机可读介质1006的处理器1004。处理器1004负责一般性处理，包括执行存储在计算机可读介质1006上的软件。该软件在由处理器1004执行时使处理系统1014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1006还可被用于存储由处理器1004在执行软件时操纵的数据。处理系统进一步包括模块904、906、908、和910中的至少一个模块。各模块可以是在处理器1004中运行的软件模块、驻留/存储在计算机可读介质1006中的软件模块、耦合至处理器1004的一个或多个硬件模块、或其某种组合。处理系统1014可以是UE 650的组件且可包括存储器660和/或包括TX处理器668、RX处理器656、和控制器/处理器659中的至少一者。

[0077] 在一个配置中，用于无线通信的设备902/902'包括用于接收要宣告私有表达的请求(该请求包括与私有表达相关联的表达码)的装置、用于由表达验证管理器(EVM)确定该表达码是否对应于之前获得并存储着的该表达码的实例的装置、用于一旦确定该表达码对应于存储着的该表达码的实例，就宣告该私有表达或该表达码中的至少一者的装置、和/或用于一旦确定该表达码不对应于存储着的该表达码的实例，就禁止宣告与该私有表达相关联的信息的装置。在另一方面，设备902/902'用于作为应用的配置过程的一部分地来获得

表达码的实例的装置。在此类方面，设备902/902'可包括用于将表达码的实例存储在安全存储器存储中的装置。在另一方面，设备902/902'可包括用于传送与该表达码相关联的不透明D2D信息的装置。在另一方面，设备902/902'用于生成的装置可被进一步配置成生成指示此不透明D2D信息的真实性的数字签名，并且其中此不透明D2D信息随所生成的数字签名一起传送。在一方面，设备902/902'可包括用于从受信任的服务器安全地获得表达码的实例的装置。在此类方面，设备902/902'可包括用于将表达码的实例存储在安全存储器存储中的装置。前述装置可以是设备902和/或设备902'的处理系统1014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个或多个模块。如前文所述，处理系统1014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叙述的功能的TX处理器668、RX处理器656、以及控制器/处理器659。

[0078] 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。

[0079] 本文中使用措词"示例性"来表示用作示例、实例或解说。本文中描述为"示例性"的任何方面或设计不必被解释为优于或胜过其他方面或设计。另外，如本文中所使用的，引述一列项目中的"至少一个"和/或"一个或多个"的短语是指这些项目的任何组合，包括单个成员。作为示例，"a、b或c中的至少一者"旨在涵盖：a、b、c、a-b、a-c、b-c、以及a-b-c。

[0080] 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。

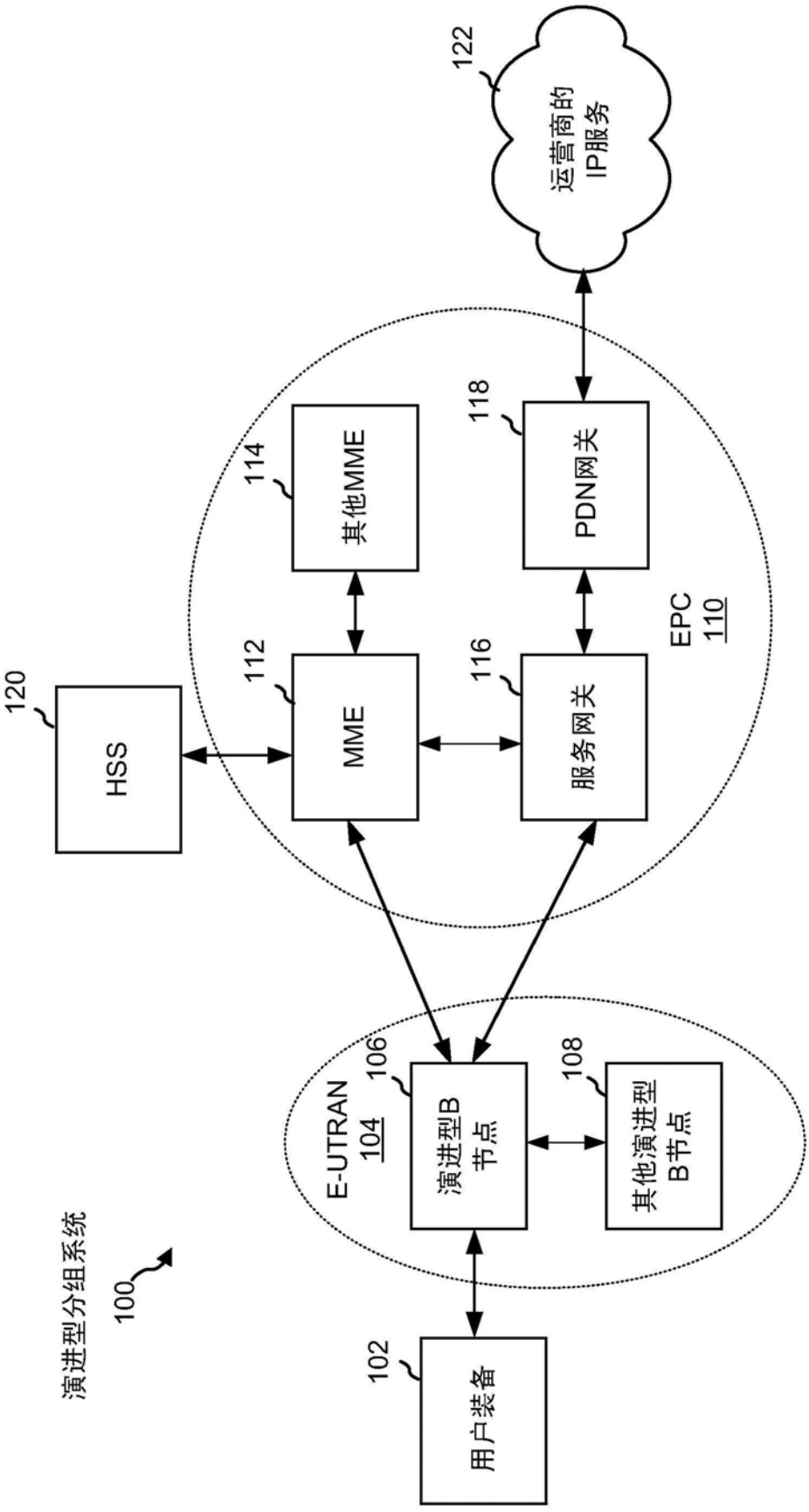

演进型分组系统
100
用户装备
102
E-UTRAN
104
演进型B节点
106
其他演进型B节点
108
HSS
120
MME
112
其他MME
114
服务网关
116
PDN网关
118
EPC
110
运营商的IP服务
122

图1

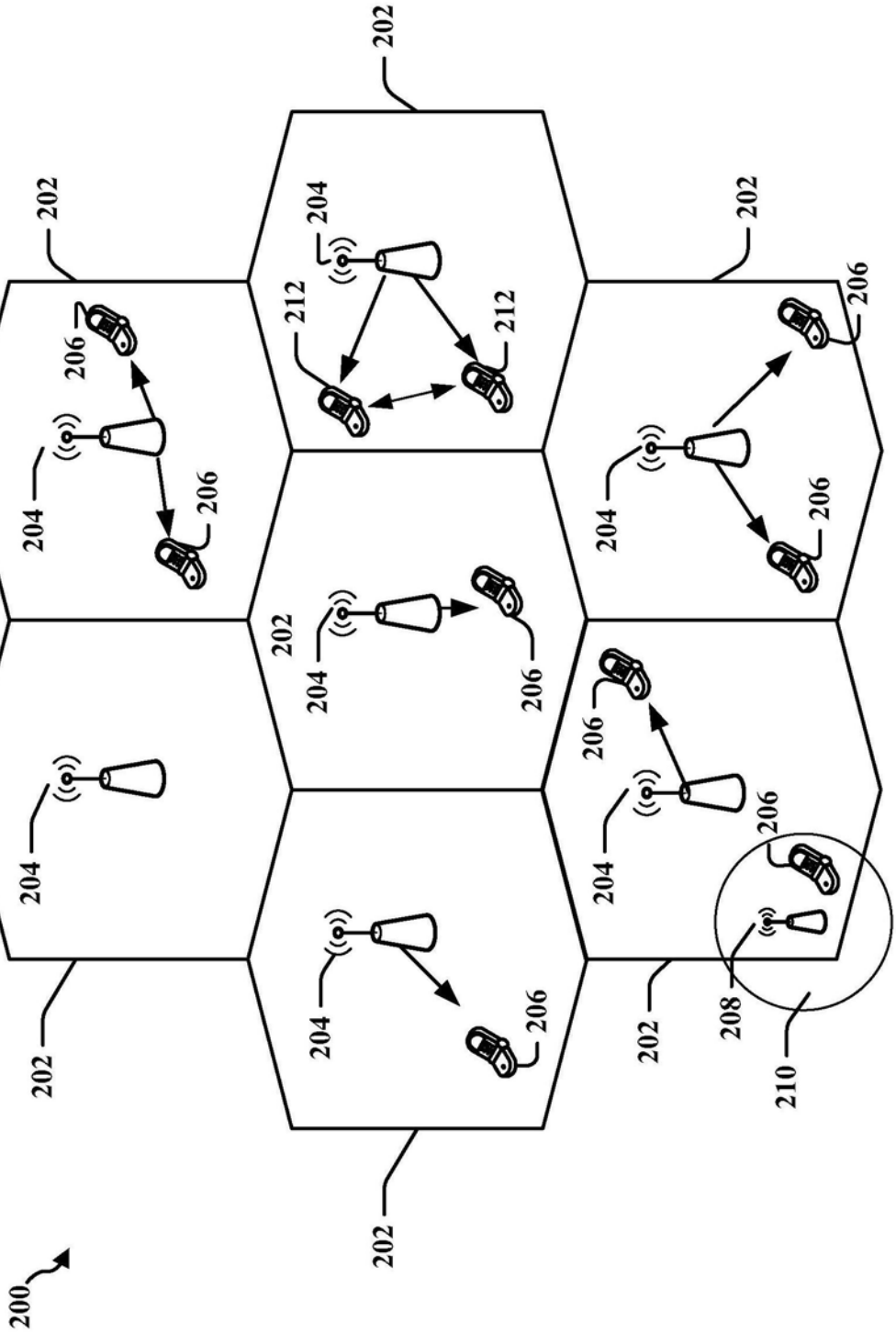


图2

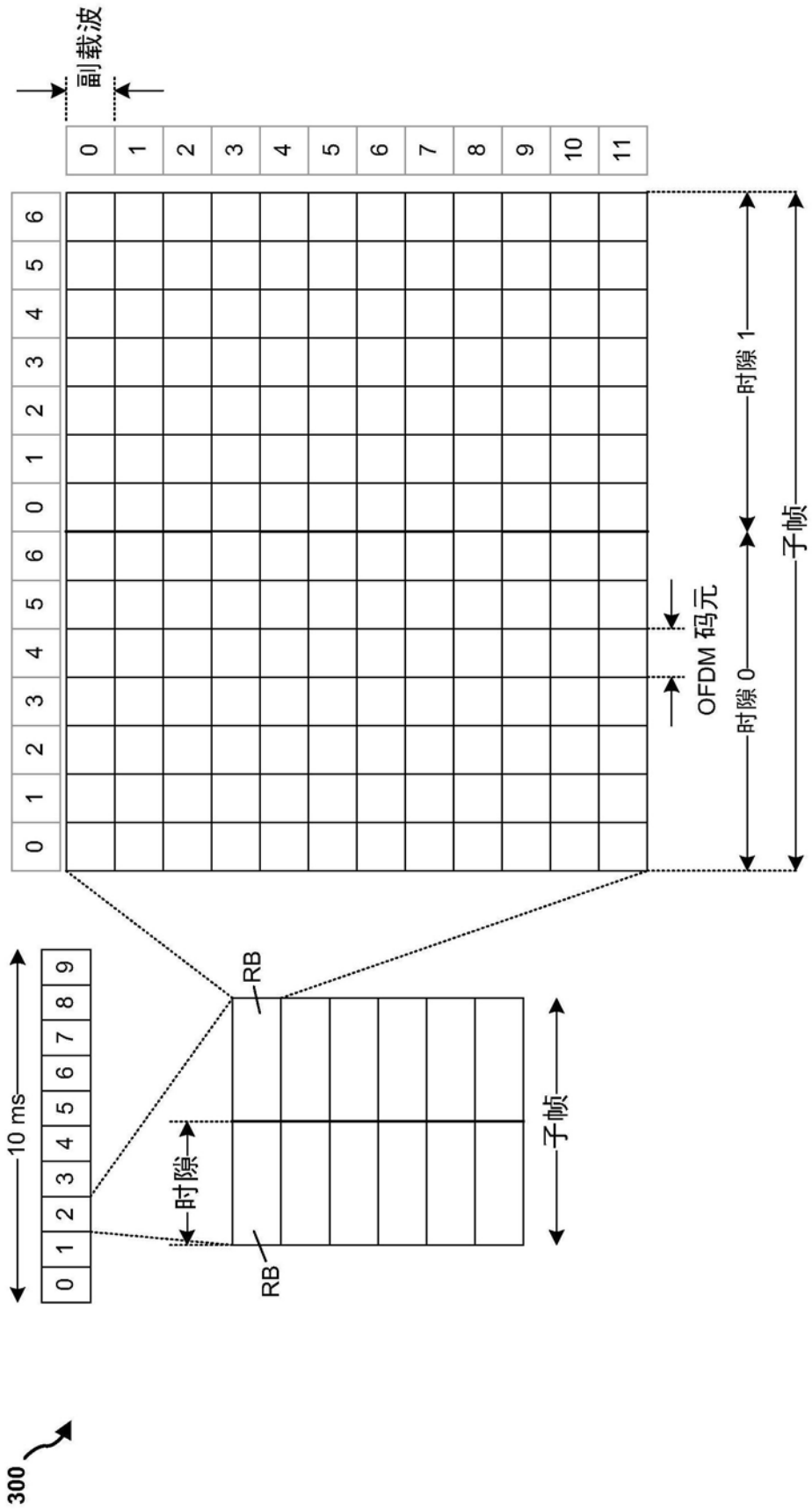

副载波
0 1 2 3 4 5 6 7 8 9 10 11
0 1 2 3 4 5 6 0 1 2 3 4 5 6
OFDM 码元
时隙 0
时隙 1
子帧
10 ms
0 1 2 3 4 5 6 7 8 9
时隙
RB
RB
子帧
300

图3

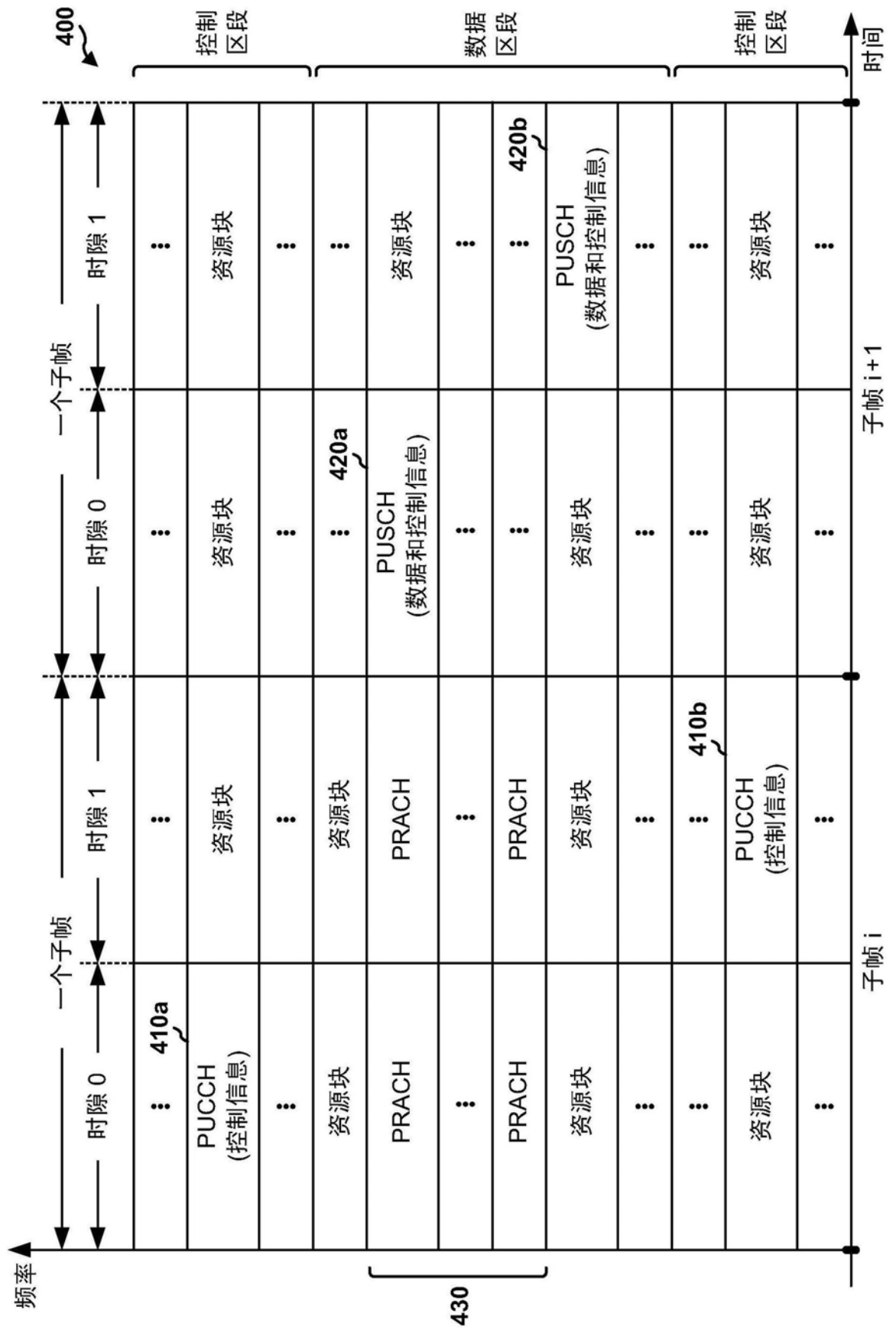

400
控制区段
数据区段
控制区段
时间
频率
一个子帧
一个子帧
时隙 0
时隙 1
时隙 0
时隙 1
410a
PUCCH
(控制信息)
资源块
420a
PUSCH
(数据和控制信息)
420b
PUSCH
(数据和控制信息)
PRACH
410b
PUCCH
(控制信息)
430
子帧 i
子帧 i+1

图4

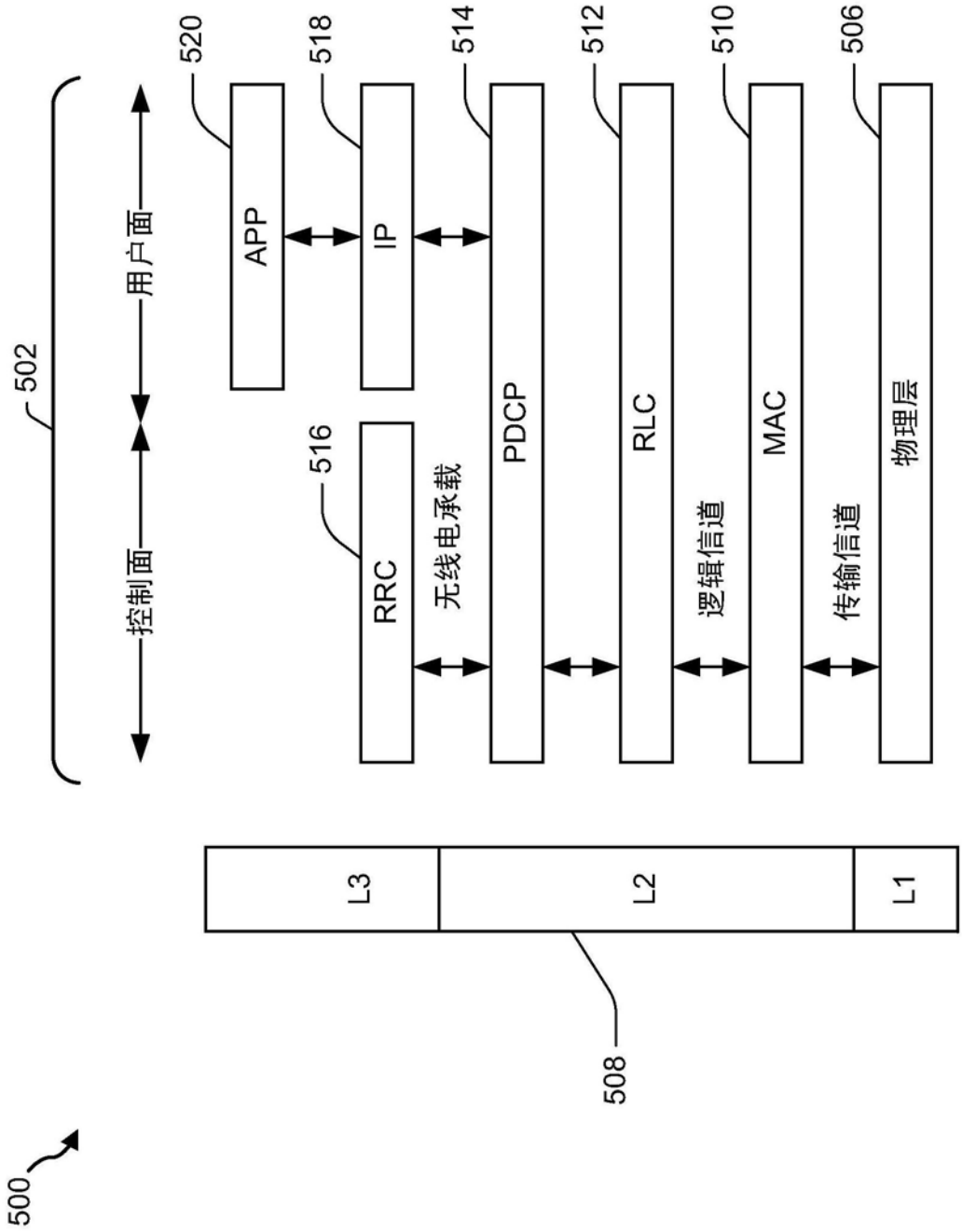

500
502
用户面
控制面
520
APP
518
IP
516
RRC
514
无线电承载
PDCP
512
RLC
510
逻辑信道
MAC
506
传输信道
物理层
L3
L2
L1
508

图5

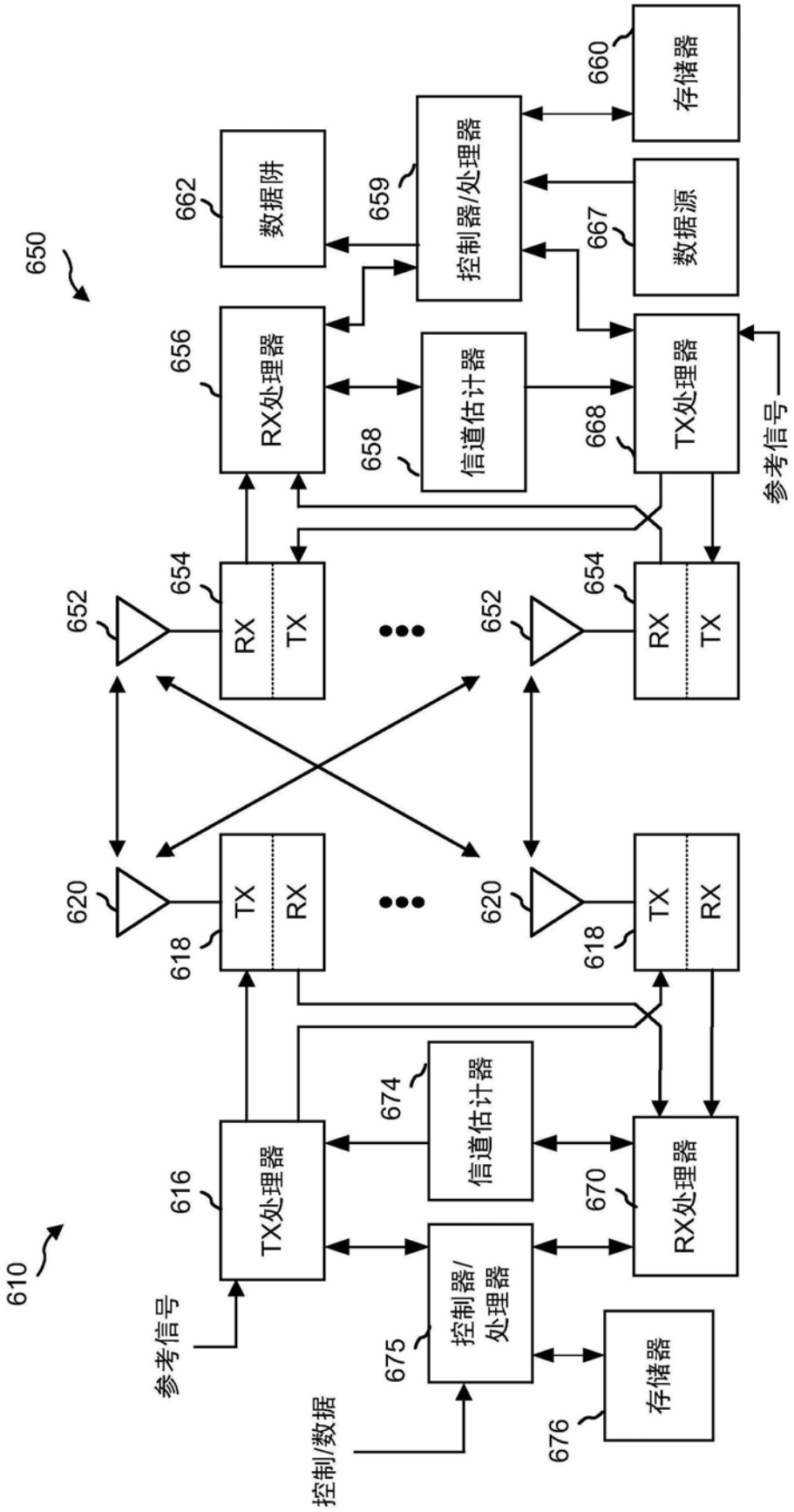

650
662
数据阱
659
控制器/处理器
660
存储器
667
数据源
656
RX处理器
658
信道估计器
668
TX处理器
参考信号
654
652
RX
TX
620
618
610
616
TX处理器
674
信道估计器
670
RX处理器
参考信号
675
控制器/
处理器
676
存储器
控制/数据

图6

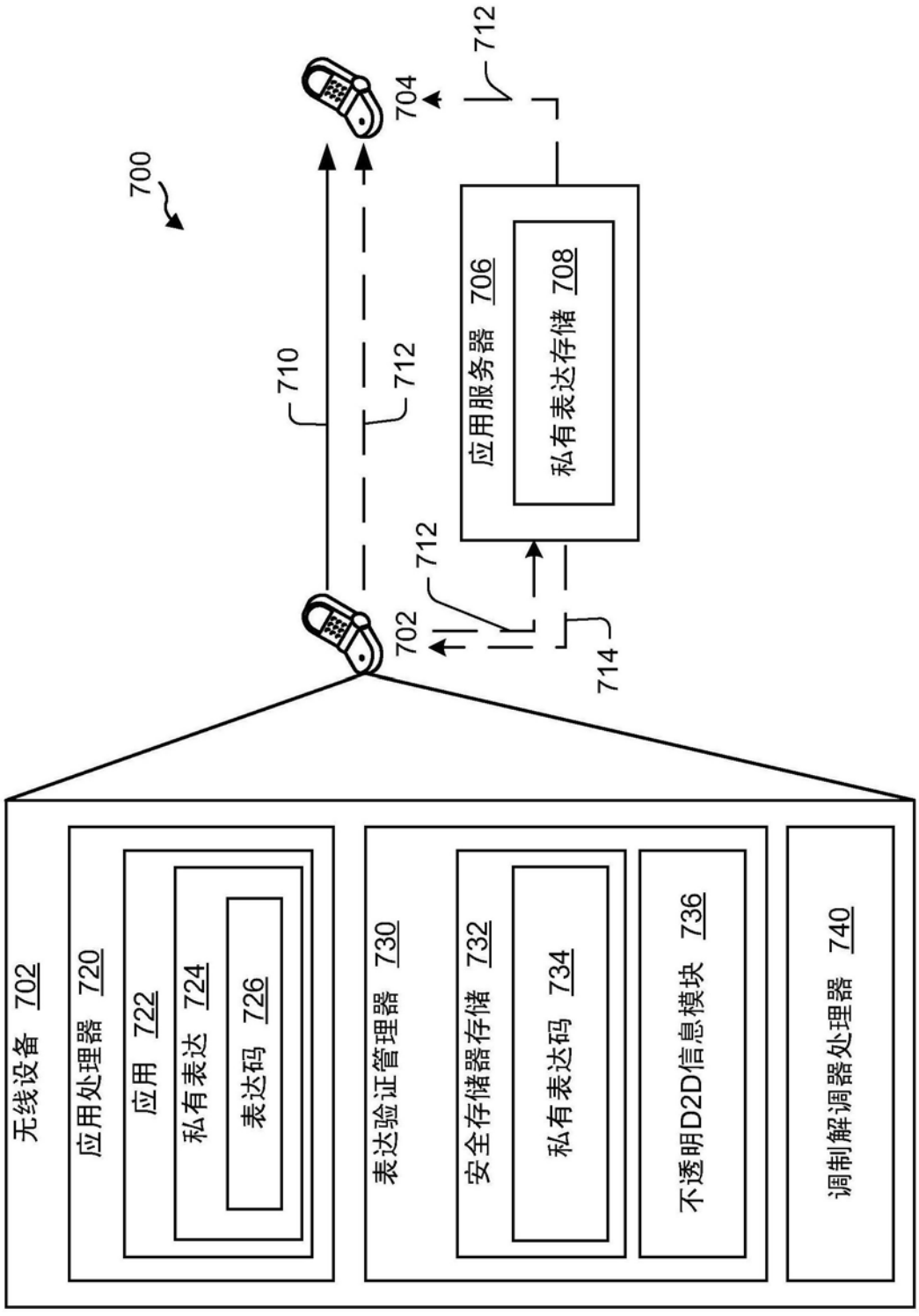

700
704
712
710
712
712
702
714
应用服务器 706
私有表达存储 708
无线设备 702
应用处理器 720
应用 722
私有表达 724
表达码 726
表达验证管理器 730
安全存储器存储 732
私有表达码 734
不透明D2D信息模块 736
调制解调器处理器 740

图7

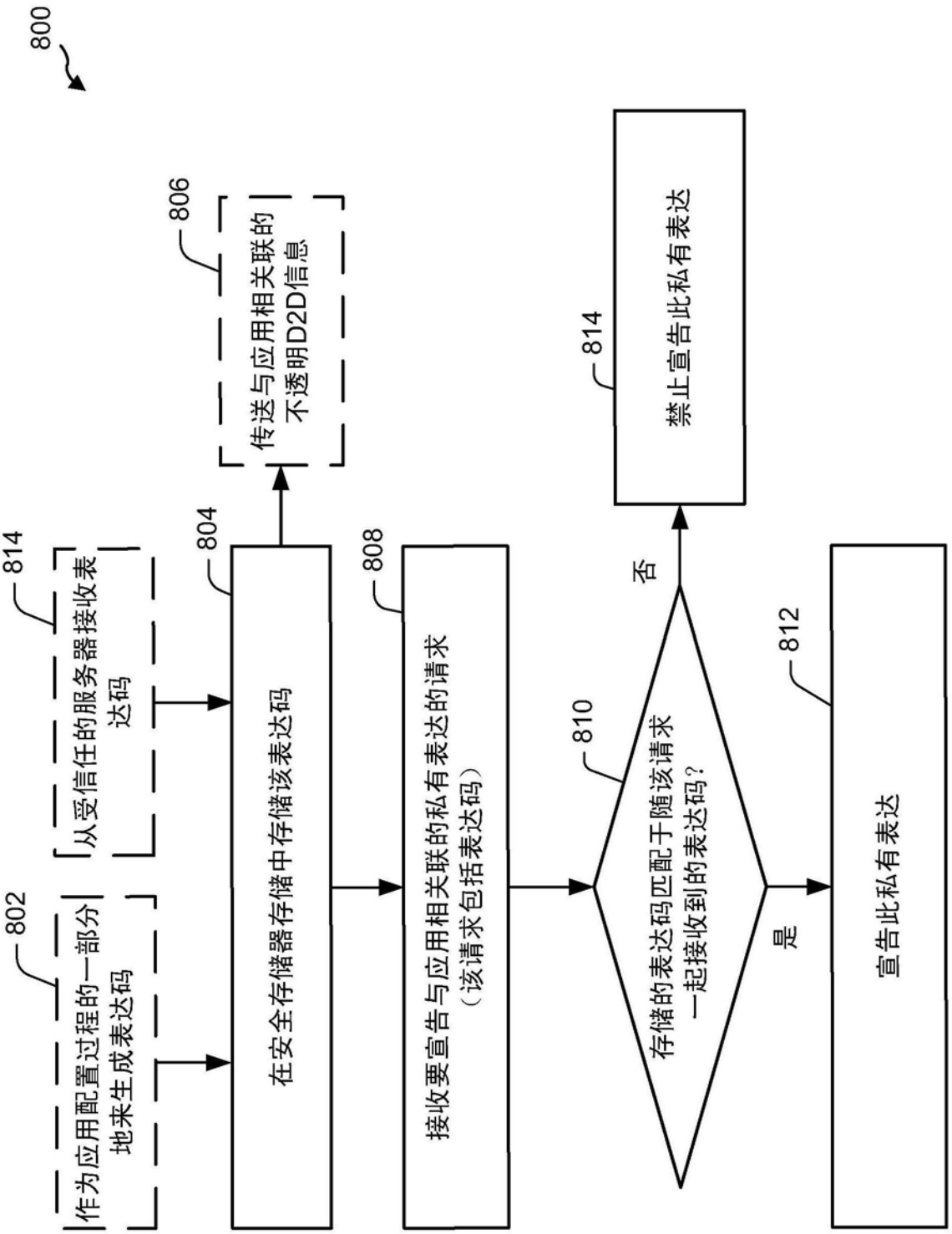

800
802
作为应用配置过程的一部分地来生成表达码
814
从受信任的服务器接收表达码
804
在安全存储器存储中存储该表达码
806
传送与应用相关联的不透明D2D信息
808
接收要宣告与应用相关联的私有表达的请求（该请求包括表达码）
810
存储的表达码匹配于随该请求一起接收到的表达码？
否
814
禁止宣告此私有表达
是
812
宣告此私有表达

图8

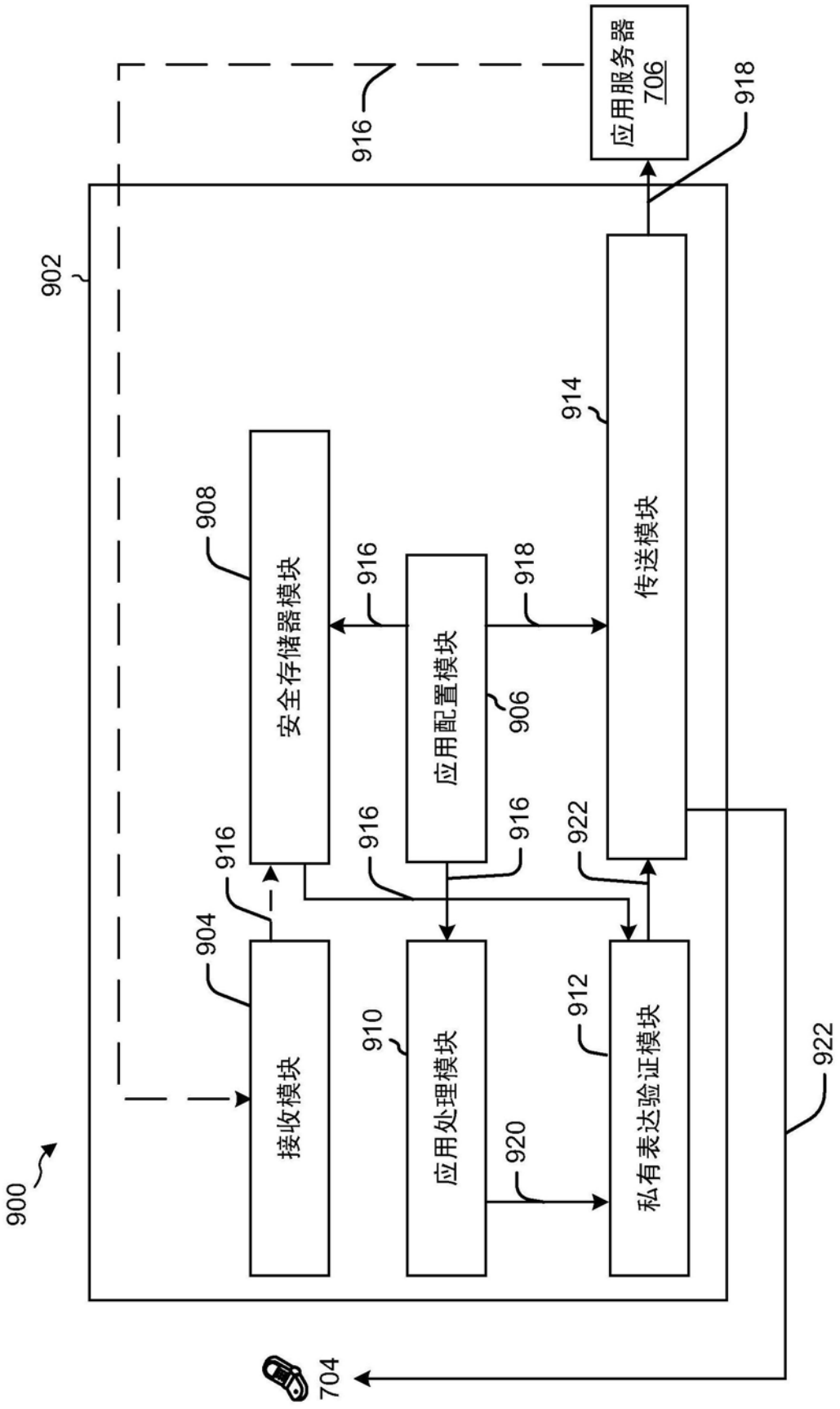

应用服务器
706
916
918
902
914
908
安全存储器模块
916
应用配置模块
906
918
传送模块
916
916
922
904
接收模块
910
应用处理模块
912
私有表达验证模块
920
922
900
704

图9

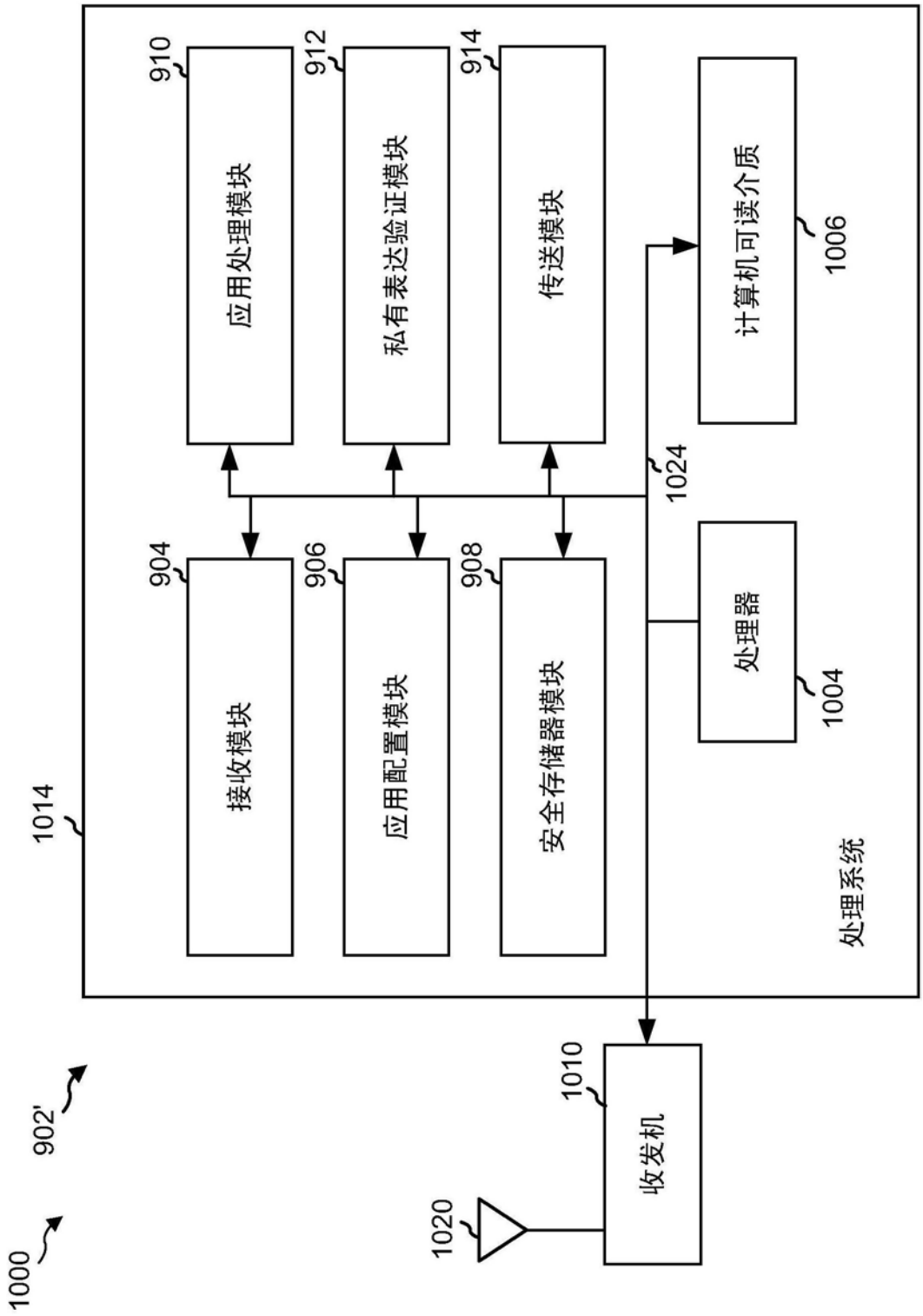

1000
902'
1014
处理系统
应用处理模块
910
私有表达验证模块
912
传送模块
914
计算机可读介质
1006
1024
接收模块
904
应用配置模块
906
安全存储器模块
908
处理器
1004
1010
收发机
1020

图10