(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 108282808 A
(43)申请公布日 2018.07.13

(21)申请号 201711407788.8

(22)申请日 2017.12.22

(71)申请人 厦门市美亚柏科信息股份有限公司
地址 361000 福建省厦门市软件园二期观日路12号美亚柏科大厦

(72)发明人 陈大钹 张永光 许清红 江瑞滨

(74)专利代理机构 深圳市博锐专利事务所 44275
代理人 张明

(51)Int.Cl.
H04W 24/08(2009.01)
H04W 64/00(2009.01)
H04L 29/12(2006.01)
H04W 8/26(2009.01)

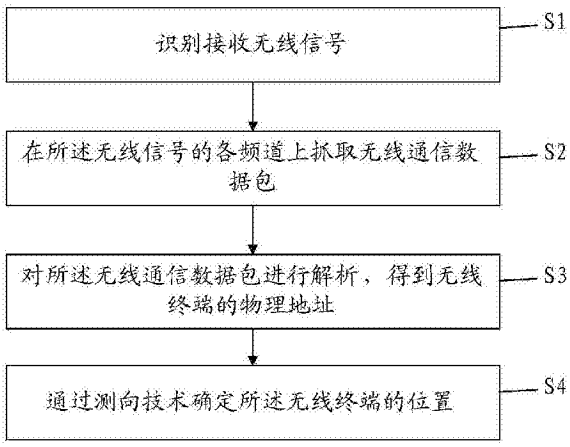
权利要求书1页 说明书4页 附图1页

(54)发明名称

无线终端的探测方法及其系统

(57)摘要

本发明公开了一种无线终端的探测方法及其系统，方法包括：识别接收无线信号；在所述无线信号的各频道上抓取无线通信数据包；对所述无线通信数据包进行解析，得到无线终端的物理地址；通过测向技术确定所述无线终端的位置。本发明可用于各级司法机关和行政执法部门对移动终端的位置快速、准确的落实确定。



CN 108282808 A

1.一种无线终端的探测方法，其特征在于，包括：

识别接收无线信号；

在所述无线信号的各频道上抓取无线通信数据包；

对所述无线通信数据包进行解析，得到无线终端的物理地址；

通过测向技术确定所述无线终端的位置。

2.根据权利要求1所述的无线终端的探测方法，其特征在于，所述“识别接收无线信号”具体为：

通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

3.根据权利要求1所述的无线终端的探测方法，其特征在于，所述“对所述无线通信数据包进行解析，得到无线终端的物理地址”具体为：

解析所述无线通信数据包的802.11协议帧，从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址；

过滤所述物理地址中的广播物理地址，得到无线终端的物理地址。

4.一种无线终端的探测系统，其特征在于，包括：

天线模块，用于识别接收无线信号；

采集模块，用于在所述无线信号的各频道上抓取无线通信数据包；

解析模块，用于对所述无线通信数据包进行解析，得到无线终端的物理地址；

测向模块，用于通过测向技术确定所述无线终端的位置。

5.根据权利要求4所述的无线终端的探测系统，其特征在于，所述天线模块具体用于通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

6.根据权利要求4所述的无线终端的探测系统，其特征在于，所述解析模块具体用于解析所述无线通信数据包的802.11协议帧，从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址；过滤所述物理地址中的广播物理地址，得到无线终端的物理地址。

7.根据权利要求4所述的无线终端的探测系统，其特征在于，还包括：

充电模块，用于为所述采集模块提供电源。

无线终端的探测方法及其系统

技术领域

[0001] 本发明涉及取证技术领域，尤其涉及一种无线终端的探测方法及其系统。

背景技术

[0002] 随着无线网络的普及，Wi-Fi已无处不在，人们也越来越离不开无线网络。Wi-Fi带来便利的同时，也存在很大的安全隐患，许多不法分子利用无线网络进行违法犯罪活动，造成严重的信息安全问题。因此需要在取证工作中寻找使用无线网络进行上网的AP(Access Point，访问接入点)以及移动终端的MAC地址(物理地址)和位置。

[0003] 现有设备可以采集获取无线AP的MAC地址，但是无法对来源的位置进行确定，且无法实时进行查看；同时，现有设备基本是在PC主机上才能用，且都是固定的，达不到可移动、便携的效果。

发明内容

[0004] 本发明所要解决的技术问题是：提供一种无线终端的探测方法及其系统，可快速准确地测试出无线终端的具体方位。

[0005] 为了解决上述技术问题，本发明采用的技术方案为：一种无线终端的探测方法，包括：

[0006] 识别接收无线信号；

[0007] 在所述无线信号的各频道上抓取无线通信数据包；

[0008] 对所述无线通信数据包进行解析，得到无线终端的物理地址；

[0009] 通过测向技术确定所述无线终端的位置。

[0010] 本发明还涉及一种无线终端的探测系统，包括：

[0011] 天线模块，用于识别接收无线信号；

[0012] 采集模块，用于在所述无线信号的各频道上抓取无线通信数据包；

[0013] 解析模块，用于对所述无线通信数据包进行解析，得到无线终端的物理地址；

[0014] 测向模块，用于通过测向技术确定所述无线终端的位置。

[0015] 本发明的有益效果在于：通过抓取无线通信数据包并进行解析，可得到使用无线网络进行上位的终端的物理地址；针对取证工作中无线网络终端位置难找的问题，运用了测向技术，针对使用无线网络进行上网的终端位置进行确定。采用便携式设计，便于在现场取证勘查工作中移动使用；本发明可用于各级司法机关和行政执法部门对无线网络AP和移动终端的位置快速、准确的落实确定。

附图说明

[0016] 图1为本发明实施例一的一种无线终端的探测方法的流程图；

[0017] 图2为本发明实施例二的一种无线终端的探测系统的结构示意图。

[0018] 标号说明：

[0019] 1、天线模块；2、采集模块；3、解析模块；4、测向模块；5、充电模块。

具体实施方式

[0020] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0021] 本发明最关键的构思在于：通过分析无线通信数据包得到MAC地址，通过测向技术获取具体位置。

[0022] 请参阅图1，一种无线终端的探测方法，包括：

[0023] 识别接收无线信号；

[0024] 在所述无线信号的各频道上抓取无线通信数据包；

[0025] 对所述无线通信数据包进行解析，得到无线终端的物理地址；

[0026] 通过测向技术确定所述无线终端的位置。

[0027] 从上述描述可知，本发明的有益效果在于：可快速准确地得到无线终端的MAC地址和具体方位。

[0028] 进一步地，所述“识别接收无线信号”具体为：

[0029] 通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

[0030] 进一步地，所述“对所述无线通信数据包进行解析，得到无线终端的物理地址”具体为：

[0031] 解析所述无线通信数据包的802.11协议帧，从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址；

[0032] 过滤所述物理地址中的广播物理地址，得到无线终端的物理地址。

[0033] 由上述描述可知，通过解析802.11协议帧的帧头，即可得到MAC地址。

[0034] 本发明还提出一种无线终端的探测系统，包括：

[0035] 天线模块，用于识别接收无线信号；

[0036] 采集模块，用于在所述无线信号的各频道上抓取无线通信数据包；

[0037] 解析模块，用于对所述无线通信数据包进行解析，得到无线终端的物理地址；

[0038] 测向模块，用于通过测向技术确定所述无线终端的位置。

[0039] 进一步地，所述天线模块具体用于通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

[0040] 进一步地，所述解析模块具体用于解析所述无线通信数据包的802.11协议帧，从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址；过滤所述物理地址中的广播物理地址，得到无线终端的物理地址。

[0041] 进一步地，还包括：

[0042] 充电模块，用于为所述采集模块提供电源。

[0043] 实施例一

[0044] 请参照图1，本发明的实施例一为：一种无线终端的探测方法，包括如下步骤：

[0045] S1：识别接收无线信号；具体地，通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

[0046] S2：在所述无线信号的各频道上抓取无线通信数据包；具体地，分时间片循环定时

地在2.4G和5.8G的各个频道上抓取无线通信数据包。

[0047] S3:对所述无线通信数据包进行解析,得到无线终端的物理地址;具体地,解析所述无线通信数据包的802.11协议帧,从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址;过滤所述物理地址中的广播物理地址,得到无线终端的物理地址。

[0048] S4:通过测向技术确定所述无线终端的位置。此时,即可得到无线终端的MAC地址和具体位置。

[0049] 本实施例通过抓取无线通信数据包并进行解析,可得到使用无线网络进行上位的终端的物理地址;针对取证工作中无线网络终端位置难找的问题,运用了测向技术,针对使用无线网络进行上网的终端位置进行确定。采用便携式设计,便于在现场取证勘查工作中移动使用;可用于各级司法机关和行政执法部门对无线网络AP和移动终端的位置快速、准确的落实确定。

[0050] 实施例二

[0051] 请参照图2,本实施例是对应实施例一的一种无线终端的探测系统,包括:

[0052] 天线模块1,用于识别接收无线信号;

[0053] 采集模块2,用于在所述无线信号的各频道上抓取无线通信数据包;

[0054] 解析模块3,用于对所述无线通信数据包进行解析,得到无线终端的物理地址;

[0055] 测向模块4,用于通过测向技术确定所述无线终端的位置。

[0056] 进一步地,所述天线模块1具体用于通过2.4G和5.8G全向天线识别接收频段为2.4G和5.8G的无线信号。

[0057] 进一步地,所述解析模块3具体用于解析所述无线通信数据包的802.11协议帧,从帧头的BSSID字段、源地址字段和目的地址字段中提取物理地址;过滤所述物理地址中的广播物理地址,得到无线终端的物理地址。

[0058] 进一步地,还包括:

[0059] 充电模块5,用于为所述采集模块提供电源。

[0060] 实施例三

[0061] 本实施例为上述实施例的一具体应用场景。

[0062] 在本实施例中,将天线模块和采集模块集成在探测装置中,将解析模块和测向模块集成在主机中;天线模块与采集模块连接,采集模块通过数据线与主机连接。进一步地,探测装置中还设有充电模块,用于为采集模块提供电源,也可以为主机充电。

[0063] 将探测装置设备置于要采集的位置(可车载,可便携或者固定部署均可),通过主机系统APP软件设置AP(无线访问接入点)设备使其工作于Monitor模式(监听模式),设置扫描频率,扫描频道等,然后采集模块分时间片循环定时地在2.4GHz和5.8GHz的各个频道上抓取Wi-Fi无线通信数据包,并发送给主机,解析模块解析各无线通信数据包的802.11协议帧的帧头,最后从帧头的BSSID字段、Source address(源地址)字段、Destination address(目的地址)字段中提取出MAC地址,在过滤掉广播MAC后即可以得到AP设备和通信终端设备的MAC地址,从而标识该MAC地址对应的无线终端,采集相关信息并通过主机展示出来。主机系统还可以设置已知的MAC地址、已知AP的SSID进行扫描,当有扫描到目标时,系统软件会提示,并报警,然后测向模块通过测向技术进行来源进行探测,最终确定出来源的实际具体位置。重复以上过程就可以全部发现探测装置周边的各种无线终端,从而达到无遗漏寻找

到无线终端的持有人的效果。

[0064] 本实施例实现简单，探测装置可做成充电宝的形状，主机为手机或平板电脑，隐蔽性好；探测装置中集成了充电模块，当主机电量不足时，可以给主机充电；采用便携式涉及，便于在现场取证勘查工作中移动使用。

[0065] 综上所述，本发明提供的一种无线终端的探测方法及其系统，通过抓取无线通信数据包并进行解析，可得到使用无线网络进行上位的终端的物理地址；针对取证工作中无线网络终端位置难找的问题，运用了测向技术，针对使用无线网络进行上网的终端位置进行确定。采用便携式设计，便于在现场取证勘查工作中移动使用；本发明可用于各级司法机关和行政执法部门对无线网络AP和移动终端的位置快速、准确的落实确定。

[0066] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等同变换，或直接或间接运用在相关的技术领域，均同理包括在本发明的专利保护范围内。

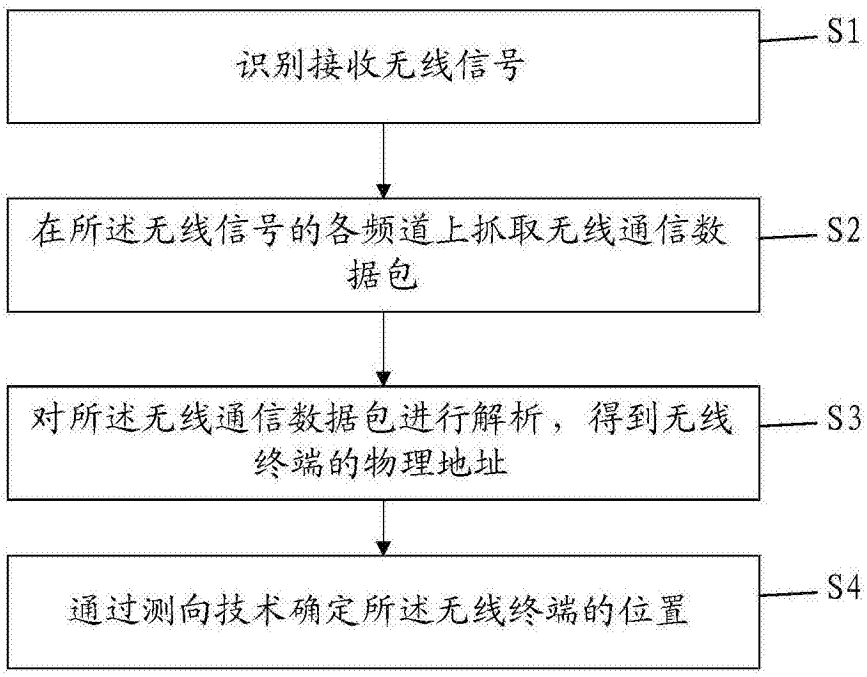

识别接收无线信号
S1
在所述无线信号的各频道上抓取无线通信数据包
S2
对所述无线通信数据包进行解析，得到无线终端的物理地址
S3
通过测向技术确定所述无线终端的位置
S4

图1

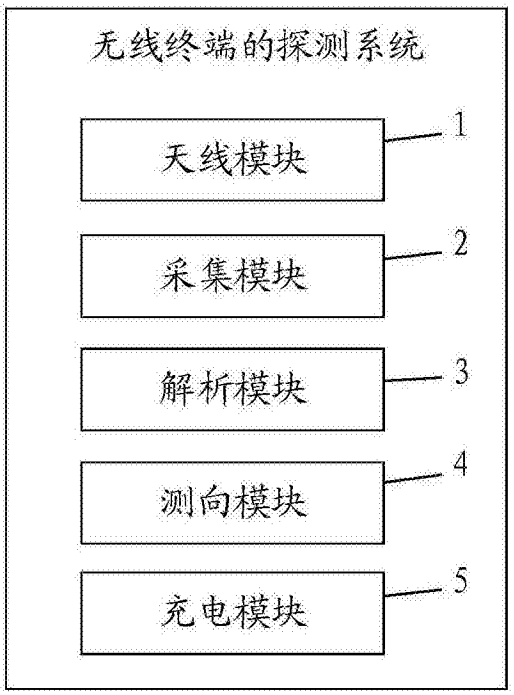

无线终端的探测系统
天线模块
1
采集模块
2
解析模块
3
测向模块
4
充电模块
5

图2