

管理通信信道的方法和装置

本申请要求于 2021 年 8 月 19 日提交中国国家知识产权局、申请号为 202110957050.9、
申请名称为“管理通信信道的方法和装置”的中国专利申请的优先权，其全部内容通过引
5 用结合在本申请中。

技术领域

本说明书实施例涉及计算机技术领域，尤其涉及一种管理通信信道的方法和装置。

10 背景技术

随着无线通信的发展，越来越多的设备通过 WiFi 联入网络，实现智能化功能。WiFi
通信的开放性特点，为终端设备联入无线网络提供了便利，同时也为攻击者提供了可乘之
机。攻击者可以伪造和重放无线网络上的任意帧，给用户信息安全带来极大的威胁。举例
来说，Beacon 帧作为无线 AP (Wireless Access Point，无线接入点) 的信标帧，通常是
15 明文传输的，任何人都可以监听和伪造。当攻击者伪造 Beacon 帧中与通信信道相关的信
息并重放时，会造成对已连接 WiFi 网络的客户端的攻击。例如，客户端接收到 Beacon 帧
中畸形的通信信道相关信息后，可能因数据解析错误而导致网络连接中断或系统崩溃。又
例如，客户端接收 Beacon 帧中伪造的通信信道相关信息，会执行错误的指令去切换信道，
从而导致连接中断或者中间人攻击。

20 因此，希望能有改进的方案，能够提高 WiFi 通信的安全性。

发明内容

本说明书实施例描述了一种管理通信信道的方法和装置，在无线接入点 AP 设备端构
建携带目标信息元素的原始管理帧，目标信息元素包括与通信信道管理相关的信息元素。
25 针对连接到 AP 设备的各个客户端，将构建的原始管理帧的目标地址设置为该客户端的 MAC
地址，并采用该客户端对应的密钥对目标信息元素中的信息进行加密，得到加密管理帧。
之后，将加密管理帧进行发送。从而实现了 AP 设备和客户端之间通信信道管理相关信息
的加密传输，防止了攻击者对管理帧中携带的通信信道管理相关信息的伪造和重放，提高
了 WiFi 通信的安全性。

30 根据第一方面，提供了一种管理通信信道的方法，通过无线接入点 AP 设备执行，包

括：构建携带目标信息元素的原始管理帧，上述目标信息元素包括与通信信道管理相关的信息元素；在确定存在客户端已连接到上述 AP 设备的情况下，针对已连接客户端中的各个客户端，执行以下步骤：将上述原始管理帧的目的地址设置为该客户端的 MAC 地址；采用该客户端对应的密钥对上述目标信息元素中的信息进行加密，得到加密管理帧；将上述

5 加密管理帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

在一个实施例中，上述方法还包括：在确定没有客户端与上述 AP 设备建立连接的情况下，在 WiFi 网络中广播上述原始管理帧。

在一个实施例中，上述采用该客户端对应的密钥对上述目标信息元素中的信息进行

10 加密，包括：获取与该客户端建立连接时握手过程中生成的二者之间的专属密钥；使用上述专属密钥对上述目标信息元素中的信息进行加密。

在一个实施例中，上述目标信息元素采用标签-长度-取值的数据格式进行存储；以及上述采用该客户端对应的密钥对上述目标信息元素中的信息进行加密，包括：采用该客户端对应的密钥对上述目标信息元素中的取值进行加密。

15 在一个实施例中，上述原始管理帧包括信标帧和探测响应帧。

在一个实施例中，上述目标信息元素包括以下之一：信道切换声明元素、信道切换封装元素、宽频信道切换元素、网状网络信道切换参数元素、信道切换时间元素、最大信道切换时间元素和未来信道引导元素。

在一个实施例中，当上述原始管理帧为信标帧，上述目标信息元素为信道切换声明

20 元素时，上述方法还包括：响应于确定信道切换完成，在上述 WiFi 网络中发送目的地址为广播地址，以及不携带信道切换声明元素的信标帧。

根据第二方面，提供了一种管理通信信道的方法，通过客户端执行，包括：接收无线接入点 AP 设备发送的加密管理帧，其中携带加密后的目标信息元素，上述目标信息元素包括与通信信道管理相关的信息元素；根据上述加密管理帧的目的地址，确定是否对该

25 加密管理帧进行处理；响应于确定对该加密管理帧进行处理，使用预先存储的密钥对上述目标信息元素进行解密；根据解密结果对通信信道进行管理。

在一个实施例中，上述根据上述加密管理帧的目的地址，确定是否对该加密管理帧进行处理，包括：在上述加密管理帧的目的地址为上述客户端的 MAC 地址时，确定对该加密管理帧进行处理。

30 在一个实施例中，上述使用预先存储的密钥对上述目标信息元素进行解密，包括：

使用与上述无线接入点 AP 设备建立连接时握手过程中生成的二者之间的专属密钥，对上述目标信息元素进行解密。

在一个实施例中，上述加密管理帧为加密的信标帧，上述目标信息元素为信道切换声明元素；上述根据解密结果对通信信道进行管理，包括：根据解密后的信道切换声明元素，进行信道切换。

5 根据第三方面，提供了一种管理通信信道的装置，设置于无线接入点 AP 设备，包括：构建单元，配置为构建携带目标信息元素的原始管理帧，上述目标信息元素包括与通信信道管理相关的信息元素；执行单元，配置为在确定存在客户端已连接到上述 AP 设备的情况下，针对已连接客户端中的各个客户端，执行预设步骤，其中，上述执行单元包括：设置模块，配置为将上述原始管理帧的目的地址设置为该客户端的 MAC 地址；加密模块，配置为采用该客户端对应的密钥对上述目标信息元素中的信息进行加密，得到加密管理帧；发送模块，配置为将上述加密管理帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

15 根据第四方面，提供了一种管理通信信道的装置，设置于客户端，包括：接收单元，配置为接收无线接入点 AP 设备发送的加密管理帧，其中携带加密后目标信息元素，上述目标信息元素包括与通信信道管理相关的信息元素；确定单元，配置为根据上述加密管理帧的目的地址，确定是否对该加密管理帧进行处理；解密单元，配置为响应于确定对该加密管理帧进行处理，使用预先存储的密钥对上述目标信息元素进行解密；管理单元，配置为根据解密结果对通信信道进行管理。

20 根据第五方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当上述计算机程序被处理器执行时，实现如第一方面中任一项的上述的方法。

根据第六方面，提供了一种无线接入点 AP 设备，包括存储器和处理器，其特征在于，上述存储器中存储有可执行代码，上述处理器执行上述可执行代码时，实现如第一方面中任一项上述的方法。

25 根据第七方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当上述计算机程序在计算机中执行时，令计算机执行如第二方面中任一项的上述的方法。

根据第八方面，提供了一种终端设备，包括存储器和处理器，其特征在于，上述存储器中存储有可执行代码，上述处理器执行上述可执行代码时，实现如第二方面中任一项上述的方法。

30 根据本说明书实施例提供的管理通信信道的方法和装置，在无线接入点 AP 设备端，

首先构建携带目标信息元素的原始管理帧，目标信息元素包括与通信信道管理相关的信息元素。针对连接到 AP 设备的各个客户端，将构建的原始管理帧的目标地址设置为该客户端的 MAC 地址，并采用该客户端对应的密钥对目标信息元素中的信息进行加密，得到加密管理帧。之后，将加密管理帧进行发送。由于 AP 设备加密过程中针对不同客户端采用的

5 密钥不同，因此，客户端只能解密目的地址与自身 MAC 地址相同的管理帧中的目标信息元素的信息，而不能解密其它管理帧中的目标信息元素的信息。从而实现了 AP 设备和客户端之间通信信道管理相关信息的加密传输，防止了攻击者对管理帧中携带的通信信道管理相关信息的伪造和重放，提高了 WiFi 通信的安全性。

10 附图说明

- 图 1 为本说明书披露的一个实施例的实施场景示意图；
- 图 2 示出了根据一个实施例的管理通信信道的方法的流程示意图；
- 图 3 示出了 Beacon 帧的主要结构的示意图；
- 图 4 示出了 CSA 的格式示意图；
- 15 图 5 示出了四次握手过程的流程示意图；
- 图 6 示出了 TLV 数据格式的示意图；
- 图 7 示出了根据又一个实施例的管理通信信道的方法的流程示意图；
- 图 8 示出了根据一个实施例的管理通信信道的装置的示意性框图；
- 图 9 示出了根据又一个实施例的管理通信信道的装置的示意性框图。

20

具体实施方式

下面通过附图和实施例，对本说明书提供的技术方案做进一步的详细描述。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。需要说明的是，

25 在不冲突的情况下，本说明书的实施例及实施例中的特征可以相互组合。

图 1 为本说明书披露的一个实施例的实施场景示意图。如图 1 所示，在图 1 的实施场景中，包括无线 AP 设备 101 和多个客户端 102。当无线 AP 设备 101 需要对通信信道进行管理（例如，切换信道）的时候，为了通知所连接的客户端 102，会构建携带目标信息元素的原始管理帧，该目标信息元素包括与通信信道管理相关的信息元素。针对已连接客户端

30 端 102 中的每一个客户端 102，将所构建的原始管理帧的目的地址设置为该客户端 102 的

MAC 地址，并采用该客户端 102 对应的密钥对应目标信息元素中的信息进行加密，得到加密管理帧。由于 WiFi 网络的开放性，WiFi 网络中传输的数据帧会被网络中的所有客户端 102 接收，因此，为了防止管理帧中加密的信息被其他客户端破解，加密时不同的客户端采用不同的密钥。最后，无线 AP 设备 101 将设置地址和加密后的加密管理帧在 WiFi 网络内进行发送。WiFi 网络内的客户端 102 接收到该加密管理帧之后，会判断该加密管理帧的目的地址是否与自身的 MAC 地址相同。如果相同，则使用预存的密钥对该加密管理帧的目标信息元素进行解密、解析等处理，最终得到通信信道管理相关信息，并根据得到的通信信道管理相关信息对通信信道进行管理。由此，实现了 AP 设备 101 和客户端 102 之间通信信道管理相关信息的加密传输，防止了攻击者对管理帧中携带的通信信道管理相关信息的伪造和重放，提高了 WiFi 通信的安全性。下面描述以上过程的具体执行方式。

图 2 示出了根据一个实施例的管理通信信道的方法。该方法可以通过无线接入点 AP 设备执行。举例来说，AP 设备可以包括无线路由器。如图 2 所示，管理通信信道的方法可以包括以下步骤：

步骤 201，构建携带目标信息元素的原始管理帧。

在本实施例中，AP 设备可以构建携带目标信息元素的管理帧，作为原始管理帧。这里，目标信息元素可以包括与通信信道管理相关的信息元素。

在一个实施例中，上述原始管理帧可以包括信标帧（Beacon 帧）和探测响应帧。

通常，无线客户端可以通过被动扫描和主动扫描的方式获取周围的无线网络信息。被动扫描是指客户端通过监听 AP 设备定期发送的 Beacon 帧获取无线网络信息。主动扫描是指客户端主动发送探测请求帧（Probe Request 帧），通过 AP 设备针对探测请求帧发回的探测响应帧（Probe Response）获取网络信号。

Beacon 帧是基于 IEEE 802.11 的无线局域网中的管理帧之一，它包含了网络的描述信息。Beacon 帧由基础设施基本服务集(Basic Service Set, BSS)中的无线接入点(AP)设备周期性地传送。Beacon 帧用于宣布无线局域网的存在，并使基本服务集的成员同步。图 3 示出了 Beacon 帧的主要结构的示意图。可以理解，图中方框上面的数字可以表示信息所占的空间，单位为八位组（octet），octets 为 octet 的复数形式。如图 3 所示，Beacon 信标帧包括 802.11 MAC Header（MAC 头）、可变（variable）长的帧主体（Frame Body）和帧检验序列（FCS）。作为示例，MAC 头可以包括以下内容：帧控制(Frame Control)、持续时间/ID (Duration/ID)、地址信息 (Address)、顺序控制 (Sequence Control)、服务质量控制 (QoS Control)、HT (High-throughput, 高吞吐量) 控制 (HT Control)

等等。Beacon 帧的帧主体部分可以包括固定长度字段和多个信息元素。其中，固定长度字段可以包括时间戳 (Timestamp)、信标间隔 (Beacon interval)、性能信息 (Capability information) 等。

与 Beacon 帧的结构相似，探测响应帧的帧主体部分也可以包括固定长度字段和多个信息元素。

在一个实施例中，上述目标信息元素可以包括以下之一：信道切换声明 (Channel Switch Announcement, CSA) 元素、信道切换封装 (Channel Switch Wrapper) 元素、宽频信道切换元素 (Wide Bandwidth Channel Switch) 元素、网状网络信道切换参数 (Mesh Channel Switch Parameters) 元素、信道切换时间 (Channel Switch Timing) 元素、最大信道切换时间 (Max Channel Switch Time) 元素和未来信道引导 (Future Channel Guidance) 元素。上述目标信息元素可以与通信信道管理相关。举例来说，AP 为了警告 WiFi 网络中的客户端即将变换信道，可以在管理帧 (例如，Beacon 帧、探测响应帧等) 中加入对应的 CSA 字段，来通知客户端即将切往的信道，以便让客户端及时切换到新的信道。图 4 示出了 CSA 的格式示意图，如图 4 所示 CSA 包括元素标识 (Element ID)、长度 (Length)、信道切换模式 (Channel Switch Mode)、新信道编号 (New Channel Number)、信道切换计时 (Channel Switch Count)。可以理解，上述目标信息元素的功能和格式在 WiFi 无线网络 802.11 技术标准中有详细的描述和记载，此处不再赘述。根据实际需要，上述目标信息元素都可以在 Beacon 帧和探测响应帧中出现。

作为示例，构建携带目标信息元素的管理帧，可以是指在管理帧的帧主体中写入目标信息元素，从而得到携带目标信息元素的管理帧。

步骤 202，在确定存在客户端已连接到 AP 设备的情况下，针对已连接客户端中的各个客户端，执行以下步骤 2021-2023。具体地：

步骤 2021，将原始管理帧的目的地址设置为该客户端的 MAC 地址。

在本实施例中，针对已经连接到 AP 设备的每一个客户端，AP 设备可以将上述携带目标信息元素的原始管理帧的目的地址设置为该客户端的 MAC 地址。

步骤 2022，采用该客户端对应的密钥对目标信息元素中的信息进行加密，得到加密管理帧。

在本实施例中，与 AP 设备连接的每一个客户端与 AP 设备之间都可以预先交换或协商一组密钥。举例来说，该密钥可以是对称密钥，也可以是非对称密钥。为了防止管理帧中加密的信息被破解，不同的客户端所对应的密钥不同。

在一个实施例中，步骤 2022 还可以具体如下实现：首先，将与该客户端建立连接时握手过程中生成的二者之间的专属密钥确定为该客户端对应的密钥。然后，使用该专属密钥对目标信息元素中的信息进行加密。

5 一般，AP 设备与客户端建立连接时，会通过握手过程交换密钥，该过程成功后会产生一个 AP 设备和客户端之间通信的密钥，用于加密通信数据。以四次握手过程为例，图 5 示出了四次握手过程的流程示意图，如图 5 所示，具体过程包括：

第一次握手，AP 设备生成随机数 ANonce，并将 ANonce、服务集标识 (Service Set Identifier, SSID) 和自身的 MAC 地址等信息，发送给客户端。客户端接收到后，可以计算出 PTK (pairwise transient key, 成对临时密钥)。其中，PTK 可以通过以下公式 (1)

10 计算：

$$PTK=HMAC(PMK+ANonce+SNonce+MAC_A+MAC_S) \quad (1)$$

其中，HMAC 表示 HMAC 算法，SNonce 是客户端生成的随机数，MAC_A表示 AP 设备的 MAC 地址，MAC_S表示客户端的 MAC 地址。这里，PMK跟认证方式有关，如果是 PSK(pre-shared key, 预共享密钥模式) 认证方式，则 PMK 通过以下公式 (2) 计算：

15
$$PMK=PBKDF2(Passphrase, SSID) \quad (2)$$

其中，PBKDF2 表示 PBKDF2 算法，Passphrase 表示用户输入的登录密码。

第二次握手，客户端将 SNonce、自身的 MAC 地址、MIC (Message Integrity code, 消息完整性代码) 等信息发送给 AP 设备。AP 设备接收之后，同样利用公式 (1) 计算 PTK 的值。

20 第三次握手，AP 设备将携带 GTK (Group Transient Key, 组临时密钥) 和 MIC 的消息发送给客户端。其中，GTK 使用 KEK (key Encryption key, 密钥加密密钥) 加密，KEK 用来加密密钥生成消息。MIC 使用 KCK (key confirmation key, 密钥确认密钥) 加密，MIC 用来计算密钥生成消息的完整性。客户端接收到上述消息后，会进行 MIC 的校验，如果校验成功，客户端就获取到了 GTK。

25 第四次握手，客户端向 AP 设备发送用于确认的消息，AP 设备对该消息认证成功，双方安装 PTK、GTK。可以理解，本说明书仅仅是对四次握手过程的简要描述，实际握手过程中的计算更加复杂，此处不再赘述。

在本实施例中，AP 设备可以将与该客户端四次握手过程中生成的 PTK 确定为该客户端对应的密钥，并使用 PTK 对目标信息元素中的信息进行加密。相对于多个客户端共享的 GTK，

30 PTK 是 AP 设备与单个客户端之间协商出来的专属密钥，各个客户端与 AP 协商出不同的专

属密钥。本实现方式，可以复用握手过程中生成的专属密钥对信息进行加密，而不需要再额外交换或协商密钥，从而简化了密钥确定步骤，提高了效率。

在一个实施例中，上述目标信息元素可以采用标签-长度-取值，即，TLV(Tag、Length、Value)，的数据格式进行存储。图 6 示出了 TLV 数据格式的示意图，如图 6 所示，以 TLV 数据格式表示的目标信息元素包括元素标识 (Element ID)、长度 (Length) 和信息 (Information)。其中，元素标识、长度和信息分别对应 TLV 数据格式中的标签、长度和取值。

基于目标信息元素的这种数据格式，步骤 2022 还可以具体如下实现：采用该客户端对应的密钥对目标信息元素中的取值进行加密。以目标信息元素为 CSA 为例，只需对信道切换模式、新信道编号、信道切换计时进行加密。本实现方式，只对目标信息元素中的取值进行加密，而不需要对目标信息元素中的所有信息都进行加密，从而在保证取值不泄露的同时，减少了加密、解密过程中的数据计算量，提高了效率。

步骤 2023，将设置地址和加密处理后得到的加密管理帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

在本实施例中，AP 设备可以将设置地址和加密处理后得到的加密管理帧在 WiFi 网络内进行发送。由于 WiFi 网络的开放性，WiFi 网络内的客户端都可以接收到该加密管理帧。WiFi 网络内的已连接客户端可以根据加密管理帧的目的地址判断是否对接收到的加密管理帧进行处理。具体的，客户端可以判断加密管理帧的目的地址是否和自身的 MAC 地址相同，如果相同，则对管理帧执行解密、解析等操作，并根据解密、解析得到的通信信道管理相关信息对信道进行管理。例如，当目标信息元素为信道切换声明元素时，可以根据解密、解析得到的信道切换声明进行信道切换。

在一个实施例中，上述管理通信信道的方法，还可以包括图 2 中未示出的以下步骤：在确定没有客户端与 AP 设备建立连接的情况下，在 WiFi 网络中广播原始管理帧。

在本实施例中，如果没有客户端与 AP 设备建立连接，则 AP 设备可以将构建的原始管理帧（例如，信标帧）的目的地址设置为广播地址，在 WiFi 网络中广播该原始管理帧，该原始管理帧携带原始的不加密的目标信息元素。以信标帧为例，在没有客户端与 AP 设备连接的情况下，发送的信标帧可以是不加密的信标帧。

在一个实施例中，当上述原始管理帧为信标帧，上述目标信息元素为信道切换声明元素时，上述管理通信信道的方法，还可以包括图 2 中示出的以下步骤：响应于确定信道切换完成，在 WiFi 网络中发送目的地址为广播地址，以及不携带信道切换声明元素的信标

帧。

在本实施例中，根据信道切换声明元素中信息，AP 设备和客户端的信道切换完成后，AP 设备将继续在 WiFi 网络中发送目的地址为广播地址，且不携带信道切换声明元素的信标帧，以宣布无线局域网的存在。

- 5 图 7 示出了根据一个实施例的管理通信信道的方法的流程示意图。该方法可以通过客户端执行。这里，客户端可以是指能够与 WiFi 网络建立连接的各种设备，包括但不限于智能手机、平板电脑、电子书阅读器、笔记本电脑等等。如图 7 所示，该管理通信信道的方法可以包括以下步骤：

- 10 步骤 701，接收无线接入点 AP 设备发送的加密管理帧，其中携带加密后的目标信息元素。

- 在本实施例中，客户端可以接收所连接的无线接入点 AP 设备发送的、携带加密后目标信息元素的管理帧。这里，管理帧可以包括信标帧（Beacon 帧）和探测响应帧。上述目标信息元素可以包括与通信信道管理相关的信息元素。例如，目标信息元素可以包括以下之一：信道切换声明（Channel Switch Announcement, CSA）元素、信道切换声明（Channel Switch Announcement, CSA）元素、信道切换封装（Channel Switch Wrapper）元素、宽频信道切换元素（Wide Bandwidth Channel Switch）元素、网状网络信道切换参数（Mesh Channel Switch Parameters）元素、信道切换时间（Channel Switch Timing）元素、最大信道切换时间（Max Channel Switch Time）元素和未来信道引导（Future Channel Guidance）元素。上述目标信息元素位于管理帧的帧主体部分。

- 20 步骤 702，根据所接收的加密管理帧的目的地址，确定是否对该加密管理帧进行处理。

- 在本实施例中，针对已经连接到 AP 设备的每一个客户端，AP 设备可以将携带加密后目标信息元素的加密管理帧的目的地址设置为该客户端的 MAC 地址。这样，WiFi 网络内的客户端可以根据所接收的加密管理帧的目的地址，确定接收到的加密管理帧是否是 AP 设备针对自己发送的，如果是，则对该加密管理帧进行处理。具体的，客户端可以判断接收
- 25 的加密管理帧的目的地址是否与自己的 MAC 地址相同，如果相同，则确定该管理帧是 AP 设备针对自己发送的，从而确定对该加密管理帧进行处理。

步骤 703，响应于确定对上述加密管理帧进行处理，使用预先存储的密钥对目标信息元素进行解密。

- 在本实施例中，与 AP 设备连接的每一个客户端与 AP 设备之间都可以预先交换或协商
- 30 一组密钥。举例来说，该密钥可以是对称密钥，也可以是非对称密钥。为了防止管理帧中

加密的信息被破解，不同的客户端所对应的密钥不同。这样，如果客户端确定对接收的管理帧进行处理，则使用预先存储的、与 AP 设备交换或协商的密钥对目标信息元素进行解密。可以理解，对目标信息元素进行解密之后，客户端还可以按照目前常规的解析管理帧的方式对管理帧进行解析。

- 5 在一个实施例中，上述使用预先存储的密钥对目标信息元素进行解密，可以具体如下进行：使用与无线接入点 AP 设备建立连接时握手过程中生成的二者之间的专属密钥，对目标信息元素进行解密。

一般，AP 设备与客户端建立连接时，会通过握手过程交换密钥，该过程成功后会产生一个 AP 设备和客户端之间通信的密钥，用于加密通信数据。以四次握手过程为例，由结合图 5 的描述可知，四次握手过程中会产生 PTK (pairwise transient key, 成对临时秘钥)，作为 AP 设备与单个客户端之间的专属秘钥。

在本实施例中，客户端可以使用与 AP 设备建立连接时四次握手过程中生成的 PTK，对目标信息元素进行解密。本实现方式，可以复用握手过程中生成的密钥对信息进行加密，而不需要再额外交换或协商密钥，从而简化了密钥确定步骤，提高了效率。

- 15 步骤 704，根据解密结果对通信信道进行管理。

在本实施例中，客户端根据对目标信息元素的解密结果，以及对管理帧的解析结果，对信道信息进行管理。例如，当加密管理帧为加密的信标帧，目标信息元素为信道切换声明元素时，可以根据解密、解析得到的信道切换声明进行信道切换。

本申请的上述实施例提供的管理通信信道的方法，实现了 AP 设备和客户端之间通信信道管理相关信息的加密传输，防止了攻击者对管理帧中携带的通信信道管理相关信息的伪造和重放，提高了 WiFi 通信的安全性。

根据另一方面的实施例，提供了一种管理通信信道的装置。上述管理通信信道的装置可以设置于无线接入点 AP 设备中。

图 8 示出了根据一个实施例的管理通信信道的装置的示意性框图。如图 8 所示，该管理通信信道的装置 800 包括：构建单元 801，配置为构建携带目标信息元素的原始管理帧，上述目标信息元素包括与通信信道管理相关的信息元素；执行单元 802，配置为在确定存在客户端已连接到上述 AP 设备的情况下，针对已连接客户端中的各个客户端，执行预设步骤，其中，上述执行单元 802 包括：设置模块 8021，配置为将上述原始管理帧的地址设置为该客户端的 MAC 地址；加密模块 8022，配置为采用该客户端对应的密钥对上述目标信息元素中的信息进行加密，得到加密管理帧；发送模块 8023，配置为将加密管理

帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

在本实施例的一些可选的实现方式中，装置 800 还包括：广播单元（图中未示出），配置为在确定没有客户端与上述 AP 设备建立连接的情况下，在 WiFi 网络中广播上述原始管理帧。

在本实施例的一些可选的实现方式中，上述加密模块 8022 进一步配置为：获取与该客户端建立连接时握手过程中生成的二者之间的专属密钥；使用上述专属密钥对上述目标信息元素中的信息进行加密。

在本实施例的一些可选的实现方式中，上述目标信息元素采用标签-长度-取值的数
10 据格式进行存储；以及上述加密模块 8022 进一步配置为：采用该客户端对应的密钥对上述目标信息元素中的取值进行加密。

在本实施例的一些可选的实现方式中，上述原始管理帧包括信标帧和探测响应帧。

在本实施例的一些可选的实现方式中，上述目标信息元素包括以下之一：信道切换声明元素、信道切换封装元素、宽频信道切换元素、网状网络信道切换参数元素、信道切
15 换时间元素、最大信道切换时间元素和未来信道引导元素。

在本实施例的一些可选的实现方式中，上述装置 800 还包括：信标帧发送单元（图中未示出），配置为响应于确定信道切换完成，在上述 WiFi 网络中发送目的地址为广播地址，以及不携带信道切换声明元素的信标帧。

根据另一方面的实施例，提供了一种管理通信信道的装置。上述管理通信信道的装
20 置可以设置于客户端。

图 9 示出了根据又一个实施例的管理通信信道的装置的示意性框图。如图 9 所示，该管理通信信道的装置 900 包括：接收单元 901，配置为接收无线接入点 AP 设备发送的加密管理帧，其中携带加密后的目标信息元素，上述目标信息元素包括与通信信道管理相关的信息元素；确定单元 902，配置为根据上述加密管理帧的目的地址，确定是否对该加密
25 管理帧进行处理；解密单元 903，配置为响应于确定对该加密管理帧进行处理，使用预先存储的密钥对上述目标信息元素进行解密；管理单元 904，配置为根据解密结果对通信信道进行管理。

在本实施例的一些可选的实现方式中，上述确定单元 902 进一步配置为：在上述加密管理帧的目的地址为上述客户端的 MAC 地址时，确定对该加密管理帧进行处理。

30 在本实施例的一些可选的实现方式中，上述解密单元 903 进一步配置为：使用与上

述无线接入点 AP 建立连接时握手过程中生成的二者之间的专属密钥，对上述目标信息元素进行解密。

在本实施例的一些可选的实现方式中，上述管理单元 904 进一步配置为：根据解密后的信道切换声明元素，进行信道切换。

- 5 根据另一方面的实施例，还提供了一种计算机可读存储介质，其上存储有计算机程序，当上述计算机程序被处理器执行时，实现如图 2 所描述的方法。

根据再一方面的实施例，还提供了一种无线接入点 AP 设备，包括存储器和处理器，其特征在于，上述存储器中存储有可执行代码，上述处理器执行上述可执行代码时，实现如图 2 所描述的方法。

- 10 根据另一方面的实施例，还提供了一种计算机可读存储介质，其上存储有计算机程序，当上述计算机程序在计算机中执行时，令计算机执行如图 7 所描述的方法。

根据再一方面的实施例，还提供了一种终端设备，包括存储器和处理器，其特征在于，上述存储器中存储有可执行代码，上述处理器执行上述可执行代码时，实现如图 7 所描述的方法。

- 15 本领域普通技术人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执轨道，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执轨道的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

- 25 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、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

1. 一种管理通信信道的方法，通过无线接入点 AP 设备执行，包括：

构建携带目标信息元素的原始管理帧，所述目标信息元素包括与通信信道管理相关的信息元素；

在确定存在客户端已连接到所述 AP 设备的情况下，针对已连接客户端中的各个客户端，执行以下步骤：

将所述原始管理帧的目的地址设置为该客户端的 MAC 地址；

采用该客户端对应的密钥对所述目标信息元素中的信息进行加密，得到加密管理帧；

将所述加密管理帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

2. 根据权利要求 1 所述的方法，其中，所述方法还包括：

在确定没有客户端与所述 AP 设备建立连接的情况下，在 WIFI 网络中广播所述原始管理帧。

3. 根据权利要求 1 所述的方法，其中，所述采用该客户端对应的密钥对所述目标信息元素中的信息进行加密，包括：

获取与该客户端建立连接时握手过程中生成的二者之间的专属密钥；

使用所述专属密钥对所述目标信息元素中的信息进行加密。

4. 根据权利要求 1 所述的方法，其中，所述目标信息元素采用标签-长度-取值的数据格式进行存储；以及

所述采用该客户端对应的密钥对所述目标信息元素中的信息进行加密，包括：

采用该客户端对应的密钥对所述目标信息元素中的取值进行加密。

5. 根据权利要求 1 所述的方法，其中，所述原始管理帧包括信标帧和探测响应帧。

6. 根据权利要求 5 所述的方法，其中，所述目标信息元素包括以下之一：信道切换声明元素、信道切换封装元素、宽频信道切换元素、网状网络信道切换参数元素、信道切换时间元素、最大信道切换时间元素和未来信道引导元素。

7. 根据权利要求 6 所述的方法, 其中, 当所述原始管理帧为信标帧, 所述目标信息元素为信道切换声明元素时, 所述方法还包括:

响应于确定信道切换完成, 在所述 WiFi 网络中发送目的地址为广播地址, 以及不携带信道切换声明元素的信标帧。

8. 一种管理通信信道的方法, 通过客户端执行, 包括:

接收无线接入点 AP 设备发送的加密管理帧, 其中携带加密后的目标信息元素, 所述目标信息元素包括与通信信道管理相关的信息元素;

根据所述加密管理帧的目的地址, 确定是否对该加密管理帧进行处理;

响应于确定对该加密管理帧进行处理, 使用预先存储的密钥对所述目标信息元素进行解密;

根据解密结果对通信信道进行管理。

9. 根据权利要求 8 所述的方法, 其中, 所述根据所述加密管理帧的目的地址, 确定是否对该加密管理帧进行处理, 包括:

在所述加密管理帧的目的地址为所述客户端的 MAC 地址时, 确定对该加密管理帧进行处理。

10. 根据权利要求 8 所述的方法, 其中, 所述使用预先存储的密钥对所述目标信息元素进行解密, 包括:

使用与所述无线接入点 AP 设备建立连接时握手过程中生成的二者之间的专属密钥, 对所述目标信息元素进行解密。

11. 根据权利要求 8 所述的方法, 其中, 所述加密管理帧为加密的信标帧, 所述目标信息元素为信道切换声明元素;

所述根据解密结果对通信信道进行管理, 包括:

根据解密后的信道切换声明元素, 进行信道切换。

12. 一种管理通信信道的装置, 设置于无线接入点 AP 设备, 包括:

构建单元，配置为构建携带目标信息元素的原始管理帧，所述目标信息元素包括与通信信道管理相关的信息元素；

执行单元，配置为在确定存在客户端已连接到所述 AP 设备的情况下，针对已连接客户端中的各个客户端，执行预设步骤，其中，所述执行单元包括：

设置模块，配置为将所述原始管理帧的目的地址设置为该客户端的 MAC 地址；

加密模块，配置为采用该客户端对应的密钥对所述目标信息元素中的信息进行加密，得到加密管理帧；

发送模块，配置为将所述加密管理帧在 WiFi 网络内进行发送，以供 WiFi 网络内的已连接客户端根据目的地址确定是否对接收到的管理帧进行处理。

13. 一种管理通信信道的装置，设置于客户端，包括：

接收单元，配置为接收无线接入点 AP 设备发送的加密管理帧，其中携带加密后目标信息元素，所述目标信息元素包括与通信信道管理相关的信息元素；

确定单元，配置为根据所述加密管理帧的目的地址，确定是否对该加密管理帧进行处理；

解密单元，配置为响应于确定对该加密管理帧进行处理，使用预先存储的密钥对所述目标信息元素进行解密；

管理单元，配置为根据解密结果对通信信道进行管理。

14. 一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序被处理器执行时，实现如权利要求 1-7 中任一项的所述的方法。

15. 一种无线接入点 AP 设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-7 中任一项所述的方法。

16. 一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 8-11 中任一项的所述的方法。

17. 一种终端设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行

代码，所述处理器执行所述可执行代码时，实现权利要求 8-11 中任一项所述的方法。