(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111164999 B
(45)授权公告日 2023.04.18

(21)申请号 201880064005.7
(22)申请日 2018.09.29
(65)同一申请的已公布的文献号
申请公布号 CN 111164999 A
(43)申请公布日 2020.05.15
(30)优先权数据
62/567,086 2017.10.02 US
16/146,709 2018.09.28 US
(85)PCT国际申请进入国家阶段日
2020.03.31
(86)PCT国际申请的申请数据
PCT/US2018/053661 2018.09.29
(87)PCT国际申请的公布数据
WO2019/070542 EN 2019.04.11

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 S·B·李 A·E·艾斯科特
A·帕拉尼格朗德
(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 陈炜 亓云

(51)Int.Cl.
H04W 12/04(2021.01)
H04W 12/10(2021.01)
H04W 12/122(2021.01)
H04L 9/40(2022.01)
(56)对比文件
CN 103004243 A,2013.03.27
审查员 董智青

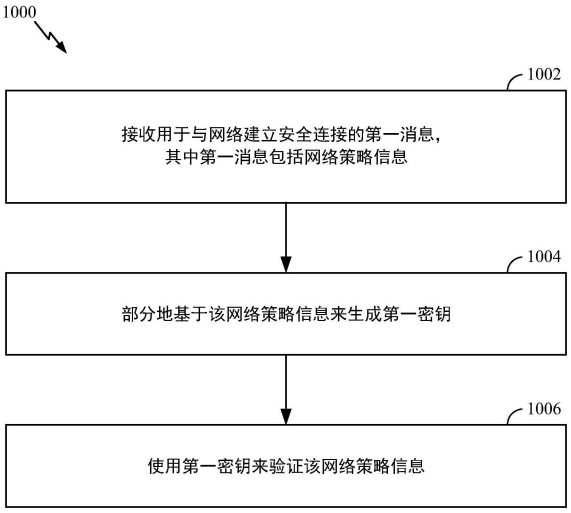
权利要求书5页 说明书18页 附图14页

(54)发明名称

在密钥生成中纳入网络策略

(57)摘要

本公开提供了可被应用于例如以安全方式提供网络策略信息的技术。在一些情形中,UE可以接收用于与网络建立安全连接的第一消息,其中第一消息包括网络策略信息;部分地基于网络策略信息来生成第一密钥;以及使用第一密钥来验证该网络策略信息。



1.一种用于由用户装备UE进行无线通信的方法,包括:

接收用于与网络建立安全连接的第一消息,其中所述第一消息包括网络策略信息;

通过密钥推导函数KDF,部分地基于作为所述KDF的输入的所述网络策略信息来生成第一密钥,其中所述网络策略信息包括所述网络的安全性特征;以及

使用所述第一密钥来验证所述网络策略信息。

2.如权利要求1所述的方法,其中,使用所述第一密钥来验证所述网络策略信息包括部分地基于所述第一密钥来确定所述第一消息是否有效。

3.如权利要求2所述的方法,其中:

所述第一消息由从第二密钥推导出的保护密钥进行完整性保护;以及

确定所述第一消息是否有效包括基于所述第一密钥对所述第一消息执行完整性验证。

4.如权利要求2所述的方法,进一步包括:

如果所述确定为所述第一消息有效,则与所述网络建立安全连接。

5.如权利要求1所述的方法,其中,所述第一消息进一步包括所述网络策略信息有效的时间量。

6.如权利要求5所述的方法,其中,所述第一密钥是进一步基于在所述UE与所述网络中的安全性锚功能SEAF之间共享的锚密钥或所述网络策略信息有效的所述时间量中的至少一者来生成的。

7.如权利要求6所述的方法,进一步包括在接收所述第一消息之前,与所述SEAF执行认证或注册规程中的至少一者,其中所述锚密钥是基于所述认证或注册规程中的至少一者来建立的。

8.如权利要求1所述的方法,其中,所述网络策略信息包括关于当与所述网络建立通信会话时所述UE是否将从所述网络中的会话管理功能SMF接收会话管理令牌的指示。

9.如权利要求1所述的方法,其中,所述第一消息是从所述网络中的接入和移动性管理功能AMF接收的。

10.如权利要求9所述的方法,其中,所述网络策略信息包括关于所述AMF是否与所述网络中的安全性锚功能SEAF共处一地的指示。

11.如权利要求9所述的方法,其中,所述网络策略信息包括所述AMF的安全性级别。

12.如权利要求1所述的方法,其中:

所述第一消息是从所述网络中的接入和移动性管理功能AMF接收的;以及

建立所述安全连接包括向所述AMF发送第二消息。

13.如权利要求12所述的方法,其中:

所述第一消息是安全性模式命令SMC消息;以及

所述第二消息是SMC完成消息。

14.如权利要求12所述的方法,其中,所述安全连接包括非接入阶层NAS安全连接。

15.如权利要求1所述的方法,进一步包括向所述网络发送UE策略信息,其中所述UE策略信息包括UE能力信息或UE安全性信息中的至少一者。

16.如权利要求15所述的方法,其中,生成所述第一密钥是基于发送至所述网络的所述UE策略信息的。

17.如权利要求15所述的方法,其中,所述网络策略信息是基于所述UE策略信息的。

18.一种用于由用户装备UE进行无线通信的装置,所述装置包括处理器,所述处理器被配置为使所述UE进行以下操作:

接收用于与网络建立安全连接的第一消息,其中所述第一消息包括网络策略信息;

通过密钥推导函数KDF,部分地基于作为所述KDF的输入的所述网络策略信息来生成第一密钥,其中所述网络策略信息包括所述网络的安全性特征;以及

使用所述第一密钥来验证所述网络策略信息。

19.如权利要求18所述的装置,其中,为了使用所述第一密钥来验证所述网络策略信息,所述处理器被配置为部分地基于所述第一密钥来确定所述第一消息是否有效。

20.如权利要求19所述的装置,其中:

所述第一消息由从第二密钥推导出的保护密钥进行完整性保护;以及

为了确定所述第一消息是否有效,所述处理器被配置为基于所述第一密钥对所述第一消息执行完整性验证。

21.如权利要求19所述的装置,其中,所述处理器被进一步配置为使所述UE进行以下操作:

如果所述确定为所述第一消息有效,则与所述网络建立安全连接。

22.如权利要求18所述的装置,其中,所述第一消息进一步包括所述网络策略信息有效的时间量。

23.如权利要求22所述的装置,其中,所述处理器被配置为进一步基于在所述UE与所述网络中的安全性锚功能SEAF之间共享的锚密钥或所述网络策略信息有效的所述时间量中的至少一者来生成所述第一密钥。

24.如权利要求23所述的装置,其中,所述处理器被进一步配置为使所述UE在接收所述第一消息之前,与所述SEAF执行认证或注册规程中的至少一者,其中所述锚密钥是基于所述认证或注册规程中的至少一者来建立的。

25.如权利要求18所述的装置,其中,所述网络策略信息包括关于当与所述网络建立通信会话时所述UE是否将从所述网络中的会话管理功能SMF接收会话管理令牌的指示。

26.如权利要求18所述的装置,其中,所述第一消息是从所述网络中的接入和移动性管理功能AMF接收的。

27.如权利要求26所述的装置,其中,所述网络策略信息包括关于所述AMF是否与所述网络中的安全性锚功能SEAF共处一地的指示。

28.如权利要求26所述的装置,其中,所述网络策略信息包括所述AMF的安全性级别。

29.如权利要求18所述的装置,其中:

所述第一消息是从所述网络中的接入和移动性管理功能AMF接收的;以及

为了建立所述安全连接,所述处理器被配置为使所述UE向所述AMF发送第二消息。

30.如权利要求29所述的装置,其中:

所述第一消息是安全性模式命令SMC消息;以及

所述第二消息是SMC完成消息。

31.如权利要求29所述的装置,其中,所述安全连接包括非接入阶层NAS安全连接。

32.如权利要求18所述的装置,其中,所述处理器被进一步配置为使所述UE向所述网络发送UE策略信息,其中所述UE策略信息包括UE能力信息或UE安全性信息中的至少一者。

33.如权利要求32所述的装置,其中,所述处理器被配置为基于发送至所述网络的所述UE策略信息生成所述第一密钥。

34.如权利要求32所述的装置,其中,所述网络策略信息是基于所述UE策略信息的。

35.一种用于由安全性锚功能SEAF进行无线通信的方法,包括:

通过密钥推导函数KDF,至少部分地基于作为所述KDF的输入的网络策略信息为网络节点生成密钥,其中所述密钥被用于建立用户装备UE和所述网络节点之间的安全连接,其中所述网络策略信息包括网络的安全性特征;以及

向所述网络节点发送所述密钥。

36.如权利要求35所述的方法,进一步包括:

在生成所述密钥之前,参与与所述UE的认证规程或注册规程中的至少一者,其中所述参与包括建立将在所述UE和所述SEAF之间共享的锚密钥。

37.如权利要求36所述的方法,其中,所述密钥是进一步基于所述锚密钥或所述网络策略信息有效的时间量中的至少一者来生成的。

38.如权利要求37所述的方法,进一步包括:

向所述网络节点发送所述网络策略信息或所述网络策略信息有效的所述时间量中的至少一者。

39.如权利要求35所述的方法,其中,所述网络策略信息包括关于所述网络节点是否与网络中的SEAF共处一地的指示。

40.如权利要求35所述的方法,其中,所述网络策略信息包括所述网络节点的安全性级别。

41.如权利要求35所述的方法,其中,所述网络策略信息包括关于网络中的会话管理功能SMF是否要为所述UE和所述网络之间的通信会话生成会话管理令牌并向所述UE传送所述会话管理令牌的指示。

42.如权利要求35所述的方法,进一步包括:

接收包括所述UE的策略信息的消息,其中所述UE策略信息包括UE能力信息或UE安全性信息中的至少一者。

43.如权利要求42所述的方法,其中,所述密钥是进一步基于所述UE策略信息来生成的。

44.如权利要求42所述的方法,其中,所述消息包括注册消息或附连请求消息。

45.如权利要求42所述的方法,其中,所述网络策略信息是基于所述UE策略信息来确定的。

46.如权利要求35所述的方法,其中,所述网络节点是网络中的接入和移动性管理功能AMF。

47.一种用于由安全性锚功能SEAF进行无线通信的装置,所述装置包括处理器,所述处理器被配置为使所述SEAF进行以下操作:

通过密钥推导函数KDF,至少部分地基于作为所述KDF的输入的网络策略信息为网络节点生成密钥,其中所述密钥被用于建立用户装备UE和所述网络节点之间的安全连接,其中所述网络策略信息包括网络的安全性特征;以及

向所述网络节点发送所述密钥。

48.一种用于由用户装备UE进行无线通信的方法,包括:

基于与网络的认证规程,建立在所述UE与所述网络中的安全性锚功能SEAF之间共享的锚密钥;

接收用于与所述网络建立安全连接的第一消息,其中所述第一消息包括用于与所述网络进行通信会话的网络策略令牌、网络策略信息、第一密钥有效的第一时间量和所述网络策略令牌有效的第二时间量;以及

在与所述网络建立所述安全连接之前,基于通过密钥推导函数KDF从作为所述KDF的输入的所述锚密钥、所述网络策略信息、所述第一时间量和所述第二时间量推导出的密钥来确定所述网络策略令牌是否有效,其中所述网络策略信息包括所述网络的安全性特征。

49.如权利要求48所述的方法,其中,所述网络策略信息包括关于所述UE是否将从所述网络中的会话管理功能SMF接收用于与所述网络进行通信会话的会话管理令牌的指示。

50.如权利要求48所述的方法,其中,所述第一消息是从所述网络中的接入和移动性管理功能AMF接收的。

51.如权利要求50所述的方法,其中,所述网络策略信息包括关于所述AMF是否与所述SEAF共处一地的指示。

52.如权利要求48所述的方法,其中,所述网络策略令牌包括与所述网络策略信息相关联的完整性保护信息。

53.如权利要求52所述的方法,其中,确定所述网络策略令牌是否有效包括基于从所述锚密钥推导出的所述密钥来验证所述完整性保护信息。

54.如权利要求48所述的方法,其中,所述第一消息由从所述第一密钥推导出的保护密钥进行完整性保护,所述方法进一步包括:

如果所述确定为所述网络策略令牌有效,则部分地基于所述锚密钥、所述第一时间量或所述第二时间量中的至少一者来生成第二密钥;以及

在生成所述第二密钥之后,部分地基于所述第二密钥来确定是否与所述网络建立所述安全连接。

55.如权利要求48所述的方法,其中,所述安全连接包括非接入阶层NAS安全连接。

56.一种用于由用户装备UE进行无线通信的装置,所述装置包括处理器,所述处理器被配置为使所述UE进行以下操作:

基于与网络的认证规程,建立在所述UE与所述网络中的安全性锚功能SEAF之间共享的锚密钥;

接收用于与所述网络建立安全连接的第一消息,其中所述第一消息包括用于与所述网络进行通信会话的网络策略令牌、网络策略信息、第一密钥有效的第一时间量和所述网络策略令牌有效的第二时间量;以及

在与所述网络建立所述安全连接之前,基于通过密钥推导函数KDF从作为所述KDF的输入的所述锚密钥、所述网络策略信息、所述第一时间量和所述第二时间量推导出的密钥来确定所述网络策略令牌是否有效,其中所述网络策略信息包括所述网络的安全性特征。

57.一种用于由安全性锚功能SEAF进行无线通信的方法,包括:

基于与用户装备UE的认证规程,建立在所述SEAF与网络中的所述UE之间共享的锚密钥;

部分地基于所述锚密钥、网络策略信息和网络策略令牌有效的第一时间量来生成所述网络策略令牌；

通过密钥推导函数KDF，部分地基于作为所述KDF的输入的所述网络策略信息来为网络节点生成密钥，其中所述网络策略信息包括所述网络的安全性特征；以及

向所述网络节点发送所述密钥、所述网络策略信息和所述网络策略令牌。

58.如权利要求57所述的方法，其中，所述网络策略令牌包括与所述网络策略信息相关联的完整性保护信息。

59.如权利要求57所述的方法，其中：

所述密钥是基于所述锚密钥或所述密钥有效的第二时间量中的至少一者生成的；以及

所述密钥被用于建立所述UE和所述网络节点之间的安全连接。

60.如权利要求59所述的方法，进一步包括向所述网络节点发送所述第一时间量和所述第二时间量。

61.如权利要求57所述的方法，其中，所述网络策略信息包括关于所述网络节点是否与所述网络中的SEAF共处一地的指示。

62.如权利要求57所述的方法，其中，所述网络策略包括关于所述网络中的会话管理功能SMF是否要为所述UE和所述网络之间的通信会话生成会话管理令牌并向所述UE传送所述会话管理令牌的指示。

63.如权利要求57所述的方法，其中，所述网络策略信息包括所述网络节点的安全性级别。

64.如权利要求57所述的方法，进一步包括：

接收包括所述UE的策略信息的消息，其中所述UE策略信息包括UE能力信息或UE安全性信息中的至少一者。

65.如权利要求57所述的方法，其中，所述网络节点是所述网络中的接入和移动性管理功能AMF。

66.一种用于由安全性锚功能SEAF进行无线通信的装置，所述装置包括处理器，所述处理器被配置为使所述SEAF进行以下操作：

基于与用户装备UE的认证规程，建立在所述SEAF与网络中的所述UE之间共享的锚密钥；

部分地基于所述锚密钥、网络策略信息和网络策略令牌有效的第一时间量来生成所述网络策略令牌；

通过密钥推导函数KDF，部分地基于作为所述KDF的输入的所述网络策略信息来为网络节点生成密钥，其中所述网络策略信息包括所述网络的安全性特征；以及

向所述网络节点发送所述密钥、所述网络策略信息和所述网络策略令牌。

在密钥生成中纳入网络策略

[0001] 根据35U.S.C.§119的优先权要求

[0002] 本申请要求于2018年9月28日提交的美国申请No.16/146,709的优先权,该美国申请要求于2017年10月2日提交的美国临时专利申请S/N.62/567,086的权益,这两篇申请的全部内容通过援引纳入于此。

技术领域

[0003] 本公开的某些方面一般涉及无线通信,尤其涉及用于在网络中建立安全通信的方法和装置。

背景技术

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

[0005] 在一些示例中,无线多址通信系统可包括数个基站,每个基站同时支持多个通信设备(另外被称为用户装备(UE))的通信。在LTE或LTE-A网络中,包含一个或多个基站的集合可定义演进型B节点(eNB)。在其他示例中(例如,在下一代或5G网络中),无线多址通信系统可包括与数个中央单元(CU)(例如,中央节点(CN)、接入节点控制器(ANC)等)处于通信的数个分布式单元(DU)(例如,边缘单元(EU)、边缘节点(EN)、无线电头端(RH)、智能无线电头端(SRH)、传送接收点(TRP)等),其中与中央单元处于通信的一个或多个分布式单元的集合可定义接入节点(例如,新无线电基站(NR BS)、新无线电B节点(NR NB)、网络节点、5G NB、gNB等)。基站或DU可与一组UE在下行链路信道(例如,用于来自基站或去往UE的传输)和上行链路信道(例如,用于从UE至基站或分布式单元的传输)上进行通信。

[0006] 这些多址技术已经在各种电信标准中被采纳以提供使不同的无线设备能够在城市、国家、地区、以及甚至全球级别上进行通信的共同协议。新兴电信标准的示例是新无线电(NR),例如,5G无线电接入。NR是对由第三代伙伴项目(3GPP)颁布的LTE移动标准的一组增强。它被设计成通过改善频谱效率、降低成本、改善服务、利用新频谱、并且更好地与在下行链路(DL)和上行链路(UL)上使用具有循环前缀(CP)的OFDMA的其他开放标准进行整合来更好地支持移动宽带因特网接入,以及支持波束成形、多输入多输出(MIMO)天线技术和载波聚集。

[0007] 然而,随着对移动宽带接入的需求持续增长,存在对NR技术中的进一步改进的需要。优选地,这些改进应当适用于其他多址技术以及采用这些技术的电信标准。

发明内容

[0008] 本公开的系统、方法和设备各自具有若干方面,其中并非仅靠任何单一方面来负

责其期望属性。在不限定如所附权利要求所表述的本公开的范围的情况下，现在将简要地讨论一些特征。在考虑此讨论后，并且尤其是在阅读题为“详细描述”的章节之后，将理解本公开的特征是如何提供包括无线网络中的改进通信的优点的。

[0009] 本公开的某些方面提供了一种用于由用户装备(UE)进行无线通信的方法。该方法通常包括接收用于与网络建立安全连接的第一消息，其中第一消息包括网络策略信息。该方法还包括部分地基于网络策略信息来生成第一密钥。该方法进一步包括使用第一密钥来验证网络信息。

[0010] 本公开的某些方面提供了一种用于由网络节点(诸如安全性锚功能(SEAF))进行无线通信的方法。该方法通常包括至少部分地基于网络策略信息来生成用于网络节点的密钥。该密钥被用于建立UE和网络节点之间的安全连接。该方法还包括向网络节点发送该密钥。

[0011] 本公开的某些方面提供了一种用于由用户装备(UE)进行无线通信的方法。该方法通常包括基于与网络的认证规程，建立在UE与网络中的安全性锚功能(SEAF)之间共享的锚密钥。该方法还包括接收用于与网络建立安全连接的第一消息，其中第一消息包括用于与网络进行通信会话的网络策略令牌、网络策略信息、第一密钥有效的第一时间量和网络策略令牌有效的第二时间量。该方法进一步包括在与网络建立安全连接之前，基于从共享锚密钥、网络策略信息、第一时间量和第二时间量推导出的密钥来确定网络策略令牌是否有效。

[0012] 本公开的某些方面提供了一种用于由网络节点(诸如安全性锚功能(SEAF))进行无线通信的方法。该方法一般包括基于与UE的认证规程，建立在SEAF与网络中的UE之间共享的锚密钥。该方法还包括部分地基于锚密钥、网络策略信息和网络策略令牌有效的第一时间量来生成网络策略令牌。该方法进一步包括为另一网络节点生成密钥；以及向该另一网络节点发送该密钥、网络策略信息和网络策略令牌。

[0013] 提供了包括能够执行以上描述的操作的方法、装备(装置)、系统、计算机程序产品、以及处理系统的众多其他方面。

[0014] 为了达成前述及相关目的，这一个或多个方面包括在下文充分描述并在权利要求中特别指出的特征。以下描述和附图详细阐述了这一个或多个方面的某些解说性特征。然而，这些特征仅仅是指示了可采用各个方面的原理的各种方式中的若干种，并且本描述旨在涵盖所有此类方面及其等效方案。

附图说明

[0015] 为了能详细理解本公开的以上陈述的特征所用的方式，可参照各方面来对以上简要概述的内容进行更具体的描述，其中一些方面在附图中解说。然而应该注意，附图仅解说了本公开的某些典型方面，故不应被认为限定其范围，因为本描述可允许有其他等同有效的方面。

[0016] 图1是概念性地解说根据本公开的某些方面的示例电信系统的框图。

[0017] 图2是解说根据本公开的某些方面的分布式RAN的示例逻辑架构的框图。

[0018] 图3是解说根据本公开的某些方面的分布式RAN的示例物理架构的示图。

[0019] 图4是概念性地解说根据本公开的某些方面的示例BS和用户装备(UE)的设计的框

图。

[0020] 图5是示出根据本公开的某些方面的用于实现通信协议栈的示例的示图。

[0021] 图6解说了根据本公开的某些方面的DL中心式子帧的示例。

[0022] 图7解说了根据本公开的某些方面的UL中心式子帧的示例。

[0023] 图8-9解说了根据本公开的某些方面的具有一个或多个非共处一地的网络节点的示例5G架构。

[0024] 图10是解说根据本公开的某些方面的用于网络中的无线通信的示例操作的流程图。

[0025] 图11是解说根据本公开的某些方面的用于网络中的无线通信的示例操作的流程图。

[0026] 图12是解说根据本公开的某些方面的示例注册规程的呼叫流图。

[0027] 图13是解说根据本公开的某些方面的用于网络中的无线通信的示例操作的流程图。

[0028] 图14是解说根据本公开的某些方面的用于网络中的无线通信的示例操作的流程图。

[0029] 图15是解说根据本公开的某些方面的示例注册规程的呼叫流图。

[0030] 为了促进理解,在可能之处使用了相同的附图标记来指定各附图共有的相同要素。构想了一个实施例中所公开的要素可有益地用在其他实施例而无需具体引述。

具体实施方式

[0031] 本公开的各方面提供了用于无线网络(诸如新无线电(NR)(新无线电接入技术或5G技术)无线网络)的装置、方法、处理系统和计算机可读介质。

[0032] NR可支持各种无线通信服务,诸如以宽带宽(例如,超过80MHz)为目标的增强型移动宽带(eMBB)、以高载波频率(例如,60GHz)为目标的毫米波(mmW)、以非后向兼容的MTC技术为目标的大规模MTC(mMTC)、和/或以超可靠低等待时间通信(URLLC)为目标的关键任务。这些服务可包括等待时间和可靠性要求。这些服务还可具有不同的传输时间区间(TTI)以满足相应的服务质量(QoS)要求。另外,这些服务可以在相同子帧中共存。

[0033] NR引入了网络切片的概念。例如,网络可具有多个切片,这可支持不同的服务,例如万物联网(IoE)、URLLC、eMBB、车辆间(V2V)通信等。切片可以被定义为包括为提供某些网络能力和网络特性所必需的一组网络功能和对应资源的完整逻辑网络。

[0034] 在一些方面,5G NR系统可以能够支持各种不同的部署场景。特别地,随着5G技术和/或服务需求不断发展,由5G网络中的一个或多个网络节点执行的服务、能力和/或功能可能会变化。由于UE可能不知道网络架构中的改变,因此向UE通知特定的网络配置、能力、安全性配置等可能是有益的。然而,使用当前技术可能不能够使网络以安全方式向UE通知网络(安全性)配置、能力和策略。

[0035] 例如,在5G系统中,UE与服务网络之间通常存在单个控制面接口(N1)。此N1接口通常用于在UE与接入和移动性管理功能(AMF)AMF之间建立非接入阶层(NAS)连接。但是,在一些部署场景中,AMF可能不负责(或无法访问)网络中的安全性功能。因此,由于AMF可能是与UE具有信令连接的唯一实体,因此可能存在(流氓的或恶意的)AMF可以拦截网络配置信息

并修改提供给UE的网络配置信息以破坏UE与网络之间的连接/通信的情形。因此，本公开的各方面提供了用于安全地向UE通知网络(安全性)配置、能力、网络策略等的技术。

[0036] 以下参照附图更全面地描述本公开的各个方面。然而，本公开可用许多不同形式来实施并且不应解释为被限于本公开通篇给出的任何具体结构或功能。相反，提供这些方面是为了使得本公开将是透彻和完整的，并且其将向本领域技术人员完全传达本公开的范围。基于本文中的教导，本领域技术人员应领会，本公开的范围旨在覆盖本文中所披露的本公开的任何方面，不论其是与本公开的任何其他方面相独立地实现还是组合地实现的。例如，可使用本文中所阐述的任何数目的方面来实现装置或实践方法。另外，本公开的范围旨在覆盖使用作为本文中所阐述的本公开的各个方面的补充或者另外的其他结构、功能性、或者结构及功能性来实践的此类装置或方法。应当理解，本文中所披露的本公开的任何方面可由权利要求的一个或多个元素来实施。

[0037] 措辞“示例性”在本文中用于意指“用作示例、实例、或解说”。本文中描述为“示例性”的任何方面不必被解释为优于或胜过其他方面。

[0038] 尽管本文描述了特定方面，但这些方面的众多变体和置换落在本公开的范围之内。尽管提到了优选方面的一些益处和优点，但本公开的范围并非旨在被限于特定益处、用途或目标。确切而言，本公开的各方面旨在宽泛地适用于不同的无线技术、系统配置、网络、和传输协议，其中一些藉由示例在附图和以下对优选方面的描述中解说。详细描述和附图仅仅解说本公开而非限定本公开，本公开的范围由所附权利要求及其等效技术方案来定义。

[0039] 本文所描述的技术可用于各种无线通信网络，诸如CDMA、TDMA、FDMA、OFDMA、SC-FDMA及其他网络。术语“网络”和“系统”常常可互换地使用。CDMA网络可以实现诸如通用地面无线电接入(UTRA)、cdma2000等无线电技术。UTRA包括宽带CDMA(WCDMA)、时分同步CDMA(TD-SCDMA)和CDMA的其他变体。cdma2000涵盖IS-2000、IS-95和IS-856标准。TDMA网络可实现诸如全球移动通信系统(GSM)之类的无线电技术。OFDMA网络可以实现诸如演进型UTRA(E-UTRA)、超移动宽带(UMB)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、Flash-OFDM®等的无线电技术。UTRA和E-UTRA是通用移动电信系统(UMTS)的一部分。频分双工(FDD)和时分双工(TDD)两者中的3GPP长期演进(LTE)和高级LTE(LTE-A)是UMTS的使用E-UTRA的新版本，其在下行链路上采用OFDMA而在上行链路上采用SC-FDMA。UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM在来自名为“第3代伙伴项目”(3GPP)的组织的文献中描述。cdma2000和UMB在来自名为“第3代伙伴项目2”(3GPP2)的组织的文献中描述。本文所描述的技术可被用于以上所提及的无线网络和无线电技术以及其他无线网络和无线电技术，诸如5G下一代/NR网络。

[0040] 示例无线通信系统

[0041] 图1解说了其中可以执行本公开的各方面(例如用于安全地向UE提供网络(安全性)策略信息(例如，网络配置、安全性信息、能力等))的示例无线网络100，诸如新无线电(NR)或5G网络。在一些情形中，网络100可以是多切片网络，其中每个切片定义为被捆绑在一起以满足特定用例或商业模型的要求的合格配置的网络功能、网络应用和底层云基础设施的组合。

[0042] 如图1中所解说的，无线网络100可包括数个BS 110和其他网络实体。BS可以是与

UE进行通信的站。每个BS 110可为特定地理区域提供通信覆盖。在3GPP中，术语“蜂窝小区”可指代B节点的覆盖区域和/或服务该覆盖区域的B节点子系统，这取决于使用该术语的上下文。在NR系统中，术语“蜂窝小区”和eNB、B节点、5G NB、AP、NR BS、NR BS、或TRP可以是可互换的。在一些示例中，蜂窝小区可以不一定是驻定的，并且该蜂窝小区的地理区域可根据移动基站的位置而移动。在一些示例中，基站可通过各种类型的回程接口(诸如直接物理连接、虚拟网络、或使用任何合适的传输网络的类似物)来彼此互连和/或互连至无线网络100中的一个或多个其他基站或网络节点(未示出)。

[0043] 一般而言，在给定的地理区域中可部署任何数目的无线网络。每个无线网络可支持特定的无线电接入技术(RAT)，并且可在一个或多个频率上工作。RAT也可被称为无线电技术、空中接口等。频率也可被称为载波、频率信道等。每个频率可在给定地理区域中支持单个RAT以避免不同RAT的无线网络之间的干扰。在一些情形中，NR或5G RAT网络可采用多切片网络架构来部署。

[0044] BS可以提供对宏蜂窝小区、微微蜂窝小区、毫微微蜂窝小区、和/或其他类型的蜂窝小区的通信覆盖。宏蜂窝小区可以覆盖相对较大的地理区域(例如，半径为数千米)，并且可允许无约束地由具有服务订阅的UE接入。微微蜂窝小区可以覆盖相对较小的地理区域，并且可允许无约束地由具有服务订阅的UE接入。毫微微蜂窝小区可以覆盖相对较小的地理区域(例如，住宅)且可允许有约束地由与该毫微微蜂窝小区有关联的UE(例如，封闭订户群(CSG)中的UE、住宅中用户的UE等)接入。用于宏蜂窝小区的BS可被称为宏BS。用于微微蜂窝小区的BS可被称为微微BS。用于毫微微蜂窝小区的BS可被称为毫微微BS或家用BS。在图1中所示的示例中，BS 110a、110b和110c可以分别是用于宏蜂窝小区102a、102b和102c的宏BS。BS 110x可以是用于微微蜂窝小区102x的微微BS。BS 110y和110z可以分别是用于毫微微蜂窝小区102y和102z的毫微微BS。BS可以支持一个或多个(例如，三个)蜂窝小区。

[0045] 无线网络100还可以包括中继站。中继站是从上游站(例如，BS或UE)接收数据和/或其他信息的传输并向下游站(例如，UE或BS)发送该数据和/或其他信息的传输的站。中继站还可以是为其他UE中继传输的UE。在图1中所示的示例中，中继站110r可以与BS 110a和UE 120r进行通信以促成BS 110a与UE 120r之间的通信。中继站也可被称为中继BS、中继等。

[0046] 无线网络100可以是包括不同类型的BS(例如，宏BS、微微BS、毫微微BS、中继等)的异构网络。这些不同类型的BS可具有不同发射功率电平、不同覆盖区域、以及对无线网络100中的干扰的不同影响。例如，宏BS可具有高发射功率电平(例如，20瓦)，而微微BS、毫微微BS和中继可具有较低的发射功率电平(例如，1瓦)。

[0047] 无线网络100可以支持同步或异步操作。对于同步操作，各BS可以具有类似的帧定时，并且来自不同BS的传输可以在时间上大致对齐。对于异步操作，各BS可以具有不同的帧定时，并且来自不同BS的传输可能在时间上并不对齐。本文中所描述的技术可被用于同步和异步操作两者。

[0048] 网络控制器130可以耦合到一组BS并提供对这些BS的协调和控制。网络控制器130可以经由回程与BS 110进行通信。BS 110还可以例如经由无线或有线回程直接或间接地彼此通信。

[0049] UE 120(例如，120x、120y等)可以分散遍及无线网络100，并且每个UE可以是驻定

或移动的。UE也可被称为移动站、终端、接入终端、订户单元、站、客户端装备(CPE)、蜂窝电话、智能电话、个人数字助理(PDA)、无线调制解调器、无线通信设备、手持式设备、膝上型计算机、无绳电话、无线本地环(WLL)站、平板设备、相机、游戏设备、上网本、智能本、超级本、医疗设备或医疗装备、生物测定传感器/设备、可穿戴设备(诸如智能手表、智能服装、智能眼镜、智能腕带、智能珠宝(例如,智能戒指、智能项链等))、娱乐设备(例如,音乐设备、视频设备、卫星无线电等)、车辆组件或传感器、智能计量仪/传感器、工业制造装备、全球定位系统设备、或者被配置成经由无线或有线介质进行通信的任何其他合适设备。一些UE可被认为是演进型或机器类型通信(MTC)设备或演进型MTC(eMTC)设备。MTC和eMTC UE包括例如机器人、无人机、远程设备、传感器、计量仪、监视器、位置标签等,其可与BS、另一设备(例如,远程设备)或某一其他实体通信。无线节点可以例如经由有线或无线通信链路来为网络(例如,广域网,诸如因特网或蜂窝网络)提供连通性或提供至该网络的连通性。一些UE可被认为是物联网(IoT)设备。

[0050] 在图1中,带有双箭头的实线指示UE与服务BS之间的期望传输,服务BS是被指定为在下行链路和/或上行链路上服务该UE的BS。带有双箭头的虚线指示UE与BS之间的干扰传输。

[0051] 某些无线网络(例如,LTE)在下行链路上利用正交频分复用(OFDM)并在上行链路上利用单载波频分复用(SC-FDM)。OFDM和SC-FDM将系统带宽划分成多个(K个)正交副载波,这些副载波也常被称为频调、频槽等。每个副载波可用数据来调制。一般而言,调制码元对于OFDM是在频域中发送的,而对于SC-FDM是在时域中发送的。毗邻副载波之间的间隔可以是固定的,且副载波的总数(K)可取决于系统带宽。例如,副载波的间隔可以是15kHz,而最小资源分配(称为'资源块')可以是12个副载波(或180kHz)。因此,对于1.25、2.5、5、10或20兆赫兹(MHz)的系统带宽,标称FFT大小可以分别等于128、256、512、1024或2048。系统带宽还可被划分成子带。例如,子带可以覆盖1.08MHz(即,6个资源块),并且对于1.25、2.5、5、10或20MHz的系统带宽,可分别有1、2、4、8或16个子带。

[0052] 虽然本文所描述的示例的各方面可与LTE技术相关联,但本公开的各方面可适用于其它无线通信系统,诸如NR/5G。

[0053] NR可以在上行链路和下行链路上利用具有CP的OFDM并且包括对使用TDD的半双工操作的支持。可以支持100MHz的单个分量载波带宽。NR资源块可在0.1ms历时上跨越具有75kHz的副载波带宽的12个副载波。每个无线电帧可包括具有10ms长度的50个子帧。因此,每个子帧可具有0.2ms的长度。每个子帧可以指示用于数据传输的链路方向(即,DL或UL),并且用于每个子帧的链路方向可动态切换。每个子帧可以包括DL/UL数据以及DL/UL控制数据。用于NR的UL和DL子帧可以在以下参照图6和7更详细地描述。可以支持波束成形并且可动态配置波束方向。还可以支持具有预编码的MIMO传输。DL中的MIMO配置可以支持至多达8个发射天线(具有至多达8个流的多层DL传输)和每UE至多达2个流。可以支持每UE至多达2个流的多层传输。可以使用至多达8个服务蜂窝小区来支持多个蜂窝小区的聚集。替换地,除了基于OFDM之外,NR可以支持不同的空中接口。NR网络可以包括诸如CU和/或DU之类的实体。

[0054] 在一些示例中,可以调度对空中接口的接入,其中调度实体(例如,基站)在其服务区域或蜂窝小区内的一些或全部设备和装备间分配用于通信的资源。在本公开内,如以下

进一步讨论的，调度实体可以负责调度、指派、重配置、以及释放用于一个或多个下级实体的资源。即，对于被调度的通信而言，下级实体利用由调度实体分配的资源。基站不是可用作调度实体的唯一实体。即，在一些示例中，UE可以用作调度实体，从而调度用于一个或多个下级实体(例如，一个或多个其他UE)的资源。在该示例中，该UE正充当调度实体，并且其他UE利用由该UE调度的资源来进行无线通信。UE可在对等(P2P)网络中和/或在网状网络中充当调度实体。在网状网络示例中，UE除了与调度实体通信之外还可以可任选地直接彼此通信。

[0055] 由此，在具有对时频资源的经调度接入并且具有蜂窝配置、P2P配置和网状配置的无线通信网络中，调度实体和一个或多个下级实体可利用所调度的资源来通信。

[0056] 如以上所提及的，RAN可以包括CU和DU。NR BS(例如，gNB、5G B节点、B节点、传送接收点(TRP)、接入点(AP))可对应于一个或多个BS。NR蜂窝小区可被配置为接入蜂窝小区(ACell)或仅数据蜂窝小区(DCell)。例如，RAN(例如，中央单元或分布式单元)可配置这些蜂窝小区。DCell可以是用于载波聚集或双连通性但不用于初始接入、蜂窝小区选择/重选、或切换的蜂窝小区。在一些情形中，DCell可以不传送同步信号——在一些情形中，DCell可以传送SS。NR BS可以向UE传送下行链路信号以指示蜂窝小区类型。基于该蜂窝小区类型指示，UE可与NR BS通信。例如，UE可以基于所指示的蜂窝小区类型来确定要考虑用于蜂窝小区选择、接入、切换和/或测量的NR BS。

[0057] 图2解说了分布式无线电接入网(RAN)200的示例逻辑架构，其可在图1中所解说的无线通信系统中实现。5G接入节点206可包括接入节点控制器(ANC)202。ANC可以是分布式RAN 200的中央单元(CU)。到下一代核心网(NG-CN)204的回程接口可在ANC处终接。到相邻下一代接入节点(NG-AN)的回程接口可在ANC处终接。ANC可以包括一个或多个TRP 208(其还可被称为BS、NR BS、B节点、5G NB、AP或某一其他术语)。如上所述，TRP可与“蜂窝小区”可互换地使用。

[0058] TRP 208可以是DU。TRP可被连接到一个ANC(ANC 202)或者一个以上ANC(未解说)。例如，对于RAN共享、无线电即服务(RaaS)和因服务而异的AND部署，TRP可被连接到一个以上ANC。TRP可以包括一个或多个天线端口。TRP可被配置成个体地(例如，动态选择)或联合地(例如，联合传输)服务至UE的话务。

[0059] 本地架构200可被用来解说去程(fronthaul)定义。该架构可被定义为支持跨不同部署类型的去程解决方案。例如，该架构可以基于传送网络能力(例如，带宽、等待时间和/或抖动)。

[0060] 该架构可与LTE共享特征和/或组件。根据诸方面，下一代AN(NG-AN)210可支持与NR的双连通性。对于LTE和NR，NG-AN可共享共用去程。

[0061] 该架构可实现各TRP 208之间和之中的协作。例如，可在TRP内和/或经由ANC 202跨各TRP预设协作。根据诸方面，可以不需要/不存在TRP间接口。

[0062] 根据诸方面，拆分逻辑功能的动态配置可存在于架构200内。如将参照图5更详细地描述的，可在DU或CU处(例如，分别在TRP或ANC处)可适应性地放置无线电资源控制(RRC)层、分组数据汇聚协议(PDCP)层、无线电链路控制(RLC)层、媒体接入控制(MAC)层、以及物理(PHY)层。根据某些方面，BS可包括中央单元(CU)(例如，ANC 202)和/或一个或多个分布式单元(例如，一个或多个TRP 208)。

[0063] 图3解说了根据本公开的诸方面的分布式RAN 300的示例物理架构。集中式核心网单元(C-CU)302可主存核心网功能。C-CU可被集中地部署。C-CU功能性可被卸载(例如,至高级无线服务(AWS))以力图处置峰值容量。

[0064] 集中式RAN单元(C-RU)304可主存一个或多个ANC功能。可任选地,C-RU可在本地主存核心网功能。C-RU可以具有分布式部署。C-RU可以更靠近网络边缘。

[0065] DU 306可以主存一个或多个TRP(边缘节点(EN)、边缘单元(EU)、无线电头端(RH)、智能无线电头端(SRH)等)。DU可位于具有射频(RF)功能性的网络的边缘处。

[0066] 图4解说了图1中所解说的BS 110和UE 120的示例组件,其可被用来实现本公开的诸方面。如上所述,BS可包括TRP。BS 110和UE 120的一个或多个组件可被用来实践本公开的诸方面。例如,UE 120的天线452、处理器466、458、464和/或控制器/处理器480、和/或BS 110的天线434、处理器430、420、438和/或控制器/处理器440可被用来执行本文中所描述且参照图10-15解说的操作。

[0067] 根据各方面,对于受约束关联场景,基站110可以是图1中的宏BS 110c,并且UE 120可以是UE 120y。基站110也可以是某种其他类型的基站。基站110可装备有天线434a到434t,并且UE 120可装备有天线452a到452r。

[0068] 在基站110处,发射处理器420可接收来自数据源412的数据以及来自控制器/处理器440的控制信息。控制信息可用于物理广播信道(PBCH)、物理控制格式指示符信道(PCFICH)、物理混合ARQ指示符信道(PHICH)、物理下行链路控制信道(PDCCH)等。数据可用于物理下行链路共享信道(PDSCH)等。处理器420可处理(例如,编码和码元映射)数据和控制信息以分别获得数据码元和控制码元。处理器420还可生成(例如,用于PSS、SSS、以及因蜂窝小区而异的参考信号的)参考码元。发射(TX)多输入多输出(MIMO)处理器430可在适用的情况下对数据码元、控制码元、和/或参考码元执行空间处理(例如,预编码),并且可将输出码元流提供给调制器(MOD)432a到432t。每个调制器432可处理各自的输出码元流(例如,针对OFDM等等)以获得输出采样流。每个调制器432可进一步处理(例如,转换至模拟、放大、滤波、及上变频)输出采样流以获得下行链路信号。来自调制器432a到432t的下行链路信号可分别经由天线434a到434t被发射。

[0069] 在UE 120处,天线452a到452r可接收来自基站110的下行链路信号并可分别向解调器(DEMOD)454a到454r提供收到信号。每个解调器454可调理(例如,滤波、放大、下变频、以及数字化)各自的收到信号以获得输入采样。每个解调器454可进一步处理输入采样(例如,针对OFDM等)以获得收到码元。MIMO检测器456可从所有解调器454a到454r获得收到码元,在适用的情况下对这些收到码元执行MIMO检测,并提供检出码元。接收处理器458可处理(例如,解调、解交织、以及解码)这些检出码元,将经解码的给UE 120的数据提供给数据阱460,并且将经解码的控制信息提供给控制器/处理器480。

[0070] 在上行链路上,在UE 120处,发射处理器464可接收并处理来自数据源462的(例如,用于物理上行链路共享信道(PUSCH)的)数据以及来自控制器/处理器480的(例如,用于物理上行链路控制信道(PUCCH)的)控制信息。发射处理器464还可生成参考信号的参考码元。来自发射处理器464的码元可在适用的情况下由TX MIMO处理器466预编码,由解调器454a到454r进一步处理(例如,针对SC-FDM等),并且向基站110传送。在BS 110处,来自UE 120的上行链路信号可由天线434接收,由调制器432处理,在适用的情况下由MIMO检测器

436检测，并由接收处理器438进一步处理以获得经解码的由UE 120发送的数据和控制信息。接收处理器438可将经解码数据提供给数据阱439并将经解码控制信息提供给控制器/处理器440。

[0071] 控制器/处理器440和480可分别指导基站110和UE 120处的操作。基站110处的处理器440和/或其他处理器和模块可执行或指导例如用于本文中所描述的技术的过程。UE 120处的处理器480和/或其他处理器和模块还可执行或指导例如图10、12-13和/或15中所解说的功能框、和/或用于本文中所描述的技术的其他过程的执行。存储器442和482可分别存储用于BS 110和UE 120的数据和程序代码。调度器444可以调度UE以进行下行链路和/或上行链路上的数据传输。

[0072] 图5解说了示出根据本公开的诸方面的用于实现通信协议栈的示例的示图500。所解说的通信协议栈可由在5G系统(例如，支持基于上行链路的移动性的系统)中操作的设备来实现。示图500解说了包括无线电资源控制(RRC)层510、分组数据汇聚协议(PDCP)层515、无线电链路控制(RLC)层520、媒体接入控制(MAC)层525和物理(PHY)层530的通信协议栈。在各种示例中，协议栈的这些层可被实现为分开的软件模块、处理器或ASIC的部分、由通信链路连接的非共处一地的设备的部分、或其各种组合。共处一地和非共处一地的实现可例如在协议栈中用于网络接入设备(例如，AN、CU和/或DU)或UE。

[0073] 第一选项505-a示出了协议栈的拆分实现，其中协议栈的实现在集中式网络接入设备(例如，图2中的ANC 202)与分布式网络接入设备(例如，图2中的TRP 208)之间拆分。在第一选项505-a中，RRC层510和PDCP层515可由中央单元实现，而RLC层520、MAC层525和PHY层530可由DU实现。在各种示例中，CU和DU可共处一地或非共处一地。第一选项505-a在宏蜂窝小区、微蜂窝小区、或微微蜂窝小区部署中可以是有用的。

[0074] 第二选项505-b示出了协议栈的统一实现，其中协议栈是在单个网络接入设备(例如，接入节点(AN)、新无线电基站(NR BS)、新无线电B节点(NR NB)、网络节点(NN)等)中实现的。在第二选项中，RRC层510、PDCP层515、RLC层520、MAC层525、以及PHY层530各自可由AN实现。第二选项505-b在毫微微蜂窝小区部署中可以是有用的。

[0075] 不管网络接入设备实现部分还是全部的协议栈，UE可实现整个协议栈(例如，RRC层510、PDCP层515、RLC层520、MAC层525、以及PHY层530)。

[0076] 图6是示出可以被用于在无线网络100中进行通信的DL中心式子帧的示例的示图600。DL中心式子帧可包括控制部分602。控制部分602可存在于DL中心式子帧的初始或开始部分中。控制部分602可包括对应于DL中心式子帧的各个部分的各种调度信息和/或控制信息。在一些配置中，控制部分602可以是物理DL控制信道(PDCCH)，如图6中所指示的。DL中心式子帧还可包括DL数据部分604。DL数据部分604有时可被称为DL中心式子帧的有效载荷。DL数据部分604可包括用于从调度实体(例如，UE或BS)向下级实体(例如，UE)传达DL数据的通信资源。在一些配置中，DL数据部分604可以是物理DL共享信道(PDSCH)。

[0077] DL中心式子帧还可包括共用UL部分606。共用UL部分606有时可被称为UL突发、共用UL突发、和/或各种其他合适术语。共用UL部分606可包括对应于DL中心式子帧的各个其他部分的反馈信息。例如，共用UL部分606可包括对应于控制部分602的反馈信息。反馈信息的非限制性示例可包括ACK信号、NACK信号、HARQ指示符、和/或各种其他合适类型的信息。共用UL部分606可以包括附加或替换信息，诸如与随机接入信道(RACH)规程、调度请求(SR)

有关的信息、以及各种其他合适类型的信息。如图6中所解说的，DL数据部分604的结束可在时间上与共用UL部分606的开始分隔开。该时间分隔有时可被称为间隙、保护时段、保护区间、和/或各种其他合适术语。这一分隔提供了用于从DL通信(例如，由下级实体(例如，UE)进行的接收操作)到UL通信(例如，由下级实体(例如，UE)进行的传输)的切换的时间。本领域普通技术人员将理解，前述内容仅仅是DL中心式子帧的一个示例，并且可存在具有类似特征的替换结构而不必偏离本文所描述的诸方面。

[0078] 图7是示出可以被用于在无线网络100中进行通信的UL中心式子帧的示例的示图700。UL中心式子帧可包括控制部分702。控制部分702可存在于UL中心式子帧的初始或开始部分中。图7中的控制部分702可类似于以上参照图6描述的控制部分。UL中心式子帧还可包括UL数据部分704。UL数据部分704有时可被称为UL中心式子帧的有效载荷。该UL部分可指用于从下级实体(例如，UE)向调度实体(例如，UE或BS)传达UL数据的通信资源。在一些配置中，控制部分702可以是物理DL控制信道(PDCCH)。

[0079] 如图7中所解说的，控制部分702的结束可在时间上与UL数据部分704的开始分隔开。该时间分隔有时可被称为间隙、保护时段、保护区间、和/或各种其他合适术语。这一分隔提供了用于从DL通信(例如，由调度实体进行的接收操作)到UL通信(例如，由调度实体进行的传输)的切换的时间。UL中心式子帧还可包括共用UL部分706。图7中的共用UL部分706可类似于以上参照图6描述的共用UL部分606。共用UL部分706可附加或替换地包括与信道质量指示符(CQI)、探通参考信号(SRS)有关的信息、以及各种其他合适类型的信息。本领域普通技术人员将理解，前述内容仅仅是UL中心式子帧的一个示例，并且可存在具有类似特征的替换结构而不必然偏离本文所描述的诸方面。

[0080] 在一些情况下，两个或更多个下级实体(例如，UE)可使用侧链路信号来彼此通信。此类侧链路通信的现实世界应用可包括公共安全、邻近度服务、UE到网络中继、交通工具到交通工具(V2V)通信、万物联网(IoE)通信、IoT通信、关键任务网状网、和/或各种其他合适应用。一般而言，侧链路信号可指从一个下级实体(例如，UE1)传达给另一下级实体(例如，UE2)而无需通过调度实体(例如，UE或BS)中继该通信的信号，即使调度实体可被用于调度和/或控制目的。在一些示例中，侧链路信号可使用有执照频谱来传达(不同于无线局域网，其通常使用无执照频谱)。

[0081] UE可在各种无线电资源配置中操作，包括与使用专用资源集传送导频相关联的配置(例如，无线电资源控制(RRC)专用状态等)、或者与使用共用资源集传送导频相关联的配置(例如，RRC共用状态等)。当在RRC专用状态中操作时，UE可选择专用资源集以用于向网络传送导频信号。当在RRC共用状态中操作时，UE可选择共用资源集以用于向网络传送导频信号。在任一情形中，由UE传送的导频信号可由一个或多个网络接入设备(诸如AN、或DU、或其诸部分)接收。每个接收方网络接入设备可被配置成接收和测量在共用资源集上传送的导频信号，并且还接收和测量在分配给UE的专用资源集上传送的导频信号，其中该网络接入设备是针对该UE的监视方网络接入设备集的成员。一个或多个接收方网络接入设备或者(诸)接收方网络接入设备向其传送导频信号测量的CU可使用这些测量来标识UE的服务蜂窝小区或者发起针对一个或多个UE的服务蜂窝小区的改变。

[0082] 在密钥生成中纳入网络策略的示例

[0083] 如以上所提及的，正为5G引入包括各特征的新空中接口，这些特征包括以宽带宽

(例如,超过80MHz)为目标的增强型移动宽带(eMBB)、以高载波频率(例如,60GHz)为目标的毫米波(mmW)、以非后向兼容MTC技术为目标的大规模MTC(mMTC)、和以超可靠低等待时间通信(URLLC)为目标的关键任务。

[0084] 随着5G服务和技术的不断发展,5G可以能够支持各种不同的部署场景。在当前的5G架构中,例如,负责在网络中执行不同功能的一个或多个网络节点(例如,安全性锚功能(SEAF)、接入和移动性管理功能(AMF)、会话管理功能(SMF)等)可以是共处一地的或是物理分离的。

[0085] 5G中引入了SEAF,以使得即使需要将AMF移动和/或定位成靠近网络边缘(例如RAN),也可以将安全性锚保持在物理安全位置中。因此,在一些部署中,SEAF可以与AMF共处一地,而在其他部署中,SEAF可以与AMF分离(例如,SEAF和AMF可以各自具有独立功能)。类似地,SMF可以与AMF和SEAF分离。在一些情形中,SMF可以与AMF是物理分离的,并且可能位于与AMF不同的安全性域内(例如,在网络共享场景的情形中)。在一些情形中,SMF可以是因切片而异的。

[0086] 图8解说了根据本公开的某些方面的5G架构800的参考示例,其中一个或多个网络节点可以是物理分离的。具体而言,架构800解说了部署场景的参考示例,其中SEAF与AMF是物理分离的(例如,与其他部署场景中共处一地的SEAF/AMF相反)。

[0087] 如图所示,5G架构800可以包括多个切片。每个切片可支持不同的服务,例如,万物联网(IoE)、URLLC、eMBB、车辆通信(即V2X,诸如车辆到车辆(V2V)、车辆到基础设施(V2I)、车辆到行人(V2P)、车辆到网络(V2N))等。

[0088] 切片可以被定义为包括为提供某些网络能力和网络特性所必需的一组网络功能和对应资源的完整逻辑网络,其可以包括5G-AN和5G-CN两者。更具体地,切片可以是被捆绑在一起以满足特定用例或商业模型的要求的合格配置的网络功能、网络应用和底层云基础设施的组合。在一些情形中,不同的切片可被指派不相交的资源,并且可具有不同的要求(诸如等待时间和/或功率)。

[0089] 在此示例中,AMF可以被配置成同时服务多个切片。例如,AMF可以在UE和网络切片之间提供移动性管理NAS安全性锚。SMF通常被配置成执行服务授权/认证,以支持因服务(切片)而异的PDU会话建立。SMF还可以执行诸如修改和释放之类的功能,包括在用户面功能(UPF)与RAN之间维护的隧道。用户面安全性可以在UDF处终止。在一些情形中,SMF可以能够支持因服务而异的QoS。

[0090] 图9解说了根据本公开的某些方面的5G架构900的另一参考示例,其中一个或多个网络节点(例如,SEAF、AMF、SMF等)可以是物理分离的。在一些情形中,5G安全性架构可被设计成原生地支持与第三方认证服务器功能(AUSF)(例如,第三方AAA)的辅助认证以用于PDU会话授权。服务认证使得能够建立因服务而异的PDU会话。类似于图8,用户面安全性可以在UPF处终止并且因服务而异的QoS可以得到支持。SMF可以能够直接与第三方AAA对接或经由SEAF与第三方AAA交互。

[0091] 如上所述,由于5G网络可能会继续发展,因此可能期望向UE提供关于特定网络配置、能力、安全性信息等的信息(在本文中统称为网络策略信息)。但是,由于在当前架构中,UE与服务网络之间的唯一控制面接口是N1(其被用于UE与AMF之间的NAS连接),因此可能无法使用当前技术以安全方式向UE提供网络策略信息。

[0092] 例如,参考架构800,由于AMF可能是与UE具有信令连接的唯一实体(例如,基于NAS信令),所以AMF可能会错误地通知UE关于从另一网络节点(例如,SEAF、SMF等)接收到的任何网络安全性策略信息。因此,如果网络策略信息包括AMF和SEAF分离的信息,则当前技术可能无法安全地向UE通知AMF和SEAF是分离的,因为UE可能仅与AMF具有信令连接(例如,与还与SEAF具有信令连接相反)。

[0093] 在这种情形中,独立(流氓)AMF可能会声称它与SEAF共处一地,这是UE无法检测到的场景。这样的独立AMF(流氓)可能会修改网络安全性能力、会话管理NAS保护、因切片而异的安全性能力/要求等,以破坏UE与网络之间的连接/会话。

[0094] 此外,在没有准确的(安全的)网络策略信息的情况下,UE可能会遭受(例如,对PDU会话建立的)降质攻击(bidding down attack)。在降质场景的一个示例中,AMF可能位于与SMF不同的安全性域中。例如,在一种情形中,AMF可以位于服务网络中靠近UE(或RAN)之处(例如,这可能是不太安全的位置),而SMF可以位于网络深处。在一种情形中,AMF可以在服务网络(例如,VPLMN)中,而SMF在家庭网络中。

[0095] 然而,尽管AMF可以位于与SMF不同的安全性域中,但是SMF仍然可以负责授权因切片而异的PDU会话创建(例如,基于不能被AMF访问的因切片而异的订阅信息)。例如,SMF通常是与AMF在逻辑上分离的网络功能,并负责PDU会话授权和管理。如以上所提及的,SMF可以是因切片而异的,并因此可以与UE交换因切片而异的PDU会话参数。

[0096] 然而,由UE请求并由SMF配置的PDU会话参数(诸如授权QoS规则、SSC模式、S-NSSAI、分配的IPv4地址等)不应该被UE和SMF之间的中间节点(例如,包括AMF)修改。相反,此类参数应由SMF使用从SEAF获得的特定密钥进行保护,并可以在UE处通过推导相同的SMF密钥进行验证。因此,在AMF与SEAF分离的情形中,(恶意的或被破坏的)AMF可能修改由UE请求的或由SMF授权的会话信息,例如以使得安全性、QoS或其他分组处理降级。

[0097] 因此,本文呈现的各方面提供了用于安全地向UE通知网络策略信息的技术,例如以最小化降质攻击。特别地,各方面提供了用于将网络策略信息纳入到用于保护UE和AMF之间的NAS连接的密钥(例如,K_{AMF})推导中的技术。如以下所描述的,通过将网络策略信息纳入到密钥推导中,UE可以能够检测从AMF接收到的任何网络策略信息是否已被更改/修改/破坏。

[0098] 注意,尽管本文描述的技术可被用于防止对PDU会话建立的降质攻击,但是本文呈现的各方面也可被用于防止由SEAF和UE之间的(诸)节点进行的UE策略降质。即,如下文描述的,本文呈现的各方面还可被用于例如,通过将UE策略信息纳入到密钥(例如,K_{AMF})推导中来保护UE策略信息(例如,UE安全性特征和/或UE能力,包括网络能力、安全性能力或其任何组合)。UE策略信息可以在注册/附连请求消息中被提供给网络。

[0099] 根据某些方面,K_{AMF}推导可被用于保护在网络中交换的(诸)参数。具体而言,当UE向网络注册时,SEAF可以通过将网络策略信息和/或UE策略信息纳入到密钥(例如,K_{AMF})推导中来向UE通知网络(安全性)策略信息(例如,网络配置、能力、安全性特征等)和/或UE策略信息(例如,由UE接收)。

[0100] 例如,SEAF可以基于网络策略信息、UE策略信息、新鲜度参数或其任何组合来推导AMF密钥(例如K_{AMF}),并将该密钥发送至AMF使得AMF和UE可以建立NAS安全性上下文,并且SEAF还可以向UE通知从UE接收到的UE策略信息。AMF和UE可以从K_{AMF}推导加密和完整性保护

密钥并保护NAS消息(例如,N1接口上的NAS消息)。

[0101] 通过将网络策略信息纳入到K_{AMF}推导中,可以防止AMF执行未经授权的行为(诸如通过修改从SEAF接收到的网络策略信息来使网络特征降质),因为网络策略信息的改变会在UE处导致不同的K_{AMF}推导。类似地,通过将UE策略信息纳入到K_{AMF}推导中,可以防止UE和SEAF之间的网络节点通过修改UE能力来使UE能力降质,因为UE能力的改变也将导致不同的K_{AMF}推导。

[0102] 图10解说了用于无线通信的示例操作1000。根据某些方面,操作1000可以例如由用户装备执行以用于与网络建立安全(例如,NAS)连接。

[0103] 操作1000可以在1002开始,其中UE(例如,从AMF)接收用于与网络建立安全连接的第一消息(例如,安全性模式命令(SMC)消息)。第一消息包括网络策略信息(例如,网络配置、能力、安全性特征等)。在1004,UE部分地基于网络策略信息来生成第一密钥(例如,K_{AMF})。

[0104] 在一些方面,网络策略信息包括关于当与网络建立通信会话时UE是否将从该网络中的SMF接收会话管理令牌的指示。在一些方面,网络策略信息包括关于AMF是否与网络中的SEAF共处一地的指示。在一些方面,网络策略信息包括AMF的安全性级别。在一些方面,网络策略信息包括SEAF的安全性域、AMF的安全性域或其任何组合。在一些方面,网络策略信息可以是响应于从UE发送到网络的UE策略信息而形成的。在一些方面,可以基于发送到网络的UE策略信息来确定第一密钥。

[0105] 在1006,UE使用第一密钥来验证网络策略信息有效。例如,在一些情形中,UE可以部分地基于第一密钥来确定第一消息(包含网络策略信息)是否有效。

[0106] 如以下更详细描述的,在一些情形中,第一消息可以是SMC消息,其由基于第二密钥(例如,从SEAF提供给AMF的K_{AMF})推导出的保护密钥进行完整性保护。UE可以通过基于第一密钥执行对第一消息的完整性验证来确定第一消息(和/或其中包含的网络策略信息)是否有效。在一个方面,如果对第一消息的完整性验证是正确的,则UE可以确定第一消息有效。

[0107] 如果UE确定第一密钥与第二密钥相同,则UE可以确定对第一消息的完整性验证是正确的。UE可以基于确定第一密钥与第二密钥相同来确定网络策略信息有效。同样,如果对第一消息的完整性验证是不正确的,则UE可以确定第一消息无效。如果第一密钥与第二密钥不同,则UE可以确定对第一消息的完整性验证是不正确的。UE可以基于确定第一密钥与第二密钥不同来确定网络策略信息无效。

[0108] 图11解说了用于无线通信的示例操作1100。根据某些方面,操作1100可以例如由网络节点(例如,SEAF)执行,以向UE安全地提供网络策略信息。

[0109] 操作1100可以在1102开始,其中网络节点至少部分地基于网络策略信息来为另一网络节点(例如,AMF)生成密钥(例如,K_{AMF})。如上所述,网络策略信息可以包括关于另一网络节点(例如,AMF)是否与该网络节点共处一地的指示。在一些情形中,网络策略信息可以包括以下至少一项:该网络节点的安全性级别,或关于网络中的SMF是否要为UE和网络之间的通信会话生成SM令牌并将该SM令牌发送给UE的指示。该密钥被用于建立UE和网络节点之间的安全连接。

[0110] 在一些方面,网络节点可以接收包括UE策略(或能力)信息的注册消息/附连请求

消息。网络节点可以将接收到的UE策略信息纳入到针对另一网络节点的密钥(例如,K_{AMF})推导中。例如,在图11的1102处,网络节点可以部分地基于网络策略信息、新鲜度参数、UE策略信息或其任何组合为另一网络节点(例如AMF)生成密钥(例如K_{AMF})。

[0111] 在1104,该网络节点向该另一网络节点发送该密钥。在一些方面,该网络节点可以进一步向网络节点发送网络策略信息或网络策略信息有效的时间量中的至少一者。

[0112] 图12是解说根据本公开的某些方面的允许SEAF安全地向UE通知网络(安全性)策略信息和/或UE策略信息的示例注册规程(例如,通过将策略信息和/或UE策略信息纳入到密钥推导中)的呼叫流程图。

[0113] 在一些方面,如图所示,UE可以最初向网络(例如,AMF、SEAF等)发送注册请求/附连请求。注册请求/附连请求包括UE策略(能力)。然后,在步骤1,UE与网络执行认证/注册规程。UE和SEAF可以基于新的认证或基于先前的认证来建立共享锚密钥(K_{SEAF})。在注册期间,AMF可从SEAF请求密钥(K_{AMF})。

[0114] 在步骤2,SEAF为AMF生成(例如,推导)用于将UE注册到网络的K_{AMF}。K_{AMF}推导纳入了网络策略信息(例如,网络配置、能力、安全性特征等)和/或UE策略信息。在一方面,网络策略信息可以包括AMF类型,例如,共处一地的AMF/SEAF、独立的AMF等。

[0115] 例如,网络策略信息可以包括一个或多个SEAF/AMF分离比特。如果请求K_{AMF}的AMF是与SEAF分离的独立AMF,则SEAF可以将SEAF/AMF分离比特设置为第一值(例如1)。如果请求K_{AMF}的AMF是共处一地的AMF/SEAF,则SEAF可以将SEAF/AMF分离比特设置为不同的第二值(例如0)。在一方面,K_{AMF}推导还可以纳入用于防止重放攻击(replay attack)的一个或多个新鲜度参数。这样的新鲜度参数的示例可以包括计数器(在UE和SEAF处都维护)、在UE和SEAF之间交换的随机值、或其任何组合。在一方面,SEAF可以使用以下公式(1)来生成(推导)K_{AMF}:

[0116] K_{AMF}=KDF(K_{SEAF},新鲜度参数,网络策略信息,UE策略)

[0117] (1)

[0118] 其中KDF是密钥推导函数(例如,HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-512、PRF-X(输出大小为X的伪随机函数)),K_{SEAF}是服务网络中(并保存在SEAF处)的锚保护密钥,新鲜度参数是用于防止重放攻击的计数器、随机值,网络策略信息包括网络配置、能力、安全性特征等,并且UE策略包括UE能力信息和/或UE安全性信息中的至少一者。

[0119] 在步骤3,SEAF向AMF提供K_{AMF}、新鲜度参数和网络策略信息。在一些方面,SEAF还可以在步骤3向AMF提供(例如,重复)UE策略。在步骤4,AMF向UE发送NAS安全性模式命令(SMC)。在一些方面,AMF还可以在步骤4向UE提供(例如,重复)UE策略。NAS SMC可以包括从SEAF获得的新鲜度参数和网络策略信息,并且NAS SMC可以基于K_{AMF}进行完整性保护。例如,一旦从SEAF接收到K_{AMF},则AMF就可以基于K_AMF推导NAS完整性保护密钥(例如,K_{NASINT}),并使用K_{NASINT}对NAS SMC消息进行完整性保护。

[0120] 在步骤5,UE使用K_{SEAF}以及NAS SMC消息中的信息(例如,新鲜度参数、网络策略信息等)来生成(例如,推导)K_{AMF},并验证NAS SMC消息。即,UE可以检测是否存在(例如,由AMF进行的)对网络策略信息的任何改变,因为网络策略信息的任何改变将在UE处导致不同的K_{AMF}推导。当UE通过将UE生成的K_{AMF}与使用K_{AMF}对NAS SMC进行的完整性保护进行比较来检查对NAS SMC的完整性保护时,UE可以检测到这种改变。因此,确定对SMC的完整性验证是正确

的意味着由UE生成的K_{AMF}与(从SEAF)提供给AMF的K_{AMF}相同,这进而意味着(从AMF)提供给UE的网络策略信息有效。

[0121] 假设对SMC的验证是正确的,则UE(在步骤6)向AMF发送NAS安全性模式完成消息。在一些方面,UE还可以检测(提供给网络的)UE策略信息是否被任何中间网络节点修改。即,在一些方面,UE可以基于UE策略信息(例如,作为网络策略信息的补充或替换)生成K_{AMF},以确定UE策略信息是否已被修改(例如,基于由UE生成的K_{AMF}和(从SEAF)提供给AMF的K_{AMF}是否相同)。

[0122] 注意,尽管图12中的呼叫流描述了将网络策略信息纳入到密钥推导中以安全地向UE通知网络策略信息,但是本文给出的技术也可被用于保护UE安全性特征。即,作为网络策略信息的补充或替换,密钥(K_{AMF})推导可以纳入UE能力(包括UE安全性特征),其中UE能力在注册/附连请求消息中被提供给网络。

[0123] 图10-12中描述的技术可被用于通过限制密钥推导中的密钥使用来防止AMF修改其中继给UE的任何网络能力参数。然而,尽管这些技术对于防止网络能力降质可能是有用的,但是这种技术可能不足以防止PDU会话参数降质(例如,SM NAS令牌)。

[0124] 因此,本文给出的各方面提供了可被用于防止(例如,对PDU会话建立和/或网络能力参数的)降质攻击的技术。

[0125] 更具体地,当UE向网络注册时,SEAF将网络策略信息(例如,网络配置、(安全性)能力等)和受完整性保护的网络策略信息(例如,网络策略令牌)连同K_{AMF}一起提供给AMF。网络策略信息使用K_{SEAF}进行完整性保护。网络策略令牌被捎带在NAS安全性模式命令上并提供给UE。网络策略令牌防止位于SEAF和UE之间的任何网络功能修改网络能力。

[0126] 图13解说了用于无线通信的示例操作1300。根据某些方面,操作1300可以例如由用户装备执行以用于与网络建立安全(例如,NAS)连接。

[0127] 操作1300可以在1302开始,其中UE基于与网络的认证规程,建立在该UE与网络中的SEAF之间共享的锚密钥(例如,K_{SEAF})。在1304,UE接收用于与网络建立安全连接的第一消息(例如,SMC消息)。第一消息包括用于与网络进行通信会话的网络策略令牌、网络策略信息、网络策略信息有效的第一时间量、和用于该安全连接的第一密钥有效的第二时间量。网络策略令牌包括与网络策略信息相关联的完整性保护信息。

[0128] 在1306,UE在与网络建立安全连接之前,基于从共享锚密钥、网络策略信息、第一时间量和第二时间量推导出的密钥来确定网络策略令牌是否有效。在一些方面,确定网络策略令牌是否有效包括基于从共享锚密钥推导出的密钥来验证完整性保护信息。在一些方面,UE可以向网络发送UE策略信息(例如,UE能力信息、UE安全性信息等)。UE可以基于发送到网络的UE策略信息来生成密钥。在一些情形中,网络策略信息可以是基于UE策略信息的。

[0129] 图14解说了用于无线通信的示例操作1400。根据某些方面,操作1400可以例如由网络节点(例如,SEAF)执行,以向UE安全地提供网络策略信息。

[0130] 操作1400可以在1402开始,其中网络节点基于与UE的认证规程,建立在该网络节点与网络中的UE之间共享的锚密钥(例如,K_{SEAF})。在1404,网络节点部分地基于锚密钥、网络策略信息和网络策略令牌有效的第一时间量来生成网络策略令牌(例如,$K_{令牌}$)。网络策略令牌包括与网络策略信息相关联的完整性保护信息。在1406,该网络节点为另一网络节点(例如,AMF)生成密钥(例如,K_{AMF})。在1408,该网络节点向该另一网络节点发送该密钥、网络

策略信息和网络策略令牌。

[0131] 在一些方面，如以上描述的，网络节点可以将UE策略信息纳入到密钥(例如，K_{AMF})推导中，例如，以防止中间节点修改从UE接收的UE策略信息。如上所述，网络节点可以经由注册/附连请求消息来接收UE策略信息。

[0132] 图15是解说根据本公开的某些方面的允许SEAF防止对PDU会话建立进行降质攻击的示例注册规程的呼叫流图。

[0133] 如图所示，在步骤1，UE与网络执行注册规程。UE和SEAF可以基于新的认证或基于先前的认证来建立共享锚密钥(K_{SEAF})。在注册期间，AMF可从SEAF请求密钥(K_{AMF})。尽管未示出，但是在一些情形中，UE可以经由注册/附连请求消息向网络提供UE策略信息(例如，UE能力信息、UE安全性信息等)。

[0134] 在步骤2，SEAF为AMF生成用于将UE注册到网络的K_{AMF}。SEAF可以使用K_{SEAF}和一个或多个第一新鲜度参数来生成K_{AMF}。另外，SEAF使用K_{SEAF}、(例如，用于防止重放攻击的)一个或多个第二新鲜度参数以及网络策略信息来生成网络策略令牌。如上所述，网络策略令牌是网络策略信息的消息认证码(或完整性保护信息)。与图12类似，网络策略信息可以包括一个或多个SEAF/AMF分离比特。在一些方面，SEAF可以进一步基于UE策略信息来生成K_{AMF}。

[0135] 在步骤3，SEAF向AMF提供K_{AMF}、第一和第二新鲜度参数、网络策略令牌和网络策略信息。在步骤4，AMF向UE发送NAS安全性模式命令。NAS安全性模式命令包括从SEAF获得的网络策略信息、第一和第二新鲜度参数以及网络策略令牌。

[0136] 在步骤5，UE使用K_{SEAF}对网络策略令牌执行验证规程。如果验证成功，则UE使用K_{SEAF}推导K_{AMF}，并使用所推导出的K_{AMF}对NAS安全性模式命令执行验证规程。假设NAS安全性模式命令得到验证，则UE(在步骤6)向AMF发送NAS安全性模式完成消息。以这种方式，SEAF可以用安全方式直接向UE指示网络能力(因为令牌是基于UE和SEAF之间的密钥来生成和验证的)。

[0137] 注意，在一些方面，(与图12中的SEAF相比)(图15的)SEAF可能必须维护UE的附加状态(例如，新鲜度参数)以用于防止重放攻击的网络策略生成。这可以类似于维护UE与SEAF之间的连接状态，该连接可能易于失去同步。进一步，注意，与图13-15所描述的技术相似的技术也可被用于防护对UE策略信息(包括UE安全性信息和/或UE能力信息)的降质攻击。

[0138] 本文中所公开的方法包括用于实现所描述的方法的一个或多个步骤或动作。这些方法步骤和/或动作可以彼此互换而不会脱离权利要求的范围。换言之，除非指定了步骤或动作的特定次序，否则具体步骤和/或动作的次序和/或使用可以改动而不会脱离权利要求的范围。

[0139] 如本文中所使用的，引述一列项目“中的至少一者”的短语是指这些项目的任何组合，包括单个成员。作为示例，“a、b或c中的至少一者”旨在涵盖：a、b、c、a-b、a-c、b-c和a-b-c，以及具有多个相同元素的任何组合(例如，a-a、a-a-a、a-a-b、a-a-c、a-b-b、a-c-c、b-b、b-b-b、b-b-c、c-c、和c-c-c，或者a、b和c的任何其他排序)。

[0140] 如本文中所使用的，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、数据库或另一数据结构中查找)、查明及诸如此类。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)及诸如此

类。“确定”还可以包括解析、选择、选取、确立及诸如此类。

[0141] 在一些情形中，设备可以并非实际上传送帧，而是可具有用于输出帧以供传输的接口。例如，处理器可经由总线接口向RF前端输出帧以供传输。类似地，设备并非实际上接收帧，而是可具有用于获得从另一设备接收的帧的接口。例如，处理器可经由总线接口从RF前端获得(或接收)帧以供传输。

[0142] 以上所描述的方法的各种操作可由能够执行相应功能的任何合适的装置来执行。这些装置可包括各种硬件和/或软件组件和/或模块，包括但不限于电路、专用集成电路(ASIC)、或处理器。一般地，在存在附图中解说的操作的场合，这些操作可具有带相似编号的相应配对装置加功能组件。

[0143] 例如，用于传送的装置、用于接收的装置、用于确定的装置、用于执行的装置、用于参与的装置、用于指示的装置、用于建立的装置、用于验证的装置、用于发送的装置、用于通信的装置、用于存储的装置、用于进入的装置、用于保护的装置、用于防止的装置、用于退出的装置、用于生成的装置、用于转发的装置和/或用于提供的装置可以包括BS 110或UE 120处的一个或多个处理器或天线，诸如BS 110处的发射处理器420、控制器/处理器440、接收处理器438、或天线434、和/或UE 120处的发射处理器464、控制器/处理器480、接收处理器458、或天线452。

[0144] 结合本公开所描述的各种解说性逻辑块、模块、以及电路可用设计成执行本文所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑器件(PLD)、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合来实现或执行。通用处理器可以是微处理器，但在替换方案中，处理器可以是任何市售的处理器、控制器、微控制器、或状态机。处理器还可以被实现为计算设备的组合，例如，DSP与微处理器的组合、多个微处理器、与DSP核心协同的一个或多个微处理器、或任何其他此类配置。

[0145] 如果以硬件实现，则示例硬件配置可包括无线节点中的处理系统。处理系统可以用总线架构来实现。取决于处理系统的具体应用和整体设计约束，总线可包括任何数目的互连总线和桥接器。总线可将包括处理器、机器可读介质、以及总线接口的各种电路链接在一起。总线接口可被用于将网络适配器等经由总线连接至处理系统。网络适配器可被用于实现PHY层的信号处理功能。在用户终端120(参见图1)的情形中，用户接口(例如，按键板、显示器、鼠标、操纵杆，等等)也可以被连接到总线。总线还可以链接各种其他电路，诸如定时源、外围设备、稳压器、功率管理电路以及类似电路，它们在本领域中是众所周知的，因此将不再进一步描述。处理器可用一个或多个通用和/或专用处理器来实现。示例包括微处理器、微控制器、DSP处理器、以及其他能执行软件的电路系统。取决于具体应用和加诸于整体系统上的总设计约束，本领域技术人员将认识到如何最佳地实现关于处理系统所描述的功能性。

[0146] 如果以软件实现，则各功能可作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。软件应当被宽泛地解释成表示指令、数据、或其任何组合，无论是被称作软件、固件、中间件、微代码、硬件描述语言、或其他。计算机可读介质包括计算机存储介质和通信介质两者，这些介质包括促成计算机程序从一地向另一地转移的任何介质。处理器可负责管理总线和一般处理，包括执行存储在机器可读存储介质上的软件模块。计算机

可读存储介质可被耦合到处理器以使得该处理器能从/向该存储介质读写信息。替换地，存储介质可被整合到处理器。作为示例，机器可读介质可包括传输线、由数据调制的载波、和/或与无线节点分开的其上存储有指令的计算机可读存储介质，其全部可由处理器通过总线接口来访问。替换地或补充地，机器可读介质或其任何部分可被集成到处理器中，诸如高速缓存和/或通用寄存器文件可能就是这种情形。作为示例，机器可读存储介质的示例可包括RAM(随机存取存储器)、闪存、ROM(只读存储器)、PROM(可编程只读存储器)、EPROM(可擦式可编程只读存储器)、EEPROM(电可擦式可编程只读存储器)、寄存器、磁盘、光盘、硬驱动器、或者任何其他合适的存储介质、或其任何组合。机器可读介质可被实施在计算机程序产品中。

[0147] 软件模块可包括单条指令、或许多条指令，且可分布在若干不同的代码段上，分布在不同的程序间以及跨多个存储介质分布。计算机可读介质可包括数个软件模块。这些软件模块包括当由装置(诸如处理器)执行时使处理系统执行各种功能的指令。这些软件模块可包括传送模块和接收模块。每个软件模块可以驻留在单个存储设备中或者跨多个存储设备分布。作为示例，当触发事件发生时，可以从硬驱动器中将软件模块加载到RAM中。在软件模块执行期间，处理器可以将一些指令加载到高速缓存中以提高访问速度。可随后将一个或多个高速缓存行加载到通用寄存器文件中以供处理器执行。在以下述及软件模块的功能性时，将理解此类功能性是在处理器执行来自该软件模块的指令时由该处理器来实现的。

[0148] 任何连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)、或无线技术(诸如红外(IR)、无线电、以及微波)从web网站、服务器、或其他远程源传送而来，则该同轴电缆、光纤电缆、双绞线、DSL或无线技术(诸如红外、无线电、以及微波)就被包括在介质的定义之中。如本文中所使用的盘(disk)和碟(disc)包括压缩碟(CD)、激光碟、光碟、数字多用碟(DVD)、软盘、和蓝光®碟，其中盘(disk)常常磁性地再现数据，而碟(disc)用激光来光学地再现数据。因此，在一些方面，计算机可读介质可包括非瞬态计算机可读介质(例如，有形介质)。另外，对于其他方面，计算机可读介质可包括瞬态计算机可读介质(例如，信号)。以上的组合应当也被包括在计算机可读介质的范围内。

[0149] 此外，应当领会，用于执行本文中所描述的方法和技术的模块和/或其他恰适装置可由用户终端和/或基站在适用的场合下载和/或以其他方式获得。例如，此类设备能被耦合到服务器以促成用于执行本文中所描述的方法的装置的转移。替换地，本文中所描述的各种方法能经由存储装置(例如，RAM、ROM、诸如压缩碟(CD)或软盘之类的物理存储介质等)来提供，以使得一旦将该存储装置耦合到或提供给用户终端和/或基站，该设备就能获得各种方法。此外，可利用适于向设备提供本文中所描述的方法和技术的任何其他合适的技术。

[0150] 将理解，权利要求并不被限于以上所解说的精确配置和组件。可在以上所描述的方法和装置的布局、操作和细节上作出各种改动、更换和变形而不会脱离权利要求的范围。

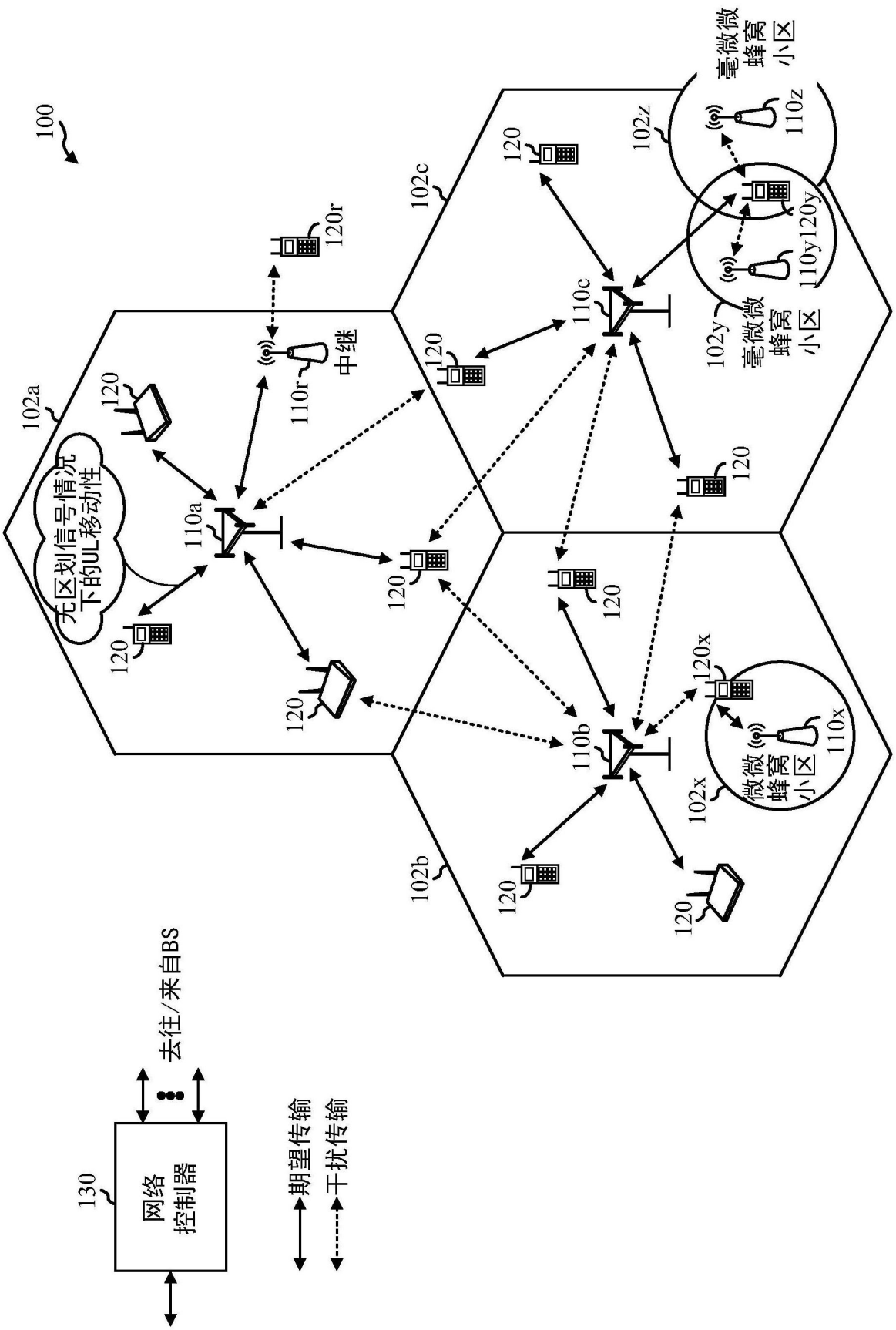

100
102a
102b
102c
102x
102y
102z
110a
110b
110c
110r
110x
110y
110z
120
120r
120x
120y
中继
无区划信号情况下的UL移动性
毫微微蜂窝小区
微微蜂窝小区
130
网络控制器
去往/来自BS
期望传输
干扰传输

图1

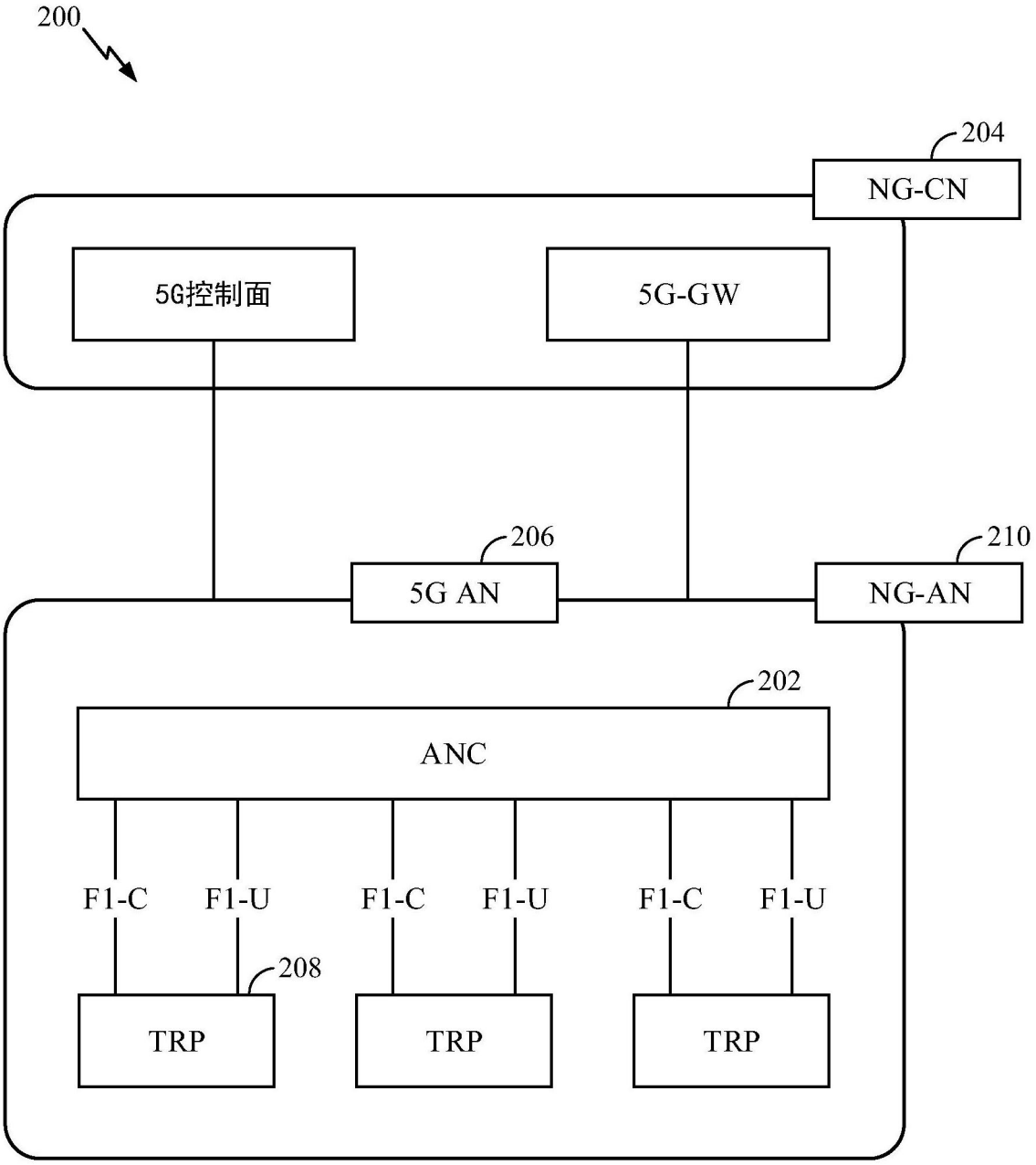

200
204
NG-CN
5G控制面
5G-GW
206
5G AN
210
NG-AN
202
ANC
F1-C
F1-U
F1-C
F1-U
F1-C
F1-U
208
TRP
TRP
TRP

图2

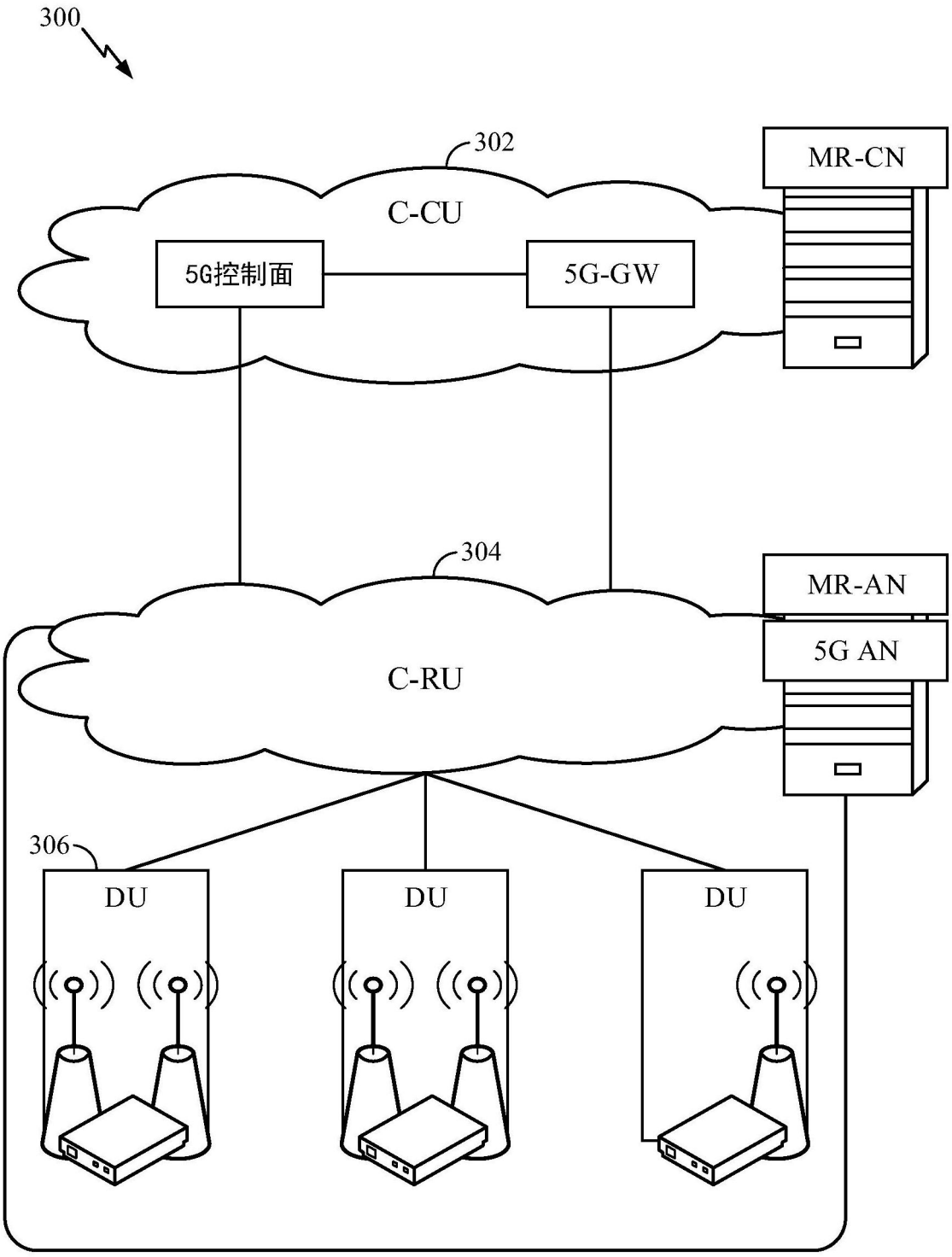


图3

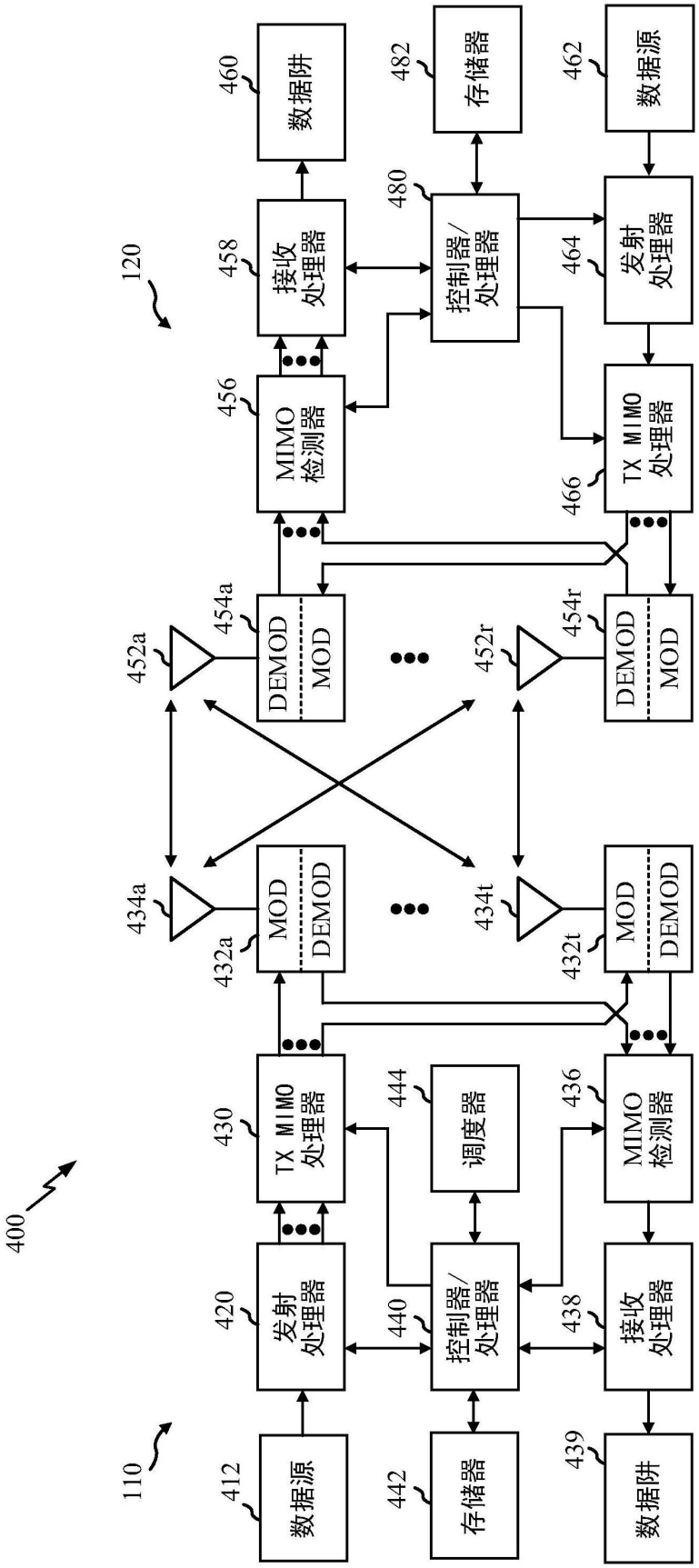

400
110
120
412 数据源
420 发射处理器
430 TX MIMO处理器
432a MOD/DEMOD
434a
452a
454a DEMOD/MOD
456 MIMO检测器
458 接收处理器
460 数据阱
440 控制器/处理器
442 存储器
444 调度器
480 控制器/处理器
482 存储器
434t
452r
454r DEMOD/MOD
432t MOD/DEMOD
436 MIMO检测器
438 接收处理器
439 数据阱
462 数据源
464 发射处理器
466 TX MIMO处理器

图4

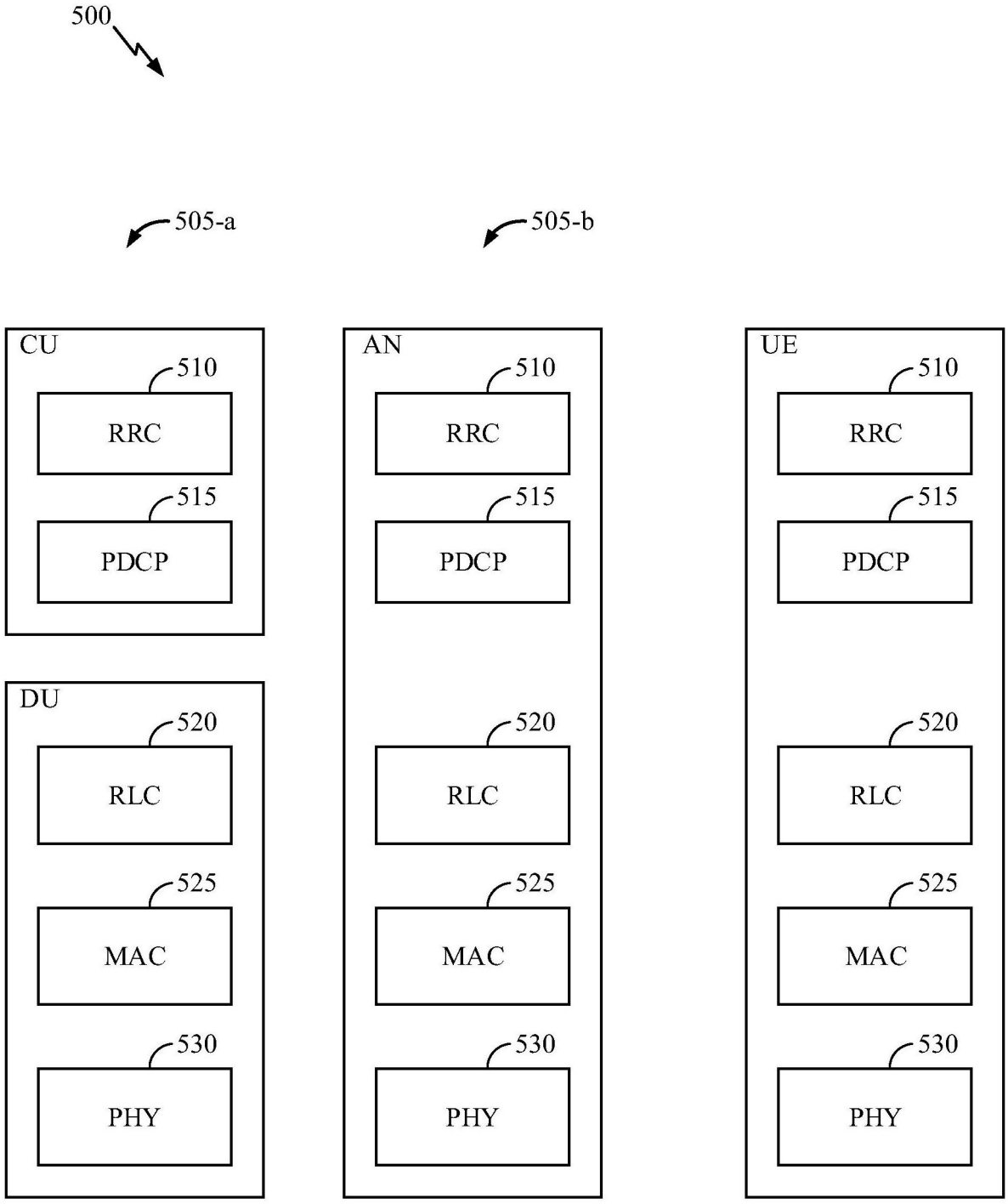

500
505-a
505-b
CU
510
RRC
515
PDCP
DU
520
RLC
525
MAC
530
PHY
AN
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY
UE
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY

图5

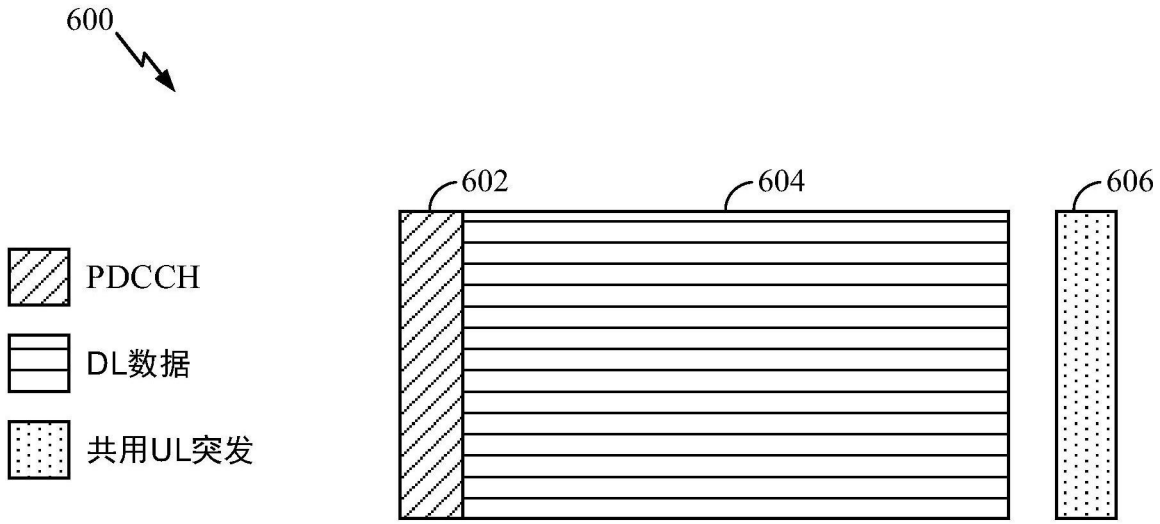

600
602
604
606
PDCCH
DL数据
共用UL突发

图6

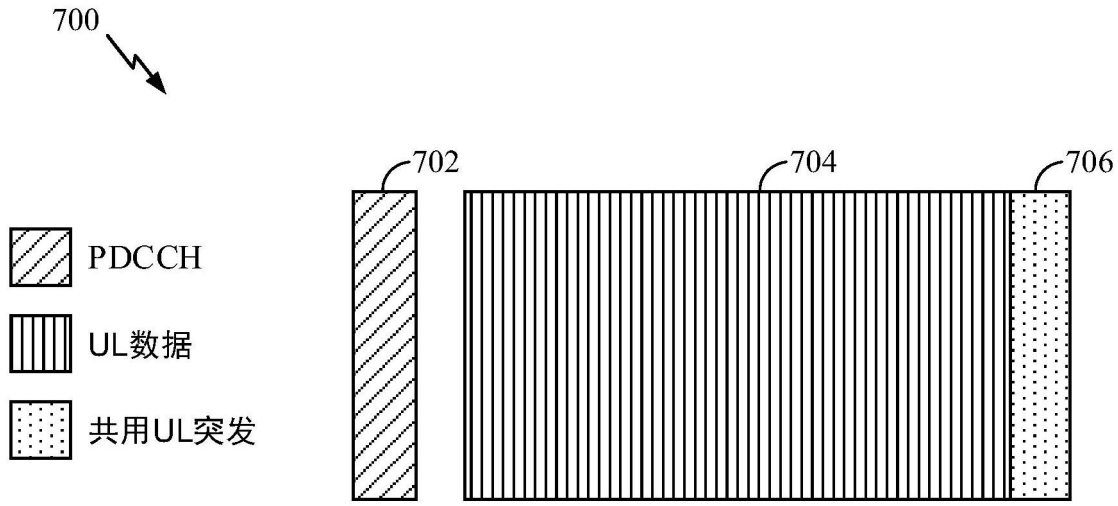

700
702
704
706
PDCCH
UL数据
共用UL突发

图7

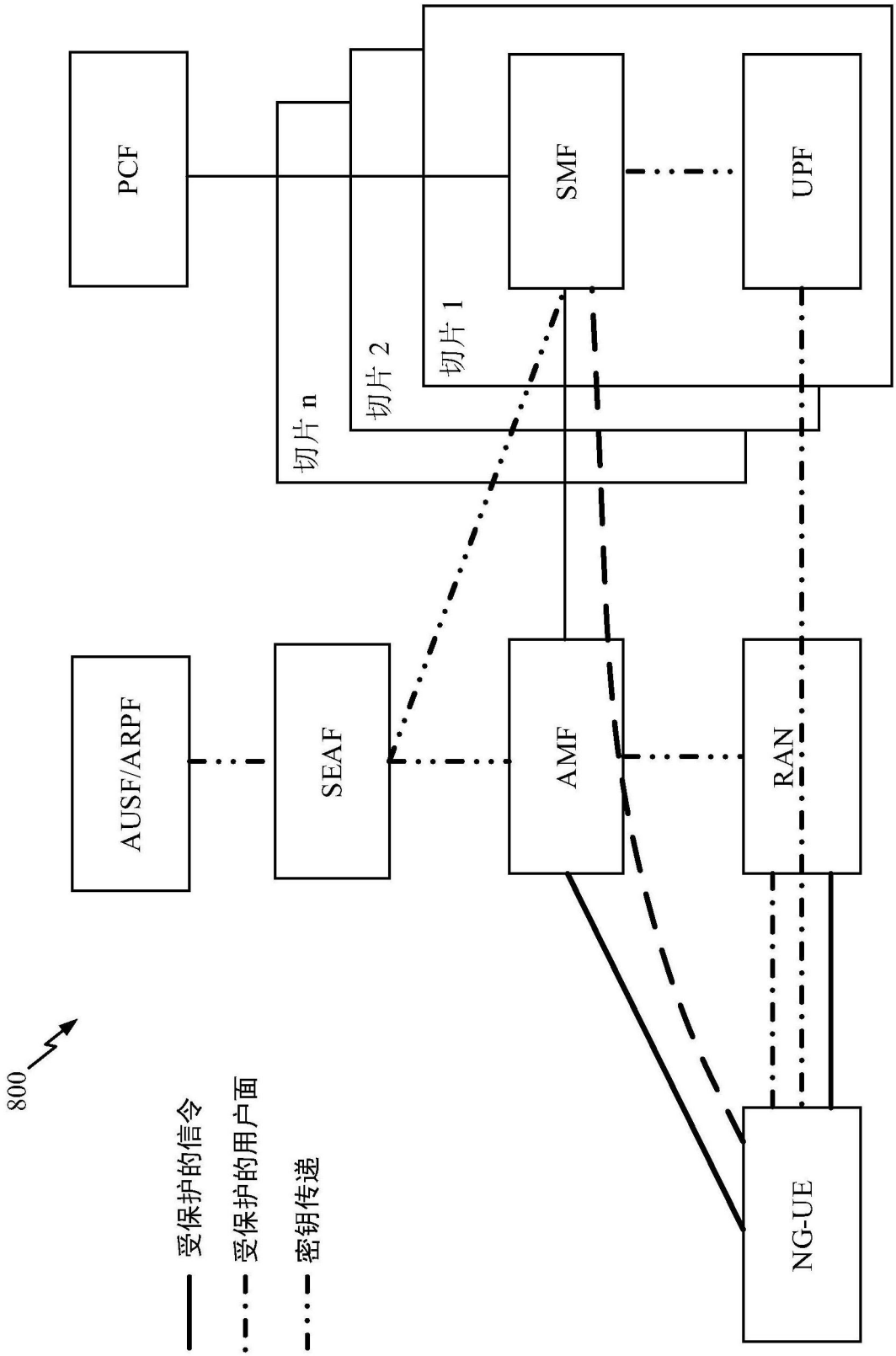

PCF
SMF
UPF
切片 1
切片 2
切片 n
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
800
受保护的信令
受保护的用户面
密钥传递

图8

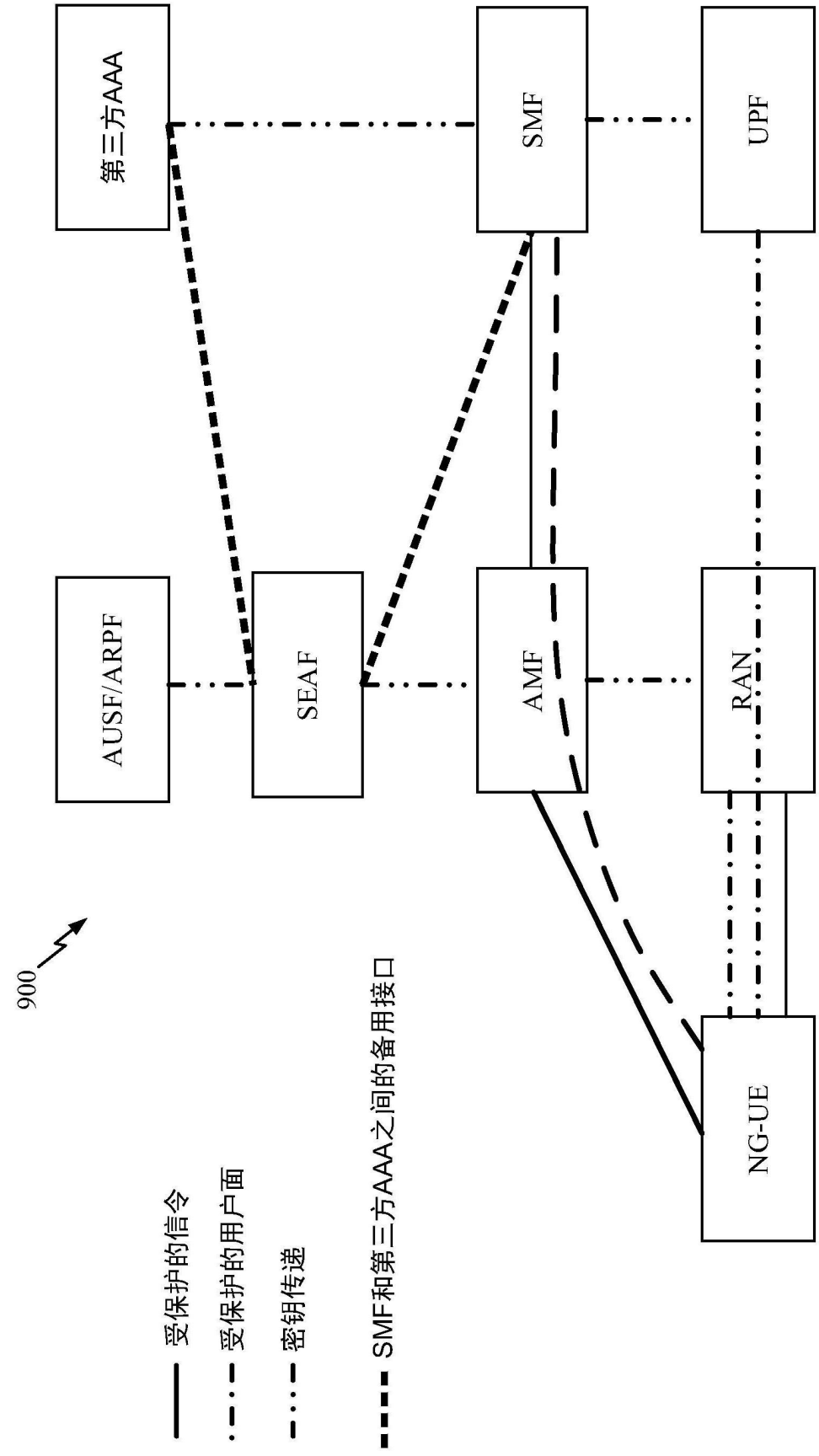

第三方AAA
SMF
UPF
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
900
受保护的信令
受保护的用户面
密钥传递
SMF和第三方AAA之间的备用接口

图9

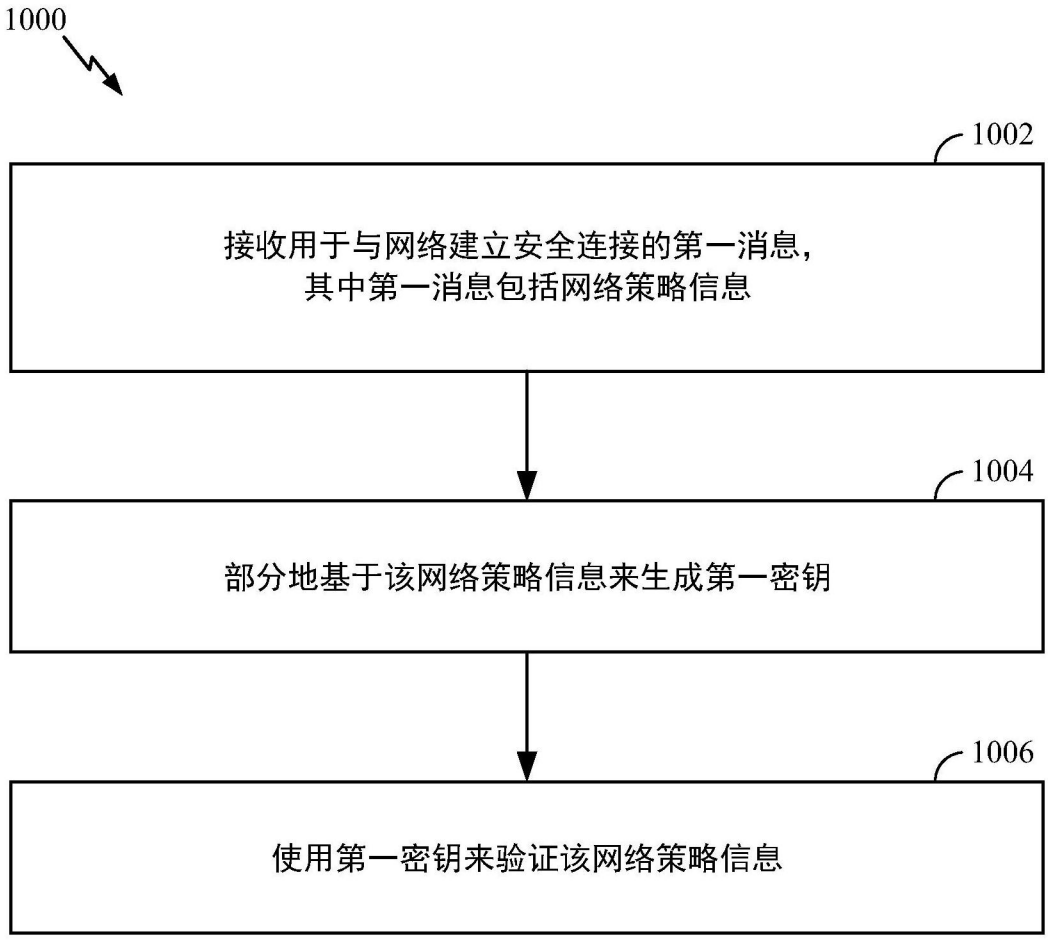

1000
1002
接收用于与网络建立安全连接的第一消息，
其中第一消息包括网络策略信息
1004
部分地基于该网络策略信息来生成第一密钥
1006
使用第一密钥来验证该网络策略信息

图10

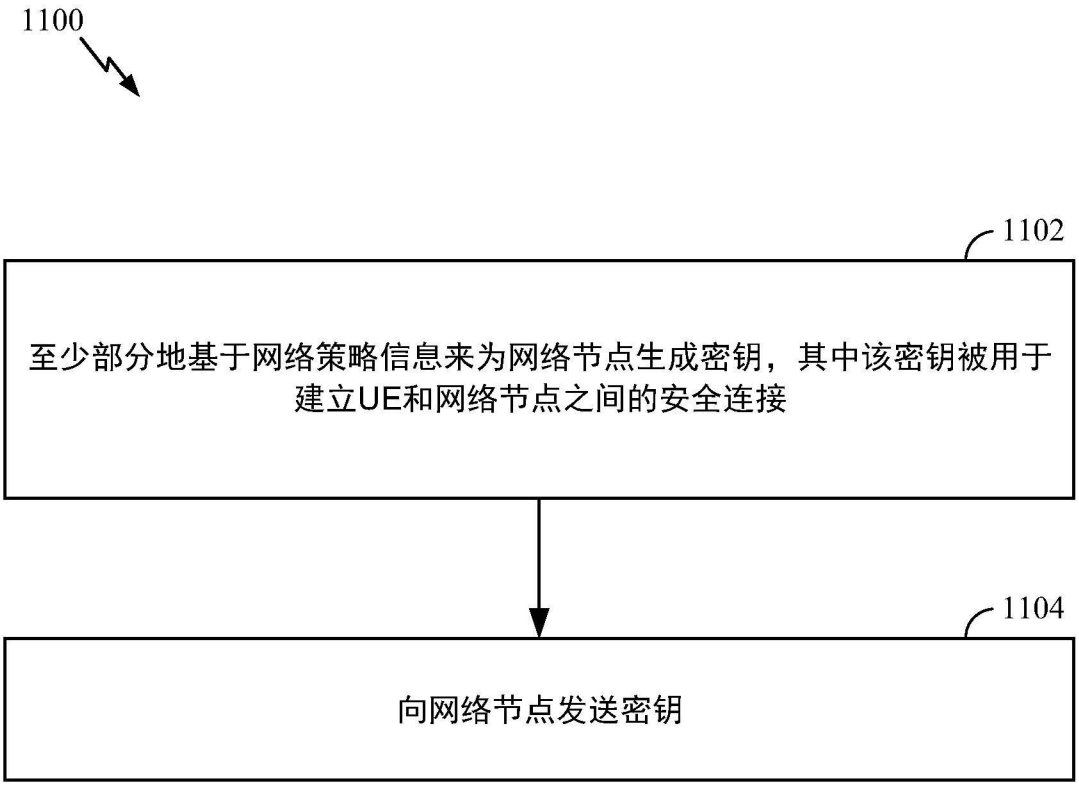

1100
1102
至少部分地基于网络策略信息来为网络节点生成密钥，其中该密钥被用于建立UE和网络节点之间的安全连接
1104
向网络节点发送密钥

图11

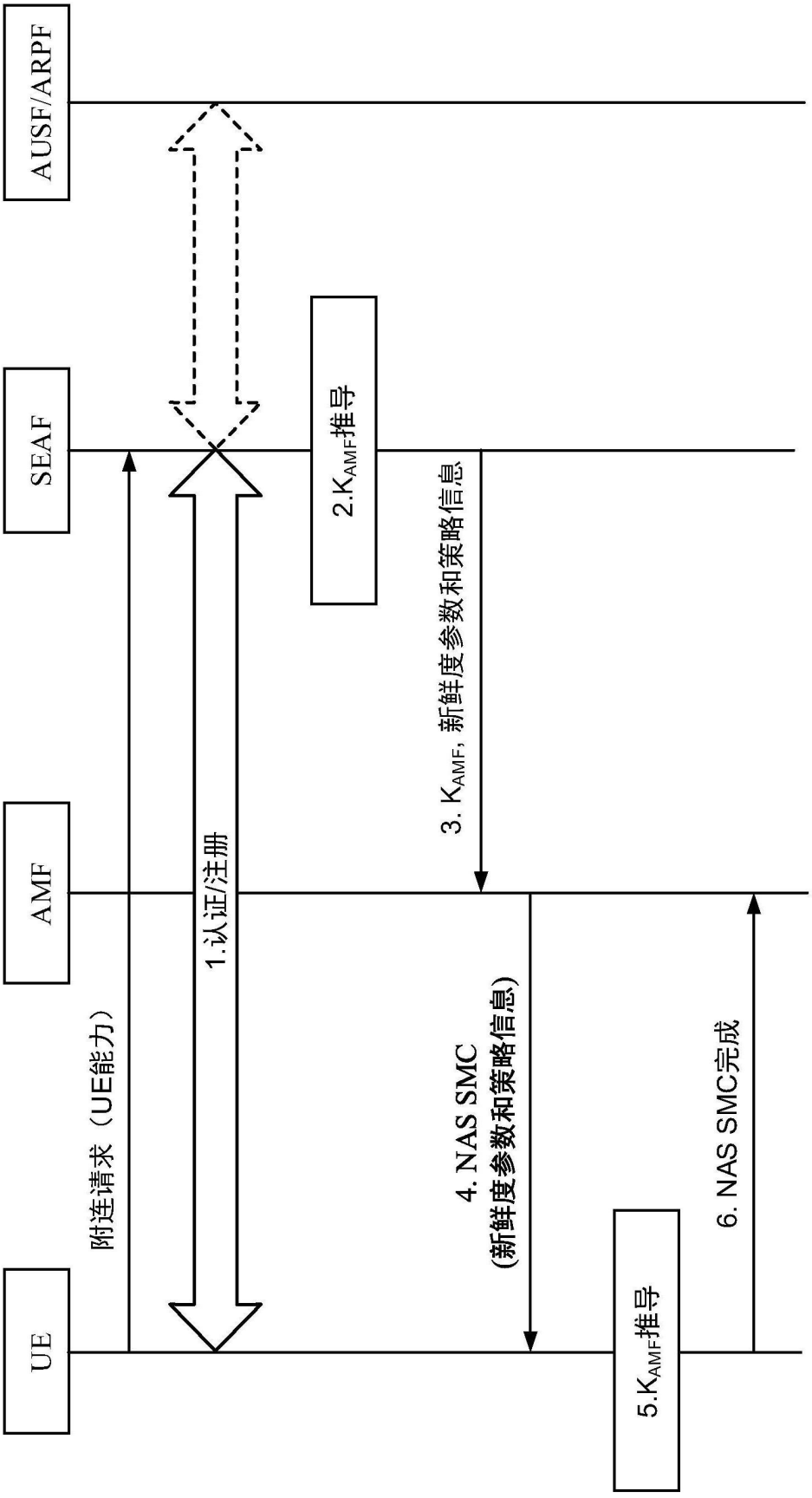

AUSF/ARPF
SEAF
AMF
UE
1.认证/注册
2.K_{AMF}推导
3. K_{AMF}, 新鲜度参数和策略信息
4. NAS SMC
(新鲜度参数和策略信息)
5.K_{AMF}推导
6. NAS SMC完成
附连请求（UE能力）

图12

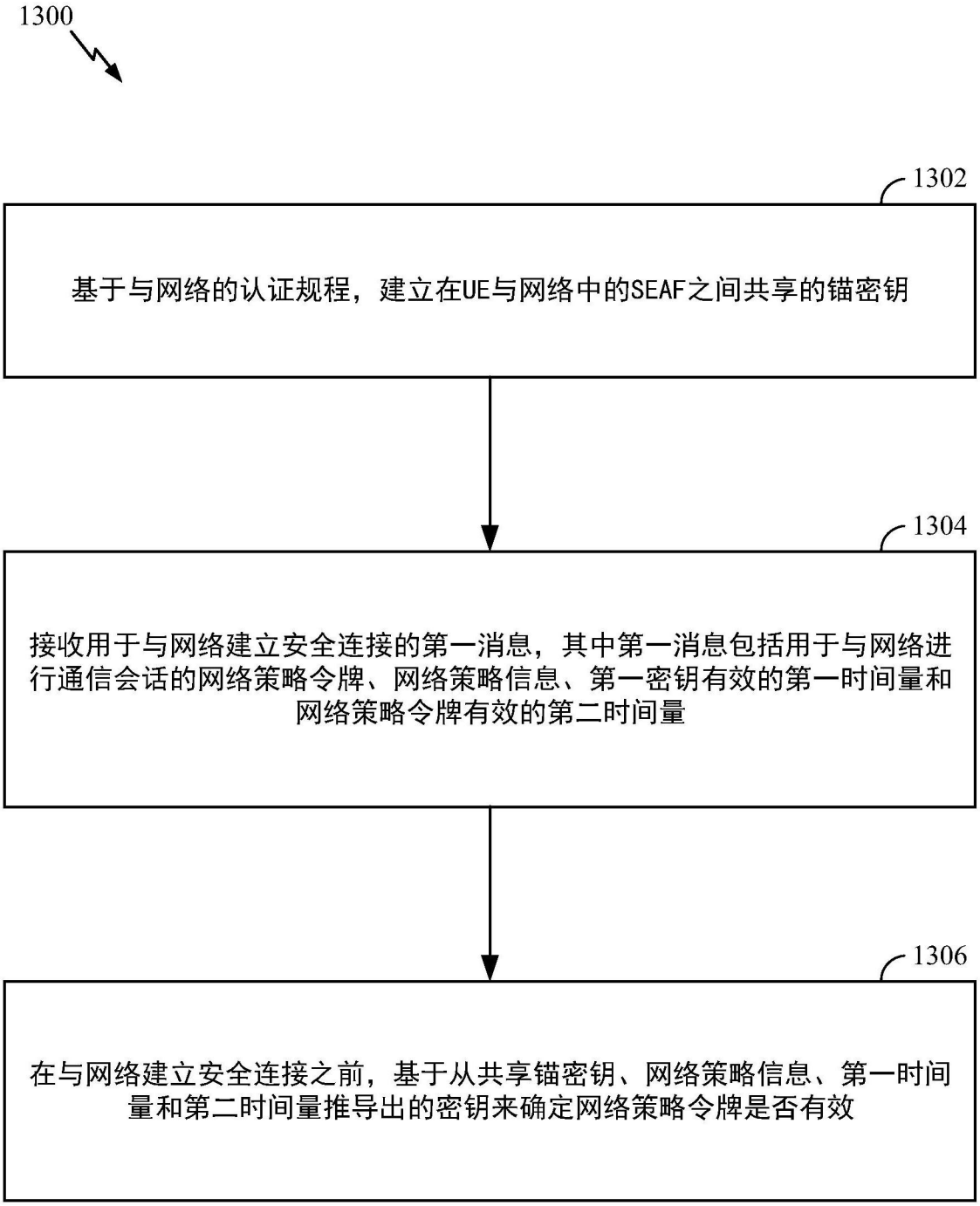

1300
1302
基于与网络的认证规程，建立在UE与网络中的SEAF之间共享的锚密钥
1304
接收用于与网络建立安全连接的第一消息，其中第一消息包括用于与网络进行通信会话的网络策略令牌、网络策略信息、第一密钥有效的第一时间量和网络策略令牌有效的第二时间量
1306
在与网络建立安全连接之前，基于从共享锚密钥、网络策略信息、第一时间量和第二时间量推导出的密钥来确定网络策略令牌是否有效

图13

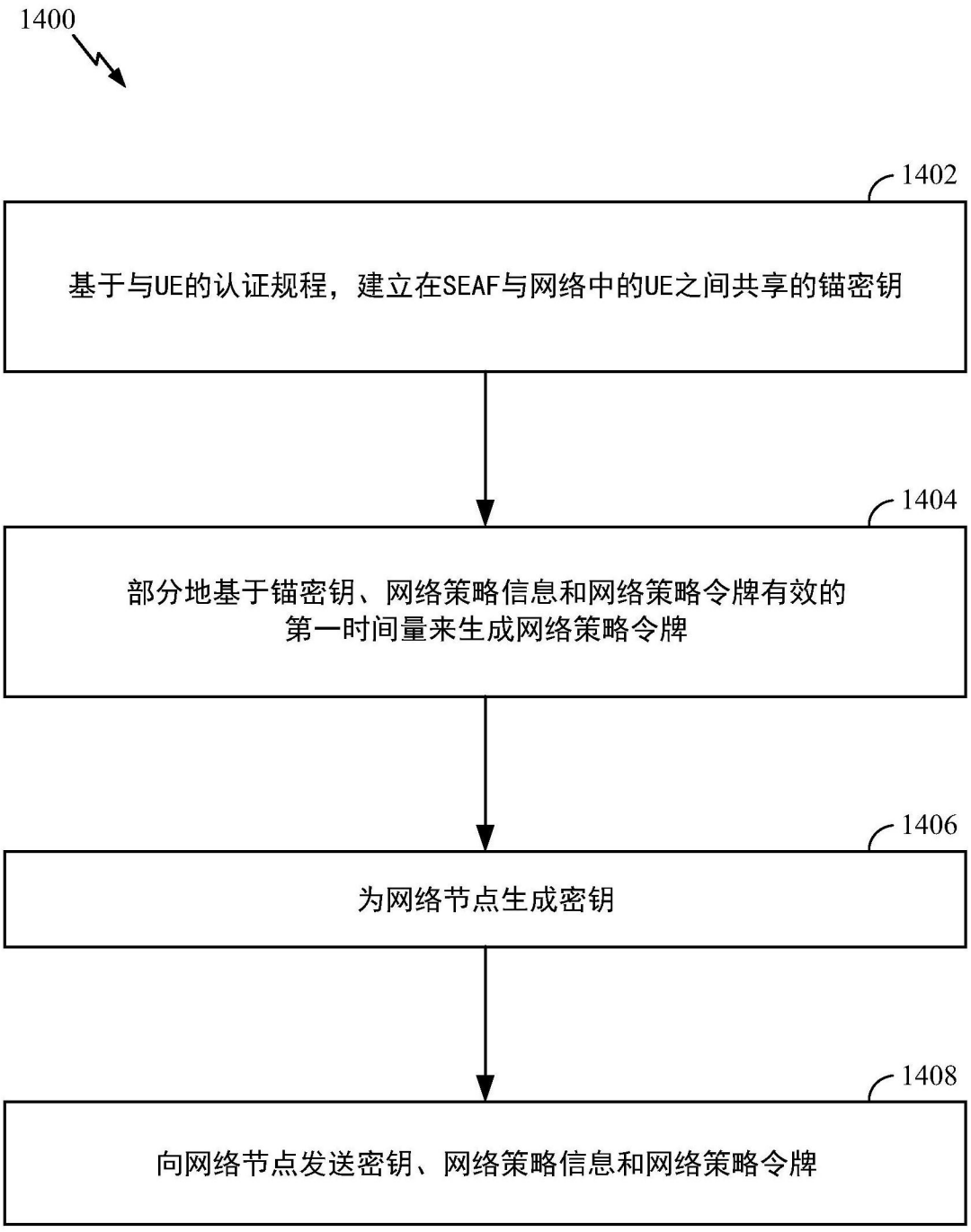

1400
1402
基于与UE的认证规程，建立在SEAF与网络中的UE之间共享的锚密钥
1404
部分地基于锚密钥、网络策略信息和网络策略令牌有效的
第一时间量来生成网络策略令牌
1406
为网络节点生成密钥
1408
向网络节点发送密钥、网络策略信息和网络策略令牌

图14

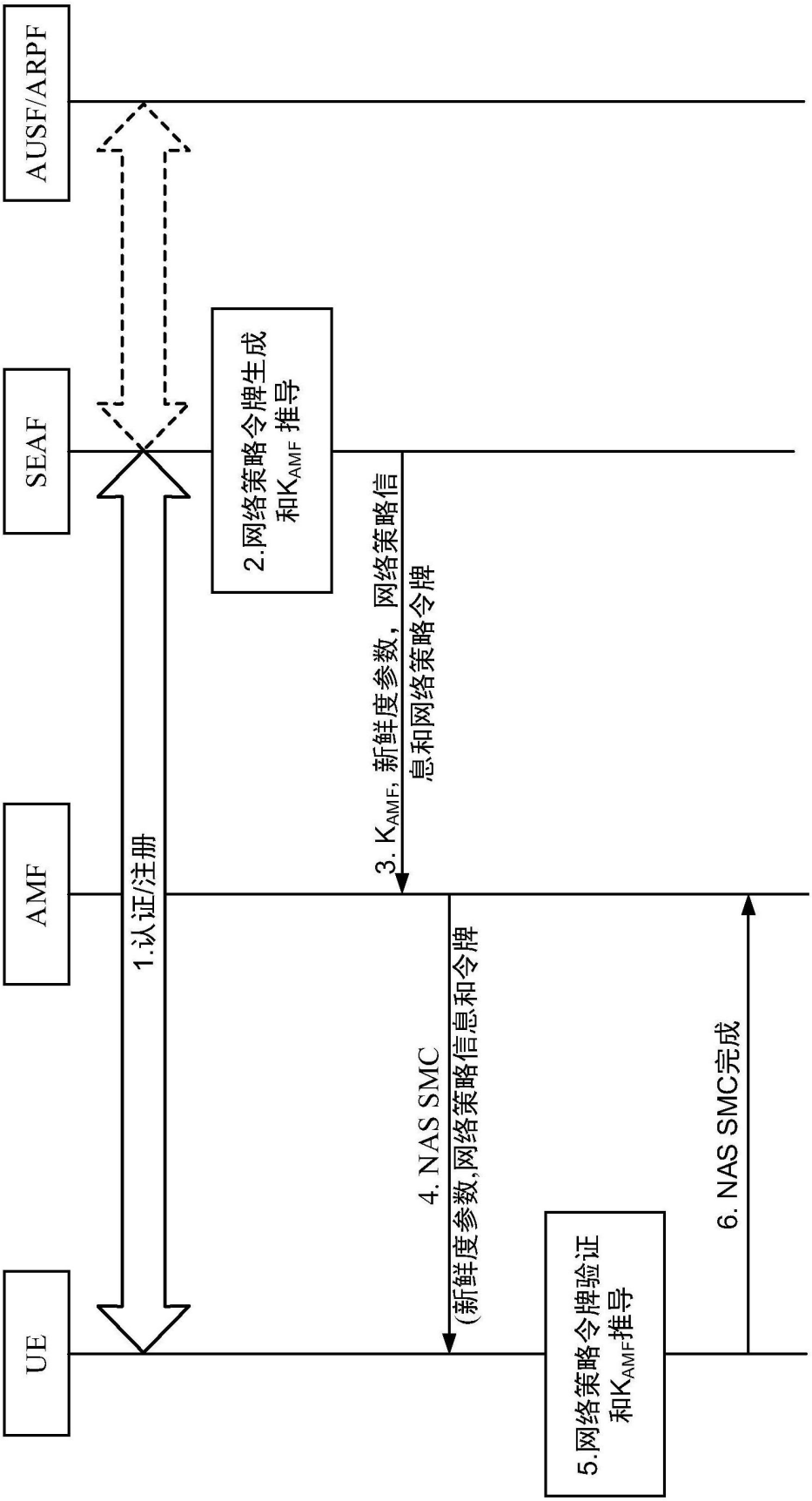

AUSF/ARPF
SEAF
AMF
UE
1.认证/注册
2.网络策略令牌生成
和K_{AMF} 推导
3. K_{AMF}, 新鲜度参数，网络策略信息和网络策略令牌
4. NAS SMC
(新鲜度参数,网络策略信息和令牌
5.网络策略令牌验证
和K_{AMF}推导
6. NAS SMC完成

图15