

Fibocom

完 美 无 线 体 验

FIBOCOM L610 系列

应用指南_WIFISCAN 定位技术

文档版本：V1.0.1

更新日期：2020-06-16



适用型号

序号	产品型号	说明
1	L610 系列	NA

FIBOCOM
Confidential

版权声明

版权所有©2020 深圳市广和通无线股份有限公司。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

商标申明



为深圳市广和通无线股份有限公司的注册商标，由所有人拥有。

版本记录

文档版本	编写人	主审人	批准人	更新日期	说明
V1.0.1	何嘉照		王海亮	2020-06-16	规范化格式
V1.0.0	董福	程涛涛 王海亮	邓利斌	2020-02-26	初始版本

目录

1	背景介绍.....	5
2	LBS	6
3	WIFI 定位.....	7
4	软件设计.....	8
4.1	简述	8
4.2	支持 GETSET 设置.....	8
5	测试.....	10
6	参考 LOG 信息	11
7	Q&A	13

FIBOCOM
Confidential

1 背景介绍

每一个无线 AP 都有一个全球唯一的 MAC 地址，并且一般来说无线 AP 在一段时间内是不会移动的。

设备在开启 Wi-Fi 的情况下,即可扫描并收集周围的 AP 信号, 无论是否加密,是否已连接, 甚至信号强度不足以显示在无线信号列表中,都可以获取到 AP 广播出来的 MAC 地址, 获取到的 MAC 信息信号强度及热点名称通过 HTTP 发给 MAP 运营商位置服务器,服务器检索出每一个 AP 的地理位置,并结合每个信号的强弱程度,计算出设备的地理位置并返回到用户设备。

基本定位: GPS、GNSS、北斗、LBS、WIFI、蓝牙等。

通过 LBS 和 WIFI 实现定位。

FIBOCOM
Confidential

2 LBS

获取注册移动网络小区及邻区 MCC, MNC, CELLID 等参数+跟地图服务商协商的 key, 通过 HTTP 将上述信息发给地图服务商服务器, 服务器回 200OK 携带有效经纬度信息下来。从而达到粗定位的目的。

缺点: 城市内移动基站小区密集, 定位误差几十米上百米上下, 农村偏远山区基站距离较远误差大大增加。

优点: 只要注册上支持 LBS 的移动网络, 只能获取到服务小区数据的情况下也能获取到 MAP 服务器下发的经纬度信息。

FIBOCOM
Confidential

3 WIFI 定位

芯片内部集成的 WIFI 模块，目前暂不支持 TX（发射），不可以与 AP 建立连接和传输数据。只有 Rx（接收），只可以 scan AP，可接收周围覆盖的 AP 广播包；AP 会向四周环境中定期发射广播包，广播的周期通常是 100ms，硬件收到广播包之后做解析，软件读取硬件寄存器可以得到 AP 的信息，包括 MAC 地址、所在的信道和信号强度。

有多个热点覆盖的地方很快能扫到几个热点并获取到 MAC 及信号强度以及热点名称，用移动网络数据，通过 HTTP 将 MAC 信息+跟地图服务商协商的 key 上报给 MAP 服务器，MAP 服务器回 200OK 携带有效经纬度信息及街道信息。

缺点：受周边热点覆盖限制，需要一定数量的热点信息，MAP 服务器才会下发经纬度信息，或取 MAC 信息不准确 MAP 服务器不会下发经纬度信息，或无热点覆盖则无法实现 WIFI 定位。模块移动扫到的是热点也在移动，也会影响 WIFI 定位精度；另外 scan AP 期间，功耗大约增加 70%左右。

优点：定位比 LBS 定位更为精确，热点覆盖及真实物理位置精度高，误差可控几十米至几米以内。

FIBOCOM
Confidential

4 软件设计

4.1 简述

AT+GTGIS=7

7 表示 WIFISCAN;

目前 A 线程开机创建, 等待 B 线程发来 WIFISCAN 请求, 收到 B 线程发来的 WIFISCAN 请求后打开内置 WIFI, 开始循环 search channel, A 线程扫到 5 个 (默认) 热点后, 停止 WIFI scan channel 并关闭 WIFI, 并发 event 通知 B 线程, A 线程进入等待接收消息状态, 等待下一次 B 线程执行 WIFISCAN 请求; B 线程收到 A 发来的指示后执行 MAPURLDNS 查询, TCP sockets 创建, 构造携带 MAC 及 RSSI 的 HTTP 数据包并发送给 MAP 位置服务器, 等待接收服务器回的 200OK 的数据, 捕获 GIS info 及街道信息。

默认 5 个 AP 包括重复的, 暂未考虑屏蔽重复热点。

4.2 支持 GTSET 设置

支持 GTSET 设置 WIFISCAN 扫热点最长时间和最多热点个数。

AT+GTSET="WIFISCAN",10,5

其中第一个数值是扫热点时间: 默认 10s, 初定取值范围 1s~30s;

第二个数值是扫热点个数: 默认 5 个, 初定取值 1~30。

只要当前环境大约等于一个热点覆盖, 循环 scan, 一定时间内都能扫够设置的热点个数, 停掉定时器, 执行定位功能;

如果当前无热点覆盖, 设置的时间超时, 停掉 WIFISCAN, 关闭 WIFI, 并上报+GTGIS: wifiscan time out and none of mac found。

由于 WIFISCAN 期间功耗会增加很多, 为了节能, 很快就能 search 一遍, 优先考虑先 search 到设置个数的热点, 后考虑定时器超时; 所以不考虑去重;

比如: 当前环境仅有 3 个热点覆盖, 设置要扫到 5 个, 如果设置的默认时间是 10s, 如果考虑去重, 则只能达到 10s 才能 scan 结束, 正常情况 3 个热点几秒内就能扫到, 再次扫一遍重复扫到记录下来即可终止 WIFISCAN, 可有效避免长时间 scan 耗电的问题;

如果当前只有两个 WIFI 覆盖, 要求扫到 5 个, 假如扫到这两个 WIFI 后, 关闭这两个 WIFI, 达到设置时间后无法扫到 5 个, 则将此两个 WIFI MAC 信息上报给 MAP 位置服务器, 这样可有效避免模块移动或热

点移动导致的一开始能搜到 WIFI MAC 后再无法搜到的场景。

FIBOCOM
Confidential

5 测试

先 AT+MIPCALL=1 拨号，再 AT+GTGIS=7；

如果默认 10 秒未 search 到默认 5 个 AP（5 个 AP 包括重复的，暂未考虑屏蔽重复热点），停掉 WIFISCAN，并上报扫到的 MAC 信息给到 MAP 位置服务器，并接收服务器下发的经纬度信息。

如果 10 秒内 search 到默认 5 个 AP（5 个 AP 包括重复的，暂未考虑屏蔽重复热点），停掉 WIFISCAN，并将 MAC 及 RSSI 上报给 MAP server，并接收服务器下发的经纬度信息。

如果 MAP server 回的 HTTP 200OK 未携带经纬度信息及街道信息，

则上报：+GTGIS: Insufficient mac found and no GIS info received from MAP server

如果 MAP server 回的 HTTP200OK 携带有效经纬度信息及街道信息，

则上报正常的+GTGIS 信息：

+GTGIS:"108.8344406,34.2069759","road":"XXXXXX"

+GTGIS:"XXXXXX"

如果无 WIFI 覆盖，默认 20 秒内未搜到任何 WIFIMAC，则终止 WIFI 定位，并上报：+GTGIS: wifiscan timeout and none of mac found

如果 WIFISCAN 正在执行，则再次执行 WIFISCAN，AT 返回 ERROR；

其他异常同 AT+GTGIS=6，如 MAPURLDNS 查询 fail，或 TCP socket 建立失败，HTTP 数据发送失败等异常；

AT+GTSET 设置 WIFISCAN 最长扫热点时间和最大扫到热点个数相关功能验证 OK。

6 参考 LOG 信息

通过 coolwatcher 工具抓取 AP log 及 PCAP log: PCAP log 通过 wireshark 打开即可看到 TCP/IP log
Log info:

Index	Received	Tick	Level	Description
6503	20:48:32.739	11160	NET /	drvPsIntfRead in
6504	20:48:32.739	11160	NET /	drvPsIntfRead out 0
Index	Received	Tick	Level	Description
38	20:48:24.301	5543	FIBO/I	[wifi_scan_handle-186]
39	20:48:24.912	13500	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 1/500
20	20:48:25.380	23985	FIBO/I	[wifi_scan_handle-194] ap_count = 0
21	20:48:25.381	23986	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 2/500
32	20:48:26.023	34471	FIBO/I	[wifi_scan_handle-194] ap_count = 0
33	20:48:26.082	34472	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 3/500
14	20:48:26.538	42992	FIBO/I	[prvWifiScanChannel-155]found ap - (mac address : a89ceddc742e, rssiVal: -83 dBm, channel: 3)
15	20:48:26.598	42992	FIBO/I	[prvWifiScanChannel-162]mac_address[1] = a8:9c:ed:dc:74:2e
16	20:48:27.542	51183	FIBO/I	[wifi_scan_handle-194] ap_count = 1
17	20:48:27.543	51183	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 4/500
78	20:48:27.560	59704	FIBO/I	[prvWifiScanChannel-155]found ap - (mac address : a89ceddc742e, rssiVal: -80 dBm, channel: 4)
79	20:48:27.613	59704	FIBO/I	[prvWifiScanChannel-162]mac_address[2] = a8:9c:ed:dc:74:2e
10	20:48:28.181	2359	FIBO/I	[wifi_scan_handle-194] ap_count = 2
11	20:48:28.239	2359	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 5/500
12	20:48:28.701	12844	FIBO/I	[wifi_scan_handle-194] ap_count = 2
13	20:48:28.754	12845	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 6/500
74	20:48:29.462	23330	FIBO/I	[wifi_scan_handle-194] ap_count = 2
75	20:48:29.462	23331	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 7/500
16	20:48:30.103	33816	FIBO/I	[wifi_scan_handle-194] ap_count = 2
17	20:48:30.161	33816	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 8/500
58	20:48:30.742	44302	FIBO/I	[wifi_scan_handle-194] ap_count = 2
39	20:48:30.801	44302	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 9/500
10	20:48:31.258	54788	FIBO/I	[wifi_scan_handle-194] ap_count = 2
11	20:48:31.317	54788	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 10/500
33	20:48:32.419	65273	FIBO/I	[wifi_scan_handle-194] ap_count = 2
34	20:48:32.420	65273	FIBO/I	[prvWifiScanChannel-134]wifi scan channel 11/500
95	20:48:32.436	8258	FIBO/I	[prvWifiScanChannel-155]found ap - (mac address : 2640bba49d05, rssiVal: -99 dBm, channel: 11)
96	20:48:32.440	8258	FIBO/I	[prvWifiScanChannel-162]mac_address[3] = a8:9c:ed:dc:74:2e
97	20:48:32.440	8258	FIBO/I	[prvWifiScanChannel-155]found ap - (mac address : 2a6bada7ac55, rssiVal: -97 dBm, channel: 11)
98	20:48:32.441	8258	FIBO/I	[prvWifiScanChannel-162]mac_address[4] = 2a:6b:ad:a7:ac:55
99	20:48:32.441	8258	FIBO/I	[prvWifiScanChannel-155]found ap - (mac address : 2ee1da36eaf, rssiVal: -96 dBm, channel: 11)
90	20:48:32.442	8258	FIBO/I	[prvWifiScanChannel-162]mac_address[5] = 2e:ea:1d:a3:6e:af
32	20:48:32.443	8259	FIBO/I	[LbsThreadEntry-1400]wifi scan search AP reach 5
10	20:48:32.750	11180	ATEN/I	AT CMD1 urc len=125: *GTGIS: "108.8344486,34.2069759","road": "111E EA" *GTGIS: "EAI-EI I: *ED NAEPC il'E EA. cXii+*EikpA'cEikpB-d-Uj02u"
16	20:48:32.937	16449	FIBO/I	[wifi_scan_handle-194] ap_count = 5

通过 coolwatcher 抓的 wireshark log 看到:

```

46 2020-01-06 20:48:32.632000 10.167.216.8 203.119.213.128 117 34 34/11 + 00 [MJA] Seq=1 Ack=1 Win=20000 Len=0
46 2020-01-06 20:48:32.632000 10.167.216.8 203.119.213.128 HTTP 482 GET /position?accessType=1&imei=8cda08mac=08macs=a8:9c:ed:dc:74:2e,-83
47 2020-01-06 20:48:32.632000 203.119.213.128 10.167.216.8 TCP 54 80 + 34711 [ACK] Seq=1 Ack=429 Min=38016 Len=0
48 2020-01-06 20:48:32.666000 203.119.213.128 10.167.216.8 HTTP 705 HTTP/1.1 200 OK (application/json)
49 2020-01-06 20:48:32.695000 203.119.213.128 10.167.216.8 TCP 54 80 + 34711 [FIN, ACK] Seq=652 Ack=429 Win=38016 Len=0
50 2020-01-06 20:48:32.736000 10.167.216.8 203.119.213.128 TCP 54 34711 + 80 [ACK] Seq=429 Ack=653 Win=23348 Len=0

{
  "Member Key": "poi",
  "String value": "西安软件新城软件研发基地2期",
  "Key": "poi",
  "Member Key": "adcode",
  "String value": "610113",
  "Key": "adcode",
  "Member Key": "street",
  "String value": "云水一路",
  "Key": "street",
  "Member Key": "desc",
  "String value": "陕西省 西安市 雁塔区 天谷八路 靠近西安软件新城软件研发基地2期",
  "Key": "desc",
  "Member Key": "country",
  "String value": "中国",
  "Key": "country",
  "Member Key": "type",
  "String value": "2",
  "Key": "type",
  "Member Key": "location",
  "String value": "108.8344486,34.2069759",
  "Key": "location",
  "Member Key": "road",
  "Member Key": "radius",
  "String value": "30"
}

```

MAP 服务器下发的经纬度信息:

```

46 2020-01-06 20:48:32.632000 10.167.216.8 203.119.213.128 HTTP 482 GET /position?accesstype=1&imei=8cdna=0&smac=0&mmac=0&macs=a8:9c:ed:dc:74:2e,-83
47 2020-01-06 20:48:32.632000 203.119.213.128 10.167.216.8 TCP 54 80 → 34711 [ACK] Seq=1 Ack=429 Win=30016 Len=0
48 2020-01-06 20:48:32.666000 203.119.213.128 10.167.216.8 HTTP 705 HTTP/1.1 200 OK (application/json)
49 2020-01-06 20:48:32.695000 203.119.213.128 10.167.216.8 TCP 54 80 → 34711 [FIN, ACK] Seq=652 Ack=429 Win=30016 Len=0
50 2020-01-06 20:48:32.736000 10.167.216.8 203.119.213.128 TCP 54 34711 → 80 [ACK] Seq=429 Ack=653 Win=23348 Len=0

> Frame 46: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits)
> Ethernet II, Src: Gall1Mot_1e:38:c1 (00:50:4c:1e:38:c1), Dst: Infolibr_2c:10:58 (00:50:48:2c:10:58)
> Internet Protocol Version 4, Src: 10.167.216.8, Dst: 203.119.213.128
> Transmission Control Protocol, Src Port: 34711, Dst Port: 80, Seq: 1, Ack: 1, Len: 428
> Hypertext Transfer Protocol

> [truncated]GET /position?accesstype=1&imei=8cdna=0&smac=0&mmac=0&macs=a8:9c:ed:dc:74:2e,-83,TP-LINK[a8:9c:ed:dc:74:2e,-80,TP-LINK[26:40:bb:a4:9d:05,-99,TP-LINK[2a:6b:ada7:ac:55,-97,TP-LINK[2e:ea:1d:a3:6e:af,-96,TP-LINK&output=json
Host: apilocate.amap.com\r\n
User-Agent: Fibo-Module/1.0\r\n
Accept: text/html,*/*\r\n
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI [truncated]]: http://apilocate.amap.com/position?accesstype=1&imei=8cdna=0&smac=0&mmac=0&macs=a8:9c:ed:dc:74:2e,-83,TP-LINK[a8:9c:ed:dc:74:2e,-80,TP-LINK[26:40:bb:a4:9d:05,-99,TP-LINK[2a:6b:ada7:ac:55,-97,TP-LINK[2e:ea:1d:a3:6e:af,-96,TP-LINK&output=json
[HTTP request 1/1]
[Response in frame: 48]
TRANSMISSION DETAIL

```

注意：

目前 WIFI 定位只在高德 MAP 上实现。

请扣上 WIFI 天线测试。



7 FAQ

7.1 为何不考虑去重扫到的 WIFI 信息

MAC 的有效性决定 MAP 位置服务器是否能下发有效的经纬度信息，经常扫到无效 MAC，但模块无法知晓该 MAC 在服务器端是否有效，所以得扫到多个一并发给 MAP 位置服务器；但由于周边 WIFI 覆盖有限，不确定需要扫到多少个才上报给服务器。且扫 WIFI 时功耗会大大增加，所以优先考虑扫到一定个数而非达到一定时间才终止 WIFISCAN。

比如当前环境就 2 个 WIFI 覆盖，默认 10s 内扫到 5 个，一般情况下循环 all channel 扫一遍在两三秒内即可扫到这两个 WIFI，有时不确定是否有弱信号 WIFI 覆盖，一遍未能扫到，所以继续扫，再次扫到这两个则记录下来，再次扫则可达到设置的扫热点个数，几秒即可完成，没必要一直扫，这样设计对功耗有很大好处。

如果当前 WIFI 覆盖充足，扫一遍即可扫出多个，很容易达到设置的个数，亦不会有重复的。

7.2 为何要设置 GTSET

在实际使用中方便客户自由设置。

FIBOCOM
Confidential