(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 1 月 30 日 (30.01.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/019328 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2018/097607

(22) 国际申请日: 2018 年 7 月 27 日 (27.07.2018)

(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: 卓超 (**ZHUO, Chao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 刘涛 (**LIU, Tao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李洪 (**LI, Hong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市海淀区宝盛南路1号院20号楼8层101-01, Beijing 100192 (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,

WO 2020/019328 A1

(54) **Title:** PSEUDO BASE-STATION IDENTIFICATION METHOD AND APPARATUS

(54) 发明名称: 一种伪基站识别方法及装置

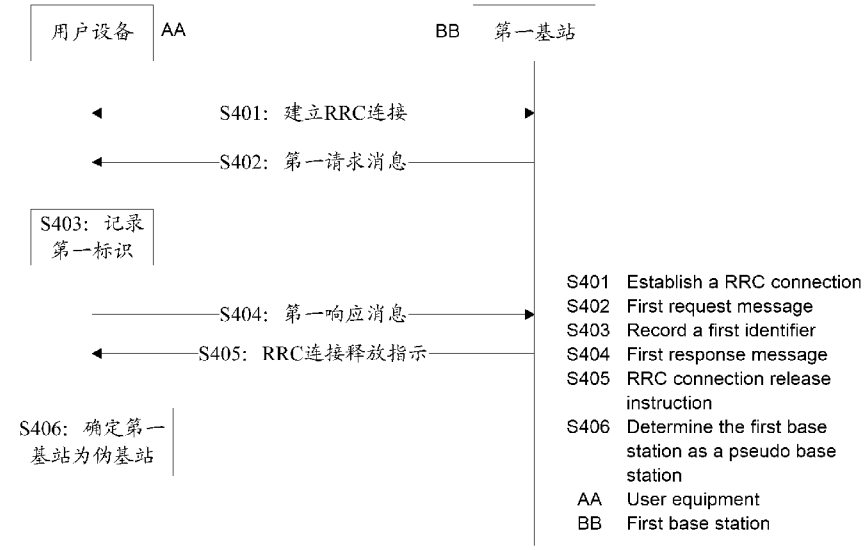

图 4

(57) **Abstract:** A pseudo base-station identification method and apparatus, for identifying a pseudo base station by a user equipment, so as to take corresponding processing to avoid the user equipment frequently from residing on a pseudo base-station cell, thereby causing that the user equipment cannot carry out normal communication. The method comprises: the user equipment establishes a RRC connection to a first base station to which a first cell where the user equipment currently resides belongs; the user equipment receives a first request message sent by the first base station, the first request message being used to request for querying an IMSI of the user equipment; the user equipment records a first identifier, the first identifier being used to instruct the first base station to request

[见续页]

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, 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))。

for querying the IMSI of the user equipment; the user equipment receives a RRC connection release instruction sent by the first base station; after receiving the RRC connection release instruction and confirming that the first identifier is recorded, the user equipment determines the first base station as a pseudo base station.

(57) 摘要：一种伪基站识别方法及装置，用以用户设备识别伪基站，从而采取相应处理，避免用户设备频繁驻留到伪基站小区，导致用户设备无法进行正常通信。方法包括：用户设备与当前驻留的第一小区所属的第一基站建立RRC连接；用户设备接收第一基站发送的第一请求消息，第一请求消息用于请求查询用户设备的IMSI；用户设备记录第一标识，第一标识用于指示第一基站请求查询用户设备的IMSI；用户设备向第一基站发送第一响应消息，第一响应消息用于指示用户设备的IMSI；用户设备接收第一基站发送的RRC连接释放指示；用户设备在接收到RRC连接释放指示后、且确认记录有第一标识时，确定第一基站为伪基站。

一种伪基站识别方法及装置

技术领域

本申请涉及通信技术领域，尤其涉及一种伪基站识别方法及装置。

背景技术

现网存在这样一类伪基站：该伪基站通过明文获取用户设备（user equipment，UE）的国际移动用户标识（international mobile subscriber identity，IMSI）信息，通过该 IMSI 信息对用户设备进行定位。这类基站主要是公安等安保部门出于维稳目的设置的，通常分布在人流较大的场所，例如火车站、广场、商场、城区主要十字路口，以及一些敏感地带，例如银行、宾馆等。

该类基站模拟周围正常基站的配置并提高自身的发射功率，同时修改基站部分配置来诱导更多用户设备驻留到该伪基站小区，并触发用户设备与伪基站建立连接，从而获取用户设备的 IMSI。

由于这类伪基站的发射功率较高等原因，用户设备易驻留到伪基站小区。即使用户设备与伪基站间的连接释放，用户设备重新进行搜网后仍然大概率会驻留到伪基站小区。

因此，亟需一种伪基站识别方案，使得用户设备能识别出这类伪基站，从而采取相应处理，避免频繁驻留到伪基站小区，导致用户设备无法进行正常通信。

发明内容

本申请实施例提供一种伪基站识别方法及装置，用以用户设备识别伪基站，从而采取相应处理，避免用户设备频繁驻留到伪基站小区，导致用户设备无法进行正常通信。

第一方面，本申请实施例提供一种伪基站识别方法，该方法包括如下步骤：用户设备与当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；用户设备接收第一基站发送的第一请求消息，第一请求消息用于请求查询用户设备的国际移动用户标识 IMSI；用户设备记录第一标识，第一标识用于指示第一基站请求查询用户设备的 IMSI；用户设备向第一基站发送第一响应消息，第一响应消息用于指示用户设备的 IMSI；用户设备接收第一基站发送的 RRC 连接释放指示；用户设备在接收到 RRC 连接释放指示后、且确认记录有第一标识时，确定第一基站为伪基站。

在第一方面提供的伪基站识别方法中，与第一基站建立 RRC 连接后，用户设备在第一基站未触发鉴权而直接发送第一请求消息时记录第一标识。在第一基站主动释放链路后，用户设备在记录有第一标识的情况下可以确定第一基站为伪基站。

在一种可能的设计中，在用户设备确定第一基站为伪基站之后，用户设备可将第一小区的小区信息加入第一受限列表，该第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区。

其中，第一受限列表也可以称为小区受限列表或者 bar 列表。用户设备的 RRC 层可维护有第一受限列表。第一受限列表中记录有小区信息，用于指示用户设备禁止驻留在记录的小区信息所对应的小区。

此外，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小

区频段；第一小区的物理小区标识 PCI、第一小区的 E-UTRA 绝对无线频率信道号 EARFCN。

将第一小区的小区信息加入第一受限列表后，可避免用户设备再次驻留在第一小区这一伪基站小区。

进一步地，在用户设备将第一小区的小区信息加入第一受限列表之后，用户设备还可进行小区搜索；然后，用户设备根据小区搜索结果驻留到第二小区，第二小区的小区信息未记录在第一受限列表中。

也就是说，将第一小区的小区信息加入第一受限列表之后，用户设备在重新进行小区搜索时，需要将第一受限列表中的小区剔除，只有在搜索到第一受限列表之外的可用小区时，才选择驻留到该小区。

采用上述方案，用户设备可重新进行搜网，从而使得用户设备可以驻留到合法基站小区，进行正常通信。

需要说明的是，需要说明的是，在上述方案中，仅限定第二小区的小区信息未记录在第一受限列表中，对第二小区的类型不做具体限定。示例性地，第二小区可以是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，第二小区可以是属于另一个伪基站的、未记录在第一受限列表中的小区，第二小区也可以是属于合法基站的小区。

若第二小区是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，或者第二小区是属于另一个伪基站的、未记录在第一受限列表中的小区，那么，用户设备可通过执行上述伪基站识别方法判断第二小区为伪基站小区，进而将第二小区的小区信息也加入第一受限列表，用户设备在再次搜网时则不会再次驻留到第二小区。若第二小区是属于合法基站的小区，则用户设备在驻留到第二小区后，可与第二小区对应的基站进行正常通信。

在一种可能的设计中，在接收第一基站发送的 RRC 连接释放指示之后，用户设备可根据用户设备的配置将第一小区的域标识加入第二受限列表，第一小区的域标识为第一小区的位置区 LA 域标识或跟踪区 TA 域标识，第二受限列表用于指示用户设备禁止驻留在第二受限列表中记录的域标识所对应的小区。

采用上述方案，用户设备可根据配置决定是否将第一小区的域标识加入第二受限列表。若将第一小区的域标识加入第二受限列表，可禁止用户设备驻留在第一小区的域标识所对应的小区内。

此外，在第一方面提供的伪基站识别方法中，若用户设备中未记录第一标识，则在用户设备接收到第一基站发送的 RRC 连接释放指示之后，且用户设备记录有第一标识时，用户设备可确定第一基站不是伪基站；然后，用户设备可将第一小区的域标识加入第三受限列表，第一小区的域标识为第一小区的 LA 域标识或 TA 域标识，第三受限列表用于指示用户设备禁止驻留在受限列表中记录的域标识所对应的小区。

其中，第三受限列表与前述第二受限列表可以是同一列表。

在上述实现方式中，第一基站在与用户设备建立连接后，并未触发后续的鉴权操作。但是，第一基站也未请求查询用户设备的 IMSI，因而用户设备中并未记录第一标识。在用户设备接收到第一基站发送的 RRC 连接释放指示后，由于第一基站与用户设备的交互流程并不符合用户设备与伪基站的交互流程，因而用户设备判断第一基站并不是伪基站。

第二方面，本申请实施例提供一种伪基站识别方法，该方法包括如下步骤：用户设备

与当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；用户设备统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数；用户设备在该次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区。

其中，通信异常情况包括但不限于：用户设备的非接入层 NAS 协议保护定时器超时；用户设备的物理层或媒体访问控制层 MAC 层向 RRC 层上报无线链路失败 RLF；第一基站未请求查询用户设备的 IMSI，且第一基站向用户设备发送 RRC 连接释放指示。

采用上述方案，伪基站在与用户设备建立 RRC 连接后，会因通信异常情况导致用户设备与伪基站的 RRC 连接释放。此外，若用户设备当前驻留小区为坏小区时，也可能发生上述通信异常情况。因此，在上述方法中，与第一基站建立 RRC 连接后，用户设备通过判断在第一小区上因通信异常情况导致 RRC 连接释放的次数是否大于第一阈值，可以确定第一基站为伪基站或者第一小区为坏小区。

在一种可能的设计中，在用户设备确定第一基站为伪基站或者第一小区为坏小区之后，用户设备可将第一小区的小区信息加入第一受限列表，该第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区；然后，用户设备进行小区搜索；若用户设备未搜索到其他可用小区，则用户设备将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区；若用户设备搜索到第二小区为可用小区，则用户设备驻留第二小区，第二小区的小区信息未记录在第一受限列表中。

其中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的 PCI、第一小区的 EARFCN。

采用上述实现方式，由于用户设备在重新进行搜网时需要剔除第一受限列表中的小区，因而将第一小区的小区信息加入第一受限列表，可以避免用户设备再次驻留到第一小区。后续，用户设备可重新进行小区搜索，并驻留到第二小区。此外，若用户设备重新进行小区搜索后未搜索到可用小区，则用户设备当前无可驻留小区，那么，用户设备可将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区。

在一种可能的设计中，在用户设备与第一小区所属的第一基站建立 RRC 连接之前，用户设备可保存第一小区的小区信息；用户设备在统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数，包括：用户设备统计记录的小区信息指示的第一小区上因通信异常情况导致 RRC 连接释放的次数。

采用上述方案，在用户设备与第一基站建立 RRC 连接之前，用户设备可保存当前驻留小区的小区信息，在后续出现通信异常情况时，用户设备可判断该通信异常情况发生在哪个小区，并针对不同小区分别统计次数。

在一种可能的设计中，在用户设备确定第一基站为伪基站或者第一小区为坏小区之后，用户设备可获取用于指示用户设备当前位置的第一位置信息；在用户设备将第一小区的小区信息加入第一受限列表之后，用户设备可获取用于指示用户设备当前位置的第二位置信息；然后，用户设备在第一位置信息指示的位置与第二位置信息指示的位置之间的距离大于第二阈值时，将第一小区的小区信息从第一受限列表中删除。

采用上述方案，可在确定第一基站为伪基站之后记录伪基站当前的第一位置，并在将第一小区的小区信息加入第一受限列表之后不断测量（例如周期性测量）用户设备的当前位置（第二位置），并与第一位置信息指示的位置进行比较。在第二位置与第一位置的距离之差大于第二阈值时，即可判断用户设备离开伪基站小区的覆盖范围，此时可将第一小

区的小区信息从第一受限列表中删除，从而使得用户设备可以驻留在与伪基站有相同配置的合法基站。

在一种可能的设计中，在用户设备与第一小区所属的第一基站建立 RRC 连接之前，用户设备可在确定第一基站的系统消息配置异常时保存类伪基站配置标识，该类伪基站配置标识用于指示第一基站的系统消息配置异常；用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区，包括：用户设备在该次数大于第一阈值、且用户设备中保存有类伪基站配置标识时，确定第一基站为伪基站。

在进行系统消息配置时，合法基站和伪基站的配置会有所不同。采用上述方案，可以通过识别第一基站的系统消息配置是否体现有伪基站的系统消息配置的特点，来判断第一基站是否为伪基站。即，通过第一基站的系统消息配置情况可判断第一基站是否为伪基站。

其中，用户设备在以下信息中的至少一种满足时，确定第一基站的系统消息配置异常：用户设备确定第一基站配置在共享公共陆地移动网络 PLMN 列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识；用户设备确定第一基站的驻留门限低于用户设备配置的驻留门限阈值；用户设备确定第一基站未配置异频邻区和异系统邻区；用户设备确定第一基站配置全球移动通信 GSM 邻区的优先级为高重选优先级。

第三方面，本申请实施例还提供一种伪基站识别装置，该装置应用于用户设备，包括收发单元和处理单元。其中，收发单元用于与用户设备当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；以及，接收第一基站发送的第一请求消息，第一请求消息用于请求查询用户设备的国际移动用户标识 IMSI；处理单元用于记录记录第一标识，第一标识用于指示第一基站请求查询用户设备的 IMSI；收发单元还用于向第一基站发送第一响应消息，第一响应消息用于指示用户设备的 IMSI；收发单元还用于接收第一基站发送的 RRC 连接释放指示；处理单元还用于在收发单元接收到 RRC 连接释放指示后、且确认记录有第一标识时，确定第一基站为伪基站。

在一种可能的设计中，处理单元还用于：在确定第一基站为伪基站之后，将第一小区的小区信息加入第一受限列表，第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区。

在一种可能的设计中，处理单元还用于：在将第一小区的小区信息加入第一受限列表之后进行小区搜索；根据小区搜索结果驻留到第二小区，第二小区的小区信息未记录在第一受限列表中。

在一种可能的设计中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的物理小区标识 PCI、第一小区的 E-UTRA 绝对无线频率信道号 EARFCN。

在一种可能的设计中，处理单元还用于：在收发单元接收第一基站发送的 RRC 连接释放指示之后，根据用户设备的配置将第一小区的域标识加入第二受限列表，第一小区的域标识为第一小区的位置区 LA 域标识或跟踪区 TA 域标识，第二受限列表用于指示用户设备禁止驻留在第二受限列表中记录的域标识所对应的小区。

在一种可能的设计中，处理单元还用于：若处理单元中未记录第一标识，则在收发单元接收到第一基站发送的 RRC 连接释放指示之后，确定第一基站不是伪基站；将第一小区的域标识加入第三受限列表，第一小区的域标识为第一小区的 LA 域标识或 TA 域标识，

第三受限列表用于指示用户设备禁止驻留在受限列表中记录的域标识所对应的小区。

第四方面，本申请实施例还提供一种伪基站识别装置，该装置应用于用户设备，包括收发单元和处理单元。其中，收发单元用于与用户设备当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；处理单元用于统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数；处理单元还用于在该次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区。

在一种可能的设计中，处理单元还用于：在确定第一基站为伪基站或者第一小区为坏小区之后，将第一小区的小区信息加入第一受限列表，第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区；进行小区搜索；若未搜索到其他可用小区，则将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区；若搜索到第二小区为可用小区，则驻留第二小区，第二小区的小区信息未记录在第一受限列表中。

在一种可能的设计中，处理单元还用于：在收发单元与第一小区所属的第一基站建立 RRC 连接之前，保存第一小区的小区信息；处理单元在统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数时，具体用于：统计记录的小区信息指示的第一小区上因通信异常情况导致 RRC 连接释放的次数。

在一种可能的设计中，处理单元还用于：在确定第一基站为伪基站或者第一小区为坏小区之后，获取用于指示用户设备当前位置的第一位置信息；在将第一小区的小区信息加入第一受限列表之后，获取用于指示用户设备当前位置的第二位置信息；在第一位置信息指示的位置与第二位置信息指示的位置之间的距离大于第二阈值时，将第一小区的小区信息从第一受限列表中删除。

在一种可能的设计中，处理单元还用于：在收发单元与第一小区所属的第一基站建立 RRC 连接之前，在确定第一基站的系统消息配置异常时保存类伪基站配置标识，类伪基站配置标识用于指示第一基站的系统消息配置异常；处理单元在第一小区上因通信异常情况导致 RRC 连接释放的次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区时，具体用于：在该次数大于第一阈值、且用户设备中保存有类伪基站配置标识时，确定第一基站为伪基站。

在一种可能的设计中，处理单元在以下信息中的至少一种满足时，确定第一基站的系统消息配置异常：处理单元确定第一基站配置在共享公共陆地移动网络 PLMN 列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识；处理单元确定第一基站的驻留门限低于用户设备配置的驻留门限阈值；处理单元确定第一基站未配置异频邻区和异系统邻区；处理单元确定第一基站配置全球移动通信 GSM 邻区的优先级为高重选优先级。

在一种可能的设计中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的物理小区标识 PCI。

在一种可能的设计中，通信异常情况包括：用户设备的非接入层 NAS 协议保护定时器超时；用户设备的物理层或媒体访问控制层 MAC 层向 RRC 层上报无线链路失败 RLF；第一基站未请求查询用户设备的 IMSI，且第一基站向用户设备发送 RRC 连接释放指示。

第五方面，本申请实施例提供一种伪基站识别装置，该装置包括处理器，所述处理器与存储器耦合，并读取所述存储器中的指令，用于执行第一方面或上述第一方面至第二方

面中任一方面或任一方面的任意一种设计所述的方法。

需要说明的是，第三方面至第五方面中任一方面或任一方面的任意一种设计提供的伪基站识别装置可视为用户设备中的集成芯片，也可以也视为用户设备。

具体地，该用户设备包括但不限于智能手机、智能手表、平板电脑、虚拟现实（virtual reality，VR）设备、增强现实（augmented reality，AR）设备、个人计算机、手持式计算机、个人数字助理。

第六方面，本申请实施例还提供了一种计算机可读存储介质，用于存储为执行上述第一方面至第二方面中任一方面或任一方面的任意一种设计的功能所用的程序，该程序被处理器执行时，用于实现上述第一方面至第二方面中任一方面或任一方面的任意一种设计所述的方法。

第七方面，本申请实施例提供了一种包含程序代码的计算机程序产品，当其包含的程序代码在计算机上运行时，使得计算机执行上述第一方面或上述第一方面至第二方面中任一方面或任一方面的任意一种设计所述的方法。

另外，第三方面至第七方面中任一种可能设计方式所带来的技术效果可参见第一方面和第二方面中不同设计方式所带来的技术效果，此处不再赘述。

附图说明

图 1 为本申请实施例提供的一种伪基站与用户设备的交互流程示意图；

图 2 为本申请实施例提供的另一种伪基站与用户设备的交互流程示意图；

图 3 为本申请实施例提供的一种本申请实施例的应用场景的示意图；

图 4 为本申请实施例提供的第一种伪基站识别方法的流程示意图；

图 5 为本申请实施例提供的第二种伪基站识别方法的流程示意图；

图 6 为本申请实施例提供的第三种伪基站识别方法的流程示意图；

图 7 为本申请实施例提供的第四种伪基站识别方法的流程示意图；

图 8 为本申请实施例提供的第五种伪基站识别方法的流程示意图；

图 9 为本申请实施例提供的第六种伪基站识别方法的流程示意图；

图 10 为本申请实施例提供的第一种伪基站识别装置的结构示意图；

图 11 为本申请实施例提供的第二种伪基站识别装置的结构示意图；

图 12 为本申请实施例提供的第三种伪基站识别装置备的结构示意图；

图 13 为本申请实施例提供的第四种伪基站识别装置的结构示意图。

具体实施方式

如背景技术中所述，公安等安保部门出于维稳目的，会在火车站、广场、商场、城区主要十字路口等人流较大的场所，或者银行、宾馆等敏感地带设置伪基站。伪基站通过模拟周围正常基站的配置并提高自身的发射功率，同时修改基站部分配置来诱导更多用户设备驻留到伪基站小区，并触发用户设备与伪基站建立连接，从而获取用户设备的 IMSI，通过该 IMSI 信息对用户设备进行定位。

由于伪基站发射功率较高等原因，用户设备易驻留到伪基站小区。即使用户设备与伪基站间的连接释放，用户设备重新进行搜网后仍然大概率会驻留到伪基站小区。

下面，介绍现有协议（3GPP TS 24.301）中给出的用户设备与伪基站的两种交互流程。

其中，流程一为用户设备与伪基站正常交互的流程；流程二为用户设备与伪基站交互过程中出现通信异常情况时的交互流程。

流程一

参见图 1，为未发生通信异常的情况下用户设备与伪基站的交互流程。该流程包括如下步骤。

1、用户设备被伪基站诱导，向伪基站发送附着请求消息（ATTACH_REQ）、跟踪区更新请求消息（TAU_REQ）或位置区更新请求消息（LAU_REQ）。

由于伪基站模拟周围正常基站的配置，且提高自身的发射功率，因而易诱导用户设备触发与伪基站建立连接。

2、用户设备向伪基站发送无线资源控制（radio resource control，RRC）连接请求消息（RRC_CONN_REQ），请求与伪基站建立 RRC 连接。

3、伪基站向用户设备发送 RRC 连接建立消息（RRC_CONN_SETUP）。

4、用户设备向伪基站发送 RRC 连接建立完成消息（RRC_CONN_SETUP_CMPLT），以指示用户设备与伪基站间的 RRC 连接建立完成。

5、伪基站在 RRC 连接建立完成后不再触发后续的鉴权操作，而是直接向用户设备发送身份识别请求消息（IDENFITY_REQ），以请求获取用户设备的 IMSI。

6、用户设备向伪基站发送身份识别响应消息（IDENFITY_RSP），其中携带该用户设备的 IMSI。

7、伪基站在查询到用户设备的 IMSI 后，即向用户设备发送附着拒绝消息（ATTACH_REJ）、跟踪区更新拒绝消息（TAU_REJ）或位置区更新拒绝消息（LAU_REJ）。

其中，ATTACH_REJ、TAU_REJ 或 LAU_REJ 中可携带拒绝原因值#13（该跟踪区不允许漫游）或#15（该跟踪区没有合适小区）。

8、伪基站向用户设备发送 RRC 连接释放消息（RRC_CONN_RELEASE），以释放与用户设备间的 RRC 连接。

在用户设备与伪基站间的 RRC 连接释放后，用户设备的非接入层（non-access stratum，NAS）指示 RRC 层将伪基站小区的跟踪区（tracking area，TA）域标识或位置区（location area，LA）域标识加入到受限（forbidden）列表中，从而禁止用户设备驻留在 TA 域标识或 LA 域标识对应的小区中。具体地，若用户设备当前驻留在 4G 小区，则 NAS 可指示 RRC 将当前小区的 TA 域标识加入受限列表；若用户设备当前驻留在 3G 小区，则 NAS 可指示 RRC 将当前小区的 LA 域标识加入受限列表。然后，用户设备重新进行搜网，驻留到其他小区。若用户设备再次驻留到伪基站小区，则重复上述步骤 1~8。

示例性地，若用户设备当前驻留在 4G 小区，则 NAS 可指示 RRC 层将伪基站小区的 TA 域标识加入受限列表；若用户设备当前驻留在 3G 小区，则 NAS 可指示 RRC 层将伪基站小区的 LA 域标识加入受限列表。

在流程一中，由于伪基站的 TA 域标识或 LA 域标识定时变化，因而在将伪基站小区的 TA 域标识或 LA 域标识加入 forbidden 列表后，用户设备极易再次驻留到伪基站小区。此外，若伪基站的 TA 域标识或 LA 域标识与合法基站相同，将伪基站小区的 TA 域标识或 LA 域标识加入 forbidden 列表还会导致用户设备无法驻留到合法基站小区，即导致限制范围过大。

由此可以看出，在流程一中，由于用户设备未明确识别出驻留基站为伪基站，并针对伪基站小区进行适当处理，导致用户设备频繁驻留到伪基站小区，无法进行正常通信；此外，在上述流程一中，用户设备直接将伪基站小区的 TA 域标识或 LA 域标识加入到 forbidden 列表，限制范围过大，导致用户设备难以驻留到合法基站小区。

流程二

参见图 2，为用户设备与伪基站交互过程中出现通信异常时的交互流程。

1、用户设备被伪基站诱导，向伪基站发送附着请求消息（ATTACH_REQ）、跟踪区更新请求消息（TAU_REQ）或位置区更新请求消息（LAU_REQ）。

2、用户设备向伪基站发送无线资源控制（radio resource control，RRC）连接请求消息（RRC_CONN_REQ），请求与伪基站建立 RRC 连接。

3、伪基站向用户设备发送 RRC 连接建立消息（RRC_CONN_SETUP）。

4、用户设备向伪基站发送 RRC 连接建立完成消息（RRC_CONN_SETUP_CMPLT），以指示用户设备与伪基站间的 RRC 连接建立完成。

5、用户设备与伪基站建立 RRC 连接以后，可能出现以下通信异常情况:

a) 用户设备的底层(物理层或介质访问控制层)检测到无线链路失败(radio link failure，RLF)，上报给接入层;

b) 在步骤 4 完成后，伪基站与用户设备没有后续交互，导致 NAS 协议保护定时器超时;

c) 在步骤 4 完成后，伪基站没有以明文方式查询 IMSI，而是直接向用户设备发送 RRC 连接释放消息（RRC_CONN_RELEASE），将用户设备释放掉。

出现上述通信异常情况会导致用户设备与伪基站的 RRC 连接释放。其中，情况 a）中，由接入层触发 RRC 连接释放；情况 b）中，由 NAS 触发 RRC 连接释放；情况 c）中，由伪基站触发 RRC 连接释放。

在出现上述三种情况时，用户设备认为与伪基站的交互过程出现通信异常情况，用户设备会对出现上述通信异常情况的次数进行统计。在出现上述通信异常情况累计次数小于 5 次时，用户设备的 NAS 会重新触发用户设备在当前制式下与其他基站建立连接（即在当前制式下重新建链）；在出现上述通信异常情况累计次数达到 5 次时，用户设备的 NAS 会触发用户设备去其他制式搜网。例如，当前通信制式为长期演进（long term evolution，LTE）时，NAS 会禁用（disable）LIE，并触发用户设备去 2G 或 3G 制式搜网。

需要说明的是，用户设备在对通信异常情况进行统计时，统计的并不是在某个伪基站小区发生通信异常情况的次数，而是用户设备在多个小区上发生通信异常情况的次数之和。即，当用户设备在任一小区发生上述通信异常情况时，均将统计次数加一。

由此可以看出，在流程二中，由于用户设备统计的通信异常情况的次数是针对多个小区的累计次数，而并不是针对某一个小区进行统计的，因而即使用户设备频繁驻留到某个伪基站小区，用户设备也无法识别出伪基站小区，导致无法针对伪基站小区进行适当处理。用户设备在通信异常情况累计次数小于 5 次并重新触发建链后，由于伪基站的发射功率大于合法基站的发射功率，因而用户设备仍然大概率驻留到伪基站小区，无法进行正常通信；用户设备在通信异常情况累计次数达到 5 次时，需要禁用（disable）当前制式，去其他制式搜网，导致用户设备长时间无法回到当前制式，影响用户设备的业务速率。

综上，在上述流程一和流程二中，由于用户设备无法识别伪基站，导致用户设备无法

针对伪基站小区进行适当处理，进而导致用户设备频繁驻留到伪基站小区，影响用户设备的正常通信。

针对以上问题，本申请实施例提供一种伪基站识别方法及装置，用以识别伪基站，从而采取相应处理，避免用户设备频繁驻留到伪基站小区，导致用户设备无法进行正常通信。

下面，对本申请实施例的应用场景加以介绍。

本申请实施例可应用于图 3 所示的通信系统中。该通信系统中包含用户设备和基站。该基站可以是伪基站，也可以是合法基站。用户设备在与基站建立 RRC 连接后，可采用本申请实施例提供的方案识别该基站是否为伪基站，并针对识别出的伪基站采取相应处理，从而避免用户设备频繁驻留到伪基站小区，影响用户设备的正常通信。

其中，基站可以是码分多址接入（code division multiple access，CDMA）中的网络设备（base transceiver station，BTS），也可以是带宽码分多址接入（wide-band code division multiple access，WCDMA）或时分同步码分多址（time division-synchronous code division multiple access，TD-SCDMA）中的网络设备（NodeB），还可以是长期演进（long term evolution，LTE）系统中的演进型网络设备（evolutional node B，eNB 或 e-NodeB）、5G 网络架构（next generation system）中的 5G 基站，也可是家庭演进基站（home evolved node B，HeNB）、家庭基站（femto）、微微基站（pico）等，本申请实施例中对基站的类型不做具体限定。

本申请实施例中的用户设备可以是向用户提供语音和/或数据连通性的设备，对应无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。用户设备可以经无线接入网（radio access network，RAN）与一个或多个核心网进行通信，用户设备可以是移动终端，如移动电话（或称为“蜂窝”电话）和对应移动终端的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。例如，个人通信业务（personal communication service，PCS）电话、无绳电话、会话发起协议（session initiated protocol，SIP）话机、无线本地环路（wireless local loop，WLL）站、个人数字助理（personal digital assistant，PDA）等设备。终端设备也可以称为系统、订户单元（subscriber unit）、订户站（subscriber station），移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point）、远程终端（remote terminal）、接入终端（access terminal）、用户终端（user terminal）、用户代理（user agent）或用户装备（user equipment），本申请实施例中并不限定。

本申请实施例中，用户设备的通信制式包括但不限于 CDMA、WCDMA、TD-SCDMA、LTE、5G 等。

下面，结合附图对本申请实施例提供的伪基站识别方案进行详细介绍。

本申请实施例提供一种伪基站识别方法及装置，用以识别伪基站，从而采取相应处理，避免用户设备频繁驻留到伪基站小区，导致用户设备无法进行正常通信。其中，方法和装置是基于同一发明构思的，由于方法及装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。

需要说明的是，本申请实施例中，多个是指两个或两个以上。另外，需要理解的是，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示

或暗示相对重要性，也不能理解为指示或暗示顺序。

参见图 4，为本申请实施例提供的一种伪基站识别方法。该方法包括如下步骤：

S401：用户设备与当前驻留的第一小区所属的第一基站建立 RRC 连接。

其中，用户设备与第一基站建立 RRC 连接的过程可参见前述流程一中的步骤 1~步骤 4，此处不再赘述。

此外，需要说明的是，第一基站为第一小区所属的基站。但是，本申请实施例中对第一基站管理的小区的数量不做具体限定，第一基站管理的小区的数量可以为一个，即第一小区；第一基站管理的小区的数量也可以为多个，第一小区为多个小区中的一个。

特别地，当第一基站为伪基站时，第一基站管理的所有小区均可视为伪基站小区；当第一基站为合法基站时，第一基站管理的所有小区均可视为合法基站小区。

S402：用户设备接收第一基站发送的第一请求消息，第一请求消息用于请求查询用户设备的 IMSI。

由 S402 可以看出，在用户设备与第一基站建立连接后，第一基站不再触发后续的鉴权操作，而是直接向用户设备发送请求获取用户设备的 IMSI 的第一请求消息。

具体地，第一基站可以以明文方式发送第一请求消息。示例性地，第一请求消息可以是前述身份识别请求消息（IDENFITY_REQ）。

S403：用户设备记录第一标识。其中，第一标识用于指示第一基站请求查询用户设备的 IMSI。具体地，可以由用户设备中的 NAS 记录该第一标识。

S404：用户设备向第一基站发送第一响应消息，第一响应消息用于指示用户设备的 IMSI。

S405：用户设备接收第一基站发送的 RRC 连接释放指示。

在用户设备接收第一基站发送的 RRC 连接释放指示之后，且用户设备记录有第一标识时，用户设备可确定第一基站为伪基站。那么，用户设备可根据用户设备的配置将第一小区的域标识加入第二受限列表，第一小区的域标识为第一小区的 LA 域标识或 TA 域标识，第二受限列表用于指示用户设备禁止驻留在第二受限列表中记录的域标识所对应的小区。

示例性地，若第一小区为 4G 小区，则用户设备可根据用户设备的配置将第一小区的 TA 域标识加入受限列表；若第一小区为 3G 小区，则用户设备可根据用户设备的配置将第一小区的 LA 域标识加入受限列表。

其中，第二受限列表可视为前述 forbidden 列表。用户设备的 NAS 可维护有第二受限列表。第二受限列表中记录有域标识，用于指示用户设备禁止驻留在记录的域标识所对应的小区。可选地，NAS 可将第二受限列表下发给 RRC 层以指导 RRC 层选网。

在上述实现方式中，用户设备在接收到第一基站发送的 RRC 连接释放指示之后，且用户设备记录有第一标识时，可以确定第一基站为伪基站。因而用户设备可根据用户设备的配置决定是否将第一小区的域标识加入第二受限列表。若将第一小区的域标识加入第二受限列表，可禁止用户设备驻留在第一小区的域标识所对应的小区内。

需要说明的是，第一小区的域标识所对应的是同一个跟踪区或位置区的所有小区，即第一小区的域标识所对应的小区并不限定为第一小区，也可以是其他伪基站小区或者合法基站小区。采用这种实现方式，可以避免用户设备再次驻留在第一小区的域标识对应的小区。但是，如前所述，若合法基站小区的域标识与第一小区的域标识相同，采用这种实现

方式会导致限制范围过大，导致用户设备无法驻留到该合法基站小区。

因此，为了避免限制范围过大（即伪基站的 TA 或 LA 与合法基站相同，导致用户设备无法驻留到该合法基站小区）的问题，本申请实施例中，执行 S405 之后，也可根据用户设备的配置，选择不将第一小区的域标识加入第二受限列表。

S406：用户设备在接收到 RRC 连接释放指示后、且确认记录有第一标识时，确定第一基站为伪基站。

根据前面的描述，在伪基站与用户设备的交互流程中，伪基站在与用户设备建立连接后，不再触发后续的鉴权操作，而是直接向用户设备发送查询 IMSI 的请求消息。因而，本申请实施例中，在用户设备与伪基站建立后，若伪基站在未触发鉴权操作的情况下直接向用户设备发送第一请求消息，则用户设备记录第一标识。在 S405 用户设备接收到第一基站发送的 RRC 连接释放指示之后，用户设备查看是否记录有第一标识，并在用户设备中记录有第一标识的情况下，确定第一基站为伪基站。

在确定第一基站为伪基站之后，用户设备可将第一小区的小区信息加入第一受限列表，该第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区。

其中，第一受限列表也可以称为小区受限列表或者 bar 列表。用户设备的 RRC 层可维护有第一受限列表。第一受限列表中记录有小区信息，用于指示用户设备禁止驻留在记录的小区信息所对应的小区。

具体地，可以由用户设备的 RRC 层将第一小区的小区信息加入第一受限列表。第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的物理小区标识（physical cell ID，PCI）、第一小区的 E-UTRA 绝对无线频率信道号（E-UTRA absolute radio frequency channel number，EARFCN）。

需要说明的是，第一小区的小区信息不限于上述几种，只要该第一小区的小区信息可用于标识第一小区即可。

在上述实现方式中，第一受限列表与前述第二受限列表（forbidden 列表）不同。第一受限列表中记录的是第一小区的小区信息，即通过将第一小区的小区信息加入第一受限列表，可以禁止用户设备驻留在第一小区（或者说与第一小区的小区信息相同的小区，例如与第一小区频点相同的小区），但是对其他小区并不做禁止。而第二受限列表中记录的是域标识（例如 TA 域标识或 LA 域标识），通过将第一小区的域标识加入第二受限列表，会禁止用户设备驻留在该域标识对应的小区。而一个域标识通常对应一个大的位置区或跟踪区内的多个基站（包括伪基站和合法基站），将第一小区的域标识加入第二受限列表，不仅会禁止用户设备驻留在伪基站小区，还会导致用户设备无法驻留到合法基站小区。也就是说，第一受限列表的限制范围较第二受限列表而言，限制范围更小。

采用上述方案，可以在识别第一基站为伪基站后，将第一小区的小区信息加入第一受限列表，从而避免用户设备再次驻留在第一小区这一伪基站小区，导致用户设备难以进行正常通信。此外，采用上述方案仅禁止用户设备驻留到第一小区，对第一小区之外的小区并无限制，因而可以避免限制范围过大导致合法基站小区被禁止驻留的现象。

此外，在用户设备将第一小区的小区信息加入第一受限列表之后，还可进行小区搜索；然后，用户设备可根据小区搜索结果驻留到第二小区，第二小区的小区信息未记录在上述第一受限列表中。

也就是说，将第一小区的小区信息加入第一受限列表之后，用户设备在重新进行小区搜索时，需要将第一受限列表中的小区剔除，只有在搜索到第一受限列表之外的可用小区时，才选择驻留到该小区。

采用上述方案，用户设备可重新进行搜网，从而使得用户设备可以驻留到合法基站小区，进行正常通信。

当然，需要说明的是，在图 4 所示方法中，仅限定第二小区的小区信息未记录在第一受限列表中，对第二小区的类型不做具体限定。示例性地，第二小区可以是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，第二小区可以是属于另一个伪基站的、未记录在第一受限列表中的小区，第二小区也可以是属于合法基站的小区。

若第二小区是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，或者第二小区是属于另一个伪基站的、未记录在第一受限列表中的小区，那么，用户设备可通过执行上述 S401~S405 判断第二小区为伪基站小区，进而将第二小区的小区信息也加入第一受限列表，用户设备在再次搜网时则不会再次驻留到第二小区。若第二小区是属于合法基站的小区，则用户设备在驻留到第二小区后，可与第二小区对应的基站进行正常通信。

也就是说，通过本申请实施例提供的方案，可以准确地识别出伪基站（伪基站小区）。在将伪基站小区加入第一受限列表中之后，用户设备不会再次驻留该伪基站小区，可以避免用户设备频繁驻留同一个伪基站小区。但是，对于之前没有驻留过的伪基站小区，用户设备只有在执行上述步骤 S401~S405 之后才可判断该基站为伪基站，并将该小区的小区信息加入第一受限列表。

此外，用户设备在进行小区重选评估、测量评估、回复其他制式测量结果时，都可以将第一受限列表中的伪基站小区剔除，避免频繁发起与伪基站小区间的互操作。

根据前述用户设备与伪基站交互的流程一可以知道，伪基站在与用户设备建立 RRC 连接后，不触发后续的鉴权操作，而是直接向用户设备发送查询 IMSI 的请求消息，并在接收到用户设备发送的携带 IMSI 的响应消息后主动释放链路。因此，在图 4 所示的伪基站识别方法中，与第一基站建立 RRC 连接后，用户设备在第一基站未触发鉴权而直接发送第一请求消息时记录第一标识。在第一基站主动释放链路后，用户设备在记录有第一标识的情况下可以确定第一基站为伪基站。

此外，依据图 4 所示的伪基站识别方法，该方法还可能有另外一种实现方式。在用户设备与第一基站建立 RRC 连接后，用户设备并未收到第一基站发送的第一请求消息，那么用户设备中也就未记录第一标识。后续，若用户设备接收到第一基站发送的 RRC 连接释放指示，则用户设备确定第一基站不是伪基站，此时用户设备可根据当前协议（3GPP TS 24.301，5.5.1.2.5）的要求将第一小区的域标识加入第三受限列表，该第三受限列表用于指示用户设备禁止驻留在受限列表中记录的域标识所对应的小区。在将第一小区的域标识加入第三受限列表后，用户设备可重新进行搜网。

其中，第三受限列表与前述第二受限列表可以是同一列表。

在上述实现方式中，第一基站在与用户设备建立连接后，并未触发后续的鉴权操作。但是，第一基站也未请求查询用户设备的 IMSI，因而用户设备中并未记录第一标识。在用户设备接收到第一基站发送的 RRC 连接释放指示后，由于第一基站与用户设备的交互流程并不符合前述流程一，因而用户设备判断第一基站并不是伪基站。

结合以上描述，在该实现方式中，第一基站在与用户设备建立 RRC 连接后，并未执行任何操作，而是直接将链路释放。在这种情况下，第一基站是合法基站，第一小区可能是属于第一基站的一个坏小区。

基于同一发明构思，本申请实施例还提供另一种伪基站识别方法，该方法可视为图 4 所示方法的一个具体示例。参见图 5，该方法包括如下步骤：

【1】用户设备搜网、本制式内互操作（例如重选、重定向、小区变更命令）、制式间互操作（例如重选、重定向、小区变更命令）等方式驻留到伪基站小区。

【2】用户设备的 NAS 向 RRC 层发送附着请求消息（ATTACH_REQ）/跟踪区更新请求消息（TAU_REQ）/位置区更新请求消息（LAU_REQ）。

【3】用户设备的 RRC 层根据 NAS 的指示与伪基站建立 RRC 连接。

其中，RRC 层与伪基站建立 RRC 连接的过程可参考前述流程一中的步骤 1~步骤 4（即图 1 中的步骤 1~步骤 4）。

【4】伪基站在未触发鉴权操作的情况下，直接以明文方式向用户设备发送身份识别请求消息，以查询用户设备的 IMSI。

其中，身份识别请求消息可视为图 4 所示方法中的第一请求消息的一个具体示例。

【5】NAS 记录明文查询 IMSI 标识。

其中，明文查询 IMSI 标识可视为图 4 所示方法中的第一标识的一个具体示例。

【6】NAS 向伪基站发送身份识别响应消息，其中携带用户设备的 IMSI。

其中，身份识别响应消息可视为图 4 所示方法中的第一响应消息的一个具体示例。

【7】伪基站向用户设备发送附着拒绝消息/跟踪区更新拒绝消息/位置区更新拒绝消息。

其中，附着拒绝消息/跟踪区更新拒绝消息/位置区更新拒绝消息中可携带拒绝原因值 #13 或#15。

【8】NAS 根据用户配置决定是否将当前小区的 TA/LA 加入第二受限列表。

【9】NAS 向 RRC 层指示当前小区为伪基站小区，即指示与用户设备建立 RRC 连接的基站为伪基站。

其中，NAS 在判断用户设备中存在明文查询 IMSI 标识后，确定当前建立连接的基站为伪基站，并将确定结果指示给 RRC 层。

【10】RRC 层根据 NAS 的指示将当前小区加入第一受限列表。

具体地，第一受限列表中可记录当前小区的小区信息，例如当前小区的小区频点、当前小区的小区频段、当前小区的 PCI、当前小区的 EARFCN。将当前小区的小区信息加入第一受限列表后，可以避免用户设备再次驻留到当前小区。

【11】用户设备重新进行小区搜索。

用户设备在重新进行小区搜索时，需要剔除第一受限列表中的小区。

【12】用户设备在搜网到第一受限列表以外的可用小区时，用户设备选择驻留到该小区，该小区为合法基站的小区。

其中，步骤【12】中用户设备驻留的小区可视为图 4 所示方法中的第二小区的一个具体示例。需要说明的是，用户设备在执行步骤【12】后，也可能驻留到另一个伪基站小区，在这种情况下，用户设备通过执行图 5 所示方法可判断出驻留到伪基站小区这一情况，进

而将该小区也加入第一受限列表，避免再次驻留该伪基站小区。在图 7 所示方法中仅以步骤【12】驻留的小区为合法基站小区为例进行示意。

需要说明的是，图 5 所示方法可视为图 4 所示方法的一个具体示例。图 5 所示方法中未详尽描述的实现方式及技术效果可参见图 4 所示方法中的相关描述。

此外，本申请实施例还提供一种伪基站识别方法。参见图 6，该方法包括如下步骤：

S601：用户设备与当前驻留的第一小区所属的第一基站建立 RRC 连接。

其中，用户设备与第一基站建立 RRC 连接的过程可参见前述流程二中的步骤 1~步骤 4，此处不再赘述。

此外，需要说明的是，第一基站为第一小区所属的基站。但是，本申请实施例中对第一基站管理的小区的数量不做具体限定，第一基站管理的小区的数量可以为一个，即第一小区；第一基站管理的小区的数量也可以为多个，第一小区为多个小区中的一个。

特别地，当第一基站为伪基站时，第一基站管理的所有小区均可视为伪基站小区；当第一基站为合法基站时，第一基站管理的所有小区均可视为合法基站小区。

S602：用户设备统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数。

具体地，可以由用户设备的 NAS 记录用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数。

此外，通信异常情况的含义与前述用户设备与伪基站的交互流程二中所述的“通信异常情况”相同。即，通信异常情况可以包括但不限于为：

1、执行 S601 后，伪基站与用户设备没有后续交互，用户设备的 NAS 协议保护定时器超时；

2、用户设备的物理层或媒体访问控制（media access control，MAC）（也可以称为层 2 或 L2）向 RRC 层上报 RLF；

3、在执行 S601 之后，第一基站在未请求查询用户设备的 IMSI 的情况下，即向用户设备发送 RRC 连接释放指示，将用户设备释放掉。

在出现上述通信异常情况下，用户设备与第一基站之间的 RRC 连接释放。其中，对于 NAS 协议保护定时器超时以及底层（物理层或 L2）上报 RLF 的情况，用户设备会主动释放与第一基站之间的 RRC 连接；对于第一基站在未请求查询 IMSI 的情况下即发送 RRC 连接释放指示的情况，第一基站主动释放与用户设备之间的 RRC 连接。

需要注意的是，本申请实施例中在统计异常情况次数时与前述流程二的不同之处在于前述流程二中，用户设备在对通信异常情况进行统计时，统计的是用户设备在多个小区上发生通信异常情况的次数之和。而 S602 中，用户设备统计的是用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数。

也就是说，本申请实施例中，用户设备会分别针对不同小区上因上述通信异常情况导致 RRC 连接释放的次数进行统计。例如，用户设备开机后，驻留到小区 1，在小区 1 上因上述通信异常情况导致 RRC 连接释放，则用户设备记录小区 1 对应的次数为 1；然后，用户设备重新搜网后驻留到小区 2，又因上述通信异常情况导致 RRC 连接释放，则用户设备记录小区 2 对应的次数为 1；接着，用户设备重新搜网后再次驻留到小区 1，又因上述通信异常情况导致 RRC 连接释放，则用户设备记录小区 1 对应的次数为 2。

针对不同小区分别统计因通信异常情况导致 RRC 连接释放的次数，可以识别出用户设备是否频繁驻留到同一小区且发生通信异常情况，从而针对该小区进行相应处理，避免用户设备再次驻留到该小区。

由于本申请实施例中需针对不同小区分别统计因通信异常情况导致 RRC 连接释放的次数，因而在用户设备与第一基站建立 RRC 连接之前，用户设备可保存当前驻留小区的小区信息，在后续出现通信异常情况时，用户设备可判断该通信异常情况发生在哪个小区，并针对不同小区分别统计次数。

即，在用户设备执行 S601 与第一小区所属的第一基站建立 RRC 连接之前，用户设备可保存第一小区的小区信息，第一小区的小区信息用于指示用户设备当前驻留的小区为第一小区。那么，用户设备在执行 S602 统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数时，可统计记录的小区信息指示的第一小区上因通信异常情况导致 RRC 连接释放的次数。

其中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的 PCI、第一小区的 EARFCN。

采用上述方案，在用户设备与第一基站建立 RRC 连接之前，用户设备可保存当前驻留小区的小区信息，在后续出现通信异常情况时，用户设备可判断该通信异常情况发生在哪个小区，并针对不同小区分别统计次数。

S603：用户设备在该次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区。

其中，该第一阈值可以为小于 5 的数值。也就是说，在用户设备根据现有协议在出现通信异常情况累计达到 5 次而去其他制式搜网之前，即确定第一基站为伪基站或者第一小区为坏小区并进行相应处理，使得用户设备能尽快尝试其他小区，避免用户设备因频繁驻留伪基站小区导致去其他制式搜网、长时间无法回到当前制式。

此外，在 S603 中判断在第一小区上因通信异常情况导致 RRC 连接释放的次数是否大于第一阈值之前，还可参照现有协议，判断用户设备在各个小区上因通信异常情况导致 RRC 连接释放的次数是否达到 5 次。若达到 5 次，则触发用户设备去其他制式搜网；若未达到 5 次，则可执行 S602 判断在第一小区上因通信异常情况导致 RRC 连接释放的次数是否大于第一阈值。

当用户设备判断在第一小区上因通信异常情况导致 RRC 连接释放的次数大于第一阈值时，用户设备可确定第一基站为伪基站（即第一小区为伪基站小区）或者第一小区为坏小区。其中，坏小区包括但不限于基站发射功率较低的小区、掉话率较高的小区、拥塞程度较高的小区、切换成功率较低的小区或者无线接通率较低的小区。

也就是说，用户设备当前驻留的第一小区为伪基站小区或坏小区时，均会导致用户设备在第一小区上发生多次通信异常情况。

在用户设备确定第一基站为伪基站或者第一小区为坏小区之后，用户设备还可将第一小区的小区信息加入第一受限列表，第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区。然后，用户设备进行小区搜索；若用户设备未搜索到其他可用小区，则用户设备将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区；若用户设备搜索到第二小区为可用小区，则用户设备驻留第二小区，第二小区的小区信息未记录在第一受限列表中。

其中，第一受限列表也可以称为小区受限列表或者 bar 列表。用户设备的 RRC 层可维护有第一受限列表。第一受限列表中记录有小区信息，用于指示用户设备禁止驻留在记录的小区信息所对应的小区。可选地，NAS 可将第二受限列表下发给 RRC 层以指导 RRC 层选网。

此外，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的 PCI、第一小区的 EARFCN。

当然，需要说明的是，在图 6 所示的方案中，仅限定第二小区的小区信息未记录在第一受限列表中，对第二小区的类型不做具体限定。示例性地，第二小区可以是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，第二小区可以是属于另一个伪基站的、未记录在第一受限列表中的小区，第二小区也可以是属于合法基站的小区。

若第二小区是属于第一基站（伪基站）的、未记录在第一受限列表中的另一个小区，或者，第二小区是属于另一个伪基站的、未记录在第一受限列表中的小区，那么用户设备可通过执行上述 S601~S603 判断第二小区为伪基站小区或坏小区，进而将第二小区的小区信息也加入第一受限列表，用户设备在再次搜网时则不会再次驻留到第二小区。若第二小区是属于合法基站的小区，则用户设备在驻留到第二小区后，可与第二小区对应的基站进行正常通信。

也就是说，通过图 6 所示方案，可以准确地识别出伪基站小区或坏小区。在将伪基站小区或坏小区加入第一受限列表中之后，用户设备不会再次驻留该小区，可以避免用户设备频繁驻留同一个伪基站小区或坏小区。但是，对于之前没有驻留过的伪基站小区或坏小区，用户设备只有在执行上述步骤 S601~S603 之后才可判断当前驻留小区为伪基站小区或坏小区，并将该小区的小区信息加入第一受限列表。

采用上述实现方式，由于用户设备在重新进行搜网时需要剔除第一受限列表中的小区，因而将第一小区的小区信息加入第一受限列表，可以避免用户设备再次驻留到第一小区。后续，用户设备可重新进行小区搜索，并驻留到第二小区。此外，若用户设备重新进行小区搜索后未搜索到可用小区，则用户设备当前无可驻留小区，那么，用户设备可将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区。

此外，用户设备在进行小区重选评估、测量评估、回复其他制式测量结果时，都可以将第一受限列表中的伪基站小区剔除，避免频繁发起与伪基站小区间的互操作。

需要说明的是，在确定第一基站为伪基站或第一小区为坏小区之后，将第一小区的小区信息加入第一受限列表。由于此时还未确定第一小区为伪基站小区还是坏小区，因而可将第一小区的受限类型设置为“搜不到网解受限”，即后续用户设备在未搜索到其他可用小区时，还可将第一小区的小区信息从第一受限列表中删除，从而避免用户设备在当前制式下无可用小区。例如，若第一小区为坏小区，在用户设备未搜索到其他可用小区后将第一小区的小区信息从第一受限列表中删除，那么，用户设备仍可驻留在第一小区，待第一小区恢复后即可在当前制式下与第一基站进行正常通信。

为了进一步判断第一小区是伪基站小区还是坏小区，还需结合用户设备与第一基站的其他交互流程。下面介绍一种进一步判断第一小区是伪基站小区还是坏小区的方式。

在用户设备与第一小区所属的第一基站建立 RRC 连接之前，用户设备可在确定第一基站的系统消息配置异常时保存类伪基站配置标识，该类伪基站配置标识用于指示第一基站的系统消息配置异常。那么，在第一小区上因通信异常情况导致 RRC 连接释放的次数

大于第一阈值、且用户设备中保存有类伪基站配置标识时，用户设备即可确定第一基站为伪基站。

其中，用户设备在以下信息中的至少一种满足时，确定第一基站的系统消息配置异常：用户设备确定第一基站配置在共享公共陆地移动网络（public land mobile network，PLMN）列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识；用户设备确定第一基站的驻留门限低于用户设备配置的驻留门限阈值；用户设备确定第一基站未配置异频邻区和异系统邻区；用户设备确定第一基站配置 GSM 邻区的优先级为高重选优先级。

在进行系统消息配置时，合法基站和伪基站的配置会有所不同。

比如，第一基站在进行系统消息配置时，会向用户设备下发共享 PLMN 列表，以指示用户设备的 PLMN 标识为该列表中的任一个时，用户设备均可与第一基站建立 RRC 连接。而用户设备中也维护有一个 PLMN 列表，该列表指示哪些 PLMN 不可由一个基站共享，例如移动运营商的 PLMN1 和电信运营商的 PLMN2 不可被一个基站共享。用户设备在收到第一基站下发的共享 PLMN 列表后，可以将该共享 PLMN 列表与自身维护的 PLMN 列表比照，若该共享 PLMN 列表中包含至少两个不可被一个基站共享的 PLMN，则用户设备认为该基站为伪基站。这是因为：伪基站通常会将多个运营商的 PLMN 标识配置在一个共享 PLMN 列表中，以诱导更多的用户设备与自身建立 RRC 连接。

比如，合法基站会配置异频邻区和/或异系统邻区，而伪基站通常不会配置异频邻区和异系统邻区。

比如，伪基站配置的驻留门限通常较低，使得基的发射功率较低时，用户设备根据该伪基站的驻留门限判断时也能判断满足驻留条件，以诱导用户设备驻留，而合法基站配置的驻留门限通常高于伪基站配置的驻留门限。

再比如，伪基站通常会将 GSM 邻区配置为高重选优先级。这是因为：GSM 没有双向鉴权，用户设备驻留在 GSM 伪基站小区上的危害更大（用户隐私泄露、发送垃圾短信）。伪基站通常将 GSM 邻区配置为高重选优先级，可以让用户设备更易重选到 GSM 伪基站小区。且现网中合法基站通常将 GSM 邻区配置为低重选优先级，避免重选到速率较低的 GSM 小区。

在上述实现方式中，可以通过识别第一基站的系统消息配置是否体现有伪基站的系统消息配置的特点，来判断第一基站是否为伪基站。即，通过第一基站的系统消息配置情况可判断第一基站是否为伪基站。

此外，在将第一小区的小区信息加入第一受限列表时，若已经确定第一基站为伪基站，则可将受限类型设置为“搜不到网不解受限”，即后续用户设备在未搜索到其他可用小区时，也不可将第一小区的小区信息从第一受限列表中删除，从而避免用户设备再次驻留在伪基站小区。通常，在用户设备未搜索到可用小区时，用户设备可禁用当前制式，去其他制式搜网。

此外，在图 6 所示的伪基站识别方法中，若确定第一基站为伪基站，那么，在确定第一基站为伪基站之后，用户设备可获取用于指示用户设备当前位置的第一位置信息；在用户设备将第一小区的小区信息加入第一受限列表之后，用户设备可再次获取用于指示用户设备当前位置的第二位置信息。然后，用户设备在第一位置信息指示的位置与第二位置信

息指示的位置之间的距离大于第二阈值时，将第一小区的小区信息从第一受限列表中删除。

可选地，用户设备可在确定第一基站为伪基站或第一小区为坏小区之后，保存获取的第一位置信息；之后，实时测量（例如周期性测量）用户设备的当前位置（第二位置），并与第一位置信息指示的位置进行比较。当获取到的当前位置（第二位置）与第一位置信息指示的位置的距离之差大于第二阈值时，将第一小区的小区信息从第一受限列表中删除。

其中，用户设备在获取第一位置信息或第二位置信息时，可通过卫星定位、设备到设备（device-to-device，D2D）、车辆外联（vehicle to everything，V2X）、小区测量等方式获取。测量操作可以由用户设备的 NAS 执行，也可以由 RRC 层执行。

通常，伪基站模拟合法基站的配置（例如，伪基站的小区频点与合法基站的小区频点相同），并通过在一定范围内提高发射功率来诱导用户设备驻留。其中，“一定范围”通常小于合法基站小区的覆盖范围。也就是说，当用户设备离开伪基站提高发射功率的“一定范围”后，用户设备即可接收到合法基站的信号，正常进行业务。

在上述实现方式中，可在确定第一基站为伪基站之后记录伪基站当前的第一位置，并在将第一小区的小区信息加入第一受限列表之后，不断测量（例如周期性测量）用户设备的当前位置（第二位置）并与第一位置信息指示的位置进行比较。在第二位置与第一位置的距离之差大于第二阈值时，即可判断用户设备离开伪基站小区的覆盖范围，此时可将第一小区的小区信息从第一受限列表中删除，从而使得用户设备可以驻留在与伪基站有相同配置的合法基站。

根据前述用户设备与伪基站交互的流程二可以知道，伪基站在与用户设备建立 RRC 连接后，会因通信异常情况导致用户设备与伪基站的 RRC 连接释放。此外，若用户设备当前驻留小区为坏小区时，也可能发生上述通信异常情况。因此，在图 6 所示的伪基站识别方法中，与第一基站建立 RRC 连接后，用户设备通过判断在第一小区上因通信异常情况导致 RRC 连接释放的次数是否大于第一阈值，可以确定第一基站为伪基站或者第一小区为坏小区。

基于同一发明构思，本申请实施例还提供以下三种伪基站识别方法，这三种方法均可视为图 6 所示方法的一个具体示例。

方法一

参见图 7，该方法包括如下步骤:

【1】用户设备搜网、本制式内互操作（例如重选、重定向、小区变更命令）、制式间互操作（例如重选、重定向、小区变更命令）等方式驻留到伪基站小区。

【2】用户设备的 NAS 记录当前驻留的第一小区的小区信息。

【3】用户设备的 NAS 向 RRC 层发送附着请求消息（ATTACH_REQ）/跟踪区更新请求消息（TAU_REQ）/位置区更新请求消息（LAU_REQ）。

【4】用户设备的 RRC 层根据 NAS 的指示与伪基站建立 RRC 连接

其中，RRC 层与伪基站建立 RRC 连接的过程可参考前述流程二中的步骤 1~步骤 4（即图 2 中的步骤 1~步骤 4）。

【5】用户设备发生以下三种通信异常情况之一时，将 NAS 尝试次数进行+1 处理，其

中，NAS 尝试次数可视为用户设备在各个小区上因通信异常情况导致 RRC 连接释放的次数:

【5-1】当前基站在未请求查询用户设备的 IMSI 的情况下，即向用户设备发送 RRC 连接释放指示，将用户设备释放掉;

【5-2】在当前基站未请求查询用户设备的 IMSI 的情况下，NAS 协议保护定时器超时;

【5-3】在当前基站未请求查询用户设备的 IMSI 的情况下，用户设备的底层向 RRC 层上报 RLF;

【6】判断 NAS 尝试次数是否达到 5 次；若达到 5 次，则执行步骤【7】；若未达到 5 次，则执行步骤【8】。

其中，该 NAS 尝试次数是指 NAS 在所有小区上的 NAS 尝试次数之和。

【7】禁用当前制式并去其他制式搜网。

【8】判断在第一小区上的 NAS 尝试次数是否达到配置次数。若是，则执行步骤【10】；若否，则执行步骤【9】。

其中，该配置次数可视为图 6 所示方法中第一阈值的一个具体示例。

【9】NAS 重新进行尝试，执行上述步骤【1】~【5】。

【10】NAS 向 RRC 层指示第一小区为伪基站小区或坏小区。

【11】RRC 层将第一小区加入第一受限列表中，并将受限类型设置为“搜不到网解受限”。

其中，第一小区的受限类型可以设置为“搜不到网解受限”。“搜不到网解受限”的含义可以是：若用户设备重新进行搜网时未搜索到其他可用小区，则将第一小区从第一受限列表中删除。

【12】RRC 层判断是否能搜索到其他可用小区。若是，则执行步骤【13】；若否，则执行步骤【14】。

【13】用户设备在搜网到第一受限列表以外的可用小区时，用户设备选择驻留到该小区，该小区为合法基站的小区。

其中，步骤【13】中用户设备驻留的小区可视为图 6 所示方法中的第二小区的一个具体示例。需要说明的是，用户设备在执行步骤【13】后，也可能驻留到另一个伪基站小区或坏小区，在这种情况下，用户设备通过执行图 7 所示方法可判断出驻留到伪基站小区或坏小区这一情况，进而将该小区也加入第一受限列表，避免再次驻留该小区。在图 7 所示方法中仅以步骤【13】驻留的小区为合法基站小区为例进行示意。

【14】用户设备未搜索到其他可用小区，将第一小区从第一受限列表中删除

【15】用户设备重新驻留到第一小区。

需要说明的是，图 7 所示方法可视为图 6 所示方法的一个具体示例。图 7 所示方法中未详尽描述的实现方式及技术效果可参见图 6 所示方法中的相关描述。

方法二

参见图 8，该方法包括如下步骤:

【1】用户设备搜网、本制式内互操作（例如重选、重定向、小区变更命令）、制式间互操作（例如重选、重定向、小区变更命令）等方式驻留到伪基站小区。

【2】用户设备的 NAS 记录当前驻留的第一小区的小区信息。

【3】用户设备的 NAS 向 RRC 层发送附着请求消息（ATTACH_REQ）/跟踪区更新请

求消息（TAU_REQ）/位置区更新请求消息（LAU_REQ）。

【4】用户设备的 RRC 层根据 NAS 的指示与伪基站建立 RRC 连接

其中，RRC 层与伪基站建立 RRC 连接的过程可参考前述流程二中的步骤 1~步骤 4（即图 2 中的步骤 1~步骤 4）。

【5】用户设备发生以下三种通信异常情况之一时，将 NAS 尝试次数进行+1 处理，其中，NAS 尝试次数可视为用户设备在各个小区上因通信异常情况导致 RRC 连接释放的次数：

【5-1】当前基站在未请求查询用户设备的 IMSI 的情况下，即向用户设备发送 RRC 连接释放指示，将用户设备释放掉；

【5-2】在当前基站未请求查询用户设备的 IMSI 的情况下，NAS 协议保护定时器超时；

【5-3】在当前基站未请求查询用户设备的 IMSI 的情况下，用户设备的底层向 RRC 层上报 RLF；

【6】判断 NAS 尝试次数是否达到 5 次；若达到 5 次，则执行步骤【7】；若未达到 5 次，则执行步骤【8】。

其中，该 NAS 尝试次数是指 NAS 在所有小区上的 NAS 尝试次数之和。

【7】禁用当前制式并去其他制式搜网。

【8】判断在第一小区上的 NAS 尝试次数是否达到配置次数。若是，则执行步骤【10】；若否，则执行步骤【9】。

其中，该配置次数可视为图 6 所示方法中第一阈值的一个具体示例。

【9】NAS 重新进行尝试，执行上述步骤【1】~【5】。

【10】NAS 向 RRC 层指示第一小区可能为伪基站小区。

【11】用户设备通过卫星定位、D2D、V2X、小区测量等方式记录用户设备当前的第一位置。

【12】RRC 层将第一小区加入第一受限列表中，并将受限类型设置为“搜不到网解受限”。

其中，第一小区的受限类型可以设置为“搜不到网解受限”。“搜不到网解受限”的含义可以是：若用户设备重新进行搜网时未搜索到其他可用小区，则将第一小区从第一受限列表中删除。

【13】用户设备通过卫星定位、D2D、V2X、小区测量等方式记录用户设备当前的第二位置。

【14】NAS 判断第二位置与第一位置的距离之差是否大于预设距离范围。若是，则执行步骤【15】；若否，则返回执行步骤【13】。

其中，预设距离范围为可以视为图 6 所示方法中第二阈值的一个具体示例。

【15】NAS 向 RRC 层指示用户设备离开伪基站小区。

此外，步骤【14】中判断第二位置与第一位置的距离之差的操作也可以由 RRC 层执行，这样的话，步骤【15】中 RRC 层则可自主判断用户设备离开伪基站小区。

【16】将第一小区从第一受限列表中删除。

【17】用户设备重新驻留到第一小区。

此外，NAS 执行步骤【14】和步骤【15】的同时，RRC 可执行如下步骤【18】：

【18】RRC 层判断是否能搜索到其他可用小区。若是，则执行步骤【19】；若否，则

执行步骤【16】~步骤【17】。

【19】用户设备在搜网到第一受限列表以外的可用小区时，用户设备选择驻留到该小区，该小区为合法基站的小区。

其中，步骤【19】中用户设备驻留的小区可视为图 6 所示方法中的第二小区的一个具体示例。需要说明的是，用户设备在执行步骤【19】后，也可能驻留到另一个伪基站小区或坏小区，在这种情况下，用户设备通过执行图 7 所示方法可判断出驻留到伪基站小区或坏小区这一情况，进而将该小区也加入第一受限列表，避免再次驻留该小区。在图 7 所示方法中仅以步骤【19】驻留的小区为合法基站小区为例进行示意。

需要说明的是，图 8 所示方法可视为图 6 所示方法的一个具体示例。图 8 所示方法中未详尽描述的实现方式及技术效果可参见图 6 所示方法中的相关描述。

方法三

参见图 9，该方法包括如下步骤:

【1】用户设备搜网、本制式内互操作（例如重选、重定向、小区变更命令）、制式间互操作（例如重选、重定向、小区变更命令）等方式驻留到伪基站小区。

【2】RRC 层判断系统消息配置是否异常。并在系统消息配置异常时保存类伪基站配置标识。

【3】用户设备的 NAS 记录当前驻留的第一小区的小区信息。

【4】用户设备的 NAS 向 RRC 层发送附着请求消息（ATTACH_REQ）/跟踪区更新请求消息（TAU_REQ）/位置区更新请求消息（LAU_REQ）。

【5】用户设备的 RRC 层根据 NAS 的指示与伪基站建立 RRC 连接

其中，RRC 层与伪基站建立 RRC 连接的过程可参考前述流程二中的步骤 1~步骤 4(即图 2 中的步骤 1~步骤 4)。

【6】用户设备发生以下三种通信异常情况之一时，将 NAS 尝试次数进行+1 处理，其中，NAS 尝试次数可视为用户设备在各个小区上因通信异常情况导致 RRC 连接释放的次数:

【6-1】当前基站在未请求查询用户设备的 IMSI 的情况下，即向用户设备发送 RRC 连接释放指示，将用户设备释放掉;

【6-2】在当前基站未请求查询用户设备的 IMSI 的情况下，NAS 协议保护定时器超时;

【6-3】在当前基站未请求查询用户设备的 IMSI 的情况下，用户设备的底层向 RRC 层上报 RLF;

【7】判断 NAS 尝试次数是否达到 5 次；若达到 5 次，则执行步骤【8】；若未达到 5 次，则执行步骤【9】。

其中，该 NAS 尝试次数是指 NAS 在所有小区上的 NAS 尝试次数之和。

【8】禁用当前制式并去其他制式搜网。

【9】判断在第一小区上的 NAS 尝试次数是否达到配置次数。若是，则执行步骤【11】；若否，则执行步骤【10】。

其中，该配置次数可视为图 6 所示方法中第一阈值的一个具体示例。

【10】NAS 重新进行尝试，执行上述步骤【1】~【6】。

【11】NAS 向 RRC 层指示在第一小区上的 NAS 尝试次数达到配置次数，第一小区可能为伪基站小区。

【12】RRC 层在判断保存有类伪基站配置标识时将第一小区加入第一受限列表中。

其中，第一小区加入第一受限列表中可以理解为第一小区的小区信息加入第一受限列表中。

其中，第一小区的受限类型可以设置为“搜不到网不解受限”。“搜不到网不解受限”的含义可以是：若用户设备重新进行搜网时未搜索到其他可用小区，则用户设备禁用当前制式，去其他制式搜网。

【13】RRC 层判断是否能搜索到其他可用小区。若是，则执行步骤【14】；若否，则执行步骤【15】。

【14】用户设备在搜网到第一受限列表以外的可用小区时，用户设备选择驻留到该小区，该小区为合法基站的小区。

其中，步骤【14】中用户设备驻留的小区可视为图 6 所示方法中的第二小区的一个具体示例。需要说明的是，用户设备在执行步骤【14】后，也可能驻留到另一个伪基站小区，在这种情况下，用户设备通过执行图 7 所示方法可判断出驻留到伪基站小区这一情况，进而将该小区也加入第一受限列表，避免再次驻留该小区。在图 7 所示方法中仅以步骤【14】驻留的小区为合法基站小区为例进行示意。

【15】用户设备未搜索到其他可用小区，则禁用当前制式，去其他制式搜网。

此外，在方法三中，还可由 NAS 记录类伪基站配置标识。在这种实现方式下，RRC 层将系统消息配置异常的情况上报给 NAS，由 NAS 保存类伪基站标识。在保存有类伪基站标识的情况下，NAS 可在步骤【11】中向 RRC 层指示第一基站为伪基站；RRC 层在步骤【12】中可直接将第一小区加入第一受限列表中，并根据保存的类伪基站标识将受限类型设置为“搜不到网不解受限”。

需要说明的是，图 9 所示方法可视为图 6 所示方法的一个具体示例。图 9 所示方法中未详尽描述的实现方式及技术效果可参见图 6 所示方法中的相关描述。

基于以上实施例，本申请实施例还提供一种伪基站识别装置，该装置应用于用户设备中。该装置可用于执行图 4 所示的伪基站识别方法。参见图 10，该伪基站识别装置 1000 包括收发单元 1001 和处理单元 1002。

其中，收发单元 1001，与用户设备当前驻留的第一小区所属的第一基站建立 RRC 连接后，接收第一基站发送的第一请求消息，第一请求消息用于请求查询用户设备的 IMSI；处理单元 1002 记录第一标识，第一标识用于指示第一基站请求查询用户设备的 IMSI；收发单元 1001 向第一基站发送第一响应消息，第一响应消息用于指示用户设备的 IMSI，并接收第一基站发送的 RRC 连接释放指示；处理单元 1002 在收发单元 1001 接收到 RRC 连接释放指示后，且确认记录有第一标识时，可以确定第一基站为伪基站。

可选地，处理单元 1002 还用于：在确定第一基站为伪基站之后，将第一小区的小区信息加入第一受限列表，第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区。

其中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的 PCI、第一小区的 EARFCN。

可选地，处理单元 1002 还用于：在将第一小区的小区信息加入第一受限列表之后进行小区搜索；根据小区搜索结果驻留到第二小区，第二小区的小区信息未记录在第一受限

列表中。

可选地，处理单元 1002 还用于：在收发单元 1001 接收第一基站发送的 RRC 连接释放指示之后，根据用户设备的配置将第一小区的域标识加入第二受限列表，第一小区的域标识为第一小区的 LA 域标识或 TA 域标识，第二受限列表用于指示用户设备禁止驻留在第二受限列表中记录的域标识所对应的小区。

可选地，处理单元 1002 还用于：若处理单元 1002 中未记录第一标识，则在收发单元 1001 接收到第一基站发送的 RRC 连接释放指示之后，确定第一基站不是伪基站；将第一小区的域标识加入第三受限列表，第一小区的域标识为第一小区的 LA 域标识或 TA 域标识，第三受限列表用于指示用户设备禁止驻留在受限列表中记录的域标识所对应的小区。

需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。在本申请的实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

同样需要说明的是，图 10 所示的伪基站识别装置 1000 可用于执行图 4 对应的实施例提供的方法，因此图 10 所示的伪基站识别装置 1000 中未详尽描述的实现方式及技术效果可参见图 4 所示方法中的相关描述。

基于同一发明构思，本申请实施例还提供一种伪基站识别装置，该伪基站识别装置可用于执行图 4 所示的伪基站识别方法，可以是与图 10 所示的伪基站识别装置 1000 相同的设备。

参见图 11，该伪基站识别装置 1100 中包括至少一个处理器 1101，用于实现本申请实施例提供的伪基站识别方法中的对应功能。伪基站识别装置 1100 还可以包括至少一个存储器 1102，用于存储程序指令和/或数据。存储器 1102 和处理器 1101 耦合。处理器 1101 可能和存储器 1102 协同操作。处理器 1101 可能执行存储器 1102 中存储的程序指令。所述至少一个存储器 1102 中的至少一个可以包括于处理器 1101 中。

伪基站识别装置 1100 中还可以包括通信接口 1103，伪基站识别装置 1100 可以通过通信接口 1103 和其它设备（例如第一基站）进行信息交互。通信接口 1103 可以是电路、总线、收发器或者其它任意可以用于进行信息交互的用户设备。其中，示例性地，该其它设备可以是基站、UE 或中继节点。处理器 1101 可以利用通信接口 1103 收发数据，示例的，通信接口 1103 用于与第一基站间的数据收发。

本申请实施例中不限定上述通信接口 1103、处理器 1101 以及存储器 1102 之间的具体连接介质。本申请实施例在图 11 中以存储器 1102、处理器 1101 以及通信接口 1103 之间

通过总线连接，总线在图 11 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 11 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本申请实施例还提供了一种芯片，该芯片包括上述通信接口和上述处理器，用于支持伪基站识别装置 1100 实现图 4 所示实施例对应的方法。

本申请实施例还提供了一种计算机可读存储介质，用于存储为执行上述处理器所需执行的计算机软件指令，其包含用于执行上述处理器所需执行的程序。

基于以上实施例，本申请实施例还提供一种伪基站识别装置。该伪基站识别装置可用于执行图 6 所示的伪基站识别方法。参见图 12，该伪基站识别装置 1200 包括收发单元 1201 和处理单元 1202。

其中，收发单元 1201，与用户设备当前驻留的第一小区所属的第一基站建立 RRC 连接后，统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数；

处理单元 1202 在因通信异常情况导致 RRC 连接释放的次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区。

其中，通信异常情况包括但不限于：用户设备的 NAS 协议保护定时器超时；用户设备的物理层或 MAC 层向 RRC 层上报 RLF；第一基站未请求查询用户设备的 IMSI，且第一基站向用户设备发送 RRC 连接释放指示。

可选地，处理单元 1202 还用于：在确定第一基站为伪基站或者第一小区为坏小区之后，将第一小区的小区信息加入第一受限列表，第一受限列表用于指示用户设备禁止驻留在第一受限列表中记录的小区信息所对应的小区；进行小区搜索；若未搜索到其他可用小区，则将第一小区的小区信息从第一受限列表中删除，并重新驻留第一小区；若搜索到第二小区为可用小区，则驻留第二小区，第二小区的小区信息未记录在第一受限列表中。

其中，第一小区的小区信息包括以下至少一种：第一小区的小区频点；第一小区的小区频段；第一小区的 PCI。

可选地，处理单元 1202 还用于：在收发单元 1201 与第一小区所属的第一基站建立 RRC 连接之前，保存第一小区的小区信息；处理单元 1202 在统计用户设备在第一小区上因通信异常情况导致 RRC 连接释放的次数时，具体用于：统计记录的小区信息指示的第一小区上因通信异常情况导致 RRC 连接释放的次数。

可选地，处理单元 1202 还用于：在确定第一基站为伪基站或者第一小区为坏小区之后，获取用于指示用户设备当前位置的第一位置信息；在将第一小区的小区信息加入第一受限列表之后，获取用于指示用户设备当前位置的第二位置信息；在第一位置信息指示的位置与第二位置信息指示的位置之间的距离大于第二阈值时，将第一小区的小区信息从第一受限列表中删除。

可选地，处理单元 1202 还用于：在收发单元 1201 与第一小区所属的第一基站建立 RRC 连接之前，在确定第一基站的系统消息配置异常时保存类伪基站配置标识，类伪基站配置标识用于指示第一基站的系统消息配置异常；处理单元 1202 在因通信异常情况导致 RRC 连接释放的次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区时，具体用于：在该次数大于第一阈值、且用户设备中保存有类伪基站配置标识时，确定第一基站为伪基站。

其中，处理单元 1202 在以下信息中的至少一种满足时，确定第一基站的系统消息配置异常：处理单元 1202 确定第一基站配置在 PLMN 列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识；处理单元 1202 确定第一基站的驻留门限低于用户设备配置的驻留门限阈值；处理单元 1202 确定第一基站未配置异频邻区和异系统邻区；处理单元 1202 确定第一基站配置 GSM 邻区的优先级为高重选优先级。

基于同一发明构思，本申请实施例还提供一种伪基站识别装置，该伪基站识别装置可用于执行图 6 所示的伪基站识别方法，可以是与图 12 所示的伪基站识别装置 1200 相同的设备。

参见图 13，该伪基站识别装置 1300 中包括至少一个处理器 1301，用于实现本申请实施例提供的伪基站识别方法中的对应功能。伪基站识别装置 1300 还可以包括至少一个存储器 1302，用于存储程序指令和/或数据。存储器 1302 和处理器 1301 耦合。处理器 1301 可能和存储器 1302 协同操作。处理器 1301 可能执行存储器 1302 中存储的程序指令。所述至少一个存储器 1302 中的至少一个可以包括于处理器 1301 中。

伪基站识别装置 1300 中还可以包括通信接口 1303，伪基站识别装置 1300 可以通过通信接口 1303 和其它设备（例如第一基站）进行信息交互。通信接口 1303 可以是电路、总线、收发器或者其它任意可以用于进行信息交互的用户设备。其中，示例性地，该其它设备可以是基站、UE 或中继节点。处理器 1301 可以利用通信接口 1303 收发数据，示例的，通信接口 1303 用于与第一基站间的数据收发。

本申请实施例中不限定上述通信接口 1303、处理器 1301 以及存储器 1302 之间的具体连接介质。本申请实施例在图 13 中以存储器 1302、处理器 1301 以及通信接口 1303 之间通过总线连接，总线在图 13 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 13 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本申请实施例还提供了一种芯片，该芯片包括上述通信接口和上述处理器，用于支持伪基站识别装置 1300 实现图 6 所示实施例对应的方法。

需要说明的是，图 10~图 13 中所示的伪基站识别装置可视为用户设备中的集成芯片，也可以也视为用户设备。

具体地，该用户设备包括但不限于智能手机、智能手表、平板电脑、VR 设备、AR 设备、个人计算机、手持式计算机、个人数字助理。

本申请实施例还提供了一种计算机可读存储介质，用于存储为执行上述处理器所需执行的计算机软件指令，其包含用于执行上述处理器所需执行的程序。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请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，本申请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。

本申请是参照根据本申请实施例的方法、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申请实施例进行各种改动和变型而不脱离本申请实施例的精神和范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种伪基站识别方法，其特征在于，包括:

用户设备与当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接;

所述用户设备接收所述第一基站发送的第一请求消息，所述第一请求消息用于请求查询所述用户设备的国际移动用户标识 IMSI;

用户设备记录第一标识，所述第一标识用于指示所述第一基站请求查询所述用户设备的 IMSI;

所述用户设备向所述第一基站发送第一响应消息，所述第一响应消息用于指示所述用户设备的 IMSI;

所述用户设备接收所述第一基站发送的 RRC 连接释放指示;

所述用户设备在接收到所述 RRC 连接释放指示后、且确认记录有第一标识时，确定所述第一基站为伪基站。

2、如权利要求 1 所述的方法，其特征在于，在所述用户设备确定所述第一基站为伪基站之后，还包括:

所述用户设备将所述第一小区的小区信息加入第一受限列表，所述第一受限列表用于指示所述用户设备禁止驻留在所述第一受限列表中记录的小区信息所对应的小区。

3、如权利要求 2 所述的方法，其特征在于，在所述用户设备将所述第一小区的小区信息加入第一受限列表之后，还包括:

所述用户设备进行小区搜索;

所述用户设备根据小区搜索结果驻留到第二小区，所述第二小区的小区信息未记录在所述第一受限列表中。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述第一小区的小区信息包括以下至少一种: 所述第一小区的小区频点; 所述第一小区的小区频段; 所述第一小区的物理小区标识 PCI、所述第一小区的 E-UTRA 绝对无线频率信道号 EARFCN。

5、如权利要求 1~4 任一项所述的方法，其特征在于，在所述用户设备接收所述第一基站发送的 RRC 连接释放指示之后，还包括:

所述用户设备根据所述用户设备的配置将所述第一小区的域标识加入第二受限列表，所述第一小区的域标识为所述第一小区的位置区 LA 域标识或跟踪区 TA 域标识，所述第二受限列表用于指示所述用户设备禁止驻留在所述第二受限列表中记录的域标识所对应的小区。

6、如权利要求 1~5 任一项所述的方法，其特征在于，若所述用户设备中未记录所述第一标识，则在所述用户设备接收到所述第一基站发送的 RRC 连接释放指示之后，还包括:

所述用户设备确定所述第一基站不是伪基站;

所述用户设备将所述第一小区的域标识加入第三受限列表，所述第一小区的域标识为所述第一小区的 LA 域标识或 TA 域标识，所述第三受限列表用于指示所述用户设备禁止驻留在所述受限列表中记录的域标识所对应的小区。

7、一种伪基站识别方法，其特征在于，包括:

用户设备与当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接;

所述用户设备统计所述用户设备在所述第一小区上因通信异常情况导致 RRC 连接释放的次数;

所述用户设备在所述次数大于第一阈值时确定所述第一基站为伪基站或者所述第一小区为坏小区。

8、如权利要求 7 所述的方法，其特征在于，在所述用户设备确定所述第一基站为伪基站或者所述第一小区为坏小区之后，还包括:

所述用户设备将所述第一小区的小区信息加入第一受限列表，所述第一受限列表用于指示所述用户设备禁止驻留在所述第一受限列表中记录的小区信息所对应的小区;

所述用户设备进行小区搜索;

若所述用户设备未搜索到其他可用小区，则所述用户设备将所述第一小区的小区信息从所述第一受限列表中删除，并重新驻留所述第一小区；若所述用户设备搜索到第二小区为可用小区，则所述用户设备驻留所述第二小区，所述第二小区的小区信息未记录在所述第一受限列表中。

9、如权利要求 7 或 8 所述的方法，其特征在于，在所述用户设备与第一小区所属的第一基站建立 RRC 连接之前，还包括:

所述用户设备保存所述第一小区的小区信息;

所述用户设备在统计所述用户设备在所述第一小区上因通信异常情况导致 RRC 连接释放的次数，包括:

所述用户设备统计记录的所述小区信息指示的所述第一小区上因通信异常情况导致 RRC 连接释放的次数。

10、如权利要求 8 或 9 所述的方法，其特征在于，在所述用户设备确定所述第一基站为伪基站或者所述第一小区为坏小区之后，还包括:

所述用户设备获取用于指示所述用户设备当前位置的第一位置信息;

在所述用户设备将所述第一小区的小区信息加入第一受限列表之后，还包括:

所述用户设备获取用于指示所述用户设备当前位置的第二位置信息;

所述用户设备在所述第一位置信息指示的位置与所述第二位置信息指示的位置之间的距离大于第二阈值时，将所述第一小区的小区信息从所述第一受限列表中删除。

11、如权利要求 7~10 任一项所述的方法，其特征在于，在所述用户设备与所述第一小区所属的第一基站建立 RRC 连接之前，还包括:

所述用户设备在确定所述第一基站的系统消息配置异常时保存类伪基站配置标识，所述类伪基站配置标识用于指示所述第一基站的系统消息配置异常;

所述用户设备在所述次数大于第一阈值时确定所述第一基站为伪基站或者所述第一小区为坏小区，包括:

所述用户设备在所述次数大于第一阈值、且所述用户设备中保存有所述类伪基站配置标识时，确定所述第一基站为伪基站。

12、如权利要求 11 所述的方法，其特征在于，所述用户设备在以下信息中的至少一种满足时，确定所述第一基站的系统消息配置异常:

所述用户设备确定所述第一基站配置在共享公共陆地移动网络 PLMN 列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识;

所述用户设备确定所述第一基站的驻留门限低于所述用户设备配置的驻留门限阈值;

所述用户设备确定所述第一基站未配置异频邻区和异系统邻区；

所述用户设备确定所述第一基站配置全球移动通信 GSM 邻区的优先级为高重选优先级。

13、如权利要求 8~12 任一项所述的方法，其特征在于，所述第一小区的小区信息包括以下至少一种：所述第一小区的小区频点；所述第一小区的小区频段；所述第一小区的物理小区标识 PCI。

14、如权利要求 7~13 任一项所述的方法，其特征在于，所述通信异常情况包括：

所述用户设备的非接入层 NAS 协议保护定时器超时；

所述用户设备的物理层或媒体访问控制层 MAC 层向 RRC 层上报无线链路失败 RLF；

所述第一基站未请求查询所述用户设备的 IMSI，且所述第一基站向所述用户设备发送 RRC 连接释放指示。

15、一种伪基站识别装置，应用于用户设备，其特征在于，包括收发单元和处理单元；

所述收发单元，用于与所述用户设备当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；以及接收所述第一基站发送的第一请求消息，所述第一请求消息用于请求查询所述用户设备的国际移动用户标识 IMSI；

所述处理单元，用于记录记录第一标识，所述第一标识用于指示所述第一基站请求查询所述用户设备的 IMSI；

所述收发单元，还用于向所述第一基站发送第一响应消息，所述第一响应消息用于指示所述用户设备的 IMSI；

所述收发单元，还用于接收所述第一基站发送的 RRC 连接释放指示；

所述处理单元，还用于在所述收发单元接收到所述 RRC 连接释放指示后、且确认记录有第一标识时，确定所述第一基站为伪基站。

16、如权利要求 15 所述的装置，其特征在于，所述处理单元还用于：

在确定所述第一基站为伪基站之后，将所述第一小区的小区信息加入第一受限列表，所述第一受限列表用于指示所述用户设备禁止驻留在所述第一受限列表中记录的小区信息所对应的小区。

17、如权利要求 16 所述的装置，其特征在于，所述处理单元还用于：

在将所述第一小区的小区信息加入第一受限列表之后进行小区搜索；

根据小区搜索结果驻留到第二小区，所述第二小区的小区信息未记录在所述第一受限列表中。

18、如权利要求 16 或 17 所述的装置，其特征在于，所述第一小区的小区信息包括以下至少一种：所述第一小区的小区频点；所述第一小区的小区频段；所述第一小区的物理小区标识 PCI、所述第一小区的 E-UTRA 绝对无线频率信道号 EARFCN。

19、如权利要求 15~18 任一项所述的装置，其特征在于，所述处理单元还用于：

在所述收发单元接收所述第一基站发送的 RRC 连接释放指示之后，根据所述用户设备的配置将所述第一小区的域标识加入第二受限列表，所述第一小区的域标识为所述第一小区的位置区 LA 域标识或跟踪区 TA 域标识，所述第二受限列表用于指示所述用户设备禁止驻留在所述第二受限列表中记录的域标识所对应的小区。

20、如权利要求 15~19 任一项所述的装置，其特征在于，所述处理单元还用于：

若所述处理单元中未记录所述第一标识，则在所述收发单元接收到所述第一基站发送

的 RRC 连接释放指示之后，确定所述第一基站不是伪基站；

将所述第一小区的域标识加入第三受限列表，所述第一小区的域标识为所述第一小区的 LA 域标识或 TA 域标识，所述第三受限列表用于指示所述用户设备禁止驻留在所述受限列表中记录的域标识所对应的小区。

21、一种伪基站识别装置，应用于用户设备，其特征在于，包括收发单元和处理单元；

所述收发单元，用于与所述用户设备当前驻留的第一小区所属的第一基站建立无线资源控制 RRC 连接；

所述处理单元，用于统计所述用户设备在所述第一小区上因通信异常情况导致 RRC 连接释放的次数；

所述处理单元，还用于在所述次数大于第一阈值时确定所述第一基站为伪基站或者所述第一小区为坏小区。

22、如权利要求 21 所述的装置，其特征在于，所述处理单元还用于：

在确定所述第一基站为伪基站或者所述第一小区为坏小区之后，将所述第一小区的小区信息加入第一受限列表，所述第一受限列表用于指示所述用户设备禁止驻留在所述第一受限列表中记录的小区信息所对应的小区；

进行小区搜索；

若未搜索到其他可用小区，则将所述第一小区的小区信息从所述第一受限列表中删除，并重新驻留所述第一小区；若搜索到第二小区为可用小区，则驻留所述第二小区，所述第二小区的小区信息未记录在所述第一受限列表中。

23、如权利要求 21 或 22 所述的装置，其特征在于，所述处理单元还用于：

在所述收发单元与第一小区所属的第一基站建立 RRC 连接之前，保存所述第一小区的小区信息；

所述处理单元在统计所述用户设备在所述第一小区上因通信异常情况导致 RRC 连接释放的次数时，具体用于：

统计记录的小区信息指示的所述第一小区上因通信异常情况导致 RRC 连接释放的次数。

24、如权利要求 22 或 23 所述的装置，其特征在于，所述处理单元还用于：

在确定所述第一基站为伪基站或者所述第一小区为坏小区之后，获取用于指示所述用户设备当前位置的第一位置信息；

在将所述第一小区的小区信息加入第一受限列表之后，获取用于指示所述用户设备当前位置的第二位置信息；

在所述第一位置信息指示的位置与所述第二位置信息指示的位置之间的距离大于第二阈值时，将所述第一小区的小区信息从所述第一受限列表中删除。

25、如权利要求 21~24 任一项所述的装置，其特征在于，所述处理单元还用于：

在所述收发单元与所述第一小区所属的第一基站建立 RRC 连接之前，在确定所述第一基站的系统消息配置异常时保存类伪基站配置标识，所述类伪基站配置标识用于指示所述第一基站的系统消息配置异常；

所述处理单元在所述次数大于第一阈值时确定所述第一基站为伪基站或者所述第一小区为坏小区时，具体用于：

在所述次数大于第一阈值、且所述用户设备中保存有所述类伪基站配置标识时，确定

所述第一基站为伪基站。

26、如权利要求 25 所述的装置，其特征在于，所述处理单元在以下信息中的至少一种满足时，确定所述第一基站的系统消息配置异常：

所述处理单元确定所述第一基站配置在共享公共陆地移动网络 PLMN 列表中的多个 PLMN 标识为禁止配置在同一共享 PLMN 列表中的 PLMN 标识；

所述处理单元确定所述第一基站的驻留门限低于所述用户设备配置的驻留门限阈值；

所述处理单元确定所述第一基站未配置异频邻区和异系统邻区；

所述处理单元确定所述第一基站配置全球移动通信 GSM 邻区的优先级为高重选优先级。

27、如权利要求 22~26 任一项所述的装置，其特征在于，所述第一小区的小区信息包括以下至少一种：所述第一小区的小区频点；所述第一小区的小区频段；所述第一小区的物理小区标识 PCI。

28、如权利要求 21~27 任一项所述的装置，其特征在于，所述通信异常情况包括：

所述用户设备的非接入层 NAS 协议保护定时器超时；

所述用户设备的物理层或媒体访问控制层 MAC 层向 RRC 层上报无线链路失败 RLF；

所述第一基站未请求查询所述用户设备的 IMSI，且所述第一基站向所述用户设备发送 RRC 连接释放指示。

29、一种伪基站识别装置，其特征在于，包括处理器，所述处理器与存储器耦合，并读取所述存储器中的指令，用于执行如权利要求 1~14 任一项所述的方法。

30、一种计算机存储介质，其特征在于，所述计算机存储介质上存储有程序，所述程序被处理器执行时，用于实现如权利要求 1~14 任一项所述的方法。

31、一种计算机程序产品，其特征在于，所述计算机程序产品包含的程序代码在计算机上运行时，使得所述计算机执行如权利要求 1~14 任一项所述的方法。


用户设备
伪基站
1、附着请求消息/跟踪区更新请求消息
2、RRC连接请求消息
3、RRC连接建立消息
4、RRC连接建立完成消息
5、身份识别请求消息（查询IMSI）
6、身份识别响应消息（IMSI）
7、附着拒绝消息/跟踪区更新拒绝消息
8、RRC连接释放消息

图 1

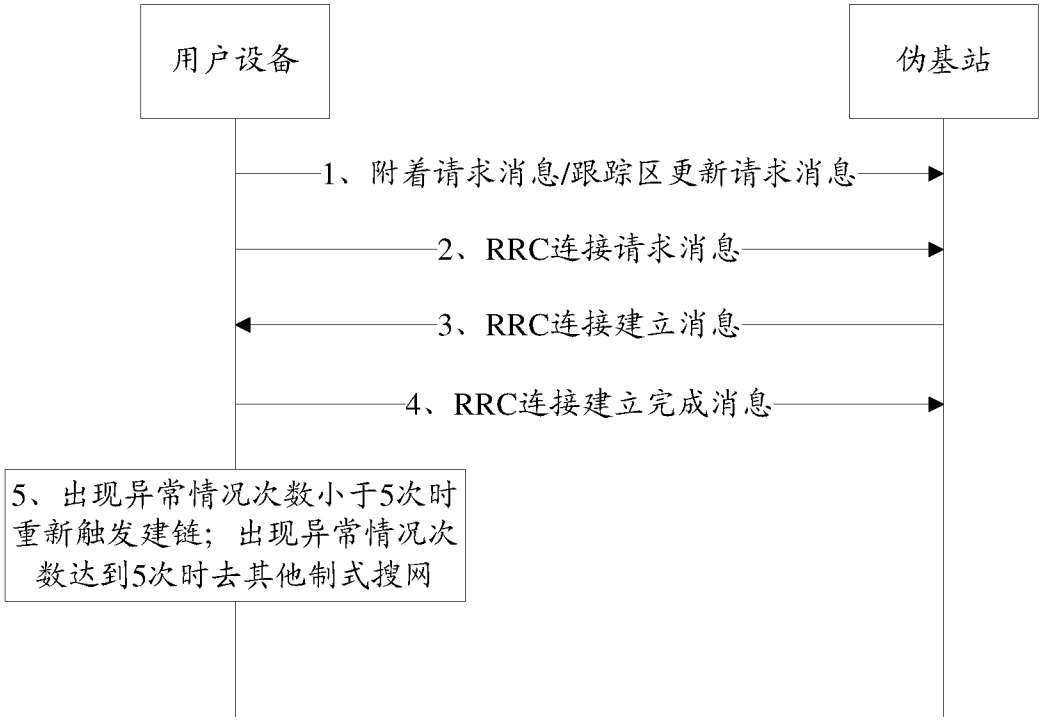
用户设备
伪基站
1、附着请求消息/跟踪区更新请求消息
2、RRC连接请求消息
3、RRC连接建立消息
4、RRC连接建立完成消息
5、出现异常情况次数小于5次时重新触发建链；出现异常情况次数达到5次时去其他制式搜网

图 2

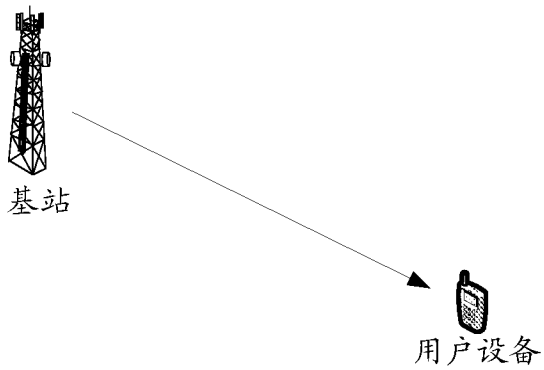
基站
用户设备

图 3

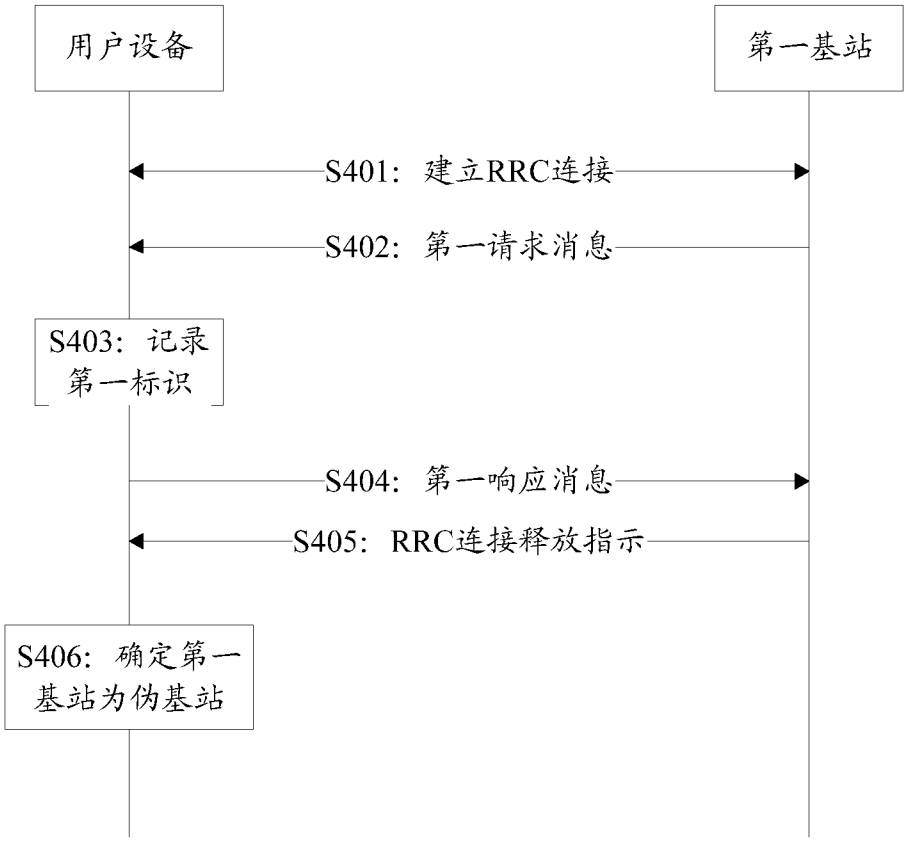
用户设备
第一基站
S401：建立RRC连接
S402：第一请求消息
S403：记录第一标识
S404：第一响应消息
S405：RRC连接释放指示
S406：确定第一基站为伪基站

图 4

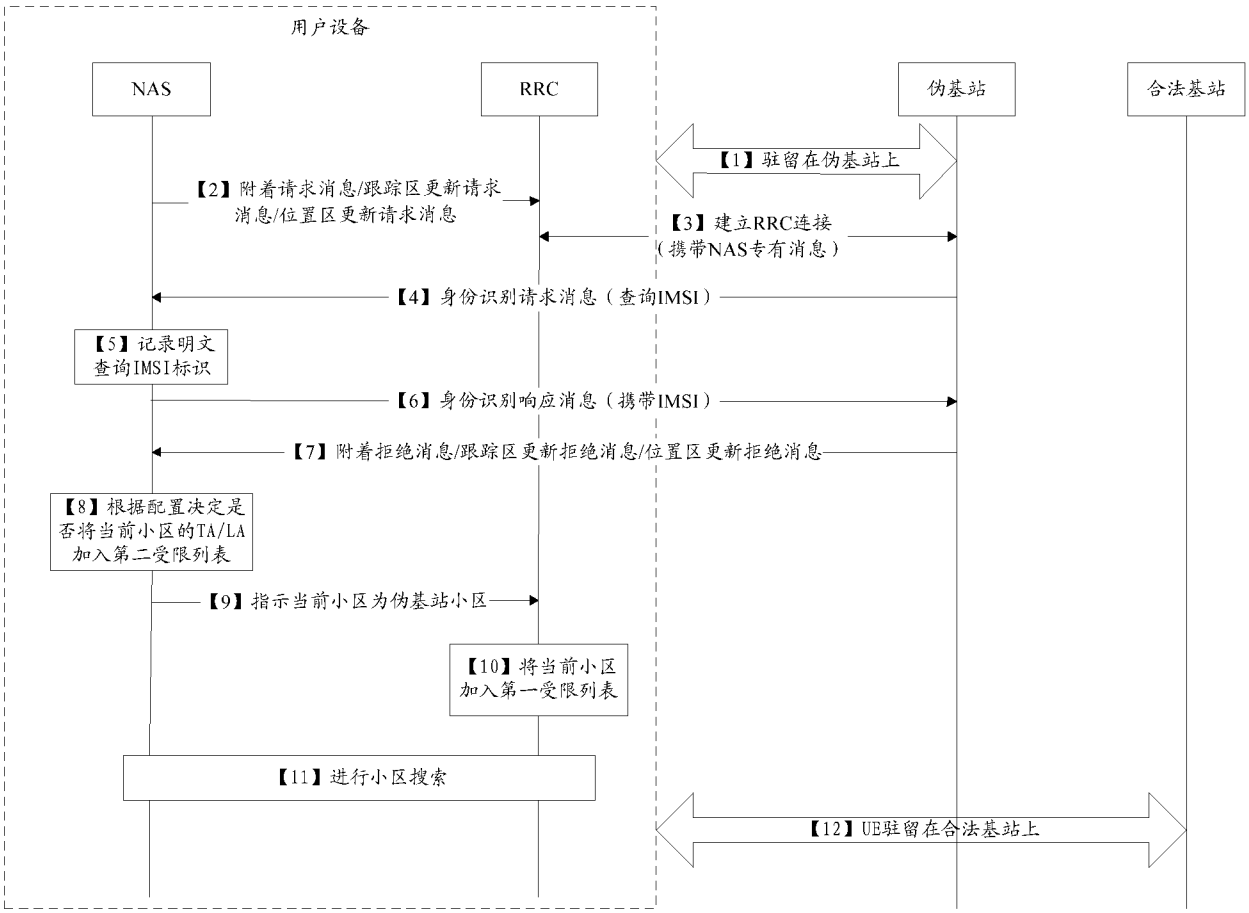
用户设备
NAS
RRC
伪基站
合法基站
【1】驻留在伪基站上
【2】附着请求消息/跟踪区更新请求消息/位置区更新请求消息
【3】建立RRC连接（携带NAS专有消息）
【4】身份识别请求消息（查询IMSI）
【5】记录明文查询IMSI标识
【6】身份识别响应消息（携带IMSI）
【7】附着拒绝消息/跟踪区更新拒绝消息/位置区更新拒绝消息
【8】根据配置决定是否将当前小区的TA/LA加入第二受限列表
【9】指示当前小区为伪基站小区
【10】将当前小区加入第一受限列表
【11】进行小区搜索
【12】UE驻留在合法基站上

图 5

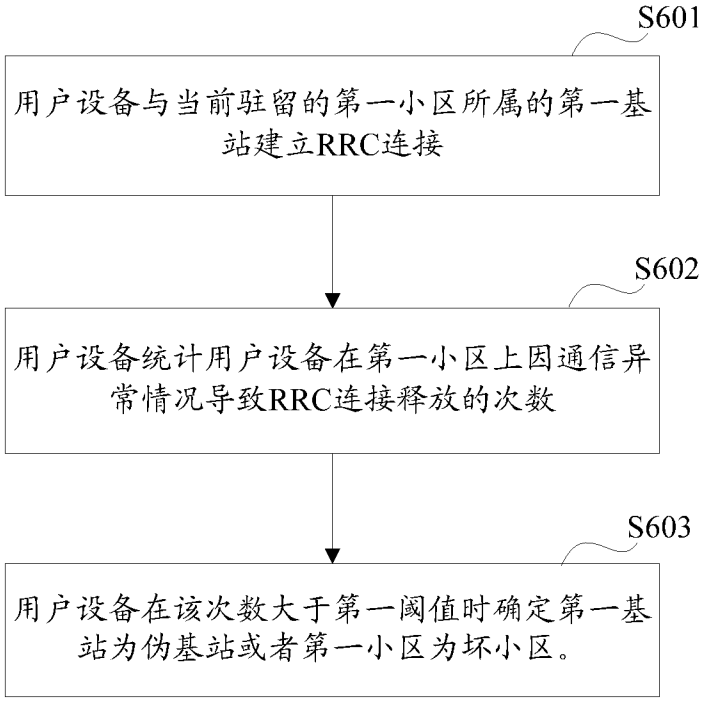
S601
用户设备与当前驻留的第一小区所属的第一基站建立RRC连接
S602
用户设备统计用户设备在第一小区上因通信异常情况导致RRC连接释放的次数
S603
用户设备在该次数大于第一阈值时确定第一基站为伪基站或者第一小区为坏小区。

图 6

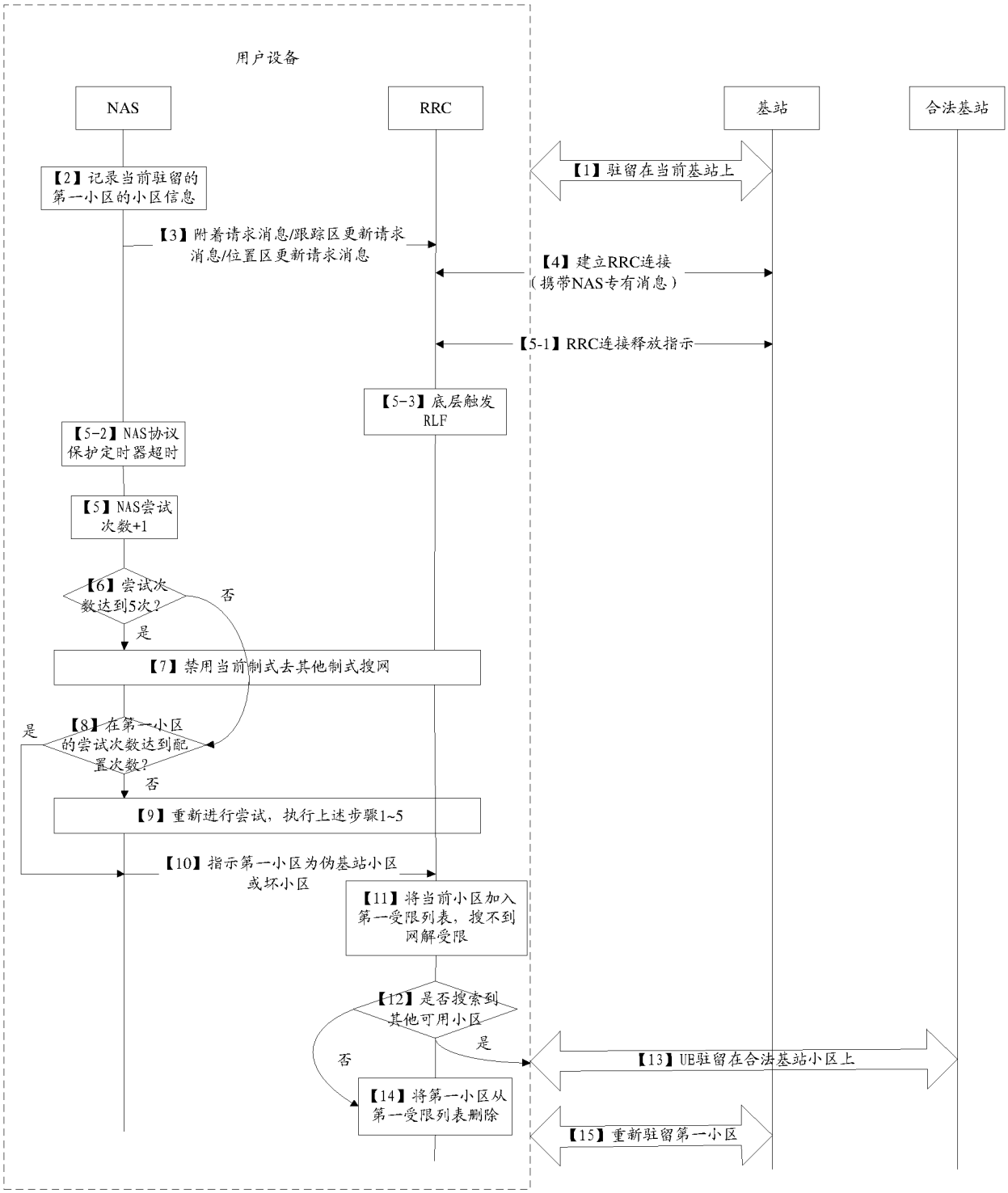
用户设备
NAS
RRC
基站
合法基站
【1】驻留在当前基站上
【2】记录当前驻留的第一小区的小区信息
【3】附着请求消息/跟踪区更新请求消息/位置区更新请求消息
【4】建立RRC连接（携带NAS专有消息）
【5-1】RRC连接释放指示
【5-3】底层触发RLF
【5-2】NAS协议保护定时器超时
【5】NAS尝试次数+1
【6】尝试次数达到5次?
否
是
【7】禁用当前制式去其他制式搜网
【8】在第一小区的尝试次数达到配置次数?
是
否
【9】重新进行尝试，执行上述步骤1~5
【10】指示第一小区为伪基站小区或坏小区
【11】将当前小区加入第一受限列表，搜不到网解受限
【12】是否搜索到其他可用小区
是
否
【13】UE驻留在合法基站小区上
【14】将第一小区从第一受限列表删除
【15】重新驻留第一小区

图 7

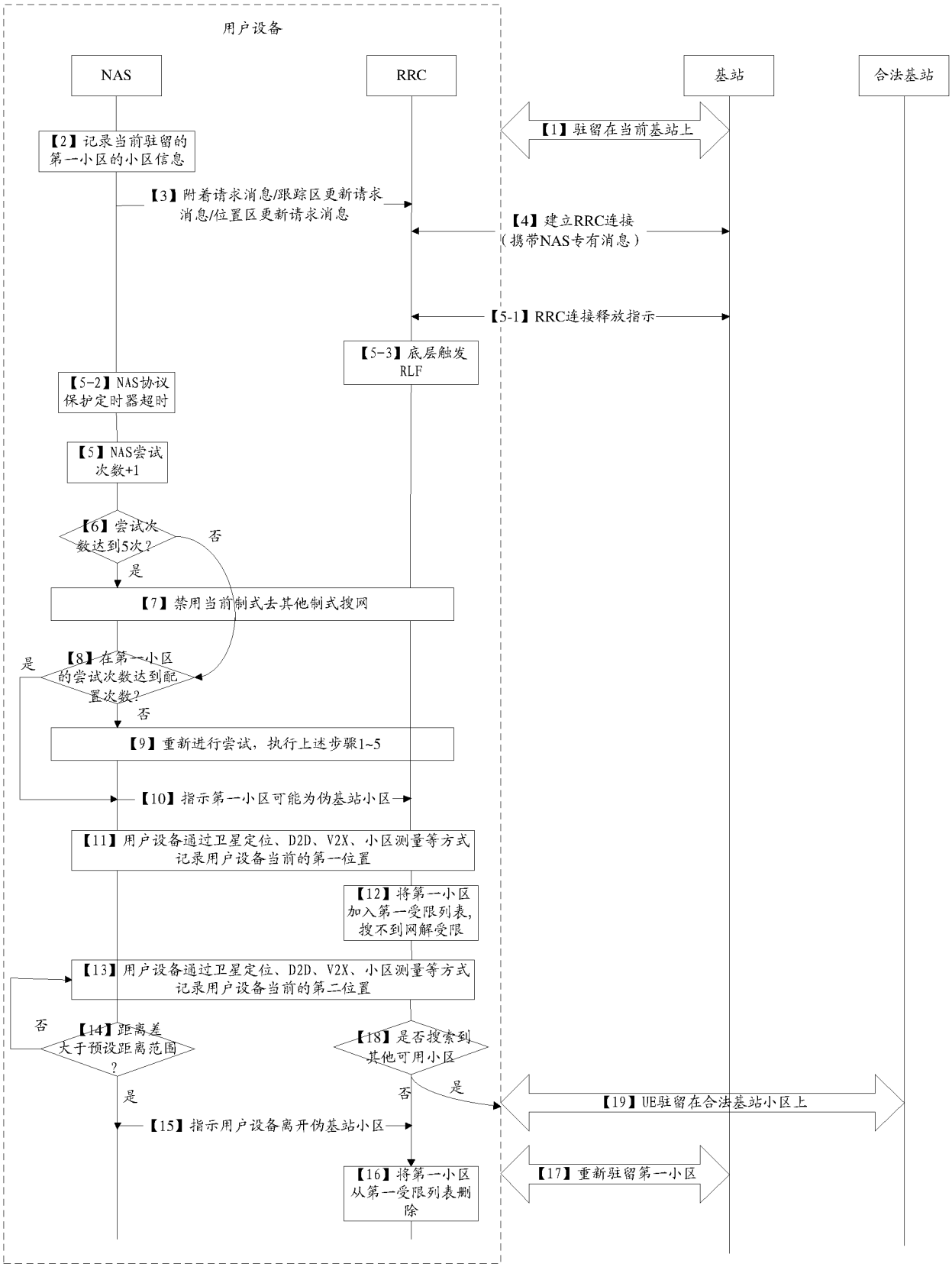
用户设备
NAS
RRC
基站
合法基站
【1】驻留在当前基站上
【2】记录当前驻留的第一小区的小区信息
【3】附着请求消息/跟踪区更新请求消息/位置区更新请求消息
【4】建立RRC连接（携带NAS专有消息）
【5-1】RRC连接释放指示
【5-3】底层触发RLF
【5-2】NAS协议保护定时器超时
【5】NAS尝试次数+1
【6】尝试次数达到5次？
否
是
【7】禁用当前制式去其他制式搜网
【8】在第一小区的尝试次数达到配置次数？
是
否
【9】重新进行尝试，执行上述步骤1~5
【10】指示第一小区可能为伪基站小区
【11】用户设备通过卫星定位、D2D、V2X、小区测量等方式记录用户设备当前的第一位置
【12】将第一小区加入第一受限列表，搜不到网解受限
【13】用户设备通过卫星定位、D2D、V2X、小区测量等方式记录用户设备当前的第二位置
否
【14】距离差大于预设距离范围？
是
【15】指示用户设备离开伪基站小区
【16】将第一小区从第一受限列表删除
【17】重新驻留第一小区
【18】是否搜索到其他可用小区
否
是
【19】UE驻留在合法基站小区上

图 8

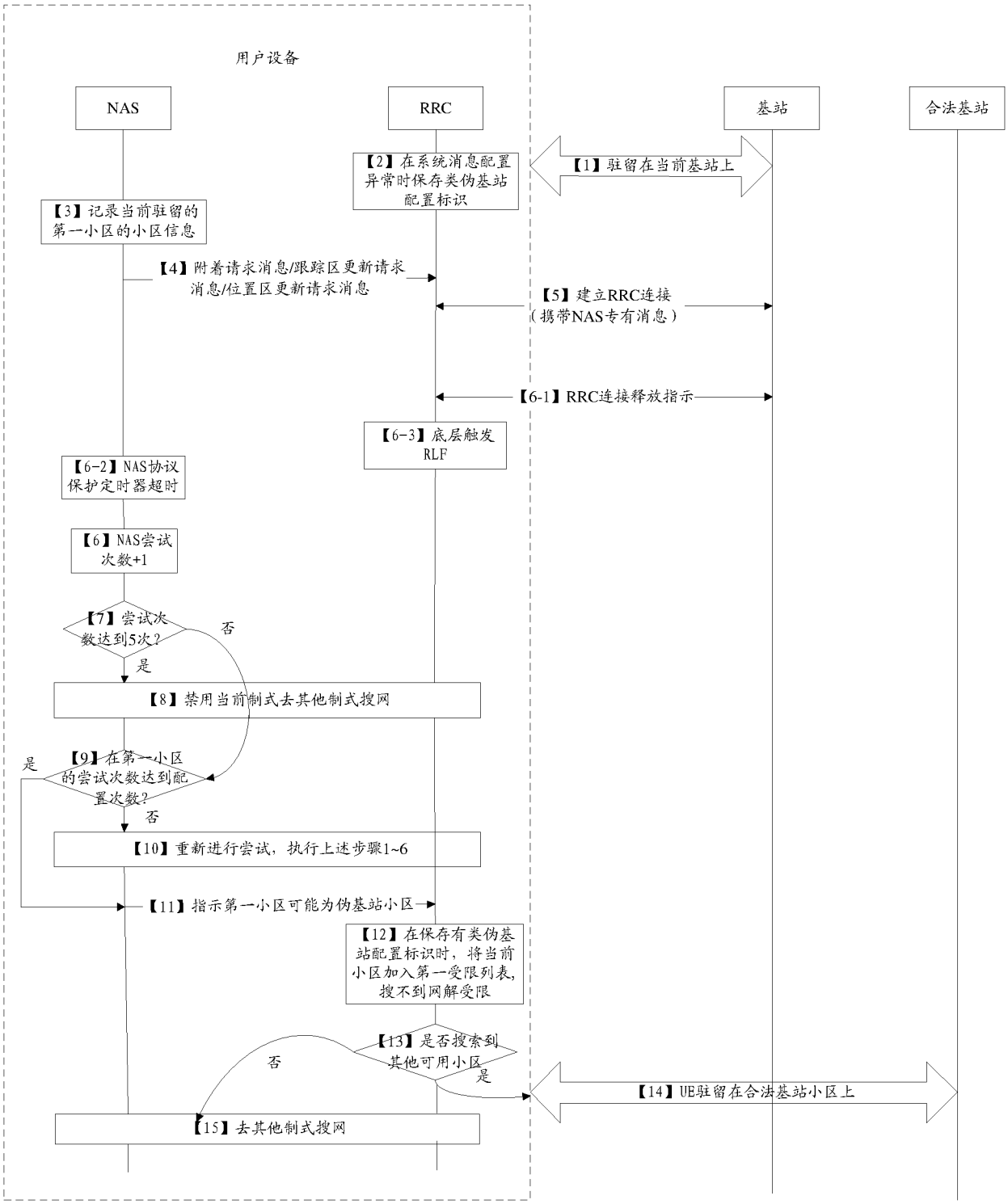
用户设备
NAS
RRC
基站
合法基站
【1】驻留在当前基站上
【2】在系统消息配置异常时保存类伪基站配置标识
【3】记录当前驻留的第一小区的小区信息
【4】附着请求消息/跟踪区更新请求消息/位置区更新请求消息
【5】建立RRC连接（携带NAS专有消息）
【6-1】RRC连接释放指示
【6-3】底层触发RLF
【6-2】NAS协议保护定时器超时
【6】NAS尝试次数+1
【7】尝试次数达到5次?
否
是
【8】禁用当前制式去其他制式搜网
是
【9】在第一小区的尝试次数达到配置次数?
否
【10】重新进行尝试，执行上述步骤1~6
【11】指示第一小区可能为伪基站小区
【12】在保存有类伪基站配置标识时，将当前小区加入第一受限列表，搜不到网解受限
【13】是否搜索到其他可用小区
否
是
【14】UE驻留在合法基站小区上
【15】去其他制式搜网

图 9

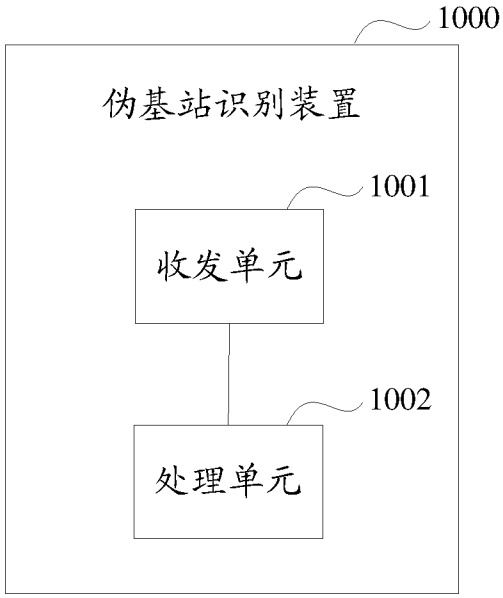
1000
伪基站识别装置
1001
收发单元
1002
处理单元

图 10

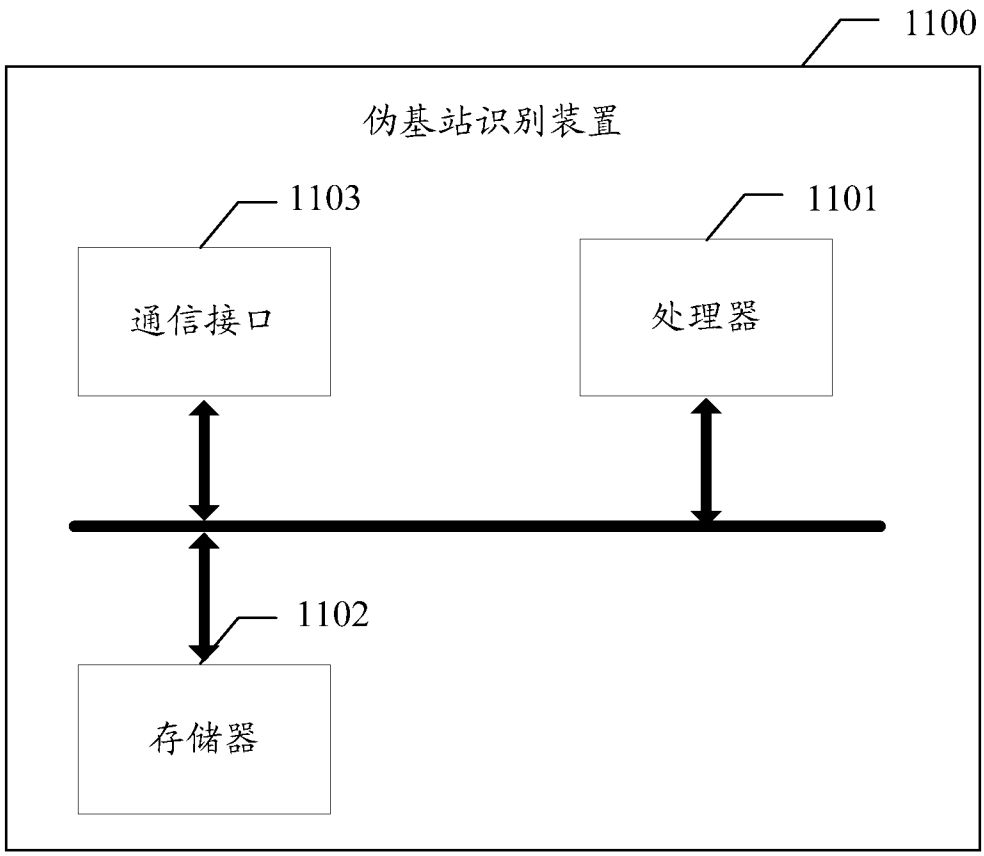
1100
伪基站识别装置
1103
通信接口
1101
处理器
1102
存储器

图 11

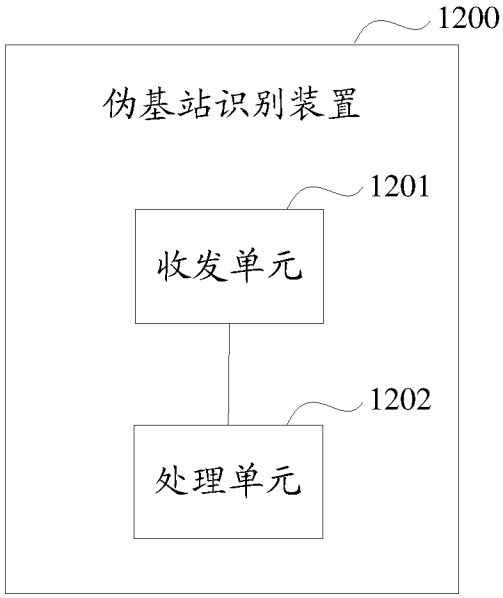
1200
伪基站识别装置
1201
收发单元
1202
处理单元

图 12

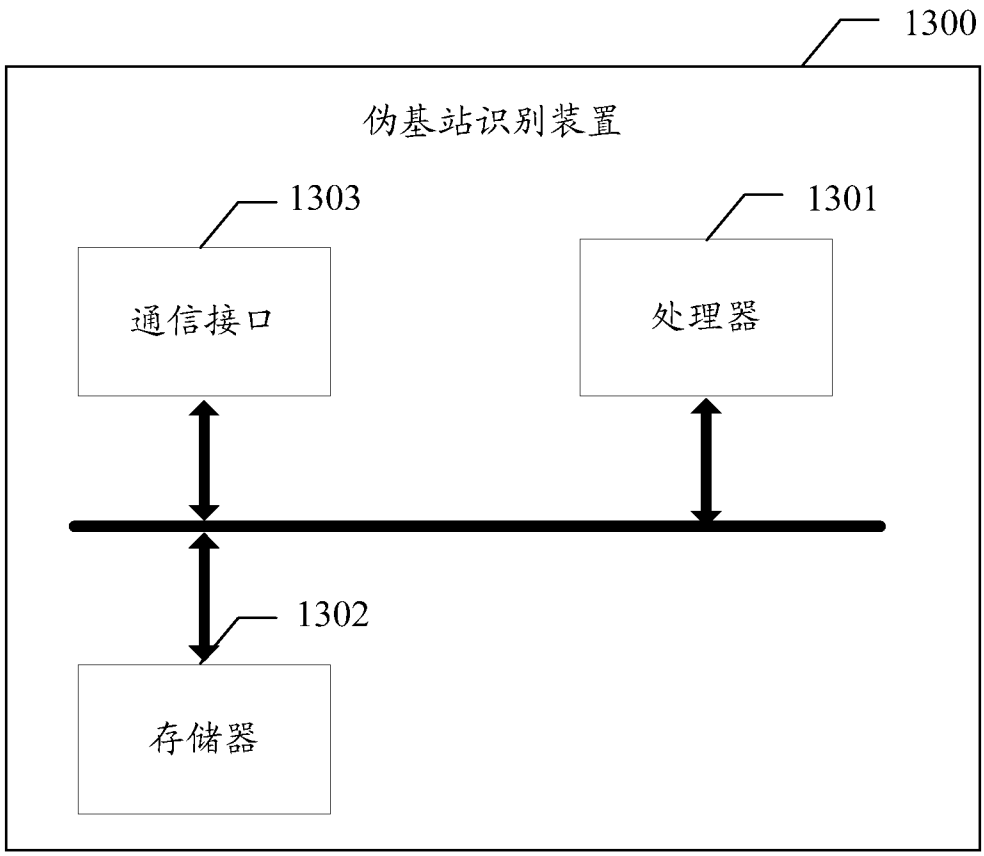
1300
伪基站识别装置
1303
通信接口
1301
处理器
1302
存储器

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/097607

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(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)

H04W12/-

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)

CPRSABS; SIPOABS; CNTXT; CNKI: 基站, 伪, 假, 非法, 小区, 接入点, 异常, 故障, 识别, 发现, 鉴别, 释放; eNB, BS, base station, access point, AP, cell, pseudo, abnormal, fake, illegal, discover, detect, identify, distinguish, discriminate, 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 107683617 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 February 2018 (2018-02-09) description, paragraphs [0026]-[0035]	1-6, 15-20, 29-31
A	CN 106358199 A (VIVO MOBILE COMMUNICATION CO., LTD.) 25 January 2017 (2017-01-25) description, paragraphs [0036]-[0059]	1-6, 15-20, 29-31
X	CN 105430653 A (CHINA TELECOM CORPORATION LIMITED) 23 March 2016 (2016-03-23) description, paragraphs [0041]-[0047]	7-9, 13, 21-23, 27
A	EP 3258719 A1 (GEMALTO M2M GMBH) 20 December 2017 (2017-12-20) entire document	1-31

☐ 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 April 2019	**16 April 2019**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/097607

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107683617	A	09 February 2018	EP	3298814	A1	28 March 2018
				US	9867039	B2	09 January 2018
				EP	3298814	A4	11 April 2018
				WO	2016206610	A1	29 December 2016
				US	2016381545	A1	29 December 2016
CN	106358199	A	25 January 2017		None		
CN	105430653	A	23 March 2016		None		
EP	3258719	A1	20 December 2017	WO	2017215946	A1	21 December 2017
				CN	109314864	A	05 February 2019

国际检索报告

国际申请号 PCT/CN2018/097607

A. 主题的分类

H04W 12/06(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)

H04W12/-

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）)

CPRSABS;SIPOABS;CNTXT;CNKI:基站，伪，假，非法，小区，接入点，异常，故障，识别，发现，鉴别，释放；eNB, BS, base station, access point, AP, cell, pseudo, abnormal, fake,illegal, discover,detect, identify, distinguish, discriminate,release

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 107683617 A (华为技术有限公司) 2018年 2月 9日 (2018-02-09) 说明书第[0026]-[0035]段	1-6、15-20、29-31
A	CN 106358199 A (维沃移动通信有限公司) 2017年 1月 25日 (2017-01-25) 说明书第[0036]-[0059]段	1-6、15-20、29-31
X	CN 105430653 A (中国电信股份有限公司) 2016年 3月 23日 (2016-03-23) 说明书第[0041]-[0047]段	7-9、13、21-23、27
A	EP 3258719 A1 (GEMALTO M2M GMBH) 2017年 12月 20日 (2017-12-20) 全文	1-31

☐ 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 4月 9日	2019年 4月 16日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 马莹莹 电话号码 86-(010)-62411362

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/097607

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	107683617	A	2018年 2月 9日	EP	3298814	A1	2018年 3月 28日
				US	9867039	B2	2018年 1月 9日
				EP	3298814	A4	2018年 4月 11日
				WO	2016206610	A1	2016年 12月 29日
				US	2016381545	A1	2016年 12月 29日
CN	106358199	A	2017年 1月 25日		无		
CN	105430653	A	2016年 3月 23日		无		
EP	3258719	A1	2017年 12月 20日	WO	2017215946	A1	2017年 12月 21日
				CN	109314864	A	2019年 2月 5日