(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 106105140 B
(45)授权公告日 2020.01.10

(21)申请号 201580013814.1

(22)申请日 2015.01.30

(65)同一申请的已公布的文献号
申请公布号 CN 106105140 A

(43)申请公布日 2016.11.09

(30)优先权数据
61/955,601 2014.03.19 US
14/609,003 2015.01.29 US

(85)PCT国际申请进入国家阶段日
2016.09.13

(86)PCT国际申请的申请数据
PCT/US2015/013804 2015.01.30

(87)PCT国际申请的公布数据
WO2015/142430 EN 2015.09.24

(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 H•程 S•K•巴盖尔
A•E•艾斯科特

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 唐杰敏

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/10(2006.01)

审查员 刘莹

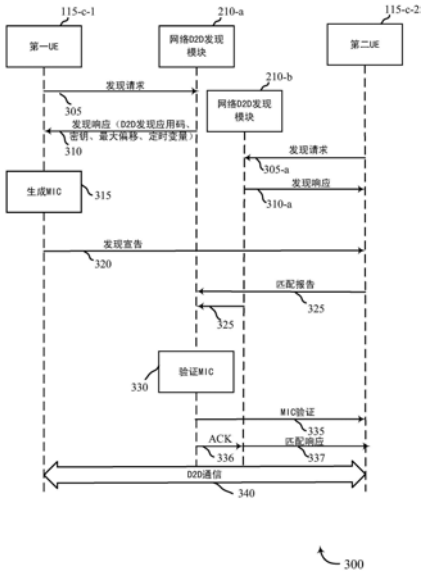
权利要求书3页 说明书25页 附图22页

(54)发明名称

在长期演进设备到设备发现中防止重放攻击

(57)摘要

描述了用于设备到设备(D2D)无线通信的方法、系统和设备。一设备可在该设备处于连通模式时接收来自网络的定时变量。该设备可随后将该定时变量用于D2D发现消息认证。该设备可将该定时变量与本地定时变量进行比较以确定这两个变量之间的差异是否在最大可允许偏移内。当该差异在最大可允许偏移内时,该设备可向另一设备宣告D2D发现消息。



CN 106105140 B

1.一种用于在无线网络中进行无线通信的方法,包括:

在设备处接收来自网络的定时变量和定时偏移允许,所述定时变量是在所述设备处于连通模式时接收的;以及

通过将所接收到的定时变量与本地定时变量进行比较以确定所接收到的定时变量与所述本地定时变量之间的差异是否在所述定时偏移允许内来将所接收到的定时变量和所述定时偏移允许用于设备到设备(D2D)发现消息认证。

2.如权利要求1所述的方法,其特征在于,进一步包括:

在所述设备处存储所接收到的定时变量以与本地定时变量进行比较。

3.如权利要求1所述的方法,其特征在于,所述定时变量是从所述网络中的基于邻近度的服务(ProSe)功能接收的。

4.如权利要求1所述的方法,其特征在于,所述定时变量是与D2D发现应用码一起被接收的。

5.如权利要求3所述的方法,其特征在于,进一步包括:

从所述网络中的所述ProSe功能接收所述定时偏移允许。

6.如权利要求5所述的方法,其特征在于,进一步包括:

当所接收到的定时变量与所述本地定时变量之间的所述差异在所述定时偏移允许内时,宣告D2D发现应用码。

7.如权利要求5所述的方法,其特征在于,进一步包括:

当所述差异大于所述定时偏移允许时,向所述ProSe功能通知异常。

8.如权利要求5所述的方法,其特征在于,接收自所述网络的所述定时变量是协调世界时(UTC)。

9.如权利要求5所述的方法,其特征在于,进一步包括:

经由系统信息块(SIB)来接收所述本地定时变量。

10.如权利要求1所述的方法,其特征在于,进一步包括:

向所述网络发送包括基于邻近度的服务(ProSe)应用标识(ID)的发现请求。

11.如权利要求10所述的方法,其特征在于,进一步包括:

从所述网络接收发现响应,所述发现响应包括所述定时变量和所述定时偏移允许。

12.如权利要求1所述的方法,其特征在于,进一步包括:

使用接收自所述网络的所述定时变量来生成要被包括在D2D发现宣告中的消息完整性码(MIC)。

13.如权利要求12所述的方法,其特征在于,所述MIC是在传送所述D2D发现宣告时基于D2D发现应用码、与所述D2D发现应用码相关联的密钥、以及所述定时变量来生成。

14.如权利要求1所述的方法,其特征在于,进一步包括:

接收包括消息完整性码(MIC)的D2D发现宣告;以及

向所述网络中的基于邻近度的服务(ProSe)功能传送所接收到的MIC和所述定时变量。

15.如权利要求9所述的方法,其特征在于,进一步包括:

如果所述设备检测到具有定时信息的一个以上SIB,则忽略所述SIB中接收到的所述本地定时变量;以及

在所述SIB以外获得所述本地定时变量。

16.如权利要求9所述的方法,其特征在于,进一步包括:

将系统信息块(SIB)中接收到的所述定时变量与本地定时变量进行比较;以及

如果所接收到的定时变量与所述本地定时变量相差超过预定阈值,则在所述SIB以外获得所述定时变量。

17.如权利要求1所述的方法,其特征在于,进一步包括:

当所述设备正在使用受网络控制的D2D发现资源分配方案时,经由无线电资源控制(RRC)消息来请求D2D发现资源,

其中所述定时变量是经由对所述RRC消息的响应来接收的。

18.如权利要求1所述的方法,其特征在于,进一步包括:

接收包括所述定时变量和空资源分配元素的无线电资源控制(RRC)消息。

19.如权利要求5所述的方法,其特征在于,进一步包括:

当所述差异小于所述定时偏移允许时,将接收自所述ProSe功能的所述定时变量与所述本地定时变量同步。

20.一种被配置成用于无线通信的装置,包括:

至少一个处理器;以及

耦合至所述至少一个处理器的存储器,其中所述至少一个处理器被配置成:

在设备处接收来自网络的定时变量和定时偏移允许,所述定时变量是在所述设备处于连通模式时接收的;以及

通过将所接收到的定时变量与本地定时变量进行比较以确定所接收到的定时变量与所述本地定时变量之间的差异是否在所述定时偏移允许内来将所接收到的定时变量和所述定时偏移允许用于设备到设备(D2D)发现消息认证。

21.如权利要求20所述的装置,其特征在于,所述定时变量是从所述网络中的基于邻近度的服务(ProSe)功能接收的。

22.如权利要求21所述的装置,其特征在于,所述至少一个处理器被进一步配置成:

从所述网络中的所述ProSe功能接收所述定时偏移允许。

23.如权利要求22所述的装置,其特征在于,所述至少一个处理器被进一步配置成:

如果所接收到的定时变量与所述本地定时变量之间的所述差异在所述定时偏移允许内时,则宣告D2D发现码。

24.一种用于在无线网络中进行无线通信的方法,包括:

进入与设备的连通模式;以及

当所述设备处于所述连通模式时向所述设备传送定时变量和定时偏移允许以供在设备到设备(D2D)发现消息认证中使用,其中所述定时变量被用于将所述定时变量与本地定时变量进行比较以确定所述定时变量与所述本地定时变量之间的差异是否在所述定时偏移允许内。

25.如权利要求24所述的方法,其特征在于,所述定时变量是从基于邻近度的服务(ProSe)功能传送的。

26.如权利要求24所述的方法,其特征在于,进一步包括:

连同D2D发现应用码一起传送所述定时变量。

27.如权利要求24所述的方法,其特征在于:

所述定时偏移允许是所述定时变量与所述设备处的所述本地定时变量之间的最大差异。

28.如权利要求24所述的方法,其特征在于,进一步包括:

从所述设备接收包括基于邻近度的服务(ProSe)应用标识(ID)的发现请求;以及

向所述设备发送发现响应,所述发现响应包括所述定时变量和所述定时偏移允许。

29.如权利要求24所述的方法,其特征在于,进一步包括:

接收对发现资源的无线电资源控制(RRC)请求,

其中传送所述定时变量包括传送对所述RRC请求的响应,所述响应包括所述定时变量。

30.一种被配置成用于无线通信的装置,包括:

至少一个处理器;以及

耦合至所述至少一个处理器的存储器,其中所述至少一个处理器被配置成:

进入与设备的连通模式;以及

当所述设备处于所述连通模式时向所述设备传送定时变量和定时偏移允许以供在设备到设备(D2D)发现消息认证中使用,其中所述定时变量被用于将所述定时变量与本地定时变量进行比较以确定所述定时变量与所述本地定时变量之间的差异是否在所述定时偏移允许内。

在长期演进设备到设备发现中防止重放攻击

[0001] 交叉引用

[0002] 本专利申请要求由Cheng等人于2015年1月29日提交的题为“Prevention of Replay Attack in Long Term Evolution Device-to-Device Discovery(在长期演进设备到设备发现中防止重放攻击)”的美国专利申请No.14/609,003、以及由Cheng等人于2014年3月19日提交的题为“Prevention of Replay Attack in Long Term Evolution Device-to-Device Discovery(在长期演进设备到设备发现中防止重放攻击)”的美国临时专利申请No.61/955,601的优先权;其中的每一件申请均被转让给本申请受让人。

[0003] 背景

[0004] 公开领域

[0005] 本公开例如涉及无线通信系统,并且尤其涉及在长期演进设备到设备发现中防止重放攻击。

[0006] 相关技术描述

[0007] 无线通信系统被广泛部署以提供诸如语音、视频、分组数据、消息接发、广播等各种类型的通信内容。这些系统可以是能够通过共享可用系统资源(例如,时间、频率和功率)来支持与多个用户通信的多址系统。此类多址系统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、以及正交频分多址(OFDMA)系统。一般而言,无线多址通信系统可包括数个基站,每一基站同时支持多个用户设备的通信。基站可在下行和上行链路上与诸设备通信。每一基站具有覆盖范围,其可被称为基站或蜂窝小区的覆盖区域。

[0008] 彼此邻近的设备(即,用户装备(UE))也可经由设备到设备(D2D) 或基于邻近度的服务(ProSe)通信来直接通信。然而,这种直接通信包括潜在的安全性弱点。具体地,例如,参与D2D发现通信的设备可能会遭受流氓基站的重放攻击。因此,可以增强参与D2D发现通信的设备的安全性。

[0009] 概述

[0010] 所描述的特征一般涉及用于管理无线通信的一种或多种改进的方法、系统或装置。这些改进的方法包括在设备处于连通模式时在该设备处接收定时变量。该定时变量可随后在设备到设备(D2D)发现通信期间被用于验证D2D 发现消息的真实性。

[0011] 根据第一组解说性示例,一种无线通信方法可包括在设备处接收来自网络的定时变量,其中该定时变量是在该设备处于连通模式时接收的。该方法还包括将定时变量用于D2D发现消息认证。定时变量还可被存储在设备处以与本地定时变量进行比较。在一些示例中,定时变量是从网络中基于邻近度的服务 (ProSe)功能接收的。定时变量可连同D2D发现应用码一起被接收并且可以是协调世界时(UTC)。另外,可从网络中的ProSe功能接收定时偏移允许,其中该方法可随后包括将所接收到的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否小于定时偏移允许。本地定时变量可经由系统信息块(SIB)来接收。如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内,则该方法可包括宣告D2D发现应用码。如果该差异大于定时偏移允许,则

该方法可包括向ProSe功能通知异常。在一些示例中，该方法可包括转变到与基站的连通模式。否则，该方法可包括经由无线电资源控制(RRC)消息来向基站作出对定时变量的请求。

[0012] 该方法还可包括在差异小于定时偏移允许时将接收自ProSe功能的定时变量与本地定时变量同步。当差异大于定时偏移允许时，可向ProSe功能通知异常。

[0013] 接收自网络的定时变量可被用于生成要被包括在D2D发现宣告中的消息完整性码(MIC)。MIC可在传送D2D发现宣告时基于D2D发现应用码、与 D2D发现应用码相关联的密钥、以及定时变量的本地版本来生成。替换地，该方法可包括接收包括MIC的D2D发现宣告，以及向网络中的ProSe功能传送所接收到的MIC和定时变量。

[0014] 在某些示例中，该方法可进一步包括在设备处于连通模式时接收参与D2D 发现的授权，以及在设备处于连通模式时检测SIB。定时变量可经由系统信息块(SIB)来接收。SIB可专用于D2D发现信息。该方法还可包括如果设备检测到不止一个具有定时信息的SIB，则忽略在该SIB中接收到的定时变量；以及在SIB以外获得定时变量。另外，该方法可包括将SIB中接收到的定时变量与本地定时变量进行比较。如果所接收到的定时变量与本地定时变量相差超过预定阈值，则该方法可包括在SIB以外获得定时变量。

[0015] 在某些示例中，该方法可包括在设备处于连通模式时经由无线电资源控制 (RRC)消息来接收用于定时变量同步的SIB。该方法还可包括当设备正在使用受网络控制的D2D发现资源分配方案时经由RRC消息来请求D2D发现资源，其中定时变量是经由对RRC消息的响应来接收的。替换地，该方法可包括当设备正在使用受设备控制的D2D发现资源分配方案时经由RRC消息来请求D2D发现资源，以及接收对RRC消息的响应，该响应包括定时变量和空资源分配元素。

[0016] 其他示例包括向另一设备转发所接收到的定时变量。定时变量可以是 UTC。替换地，定时变量可以是随D2D发现周期递增的计数器。

[0017] 根据第二组解说性示例，一种用于无线通信的装备可包括用于在设备处接收来自网络的定时变量的装置，该定时变量是在该设备处于连通模式时接收的，以及用于将该定时变量用于D2D发现消息认证的装置。定时变量可从网络中的ProSe功能接收。定时变量可连同D2D发现应用码一起被接收并且可以是UTC。该装备可进一步包括用于从网络中的ProSe功能接收定时偏移允许的装置，以及用于将接收自网络的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否小于定时偏移允许的装置。该装备还可包括用于如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内则宣告D2D发现应用码的装置。还可包括用于使用定时变量来生成要被包括在D2D发现宣告中的MIC的装置。替换地，该装备可包括用于接收包括MIC的D2D发现宣告的装置，以及用于向网络中的ProSe功能传送所接收到的MIC和定时变量的装置。该装备可进一步包括用于在设备处于连通模式时接收参与D2D发现的授权的装置。还可包括用于经由SIB来接收本地定时变量的装置。

[0018] 在某些示例中，该装备可进一步包括用于在设备处于连通模式时经由 RRC消息来接收用于定时变量同步的SIB的装置。在其他示例中，该装备包括用于当设备正在使用受网络控制的D2D发现资源分配方案时经由RRC消息来请求D2D发现资源的装置，其中定时变量是经由对RRC消息的响应来接收的。该装备可包括用于当设备正在使用受设备控制的D2D发现资源分配方案时经由RRC消息来请求D2D发现资源的装置。

[0019] 根据另一组解说性示例，一种配置成用于无线通信的装置可包括至少一个处理器以及耦合至该至少一个处理器的存储器。该至少一个处理器可被配置成在设备处接收来自网络的定时变量，该定时变量是在该设备处于连通模式时接收的，以及将该定时变量用于D2D发现消息认证。定时变量可从网络中的ProSe 功能接收。定时变量可连同D2D发现应用码一起被接收并且可以是UTC。该处理器可被进一步配置成从网络中的ProSe功能接收定时偏移允许，以及将接收自网络的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否小于定时偏移允许。另外，该处理器可被配置成如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内则宣告D2D发现应用码。

[0020] 根据又一组解说性示例，一种计算机程序产品可包括至少一个处理器以及其上记录有非瞬态程序代码的非瞬态计算机可读介质。该非瞬态程序代码可包括用于在设备处接收来自网络的定时变量的程序代码，该定时变量是在该设备处于连通模式时接收的，以及用于将该定时变量用于D2D发现消息认证的程序代码。定时变量可从网络中的ProSe功能接收。定时变量可连同D2D发现应用码一起被接收并且可以是UTC。该程序代码可进一步包括用于从网络中的 ProSe功能接收定时偏移允许，以及将接收自网络的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否小于定时偏移允许的程序代码。另外，该程序代码可包括用于如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内则宣告D2D发现应用码的程序代码。

[0021] 根据又一组解说性示例，一种无线网络中的无线通信方法可包括进入与设备的连通模式，以及在该设备处于连通模式时向该设备传送定时变量以供在 D2D发现消息认证中使用。定时变量可从ProSe功能传送。定时变量可连同 D2D发现应用码一起被传送并且可以是UTC。该方法可包括向设备传送定时偏移允许，其中该定时偏移允许是定时变量与该设备处的本地定时变量之间的最大差异。在一些示例中，该方法还可包括从设备接收包括基于邻近度的服务 (ProSe)应用ID的发现请求，以及向设备发送包括定时变量、D2D发现应用码、与D2D发现应用码相关联的密钥、和定时偏移允许的发现响应。替换地，该方法可包括传送包括SIB的RRC消息，该SIB包括定时变量。在其他示例中，该方法可包括接收对发现资源的RRC请求，其中传送定时变量包括传送对RRC请求的响应，该响应包括定时变量。

[0022] 根据又一组解说性示例，一种用于无线网络中的无线通信的装备可包括用于进入与设备的连通模式的装置，以及用于在该设备处于连通模式时向该设备传送定时变量以供在D2D发现消息认证中使用的装置。定时变量可从ProSe 功能传送。定时变量可连同D2D发现应用码一起被传送并且可以是UTC。该装备还可包括用于向设备传送定时偏移允许的装置，其中该定时偏移允许是定时变量与该设备处的本地定时变量之间的最大差异。该装备还可包括用于从设备接收包括基于ProSe应用ID的发现请求的装置，以及用于向设备发送包括定时变量、D2D发现应用码、与D2D发现应用码相关联的密钥、和定时偏移允许的发现响应的装置。另外，该装备可包括用于传送包括SIB的RRC消息的装置，该SIB包括定时变量。在其他示例中，该装备可包括用于接收对发现资源的RRC请求的装置，其中传送定时变量包括传送对RRC请求的响应，该响应包括定时变量。

[0023] 在另一组解说性示例中，一种配置成用于无线通信的装置可包括至少一个处理器以及耦合至该至少一个处理器的存储器。该至少一个处理器可被配置成进入与设备的连通

模式，以及在设备处于连通模式时向该设备传送定时变量以供在D2D发现消息认证中使用。定时变量可从ProSe功能传送。定时变量可连同D2D发现应用码一起被传送并且可以是基于UTC的计数器。该处理器可被进一步配置成向设备传送定时偏移允许，其中该定时偏移允许是定时变量与该设备处的本地定时变量之间的最大差异。该处理器还可被配置成从设备接收包括基于ProSe应用ID的发现请求，以及向设备发送包括定时变量、D2D发现应用码、与D2D发现应用码相关联的密钥、和定时偏移允许的发现响应。替换地，该处理器可被配置成传送包括SIB的RRC消息，该SIB包括定时变量。在其他示例中，该处理器可被进一步配置成接收对发现资源的RRC请求，其中传送定时变量包括传送对RRC请求的响应，该响应包括定时变量。

[0024] 根据又一组解说性示例，一种计算机程序产品可包括其上记录有非瞬态程序代码的非瞬态计算机可读介质。该非瞬态程序代码可包括用于进入与设备的连通模式的程序代码，以及用于在设备处于连通模式时向该设备传送定时变量以供在D2D发现消息认证中使用的程序代码。定时变量可从ProSe功能传送。定时变量可连同D2D发现应用码一起被传送并且可以是UTC。该程序代码可进一步包括用于向设备传送定时偏移允许的程序代码，其中该定时偏移允许是定时变量与该设备处的本地定时变量之间的最大差异。该程序代码还可包括用于从设备接收包括基于ProSe应用ID的发现请求，以及向设备发送包括定时变量、D2D发现应用码、与D2D发现应用码相关联的密钥、和定时偏移允许的发现响应的程序代码。该程序代码还可包括用于传送包括SIB的RRC消息的程序代码，该SIB包括定时变量。在其他示例中，该程序代码可包括用于接收对发现资源的RRC请求的程序代码，其中传送定时变量包括传送对RRC请求的响应，该响应包括定时变量。

[0025] 所描述的方法和装备的适用性的进一步范围将因以下具体描述、权利要求和附图而变得明了。详细描述和具体示例仅是藉由解说来给出的，因为落在该描述的精神和范围内的各种变化和改动对于本领域技术人员而言将变得显而易见。

[0026] 附图简述

[0027] 通过参照以下附图可实现对本发明的本质和优势的更进一步的理解。在附图中，类似组件或特征可具有相同的附图标记。此外，相同类型的各个组件可通过在附图标记后跟随短划线以及在类似组件之间进行区分的第二标记来加以区分。如果在说明书中仅使用第一附图标记，则该描述可应用于具有相同的第一附图标记的类似组件中的任何一个组件而不论第二附图标记如何。

[0028] 图1示出了根据本公开的各个方面的无线通信系统的示例的框图；

[0029] 图2是根据本公开的各个方面的用于设备到设备(D2D)发现以及无线通信的系统的示例的框图；

[0030] 图3示出了解说根据本公开的各个方面的参与D2D发现的用户装备(UE) 与网络中的基于邻近度的服务(ProSe)功能之间的通信的消息流图；

[0031] 图4示出了根据本公开的各种方面的供在无线通信中使用的装置的框图；

[0032] 图5示出了解说根据本公开的各个方面的参与D2D发现的UE与基站之间的通信的消息流图；

[0033] 图6示出了解说根据本公开的各个方面的参与D2D发现的UE与基站之间的通信的消息流图；

[0034] 图7示出了解说根据本公开的各个方面的参与D2D发现的UE与基站之间的通信的消息流图；

[0035] 图8示出了解说根据本公开的各个方面的参与D2D发现的UE、ProSe功能与基站之间的通信的消息流图；

[0036] 图9示出了根据本公开的各种方面的供在无线通信中使用的UE的框图；

[0037] 图10示出了根据本公开的各种方面的供在无线通信中使用的装置的框图；

[0038] 图11示出了根据本公开的各个方面的被配置用于接收和传送D2D发现通信的通信系统的框图；

[0039] 图12示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0040] 图13示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0041] 图14示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0042] 图15示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0043] 图16示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0044] 图17示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0045] 图18示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0046] 图19示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0047] 图20示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；

[0048] 图21示出了解说根据本公开的各个方面的无线通信方法的示例的流程图；以及

[0049] 图22示出了解说根据本公开的各个方面的无线通信方法的示例的流程图。

[0050] 详细描述

[0051] 通常，设备(即，用户装备(UE))通过与无线通信系统的基站通信来参与无线通信。然而，这些设备还可参与直接设备到设备(D2D)或基于邻近度的服务(ProSe)无线通信。D2D发现允许处于彼此的射程内的各UE彼此直接通信，而非通过基站进行通信。何时可期望D2D无线通信的示例是在UE 意欲与紧邻的其他UE具有通信会话、或者仅对相同位置中的其他UE可见的时候。UE可广播D2D发现宣告(诸如长期演进(LTE)系统中的直接对等方发现信号)，其随后可被邻域中正在监视此类发现通信的UE接收。宣告方 UE可在空中(OTA)发现宣告消息中包括诸如D2D发现应用码之类的代码。D2D发现应用码可指示宣告方UE的期望意图或功能。监视方UE可接收具有其D2D发现应用码的D2D发现宣告，并且可随后确定监视方UE是否可用于参与同宣告方UE的D2D通信。

[0052] 然而，在没有附加信息或动作的情况下，监视方UE可能不能够验证D2D 发现宣告的真实性。为了减轻此潜在的安全性风险，宣告方UE可在其D2D发现宣告中包括消息完整性码(MIC)，监视方UE可协同无线网络中的D2D发现模块来使用该MIC以确定D2D发现通信的真实性。在MIC的生成期间使用的元素是定时变量。由于宣告方UE对MIC的生成和监视方设备对MIC的分析要求这两个UE能够访问准确的定时变量，因而存在确保UE能够安全地获得或确定定时变量的需要。

[0053] 以下描述提供示例而并非限定权利要求中阐述的范围、适用性或者配置。可以对所讨论的要素的功能和布置作出改变而不会脱离本公开的精神和范围。各种示例可恰适地省略、替代、或添加各种规程或组件。例如，可以按不同于所描述的次序来执行所描述的方法，并且可以添加、省去、或组合各种步骤。另外，关于某些示例所描述的特征可在其他示例

中被组合。

[0054] 图1示出了根据本公开的各个方面的无线通信系统100的示例的框图。无线通信系统100包括基站(或蜂窝小区)105、通信设备115和核心网130。基站105可在基站控制器(未示出)的控制下与通信设备115通信,在各种示例中,该基站控制器可以是核心网130或基站105的部分。基站105可以通过回程链路132与核心网130传达控制信息或用户数据。在各示例中,基站105可以直接或间接地在回程链路134上彼此通信,回程链路134可以是有线或无线通信链路。无线通信系统100可支持多个载波(不同频率的波形信号)上的操作。多载波发射机能同时在这多个载波上传送经调制信号。例如,每个通信链路125可以是根据以上描述的各种无线电技术调制的多载波信号。每个经调制信号可在不同的载波上发送并且可携带控制信息(例如,参考信号、控制信道等)、开销信息、数据等。

[0055] 基站105可经由一个或多个基站天线与UE 115进行无线通信。基站105 站点中的每一个站点可为相应的覆盖区域110提供通信覆盖。在一些示例中,基站105可被称为基收发机站、无线电基站、接入点、无线电收发机、基本服务集(BSS)、扩展服务集(ESS)、B节点、演进型B节点(eNB)、家用B 节点、家用演进型B节点或其他某个合适的术语。基站的覆盖区域110可被划分成仅构成该覆盖区域的一部分的扇区(未示出)。无线通信系统100可包括不同类型的基站105(例如宏基站、微基站、或微微基站)。可能存在不同技术的交叠覆盖区域。

[0056] 在各示例中,无线通信系统100是LTE/LTE-A网络。在LTE/LTE-A网络中,术语演进型B节点(eNB)和UE可一般用来分别描述基站105和UE 115。无线通信系统100可以是异构LTE/LTE-A网络,其中不同类型的基站提供对各种地理区划的覆盖。例如,每个基站105可提供对宏蜂窝小区、微微蜂窝小区、毫微微蜂窝小区、或其他类型的蜂窝小区的通信覆盖。宏蜂窝小区一般覆盖相对较大的地理区域(例如,半径为数千米的区域),并且可允许无约束地由与网络供应商具有服务订阅的UE接入。微微蜂窝小区一般将覆盖相对较小的地理区域并且可允许无约束地由具有与网络供应商的服务订阅的UE接入。毫微微蜂窝小区也一般将覆盖相对较小的地理区域(例如,住宅)且除了无约束的接入之外还可提供有约束地由与该毫微微蜂窝小区有关联的UE(例如,封闭订户群(CSG)中的UE、该住宅中的用户的UE、等等)接入。宏蜂窝小区的基站可被称为例如宏eNB。微微蜂窝小区的基站可被称为例如微微eNB。并且,用于毫微微蜂窝小区的基站可被称为毫微微eNB或家用eNB。基站可支持一个或多个(例如,两个、三个、四个、等等)蜂窝小区。

[0057] 核心网130可以经由回程链路132(例如,S1等)与基站105通信。基站 105还可例如直接或者经由回程链路134(例如,X2等)或经由回程链路132 (例如,通过核心网130)间接地彼此通信。无线通信系统100可支持同步或异步操作。对于同步操作,基站可具有相似的帧定时,并且来自不同基站的传输可以在时间上大致对齐。对于异步操作,基站可以具有不同的帧定时,并且来自不同基站的传输可能在时间上并不对齐。本文中描述的技术可被用于同步或异步操作。

[0058] 基站105还可向UE 115传达信息和命令。例如,当UE 115进入与基站 105的连通模式时,基站105和UE 115彼此相互认证。一旦被认证,基站105 就可安全地向UE 115传达信息。可从基站105向UE 115传达的信息包括与当前时间或某个其他定时变量有关的信息,以使得UE 115可与基站105(以及无线通信系统100中的其他设备)完全同步。当前时间或其他定时变量可由 UE 115在D2D发现消息的认证期间使用,如以下示例中进一步解释的。

[0059] UE 115分散遍及无线通信系统100，并且每个UE可以是驻定的或移动的。UE 115也可被本领域技术人员称为UE、移动设备、移动站、订户站、移动单元、订户单元、无线单元、远程单元、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、中继、或其他某个合适的术语。UE 115可以是蜂窝电话、个人数字助理(PDA)、无线调制解调器、无线通信设备、手持式设备、平板计算机、膝上型计算机、无绳电话、无线本地环路(WLL)站、等等。UE可以能够与宏eNB、微微eNB、毫微微eNB、中继等通信。UE 115-a还可经由D2D无线通信来与另一UE 115直接通信。在一个示例中，基站105的覆盖区域110-a内的UE 115-a-1可充当在基站105的覆盖区域110-a外部的UE 115-a-2的中继。覆盖内UE 115-a-1可以中继(或重传)从基站105到覆盖外UE 115-a-2的通信。类似地，覆盖内UE 115-a-1可以中继从覆盖外UE 115-a-2 到基站105的通信。另外，D2D无线通信可在各自为覆盖内的UE 115之间发生并且可出于许多不同原因而发生。由此，覆盖内UE 115-a-1可参与同覆盖内 UE 115-a-3的D2D无线通信。UE 115-a-3也可参与同UE 115-a-2的D2D无线通信。

[0060] 为了使UE 115参与D2D无线通信，UE 115可首先参与D2D发现。D2D 发现允许UE 115发现能够参与D2D通信的其他UE。D2D发现包括广播D2D 发现宣告的宣告方UE和监视D2D发现宣告的监视方UE。监视方UE可接收 D2D发现宣告并且可随后响应和参与同宣告方UE的D2D无线通信。然而，从此D2D通信中排除基站或其他网络模块可能使通信暴露于安全性风险。以下解释这些风险的示例以及如何减轻这些风险。

[0061] 无线通信系统100中示出的通信链路125可包括从UE 115到基站105的上行链路(UL)传输、或者从基站105到UE 115的下行链路(DL)传输。下行链路传输也可被称为前向链路传输，而上行链路传输也可被称为反向链路传输。通信链路125还可包括在UE 115之间交换的D2D消息(包括D2D发现消息)。

[0062] 图2示出了根据本公开的各个方面的用于D2D发现和无线通信的系统200 的示例的框图。图2的系统200可以是参照图1描述的无线通信系统100的示例。在一种配置中，基站105-a-1可以与落在基站105-a-1的覆盖区域110-b-1 内的一个或多个设备通信。覆盖内UE 115-b-1可以接收来自基站105-a-1的通信/向基站105-a-1传送通信。一个或多个UE 115-b-2、115-b-3、115-b-4可以在基站105-a-1的覆盖区域110-b-1外部并可参与D2D通信。其他UE 115-b-5 可以在基站105-a-1的覆盖区域110-b-1内，但也可参与D2D通信。UE 115-b-2、115-b-3也可以在不同基站105-a-2的覆盖区域110-b-2内，且可以与基站 105-a-2处于通信。基站105-a和UE 115-b可以是参考图1描述的基站105和UE 115的示例。

[0063] 在一个实施例中，覆盖内UE 115-b-1可以经由通信链路125广播、多播、或单播D2D发现信号。该信号可以被发送给处于覆盖内或覆盖外的一个或多个UE。D2D发现信号可以是D2D发现宣告消息。D2D发现宣告消息可指示例如覆盖内UE 115-b-1的标识符。例如，该标识符可以是覆盖内UE 115-b-1 的媒体接入控制(MAC)地址。另外，D2D发现信号可包括UE 115-b-1的D2D 发现应用码。

[0064] 在一种配置中，覆盖外UE可以将D2D发现信号传送给一个或多个覆盖内UE 115-b-1。对等方发现信号可以指示覆盖外UE在覆盖外或正在请求中继服务。该信号可包括覆盖外UE的标识符。在一种配置中，UE在其感测到它将要在基站105-a-1的覆盖区域110-b-1之外时可以广播D2D发现信号。在另一实施例中，UE可以在它已经在覆盖区域110-b-1之外时广

播信号。

[0065] 作为附加示例,两个覆盖内UE 115-b-1、115-b-5也可经由直接D2D连接彼此通信。在此示例中,UE 115-b-5可传送请求与邻近UE 115-b-5的其他UE 的直接D2D连接的信号。UE 115-b-1可以接收该请求并随后发起与UE 115-b-5 的直接D2D通信。在一附加示例中,UE 115-b-2、115-b-3可各自经由直接D2D 连接与UE 115-b-1通信。例如,UE 115-b-1可以充当UE 115-b-2、115-b-3的中继。

[0066] 在UE 115可参与D2D无线通信之前,可以首先授权UE 115。授权由核心网130-a授予。具体地,核心网130-a可包括被启用以授权D2D通信的网络 D2D发现模块210。网络D2D发现模块210的示例为ProSe功能。UE 115可通过经由无线接口215(诸如PC3接口)与网络D2D发现模块210通信来请求对D2D通信的授权。网络D2D发现模块210可通过授权请求方UE 115来响应。

[0067] 在D2D通信的授权期间,网络D2D发现模块210生成D2D发现应用码 (诸如ProSe应用码)。例如,D2D发现应用码对应于要由宣告方UE 115-b-1 参与的D2D功能。由此,一旦被授权,宣告方UE 115-b-1就可广播作为D2D 发现宣告的一部分的D2D发现应用码。

[0068] 网络D2D发现模块210还可被用于生成由参与D2D发现的UE 115使用的安全性元素以保护D2D发现消息。可提供抵抗流氓基站(诸如系统200中的基站105-a-3)的保护。基站105-a-3可被用于劫持源自UE 115的D2D通信。因此,安全性方案可由UE 115和网络D2D发现模块210使用以保护免受流氓基站105-a-3的风险。

[0069] 图3示出了解说根据本公开的各个方面的由参与D2D发现的UE 115-c-1、115-c-2以及网络D2D发现模块210-a使用的安全性方案的消息流图300。UE 和网络D2D发现模块可以是图1和/或2中描述的UE 115以及图2中描述的网络D2D发现模块210的示例。

[0070] 宣告方UE 115-c-1可向网络中的网络D2D发现模块210-a发送发现请求 305以被允许向其他设备(诸如监视方UE 115-c-2)宣告D2D发现应用码。作为响应,网络中的D2D发现模块210-a可向宣告方UE 115-c-1返回D2D发现应用码。除了为宣告方UE 115-c-1生成D2D发现应用码之外,网络D2D发现模块210-a还可生成与D2D发现应用码相关联的密钥。网络D2D发现模块 210-a可向宣告方UE 115-c-1传送发现响应消息310,该发现响应消息310包括D2D发现应用码和相关联的密钥。另外,网络D2D发现模块210-a可向宣告方UE 115-c-1提供当前时间(CURRENT_TIME)参数,该CURRENT_TIME 参数可包括D2D发现模块210-a处的当前定时信息(例如,定时变量)和定时偏移允许。网络中的D2D发现模块210-a可以是服务UE的归属公共陆地移动网络(HPLMN)或受访PLMN(VPMLN)中的ProSe功能。定时偏移允许可在本文中被称为指示定时变量与UE处的本地定时变量之间的最大差异的最大偏移(MAX_OFFSET)。宣告方UE 115-c-1可使用所接收到的D2D发现应用码和相关联的密钥以及定时变量来生成消息完整性码(MIC)(在步骤 315)。定时变量可以是定时信息的元素,诸如协调世界时(UTC)或某个其他系统时间。替换地,定时变量可以是例如每个D2D发现周期递增但不是非常频繁地绕回的计数器值。在任一情形中,定时变量可从其他源获得。例如,定时变量可经由网络身份和时区(NITZ)、网络时间协议(NTP)、广播系统信息块16(SIB16)、或全球定位系统(GPS)等获得。宣告方UE 115-c-1可随后将接收自D2D发现模块210-a的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否在定时偏移允许(例如, MAX_OFFSET)内。如果确定接收自网络的定时变量与本地定时变量之间

的差异在定时偏移允许内，则宣告方UE 115-c-1可开始宣告D2D应用码(诸如 ProSe应用码)。如果该差异大于定时偏移允许，则宣告方UE 115-c-1可认识到已发生异常并且尝试可由ProSe功能预先配置或配置的某个其他方法来接收经更新的定时变量。例如，宣告方UE 115-c-1可向ProSe功能通知异常。或者，宣告方UE 115-c-1可转变到连通模式并且经由RRC消息向基站(例如，eNB) 作出对经更新的定时变量的请求。

[0071] 宣告方UE 115-c-1可使用相关联的发现密钥和定时变量来生成要被包括在D2D发现应用码中的MIC(步骤315)。宣告方UE 115-c-1可随后在其D2D 发现宣告消息320中包括MIC连同D2D发现应用码。监视方UE 115-c-2可由不同于服务宣告方UE 115-c-1的网络的网络服务。由此，监视方UE 115-c-2 的网络D2D发现模块可以不同于宣告方UE 115-c-1的网络D2D发现模块 210-a。在此类情形中，监视方UE的D2D发现模块和宣告方UE的D2D发现模块可交换监视请求和响应消息。

[0072] 在接收到D2D发现宣告消息320之前，监视方UE 115-c-2可与其自己的网络的D2D发现模块210-b交换发现请求305-a和响应消息310-a。例如，监视方UE 115-c-2可向网络中的D2D发现模块(例如，ProSe功能)发送包含 D2D应用码的发现请求消息以获得它想要监听的发现过滤器。网络中的 D2D发现模块可随后返回包含D2D应用码或ProSe掩码或这二者连同 CURRENT_TIME和MAX_OFFSET参数的发现过滤器。随后，监视方UE 115-c-2可将其ProSe时钟设置成CURRENT_TIME并且存储盖写任何先前值的MAX_OFFSET。如同宣告方UE 115-c-1，监视方UE 115-c-2可能已经从可供监视方UE 115-c-2使用的各种源(例如，SIB16、NITZ、NTP或GPS)接收到定时变量。所接收到的定时变量可由监视方UE 115-c-2存储并且根据由定时变量表示的定时信息的类型来递增。通过所接收到的发现过滤器，监视方 UE 11 5 -c-2可监听在定时变量在其ProSe时钟的MAX_OFFSET内的情况下匹配该发现过滤器的发现宣告消息。

[0073] 当监视方UE 115-c-2接收到D2D发现宣告消息320时，监视方UE 115-c-2 在消息325中向网络D2D发现模块210-a传送所接收到的D2D发现应用码以进行验证。消息320还包括如由监视方UE 115-c-2知晓的定时变量。在一些示例中，该消息可以是包含基于UTC的定时变量的匹配报告325，该定时变量具有与连同发现宣告消息一起接收的四个最低有效位(LSB)相等的四个LSB并且与监视方UE的关联于在其中听到发现宣告的发现时隙的定时变量最接近。在监视方UE 115-c-2的网络D2D发现模块不同于宣告方UE 115-c-1的网络 D2D发现模块210-a的情形中，服务监视方UE 115-c-2的网络的D2D发现模块210-b将匹配报告325传递给服务宣告方UE 115-c-1的网络的D2D发现模块210-a。

[0074] 网络D2D发现模块210-a通过使用接收自监视方UE 115-c-2的定时变量来验证MIC(在步骤330)。例如，如果接收自监视方UE 115-c-2的定时变量在定时偏移允许内，则MIC可被验证。如果由宣告方UE 115-c-1用于生成MIC 的定时变量类似于由监视方UE 115-c-2传送给网络D2D发现模块210-a的定时变量，则MIC可被验证。如果MIC被验证，则网络D2D发现模块210-a经由潜在地具有关于D2D通信的附加信息的消息335来通知监视方UE 115-c-2。在监视方UE 115-c-2的网络D2D发现模块210-b不同于宣告方UE 115-c-1的网络D2D发现模块210-a的情形中，宣告方UE 115-c-1的D2D发现模块210-a 可在匹配报告ACK消息336中向服务监视方UE 115-c-2的网络的D2D发现模块210-b发送对MIC的成功验证的确收。监视方UE 115-c-2的D2D发现模块 210-b可随后向监视方UE 115-c-2发送匹配响应337。随后，监

视方UE 115-c-2 可参与同宣告方UE 115-c-1的D2D无线通信340。

[0075] 在上述安全性方案中，宣告方和监视方UE两者均可使用不受保护的时间来获得与发现时隙相关联的定时变量。这意味着如果UE被欺骗使用不同于当前时间的时间，则发现宣告消息可被攻击者(诸如(图2的)流氓基站105-a-3) 成功地重放。

[0076] 例如，流氓基站105-a-3可被用于在SIB中广播在实际UTC之前的不同系统时间。如果宣告方UE同步至所广播时间，则宣告方UE将广播基于时间值尚未出现的定时变量的MIC。流氓基站105-a-3可从宣告方UE接收D2D发现宣告消息并且存储相关联的D2D发现应用码和MIC。随后，在对应于由流氓基站105-a-c错误地广播的时间的稍后时间，攻击者可作为广播“重放”存储着的D2D发现应用码和MIC，由此潜在地欺骗其他监视方UE参与同非法实体的D2D通信。

[0077] 在另一示例中，攻击者可记录来自宣告方UE的广播D2D发现宣告(记录D2D发现应用码和MIC两者)以及广播D2D发现宣告的系统时间。在某个稍后时间，攻击者可部署流氓基站105-a-3，该流氓基站105-a-3广播包括错误的定时变量的SIB。取代包括正确的时间，错误地广播的SIB包括对应于宣告方UE广播其D2D发现宣告的系统时间。如果监视方UE使其定时变量同步至错误地广播的SIB，则攻击者能够重放所记录的D2D发现消息并且由此欺骗监视方UE参与同攻击者的D2D通信。

[0078] 因此，本文公开了用于排除涉及定时变量的此类重放攻击的方法和装置。在所公开的示例中，宣告方和监视方UE两者都可以能够以安全的方式获得所接收到的定时变量并且与所接收到的定时变量同步。

[0079] 定时偏移允许(例如，MAX_OFFSET)可被用于限制攻击者成功地重放发现消息或者获得经正确地完整性检查的发现消息以供稍后使用的能力。例如，MAX_OFFSET被用作与发现时隙相关联的基于UTC的时间和存储在监视方设备处的本地定时变量(例如，由监视方设备保持的ProSe时钟)之间的最大差异。在一些示例中，UE可在其处于连通模式时接收定时变量以安全地获得定时变量。例如，当UE处于无线电资源控制(RRC)连通模式时，UE和经连通实体(例如，基站)被相互认证。由此，可以保护此时在经连通实体之间交换的信息。由UE在处于连通模式时接收到的定时变量可以因此被认为是安全的或者可以至少被验证为是有效的。

[0080] 因为进入连通模式在UE处的电池寿命、频谱和处理方面是昂贵的，所以定时变量的接收应当在UE已处于连通模式时发生。换言之，UE应当避免简单地为了获得定时变量和同步至定时变量的目的而进入连通模式。取而代之的是，UE可在其已进入连通模式以例如获得D2D发现授权时获得定时变量。由此，在被授权进行D2D发现通信时，UE也可获得定时变量。

[0081] 图4示出了根据本公开的各个方面的供在无线通信中使用的装置405的框图400。在一些示例中，装置405可以是参照图1、2、和/3描述的一个或多个 UE 115的各方面的示例，并且可以参与D2D无线通信。装置405也可以是处理器。装置405可包括接收机模块410、D2D发现模块415、和/或发射机模块 420。这些组件中的每一者可与彼此处于通信。

[0082] 装置405的组件可个体地或整体地用一个或多个适配成以硬件执行一些或所有适用功能的专用集成电路(ASIC)来实现。替换地，这些功能可以由一个或多个集成电路上的一个或多个其他处理单元(或核)来执行。在其他示例中，可使用可按本领域所知的任何方

式来编程的其他类型的集成电路(例如,结构化/平台ASIC、现场可编程门阵列(FPGA)、以及其他半定制IC)。每个单元的功能也可以整体或部分地用实施在存储器中的、被格式化成由一或多个通用或专用处理器执行的指令来实现。

[0083] 在一些示例中,接收机模块410可包括至少一个射频(RF)接收机,诸如可操作用于在射频频谱上接收传输的至少一个RF接收机。在一些示例中,该射频频谱可被用于LTE/LTE-A通信,如例如参照图1、2和/或3描述的。接收机模块410可被用来在无线通信系统的一条或多条通信链路(诸如参照图1 和/或2描述的无线通信系统100的一条或多条通信链路125)上接收各种类型的数据和/或控制信号(即,传输)。另外,接收机模块410还可被用来在无线通信系统的一条或多条通信链路(诸如无线通信系统100的一条或多条通信链路125)上接收D2D通信。由接收机模块410接收的D2D通信的一些类型的具体示例包括消息305、315和330以及D2D无线通信335,如参照图3所描述的。

[0084] 在一些示例中,发射机模块420可包括至少一个RF发射机,诸如可操作用于传送D2D消息的至少一个RF发射机。发射机模块420可被用来在无线通信系统的一条或多条通信链路(诸如参照图1和/或2描述的无线通信系统100 的一条或多条通信链路125)上传送各种类型的数据和/或控制信号(即,传输)。另外,发射机模块420还可被用来在一条或多条通信链路125上传送D2D通信。由发射机模块420接收的数据或控制信号的类型的示例包括消息315和320 以及D2D无线通信335,如参照图3所描述的。

[0085] 在一些示例中,D2D发现模块415可被用来管理经由接收机模块410和/ 或发射机模块420对D2D发现消息和D2D通信的接收和传送。管理D2D发现消息的传送和接收可包括从网络D2D发现模块接收D2D发现应用码和密钥,传送D2D发现应用码、MIC和本地定时变量,以及接收MIC验证,如图 3的消息305、310、315、320、325和335以及步骤310中展示的。D2D发现模块415的MIC模块425可在宣告方UE中被用于从接收自网络的D2D发现应用码、密钥和定时变量生成MIC。MIC模块425还可被用于在监视方UE中辅助验证MIC。此外,为了提高MIC的安全性,D2D发现模块415可包括定时变量模块430,该定时变量模块430可被用于接收和存储用于生成和/或验证 MIC的定时变量。定时变量模块430可使用若干不同的替换方法来达成此举。

[0086] 图5示出了根据本公开的各个方面的解说参与D2D发现的UE 115-d与基站105-b之间的通信的消息流图500。该UE和基站可以是图1、2、3、和/或4 中描述的UE 115以及图1和/或2中描述的基站105的示例。

[0087] 一旦UE 115-d处于与基站105-b的连通模式505,UE 115-d和基站105-b 就相互认证,并且由此在此连通模式505期间在这两个实体之间交换的通信可以是安全的。基站105-b能够确定(在框510)UE 115-d是否已被授权参与D2D 发现通信(例如,经由从网络D2D发现模块接收授权)。UE 115-d可向基站 105-b发送发现请求消息510以被允许宣告D2D发现应用码。作为响应,基站 105-b可返回D2D发现应用码和与该D2D发现应用码相关联的发现密钥,以使得UE 115-d能够进行宣告。一旦基站105-b识别出UE 115-d是D2D UE,基站105-b就可向UE 115-d发送包括应用码和相关联的发现密钥的发现响应 515。发现响应还可包括CURRENT_TIME参数(其可包括D2D发现模块210-a 处的基于UTC的时间)、MAX_OFFSET、和/或有效性定时器,如参照图3 所描述的。

[0088] 当UE 115-d接收到发现响应515时,UE 115-d可将其用于认证的时钟(例如,ProSe

时钟)设置成CURRENT_TIME的值并且存储MAX_OFFSET,从而盖写先前值。在一些示例中,UE 115-d可接收基于UTC的计数器的关联于发现时隙的值。该计数器可被设置成以秒为粒度的UTC时间值。在一些情形中,UE 115-d例如经由SIB广播消息520来寻求检测和获得定时变量。例如, UE 115-d可经由通常由UE在连通模式中获取的系统信息块类型1来获得SIB 广播调度。SIB一般是在下行链路信道DL_SCH中传送的。当UE 115-d接收到SIB和包括在SIB内的定时变量时,UE 115-d可验证没有发生异常(步骤 525)并且随后存储所接收到的定时变量以将该定时变量与它自己的本地定时变量进行比较(步骤530)。

[0089] 在流氓基站活跃的某些情况下,对没有发生异常的验证可以是必要的。例如,流氓基站还可从合法基站105-b接收SIB调度信息并且随后尝试将与定时相关的SIB注入到由合法基站105-b调度的同一个广播时隙中。因此,在此情况下,UE 115-d可能观察到相同类型的多个SIB被同时广播。许多UE不能够处置在相同广播时隙内接收到相同类型的两个SIB,并且可能默认仅读取所接收到的SIB之一。其他UE能够接收相同类型的多个SIB,但是可能随后比较包括在所接收到的SIB中的定时变量(例如,基于UTC的时间)以确定是否存在冲突。如果UE 115-d接收到相同类型的多个SIB或者确定在所接收到的 SIB的所接收到的定时变量之间存在差异,则UE 115-d可以选择不存储和同步所接收到的定时变量,而是继续使用它自己的本地副本。另外,UE 115-d可以选择将一不同方法(如下所述)用于经更新的定时变量。

[0090] 当流氓基站在与合法基站105-b广播相同类型的SIB相同的时间广播SIB 时,可能在UE 115-d处发生各种异常。如以上描述的,UE 115-d可接收所广播的两个SIB。替换地,所广播的SIB可能彼此冲突,在此情形中UE 115-d 不能够接收所广播的SIB中的任一者。在又一情形中,合法SIB可用充分的功率来广播,以使得UE 115-d仅检测伪造的SIB。由此,使UE 115-d将所接收到的定时变量与它自己的本地副本进行比较并且确定是否存在显著的差异是有用的。如果存在显著的差异(即,差异超过某个预定阈值),则UE 115-d 可识别出已经发生异常并且UE 115-d应当尝试用于接收经更新的定时变量的某个其他方法。

[0091] 图6解说了用于获得定时变量的方法。图6示出了根据本公开的各个方面的解说参与D2D发现的UE 115-e与基站105-c之间的通信的消息流图600。该UE和基站可以是图1、2、3、和/或4中描述的UE 115以及图1和/或2中描述的基站105的示例。

[0092] 一旦UE 115-e处于与基站105-c的连通模式605,UE 115-e和基站105-c 就相互认证,并且由此在此连通模式605期间在这两个实体之间交换的通信可以是安全的。基站105-c能够确定(在框610)UE 115-e是否已被授权参与D2D 发现通信(例如,经由从网络D2D发现模块接收授权)。一旦基站105-c识别出UE 115-e是D2D UE,基站105-c就可主动地向UE 115-e转发RRC消息615,而无需等待来自UE 115-e的请求。RRC消息615可包括具有所需要的定时变量的SIB。例如,RRC消息615可以是RRC连接重配置消息并且可包括SIB16 或者专用于包括定时变量的D2D通信的某个其他SIB。一旦UE 115-e经由RRC 消息615接收到定时变量,UE 115-e就可将它自己的本地定时变量与所接收到的定时变量进行比较(步骤620)。注意,基站仅可在信令中向被授权进行D2D 通信的UE发送附加的定时变量,因此通过不影响不参与D2D通信的其他UE 来维持传统支持。

[0093] 图7解说了用于获得定时变量的另一方法。图7示出了根据本公开的各个方面的解说参与D2D发现的UE 115-f与基站105-d之间的通信的消息流图 700。该UE和基站可以是图

1、2、3、和/或4中描述的UE 115以及图1和/ 或2中描述的基站105的示例。

[0094] 一旦UE 115-f处于与基站105-d的连通模式705,UE 115-f和基站105-d 就相互认证,并且由此在此连通模式705期间在这两个实体之间交换的通信可以是安全的。在此方法中,UE 115-f利用可能已经对于参与D2D通信而言必需的附加消息。例如,UE 115-f可向基站105-d传送专用RRC消息710以请求D2D资源。D2D资源可由基站根据类型1(公共或受设备控制的)资源分配或者类型2(专用或受网络控制的)资源分配来分配。受设备控制的或类型1的发现资源不是任何给定UE专用的,而是表示一个以上UE可自主地从中选择资源以用于D2D发现的发现资源池。类型2或受网络控制的资源被唯一地分配给个体UE。

[0095] 因此,当UE 115-f正使用类型2分配时,UE 115-f可向基站105-d发送 RRC请求710以接收其特定的资源分配。基站105-d可响应于RRC请求710 而向UE 115-f返回RRC响应715。在类型2分配的情形中,RRC响应715可包括用于D2D通信的资源的分配。另外,然而,RRC响应715还可包括必需的定时变量。

[0096] 当UE 115-f正使用对D2D资源的类型1分配时,UE 115-f可不被要求从基站105-d获得特定的资源分配。然而,在此方法中,UE 115-f仍向基站105-d 发送RRC请求710。基站105-d可用RRC响应715来响应。然而,因为不从基站105-d要求资源分配,所以RRC响应715可不包括资源分配,而是取而代之可仅包括必需的定时变量。

[0097] 因此,无论UE 115-f正在使用对D2D资源的类型1还是类型2分配,UE 115-f皆可向基站105-d发送RRC请求710。在任一情形中,基站105-d将向 UE 115-f发送RRC响应715,其中RRC响应715包括必需的定时变量。可由 UE 115-f发送的RRC请求710的示例为RRCPRoSe资源分配请求。可被接收的RRC响应715的示例为RRCProSe资源分配。一旦UE 115-f 经由RRC响应 715接收到定时变量,UE 115-f就可将它自己的本地定时变量同步到所接收到的定时变量(步骤720)。

[0098] 图8中解说了用于安全地获得定时变量的附加方法,其示出了根据解说本公开的各个方面在参与D2D发现的UE 115-g、网络D2D发现模块210-b与基站105-e之间的通信的消息流图800。该UE可以是图1、2、3、和/或4中描述的UE 115的示例。该基站可以是图1和/或2中描述的基站105的示例。网络D2D发现模块210-b可以是参照图2和/或3描述的网络D2D发现模块210 和/或210-a的示例。

[0099] 在此情景中,定时变量信息最初不是从基站105-e获得的,而是取而代之从网络D2D发现模块210-b 获得的。这在UE 115-g正在从网络D2D发现模块 210-b 寻求参与D2D通信的授权时发生。为了达成此举,UE 115-g进入与网络 D2D发现模块210-b 的连通模式805。UE 115-g随后向网络D2D发现模块210-b 提交针对D2D发现授权的请求810。网络D2D发现模块210-b用响应815来响应,该响应815可包括授权以及所需要的定时变量。UE 115-g可随后同步所接收到的定时变量(步骤820)。

[0100] 响应815还可包括定时偏移允许。因为UE 115-g与网络D2D发现模块 210-b 之间的通信可能遭受各种网络延迟,所以连同定时变量一起包括定时偏移允许以指示可被用于防止上述重放攻击的最大定时偏移。定时偏移允许使 UE 115-g能够评价稍后接收到的定时变量的准确性,如以下所解释的。

[0101] 在存储并且同步经由消息815从网络D2D发现模块210-b接收到的定时变量(步骤820)之后,UE 115-g可在广播SIB中检测本地定时变量。例如,基站105-e可广播包括定时变

量的SIB广播消息825。UE 115-g可随后将(先前与由网络D2D发现模块210-b提供的定时变量同步的)定时变量与所广播的 SIB中提供的本地定时变量进行比较,由此标识任何异常(框830)。如果这两个定时变量在由定时偏移允许指定的可允许偏移内,则UE 115-g可假定所广播的SIB是真实的并且UE 115-g可存储连同所广播的SIB一起包括的本地定时变量(框835)。如果这两个定时变量之间的差异大于由定时偏移允许所允许的偏移,则UE 115-g可将此标记为异常,并且可继续使用存储着的定时变量、可通知网络D2D发现模块210-b、和/或可使用上述不同方法之一来获得经更新的定时变量。

[0102] 定时偏移允许还可由网络D2D发现模块210在MIC的验证期间使用(如参照图3所描述的)。因此,当网络D2D发现模块210验证MIC时,定时偏移允许可被用于定义用于生成MIC的定时变量与由监视方UE传送的定时变量之间的可接受差异。

[0103] 当定时变量模块430可使用以上参照图5、6、7和/或8描述的任何方法来执行与定时变量相关的功能时,(图4的)MIC模块425使用定时变量来生成和/或验证MIC。

[0104] 再次返回到图4,MIC模块425在UE 115已准备好广播MIC(例如经由图3的消息320)时基于定时变量来生成MIC。例如,MIC模块425可例如从发射机模块420获得估计的消息传输时间。该传输时间估计可基于D2D发现时隙、由网络分配的可用D2D发现资源、以及UE的定时变量。作为示例,发现时隙可由网络每十秒钟设置一次,并且D2D发现消息仅可在某些无线电资源内在某些无线电帧内被发送。因此,除了其当前状态之外,发射机模块420 还可在确定传输的估计时间时考虑这些因素(例如,在其队列中的D2D发现消息的数目、基于控制算法的传输机会、准备消息以供传输中的任何估计延迟、等等)。发射机模块420可随后在可在空中发送MIC消息时提供估计时间并且随后将该估计时间提供给MIC模块425。MIC模块425可随后在其MIC的生成中使用该估计时间。

[0105] 如果装置405是监视方UE,则MIC模块425可接收MIC并且使用UE 的定时变量来对收到消息加时间戳。装置405随后将所接收到的MIC、所接收到的D2D发现应用码、以及基于定时变量的时间戳传递给网络D2D发现模块 210。

[0106] 替换地,监视方UE可在其给网络D2D发现模块210的消息中包括表示监视方接收到MIC的时间与监视方UE将MIC传送给网络D2D发现模块210 的时间之间的流逝时间的时间差。在此情形中,网络D2D发现模块210可使用该时间差来确定MIC被接收到时的定时变量值。

[0107] 因此,D2D发现模块415可在宣告方和监视方UE两者中被使用以接收定时变量并且生成和/或转发MIC。另外,装置405可使用D2D发现模块415来向其他UE(诸如覆盖外UE(例如,图2的UE 115-b-4))转发定时变量。

[0108] 图9示出了根据本公开的各种方面的供在无线通信中使用的UE 115-i的框图900。UE 115-i可具有各种配置,并且可被包括在个人计算机(例如,膝上型计算机、上网本计算机、平板计算机等)、蜂窝电话、智能电话、PDA、数字视频记录器(DVR)、互联网电器、游戏控制台、电子阅读器等中或是其一部分。UE 115-i在一些示例中可具有内部电源(未示出),诸如小电池,以促成移动操作。在一些示例中,UE 115-i可以是参照图1、2、3、4、5、6、7、和/或8描述的UE 115或装置405之一的一个或多个方面的示例。UE 115-i可被配置成实现参照图1、2、3、4、5、6、7和/或8描述的特征和功能中的至少一些。

[0109] UE 115-i可包括UE处理器模块905、UE存储器模块910、至少一个UE 收发机模块

(由UE收发机模块930表示)、至少一个UE天线(由 UE天线935表示)、或D2D发现模块415-a。这些组件中的每一者可在一条或多条UE总线925上直接或间接地彼此通信。UE 115-i还可包括基站通信模块925,该基站通信模块925可执行关于与一个或多个基站的通信的操作。

[0110] UE存储器模块910可包括随机存取存储器(RAM)或只读存储器(ROM)。UE存储器模块910可存储包含指令的计算机可读、计算机可执行UE软件(SW) 代码920,这些指令被配置成在被执行时使得UE处理器模块905执行本文描述的用于传达例如D2D发现相关消息的各种功能。替换地,UE软件代码920 可以是不能由UE处理器模块905直接执行的,而是被配置成(例如,当被编译和执行时)使UE 115-i执行本文描述的各种功能。

[0111] UE处理器模块905可包括智能硬件设备,例如,中央处理单元(CPU) (诸如由INTEL®公司或AMD®制造的那些)、微控制器、专用集成电路(ASIC) 等。UE处理器模块905可处理通过UE收发机模块930接收到的信息或将发送给UE收发机模块930以供通过UE天线935传输的信息。UE处理器模块905可以单独地或与D2D发现模块415-a相结合地处置传送、接收以及管理D2D发现通信的各个方面。

[0112] UE收发机模块930 可包括调制解调器,该调制解调器被配置成调制分组并将经调制分组提供给UE天线935以供传输、以及解调从 UE天线935接收到的分组。UE收发机模块930在一些示例中可被实现为一个或多个发射机模块以及一个或多个分开的接收机模块。UE 收发机模块930可以支持D2D发现相关通信。UE收发机模块930可被配置成经由UE天线935和通信链路125与例如基站105-f(其可以是参照图1、2、5、6、7和/或8描述的一个或多个基站105)进行双向通信。UE收发机模块930还可被配置成经由UE天线935和通信链路125与例如UE 115-h(其可以是参照图1、2、3、5、6、7和/或8描述的UE 115或者参照图4描述的装置405中的一者或多者)进行双向通信。虽然UE 115-i可包括单个UE天线,但存在其中UE 115-i可包括多个UE天线935的示例。

[0113] D2D发现模块415-a可被配置成执行或控制参照图1、2、3、4、5、6、7、和/或8描述的与D2D发现相关的特征或功能中的一些或全部。例如,D2D发现模块415-a可被配置成支持D2D发现消息的传送和接收以及对由D2D发现消息实现的D2D发现的管理。在一些示例中,并且作为示例,D2D发现模块 415-a可以是参照图4、5、6、7、和/或8描述的D2D发现模块415的一个或多个方面的示例。D2D发现模块415-a可包括MIC模块425-a(其可以是图4 的MIC模块425的示例)以及定时变量模块430-a(其可以是图4的定时变量模块430的示例)。D2D发现模块415-a或其各部分可包括处理器,或者D2D 发现模块415-a的一些或全部功能可由UE处理器模块905执行或与UE处理器模块905相结合地执行。另外,D2D发现模块415-a或其各部分可包括存储器,或者D2D发现模块415-a的一些或全部功能可以使用UE存储器模块910 或与UE存储器模块910相结合地使用。

[0114] 图10示出了根据本公开的各种方面的供在无线通信中使用的装置1005 的框图1000。在一些示例中,装置1005可以是参照图1、2、5、6、7、和/或 8描述的一个或多个基站105的各方面的示例。装置1005也可以是处理器。装置1005可包括基站接收机模块1010、基站D2D发现模块1015、或者基站发射机模块1020。这些组件中的每一者可与彼此处于通信。

[0115] 装置1005的组件可个体地或整体地使用一个或多个适配成以硬件执行一些或所有适用功能的ASIC来实现。替换地,这些功能可以由一个或多个集成电路上的一个或多个其他处理单元(或核)来执行。在其他示例中,可使用可按本领域所知的任何方式来编程的

其他类型的集成电路(例如,结构化/平台 ASIC、FPGA、以及其他半定制IC)。每个单元的功能也可以整体或部分地用实施在存储器中的、被格式化成由一或多个通用或专用处理器执行的指令来实现。

[0116] 在一些示例中,基站接收机模块1010可包括至少一个RF接收机,诸如可操作用于在射频频谱上接收传输的至少一个RF接收机。在一些示例中,该射频频谱可被用于LTE/LTE-A通信,如例如参照图1、2或7描述的。基站接收机模块1010可被用来在无线通信系统的一条或多条通信链路(诸如参照图1 或2描述的无线通信系统100的一条或多条通信链路125、134)上接收各种类型的数据或控制信号(即,传输)。基站接收机模块1010接收的数据或控制信号的类型的示例包括参照图5、6、7或8描述的D2D发现通信。

[0117] 在一些示例中,基站发射机模块1020可包括至少一个RF发射机,诸如能操作用于传送D2D发现通信的至少一个RF发射机。基站发射机模块1020 可被用来在无线通信系统的一条或多条通信链路(诸如参照图1或2描述的无线通信系统100的一条或多条通信链路125、134)上传送各种类型的数据或控制信号(即,传输)。基站发射机模块1020传送的数据或控制信号的类型的示例包括参照图5、6、7或8描述的D2D发现通信。

[0118] 在一些示例中,基站D2D发现模块1015可被用来管理经由基站接收机模块1010和/或基站发射机模块1020对D2D发现请求710的接收和对D2D发现消息515、520、615、715或825(参见图5、6、7、8)的传送。管理D2D发现通信的接收和传送可包括在UE处于与装置1005的连通模式时向UE传送定时变量。例如,参照图5,基站D2D发现模块1015可管理消息520中对SIB的传达。在一附加示例中,参照图6,基站D2D发现模块1015可管理RRC消息615至经连通UE 115-e的传达,其中该RRC消息包括具有定时变量的SIB。参照图7,基站D2D发现模块1015可管理对资源的RRC请求710的接收,并且响应于请求710而用包括定时变量的RRC响应715来响应。参照图8,装置 1005可在SIB消息825中广播具有定时变量的SIB。

[0119] 图11示出了根据本公开的各方面的可被配置成在接收和传送D2D发现通信中使用的通信系统1100的框图。系统1100可以是图1和/或2中描述的无线通信系统100和/或200的各方面的示例。系统1100可包括基站105-g。基站105-g 可包括基站天线1145、基站收发机模块1150、基站存储器1180、以及基站处理器模块1170,其各自可彼此处于直接或间接通信(例如,在一条或多条总线上)。基站收发机模块1150可被配置成经由基站天线1145 来与UE 115-j(其可以是图1、2、3、5、6、7和/或8的UE 115和/或图4的装置405的示例)进行双向通信。基站收发机模块1150(和/或基站105-g的其他组件)还可被配置成与一个或多个网络进行双向通信。在一些情形中,基站105-g可通过网络通信模块1175与核心网130-b 和/或控制器1120通信。基站105-g可以是图1、2、5、6、7、和/或8的基站105和/或图10的装置1005 的示例,且也可以是演进型B节点基站、家用演进型B节点基站、B节点基站、和/或家用B节点基站。在一些情形中,控制器1120可以被集成到基站105-g 中,诸如对于演进型B节点基站。

[0120] 基站105-g还可与其他基站105(诸如基站1005-m和基站1005-n)通信。基站105中的每一者可以使用不同的无线通信技术(诸如不同的无线电接入技术)与UE 115-j通信。在一些情形中,基站105-g可以利用基站通信模块1165 与其他基站(诸如1005-m和/或1005-n)通信。在一些示例中,基站通信模块 1165可以提供LTE无线通信技术内的X2接口以提供在一些基站105之间的通信。在一些示例中,基站105-g可通过控制器1120和/或核心网130-b 来与其他基站进行通信。

[0121] 基站存储器1180可包括RAM和ROM。基站存储器1180还可存储计算机可读、计算机可执行软件代码1185，该软件代码1185包含配置成在被执行时使基站处理器模块1170执行本文所描述的各种功能(例如，接收和传送D2D 发现通信)的指令。替换地，软件代码1185可以是不能由基站处理器模块1170 直接执行的，而是被配置成(例如，在被编译和执行时)使计算机执行本文描述的功能。

[0122] 基站处理器模块1170可包括智能硬件设备，例如，CPU、微控制器、ASIC 等。基站处理器模块1170可包括语音编码器(未示出)，该语音编码器被配置成经由话筒接收音频、将该音频转换成代表收到音频的分组(例如，长30ms 等)、将这些音频分组提供给基站收发机模块1150、以及提供对用户是否正在说话的指示。替换地，编码器可以仅向基站收发机模块1150提供分组，其中由分组本身的提供或扣留/抑制来提供对用户是否正在说话的指示。

[0123] 基站收发机模块1150可包括配置成调制分组并将经调制分组提供给基站天线1145以供传输、以及解调从基站天线1145接收到的分组的调制解调器。尽管基站105-g的一些示例可包括单个基站天线1145，但基站105-g 优选地包括用于多条链路的多个基站天线1145，它们可支持载波聚集。例如，一条或多条链路可被用于支持与UE 115-j的宏通信。

[0124] 根据图11的架构，基站105-g可进一步包括通信管理模块1160。通信管理模块1160可以管理与其他基站105的通信。作为示例，通信管理模块1160 可以是基站105-g的组件，该组件经由总线与基站105-g的其他组件中的一些和全部处于通信。替换地，通信管理模块1160的功能性可被实现为基站收发机模块1150的组件、实现为计算机程序产品和/或实现为基站处理器模块1170 的一个或多个控制器元件。

[0125] 基站105-g的组件可被配置成实现以上关于图10的装置1005所讨论的各方面，并且可出于简明起见而不在此重复。例如，基站105-g可包括基站D2D 发现模块1015-a。基站D2D发现模块1015-a可以是图10的基站D2D发现模块1015的示例。基站D2D发现模块1015-a可被配置成执行或控制参照图1、 2、5、6、7、8和/或10描述的与D2D发现相关的特征或功能中的一些或全部。例如，基站D2D发现模块1015-a可被配置成支持D2D发现通信的接收和传送。具体地，基站D2D发现模块1015-a可被配置成在UE处于与基站105-g的连通模式时支持定时变量至UE(例如，UE 115-j)的传送。基站D2D发现模块 1015-a或其各部分可包括处理器，或者基站D2D发现模块1015-a的一些或全部功能可由基站处理器模块1170执行或与基站处理器模块1170相结合地执行。另外，基站D2D发现模块1015-a或其各部分可包括存储器，或者基站D2D 发现模块1015-a的一些或全部功能可以使用基站存储器1180或与基站存储器 1180相结合地使用。

[0126] 图12是解说根据本公开的各个方面的无线通信方法1200的示例的流程图。出于清楚起见，方法1200在以下是参照关于图1、2、3、5、6、7、8和/ 或9描述的UE 115中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述的。在一些示例中，UE(诸如UE 115之一)或装置(诸如装置405)可执行一个或多个代码集以控制该UE或装置的功能元件来执行以下描述的功能。

[0127] 在框1205，方法1200可包括在设备处接收来自网络的定时变量，该定时变量是在该设备处于连通模式时接收的。定时变量可按消息520、615、715、 815、和/或825的形式来接收，如以上参照图5、6、7和/或8所描述的。

[0128] 在框1210，方法1200可包括将定时变量用于D2D发现消息认证。例如，所接收到的

定时变量可被用于生成MIC或者验证MIC，如以上参照图3所描述的。

[0129] 在一些示例中，框1205或1210处的操作可使用参照图4和/或9描述的 D2D发现模块415来执行。然而，应注意，方法1200仅仅是一个实现并且方法1200的操作可被重新排列或以其他方式修改以使得其它实现是可能的。

[0130] 图13是解说根据本公开的各个方面的无线通信方法1300的示例的流程图。出于清楚起见，方法1300在以下是参照分别关于图1、2、3、5、6、和/ 或9描述的UE 115中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述的。在一些示例中，UE(诸如UE 115之一)或装置(诸如装置405)可执行一个或多个代码集以控制该UE或装置的功能元件来执行以下描述的功能。

[0131] 方法1300解说了由路径1335和1340表示的两个替换流程路径。在框 1305，方法1300可包括进入连通模式。如以上所解释的，UE可受益于在UE 处于连通模式(诸如RRC_连通模式)时接收定时变量，其中UE和经连通实体相互认证。因此，在框1305，UE进入连通模式，如例如通过图5和/或6中的连通模式505和/或605所解说的。UE可随后使用流程路径1335、1340之一来获得所需要的定时变量。在以下描述的图14中解说附加的替换流程路径。

[0132] 遵循流程路径1335，在框1310，方法1300可包括检测具有所需要的定时变量的SIB。对SIB的检测是响应于接收到这么做的命令的。在UE仍处于连通模式时检测SIB。此SIB检测的示例在图5中通过消息520解说。

[0133] 在框1315，方法1300可包括验证不存在与所接收到的定时变量相关的异常的步骤。此步骤的示例在图5中通过步骤525解说。在流氓基站活跃的某些情况下，没有发生异常的验证可以是必要的。例如，流氓基站可能尝试将定时相关的SIB注入到由合法基站调度的相同广播时隙中。因此，在此情况下，UE 可能观察到相同类型的多个SIB被同时广播。替换地，多个SIB可能冲突，以使得UE没有接收到SIB。此外，UE可能仅接收到由流氓基站广播的SIB，其中UE确定在所接收到的定时变量(来自合法SIB)与UE的本地存储的定时变量之间存在显著差异。在这些情形中的每一者中，UE可确定已发生异常并且应当使用不同方法来获得定时变量。

[0134] 如果被认为没有发生任何异常，则所接收到的定时变量被存储在UE处(在框1320)。在图5中在步骤530处描述类似步骤。

[0135] 如果用于获得定时变量的替换路径(诸如路径1340)被使用，则方法1300 包括框1330。在框1330，方法1300包括接收RRC消息，该RRC消息包括具有所需要的定时变量的SIB。所接收到的RRC消息的示例可包括消息615，如图6中所解说的。RRC消息可在UE不需要专门请求该消息的情况下被接收，因为传送方基站可独立地确定UE正在参与D2D发现通信。一旦UE接收到具有其定时变量的RRC消息，UE就能够在框1320处存储该定时变量。

[0136] 应注意，方法1300仅仅是一个实现并且方法1300的操作可被重新排列或以其他方式修改以使得其它实现是可能的。作为具体示例，并非在方法1300 中解说的每一操作都需要被执行，并且许多操作可以按与图13中解说的不同次序执行。

[0137] 图14是解说根据本公开的各个方面的无线通信方法1400的示例的流程图。出于清楚起见，方法1400在以下是参照分别关于图1、2、3、7、8、和/ 或9描述的UE 115中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述的。在一些示例中，UE(诸如UE 115之一)或装置(诸如装置405)可执行一个或多个代码集以控制该UE或装

置的功能元件来执行以下描述的功能。

[0138] 方法1400解说了由路径1450和1455表示的两个替换流程路径。在框 1405，方法1400可包括进入连通模式。如以上所解释的，UE可受益于在UE 处于连通模式(诸如RRC_连通模式)时接收定时变量，其中UE和经连通实体相互认证。因此，在框1405，UE进入连通模式，如例如通过图7和/或8中的连通模式705和/或805所解说的。UE可随后使用流程路径1450、1455之一来获得所需要的定时变量。在以上描述的图13中解说附加的替换流程路径。

[0139] 遵循流程路径1450，在框1410，方法1400可包括传送对发现资源的RRC 请求。可将RRC请求从UE传送给基站。RRC请求可被传送，而无论UE 正在使用类型1(或受设备控制的)资源分配还是类型2(或受网络控制的) 资源分配。受设备控制的或类型1的发现资源不是任何给定UE专用的，而是表示一个以上UE可自主地从中选择资源以用于D2D发现的发现资源池。类型 2或受网络控制的资源被唯一地分配给个体UE。因此，当UE 115正在使用类型2分配时，UE被要求向基站发送RRC请求以接收其特定的资源分配。当 UE正在使用对D2D资源的类型1分配时，UE不被要求从基站获得特定的资源分配。然而，在方法1400中，UE仍发送RRC请求，而无论UE正在使用类型1还是类型2资源分配。所传送的RRC请求的示例为图7的RRC请求710。

[0140] 在框1415，UE接收包括定时变量的RRC响应。如果UE正在使用类型2 资源分配，则所接收到的RRC响应可包括资源分配和定时变量两者。如果UE 正在使用类型1资源分配，则所接收到的RRC响应可不包括实际的资源分配，而是可仅包括定时变量。所接收到的RRC响应的示例为图7的RRC响应715。

[0141] 一旦被接收，定时变量就被存储在UE处(框1430)。在图7中在框720 处描述类似步骤。

[0142] 如果用于获得定时变量的替换路径(诸如路径1455)被使用，则方法1400 包括框1420、1425、1430、1435、、1440和1445。在框1420，方法1400包括传送对D2D发现授权的请求。所传送的请求是从UE传送给网络D2D发现模块(诸如ProSe功能)的。所传送的请求的示例为图8的请求810。

[0143] 在框1425，UE从网络D2D发现模块接收授权消息。所接收到的授权消息还可包括定时变量。所接收到的授权消息可附加地包括定时偏移允许(诸如 MAX_OFFSET)。所接收到的具有定时变量和定时偏移允许的授权消息的示例为图8的消息815。

[0144] 接收自网络D2D发现模块的定时变量可由UE用于与其自己的本地存储的定时变量进行比较。由此，在框1430，UE可存储所接收到的定时变量。此步骤的示例在图8的框820处解说。另外，如果还接收到定时偏移允许，则可以存储该定时偏移允许。UE可使用所接收到的定时偏移允许来确定所接收到的定时变量与本地定时变量之间的差异是否在定时偏移变量内，如以下并且结合图8所解释的。

[0145] 在框1435，UE可从基站接收SIB广播。所接收到的SIB可包括本地定时变量。由UE接收到的SIB广播消息的示例可包括图8的消息825。

[0146] 在框1440，UE验证在(接收自网络D2D发现模块的)所接收到的定时变量与作为SIB的一部分从基站接收到的本地定时变量之间不存在异常。在比较这两个定时变量时，UE使用先前接收到的定时偏移允许。如果这两个定时变量相差大于所接收到的定时偏移允许的量，则可能存在异常并且UE可能需要使用不同方法来获得经更新的定时变量。然而，如果这

两个定时变量相差小于所接收到的定时偏移允许的量，则UE可推断不存在异常。此验证步骤的示例在图8的框830处解说。

[0147] 如果不存在异常，则UE可在框1445开始广播发现宣告消息(诸如ProSe 应用码)，如参照图3所描述的。此宣告步骤的示例在图8的框835处解说。

[0148] 应注意，方法1400仅仅是一个实现并且方法1400的操作可被重新排列或以其他方式修改以使得其它实现是可能的。作为具体示例，并非在方法1400 中解说的每一操作都需要被执行，并且许多操作可以按与图14中解说的不同次序执行。

[0149] 图15是解说根据本公开的各个方面的无线通信方法1500的示例的流程图。出于清楚起见，以下参照关于图1、2、5、6、7、8、和/或11描述的基站 105中的一者或多者的各方面或者参照图10描述的装置1005中的一者或多者的各方面来描述方法1500。在一些示例中，基站(诸如基站105之一)或装置 (诸如装置1005)可执行一个或多个代码集以控制该基站或装置的功能元件来执行以下描述的功能。

[0150] 在框1505，方法1500可包括进入与设备的连通模式。连通模式(诸如图 5、6和/或7的连通模式505、605和/或705)可确保基站和经连通UE两者相互认证。

[0151] 在框1510，方法1500可包括在设备处于连通模式时向该设备传送定时变量。定时变量可按消息520、615、和/或715的形式来传送，如以上参照图5、 6、和/或7所描述的。

[0152] 在一些示例中，框1205或1210处的操作可使用参照图10和/或11描述的基站D2D发现模块1015来执行。然而，应注意，方法1500仅仅是一个实现并且方法1500的操作可被重新排列或以其他方式修改以使得其它实现是可能的。

[0153] 图16是解说根据本公开的各个方面的无线通信方法1600的示例的流程图。出于清楚起见，以下参照关于图1、2、5、6、7、和/或11描述的基站105 中的一者或多者的各方面或者参照图10描述的装置1005中的一者或多者的各方面来描述方法1600。在一些示例中，基站(诸如基站105之一)或装置(诸如装置1005)可执行一个或多个代码集以控制该基站或装置的功能元件来执行以下描述的功能。

[0154] 方法1600解说了由路径1645、1650和1655表示的三个替换流程路径。在框1605，方法1600可包括进入与处于连通模式的UE的通信。如以上所解释的，UE可受益于在UE处于连通模式(诸如RRC_连通模式)时接收定时变量，其中UE和基站相互认证。因此，在框1605，基站与处于连通模式的UE 处于通信中，如例如通过图5、6和/或7中的连通模式505、605和/或705所解说的。基站可随后使用流程路径1645、1650、1655之一来获得所需要的定时变量。

[0155] 遵循流程路径1645，在框1610，方法1600可包括确定经连通UE被授权进行D2D发现。例如，基站可以能够经由从网络D2D发现模块接收授权来确定经连通UE是否已被授权参与D2D发现通信。此步骤的示例在图5的框510 处解说。

[0156] 在框1615，方法1600可包括广播包括定时变量的SIB。所广播的SIB(诸如图5的SIB消息520)可以是SIB16或者可以是因D2D发现而异的SIB。以此方式，使接收方UE能够在该UE处于与基站的连通模式时接收定时变量。

[0157] 替换地，可以遵循流程路径1650。在流程路径1650中，在框1625，方法 1600可包括确定经连通UE被授权进行D2D发现。例如，基站可以能够经由从网络D2D发现模块接收授权来确定经连通UE是否已被授权参与D2D发现通信。此步骤的示例在图6的框610处解说。

[0158] 在框1630，方法1600可包括传送RRC消息，该RRC消息包括具有定时变量的SIB。因

为基站已确定经连通UE被授权进行D2D发现，所以基站可传送RRC消息，而无需等待来自经连通UE的请求。所传送的RRC消息的示例可包括图6的RRC消息615。

[0159] 替换地，可以遵循流程路径1655。在流程路径1655中，在框1635，方法 1600可包括接收对发现资源的RRC请求(诸如图7的RRC请求710)。RRC 请求可以来自将类型1(受设备控制的)或类型2(受网络控制的)资源分配用于D2D发现的UE。

[0160] 在框1640，方法1600可包括传送对RRC请求的RRC响应。如果经连通 UE正在使用类型2(受网络控制的)资源分配，则RRC响应可包括所分配的资源和定时变量两者。如果经连通UE正在使用类型1(受设备控制的)资源分配，则RRC响应不需要包括任何资源分配，而是可取而代之仅包括定时变量。在任一情形中，定时变量被包括作为RRC响应的一部分。RRC响应的示例可包括图7的RRC响应715。

[0161] 应注意，方法1600仅仅是一个实现并且方法1600的操作可被重新排列或以其他方式修改以使得其它实现是可能的。作为具体示例，并非在方法1600 中解说的每一操作都需要被执行，并且许多操作可以按与图16中解说的不同次序执行。

[0162] 图17是解说根据本公开的各个方面的无线通信方法1700的示例的流程图。出于清楚起见，以下参照分别关于图1、2、3、5、6、和/或9描述的UE 115 中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述方法1700。在一些示例中，UE(诸如UE 115之一)或装置(诸如装置405)可执行一个或多个代码集以控制该UE或装置的功能元件来执行以下描述的功能。

[0163] 在框1705，方法1700包括向网络中的ProSe功能发送发现请求以被允许宣告D2D发现应用码，如以上参照图3所描述的。发现请求可包含ProSe应用ID。发现请求可被发送给D2D发现模块(诸如服务UE的HPLMN或VPMLN 中的ProSe功能)。框1705的(各)操作可由D2D发现模块415结合以上参照图4描述的发射机模块420来执行。

[0164] 在框1710，方法1700包括从网络接收发现响应，如以上参照图3所描述的。发现响应可包括定时变量和定时偏移允许。框1710的(各)操作可由D2D 发现模块415结合以上参照图4描述的接收机模块410来执行。

[0165] 图18是解说根据本公开的各个方面的无线通信方法1800的示例的流程图。出于清楚起见，以下参照分别关于图1、2、3、5、6、和/或9描述的UE 115 中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述方法1800。

[0166] 在框1805，方法1800包括向网络发送发现请求以被允许宣告D2D发现应用码，如以上参照图3所描述的。发现请求可包含ProSe应用ID。发现请求可被发送给D2D发现模块(诸如服务UE的PLMN或VPMLN中的ProSe功能)。框1805的(各)操作可由D2D发现模块415结合以上参照图4描述的发射机模块420来执行。

[0167] 在框1810，方法1800包括从网络接收发现响应，如以上参照图3所描述的。发现响应可包括定时变量和定时偏移允许。框1810的(各)操作可由D2D 发现模块415结合以上参照图4描述的接收机模块410来执行。

[0168] 在框1815，方法1800包括将接收自网络的定时变量与设备处的本地定时变量进行比较以确定来自网络的定时变量与本地定时变量之间的差异是否在接收自网络的定时偏移内，如以上参照图3所描述的。框1815的(各)操作可由如以上参照图4所描述的定时变量模块430来执行。

[0169] 在框1820，方法1800包括如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内，则广播D2D发现宣告，如以上参照图3所描述的。框1820的(各)操作可由如以上参照图4所描述的定时变量模块430来执行。

[0170] 图19是解说根据本公开的各个方面的无线通信方法1900的示例的流程图。出于清楚起见，以下参照分别关于图1、2、3、5、6、和/或9描述的UE 115 中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述方法1900。

[0171] 在框1905，方法1900包括向网络发送发现请求以被允许宣告D2D发现应用码，如以上参照图3所描述的。发现请求可包含ProSe应用ID。发现请求可被发送给D2D发现模块(诸如服务UE的PLMN或VPMLN中的ProSe功能)。框1905的(各)操作可由D2D发现模块415结合以上参照图4描述的发射机模块420来执行。

[0172] 在框1910，方法1900包括从网络接收发现响应，如以上参照图3所描述的。发现响应可包括定时变量和定时偏移允许。框1910的(各)操作可由D2D 发现模块415结合以上参照图4描述的接收机模块410来执行。

[0173] 在框1915，方法1900包括将接收自网络的定时变量与设备处的本地定时变量进行比较以确定来自网络的定时变量与本地定时变量之间的差异是否在接收自网络的定时偏移内，如以上参照图3所描述的。框1915的(各)操作可由如以上参照图4所描述的定时变量模块430来执行。

[0174] 在框1920，方法1900包括生成要被包括在D2D发现宣告中的MIC，如以上参照图3所描述的。框1920的(各)操作可由如以上参照图4所描述的 MIC模块425来执行。

[0175] 在框1925，方法1900包括如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内，则广播D2D发现宣告，如以上参照图3所描述的。D2D发现码包括MIC以及D2D发现应用码。框1925的(各)操作可由定时变量模块430结合以上参照图4描述的发射机模块420来执行。

[0176] 图20是解说根据本公开的各个方面的无线通信方法2000的示例的流程图。以下参照分别关于图1、2、3、5、6、和/或9描述的UE 115中的一者或多者的各方面或者参照图4描述的装置405中的一者或多者的各方面来描述方法2000。

[0177] 在框2005，方法2000包括由监视方UE 115-c-2接收D2D发现宣告，如以上参照图3所描述的。D2D发现宣告可包括D2D发现应用码和在图3的宣告方UE 115-c-1中生成的MIC。框2005的(各)操作可由如以上参照图4所描述的接收机模块410来执行。

[0178] 在框2010，方法2000包括向网络发送匹配报告以用于验证，如以上参照图3所描述的。匹配报告可包括D2D发现应用码、MIC、以及定时变量。框 2010的(各)操作可由如以上参照图4所描述的发射机模块420来执行。

[0179] 图21是解说根据本公开的各个方面的无线通信方法2100的示例的流程图。出于清楚起见，以下参照关于图1、2、5、6、7、8、和/或11描述的基站 105和核心网130中的一者或多者的各方面或者参照图10描述的装置1005中的一者或多者的各方面来描述方法2100。在一些示例中，基站(诸如基站105 之一)或装置(诸如装置1005)可执行一个或多个代码集以控制该基站或装置的功能元件来执行以下描述的功能。

[0180] 在框2105，方法2100可包括从设备接收发现请求，如以上参照图3所描述的。框2105的(各)操作可由如以上参照图10所描述的接收机模块1010 来执行。

[0181] 在框2110，方法2100可包括向设备发送发现响应，如以上参照图3所描述的。发现响应可包括定时变量和定时偏移允许。框2110的(各)操作可由如以上参照图10所描述的发射机模块1020来执行。

[0182] 图22是解说根据本公开的各个方面的无线通信方法2200的示例的流程图。出于清楚起见，以下参照关于图2、3、8和/或10描述的网络D2D发现模块210和/或1015的各方面来描述方法2200。在一些示例中，装置(诸如装置 1005)可执行一个或多个代码集以控制基站或装置的功能元件来执行以下描述的功能。

[0183] 在框2205，方法2200可包括从设备接收匹配报告，如以上参照图3所描述的。匹配报告可从监视方UE接收，并且可包含MIC和定时变量以及D2D 发现应用码。框2205的(各)操作可由如以上参照图10所描述的接收机模块 1010来执行。

[0184] 在框2210，方法2200可包括验证包括在匹配报告中的MIC是有效的，如参照图3所描述的。框2210的(各)操作可由如以上参照图2、3、8和/或 10所描述的D2D发现模块210和/或1015来执行。

[0185] 在框2215，方法2200可包括向设备发送匹配响应，如以上参照图3所描述的。该匹配响应可包括指示网络处的当前时间的定时变量以及ProSe应用 ID。框2215的(各)操作可由D2D发现模块210和/或1015结合以上参照图 10描述的发射机模块1020来执行。

[0186] 应注意，由流程图1700、1800、1900、2000、2100和2200解说的方法仅是示例实现，并且方法和步骤的操作可被重新安排或以其他方式被修改，以使得其他实现也是可能的。

[0187] 以上结合附图阐述的详细说明描述了示例而不代表可被实现或者落在权利要求的范围内的仅有示例。术语“示例”和“示例性”在本说明书中使用时意指“用作示例、实例或解说”，并且并不意指“优于”或“胜过其他示例”。本详细描述包括具体细节以提供对所描述的技术的理解。然而，可以在没有这些具体细节的情况下实践这些技术。在一些实例中，众所周知的结构和设备以框图形式示出以避免模糊所描述的示例的概念。

[0188] 本文所描述的技术可用于各种无线通信系统，诸如CDMA、TDMA、 FDMA、OFDMA、SC-FDMA和其它系统。术语“系统”和“网络”常被可互换地使用。CDMA系统可实现诸如CDMA2000、通用地面无线电接入(UTRA)等无线电技术。CDMA2000涵盖IS-2000、IS-95和IS-856标准。IS-2000版本0 和A常被称为CDMA2000 1X、1X等。IS-856(TIA-856)常被称为CDMA2000 1xEV-DO、高速率分组数据(HRPD)等。UTRA包括宽带CDMA(WCDMA) 和其他CDMA变体。TDMA系统可实现诸如全球移动通信系统(GSM)之类的无线电技术。OFDMA系统可实现诸如超移动宽带(UMB)、演进型UTRA (E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、 Flash-OFDM等无线电技术。UTRA和E-UTRA是通用移动电信系统(UMTS) 的部分。3GPP长期演进(LTE)和高级LTE(LTE-A)是使用E-UTRA的新 UMTS版本。UTRA、E-UTRA、UMTS、LTE、LTE-A以及GSM在来自名为“第三代伙伴项目”(3GPP)的组织的文献中描述。CDMA2000和UMB在来自名为“第三代伙伴项目2”(3GPP2)的组织的文献中描述。本文所描述的技术既可用于以上提及的系统和无线电技术，也可用于其他系统和无线电技术。然而，以上描述出于示例目的描述了LTE系统，并且在以上大部分描述中使用了LTE术语，但这些技术也可应用于LTE应用以外的应用。

[0189] 可容适各种所公开的示例中的一些示例的通信网络可以是根据分层协议栈进行操作的基于分组的网络。例如，承载或分组数据汇聚协议(PDCP)层的通信可以是基于IP的。

无线电链路控制(RLC)层可执行分组分段和重装以在逻辑信道上通信。媒体接入控制(MAC)层可执行优先级处置并将逻辑信道复用成传输信道。MAC层还可使用混合自动重复请求(HARQ)以提供MAC 层的重传，从而提高链路效率。在物理层，传输信道可被映射到物理信道。

[0190] 信息和信号可使用各种各样的不同技艺和技术中的任一种来表示。例如，贯穿上面描述始终可能被述及的数据、指令、命令、信息、信号、位(比特)、码元、以及码片可由电压、电流、电磁波、磁场或磁粒子、光场或光粒子、或其任何组合来表示。

[0191] 结合本文中的公开所描述的各种解说性框以及模块可用设计成执行本文所描述的功能的通用处理器、数字信号处理器(DSP)、ASIC、FPGA或其他可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合来实现或执行。通用处理器可以是微处理器，但在替换方案中，处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可被实现为计算设备的组合，例如DSP与微处理器的组合、多个微处理器、与DSP核心协同的一个或多个微处理器、或者任何其他此类配置。在一些情形中，处理器可与存储器处于电通信，其中存储器存储可由处理器执行的指令。

[0192] 本文中所描述的功能可以在硬件、由处理器执行的软件、固件、或其任何组合中实现。如果在由处理器执行的软件中实现，则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。其他示例和实现落在本公开及所附权利要求的范围和精神内。例如，由于软件的本质，以上描述的功能可使用由处理器执行的软件、硬件、固件、硬连线或其任何组合来实现。实现功能的特征也可物理地位于各种位置，包括被分布以使得功能的各部分在不同的物理位置处实现。另外，如本文中(包括权利要求中)所使用的，在项目列举中使用的“或”指示析取式列举，以使得例如“A、B或C中的至少一个”的列举表示A或B或C或AB或AC或BC或ABC(即，A和B和C)。

[0193] 计算机程序产品或计算机可读介质两者均包括计算机可读存储介质和通信介质，包括促成计算机程序从一地到另一地的转移的任何介质。存储介质可以是能被通用或专用计算机访问的任何介质。作为示例而非限定，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、或者能用来携带或存储指令或数据结构形式的期望计算机可读程序代码且能由通用或专用计算机、或者通用或专用处理器访问的任何其他介质。任何连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)、或诸如红外、无线电、以及微波之类的无线技术从web网站、服务器、或其它远程光源传送而来，则该同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之中。如本文所用的盘(disk)和碟(disc)包括压缩碟(CD)、激光碟、光碟、数字多用碟(DVD)、软盘以及蓝光碟，其中盘(disk)常常磁性地再现数据，而碟(disc)用激光来光学地再现数据。上述的组合也被包括在计算机可读介质的范围内。

[0194] 提供对本公开的先前描述是为使得本领域技术人员皆能够制作或使用本公开。对本公开的各种修改对本领域技术人员而言将容易是显而易见的，并且本文中所定义的普适原理可被应用到其他变型而不会脱离本公开的精神或范围。贯穿本公开的术语“示例”指示了示例或实例并且并不暗示或要求对所提及的示例的任何偏好。由此，本公开并非被限定于本文中所描述的示例和设计，而是应被授予与本文中所公开的原理和新颖性特征相一致

的最广范围。

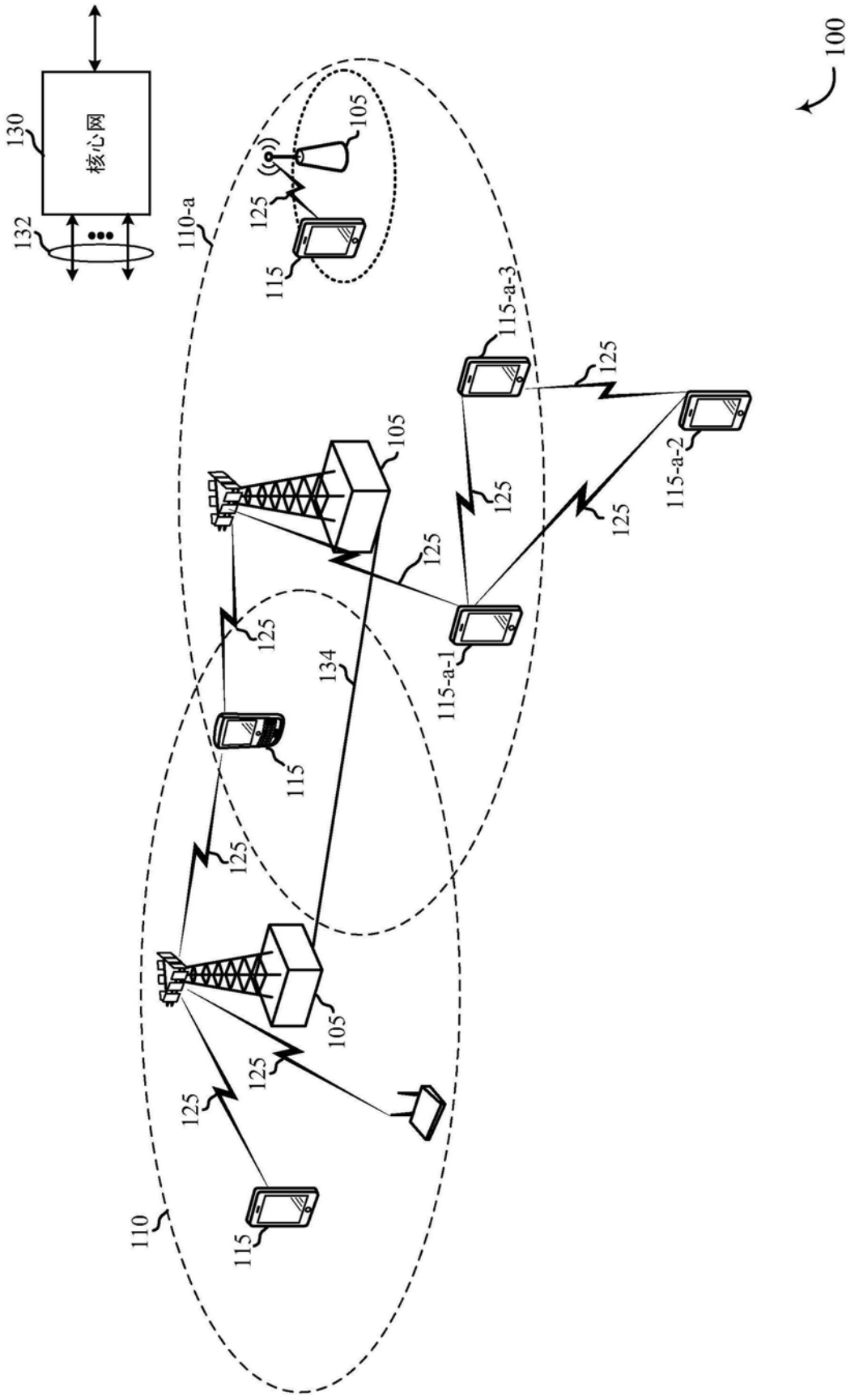

100
130
核心网
132
110-a
105
125
115
115-a-3
125
105
125
115-a-2
125
125
115-a-1
134
115
125
105
125
125
110
115

图1

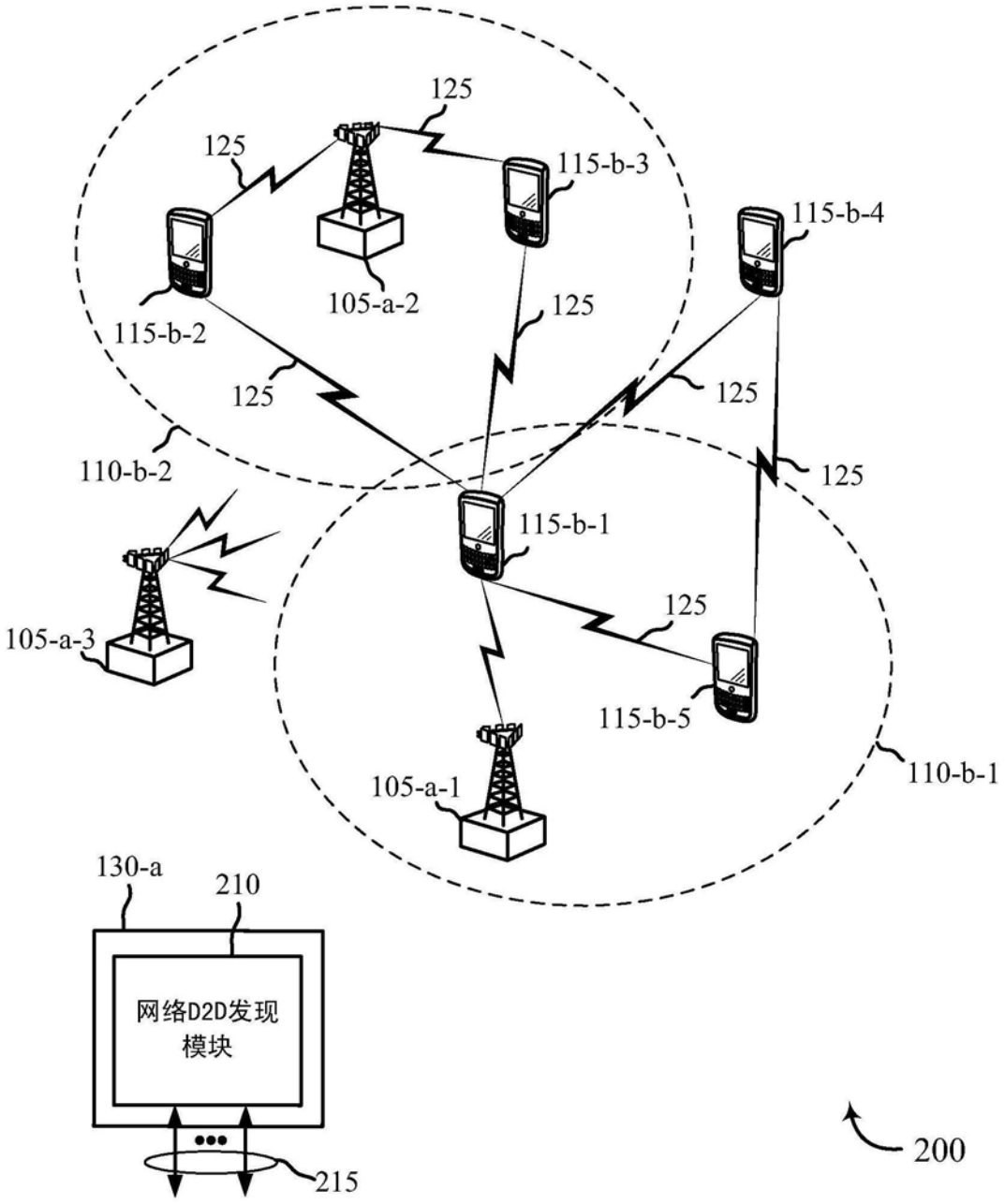

125
125
115-b-3
115-b-4
105-a-2
115-b-2
125
125
125
110-b-2
125
115-b-1
105-a-3
125
115-b-5
105-a-1
110-b-1
130-a
210
网络D2D发现
模块
215
200

图2

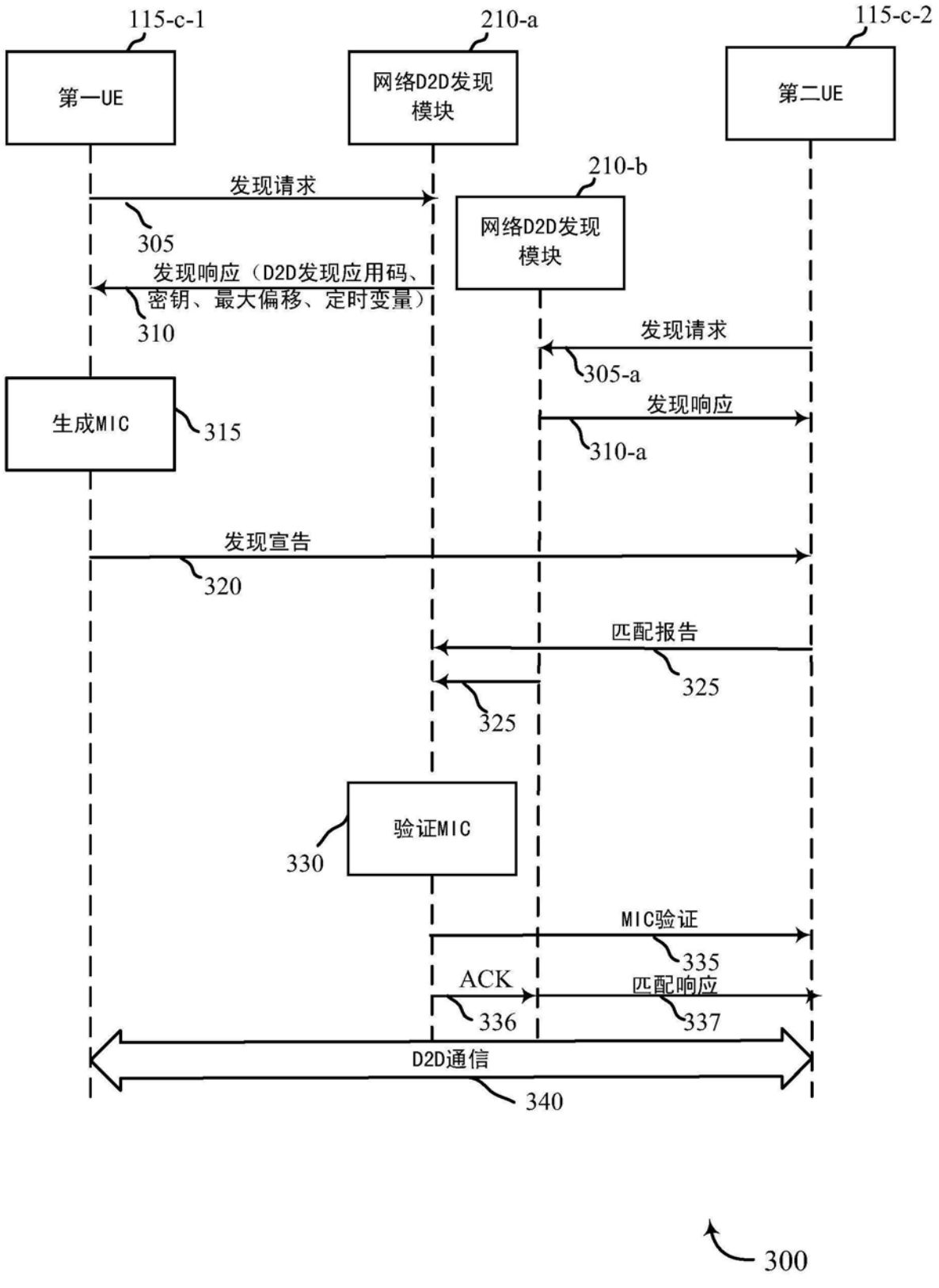

115-c-1
第一UE
210-a
网络D2D发现模块
115-c-2
第二UE
210-b
网络D2D发现模块
发现请求
305
发现响应（D2D发现应用码、密钥、最大偏移、定时变量）
310
发现请求
305-a
发现响应
310-a
生成MIC
315
发现宣告
320
匹配报告
325
325
验证MIC
330
MIC验证
335
ACK
336
匹配响应
337
D2D通信
340
300

图3

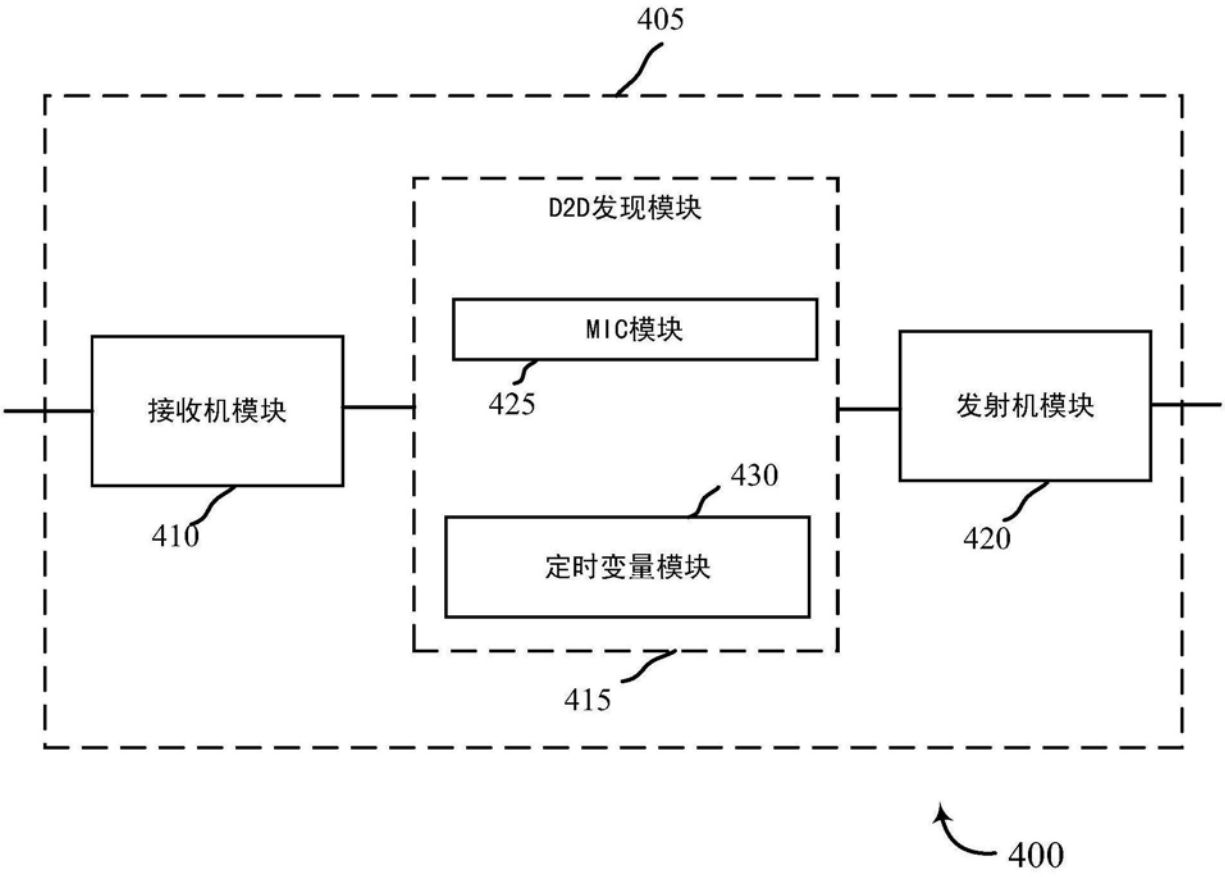


图4

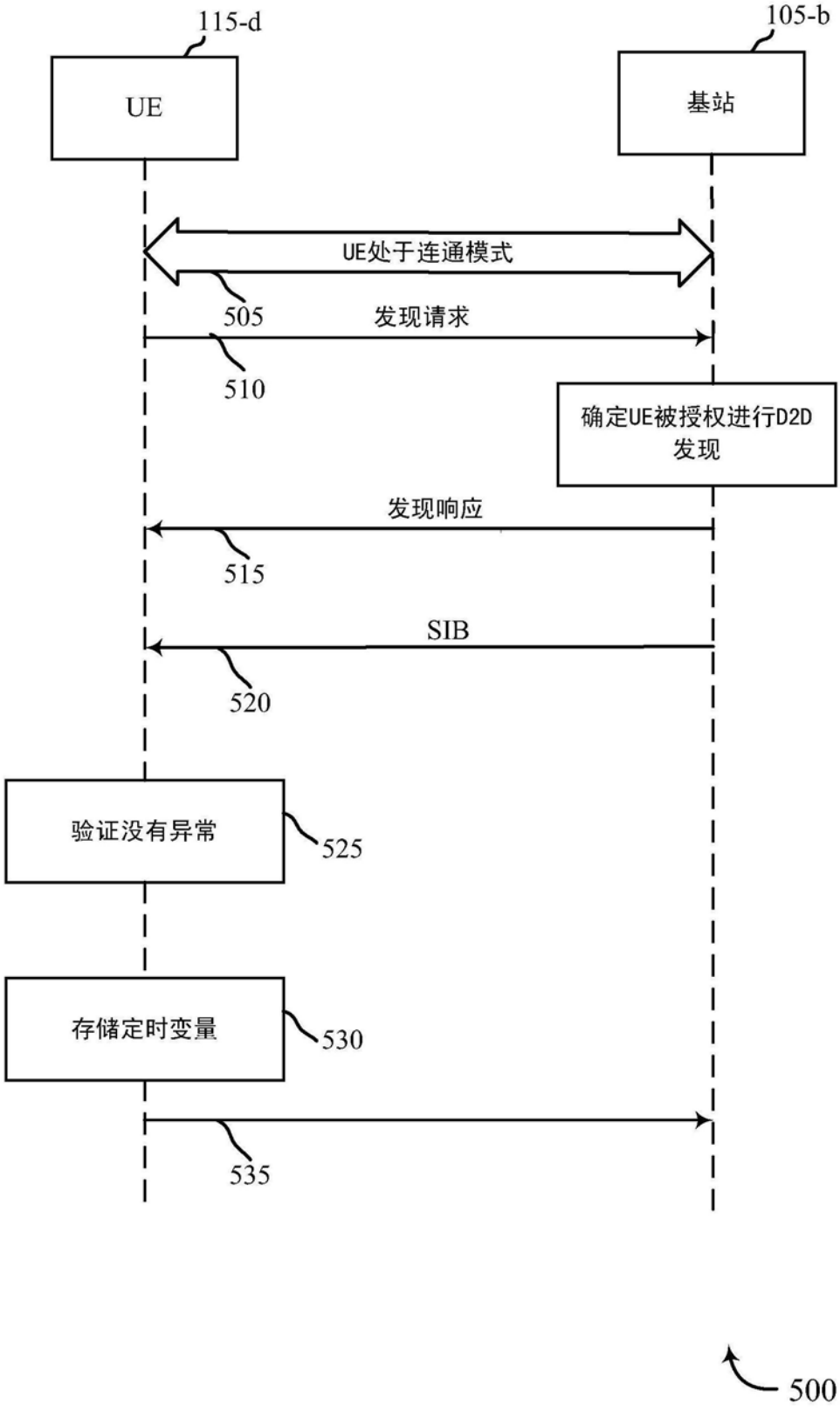

115-d
UE
105-b
基站
UE处于连通模式
505
发现请求
510
确定UE被授权进行D2D发现
发现响应
515
SIB
520
验证没有异常
525
存储定时变量
530
535
500

图5

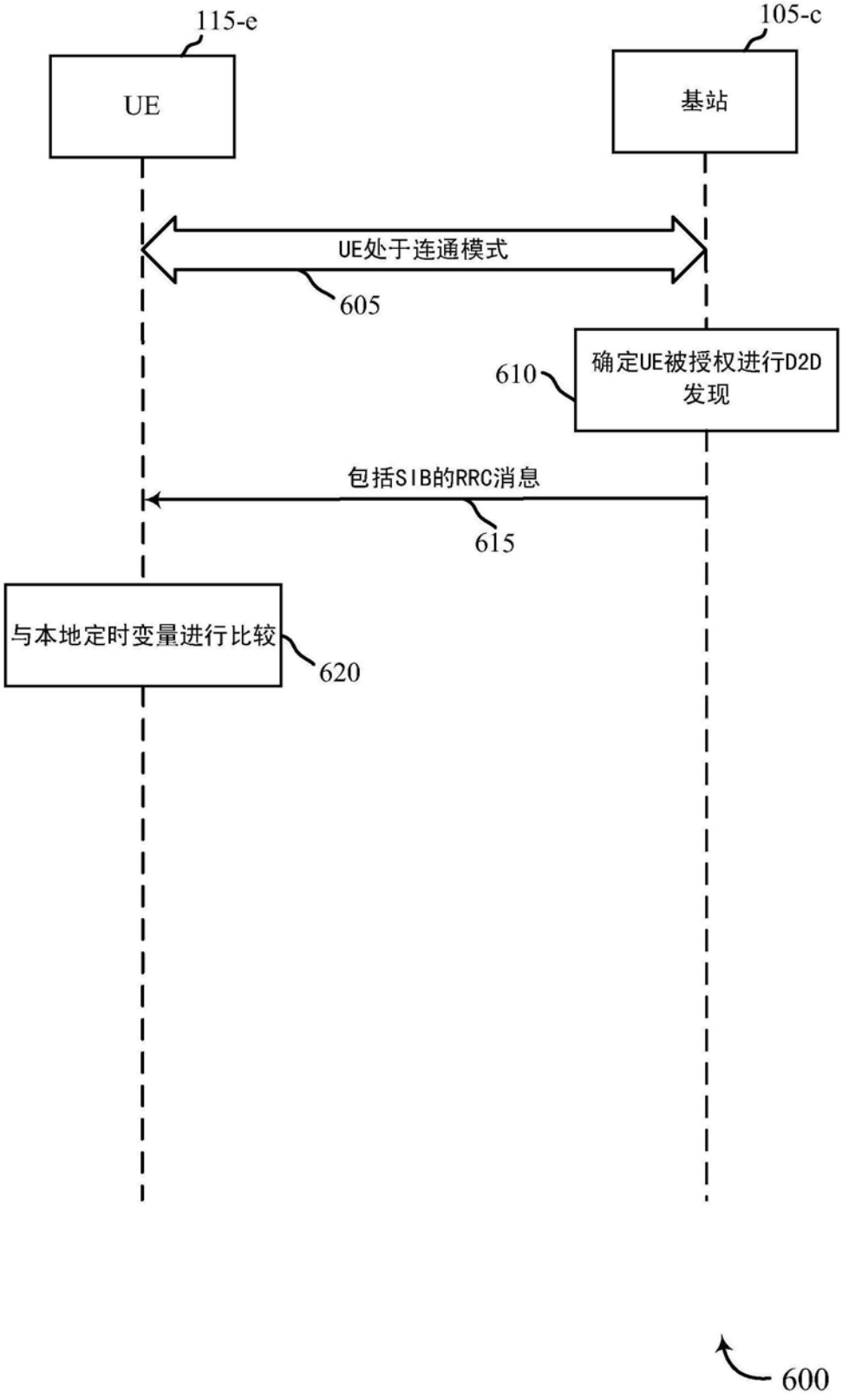

115-e
UE
105-c
基站
UE处于连通模式
605
610
确定UE被授权进行D2D发现
包括SIB的RRC消息
615
与本地定时变量进行比较
620
600

图6

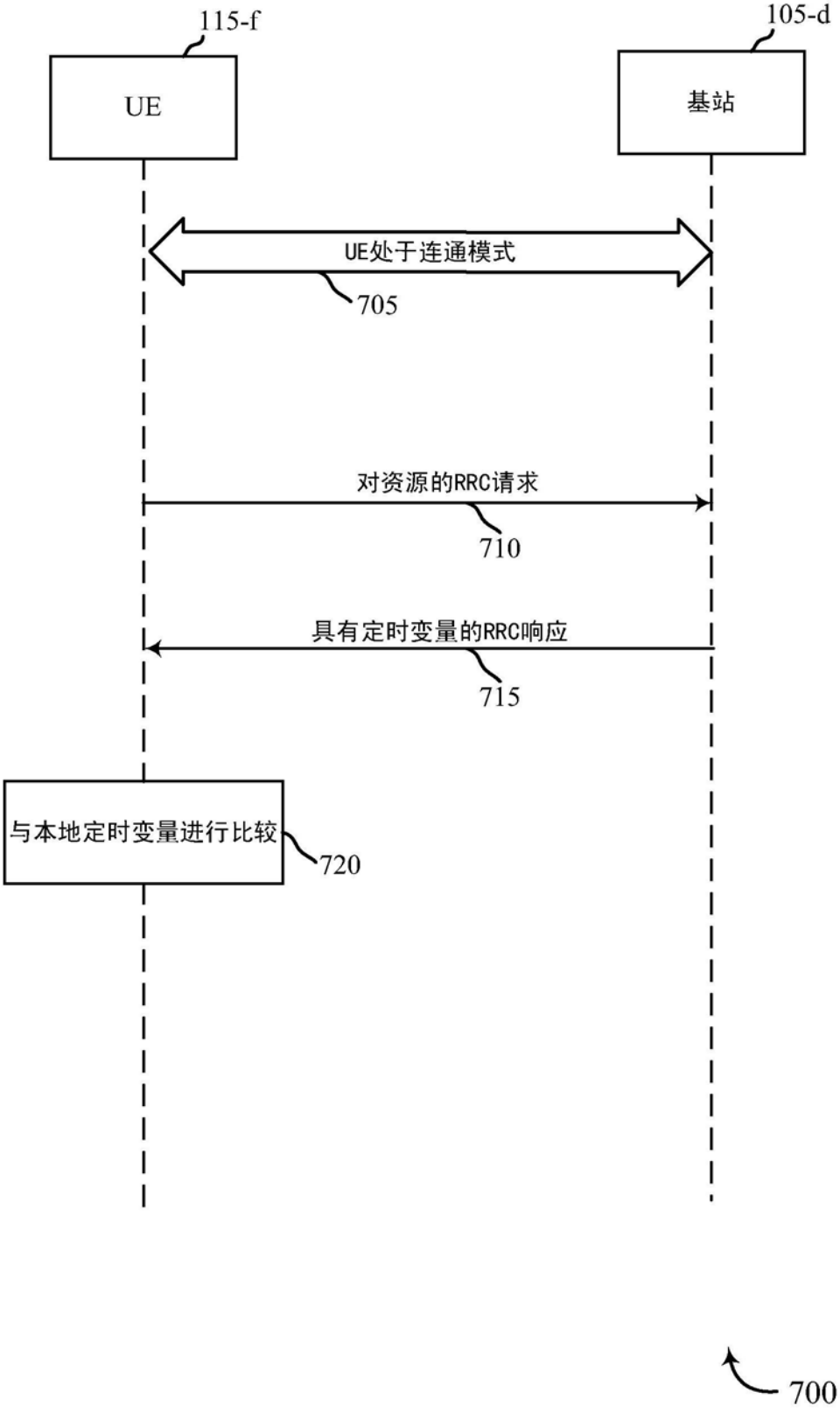

115-f
105-d
UE
基站
UE处于连通模式
705
对资源的RRC请求
710
具有定时变量的RRC响应
715
与本地定时变量进行比较
720
700

图7

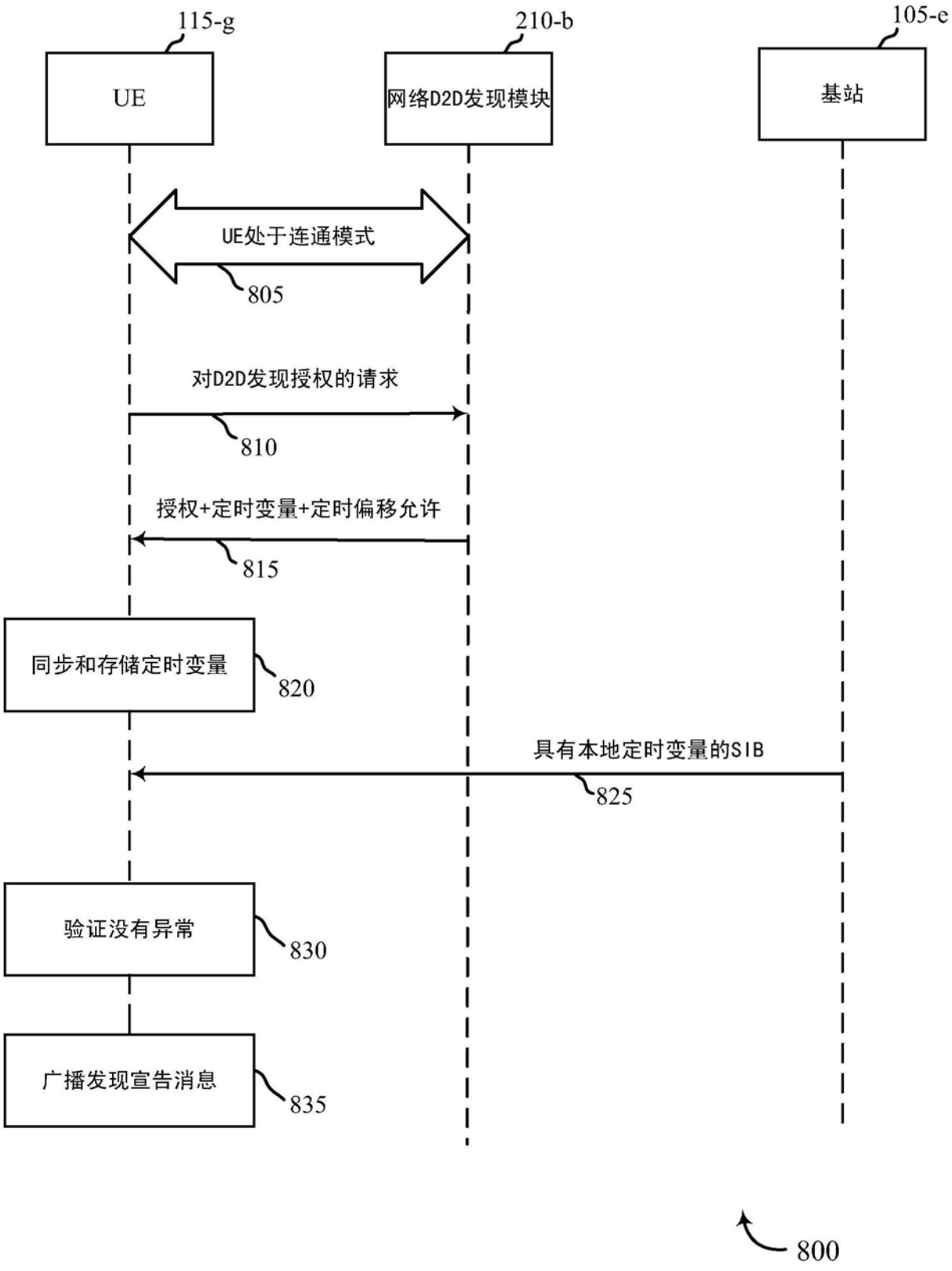

115-g
210-b
105-e
UE
网络D2D发现模块
基站
UE处于连通模式
805
对D2D发现授权的请求
810
授权+定时变量+定时偏移允许
815
同步和存储定时变量
820
具有本地定时变量的SIB
825
验证没有异常
830
广播发现宣告消息
835
800

图8

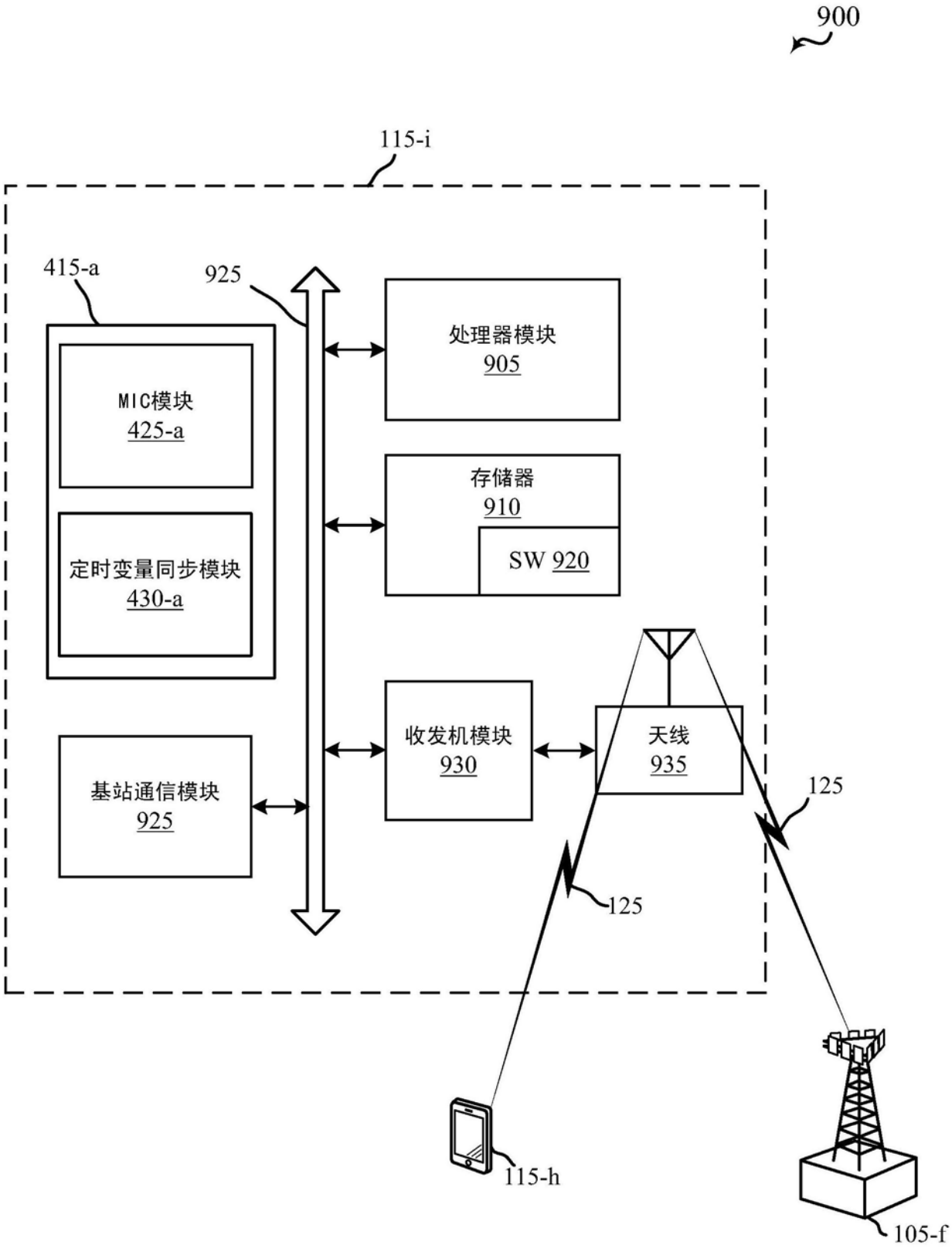

900
115-i
415-a
925
处理器模块
905
MIC模块
425-a
存储器
910
SW 920
定时变量同步模块
430-a
收发机模块
930
天线
935
基站通信模块
925
125
125
115-h
105-f

图9

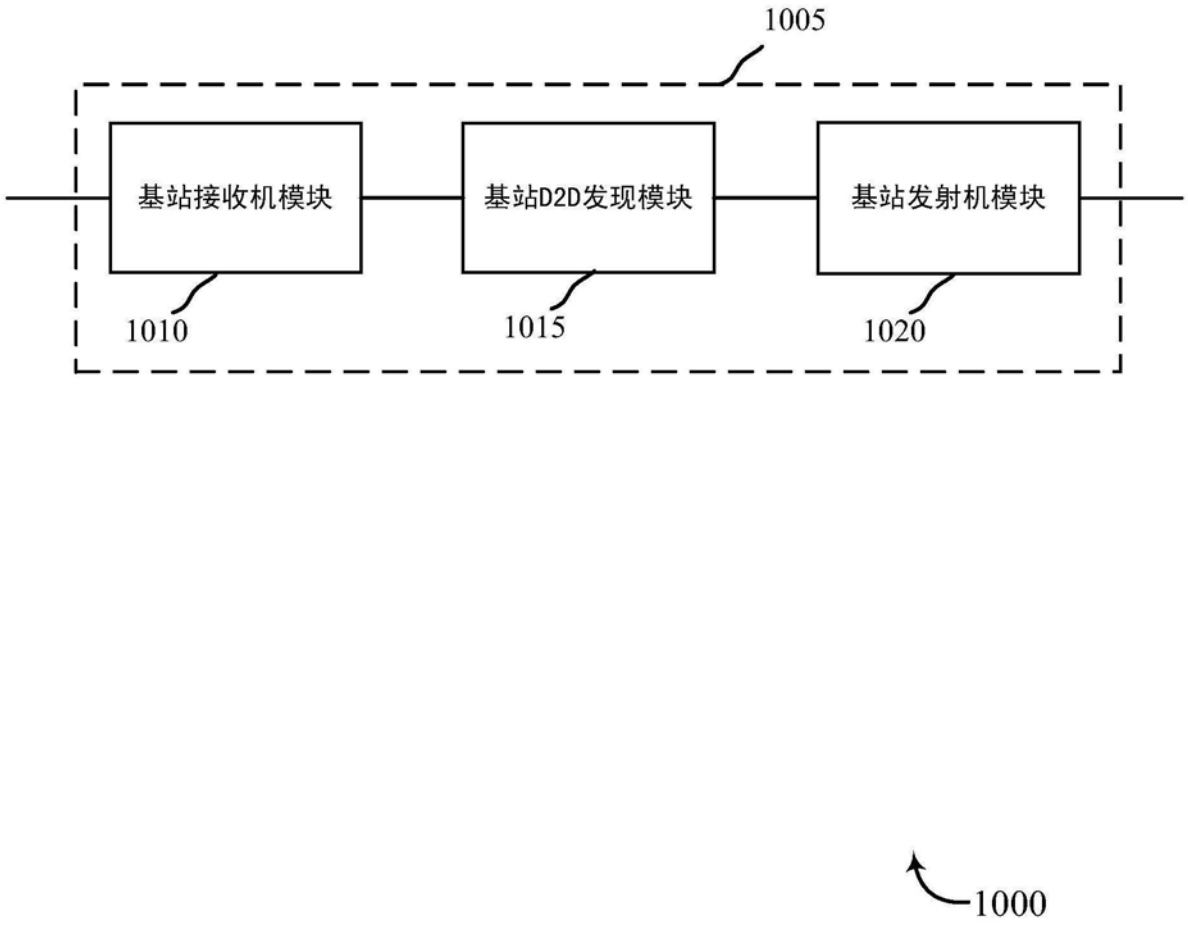


图10

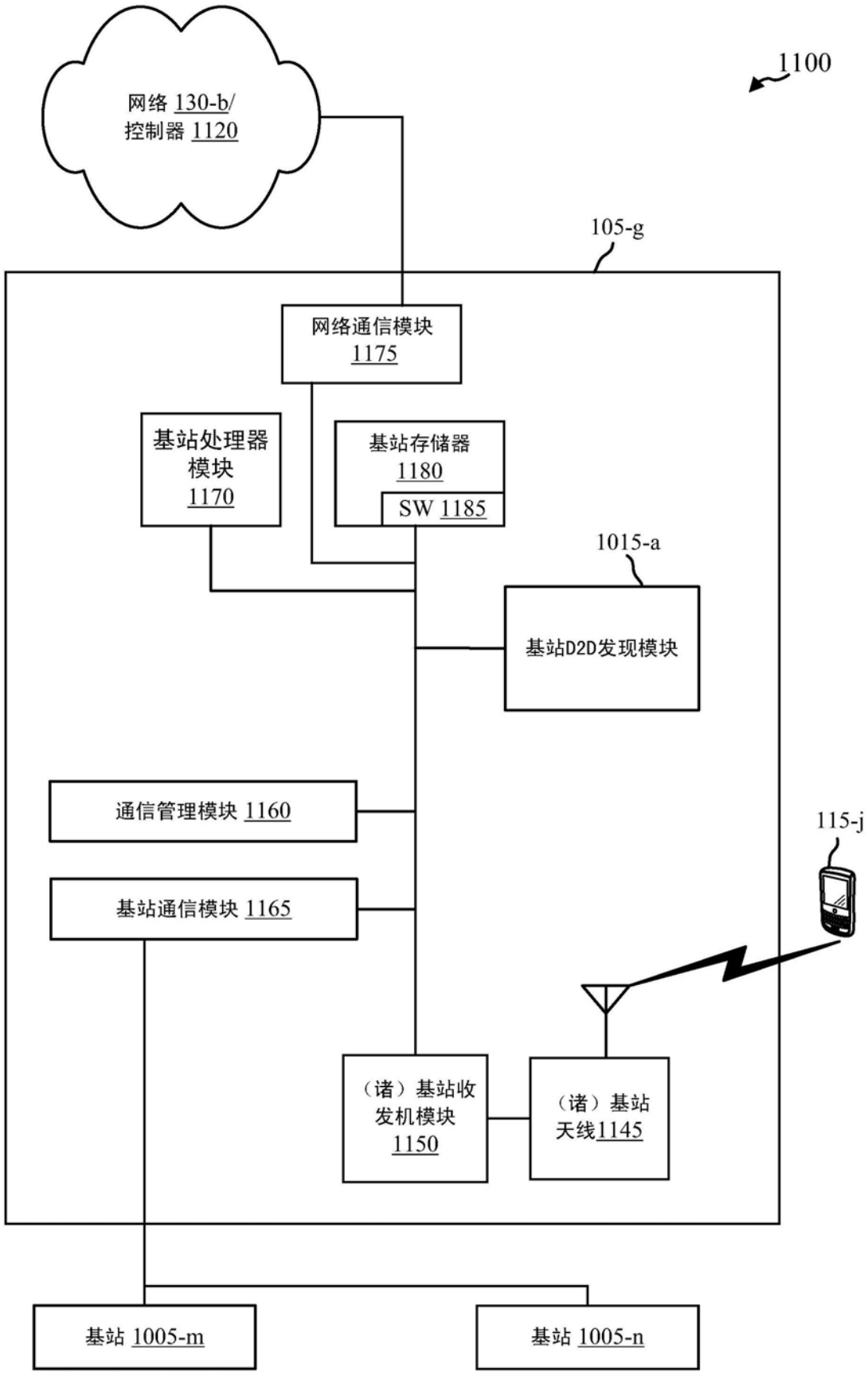

1100
网络 130-b/
控制器 1120
105-g
网络通信模块
1175
基站处理器
模块
1170
基站存储器
1180
SW 1185
1015-a
基站D2D发现模块
通信管理模块 1160
基站通信模块 1165
115-j
（诸）基站收
发机模块
1150
（诸）基站
天线1145
基站 1005-m
基站 1005-n

图11

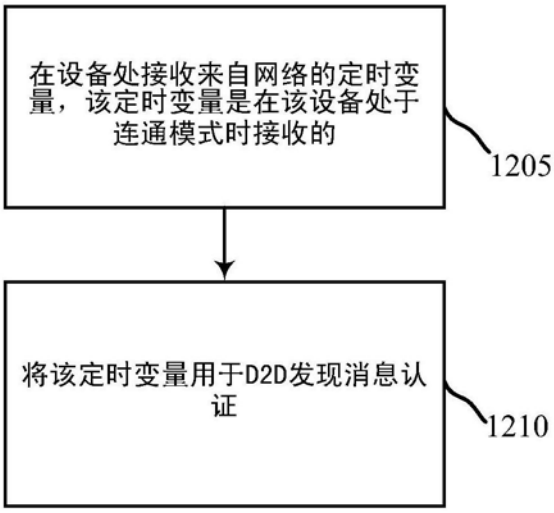

在设备处接收来自网络的定时变量，该定时变量是在该设备处于连通模式时接收的
1205
将该定时变量用于D2D发现消息认证
1210
1200

图12

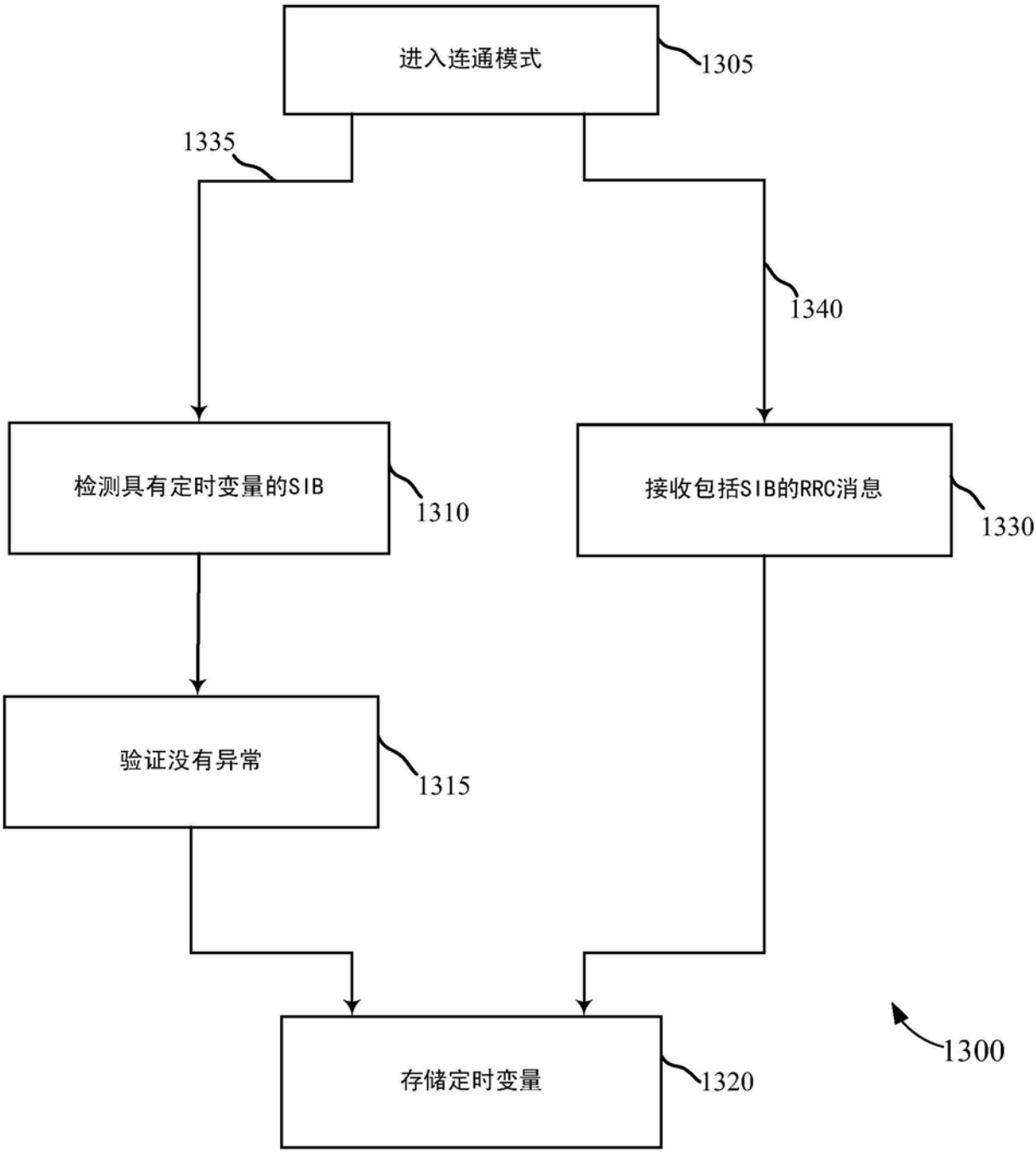

进入连通模式
1305
1335
1340
检测具有定时变量的SIB
1310
接收包括SIB的RRC消息
1330
验证没有异常
1315
存储定时变量
1320
1300

图13

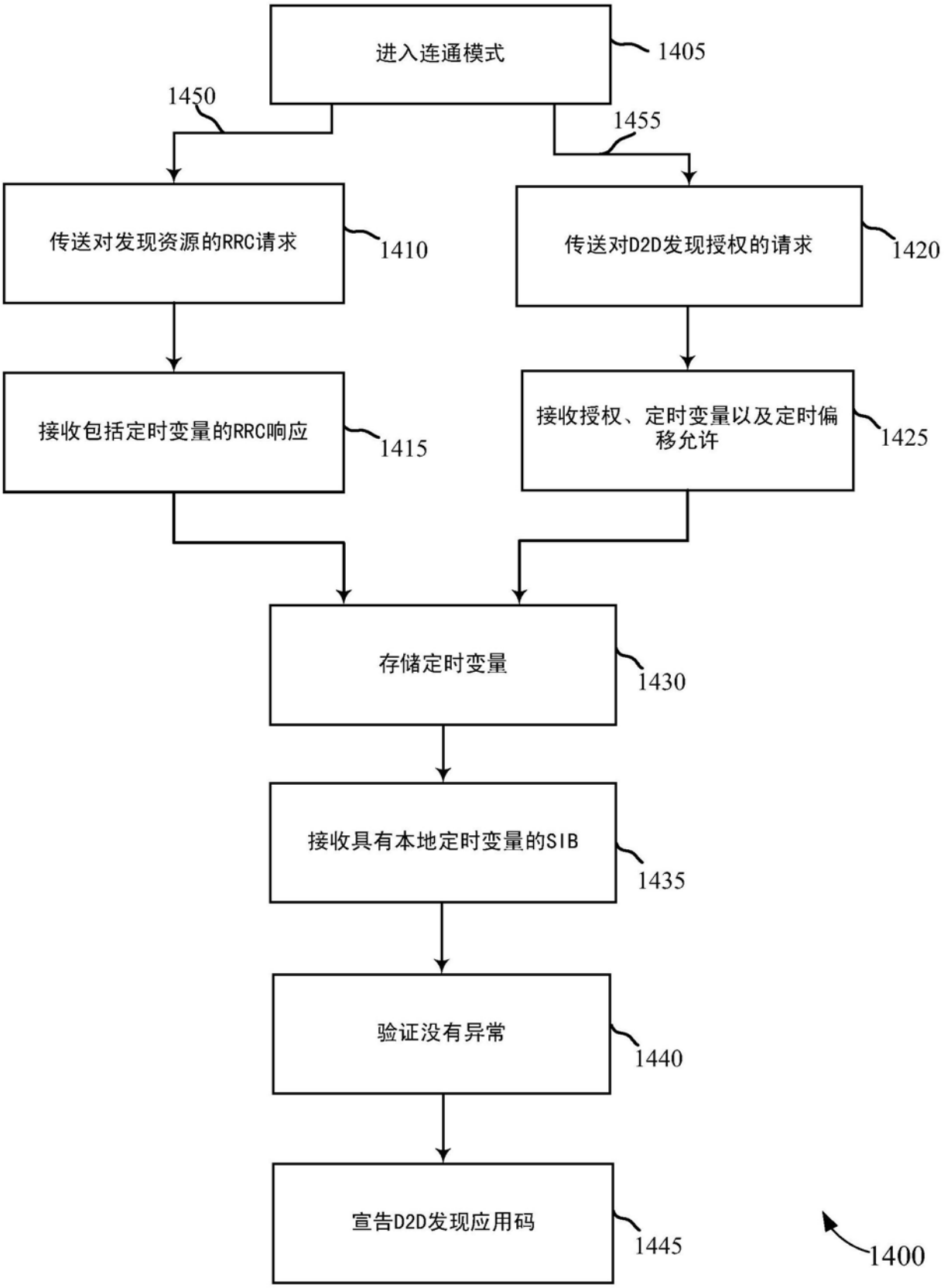

进入连通模式
1405
1450
1455
传送对发现资源的RRC请求
1410
传送对D2D发现授权的请求
1420
接收包括定时变量的RRC响应
1415
接收授权、定时变量以及定时偏移允许
1425
存储定时变量
1430
接收具有本地定时变量的SIB
1435
验证没有异常
1440
宣告D2D发现应用码
1445
1400

图14

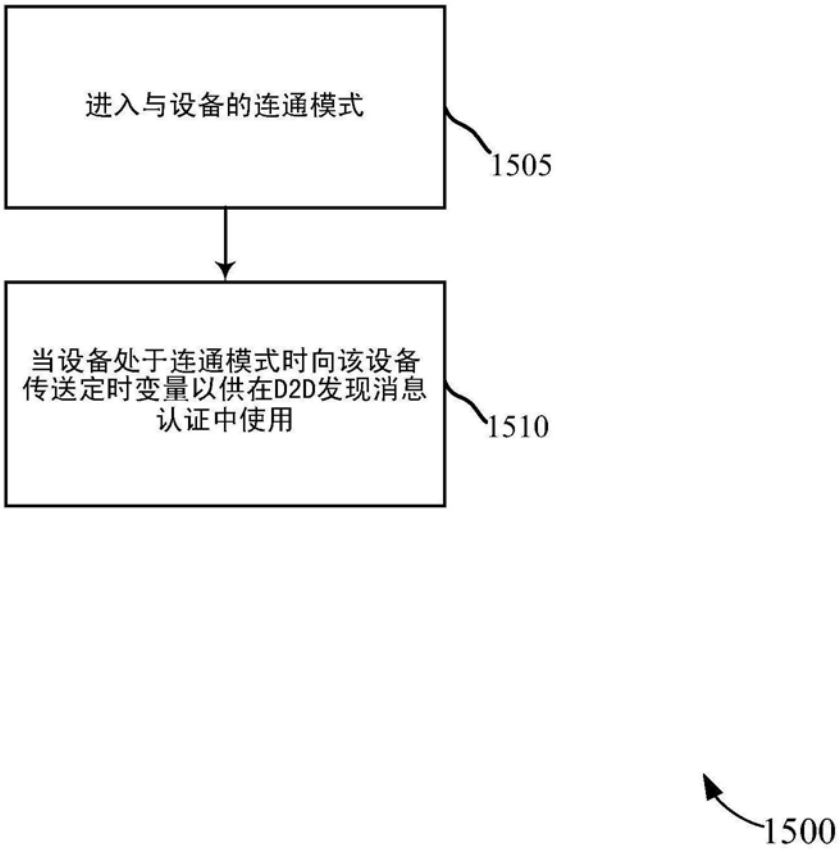

进入与设备的连通模式
1505
当设备处于连通模式时向该设备传送定时变量以供在D2D发现消息认证中使用
1510
1500

图15

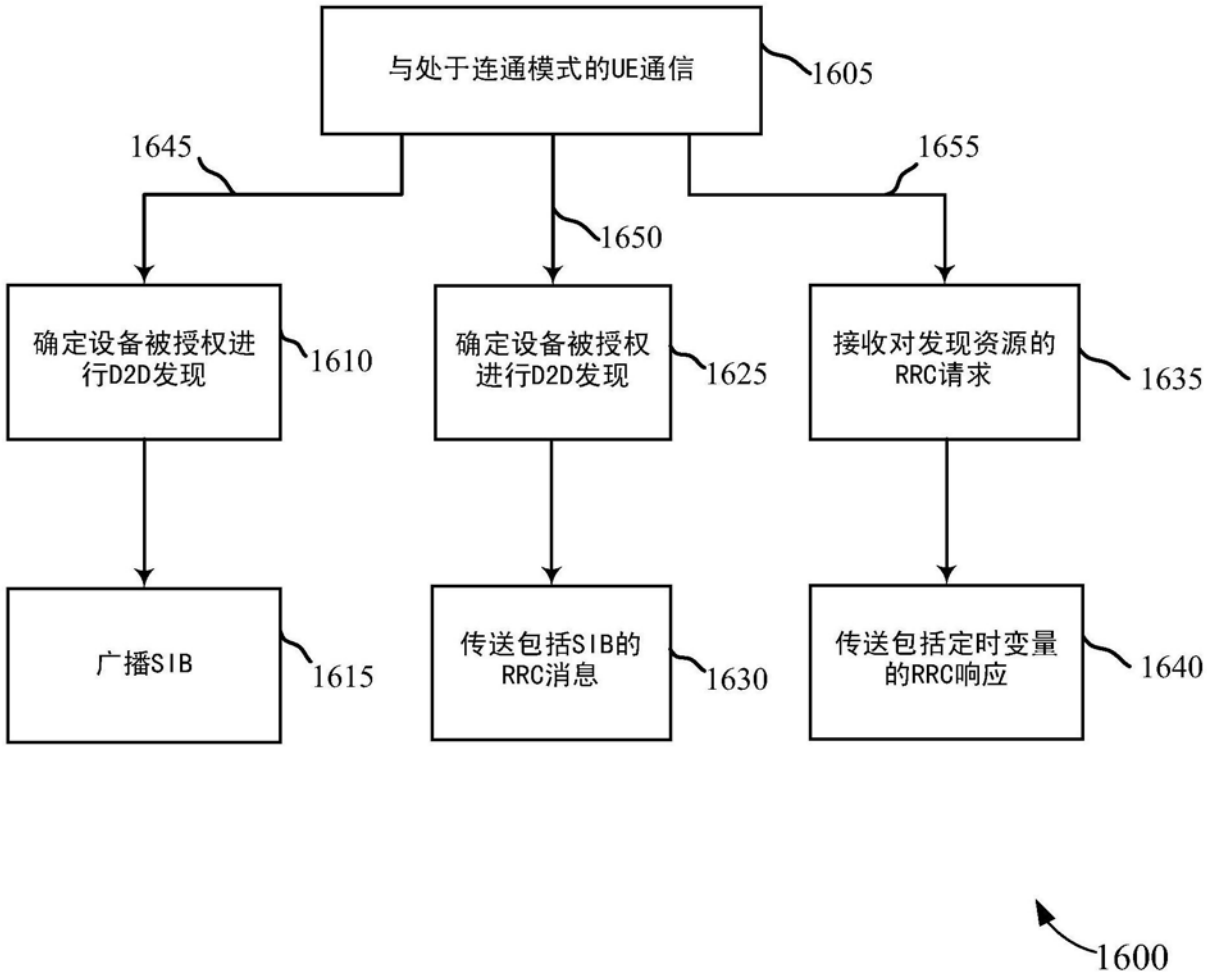

与处于连通模式的UE通信
1605
1645
1650
1655
确定设备被授权进行D2D发现
1610
确定设备被授权进行D2D发现
1625
接收对发现资源的RRC请求
1635
广播SIB
1615
传送包括SIB的RRC消息
1630
传送包括定时变量的RRC响应
1640
1600

图16

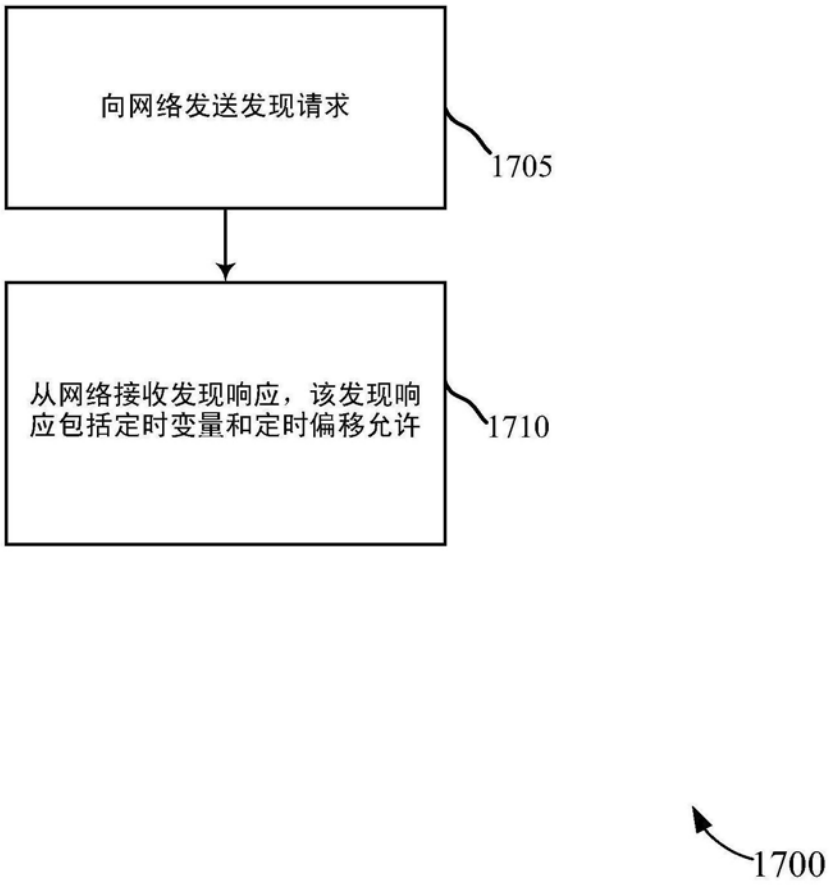


图17

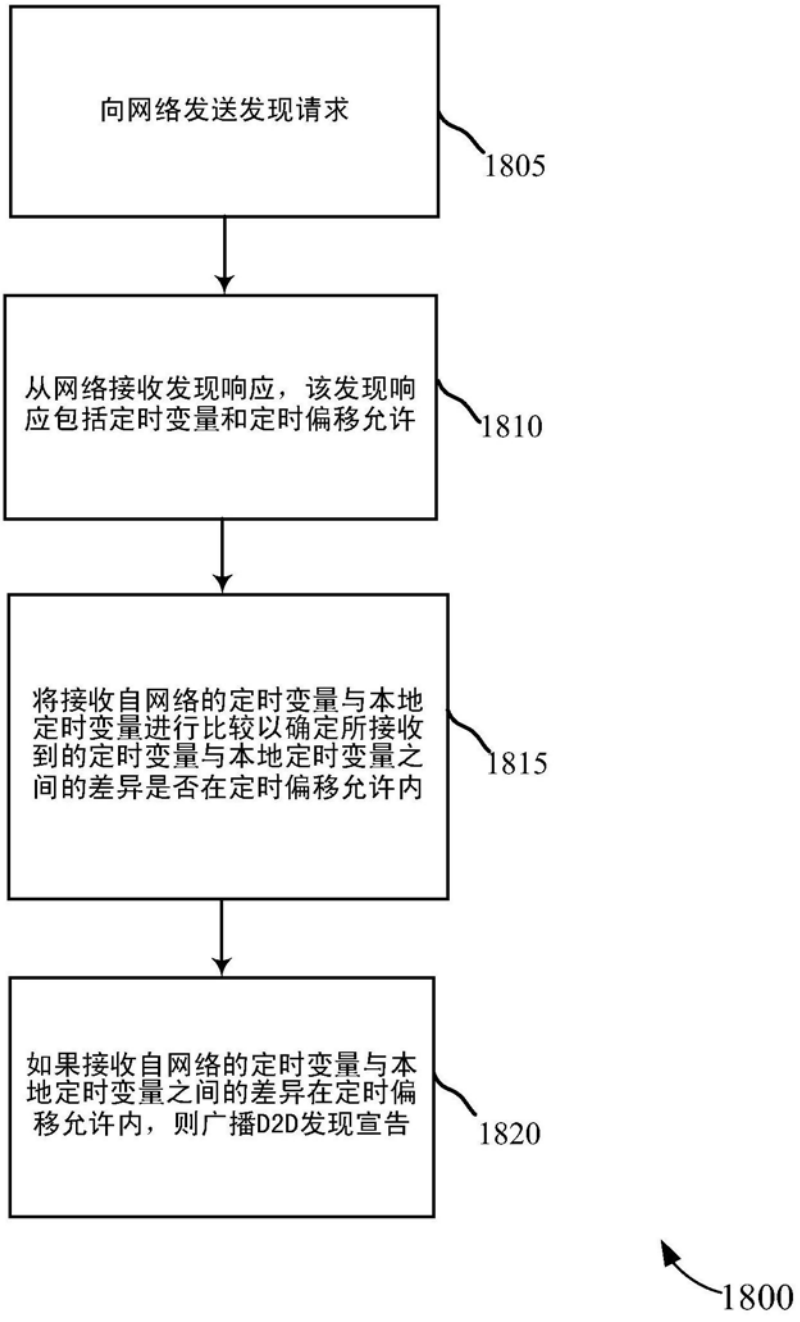

向网络发送发现请求
1805
从网络接收发现响应，该发现响应包括定时变量和定时偏移允许
1810
将接收自网络的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否在定时偏移允许内
1815
如果接收自网络的定时变量与本地定时变量之间的差异在定时偏移允许内，则广播D2D发现宣告
1820
1800

图18

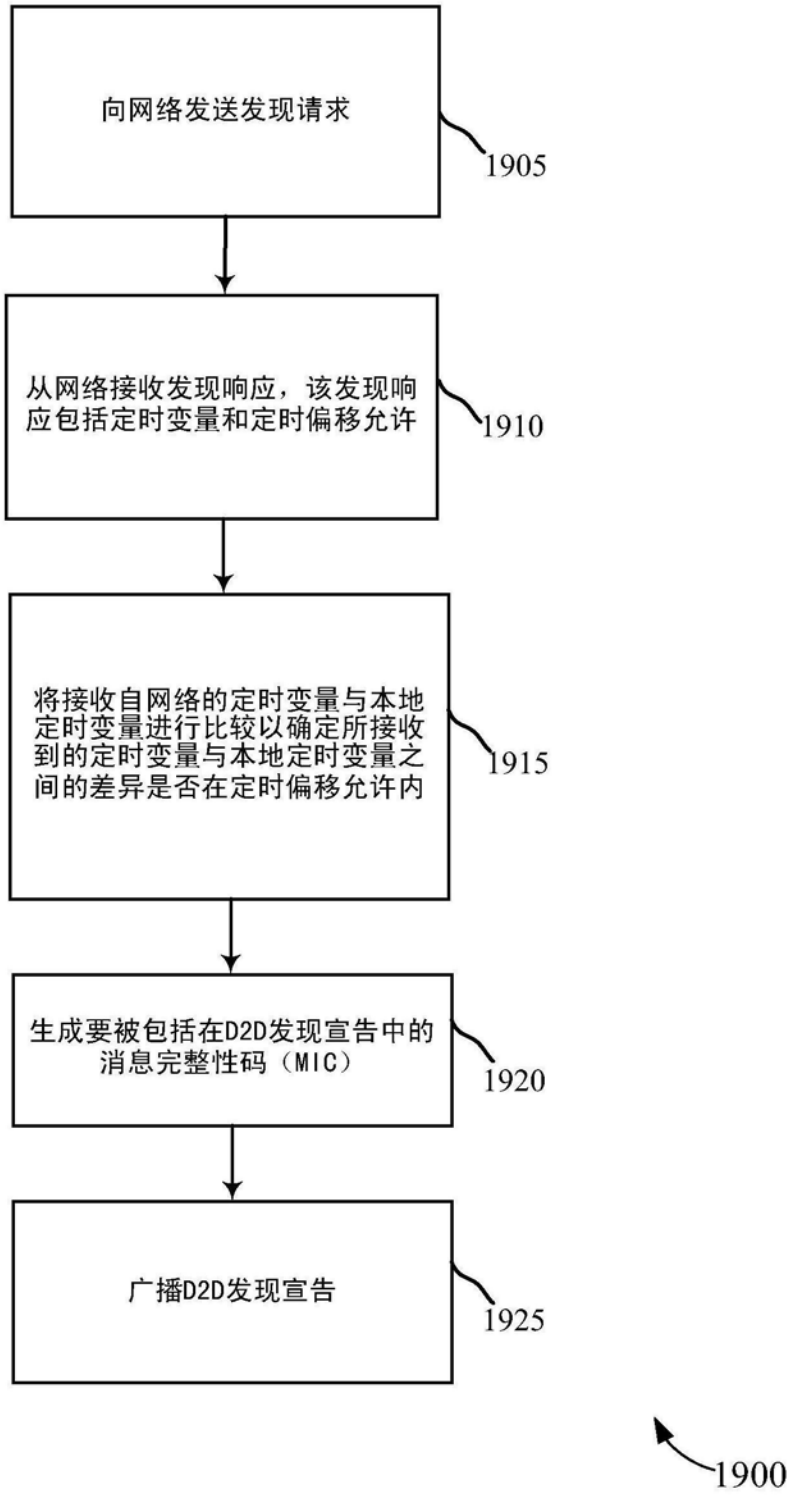

向网络发送发现请求
1905
从网络接收发现响应，该发现响应包括定时变量和定时偏移允许
1910
将接收自网络的定时变量与本地定时变量进行比较以确定所接收到的定时变量与本地定时变量之间的差异是否在定时偏移允许内
1915
生成要被包括在D2D发现宣告中的消息完整性码（MIC）
1920
广播D2D发现宣告
1925
1900

图19

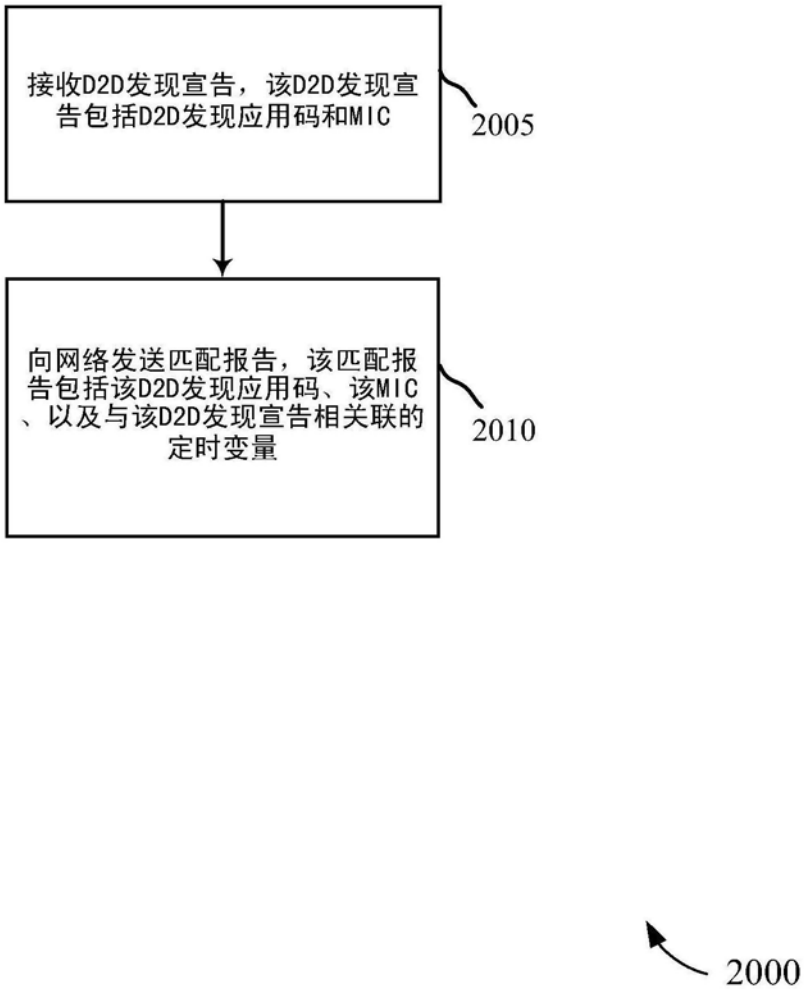

接收D2D发现宣告，该D2D发现宣告包括D2D发现应用码和MIC
2005
向网络发送匹配报告，该匹配报告包括该D2D发现应用码、该MIC、以及与该D2D发现宣告相关联的定时变量
2010
2000

图20

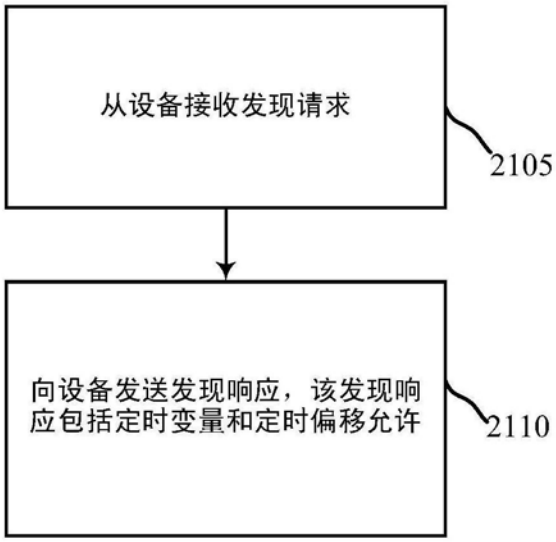


图21

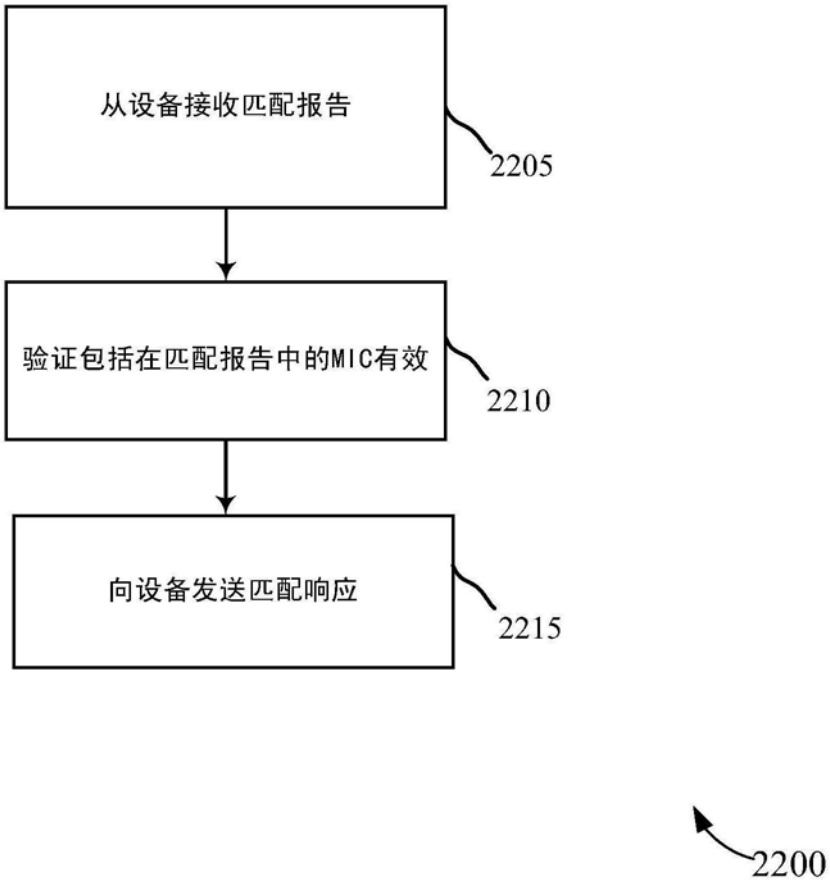

从设备接收匹配报告
2205
验证包括在匹配报告中的MIC有效
2210
向设备发送匹配响应
2215
2200

图22