(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107094293 A
(43)申请公布日 2017.08.25

(21)申请号 201710497610.0

(22)申请日 2017.06.27

(71)申请人 南京赢纳信息科技有限公司
地址 210017 江苏省南京市建邺区嘉陵江东街18号04栋810

(72)发明人 李新 李征宇

(74)专利代理机构 北京恒泰铭睿知识产权代理有限公司 11642
代理人 胡艳

(51)Int.Cl.
H04W 8/26(2009.01)
H04W 12/06(2009.01)
H04L 29/12(2006.01)
H04W 48/14(2009.01)

权利要求书1页 说明书3页 附图1页

(54)发明名称

一种获取WiFi终端真实MAC地址的装置及方法

(57)摘要

本发明公开一种获取WiFi终端真实MAC地址的装置及方法，所述装置包括WiFi终端和MAC地址获取装置。本发明对于在WiFi网络扫描阶段采用随机MAC地址的WiFi终端，MAC地址获取装置从收集到的Probe request消息中提取到源MAC地址，并对源MAC地址类型进行辨别，若源MAC地址不是WiFi终端的真实MAC地址，则引导WiFi终端向MAC地址获取装置发起802.11关联流程，从WiFi终端发送的Association request消息中提取WiFi终端的真实MAC地址，保存获取的地址并上报给相关应用程序。本发明提出的方法可以自动切换成更简单更快速的获取方法。

CN 107094293 A

1.一种获取WiFi终端真实MAC地址的装置，包括WiFi终端和MAC地址获取装置，所述WiFi终端为各种用户设备，包括手机、平板电脑、笔记本电脑，其特征在于：所述MAC地址获取装置包括终端探测模块、决策模块、无线控制模块和存储通信模块，所述终端探测模块负责监听抓取WiFi空口中的各类数据包并对其进行解析；所述决策模块根据终端探测模块对监听到的数据包的分析结果进行判断和决策，并向其它模块发出执行指令；所述无线控制模块根据终端探测模块或决策模块的指令，执行无线扫描和WiFi网络连接协商等流程；所述存储通信模块根据决策模块的指令，对收集到的WiFi终端MAC地址进行保存或者传送。

2.根据权利要求1所述的一种获取WiFi终端真实MAC地址的装置，其特征在于：各模块之间采用本地进程间通信方式进行信息传递。

3.一种获取WiFi终端真实MAC地址的方法，其特征在于：包括如下步骤：

步骤一：当WiFi终端进入MAC地址获取装置覆盖范围内时，由于WiFi终端会通过周期性发送Probe request信息的方式对周围的WiFi网络进行探测，位于MAC地址获取位置中的终端探测模块收集到该WiFi终端发出的Probe request消息。

4.步骤二：MAC地址获取装置从收集到的Probe request消息中提取到源MAC地址，并对源MAC地址类型进行辨别，若源MAC地址不是本地管理(locally administered)类型地址，则该源MAC地址即为WiFi终端真实MAC地址，跳转到步骤(八)。

5.步骤三：MAC地址获取装置对WiFi终端回应Probe response消息，其中包含约定的SSID名称和认证方式。

6.步骤四：WiFi终端向MAC地址获取装置发起认证流程，双方按约定的Open或者WPA2认证方式完成认证过程。

7.步骤五：WiFi终端向MAC地址获取装置发起802.11关联流程，在WiFi终端发出的Association request消息中，WiFi终端会包含真实的MAC地址。

8.步骤六：MAC地址获取装置向WiFi终端响应Association response消息，其中该消息中的状态码status code置为非0值，以拒绝WiFi终端的关联请求。

9.步骤七：MAC地址获取装置从WiFi终端发送的Association request消息中提取WiFi终端的真实MAC地址。

10.步骤八：保存获取的WiFi终端MAC地址并上报给相关应用程序。

11.根据权利要求3所述的一种获取WiFi终端真实MAC地址的方法，其特征在于：步骤三中约定的SSID名称和认证方式的获取可以是读取本地配置文件，或者是通过网络接口从外部服务器或者云平台查询得到。

12.根据权利要求3所述的一种获取WiFi终端真实MAC地址的方法，其特征在于：步骤二中对于源MAC地址是否为合法的本地地址的判定，MAC地址获取装置还可以执行更为严格的规则，例如通过提取MAC地址的组织统一标识符OUI: Organizationally Unique Identifier查询对应的厂商信息进行有效性判别。

一种获取WiFi终端真实MAC地址的装置及方法

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及一种获取WiFi终端真实MAC地址的装置及方法。

背景技术

[0002] WiFi已日益成为各种移动智能终端的主要联网方式，随着WiFi网络的广泛部署，人们对WiFi网络泄露个人隐私的担忧日益加深。例如，利用WiFi探针设备侦听WiFi终端周期性发出的Probe request帧，就可以从中提取出WiFi终端的MAC地址，从而可以对使用该WiFi终端的用户进行追踪。

[0003] 为了解决这种隐私泄露问题，各种WiFi设备在新版本的操作系统(例如Apple iOS 8，Google Android 6.0)中引入了随机MAC地址机制，这些终端在主动扫描阶段发送的Probe request帧中使用虚拟的MAC地址，并且这种虚拟地址会经常变化，这样就可以避免探针设备通过侦听Probe request帧的方法对用户终端进行追踪。

[0004] 采用虚拟MAC地址的方法虽然解决了隐私泄露的问题，但是对一些需要在非联网状态获取WiFi设备标识的应用带来了问题。

发明内容

[0005] 针对上述问题，本发明提供了一种获取WiFi终端真实MAC地址的装置及方法，其目的在于：随时获取WiFi终端的真实MAC地址以实现对人员或者物品的追踪和定位。

[0006] 本发明的技术解决方案：

一种获取WiFi终端真实MAC地址的装置，包括WiFi终端和MAC地址获取装置，所述WiFi终端为各种用户设备，包括手机、平板电脑、笔记本电脑，其特征在于：所述MAC地址获取装置包括终端探测模块、决策模块、无线控制模块和存储通信模块，各模块之间采用本地进程间通信方式进行信息传递，所述终端探测模块负责监听抓取WiFi空口中的各类数据包并对其进行解析；所述决策模块根据终端探测模块对监听到的数据包的分析结果进行判断和决策，并向其它模块发出执行指令；所述无线控制模块根据终端探测模块或决策模块的指令，执行无线扫描和WiFi网络连接协商等流程；所述存储通信模块根据决策模块的指令，对收集到的WiFi终端MAC地址进行保存或者传送。

[0007] 一种获取WiFi终端真实MAC地址的方法：

步骤一：当WiFi终端进入MAC地址获取装置覆盖范围内时，由于WiFi终端会通过周期性发送Probe request信息的方式对周围的WiFi网络进行探测，位于MAC地址获取位置中的终端探测模块收集到该WiFi终端发出的Probe request消息。

[0008] 步骤二：MAC地址获取装置从收集到的Probe request消息中提取到源MAC地址，并对源MAC地址类型进行辨别，若源MAC地址不是本地管理(locally administered)类型地址，则该源MAC地址即为WiFi终端真实MAC地址，跳转到步骤(八)。进一步地，对于源MAC地址是否为合法的本地地址的判定，MAC地址获取装置还可以执行更为严格的规则，例如通过提

取MAC地址的组织统一标识符(OUI: Organizationally Unique Identifier)查询对应的厂商信息进行有效性判别。

[0009] 步骤三:MAC地址获取装置对WiFi终端回应Probe response消息,其中包含约定的SSID名称和认证方式,约定的SSID名称和认证方式的获取可以是读取本地配置文件,或者是通过网络接口从外部服务器或者云平台查询得到。

[0010] 步骤四:WiFi终端向MAC地址获取装置发起认证流程,双方按约定的Open或者WPA2认证方式完成认证过程。

[0011] 步骤五:WiFi终端向MAC地址获取装置发起802.11关联流程,在WiFi终端发出的Association request消息中,WiFi终端会包含真实的MAC地址。

[0012] 步骤六:MAC地址获取装置向WiFi终端响应Association response消息,其中该消息中的状态码status code置为非0值,以拒绝WiFi终端的关联请求。

[0013] 步骤七:MAC地址获取装置从WiFi终端发送的Association request消息中提取WiFi终端的真实MAC地址。

[0014] 步骤八:保存获取的WiFi终端MAC地址并上报给相关应用程序。

[0015] 本发明的有益效果:

1、本发明对于在WiFi网络扫描阶段采用随机MAC地址的WiFi终端,本发明提出的方法在不需要WiFi终端联网的情况下即可获取到WiFi终端的真实MAC地址。

[0016] 2、对于未采用随机MAC地址方案的WiFi终端,本发明提出的方法可以自动切换成更简单更快速的获取方法。

附图说明

[0017] 图1:本发明结构原理示意图。

[0018] 图2:本发明MAC地址获取装置工作流程图。

具体实施方式

[0019] 下面结合附图和实施例来对本发明做进一步描述:

本发明的实施方式如下:

S201:当WiFi终端进入MAC地址获取装置覆盖范围内时,装置中的终端探测模块抓取到来自该WiFi终端发送的Probe request消息。WiFi终端通过发送Probe request消息主动发现周围可用的WiFi网络。

[0020] 如前所述,Probe request消息中的源MAC地址可能是WiFi终端的真实MAC地址,也可能是一个随机产生的MAC地址。随机MAC地址是动态变化的,无法用于标识或定位该WiFi终端。

[0021] 终端探测模块的具体实现方式是向无线控制模块发送指令,将装置中的无线模块置为监听(monitor)模式,周期性扫描各个无线信道并对收到的Probe request消息进行保存和分析。

[0022] S202:终端探测模块从Probe request信息中提取源MAC地址并发送给决策模块。

[0023] S203:决策模块对源MAC地址进行判断,如果源MAC地址不是本地管理类型,则表示该源MAC地址为WiFi终端的真实MAC地址,跳转到步骤S208。

[0024] MAC地址是否为本地管理类型的判定方法为:根据IEEE 802 MAC地址的定义,若MAC地址第一个字节的从低位开始的第二个bit为1,则表示该MAC地址类型为本地管理类型,本地管理类型MAC地址不保证是全局唯一的。随机MAC一般选用本地管理类型的MAC地址。

[0025] 需要说明的是,本地管理类型MAC仅为随机MAC的一种,本发明提出的方法同样适用于其它类型的随机MAC。特别地,若无法辨别MAC地址是否为随机MAC,则将其作为随机MAC对待。

[0026] S204:决策模块向无线控制模块发出指令,后者向WiFi终端发送Probe response响应消息,其中包含预置的SSID名称和认证方式。

[0027] 预置SSID和认证方式的获取可以是读取本地配置文件,或者是通过网络接口从外部服务器或者云平台查询得到。该SSID是WiFi终端预先连接过的WiFi网络,例如,为了使用某种基于MAC地址的业务,该业务可以要求WiFi终端至少连接该SSID一次。

[0028] 预置SSID的认证方式可以是Open或者WPA2等方式,如果采用需要提供密码的认证方式,WiFi终端在第一次连接该SSID时需要提供正确的认证密码以完成WiFi连接的认证过程。

[0029] S205:根据802.11 WiFi网络连接协议,当WiFi终端收到正确的Probe response消息及完成相应的认证过程后,WiFi终端将向MAC地址获取装置发送Association request消息以启动网络关联(association)流程。

[0030] 虽然WiFi终端在Probe request消息中可能采用随机MAC地址,为了保证WiFi连接流程的正常执行,WiFi终端会在Association request消息中提供真实的MAC地址。

[0031] S206:MAC地址获取装置收到Association request消息后,向WiFi终端回应Association response消息,其中该消息中的状态码status code(例如,12:Association denied)。MAC地址获取装置通过发送关联拒绝消息防止WiFi终端连接到该SSID。

[0032] WiFi终端在收到关联拒绝消息后,会重新发起对其它WiFi网络的尝试,只到连接到可正常联网的无线热点。因而,本装置不会对WiFi终端的正常联网造成影响。

[0033] S207:决策模块从无线控制模块中提取来自WiFi终端Association request消息的源MAC地址。如前所述,该源MAC地址为WiFi终端的真实MAC地址。

[0034] S208:决策模块将提取的源MAC地址发送给存储通信模块。存储通信模块可以将获取到的真实WiFi终端MAC地址保持到本地数据库供其它业务调用,或者通过网络接口发送到外部服务器或者云平台供其它业务使用。

[0035] 综上,当WiFi终端进入MAC地址获取装置覆盖范围时,在不对WiFi终端联网进行干扰的情况下,MAC地址获取装置即可得到WiFi终端的真实MAC地址,并可以传送给其它服务程序实现相关业务应用。

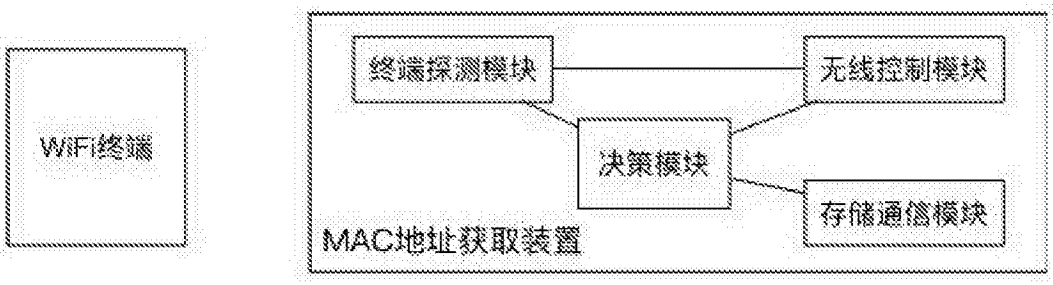
WiFi终端
终端探测模块
无线控制模块
决策模块
存储通信模块
MAC地址获取装置

图1

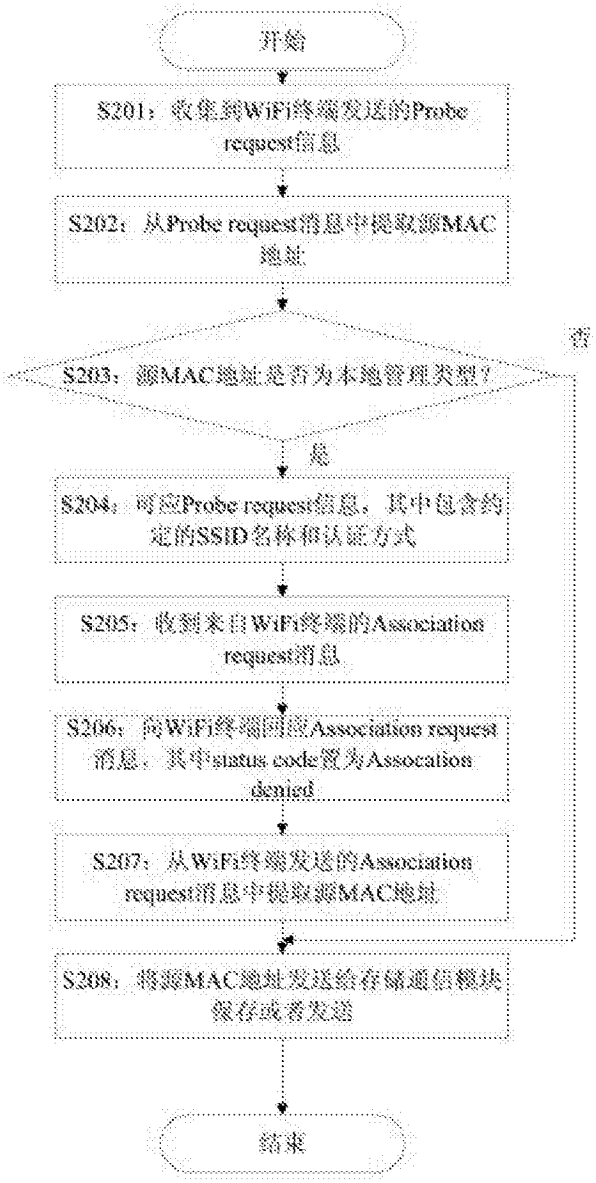
开始
S201：收集到WiFi终端发送的Probe request信息
S202：从Probe request消息中提取源MAC地址
S203：源MAC地址是否为本地管理类型？
否
是
S204：响应Probe request信息，其中包含约定的SSID名称和认证方式
S205：收到来自WiFi终端的Association request消息
S206：向WiFi终端回应Association request消息，其中status code置为Assocation denied
S207：从WiFi终端发送的Association request消息中提取源MAC地址
S208：将源MAC地址发送给存储通信模块保存或者发送
结束

图2