

(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
2017年8月3日 (03.08.2017)



(10) 国际公布号
WO 2017/128542 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01)
- (21) 国际申请号: PCT/CN2016/080822
- (22) 国际申请日: 2016年4月29日 (29.04.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610064472.2 2016年1月29日 (29.01.2016) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。
- (72) 发明人: 张祖辉 (ZHANG, Zuhui); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。
- (74) 代理人: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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))。

(54) Title: NETWORK RESIDING METHOD, NETWORK RESIDING SYSTEM AND TERMINAL

(54) 发明名称: 网络驻留方法、网络驻留系统和终端

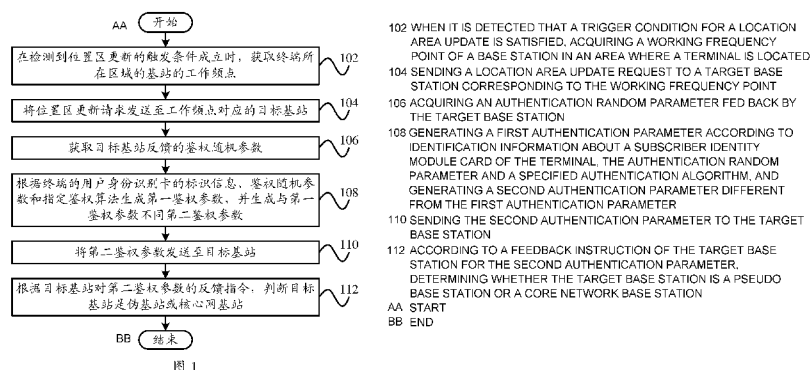


图 1

(57) Abstract: Provided are a network residing method, a network residing system and a terminal. The network residing method comprises: when it is detected that a trigger condition for a location area update is satisfied, acquiring a working frequency point of a base station in an area where a terminal is located; sending a location area update request to a target base station corresponding to the working frequency point; acquiring an authentication random parameter fed back by the target base station; generating a first authentication parameter according to identification information about a subscriber identity module card of the terminal, the authentication random parameter and a specified authentication algorithm, and generating a second authentication parameter different from the first authentication parameter; sending the second authentication parameter to the target base station; and according to a feedback instruction of the target base station for the second authentication parameter, determining whether the target base station is a pseudo base station or a core network base station. By means of the technical solution of the present invention, the probability of a user terminal residing in a pseudo base station is reduced, the interference of the pseudo base station on a communication service of the user terminal is lowered, and the use security of the user terminal is improved.

(57) 摘要:

[见续页]

WO 2017/128542 A1



本发明提供了一种网络驻留方法、网络驻留系统和终端，其中，网络驻留方法包括：在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；将位置区更新请求发送至工作频点对应的目标基站；获取目标基站反馈的鉴权随机参数；根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与第一鉴权参数不同第二鉴权参数；将第二鉴权参数发送至目标基站；根据目标基站对第二鉴权参数的反馈指令，判断目标基站是伪基站或核心网基站。通过本发明技术方案，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

网络驻留方法、网络驻留系统和终端

本申请要求于 2016 年 01 月 29 日提交中国专利局，申请号为 201610064472.2、发明名称为“网络驻留方法、网络驻留系统和终端”的中国专利申请优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及通信技术领域，具体而言，涉及一种网络驻留方法、一种网络驻留系统和一种终端。

10 背景技术

随着通信技术的发展，伪基站设备运行时，通常以高于核心网基站的功率运行，进而误导用户终端驻留于伪基站网络，导致用户无法正常使用运营商提供的服务，伪基站强行向用户终端发送诈骗、广告推销等短信息，不仅影响了用户的正常通讯，甚至会给用户造成财务损失。

15 在相关技术中，终端都是按照网络协议规范进行邻区测量和小区重选判断，并且由于网络的鉴权属于单向鉴权，而终端不会鉴权网络，这样就导致终端无法判断网络的真实性。

因此，如何设计一种新的小区驻留方案，以实现终端对网络的甄别和准确驻留成为亟待解决的技术问题。

20

发明内容

本发明正是基于上述技术问题至少之一，提出了一种新的网络驻留方案，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

25

有鉴于此，本发明提出了一种网络驻留方法，包括：在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；将位置区

更新请求发送至工作频点对应的目标基站；获取目标基站反馈的鉴权随机参数；根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与第一鉴权参数不同的第二鉴权参数；将第二鉴权参数发送至目标基站；根据目标基站对第二鉴权参数的反馈指令，
5 判断目标基站是伪基站或核心网基站。

在该技术方案中，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

10 具体地，空闲状态下的用户终端需要完成的过程包括 PLMN（Public Land Mobile Network，公共陆地移动网络）选择，小区选择/重选、位置登记等，一旦完成驻留，用户终端可以读取系统信息（如驻留、接入和重选相关信息、位置区域信息等），读取寻呼信息，发起连接建立过程。

其中，第一鉴权参数生成的一种方式是终端根据 SIM 卡（Subscriber
15 Identity Module）的标识信息、获取来自网络的鉴权随机参数和指定鉴权算法（取自于核心网基站和 SIM 卡采用的通信协议）。但是，终端在接入网络之前，生成与第一鉴权参数不同的第二鉴权参数，也即第二鉴权参数对于核心网基站而言是不能被识别的错误参数。如果目标基站在接收错误参数的前提下，对终端的鉴权结果仍为正确，那终端可以据此判定目标基站
20 为伪基站。另外，如果目标基站的鉴权结果为错误，则此目标基站可能为核心网基站，则终端可以继续通过第一鉴权参数请求驻留于上述核心网基站，从而实现业务通信。

在上述技术方案中，优选地，根据目标基站对第二鉴权参数的反馈指令，判断目标基站是伪基站或核心网基站，具体包括以下步骤：在获取反
25 馈指令为鉴权失败指令时，判定目标基站是核心网基站；将第一鉴权参数发送至核心网基站，以供核心网基站根据鉴权随机参数和第一鉴权参数判断终端是否具有驻留权限；在获取核心网基站发送的鉴权成功指令后，根据核心网基站的小区的信道质量选择驻留的小区。

在该技术方案中，通过获取目标基站的反馈指令为鉴权失败，判定目
30 标基站为非伪基站，通过向目标基站发送正确的鉴权参数获取驻留权限，

实现了终端在核心网基站的网络驻留，保证了终端网络驻留的安全性和通讯的流畅性。

而在终端获取目标基站的反馈指令为鉴权成功时，进一步地根据小区重选准确确定驻留的基站，例如，小区选择遵循 C1 准则，即小区选择的 C1 值 $C1 > 0$ 时允许驻留：（该专利是正对 GSM，所以小区选择判断准则是基于 C1，S 准则是正对 3G 而言）

$C1 = (A - \text{Max}(B, 0))$ ，其中， $\text{Max}(B, 0)$ 表示取 B 和 0 两个数据中的最大值
 $A = \text{RLA_C} - \text{RXLEV_ACCESS_MIN}$;

$B = \text{MS_TXPWR_MAX_CCH} - P$,

10 其中，C1 表征小区选择判断准则，RLA_C 表征测量小区的平均接收信号电平（average of received signal level）值，RXLEV_ACCESS_MIN 表征网络允许的终端最小接入功率等级。MS_TXPWR_MAX_CCH 表征网络允许的终端最大发射功率等级。P 表征终端最大射频发射功率。

在上述技术方案中，优选地，还包括：在终端驻留核心网基站的小区后，检测终端是否移动至核心网基站的小区以外的区域；在检测到终端移动至核心网基站的小区以外的区域时，确定位置区更新的触发条件成立。

在该技术方案中，通过检测终端的位置变化不等于预设位置变化值时，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

20 具体地，小区重选的目的是选择属于这个 PLMN 中信号最好的小区进行驻留，当终端处于高速移动状态时，终端驻留的服务小区质量会由于距离的增加而降低，当下降到规定的门限值时，即服务小区 $C2 < \text{邻区 } C2$ ，且持续小于 5s 以上，将触发小区重选。

在上述任一项技术方案中，优选地，还包括：在获取反馈指令为鉴权成功指令时，判定目标基站是伪基站；确定伪基站的工作频点，将位置区更新请求发送至除伪基站以外的基站。

25 在该技术方案中，通过获取目标基站的反馈指令为鉴权成功，判定该目标基站为伪基站，防止了用户终端与伪基站之间的通讯，降低了用户遭到短信和电话骚扰以及诈骗的风险。

具体地，伪基站为了让用户驻留，通常不会进行鉴权，因此无论用户终端发送的鉴权参数是否为通过鉴权算法生成的正确结果，伪基站均会将鉴权成功的反馈指令发送至用户终端，因此将随机生成的与根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成的正确鉴权参数不同的错误鉴权参数发送至目标基站，即可判定该基站是否为伪基站。

在上述任一项技术方案中，优选地，还包括：确定预存储的驻留更新周期；在终端驻留小区后，终端的运行时间大于或等于驻留更新周期时，确定位置区更新的触发条件成立。

10 在该技术方案中，通过终端的运行时间大于或等于驻留更新周期，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

具体地，对于同等优先级频点/同频，采用同频小区重选的 R 准则至少持续 Treselection（小区重选定时器时长）时间；对于低优先级频率的小区重选，当驻留原小区时间超过 1s，且服务小区的 s 值小于预设的门限，并且低优先级频率小区的 s 值大于预设的门限，且持续时间超过 Treselection，进行重选。

根据本发明第二方面，还提出了一种网络驻留系统，包括：获取单元，用于在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；发送单元，用于将位置区更新请求发送至工作频点对应的目标基站；获取单元还用于：获取目标基站反馈的鉴权随机参数；网络驻留系统还包括：生成单元，用于根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与第一鉴权参数不同的第二鉴权参数；发送单元还用于：将第二鉴权参数发送至目标基站；网络驻留系统还包括：判断单元，用于根据目标基站对第二鉴权参数的反馈指令，判断目标基站是伪基站或核心网基站。

在该技术方案中，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，

提升了用户终端使用的安全性。

具体地，空闲状态下的用户终端需要完成的过程包括 PLMN (Public Land Mobile Network, 公共陆地移动网络) 选择, 小区选择/重选、位置登记等, 一旦完成驻留, 用户终端可以读取系统信息 (如驻留、接入和重选
5 相关信息、位置区域信息等), 读取寻呼信息, 发起连接建立过程。

其中, 第一鉴权参数生成的一种方式终端根据 SIM 卡 (Subscriber Identity Module) 的标识信息、获取来自网络的鉴权随机参数和指定鉴权算法 (取自于核心网基站和 SIM 卡采用的通信协议)。但是, 终端在接入网络之前, 生成与第一鉴权参数不同的第二鉴权参数, 也即第二鉴权参数对于核心网基站而言是不能被识别的错误参数。如果目标基站在接收错误参
10 数的前提下, 对终端的鉴权结果仍为正确, 那终端可以据此判定目标基站为伪基站。另外, 如果目标基站的鉴权结果为错误, 则次目标基站可能为核心网基站, 则终端可以继续通过第一鉴权参数请求驻留于上述核心网基站, 从而实现业务通信。

在上述技术方案中, 优选地, 判断单元还用于: 在获取反馈指令为鉴权失败指令时, 判定目标基站是核心网基站; 发送单元还用于: 将第一鉴权参数发送至核心网基站, 以供核心网基站根据鉴权随机参数和第一鉴权参数判断终端是否具有驻留权限; 网络驻留系统还包括: 选择单元, 用于在获取核心网基站发送的鉴权成功指令后, 根据核心网基站的小区的信道
20 质量选择驻留的小区。

在该技术方案中, 通过获取目标基站的反馈指令为鉴权失败, 判定目标基站为非伪基站, 通过向目标基站发送正确的鉴权参数获取驻留权限, 实现了终端在核心网基站的网络驻留, 保证了终端网络驻留的安全性和通讯的流畅性。

而在终端获取目标基站的反馈指令为鉴权成功时, 进一步地根据小区重选准确确定驻留的基站, 例如, 小区选择遵循 C1 准则, 即小区选择的 C1 值 $C1 > 0$ 时允许驻留:

$C1 = (A - \text{Max}(B, 0))$, 其中, $\text{Max}(B, 0)$ 表示取 B 和 0 两个数据中的最大值

$A = \text{RLA_C-RXLEV_ACCESS_MIN}$;

$B = \text{MS_TXPWR_MAX_CCH-P}$,

其中，C1 表征小区选择判断准则，RLA_C 表征测量小区的平均接收信号电平（average of received signal level）值，RXLEV_ACCESS_MIN 表征网络允许的终端最小接入功率等级。MS_TXPWR_MAX_CCH 表征网络允许的终端最大发射功率等级。P 表征终端最大射频发射功率。

5 在上述技术方案中，优选地，还包括：检测单元，用于在终端驻留核心网基站的小区后，检测终端是否移动至所述核心网基站的小区以外的区域；确定单元，用于在检测到终端移动至核心网基站的小区以外的区域时，确定位置区更新的触发条件成立。

10 在该技术方案中，通过检测终端的位置变化不等于预设位置变化值时，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

15 具体地，小区重选的目的是选择属于这个 PLMN 中信号最好的小区进行驻留，当终端处于高速移动状态时，终端驻留的服务小区质量会由于距离的增加而降低，当下降到规定的门限值时，即服务小区 $C2 < \text{邻区 } C2$ ，且持续小于 5s 以上，将触发小区重选。

 在上述任一项技术方案中，优选地，判断单元还用于：在获取反馈指令为鉴权成功指令时，判定目标基站是伪基站；发送单元还用于：确定伪基站的工作频点，将位置区更新请求发送至除伪基站以外的基站。

20 在该技术方案中，通过获取目标基站的反馈指令为鉴权成功，判定该目标基站为伪基站，防止了用户终端与伪基站之间的通讯，降低了用户遭到短信和电话骚扰以及诈骗的风险。

25 具体地，伪基站为了让用户驻留，通常不会进行鉴权，因此无论用户终端发送的鉴权参数是否为通过鉴权算法生成的正确结果，伪基站均会将鉴权成功的反馈指令发送至用户终端，因此将随机生成的与根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成的正确鉴权参数不同的错误鉴权参数发送至目标基站，即可判定该基站是否为伪基站。

 在上述任一项技术方案中，优选地，确定单元还用于：确定预存储的驻留更新周期；确定单元还用于：在终端驻留小区后，终端的运行时间大于或等于驻留更新周期时，确定位置区更新的触发条件成立。

30 在该技术方案中，通过终端的运行时间大于或等于驻留更新周期，触

发终端进行小区重选,保证了终端网络信号的强度,提高了通话的流畅性,提升了用户通话体验。

具体地,对于同等优先级频点/同频,采用同频小区重选的 R 准则至少持续 Treselection (小区重选定时器时长) 时间;对于低优先级频率的小区重选,当驻留原小区时间超过 1s,且服务小区的 s 值小于预设的门限,并且低优先级频率小区的 s 值大于预设的门限,且持续时间超过 Treselection,进行重选。

根据本发明第三方面,还提出了一种终端,包括通信总线、输入装置、输出装置、存储器以及处理器,其中:

10 所述通信总线,用于实现所述输入装置、输出装置、存储器以及处理器之间的连接通信;

所述输入装置,用于获取目标基站对第二鉴权参数的反馈指令;

所述输出装置,用于发送位置区更新请求,以及第二鉴权参数;

15 所述存储器中存储一组程序代码,且所述终端调用所述存储器中存储的程序代码,用于执行以下操作:

所述处理器在检测到位置区更新的触发条件成立时,获取终端所在区域的基站的工作频点;

所述输出装置将位置区更新请求发送至所述工作频点对应的目标基站;

所述处理器获取所述目标基站反馈的鉴权随机参数;

20 所述处理器根据所述终端的用户身份识别卡的标识信息、所述鉴权随机参数和指定鉴权算法生成第一鉴权参数,并生成与所述第一鉴权参数不同的第二鉴权参数;

所述输出装置将所述第二鉴权参数发送至所述目标基站;

25 所述处理器根据所述目标基站对所述第二鉴权参数的反馈指令,判断所述目标基站是伪基站或核心网基站。

可选的,所述处理器根据所述目标基站对所述第二鉴权参数的反馈指令,判断所述目标基站是伪基站或核心网基站,具体包括以下步骤:

所述处理器在获取所述反馈指令为鉴权失败指令时,判定所述目标基站是核心网基站;

所述输出装置将所述第一鉴权参数发送至所述核心网基站，以供所述核心网基站根据所述鉴权随机参数和所述第一鉴权参数判断所述终端是否具有驻留权限；

5 在所述输入装置获取所述核心网基站发送的鉴权成功指令后，所述处理器根据所述核心网基站的小区的信道质量选择驻留的小区。

可选的，还包括：

所述处理器在所述终端驻留所述核心网基站的小区后，检测所述终端是否移动至所述核心网基站的小区以外的区域；

10 所述处理器在检测到所述终端移动至所述核心网基站的小区以外的区域时，确定所述位置区更新的触发条件成立。

可选的，还包括：

在所述输入装置获取所述反馈指令为鉴权成功指令时，所述处理器判定所述目标基站是伪基站；

15 所述处理器确定所述伪基站的工作频点，将位置区更新请求发送至除所述伪基站以外的基站。

可选的，还包括：

所述处理器确定预存储的驻留更新周期；

所述处理器在所述终端驻留小区后，所述终端的运行时间大于或等于所述驻留更新周期时，确定所述位置区更新的触发条件成立。

20 通过以上技术方案，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

25 附图说明

图 1 示出了根据本发明的实施例的网络驻留方法的示意图；

图 2 示出了根据本发明的实施例的网络驻留系统的示意框图；

图 3 示出了根据本发明的实施例的终端的示意框图；

图 4 示出了根据本发明的一个实施例的网络驻留方案的示意图；

30 图 5 示出了根据本发明的另一个实施例的网络驻留方案的示意图

图 6 示出了根据本发明的实施例的网络驻留方案的示意图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用第三方不同于在此描述的第三方方式来实现，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的实施例的网络驻留方法的示意图。

如图 1 所示，根据本发明的实施例的网络驻留方法，包括：步骤 102，在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；步骤 104，将位置区更新请求发送至工作频点对应的目标基站；步骤 106，获取目标基站反馈的鉴权随机参数；步骤 108，根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与第一鉴权参数不同的第二鉴权参数；步骤 110，将第二鉴权参数发送至目标基站；步骤 112，根据目标基站对第二鉴权参数的反馈指令，判断目标基站是伪基站或核心网基站。

在该技术方案中，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

具体地，空闲状态下的用户终端需要完成的过程包括 PLMN (Public Land Mobile Network, 公共陆地移动网络) 选择，小区选择/重选、位置登记等，一旦完成驻留，用户终端可以读取系统信息 (如驻留、接入和重选相关信息、位置区域信息等)，读取寻呼信息，发起连接建立过程。

其中，第一鉴权参数生成的一种方式是根据 SIM 卡 (Subscriber Identity Module) 的标识信息、获取来自网络的鉴权随机参数和指定鉴权算法 (取自于核心网基站和 SIM 卡采用的通信协议)。但是，终端在接入网络之前，生成与第一鉴权参数不同的第二鉴权参数，也即第二鉴权参数对

于核心网基站而言是不能被识别的错误参数。如果目标基站在接收错误参数的前提下，对终端的鉴权结果仍为正确，那终端可以据此判定目标基站为伪基站。另外，如果目标基站的鉴权结果为错误，则此目标基站可能为核心网基站，则终端可以继续通过第一鉴权参数请求驻留于上述核心网基站，从而实现业务通信。

在上述技术方案中，优选地，根据目标基站对第二鉴权参数的反馈指令，判断目标基站是伪基站或核心网基站，具体包括以下步骤：在获取反馈指令为鉴权失败指令时，判定目标基站是核心网基站；将第一鉴权参数发送至核心网基站，以供核心网基站根据鉴权随机参数和第一鉴权参数判断终端是否具有驻留权限；在获取核心网基站发送的鉴权成功指令后，根据核心网基站的小区的信道质量选择驻留的小区。

在该技术方案中，通过获取目标基站的反馈指令为鉴权失败，判定目标基站为非伪基站，通过向目标基站发送正确的鉴权参数获取驻留权限，实现了终端在核心网基站的网络驻留，保证了终端网络驻留的安全性和通讯的流畅性。

而在终端获取目标基站的反馈指令为鉴权成功时，进一步地根据小区重选准确确定驻留的基站，

例如，小区选择遵循 C1 准则，即小区选择的 C1 值 $C1 > 0$ 时允许驻留：

$C1 = (A - \text{Max}(B, 0))$ ，其中， $\text{Max}(B, 0)$ 表示取 B 和 0 两个数据中的最大值
 $A = \text{RLA_C} - \text{RXLEV_ACCESS_MIN}$ ；

$B = \text{MS_TXPWR_MAX_CCH} - P$ ，

其中，C1 表征小区选择判断准则，RLA_C 表征测量小区的平均接收信号电平（average of received signal level）值，RXLEV_ACCESS_MIN 表征网络允许的终端最小接入功率等级。MS_TXPWR_MAX_CCH 表征网络允许的终端最大发射功率等级。P 表征终端最大射频发射功率。

在上述技术方案中，优选地，还包括：在终端驻留核心网基站的小区后，检测终端是否移动至核心网基站的小区以外的区域；在检测到终端移动至核心网基站的小区以外的区域时，确定位置区更新的触发条件成立。

在该技术方案中，通过检测终端的位置变化大于或等于预设位置变化

值时，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

具体地，小区重选的目的是选择属于这个 PLMN 中信号最好的小区进行驻留，当终端处于高速移动状态时，终端驻留的服务小区质量会由于距离的增加而降低，当下降到规定的门限值时，即服务小区 $C2 < \text{邻区 } C2$ ，且持续小于 5s 以上，将触发小区重选。

在上述任一项技术方案中，优选地，还包括：在获取反馈指令为鉴权成功指令时，判定目标基站是伪基站；确定伪基站的工作频点，将位置区更新请求发送至除伪基站以外的基站。

10 在该技术方案中，通过获取目标基站的反馈指令为鉴权成功，判定该目标基站为伪基站，防止了用户终端与伪基站之间的通讯，降低了用户遭到短信和电话骚扰以及诈骗的风险。

具体地，伪基站为了让用户驻留，通常不会进行鉴权，因此无论用户终端发送的鉴权参数是否为通过鉴权算法生成的正确结果，伪基站均会将鉴权成功的反馈指令发送至用户终端，因此将随机生成的与根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成的正确鉴权参数不同的错误鉴权参数发送至目标基站，即可判定该基站是否为伪基站。

在上述任一项技术方案中，优选地，还包括：确定预存储的驻留更新周期；在终端驻留小区后，终端的运行时间大于或等于驻留更新周期时，20 确定位置区更新的触发条件成立。

在该技术方案中，通过终端的运行时间大于或等于驻留更新周期，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

具体地，对于同等优先级频点/同频，采用同频小区重选的 R 准则至少持续 Treselection（小区重选定时器时长）时间；对于低优先级频率的小区重选，当驻留原小区时间超过 1s，且服务小区的 s 值小于预设的门限，并且低优先级频率小区的 s 值大于预设的门限，且持续时间超过 Treselection，进行重选。

根据本发明第二方面，还提出了一种网络驻留系统 200，包括：获取

单元 202, 用于在检测到位置区更新的触发条件成立时, 获取终端所在区域的基站的工作频点; 发送单元 204, 用于将位置区更新请求发送至工作频点对应的目标基站; 获取单元 202 还用于: 获取目标基站反馈的鉴权随机参数; 网络驻留系统还包括: 生成单元 206, 用于根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数, 并生成与第一鉴权参数不同的第二鉴权参数; 发送单元 204 还用于: 将第二鉴权参数发送至目标基站; 网络驻留系统还包括: 判断单元 208, 用于根据目标基站对第二鉴权参数的反馈指令, 判断目标基站是伪基站或核心网基站。

- 10 在该技术方案中, 通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令, 实现了由终端对网络的鉴权甄别和准确驻留, 减少了用户终端驻留伪基站的可能性, 降低了伪基站对用户终端的通信业务的干扰, 提升了用户终端使用的安全性。

- 15 具体地, 空闲状态下的用户终端需要完成的过程包括 PLMN (Public Land Mobile Network, 公共陆地移动网络) 选择, 小区选择/重选、位置登记等, 一旦完成驻留, 用户终端可以读取系统信息 (如驻留、接入和重选相关信息、位置区域信息等), 读取寻呼信息, 发起连接建立过程。

- 其中, 第一鉴权参数生成的一种方式是根据 SIM 卡 (Subscriber Identity Module) 的标识信息、获取来自网络的鉴权随机参数和指定鉴权算法 (取自于核心网基站和 SIM 卡采用的通信协议)。但是, 终端在接入网络之前, 生成与第一鉴权参数不同的第二鉴权参数, 也即第二鉴权参数对于核心网基站而言是不能被识别的错误参数。如果目标基站在接收错误参数的前提下, 对终端的鉴权结果仍为正确, 那终端可以据此判定目标基站为伪基站。另外, 如果目标基站的鉴权结果为错误, 则此目标基站可能为核心网基站, 则终端可以继续通过第一鉴权参数请求驻留于上述核心网基站, 从而实现业务通信。

在上述技术方案中, 优选地, 判断单元 208 还用于: 在获取反馈指令为鉴权失败指令时, 判定目标基站是核心网基站; 发送单元 204 还用于: 将第一鉴权参数发送至核心网基站, 以供核心网基站根据鉴权随机参数和

第一鉴权参数判断终端是否具有驻留权限；网络驻留系统还包括：选择单元 210，用于在获取核心网基站发送的鉴权成功指令后，根据核心网基站的小区信道质量选择驻留的小区。

在该技术方案中，通过获取目标基站的反馈指令为鉴权失败，判定目标基站为非伪基站，通过向目标基站发送正确的鉴权参数获取驻留权限，实现了终端在核心网基站的网络驻留，保证了终端网络驻留的安全性和通讯的流畅性。

而在终端获取目标基站的反馈指令为鉴权成功时，进一步地根据小区重选准确确定驻留的基站，例如，小区选择遵循 C1 准则，即小区选择的 C1 值 $C1 > 0$ 时允许驻留：

$C1 = (A - \text{Max}(B, 0))$ ，其中， $\text{Max}(B, 0)$ 表示取 B 和 0 两个数据中的最大值 $A = \text{RLA_C} - \text{RXLEV_ACCESS_MIN}$ ；

$B = \text{MS_TXPWR_MAX_CCH} - P$ ，

其中，C1 表征小区选择判断准则，RLA_C 表征测量小区的平均接收信号电平（average of received signal level）值，RXLEV_ACCESS_MIN 表征网络允许的终端最小接入功率等级。MS_TXPWR_MAX_CCH 表征网络允许的终端最大发射功率等级。P 表征终端最大射频发射功率。

在上述技术方案中，优选地，还包括：检测单元 212，用于在终端驻留核心网基站的小区后，检测终端是否移动至核心网基站的小区以外的区域值；确定单元 214，用于在检测到终端移动至核心网基站的小区以外的区域时，确定位置区更新的触发条件成立。

在该技术方案中，通过检测终端的位置变化大于或等于预设位置变化值时，触发终端进行小区重选，保证了终端网络信号的强度，提高了通话的流畅性，提升了用户通话体验。

具体地，小区重选的目的是选择属于这个 PLMN 中信号最好的小区进行驻留，当终端处于高速移动状态时，终端驻留的服务小区质量会由于距离的增加而降低，当下降到规定的门限值时，即服务小区 $C2 < \text{邻区 } C2$ ，且持续小于 5s 以上，将触发小区重选。

在上述任一项技术方案中，优选地，判断单元 208 还用于：在获取反

馈指令为鉴权成功指令时,判定目标基站是伪基站;发送单元 204 还用于:确定伪基站的工作频点,将位置区更新请求发送至除伪基站以外的基站。

在该技术方案中,通过获取目标基站的反馈指令为鉴权成功,判定该目标基站为伪基站,防止了用户终端与伪基站之间的通讯,降低了用户遭到短信和电话骚扰以及诈骗的风险。

具体地,伪基站为了让用户驻留,通常不会进行鉴权,因此无论用户终端发送的鉴权参数是否为通过鉴权算法生成的正确结果,伪基站均会将鉴权成功的反馈指令发送至用户终端,因此将随机生成的与根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成的正确鉴权参数不同的错误鉴权参数发送至目标基站,即可判定该基站是否为伪基站。

在上述任一项技术方案中,优选地,确定单元 214 还用于:确定预存储的驻留更新周期;确定单元 214 还用于:在终端驻留小区后,终端的运行时间大于或等于驻留更新周期时,确定位置区更新的触发条件成立。

在该技术方案中,通过终端的运行时间大于或等于驻留更新周期,触发终端进行小区重选,保证了终端网络信号的强度,提高了通话的流畅性,提升了用户通话体验。

具体地,对于同等优先级频点/同频,采用同频小区重选的 R 准则至少持续 Treselection (小区重选定时器时长) 时间;对于低优先级频率的小区重选,当驻留原小区时间超过 1s,且服务小区的 s 值小于预设的门限,并且低优先级频率小区的 s 值大于预设的门限,且持续时间超过 Treselection,进行重选。

图 3 示出了根据本发明的实施例的终端的示意框图。如图 3 所示,根据本发明的实施例的终端,包括通信总线 302、输入装置 303、输出装置 304、存储器 305 以及处理器 301,其中:

所述通信总线 302,用于实现所述输入装置 303、输出装置 304、存储器 305 以及处理器 301 之间的连接通信;

所述输入装置 303,用于获取目标基站对第二鉴权参数的反馈指令;

所述输出装置 304,用于发送位置区更新请求,以及第二鉴权参数;

所述存储器 305 中存储一组程序代码,且所述终端调用所述存储器 305

中存储的程序代码，用于执行以下操作：

所述处理器 301 在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；

5 所述输出装置 304 将位置区更新请求发送至所述工作频点对应的目标基站；

所述处理器 301 获取所述目标基站反馈的鉴权随机参数；

所述处理器 301 根据所述终端的用户身份识别卡的标识信息、所述鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与所述第一鉴权参数不同的第二鉴权参数；

10 所述输出装置 304 将所述第二鉴权参数发送至所述目标基站；

所述处理器 301 根据所述目标基站对所述第二鉴权参数的反馈指令，判断所述目标基站是伪基站或核心网基站。

可选的，所述处理器 301 根据所述目标基站对所述第二鉴权参数的反馈指令，判断所述目标基站是伪基站或核心网基站，具体包括以下步骤：

15 所述处理器 301 在获取所述反馈指令为鉴权失败指令时，判定所述目标基站是核心网基站；

所述输出装置 304 将所述第一鉴权参数发送至所述核心网基站，以供所述核心网基站根据所述鉴权随机参数和所述第一鉴权参数判断所述终端是否具有驻留权限；

20 在所述输入装置 303 获取所述核心网基站发送的鉴权成功指令后，所述处理器 301 根据所述核心网基站的小区的信道质量选择驻留的小区。

可选的，还包括：

所述处理器 301 在所述终端驻留所述核心网基站的小区后，检测所述终端是否移动至所述核心网基站的小区以外的区域；

25 所述处理器 301 在检测到所述终端移动至所述核心网基站的小区以外的区域时，确定所述位置区更新的触发条件成立。

可选的，还包括：

在所述输入装置 303 获取所述反馈指令为鉴权成功指令时，所述处理器 301 判定所述目标基站是伪基站；

所述处理器 301 确定所述伪基站的工作频点，将位置区更新请求发送至除所述伪基站以外的基站。

可选的，还包括：

所述处理器 301 确定预存储的驻留更新周期；

- 5 所述处理器 301 在所述终端驻留小区后，所述终端的运行时间大于或等于所述驻留更新周期时，确定所述位置区更新的触发条件成立。

图 4 和图 5 示出了根据本发明的实施例的网络驻留方案的示意图。

- 10 如图 4 所示，当终端开机后，需要选择一个合适的网络小区驻留，终端根据工作频点确定目标基站 1 和目标基站 2 等，此时为了鉴别目标基站 1 和目标基站 2 是否是伪基站，向目标基站 1 和目标基站 2 发送不同于正
确的第一鉴权参数的第二鉴权参数，由于伪基站为了让终端驻留，不进行鉴权就会向终端发送鉴权成功指令，当用户接收到错误的第二鉴权参数鉴权成功的反馈指令时，则可判定目标基站 1 为伪基站，目标基站 2 是核心网基站，如图 5 所示，终端向目标基站 2 发送正确的第一鉴权参数，鉴权
15 成功后即可驻留在目标基站 1 的网络。

- 20 如图 5 所示，当终端位置的变化大于或等于预设位置变化时，或终端的运行时间大于或等于驻留更新周期时，触发终端进行小区重选，小区重选过程向目标基站 2 发送第一鉴权参数，第一鉴权参数根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成，在不同网络制式下，指定鉴权算法也不同。

实施例一：

- 25 在 2G 网络中，移动用户号码簿号码(MDN, Mobile Directory Number)为主叫用户呼叫一个移动用户时所拨的号码，IMSI (International Mobile Subscriber Identification, 国际移动台标识)是在移动网中唯一识别一个移动用户的号码，以 CDMA (Code Division Multiple Access: 码分多址通信技术)网络 2G 阶段为例，当终端开机登记时使用 CAVE 算法，入参 IMSI、ESN (UIM ID)、SSD-A (共享加密数据)和 RAND (随机数据)，计算得到 AUTHR (计算结果)。终端发送登记信令，包括鉴权数据：RAND、AUTHR。其中，CAVE 算法是蜂窝鉴权和语音加密 (Cellular Authentication
30 Voice Encryption) 算法，是 CDMA 网络授权的鉴权加密算法，A-KEY 是

发布给一个 CDMA 终端的鉴权密钥,网络收到鉴权信令后,使用参数 IMSI、ESN、SSD-A (共享加密数据) 和同一个 RAND (随机数据) 通过 CAVE 算法得到 AUTHR, 然后与终端计算得到的 AUTHR 进行比较, 如果相同, 则鉴权成功。

5 实施例二:

进入 3G 演进阶段后, 3G 演进时存在两条不同的技术路线, 一条是 1xEV-DO (Evolution Data only: CDMA2000 演进第一阶段), 一条是 1xEV-DV (Evolution Data and Voice: CDMA2000 演进第二阶段), 1xEV-DO 的接入鉴权方式采用的是基于 MD5 (Message Digest 5) 算法的 CHAP
10 (Challenge Handshake Authentication Protocol) 鉴权, 1xEV-DO 网络中增加了新的鉴权设备支持 MD5 算法。

实施例三:

进入 LTE (Long Term Evolution, 长期演进) 4G 时代后, 鉴权向量包括 RAND (一个 128bit 的随机数), XERS (一个 64 位的期望响应), AUTH
15 (鉴权令牌), KASME (接入安全管理实体的 K 值), 使用基于 AES-128 循环移位+异或的 Milenage 算法实现鉴权过程。

图 6 示出了根据本发明的实施例的网络驻留方案的示意图。

如图 6 所示, 根据本发明的实施例的网络驻留方案:

步骤 602, 终端开机后搜索基站的工作频点; 步骤 604, 将位置区更新
20 请求发送至目标基站; 步骤 606, 获取目标基站反馈的鉴权随机参数; 步骤 608, 根据终端的用户身份识别卡的标识信息、鉴权随机参数和指定鉴权算法生成第一鉴权参数, 并生成与第一鉴权参数不同第二鉴权参数; 步骤 610, 将第二鉴权参数发送至目标基站; 步骤 612, 判断鉴权是否成功, 若是, 则执行步骤 622, 若否, 则执行步骤 614; 步骤 614, 目标基站是核
25 心网基站; 步骤 616, 将第一鉴权参数发送至核心网基站; 步骤 618, 选择驻留的小区, 并且周期性测量服务小区和邻区信号强度, 计算小区重选准则; 步骤 620, 满足小区重选准则后, 终端强制执行周期性位置区更新; 步骤 622, 目标基站为伪基站; 步骤 624, 将位置区更新请求发送至除伪基站以外的基站, 并循环执行步骤 606。

30 在该技术方案中, 通过将错误的鉴权参数发送至目标基站后得到目标

基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

5 以上结合附图详细说明了本发明的技术方案，考虑到相关技术中如何实现终端对网络的甄别和准确驻留的技术问题，本发明提出了一种新的网络驻留方案，通过将错误的鉴权参数发送至目标基站后得到目标基站的反馈指令，实现了由终端对网络的鉴权甄别和准确驻留，减少了用户终端驻留伪基站的可能性，降低了伪基站对用户终端的通信业务的干扰，提升了用户终端使用的安全性。

10 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求

1. 一种网络驻留方法，适用于终端，其特征在于，包括：

在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；

5 将位置区更新请求发送至所述工作频点对应的目标基站；

获取所述目标基站反馈的鉴权随机参数；

根据所述终端的用户身份识别卡的标识信息、所述鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与所述第一鉴权参数不同的第二鉴权参数；

10 将所述第二鉴权参数发送至所述目标基站；

根据所述目标基站对所述第二鉴权参数的反馈指令，判断所述目标基站是伪基站或核心网基站。

2. 根据权利要求 1 所述的网络驻留方法，其特征在于，根据所述目标基站对所述第二鉴权参数的反馈指令，判断所述目标基站是伪基站或核心

15 网基站，具体包括以下步骤：

在获取所述反馈指令为鉴权失败指令时，判定所述目标基站是核心网基站；

将所述第一鉴权参数发送至所述核心网基站，以供所述核心网基站根据所述鉴权随机参数和所述第一鉴权参数判断所述终端是否具有驻留权限；

20 在获取所述核心网基站发送的鉴权成功指令后，根据所述核心网基站的小区的信道质量选择驻留的小区。

3. 根据权利要求 2 所述的网络驻留方法，其特征在于，还包括：

在所述终端驻留所述核心网基站的小区后，检测所述终端是否移动至所述核心网基站的小区以外的区域；

25 在检测到所述终端移动至所述核心网基站的小区以外的区域时，确定所述位置区更新的触发条件成立。

4. 根据权利要求 1 所述的网络驻留方法，其特征在于，还包括：

在获取所述反馈指令为鉴权成功指令时，判定所述目标基站是伪基站；

确定所述伪基站的工作频点，将位置区更新请求发送至除所述伪基站

以外的基站。

5. 根据权利要求 1 至 4 中任一项所述的网络驻留方法，其特征在于，还包括：

确定预存储的驻留更新周期；

5 在所述终端驻留小区后，所述终端的运行时间大于或等于所述驻留更新周期时，确定所述位置区更新的触发条件成立。

6. 一种网络驻留系统，适用于终端，其特征在于，包括：

获取单元，用于在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；

10 发送单元，用于将位置区更新请求发送至所述工作频点对应的目标基站；

所述获取单元还用于：获取所述目标基站反馈的鉴权随机参数；

所述网络驻留系统还包括：

15 生成单元，用于根据所述终端的用户身份识别卡的标识信息、所述鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与所述第一鉴权参数不同的第二鉴权参数；

所述发送单元还用于：将所述第二鉴权参数发送至所述目标基站；

所述网络驻留系统还包括：

20 判断单元，用于根据所述目标基站对所述第二鉴权参数的反馈指令，判断所述目标基站是伪基站或核心网基站。

7. 根据权利要求 6 所述的网络驻留系统，其特征在于，

所述判断单元还用于：在获取所述反馈指令为鉴权失败指令时，判定所述目标基站是核心网基站；

25 所述发送单元还用于：将所述第一鉴权参数发送至所述核心网基站，以供所述核心网基站根据所述鉴权随机参数和所述第一鉴权参数判断所述终端是否具有驻留权限；

所述网络驻留系统还包括：

选择单元，用于在获取所述核心网基站发送的鉴权成功指令后，根据所述核心网基站的小区的信道质量选择驻留的小区。

8. 根据权利要求 7 所述的网络驻留系统，其特征在于，还包括：

检测单元，用于在所述终端驻留所述核心网基站的小区后，检测所述终端是否移动至所述核心网基站的小区以外的区域；

5 确定单元，用于在检测到所述终端移动至所述核心网基站的小区以外的区域时，确定所述位置区更新的触发条件成立。

9. 根据权利要求 6 所述的网络驻留系统，其特征在于，

所述判断单元还用于：在获取所述反馈指令为鉴权成功指令时，判定所述目标基站是伪基站；

10 所述发送单元还用于：确定所述伪基站的工作频点，将位置区更新请求发送至除所述伪基站以外的基站。

10. 根据权利要求 6 至 9 中任一项所述的网络驻留系统，其特征在于，

所述确定单元还用于：确定预存储的驻留更新周期；

15 所述确定单元还用于：在所述终端驻留小区后，所述终端的运行时间大于或等于所述驻留更新周期时，确定所述位置区更新的触发条件成立。

11. 一种终端，其特征在于，包括通信总线、输入装置、输出装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、输出装置、存储器以及处理器之间的连接通信；

20 所述输入装置，用于获取目标基站对第二鉴权参数的反馈指令；

所述输出装置，用于发送位置区更新请求，以及第二鉴权参数；

所述存储器中存储一组程序代码，且所述终端调用所述存储器中存储的程序代码，用于执行以下操作：

25 所述处理器在检测到位置区更新的触发条件成立时，获取终端所在区域的基站的工作频点；

所述输出装置将位置区更新请求发送至所述工作频点对应的目标基站；

所述处理器获取所述目标基站反馈的鉴权随机参数；

所述处理器根据所述终端的用户身份识别卡的标识信息、所述鉴权随机参数和指定鉴权算法生成第一鉴权参数，并生成与所述第一鉴权参数不

同的第二鉴权参数;

所述输出装置将所述第二鉴权参数发送至所述目标基站;

所述处理器根据所述目标基站对所述第二鉴权参数的反馈指令, 判断所述目标基站是伪基站或核心网基站。

- 5 12. 根据权利要求 11 所述的终端, 其特征在于, 所述处理器根据所述目标基站对所述第二鉴权参数的反馈指令, 判断所述目标基站是伪基站或核心网基站, 具体包括以下步骤:

所述处理器在获取所述反馈指令为鉴权失败指令时, 判定所述目标基站是核心网基站;

- 10 所述输出装置将所述第一鉴权参数发送至所述核心网基站, 以供所述核心网基站根据所述鉴权随机参数和所述第一鉴权参数判断所述终端是否具有驻留权限;

在所述输入装置获取所述核心网基站发送的鉴权成功指令后, 所述处理器根据所述核心网基站的小区的信道质量选择驻留的小区。

- 15 13. 根据权利要求 12 所述的终端, 其特征在于, 还包括:

所述处理器在所述终端驻留所述核心网基站的小区后, 检测所述终端是否移动至所述核心网基站的小区以外的区域;

所述处理器在检测到所述终端移动至所述核心网基站的小区以外的区域时, 确定所述位置区更新的触发条件成立。

- 20 14. 根据权利要求 11 所述的终端, 其特征在于, 还包括:

在所述输入装置获取所述反馈指令为鉴权成功指令时, 所述处理器判定所述目标基站是伪基站;

所述处理器确定所述伪基站的工作频点, 将位置区更新请求发送至除所述伪基站以外的基站。

- 25 15. 根据权利要求 11 至 14 中任一项所述的终端, 其特征在于, 还包括:

所述处理器确定预存储的驻留更新周期;

所述处理器在所述终端驻留小区后, 所述终端的运行时间大于或等于所述驻留更新周期时, 确定所述位置区更新的触发条件成立。

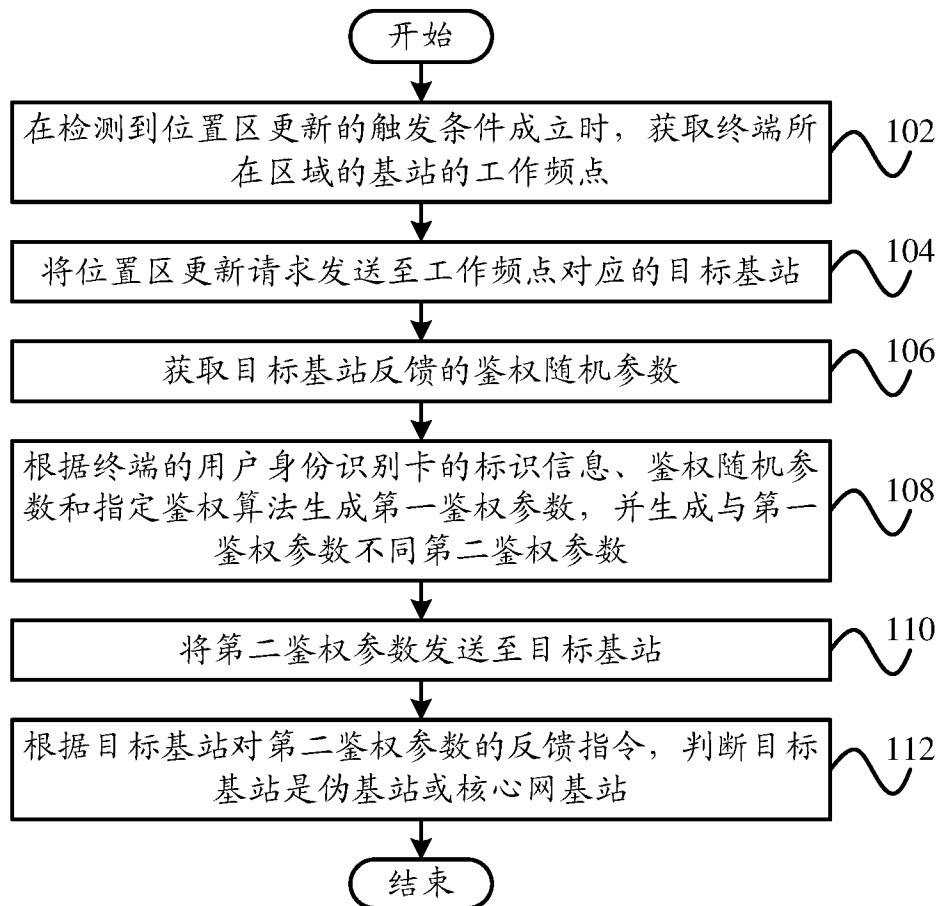


图 1

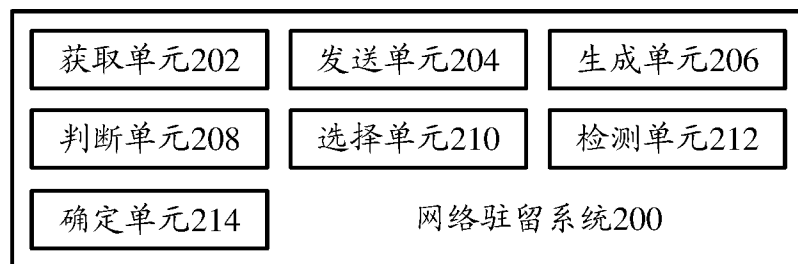


图 2

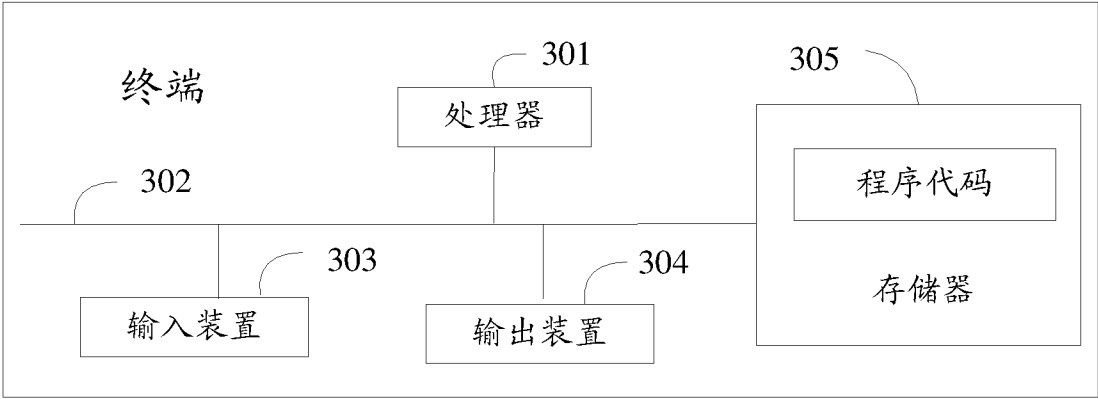


图 3

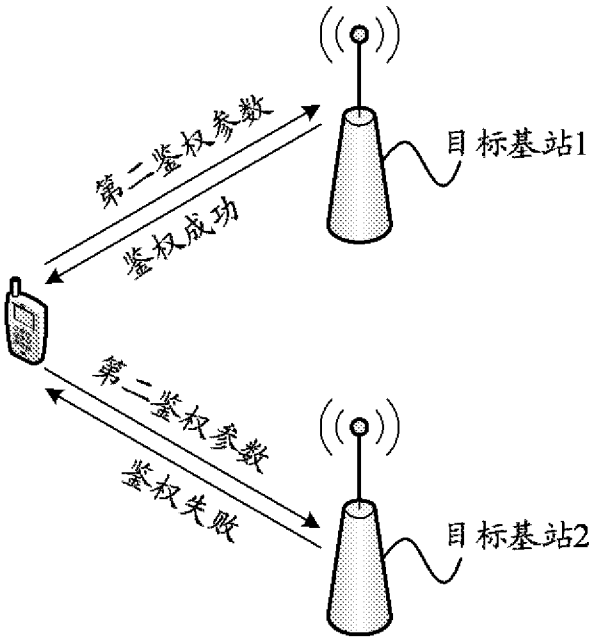


图 4

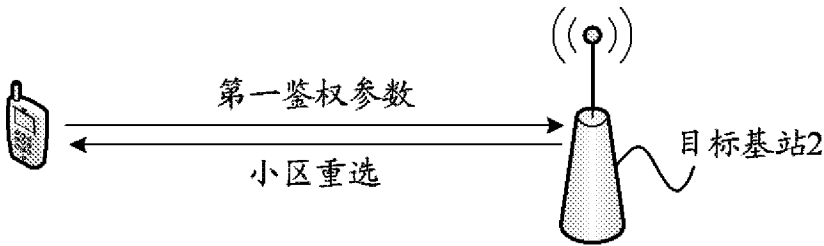


图 5

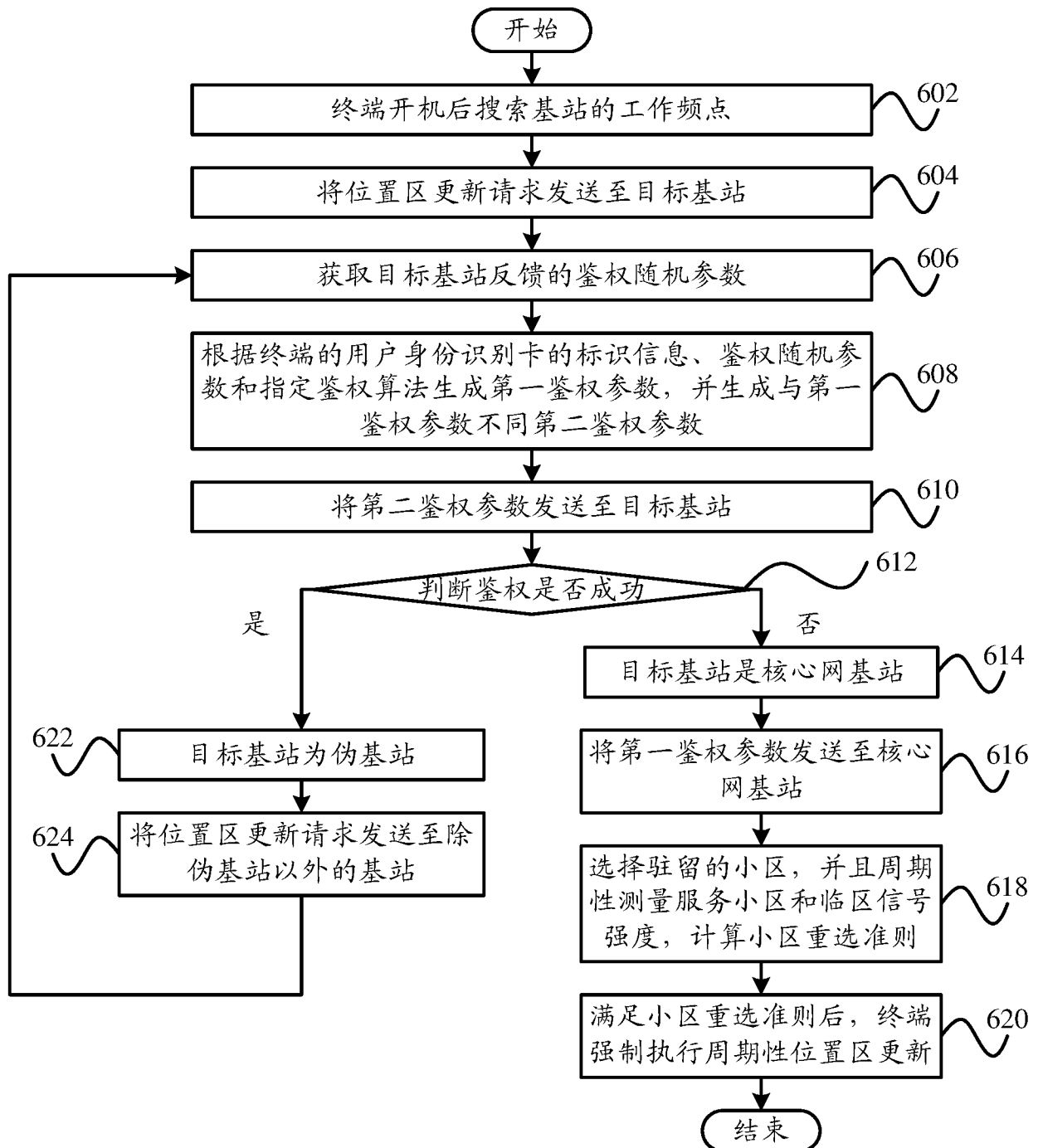


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/080822

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)

H04L; H04W

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)

CNABS; CNTXT; CNKI; VEN: pseudo base station, fake base station, fake, false, base station?, nodeb, authenticat+, parameter?, factor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105101200 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 25 November 2015 (25.11.2015), description, paragraphs [0072]-[0090]	1-15
A	WO 2014154634 A1 (GEMALTO SA), 02 October 2014 (02.10.2014), the whole document	1-15
A	CN 104581732 A (HANGZHOU TELEHEMS ELECTRONICS TECHNOLOGY CO., LTD.), 29 April 2015 (29.04.2015), the whole document	1-15

☐ 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 01 October 2016 (01.10.2016)	Date of mailing of the international search report 02 November 2016 (02.11.2016)
Name and mailing address of the ISA/CN: 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 LI, Xiaoling Telephone No.: (86-10) 62089574

International application No.
PCT/CN2016/080822

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

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) H04L; H04W 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)) CNABS; CNTXT; CNKI; VEN: 伪基站, 假基站, 假, 错, 误, 鉴权, 参数, 因子, fake, false, base station?, nodeb, authenticat+, parameter?, factor														
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>X</td> <td>CN 105101200 A (中国移动通信集团公司) 2015年 11月 25日 (2015 - 11 - 25) 说明书第[0072]-[0090]段</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>WO 2014154634 A1 (GEMALTO SA) 2014年 10月 2日 (2014 - 10 - 02) 全文</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 104581732 A (杭州赫智电子科技有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文</td> <td>1-15</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	X	CN 105101200 A (中国移动通信集团公司) 2015年 11月 25日 (2015 - 11 - 25) 说明书第[0072]-[0090]段	1-15	A	WO 2014154634 A1 (GEMALTO SA) 2014年 10月 2日 (2014 - 10 - 02) 全文	1-15	A	CN 104581732 A (杭州赫智电子科技有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-15
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
X	CN 105101200 A (中国移动通信集团公司) 2015年 11月 25日 (2015 - 11 - 25) 说明书第[0072]-[0090]段	1-15												
A	WO 2014154634 A1 (GEMALTO SA) 2014年 10月 2日 (2014 - 10 - 02) 全文	1-15												
A	CN 104581732 A (杭州赫智电子科技有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-15												
☐ 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> * 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> “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 2016年 10月 1日		国际检索报告邮寄日期 2016年 11月 2日												
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 李晓玲 电话号码 (86-10) 62089574												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/080822

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	105101200	A	2015年 11月 25日	无	
WO	2014154634	A1	2014年 10月 2日	EP 2785090 A1	2014年 10月 1日
CN	104581732	A	2015年 4月 29日	无	