

(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
2018 年 11 月 8 日 (08.11.2018)



(10) 国际公布号
WO 2018/201440 A1

(51) 国际专利分类号:
H04W 12/08 (2009.01)

陈璟(CHEN, Jing); 中国广东省深圳市龙岗区坂田
华为总部办公楼, Guangdong 518129 (CN)。

(21) 国际申请号: PCT/CN2017/083190

(22) 国际申请日: 2017 年 5 月 5 日 (05.05.2017)

(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: 胡力(HU, Li); 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: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, 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,

(54) Title: COMMUNICATION METHOD, DEVICE AND SYSTEM

(54) 发明名称: 通信方法、装置以及系统

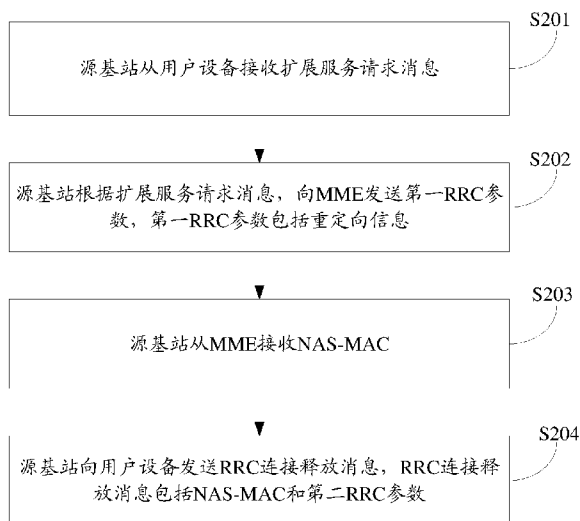


图 2

- S201 A source base station receives from user equipment an extended service request message
S202 The source base station sends, according to the extended service request message, to an MME a first RRC parameter, the first RRC parameter comprising redirection information
S203 The source base station receives an NAS-MAC from the MME
S204 The source base station sends to the user equipment an RRC connection release message, the RRC connection release message comprising the NAS-MAC and a second RRC parameter

(57) Abstract: Disclosed in the embodiments of the present invention are a communication method, device and system. Said method comprises: user equipment sending to a source base station an extended service request message; the user equipment receiving an RRC connection release message sent by the source base station, the RRC connection release message comprising an NAS-MAC and a second RRC parameter, the second RRC parameter being a parameter generated from the NAS-MAC, the second RRC parameter comprising redirection information; the user equipment checking the NAS-MAC according to an NAS integrity key of the user equipment and the second RRC parameter; if the NAS-MAC has successfully passed the check, the user equipment being redirected to a target base station indicated by the redirection information. The embodiments of the present invention can be used to perform identity recognition on the source base station, improving the security for the user equipment performing CSFB.

(57) 摘要: 本发明实施例公开了通信方法、装置以及系统, 所述方法包括: 用户设备向源基站发送扩展服务请求消息; 用户设备接收源基站发送的RRC连接释放消息, RRC连接释放消息包括NAS-MAC和第二RRC参数, 第二RRC参数为NAS-MAC的生成参数, 第二RRC参数包括重定向信息; 用户设备根据用户设备的NAS完整性密钥和第二RRC参数, 校验NAS-MAC; 当NAS-MAC校验成功时, 用户设备重定向到重定向信息所指示的目标基站。采用本发明实施例, 可对源基站进行身份识别, 提高用户设备执行CSFB的安全性。

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,
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))。

通信方法、装置以及系统

技术领域

本申请涉及通信技术领域，尤其涉及通信方法、装置以及系统。

背景技术

在长期演进（Long Term Evolution, LTE）网络中，用户设备（User Equipment, UE）在拨打电话时，网络侧将触发电路域交换回落（Circuit Switched Fallback, CSFB）流程，使用户设备从演进型通用陆地无线接入网（evolved universal terrestrial radio access network, E-UTRAN）断开，并接入 GSM/EDGE 无线接入网（GSM/EDGE radio access network, GERAN），或者 UMTS 陆地无线接入网（universal terrestrial radio access network, UTRAN），使网络通过电路域（Circuit Switched Domain, CS domain）来传输电话业务。

然而，CSFB 流程发生于接入层（Access Stratum, AS）安全激活之前，由网络侧向用户设备发送无线资源控制（Radio Resource Control, RRC）连接释放（RRC Connection Release）消息，该 RRC Connection Release 消息带有指示用户设备连接到某个目标基站的指示信息，由于该 RRC Connection Release 消息没有任何安全保护，存在被篡改、伪造或者监听的风险。例如，存在一种中间人攻击，即一个 4G 伪源基站或者 5G 伪源基站利用强信号使用户设备驻留到该源基站上，再伪造上述 RRC Connection Release 消息，通过 RRC Connection Release 消息中的指示信息使用户设备连接到攻击者控制的另一个 2G 的伪目标基站，由于 2G 的安全保护相对 4G、5G 的安全保护较差，攻击者可以更容易地发起其他攻击，如钓鱼短信等，导致用户设备的安全性较低。

发明内容

本发明实施例公开了通信方法、装置以及系统，可对源基站进行身份识别，提高用户设备执行 CSFB 的安全性。

第一方面，本发明实施例提供了一种通信方法，用户设备向源基站发送扩展服务请求（Extended Service Request）消息；源基站根据扩展服务请求消息，向移动性管理实体（Mobility Management Entity, MME）发送第一 RRC 参数，第一 RRC 参数包括重定向信息；MME 根据该用户设备的非接入层（Non-access stratum, NAS）完整性密钥和生成非接入层-消息验证码（NAS-Message Authentication Code）NAS-MAC 的第二 RRC 参数，获得 NAS-MAC，第二 RRC 参数包含第一 RRC 参数的明文或密文；MME 向源基站发送 NAS-MAC；源基站向用户设备发送 RRC 连接释放消息，RRC 连接释放消息包括 NAS-MAC 和生成 NAS-MAC 的第二 RRC 参数；用户设备根据用户设备的 NAS 完整性密钥和第二 RRC 参数，校验 NAS-MAC；当 NAS-MAC 校验成功时，用户设备重定向到重定向信息所指示的目标基站；当 NAS-MAC 校验失败时，用户设备断开与源基站之间的连接。

在该技术方案中，伪基站在 UE 侧看来是一个基站，但在基站侧看来是一个 UE，则伪基站无法将正确的 RRC 参数发送给 MME，基于此，本发明实施例中 MME 根据源基站发送的第二 RRC 参数生成 NAS-MAC，MME 通过源基站将 NAS-MAC 发送给 UE，UE 校验

NAS-MAC, 当 NAS-MAC 校验成功时, 用户设备识别源基站为真实的基站, 进而重定向到重定向信息所指示的目标基站; 当 NAS-MAC 校验失败时, 用户设备识别源基站为伪基站, 进而断开与源基站之间的连接, 也就是说, 本发明实施例可以使用户设备校验当前收到的 RRC 参数是否为伪造参数或篡改参数, 从而防止伪基站主动触发 CSFB 流程, 使终端连接到 2G 的伪基站上, 可对源基站进行身份识别, 以提高用户设备执行 CSFB 的安全性。

其中, 扩展服务请求消息封装在 RRC 连接设置完成 (RRC ConnectionSetupComplete) 消息中, 扩展服务请求消息可以包含服务类型(Service Type)指示信息, 服务类型指示信息用于指示 UE 请求执行的服务类型为 CSFB, 例如, 主叫的电路交换域回落(mobile originating CS fallback), 被叫的电路交换域回落(mobile terminating CS fallback), 紧急呼叫的电路交换域回落(mobile originating CS fallback emergency call)等。

其中, 第一 RRC 参数可以包括重定向信息, 重定向信息用于指示用户设备重定向的目标基站, 重定向信息可以包括重定向控制信息(redirection control information)或者物理小区标识 (physical cell identity, PCI) 中的至少一种, PCI 用于指示用户设备重定向的目标基站的基站标识。当重定向信息包括重定向控制信息时, UE 可以查找重定向控制信息对应的 PCI, 进而将该 PCI 对应的基站作为目标基站, 并重定向到该目标基站。当重定向信息包括 PCI 时, UE 可以将该 PCI 对应的基站作为目标基站, 并重定向到该目标基站。可选的, 第一 RRC 参数还可以包括释放原因(ReleaseCause, 原因值固定为 CS Fallback High Priority), 或者与 PCI 相关的系统信息(System Information)等。

其中, 第二 RRC 参数可以包括第一 RRC 参数的明文或者密文。当第二 RRC 参数包括第一 RRC 参数的明文时, 第二 RRC 参数与第一 RRC 参数相同。当第二 RRC 参数包括第一 RRC 参数的密文时, MME 接收到源基站发送的第一 RRC 参数之后, 可以根据该用户设备的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第一 RRC 参数的密文, 并将该第一 RRC 参数的密文作为第二 RRC 参数。可选的, 当第二 RRC 参数包括第一 RRC 参数的密文时, MME 接收到源基站发送的第一 RRC 参数之后, 可以根据该用户设备的接入安全管理实体 (Access Security Management Entity, ASME) 和 NAS 计数 (NAS COUNT), 获得衍生的 NAS 加密密钥, MME 可以使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第一 RRC 参数的密文, 并将该第一 RRC 参数的密文作为第二 RRC 参数。

可选的, MME 可以使用用户设备的 NAS 完整性密钥, 对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

可选的, MME 可以使用用户设备的 NAS 完整性密钥, 对第二 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC; MME 将该 NAS-MAC 和 NAS 计数的部分比特位发送给源基站; 源基站向用户设备发送 RRC 连接释放消息, 该连接释放消息包括 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位; 用户设备根据 NAS 计数的部分比特位, 获取 NAS 计数; 用户设备根据该用户设备的 NAS 完整性密钥、第二 RRC 参数以及 NAS 计数, 校验 NAS-MAC。

在该技术方案中, NAS 计数为 NAS 层的新鲜性参数, NAS 计数可实时进行更新, 则 MME 每次生成的 NAS-MAC 各不相同, 可抵抗重放攻击。

可选的, MME 根据用户设备的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 完整性密

钥;MME使用衍生的NAS完整性密钥对第二RRC参数进行完整性保护,生成NAS-MAC;MME将该NAS-MAC和NAS计数的部分比特位发送给源基站;源基站向用户设备发送RRC连接释放消息,RRC连接释放消息包括该NAS-MAC、第二RRC参数和NAS计数的部分比特位;用户设备根据NAS计数的部分比特位,获取NAS计数;用户设备根据用户设备的ASME密钥和NAS计数,获得衍生的NAS完整性密钥;用户设备根据衍生的NAS完整性密钥和第二RRC参数,校验NAS-MAC。

在该技术方案中,NAS计数为NAS层的新鲜性参数,NAS计数可实时进行更新,则每次根据NAS计数得到的衍生的NAS完整性密钥各不相同,基于衍生的NAS完整性密钥生成的NAS-MAC也各不相同,可抵抗重放攻击。

可选的,MME使用用户设备的NAS加密密钥对第一RRC参数进行加密,得到第二RRC参数;MME使用用户设备的NAS完整性密钥,对第二RRC参数进行完整性保护,生成NAS-MAC;MME将该NAS-MAC发送给源基站;源基站向用户设备发送RRC连接释放消息,该连接释放消息包括NAS-MAC和第二RRC参数;用户设备根据该用户设备的NAS完整性密钥和第二RRC参数,校验NAS-MAC;当NAS-MAC校验成功时,用户设备使用该用户设备的NAS加密密钥对第二RRC参数进行解密,获得重定向信息;用户设备重定向到重定向信息所指示的目标基站。

在该技术方案中,MME对源基站发送的第一RRC参数进行加密保护,可防止第一RRC参数被伪造、篡改或者监听等,提升用户设备的安全性。

可选的,MME使用用户设备的NAS加密密钥对第一RRC参数进行加密,得到第二RRC参数;MME使用用户设备的NAS完整性密钥,对第二RRC参数和NAS计数进行完整性保护,生成NAS-MAC;MME将该NAS-MAC和NAS计数的部分比特位发送给源基站;源基站向用户设备发送RRC连接释放消息,该连接释放消息包括NAS-MAC、第二RRC参数和NAS计数的部分比特位;用户设备根据NAS计数的部分比特位,获取NAS计数;用户设备根据该用户设备的NAS完整性密钥、第二RRC参数和NAS计数,校验NAS-MAC;当NAS-MAC校验成功时,用户设备使用该用户设备的NAS加密密钥对第二RRC参数进行解密,获得重定向信息;用户设备重定向到重定向信息所指示的目标基站。

在该技术方案中,NAS计数为NAS层的新鲜性参数,NAS计数可实时进行更新,则MME每次生成的NAS-MAC各不相同,可抵抗重放攻击。另外,MME对源基站发送的第一RRC参数进行加密保护,可防止第一RRC参数被伪造、篡改或者监听等,提升用户设备的安全性。

可选的,MME根据用户设备的ASME密钥和NAS计数,获得衍生的NAS完整性密钥和衍生的NAS加密密钥;MME使用衍生的NAS加密密钥对第一RRC参数进行加密,得到第二RRC参数;MME使用衍生的NAS完整性密钥对第二RRC参数进行完整性保护,生成NAS-MAC;MME将该NAS-MAC和NAS计数的部分比特位发送给源基站;源基站向用户设备发送RRC连接释放消息,RRC连接释放消息包括该NAS-MAC、第二RRC参数和NAS计数的部分比特位;用户设备根据NAS计数的部分比特位,获取NAS计数;用户设备根据用户设备的ASME密钥和NAS计数,获得衍生的NAS完整性密钥和衍生的NAS加密密钥;用户设备根据衍生的NAS完整性密钥和第二RRC参数,校验NAS-MAC;

当 NAS-MAC 校验成功时,用户设备使用衍生的 NAS 加密密钥对第二 RRC 参数进行解密,获得重定向信息;用户设备重定向到重定向信息所指示的目标基站。

在该技术方案中,NAS 计数为 NAS 层的新鲜性参数,NAS 计数可实时进行更新,则每次根据 NAS 计数得到的衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥各不相同,基于衍生的 NAS 加密密钥得到的第二 RRC 参数各不相同,基于衍生的 NAS 完整性密钥生成的 NAS-MAC 也各不相同,可抵抗重放攻击。另外,MME 对源基站发送的第一 RRC 参数进行加密保护,可防止第一 RRC 参数被伪造、篡改或者监听等,提升用户设备的安全性。

第二方面,本发明实施例提供一种计算机存储介质,所述计算机存储介质存储有程序,所述程序执行时包括本发明实施例第一方面提供的通信方法中全部或部分的步骤。

第三方面,本发明实施例提供一种通信装置,该通信装置包括用于执行本发明实施例第一方面公开的通信方法的模块。

第四方面,本发明实施例提供一种基站,其特征在于,包括处理器、存储器以及收发器,存储器中存储一组程序代码,且处理器调用存储器中存储的程序代码,用于执行以下操作:

从用户设备接收扩展服务请求消息;根据扩展服务请求消息,向 MME 发送第一 RRC 参数,第一 RRC 参数包括重定向信息,重定向信息用于指示用户设备重定向的目标基站;从 MME 接收 NAS-MAC;向用户设备发送 RRC 连接释放消息,RRC 连接释放消息包括 NAS-MAC 和生成 NAS-MAC 的第二 RRC 参数,第二 RRC 参数包括第一 RRC 参数的明文或密文。

第五方面,本发明实施例提供一种用户设备,其特征在于,包括处理器、存储器以及收发器,存储器中存储一组程序代码,且处理器调用存储器中存储的程序代码,用于执行以下操作:

向源基站发送扩展服务请求消息;接收源基站发送的 RRC 连接释放消息,RRC 连接释放消息包括 NAS-MAC 和生成 NAS-MAC 的第二 RRC 参数,第二 RRC 参数包括重定向信息;根据用户设备的 NAS 完整性密钥和第二 RRC 参数,校验 NAS-MAC;当 NAS-MAC 校验成功时,重定向到重定向信息所指示的目标基站。

第六方面,本发明实施例提供一种 MME,其特征在于,包括处理器、存储器以及收发器,存储器中存储一组程序代码,且处理器调用存储器中存储的程序代码,用于执行以下操作:

从用户设备的源基站接收第一 RRC 参数,第一 RRC 参数包括重定向信息,重定向信息用于指示用户设备重定向的目标基站;根据用户设备的 NAS 完整性密钥和生成 NAS-MAC 的第二 RRC 参数,获得 NAS-MAC,第二 RRC 参数包含第一 RRC 参数的明文或密文;向源基站发送 NAS-MAC。

第七方面，本发明实施例提供一种通信系统，包括本发明实施例第四方面所公开的基站、第五方面所公开的用户设备以及第六方面所公开的 MME。

附图说明

为了更清楚地说明本发明实施例或背景技术中的技术方案，下面将对本发明实施例或背景技术中所需要使用的附图进行说明。

- 图1是本发明实施例公开的一种通信系统的架构示意图；
- 图2是本发明实施例公开的一种通信方法的流程示意图；
- 图3是本发明另一实施例公开的一种通信方法的流程示意图；
- 图4是本发明另一实施例公开的一种通信方法的流程示意图；
- 图5是本发明另一实施例公开的一种通信方法的流程示意图；
- 图6是本发明另一实施例公开的一种通信方法的流程示意图；
- 图7是本发明另一实施例公开的一种通信方法的流程示意图；
- 图8是本发明另一实施例公开的一种通信方法的流程示意图；
- 图9是本发明另一实施例公开的一种通信方法的流程示意图；
- 图10是本发明另一实施例公开的一种通信方法的流程示意图；
- 图11是本发明实施例公开的一种通信装置的结构示意图；
- 图12是本发明实施例公开的一种基站的结构示意图；
- 图13是本发明另一实施例公开的一种通信装置的结构示意图；
- 图14是本发明实施例公开的一种用户设备的结构示意图；
- 图15是本发明另一实施例公开的一种通信装置的结构示意图；
- 图16是本发明实施例公开的一种移动性管理实体的结构示意图；
- 图17是本发明实施例公开的一种通信系统的结构示意图。

具体实施方式

下面结合本发明实施例中的附图对本发明实施例进行描述。

为了更好的理解本发明实施例公开的一种通信方法及装置，下面首先对本发明实施例适用的网络架构进行描述。请参见图 1，图 1 是本发明实施例公开的一种通信系统的架构示意图。如图 1 所示，该通信系统可以包括用户设备 10、通用分组无线服务技术（General Packet Radio Service, GPRS）业务支撑节点（serving GPRS support node, SGSN）20 以及 MME30。其中，用户设备 10、SGSN20 以及 MME30 之间可以通过通信连接进行数据传输。

其中，用户设备 10 可以通过 E-UTRAN 与 MME30 之间建立通信连接，E-UTRAN 中的基站可以包括演进型基站（Evolutional Node B, eNB）等。用户设备 10 可以通过 UTRAN 或者 GERAN 与 SGSN20 之间建立通信连接，UTRAN 中的基站可以包括基站收发信台（Base Transceiver Station, BTS）或者基站控制器（Base Station Controller, BSC）等，GERAN 中的基站可以包括基站（NodeB, NB）或者无线网络控制器（Radio Network Controller, RNC）

等。

其中，用户设备 10 可以称为移动台、接入终端、用户单元、用户站、移动站、远方站、远程终端、移动设备、终端、无线通信设备、用户代理或用户装置等，其具体可以是 WLAN 中的站点 (Station, ST)、蜂窝电话、无绳电话、会话启动协议 (Session Initiation Protocol, SIP) 电话、无线本地环路 (Wireless Local Loop, WLL) 站、个人数字处理 (Personal Digital Assistant, PDA)、具有无线通信功能的手持设备、计算设备、连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、未来 5G 网络中的移动台以及未来演进的公共陆地移动网络 (Public Land Mobile Network, PLMN) 网络中的终端设备等中的任意一种。

其中，MME30 是 3GPP 协议 LTE 接入网络的关键控制节点，可用于 NAS 信令的加密和完整性保护。

应理解，本发明实施例的技术方案可以应用于各种通信系统，例如：全球移动通信系统 (Global System for Mobile Communication, GSM)、码分多址 (Code Division Multiple Access, CDMA) 系统、宽带码分多址 (Wideband Code Division Multiple Access, WCDMA) 系统、通用分组无线业务 (General Packet Radio Service, 简称 GPRS)、LTE 系统、LTE 频分双工 (Frequency Division Duplex, 简称 FDD) 系统、LTE 时分双工 (Time Division Duplex, 简称 TDD)、通用移动通信系统 (Universal Mobile Telecommunication System, 简称 UMTS) 或全球互联微波接入 (Worldwide Interoperability for Microwave Access, 简称 WiMAX) 通信系统等。

基于图 1 所示的通信系统的架构示意图，请参见图 2，图 2 是本发明实施例提供的一种通信方法，该方法包括但不限于如下步骤：

步骤 S201：源基站从用户设备接收扩展服务请求消息。

其中，上述源基站可以是 LTE 系统中的 eNB。

其中，扩展服务请求消息可以封装在 RRC 连接设置完成消息中。

其中，扩展服务请求消息可以包含服务类型指示信息，服务类型指示信息用于指示 UE 请求执行的服务类型为 CSFB，例如，主叫的电路交换域回落，被叫的电路交换域回落，紧急呼叫的电路交换域回落等。

步骤 S202：源基站根据扩展服务请求消息，向 MME 发送第一 RRC 参数，第一 RRC 参数包括重定向信息。

其中，第一 RRC 参数包括重定向信息，重定向信息用于指示用户设备重定向的目标基站。

其中，重定向信息可以包括重定向控制信息和 PCI 中的至少一种。

其中，重定向控制信息可以用于指示用户设备重定向的目标基站，例如，可以是目标基站的标识。

其中，PCI 可以用于区分不同的小区，例如，可以查找该 PCI 对应的小区，将该小区所属基站作为目标基站，以便重定向到该目标基站。

其中，第一 RRC 参数可以是源基站发送给 UE 的 RRC 连接释放消息所包含的部分或者全部参数，例如，重定向信息、释放原因，以及与 PCI 相关的系统信息等。

其中, PCI 相关的系统信息包括 PCI 对应的小区系统参数, 例如, 服务频点, 邻区频点, 普通或共享的信道信息等。

步骤 S203: 源基站从 MME 接收 NAS-MAC。

在一个示例中, 上述方法还包括: 源基站可以从 MME 接收 NAS 计数的部分比特位。

在一个示例中, 上述方法还包括: 源基站可以从 MME 接收第二 RRC 参数。其中, 第二 RRC 参数为 NAS-MAC 的生成参数, 第二 RRC 参数包括第一 RRC 参数的明文或密文。

步骤 S204: 源基站向用户设备发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数。

在一个示例中, 若源基站从 MME 接收到 NAS 计数的部分比特位, 则源基站向用户设备发送的 RRC 连接释放消息还可以包括 NAS 计数的部分比特位, 例如, NAS 计数的低 4 比特。

在一个示例中, 若源基站从 MME 接收到的第二 RRC 参数, 则源基站发送给用户设备的 RRC 连接释放消息还可以包括第二 RRC 参数。

在图 2 所描述的方法中, 源基站根据用户设备发送的扩展服务请求消息, 向 MME 发送第一 RRC 参数, 从 MME 接收 NAS-MAC, 向用户设备发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数, 第二 RRC 参数为 NAS-MAC 的生成参数, 第二 RRC 参数包括第一 RRC 参数的明文或密文, 由于伪基站无法将正确的第一 RRC 参数告知 MME, 因此无法通过篡改第一 RRC 参数使用户设备下沉至 2G, 提升用户设备执行 CSFB 的安全性。

基于图 1 所示的通信系统的架构示意图, 请参见图 3, 图 3 是本发明实施例提供的一种通信方法, 该方法包括但不限于如下步骤:

步骤 S301: 用户设备向源基站发送扩展服务请求消息。

步骤 S302: 用户设备接收源基站发送的 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数。

其中, 第二 RRC 参数为 NAS-MAC 的生成参数, 第二 RRC 参数包括重定向信息, 重定向信息用于指示用户设备重定向的目标基站。

其中, 第二 RRC 参数可以包括第一 RRC 参数的明文或者密文。

其中, 第一 RRC 参数可以包括重定向信息。

在一个示例中, RRC 连接释放消息还可以包括 NAS 计数的部分比特位。

需要指出的是, 上述第一 RRC 参数, 第二 RRC 参数, NAS 计数以及重定向信息均可以参见图 2 所示实施例中的相关描述, 不再赘述。

步骤 S303: 用户设备根据用户设备的 NAS 完整性密钥和第二 RRC 参数, 校验 NAS-MAC。

在一个示例中, 用户设备可以基于其与 MME 之间的 NAS 完整性算法以及该用户设备的 NAS 完整性密钥, 对第二 RRC 参数进行完整性保护, 生成 NAS-MAC; 用户设备将该用户设备生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较, 当该用户设备生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, NAS-MAC 校验成功;

当该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC不相同, NAS-MAC校验失败。

在另一个示例中, 若RRC连接释放消息包括NAS计数的部分比特位, 则用户设备可以根据NAS计数的部分比特位, 获取NAS计数, 并根据NAS完整性密钥、第二RRC参数以及NAS计数, 校验NAS-MAC。

具体实现中, 用户设备可以根据NAS计数的部分比特位和NAS计数的对应关系, 获取上述NAS计数的部分比特位对应的NAS计数。用户设备可以基于其与MME之间的NAS完整性算法以及该用户设备的NAS完整性密钥, 对第二RRC参数和获取到的NAS计数进行完整性保护, 生成NAS-MAC; 用户设备将该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC进行比较, 当该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC相同时, NAS-MAC校验成功; 当该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC不相同, NAS-MAC校验失败。

在另一个示例中, 若RRC连接释放消息包括NAS计数的部分比特位, 则用户设备可以根据NAS计数的部分比特位, 获取NAS计数, 根据用户设备的ASME密钥(例如, Kasme)和NAS计数, 获得衍生的NAS完整性密钥, 并根据衍生的NAS完整性密钥和第二RRC参数, 校验NAS-MAC。

具体实现中, 用户设备可以通过预设的或者其与MME之间的密钥衍生算法, 对该用户设备的ASME密钥和获取到的NAS计数进行处理, 得到衍生的NAS完整性密钥。用户设备可以基于其与MME之间的NAS完整性算法以及获得的衍生的NAS完整性密钥, 对第二RRC参数进行完整性保护, 生成NAS-MAC。用户设备将该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC进行比较, 当该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC相同时, NAS-MAC校验成功; 当该用户设备生成的NAS-MAC和RRC连接释放消息中的NAS-MAC不相同, NAS-MAC校验失败。

步骤S304: 当NAS-MAC校验成功时, 用户设备重定向到重定向信息所指示的目标基站。

在一个示例中, 当NAS-MAC校验成功, 且第二RRC参数为第一RRC参数的密文时, 用户设备可以使用该用户设备的NAS加密密钥对第二RRC参数进行解密, 获得重定向信息, 并重定向到该重定向信息所指示的目标基站。

在另一个示例中, 当NAS-MAC校验成功, 且第二RRC参数为第一RRC参数的密文时, 用户设备可以根据用户设备的ASME密钥和NAS计数, 获得衍生的NAS加密密钥, 使用衍生的NAS加密密钥对第二RRC参数进行解密, 获得重定向信息, 并重定向到重定向信息所指示的目标基站。

在另一个示例中, 当NAS-MAC校验失败时, 用户设备可以断开与源基站之间的连接。

在图3所描述的方法中, 用户设备接收源基站发送的NAS-MAC和第二RRC参数, 第二RRC参数为NAS-MAC的生成参数, 第二RRC参数包括重定向信息, 用户设备根据用户设备的NAS完整性密钥和第二RRC参数, 校验NAS-MAC, 当NAS-MAC校验成功时, 用户设备重定向到重定向信息所指示的目标基站, 用户设备通过校验NAS-MAC, 对源基站进行身份识别, 可提高用户设备执行CSFB的安全性。

基于图 1 所示的通信系统的架构示意图, 请参见图 4, 图 4 是本发明实施例提供的一种通信方法, 该方法包括但不限于如下步骤:

步骤 S401: MME 从用户设备的源基站接收第一 RRC 参数, 第一 RRC 参数包括重定向信息。

步骤 S402: MME 根据用户设备的 NAS 完整性密钥和第二 RRC 参数, 获得 NAS-MAC, 第二 RRC 参数为 NAS-MAC 的生成参数。

例如, MME 可以基于其与用户设备协商得到的 NAS 完整性算法, 以及该用户设备的 NAS 完整性密钥, 对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

其中, 第二 RRC 参数可以包括第一 RRC 参数的明文或者密文。

其中, 第二 RRC 参数, 第一 RRC 参数, 以及重定向信息等均可以参见图 2 所示实施例中的相关描述, 不再赘述。

在一个示例中, MME 可以使用用户设备的 NAS 完整性密钥, 对该第二 RRC 参数进行完整性保护, 生成 NAS-MAC。其中, 该示例中的第二 RRC 参数可以为第一 RRC 参数的明文。

在另一个示例中, MME 可以使用用户设备的 NAS 完整性密钥, 对第二 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC。其中, 该示例中的第二 RRC 参数可以为第一 RRC 参数的明文。

在另一个示例中, MME 根据用户设备的 NAS 完整性密钥和第二 RRC 参数, 获得 NAS-MAC 之前, 可以使用该用户设备的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数。其中, 该示例中的第二 RRC 参数可以为第一 RRC 参数的密文。

在另一个示例中, MME 可以根据用户设备的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 完整性密钥, 使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。其中, 该示例中的第二 RRC 参数可以为第一 RRC 参数的明文。

在另一个示例中, MME 根据用户设备的 NAS 完整性密钥和第二 RRC 参数, 获得 NAS-MAC 之前, 可以根据该用户设备的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 加密密钥, 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数。其中, 该示例中的第二 RRC 参数可以为第一 RRC 参数的密文。

步骤 S403: MME 向源基站发送 NAS-MAC。

在一个示例中, 若 MME 使用该用户设备的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数, 并根据用户设备的 NAS 完整性密钥和该第二 RRC 参数, 获得 NAS-MAC, 则 MME 可以向源基站发送该 NAS-MAC 和该第二 RRC 参数。

在另一个示例中, 若 MME 根据该用户设备的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 加密密钥, 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数, 并根据用户设备的 NAS 完整性密钥和该第二 RRC 参数, 获得 NAS-MAC, 则 MME 可以向源基站发送该 NAS-MAC 和该第二 RRC 参数。

在另一个示例中, 若 MME 使用用户设备的 NAS 完整性密钥, 对第二 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC, 则 MME 可以向源基站发送该 NAS-MAC 和该 NAS

计数的部分比特位。

在另一个示例中，若 MME 根据用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 完整性密钥，使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，生成 NAS-MAC，则 MME 可以向源基站发送该 NAS-MAC 和该 NAS 计数的部分比特位。

在另一个示例中，若 MME 根据用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥，且 MME 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密，得到第二 RRC 参数，并使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，生成 NAS-MAC，则 MME 可以向源基站发送该 NAS-MAC 和 NAS 计数的部分比特位。

在图 4 所描述的方法中，MME 从用户设备的源基站接收第一 RRC 参数，第一 RRC 参数包括重定向信息，根据用户设备的 NAS 完整性密钥和第二 RRC 参数，获得 NAS-MAC，第二 RRC 参数为 NAS-MAC 的生成参数，并向源基站发送 NAS-MAC，MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，可避免对第一 RRC 参数进行篡改，提高用户设备执行 CSFB 的安全性。

基于图 1 所示的通信系统的架构示意图，请参见图 5，图 5 是本发明实施例提供的一种通信方法，该方法包括但不限于如下步骤：

步骤 S501：UE 向源基站发送扩展服务请求消息。

其中，上述源基站可以是 LTE 系统中的 eNB。

在一个示例中，当 UE 准备连接到网络时，UE 可以向 eNB 发送扩展服务请求消息。

在另一个示例中，当 UE 准备连接到网络时，UE 可以主动发送 RRC 连接请求（RRC Connection Request）消息到 eNB，RRC 连接请求消息可以携带 UE 请求建立 RRC 连接的原因（establishment Cause）。eNB 响应该 RRC 连接请求消息，向 UE 发送 RRC 连接设置（RRC Connection Setup）消息。UE 响应该 RRC 连接设置消息，向 eNB 发送携带有服务类型指示信息的扩展服务请求消息。

其中，服务类型指示信息用于指示 UE 请求执行的服务类型为 CSFB，例如，主叫的电路交换域回落，被叫的电路交换域回落，紧急呼叫的电路交换域回落等。

步骤 S502：源基站根据扩展服务请求消息，向 MME 发送第一 RRC 参数。

其中，第一 RRC 参数包括重定向信息，重定向信息用于指示用户设备重定向的目标基站。

其中，重定向信息可以包括重定向控制信息和 PCI 中的至少一种。

需要说明的是，重定向信息，重定向控制信息，PCI，第一 RRC 参数，第二 RRC 参数等均可以参见图 2-4 任一附图所示实施中的相关描述，不再赘述。

以源基站为 eNB 为例，UE 向 eNB 发送扩展服务请求消息之后，eNB 可以向 MME 发送初始化 UE 消息，初始化 UE 消息携带第一 RRC 参数。该第一 RRC 参数可以是 eNB 发送给 UE 的 RRC 连接释放消息所包含的部分或者全部参数，例如，重定向信息、释放原因，以及与 PCI 相关的系统信息等。其中，初始化 UE 消息可以封装有扩展服务请求消息。

可选的，以源基站为 eNB 为例，eNB 向 MME 发送初始化 UE 消息之前，eNB 可以通

过以下两种方式得知需要在初始化 UE 消息中携带第一 RRC 参数。

第一种方式：若 UE 主动发送 RRC 连接请求消息到 eNB，则 eNB 可以获取 RRC 连接请求消息携带的 UE 请求建立 RRC 连接的原因，当 UE 请求建立 RRC 连接的原因指示 UE 将发起 CSFB 或指示发起的连接类型包含 CSFB 时，eNB 可以向 MME 发送携带有第一 RRC 参数的初始化 UE 消息。

第二种方式：当 eNB 接收到扩展服务请求消息时，eNB 可以向 MME 发送携带有第一 RRC 参数的初始化 UE 消息。可选的，eNB 可以识别扩展服务请求消息携带的服务类型指示信息，当该服务类型指示信息用于指示 UE 请求执行的服务类型为 CSFB 时，eNB 可以向 MME 发送携带有第一 RRC 参数的初始化 UE 消息。

步骤 S503：MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，生成 NAS-MAC。

在一个示例中，MME 接收到初始化 UE 消息之后，可以根据扩展服务请求消息决定进行 CSFB，进而基于其与 UE 协商得到的 NAS 完整性算法，以及该 UE 的 NAS 完整性密钥 Knas-int 对第二 RRC 参数进行完整性保护，生成 NAS-MAC。

其中，第二 RRC 参数可以为第一 RRC 参数的明文。

步骤 S504：MME 向源基站发送 NAS-MAC。

以源基站为 eNB 为例，MME 可以向 eNB 发送 UE 上下文改变请求（UE Context Modification Request）消息，UE 上下文改变请求消息可以包括上述生成得到的 NAS-MAC。

在一个示例中，UE 上下文改变请求消息还可以包括 CSFB 指示（CS Fallback Indication）信息，CSFB 指示信息用于指示源基站对 UE 执行 CSFB。

步骤 S505：源基站向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数。

在一个示例中，若 UE 上下文改变请求消息包括 CSFB 指示信息，则源基站可以响应该 CSFB 指示信息，向 UE 发送 RRC 连接释放消息，该 RRC 连接释放消息可以包括 UE 上下文改变请求消息中的 NAS-MAC 和第二 RRC 参数。

在另一个示例中，源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新，则源基站可以将将在步骤 S502 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较，当在步骤 S502 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同时，源基站可以将更新后的第一 RRC 参数发送给 MME，MME 基于更新后的第一 RRC 参数得到更新后的第二 RRC 参数，并使用 UE 的 NAS 完整性密钥对更新后的第二 RRC 参数进行完整性保护，生成更新后的 NAS-MAC，源基站接收到 MME 发送的更新后的 NAS-MAC 之后，可以向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括更新后的 NAS-MAC 和更新后的第二 RRC 参数。当源基站未对第一 RRC 参数进行更新时，源基站可以确定第一 RRC 参数保持不变，即在步骤 S502 发送给 MME 的第一 RRC 参数和需要发送给 UE 的第二 RRC 参数相同，源基站可以向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括 MME 在步骤 S503 生成的 NAS-MAC 和在步骤 S502 发送给 MME 的第一 RRC 参数。

步骤 S506：UE 使用该 UE 的 NAS 完整性密钥和第二 RRC 参数，校验 NAS-MAC。

具体实现中，UE 可以基于与 MME 协商得到的 NAS 完整性算法，使用自己的 NAS 完

完整性密钥对第二 RRC 参数进行完整性保护,生成 NAS-MAC,进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较,当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时,UE 可以确定 NAS-MAC 校验成功;当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同,UE 可以确定 NAS-MAC 校验失败。

步骤 S507: 当 NAS-MAC 校验成功时,UE 重定向到重定向信息所指示的目标基站。

示例性的,当 NAS-MAC 校验成功时,UE 可以重定向到重定向信息所指示的 2G 基站,以实现 CSFB。

步骤 S508: 当 NAS-MAC 校验失败时,UE 断开与源基站之间的连接。

具体实现中,当 NAS-MAC 校验失败时,UE 可以释放当前连接的源基站,重选一个基站接入。

在图 5 所描述的方法中,MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护,生成 NAS-MAC,由于伪基站无法将正确的第一 RRC 参数通过初始化 UE 消息告知 MME,也不具备 UE 的 NAS 完整性密钥,因此无法通过篡改第二 RRC 参数使 UE 下沉至 2G,解决了一个威胁场景,另外 NAS-MAC 校验失败后,UE 可以断开与伪基站之间的连接,提升 UE 的安全性。

基于图 1 所示的通信系统的架构示意图,请参见图 6,图 6 是本发明另一实施例提供的一种通信方法,该方法包括但不限于如下步骤:

步骤 S601: UE 向源基站发送扩展服务请求消息。

本发明实施例中的步骤 S601 具体可以参见实施例五中的步骤 S501,本发明实施例不再赘述。

步骤 S602: 源基站根据扩展服务请求消息,向 MME 发送第一 RRC 参数。

本发明实施例中的步骤 S602 具体可以参见实施例五中的步骤 S502,本发明实施例不再赘述。

步骤 S603: MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数和 NAS 计数进行完整性保护,生成 NAS-MAC。

在一个示例中,MME 接收到源基站发送的初始化 UE 消息之后,可以获取对应 UE 的上下文中的 NAS 计数,并基于其与 UE 协商得到的 NAS 完整性算法,以及该 UE 的 NAS 完整性密钥,对第二 RRC 参数和获取到的 NAS 计数进行完整性保护,生成 NAS-MAC。

其中,MME 获取到的 NAS 计数可以为下行 NAS 计数。

其中,第二 RRC 参数可以为第一 RRC 参数的明文。

步骤 S604: MME 向源基站发送 NAS-MAC 和 NAS 计数的部分比特位。

以源基站为 eNB 为例,MME 可以向 eNB 发送 UE 上下文改变请求消息,UE 上下文改变请求消息可以包括上述生成得到的 NAS-MAC 和 NAS 计数的部分比特位。示例性的,NAS 计数的部分比特位可以为 NAS 计数的低 3-8 位。

在一个示例中,UE 上下文改变请求消息还可以包括 CSFB 指示信息,CSFB 指示信息用于指示源基站对 UE 执行 CSFB。

步骤 S605: 源基站向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

在一个示例中, 若 UE 上下文改变请求消息包括 CSFB 指示信息, 则源基站可以响应该 CSFB 指示信息, 向 UE 发送 RRC 连接释放消息, 该 RRC 连接释放消息可以包括 UE 上下文改变请求消息中的 NAS-MAC、第二 RRC 参数以及 MME 发送给源基站的 NAS 计数的部分比特位。

在另一个示例中, 源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新, 则源基站可以将步骤 S602 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较, 当在步骤 S602 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同, 源基站可以将更新后的第一 RRC 参数发送给 MME, MME 基于更新后的第一 RRC 参数得到更新后的第二 RRC 参数, 并使用 UE 的 NAS 完整性密钥对更新后的第二 RRC 参数和 NAS 计数进行完整性保护, 生成更新后的 NAS-MAC, 源基站接收到 MME 发送的更新后的 NAS-MAC 之后, 可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括更新后的 NAS-MAC、更新后的第二 RRC 参数和 NAS 计数的部分比特位。当源基站未对第一 RRC 参数进行更新时, 源基站可以确定第一 RRC 参数保持不变, 即在步骤 S602 发送给 MME 的第一 RRC 参数和需要发送给 UE 的第二 RRC 参数相同, 源基站可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 MME 在步骤 S603 生成的 NAS-MAC、在步骤 S602 发送给 MME 的第一 RRC 参数和 NAS 计数的部分比特位。

步骤 S606: UE 根据 NAS 计数的部分比特位获取该 NAS 计数。

具体实现中, UE 可以根据 NAS 计数的部分比特位和 NAS 计数的对应关系, 获取上述 NAS 计数的部分比特位对应的 NAS 计数。其中, 各个 NAS 计数的部分比特位及其对应的 NAS 计数可以是预先存储到 UE 的存储器中的。

步骤 S607: UE 使用该 UE 的 NAS 完整性密钥、第二 RRC 参数和获取到的 NAS 计数, 校验 NAS-MAC。

具体实现中, UE 可以基于其与 MME 协商得到的 NAS 完整性算法, 以及该 UE 的 NAS 完整性密钥, 对第二 RRC 参数和获取到的 NAS 计数进行完整性保护, 生成 NAS-MAC, 进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较, 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, UE 可以确定 NAS-MAC 校验成功; 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同, UE 可以确定 NAS-MAC 校验失败。

步骤 S608: 当 NAS-MAC 校验成功时, UE 重定向到重定向信息所指示的目标基站。

本发明实施例中的步骤 S608 具体可以参见实施例五中的步骤 S507, 本发明实施例不再赘述。

步骤 S609: 当 NAS-MAC 校验失败时, UE 断开与源基站之间的连接。

本发明实施例中的步骤 S609 具体可以参见实施例五中的步骤 S508, 本发明实施例不再赘述。

需要说明的是, 重定向信息, 重定向控制信息, PCI, 第一 RRC 参数, 第二 RRC 参数等均可以参见图 2-4 任一附图所示实施中的相关描述, 不再赘述。

在图 6 所描述的方法中, MME 根据 NAS 计数和 RRC 参数生成 NAS-MAC, 并在下行消息中带上 NAS 计数的部分比特位。由于 NAS 计数为 NAS 层的新鲜参数, 可使每次生成的 NAS-MAC 各不相同, 从而可以抵抗重放攻击。

基于图 1 所示的通信系统的架构示意图, 请参见图 7, 图 7 是本发明另一实施例提供的一种通信方法, 该方法包括但不限于如下步骤:

步骤 S701: UE 向源基站发送扩展服务请求消息。

本发明实施例中的步骤 S701 具体可以参见实施例五中的步骤 S501, 本发明实施例不再赘述。

步骤 S702: 源基站根据扩展服务请求消息, 向 MME 发送第一 RRC 参数。

本发明实施例中的步骤 S702 具体可以参见实施例五中的步骤 S502, 本发明实施例不再赘述。

步骤 S703: MME 根据 UE 的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 完整性密钥。

具体实现中, MME 可以通过预设的或者与 UE 协商得到的密钥衍生算法对 UE 的 ASME 密钥和 NAS 计数进行处理, 得到衍生的 NAS 完整性密钥 Kcsfb。

在一个示例中, MME 可以通过与 UE 协商得到的密钥衍生算法对 UE 的 ASME 密钥、NAS 计数和第一预设常量进行处理, 得到衍生的 NAS 完整性密钥 Kcsfb。示例性的, 第一预设常量可以是一个字符串, 如“CSFB-INT”。

步骤 S704: MME 使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

在一个示例中, MME 接收到初始化 UE 消息之后, 可以根据扩展服务请求消息决定进行 CSFB, 进而基于其与 UE 协商得到的 NAS 完整性算法, 以及获得的衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

其中, 第二 RRC 参数可以为第一 RRC 参数的明文。

步骤 S705: MME 向源基站发送 NAS-MAC 和 NAS 计数的部分比特位。

以源基站为 eNB 为例, MME 可以向 eNB 发送 UE 上下文改变请求消息, UE 上下文改变请求消息可以包括上述生成得到的 NAS-MAC 和 NAS 计数的部分比特位。示例性的, NAS 计数的部分比特位可以为 NAS 计数的低 3-8 位。

在一个示例中, UE 上下文改变请求消息还可以包括第一预设常量。

在另一个示例中, UE 上下文改变请求消息还可以包括 CSFB 指示信息, CSFB 指示信息用于指示源基站对 UE 执行 CSFB。

步骤 S706: 源基站向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

在一个示例中, 若 UE 上下文改变请求消息包括 CSFB 指示信息, 则源基站可以响应该 CSFB 指示信息, 向 UE 发送 RRC 连接释放消息, 该 RRC 连接释放消息可以包括 UE 上下文改变请求消息中的 NAS-MAC、第二 RRC 参数以及 MME 发送给源基站的 NAS 计数的部分比特位。

在另一个示例中, 该 RRC 连接释放消息还可以包括第一预设常量。

可选的,源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新,则源基站可以将步骤 S702 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较,当在步骤 S702 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同,源基站可以将更新后的第一 RRC 参数发送给 MME, MME 根据 UE 的 ASME 密钥和 NAS 计数,获得衍生的 NAS 完整性密钥, MME 基于更新后的第一 RRC 参数得到更新后的第二 RRC 参数,并使用衍生的 NAS 完整性密钥对更新后的第二 RRC 参数进行完整性保护,生成更新后的 NAS-MAC,源基站接收到 MME 发送的更新后的 NAS-MAC 之后,可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括更新后的 NAS-MAC、更新后的第二 RRC 参数和该 NAS 计数的部分比特位。当源基站未对第一 RRC 参数进行更新时,源基站可以确定第一 RRC 参数保持不变,即在步骤 S702 发送给 MME 的第一 RRC 参数和需要发送给 UE 的第二 RRC 参数相同,源基站可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 MME 在步骤 S704 生成的 NAS-MAC 和在步骤 S702 发送给 MME 的第一 RRC 参数。

步骤 S707: UE 根据 NAS 计数的部分比特位获取该 NAS 计数。

本发明实施例中的步骤 S707 具体可以参见实施例六中的步骤 S606,本发明实施例不再赘述。

步骤 S708: UE 使用该 UE 的 ASME 密钥和获取到的 NAS 计数,获得衍生的 NAS 完整性密钥。

具体实现中, UE 可以通过预设的或者与 MME 协商得到的密钥衍生算法对自己的 ASME 密钥和获取到的 NAS 计数进行处理,得到衍生的 NAS 完整性密钥。

在一个示例中, UE 可以通过与 MME 协商得到的密钥衍生算法对自己的 ASME 密钥、NAS 计数和第一预设常量进行处理,得到衍生的 NAS 完整性密钥 Kcsfb。

步骤 S709: UE 使用获得的衍生的 NAS 完整性密钥和第二 RRC 参数,校验 NAS-MAC。

具体实现中, UE 可以基于其与 MME 协商得到的 NAS 完整性算法以及获得的衍生的 NAS 完整性密钥,对第二 RRC 参数进行完整性保护,生成 NAS-MAC,进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较,当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, UE 可以确定 NAS-MAC 校验成功;当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同, UE 可以确定 NAS-MAC 校验失败。

步骤 S710: 当 NAS-MAC 校验成功时, UE 重定向到重定向信息所指示的目标基站。

本发明实施例中的步骤 S710 具体可以参见实施例五中的步骤 S507,本发明实施例不再赘述。

步骤 S711: 当 NAS-MAC 校验失败时, UE 断开与源基站之间的连接。

本发明实施例中的步骤 S711 具体可以参见实施例五中的步骤 S508,本发明实施例不再赘述。

需要说明的是,重定向信息,重定向控制信息, PCI, 第一 RRC 参数,第二 RRC 参数等均可以参见图 2-4 任一附图所示实施中的相关描述,不再赘述。

在图 7 所描述的方法中, MME 根据 UE 的 ASME 密钥和 NAS 计数得到衍生的 NAS 完整性密钥,使用衍生的 NAS 完整性密钥对 RRC 参数进行完整性保护,获得 NAS-MAC。

由于 NAS 计数为 NAS 层的新鲜参数，可使每次得到的衍生的 NAS 完整性密钥各不相同，导致每次生成的 NAS-MAC 也各不相同，从而可以抵抗重放攻击。

基于图 1 所示的通信系统的架构示意图，请参见图 8，图 8 是本发明另一实施例提供的一种通信方法，该方法包括但不限于如下步骤：

步骤 S801：UE 向源基站发送扩展服务请求消息。

本发明实施例中的步骤 S801 具体可以参见实施例五中的步骤 S501，本发明实施例不再赘述。

步骤 S802：源基站根据扩展服务请求消息，向 MME 发送第一 RRC 参数。

本发明实施例中的步骤 S802 具体可以参见实施例五中的步骤 S502，本发明实施例不再赘述。

步骤 S803：MME 使用 UE 的 NAS 加密密钥对第一 RRC 参数进行加密，得到第二 RRC 参数。

在一个示例中，MME 接收到初始化 UE 消息之后，可以根据扩展服务请求消息决定进行 CSFB，进而基于其与 UE 协商得到的 NAS 机密性算法，以及该 UE 的 NAS 加密密钥 Knas-enc，对源基站发送的第一 RRC 参数进行加密，得到第二 RRC 参数。

其中，第二 RRC 参数可以为第一 RRC 参数的密文。

步骤 S804：MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，生成 NAS-MAC。

在一个示例中，MME 可以基于其与 UE 协商得到的 NAS 完整性算法，以及该 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护，生成 NAS-MAC。

在另一个示例中，MME 可以基于其与 UE 协商得到的 NAS 完整性算法，以及该 UE 的 NAS 完整性密钥对第一 RRC 参数进行完整性保护，生成 NAS-MAC。

步骤 S805：MME 向源基站发送 NAS-MAC 和第二 RRC 参数。

步骤 S806：源基站向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数。

可选的，源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新，则源基站可以将将在步骤 S802 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较，当在步骤 S802 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同时，源基站可以将更新后的第一 RRC 参数发送给 MME，MME 使用 UE 的 NAS 加密密钥对更新后的第一 RRC 参数进行加密，得到更新后的第二 RRC 参数，MME 根据 UE 的 NAS 完整性密钥对更新后的第二 RRC 参数进行完整性保护，生成更新后的 NAS-MAC，源基站接收到 MME 发送的更新后的 NAS-MAC 之后，可以向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括更新后的 NAS-MAC 和更新后的第二 RRC 参数。当源基站未对第一 RRC 参数进行更新时，源基站可以确定第一 RRC 参数保持不变，即在步骤 S802 发送给 MME 的第一 RRC 参数所包含的信息和需要发送给 UE 的第二 RRC 参数所包含的信息相同，源基站可以向 UE 发送 RRC 连接释放消息，RRC 连接释放消息包括 MME 在步骤 S804 生成的 NAS-MAC 和第二 RRC 参数。

步骤 S807: UE 使用该 UE 的 NAS 完整性密钥和第二 RRC 参数, 校验 NAS-MAC。

具体实现中, UE 可以基于其与 MME 协商得到的 NAS 完整性算法, 以及该 UE 的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC, 进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较, 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, UE 可以确定 NAS-MAC 校验成功; 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同, UE 可以确定 NAS-MAC 校验失败。

步骤 S808: 当 NAS-MAC 校验成功时, UE 使用该 UE 的 NAS 加密密钥对第二 RRC 参数进行解密, 得到重定向信息。

当 NAS-MAC 校验成功时, UE 可以基于其与 MME 协商得到的 NAS 机密性算法, 以及该 UE 的 NAS 加密密钥, 对第二 RRC 参数进行解密, 得到重定向信息。

步骤 S809: UE 重定向到重定向信息所指示的目标基站。

步骤 S810: 当 NAS-MAC 校验失败时, UE 断开与源基站之间的连接。

需要说明的是, 重定向信息, 重定向控制信息, PCI, 第一 RRC 参数, 第二 RRC 参数等均可以参见图 2-4 任一附图所示实施中的相关描述, 不再赘述。

在图 8 所描述的方法中, MME 对源基站发送的第一 RRC 参数增加了加密保护, 可避免第一 RRC 参数被伪造、篡改或者监听, 提升第一 RRC 参数的安全性。

基于图 1 所示的通信系统的架构示意图, 请参见图 9, 图 9 是本发明另一实施例提供的一种通信方法, 该方法包括但不限于如下步骤:

步骤 S901: UE 向源基站发送扩展服务请求消息。

本发明实施例中的步骤 S901 具体可以参见实施例五中的步骤 S501, 本发明实施例不再赘述。

步骤 S902: 源基站根据扩展服务请求消息, 向 MME 发送第一 RRC 参数。

本发明实施例中的步骤 S902 具体可以参见实施例五中的步骤 S502, 本发明实施例不再赘述。

步骤 S903: MME 使用 UE 的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数。

本发明实施例中的步骤 S903 具体可以参见实施例八中的步骤 S803, 本发明实施例不再赘述。

步骤 S904: MME 使用 UE 的 NAS 完整性密钥对第二 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC。

在一个示例中, MME 可以基于其与 UE 协商得到的 NAS 完整性算法, 以及该 UE 的 NAS 完整性密钥, 对第二 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC。

在另一个示例中, MME 可以基于其与 UE 协商得到的 NAS 完整性算法, 以及该 UE 的 NAS 完整性密钥, 对第一 RRC 参数和 NAS 计数进行完整性保护, 生成 NAS-MAC。

步骤 S905: MME 向源基站发送 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

步骤 S906: 源基站向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

可选的, 源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新, 则源基站可以将步骤 S902 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较, 当在步骤 S902 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同, 源基站可以将更新后的第一 RRC 参数发送给 MME, MME 使用 UE 的 NAS 加密密钥对更新后的第一 RRC 参数进行加密, 得到更新后的第二 RRC 参数, MME 使用 UE 的 NAS 完整性密钥对更新后的第二 RRC 参数和 NAS 计数进行完整性保护, 生成更新后的 NAS-MAC, 源基站接收到 MME 发送的更新后的 NAS-MAC 之后, 可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括更新后的 NAS-MAC、更新后的第二 RRC 参数和该 NAS 计数的部分比特位。当源基站未对第一 RRC 参数进行更新时, 源基站可以确定第一 RRC 参数保持不变, 即在步骤 S902 发送给 MME 的第一 RRC 参数所包含的信息和需要发送给 UE 的第二 RRC 参数所包含的信息相同, 源基站可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 MME 在步骤 S904 生成的 NAS-MAC 和第二 RRC 参数。

步骤 S907: UE 根据 NAS 计数的部分比特位获取该 NAS 计数。

本发明实施例中的步骤 S907 具体可以参见实施例六中的步骤 S606, 本发明实施例不再赘述。

步骤 S908: UE 使用该 UE 的 NAS 完整性密钥、第二 RRC 参数和获取到的 NAS 计数, 校验 NAS-MAC。

具体实现中, UE 可以基于其与 MME 协商得到的 NAS 完整性算法, 以及该 UE 的 NAS 完整性密钥, 对第二 RRC 参数和获取到的 NAS 计数进行完整性保护, 生成 NAS-MAC, 进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较, 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, UE 可以确定 NAS-MAC 校验成功; 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同, UE 可以确定 NAS-MAC 校验失败。

步骤 S909: 当 NAS-MAC 校验成功时, UE 使用该 UE 的 NAS 加密密钥对第二 RRC 参数进行解密, 得到重定向信息。

当 NAS-MAC 校验成功时, UE 可以基于其与 MME 协商得到的 NAS 机密性算法, 以及该 UE 的 NAS 加密密钥, 对第二 RRC 参数进行解密, 得到重定向信息。

步骤 S910: UE 重定向到重定向信息所指示的目标基站。

步骤 S911: 当 NAS-MAC 校验失败时, UE 断开与源基站之间的连接。

需要说明的是, 重定向信息, 重定向控制信息, PCI, 第一 RRC 参数, 第二 RRC 参数等均可以参见图 2-4 任一附图所示实施中的相关描述, 不再赘述。

在图 9 所描述的方法中, MME 对第一 RRC 参数增加了加密保护, 可避免第一 RRC 参数被伪造、篡改或者监听, 提升第一 RRC 参数的安全性, 另外, MME 根据 NAS 计数和第二 RRC 参数生成 NAS-MAC, 由于 NAS 计数为 NAS 层的新鲜参数, 可使每次生成的 NAS-MAC 各不相同, 从而可以抵抗重放攻击。

基于图 1 所示的通信系统的架构示意图, 请参见图 10, 图 10 是本发明另一实施例提供的一种通信方法, 该方法包括但不限于如下步骤:

步骤 S1001: UE 向源基站发送扩展服务请求消息。

本发明实施例中的步骤 S1001 具体可以参见实施例五中的步骤 S501, 本发明实施例不再赘述。

步骤 S1002: 源基站根据扩展服务请求消息, 向 MME 发送第一 RRC 参数。

本发明实施例中的步骤 S1002 具体可以参见实施例五中的步骤 S502, 本发明实施例不再赘述。

步骤 S1003: MME 根据 UE 的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥。

具体实现中, MME 可以通过预设的或其与 UE 协商得到的密钥衍生算法对该 UE 的 ASME 密钥和 NAS 计数进行处理, 得到衍生的 NAS 完整性密钥 Kcsfb-int 和衍生的 NAS 加密密钥 Kcsfb-enc。

在一个示例中, MME 可以通过其与 UE 协商得到的密钥衍生算法对该 UE 的 ASME 密钥、NAS 计数和第二预设常量进行处理, 得到衍生的 NAS 完整性密钥。示例性的, 第二预设常量可以是一个字符串, 如“CSFB-INT”。

在一个示例中, MME 可以通过其与 UE 协商得到的密钥衍生算法对该 UE 的 ASME 密钥、NAS 计数和第三预设常量进行处理, 得到衍生的 NAS 加密密钥。示例性的, 第三预设常量可以是一个字符串, 如“CSFB-ENC”。

步骤 S1004: MME 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数。

在一个示例中, MME 接收到初始化 UE 消息之后, 可以根据扩展服务请求消息决定进行 CSFB, 进而基于与 UE 协商得到的 NAS 机密性算法, 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数。

其中, 第二 RRC 参数可以为第一 RRC 参数的密文。

步骤 S1005: MME 使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

MME 可以基于其与 UE 协商得到的 NAS 完整性算法, 以及衍生的 NAS 完整性密钥, 对第二 RRC 参数进行完整性保护, 生成 NAS-MAC。

步骤 S1006: MME 向源基站发送 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

步骤 S1007: 源基站向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 NAS-MAC、第二 RRC 参数和 NAS 计数的部分比特位。

可选的, 源基站可以根据 UE 上下文改变请求消息对第一 RRC 参数进行更新, 则源基站可以将将在步骤 S1002 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数进行比较, 当在步骤 S1002 发送给 MME 的第一 RRC 参数和更新后的第一 RRC 参数不相同, 源基站可以将更新后的第一 RRC 参数发送给 MME, MME 根据 UE 的 ASME 密钥和 NAS 计数, 获得衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥, MME 使用衍生的 NAS 加密密钥对

更新后的第一 RRC 参数进行加密, 得到更新后的第二 RRC 参数, MME 使用衍生的 NAS 完整性密钥对更新后的第二 RRC 参数进行完整性保护, 生成更新后的 NAS-MAC, 源基站接收到 MME 发送的更新后的 NAS-MAC 之后, 可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括更新后的 NAS-MAC、更新后的第二 RRC 参数和该 NAS 计数的部分比特位。当源基站未对第一 RRC 参数进行更新时, 源基站可以确定第一 RRC 参数保持不变, 即在步骤 S1002 发送给 MME 的第一 RRC 参数所包含的信息和需要发送给 UE 的第二 RRC 参数所包含的信息相同, 源基站可以向 UE 发送 RRC 连接释放消息, RRC 连接释放消息包括 MME 在步骤 S1005 生成的 NAS-MAC 和第二 RRC 参数。

步骤 S1008: UE 根据 NAS 计数的部分比特位获取该 NAS 计数。

本发明实施例中的步骤 S1008 具体可以参见实施例六中的步骤 S606, 本发明实施例不再赘述。

步骤 S1009: UE 使用该 UE 的 ASME 密钥和获取到的 NAS 计数, 获得衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥。

具体实现中, UE 可以通过预设的或与其与 MME 协商得到的密钥衍生算法对该 UE 的 ASME 密钥和获取到的 NAS 计数进行处理, 得到衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥。

在一个示例中, UE 可以通过其与 MME 协商得到的密钥衍生算法对该 UE 的 ASME 密钥、获取到的 NAS 计数和第二预设常量进行处理, 得到衍生的 NAS 完整性密钥。

在一个示例中, UE 可以通过其与 MME 协商得到的密钥衍生算法对该 UE 的 ASME 密钥、获取到的 NAS 计数和第三预设常量进行处理, 得到衍生的 NAS 加密密钥。

步骤 S1010: UE 使用获得的衍生的 NAS 完整性密钥和第二 RRC 参数, 校验 NAS-MAC。

具体实现中, UE 可以基于其与 MME 协商得到的 NAS 完整性算法, 使用获得的衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 生成 NAS-MAC, 进而 UE 可以将 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 进行比较, 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 相同时, UE 可以确定 NAS-MAC 校验成功; 当 UE 生成的 NAS-MAC 和 RRC 连接释放消息中的 NAS-MAC 不相同, UE 可以确定 NAS-MAC 校验失败。

步骤 S1011: 当 NAS-MAC 校验成功时, UE 使用获得的衍生的 NAS 加密密钥对第二 RRC 参数进行解密, 得到重定向信息。

当 NAS-MAC 校验成功时, UE 可以基于其与 MME 协商得到的 NAS 机密性算法, 使用获得的衍生的 NAS 加密密钥对第二 RRC 参数进行解密, 得到重定向信息。

步骤 S1012: UE 重定向到重定向信息所指示的目标基站。

步骤 S1013: 当 NAS-MAC 校验失败时, UE 断开与源基站之间的连接。

在图 10 所描述的方法中, MME 对第一 RRC 参数增加了加密保护, 可避免第一 RRC 参数被伪造、篡改或者监听, 提升第一 RRC 参数的安全性, 另外, MME 根据 UE 的 ASME 密钥和 NAS 计数得到衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥, 使用衍生的 NAS 加密密钥对第一 RRC 参数进行加密, 得到第二 RRC 参数, 使用衍生的 NAS 完整性密钥对第二 RRC 参数进行完整性保护, 获得 NAS-MAC, 由于 NAS 计数为 NAS 层的新鲜参数,

可使每次得到的衍生的 NAS 完整性密钥和衍生的 NAS 加密密钥各不相同，导致每次生成的 NAS-MAC 也各不相同，从而可以抵抗重放攻击。

上述详细阐述了本发明实施例的方法，下面提供了本发明实施例的装置。

请参见图 11，图 11 是本发明实施例提供的一种通信装置的结构示意图，该通信装置可以包括接收模块 1101 以及发送模块 1102，其中，各个模块的详细描述如下。

接收模块 1101，用于从用户设备接收扩展服务请求消息。

发送模块 1102，用于根据所述扩展服务请求消息，向 MME 发送第一 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站。

所述接收模块 1101，还用于从所述 MME 接收 NAS-MAC。

所述发送模块 1102，还用于向所述用户设备发送 RRC 连接释放消息，所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括所述第一 RRC 参数的明文或密文。

可选的，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位，则所述接收模块 1101，还用于所述发送模块 1102 向所述 MME 发送所述第一 RRC 参数之后，从所述 MME 接收所述 NAS 计数的部分比特位。

可选的，所述第二 RRC 参数包括所述第一 RRC 参数的密文，则所述接收模块 1101，还用于从所述 MME 接收所述第二 RRC 参数。

需要说明的是，本发明实施例可具体参见图 2、5~10 所示实施例的相关描述，不再赘述。

在图 11 所描述的通信装置中，接收模块 1101 从用户设备接收扩展服务请求消息，发送模块 1102 根据所述扩展服务请求消息，向 MME 发送第一 RRC 参数，所述第一 RRC 参数包括重定向信息，接收模块 1101 从所述 MME 接收 NAS-MAC，发送模块 1102 向所述用户设备发送 RRC 连接释放消息，所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数，可对源基站进行身份识别，提高用户设备执行 CSFB 的安全性。

请参见图 12，图 12 是本发明实施例提供的一种基站，该基站包括处理器 1201、存储器 1202 以及收发器 1203，所述处理器 1201、存储器 1202 以及收发器 1203 通过总线相互连接。

存储器 1202 包括但不限于是随机存储记忆体 (Random Access Memory, RAM)、只读存储器 (Read-Only Memory, ROM)、可擦除可编程只读存储器 (Erasable Programmable Read Only Memory, EPROM)、或便携式只读存储器 (Compact Disc Read-Only Memory, CD-ROM)，该存储器 1202 用于存储相关指令及数据，例如扩展服务请求消息、用户设备的第一 RRC 参数等。收发器 1203 用于接收和发送数据，例如从用户设备接收扩展服务请求消息，或者向 MME 发送第一 RRC 参数等。

处理器 1201 可以是一个或多个中央处理器 (Central Processing Unit, CPU)，或者一个或多个微控制单元 (Microcontroller Unit, MCU)。在处理器 1201 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。其中，处理器 1201 可结合图 11 所示的通

信装置。

该基站中的处理器 1201 用于读取所述存储器 1202 中存储的程序代码,执行以下操作:

通过收发器 1203 从用户设备接收扩展服务请求消息;

根据扩展服务请求消息,通过收发器 1203 向 MME 发送第一 RRC 参数,所述第一 RRC 参数包括重定向信息,所述重定向信息用于指示所述用户设备重定向的目标基站;

通过收发器 1203 从所述 MME 接收 NAS-MAC;

通过收发器 1203 向所述用户设备发送 RRC 连接释放消息,所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数,所述第二 RRC 参数为所述 NAS-MAC 的生成参数,所述第二 RRC 参数包括所述第一 RRC 参数的明文或密文。

可选的,所述 RRC 连接释放消息还包括 NAS 计数的部分比特位,处理器 1201 通过收发器 1203 向 MME 发送所述第一 RRC 参数之后,还可以执行以下操作:

通过收发器 1203 从所述 MME 接收所述 NAS 计数的部分比特位。

可选的,所述第二 RRC 参数包括所述第一 RRC 参数的密文,处理器 1201 通过收发器 1203 还可以执行以下操作:从所述 MME 接收所述第二 RRC 参数。

需要说明的是,本发明实施例可具体参见图 2、5~10 所示实施例的相关描述,不再赘述。

在图 12 所描述的基站中,处理器 1201 通过收发器 1203 从用户设备接收扩展服务请求消息,根据扩展服务请求消息,向 MME 发送第一 RRC 参数,第一 RRC 参数包括重定向信息,从 MME 接收 NAS-MAC,向用户设备发送 RRC 连接释放消息,RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数,可对该基站进行身份识别,提高用户设备执行 CSFB 的安全性。

请参见图 13,图 13 是本发明实施例提供的一种通信装置的结构示意图,该通信装置可以包括发送模块 1301、接收模块 1302、校验模块 1303 以及定向模块 1304,其中,各个模块的详细描述如下。

发送模块 1301,用于向源基站发送扩展服务请求消息。

接收模块 1302,用于接收所述源基站发送的 RRC 连接释放消息,所述 RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数,所述第二 RRC 参数为所述 NAS-MAC 的生成参数,所述第二 RRC 参数包括重定向信息。

校验模块 1303,用于根据所述通信装置的 NAS 完整性密钥和所述第二 RRC 参数,校验所述 NAS-MAC。

定向模块 1304,用于当所述 NAS-MAC 校验成功时,重定向到所述重定向信息所指示的目标基站。

可选的,所述 RRC 连接释放消息还包括 NAS 计数的部分比特位。

可选的,所述校验模块 1303,具体用于:

根据所述 NAS 计数的部分比特位,获取所述 NAS 计数;

根据所述 NAS 完整性密钥、所述第二 RRC 参数以及所述 NAS 计数,校验所述 NAS-MAC。

可选的,当所述第二RRC参数为密文时,所述定向模块1304,具体用于:

使用所述通信装置的NAS加密密钥对所述第二RRC参数进行解密,获得所述重定向信息;

重定向到所述重定向信息所指示的目标基站。

可选的,所述校验模块1303,具体用于:

根据所述NAS计数的部分比特位,获取所述NAS计数;

根据所述通信装置的ASME密钥和所述NAS计数,获得衍生的NAS完整性密钥;

根据所述衍生的NAS完整性密钥和所述第二RRC参数,校验所述NAS-MAC。

可选的,当所述第二RRC参数为密文时,所述定向模块1304,具体用于:

根据所述通信装置的ASME密钥和所述NAS计数,获得衍生的NAS加密密钥;

使用所述衍生的NAS加密密钥对所述第二RRC参数进行解密,获得所述重定向信息;

重定向到所述重定向信息所指示的目标基站。

可选的,本发明实施例中的通信装置还可以包括:

断开模块1305,用于当所述NAS-MAC校验失败时,断开与所述源基站之间的连接。

需要说明的是,本发明实施例可具体参见图3、5~10所示实施例的相关描述,不再赘述。

在图13所描述的通信装置中,发送模块1301向源基站发送扩展服务请求消息,接收模块1302接收源基站发送的RRC连接释放消息,RRC连接释放消息包括NAS-MAC和第二RRC参数,第二RRC参数包括重定向信息,校验模块1303根据通信装置的NAS完整性密钥和第二RRC参数,校验NAS-MAC,当NAS-MAC校验成功时,定向模块1304重定向到重定向信息所指示的目标基站,可对源基站进行身份识别,提高用户设备执行CSFB的安全性。

请参见图14,图14是本发明实施例提供的一种用户设备,该用户设备包括处理器1401、存储器1402以及收发器1403,所述处理器1401、存储器1402以及收发器1403通过总线相互连接。

存储器1402包括但不限于是RAM、ROM、EPROM、或CD-ROM,该存储器1402用于存储相关指令及数据,例如NAS-MAC、第二RRC参数等。收发器1403用于接收和发送数据,例如向源基站发送扩展服务请求消息,或者接收源基站发送的RRC连接释放消息等。

处理器1401可以是一个或多个CPU,或者一个或多个MCU。在处理器1401是一个CPU的情况下,该CPU可以是单核CPU,也可以是多核CPU。其中,处理器1401可结合图13所示的通信装置。

该用户设备中的处理器1401用于读取所述存储器1402中存储的程序代码,执行以下操作:

通过收发器1403向源基站发送扩展服务请求消息。

通过收发器1403接收所述源基站发送的RRC连接释放消息,所述RRC连接释放消息包括NAS-MAC和第二RRC参数,所述第二RRC参数为所述NAS-MAC的生成参数,所

述第二 RRC 参数包括重定向信息。

根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC。

当所述 NAS-MAC 校验成功时，重定向到所述重定向信息所指示的目标基站。

可选的，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位。

可选的，处理器 1401 根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC，具体可以为：

根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

根据所述 NAS 完整性密钥、所述第二 RRC 参数以及所述 NAS 计数，校验所述 NAS-MAC。

可选的，当所述第二 RRC 参数为密文时，处理器 1401 重定向到所述重定向信息所指示的目标基站，具体可以为：

使用所述用户设备的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

重定向到所述重定向信息所指示的目标基站。

可选的，处理器 1401 根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC，具体可以为：

根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

根据所述用户设备的 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 完整性密钥；

根据所述衍生的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC。

可选的，当所述第二 RRC 参数为密文时，处理器 1401 重定向到所述重定向信息所指示的目标基站，具体可以为：

根据所述用户设备的 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 加密密钥；

使用所述衍生的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

重定向到所述重定向信息所指示的目标基站。

可选的，处理器 1401 还可以执行以下操作：

当所述 NAS-MAC 校验失败时，断开与所述源基站之间的连接。

需要说明的是，本发明实施例可具体参见图 3、5~10 所示实施例的相关描述，不再赘述。

在图 14 所描述的用户设备中，处理器 1401 通过收发器 1403 向源基站发送扩展服务请求消息，接收源基站发送的 RRC 连接释放消息，RRC 连接释放消息包括 NAS-MAC 和第二 RRC 参数，第二 RRC 参数包括重定向信息，根据用户设备的 NAS 完整性密钥和第二 RRC 参数，校验 NAS-MAC，当 NAS-MAC 校验成功时，重定向到重定向信息所指示的目标基站，可对源基站进行身份识别，提高用户设备执行 CSFB 的安全性。

请参见图 15，图 15 是本发明另一实施例提供的一种通信装置的结构示意图，该通信装置可以包括接收模块 1501、获取模块 1502 以及发送模块 1503，其中，各个模块的详细描述如下。

接收模块 1501，用于从用户设备的源基站接收第一 RRC 参数，所述第一 RRC 参数包

括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站。

获取模块 1502，用于根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得 NAS-MAC，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包含所述第一 RRC 参数的明文或密文。

发送模块 1503，用于向所述源基站发送所述 NAS-MAC。

可选的，所述获取模块 1502，具体用于：

使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC；或者，

使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数和 NAS 计数进行完整性保护，生成所述 NAS-MAC。

可选的，所述获取模块 1502，还用于根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，使用所述用户设备的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

可选的，所述获取模块 1502，具体用于：

根据所述用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 完整性密钥；

使用所述衍生的 NAS 完整性密钥对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC。

可选的，所述获取模块 1502，还用于根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，根据所述用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 加密密钥；使用所述衍生的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

可选的，所述发送模块 1503，还用于向所述源基站发送所述第二 RRC 参数。

可选的，所述发送模块 1503，还用于向所述源基站发送所述 NAS 计数的部分比特位。

可选的，所述重定向信息包括重定向控制信息或者物理小区标识 PCI 中的至少一种。

需要说明的是，本发明实施例可具体参见图 4~10 所示实施例的相关描述，不再赘述。

在图 15 所描述的通信装置中，接收模块 1501 从用户设备的源基站接收第一 RRC 参数，第一 RRC 参数包括重定向信息，获取模块 1502 根据用户设备的 NAS 完整性密钥和第二 RRC 参数，获得 NAS-MAC，发送模块 1503 向源基站发送 NAS-MAC，可对源基站进行身份识别，提高用户设备执行 CSFB 的安全性。

请参见图 16，图 16 是本发明实施例提供的一种移动性管理实体，该移动性管理实体包括处理器 1601、存储器 1602 以及收发器 1603，所述处理器 1601、存储器 1602 以及收发器 1603 通过总线相互连接。

存储器 1602 包括但不限于是 RAM、ROM、EPROM、或 CD-ROM，该存储器 1602 用于存储相关指令及数据，例如用户设备的第一 RRC 参数，NAS-MAC 等。收发器 1603 用于接收和发送数据，例如从用户设备的源基站接收第一 RRC 参数，或者向源基站发送 NAS-MAC 等。

处理器 1601 可以是一个或多个 CPU，或者一个或多个 MCU。在处理器 1601 是一个

CPU 的情况下,该 CPU 可以是单核 CPU,也可以是多核 CPU。其中,处理器 1601 可结合图 15 所示的通信装置。

该 MME 中的处理器 1601 用于读取所述存储器 1602 中存储的程序代码,执行以下操作:

通过收发器 1603 从用户设备的源基站接收第一 RRC 参数,所述第一 RRC 参数包括重定向信息,所述重定向信息用于指示所述用户设备重定向的目标基站;

根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数,获得 NAS-MAC,所述第二 RRC 参数为所述 NAS-MAC 的生成参数,所述第二 RRC 参数包含所述第一 RRC 参数的明文或密文;

通过收发器 1603 向所述源基站发送所述 NAS-MAC。

可选的,处理器 1601 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数,获得 NAS-MAC,具体可以为:

使用所述用户设备的 NAS 完整性密钥,对所述第二 RRC 参数进行完整性保护,生成所述 NAS-MAC;或者,

使用所述用户设备的 NAS 完整性密钥,对所述第二 RRC 参数和 NAS 计数进行完整性保护,生成所述 NAS-MAC。

可选的,处理器 1601 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数,获得所述 NAS-MAC 之前,还可以执行以下操作:

使用所述用户设备的 NAS 加密密钥对所述第一 RRC 参数进行加密,得到所述第二 RRC 参数。

可选的,处理器 1601 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数,获得 NAS-MAC,具体可以为:

根据所述用户设备的 ASME 密钥和 NAS 计数,获得衍生的 NAS 完整性密钥;

使用所述衍生的 NAS 完整性密钥对所述第二 RRC 参数进行完整性保护,生成所述 NAS-MAC。

可选的,处理器 1601 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数,获得所述 NAS-MAC 之前,还可以执行以下操作:

根据所述用户设备的 ASME 密钥和 NAS 计数,获得衍生的 NAS 加密密钥;

使用所述衍生的 NAS 加密密钥对所述第一 RRC 参数进行加密,得到所述第二 RRC 参数。

可选的,处理器 1601 还可以执行以下操作:

通过收发器 1603 向所述源基站发送所述第二 RRC 参数。

可选的,处理器 1601 还可以执行以下操作:

通过收发器 1603 向所述源基站发送所述 NAS 计数的部分比特位。

可选的,所述重定向信息包括重定向控制信息或者物理小区标识 PCI 中的至少一种。

需要说明的是,本发明实施例可具体参见图 4~10 所示实施例的相关描述,不再赘述。

在图 16 所描述的基站中,处理器 1601 从用户设备的源基站接收第一 RRC 参数,第一 RRC 参数包括重定向信息,根据用户设备的 NAS 完整性密钥和第二 RRC 参数,获得

NAS-MAC, 向源基站发送 NAS-MAC, 可对该基站进行身份识别, 提高用户设备执行 CSFB 的安全性。

请参见图 17, 图 17 是本发明实施例提供的一种通信系统, 该通信系统包括图 12 所示的基站 1701、图 14 所示的用户设备 1702 以及图 16 所示的移动性管理实体 1703, 具体可以参见图 12、14 以及 16 的描述, 本发明实施例不再赘述。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程, 该流程可以由计算机程序来指令相关的硬件完成, 该程序可存储于计算机可读取存储介质中, 该程序在执行时, 可包括如上述各方法实施例的流程。而前述的存储介质包括: ROM 或随机存储记忆体 RAM、磁碟或者光盘等各种可存储程序代码的介质。

权利要求书

1、一种通信方法，其特征在于，所述方法包括：

源基站从用户设备接收扩展服务请求消息；

所述源基站根据所述扩展服务请求消息，向移动性管理实体 MME 发送第一无线资源控制 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站；

所述源基站从所述 MME 接收非接入层-消息验证码 NAS-MAC；

所述源基站向所述用户设备发送 RRC 连接释放消息，所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括所述第一 RRC 参数的明文或密文。

2、如权利要求 1 所述的方法，其特征在于，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位，所述源基站向 MME 发送所述第一 RRC 参数之后，还包括：

所述源基站从所述 MME 接收所述 NAS 计数的部分比特位。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述第二 RRC 参数包括所述第一 RRC 参数的密文，所述方法还包括：

所述源基站从所述 MME 接收所述第二 RRC 参数。

4、一种通信方法，其特征在于，所述方法包括：

用户设备向源基站发送扩展服务请求消息；

所述用户设备接收所述源基站发送的无线资源控制 RRC 连接释放消息，所述 RRC 连接释放消息包括非接入层-消息验证码 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括重定向信息；

所述用户设备根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC；

当所述 NAS-MAC 校验成功时，所述用户设备重定向到所述重定向信息所指示的目标基站。

5、如权利要求 4 所述的方法，其特征在于，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位。

6、如权利要求 5 所述的方法，其特征在于，所述用户设备根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC，包括：

所述用户设备根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

所述用户设备根据所述 NAS 完整性密钥、所述第二 RRC 参数以及所述 NAS 计数，校验所述 NAS-MAC。

7、如权利要求 4 或 6 所述的方法，其特征在于，当所述第二 RRC 参数为密文时，所述用户设备重定向到所述重定向信息所指示的目标基站，包括：

所述用户设备使用所述用户设备的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

所述用户设备重定向到所述重定向信息所指示的目标基站。

8、如权利要求 5 所述的方法，其特征在于，所述用户设备根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC，包括：

所述用户设备根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

所述用户设备根据所述用户设备的接入安全管理实体 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 完整性密钥；

所述用户设备根据所述衍生的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC。

9、如权利要求 8 所述的方法，其特征在于，当所述第二 RRC 参数为密文时，所述用户设备重定向到所述重定向信息所指示的目标基站，包括：

所述用户设备根据所述用户设备的 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 加密密钥；

所述用户设备使用所述衍生的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

所述用户设备重定向到所述重定向信息所指示的目标基站。

10、如权利要求 4~9 任一项所述的方法，其特征在于，所述方法还包括：

当所述 NAS-MAC 校验失败时，所述用户设备断开与所述源基站之间的连接。

11、一种通信方法，其特征在于，所述方法包括：

移动性管理实体 MME 从用户设备的源基站接收第一无线资源控制 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站；

所述 MME 根据所述用户设备的非接入层 NAS 完整性密钥和第二 RRC 参数，获得非接入层-消息验证码 NAS-MAC，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包含所述第一 RRC 参数的明文或密文；

所述 MME 向所述源基站发送所述 NAS-MAC。

12、如权利要求 11 所述的方法，其特征在于，所述 MME 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC，包括：

所述 MME 使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC；或者，

所述 MME 使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数和 NAS 计数

进行完整性保护，生成所述 NAS-MAC。

13、如权利要求 12 所述的方法，其特征在于，所述 MME 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，所述方法还包括：

所述 MME 使用所述用户设备的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

14、如权利要求 11 所述的方法，其特征在于，所述 MME 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC，包括：

所述 MME 根据所述用户设备的接入安全管理实体 ASME 密钥和 NAS 计数，获得衍生的 NAS 完整性密钥；

所述 MME 使用所述衍生的 NAS 完整性密钥对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC。

15、如权利要求 14 所述的方法，其特征在于，所述 MME 根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，所述方法还包括：

所述 MME 根据所述用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 加密密钥；

所述 MME 使用所述衍生的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

16、如权利要求 13 或 15 所述的方法，其特征在于，所述方法还包括：

所述 MME 向所述源基站发送所述第二 RRC 参数。

17、如权利要求 12，14 或 15 所述的方法，其特征在于，所述方法还包括：

所述 MME 向所述源基站发送所述 NAS 计数的部分比特位。

18、如权利要求 1-17 任一项所述的方法，其特征在于，所述重定向信息包括重定向控制信息或者物理小区标识 PCI 中的至少一种。

19、一种通信装置，其特征在于，所述装置包括：

接收模块，用于从用户设备接收扩展服务请求消息；

发送模块，用于根据所述扩展服务请求消息，向移动性管理实体 MME 发送第一无线资源控制 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站；

所述接收模块，还用于从所述 MME 接收非接入层-消息验证码 NAS-MAC；

所述发送模块，还用于向所述用户设备发送 RRC 连接释放消息，所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括所述第一 RRC 参数的明文或密文。

20、如权利要求 19 所述的装置，其特征在于，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位；

所述接收模块，还用于所述发送模块向所述 MME 发送所述第一 RRC 参数之后，从所述 MME 接收所述 NAS 计数的部分比特位。

21、如权利要求 19 或 20 所述的装置，其特征在于，所述第二 RRC 参数包括所述第一 RRC 参数的密文；

所述接收模块，还用于从所述 MME 接收所述第二 RRC 参数。

22、一种基站，其特征在于，所述基站包括处理器、存储器以及收发器，其中，所述存储器中存储一组程序代码，且所述处理器用于调用存储器中存储的程序代码，用于执行以下操作：

从用户设备接收扩展服务请求消息；

根据所述扩展服务请求消息，向移动性管理实体 MME 发送第一无线资源控制 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站；

从所述 MME 接收非接入层-消息验证码 NAS-MAC；

向所述用户设备发送 RRC 连接释放消息，所述 RRC 连接释放消息包括所述 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括所述第一 RRC 参数的明文或密文。

23、一种通信装置，其特征在于，所述装置包括：

发送模块，用于向源基站发送扩展服务请求消息；

接收模块，用于接收所述源基站发送的无线资源控制 RRC 连接释放消息，所述 RRC 连接释放消息包括非接入层-消息验证码 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括重定向信息；

校验模块，用于根据所述通信装置的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC；

定向模块，用于当所述 NAS-MAC 校验成功时，重定向到所述重定向信息所指示的目标基站。

24、如权利要求 23 所述的装置，其特征在于，所述 RRC 连接释放消息还包括 NAS 计数的部分比特位。

25、如权利要求 24 所述的装置，其特征在于，所述校验模块，具体用于：

根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

根据所述 NAS 完整性密钥、所述第二 RRC 参数以及所述 NAS 计数，校验所述

NAS-MAC。

26、如权利要求 23 或 25 所述的装置，其特征在于，当所述第二 RRC 参数为密文时，所述定向模块，具体用于：

使用所述通信装置的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

重定向到所述重定向信息所指示的目标基站。

27、如权利要求 24 所述的装置，其特征在于，所述校验模块，具体用于：

根据所述 NAS 计数的部分比特位，获取所述 NAS 计数；

根据所述通信装置的接入安全管理实体 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 完整性密钥；

根据所述衍生的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC。

28、如权利要求 27 所述的装置，其特征在于，当所述第二 RRC 参数为密文时，所述定向模块，具体用于：

根据所述通信装置的 ASME 密钥和所述 NAS 计数，获得衍生的 NAS 加密密钥；

使用所述衍生的 NAS 加密密钥对所述第二 RRC 参数进行解密，获得所述重定向信息；

重定向到所述重定向信息所指示的目标基站。

29、如权利要求 23~28 任一项所述的装置，其特征在于，所述装置还包括：

断开模块，用于当所述 NAS-MAC 校验失败时，断开与所述源基站之间的连接。

30、一种用户设备，其特征在于，所述用户设备包括处理器、存储器以及收发器，其中，所述存储器中存储一组程序代码，且所述处理器用于调用存储器中存储的程序代码，用于执行以下操作：

向源基站发送扩展服务请求消息；

接收所述源基站发送的无线资源控制 RRC 连接释放消息，所述 RRC 连接释放消息包括非接入层-消息验证码 NAS-MAC 和第二 RRC 参数，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，所述第二 RRC 参数包括重定向信息；

根据所述用户设备的 NAS 完整性密钥和所述第二 RRC 参数，校验所述 NAS-MAC；

当所述 NAS-MAC 校验成功时，重定向到所述重定向信息所指示的目标基站。

31、一种通信装置，其特征在于，所述装置包括：

接收模块，用于从用户设备的源基站接收第一无线资源控制 RRC 参数，所述第一 RRC 参数包括重定向信息，所述重定向信息用于指示所述用户设备重定向的目标基站；

获取模块，用于根据所述用户设备的非接入层 NAS 完整性密钥和第二 RRC 参数，获得非接入层-消息验证码 NAS-MAC，所述第二 RRC 参数为所述 NAS-MAC 的生成参数，

所述第二 RRC 参数包含所述第一 RRC 参数的明文或密文；
发送模块，用于向所述源基站发送所述 NAS-MAC。

32、如权利要求 31 所述的装置，其特征在于，所述获取模块，具体用于：

使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC；或者，

使用所述用户设备的 NAS 完整性密钥，对所述第二 RRC 参数和 NAS 计数进行完整性保护，生成所述 NAS-MAC。

33、如权利要求 32 所述的装置，其特征在于，

所述获取模块，还用于根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，使用所述用户设备的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

34、如权利要求 31 所述的装置，其特征在于，所述获取模块，具体用于：

根据所述用户设备的接入安全管理实体 ASME 密钥和 NAS 计数，获得衍生的 NAS 完整性密钥；

使用所述衍生的 NAS 完整性密钥对所述第二 RRC 参数进行完整性保护，生成所述 NAS-MAC。

35、如权利要求 34 所述的装置，其特征在于，

所述获取模块，还用于根据所述用户设备的 NAS 完整性密钥和第二 RRC 参数，获得所述 NAS-MAC 之前，根据所述用户设备的 ASME 密钥和 NAS 计数，获得衍生的 NAS 加密密钥；使用所述衍生的 NAS 加密密钥对所述第一 RRC 参数进行加密，得到所述第二 RRC 参数。

36、如权利要求 33 或 35 所述的装置，其特征在于，

所述发送模块，还用于向所述源基站发送所述第二 RRC 参数。

37、如权利要求 32，34 或 35 所述的装置，其特征在于，

所述发送模块，还用于向所述源基站发送所述 NAS 计数的部分比特位。

38、如权利要求 19-37 任一项所述的方法，其特征在于，所述重定向信息包括重定向控制信息或者物理小区标识 PCI 中的至少一种。

39、一种通信系统，其特征在于，所述通信系统包括如权利要求 19-21 任一项所述的基站、如权利要求 23-29 任一项所述的用户设备以及如权利要求 31-38 任一项所述的移动通信管理实体 MME。

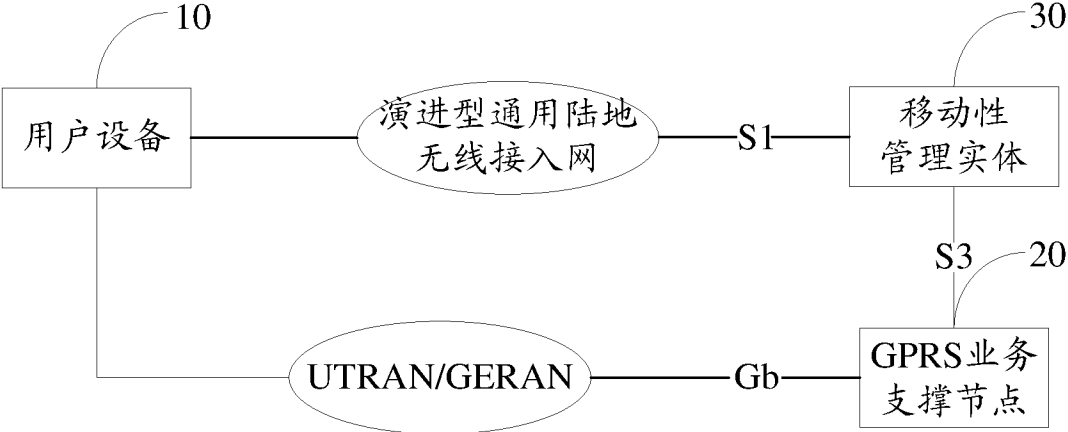


图 1

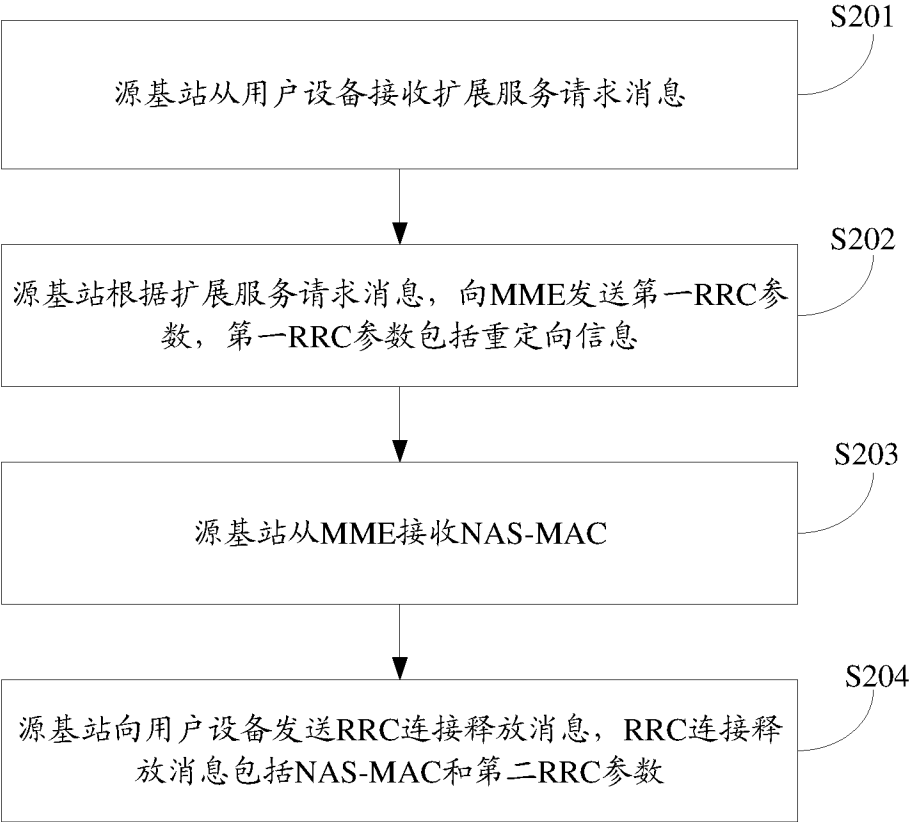


图 2

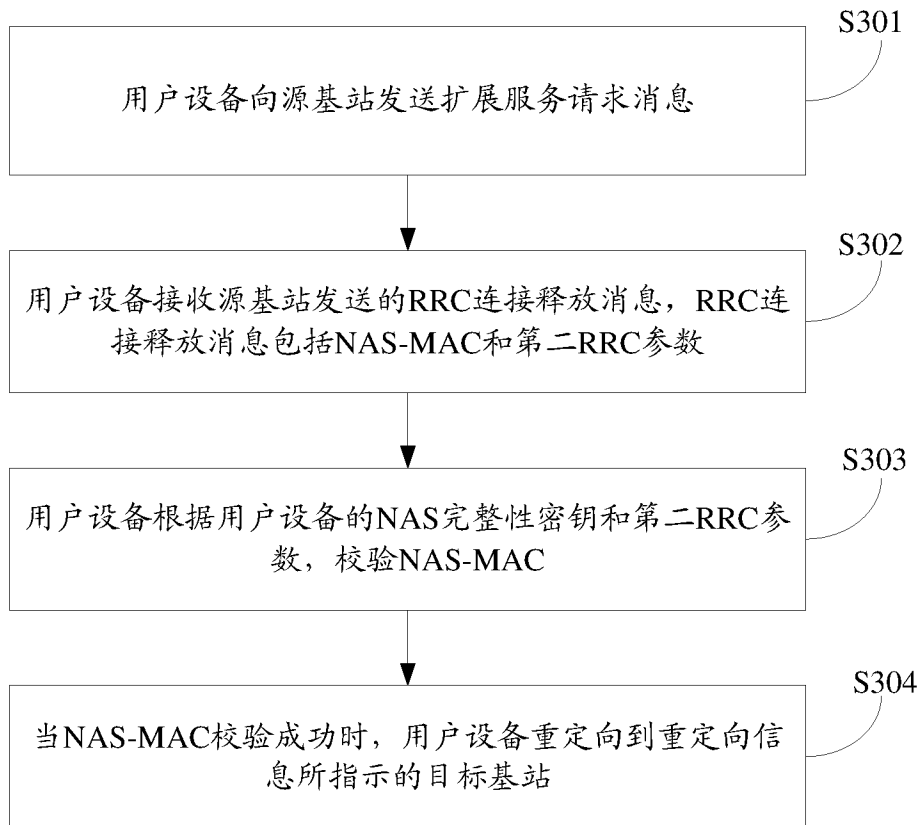


图 3

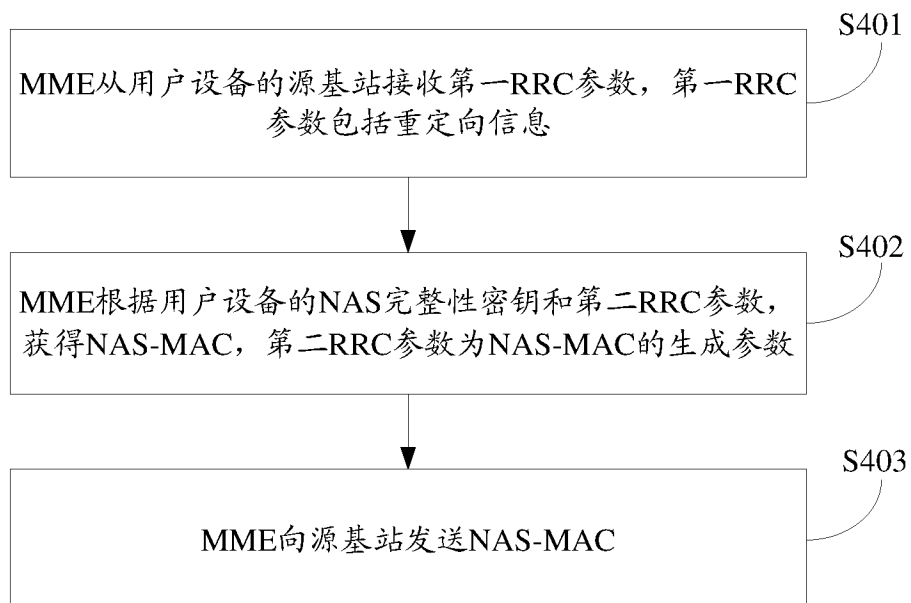


图 4

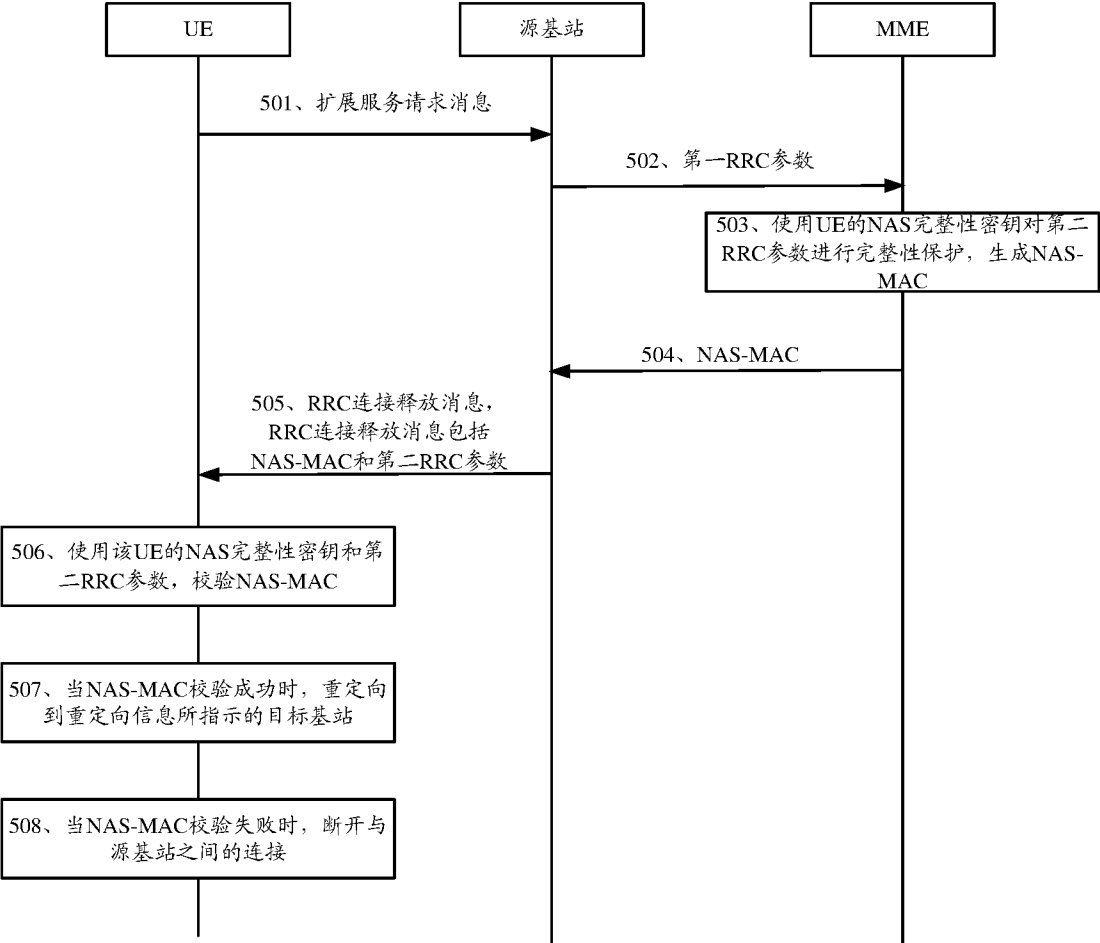


图 5

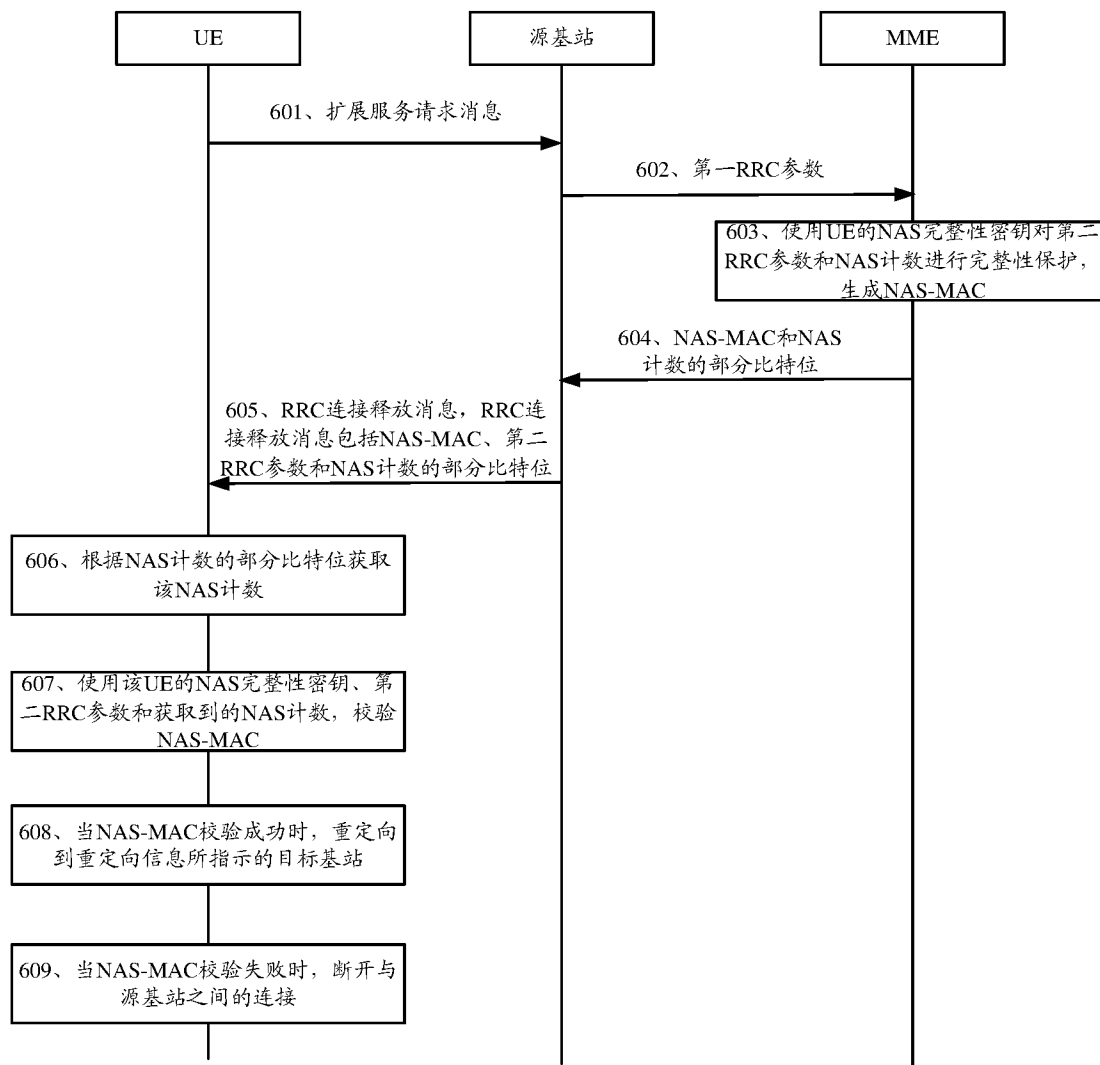


图 6

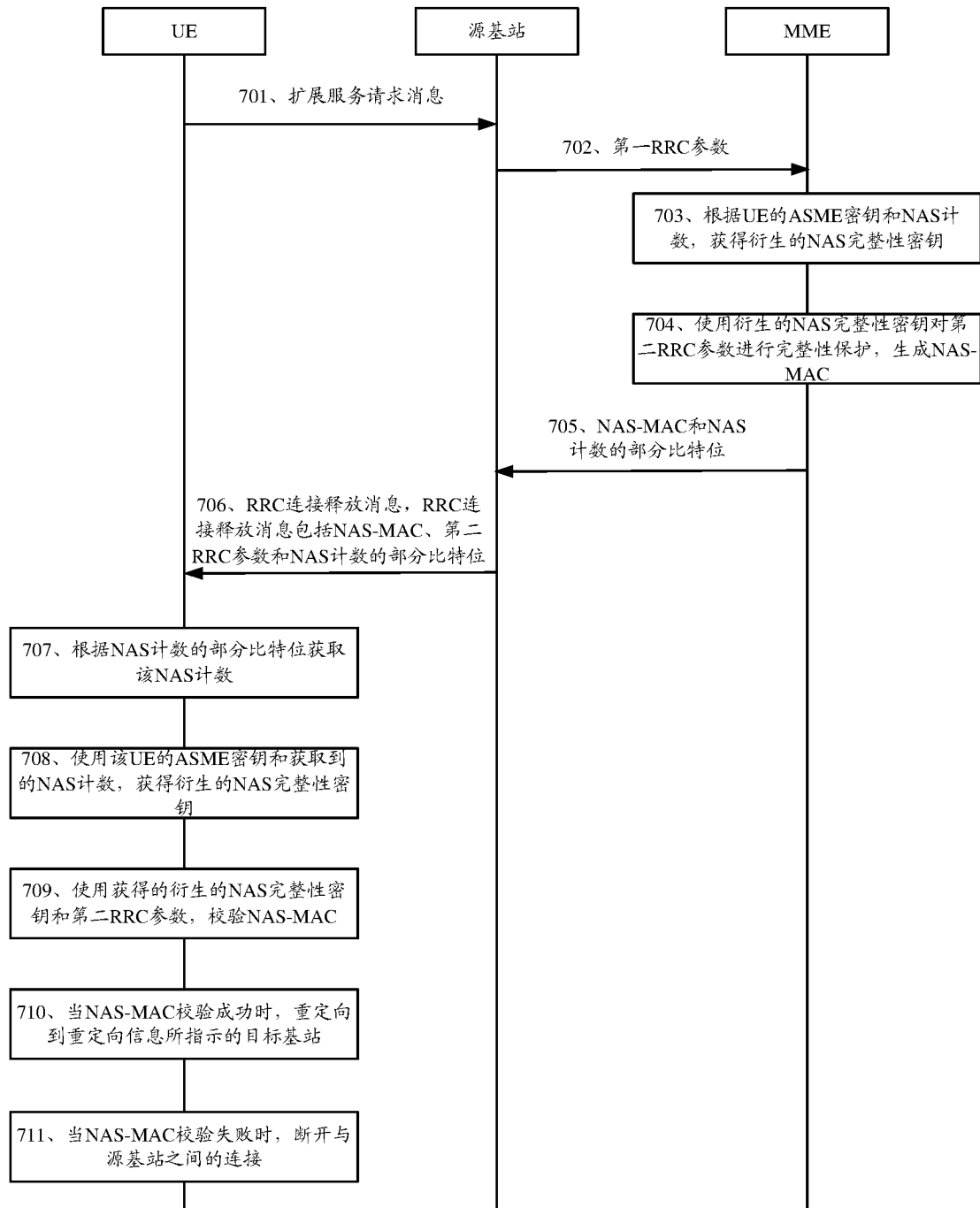


图 7

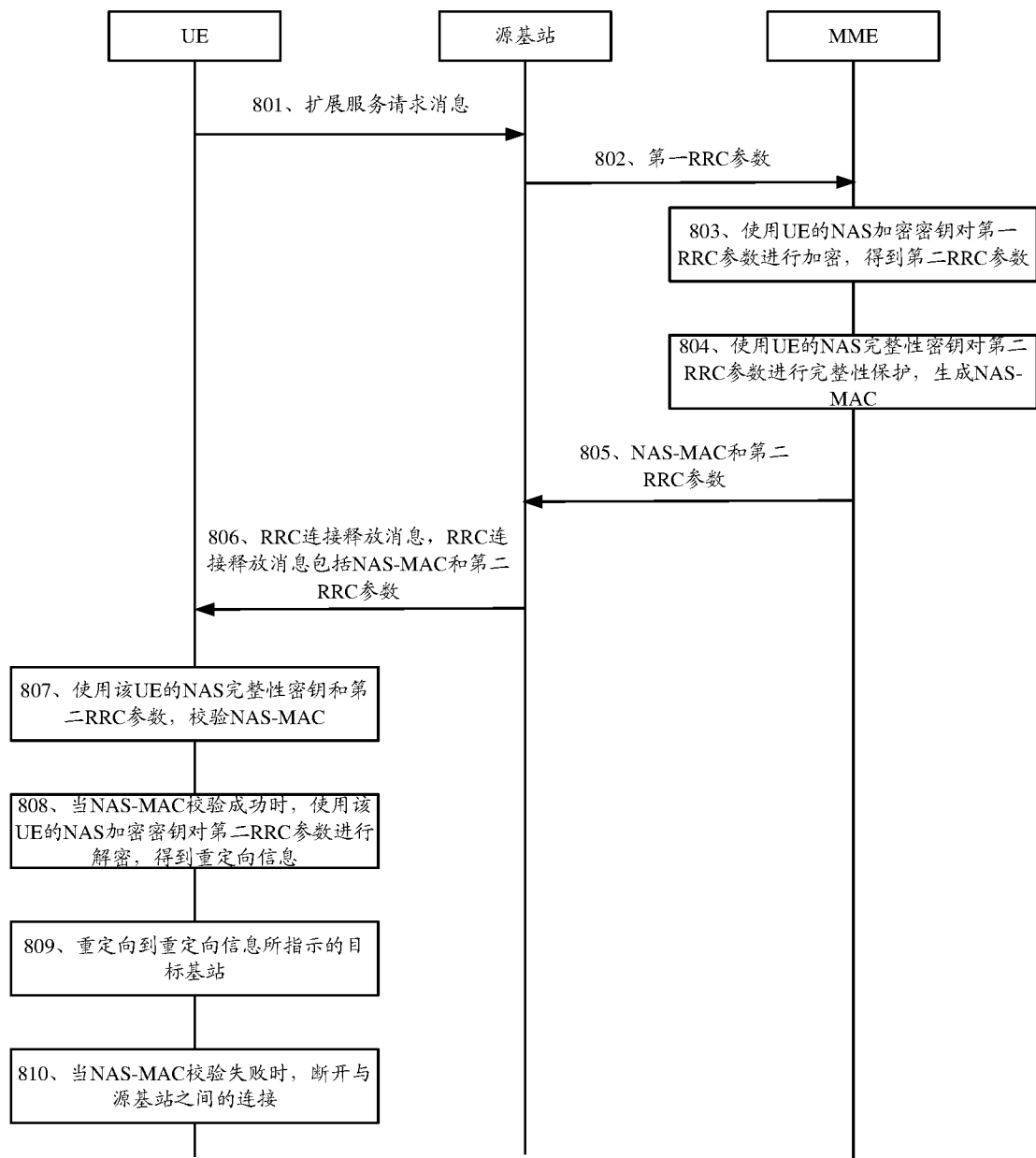


图 8

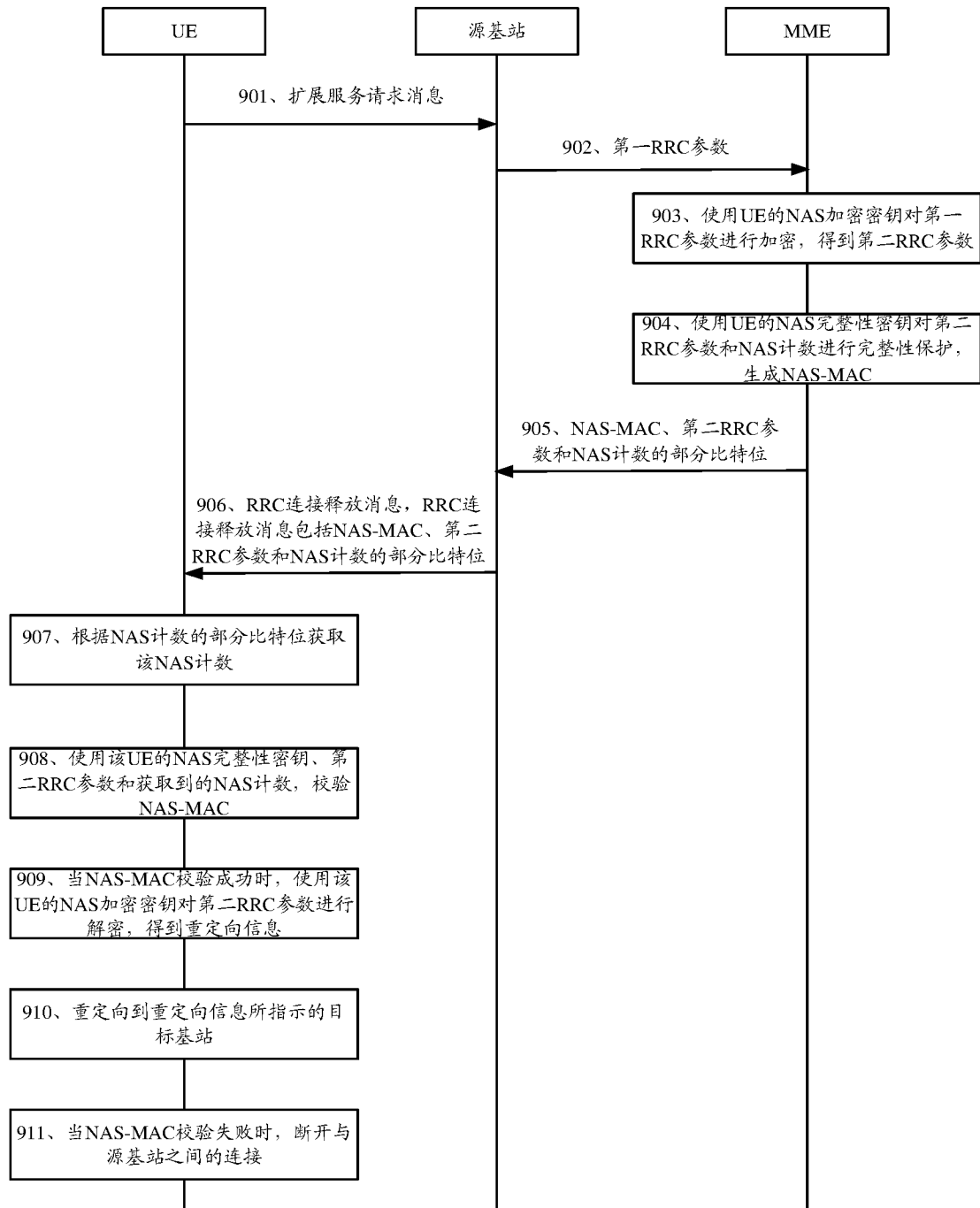


图 9

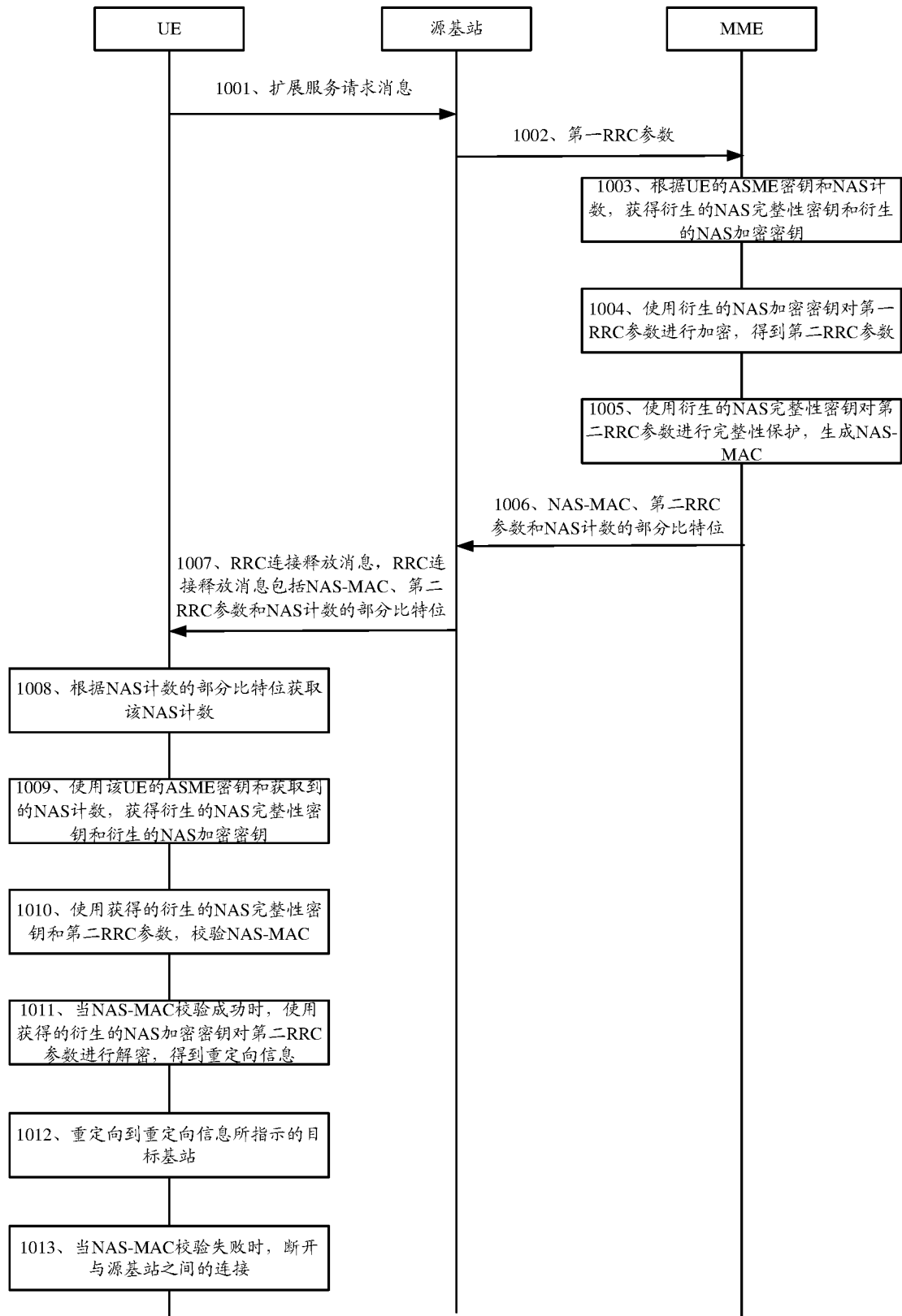


图 10

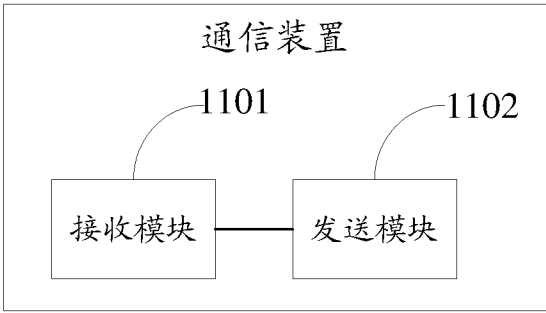


图 11

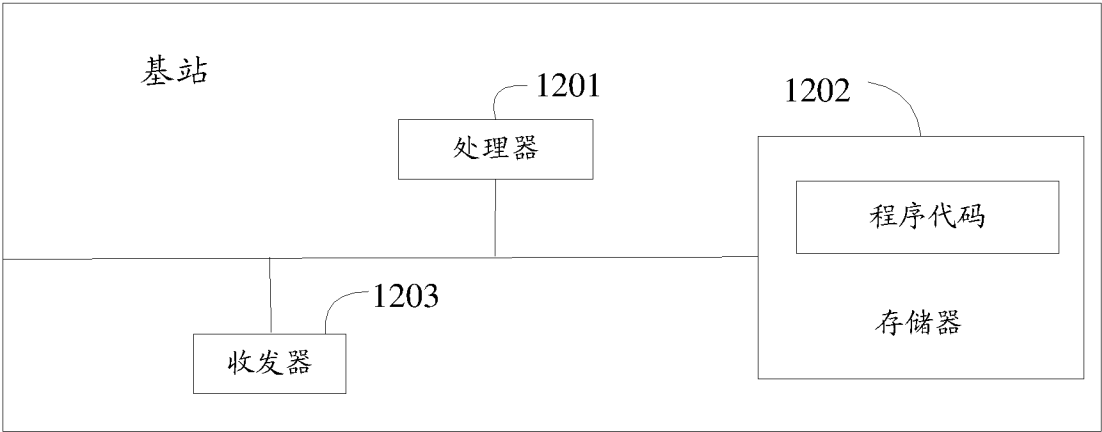


图 12

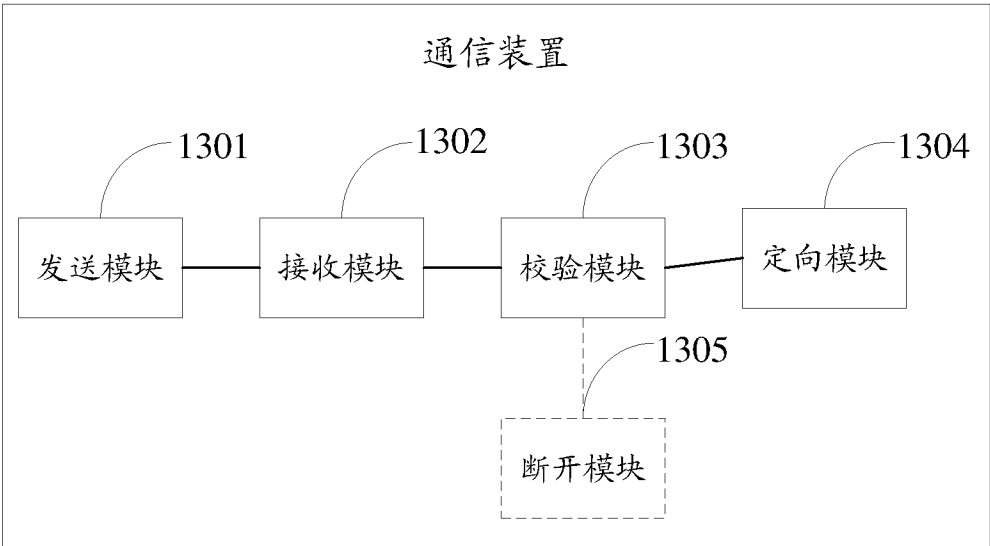


图 13

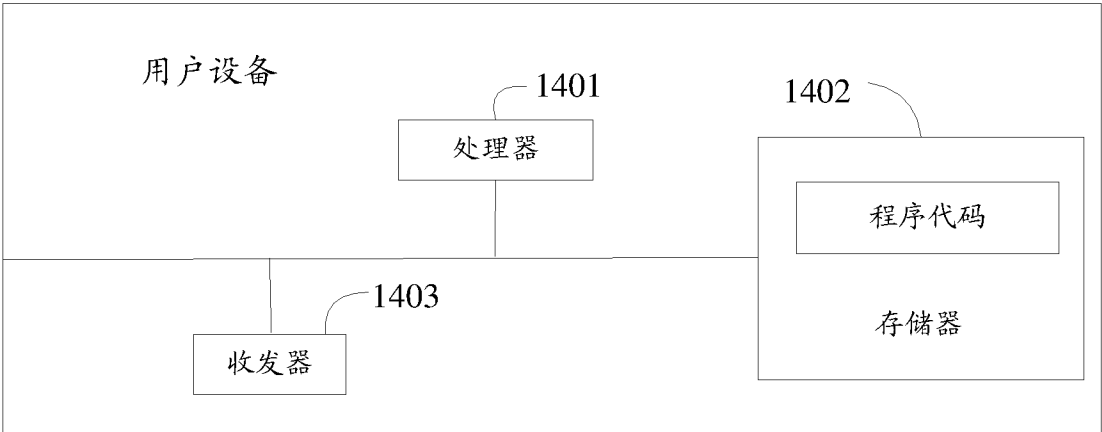


图 14

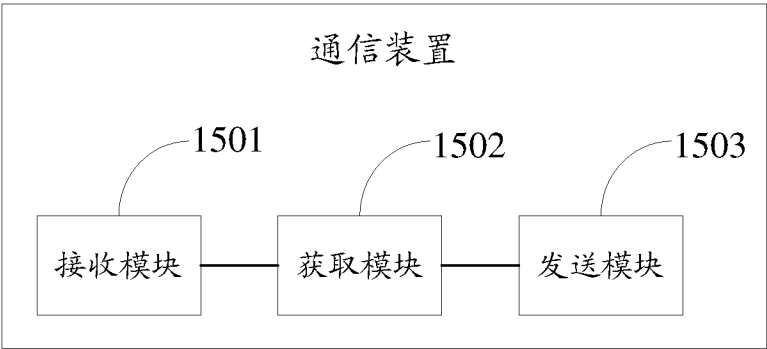


图 15

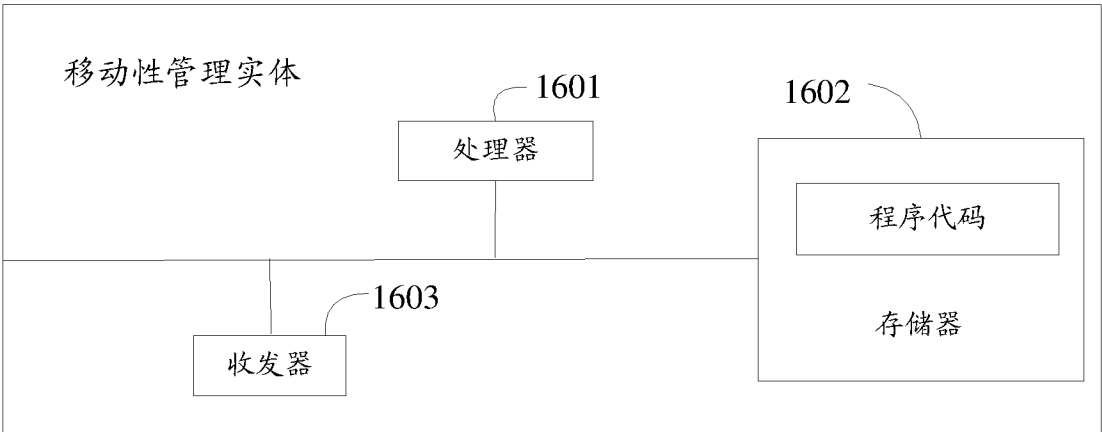


图 16

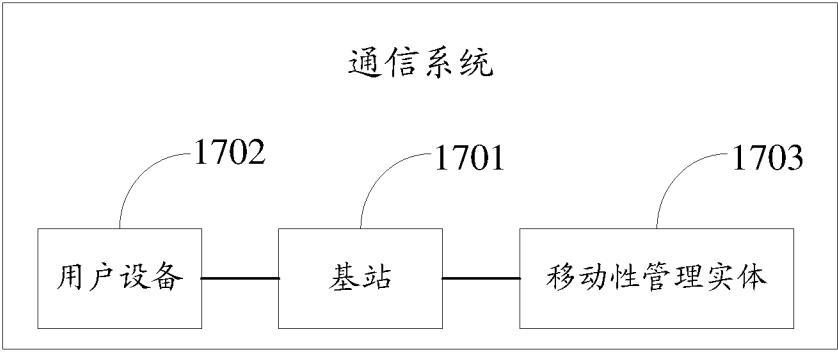


图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/083190

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08 (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; H04Q; 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; WPI; EPODOC; 3GPP: 伪基站, 电路域, 回落, 回退, 扩展服务请求, 扩展业务请求, 非接入层, 消息验证, 消息认证, 源, 目标, 目的, 基站, ENODEB, 移动性管理实体, 移动管理实体, MME, 重定向, 无线资源控制, RRC, 释放, fake, CSFB, ESR, extended service request, NAS, MAC, Message Authentication Code, source, target, redirection, release

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102232317 A (HUAWEI TECHNOLOGIES CO., LTD.), 02 November 2011 (02.11.2011), description, paragraphs [0062]-[0066], and figure 3	1-39
A	CN 103607783 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 26 February 2014 (26.02.2014), entire document	1-39
A	CN 101867986 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 20 October 2010 (20.10.2010), entire document	1-39
A	CN 103813300 A (HUAWEI DEVICE CO., LTD.), 21 May 2014 (21.05.2014), entire document	1-39
A	US 2016007239 A1 (SAMSUNG ELECTRONICS CO., LTD.), 07 January 2016 (07.01.2016), entire document	1-39
A	US 2013201924 A1 (QUALCOMM INCORPORATED), 08 August 2013 (08.08.2013), entire document	1-39

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 11 January 2018	Date of mailing of the international search report 29 January 2018
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 NIU, Xiangchao Telephone No. (86-10) 010-53961672

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/083190

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	HUAWEI et al., "3GPP TSG SA WG3 (Security) Meeting #87 S3-171245", Enhanced NAS Token Solution for LTE Redirection Attack, 19 May 2017 (19.05.2017), entire document	1-39

International application No.
PCT/CN2017/083190

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/083190

A. 主题的分类 H04W 12/08 (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; H04Q; 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; WPI; EPDOC; 3GPP: 伪基站, 电路域, 回落, 回退, 扩展服务请求, 扩展业务请求, 非接入层, 消息验证, 消息认证, 源, 目标, 目的, 基站, ENODEB, 移动性管理实体, 移动管理实体, MME, 重定向, 无线资源控制, RRC, 释放, fake, CSFB, ESR, extended service request, NAS, MAC, Message Authentication Code, source, target, redirection, release																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 102232317 A (华为技术有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书第[0062]-[0066]段, 图3</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>CN 103607783 A (中国联合网络通信集团有限公司) 2014年 2月 26日 (2014 - 02 - 26) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>CN 101867986 A (大唐移动通信设备有限公司) 2010年 10月 20日 (2010 - 10 - 20) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>CN 103813300 A (华为终端有限公司) 2014年 5月 21日 (2014 - 05 - 21) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>US 2016007239 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2016年 1月 7日 (2016 - 01 - 07) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>US 2013201924 A1 (QUALCOMM INCORPORATED) 2013年 8月 8日 (2013 - 08 - 08) 全文</td> <td>1-39</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 102232317 A (华为技术有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书第[0062]-[0066]段, 图3	1-39	A	CN 103607783 A (中国联合网络通信集团有限公司) 2014年 2月 26日 (2014 - 02 - 26) 全文	1-39	A	CN 101867986 A (大唐移动通信设备有限公司) 2010年 10月 20日 (2010 - 10 - 20) 全文	1-39	A	CN 103813300 A (华为终端有限公司) 2014年 5月 21日 (2014 - 05 - 21) 全文	1-39	A	US 2016007239 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2016年 1月 7日 (2016 - 01 - 07) 全文	1-39	A	US 2013201924 A1 (QUALCOMM INCORPORATED) 2013年 8月 8日 (2013 - 08 - 08) 全文	1-39
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
A	CN 102232317 A (华为技术有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书第[0062]-[0066]段, 图3	1-39																					
A	CN 103607783 A (中国联合网络通信集团有限公司) 2014年 2月 26日 (2014 - 02 - 26) 全文	1-39																					
A	CN 101867986 A (大唐移动通信设备有限公司) 2010年 10月 20日 (2010 - 10 - 20) 全文	1-39																					
A	CN 103813300 A (华为终端有限公司) 2014年 5月 21日 (2014 - 05 - 21) 全文	1-39																					
A	US 2016007239 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2016年 1月 7日 (2016 - 01 - 07) 全文	1-39																					
A	US 2013201924 A1 (QUALCOMM INCORPORATED) 2013年 8月 8日 (2013 - 08 - 08) 全文	1-39																					
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td style="vertical-align: top;"> * 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 </td> <td style="vertical-align: top;"> “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 </td> </tr> </table>			* 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																			
* 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 2018年 1月 11日		国际检索报告邮寄日期 2018年 1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		授权官员 牛相潮 电话号码 (86-10) 010-53961672																					

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
T	HUAWEI et al. "3GPP TSG SA WG3 (Security) Meeting #87 S3-171245" Enhanced NAS token solution for LTE redirection attack, 2017年 5月 19日 (2017 - 05 - 19), 全文	1-39

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/083190

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	102232317	A	2011年 11月 2日	WO	2012055093	A1	2012年 5月 3日
CN	103607783	A	2014年 2月 26日	无			
CN	101867986	A	2010年 10月 20日	无			
CN	103813300	A	2014年 5月 21日	无			
US	2016007239	A1	2016年 1月 7日	CN	105027622	A	2015年 11月 4日
				WO	2014133313	A1	2014年 9月 4日
				EP	2962492	A1	2016年 1月 6日
				KR	20150128756	A	2015年 11月 18日
				IN	201300828	I4	2016年 6月 3日
US	2013201924	A1	2013年 8月 8日	WO	2013119375	A1	2013年 8月 15日