

(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 2018/000674 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01) H04W 12/08 (2009.01)

(21) 国际申请号: PCT/CN2016/103876

(22) 国际申请日: 2016 年 10 月 29 日 (29.10.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610514279.4 2016年6月30日 (30.06.2016) 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)。

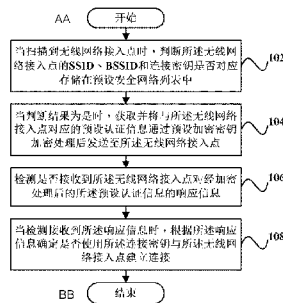
(72) 发明人: 田永胜 (TIAN, Yongsheng); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(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, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) Title: NETWORK CONNECTION METHOD, NETWORK CONNECTION DEVICE, AND TERMINAL

(54) 发明名称: 网络连接方法、网络连接装置和终端



[Fig. 1]

102 WHEN A WIRELESS NETWORK ACCESS POINT IS SCANNED, DETERMINING WHETHER AN SSID, A BSSID AND A CONNECTION SECRET KEY OF THE WIRELESS NETWORK ACCESS POINT ARE CORRESPONDINGLY STORED IN A PRE-SET SECURE NETWORK LIST

104 WHEN THE DETERMINATION RESULT IS YES, ACQUIRING PRE-SET AUTHENTICATION INFORMATION CORRESPONDING TO THE WIRELESS NETWORK ACCESS POINT AND PERFORMING ENCRYPTION PROCESSING ON SAME BY MEANS OF A PRE-SET ENCRYPTION KEY, AND THEN SENDING SAME TO THE WIRELESS NETWORK ACCESS POINT

106 DETECTING WHETHER RESPONSE INFORMATION ABOUT THE WIRELESS NETWORK ACCESS POINT TO THE PRE-SET AUTHENTICATION INFORMATION SUBJECTED TO ENCRYPTION PROCESSING IS RECEIVED

108 WHEN THE RESPONSE INFORMATION IS RECEIVED, DETERMINING, ACCORDING TO THE RESPONSE INFORMATION, WHETHER TO USE THE CONNECTION SECRET KEY TO ESTABLISH A CONNECTION WITH THE WIRELESS NETWORK ACCESS POINT

AA START
BB END

(57) Abstract: Provided are a network connection method, a network connection device, and a terminal. The network connection method comprises: when a wireless network access point is scanned, determining whether an SSID, a BSSID and a connection secret key of the wireless network access point are correspondingly stored in a pre-set secure network list; when the determination result is yes, acquiring pre-set authentication information corresponding to the wireless network access point and performing encryption processing on same by means of a pre-set encryption key, and then sending same to the wireless network access point; detecting whether response information about the wireless network access point to the pre-set authentication information subjected to encryption processing is received; and when it is detected that the response information is received, determining, according to the response information, whether to use the connection secret key to establish a connection with the wireless network access point. The technical solution can effectively improve the security of automatic connection to a wireless network, and avoid the phishing, thereby ensuring the information security of a user and improving the usage security experience of the user.

(57) 摘要: 本发明提出了一种网络连接方法、网络连接装置和终端, 其中, 所述网络连接方法包括: 当扫描到无线网络接入点时, 判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中; 当判断结果为是时, 获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密处理后发送至所述无线网络接入点; 检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息; 当检测接收到所述响应信息时, 根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。该技术方案, 可以有效地提高自动连接无线网络的安全性, 避免连接到钓鱼网络, 从而确保用户的信息安全, 提升用户的使用安全性体验。

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))。

网络连接方法、网络连接装置和终端

- [1] 本申请要求于2016年6月30日提交中国专利局，申请号为201610514279.4、发明名称为“网络连接方法、网络连接装置和终端”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] 本发明涉及通信技术领域，具体而言，涉及一种网络连接方法、网络连接装置和终端。

背景技术

- [3] 目前，AP（Access Point，接入点）热点（也称WIFI（Wireless Fidelity，无线网络）热点）安全问题越来越受重视。其中一个使用场景如下：用户习惯于将WIFI设置中的自动连接功能打开，当下次碰到具有相同的SSID（Service Set Identifier，服务集识别码）和连接密钥的AP热点时可以自动连接，比如，曾经连接过某商场的公共AP热点后，下次再次来到该商场后即可自动连接到该AP热点，从而畅游网络。
- [4] 但是，一些违法分子会利用搭建与某AP热点相同的SSID和连接密钥的钓鱼AP热点，诱导用户的终端（比如手机、平板电脑等）进行自动连接，从而盗取用户信息，比如，用户在某处连接过SSID为AAA、连接密钥为PPP的公共热点，同时设置了自动连接，则在违法分子建立了具有相同的SSID和连接密钥的钓鱼AP热点后，由于用户设置了自动连接功能，当进入到钓鱼AP热点的覆盖区域时，用户的终端则会立即连接到该钓鱼AP热点，然后违法分子便可以利用相关技术窃取用户信息。
- [5] 同时，在某些技术方案中，用户的终端在连接合法AP热点后，获取此AP热点的BSSID（Basic Service Set Identifier，基础服务集标识）并记录到终端中，当下次再次连接时，在验证SSID和连接密钥的同时也要验证BSSID，从而达到避免连接到钓鱼AP热点的目的，但某些高级违法分子，可以通过技术手段伪装钓鱼AP热点的BSSID，即伪装成合法AP的BSSID，从而使得该技术方案中通过验证A

P的BSSID来避免连接到钓鱼AP热点失去效力。

- [6] 因此，如何提高自动连接无线网络的安全性，避免连接到钓鱼网络，从而确保用户的信息安全，提升用户的使用安全性体验，成为亟待解决的技术问题。

对发明的公开

发明内容

- [7] 本发明正是基于上述问题，提出了一种新的技术方案，可以有效地提高自动连接无线网络的安全性，避免连接到钓鱼网络，从而确保用户的信息安全，提升用户的使用安全性体验。
- [8] 有鉴于此，根据本发明的第一方面，提出了一种网络连接方法，包括：当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；当判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密处理后发送至所述无线网络接入点；检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。
- [9] 在该技术方案中，当终端启动自动连接网络功能并扫描到之前连接过的无线网络接入点时，在自动连接之前，首先判断该无线网络接入点是否为安全接入点，即判断其SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中，并在判定为是时，通过预设加密密钥对与该无线网络接入点对应的预设认证信息进行加密处理后发送至该无线网络接入点，进而根据该无线网络接入点反馈的对上述经过加密处理的预设认证信息的响应信息确定是否使用对应的连接密钥与该无线网络接入点建立连接，如此，通过多层验证实现对合法的无线网络的验证识别，从而避免连接到钓鱼网络，确保用户的信息安全，则有效地提高了自动连接无线网络的安全性，提升了用户的使用安全性体验。
- [10] 在上述技术方案中，优选地，可以先判断所述无线网络接入点的SSID和连接密钥是否对应存储在预设安全网络列表中，并当判定为是时，进一步判断所述无线网络接入点的BSSID是否与所述SSID和连接密钥对应存储在所述预设安全网络列表中，以对该无线网络接入点进行初步的安全验证。

- [11] 在上述技术方案中，优选地，所述当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接，具体包括：判断所述响应消息是否与预设信息匹配；当判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；当判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。
- [12] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，根据该响应信息是否与预设信息匹配的判断结果确定是否可以使用对应的连接密钥安全地连接至该无线网络接入点，即通过与无线网络接入点之间预先协商好的安全验证方式，在自动连接该无线网络接入点之前先进行安全性验证，则可以确保连接的无线网络为可信任的安全网络，具体地，当无线网络接入点反馈的响应信息与预设信息匹配时，则使用对应的连接密钥自动与该无线网络接入点建立连接，否则可以通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。
- [13] 在上述任一技术方案中，优选地，在所述判断所述响应消息是否与预设信息匹配之前，包括：通过预设解密密钥对所述响应信息进行解密处理；以及所述判断所述响应消息是否与预设信息匹配，具体包括：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。
- [14] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，首先通过预设解密密钥对该响应信息进行解密处理，进而通过判断经解密处理后的响应信息是否与预设信息匹配，以确定是否使用对应的连接密钥与该无线网络接入点建立连接，即在与无线网络接入点之间进行预设认证信息和响应信息的传输过程中，进行加解密处理，以提高信息传输过程中的安全性，进一步提高网络连接的安全性。
- [15] 其中，预设加密密钥和预设解密密钥可以对应的存储在上述预设安全网络列表中进行统一管理，进一步地，预设加密密钥和预设解密密钥为同一密钥，即在

该预设安全网络列表中，对应存储任一已安全连接过的无线网络接入点的SSID、BSSID、连接密钥、预设认证信息以及用于对该预设认证信息进行加解密处理的加解密密钥。

[16] 在上述任一技术方案中，优选地，当检测在预设时间内未接收所述响应信息时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[17] 在该技术方案中，当向无线网络接入点发送经加密处理的预设认证信息后，若在预设时间内未接收到该无线网络接入点对应的响应信息时，即可通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[18] 根据本发明的第二方面，提出了一种网络连接装置，包括：判断模块，设置为当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；处理模块，设置为当所述判断模块的判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密后发送至所述无线网络接入点；检测模块，设置为检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；确定模块，设置为当所述检测模块检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。

[19] 在该技术方案中，当终端启动自动连接网络功能并扫描到之前连接过的无线网络接入点时，在自动连接之前，首先判断该无线网络接入点是否为安全接入点，即判断其SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中，并在判定为是时，通过预设加密密钥对与该无线网络接入点对应的预设认证信息进行加密处理后发送至该无线网络接入点，进而根据该无线网络接入点反馈的对上述经过加密处理的预设认证信息的响应信息确定是否使用对应的连接密钥与该无线网络接入点建立连接，如此，通过多层验证实现对合法的无线网络的验证识别，从而避免连接到钓鱼网络，确保用户的信息安全，则有效地提高了自动连接无线网络的安全性，提升了用户的使用安全性体验。

[20] 在上述技术方案中，优选地，可以先判断所述无线网络接入点的SSID和连接密

钥是否对应存储在预设安全网络列表中，并当判定为是时，进一步判断所述无线网络接入点的BSSID是否与所述SSID和连接密钥对应存储在所述预设安全网络列表中，以对该无线网络接入点进行初步的安全验证。

[21] 在上述技术方案中，优选地，所述确定模块具体包括：判断子模块，设置为判断所述响应消息是否与预设信息匹配；网络连接子模块，设置为当所述判断子模块判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；提示子模块，设置为当所述判断子模块判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[22] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，根据该响应信息是否与预设信息匹配的判断结果确定是否可以使用对应的连接密钥安全地连接至该无线网络接入点，即通过与无线网络接入点之间预先协商好的安全验证方式，在自动连接该无线网络接入点之前先进行安全性验证，则可以确保连接的无线网络为可信任的安全网络，具体地，当无线网络接入点反馈的响应信息与预设信息匹配时，则使用对应的连接密钥自动与该无线网络接入点建立连接，否则可以通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[23] 在上述任一技术方案中，优选地，所述确定模块具体还包括：解密子模块，设置为通过预设解密密钥对所述响应信息进行解密处理；以及所述判断子模块具体设置为：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。

[24] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，首先通过预设解密密钥对该响应信息进行解密处理，进而通过判断经解密处理后的响应信息是否与预设信息匹配，以确定是否使用对应的连接密钥与该无线网络接入点建立连接，即在与无线网络接入点之间进行预设认证信息和响应信息的传输过程中，进行加解密处理，以提高信息传输过程中的安全

性，进一步提高网络连接的安全性。

[25] 其中，预设加密密钥和预设解密密钥可以对应的存储在上述预设安全网络列表中进行统一管理，进一步地，预设加密密钥和预设解密密钥为同一密钥，即在该预设安全网络列表中，对应存储任一已安全连接过的无线网络接入点的SSID、BSSID、连接密钥、预设认证信息以及用于对该预设认证信息进行加解密处理的加解密密钥。

[26] 在上述任一技术方案中，优选地，还包括：提示模块，设置为当所述检测模块检测在预设时间内未接收所述响应信息时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[27] 在该技术方案中，当向无线网络接入点发送经加密处理的预设认证信息后，若在预设时间内未接收到该无线网络接入点对应的响应信息时，即可通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[28] 根据本发明的第三方面，提出了一种终端，包括：如上述技术方案中任一项所述的网络连接装置，因此，该终端具有如上述技术方案中任一项所述的网络连接装置的所有有益效果，在此不再赘述。

[29] 通过本发明的技术方案，可以有效地提高自动连接无线网络的安全性，避免连接到钓鱼网络，从而确保用户的信息安全，提升用户的使用安全性体验。

附图说明

[30] 图1示出了根据本发明的第一实施例的网络连接方法的流程示意图；

[31] 图2示出了根据本发明的实施例的响应信息与预设信息的匹配判断流程示意图；

[32] 图3示出了根据本发明的实施例网络连接装置的示意框图；

[33] 图4示出了图3中所示的确定模块的示意框图；

[34] 图5示出了根据本发明的实施例的终端的示意框图；

[35] 图6示出了根据本发明的实施例的终端和无线网络接入点的交互流程示意图；

[36] 图7示出了根据本发明的第二实施例的网络连接方法的流程示意图；

[37] 图8示出了根据本发明的实施例的终端的示意框图。

具体实施方式

[38] 为了可以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。

[39] 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，本发明还可以采用其他不同于在此描述的方式来实施，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。

[40] 图1示出了根据本发明的第一实施例的网络连接方法的流程示意图。

[41] 如图1所示，根据本发明的第一实施例的网络连接方法，包括以下流程步骤：

[42] 步骤102，当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；

[43] 步骤104，当判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密处理后发送至所述无线网络接入点；

[44] 步骤106，检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；

[45] 步骤108，当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。

[46] 在该技术方案中，当终端启动自动连接网络功能并扫描到之前连接过的无线网络接入点时，在自动连接之前，首先判断该无线网络接入点是否为安全接入点，即判断其SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中，并在判定为是时，通过预设加密密钥对与该无线网络接入点对应的预设认证信息进行加密处理后发送至该无线网络接入点，进而根据该无线网络接入点反馈的对上述经过加密处理的预设认证信息的响应信息确定是否使用对应的连接密钥与该无线网络接入点建立连接，如此，通过多层验证实现对合法的无线网络的验证识别，从而避免连接到钓鱼网络，确保用户的信息安全，则有效地提高了自动连接无线网络的安全性，提升了用户的使用安全性体验。

[47] 在上述技术方案中，优选地，可以先判断所述无线网络接入点的SSID和连接密

钥是否对应存储在预设安全网络列表中，并当判定为是时，进一步判断所述无线网络接入点的BSSID是否与所述SSID和连接密钥对应存储在所述预设安全网络列表中，以对该无线网络接入点进行初步的安全验证，具体地，预设安全网络列表可以表现为如下表1所示：

[48] 表1

[49] [Table 1]

编号	SSID	PSK	BSSID	加解密密钥	认证信息
1	SSID1	xxx	BSSID1	密钥1	认证信息1
2	SSID2	xxx	BSSID2	密钥2	认证信息2
...	...	...	...	...	...

[50] 在该表1中，SSID即为无线网络名称，PSK（Pre-shared Key，预共享密钥）表示连接到对应的无线网络的连接密钥，BSSID即要连接的接入点的BSSID，这里，预设加密密钥和预设解密密钥相同，上述表结构为基础表结构，如有需要可适当增删。

[51] 其中，与该无线网络接入点对应的预设认证信息和其对该预设认证信息的响应信息可以为相同的信息，也可以为不同的信息，具体可以为系统默认值也可以由用户自行设定，以用于终端与接入点之间的进行网络安全性的验证协商，比如，可以为无线网络的SSID或BSSID中一个部分或变形，也可以为二者的组合。

[52] 如图2所示，步骤108具体包括以下流程步骤：

[53] 步骤1082，判断所述响应消息是否与预设信息匹配；

[54] 步骤1084，当判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；

[55] 步骤1086，当判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[56] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，根据该响应消息是否与预设信息匹配的判断结果确定是否可以使用

对应的连接密钥安全地连接至该无线网络接入点，即通过与无线网络接入点之间预先协商好的安全验证方式，在自动连接该无线网络接入点之前先进行安全性验证，则可以确保连接的无线网络为可信任的安全网络，具体地，当无线网络接入点反馈的响应信息与预设信息匹配时，则使用对应的连接密钥自动与该无线网络接入点建立连接，否则可以通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[57] 当然，在该技术方案中，当检测到响应信息与预设信息不匹配时，可以直接拒绝连接到该无线网络接入点，避免任何由于连接到该无线网络接入点可能带来的安全隐患。

[58] 根据本发明的实施例，在上述步骤1082之前，包括：通过预设解密密钥对所述响应信息进行解密处理；以及步骤1082进一步地具体包括：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。

[59] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，首先通过预设解密密钥对该响应信息进行解密处理，进而通过判断经解密处理后的响应信息是否与预设信息匹配，以确定是否使用对应的连接密钥与该无线网络接入点建立连接，即在与无线网络接入点之间进行预设认证信息和响应信息的传输过程中，进行加解密处理，以提高信息传输过程中的安全性，进一步提高网络连接的安全性。

[60] 其中，预设加密密钥和预设解密密钥可以对应的存储在上述预设安全网络列表中进行统一管理，进一步地，预设加密密钥和预设解密密钥为同一密钥，即在该预设安全网络列表中，对应存储任一已安全连接过的无线网络接入点的SSID、BSSID、连接密钥、预设认证信息以及用于对该预设认证信息进行加解密处理的加解密密钥。

[61] 在上述任一实施例中，若上述步骤106的检测结果为未接收到无线网络接入点对经加密处理的预设认证信息的响应信息，且未接收到的时间达到了预设时间，则提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

- [62] 在该技术方案中，当向无线网络接入点发送经加密处理的预设认证信息后，若在预设时间（比如2分钟）内未接收到该无线网络接入点对应的响应信息时，即可通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。
- [63] 当然，在该技术方案中，当未接收到响应信息时，可以直接拒绝连接到该无线网络接入点，避免任何由于连接到该无线网络接入点可能带来的安全隐患。
- [64] 图3示出了根据本发明的第一实施例的网络连接装置的示意框图。
- [65] 如图3所示，根据本发明的第一实施例的网络连接装置300，包括：判断模块302、处理模块304、检测模块306和确定模块308。
- [66] 其中，判断模块302，设置为当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；处理模块304，设置为当所述判断模块302的判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密后发送至所述无线网络接入点；检测模块306，设置为检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；确定模块308，设置为当所述检测模块306检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。
- [67] 在该技术方案中，当终端启动自动连接网络功能并扫描到之前连接过的无线网络接入点时，在自动连接之前，首先判断该无线网络接入点是否为安全接入点，即判断其SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中，并在判定为是时，通过预设加密密钥对与该无线网络接入点对应的预设认证信息进行加密处理后发送至该无线网络接入点，进而根据该无线网络接入点反馈的对上述经过加密处理的预设认证信息的响应信息确定是否使用对应的连接密钥与该无线网络接入点建立连接，如此，通过多层验证实现对合法的无线网络的验证识别，从而避免连接到钓鱼网络，确保用户的信息安全，则有效地提高了自动连接无线网络的安全性，提升了用户的使用安全性体验。
- [68] 其中，与该无线网络接入点对应的预设认证信息和其对该预设认证信息的响应

信息可以为相同的信息，也可以为不同的信息，具体可以为系统默认值也可以由用户自行设定，以用于终端与接入点之间的进行网络安全性的验证协商，比如，可以为无线网络的SSID或BSSID中一个部分或变形，也可以为二者的组合。

[69] 如图4所示，所述确定模块308具体包括：判断子模块3082、网络连接子模块3084、提示子模块3086和解密子模块3088。

[70] 其中，判断子模块3082，设置为判断所述响应消息是否与预设信息匹配；网络连接子模块3084，设置为当所述判断子模块3082判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；提示子模块3086，设置为当所述判断子模块3082判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[71] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响应消息时，根据该响应信息是否与预设信息匹配的判断结果确定是否可以使用对应的连接密钥安全地连接至该无线网络接入点，即通过与无线网络接入点之间预先协商好的安全验证方式，在自动连接该无线网络接入点之前先进行安全性验证，则可以确保连接的无线网络为可信任的安全网络，具体地，当无线网络接入点反馈的响应信息与预设信息匹配时，则使用对应的连接密钥自动与该无线网络接入点建立连接，否则可以通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[72] 当然，在该技术方案中，当检测到响应信息与预设信息不匹配时，可以直接拒绝连接到该无线网络接入点，避免任何由于连接到该无线网络接入点可能带来的安全隐患。

[73] 其中，解密子模块3088，设置为通过预设解密密钥对所述响应信息进行解密处理；以及所述判断子模块3082具体设置为：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。

[74] 在该技术方案中，当接收到无线网络接入点对经加密处理的预设认证信息的响

应消息时，首先通过预设解密密钥对该响应信息进行解密处理，进而通过判断经解密处理后的响应信息是否与预设信息匹配，以确定是否使用对应的连接密钥与该无线网络接入点建立连接，即在与无线网络接入点之间进行预设认证信息和响应信息的传输过程中，进行加解密处理，以提高信息传输过程中的安全性，进一步提高网络连接的安全性。

[75] 其中，预设加密密钥和预设解密密钥可以对应的存储在上述预设安全网络列表中进行统一管理，进一步地，预设加密密钥和预设解密密钥为同一密钥，即在该预设安全网络列表中，对应存储任一已安全连接过的无线网络接入点的SSID、BSSID、连接密钥、预设认证信息以及用于对该预设认证信息进行加解密处理的加解密密钥。

[76] 在上述任一技术方案中，优选地，还包括：提示模块310，设置为当所述检测模块306检测在预设时间内未接收所述响应信息时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[77] 在该技术方案中，当向无线网络接入点发送经加密处理的预设认证信息后，若在预设时间内未接收到该无线网络接入点对应的响应信息时，即可通过预设方式向用户发出提示，比如通过文字结合声音和/或光的方式提示用户，进而由用户决定是否使用对应的连接密钥与无线网络接入点建立而使用该无线网络接入点提供的网络服务，以全方位满足用户连接网络的需求。

[78] 当然，在该技术方案中，当未接收到响应信息时，可以直接拒绝连接到该无线网络接入点，避免任何由于连接到该无线网络接入点可能带来的安全隐患。

[79] 图5示出了根据本发明的实施例的终端的示意框图。

[80] 如图5所示，根据本发明的实施例的终端500，包括：如上述技术方案中任一项所述的网络连接装置300，因此，该终端500具有如上述技术方案中任一项所述的网络连接装置300的所有有益效果，在此不再赘述。

[81] 图6示出了根据本发明的实施例的终端和无线网络接入点的交互流程，具体包括以下步骤：

[82] 步骤602，当终端判定当前连接的无线网络接入点为安全接入点时，将该无线网络接入点的SSID、BSSID和连接密钥对应存储在预设安全网络列表，同时针

对该无线网络接入点设置预设认证信息和预设加解密密钥，并将预设认证信息、预设加解密密钥也对应存储在该预设安全网络列表。

[83] 步骤604，当终端开启网络自动连接功能，且扫描到相同的无线网络接入点时，判断该无线网络接入点的SSID是否存储在上述预设安全网络列表中，当判定为是时，执行步骤606。

[84] 步骤606，判断该无线网络接入点的BSSID是否存储在上述预设安全网络列表中，当判定为是时，执行步骤608。

[85] 步骤608，终端通过预设加解密密钥对预设认证信息进行加密，并将加密后的预设认证信息发送至无线网络接入点。

[86] 步骤610，无线网络接入点通过存储的预设加解密密钥对终端发来的经加密处理的预设认证信息进行解密处理，并判断解密后的预设认证信息是否与存储的预设认证信息匹配，若匹配，则执行步骤612。

[87] 步骤612，无线网络接入点通过预设加解密密钥对解密后的预设认证信息进行加密处理，并将加密后的预设认证信息发送至终端。

[88] 步骤614，终端通过存储的预设加解密密钥对无线网络接入点发送的经加密处理的预设认证信息进行解密处理，并判断解密后的预设认证信息是否与存储的预设认证信息匹配，若匹配，则执行步骤616。

[89] 步骤616，终端使用连接密钥与无线网络接入点建立连接。

[90] 在该实施例中终端和无线网络接入点共同维护一套预设认证信息和预设加解密密钥。若具有相同的SSID、连接密钥和BSSID的无线网络接入点无法对终端通过预设加解密密钥进行加密处理的预设认证信息进行解密，则可确定该无线网络接入点为钓鱼网络，终端不与无线网络接入点建立连接。

[91] 图7示出了根据本发明的第二实施例的网络连接方法的流程示意图。

[92] 如图7所示，根据本发明的第二实施例的网络连接方法，具体包括以下流程步骤：

[93] 步骤702，当用户判断当前所连接的AP热点为安全热点后，将此AP信息添加到安全AP热点表（即预设安全网络列表）中，同时，终端对此AP热点生成一个加解密密钥，由终端和AP侧共同维护，即终端侧和AP侧同时保存一个一对一的加

解密密钥，即终端侧和AP侧用于加解密处理的预设加密密钥和预设解密密钥为同一密钥。

- [94] 步骤704，当终端在移动过程中，扫描到了与之前连接的AP热点具有相同SSID和PSK的AP热点时，且终端开启了自动连接功能，在自动连接前增加执行以下步骤。
- [95] 步骤706，判断此AP信息是否在安全AP热点表中，即判断此AP热点的SSID是否在安全热点AP表中，若不在此表中，则默认为危险AP热点，在终端中进行提示由用户决定是否进行自动连接，若存在执行步骤708。
- [96] 步骤708，判断此AP热点的BSSID是否与当前表中的一致，即判断当前AP侧MAC（Media Access Control，媒体访问控制）地址是否与安全热点AP表中所对应的MAC地址保持一致，若不一致，则默认为危险AP热点，在终端中进行提示由用户决定是否进行自动连接，若存在执行步骤710。
- [97] 步骤710，使用对应的加密密钥对认证信息进行加密，并将加密后的信息发送到AP侧。
- [98] 步骤712，判断是否能收到AP侧返回的认证Response（响应），即等待AP侧反馈Response信息，即在AP侧对认证信息使用相同的密钥进行解密，若在固定周期内无反馈信息，在终端中进行提示由用户决定是否进行自动连接，若接收到反馈信息则匹配反馈信息是否与表中信息保持一致，若一致则发送自动连接请求，以进行自动连接。
- [99] 步骤714，根据自动连接请求，根据WIFI连接策略进行连接。
- [100] 在步骤702中，需要AP侧和终端侧共同维护加解密密钥和认证信息，AP侧针对所连接的设备进行维护，保存加解密密钥和认证信息。
- [101] 在步骤702中，AP侧需要使用相同的加解密密钥对认证信息进行解密，并将解密信息发回到终端侧。而钓鱼AP热点由于没有加解密密钥则不会对其进行解密，也不知道发回什么Response，则最终保证AP热点的安全性。
- [102] 综上，该技术方案的目的维护用户确认的安全AP热点表，当碰到相同SSID和密码的AP热点时，通过上述三次判断来确认是否为安全可连接的AP热点。
- [103] 通过上述实施例，利用三个层次的防范来防止用户在开启自动连接AP热点功

能后连接到具有相同SSID和连接密钥的钓鱼AP热点，即当用户连接上某AP热点后，若用户确定此AP热点安全，则将此AP热点的信息添加到安全热点AP表中，同时移动终端与AP侧共同维护一个加解密密钥和认证信息；当用户在开启自动连接功能后，碰到具有相同SSID和密码的AP热点后，在自动连接之前增加认证过程：首先判断是否在安全热点AP表中，若是继续判断当前AP的BSSID与保存在AP列表中的是否保持一致，若是则使用此AP所对应的加解密密钥对认证信息进行加密后发送给AP侧，若能收到AP侧反馈回来的连接Response并且解密出来的认证信息正确（只有具有解密密钥的AP进行解密匹配后才能反馈Response）则进行更进一步的自动连接操作，对不在安全AP热点表的AP热点、BSSID不正确、没有反馈连接Response的热点不进行自动连接操作，如此，可极大提高用户的安全体验，具有有益效果。

- [104] 在进一步的实施例中，结合图3至图5，如图8所示，是本发明实施例提供的终端的结构示意图。所述的终端500包括：至少一个处理器501，例如CPU，至少一个接收器503，至少一个存储器504，至少一个发送器505，至少一个通信总线502。其中，所述通信总线502用于实现这些组件之间的连接通信。其中，所述接收器503和所述发送器505可以是有线发送端口，也可以为无线设备，例如包括天线装置，用于与其他设备进行数据通信。所述存储器504可以是高速RAM存储器，也可以是非暂态存储器（non-transitory memory）。
- [105] 所述处理器501可执行所述终端500的操作系统以及安装的各类应用程序、程序代码等，例如，上述的各个模块，包括所述判断模块302、所述处理模块304等。
- [106] 所述存储器504中存储有程序代码，且所述处理器501可通过通信总线502，调用所述存储器504中存储的程序代码以执行相关的功能。例如，图3、4中所述的各个模块或子模块（例如，所述判断模块302、所述处理模块304等）是存储在所述存储器504中的程序代码，并由所述处理器501所执行，从而实现所述各个模块的功能。
- [107] 在本发明的一个实施例中，所述存储器504存储多个指令，所述多个指令被所述处理器501所执行以实现网络连接方法。具体而言，所述处理器501对所述多

个指令的执行包括：当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；当判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密处理后发送至所述无线网络接入点；检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。

[108] 在进一步的实施例中，所述当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接，具体包括：判断所述响应消息是否与预设信息匹配；当判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；当判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[109] 在进一步的实施例中，在所述判断所述响应消息是否与预设信息匹配之前，所述处理器501通过预设解密密钥对所述响应信息进行解密处理；以及所述判断所述响应消息是否与预设信息匹配，具体包括：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。

[110] 在进一步的实施例中，当检测在预设时间内未接收所述响应信息时，所述处理器501提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

[111] 具体地，所述处理器501对上述指令的具体实现方法可参考图1-2与图6-7对应实施例中相关步骤的描述，在此不赘述。

[112] 以上结合附图详细说明了本发明的技术方案，通过本发明的技术方案，可以有效地提高自动连接无线网络的安全性，避免连接到钓鱼网络，从而确保用户的信息安全，提升用户的使用安全性体验。

[113] 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。

权利要求书

- [权利要求 1] 一种网络连接方法，其特征在于，包括：
- 当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；
- 当判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密处理后发送至所述无线网络接入点；
- 检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；
- 当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。
- [权利要求 2] 根据权利要求1所述的网络连接方法，其特征在于，所述当检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接，具体包括：
- 判断所述响应消息是否与预设信息匹配；
- 当判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；
- 当判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。
- [权利要求 3] 根据权利要求2所述的网络连接方法，其特征在于，在所述判断所述响应消息是否与预设信息匹配之前，包括：
- 通过预设解密密钥对所述响应信息进行解密处理；以及
- 所述判断所述响应消息是否与预设信息匹配，具体包括：
- 判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。
- [权利要求 4] 根据权利要求1至3中任一项所述的网络连接方法，其特征在于，当检测在预设时间内未接收所述响应信息时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

- [权利要求 5] 一种网络连接装置，其特征在于，包括：
- 判断模块，设置为当扫描到无线网络接入点时，判断所述无线网络接入点的SSID、BSSID和连接密钥是否对应存储在预设安全网络列表中；
- 处理模块，设置为当所述判断模块的判断结果为是时，获取并将与所述无线网络接入点对应的预设认证信息通过预设加密密钥加密后发送至所述无线网络接入点；
- 检测模块，设置为检测是否接收到所述无线网络接入点对经加密处理后的所述预设认证信息的响应信息；
- 确定模块，设置为当所述检测模块检测接收到所述响应信息时，根据所述响应信息确定是否使用所述连接密钥与所述无线网络接入点建立连接。
- [权利要求 6] 根据权利要求5所述的网络连接装置，其特征在于，所述确定模块具体包括：
- 判断子模块，设置为判断所述响应消息是否与预设信息匹配；
- 网络连接子模块，设置为当所述判断子模块判定所述响应信息与所述预设信息匹配时，使用所述连接密钥与所述无线网络接入点建立连接；
- 提示子模块，设置为当所述判断子模块判定所述响应信息与所述预设信息不匹配时，提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。
- [权利要求 7] 根据权利要求6所述的网络连接装置，其特征在于，所述确定模块具体还包括：
- 解密子模块，设置为通过预设解密密钥对所述响应信息进行解密处理；以及
- 所述判断子模块具体设置为：判断通过所述预设解密密钥解密处理后的所述响应消息是否与所述预设信息匹配。
- [权利要求 8] 根据权利要求5至7中任一项所述的网络连接装置，其特征在于，

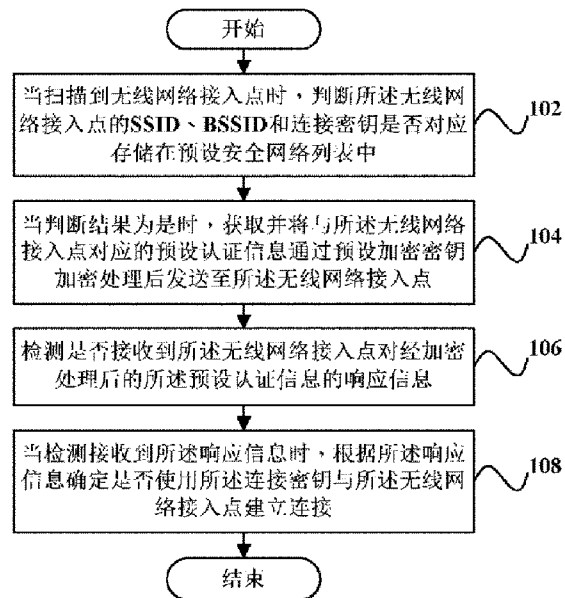
还包括:

提示模块, 设置为当所述检测模块检测在预设时间内未接收所述响应信息时, 提示用户是否使用所述连接密钥与所述无线网络接入点建立连接。

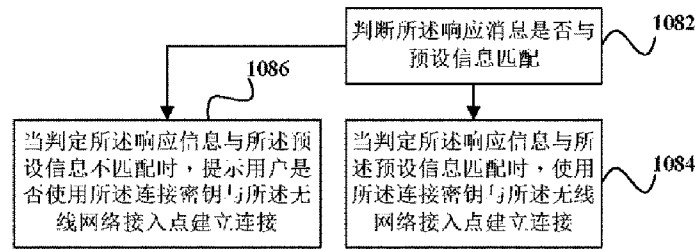
[权利要求 9]

一种终端, 其特征在于, 包括: 如权利要求5至7中任一项所述的网络连接装置。

[Fig. 1]



[Fig. 2]



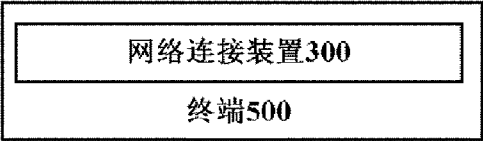
[Fig. 3]



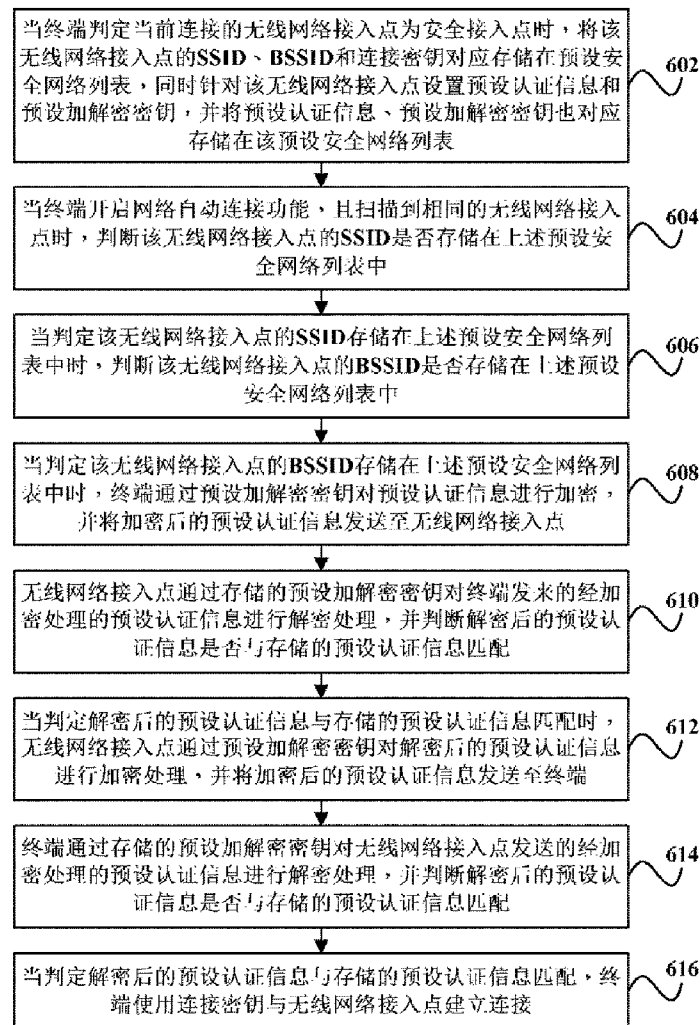
[Fig. 4]



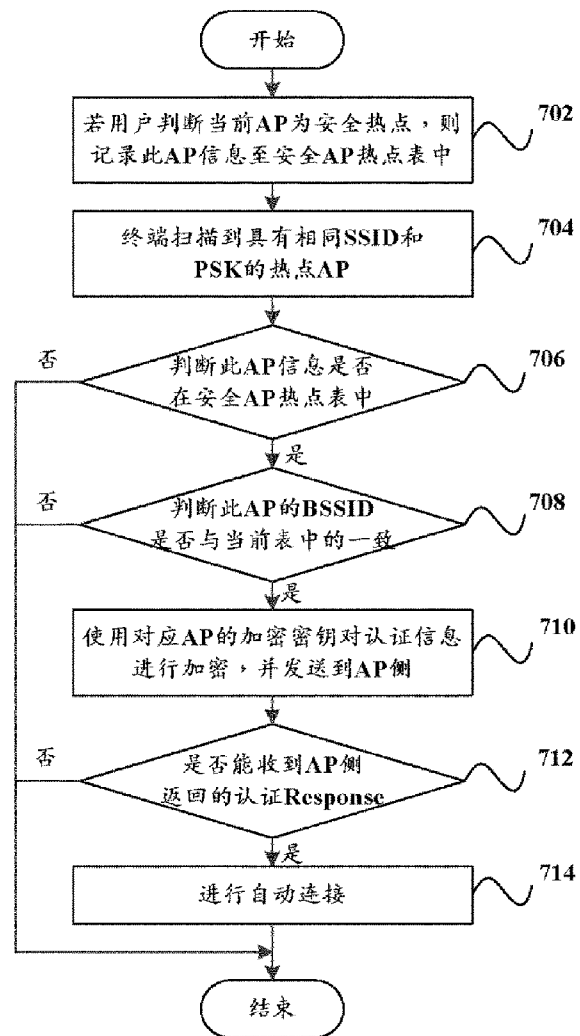
[Fig. 5]



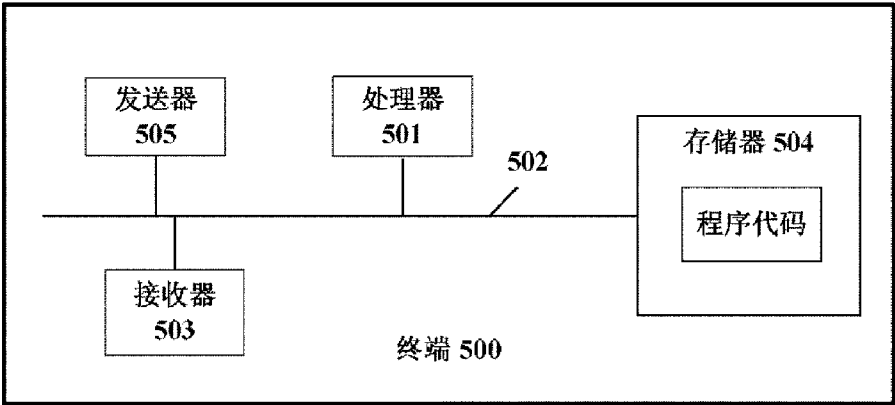
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/103876

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; H04W 12/08 (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

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; VEN; CNKI; USTXT: illegal, pseudo base station, authentication information, basic service set, encrypt, counterfeit, falsity, pseudo access point, wlan, fraud+, fishing, hotspot, wifi, phishing, phing, access point, key, AP, SSID, BSSID, authenticat+, response, security, list, preset, encrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103648094 A (HUAWEI TECHNOLOGIES CO., LTD.), 19 March 2014 (19.03.2014), description, paragraphs [0129]-[0146], and figure 8	1-9
Y	CN 105636037 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 01 June 2016 (01.06.2016), description, paragraphs [0109]-[0142]	1-9
A	CN 104394533 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 04 March 2015 (04.03.2015), the whole document	1-9
A	CN 105163316 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 16 December 2015 (16.12.2015), the whole document	1-9
A	CN 104023336 A (ZHANG, Lijun), 03 September 2014 (03.09.2014), the whole document	1-9

☐ 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 24 March 2017 (24.03.2017)	Date of mailing of the international search report 06 April 2017 (06.04.2017)
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 FU, Haiwang Telephone No.: (86-10) 62411393

International application No.
PCT/CN2016/103876

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

国际检索报告

国际申请号

PCT/CN2016/103876

A. 主题的分类

H04W 12/06(2009.01)i; H04W 12/08(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

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;VEN;CNKI;USTXT:非法, 接入点, 伪基站, 钓鱼, 认证信息, 欺诈, 欺骗, 密钥, 基本服务集, 加密, 响应, 名单, 假冒, 虚假, 列表, 伪造, 预设, 伪接入点, 热点, wlan, fraud+, fishing, hotspot, wifi, phishing, phing, access point, key, AP, SSID, BSSID, authenticat+, response, security, list, preset, encrypt+

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
Y	CN 103648094 A (华为技术有限公司) 2014年 3月 19日 (2014 - 03 - 19) 说明书第[0129]-[0146]段, 图8	1-9
Y	CN 105636037 A (宇龙计算机通信科技深圳有限公司) 2016年 6月 1日 (2016 - 06 - 01) 说明书第[0109]-[0142]段	1-9
A	CN 104394533 A (中国联合网络通信集团有限公司) 2015年 3月 4日 (2015 - 03 - 04) 全文	1-9
A	CN 105163316 A (腾讯科技深圳有限公司) 2015年 12月 16日 (2015 - 12 - 16) 全文	1-9
A	CN 104023336 A (张力军) 2014年 9月 3日 (2014 - 09 - 03) 全文	1-9

☐ 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 3月 24日

国际检索报告邮寄日期

2017年 4月 6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

傅海望

电话号码 (86-10)62411393

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/103876

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	103648094	A	2014年 3月 19日	WO	2015074367	A1	2015年 5月 28日
CN	105636037	A	2016年 6月 1日	无			
CN	104394533	A	2015年 3月 4日	无			
CN	105163316	A	2015年 12月 16日	无			
CN	104023336	A	2014年 9月 3日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)