(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
2008 年12 月31 日 (31.12.2008)

PCT

(10) 国际公布号
WO 2009/000206 A1

(51) 国际专利分类号:
H04Q 7/38 (2006.01)

(21) 国际申请号: PCT/CN2008/071432

(22) 国际申请日: 2008 年6 月25 日 (25.06.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710123494.2
2007 年6 月25 日 (25.06.2007) CN

(71) 申请人 (对除美国外的所有指定国): **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基地总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **牛卫国 (NIU, Weiguo)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 **杨利 (YANG, Li)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京同立钧成知识产权代理有限公司 (LEADER PATENT & TRADEMARK FIRM)**; 中国北京市朝阳区北辰西路69号峻峰华亭A座902, Beijing 100029 (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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

[见续页]

(54) **Title:** METHOD AND SYSTEM FOR ACCESS CONTROL OF HOME NODE B

(54) **发明名称:** 家用微型基站接入控制方法及系统

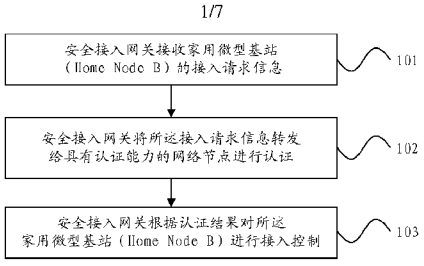


图 1 /Fig.1

101 A SECURITY ACCESS GATEWAY RECEIVES ACCESS REQUEST INFORMATION OF A HOME NODE B
102 THE SECURITY ACCESS GATEWAY FORWARDS THE ACCESS REQUEST INFORMATION TO A NETWORK NODE CAPABLE OF AUTHENTICATION TO PERFORM AUTHENTICATION
103 THE SECURITY ACCESS GATEWAY PERFORMS ACCESS CONTROL OF THE HOME NODE B ACCORDING TO A RESULT OF AUTHENTICATION

(57) **Abstract:** The invention provides a method for access control of a home node B, which includes: receiving, by a security access gateway, access request information of the home node B; forwarding, by the security access gateway, the access request information to a network node capable of authentication to perform authentication; performing, by the security access gateway, access control of the home node B according to a result of authentication. The invention further provides a system for access control of the home node B. The method and system for access control of the home node B provided by the invention ensure the security of the mobile network, the stability of the wireless environment, and implementing the strategy of an operator, performing access control before allocating resources to the home node B by the network, avoiding waste of network resources, effectively eliminating the influence to the network caused by the home node B that does not conform with the access condition accessing the network.

[见续页]

WO 2009/000206 A1

MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

(57) 摘要：

本发明涉及一种家用微型基站接入控制的方法，包括安全接入网关接收家用微型基站的接入请求信息；安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证；安全接入网关根据认证结果对上述家用微型基站进行接入控制。本发明还涉及一种家用微型基站接入控制系统。本发明涉及家用微型基站接入控制的方法及系统能够保证移动网络的安全、无线环境的稳定，以及运营商的策略的实施，在网络为家用微型基站分配资源之前进行接入控制，避免了网络资源的浪费，有效的避免了不符合接入条件的家用微型基站接入网络给网络所带来的影响。

家用微型基站接入控制方法及系统

技术领域

本发明涉及一种 Home Node B（以下简称家用微型基站）接入移动网络的方法，尤其是一种对家用微型基站接入移动网络进行控制的方法；本发明还涉及一种家用微型基站接入控制系统，尤其是一种能够有效控制家用微型基站接入移动网络的系统。

背景技术

在目前的移动通信网络中，对于网络节点的布置，大多是由运营商事先规划好，并根据规划的内容完成网络布置。网络中位于同一位置区域的用户共享小区的资源，当有高速率、高带宽的业务接入时，会对其他用户的接入造成影响；另外，网络中可能会存在覆盖问题，特别是处于室内时。家用微型基站作为一种家用的微型基站，可以提供家庭，办公场所等热点覆盖，家用微型基站通过因特网（简称 Internet）接入移动通信网络，来获得无线通信服务。家用微型基站的引入，解决了无线数据业务中空口资源瓶颈问题，使得用户可以享用到高速率、高带宽的网络服务；其次，家用微型基站可以优化网络覆盖，为用户提供更好的服务，但应当对请求接入的家用微型基站进行有效地控制。

现有技术中，一般采用以下两种方式进行网络节点的接入控制。在方式一中，由于具有较大覆盖面积的基站（以下简称：宏 Node B）接入的时间、地点以及接入时的配置对于当前的无线网络来说都是已知的，因此对于宏 Node B 的接入，是由运营商网络事先规划好的。在宏 Node B 请求接入时，只需要根据网规的数据，配置相应的接入参数，便可完成宏 Node B 的接入，无需专门的控制机制。方式二中，考虑到网络规划覆盖到和网络规划覆盖不到的两种情况，对于网络规划覆盖到的情况，比如宏 Node B 的接入，利用网络规划的数据参照上述方式一进行接入；而对于网络规划覆盖不到的情况，

比如家用微型基站，则不进行专门的接入控制，直接允许其接入网络，然后在网络运行的过程中对来自于不合法的家用微型基站的呼叫请求（包括接入节点本身不合法，接入节点位置不合法等情况）给予拒绝。

上述两种网络节点接入控制方式存在以下缺陷:

方式一: 首先，由于家用微型基站的数量众多，远超过宏 Node B 的数量，网规数据很难覆盖到所有的家用微型基站，大量的家用微型基站给网络规划工作带来了难题；其次，由于家用微型基站的接入时间，地点等都是由用户控制的，是随机发生的，网络无法预知到这些信息，所以网络规划也不可能考虑到家用微型基站接入情况。

方式二: 此接入控制方式对于网络规划覆盖不到的家用微型基站的情况的缺点比较明显。首先，对于请求接入的家用微型基站不进行控制，极有可能导致不合法的家用微型基站接入网络，例如无权限的、不合规格的家用微型基站接入网络，或一些家用微型基站的恶意接入。由于此类家用微型基站已经接入了网络，网络就必须为其分配相应的资源，包括链路资源、无线资源等，造成网络的不安全和网络资源的浪费；其次，还可能导致在不合适位置的家用微型基站接入网络，比如家用微型基站的漫游接入，家用微型基站是在一个地方注册的，如果其在另一地方通过因特网接入注册地网络，会给另一地方的无线环境造成影响，且注册地的网络给其分配的无线资源（比如频点）与另一地方无线环境规划相冲突，将导致资源分配的混乱，给网络的规划和协调带来问题，影响运营商的网络运营策略。

发明内容

本发明的一个方面是提供一种家用微型基站接入控制方法。

本发明的另一方面是提供一种家用微型基站接入控制系统。

本发明的再一方面是提供一种通信设备。

为实现本发明的第一个方面，本发明的一些实施例提供了一种家用微型

基站接入控制的方法，包括安全接入网关接收家用微型基站的接入请求信息；安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证；安全接入网关根据认证结果对上述家用微型基站进行接入控制。

本方法能够保证移动网络的安全、无线环境的稳定，以及运营商的策略的实施，为用户提供更好的服务。

为实现本发明的第二个方面，本发明的另外一些实施例提供了一种家用微型基站接入控制系统，包括家用微型基站，用于发送所述家用微型基站的接入请求信息；安全接入网关，用于接收并转发上述家用微型基站的接入请求信息，根据认证结果控制述家用微型基站的接入；第一功能模块，用于根据接收到的接入请求信息对上述家用微型基站的进行接入认证。

本发明的另外一些实施例提供了一种通信设备，用于控制家用基站的接入，包括信息接发模块，用于接收来自家用微型基站的接入请求；发送模块，用于转发所述接入请求；控制模块，用于根据认证结果对所述家用微型基站进行接入控制。

上述技术方案的系统可增加网络的安全性，避免网络资源的浪费，并且增加了用户和运营商的方便性，减少了成本。

附图说明

图 1 为本发明家用微型基站接入控制的方法流程示意图；

图 2 为本发明 EMS 对家用微型基站设备物理标识认证的接入控制方法一实施例流程示意图；

图 3 为本发明 EMS 对家用微型基站设备物理标识认证的接入控制方法另一实施例流程示意图；

图 4 为本发明签约信息认证服务器根据家用微型基站标识信息进行认证的接入控制方法实施例流程示意图；

图 5 为本发明通过家用微型基站的测量信息进行认证的接入控制方法实

施例流程示意图;

图 6 为本发明通过家用微型基站的地理位置信息进行认证的接入控制方法实施例流程示意图;

图 7 为本发明根据家用微型基站地址信息的归属地信息进行接入控制方法实施例流程示意图;

图 8 为本发明根据允许接入的家用微型基站的 IP 地址信息进行接入控制方法实施例流程示意图;

图 9 为本发明根据家用微型基站与因特网地址绑定关系进行接入控制方法实施例流程示意图;

图 10 为本发明家用微型基站接入控制的方法信令流程示意图;

图 11 为本发明家用微型基站与移动网络建立传输层安全链路连接流程示意图;

图 12 为本发明家用微型基站接入控制系统结构示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

实施例一、

如图 1 所示，一种家用微型基站接入控制的方法，包括：步骤 101，安全接入网关接收家用微型基站的接入请求信息；步骤 102，安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证；步骤 103，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

本实施例所提供的方法在家用微型基站上电后需要接入网络时，自动地对家用微型基站的接入进行控制，不需要人工的干预或者网规数据的指示，减少了运营商和用户在使用家用微型基站时所需要花费的努力，降低了家用微型基站接入网络的难度和成本。其次，该方法在网络为家用微型基站分配

资源之前进行接入控制，避免了网络资源的浪费，有效的避免了不符合接入条件的家用微型基站接入网络给网络所带来的影响。

实施例二、

基于前述的实施例一，家用微型基站在通过因特网接入移动网络时，由于用户根据需要随时随地启动接入，网络无法预知和规划家用微型基站的接入时间和接入地点，因此，家用微型基站的接入对网络资源的管理提出了新的需求。而且，由于用户家用微型基站接入地点的变化，将对网络资源的分配和协调以及无线环境造成一定的影响，也会对运营商的计费策略带来影响，因此，需要一定的策略来控制家用微型基站的接入。

如图 2 所示，本实施例，与实施例一不同之处在于，上述的安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证的过程，具体为设备认证服务器对家用微型基站设备物理标识的认证过程，上述安全接入网关根据接入请求信息中的设备认证服务器对应信息查询是否存在对应的设备认证服务器，若存在，则上述安全接入网关向上述设备认证服务器转发上述接入请求信息，否则拒绝接入；上述设备认证服务器接收到上述接入请求信息后，对上述家用微型基站进行认证，本实施例中，选用网元管理系统(Element Management System；以下简称：EMS)作为设备认证服务器对家用微型基站设备物理标识的认证。由于家用微型基站和 EMS 之间接口的私有性，来自于不同厂商的不同型号家用微型基站，可能只能接入相对应的 EMS。对于与接入请求时所访问的 EMS 不兼容的家用微型基站，网络可以拒绝该接入请求，拒绝为其分配资源。

家用微型基站发送接入请求到安全接入网关，携带自身的设备标识信息，上述设备标识信息包括厂商标识，设备型号等信息，接入控制的具体步骤如下：

步骤 201，安全接入网关接收家用微型基站的接入请求信息；

步骤 202，上述安全接入网关根据接入请求信息中包含的厂商标识信息为

上述家用微型基站指定相应的 EMS，并向上述 EMS 转发上述接入请求信息；

具体为安全接入网关根据接入请求信息中包含的厂商标识信息判断是否存在对应的 EMS，若存在，则上述安全接入网关向上述 EMS 转发接入请求信息；否则拒绝接入。

步骤 203，上述 EMS 接收到接入请求信息后，对上述家用微型基站进行认证；

步骤 204，上述 EMS 向上述安全接入网关返回认证结果；

步骤 205，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

安全接入网关接收到认证结果，若认证成功，则允许上述家用微型基站接入；若认证失败，则拒绝上述家用微型基站接入。

进一步地，如图 3 所示，步骤 203 上述 EMS 接收到接入请求信息后，对上述家用微型基站进行如下认证操作：

步骤 203a，上述 EMS 收到上述家用微型基站的接入请求信息后，首先根据上述家用微型基站的厂商标识判断该家用微型基站与本 EMS 是否兼容，如果兼容，则进行步骤 203b；否则，认证失败；

步骤 203b，上述 EMS 根据家用微型基站的设备型号判断该家用微型基站是否是该 EMS 可以服务的对象，如果型号符合，则认证成功；若不符合，则认证失败。

EMS 返回判决结果给接入网关，接入网关根据 EMS 的判决结果决定接受或者拒绝该家用微型基站的接入请求。

实施例三、

为了避免不合法的家用微型基站或者没有权限的家用微型基站接入网络，给网络带来不安全的因素，以及为了防止某些家用微型基站的恶意接入，需要对请求接入的家用微型基站身份和签约信息进行认证和鉴权。如图 4 所示，本实施例中，与实施例一和实施例二的不同之处在于，上述的安全接入

网关将上述接入请求信息转发给具有认证能力的网络节点进行认证的过程，还可以为签约信息认证服务器根据上述家用微型基站标识信息进行的接入认证的过程.

家用微型基站发送接入请求到移动网络的安全接入网关，携带自身的标识信息，上述标识信息包括家用微型基站的签约标识信息,具体的步骤如下:

步骤 301，安全接入网关接收家用微型基站的接入请求信息;

步骤 302,上述安全接入网关将包含有家用微型基站标识信息的接入请求信息转发给签约信息认证服务器;

上述签约信息认证服务器可以为 AAA 服务器; 上述接入请求信息携带家用微型基站的标识信息;

步骤 303,上述签约信息认证服务器根据上述家用微型基站标识信息对上述家用微型基站进行认证;

签约信息认证服务器根据该家用微型基站的标识信息，对上述家用微型基站的身份进行认证和鉴权，判断该家用微型基站身份的合法性以及接入权限（如付费息等）正确性;

步骤 304，上述签约信息认证服务器向上述安全接入网关返回认证结果;

步骤 305，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

上述签约信息认证服务器返回认证和鉴权的结果给安全接入网关，安全接入网关根据上述签约信息认证服务器返回的认证结果决定接受或者拒绝上述家用微型基站的接入请求。

实施例四、

如图 5 所示，本实施例中，与实施例一、二、三的不同之处在于，上述的安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证的过程，又可以是签约信息认证服务器根据上述家用微型基站的测量信息进行接入认证的过程。

在家用微型基站接入的时候，家用微型基站需要提供其对周围环境的测量信息，根据上述测量信息来进行接入认证。测量信息可通过家用微型基站上电之后，对周围环境进行测量；还可以采用与上述家用微型基站绑定的手机对上述家用微型基站周围的环境信息进行测量的方式，测量至少包括：家用微型基站所在位置的已有的小区/基站的标识等信息。上述的预先测量需要家用微型基站在上电后能够自动进行。家用微型基站通过因特网向接入网关发送接入请求，携带其预先对周围环境的测量信息，具体接入控制步骤如下：

步骤 401，安全接入网关接收上述家用微型基站的接入请求信息；

步骤 402，上述安全接入网关向签约信息认证服务器转发包含有上述测量信息的接入请求信息；

步骤 403，上述签约信息认证服务器分析上述测量信息中包含的小区/基站标识信息，判断上述家用微型基站所处区域；

接入网关转发该测量信息到签约信息认证服务器，签约信息认证服务器分析家用微型基站所携带测量信息中的已有小区/基站的标识，判断家用微型基站的所处的区域。

步骤 404，签约信息认证服务器将接收到的家用微型基站所处区域信息与签约信息中允许接入的区域信息进行对比，符合，则认证成功；否则，认证失败；

步骤 405，上述签约信息认证服务器向上述安全接入网关返回认证结果；

步骤 406，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

实施例五、

如图 6 所示，本实施例中，与实施例一、二、三、四的不同之处在于，上述的安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证的过程，再可以是签约信息认证服务器根据家用微型基站的地理位置信息进行接入认证。

家用微型基站上电之后，通过因特网向接入网关发送接入请求，具体接入控制步骤如下：

步骤 501，安全接入网关接收家用微型基站的接入请求信息；

步骤 502，上述安全接入网关根据上述接入请求信息触发网络中的物理位置测量实体对上述家用微型基站进行定位测量；

安全接入网关收到接入请求信息后，根据接入请求信息中的相关信息触发相应的物理位置测量实体对家用微型基站的位置进行定位测量；

步骤 503，上述物理位置测量实体对上述家用微型基站的地理位置进行定位测量，并向安全接入网关返回定位测量信息；

上述网络中的物理位置测量实体根据上述接入请求信息对上述家用微型基站的地理位置进行定位，并向安全接入网关返回定位测量信息；上述网络中的物理位置测量实体可采取例如全球定位系统(Global Positioning System；以下简称：GPS)定位机制、观察到达时间差定位机制（Observed Time Difference of Arrival；以下简称：OTDOA）等对家用微型基站进行定位测量，将结果报告给接入网关。

步骤 504，上述安全接入网关将包含有上述定位测量信息的接入请求信息发送给签约信息认证服务器；

步骤 505，签约信息认证服务器将接收到的上述家用微型基站的定位信息与签约信息中允许接入的区域信息进行对比，符合，则认证成功；否则，认证失败；

步骤 506，上述签约信息认证服务器向上述安全接入网关返回认证结果；

步骤 507，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

上述签约信息认证服务器返回认证结果给安全接入网关，安全接入网关根据上述签约信息认证服务器返回的认证结果决定接受或者拒绝上述家用微型基站的接入请求。

实施例六、

本实施例中，与上述各实施例不同之处在于，上述的安全接入网关将上述接入请求信息转发给具有认证能力的网络节点进行认证，也可以是为签约信息认证服务器接收到上述安全接入网关转发的上述接入请求信息后，对上述接入请求信息中的上述家用微型基站的网络地址信息进行分析认证。

家用微型基站通过因特网接入移动运营商的网络，在请求接入的时候，安全接入网关根据其在因特网的地址信息来进行接入控制。具体步骤如下：首先，家用微型基站通过因特网向安全接入网关发送接入请求，携带其在因特网中的网络地址信息。然后，安全接入网关对家用微型基站的因特网地址信息进行分析，根据地址信息进行接入控制。包括两种接入控制方式，第一种为根据家用微型基站地址信息的地域性进行接入控制；第二种为根据家用微型基站与因特网地址绑定关系进行接入控制。

由于在因特网中地址的划分有一定的地域性，比如 网际协议(ernet Protocol;以下简称：IP)地址分配的地域性，因此可以根据家用微型基站在因特网中的地址信息归属地信息判断其是否可以接入。如图 7 所示，第一种接入控制方式中，签约信息认证服务器根据家用微型基站的地址信息判断其接入位置的归属地，签约信息认证服务器与允许其接入的归属地进行对比，根据对比结果进行控制，步骤如下：

步骤 601，安全接入网关接收家用微型基站的接入请求信息；

步骤 602，上述安全接入网关向签约信息认证服务器转发上述包含有家用微型基站网络地址信息的接入请求信息；

步骤 603，签约信息认证服务器根据上述家用微型基站的网络地址信息判断接入位置的归属地；

步骤 604，签约信息认证服务器将上述家用微型基站的归属地信息与签约信息中允许接入的位置信息进行对比，符合，则认证成功；否则，认证失败；

步骤 605，上述签约信息认证服务器向上述安全接入网关返回认证结果；

步骤 606，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

如图 8 所示，第一种接入控制方式中，还可以在签约信息认证服务器关中设定只允许某些指定的网络地址的家用微型基站可以接入，对于不在指定网络地址的家用微型基站的接入请求给予拒绝，步骤如下：

步骤 701，安全接入网关接收家用微型基站的接入请求信息；

步骤 702，上述安全接入网关向签约信息认证服务器转发上述包含有家用微型基站地址信息的接入请求信息；

步骤 703，签约信息认证服务器将家用微型基站的网络地址信息与上述签约信息认证服务器中预先设定的允许接入的网络地址信息进行对比，符合，则认证成功；否则，认证失败；

步骤 704，上述签约信息认证服务器向上述安全接入网关返回认证结果；

步骤 705，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

第二种接入控制方式中，采用根据家用微型基站与因特网地址绑定关系进行接入控制。如图 9 所示，接入控制步骤如下：

步骤 801，安全接入网关接收家用微型基站的接入请求信息；

步骤 802，上述安全接入网关向签约信息认证服务器转发上述包含有家用微型基站网络地址信息的接入请求信息；

步骤 803，签约信息认证服务器将家用微型基站的网络地址信息与签约信息中的绑定关系信息进行对比，符合，则认证成功；否则，认证失败；

步骤 804，上述签约信息认证服务器向上述安全接入网关返回认证结果；

步骤 805，安全接入网关根据认证结果对上述家用微型基站进行接入控制。

家用微型基站用户在订阅服务的时候，提供其可能接入的包含有接入端口信息的因特网地址信息，网络将这些地址信息与家用微型基站的标识信息

进行绑定，并保存在签约信息认证服务器中。安全接入网关在接入控制时通过家用微型基站的标识信息与地址信息的绑定关系来控制其接入。上述的地址信息不是严格的限制于某一特定的地址，有可能是一个小的地址范围。例如，对于有固定 IP 地址的用户，其地址信息可以包括一组 IP 地址；对于可变 IP 地址的用户，其地址信息可以包括因特网接入点的端口信息，比如 TCP/IP 协议第 2 层物理端口等。安全接入网关在判决时，比较家用微型基站实际接入的地址信息与签约信息认证服务器中注册的绑定关系中的地址信息，如果符合则允许接入，否则拒绝接入。

实施例七、

基于前述的各实施例，家用微型基站通过因特网接入移动网络，首先需要在家用微型基站与移动网络之间建立传输层安全链路连接，可以采用“VPN”，“Ipsec”等安全技术建立安全连接。在安全连接的建立过程中，移动网络和家用微型基站之间需要利用安全信息相互进行认证和鉴权，其中所使用的安全信息有可能与家用微型基站本身没有关系，比如，“IpSec”所使用的安全“Credential”与家用微型基站本身没有关系，而是另外的用户名、密码、证书等；所使用的安全信息也有可能与家用微型基站本身的信息有一定关系，比如与家用微型基站 设备厂商、序列号等可能有绑定关系。完成认证和鉴权过程后，由 EMS 控制为其分配相应的资源（如链路资源，无线资源），完成接入过程。因此，对于家用微型基站的接入控制，接入网关为控制点，通过其他网络功能节点的配合，在网络为其分配相应的资源之前来进行控制，具体流程如图 10 所示：

步骤 a，家用微型基站与移动通信网络建立传输层安全链路连接；

步骤 b，家用微型基站向安全接入网关发送接入请求信息；

步骤 c，接入网关分析接入请求信息；

步骤 d，安全接入网关转发接入请求信息；

步骤 e，网络功能节点根据接入请求信息进行认证；

步骤 f, 网络功能节点向安全接入网关返回认证结果;

步骤 g, 安全接入网关根据认证结果控制家用微型基站接入。

如图 11 所示，建立传输层安全链路连接的具体步骤如下:

步骤 a1，家用微型基站向安全接入网关发送上述家用微型基站的传输层安全链路认证信息;

步骤 a2，上述安全接入网关接收所到上述家用微型基站的传输层安全链路认证信息后，对上述家用微型基站进行认证，认证成功，则向上述家用微型基站发送认证成功信息，上述认证成功信息包含有上述安全接入网关的传输层安全链路认证信息；认证失败，则不响应或发送认证失败信息;

步骤 a3，上述家用微型基站对上述安全接入网关进行认证，认证成功，则传输层安全链路建立成功；否则，传输层安全链路建立失败。

上述家用微型基站接收到上述安全接入网关发送的上述认证成功信息后，根据上述安全接入网关的传输层安全链路认证信息进行上述安全接入网关的传输层安全链路认证，认证成功，则传输层安全链路建立成功；否则，传输层安全链路建立失败。

在上述家用微型基站与移动网络建立传输层安全链路连接之前，上述家用微型基站还需要知道上述安全接入网关的地址，配置方法可以是预先在上述家用微型基站上设置安全接入网关的地址，例如可由移动运营商或用户预先设置，或者在上述家用微型基站进行接入请求时，由公网的自动地址分配服务器为上述家用微型基站配置安全网关的地址。

上述各实施例所提供的接入控制方法都是针对接入控制过程中某一方面的问题所提出来的解决方案，在实际应用时，不局限于采用某一种或者某几种方法，即可以采用其中的某一种方法，或者采用其中的某几种方案的组合，具体采用哪一种认证控制方法，需要结合实际情况，根据一定的接入策略来确定。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤

可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

实施例八、

如图 12 所示，本实施例提供一种家用微型基站接入控制系统，包括：家用微型基站 1，用于发送家用微型基站 1 的接入请求信息；安全接入网关 2，用于接收并转发上述家用微型基站的接入请求信息，根据认证结果控制上述家用微型基站的接入；第一功能模块 3，用于根据接收到的接入请求信息对上述家用微型基站进行接入认证。

在家用微型基站 1 接入移动网络时，首先要访问的是移动网络的安全接入网关 2，在家用微型基站 1 和移动网络之间建立一个安全的连接，安全接入网关 2 包括信息接发模块 21，用于接收和转发信息；信息分析模块 22 与信息接发模块 21 连接，对接收的信息进行分析；接入判决模块 23 与信息分析模块 22 连接，用于根据分析结果对家用微型基站的接入进行控制。信息接发模块 21 接收家用微型基站的接入请求信息后，经过信息分析模块 22 分析，通过信息接发模块 21 将家用微型基站的接入请求信息转发给第一功能模块 3，然后经第一功能模块 3 根据接入请求信息进行家用微型基站的接入认证和鉴权过程，其中上述第一功能模块 3 为设备认证服务器、EMS 或签约信息认证服务器，以及其他可完成认证功能等网络功能实体，第一功能模块 3 中还存储有用于认证的必要信息，如签约信息认证服务器中存储有家用微型基站的签约信息、允许接入的 IP 地址段信息；认证成功后，安全接入网关接收到认证结果后，由接入判决模块 23 根据认证结果控制家用微型基站 1 接入，并由 EMS 控制为其分配相应的资源（如链路资源，无线资源），完成接入过程。家用微型基站的接入控制系统中，以安全接入网关为控制点，通过其他网络功能节点的配合，在网络为其分配相应的资源之前来进行控制。

该系统充分满足了用户对于无线网络的高速、便捷、低成本等方面的需求和网络的发展需求。随着网络复杂程度的逐渐增加和无线通信技术的发展，网络中的家用微型基站数量将会十分庞大，对于运营商来说，需要避免在家用微型基站接入时花费大量的精力；对于用户来说，希望能够方便地使用家用微型基站所带来的服务。应用本实施例所提供的家用微型基站接入控制系统，可很好地满足需求。

本发明实施例提供一种通信设备，用于控制家用微型基站的接入，包括信息接发模块，用于接收来自家用微型基站的接入请求；发送模块，用于转发所述接入请求；控制模块，用于根据认证结果对家用微型基站进行接入控制。通信设备可以为安全接入网关或其它网元功能实体。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种家用微型基站接入控制方法，其特征在于，包括:

安全接入网关接收到家用微型基站的接入请求信息时，将所述接入请求信息转发给具有认证能力的网络节点进行认证;

所述安全接入网关根据认证的结果对所述家用微型基站进行接入控制。

2、根据权利要求 1 所述的方法，其特征在于，所述的安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证，包括:

所述安全接入网关根据接入请求信息中的设备认证服务器对应信息查询是否存在对应的设备认证服务器，如果存在对应的设备认证服务器，所述安全接入网关向所述设备认证服务器转发所述接入请求信息，如果不存在对应的设备认证服务器，拒绝接入。

3、根据权利要求 2 所述的方法，其特征在于，所述的安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证进一步包括:

所述设备认证服务器根据所述接入请求信息中的设备认证服务器对应信息判断所述家用微型基站与所述设备认证服务器是否兼容，如果所述家用微型基站与所述设备认证服务器不兼容，则认证失败;

如果所述家用微型基站与所述设备认证服务器兼容，根据所述接入请求信息中的设备认证服务器对应信息判断所述家用微型基站是否是所述设备认证服务器服务的对象，如果所述家用微型基站是所述设备认证服务器服务的对象，则认证成功，若所述家用微型基站不是所述设备认证服务器服务的对象，则认证失败。

4、根据权利要求 1 所述的方法，其特征在于，所述的安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证，包括:

所述安全接入网关将包含有所述家用微型基站标识信息的接入请求信息转发给签约信息认证服务器;

所述签约信息认证服务器根据所述家用微型基站标识信息对所述家用微

型基站进行认证。

5、根据权利要求 1 所述的方法，其特征在于，所述的安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证，包括:

所述安全接入网关向签约信息认证服务器转发包含有所述家用微型基站测量信息的接入请求信息;

所述签约信息认证服务器分析所述测量信息中包含的小区/基站标识信息，判断家用微型基站所处区域;

所述签约信息认证服务器将所述家用微型基站所处区域信息与签约信息中允许接入的区域信息进行对比，如果所述家用微型基站所处区域信息与签约信息中允许接入的区域信息符合，则认证成功，如果所述家用微型基站所处区域信息与签约信息中允许接入的区域信息不符合，认证失败。

6、根据权利要求 5 所述的方法，其特征在于，在所述安全接入网关向签约信息认证服务器转发包含有所述家用微型基站测量信息的接入请求信息之前，所述家用微型基站或与所述家用微型基站绑定的终端对其周围环境信息进行测量，获得所述的测量信息；或者

所述安全接入网关根据所述接入请求信息触发网络中的物理位置测量实体对所述家用微型基站的地理位置进行定位测量，并向安全接入网关返回定位测量信息。

7、根据权利要求 6 所述的方法，其特征在于，所述网络中的物理位置测量实体对所述家用微型基站的地理位置进行定位测量具体为，所述网络中的物理位置测量实体采取全球定位系统定位机制或者观察到达时间差定位机制对所述家用微型基站进行定位测量，获得所述家用微型基站的地理位置信息。

8、根据权利要求 1 所述的方法，其特征在于，所述的安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证，具体为所述具有认证能力的网络节点接收到所述安全接入网关转发的所述接入请求信息后，对所述接入请求信息中的所述家用微型基站的网络地址信息进行分析认证。

9、根据权利要求 8 所述的方法，其特征在于，所述具有认证能力的网络节点对所述接入请求信息中的所述家用微型基站的网络地址信息进行分析认证，包括:

签约信息认证服务器根据所述家用微型基站的网络地址信息判断接入位置的归属位置信息;

所述签约信息认证服务器将所述家用微型基站的归属地信息与签约信息中允许接入的位置信息进行对比，如果所述家用微型基站的归属地信息与签约信息中允许接入的位置信息符合，则认证成功；如果所述家用微型基站的归属地信息与签约信息中允许接入的位置信息不符合，认证失败。

10、根据权利要求 8 所述的方法，其特征在于，所述具有认证能力的网络节点对所述接入请求信息中的所述家用微型基站的网络地址信息进行分析认证，包括:

签约信息认证服务器将所述家用微型基站的网络地址信息与所述签约信息认证服务器中预先设定的允许接入的网络地址信息或所述签约信息认证服务器中预先存储的绑定关系信息进行对比，如果所述家用微型基站的网络地址信息与所述签约信息认证服务器中预先设定的允许接入的网络地址信息或所述签约信息认证服务器中预先存储的绑定关系信息符合，则认证成功，如果所述家用微型基站的网络地址信息与所述签约信息认证服务器中预先设定的允许接入的网络地址信息或所述签约信息认证服务器中预先存储的绑定关系信息不符合，认证失败。

11、根据权利要求 10 所述的方法，其特征在于，在签约信息认证服务器将所述家用微型基站的网络地址信息与在所述签约信息认证服务器中预先存储的绑定关系信息进行对比之前，还包括:

所述家用微型基站订阅服务时，预先提供接入网络地址信息;

将所述家用微型基站的预先提供的接入网络地址信息与所述家用微型基站的标识信息进行绑定，并存储在所述签约服务器中。

12、根据权利要求 11 所述，其特征在于，所述预先提供接入网络地址信息具体为预先提供包含有接入端口信息的所述接入网络地址信息。

13、根据权利要求 1 至 12 所述的任一方法，其特征在于，所述安全接入网关接收家用微型基站的接入请求信息之前，还包括：所述家用微型基站与移动网络建立传输层安全链路连接。

14、根据权利要求 13 所述的方法，其特征在于，所述家用微型基站与移动网络建立传输层安全链路连接，包括：

所述家用微型基站向所述安全接入网关发送所述家用微型基站的传输层安全链路认证信息；

所述安全接入网关接收到所述家用微型基站的传输层安全链路认证信息后，进行所述家用微型基站的传输层安全链路认证,认证成功，则向所述家用微型基站发送认证成功信息，所述认证成功信息中包含有所述安全接入网关的传输层安全链路认证信息；认证失败，则不响应或发送认证失败信息；

所述家用微型基站接收到所述安全接入网关发送的所述认证成功信息后，进行所述安全接入网关的传输层安全链路认证，认证成功，则传输层安全链路建立成功；否则，传输层安全链路建立失败。

15、根据权利要求 14 所述的方法，其特征在于，所述家用微型基站与移动网络建立传输层安全链路连接之前，还包括：

预先在所述家用微型基站上配置安全接入网关的地址，或者在家用微型基站进行接入请求时，由所述由公网的自动地址分配服务器为所述家用微型基站配置安全网关的地址。

16、一种家用微型基站接入控制系统，其特征在于，包括：

家用微型基站，用于发送所述家用微型基站的接入请求信息；

安全接入网关，用于接收并转发所述家用微型基站的接入请求信息，根据认证结果控制述家用微型基站的接入；

第一功能模块，用于根据接收到的接入请求信息对所述家用微型基站的

进行接入认证。

17、根据权利要求 16 所述的系统，其特征在于，所述第一功能模块为设备认证服务器、网元管理系统或签约信息认证服务器。

18、一种通信设备，用于控制家用微型基站的接入，其特征在于，所述通信设备包括:

信息接发模块，用于接收来自家用微型基站的接入请求;

发送模块，用于转发所述接入请求;

控制模块，用于根据认证结果对所述家用微型基站进行接入控制。

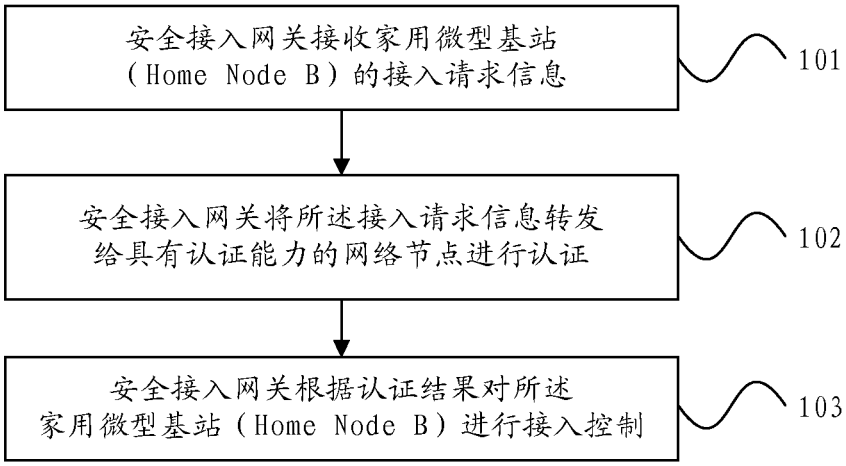

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
101
安全接入网关将所述接入请求信息转发给具有认证能力的网络节点进行认证
102
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
103

图 1

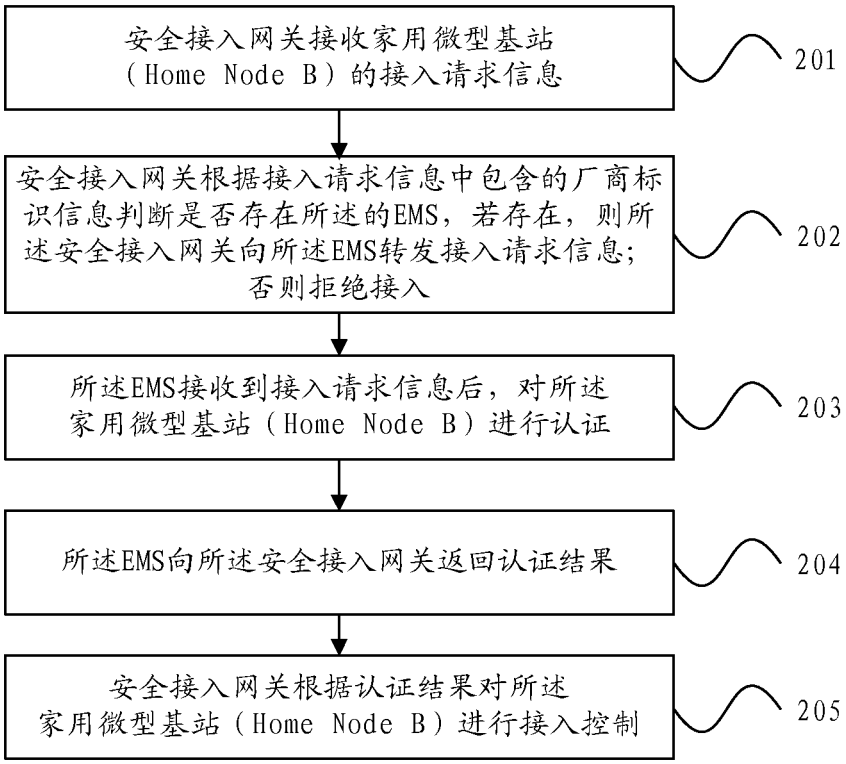

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
201
安全接入网关根据接入请求信息中包含的厂商标识信息判断是否存在所述的EMS，若存在，则所述安全接入网关向所述EMS转发接入请求信息；否则拒绝接入
202
所述EMS接收到接入请求信息后，对所述家用微型基站（Home Node B）进行认证
203
所述EMS向所述安全接入网关返回认证结果
204
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
205

图 2

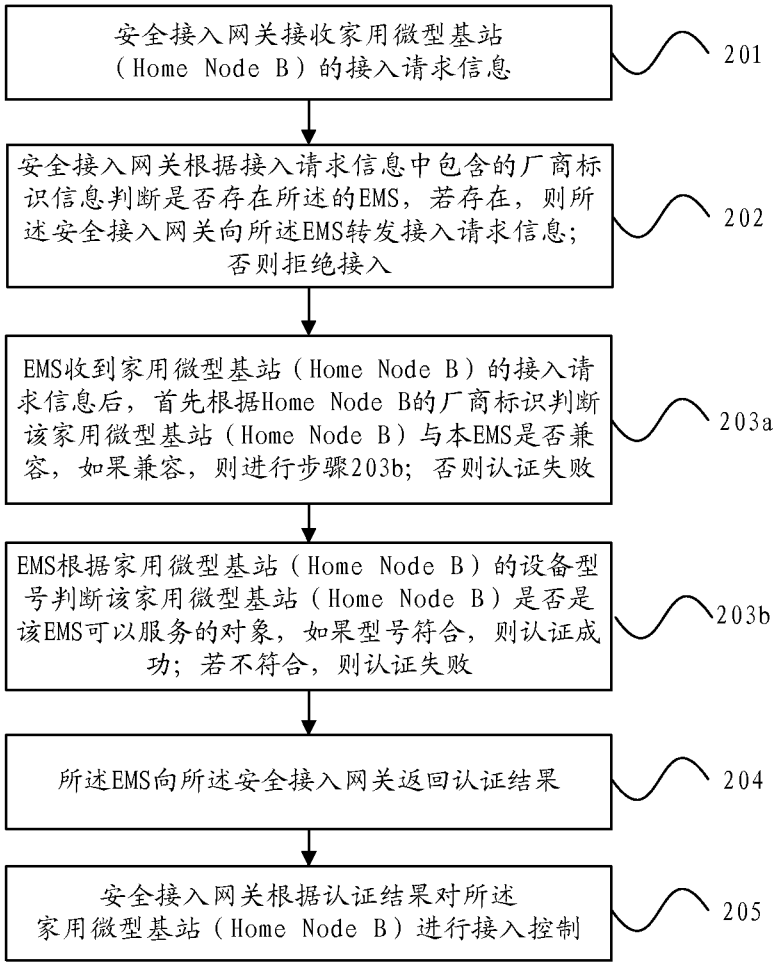

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
201
安全接入网关根据接入请求信息中包含的厂商标识信息判断是否存在所述的EMS，若存在，则所述安全接入网关向所述EMS转发接入请求信息；否则拒绝接入
202
EMS收到家用微型基站（Home Node B）的接入请求信息后，首先根据Home Node B的厂商标识判断该家用微型基站（Home Node B）与本EMS是否兼容，如果兼容，则进行步骤203b；否则认证失败
203a
EMS根据家用微型基站（Home Node B）的设备型号判断该家用微型基站（Home Node B）是否是该EMS可以服务的对象，如果型号符合，则认证成功；若不符合，则认证失败
203b
所述EMS向所述安全接入网关返回认证结果
204
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
205

图 3

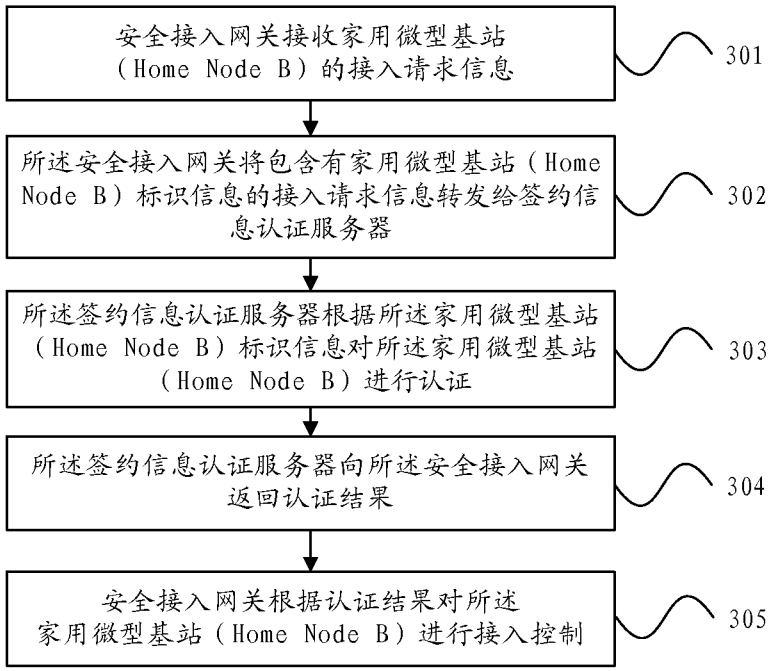

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
301
所述安全接入网关将包含有家用微型基站（Home Node B）标识信息的接入请求信息转发给签约信息认证服务器
302
所述签约信息认证服务器根据所述家用微型基站（Home Node B）标识信息对所述家用微型基站（Home Node B）进行认证
303
所述签约信息认证服务器向所述安全接入网关返回认证结果
304
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
305

图 4

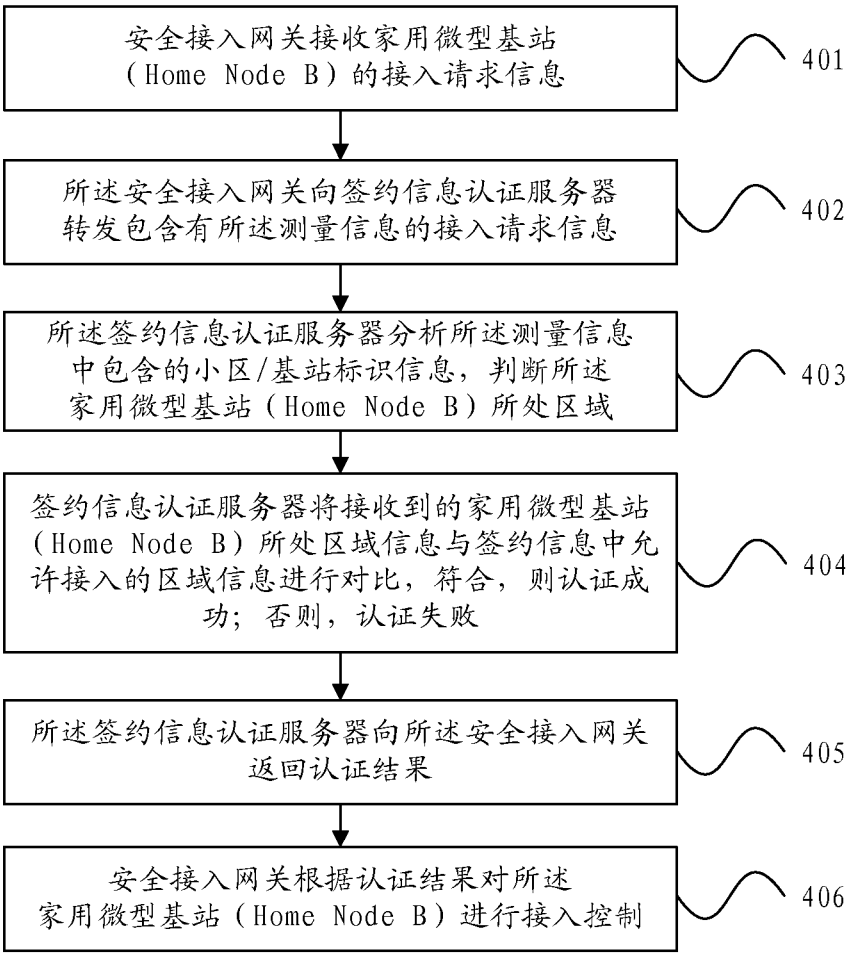

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
401
所述安全接入网关向签约信息认证服务器转发包含有所述测量信息的接入请求信息
402
所述签约信息认证服务器分析所述测量信息中包含的小区/基站标识信息，判断所述家用微型基站（Home Node B）所处区域
403
签约信息认证服务器将接收到的家用微型基站（Home Node B）所处区域信息与签约信息中允许接入的区域信息进行对比，符合，则认证成功；否则，认证失败
404
所述签约信息认证服务器向所述安全接入网关返回认证结果
405
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
406

图 5

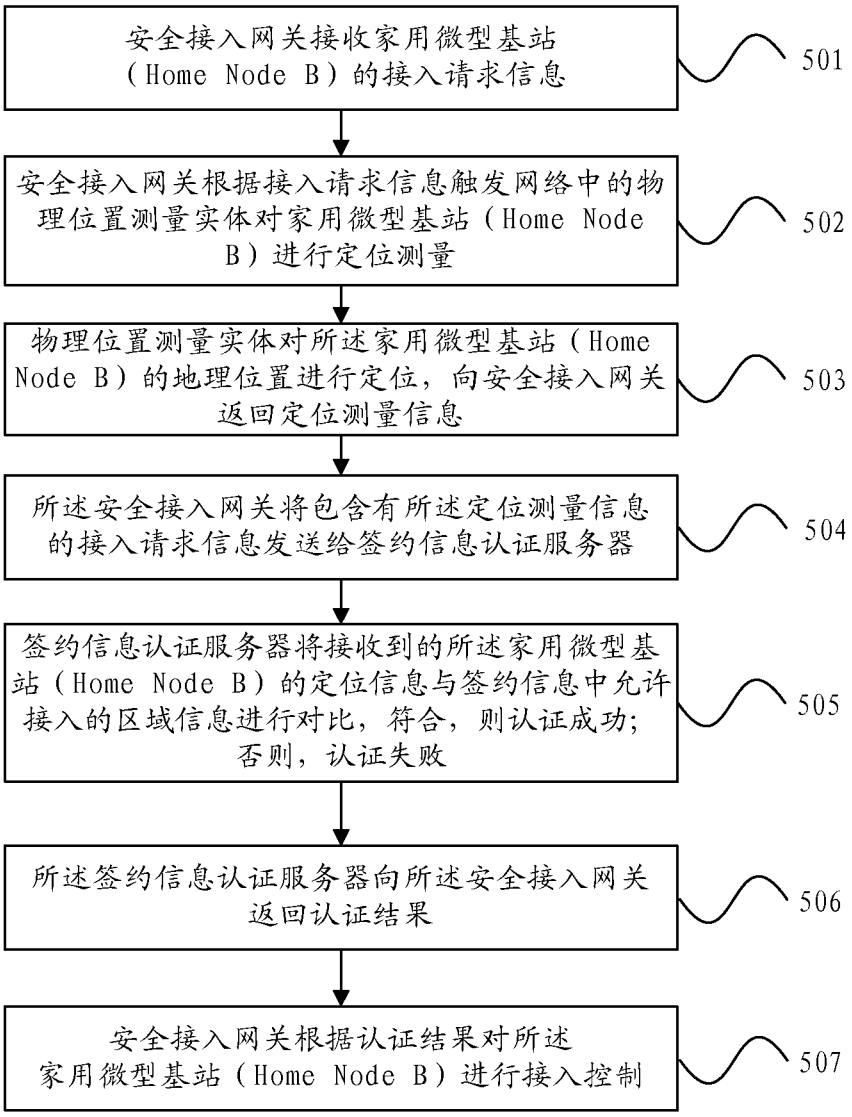

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
501
安全接入网关根据接入请求信息触发网络中的物理位置测量实体对家用微型基站（Home Node B）进行定位测量
502
物理位置测量实体对所述家用微型基站（Home Node B）的地理位置进行定位，向安全接入网关返回定位测量信息
503
所述安全接入网关将包含有所述定位测量信息的接入请求信息发送给签约信息认证服务器
504
签约信息认证服务器将接收到的所述家用微型基站（Home Node B）的定位信息与签约信息中允许接入的区域信息进行对比，符合，则认证成功；否则，认证失败
505
所述签约信息认证服务器向所述安全接入网关返回认证结果
506
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
507

图 6

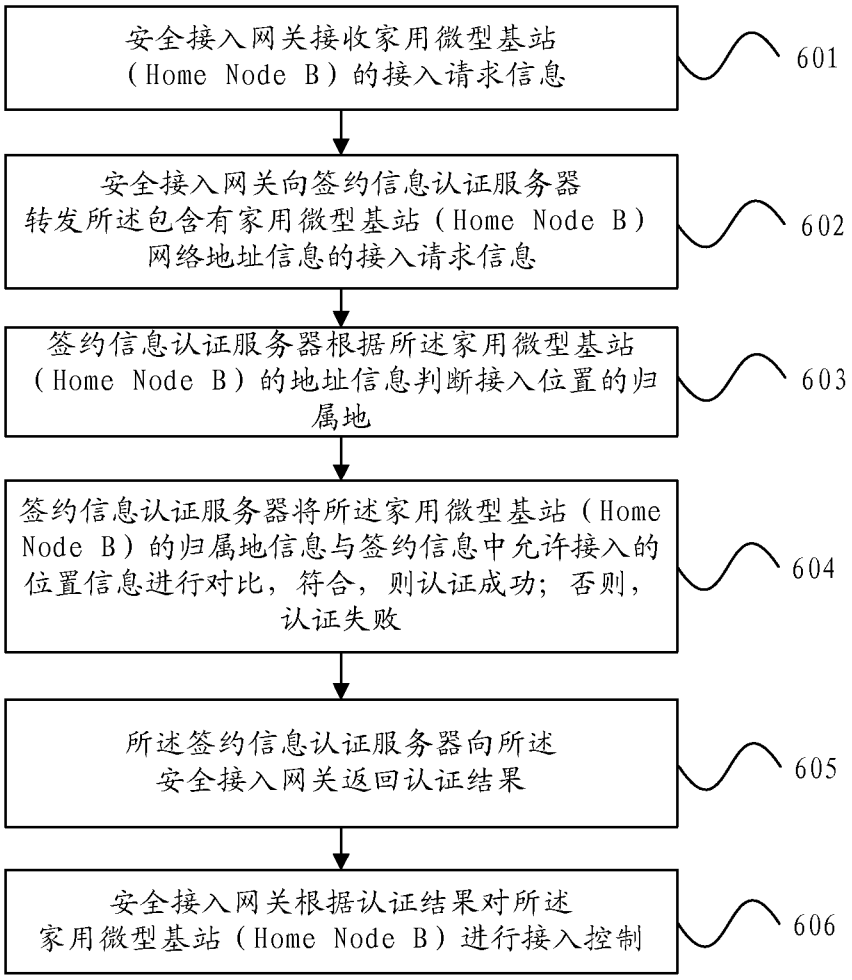

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
601
安全接入网关向签约信息认证服务器转发所述包含有家用微型基站（Home Node B）网络地址信息的接入请求信息
602
签约信息认证服务器根据所述家用微型基站（Home Node B）的地址信息判断接入位置的归属地
603
签约信息认证服务器将所述家用微型基站（Home Node B）的归属地信息与签约信息中允许接入的位置信息进行对比，符合，则认证成功；否则，认证失败
604
所述签约信息认证服务器向所述安全接入网关返回认证结果
605
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
606

图 7

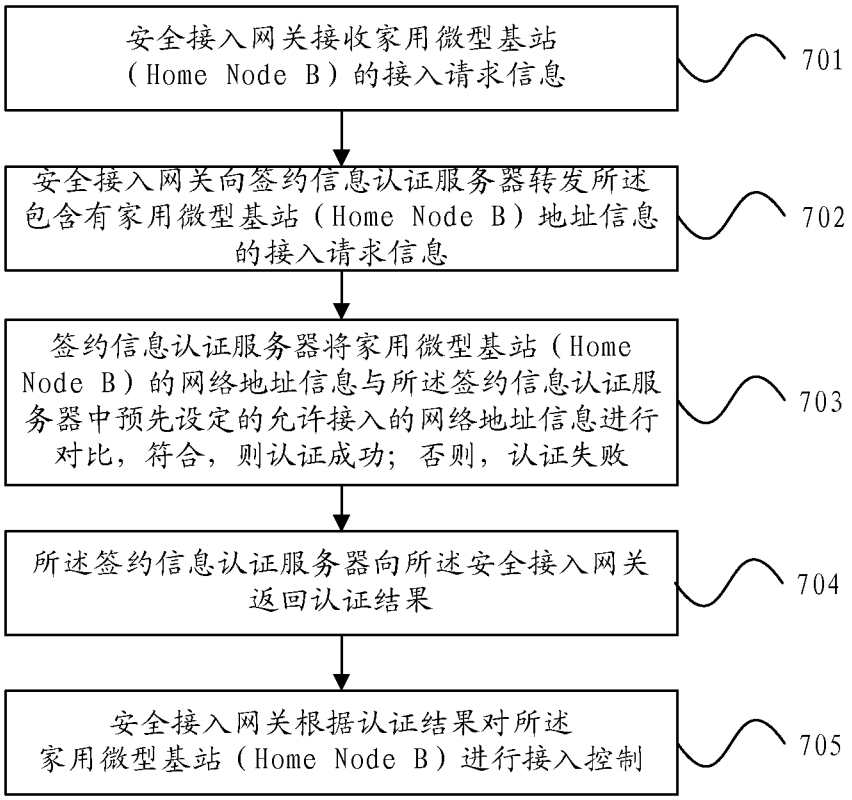

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
701
安全接入网关向签约信息认证服务器转发所述包含有家用微型基站（Home Node B）地址信息的接入请求信息
702
签约信息认证服务器将家用微型基站（Home Node B）的网络地址信息与所述签约信息认证服务器中预先设定的允许接入的网络地址信息进行对比，符合，则认证成功；否则，认证失败
703
所述签约信息认证服务器向所述安全接入网关返回认证结果
704
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
705

图 8

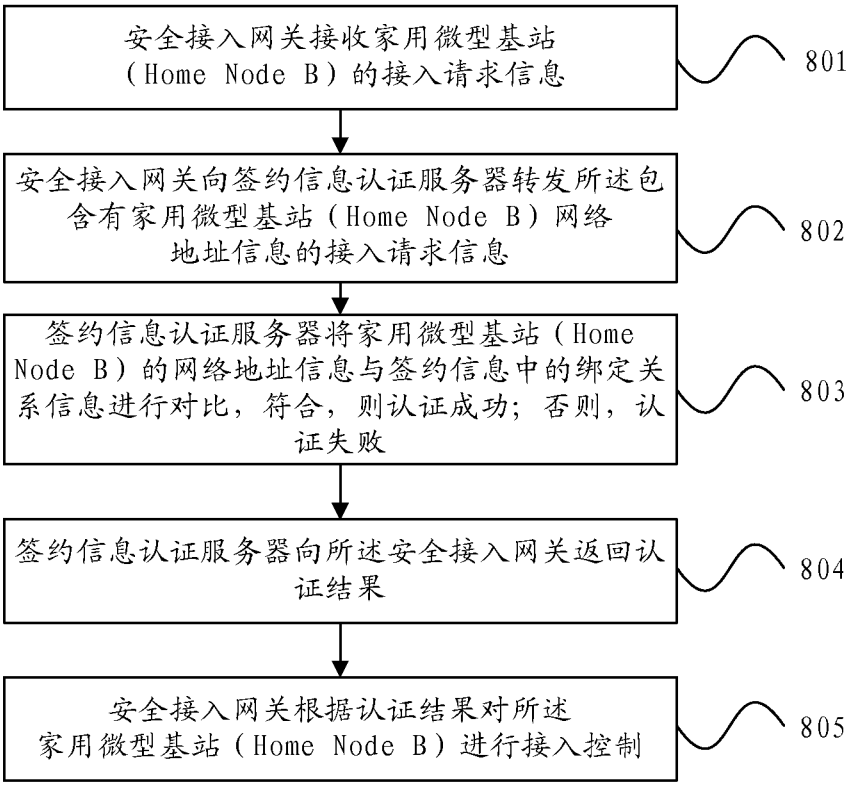

安全接入网关接收家用微型基站（Home Node B）的接入请求信息
801
安全接入网关向签约信息认证服务器转发所述包含有家用微型基站（Home Node B）网络地址信息的接入请求信息
802
签约信息认证服务器将家用微型基站（Home Node B）的网络地址信息与签约信息中的绑定关系信息进行对比，符合，则认证成功；否则，认证失败
803
签约信息认证服务器向所述安全接入网关返回认证结果
804
安全接入网关根据认证结果对所述家用微型基站（Home Node B）进行接入控制
805

图 9

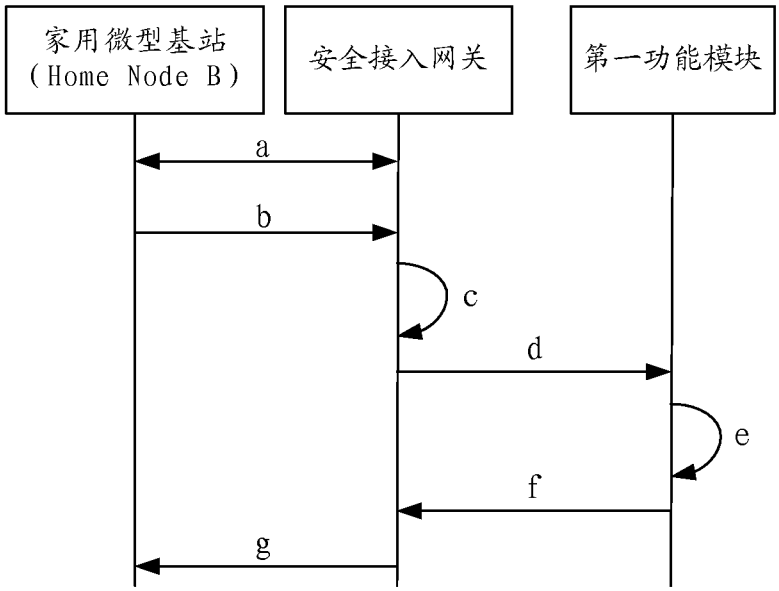

家用微型基站
(Home Node B)
安全接入网关
第一功能模块
a
b
c
d
e
f
g

图 10

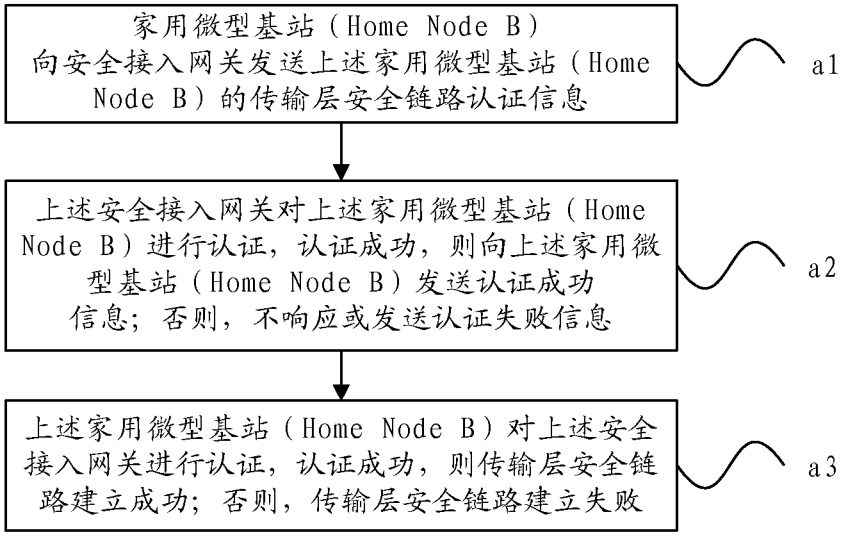

家用微型基站（Home Node B）向安全接入网关发送上述家用微型基站（Home Node B）的传输层安全链路认证信息
a1
上述安全接入网关对上述家用微型基站（Home Node B）进行认证，认证成功，则向上述家用微型基站（Home Node B）发送认证成功信息；否则，不响应或发送认证失败信息
a2
上述家用微型基站（Home Node B）对上述安全接入网关进行认证，认证成功，则传输层安全链路建立成功；否则，传输层安全链路建立失败
a3

图 11

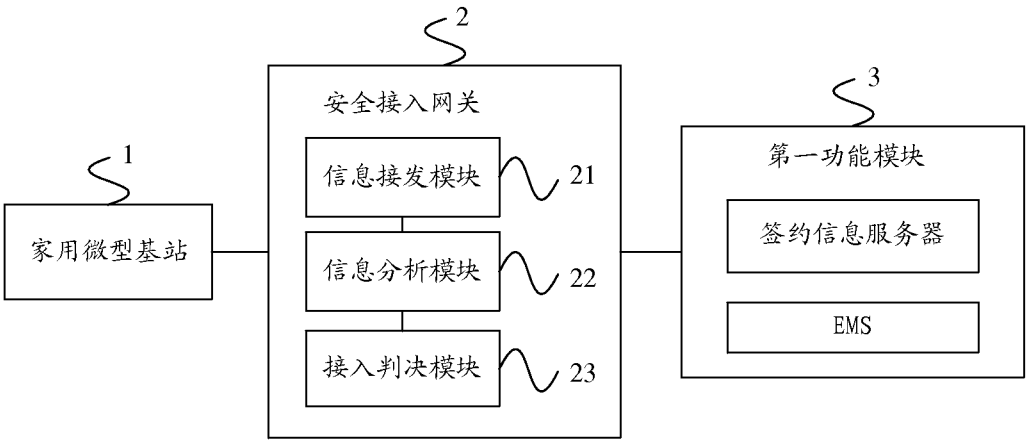

2
安全接入网关
信息接发模块
21
信息分析模块
22
接入判决模块
23
1
家用微型基站
3
第一功能模块
签约信息服务器
EMS

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/071432

A. CLASSIFICATION OF SUBJECT MATTER

H04Q 7/38 (2006.01)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)

IPC: H04Q; H04B; H04M; 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)

CPRS, CNKI, WPI, EPODOC, PAJ: home, pico, femto, indoor, office, base station, node b, hbs, hnd, authen+, verif+, certif+, author+, identi+,regist+, access, control

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US2005239453A1 (VIKBERG,J.T. et al.) 27 Oct. 2005 (27.10.2005) Paragraph 0035 of the description	1-2,4,8,13,16-18
A		3,5-7,9-12,14-15
X	WO0141471A1(ORANGE PERSONAL COMMUNICATIONS SERVICE) 07 June 2001 (07.06.2001) Page 11 lines 1 to 13, page 13 lines 4 to 5, page 19 lines 10 to 13 of the description	1-2,4,8,13,16-18
A		3,5-7,9-12,14-15
A	CN1894979A(INTEL CORP) 10 Jan. 2007 (10.01.2007) The whole document	1-18

☐ 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
28 Aug. 2008 (28.08.2008)	**16 Oct. 2008 (16.10.2008)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WANG,Xiaoli Telephone No. (86-10)62411389

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2008/071432

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2005239453A1	27.10.2005	EP1351530A1	08.10.2003
		EP1351530B1	27.04.2005
		DE60019817E	02.06.2005
		ES2240891T3	16.10.2005
		DE60019817T2	26.01.2006
WO0141471A1	07.06.2001	GB2357009A	06.06.2001
		AU1538301A	12.06.2001
CN1894979A	10.01.2007	WO2005015917A2	17.02.2005
		US2005148368A1	07.07.2005
		EP1661413A2	31.05.2006
		KR20060095937A	05.09.2006

国际检索报告

国际申请号
PCT/CN2008/071432

A. 主题的分类

H04Q 7/38 (2006.01)i

按照国际专利分类表(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)

IPC: H04Q; H04B; H04M; 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））

WPI, EPODOC, PAJ: home, pico, femto, indoor, office, base station, node b, hbs, hnd, authen+, verif+, certif+, author+, identi+,regist+, access, control

CPRS, CNKI: 家用 家庭 微型 皮可 室内 建筑物 基站 节点 接入点 认证 鉴权 鉴别 注册 接入

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	US2005239453A1 (VIKBERG,J.T.等) 27.10 月 2005 (27.10.2005) 说明书第 0035 段	1-2,4,8,13,16-18
A		3,5-7,9-12,14-15
X	WO0141471A1(奥林奇私人通讯服务有限公司) 07.06 月 2001 (07.06.2001) 说明书第 11 页第 1-13 行、第 13 页第 4-5 行、第 19 页 10-13 行	1-2,4,8,13,16-18
A		3,5-7,9-12,14-15
A	CN1894979A(英特尔公司) 10.01 月 2007 (10.01.2007) 说明书全文	1-18

☐ 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

"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
28.8 月 2008 (28.08.2008)	**16.10 月 2008 (16.10.2008)**
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 王晓丽 电话号码：(86-10) **62411389**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2008/071432

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2005239453A1	27.10.2005	EP1351530A1	08.10.2003
		EP1351530B1	27.04.2005
		DE60019817E	02.06.2005
		ES2240891T3	16.10.2005
		DE60019817T2	26.01.2006
WO0141471A1	07.06.2001	GB2357009A	06.06.2001
		AU1538301A	12.06.2001
CN1894979A	10.01.2007	WO2005015917A2	17.02.2005
		US2005148368A1	07.07.2005
		EP1661413A2	31.05.2006
		KR20060095937A	05.09.2006