(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 107852601 B
(45)授权公告日 2021.05.14

(21)申请号 201680040888.9
(22)申请日 2016.06.13
(65)同一申请的已公布的文献号
申请公布号 CN 107852601 A
(43)申请公布日 2018.03.27
(30)优先权数据
62/191,457 2015.07.12 US
62/320,506 2016.04.09 US
15/160,198 2016.05.20 US
(85)PCT国际申请进入国家阶段日
2018.01.10
(86)PCT国际申请的申请数据
PCT/US2016/037279 2016.06.13
(87)PCT国际申请的公布数据
WO2017/039777 EN 2017.03.09
(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 G·B·霍恩
A·帕拉尼格朗德
A·E·艾斯科特 S·法琴
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李小芳 袁逸
(51)Int.Cl.
H04W 12/033(2021.01)
H04W 12/037(2021.01)
H04W 12/02(2009.01)
H04W 12/041(2021.01)
H04W 12/0431(2021.01)
H04W 40/02(2009.01)
H04L 29/06(2006.01)
H04W 4/70(2018.01)
H04W 68/00(2009.01)
(56)对比文件
CN 104272671 A,2015.01.07
US 2012269167 A1,2012.10.25
US 2014053241 A1,2014.02.20
US 2002184217 A1,2002.12.05
EP 2804441 A1,2014.11.19
US 2013305386 A1,2013.11.14
CN 103297958 A,2013.09.11
审查员 张长梅

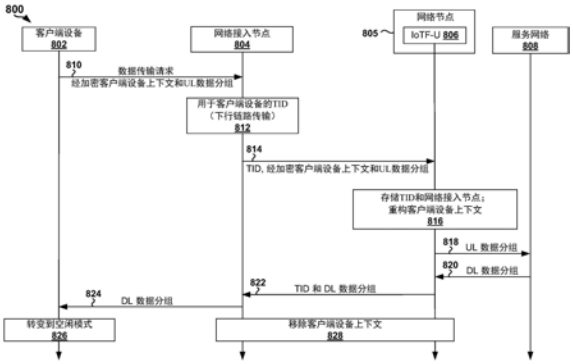
权利要求书6页 说明书48页 附图35页

(54)发明名称

用于具有上下文的网络架构和安全性的方法和装置

(57)摘要

在一方面,网络可支持数个客户端设备。在此类网络中,客户端设备传送要与网络通信的请求,建立安全性上下文,并从网络接收一个或多个经加密客户端设备上下文。经加密客户端设备上下文使得能在网络处重构用于与客户端设备通信的上下文,其中该上下文包括与该客户端设备相关联的网络状态信息。客户端设备向网络传送包括至少一个经加密客户端设备上下文的消息(例如,包括上行链路数据分组)。由于网络设备能够基于经加密客户端设备上下文来重构关于客户端设备的上下文,因此网络设备可以减少在网络设备处维持的上下文量,从而支持更大数目的客户端设备。



CN 107852601 B

1.一种用于客户端设备的方法,包括:

传送要与网络通信的请求;

建立用于与所述网络的连接的安全性上下文,其中所述安全性上下文包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合中的至少一者;

响应于所述请求而从所述网络接收一个或多个经加密客户端设备上下文,其中所述一个或多个经加密客户端设备上下文包括与所述客户端设备相关联的网络状态信息,所述网络状态信息至少包括所述安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息;以及

向所述网络传送包括所述一个或多个经加密客户端设备上下文中的至少一者的消息,其中所述一个或多个经加密客户端设备上下文使得能在所述网络处重构用于与所述客户端设备通信的上下文,所述上下文包括所述网络状态信息。

2.如权利要求1所述的方法,其中所述上下文在所述网络处被移除。

3.如权利要求1所述的方法,进一步包括:

基于所述消息包括数据还是控制信息来确定所述一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文。

4.如权利要求1所述的方法,其中所述经加密客户端设备上下文包括将用于与所述客户端设备的数据相关通信的第一上下文和将用于与所述客户端设备的控制相关通信的第二上下文。

5.如权利要求1所述的方法,其中所述一个或多个经加密客户端设备上下文包括以下至少一者:安全性上下文、承载的服务质量、隧道端点标识符、或其组合。

6.如权利要求1所述的方法,其中所述请求包括关于所述客户端设备正请求所述一个或多个经加密客户端设备上下文的指示。

7.如权利要求1所述的方法,其中所述请求包括对所述客户端设备正请求的服务的指示。

8.如权利要求1所述的方法,其中所述一个或多个经加密客户端设备上下文包括用户面经加密客户端设备上下文和控制面经加密客户端设备上下文,并且其中所述消息包括:

带有所述用户面经加密客户端设备上下文的第一数据分组,或者

带有所述控制面经加密客户端设备上下文的控制分组。

9.如权利要求8所述的方法,其中所述加密密钥是用户面加密密钥且所述完整性保护密钥是用户面完整性保护密钥,其中所述用户面加密密钥和所述用户面完整性保护密钥维持在所述客户端设备处,并且其中所述第一数据分组至少用所述用户面完整性保护密钥来进行完整性保护或用所述用户面加密密钥来加密。

10.如权利要求8所述的方法,其中传送包括所述第一数据分组的所述消息不与所述网络的网络接入节点建立无线电资源控制连接。

11.如权利要求8所述的方法,进一步包括在传送包括所述第一数据分组的所述消息之后立即进入空闲模式。

12.如权利要求8所述的方法,进一步包括:

接收第二数据分组,其中接收所述第二数据分组不与网络接入节点建立无线电资源控制连接。

13.如权利要求12所述的方法，其中所述加密密钥是用户面加密密钥且所述完整性保护密钥是用户面完整性保护密钥，其中所述用户面加密密钥和所述用户面完整性保护密钥维持在所述客户端设备处，并且其中接收所述第二数据分组包括以下至少一者：用所述用户面完整性保护密钥来验证所述第二数据分组，或者用所述用户面加密密钥来解密所述第二数据分组。

14.如权利要求8所述的方法，其中所述控制分组是追踪区域更新。

15.如权利要求1所述的方法，进一步包括：

从所述网络接收寻呼消息。

16.如权利要求1所述的方法，进一步包括：

向所述网络传送带有用户面经加密客户端设备上下文的空分组。

17.如权利要求1所述的方法，其中经加密客户端设备上下文是作为与所述网络的成功认证的结果而从所述网络接收的。

18.如权利要求17所述的方法，其中与所述网络的成功认证不建立接入阶层安全性上下文。

19.如权利要求1所述的方法，进一步包括将所述一个或多个经加密客户端设备上下文存储在本地存储中。

20.如权利要求1所述的方法，其中所述一个或多个经加密客户端设备上下文在所述客户端设备处不被解密，并且其中所述一个或多个经加密客户端设备上下文仅被生成所述一个或多个经加密客户端设备上下文的网络设备解密。

21.如权利要求1所述的方法，其中所述消息进一步包括资源建立请求，所述方法进一步包括：

响应于所述消息而接收用于所述客户端设备的网络地址；以及

向所述网络传送包括所述网络地址的多个数据分组。

22.如权利要求1所述的方法，进一步包括：

向所述网络传送资源释放请求消息，其中所述资源释放请求消息使得所述网络能释放用于所述客户端设备的一个或多个资源。

23.如权利要求1所述的方法，其中在从所述网络接收所述一个或多个经加密客户端设备上下文之后，在所述网络处移除所述上下文。

24.一种客户端设备，包括：

配置成与网络接入节点通信的无线通信电路；以及

耦合至所述无线通信电路的处理电路，所述处理电路被配置成：

传送要与网络通信的请求；

建立用于与所述网络的连接的安全性上下文，其中所述安全性上下文包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合中的至少一者；

响应于所述请求而从所述网络接收一个或多个经加密客户端设备上下文，其中所述一个或多个经加密客户端设备上下文包括与所述客户端设备相关联的网络状态信息，所述网络状态信息至少包括所述安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息；以及

向所述网络传送包括所述一个或多个经加密客户端设备上下文中的至少一者的消息，

其中所述一个或多个经加密客户端设备上下文使得能在所述网络处重构用于与所述客户端设备通信的上下文,所述上下文包括所述网络状态信息。

25.如权利要求24所述的客户端设备,其中所述上下文在所述网络处被移除。

26.如权利要求24所述的客户端设备,其中所述处理电路被进一步配置成:

基于所述消息包括数据还是控制信息来确定所述一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文。

27.如权利要求24所述的客户端设备,其中所述经加密客户端设备上下文包括将用于与所述客户端设备的数据相关通信的第一上下文和将用于与所述客户端设备的控制相关通信的第二上下文。

28.如权利要求24所述的客户端设备,其中所述一个或多个经加密客户端设备上下文包括以下至少一者:安全性上下文、承载的服务质量、隧道端点标识符、或其组合。

29.如权利要求24所述的客户端设备,其中所述处理电路被进一步配置成:

将所述一个或多个经加密客户端设备上下文存储在本地存储中。

30.如权利要求24所述的客户端设备,其中所述一个或多个经加密客户端设备上下文包括用户面经加密客户端设备上下文和控制面经加密客户端设备上下文,并且其中所述消息包括:

带有所述用户面经加密客户端设备上下文的第一数据分组,或者

带有所述控制面经加密客户端设备上下文的控制分组。

31.如权利要求30所述的客户端设备,其中所述加密密钥是用户面加密密钥且所述完整性保护密钥是用户面完整性保护密钥,其中所述用户面加密密钥和所述用户面完整性保护密钥维持在所述客户端设备处,并且其中所述第一数据分组至少用所述用户面完整性保护密钥来进行完整性保护或用所述用户面加密密钥来加密。

32.一种用于网络设备的方法,包括:

从客户端设备接收要与网络通信的请求;

与所述客户端设备建立至少一个上下文,所述至少一个上下文包括与所述客户端设备和所述网络之间的连接相关联的网络状态信息,其中所述网络状态信息至少包括安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息,并且其中所述安全性上下文包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合中的至少一者;

生成一个或多个经加密客户端设备上下文,其中所述一个或多个经加密客户端设备上下文包括所述网络状态信息并且使得能在所述网络处重构用于与所述客户端设备通信的所述至少一个上下文;以及

向所述客户端设备传送所述一个或多个经加密客户端设备上下文。

33.如权利要求32所述的方法,进一步包括确定要生成所述一个或多个经加密客户端设备上下文,其中所述确定基于以下至少一者:所述请求中指示的经加密客户端设备上下文使用信息、所述客户端设备的订阅、策略、或其组合。

34.如权利要求32所述的方法,其中所述经加密客户端设备上下文包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。

35.如权利要求32所述的方法,进一步包括:

向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息;以及

与所述客户端设备执行相互认证。

36.如权利要求32所述的方法，进一步包括：

从所述客户端设备接收控制分组和经加密客户端设备上下文；

验证从所述客户端设备接收的所述经加密客户端设备上下文；

从所述经加密客户端设备上下文重构所述至少一个上下文；

使用所述至少一个上下文来处理所述控制分组，其中所述处理包括以下至少一者：使用所述上下文来验证所述控制分组、解密所述控制分组、或其组合；

存储用于针对所述客户端设备的下行链路分组的临时标识符；以及

将所述控制分组的有效载荷部分转发给应用服务器或分组数据网络网关。

37.如权利要求36所述的方法，其中所述加密密钥至少包括控制面加密密钥、用户面加密密钥、或其组合，并且所述完整性保护密钥至少包括用户面完整性保护密钥、控制面完整性保护密钥、或其组合。

38.如权利要求36所述的方法，其中验证所述经加密客户端设备上下文包括：

确定所述经加密客户端设备上下文是否已期满；

在先前经加密客户端设备上下文已期满时生成一个或多个新的经加密客户端设备上下文；以及

在所述先前经加密客户端设备上下文已期满时将所述一个或多个新的经加密客户端设备上下文传送给所述客户端设备。

39.如权利要求32所述的方法，进一步包括：

从第二客户端设备接收控制分组；

向第二网络设备请求关于所述第二客户端设备的上下文，所述请求包括控制面经加密客户端设备上下文；

从所述第二网络设备接收关于所述第二客户端设备的上下文；

生成新的经加密客户端设备上下文；以及

向所述第二客户端设备传送所述新的经加密客户端设备上下文。

40.如权利要求36所述的方法，其中验证所述经加密客户端设备上下文包括确定用于验证所述经加密客户端设备上下文的密钥。

41.如权利要求32所述的方法，进一步包括：

移除所述至少一个上下文；

从所述客户端设备接收包括资源建立请求以及所述一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息；

响应于所述消息而获得用于所述客户端设备的网络地址；以及

向所述客户端设备传送所述网络地址。

42.如权利要求41所述的方法，进一步包括：

从所述客户端设备接收资源释放请求消息；以及

从所述客户端设备向网关传送所述资源释放请求消息，其中所述资源释放请求消息使得所述网关能释放用于所述客户端设备的一个或多个资源。

43.如权利要求41所述的方法，进一步包括：

当定时器在从所述客户端设备至所述网络的传输之前或在从所述网络至所述客户端

设备的传输之前期满时向网关传送资源释放请求消息，其中所述资源释放请求消息使得所述网关能释放用于所述客户端设备的一个或多个资源。

44.一种网络设备，包括：

配置成与一个或多个网络实体通信的网络通信接口；以及

耦合到所述网络通信接口的处理电路，所述处理电路配置成：

从客户端设备接收要与网络通信的请求；

与所述客户端设备建立至少一个上下文，所述至少一个上下文包括与所述客户端设备和所述网络之间的连接相关联的网络状态信息，其中所述网络状态信息至少包括安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息，并且其中所述安全性上下文包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合中的至少一者；

生成一个或多个经加密客户端设备上下文，其中所述一个或多个经加密客户端设备上下文包括所述网络状态信息并且使得能在所述网络处重构用于与所述客户端设备通信的所述至少一个上下文；以及

向所述客户端设备传送所述一个或多个经加密客户端设备上下文。

45.一种用于网络设备的方法，包括：

获得用于与客户端设备相关联的经加密客户端设备上下文的密钥；

从所述客户端设备接收第一数据分组和所述经加密客户端设备上下文，其中所述经加密客户端设备上下文包括与所述客户端设备相关联的网络状态信息，所述网络状态信息至少包括安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息；

使用所述密钥从所述经加密客户端设备上下文获得所述网络状态信息；

基于所述安全性上下文来解密和验证所述第一数据分组；以及

在所述解密和验证成功时将所述第一数据分组转发给服务网络。

46.如权利要求45所述的方法，其中获得所述网络状态信息包括基于所述密钥来解密所述经加密客户端设备上下文，并且其中所述安全性上下文包括用户面加密密钥、用户面完整性保护密钥、或其组合中的至少一者。

47.如权利要求46所述的方法，其中所述第一数据分组至少用所述用户面完整性保护密钥来验证或用所述用户面加密密钥来解密。

48.如权利要求45所述的方法，其中所述安全性上下文包括用户面加密密钥和用户面完整性保护密钥，所述方法进一步包括：

从服务器或分组数据网络网关接收第二数据分组；

确定所述第二数据分组被转发到的网络接入节点；

向所述第二数据分组添加临时标识符，所述临时标识符使得所述网络接入节点能确定所述客户端设备；

使用所述用户面加密密钥或所述用户面完整性保护密钥来对所述第二数据分组进行加密或完整性保护；以及

将所述第二数据分组转发给所述客户端设备。

49.一种网络设备，包括：

配置成与一个或多个网络实体通信的网络通信接口；以及

耦合到所述网络通信接口的处理电路，所述处理电路配置成：

获得用于与客户端设备相关联的经加密客户端设备上下文的密钥；

从所述客户端设备接收第一数据分组和所述经加密客户端设备上下文，其中所述经加密客户端设备上下文包括与所述客户端设备相关联的网络状态信息，所述网络状态信息至少包括安全性上下文和与用于所述客户端设备的一个或多个承载相关联的信息；

使用所述密钥从所述经加密客户端设备上下文获得所述网络状态信息；

基于所述安全性上下文来解密和验证所述第一数据分组；以及

在所述解密和验证成功时将所述第一数据分组转发给服务网络。

50.如权利要求49所述的网络设备，其中被配置成获得所述网络状态信息的所述处理电路被进一步配置成：

基于所述密钥来解密所述经加密客户端设备上下文，其中所述安全性上下文至少包括用户面加密密钥或用户面完整性保护密钥。

51.如权利要求49所述的网络设备，其中所述安全性上下文包括用户面加密密钥和用户面完整性保护密钥，其中所述处理电路被进一步配置成：

从服务器或分组数据网络网关接收第二数据分组；

确定所述第二数据分组被转发到的网络接入节点；

向所述第二数据分组添加临时标识符，所述临时标识符使得所述网络接入节点能确定所述客户端设备；

使用所述用户面加密密钥或所述用户面完整性保护密钥来对所述第二数据分组进行加密或完整性保护；以及

将所述第二数据分组转发给所述客户端设备。

用于具有上下文的网络架构和安全性的方法和装置

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年7月12日在美国专利商标局提交的临时申请No.62/191,457、于2016年4月9日在美国专利商标局提交的临时申请No.62/320,506、以及于2016年5月20日在美国专利商标局提交的非临时申请No.15/160,198的优先权，以上申请的全部内容通过援引纳入于此。

[0003] 引言

[0004] 公开领域

[0005] 本公开的各方面一般涉及网络通信，尤其但不排他地涉及物联网(IoT)网络架构。

背景技术

[0006] 电子设备收集、处理、以及交换数据的能力在持续增长。不仅如此，这些电子设备中增长数目的电子设备被提供网络连通性。此类能力和特征正使得许多电子设备能演进成物联网(IoT)设备。随着这些类型的电子设备的数目持续快速增加，网络可能没有资源来充分地支持这些电子设备。

[0007] 例如，在IoT环境中，网络(例如，LTE网络)可能需要支持大量(例如，数十亿)IoT设备。由于网络分配用于IoT目的的资源量可能是有限的，因此网络可能无法维持关于这些类型的设备的所有上下文。此外，由于IoT设备可能不频繁地活跃并且具有有限资源，因此这些设备可能无法执行连通性所需的复杂信令。

[0008] 概述

[0009] 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。

[0010] 在一方面，提供了一种用于网络接入节点的方法。该网络接入节点获得用于与客户端设备相关联的经加密客户端设备上下文的密钥，从客户端设备接收第一数据分组和经加密客户端设备上下文，使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文，基于安全性上下文来解密和/或验证第一数据分组，以及在解密和验证成功时将第一数据分组转发给服务网络。在一方面，该网络接入节点通过基于该密钥解密该经加密客户端设备上下文来获得安全性上下文，并且其中该安全性上下文至少包括用户面加密密钥、用户面完整性保护密钥、或其组合。在一方面，第一数据分组至少用该用户面完整性保护密钥来验证或用该用户面加密密钥来解密。在一方面，该安全性上下文包括用户面加密密钥和用户面完整性保护密钥。在此类方面，该网络接入节点可从服务器或分组数据网络网关接收第二数据分组，使用该用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护，以及将第二数据分组转发给客户端设备。该网络接入节点可移除该至少一个上下文。该网络接入节点可从客户端设备接收包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息。该网络

接入节点可响应于该消息而获得用于客户端设备的网络地址。该网络接入节点可向客户端设备传送网络地址。在一方面，该网络接入节点可从客户端设备接收资源释放请求消息并且可将来自客户端设备的资源释放请求消息转发给网关，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在另一方面，当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时，该网络接入节点可向网关传送资源释放请求消息，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在一方面，当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时，该网络接入节点可释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在另一方面，该网络接入节点可从客户端设备接收资源释放请求消息。在此类方面，该网络接入节点可响应于资源释放请求消息而释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。

[0011] 在一方面，提供了一种网络接入节点。该网络接入节点包括：用于获得用于与客户端设备相关联的经加密客户端设备上下文的密钥的装置，用于从客户端设备接收第一数据分组和经加密客户端设备上下文的装置，用于使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文的装置，用于基于安全性上下文来解密和/或验证第一数据分组的装置，以及用于在解密和验证成功时将第一数据分组转发给服务网络的装置。在一方面，用于获得安全性上下文的装置被配置成基于该密钥来解密该经加密客户端设备上下文，并且该安全性上下文至少包括用户面加密密钥、用户面完整性保护密钥、或其组合。在一方面，第一数据分组至少用该用户面完整性保护密钥来验证或用该用户面加密密钥来解密。在一方面，该安全性上下文包括用户面加密密钥和用户面完整性保护密钥。在此类方面，网络接入节点可包括：用于从服务器或分组数据网络网关接收第二数据分组的装置，用于使用该用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护的装置，以及用于将第二数据分组转发给客户端设备的装置。在一方面，该网络接入节点包括用于移除该至少一个上下文的装置。在一方面，该网络接入节点包括用于从客户端设备接收包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息的装置。在一方面，该网络接入节点包括用于响应于该消息而获得用于客户端设备的网络地址的装置。在一方面，该网络接入节点包括用于向客户端设备传送网络地址的装置。在一方面，该网络接入节点包括用于从客户端设备接收资源释放请求消息的装置以及用于将来自客户端设备的资源释放请求消息转发给网关的装置，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在另一方面，该网络接入节点包括用于当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息的装置，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在一方面，该网络接入节点包括用于当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时释放用于该客户端

设备的一个或多个资源的装置。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。在另一方面，该网络接入节点包括用于从客户端设备接收资源释放请求消息的装置。在此类方面，该网络接入节点包括用于响应于资源释放请求消息而释放用于该客户端设备的一个或多个资源的装置。在一方面，该一个或多个资源至少包括用于该客户端设备的网络地址或承载。

[0012] 在一方面，提供了一种用于客户端设备的方法。该客户端设备传送要与网络通信的请求；建立用于与网络的连接的安全性上下文，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；以及响应于该请求而从网络接收一个或多个经加密客户端设备上下文。该客户端设备向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息，其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文，该上下文包括与该客户端设备相关联的网络状态信息。在一方面，该上下文在网络处被移除。在一方面，该客户端设备基于该消息包括数据还是控制信息来确定该一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文。在一方面，该一个或多个经加密客户端设备上下文包括将用于与客户端设备的数据相关通信的第一上下文和将用于与客户端设备的控制相关通信的第二上下文。在一方面，该一个或多个经加密客户端设备上下文包括以下至少一者：安全性上下文、承载的服务质量、隧道端点标识符、或其组合。在一方面，该请求包括关于客户端设备正请求一个或多个经加密客户端设备上下文的指示。在一方面，该请求包括对客户端设备正请求的服务的指示。在一方面，该一个或多个经加密客户端设备上下文包括用户面经加密客户端设备上下文和控制面经加密客户端设备上下文。在此类方面，该消息包括带有用户面经加密客户端设备上下文的第一数据分组或带有控制面经加密客户端设备上下文的控制分组。在一方面，加密密钥是用户面加密密钥且完整性保护密钥是用户面完整性保护密钥，其中该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处，并且其中第一数据分组至少用该用户面完整性保护密钥来进行完整性保护或用该用户面加密密钥来加密。在一方面，传送包括第一数据分组的消息不与网络的网络接入节点建立无线电资源控制连接。在一方面，该客户端设备在传送包括第一数据分组的消息之后立即进入空闲模式。在一方面，该客户端设备接收第二数据分组，其中接收第二数据分组不与网络接入节点建立无线电资源控制连接。在一方面，该加密密钥是用户面加密密钥且该完整性保护密钥是用户面完整性保护密钥，其中该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处，并且其中接收第二数据分组包括以下至少一者：用该用户面完整性保护密钥来验证第二数据分组，或者用该用户面加密密钥来解密第二数据分组。在一方面，控制分组是追踪区域更新。在一方面，该客户端设备从网络接收寻呼消息。在一方面，该客户端设备向网络传送带有用户面经加密客户端设备上下文的空分组。在一方面，作为与网络的成功认证的结果而从网络接收经加密客户端设备上下文。在一方面，与网络的成功认证不建立接入阶层安全性上下文。在一方面，该客户端设备将该一个或多个经加密客户端设备上下文存储在本地存储中。在一方面，该一个或多个经加密客户端设备上下文在客户端设备处不被解密，并且该一个或多个经加密客户端设备上下文仅被生成该一个或多个经加密客户端设备上下文的网络设备解密。在一方面，该消息进一步包括资源建立请求。在此类方面，该客户端设备响应于该消息而接收用于该客户端设备的网络地址，并将包括该网络地址的

多个数据分组传送给网络。在一方面，该客户端设备向网络传送资源释放请求消息，其中资源释放请求消息使得网络能释放用于该客户端设备的一个或多个资源。在一方面，在从网络接收该一个或多个经加密客户端设备上下文之后，该上下文在网络处被移除。

[0013] 在一方面，提供了一种客户端设备。该客户端设备包括：用于传送要与网络通信的请求的装置；用于建立用于与网络的连接的安全性上下文的装置，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；用于响应于该请求而从网络接收一个或多个经加密客户端设备上下文的装置；以及用于向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息的装置，其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与客户端设备通信的上下文，该上下文包括与客户端设备相关联的网络状态信息。在一方面，该上下文在网络处被移除。在一方面，该客户端设备包括用于基于该消息包括数据还是控制信息来确定该一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文的装置。在一方面，该一个或多个经加密客户端设备上下文包括将用于与客户端设备的数据相关通信的第一上下文和将用于与客户端设备的控制相关通信的第二上下文。在一方面，该一个或多个经加密客户端设备上下文包括以下至少一者：安全性上下文、承载的服务质量、隧道端点标识符、或其组合。在一方面，该请求包括关于客户端设备正请求一个或多个经加密客户端设备上下文的指示。在一方面，该请求包括对客户端设备正请求的服务的指示。在一方面，该一个或多个经加密客户端设备上下文包括用户面经加密客户端设备上下文和控制面经加密客户端设备上下文。在此类方面，该消息包括带有用户面经加密客户端设备上下文的第一数据分组或带有控制面经加密客户端设备上下文的控制分组。在一方面，加密密钥是用户面加密密钥且完整性保护密钥是用户面完整性保护密钥，其中该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处，并且其中第一数据分组至少用该用户面完整性保护密钥来进行完整性保护或用该用户面加密密钥来加密。在一方面，传送包括第一数据分组的消息不与网络的网络接入节点建立无线电资源控制连接。在一方面，该客户端设备包括用于在传送包括第一数据分组的消息之后立即进入空闲模式的装置。在一方面，该客户端设备包括用于接收第二数据分组的装置，其中接收第二数据分组不与网络接入节点建立无线电资源控制连接。在一方面，该加密密钥是用户面加密密钥且该完整性保护密钥是用户面完整性保护密钥，其中该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处，并且其中接收第二数据分组包括以下至少一者：用该用户面完整性保护密钥来验证第二数据分组，或者用该用户面加密密钥来解密第二数据分组。在一方面，控制分组是追踪区域更新。在一方面，该客户端设备包括用于从网络接收寻呼消息的装置。在一方面，该客户端设备包括用于向网络传送带有用户面经加密客户端设备上下文的空分组的装置。在一方面，作为与网络的成功认证的结果而从网络接收经加密客户端设备上下文。在一方面，与网络的成功认证不建立接入阶层安全性上下文。在一方面，该客户端设备包括用于将该一个或多个经加密客户端设备上下文存储在本地存储中的装置。在一方面，该一个或多个经加密客户端设备上下文在客户端设备处不被解密，并且其中该一个或多个经加密客户端设备上下文仅被生成该一个或多个经加密客户端设备上下文的网络设备解密。在一方面，该消息进一步包括资源建立请求。在此类方面，该客户端设备包括用于响应于该消息而接收用于该客户端设备的网络地址的装置，以及用于将包括该网络地址的多个数据分组传送给网络的装

置。在一方面，该客户端设备包括用于向网络传送资源释放请求消息的装置，其中资源释放请求消息使得网络能释放用于该客户端设备的一个或多个资源。在一方面，在从网络接收该一个或多个经加密客户端设备上下文之后，该上下文在网络处被移除。

[0014] 在一方面，提供了一种用于客户端设备的方法。该客户端设备传送要与网络通信的请求；建立用于与网络的连接的安全性上下文，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；以及响应于该请求而从网络接收一个或多个经加密客户端设备上下文。该客户端设备向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文的至少一部分，该上下文包括与该客户端设备相关联的网络状态信息。在一方面，该一个或多个经加密客户端设备上下文中的每一者与网络提供的多个服务之一相关联。在一方面，该客户端设备获得消息，其中该消息与网络提供的服务相关联。在此类方面，该客户端设备确定该一个或多个经加密客户端设备上下文中与服务相关联的至少一个经加密客户端设备上下文，其中该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文使得能重构支持该服务的客户端设备上下文部分。例如，该多个服务可包括移动宽带服务、超可靠低等待时间通信(URLLC)服务、高优先级接入服务、耐延迟接入服务、和/或机器型通信(MTC)服务。该客户端设备获得与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息。在一方面，与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面，该使用信息可包括与针对网络提供的服务类型将由网络重构的上下文(或上下文部分)相关联的值(例如，索引号或其他值)。在一方面，该部分上下文被维持在网络处达基于该消息的传输是缩减数据传输还是突发数据传输来确定的时间段。在一方面，该消息包括使用信息。在一方面，该一个或多个经加密客户端设备上下文包括使得能在网络中的第一实体处重构关于该客户端设备的第一上下文的第一用户面经加密客户端设备上下文、以及使得能在网络中的第二实体处重构关于该客户端设备的第二上下文的第二用户面经加密客户端设备上下文。在此类方面，该消息至少包括第一用户面经加密客户端设备上下文和第二用户面经加密客户端设备上下文。

[0015] 在一方面，提供了一种客户端设备。该客户端设备包括：用于传送要与网络通信的请求的装置；用于建立用于与网络的连接的安全性上下文的装置，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；以及响应于该请求而从网络接收一个或多个经加密客户端设备上下文。该客户端设备进一步包括用于向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息的装置。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文的至少一部分，该上下文包括与该客户端设备相关联的网络状态信息。在一方面，该一个或多个经加密客户端设备上下文中的每一者与网络提供的多个服务之一相关联。在一方面，该客户端设备包括用于获得消息的装置，其中该消息与网络提供的服务相关联。在此类方面，该客户端设备包括用于确定该一个或多个经加密客户端设备上下文中与服务相关联的至少一个经加密客户端设备上下文的装置，其中该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文使得能重构支持该服务的客户端设备上下

文部分。例如，该多个服务可包括移动宽带服务、超可靠低等待时间通信(URLLC)服务、高优先级接入服务、耐延迟接入服务、和/或机器型通信(MTC)服务。在一方面，该客户端设备包括用于获得与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息的装置。在一方面，与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面，该使用信息可包括与针对网络提供的服务类型将由网络重构的上下文(或上下文部分)相关联的值(例如，索引号或其他值)。在一方面，该部分上下文被维持在网络处达基于该消息的传输是缩减数据传输还是突发数据传输来确定的时间段。在一方面，该消息包括使用信息。在一方面，该一个或多个经加密客户端设备上下文包括使得能在网络中的第一实体处重构关于该客户端设备的第一上下文的第一用户面经加密客户端设备上下文、以及使得能在网络中的第二实体处重构关于该客户端设备的第二上下文的第二用户面经加密客户端设备上下文。在此类方面，该消息至少包括第一用户面经加密客户端设备上下文和第二用户面经加密客户端设备上下文。

[0016] 在一方面，提供了一种用于网络设备的方法。该网络设备从客户端设备接收要与网络通信的请求；与客户端设备建立至少一个上下文，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中网络状态信息至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；生成一个或多个经加密客户端设备上下文，其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与客户端设备通信的至少一个上下文；以及向客户端设备传送该一个或多个经加密客户端设备上下文。在一方面，该网络设备确定要生成该一个或多个经加密客户端设备上下文，其中该确定基于以下至少一者：该请求中指示的经加密客户端设备上下文使用信息、客户端设备的订阅、策略、或其组合。在一方面，该一个或多个经加密客户端设备上下文包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。在一方面，该网络设备向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息，以及与客户端设备执行相互认证。在一方面，该网络设备从客户端设备接收控制分组和经加密客户端设备上下文；验证从客户端设备接收的经加密客户端设备上下文；从经加密客户端设备上下文重构至少一个上下文；使用该至少一个上下文来处理控制分组，其中该处理包括以下至少一者：使用该上下文来验证控制分组、解密控制分组、或其组合；存储用于针对客户端设备的下行链路分组的临时标识符；以及将控制分组的有效载荷部分转发给应用服务器或分组数据网络网关。在一方面，加密密钥至少包括控制面加密密钥、用户面加密密钥、或其组合，并且完整性保护密钥至少包括用户面完整性保护密钥、控制面完整性保护密钥、或其组合。在一方面，验证经加密客户端设备上下文包括：确定经加密客户端设备上下文是否已期满，在先前经加密客户端设备上下文已期满时生成一个或多个新的经加密客户端设备上下文，以及在先前经加密客户端设备上下文已期满时将该一个或多个新的经加密客户端设备上下文传送给客户端设备。在一方面，该网络设备从第二客户端设备接收控制分组，向第二网络设备请求关于第二客户端设备的上下文，该请求包括控制面经加密客户端设备上下文，从第二网络设备接收关于第二客户端设备的上下文，生成新的经加密客户端设备上下文，以及向第二客户端设备传送新的经加密客户端设备上下文。在一方面，验证经加密客户端设备上下文包括确定用于验证经加密客户端设备上下文的密钥。在一方面，该网络设备移除该至少一个上

下文，从客户端设备接收包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息，响应于该消息而获得用于客户端设备的网络地址，以及向客户端设备传送网络地址。在一方面，该网络设备从客户端设备接收资源释放请求消息并且将来自客户端设备的资源释放请求消息传送给网关，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一方面，当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时，该网络设备向网关传送资源释放请求消息，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。

[0017] 在一方面，提供了一种网络设备。该网络设备包括：用于从客户端设备接收要与网络通信的请求的装置；用于与客户端设备建立至少一个上下文的装置，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中网络状态信息至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合；用于生成一个或多个经加密客户端设备上下文的装置，其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与客户端设备通信的至少一个上下文；以及用于向客户端设备传送该一个或多个经加密客户端设备上下文的装置。在一方面，该网络设备包括用于确定要生成该一个或多个经加密客户端设备上下文的装置，其中该确定基于以下至少一者：该请求中指示的经加密客户端设备上下文使用信息、客户端设备的订阅、策略、或其组合。在一方面，该一个或多个经加密客户端设备上下文包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。在一方面，该网络设备包括用于向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息的装置，以及用于与客户端设备执行相互认证的装置。在一方面，该网络设备包括：用于从客户端设备接收控制分组和经加密客户端设备上下文的装置；用于验证从客户端设备接收的经加密客户端设备上下文的装置；用于从经加密客户端设备上下文重构至少一个上下文的装置；用于使用该至少一个上下文来处理控制分组的装置，其中该处理包括以下至少一者：使用该上下文来验证控制分组、解密控制分组、或其组合；用于存储用于针对客户端设备的下行链路分组的临时标识符的装置；以及用于将控制分组的有效载荷部分转发给应用服务器或分组数据网络网关的装置。在一方面，加密密钥至少包括控制面加密密钥、用户面加密密钥、或其组合，并且完整性保护密钥至少包括用户面完整性保护密钥、控制面完整性保护密钥、或其组合。在一方面，用于验证经加密客户端设备的装置被配置成：确定经加密客户端设备上下文是否已期满，在先前经加密客户端设备上下文已期满时生成一个或多个新的经加密客户端设备上下文，以及在先前经加密客户端设备上下文已期满时将该一个或多个新的经加密客户端设备上下文传送给客户端设备。在一方面，该网络设备包括：用于从第二客户端设备接收控制分组的装置；用于向第二网络设备请求关于第二客户端设备的上下文的装置，该请求包括控制面经加密客户端设备上下文；用于从第二网络设备接收关于第二客户端设备的上下文的装置；用于生成新的经加密客户端设备上下文的装置；以及用于向第二客户端设备传送新的经加密客户端设备上下文的装置。在一方面，用于验证经加密客户端设备上下文的装置被配置成确定用于验证该经加密客户端设备上下文的密钥。在一方面，该网络设备包括：用于移除该至少一个上下文的装置，用于从客户端设备接收包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息的装置，用于响应于该消息而获得用于客户

端设备的网络地址的装置，以及用于向客户端设备传送网络地址的装置。在一方面，该网络设备包括：用于从客户端设备接收资源释放请求消息的装置，以及用于从客户端设备向网关传送资源释放请求消息的装置，其中资源释放请求消息使得网关能释放用于客户端设备的一个或多个资源。在一方面，该网络设备包括用于当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息的装置，其中该资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。

[0018] 在一方面，提供了一种用于网络设备的方法。该网络设备从客户端设备接收要与网络通信的请求。该网络设备与客户端设备建立至少一个上下文，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中网络状态信息至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合。该网络设备可生成一个或多个经加密客户端设备上下文。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的至少一个上下文。该网络设备可向客户端设备传送该一个或多个经加密客户端设备上下文。该网络设备移除该至少一个上下文。该网络设备从客户端设备接收消息，该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息。在一方面，使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面，该网络设备可基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文。在一方面，该网络设备在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段，第二阈值时间段大于第一阈值时间段。

[0019] 在一方面，提供了一种网络设备。该网络设备包括用于从客户端设备接收要与网络通信的请求的装置。该网络设备进一步包括用于与客户端设备建立至少一个上下文的装置，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中网络状态信息至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合。在一方面，该网络设备包括用于生成一个或多个经加密客户端设备上下文的装置。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的至少一个上下文。在一方面，该网络设备包括用于将该一个或多个经加密客户端设备上下文传送给客户端设备的装置。在一方面，该网络设备包括用于移除该至少一个上下文的装置。在一方面，该网络设备包括用于从客户端设备接收消息的装置，该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息。在一方面，使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面，该网络设备包括用于基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文的装置。在一方面，该网络设备包括用于在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段的装置，第二阈值时间段大于第一阈值时间段。

[0020] 在一方面，提供了一种用于网络设备的方法。该网络设备获得用于与客户端设备相关联的经加密客户端设备上下文的密钥，从客户端设备接收第一数据分组和经加密客户端设备上下文，使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下

文，基于该安全性上下文来解密和验证第一数据分组，以及在解密和验证成功时将第一数据分组转发给服务网络。在一方面，该网络设备通过基于该密钥解密该经加密客户端设备上下文来获得安全性上下文，并且其中该安全性上下文至少包括用户面加密密钥、用户面完整性保护密钥、或其组合。在一方面，第一数据分组至少用该用户面完整性保护密钥来验证或用该用户面加密密钥来解密。在一方面，该安全性上下文包括用户面加密密钥和用户面完整性保护密钥。在此类方面，该网络设备从服务器或分组数据网络网关接收第二数据分组，确定第二数据分组被转发到的网络接入节点，向第二数据分组添加临时标识符，该临时标识符使得网络接入节点能确定客户端设备，使用该用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护，以及将第二数据分组转发给客户端设备。

[0021] 在一方面，提供了一种网络设备。该网络设备包括：用于获得用于与客户端设备相关联的经加密客户端设备上下文的密钥的装置，用于从客户端设备接收第一数据分组和经加密客户端设备上下文的装置，用于使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文的装置，用于基于安全性上下文来解密和验证第一数据分组、以及在解密和验证成功时将第一数据分组转发给服务网络的装置。在一方面，用于获得安全性上下文的装置被配置成基于该密钥来解密该经加密客户端设备上下文，并且其中该安全性上下文至少包括用户面加密密钥、用户面完整性保护密钥、或其组合。在一方面，第一数据分组至少用该用户面完整性保护密钥来验证或用该用户面加密密钥来解密。在一方面，该安全性上下文包括用户面加密密钥和用户面完整性保护密钥。在此类方面，该网络设备包括：用于从服务器或分组数据网络网关接收第二数据分组的装置，用于确定第二数据分组被转发到的网络接入节点的装置，用于向第二数据分组添加临时标识符的装置，该临时标识符使得网络接入节点能确定客户端设备，用于使用该用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护的装置，以及用于将第二数据分组转发给客户端设备的装置。

[0022] 在一方面，提供了一种用于网络接入节点的方法。该网络接入节点从客户端设备接收带有要与网络通信的请求的第一数据分组，确定第一数据分组旨在去往的网络节点，从在网络节点处实现的网络功能接收第二数据分组，以及确定第二数据分组将被转发到的客户端设备。在一方面，该网络接入节点存储用于客户端设备的临时标识符，其中该临时标识符是蜂窝小区无线电网络临时标识符(C-RNTI)，并且其中该临时标识符被存储达预定时间段。在一方面，该网络接入节点向第一数据分组添加临时标识符。在一方面，该网络接入节点确定该请求将被转发到的网络功能，其中该确定是在网络接入节点处预配置的，以及将第一数据分组转发给网络功能。在一方面，该网络接入节点移除第二数据分组中的临时标识符，以及将第二数据分组转发给客户端设备。在一方面，该网络接入节点通过从第二数据分组中的临时标识符标识客户端设备来确定第二数据分组将被转发到的客户端设备。

[0023] 在一方面，提供了一种网络接入节点。该网络接入节点包括：用于从客户端设备接收带有要与网络通信的请求的第一数据分组的装置，用于确定第一数据分组旨在去往的网络节点的装置，用于从在网络节点处实现的网络功能接收第二数据分组的装置，以及用于确定第二数据分组将被转发到的客户端设备的装置。在一方面，该网络接入节点包括用于存储用于客户端设备的临时标识符的装置，其中该临时标识符是蜂窝小区无线电网络临时

标识符(C-RNTI),并且其中该临时标识符被存储达预定时间段。在一方面,该网络接入节点包括用于向第一数据分组添加临时标识符的装置。在一方面,该网络接入节点包括用于确定该请求将被转发到的网络功能的装置,其中该确定是在网络接入节点处预配置的;以及用于将第一数据分组转发给网络功能的装置。在一方面,该网络接入节点包括用于移除第二数据分组中的临时标识符的装置,以及用于将第二数据分组转发给客户端设备的装置。在一方面,用于确定第二数据分组将被转发到的客户端设备的装置被配置成从第二数据分组中的临时标识符来标识该客户端设备。

[0024] 本公开的这些和其他方面将在阅览以下详细描述后得到更全面的理解。在结合附图研读了下文对本公开的具体实现的描述之后,本公开的其他方面、特征和实现对于本领域普通技术人员将是明显的。尽管本公开的特征在以下可能是针对某些实现和附图来讨论的,但本公开的所有实现可包括本文所讨论的有利特征中的一个或多个。换言之,尽管可能讨论了一个或多个实现具有某些有利特征,但也可以根据本文讨论的本公开的各种实现使用此类特征中的一个或多个特征。以类似方式,尽管一些实现在下文可能是作为设备、系统或方法实现进行讨论的,但是应该理解,此类实现可以在各种设备、系统、和方法中实现。

[0025] 附图简要说明

[0026] 图1是根据本公开的各个方面的物联网(IoT)网络架构的框图。

[0027] 图2是解说根据本公开的各个方面的用于IoT网络架构的密钥层级的示图。

[0028] 图3是解说根据本公开的各个方面的在IoT网络架构中用于加密上下文的密钥层级的示图。

[0029] 图4是解说关于网络中的客户端设备的各种上下文(例如,网络状态信息)的示图。

[0030] 图5是解说根据本公开的各个方面的由IoT网络架构中的客户端设备进行的初始附连规程的框图。

[0031] 图6是根据本公开的各个方面的由IoT网络架构中的客户端设备进行的附连规程的信号流图。

[0032] 图7是解说根据本公开的各个方面的由IoT网络架构中的客户端设备发起的数据传输的框图。

[0033] 图8是解说根据本公开的各个方面的由IoT网络架构中的客户端设备发起的数据传输的信号流图。

[0034] 图9是根据本公开的各个方面的IoT网络架构中的客户端设备终接数据传输的信号流图。

[0035] 图10是根据本公开的各个方面的IoT网络架构中的示例性资源建立和释放的信号流图。

[0036] 图11是根据本公开的各个方面的由IoT网络架构中的客户端设备进行的示例性附连规程的信号流图。

[0037] 图12是根据本公开的各个方面的IoT网络架构中的示例性资源建立和释放的信号流图。

[0038] 图13是根据本公开的各个方面的用于IoT数据传输的控制面协议栈。

[0039] 图14是解说根据本公开的各个方面的用于IoT数据传输的用户面协议栈的示图。

[0040] 图15是根据本公开的各个方面的分组格式的示图。

[0041] 图16是根据本公开的各个方面的IoT网络架构中的追踪区域更新(TAU)规程的信号流图。

[0042] 图17是根据本公开的各个方面的配置成支持与IoT网络架构中的通信有关的操作的装置的解说。

[0043] 图18(包括图18A和18B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0044] 图19解说了根据本公开的各个方面的用于与网络通信的方法。

[0045] 图20解说了根据本公开的各个方面的用于与网络通信的方法。

[0046] 图21是根据本公开的各个方面的配置成支持与IoT网络架构中的通信有关的操作的装置的解说。

[0047] 图22(包括图22A和22B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0048] 图23(包括图23A和23B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0049] 图24解说了根据本公开的各个方面的用于在IoT网络架构中通信的装置中可操作的方法。

[0050] 图25(包括图25A和25B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0051] 图26(包括图26A和26B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0052] 图27是根据本公开的各个方面的配置成支持与IoT网络架构中的通信有关的操作的装置的解说。

[0053] 图28解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0054] 图29(包括图29A和29B)解说了根据本公开的各个方面的用于在IoT网络架构中通信的方法。

[0055] 详细描述

[0056] 以下结合附图阐述的详细描述旨在作为各种配置的描述,而无意表示可实践本文所描述的概念的仅有配置。本详细描述包括具体细节以提供对各种概念的透彻理解。然而,对于本领域技术人员将显而易见的是,没有这些具体细节也可实践这些概念。在一些实例中,以框图形式示出众所周知的结构和组件以避免淡化此类概念。

[0057] 如以上所讨论的,在IoT环境中,网络(例如,LTE网络)可能需要支持大量(例如,数十亿)客户端设备(也被称为物联网(IoT)设备)。客户端设备可以是蜂窝电话(例如,智能电话)、个人计算机(例如,膝上型计算机)、游戏设备、用户装备(UE)、或配置成与网络(例如,LTE网络)通信的任何其他合适的设备。各客户端设备对于数据传输和安全性可具有不同要求。例如,客户端设备话务(也被称为IoT话务)可以是耐延迟的或者不要求可靠的传输。在另一示例中,客户端设备话务可能不要求接入阶层(AS)安全性以减少开销。

[0058] 常规情况下,当客户端设备从空闲模式转变到连通模式时,可引发信令开销。例如,客户端设备可与网络接入节点(例如,演进型B节点(eNB)、基站、或网络接入点)建立连接,并且网络接入节点可生成关于该客户端设备的上下文。当客户端设备随后进入空闲模

式时,网络接入节点可以不再维持该客户端设备上下文。

[0059] 当客户端设备连接至网络时,网络中关于该客户端设备的上下文可允许该设备执行较少信令以传送数据。例如,注册了的客户端设备可以不被要求执行完整认证规程。然而,为了达成此类效率,网络可能使用大量的资源来维持关于大量的所连接客户端设备中的每一者的一个或多个上下文。

[0060] 如本文所使用的,客户端设备的"上下文"可以指与客户端设备相关联的网络状态信息。例如,上下文可以指客户端设备安全性上下文、与E-UTRAN无线电接入承载(eRAB)相关联的上下文、和/或与无线电承载和S1承载相关联的上下文。

[0061] 由于网络分配用于IoT目的的资源(例如,实现网络功能的装备)量可能是有限的,因此网络功能可能无法维持针对不频繁地活跃的客户端设备的所有上下文(例如,网络状态信息)。例如,一些客户端设备可能每隔10分钟或更久地苏醒,向服务器发送话务(例如,传送数据),并立即进入休眠模式。作为另一示例,一些客户端设备可在发生非预期事件时向服务器发送警告。此外,一些客户端设备可具有有限的资源(例如,存储器、处理器、电池),并且可能不适合处置复杂的协议栈和/或信令规程。

[0062] 长期演进(LTE)移动性管理和会话管理引发太多开销而难以缩放到用于潜在数十亿的客户端设备。具体地,网络节点处的上下文管理和存储可能提出挑战。

[0063] 例如,当客户端设备从空闲模式苏醒并进入连通模式时,网络接入节点经由至移动性管理实体(MME)的服务请求来建立新的客户端设备上下文。当客户端设备处于演进分组系统移动性管理(EMM)注册状态时,该客户端设备上下文可维持在MME和服务网关(S-GW)处。因此,为了支持许多客户端设备,MME和S-GW需要配备有大量存储来维持关于可在大部分时间里保持在空闲模式的客户端设备的上下文。

[0064] 本文所公开的各方面包括用于客户端设备(也被称为物联网(IoT)设备)的网络架构,从较高层的观点而言,该网络架构用于达成超低客户端设备功耗、每蜂窝小区的大量客户端设备、小频谱、和/或蜂窝小区中增加的覆盖区域。引入了专用网络功能以实现独立部署并且去除可缩放性/互通要求。安全性被锚定在IoT网络功能(也被称为IoT功能(IoTF))处。

[0065] 根据各个方面,该架构可允许在网络接入节点(例如,eNB、基站、网络接入点)处没有安全性上下文以向或从客户端设备进行数据传输。为了避免影响正常客户端设备的PDN连接/话务,专用核心网资源被分配用于小数据传输。网络可分配用于接入控制的专用物理(PHY)层资源以便还限制小数据话务。客户端设备上下文被用于小数据传输,以消除在空闲状态期间在IoTF处的关于客户端设备的半永久上下文。为了达成IoT设备的高效数据传输,所公开的网络架构可包括在网络设备处实现的IoTF。此类IoTF可包括控制面IoTF(IoTF-C)和用户面IoTF(IoTF-U)。在一方面,IoTF-C可具有与移动性管理实体相似的功能。在一方面,IoTF-U可以是用户面数据话务的移动性和安全性锚点。在一方面,IoTF-U可具有与服务网关(S-GW)和/或网络接入节点(例如,演进型B节点(eNB)、基站、或网络接入点)相似的功能。

[0066] 为了允许网络功能(例如,IoTF-C、IoTF-U)优化针对客户端设备的资源使用,所公开的IoT网络架构的各个方面可实现设计协议,其中客户端设备上下文携带在分组(例如,IP分组)中且IoTF(例如,包括IoTF-C和IoTF-U的IoTF)伺机创建客户端设备上下文。这使得

网络功能几乎不维持关于客户端设备的网络状态信息且几乎没有信令开销。客户端设备例如可以是蜂窝电话(例如,智能电话)、个人计算机(例如,膝上型计算机)、游戏设备、汽车、电器、或配置成与网络通信的任何其他合适的设备。在一些方面,客户端设备可被称为用户装备(UE)或接入终端(AT)。在一些方面,本文中所引述的客户端设备可以是移动设备或静态设备。应理解,所公开的IoT网络架构和其中所包括的功能可被用于与除了客户端设备以外的设备进行小数据传输。在一方面,客户端设备可具有标称模式——其中它建立连接并传递数据,但是也使用本文所公开的规程以使用客户端设备上下文来传递数据。

[0067] IoT网络架构

[0068] 图1是根据本公开的各个方面的IoT网络架构100的框图。如图1中所示,IoT网络架构100包括客户端设备102(也被称为IoT设备)、网络接入节点104、网络设备105、服务网络110、以及归属订户服务器(HSS)/认证授权记账(AAA)服务器112。在一个方面,网络接入节点104可以是eNB、基站、或网络接入点。

[0069] 在一个方面,网络设备105可包括被配置成实现IoTF的一个或多个处理电路和/或其他恰适硬件。在本公开的一个方面,IoTF可包括控制面IoT功能(IoTF-C)106和用户面IoT功能(IoTF-U)108。例如,IoTF-C 106可在第一网络节点107处实现,而IoTF-U 108可在第二网络节点109处实现。根据本文所公开的各个方面,术语“节点”可表示被包括在网络设备105中的物理实体,诸如处理电路、设备、服务器、或网络实体。相应地,例如,网络节点可被称为网络节点设备。

[0070] 在一个方面,IoTF-C 106和IoTF-U 108可在同一个硬件平台(例如,处理电路和其他相关联的硬件组件,诸如存储器)处实现。在此类方面,例如,IoTF-C 106可在硬件平台(例如,网络设备105)上提供的第一虚拟机(例如,第一操作系统)处实现,而IoTF-U 108可在该硬件平台上提供的第二虚拟机(例如,第二操作系统)处实现。

[0071] 如图1中所示,IoTF-C 106经由第一S1连接116与网络接入节点104处于通信中,而IoTF-U 108经由第二S1连接114与网络接入节点104处于通信中。在一方面,服务网络110可包括被配置成提供各种类型的服务的数个实体、功能、网关、和/或服务器。例如,服务网络110可包括短消息实体(SME)118、机器型通信互通功能(MTC-IWF)120、IoT服务器122、和/或分组数据网络(PDN)网关(P-GW)124。应理解,图1中所公开的服务网络110用作一个示例,而在其他方面,服务网络110可包括与图1中所公开的那些不同类型的实体、功能、和/或服务器。

[0072] 在本公开的一方面,在网络设备105处实现的IoTF可提供控制面和用户面功能性。在一方面,IoTF-C 106处置针对客户端设备的控制面信令(例如,携带控制信息的分组,本文中称为“控制分组”)。例如,IoTF-C 106可执行客户端设备的移动性和会话管理,执行与客户端设备的认证和密钥协定(也被称为AKA规程),和/或可创建关于客户端设备的安全性上下文。在一方面,IoTF-C 106可推导出用于与客户端设备102相关联的控制面话务的控制面(CP)密钥126、用于与客户端设备102相关联的用户面话务的用户面(UP)密钥128、和/或用于生成关于客户端设备102的经加密上下文的上下文密钥130。在一方面,IoTF-C 106可将用户面密钥128和/或至少一个上下文密钥130提供给IoTF-U 108。相应地,在一些方面,IoTF-U 108可包括由IoTF-C 106提供的用户面密钥128和/或上下文密钥130。

[0073] 在一方面,IoTF-U 108可处置客户端设备的用户面话务。例如,IoTF-U 108可推导

出暗码化密钥和完整性密钥(例如,使用UP密钥128的带有关联数据的认证加密(AEAD)密码),在运行中创建客户端设备上下文,认证和解译由客户端设备发送的上行链路分组并将这些上行链路分组转发给PDN或P-GW(例如,P-GW 124),将针对连通客户端设备的下行链路分组进行暗码化和认证并将这些下行链路分组转发给下一跳网络接入节点(例如,eNB),和/或在寻呼期间缓冲针对空闲客户端设备的下行链路分组。在一方面,IoTF-U 108可被认为是数据话务的移动性和安全性锚点。

[0074] 用于IoT网络的示例性密钥层级

[0075] 图2是解说根据本公开的各个方面的用于IoT网络架构(例如,IoT网络架构100)的密钥层级200的示图。在图2中,密钥K_{IoT} 202可以是永久地存储在客户端设备(例如,客户端设备102)的通用移动电信系统(UMTS)订户身份模块(USIM)和网络的认证中心(AuC)中的秘密密钥。完整性密钥(IK)和密码密钥(CK)(在图2中示为IK、CK 204)是在AKA规程期间在AuC和USIM中推导出的密钥对。参照图1,在AKA规程期间,IoTF-C 106可从HSS/AAA服务器112接收认证向量(AV),这些AV包含来自接入安全性管理实体(ASME)的密钥(在图2中示为密钥K_{ASME} 206)。IoTF-C 106可从密钥K_{ASME} 206推导出控制面密钥(K_{CP})208和用户面密钥(K_{UP})214。IoTF-C 106可将密钥K_{UP} 214提供给IoTF-U 108。IoTF-C 106可从密钥K_{CP} 208推导出加密密钥$K_{IoT-CPenc}$ 210和完整性保护密钥$K_{IoT-CPint}$ 212。IoTF-U 108可从密钥K_{UP} 214推导出加密密钥$K_{IoT-UPenc}$ 216和完整性保护密钥$K_{IoT-UPint}$ 218。

[0076] 图3是解说根据本公开的各个方面的用于加密IoT网络架构(例如,IoT网络架构100)中的上下文的密钥层级300的示图。在本公开的一方面,参照图1,IoTF-C 106可基于客户端设备的上下文密钥$K_{CDC-IoTF}$ 302随机地生成用于客户端设备(例如,客户端设备102)的控制面客户端设备上下文加密密钥($K_{CDC-IoTF-C}$)304和用户面客户端设备上下文加密密钥($K_{CDC-IoTF-U}$)306。

[0077] 客户端设备的示例性网络状态

[0078] 在无线通信系统(例如,LTE网络)中,为客户端设备定义用于移动性管理(例如,演进分组系统移动性管理(EMM))的网络状态。此类网络状态实现了客户端设备与网络中的其他实体之间的高效通信。

[0079] 在本公开的一方面,客户端设备(例如,图1中的客户端设备102)可处于注销状态或注册状态。例如,当客户端设备处于注销状态时,该客户端设备的上下文可被存储在HSS中。网络不保持该客户端设备的有效位置或路由信息,并且该客户端设备是不可达的。

[0080] 作为另一示例,客户端设备可通过与网络的成功注册而进入注册状态。在本公开的一方面,客户端设备可通过执行与网络的附连规程来执行此类注册。在注册状态,客户端设备具有至少一个活跃PDN连接。客户端设备还建立了演进分组系统(EPS)安全性上下文。应注意,注销状态和注册状态假定客户端设备具有针对该网络的凭证(例如,在HSS中有可用的订阅)。

[0081] 无线通信网络(例如,LTE网络)可进一步包括为客户端设备定义的用于演进分组系统连接管理(ECM)的网络状态。相应地,处于注册状态的客户端设备(例如,图1中的客户端设备102)可处于两种状态(也被称为注册状态的子状态)之一,诸如空闲状态或连通状态。在空闲状态,客户端设备与其他网络实体之间不存在非接入阶层(NAS)信令连接。另外,客户端设备可执行蜂窝小区选择/重选和公共陆地移动网络(PLMN)选择,并且RAN(例如,网

络接入节点)中可能没有关于该客户端设备的上下文。此外,处于空闲状态的客户端设备可能没有S1-MME和S1-U连接。

[0082] 在连通状态,客户端设备的位置以服务接入网标识符(例如,eNB标识符(ID)、基站ID、或网络接入点ID)的准确度在MME中是已知的。客户端设备的移动性由切换规程来处置。在连通状态,客户端设备与MME之间存在信令连接。该信令连接可由两部分构成:无线电资源控制(RRC)连接和S1-MME连接。

[0083] 图4是解说在网络400中的各种实体处维持的客户端设备的示例网络状态的示图。如图4中所示,网络400包括客户端设备402、网络接入节点404、以及演进分组核心(EPC)406。如图4中进一步所示,EPC 406包括归属订户服务器(HSS)412、移动性管理实体(MME)408、以及分组数据网络网关(P-GW)/服务网关(S-GW)410。在本公开的一方面,网络400可以是4G网络。在其他方面,网络400可以是3G网络、LTE网络、5G网络、或其他恰适网络。

[0084] 例如,参照图4,网络接入节点404可在客户端设备402处于连通状态时维持关于客户端设备402的上下文414(也被称为网络状态信息)。MME 408可在客户端设备402处于连通状态时维持关于客户端设备402的上下文416,以及在客户端设备402处于空闲状态时维持关于客户端设备402的上下文418。P-GW/S-GW 410可在客户端设备402处于连通状态时维持关于客户端设备402的上下文426,以及在客户端设备402处于空闲状态时维持关于客户端设备402的上下文428。HSS 412可在客户端设备402处于连通状态时维持关于客户端设备402的上下文420,在客户端设备402处于空闲状态时维持关于客户端设备402的上下文422,以及在客户端设备402处于注销状态时维持关于客户端设备402的上下文424。在本公开的一方面,如果网络400被实现为3G网络,则P-GW/S-GW 410在客户端设备402处于空闲状态时可以不维持关于客户端设备402的上下文。

[0085] 在本公开的一方面,可生成经加密客户端设备上下文以使网络功能(诸如图1中的IoTF-C 106和IoTF-U 108)实现对关于客户端设备的上下文(也被称为客户端设备上下文)的伺机重构。例如,经加密客户端设备上下文可使得网络实体能在几乎不维持关于客户端设备的网络状态信息的情况下重构客户端设备上下文。因此,经加密客户端设备上下文可使得网络实体能重构客户端设备上下文而无需存储或高速缓存任何网络状态信息。

[0086] 应注意,在存在不频繁地传送话务的潜在数十亿客户端设备的情况下,使网络功能(例如,MME 408、P-GW/S-GW 410)维持关于客户端设备的上下文(包括安全性上下文)是不期望的。而且,经加密客户端设备上下文可消除在切换期间或在从空闲模式转变到连通模式期间在网络接入节点(例如,eNB、基站、或网络接入点)处的信令开销。经加密客户端设备上下文可被用于显著减少或消除信令开销,因为可避免与MME/控制器的通信。

[0087] 用户面经加密客户端设备上下文

[0088] 在本公开的一方面,可针对客户端设备生成用户面(UP)经加密客户端设备上下文。例如,参照图1,用户面经加密客户端设备上下文可在IoTF-U 108处用于上行链路(UL)数据传输。在本公开的一方面,用户面经加密客户端设备上下文可包括承载ID、演进分组系统(EPS)承载服务质量(QoS)、用于用户面通用分组无线电服务(GPRS)隧穿协议(GTP-U)的S5隧道端点标识符(TEID)、IoTF-U 108将UL数据转发至的P-GW网际协议(IP)地址(或等效信息)、安全性上下文(例如,所选加密算法和用户面(UP)密钥128),以及网络向客户端设备提供服务可能需要的任何其他参数、值、设置、或特征。例如,UP密钥128可以是密钥K_{UP} 214,

从密钥K_{UP} 214可推导出密钥$K_{IoT-UPenc}$216和密钥$K_{IoT-UPint}$ 218。可通过使用IoTF-U 108的秘密密钥(诸如图3中所示的密钥$K_{CDC-IoTF-U}$ 306)对关于客户端设备的用户面上下文进行加密来生成用户面经加密客户端设备上下文。在本公开的一方面,IoTF-U 108的秘密密钥(诸如密钥$K_{CDC-IoTF-U}$ 306)可由IoTF-C 106置备。用户面经加密客户端设备上下文可由具有该秘密密钥(例如,密钥$K_{CDC-IoTF-U}$ 306)的IoTF解密。相应地,用户面经加密客户端设备上下文可由生成该用户面经加密客户端设备上下文的IoTF解密。

[0089] 控制面经加密客户端设备上下文

[0090] 可通过对用于控制消息(例如,控制分组或包括控制分组的消息)的控制面客户端设备上下文进行加密来生成控制面(CP)经加密客户端设备上下文。在一方面,控制面经加密客户端设备上下文可包括客户端设备标识符、客户端设备安全性上下文(例如,控制面密钥,诸如密钥K_{IoT}(K_{ASME}等效物)、密钥$K_{IoT-CPenc}$ 210、密钥$K_{IoT-CPint}$ 212)、客户端设备安全性能力(例如,演进分组系统加密算法(EEA)、演进分组系统完整性算法(EIA))、和/或下一跳(S5/S8)配置信息。例如,下一跳配置信息可包括IoT服务器地址、P-GW地址、和/或TEID。例如,参照图1,用于控制消息的控制面客户端设备上下文可用IoTF-C 106的秘密密钥(诸如图3中所示的密钥$K_{CDC-IoTF-C}$ 304)来加密。控制面经加密客户端设备上下文可由具有该秘密密钥(例如,密钥$K_{CDC-IoTF-C}$304)的IoTF解密。相应地,控制面经加密客户端设备上下文可由生成该控制面经加密客户端设备上下文的IoTF解密。

[0091] 初始附连规程

[0092] 图5是解说根据本公开的各个方面的由IoT网络架构500中的客户端设备进行的初始附连规程的框图。在一些方面,如本文所描述的附连规程也被称为网络附连规程或注册规程。

[0093] 如图5中所示,IoT网络架构500包括客户端设备502(也被称为IoT设备)、网络接入节点504(例如,eNB、基站、网络接入点)、网络设备505、服务网络510、以及归属订户服务器(HSS)/认证授权记账(AAA)服务器512。

[0094] 在一个方面,网络设备505可包括被配置成实现IoTF的一个或多个处理电路和/或其他恰适硬件。例如,IoTF可包括控制面IoT功能(IoTF-C)506和用户面IoT功能(IoTF-U)508。在此类方面,IoTF-C 506可在网络节点507处实现,而IoTF-U 508可在网络节点509处实现。在一个方面,IoTF-C 506和IoTF-U 508可在同一个硬件平台处实现,以使得IoTF-C 506和IoTF-U 508各自表示架构500中的独立节点。在此类方面,例如,IoTF-C 506可在硬件平台(例如,网络设备505)上提供的第一虚拟机(例如,第一操作系统)处实现,而IoTF-U 508可在该硬件平台上提供的第二虚拟机(例如,第二操作系统)处实现。

[0095] 如图5中所示,IoTF-C 506经由第一S1连接516与网络接入节点504处于通信中,而IoTF-U 508经由第二S1连接514与网络接入节点504处于通信中。在本公开的一方面,服务网络510可包括被配置成提供各种类型的服务的数个实体、功能、网关、和/或服务器。例如,服务网络510可包括短消息实体(SME)518、机器型通信互通功能(MTC-IWF)520、IoT服务器522、和/或分组数据网络(PDN)网关(P-GW)524。应理解,图5中所公开的服务网络510用作一个示例,而在其他方面,服务网络510可包括与图5中所公开的那些不同类型的实体、功能、和/或服务器。

[0096] 如图5中所示,客户端设备502可向网络传送附连请求532,该附连请求532可由网

络接入节点504接收。在本公开的一方面，附连请求532可提供一个或多个指示。例如，附连请求532可指示：1)客户端设备502将作为IoT设备来附连，2)附连请求532是执行小量(缩减)数据传输的请求，和/或3)客户端设备502正在低功耗模式中操作。附连请求532可进一步指示应当从其检索认证信息的归属域(例如，HPLMN ID或完全合格域名(FQDN))。网络接入节点504可将该请求转发给其所属的IoTF-C 506。

[0097] IoTF-C 506可从由客户端设备502提供的归属域信息确定HSS/AAA服务器512的地址，并且可向HSS/AAA服务器512传送对关于客户端设备502的认证信息的请求534。IoTF-C 506可从HSS/AAA服务器512接收认证信息535。

[0098] IoTF-C 506可与客户端设备502执行相互认证(例如，AKA规程)。在AKA规程期间，IoTF-C 506可通过认证信息535从HSS/AAA服务器512接收AV。例如，AV可包含来自接入安全性管理实体(ASME)的密钥(在图2中示为密钥K_{ASME} 206)。例如，IoTF-C 506可通过信号536将密钥K_{ASME} 206提供给客户端设备502。当AKA规程完成时，IoTF-C 506和客户端设备502可从密钥K_{ASME} 206或从密钥K_{IoT} 202推导出CP密钥526(诸如密钥K_{CP} 208、密钥$K_{IoT-CPenc}$ 210和/或密钥$K_{IoT-CPint}$ 212)，并且可推导出UP密钥528(诸如密钥K_{UP} 214、密钥$K_{IoT-UPenc}$ 216和/或密钥$K_{IoT-UPint}$ 218)。

[0099] 在一些方面，IoTF-C 506可经由消息538将密钥K_{UP} 214以及用户面加密密钥和完整性保护密钥(诸如密钥$K_{IoT-UPenc}$ 216和密钥$K_{IoT-UPint}$ 218)传送给IoTF-U 508。

[0100] 在本公开的一方面，IoTF-C 506可通过使用上下文密钥530加密客户端设备上下文来生成关于客户端设备502的一个或多个经加密客户端设备上下文。IoTF-C 506随后可将该一个或多个经加密客户端设备上下文传送给客户端设备502。例如，IoTF-C 506可生成控制面的经加密客户端设备上下文和用户面的经加密客户端设备上下文。在此类示例中，上下文密钥530可包括用于生成控制面的经加密客户端设备上下文的第一上下文密钥(例如，密钥$K_{CDC-IoTF-C}$304)和用于生成用户面的经加密客户端设备上下文的第二上下文密钥(例如，密钥$K_{CDC-IoTF-U}$ 306)。在本公开的一方面，IoTF-C 506可将一个或多个上下文密钥530提供给IoTF-U 508。例如，IoTF-C 506可经由消息538将用于生成用户面的经加密客户端设备上下文的第二上下文密钥(例如，密钥$K_{CDC-IoTF-U}$ 306)传送给IoTF-U 508。相应地，在一些方面，IoTF-U 508可包括由IoTF-C 506提供的上下文密钥531。

[0101] 图6是根据本公开的各个方面的由IoT网络架构(例如，IoT网络架构100、500)中的客户端设备进行的示例性附连规程的信号流图600。如图6中所示，信号流图600包括客户端设备602(也被称为IoT设备)、网络接入节点604(例如，eNB、基站、或网络接入点)、在网络节点605处实现的IoTF-C 606、在网络节点607处实现的IoTF-U 608、服务网络609、以及归属订户服务器(HSS)610。

[0102] 如图6中所示，客户端设备602可向网络接入节点604传送请求612(例如，RRC连接请求)以与网络通信。客户端设备602可接收RRC连接设立消息614，其可包括信令无线电承载(SRB)配置(例如，用于在专用控制信道(DCCH)上传送NAS消息的SRB1配置)。客户端设备602可向网络接入节点604传送RRC连接设立完成消息616。例如，RRC连接设立完成消息616可指示附连请求。

[0103] 网络接入节点604可向IoTF-C 606传送初始客户端设备消息618。IoTF-C606可从由客户端设备602提供的归属域信息确定HSS服务器610的地址，并且可与HSS 610通信

(621)。例如,IoTF-C 606可向HSS服务器610传送对关于客户端设备602的认证信息的请求,并且可从HSS服务器610接收认证信息。

[0104] 如图6中所示,IoTF-C 606可与客户端设备602执行相互认证(例如,AKA规程620)。在AKA规程620完成时,IoTF-C 606和客户端设备602可从密钥K_{ASME} 206或从密钥K_{IoT} 202推导出控制面密钥,诸如密钥$K_{IoT-CPenc}$ 210和/或密钥$K_{IoT-CPint}$ 212。IoTF-C 606和客户端设备602可进一步从密钥K_{ASME}206或从密钥K_{IoT} 202推导出用户面密钥,诸如密钥$K_{IoT-UPenc}$ 216和/或密钥$K_{IoT-UPint}$ 218。

[0105] 在本公开的一方面,IoTF-C 606可通过使用密钥$K_{CDC-IoTF-C}$ 304对客户端设备602的控制面上下文进行加密来生成控制面经加密客户端设备上下文,和/或可通过使用密钥$K_{CDC-IoTF-U}$ 306对客户端设备602的用户面上下文进行加密来生成用户面经加密客户端设备上下文。IoTF-C 606可经由消息622将一个或多个密钥(例如,用户面密钥,诸如密钥$K_{IoT-UPenc}$ 216和/或密钥$K_{IoT-UPint}$ 218、和/或密钥$K_{CDC-IoTF-U}$ 306)传递给IoTF-U 608。

[0106] IoTF-C 606可向客户端设备602传送带有经加密客户端设备上下文(例如,控制面经加密客户端设备上下文和/或用户面经加密客户端设备上下文)的初始上下文设立请求消息623。因此,经加密客户端设备上下文可包括与IoTF-C606和/或IoTF-U 608相关联的客户端设备上下文,其中该客户端设备上下文可被用于由客户端设备602进行的上行链路数据传输。

[0107] 在本公开的一方面,加密密钥仅为IoTF所知(例如,客户端设备安全性上下文可排他地由IoTF-C 606和/或IoTF-U 608检索)。相应地,在此类方面,加密密钥可以是$K_{CDC-IoTF-U}$ 306,其对于在IoTF外部的网络实体(诸如网络接入节点604或客户端设备602)而言是未知的。在本公开的一方面,每个经加密客户端设备上下文对应于一个数据无线电承载(DRB)。

[0108] 网络接入节点604可向客户端设备602传送RRC连接重配置消息626。在本公开的一方面,RRC连接重配置消息626可包括经加密客户端设备上下文。客户端设备602可向网络接入节点604传送RRC连接重配置完成消息628。

[0109] 客户端设备602可向网络接入节点604传送包括数据分组(例如,UL数据分组)的第一消息630。网络接入节点604可经由第二消息632将该数据分组转发给服务网络609。举例而言,并且如图6中所示,第二消息632可由网络接入节点604和IoTF-U 608转发给服务网络609。

[0110] 服务网络609可将包括数据分组(例如,DL数据分组)的第三消息634传送给客户端设备602。举例而言,并且如图6中所示,第三消息634可由IoTF-U 608和网络接入节点604转发给客户端设备602。客户端设备602随后可转变(636)到空闲模式。网络接入节点604、IoTF-C 606和IoTF-U 608可前进至移除(638)客户端设备上下文。

[0111] IoT上行链路(UL)数据传输

[0112] 图7是解说根据本公开的各个方面的由IoT网络架构700中的客户端设备发起的数据传输的框图。如图7中所示,IoT网络架构700包括客户端设备702(也被称为IoT设备)、网络接入节点704(例如,eNB、基站、网络接入点)、网络设备705、服务网络710、以及归属订户服务器(HSS)/认证授权记账(AAA)服务器712。

[0113] 在一个方面,网络设备705可包括被配置成实现IoTF的一个或多个处理电路和/或

其他恰适硬件。例如，IoTF可包括控制面IoT功能(IoTF-C)706和用户面IoT功能(IoTF-U)708。在此类方面，IoTF-C 706可在网络节点707处实现，而IoTF-U 708可在网络节点709处实现。在一个方面，IoTF-C 706和IoTF-U 708可在同一个硬件平台处实现，以使得IoTF-C 706和IoTF-U 708各自表示架构700中的独立节点。在此类方面，例如，IoTF-C 706可在硬件平台(例如，网络设备705)上提供的第一虚拟机(例如，第一操作系统)处实现，而IoTF-U 708可在该硬件平台上提供的第二虚拟机(例如，第二操作系统)处实现。

[0114] 在本公开的一方面，服务网络710可包括被配置成提供各种类型的服务的数个实体、功能、网关、和/或服务器。例如，服务网络710可包括短消息实体(SME)718、机器型通信互通功能(MTC-IWF)720、IoT服务器722、和/或分组数据网络(PDN)网关(P-GW)724。应理解，图7中所公开的服务网络710用作一个示例，而在其他方面，服务网络710可包括与图7中所公开的那些不同类型的实体、功能、和/或服务器。

[0115] 在图7的一方面，IoTF-C 706可以已生成控制面的经加密客户端设备上下文和用户面的经加密客户端设备上下文。在此类方面，上下文密钥730可包括用于生成控制面的经加密客户端设备上下文的第一上下文密钥(例如，密钥$K_{CDC\text{-}IoTF\text{-}C}$ 304)和用于生成用户面的经加密客户端设备上下文的第二上下文密钥(例如，密钥$K_{CDC\text{-}IoTF\text{-}U}$ 306)。例如，IoTF-C 706可以已将用于生成用户面的经加密客户端设备上下文的第二上下文密钥(例如，密钥$K_{CDC\text{-}IoTF\text{-}U}$ 306)传送给IoTF-U 708。相应地，在此类示例中，IoTF-U 708可包括由IoTF-C 706提供的上下文密钥731，如图7中所示。在图7的该方面，客户端设备702已按照先前所讨论的方式推导出CP密钥726和UP密钥728。

[0116] 如图7中所示，客户端设备702可向网络接入节点704传送包括数据分组和由IoTF-C 706提供的经加密客户端设备上下文的第一消息732。网络接入节点704可从该数据分组中的IoTF-U标识符确定IoTF-U 708的地址，并且可经由第二消息734将该数据分组转发给IoTF-U 708。在一方面，网络接入节点704可在不验证该数据分组的情况下将该分组转发给由客户端设备702指示的下一跳节点(例如，IoTF-U 708)。IoTF-U 708可验证经加密客户端设备上下文并且可使用上下文密钥731(例如，用于生成用户面的经加密客户端设备上下文的密钥$K_{CDC\text{-}IoTF\text{-}U}$ 306)来解密该经加密客户端设备上下文。IoTF-U 708随后可基于经解密的信息来重构客户端设备上下文。IoTF-U 708随后可用加密密钥和完整性密钥(例如，UP密钥728)来解密并验证该数据分组。

[0117] 图8是解说根据本公开的各个方面的由IoT网络架构(例如，IoT网络架构700)中的客户端设备发起的示例性数据传输的信号流图800。如图8中所示，信号流图800包括客户端设备802(也被称为IoT设备)、网络接入节点804(例如，eNB、基站、或网络接入点)、在网络节点805处实现的IoTF-U 806、以及服务网络808。客户端设备802可向网络接入节点804传送包括经加密客户端设备上下文和数据分组(例如，UL数据分组)的数据传输请求消息810。在一方面，数据传输请求消息810可由客户端设备802在不与网络接入节点804建立RRC连接的情况下发送。

[0118] 网络接入节点804在接收到数据传输请求消息810之际可向客户端设备802指派(812)临时标识符(TID)以用于潜在下行链路(DL)话务。例如，TID可以是蜂窝小区无线电网络临时标识符(C-RNTI)。网络接入节点804可确定该数据分组的报头中所包括的IoTF-U标识符。包括此类报头的数据分组的示例格式在本文中参照图12来讨论。

[0119] 网络接入节点804可确定IoTF-U 806的IP地址，并且可经由第一消息814将该数据分组转发给IoTF-U 806。例如，作为运营和维护(OAM)规程的一部分，网络接入节点804可配置有IoTF-U标识符和对应IP地址的集合，或者替换地，网络接入节点804可使用基于IoTF-U ID的域名系统(DNS)查询来确定IoTF-U 806的IP地址。在本公开的一方面，并且如图8中所示，网络接入节点804可在第一消息814中连同该数据分组一起包括TID和经加密客户端设备上下文。在本公开的一方面，TID被存储在网络接入节点804处达预定义时间区间。在此类方面，网络接入节点804可在第一消息814中连同TID一起将TID期满时间传送给IoTF-U 806。IoTF-U 806可解密该经加密客户端设备上下文，并且可重构(816)客户端设备上下文(例如，S5承载)。IoTF-U 806可经由第二消息818将该数据分组转发给服务网络808(例如，服务网络808中的P-GW或服务网络808中的其他实体)。

[0120] 响应于上行链路数据(例如，第二消息818中的UL数据分组)，IoTF-U 806可经由第三消息820从服务网络808(例如，服务网络808中的P-GW或服务网络808中的对应实体)接收数据分组(例如，DL数据分组)。IoTF-U 806可在第四消息822中将接收到的数据分组与TID一起传送给网络接入节点804。网络接入节点804可使用TID来标识客户端设备802并且可在第五消息824中将该数据分组传送给客户端设备802。客户端设备802可基于预配置的定时器转变(826)到空闲模式。网络接入节点804和IoTF-U 806可前进至移除(828)在运行中从经加密客户端设备上下文创建的客户端设备上下文。

[0121] 客户端设备终接数据传输(寻呼)

[0122] 图9是根据本公开的各个方面的IoT网络架构(例如，IoT网络架构100)中的示例性客户端设备终接数据传输的信号流图900。如图9中所示，信号流图900包括客户端设备902(也被称为IoT设备)、网络接入节点904(例如，eNB、基站、网络接入点)、在网络节点905处实现的IoTF-C 906和在网络节点907处实现的IoTF-U 908、P-GW 910、以及IoT服务器912。IoT服务器912可向P-GW 910传送下行链路(DL)消息914，其包括DL数据分组和全局IoTF标识符(GIOTFI)。P-GW 910可基于GIOTFI来定位IoTF-U 908，并且可在转发消息916中将该DL数据分组转发给IoTF-U 908。IoTF-U 908可向IoTF-C 906传送DL数据通知消息918。在本公开的一方面，如果DL数据分组小到足以在寻呼消息中携带，则DL数据通知消息918可包括该DL数据分组。IoTF-C 906可向一个或多个网络接入节点(例如，网络接入节点9014)传送寻呼消息920。网络接入节点904随后可通过传送寻呼消息922来寻呼客户端设备902。

[0123] 客户端设备902可向IoTF-U 908传送包括UL数据分组的RRC连接请求消息924。在本公开的一方面，由客户端设备902传送的UL数据分组可以是空的。网络接入节点904可向客户端设备902指派(926)临时标识符(TID)以用于潜在下行链路(DL)话务。例如，TID可以是蜂窝小区无线电网络临时标识符(C-RNTI)。网络接入节点904然后可在转发消息928中将UL数据分组与TID和经加密客户端设备上下文一起转发给IoTF-U 908。IoTF-U 908可存储(930)该TID和网络接入节点904的ID。

[0124] IoTF-U 908可向IoTF-C 906传送客户端设备响应通知消息932。在本公开的一方面，如果IoTF-U 908不能在DL数据通知消息918中包括DL数据分组，则IoTF-U 908可向客户端设备902传送包括DL数据分组和客户端设备902的TID的消息934。网络接入节点904可在转发消息936中将该DL数据分组转发给客户端设备902。客户端设备902随后可转变(938)到空闲模式。网络接入节点904和IoTF-C 906可移除(940)客户端设备上下文。

[0125] 资源建立和释放

[0126] 图10是根据本公开的各个方面的IoT网络架构(例如,IoT网络架构100)中的示例性资源建立和释放的信号流图1000。如图10中所示,信号流图1000包括客户端设备1002(也被称为IoT设备)、在网络节点1006处实现的IoTF-C1004、在网络节点1010处实现的IoTF-U 1008、以及P-GW 1012。

[0127] 如图10中所示,IoTF-C 1004、IoTF-U 1008、和/或P-GW 1012可移除(1014)关于客户端设备1002的上下文。在一个方面,IoTF-C 1004和/或IoTF-U1008可在IoTF-C 1006已向客户端设备1002提供经加密客户端设备上下文之后移除关于客户端设备1002的上下文。如图10中所示,客户端设备1002可向IoTF-C 1004传送资源建立请求消息1016。例如,在客户端设备1002将向网络(例如,向P-GW 1012)传送不频繁的突发数据传输时,客户端设备1002可传送资源建立请求消息1016。例如,突发数据传输可包括协议数据单元(PDU)(诸如IP分组)的序列。在一方面,资源建立请求消息1016可包括经加密客户端设备上下文(例如,控制面的客户端设备上下文)。

[0128] 在资源建立操作1018期间,IoTF-C 1004可验证来自客户端设备1002的经加密客户端设备上下文,并且在成功验证之际,IoTF-C 1004可解密该经加密客户端设备上下文。IoTF-C 1004随后可重构关于客户端设备1002的上下文。在一方面,IoTF-U 1008和P-GW 1012也可重构关于客户端设备1002的上下文。在一方面,IoTF-C 1004可获得用于客户端设备1002的网络地址(例如,IP地址),并且可在资源建立操作1018期间将该网络地址提供给客户端设备1002。如图10中所示,客户端设备1002可经由IoTF-U 1008向P-GW 1012传送上行链路(UL)数据1020。在一方面,客户端设备1002可在包括客户端设备1002的网络地址的一个或多个PDU中传送UL数据1020。

[0129] 在一个方面,客户端设备1002可确定将不向网络进行进一步的数据传输。在此类方面,客户端设备1002可以可任选地向IoTF-C 1004传送资源释放请求消息1 1022。客户端设备1002随后可进入空闲模式1024。IoTF-C 1004可将资源释放请求消息1 1022传送给P-GW 1012。在一方面,资源释放请求消息11022使得P-GW 1012能释放用于客户端设备1002的一个或多个资源。例如,该一个或多个资源可包括指派给客户端设备1002的网络地址(例如,以允许重新分配该网络地址)、用于客户端设备1002的承载、和/或用于客户端设备1002的其他资源。IoTF-C 1004和IoTF-U 1008随后可移除(1030)关于客户端设备1002的上下文。在另一方面,在IoTF-U 1008处接收到UL数据1020之后,IoTF-C 1004和/或IoTF-U 1008可发起定时器1026。如果定时器1026在从客户端设备1002接收到任何新UL数据(例如,在UL数据1020之后的附加UL数据)之前和/或在向客户端设备1002传送任何下行链路(DL)数据之前期满,则IoTF-C 1004和/或IoTF-U 1008可确定客户端设备1002处于空闲模式1024。在此类场景中,IoTF-C 1004可向P-GW 1012传送资源释放请求消息2 1028。在一方面,资源释放请求消息2 1028使得P-GW 1012能释放用于客户端设备1002的一个或多个资源。例如,该一个或多个资源可包括指派给客户端设备1002的网络地址(例如,以允许重新分配该网络地址)、用于客户端设备1002的承载、和/或用于客户端设备1002的其他资源。IoTF-C 1004和IoTF-U 1008随后可移除(1030)关于客户端设备1002的上下文。在一个方面,当在定时器1026期满之前在IoTF-U 1008处从客户端设备1002接收到新UL数据传输(例如,在UL数据1020之后的附加UL数据)时,定时器1026可被IoTF-C 1004和/或IoTF-U 1008重置。

[0130] 图11是根据本公开的各个方面的由IoT网络架构中的客户端设备进行的示例性附连规程的信号流图1100。如图11中所示，信号流图1100包括客户端设备1102(也被称为IoT设备)、在网络接入节点1104(例如，eNB、基站、或网络接入点)处实现的用户面功能1112、在网络节点1106处实现的控制面功能1114、服务网络1108、以及归属订户服务器(HSS)1110。

[0131] 如图11中所示，客户端设备1102可向网络接入节点1104传送请求1116(例如，RRC连接请求)以与网络通信。客户端设备1102可接收RRC连接设立消息1118，其可包括信令无线电承载(SRB)配置(例如，用于在专用控制信道(DCCH)上传送NAS消息的SRB1配置)。客户端设备1102可向网络接入节点1104传送RRC连接设立完成消息1120。例如，RRC连接设立完成消息1120可指示附连请求。

[0132] 网络接入节点1104可向网络节点1106传送初始客户端设备消息1122。控制面功能1114可从由客户端设备1102提供的归属域信息确定HSS服务器1110的地址，并且可与HSS 1110通信(1126)。例如，控制面功能1114可向HSS服务器1110传送对关于客户端设备1102的认证信息的请求，并且可从HSS服务器1110接收认证信息。

[0133] 如图11中所示，控制面功能1114可与客户端设备1102执行相互认证(诸如AKA规程1124)。在AKA规程1124完成时，控制面功能1114和客户端设备1102可从密钥K_{ASME} 206或从密钥K_{IoT} 202推导出控制面密钥，诸如密钥$K_{IoT\text{-}CPenc}$ 210和/或密钥$K_{IoT\text{-}CPint}$ 212。控制面功能1114和客户端设备1102可进一步从密钥K_{ASME} 206或从密钥K_{IoT} 202推导出用户面密钥，诸如密钥$K_{IoT\text{-}UPenc}$ 216和/或密钥$K_{IoT\text{-}UPint}$ 218。

[0134] 在本公开的一方面，控制面功能1114可通过使用密钥$K_{CDC\text{-}IoTF\text{-}C}$ 304对客户端设备1102的控制面上下文进行加密来生成控制面经加密客户端设备上下文，和/或可通过使用密钥$K_{CDC\text{-}IoTF\text{-}U}$ 306对客户端设备1102的用户面上下文进行加密来生成用户面经加密客户端设备上下文。

[0135] 控制面功能1114可向客户端设备1102传送带有经加密客户端设备上下文(例如，控制面经加密客户端设备上下文和/或用户面经加密客户端设备上下文)的初始上下文设立请求消息1128。因此，经加密客户端设备上下文可包括与控制面功能1114和/或用户面功能1112相关联的客户端设备上下文，其中该客户端设备上下文可被用于由客户端设备1102进行的上行链路数据传输。在一方面，控制面功能1114可经由消息1128将一个或多个密钥(例如，用户面密钥，诸如密钥$K_{IoT\text{-}UPenc}$ 216和/或密钥$K_{IoT\text{-}UPint}$ 218、和/或密钥$K_{CDC\text{-}IoTF\text{-}U}$ 306)传递给用户面功能1112。

[0136] 在本公开的一方面，加密密钥仅为用户面功能1112和/或控制面功能1114所知(例如，客户端设备安全性上下文可排他地由用户面功能1112和/或控制面功能1114检索)。在此类方面，例如，加密密钥可以是K_{CDC}-IoTF-U 306。在本公开的一方面，每个经加密客户端设备上下文对应于一个数据无线电承载(DRB)。

[0137] 网络接入节点1104可向客户端设备1102传送RRC连接重配置消息1130。在本公开的一方面，RRC连接重配置消息1130可包括经加密客户端设备上下文。客户端设备1102可向网络接入节点1104传送RRC连接重配置完成消息1132。

[0138] 客户端设备1102可向网络接入节点1104传送包括数据分组(例如，UL数据分组)的第一消息1134。在网络接入节点1104处实现的用户面功能1112可将该数据分组转发给服务网络1108。服务网络1108可将包括数据分组(例如，DL数据分组)的第二消息1136传送给客

户端设备1102。举例而言，并且如图11中所示，第二消息1136可由网络接入节点1104处的用户面功能1112转发给客户端设备1102。客户端设备1102随后可转变(1138)到空闲模式。网络接入节点1104和网络节点1106可前进至移除(1140)客户端设备上下文。

[0139] 图12是根据本公开的各个方面的IoT网络架构中的示例性资源建立和释放的信号流图1200。如图12中所示，信号流图1200包括客户端设备1202(也被称为IoT设备)、在网络接入节点1204处实现的用户面功能1210、在网络节点1206处实现的控制面功能1212、以及P-GW 1208。在一方面，图12的网络接入节点1204、用户面功能1210、网络节点1206、以及控制面功能1212可分别对应于图11的网络接入节点1104、用户面功能1112、网络节点1106、以及控制面功能1114。

[0140] 如图12中所示，网络接入节点1204、网络节点1206、和/或P-GW 1208可移除(1214)关于客户端设备1202的上下文。在一个方面，网络接入节点1204和/或网络节点1206可在控制面功能1212已向客户端设备1202提供经加密客户端设备上下文之后移除关于客户端设备1202的上下文。如图12中所示，客户端设备1202可向网络接入节点1204传送资源建立请求1216。例如，在客户端设备1202将向网络(例如，向P-GW 1208)传送不频繁的突发数据传输时，客户端设备1202可传送资源建立请求1216。例如，突发数据传输可包括协议数据单元(PDU)(诸如IP分组)的序列。在一方面，资源建立请求1216可包括经加密客户端设备上下文(例如，控制面的客户端设备上下文)。

[0141] 在资源建立操作1218期间，控制面功能1212可验证来自客户端设备1202的经加密客户端设备上下文，并且在成功验证之际，控制面功能1212可解密该经加密客户端设备上下文。控制面功能1212随后可重构关于客户端设备1202的上下文。在一方面，用户面功能1210和P-GW 1208也可重构关于客户端设备1202的上下文。在一方面，控制面功能1212可获得用于客户端设备1202的网络地址(例如，IP地址)，并且可在资源建立操作1218期间将该网络地址提供给客户端设备1202。如图12中所示，客户端设备1202可经由网络接入节点1204向P-GW 1208传送上行链路(UL)数据1220。在一方面，客户端设备1202可在包括客户端设备1202的网络地址的一个或多个PDU中传送UL数据1220。

[0142] 在一个方面，客户端设备1202可确定将不向网络进行进一步的数据传输。在此类方面，客户端设备1202可以可任选地向网络接入节点1204传送资源释放请求消息1 1222。客户端设备1202随后可进入空闲模式1224。如图12中所示，网络接入节点1204可经由网络节点1206将资源释放请求消息1 1222传送给P-GW 1208。在一方面，资源释放请求消息1 1222使得P-GW 1208能释放用于客户端设备1202的一个或多个资源。例如，该一个或多个资源可包括指派给客户端设备1202的网络地址(例如，以允许重新分配该网络地址)、用于客户端设备1202的承载、和/或用于客户端设备1202的其他资源。控制面功能1212和用户面功能1210随后可移除(1232)关于客户端设备1202的上下文。在另一方面，在接收到UL数据1220之后，用户面功能1210和/或控制面功能1212可发起定时器1226。如果定时器1226在从客户端设备1202接收到任何新UL数据(例如，在UL数据1220之后的附加UL数据)之前和/或在向客户端设备1202传送任何下行链路(DL)数据之前期满，则控制面功能1212和/或用户面功能1210可确定客户端设备1202处于空闲模式1224。在此类场景中，根据一个方面，用户面功能1210可经由网络节点1206向P-GW 1208传送资源释放请求消息2 1228。替换地，根据另一方面，控制面功能1212可向P-GW 1208传送资源释放请求消息3 1230。在一方面，资源

释放请求消息21228或资源释放请求消息3 1230使得P-GW 1208能释放用于客户端设备1202的一个或多个资源。例如，该一个或多个资源可包括指派给客户端设备1202的网络地址(例如，以允许重新分配该网络地址)、用于客户端设备1202的承载、和/或用于客户端设备1202的其他资源。控制面功能1212和用户面功能1210随后可移除(1232)关于客户端设备1202的上下文。在一个方面，当在定时器1226期满之前在用户面功能1210处从客户端设备1202接收到新UL数据传输(例如，在UL数据1220之后的附加UL数据)时，定时器1226可被控制面功能1212和/或用户面功能1210重置。

[0143] 控制面协议栈

[0144] 图13是解说根据本公开的各个方面的用于IoT数据传输的控制面协议栈1300的示图。如图13中所示，协议栈1300可包括客户端设备协议栈1302(也被称为IoT设备协议栈)、网络接入节点协议栈1304、在网络节点1305处实现的IoTF协议栈1306、以及服务网络协议栈1308。例如，网络接入节点协议栈1304可以在eNB、基站、或网络接入点中实现。作为另一示例，服务网络协议栈1308可以在P-GW中实现。如图13中所示，客户端设备协议栈1302可包括物理(PHY)层1310、媒体接入控制(MAC)层1312、无线电链路控制(RLC)层1314、分组数据汇聚协议(PDCP)层1316、以及控制(Ctrl)层1320。如图13中进一步所示，客户端设备协议栈1302可实现用于传达控制面经加密客户端设备上下文(在图13中缩写为“CDC_{CP}”)的上下文协议层1318。上下文协议层1318可进一步使得能传达指示存在经加密客户端设备上下文的IoTF ID(IID)和/或安全性报头(在图13中缩写为“Sec”)。

[0145] 如图13中所示，网络接入节点协议栈1304可包括PHY层1322、MAC层1324、RLC层1326、以及PDCP层1328，其分别与客户端设备协议栈1302的PHY层1310、MAC层1312、RLC层1314、以及PDCP层1316对接。网络接入节点协议栈1304可进一步包括以太网层1330、MAC层1332、网际协议(IP)层1334、用户数据报协议(UDP)层1336、以及控制面GPRS隧穿协议(GTP-C)层1338。

[0146] 如图13中所示，IoTF协议栈1306可包括以太网层1340、MAC层1342、IP层1344、UDP层1346、GTP-C层1348、以及控制(Ctrl)层1352。如图13中进一步所示，IoTF协议栈1306可实现用于传达控制面经加密客户端设备上下文(在图13中缩写为“CDC_{CP}”)的上下文协议层1350。上下文协议层1350还可使得能传达指示存在经加密客户端设备上下文的IoTF ID(IID)和/或安全性报头(在图13中缩写为“Sec”)。如图13中所示，客户端设备协议栈1302的上下文协议层1318与IoTF协议栈1306的上下文协议层1350处于通信中。在一方面，根据关于图15描述的示例性IoT分组格式，可在用户面消息之外的分组报头中携带经加密客户端设备上下文。

[0147] 服务网络协议栈1308可包括IP层1354、UDP层1356、GTP-C层1358、以及Ctrl层1360，其分别与IoTF协议栈1306的IP层1344、UDP层1346、GTP-C层1348以及Ctrl层1352对接。在本公开的一方面，如果网络架构被实现为GSM EDGE无线电接入网(GERAN)，则可使用与IP协议1364不同的协议。在本公开的一方面，由区域1362和1366指示的GTP-C和UDP协议可被省略

[0148] 用户面协议栈

[0149] 图14是解说根据本公开的各个方面的用于IoT数据传输的用户面协议栈1400的示图。如图14中所示，协议栈1400可包括客户端设备协议栈1402(也被称为IoT设备协议栈)、

网络接入节点协议栈1404、在网络节点1405处实现的IoTF协议栈1406、以及服务网络协议栈1408。例如，网络接入节点协议栈1404可以在eNB、基站、或网络接入点处实现。作为另一示例，服务网络协议栈1408可以在P-GW中实现。如图14中所示，客户端设备协议栈1402可包括物理(PHY)层1410、媒体接入控制(MAC)层1412、无线电链路控制(RLC)层1414、分组数据汇聚协议(PDCP)层1416、以及用户面(UP)层1420。如图14中进一步所示，客户端设备协议栈1402可实现用于传达用户面经加密客户端设备上下文(在图14中缩写为“CDC_{UP}”)的上下文协议层1418。上下文协议层1418可进一步使得能传达指示存在经加密客户端设备上下文的IoTF ID(IID)和/或安全性报头(在图14中缩写为“Sec”)。

[0150] 如图14中所示，网络接入节点协议栈1404可包括PHY层1422、MAC层1424、RLC层1426、以及PDCP层1428，其分别与客户端设备协议栈1402的PHY层1410、MAC层1412、RLC层1414、以及PDCP层1416对接。网络接入节点协议栈1404可进一步包括以太网层1430、MAC层1432、网际协议(IP)层1434、用户数据报协议(UDP)层1436、以及用户面GPRS隧穿协议(GTP-U)层1438。

[0151] 如图14中所示，IoTF协议栈1406可包括以太网层1440、MAC层1442、IP层1444、UDP层1446、以及GTP-U层1448。如图14中进一步所示，IoTF协议栈1406可实现用于传达用户面经加密客户端设备上下文(在图14中缩写为“CDC_{UP}”)的上下文协议层1450。上下文协议层1450还可使得能传达指示存在经加密客户端设备上下文的IoTF ID(IID)和/或安全性报头(在图14中缩写为“Sec”)。如图14中所示，客户端设备协议栈1402的上下文协议层1418与IoTF协议栈1406的上下文协议层1450处于通信中。在一方面，根据关于图15描述的示例性IoT分组格式，可在UP消息之外的分组报头中携带用户面经加密客户端设备上下文。

[0152] 服务网络协议栈1408可包括IP层1454、UDP层1456、GTP-U层1458、以及UP层1460，其分别与IoTF协议栈1406的IP层1444、UDP层1446、GTP-U层1448以及UP层1452对接。在本公开的一方面，如果网络架构被实现为GSM EDGE无线电接入网(GERAN)，则可使用与IP协议1464不同的协议。在本公开的一方面，由区域1462和1466指示的GTP-U和UDP协议可被省略在本公开的一方面，如果IP协议被用于UP消息递送，则用户面经加密网络可达性上下文可被携带在IP选项字段(IPv4)或IP扩展报头(IPv6)中。

[0153] IoT分组格式

[0154] 图15是根据本公开的各个方面的用于IoT网络架构中的传输的分组格式1500的示图。参照图15，临时标识符(TID)字段1502可被网络接入节点(例如，eNB、基站、或网络接入点)用来局部地标识客户端设备(也被称为IoT设备)。例如，由网络接入节点指派给TID字段1502以用于标识客户端设备的值可以是C-RNTI或等效物。

[0155] 在本公开的一方面，IoTF ID(IID)字段1504可包括全局唯一临时标识符(GUTI)。例如，GUTI可包括与IoTF相关联的标识符以及与客户端设备相关联的标识符(例如，临时标识符，诸如移动性管理实体(MME)临时移动订户身份(M-TMSI))。例如，GUTI可被网络接入节点用来标识IoTF，并且GUTI可被IoTF用来标识客户端设备。在另一方面，IID字段1504可包括全局IoTF标识符(GIOTFI)以及与客户端设备相关联的标识符(例如，临时标识符，诸如M-TMSI)。例如，GIOTFI可以是IoTF的全局唯一移动性管理实体标识符(GUMMEI)的等效物。在本公开的一方面，M-TMSI可出于客户端设备隐私性而被加密。应注意，使用IoTF IP地址可公开网络拓扑。

[0156] 安全性报头字段1506可指示经加密客户端设备上下文、控制面(CP)/用户面(UP)指示、序列号、时间戳值和/或随机值的存在。例如,时间戳值可基于时间和计数器,其中该时间是网络接入节点时间或IoTF时间。客户端设备上下文字段1508可包括经加密客户端设备上下文。应注意,如果时间戳而非序列号被用于加密,则IoTF可能不需要维持任何客户端设备网络状态。随机值可基于随机数和计数器。随机值由网络接入节点或客户端设备、或其组合生成。计数器可针对每个分组递增特定值(例如,1)。如果随机值而非序列号被用于加密,则客户端设备可基于安全性上下文中的加密密钥以及随机数来生成新的加密密钥。如果随机值而非序列号被用于完整性保护,则客户端设备可基于安全性上下文中的完整性保护密钥以及随机数来生成新的完整性保护密钥,并且可使用新的完整性保护密钥来保护消息。有效载荷字段1510可包括数据或控制信息(例如,数据分组或控制分组)。

[0157] 消息认证码(MAC)字段1512可用于完整性保护。例如,MAC字段1512可包括由传送方设备或实体生成的消息认证码。MAC字段1512中的消息认证码随后可被接收方设备或实体用来验证消息的完整性是否已受损(例如,该消息的内容是否已被更改或操纵)。在一个方面,MAC字段1512中的消息认证码可在传送方设备或实体处通过应用消息认证码生成算法(例如,AEAD密码)来生成,其中消息(例如,分组)和用户面密钥或控制面密钥被用作该消息认证码生成算法的输入。该消息认证码生成算法的输出可以是MAC字段1512中所包括的消息认证码。接收方设备或实体可通过对接收到的消息应用该消息认证码生成算法(例如,AEAD密码)来验证该消息的完整性。例如,接收到的消息(例如,分组)和用户面密钥或控制面密钥可被用作该消息认证码生成算法的输入。接收方设备或实体随后可将该消息认证码生成算法的输出与MAC字段1512中所包括的消息认证码作比较。在此类示例中,当该消息认证码生成算法的输出匹配MAC字段1512中所包括的消息认证码时,接收方设备或实体可确定该消息已被成功验证。

[0158] 经加密客户端设备上下文设计和生成

[0159] 根据本文所公开的各方面,经加密客户端设备上下文可包含网络向客户端设备提供服务可能需要的信息。例如,客户端设备上下文可包括安全性上下文、承载ID、演进分组系统(EPS)承载服务质量(QoS)和S5-TEID,和/或网络向客户端设备提供服务可能需要的其他服务、参数、值、设置、或特征。在一些方面,客户端设备上下文可在AKA规程期间建立。

[0160] 在一些方面,经加密客户端设备上下文除了客户端设备上下文之外还可包括一个或多个信息项。例如,经加密客户端设备上下文可包括由IoTF-C 106设置(或在客户端设备上下文中指示)的期满时间,其限制经加密客户端设备上下文的生命期(例如,以防止永久重用)。作为另一示例,经加密客户端设备上下文可具有标识用于生成该经加密客户端设备上下文的密钥的密钥索引。

[0161] 在一些方面,经加密客户端设备上下文可使用仅为网络中的实体所知的秘密密钥来生成,且由此不能被客户端设备解读和/或修改。例如,可通过使用IoTF-U(例如,IoTF-U 108)的秘密密钥对客户端设备上下文进行加密来生成经加密客户端设备上下文。在一些方面,经加密客户端设备上下文可用IoTF-U(例如,IoTF-U 108)的秘密密钥进行完整性保护,且由此不能被客户端设备操纵和/或修改。

[0162] 在一方面,可由IoTF-C(例如,IoTF-C 106)将经加密客户端设备上下文提供给客户端设备(例如,客户端设备102)作为认证和上下文(例如,承载)设立的成功完成。在一方

面,客户端设备可在一个或多个用户面分组(例如,UL数据分组)中包括经加密客户端设备上下文以使得IoTF-U(例如,IoTF-U108)能在运行中重构客户端设备上下文。例如,如果客户端设备需要顺序地传送多个分组,则客户端设备可在第一分组中包括经加密客户端设备上下文,而在后续分组中不包括经加密客户端设备上下文。在一些方面,经加密客户端设备上下文可以是因客户端设备而异的,且因此向一客户端设备发出的经加密客户端设备上下文不能被任何其他客户端设备使用。

[0163] 控制面经加密客户端设备上下文

[0164] 在本公开的一方面,IoTF(例如,图1中的IoTF-C 106)可通过级联一个或多个信息项来生成经加密客户端设备上下文。例如,控制面(CP)经加密客户端设备上下文(CDC_{CP})可基于表达式KeyID||$Enc\_K_{CDC-IoTF-C}(CDC_{CP})$||MAC来生成。在本公开的一方面,密钥$K_{CDC-IoTF-C}$(例如,图3中的密钥$K_{CDC-IoTF-C}$ 304)可与密钥$K_{CDC-IoTF}$(例如,图3中的密钥$K_{CDC-IoTF}$ 302)相同或从密钥$K_{CDC-IoTF}$推导出。项KeyID可表示(用于生成经加密客户端设备上下文的)密钥索引。项CDC_{CP}可表示控制面客户端设备上下文。例如,控制面客户端设备上下文可包括客户端设备标识符、客户端设备安全性上下文(例如,控制面密钥,诸如密钥K_{IoT}(K_{ASME}等效物)、密钥$K_{IoT-CPenc}$ 210、密钥$K_{IoT-CPint}$ 212)、客户端设备安全性能力(例如,演进分组系统加密算法(EEA)、演进分组系统完整性算法(EIA))、和/或下一跳(S5/S8)配置信息。例如,下一跳配置信息可包括IoT服务器地址、P-GW地址、和/或TEID。项MAC可指示加密模式和/或消息认证码生成算法(也被称为MAC算法),其可由移动网络运营商(MNO)选取并配置到IoTF。因此,项$Enc_K_{CDC-IoTF-C}(CDC_{CP})$可表示使用密钥$K_{CDC-IoTF-C}$对控制面客户端设备上下文执行的加密操作的结果。

[0165] 用户面经加密客户端设备上下文

[0166] 作为另一示例,用户面(UP)经加密客户端设备上下文(CDC_{UP})可基于表达式KeyID||$Enc\_K_{CDC-IoTF-U}(CDC_{UP})$||MAC来生成。项$CDC_{UP}$可表示用户面客户端设备上下文。例如,用户面客户端设备上下文可包括客户端设备标识符、承载ID、演进分组系统(EPS)承载服务质量(QoS)、用于用户面通用分组无线电服务(GPRS)隧穿协议(GTP-U)的S5隧道端点标识符(TEID)、IoTF-U 108将UL数据转发至的P-GW网际协议(IP)地址(或等效信息)、客户端设备安全性上下文(例如,所选加密算法和用户面密钥,诸如密钥$K_{IoT-UPenc}$ 216、密钥$K_{IoT-UPint}$ 218)、客户端设备安全性能力(例如,演进分组系统加密算法(EEA)、演进分组系统完整性算法(EIA))、和/或下一跳(S5/S8)配置信息。例如,下一跳配置信息可包括IoT服务器地址、P-GW地址、和/或TEID。因此,项$Enc_K_{CDC-IoTF-U}(CDC_{UP})$可表示使用密钥$K_{CDC-IoTF-U}$对用户面客户端设备上下文执行的加密操作的结果。在本公开的一方面,经加密客户端设备上下文可仅被该客户端设备附连/关联至的IoTF(例如,IoTF-C 106和/或IoTF-U 108)解密。在本公开的一方面,客户端设备上下文可在加密之前被压缩。

[0167] 经加密客户端设备上下文可具有一个或多个特性。例如,经加密客户端设备上下文可包含与特定客户端设备相关联的网络状态信息,且因此不能被传递给其他客户端设备。IoTF-C/U(例如,IoTF-C 106和/或IoTF-U 108)不包含客户端设备的上下文(例如,网络状态信息)。相应地,此类IoTF-C/U可使用其自己的秘密密钥来从经加密客户端设备上下文恢复出客户端设备上下文,且由此IoTF-C/U不需要存储任何附加信息就能恢复出客户端设备上下文。IoTF-C/U可在某些条件下(例如,演进分组系统连接管理(ECM)空闲或紧接在小

数据传递之后)移除客户端设备上下文并在需要时恢复客户端设备上下文(例如,用于数据传递)。

[0168] 客户端设备可存储由IoTF-C提供的经加密客户端设备上下文以进行快速UL数据传递/快速控制面消息传递。客户端设备可在传送一个或多个数据分组之后立即进入休眠模式。由于IoTF-U重构客户端设备上下文可以没有消息交换开销,因此小数据分组传输可以不经历延迟。在本公开的一方面,在客户端设备处于空闲模式时,用户面数据传输可以不使用控制面消息。

[0169] 追踪区域更新

[0170] 当客户端设备在空闲模式期间进入新的追踪区域时,客户端设备可执行追踪区域更新(TAU)规程。TAU消息可包括当前追踪区域id(TAI)和源IoTF-C的GIOTFI或等效物(例如,全局唯一移动性管理实体标识符(GUMMEI))。目标IoTF-C可连同经加密网络可达性上下文一起更新客户端设备的位置以及到一个或多个网络实体(例如,P-GW)的移动性锚点(例如,IoTF-U ID)。在本公开的一方面,经加密网络可达性上下文可使得IoTF-U能验证下行链路分组。在本公开的一方面,应用服务器(例如,IoT服务器)和/或P-GW可向(由GIOTFI标识的)IoTF-U/C传送带有经加密网络可达性上下文的下行链路(DL)分组。

[0171] 图16是根据本公开的各个方面的IoT网络架构(例如,IoT网络架构100)中的TAU规程的信号流图1600。如图16中所示,信号流图1600包括客户端设备1602(也被称为IoT设备)、网络接入节点1604(例如,eNB、基站、网络接入点)、在目标网络设备1605处实现的目标IoTF-C 1606、在源网络设备1607处实现的源IoTF-C 1608、P-GW 1610、以及IoT服务器1612(也被称为应用服务器)。客户端设备1602可向网络接入节点1604传送包括经加密客户端设备上下文(例如,控制面(CP)经加密客户端上下文)和TAU请求的数据传输请求消息1614。在本公开的一方面,数据传输请求消息1614可由客户端设备1602在不建立RRC连接的情况下发送。

[0172] 网络接入节点1604可确定(1616)该TAU请求中所包括的目标IoTF-C标识符。网络接入节点1604随后可确定目标IoTF-C 1606的IP地址,并且可向目标IoTF-C 1606传送包括与客户端设备1602相关联的TID、经加密客户端设备上下文、以及TAU请求的消息1618。目标IoTF-C 1606可向源IoTF-C 1608传送包括对客户端设备上下文的请求和经加密客户端设备上下文的消息1620。

[0173] 源IoTF-C 1608可向目标IoTF-C 1606传送包括客户端设备上下文的消息1622。目标IoTF-C 1606可存储(1624)客户端设备的TID以及网络接入节点1604的ID,并且可基于接收到的客户端设备上下文来为客户端设备1602生成(1624)新的GUTI和新的经加密客户端设备上下文。在本公开的一方面,目标IoTF-C 1606可生成用户面(UP)密钥和上下文生成密钥并且可将这些密钥提供给IoTF-U。

[0174] 目标IoTF-C 1606可向IoT服务器1612(或P-GW 1610)传送包括追踪区域ID(TAI)和目标IoTF-C 1606的ID(例如,GIOTFI)的消息1626。目标IoTF-C 1606可向客户端设备1602传送包括TID、新的GUTI、新的经加密客户端设备上下文、以及TAU响应的消息1628。网络接入节点1604可基于TID在消息1630中将新的GUTI、新的经加密客户端设备上下文、以及TAU响应转发给客户端设备1602。

[0175] 本文所公开的各方面提供了具有新的专用网络功能的架构,这些功能实现了独立

部署并且避免了可缩放性/互通要求。本文所公开的各方面可使得网络接入节点(例如,基站)能向或从客户端设备传递数据而无需存储或维持关于客户端设备的安全性上下文,由此避免消耗网络接入节点(或其他网络实体)处的大量资源。安全性特征可被锚定在新的网络功能(被称为IoT功能(IoTF))处。专用资源被分配用于IoT数据传输,以避免影响正常客户端设备的PDN连接/话务。经加密UE上下文可被用于数据传输,以消除当UE处于空闲状态时在IoTF处的关于UE的半永久上下文。MME/S-GW不应当维持不频繁地传送话务的IoT设备的大量状态(即,上下文)。IoT设备可仅需要成本高效的数据递送,而不会耗尽昂贵的核心网资源。

[0176] 经加密客户端设备上下文使用信息

[0177] 根据本公开的各个方面,客户端设备(例如,图7中的客户端设备702)在其向网络传送经加密客户端设备上下文时可传送与经加密客户端设备上下文相关联的使用信息(也被称为经加密客户端设备上下文使用信息)。

[0178] 在一个方面,经加密客户端设备上下文使用信息可指示要从客户端设备传送的数据量。例如,数据量可被指示为缩减数据传输(例如,包括单个数据分组的传输)或突发数据传输(例如,包括若干个数据分组的一个或多个传输)。在一方面,要从客户端设备传送的数据量可使用单个比特(例如,作为分组报头中的信息元素(IE)的一部分)来指示。在此类方面,例如,客户端设备可启用该比特(例如,将该比特设为‘1’)以指示要从客户端设备传送的数据量是缩减数据传输,或者可禁用该比特(例如,将该比特设为‘0’)以指示要从客户端设备传送的数据量是突发数据传输。

[0179] 在一个方面,当客户端设备指示要传送的数据量是缩减数据传输时,网络(例如,网络节点(诸如网络节点707、709)、和/或网络接入节点(诸如网络接入节点704))可在从客户端设备接收到该缩减数据传输之后立即移除关于该客户端设备的上下文。在另一方面,当客户端设备指示要传送的数据量是缩减数据传输时,网络可维持关于该客户端设备的上下文达第一阈值时间段。例如,网络可实现被配置成测量第一阈值时间段的第一定时器。在这方面,网络可在第一定时器期满之际移除关于该客户端设备的上下文。在一个方面,如果网络在第一定时器期满之前从该客户端设备接收到数据传输(例如,分组),则网络可重置第一定时器并且可维持关于该客户端设备的上下文直至第一定时器期满。

[0180] 在另一方面,当客户端设备指示要传送的数据量是突发数据传输时,网络可维持关于该客户端设备的上下文达第二阈值时间段。例如,网络可实现被配置成测量第二阈值时间段的第二定时器。在这方面,网络可在第二定时器期满之际移除关于该客户端设备的上下文。在一个方面,如果网络在第二定时器期满之前从该客户端设备接收到数据传输(例如,分组),则网络可重置第二定时器并且可维持关于该客户端设备的上下文直至第二定时器期满。例如,第二阈值时间段可以大于第一阈值时间段。

[0181] 在一个方面,经加密客户端设备上下文使用信息可被包括在传送给网络的分组的报头中。在另一方面,客户端设备可在RRC信令规程期间将经加密客户端设备上下文使用信息提供给网络。

[0182] 在一个方面,网络(例如,图6中的网络节点605)可向客户端设备(例如,图6中的客户端设备602)提供多种类型的经加密客户端设备上下文。在此类方面,每种类型的经加密客户端设备上下文可被网络(例如,图9中的网络节点907)用来重构关于客户端设备的上下

文的一部分(例如,关于客户端设备的上下文的子集)。例如,第一类型的经加密客户端设备上下文可与由网络提供的第一服务(例如,移动宽带服务)相关联,其中第一类型的经加密客户端设备上下文使得网络能重构用于支持第一服务所需要的第一部分客户端设备上下文。在此类示例中,第二类型的经加密客户端设备上下文可与由网络提供的第二服务(例如,超可靠低等待时间通信(URLLC))相关联,其中第二类型的经加密客户端设备上下文使得网络能重构用于支持第二服务所需要的第二部分客户端设备上下文。在一方面,第一部分客户端设备上下文和第二部分客户端设备上下文可包括比网络原始针对客户端设备生成的客户端设备上下文更少的上下文信息。

[0183] 在一方面,客户端设备可基于要发送给(或接收自)网络的传输类型来确定该多种类型的经加密客户端设备上下文中要使用的一个或多个经加密客户端设备上下文。举例而言,并且参考以上提供的示例,如果客户端设备将传送与移动宽带服务相关联的数据,则客户端设备可将第一类型的经加密客户端设备上下文传送给网络。作为另一示例,如果客户端设备将传送与URLLC服务相关联的数据,则客户端设备可将第二类型的经加密客户端设备上下文传送给网络。应理解,作为以上提供的示例的补充或代替,网络可提供其他类型的服务,诸如高优先级接入服务、耐延迟接入服务、或机器型通信(MTC)服务。

[0184] 根据本公开的各个方面,当客户端设备向网络传送经加密客户端设备上下文时,客户端设备可在先前描述的使用信息中指示经加密客户端设备上下文的类型。在一个方面,经加密客户端设备上下文使用信息可指示正从客户端设备传送的信息类型。例如,经加密客户端设备上下文使用信息可指示正从客户端设备传送的信息与用户面(例如,数据)或控制面(例如,控制信息)相关联。可以领会,由于先前讨论的不同类型的经加密客户端设备上下文中的每一者可被网络用来重构关于客户端设备的上下文的一部分(例如,关于客户端设备的上下文的子集),因此相比于使得能够重构整个(例如,完整)客户端设备上下文的经加密客户端设备上下文相比,此类不同类型的经加密客户端设备上下文在大小上可以缩减。

[0185] 在一方面,针对由网络(例如,在图9中的IoT服务器912处)提供的服务类型将由网络(例如,在图9中的网络节点907处)重构的上下文(或上下文部分)可与值(例如,索引号或其他值)相关联。在此类方面,客户端设备(例如,图9中的客户端设备902)可连同经加密客户端设备上下文一起传送索引号以促成在网络处针对特定服务(或其他具体使用或应用)来重构上下文。例如,索引号“1”可指示移动宽带服务的特定服务质量(QoS)以及重构用于支持该QoS的上下文所需要的信息。在此类示例中,客户端设备可传送与移动宽带服务相关联的经加密客户端设备上下文以及索引号“1”以促成重构支持移动宽带服务的客户端设备上下文部分。

[0186] 多个用户面网络功能

[0187] 在本公开的一个方面,网络可尤其包括客户端设备、网络接入节点(例如,eNB、基站、网络接入点)、以及网络实体(例如,服务网关(S-GW)、分组数据网络网关(P-GW))。在此类方面,网络接入节点可实现第一用户面网络功能,且网络实体可实现第二用户面网络功能。相应地,网络接入节点可获得第一用户面经加密客户端设备上下文并将其传送给客户端设备,且网络实体可获得第二用户面经加密客户端设备上下文并将其传送给客户端设备。在一方面,第一用户面经加密客户端设备上下文可使得第一用户面网络功能能够重构

用于处理客户端设备的用户数据话务(例如,用于验证和/或解密用户数据分组)的关于该客户端设备的第一上下文(例如,第一安全上下文),且第二用户面经加密客户端设备上下文可使得第二用户面网络功能能够重构用于处理客户端设备的用户数据话务(例如,用于验证和/或解密用户数据分组)的关于该客户端设备的第二上下文(例如,第二安全上下文)。在一个方面,客户端设备可连同UL数据话务一起将多个经加密客户端设备上下文传送给网络。例如,客户端设备可连同UL数据话务一起传送第一用户面经加密客户端设备上下文和第二用户面经加密客户端设备上下文两者。在一个方面,第一和第二用户面经加密客户端设备上下文可同时被传送(例如,在从客户端设备传送的同一个分组中)。因此,可以领会,在一些方面,从客户端设备传送的多个经加密客户端设备上下文可使得能重构与网络中的不同实体(例如,网络接入节点、S-GW)相关联的独立客户端设备上下文。

[0188] 示例性装置(例如,客户端设备)和该装置上的方法

[0189] 图17是根据本公开的一个或多个方面(例如,与以下描述的图18-20的方法有关的各方面)的配置成基于IoT网络架构来与网络通信的装置1700的解说。装置1700包括通信接口(例如,至少一个收发机)1702、存储介质1704、用户接口1706、存储器设备1708以及处理电路1710。

[0190] 这些组件可以经由信令总线或其他合适的组件(由图17中的连接线一般化地表示)彼此耦合和/或彼此进行电通信。取决于处理电路1710的具体应用和整体设计约束,信令总线可包括任何数目的互连总线和桥接器。信令总线将各种电路链接在一起以使得通信接口1702、存储介质1704、用户接口1706和存储器设备1708中的每一者与处理电路1710耦合和/或进行电通信。信令总线还可链接各种其他电路(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,且因此将不再进一步描述。

[0191] 通信接口1702可被适配成促成装置1700的无线通信。例如,通信接口1702可包括被适配成促成关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/或代码(例如,指令)。通信接口1702可耦合到一个或多个天线1712以用于在无线通信系统内进行无线通信。通信接口1702可以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1702包括发射机1714和接收机1716。

[0192] 存储器设备1708可表示一个或多个存储器设备。如所指示的,存储器设备1708可维持网络相关信息/连同由装置1700使用的其他信息。在一些实现中,存储器设备1708和存储介质1704被实现为共用存储器组件。存储器设备1708还可被用于存储由处理电路1710或由装置1700的某个其他组件操纵的数据。

[0193] 存储介质1704可表示用于存储代码(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计算机可读、机器可读、和/或处理器可读设备。存储介质1704还可被用于存储由处理电路1710在执行代码时操纵的数据。存储介质1704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、包含或携带代码的各种其他介质。

[0194] 作为示例而非限制,存储介质1704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

问和读取的代码的合适介质。存储介质1704可以实施在制品(例如,计算机程序产品)中。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1704可以是非瞬态(例如,有形)存储介质。

[0195] 存储介质1704可被耦合至处理电路1710以使得处理电路1710能从存储介质1704读取信息和向存储介质1704写入信息。即,存储介质1704可耦合到处理电路1710,以使得存储介质1704至少能由处理电路1710访问,包括其中至少一个存储介质被集成到处理电路1710的示例和/或其中至少一个存储介质与处理电路1710分开(例如,驻留在装置1700中、在装置1700外部、跨多个实体分布等)的示例。

[0196] 由存储介质1704存储的代码和/或指令在由处理电路1710执行时使处理电路1710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1704可包括被配置用于以下动作的操作:调节处理电路1710的一个或多个硬件块处的操作以及利用通信接口1702通过利用其相应通信协议来进行无线通信。

[0197] 处理电路1710一般被适配成用于处理,包括执行存储在存储介质1704上的此类代码/指令。如本文中使用的,术语“代码”或“指令”应当被宽泛地解读成包括但不限于编程、指令、指令集、数据、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行件、执行的线程、规程、函数等,无论其被称为软件、固件、中间件、微代码、硬件描述语言、还是其他术语。

[0198] 处理电路1710被安排成获得、处理和/或发送数据,控制数据访问和存储,发布命令,以及控制其他期望操作。在至少一个示例中,处理电路1710可包括被配置成实现由恰适介质提供的期望代码的电路系统。例如,处理电路1710可被实现为一个或多个处理器、一个或多个控制器、和/或配置成执行可执行代码的其他结构。处理电路1710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、或者其任何组合。通用处理器可包括微处理器,以及任何常规处理器、控制器、微控制器、或状态机。处理电路1710还可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1710的这些示例是为了解说,并且还设想了落在本公开范围内的其他合适的配置。

[0199] 根据本公开的一个或多个方面,处理电路1710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。如本文所使用的,涉及处理电路1710的术语“适配”可指处理电路1710被配置、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。

[0200] 根据装置1700的至少一个示例,处理电路1710可包括传送电路/模块1720、接收电路/模块1722、经加密客户端设备上下文存储电路/模块1724、经加密客户端设备上下文确定电路/模块1726、空闲模式进入电路/模块1728、安全性上下文建立电路/模块1730、消息获得电路/模块1732、以及使用信息获得电路/模块1733中的一者或多者,它们被适配成执行本文描述的任何或所有特征、过程、功能、操作、和/或例程(例如,关于图18-20描述的特征、过程、功能、操作、和/或例程)。

[0201] 传送电路/模块1720可包括适配成执行与例如以下操作有关的若干功能的电路系

统和/或指令(例如,存储在存储介质1704上的传送指令1734):传送要与网络通信的请求,向网络传送包括一个或多个经加密客户端设备上下文中的至少一者的消息,向网络传送带有UP经加密客户端设备上下文的空分组,向网络传送包括网络地址的多个数据分组,以及向网络传送资源释放请求消息,其中资源释放请求消息使得网络能释放用于该客户端设备的一个或多个资源。

[0202] 接收电路/模块1722可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的接收指令1736):响应于请求而从网络接收一个或多个经加密客户端设备上下文,接收第二数据分组,其中接收第二数据分组不与网络接入节点建立无线电资源控制(RRC)连接,从网络接收寻呼消息,以及响应于消息而接收客户端设备的网络地址。

[0203] 经加密客户端设备上下文存储电路/模块1724可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的经加密客户端设备上下文存储指令1738):将一个或多个经加密客户端设备上下文存储在本地存储中。

[0204] 经加密客户端设备上下文确定电路/模块1726可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的经加密客户端设备上下文确定指令1740):基于通信包括数据还是控制信息来确定该一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文,以及确定该一个或多个经加密客户端设备上下文中与服务相关联的至少一个经加密客户端设备上下文,其中该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文使得能重构支持该服务的客户端设备上下文部分。

[0205] 空闲模式进入电路/模块1728可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的空闲模式进入指令1742):在传送包括第一数据分组的消息之后立即进入空闲模式。

[0206] 安全性上下文建立电路/模块1730可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的安全性上下文建立指令1744):建立用于与网络的连接的安全性上下文,其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合。

[0207] 消息获得电路/模块1732可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的消息获得指令1746):获得消息,其中该消息与网络提供的服务相关联。

[0208] 使用信息获得电路/模块1733可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质1704上的使用信息获得指令1747):获得与该一个或多个经加密客户端设备上下文中的至少一者相关联的使用信息。

[0209] 如上所提及的,由存储介质1704存储的指令在由处理电路1710执行时使处理电路1710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1704可包括以下一者或多者:传送指令1734、接收指令1736、经加密客户端设备上下文存储指令1738、经加密客户端设备上下文确定指令1740、空闲模式进入指令1742、安全性上下文建立指令1744、消息获得指令1746、以及使用信息获得指令1747。

[0210] 图18(包括图18A和18B)是解说根据本公开的各个方面的用于与网络通信的方法

的流程图1800。该方法可由诸如客户端设备之类的装置(例如,客户端设备102、502或装置1700)执行。应理解,图18中由虚线指示的操作表示可选操作。

[0211] 客户端设备传送要与网络通信的请求(1802)。在一个示例中,该请求可以是先前关于图6描述的请求612。在一方面,该请求可包括关于客户端设备正请求经加密客户端设备上下文的指示和/或对客户端设备正请求的服务的指示。客户端设备建立用于与网络的连接的安全性上下文,其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥(1803)。在一方面,加密密钥是用户面加密密钥且完整性保护密钥是用户面完整性保护密钥,该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处,并且第一数据分组至少用该用户面完整性保护密钥来进行完整性保护或用该用户面加密密钥来加密。

[0212] 客户端设备响应于该请求而从网络接收一个或多个经加密客户端设备上下文(1804)。在一个示例中,该一个或多个经加密客户端设备上下文可以是图6中由客户端设备602接收的RRC连接重配置消息626中的经加密客户端设备上下文。在一个方面,可作为与网络的成功认证的结果而从网络接收经加密客户端设备上下文。在此类方面,与网络的成功认证不建立接入阶层(AS)安全性上下文。例如,该一个或多个经加密客户端设备上下文可包括以下至少一者:安全性上下文、承载的服务质量(QoS)、和/或隧道端点标识符(TEID)。在一方面,该一个或多个经加密客户端设备上下文可包括将用于与客户端设备的数据相关通信的第一上下文和将用于与客户端设备的控制相关通信的第二上下文。在一方面,该一个或多个经加密客户端设备上下文在客户端设备处不能被解密。在此类方面,该一个或多个经加密客户端设备上下文只能由生成该一个或多个经加密客户端设备上下文的网络设备解密。

[0213] 客户端设备将该一个或多个经加密客户端设备上下文存储在本地存储中(1806)。客户端设备基于将从该客户端设备传送的消息(例如,分组)包括数据还是控制信息来确定该一个或多个经加密客户端设备上下文中将使用的至少一个经加密客户端设备上下文(1808)。例如,该一个或多个经加密客户端设备上下文可包括用户面(UP)经加密客户端设备上下文和控制面(CP)经加密客户端设备上下文。在此类示例中,客户端设备可传送带有UP经加密客户端设备上下文的第一数据分组、或带有CP经加密客户端设备上下文的控制分组。例如,控制分组可以是追踪区域更新(TAU)分组。

[0214] 客户端设备向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息(1810)。在一个示例中,该消息可以是包括经加密客户端设备上下文和图8中由客户端设备802传送给网络接入节点804的数据分组的数据传输请求消息810。在一方面,该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文,该上下文包括与该客户端设备相关联的网络状态信息。在一方面,该上下文在网络处被移除(例如,删除或不再维持)。在一方面,客户端设备可在不与网络的网络接入节点建立无线电资源控制(RRC)连接的情况下传送包括第一数据分组的消息。客户端设备在传送包括第一数据分组的消息之后立即进入空闲模式(1812)。

[0215] 客户端设备接收第二数据分组,其中接收第二数据分组不与网络接入节点建立RRC连接(1814)。在一个示例中,第二数据分组可以是图8中从网络接入节点804传送给客户端设备802的第五消息824中的数据分组。在一方面,加密密钥是用户面加密密钥且完整性

保护密钥是用户面完整性保护密钥，其中该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处。在此类方面，在接收第二数据分组时，客户端设备用该用户面完整性保护密钥来验证第二数据分组和/或用该用户面加密密钥来解密第二数据分组。客户端设备从网络接收寻呼消息(1816)。客户端设备向网络传送带有UP经加密客户端设备上下文的空分组(1818)。

[0216] 图19是解说根据本公开的各个方面的用于与网络通信的方法的流程图1900。该方法可由诸如客户端设备之类的装置(例如，客户端设备102、502或装置1700)执行。应理解，图19中由虚线指示的操作表示可选操作。

[0217] 客户端设备传送要与网络通信的请求(1902)。在一个示例中，该请求可以是先前关于图6描述的请求612。在一方面，该请求可包括关于客户端设备正请求经加密客户端设备上下文的指示和/或对客户端设备正请求的服务的指示。客户端设备建立用于与网络的连接的安全性上下文，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥(1904)。在一方面，加密密钥是用户面加密密钥且完整性保护密钥是用户面完整性保护密钥，该用户面加密密钥和用户面完整性保护密钥维持在客户端设备处，并且第一数据分组至少用该用户面完整性保护密钥来进行完整性保护或用该用户面加密密钥来加密。

[0218] 客户端设备响应于该请求而从网络接收一个或多个经加密客户端设备上下文(1906)。在一个示例中，该一个或多个经加密客户端设备上下文可以是图6中由客户端设备602接收的RRC连接重配置消息626中的经加密客户端设备上下文。在一个方面，可作为与网络的成功认证的结果而从网络接收经加密客户端设备上下文。在此类方面，与网络的成功认证不建立接入阶层(AS)安全性上下文。例如，该一个或多个经加密客户端设备上下文可包括以下至少一者：安全性上下文、承载的服务质量(QoS)、和/或隧道端点标识符(TEID)。在一方面，该一个或多个经加密客户端设备上下文可包括将用于与客户端设备的数据相关通信的第一上下文和将用于与客户端设备的控制相关通信的第二上下文。在一方面，该一个或多个经加密客户端设备上下文在客户端设备处不能被解密。在此类方面，该一个或多个经加密客户端设备上下文只能由生成该一个或多个经加密客户端设备上下文的网络设备解密。在一方面，在客户端设备从网络接收该一个或多个经加密客户端设备上下文之后，该上下文在网络处被移除。客户端设备向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息(1908)。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文，该上下文包括与该客户端设备相关联的网络状态信息。在一方面，该消息进一步包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文。例如，该消息可以是资源建立请求消息1016。客户端设备响应于该消息而接收用于该客户端设备的网络地址(1910)。客户端设备向网络传送包括该网络地址的多个数据分组(1912)。客户端设备向网络传送资源释放请求消息，其中资源释放请求消息使得网络能释放用于该客户端设备的一个或多个资源(1914)。

[0219] 图20是解说根据本公开的各个方面的用于与网络通信的方法的流程图2000。该方法可由诸如客户端设备之类的装置(例如，客户端设备102、502或装置1700)执行。应理解，图20中由虚线指示的操作表示可选操作。

[0220] 在一方面，提供了一种用于客户端设备的方法。客户端设备传送要与网络通信的请求(2002)。客户端设备建立用于与网络的连接的安全性上下文，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合(2004)。客户端设备响应于该请求而从网络接收一个或多个经加密客户端设备上下文(2006)。

[0221] 客户端设备获得消息，其中该消息与网络提供的服务相关联(2008)。在一方面，该一个或多个经加密客户端设备上下文中的每一者与网络提供的多个服务之一相关联。在此类方面，客户端设备确定该一个或多个经加密客户端设备上下文中与该服务相关联的至少一个经加密客户端设备上下文，其中该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文使得能重构支持该服务的客户端设备上下文部分(2010)。例如，该多个服务可包括移动宽带服务、超可靠低等待时间通信(URLLC)服务、高优先级接入服务、耐延迟接入服务、和/或机器型通信(MTC)服务。

[0222] 客户端设备获得与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息(2012)。在一方面，与该一个或多个经加密客户端设备上下文中的该至少一个经加密客户端设备上下文相关联的使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面，该使用信息可包括与针对网络提供的服务类型将由网络重构的上下文(或上下文部分)相关联的值(例如，索引号或其他值)。

[0223] 客户端设备向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息(2014)。在一方面，该消息包括使用信息。在一方面，该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文的至少一部分，该上下文包括与该客户端设备相关联的网络状态信息。在一方面，该部分上下文被维持在网络处达基于该消息的传输是缩减数据传输还是突发数据传输来确定的时间段。在一方面，该一个或多个经加密客户端设备上下文包括使得能在网络中的第一实体处重构关于该客户端设备的第一上下文的第一用户面经加密客户端设备上下文、以及使得能在网络中的第二实体处重构关于该客户端设备的第二上下文的第二用户面经加密客户端设备上下文。在此类方面，该消息至少包括第一用户面经加密客户端设备上下文和第二用户面经加密客户端设备上下文。

[0224] 示例性装置(例如，网络设备)和该装置上的方法

[0225] 图21是根据本公开的一个或多个方面(例如，与以下描述的图22-26的方法有关的各方面)的装置2100的解说。装置2100包括网络通信接口(例如，至少一个收发机)2102、存储介质2104、用户接口2106、存储器设备2108以及处理电路2110。在一方面，装置2100可以是实现物联网(IoT)功能的网络设备(例如，网络设备105、505、705)。例如，装置2100可实现控制面IoT功能(例如，IoTF-C 106、506、606、706、906、1406)和/或用户面IoT功能(例如，IoTF-U 108、508、608、708、806、908)。应理解，此类网络设备可被实现为单个网络实体或多个网络实体。

[0226] 这些组件可以经由信令总线或其他合适的组件(由图21中的连接线一般化地表示)彼此耦合和/或彼此进行电通信。取决于处理电路2110的具体应用和整体设计约束，信令总线可包括任何数目的互连总线和桥接器。信令总线将各种电路链接在一起以使得网络通信接口2102、存储介质2104、用户接口2106和存储器设备2108中的每一者与处理电路2110相耦合和/或进行电通信。信令总线还可链接各种其他电路(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，且因此将不再进一步描述。

[0227] 网络通信接口2102可被适配成促成装置2100的通信。例如，网络通信接口2102可包括适配成促成关于网络中的一个或多个网络实体双向地进行信息通信的电路系统和/或代码(例如，指令)。网络通信接口2102可以配置有一个或多个独立接收机和/或发射机以及一个或多个收发机。

[0228] 存储器设备2108可表示一个或多个存储器设备。如所指示的，存储器设备2108可维持网络相关信息/连同由装置2100使用的其他信息。在一些实现中，存储器设备2108和存储介质2104被实现为共用存储器组件。存储器设备2108还可被用于存储由处理电路2110或由装置2100的某个其他组件操纵的数据。

[0229] 存储介质2104可表示用于存储代码(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计算机可读、机器可读、和/或处理器可读设备。存储介质2104还可被用于存储由处理电路2110在执行代码时操纵的数据。存储介质2104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、包含或携带代码的各种其他介质。

[0230] 作为示例而非限制，存储介质2104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代码的合适介质。存储介质2104可以实施在制品(例如，计算机程序产品)中。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2104可以是非瞬态(例如，有形)存储介质。

[0231] 存储介质2104可被耦合至处理电路2110以使得处理电路2110能从存储介质2104读取信息和向存储介质2104写入信息。即，存储介质2104可耦合到处理电路2110，以使得存储介质2104至少能由处理电路2110访问，包括其中至少一个存储介质被集成到处理电路2110的示例和/或其中至少一个存储介质与处理电路2110分开(例如，驻留在装置2100中、在装置2100外部、跨多个实体分布等)的示例。

[0232] 由存储介质2104存储的代码和/或指令在由处理电路2110执行时使处理电路2110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2104可包括被配置用于以下动作的操作：调节处理电路2110的一个或多个硬件块处的操作以及将网络通信接口2102用于利用其相应通信协议进行的网络通信。

[0233] 处理电路2110一般被适配成用于处理，包括执行存储在存储介质2104上的此类代码/指令。如本文中使用的，术语“代码”或“指令”应当被宽泛地解读成包括但不限于编程、指令、指令集、数据、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行件、执行的线程、规程、函数等，无论其被称为软件、固件、中间件、微代码、硬件描述语言、还是其他术语。

[0234] 处理电路2110被安排成获得、处理和/或发送数据，控制数据访问和存储，发布命令，以及控制其他期望操作。在至少一个示例中，处理电路2110可包括被配置成实现由恰适介质提供的期望代码的电路系统。例如，处理电路2110可被实现为一个或多个处理器、一个

或多个控制器、和/或配置成执行可执行代码的其他结构。处理电路2110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、或者其任何组合。通用处理器可包括微处理器，以及任何常规处理器、控制器、微控制器、或状态机。处理电路2110还可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2110的这些示例是为了解说，并且还设想了落在本公开范围内的其他合适的配置。

[0235] 根据本公开的一个或多个方面，处理电路2110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。如本文所使用的，涉及处理电路2110的术语“适配”可指处理电路2110被配置、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。

[0236] 根据装置2100的至少一个示例，处理电路2110可包括传送电路/模块2120、接收电路/模块2122、认证和验证电路/模块2124、经加密客户端设备上下文生成电路/模块2126、上下文重构/移除电路/模块2128、分组处理电路/模块2130、存储电路/模块2132、网络接入节点确定电路/模块2134、临时标识符添加电路/模块2136、网络地址获得/释放电路/模块2137、分组加密和保护电路/模块2138、以及安全性上下文建立电路/模块2139中的一者或多者，它们被适配成执行本文描述的任何或所有特征、过程、功能、操作、和/或例程(例如，关于图22-26描述的特征、过程、功能、操作、和/或例程)。

[0237] 传送电路/模块2120可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如，存储在存储介质2104上的传送指令2140)：向客户端设备传送一个或多个经加密客户端设备上下文，向第二客户端设备传送新的经加密客户端设备上下文，将控制分组的有效载荷部分转发给应用服务器或分组数据网络网关(P-GW)，将控制分组转发给客户端设备，将第一数据分组转发给服务网络，将第二数据分组转发给客户端设备，和/或向客户端设备传送网络地址。

[0238] 接收电路/模块2122可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如，存储在存储介质2104上的接收指令2142)：从客户端设备接收要与网络通信的请求，从客户端设备接收控制分组和经加密客户端设备上下文，从客户端设备接收第一数据分组和经加密客户端设备上下文，从服务器或分组数据网络网关(P-GW)接收第二数据分组，从第二客户端设备接收控制分组，从第二网络设备接收关于第二客户端设备的上下文，从客户端设备接收包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息，从客户端设备接收消息，该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息，和/或从客户端设备接收资源释放请求消息。

[0239] 认证和验证电路/模块2124可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如，存储在存储介质2104上的认证和验证指令2144)：向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息，与客户端设备执行相互认证，以及验证从客户端设备接收的经加密客户端设备上下文。

[0240] 经加密客户端设备上下文生成电路/模块2126可包括适配成执行与例如以下操作

有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的经加密客户端设备上下文生成指令2146):生成一个或多个经加密客户端设备上下文,其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与客户端设备通信的至少一个上下文,确定经加密客户端设备上下文是否已期满,生成新的经加密客户端设备上下文,确定要生成一个或多个经加密客户端设备上下文,其中该确定基于请求中指示的经加密客户端设备上下文使用信息、设备的订阅、或策略中的至少一者,以及向第二网络设备请求关于第二客户端设备的客户端设备上下文,该请求包括控制面(CP)经加密客户端设备上下文。例如,该一个或多个经加密客户端设备上下文可包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。

[0241] 上下文重构/移除电路/模块2128可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的上下文重构/移除指令2148):获得用于与客户端设备相关联的经加密客户端设备上下文的密钥(例如,密钥$K_{CDC-IoTF-U}$),基于该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文,从经加密客户端设备上下文重构至少一个上下文,基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文,移除至少一个上下文,和/或在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段,第二阈值时间段大于第一阈值时间段。

[0242] 分组处理电路/模块2130可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的分组处理指令2150):使用该至少一个上下文来处理控制分组,其中该处理包括以下至少一者:使用该上下文来验证或解密控制分组。

[0243] 存储电路/模块2132可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的存储指令2152):存储用于针对客户端设备的下行链路分组的临时标识符(ID)。

[0244] 网络接入节点确定电路/模块2134可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的网络接入节点确定指令2154):确定第二数据分组被转发到的网络接入节点。

[0245] 临时标识符添加电路/模块2136可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的临时标识符添加指令2156):向第二数据分组添加临时标识符,该临时标识符使得网络接入节点能确定客户端设备。

[0246] 网络地址获得/释放电路/模块2137可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的网络地址获得/释放指令2157):响应于消息而获得用于客户端设备的网络地址,从客户端设备向网关传送资源释放请求消息,其中资源释放请求消息使得网关能释放用于该客户端设备的网络地址,和/或当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息,其中资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。

[0247] 分组加密和保护电路/模块2138可包括适配成执行与例如以下操作有关的若干功

能的电路系统和/或指令(例如,存储在存储介质2104上的分组加密和保护指令2158):使用用户面(UP)客户端设备密钥来对分组进行加密或完整性保护,基于安全性上下文来解密和验证第一数据分组,和/或使用用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护。

[0248] 安全性上下文建立电路/模块2139可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2104上的安全性上下文建立指令2159):与客户端设备建立至少一个上下文,该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息,其中该网络状态信息至少包括加密算法、加密密钥、完整性保护算法、完整性保护密钥、或其组合。

[0249] 如上所提及的,由存储介质2104存储的指令在由处理电路2110执行时使处理电路2110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2104可包括以下一者或多者:传送指令2140、接收指令2142、认证和验证指令2144、经加密客户端设备上下文生成指令2146、上下文重构/移除指令2148、分组处理指令2150、存储指令2152、网络接入节点确定指令2154、临时标识符添加指令2156、网络地址获得/释放指令2157、分组加密和保护指令2158、以及安全性上下文建立指令2159。

[0250] 图22(包括图22A和22B)是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2200。该方法可由实现IoT功能(例如,控制面IoTF,诸如图1的控制面IoTF 106)的诸如网络设备之类的装置(例如,图1的网络设备105或图21的装置2100)执行。应理解,图22中用虚线指示的操作表示可选操作。

[0251] 该装置从客户端设备接收要与网络通信的请求(2202)。该装置向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息(2204)。该装置与客户端设备执行相互认证(2206)。

[0252] 该装置与客户端设备建立至少一个上下文,该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息(2207)。在一方面,该网络状态信息至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥。该装置确定要生成一个或多个经加密客户端设备上下文,其中该确定基于请求中指示的经加密客户端设备上下文使用信息、客户端设备的订阅、和/或策略中的至少一者(2208)。

[0253] 该装置生成一个或多个经加密客户端设备上下文(2210)。在一方面,该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文。在一方面,该一个或多个经加密客户端设备上下文包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。该装置向客户端设备传送该一个或多个经加密客户端设备上下文(2212)。

[0254] 该装置从客户端设备接收控制分组和经加密客户端设备上下文(2214)。该装置验证从客户端设备接收的经加密客户端设备上下文(2216)。在一方面,该装置通过确定经加密客户端设备上下文是否已期满来验证从客户端设备接收的经加密客户端设备上下文,在先前经加密客户端设备上下文已期满时生成一个或多个新的经加密客户端设备上下文,以及在先前经加密客户端设备上下文已期满时将该一个或多个新的经加密客户端设备上下文传送给客户端设备。在一方面,验证经加密客户端设备上下文包括确定用于验证经加密客户端设备上下文的密钥。

[0255] 该装置从经加密客户端设备上下文重构至少一个上下文(2218)。该装置使用该至少一个上下文来处理控制分组,其中该处理包括以下至少一者:使用该至少一个上下文来验证或解密控制分组(2220)。该装置存储用于针对客户端设备的下行链路分组的临时标识符(ID)(2222)。该装置将控制分组的有效载荷部分转发给应用服务器或分组数据网络网关(P-GW)(2224)。

[0256] 图23(包括图23A和23B)是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2300。该方法可由实现IoT功能(例如,控制面IoTF,诸如图1的控制面IoTF 106)的诸如网络设备之类的装置(例如,图1的网络设备105或图21的装置2100)执行。应理解,图23中用虚线指示的操作表示可选操作。

[0257] 该装置从客户端设备接收要与网络通信的请求(2302)。该装置与客户端设备建立至少一个上下文,该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息,其中该网络状态信息至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥(2304)。该装置生成一个或多个经加密客户端设备上下文(2306)。在一方面,该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的至少一个上下文。该装置向客户端设备传送该一个或多个经加密客户端设备上下文(2308)。该装置移除该至少一个上下文(2310)。该装置从客户端设备接收消息,该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息(2312)。在一方面,使用信息指示该消息的传输是缩减数据传输还是突发数据传输。在一方面,网络设备可基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文。在一方面,来自客户端设备的该消息包括资源建立请求以及该一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文。例如,该消息可以是图10中的资源建立请求消息1016。该装置响应于该消息而获得用于客户端设备的网络地址(2314)。该装置向客户端设备传送该网络地址(2316)。在一方面,该装置在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段,第二阈值时间段大于第一阈值时间段。在一个方面,该装置当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息(2318)。在一方面,资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在另一方面,该装置从客户端设备接收资源释放请求消息(2320)。在此类方面,该装置将来自客户端设备的资源释放请求消息传送给网关(2322)。在一方面,资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一些方面,操作2318与操作2320和2322可以相替代地执行。例如,如果操作2318被执行,则操作2320和2322可以不被执行。作为另一示例,如果操作2320和2322被执行,则操作2318可以不被执行。

[0258] 图24是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2400。该方法可由实现IoT功能(例如,控制面IoTF,诸如图1的控制面IoTF 106)的诸如网络设备之类的装置(例如,图1的网络设备105或图21的装置2100)执行。

[0259] 该装置从第二客户端设备接收控制面分组(2402)。在一方面,第二客户端设备不同于初始从其接收到要与网络通信的请求的客户端设备。该装置向第二网络设备请求关于第二客户端设备的上下文,该请求包括控制面(CP)经加密客户端设备上下文(2404)。该装

置从第二网络设备接收关于第二客户端设备的上下文(2406)。该装置生成新的经加密客户端设备上下文(2408)。该装置将新的经加密客户端设备上下文传送给第二客户端设备(2410)。

[0260] 图25(包括图25A和25B)是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2500。该方法可由实现IoT功能(例如,用户面IoTF,诸如图1的用户面IoTF 108)的诸如网络设备之类的装置(例如,图1的网络设备105或图21的装置2100)执行。应理解,图25中用虚线指示的操作表示可选操作。

[0261] 该装置获得用于与客户端设备相关联的经加密客户端设备上下文的密钥(例如,密钥$K_{CDC-IoTF-U}$)(2502)。该装置从客户端设备接收第一数据分组(例如,UL数据分组)和经加密客户端设备上下文(2504)。该装置使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文(2506)。该装置基于安全性上下文来解密和验证第一数据分组(2508)。该装置在解密和验证成功时将第一数据分组转发给服务网络(2510)。

[0262] 在一方面,该装置从服务器或分组数据网络网关接收第二数据分组(例如,图9的消息914中的DL数据分组)(2512)。该装置确定第二数据分组被转发到的网络接入节点(2514)。该装置向第二数据分组添加临时标识符,该临时标识符使得网络接入节点能确定客户端设备(2516)。该装置使用用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护(2518)。该装置(例如,经由图9中的消息934)将第二数据分组转发给客户端设备(2520)。

[0263] 图26(包括图26A和26B)是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2600。该方法可由实现IoT功能(例如,控制面IoTF,诸如图1的控制面IoTF 106)的诸如网络设备之类的装置(例如,图1的网络设备105或图21的装置2100)执行。应理解,图26中用虚线指示的操作表示可选操作。

[0264] 该装置从客户端设备接收要与网络通信的请求(2602)。该装置向归属订户服务器(HSS)/认证授权记账(AAA)服务器请求认证信息(2604)。该装置与客户端设备执行相互认证(2606)。

[0265] 该装置与客户端设备建立至少一个上下文,该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息(2608)。在一方面,该网络状态信息至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥。该装置确定要生成一个或多个经加密客户端设备上下文,其中该确定基于请求中指示的经加密客户端设备上下文使用信息、客户端设备的订阅、和/或策略中的至少一者(2610)。

[0266] 该装置生成一个或多个经加密客户端设备上下文(2612)。在一方面,该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文。在一方面,该一个或多个经加密客户端设备上下文包括将用于数据相关通信的第一上下文和将用于控制相关通信的第二上下文。该装置向客户端设备传送该一个或多个经加密客户端设备上下文(2614)。该装置移除该至少一个上下文(2616)。该装置从客户端设备接收消息,该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息(2618)。该装置基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文(2620)。该装置在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发

数据传输时维持该至少一部分上下文达第二阈值时间段，第二阈值时间段大于第一阈值时间段(2622)。

[0267] 示例性装置(例如，网络接入节点)和该装置上的方法

[0268] 图27是根据本公开的一个或多个方面(例如，与以下描述的图28和29的方法有关的各方面)的装置2700的解说。装置2700包括通信接口(例如，至少一个收发机)2702、网络通信接口2703、存储介质2704、用户接口2706、存储器设备2708以及处理电路2710。

[0269] 这些组件可以经由信令总线或其他合适的组件(由图27中的连接线一般化地表示)彼此耦合和/或彼此进行电通信。取决于处理电路2710的具体应用和整体设计约束，信令总线可包括任何数目的互连总线和桥接器。信令总线将各种电路链接在一起以使得通信接口2702、网络通信接口2703、存储介质2704、用户接口2706和存储器设备2708中的每一者与处理电路2710耦合和/或进行电通信。信令总线还可链接各种其他电路(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，且因此将不再进一步描述。

[0270] 通信接口2702可被适配成促成装置2700的无线通信。例如，通信接口2702可包括被适配成促成关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/或代码(例如，指令)。通信接口2702可耦合到一个或多个天线2712以用于在无线通信系统内进行无线通信。通信接口2702可以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2702包括发射机2714和接收机2716。

[0271] 网络通信接口2703可被适配成促成装置2700的通信。例如，网络通信接口2703可包括适配成促成关于网络中的一个或多个网络实体双向地进行信息通信的电路系统和/或代码(例如，指令)。网络通信接口2703可以配置有一个或多个独立接收机和/或发射机以及一个或多个收发机。

[0272] 存储器设备2708可表示一个或多个存储器设备。如所指示的，存储器设备2708可维持网络相关信息/连同由装置2700使用的其他信息。在一些实现中，存储器设备2708和存储介质2704被实现为共用存储器组件。存储器设备2708还可被用于存储由处理电路2710或由装置2700的某个其他组件操纵的数据。

[0273] 存储介质2704可表示用于存储代码(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计算机可读、机器可读、和/或处理器可读设备。存储介质2704还可被用于存储由处理电路2710在执行代码时操纵的数据。存储介质2704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、包含或携带代码的各种其他介质。

[0274] 作为示例而非限制，存储介质2704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代码的合适介质。存储介质2704可以实施在制品(例如，计算机程序产品)中。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2704可以是非瞬态(例如，有形)存储介质。

[0275] 存储介质2704可被耦合至处理电路2710以使得处理电路2710能从存储介质2704

读取信息和向存储介质2704写入信息。即，存储介质2704可耦合到处理电路2710，以使得存储介质2704至少能由处理电路2710访问，包括其中至少一个存储介质被集成到处理电路2710的示例和/或其中至少一个存储介质与处理电路2710分开(例如，驻留在装置2700中、在装置2700外部、跨多个实体分布等)的示例。

[0276] 由存储介质2704存储的代码和/或指令在由处理电路2710执行时使处理电路2710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2704可包括被配置用于以下动作的操作：调节处理电路2710的一个或多个硬件块处的操作以及利用通信接口2702通过利用其相应通信协议来进行无线通信。

[0277] 处理电路2710一般被适配成用于处理，包括执行存储在存储介质2704上的此类代码/指令。如本文中使用的，术语“代码”或“指令”应当被宽泛地解读成包括但不限于编程、指令、指令集、数据、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行件、执行的线程、规程、函数等，无论其被称为软件、固件、中间件、微代码、硬件描述语言、还是其他术语。

[0278] 处理电路2710被安排成获得、处理和/或发送数据，控制数据访问和存储，发布命令，以及控制其他期望操作。在至少一个示例中，处理电路2710可包括被配置成实现由恰适介质提供的期望代码的电路系统。例如，处理电路2710可被实现为一个或多个处理器、一个或多个控制器、和/或配置成执行可执行代码的其他结构。处理电路2710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、或者其任何组合。通用处理器可包括微处理器，以及任何常规处理器、控制器、微控制器、或状态机。处理电路2710还可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2710的这些示例是为了解说，并且还设想了落在本公开范围内的其他合适的配置。

[0279] 根据本公开的一个或多个方面，处理电路2710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。如本文所使用的，涉及处理电路2710的术语“适配”可指处理电路2710被配置、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。

[0280] 根据装置2700的至少一个示例，处理电路2710可包括接收电路/模块2722、临时标识符添加电路/模块2724、存储电路/模块2726、临时标识符移除电路/模块2728、数据分组转发电路/模块2730、分组处理电路/模块2732、分组加密和保护电路/模块2734、上下文重构/移除电路/模块2738、以及网络地址获得/释放电路/模块2740中的一者或多者，它们被适配成执行本文描述的任何或所有特征、过程、功能、操作、和/或例程(例如，关于图28和29描述的特征、过程、功能、操作、和/或例程)。

[0281] 接收电路/模块2722可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如，存储在存储介质2704上的接收指令2742)：从客户端设备接收带有要与网络通信的请求的第一数据分组，从客户端设备接收第一数据分组和经加密客户端设备上下文，从在网络节点处实现的网络功能接收第二数据分组，以及从客户端设备接收包括资源建立请求以及一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上

下文的消息。

[0282] 临时标识符添加电路/模块2724可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的临时标识符添加指令2744):向第一数据分组添加临时标识符。

[0283] 存储电路/模块2726可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的存储指令2746):存储用于客户端设备的临时标识符。例如,临时标识符可以是蜂窝小区无线电网络临时标识符(C-RNTI)。在一方面,临时标识符被存储达预定时间段。

[0284] 临时标识符移除电路/模块2728可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的临时标识符移除指令2748):移除第二数据分组中的临时标识符。

[0285] 数据分组转发电路/模块2730可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的数据分组转发指令2750):确定第一数据分组旨在去往的第一网络节点,在解密和验证成功时将第一数据分组转发给服务网络,确定请求将被转发到的网络功能,其中该确定是在网络接入节点处预配置的,确定第二数据分组将被转发到的客户端设备,以及将第二数据分组转发给客户端设备。

[0286] 分组处理电路/模块2732可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的分组处理指令2752):基于安全性上下文来解密和验证第一数据分组。

[0287] 分组加密和保护电路/模块2734可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的分组加密和保护指令2754):使用用户面(UP)客户端设备密钥来对分组进行加密或完整性保护,基于安全性上下文来解密和验证第一数据分组,和/或使用用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护。

[0288] 上下文重构/移除电路/模块2738可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的上下文重构/移除指令2758):获得用于与客户端设备相关联的经加密客户端设备上下文的密钥(例如,密钥$K_{CDC-IoTF-U}$),使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文,从经加密客户端设备上下文重构至少一个上下文,基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文,移除至少一个上下文,和/或在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段,第二阈值时间段大于第一阈值时间段。

[0289] 网络地址获得/释放电路/模块2740可包括适配成执行与例如以下操作有关的若干功能的电路系统和/或指令(例如,存储在存储介质2704上的网络地址获得/释放指令2760):响应于该消息而获得用于客户端设备的网络地址,向客户端设备传送网络地址,从客户端设备向网关传送资源释放请求消息,其中资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源,和/或当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息,其中资源释放请求消

息使得网关能释放用于该客户端设备的一个或多个资源。

[0290] 如上所提及的，由存储介质2704存储的指令在由处理电路2710执行时使处理电路2710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2704可包括以下一者或多者：接收指令2742、临时标识符添加指令2744、存储指令2746、临时标识符移除指令2748、数据分组转发指令2750、分组处理指令2752、分组加密和保护指令2754、上下文重构/移除指令2758、以及网络地址获得/释放指令2760。

[0291] 图28是解说根据本公开的各个方面的用于在IoT网络架构中通信的方法的流程图2800。该方法可由诸如网络接入节点之类的装置(例如，图1的网络接入节点104或图27的装置2700)执行。

[0292] 该装置从客户端设备接收带有要与网络通信的请求的第一数据分组(2802)。该装置存储用于客户端设备的临时标识符(2804)。例如，临时标识符可以是蜂窝小区无线电网络临时标识符(C-RNTI)，并且临时标识符可被存储达预定时间段。该装置向第一数据分组添加临时标识符(2806)。

[0293] 该装置确定第一数据分组旨在去往的第一网络节点(2808)。该装置确定该请求将被转发到的网络功能，其中该确定是在网络接入节点处预配置的(2810)。该装置将第一数据分组转发给该网络功能(2812)。

[0294] 该装置从在网络节点处实现的网络功能接收第二数据分组(2814)。该装置确定第二数据分组将被转发到的客户端设备(2816)。在一方面，该装置通过从第二数据分组中的临时标识符标识客户端设备来确定第二数据分组将被转发到的客户端设备。该装置移除第二数据分组中的临时标识符(2818)。该装置将第二数据分组转发给客户端设备(2820)。

[0295] 图29(包括图29A和29B)是解说根据本公开的各个方面的用于在网络中通信的方法的流程图2900。该方法可由诸如网络接入节点之类的装置(例如，图12的网络接入节点1204或图27的装置2700)执行。应理解，图27中用虚线指示的操作表示可选操作。

[0296] 该装置获得用于与客户端设备相关联的经加密客户端设备上下文的密钥(例如，密钥$K_{CDC\text{-}IoTF\text{-}U}$) (2902)。该装置从客户端设备接收第一数据分组(例如，UL数据分组)和经加密客户端设备上下文(2904)。该装置使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文(2906)。该装置基于安全性上下文来解密和/或验证第一数据分组(2908)。该装置在解密和验证成功时将第一数据分组转发给服务网络(2910)。该装置从服务器或分组数据网络网关接收第二数据分组(例如，DL数据分组) (2912)。该装置使用用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护(2914)。该装置将第二数据分组转发给客户端设备(2916)。该装置移除至少一个上下文(2918)。该装置从客户端设备接收包括资源建立请求以及一个或多个经加密客户端设备上下文中的至少一个经加密客户端设备上下文的消息(2920)。该装置响应于该消息而获得用于客户端设备的网络地址(2922)。该装置向客户端设备传送该网络地址(2924)。在一个方面，该装置当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息(2926)。在一方面，资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在另一方面，该装置从客户端设备接收资源释放请求消息(2928)。在此类方面，该装置将来自客户端设备的资源释放请求消息传送给网关(2930)。在一方面，资源释放请求消息使得网关能释放用于该客户端设备的一个或多个资源。在一些

方面，操作2926与操作2928和2930可以相替代地执行。例如，如果操作2926被执行，则操作2928和2930可以不被执行。作为另一示例，如果操作2928和2930被执行，则操作2926可以不被执行。

[0297] 附图中解说的一个或多个组件、步骤、特征和/或功能可以被重新编排和/或组合成单个组件、步骤、特征或功能，或实施在数个组件、步骤或功能中。也可添加附加的元件、组件、步骤、和/或功能而不会脱离本文中所公开的新颖性特征。附图中所解说的装置、设备和/或组件可以被配置成执行本文所描述的一个或多个方法、特征、或步骤。本文中描述的新颖算法还可以高效地实现在软件中和/或嵌入到硬件中。

[0298] 应理解，所公开的方法中各步骤的具体次序或阶层是示例性过程的解说。基于设计偏好，应理解，可以重新编排这些方法中各步骤的具体次序或阶层。所附方法权利要求以样本次序呈现各种步骤的要素，且并不意味着被限定于所呈现的具体次序或阶层，除非在本文中有特别叙述。附加的元件、组件、步骤、和/或功能也可被添加或不被利用，而不会脱离本公开。

[0299] 尽管本公开的特征可能已经针对某些实现和附图作了讨论，但本公开的所有实现可包括本文所讨论的有利特征中的一个或多个。换言之，尽管可能讨论了一个或多个实现具有某些有利特征，但也可以根据本文中讨论的各种实现中的任一实现来使用此类特征中的一个或多个。以类似方式，尽管示例性实现在本文中可能是作为设备、系统或方法实现来进行讨论的，但是应该理解，此类示例性实现可以在各种设备、系统、和方法中实现。

[0300] 另外，注意到至少一些实现是作为被描绘为流图、流程图、结构图、或框图的过程来描述的。尽管流程图可能会将各操作描述为顺序过程，但是这些操作中的许多操作能够并行或并发地执行。另外，这些操作的次序可被重新安排。过程在其操作完成时终止。在一些方面，过程可对应于方法、函数、规程、子例程、子程序等。当过程对应于函数时，它的终止对应于该函数返回调用方函数或主函数。本文中描述的各种方法中的一种或多种方法可部分地或全部地由可存储在机器可读、计算机可读和/或处理器可读存储介质中并由一个或多个处理器、机器和/或设备执行的编程(例如，指令和/或数据)来实现。

[0301] 本领域技术人员将可进一步领会，结合本文中公开的实现描述的各种解说性逻辑框、模块、电路、和算法步骤可被实现为硬件、软件、固件、中间件、微代码、或其任何组合。为了清楚地解说这种可互换性，各种解说性组件、框、模块、电路和步骤在上文已经以其功能性的形式一般性地作了描述。此类功能性是被实现为硬件还是软件取决于具体应用和施加于整体系统的设计约束。

[0302] 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”在本文中用于指代两个对象之间的直接或间接耦合。例如，如果对象A物理地接触对象B，且对象B接触对象C，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物理接触。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。

[0303] 如本文所使用的，术语“确定”涵盖各种各样的动作。例如，“确定”可包括演算、计算、处理、推导、研究、查找(例如，在表、数据库或其他数据结构中查找)、查明、及类似动作。而且，“确定”可包括接收(例如接收信息)、访问(例如访问存储器中的数据)、及类似动作。同样，“确定”还可包括解析、选择、选取、建立、及类似动作。如本文中所使用的，术语“获得”可包括一个或多个动作，包括但不限于接收、生成、确定、或其任何组合。

[0304] 提供先前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个方面。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”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第六款的规定下来解释，除非该要素是使用措辞“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措辞“用于.....的步骤”来叙述的。

[0305] 相应地，与本文中所描述的和附图中所示的示例相关联的各种特征可实现在不同示例和实现中而不会脱离本公开的范围。因此，尽管某些具体构造和安排已被描述并在附图中示出，但此类实现仅是解说性的并且不限制本公开的范围，因为对所描述的实现的各种其他添加和修改、以及删除对于本领域普通技术人员而言将是明显的。因此，本公开的范围仅由所附权利要求的字面语言及其法律等效来确定。

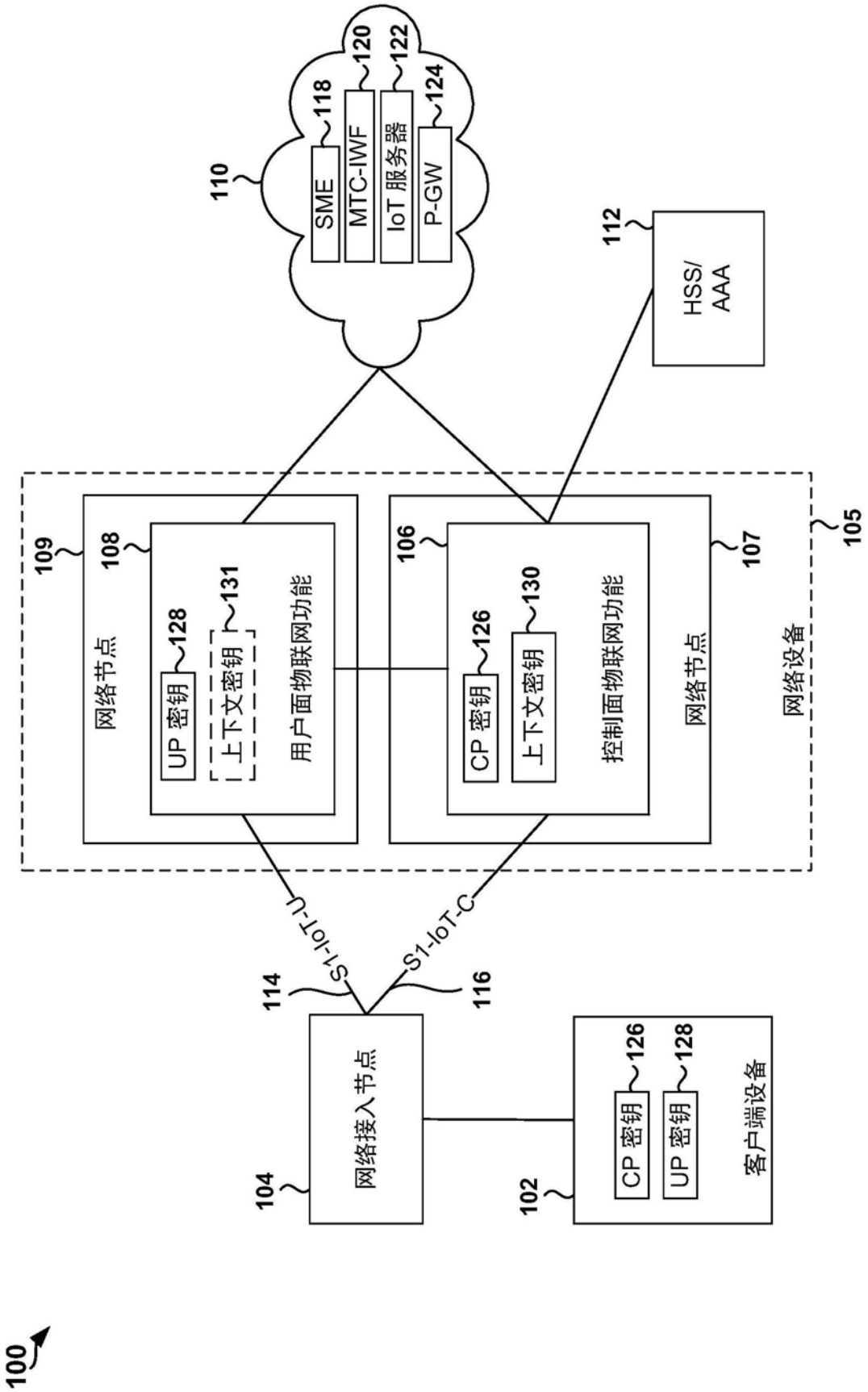

100
110
SME
118
MTC-IWF
120
IoT 服务器
122
P-GW
124
112
HSS/
AAA
105
网络设备
109
网络节点
108
UP 密钥
128
上下文密钥
131
用户面物联网功能
106
CP 密钥
126
上下文密钥
130
控制面物联网功能
107
网络节点
S1-IoT-U
S1-IoT-C
114
116
104
网络接入节点
102
CP 密钥
126
UP 密钥
128
客户端设备

图1

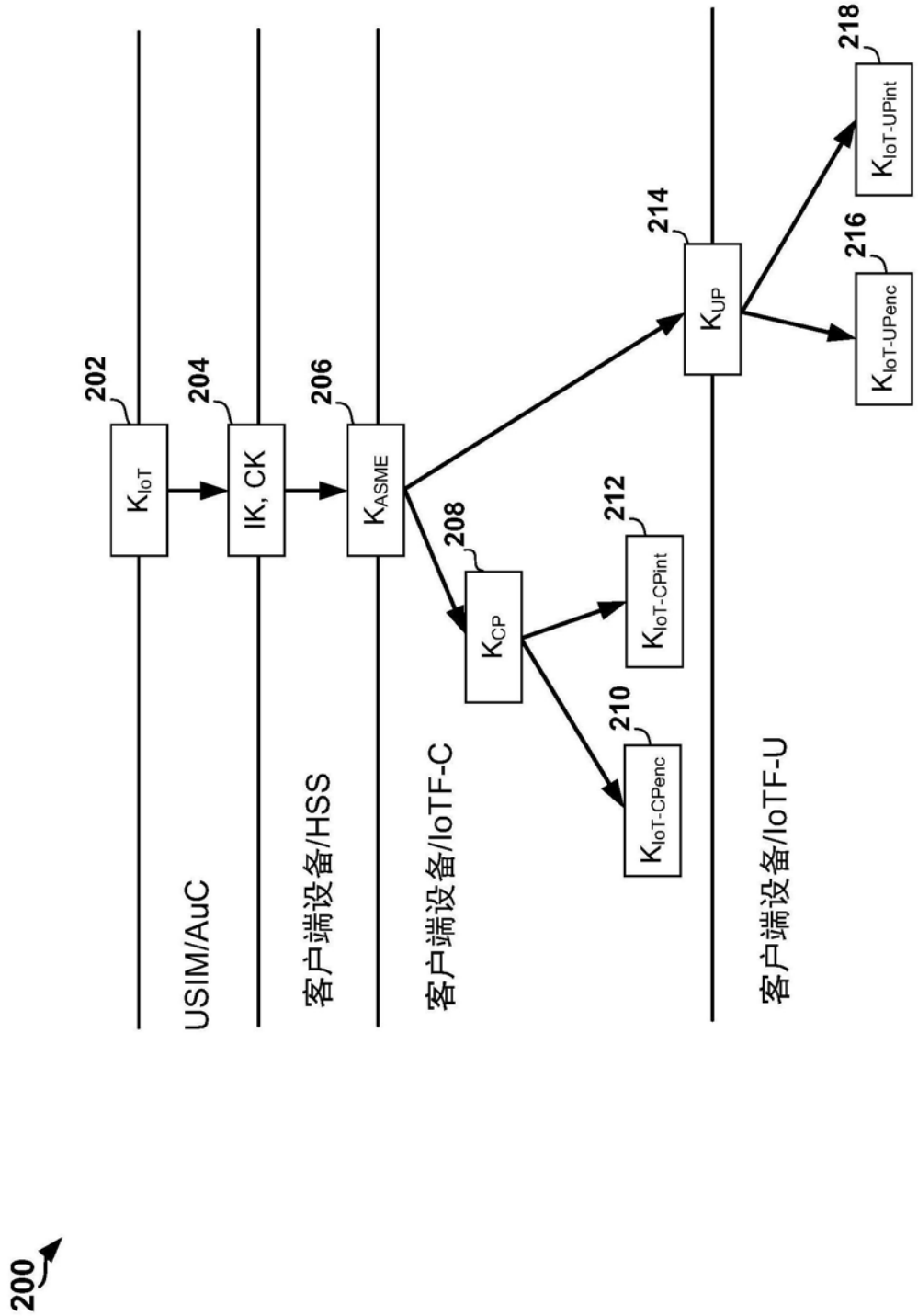

200
202
204
206
208
210
212
214
216
218
K_{IoT}
IK, CK
K_{ASME}
K_{CP}
$K_{IoT-CPenc}$
$K_{IoT-CPint}$
K_{UP}
$K_{IoT-UPenc}$
$K_{IoT-UPint}$
USIM/AuC
客户端设备/HSS
客户端设备/IoTF-C
客户端设备/IoTF-U

图2

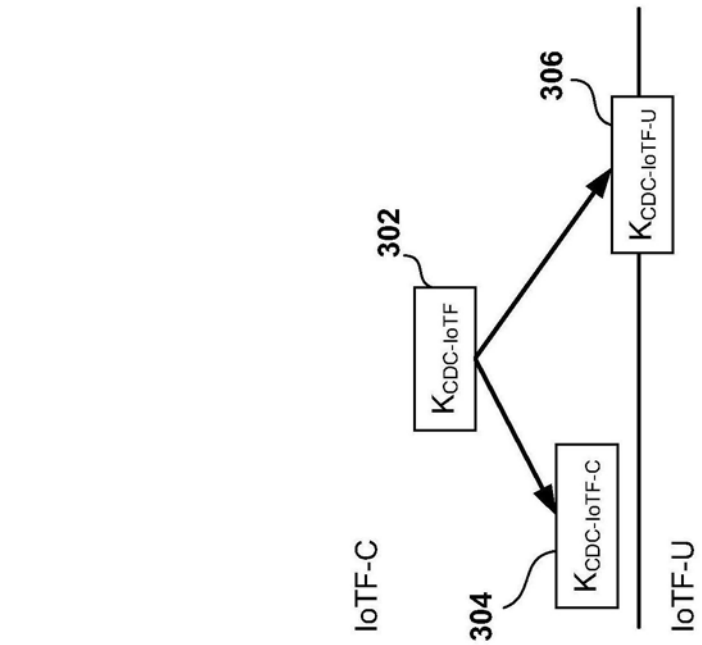


图3

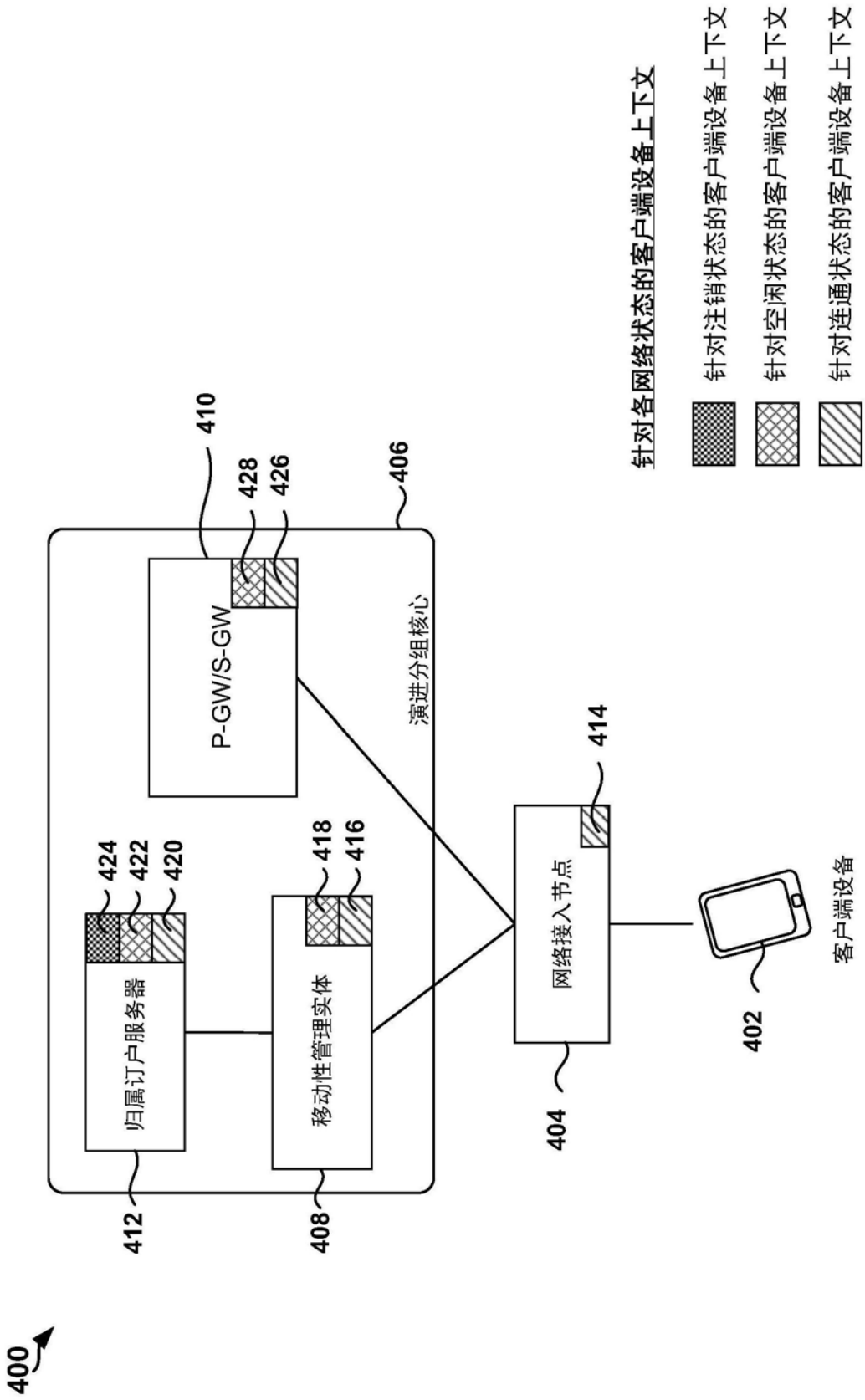

400
410
428
426
406
P-GW/S-GW
演进分组核心
424
422
420
418
416
归属订户服务器
移动性管理实体
414
网络接入节点
412
408
404
402
客户端设备
针对各网络状态的客户端设备上下文
针对注销状态的客户端设备上下文
针对空闲状态的客户端设备上下文
针对连通状态的客户端设备上下文

图4

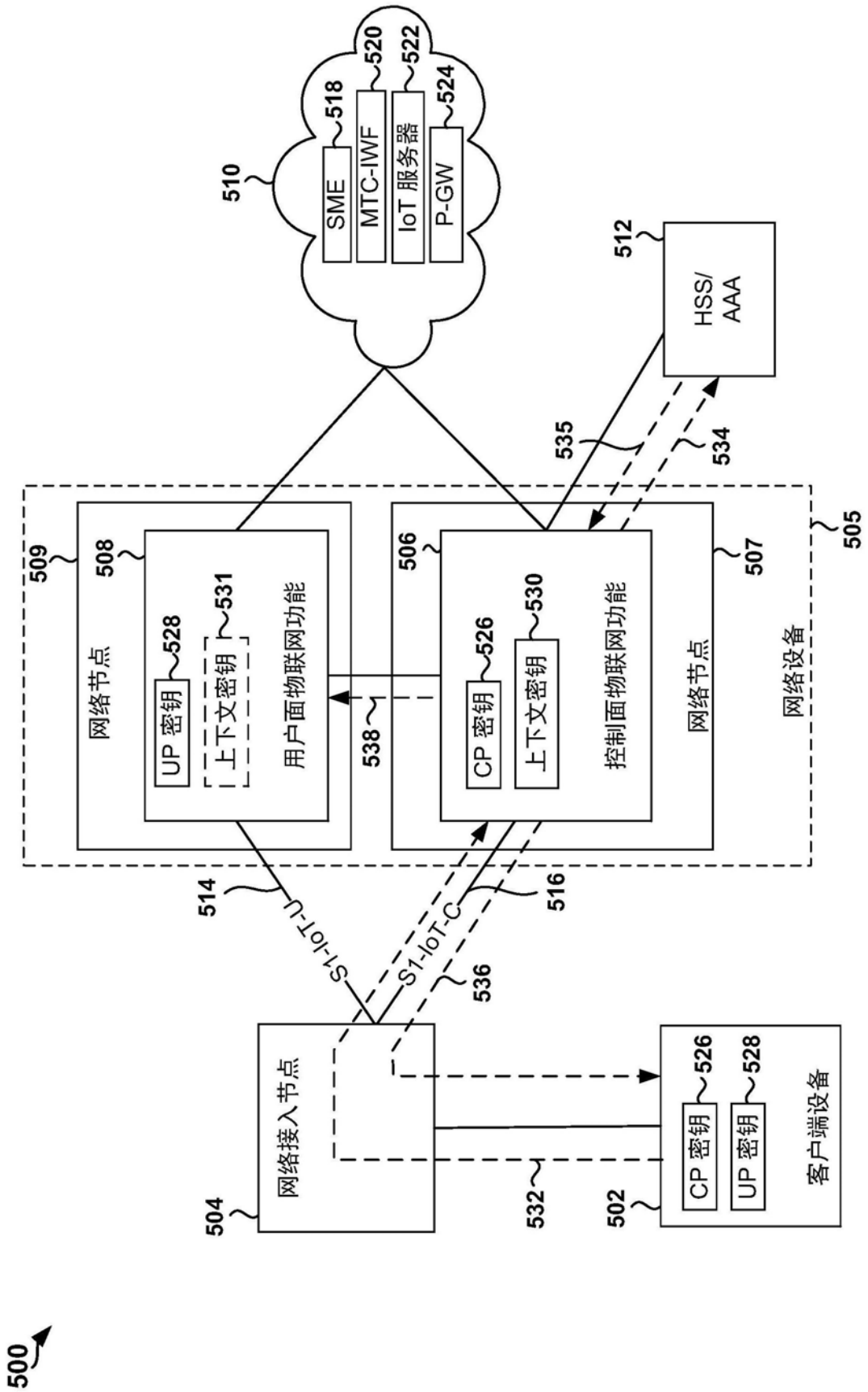

500
510
SME
518
MTC-IWF
520
IoT 服务器
522
P-GW
524
512
HSS/
AAA
535
534
505
网络设备
509
网络节点
508
UP 密钥
528
上下文密钥
531
用户面物联网功能
538
506
CP 密钥
526
上下文密钥
530
控制面物联网功能
网络节点
507
514
S1-IoT-U
S1-IoT-C
516
536
网络接入节点
504
532
502
CP 密钥
526
UP 密钥
528
客户端设备

图5

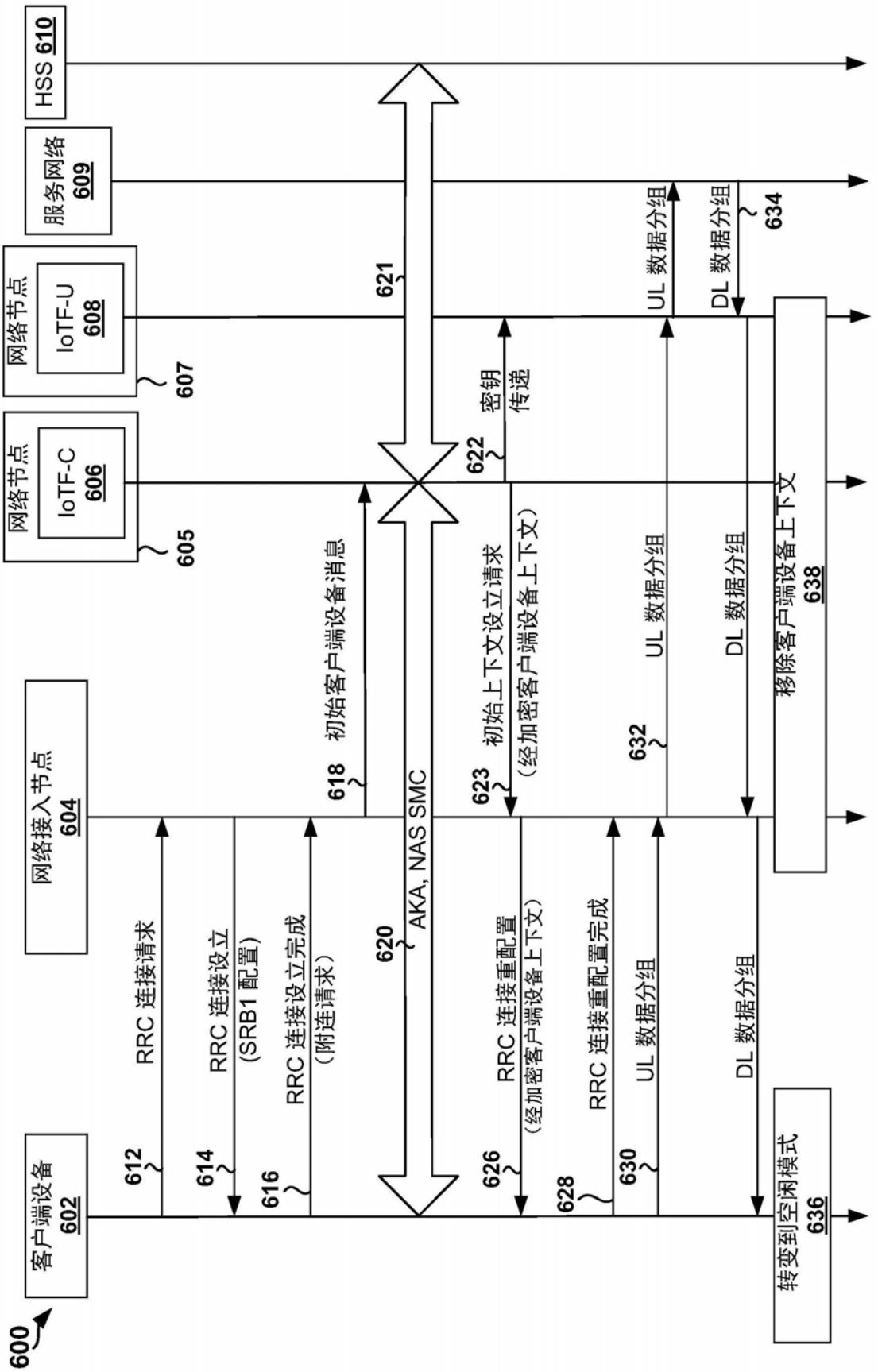

600
客户端设备 602
网络接入节点 604
网络节点 IoTF-C 606
网络节点 IoTF-U 608
服务网络 609
HSS 610
612 RRC 连接请求
614 RRC 连接设立 (SRB1 配置)
616 RRC 连接设立完成 (附连请求)
618 初始客户端设备消息
620 AKA, NAS SMC
621
622 密钥传递
623 初始上下文设立请求 (经加密客户端设备上下文)
626 RRC 连接重配置 (经加密客户端设备上下文)
628 RRC 连接重配置完成
630 UL 数据分组
632 UL 数据分组
634 DL 数据分组
636 转变到空闲模式
638 移除客户端设备上下文

图6

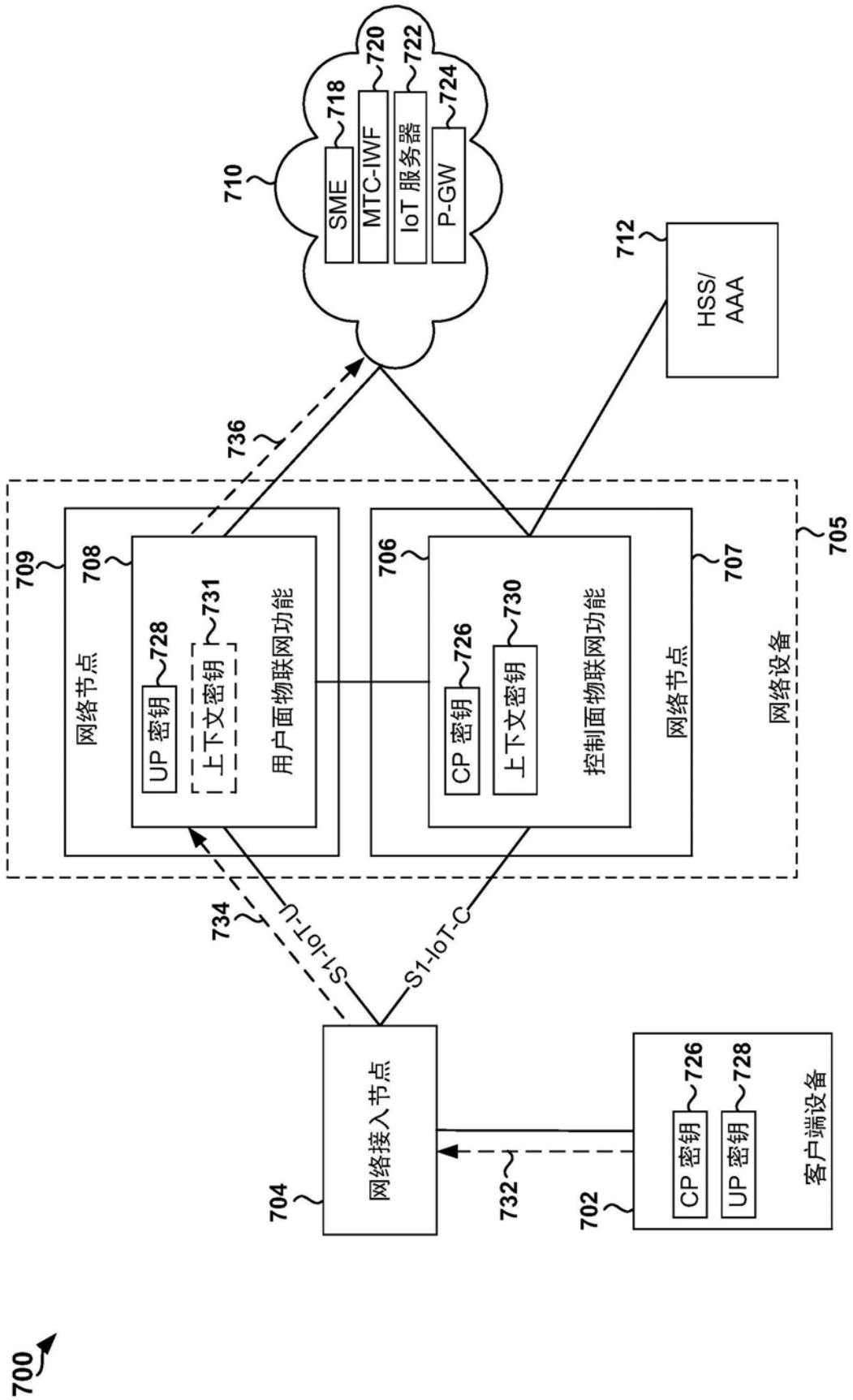

700
710
SME
718
MTC-IWF
720
IoT 服务器
722
P-GW
724
712
HSS/
AAA
736
705
网络设备
709
网络节点
708
UP 密钥
728
上下文密钥
731
用户面物联网功能
706
CP 密钥
726
上下文密钥
730
控制面物联网功能
网络节点
707
734
S1-IoT-U
S1-IoT-C
网络接入节点
704
732
702
CP 密钥
726
UP 密钥
728
客户端设备

图7

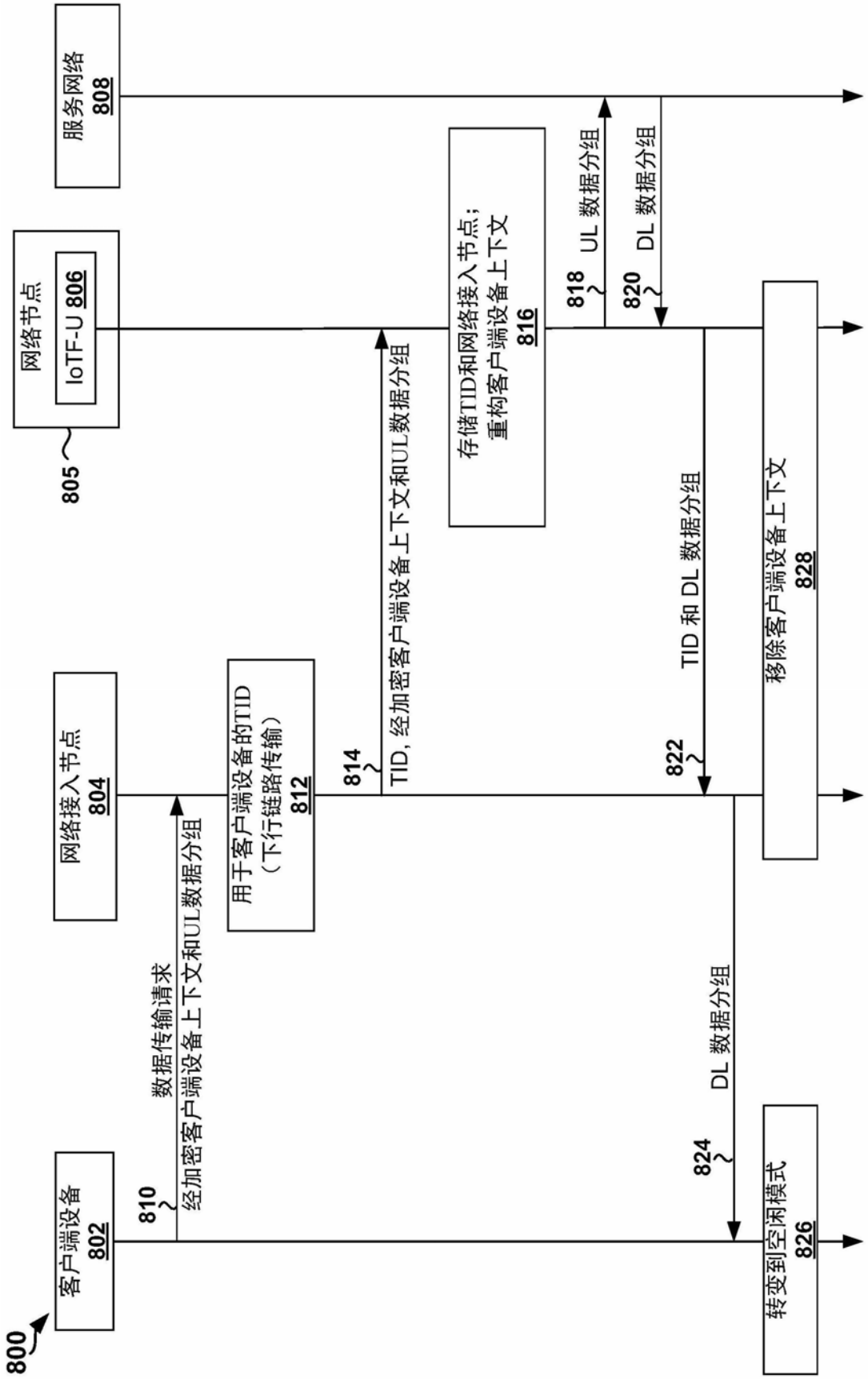

800
客户端设备
802
网络接入节点
804
网络节点
IoTF-U 806
805
服务网络
808
用于客户端设备的TID
（下行链路传输）
812
存储TID和网络接入节点；
重构客户端设备上下文
816
移除客户端设备上下文
828
转变到空闲模式
826
810
数据传输请求
经加密客户端设备上下文和UL数据分组
814
TID，经加密客户端设备上下文和UL数据分组
818
UL 数据分组
820
DL 数据分组
822
TID 和 DL 数据分组
824
DL 数据分组

图8

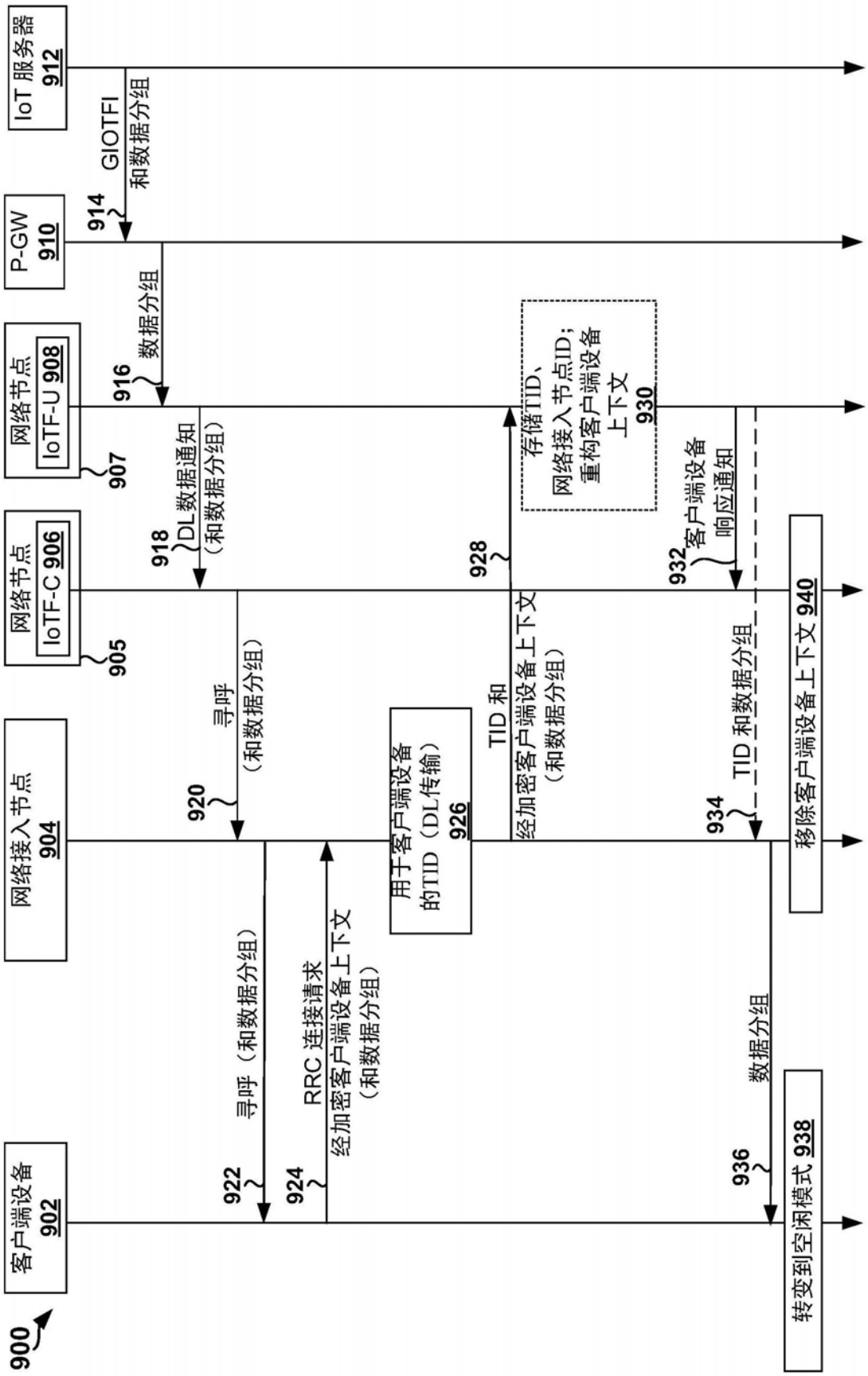

900
客户端设备 902
网络接入节点 904
网络节点 IoTF-C 906
网络节点 IoTF-U 908
P-GW 910
IoT 服务器 912
914 GIOTFI 和数据分组
916 数据分组
907
905
918 DL数据通知（和数据分组）
920 寻呼（和数据分组）
922 寻呼（和数据分组）
924 RRC 连接请求 经加密客户端设备上下文（和数据分组）
用于客户端设备的TID（DL传输）926
928 TID 和 经加密客户端设备上下文（和数据分组）
存储TID、网络接入节点ID；重构客户端设备上下文 930
932 客户端设备响应通知
934 TID 和数据分组
移除客户端设备上下文 940
936 数据分组
转变到空闲模式 938

图9

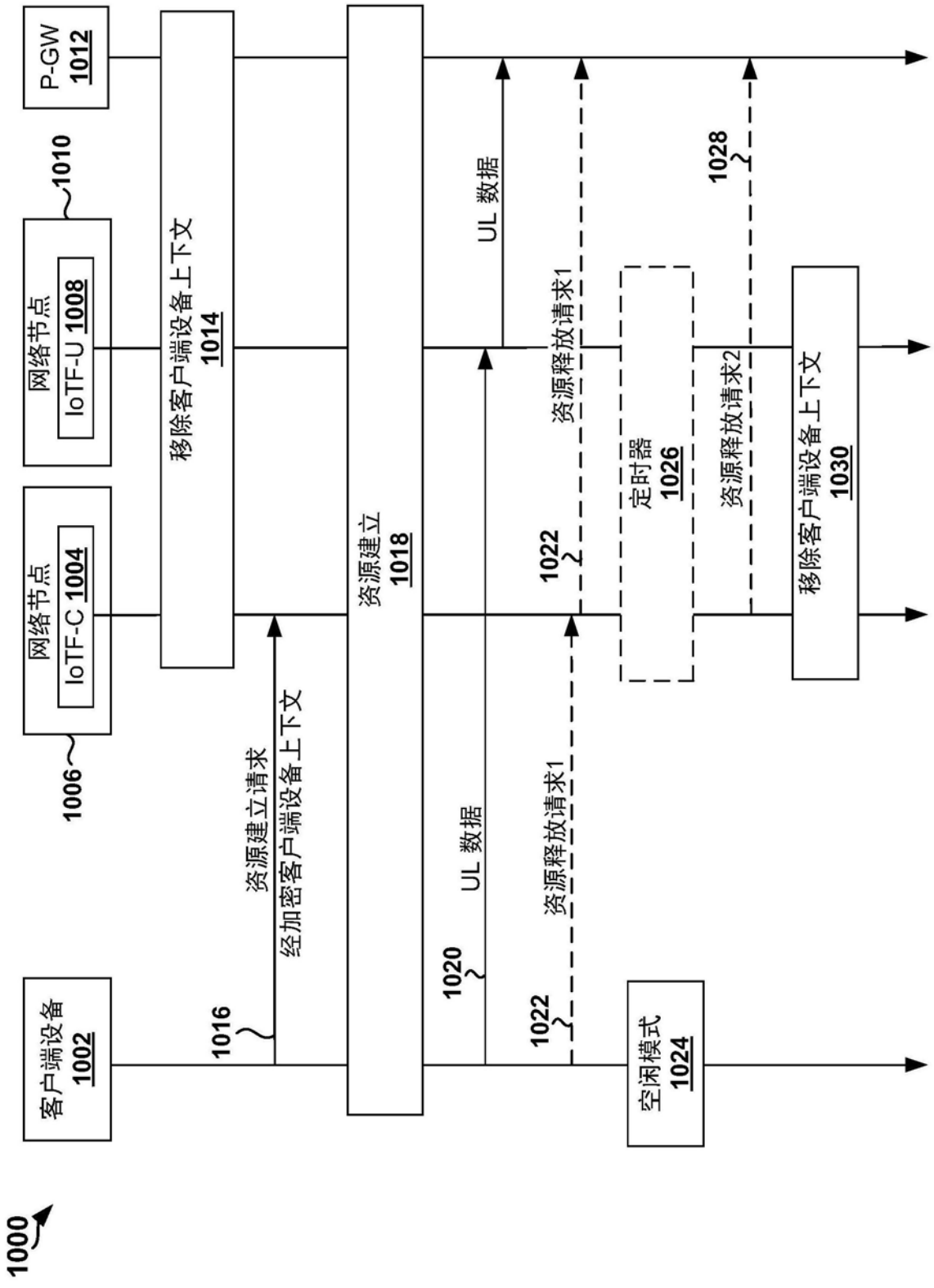

1000
客户端设备 1002
网络节点 IoTF-C 1004
1006
网络节点 IoTF-U 1008
1010
P-GW 1012
移除客户端设备上下文 1014
1016
资源建立请求
经加密客户端设备上下文
资源建立 1018
1020
UL 数据
1022
资源释放请求1
空闲模式 1024
1022
资源释放请求1
定时器 1026
1028
资源释放请求2
移除客户端设备上下文 1030
UL 数据

图10

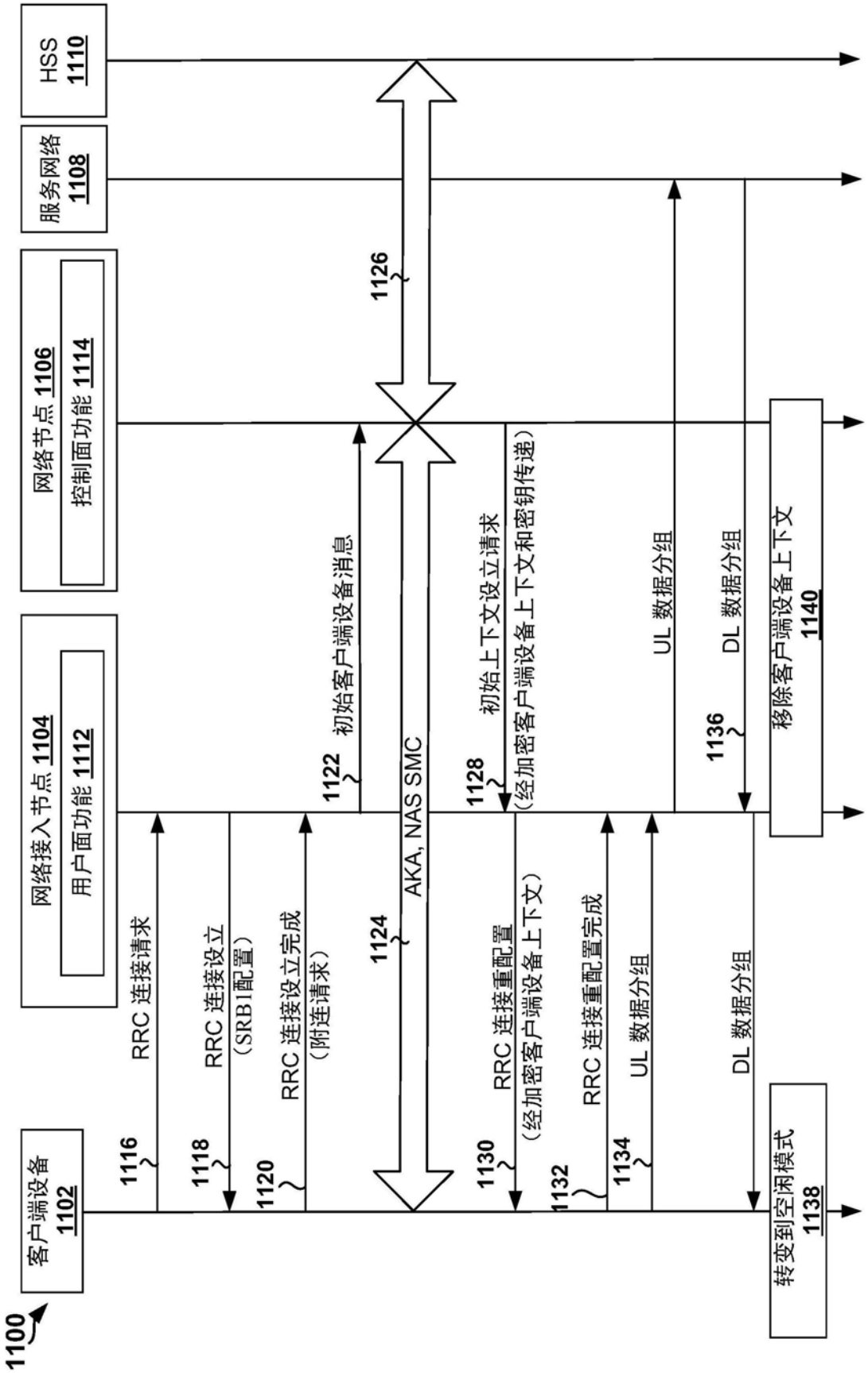

1100
客户端设备 1102
网络接入节点 1104
用户面功能 1112
网络节点 1106
控制面功能 1114
服务网络 1108
HSS 1110
1116 RRC 连接请求
1118 RRC 连接设立 (SRB1配置)
1120 RRC 连接设立完成 (附连请求)
1122 初始客户端设备消息
1124 AKA, NAS SMC
1126
1128 初始上下文设立请求 (经加密客户端设备上下文和密钥传递)
1130 RRC 连接重配置 (经加密客户端设备上下文)
1132 RRC 连接重配置完成
1134 UL 数据分组
1136 DL 数据分组
UL 数据分组
DL 数据分组
移除客户端设备上下文 1140
转变到空闲模式 1138

图11

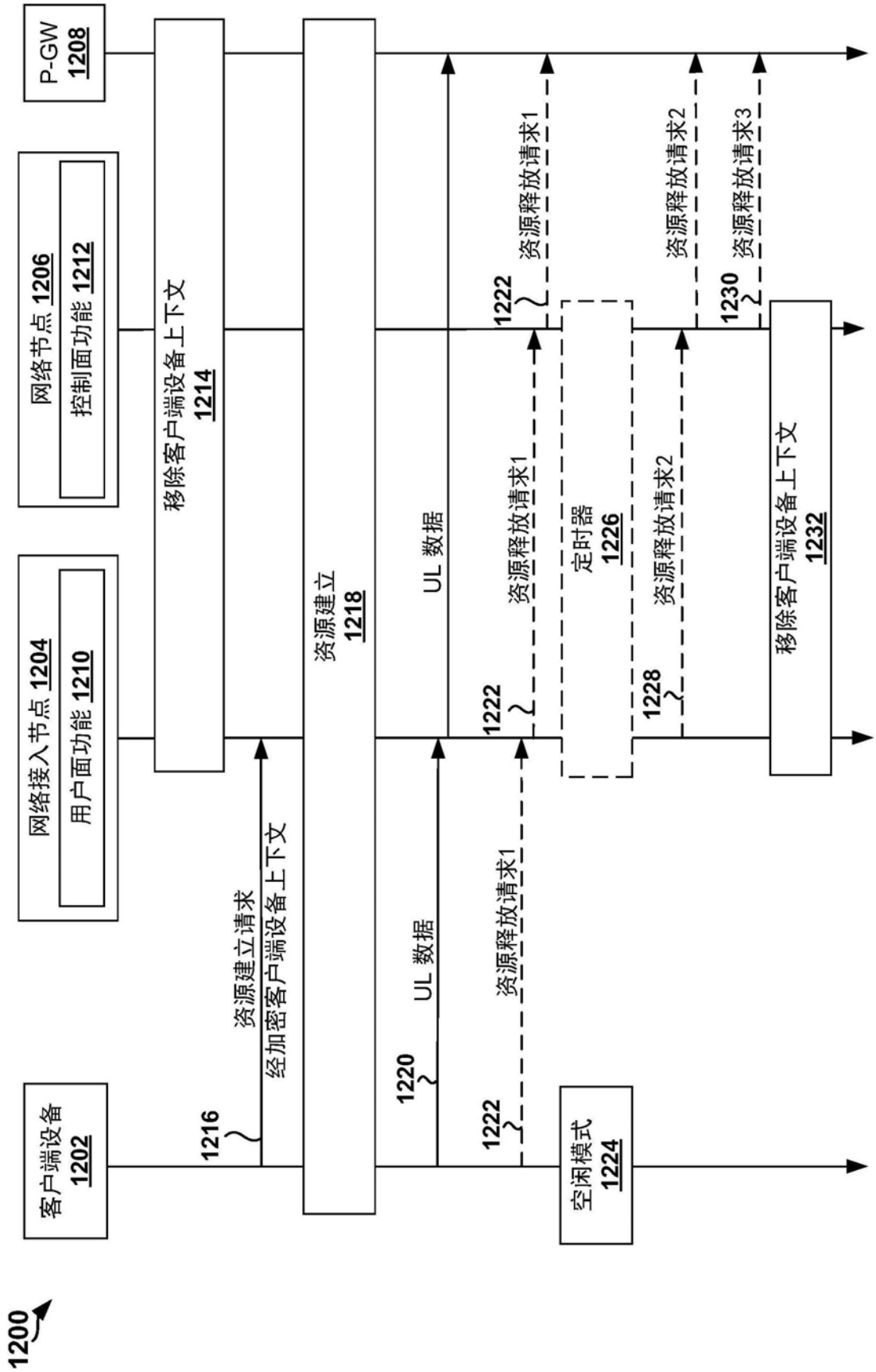

1200
客户端设备 1202
网络接入节点 1204
用户面功能 1210
网络节点 1206
控制面功能 1212
P-GW 1208
移除客户端设备上下文 1214
资源建立 1218
资源建立请求
经加密客户端设备上下文
1216
UL 数据
1220
资源释放请求1
1222
空闲模式 1224
定时器 1226
资源释放请求2
1228
资源释放请求3
1230
移除客户端设备上下文 1232

图12

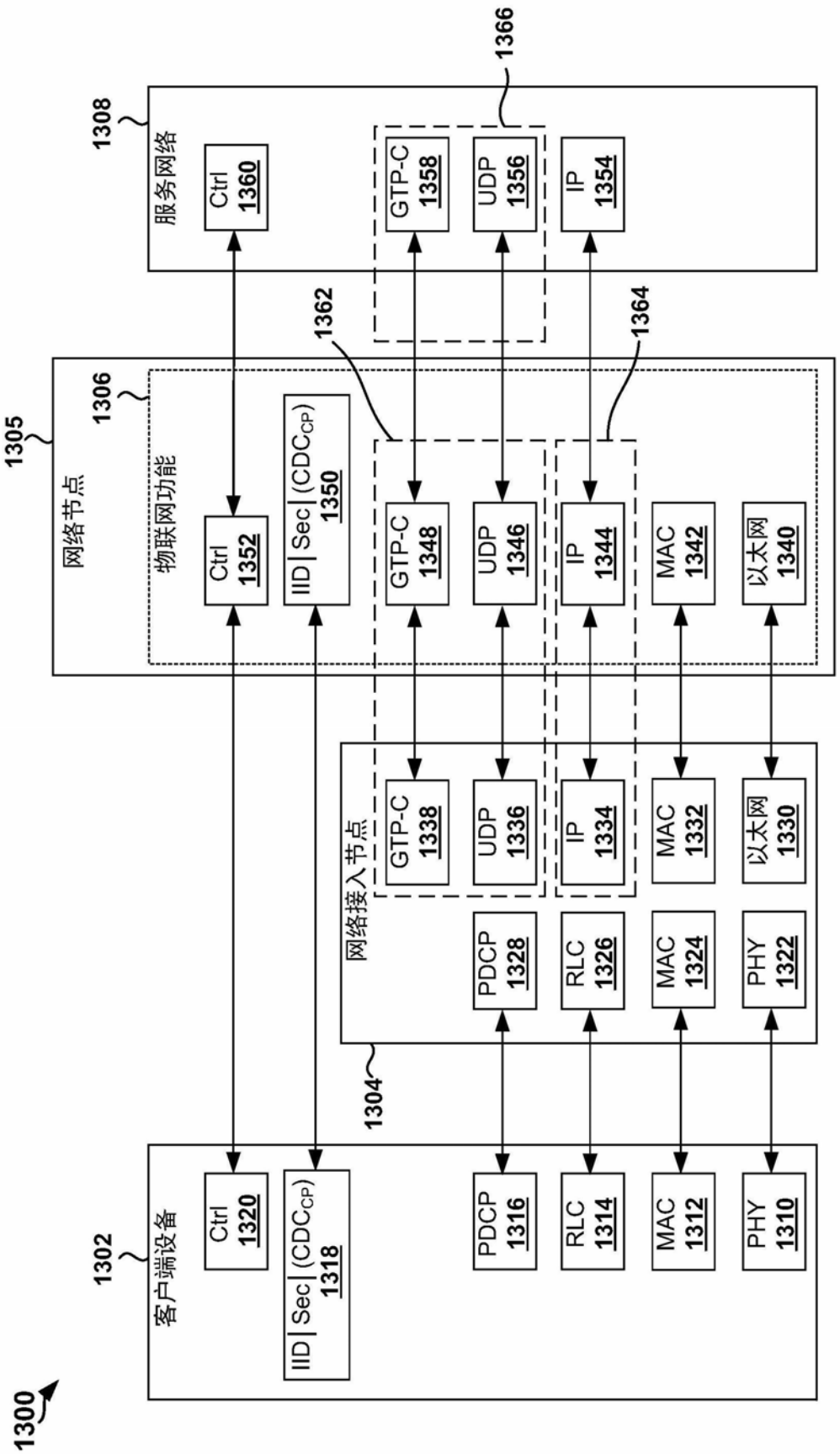

1300
1302
客户端设备
Ctrl 1320
IID | Sec | (CDCCP) 1318
PDCP 1316
RLC 1314
MAC 1312
PHY 1310
1304
网络接入节点
GTP-C 1338
UDP 1336
IP 1334
MAC 1332
以太网 1330
PDCP 1328
RLC 1326
MAC 1324
PHY 1322
1305
网络节点
1306
物联网功能
Ctrl 1352
IID | Sec | (CDCCP) 1350
GTP-C 1348
UDP 1346
IP 1344
MAC 1342
以太网 1340
1362
1364
1308
服务网络
Ctrl 1360
GTP-C 1358
UDP 1356
IP 1354
1366

图13

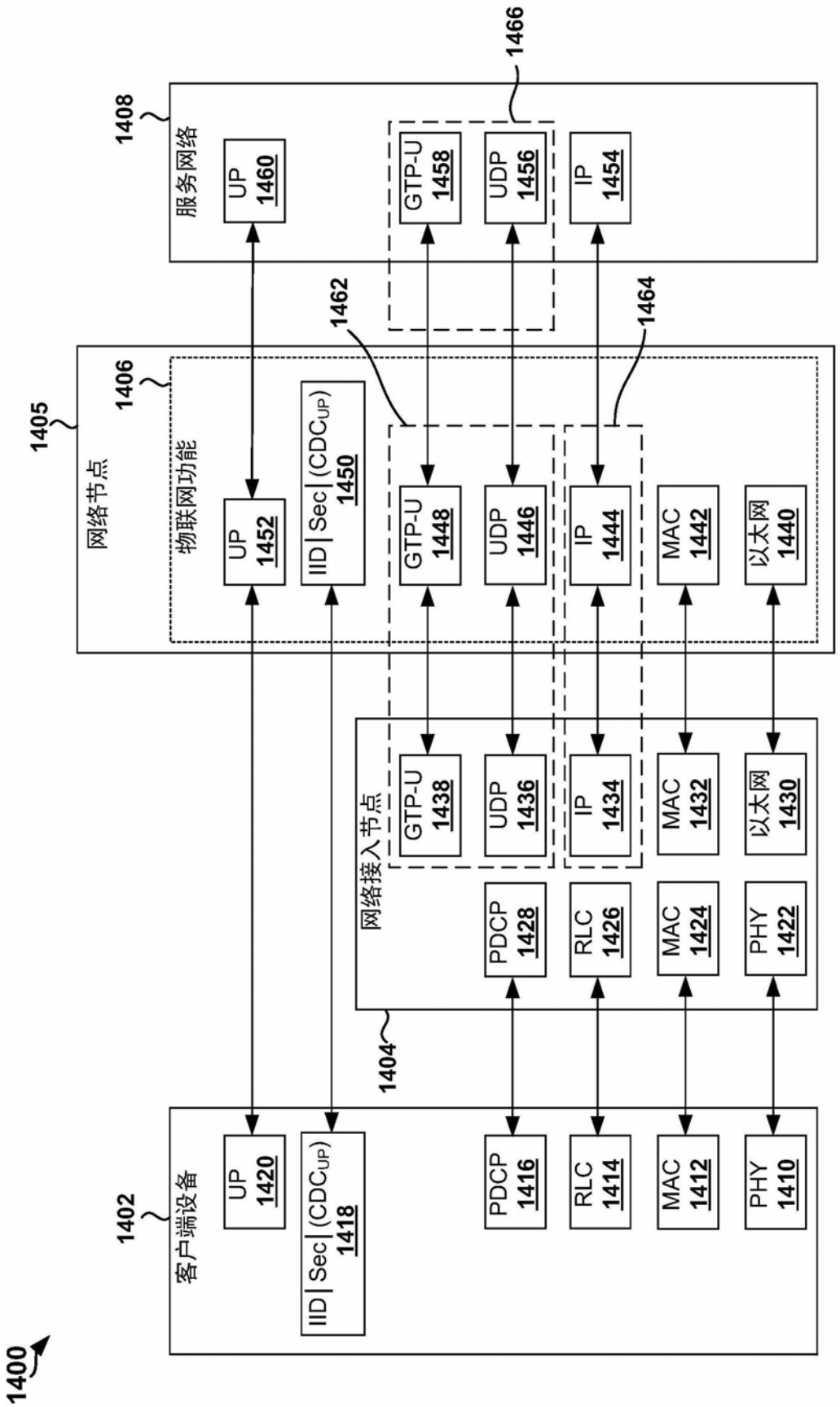

1400
1402
客户端设备
UP 1420
IID | Sec | (CDCUP) 1418
PDCP 1416
RLC 1414
MAC 1412
PHY 1410
1404
网络接入节点
GTP-U 1438
UDP 1436
IP 1434
MAC 1432
以太网 1430
PDCP 1428
RLC 1426
MAC 1424
PHY 1422
1405
网络节点
1406
物联网功能
UP 1452
IID | Sec | (CDCUP) 1450
GTP-U 1448
UDP 1446
IP 1444
MAC 1442
以太网 1440
1408
服务网络
UP 1460
GTP-U 1458
UDP 1456
IP 1454
1462
1464
1466

图14

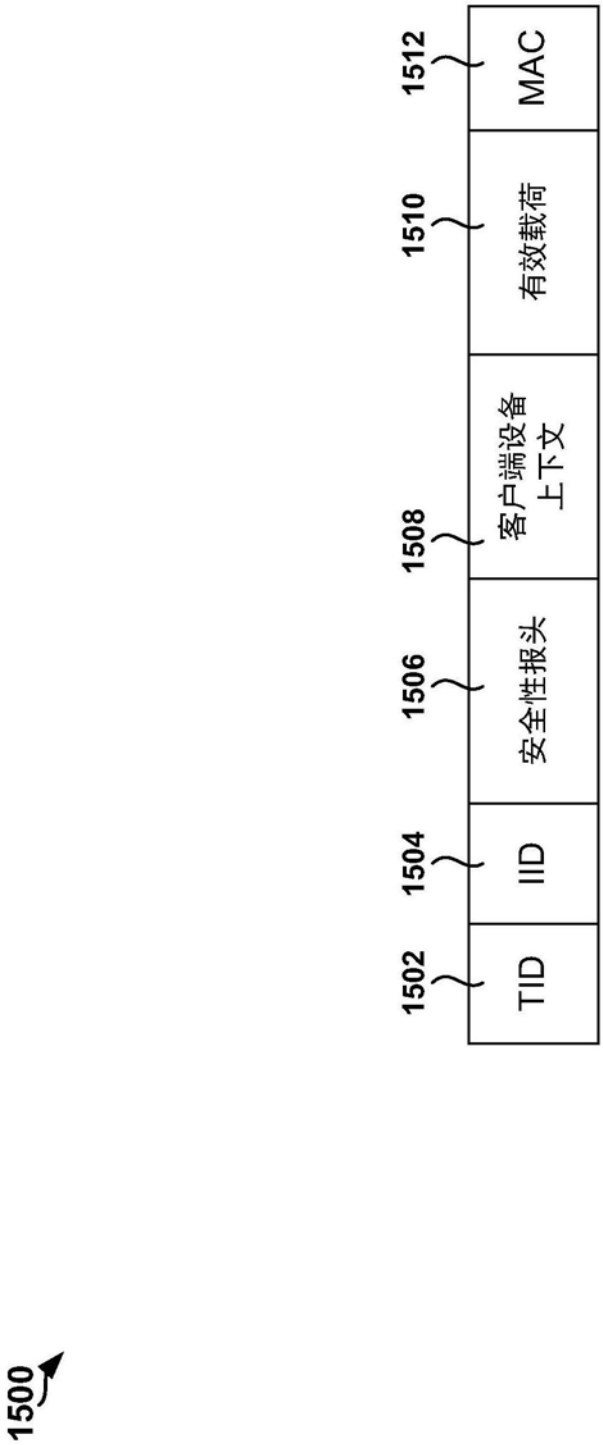

1500
1502
TID
1504
IID
1506
安全性报头
1508
客户端设备
上下文
1510
有效载荷
1512
MAC

图15

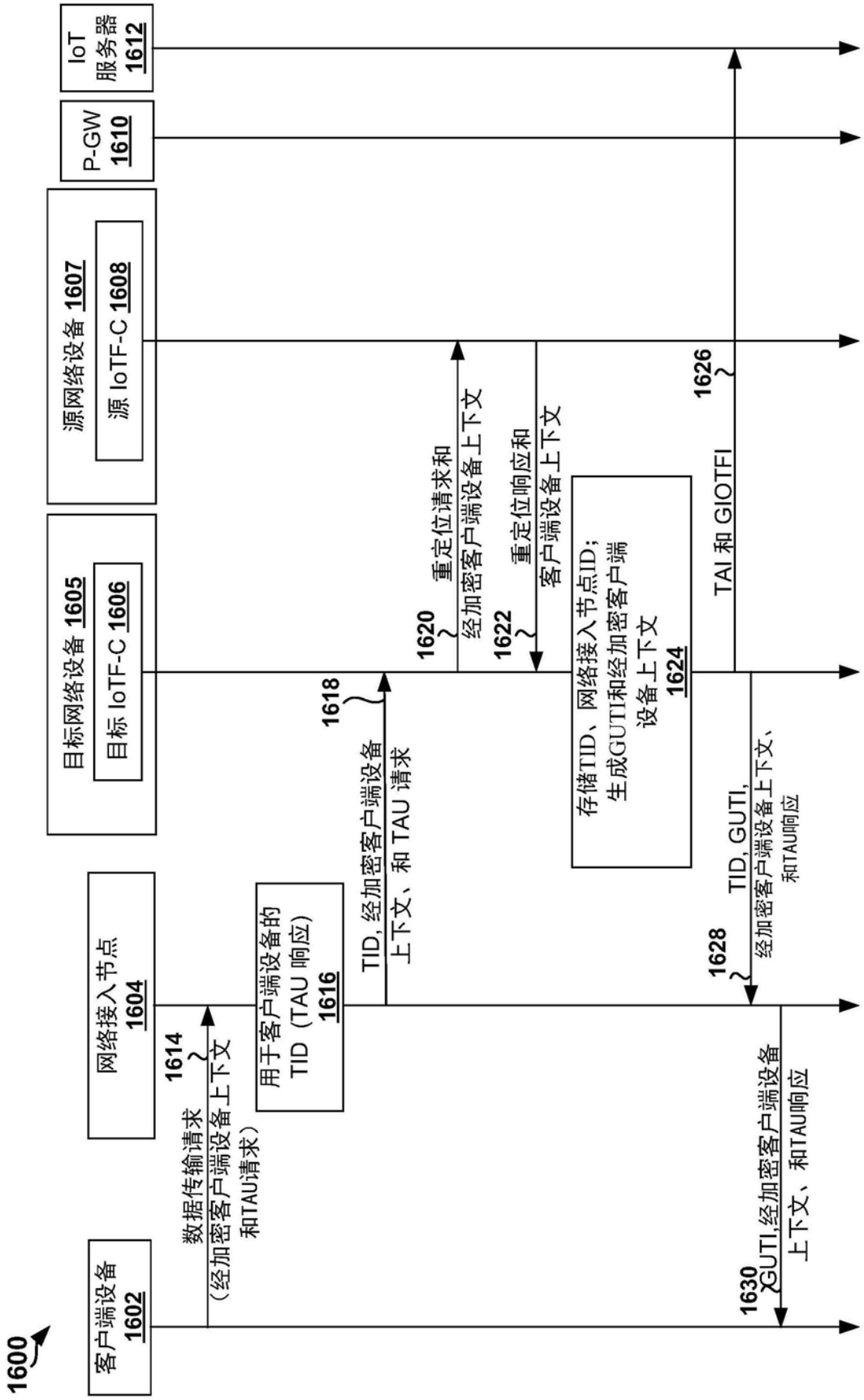

1600
客户端设备 1602
网络接入节点 1604
目标网络设备 1605
目标 IoTF-C 1606
源网络设备 1607
源 IoTF-C 1608
P-GW 1610
IoT 服务器 1612
1614
数据传输请求
（经加密客户端设备上下文和TAU请求）
用于客户端设备的 TID（TAU 响应）1616
1618
TID, 经加密客户端设备上下文、和 TAU 请求
1620
重定位请求和经加密客户端设备上下文
1622
重定位响应和客户端设备上下文
存储TID、网络接入节点ID；生成GUTI和经加密客户端设备上下文 1624
1626
TAI 和 GIOTFI
1628
TID, GUTI, 经加密客户端设备上下文、和TAU响应
1630
GUTI,经加密客户端设备上下文、和TAU响应

图16

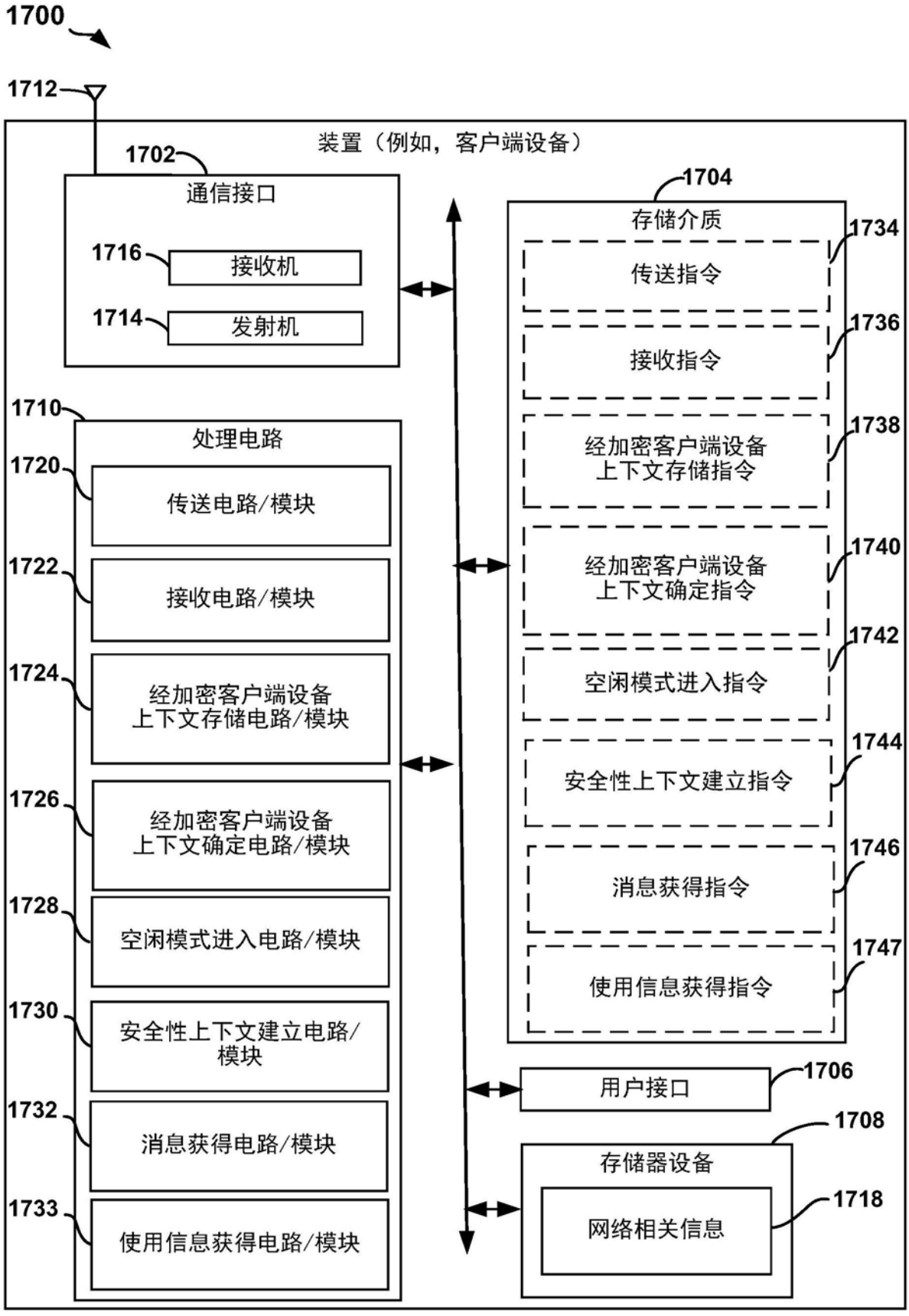

1700
1712
装置（例如，客户端设备）
1702
通信接口
1716
接收机
1714
发射机
1710
处理电路
1720
传送电路/模块
1722
接收电路/模块
1724
经加密客户端设备
上下文存储电路/模块
1726
经加密客户端设备
上下文确定电路/模块
1728
空闲模式进入电路/模块
1730
安全性上下文建立电路/
模块
1732
消息获得电路/模块
1733
使用信息获得电路/模块
1704
存储介质
1734
传送指令
1736
接收指令
1738
经加密客户端设备
上下文存储指令
1740
经加密客户端设备
上下文确定指令
1742
空闲模式进入指令
1744
安全性上下文建立指令
1746
消息获得指令
1747
使用信息获得指令
1706
用户接口
1708
存储器设备
1718
网络相关信息

图17

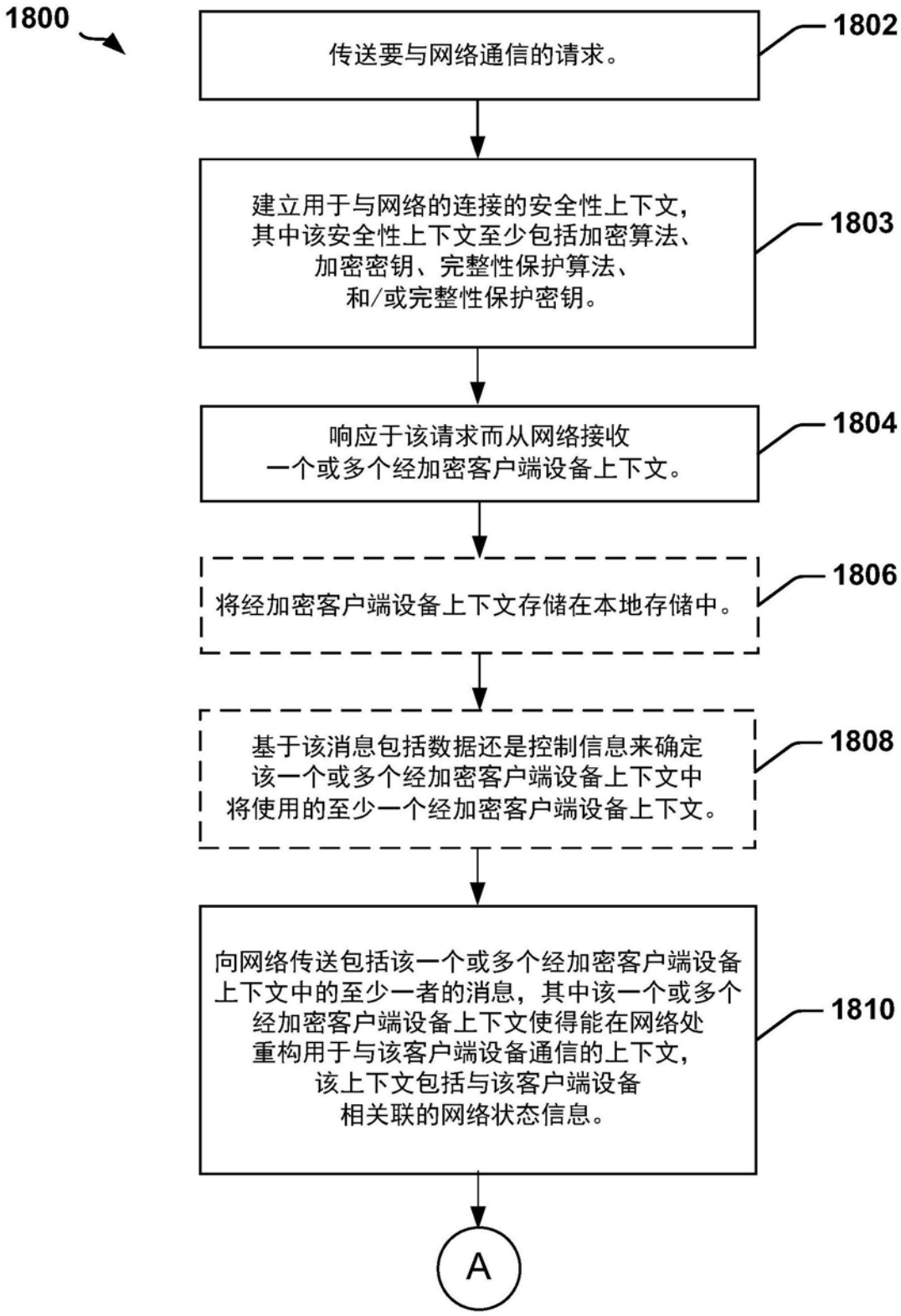

1800
传送要与网络通信的请求。
1802
建立用于与网络的连接的安全性上下文，
其中该安全性上下文至少包括加密算法、
加密密钥、完整性保护算法、
和/或完整性保护密钥。
1803
响应于该请求而从网络接收
一个或多个经加密客户端设备上下文。
1804
将经加密客户端设备上下文存储在本地存储中。
1806
基于该消息包括数据还是控制信息来确定
该一个或多个经加密客户端设备上下文中
将使用的至少一个经加密客户端设备上下文。
1808
向网络传送包括该一个或多个经加密客户端设备
上下文中的至少一者的消息，其中该一个或多个
经加密客户端设备上下文使得能在网络处
重构用于与该客户端设备通信的上下文，
该上下文包括与该客户端设备
相关联的网络状态信息。
1810
A

图18A

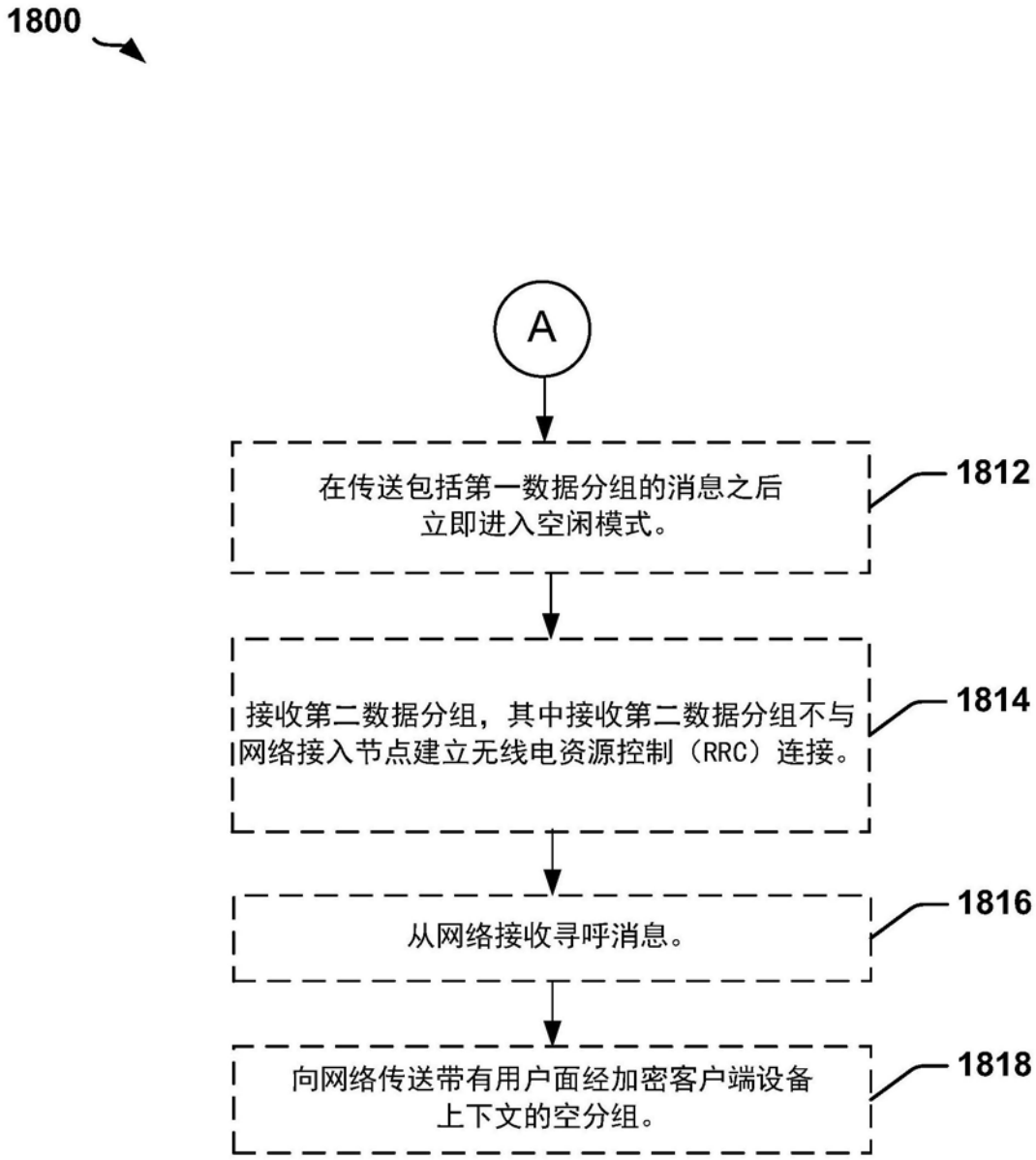

1800
A
在传送包括第一数据分组的消息之后
立即进入空闲模式。
1812
接收第二数据分组，其中接收第二数据分组不与
网络接入节点建立无线电资源控制（RRC）连接。
1814
从网络接收寻呼消息。
1816
向网络传送带有用户面经加密客户端设备
上下文的空分组。
1818

图18B

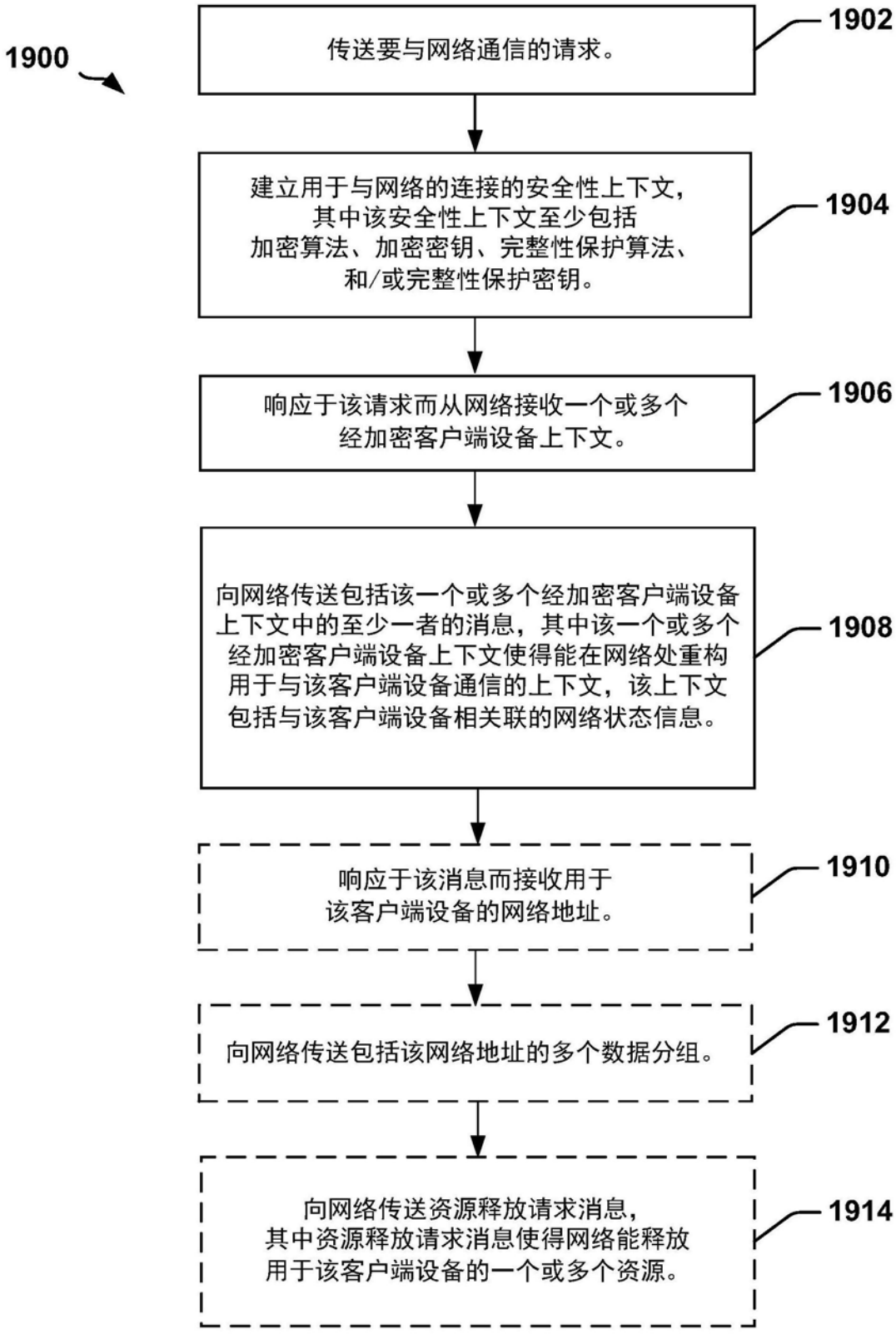

1900
传送要与网络通信的请求。
1902
建立用于与网络的连接的安全性上下文，其中该安全性上下文至少包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥。
1904
响应于该请求而从网络接收一个或多个经加密客户端设备上下文。
1906
向网络传送包括该一个或多个经加密客户端设备上下文中的至少一者的消息，其中该一个或多个经加密客户端设备上下文使得能在网络处重构用于与该客户端设备通信的上下文，该上下文包括与该客户端设备相关联的网络状态信息。
1908
响应于该消息而接收用于该客户端设备的网络地址。
1910
向网络传送包括该网络地址的多个数据分组。
1912
向网络传送资源释放请求消息，其中资源释放请求消息使得网络能释放用于该客户端设备的一个或多个资源。
1914

图19

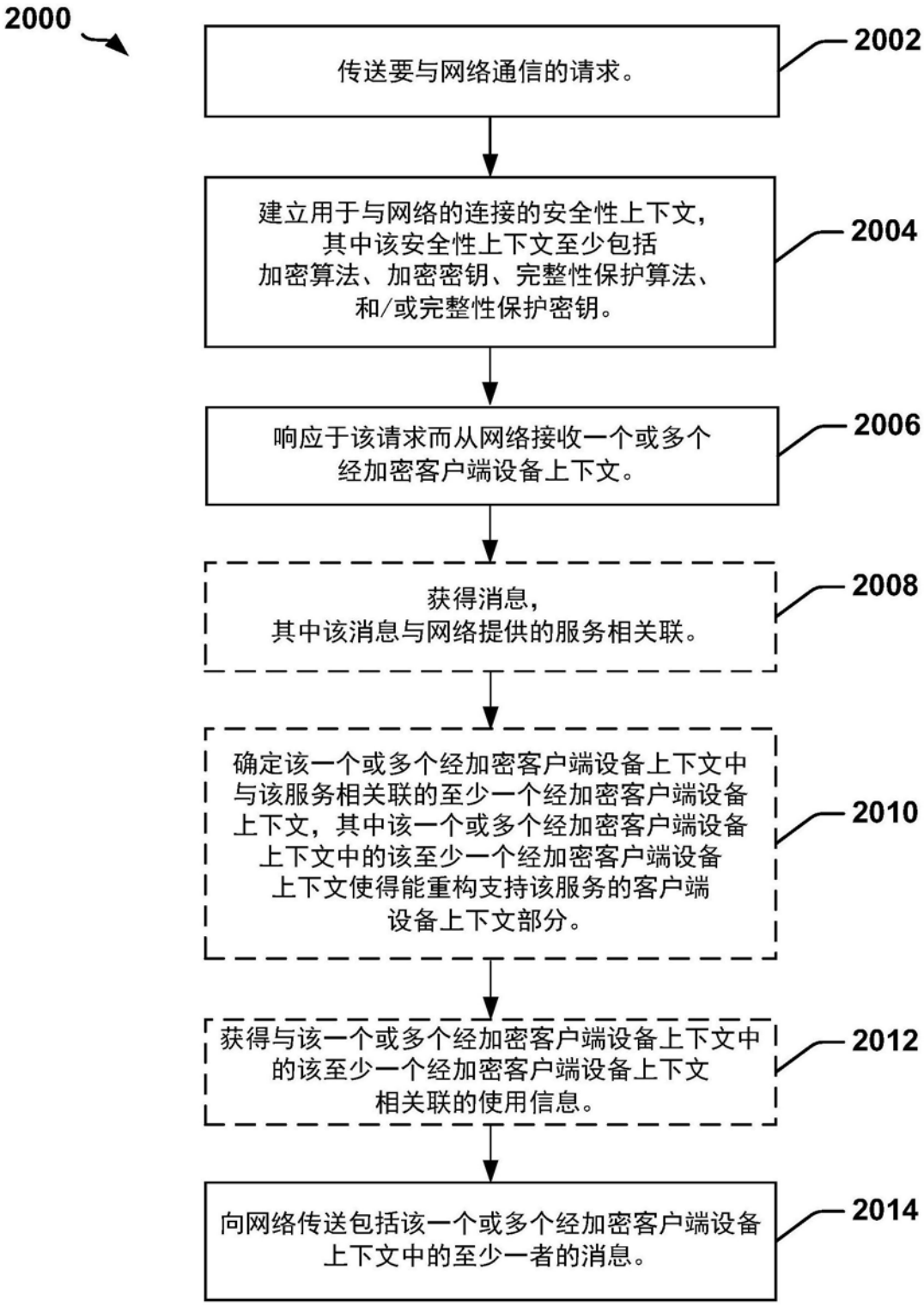

2000
传送要与网络通信的请求。
2002
建立用于与网络的连接的安全性上下文，
其中该安全性上下文至少包括
加密算法、加密密钥、完整性保护算法、
和/或完整性保护密钥。
2004
响应于该请求而从网络接收一个或多个
经加密客户端设备上下文。
2006
获得消息，
其中该消息与网络提供的服务相关联。
2008
确定该一个或多个经加密客户端设备上下文中
与该服务相关联的至少一个经加密客户端设备
上下文，其中该一个或多个经加密客户端设备
上下文中的该至少一个经加密客户端设备
上下文使得能重构支持该服务的客户端
设备上下文部分。
2010
获得与该一个或多个经加密客户端设备上下文中
的该至少一个经加密客户端设备上下文
相关联的使用信息。
2012
向网络传送包括该一个或多个经加密客户端设备
上下文中的至少一者的消息。
2014

图20

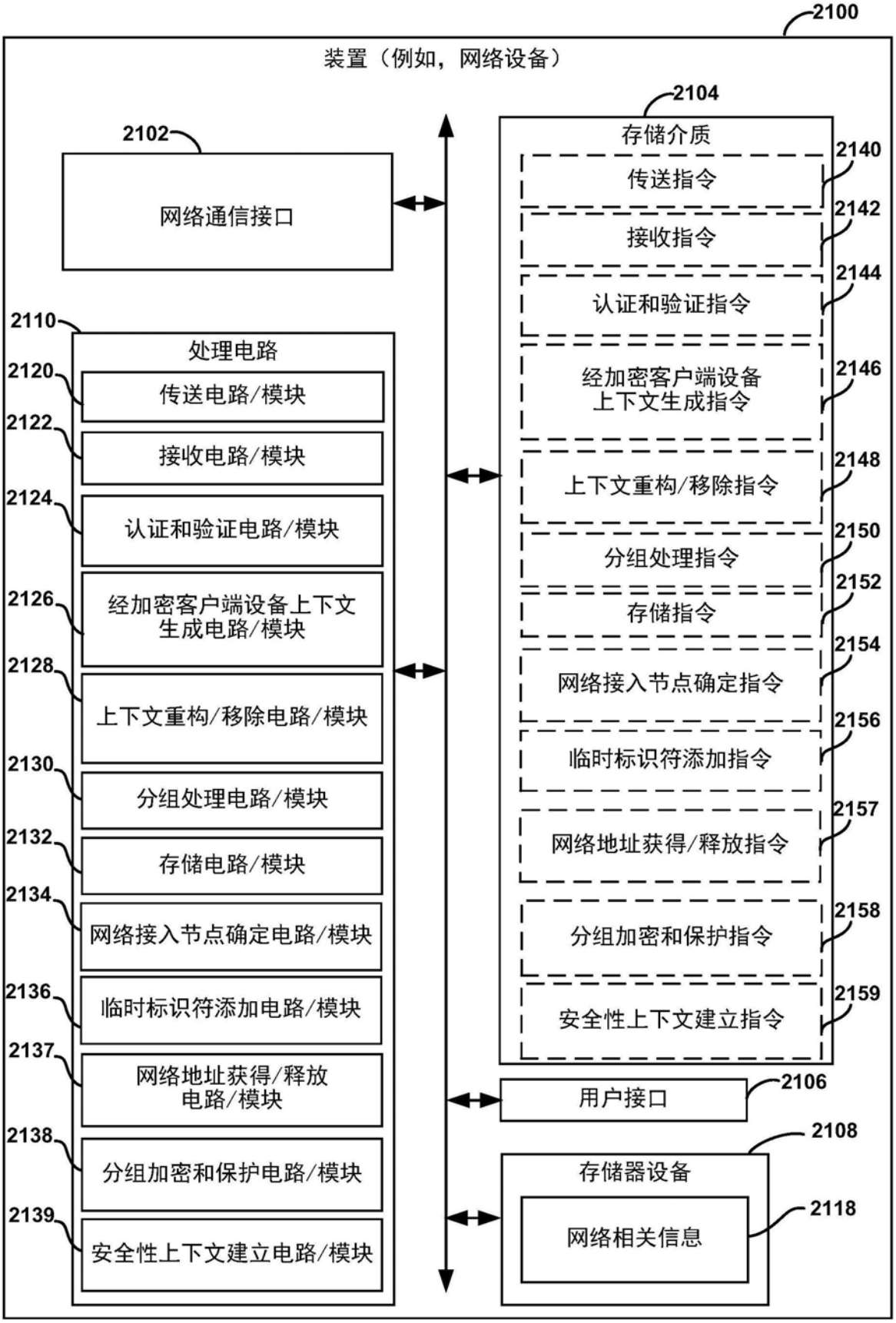

2100
装置（例如，网络设备）
2102
网络通信接口
2104
存储介质
2140
传送指令
2142
接收指令
2144
认证和验证指令
2146
经加密客户端设备上下文生成指令
2148
上下文重构/移除指令
2150
分组处理指令
2152
存储指令
2154
网络接入节点确定指令
2156
临时标识符添加指令
2157
网络地址获得/释放指令
2158
分组加密和保护指令
2159
安全性上下文建立指令
2110
处理电路
2120
传送电路/模块
2122
接收电路/模块
2124
认证和验证电路/模块
2126
经加密客户端设备上下文生成电路/模块
2128
上下文重构/移除电路/模块
2130
分组处理电路/模块
2132
存储电路/模块
2134
网络接入节点确定电路/模块
2136
临时标识符添加电路/模块
2137
网络地址获得/释放电路/模块
2138
分组加密和保护电路/模块
2139
安全性上下文建立电路/模块
2106
用户接口
2108
存储器设备
2118
网络相关信息

图21

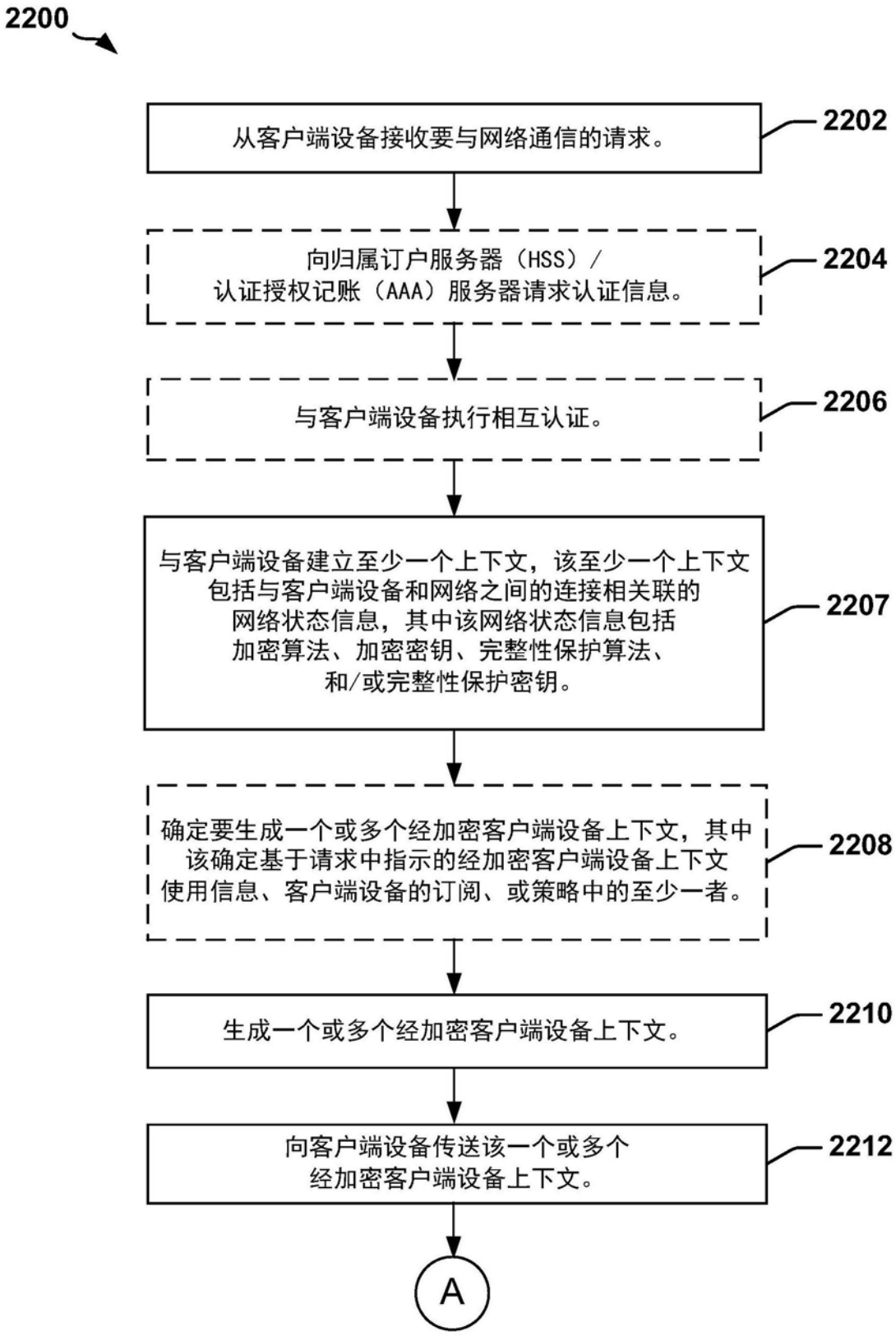

2200
从客户端设备接收要与网络通信的请求。
2202
向归属订户服务器（HSS）/
认证授权记账（AAA）服务器请求认证信息。
2204
与客户端设备执行相互认证。
2206
与客户端设备建立至少一个上下文，该至少一个上下文
包括与客户端设备和网络之间的连接相关联的
网络状态信息，其中该网络状态信息包括
加密算法、加密密钥、完整性保护算法、
和/或完整性保护密钥。
2207
确定要生成一个或多个经加密客户端设备上下文，其中
该确定基于请求中指示的经加密客户端设备上下文
使用信息、客户端设备的订阅、或策略中的至少一者。
2208
生成一个或多个经加密客户端设备上下文。
2210
向客户端设备传送该一个或多个
经加密客户端设备上下文。
2212
A

图22A

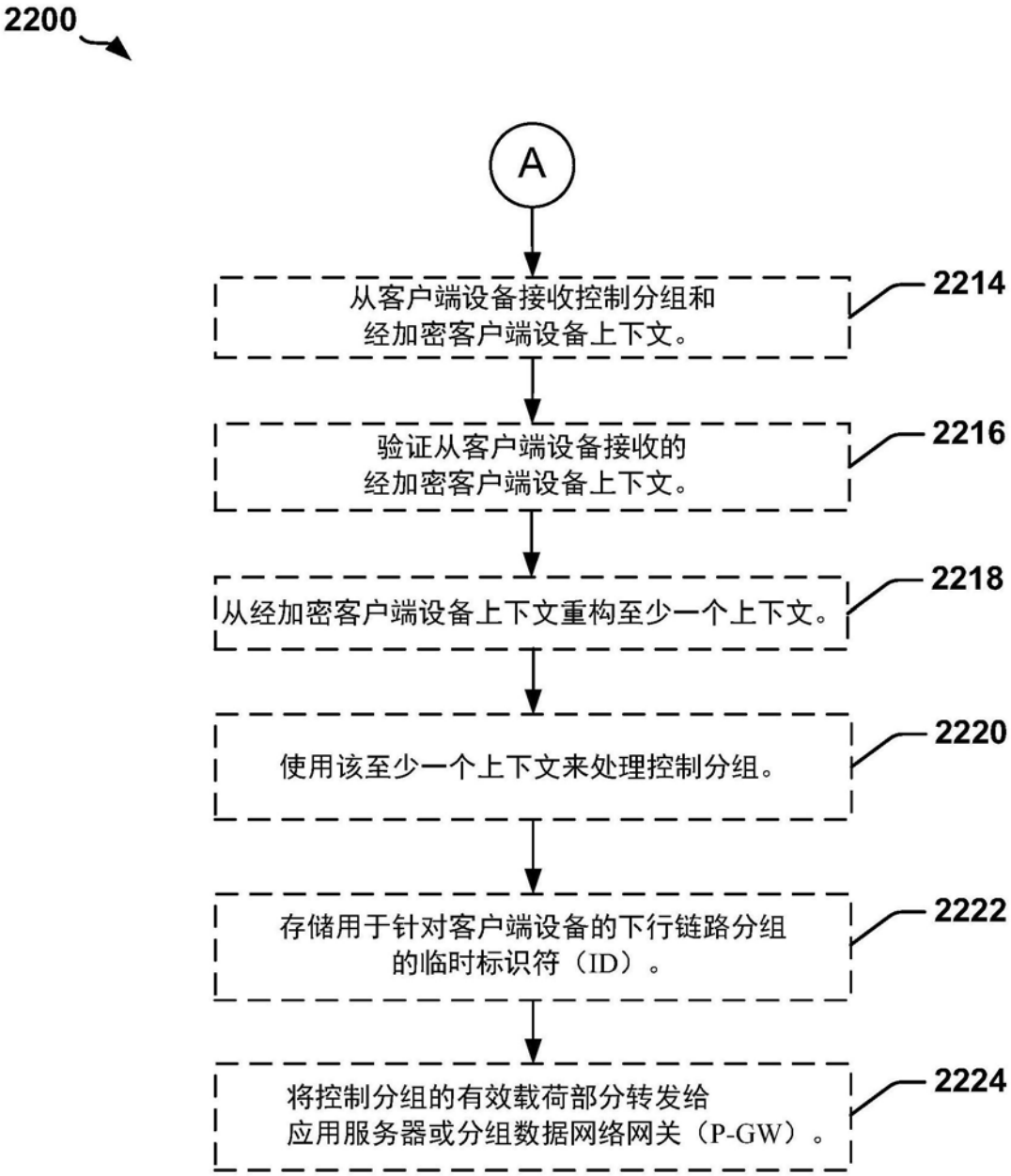

2200
A
从客户端设备接收控制分组和
经加密客户端设备上下文。
2214
验证从客户端设备接收的
经加密客户端设备上下文。
2216
从经加密客户端设备上下文重构至少一个上下文。
2218
使用该至少一个上下文来处理控制分组。
2220
存储用于针对客户端设备的下行链路分组
的临时标识符（ID）。
2222
将控制分组的有效载荷部分转发给
应用服务器或分组数据网络网关（P-GW）。
2224

图22B

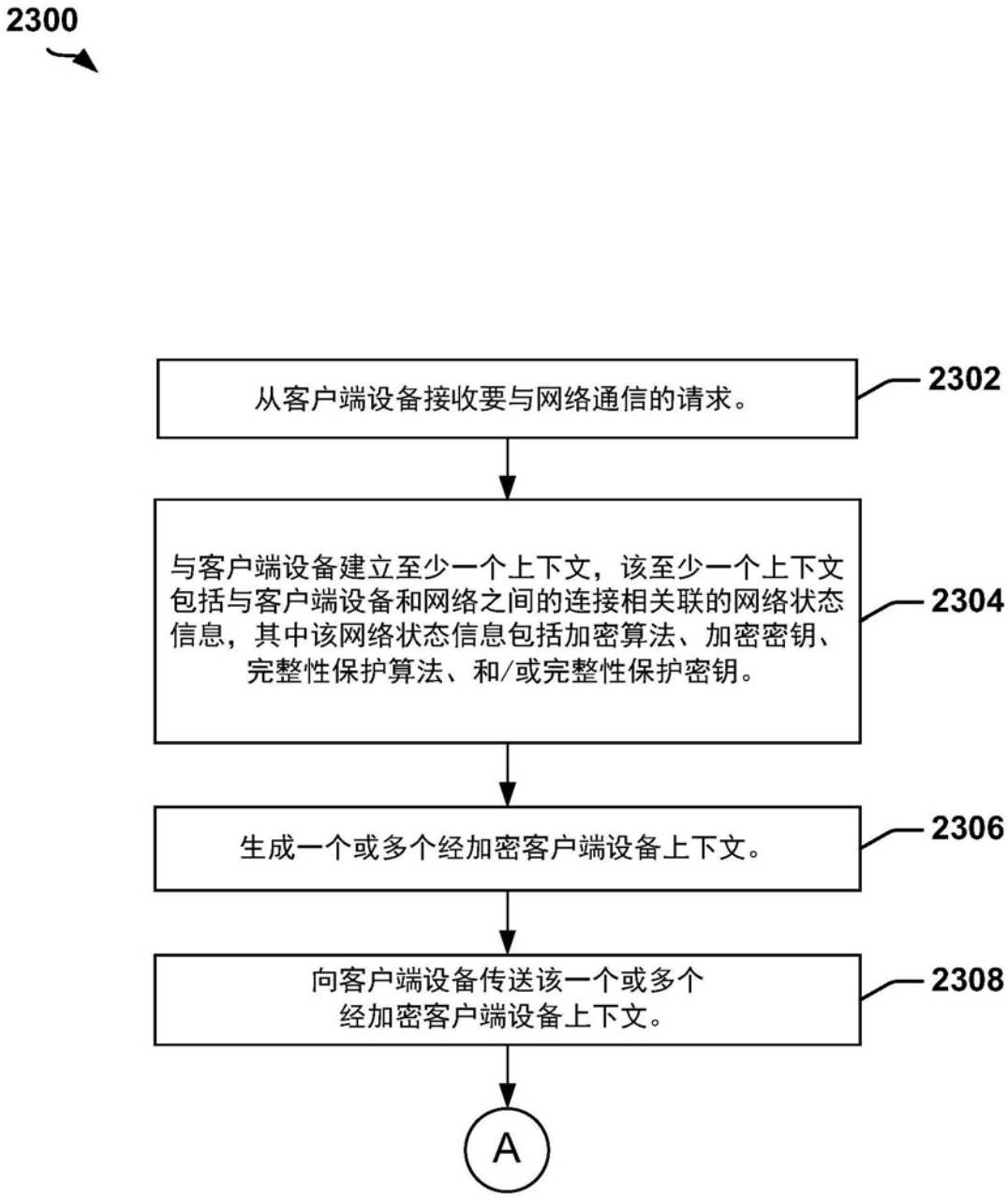

2300
从客户端设备接收要与网络通信的请求。
2302
与客户端设备建立至少一个上下文，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中该网络状态信息包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥。
2304
生成一个或多个经加密客户端设备上下文。
2306
向客户端设备传送该一个或多个经加密客户端设备上下文。
2308
A

图23A

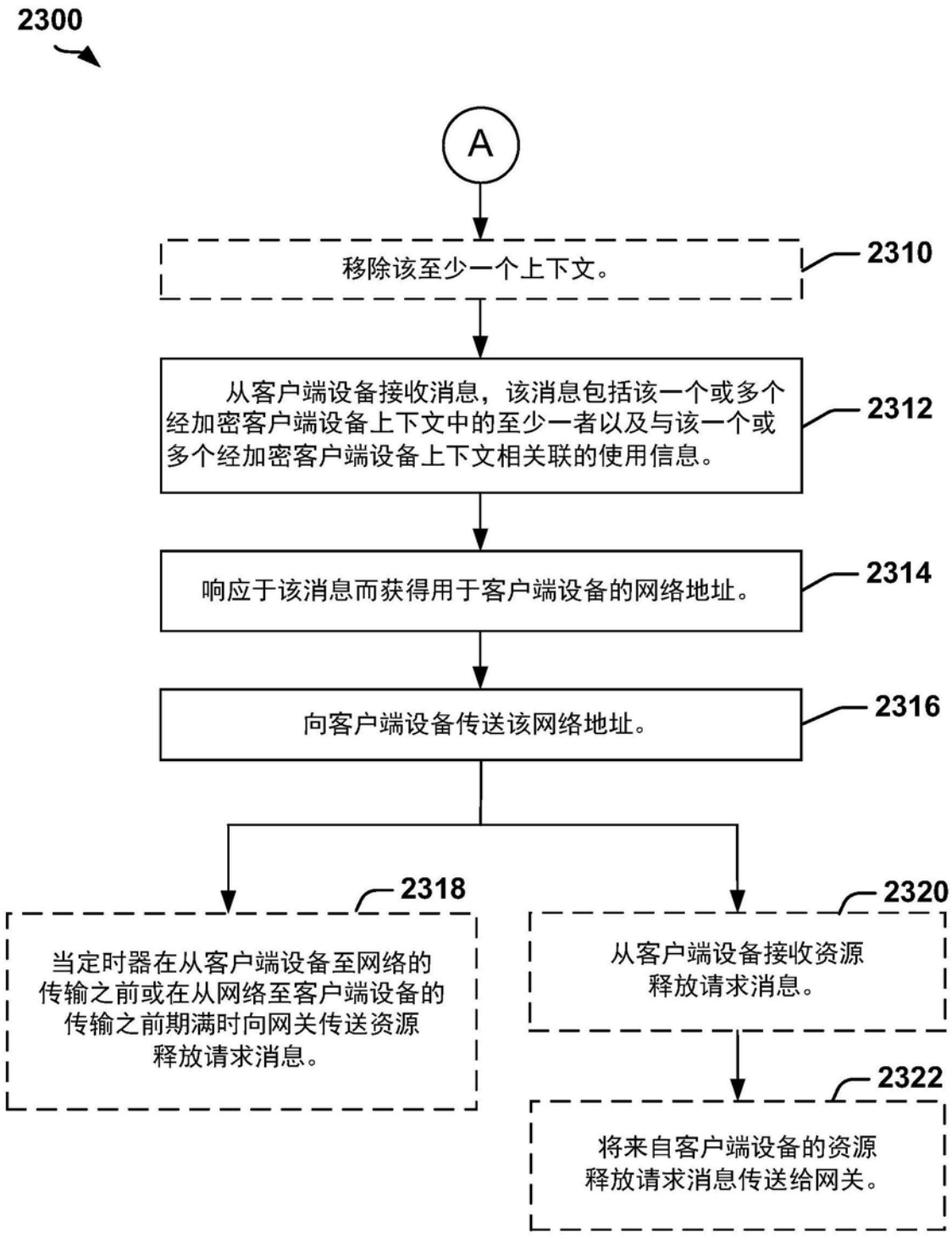

2300
A
移除该至少一个上下文。
2310
从客户端设备接收消息，该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息。
2312
响应于该消息而获得用于客户端设备的网络地址。
2314
向客户端设备传送该网络地址。
2316
2318
当定时器在从客户端设备至网络的传输之前或在从网络至客户端设备的传输之前期满时向网关传送资源释放请求消息。
2320
从客户端设备接收资源释放请求消息。
2322
将来自客户端设备的资源释放请求消息传送给网关。

图23B

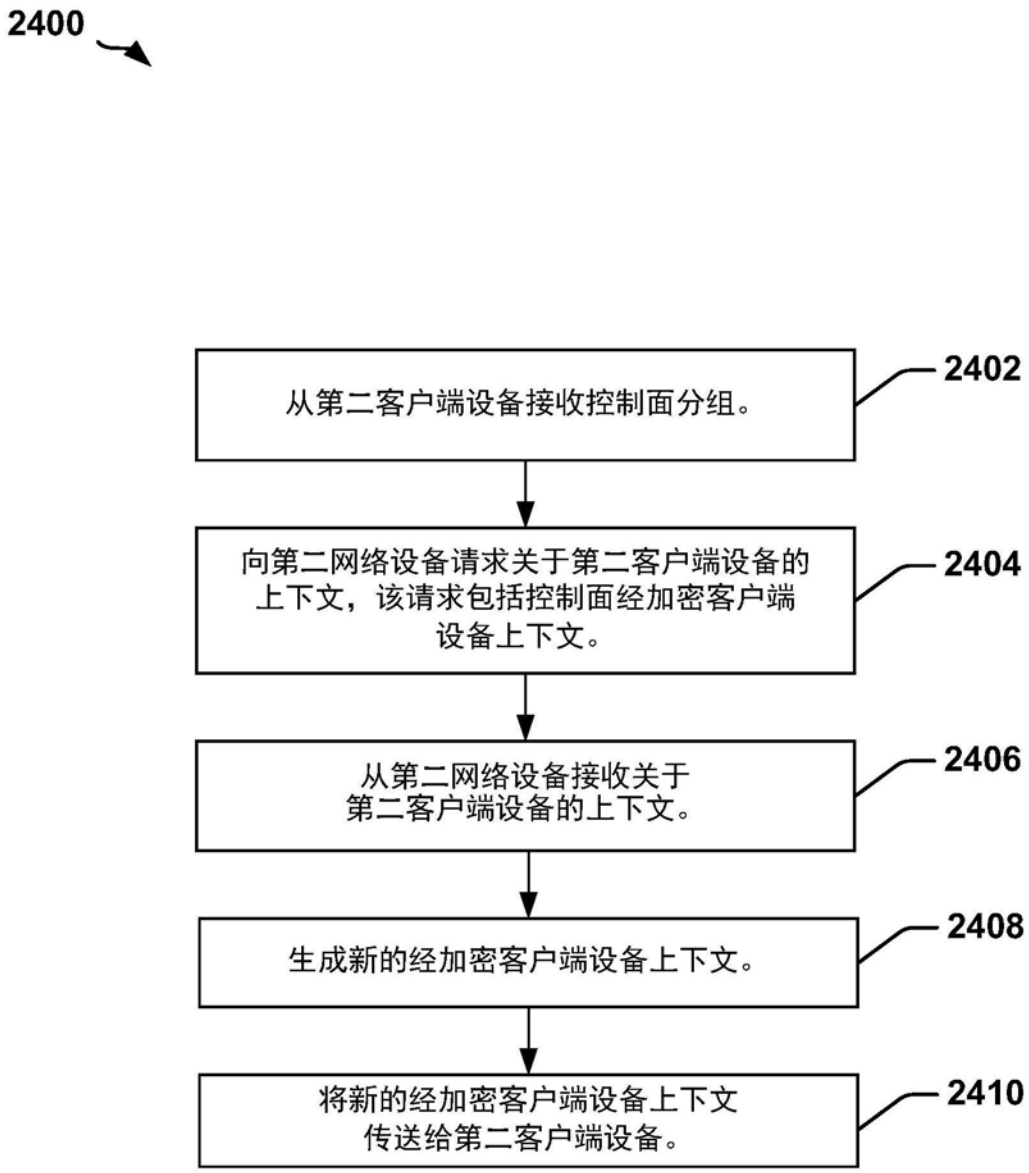

2400
从第二客户端设备接收控制面分组。
2402
向第二网络设备请求关于第二客户端设备的上下文，该请求包括控制面经加密客户端设备上下文。
2404
从第二网络设备接收关于第二客户端设备的上下文。
2406
生成新的经加密客户端设备上下文。
2408
将新的经加密客户端设备上下文传送给第二客户端设备。
2410

图24

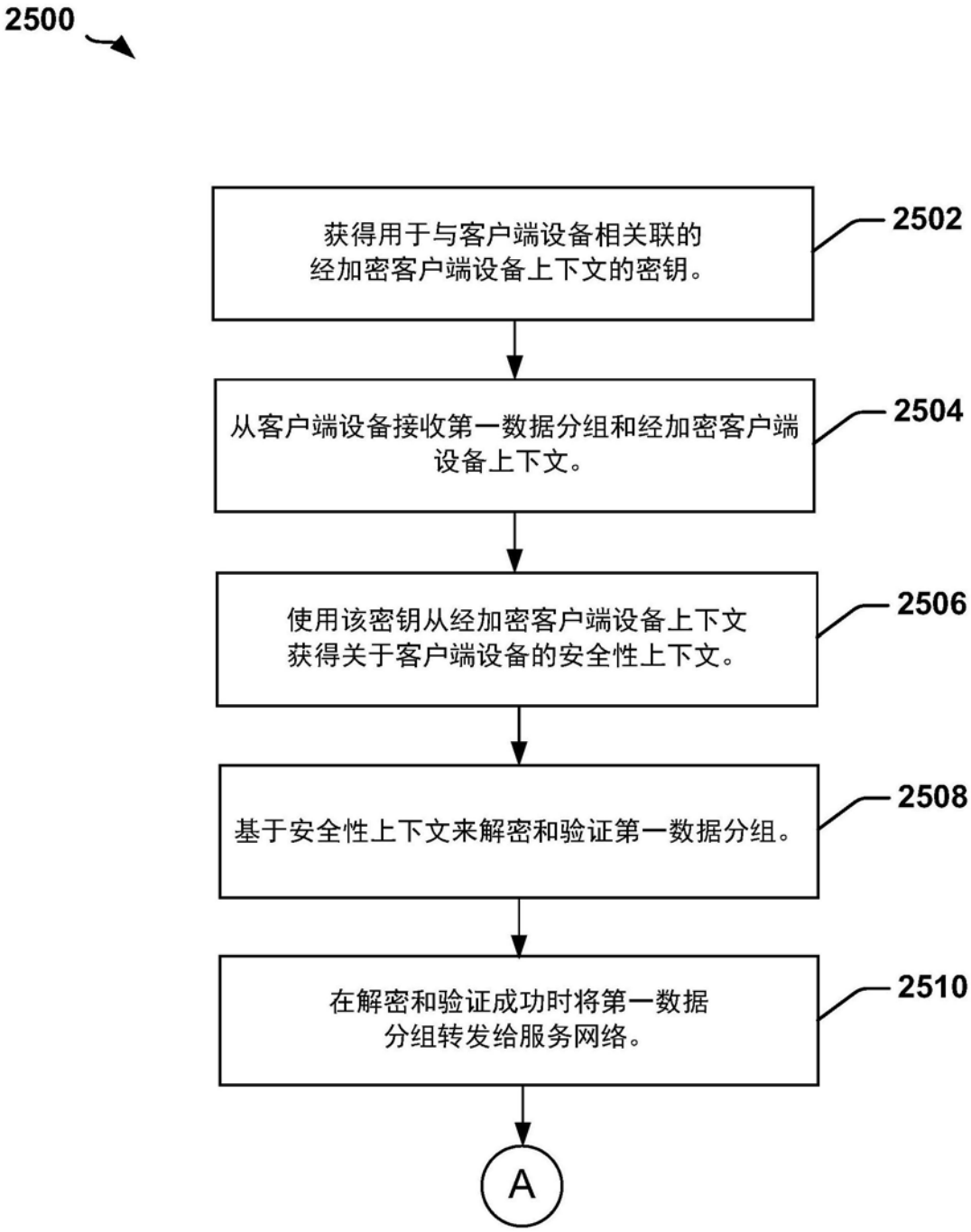

2500
获得用于与客户端设备相关联的经加密客户端设备上下文的密钥。
2502
从客户端设备接收第一数据分组和经加密客户端设备上下文。
2504
使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文。
2506
基于安全性上下文来解密和验证第一数据分组。
2508
在解密和验证成功时将第一数据分组转发给服务网络。
2510
A

图25A

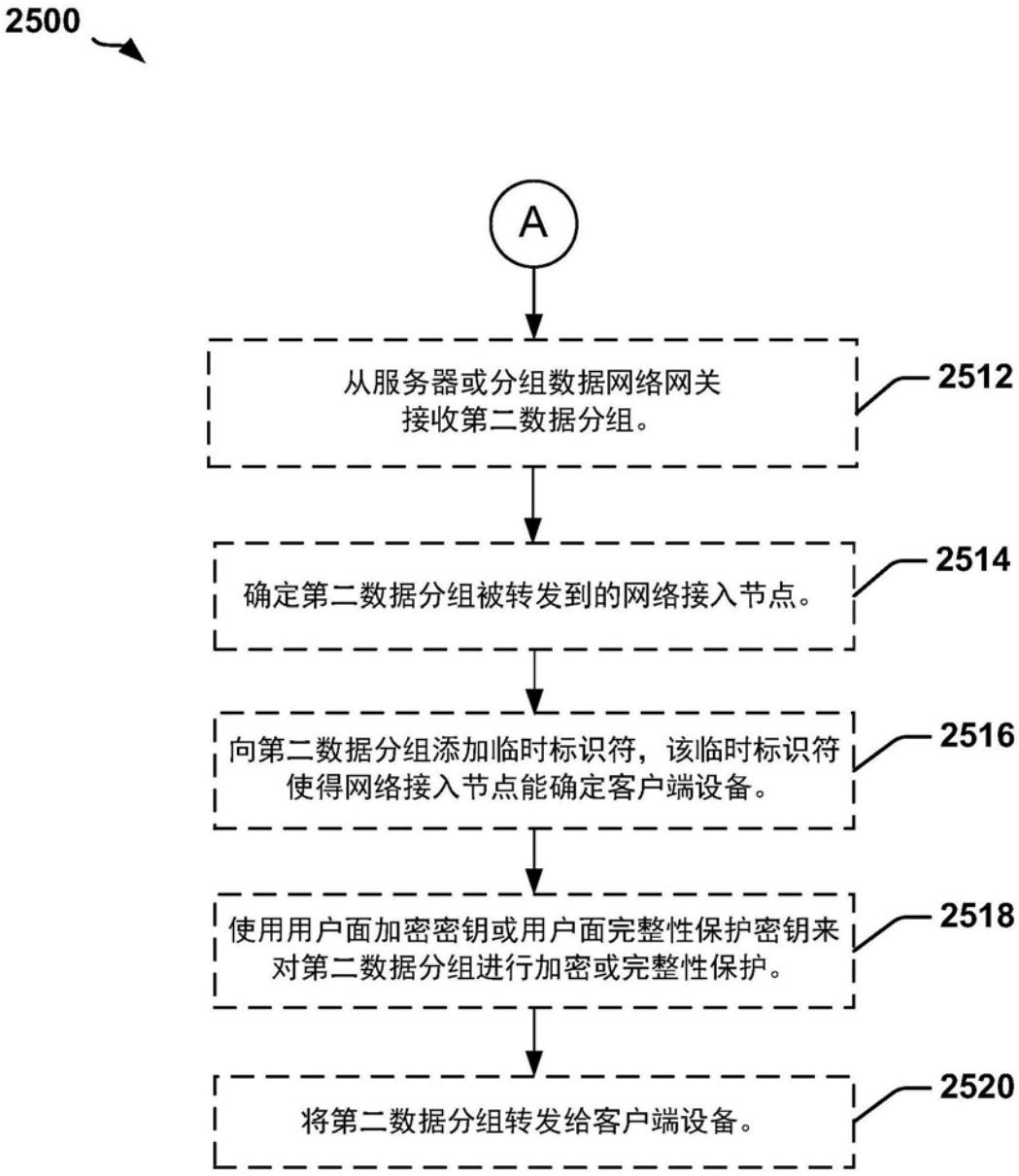

2500
A
从服务器或分组数据网络网关
接收第二数据分组。
2512
确定第二数据分组被转发到的网络接入节点。
2514
向第二数据分组添加临时标识符，该临时标识符
使得网络接入节点能确定客户端设备。
2516
使用用户面加密密钥或用户面完整性保护密钥来
对第二数据分组进行加密或完整性保护。
2518
将第二数据分组转发给客户端设备。
2520

图25B

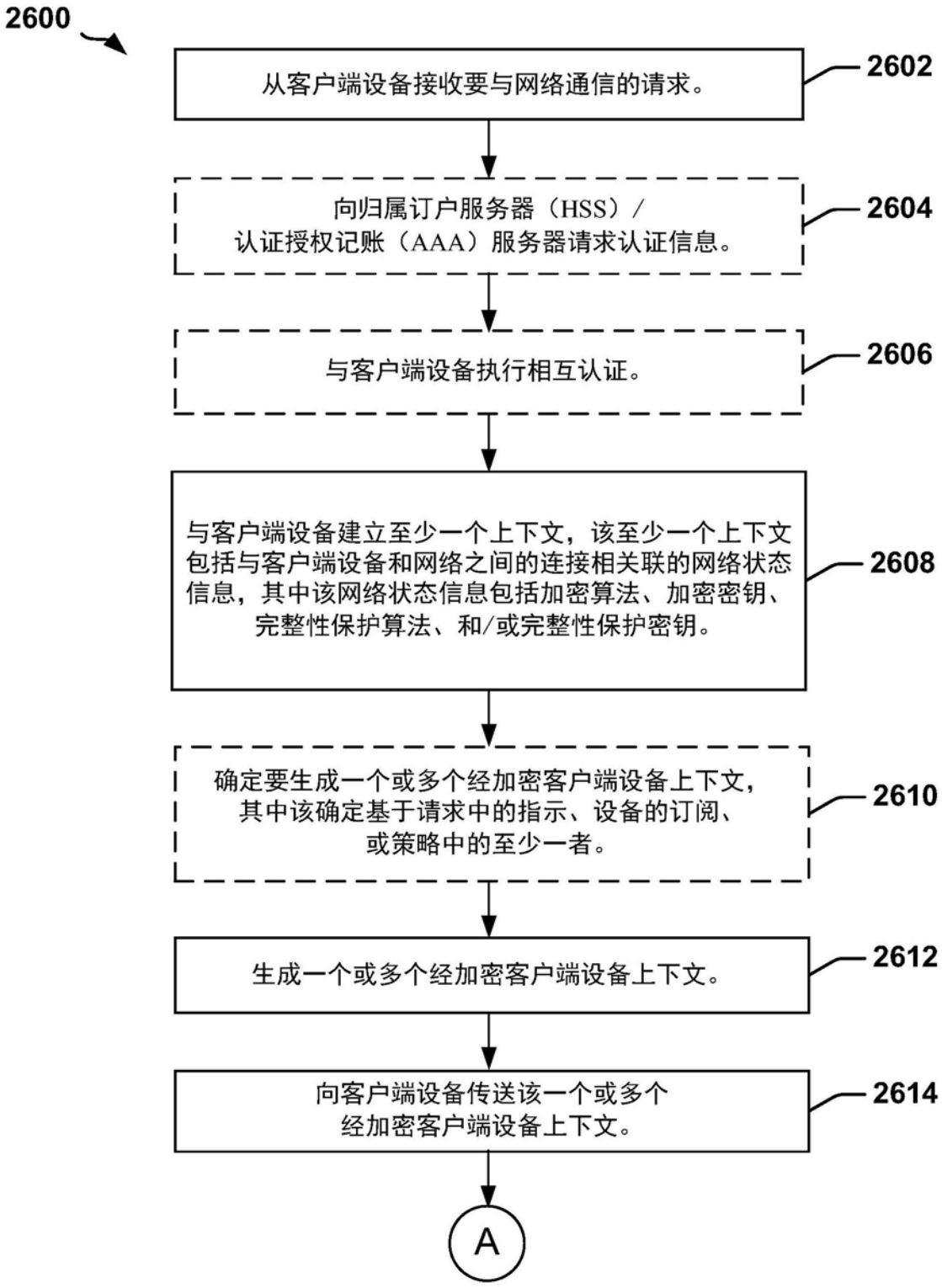

2600
从客户端设备接收要与网络通信的请求。
2602
向归属订户服务器（HSS）/
认证授权记账（AAA）服务器请求认证信息。
2604
与客户端设备执行相互认证。
2606
与客户端设备建立至少一个上下文，该至少一个上下文包括与客户端设备和网络之间的连接相关联的网络状态信息，其中该网络状态信息包括加密算法、加密密钥、完整性保护算法、和/或完整性保护密钥。
2608
确定要生成一个或多个经加密客户端设备上下文，
其中该确定基于请求中的指示、设备的订阅、
或策略中的至少一者。
2610
生成一个或多个经加密客户端设备上下文。
2612
向客户端设备传送该一个或多个
经加密客户端设备上下文。
2614
A

图26A

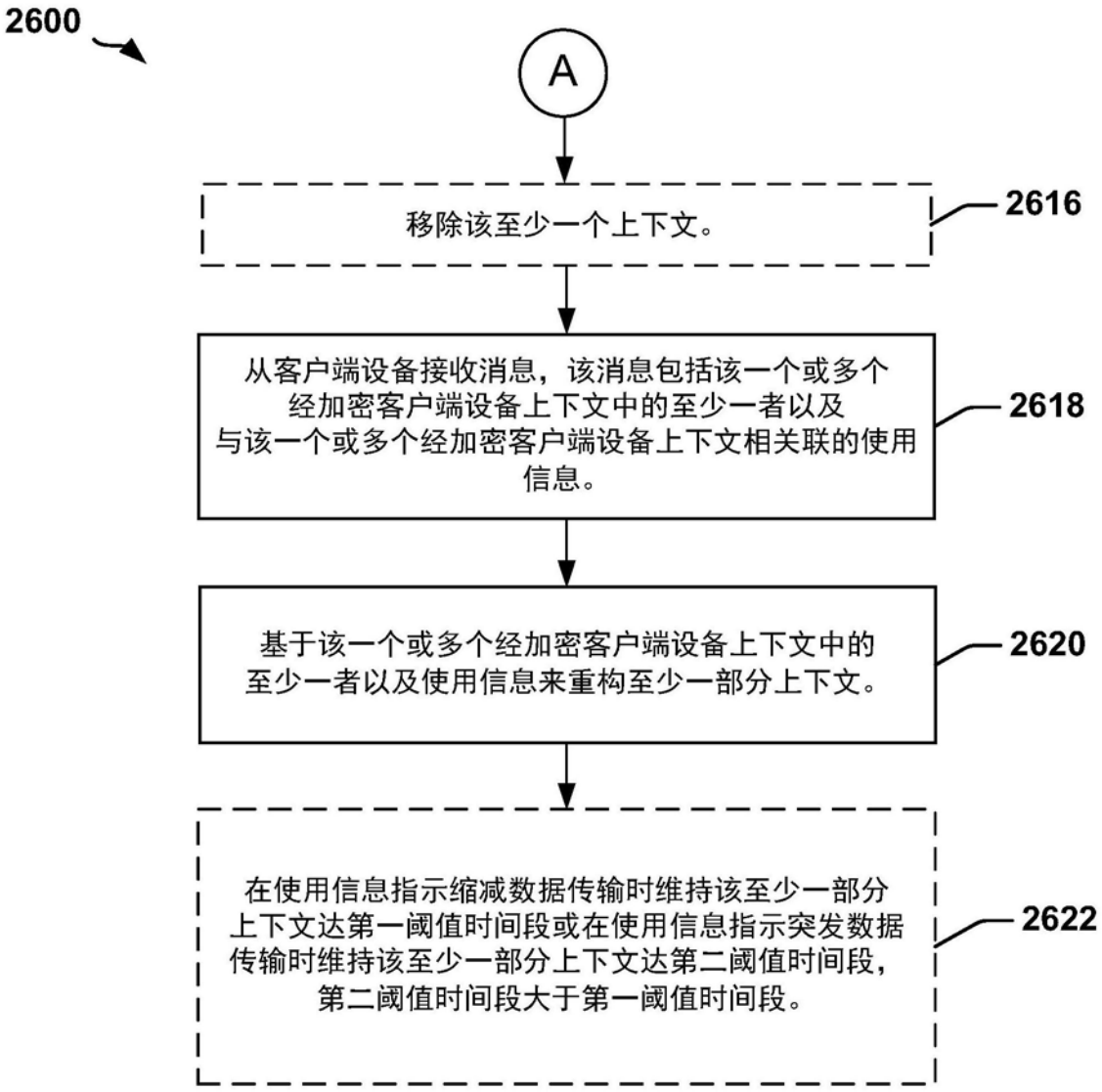

2600
A
移除该至少一个上下文。
2616
从客户端设备接收消息，该消息包括该一个或多个经加密客户端设备上下文中的至少一者以及与该一个或多个经加密客户端设备上下文相关联的使用信息。
2618
基于该一个或多个经加密客户端设备上下文中的至少一者以及使用信息来重构至少一部分上下文。
2620
在使用信息指示缩减数据传输时维持该至少一部分上下文达第一阈值时间段或在使用信息指示突发数据传输时维持该至少一部分上下文达第二阈值时间段，第二阈值时间段大于第一阈值时间段。
2622

图26B

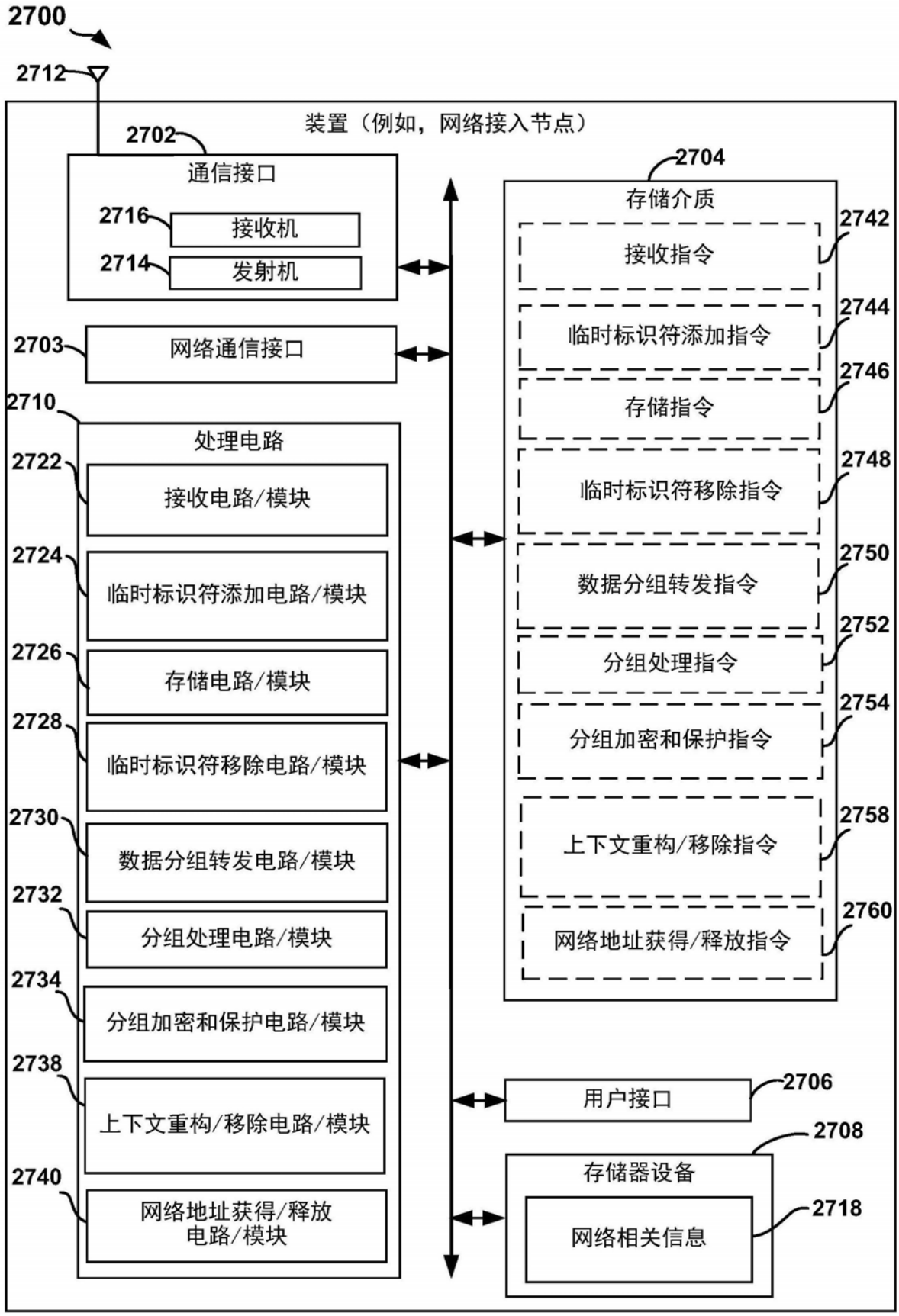

2700
2712
装置（例如，网络接入节点）
2702
通信接口
2716
接收机
2714
发射机
2703
网络通信接口
2710
处理电路
2722
接收电路/模块
2724
临时标识符添加电路/模块
2726
存储电路/模块
2728
临时标识符移除电路/模块
2730
数据分组转发电路/模块
2732
分组处理电路/模块
2734
分组加密和保护电路/模块
2738
上下文重构/移除电路/模块
2740
网络地址获得/释放电路/模块
2704
存储介质
2742
接收指令
2744
临时标识符添加指令
2746
存储指令
2748
临时标识符移除指令
2750
数据分组转发指令
2752
分组处理指令
2754
分组加密和保护指令
2758
上下文重构/移除指令
2760
网络地址获得/释放指令
2706
用户接口
2708
存储器设备
2718
网络相关信息

图27

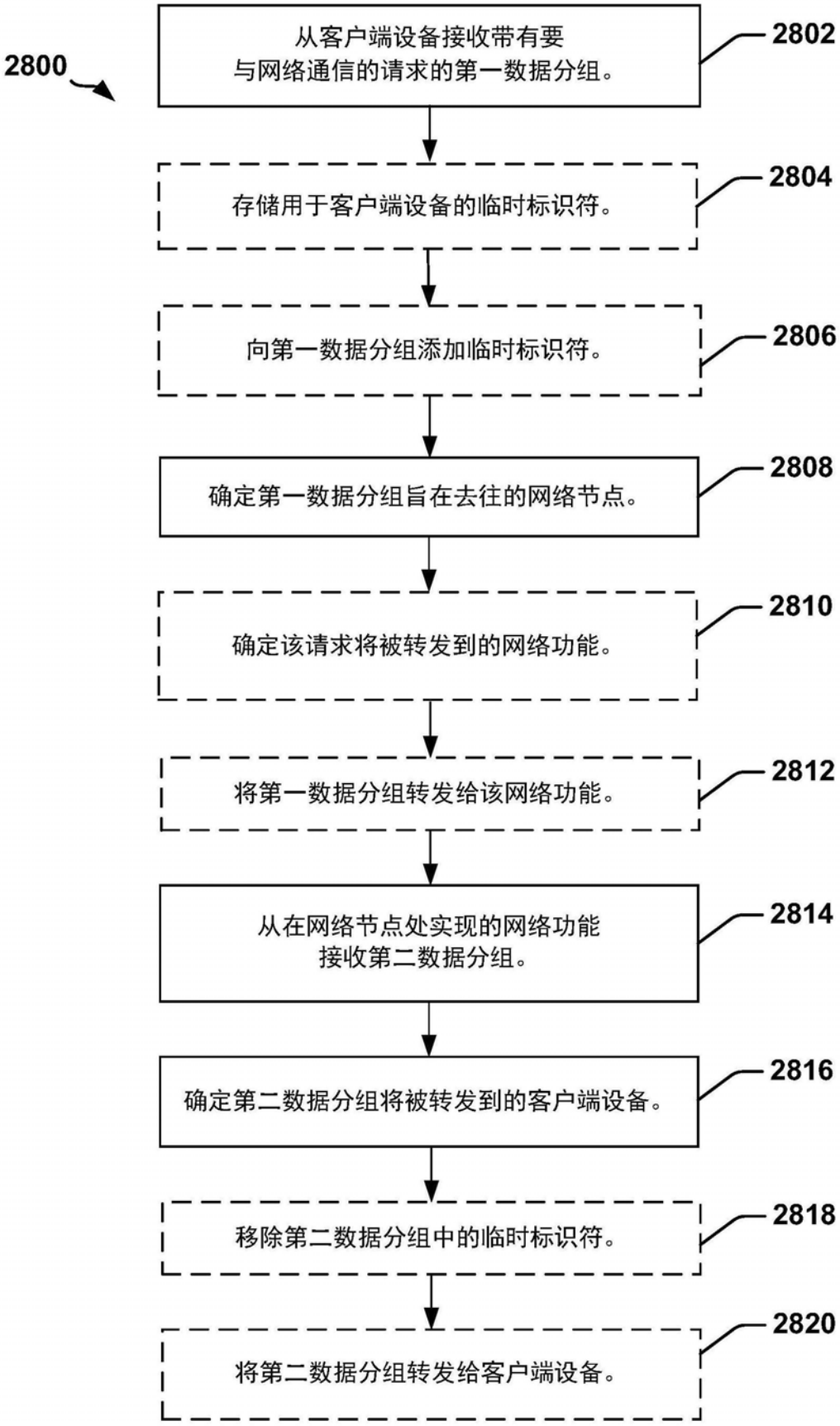

2800
从客户端设备接收带有要与网络通信的请求的第一数据分组。
2802
存储用于客户端设备的临时标识符。
2804
向第一数据分组添加临时标识符。
2806
确定第一数据分组旨在去往的网络节点。
2808
确定该请求将被转发到的网络功能。
2810
将第一数据分组转发给该网络功能。
2812
从在网络节点处实现的网络功能接收第二数据分组。
2814
确定第二数据分组将被转发到的客户端设备。
2816
移除第二数据分组中的临时标识符。
2818
将第二数据分组转发给客户端设备。
2820

图28

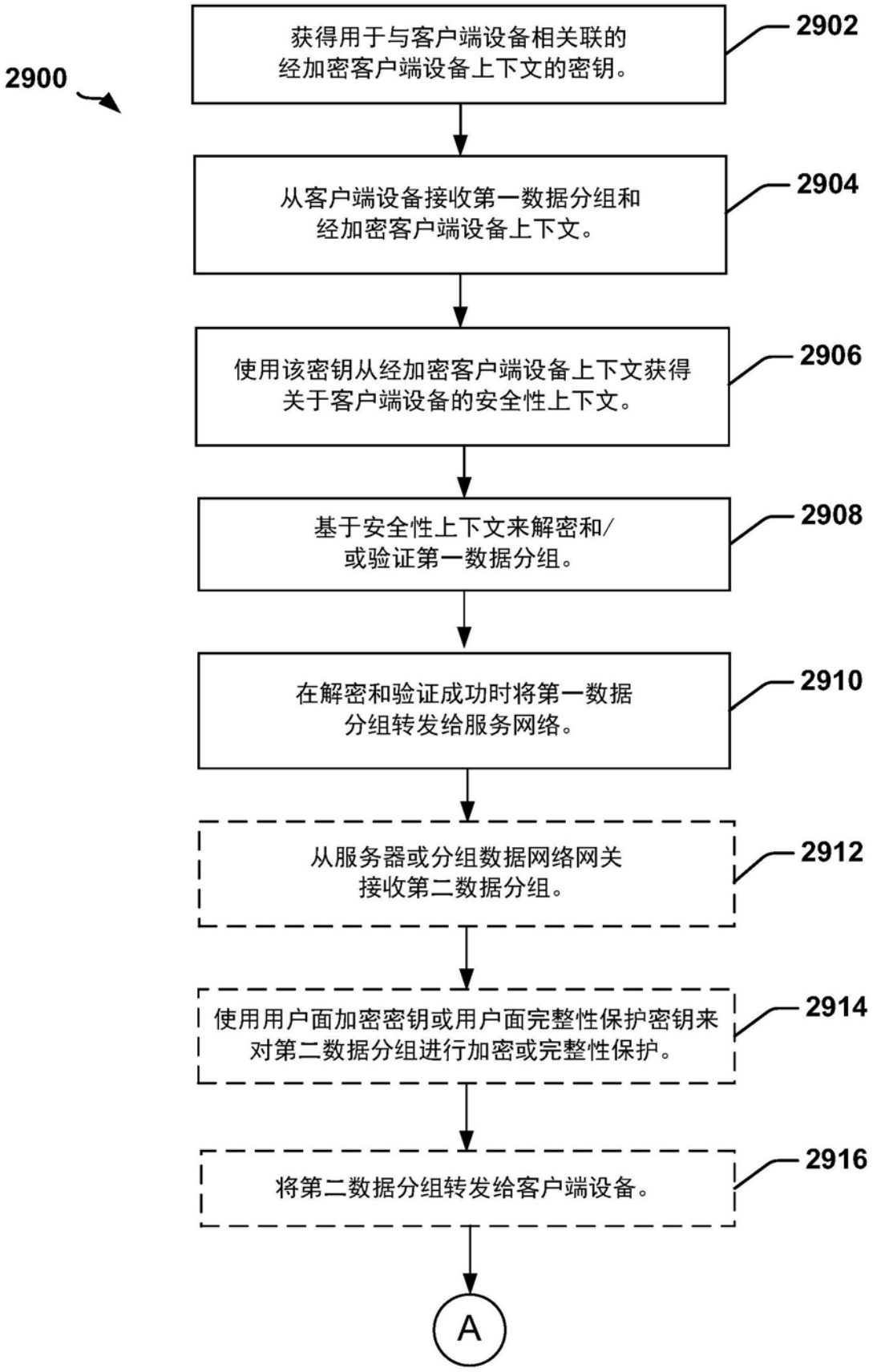

2900
获得用于与客户端设备相关联的经加密客户端设备上下文的密钥。
2902
从客户端设备接收第一数据分组和经加密客户端设备上下文。
2904
使用该密钥从经加密客户端设备上下文获得关于客户端设备的安全性上下文。
2906
基于安全性上下文来解密和/或验证第一数据分组。
2908
在解密和验证成功时将第一数据分组转发给服务网络。
2910
从服务器或分组数据网络网关接收第二数据分组。
2912
使用用户面加密密钥或用户面完整性保护密钥来对第二数据分组进行加密或完整性保护。
2914
将第二数据分组转发给客户端设备。
2916
A

图29A

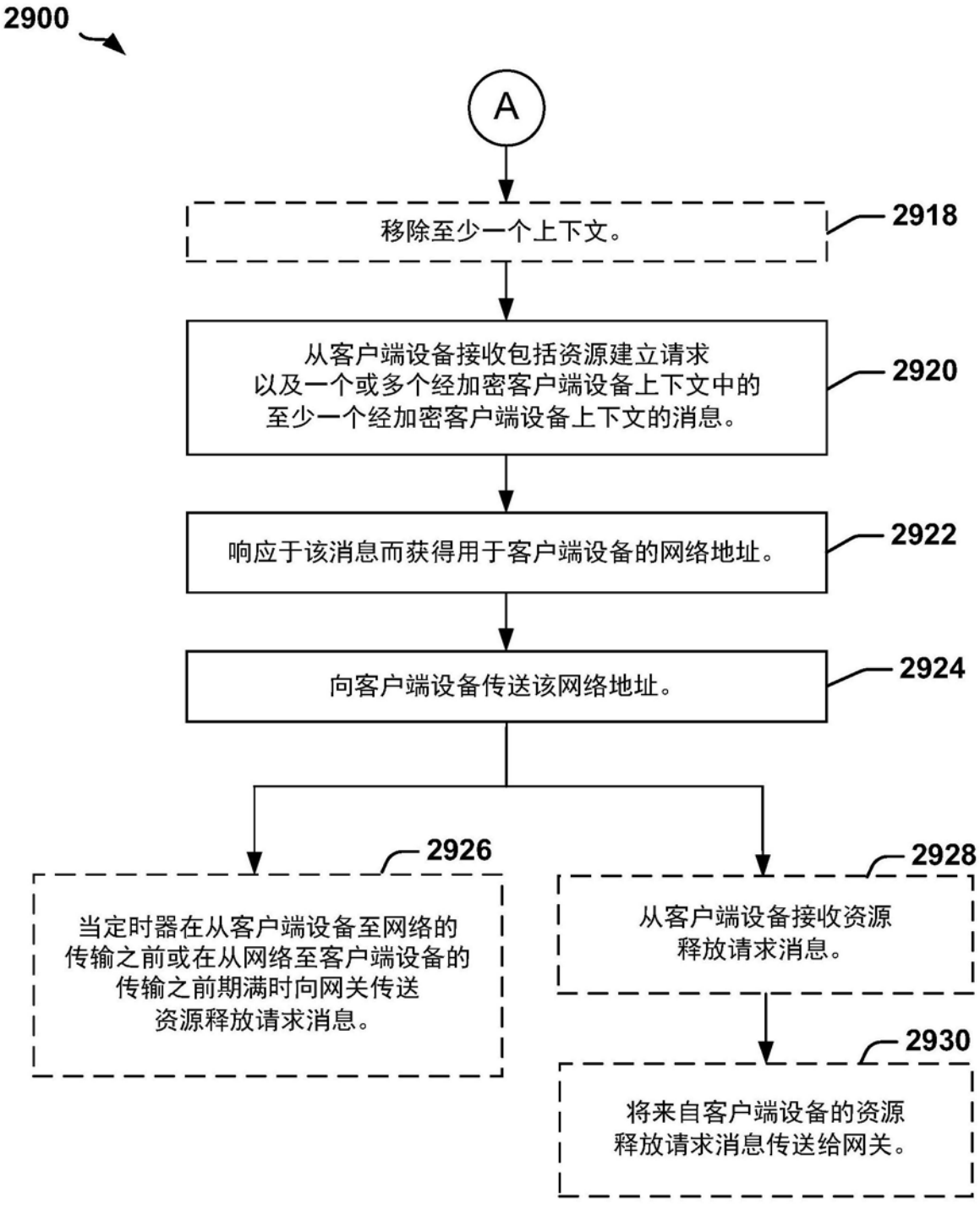

2900
A
移除至少一个上下文。
2918
从客户端设备接收包括资源建立请求
以及一个或多个经加密客户端设备上下文中的
至少一个经加密客户端设备上下文的消息。
2920
响应于该消息而获得用于客户端设备的网络地址。
2922
向客户端设备传送该网络地址。
2924
2926
当定时器在从客户端设备至网络的
传输之前或在从网络至客户端设备的
传输之前期满时向网关传送
资源释放请求消息。
2928
从客户端设备接收资源
释放请求消息。
2930
将来自客户端设备的资源
释放请求消息传送给网关。

图29B