(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114615688 B
(45)授权公告日 2022.09.30

(21)申请号 202210327071.7
(22)申请日 2022.03.30
(65)同一申请的已公布的文献号
申请公布号 CN 114615688 A
(43)申请公布日 2022.06.10
(73)专利权人 广州芯德通信科技股份有限公司
地址 510663 广东省广州市黄埔区科学大道162号创意大厦B2栋601室
(72)发明人 何锋 饶东盛 江泽欢
(74)专利代理机构 广州粤高专利商标代理有限公司 44102
专利代理师 禹小明
(51)Int.Cl.
H04W 24/02(2009.01)
H04W 12/06(2021.01)
H04W 52/02(2009.01)

(56)对比文件
WO 2014134544 A1,2014.09.04
AU 2011204969 A1,2012.03.15
US 10212163 B1,2019.02.19
CN 110740460 A,2020.01.31
CN 108924827 A,2018.11.30
CN 110830336 A,2020.02.21
CN 113613211 A,2021.11.05
CN 101599850 A,2009.12.09

审查员 王湘

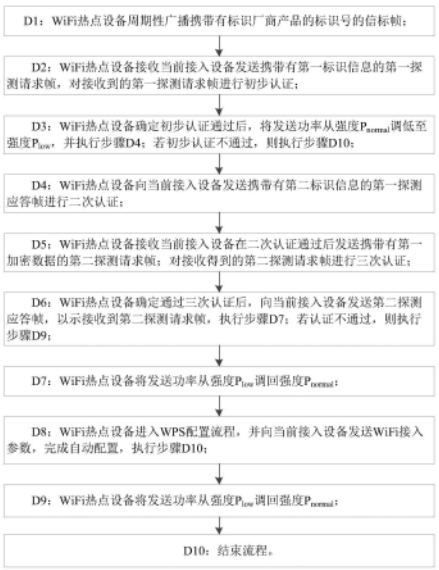
权利要求书3页 说明书12页 附图3页

(54)发明名称

一种WiFi热点设备与当前接入设备之间近距离自动配置方法

(57)摘要

本发明公开了一种WiFi热点设备与当前接入设备之间近距离自动配置方法,如下:周期性广播信标帧;接收当前接入设备发送携带有第一标识信息的第一探测请求帧,对第一探测请求帧进行初步认证;确定初步认证通过后,将发送功率从强度P_{normal}调低至强度P_{low};向当前接入设备发送携带有第二标识信息的第一探测应答帧进行二次认证;接收当前接入设备在二次认证通过后发送携带有第一加密数据的第二探测请求帧;对第二探测请求帧进行三次认证;确定通过三次认证后,向当前接入设备发送第二探测应答帧;将发送功率从强度P_{low}调回强度P_{normal};进入WPS配置流程,并向当前接入设备发送WiFi接入参数,完成自动配置;结束流程。



CN 114615688 B

1.一种WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:所述的方法包括步骤如下:

D1:WiFi热点设备周期性广播携带有标识厂商产品的标识号的信标帧;

D2:WiFi热点设备接收当前接入设备在触发自动配置流程后发送携带有第一标识信息的第一探测请求帧,对接收到的第一探测请求帧进行初步认证;

D3:WiFi热点设备确定初步认证通过后,将发送功率从强度P_{normal}调低至强度P_{low},并执行步骤D4;若初步认证不通过,则执行步骤D10;

D4:WiFi热点设备以发送功率为P_{low}向当前接入设备发送携带有第二标识信息的第一探测应答帧进行二次认证;

D5:WiFi热点设备接收当前接入设备在二次认证通过后发送携带有第一加密数据的第二探测请求帧;对接收得到的第二探测请求帧进行三次认证;

D6:WiFi热点设备确定通过三次认证后,以发送功率为P_{low}向当前接入设备发送第二探测应答帧,以示接收到第二探测请求帧,执行步骤D7;若认证不通过,则执行步骤D9;

D7:WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal};

D8:WiFi热点设备进入WiFi安全保护设置WPS配置流程,并向当前接入设备发送WiFi接入参数,完成自动配置,执行步骤D10;

D9:WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal};

D10:结束流程。

2.根据权利要求1所述的WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:

所述的第一标识信息包括明文、当前接入设备生成的第一随机数、第一数据摘要;其中所述的第一数据摘要根据明文、第一随机数、预置在当前接入设备上的第一认证密码通过数据摘要算法运算得到。

3.根据权利要求2所述的WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:

所述的初步认证具体如下:

通过对明文、第一随机数、预置在WiFi热点设备上的第二认证密码进行数据摘要算法运算得到第二数据摘要;

判断第二数据摘要是否等于第一数据摘要;

确认第二数据摘要等于第一数据摘要,则表明预置在WiFi热点设备上的第二认证密码与当前接入设备预置的第一认证密码相同,初步认证通过;

确认第二数据摘要不等于第一数据摘要,初步认证不通过。

4.根据权利要求3所述的WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:

所述的第二标识信息包括明文、WiFi热点设备生成的第二随机数、第三数据摘要;

所述的第三数据摘要根据明文、第一随机数、第二随机数、预置在WiFi热点设备上的第二认证密码通过数据摘要算法运算得到。

5.根据权利要求4所述的WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:所述的当前接入设备对携带有第二标识信息的第一探测应答帧进行二次认证,

具体如下：

所述的二次认证，具体如下：

将第一随机数、第二随机数串接后与明文、第一认证密码通过数据摘要算法运算得到第四数据摘要；

判断第四数据摘要是否等于第三数据摘要，确认第四数据摘要等于第三数据摘要，则表明WiFi热点设备预置的第二认证密码与当前接入设备预置的第一认证密码相同，此时确定WiFi热点设备是可信任的。

6.根据权利要求5所述的WiFi热点设备与当前接入设备之间近距离自动配置方法，其特征在于：所述的第一加密数据包括密文、第五数据摘要；

其中所述的密文以第一随机数、第二随机数、第一认证密码串接作为密钥，运用对称加密算法对待传输数据进行加密得到；

所述的第五数据摘要运用数据摘要算法对密文、第一随机数、第二随机数、第一认证密码运算得到。

7.根据权利要求6所述的WiFi热点设备与当前接入设备之间近距离自动配置方法，其特征在于：所述的三次认证具体如下：

先对密文、第一随机数、第二随机数、第二认证密码进行数据摘要运算，得到第一校验码；

再判断第一校验码是否等于第五数据摘要；

确认第一校验码等于第五数据摘要，对密文进行解密操作得到待传输数据；

确认待传输数据为合法指令，则向当前接入设备发送第二探测应答帧；并进入WPS配置流程；

确认第一校验码不等于第五数据摘要，则表明存在异常，则认证不通过，并将发送功率从强度P_{low}调回强度P_{normal}。

8.一种WiFi热点设备与当前接入设备之间近距离自动配置方法，其特征在于：所述的方法与如权利要求1～7任一项所述的方法相互配合，实现WiFi近距离自动配置；所述的方法包括步骤如下：

S1：当前接入设备接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧；

S2：当前接入设备根据信标帧判断是否触发自动配置流程，在确定触发自动配置流程后，向WiFi热点设备发送携带有第一标识信息的第一探测请求帧进行初步认证，并执行步骤S3；若不触发自动配置流程，则返回步骤S1；

S3：当前接入设备接收WiFi热点设备在初步认证通过后以发送功率为P_{low}发送携带有第二标识信息的第一探测应答帧；

S4：当前接入设备根据接收到的第一探测应答帧，结合携带有第一标识信息的第一探测请求帧进行二次认证；

S5：当前接入设备在确定通过二次认证后，向WiFi热点设备发送携带有第一加密数据的第二探测请求帧进行三次认证，并执行步骤S6；若二次认证不通过，则返回步骤S1；

S6：当前接入设备接收WiFi热点设备在三次认证通过后以发送功率为P_{low}发送用于表示WiFi热点设备接收到第二探测请求帧的第二探测应答帧；

S7：当前接入设备在接收到第二探测应答帧后进入WPS配置流程，接收WiFi热点设备发

送的WiFi接入参数,完成自动配置;

S8:结束流程。

9.根据权利要求8所述的WiFi热点设备与当前接入设备之间近距离自动配置方法,其特征在于:判断是否触发自动配置流程需要满足以下两个条件:

条件1:接收到带正确标识号的信标帧,而且信号强度大于阈值A;

条件2:当前接入设备的WiFi配置为空,或使用当前WiFi配置无法正常接入WiFi热点设备。

10.一种电子设备,其特征在于,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行如权利要求1-7中任一项所述的WiFi热点设备与当前接入设备之间近距离自动配置方法或如权利要求8-9中任一项所述的WiFi热点设备与当前接入设备之间近距离自动配置方法。

一种WiFi热点设备与当前接入设备之间近距离自动配置方法

技术领域

[0001] 本发明涉及无线局域网技术领域，更具体的，涉及一种WiFi热点设备与当前接入设备之间近距离自动配置方法。

背景技术

[0002] 在WiFi设备使用中，普通用户最头疼的问题就是参数设置问题，参数含义过于技术性、操作步骤繁琐，用户使用体验不好。随着WiFi技术广泛应用，其易用性受到大家的关注。不少WiFi模块厂家提出了smartConfig的概念，利用手机等智能终端在WiFi环境下发送广播/组播包，通过包长度或MAC地址携带信息，以串行的方式向WiFi设备发送SSID/PASSWORD等关键配置参数，从而实现WiFi设备参数快速配置，大大降低WiFi设备使用的复杂度。这种方法需要智能终端先连接上WiFi热点，然后通过WiFi设备上的按键将其设置于配置模式，每一个广播/组播包携带一个字节的数据，配置时间长，可靠性低。

[0003] WiFi联盟也在WiFi简便配置上做了不少工作。其提出的easyConnect技术，通过使用二维码、NFC、蓝牙等手段初始化WiFi配置流程。WPS(WiFi安全保护设置)技术帮助用户在不了解WiFi细节的情况下，建立安全可靠的链接。这种方法增加设备成本，需添加NFC或蓝牙功能。另一种方式是通过按钮触发配置流程，增加设备机械结构的复杂性。

[0004] 公开号CN105898892A的文献《利用wifi probe请求以及响应包实现快速通信的方法》描述了基于wifi管理帧probe request和probe response帧在未建立WiFi连接的情况下进行数据通信的方法。但是这个方法缺少安全方面的考虑，通信数据容易被窃取、篡改。

发明内容

[0005] 本发明为了解决以上现有技术存在的不足与缺陷的问题，提供了一种WiFi热点设备与当前接入设备之间近距离自动配置方法，其具有配置过程速度快、可靠性高的优点。

[0006] 为实现上述本发明目的，采用的技术方案如下：

[0007] 一种WiFi热点设备与当前接入设备之间近距离自动配置方法，所述的方法包括步骤如下：

[0008] D1:WiFi热点设备周期性广播携带有标识厂商产品的标识号的信标帧；

[0009] D2:WiFi热点设备接收当前接入设备在触发自动配置流程后发送携带有第一标识信息的第一探测请求帧，对接收到的第一探测请求帧进行初步认证；

[0010] D3:WiFi热点设备确定初步认证通过后，将发送功率从强度P_{normal}调低至强度P_{low}，并执行步骤D4；若初步认证不通过，则执行步骤D10；

[0011] D4:WiFi热点设备以发送功率为P_{low}向当前接入设备发送携带有第二标识信息的第一探测应答帧进行二次认证；

[0012] D5:WiFi热点设备接收当前接入设备在二次认证通过后发送携带有第一加密数据的第二探测请求帧；对接收得到的第二探测请求帧进行三次认证；

[0013] D6:WiFi热点设备确定通过三次认证后，以发送功率为P_{low}向当前接入设备发送第

二探测应答帧，以示接收到第二探测请求帧，执行步骤D7；若认证不通过，则执行步骤D9；

[0014] D7：WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal}；

[0015] D8：WiFi热点设备进入WPS配置流程，并向当前接入设备发送WiFi接入参数，完成自动配置，执行步骤D10；

[0016] D9：WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal}；

[0017] D10：结束流程。

[0018] 优选地，所述的第一标识信息包括明文、自身生成的第一随机数、第一数据摘要；其中所述的第一数据摘要根据明文、第一随机数、预置的第一认证密码通过数据摘要算法运算得到。

[0019] 进一步地，所述的初步认证具体如下：

[0020] 通过对明文、第一随机数、预置的第二认证密码进行数据摘要算法运算得到第二数据摘要；

[0021] 判断第二数据摘要是否等于第一数据摘要；

[0022] 确认第二数据摘要等于第一数据摘要，则表明预置的第二认证密码与当前接入设备预置的第一认证密码相同，初步认证通过；

[0023] 确认第二数据摘要不等于第一数据摘要，初步认证不通过。

[0024] 再进一步地，所述的第二标识信息包括明文、WiFi热点设备生成的第二随机数、第三数据摘要；

[0025] 所述的第三数据摘要根据明文、第一随机数、第二随机数、预置在WiFi热点设备上的第二认证密码通过数据摘要算法运算得到。

[0026] 再进一步地，所述的当前接入设备对携带有第二标识信息的第一探测应答帧进行二次认证，具体如下：

[0027] 所述的二次认证，具体如下：

[0028] 将第一随机数、第二随机数串接后与明文、第一认证密码通过数据摘要算法运算得到第四数据摘要；

[0029] 判断第四数据摘要是否等于第三数据摘要，确认第四数据摘要等于第三数据摘要，则表明WiFi热点设备预置的第二认证密码与当前接入设备预置的第一认证密码相同，此时确定WiFi热点设备是可信任的。

[0030] 再进一步地，所述的第一加密数据包括密文、第五数据摘要；

[0031] 其中所述的密文以第一随机数、第二随机数、第一认证密码串接作为密钥，运用对称加密算法对待传输数据进行加密得到；

[0032] 所述的第五数据摘要运用数据摘要算法对密文、第一随机数、第二随机数、第一认证密码运算得到。

[0033] 再进一步地，所述的三次认证步骤具体如下：

[0034] 先对密文、第一随机数、第二随机数、第二认证密码进行数据摘要运算，得到第一校验码；

[0035] 再判断第一校验码是否等于第五数据摘要；

[0036] 确认第一校验码等于第五数据摘要，对密文进行解密操作得到待传输数据；

[0037] 确认待传输数据为合法指令，则向当前接入设备发送第二探测应答帧；并进入WPS

配置流程。

[0038] 确认第一校验码不等于第五数据摘要，则表明存在异常，则认证不通过，并将发送功率从强度P_{low}调回强度P_{normal}。

[0039] 一种WiFi热点设备与当前接入设备之间近距离自动配置方法，所述的方法与如上述的方法相互配合，实现WiFi近距离自动配置；所述的方法包括步骤如下：

[0040] S1：当前接入设备接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧；

[0041] S2：当前接入设备根据信标帧判断是否触发自动配置流程，在确定触发自动配置流程后，向WiFi热点设备发送携带有第一标识信息的第一探测请求帧进行初步认证，并执行步骤S3；若不触发自动配置流程，则返回步骤S1；

[0042] S3：当前接入设备接收WiFi热点设备在初步认证通过后以发送功率为P_{low}发送携带有第二标识信息的第一探测应答帧；

[0043] S4：当前接入设备根据接收到的第一探测应答帧，结合携带有第一标识信息的第一探测请求帧进行二次认证；

[0044] S5：当前接入设备在确定通过二次认证后，向WiFi热点设备发送携带有第一加密数据的第二探测请求帧进行三次认证，并执行步骤S6；若二次认证不通过，则返回步骤S1；

[0045] S6：当前接入设备接收WiFi热点设备在三次认证通过后以发送功率为P_{low}发送用于表示WiFi热点设备接收到第二第探测请求帧的第二探测应答帧；

[0046] S7：当前接入设备在接收到第二探测应答帧后进入WPS配置流程，接收WiFi热点设备发送的WiFi接入参数，完成自动配置；

[0047] S8：结束流程。

[0048] 优选地，判断是否触发自动配置流程需要满足以下两个条件：

[0049] 条件1：接收到带正确标识号的信标帧，而且信号强度大于阀值A；

[0050] 条件2：当前接入设备的WiFi配置为空，或使用当前WiFi配置无法正常接入WiFi热点设备。

[0051] 一种电子设备，包括：

[0052] 至少一个处理器；以及，

[0053] 与所述至少一个处理器通信连接的存储器；其中，

[0054] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行如所述的WiFi热点设备与当前接入设备之间近距离自动配置方法。

[0055] 本发明的有益效果如下：

[0056] 本发明提供一种简单、快速、安全的WiFi热点设备与当前接入设备之间近距离自动配置方法。比较现有技术smartConfig方法，本发明喊少了按钮操作，配置过程速度更快、可靠性更高。比较普通WPS方式，减少按钮或网页操作，有利于提高用户使用体验和优化产品外观。比较以往基于WiFi管理帧传输数据的方法，本发明具有认证、加密能力，数据通信安全性高。通过当前接入设备与WiFi热点设备的近距离无线交互过程，替代传统的WPS按钮功能，在不降低安全性的前提下简化操作步骤。

[0057] 本发明通过将当前接入设备放置在WiFi热点设备附近，提高信标帧接收强度，从

而触发当前接入设备启动与WiFi热点设备的自动配置流程。

[0058] 本发明通过降低发送功率的强度,避免安全范围以外的设备接收到流程中的WiFi报文,有效的提高自动配置流程的安全性。

[0059] 本发明通过三次认证,实现双方身份合法性认证,进一步的提高自动配置流程的安全性。

[0060] 本发明第二探测请求帧携带有第一加密数据,再进一步提高数据传输的安全性。

附图说明

[0061] 图1是实施例1所述的WiFi热点设备与当前接入设备之间近距离自动配置方法的流程图。

[0062] 图2是实施例2所述的WiFi热点设备与当前接入设备之间近距离自动配置方法的流程图。

[0063] 图3是实施例3WiFi热点设备、当前接入设备实现WiFi近距离自动配置方法的系统框图。

[0064] 图4是实施例3WiFi热点设备、当前接入设备实现WiFi近距离自动配置方法的流程图。

具体实施方式

[0065] 下面结合附图和具体实施方式对本发明做详细描述。

[0066] Wi-Fi是一种允许电子设备连接到一个无线局域网(WLAN)的技术,通常使用2.4G UHF或5G SHF ISM射频频段。连接到无线局域网通常是有密码保护的;但也可是开放的,这样就允许任何在WLAN范围内的设备可以连接上。

[0067] 实施例1

[0068] 本实施例简化了当前接入设备的配置步骤,使用户在新的WiFi环境下通过直观的操作,将可移动的当前接入设备(如手机、笔记本等),靠近要接入的WiFi热点设备(通常是放置在桌面的无线路由器产品),即可自动完成WiFi接入参数的配置,获得上网权限。本实施例从WiFi热点设备端触发详细介绍,具体如下:

[0069] 如图1所示,本实施例提供的一种WiFi热点设备与当前接入设备之间近距离自动配置方法,所述的方法包括步骤如下:

[0070] D1:WiFi热点设备周期性(如100毫秒)广播携带有标识厂商产品的标识号的信标帧;在本实施例中,在信标帧(beacon帧)中加入厂商自定义的信息单元(IE),此信息单元中包括一个标识厂商产品的标识号MID。

[0071] D2:WiFi热点设备接收当前接入设备在触发自动配置流程后发送携带有第一标识信息的第一探测请求帧,对接收到的第一探测请求帧进行初步认证;

[0072] D3:WiFi热点设备确定初步认证通过后,将发送功率从强度P_{normal}调低至强度P_{low},并执行步骤D4;若初步认证不通过,则执行步骤D10;

[0073] D4:WiFi热点设备以发送功率为P_{low}向当前接入设备发送携带有第二标识信息的第一探测应答帧进行二次认证;

[0074] D5:WiFi热点设备接收当前接入设备在二次认证通过后发送携带有第一加密数据

的第二探测请求帧;对接收得到的第二探测请求帧进行三次认证;

[0075] D6:WiFi热点设备确定通过三次认证后,以发送功率为P_{low}向当前接入设备发送第二探测应答帧,以示接收到第二探测请求帧,执行步骤D7;若认证不通过,则执行步骤D9;

[0076] D7:WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal};

[0077] D8:WiFi热点设备进入WPS配置流程,并向当前接入设备发送WiFi接入参数,完成自动配置,执行步骤D10;

[0078] D9:WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal};

[0079] D10:结束流程。

[0080] 本实施例在当前接入设备在触发自动配置流程,对当前接入设备进行初步认证,初步判断当前接入设备是否为可靠的设备,在初步认证通过之后将发送功率从强度P_{normal}调低至强度P_{low},其目的是避免其他人恶意接入,有利于提高安全配置。

[0081] 在本实施例中,所述的第一标识信息包括明文、当前接入设备生成的第一随机数、第一数据摘要;其中所述的第一数据摘要根据明文、第一随机数、预置在当前接入设备上的第一认证密码通过数据摘要算法运算得到,具体公式表示如下:

[0082] ADS1=AF(PT,Nonce1,AuthPwd1)

[0083] 式中,ADS1表示第一数据摘要;PT表示明文;Nonce1表示自身生成的第一随机数;AuthPwd1表示预置在本设备上的第一认证密码;AF表示数据摘要算法。本实施例中所述的数据摘要算法AF可根据需要选择当前标准的算法或自定义算法。本实施例通过第一探测请求帧中厂商自定义信息单元(IE)携带Nonce1、PT和ADS1信息。

[0084] 在一个具体的实施例中,所述的初步认证具体如下:

[0085] 通过对明文、第一随机数、预置的第二认证密码进行数据摘要算法运算得到第二数据摘要,具体如下:

[0086] ADS2=AF(PT,Nonce1,AuthPwd2)

[0087] 式中,ADS2表示第二数据摘要;AuthPwd2表示预置在WiFi热点设备上的第二认证密码。

[0088] 判断第二数据摘要是否等于第一数据摘要;

[0089] 确认第二数据摘要等于第一数据摘要,则表明预置的第二认证密码与当前接入设备预置的第一认证密码相同,初步认证通过;WiFi热点设备将当前WiFi热点的发送功率从强度P_{normal}调低至强度P_{low}。

[0090] 确认第二数据摘要不等于第一数据摘要,初步认证不通过,结束当前流程,可以返回继续广播携带有标识厂商产品的标识号的信标帧。

[0091] 该步骤由WiFi热点设备完成对请求接入的当前接入设备进行判断,判断当前接入设备是否可信。如可信,则将发送功率从强度P_{normal}调低至强度P_{low},避免安全范围以外的设备接收到流程中的WiFi报文(通信数据),有效的提高自动配置流程的安全性。原因是:在现实生活中一般能进入你的住所,并将当前接入设备靠近你的无线路由器的人,都是你可以信任的人,他们应该获得上网权限。对于其他你所不信任的人员,因为无法进入你的住所,只能通过远距离无线接入,又由于墙壁等障碍物的阻隔,WiFi信号大大衰减,以P_{low}功率发送的第一探测应答帧只有近距离接入设备可以正常接收。远距离恶意接入设备因为无法获得第二标识信息,所以无法构造正确的第二探测请求帧,恶意接入被迫中止。

[0092] 本实施例中，在确认当前接入设备可信后，WiFi热点设备向当前接入设备发送携带有第二标识信息的第一探测应答帧，供当前接入设备进行二次认证；所述的第二标识信息包括明文、自身生成的第二随机数、第三数据摘要；

[0093] 所述的第三数据摘要根据明文、第一随机数、第二随机数、预置的第二认证密码通过数据摘要算法运算得到，具体公式如下：

[0094] ADS3＝AF(PT,Nonce1|Nonce2,AuthPwd2)

[0095] 式中，ADS3表示第三数据摘要，PT表示明文，Nonce1|Nonce2表示将第一随机数、第二随机数串接；AuthPwd2表示预置的第二认证密码；Nonce2表示第二认证密码。

[0096] 在一个具体的实施例中，所述的二次认证用于判断WiFi热点设备是否可信，所述的当前接入设备对携带有第二标识信息的第一探测应答帧进行二次认证，具体如下：

[0097] 将第一随机数、第二随机数串接后与明文、第一认证密码通过数据摘要算法运算得到第四数据摘要，具体公式如下：

[0098] ADS4＝AF(PT,Nonce1|Nonce2,AuthPwd1)

[0099] 式中，ADS4表示第四数据摘要。

[0100] 判断第四数据摘要是否等于第三数据摘要，确认第四数据摘要等于第三数据摘要，则表明WiFi热点设备预置的第二认证密码与当前接入设备预置的第一认证密码相同，此时确定WiFi热点设备是可信任的。

[0101] 在本实施例中，若确认第四数据摘要不等于第三数据摘要，则表示WiFi热点设备是不可信任的，结束当前流程，返回步骤S1继续接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧。

[0102] 本实施例中，在当前接入设备对WiFi热点设备二次认证通过后，WiFi热点设备接收当前接入设备发送携带有第一加密数据的第二探测请求帧；所述的第一加密数据包括密文、第五数据摘要；

[0103] 其中所述的密文以第一随机数、第二随机数、第一认证密码串接作为密钥，运用对称加密算法对待传输数据进行加密得到，具体公式如下：

[0104] EDT＝SFencrypt(PDT,Nonce1|Nonce2|AuthPwd1)

[0105] 式中，EDT表示密文；Nonce1|Nonce2|AuthPwd1表示以Nonce1|Nonce2|AuthPwd1作为密钥；PDT表示待传输数据；SFencrypt表示对称加密算法。

[0106] 所述的第五数据摘要运用数据摘要算法对密文、第一随机数、第二随机数、第一认证密码运算得到，具体公式如下：

[0107] DS＝AF(EDT,Nonce1|Nonce2,AuthPwd1)

[0108] 式中，DS表示第五数据摘要。

[0109] 在本实施例中，通过对待传输数据进行加密，提高数据传输的安全性。

[0110] 在一个具体的实施例中，所述的三次认证步骤具体如下：

[0111] 先对密文、第一随机数、第二随机数、第二认证密码进行数据摘要运算，得到第一校验码，具体公式如下：

[0112] VS＝AF(EDT,Nonce1|Nonce2,AuthPwd2)

[0113] 式中，VS表示第一校验码；

[0114] 再判断第一校验码是否等于第五数据摘要；

[0115] 确认第一校验码等于第五数据摘要，对密文进行解密操作得到待传输数据，具体公式如下：

[0116] PDT＝SFdecrypt(EDT,Nonce1|Nonce2|AuthPwd2)

[0117] 并判断待传输数据是否为合法指令，确定待传输数据为合法指令，则向当前接入设备发送第二探测应答帧，并进入WPS配置流程。确定待传输数据为不合法指令，结束当前流程，继续广播携带有标识厂商产品的标识号的信标帧。

[0118] 确认第一校验码不等于第五数据摘要，则表明存在异常，则认证不通过，并将发送功率从强度P_{low}调回强度P_{normal}，并结束当前流程。

[0119] 本实施例所述的当前接入设备包括但不限于手机、笔记本、ipad等移动智能终端，也可以是其他带有WiFi功能的智能终端，如车载显示系统，或路由器。

[0120] 实施例2

[0121] 本实施例主要以当前接入设备执行WiFi热点设备与当前接入设备之间近距离自动配置方法进行自动配置为例详细说明，本实施例所述的方法与实施例1所述的方法相互配合，实现WiFi近距离自动配置。

[0122] 如图2所示，本实施例提供的一种当前接入设备与WiFi热点设备之间近距离自动配置方法，所述的方法包括步骤如下：

[0123] S1：当前接入设备接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧；

[0124] S2：当前接入设备根据信标帧判断是否触发自动配置流程，在确定触发自动配置流程后，向WiFi热点设备发送携带有第一标识信息的第一探测请求帧进行初步认证，并执行步骤S3；若不触发自动配置流程，则返回步骤S1；

[0125] S3：当前接入设备接收WiFi热点设备在初步认证通过后发送携带有第二标识信息的第一探测应答帧；

[0126] S4：当前接入设备根据接收到的第一探测应答帧，结合携带有第一标识信息的第一探测请求帧进行二次认证；

[0127] S5：当前接入设备在确定通过二次认证后，向WiFi热点设备发送携带有第一加密数据的第二探测请求帧进行三次认证，并执行步骤S6；若二次认证不通过，则返回步骤S1；

[0128] S6：当前接入设备接收WiFi热点设备在三次认证通过后发送用于表示WiFi热点设备接收到第二第探测请求帧的第二探测应答帧；

[0129] S7：当前接入设备在接收到第二探测应答帧后进入WPS配置流程，接收WiFi热点设备发送的WiFi接入参数，完成自动配置；

[0130] S8：结束流程。

[0131] 在本实施例中，在信标帧(beacon帧)中加入厂商自定义的信息单元(IE)，此信息单元中包括一个标识厂商产品的标识号MID。此标识号MID主要用途是使当前接入设备获知WiFi热点设备是否支持本实施例所述的WiFi近距离自动配置方法的流程。

[0132] 在一个具体的实施例中，判断是否触发自动配置流程需要满足以下两个条件：

[0133] 条件1：接收到带正确标识号的信标帧，而且信号强度大于阀值A；

[0134] 条件2：当前接入设备的WiFi配置为空，或使用当前WiFi配置无法正常接入WiFi热点设备。

[0135] 本实施例通过接收到的信标帧判断是否触发自动配置流程，有效的提高自动配置的效率，在确定不会触发自动配置流程后，当前接入设备可以结束当前流程，返回步骤S1继续接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧。具体地：当当前接入设备接收到带正确标识号的信标帧，但信号强度小于阀值A，此时说明当前接入设备距离WiFi热点设备距离比较远，认为WiFi热点设备不可信，不具有安全性；若此时当前接入设备的WiFi配置为空，则返回步骤S1；若当前接入设备已完成WiFi配置，则停止WiFi自动配置流程。

[0136] 在本实施例中，通过信号强度大于阀值A判断WiFi热点设备可信，阀值A的大小表示当前接入设备与WiFi热点设备之间的距离远近，通过设置阈值A间接限定当前接入设备与WiFi热点设备之间的距离，如设置阈值A在较近距离(如1米内)才触发自动配置流程，避免一些无意中的触发情况。

[0137] 本实施例通过将当前接入设备放置在WiFi热点设备一定的范围内，提高信标帧接收强度，从而触发当前接入设备启动与WiFi热点设备的自动配置流程。避免一些无意中的触发情况，也有利于保证当前接入设备的可靠性。

[0138] 本实施例可以先通过判断是否满足条件1，再判断是否满足条件2；也可以先判断是否满足条件2，再判断是否满足条件1；对于触发条件没有先后顺序的限定。

[0139] 在一个具体的实施例中，所述的第一标识信息包括明文、自身生成的第一随机数、第一数据摘要；其中所述的第一数据摘要根据明文、第一随机数、预置的第一认证密码通过数据摘要算法运算得到，具体公式表示如下：

[0140] ADS1＝AF(PT,Nonce1,AuthPwd1)

[0141] 式中，ADS1表示第一数据摘要；PT表示明文；Nonce1表示自身生成的第一随机数；AuthPwd1表示预置在本设备上的第一认证密码；AF表示数据摘要算法。本实施例中所述的数据摘要算法AF可根据需要选择当前标准的算法或自定义算法。本实施例通过第一探测请求帧中厂商自定义信息单元(IE)携带Nonce1、PT和ADS1信息。

[0142] 在一个具体的实施例中，所述的第二标识信息包括明文、WiFi热点设备生成的第二随机数、第三数据摘要；

[0143] 所述的第三数据摘要根据明文、第一随机数、第二随机数、预置在WiFi热点设备上的第二认证密码通过数据摘要算法运算得到，具体公式如下：

[0144] ADS3＝AF(PT,Nonce1|Nonce2,AuthPwd2)

[0145] 式中，ADS3表示第三数据摘要，PT表示明文，Nonce1|Nonce2表示将第一随机数、第二随机数串接；AuthPwd2表示预置的第二认证密码；Nonce2表示第二认证密码。

[0146] 在本实施例中，所述的第一探测应答帧中厂商自定义信息单元携带Nonce2、PT和ADS3信息。

[0147] 在一个具体的实施例中，所述的二次认证用于判断WiFi热点设备是否可信，具体如下：

[0148] 将第一随机数、第二随机数串接后与明文、第一认证密码通过数据摘要算法运算得到第四数据摘要，具体公式如下：

[0149] ADS4＝AF(PT,Nonce1|Nonce2,AuthPwd1)

[0150] 式中，ADS4表示第四数据摘要。

[0151] 判断第四数据摘要是否等于第三数据摘要，确认第四数据摘要等于第三数据摘要，则表明WiFi热点设备预置的第二认证密码与当前接入设备预置的第一认证密码相同，此时确定WiFi热点设备是可信任的。

[0152] 在本实施例中，若确认第四数据摘要不等于第三数据摘要，则表示WiFi热点设备是不可信任的，结束当前流程，返回步骤S1继续接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧。

[0153] 本实施例中，利用先利用认证密码对明文进行相应的运算得到对应的数据摘要，实现对相关数据进行加密，再通过对比来自WiFi热点设备和当前接入设备自身的数据摘要是否相等间接，判断预置在WiFi热点设备的第二认证密码与预置在当前接入设备自身的第一认证密码是否相同，实现双方身份合法性认证，同时有效的保障相关数据的安全性。

[0154] 在一个具体的实施例中，所述的第一加密数据包括密文、第五数据摘要；

[0155] 其中所述的密文以第一随机数、第二随机数、第一认证密码串接作为密钥，运用对称加密算法对待传输数据进行加密得到，具体公式如下：

[0156] EDT＝SFencrypt(PDT,Nonce1|Nonce2|AuthPwd1)

[0157] 式中，EDT表示密文;Nonce1|Nonce2|AuthPwd1表示以Nonce1|Nonce2|AuthPwd1作为密钥。

[0158] 所述的第五数据摘要运用数据摘要算法对密文、第一随机数、第二随机数、第一认证密码运算得到，具体公式如下：

[0159] DS＝AF(EDT,Nonce1|Nonce2,AuthPwd1)

[0160] 式中，DS表示第五数据摘要。

[0161] 在本实施例中，通过对待传输数据进行加密，提高数据传输的安全性。

[0162] 在本实施例中，当前接入设备发送相应的探测请求帧给WiFi热点设备，由WiFi热点设备完成初步认证、三次认证。先由WiFi热点设备进行初步认证，判断当前接入设备是否可信;在由当前接入设备进行二次认证，判断WiFi热点设备是否可信;在判断双方都可信的提前下，再对待传输数据进行加密通信传输给WiFi热点设备，因此本实施例所述的WiFi近距离自动配置方法具有认证、加密能力，数据通信安全性高的特点。

[0163] 实施例3

[0164] 本实施例以无线mesh路由器的组网过程为例。目前市场上无线mesh路由器多数为两个或三个组合使用。其中一个为主路由器，其他为从路由器。从路由器作为当前接入设备自动连接主路由器(WiFi热点设备)，建立mesh网络中的后传(backhaul)连接。这个连接是用于主、从路由器之间传递数据的。

[0165] 从路由器能成功连接主路由器，是因为出厂时已作好默认配置，从路由器和主路由器配置是匹配的，即SSID和密码是正确的，才能连接上。假设用户开始买了两个已配对好的mesh路由器，而现在想再增加一个从路由器(一般主、从路由器均为同一厂家产品，不同厂家不同对通)，则必须对新的从路由器通过网页进行WiFi参数配置，或者使用WPS按钮功能，在主路由器和从路由器上分别按一下WPS按钮，路由器通过WPS流程完成参数配置。

[0166] 使用实施例1和实施例所述的wifi近距离自动配置方法实现自动配置，如图3所示，只需把新的从路由器放置在主路由器旁边，上电启动，等待自动配置完成后即可使用。

[0167] 本实施例以主路由器发送的信标帧，带有厂商信息，MID＝“VSOL”。主路由器中预

置的第二认证密码和从路由器中预置的第一认证密码均为AuthPwd＝“VSOL-051AC68”。认证过程中随机数长度为32bit，数据摘要算法AF为采用MD5算法，SFencrypt、SFdecrypt算法采用AES-ECB算法，其中密钥经MD5算法转为128bit。

[0168] 如图4所示，以下举例说明主路由器和从路由器2的自动配置过程：

[0169] Step1：主路由器每100ms广播一次信标帧，带有MID＝“VSOL”信息。

[0170] Step2：从路由器2接收到主路由器发出的信标帧，且信号强度大于阀值-30dBm；同时目前从路由器2一直无法连接其出厂设置的回传热点；于是从路由器2触发自动配置流程。

[0171] Step3：从路由器2内部生成一个第一随机数Nonce1，值为“00010203”。明文PT取值为从路由器2的MAC地址字符串表达形式PT＝“8014a8000002”。根据明文、第一随机数、预置的第一认证密码通过数据摘要算法运算得到第一数据摘要ADS1如下：

[0172] ADS1＝AF(“8014a8000002”,“00010203”,“VSOL-051AC68”)

[0173] ＝MD5(“8014a800000200010203VSOL-051AC68”)

[0174] ＝“4fd30854d2d095fe19a8339425e66f04”

[0175] 从路由器2向主路由器发送第一探测请求帧M1，通过厂商自定义信息单元(IE)携带Nonce1、PT和ADS1信息。从而将PT、Nonce1、ADS1通过第一探测请求帧M1消息发送到主路由器。

[0176] Step4：主路由器接收到第一探测请求帧M1，通过预置的第二认证密码对明文进行数据摘要算法运算得到第二数据摘要ADS2：

[0177] ADS2＝AF(“8014a8000002”,“00010203”,“VSOL-051AC68”)

[0178] ＝MD5(“8014a800000200010203VSOL-051AC68”)

[0179] ＝“4fd30854d2d095fe19a8339425e66f04”

[0180] 若ADS1等于ADS2，则初步认证通过。主路由器将发送功率调至强度P_{low}＝-20dBm。

[0181] Step5：主路由器生成第二随机数Nonce2，其值为“11223344”；根据明文、第二随机数、预置的第二认证密码通过数据摘要算法运算得到第三数据摘要ADS3：

[0182] ADS3＝AF(“8014a8000002”,“0001020311223344”,“VSOL-051AC68”)

[0183] ＝MD5(“8014a8000002000102031122334 4VSOL-051AC68”)

[0184] ＝“00e2f5204bd28e748970b410a8f8dd14”

[0185] 主路由器向从路由器2发送第一探测应答帧M2，通过厂商自定义信息单元携带Nonce2、PT和ADS3信息，实现第一探测应答帧M2携带有PT、Nonce2和ADS3信息。

[0186] Step6：从路由器2接收到对第一探测应答帧M2后，进行以下校验完成二次认证，得到第四数据摘要ADS4：

[0187] ADS4＝AF(PT,Nonce1|Nonce2,AuthPwd1)

[0188] 如果ADS3等于ADS4，则认证通过。

[0189] Step7：从路由器2以Nonce1|Nonce2|AuthPwd为密钥，运用AES-ECB算法，对待传输数据PDT(待传输数据为“button push”)进行加密，得到密文EDT：

[0190] EDT＝SFEncrypt(“button push”,“0001020311223344VSOL-051AC68”)

[0191] ＝$AES\text{-}ECB_{encrypt}$(“button push”,MD5(“0001020311223344VSOL-051AC68”))

[0192] ＝$AES\text{-}ECB_{encrypt}$(“button push”,“859a073d0b37c7f6cf1f94ee67811791”)

[0193] ＝“qjvBMtjfwxeHGqTOUX6e7Q＝＝”

[0194] 再运用数据摘要算法AF,求出密文EDT的第五数据摘要DS:

[0195] DS＝AF(“qjvBMtjfwxeHGqTOUX6e7Q＝＝”,“0001020311223344”,“VSOL-051AC68”)

[0196] ＝MD5(“qjvBMtjfwxeHGqTOUX6e7Q＝＝0001020311223344VSOL-051AC68”)

[0197] ＝“045dc3d337c3f44789ea3f24cb9a5298”

[0198] 从路由器2向主路由器发送携带有EDT、DS信息的第二探测请求帧M3,具体在厂商自定义信息单元中携带EDT、DS信息。

[0199] Step8:主路由器接收到第二探测请求帧M3,首先对密文EDT进行校验,得到第一校验码VS:

[0200] VS＝AF(“qjvBMtjfwxeHGqTOUX6e7Q＝＝”,“0001020311223344”,

[0201] “VSOL-051AC68”)

[0202] ＝MD5(“qjvBMtjfwxeHGqTOUX6e7Q＝＝0001020311223344VSOL-051AC68”)

[0203] ＝“045dc3d337c3f44789ea3f24cb9a5298”

[0204] 若VS等于DS,对密文EDT进行解密操作:

[0205] PDT＝SFdecrypt(“qjvBMtjfwxeHGqTOUX6e7Q＝＝”,

[0206] “0001020311223344VSOL-051AC68”)

[0207] ＝$AES\text{-}ECB_{decrypt}$(“qjvBMtjfwxeHGqTOUX6e7Q＝＝”,

[0208] MD5(“0001020311223344VSOL-051AC68”))

[0209] ＝$AES\text{-}ECB_{decrypt}$(“qjvBMtjfwxeHGqTOUX6e7Q＝＝”,

[0210] “859a073d0b37c7f6cf1f94ee67811791”)

[0211] ＝“button push”

[0212] 若VS不等于DS,则执行Step12;

[0213] Step9:主路由器向从路由器2发送第二探测应答帧M4,表明之前的第二探测请求帧M3已收到。从路由器2执行与按下WPS按钮相同的操作,开始WPS配置流程。

[0214] Step10:主路由器将发送功率调回P_{normal}＝19dBm。

[0215] Step11:主路由器和从路由器2进入正常WPS配置流程,主路由器将当前的SSID、连接密码等WiFi接入参数传递到从路由器2,完成配置,执行步骤Step13。

[0216] Step12:主路由器将发送功率调回P_{normal}＝19dBm,

[0217] Step13:流程结束。

[0218] 实施例4

[0219] 一种电子设备,包括:至少一个处理器;以及,与所述至少一个处理器通信连接的存储器;其中,所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述任一方法实施例中WiFi热点设备与当前接入设备之间近距离自动配置方法。

[0220] 其中,存储器和处理器采用总线方式连接,总线可以包括任意数量的互联的总线和桥,总线将一个或多个处理器和存储器的各种电路连接在一起。总线还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路连接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口在总线和收发机之间提供接口。收发机

可以是一个元件,也可以是多个元件,比如多个接收器和发送器,提供用于在传输介质上与各种其他装置通信的单元。经处理器处理的数据通过天线在无线介质上进行传输,进一步,天线还接收数据并将数据传送给处理器。

[0221] 本实施例还提供了一种计算机可读存储介质,存储有计算机程序,所述计算机程序被处理器执行时实现上述任一方法实施例中WiFi热点设备与当前接入设备之间近距离自动配置方法。

[0222] 即,本领域技术人员可以理解,实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序存储在一个存储介质中,包括若干指令用以使得一个设备(可以是单片机,芯片等)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-OnlyMemory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0223] 显然,本发明的上述实施例仅仅是为清楚地说明本发明所作的举例,而并非是对本发明的实施方式的限定。凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明权利要求的保护范围之内。

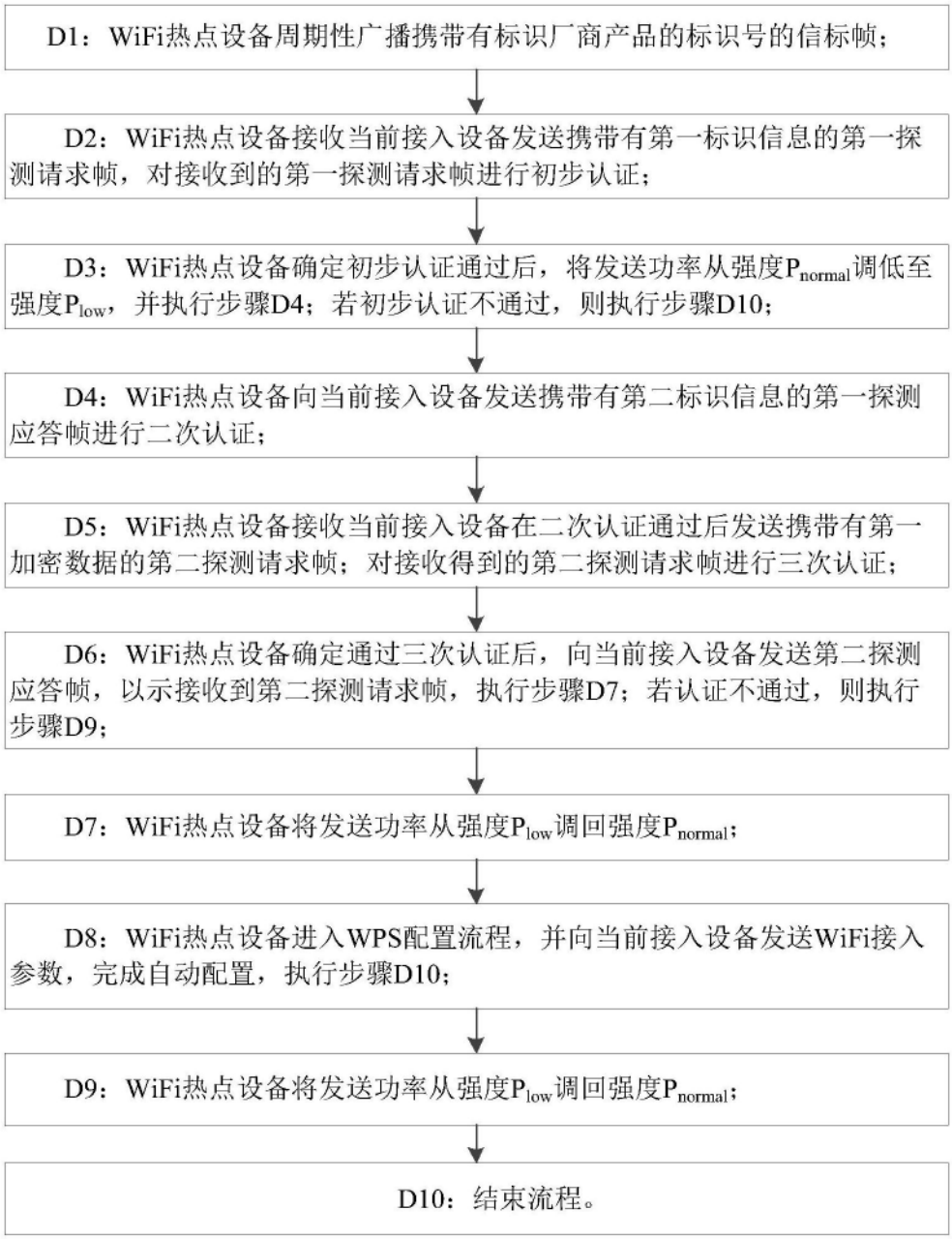

D1：WiFi热点设备周期性广播携带有标识厂商产品的标识号的信标帧；
D2：WiFi热点设备接收当前接入设备发送携带有第一标识信息的第一探测请求帧，对接收到的第一探测请求帧进行初步认证；
D3：WiFi热点设备确定初步认证通过后，将发送功率从强度P_{normal}调低至强度P_{low}，并执行步骤D4；若初步认证不通过，则执行步骤D10；
D4：WiFi热点设备向当前接入设备发送携带有第二标识信息的第一探测应答帧进行二次认证；
D5：WiFi热点设备接收当前接入设备在二次认证通过后发送携带有第一加密数据的第二探测请求帧；对接收得到的第二探测请求帧进行三次认证；
D6：WiFi热点设备确定通过三次认证后，向当前接入设备发送第二探测应答帧，以示接收到第二探测请求帧，执行步骤D7；若认证不通过，则执行步骤D9；
D7：WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal}；
D8：WiFi热点设备进入WPS配置流程，并向当前接入设备发送WiFi接入参数，完成自动配置，执行步骤D10；
D9：WiFi热点设备将发送功率从强度P_{low}调回强度P_{normal}；
D10：结束流程。

图1

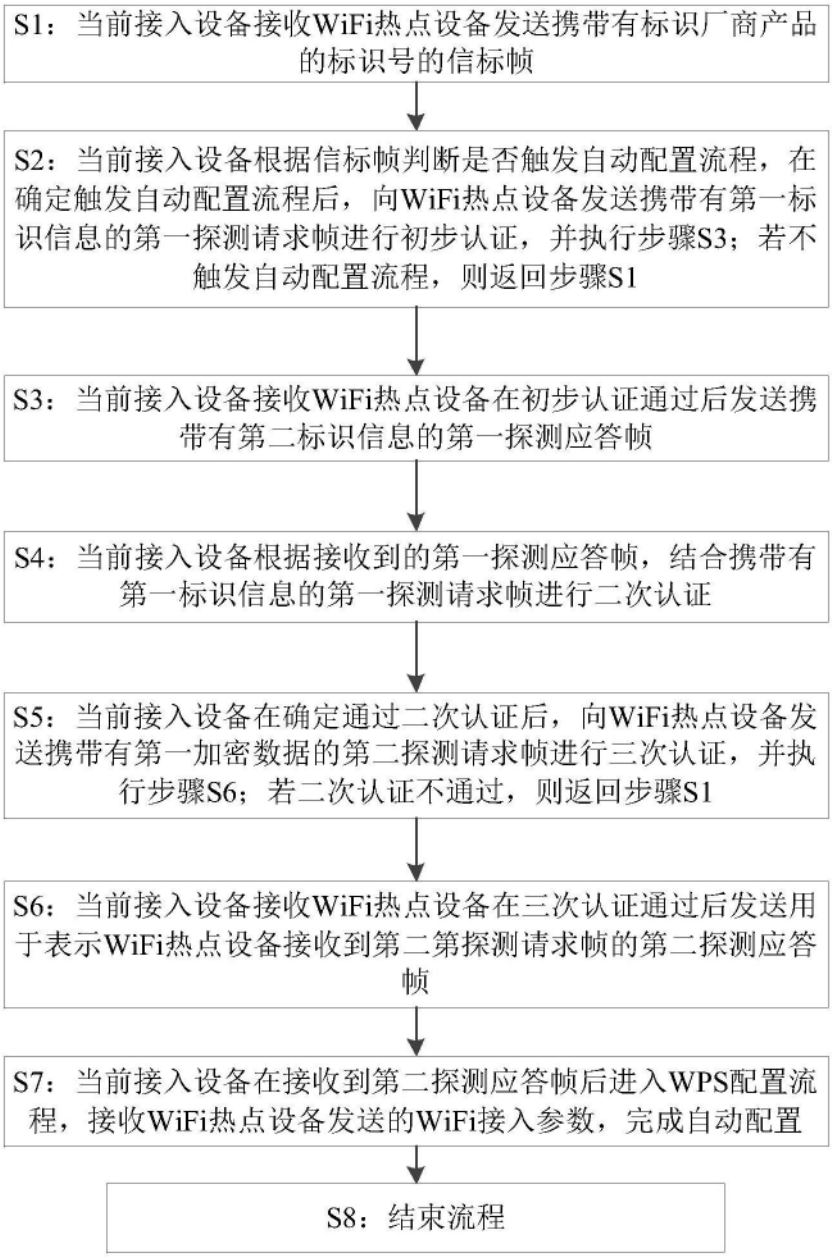

S1：当前接入设备接收WiFi热点设备发送携带有标识厂商产品的标识号的信标帧
S2：当前接入设备根据信标帧判断是否触发自动配置流程，在确定触发自动配置流程后，向WiFi热点设备发送携带有第一标识信息的第一探测请求帧进行初步认证，并执行步骤S3；若不触发自动配置流程，则返回步骤S1
S3：当前接入设备接收WiFi热点设备在初步认证通过后发送携带有第二标识信息的第一探测应答帧
S4：当前接入设备根据接收到的第一探测应答帧，结合携带有第一标识信息的第一探测请求帧进行二次认证
S5：当前接入设备在确定通过二次认证后，向WiFi热点设备发送携带有第一加密数据的第二探测请求帧进行三次认证，并执行步骤S6；若二次认证不通过，则返回步骤S1
S6：当前接入设备接收WiFi热点设备在三次认证通过后发送用于表示WiFi热点设备接收到第二第探测请求帧的第二探测应答帧
S7：当前接入设备在接收到第二探测应答帧后进入WPS配置流程，接收WiFi热点设备发送的WiFi接入参数，完成自动配置
S8：结束流程

图2

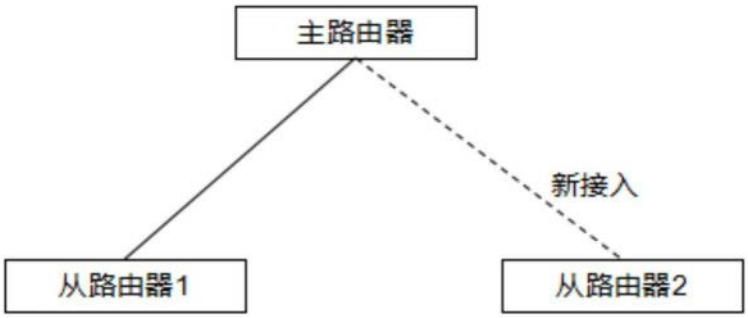

主路由器
新接入
从路由器1
从路由器2

图3

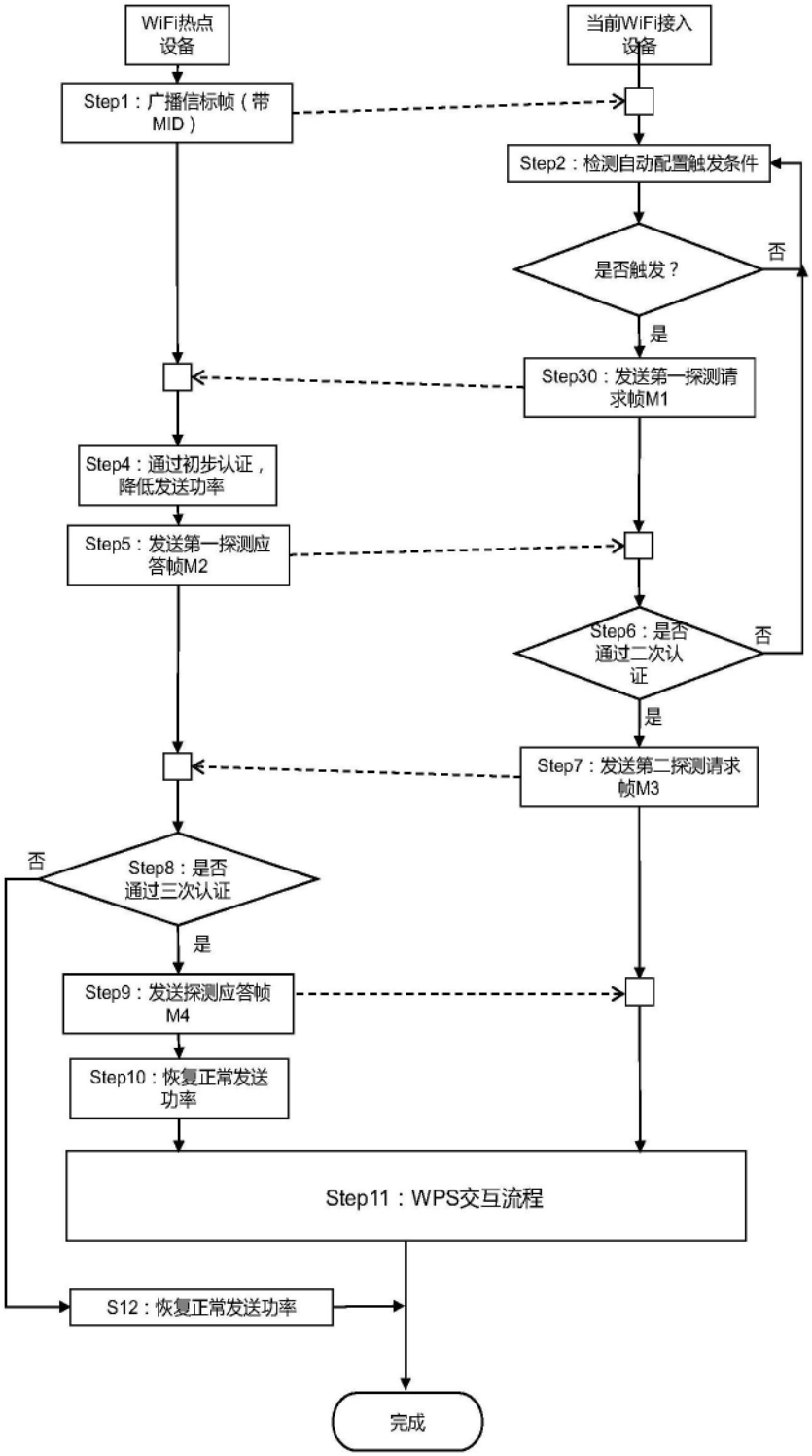

WiFi热点设备
当前WiFi接入设备
Step1：广播信标帧（带MID）
Step2：检测自动配置触发条件
是否触发？
否
是
Step30：发送第一探测请求帧M1
Step4：通过初步认证，降低发送功率
Step5：发送第一探测应答帧M2
Step6：是否通过二次认证
否
是
Step7：发送第二探测请求帧M3
否
Step8：是否通过三次认证
是
Step9：发送探测应答帧M4
Step10：恢复正常发送功率
Step11：WPS交互流程
S12：恢复正常发送功率
完成

图4