(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 103763697 B
(45)授权公告日 2018.01.16

(21)申请号 201310526582.2

(22)申请日 2013.10.29

(65)同一申请的已公布的文献号
申请公布号 CN 103763697 A

(43)申请公布日 2014.04.30

(73)专利权人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区广富林路4855弄20号、90号

(72)发明人 张剑

(74)专利代理机构 杭州千克知识产权代理有限公司 33246
代理人 周希良

(51)Int.Cl.
*H04W 12/04*(2009.01)
*H04W 12/06*(2009.01)

(56)对比文件
CN 102204304 A,2011.09.28,
US 2009/0190763 A1,2009.07.30,
WO 2010/034728 A1,2010.04.01,
CN 103096307 A,2013.05.08,
CN 102904713 A,2013.01.30,

审查员 丁滔

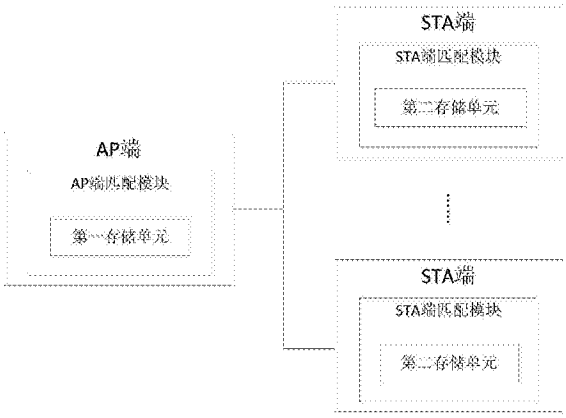
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种无线接入点多密钥支持系统及方法

(57)摘要

本发明公开了一种无线接入点多密钥支持系统及方法，属于无线AP连接安全性技术领域，系统包括AP端的AP端匹配模块和多个STA端的STA端匹配模块；AP端匹配模块与STA端匹配模块进行匹配，并根据匹配结果选择相应的STA端密钥进行远程连接；方法包括：在AP端以预置的第一方法形成多个标准加密数据；在STA端以预置的第二方法形成多个加密数据；以预置的策略将加密数据与标准加密数据进行匹配；根据匹配结果，AP端采用STA端密钥与STA端建立远程连接。上述技术方案的有益效果是：可以使得密钥的获知范围最大限度地缩小，增加了系统的连接安全性，有利于隐私保护。




CN 103763697 B

1.一种无线接入点多密钥支持系统，其特征在于，包括AP端和多个STA端；

所述AP端包括一AP端匹配模块；每个STA端包括一STA端匹配模块；

每个STA端匹配模块中设有一个预置的STA端密钥；

所述AP端匹配模块中设有多个预置的AP端密钥；

所述AP端匹配模块与所述STA端匹配模块采用预置的策略，将所述STA端密钥与多个所述预置的AP端密钥进行匹配；所述AP端根据匹配结果，以所述STA端密钥与对应的所述STA端建立远程连接；

所述AP端匹配模块中包括第一存储单元；所述第一存储单元内设有用于保存多个预置的AP端密钥的第一存储空间；

所述AP端匹配模块根据多个所述预置的AP端密钥，以预置的第一方法生成多个相应的标准加密数据；

所述第一存储单元中还包括用于保存多个所述标准加密数据的第二存储空间；所述标准加密数据与所述AP端密钥一一对应；

所述预置的第一方法包括：

所述AP端匹配模块生成一个认证数据，并以多个预置的所述AP端密钥分别对所述认证数据进行加密，以形成对应的多个标准加密数据。

2.如权利要求1所述的无线接入点多密钥支持系统，其特征在于，所述STA端匹配模块包括第二存储单元；所述第二存储单元适于保存对应于所述STA端的所述STA端密钥；

所述STA端匹配模块根据所述STA端密钥，以预置的第二方法生成一个相应的加密数据；所述预置的第二方法包括：

所述STA端匹配模块读取所述AP端匹配模块生成的所述认证数据，并以所述STA端密钥进行加密，以形成相应的加密数据。

3.如权利要求2所述的无线接入点多密钥支持系统，其特征在于，所述预置的策略包括：

所述AP端匹配模块读取所述加密数据，并将所述加密数据与多个所述标准加密数据进行匹配；

若匹配成功，则所述AP端以所述STA端密钥与所述STA端建立连接。

4.一种无线接入点多密钥支持方法，其特征在于，包括AP端与多个STA端；每个所述STA端内设有一个预置的STA端密钥；

所述无线接入点多密钥支持方法包括：

步骤1，在所述AP端以预置的第一方法形成多个标准加密数据；

步骤2，在每个STA端以预置的第二方法形成一个对应的加密数据；

步骤3，以预置的策略将所述加密数据与所述标准加密数据进行匹配；

步骤4，根据匹配结果，采用所述STA端密钥将所述AP端与所述STA端建立远程连接；

所述预置的第一方法包括：

步骤11，在所述AP端形成一个认证数据；

步骤12，以所述AP端中预置的多个AP端密钥，对所述认证数据进行加密，以形成多个对应的所述标准加密数据；

所述预置的第二方法包括：

步骤21，由所述STA端读取所述认证数据；

步骤22，根据所述STA端密钥对所述认证数据进行加密，以形成一个对应的所述加密数据；

步骤23，将所述加密数据发送至所述AP端。

5.如权利要求4所述的无线接入点多密钥支持方法，其特征在于，所述预置的策略包括：

步骤41，将所述加密数据与多个所述标准加密数据进行匹配；

若匹配成功，转至步骤42；

若匹配失败，则向所述STA端发送连接失败的信号，并退出连接；

步骤42，采用所述STA端密钥在所述AP端与所述STA端之间建立远程连接。

# 一种无线接入点多密钥支持系统及方法

## 技术领域

[0001] 本发明涉及无线局域网络技术领域，尤其涉及一种无线接入点多密钥支持系统及方法。

## 背景技术

[0002] 现有的IEEE Std802.11认证方式包括了开放式的系统认证和共享密钥认证，且上述两种认证方式都可以用于独立基本服务集(Independent Basic Service Set,IBSS)和基本服务集(Infrastructure Basic Service Set,Infrastructure BSS)。

[0003] IEEE Std802.11标准中详细描述了共享密钥认证的过程：

[0004] 首先，共享密钥认证要求双方必须有一个公共密钥，这个过程只能在使用WEP(Wired Equivalent Privacy，加密技术)机制的工作站之间进行，以避免明文传输。

[0005] 使用共享密钥认证的鉴别过程简述如下：

[0006] 1.无线客户端(Station,STA)向无线接入点(Access Point,AP)发送验证请求；

[0007] 2.无线接入点发布一个随机产生的无格式的文本，从无线接入点清晰地发送到无线客户端；

[0008] 3.无线客户端响应请求，并使用自身的密钥加密该文本，并将经过加密的文本发回到无线接入点；

[0009] 无线接入点通过识别该经过加密的文本，并匹配WEP密钥，通过匹配成功的WEP密钥实现无线客户端与无线接入点之间的连接。

[0010] 现有的共享密钥认证方式仅仅只能对共享密钥认证的单个服务集标识(Service Set Identifier,SSID)提供一个密钥，从而导致所有需要连接到该SSID的无线客户端都必须知道这个密钥，这样会使得知晓密钥的范围扩大，降低了系统的安全性；另一方面，当其他用户破译该密钥时就可以非常方便地获取该网络中传输的所有数据，从而进一步降低了系统的安全性。

[0011] 中国专利(CN102711082A)公开了一种在移动通信中共享信任无线接入点信息的方法及系统，该方法包括：移动终端向与其建立共享无线接入点信息连接的其他移动终端，发送信任无线接入点列表；所述其他移动终端将接收到的信任无线接入点列表中所具有的而其自身的信任无线接入点列表中不具有的信任无线接入点信息，存储到其自身的信任无线接入点列表中；由用户主动控制在信任的移动终端之间共享信任无线接入点信息，从而只需要在一个移动终端上输入密钥，然后将该无线接入点信息共享给其它移动终端，其它移动终端就可以不用输入密码直接连接该无线接入点，以此增强了用户体验，提升产品附加价值。上述技术方案仍然涉及了共享密钥，甚至其他移动终端可以不用输入密码直接连接无线接入点，降低了连接的安全性。

[0012] 中国专利(CN103188801A)公开了一种STA控制方法和装置，其中，该方法包括：AP获取与AP关联的STA发送的Null_Data帧的参数信息；AP将参数信息与第一预定阈值进行比较；AP根据比较的结果对STA进行控制。上述技术方案并未涉及到STA与AP之间的连接方式，

也未涉及连接时使用的密钥，不能解决现有技术中存在的问题。

## 发明内容

[0013] 根据现有技术中存在的缺陷，现提供一种无线接入点多密钥支持系统及方法，具体包括：

[0014] 一种无线接入点多密钥支持系统，其中，包括AP端和多个STA端；

[0015] 所述AP端包括一AP端匹配模块；所述STA端包括一STA端匹配模块；

[0016] 每个所述STA端匹配模块中设有一个预置的STA端密钥；

[0017] 所述AP端匹配模块中设有一个预置的AP端密钥；

[0018] 所述AP端匹配模块与所述STA端匹配模块采用预置的策略，将所述STA端密钥与多个所述AP端密钥进行匹配；所述AP端根据匹配结果，以所述STA端密钥与对应的所述STA端建立远程连接。

[0019] 优选的，该无线接入点多密钥支持系统，其中，所述AP端匹配模块中包括第一存储单元；所述第一存储单元内设有用于保存多个预置的AP端密钥的第一存储空间；

[0020] 所述AP端匹配模块根据多个预置的所述AP端密钥，以预置的第一方法生成多个相应的标准加密数据；

[0021] 所述第一存储单元中还包括用于保存多个所述标准加密数据的第二存储空间；所述标准加密数据与所述AP端密钥一一对应。

[0022] 优选的，该无线接入点多密钥支持系统，其中，所述预置的第一方法包括：

[0023] 所述AP端匹配模块生成一个认证数据，并以多个预置的所述AP端密钥分别对所述认证数据进行加密，以形成对应的多个所述标准加密数据。

[0024] 优选的，该无线接入点多密钥支持系统，其中，所述STA端匹配模块包括第二存储单元；所述第二存储单元适于保存对应于所述STA端的所述STA端密钥；

[0025] 所述STA端匹配模块根据所述STA端密钥，以预置的第二方法生成一个相应的加密数据。

[0026] 优选的，该无线接入点多密钥支持系统，其中，所述预置的第二方法包括：

[0027] 所述STA端匹配模块读取所述AP端匹配模块生成的所述认证数据，并以所述STA端密钥进行加密，以形成相应的所述加密数据。

[0028] 优选的，该无线接入点多密钥支持系统，其中，所述预置的策略包括：

[0029] 所述AP端匹配模块读取所述加密数据，并将所述加密数据与多个所述标准加密数据进行匹配；

[0030] 若匹配成功，则所述AP端以所述STA端密钥与所述STA端建立连接。

[0031] 一种无线接入点多密钥支持方法，其中，包括AP端与多个STA端，每个所述STA端与所述AP端远程连接；

[0032] 每个所述STA端内设有一个预置的STA端密钥；

[0033] 所述无线接入点多密钥支持方法包括：

[0034] 步骤1，在所述AP端以预置的第一方法形成多个标准加密数据；

[0035] 步骤2，在每个所述STA端以预置的第二方法形成一个对应的加密数据；

[0036] 步骤3，以预置的策略将所述加密数据与所述标准加密数据进行匹配；

[0037] 步骤4，根据匹配结果，采用所述STA端密钥将所述AP端与所述STA端建立远程连接。

[0038] 优选的，该无线接入点多密钥支持方法，其中，所述预置的第一方法包括：

[0039] 步骤11，在所述AP端形成一个认证数据；

[0040] 步骤12，以所述AP端中预置的多个AP端密钥，对所述认证数据进行加密，以形成多个对应的所述标准加密数据。

[0041] 优选的，该无线接入点多密钥支持方法，其中，所述预置的第二方法包括：

[0042] 步骤21，由所述STA端读取所述认证数据；

[0043] 步骤22，根据所述STA端密钥对所述认证数据进行加密，以形成一个对应的所述加密数据；

[0044] 步骤23，将所述加密数据发送至所述AP端。

[0045] 优选的，该无线接入点多密钥支持方法，其中，所述预置的策略包括：

[0046] 步骤41，将所述加密数据与多个所述标准加密数据进行匹配；

[0047] 若匹配成功，转至步骤42；

[0048] 若匹配失败，则向所述STA端发送连接失败的信号，并退出连接；

[0049] 步骤42，采用所述STA端密钥在所述AP端与所述STA端之间建立远程连接。

[0050] 上述技术方案的有益效果是：无线连接点根据不同的密钥认证不同的无线客户端，可以使得密钥的获知范围最大限度地缩小，增加了系统的连接安全性，有利于隐私保护。

## 附图说明

[0051] 图1是本发明的实施例中，一种无线接入点多密钥支持系统的结构示意图；

[0052] 图2-5是本发明的实施例中，一种无线接入点多密钥支持方法的流程示意图。

## 具体实施方式

[0053] 下面结合附图和具体实施例对本发明作进一步说明，但不作为本发明的限定。

[0054] 如图1所示，本发明的较佳的实施例中，提供一种无线接入点多密钥支持系统，包括了多个无线客户端(STA端)和无线接入点(AP端)。每个STA端均可以与AP端进行远程通信。

[0055] 在AP端内设置有一AP端匹配模块，同样的在STA端内设置有一STA端匹配模块。在AP端匹配模块内设置了第一存储单元。在STA端匹配模块内设置了第二存储单元。

[0056] 本发明的较佳的实施例中，上述第一存储单元中包括了第一存储空间(未示出)，该第一存储空间用于保存多个预置的AP端密钥，具体而言，本发明的较佳的实施例中，第一存储空间中包括多个独立的第一存储块(未示出)，每个第一存储块中保存有一个单独的AP端密钥，即在第一存储空间中构成一个AP端密钥列表。

[0057] AP端匹配模块根据其预置的多个AP端密钥，采用预置的第一方法形成多个相应的标准加密数据；

[0058] 本发明的较佳的实施例中，上述预置的第一方法具体为：AP端匹配模块产生一个认证数据，并用以保存于第一存储空间中的所有预置的AP端密钥，对该认证数据分别进行

加密操作，以形成多个经过加密的标准加密数据。每个标准加密数据对应一个AP端密钥。本发明的较佳的实施例中，上述第一存储单元中还包括有第二存储空间，每个第二存储空间中包括了多个独立的第二存储块。每个第二存储块中用于存放一个标准加密数据，即上述第二存储空间中保存有标准加密数据列表，该列表中的标准加密数据与上述AP端密钥列表中的AP端密钥一一对应。

[0059] 本发明的较佳的实施例中，STA端匹配模块中包括了一个第二存储单元，该第二存储单元中保存有一个预置的STA端密钥。每个STA端内设置一个特定的STA端密钥。

[0060] STA端匹配模块根据上述STA端密钥，以预置的第二方法形成一个相应的加密数据。

[0061] 本发明的较佳的实施例中，上述预置的第二方法具体为：STA端匹配模块读取自远程的AP端传输来的认证数据，并以STA端密钥对该认证数据进行加密，以形成相应的一个加密数据。STA端匹配模块将该加密数据远程传输回AP端。

[0062] 于上述技术方案的基础上，上述AP端匹配模块与STA端匹配模块以预置的策略对上述STA端密钥和AP端密钥进行匹配，并根据匹配的结果选择STA端密钥连接AP端和STA端。

[0063] 本发明的较佳的实施例中，上述预置的策略具体为：AP端匹配模块接收到由STA端匹配模块发送的加密数据后，将该加密数据与第一存储单元中内置的包括标准加密数据的列表进行匹配。当第一存储单元保存的关于标准加密数据的列表中包括有该STA端匹配模块所发送的加密数据时，则表明AP端与STA端匹配成功，此时，AP端匹配模块即判断该STA端是合法的STA端，AP端与STA端之间根据相应的STA端密钥进行远程连接。

[0064] 在AP端与相应的STA端进行连接之后，AP端匹配模块在已经取得连接的STA端与对应的STA端密钥之间建立对应关系，并存储至第一存储单元中。也就是说，若加密数据与标准加密数据相一致，则说明该STA端密钥与AP端密钥列表中的某个AP端密钥相匹配，因此，此处的STA端密钥可以等同于相应的一个AP端密钥。上述操作可以等同于在STA端(本发明的较佳的实施例中可以以序号来表示STA端)与相应的AP端密钥之间建立对应关系。

[0065] 本发明的较佳的实施例中，第一存储单元的第一存储空间中还可以包括多个独立的第三存储块，每个独立的第三存储块中保存有一个STA端的识别信息，例如序列号等。当AP端与一个STA端成功建立连接后，该AP端中的AP端匹配模块将该STA端的识别信息写入上述第三存储块中，并将该第三存储块与保存有对应的AP端密钥的第一存储块之间建立对应关系。若该STA端需要与AP端进行再一次的远程通信，则无需重新进行密钥处理，直接采用对应的密钥建立连接即可。

[0066] 相应的，若AP端发现加密数据与标准加密数据列表匹配失败，则AP端匹配模块将连接失败的信号反馈给STA端，并退出。AP端与该STA端不建立连接。

[0067] 于上述技术方案的基础上，上述预置的第一方法、预置的第二方法、预置的策略以及其他可被选择的技术特征，均仅包括在本发明的较佳的实施例中，并非因此限制本发明的保护范围。

[0068] 于上述技术方案的基础上，上述AP端匹配模块的基本结构以及连接关系，STA端匹配模块的基本结构以及连接关系，均可以采用相应的硬件结构实现，在本发明的其他实施例中也可以采用软件形式实现上述结构之间的连接关系。本发明的较佳的实施例中所述的连接关系并非因此限制本发明的保护范围。

[0069] 如图2-5是本发明的实施例中，一种采用上述系统实现的无线接入点多密钥支持方法。

[0070] 图2为该方法的总体流程图，具体包括：

[0071] 步骤1，在AP端以预置的第一方法形成多个标准加密数据；本发明的较佳的实施例中，在AP端内设有多个预置的AP端密钥，根据该AP端密钥，以预置的第一方法形成多个相应的标准加密数据。生成标准加密数据的过程在AP端内设置的一个AP端匹配模块中进行。本发明的较佳的实施例中，该AP端匹配模块的基本结构可参照上文中所述的结构实现。

[0072] 步骤2，在每个STA端以预置的第二方法形成一个对应的加密数据；本发明的较佳的实施例中，在实行上述步骤前，希望建立连接的STA端首先会向AP端发送一个请求建立连接的请求信号，此时AP端才开始与STA端之间的认证过程。在STA端内设有一个预置的STA端密钥，根据该STA端密钥，以预置的第二方法形成一个相应的加密数据。生成加密数据的过程在STA端内设置的一个STA端匹配模块中进行。本发明的较佳的实施例中，该STA端匹配模块的基本结构可参照上文中所述的结构实现。

[0073] 步骤3，以预置的策略将加密数据与标准加密数据进行匹配；本发明的较佳的实施例中，实际在上述加密数据和标准加密数据之间进行匹配，但是由于加密数据对应于STA端密钥，标准加密数据对应于AP端密钥，因此，也可以说是对STA端密钥和AP端密钥进行匹配。本发明的较佳的实施例中，上述过程同样可以由AP端匹配模块和STA端匹配模块完成。

[0074] 步骤4，根据匹配结果，采用STA端密钥将AP端与STA端建立远程连接。本发明的较佳的实施例中，若匹配成功，则AP端与STA端之间采用STA端密钥建立连接；若匹配不成功，则AP端直接退出该连接。

[0075] 如图3所示，本发明的较佳的实施例中，上述预置的第一方法具体包括：

[0076] 步骤11，在AP端形成一个认证数据；本发明的较佳的实施例中，可以采用AP端匹配模块随机生成一个认证数据，该认证数据是可以被加密的。

[0077] 步骤12，以AP端中预置的多个AP端密钥，对认证数据进行加密，以形成多个对应的标准加密数据。本发明的较佳的实施例中，可以采用上述AP端匹配模块，从其第一存储单元中获取预置的所有AP端密钥，并以该所有AP端密钥，分别对上述认证数据进行加密，以形成对应的多个标准加密数据，每个AP端密钥对应一个标准加密数据。上述过程重复多次，直到采用所有AP端密钥对认证数据进行加密，以生成了对应所有AP端密钥的多个标准加密数据为止。AP端匹配模块将上述多个标准加密数据以列表的形式保存在第一存储单元内。

[0078] 如图4所示，本发明的较佳的实施例中，上述预置的第二方法具体包括：

[0079] 步骤21，由STA端读取认证数据；本发明的较佳的实施例中，采用STA端匹配模块，通过远程通信的方式从AP端读取上述认证数据。

[0080] 本发明的较佳的实施例中，STA端在读取认证数据之前，首先向AP端发送一个请求建立连接的请求信号；AP端收到该信号后，才会生成认证数据并将其发送至STA端。同时，AP端会向STA端发送一个响应请求的反馈信号。因此，AP端实际发送的是一个包括了上述认证数据和反馈信号的数据报文。

[0081] 步骤22，根据STA端密钥对认证数据进行加密，以形成一个对应的加密数据；本发明的较佳的实施例中，上述STA端匹配模块从其第二存储单元中获取STA端密钥，并以该STA端密钥对上述认证数据进行加密，以形成相应的一个加密数据。

[0082] 步骤23，将加密数据发送至AP端。

[0083] 如图5所示，本发明的较佳的实施例中，上述预置的策略具体包括：

[0084] 步骤41，将加密数据与多个标准加密数据进行匹配；

[0085] 若匹配成功，转至步骤42；

[0086] 若匹配失败，则向STA端发送连接失败的信号，并退出连接；

[0087] 本发明的较佳的实施例中，STA端匹配模块将加密数据发送至AP端匹配模块；AP端匹配模块根据该加密数据，在包括所有标准加密数据的列表中进行匹配；若匹配成功(即加密数据包括在标准加密数据列表中)，则判断该STA端为合法的连接用户，AP端与STA端之间采用该STA端密钥建立连接；若匹配不成功，则判断该STA端为非法的连接用户，则AP端匹配模块向STA端发送连接失败的反馈信号，同时退出连接。

[0088] 步骤42，采用STA端密钥在AP端与STA端之间建立远程连接。

[0089] 与现有技术中采用共享密钥的连接方式不同的是，本发明的较佳的实施例中，对每个合法的STA端均采用一个特定的密钥(即该STA端对应的STA端密钥)进行连接，而当加密数据与某个标准加密数据吻合时，说明该STA端密钥就存在于AP端预置的AP端密钥列表中。即：本发明的实际发明目的在于，在AP端预置一个密钥列表，并根据不同的合法的STA端来挑选不同的密钥进行连接。

[0090] 本发明的较佳的实施例中，当AP端与STA端之间成功建立连接后，AP端更新密钥与STA端之间的对应关系。一个可行的方法在于：在被使用的密钥后更新表示该被连接的STA端的属性信息(例如该STA端的序列号等)。这样当该STA端再一次请求连接时，AP端无需进行重复的认证过程即可调取相关密钥直接进行远程通信。

[0091] 于上述技术方案的基础上，上述预置的第一方法、预置的第二方法、预置的策略，以及其他可被选择的技术特征均仅包括在本发明的较佳的实施例中，并非因此限制本发明的保护范围。

[0092] 以上所述仅为本发明较佳的实施例，并非因此限制本发明的实施方式及保护范围，对于本领域技术人员而言，应当能够意识到凡运用本发明说明书及图示内容所作出的等同替换和显而易见的变化所得到的方案，均应当包含在本发明的保护范围内。

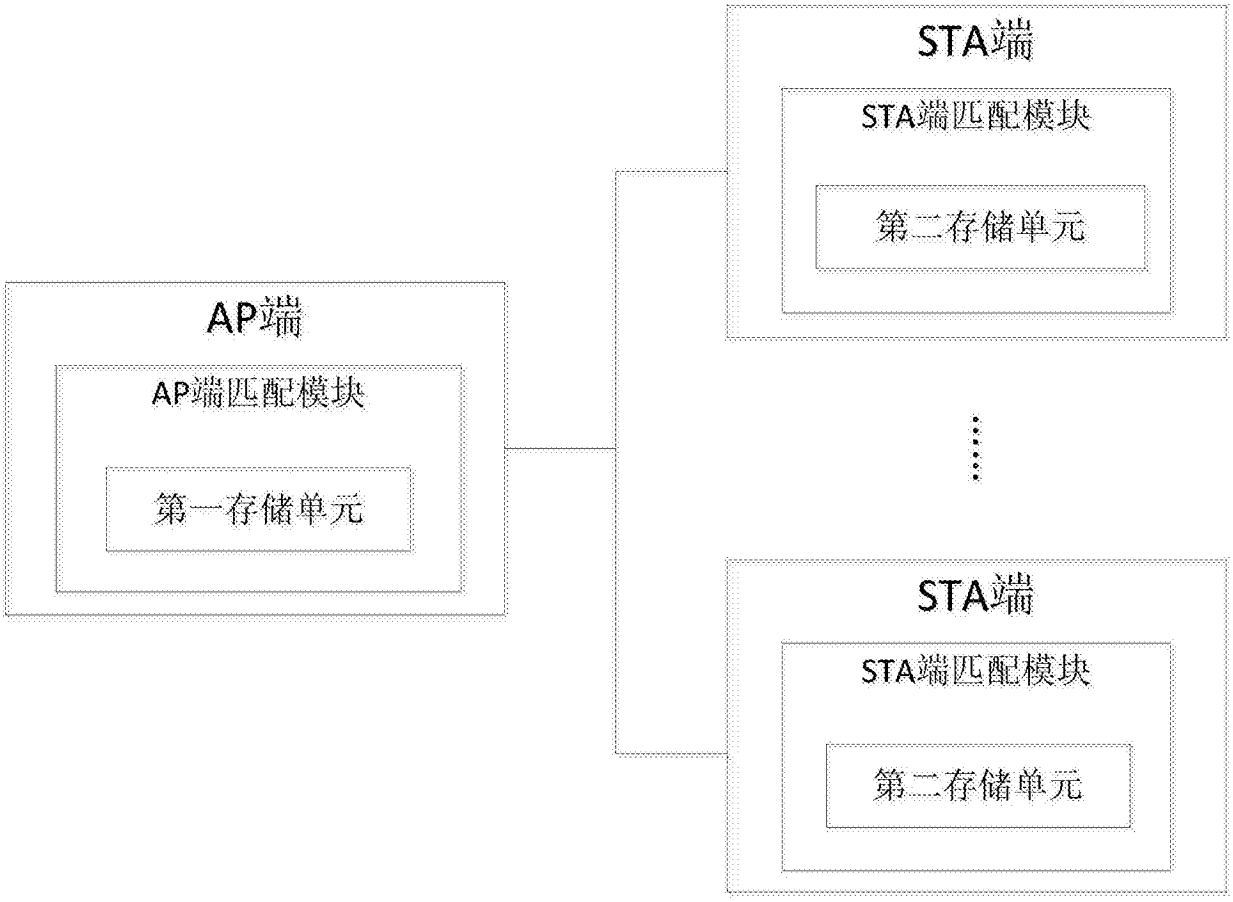

STA端
STA端匹配模块
第二存储单元
AP端
AP端匹配模块
第一存储单元
STA端
STA端匹配模块
第二存储单元

图1

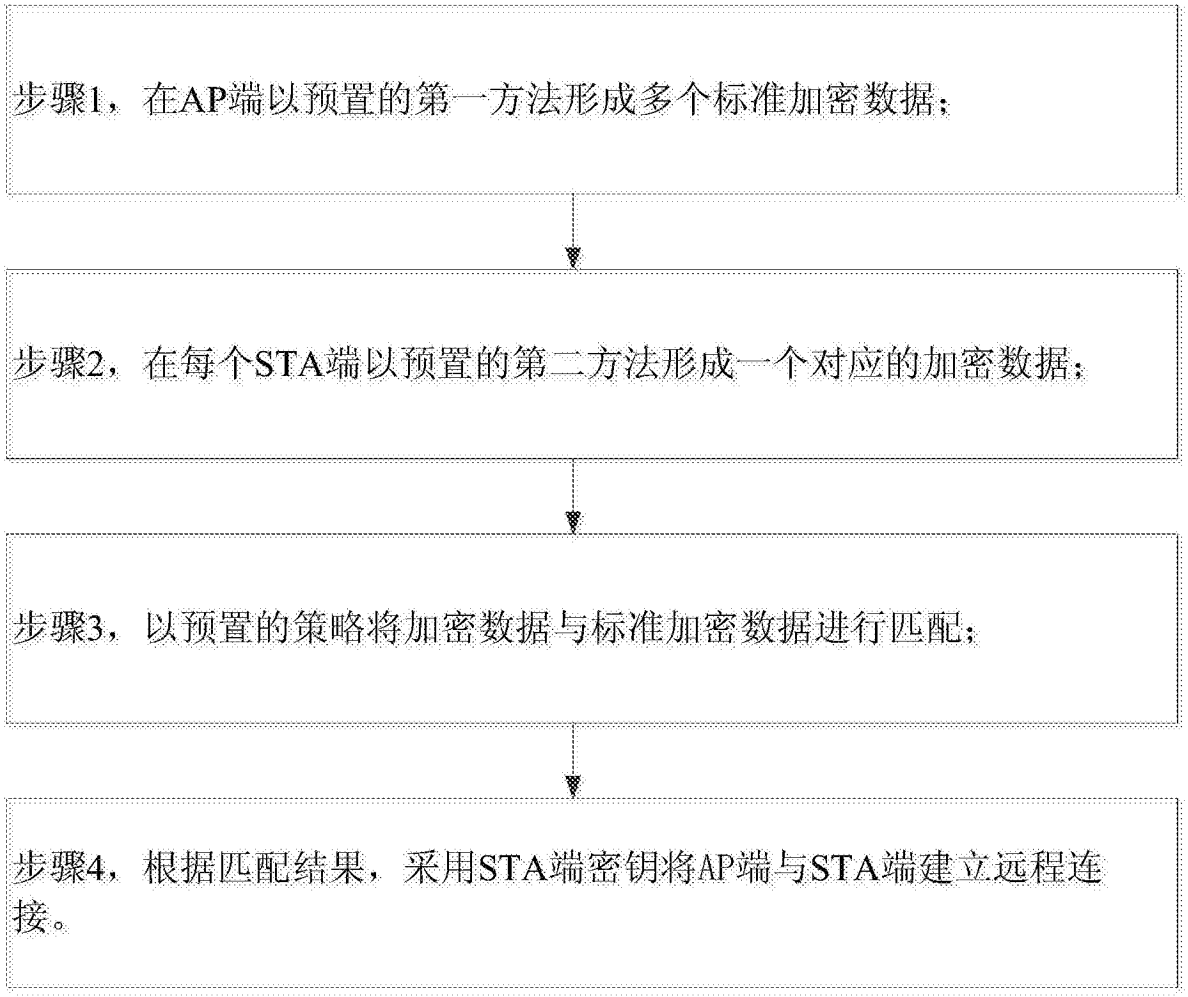

步骤1，在AP端以预置的第一方法形成多个标准加密数据；
步骤2，在每个STA端以预置的第二方法形成一个对应的加密数据；
步骤3，以预置的策略将加密数据与标准加密数据进行匹配；
步骤4，根据匹配结果，采用STA端密钥将AP端与STA端建立远程连接。

图2

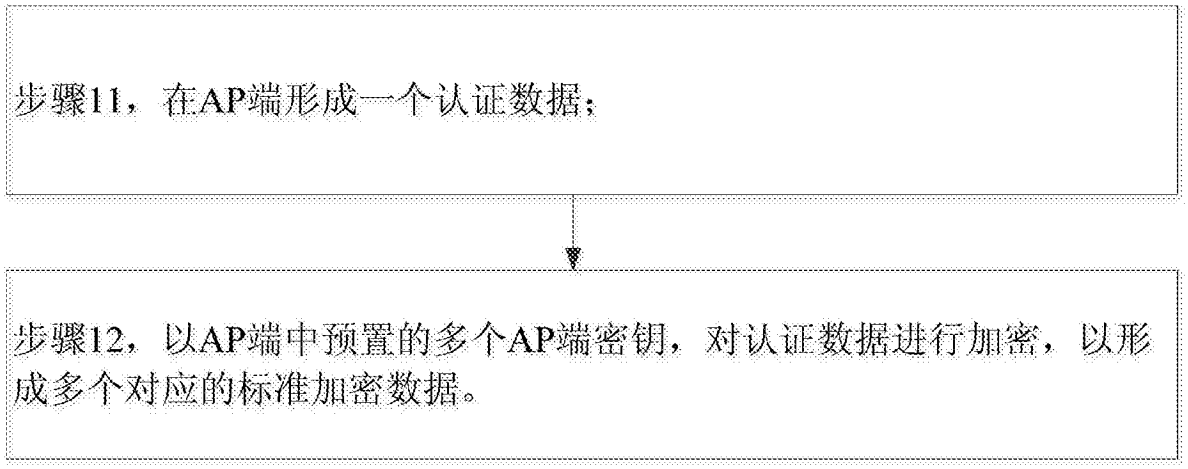

步骤11，在AP端形成一个认证数据；
步骤12，以AP端中预置的多个AP端密钥，对认证数据进行加密，以形成多个对应的标准加密数据。

图3


步骤21，由STA端读取认证数据；
步骤22，根据STA端密钥对认证数据进行加密，以形成一个对应的加密数据；
步骤23，将加密数据发送至AP端。

图4

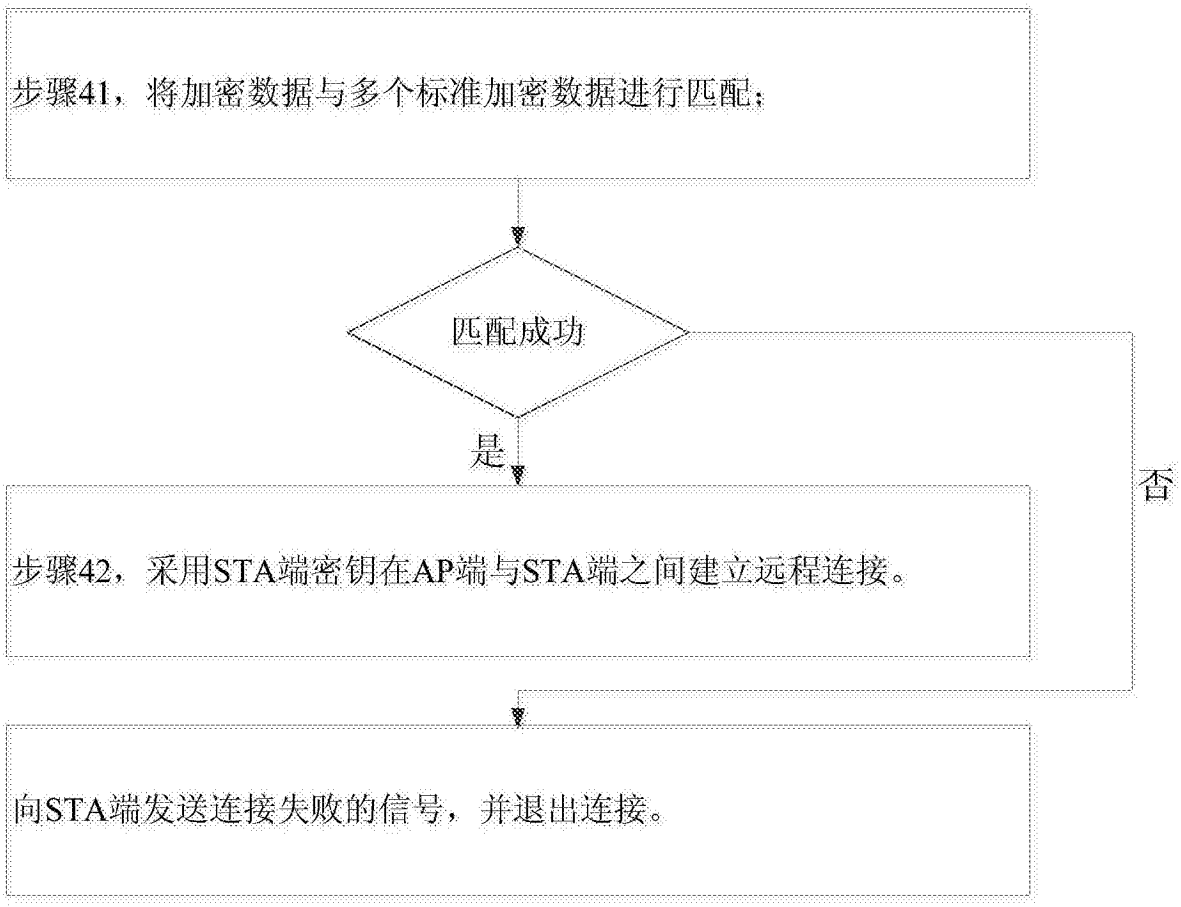

步骤41，将加密数据与多个标准加密数据进行匹配；
匹配成功
是
否
步骤42，采用STA端密钥在AP端与STA端之间建立远程连接。
向STA端发送连接失败的信号，并退出连接。

图5