(12) 按照专利合作条约所公布的国际申i青

(19) 世界知识产权组织
, 国际局
三(43) 国际公布日
2018 年 4 月 5 日 (05.04.2018)

爹
WIPO | PCT

(10) 国际公布号
WO 2018/058687 A1

(51) 国际专利分类号三:
H04W 24/10 (2009.01)

(21) 国际申请号:
PCT/CN2016/101410

(22) 国际申请日:
2016 年 9 月 30 日 (30.09.2016)

(25) 申请语言:
中文

(26) 公布语言:
中文

(71) 申请人:华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN];中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人:徐海博 (XU, Haibo);中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。王学龙 (WANG, Xuelong);中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。坦尼纳坦·爱德华 (TENNY, Nathan, Edward);中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。尤心 (YOU, Xin);中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人:北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT & TRADEMARK AGENT LTD.);中国北京市海淀区交大东路31号11号楼8层, Beijing 100044 (CN)。

(81) 指定国 (除另有指明,要求每一种可提供的国家保护):AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明,要求每一种可提供的地区保护):ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

(54) Title: METHOD, DEVICE AND SYSTEM FOR PROCESSING CONTROL SIGNALLING

(54) 发明名称:一种处理控制信令的方法、设备及系统

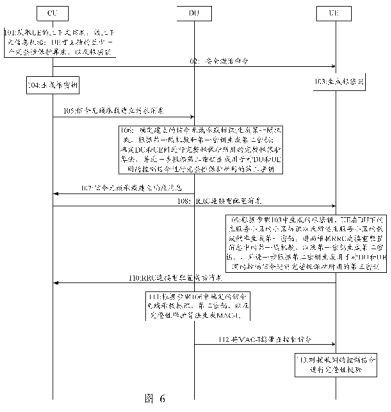

图 6

101 Acquiring context information about a UE, wherein the context information comprises: at least one integrity protection algorithm that can be supported by a UE, and a root key
102 Security activation command
103 Generating a root key
104 Generating a root key
105 Signalling radio bearer establishment request message
106 Determining an identifier of an established signalling radio bearer; generating a first random number; generating a second key according to the first random number and the first key; determining an integrity protection algorithm used for integrity protection between the DU and the UE, and further generating, according to the second key, a third key for performing integrity protection on control signalling between the DU and the UE
107 Signalling radio bearer establishment response message
108 RRC connection reconfiguration message
109 Generating a first key according to the root key generated in step 103, a cell identifier of a primary se ll of the UE under the DU a e carrier frequency of the primary ser ce generating a second key ac ng to the first random number in the RRC c on reconfiguration messag the first key; and further generating, according to the second key, a third key for performing integrity protection on the control signalling between the DU and the UE
110 RRC connection reconfiguration success message
111 Generating an MAC-I according to the signalling radio bear identifier, the second key and the integrity protection algorithm determined in step 106
112 Carrying the MAC-I in the control signalling
113 Performing integrity check on the received control signalling

(57) Abstract: A method, device and system for processing control signalling, which relate to the technical field of communications and solve the problem of performing integrity protection on control signalling interacted between a DU and a UE under a CU-DU-separated access network architecture. The method comprises: a DU determines an integrity protection parameter and an integrity protection algorithm, wherein the integrity protection parameter and the integrity protection algorithm are used for integrity protection of a signalling radio bearer between the DU and the UE; the DU determines a message authentication code (MAC-I) according to the integrity protection parameter and the integrity protection algorithm; and the DU receives control signalling sent by an RRC layer of the DU, and carries the MAC-I in the control signalling and sends same to the UE.

(57) 摘要:一种处理控制信令的方法、设备及系统,涉及通信技术领域,以解决在CU-DU分离的接入网架构下,对DU和UE之间交互的控制信令进行完整性保护的问题。该方法包括:DU确定完整性保护参数、以及完整性保护算法,完整性保护参数和完整性保护算法用于对DU与UE间的信令无线承载进行完整性保护;DU根据完整性保护参数、以及完整性保护算法确定消息鉴权码MAC-I;DU接收DU的RRC层发送的控制信令,将MAC-I携带在控制信令内向UE发送。

WO 2018/058687 A1

[见续页]

NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚（AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

- 包括国际检索报告（条约第21条(3)）。

一种处理控制信令的方法、设备及系统

技术领域

本发明涉及通信技术领域,尤其涉及一种处理控制信令的方法、设备及系统。

背景技术

目前,第三代合作伙伴计戈(英文:3rd Generation Partnership Proj ect, 3GPP)已经开始讨论面向第五代移动通信技术(英文5th-Generation, 5G)应用的网络架构,该网络架构包括接入网和核心网。其中,为了提高数据传输容量,一种接入网架构是分层架构,即接入网有两种网元组成,一个为中心单元(英文:Central Unit, CU),另一个为分布单元(英文:Distributed Unit, DU),一个CU下面会连接多个DU,一个DU下面会连接会连接多个用户设备(英文User Equipment, UE)。在这种接入网架构中,一种可能的CU和DU间的控制面协议栈的划分如图1所示,CU包括无线资源控制协议(英文:Radio Resource Control, RRC)层、分组数据汇聚协议(英文:Packet Data Convergence Protocol, PDCP)层,DU包括:无线链路控制(英文:Radio Link Control, RLC)层、媒体接入控制(英文:Medium Access Control, MAC)层以及物理层(英文:Physical layer)。

在这种接入网架构中,如果只有CU具备无线资源控制/管理功能,会存在以下两方面的问题:1)当需要在CU和UE之间传输控制信令时,CU和DU间的非理想链路会导致控制信令的传输时延加大;2)当UE在不同的DU之间移动时,CU需要通过DU来传输和UE之间的控制信令,例如,DU会将UE的测量结果上报至CU,由CU通过DU向UE发送切换信令控制UE的切换,此时,CU和DU间的控制信令的传递会导致信令开销的增加。

为解决上述两个问题,一种方法是将CU的部分无线资源控制

功能下放到DU，例如：当UE在同一个CU下的不同DU之间切换时，可以直接由DU来控制，而不需要将测量结果通过DU上报给CU，再将CU产生的切换命令通过DU传递给UE。虽然这种方法可以解决上述两方面问题，但是，为了实现DU侧的控制功能，需要定义DU和UE之间交互的控制信令，并且对这些控制信令需要进行完整性保护的处理，而在这种CU-DU分离的接入网架构下，如何对DU和UE之间交互的控制信令进行完整性保护目前尚未有解决办法。

发明内容

本申请提供一种对控制信令进行完整性保护的方法、设备及系统，以解决在CU-DU分离的接入网架构下，对DU和UE之间交互的控制信令进行完整性保护的问题。

为达到上述目的，本申请采用如下技术方案：

第一方面，提供一种处理控制信令的方法，该可以应用于包括第一网络设备和第二网络设备的接入网架构，第一网络设备下可以下挂多个第二网络设备，第二网络设备下可以下挂多个用户设备UE，由第二网络设备执行，第二网络设备可以包括第一协议层实体和第二协议层实体，该方法可以包括：

第二网络设备与用户设备UE间建立信令无线承载，并通过信令无线承载传输第二网络设备与UE间的控制信令，第二网络设备的第一协议层实体确定对控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法，触发第二网络设备的第二协议层实体根据完整性保护参数、以及完整性保护算法确定消息鉴权码MAC-I，第二网络设备的第二协议层实体接收第二网络设备的第一协议层实体发送的控制信令，将MAC-I携带在控制信令内向UE发送。

其中，第一网络设备可以为位于中心机房的中心单元，如：基带处理单元，第二网络设备可以为距离UE比较近的分布单元，如：射频拉远单元，第二网络设备的第一协议层实体可以为无线资源控

制协议 RRC 层，第二网络设备的第二协议层实体可以为分组汇聚数据协议 PDCP 层。

如此，第二网络设备可以通过自身内置的第一协议层实体、以及第二协议层实体实现对第二网络设备与 UE 间控制信令的交互，并对控制信令进行完整性保护。当第一网络设备为 CU，第二网络设备为 DU 时，实现了 CU-DU 分离的接入网架构中，DU 对 DU 与 UE 间交互的控制信令进行完整性保护的功能。

可选的，上述完整性保护参数可以包括但不限于：信令无线承载标识、以及第二网络设备与 UE 间的信令无线承载进行完整性保护所用的第三密钥；

在第一方面的一种可实现方式中，结合第一方面，可以通过下述方式获取上述完整性保护参数以及完整性保护算法：

在第二网络设备与用户设备 UE 间建立信令无线承载之前，第二网络设备接收第一网络设备发送的用于请求第二网络设备与 UE 间建立信令无线承载的信令无线承载建立请求，并确定信令无线承载标识，该信令无线承载建立请求可以包含：第一密钥以及 UE 可支持的至少一个完整性保护算法；

第二网络设备的第一协议层实体获取第一网络设备发送的第一密钥，以及 UE 可支持的至少一个完整性保护算法；

第二网络设备的第一协议层实体生成第一随机数；

第二网络设备的第一协议层实体根据第一随机数以及第一密钥生成第二密钥，根据第二密钥生成第二网络设备与 UE 间的信令无线承载进行完整性保护所用的第三密钥；

第二网络设备的第一协议层实体从 UE 可支持的至少一个完整性保护算法中确定完整性保护算法。

其中，第一由第一网络设备根据 UE 在第二网络设备下的主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成。

所述根密钥可以用于产生对 CU 和 UE 间的控制信令进行完整性保护所用的密钥。

如此，第二网络设备可以获取到进行完整性保护所需要的完整性保护参数和完整性保护算法。

相对应的，对于对端 UE 而言，需要上述完整性保护参数和完整性保护算法对接收到的控制信令进行完整性校验，此时，第二网络设备可以直接将进行完整性保护所需要的完整性保护参数和完整性保护算法发送至 UE，也可以通过第一网络设备将进行完整性保护所需要的完整性保护参数和完整性保护算法发送至 UE。

具体的，在第一方面的一种可实现方式中，结合第一方面或第一方面的任一种可实现方式，该方法还可以包括：

第二网络设备向第一网络设备返回信令无线承载建立响应消息，信令无线承载建立响应消息包含：信令无线承载标识、第一随机数、以及完整性保护算法；

在该实现方式中，信令无线承载建立请求可以包含：第一密钥以及 UE 可支持的至少一个完整性保护算法。

在第一方面的又一种可实现方式中，结合第一方面或第一方面的任一种可实现方式，所述方法还可以包括：

第二网络设备向第一网络设备返回包含：信令无线承载标识的信令无线承载建立响应消息；

第二网络设备接收第一网络设备发送的包含：第一密钥、以及 UE 可支持的至少一个完整性保护算法的 UE 的安全上下文建立请求消息；

第二网络设备向第一网络设备返回安全上下文建立响应消息；

第二网络设备的第一协议层实体从 UE 可支持的至少一个完整性保护算法中确定完整性保护算法

第二网络设备的第一协议层实体向 UE 发送安全激活消息，安全激活消息包含：第一随机数以及完整性保护算法。

如此，可以通过第一网络设备或者第二网络设备将进行完整性保护所需要的完整性保护参数或者进一步衍生出完整性保护所需要的完整性保护参数的参数、以及完整性保护算法发送至对端 UE。

进一步的，在某些情况下（如下述情况一或二），DU与UE间进行完整性保护所需要的密钥会发生更新：一、根密钥发生；二、DU与UE间需要密钥更新时，如：随机数发生变化，此时，不论在哪种情况下发生密钥更新，DU和UE双发都需要根据更新情况同时进行密钥的变更，以避免进行完整性保护时需要的完整性保护参数不一致导致的完整性保护失败。

具体的，在第一方面的再一种可实现方式中，结合第一方面或第一方面的任一种可实现方式，若根密钥发生变化，则所述方法还可以包括：

第二网络设备接收第一网络设备发送的包含根据变化后的根密钥生成的新的第一密钥的密钥更新请求消息；

第二网络设备的第一协议层实体生成第二随机数；

第二网络设备的第一协议层实体向UE发送密钥修改请求消息，密钥修改请求消息包含第二随机数；

第二网络设备的第一协议层实体接收UE返回的密钥修改响应消息。

在第一方面的再一种可实现方式中，结合第一方面或第一方面的任一种可实现方式，该方法还可以包括：

第二网络设备的第一协议层实体生成第三随机数；该第三随机数可以与原有的第一随机数相同，也可以不相同；

第二网络设备的第一协议层实体向UE发送密钥修改请求消息，密钥修改请求消息包含第三随机数；

第二网络设备的第一协议层实体接收UE返回的密钥修改响应消息。

如此，在密钥发生变化的情况下，DU与UE两端及时更新进行完整性保护所需的密钥，以避免完整性保护失败的问题。

第二方面，提供一种处理控制信令的方法，由用户设备UE执行，该方法可以包括：

UE与第二网络设备间建立信令无线承载，并通过信令无线承载

传输UE与第二网络设备间的控制信令，UE确定对控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；UE接收第二网络设备的第二协议层实体发送的携带有消息鉴权码MAC-I的控制信令，UE根据完整性保护参数、以及完整性保护算法，对控制信令进行完整性校验。

其中，UE根据完整性保护参数、以及完整性保护算法对控制信令进行完整性校验可以包括：

UE根据完整性保护参数、以及完整性保护算法获得MAC-I，将获得到MAC-I与接收到的控制信令中的MAC-I进行比较，若二者相同，则表示完整性校验成功，若二者不同，则表示完整性校验失败。

如此，UE可以通过获得的完整性保护参数、以及完整性保护算法对接收到的DU发出的控制信令进行完整性保护校验，实现了UE和DU间控制信令的完整性保护。

可选的，上述完整性保护参数可以包括但不限于：第二网络设备与UE间的信令无线承载标识、以及对第二网络设备与UE间的信令无线承载进行完整性保护所用的第三密钥；

在第二方面的一种可实现方式中，结合第二方面，UE可以从第一网络设备发送的消息中确定出完整性保护参数、以及完整性保护算法，具体实现如下：

UE接收第一网络设备发送的包含对第一网络设备和UE间的信令无线承载进行完整性保护所用的完整性保护算法的、用于激活对第一网络设备和UE间的信令无线承载执行完整性保护的安全激活命令；

UE根据安全激活命令，生成根密钥；

UE接收第一网络设备发送的无线资源控制RRC连接重配置消息，从RRC连接重配置消息中获取用户设备和第二网络设备间的信令无线承载标识、第一随机数以及完整性保护算法，并建立与第二网络设备间的信令无线承载；第一随机数由第二网络设备生成，完

整性保护算法由第二网络设备从 UE 可支持的至少一个完整性保护算法中选择；

UE 根据根密钥生成第一密钥；

UE 根据第一随机数以及第一密钥生成第二密钥，根据第二密钥生成第二网络设备与 UE 间的信令无线承载进行完整性保护所用的第三密钥。

在第二方面的又一种可实现方式中，结合第二方面，UE 可以直接从第二网络设备发送的消息中确定出完整性保护参数以及完整性保护算法，具体实现如下：

UE 接收第一网络设备发送的包含对第一网络设备和 UE 间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对第一网络设备和 UE 间的信令无线承载执行完整性保护的安全激活命令；

UE 根据安全激活命令，生成根密钥；

UE 接收第一网络设备发送的无线资源控制 RRC 连接重配置消息，从 RRC 连接重配置消息中获取第二网络设备与 UE 间的信令无线承载标识；

UE 接收第二网络设备发送的安全激活消息，从安全激活消息中获取第一随机数以及完整性保护算法；第一随机数由第二网络设备生成，完整性保护算法由第二网络设备从 UE 可支持的至少一个完整性保护算法中选择；

UE 根据根密钥生成第一密钥；

UE 根据第一随机数以及第一密钥生成第二密钥，根据第二密钥生成第二网络设备与 UE 间的信令无线承载进行完整性保护所用的第三密钥。

可选的，在上述两种方式中，UE 根据根密钥生成第一密钥可以包括：

UE 根据 UE 在第二网络设备下的主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成第一密钥。

如此,UE可以从第一网络设备或者第二网络设备获取到用于衍生出DU与UE间进行完整性保护所需要的密钥的随机数、信令无线承载标识、以及确定出完整性保护算法。

进一步的,与第一方面雷同,在某些情况下(如下述情况一或二),DU与UE间进行完整性保护所需要的密钥会发生更新:一、根密钥发生;二、DU与UE间需要密钥更新时,如:随机数发生变化,此时,不论在哪种情况下发生密钥更新,DU和UE双发都需要根据更新情况同时进行密钥的变更,以避免进行完整性保护时需要的完整性保护参数不一致导致的完整性保护失败。

具体的,在第二方面的再一种可实现方式中,结合第二方面或第二方面的任一种可实现方式,若根密钥发生变化,则所述方法还可以包括:

UE生成新的根密钥;

UE接收第二网络设备发送的密钥修改请求消息,密钥修改请求消息包含第二随机数;

UE根据新的根密钥生成新的第一密钥;

UE根据第二随机数以及新的第一密钥生成新的第二密钥,根据新的第二密钥生成第二网络设备与UE间的信令无线承载进行完整性保护所用的新的第三密钥,

UE向第二网络设备返回密钥修改响应消息。

在第二方面的再一种可实现方式中,结合第二方面或第二方面的任一种可实现方式,该方法还可以包括:

UE接收第二网络设备发送的密钥修改请求消息,密钥修改请求消息包含第三随机数;

UE根据第三随机数以及第一密钥生成新的第二密钥,根据新的第二密钥生成第二网络设备与UE间的信令无线承载进行完整性保护所用的新的第三密钥,

UE向第二网络设备返回密钥修改响应消息。

如此,在密钥发生变化的情况下,DU与UE两端及时更新进行

完整性保护所需的密钥，以避免完整性保护失败的问题。

第三方面，提供一种处理控制信令的方法，由第一网络设备执行，该方法可以包括：

第一网络设备获取包括：根密钥、以及UE可支持的至少一个完整性保护算法的UE的上下文信息，向UE发送包含对第一网络设备和UE间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对第一网络设备和UE间的信令无线承载执行完整性保护的安全激活命令，向第二网络设备发送用于请求第二网络设备与UE间建立信令无线承载的信令无线承载建立请求，接收第二网络设备返回的信令无线承载建立响应消息，向UE发送用于建立第二网络设备与UE间的信令无线承载的无线资源控制RRC连接重配置消息，接收UE返回的RRC连接重配置成功消息。

如此，第一网络设备可以向UE和第二网络设备发送衍生出完整性保护所需要的完整性保护参数的密钥、以及多个可选的完整性保护算法，以便UE和第二网络设备可以根据接收到密钥、以及多个完整性保护算法，确定出进行完整性保护最终需要的完整性保护参数、以及完整性保护算法，实现第二网络设备与UE间的完整性保护功能。

在第三方面的一种可实现方式中，结合第三方面，所述方法还可以包括：

在第一网络设备向第二网络设备发送信令无线承载建立请求之前，第一网络设备根据根密钥生成第一密钥；

在该实现方式中，信令无线承载建立请求包含第一密钥、以及UE可支持的至少一个完整性保护算法；信令无线承载建立响应消息、以及RRC连接重配置消息包含：第一随机数、信令无线承载标识以及完整性保护算法。

在第三方面的一种可实现方式中，结合第三方面，所述方法还可以包括：

在第一网络设备接收UE返回的RRC连接重配置成功消息之

后，第一网络设备根据根密钥生成第一密钥；

第一网络设备向第二网络设备发送安全上下文建立请求消息；安全上下文建立请求消息包含：第一密钥、以及 UE 可支持的至少一个完整性保护算法；

第一网络设备接收第二网络设备返回的安全上下文建立响应消息。

在该可实现方式中，信令无线承载建立响应消息、以及 RRC 连接重配置消息包含信令无线承载标识。

可选的，在上述两种可实现方式中，第一网络设备根据根密钥生成第一密钥可以包括：

第一网络设备根据 UE 在第二网络设备下的主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成第一密钥。

如此，第一网络设备可以根据根密钥生成用于衍生出第二网络设备与 UE 间进行完整性保护所需要的密钥的第一密钥。

第四方面，提供一种完整性保护算法，该可以应用于包括第一网络设备和第二网络设备的接入网架构，第一网络设备下可以下挂多个第二网络设备，第二网络设备下可以下挂多个用户设备 UE，由第二网络设备执行，第二网络设备可以第一协议层实体，该方法可以包括：

第二网络设备的第一协议层实体产生第二网络设备和 UE 间的控制信令，第二网络设备的第一协议层实体确定用于对控制信令进行完整性保护的完整性保护参数、以及完整性保护算法，根据完整性保护参数、以及完整性保护算法确定消息鉴权码 MAC-I，第二网络设备的第一协议层实体将 MAC-I 携带在控制信令内向 UE 发送。

其中，第一网络设备可以为位于中心机房的中心单元，如：基带处理单元，第二网络设备可以为距离 UE 比较近的分布单元，如：射频拉远单元，第一协议层实体为无线链路控制 RLC 层、或者媒体接入控制 MAC 层。

如此，第二网络设备可以通过自身原有控制协议栈中的 layer2

协议栈中的任意协议层实现对第二网络设备与UE间控制信令的交互，并对控制信令进行完整性保护。当第一网络设备为CU，第二网络设备为DU时，实现了CU-DU分离的接入网架构中，DU对DU与UE间交互的控制信令进行完整性保护的功能。

可选的，上述完整性保护参数可以包括但不限于：BEARER参数值、计数值、以及第二网络设备与UE间进行完整性保护所用的第三密钥；

在第四方面的一种可实现方式中，结合第四方面，可以通过下述方式获取上述完整性保护参数、以及完整性保护算法：

第二网络设备的第一协议层实体接收第一网络设备发送的包含：第一密钥、以及UE可支持的至少一个完整性保护算法的安全上下文建立请求消息；

第二网络设备的第一协议层实体生成第一随机数；

第二网络设备的第一协议层实体根据第一随机数以及第一密钥生成第二密钥，根据第二密钥生成第二网络设备与UE间进行完整性保护所用的第三密钥；

第二网络设备的第一协议层实体从UE可支持的至少一个完整性保护算法中确定出完整性保护算法。

其中，第一密钥由第一网络设备根据UE在第二网络设备下的主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成；

所述根密钥可以用于产生对CU和UE间的控制信令进行完整性保护所用的密钥。

如此，第二网络设备可以获取到进行完整性保护所需要的完整性保护参数和完整性保护算法。

相对应的，对于对端UE而言，需要上述完整性保护参数和完整性保护算法对接收到的控制信令进行完整性校验，此时，第二网络设备可以直接将进行完整性保护所需要的完整性保护参数和完整性保护算法发送至UE。

具体的，在第四方面的一种可实现方式中，结合第四方面或第

四方面的任一种可实现方式，该方法还可以包括：

第二网络设备的第一协议层实体向第一网络设备返回安全上下文建立响应消息；

第二网络设备的第一协议层实体向UE发送包含：第一随机数、BEARER 参数值以及完整性保护算法的安全激活消息。

进一步的，在某些情况下（如下述情况一或二），DU与UE间进行完整性保护所需要的密钥会发生更新：一、根密钥发生；二、DU与UE间需要密钥更新时，如：随机数发生变化，此时，不论在哪种情况下发生密钥更新，DU和UE双发都需要根据更新情况同时进行密钥的变更，以避免进行完整性保护时需要的完整性保护参数不一致导致的完整性保护失败。

具体的，在第四方面的又一种可实现方式中，结合第四方面或第四方面的任一种可实现方式，该方法还可以包括：

第二网络设备的第一协议层实体接收第一网络设备发送的密钥更新请求消息，密钥更新请求消息包含根据变化后的根密钥生成的新的第一密钥；

第二网络设备的第一协议层实体生成第二随机数；

第二网络设备的第一协议层实体向UE发送密钥修改请求消息，密钥修改请求消息包含第二随机数；

第二网络设备的第一协议层实体接收UE返回的密钥修改响应消息。

在第四方面的再一种可实现方式中，结合第四方面或第四方面的任一种可实现方式，该方法还可以包括：

第二网络设备的第一协议层实体生成第三随机数；

第二网络设备的第一协议层实体向UE发送密钥修改请求消息，密钥修改请求消息包含第三随机数；

第二网络设备的第一协议层实体接收UE返回的密钥修改响应消息。

如此，在密钥发生变化的情况下，DU与UE两端及时更新进行

完整性保护所需的密钥，以避免完整性保护失败的问题。

第五方面，提供一种处理控制信令的方法，由用户设备 UE 执行，该方法可以包括：

UE 确定用于对第二网络设备与 UE 间传输的控制信令进行完整性保护的完整性保护参数、以及完整性保护算法，接收第二网络设备的第一协议层实体发送的携带有消息鉴权码 MAC-I 的控制信令，UE 根据完整性保护参数、以及完整性保护算法，对控制信令进行完整性校验。

其中，UE 根据完整性保护参数、以及完整性保护算法对控制信令进行完整性校验可以包括：

UE 根据完整性保护参数、以及完整性保护算法获得 MAC-I，将获得到 MAC-I 与接收到的控制信令中的 MAC-I 进行比较，若二者相同，则表示完整性校验成功，若二者不同，则表示完整性校验失败。

如此，UE 可以通过获得的完整性保护参数、以及完整性保护算法对接收到的 DU 发出的控制信令进行完整性保护校验，实现了 UE 和 DU 间控制信令的完整性保护。

可选的，上述完整性保护参数可以包括但不限于：BEARER 参数值、计数值、以及第二网络设备与 UE 间进行完整性保护所用的第三密钥；

在第五方面的一种可实现方式中，结合第五方面，UE 可以从第二网络设备发送的消息中确定出完整性保护参数、以及完整性保护算法，具体实现如下：

UE 接收第一网络设备发送的包含对第一网络设备和 UE 间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对第一网络设备和 UE 间的信令无线承载执行完整性保护的安全激活命令；

UE 根据安全激活命令，生成根密钥；

UE 接收第二网络设备发送的安全激活消息，从安全激活消息中

获取第一随机数、BEARER 参数值以及完整性保护算法；第一随机数由第二网络设备生成，完整性保护算法由第二网络设备从 UE 可支持的至少一个完整性保护算法中选择；

UE 根据根密钥生成第一密钥；

UE 根据第一随机数以及第一密钥生成第二密钥，根据第二密钥生成第二网络设备与 UE 间的信令无线承载进行完整性保护所用的第三密钥。

可选的，在上述方式中，UE 根据根密钥生成第一密钥可以包括：

UE 根据 UE 在第二网络设备下的主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成第一密钥。

如此，UE 可以从第二网络设备获取到用于衍生出 DU 与 UE 间进行完整性保护所需要的密钥的随机数、信令无线承载标识、以及确定出完整性保护算法。

进一步的，与第一方面雷同，在某些情况下（如下述情况一或二），DU 与 UE 间进行完整性保护所需要的密钥会发生更新：一、根密钥发生；二、DU 与 UE 间需要密钥更新时，如：随机数发生变化，此时，不论在哪种情况下发生密钥更新，DU 和 UE 双发都需要根据更新情况同时进行密钥的变更，以避免进行完整性保护时需要的完整性保护参数不一致导致的完整性保护失败。

具体的，在第五方面的再一种可实现方式中，结合第五方面或第五方面的任一种可实现方式，所述方法还可以包括：

UE 生成新的根密码；

UE 接收第二网络设备发送的密钥修改请求消息，密钥修改请求消息包含第二随机数；

UE 根据新的根密钥生成新的第一密钥；

UE 根据第二随机数以及新的第一密钥生成新的第二密钥，根据新的第二密钥生成第二网络设备与 UE 间的信令无线承载进行完整性保护所用的新的第三密钥，

UE 向第二网络设备返回密钥修改响应消息。

在第五方面的再一种可实现方式中，结合第五方面或第五方面的任一种可实现方式，该方法还可以包括：

UE接收第二网络设备发送的密钥修改请求消息，密钥修改请求消息包含第三随机数；

UE根据第三随机数以及第一密钥生成新的第二密钥，根据新的第二密钥生成第二网络设备与UE间的信令无线承载进行完整性保护所用的新的第三密钥，

UE向第二网络设备返回密钥修改响应消息。

如此，在密钥发生变化的情况下，DU与UE两端及时更新进行完整性保护所需的密钥，以避免完整性保护失败的问题。

第六方面，提供一种处理控制信令的方法，由第一网络设备执行，该方法可以包括：

第一网络设备获取包括：根密钥、以及UE可支持的至少一个完整性保护算法的UE的上下文信息，向UE发送包含对第一网络设备和UE间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对第一网络设备和UE间的信令无线承载执行完整性保护的安全激活命令，根据根密钥生成第一密钥，向第二网络设备发送包含：第一密钥、以及UE可支持的至少一个完整性保护算法的安全上下文建立请求消息；第一网络设备接收第二网络设备返回的安全上下文建立响应消息。

如此，第一网络设备可以向UE和第二网络设备发送衍生出完整性保护所需要的完整性保护参数的密钥、以及多个可选的完整性保护算法，以便UE和第二网络设备可以根据接收到密钥、以及多个完整性保护算法，确定出进行完整性保护最终需要的完整性保护参数、以及完整性保护算法，实现第二网络设备与UE间的完整性保护功能。

在第六方面的一种可实现方式中，结合第六方面，第一网络设备根据根密钥生成第一密钥可以包括：

第一网络设备根据UE在第二网络设备下的主服务小区的小区

标识、主服务小区的载波频率、以及根密钥生成第一密钥。

如此，第一网络设备可以根据根密钥生成用于衍生出第二网络设备与UE间进行完整性保护所需要的密钥的第一密钥。

第七方面，本发明提供一种第二网络设备，该第二网络设备可以包括第一协议层实体和第二协议层实体，所述设备包括：

建立单元，用于与用户设备 UE 间建立信令无线承载，所述信令无线承载用于传输所述第二网络设备与所述UE间的控制信令；

第一确定单元，用于确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法，所述第一确定单元位于所述第一协议层实体；

第二确定单元，用于根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码 MAC-I，所述第二确定单元位于所述第二协议层实体；

接收单元，用于接收所述第二网络设备的第一协议层实体发送的控制信令；

发送单元，用于将所述 MAC-I 携带在所述控制信令内向所述UE发送。

其中，第七方面的具体实现方式可以参考第一方面或第一方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第七方面提供的第二网络设备可以达到与第一方面相同的有益效果。

第八方面，本发明提供一种第二网络设备，该第二网络设备可以包括第一协议层实体和第二协议层实体，所述设备与用户设备 UE 间建立信令无线承载，所述信令无线承载用于传输所述第二网络设备与所述UE间的控制信令；所述设备包括：

处理器，用于确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法，所述第一确定单元位于所述第一协议层实体；

以及，根据所述完整性保护参数、以及所述完整性保护算法确

定消息鉴权码 MAC-I ，所述第二确定单元位于所述第二协议层实体；

收发器，用于接收所述第二网络设备的第一协议层实体发送的控制信令；

以及，将所述 MAC-I 携带在所述控制信令内向所述 UE 发送。

其中，第八方面的具体实现方式可以参考第一方面或第一方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第八方面提供的第二网络设备可以达到与第一方面相同的有益效果。

第九方面，本发明提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第七方面或第八方面或上述任一种可能的实现方式所述的第二网络设备执行时，使第二网络设备执行以下事件：

与用户设备 UE 间建立用于传输所述第二网络设备与所述 UE 间的控制信令的信令无线承载，确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法，所述第一确定单元位于所述第一协议层实体，根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码 MAC-I ，所述第二确定单元位于所述第二协议层实体，接收所述第二网络设备的第一协议层实体发送的控制信令，将所述 MAC-I 携带在所述控制信令内向所述 UE 发送。

其中，第九方面的具体实现方式可以参考第一方面或第一方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第九方面提供的第二网络设备可以达到与第一方面相同的有益效果。

第十方面，提供一种 UE，所述 UE 可以包括：

建立单元，用于与第二网络设备间建立信令无线承载，并通过所述信令无线承载传输所述 UE 与所述第二网络设备间的控制信令；

确定单元，用于确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；

接收单元，用于接收所述第二网络设备的第二协议层实体发送

的携带有消息鉴权码 MAC-I 的控制信令；

校验单元，用于根据所述确定单元确定出的完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第十方面的具体实现方式可以参考第二方面或第二方面的可能的实现方式提供的处理控制信令的方法中 UE 的行为功能，在此不再重复赘述。因此，第十方面提供的 UE 可以达到与第二方面相同的有益效果。

第十一方面，提供一种 UE，所述 UE 与第二网络设备间建立信令无线承载，并通过所述信令无线承载传输所述 UE 与所述第二网络设备间的控制信令，该 UE 可以包括：

处理器，用于确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；

收发器，用于接收所述第二网络设备的第二协议层实体发送的携带有消息鉴权码 MAC-I 的控制信令；

处理器，还用于根据所述处理器确定出的完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第十一方面的具体实现方式可以参考第二方面或第二方面的可能的实现方式提供的处理控制信令的方法中UE的行为功能，在此不再重复赘述。因此，第十一方面提供的 UE 可以达到与第二方面相同的有益效果。

第十二方面，本发明提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第十方面或第十一方面或上述任一种可能的实现方式所述的 UE 执行时，使 UE 执行以下事件：

与第二网络设备间建立信令无线承载，并通过所述信令无线承载传输所述 UE 与所述第二网络设备间的控制信令，确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法，接收所述第二网络设备的第二协议层实体发送的携带有消息鉴权码 MAC-I 的控制信令，根据所述确定单元确定出的完整性保护参

数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第十二方面的具体实现方式可以参考第二方面或第二方面的可能的实现方式提供的处理控制信令的方法中UE的行为功能，在此不再重复赘述。因此，第十二方面提供的UE可以达到与第二方面相同的有益效果。

第十三方面，提供一种第一网络设备，该第一网络设备可以包括：

获取单元，用于获取UE的上下文信息，所述上下文信息包括：根密钥、以及所述UE可支持的至少一个完整性保护算法；

发送单元，用于向所述UE发送安全激活命令；所述安全激活命令包含对第一网络设备和UE间的信令无线承载进行完整性保护所用的完整性保护算法，安全激活命令用于激活对第一网络设备和UE间的信令无线承载执行完整性保护；

所述发送单元，还用于向第二网络设备发送信令无线承载建立请求，所述信令无线承载建立请求用于请求所述第二网络设备与所述UE间建立信令无线承载；

接收单元，用于接收所述第二网络设备返回的信令无线承载建立响应消息；

所述发送单元，还用于向所述UE发送无线资源控制RRC连接重配置消息，用于建立所述第二网络设备与所述UE间的信令无线承载；

所述接收单元，还用于接收所述UE返回的RRC连接重配置成功消息。

其中，第十三方面的具体实现方式可以参考第三方面或第三方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第十三方面提供的第一网络设备可以达到与第三方面相同的有益效果。

第十四方面，提供一种第一网络设备，该第一网络设备可以包括：

处理器，用于获取包括：根密钥、以及所述 UE 可支持的至少一个完整性保护算法的 UE 的上下文信息；

收发器，用于向所述 UE 发送安全激活命令；所述安全激活命令包含对第一网络设备和 UE 间的信令无线承载进行完整性保护所用的完整性保护算法，安全激活命令用于激活对第一网络设备和 UE 间的信令无线承载执行完整性保护；

以及，向第二网络设备发送信令无线承载建立请求，所述信令无线承载建立请求用于请求所述第二网络设备与所述 UE 间建立信令无线承载；

接收所述第二网络设备返回的信令无线承载建立响应消息；

向所述 UE 发送无线资源控制 RRC 连接重配置消息，用于建立所述第二网络设备与所述 UE 间的信令无线承载；

接收所述 UE 返回的 RRC 连接重配置成功消息。

其中，第十四方面的具体实现方式可以参考第三方面或第三方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第十四方面提供的第一网络设备可以达到与第三方面相同的有益效果。

第十五方面，本发明提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第十三方面或第十四方面或上述任一种可能的实现方式所述的第一网络设备执行时，使第一网络设备执行以下事件：

获取包括：根密钥、以及所述 UE 可支持的至少一个完整性保护算法的 UE 的上下文信息，向所述 UE 发送包含对第一网络设备和 UE 间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对第一网络设备和 UE 间的信令无线承载执行完整性保护的安全激活命令，以及，向第二网络设备发送用于请求所述第二网络设备与所述 UE 间建立信令无线承载的信令无线承载建立请求，接收所述第二网络设备返回的信令无线承载建立响应消息，向所述 UE 发送无线资源控制 RRC 连接重配置消息，用于建立所述第二网络设

备与所述UE间的信令无线承载，接收所述UE返回的RRC连接重配置成功消息。

其中，第十五方面的具体实现方式可以参考第三方面或第三方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第十五方面提供的第一网络设备可以达到与第三方面相同的有益效果。

第十六方面，提供一种第二网络设备，该第二网络设备包括第一协议层实体，所述第二网络设备的第一协议层实体包括：

生成单元，用于生成所述第二网络设备和UE间的控制信令；

确定单元，用于确定完整性保护参数、以及完整性保护算法；所述完整性保护参数和完整性保护算法用于对所述控制信令进行完整性保护；

以及、根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码MAC-I；

发送单元，用于将所述MAC-I携带在所述控制信令内向所述UE发送。

其中，第十六方面的具体实现方式可以参考第四方面或第四方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第十六方面提供的第二网络设备可以达到与第四方面相同的有益效果。

第十七方面，提供一种第二网络设备，该第二网络设备包括第一协议层实体，所述第二网络设备的第一协议层实体包括：

处理器，用于生成所述第二网络设备和UE间的控制信令；

以及，确定完整性保护参数、以及完整性保护算法；所述完整性保护参数和完整性保护算法用于对所述控制信令进行完整性保护；根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码MAC-I；

收发器，用于将所述MAC-I携带在所述控制信令内向所述UE发送。

其中，第十七方面的具体实现方式可以参考第四方面或第四方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第十七方面提供的第二网络设备可以达到与第四方面相同的有益效果。

第十八方面，提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第十六方面或第十七方面或上述任一种可能的实现方式所述的第一网络设备执行时，使第一网络设备执行以下事件：

生成所述第二网络设备和 UE 间的控制信令，确定用于对所述控制信令进行完整性保护的完整性保护参数、以及完整性保护算法，根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码 MAC-I，将所述 MAC-I 携带在所述控制信令内向所述 UE 发送。

其中，第十八方面的具体实现方式可以参考第四方面或第四方面的可能的实现方式提供的处理控制信令的方法中第二网络设备的行为功能，在此不再重复赘述。因此，第十八方面提供的第二网络设备可以达到与第四方面相同的有益效果。

第十九方面，提供一种用户设备 UE，该 UE 可以包括：

确定单元，用于确定完整性保护参数、以及完整性保护算法，所述完整性保护参数和完整性保护算法用于对第二网络设备与所述 UE 间传输的控制信令进行完整性保护；

接收单元，用于接收所述第二网络设备的第一协议层实体发送的携带有消息鉴权码 MAC-I 的控制信令；

校验单元，用于根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第十九方面的具体实现方式可以参考第五方面或第五方面的可能的实现方式提供的处理控制信令的方法中 UE 的行为功能，在此不再重复赘述。因此，第十九方面提供的 UE 可以达到与第五方面相同的有益效果。

第二十方面，提供一种用户设备 UE，该 UE 可以包括：

处理器，用于确定完整性保护参数、以及完整性保护算法，所述完整性保护参数和完整性保护算法用于对第二网络设备与所述UE间传输的控制信令进行完整性保护；

收发器，用于接收所述第二网络设备的第一协议层实体发送的携带有消息鉴权码MAC-I 的控制信令；

处理器，还用于根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第二十方面的具体实现方式可以参考第五方面或第五方面的可能的实现方式提供的处理控制信令的方法中UE的行为功能，在此不再重复赘述。因此，第二十方面提供的UE可以达到与第五方面相同的有益效果。

第二十一方面，提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第十九方面或第二十方面或上述任一种可能的实现方式所述的UE执行时，使UE执行以下事件：

确定用于对第二网络设备与所述UE间传输的控制信令进行完整性保护的完整性保护参数、以及完整性保护算法，接收所述第二网络设备的第一协议层实体发送的携带有消息鉴权码MAC-I 的控制信令，根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

其中，第二十一方面的具体实现方式可以参考第五方面或第五方面的可能的实现方式提供的处理控制信令的方法中UE的行为功能，在此不再重复赘述。因此，第二十一方面提供的UE可以达到与第五方面相同的有益效果。

第二十二方面，提供一种第一网络设备执行，该第一网络设备可以包括：

获取单元，获取UE的上下文信息，所述上下文信息包括：根密钥、以及所述UE可支持的至少一个完整性保护算法；

发送单元，用于向所述UE发送安全激活命令，所述安全激活

命令包含对所述第一网络设备和所述 UE 间的信令无线承载进行完整性保护所用的完整性保护算法，安全激活命令用于激活对所述第一网络设备和所述 UE 间的信令无线承载执行完整性保护；

生成单元，用于根据所述根密钥生成第一密钥；

所述发送单元，还用于向所述第二网络设备发送安全上下文建立请求消息；所述安全上下文建立请求消息包含：所述第一密钥、以及所述 UE 可支持的至少一个完整性保护算法；

接收单元，用于接收所述第二网络设备返回的安全上下文建立响应消息。

其中，第二十二方面的具体实现方式可以参考第六方面或第六方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第二十二方面提供的第一网络设备可以达到与第六方面相同的有益效果。

第二十三方面，提供一种第一网络设备执行，该第一网络设备可以包括：

处理器，用于获取包括：根密钥、以及所述 UE 可支持的至少一个完整性保护算法的 UE 的上下文信息；

收发器，用于向所述 UE 发送包含对所述第一网络设备和所述 UE 间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对所述第一网络设备和所述 UE 间的信令无线承载执行完整性保护的安全激活命令；

处理器，还用于根据所述根密钥生成第一密钥；

收发器，还用于向所述第二网络设备发送安全上下文建立请求消息；所述安全上下文建立请求消息包含：所述第一密钥、以及所述 UE 可支持的至少一个完整性保护算法；

以及，接收所述第二网络设备返回的安全上下文建立响应消息。

其中，第二十三方面的具体实现方式可以参考第六方面或第六方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第二十三方面提供的第一

网络设备可以达到与第六方面相同的有益效果。

第二十四方面，提供一种存储一个或多个程序的非易失性计算机可读存储介质，该一个或多个程序包括指令，指令当被包括第二十二方面或第二十三方面或上述任一种可能的实现方式所述的第一网络设备执行时，使第一网络设备执行以下事件：

获取包括：根密钥、以及所述 UE 可支持的至少一个完整性保护算法的 UE 的上下文信息，向所述 UE 发送包含对所述第一网络设备和所述 UE 间的信令无线承载进行完整性保护所用的完整性保护算法、用于激活对所述第一网络设备和所述 UE 间的信令无线承载执行完整性保护的安全激活命令，根据所述根密钥生成第一密钥，向所述第二网络设备发送包含：所述第一密钥、以及所述 UE 可支持的至少一个完整性保护算法的安全上下文建立请求消息，以及，接收所述第二网络设备返回的安全上下文建立响应消息。

其中，第二十四方面的具体实现方式可以参考第六方面或第六方面的可能的实现方式提供的处理控制信令的方法中第一网络设备的行为功能，在此不再重复赘述。因此，第二十四方面提供的第一网络设备可以达到与第六方面相同的有益效果。

第二十五方面，提供一种处理控制信令的系统，包括：如第七方面或第八方面或第九方面或上述任一可实现方式所述的第二网络设备、如第十方面或第十一方面或第十二方面或上述任一可实现方式所述的 UE、以及如第十三方面或第十四方面或第十五方面或上述任一可实现方式所述的第一网络设备；

或者，如第十六方面或第十七方面或第十八方面或上述任一可实现方式所述的第二网络设备、如第十九方面或第二十方面或第二十一方面或上述任一可实现方式所述的 UE、以及如第二十二方面或第二十三方面或第二十四方面或上述任一可实现方式所述的第一网络设备。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下

面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为现有分层的接入网架构的控制面协议栈的示意图；

图 2 为本发明实施例提供的一种网络架构示意图；

图 3 为本发明实施例提供一种控制面协议栈架构示意图；

图 4a 为本发明实施例提供的又一种控制面协议架构示意图；

图 4b 为本发明实施例提供的又一种控制面协议架构示意图；

图 5 为本发明实施例提供的再一种控制面协议架构示意图；

图 6 为本发明实施例提供的一种处理控制信令的方法的流程图；

图 7 为本发明实施例提供的一种处理控制信令的方法的流程图；

图 8 为本发明实施例提供的一种处理控制信令的方法的流程图；

图 9 为本发明实施例提供的一种第一网络设备 10 的结构示意图；

图 10 为本发明实施例提供的一种第一网络设备 10 的结构示意图；

图 11 为本发明实施例提供的一种第二网络设备 20 的结构示意图；

图 12 为本发明实施例提供的一种第二网络设备 20 的结构示意图；

图 13 为本发明实施例提供的一种 UE3 0 的结构示意图；

图 14 为本发明实施例提供的一种 UE3 0 的结构示意图；

图 15 为本发明实施例提供的一种第一网络设备 40 的结构示意图；

图 16 为本发明实施例提供的一种第二网络设备 50 的结构示意

图；

图 17 为本发明实施例提供的一种 UE60 的结构示意图。

具体实施方式

本发明的原理是:在 DU 的控制面协议栈内新增 RRC 层和 PDCP 层，DU 的控制功能由 RRC 层完成，UE 和 DU 之间建立信令无线承载来传输 DU 和 UE 之间的控制信令，对该控制信令的完整性保护由 PDCP 层来实现；或者，在现有 DU 的控制面协议栈的基础上，DU 的控制功能由 DU 的层 2 中的任一层（如 RLC 层或者 MAC 层）来实现，通过层 2 的消息来传输 UE 和 DU 间的控制信令，并由层 2 对承载控制信令的层 2 消息进行完整性保护。

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

在本发明的描述中，需要理解的是，术语"第一"、"第二"、"另一"等指示的系统或元件为基于实施例描述的具有一定功能的系统或元件，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的系统或元件必须有此命名，因此不能理解为对本发明的限制。

详细描述本方案之前，为了便于理解本发明所述的技术方案，对本发明中的一些重要名词进行详细解释，需要理解的是，下述名词仅是本发明技术人员为了描述方便进行的命名，并不代表或暗示所指的系统或元件必须有此命名，因此不能理解为对本发明的限制：

RRC 层:主要功能包括系统信息广播、寻呼、建立释放维护 RRC 连接等，RRC 状态分为 RRC—IDLE（空闲态）和 RRC—CONNECTED（连接态）。

PDCP 层：主要功能包括报头压缩、安全性功能（如：完整性保护、加密）以及对切换时重排序和重传的支持。

RLC 层：主要功能包括分割与重组上层数据包，使得分割与重

组后的上层数据包的大小适应于无线接口进行的实际传输。对于需无差错传输的资源块（英文：Resource Block，RB）来说，RLC层也可通过重传来恢复丢失的包。另外，RLC层通过重排序来弥补由于底层混合自动重传请求（英文：Hybrid Automatic Repeat reQuest，HARQ）操作产生的乱序接收。

MAC层：主要功能包括实现逻辑信道映射到传输信道，复用从一条或多条逻辑信道下来的数据（MAC SDUs）到传输块，并通过传输信道发给物理层；把从传输信道传送上来的传输块解复用成MAC SDU，并通过相应的逻辑信道上交给RLC层；调度信息的报告；基于HARQ机制的错误纠正功能；通过动态调度的方式，处理不同用户的优先级以及对同一用户的不同逻辑信道的优先级处理；传输格式的选择，通过物理层上报的测量信息，用户能力等，选择相应的传输格式，从而达到最有效的资源利用等。

物理层：通过传输信道给高层提供数据传输服务，物理层提供的功能包括传输信道的错误检测并向高层提供指示、传输信道的前向纠错编解码、混合自动重传请求软合并、编码的传输信道与物理信道之间的速度匹配、编码的传输信道与物理信道之间的映射等功能。

本发明所述的处理控制信令的方法可以应用于图2所示的网络架构，该网络架构可以为5G的网络架构，如图2所示，该网络架构可以包括：接入网、UE，接入网由第一网络设备和第二网络设备两种网元组成，为第一网络设备-第二网络设备分离的接入网架构，一个第一网络设备下面可以连接多个第二网络设备，一个第二网络设备下面可以连接多个UE，UE可以在第二网络设备之间进行切换。其中，第一网络设备可以为CU，如：基带处理单元（英文：Base band Unit，BBU），通常位于中心机房内，第二网络设备可以为DU，如：射频拉远单元（英文：Remote Radio Unit，RRU），距离UE比较近。需要说明的是，图2仅为示意图，图3所示节点只是示例，其个数对本申请所述方案不构成限制。此外，为了便于描述，本发明实施

例仅以第一网络设备为 CU，第二网络设备为 DU 为例，对本发明提供的处理控制信令的方法、设备及系统进行介绍。

目前讨论的 CU-DU 分离接入网架构下，只有 CU 具有控制面功能，其中一种可能的接入网的控制面协议栈如图 1 所示，DU 仅包含 RLC 层、MAC 层、以及物理层，在 DU 侧需要实现部分控制功能的情况下，因 DU 内没有实现完整性保护功能的 PDCP 层，无法对 DU 和 CU 之间交互的控制信令进行完整性保护。

基于此，在本发明实施例的一种实现方案中，可以使 DU 控制面协议栈内包含第一协议层实体、第二协议层实体，由第一协议层实体完成 DU 的控制功能，下发控制信令，并由 DU 内的第二协议层实体对该控制信令进行完整性保护。其中，第一协议层实体可以为 RRC 层（又称辅助（Secondary）RRC 层）实体（又可称为 RRC 层）、第二协议层实体可以为 PDCP 层实体（又可称为 PDCP 层）。例如，图 3 为本发明实施例提供的 DU 和 UE 之间的控制面协议栈架构，如图 3 所示，DU 内包含辅助 RRC 层、PDCP 层、RLC 层、MAC 层以及 Physical layer，UE 内包含 RRC 层、PDCP 层、RLC 层、MAC 层以及 Physical layer,DU 可以通过辅助 RRC 层与 UE 间建立信令无线承载，传输 UE 和 DU 间的控制信令，辅助 RRC 层产生一个控制信令后交给底层的 PDCP 层进行处理，PDCP 层在收到辅助 RRC 层的控制信令后，基于该控制信令产生一个完整性消息鉴权码（英文：Message Authentication Code for Integrity，MAC-I），并将该 MAC-I 会和控制信令一起发送给 UE；其中，PDCP 层确定 MAC-I 时采用的完整性保护算法和一些完整性保护参数（如 DU 和 UE 间进行完整性保护所需的密钥）可以从辅助 RRC 层处获取。

由图 3 可知，为了实现 DU 和 CU 间信令无线承载的完整性保护，DU 需要具有可以实现完整性保护功能的 PDCP 层，由于 CU 通过 DU 实现对 UE 的控制功能，因此，在本发明实施例中，对于 CU 和 UE 间传输的控制信令而言，可以采用 DU 的 PDCP 层对 CU 下发的控制信令进行完整性保护（如图 4a 所示）；也可以不采用 DU 的

PDCP 层进行完整性保护,而是采用 CU 自身的 PDCP 层对 CU 和 DU 间控制信令进行完整性保护 (如图 4b 所示)。

在本发明实施例的又一可实现方案中,还可以不用改变 DU 内原有的控制面协议栈架构,使用 DU 目前包含的原不具备控制功能的第一协议层实体来实现 DU 的控制功能、以及完整性保护功能,其中,该第一协议层实体可以为层 2 中的任一层。例如,仅在图 5 所示的控制面协议栈架构的基础上,通过 DU 的层 2 中的任一层 (如 RLC 层或者 MAC 层)来实现 DU 的控制功能,UE 和 DU 之间不需要建立信令无线承载来传输 UE 和 DU 间的控制信令,而是通过层 2 的消息来处理控制信令,并由层 2 产生 MAC-I ,将该 MAC-I 和承载控制信令的层 2 消息一起发送给 UE, 以此实现 DU 和 UE 间的完整性保护;其中,层 2 确定 MAC-I 时采用的完整性保护算法和一些完整性保护参数 (如 DU 和 UE 间进行完整性保护所需的密钥)可以从 CU 处获取。

为使本发明的方案更清楚、目的更明确,下面结合图 2 所示的网络架构、以及图 6~图 8 所示的方法流程图对本发明提供的处理控制信令的方法进行详细说明。

图 6 为本发明实施例提供的一种处理控制信令的方法的流程图,该方法应用于图 3 所示的 DU 和 UE 间的控制面协议栈架构下,由图 2 所示的 CU、DU 以及 UE 交互执行,在该控制面协议架构下 DU 的控制功能通过 DU 内的 RRC 层来实现,UE 和 DU 之间建立信令无线承载来传输 UE 和 DU 之间的控制信令,对该信令无线承载的完整性保护由该 DU 内的 PDCP 层来实现。如图 6 所示,该方法可以包括以下步骤:

步骤 101: CU 获取 UE 的上下文信息,该上下文信息包括:UE 可支持的至少一个完整性保护算法、以及根密钥。

可选的,CU 可以从核心网 (如移动管理实体 (英文:Mobile Manager Entity , MME)) 处获取 UE 的上下文信息。

其中,上述根密钥用于生成对 CU 和 UE 间的控制信令进行完

整性保护所用的密钥，该根密钥可以由核心网中的网元产生；可选的，可以采用类似于目前 LTE 系统中对 UE 和 eNB 之间的控制信令进行完整性保护所用的根密钥的产生方法来产生上述根密钥，如：可以先获取几个输入参数，将获取到的输入参数作为密钥生成函数（英文：Key Derivation Function，KDF）的输入，通过 KDF 最终输出根密钥。具体的，可参见 TS33.401V13.2.0 中根密钥的产生方法，在此不再详细赘述。

步骤 102：CU 向 UE 发送安全激活命令，该安全激活命令用于激活 UE 和 CU 间的信令无线承载的完整性保护功能。

步骤 103：UE 接收 CU 发送的安全激活命令，生成根密钥。

其中，步骤 103 中 UE 生成根密钥的方法与步骤 101 中核心网中的网元产生根密钥的方法相同，即所用的密钥生成函数 KDF 以及所需要的输入参数都相同，因此步骤 103 中 UE 生成的根密钥与 CU 从核心网获取的根密钥相同。

步骤 104：CU 根据 CU 获取到的根密钥生成第一密钥。

其中，第一密钥用于生成对 DU 和 UE 间的信令无线承载进行完整性保护所用的密钥。

可选的，CU 可以获取 UE 在 DU 下的主服务小区的小区标识、以及该主服务小区的载波频率，根据主服务小区的小区标识、主服务小区的载波频率、以及根密钥生成第一密钥。

步骤 105：CU 向 DU 发送信令无线承载建立请求消息。

其中，该信令无线承载建立请求消息用于通知 DU 建立和 UE 间的信令无线承载，该信令无线承载建立请求消息可以包含 CU 获取的 UE 可支持的至少一个完整性保护算法、以及步骤 104 中 CU 生成的第一密钥。

步骤 106：DU 接收信令无线承载建立请求消息，与 UE 建立信令无线承载，并执行下述三个动作：

1）确定建立的信令无线承载标识；

2）生成第一随机数，根据第一随机数和第一密钥生成第二密钥，

并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥；

3）确定DU和UE间进行完整性保护所用的完整性保护算法。

至此，DU已成功激活DU和UE间信令无线承载的完整性保护功能。

其中，信令无线承载标识用于标识DU和UE建立的信令无线承载。可理解的是，DU不限于仅确定信令无线承载标识，还可以确定其他信令无线承载配置，在此不再一一赘述。

第三密钥为对DU和UE间的信令无线承载进行完整性保护所用的密钥，在该发明中通过第二密钥生成，可选的，可参照现有技术来生成第二密钥和第三密钥，在此不再详细赘述。

可选的，可以从UE可支持的至少一个完整性保护算法中选取任一完整性保护算法来作为DU和UE间进行完整性保护所用的算法。

步骤107：DU向CU返回信令无线承载建立响应消息。

其中，该信令无线承载响应消息包含：DU确定的完整性保护算法、第一随机数以及信令无线承载标识。

步骤108：CU接收信令无线承载建立响应消息，向UE发送RRC连接重配置配置消息。

其中，该无线资源控制（英文：Radio Resource Control，RRC）连接重配置消息用于指示UE建立与DU间的信令无线承载，该RRC连接重配置消息包含：DU确定的完整性保护算法、第一随机数、以及信令无线承载标识。

步骤109：UE接收RRC连接重配置消息，与DU间建立信令无线承载，并根据步骤103中生成的根密钥、UE在DU下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，进而根据RRC连接重配置消息中的第一随机数、以及第一密钥生成第二密钥，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥。

至此，UE 已成功激活对 DU 和 UE 间信令无线承载的完整性保护功能。

步骤 110: UE 向 CU 返回 RRC 连接重配置成功消息。

其中，该 RRC 连接重配置成功消息用于指示 UE 和 DU 间已建立好信令无线承载。

步骤 111: DU 根据步骤 106 中确定的信令无线承载标识、第三密钥、以及完整性保护算法生成 MAC-I 。

可选的，DU 可以根据信令无线承载标识、第三密钥、以及完整性保护算法生成 MAC-I 的过程可以参照现有技术，在此不再详细赘述。

步骤 112: DU 将 MAC-I 携带在控制信令中向 UE 发送。

步骤 113: UE 对接收到的控制信令进行完整性校验。

其中，UE 对接收到的控制信令进行完整性校验可以包括：

UE 根据步骤 109 中获取到的信令无线承载标识、完整性保护算法以及在步骤 109 中生成的第三密钥生成 MAC-I，将该 MAC-I 与携带在控制信令中的 MAC-I 进行比较，若二者相同，则表示完整性校验成功，若二者不同，则表示完整性校验失败。

需要说明的是，在图 6 所示的方法流程中，步骤 106~107 具体由图 3 所示 DU 中的 RRC 层执行，步骤 111~112 具体由图 3 所示 DU 中的 PDCP 层执行，如此，可以基于图 3 所示的 DU 和 UE 间的控制面协议栈架构，对 DU 和 UE 之间交互的控制信令提供完整性保护。此外，计算 MAC-I 需要的参数包括但不限于：信令无线承载标识、密钥、以及完整性保护算法，还可以包括：控制信令传输的方向（direction），在此不进行限定。

进一步的，在实际应用中的某些情况下，UE 和 DU 间进行完整性保护的密钥需要更新，根据更新的触发原因不同，可以分为下述两种情况：

第一种情况：由于 CU 和 UE 之间的根密钥更新，导致 DU 和 UE 之间的密钥需要更新；

第二种情况：仅DU和UE之间的密钥需要更新。

下述分别针对上述两种情况下的密钥更新过程进行详细描述：

（1）CU和UE之间的根密钥发生更新

Step 1：当UE和CU之间的根密钥发生更新后，CU和UE之间分别通过上述步骤S101和S103同步得到新的根密钥。

Step2：CU根据新的根密钥、UE在DU下的主服务小区的小区标识、以及主服务小区的载波频率推演出新的第一密钥。

Step3：CU向DU发送密钥更新请求消息，该密钥更新请求消息中包含新的第一密钥。

Step4：DU接收密钥更新请求消息，生成第二随机数，并根据第二随机数、以及新的第一密钥生成新的第二密钥。

其中，第二随机数可以与上述第一随机数相同，也可以不同，在此不进行限定。

Step 5：DU向UE发送密钥修改请求消息，该密钥修改请求消息中包含第二随机数。

Step6：UE接收密钥修改请求消息，先根据 Step l 中生成的新的根密钥、UE在DU下的主服务小区的小区标识、以及主服务小区的载波频率生成新的第一密钥，再根据新的第一密钥、以及第二随机数生成新的第二密钥，并进一步根据第二密钥推演出对DU和UE间的控制信令进行完整性保护所用的新的第三密钥。

Step7：UE向DU返回密钥》爹改响应消息，该密钥》爹改响应消息用于通知DU: UE已经成功》爹改对DU和UE间控制信令进行完整性保护所用的密钥。

（2）仅DU和UE之间的密钥需要更新

Step l：当UE和DU之间的密钥需要更新时，DU生成第三随机数，并根据上述步骤S106中接收到信令无线承载建立请求消息中的第一密钥、以及第三随机数生成新的第二密钥。

其中，第三随机数可以与第一随机数相同，也可以与第一随机数不同，在此不进行限定。

Step2 ：DU 向 UE 发送密钥修改请求消息，该密钥修改请求消息中包含第三随机数。

Step3： UE 接收密钥修改请求消息，根据上述步骤 109 中生成的第一密钥、以及第三随机数生成新的第二密钥，并进一步根据第二密钥推演出对 DU 和 UE 间的控制信令进行完整性保护所用的新的第三密钥。

Step4 ：UE 向 DU 返回密钥修改响应消息，该密钥修改响应消息用于通知 DU: UE 已经成功》爹改对 DU 和 UE 间控制信令进行完整性保护所用的密钥。

由图 6 所示过程可知，在该方案中，DU 侧确定的完整性保护算法、随机数先通知给 CU，再由 CU 通知给 UE，而不是直接由 DU 通知给 UE。

进一步可选的，为了降低通知的复杂度同时避免将 DU 选择的完整性保护算法通知给 CU，可替代的，在本发明实施例的又一可实现方案中，还可以在 CU 不可知的情况下，由 DU 直接将 DU 确定的完整性保护算法以及随机数通知给 UE，具体实现如图 7 所示。

图 7 为本发明实施例提供的又一种处理控制信令的方法的流程图，该方法也可以应用于图 3 所示的 DU 和 UE 间的控制面协议栈架构下，由图 2 所示的 CU、DU 以及 UE 交互执行，在该控制面协议栈架构下，DU 的控制功能通过 DU 内的 RRC 层来实现，UE 和 DU 之间建立信令无线承载来传输 UE 和 DU 之间的控制信令，对该信令无线承载的完整性保护由该 DU 内的 PDCP 层来实现。如图 7 所示，该方法可以包括以下步骤：

步骤 201: CU 获取 UE 的上下文信息，该上下文信息包括：UE 可支持的至少一个完整性保护算法、以及根密钥。

其中，步骤 201 中 CU 获取 UE 的上下文信息的过程与步骤 S101 相同，在此不再详细赘述。

步骤 202： CU 向 UE 发送安全激活命令，该安全激活命令用于激活 UE 和 CU 间的信令无线承载的完整性保护功能。

步骤 203：UE 接收 CU 发送的安全激活命令，生成根密钥。

步骤 204：CU 向 DU 发送信令无线承载建立请求消息。

其中，该信令无线承载建立请求消息用于通知 DU 建立和 UE 间的信令无线承载。

步骤 205：DU 接收信令无线承载建立请求消息，确定信令无线承载标识。

步骤 206：DU 向 CU 返回信令无线承载建立响应消息，该信令无线承载建立响应消息包含信令无线承载标识。

步骤 207：CU 接收信令无线承载建立响应消息，向 UE 发送 RRC 连接重配置消息，该 RRC 链接重建消息包含信令无线承载标识。

步骤 208：UE 接收 RRC 连接重配置消息，与 DU 间建立信令无线承载。

步骤 209：UE 向 CU 返回 RRC 连接重配置成功消息。

步骤 210：CU 根据根密钥生成第一密钥。

需要说明的是，图 7 所示的步骤仅为示例性步骤，其执行顺序不限于此，可选的，步骤 210 还可以在步骤 201 和步骤 202 间执行。

其中，步骤 201 的具体实现过程与步骤 104 相同，在此不再详细赘述。

步骤 211：CU 向 DU 发送安全上下文建立请求消息，该安全上下文建立请求消息包含第一密钥、以及步骤 201 获取的 UE 可支持的至少一个完整性保护算法。

步骤 212：DU 接收安全上下文建立请求消息，生成第一随机数，根据第一随机数和第一密钥生成第二密钥，并进一步根据第二密钥生成用于对 DU 和 UE 间的控制信令进行完整性保护所用的第三密钥，并确定 DU 和 UE 间进行完整性保护所用的完整性保护算法。

至此，DU 已成功激活 DU 和 UE 间信令无线承载的完整性保护功能。

步骤 213：DU 向 CU 返回安全上下文建立响应消息，该安全上下文响应消息用于通知 CU：DU 已经成功获取 UE 的安全上下文消

息。

步骤 214: DU 向 UE 发送安全激活消息，该安全激活消息包含 DU 确定的完整性保护算法、第一随机数。

步骤 215: UE 接收 CU 发送的安全激活消息，先根据步骤 203 中生成的根密钥、UE 在 DU 下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，再根据安全激活消息中的第一随机数、以及第一密钥生成第二密钥，并进一步根据第二密钥生成用于对 DU 和 UE 间的控制信令进行完整性保护所用的第三密钥。

至此，UE 已成功激活对 DU 和 UE 间信令无线承载的完整性保护功能。

步骤 216：UE 向 DU 返回安全激活响应消息，该安全激活响应消息用于通知 DU: UE 已经成功激活 DU 和 UE 间的完整性保护功能。

步骤 217: DU 根据步骤 205 中确定的信令无线承载标识、步骤 201 中确定的第三密钥、以及完整性保护算法生成 MAC-I 。

可选的，步骤 217 与步骤 111 相同，在此不再详细赘述。

步骤 218: DU 将 MAC-I 携带在控制信令中向 UE 发送。

步骤 219: UE 对接收到的控制信令进行完整性校验。

其中，步骤 219 与步骤 113 相同，在此不再详细赘述。

需要说明的是，在图 7 所示的方法流程中，步骤 205、207、212~214 具体由图 3 所示 DU 中的 RRC 层执行，步骤 217~1218 具体由图 3 所示 DU 中的 PDCP 层执行。此外，计算 MAC-I 需要的参数包括但不限于：信令无线承载标识、密钥、以及完整性保护算法，还可以包括：控制信令传输的方向 (direction)，在此不进行限定。

进一步可选的，在执行图 7 的过程中，也会在上述第一种情况或第二种情况下发生密钥更新，其中，在密钥更新时的具体执行过程可参照上述过程，在此不再详细赘述。

由上可知，图 6 和图 7 所示方案均基于图 3 所示的 DU 和 UE 间的控制面协议栈架构中 DU 的 RRC 层和 PDCP 层执行，需要在 DU

和 UE 之间具有对等的 RRC 层和 PDCP 层。

进一步可选的,为了避免 UE 需要同时维护和 CU 以及 DU 之间的 RRC 连接所带来的复杂度,可替代的,在本发明实施例的再一可实现方案中,还可以由 DU 的层 2 中任一层来实现 DU 的控制功能,并对控制信令进行完整性保护,具体的,该实现过程如图 8 所示。

图 8 为本发明实施例提供的再一种处理控制信令的方法的流程图,该方法可以应用于图 5 所示的 DU 和 UE 间的控制面协议栈架构下,由图 2 所示的 CU、DU 以及 UE 交互执行,在该控制面协议栈架构下,DU 的控制功能通过层 2 中的某一层 (RLC 层或 MAC 层) 来实现,UE 和 DU 之间不需要建立信令无线承载来传输 UE 和 DU 之间的控制信令,而是通过层 2 的消息来传输,对承载控制信令的层 2 消息进行完整性保护。如图 8 所示,该方法可以包括以下步骤:

步骤 301: CU 获取 UE 的上下文信息,该上下文信息包括:UE 可支持的至少一个完整性保护算法、以及根密钥。

其中,步骤 301 与步骤 101 相同,在此不再详细赘述。

步骤 302: CU 向 UE 发送安全激活命令,该安全激活命令用于激活 UE 和 CU 间的信令无线承载的完整性保护功能。

步骤 303: UE 接收 CU 发送的安全激活命令,生成根密钥。

其中,步骤 303 中与步骤 103 相同,在此不再详细赘述。

步骤 304: CU 根据 CU 获取到的根密钥生成第一密钥。

其中,步骤 304 与步骤 104 相同,在此不再详细赘述。

步骤 305: CU 向 DU 发送安全上下文建立请求消息,该安全上下文建立请求消息包含第一密钥、以及步骤 201 获取的 UE 可支持的至少一个完整性保护算法。

步骤 306: DU 接收安全上下文建立请求消息,并执行下述三个动作:

1)生成第一随机数,根据第一随机数和第一密钥生成第二密钥;

2)确定 DU 和 UE 间进行完整性保护所用的完整性保护算法;

3)确定 BEARER 参数值。

至此，DU 已成功激活 DU 和 UE 间信令无线承载的完整性保护功能。

其中，BEARER 参数值可以为 DU 为 DU 和 UE 间的控制信道分配的一个逻辑信道标识，该逻辑信道标识用于指示其对应的媒体接入控制层服务单元（英文：Medium Access Control Service Data Unit，MAC SDU）为 L2 控制信令；

或者，BEARER 参数值可以固定为一个特殊值，例如：若 BEARER 参数的比特数为 5 个，那么 BEARER 参数的取值可以为 11111。

步骤 307：DU 向 CU 返回安全上下文建立响应消息，该安全上下文响应消息用于通知 CU：DU 已经成功获取 UE 的安全上下文消息。

步骤 308：DU 向 UE 发送安全激活消息，该安全激活消息包含 DU 确定的完整性保护算法、第一随机数、以及 BEARER 参数值。

步骤 309：UE 接收 CU 发送的安全激活消息，先根据步骤 303 中生成的根密钥、UE 在 DU 下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，再根据安全激活消息中的第一随机数、以及第一密钥生成第二密钥，并进一步根据第二密钥生成用于对 DU 和 UE 间的控制信令进行完整性保护所用的第三密钥。

至此，UE 已成功激活对 DU 和 UE 间信令无线承载的完整性保护功能。

步骤 310：UE 向 DU 返回安全激活响应消息，该安全激活响应消息用于通知 DU：UE 已经成功激活 DU 和 UE 间的完整性保护功能。

步骤 311：DU 根据步骤 306 中确定的第三密钥、完整性保护算法、BEARER 参数值、以及计数值（COUNTER）生成 MAC-I。

其中，可以为每一个 UE 和 DU 之间的 L2 层控制信令关联一个序列号（英文：Sequence Number，SN）号，并将该 SN 和控制信令一起发送给 UE，将该 SN 作为计数值；

或者，在DU侧维护一个本地变量（VarCount），将VarCount作为该计数值，其中，当DU向UE每发送一个UE和DU之间的L2层控制信令，并且收到UE反馈的成功接收到L2层控制信令的确认（英文：Acknowledgement，ACK）消息后，更新该本地变量的值为VarCount +1。

步骤312：DU将MAC-I携带在控制信令中向UE发送。

其中，该控制信令承载在层2消息中。

步骤313：UE对接收到的控制信令进行完整性校验。

其中，UE对接收到的控制信令进行完整性校验可以包括：

UE根据步骤309中获取到的逻辑信道标识、第三密钥、BEARER参数值、以及自身维护的计数值生成MAC-I，将该MAC-I与携带在控制信令中的MAC-I进行比较，若二者相同，则表示完整性校验成功，若二者不同，则表示完整性校验失败。

其中，可以将UE接收到的包含SN的控制信令中的SN作为步骤313检验过程中的计数值；

或者，在UE侧维护一个本地变量（VarCount），将VarCount作为该计数值，其中，当UE接收到DU发送的一个UE和DU之间的L2层控制信令，并且向DU反馈确认（英文：Acknowledgement，ACK）消息后，更新该本地变量的值为VarCount +1。

需要说明的是，在图8所示的方法流程中，涉及DU执行的步骤由图5所示DU中的RLC层或者MAC层执行。此外，计算MAC-I需要的参数包括但不限于：BEARER参数值、密钥、计数值、以及完整性保护算法，还可以包括：控制信令传输的方向（direction），在此不进行限定。

进一步可选的，在执行图8的过程中，也会在上述第一种情况或第二种情况下发生密钥更新，其中，在密钥更新时的具体执行过程可参照上述过程，在此不再详细赘述。

上述主要以第一网络设备为CU、第二网络设备为DU，从第一网络设备、第二网络设备、以及UE交互的角度对本发明实施例提

供的完整性保护方案进行了介绍。可以理解的是，第一网络设备、第二网络设备、UE为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本发明能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

本发明实施例可以根据上述方法示例、结合附图6~8对第一网络设备、第二网络设备以及UE进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本发明实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

在采用对应各个功能划分各个功能模块的情况下，图9为本发明实施例中所涉及的第一网络设备的一种可能的结构示意图，如图9所示，第一网络设备10可以用于实施上述图6-7所示方法实施例中CU所执行的方法，该第一网络设备10可以包括：获取单元101、发送单元102、接收单元103、以及生成单元104；如：获取单元101用于支持第一网络设备执行图6中的过程101、以及图7中的过程201，发送单元102用于支持第一网络设备执行图6中的过程102、105、108、以及图7中的过程202、204、207、211，接收单元103用于支持第一网络设备执行图6中的过程107、110、以及图7中的过程206、209、213，生成单元104用于支持第一网络设备执行图6中的过程102、以及图7中的过程210。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下,图 10 为本发明实施例中所涉及的第一网络设备的一种可能的结构示意图,如图 10 所示,第一网络设备 10 可以包括:处理器 1011、收发器 1012、存储器 1013、以及通信总线 1014;

其中,处理器 1011 可以是中央处理器(英文:central processing unit,CPU),网络处理器(英文:network processor,NP),硬件芯片或者其任意组合。上述硬件芯片可以是专用集成电路(英文:application-specific integrated circuit,ASIC),可编程逻辑器件(英文:programmable logic device,PLD)或其组合。上述 PLD 可以是复杂可编程逻辑器件(英文:complex programmable logic device,CPLD),现场可编程逻辑门阵列(英文:field-programmable gate array,FPGA),通用阵列逻辑(英文:generic array logic,GAL)或其任意组合。

收发器 1012 可用于与外部网元之间进行数据交互,收发器 1012 可以为天线。

存储器 1013,可以是易失性存储器(英文:Volatile Memory),例如随机存取存储器(英文:Random-Access Memory,RAM);或者非易失性存储器(英文:Non-volatile Memory),例如只读存储器(英文:Read-only Memory,ROM),快闪存储器(英文:Flash Memory),硬盘(英文:Hard Disk Drive,HDD)或固态硬盘(英文:Solid-state Drive,SSD);或者上述种类的存储器的组合。处理器 1011 可以通过运行或执行存储在存储器 1013 内的程序代码,以及调用存储在存储器 1013 内的数据,实现第一网络设备的各种功能。

通信总线 1014 可以分为地址总线、数据总线、控制总线等,可以是工业标准体系结构(英文:Industry Standard Architecture,ISA)总线、外部设备互连(英文:Peripheral Component,PCI)总线或扩展工业标准体系结构(英文:Extended Industry Standard Architecture,EISA)总线等。为便于表示,图 10 中仅用一条粗线

表示，但并不表示仅有一根总线或一种类型的总线。

需要说明的是，图 9 所示的获取单元 101、生成单元 104 可以集成在图 10 所示处理器 1011 中，使处理器 1011 执行获取单元 101、生成单元 104 的具体功能，发送单元 102、接收单元 103 可以集成在图 10 所示的收发器 1012 中，使收发器 1012 执行发送单元 102、接收单元 103 的具体功能。

在采用对应各个功能划分各个功能模块的情况下，图 11 为本发明实施例中所涉及的第二网络设备的一种可能的结构示意图，如图 11 所示，第二网络设备 20 可以用于实施上述图 6-7 所示方法实施例中所执行的方法，该第二网络设备具备图 3 所示的控制协议栈，该第二网络设备 20 可以包括：建立单元 201、第一确定单元 202、第二确定单元 203、接收单元 204、发送单元 205，其中，第一确定单元 202 位于第二网络设备 20 的第一协议层实体，第二确定单元 203 位于第二网络设备 20 的第二协议层实体。例如：第一确定单元 202 用于支持第二网络设备执行图 6 中的过程 106 以及图 7 中的过程 205、212，接收单元 204 用于支持第二网络设备执行图 6 中的过程 105 以及图 7 中的过程 204、211、216，发送单元 205 用于支持第二网络设备执行图 6 中的过程 107、112、以及图 7 中的过程 206、213、214、218，第二确定单元 203 用于支持第二网络设备执行图 6 中的过程 111、以及图 7 中的过程 217。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下，图 12 为本发明实施例中所涉及的第一网络设备的一种可能的结构示意图，如图 12 所示，第一网络设备 20 可以包括：处理器 2011、收发器 2012、存储器 2013、以及通信总线 2014；

其中，处理器 2011 可以是 CPU，NP，硬件芯片或者其任意组合。上述硬件芯片可以是 ASIC，PLD 或其组合。上述 PLD 可以是 CPLD、FPGA、GAL 或其任意组合。

收发器2012可用于与外部网元之间进行数据交互,收发器2012可以为天线。

存储器2013，可以是易失性存储器，例如RAM; 或者非易失性存储器，例如ROM，快闪存储器(英文：Flash Memory)，HDD或SSD；或者上述种类的存储器的组合。处理器2011可以通过运行或执行存储在存储器2013内的程序代码，以及调用存储在存储器2013内的数据，实现第二网络设备的各种功能。

通信总线2014可以分为地址总线、数据总线、控制总线等，可以是ISA总线、PCI总线或EISA总线等。为便于表示，图12中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

需要说明的是，图11所示的建立单元201、第一确定单元202、第二确定单元203可以集成在图12所示处理器2011中，使处理器2011执行建立单元201、第一确定单元202、第二确定单元203的具体功能，接收单元204、发送单元205可以集成在图12所示的收发器2012中，使收发器2012执行接收单元204、发送单元205的具体功能。

在采用对应各个功能划分各个功能模块的情况下，图13为本发明实施例中所涉及的UE的一种可能的结构示意图，如图13所示，UE30可以用于实施上述图6-7所示方法实施例中所执行的方法，该UE30可以包括：建立单元301、确定单元302、接收单元303、校验单元304、以及发送单元305; 例如，建立单元301用于支持UE30执行图7中的过程208，确定单元302用于支持UE执行图6中的过程103、109以及图7中的过程203、215，接收单元303用于支持UE执行图6中的过程102、108、112以及图7中的过程207、214、218，校验单元304用于支持UE执行图6中的过程113以及图7中的过程219，发送单元305用于支持UE执行图6中的过程110以及图7中的过程209、216。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下,图 14 为本发明实施例中所涉及的 UE 的一种可能的结构示意图,如图 13 所示,UE30 可以包括:处理器 3011、收发器 3012、存储器 3013、以及通信总线 3014;

其中,处理器 3011 可以是 CPU, NP, 硬件芯片或者其任意组合。上述硬件芯片可以是 ASIC, PLD 或其组合。上述 PLD 可以是 CPLD、FPGA、GAL 或其任意组合。

收发器 3012 可用于与外部网元之间进行数据交互,收发器 3012 可以为天线。

存储器 3013, 可以是易失性存储器,例如 RAM; 或者非易失性存储器,例如 ROM, 快闪存储器 (英文:Flash Memory), HDD 或 SSD; 或者上述种类的存储器的组合。处理器 3011 可以通过运行或执行存储在存储器 3013 内的程序代码,以及调用存储在存储器 3013 内的数据,实现 UE 的各种功能。

通信总线 3014 可以分为地址总线、数据总线、控制总线等,可以是 ISA 总线、PCI 总线或 EISA 总线等。为便于表示,图 14 中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

需要说明的是,图 13 所示的建立单元 301、确定单元 302、校验单元 304 可以集成在图 14 所示处理器 3011 中,使处理器 3011 执行建立单元 301、确定单元 302、校验单元 304 的具体功能,接收单元 303、发送单元 305 可以集成在图 14 所示的收发器 3012 中,使收发器 3012 执行接收单元 303、发送单元 305 的具体功能。

在采用对应各个功能划分各个功能模块的情况下,图 15 为本发明实施例中所涉及的第一网络设备的一种可能的结构示意图,如图 15 所示,第一网络设备 40 可以用于实施上述图 8 所示方法实施例中 CU 所执行的方法,该第一网络设备 40 可以包括:获取单元 401、发送单元 402、生成单元 403、以及接收单元 404。例如:获取单元 401 用于支持第一网络设备执行图 8 中的过程 301, 发送单元 402 用于支持第一网络设备执行图 8 中的过程 302、305, 接收单元 404 用于支持第一网络设备执行图 8 中的过程 307, 生成单元 403 用于支

持第一网络设备执行图 8 中的过程 304。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下，图 15 所示的获取单元 401、生成单元 403 可以集成在图 10 所示处理器 1011 中，使处理器 1011 执行获取单元 401、生成单元 403 的具体功能，发送单元 402、接收单元 404 可以集成在图 10 所示的收发器 1012 中，使收发器 1012 执行发送单元 402、接收单元 404 的具体功能。

在采用对应各个功能划分各个功能模块的情况下，图 16 为本发明实施例中所涉及的第二网络设备的一种可能的结构示意图，如图 16 所示，第二网络设备 50 可以用于实施上述图 8 所示方法实施例中所执行的方法，该第二网络设备具备图 5 所示的控制协议栈，该第二网络设备 50 可以包括：生成单元 501、确定单元 502、发送单元 503、接收单元 504。例如：生成单元 501 用于支持第二网络设备执行图 8 中的过程 306、311，确定单元 502 用于支持第二网络设备执行图 8 中的过程 306，发送单元 503 用于支持第二网络设备执行图 8 中的过程 307、308、312，接收单元 504 用于支持第二网络设备执行图 8 中的过程 305、310。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下，图 16 所示的生成单元 501、确定单元 502 可以集成在图 12 所示处理器 2011 中，使处理器 2011 执行生成单元 501、确定单元 502 的具体功能，发送单元 503、接收单元 504 可以集成在图 12 所示的收发器 2012 中，使收发器 2012 执行发送单元 503、接收单元 504 的具体功能。

在采用对应各个功能划分各个功能模块的情况下，图 17 为本发明实施例中所涉及的 UE 的一种可能的结构示意图，如图 17 所示，UE60 可以用于实施上述图 8 所示方法实施例中所执行的方法，该 UE60 可以包括：确定单元 601、接收单元 602、校验单元 603、以

及发送单元 604；例如，确定单元 601 用于支持 UE60 执行图 8 中的过程 303、309，接收单元 602 用于支持 UE60 执行图 8 中的过程 302、308、312，校验单元 603 用于支持 UE60 执行图 8 中的过程 313，发送单元 604 用于支持 UE60 执行图 8 中的过程 310。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再重复赘述。

在采用集成的单元的情况下，图 17 所示的确定单元 601、校验单元 603 可以集成在图 14 所示处理器 3011 中，使处理器 3011 执行确定单元 601、校验单元 603 的具体功能，接收单元 602、以及发送单元 604 可以集成在图 14 所示的收发器 3012 中，使收发器 3012 执行接收单元 602、以及发送单元 604 的具体功能。

再一方面，本发明实施例还提供一种处理控制信令的系统，该处理控制信令的系统可以包括：上述任一实施例所述的第一网络设备 10、第二网络设备 20、UE3 0；

或者，上述任一实施例所述的第一网络设备 40、第二网络设备 50、UE60 。

本发明实施例提供的处理控制信令的系统，实现上述图 6~图 8 所示的处理控制信令的方法，因此，可以达到与上述业务传输方法相同的有益效果，此处不再重复赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可

以位于一个地方，或者也可以分布到多个网络设备上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个功能单元独立存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备 (可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括 :通用串行总线 (英文 :Universal Serial Bus，USB) 闪存驱动器 (英文：USB flash drive)、移动硬盘、只读存储器 (英文：read-only memory，ROM)、随机存取存储器 (英文：random access memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案脱离权利要求的范围。

权 利 要 求 书

1、一种处理控制信令的方法，所述方法应用于包括第一网络设备和第二网络设备的接入网架构，所述第一网络设备与所述第二网络设备连接，所述第二网络设备与至少一个用户设备 UE 连接，该方法由所述第二网络设备执行，其特征在于，所述第二网络设备包括第一协议层实体和第二协议层实体，所述方法包括：

所述第二网络设备与 UE 间建立信令无线承载，所述信令无线承载用于传输所述第二网络设备与所述 UE 间的控制信令，所述 UE 为所述至少一个 UE 任一 UE；

所述第二网络设备的第一协议层实体确定对所述第二网络设备与所述 UE 间的控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；

所述第二网络设备的第二协议层实体根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码 MAC-I ；

所述第二网络设备的第一协议层实体生成控制信令，并向所述第二网络设备的第二协议层实体发送所述控制信令；

所述第二网络设备的第二协议层实体接收所述第二网络设备的第一协议层实体发送的所述控制信令，将所述 MAC-I 携带在所述控制信令内向所述 UE 发送。

2、根据权利要求 1 所述的方法，其特征在于，所述完整性保护参数包括：信令无线承载标识、以及所述第二网络设备与所述 UE 间的信令无线承载进行完整性保护所用的第三密钥；在所述第二网络设备与用户设备 UE 间建立信令无线承载之前，所述方法还包括：

所述第二网络设备接收所述第一网络设备发送的信令无线承载建立请求，并确定所述信令无线承载标识；所述信令无线承载建立请求用于请求所述第二网络设备与所述 UE 间建立信令无线承载；

所述第二网络设备的第一协议层实体确定完整性保护参数、以及完整性保护算法，包括：

所述第二网络设备的第一协议层实体获取所述第一网络设备发

送的第一密钥，以及所述UE可支持的至少一个完整性保护算法；

所述第二网络设备的第一协议层实体生成第一随机数；

所述第二网络设备的第一协议层实体根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥；

所述第二网络设备的第一协议层实体从所述UE可支持的至少一个完整性保护算法中确定所述完整性保护算法。

3、根据权利要求2所述的方法，其特征在于，

所述第一密钥由所述第一网络设备根据所述UE在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成；

所述根密钥可以用于产生对CU和UE间的控制信令进行完整性保护所用的密钥。

4、根据权利要求2或3所述的方法，其特征在于，所述第一密钥以及所述UE可支持的至少一个完整性保护算法包含在所述信令无线承载建立请求中，所述方法还包括：

所述第二网络设备向所述第一网络设备返回信令无线承载建立响应消息，所述信令无线承载建立响应消息包含：所述信令无线承载标识、所述第一随机数、以及所述完整性保护算法。

5、根据权利要求2或3所述的方法，其特征在于，所述方法还包括：

所述第二网络设备向所述第一网络设备返回信令无线承载建立响应消息，所述信令无线承载建立响应消息包含：所述信令无线承载标识；

所述第二网络设备接收所述第一网络设备发送的所述UE的安全上下文建立请求消息，所述UE的安全上下文建立请求消息包含：所述第一密钥、以及所述UE可支持的至少一个完整性保护算法；

所述第二网络设备向所述第一网络设备返回安全上下文建立响应消息；

所述第二网络设备的第一协议层实体向所述UE发送安全激活消息，所述安全激活消息包含：所述第一随机数以及所述完整性保护算法。

6、根据权利要求3-5任一项所述的方法，其特征在于，若所述根密钥发生变化，则所述方法还包括：

所述第二网络设备接收所述第一网络设备发送的密钥更新请求消息，所述密钥更新请求消息包含根据所述变化后的根密钥生成的新的第一密钥；

所述第二网络设备的第一协议层实体生成第二随机数；

所述第二网络设备的第一协议层实体向所述UE发送密钥修改请求消息，所述密钥修改请求消息包含所述第二随机数；

所述第二网络设备的第一协议层实体接收所述UE返回的密钥修改响应消息。

7、根据权利要求2-5任一项所述的方法，其特征在于，所述方法还包括：

所述第二网络设备的第一协议层实体生成第三随机数；

所述第二网络设备的第一协议层实体向所述UE发送密钥修改请求消息，所述密钥修改请求消息包含所述第三随机数；

所述第二网络设备的第一协议层实体接收所述UE返回的密钥修改响应消息。

8、根据权利要求1-7任一项所述的方法，其特征在于，

所述第一协议层实体为无线资源控制协议RRC层实体；

所述第二协议层实体为分组数据汇聚协议PDCP层实体。

9、一种处理控制信令的方法，由用户设备UE执行，其特征在于，所述方法包括：

所述UE与第二网络设备间建立信令无线承载，并通过所述信令无线承载传输所述UE与所述第二网络设备间的控制信令；

所述UE确定对所述控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；

所述UE接收所述第二网络设备发送的携带有消息鉴权码MAC-1的控制信令；

所述UE根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

10、根据权利要求9所述的方法，其特征在于，所述完整性保护参数包括：所述第二网络设备与UE间的信令无线承载标识、以及对所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥；所述UE确定完整性保护参数、以及完整性保护算法，包括：

所述UE接收第一网络设备发送的安全激活命令，所述安全激活命令包含对所述第一网络设备和所述UE间的信令无线承载进行完整性保护所用的完整性保护算法，所述安全激活命令用于激活对所述第一网络设备和所述UE间的信令无线承载；

所述UE根据所述安全激活命令，生成根密钥；

所述UE接收所述第一网络设备发送的无线资源控制RRC连接重配置消息，从所述RRC连接重配置消息中获取所述用户设备和第二网络设备间的信令无线承载标识、第一随机数以及所述完整性保护算法，并建立与第二网络设备间的信令无线承载；所述第一随机数由所述第二网络设备生成，所述完整性保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择；

所述UE根据所述根密钥生成第一密钥；

所述UE根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

11、根据权利要求9所述的方法，其特征在于，所述完整性保护参数包括：所述第二网络设备与UE间的信令无线承载标识、以及对所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的密钥；所述UE确定完整性保护参数、以及完整性保护算法，包括：

所述UE接收第一网络设备发送的安全激活命令，所述安全激活

命令包含对所述第一网络设备和所述UE间的信令无线承载进行完整性保护所用的完整性保护算法,所述安全激活命令用于激活对所述第一网络设备和所述UE间的信令无线承载;

所述UE根据所述安全激活命令,生成根密钥;

所述UE接收所述第一网络设备发送的无线资源控制RRC连接重配置消息,从所述RRC连接重配置消息中获取所述第二网络设备与UE间的信令无线承载标识;

所述UE接收所述第二网络设备发送的安全激活消息,从所述安全激活消息中获取第一随机数以及所述完整性保护算法;所述第一随机数由所述第二网络设备生成,所述完整性保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择;

所述UE根据所述根密钥生成第一密钥;

所述UE根据所述第一随机数以及所述第一密钥生成第二密钥,根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

12、根据权利要求10或11所述的方法,其特征在于,所述UE根据所述根密钥生成第一密钥,包括:

所述UE根据所述UE在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成所述第一密钥。

13、根据权利要求10-12任一项所述的方法,其特征在于,所述方法还包括:

所述UE生成新的根密钥;

所述UE接收所述第二网络设备发送的密钥修改请求消息,所述密钥修改请求消息包含第二随机数;

所述UE根据所述新的根密钥生成新的第一密钥;

所述UE根据所述第二随机数以及所述新的第一密钥生成新的第二密钥,根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥,

所述UE向所述第二网络设备返回密钥修改响应消息。

14、根据权利要求 10-12 任一项所述的方法，其特征在于，所述方法还包括：

所述 UE 接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第三随机数；

所述 UE 根据所述第三随机数以及所述第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述 UE 间的信令无线承载进行完整性保护所用的新的第三密钥，

所述 UE 向所述第二网络设备返回密钥修改响应消息。

15、一种处理控制信令的方法，所述方法应用于包括第一网络设备和第二网络设备的接入网架构，所述第一网络设备与所述第二网络设备连接，所述第二网络设备与至少一个用户设备 UE 连接，所述方法由所述第二网络设备执行，所述第二网络设备包括第一协议层实体，其特征在于，所述方法包括：

所述第二网络设备的第一协议层实体产生所述第二网络设备和用户设备 UE 间的控制信令；

所述第二网络设备的第一协议层实体确定完整性保护参数、以及完整性保护算法；所述完整性保护参数和完整性保护算法用于对所述第二网络设备和用户设备 UE 间的控制信令进行完整性保护；

所述第二网络设备的第一协议层实体根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码 MAC-I ；

所述第二网络设备的第一协议层实体生产控制信令，并将所述 MAC-I 携带在所述控制信令内向所述 UE 发送。

16、根据权利要求 15 所述的方法，其特征在于，

所述第一协议层实体为无线链路控制 RLC 层实体、或者媒体接入控制 MAC 层实体。

17、根据权利要求 15 或 16 所述的方法，其特征在于，所述完整性保护参数包括：BEARER 参数值、计数值、以及所述第二网络设备与所述 UE 间进行完整性保护所用的第三密钥；所述第二网络设备的第一协议层实体确定完整性保护参数、以及完整性保护算法，包括：

所述第二网络设备的第一协议层实体接收所述第一网络设备发送的安全上下文建立请求消息，所述 UE 的安全上下文建立请求消息包含：第一密钥、以及所述 UE 可支持的至少一个完整性保护算法；

所述第二网络设备的第一协议层实体生成第一随机数；

所述第二网络设备的第一协议层实体根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述 UE 间进行完整性保护所用的第三密钥；

所述第二网络设备的第一协议层实体从所述 UE 可支持的至少一个完整性保护算法中确定出所述完整性保护算法。

18、根据权利要求 17 所述的方法，其特征在于，

所述第一密钥由所述第一网络设备根据所述 UE 在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成。

19、根据权利要求 17 或 18 所述的方法，其特征在于，所述方法还包括：

所述第二网络设备的第一协议层实体向所述第一网络设备返回安全上下文建立响应消息；

所述第二网络设备的第一协议层实体向所述 UE 发送安全激活消息，所述安全激活消息包含：所述第一随机数、所述 BEARER 参数值以及所述完整性保护算法。

20、根据权利要求 18 所述的方法，其特征在于，若所述根密钥发生变化，则所述方法还包括：

所述第二网络设备的第一协议层实体接收所述第一网络设备发送的密钥更新请求消息，所述密钥更新请求消息包含根据所述变化后的根密钥生成的新的第一密钥；

所述第二网络设备的第一协议层实体生成第二随机数；

所述第二网络设备的第一协议层实体向所述 UE 发送密钥修改请求消息，所述密钥修改请求消息包含所述第二随机数；

所述第二网络设备的第一协议层实体接收所述 UE 返回的密钥修

改响应消息。

21、根据权利要求 17-19 任一项所述的方法，其特征在于，所述方法还包括：

所述第二网络设备的第一协议层实体生成第三随机数；

所述第二网络设备的第一协议层实体向所述UE发送密钥修改请求消息，所述密钥修改请求消息包含所述第三随机数；

所述第二网络设备的第一协议层实体接收所述UE返回的密钥修改响应消息。

22、一种处理控制信令的方法，由用户设备 UE 执行，其特征在于，所述方法包括：

所述 UE 确定完整性保护参数、以及完整性保护算法，所述完整性保护参数和完整性保护算法用于对第二网络设备与所述 UE 间传输的控制信令进行完整性保护；

所述UE接收所述第二网络设备发送的携带有消息鉴权码 MAC-1 的控制信令；

所述 UE 根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

23、根据权利要求 22 所述的方法，其特征在于，所述完整性保护参数包括：BEARER 参数值、计数值、以及所述第二网络设备与所述 UE 间进行完整性保护所用的第三密钥；所述 UE 确定完整性保护参数、以及完整性保护算法，包括：

所述 UE 接收第一网络设备发送的安全激活命令，所述安全激活命令包含对所述第一网络设备和所述 UE 间的信令无线承载进行完整性保护所用的完整性保护算法，所述安全激活命令用于激活对所述第一网络设备和所述 UE 间的信令无线承载；

所述 UE 根据所述安全激活命令，生成根密钥；

所述 UE 接收所述第二网络设备发送的安全激活消息，从所述安全激活消息中获取第一随机数、所述 BEARER 参数值以及所述完整性保护算法；所述第一随机数由所述第二网络设备生成，所述完整性

保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择；

所述UE根据所述根密钥生成第一密钥；

所述UE根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

24、根据权利要求23所述的方法，其特征在于，所述UE根据所述根密钥生成第一密钥，包括：

所述UE根据所述UE在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及所述根密钥生成所述第一密钥。

25、根据权利要求23或24所述的方法，其特征在于，所述方法还包括：

所述UE生成新的根密码；

所述UE接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第二随机数；

所述UE根据所述新的根密钥生成新的第一密钥；

所述UE根据所述第二随机数以及所述新的第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述UE向所述第二网络设备返回密钥修改响应消息。

26、根据权利要求23或24所述的方法，其特征在于，所述方法还包括：

所述UE接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第三随机数；

所述UE根据所述第三随机数以及所述第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述UE向所述第二网络设备返回密钥修改响应消息。

27、一种第二网络设备，其特征在于，所述第二网络设备包括第一协议层实体和第二协议层实体，所述设备包括：

处理器，用于与用户设备UE间建立信令无线承载，所述信令无线承载用于传输所述第二网络设备与所述UE间的控制信令，所述处理器用于控制所述第一协议层实体和所述第二协议层实体；

所述处理器，还用于确定对所述第二网络设备与所述UE间的控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；并根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码MAC-I；

通信接口，用于接收所述处理器生成的控制信令；

所述通信接口，还用于将所述MAC-I携带在所述控制信令内向所述UE发送。

28、根据权利要求27所述的设备，其特征在于，所述完整性保护参数包括：信令无线承载标识、以及所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥；

所述通信接口，还用于在所述处理器与用户设备UE间建立信令无线承载之前接收所述第一网络设备发送的信令无线承载建立请求，并确定所述信令无线承载标识；所述信令无线承载建立请求用于请求所述第二网络设备与所述UE间建立信令无线承载；

所述处理器，具体用于获取所述第一网络设备发送的第一密钥，以及所述UE可支持的至少一个完整性保护算法；

生成第一随机数；

根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥；

从所述UE可支持的至少一个完整性保护算法中确定所述完整性保护算法。

29、根据权利要求28所述的设备，其特征在于，

所述第一密钥由所述第一网络设备根据所述UE在所述第二网络

设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成。

30、根据权利要求 28 或 29 所述的设备，其特征在于，所述第一密钥以及所述 UE 可支持的至少一个完整性保护算法包含在所述信令无线承载建立请求中；

所述通信接口，还用于向所述第一网络设备返回信令无线承载建立响应消息，所述信令无线承载建立响应消息包含：所述信令无线承载标识、所述第一随机数、以及所述完整性保护算法。

31、根据权利要求 28 或 29 所述的设备，其特征在于，所述通信接口，还用于：

向所述第一网络设备返回信令无线承载建立响应消息，所述信令无线承载建立响应消息包含：所述信令无线承载标识；

所述通信接口，还用于接收所述第一网络设备发送的所述 UE 的安全上下文建立请求消息，所述 UE 的安全上下文建立请求消息包含：所述第一密钥、以及所述 UE 可支持的至少一个完整性保护算法；

所述通信接口，还用于向所述第一网络设备返回安全上下文建立响应消息；

以及，向所述 UE 发送安全激活消息，所述安全激活消息包含：所述第一随机数以及所述完整性保护算法。

32、根据权利要求 29-31 任一项所述的设备，其特征在于，若所述根密钥发生变化，则所述通信接口，还用于接收所述第一网络设备发送的密钥更新请求消息，所述密钥更新请求消息包含根据所述变化后的根密钥生成的新的第一密钥；

所述处理器，还用于生成第二随机数；

所述通信接口，还用于向所述 UE 发送密钥修改请求消息，所述密钥修改请求消息包含所述第二随机数；

所述通信接口，还用于接收所述 UE 返回的密钥修改响应消息。

33、根据权利要求 28-31 任一项所述的设备，其特征在于，所述处理器，还用于生成第三随机数；

所述通信接口，还用于向所述UE发送密钥修改请求消息，所述密钥修改请求消息包含所述第三随机数；

所述通信接口，还用于接收所述UE返回的密钥修改响应消息。

34、根据权利要求27-33任一项所述的设备，其特征在于，

所述第一协议层实体为无线资源控制协议RRC层实体；

所述第二协议层实体为分组数据汇聚协议PDCP层实体。

35、一种用户设备UE，其特征在于，所述UE包括：

处理器，用于与第二网络设备间建立信令无线承载，并通过所述信令无线承载传输所述UE与所述第二网络设备间的控制信令；

所述处理器，还用于确定对所述UE与所述第二网络设备间的控制信令进行完整性保护所用的完整性保护参数、以及完整性保护算法；

通信接口，用于接收所述第二网络设备发送的携带有消息鉴权码MAC-I的控制信令；

所述处理器，还用于根据所述处理器确定出的完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

36、根据权利要求35所述的UE，其特征在于，所述完整性保护参数包括：所述第二网络设备与UE间的信令无线承载标识、以及对所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥；

所述通信接口，还用于接收第一网络设备发送的安全激活命令，所述安全激活命令包含对所述第一网络设备和所述UE间的信令无线承载进行完整性保护所用的完整性保护算法，所述安全激活命令用于激活对所述第一网络设备和所述UE间的信令无线承载；

所述处理器，具体用于根据所述安全激活命令，生成根密钥；

所述通信接口，还用于接收所述第一网络设备发送的无线资源控制RRC连接重配置消息，从所述RRC连接重配置消息中获取所述用户设备和第二网络设备间的信令无线承载标识、第一随机数以及所述完整性保护算法，并建立与第二网络设备间的信令无线承载；所述第

一随机数由所述第二网络设备生成，所述完整性保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择；

所述处理器，具体用于根据所述根密钥生成第一密钥；

根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

37、根据权利要求35所述的UE，其特征在于，所述完整性保护参数包括：所述第二网络设备与UE间的信令无线承载标识、以及对所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的密钥；

所述通信接口，还用于接收第一网络设备发送的安全激活命令，所述安全激活命令包含对所述第一网络设备和所述UE间的信令无线承载进行完整性保护所用的完整性保护算法，所述安全激活命令用于激活对所述第一网络设备和所述UE间的信令无线承载；

所述处理器，具体用于根据所述安全激活命令，生成根密钥；

所述通信接口，还用于接收所述第一网络设备发送的无线资源控制RRC连接重配置消息，从所述RRC连接重配置消息中获取所述第二网络设备与UE间的信令无线承载标识；以及，接收所述第二网络设备发送的安全激活消息；

所述处理器，具体用于从所述安全激活消息中获取第一随机数以及所述完整性保护算法；所述第一随机数由所述第二网络设备生成，所述完整性保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择；

根据所述根密钥生成第一密钥；

根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

38、根据权利要求36或37所述的UE，其特征在于，

所述处理器，具体用于根据所述UE在所述第二网络设备下的主

服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成所述第一密钥。

39、根据权利要求 36-38任一项所述的UE，其特征在于，

所述处理器，还用于生成新的根密钥；

所述通信接口，还用于接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第二随机数；

所述处理器，还用于根据所述新的根密钥生成新的第一密钥；

根据所述第二随机数以及所述新的第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述通信接口，还用于向所述第二网络设备返回密钥修改响应消息。

40、根据权利要求 36-38任一项所述的UE，其特征在于，

所述通信接口，还用于接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第三随机数；

所述处理器，还用于根据所述第三随机数以及所述第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述通信接口，还用于向所述第二网络设备返回密钥修改响应消息。

41、一种第二网络设备，其特征在于，所述第二网络设备包括第一协议实体，所述第二网络设备还包括：

处理器，用于生成所述第二网络设备和用户设备UE间的控制信令；所述处理器用于控制和管理所述第一协议层实体；

所述处理器，还用于确定完整性保护参数、以及完整性保护算法；所述完整性保护参数和完整性保护算法用于对所述第二网络设备和UE间的控制信令进行完整性保护；以及、根据所述完整性保护参数、以及所述完整性保护算法确定消息鉴权码MAC-I；

通信接口，用于将所述MAC-I携带在所述控制信令内向所述UE

发送。

42、根据权利要求41所述的第二网络设备，其特征在于，

所述第一协议层实体为无线链路控制RLC层实体、或者媒体接入控制MAC层实体。

43、根据权利要求41或42所述的第二网络设备，其特征在于，所述完整性保护参数包括：BEARER参数值、计数值、以及所述第二网络设备与所述UE间进行完整性保护所用的第三密钥；

所述通信接口，还用于接收所述第一网络设备发送的安全上下文建立请求消息，所述UE的安全上下文建立请求消息包含：第一密钥、以及所述UE可支持的至少一个完整性保护算法；

所述处理器，具体用于生成第一随机数；

根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间进行完整性保护所用的第三密钥；

从所述UE可支持的至少一个完整性保护算法中确定出所述完整性保护算法。

44、根据权利要求43所述的第二网络设备，其特征在于，

所述第一密钥由所述第一网络设备根据所述UE在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及根密钥生成。

45、根据权利要求43或44所述的第二网络设备，其特征在于，

所述通信接口，还用于向所述第一网络设备返回安全上下文建立响应消息；以及，向所述UE发送安全激活消息，所述安全激活消息包含：所述第一随机数、所述BEARER参数值以及所述完整性保护算法。

46、根据权利要求44所述的第二网络设备，其特征在于，若所述根密钥发生变化，则所述通信接口，还用于接收所述第一网络设备发送的密钥更新请求消息，所述密钥更新请求消息包含根据所述变化后的根密钥生成的新的第一密钥；

所述处理器，还用于生成第二随机数；

所述通信接口，还用于向所述 UE 发送密钥修改请求消息，所述密钥修改请求消息包含所述第二随机数；

所述通信接口，还用于接收所述 UE 返回的密钥修改响应消息。

47、根据权利要求 43-45 任一项所述的第二网络设备，其特征在于，所述处理器，还用于生成第三随机数；

所述通信接口，还用于向所述 UE 发送密钥修改请求消息，所述密钥修改请求消息包含所述第三随机数；

所述通信接口，还用于接收所述 UE 返回的密钥修改响应消息。

48、一种用户设备 UE，其特征在于，所述 UE 包括：

处理器，用于确定完整性保护参数、以及完整性保护算法，所述完整性保护参数和完整性保护算法用于对第二网络设备与所述 UE 间传输的控制信令进行完整性保护；

通信接口，用于接收所述第二网络设备发送的携带有消息鉴权码 MAC-I 的控制信令；

所述处理器，还用于根据所述完整性保护参数、以及所述完整性保护算法，对所述控制信令进行完整性校验。

49、根据权利要求 48 所述的 UE，其特征在于，所述完整性保护参数包括：BEARER 参数值、计数值、以及所述第二网络设备与所述 UE 间进行完整性保护所用的第三密钥；

所述通信接口，还用于接收第一网络设备发送的安全激活命令，所述安全激活命令包含对所述第一网络设备和所述 UE 间的信令无线承载进行完整性保护所用的完整性保护算法，所述安全激活命令用于激活对所述第一网络设备和所述 UE 间的信令无线承载；

所述处理器，具体用于根据所述安全激活命令，生成根密钥；

所述通信接口，还用于接收所述第二网络设备发送的安全激活消息；

所述处理器，具体用于从所述安全激活消息中获取第一随机数、所述 BEARER 参数值以及所述完整性保护算法；所述第一随机数由

所述第二网络设备生成，所述完整性保护算法由所述第二网络设备从所述UE可支持的至少一个完整性保护算法中选择；

根据所述根密钥生成第一密钥；

根据所述第一随机数以及所述第一密钥生成第二密钥，根据所述第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的第三密钥。

50、根据权利要求49所述的UE，其特征在于，所述处理器，具体用于：

根据所述UE在所述第二网络设备下的主服务小区的小区标识、所述主服务小区的载波频率、以及所述根密钥生成所述第一密钥。

51、根据权利要求49或50所述的UE，其特征在于，

所述处理器，还用于生成新的根密码；

所述通信接口，还用于接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第二随机数；

所述处理器，还用于根据所述新的根密钥生成新的第一密钥；

以及根据所述第二随机数以及所述新的第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述通信接口，还用于向所述第二网络设备返回密钥修改响应消息。

52、根据权利要求49或50所述的UE，其特征在于，

所述通信接口，还用于接收所述第二网络设备发送的密钥修改请求消息，所述密钥修改请求消息包含第三随机数；

所述处理器，还用于根据所述第三随机数以及所述第一密钥生成新的第二密钥，根据所述新的第二密钥生成所述第二网络设备与所述UE间的信令无线承载进行完整性保护所用的新的第三密钥，

所述通信接口，还向所述第二网络设备返回密钥修改响应消息。

53、一种处理控制信令的系统，其特征在于，包括如权利要求27-34任一项所述的第二网络设备、如权利要求35-40任一项所述的

UE、以及第一网络设备；

或者，如权利要求41-47任一项所述的第二网络设备、如权利要求48-52任一项所述的UE、以及第一网络设备。

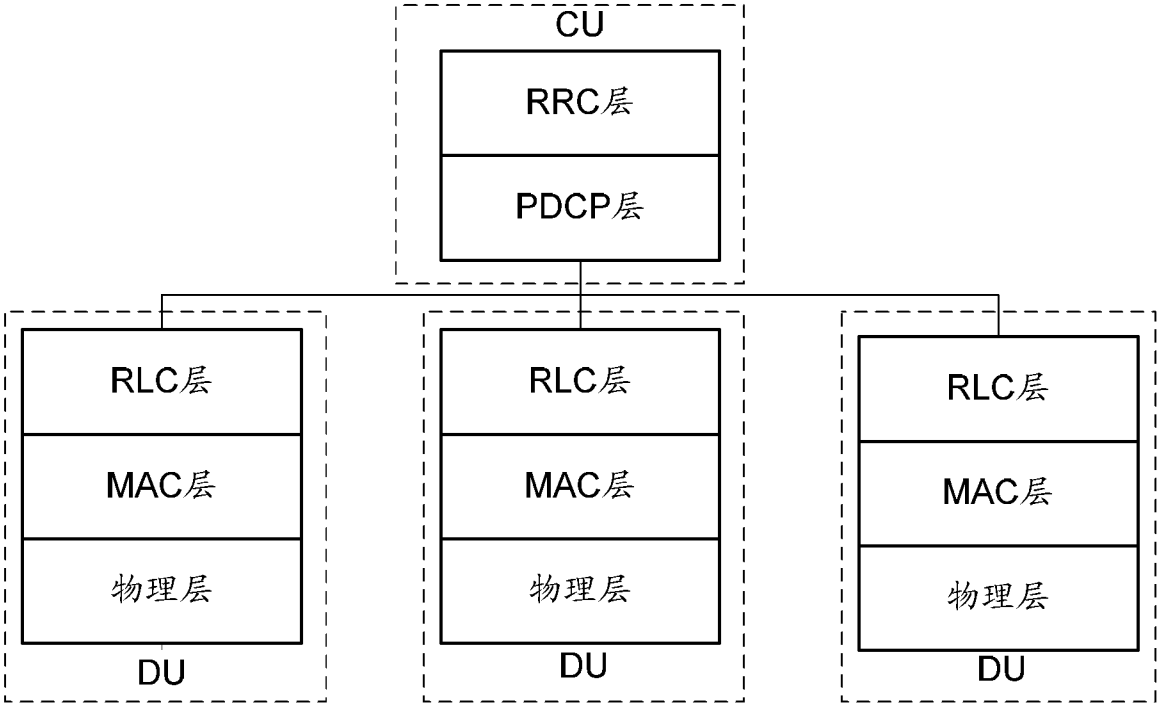
CU
RRC层
PDCP层
RLC层
MAC层
物理层
DU
RLC层
MAC层
物理层
DU
RLC层
MAC层
物理层
DU

图 1

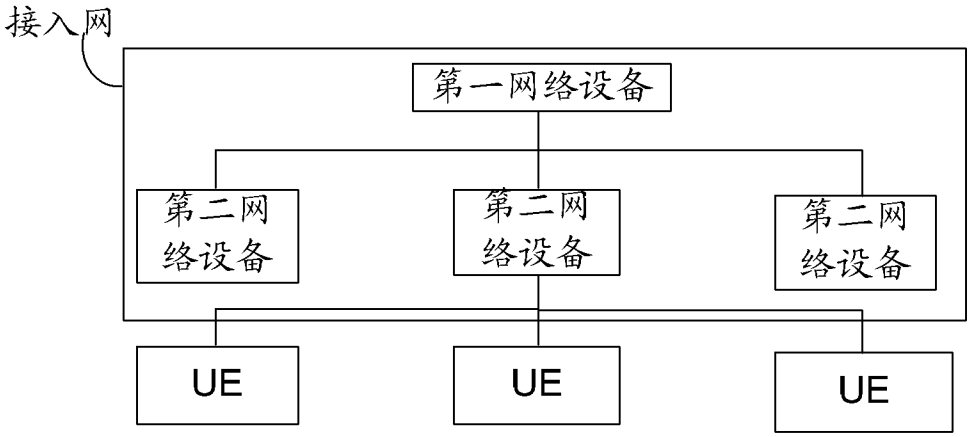
接入网
第一网络设备
第二网络设备
第二网络设备
第二网络设备
UE
UE
UE

图 2

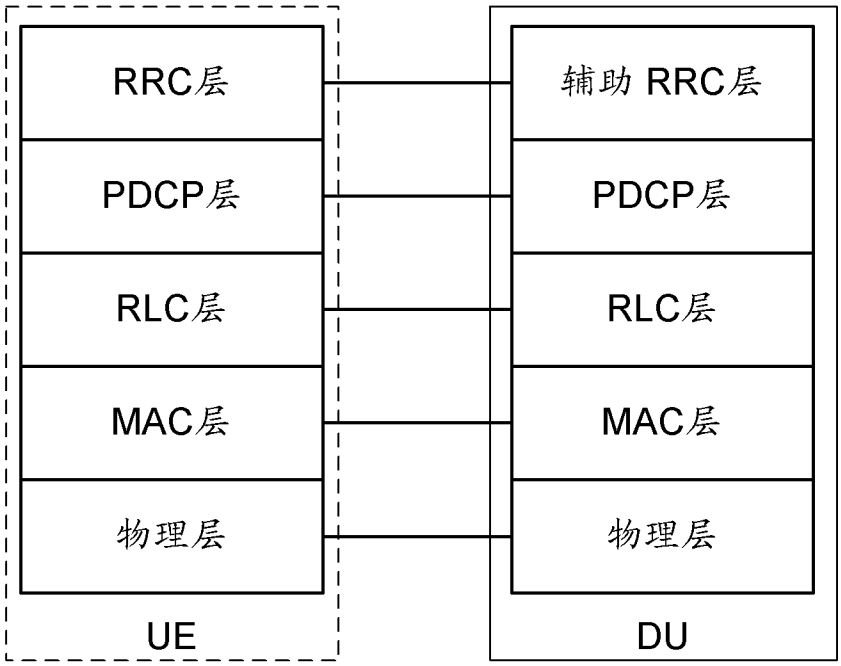
RRC层
PDCP层
RLC层
MAC层
物理层
UE
辅助 RRC层
PDCP层
RLC层
MAC层
物理层
DU

图 3

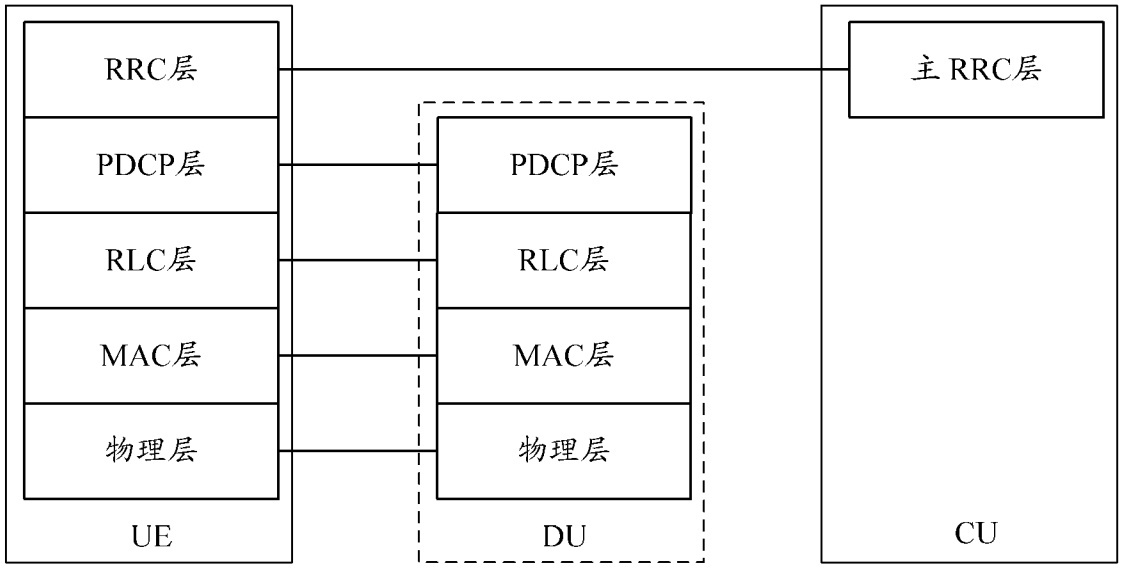
RRC层
PDCP层
RLC层
MAC层
物理层
UE
PDCP层
RLC层
MAC层
物理层
DU
主 RRC层
CU

图 4a

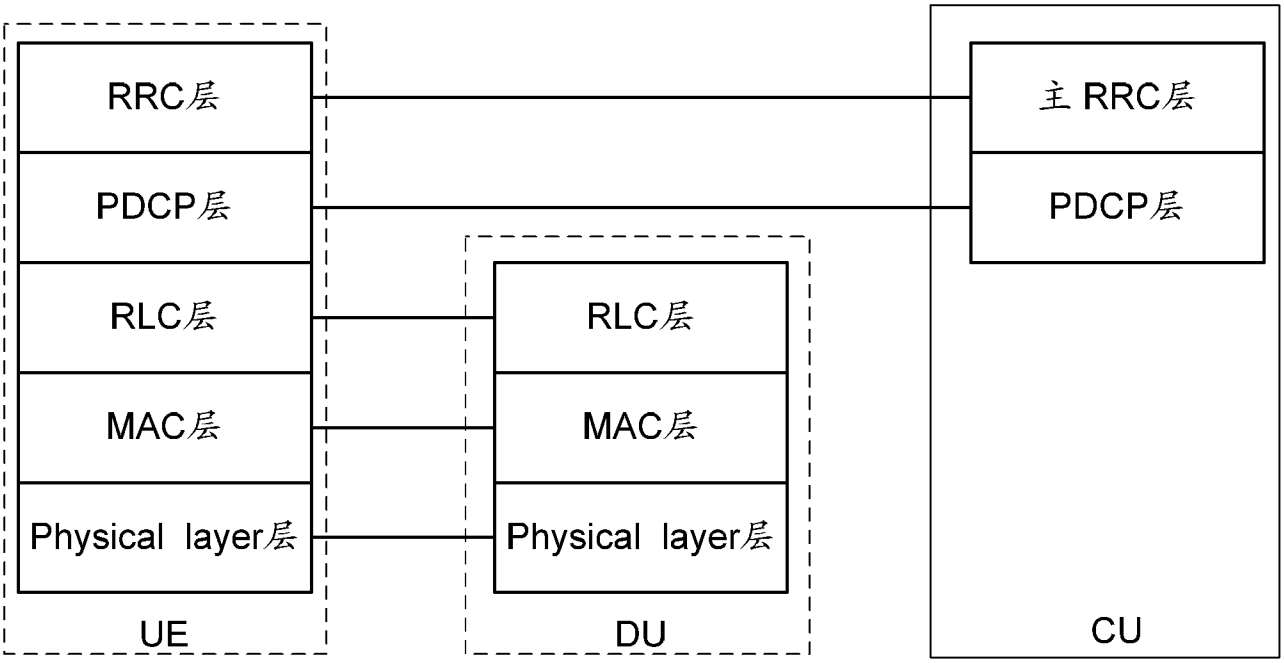
RRC层
PDCP层
RLC层
MAC层
Physical layer层
UE
RLC层
MAC层
Physical layer层
DU
主 RRC层
PDCP层
CU

图 4b

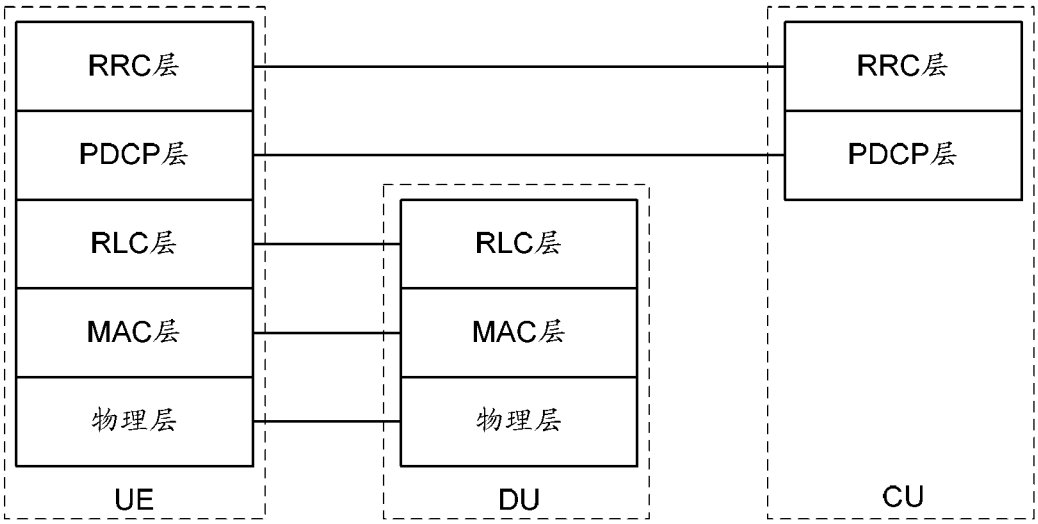
RRC层
PDCP层
RLC层
MAC层
物理层
UE
RLC层
MAC层
物理层
DU
RRC层
PDCP层
CU

图 5

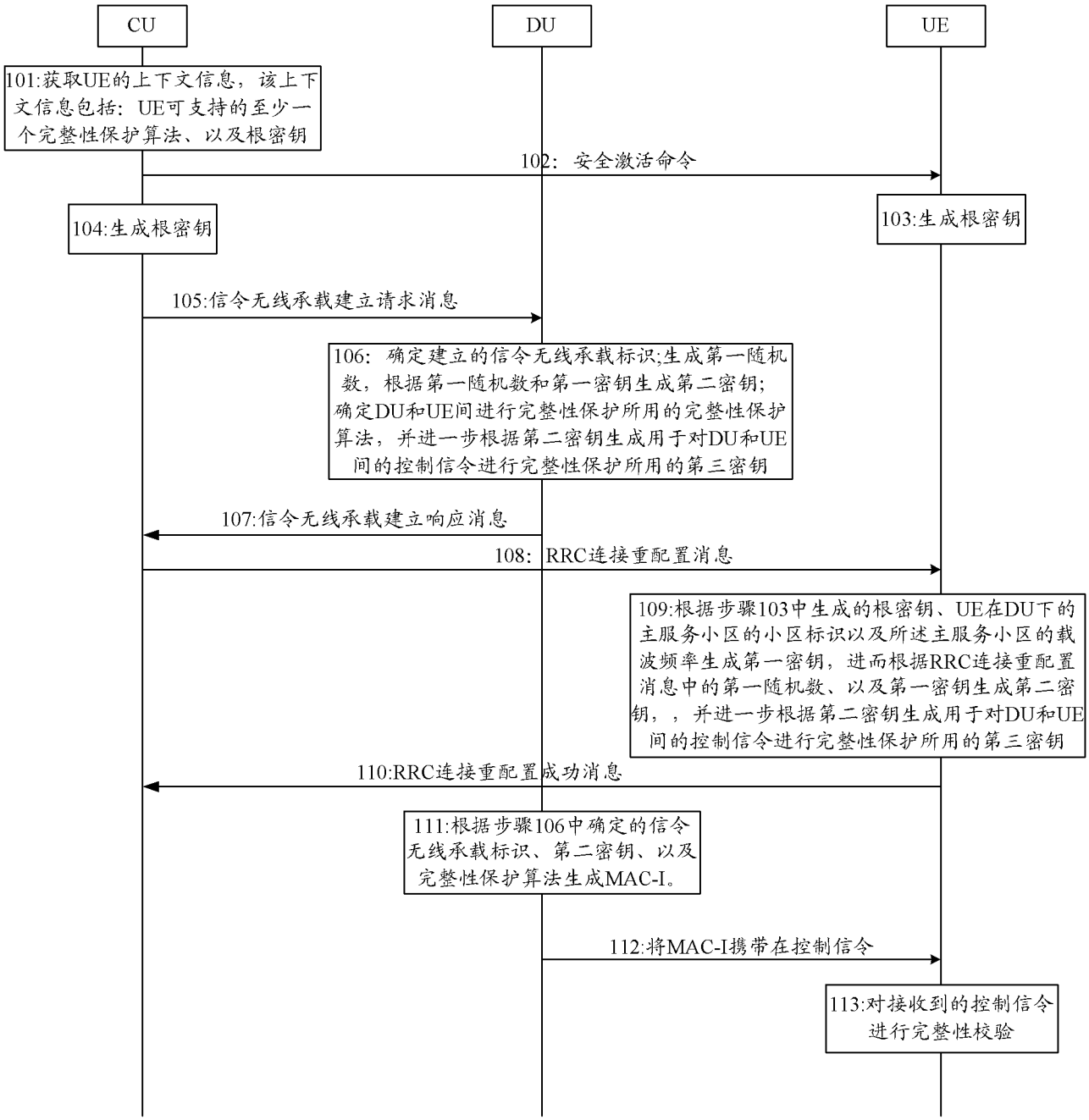
CU
DU
UE
101:获取UE的上下文信息，该上下文信息包括：UE可支持的至少一个完整性保护算法、以及根密钥
102：安全激活命令
104:生成根密钥
103:生成根密钥
105:信令无线承载建立请求消息
106：确定建立的信令无线承载标识;生成第一随机数，根据第一随机数和第一密钥生成第二密钥;确定DU和UE间进行完整性保护所用的完整性保护算法，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥
107:信令无线承载建立响应消息
108：RRC连接重配置消息
109:根据步骤103中生成的根密钥、UE在DU下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，进而根据RRC连接重配置消息中的第一随机数、以及第一密钥生成第二密钥，，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥
110:RRC连接重配置成功消息
111:根据步骤106中确定的信令无线承载标识、第二密钥、以及完整性保护算法生成MAC-I。
112:将MAC-I携带在控制信令
113:对接收到的控制信令进行完整性校验

图 6

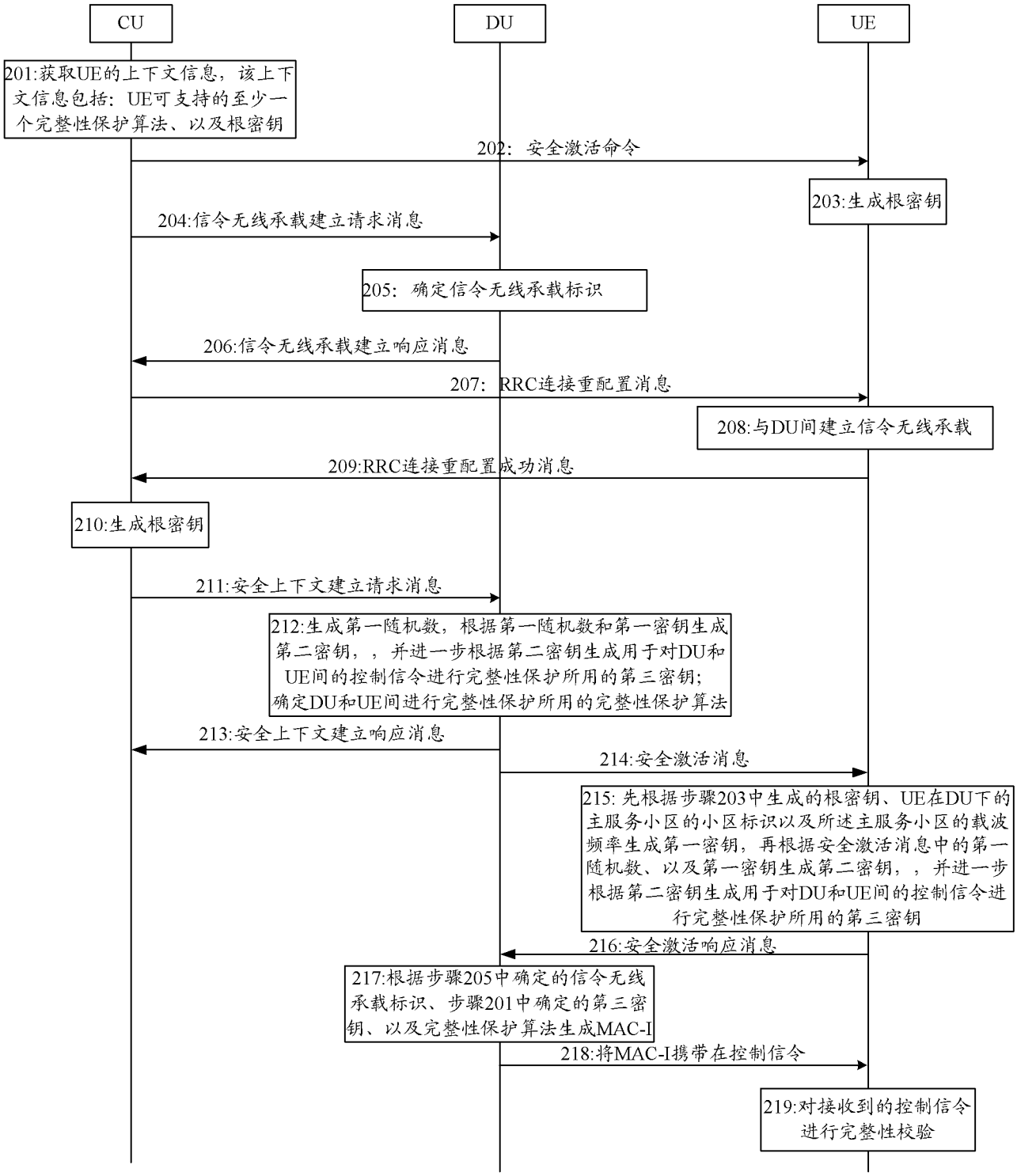
CU
DU
UE
201:获取UE的上下文信息，该上下文信息包括：UE可支持的至少一个完整性保护算法、以及根密钥
202：安全激活命令
203:生成根密钥
204:信令无线承载建立请求消息
205：确定信令无线承载标识
206:信令无线承载建立响应消息
207：RRC连接重配置消息
208:与DU间建立信令无线承载
209:RRC连接重配置成功消息
210:生成根密钥
211:安全上下文建立请求消息
212:生成第一随机数，根据第一随机数和第一密钥生成第二密钥，，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥；确定DU和UE间进行完整性保护所用的完整性保护算法
213:安全上下文建立响应消息
214:安全激活消息
215: 先根据步骤203中生成的根密钥、UE在DU下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，再根据安全激活消息中的第一随机数、以及第一密钥生成第二密钥，，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥
216:安全激活响应消息
217:根据步骤205中确定的信令无线承载标识、步骤201中确定的第三密钥、以及完整性保护算法生成MAC-I
218:将MAC-I携带在控制信令
219:对接收到的控制信令进行完整性校验

图 7

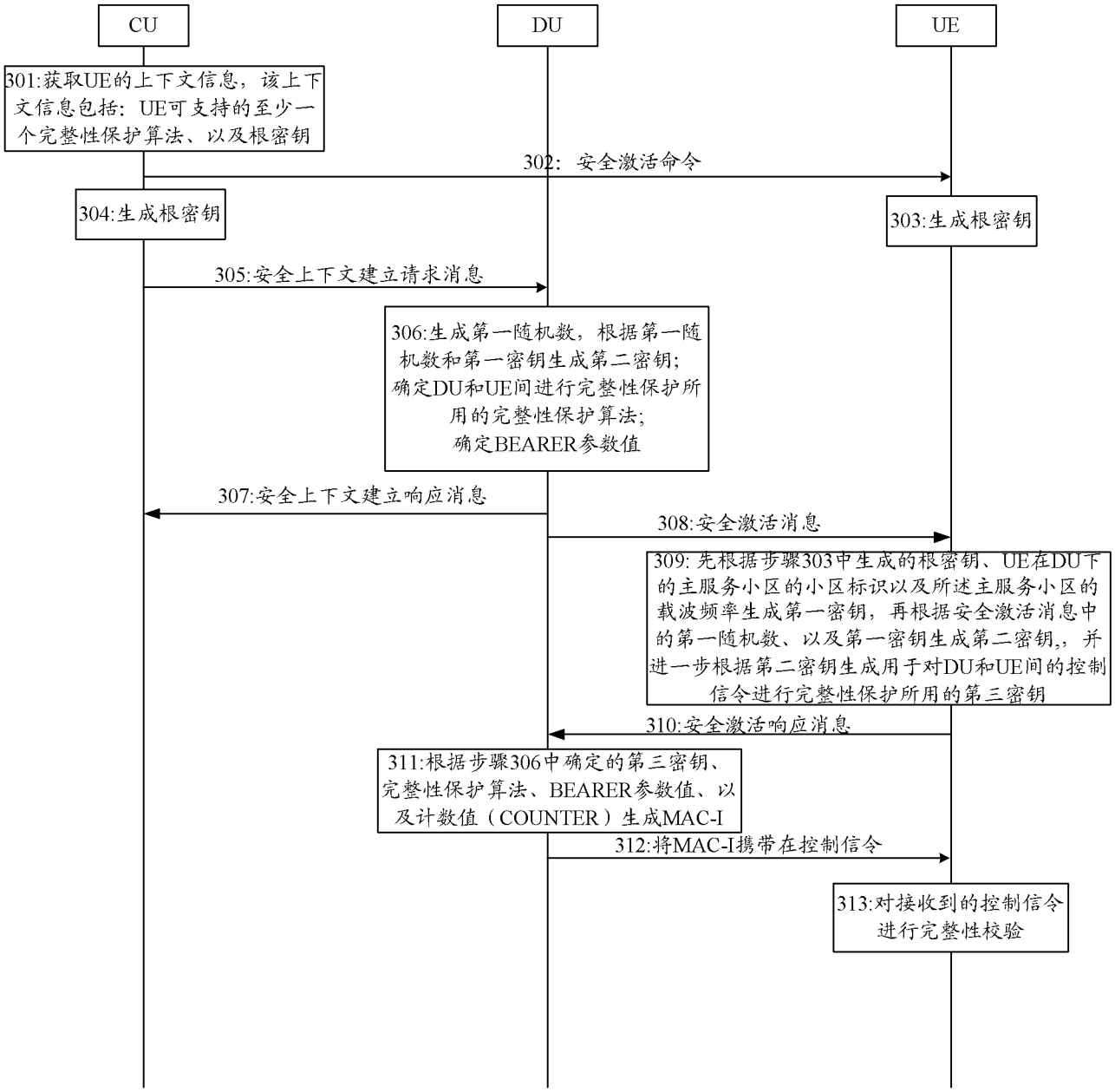
CU
DU
UE
301:获取UE的上下文信息，该上下文信息包括：UE可支持的至少一个完整性保护算法、以及根密钥
302：安全激活命令
304:生成根密钥
303:生成根密钥
305:安全上下文建立请求消息
306:生成第一随机数，根据第一随机数和第一密钥生成第二密钥；
确定DU和UE间进行完整性保护所用的完整性保护算法；
确定BEARER参数值
307:安全上下文建立响应消息
308:安全激活消息
309: 先根据步骤303中生成的根密钥、UE在DU下的主服务小区的小区标识以及所述主服务小区的载波频率生成第一密钥，再根据安全激活消息中的第一随机数、以及第一密钥生成第二密钥，，并进一步根据第二密钥生成用于对DU和UE间的控制信令进行完整性保护所用的第三密钥
310:安全激活响应消息
311:根据步骤306中确定的第三密钥、完整性保护算法、BEARER参数值、以及计数值（COUNTER）生成MAC-I
312:将MAC-I携带在控制信令
313:对接收到的控制信令进行完整性校验

图 8

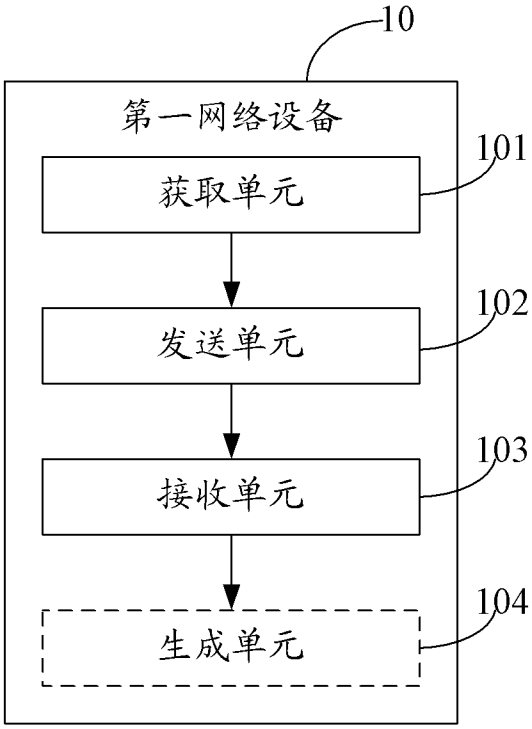
10
第一网络设备
101
获取单元
102
发送单元
103
接收单元
104
生成单元

图 9

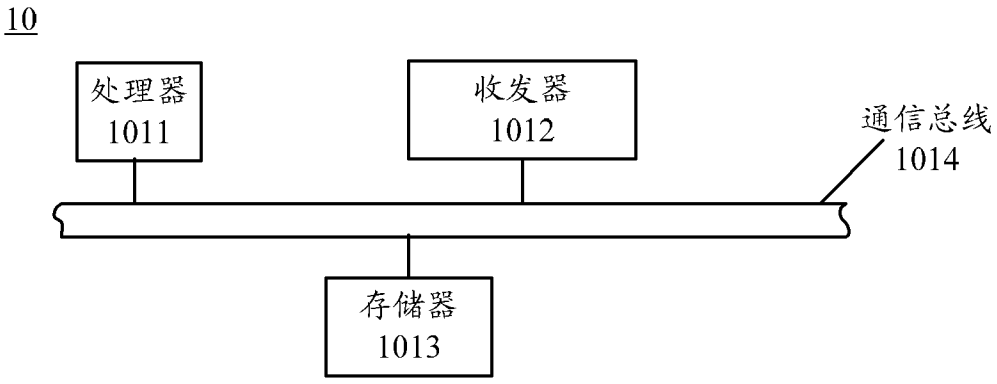
10
处理器
1011
收发器
1012
通信总线
1014
存储器
1013

图 10

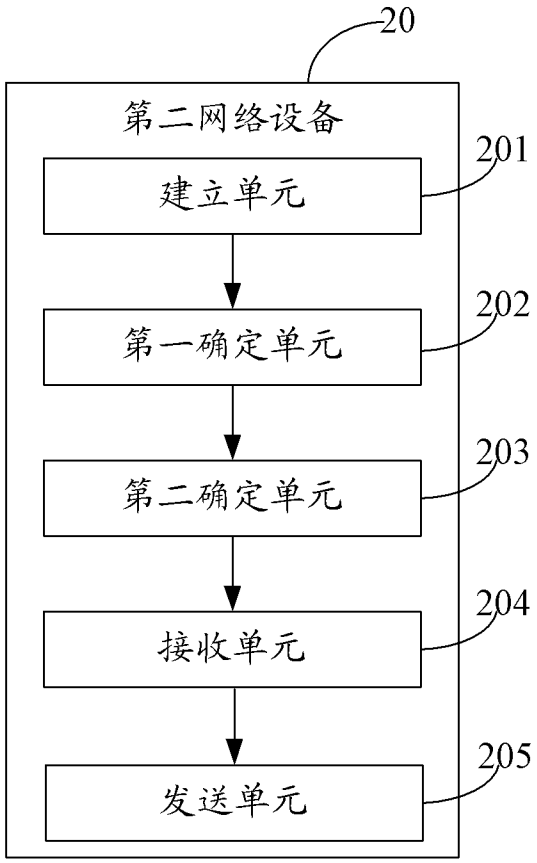
20
第二网络设备
201
建立单元
202
第一确定单元
203
第二确定单元
204
接收单元
205
发送单元

图 11

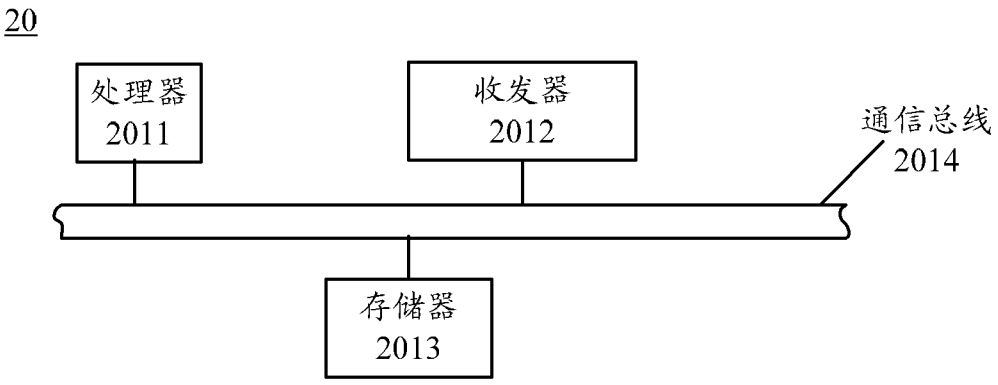
20
处理器
2011
收发器
2012
通信总线
2014
存储器
2013

图 12

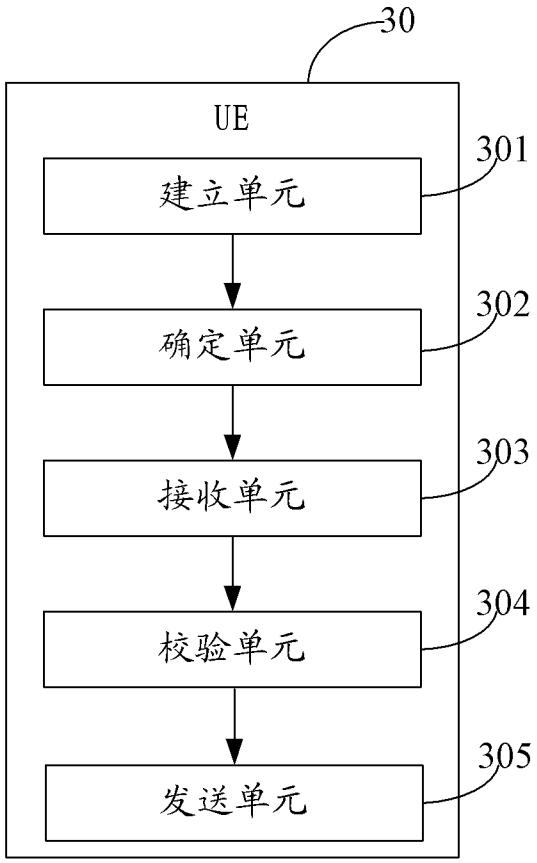
30
UE
301
建立单元
302
确定单元
303
接收单元
304
校验单元
305
发送单元

图 13

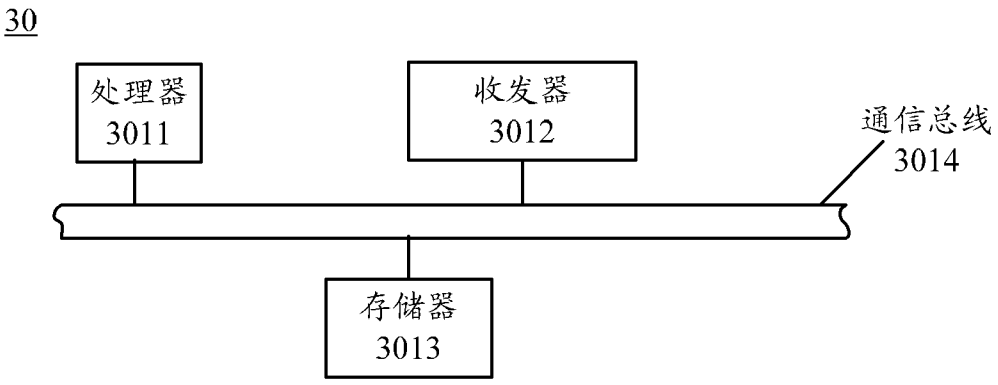
30
处理器
3011
收发器
3012
通信总线
3014
存储器
3013

图 14

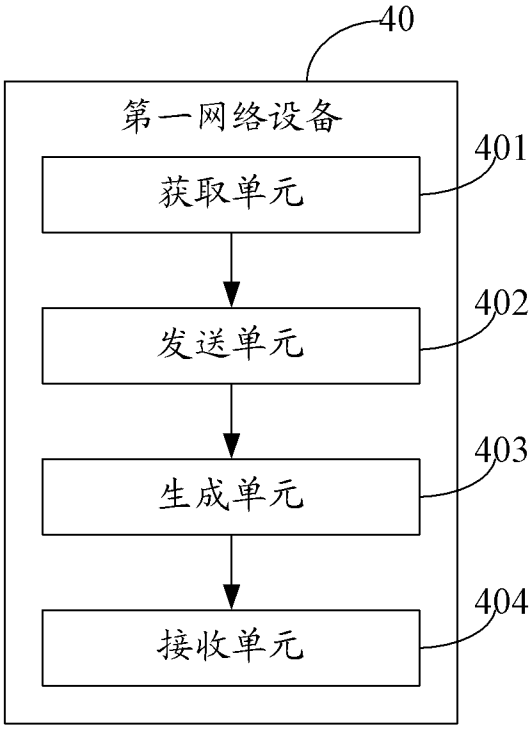
40
第一网络设备
401
获取单元
402
发送单元
403
生成单元
404
接收单元

图 15

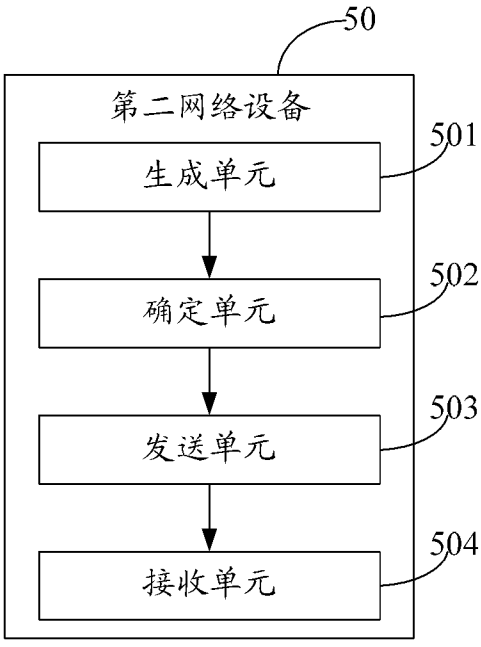
50
第二网络设备
501
生成单元
502
确定单元
503
发送单元
504
接收单元

图 16

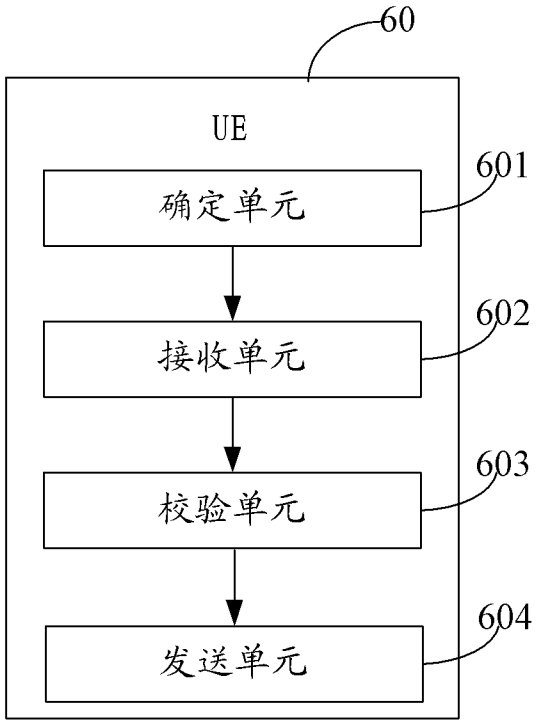

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/101410

A. CLASSIFICATION OF SUBJECT MATTER

H04W 24/10 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, IEEE: 无线接入网,RAN, 中心单元,CU, 分布单元,DU, 拉远单元,用户设备,UE, 控制信令,分离, 协议, 完整性, central, distributed, control, message, protocol, integrality

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101159893 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 April 2008 (09.04.2008), description, page 2, the sixth line from the bottom to page 4, line 8, and figures 1-9	1-53
A	CN 103945559 A (ZTE CORPORATION) 23 July 2014 (23.07.2014), entire document	1-53
A	CN 102883440 A (HUAWEI TECHNOLOGIES CO., LTD.) 16 January 2013 (16.01 .2013)., entire document	1-53
A	WO 2013173957 A1 (NOKIA CORPORATION) 28 November 2013 (28.11 .2013), entire document	1-53

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 June 2017	29 June 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer WANG, Jing Telephone No. (86-10) 62413686

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/101410

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101159893 A	09 April 2008	WO 2008119295 A1	09 October 2008
		CN 101052003 A	10 October 2007
CN 103945559 A	23 July 2014	JP 2016507976 A	10 March 2016
		EP 2947950 A2	25 November 2015
		WO 2013174335 A2	28 November 2013
		US 2015359019 A1	10 December 2015
CN 102883440 A	16 January 2013	WO 2013010418 A1	24 January 2013
		EP 271 3650 A1	02 April 2014
		JP 2014523199 A	08 September 2014
		CN 105357773 A	24 February 2016
		US 2014128092 A1	08 May 2014
WO 2013173957 A1	28 November 2013	CN 104322123 A	28 January 2015
		EP 2853123 A1	01 April 2015
		US 2015092696 A1	02 April 2015

国际检索报告

国际申请号

PCT/CN2016/101410

A. 主题的分类

H04W 24/10 (2009. 01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04W; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称，和使用的检索词 (如使用))

CNPAT, CNKI, WPI, EPODOC, IEEE:无线接入网，RAN, 中心单元，CU, 分布单元，DU, 拉远单元，用户设备，UE，控制信令，分离，协议，完整性，central, distributed, control, message, protocol, integrality

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 101159893 A (华为技术有限公司) 2008年 4月 9日 (2008 - 04 - 09) 说明书第2页倒数第6行至第4页第8行，附图1-9	1-53
A	CN 103945559 A (中兴通讯股份有限公司) 2014年 7月 23日 (2014 - 07 - 23) 全文	1-53
A	CN 102883440 A (华为技术有限公司) 2013年 1月 16日 (2013 - 01 - 16) 全文	1-53
A	WO 2013173957 A1 (NOKIA CORPORATION) 2013年 11月 28日 (2013 - 11 - 28) 全文	1-53

□ 其余文件在c栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017 年 6月 9日	2017 年 6月 29日
ISA/CN 的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451	受权官员 王静 电话号码 (86-10) 010-62413686

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/101410

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	101159893	A	2008年4月9日	WO	2008119295	A1	2008年10月9日
				CN	101052003	A	2007年10月10日
CN	103945559	A	2014年7月23日	JP	2016507976	A	2016年3月10日
				EP	2947950	A2	2015年11月25日
				WO	2013174335	A2	2013年11月28日
				US	2015359019	A1	2015年12月10日
CN	102883440	A	2013年1月16日	WO	2013010418	A1	2013年1月24日
				EP	2713650	A1	2014年4月2日
				JP	2014523199	A	2014年9月8日
				CN	105357773	A	2016年2月24日
				US	2014128092	A1	2014年5月8日
WO	2013173957	A1	2013年11月280	CN	104322123	A	2015年1月280
				EP	2853123	A1	2015年4月1日
				US	2015092696	A1	2015年4月2日