(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105959943 B
(45)授权公告日 2019.04.02

(21)申请号 201610287903.1

(22)申请日 2016.05.04

(65)同一申请的已公布的文献号
申请公布号 CN 105959943 A

(43)申请公布日 2016.09.21

(73)专利权人 深圳市蜂联科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路鲤鱼门街1号前海深港合作区管理局综合办公楼A201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 赖锐斌 叶柯 汪宇 崔营

(74)专利代理机构 成都众恒智合专利代理事务所(普通合伙) 51239
代理人 刘华平

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/06(2009.01)
H04W 48/10(2009.01)
H04W 48/16(2009.01)
H04W 76/11(2018.01)

(56)对比文件
CN 105472700 A,2016.04.06,
CN 103533608 A,2014.01.22,
CN 105554687 A,2016.05.04,
CN 104202308 A,2014.12.10,
CN 102547699 A,2012.07.04,
CN 105451188 A,2016.03.30,
CN 105208631 A,2015.12.30,
US 2015305081 A1,2015.10.22,

审查员 杨钰娟

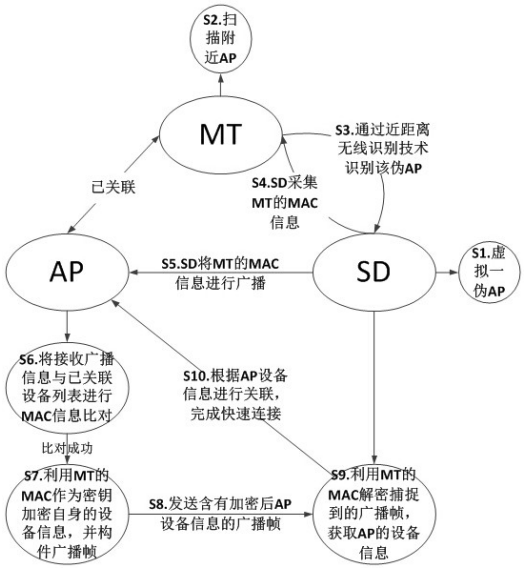
权利要求书2页 说明书4页 附图3页

(54)发明名称

一种利用第三方移动终端MT实现SD和AP快速连接的方法

(57)摘要

本发明公开了一种利用第三方移动终端MT实现SD和AP快速连接的方法,还包括第三方移动终端MT,步骤为:SD虚拟出伪AP;MT主动扫描附近AP,通过近距离无线识别技术识别出该伪AP,由SD采集到MT的MAC,并将该MAC通过广播帧发送给AP;AP识别该MAC后,用该MAC将自身的设备信息加密组成数据流,再嵌入广播帧内形成广播包发送;SD接收广播包后用该MT的MAC解密,提取出AP的设备信息,由此与AP进行关联,完成快速连接。本发明巧妙地利用了第三方移动终端MT作为中介并利用了MT的MAC信息作为密钥加密AP自身的设备信息,使得AP在主动广播的自身设备信息时能够限定接收方,完全避免了智能组网过程中的误连接情况,准确可靠,安全性高。



CN 105959943 B

1.一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，还包括一与AP已关联的第三方移动终端MT，所述SD为智能设备，该方法通过如下步骤实现：

(S1)所述SD虚拟出一个可响应第三方移动终端MT扫描的伪AP；

(S2)所述第三方移动终端MT主动扫描附近AP，获得包含所述伪AP的AP连接列表；

(S3)所述MT逐渐靠近所述SD，通过近距离WIFI无线识别技术从该AP连接列表中识别出所述伪AP，同时所述SD也识别出所述MT；

(S4)所述SD采集到所述MT的MAC信息；

(S5)所述SD将所述MT的MAC信息嵌入到广播帧内进行广播；

(S6)所述AP通过接收广播帧提取到其内嵌的数据信息，并调用自身的已关联设备列表进行MAC信息比对；

(S7)所述AP将比对成功的数据信息识别为所述MT的MAC信息，并利用该MAC信息作为密钥加密由其自身提取出的设备信息，组成数据流，然后将数据流中的数据信息内嵌到多个广播帧内形成广播包；

(S8)所述AP在当前信道周期性地发送所述广播包；

(S9)所述SD周期性地切换工作信道捕捉广播帧，并在捕捉到完整的广播包后，利用获得的所述MT的MAC信息作为密钥解析该广播包，提取其内嵌的AP设备信息；

(S10)所述SD根据获得的AP设备信息向AP定向发送链路认证请求，与AP进行关联，完成快速连接。

2.根据权利要求1所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述步骤(S3)中的近距离WIFI无线识别技术通过如下步骤实现：

(S3a)所述MT主动扫描并逐渐接近SD，此时SD虚拟出的伪AP的响应信号强度逐渐变大；

(S3b)所述MT实时监测所述AP连接列表内的各AP的信号强度信息，当一AP的信号强度大于设定的固定阈值或/和一AP的信号强度增强幅度大于设定的另一固定阈值时，识别出该AP为所述伪AP。

3.根据权利要求1所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述步骤(S7)中，AP的设备信息包括服务集标识SSID、密码Key、带宽信息BANDWIDTH、认证方式信息AUTHENTICATION、加解密方式信息ENCRYPTION、信道信息CHANNEL和可选信息OPTION。

4.根据权利要求3所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述数据流由数据流的长度信息、数据主体和CRC校验信息组成，其中，所述数据主体部分为经过MT的MAC信息加密的AP设备信息。

5.根据权利要求4所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述广播帧根据802.11标准生成，由标头Header、嵌入数据区和帧校验序列FCS组成，每一个广播帧的嵌入数据区内存储有所述数据流内的至少一个数据。

6.根据权利要求5所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，在一组完整的所述广播包内，在连续一定数目的广播帧后插入连续的3个长度之差固定的广播识别帧。

7.根据权利要求6所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述步骤(S9)中SD在捕捉到当前信道内的广播帧后，还对捕捉到的连续多个广

播帧进行验证，判断这些连续的广播帧中是否存在广播识别帧，若是，则所述SD停留在当前信道接收完整组广播帧，否则所述SD在一设定时间后将工作信道切换至相邻信道。

8.根据权利要求4～7任一项所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述步骤(S9)中SD对捕捉的广播帧进行解析时，通过验证提取到的数据流信息内的长度信息判断一组广播帧的数量是否接收完整，若不完整，则丢弃所接收到的广播帧，并重新接收；若广播帧的数量完整，则通过验证提取到的数据流信息内的CRC校验信息判断该组广播包的内容是否完整，若不完整，则丢弃所接收到的广播帧，并重新接收，若广播包的内容完整则继续利用MT的MAC信息解密。

9.根据权利要求1～7任一项所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，所述步骤(S10)中，在所述AP与SD关联后，进行接入认证、通过密钥协商，SD获取IP地址，接入无线网络，同时AP中止广播帧的广播。

10.根据权利要求9所述的一种利用第三方移动终端MT实现SD和AP快速连接的方法，其特征在于，在所述SD接入无线网络后，所述SD取消虚拟出的伪AP。

一种利用第三方移动终端MT实现SD和AP快速连接的方法

技术领域

[0001] 本发明涉及无线通信技术领域，具体地讲，是涉及一种在无关联的WIFI环境下利用第三方移动终端MT实现SD和AP快速连接的方法。

背景技术

[0002] 随着互联网不断兴起，移动需求的日益凸显，无线互联的需求也越发强烈。在现有的无线通信技术中，蓝牙通信技术覆盖范围小，红外线通信技术受到环境影响大穿墙效果不理想。而WIFI通信技术由于应用广泛，逐渐被企业、家庭接受。在传统的基于标准的IEEE802.11定义了无线网络的规范：一个无线点作为AP(Access Point)模式，其他的无线点作为STA(STAtion)模式，通过STA关联到AP后，STA才能与AP之间进行通信，STA与STA之间的通信也依靠AP进行中转，类似移动通信的基站与手机的模式。在没有进行认证关联并关联成功之前，STA与AP、STA与STA这些设备之间是不能够进行数据通信的。在通常的网络通信中STA和AP提供认证、解除认证、数据加密、数据传输的服务，这种设计方案的安全性很高，在正常情况下，STA和AP建立连接的过程如图1所示，即是人为地控制STA以主动或被动的方式扫描周围的AP，获得周围AP的信息，然后STA通过手动或自动地输入key，进行链路认证，建立与AP的关联。

[0003] 但是针对某些的特殊智能设备，如一些没有输入设备、没有串口、没有触摸屏的智能设备SD(Smart Device)，想要与AP进行关联通信，现有的这种技术方案就无能为力了。另一方面，用户在使用绝对安全可靠的SD设备连接AP时，希望获得一种比现有技术方案更为快速高效的连接方案，而在目前的市场上暂时没有合理快速高效的解决方案。而且在智能家居的组网应用中，通常可能存在很多SD，就会导致一些误组网的情况发生，但这并不是设计者所希望看到的，因此这也是一个需要解决的问题。

发明内容

[0004] 为克服现有技术中的上述问题，本发明提供一种构思新颖、设计巧妙、能有效解决误组网问题的利用第三方移动终端MT实现SD和AP快速连接的方法。

[0005] 为了实现上述目的，本发明采用的技术方案如下：

[0006] 一种利用第三方移动终端MT实现SD和AP快速连接的方法，还包括一与AP已关联的第三方移动终端MT，该方法通过如下步骤实现：

[0007] (S1)所述SD虚拟出一个可响应第三方移动终端MT扫描的伪AP；

[0008] (S2)所述第三方移动终端MT主动扫描附近AP，获得包含所述伪AP的AP连接列表；

[0009] (S3)所述MT逐渐靠近所述SD，通过近距离无线识别技术从该AP连接列表中识别出所述伪AP，同时所述SD也识别出所述MT；

[0010] (S4)所述SD采集到所述MT的MAC信息；

[0011] (S5)所述SD将所述MT的MAC信息嵌入到广播帧内进行广播；

[0012] (S6)所述AP通过接收广播帧提取到其内嵌的数据信息，并调用自身的已关联设备

列表进行MAC信息比对；

[0013] (S7)所述AP将比对成功的数据信息识别为所述MT的MAC信息，并利用该MAC信息作为密钥加密由其自身提取出的设备信息，组成数据流，然后将数据流中的数据信息内嵌到多个广播帧内形成广播包；

[0014] (S8)所述AP在当前信道周期性地发送所述广播包；

[0015] (S9)所述SD周期性地切换工作信道捕捉广播帧，并在捕捉到完整的广播包后，利用获得的所述MT的MAC信息作为密钥解析该广播包，提取其内嵌的AP设备信息；

[0016] (S10)所述SD根据获得的AP设备信息向AP定向发送链路认证请求，与AP进行关联，完成快速连接。

[0017] 具体地，所述步骤(S3)中的近距离无线识别技术通过如下步骤实现：

[0018] (S3a)所述MT主动扫描并逐渐接近SD，此时SD虚拟出的伪AP的响应信号强度逐渐变大；

[0019] (S3b)所述MT实时监测所述AP连接列表内的各AP的信号强度信息，当一AP的信号强度大于设定的固定阈值或/和一AP的信号强度增强幅度大于设定的另一固定阈值时，识别出该AP为所述伪AP。

[0020] 进一步地，所述步骤(S7)中，AP的设备信息包括服务集标识SSID、密码Key、带宽信息BANDWIDTH、认证方式信息AUTHENTICATION、加解密方式信息ENCRYPTION、信道信息CHANNEL和可选信息OPTION。

[0021] 进一步地，所述数据流由数据流的长度信息、数据主体和CRC校验信息组成，其中，所述数据主体部分为经过MT的MAC信息加密的AP设备信息。

[0022] 进一步地，所述广播帧根据802.11标准生成，由标头Header、嵌入数据区和帧校验序列FCS组成，每一个广播帧的嵌入数据区内存储有所述数据流内的至少一个数据。

[0023] 为了便于识别，在一组完整的所述广播包内，在连续一定数目的广播帧后插入连续的3个长度之差固定的广播识别帧。

[0024] 相应地，所述步骤(S9)中SD在捕捉到当前信道内的广播帧后，还对捕捉到的连续多个广播帧进行验证，判断这些连续的广播帧中是否存在广播识别帧，若是，则所述SD停留在当前信道接收完整组广播帧，否则所述SD在一设定时间后将工作信道切换至相邻信道。

[0025] 为了SD接收内容的准确性，所述步骤(S9)中SD对捕捉的广播帧进行解析时，通过验证提取到的数据流信息内的长度信息判断一组广播帧的数量是否接收完整，若不完整，则丢弃所接收到的广播帧，并重新接收；若广播帧的数量完整，则通过验证提取到的数据流信息内的CRC校验信息判断该组广播包的内容是否完整，若不完整，则丢弃所接收到的广播帧，并重新接收，若广播包的内容完整则继续利用MT的MAC信息解密。

[0026] 更具体地，所述步骤(S10)中，在所述AP与SD关联后，进行接入认证、通过密钥协商，SD获取IP地址，接入无线网络，同时AP中止广播帧的广播。

[0027] 相应地，在所述SD接入无线网络后，所述SD取消虚拟出的伪AP。

[0028] 与现有技术相比，本发明具有以下有益效果：

[0029] 本发明巧妙地利用了第三方移动终端MT作为中介采集MT的MAC信息，并以此为密钥加密AP自身的设备信息，使得AP在主动广播的自身设备信息时能够限定接收方，完全避免了智能组网过程中的误连接情况，准确可靠，安全性高，同时在整个过程中SD设备不需要

任何输入信息，特别方便了没有串口没有触摸屏等没有输入装置的智能设备进行与AP的关联，方便快捷，具有广泛的应用前景，适合推广应用。

附图说明

[0030] 图1为现有技术中AP和SD建立连接的流程示意图。

[0031] 图2为本发明的流程示意图。

[0032] 图3为本发明中数据流结构和设备信息组成示意图。

[0033] 图4为本发明中广播帧的封装示意图。

具体实施方式

[0034] 下面结合附图和实施例对本发明作进一步说明，本发明的实施方式包括但不限于下列实施例。

实施例

[0035] 如图2至图4所示，该利用第三方移动终端MT实现SD和AP快速连接的方法，主要是为了解决现有技术中没有串口、没有触摸屏等没有输入装置的智能设备SD无法直接与AP建立连接的问题，以及加快安全可靠的SD设备与AP间的连接效率，可以适应各种复杂的无线网络通信环境，包括AD-Hoc网络、BSS网络、ESS网络；并且本方法是基于802.11标准设计，可以扩展兼容802.11协议族。

[0036] 该方法涉及的装置包括智能设备SD、无线点AP以及与AP已关联的第三方移动终端MT，其具体实现包括如下步骤：

[0037] (S1)所述SD虚拟出一个可响应第三方移动终端MT扫描的伪AP。

[0038] (S2)所述第三方移动终端MT主动扫描附近AP，获得包含所述伪AP的AP连接列表。

[0039] (S3)所述MT逐渐靠近所述SD，通过近距离无线识别技术从该AP连接列表中识别出所述伪AP，同时所述SD也识别出所述MT；具体地，

[0040] (S3a)所述MT主动扫描并逐渐接近SD，此时SD虚拟出的伪AP的响应信号强度逐渐变大；

[0041] (S3b)所述MT实时监测所述AP连接列表内的各AP的信号强度信息，当一AP的信号强度大于设定的固定阈值或/和一AP的信号强度增强幅度大于设定的另一固定阈值时，识别出该AP为所述伪AP。

[0042] (S4)所述SD采集到所述MT的MAC信息。

[0043] (S5)所述SD将所述MT的MAC信息嵌入到广播帧内进行广播。

[0044] (S6)所述AP通过接收广播帧提取到其内嵌的数据信息，并调用自身的已关联设备列表进行MAC信息比对。

[0045] (S7)所述AP将比对成功的数据信息识别为所述MT的MAC信息，并利用该MAC信息作为密钥加密由其自身提取出的设备信息，组成数据流，然后将数据流中的数据信息内嵌到多个广播帧内形成广播包；

[0046] 其中，所述AP的设备信息包括服务集标识SSID、密码Key、带宽信息BANDWIDTH、认证方式信息AUTHENTICATION、加解密方式信息ENCRYPTION、信道信息CHANNEL和可选信息

OPTION。

[0047] 所述数据流由数据流的长度信息、数据主体和CRC校验信息组成，其中，所述数据主体部分为经过MT的MAC信息加密的AP设备信息。

[0048] 所述广播帧根据802.11标准生成，由标头Header、嵌入数据区和帧校验序列FCS组成，每一个广播帧的嵌入数据区内存储有所述数据流内的至少一个数据。

[0049] 为了便于识别，在一组完整的所述广播包内，在连续一定数目的广播帧后插入连续的3个长度之差固定的广播识别帧。

[0050] (S8)所述AP在当前信道周期性地发送所述广播包。

[0051] (S9)所述SD周期性地切换工作信道捕捉广播帧，并在捕捉到完整的广播包后，利用获得的所述MT的MAC信息作为密钥解析该广播包，提取其内嵌的AP设备信息。

[0052] 所述SD在捕捉到当前信道内的广播帧后，还对捕捉到的连续多个广播帧进行验证，判断这些连续的广播帧中是否存在广播识别帧，若是，则所述SD停留在当前信道接收完整组广播帧，否则所述SD在一设定时间后将工作信道切换至相邻信道。

[0053] 为了SD接收内容的准确性，所述SD对捕捉的广播帧进行解析时，通过验证提取到的数据流信息内的长度信息判断一组广播帧的数量是否接收完整，若不完整，则丢弃所接收到的广播帧，并重新接收；若广播帧的数量完整，则通过验证提取到的数据流信息内的CRC校验信息判断该组广播包的内容是否完整，若不完整，则丢弃所接收到的广播帧，并重新接收，若广播包的内容完整则继续利用MT的MAC信息解密。

[0054] (S10)所述SD根据获得的AP设备信息向AP定向发送链路认证请求，与AP进行关联，进行接入认证、通过密钥协商，SD获取IP地址，接入无线网络，完成快速连接。同时AP中止广播帧的广播。相应地，在所述SD接入无线网络后，所述SD取消虚拟出的伪AP，以降低消耗和信道的占用。

[0055] 在实际应用中，当用户购买了应用本发明的智能设备，如智能路由器AP和智能灯SD，由于智能灯SD没有触摸屏、没有串口、没有任何输入装置，因此其无法直接通过操作连接AP，此时即可采用本发明方法，利用与AP已关联的智能手机MT，通过近距离无线识别技术与SD关联，由SD采集MT的MAC信息，并将该MAC信息通过嵌入广播帧发送给AP比对，而AP将自身设备信息利用该MAC信息加密，生成广播帧并广播。当智能灯SD接收到相应广播帧后，用MT的MAC信息解密后提取出的AP设备信息，然后与AP进行关联，便能快速完成连接，从而实现对智能灯的控制。

[0056] 上述实施例仅为本发明的优选实施例，并非对本发明保护范围的限制，但凡采用本发明的设计原理，以及在此基础上进行非创造性劳动而作出的变化，均应属于本发明的保护范围之内。

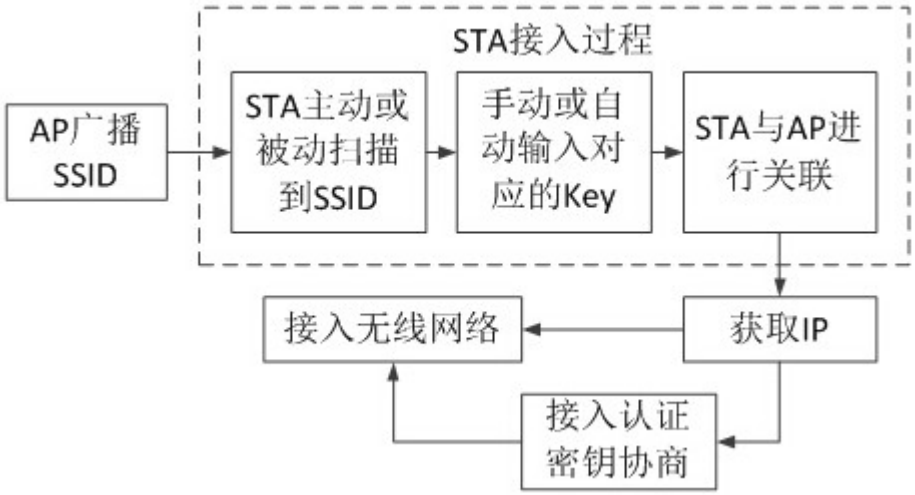

STA接入过程
AP广播SSID
STA主动或被动扫描到SSID
手动或自动输入对应的Key
STA与AP进行关联
获取IP
接入无线网络
接入认证密钥协商

图1

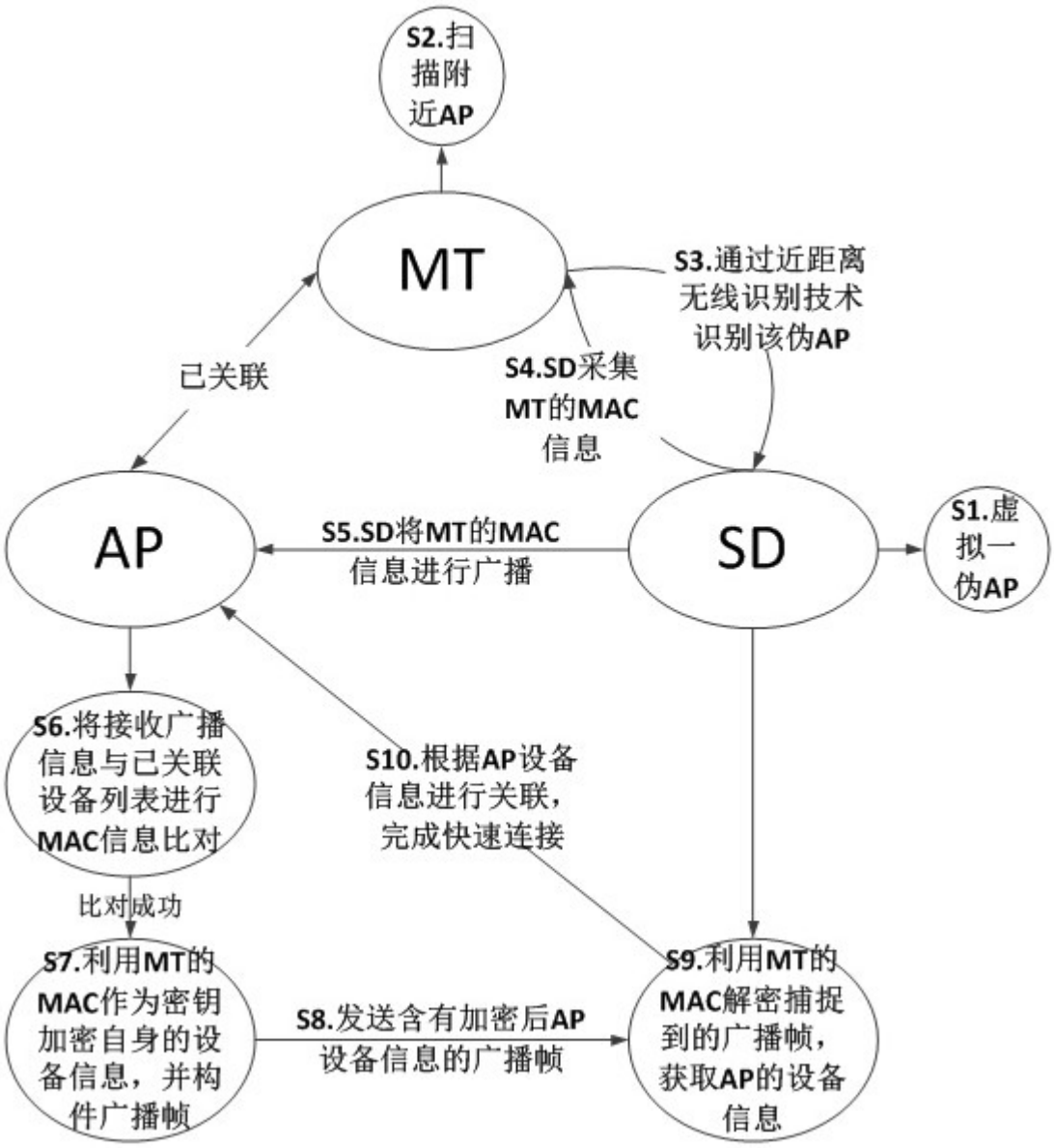

S2.扫描附近AP
MT
S3.通过近距离无线识别技术识别该伪AP
已关联
S4.SD采集MT的MAC信息
AP
S5.SD将MT的MAC信息进行广播
SD
S1.虚拟一伪AP
S6.将接收广播信息与已关联设备列表进行MAC信息比对
S10.根据AP设备信息进行关联，完成快速连接
比对成功
S7.利用MT的MAC作为密钥加密自身的设备信息，并构件广播帧
S8.发送含有加密后AP设备信息的广播帧
S9.利用MT的MAC解密捕捉到的广播帧，获取AP的设备信息

图2

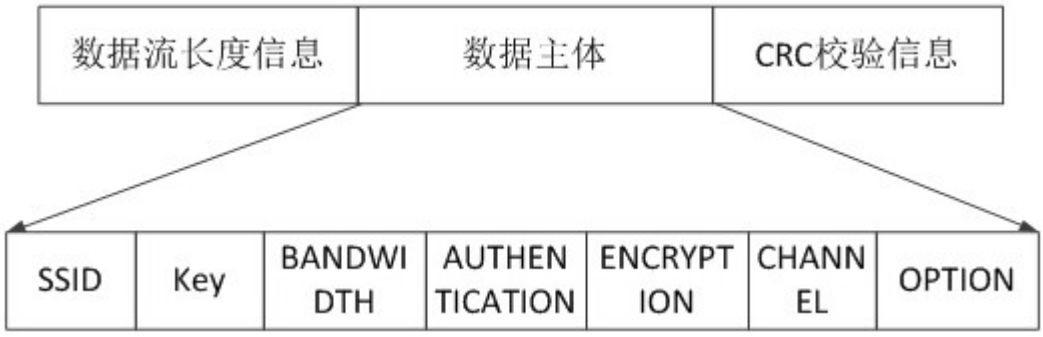

数据流长度信息
数据主体
CRC校验信息
SSID
Key
BANDWIDTH
AUTHENTICATION
ENCRYPTION
CHANNEL
OPTION

图3

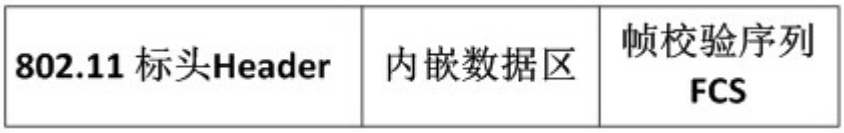


图4