

(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 1 月 4 日 (04.01.2018)



(10) 国际公布号
WO 2018/000787 A1

(51) 国际专利分类号:
H04W 12/12 (2009.01)

(21) 国际申请号: PCT/CN2016/113380

(22) 国际申请日: 2016 年 12 月 30 日 (30.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610486479.3 2016 年 6 月 28 日 (28.06.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATIONS 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: 徐杏绍 (XU, Xingshao); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 郭德英 (GUO, Deying); 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: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路 83 号荣群大厦 9 楼, Guangdong 518109 (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,

(54) Title: TERMINAL, AND METHOD AND SYSTEM FOR IDENTIFYING PSEUDO BASE STATION

(54) 发明名称: 一种终端、伪基站识别方法及系统

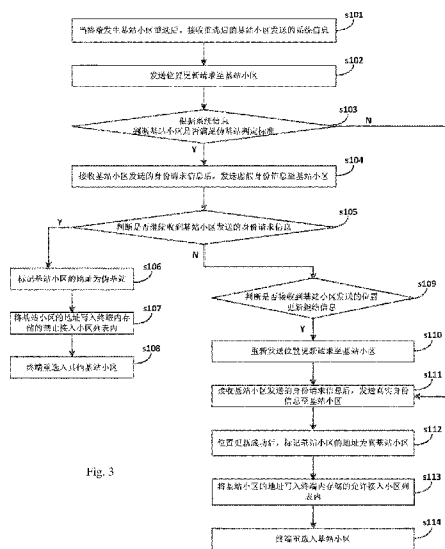


Fig. 3

s101 Upon occurrence of reselection of a base station cell, a terminal receives system information transmitted by a reselected base station cell
s102 Transmit a location update request to the base station cell
s103 Determine, according to the system information, whether the base station cell satisfies a pseudo base station determination criterion
s104 After receiving identification request information transmitted by the base station cell, transmit pseudo identification information to the base station cell
s105 Determine whether the identification request information is continuously received from the base station cell
s106 Mark an address of the base station cell as a pseudo base station
s107 Write the address of the base station cell to an access-prohibited cell list stored in the terminal
s108 The terminal reselects and accesses another base station cell
s109 Determine whether location update rejection information transmitted by the base station cell has been received
s110 Re-transmit a location update request to the base station cell
s111 After receiving identification request information transmitted by the base station cell, transmit authentic identification information to the base station cell
s112 After a successful location update, mark an address of the base station cell as an authentic base station cell
s113 Write the address of the base station cell to an access-permitted cell list stored in the terminal
s114 The terminal reselects and accesses the base station cell

(57) Abstract: Disclosed are a method and system for identifying a pseudo base station applicable to a terminal. The method comprises: upon occurrence of reselection of a base station cell, receiving, by a terminal, system information transmitted by a reselected base station cell; transmitting a location update request to the base station cell; determining, according to the system information, whether the base station cell satisfies a pseudo base station determination criterion, and if so, after receiving identification request information transmitted by the base station cell, transmitting pseudo identification information to the base station cell; determining whether the identification

JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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))。

request information is continuously received from the base station cell, and if so, marking an address of the base station cell as a pseudo base station; and reselecting and accessing, by the terminal, another base station cell. The invention can not only identify a pseudo base station but also prevent information of a terminal user from being disclosed during an identification process, thereby greatly ensuring network security for the terminal user. Also provided is a terminal comprising the above system for identifying a pseudo base station. Since the terminal also has the above advantages, no repetitive description is given thereon.

(57) 摘要: 本发明公开了一种伪基站识别方法及系统, 用于终端, 包括当终端发生基站小区重选后, 接收重选后的基站小区发送的系统信息; 发送位置更新请求至基站小区; 根据系统信息判断基站小区是否满足伪基站判定标准, 如果是, 接收基站小区发送的身份请求信息后, 发送虚假身份信息至基站小区; 判断是否继续收到基站小区发送的身份请求信息, 如果是, 标记基站小区的地址为伪基站; 终端重选入其他基站小区。本发明不仅能够识别伪基站, 同时在识别过程中也避免了终端用户的信息泄露, 极大地保证了终端用户的网络安全性。本发明还提供了一种终端, 包括上述伪基站识别系统, 该终端也具有上述有益效果, 在此不再赘述。

说明书

发明名称：一种终端、伪基站识别方法及系统

- [1] 本申请要求于2016年6月28日提交中国专利局，申请号为201610486479.3、发明名称为“一种终端、伪基站识别方法及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

- [2] 本发明涉及GSM通信技术领域，特别是涉及一种伪基站识别方法及系统。本发明还涉及一种终端。

背景技术

- [3] 伪基站是不法分子伪造的公共移动运营商基站，伪基站通过伪造部分网络参数和加大自身发射功率来吸收周围的手机用户，当手机用户成功驻留伪基站后，伪基站即可获取手机用户的身份信息，随后进行大容量的非法信息传递，进而从中获取非法盈利。参见图1所示，图1为目前的伪基站工作的过程的流程图。
- [4] 而现有GSM（Global System for Mobile Communication，全球移动通信系统）移动通信系统存在单向鉴权的缺陷，即只有网络对终端进行鉴权，而终端无法识别网络身份的合法性，由于无法识别伪基站，用户连接网络时的安全性低，容易受到伪基站的侵扰。
- [5] 因此，如何提供一种能够提高用户的网络安全性的终端、伪基站识别方法及系统是本领域技术人员目前需要解决的问题。

对发明的公开

发明内容

- [6] 本发明的目的是提供一种伪基站识别方法及系统，不仅能够识别伪基站，同时在识别过程中也避免了终端用户的信息泄露，极大地保证了终端用户的网络安全性。本发明的另一目的是提供一种具有上述效果的终端。
- [7] 为解决上述技术问题，本发明提供了一种伪基站识别方法，用于终端，包括：
- [8] 步骤s101：当所述终端发生基站小区重选后，接收重选后的所述基站小区发送的系统信息；

- [9] 步骤s102: 发送位置更新请求至所述基站小区;
- [10] 步骤s103: 根据所述系统信息判断所述基站小区是否满足伪基站判定标准, 如果是, 进入步骤s104;
- [11] 步骤s104: 接收所述基站小区发送的身份请求信息后, 发送虚假身份信息至所述基站小区;
- [12] 步骤s105: 判断是否继续收到所述基站小区发送的身份请求信息, 如果是, 标记所述基站小区的地址为伪基站; 所述终端重选入其他基站小区。
- [13] 优选地, 标记所述基站小区为伪基站后还包括:
- [14] 将所述基站小区的地址写入所述终端内存储的禁止接入小区列表内。
- [15] 优选地, 所述系统信息包括位置区码以及周期性位置更新时间;
- [16] 所述根据所述系统信息判断所述基站小区是否满足伪基站判定标准的过程具体为:
- [17] 当所述终端发生基站小区重选时, 若收到的信号在预设时间内的增大数值超出预设信号阈值;
- [18] 且所述基站小区的所述位置区码超出预设区码范围;
- [19] 且所述基站小区的所述周期性位置更新时间小于预设周期, 则所述基站小区满足所述伪基站判定标准, 否则, 所述基站小区不满足所述伪基站判定标准。
- [20] 优选地, 所述步骤s103后还包括:
- [21] 若所述基站小区不满足伪基站判定标准, 接收所述基站小区发送的身份请求信息后, 发送真实身份信息至所述基站小区;
- [22] 位置更新成功后, 标记所述基站小区的地址为真基站小区, 所述终端重选入所述基站小区。
- [23] 优选地, 所述步骤s105后还包括:
- [24] 若未继续收到所述基站小区发送的身份请求信息, 判断是否接收到所述基站小区发送的位置更新拒绝信息, 如果是, 重新发送位置更新请求至所述基站小区;
- [25] 接收所述基站小区发送的身份请求信息后, 发送真实身份信息至所述基站小区;

- [26] 位置更新成功后，标记所述基站小区的地址为真基站小区，所述终端重选入所述基站小区。
- [27] 优选地，所述标记所述基站小区的地址为真基站小区后还包括：
- [28] 将所述基站小区的地址写入所述终端内存储的允许接入小区列表内。
- [29] 为解决上述技术问题，本发明还提供了一种伪基站识别系统，用于终端，包括：
- [30] 基站信息接收模块，设置为当所述终端发生基站小区重选后，接收重选后的所述基站小区发送的系统信息，并触发位置更新请求发送模块；
- [31] 所述位置更新请求发送模块，设置为发送位置更新请求至所述基站小区；
- [32] 第一判断模块，设置为根据所述系统信息判断所述基站小区是否满足伪基站判定标准，如果是，触发第一身份信息发送模块；
- [33] 所述第一身份信息发送模块，设置为接收所述基站小区发送的身份请求信息后，发送虚假身份信息至所述基站小区；
- [34] 第二判断模块，设置为判断是否继续收到所述基站小区发送的身份请求信息，如果是，标记所述基站小区的地址为伪基站；所述终端重选入其他基站小区。
- [35] 优选地，还包括：
- [36] 伪基站写入模块，设置为当标记所述基站小区的地址为伪基站时，将所述基站小区的地址写入所述终端内存储的禁止接入小区列表内。
- [37] 优选地，所述第一判断模块具体设置为：
- [38] 当所述系统信息包括位置区码以及周期性位置更新时间时，判断所述终端发生基站小区重选时，收到的信号在预设时间内的增大数值是否超出预设信号阈值，以及所述基站小区的所述位置区码是否超出预设区码范围，以及所述基站小区的所述周期性位置更新时间是否小于预设周期，如果是，则所述基站小区满足所述伪基站判定标准，触发所述第一身份信息发送模块；否则，所述基站小区不满足所述伪基站判定标准。
- [39] 优选地，还包括：
- [40] 第二身份信息发送模块，设置为接收所述基站小区发送的身份请求信息后，发送真实身份信息至所述基站小区，并在位置更新后，触发真基站标记模块；其

中，当所述第一判断模块判断所述基站小区不满足所述伪基站判定标准时，触发所述第二身份信息发送模块；

[41] 所述真基站标记模块，设置为标记所述基站小区的地址为真基站小区。

[42] 优选地，还包括：

[43] 第三判断模块，设置为当所述第二判断模块判断未继续收到所述基站小区发送的身份请求信息时，判断是否接收到所述基站小区发送的位置更新拒绝信息，如果是，触发所述位置更新请求发送模块重新发送位置更新请求至所述基站小区；

[44] 所述位置更新请求发送模块重新发送所述位置更新请求并接收到所述基站小区发送的身份请求信息后，触发所述第二身份信息发送模块。

[45] 优选地，还包括：

[46] 真基站写入模块，设置为当标记所述基站小区的地址为真基站小区后，将所述基站小区的地址写入所述终端内存储的允许接入小区列表内。

[47] 为解决上述技术问题，本发明还提供了一种终端，包括以上任一项所述的伪基站识别系统。

[48] 优选地，所述终端具体包括处理器、分别通过接口与所述处理器相连接的输入装置和输出装置以及通过总线与所述处理器相连接的存储器；

[49] 所述伪基站识别系统存储于所述存储器内；

[50] 所述处理器通过所述总线调用所述存储器内的所述伪基站识别系统进行伪基站识别操作。

[51] 本发明提供了一种伪基站识别方法及系统，由于伪基站的目的是为了获取终端用户的身份信息来进行非法信息传递，故本发明中当终端发生基站小区重选后，首先判断一下该基站小区是否可能为伪基站（即基站小区是否满足伪基站判定标准），若可能是，则终端发送虚假身份信息来试探该基站小区，若基站小区仍继续发送身份请求信息，则表明该基站小区为伪基站（真基站小区会发送位置更新拒绝信息）。故本发明不仅能够识别伪基站，同时在识别过程中也避免了终端用户的信息泄露，极大地保证了终端用户的网络安全性。本发明还提供了一种终端，具有上述有益效果，在此不再赘述。

附图说明

- [52] 为了更清楚地说明本发明实施例中的技术方案，下面将对现有技术和实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。
- [53] 图1为目前的伪基站工作的过程的流程图；
- [54] 图2为本发明提供的一种伪基站识别方法的过程的流程图；
- [55] 图3为本发明提供的另一种伪基站识别方法的过程的流程图；
- [56] 图4为本发明提供的一种伪基站识别系统的结构示意图；
- [57] 图5为本发明提供的一种终端的结构示意图。

具体实施方式

- [58] 本发明的核心是提供一种伪基站识别方法及系统，不仅能够识别伪基站，同时在识别过程中也避免了终端用户的信息泄露，极大地保证了终端用户的网络安全。本发明的另一核心是提供一种具有上述效果的终端。
- [59] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。
- [60] 实施例一
- [61] 本发明提供了一种伪基站识别方法，用于终端，参见图2所示，图2为本发明提供的一种伪基站识别方法的过程的流程图；该方法包括：
- [62] 步骤s101：当终端发生基站小区重选后，接收重选后的基站小区发送的系统信息；
- [63] 步骤s102：发送位置更新请求至基站小区；
- [64] 步骤s103：根据系统信息判断基站小区是否满足伪基站判定标准，如果是，进入步骤s104；
- [65] 步骤s104：接收基站小区发送的身份请求信息后，发送虚假身份信息至基站小

区；

[66] 步骤s105：判断是否继续收到基站小区发送的身份请求信息，如果是，标记基站小区的地址为伪基站；终端重选入其他基站小区。

[67] 本发明提供了一种伪基站识别方法，由于伪基站的目的是为了获取终端用户的身份信息来进行非法信息传递，故本发明中当终端发生基站小区重选后，首先判断一下该基站小区是否可能为伪基站（即基站小区是否满足伪基站判定标准），若可能是，则终端发送虚假身份信息来试探该基站小区，若基站小区仍继续发送身份请求信息，则表明该基站小区为伪基站（真基站小区会发送位置更新拒绝信息）。故本发明不仅能够识别伪基站，同时在识别过程中也避免了终端用户的信息泄露，极大地保证了终端用户的网络安全性。

[68] 实施例二

[69] 基于实施例一的基础上，本发明还提供了另一种伪基站识别方法。参见图3所示，图3为本发明提供的另一种伪基站识别方法的过程的流程图；该方法包括：

[70] 步骤s101：当终端发生基站小区重选后，接收重选后的基站小区发送的系统信息；

[71] 这里的终端为手机或平板电脑等，当然，本发明对此不作限定。

[72] 伪基站一般工作在GSM900频段，只有一个GSM频点，即仅包括一个基站小区，伪基站能将自身的频点更改为现网频点，同时可调整自身的发射功率。由于空闲状态下终端一直测量周边邻区信号，当邻区信号强度大于目前所位于的基站小区时就重选该邻区。故伪基站工作时，通过加大发射功率，即可迅速使周边空闲状态的终端重选到伪基站内。

[73] 步骤s102：发送位置更新请求至基站小区；

[74] 位置更新请求（Location update request）是当终端发现当前位置区改变时，向网络发送的、用以告知网络当前所在的位置的请求信息。

[75] 步骤s103：根据系统信息判断基站小区是否满足伪基站判定标准，如果是，进入步骤s104；如果否，进入步骤s111；

[76] 其中，系统信息包括位置区码（Location area code, LAC）以及周期性位置更新时间T3212；

- [77] 本发明中根据系统信息判断基站小区是否满足伪基站判定标准的过程具体为：
- [78] 当终端发生基站小区重选时，若收到的信号在预设时间内的增大数值超出预设信号阈值；
- [79] 且基站小区的位置区码超出预设区码范围；
- [80] 且基站小区的周期性位置更新时间小于预设周期，则基站小区满足伪基站判定标准，否则，基站小区不满足伪基站判定标准。
- [81] 可以理解的是，每个基站小区都会有单独的位置区码，但是真基站小区的位置区码均位于一定的范围内（可将该范围设置为预设区码范围），而伪基站的位置区码通常不属于真基站小区的位置区码范围，故通过判断重选后的基站小区的位置区码是否位于预设区码范围，即可初步判断该基站小区是否可能为伪基站。
- [82] 另外，伪基站开始工作时，为吸引终端重选过去，会突然增大发射功率，即伪基站的发射信号要强于真基站小区的发射信号，且伪基站的发射信号通常为突然出现，从而导致终端接收到的信号会在较短的时间内突然增强，故可以设置一个较短的预设时间（例如几秒钟），并判断终端接收到的信号在该预设时间内的增大数值是否超出预设信号阈值，从而初步判断该基站小区是否可能为伪基站。
- [83] 不同的基站小区会设置有不同的周期性位置更新时间，当终端位置更新后，即会启动终端所位于的基站小区内设置的T3212定时器，若终端一直位于该基站小区，T3212定时器一旦到达预定时间，则会控制终端向网络侧发送位置更新请求来报告当前位置，避免网络侧失去终端位置而无法与终端进行连接。一般真基站小区的周期性位置更新时间较长，例如为60分钟或120分钟。而由于终端接入伪基站后会导致终端无法正常使用运营商提供的服务，终端用户一般会暂时脱网，故为了避免用户发现异常，用户接入伪基站的时间一般较短，即伪基站的周期性位置更新时间较短（例如为6分钟），一旦T3212定时器的预定时间到达，伪基站则会释放终端，终端重新发送位置更新请求，重新驻留在真基站小区内。故通过判断重选后的基站小区的周期性位置更新时间，若其小于预设周期，则可初步判断该基站小区是否可能为伪基站。

- [84] 为了提高伪基站判定标准的准确性，本发明只有在以上三种情况均出现的情况下才判定重选后的基站小区符合伪基站判定标准，进而启动后续流程。
- [85] 另外，本发明不限定预设时间、预设信号阈值、预设区码范围以及预设周期的数值，工作人员可根据实际情况自行设定。
- [86] 步骤s104：接收基站小区发送的身份请求信息后，发送虚假身份信息至基站小区；
- [87] 其中，这里的身份请求信息（Identity request）是指基站小区用来向终端索取IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码）、TMSI（Temporary Mobile Subscriber Identity，临时识别码）、IMEI（International Mobile Equipment Identity，国际移动设备标识）等信息进行鉴权来核实终端用户的身份是否可以接入网络的一种请求信息。
- [88] 可以理解的是，在该基站小区可能为伪基站的情况下，发送虚假身份信息来试探该基站小区，进一步避免了用户身份信息的泄露，提高了网络安全性。
- [89] 步骤s105：判断是否继续收到基站小区发送的身份请求信息，如果是，进入步骤s106；如果否，进入步骤s109；
- [90] 步骤s106：标记基站小区的地址为伪基站；
- [91] 步骤s107：将基站小区的地址写入终端内存储的禁止接入小区列表内；
- [92] 该操作使终端在再次重选入该伪基站时，能够及时发现，断开连接，而不必再进行上述操作，提高了伪基站的识别效率。
- [93] 步骤s108：终端重选入其他基站小区；
- [94] 步骤s109：判断是否接收到基站小区发送的位置更新拒绝信息，如果是，进入步骤s110；
- [95] 可以理解的是，真基站小区在接收到终端发送的身份信息后，若该信息为虚假身份信息，真基站小区会发送位置更新拒绝信息（Location update reject）；若该信息为真实身份信息，真基站小区会发送位置更新接受信息（Location update accept），从而成功进行位置更新。
- [96] 步骤s110：重新发送位置更新请求至基站小区；

- [97] 步骤s111: 接收基站小区发送的身份请求信息后, 发送真实身份信息至基站小区;
- [98] 步骤s112: 位置更新成功后, 标记基站小区的地址为真基站小区;
- [99] 步骤s113: 将基站小区的地址写入终端内存储的允许接入小区列表内;
- [100] 该操作使终端在再次重选入该真基站小区时, 能够及时发现, 而不必再进行上述判断操作, 提高了终端接入基站小区的效率。
- [101] 步骤s114: 终端重选入基站小区。
- [102] 与实施例一相比, 本实施例还增加了当判断基站小区为真基站时, 发送真实身份信息至基站小区的步骤, 使得终端在伪基站识别流程完成后正常接入真基站小区, 避免了伪基站识别流程对终端正常联网的影响; 且本实施例在识别完成后还增加了将该基站小区的地址对应写入终端内存储的禁止接入小区列表或允许接入小区列表内, 使终端在再次重选至该基站小区后, 能够及时了解该基站小区的类型, 而不必再重复进行识别操作, 提高了终端接入基站小区的工作效率。
- [103] 需要注意的是, 本实施例中的各个步骤可以根据实际需要进行顺序调整、合并和删减。
- [104] 本发明还提供了一种伪基站识别系统, 用于终端, 参见图4所示, 图4为本发明提供的一种伪基站识别系统的结构示意图。该系统包括:
- [105] 基站信息接收模块11, 设置为当终端发生基站小区重选后, 接收重选后的基站小区发送的系统信息, 并触发位置更新请求发送模块12;
- [106] 位置更新请求发送模块12, 设置为发送位置更新请求至基站小区;
- [107] 第一判断模块13, 设置为根据系统信息判断基站小区是否满足伪基站判定标准, 如果是, 触发身份信息发送模块14;
- [108] 第一身份信息发送模块14, 设置为接收基站小区发送的身份请求信息后, 发送虚假身份信息至基站小区;
- [109] 第二判断模块15, 设置为判断是否继续收到基站小区发送的身份请求信息, 如果是, 标记基站小区的地址为伪基站; 终端重选入其他基站小区。
- [110] 其中, 这里的第一判断模块13具体设置为:

- [111] 当系统信息包括位置区码以及周期性位置更新时间时，判断终端发生基站小区重选时，收到的信号在预设时间内的增大数值是否超出预设信号阈值，以及基站小区的位置区码是否超出预设区码范围，以及基站小区的周期性位置更新时间是否小于预设周期，如果是，则基站小区满足伪基站判定标准，触发第一身份信息发送模块14；否则，基站小区不满足伪基站判定标准。
- [112] 作为优选地，该系统还包括：
- [113] 伪基站写入模块16，设置为当标记基站小区的地址为伪基站时，将基站小区的地址写入终端内存储的禁止接入小区列表内。
- [114] 作为优选地，该系统还包括：
- [115] 第二身份信息发送模块18，设置为接收基站小区发送的身份请求信息后，发送真实身份信息至基站小区，并在位置更新后，触发真基站标记模块19；其中，当第一判断模块13判断基站小区不满足伪基站判定标准时，触发第二身份信息发送模块18；
- [116] 真基站标记模块19，设置为标记基站小区的地址为真基站小区。
- [117] 进一步的，该系统还包括：
- [118] 第三判断模块17，设置为当第二判断模块15判断未继续收到基站小区发送的身份请求信息时，判断是否接收到基站小区发送的位置更新拒绝信息，如果是，触发位置更新请求发送模块12重新发送位置更新请求至基站小区；
- [119] 位置更新请求发送模块12重新发送位置更新请求并接收到基站小区发送的身份请求信息后，触发第二身份信息发送模块18。
- [120] 作为优选地，该系统还包括：
- [121] 真基站写入模块20，设置为当标记基站小区的地址为真基站小区时，将基站小区的地址写入终端内存储的允许接入小区列表内。
- [122] 本发明提供了一种伪基站识别系统，由于伪基站的目的是为了获取终端用户的身份信息来进行非法信息传递，故本发明中当终端发生基站小区重选后，首先判断一下该基站小区是否可能为伪基站（即基站小区是否满足伪基站判定标准），若可能是，则终端发送虚假身份信息来试探该基站小区，若基站小区仍继续发送身份请求信息，则表明该基站小区为伪基站（真基站小区会发送位置更

新拒绝信息)。故本发明不仅能够识别伪基站,同时在识别过程中也避免了终端用户的信息泄露,极大地保证了终端用户的网络安全性。

[123] 需要注意的是,本发明实施例中的各个模块可以根据实际需要进行合并、划分和删减。

[124] 本发明还提供了一种终端,参见图5所示,图5为本发明提供的一种终端的结构示意图;该终端包括上述伪基站识别系统。

[125] 其中,终端具体包括处理器31、分别通过接口32与处理器31相连接的输入装置35和输出装置36以及通过总线33与处理器31相连接的存储器34;

[126] 伪基站识别系统存储于存储器内;

[127] 处理器通过总线调用存储器内的伪基站识别系统进行伪基站识别操作。

[128] 可以理解的是,图5所示的终端可用于实施上述图2~图3所示的本发明各实施例实现的方法,为了便于说明,仅示出了与本发明各实施例相关的部分,具体技术细节未揭示的,请参照图2~图3所示的本发明各实施例。

[129] 其中,存储器34用于存储伪基站识别系统,该伪基站识别系统为一组程序代码。

[130] 处理器31用于调用该程序代码,来执行以下操作:

[131] 当终端发生基站小区重选后,通过输入装置35接收重选后的基站小区发送的系统信息;

[132] 通过输出装置36发送位置更新请求至基站小区;

[133] 根据系统信息判断基站小区是否满足伪基站判定标准,如果是,通过输入装置35接收基站小区发送的身份请求信息后,通过输出装置36发送虚假身份信息至基站小区;

[134] 判断输入装置35是否继续收到基站小区发送的身份请求信息,如果是,标记基站小区的地址为伪基站;终端重选入其他基站小区。

[135] 作为一种可选的实施方式,处理器31用于调用该程序代码,还用于执行以下操作:

[136] 当标记基站小区的地址为伪基站后,将基站小区的地址写入终端内存储的禁止接入小区列表内。

- [137] 作为一种可选的实施方式，处理器31用于调用该程序代码，还用于执行以下操作：
- [138] 若判断基站小区不满足伪基站判定标准，通过输入装置35接收基站小区发送的身份请求信息后，发送真实身份信息至基站小区；
- [139] 位置更新成功后，标记基站小区的地址为真基站小区；终端重选入基站小区。
- [140] 作为一种可选的实施方式，处理器31用于调用该程序代码，还用于执行以下操作：
- [141] 若通过输入装置35未继续收到基站小区发送的身份请求信息，判断通过输入装置35是否接收到基站小区发送的位置更新拒绝信息，如果是，通过输出装置36重新发送位置更新请求至基站小区；
- [142] 通过输入装置35接收基站小区发送的身份请求信息后，发送真实身份信息至基站小区；
- [143] 位置更新成功后，标记基站小区的地址为真基站小区；终端重选入基站小区。
- [144] 作为一种可选的实施方式，处理器31用于调用该程序代码，还用于执行以下操作：
- [145] 当标记基站小区的地址为真基站小区后，将基站小区的地址写入终端内存储的允许接入小区列表内。
- [146] 可见，实施图5描述的终端，可以对伪基站进行识别，避免终端接入伪基站，还可以将识别出来的伪基站地址存入终端内的进行接入小区列表内。
- [147] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。
- [148] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通程序指令相关的硬件来完成，该程序可以存储于计算机可读存储介质中，存储介质包括只读存储器（Read-Only Memory，ROM）、随机存储器（Random Access Memory，RAM）、可编程只读存储器（Programmable Read-only Memory，PROM）、可擦除可编程只读存储

器（Erasable Programmable Read Only Memory, EPROM）、一次可编程只读存储器（One-time Programmable Read-Only Memory, OTPROM）、电子擦除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory, EEPROM）、只读光盘（Compact Disc Read-Only Memory, CD-ROM）或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

[149] 还需要说明的是，在本说明书中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[150] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其他实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权利要求书

- [权利要求 1] 一种伪基站识别方法，其特征在于，用于终端，包括：
- 步骤s101：当所述终端发生基站小区重选后，接收重选后的所述基站小区发送的系统信息；
- 步骤s102：发送位置更新请求至所述基站小区；
- 步骤s103：根据所述系统信息判断所述基站小区是否满足伪基站判定标准，如果是，进入步骤s104；
- 步骤s104：接收所述基站小区发送的身份请求信息后，发送虚假身份信息至所述基站小区；
- 步骤s105：判断是否继续收到所述基站小区发送的身份请求信息，如果是，标记所述基站小区的地址为伪基站；所述终端重选入其他基站小区。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，标记所述基站小区为伪基站后还包括：
- 将所述基站小区的地址写入所述终端内存储的禁止接入小区列表内。
- [权利要求 3] 根据权利要求1所述的方法，其特征在于，所述系统信息包括位置区码以及周期性位置更新时间；
- 所述根据所述系统信息判断所述基站小区是否满足伪基站判定标准的过程具体为：
- 当所述终端发生基站小区重选时，若收到的信号在预设时间内的增大数值超出预设信号阈值；
- 且所述基站小区的所述位置区码超出预设区码范围；
- 且所述基站小区的所述周期性位置更新时间小于预设周期，则所述基站小区满足所述伪基站判定标准，否则，所述基站小区不满足所述伪基站判定标准。
- [权利要求 4] 根据权利要求3所述的方法，其特征在于，所述步骤s103后还包括：

若所述基站小区不满足伪基站判定标准，接收所述基站小区发送的身份请求信息后，发送真实身份信息至所述基站小区；
位置更新成功后，标记所述基站小区的地址为真基站小区，所述终端重选入所述基站小区。

[权利要求 5] 根据权利要求4所述的方法，其特征在于，所述步骤s105后还包括：

若未继续收到所述基站小区发送的身份请求信息，判断是否接收到所述基站小区发送的位置更新拒绝信息，如果是，重新发送位置更新请求至所述基站小区；
接收所述基站小区发送的身份请求信息后，发送真实身份信息至所述基站小区；
位置更新成功后，标记所述基站小区的地址为真基站小区，所述终端重选入所述基站小区。

[权利要求 6] 根据权利要求4或5所述的方法，其特征在于，所述标记所述基站小区的地址为真基站小区后还包括：
将所述基站小区的地址写入所述终端内存储的允许接入小区列表内。

[权利要求 7] 一种伪基站识别系统，其特征在于，用于终端，包括：
基站信息接收模块，设置为当所述终端发生基站小区重选后，接收重选后的所述基站小区发送的系统信息，并触发位置更新请求发送模块；
所述位置更新请求发送模块，设置为发送位置更新请求至所述基站小区；
第一判断模块，设置为根据所述系统信息判断所述基站小区是否满足伪基站判定标准，如果是，触发第一身份信息发送模块；
所述第一身份信息发送模块，设置为接收所述基站小区发送的身份请求信息后，发送虚假身份信息至所述基站小区；
第二判断模块，设置为判断是否继续收到所述基站小区发送的身

份请求信息，如果是，标记所述基站小区的地址为伪基站；所述终端重选入其他基站小区。

[权利要求 8]

根据权利要求7所述的系统，其特征在于，还包括：

伪基站写入模块，设置为当标记所述基站小区的地址为伪基站时，将所述基站小区的地址写入所述终端内存储的禁止接入小区列表内。

[权利要求 9]

根据权利要求7所述的系统，其特征在于，所述第一判断模块具体设置为：

当所述系统信息包括位置区码以及周期性位置更新时间时，判断所述终端发生基站小区重选时，收到的信号在预设时间内的增大数值是否超出预设信号阈值，以及所述基站小区的所述位置区码是否超出预设区码范围，以及所述基站小区的所述周期性位置更新时间是否小于预设周期，如果是，则所述基站小区满足所述伪基站判定标准，触发所述第一身份信息发送模块；否则，所述基站小区不满足所述伪基站判定标准。

[权利要求 10]

根据权利要求9所述的系统，其特征在于，还包括：

第二身份信息发送模块，设置为接收所述基站小区发送的身份请求信息后，发送真实身份信息至所述基站小区，并在位置更新后，触发真基站标记模块；其中，当所述第一判断模块判断所述基站小区不满足所述伪基站判定标准时，触发所述第二身份信息发送模块；

所述真基站标记模块，设置为标记所述基站小区的地址为真基站小区。

[权利要求 11]

根据权利要求10所述的系统，其特征在于，还包括：

第三判断模块，设置为当所述第二判断模块判断未继续收到所述基站小区发送的身份请求信息时，判断是否接收到所述基站小区发送的位置更新拒绝信息，如果是，触发所述位置更新请求发送模块重新发送位置更新请求至所述基站小区；

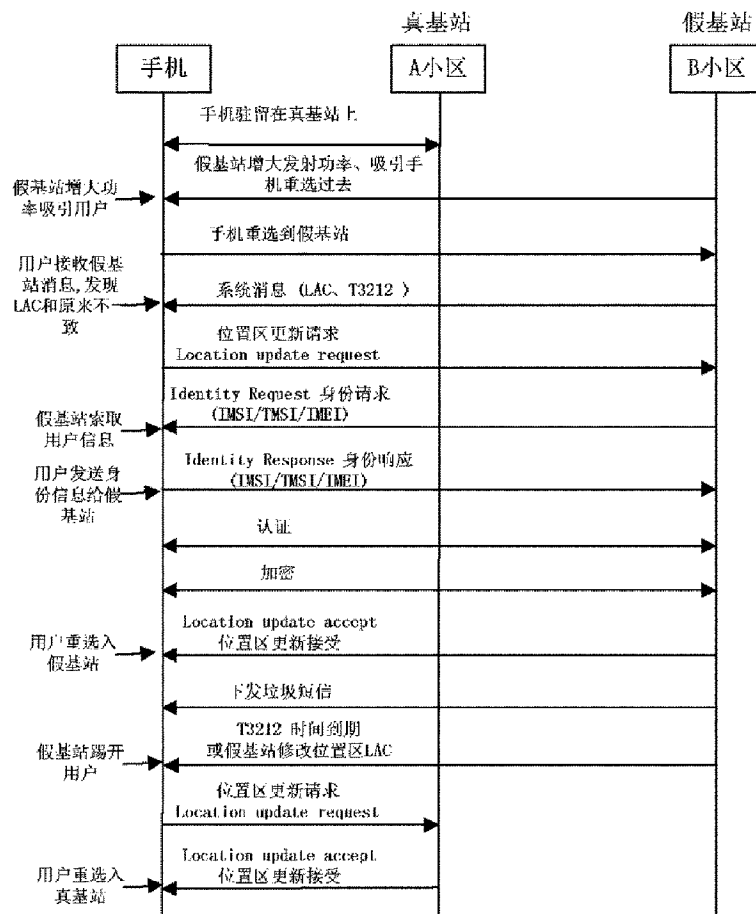
所述位置更新请求发送模块重新发送所述位置更新请求并接收到所述基站小区发送的身份请求信息后，触发所述第二身份信息发送模块。

[权利要求 12] 根据权利要求10或11所述的系统，其特征在于，还包括：
真基站写入模块，设置为当标记所述基站小区的地址为真基站小区后，将所述基站小区的地址写入所述终端内存储的允许接入小区列表内。

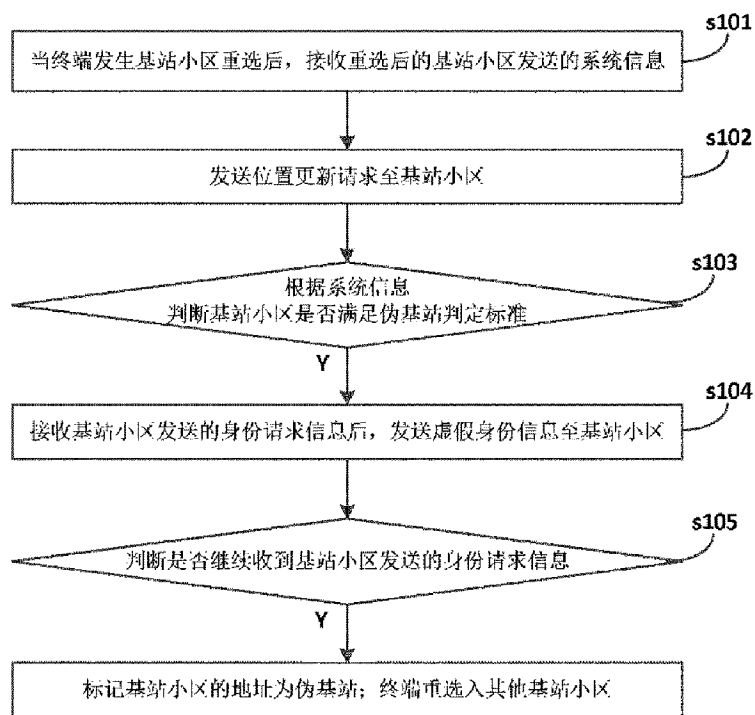
[权利要求 13] 一种终端，其特征在于，包括如权利要求7-12任一项所述的伪基站识别系统。

[权利要求 14] 根据权利要求13所述的终端，其特征在于，所述终端具体包括处理器、分别通过接口与所述处理器相连接的输入装置和输出装置以及通过总线与所述处理器相连接的存储器；
所述伪基站识别系统存储于所述存储器内；
所述处理器通过所述总线调用所述存储器内的所述伪基站识别系统进行伪基站识别操作。

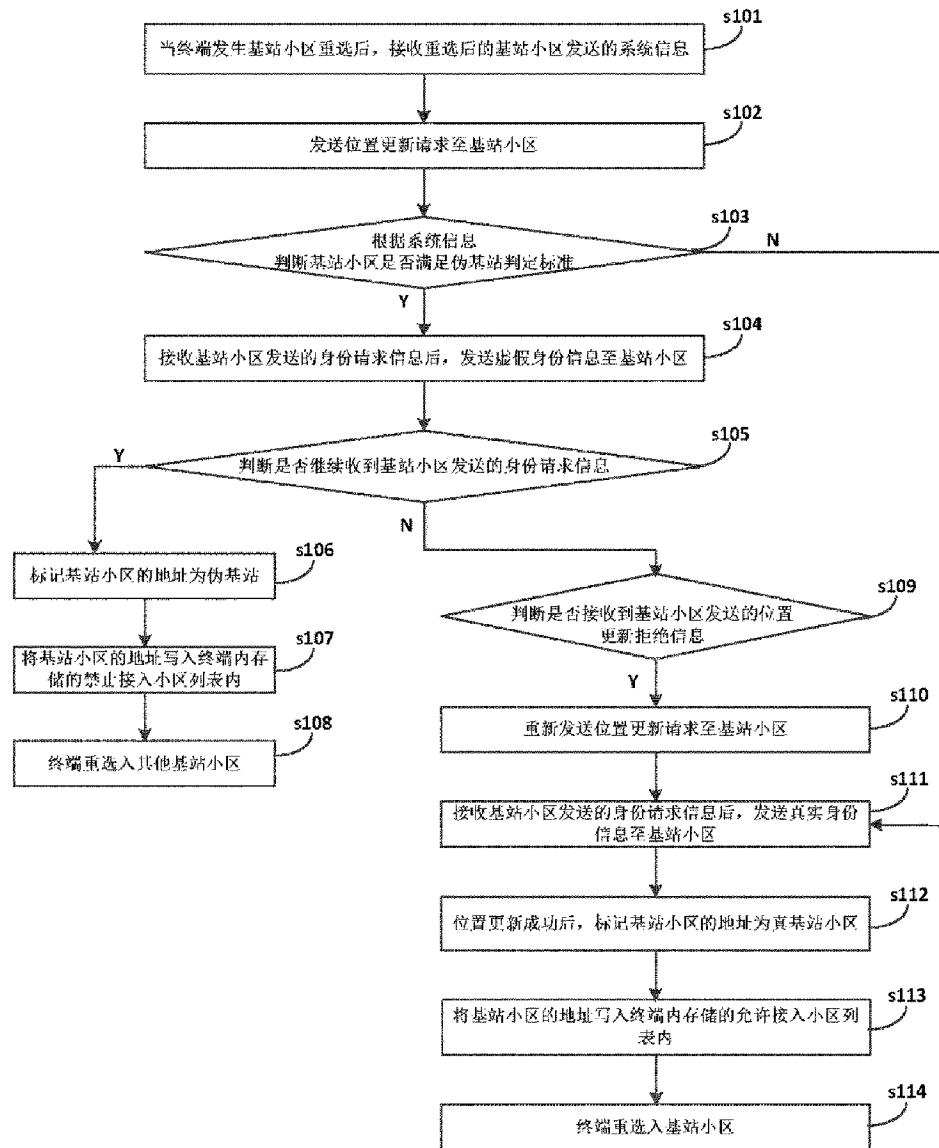
[Fig. 1]



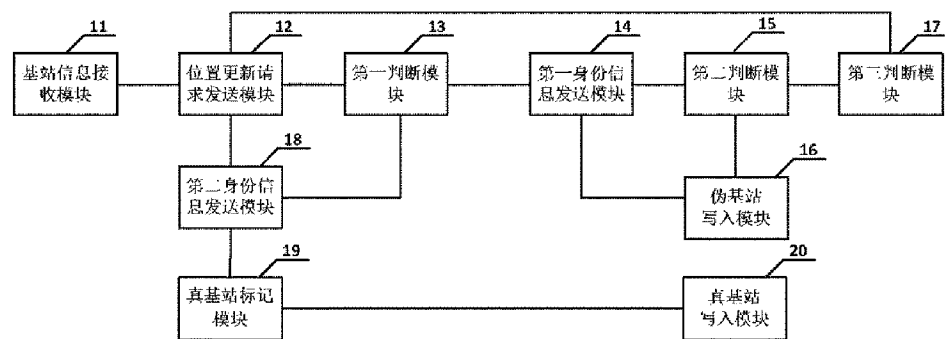
[Fig. 2]



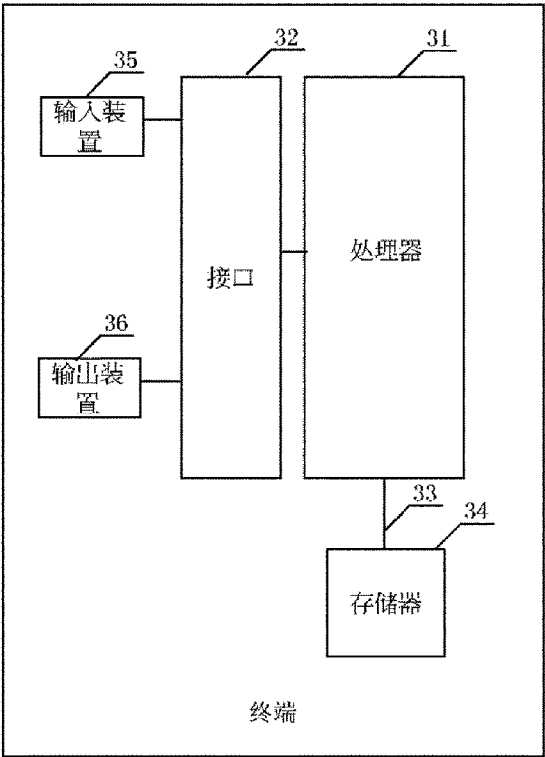
[Fig. 3]



[Fig. 4]



[Fig. 5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/113380

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/12 (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, CNKI, WPI, EPODOC: pseudo-base station, illegal, cheat, pretend, identify, fake, bogus, clone, false, identity, recognise

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106211167 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 07 December 2016 (07.12.2016), claims 1-14	1-14
A	CN 105101200 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 25 November 2015 (25.11.2015), the whole document	1-14
A	CN 104168568 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 26 November 2014 (26.11.2014), the whole document	1-14
A	CN 101959183 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES), 26 January 2011 (26.01.2011), the whole document	1-14
A	CN 104602241 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES), 06 May 2015 (06.05.2015), the whole document	1-14
A	EP 3035740 A1 (GEMALTO M2M GMBH), 22 June 2016 (22.06.2016), the whole document	1-14

☐ 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 10 February 2017 (10.02.2017)	Date of mailing of the international search report 02 March 2017 (02.03.2017)
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 LEI, Yongjun Telephone No.: (86-10) 62413422

International application No.
PCT/CN2016/113380

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

A. 主题的分类 H04W 12/12 (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, CNKI, WPI, EPODOC: 伪基站, 克隆, 非法, 欺骗, 虚假, 伪装, 身份, 识别, fake, bogus, clone, false, identity, recognise		
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
PX	CN 106211167 A (宇龙计算机通信科技深圳有限公司) 2016年 12月 7日 (2016 - 12 - 07) 权利要求1-14	1-14
A	CN 105101200 A (中国移动通信集团公司) 2015年 11月 25日 (2015 - 11 - 25) 全文	1-14
A	CN 104168568 A (中国联合网络通信集团有限公司) 2014年 11月 26日 (2014 - 11 - 26) 全文	1-14
A	CN 101959183 A (中国科学院软件研究所) 2011年 1月 26日 (2011 - 01 - 26) 全文	1-14
A	CN 104602241 A (中国科学院信息工程研究所) 2015年 5月 6日 (2015 - 05 - 06) 全文	1-14
A	EP 3035740 A1 (GEMALTO M2M GMBH) 2016年 6月 22日 (2016 - 06 - 22) 全文	1-14
☐ 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 2017年 2月 10日		国际检索报告邮寄日期 2017年 3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		授权官员 雷永俊 电话号码 (86-10) 62413422

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/113380

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	106211167	A	2016年 12月 7日	无	
CN	105101200	A	2015年 11月 25日	无	
CN	104168568	A	2014年 11月 26日	无	
CN	101959183	A	2011年 1月 26日	无	
CN	104602241	A	2015年 5月 6日	无	
EP	3035740	A1	2016年 6月 22日	WO 2016096560 A1	2016年 6月 23日