



苹果终端伪 MAC 功能

苹果的伪装 MAC 功能是在 iOS8 的系统更新时加入的。要想让苹果的这项反追踪功能发挥作用，你的 iPhone 就必须满足 3 个条件：

- 1、必须关闭移动数据（3G、4G 和 LTE）。
- 2、手机必须处于休眠模式或锁屏状态下。
- 3、必须在隐私设置中将地理位置服务的开关关掉。

在实际使用中，几乎没有人会让自己的手机处于这种状态下。首先，大多数的热门的应用如：地图、微博、微信、团购等应用都会提示用户将地理位置服务打开，以获取附近的人和店铺。。

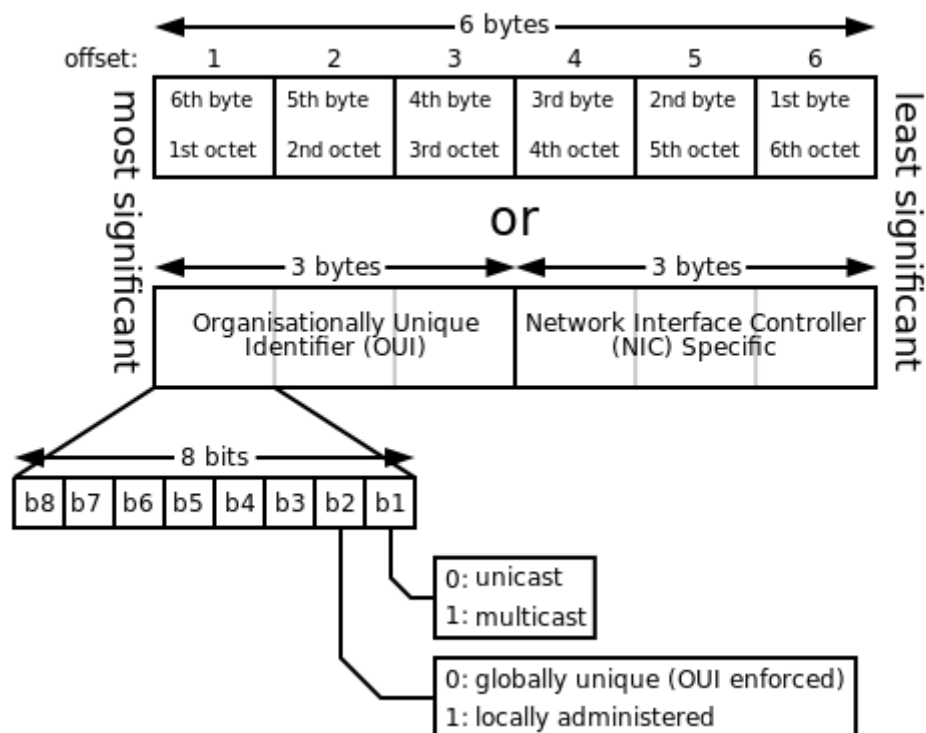
另外，手机一旦被唤醒，就会离开这种状态，所以广大普通用户的手机都是不会处于这种状态下的。

另一方面，对于苹果使用伪 MAC 连接 WIFI 的过程，我们进行研究和测试确认，它的连接形为如下：

- 1、iOS8 或以上系统版本的 iPhone 终端在没有连上 WIFI 时，发出探测报文 (Probe Request) 的源 MAC 地址不是终端本身的 MAC，是一个随机伪 MAC，在没有连上 WIFI 前这个伪 MAC 不会变。
- 2、等终端连上 WIFI 后，发出探测报文 (Probe Request) 的源 MAC 地址就是终端本身的 MAC 地址。
- 3、等终端断开 WIFI 连接后，发出探测报文 (Probe Request) 的源 MAC 地址又不是终端本身的 MAC，是一个新的随机伪 MAC，和之前的伪 MAC 也不一样，在没有连上 WIFI 前这个新伪 MAC 也不会变。

而它的随机伪 MAC 的格式，也是具有特征的，即它伪装的是 MAC 地址是一个本地管理地址，如下图所示，伪装的 MAC 地址的第一个字节的 b2 位都是为 1 的：

1648	2070.434	4a:da:e6:96:10:44	Broadcast	34	3	Probe Request, SN=9, FN=0, Flags=.....C, SSID=Broadcas
1738	2205.345	4a:da:e6:96:10:44	Broadcast	80	11	Probe Request, SN=6, FN=0, Flags=.....C, SSID=Broadcas
1739	2205.366	4a:da:e6:96:10:44	Broadcast	25	1	Probe Request, SN=7, FN=0, Flags=.....C, SSID=Broadcas
1740	2205.388	4a:da:e6:96:10:44	Broadcast	33	2	Probe Request, SN=8, FN=0, Flags=.....C, SSID=Broadcas
1741	2205.412	4a:da:e6:96:10:44	Broadcast	35	3	Probe Request, SN=9, FN=0, Flags=.....C, SSID=Broadcas
1855	2340.326	4a:da:e6:96:10:44	Broadcast	82	11	Probe Request, SN=6, FN=0, Flags=.....C, SSID=Broadcas
1856	2340.347	4a:da:e6:96:10:44	Broadcast	25	1	Probe Request, SN=7, FN=0, Flags=.....C, SSID=Broadcas
1857	2340.414	4a:da:e6:96:10:44	Broadcast	36	4	Probe Request, SN=10, FN=0, Flags=.....C, SSID=Broadcas
2007	2535.547	b6:b7:d5:58:1f:5b	Broadcast	81	11	Probe Request, SN=6, FN=0, Flags=.....C, SSID=Broadcas
2008	2535.577	b6:b7:d5:58:1f:5b	Broadcast	25	1	Probe Request, SN=7, FN=0, Flags=.....C, SSID=Broadcas
2009	2535.592	b6:b7:d5:58:1f:5b	Broadcast	34	2	Probe Request, SN=8, FN=0, Flags=.....C, SSID=Broadcas
2010	2535.615	b6:b7:d5:58:1f:5b	Broadcast	34	3	Probe Request, SN=9, FN=0, Flags=.....C, SSID=Broadcas
2105	2670.411	b6:b7:d5:58:1f:5b	Broadcast	7	6	Probe Request, SN=1, FN=0, Flags=.....C, SSID=Broadcas



针对于伪装 MAC 的这个特征，我们可以精准地识别出苹果的伪装 MAC 地址。在进行客流分析统计客流量时，将排除掉所有伪装的 MAC 地址，保障客流量数据来源的准确性。

无线定位以及蓝牙定位功能

无线定位，是通过获取采集移动设备到周围各个 AP（Access Point）的信号强度 RSSI，利用 RSSI 估算距离进行定位的。其实现方式分为主动采集和被动采集：主动采集，是依赖于 AP 主动采集移动设备的信号强度，在实际使用中，由于 AP 部署稀疏，且相邻的 AP 处于不同的无线信道，主动采集到的数据量不足，定位的效果普遍不佳。

被动采集，是在移动设备上安装 APP 应用的方式，由 APP 在后台主动向 AP 发送消息，增加被采集到的数据量，能提升定位的效果。但需要结合 APP 使用，在客户的推广接受程度会受到限制。

蓝牙定位也称 beacon 定位，同样是基于 RSSI 的。其实现是通过蓝牙信标主动地广播宣告自己的位置来感知所处的位置。但是传送距离短小，决定了蓝牙设备的部署密度非常大。并且由于电源无法长久使用，当设备电量用完后，更换设备的维护成本也是一笔不菲的开销。



无线定位和蓝牙定位的简要对比如下：

蓝牙定位	采用基于蓝牙的 RSSI 定位技术，除了使用集成在移动终端上的蓝牙模块外，还需要部署蓝牙基站。	1. 低功耗 2. 定位精度高	1. 除了使用集成在移动终端上的蓝牙模块，还需要蓝牙基站，但是蓝牙基站不普及，且蓝牙器材和设备价格比较昂贵，目前尚未大规模推广； 2. iBeacon 一般通过电池供电，有些可用 3-5 年，不过这也意味着每 3-5 年就需要更换电池。维护成本高。	定位精度 2 米-3 米
无线定位	Wi-Fi 定位基于现有 WLAN 网络，采用 RSSI 定位方式。	1. 网络已广泛部署，产品成熟，价格低廉。 2. 无需额外设备，成本低。 3. 使用方便。	1. 射频信号易受环境干扰。 2. 定位精度和准确度较差，且具有较强的时变特性。 3. 指纹识别训练数据采集工作量大。 4. 不适于高精度实时跟踪场景。	定位精度 3 米-15 米

就定位的算法而言，目前基于 RSSI 定位主要有二个算法：三角定位算法，指纹识别算法

1、三角定位算法：

如果我们已经知道了这些 AP 的位置，我们可以利用信号 RSSI 衰减模型估算出移动设备距离各个 AP 的距离，然后根据智能机到周围 AP 距离画圆。在实际使用中，只要知道被搜寻设备与周围三个点的距离，就可以依此画出三个圆圈，而三个圆圈的交会位置，便是设备的位置。

定位的过程可分成两个阶段：测距与定位

①测距阶段：

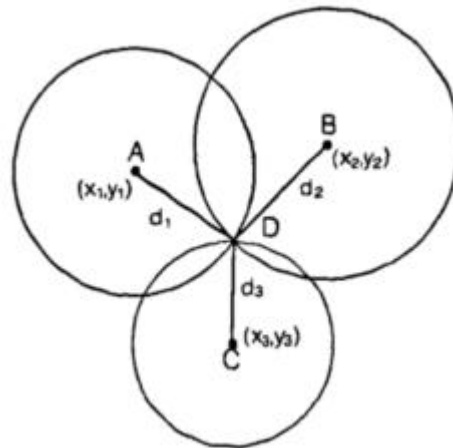
待测点首先接收来自三个不同已知位置 WIFI 接入点的 RSS，然后依照无线信号的传输损耗模型将其转换成待测目标到相应 WIFI 接入点的距离。无线信号在传输过程中通常会受路径损耗、阴影衰落等的影响，接收信号功率随距离的变化关系可由信号传输损耗模型给出。

②定位阶段：

通过三角形算法计算待测点位置，即分别以已知位置的三个 WIFI 接入点为圆心，以其各自到待测点的距离为半径为范围，所得三个圆形范围的交点即为待测点位



置。



三角定位的理论很简单，但其缺点也非常明显，就是定位结果非常不精准。原因很简单，因为 AP 的位置和移动设备距离 AP 的长度都是推算出的，误差+误差=更大的误差。

2、指纹识别算法：

指纹识别算法需要提前绘制一幅信号 map，相当于对每个一点都采样标记出它的信道强度情况。然后在定位时，在信号 map 中进行匹配，匹配出的信号最相似位置，即设备的位置。

其方法类似于机器学习算法，分为两个阶段：



①离线训练阶段：

其目标在于建立一个位置指纹识别数据库。首先，选择合理的参考点分布，确保能为定位阶段的准确位置估计提供足够的信息。接着依次在各个参考点上测量来自不同 AP 的 RSS 值，将相应的 MAC 地址与参考点的位置信息记录在数据库中，直至遍历关注区域内所有的参考点。由于受环境影响，无线信号强度并不稳定，为了克服 RSS 不稳定对定位的影响，通常在每个参考点上多次测量取平均。

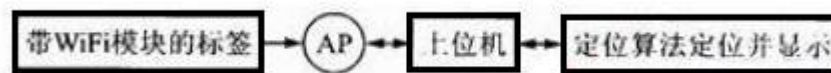
②在线定位阶段：



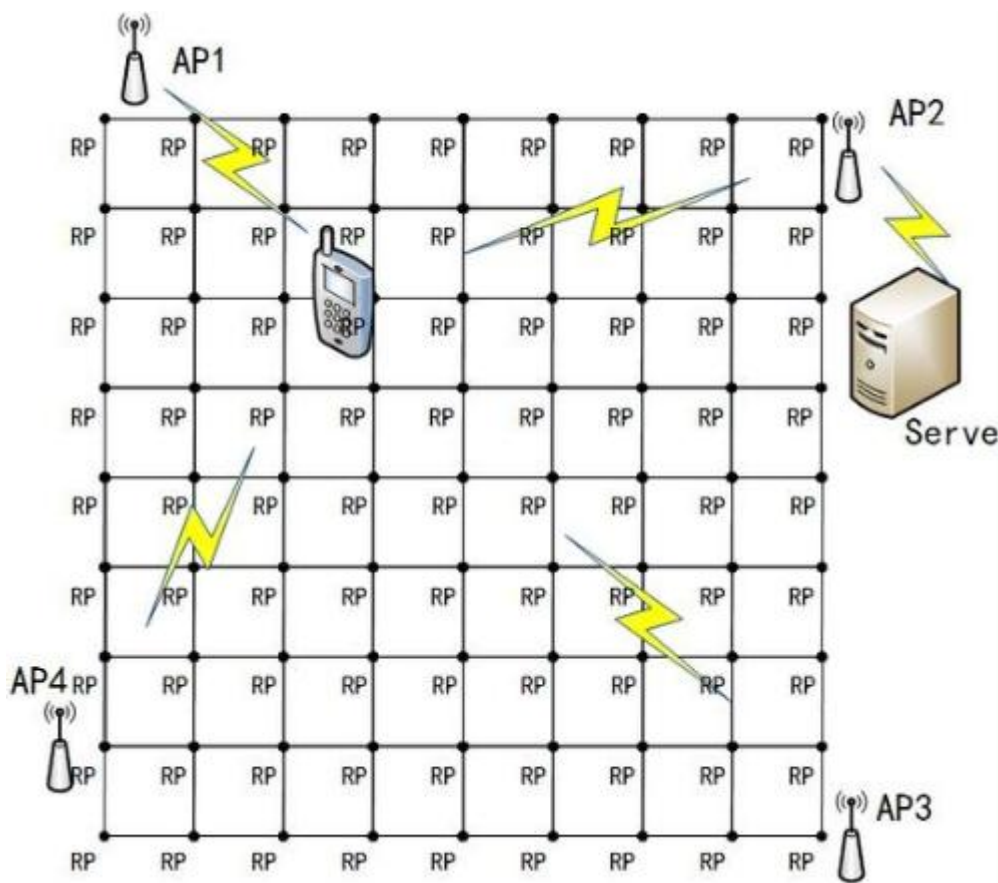
给定数据库后，依据一定的匹配算法将待测点上接收的 AP RSS 与数据库中的已有数据进行比较，计算位置估计值。常用的匹配算法有最近邻法（NN）、KNN、神经网络等。

相比三角测量基于信号传输模型来估算无线终端与 WIFI 接入点间的相对距离，指纹识别具有更高的准确度，因为它使用的是真实采集的信号信息而不是根据经验公式来推算。但该法同样存在很大的问题：首先，指纹识别数据库的构建需要耗费大量的人力物力，数据库完备程度会影响到定位的精度。其次，WLAN 无线信号时变特性导致预先采集的数据在某种意义上只具有“瞬时”有效性，而且所部署环境的变化都会导致 RSS 或大或小的变化，使得需要重构指纹识别数据库。因此在实际使用中，每三个月或半年就需要重采一次以保证高精度。而且每次的采集量需要非常大，其收集和更新指纹的成本费用非常高。

此外，目前还有一种热门的定位方式是 WIFI + RFID 电子标签的方式。把无线 WiFi 技术和 RFID 技术结合起来，进一步地提高定位的范围和精度。其系统硬件结构如下图所示：



其实现是在环境中按网格部署大量的电子标签，通过电子标签来构造指纹识别的数据库，定位的过程如下：



①在公司大楼的走道和三间房内各安置每隔 3 m 固定一个电子标签(参考标签), 在该层楼的东南两北角各放置一个 AP。做好上位机与下位机的无线通信(软件程序的服务器和客户端的连接)。

②实验进行时, 当待测标签进入到 AP (4 个) 的范围内, 开始接收到待测标签发出的信号场强, 并传入上位机。同时也接收各个参考标签在各个 AP 的信号场强, 并传入上位机。

③定位算法则把待测标签在 4 个 AP (AP1, AP2, AP3, AP4) 上的场强建立一个场强矢量, 同时参考标签也建立成场强矢量。通过 LANDMARC 算法即通过比较待测标签场强矢量与参考标签场强矢量的欧氏距离, 找出 3 个欧氏距离最小的参考标签, 并得知 3 个参考标签的具体位置。对于 3 个参考点, 不用再根据信号的强度来决定其半径, 而是 3 个以参考点为圆心, 以最近参考标签之间的距离(以确定每隔几米放置一个参考标签)的 $3/4$ 长度为半径做 3 个圆, 这样 3 个圆两两相交的可能性会增加。

这种定位方式的优势是在原来 LANDMARC 算法的定位精度上, 再进行三角定位, 进一步提高定位精度。同时, 以参考标签之间的距离来进行进一步的三角定位, 可以减少额外的计算, 并且可以减少由于参考标签场强的变化带来的重复测量。其缺点在于 RFID 的距离短小, 难以大规模的部署。



RFID	可以通过无线电信号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或者光学接触。	1. 无源 RFID 标签定位成本低 2. 有源 RFID 标签定位范围相对较大 3. 可根据不同的应用需求选择不同的定位方法	1. 无源 RFID 读写器成本较高 2. 需要部署多个读写器构建定位基础设施 3. 难以大规模部署	定位精度 1.5 米 增加参考标签可以进一步提高定位精度。
------	--	---	--	---