

(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 2017/128546 A1

- (51) 国际专利分类号:
H04W 12/08 (2009.01) *H04W 12/12* (2009.01)
- (21) 国际申请号: PCT/CN2016/080837
- (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:
201610066994.6 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: 张子敬 (ZHANG, Zijing); 中国广东省深圳
市南山区科技园北区梦溪道2号, Guangdong 518057
(CN)。 路雄博 (LU, Xiongbo); 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 (GUANG-
ZHOU 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: METHOD AND APPARATUS FOR SECURELY ACCESSING WIFI NETWORK

(54) 发明名称: 一种WiFi网络安全接入方法及装置

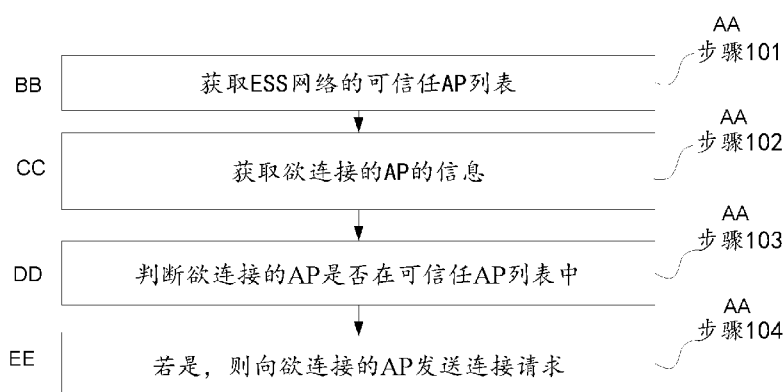


图 1

AA STEP
BB ACQUIRING A TRUSTED AP LIST OF AN ESS NETWORK
CC ACQUIRING INFORMATION ABOUT AN AP TO BE CONNECTED
DD DETERMINING WHETHER THE AP TO BE CONNECTED IS IN THE
TRUSTED AP LIST
EE IF SO, SENDING A CONNECTION REQUEST TO THE AP TO BE
CONNECTED

(57) Abstract: Disclosed are a method and ap-
paratus for securely accessing a WiFi network.
The method comprises: acquiring a trusted
wireless access point (AP) list of an extended
service set (ESS) network; acquiring informa-
tion about an AP to be connected; determining
whether the AP to be connected is in the trusted
AP list; and if so, sending a connection re-
quest to the AP to be connected. According to
the present invention, by checking whether an
AP to be associated with a terminal is a trusted
AP in an ESS network, an attack from a WiFi
rogue access point can be effectively preven-
ted, thereby improving the security of WiFi
network access, and adding to the user experi-
ence.

(57) 摘要: 本发明公开了一种WiFi网络
安全接入方法及装置。该方法包括:
获取扩展服务集ESS网络的可信任无线
接入点AP列表; 获取欲连接的AP的
信息; 判断欲连接的AP是否在可信任
AP列表中; 若是, 则向欲连接的AP发
送连接请求。本发明通过核查终端欲
关联的AP是否为ESS网络中可信任

AP, 可有效阻止WiFi流氓接入点的攻击, 提高WiFi网络接入的安全性, 增加用户体验。

WO 2017/128546 A1

一种 WiFi 网络安全接入方法及装置

本申请要求于 2016 年 1 月 29 日提交中国专利局，申请号为 201610066994.6、发明名称为“一种 WiFi 网络安全接入方法及装置”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。

5

技术领域

本发明涉及网络安全领域，尤其涉及一种 WiFi 网络安全接入方法及装置。

背景技术

10 现有无线网络组网中，通常通过 ESS (Extended Service Set, 扩展服务集) 网络来扩展 WiFi 的覆盖范围。ESS 网络是将几个 BSS (Basic Service Set, 基本服务集) 联合工作以构建一个覆盖更大的网络。在 ESS 网络中，各 BSS 使用相同的 SSID (Service Set Identifier, 服务集标识)，而有不同的 BSSID (Basic Service Set Identifier, 基本服务集标识)，SSID 会显示在各 STA (Station, 站
15 点) 终端的扫描列表中。

对于 STA 终端来说，整个 ESS 网络就像是一个 BSS。在其扫描列表仅能看到 ESS 网络中的一个 AP (Access Point, 无线接入点) 热点，这个热点一般是 ESS 网络中当前位置信号最好的热点。例如，在某大厦中部署了一个 ESS 网络，其网络名称 SSID 为 xinxigang，由于该大厦面积比较大，一个 AP 难以
20 覆盖全面，因此其设立了多个 AP 热点。而这些 AP 热点的 SSID 都设置为 xinxigang，但各 AP 的 BSSID (通常为 Mac 地址) 却是不同的，各 AP 也可工作在不同的信道上。STA 终端在其扫描列表中仅能看到一个 xinxigang 的 AP 热点。

然而在上述场景中，攻击者可能会设置一个 SSID 为 xinxigang 的流氓接入点 AP。通过增大发射功率，来诱骗 STA 终端关联该流氓接入点 AP。攻击者可以对 STA 终端进行中间人攻击 (MITM) 进而盗取用户的资料，对用户的人身及财产造成威胁。因此，WiFi 流氓接入点的存在给 WiFi 安全带来了极大的安全隐患。

30 发明内容

本发明提供了一种 WiFi 网络安全接入方法及装置，用于解决现有技术中 STA 终端连接 WiFi 网络时，容易遭受流氓接入点攻击的问题。

为实现上述发明目的，本发明采用下述的技术方案：

依据本发明的一方面，提供一种 WiFi 网络安全接入方法，包括：

5 获取扩展服务集 ESS 网络的可信任无线接入点 AP 列表；

获取欲连接的 AP 的信息；

判断所述欲连接的 AP 是否在所述可信任 AP 列表中，若是，则向所述欲连接的 AP 发送连接请求。

10 进一步地，获取所述可信任 AP 列表的方式包括数据网络、可识别标签或者手动添加任一种或多种。

进一步地，所述可识别标签包括近场通信 NFC 标签、二维码以及无线射频识别 RFID 标签中任一种或多种。

进一步地，通过所述数据网络获取所述可信任 AP 列表，包括：

15 获取当前的位置信息，将所述位置信息通过所述数据网络发送至管理所述 ESS 网络的服务器，接收所述服务器根据所述位置信息反馈的可信任 AP 列表；

或者，接收管理所述 ESS 网络的服务器通过所述数据网络推送的所述可信任 AP 列表。

进一步地，所述可信任 AP 列表包括所述 ESS 网络中的服务集标识 SSID 以及可信任 AP 的唯一标识码。

20 进一步地，所述唯一标识码为媒介访问控制 MAC 地址或者由管理所述 ESS 网络的服务器配置。

依据本发明的另一方面，提供一种 WiFi 网络安全接入装置，其特征在于，包括：

25 第一获取模块，用于获取扩展服务集 ESS 网络的可信任无线接入点 AP 列表；

第二获取模块，用于获取欲连接的 AP 的信息；

判断模块，用于判断所述欲连接的 AP 是否在所述可信任 AP 列表中；

发送模块，用于当判断所述欲连接的 AP 在所述可信任 AP 列表中，向所述欲连接的 AP 发送连接请求。

30 进一步地，所述第一获取模块获取所述可信任 AP 列表的方式包括数据网

络、可识别标签或者手动添加中的任一种或多种。

进一步地,所述可识别标签包括近场通信 NFC 标签、二维码以及无线射频识别 RFID 标签中的任一种或多种。

进一步地,所述第一获取模块通过所述数据网络获取所述可信任 AP 列表,

5 包括:

获取单元,用于获取当前的位置信息;

发送单元,用于将所述获取单元获取的位置信息通过所述数据网络发送至管理所述 ESS 网络的服务器;

10 第一接收单元,用于接收所述服务器根据所述发送单元发送的位置信息反馈的可信任 AP 列表;

或者包括第二接收单元,用于接收管理所述 ESS 网络的服务器通过所述数据网络推送的所述可信任 AP 列表。

进一步地,所述第一获取模块获取的所述可信任 AP 列表包括所述 ESS 网络的服务集标识 SSID 以及可信任 AP 的唯一标识码。

15 进一步地,所述唯一标识码为媒介访问控制 MAC 地址或者由管理所述 ESS 网络的服务器配置。

本发明有益效果如下:

20 本发明所提供的 WiFi 网络安全接入方法及装置,由 ESS 网络管理者发布该 ESS 网络可信任 AP 列表;当 STA 终端欲和该 ESS 网络的某 AP 关联时,通过可信任 AP 列表中的 AP 信息,核查欲关联的 AP 是否为可信任 AP;当核查通过后,才允许关联,否则不予关联。本发明通过核查终端欲关联的 AP 是否为 ESS 网络中可信任 AP 可有效阻止 WiFi 流氓接入点的攻击,提高 WiFi 网络接入的安全性,增加用户体验。

25 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

30 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍,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性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例中 WiFi 网络安全接入方法的流程图；

图 2 为本发明实施例中采用的可信任 AP 列表的示意图；

5 图 3 为本发明实施例中 WiFi 网络安全接入装置的结构示意图。

具体实施方式

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，所描述的实施例仅仅是本发明一部分实施例，而不是
10 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。

实施例 1

本发明实施例提供了一种 WiFi 网络安全接入方法，适用于 STA 终端，如图 1 所示，该方法具体包括：

- 15 步骤 101，获取 ESS 网络的可信任无线接入点 AP 列表；
步骤 102，获取欲连接的 AP 的信息；
步骤 103，判断欲连接的 AP 是否在所述可信任 AP 列表中；
步骤 104，若是，则向所述欲连接的 AP 发送连接请求。

本实施例中以及下文的几个实施例中提到的 ESS 网络的可信任 AP 列表，
20 具体包括 ESS 网络的 SSID 以及 AP 的唯一标识码。其中，对于唯一标识码，本发明实施例中优选采用 AP 的 MAC (Medium/Media Access Control, 媒介访问控制) 地址，具体形式，如图 2 所示。当然，该唯一标识码也可以由管理 ESS 网络的服务器配置，对每个 AP 进行唯一指定。

在步骤 101 中，对于获取 ESS 网络可信任 AP 列表的方法很多，由 ESS
25 网络通过可信任途径发布，STA 终端通过具有一定安全级别的通信方式获取。具体地，本发明实施例中获取可信任 AP 列表的方式包括：数据网络、可识别标签以及手动添加任一种或多种，后面将结合具体的实施例对获取可信任 AP 列表的过程进行说明，这里不做过多介绍。

在步骤 102 中，对于获取欲连接的 AP 的信息的具体过程，可以由 AP 主
30 动向 STA 终端发送信息，信息中携带 AP 的相关信息，例如 MAC 地址以及信

号强度等；还可以由 STA 终端向 AP 请求获取，对于具体的实现过程，其已经为本领域人员所熟知的技术，具体地，在无线局域网标准 IEEE 802.11 协议簇中有相关介绍，本文不再进行赘述。

在步骤 103~104 中，当 STA 终端获取欲连接的 AP 信息后，根据 SSID 对每个可信任的 AP 信息进行遍历，并将遍历的 AP 信息与欲连接的 AP 信息进行对比；当对比结果一致时，则向欲连接 AP 发送连接请求；当对比结果不一致时，不允许关联该 AP，同时提示用户当前 AP 具有一定的危险性。

实施例 2

本实施例基于实施例 1，在获取 ESS 网络的可信任 AP 列表，通过数据网络实现，具体包括两种方式：主动方式、被动方式。

对于通过数据网络主动获取可信任 AP 列表，包括如下步骤：

获取当前位置信息；

将位置信息通过数据网络发送至管理 ESS 网络的服务器；

当接收到服务器根据该位置信息反馈的可信任 AP 列表后，将可信任 AP 列表配置于本地。

本实施例中获取可信任 AP 列表时，基于用户的位置实现。具体地，STA 终端用户需要首先关注部署该 ESS 网络的管理者信息（例如微信的公共账号等）。通过该 ESS 网络的管理者实现与管理 ESS 网络的服务器侧的信息交互。其中，ESS 网络服务器中预先存储了该 ESS 网络的位置区域。ESS 网络的服务器根据 STA 终端位置可以获取该 ESS 网络的可信任 AP 列表。

以麦当劳为例进行说明。STA 终端用户刚进入某地麦当劳，STA 终端通过 GPS（Global Positioning System，全球定位系统）获取当前的位置信息，并将该位置信息发送至麦当劳公众账号；麦当劳公众账号根据该位置信息判断该位置是否在预先设置的位置区域内；当判断该位置在相应的部署区域时，将该区域的 ESS 网络对应的可信任 AP 列表通过数据网络发送至 STA 终端。

当然，STA 终端可以自动检测并连接可信任的 AP。具体地，STA 终端自动检测当前环境是否存在 ESS 网络；当存在时，获取当前的位置信息，并将该位置信息发送至关注的所有 ESS 网络的管理者；所有 ESS 网络的服务器根据该位置信息判断是否在所属的部署区域内，当确定在部署区域内时，获取可信任的 AP 列表。若当前区域存在多个可用 ESS 网络时，用户可以自行选取可

用网络也可以根据用户预先设置的 ESS 网络信任排名对网络自动选取。对于多个可用 ESS 网络具体的选取过程，可以有多种，本发明不做具体的限定。

对于通过数据网络被动获取可信任 AP 列表时，只需接收 ESS 网络推送的可信任 AP 列表即可。

5 具体地，由 ESS 网络检测进入覆盖区域的 STA 终端信息；当检测到 STA 终端进入 ESS 网络后，通过数据网络将可信任 AP 列表推送至该 STA 终端中。

具体地，对于 ESS 网络推送可信任 AP 列表的时间，需要经过 STA 终端的用户允许，才允许推送。例如，当用户打开 WIFI，需要接入 ESS 网络时，ESS 网络开始向 STA 终端进行推送；或者，当 WIFI 处于打开状态时，ESS 网络检测到 STA 终端进行网络所覆盖的区域时，向 STA 终端询问是否需要连接，当需要时，将可信任 AP 列表推送至 STA 终端。STA 终端接收 ESS 网络推送的可信任 AP 列表，将可信任 AP 列表配置于本地即可。

实施例 3

本实施例基于实施例 1，在获取 ESS 网络的可信任 AP 列表时，通过可识别标签由终端主动获取实现。其中，可识别标签包括 NFC（Near Field Communication，近场通信）标签、二维码以及 RFID（Radio Frequency Identification，无线射频识别）标签等可用于识别并且携带信息的标签。

具体地，本实施例中，可将该 ESS 网络的可信任 AP 列表配置到 NFC 标签/二维码中，或者将可以获取的到该 ESS 网络的可信任 AP 列表信息的链接写入到 NFC 标签/二维码中，STA 终端只有读的权限，STA 终端用户进入该地区时，直接通过 STA 终端的 NFC 功能刷 NFC 标签/二维码即可获取到上述信息，并配置到 STA 终端中。对于读取 RFID 标签，STA 终端可以通过 RFID 读取器读取 RFID 标签的信息。对于 RFID 读取器可以集成于 STA 终端，或者由 ESS 网络侧提供。

25 需要说明的是，本发明对于 STA 终端获取可信任 AP 列表的具体方式并不局限于上述的实施例，用户还通过输入操作将 ESS 网络发布的可信任 AP 通过手动的方式进行添加。因此，对于 STA 终端通过其他方式获取可信任 AP 列表的方法都在本发明的保护范围之内。

实施例 4

30 本发明实施例还提供了一种 WiFi 网络安全接入装置，用于实现实施例 1~3

中任一实施例所提供的方法。参见图 3, 该 WiFi 网络安全接入装置包括:

第一获取模块 201, 用于获取扩展服务集 ESS 网络的可信任无线接入点 AP 列表;

第二获取模块 202, 用于获取欲连接的 AP 的信息;

5 判断模块 203, 用于判断欲连接的 AP 是否在可信任 AP 列表中;

发送模块 204, 用于当判断欲连接的 AP 在可信任 AP 列表中, 向欲连接的 AP 发送连接请求。

进一步地, 第一获取模块 201 获取可信任 AP 列表的方式包括数据网络、可识别标签或者手动添加中的任一种或多种。

10 进一步地, 可识别标签包括近场通信 NFC 标签、二维码以及无线射频识别 RFID 标签中的任一种或多种。

进一步地, 第一获取模块 201 通过数据网络获取可信任 AP 列表, 包括: 获取单元, 用于获取当前的位置信息;

15 发送单元, 用于将获取单元获取的位置信息通过数据网络发送至管理 ESS 网络的服务器;

第一接收单元, 用于接收服务器根据发送单元发送的位置信息反馈的可信任 AP 列表;

或者包括第二接收单元, 用于接收管理 ESS 网络的服务器通过数据网络推送的可信任 AP 列表。

20 进一步地, 第一获取模块 201 获取的可信任 AP 列表包括 ESS 网络的服务集标识 SSID 以及可信任 AP 的唯一标识码。

进一步地, 唯一标识码为媒介访问控制 MAC 地址或者由管理 ESS 网络的服务器配置。

25 综上所述, 本发明实施例所提供的 WiFi 网络安全接入方法及装置, 由 ESS 网络管理者发布该 ESS 网络可信任 AP 列表; 当 STA 终端欲和该 ESS 网络的某 AP 关联时, 通过可信任 AP 列表中的 AP 信息, 核查欲关联的 AP 是否为可信任 AP; 当核查通过后, 才允许关联, 否则不予关联。本发明通过核查终端欲关联的 AP 是否为 ESS 网络中可信任 AP, 可有效阻止 WiFi 流氓接入点的攻击, 提高 WiFi 网络接入的安全性, 增加用户体验。

30 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,

是可以通过计算机程序来指令相关的硬件来完成,程序可存储于计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。

虽然通过实施例描述了本申请,本领域的技术人员知道,本申请有许多变形和变化而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

权利要求

1、一种 WiFi 网络安全接入方法，其特征在于，包括：

获取扩展服务集 ESS 网络的可信任无线接入点 AP 列表；

5 获取欲连接的 AP 的信息；

判断所述欲连接的 AP 是否在所述可信任 AP 列表中；

若是，则向所述欲连接的 AP 发送连接请求。

2、如权利要求 1 所述的方法，其特征在于，获取所述可信任 AP 列表的方式包括数据网络、可识别标签或者手动添加中的任一种或多种。

10 3、如权利要求 2 所述的方法，其特征在于，所述可识别标签包括近场通信 NFC 标签、二维码以及无线射频识别 RFID 标签中的任一种或多种。

4、如权利要求 2 所述的方法，其特征在于，通过所述数据网络获取所述可信任 AP 列表，包括：

15 获取当前的位置信息，将所述位置信息通过所述数据网络发送至管理所述 ESS 网络的服务器，接收所述服务器根据所述位置信息反馈的可信任 AP 列表；
或者，接收管理所述 ESS 网络的服务器通过所述数据网络推送的所述可信任 AP 列表。

5、如权利要求 1~4 任一项所述的方法，其特征在于，所述可信任 AP 列表包括所述 ESS 网络中的服务集标识 SSID 以及可信任 AP 的唯一标识码。

20 6、如权利要求 5 所述的方法，其特征在于，所述唯一标识码为媒介访问控制 MAC 地址或者由管理所述 ESS 网络的服务器配置。

7、一种 WiFi 网络安全接入装置，其特征在于，包括：

第一获取模块，用于获取扩展服务集 ESS 网络的可信任无线接入点 AP 列表；

25 第二获取模块，用于获取欲连接的 AP 的信息；

判断模块，用于判断所述欲连接的 AP 是否在所述可信任 AP 列表中；

发送模块，用于当判断所述欲连接的 AP 在所述可信任 AP 列表中，向所述欲连接的 AP 发送连接请求。

30 8、如权利要求 7 所述的装置，其特征在于，所述第一获取模块获取所述可信任 AP 列表的方式包括数据网络、可识别标签或者手动添加中的任一种或

多种。

9、如权利要求 8 所述的装置，其特征在于，所述可识别标签包括近场通信 NFC 标签、二维码以及无线射频识别 RFID 标签中的任一种或多种。

10、如权利要求 7 所述的装置，其特征在于，所述第一获取模块通过所述
5 数据网络获取所述可信任 AP 列表，包括：

获取单元，用于获取当前的位置信息；

发送单元，用于将所述获取单元获取的位置信息通过所述数据网络发送至
管理所述 ESS 网络的服务器；

10 第一接收单元，用于接收所述服务器根据所述发送单元发送的位置信息反
馈的可信任 AP 列表；

或者包括第二接收单元，用于接收管理所述 ESS 网络的服务器通过所述
数据网络推送的所述可信任 AP 列表。

11、如权利要求 7~10 任一项所述的装置，其特征在于，所述第一获取模
块获取的所述可信任 AP 列表包括所述 ESS 网络的服务集标识 SSID 以及可信
15 任 AP 的唯一标识码。

12、如权利要求 11 所述的装置，其特征在于，所述唯一标识码为媒介访问控制 MAC 地址或者由管理所述 ESS 网络的服务器配置。

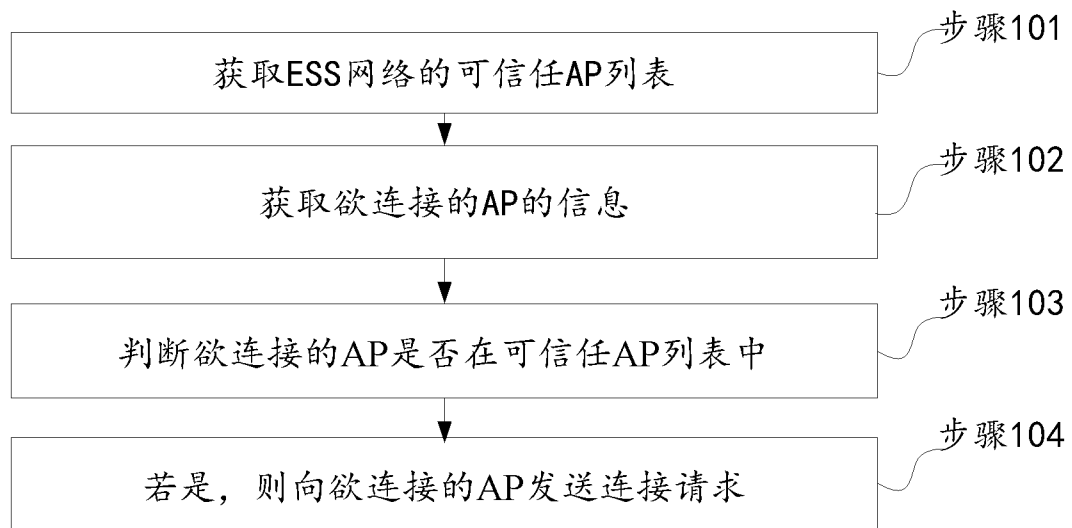


图 1

ESS 网络 SSID	可信任 AP 的 MAC 地址列表
WanKe	11:22:33:44:55:66
	11:22:33:44:55:67
	11:22:33:44:55:68
xinxigang	11:22:33:44:55:69
	11:22:33:44:55:70
	11:22:33:44:55:71
KFC-YingHua	11:22:33:44:55:72

图 2



图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/080837

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08 (2009.01) i; 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, H04L, H04Q

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; SIPOABS; VEN; USTXT; CNKI: extended service set; wifi, access, connect, link, safe, trust, AP, ESS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104580152 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES), 29 April 2015 (29.04.2015), description, paragraphs [0006]-[0084]	1-12
X	CN 102231887 A (SHENZHEN TEMOBI SCIENCE & TECH DEVELOPMENT CO., LTD.), 02 November 2011 (02.11.2011), description, paragraphs [0010]-[0013]	1-12
A	CN 104270366 A (BEIJING KINGSOFT SECURITY SOFTWARE CO., LTD.), 07 January 2015 (07.01.2015), the whole document	1-12
A	US 7693516 B2 (VTECH TELECOMMUNICATIONS LIMITED et al.), 06 April 2010 (06.04.2010), the whole document	1-12
A	CN 104320408 A (SUN YAT-SEN UNIVERSITY), 28 January 2015 (28.01.2015), the whole document	1-12
A	CN 103188824 A (SAMSUNG SDI CO., LTD.), 03 July 2013 (03.07.2013), the whole document	1-12

☒ 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 02 September 2016 (02.09.2016)	Date of mailing of the international search report 13 October 2016 (13.10.2016)
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 CAO, Juan Telephone No.: (86-10) 62411251

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/080837

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102355668 A (SHENZHEN TEMOBI SCIENCE & TECH DEVELOPMENT CO., LTD.), 15 February 2012 (15.02.2012), the whole document	1-12

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/080837

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104580152 A	29 April 2015	None	
CN 102231887 A	02 November 2011	None	
CN 104270366 A	07 January 2015	None	
US 7693516 B2	06 April 2010	US 2006209773 A1	21 September 2006
CN 104320408 A	28 January 2015	None	
CN 103188824 A	03 July 2013	EP 2611079 A1	03 July 2013
		KR 20130080487 A	15 July 2013
		US 2013173811 A1	04 July 2013
CN 102355668 A	15 February 2012	None	

国际检索报告

国际申请号

PCT/CN2016/080837

A. 主题的分类 H04W 12/08(2009.01)i; 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, H04L, H04Q 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;SIPOABS;VEN;USTXT;CNKI:wifi、访问、接入、连接、安全、信任、AP、扩展服务集、ESS:wifi, access, connect, link, safe, trust, AP, ESS																							
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 104580152 A (中国科学院信息工程研究所) 2015年 4月 29日 (2015 - 04 - 29) 说明书第[0006]-[0084]段</td> <td>1-12</td> </tr> <tr> <td>X</td> <td>CN 102231887 A (深圳市融创天下科技股份有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书[0010]-[0013]段</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 104270366 A (北京金山安全软件有限公司) 2015年 1月 7日 (2015 - 01 - 07) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>US 7693516 B2 (伟易达电讯有限公司等) 2010年 4月 6日 (2010 - 04 - 06) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 104320408 A (中山大学) 2015年 1月 28日 (2015 - 01 - 28) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 103188824 A (三星电子株式会社) 2013年 7月 3日 (2013 - 07 - 03) 全文</td> <td>1-12</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 104580152 A (中国科学院信息工程研究所) 2015年 4月 29日 (2015 - 04 - 29) 说明书第[0006]-[0084]段	1-12	X	CN 102231887 A (深圳市融创天下科技股份有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书[0010]-[0013]段	1-12	A	CN 104270366 A (北京金山安全软件有限公司) 2015年 1月 7日 (2015 - 01 - 07) 全文	1-12	A	US 7693516 B2 (伟易达电讯有限公司等) 2010年 4月 6日 (2010 - 04 - 06) 全文	1-12	A	CN 104320408 A (中山大学) 2015年 1月 28日 (2015 - 01 - 28) 全文	1-12	A	CN 103188824 A (三星电子株式会社) 2013年 7月 3日 (2013 - 07 - 03) 全文	1-12
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
X	CN 104580152 A (中国科学院信息工程研究所) 2015年 4月 29日 (2015 - 04 - 29) 说明书第[0006]-[0084]段	1-12																					
X	CN 102231887 A (深圳市融创天下科技股份有限公司) 2011年 11月 2日 (2011 - 11 - 02) 说明书[0010]-[0013]段	1-12																					
A	CN 104270366 A (北京金山安全软件有限公司) 2015年 1月 7日 (2015 - 01 - 07) 全文	1-12																					
A	US 7693516 B2 (伟易达电讯有限公司等) 2010年 4月 6日 (2010 - 04 - 06) 全文	1-12																					
A	CN 104320408 A (中山大学) 2015年 1月 28日 (2015 - 01 - 28) 全文	1-12																					
A	CN 103188824 A (三星电子株式会社) 2013年 7月 3日 (2013 - 07 - 03) 全文	1-12																					
☒ 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 2016年 9月 2日		国际检索报告邮寄日期 2016年 10月 13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 曹娟 电话号码 (86-10)62411251																					

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 102355668 A (深圳市融创天下科技股份有限公司) 2012年 2月 15日 (2012 - 02 - 15) 全文	1-12

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/080837

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	104580152	A	2015年 4月 29日	无			
CN	102231887	A	2011年 11月 2日	无			
CN	104270366	A	2015年 1月 7日	无			
US	7693516	B2	2010年 4月 6日	US	2006209773	A1	2006年 9月 21日
CN	104320408	A	2015年 1月 28日	无			
CN	103188824	A	2013年 7月 3日	EP	2611079	A1	2013年 7月 3日
				KR	20130080487	A	2013年 7月 15日
				US	2013173811	A1	2013年 7月 4日
CN	102355668	A	2012年 2月 15日	无			