(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 3 月 19 日 (19.03.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/052362 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01)

(21) 国际申请号: PCT/CN2019/098811

(22) 国际申请日: 2019 年 8 月 1 日 (01.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811064727.0 2018年9月12日 (12.09.2018) CN

(71) 申请人: 维沃移动通信有限公司 (VIVO MOBILE COMMUNICATION CO., LTD.) [CN/CN]; 中国广东省东莞市长安镇乌沙步步高大道 283 号, Guangdong 523860 (CN)。

(72) 发明人: 郑倩 (ZHENG, Qian); 中国广东省东莞市长安镇乌沙步步高大道 283 号, Guangdong 523860 (CN)。 吴昱民 (WU, Yumin); 中国广东省东莞市长安镇乌沙步步高大道 283 号, Guangdong 523860 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街32号院枫蓝国际中心2号楼10层, Beijing 100082 (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, JO, JP, KE, KG, KH, 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, 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,

(54) **Title:** PROCESSING METHOD AND DEVICE

(54) **发明名称:** 处理方法和设备

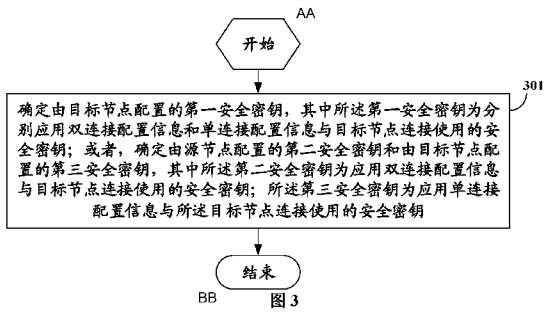


图 3

301 Determine a first security key configured by a target node, wherein the first security key is a security key for connection to the target node by respectively applying dual connectivity configuration information and single connectivity configuration information; or determine a second security key configured by a source node and a third security key configured by the target node, wherein the second security key is a security key for connection to the target node by applying the dual connectivity configuration information, and the third security key is a security key for connection to the target node by applying the single connectivity configuration information

AA Start

BB End

(57) **Abstract:** Embodiments of the present invention provide a processing method and device. The method comprises: determining a first security key configured by a target node, wherein the first security key is a security key for connection to the target node by respectively applying dual connectivity configuration information and single connectivity configuration information; or determining a second security key configured by a source node and a third security key configured by the target node, wherein the second security key is a security key for connection to the target node by applying the dual connectivity configuration information, and the third security key is a security key for connection to the target node by applying the single connectivity configuration information.

(57) **摘要:** 本公开实施例提供一种处理方法和设备。所述方法包括: 确定由目标节点配置的第一安全密钥, 其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥; 或者确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥, 其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥; 所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

WO 2020/052362 A1

[见续页]

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))。

处理方法和设备

相关申请的交叉引用

本申请主张在 2018 年 9 月 12 日在中国提交的中国专利申请 No.201811064727.0 的优先权，其全部内容通过引用包含于此。

技术领域

本公开实施例涉及通信技术领域，具体涉及一种处理方法和设备。

背景技术

为了提高通信服务质量，引入了以下通信技术：

（1）基于双连接（Dual Connectivity，DC）的移动性：

在第五代移动通信技术（Fifth-generation，5G）系统中，由于要满足 0ms 的移动性过程的中断延时，因此需要终端在移动的过程中同时在源节点和目标节点有连接进行数据的收发。要在源节点和目标节点同时保持数据连接，一种数据传输方式是采用 DC 的架构。

双连接终端的服务基站中有一个为主基站（Master Node，MN），一个为辅基站（Secondary Node，SN）。MN 的所有服务小区统称为主服务小区群组（Master Cell Group，MCG），SN 的所有服务小区统称为辅服务小区群组（Secondary Cell Group，SCG）。

（2）DC 安全机制简介：

在相关技术中的 DC 机制中，终端与 SN 通信所使用的基站密钥（Key of SN，简写为 K_{SN}）由 MN 分配，每一次 K_{SN} 的更新关联一个对应的 SN 计数值（SN Counter）。如图 1 所示，终端将基于最新获得的 K_{SN} 发起到 SN 的随机接入信道（Random Access Channel，RACH）过程，SN 通过接收终端的随机接入请求确认 SN 安全参数激活。

根据相关技术中的安全机制，当终端采用 DC 连接时，终端与目标节点（例如：SN）通信的安全密钥由源节点（例如：MN）分配，并且通过 RACH 过程确认目标节点安全参数的激活。

在采用 DC 的移动性管理的方式时，网络侧会给终端配置两套连接配置，连接配置 1 用于在移动性过程中终端同时与源节点和目标节点建立连接，连接配置 2 用于在移动性过程后终端与目标节点建立连接。

然而，相关技术中的安全机制仅能解决存在连接配置 1 时的安全更新方法，当网络存在两套连接配置如何分配目标节点使用的安全性秘钥尚没有解决方案。

发明内容

本公开实施例的一个目的在于提供一种处理方法和设备，解决在采用双连接的移动性管理过程中，当网络存在两套连接配置时，如何分配目标节点使用的安全秘钥的问题。

第一方面，本公开实施例提供一种处理方法，应用于终端，所述方法包括：

确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者

确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第二方面，本公开实施例还提供一种处理方法，应用于目标节点，所述方法包括：

根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

第三方面，本公开实施例还提供了一种处理方法，应用于源节点，所述方法包括：

向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第四方面，本公开实施例还提供了一种处理方法，应用于目标节点，所述方法包括：

向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第五方面，本公开实施例还提供了一种终端，包括：

第一确定模块，用于确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者，

第二确定模块，用于确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第六方面，本公开实施例还提供了一种目标节点，包括：

第一确认模块，用于根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

第二确认模块，用于根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

第七方面，本公开实施例还提供了一种源节点，包括：

第五发送模块，用于向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第八方面， 本公开实施例还提供了一种目标节点，包括：

第七发送模块，用于向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

第九方面，本公开实施例还提供了一种终端，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如第一方面所述的处理方法的步骤。

第十方面，本公开实施例还提供了一种网络设备，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如第二方面、第三方面或第四方面所述的处理方法的步骤。

第十一方面，本公开实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面、第二方面、第三方面或第四方面所述的处理方法的步骤。

在本公开实施例中，当网络存在两套连接配置时，可以确定目标节点使用的安全秘钥，实现在双连接架构中进行移动性管理的安全密钥更新，确保通信的可靠性。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本公开的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图1为相关技术中的双连接安全机制流程；

图2为本公开实施例的无线通信系统的架构示意图；

图3为本公开实施例的处理方法的流程图之一；

图4为本公开实施例的处理方法的流程图之二；

图5为本公开实施例的处理方法的流程图之三；

图6为本公开实施例的处理方法的流程图之四；

图7为本公开实施例的处理方法的流程图之五；

图8为本公开实施例的处理方法的流程图之六；

图9为本公开实施例的处理方法的流程图之七；

图10为本公开实施例的处理方法的流程图之八；

图11为本公开实施例的终端的结构图之一；

图12为本公开实施例的目标节点的结构图之一；

图13为本公开实施例的源节点的结构图；

图14为本公开实施例的目标节点的结构图之二；

图15为本公开实施例的终端的结构图之二；

图 16 为本公开实施例的网络设备的结构图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，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，都属于本公开保护的范围。

本申请的说明书和权利要求书中的术语“包括”以及它的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系

统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少其中之一，例如A和/或B，表示包含单独A，单独B，以及A和B都存在三种情况。

在本公开实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本公开实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

下面结合附图介绍本公开的实施例。本公开实施例提供的处理方法和设备可以应用于无线通信系统中。该无线通信系统可以为采用 5G 系统，或者演进型长期演进（Evolved Long Term Evolution，eLTE）系统，或者后续演进通信系统。参考图 2，为本公开实施例提供的一种无线通信系统的架构示意图。如图 2 所示，该无线通信系统可以包括：第一网络设备 20、第二网络设备 21 和用户设备（User Equipment，UE），例如，用户设备记做 UE22，UE22 可以与第一网络设备 20 和第二网络设备 21 通信（传输信令或传输数据）。在实际应用中上述各个设备之间的连接可以为无线连接，为了方便直观地表示各个设备之间的连接关系，图 2 中采用实线示意。

需要说明的是，上述通信系统可以包括多个 UE22，第一网络设备 20 和第二网络设备 22 可以与多个 UE22 通信。

本公开实施例提供的第一网络设备 20、第二网络设备 21 可以为基站，该基站可以为通常所用的基站，也可以为演进型基站（evolved Node Base station，eNB），还可以为 5G 系统中的网络设备（例如，下一代基站（next generation Node Base station，gNB）或发送和接收点（Transmission and Reception Point，TRP））等设备。

本公开实施例提供的用户设备可以为手机、平板电脑、笔记本电脑、超级移动个人计算机（Ultra-Mobile Personal Computer，UMPC）、上网本或者个人数字助理（Personal Digital Assistant，PDA）等。

参见图 3，本公开实施例提供一种处理方法，该方法的执行主体可以为终端，具体步骤如下：

步骤 301：确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者，

确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

其中，第一安全密钥可以称为Key，第二安全密钥可以称为Key_1，第三安全密钥可以称为Key_2。

本公开实施例中，可选地，确定由目标节点配置的第一安全密钥，包括：

从源节点接收由所述目标节点配置的第一参数，所述第一参数用于计算所述第一安全密钥；根据所述第一参数，计算所述第一安全密钥。

其中，第一参数可以是用于导出第一安全密钥（Key）的输入参数，例如：计数值（Counter）。

本公开实施例中，可选地，确定由源节点配置的第二安全密钥和目标节点配置的第三安全密钥，包括：

从所述源节点接收由源节点配置的第二参数和由所述目标节点配置的第三参数，其中，所述第二参数用于计算所述第二安全密钥，所述第三参数用于计算所述第三安全密钥；根据所述第二参数，计算所述第二安全密钥，以及根据所述第三参数，计算所述第三安全密钥。

其中，第二参数可以是用于导出第二安全密钥（Key_1）的输入参数，例如：计数值（Counter_1）。

其中，第三参数可以是用于导出第三安全密钥（Key_2）的输入参数，例如：计数值（Counter_2）。

本公开实施例中，可选地，第一参数携带在由源节点发送的无线资源控制（Radio Resource Control，RRC）重配置消息中，或者第二参数和所述第三参数携带在由源节点发送的RRC重配置消息中。

本公开实施例中，可选地，所述RRC重配置消息中还携带有以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息。

进一步地，可选地，所述RRC重配置消息中携带部分的终端的移动性管理的配置信息，该部分的终端的移动性管理的配置信息包括：用于与所述源节点和所述目标节点建立连接的双连接配置信息；用于与所述目标节点建立连接的单连接配置信息；第一参数。

或者，所述RRC重配置消息中携带部分的终端的移动性管理的配置信息，该部分的终端的移动性管理的配置信息包括：用于与所述源节点和所述目标节点建立连接的双连接配置信息；用于与所述目标节点建立连接的单连接配置信息；第三参数。

其中，终端的移动性管理的配置信息是由目标节点配置的。

本公开实施例中，可选地，在所述接收到RRC重配置消息之后，所述方法还包括：

根据所述双连接配置信息建立与所述目标节点和所述源节点的连接；

向所述源节点发送用于响应所述RRC重配置消息的RRC重配置完成消息。

可以理解的是，RRC重配置完成消息中可以携带完整性保护的消息认证码（Message Authentication Code-Integrity ，MAC-I）或截短（short）的MAC-I，也可以不携带MAC-I或截短的MAC-I。

本公开实施例中，可选地，RRC重配置完成消息包括：MAC-I或截短的MAC-I。

本公开实施例中，可选地，所述方法还包括：

在向所述源节点发送用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送随机接入请求消息；

可以理解的是，随机接入请求消息中可以携带MAC-I或截短的MAC-I，也可以不携带MAC-I或截短的MAC-I。

其中，所述MAC-I至少通过所述第一安全密钥（Key）或所述第三安全密钥（Key_2）计算获得。

进一步地，可选地，所述MAC-I通过所述第一安全密钥（Key）、所述源节点的物理小区标识（Physical Cell ID，PCI）、所述源节点给所述终端分配的小区无线网络临时标识（Cell Radio Network Temporary Identifier，C-RNTI）、所述目标节点的小区标识（ID）中的一项或多项计算获得；

或者，所述MAC-I通过所述第三安全密钥（Key_2）、所述源节点的PCI、所述源节点给所述终端分配的C-RNTI、所述目标节点的小区ID中的一项或多项计算获得。

本公开实施例中，可选地，在向所述目标节点发起的随机接入过程完成之后，所述方法还包括：

根据所述单连接配置建立与所述目标节点的连接，并生成单连接配置完成消息；

向所述目标节点发送所述单连接配置完成消息；

其中所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；或者，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护。

本公开实施例适用于采用双连接架构进行移动性管理的安全密钥更新，提高通信的可靠性，进一步地，支持终端与目标节点通信的加密和/或完整性保护功能。

参见图 4，本公开实施例还提供一种处理方法，该方法的执行主体可以为目标节点，具体步骤如下：

步骤 401：根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

本公开实施例中，可选地，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从所述源节点接收到所述双连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过第一安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述随机接入请求消息时，确认所述终端的加密和/或完整性保护功能的激活；

当从所述终端接收到所述单连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥。

本公开实施例中，可选地，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括：

当从所述源节点接收到所述双连接配置完成消息，或者从所述终端接收到所述随机接入请求消息时，确认基于第二安全密钥的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过所述第二安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述单连接配置完成消息时，确认基于所述第三安全密钥的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护；

当确认基于所述第二安全密钥的加密和/或完整性保护功能的激活，以及确认基于所述第三安全密钥的加密和/或完整性保护功能的激活时，确认所述终端的加密和/或完整性保护功能的激活；

其中，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例中，可选地，所述根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第一安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第一安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第三安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第三安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例适用于采用双连接架构进行移动性管理的安全密钥更新，提高通信的可靠性，进一步地，支持终端与目标节点通信的加密和/或完整性保护功能。

参见图 5，本公开实施例还提供一种处理方法，该方法的执行主体可以为源节点，具体步骤如下：

步骤 501：向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例中，可选地，所述向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数，包括：

向终端发送RRC重配置消息，其中，所述RRC重配置消息包括：所述终端的移动性管理的配置信息，所述终端的移动性管理的配置信息至少包括：由目标节点配置的第一参数；或者所述终端的移动性管理的配置信息至少包括：由所述源节点配置的第二参数和由所述目标节点配置的第三参数。

本公开实施例中，可选地，所述方法还包括：

在接收到用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送双连接配置完成消息。

本公开实施例中，可选地，从所述RRC重配置完成消息中获取MAC-I或截短的MAC-I；向所述目标节点发送双连接配置完成消息，所述双连接配置完成消息包括：所述MAC-I或截短的MAC-I；

其中，所述MAC-I通过所述第一安全密钥或第三安全密钥计算获得。

进一步地，可选地，所述MAC-I通过所述第一安全密钥（Key）、所述源节点的物理小区标识（Physical Cell ID，PCI）、所述源节点给所述终端分配的小区无线网络临时标识（Cell Radio Network Temporary Identifier，C-RNTI）、所述目标节点的小区标识（ID）中的一项或多项计算获得；

或者，所述MAC-I通过所述第三安全密钥（Key_2）、所述源节点的PCI、所述源节点给所述终端分配的C-RNTI、所述目标节点的小区ID中的一项或多项计算获得。

本公开实施例中，可选地，在所述向终端发送RRC重配置消息之前，所述方法还包括：

从所述目标节点接收所述终端的移动性管理的配置信息。

本公开实施例中，可选地，所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

本公开实施例适用于采用双连接架构进行移动性管理的安全密钥更新，提高通信的可靠性，进一步地，支持终端与目标节点通信的加密和/或完整性保护功能。

参见图 6，本公开实施例还提供一种处理方法，该方法的执行主体可以为目标节点，具体步骤如下：

步骤 601：向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例，可选地，所述向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数，包括：

向源节点发送终端的移动性管理的配置信息，所述终端的移动性管理的配置信息包括：由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数。

本公开实施例，可选地，所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

本公开实施例，可选地，所述方法还包括：

根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

本公开实施例中，可选地，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从所述源节点接收到所述双连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过第一安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述随机接入请求消息时，确认所述终端的加密和/或完整性保护功能的激活；

当从所述终端接收到所述单连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥。

本公开实施例中，可选地，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括：

当从所述源节点接收到所述双连接配置完成消息，或者从所述终端接收到所述随机接入请求消息时，确认基于第二安全密钥的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过所述第二安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述单连接配置完成消息时，确认基于所述第三安全密钥的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护；

当确认基于所述第二安全密钥的加密和/或完整性保护功能的激活，以及确认基于所述第三安全密钥的加密和/或完整性保护功能的激活时，确认所述终端的加密和/或完整性保护功能的激活；

其中，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例中，可选地，所述根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第一安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第一安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第三安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第三安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例适用于采用双连接架构进行移动性管理的安全密钥更新，提高通信的可靠性，进一步地，支持终端与目标节点通信的加密和/或完整性保护功能。

示例 1：

在示例 1 中，分别应用两套配置信息与目标节点连接使用的安全密钥（Key）由目标节点分配，目标节点通过双连接配置完成消息、随机接入请求、单连接配置完成消息中的任意一项确认终端的加密功能和/或完整性保护功能的激活。

其中，两套配置信息包括：双连接配置（dcConfig）信息和单连接配置（targetConfig）信息。参见图 7，具体步骤如下：

步骤 1：源节点发送移动性管理请求信息给目标节点。

例如：移动性管理请求信息可以为切换请求，该移动性管理请求信息包括：终端的安全能力信息，其中终端的安全能力信息可以是以下一项或多项：支持的用户面（User Plane，UP）加密算法、UP 完整性保护算法、支持的控制面无线资源控制（Radio Resource Control，RRC）加密算法、RRC 完整性保护算法。

步骤 2：根据步骤 1 中的移动性管理请求信息，目标节点生成终端的移动性管理的配置信息，并将该终端的移动性管理的配置信息发送给源节点。

例如：终端的移动性管理的配置信息可以为切换命令，其中，该终端的移动性管理的配置信息包括：

（1）用于同时保持源节点和目标节点连接的双连接配置（dcConfig）信息。可以理解的是，该双连接配置信息仅临时用于移动性过程中终端同时保持源节点和目标节点的连接。

（2）用于目标节点连接的单连接配置（targetConfig）信息。可以理解的是，该单连接配置信息用于移动性过程结束后终端和目标节点的连接。

（3）应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥（Key）。

（4）安全密钥（Key）导出的输入参数，例如：计数值（Counter）。

步骤 3：源节点将步骤 2 中部分终端的移动性管理的配置信息下发给终端，例如：通过 RRC 重配置消息将部分终端的移动性管理的配置信息发送给终端。

可以理解的是，将步骤 2 中除了“（3）应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥（Key）”之外的内容下发给终端。安全密钥（Key）不能在空口中发送，终端可以通过计数值（Counter）导出安全密钥（Key）。

终端接收到 RRC 重配置消息后，可以执行以下一项或多项动作：

（1）根据计数值（Counter）导出终端使用的安全密钥（Key）；

（2）应用双连接配置（dcConfig）信息同时建立与源节点和目标节点的连接。

步骤 4：终端向源节点发送 RRC 重配置完成消息。

步骤 5：在步骤 4 完成后，源节点发送双连接配置完成消息给目标节点，若目标节点成功接收到双连接配置完成消息，目标节点确认该终端的加密功能和/或完整性保护功能的激活。

步骤 6：在步骤 4 完成后，终端向目标节点发起随机接入请求，若目标节点成功接收到该终端的随机接入请求消息，目标节点确认该终端的加密和/或完整性保护功能的激活。

步骤 7：在步骤 6 完成后，终端执行如下动作：

（1）应用单连接配置（targetConfig）信息仅建立与目标节点的连接。

（2）生成单连接配置（targetConfig）完成消息，所述单连接配置（targetConfig）完成消息用安全密钥（Key）进行加密和/或完整性保护。

（3）向目标节点发送单连接配置（targetConfig）完成消息，若目标节点成功接收到单连接配置（targetConfig）完成消息，目标节点确认该终端的加密和/或完整性保护功能的激活。

可以理解的是，步骤 5、步骤 6 和步骤 7 中“目标节点确认该终端的加密功能和/或完整性保护功能的激活”的条件任一项满足时，目标节点确认该终端的加密和/或完整性保护功能的激活。

示例 2：

在示例 2 中，应用双连接配置（dcConfig）信息与目标节点连接使用的安全密钥（以下简称为 Key_1）由源节点分配，应用单连接配置（targetConfig）信息与目标节点连接使用的安全密钥（以下简称为 Key_2）由目标节点分配，目标节点通过双连接配置完成消息、随机接入请求、单连接配置完成消息中的任意一项确认终端的加密功能和/或完整性保护功能的激活。参见图 8，具体步骤如下：

步骤 1：源节点发送移动性管理请求信息给目标节点。

例如：移动性管理请求信息可以为切换请求，该移动性管理请求信息包括：终端的安全能力信息和应用双连接配置（dcConfig）信息与目标节点连接使用的 Key_1。

其中，终端的安全能力信息可以是以下一项或多项：支持的 UP 加密算法、UP 完整性保护算法、支持的控制面 RRC 加密算法和 RRC 完整性保护算

法。

步骤 2：根据步骤 1 中的移动性管理请求信息，目标节点生成终端的移动性管理的配置信息，并将该终端的移动性管理的配置信息发送给源节点。

例如：终端的移动性管理的配置信息可以为切换命令，其中，该终端的移动性管理的配置信息包括：

（1）用于同时保持源节点和目标节点连接的双连接配置（dcConfig）信息。可以理解的是，该双连接配置信息仅临时用于移动性过程中终端同时保持源节点和目标节点的连接。

（2）用于目标节点连接的单连接配置（targetConfig）信息，可以理解的是，该单连接配置信息用于移动性过程结束后终端和目标节点的连接。

（3）应用单连接配置（targetConfig）信息与目标节点连接使用的 Key_2。

（4）Key_2 导出的输入参数，例如：计数值（Counter_2）。

步骤 3：源节点将步骤 2 中终端的移动性管理的配置信息和 Key_1 导出的输入参数（例如：计数值（Counter_1））下发给终端，例如：通过 RRC 重配置消息将终端的移动性管理的配置信息和 Counter_1 发送给终端。

可以理解的是，将步骤 2 中除了“（3）应用单连接配置（targetConfig）信息与目标节点连接使用的 Key_2”之外的内容下发给终端。Key_2 不能在空口中发送，终端可以通过输入参数（计数值（Counter_2））导出 Key2。

需要说明的是，由于 Key_1 是源节点分配，因此对应的 Key_1 导出的输入参数（例如：计数值（Counter_1））也由源节点配置，因此不需要体现在步骤 2 中，而是在步骤 2 完成后，跟随步骤 2 获得的部分“终端的移动性管理的配置信息”一起下发给终端。

可选地，终端接收到 RRC 重配置消息后，可以执行以下一项或多项动作：

（1）根据计数值（Counter_1）导出终端使用的安全密钥 Key_1；

（2）根据计数值（Counter_2）导出终端使用的安全密钥 Key_2；

（3）应用双连接配置（dcConfig）信息同时建立与源节点和目标节点的连接。

步骤 4：终端向源节点发送 RRC 重配置完成消息。

步骤 5：在步骤 4 完成后，源节点发送双连接配置（dcConfig）完成消息

给目标节点，若目标节点成功接收到双连接配置（dcConfig）完成消息，目标节点确认基于 Key_1 的加密和/或完整性保护功能激活。

步骤 6：在步骤 4 完成后，终端向目标节点发起随机接入请求，若目标节点成功接收到终端的随机接入请求消息，目标节点确认基于 Key_1 的加密和/或完整性保护功能激活。

步骤 7：在步骤 6 完成后，终端执行如下动作：

（1）应用单连接配置（targetConfig）信息仅建立与目标节点的连接；

（2）生成单连接配置（targetConfig）完成消息，所述单连接配置（targetConfig）完成消息用所述 Key_2 进行加密和/或完整性保护；

（3）向目标节点发送所述单连接配置（targetConfig）完成消息，若目标节点成功接收到单连接配置（targetConfig）完成消息，目标节点确认基于 Key_2 的加密和/或完整性保护功能激活。

可以理解的是，当确认基于 Key_1 的加密和/或完整性保护功能激活，以及基于 Key_2 的加密和/或完整性保护功能激活时，目标节点确认该终端的加密和/或完整性保护功能的激活。

示例 3：

在示例 1 的基础上，目标节点基于双连接配置完成消息、随机接入请求消息其中任意一项所携带的 MAC-I 或截短的 MAC-I 验证，确认终端的加密功能和/或完整性保护功能的激活。参见图 9，具体步骤如下：

步骤 1：源节点发送移动性管理请求信息给目标节点。

步骤 2：根据步骤 1 中的移动性管理请求信息，目标节点生成终端的移动性管理的配置信息，并将该终端的移动性管理的配置信息发送给源节点。

步骤 3：源节点将步骤 2 中部分终端的移动性管理的配置信息下发给终端，例如：通过 RRC 重配置消息将部分终端的移动性管理的配置信息发送给终端。

需要说明的是，示例 3 中的步骤 1~步骤 3 的内容与示例 1 中的步骤 1~步骤 3 的内容相同。

步骤 4：终端向源节点发送 RRC 重配置完成消息，RRC 重配置完成消息包含 MAC-I 或截短的 MAC-I。

其中，MAC-I 通过 Key、源节点的物理小区标识（Physical Cell Identifier，PCI），源节点给终端分配的 小区无线网络临时标识（Cell Radio Network Temporary Identifier，C-RNTI），目标节点的小区标识（Identification，ID）中的一项或多项计算获得，所述截短的 MAC-I 是 MAC-I 的截短形式。

步骤 5：源节点将步骤 4 中的 MAC-I 或截短的 MAC-I 通过双连接配置（dcConfig）完成消息转发给目标节点，若目标节点用所述 Key 对 MAC-I 或截短的 MAC-I 验证通过，目标节点确认该终端的加密和/或完整性保护功能的激活。

步骤 6：在步骤 4 完成后，终端向目标节点发送随机接入请求消息，且在随机接入请求消息中包含 MAC-I 或截短的 MAC-I，若目标节点用所述 Key 对 MAC-I 或截短的 MAC-I 完整性验证通过，目标节点确认该终端的加密和/或完整性保护功能的激活。

可以理解的是，步骤 5、步骤 6 和步骤 7 中“目标节点确认该终端的加密功能和/或完整性保护功能的激活”的条件任一项满足时，目标节点确认该终端的加密和/或完整性保护功能的激活。

示例 4：

在示例 2 的基础上，目标节点通过基于双连接配置完成消息、随机接入请求消息的其中一项所携带的 MAC-I 或截短的 MAC-I，确认终端的加密功能和/或完整性保护功能的激活。参见图 10，具体步骤如下：

步骤 1：源节点发送移动性管理请求信息给目标节点。

步骤 2：根据步骤 1 中的移动性管理请求信息，目标节点生成终端的移动性管理的配置信息，并将该终端的移动性管理的配置信息发送给源节点。

步骤 3：源节点将步骤 2 中部分终端的移动性管理的配置信息和 Key_1 导出的输入参数（例如：计数值（Counter_1））下发给终端。

需要说明的是，示例 3 中的步骤 1~步骤 3 的内容与示例 1 中的步骤 1~步骤 3 的内容相同。

步骤 4：终端向源节点发送 RRC 重配置完成消息，所述 RRC 重配置完成消息包含：MAC-I 或截短的 MAC-I。

其中，MAC-I 通过 Key_2、源节点的 PCI、源节点给终端分配的 C-RNTI、

目标节点的小区 ID 中的一项或多项计算获得。所述截短的 MAC-I 是 MAC-I 的截短形式。

步骤 5：源节点将步骤 4 中的 MAC-I 或截短的 MAC-I 通过双连接配置（dcConfig）完成消息转发给目标节点，若目标节点成功接收到双连接配置（dcConfig)完成消息，并且目标节点用所述 Key_2 对 MAC-I 或截短的 MAC-I 验证通过，目标节点确认该终端的加密和/或完整性保护功能激活。

步骤 6：在步骤 4 完成后，终端向目标节点发起随机接入请求，所述随机接入请求消息中包含 MAC-I 或截短的 MAC-I，若目标节点成功接收到该终端的随机接入请求消息，并且目标节点用所述 Key_2 对 MAC-I 或截短的 MAC-I 完整性验证通过，目标节点确认该终端的加密和/或完整性保护功能激活。

示例 1 至示例 4 描述了基于DC架构进行切换的场景，可以理解的是，本公开实施例不仅适用于基于DC架构进行切换的场景，还可以适用于DC架构的SCG变更、SCG删除和SCG添加场景。

本公开实施例中还提供了一种终端，由于终端解决问题的原理与本公开实施例中处理方法相似，因此该终端的实施可以参见方法的实施，重复之处不再敷述。

参见图 11，本公开实施例还提供一种终端，该终端 1100 包括：

第一确定模块 1101，用于确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者，

第二确定模块 1102，用于确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例，可选地，所述第一确定模块进一步用于：从所述源节点接收由所述目标节点配置的第一参数，所述第一参数用于计算所述第一安全密钥；根据所述第一参数，计算所述第一安全密钥。

本公开实施例，可选地，所述第二确定模块进一步用于：从所述源节点接收由所述源节点配置的第二参数和由所述目标节点配置的第三参数，其中，所述第二参数用于计算所述第二安全密钥，所述第三参数用于计算所述第三安全密钥；根据所述第二参数，计算所述第二安全密钥，以及根据所述第三参数，计算所述第三安全密钥。

本公开实施例，可选地，所述第一参数携带在由所述源节点发送的RRC重配置消息中，或者所述第二参数和所述第三参数携带在由所述源节点发送的RRC重配置消息中。

本公开实施例，可选地，所述RRC重配置消息中还携带有以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

本公开实施例，可选地，所述终端还包括：

第一连接模块，用于根据所述双连接配置信息建立与所述目标节点和所述源节点的连接；

第一发送模块，用于向所述源节点发送用于响应RRC重配置消息或RRC重配置消息的RRC重配置完成消息。

本公开实施例，可选地，所述终端还包括：

第二发送模块，用于在向所述源节点发送用于响应所述RRC重配置消息或RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送随机接入请求消息。

本公开实施例，可选地，所述RRC重配置完成消息或所述随机接入请求消息包括：完整性保护的消息认证码MAC-I或截短的MAC-I；

其中，所述MAC-I至少通过所述第一安全密钥或所述第三安全密钥计算获得。

本公开实施例，可选地，第二连接模块，用于在向所述目标节点发起的随机接入过程完成之后，根据所述单连接配置建立与所述目标节点的连接，并生成单连接配置完成消息；

第三发送模块，用于向所述目标节点发送所述单连接配置完成消息；

其中，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；或者，

所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护。

本公开实施例提供的终端，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

本公开实施例中还提供了一种目标节点，由于目标节点解决问题的原理与本公开实施例中处理方法相似，因此该目标节点的实施可以参见方法的实施，重复之处不再敷述。

参见图 12，本公开实施例还提供一种目标节点，该目标节点 1200 包括：

第一确认模块 1201，用于根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

第二确认模块 1202，用于根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

本公开实施例，可选地，所述第一确认模块进一步用于执行以下任意一项：

当从所述源节点接收到所述双连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过第一安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述随机接入请求消息时，确认所述终端的加密和/或完整性保护功能的激活；

当从所述终端接收到所述单连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥。

本公开实施例，可选地，所述第一确认模块进一步用于：

当从所述源节点接收到所述双连接配置完成消息，或者从所述终端接收到所述随机接入请求消息时，确认基于第二安全密钥的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过所述第二安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述单连接配置完成消息时，确认基于所述第三安全密钥的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护；

当确认基于所述第二安全密钥的加密和/或完整性保护功能的激活，以及确认基于所述第三安全密钥的加密和/或完整性保护功能的激活时，确认所述终端的加密和/或完整性保护功能的激活；

其中，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例，可选地，所述第二确认模块进一步用于执行以下任意一项：

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第一安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第一安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第三安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第三安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置与所述目标节点连接使用的安全密钥。

本公开实施例提供的目标节点，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

本公开实施例中还提供了一种源节点，由于源节点解决问题的原理与本公开实施例中处理方法相似，因此该源节点的实施可以参见方法的实施，重复之处不再敷述。

参见图 13，本公开实施例还提供一种源节点，该源节点 1300 包括：

第五发送模块 1301，用于向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例，可选地，第五发送模块 1301 进一步用于：向终端发送RRC重配置消息，其中，所述RRC重配置消息包括：所述终端的移动性管理的配置信息，所述终端的移动性管理的配置信息至少包括：由目标节点配置的第一参数；或者所述终端的移动性管理的配置信息至少包括：由所述源节点配置的第二参数和由所述目标节点配置的第三参数

本公开实施例，可选地，所述源节点还包括：

第六发送模块，用于在接收到用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送双连接配置完成消息。

本公开实施例，可选地，所述第六发送模块进一步用于：从所述RRC重配置完成消息中获取MAC-I或截短的MAC-I；向所述目标节点发送双连接配置完成消息，所述双连接配置完成消息包括：所述MAC-I或截短的MAC-I；

其中，所述MAC-I至少通过所述第一安全密钥或第三安全密钥计算获得。

本公开实施例，可选地，所述源节点还包括：第三接收模块，用于从所述目标节点接收所述终端的移动性管理的配置信息。

本公开实施例，可选地，所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

本公开实施例提供的源节点，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

本公开实施例中还提供了一种目标节点，由于目标节点解决问题的原理与本公开实施例中处理方法相似，因此该目标节点的实施可以参见方法的实施，重复之处不再敷述。

参见图 14，本公开实施例还提供一种目标节点，该目标节点 1400 包括：

第七发送模块 1401，用于向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例，可选地，所述向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数，包括：

向源节点发送终端的移动性管理的配置信息，所述终端的移动性管理的配置信息包括：由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数。

本公开实施例，可选地，所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

本公开实施例，可选地，所述目标节点还包括：

第三确认模块，用于根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

第四确认模块，用于根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

本公开实施例提供的目标节点，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

如图 15 所示，图 15 所示的终端 1500 包括：至少一个处理器 1501、存储器 1502、至少一个网络接口 1504 和用户接口 1503。终端 1500 中的各个组件通过总线系统 1505 耦合在一起。可理解，总线系统 1505 用于实现这些组件之间的连接通信。总线系统 1505 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 15 中将各种总线都标为总线系统 1505。

其中，用户接口 1503 可以包括显示器、键盘或者点击设备（例如，鼠标，轨迹球（trackball）、触感板或者触摸屏等。

可以理解，本公开实施例中的存储器 1502 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data rate

SDRAM，DDRSDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（Synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DRRAM）。本公开实施例描述的系统和方法的存储器 1502 旨在包括但不限于这些和任意其它适合类型的存储器。

在一些实施方式中，存储器 1502 保存了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：操作系统 15021 和应用程序 15022。

其中，操作系统 15021，包含各种系统程序，例如框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。应用程序 15022，包含各种应用程序，例如媒体播放器（Media Player）、浏览器（Browser）等，用于实现各种应用业务。实现本公开实施例方法的程序可以包含在应用程序 15022 中。

在本公开的一个实施例中，通过调用存储器 1502 保存的程序或指令，具体的，可以是应用程序 15022 中保存的程序或指令，执行时实现以下步骤：确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

本公开实施例提供的终端，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

请参阅图 16，图 16 是本公开实施例应用的网络设备的结构图，如图 16 所示，网络设备 1600 包括：处理器 1601、收发机 1602、存储器 1603 和总线接口，其中：

在本公开的一个实施例中，网络设备 1600 还包括：存储在存储器上 1603 并可在处理器 1601 上运行的程序，程序被处理器 1601 执行时实现如下步骤：根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，根据双连接

配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

在本公开的另一个实施例中，网络设备 1600 还包括：存储在存储器上 1603 并可在处理器 1601 上运行的程序，程序被处理器 1601 执行时实现如下步骤：向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

在本公开的又一个实施例中，网络设备 1600 还包括：存储在存储器上 1603 并可在处理器 1601 上运行的程序，程序被处理器 1601 执行时实现如下步骤：向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

在图 16 中，总线架构可以包括任意数量的互联的总线和桥，具体由处理器 1601 代表的一个或多个处理器和存储器 1603 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 1602 可以是多个元件，即包括发送机和接收机，提供用于在传输介质上与各种其他装置通信的单元。

处理器 1601 负责管理总线架构和通常的处理，存储器 1603 可以存储处理器 1601 在执行操作时所使用的数据。

本公开实施例提供的网络设备，可以执行上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

结合本公开公开内容所描述的方法或者算法的步骤可以硬件的方式来实

现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于RAM、闪存、ROM、EPROM、EEPROM、寄存器、硬盘、移动硬盘、只读光盘或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于核心网接口设备中。当然，处理器和存储介质也可以作为分立组件存在于核心网接口设备中。

本领域技术人员应该可以意识到，在上述一个或多个示例中，本公开所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

以上所述的具体实施方式，对本公开的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本公开的具体实施方式而已，并不用于限定本公开的保护范围，凡在本公开的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本公开的保护范围之内。

本领域内的技术人员应明白，本公开实施例可提供为方法、系统、或计算机程序产品。因此，本公开实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本公开实施例是参照根据本公开实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机

器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本公开实施例进行各种改动和变型而不脱离本公开的精神和范围。这样，倘若本公开实施例的这些修改和变型属于本公开权利要求及其等同技术的范围之内，则本公开也意图包含这些改动和变型在内。

权 利 要 求 书

1. 一种处理方法，应用于终端，其中，所述方法包括：

确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者

确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

2. 根据权利要求 1 所述的方法，其中，所述确定由目标节点配置的第一安全密钥，包括：

从所述源节点接收由所述目标节点配置的第一参数，所述第一参数用于计算所述第一安全密钥；

根据所述第一参数，计算所述第一安全密钥。

3. 根据权利要求 1 所述的方法，其中，所述确定由源节点配置的第二安全密钥和目标节点配置的第三安全密钥，包括：

从所述源节点接收由所述源节点配置的第二参数和由所述目标节点配置的第三参数，其中，所述第二参数用于计算所述第二安全密钥，所述第三参数用于计算所述第三安全密钥；

根据所述第二参数，计算所述第二安全密钥，以及根据所述第三参数，计算所述第三安全密钥。

4. 根据权利要求 2 或 3 所述的方法，其中，所述第一参数携带在由所述源节点发送的RRC重配置消息中，或者所述第二参数和所述第三参数携带在由所述源节点发送的RRC重配置消息中。

5. 根据权利要求 4 所述的方法，其中，所述RRC重配置消息中还携带有以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述方法还包括：

根据所述双连接配置信息建立与所述目标节点和所述源节点的连接；

向所述源节点发送用于响应所述RRC重配置消息的RRC重配置完成消息。

6. 根据权利要求 5 所述的方法，还包括：

在向所述源节点发送用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送随机接入请求消息。

7. 根据权利要求 5 或 6 所述的方法，还包括：

所述RRC重配置完成消息或所述随机接入请求消息包括：完整性保护的消息认证码MAC-I或截短的MAC-I；

其中，所述MAC-I至少通过所述第一安全密钥或所述第三安全密钥计算获得。

8. 根据权利要求 6 所述的方法，其中，在向所述目标节点发起的随机接入过程完成之后，所述方法还包括：

根据所述单连接配置建立与所述目标节点的连接，并生成单连接配置完成消息；向所述目标节点发送所述单连接配置完成消息；

其中，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；或者，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护。

9. 一种处理方法，应用于目标节点，其中，所述方法包括：

根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

10. 根据权利要求 9 所述的方法，其中，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从源节点接收到所述双连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过第一安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述随机接入请求消息时，确认所述终端的加密和/或完整性保护功能的激活；

当从所述终端接收到所述单连接配置完成消息时，确认所述终端的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第一安全密钥进行加密和/或完整性保护；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥。

11. 根据权利要求 9 所述的方法，其中，所述根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活，包括：

当从源节点接收到所述双连接配置完成消息，或者从所述终端接收到所述随机接入请求消息时，确认基于第二安全密钥的加密和/或完整性保护功能的激活，所述双连接配置完成消息通过所述第二安全密钥进行加密和/或完整性保护；

当从所述终端接收到所述单连接配置完成消息时，确认基于第三安全密钥的加密和/或完整性保护功能的激活，所述单连接配置完成消息通过所述第三安全密钥进行加密和/或完整性保护；

当确认基于所述第二安全密钥的加密和/或完整性保护功能的激活，以及确认基于所述第三安全密钥的加密和/或完整性保护功能的激活时，确认所述终端的加密和/或完整性保护功能的激活；

其中，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

12. 根据权利要求 9 所述的方法，其中，所述根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活，包括以下任意一项：

当从源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第一安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第一安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述源节点接收双连接配置完成消息，且所述双连接配置完成消息中携带的MAC-I或截短的MAC-I通过第三安全密钥的验证时，确认终端的加密和/或完整性保护功能的激活；

当从所述终端接收随机接入请求消息，且所述随机接入请求消息中携带的MAC-I或截短的MAC-I通过第三安全密钥验证时，确认终端的加密和/或完整性保护功能的激活；

其中，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

13. 一种处理方法，应用于源节点，其中，所述方法包括：

向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

14. 根据权利要求 13 所述的方法，其中，

所述向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数，包括：

向终端发送RRC重配置消息，其中，所述RRC重配置消息包括：所述终端的移动性管理的配置信息，所述终端的移动性管理的配置信息至少包括：由目标节点配置的第一参数；或者所述终端的移动性管理的配置信息至少包括：由所述源节点配置的第二参数和由所述目标节点配置的第三参数。

15. 根据权利要求 14 所述的方法，还包括：

在接收到用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送双连接配置完成消息。

16. 根据权利要求 15 所述的方法，其中，所述在接收到用于响应所述RRC重配置消息的RRC重配置完成消息之后，向所述目标节点发送双连接配置完成消息，包括：

从所述RRC重配置完成消息中获取MAC-I或截短的MAC-I；

向所述目标节点发送双连接配置完成消息，所述双连接配置完成消息包括：所述MAC-I或截短的MAC-I；

其中，所述MAC-I至少通过所述第一安全密钥或第三安全密钥计算获得。

17. 根据权利要求 14 所述的方法，其中，在所述向终端发送RRC重配置消息之前，所述方法还包括：

从所述目标节点接收所述终端的移动性管理的配置信息。

18. 根据权利要求 13 至 17 任一项所述的方法，其中，

所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

19. 一种处理方法，应用于目标节点，其中，所述方法包括：

向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

20. 根据权利要求 19 所述的方法，其中，所述向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数，包括：

向源节点发送终端的移动性管理的配置信息，所述终端的移动性管理的配置信息包括：由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数。

21. 根据权利要求 20 所述的方法，其中，所述终端的移动性管理的配置信息还包括以下一项或多项：

用于与所述源节点和所述目标节点建立连接的双连接配置信息；

用于与所述目标节点建立连接的单连接配置信息；

所述第一安全密钥；

所述第三安全密钥。

22. 根据权利要求 19 所述的方法，还包括：

根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

23. 一种终端，包括：

第一确定模块，用于确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者，

第二确定模块，用于确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

24. 一种目标节点，包括：

第一确认模块，用于根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；或者，

第二确认模块，用于根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活。

25. 一种源节点，包括：

第五发送模块，用于向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第二参数用于计算第二安全密钥，所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

26. 一种目标节点，包括：

第七发送模块，用于向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数；

其中，所述第一参数用于计算第一安全密钥，所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；

所述第三参数用于计算第三安全密钥，所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥。

27. 一种终端，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 1 至 8 中任一项所述的处理方法的步骤。

28. 一种网络设备，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 9 至 12 中任一项所述的处理方法的步骤；或者，实现如权利要求 13 至 18 中任一项所述的处理方法的步骤；或者，实现如权利要求 19 至 22 中任一项所述的处理方法的步骤。

29. 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 8 中任一项所述的处理方法的步骤；或者实现如权利要求 9 至 12 中任一项所述的处理方法的步骤；或者，实现如权利要求 13 至 18 中任一项所述的处理方法的步骤；或者，实现如权利要求 19 至 22 中任一项所述的处理方法的步骤。

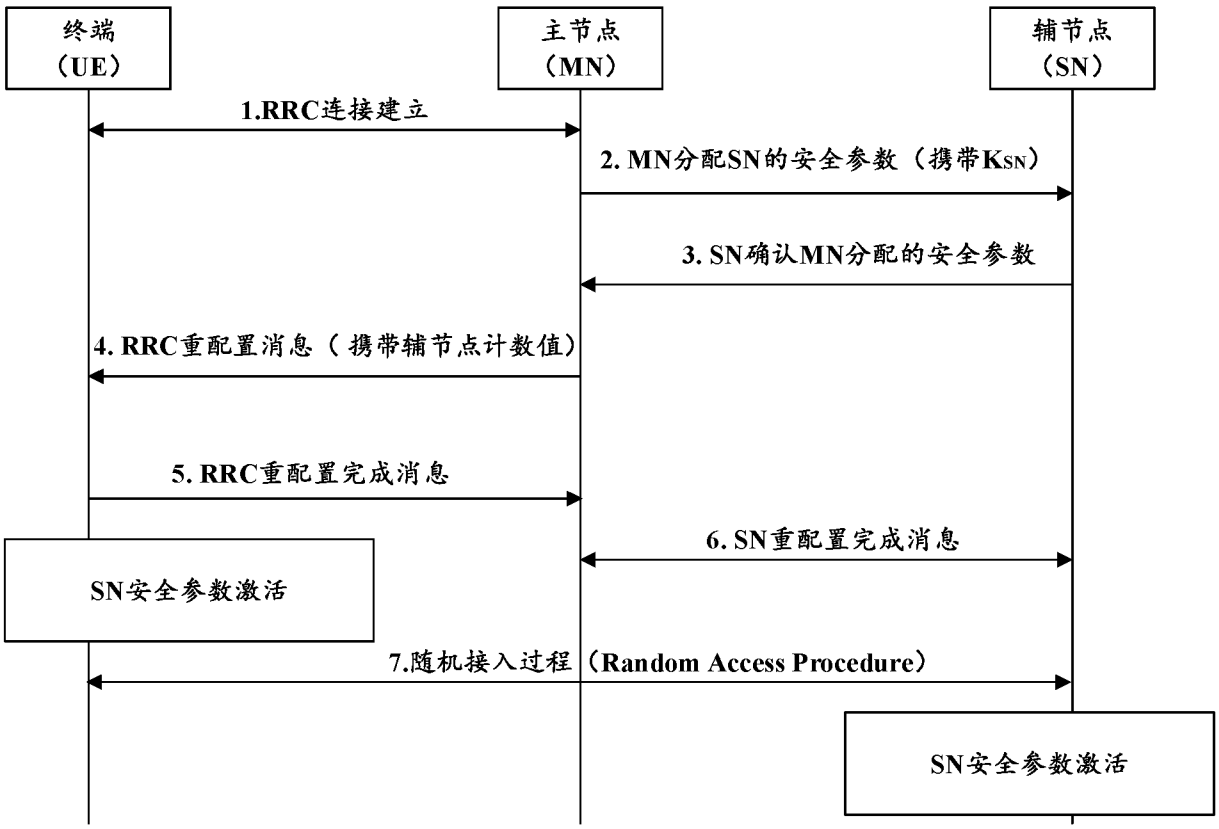

终端
（UE）
主节点
（MN）
辅节点
（SN）
1.RRC连接建立
2. MN分配SN的安全参数（携带KSN）
3. SN确认MN分配的安全参数
4. RRC重配置消息（携带辅节点计数值）
5. RRC重配置完成消息
6. SN重配置完成消息
SN安全参数激活
7.随机接入过程（Random Access Procedure）
SN安全参数激活

图 1

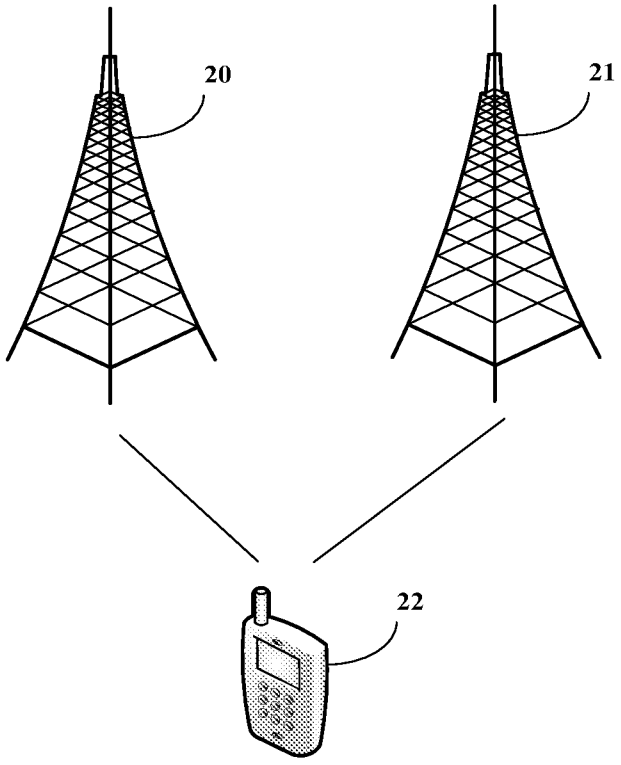

20
21
22

图 2

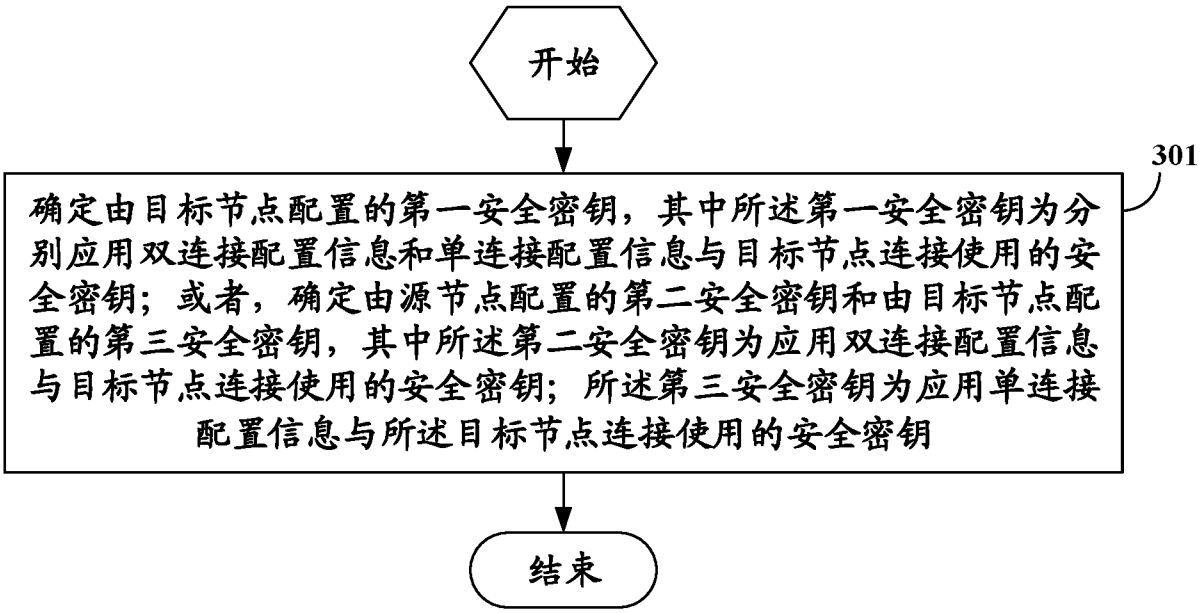

开始
301
确定由目标节点配置的第一安全密钥，其中所述第一安全密钥为分别应用双连接配置信息和单连接配置信息与目标节点连接使用的安全密钥；或者，确定由源节点配置的第二安全密钥和由目标节点配置的第三安全密钥，其中所述第二安全密钥为应用双连接配置信息与目标节点连接使用的安全密钥；所述第三安全密钥为应用单连接配置信息与所述目标节点连接使用的安全密钥
结束

图 3

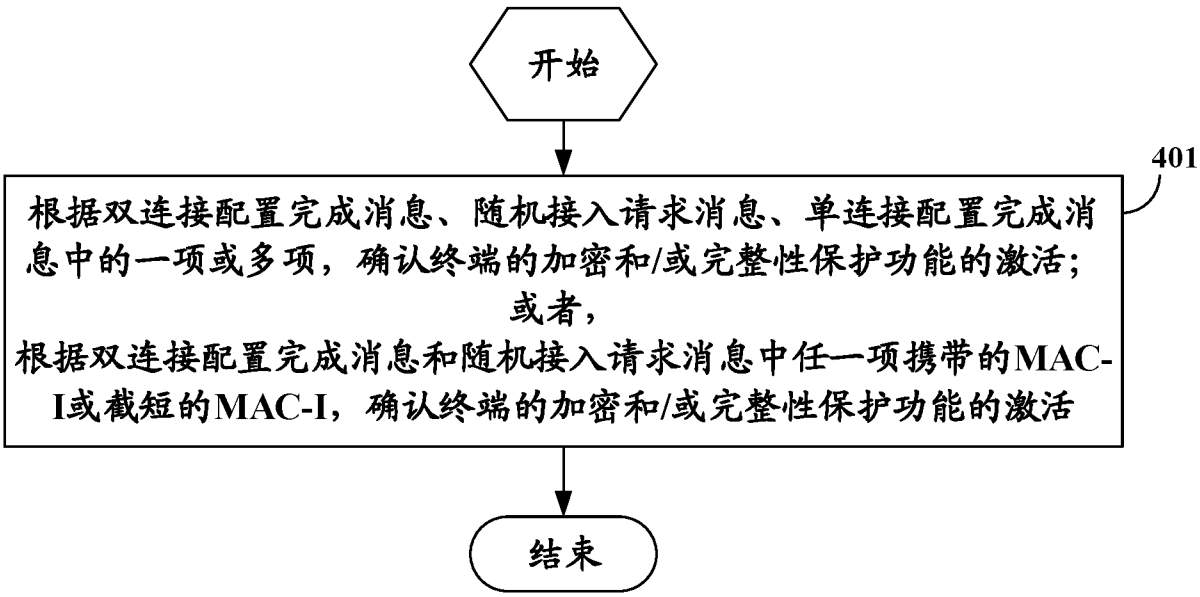

开始
401
根据双连接配置完成消息、随机接入请求消息、单连接配置完成消息中的一项或多项，确认终端的加密和/或完整性保护功能的激活；
或者，
根据双连接配置完成消息和随机接入请求消息中任一项携带的MAC-I或截短的MAC-I，确认终端的加密和/或完整性保护功能的激活
结束

图 4

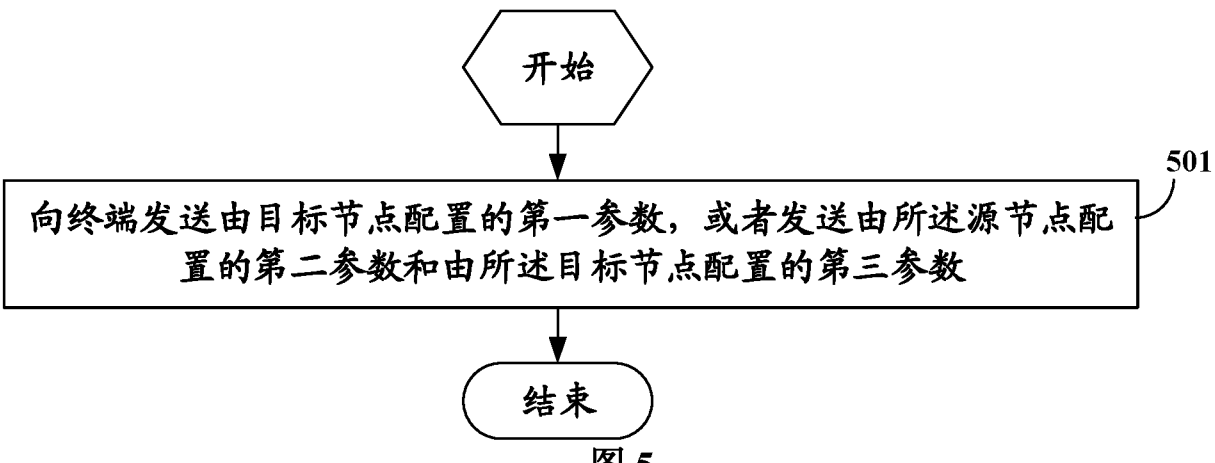

开始
501
向终端发送由目标节点配置的第一参数，或者发送由所述源节点配置的第二参数和由所述目标节点配置的第三参数
结束

图 5

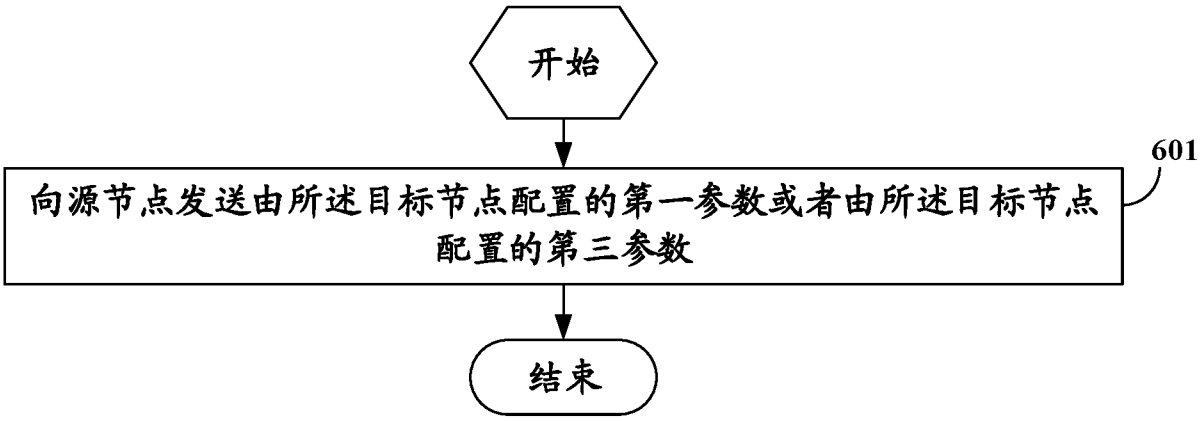

开始
601
向源节点发送由所述目标节点配置的第一参数或者由所述目标节点配置的第三参数
结束

图 6

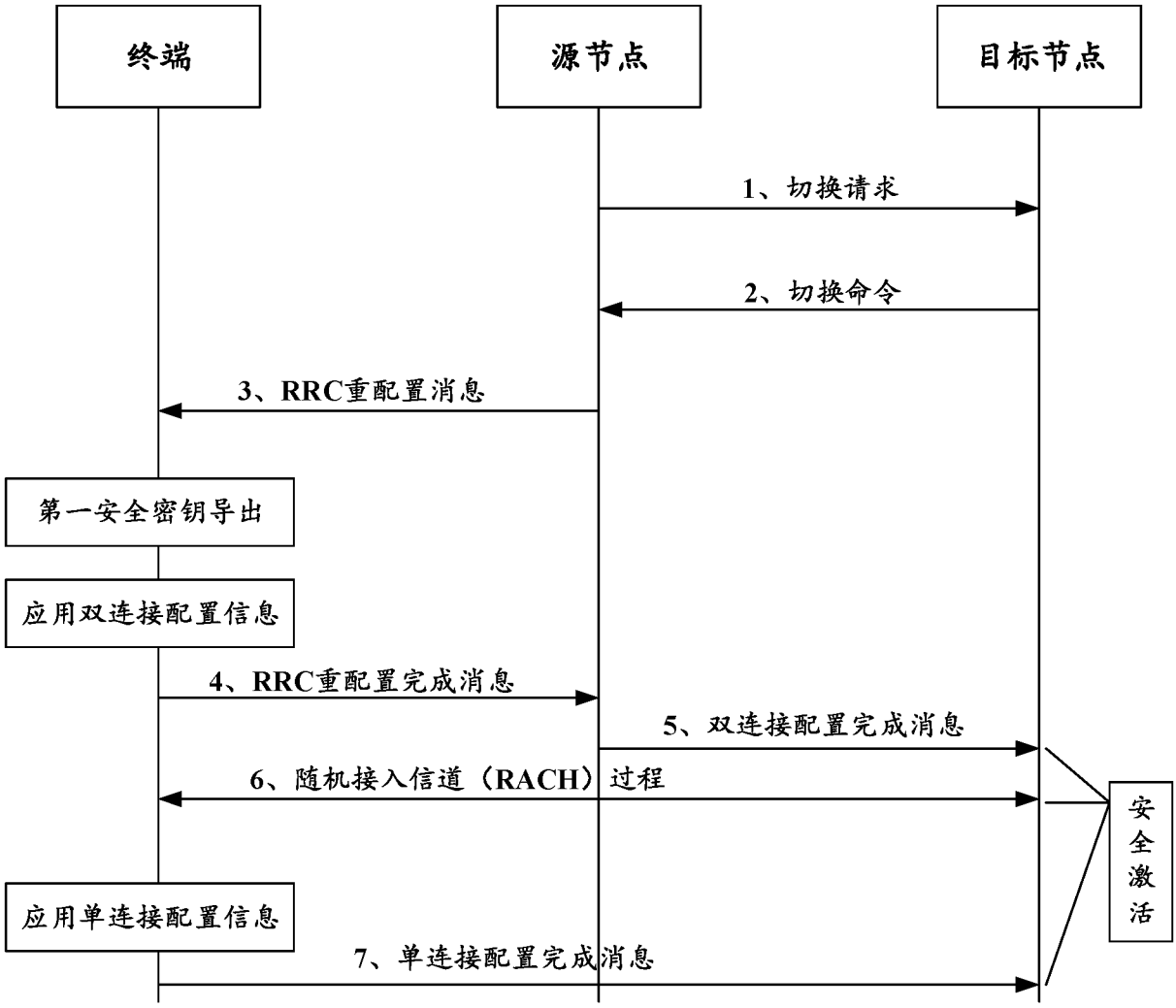

终端
源节点
目标节点
1、切换请求
2、切换命令
3、RRC重配置消息
第一安全密钥导出
应用双连接配置信息
4、RRC重配置完成消息
5、双连接配置完成消息
6、随机接入信道（RACH）过程
安全激活
应用单连接配置信息
7、单连接配置完成消息

图 7

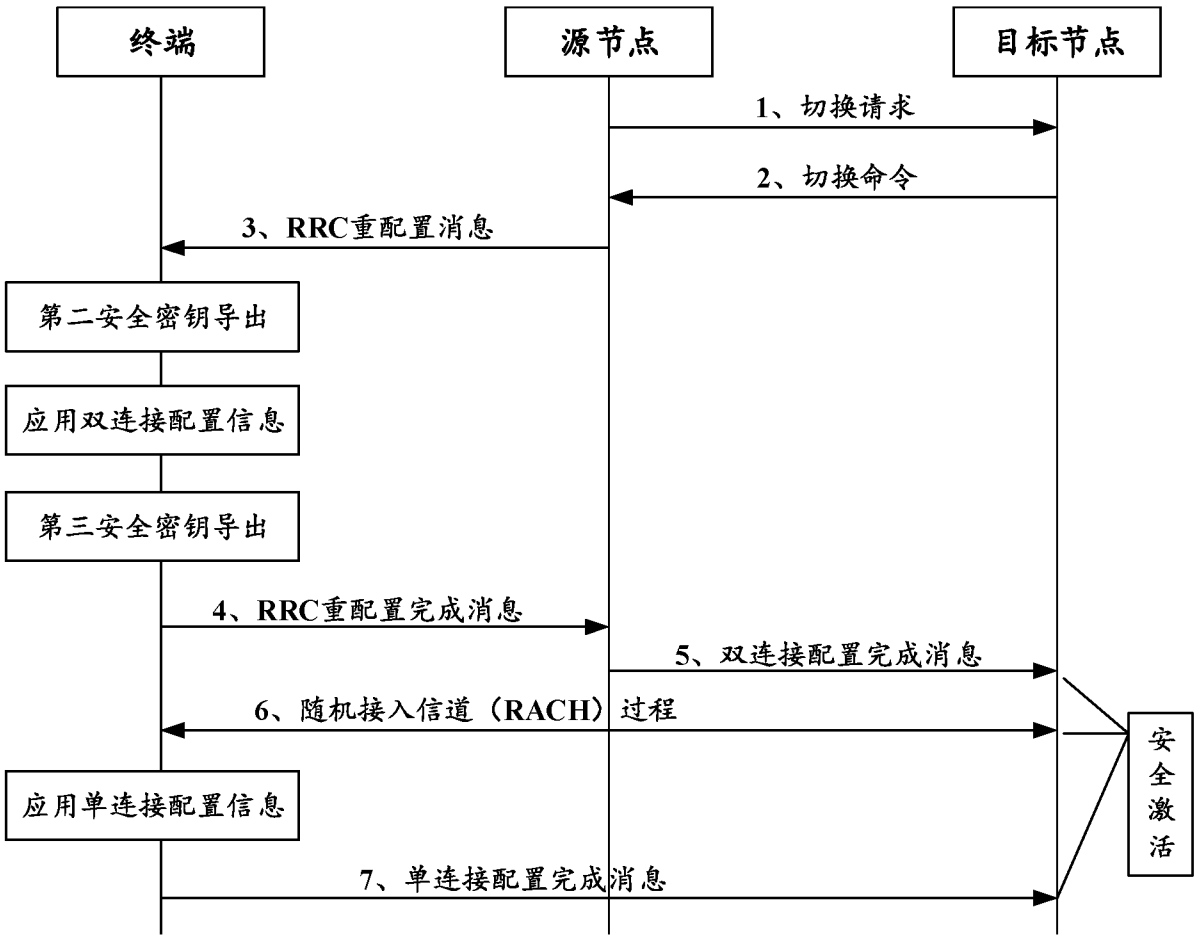

终端
源节点
目标节点
1、切换请求
2、切换命令
3、RRC重配置消息
第二安全密钥导出
应用双连接配置信息
第三安全密钥导出
4、RRC重配置完成消息
5、双连接配置完成消息
6、随机接入信道（RACH）过程
安全激活
应用单连接配置信息
7、单连接配置完成消息

图 8

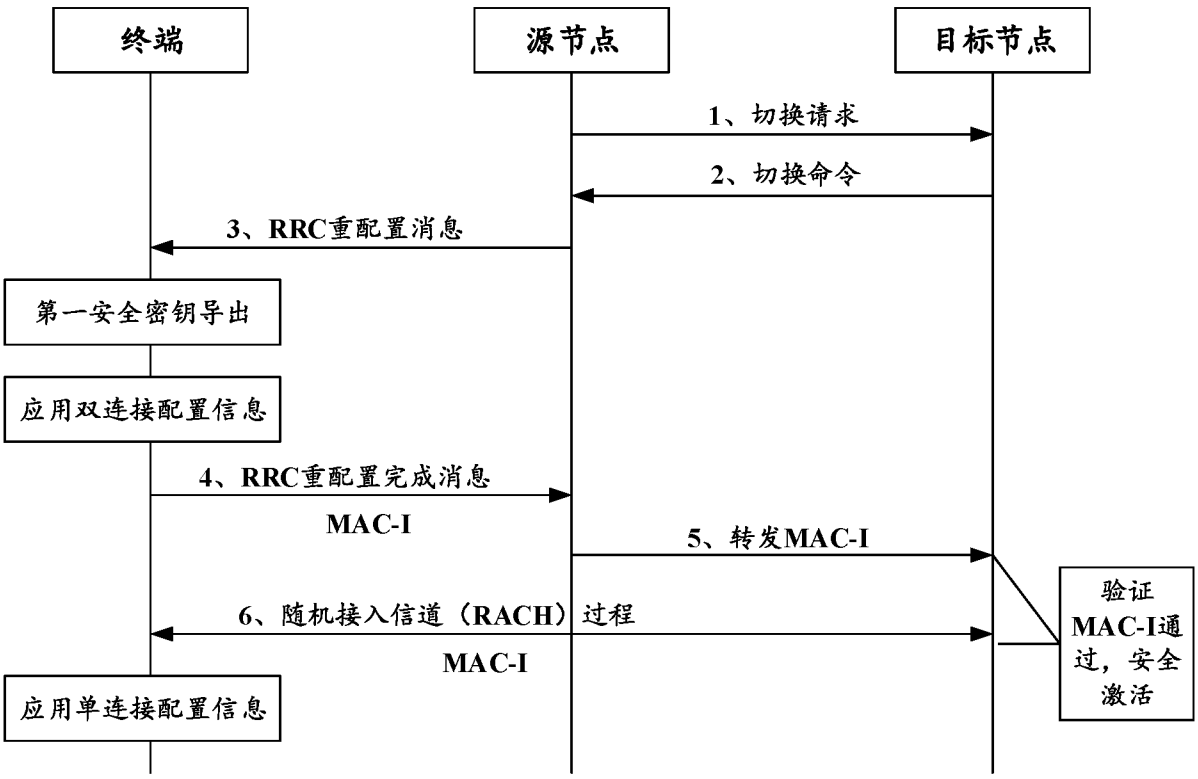

终端
源节点
目标节点
1、切换请求
2、切换命令
3、RRC重配置消息
第一安全密钥导出
应用双连接配置信息
4、RRC重配置完成消息
MAC-I
5、转发MAC-I
6、随机接入信道（RACH）过程
MAC-I
验证MAC-I通过，安全激活
应用单连接配置信息

图 9

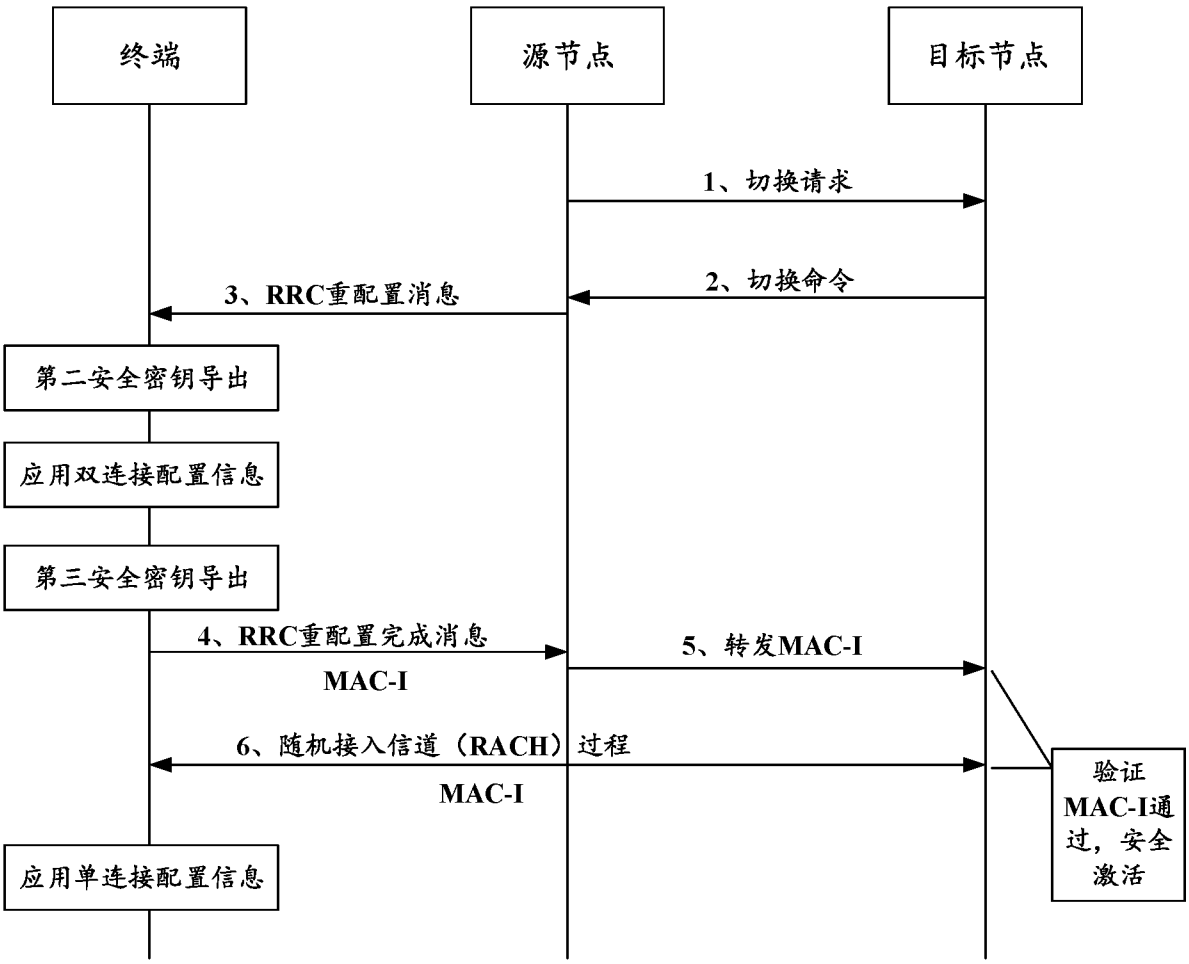

终端
源节点
目标节点
1、切换请求
2、切换命令
3、RRC重配置消息
第二安全密钥导出
应用双连接配置信息
第三安全密钥导出
4、RRC重配置完成消息
MAC-I
5、转发MAC-I
6、随机接入信道（RACH）过程
MAC-I
应用单连接配置信息
验证MAC-I通过，安全激活

图 10

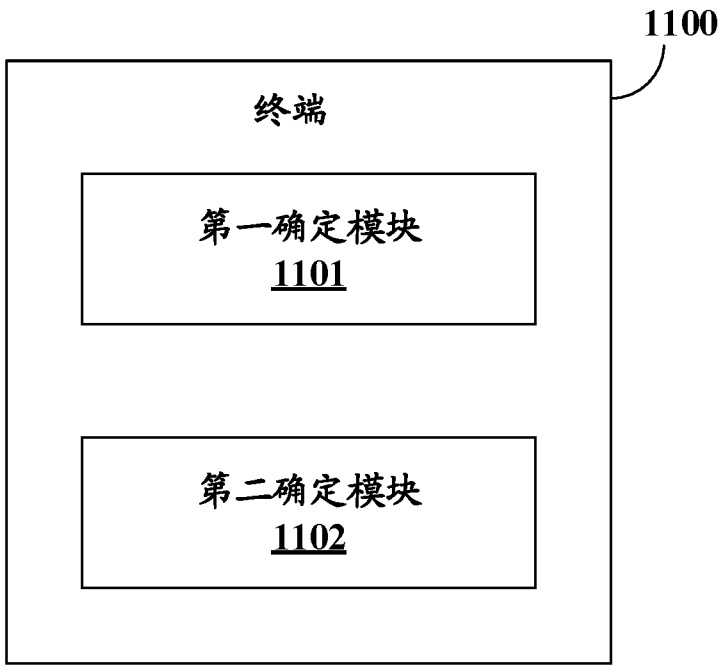

1100
终端
第一确定模块
1101
第二确定模块
1102

图 11

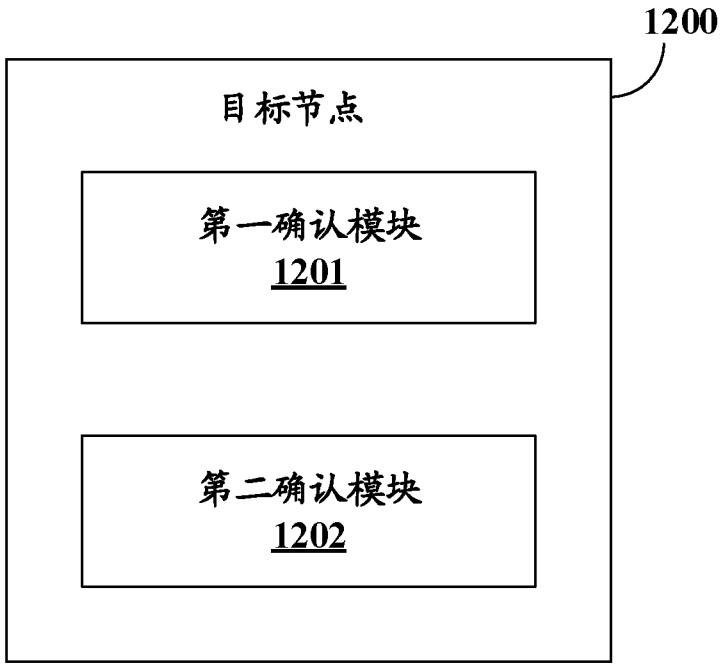

1200
目标节点
第一确认模块
1201
第二确认模块
1202

图 12

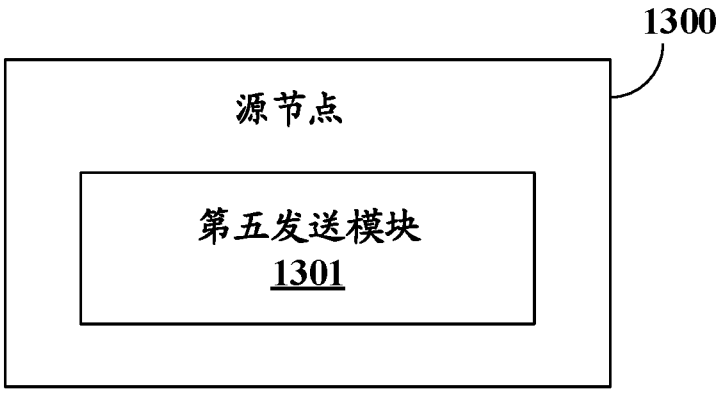

1300
源节点
第五发送模块
1301

图 13


1400
目标节点
第七发送模块
1401

图 14

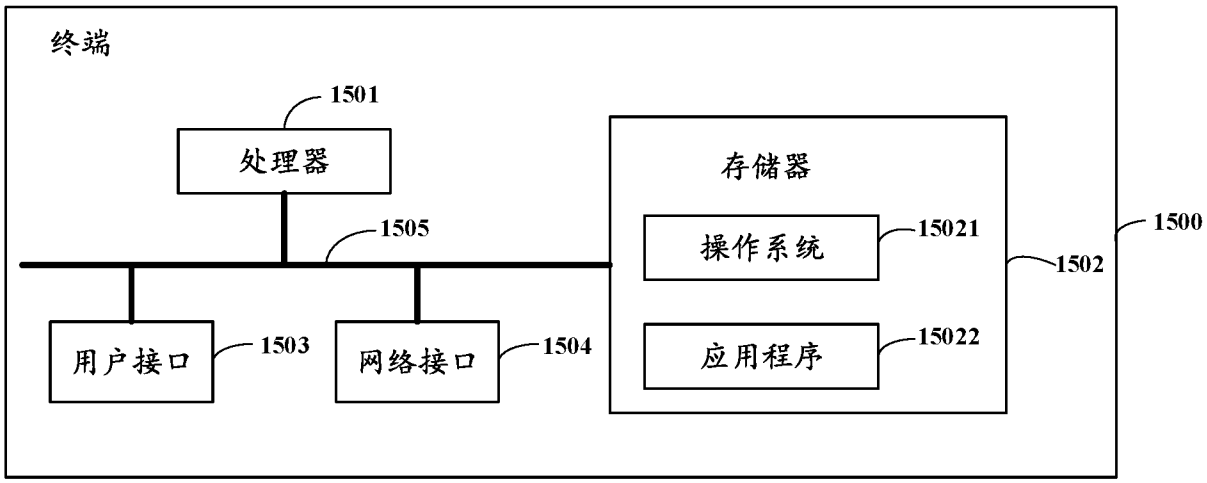

终端
1501
处理器
1505
存储器
操作系统
15021
1500
1502
用户接口
1503
网络接口
1504
应用程序
15022

图 15

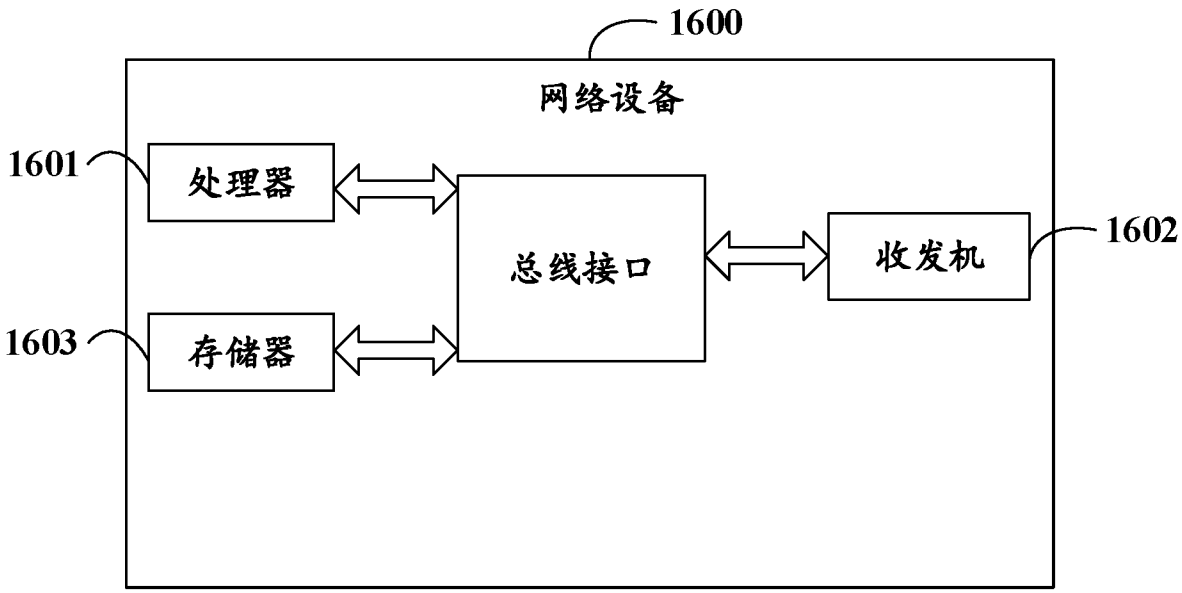

1600
网络设备
1601
处理器
总线接口
收发机
1602
1603
存储器

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/098811

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04(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; H04B; H04Q

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, GOOGLE, 3GPP: 密钥, 秘钥, 目的, 目标, 双, 多, 两, 单, 连接, 配置, 随机接入, 完整性保护, 激活, key+, target, second+, slave, destinat+, double, two, single, connect+, DC, config+, deploy+, integrity, protect+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104918242 A (ZTE CORPORATION) 16 September 2015 (2015-09-16) description, paragraphs [0173]-[0251]	19-21, 26, 28, 29
X	CN 105453672 A (INTERDIGITAL PATENT HOLDINGS, INC.) 30 March 2016 (2016-03-30) description, paragraphs [0376] and [0419]	9, 24, 28, 29
Y	CN 104918242 A (ZTE CORPORATION) 16 September 2015 (2015-09-16) description, paragraphs [0173]-[0251]	22
Y	CN 105453672 A (INTERDIGITAL PATENT HOLDINGS, INC.) 30 March 2016 (2016-03-30) description, paragraphs [0376] and [0419]	22
A	WO 2016042766 A1 (NEC CORPORATION) 24 March 2016 (2016-03-24) entire document	1-29
A	AT&T. "Key requirements for MR-DC and NR-NR DC" *R2-1812408,* 24 August 2018 (2018-08-24), entire document	1-29

☐ 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 October 2019	**30 October 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/098811

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

[1] The same or corresponding technical features between claims (1, 13, 19, 23, 25, 26, and 27) and claims (9 and 24) are: a dual connection configuration and a single connection configuration; and the aforementioned features are common means in the art, which do not constitutes to the prior art. Therefore, the aforementioned two groups of claims are not interrelated by the same or corresponding specific technical features, which define two different inventions, and the inventions are not related to each other by means of a general inventive concept; and therefore, the two groups of claims do not comply with the requirement of unity of invention as defined in PCT Rule 13.1 and PCT Rule 13.2.

[2] The applicant is reminded that, the method implemented by a processor of a network device set forth in claim 28 executing a program relates to the method according to any one of claims 9-12, and the program stored in computer readable storage medium set forth in claim 29 is executed by the processor, and the implemented method also relates to the method according to any one of claims 9-12. Therefore, if the second group of claims (9 and 24) is not searched, the solutions of claims 28 and 29 which relate to claims 9-12 also cannot be searched.

1. ☑ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☑ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/098811

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104918242	A	16 September 2015	WO	2015135292	A1	17 September 2015
CN	105453672	A	30 March 2016	WO	2015021185	A1	12 February 2015
				JP	2016527845	A	08 September 2016
				EP	3031262	A1	15 June 2016
				KR	20160041048	A	15 April 2016
				US	2016183276	A1	23 June 2016
				TW	201521487	A	01 June 2015
				KR	20180035946	A	06 April 2018
				CA	2920501	A1	12 February 2015
				JP	2018174564	A	08 November 2018
				SG	11201600892	A	30 March 2016
WO	2016042766	A1	24 March 2016	JP	2017528993	A	28 September 2017
				US	2017245181	A1	24 August 2017

国际检索报告

国际申请号
PCT/CN2019/098811

A. 主题的分类

H04W 12/04(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; H04B; H04Q

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, GOOGLE, 3GPP: 密钥, 秘钥, 目的, 目标, 双, 多, 两, 单, 连接, 配置, 随机接入, 完整性保护, 激活, key+, target, second+, slave, destinat+, double, two, single, connect+, DC, config+, deploy+, integrity, protect+

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
X	CN 104918242 A (中兴通讯股份有限公司) 2015年 9月 16日 (2015-09-16) 说明书第[0173]-[0251]段	19-21, 26, 28-29
X	CN 105453672 A (交互数字专利控股公司) 2016年 3月 30日 (2016-03-30) 说明书第[0376]、[0419]段	9, 24, 28-29
Y	CN 104918242 A (中兴通讯股份有限公司) 2015年 9月 16日 (2015-09-16) 说明书第[0173]-[0251]段	22
Y	CN 105453672 A (交互数字专利控股公司) 2016年 3月 30日 (2016-03-30) 说明书第[0376]、[0419]段	22
A	WO 2016042766 A1 (NEC CORPORATION) 2016年 3月 24日 (2016-03-24) 全文	1-29
A	AT&T. "Key requirements for MR-DC and NR-NR DC" R2-1812408, 2018年 8月 24日 (2018-08-24), 全文	1-29

☐ 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
2019年 10月 9日	2019年 10月 30日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王怡轩
传真号 (86-10)62019451	电话号码 86-10-53961621

国际检索报告

国际申请号
PCT/CN2019/098811

第III栏　缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明，即：

[1]　权利要求（1,13,19,23,25,26,27）与权利要求（9,24）之间相同或相应的技术特征是：双连接配置、单连接配置，上述特征属于本领域惯用手段，不构成对现有技术的贡献。因此，上述两组权利要求之间没有通过相同或者相应的特定技术特征相互关联，其定义了2项不同的发明，而这些发明没有通过一个总的发明构思相互关联，因此这两组权利要求之间不具备PCT实施细则13.1和13.2规定的发明单一性。

[2]　提醒申请人，权利要求28请求保护的网络设备，其处理器执行程序所实现的方法中涉及权利要求9-12任一项的方法，权利要求29请求保护的计算机可读存储介质，其存储的程序被处理器执行，所实现的方法中也涉及权利要求9-12的方法，因此，如果对第二组权利要求（9,24）不进行检索，将会导致权利要求28-29中涉及权利要求9-12的方案也无法进行检索。

1. ☑ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。

2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是：

对异议的意见

☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。

☑ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/098811

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	104918242	A	2015年 9月 16日	WO	2015135292	A1	2015年 9月 17日
CN	105453672	A	2016年 3月 30日	WO	2015021185	A1	2015年 2月 12日
				JP	2016527845	A	2016年 9月 8日
				EP	3031262	A1	2016年 6月 15日
				KR	20160041048	A	2016年 4月 15日
				US	2016183276	A1	2016年 6月 23日
				TW	201521487	A	2015年 6月 1日
				KR	20180035946	A	2018年 4月 6日
				CA	2920501	A1	2015年 2月 12日
				JP	2018174564	A	2018年 11月 8日
				SG	11201600892	A	2016年 3月 30日
WO	2016042766	A1	2016年 3月 24日	JP	2017528993	A	2017年 9月 28日
				US	2017245181	A1	2017年 8月 24日