(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 108432206 B
(45)授权公告日 2021.04.27

(21)申请号 201680075922.6
(22)申请日 2016.12.14
(65)同一申请的已公布的文献号
申请公布号 CN 108432206 A
(43)申请公布日 2018.08.21
(30)优先权数据
62/387,499 2015.12.23 US
15/199,924 2016.06.30 US
(85)PCT国际申请进入国家阶段日
2018.06.22
(86)PCT国际申请的申请数据
PCT/US2016/066702 2016.12.14
(87)PCT国际申请的公布数据
WO2017/112491 EN 2017.06.29
(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 S·B·李 A·帕拉尼格朗德
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 陈炜
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/0433(2021.01)
H04W 12/041(2021.01)
H04W 12/106(2021.01)
H04W 4/70(2018.01)
H04L 29/08(2006.01) (续)

(56)对比文件
US 8660270 B2,2014.02.25
CN 104322089 A,2015.01.28
US 2010146274 A1,2010.06.10
WO 2014205697 A1,2014.12.31
CN 101656956 A,2010.02.24
CN 101945387 A,2011.01.12
WO 2015015714 A1,2015.02.05
US 2008298595 A1,2008.12.04
Samsung."Security aspects of connectionless Data Transmission".《3GPP TSG SA WG3 (Security) Meeting #72》.2013,
Steve Babbage."LS on new security work item for NB-IoT".《3GPP TSG SA WG3 (Security) Meeting #81》.2015,

审查员 齐丽静

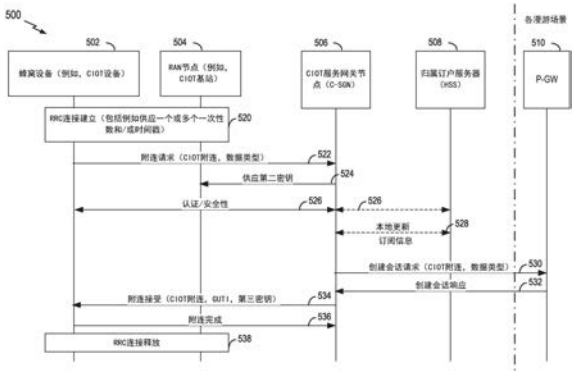
权利要求书5页 说明书27页 附图15页

(54)发明名称

用于蜂窝物联网的无状态接入阶层安全性

(57)摘要

描述了安全方案(例如,完整性保护、加密、或二者)的各方面。可以实现接入阶层安全性的措施,而无需蜂窝物联网(C-IoT)基站(C-BS)处的与建立和/或维护每蜂窝设备接入阶层安全性上下文相关联的开销。网关(例如,CIoT服务网关节点(C-SGN))可以导出第一密钥。该第一密钥可以是仅对该C-SGN网关已知的。该C-SGN可以从该第一密钥和对于该C-BS而言独有的参数导出第二密钥。该C-SGN还可以从该第二密钥和蜂窝设备的身份导出第三密钥。该C-SGN可以将该第二密钥和该第三密钥分别发送到该C-BS和该蜂窝设备。由该蜂窝设备加密和/或完整性保护的小数据消息可以由该C-BS解密和/或验证。



CN 108432206 B

[转续页]

[接上页]

(51)Int.Cl.

H04L 12/24(2006.01)

H04L 9/08(2006.01)

1.一种用于保护小数据消息的方法,包括:

在网络节点处获得第一密钥;

在所述网络节点处获得第二密钥,所述第二密钥基于所述第一密钥以及对于无线电接入网RAN节点而言独有的参数,所述RAN节点与所述网络节点分开;

由所述网络节点将所述第二密钥供应给所述RAN节点;

在所述网络节点处获得第三密钥,所述第三密钥基于所述第二密钥和对于蜂窝设备而言独有的参数;以及

由所述网络节点将所述第三密钥供应给所述蜂窝设备,

其中,所述小数据消息是使用所述第三密钥在所述蜂窝设备与所述RAN节点之间进行保护的且所述小数据消息是在所述RAN节点使用无状态接入阶层安全性通过所述第二密钥和所述小数据消息中包括的对于所述蜂窝设备而言独有的参数来验证后由所述网络节点从所述RAN节点接收的。

2.如权利要求1所述的方法,其中,所述网络节点是蜂窝物联网服务网关节点(C-SGN)。

3.如权利要求1所述的方法,其中,所述第一密钥不是从任何其他密钥获得的或所述第一密钥是在所述网络节点处随机生成的或所述第一密钥不是从任何其他密钥获得的而是在所述网络节点处随机生成的。

4.如权利要求1所述的方法,其中,所述RAN节点是蜂窝物联网(CIoT)基站C-BS或演进型B节点(eNodeB),并且其中对于所述RAN节点而言独有的所述参数是C-BS身份或演进型B节点身份。

5.如权利要求1所述的方法,其中,所述第二密钥在非接入阶层NAS消息中被供应给所述RAN节点。

6.如权利要求1所述的方法,其中,所述第三密钥在非接入阶层NAS消息中被供应给所述蜂窝设备。

7.如权利要求6所述的方法,其中,所述NAS消息是安全NAS消息。

8.如权利要求1所述的方法,其中,所述第三密钥作为经加密信息元素IE被供应给所述蜂窝设备。

9.如权利要求8所述的方法,其中,所述IE包括标识用于加密所述IE的算法的算法标识符。

10.一种用于保护小数据消息的通信装置,包括:

通信接口,所述通信接口用于与通信网络的节点通信;

耦合至所述通信接口的处理电路,所述处理电路适配成:

获得第一密钥;

获得第二密钥,所述第二密钥基于所述第一密钥以及对于无线电接入网RAN节点而言独有的参数;

将所述第二密钥供应给所述RAN节点;

获得第三密钥,所述第三密钥基于所述第二密钥和对于蜂窝设备而言独有的参数;以及

将所述第三密钥供应给所述蜂窝设备,

其中,所述小数据消息是使用所述第三密钥在所述蜂窝设备与所述RAN节点之间进行

保护的且所述小数据消息是在所述RAN节点使用无状态接入阶层安全性通过所述第二密钥和所述小数据消息中包括的对于所述蜂窝设备而言独有的参数来验证后由所述网络节点从所述RAN节点接收的。

11.如权利要求10所述的通信装置,其中,所述处理电路被进一步适配成:

在不从任何其他密钥获得所述第一密钥的情况下获得所述第一密钥;或

通过在所述通信装置处随机生成所述第一密钥来获得所述第一密钥;或

在不从任何其他密钥获得所述第一密钥的情形下,通过在所述通信装置处随机生成所述第一密钥来获得所述第一密钥。

12.如权利要求10所述的通信装置,其中,所述处理电路被进一步适配成:

在非接入阶层(NAS)消息中将所述第二密钥供应给所述RAN节点。

13.如权利要求10所述的通信装置,其中,所述处理电路被进一步适配成:

在非接入阶层(NAS)消息中将所述第三密钥供应给所述蜂窝设备。

14.如权利要求10所述的通信装置,其中,所述处理电路被进一步适配成:

在经加密信息元素(IE)中将所述第三密钥供应给所述蜂窝设备。

15.一种用于通信的装置,所述装置是无线电接入网RAN节点,所述装置包括:

通信接口,所述通信接口用于与通信网络的节点通信;

耦合至所述通信接口的处理电路,所述处理电路适配成:

从网络节点获得第二密钥,所述第二密钥基于第一密钥以及对于所述装置而言独有的参数;

从蜂窝设备获得包括所述蜂窝设备的设备身份和第一完整性保护值的小数据消息;

产生基于所述第二密钥和所述小数据消息中包括的所述蜂窝设备的设备身份的第三密钥;

获得基于所述第三密钥的第二完整性保护值;

将所述第一完整性保护值与所述第二完整性保护值进行比较;

如果比较结果指示所述第一完整性保护值不等于所述第二完整性保护值,则丢弃所述小数据消息;以及

如果所述比较结果指示所述第一完整性保护值等于所述第二完整性保护值,则向所述网络节点发送所述小数据消息。

16.如权利要求15所述的装置,其中,所述第一完整性保护值和所述第二完整性保护值是使用至少一个一次性数和/或时间戳来获得的,所述处理电路被进一步适配成:

将第一一次性数和/或所述时间戳供应给由所述设备身份标识的所述蜂窝设备;和/或

从所述蜂窝设备获得第二一次性数。

17.如权利要求16所述的装置,其中,所述处理电路被进一步适配成:

在随机接入过程期间,供应所述第一一次性数和/或所述时间戳并且获得所述第二一次性数。

18.如权利要求15所述的装置,其中,所述小数据消息用所述第三密钥来加密,并且所述处理电路被进一步适配成:

使用所述第三密钥来解密所述小数据消息。

19.如权利要求15所述的装置,其中,所述处理电路被进一步适配成:

监视话务负载值；

检测所述话务负载值超过预定阈值；以及

响应于检测到所述话务负载值超过所述预定阈值，向由所述设备身份标识的所述蜂窝设备发送消息，所述消息请求所述蜂窝设备将所述第一完整性保护值包括在发送到所述装置的下一个或多个消息中。

20.如权利要求19所述的装置，其中，网络配置所述预定阈值。

21.如权利要求15所述的装置，其中，所述网络节点是网关。

22.如权利要求21所述的装置，其中，所述网关是蜂窝物联网服务网关节点(C-SGN)。

23.如权利要求15所述的装置，其中，所述装置是蜂窝物联网(CIoT)基站C-BS或演进型B节点(eNodeB)，并且其中对于所述装置而言独有的所述参数是C-BS身份或演进型B节点身份。

24.如权利要求15所述的装置，其中，所述处理电路被进一步适配成：

使用至少一个一次性数和/或时间戳来获得所述第一完整性保护值和所述第二完整性保护值。

25.如权利要求15所述的装置，其特征于，所述处理电路被进一步适配成：

在与所述蜂窝设备的初始附连过程期间协商接入阶层安全性配置，其中所述接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、或具有按需完整性保护的情况下是否从所述蜂窝设备发送小数据消息，其中完整性保护和加密使用所述第三密钥来执行。

26.一种装置处用于通信的方法，所述装置是无线电接入网RAN节点，所述方法包括：

从网络节点获得第二密钥，所述第二密钥基于第一密钥以及对于所述装置而言独有的参数；

从蜂窝设备获得包括设备身份和第一完整性保护值的小数据消息；

产生基于所述第二密钥和所述小数据消息中包括的所述蜂窝设备的设备身份的第三密钥；

获得基于所述第三密钥的第二完整性保护值；

将所述第一完整性保护值与所述第二完整性保护值进行比较；

如果比较结果指示所述第一完整性保护值不等于所述第二完整性保护值，则丢弃所述小数据消息；以及

如果所述比较结果指示所述第一完整性保护值等于所述第二完整性保护值，则向所述网络节点发送所述小数据消息。

27.如权利要求26所述的方法，其中，所述第一完整性保护值和所述第二完整性保护值是使用至少一个一次性数和/或时间戳来获得的，所述方法进一步包括：

将第一一次性数和/或所述时间戳供应给由所述设备身份标识的所述蜂窝设备；和/或

从所述蜂窝设备获得第二一次性数。

28.如权利要求27所述的方法，其进一步包括：

在随机接入过程期间，供应所述第一一次性数和/或所述时间戳并且获得所述第二一次性数。

29.如权利要求26所述的方法，其中，所述小数据消息用所述第三密钥来加密，所述方

法进一步包括：

使用所述第三密钥来解密所述小数据消息。

30.如权利要求26所述的方法，所述方法进一步包括：

监视话务负载值；

检测所述话务负载值超过预定阈值；以及

响应于检测到所述话务负载值超过所述预定阈值，向由所述设备身份标识的所述蜂窝设备发送消息，所述消息请求所述蜂窝设备将所述第一完整性保护值包括在发送到所述装置的下一个或多个消息中。

31.如权利要求30所述的方法，其中，网络配置所述预定阈值。

32.如权利要求31所述的方法，其中，所述网络节点是网关。

33.如权利要求32所述的方法，其中，所述网关是蜂窝物联网服务网关节点(C-SGN)。

34.如权利要求26所述的方法，其中，所述装置是蜂窝物联网(CIoT)基站C-BS或演进型B节点(eNodeB)，并且其中对于所述装置而言独有的所述参数是C-BS身份或演进型B节点身份。

35.如权利要求26所述的方法，其进一步包括：

使用至少一个一次性数和/或时间戳来获得所述第一完整性保护值和所述第二完整性保护值。

36.如权利要求26所述的方法，其进一步包括：

在与所述蜂窝设备的初始附连过程期间协商接入阶层安全性配置，其中所述接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、或具有按需完整性保护的情况下是否从所述蜂窝设备发送小数据消息，其中完整性保护和加密使用所述第三密钥来执行。

37.一种用于通信的装置，包括：

通信接口，所述通信接口用于与通信网络的各节点通信；

耦合至所述通信接口的处理电路，所述处理电路适配成：

从与所述装置分开的网络节点通过安全非接入阶层NAS消息获得第三密钥，所述第三密钥基于第二密钥以及对于所述装置而言独有的参数，其中，所述第二密钥基于第一密钥以及对于无线电接入网RAN节点而言独有的参数；

与所述RAN节点协商接入阶层安全性配置；

使用所述第三密钥基于所述接入阶层安全性配置在所述装置和所述RAN节点之间保护小数据消息；以及

向所述RAN节点发送使用所述第三密钥来保护的所述小数据消息。

38.如权利要求37所述的装置，其中，所述第一密钥对所述装置未知，对所述网络节点已知。

39.如权利要求37所述的装置，其中，所述处理电路被进一步适配成：

在初始附连过程期间协商所述接入阶层安全性配置。

40.如权利要求37所述的装置，其中，所述接入阶层安全性配置是在与所述RAN节点的初始附连过程期间协商的，其中所述接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、或具有按需完整性保护的情况下是否从所述装置

发送小数据消息,其中完整性保护和加密使用所述第三密钥来执行。

41.一种在装置处执行的方法,包括:

从与所述装置分开的网络节点通过安全非接入阶层NAS消息获得第三密钥,所述第三密钥基于第二密钥以及对于所述装置而言独有的参数,其中,所述第二密钥基于第一密钥以及对于无线电接入网RAN节点而言独有的参数;

与所述RAN节点协商接入阶层安全性配置;

使用所述第三密钥基于所述接入阶层安全性配置来保护小数据消息;以及

向所述RAN节点发送使用所述第三密钥保护的所述小数据消息。

42.如权利要求41所述的方法,其中,所述第一密钥对所述装置未知,对所述网络节点已知。

43.如权利要求41所述的方法,其进一步包括:

在初始附连过程期间协商所述接入阶层安全性配置。

44.如权利要求41所述的方法,其中,所述接入阶层安全性配置是在与所述RAN节点的初始附连过程期间协商的,其中所述接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、或具有按需完整性保护的情况下是否从所述装置发送小数据消息,其中完整性保护和加密使用所述第三密钥来执行。

用于蜂窝物联网的无状态接入阶层安全性

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年12月23日在美国专利商标局提交的临时申请No.62/387,499以及于2016年6月30日在美国专利商标局提交的非临时申请No.15/199,924的优先权和权益,该申请的全部内容通过援引如同在下文全面阐述那样且出于所有适用目的被纳入于此。

[0003] 引言

[0004] 本公开的各方面一般涉及无线通信,并且尤其但不排他地涉及以无状态方式达成用于蜂窝物联网(CIoT)消息的接入阶层安全性的技术。

[0005] 国际电信联盟(ITU)将物联网(IoT)描述为基于可互操作的信息和通信技术来连接物理和虚拟物体的基础设施。如本文使用的,并且在IoT的上下文中,“物体”是能够被标识和集成到通信网络中的、物理世界中的对象(例如,物理物体)或信息世界中的对象(例如,虚拟物体)。ITU-T Y.2060建议书。诸如无线广域网(WWAN)和/或无线局域网(无线LAN)之类的无线通信网络是可与IoT设备互操作的信息和通信技术。

[0006] 根据长期演进(LTE)范例,为无线电连接定义了两种模式:连接模式;以及空闲模式。在连接模式中,蜂窝设备正在发送和接收数据。在连接模式中建立用户装备(UE)上下文(“UE上下文”)或“无线电资源控制(RRC)连接”。对于UE上下文,建立无线电承载以在蜂窝设备与核心网(例如,演进型分组核心(EPC))之间中继数据。被称为演进型无线电接入承载(eRAB)的无线电承载包括无线电承载部分和S1承载部分。通过LTE-Uu参考点在蜂窝设备与演进型B节点(eNodeB)之间建立无线电承载。通过S1参考点在演进型B节点与服务网关(S-GW)之间建立S1承载。建立安全性上下文以使通信安全。

[0007] 在空闲模式中,eRAB承载(无线电承载和S1承载)被释放并且安全性上下文被丢弃。以此方式,释放了不必要的无线电资源。无线电承载和安全性上下文仅在存在要发送/接收的数据时(即,在连接模式中)才被建立和维护。当蜂窝设备苏醒(例如,从空闲模式)时,演进型B节点经由对移动性管理实体(MME)的服务请求来建立新的UE上下文和安全性上下文并且进入连接模式。当蜂窝设备变得空闲时,演进型B节点移除UE上下文(例如,eRAB承载)和安全性上下文,并且进入空闲模式。

[0008] 对于蜂窝物联网(CIoT)设备和支持CIoT设备的网络,LTE移动性管理和会话管理规程可能在例如能耗方面引发显著开销,因为用于建立UE上下文的信令延迟将延长CIoT设备苏醒时段。开销导致等待时间增加,这也是不期望的。

[0009] 为了减小开销和等待时间,已经提出了与对于通过蜂窝设备的其他通信的要求相比,对于CIoT的移动性管理和安全性功能的不同要求。这些不同要求可以减小与在蜂窝网络中操作的IoT设备的移动性管理和安全性功能有关的开销。然而,这些不同要求可能使无线电接入网(RAN)节点和核心网节点具有不期望的弱点,诸如举例而言拒绝服务(DoS)和/或分组洪泛攻击。因此,找到在不增大开销和等待时间的情况下克服或防止这些不期望的弱点的方法是期望的。

[0010] 概述

[0011] 以下给出本公开的一些方面的简要概述以提供对这些方面的基本理解。此概述不是本公开的所有构想到的特征的详尽综览，并且既非旨在标识出本公开的所有方面的关键性或决定性要素亦非试图界定本公开的任何或所有方面的范围。其唯一目的是要以简化形式给出本公开的一些方面的各种概念以作为稍后给出的更详细描述之序。

[0012] 在一些实现中，一种通信方法可包括在网关处导出可仅对该网关已知的第一密钥。该网关还可以导出第二密钥，该第二密钥可基于该第一密钥和可对于无线电接入网(RAN)的节点而言独有的参数。该网关可以将该第二密钥发送到该RAN的节点。该网关也可以导出第三密钥。该第三密钥可基于该第二密钥和可对于蜂窝设备而言独有的参数。该网关可随后将该第三密钥发送到该蜂窝设备。

[0013] 在一些实现中，一种通信装置可包括：可以与通信网络的各节点通信的通信接口，以及可以耦合至该通信接口的处理电路。处理电路可以被构造、适配、和/或配置成导出可仅对该通信装置已知的第一密钥。该处理电路还可以导出第二密钥，该第二密钥可基于该第一密钥和可对于无线电接入网(RAN)的节点而言独有的参数。该处理电路可使得该通信装置将该第二密钥发送到该RAN的节点。该处理电路还可以导出第三密钥，该第三密钥可基于该第二密钥和对于蜂窝设备而言独有的参数。该处理电路可使得该通信装置将该第三密钥发送到该蜂窝设备。

[0014] 在一些实现中，一种完整性保护通信的方法可包括在无线电接入网(RAN)节点处接收第二密钥。该第二密钥可以基于第一密钥和对于该RAN节点而言独有的参数。该方法还可包括：在该RAN节点处接收包括设备身份和第一完整性保护值(例如，归属于消息认证码(MAC)或令牌的值)的小数据消息。该RAN节点可以导出第三密钥，该第三密钥可以基于第二密钥和该设备身份。该RAN节点可以随后使用该第三密钥来导出第二完整性保护值。可以进行该第一完整性保护值与该第二完整性保护值的比较。如果该比较的结果指示该第一完整性保护值和该第二完整性保护值不相等，则该RAN节点可丢弃该小数据消息。然而，如果该比较的结果指示该第一完整性保护值和该第二完整性保护值相等，则该RAN节点可将该小数据消息发送到网关。

[0015] 在一些实现中，可以实践一种无状态接入阶层安全性的方法。该方法可包括在无线电接入网(RAN)节点处接收第二密钥。该第二密钥可以基于第一密钥和对于该RAN节点而言独有的参数。该RAN节点可以接收包括设备身份的经加密小数据消息。该小数据消息可以用第三密钥来加密。该RAN节点可以导出该第三密钥，该第三密钥可以基于该第二密钥和该设备身份。该RAN节点可以随后使用该第三密钥来解密该小数据消息。

[0016] 在一些实现中，可以实践另一种无状态接入阶层安全性的方法。该方法可包括在无线电接入网(RAN)节点处接收第二密钥。该第二密钥可以基于第一密钥和对于该RAN节点而言独有的参数。该RAN节点可以接收包括设备身份的小数据消息。该小数据消息可以使用第三密钥来加密，并且该小数据消息可包括完整性保护值，其中使用该第三密钥来实现完整性保护。该RAN节点可以导出该第三密钥，该第三密钥可以基于该第二密钥和该设备身份。该小数据消息可以在该RAN节点处使用该第三密钥来解密。附加地，该完整性保护值可以在该RAN节点处使用该第三密钥来验证。

[0017] 在一些实现中，可以提供一种按需完整性保护的方法。该方法可包括由无线电接入网(RAN)节点监视话务负载值。该RAN节点可以检测该话务负载值超过预定阈值。该RAN节

点响应于检测到话务负载值超过预定阈值而可以向蜂窝设备发送消息。该消息可以请求该蜂窝设备在发送到该RAN节点的下一个或多个消息中包括令牌。

[0018] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。该装置可被用于完整性保护通信。在一些实现中，该处理电路可以被构造、适配、和/或配置成接收第二密钥。该第二密钥可以基于第一密钥和对于该装置而言独有的参数。该处理电路还可接收包括设备身份和第一完整性保护值的小数据消息。该处理电路可导出第三密钥，该第三密钥可以基于第二密钥和该设备身份。该处理电路可随后使用该第三密钥来导出第二完整性保护值。在该处理电路处，可以进行该第一完整性保护值与该第二完整性保护值的比较。如果该比较的结果指示该第一完整性保护值和该第二完整性保护值不相等，则该处理电路可使得该装置丢弃该小数据消息。然而，如果该比较的结果指示该第一完整性保护值和该第二完整性保护值相等，则该处理电路可使得该装置将该小数据消息发送到网关。

[0019] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。该装置可被用于实践无状态接入阶层安全性。在一些实现中，该处理电路可以被构造、适配、和/或配置成接收第二密钥。该第二密钥可以基于第一密钥和对于该装置而言独有的参数。该处理电路还可以接收包括设备身份的经加密小数据消息。在一些实现中，该小数据消息可以用第三密钥来加密。该处理电路可以导出该第三密钥。该第三密钥可以基于该第二密钥和该设备身份。该处理电路可以随后使用该第三密钥来解密该小数据消息。

[0020] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。该装置也可被用于实践无状态接入阶层安全性。在一些实现中，该处理电路可以被构造、适配、和/或配置成接收第二密钥。该第二密钥可以基于第一密钥和对于该装置而言独有的参数。该处理电路还可以接收包括设备身份的小数据消息。该小数据消息可以用第三密钥来加密，并且该小数据消息可包括使用该第三密钥导出的完整性保护值。该处理电路可以导出该第三密钥，该第三密钥可以基于该第二密钥和该设备身份。该处理电路可以使用该第三密钥来解密该小数据消息。该处理电路还可使用该第三密钥来验证该完整性保护值。

[0021] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。该装置可被用于按需完整性保护通信。在一些实现中，该处理电路可以被构造、适配、和/或配置成监视话务负载值。该处理电路可以检测该话务负载值超过预定阈值。响应于检测到话务负载值超过该预定阈值，该处理电路随后可以使得该装置向蜂窝设备发送消息，该消息请求该蜂窝设备将令牌包括在发送到该装置的下一个或多个消息中。

[0022] 在一些实现中，一种通信方法可包括在蜂窝设备处接收第三密钥。该第三密钥可以基于第二密钥和该蜂窝设备的身份，并且该第二密钥可以基于第一密钥和无线电接入网(RAN)节点身份。该方法可进一步包括在初始附连规程期间配置和/或协商安全协议。安全协议可以确定该蜂窝设备是否可以在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、和/或具有按需完整性保护的情况下发送小数据消息。在一些实现中，该完整性保护和加密可以基于该第三密钥。

[0023] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。在一些实现中，该处理电路可以被构造、适配、和/或配置成接收第三密钥。该第三密钥可以基于第二密钥和该装置的身份。该第二密钥可以基于第一密钥和无线电接入网(RAN)节点身份。该处理电路可以被进一步构造、适配、和/或配置成在初始附连规程期间配置和/或协商安全协议。在一些实现中，该安全协议可以确定该装置是否可以在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、和/或具有按需完整性保护的情况下发送小数据消息。在一些实现中，该完整性保护和加密可以基于该第三密钥。

[0024] 在一些实现中，一种装置(诸如通信装置)可包括：用于与通信网络的各节点通信的通信接口，以及耦合至该通信接口的处理电路。该装置也可被用于实践无状态接入阶层安全性。在一些实现中，处理电路可以被构造、适配、和/或配置成：获得基于第二密钥和对于该装置而言独有的参数的第三密钥、协商接入阶层安全性配置、基于该接入阶层安全性配置使用该第三密钥来保护小数据消息、以及发送使用该第三密钥保护的小数据消息。在一些实现中，处理电路可以进一步适配成与RAN节点协商该接入阶层安全性配置，并且将使用该第三密钥保护的小数据消息发送到该RAN节点。在一些实现中，处理电路可被进一步适配成从网关获得该第三密钥，其中该第二密钥基于第一密钥和对于RAN节点而言独有的参数，并且该第一密钥仅对该网关已知。在一些方面，该处理电路可被进一步适配成在初始附连规程期间协商该接入阶层安全性配置。在一些方面，该处理电路可被进一步适配成在与设备的初始附连规程期间协商接入阶层安全性配置，其中该接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、和/或具有按需完整性保护的情况下是否从该设备发送小数据消息，其中完整性保护和加密使用该第三密钥来执行。

[0025] 附图简述

[0026] 在结合附图理解下面阐述的详细描述时，各种特征、本质和优点会变得明显，在附图中，相像的附图标记贯穿始终作相应标识。

[0027] 图1是解说本公开的各方面可在其中找到应用的通信网络的示例的示图。

[0028] 图2是解说本公开的各方面可在其中找到应用的通信网络的另一示例的示图。

[0029] 图3是解说本公开的各方面可在其中找到应用的通信网络的又一示例的示图。

[0030] 图4是解说根据本公开的一些方面的接入阶层安全密钥推导和供应过程的示例的流程图。

[0031] 图5是解说根据本公开的一些方面的蜂窝物联网(CIoT)下的附连规程的相关联的示例的呼叫流程图。

[0032] 图6是解说根据本公开的一些方面的可支持无状态接入阶层安全性以及安全密钥的获得、供应、和使用中的一者或多者的装置的硬件实现的示例的框图。

[0033] 图7是解说根据本公开的一些方面的无状态接入阶层安全性过程的示例的流程图。

[0034] 图8是解说根据本公开的一个或多个方面的可支持无状态接入阶层安全性以及安全密钥的获得、供应、和使用中的一者或多者的装置的硬件实现的另一示例的框图。

[0035] 图9是解说根据本公开的一些方面的无状态接入阶层安全性过程的另一示例的流程图。

[0036] 图10是解说根据本公开的一些方面的无状态接入阶层安全性过程的另一示例的流程图。

[0037] 图11是解说根据本公开的一些方面的无状态接入阶层安全性过程的另一示例的流程图。

[0038] 图12是解说根据本公开的一些方面的无状态接入阶层安全性过程的另一示例的流程图。

[0039] 图13是解说根据本公开的一个或多个方面的可支持无状态接入阶层安全性以及安全密钥的获得、供应、和使用中的一者或多者的装置的硬件实现的另一示例的框图。

[0040] 图14是解说根据本公开的一些方面的无状态接入阶层安全性过程的另一示例的流程图。

[0041] 图15是包括如可出现在本公开的一些方面的多个通信实体的无线通信网络的示意性解说。

[0042] 详细描述

[0043] IoT设备可包括但不限于具有通信能力以及感测、致动、数据捕获、数据存储、和/或数据处理的可任选能力的任何设备。蜂窝设备(例如,芯片组件、无线设备、移动设备、用户装备(UE)、终端)可以与IoT设备对接。对接可被直接达成(例如,IoT设备可集成到蜂窝设备)或者间接达成(例如,IoT设备可以经由诸如蓝牙之类的局域网来与蜂窝设备对接)。为了便于参考,将理解,除非另有说明,否则本文中作出的对蜂窝设备的任何引用都是对与IoT设备(即,CIoT设备)对接的蜂窝设备的引用。

[0044] 如本文所使用的,词语“获得”可以表示导出、生成、计算、检索、接收、请求等,并且可涵盖本地地获得和/或远程地获得。如本文所使用的,词语“获得”可涵盖部分地获得和/或完全地获得。

[0045] 如本文所使用的,短语“在运行中”可以描述可动态地或者按需地发生的动作。

[0046] 概览

[0047] 当UE从空闲模式转换到连接模式时,UE和支持UE的网络传统地建立UE安全性上下文(例如,每蜂窝设备接入阶层(AS)安全性上下文)和eRAB承载。然而,对于蜂窝物联网(CIoT)设备(例如,与IoT设备对接的UE),为了减小开销,各方提出消除接入阶层(AS)安全性上下文的建立并且消除移动性管理。消除移动性管理(例如,消除MME)必需改变网络架构。相应地,CIoT架构引入了被称为CIoT服务网关节点(C-SGN)的新节点。C-SGN将MME中剩余的任何所需功能性与服务网关(S-GW)的功能性相组合。

[0048] 然而,消除CIoT设备的接入阶层(AS)安全性和移动性管理可能使无线电接入网(RAN)节点(例如,eNB)和核心网节点具有不期望的弱点,诸如拒绝服务(DoS)和/或分组洪泛攻击。

[0049] 本公开在一些方面涉及安全性方案(例如,完整性保护、加密、或两者),该安全性方案可以在不建立和/或维护RAN节点处(诸如蜂窝物联网(CIoT)基站(C-BS)处)的每蜂窝设备接入阶层(AS)安全性上下文的情况下达成。可以实现接入阶层安全性的至少一些措施,而无需与建立和/或维护每蜂窝设备接入阶层安全性上下文相关联的开销。

[0050] 网关(例如,C-SGN)可以获得三个密钥。第一密钥不可从任何其他密钥导出,并且该第一密钥可仅对C-SGN已知。例如,第一密钥可以由C-SGN随机生成。第二密钥可以基于第

一密钥和对于无线电接入网(RAN)节点而言独有的参数(例如,eNB或C-BS的身份)(例如,使用第一密钥和该参数来导出、使用第一密钥和该参数来生成)。第三密钥可以基于第二密钥和蜂窝设备的身份。身份可以是例如SAE临时移动订户身份(S-TMSI)。

[0051] C-SGN可以将第二密钥供应(例如,提供、发送、递送)给RAN节点,并将第三密钥供应(例如,提供、发送、递送)给蜂窝设备。例如,可以通过安全NAS消息将第三密钥提供给蜂窝设备。

[0052] 当蜂窝设备发送CIoT消息(称为"小数据消息")时,蜂窝设备可以向CIoT消息添加完整性保护和/或加密。完整性保护和/或加密可以使用第三密钥来执行。如所陈述的,第三密钥可以基于第二密钥和设备的身份(例如,使用第二密钥和设备的身份来导出、生成)。蜂窝设备向RAN节点发送经完整性保护和/或经加密的CIoT消息(例如,小数据消息)。

[0053] 在一些实现中,RAN节点可不建立和/或维护与设备的接入阶层(AS)安全性上下文(例如,UE安全性上下文)。建立和/或维护接入阶层安全性上下文要求使用状态表和处理与状态表相关联的数据;这种开销是不期望的。在一些实现中,RAN节点可以使用RRC信令来将设备配置成启用/禁用用于CIoT消息的接入阶层安全性配置(例如,加密或完整性保护)。接入阶层安全性配置还可以被称为接入阶层安全性保护配置。接入阶层安全性配置可以由RAN节点或由C-SGN在触发事件之际触发。触发事件可包括例如检测臆造的(例如,假的、伪造的、非真正的)分组注入或检测诸如拒绝服务攻击之类的攻击。

[0054] 如在本文所呈现的示例中描述的,当触发或使用接入阶层安全性时,RAN节点可以使用第二密钥(其由C-SGN供应给RAN节点)和蜂窝设备的身份来在运行中获得(例如,导出、生成)第三密钥的副本。蜂窝设备的身份与RAN节点处获得的每个小数据消息包括在一起,并且第二密钥独立于蜂窝设备的身份;相应地,安全性方案是无状态的,因为不需要状态表。使用第三个密钥,RAN节点可以基于配置来对小数据进行验证、解密、或两者。在一个方面,RAN节点可以接收由第三密钥保护(完整性保护和/或加密)的小数据消息,并且随后可以验证小数据消息的完整性保护(即,验证小数据消息发送自从C-SGN获得第三密钥的设备)和/或解密小数据消息。

[0055] 示例性操作环境

[0056] 图1是解说本公开的各方面可在其中找到应用的通信网络100的示例的示图。无线电接入网(RAN)可包括一个或多个网络接入节点(例如,物联网(CIoT)基站(C-BS)、演进型B节点)(被称为RAN节点102)。本文中呈现的技术可被用于向RAN节点102(例如,C-BS、演进型B节点)、蜂窝设备116、122、和/或CIoT设备136、142供应密钥。密钥(例如,密码密钥、数学导出密钥)可被用于完整性保护和/或加密小数据消息。小数据消息的完整性保护和/或加密期望地将接入阶层安全性和保护添加到通信网络100。

[0057] 在图1的示例中,RAN节点102可包括多个天线群:包括天线104和106的一个群、包括天线108和110的另一个群、以及包括天线112和114的附加群。在图1中,对于每个天线群示出了两个天线;然而,对于每个天线群可以利用更多或更少的天线。蜂窝设备116可以与天线112和114处于通信,其中天线112和114在前向链路120(例如,下行链路)上向蜂窝设备116传送信息并且在反向链路118(例如,上行链路)上从蜂窝设备116接收信息。蜂窝设备122可以与天线104和106处于通信,其中天线104和106在前向链路126上向蜂窝设备122传送信息并且在反向链路124上从蜂窝设备122接收信息。RAN节点102也可以与其他蜂窝设备

处于通信，其他蜂窝设备可以例如与物联网(IoT)设备对接。例如，IoT设备150可以与蜂窝设备116处于通信，其中可以在前向链路121上向IoT设备150传送信息，并且可以在反向链路119上从IoT设备150向蜂窝设备116发送信息。与IoT设备(统称为蜂窝物联网设备(CIoT)设备136或CIoT设备136)(例如，直接或间接)对接的蜂窝设备可以与RAN节点102的一个或多个其他天线处于通信，其中这些天线在前向链路140上向CIoT设备136传送信息，并且在反向链路138上从CIoT设备136接收信息。CIoT设备142可以与RAN节点102的一个或多个其他天线处于通信，其中这些天线在前向链路146上向CIoT设备142传送信息，并且在反向链路144上从CIoT设备142接收信息。RAN节点102可以通过一个或多个通信链路和/或参考点128来耦合至核心网130。

[0058] 贯穿本公开给出的各种概念可跨种类繁多的电信系统、网络架构、和通信标准来实现。例如，第三代伙伴计划(3GPP)是定义涉及演进型分组系统(EPS)的网络(通常称为长期演进(LTE)网络)的若干无线通信标准的标准团体。诸如第五代(5G)网络之类的LTE网络的演进版本可以提供许多不同类型的服务或应用，包括但不限于网页浏览、视频流送、VoIP、任务关键型应用、多跳网络、具有实时反馈的远程操作(例如，远程手术)等。LTE网络的演进是正在进行的过程。演进包括为改进与所有蜂窝设备(包括与IoT设备对接的蜂窝设备)的互操作性而作出的改变/修改/替换。相应地，本文描述了设备116、122、150、136、142、RAN节点102、以及核心网130内的节点的改变/修改/替换的各示例。

[0059] 无线蜂窝通信网络解决了两个级别的安全性。这些级别被称为接入阶层(AS)和非接入阶层(NAS)。使用长期演进(LTE)作为示例，接入阶层可以被描述为RAN与蜂窝设备之间的无线电信协议栈中的功能层。接入阶层协议层可以负责在RAN与蜂窝设备之间的无线连接上传输数据并且负责管理无线电资源。非接入阶层可以是核心网与蜂窝设备之间的无线电信协议栈中的功能层。非接入阶层协议层可被用于管理通信会话的建立并且用于在蜂窝设备移动时维护与该蜂窝设备的连续通信。非接入阶层协议层还可被用于在蜂窝设备与核心网的节点(例如，MME或C-SGN)之间接发消息，其中这些消息被透明地传递通过RAN。NAS消息的示例包括更新消息、附连请求消息、附连接受消息、认证消息以及服务请求。

[0060] 为了减小开销和等待时间，3GPP标准设定团体已经提议了与对于通过蜂窝设备传递的其他通信的要求相比的对于CIoT的不同要求。然而，这些要求可能使RAN节点和核心网具有不期望的弱点。

[0061] 不同要求之中包括消除接入阶层安全性。接入阶层安全性涉及蜂窝设备与演进型B节点之间的空中接口的安全性。提议在控制平面中的NAS层中将CIoT消息从蜂窝设备发送到核心网。CIoT消息(本文称为小数据消息)因此受现有NAS安全性的保护。然而，如下所解释的，消除AS安全性可能使RAN节点和核心网具有不期望的弱点。

[0062] 而且，不同要求之中包括消除对于CIoT的移动性支持。IoT设备可以通过一整天发送周期性报告来操作；他们不保持连接到核心网达很长时间。许多IoT设备是驻定的，它们不移动通过蜂窝小区，而是保留在一个蜂窝小区的各边界内的固定位置中。其他IoT设备，诸如耦合至汽车、人类、包裹等的那些IoT设备移动通过蜂窝小区，即，它们漫游。随着IoT设备漫游通过网络，在它们发送报告的时间到来时，它们会在蜂窝小区中苏醒，并且从该蜂窝小区内发送它们的报告；可能不需要蜂窝小区到蜂窝小区连接模式移动性。

[0063] 因此，CIoT架构中可以不支持连接模式移动性。消除移动性管理为RAN中的演进型

B节点和核心网中的MME提供了开销的降低。相应地，CIoT架构引入了被称为CIoT服务网关节点(C-SGN)的新节点。C-SGN将从MME剩余的任何所需功能与服务网关(S-GW)的功能性相组合。C-SGN可以等效于3G中的服务通用分组无线电服务(GPRS)支持节点(SGSN)。

[0064] 图2是解说本公开的各方面可在其中找到应用的通信网络200的另一示例的示图。例如，本文呈现的技术可以由网关202(例如，C-SGN)用来将密钥供应给第一RAN节点204(例如，C-BS)和CIoT设备206。图2的示例性解说代表涉及CIoT设备206的非漫游场景的CIoT架构。在图2的一方面，分组数据网络网关(P-GW)的功能可以与网关202(例如，C-SGN)的功能集成。附加地或替换地，作为实现选项240，P-GW的功能可以与P-GW 237中的网关202分开。根据实现选项240，S5参考点239可以在网关202(例如，C-SGN)与P-GW 237之间使用。S5参考点可以在网关202(例如，C-SGN)与P-GW 237之间提供用户面隧穿和隧道管理。例如，如果网关202(例如，C-SGN)连接到用于分组数据网络连通性的不共处一地的P-GW 237，则可以使用S5参考点。因此，即使在图2的示例性非漫游场景中，网关202(例如，C-SGN)和P-GW237也可以可选地是分开的实体(例如，它们可以不共处一地)。

[0065] 在图2的示例性解说中，由网关202供应的密钥可被用于完整性保护和/或加密小数据消息，由此向通信网络200提供接入阶层保护。

[0066] 在图2的示例中，可以将CIoT设备206表示为与蜂窝设备210对接的IoT设备208。对接可以是直接的(例如，IoT设备208可以硬连线到蜂窝设备210)或者间接的(例如，IoT设备208可以经由中间通信网络(诸如蓝牙无线网络)来耦合至蜂窝设备210)。CIoT设备206可以在C-Uu参考点212(参考点也可以称为网络接口)上与第一RAN节点204(例如，C-BS)无线地通信。第一RAN节点204(例如，C-BS)可以在S1或等效参考点上与网关202(例如，C-SGN)通信。在一些方面，如在图2中所解说的，第一RAN节点204可以在S1-轻量(S1-lite)214参考点上与网关202通信。S1-轻量是S1的“轻量级”版本，其针对小数据消息被优化。例如，仅支持CIoT过程所需要的S1应用协议(S1AP)消息和信息元素(IE)可被包括在S1-轻量中。一般而言，参考点(例如，网络接口)可以是S1、S1-轻量214、或等效物。

[0067] 还在图2中描绘了长期演进(LTE)或机器类型通信(MTC)蜂窝设备216。LTE或MTC蜂窝设备216可以在LTE Uu(eMTC)参考点218上与第二RAN节点220(例如，演进型B节点)无线地通信。

[0068] 第二RAN节点220可以在S1参考点上与网关202通信。在一些方面，如在图2中所解说的，第二RAN节点220可以在S1-轻量222参考点上与网关202通信。

[0069] 网关202可以与归属订户服务器224(HSS)通信。HSS 224可以存储和更新包含用户订阅信息的数据库并且从用户身份密钥生成安全信息。HSS 224可以在S6a 226参考点上与网关202通信。S6a 226参考点使得能够传输用于认证/授权对通信网络200的用户接入的订阅和认证数据。网关202可以与短消息服务(SMS)网关移动交换中心(SMS-GMSC)/互通移动交换中心(IWMSC)/SMS路由器(即，SMS-GMSC/IWMSC/SMS路由器228)通信。一般而言，SMS-GMSC/IWMSC/SMS路由器228是用于与其他网络的短消息服务的联系点。SMS-GMSC/IWMSC/SMS路由器228可以在Gd/Gdd 230参考点上与网关202通信。网关202可以与应用服务器232通信。

[0070] 一般而言，应用服务器232可以主存服务提供商的应用。应用服务器232可位于分组数据网络(例如，因特网)中。应用服务器232可以在SGi 234参考点上与网关202通信。Sgi

234是网关202(例如,C-SGN)与分组数据网络之间的参考点。

[0071] 图3是解说本公开的各方面可在其中找到应用的通信网络300的又一示例的示图。例如,本文呈现的技术可以由网关302(例如,C-SGN)用来将密钥供应给第一RAN节点304(例如,C-BS)和CIoT设备306。图3的示例性解说代表涉及CIoT设备306的漫游场景的CIoT架构。

[0072] 在图3的示例性解说中,由网关302供应的密钥可被用于完整性保护和/或加密小数据消息,由此向通信网络300提供接入阶层保护。

[0073] 图3的各节点与图2的那些节点相同或相似,除了添加了在网关302(例如,C-SGN)外部和/或不与网关302共处一地的分组数据网络(PDN)网关(P-GW)336节点之外。为了完整起见,图3的描述如下。

[0074] 在图3的示例中,可以将CIoT设备306表示为与蜂窝设备310对接的IoT设备308。对接可以是直接的(例如,IoT设备308可以硬连线到蜂窝设备310)或者间接的(例如,IoT设备308可以经由中间通信网络(诸如蓝牙无线网络)来耦合至蜂窝设备310)。CIoT设备306可以在C-Uu参考点312(参考点也可以称为网络接口)上与第一RAN节点304(例如,C-BS)无线地通信。第一RAN节点304(例如,C-BS)可以在S1参考点上与网关302(例如,C-SGN)通信。在一些方面,如在图3中所解说的,第一RAN节点304可以在S1-轻量314参考点上与网关302通信。S1-轻量是S1的针对小数据消息优化的版本。例如,仅支持CIoT过程所需要的S1应用协议(S1AP)消息和信息元素(IE)可被包括在S1-轻量中。一般而言,参考点(例如,网络接口)可以是S1、S1-轻量314、或等效物。

[0075] 还在图3中描绘了长期演进(LTE)或机器类型通信(MTC)蜂窝设备316。LTE或MTC蜂窝设备316可以在LTE Uu(eMTC)参考点318上与第二RAN节点320(例如,演进型B节点)无线地通信。

[0076] 第二RAN节点320可以在S1参考点上与网关302通信。在一些方面,如在图3中所解说的,第二RAN节点320可以在S1-轻量322参考点上与网关302通信。

[0077] 网关302可以与归属订户服务器324(HSS)通信。HSS 324可以存储和更新包含用户订阅信息的数据库并且从用户身份密钥生成安全信息。HSS 324可以在S6a 326参考点上与网关302通信。S6a 326参考点使得能够传输用于认证/授权对通信网络300的用户接入的订阅和认证数据。网关302可以与短消息服务(SMS)网关移动交换中心(SMS-GMSC)/互通移动交换中心(IWMSC)/SMS路由器(即,SMS-GMSC/IWMSC/SMS路由器328)通信。一般而言,SMS-GMSC/IWMSC/SMS路由器328是用于与其他网络的短消息服务的联系点。SMS-GMSC/IWMSC/SMS路由器328可以在Gd/Gdd 330参考点上与网关302通信。网关302可以与应用服务器332通信。

[0078] 一般而言,应用服务器332可以主存服务提供商的应用。应用服务器332可位于分组数据网络(例如,因特网)中。应用服务器332可以在SGi 334参考点上与P-GW 336通信。SGi 334是分组数据网络中的P-GW 336与应用服务器332之间的参考点。P-GW 336可以在S8 338参考点上与网关302(例如,C-SGN)通信。S8 338参考点是公共陆地移动网络间(PLMN间)参考点,其一般在访客公共陆地移动网络(VPLMN)中的服务GW(或者在图3的情形中,C-SGN)与归属公共陆地移动网络(HPLMN)中的P-GW之间提供用户和控制面接口。

[0079] 在图3的一方面,P-GW功能可以与P-GW 336中的网关302分开或者作为实现选项340与P-GW 337中的网关302分开。在实现选项340的情形中,S5参考点339可以在网关302

(例如,C-SGN)与P-GW 337之间使用。S5参考点可以在网关302(例如,C-SGN)与P-GW 337之间提供用户面隧穿和隧道管理。例如,如果网关302(例如,C-SGN)连接到用于分组数据网络连通性的不共处一地的P-GW 237,则可以使用S5参考点。

[0080] 在本文描述的示例性方面,蜂窝设备可以与物联网(IoT)设备对接。各示例性方面是关于经由蜂窝设备在IoT设备与核心网之间发送数据消息(例如,小数据消息)来描述的;然而,本文描述的各方面不限于小数据消息并且对其他类型的数据消息具有适用性。

[0081] 示例性无状态接入阶层安全性过程

[0082] 图4是解说根据本公开的一些方面的接入阶层安全密钥推导和供应过程400的示例的流程图。网关可首先获得(402)(例如,导出、生成、计算、检索、接收、请求等)第一密钥。网关可以是CIoT服务网关节点(C-SGN)。C-SGN可以是可被实现以支持用于CIoT使用情形的功能性的网关。C-SGN可以纳入对于CIoT使用情形有用的LTE移动性管理实体(MME)、LTE服务网关(S-GW)、以及LTE分组数据网络网关(P-GW)的那些方面。本文对C-SGN的引用是出于方便起见的。本文描述的各方面不限于使用C-SGN作为网关的实现。在一些方面,术语C-SGN和网关可以在本文中互换地使用。

[0083] 第一密钥可以被称为主接入阶层安全密钥(MASK)。在一些方面,第一密钥不是从任何其他密钥获得的。例如,第一密钥不是从其他密钥材料导出的。在一些方面,第一密钥可以在C-SGN处随机地获得。例如,在一些方面,第一密钥可以在C-SGN处随机地生成。第一密钥可以仅对C-SGN网关已知。

[0084] C-SGN可以接下来获得(404)第二密钥。第二密钥可以被称为基站接入阶层安全密钥(BASK)。可以从第一密钥(例如,MASK)和对于无线电接入网(RAN)节点(例如,演进型B节点、C-BS)而言独有的参数获得第二密钥。对于RAN节点而言独有的参数可以是RAN节点的身份。在一个方面,RAN节点的身份可以是CIoT基站身份(C-BS ID)。C-BS ID可以等效于例如LTE中的演进型B节点ID。第二密钥可以使用密钥导出函数(KDF)来获得。例如,第二密钥可以如下给出:

[0085] 第二密钥=KDF(MASK,C-BS ID),

[0086] 其中KDF是密钥导出函数,MASK是第一密钥,并且C-BS ID是CIoT基站身份。

[0087] 第二密钥可以由网关供应(406)给RAN节点(例如,C-BS)。至少因为第二密钥基于第一密钥和对于无线电接入网(RAN)节点而言独有的参数,所以可以在将蜂窝设备初始附连到蜂窝网络之前、期间或之后将第二密钥供应给RAN节点。

[0088] C-SGN仍可进一步获得第三密钥。第三密钥可以被称为设备接入阶层安全密钥(DASK)。第三密钥可以从第二密钥(例如,BASK)和对于蜂窝设备而言独有的参数获得。对于蜂窝设备而言独有的参数可以是蜂窝设备的身份。蜂窝设备的身份可以是例如SAE临时移动订户身份(S-TMSI)。

[0089] 第三密钥可以使用密钥导出函数(KDF)来获得。例如,第三密钥可以如下给出:

[0090] 第三密钥=KDF(BASK,蜂窝设备ID),

[0091] 其中KDF是密钥导出函数,BASK是第二密钥,并且蜂窝设备ID是蜂窝设备的身份。

[0092] 在一些方面,网关(例如,C-GSN)可以将第三密钥(例如,DASK)供应(410)给蜂窝设备。

[0093] 在一些方面,蜂窝设备可以向小数据消息添加完整性保护,其中完整性保护可以

例如基于第三密钥(例如,DASK)和设备的身份。蜂窝设备可以附加地或替换地加密小数据消息,其中可以使用第三密钥(例如,DASK)来执行加密。可以从蜂窝设备向RAN节点发送经完整性保护和/或经加密的小数据消息。

[0094] 第三密钥可以在安全非接入阶层(NAS)消息上被供应(例如,发送)给蜂窝设备(即,完成了NAS安全模式命令)。安全NAS消息的一个示例可以是在成功完成初始附连规程之际向蜂窝设备发送的附连接受消息。作为替换方案,第三密钥可以作为经加密信息元素(IE)发送到蜂窝设备。在该替换方案中,IE可包括标识用于加密IE的算法的算法标识符。

[0095] 在一些方面,RAN节点不建立和/或维护与设备的接入阶层安全性上下文。建立和/或维护接入阶层安全性上下文可能需要使用状态表并且处理与状态表相关联的数据。状态表和相关联的处理可以表示开销的消耗,这例如在CIoT中是不期望的。相反,本文公开了无状态安全性方案的各方面。例如,RAN节点拥有由网关(例如,C-SGN)供应给RAN节点的第二密钥(例如,BASK)。在一个示例中,RAN节点可以在运行中(例如,动态地、按需地)从第二密钥(例如,BASK)和蜂窝设备的身份获得第三密钥(例如,DASK)。蜂窝设备的身份与在RAN节点处获得的每个小数据消息包括在一起,并且第二密钥独立于蜂窝设备的身份;相应地,安全性方案是无状态的,至少因为不需要状态表。

[0096] 随后,RAN节点可以使用它在运行中获得(例如,导出、生成)的第三密钥(例如,DASK)来验证从设备获得的小数据消息的完整性和/或解密该小数据消息。使用本文描述的示例性密钥生成和供应方案,可以借助于现有消息来实现AS安全性措施。开销不增大。RAN节点可以保护其自己和核心网不受诸如拒绝服务和/或洪泛攻击之类的弱点的影响。

[0097] 图5是解说根据本公开的一些方面的蜂窝物联网(CIoT)下的附连规程的示例的呼叫流程图500。在图5的各方面,包括蜂窝设备502(例如,CIoT设备)、RAN节点504(例如,C-BS)、核心网网关(例如,CIoT服务网关节点(C-SGN)506)、归属订户服务器(HSS)508、以及P-GW 510。P-GW 510被描绘用于其中蜂窝设备502正在漫游的场景。

[0098] 图5的示例性呼叫流程可以在执行(520)RRC连接建立规程时开始。在执行RRC连接建立规程期间,蜂窝设备502和RAN节点504可以向彼此提供一个或多个一次性数值(例如,一次性数设备、一次性数RAN)和/或一个或多个时间戳值,如本文稍后所解释的。蜂窝设备502可以执行通过发送附连请求522所指示的附连规程。在附连规程期间,蜂窝设备502可以指示附连是用于CIoT小数据消息的(例如,“CIoT附连”可以被包括为附连请求522的参数)。RAN节点504(例如,C-BS)可以基于蜂窝设备指示或基于预先配置来选择针对CIoT优化的C-SGN 506。蜂窝设备502还可以指示特定数据类型(例如,IP和/或非IP和/或SMS)。可以指示接入点名称(APN)。APN可以标识蜂窝设备502向其请求连通性的C-SGN 506和/或P-GW 510,并且可包括标识C-SGN506位于其中的公共陆地移动网络(PLMN)和/或P-GW 510位于其中的PLMN的APN运营商标识符。

[0099] 如以上指示的,C-SGN 506可以获得用于RAN节点504(例如,C-BS)的第二密钥(例如,BASK)。C-SGN 506可以在NAS消息524中将第二密钥供应给RAN节点504(例如,C-BS)。

[0100] C-SGN 506可以执行任何所需要的认证/安全性规程526。

[0101] C-SGN 506可以与归属订户服务器508(HSS)一起执行位置更新并且可以检索订阅信息528。

[0102] C-SGN 506可以处理附连请求522,并且可以基于与附连请求522一起提供的参数

来决定是否存在建立IP承载服务的需要。如果数据类型参数被标识为“IP”，则PDN类型指示要分配的IP地址类型(即，IPv4、IPv6)。C-SGN 506可以基于附连请求522中的PDN类型来分配IP地址。NAS会话管理信令可能不需要。在漫游场景中，C-SGN 506可向P-GW发送创建会话请求(或新的控制消息)，从而指示这是CIoT附连请求以及指示数据类型530。P-GW可基于附连请求中的PDN类型来分配IP地址。

[0103] 仅在漫游场景中，取决于数据类型，P-GW可以向C-SGN 532发送创建会话响应(或新的控制消息)。对于IP数据情形(例如，数据类型＝IP)而言，创建会话响应可包括所分配的IP地址。

[0104] C-SGN可以通过向蜂窝设备502发送附连接受消息534来响应，而无需任何会话管理消息。对于数据类型＝IP而言，所分配的IP地址可被发送到蜂窝设备502。附连接受消息可包括全球唯一临时标识符(GUTI)。GUTI可以在蜂窝设备502的初始附连规程期间由C-SGN(或C-SGN的MME功能)来指派。

[0105] 如以上所指示的，在附连规程(例如，初始附连)期间，C-SGN 506可以获得用于蜂窝设备502的第三密钥(例如，DASK)。根据一些方面，C-SGN 506可以在NAS消息中(例如，在附连接受消息534中)将第三密钥供应给蜂窝设备。

[0106] 蜂窝设备502可以用附连完成消息536来响应。

[0107] RRC连接可被释放538。

[0108] 图6是解说根据本公开的各方面的可支持无状态接入阶层安全性以及安全密钥的获得(例如，导出、生成、计算、检索、接收、请求等)、供应、和使用中的一者或多者的装置600(例如，电子设备)的硬件实现的示例的框图。装置600可以在网关(例如，C-SGN)、RAN节点(例如，基站、eNB、C-BS)、蜂窝设备(例如，CIoT设备)或支持无线通信的一些其他类型的设备(诸如移动电话、智能电话、平板设备、便携式计算机、服务器、个人计算机、传感器、娱乐设备、医疗设备或具有无线通信电路系统的任何其他电子设备)内实现。

[0109] 装置600(例如，通信装置)可包括通信接口602(例如，至少一个收发机)、存储介质604、用户接口606、存储器设备608(例如，存储一个或多个安全密钥618)、以及处理电路610。在各种实现中，用户接口606可包括以下一者或多者：按键板、显示器、扬声器、话筒、触摸屏显示器、或者用于从用户接收输入或向用户发送输出的某种其他电路系统。

[0110] 这些组件可以经由信令总线640或其他合适的组件(由图6中的连接线一般地表示)彼此耦合和/或彼此置于电通信中。取决于处理电路610的具体应用和整体设计约束，信令总线640可包括任何数目的互连总线和桥接器。信令总线640将各种电路链接在一起以使得通信接口602、存储介质604、用户接口606和存储器设备608中的每一者与处理电路610耦合和/或处于电通信。信令总线640还可链接各种其它电路(未示出)，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。

[0111] 通信接口602可被适配成促成装置600的无线通信。例如，通信接口602可包括被适配成促成相对于网络中的一个或多个通信设备进行双向信息通信的电路系统和/或编程。在一些实现中，通信接口602可被构造、适配、和/或配置成用于基于有线的通信。在一些实现中，通信接口602可耦合至一个或多个天线612以用于无线通信系统内的无线通信。通信接口602可以被构造、适配、和/或配置有一个或多个自立接收机和/或发射机，以及一个或

多个收发机。在所解说的示例中，通信接口602包括发射机614和接收机616。

[0112] 存储器设备608可表示一个或多个存储器设备。如所指示的，存储器设备608可维护安全密钥618以及由装置600使用的其他信息。在一些实现中，存储器设备608和存储介质604被实现为共用存储器组件。存储器设备608也可被用于存储由处理电路610或装置600的一些其它组件操纵的数据。

[0113] 存储介质604可表示用于存储编程(诸如处理器可执行代码或指令(例如，软件、固件))、电子数据、数据库、或其他数字信息的一个或多个非瞬态计算机可读、机器可读、和/或处理器可读设备。存储介质604也可被用于存储由处理器610在执行编程时操纵的数据。存储介质604可以是能被通用或专用处理器访问的任何可用介质，包括便携式或固定存储设备、光学存储设备、以及能够存储、包含或携带编程的各种其他介质。

[0114] 作为示例而非限制，存储介质604可包括：磁存储设备(例如，硬盘、软盘、磁条)、光盘(例如，压缩碟(CD)或数字多功能碟(DVD))、智能卡、闪存存储器设备(例如，记忆卡、记忆棒、或钥匙驱动器)、随机存取存储器(RAM)、只读存储器(ROM)、可编程ROM(PROM)、可擦式PROM(EPROM)、电可擦式PROM(EEPROM)、寄存器、可移动盘、以及任何其他用于存储可由计算机访问和读取的软件和/或指令的合适介质。存储介质604可以在制品(例如，计算机程序产品)中实现。作为示例，计算机程序产品可包括封装材料中的计算机可读介质。鉴于上述内容，在一些实现中，存储介质604可以是非瞬态(例如，有形的)存储介质。

[0115] 存储介质604可被耦合至处理电路610，以使得处理电路610能从存储介质604读取信息和向存储介质604写入信息。即，存储介质604可耦合至处理电路610，以使得存储介质604至少能由处理电路610访问，包括其中至少一个存储介质被集成到处理电路610的示例和/或其中至少一个存储介质与处理电路610分开(例如，驻留在装置600中、在装置600外部、跨多个实体分布等)的示例。

[0116] 由存储介质604存储的编程在由处理电路610执行时使处理电路610执行本文描述的各种功能和/或过程操作中的一者或多者。例如，存储介质604可包括被配置用于以下动作的操作：调节处理电路610的一个或多个硬件块处的操作、以及将通信接口602用于利用其相应通信协议的无线(或在一些实现中有线)通信。

[0117] 处理电路610一般适配成用于处理，包括执行存储在存储介质604上的此类编程。如本文中使用的，术语“代码”或“编程”应当被宽泛地解释成不构成限定地包括指令、指令集、数据、代码、代码段、程序代码、程序、编程、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，无论其被称为软件、固件、中间件、微代码、硬件描述语言、还是其他术语。

[0118] 处理电路610可被布置成获得、处理和/或发送数据、控制数据访问和存储、发布命令、以及控制其它期望操作。处理电路610可包括构造、适配、和/或配置成实现由至少一个示例中的恰适介质提供的期望编程的电路系统。例如，处理电路610可被实现为一个或多个处理器、一个或多个控制器、和/或构造、适配、和/或配置成执行可执行编程的其他结构。处理电路610的示例可包括被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)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑组件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合。通用处理器可包括微处理器，以及任何常规的处理器、控制器、微控制器、或状态机。处理电路610还可被实现为计算组件的组合，诸

如DSP与微处理器的组合、数个微处理器、与DSP核协作的一个或多个微处理器、ASIC和微处理器、或任何其他数目的变化配置。处理电路610的这些示例是用于解说的，并且本公开范围内的其它适合配置是可以构想的。

[0119] 根据本公开的一个或多个方面，处理电路610可适配成执行用于本文中描述的任何或所有装置的特征、过程、功能、操作和/或例程中的任一者或全部。例如，处理电路610可被适配成执行和/或实行关于图4、5、7、9-12和14标识的各框中描述的操作中的任一者。如本文所使用的，涉及处理电路610的术语“适配”可指处理电路610被构造、配置、采用、实现和/或编程(以上一者或多者)为执行根据本文描述的各种特征的特定过程、功能、操作和/或例程。

[0120] 处理电路610可以是用作用于执行和/或实行关于图4、5、7、9-12和14标识的各框中描述的操作中的任一者的装置(例如，结构)的专用处理器，诸如专用集成电路(ASIC)。处理电路610可用作用于传送的装置和/或用于接收的装置的一个示例。

[0121] 根据装置600的至少一个示例，处理电路610可包括用于传达的电路/模块620、用于确定的电路/模块622、用于供应的电路/模块624、用于发送的电路/模块626、用于等待的电路/模块628、或者用于获得的电路/模块629中的一者或多者。

[0122] 如以上所提及的，由存储介质604存储的编程在由处理电路610执行时使得处理电路610执行本文描述的各种功能和/或过程操作中的一者或多者。例如，存储介质604可包括用于传达的代码630、用于确定的代码632、用于供应的代码634、用于发送的代码636、用于等待的代码638、或者用于获得的代码639中的一者或多者。

[0123] 图7是解说根据本公开的一些方面的无状态接入阶层安全性过程700的示例的流程图。无状态接入阶层安全性过程700可以在处理电路(例如，图6的处理电路610)内发生，该处理电路可位于网关(例如，C-SGN)或某个其他合适的装置中。相应地，无状态接入阶层安全性过程700可以在网关(例如，C-SGN)或一些其他合适的装置处操作。在本公开的范围内的各个方面，无状态接入阶层安全性过程700可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性(包括获得、供应和使用安全密钥中的一者或多者)的任何合适装置来实现。

[0124] 根据一些方面，无状态接入阶层安全性过程700可以被描述为一种通信方法，其可包括在装置(例如，网关、C-SGN)处获得仅对该装置已知的第一密钥(702)。在装置处获得基于第一密钥以及对于无线电接入网(RAN)节点而言独有的参数(例如，使用第一密钥和该参数导出、使用第一密钥和该参数生成)的第二密钥(704)。由装置将第二密钥供应给RAN节点(706)。在装置处获得基于第二密钥和对于蜂窝设备708而言独有的参数的第三密钥。并且可以进一步包括：由装置将第三密钥供应给蜂窝设备(710)。

[0125] 根据一些方面，装置(例如，网关、C-SGN、通信装置)可以获得仅对装置702已知的第一密钥(例如，主接入阶层密钥——MASK)。在一些方面，第一密钥可以不是从任何其他密钥获得的。换言之，装置可以在不从任何其他密钥获得第一密钥的情况下获得第一密钥。在一些方面，装置可以随机地生成第一密钥。换言之，装置可以通过在装置处随机地生成第一密钥来获得第一密钥。在一些方面，装置可以是蜂窝物联网服务网关节点(C-SGN)。在一些方面，仅该装置(例如，网关、C-SGN)知道第一密钥(例如，MASK)。换言之，在一些方面，第一密钥仅对该装置是已知的。

[0126] 装置可获得第二密钥(例如,主接入阶层安全密钥——MASK),该第二密钥可基于第一密钥和对于无线电接入网(RAN)节点704而言独有的参数。在一些方面,对于RAN节点而言独有的参数可以是RAN节点的身份。在一些方面,RAN节点可以是CIoT基站(C-BS)或演进型B节点(eNodeB),并且对于RAN节点而言独有的参数可以是C-BS身份或演进型B节点身份。在一些方面,密钥导出函数可被用于获得(例如,导出、生成)第二密钥。

[0127] 装置可以将第二密钥供应给RAN节点706。在一些方面,装置可在非接入阶层(NAS)消息中将第二密钥供应给RAN节点。在一些方面,非接入阶层消息可以是安全NAS消息。

[0128] 装置可获得第三密钥(例如,设备接入阶层安全密钥——DASK),该第三密钥可基于第二密钥和对于蜂窝设备708而言独有的参数。在一些方面,对于蜂窝设备而言独有的参数可以是蜂窝设备身份。在一些方面,对于蜂窝设备而言独有的参数可以是系统架构演进(SAE)临时移动订户身份(S-TMSI)。S-TMSI可被用于本地地标识MME群内的蜂窝设备。S-TMSI可被用于寻呼蜂窝设备。S-TMSI可以由MME码和MME移动订户身份(M-TMSI)构成。在一些方面,密钥导出函数可被用于获得(例如,导出、生成)第三密钥。

[0129] 装置可以将第三密钥供应给蜂窝设备710。在一些方面,装置可在非接入阶层(NAS)消息中将第三密钥供应给蜂窝设备。在一些方面,非接入阶层消息可以是安全NAS消息。在一些方面,非接入阶层消息可以是附连接受消息。在一些方面,装置可以将第三密钥作为经加密信息元素(IE)供应到蜂窝设备。IE可包括标识用于加密IE的算法的算法标识符。

[0130] 图8是解说根据本公开的各方面的可支持无状态接入阶层安全性以及安全密钥的获得、供应、和使用中的一者或多者的装置800(例如,电子设备、通信装置)的硬件实现的另一示例的框图。装置800可以在网关(例如,C-SGN)、RAN节点(例如,eNB、C-BS)、蜂窝设备(例如,CIoT设备)或支持无线通信的一些其他类型的设备(诸如移动电话、智能电话、平板设备、便携式计算机、服务器、个人计算机、传感器、娱乐设备、医疗设备或具有无线通信电路系统的任何其他电子设备)内实现。

[0131] 装置800可包括通信接口(例如,至少一个收发机)802、存储介质804、用户接口806、存储器设备808(例如,存储一个或多个安全密钥818)、以及处理电路810。在各种实现中,用户接口806可包括以下一者或多者:按键板、显示器、扬声器、话筒、触摸屏显示器、或者用于从用户接收输入或向用户发送输出的某种其他电路系统。一般而言,图8的各组件可以类似于图6的装置600的对应组件。

[0132] 根据本公开的一个或多个方面,处理电路810可适配成执行用于本文中描述的任何或所有装置的特征、过程、功能、操作和/或例程中的任一者或全部。例如,处理电路810可被适配成执行关于图4、5、7、9-12和14描述的各框中的任一者。如本文所使用的,涉及处理电路810的术语“适配”可指处理电路810被构造、配置、采用、实现、和/或编程(以上一者或多者)为执行根据本文描述的各种特征的特定过程、功能、操作和/或例程。

[0133] 处理电路810可以是用作用于实行结合图4、5、7、9-12、和14描述的操作中的任一者的装置(例如,结构)的专用处理器,诸如专用集成电路(ASIC)。处理电路810可用作用于传送的装置和/或用于接收的装置的一个示例。

[0134] 根据装置800的至少一个示例,处理电路810可包括用于传达的电路/模块820、用于接收的电路/模块822、用于比较的电路/模块824、用于丢弃的电路/模块826、用于发送的

电路/模块828、用于获得的电路/模块830、用于解密的电路/模块832、用于验证的电路/模块834、用于检测的电路/模块836、或用于监视的电路/模块838中的一者或多者。

[0135] 如以上所提及的，由存储介质804存储的编程在由处理电路610执行时，可使得处理电路810执行本文描述的各种功能和/或过程操作中的一者或多者。例如，存储介质804可包括用于传达的代码840、用于接收的代码842、用于比较的代码844、用于丢弃的代码846、用于发送的代码848、用于获得的代码850、用于解密的代码852、用于验证的代码854、用于检测的代码856、或用于监视的代码858中的一者或多者。

[0136] 图9是解说根据本公开的一些方面的无状态接入阶层安全性保护通信的方法900的示例的流程图。无状态接入阶层安全性保护通信的方法900可以在处理电路(例如，图8的处理电路810)内发生，该处理电路可位于无线电接入网(RAN)节点(例如，eNB、C-BS)或某个其他合适的装置中。相应地，无状态接入阶层安全性保护通信的方法900可以在RAN节点或某个其他合适的装置处操作。在本公开的范围内的各个方面，无状态接入阶层安全性保护通信的方法900可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性(包括获得、供应和使用安全密钥中的一者或多者)的任何合适装置来实现。

[0137] 在图9的一方面，当蜂窝设备向RAN节点(例如，eNB、C-BS)发送小数据消息时，蜂窝设备可以通过使用由网关(例如，C-SGN)在初始附连规程期间供应给蜂窝设备的第三密钥(例如，DASK)来保护(例如，完整性保护和/或加密)小数据消息。用第三密钥保护(例如，完整性保护和/或加密)的小数据消息在本文中可以被称为“受保护消息”。第三密钥可基于第二密钥(例如，BASK)和蜂窝设备的身份。第二密钥可以在设备将受保护消息发送到RAN节点之前、期间、或之后由网关供应给RAN节点。第二密钥可被存储在RAN节点处，例如，在长期存储器设备(例如，图8的存储器设备808)、临时存储器、或高速缓存中。

[0138] 当RAN节点从蜂窝设备接收受保护消息时，RAN节点可以确定该消息包括完整性保护值(例如，消息认证码(MAC)、令牌)。RAN节点可以使用例如RAN节点可以在运行中从对RAN节点已知或可用的项目(例如，第二密钥、设备ID)获得(例如，导出、生成)的第三密钥来验证完整性保护值。例如，如所陈述的，第三密钥可以基于第二密钥(例如，BASK)和蜂窝设备的身份(例如，设备ID、S-TMSI)(例如，使用第二密钥和设备的身份来导出、生成)。第二密钥可以从网关供应给RAN节点，而蜂窝设备的身份(例如，S-TMSI)可被包括在由RAN节点接收的小数据消息中。

[0139] 根据本文描述的示例性方面，第二密钥(例如，BASK)可能不是因蜂窝设备而异的(例如，第二密钥可能不是给定蜂窝设备独有的)。尽管第三密钥可以是因蜂窝设备而异的，但是RAN节点(例如，基站、eNB、C-BS)没有义务维护关于蜂窝设备的安全性上下文(UE状态、蜂窝设备状态)以实现接入阶层安全性。取而代之的是，为了验证和/或解密来自蜂窝设备的受保护消息，RAN节点可以在运行中使用第二密钥(例如，BASK)和设备ID来获得第三密钥，并且使用第三密钥来验证和/或解密来自蜂窝设备的受保护消息。第二密钥可以由RAN节点与之相关联的每个网关(例如，C-SGN)来供应给RAN节点。设备ID可与要被验证和/或解密的小数据消息包括在一起。在RAN节点从蜂窝设备接收到受保护消息时，RAN节点可以在运行中获得(例如，导出、生成、计算、检索、接收、请求等)蜂窝设备的第三密钥。相应地，与获得第三密钥(例如，DASK)有关的示例性接入阶层安全性方案是无状态的。

[0140] 在一些实现中，第二密钥可以是因RAN节点而异的。在其它实现中，第二密钥可以

是因RAN节点群而异的(例如,多个RAN节点可以具有公共群标识符)。在其中第二密钥是因RAN节点群而异的实现中,第二密钥可以在给定群中的多个RAN节点之中共享。当第二密钥在多个RAN节点之间共享时,即使蜂窝设备连接到给定群中的不同RAN节点,蜂窝设备也可能不需要针对给定群中遇到的每个RAN节点从网关(例如,C-SGN)获得新的第三密钥(例如,DASK)。因此,取代基于第一密钥(例如,MASK)和RAN节点身份(例如,eNB ID)来获得(例如,导出、生成)第二密钥(例如,BASK),网关(例如,C-SGN)可以从第一密钥(例如,MASK)和RAN节点群身份获得第二密钥(例如,BASK)。换言之,在给定RAN节点群(即,给定RAN节点群)的覆盖内,给定群的各RAN节点共享相同的第二密钥(例如,BASK)。相应地,蜂窝设备(例如,CIoT设备、UE)可以使用对于给定RAN节点群中的多个RAN节点而言公共的第三密钥(例如,DASK)来保护在给定RAN节点群的覆盖内发送的小数据消息(和/或验证和/或解密所接收到的小数据消息)。在一些实现中,网络可以配置RAN节点群并且将RAN节点群的可用性宣告为系统信息(SI)的一部分。

[0141] 根据一些方面,无状态接入阶层安全性保护通信的方法900可以被描述为安全性保护通信的方法。无状态接入阶层安全性保护通信可以用例如完整性保护和/或加密(在本文中一般称为加密或解密)来保护通信。该方法可包括:在装置(例如,RAN节点、C-BS、eNB)处获得基于第一密钥和对于装置而言独有的参数(例如,使用第一密钥和对于装置而言独有的参数导出、生成)的第二密钥(902)。在装置处获得包括设备身份和第一完整性保护值的小数据消息(904)。在装置处获得基于第二密钥和设备身份的第三密钥(906)。在装置处获得使用第三密钥获得(例如,导出、生成)的第二完整性保护值(908)。完整性保护过程可以使用第三密钥来执行(以产生完整性保护值),并且可以进一步使用例如设备身份、一个或多个一次性数、以及受保护的小数据消息来执行。在装置处将第一完整性保护值与第二完整性保护值进行比较(910)。获得比较结果/确定第一完整性保护值是否等于第二完整性保护值(912)。如果比较结果指示第一完整性保护值不等于第二完整性保护值,则从装置丢弃小数据消息(914)。替换地,如果比较结果指示第一完整性保护值等于第二完整性保护值,则从装置向网关发送小数据消息(916)。

[0142] 根据一些方面,装置(例如,RAN节点、C-BS、eNB)可获得第二密钥(例如,BASK),其中该第二密钥基于第一密钥和对于装置902而言独有的参数。在一些方面,从网关获得第二密钥。在一些方面,第一密钥仅对网关是已知的。在一些方面,网关是C-SGN。在一些方面,对于RAN节点而言独有的参数是RAN节点的身份。例如,RAN节点可以是CIoT基站(C-BS)或演进型B节点(eNodeB),并且对于RAN节点而言独有的参数可以是C-BS身份或演进型B节点身份。

[0143] 装置(为了方便起见称为“装置”,或者替换地称为与图9的以下描述相关联的“RAN节点”)可以接收包括设备身份和第一完整性保护值的小数据消息(904)。

[0144] 装置可以获得基于第二密钥和设备身份的第三密钥(例如,DASK)(906)。

[0145] 装置可以使用第三密钥来获得第二完整性保护值(908)。

[0146] 在一个方面,第一完整性保护值和第二完整性保护值可以是归属于令牌(例如,归因于令牌、从令牌计算)的值。在一个方面,第一完整性保护值和第二完整性保护值可以是归属于消息认证码(MAC)的值。如本文使用的,令牌和/或MAC可被称为完整性保护参数。例如,在其中本文描述的AS安全性保护的各方面被用于上行链路话务(例如,从设备到RAN节点)的场景中,RAN节点可能需要向设备提供一次性数(例如,一次性数RAN)以供在AS安全性

保护中使用。在此类场景中，可以使用如下所示的MAC：

[0147] MAC＝F(DASK,S-TMSI|一次性数RAN|消息)。

[0148] 根据一个替换方案，获得MAC的另一方式可以使用下式：

[0149] K_{MAC}＝KDF(DASK,一次性数RAN)，其中K_{MAC}是基于DASK和一次性数RAN获得的一次性MAC生成密钥；而KDF是密钥导出函数。

[0150] MAC＝F(K_{MAC},消息)。

[0151] 根据又一替换方案，为了计及针对单个连接(例如，RRC连接)发送多个消息的情况，可以纳入计数器以生成每个消息的MAC，即，

[0152] MAC＝F(K_{MAC},计数器|消息)，

[0153] 其中在导出新密钥(即，K_{MAC})时计数器被初始化(例如，归零)，并且对于用于连接的每一单个消息使计数器增大特定值(例如，1)。

[0154] 在又一替换方案中，在其中本文描述的AS安全性保护的各方面被用于上行链路话务(例如，从设备到RAN节点)和/或下行链路话务(例如，从RAN节点到设备)的场景中，设备可能需要向RAN节点提供一次性数(例如，一次性数设备)以供在AS安全性保护中使用。在此类场景中，可以使用如下所示的MAC：

[0155] MAC＝F(DASK,S-TMSI|一次性数设备|一次性数RAN|消息)。

[0156] 其中，对于以上所示出的所有等式，F是MAC生成函数(例如，CMAC,HMAC)(本文中可将“F”可替换地称为完整性保护算法)，DASK是第二密钥的示例，S-TMSI是蜂窝设备的身份的示例，一次性数设备是可仅被使用一次并且由设备提供的第一任意数字，一次性数RAN是可仅被使用一次并且由RAN节点提供的第二任意数字，并且消息是正在发送的消息(例如，小数据消息)。

[0157] 根据另一替换方案，获得MAC的另一方式可以使用下式：

[0158] K_{MAC}＝KDF(DASK,S-TMSI|一次性数设备|一次性数RAN)，其中K_{MAC}是基于DASK、一次性数设备、以及一次性数RAN获得的一次性MAC生成密钥；而KDF是密钥导出函数。

[0159] MAC＝F(K_{MAC},消息)

[0160] 根据又一替换方案，为了计及针对单个连接(例如，RRC连接)发送多个消息的情况，可以纳入计数器以生成每个消息的MAC，即，

[0161] MAC＝F(K_{MAC},计数器|消息)，

[0162] 其中在导出新密钥(即，K_{MAC})时计数器被初始化(例如，归零)，并且对于用于连接的每一单个消息使计数器增大特定值(例如，1)。

[0163] 完整性保护参数(例如，MAC、令牌)可以纳入一个或多个一次性数(例如，一次性数设备和/或一次性数RAN)以防止重放攻击。换言之，一个或多个一次性数可被用于重放保护。在随机接入规程期间，可以在设备与RAN节点之间交换一次性数设备和/或一次性数RAN。例如，设备可以在随机接入规程的消息3(RRC连接请求)中将该一次性数设备发送到RAN节点，并且RAN节点可以在随机接入规程的消息4(RRC连接建立)中将该一次性数RAN发送到设备。如果存在不止一个消息要发送，则对于每个消息，该一次性数(例如，一次性数设备和/或一次性数RAN)可以增大预定的固定量(例如，1)。

[0164] 作为一次性数(例如，一次性数设备和/或一次性数RAN)的替换方案，可被改变(例如，以防止重放攻击)的任何随机数是可接受的。在一些方面，一次性数可以用时间戳来替

代(例如,由时间戳来置换)。如果蜂窝设备和装置(例如,RAN节点、C-BS)具有定时器,则可以使用时间戳。相应地,在一些方面,并且作为示例,以上提供的示例性MAC中的一次性数(例如,一次性数设备和/或一次性数RAN)中的一者或多者可以用随机地选择的数字和/或时间戳来替代(例如,由随机地选择的数字和/或时间戳来置换)。

[0165] 作为又一替换方案,在一些方面,以上提供的示例性MAC中的一次性数(例如,一次性数设备和/或一次性数RAN)中的一者或多者可以用蜂窝小区无线电网络临时身份(C-RNTI)来替代(例如,由蜂窝小区无线电网络临时身份(C-RNTI)来置换)。C-RNTI可以是用于标识RRC连接以及专用于特定蜂窝设备的(例如,设备独有的)调度的唯一标识。例如,在此类场景中,第一和第二完整性保护参数可以是使用参数C-RNTI而不是一次性数设备和一次性数RAN获得的消息认证码(MAC)。例如,

[0166] MAC=F(DASK,S-TMSI|C-RNTI|消息),

[0167] 其中,F是MAC生成功能(例如,CMAC、HMAC),DASK是第二密钥的示例,S-TMSI是蜂窝设备的身份的示例,C-RNTI是RRC连接建立期间指派给设备的身份,并且消息是正在发送的消息(例如,小数据消息)。使用该替换方案可能受由网络在指派S-TMSI和C-RNTI标识符时使用的隐私策略的强度影响。例如,可以在假定网络具有用于指派那些标识符的良好隐私策略的情况下使用该替换方案。

[0168] K_{MAC}=KDF(DASK,S-TMSI|C-RNTI),

[0169] 其中K_{MAC}是基于DASK、S-TMSI、以及C-RNTI获得的一次性MAC生成密钥;而KDF是密钥导出函数。

[0170] MAC=F(K_{MAC},消息)

[0171] 为了计及针对单个连接(例如,RRC连接)发送多个消息的情况,可以纳入计数器以生成每个消息的MAC,即,

[0172] MAC=F(K_{MAC},计数器|消息)

[0173] 其中在导出新密钥(即,K_{MAC})时计数器被初始化(例如,归零),并且对于用于连接的每一单个消息使计数器增大特定值(例如,1)。

[0174] 在上述示例性替换方案中,用于获得(例如,导出、生成)完整性保护参数(例如,MAC、令牌)的完整性保护算法(例如,函数F)可以由网络确定并且向设备通知。这还适用于加密算法,如下所述。

[0175] 相应地,在一些方面,第一完整性保护参数和第二完整性保护参数可以纳入一个或多个一次性数、随机数、时间戳和/或网络指派的唯一性(例如,C-RNTI)参数。在RAN节点处操作的方法可包括由RAN节点向蜂窝设备供应一次性数(例如,一次性数RAN)、随机数、时间戳和/或网络指派的唯一性(例如,C-RNTI)参数。在RAN节点处操作的方法可包括在随机接入规程期间,由RAN节点向蜂窝设备供应一次性数(例如,一次性数RAN)、随机数、时间戳和/或网络指派的唯一性(例如,C-RNTI)参数。在设备处操作的方法可包括由设备向RAN节点供应一次性数(例如,一次性数设备)、随机数、时间戳和/或网络指派的唯一性参数。在设备处操作的方法可包括在随机接入规程期间由设备向RAN节点供应一次性数(例如,一次性数RAN)、随机数、时间戳和/或网络指派的唯一性参数。

[0176] 装置可将第一完整性保护值与第二完整性保护值进行比较(910)。

[0177] 如果比较结果指示第一完整性保护值不等于第二完整性保护值,则装置可丢弃小

数据消息(914)。

[0178] 如果比较结果指示第一完整性保护值等于第二完整性保护值,则装置可向网关(例如,下一跳)发送小数据消息(916)。

[0179] 如以上所指示的,在一些方面,第一完整性保护参数和第二完整性保护参数可以纳入随机数和/或时间戳以防止重放攻击。在一些方面,RAN节点可以从由设备身份标识的设备接收小数据消息,并且RAN节点向设备供应随机数。例如,可以从由设备身份标识的设备获得小数据消息,并且随机数可以是在随机接入规程期间由RAN节点提供给设备的一次性数。对于从RAN节点发送到设备的每个消息,一次性数可以增大预定的固定量。

[0180] 以下过程也可被用于实现一种安全性保护通信的方法。该方法可包括:在无线电接入网(RAN)节点处获得基于第一密钥和对于RAN节点而言独有的参数的第二密钥,在RAN节点处获得包括设备身份和第一完整性保护值的小数据消息,在RAN节点处获得基于第二密钥和设备身份的第三密钥,在RAN节点处基于第三密钥来获得第二完整性保护值,在RAN节点处将第一完整性保护值与第二完整性保护值进行比较,如果比较结果指示第一完整性保护值不等于第二完整性保护值则从RAN节点丢弃小数据消息,以及如果比较结果指示第一完整性保护值等于第二完整性保护值,则从RAN节点向网关发送小数据消息。根据一些方面,从网关获得第二密钥。根据一些方面,网关是蜂窝物联网服务网关节点(C-SGN)。根据一些方面,RAN节点是蜂窝物联网(CIoT)基站(C-BS)或演进型B节点(eNodeB),并且对于RAN节点而言独有的参数是C-BS身份或演进型B节点身份。根据一些方面,第一完整性保护值和第二完整性保护值是使用至少一个一次性数和/或时间戳来获得的。根据一些方面,设备身份标识设备,并且该方法进一步包括向设备供应第一一次性数和/或时间戳和/或从设备获得第二一次性数。根据一些方面,供应第一一次性数和/或时间戳并且获得第二一次性数发生在随机接入规程期间。根据一些方面,小数据消息用第三密钥来加密,并且该方法进一步包括使用第三密钥在RAN节点处解密小数据消息。根据一些方面,在获得小数据消息之前,该方法进一步包括:由RAN节点监视话务负载值;由RAN节点检测话务负载值超过预定阈值;以及

[0181] 响应于检测到话务负载值超过了预定阈值而向由设备身份标识的设备发送消息,该消息请求设备将第一完整性保护值包括在发送到RAN节点的下一个或多个消息中。根据一些方面,网络配置预定阈值。根据一些方面,在获得小数据消息之前,该方法进一步包括:在与由设备身份标识的设备的初始附连规程期间,配置和/或协商接入阶层安全性配置,其中接入阶层安全性配置指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、和/或具有按需完整性保护的情况下是否从设备发送小数据消息,其中使用第三密钥来执行完整性保护和加密。

[0182] 图10是解说根据本公开的一些方面的无状态接入阶层安全性过程1000的另一示例的流程图。无状态接入阶层安全性过程1000可以在处理电路(例如,图8的处理电路810)内发生,该处理电路可位于无线电接入网(RAN)节点(例如,C-BS)或某个其他合适的装置中。相应地,无状态接入阶层安全性过程1000可以在RAN节点(例如,C-BS)或某个其他合适的装置处操作。当然,在本公开的范围内的各个方面,无状态接入阶层安全性过程1000可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性的(包括获得、供应和使用安全密钥中的一者或多者的)任何合适装置来实现。

[0183] 在图10的一方面，当蜂窝设备向RAN节点(例如，C-BS)发送小数据消息时，蜂窝设备可以通过使用由网关(例如，C-SGN)在初始附连规程期间供应给蜂窝设备的第三密钥(例如，DASK)来加密小数据消息。当RAN节点(例如，C-BS)从蜂窝设备接收小数据消息时，RAN节点可以使用可以由网关供应给RAN节点的第二密钥(例如，BASK)和可以与由RAN节点获得的经加密小数据消息一起携带的蜂窝设备的身份来在运行中获得第三密钥(例如，DASK)。例如，经加密小数据消息可以与蜂窝设备的S-TMSI一起携带。

[0184] 加密可以在随机接入规程期间使用由RAN节点(例如，C-BS)提供给蜂窝设备的一次性数。在一个方面，一次性数可以作为初始化向量(IV)来提供。例如：

[0185] 密码文本＝Enc(DASK，IV，消息)，

[0186] 其中Enc是加密函数(例如，AES-CTR，...)，DASK是第二密钥的示例，并且IV是作为初始化向量提供的一次性数。

[0187] 使用一次性密钥来加密的另一替换方式，如之前的：

[0188] K_{Enc}＝KDF(DASK，一次性数)，

[0189] 其中K_{Enc}是基于DASK和S-TMSI、C-RNTI、一次性数设备、一次性数RAN或其组合来获得的一次性加密密钥；而KDF是密钥导出函数。

[0190] 密码文本＝Enc(K_{Enc}，IV，消息)，

[0191] 其中IV被初始化为特定值(例如，0、或者基于S-TMSI、C-RNTI、一次性数RAN、一次性数设备或其组合来获得的值)。

[0192] 为了计及针对单个连接(例如，RRC连接)发送多个消息的情况，可以纳入计数器以生成每个消息的密码文本，即，

[0193] 密码文本＝Enc(K_{Enc}，IV，消息)，

[0194] 其中在导出新密钥(即，K_{Enc})时IV被初始化(例如，0、或者基于S-TMSI、C-RNTI、一次性数RAN、一次性数设备或其组合来获得的值)，并且对于用于连接的每一单个消息使IV增大特定值(例如，1)。

[0195] 如之前所述的，RAN节点可以基于第二密钥(例如，BASK)和蜂窝设备的身份来获得第三密钥(例如，DASK)。

[0196] 在一些方面，因为RAN节点(例如，C-BS)可以将一次性数(例如，被用作/设置为IV的一次性数)存储达较短时间量(例如，达RRC连接的历时)，所以在消息中包含IV是可任选的。

[0197] 在一些方面，一次性数是随机接入规程期间由装置(例如，RAN节点、C-BS)提供给蜂窝设备的随机选择的数字。如果存在不止一个消息要发送，则对于每个消息，该一次性数可以递增预定的固定量(例如，1)。替换地，由装置(例如，RAN节点、C-BS)提供给蜂窝设备并且可以被改变(例如，以防止重放攻击)的任何随机数是可接受的。在一些方面，一次性数可以用C-RNTI来替代。在一些方面，一次性数可以由时间戳来替代。如果蜂窝设备和装置(例如，RAN节点、C-BS)具有定时器，则可以使用时间戳。

[0198] 现在转到图10，装置(例如，RAN节点、C-BS)可接收第二密钥(例如，BASK)，其中该第二密钥基于第一密钥和对于装置(例如，RAN节点、C-BS)而言独有的参数(1002)。在一些方面，RAN节点从网关接收第二密钥，并且第一密钥仅由网关知晓。在一些方面，网关是C-SGN。在一些方面，对于RAN节点而言独有的参数是RAN节点的身份。例如，RAN节点可以是

CIoT基站(C-BS)或演进型B节点(eNodeB),并且对于RAN节点而言独有的参数可以是C-BS身份或演进型B节点身份。

[0199] 装置可以接收包括设备身份的经加密小数据消息。在一些方面,小数据消息用第三密钥(例如,DASK)来加密(1004)。

[0200] 装置可以获得基于第二密钥和设备身份的第三密钥(例如,DASK)(1006)。

[0201] 装置可以使用第三密钥来解密该小数据消息(1008)。

[0202] 在一些方面,加密和解密可以纳入随机数和/或时间戳以防止重放攻击。在一些方面,可以从由设备身份标识的设备获得小数据消息,并且RAN节点向设备供应随机数。例如,可以从由设备身份标识的设备获得小数据消息,并且随机数可以是随机接入规程期间由RAN节点提供给设备的一次性数。对于从RAN节点发送到设备的每个消息,一次性数可以递增预定的固定量。

[0203] 图11是解说根据本公开的一些方面的无状态接入阶层安全性过程1100的另一示例的流程图。无状态接入阶层安全性过程1100可以在处理电路(例如,图8的处理电路810)内发生,该处理电路可位于无线电接入网(RAN)节点(例如,C-BS)或某个其他合适的装置中。相应地,无状态接入阶层安全性过程1100可以在RAN节点(例如,C-BS)或某个其他合适的装置处操作。当然,在本公开的范围内的各个方面,无状态接入阶层安全性过程1100可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性的(包括获得、供应和使用安全密钥中的一者或多者的)任何合适装置来实现。

[0204] 在图11的一方面,可以启用加密和完整性保护两者。当加密和完整性保护两者被配置以供使用时,可以使用具有相关联数据的认证加密(AEAD)密码。在初始附连规程期间可以配置和/或协商接入阶层安全性。

[0205] 现在转到图11,装置(例如,无线电接入网(RAN)节点、C-BS)可接收第二密钥(例如,BASK),其中该第二密钥基于第一密钥和对于装置(例如,RAN节点、C-BS)而言独有的参数(1102)。在一些方面,RAN节点从网关接收第二密钥,并且第一密钥仅由网关知晓。在一些方面,网关是C-SGN。在一些方面,对于RAN节点而言独有的参数是RAN节点的身份。例如,RAN节点可以是CIoT基站(C-BS)或演进型B节点(eNodeB),并且对于RAN节点而言独有的参数可以是C-BS身份或演进型B节点身份。

[0206] 装置可以接收包括设备身份的小数据消息。在一些方面,小数据消息可以用第三密钥(例如,DASK)来加密,并且小数据消息可包括使用第三密钥导出或生成的完整性保护值(1104)。

[0207] 装置可以获得基于第二密钥和设备身份的第三密钥(例如,DASK)(1106)。

[0208] 设备可以使用第三密钥来解密小数据消息(1108)。

[0209] 设备可以使用第三密钥来验证完整性保护值(1110)。

[0210] 图12是解说根据本公开的一些方面的无状态接入阶层安全性过程1200的另一示例的流程图。无状态接入阶层安全性过程1200可以在处理电路(例如,图8的处理电路810)内发生,该处理电路可位于无线电接入网(RAN)节点(例如,C-BS)或某个其他合适的装置中。相应地,无状态接入阶层安全性过程1200可以在RAN节点(例如,C-BS)或某个其他合适的装置处操作。当然,在本公开的范围内的各个方面,无状态接入阶层安全性过程1200可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性的(包括获得、供应和

使用安全密钥中的一者或多者的)任何合适装置来实现。

[0211] 在图12的一方面,描绘了采用令牌的示例性按需完整性保护过程。根据一个方面,在正常操作模式或第一操作模式中,不配置接入阶层安全性;在第二操作模式中,配置接入阶层安全性。例如,当在RAN节点(例如,C-BS)或某个其他网络节点处检测到拥塞和/或过载时,RAN节点(例如,C-BS)可以向蜂窝设备发送消息(例如,指示、请求、指令、命令)。该消息可导致(或可触发)蜂窝设备将令牌与发送到RAN节点(例如,C-BS)的一个或多个消息(例如,小数据消息)包括在一起。在一个示例中,可以基于大量小数据消息传输来检测拥塞和/或过载。在一个示例中,可以在话务负载超过给定阈值时检测到拥塞和/或过载,并且可以触发指示/请求/指令/命令的发送。在一些方面,阈值可以是预定义的。在一方面,网络可以配置阈值。

[0212] 根据一些方面,令牌可以按与用于完整性的MAC完全相同的方式来创建;然而,与用于完整性的MAC不同,根据这一方面的令牌是从RAN节点按需提供的(例如,响应于来自RAN节点的需求而提供的)。

[0213] 例如,在随机接入规程期间,RAN节点(例如,C-BS)和设备可以如先前所解释的那样交换各自的一次性数(例如,一次性数RAN、一次性数设备)。附加地,RAN节点可以向蜂窝设备提供指示/请求/指令/命令,以与所传输的下一个或多个小数据消息一起发送令牌。令牌可被创建为

[0214] 令牌=F(DASK,S-TMSI|一次性数设备|一次性数RAN|消息),其中

[0215] F是令牌生成函数(例如,CMAC、HMAC),DASK是第三密钥,S-TMSI是蜂窝设备的身份(可以使用标识蜂窝设备的其他参数),一次性数设备和一次性数RAN在以上描述,并且消息是正在发送的消息。如果存在不止一个消息要发送,则对于每个消息,该一次性数可以递增固定量(例如,1)。

[0216] 当RAN节点(例如,C-BS)从蜂窝设备接收携带令牌的消息时,RAN节点可以在运行中获得第三密钥(例如,DASK),其中该第三密钥可以基于第二密钥(例如,BASK)和蜂窝设备的身份。随后,RAN节点可以验证令牌,例如,通过根据上面提供的等式来获得(例如,导出、生成)第二令牌,并且将接收到的令牌与第二令牌进行比较。

[0217] 在一些方面,一次性数可以被携带在蜂窝设备消息中或临时存储在RAN节点(例如,C-BS)处。

[0218] 因为在各种实现中,采用令牌的按需完整性保护过程在拥塞/过载期间被触发,所以按需完整性保护过程使在接入阶层安全性(例如,LTE接入阶层安全性)一直被激活的情况下原本将对蜂窝设备和RAN节点(例如,C-BS)招致的计算开销最小化。

[0219] 现在转到图12,装置(例如,无线电接入网(RAN)节点)可以监视话务负载值(1202)。

[0220] 装置可以检测话务负载值超过预定阈值(1204)。在一个示例中,网络(例如,核心网)可以配置预定阈值。

[0221] 响应于检测到话务负载值超过预定阈值,装置可以向蜂窝设备(例如,CIoT设备)发送消息(例如,指示、请求、指令、命令),该消息请求蜂窝设备将令牌包括在向装置(RAN节点、C-BS)发送的下一个或多个消息中(1206)。

[0222] 图13是解说根据本公开的一个或多个方面的可支持无状态接入阶层安全性以及

获得、供应、和使用安全密钥中的一者或多者的装置1300(例如,蜂窝设备、CIoT设备、电子设备、通信装置)的硬件实现的另一示例的框图。装置1300可以在网关(例如,C-SGN)、RAN节点(例如,基站、eNB、C-BS)、蜂窝设备、CIoT设备、或支持无线通信的一些其他类型的设备(诸如移动电话、智能电话、平板设备、便携式计算机、服务器、个人计算机、传感器、娱乐设备、医疗设备或具有无线通信电路系统的任何其他电子设备)内实现。

[0223] 装置1300包括通信接口(例如,至少一个收发机)1302、存储介质1304、用户接口1306、存储器设备1308(例如,存储一个或多个安全密钥1318)、以及处理电路1310。在各种实现中,用户接口1306可包括以下一者或多者:按键板、显示器、扬声器、话筒、触摸屏显示器、或者用于从用户接收输入或向用户发送输出的某种其他电路系统。一般而言,图13的各组件可以类似于图6的装置600的对应组件。

[0224] 根据本公开的一个或多个方面,处理电路1310可适配成执行用于本文中描述的任何或所有装置的特征、过程、功能、操作和/或例程中的任一者或全部。例如,处理电路1310可被适配成执行关于图4、5、7、9-12和14描述的框、步骤、功能、和/或过程中的任一者。如本文所使用的,涉及处理电路1310的术语"适配"可指处理电路1310被构造、配置、采用、实现、和/或编程(以上一者或多者)为执行根据本文描述的各种特征的特定过程、功能、操作和/或例程。

[0225] 处理电路1310可以是用作用于实行结合图4、5、7、9-12、和14描述的操作中的任一者的装置(例如,结构)的专用处理器,诸如专用集成电路(ASIC)。处理电路1310可用作用于传送的装置和/或用于接收的装置的一个示例。

[0226] 根据装置1300的至少一个示例,处理电路1310可包括用于传达的电路/模块1320、用于接收的电路/模块1322、用于配置的电路/模块1324、用于协商的电路/模块1326、用于发送的电路/模块1328、用于获得完整性参数的电路/模块1330、或者用于加密的电路/模块1332中的一者或多者。

[0227] 如以上所提及的,由存储介质1304存储的编程在由处理电路1310执行时使得处理电路1310执行本文描述的各种功能和/或过程操作中的一者或多者。例如,存储介质1304可包括用于传达的代码1340、用于接收的代码1342、用于配置的代码1344、用于协商的代码1346、用于发送的代码1348、用于获得完整性参数的代码1350、或者用于加密的代码1352中的一者或多者。

[0228] 图14是解说根据本公开的各方面的无状态接入阶层安全性过程1400的另一示例的流程图。无状态接入阶层安全性过程1400可以在处理电路(例如,图13的处理电路1310)内发生,该处理电路可位于蜂窝设备(例如,CioT设备)或某个其他合适的装置中。相应地,无状态接入阶层安全性过程1400可以在蜂窝设备或某个其他合适的装置处操作。当然,在本公开的范围内的各个方面,无状态接入阶层安全性过程1400可以由根据本公开的一个或多个方面的能够支持无状态接入阶层安全性的(包括获得、供应和使用安全密钥中的一者或多者的)任何合适装置来实现。

[0229] 现在转到图14,装置(例如,蜂窝设备、CIoT设备)可获得基于第二密钥(例如,BASK)和对于装置而言独有的参数的第三密钥(例如,DASK)(1402)。在一些方面,对于装置而言独有的参数可以是装置的身份(例如,蜂窝设备的身份、蜂窝设备ID、CIoT设备ID)。在一些方面,第二密钥可以基于第一密钥和RAN节点身份或RAN节点群身份。装置可能不知道

第二密钥和第一密钥。在一些方面，例如，第二密钥可以基于第一密钥和对于RAN节点而言独有的参数，并且第一密钥可仅对网关是已知的。

[0230] 装置可以配置和/或协商接入阶层安全性配置(1404)。在一些方面，装置可以与RAN节点协商接入阶层安全性配置。在一些方面，装置可以在初始附连规程期间协商接入阶层安全性配置。在一些方面，装置可以在初始附连规程期间与RAN节点协商接入阶层安全性配置。根据一些方面，接入阶层安全性配置可指定在没有安全性、具有完整性保护、具有加密、具有完整性保护和加密、和/或具有按需完整性保护的情况下是否从蜂窝设备发送小数据消息，其中完整性保护和加密可以使用第三密钥来执行。

[0231] 装置可以使用第三密钥基于接入阶层安全性配置来保护小数据消息(1406)。装置可以用使用第三密钥的完整性保护和/或加密来保护小数据消息。装置可以发送使用第三密钥来保护的小数据消息(1408)。在一些方面，该装置可以将使用第三密钥保护的小数据消息发送到RAN节点。

[0232] 关于本文描述的所有方面和实现，网关(例如，C-SGN)可以周期性地改变第一密钥(例如，MASK)。根据一些方面，第一密钥可以与第一索引(例如，MASK索引)相关联。例如，第一密钥可以由第一索引确定。在一个方面，每当第一密钥改变时(每个周期)，第一索引可以改变。

[0233] 根据一些方面，第二密钥(例如，BASK)可以与第二索引(例如，BASK索引)相关联。第二索引可以由第一索引(例如，MASK索引)确定。例如，可以向RAN节点(例如，C-BS)供应第二密钥，该第二密钥具有与当前有效(例如，未期满、活跃)的第一索引相对应的第二索引。

[0234] 根据一些方面，第三密钥(例如，DASK)可以与第三索引(例如，DASK索引)相关联。第三索引可以由第二索引(例如，BASK索引)确定。例如，可以向蜂窝设备(例如，CIoT设备)供应第三密钥，该第三密钥具有与当前有效(例如，未期满、活跃)的第二索引相对应的第三索引。

[0235] 第三密钥索引(例如，DASK索引)可被包括在小数据消息中，以使得根据本文描述的各方面，获得小数据消息的实体(例如，RAN节点、C-BS)可以获得(例如，导出、生成)应当用于接入阶层安全性验证和/或解密的第三密钥(例如，DASK)。

[0236] 例如，任何密钥(例如，第一、第二、和/或第三密钥)的改变可以由于时间期满、安全性、维护、检测到密钥泄露、或检测到(一个或多个)恶意设备。

[0237] 根据一个方面，当密钥无效(例如，由于时间期满、安全性、维护、检测到密钥泄露、检测到(一个或多个)恶意设备等)时，错误消息可以被发送到蜂窝设备和/或网关(例如，C-SGN)。

[0238] 在蜂窝设备处，在获得错误消息之际，蜂窝设备可以向网关(例如，C-SGN)发送对第三密钥(例如，DASK)的请求。对第三密钥的请求可以被称为密钥请求消息(并且可以被替换地称为DASK更新消息)。密钥请求消息可能不受接入阶层安全性保护，如本文描述的各方面所讨论的。

[0239] 例如，密钥请求消息和/或错误消息可以被发送到网关，以触发网关使用安全NAS控制消息来向蜂窝设备发送(例如，推送)新的第三密钥(例如，新DASK)。在一个方面，在网关改变用于给定蜂窝设备的密钥(例如，发送新的第三密钥)时，网关可以同时向其他蜂窝设备(例如，其第三密钥可能基于泄露的第二密钥的那些设备)供应相应的新密钥。然而，根

据其他方面，在网关改变用于给定蜂窝设备的密钥(例如，发送新的第三密钥)时，网关可以不同时向其他蜂窝设备供应相应的新密钥。

[0240] 替换地，密钥请求消息(例如，DASK更新)可以由设备通过向网关(例如，C-SGN)发送用旧密钥保护的消息来触发。

[0241] 网关(例如，C-SGN)可以同时使用多个不同的第一密钥(例如，MASK)和对应的不同的第二密钥(例如，BASK)。同时使用不同的第一密钥和对应的不同的第二密钥例如可以减小密钥改变的影响和/或一般而言改进安全性。

[0242] 根据一些方面，在RAN节点(例如，C-BS)处，接入阶层安全性保护消息可以获得比不使用接入阶层安全性保护的消息更高的优先级(例如，可以优先于不使用接入阶层安全性保护的消息)。根据一些方面，当RAN节点(例如，C-BS)拥塞或过载时，在RAN节点处，接入阶层安全性保护消息可以获得比不使用接入阶层安全性保护的消息更高的优先级(例如，可以优先于不使用接入阶层安全性保护的消息)。

[0243] 根据一些方面，CIoT可能不支持连接模式移动性(即，切换规程)。相应地，根据本文描述的一些方面的接入阶层安全性也可能不支持连接模式移动性。

[0244] 根据本文描述的一些方面，当蜂窝设备(例如，CIoT设备)附连到新的RAN节点(例如，C-BS)时，蜂窝设备可以发送密钥请求消息，如上所述。例如，蜂窝设备可以向新的RAN节点发送密钥请求消息。根据一些方面，如果蜂窝设备被附连到先前附连的RAN节点(例如，C-BS)，则蜂窝设备可以使用与先前附连的RAN节点相关联的第三密钥(例如，DASK)(如果第三密钥没有被移除和/或如果任何相关联的密钥索引没有被改变)。

[0245] 图15是包括如可出现在本公开的一些方面中的RAN 1502和多个通信实体的无线通信网络1500的一部分的示意性解说。如本文所描述的，蜂窝设备、CIoT设备、LTE无线蜂窝设备、和/或机器类型通信无线蜂窝设备可以例如驻留在以下各项中或者可以是以下各项的一部分：IoT设备1504、智能警报器1506、远程传感器1508、智能电话1510、移动电话1512、智能仪表1514、个人数字助理(PDA)1516、个人计算机1518、网状节点1520、和/或平板计算机1522。当然，所解说的设备和组件是示例，并且任何合适的节点或设备可出现在本公开的范围内的无线通信网络内。提供这些示例是用于解说本公开的某些概念。本领域普通技术人员将领会，这些示例在本质上是示例性的，且其他示例可落在本公开和所附权利要求的范围内。

[0246] 如本领域普通技术人员将容易领会的那样，贯穿本公开描述的各个方面可扩展到任何合适的电信系统、网络架构和通信标准。作为示例，各方面可被应用于UMTS系统，诸如W-CDMA、TD-SCDMA、和TD-CDMA。各个方面还可被应用于采用长期演进(LTE)(在FDD、TDD或这两种模式中)、高级LTE(LTE-A)(在FDD、TDD或这两种模式中)、CDMA 2000、演进数据最优化(EV-DO)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、超宽带(UWB)、蓝牙的系统和/或其他合适的系统，包括由待定义的广域网标准所描述的那些系统。所采用的实际的电信标准、网络架构和/或通信标准将取决于具体应用以及加诸于该系统的整体设计约束。

[0247] 在本公开内，措辞“示例性”用于表示“用作示例、实例或解说”。本文中描述为“示例性”的任何实现或方面不必被解释为优于或胜过本公开的其他方面。同样，术语“方面”不要求本公开的所有方面都包括所讨论的特征、优点或操作模式。术语“耦合”在本文中用于

指两个对象之间的直接或间接机械和/或电耦合。例如，如果对象A物理上接触对象B和/或与对象B电通信，并且对象B物理上接触对象C和/或与对象C电通信，则对象A和C可仍被认为是彼此耦合的——即便它们并非彼此直接地物理上接触和/或与彼此电通信。例如，第一管芯可以在封装中耦合至第二管芯，即便第一管芯从不直接与第二管芯物理接触。术语“电路”和“电路系统”被宽泛地使用且意在包括电子器件和导体的硬件实现以及信息和指令的软件实现两者，这些电子器件和导体在被连接和配置时使得能执行本公开中描述的功能而在电子电路的类型上没有限制，这些信息和指令在由处理器执行时使得能执行本公开中描述的功能。

[0248] 以上中解说的组件、框、特征和/或功能之中的一者或多者可以被重新安排和/或组合成单个组件、框、特征或功能，或可以实现在若干组件、步骤或功能中。也可添加附加的组件、框、特征、和/或功能，而不会脱离本文中所公开的新颖性特征。以上解说的装置、设备、和/或组件可以被适配(例如，构造、配置、采用、实现、和/或编程)成执行本文所描述的方法、框、特征、和/或功能中的一者或多者。本文中描述的算法也可以高效地实现在软件中和/或嵌入在硬件中。

[0249] 应理解，所公开的方法中各框的具体次序或阶层是示例性过程的解说。应理解，可以重新安排这些方法中各框的具体次序或阶层。所附方法权利要求以样本次序呈现各个框的要素，且并不意味着被限定于所呈现的具体次序或阶层，除非在本文中有特别叙述。

[0250] 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。对这些方面的各种修改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各方面，而是应被授予与权利要求的语言相一致的全部范围，其中对要素的单数形式的引述并非旨在表示“有且仅有一个”——除非特别如此声明，而是旨在表示“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。引述一列项目“中的至少一个”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和b；a和c；b和c；以及a、b和c。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。权利要求的任何要素都不应当在35U.S.C.§112(f)的规定下来解释，除非该要素是使用短语“用于.....的装置”来明确叙述的或者在方法权利要求情形中该要素是使用短语“用于.....的步骤”来叙述的。

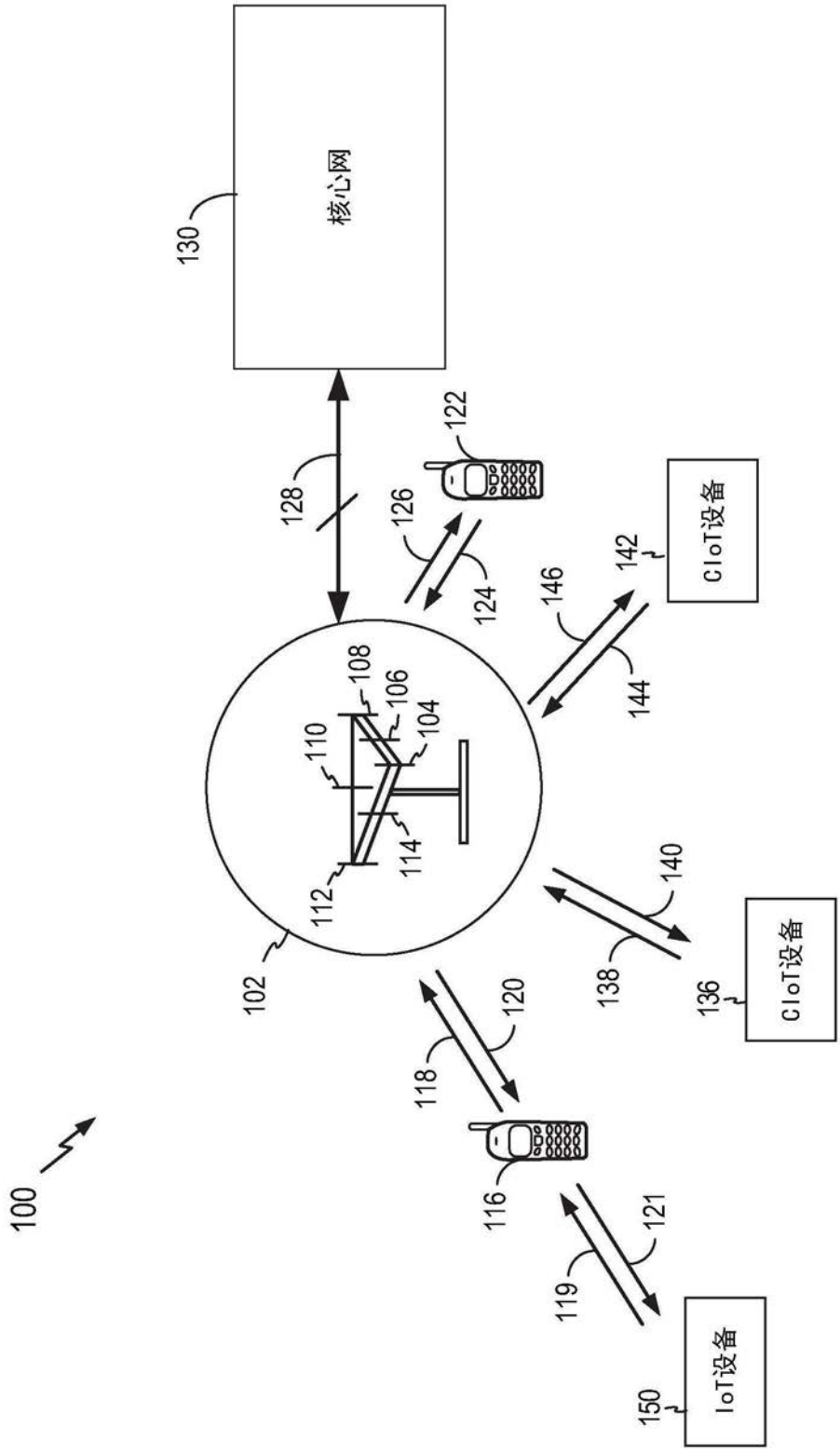

核心网
130
128
122
126
124
142
CIoT设备
146
144
108
106
104
110
114
112
102
140
138
136
CIoT设备
120
118
116
121
119
150
IoT设备
100

图1

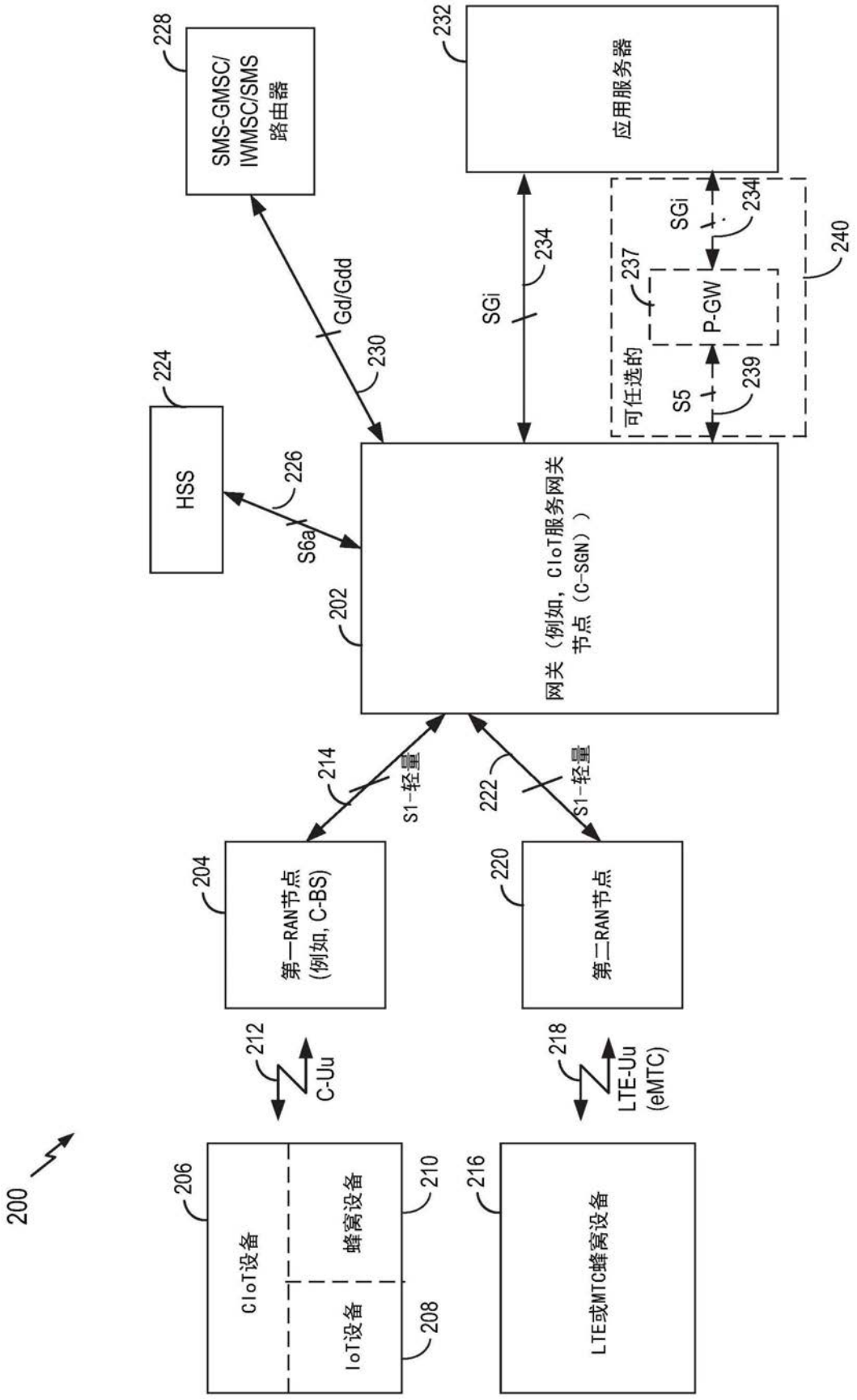

200
206
CIoT设备
蜂窝设备
210
IoT设备
208
212
C-Uu
204
第一RAN节点
(例如, C-BS)
214
S1-轻量
216
LTE或MTC蜂窝设备
218
LTE-Uu
(eMTC)
220
第二RAN节点
222
S1-轻量
202
网关（例如，CIoT服务网关
节点（C-SGN））
224
HSS
226
S6a
228
SMS-GMSC/
IWMSC/SMS
路由器
230
Gd/Gdd
232
应用服务器
234
SGi
234
SGi
240
可任选的
237
P-GW
S5
239

图2

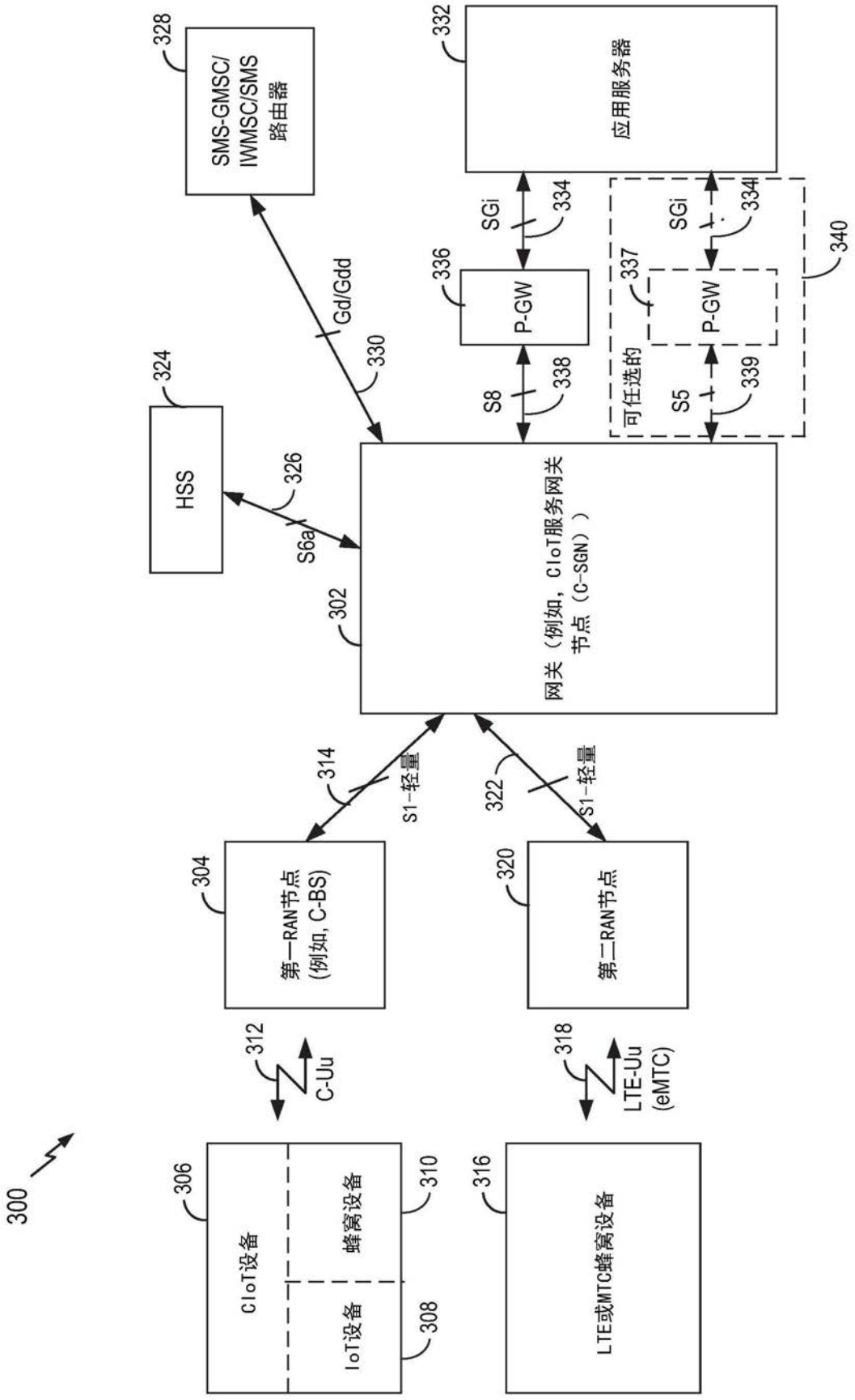

300
306
CIoT设备
蜂窝设备
310
IoT设备
308
316
LTE或MTC蜂窝设备
312
C-Uu
318
LTE-Uu
(eMTC)
304
第一RAN节点
(例如, C-BS)
320
第二RAN节点
314
S1-轻量
322
S1-轻量
302
网关（例如，CIoT服务网关
节点（C-SGN））
324
HSS
326
S6a
328
SMS-GMSC/
IWMSC/SMS
路由器
330
Gd/Gdd
332
应用服务器
336
P-GW
338
S8
SGi
334
可任选的
337
P-GW
339
S5
SGi
334
340

图3

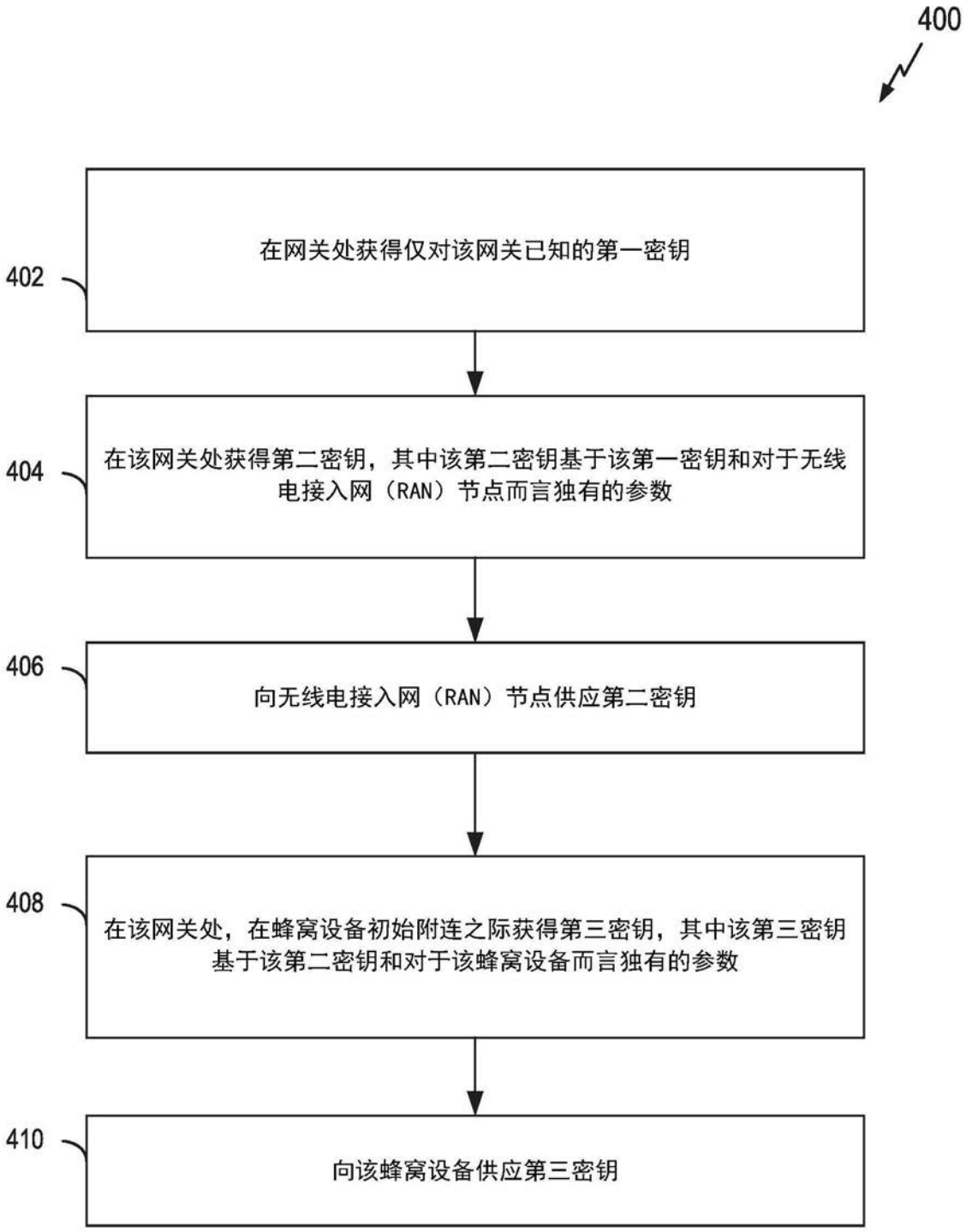

400
402
在网关处获得仅对该网关已知的第一密钥
404
在该网关处获得第二密钥，其中该第二密钥基于该第一密钥和对于无线电接入网（RAN）节点而言独有的参数
406
向无线电接入网（RAN）节点供应第二密钥
408
在该网关处，在蜂窝设备初始附连之际获得第三密钥，其中该第三密钥基于该第二密钥和对于该蜂窝设备而言独有的参数
410
向该蜂窝设备供应第三密钥

图4

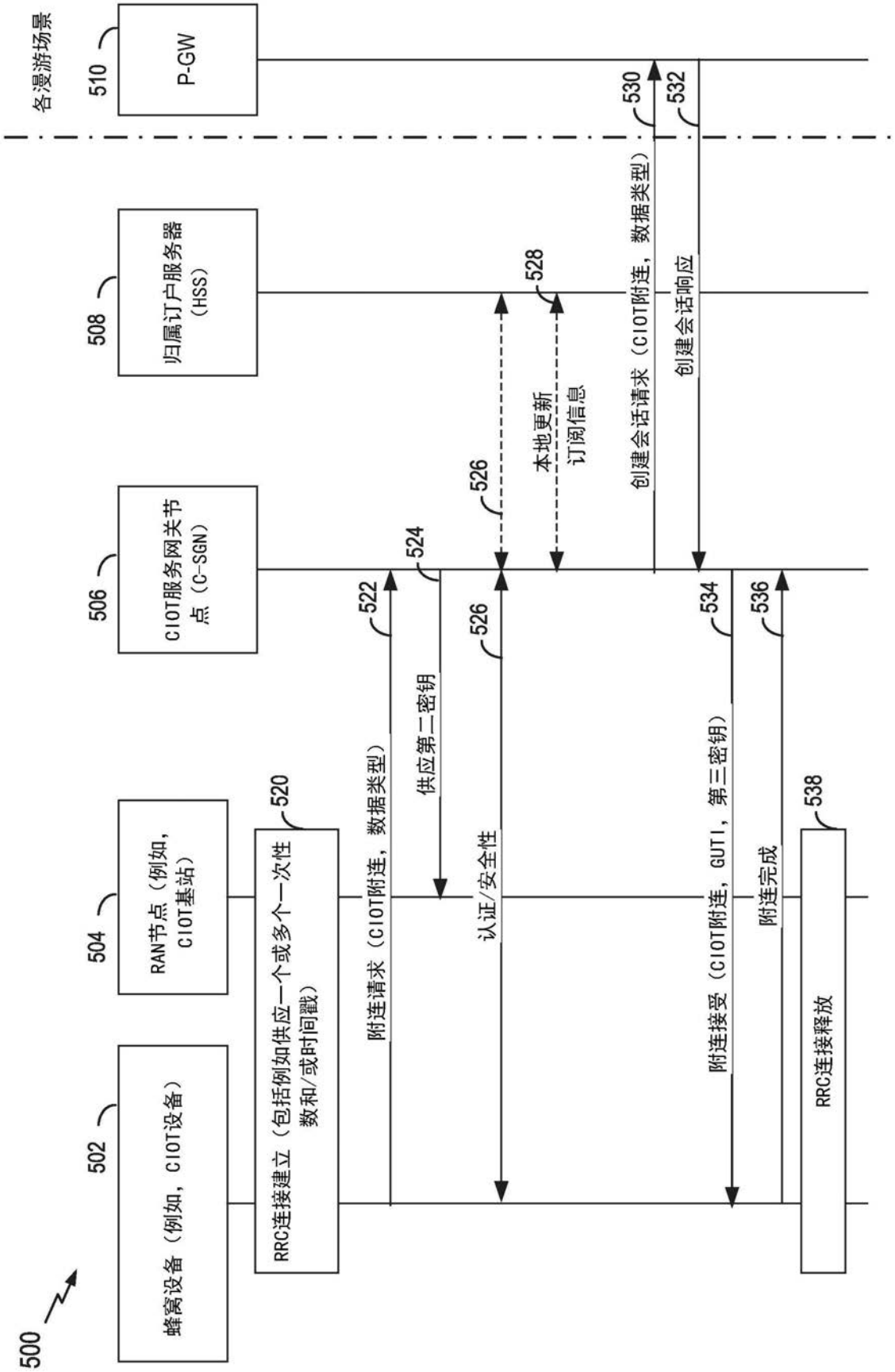

500
蜂窝设备（例如，CIOT设备）
502
RAN节点（例如，CIOT基站）
504
CIOT服务网关节点（C-SGN）
506
归属订户服务器（HSS）
508
P-GW
510
各漫游场景
RRC连接建立（包括例如供应一个或多个一次性数和/或时间戳）
520
附连请求（CIOT附连，数据类型）
522
供应第二密钥
524
认证/安全性
526
本地更新订阅信息
528
创建会话请求（CIOT附连，数据类型）
530
创建会话响应
532
附连接受（CIOT附连，GUTI，第三密钥）
534
附连完成
536
RRC连接释放
538

图5

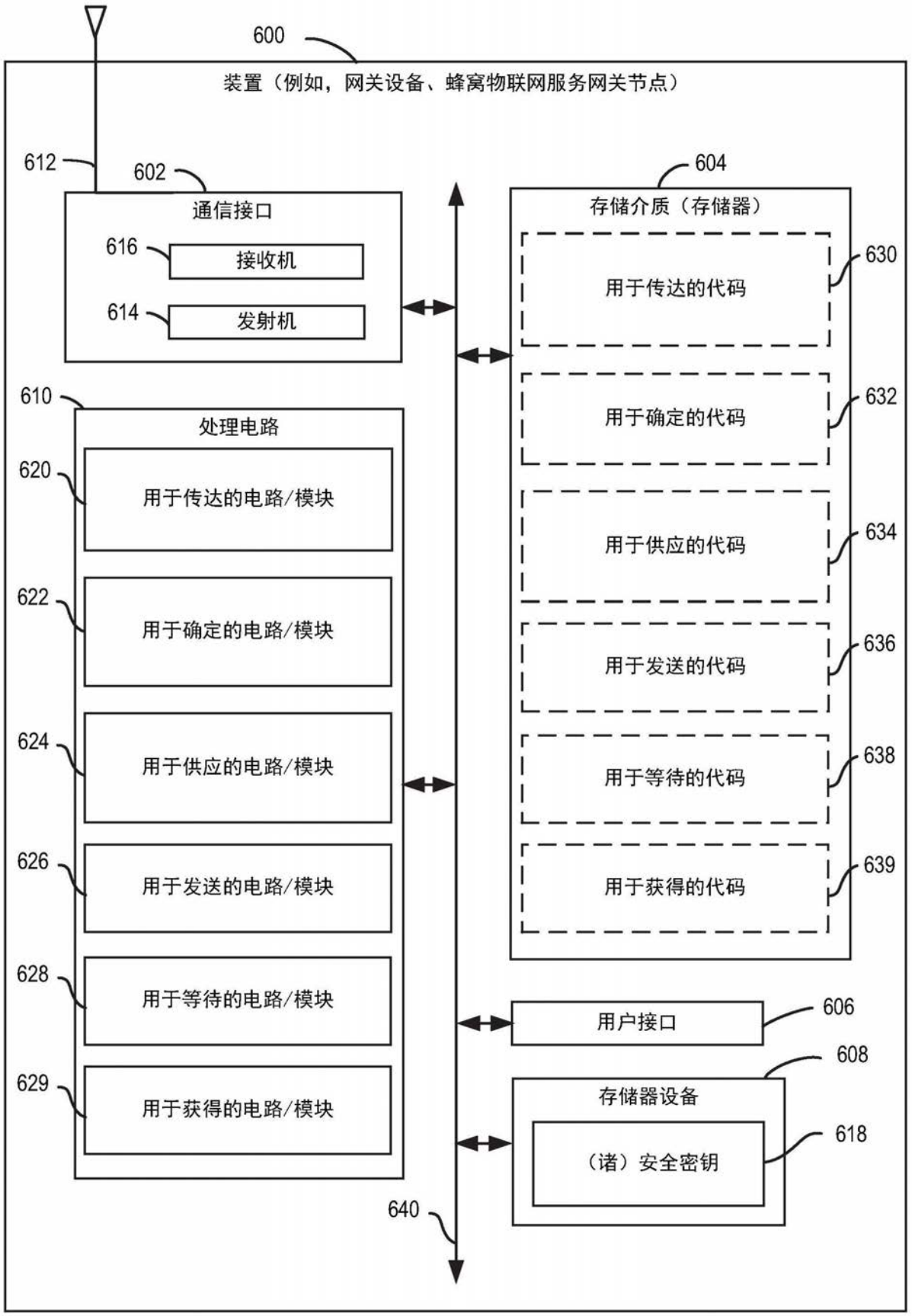

600
装置（例如，网关设备、蜂窝物联网服务网关节点）
612
602
通信接口
616
接收机
614
发射机
604
存储介质（存储器）
630
用于传达的代码
632
用于确定的代码
634
用于供应的代码
636
用于发送的代码
638
用于等待的代码
639
用于获得的代码
610
处理电路
620
用于传达的电路/模块
622
用于确定的电路/模块
624
用于供应的电路/模块
626
用于发送的电路/模块
628
用于等待的电路/模块
629
用于获得的电路/模块
606
用户接口
608
存储器设备
618
（诸）安全密钥
640

图6

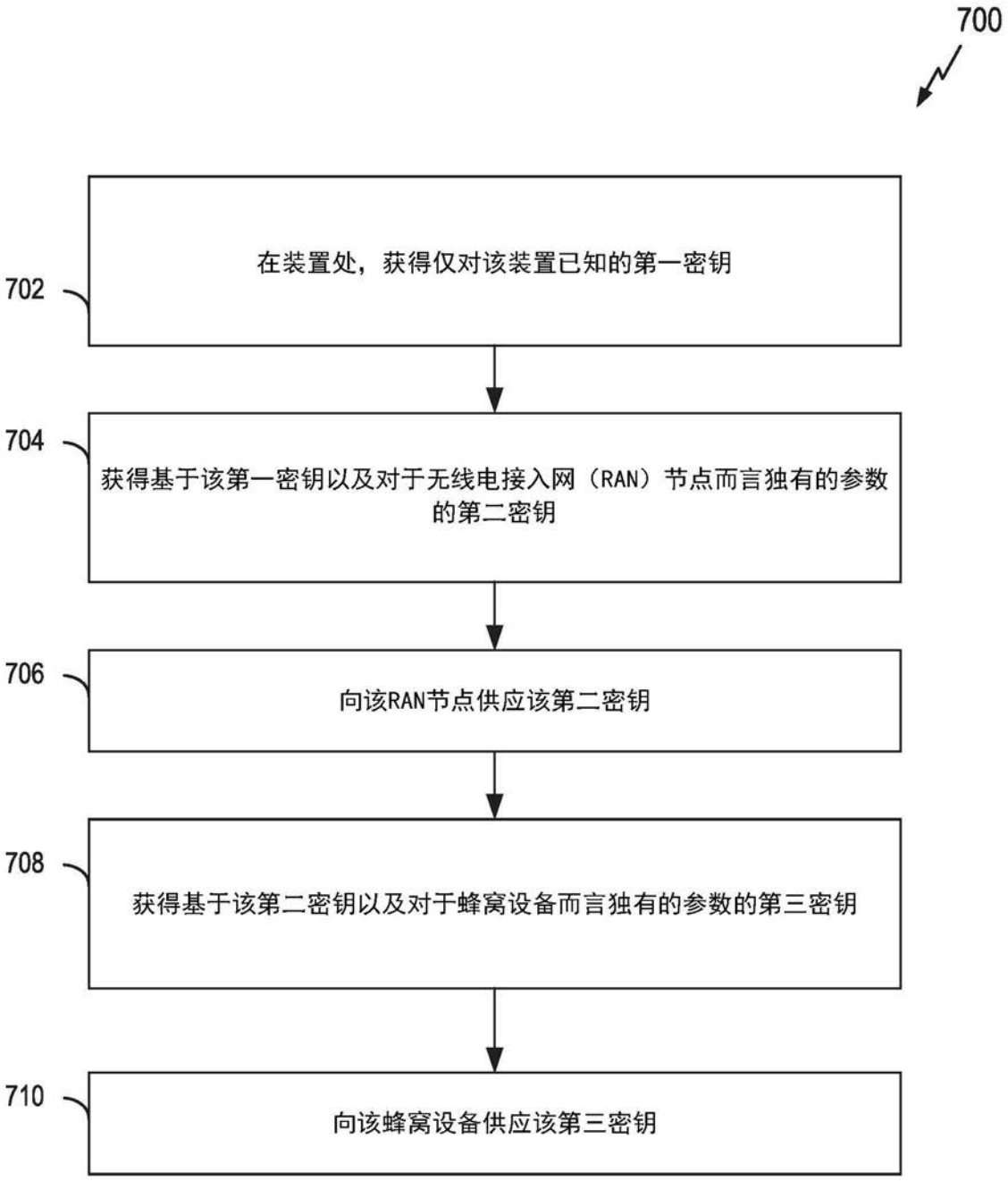

700
702
在装置处，获得仅对该装置已知的第一密钥
704
获得基于该第一密钥以及对于无线电接入网（RAN）节点而言独有的参数的第二密钥
706
向该RAN节点供应该第二密钥
708
获得基于该第二密钥以及对于蜂窝设备而言独有的参数的第三密钥
710
向该蜂窝设备供应该第三密钥

图7

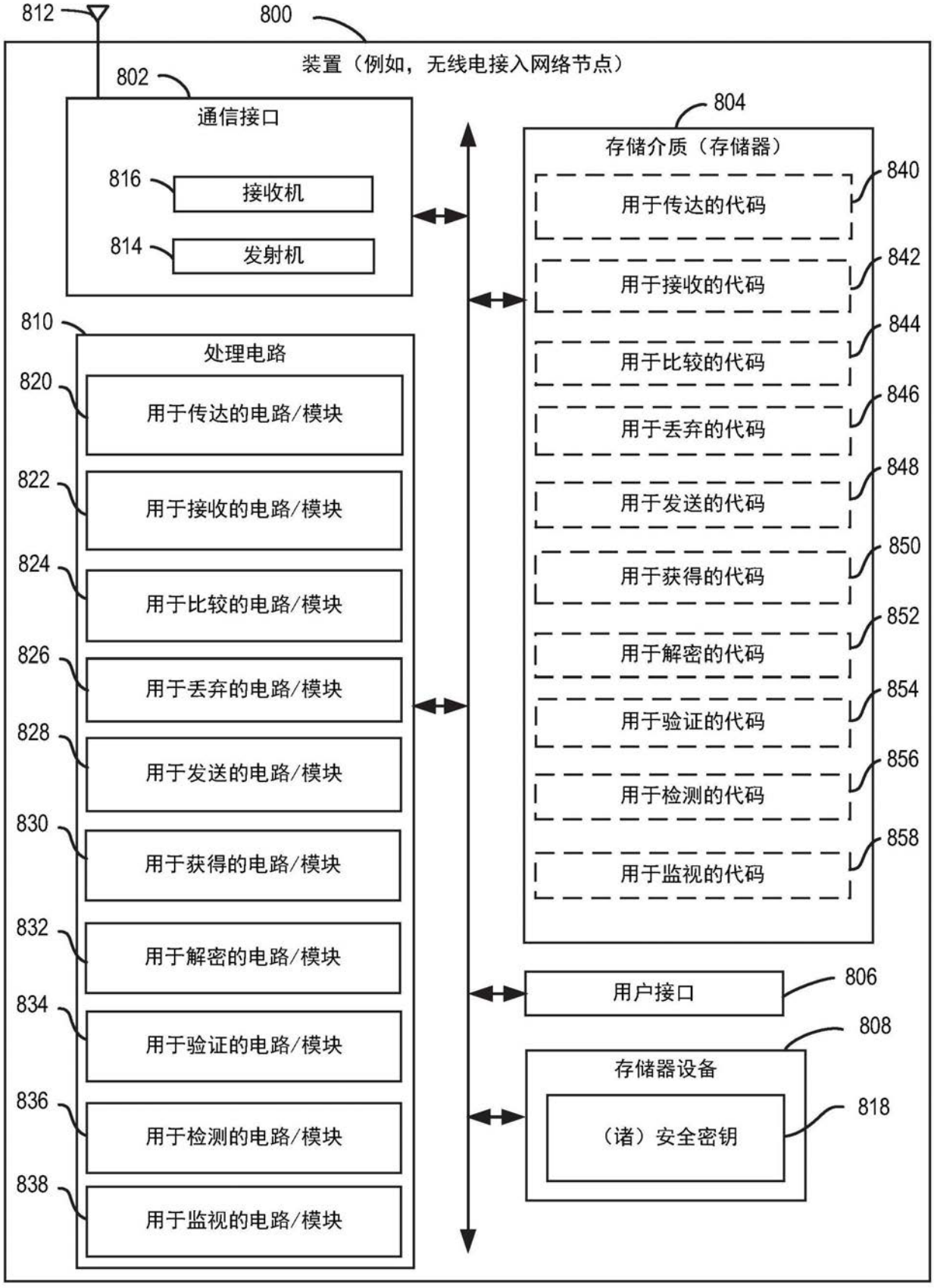

812
800
装置（例如，无线电接入网络节点）
802
通信接口
816
接收机
814
发射机
804
存储介质（存储器）
840
用于传达的代码
842
用于接收的代码
844
用于比较的代码
846
用于丢弃的代码
848
用于发送的代码
850
用于获得的代码
852
用于解密的代码
854
用于验证的代码
856
用于检测的代码
858
用于监视的代码
810
处理电路
820
用于传达的电路/模块
822
用于接收的电路/模块
824
用于比较的电路/模块
826
用于丢弃的电路/模块
828
用于发送的电路/模块
830
用于获得的电路/模块
832
用于解密的电路/模块
834
用于验证的电路/模块
836
用于检测的电路/模块
838
用于监视的电路/模块
806
用户接口
808
存储器设备
818
（诸）安全密钥

图8

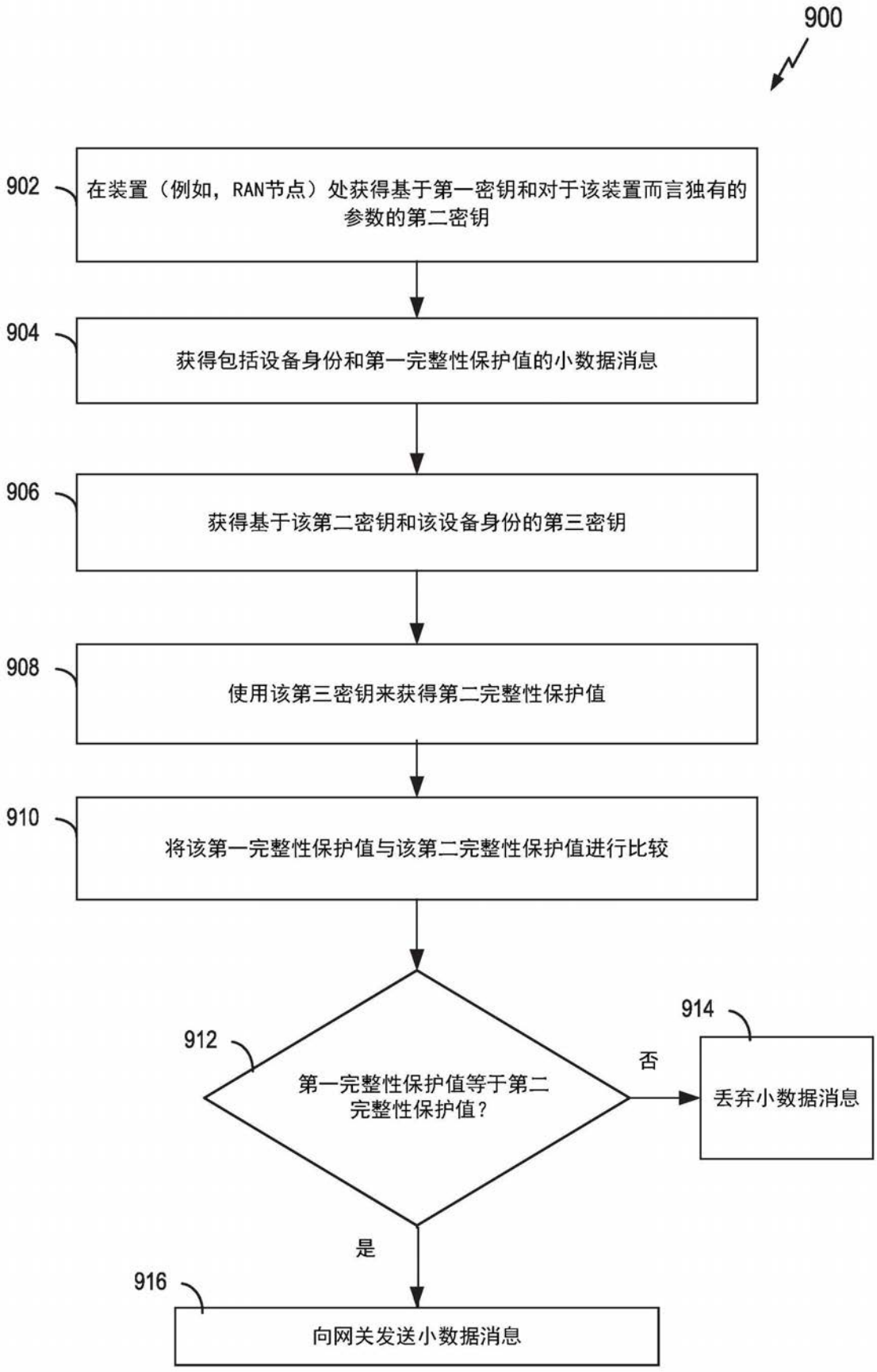

900
902
在装置（例如，RAN节点）处获得基于第一密钥和对于该装置而言独有的参数的第二密钥
904
获得包括设备身份和第一完整性保护值的小数据消息
906
获得基于该第二密钥和该设备身份的第三密钥
908
使用该第三密钥来获得第二完整性保护值
910
将该第一完整性保护值与该第二完整性保护值进行比较
912
第一完整性保护值等于第二完整性保护值？
否
914
丢弃小数据消息
是
916
向网关发送小数据消息

图9

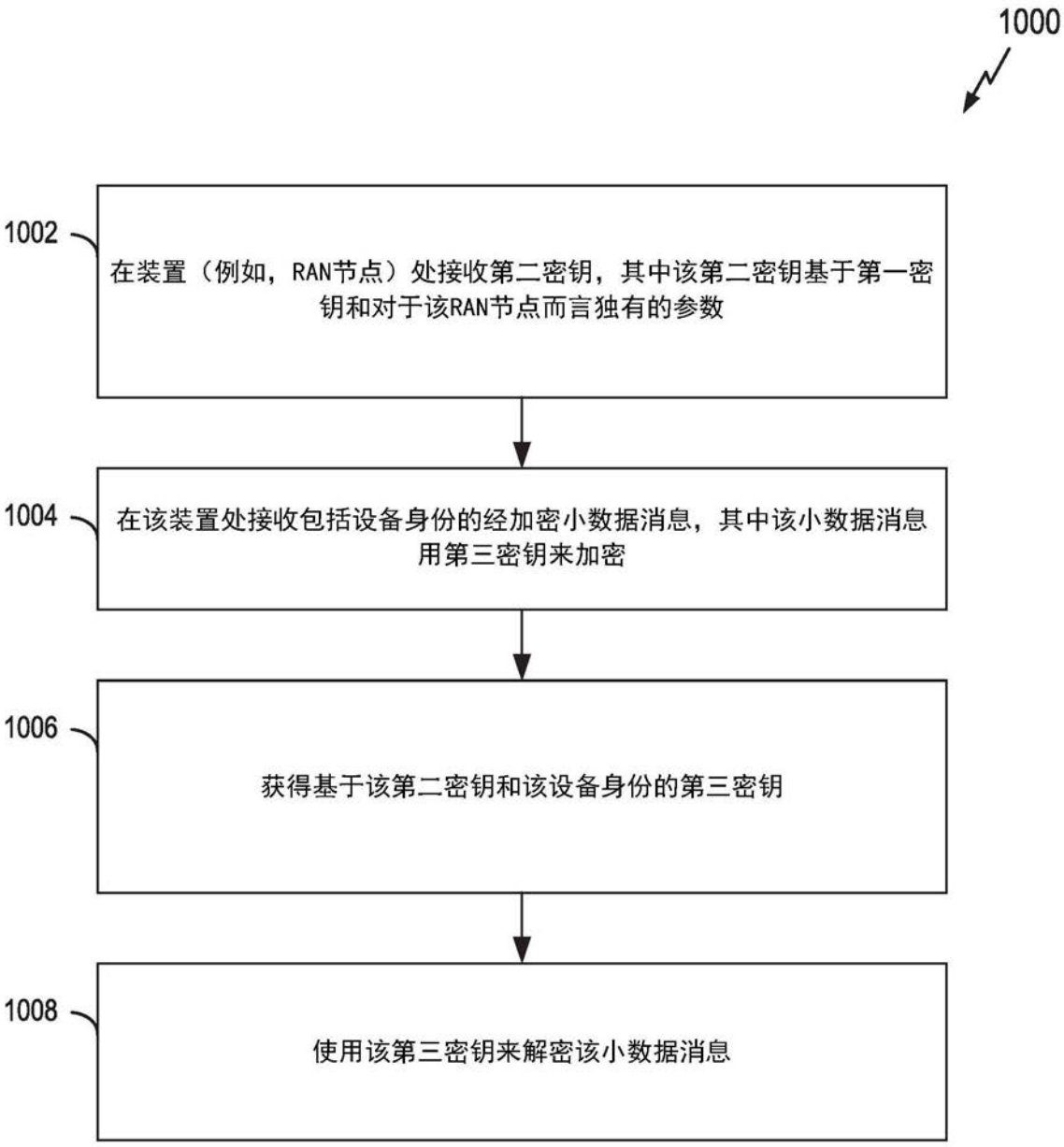

1000
1002
在装置（例如，RAN节点）处接收第二密钥，其中该第二密钥基于第一密钥和对于该RAN节点而言独有的参数
1004
在该装置处接收包括设备身份的经加密小数据消息，其中该小数据消息用第三密钥来加密
1006
获得基于该第二密钥和该设备身份的第三密钥
1008
使用该第三密钥来解密该小数据消息

图10

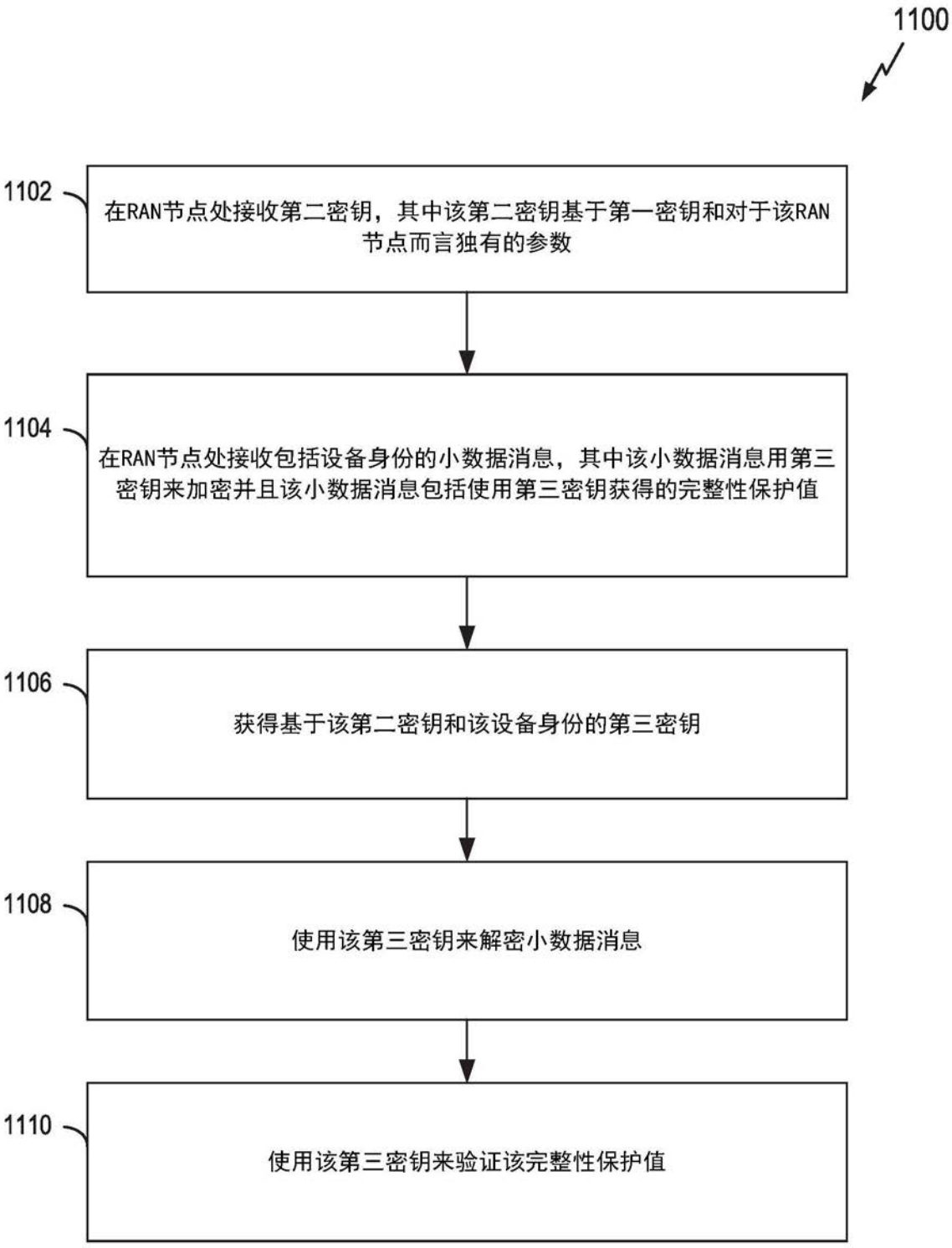

1100
1102
在RAN节点处接收第二密钥，其中该第二密钥基于第一密钥和对于该RAN节点而言独有的参数
1104
在RAN节点处接收包括设备身份的小数据消息，其中该小数据消息用第三密钥来加密并且该小数据消息包括使用第三密钥获得的完整性保护值
1106
获得基于该第二密钥和该设备身份的第三密钥
1108
使用该第三密钥来解密小数据消息
1110
使用该第三密钥来验证该完整性保护值

图11

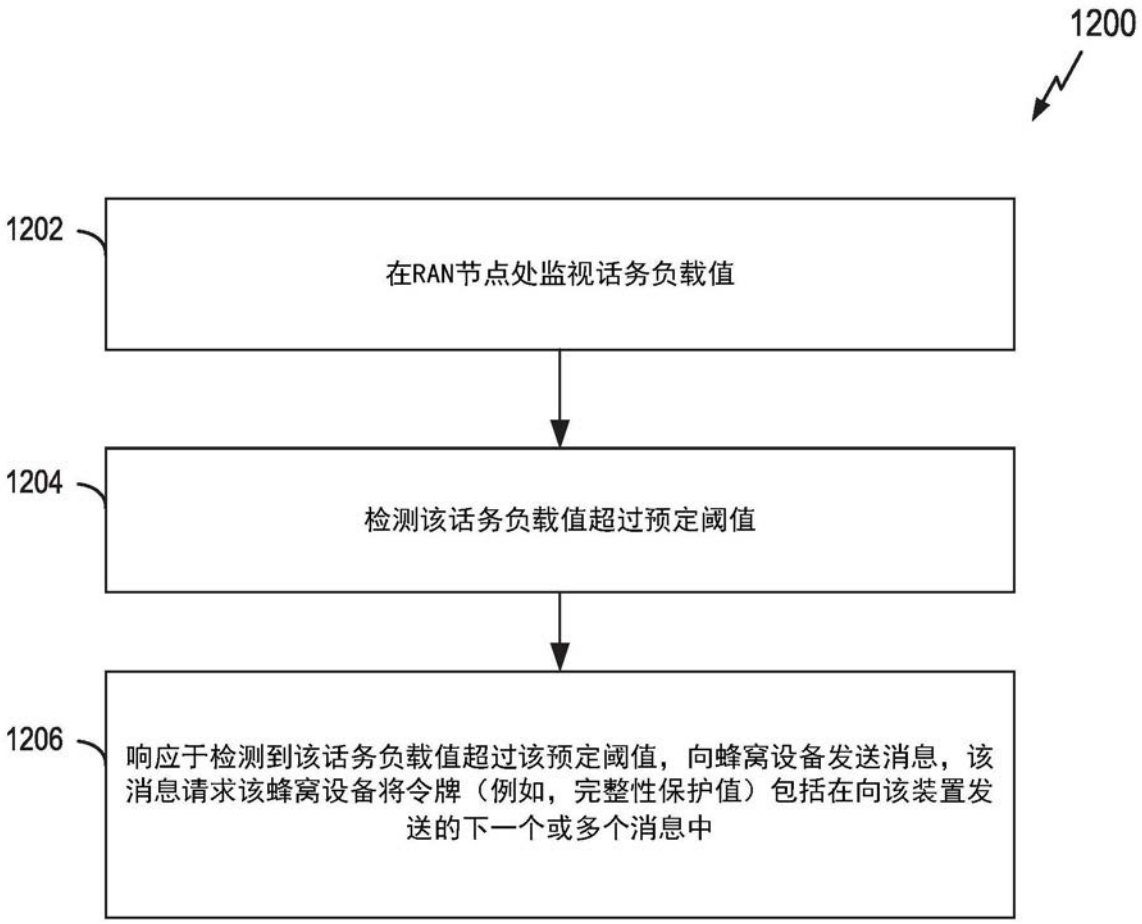

1200
1202
在RAN节点处监视话务负载值
1204
检测该话务负载值超过预定阈值
1206
响应于检测到该话务负载值超过该预定阈值，向蜂窝设备发送消息，该消息请求该蜂窝设备将令牌（例如，完整性保护值）包括在向该装置发送的下一个或多个消息中

图12

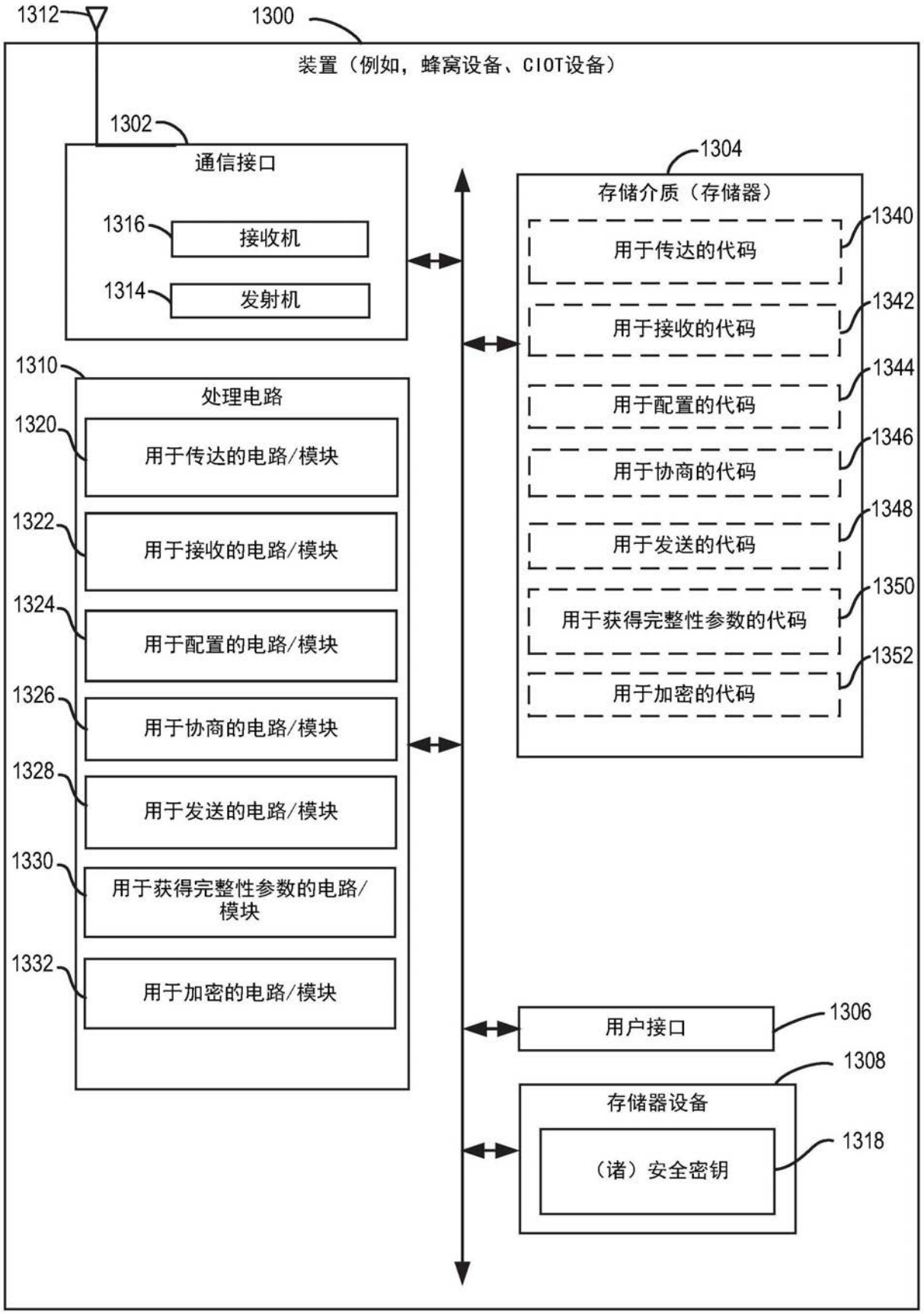

1312
1300
装置（例如，蜂窝设备、CIOT设备）
1302
通信接口
1316
接收机
1314
发射机
1304
存储介质（存储器）
1340
用于传达的代码
1342
用于接收的代码
1344
用于配置的代码
1346
用于协商的代码
1348
用于发送的代码
1350
用于获得完整性参数的代码
1352
用于加密的代码
1310
处理电路
1320
用于传达的电路/模块
1322
用于接收的电路/模块
1324
用于配置的电路/模块
1326
用于协商的电路/模块
1328
用于发送的电路/模块
1330
用于获得完整性参数的电路/模块
1332
用于加密的电路/模块
用户接口
1306
1308
存储器设备
（诸）安全密钥
1318

图13

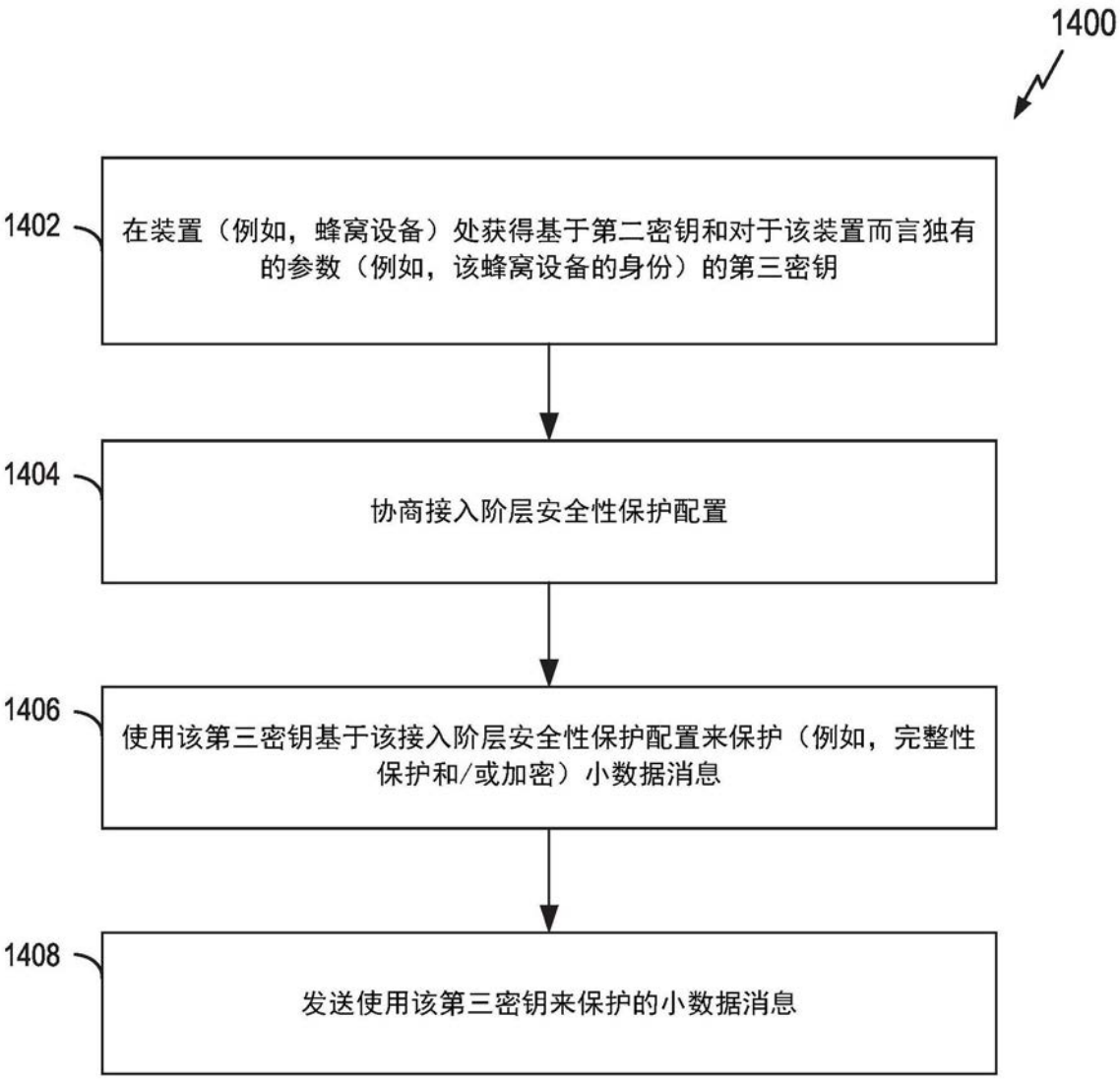

1400
1402
在装置（例如，蜂窝设备）处获得基于第二密钥和对于该装置而言独有的参数（例如，该蜂窝设备的身份）的第三密钥
1404
协商接入阶层安全性保护配置
1406
使用该第三密钥基于该接入阶层安全性保护配置来保护（例如，完整性保护和/或加密）小数据消息
1408
发送使用该第三密钥来保护的小数据消息

图14

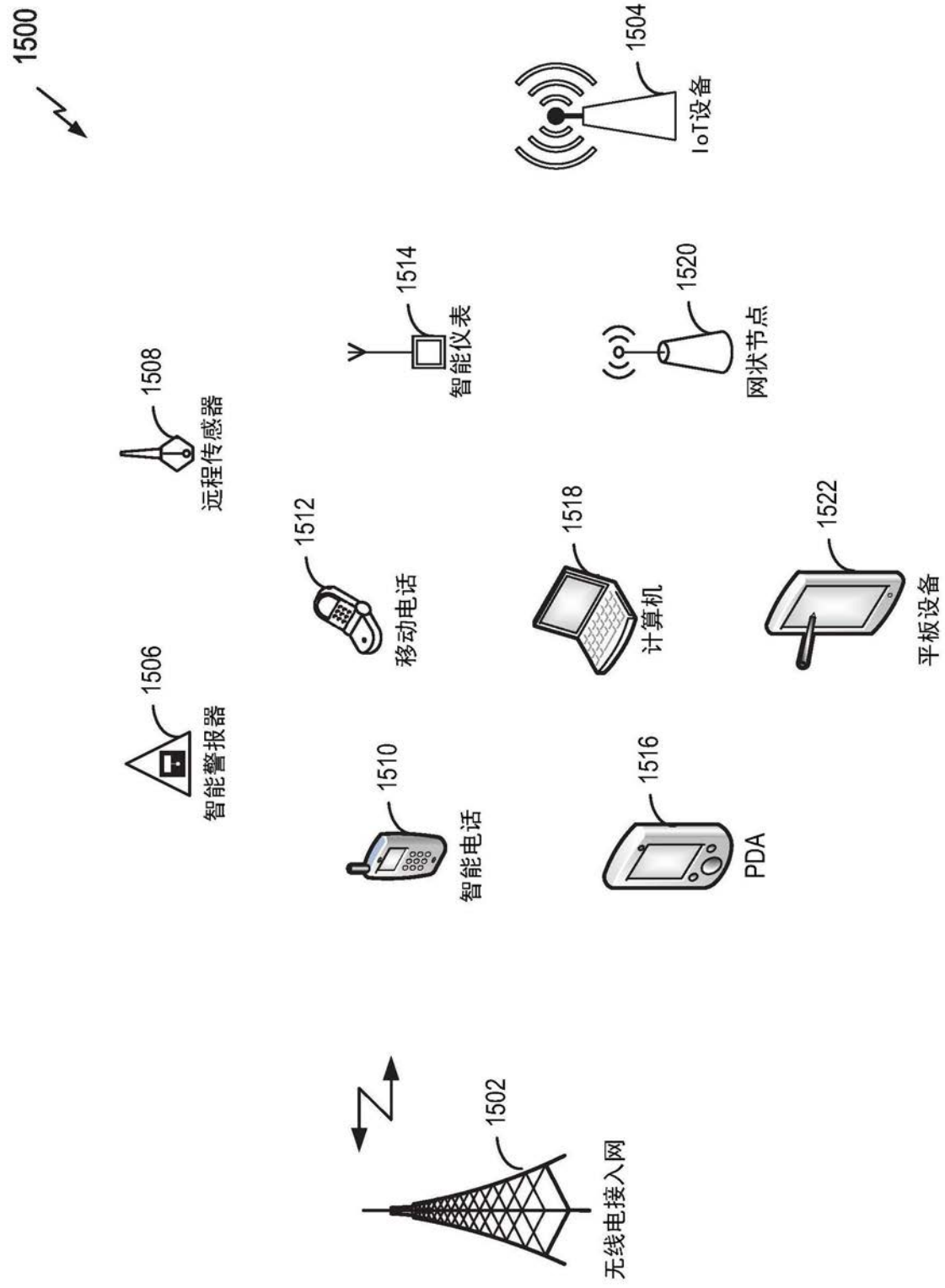

1500
1502
无线电接入网
1504
IoT设备
1506
智能警报器
1508
远程传感器
1510
智能电话
1512
移动电话
1514
智能仪表
1516
PDA
1518
计算机
1520
网状节点
1522
平板设备

图15