(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107257353 A
(43)申请公布日 2017.10.17

(21)申请号 201710682467.2
(22)申请日 2014.01.30
(30)优先权数据
61/758,373 2013.01.30 US
(62)分案原申请数据
201480006530.5 2014.01.30
(71)申请人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩
(72)发明人 S•瓦格尔 V•维尔基
O•特耶布 N•约翰逊 K•诺曼
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 张曦
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2009.01)

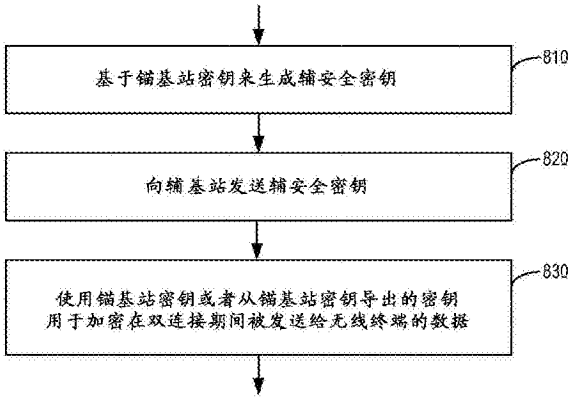
权利要求书1页 说明书16页 附图6页

(54)发明名称

用于双连接的安全密钥生成

(57)摘要

用于安全生成加密密钥集合以被使用用于在双连接场景中的无线终端与辅基站之间的通信的技术。一种示例方法包括:基于锚基站密钥来生成(810)用于辅基站的辅安全密钥。所生成的辅安全密钥被发送(820)给辅基站,以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用,该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时被发送给无线终端的数据流量进行加密。使用(830)锚基站密钥、或者从锚基站密钥导出的密钥用于对由锚基站发送给无线终端的数据进行加密。



CN 107257353 A

1.一种在无线终端(505B)中的方法,用于针对所述无线终端(505B)与辅基站之间的受保护通信的安全密钥生成,其中所述无线终端(505B)双连接到或者即将双连接到锚基站和所述辅基站,其中所述锚基站和所述无线终端(505B)已知主安全密钥,所述方法包括:

至少部分地基于所述主安全密钥生成辅安全密钥;

在生成用于加密数据流量的一个或多个附加辅安全密钥时使用所述辅安全密钥,其中当所述无线终端(505B)双连接到所述锚基站和所述辅基站时,所述数据流量从所述无线终端(505B)发送给所述辅基站。

2.根据权利要求1所述的方法,其中生成的所述辅安全密钥包括用于在生成一个或多个附加辅安全密钥时使用的基本辅安全密钥,所述一个或多个附加辅安全密钥用于加密由所述辅基站发送给所述无线终端(505B)的数据流量。

3.根据权利要求1或2所述的方法,其中生成所述辅安全密钥包括:使用单向函数从所述主密钥得出所述辅安全密钥。

4.根据权利要求3所述的方法,其中所述单向函数是HMAC-SHA-256密码函数。

5.根据权利要求1-4中任一项所述的方法,其中生成所述辅安全密钥进一步基于新鲜度参数。

6.一种无线终端(505B),用于针对所述无线终端(505B)与辅基站之间的受保护通信的安全密钥生成,所述无线终端(505B)包括接口电路(510B)、处理电路(520B)和存储器(530B),其中所述无线终端(505B)被配置为双连接到锚基站和所述辅基站,并且其中所述处理电路(520B)被配置为:

至少部分地基于所述锚基站和所述无线终端(505B)已知的主安全密钥生成辅安全密钥;

在生成用于加密数据流量的一个或多个附加辅安全密钥时使用所述辅安全密钥,其中当所述无线终端(505B)双连接到所述锚基站和所述辅基站时,所述数据流量从所述无线终端(505B)发送给所述辅基站。

7.根据权利要求6所述的无线终端(505B),其中所述处理电路(520B)进一步被配置为:通过使用单向函数从所述主密钥得出所述辅安全密钥来生成所述辅安全密钥。

8.根据权利要求7所述的无线终端(505B),其中所述单向函数是HMAC-SHA-256密码函数。

9.根据权利要求6-8中任一项所述的无线终端(505B),其中所述处理电路(520B)进一步被配置为:基于新鲜度参数生成所述辅安全密钥。

10.根据权利要求6-9中任一项所述的无线终端(505B),进一步被配置为:将所述主密钥和/或所述辅安全密钥存储在所述存储器(530B)中。

11.根据权利要求9或10所述的无线终端(505B),进一步被配置为:将所述新鲜度参数存储在所述存储器(530B)中。

用于双连接的安全密钥生成

[0001] 本申请是申请日为2014年1月30日、申请号为201480006530.5、发明名称为“用于双连接的安全密钥生成”的发明专利申请的分案申请。

技术领域

[0002] 本文所公开的技术一般性地涉及无线电信网络，并且更特别地涉及用于处置双连接场景中的安全密钥的技术，双连接场景即移动终端同时连接到多个基站的场景。

背景技术

[0003] 在典型的蜂窝无线电系统中，移动终端(也称为用户设备UE、无线终端、和/或移动台)经由无线电接入网络(RAN)与一个或多个核心网络进行通信，该一个或多个核心网络提供对数据网络(诸如互联网)和/或对公共交换电信网络(PSTN)的接入。RAN覆盖被划分为小区区域的地理区域，每个小区区域由无线电基站(也称为基站、RAN节点、“NodeB”、和/或增强型NodeB或“eNodeB”)来服务。小区区域是一个地理区域，在该地理区域上，无线电覆盖由位于基站站点的基站装备来提供。基站通过无线电通信信道来与基站的范围内的无线终端进行通信。

[0004] 蜂窝通信系统运营商已经开始供应基于例如WCDMA(宽带码分多址)、HSFA(高速分组接入)、以及长期演进(LTE)无线技术的移动宽带数据服务。由被设计用于数据应用的新设备的引入所推动，终端用户性能要求持续增加。对移动宽带的增加的采用已经导致了由高速无线数据网络处置的流量上的显著增长。因此，期望有允许蜂窝运营商更高效地管理网络的技术。

[0005] 改进下行链路性能的技术可以包括多输入多输出(MIMO)多天线发射技术、多流通信、多载波部署，等等。因为每链路的频谱效率可能正接近于理论极限，所以接下来的步骤可以包括改进每单位区域的频谱效率。例如，通过改变传统网络的拓扑结构以提供遍及小区的用户体验的增加的一致性，可以实现对于无线网络而言的进一步的效率。一种方法是通过对所谓的异构网络的部署。

[0006] 同构网络是采用所规划的布局的基站(也称为NodeB、增强型NodeB、或者eNB)的网络，其为用户终端(也称为用户设备节点UE、和/或无线终端)的集合提供通信服务，其中所有的基站通常具有类似的发射功率电平、天线图案、接收机本底噪声、和/或通向数据网络的回程连接。此外，同构网络中的所有基站一般可以向网络中的用户终端供应不受局限的接入，并且每个基站可以服务于大致相同数目的用户终端。在这个分类中的当前的蜂窝无线通信系统可以包括，例如，GSM(全球移动通信系统)、WCDMA、HSDPA(高速下行链路分组接入)、LTE(长期演进)、WiMAX(全球微波接入互操作性)，等等。

[0007] 在异构网络中，低功率基站(也称为低功率节点(LPN)、微节点、微微节点、毫微微节点、中继节点、远程无线电单元节点、RRU节点、小小区、RRU，等等)可以连同所规划的和/或规律放置的宏基站一起被部署或者被部署作为对所规划的和/或规律放置的宏基站的覆叠。宏基站(MBS)因此可以在相对大的宏小区区域上提供服务，并且每个LPN可以为该相对

大的宏小区区域内的相应的相对小的LPN小区区域提供服务。

[0008] 相比于由宏基站发射的功率(对于典型的宏基站而言其可以是40瓦特),由LPN发射的功率可以相对地小,例如2瓦特。LPN可以被部署,例如,以减少/消除由宏基站提供的覆盖中的(多个)覆盖空洞,和/或以从宏基站卸载流量,诸如以增加高流量地点或者所谓的热点上的容量。归因于它的较低发射功率和较小物理尺寸,LPN可以为站点获取供应更大的灵活性。

[0009] 因此,异构网络的特征是:对高功率节点(HPN)(诸如宏基站)以及低功率节点(LPN)(诸如所谓的微微基站或者微微节点)的多层化的部署。异构网络的给定地区中的LPN和HPN可以操作在相同的频率上,在该情况中,该部署可以被称为共信道的异构部署,或者操作在不同的频率上,在该情况中,该部署可以被称为频率间或者多载波或者多频率的异构部署。

[0010] 第三代合作伙伴计划(3GPP)正在继续开发如下的规范,这些规范针对被称为LTE(长期演进)的第四代无线电信系统的情境中的高级的和改进的特征。在LTE规范的发布12和更高的发布中,将会在“小小区增强”行动的伞之下考虑到与低功率节点和异构部署有关的进一步增强。这些行动中的一些行动将聚焦于实现宏层与低功率层之间的甚至更高程度的交互工作,包括通过使用一组技术以及被称为“双层连接”或简称为“双连接”的技术。

[0011] 如图1中所示出的,双连接意味着设备具有通向宏层和低功率层两者的同时连接。图1图示了异构网络的一个示例,其中移动终端101使用多个流,例如,来自宏基站(或者“锚eNB”)401A的锚流以及来自微微基站(或者“辅eNB”)401B的辅流。注意,术语可能变化—如图1中所示出的配置中的锚基站和辅基站有时可以称为“主”基站和“从”基站或者根据其他的名称。应当进一步注意,尽管术语“锚/辅”和“主/从”暗示了双连接场景中所牵涉到的在基站之间的层级关系,但是与双连接相关联的原理和技术中的许多原理和技术可以被应用到(例如,在对等基站之间)不存在这种层级关系的部署场景。因此,尽管本文中使用了术语“锚基站”和“辅基站”,但是应当理解,本文所描述的技术和装置不限制于使用该术语的实施例,它们也不必然限制于具有图1所暗示的层级关系的实施例。

[0012] 双连接可以意味着,在各种实施例和/或场景中:

[0013] • 控制与数据分离,其中例如在经由低功率层来提供高速数据连接的同时经由宏层来提供用于移动性的控制信令。

[0014] • 下行链路与上行链路之间的分离,其中经由不同的层来提供下行链路和上行链路连接。

[0015] • 针对控制信令的分集,其中可以经由多个链路来提供无线电资源控制(RRC)信令,进一步增强了移动性性能。

[0016] 包括双连接的宏辅助可以提供若干益处:

[0017] • 对于移动性的增强的支持—通过维持宏层中的移动性锚点,如上面所描述的,有可能维持宏层与低功率层之间、以及低功率节点之间的无缝移动性。

[0018] • 来自低功率层的低开销发射—通过仅发射为了个体的用户体验所要求的信息,例如,有可能避免来自于在局部区域层内支持空闲模式移动性的开销。

[0019] • 能量高效的负载平衡—通过在没有进行中的数据发射时关闭低功率节点,有可能减少低功率层的能量消耗。

[0020] • 每链路的优化—通过分离地针对上行链路和下行链路来选择终接点，能够针对每个链路来优化节点选择。

[0021] 在使用双连接中的问题之一是如何将数据无线电承载(DRB)分别映射到锚流和辅流上。一种用于在如图1中所示出的两个基站之间拆分DRB的选择是，将控制平面(RRC)保持在锚eNB中并且将PDCP实体进行分布，使得它们中的一些在锚eNB中并且它们中的一些在辅eNB中。如下面以进一步细节所讨论的，这种方法可以产生一些重要的系统效率益处。然而，这种方法造成了与安全密钥的处置有关的问题，这些安全密钥被使用用于向移动终端和从移动终端发射的数据的机密性和完整性保护。

发明内容

[0022] 在LTE系统中，无线电资源控制(RRC)层利用密码密钥和配置数据，诸如指示在具有对应的无线电承载的连接中应当应用哪些安全算法的数据，来配置分组数据汇聚协议(PDCP)实体。在双连接场景中，RRC层可以排他地由锚节点来处置，而PDCP实体可以在锚基站节点和辅基站节点中的每个中加以管理。因为锚基站和辅基站可以被实施在物理上分离的节点中，所以RRC能够经由内部的应用程序接口(API)来配置PDCP实体的假设不再适用。

[0023] 本文所公开的示例实施例针对安全生成加密密钥的集合，以被使用用于在处于双连接中的无线终端与辅eNB之间的通信。在一些实施例中，从锚eNB的安全密钥来生成用于辅eNB的基本密钥。该基本密钥然后能够被用来生成用于在无线终端与辅eNB之间的安全通信的密钥。

[0024] 所公开的技术的实施例包括，例如，一种适合用于实施在网络节点中的方法，用于针对在无线终端与锚基站之间以及在无线终端与辅基站之间的受保护通信的安全密钥生成，其中无线终端双连接到或者即将双连接到锚基站和辅基站。该示例方法包括：至少部分地基于锚基站密钥来生成用于辅基站的辅安全密钥。所生成的辅安全密钥然后被发送给辅基站，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端的数据流量进行加密。使用锚基站密钥、或者从锚基站密钥导出的密钥用于对当无线终端双连接到锚基站和辅基站时由锚基站发送给无线终端的数据进行加密。

[0025] 本文还公开的是另一种用于生成用于辅基站的辅安全密钥的方法。如同上面所概述的方法，这个方法也适合用于实施在网络节点中，用于针对在无线终端与锚基站之间以及在无线终端与辅基站之间的受保护通信的安全密钥生成，其中无线终端双连接到或者即将双连接到锚基站和辅基站。然而，在这个方法中，可以使用对锚基站而言可以是未知的主密钥在除了锚基站之外的网络节点中执行该方法。

[0026] 根据这个第二示例方法，在网络节点与无线终端之间共享主安全密钥。在一些实施例中，这个密钥对锚基站而言可以是未知的。该方法继续于：至少部分地基于主安全密钥来生成用于辅基站的辅安全密钥。所生成的辅安全密钥然后被发送给辅基站，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端的数据流量进行加密。在一些实施例中，所生成的辅安全密钥直接

被发送给辅基站，从而锚基站不知晓该密钥，而在其他实施例中，所生成的辅安全密钥经由锚基站而间接地被发送给辅基站。

[0027] 本文所公开的技术的其他实施例包括网络节点装置和移动终端装置，它们每个都被配置为执行上面所概述的示例方法之一或者它们的变型。

附图说明

[0028] 图1是图示了具有通向移动终端的同时的锚流和辅流的异构双连接部署的一个示例的示意图。

[0029] 图2图示了E-UTRAN系统架构的组件。

[0030] 图3图示了双连接场景中的基站协议架构的细节。

[0031] 图4图示了基于锚基站密钥的密钥推导层级结构。

[0032] 图5图示了基于MME密钥的密钥推导层级结构。

[0033] 图6是图示了由示例网络节点实施的示例方法的过程流程图。

[0034] 图7是图示了由无线终端实施的示例方法的过程流程图。

[0035] 图8和图9每个都图示了与目前所公开的技术的示例实施例相对应的过程流程图。

[0036] 图10是图示了根据目前所公开的技术的示例锚基站装置的框图。

[0037] 图11是图示了根据目前所公开的技术的另一示例网络节点装置的框图。

[0038] 图12图示了根据目前所公开的实施例中的一些实施例来配置的示例无线终端的组件。

具体实施方式

[0039] 现在将在后文中参考附图更完全地描述发明概念，在附图中示出了发明概念的实施例的示例。然而，这些发明概念可以按许多不同的形式被具体化并且不应当解释为被限制于本文所阐述的实施例。确切地说，这些实施例被提供而使得这一公开内容将是透彻的和完整的，并且完全地向本领域的技术人员传达了本发明概念的范围。还应当注意，这些实施例并不是相互排斥的。来自一个实施例的组件可以默示地被假设为存在于或者被使用在另一实施例中。

[0040] 仅为了说明和解释的目的，本文在通过无线电通信信道与移动终端(也称为无线终端或者UE)进行通信的无线电接入网络(RAN)中进行操作的情境中描述了本发明概念的这些和其他实施例。如本文中所使用的，移动终端、无线终端、或者UE能够包括从通信网络接收数据的任何设备，并且可以包括但不限于，移动电话(“蜂窝”电话)、膝上型/便携式计算机、口袋式计算机、手持式计算机、台式计算机、机器到机器(M2M)或MTC类型设备、具有无线通信接口的传感器，等等。

[0041] 通用移动电信系统(UMTS)是第三代移动通信系统，其从全球移动通信系统(GSM)演进而来，并且意图为基于宽带码分多址(WCDMA)技术来提供改进的移动通信服务。UTRAN(用于UMTS陆上无线电接入网络的缩写)是用于组成UMTS无线电接入网络的节点B和无线电网络控制器的集合术语。因此，UTRAN本质上是针对UE使用宽带码分多址(WCDMA)的无线电接入网络。

[0042] 第三代合作伙伴计划(3GPP)已经着手进一步演进基于UTRAN和GSM的无线电接入

网络技术。在这个方面，用于演进型通用陆上无线电接入网络(E-UTRAN)的规范在3GPP内正在进行中。演进型通用陆上无线电接入网络(E-UTRAN)包括长期演进(LTE)和系统架构演进(SAE)。

[0043] 注意，尽管在这一公开内容中一般使用来自LTE的术语来例证发明概念的实施例，但是这不应当被视为将发明概念的范围限制于仅这些系统。其他的无线系统，包括3GPP LTE和WCDMA系统的变型和后继、WiMAX(全球微波接入互操作性)、UMB(超移动宽带)、HSPDA(高速下行链路分组接入)、GSM(全球移动通信系统)等，也可以从利用本文所公开的本发明概念的实施例中受益。

[0044] 还要注意，诸如基站(也称为NodeB、eNodeB、或演进型节点B)以及无线终端或移动终端(也称为用户设备节点或UE)的术语应当考虑为是非限制性的并且不意味着这两者之间的某种层级关系。一般而言，基站(例如，“NodeB”或“eNodeB”)和无线终端(例如，“UE”)可以被考虑为是通过无线的无线电信道彼此进行通信的相应的不同的通信设备的示例。

[0045] 尽管本文所讨论的实施例可能聚焦于如下的示例实施例，在这些示例实施例中，所描述的解决方案被应用在异构网络中，这些异构网络包括相对较高功率基站(例如，“宏”基站，其也可以被称为广域基站或者广域网络节点)与相对较低功率节点(例如，“微微”基站，其也可以被称为局域基站或者局域网络节点)的混合，但是所描述的技术可以被应用在任何适合类型的网络中，包括同构配置和异构配置两者。因此，在所描述的配置中牵涉到的基站可以类似于或相同于彼此，或者可以在发射功率、发射机-接收机天线的数目、处理功率、接收机和发射机特性、和/或任何其他功能或物理能力的方面上不同。

[0046] 演进型UMTS陆上无线电接入网络(E-UTRAN)包括称为增强型NodeB(eNB或eNodeB)的基站，提供朝向UE的E-UTRA用户平面和控制平面协议终接。使用X2接口将eNB彼此互连。还使用S1接口将eNB连接到EPC(演进型分组核心)，更具体地是借助于S1-MME接口而连接到MME(移动性管理实体)并且借助于S1-U接口而连接到服务网关(S-GW)。S1接口支持MME/S-GW与eNB之间的多对多关系。图2中图示了E-UTRAN架构的简化视图。

[0047] eNB 210主控(host)如下的功能，诸如无线电资源管理(RRM)、无线电承载控制、接纳控制、朝向服务网关的用户平面数据的头部压缩、和/或对朝向服务网关的用户平面数据的路由。MME 220是处理UE与CN(核心网络)之间的信令的控制节点。MME 220的重大功能涉及经由非接入层(NAS)协议来处置的连接管理和承载管理。S-GW 230是用于UE移动性的锚点，并且还包括其他功能，诸如当UE正在被寻呼时的临时DL(下行链路)数据缓冲、向正确eNB的分组路由和转发、和/或对用于计费和合法拦截的信息的收集。PDN网关(P-GW，未示出在图2中)是负责UE IP地址分配以及(如下面进一步讨论的)服务质量(QoS)强制的节点。对于不同节点的功能的进一步细节，读者请参考3GPP TS 36.300和其中的参考文献。

[0048] 在描述目前公开的技术的各种实施例中，可能使用非限制性的术语“无线电网络节点”来指代服务于UE和/或连接到其他网络节点或网络元件或UE从其接收信号的任何无线电节点的任何类型的网络节点。无线电网络节点的示例是节点B、基站(BS)、多标准无线电(MSR)无线电节点(诸如MSR BS)、eNodeB、网络控制器、无线电网络控制器(RNC)、基站控制器、中继、施主节点控制中继、基站收发机(BTS)、接入点(AP)、无线路由器、发射点、发射节点、远程无线电单元(RRU)、远程无线电头端(RRH)、分布式天线系统(DAS)中的节点，等等。

[0049] 在一些情况中，使用了更一般的术语“网络节点”；这个术语可以对应于任何类型的无线电网络节点或者与至少无线电网络节点进行通信的任何网络节点。网络节点的示例是上面所陈述的任何无线电网络节点、核心网络节点(例如，MSC、MME等)、O&M、OSS、SON、定位节点(例如，E-SMLC)、MDT，等等。

[0050] 在描述一些实施例中，术语“用户设备(UE)”被使用并且指代与蜂窝或移动通信系统中的无线电网络节点进行通信的任何类型的无线设备。UE的示例是目标设备、设备到设备UE、机器类型UE或能够进行机器到机器通信的UE、PDA、启用无线的桌式计算机、移动终端、智能电话、膝上型嵌入式装备(LEE)、膝上型安装式装备(LME)、USB电子狗、客户驻地装备(CPE)，等等。如本文所使用的术语“移动终端”应当理解为与本文中以及在由3GPP颁布的各种规范中所使用的术语“UE”一般是可互换的，但是不应当理解为被限制于符合于3GPP标准的设备。

[0051] 本文所提出的示例实施例具体地针对当在宏小区与辅eNB小区之间拆分LTE Uu-协议栈时的密钥生成。各技术和装置更一般地可应用到其他双连接场景中的密钥生成。

[0052] 如上面所提及的，一种用于在双连接场景中的两个基站之间拆分数据无线电承载(DRB)的选择是，将由无线电资源控制(RRC)协议管理的控制平面保持在锚eNB中，而将与个体无线电承载相关联的分组数据汇聚协议(PDCP)实体进行分布，使得一个或多个终止于锚eNB中并且一个或多个终止于辅eNB中。

[0053] RRC层对它与之相关联的所有PDCP实体进行配置。这图示在图3中，图3示出了用于多连接的协议架构的一个示例。

[0054] 更特别地，RRC利用密码密钥和配置数据(诸如指示在具有对应的无线电承载的连接中应当应用哪些安全算法的数据)来配置PDCP实体。对于与给定的移动终端相关联的连接，RRC利用一个且相同的加密密钥KUP-enc来配置用于用户平面流量(DRB)的所有PDCP实体，并且利用一个且相同的加密密钥KRRC-enc以及一个且相同的完整性保护密钥KRRC-int来配置用于控制平面流量(SRB)的所有PDCP实体。对于被用来保护施主-eNB与中继节点之间的数据的DRB，RRC也利用完整性保护密钥KUP-int来配置这些DRB。

[0055] 因为锚eNB和辅eNB可以被实施在分离的物理节点中，所以RRC能够经由内部的应用程序接口(API)来配置PDCP实体的假设不再适用。也就是说，安全配置数据能够被假设为安全地被保持在eNB的物理上安全的环境里面的当前情形不再成立。替代地，锚eNB中的RRC实体必须配置辅eNB中的PDCP实体，而辅eNB在锚eNB的安全环境外面。

[0056] 这里使用锚eNB和辅eNB来定义从UE或无线终端视角来看的eNB的不同角色。所承认的是，这只是一种示例命名并且它们也可以被称为其他的事物，如锚和助推器(booster)、主和从、或者简单地是eNB_1和eNB_2。

[0057] LTE的安全设计一般提供了对安全功能的区分。这种区分意图是确保如果攻击者破坏了一个功能的安全性，则仅该功能被危害。例如，存在被使用用于RRC协议的加密的一个密钥以及被使用用于RRC协议的完整性保护的另一密钥。如果攻击者破坏了加密密钥，则他能够解密并且读取所有的RRC消息。然而，因为完整性密钥不同于加密密钥，所以攻击者不能修改或者注入RRC消息。

[0058] LTE中所使用的区分方法的另一方面是每个eNB都使用分离的密钥集合。针对这一点的理论基础是，这种方法确保了破坏进入一个eNB的攻击者不会得到和在无线终端与另

一物理上不同的eNB之间发射的数据有关的任何信息。在双连接场景中，那么，为了维持如下的性质：破坏进入一个物理RAN节点(即，eNB)不会有助于攻击另一RAN节点，辅eNB应当使用它自己的与锚eNB中使用的密钥集合分离的密钥集合。

[0059] 双连接架构对于潜在的安全攻击可能开放三个新的路径，这取决于为了处置安全密钥和参数所采用的技术。第一，安全配置和密码密钥从锚eNB到辅eNB的运输提供了如下的点，在该点处，攻击者可以窃听或者可以修改密钥和配置数据。第二，攻击者可以物理地破坏进入辅eNB，并且在那里窃听或者修改密钥和配置数据。另外，物理地破坏进入辅eNB的攻击者可以读取、修改、或注入用于被连接到辅eNB的任何无线终端的用户平面数据。第三，攻击者可以在辅eNB发送和接收用户平面数据时接入并修改它。这是真实的，不论用户平面数据是否在辅eNB与锚eNB之间、在辅eNB与S-GW之间流动，或者数据局部地在辅eNB中是否突破到互联网。

[0060] 本文所公开的示例实施例针对将被使用用于处于双连接中的无线终端与辅eNB之间的通信的加密密钥集合的安全生成。在一些实施例中，从锚eNB的安全密钥生成用于辅eNB的基本密钥。该基本密钥然后能够被用来生成用于无线终端与辅eNB之间的安全通信的密钥。

[0061] 用于辅eNB的密钥建立

[0062] 在LTE中，eNB中的密钥集合包括K_{eNB}、以及K_{UP-enc}、$K_{RRC-enc}$和$K_{RRC-int}$。取决于辅eNB提供什么功能，辅eNB所需要的密钥集合将是不同的。因为辅eNB将至少终止用户平面加密，所以建立辅eNB与无线终端共享的加密密钥是有用的。如果辅eNB将为中继节点提供服务，则对于完整性密钥而言还存在对运载中继节点控制平面流量的DRB进行保护的需要。因此建立类似于K_{eNB}的用于辅eNB的基本密钥是有用的，从该基本密钥能够导出其他密钥。此后，本讨论将有关于建立被称为$K_{assisting_eNB}$的基本密钥，但是相同的推理能够显而易见地被应用到例如仅建立了加密密钥的情况。

[0063] 图4示出了如何能够基于锚eNB的K_{eNB}来生成$K_{assisting_eNB}$。该图示出了用于辅eNB的可能的密钥层级结构。在这个示例中，辅eNB与无线终端共享$K_{assisting_eNB}$、$K_{assisting_eNB-enc}$和$K_{assisting_eNB-int}$密钥，它们中的全部都直接地或者间接地从用于锚eNB的K_{eNB}导出。

[0064] 图4中的箭头指示了密钥推导函数(KDF)的应用。为了所有实际的目的，KDF能够被考虑为是单向函数。正如熟悉于密码技术的人们所熟知的，单向函数易于在正向方向(箭头的方向)上计算，但是计算上不可实行于逆向。这一点的含义是，对密钥层级结构中较低的密钥的访问并不给出与该层级结构中向上较高的密钥有关的任何有用信息。KDF的一个示例是HMAC-SHA256函数，它是在LTE中以及在许多其他3GPP系统中使用的KDF。

[0065] 图4中是一个具体的示例。如果$K_{assisting_eNB}$密钥在锚eNB中被生成并且被发送给辅eNB，则辅eNB具有对$K_{assisting_eNB}$以及它导出的加密密钥和完整性密钥的访问。然而，它将不具有对K_{eNB}的访问。

[0066] 因为假设了KDF是已知的，所以在另一方面，锚eNB节点将具有对辅eNB使用的所有密钥的访问。如果它在其最严格的意义上被解读的话，这破坏了区分原则。然而，这个场景中的安全级别类似于在X2-切换时获得的安全级别，X2-切换是LTE中的一种切换，其不牵涉到移动管理实体(MME)而被处置。在X2-切换时，源eNB基于当前使用的K_{eNB}来运算新密钥，并且将该新密钥提供给目标eNB。类似情形的另一示例出现在中继节点的情境中。在中继节点

的情况中，施主-eNB充当用于中继节点的S1-代理。作为结果，施主-eNB具有对中继节点使用的所有密钥的访问。因为该安全情形类似于已经出现在LTE网络中的若干安全情形，所以从安全的视点来看，使用K_{eNB}作为用于$K_{assisting_eNB}$的基础加密钥材料可以被考虑为可接受。

[0067] 在双连接场景中可以有利地采用图4中所示出的密钥层级结构，其中锚eNB控制辅eNB中的PDCP实体，即锚eNB可以建立新的PDCP实体、删除它们、以及重启先前所删除的PDCP实体。锚eNB和移动终端(例如，LTE UE)每个都将像这样从KeNB导出$K_{assisting_eNB}$：$K_{assisting\_eNB}$＝KDF(KeNB，其他_参数)。

[0068] 为了避免公知攻击的可能性(这些公知攻击利用了对携带已知底层数据的经加密数据的重复传输)，应当确保$K_{assisting_eNB}$在每次PDCP实体重新使用相同的COUNT值时都是“新鲜的”。因此，对$K_{assisting_eNB}$的推导应当优选地包括适当的新鲜度参数。一种实现新鲜度的方式是使用与某个预定的RRC消息相关联的序列号PDCP COUNT，预定的RRC消息诸如最新的RRC安全模式命令或切换命令，或者被用来建立辅eNB中的PDCP实体的“RRC重配置请求”或“RRC重配置完成”消息之一。当然，可以替代地使用与其他RRC消息相关联的序列号。用于将新鲜度并入到$K_{assisting_eNB}$的生成中的其他选择包括：在一些预定的RRC消息或者其他协议消息中，将新鲜的“随机数(nonce)”从无线终端发送给锚eNB或辅eNB，从锚eNB或辅eNB发送给无线终端(或者在两个方向上)。随机数是(伪)随机地生成的数字，其以充分高的概率将关于K_{eNB}是唯一的。

[0069] 不论新鲜度参数是什么，它们然后被包括在$K_{assisting_eNB}$推导中或者对从Kassisting eNB导出的密钥的推导中。也有可能重新使用RRC消息中的已有信息元素、或者从锚eNB或辅eNB在系统信息块中传输的信息。能够使用任何信息，只要它以充分高的概率提供了(统计上)唯一的输入。

[0070] 另一种可能的设计是，锚eNB不利用任何新鲜度参数从KeNB导出$K_{assisting_eNB}$。根据这种替换方法，如果辅eNB或锚eNB检测到辅eNB中的PDCP COUNT即将返转(wrap around)，则锚eNB经由小区内切换来发起KeNB密钥刷新。小区内切换的结果是，无线终端和锚eNB不仅刷新K_{eNB}，而且还刷新$K_{assisting_eNB}$；$K_{assisting_eNB}$可以按它第一次被导出的相同方式被重新运算。这种方法可能要求辅eNB必须向锚eNB通知即将被重新使用的PDCP COUNT。

[0071] 将$K_{assisting_eNB}$从锚eNB运输到辅eNB能够通过这两者之间的控制信道来完成。如已经陈述的，控制信道必须被机密性和完整性保护。

[0072] 在上面所描述的技术的各种实施例中，除了明确提到的那些参数之外的其他参数也可以输入到KDF。可以按各种不同顺序中的任何顺序来摆放这些参数。进一步地，用于KDF的参数中的任何一个或多个参数可以在被输入到KDF之前加以变形。例如，对于某个非负整数n而言，参数集合P1、P2、…、Pn可以通过首先经过变形函数f来运行而加以变形，并且其结果，即f(P1,P2,…,Pn)被输入到KDF。

[0073] 在密钥推导的一个示例中，参数P1在被输入到KDF之前首先加以变形，以运算被称为“output_key”的密钥：output_key＝KDF(f(P1),P2)，其中f是某个任意的函数或者函数链，并且P1和P2是输入参数。参数P2例如可以是0、1、或者例如被用来将密钥绑定到某个情境的更多其他参数。参数可以作为分离的参数而被输入，或者可以被级联在一起并且然后在一个单个输入中输入到KDF。即使在使用诸如这些的KDF的变型时，思想的核心保持相同。

[0074] 不论使用了哪种密钥建立方法，已有的切换过程在将具有双连接的移动终端切换

到另一基站时一般不受影响，而不论目标基站的类型。锚eNB能够拆除辅eNB中的DRB，并且根据已有的规范来执行向目标基站的切换。

[0075] 在将无线终端切换到目标eNB和目标辅eNB时，能够个别地执行K_{eNB}密钥和$K_{assisting_eNB}$密钥的推导。

[0076] 基于K_{ASME}的密钥推导

[0077] 替代使用锚节点的基本密钥作为用于生成$K_{assisting_eNB}$的基础，可以替代地使用与无线网络中的另一节点相关联并且对移动终端而言是已知的密钥。例如，如图5中所示出的，使用K_{ASME}作为用于$K_{assisting_eNB}$的加密钥材料基础相比于使用上面所描述的K_{eNB}而言允许了更高的安全级别。如图5中所看到的，能够从K_{ASME}导出$K_{assisting_eNB}$，并且从结果的$K_{assisting_eNB}$导出用于辅eNB的加密密钥和完整性密钥。

[0078] K_{ASME}是经由LTE中的订户认证而建立的密钥，并且它在MME与无线终端之间共享。如果从K_{ASME}导出$K_{assisting_eNB}$并且MME直接向辅eNB提供这个$K_{assisting_eNB}$，则锚节点不具有对$K_{assisting_eNB}$或者从它导出的加密密钥和完整性密钥的访问。在这种情况中，那么，在更严格的意义上遵守了上面所讨论的区分原则。

[0079] 使$K_{assisting_eNB}$的推导基于K_{ASME}要求使MME知晓辅eNB何时需要对密钥的访问，并且进一步要求在这两者之间存在通信路径。MME是否知晓无线终端何时连接到辅eNB(并且因此需要密钥)以及在MME与辅eNB之间是否存在信令路径取决于辅eNB如何被控制。如果这些条件没有被满足，使用K_{ASME}作为加密钥材料基础尽管仍然是可能的但是较为无用，因为MME将必须把$K_{assisting_eNB}$发送给锚节点，锚节点进而将它提供给辅eNB。在这种场景中，当然，锚节点具有对$K_{assisting_eNB}$的访问。

[0080] 使用K_{ASME}作为加密钥材料基础意味着使用密钥推导函数$K_{assisting_eNB}$=KDF(KASME,[其他_参数])从K_{ASME}导出$K_{assisting_eNB}$，其中可选的“其他_参数”可以包括一个或多个新鲜度参数。

[0081] 如早先所描述的，当PDCP分组计数器(PDCP COUNT)被重置时，加密密钥和完整性密钥应当被更新。如果相同的密钥与相同的PDCP COUNT一起使用，则将存在密钥流重用，并且潜在地，重放攻击是可能的。因此，MME和无线终端可以将新鲜度参数包括在密钥推导中。例如，与当针对锚节点(eNB)导出K_{eNB}时使用的新鲜度参数相同的新鲜度参数。使用哪个新鲜度参数用于K_{eNB}推导可以取决于情形。可能的新鲜度参数包括MME与无线终端交换的随机数(一次使用的随机数字)。其他的可能性是分组计数器(诸如NAS上行链路或下行链路COUNT)、或者从无线终端向MME或从MME向无线终端传输的新引入的计数器。新引入的计数器的一个缺点是，如果它脱离同步，则它必须通过某种新的重新同步机制来重新同步。

[0082] 其他参数也可以被包括在$K_{assisting_eNB}$推导中。例如，能够使用辅eNB的标识或者辅eNB使用的小区作为输入。这类似于K_{eNB}如何被绑定到小区标识。目的可能是进一步区分潜在的安全破坏。

[0083] 一旦MME已经导出了$K_{assisting_eNB}$，MME还必须将它传送给辅eNB。将$K_{assisting_eNB}$传送给辅eNB能够按两种方式之一来进行，直接地传送给辅eNB，或者间接地通过首先将$K_{assisting_eNB}$传送给eNB并且然后让eNB在必要时将它传送给辅eNB。

[0084] 将$K_{assisting_eNB}$直接从MME传送给辅eNB一般而言是一种安全性优点。以这种方式，仅MME、辅eNB和无线终端知道密钥。如果用于在辅eNB与无线终端之间建立连接的信令使得

牵涉到MME，则这是更可取的。

[0085] 其他的替换方式是对于MME而言将$K_{assisting_eNB}$发送给eNB，eNB简单地将$K_{assisting_eNB}$转发给辅eNB。这种方法具有安全性缺点，因为eNB现在也知晓$K_{assisting_eNB}$。然而，如果在MME与辅eNB之间不存在直接的信令路径并且K_{ASME}是被使用作为用于$K_{assisting_eNB}$推导的基础的加密钥材料，则该方法可能是有用的。

[0086] 示例方法

[0087] 鉴于上面所描述的详细示例，将会意识到，图6和7是描绘了分别由网络节点和无线终端可能采取的示例操作的流程图，其中网络在各种实施例中可以是锚基站或MME。所图示的过程流程图包括以实线边界图示的一些操作以及以虚线边界图示的一些操作。被包括在实线边界中的操作是被包括在最宽的示例实施例中的操作。被包括在虚线边界中的操作是可以被包括在较宽示例实施例中或者是较宽示例实施例的一部分，或者是可以除了较宽示例实施例的操作之外又采取的进一步操作。因此，在虚线轮廓中示出的这些操作，在它们可能不出现在所图示的过程的每个实施例的每个实例中的意义上，可以被考虑为是“可选的”。还应当意识到，图6和7的操作仅作为一种示例而被提供。

[0088] 更特别地，图6图示了一种用于在双连接场景中生成辅安全密钥以用于由辅基站使用的过程。图6中所示出的过程可以被实施在网络节点中，诸如在锚基站(例如，LTE锚eNB)中或者在某个其他的网络节点(诸如MME)中。如在框10处所示出的，网络节点首先确定对于将被生成的辅安全密钥的需求。例如，这可以由双连接场景的建立来触发。响应于这一确定，网络节点至少部分地基于主安全密钥来生成辅安全密钥。这示出在框12处。如上面详细解释的，这个主安全密钥在各种实施例中可以是锚节点基本密钥(例如，K_{eNB})或者对网络节点和感兴趣的移动终端而言是已知的其他密钥，诸如MME密钥(例如，K_{ASME})。

[0089] 如在框12和16处所示出的，辅安全密钥的生成可以包含对KDF(例如，单向密码函数)以及一个或多个新鲜度参数的使用。如在框17处所示出的，在一些实施例中，可以维护已经被使用的新鲜度参数的列表。

[0090] 如在框18处所示出的，所生成的辅安全密钥然后被发送给辅基站。在一些情况中，如上面所详述的，辅安全密钥然后被用来生成一个或多个附加密钥以用于保护向移动终端和从移动终端传送的数据，尽管在一些实施例中可能为了这样的目的而直接使用辅安全密钥。

[0091] 图7图示了诸如可能在移动终端中执行的对应方法。如在框30处所示出的，移动终端至少部分地基于由图6中的网络节点使用的相同主安全密钥来生成辅安全密钥。再一次地，这个主安全密钥在各种实施例中可以是锚节点基本密钥(例如，K_{eNB})或者对网络节点和感兴趣的移动终端而言是已知的其他密钥，诸如MME密钥(例如，K_{ASME})。如在框32和34处所示出的，辅安全密钥的生成可以包含对KDF(例如，单向密码函数)以及一个或多个新鲜度参数的使用。如在框17处所示出的，在一些实施例中，可以维护已经被使用的新鲜度参数的列表。

[0092] 如在框36处所示出的，所生成的辅安全密钥然后被应用到对向辅基站和从辅基站发送的数据的保护。在一些情况中，如上面所详述的，辅安全密钥被用来生成一个或多个附加密钥以用于保护向移动终端和从移动终端传送的数据，尽管在一些实施例中可能为了这样的目的而直接使用辅安全密钥。

[0093] 如上面所讨论的，在各种实施例中，可以从锚节点密钥或者从与另一节点(诸如MME)相对应的安全密钥来生成辅安全密钥。图8和9是分别与这两种场景相对应的过程流程图。这些方法可以在例如LTE网络中执行，但是也能够被应用到采用双连接的其他无线网络。

[0094] 图8因此图示了一种适合用于实施在网络节点中的方法，以用于针对在无线终端与锚基站之间以及在无线终端与辅基站之间的受保护通信的安全密钥生成，其中无线终端双连接到或者即将双连接到锚基站和辅基站。如在框810处所示出的，所图示的方法包括：至少部分地基于锚基站密钥来生成用于辅基站的辅安全密钥。如在框820处所示出的，所生成的辅安全密钥然后被发送给辅基站，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端的数据流量进行加密。如在框830处所示出的，使用锚基站密钥、或者从锚基站密钥导出的密钥用于对当无线终端双连接到锚基站和辅基站时由锚基站发送给无线终端的数据进行加密。

[0095] 在图8中所图示的方法的一些实施例中，所生成的辅安全密钥包括用于在生成一个或多个附加辅安全密钥中使用的基本辅安全密钥，该一个或多个附加辅安全密钥用于对由辅基站发送给无线终端的数据流量进行加密。在这些实施例中的一些实施例中，锚基站和移动终端可以每个都从锚基站密钥来导出加密密钥、或者完整性密钥、或者两者，并且使用所导出的密钥或多个密钥用于保护当无线终端双连接到锚基站和辅基站时由锚基站向无线终端发送或者从无线终端接收的数据。

[0096] 在图8中所示出的实施例中的一些实施例中，生成辅安全密钥包括：使用单向函数从锚基站密钥导出辅安全密钥。在一些实施例中，单向函数可以是HMAC-SHA-256密码函数。在这些实施例中的一些实施例中以及在一些其他的实施例中，辅安全密钥的生成进一步基于新鲜度参数。

[0097] 在一些实施例中，所图示的方法可以进一步包括：检测辅基站中的分组数据汇聚协议(PDCP)COUNT参数即将返转，以及作为响应，发起对锚基站密钥的刷新并且重新运算辅安全密钥。

[0098] 在一些实施例中，使用单个辅安全密钥来生成密钥集合以在所有的数据无线电承载中使用。在其他实施例中，可以使用多个辅安全密钥，在该情况中，针对在无线终端与辅基站之间建立的多个数据无线电承载中的每个数据无线电承载来重复上面所描述的生成操作，使得结果的辅安全密钥对于每个数据无线电承载是不同的。在一些实施例中，结果的若干密钥中的多个密钥可以同时被发送。

[0099] 图9是图示了用于生成用于辅基站的辅安全密钥的另一方法的过程流程图。如同图8中所示出的方法，图9的过程适合用于实施在网络节点中，以用于针对在无线终端与锚基站之间以及在无线终端与辅基站之间的受保护通信的安全密钥生成，其中无线终端双连接到或者即将双连接到锚基站和辅基站。然而，在这个方法中，可以使用对锚基站而言可以是未知的主密钥，在除了锚基站之外的网络节点中执行该方法。

[0100] 如在框910处所示出的，所图示的方法包括：与无线终端共享主安全密钥。在一些实施例中，这个密钥对锚基站而言可以是未知的。一种示例是上面所讨论的K_{ASME}密钥，其在LTE MME与移动终端之间共享。

[0101] 如在框920处所示出的，该方法继续于：至少部分地基于主安全密钥来生成用于辅基站的辅安全密钥。如在框930处所示出的，所生成的辅安全密钥然后被发送给辅基站，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端的数据流量进行加密。在一些实施例中，所生成的辅安全密钥直接被发送给辅基站，从而锚基站不知晓该密钥，而在其他实施例中，所生成的辅安全密钥经由锚基站而间接地被发送给辅基站。

[0102] 在一些实施例中，所生成的辅安全密钥包括用于在生成一个或多个附加辅安全密钥中使用的基本辅安全密钥，该一个或多个附加辅安全密钥用于对由辅基站发送给无线终端的数据流量进行加密。在这些实施例中的一些实施例中以及在一些其他的实施例中，生成辅安全密钥包括：使用单向函数从锚基站密钥导出辅安全密钥。例如，单向函数可以是HMAC-SHA-256密码函数。如上面详细讨论的，在一些实施例中，生成辅安全密钥可以进一步基于新鲜度参数。

[0103] 示例硬件实施方式

[0104] 可以使用网络节点(诸如锚基站)中或者MME中所提供的电子数据处理电路和无线电电路或者其他接口电路来实施上面所描述的技术和方法中的若干技术和方法，而可以使用无线终端中所提供的无线电电路和电子数据处理电路来实施其他的技术和方法。

[0105] 图10图示了可以执行本文所描述的示例实施例中的一些示例实施例的锚基站401A的一种示例节点配置。锚基站401A可以包括：可以被配置为接收和/或发射通信测量、数据、指令、和/或消息的无线电电路或通信端口410A。锚基站401A可以进一步包括：可以被配置为例如向其他网络节点和从其他网络节点接收或发送网络通信的网络接口电路440A。应当意识到，无线电电路或通信端口410A可以被包括作为任何数目的收发、接收、和/或发射单元或电路。应当进一步意识到，无线电电路或通信410A可以采用本领域中已知的任何输入或输出通信端口的形式。无线电电路或通信410A和/或网络接口440A可以包括RF电路和基带处理电路，它们的细节对熟悉于基站设计的人们而言是熟知的。

[0106] 锚基站401A还可以包括处理单元或电路420A，处理单元或电路420A可以被配置为执行与如本文所描述的对辅安全密钥(例如，用于辅eNB的安全密钥)的生成有关的操作。处理电路420A可以是任何合适类型的计算单元，例如微处理器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、或者专用集成电路(ASIC)、或者任何其他形式的电路。锚基站401A可以进一步包括存储器单元或电路430A，存储器单元或电路430A可以是任何适合类型的计算机可读存储器并且可以具有易失性和/或非易失性的类型。存储器430A可以被配置为存储所接收的、所发射的、和/或与安全密钥的生成有关的任何信息或新鲜度参数、设备参数、通信优先级、和/或可执行的程序指令。

[0107] 例如，当利用存储器430A中存储的适当程序代码被配置时，处理电路420A的典型功能包括对所发射的信号的调制和编码以及对所接收的信号的解调和解码。在本发明的若干实施例中，使用程序存储存储器430A中存储的适合程序代码将处理电路420A适配为，例如，执行上面所描述的用于处置双连接场景中的安全密钥的技术之一。当然，将意识到，并不是这些技术的步骤中的所有步骤都必然在单个微处理器中或者甚至是在单个模块中被执行。

[0108] 将意识到，当利用程序和数据存储器430A中存储的程序代码被适配时，处理电路420A能够使用功能“模块”的布置来实施图8的过程流程(或者它的变型)，其中这些模块是在处理器电路420A上执行的计算机程序或者计算机程序的部分。因此，装置410A能够被理解为包括被配置为与辅基站进行通信的通信接口440A，并且进一步包括处理电路420A中所实施的若干功能模块。这些功能模块包括：生成模块，用于至少部分地基于锚基站密钥来生成用于辅基站的辅安全密钥；发送模块，用于使用接口电路向辅基站发送所生成的辅安全密钥，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端的数据流量进行加密；以及加密模块，用于使用锚基站密钥、或者从锚基站密钥导出的密钥，用于对当无线终端双连接到锚基站和辅基站时由锚基站发送给无线终端的数据进行加密。

[0109] 图11图示了可以执行本文所描述的示例实施例中的一些示例实施例的移动性管理节点505A(例如，MME、SGSN、S4-SGSN)的一种示例节点配置。移动性管理节点505A可以包括：可以被配置为接收和/或发射通信测量、数据、指令、和/或消息的接口电路或通信端口510A。应当意识到，无线电电路或通信端口510A可以被包括作为任何数目的收发、接收、和/或发射单元或电路。应当进一步意识到，无线电电路或通信510A可以采用本领域中已知的任何输入或输出通信端口的形式。接口电路或通信510A可以包括RF电路和基带处理电路(未示出)。

[0110] 移动性管理节点505A还可以包括处理单元或电路520A，处理单元或电路520A可以被配置为执行与如本文所描述的对辅安全密钥(例如，用于辅eNB的安全密钥)的生成有关的操作。处理电路520A可以是任何合适类型的计算单元，例如微处理器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、或者专用集成电路(ASIC)、或者任何其他形式的电路。移动性管理节点505A可以进一步包括存储器单元或电路530A，存储器单元或电路530A可以是任何适合类型的计算机可读存储器并且可以具有易失性和/或非易失性的类型。存储器530A可以被配置为存储所接收的、所发射的、和/或与安全密钥的生成有关的任何信息或新鲜度参数、设备参数、通信优先级、和/或用于由处理电路520A使用的可执行的程序指令。

[0111] 在本发明的若干实施例中，使用程序存储存储器530A中存储的适合程序代码将处理电路520A适配为，例如，执行上面所描述的用于处置双连接场景中的安全密钥的技术之一。当然，将意识到，并不是这些技术的步骤中的所有步骤都必然在单个微处理器中或者甚至是在单个模块中被执行。

[0112] 将意识到，当利用程序和数据存储器530A中存储的程序代码被适配时，处理电路520A能够使用功能“模块”的布置来实施图9的过程流程(或者它的变型)，其中这些模块是在处理器电路520A上执行的计算机程序或者计算机程序的部分。因此，装置510A能够被理解为包括被配置为与辅基站进行通信的通信接口540A，并且进一步包括处理电路520A中所实施的若干功能模块。这些功能模块包括：共享模块，用于与无线终端共享主安全密钥；生成模块，用于至少部分地基于主安全密钥来生成用于辅基站的辅安全密钥；以及发送模块，用于经由接口电路向辅基站发送所生成的辅安全密钥，以用于由辅基站在对被发送给无线终端的数据流量进行加密中或者在生成一个或多个附加辅安全密钥中使用，该一个或多个附加辅安全密钥用于对当无线终端双连接到锚基站和辅基站时由辅基站发送给无线终端

的数据流量进行加密。图12图示了可以被配置为执行本文所描述的示例方法中的一些示例方法的无线终端505B的一种示例节点配置。无线终端505B可以包括：可以被配置为接收和/或发射通信测量、数据、指令、和/或消息的接口电路或通信端口510B。应当意识到，无线电电路或通信端口510B可以被包括作为任何数目的收发、接收、和/或发射单元或电路。应当进一步意识到，无线电电路或通信510B可以采用本领域中已知的任何输入或输出通信端口的形式。接口电路或通信510B可以包括RF电路和基带处理电路(未示出)。

[0113] 无线终端505B还可以包括处理单元或电路520B，处理单元或电路520B可以被配置为执行与如本文所描述的对辅安全密钥(例如，用于辅eNB的安全密钥)的生成有关的操作。处理电路520B可以是任何合适类型的计算单元，例如微处理器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、或专用集成电路(ASIC)、或任何其他形式的电路。无线终端505B可以进一步包括存储器单元或电路530B，存储器单元或电路530B可以是任何适合类型的计算机可读存储器并且可以具有易失性和/或非易失性的类型。存储器530B可以被配置为存储所接收的、所发射的、和/或与安全密钥的生成有关的任何信息或新鲜度参数、设备参数、通信优先级、和/或可执行的程序指令。

[0114] 因此，在本发明的各种实施例中，处理电路(诸如处理电路520A和520B)以及它们的对应存储器电路530A和530B被配置为执行上面详细描述的技术中的一种或多种技术。其他实施例可以包括基站和/或包括一个或多个这种处理电路的其他网络节点。在一些情况中，利用一个或多个适合的存储器设备中所存储的适当程序代码来配置这些处理电路，以实施本文所描述的技术中的一种或多种技术。当然，将意识到，并不是这些技术的步骤中的所有步骤都必然在单个微处理器中或者甚至是在单个模块中被执行。

[0115] 本领域的技术人员将意识到，不偏离本发明的范围，可以对上面所描述的实施例做出各种修改。例如，尽管已经利用包括符合于3GPP所规定的LTE标准的通信系统的示例描述了本发明的实施例，但是应当注意，所提出的解决方案可以等同地良好地可应用到支持双连接的其他网络。上面所描述的具体实施例因此应当被考虑为是示例性的而不是限制本发明的范围。因为描述各组件或各技术的每一种可构想的组合当然是不可能的，所以本领域的技术人员将意识到，不偏离本发明的关键特性，本发明能够以除了本文具体阐述的那些方式之外的其他方式加以实施。目前的实施例因此在所有方面都将被考虑为是说明性的而不是局限性的。

[0116] 在本发明概念的各种实施例的目前描述中，将理解，本文所使用的专业用语仅用于描述特定实施例的目的，并且不意图为限制本发明概念。除非另有定义，本文所使用的所有术语(包括技术术语和科学术语)具有与这些发明的概念所属于的领域中的普通技术人员通常理解的相同含义。将进一步理解，诸如通常使用的词典中所定义的那些术语的术语应当解释为具有与它们在本说明书的上下文中和相关技术领域中的含义相一致的含义，并且将不在理想化或过于正式的意义上进行解释，除非本文明确地如此定义。

[0117] 当元件被称为“连接至”、“耦合至”、“响应于”另一个元件或者它们的变体时，它能够直接地连接至、耦合至、或响应于另一个元件或者可以存在中间元件。相对照地，当元件被称为“直接连接至”、“直接耦合至”、“直接响应于”另一个元件或者它们的变体时，不存在中间元件。自始至终，相似的标号指代相似的元件。此外，本文所使用的“耦合”、“连接”、“响应”或者它们的变体可以包括无线地耦合、连接、或响应。如本文所使用的，单数形式的“一

种”、“一个”或者“该”意图为也包括复数形式，除非上下文清楚地另有指示。公知的功能或构造可能为了简洁和/或清楚而没有被描述。术语“和/或”包括相关联的所列出的项目中的一个或多个项目的任何组合和所有组合。

[0118] 将理解，尽管术语第一、第二、第三等可能在本文中用来描述各种元件/操作，但是这些元件/操作不应当被这些术语限制。这些术语仅用来区分一个元件/操作与另一个元件/操作。因此，不偏离本发明概念的教导，一些实施例中的第一元件/操作可以在其他实施例中称为第二元件/操作。贯穿本说明书，相同的参考数字或相同的参考标志指示相同或类似的元件。

[0119] 如本文所使用的，术语“包括”、“包括有”、“包括了”、“包含”、“包含有”、“包含了”、“具有”、“含有”、“拥有”或者它们的变体是开放式的，并且包括一个或多个所陈述的特征、整数、元件、步骤、组件或功能，但是不排除一个或多个其他的特征、整数、元件、步骤、组件、功能或它们的组的存在或添加。此外，如本文所使用的，从拉丁短语“举例来说”衍生的通用缩写“例如”可以被用来引入或规定先前提到的项目的一般示例或多个示例，并且不意图为对这样的项目的限制。从拉丁短语“也就是”衍生的通用缩写“即”可以被用来规定来自更一般记载的特定项目。

[0120] 在本文中参考计算机实施的方法、装置(系统和/或设备)和/或计算机程序产品的框图和/或流程图图示描述了示例实施例。要理解的是，框图和流程图图示的框，以及框图和流程图图示的框的组合，能够由一个或多个计算机电路执行的计算机程序指令来实施。这些计算机程序指令可以被提供给通用计算机电路、专用计算机电路、和/或其他可编程数据处理电路的处理器电路，以产生一种机器，使得经由该计算机和/或其他可编程数据处理装置的处理器执行的这些指令变换和控制晶体管、存储器位置中所存储的值、以及这种电路中的其他硬件组件，以实施这些框图和/或流程图框或多个框中所规定的功能/动作，并且由此创建用于实施这些框图和/或(多个)流程图框中所规定的功能/动作的装置(功能)和/或结构。

[0121] 这些计算机程序指令还可以存储在有形的计算机可读介质中，该有形的计算机可读介质能够指引计算机或其他可编程数据处理装置以特定的方式运转，使得该计算机可读介质中存储的指令产生一种制品，该制品包括实施这些框图和/或流程图框或多个框中所规定的功能/动作的指令。相应地，本发明概念的实施例可以具体化在硬件中和/或具体化在处理器(诸如数字信号处理器)上运行的软件中，它们可以统称为“电路”、“模块”或者它们的变体。

[0122] 还应当注意，在一些替换实施方式中，各框中指出的功能/动作可以不按流程图中指出的顺序发生。例如，取决于所涉及的功能/动作，连续示出的两个框可能事实上基本并发地被执行，或者各框有时可以以相反的顺序来执行。此外，流程图和/或框图的给定框的功能可以分开到多个框中，和/或流程图和/或框图中的两个或更多框的功能可以至少部分地被集成。最后，其他框可以被添加/插入在所图示的框之间，并且/或者不偏离本发明概念的范围，各框/各操作可以被省略。此外，尽管附图中的一些附图包括在通信路径上的箭头以示出通信的主要方向，但是将理解，通信也可以发生在与所描绘的箭头相反的方向上。

[0123] 不实质地偏离本发明概念的原理，能够对各实施例做出许多变化和修改。所有这样的变化和修改在本文中意图为包括在本发明概念的范围内。因此，上面所公开的主题将

考虑为是说明性的，并且不是局限性的，并且所附实施例的示例意图为覆盖所有这样的修改、增强、以及落在本发明概念的精神和范围内的其他实施例。因此，到法律所允许的最大程度，本发明概念的范围将由本公开内容的最宽的可准许解释来确定，并且不应该被前述的详细描述局限或限制。

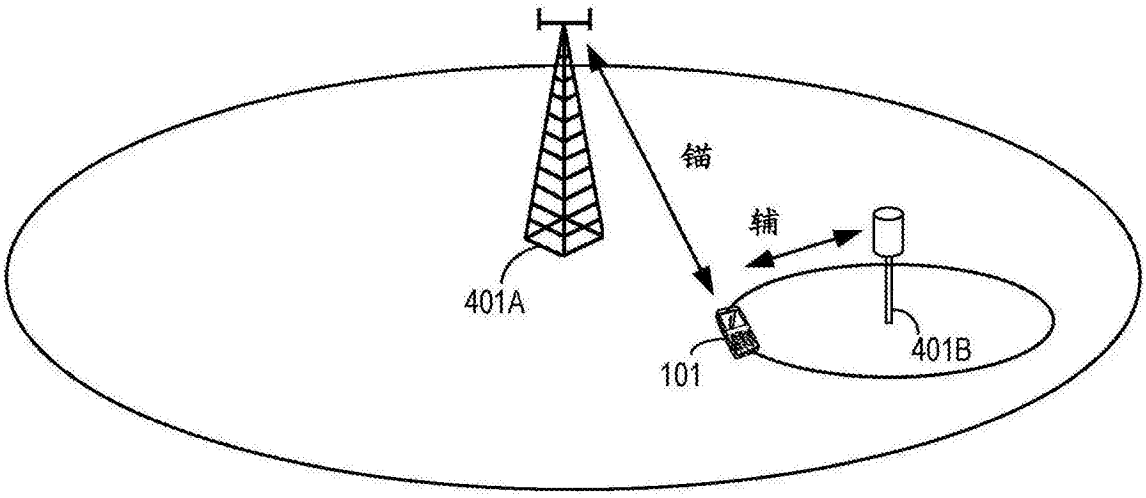

锚
辅
401A
401B
101

图1

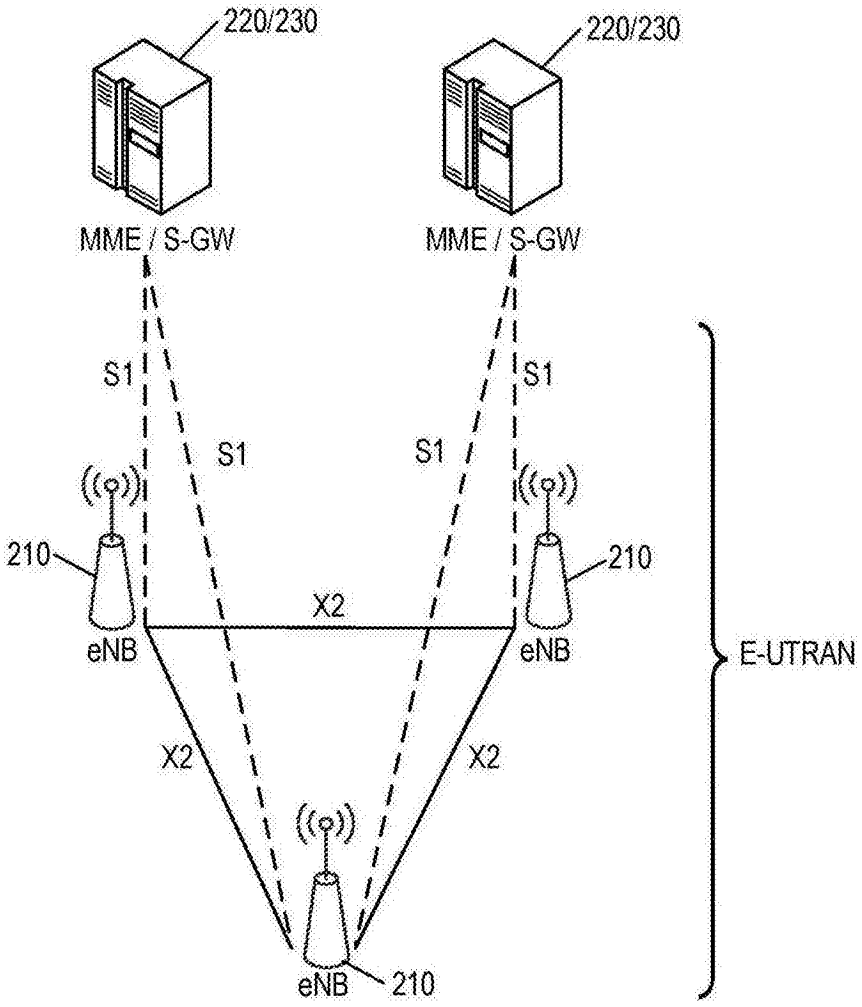

220/230
220/230
MME / S-GW
MME / S-GW
S1
S1
S1
S1
210
210
X2
eNB
eNB
X2
X2
eNB
210
E-UTRAN

图2

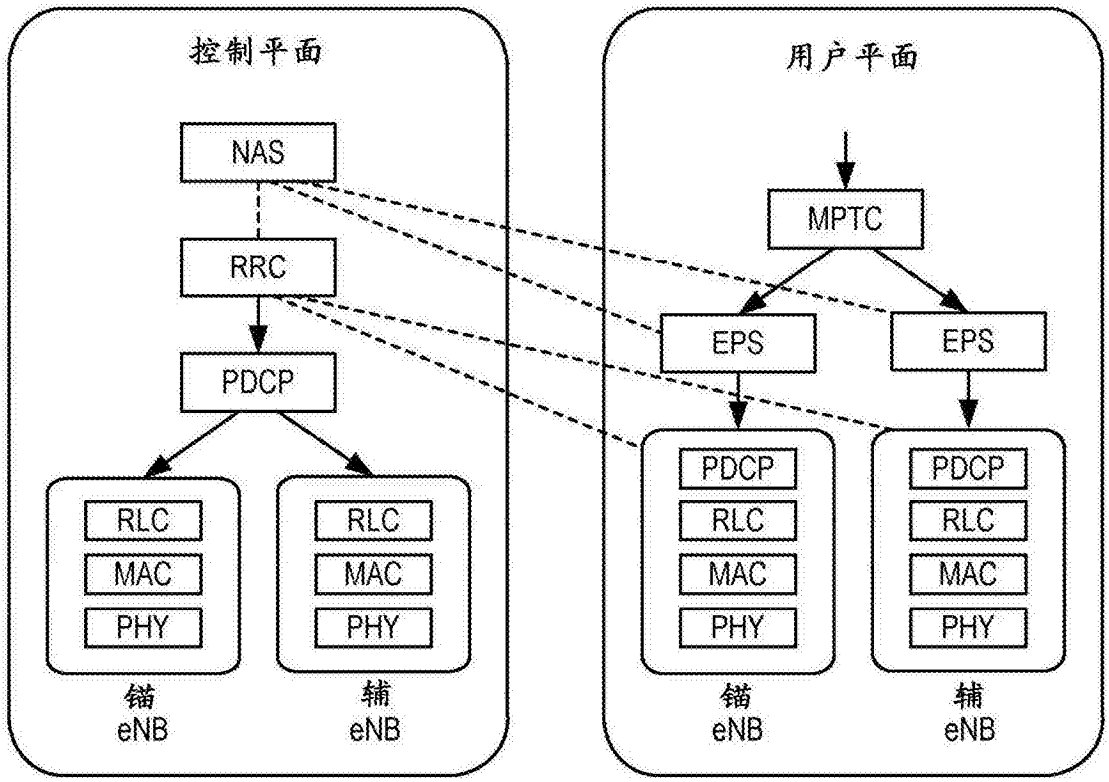

控制平面
用户平面
NAS
RRC
PDCP
RLC
MAC
PHY
RLC
MAC
PHY
锚
eNB
辅
eNB
MPTC
EPS
EPS
PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
锚
eNB
辅
eNB

图3

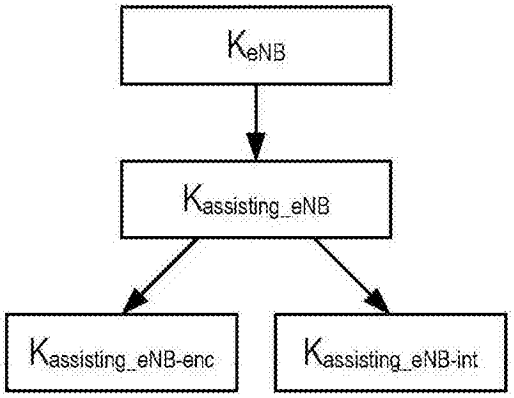

KeNB
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

图4

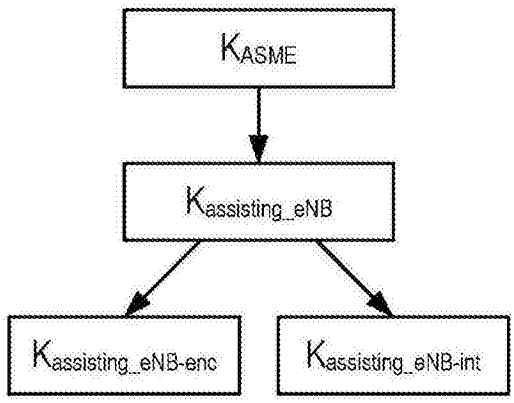

KASME
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

图5

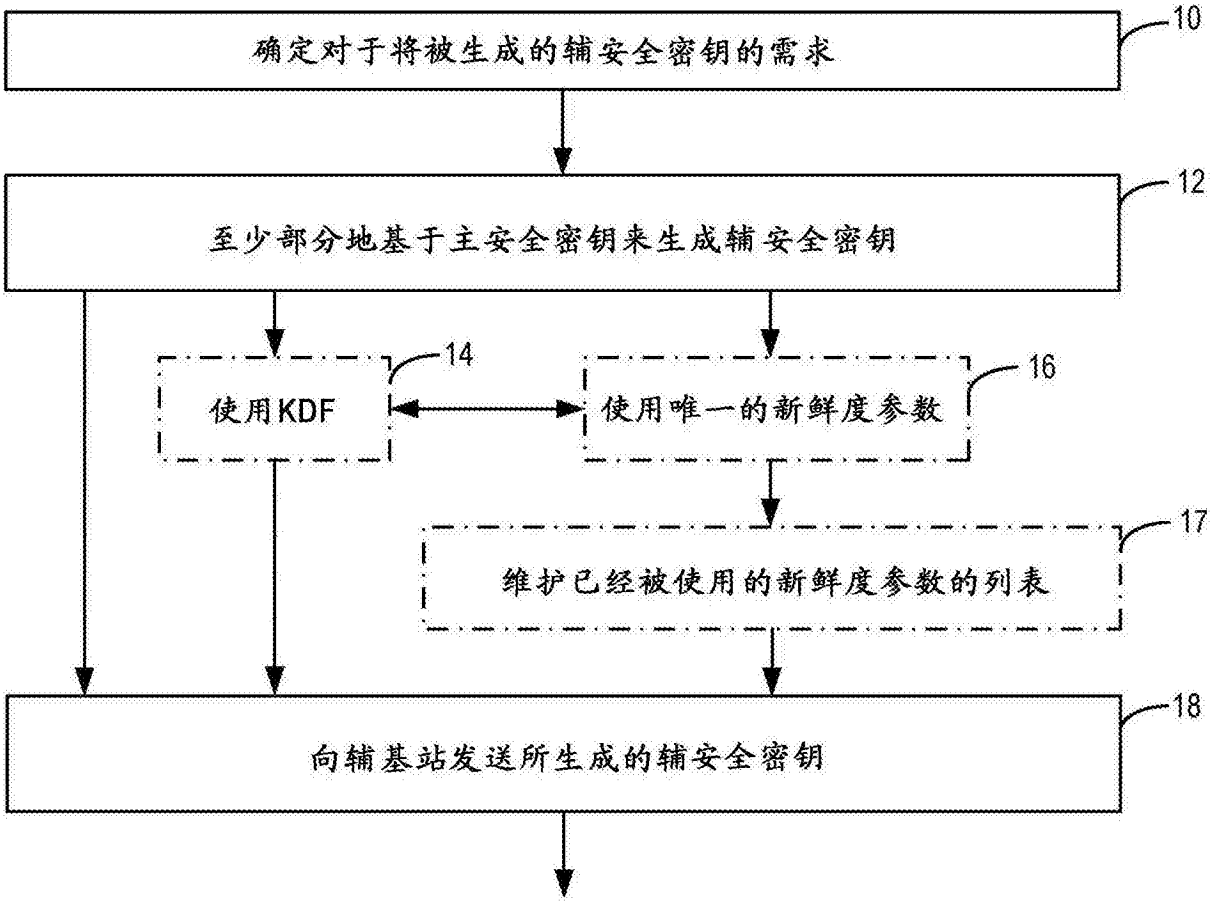

确定对于将被生成的辅安全密钥的需求
10
至少部分地基于主安全密钥来生成辅安全密钥
12
使用KDF
14
使用唯一的新鲜度参数
16
维护已经被使用的新鲜度参数的列表
17
向辅基站发送所生成的辅安全密钥
18

图6

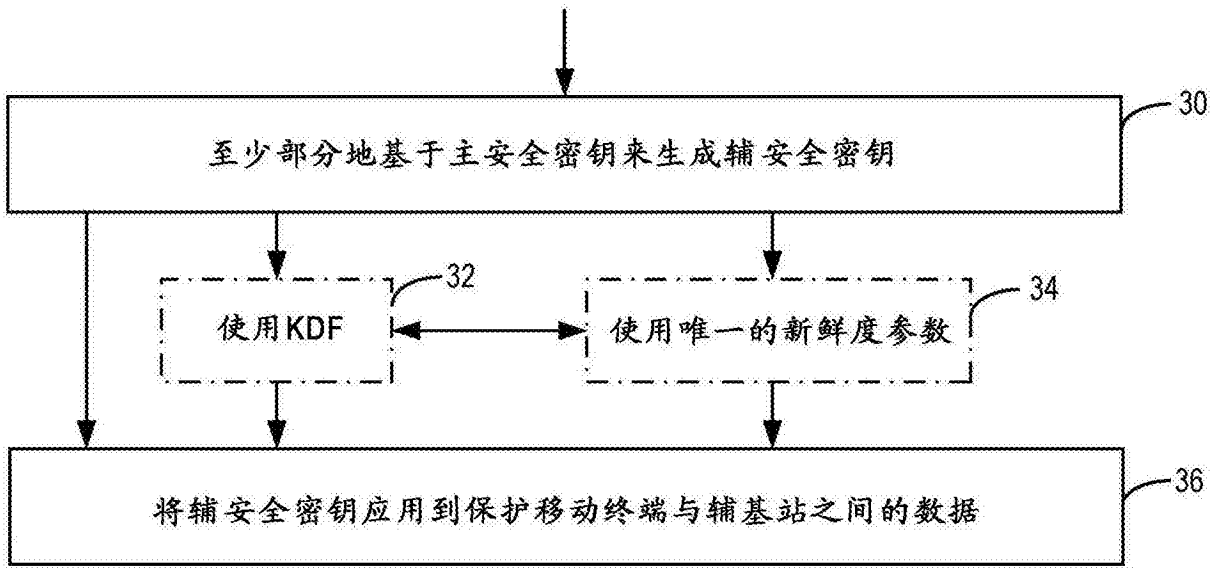

至少部分地基于主安全密钥来生成辅安全密钥
30
使用KDF
32
使用唯一的新鲜度参数
34
将辅安全密钥应用到保护移动终端与辅基站之间的数据
36

图7

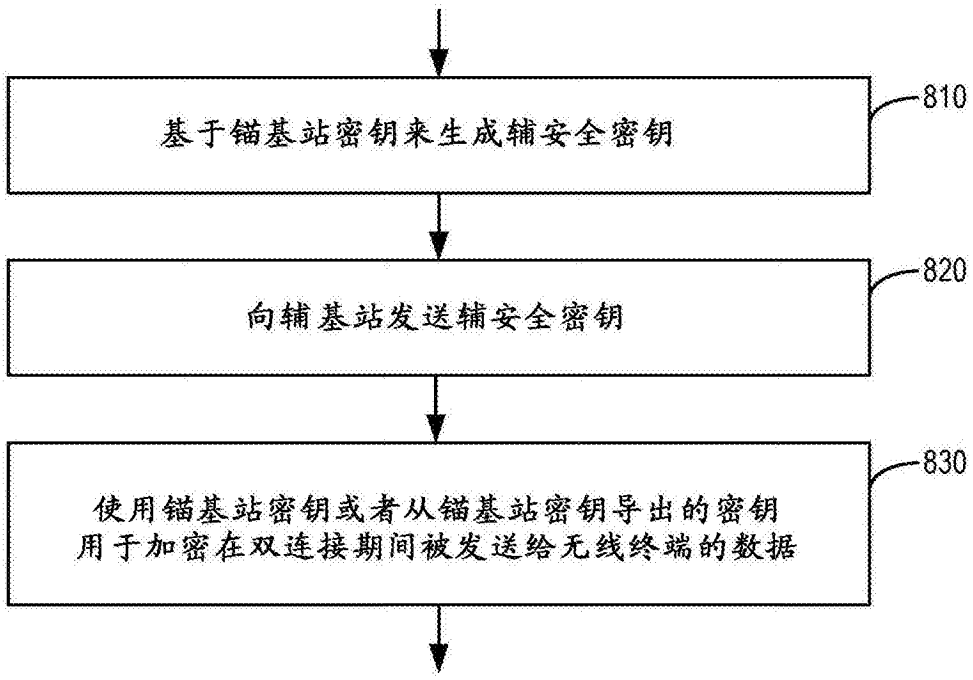

基于锚基站密钥来生成辅安全密钥
810
向辅基站发送辅安全密钥
820
使用锚基站密钥或者从锚基站密钥导出的密钥
用于加密在双连接期间被发送给无线终端的数据
830

图8

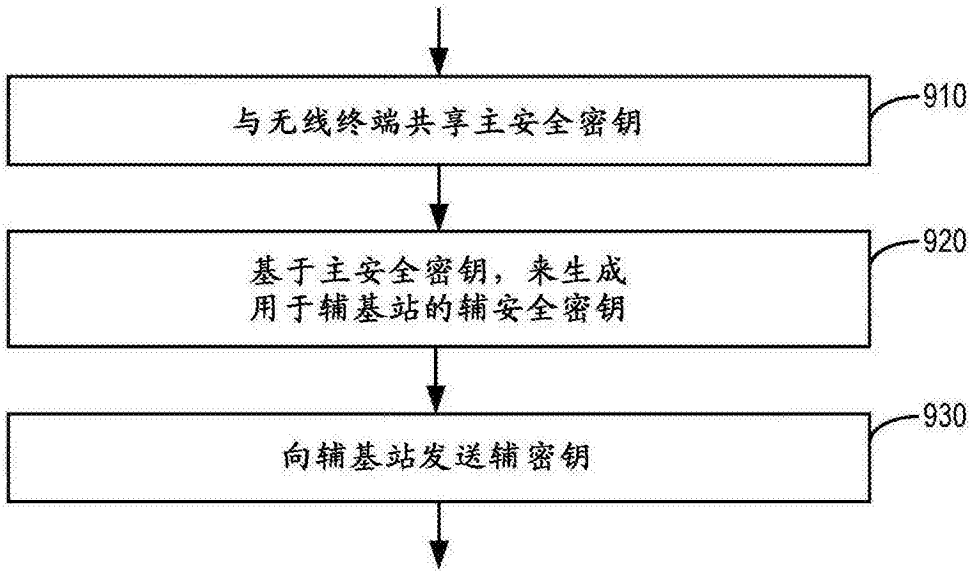

与无线终端共享主安全密钥
910
基于主安全密钥，来生成
用于辅基站的辅安全密钥
920
向辅基站发送辅密钥
930

图9

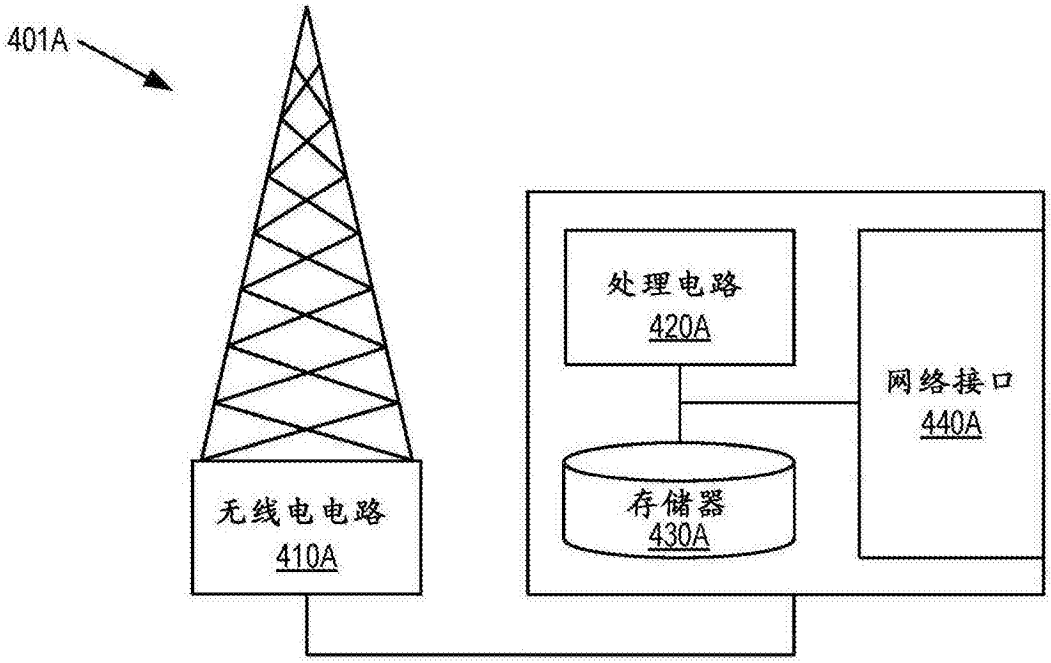

401A
无线电电路
410A
处理电路
420A
存储器
430A
网络接口
440A

图10

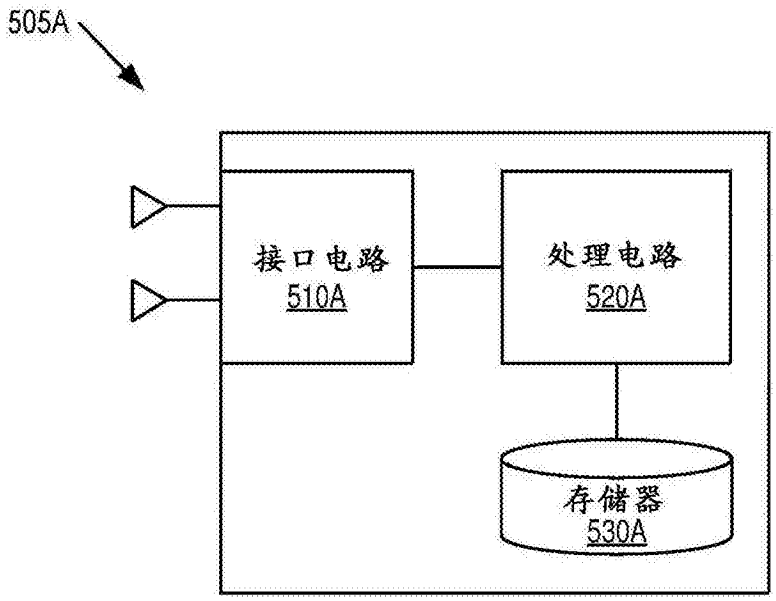

505A
接口电路
510A
处理电路
520A
存储器
530A

图11

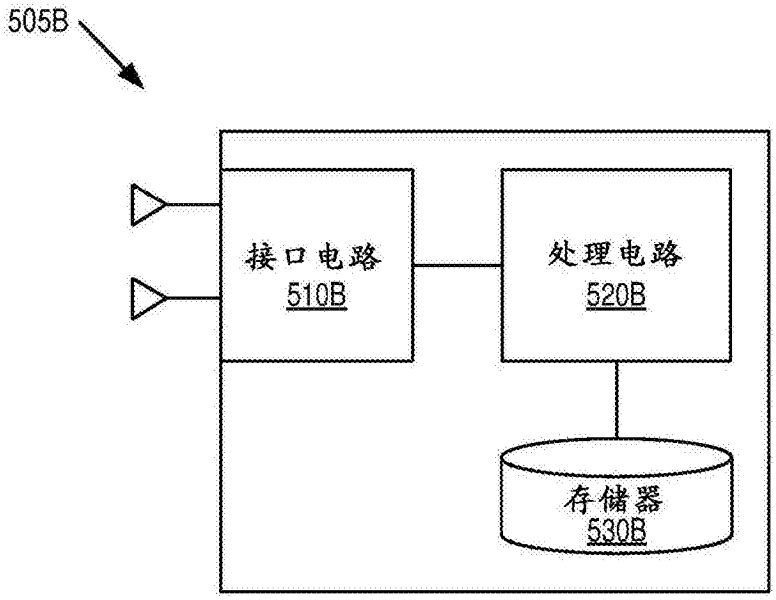

505B
接口电路
510B
处理电路
520B
存储器
530B

图12