



“探真” WiFi 无线嗅探设备 DS-003
成都数据天空科技有限公司

规格书

版本 1.0

2016 年 3 月 15 日

免责声明和版权公告

本文中的信息，包括供参考的 URL 地址，如有变更，恕不另行通知。

文档“按现状”提供，不负任何担保责任，包括对适销性、适用于特定用途或非侵权性的任何担保，和任何提案、规格或样品在他处提到的任何担保。本文档不负任何责任，包括使用本文档内信息产生的侵犯任何专利权行为的责任。本文档在此未以禁止反言或其他方式授予任何知识产权使用许可，不管是明示许可还是暗示许可。

Wi-Fi 联盟成员标志归 Wi-Fi 联盟所有。

文中提到的所有商标名称、商标和注册商标均属其各自所有者的财产，特此声明。

注 意

由于产品版本升级或其他原因，本手册内容有可能变更。成都数据天空科技有限公司保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，成都数据天空科技有限公司尽全力在本手册中提供准确的信息，但是成都数据天空科技有限公司并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

目录

- 1. 产品概述2
 - 1.1. 特点4
 - 1.2. 主要参数5
- 2. 接口定义6
- 3. 外型与尺寸8
- 4. 功能描述8
 - 4.1. 系统框图8
 - 4.2. 配置说明9
 - 4.2.1. 浏览器配置说明.....9
 - 4.2.2. PC 端软件配置说明9
 - 4.3. 数据格式11
 - 4.3.1. JSON 数据格式介绍11
 - 4.3.2. PHP 接收 API 程序实例.....13
 - 4.4. 探测技术14
- 5. 产品试用14

1. 产品概述

DS-003 WiFi 嗅探设备-“探真”，是由成都数据天空科技有限公司开发的，该设备采用双网卡设计。采用自主设计的双网卡架构，数据采集和网络传输并行进行，自主研发了高效率的全信道全协议采集算法，性能高于刷 openwrt 系统的路由器，采集效率和准确度国内领先，设备专门为大数据分析平台公司客户设计！！！！通过 PC 端或手机浏览器配置设备参数(设备连接的 WIFI,服务器 IP/域名和端口号等)，数据通过 http post 的方式发送给指定云服务器，效率高对接简单，数据内容丰富，不单单只是 mac 地址和信号强度！！我们提供的数据有：手机的 mac 和信号强度、手机距离探针设备的距离、手机是否连接 WIFI、手机连接的 WIFI 的 ssid 和 mac 地址、手机曾经连接的 WIFI 的信息、手机是否处于睡眠状态、探针设备的经纬度和地址等，设备已经大批量用于商场店铺地铁客流量统计、客户活动轨迹、热力图绘制、人员定位跟踪等，再配合我司专门研制的路由器(提供微信认证、短信认证等，实现 mac 地址和微信 ID、电话号码关联)和工业级路由器交换机，我司为您提供一整套的软硬件解决方案。

众所周知，大数据时代，数据的价值极高，我司承诺绝对不会将客户数据上传到我司服务器！！！！特别提醒：您采购一台设备就是采购一台采集数据的传感器，最好将数据保存到您自己的 PC 或者服务器，不要上传到其他公司的服务器！！！！

本公司产品已经成为工信部主办的“2017 中国软件杯大赛”A 组比赛项目指定参赛硬件：
<http://www.cnsoftbei.com/bencandy.php?fid=148&aid=1515>

核心处理器较小尺寸封装中集成了业界领先的 Tensilica L106 超低功耗 32 位微型 MCU，带有 16 位精简模式，主频支持 80 MHz 和 160 MHz，支持 RTOS，集成 Wi-Fi MAC/ BB/RF/PA/LNA，板载天线、外接天线。

该设备支持标准的 IEEE802.11 b/g/n 协议，完整的 TCP/IP 协议栈。该设备具有联网功能，也可以构建独立的网络，支持 AP/STA 模式共存。

Tensilica L106 是高性能无线 SOC，以最低成本提供最大实用性，为 WiFi 功能嵌入其他系统提供无限可能。

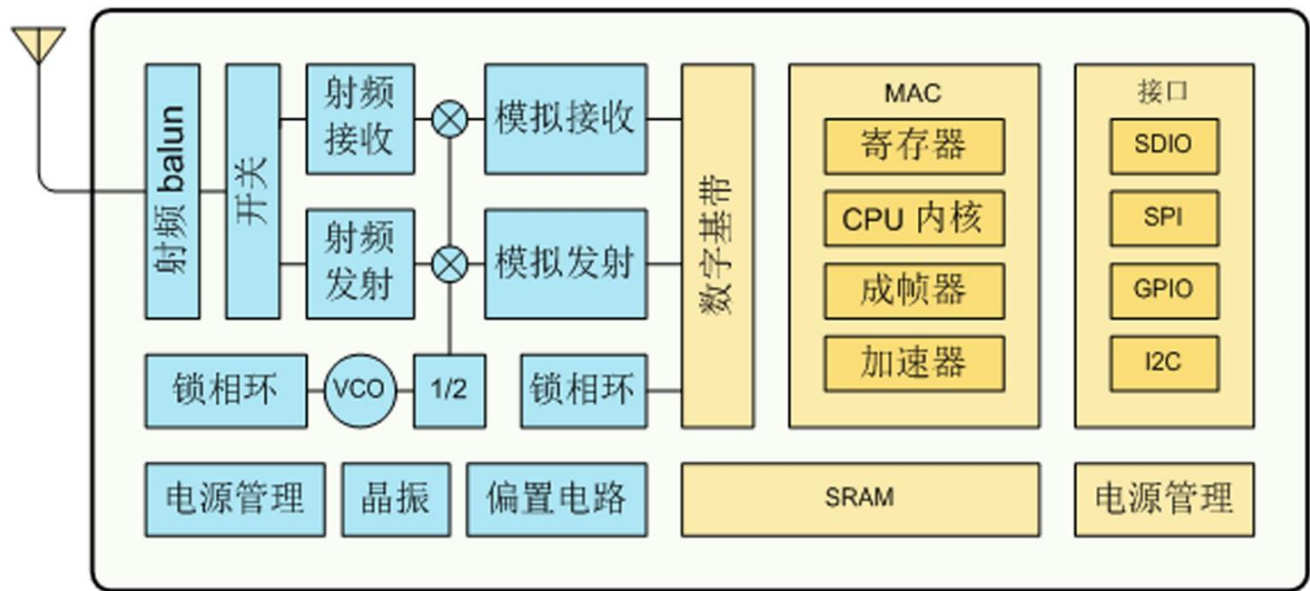


图 1 DS-003 探针设备 结构图

DS-003 嗅探设备是一个完整且自成体系的 WiFi 嗅探网络解决方案。DS-003 设备 SOC 直接从外接闪存中启动，并且内置高速缓冲存储器。

DS-003 高度片内集成，包括天线开关 balun、电源管理转换器，因此仅需极少的外部电路，且包括前端模组在内的整个解决方案在设计时将所占 PCB 空间降到最低。系统表现出来的领先特征有：节能在睡眠/唤醒模式之间的快速切换、配合低功率操作的自适应无线电偏置、前端信号的处理功能、故障排除和无线电系统共存特性为消除蜂窝/蓝牙/DDR/LVDS/LCD 干扰。

硬件架构方面，我司采用自主设计的双网卡架构，数据采集和网络传输并行进行，自主研发了高效率的全信道全协议采集算法，性能高于刷 openwrt 系统的路由器，采集效率和准确度国内领先，设备专门为大数据分析平台公司客户设计！！！！通过 PC 端或手机浏览器配置设备参数(设备连接的 WIFI,服务器 IP/域名和端口号等)，数据通过 http post 的方式发送给指定云服务器，效率高对接简单，数据内容丰富，不单单只是 mac 地址和信号强度！！我们提供的数据有：手机的 mac 和信号强度、手机距离探针设备的距离、手机是否连接 WIFI、手机连接的 WIFI 的 ssid 和 mac 地址、手机曾经连接的 WIFI 的信息、手机是否处于睡眠状态、探针设备的经纬度和地址等，设备已经大批量用于商场店铺地铁客流量统计、客户活动轨迹、热力图绘制、人员定位跟踪等，再配合我司专门研制的路由器(提供微信认证、短信认证等，实现 mac 地址和微信 ID、电话号码关联)和工业级路由器交换机，我司为您提供一整套的软硬件解决方案。

支持全信道、全协议采集 WIFI 数据，并集成我公司特有的采集算法，完成设备端的数据深度挖掘，为客户提供丰富而又价值的大数据信息。

1.1. 特点

- 802.11 b/g/n
- 内置 Tensilica L106 超低功耗 32 位微型 MCU , 主频 160 MHz
- 内置 TCP/IP 协议栈
- 内置 TR 开关、balun、LNA、功率放大器和匹配网络
- 内置 PLL、稳压器和电源管理组件 , 802.11b 模式下+20 dBm 的输出功率
- A-MPDU 、 A-MSDU 的聚合和 0.4 s 的保护间隔
- WiFi @ 2.4 GHz , 支持 WPA/WPA2 安全模式
- 支持 STA+AP 工作模式
- 2 ms 之内连接并传递数据包
- 工作温度范围 : -40°C- 125°C
- 加密类型 : WEP/TKIP/AES
- 数据上报格式 : http post json 数据
- 传输方式 : WIFI 网络(本产品)、以太网、本地存储、GPRS (公司其他产品)
- 配置方式 : PC/手机端软件配置(本产品)、web 网页配置 (其他)

1.2. 主要参数

表 1 介绍了该模组的主要参数。

表 1 参数表

类别	参数	说明
无线参数	无线标准	802.11 b/g/n
	频率范围	2.4GHz-2.5GHz (2400M-2483.5M)
	数据接口	UART/HSPI/I2C/I2S/Ir Remote Contorl
硬件参数	工作电压	GPIO
		3.0~3.6V (建议 3.3V)
	工作电流	平均值： 80mA
	工作温度	-40°~125°
	存储温度	常温
	封装大小	18mm * 20mm * 3mm
	外部接口	N/A
	无线网络模式	AP+station
软件参数	安全机制	WPA/WPA2
	加密类型	WEP/TKIP/AES
	升级固件	本地串口烧录 / 云端升级 / 主机下载烧录
	软件开发	支持客户自定义服务器
	网络协议	TCP/HTTP
	用户配置	PC 软件,WEB 界面, 云端服务器, Android APP

2. 接口定义

DS-003 共接出 4 个接口，表 2 是接口定义。

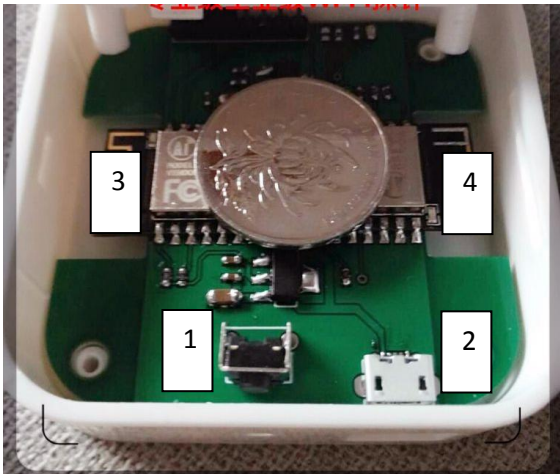


图 2 DS-003 设备实物图

表 2 DS-003 接口功能定义

序号	名称	功能说明
1	复位按键	复位设备等
2	Micro USB	供电电源，5V/1A
3	采集网卡	专用采集数据
4	传输网卡	传输数据、服务器通信、保存配置等

表 3 网卡接收灵敏度

参数	最小小值	典型值	最大值	单位
输入频率	2412		2484	MHz
输入电阻		50		Ω

DS-003 WIFI 嗅探设备说明书

输入反射			-10	dB
72.2 Mbps 下, PA 的输出功率	14	15	16	dBm
11b 模式下, PA 的输出功率	17.5	18.5	19.5	dBm
灵敏度				
DSSS, 1 Mbps		-98		dBm
CCK, 11 Mbps		-91		dBm
6 Mbps (1/2 BPSK)		-93		dBm
54 Mbps (3/4 64-QAM)		-75		dBm
HT20, MCS7 (65 Mbps, 72.2 Mbps)		-72		dBm
邻频抑制				
OFDM, 6 Mbps		37		dB
OFDM, 54 Mbps		21		dB
HT20, MCS0		37		dB
HT20, MCS7		20		dB

3. 外型与尺寸

DS-003 WIFI 嗅探设备的外观尺寸为 60mm * 60mm * 15mm (如图 3 所示)



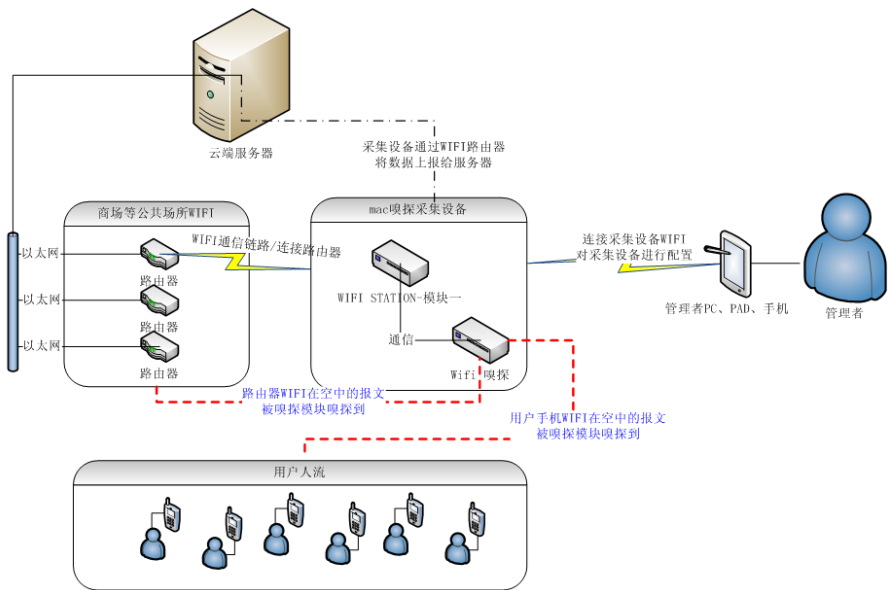
图 3 DS-003 设备外观

表 4 DS-003 尺寸对照表

长	宽	高
60mm	60mm	15 mm

4. 功能描述

4.1. 系统框图



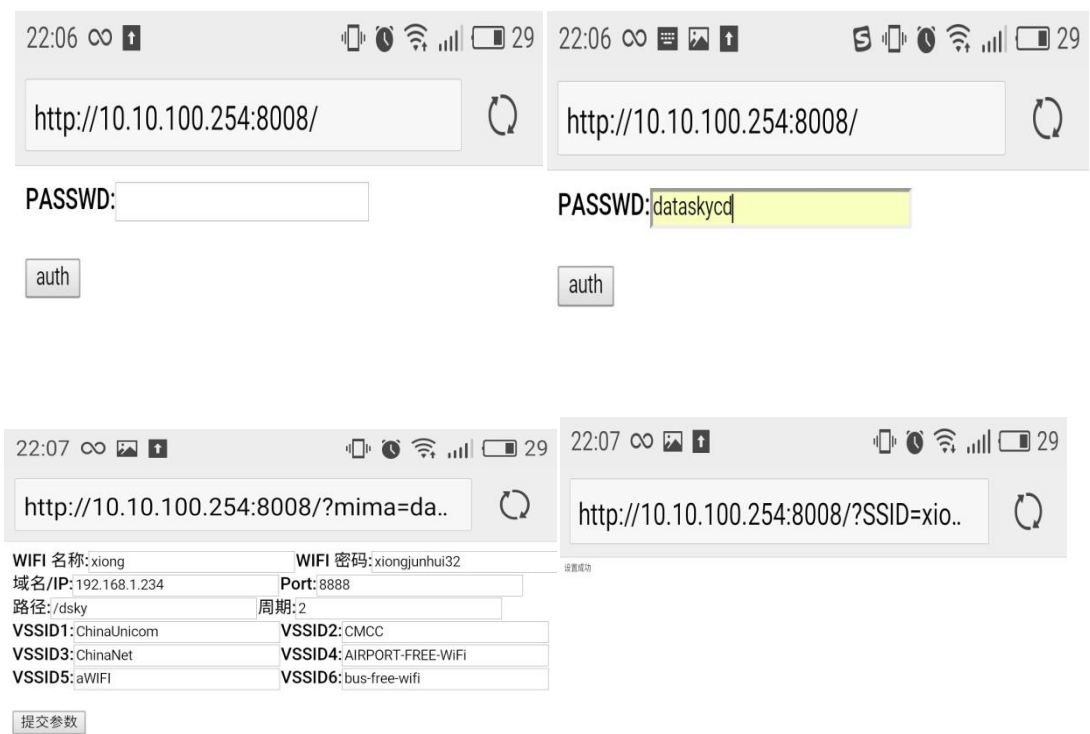
上图展示的是 DS_003 型嗅探器，通过路由器 WIFI，上传采集数据到云服务器的系统框图。另外，用户还可以通过 PC 直接连接嗅探器本身的 AP，并在 PC 机端本地布置小型服务器，PC 和嗅探器组成局域网，将数据直接上传到 PC 端服务器，实现本地存储数据、分析数据等功能，此方法可替代使用 U 盘或者通过串口上传数据到 PC 等存储数据的功能。

4.2. 配置说明

DS_003 型探针支持 PC 端客户端配置和浏览器配置。其中浏览器配置相对比较简单方便，可以用手机或者电脑，推荐客户使用浏览器配置。

4.2.1. 浏览器配置说明

如下图所示(手机浏览器)：首先将设备上电，打开手机 WIFI，连接探针 KT_XXXX 这个热点(XXX 为探针的 ID)， 密码:88888888，然后打开浏览器，输入 10.10.100.254:8008，会看到图一的界面，在编辑框中填写密码:dataskycd 然后点击 auth。认证通过后出现如下界面，填写配置信息，然后点击提交参数，参数设置成功后会出现：“设置成功” 界面。等待 1-2s 设备会自动重启，然后参数奏效。手机 PC 都可以用，支持中文不支持空格字符。



4.2.2. PC 端软件配置说明

DS-003 WIFI 嗅探设备说明书



WIFI SSID：要连接的路由器热点名称

WIFI 密码：要连接的路由器热点密码

IP：四个编辑框，填写服务器 IP

域名：服务器的域名，例如 www.baidu.com

端口号：服务器的应用程序对应的端口号

路径：http post 路径，如 post 的 url 为 http://1.1.1.1:1234/mac，则路径配置为/mac

MAC 上报周期：单位为 s

读参数按钮：读取系统参数

写参数按钮：将参数设置到模块中

升级按钮：用于模块升级

使用方法：首先将模块上电(电源 5v)，之后 PC 端 WIFI 搜索名为 KT_XXX(XXX 为此设备 ID)的 WIFI 热点，点击连接，密码为 88888888，WIFI 连接成功之后，打开 PC 端配置软件，点击读参数。读取成功，然后将 WIFI SSID、WIFI 密码、TCP 服务器 IP 地址、MAC 地址上报周期填写好之后，点击写参数，写成功之后会弹出 set config 成功的对话框，点击确定。至此，参数设置成功。

4.3. 数据格式

4.3.1. JSON 数据格式介绍

数据格式为 JSON 格式，如下所示：

```
data={  
    "id": "0010f377", //嗅探器设备 id  
    "mmac": "5e:cf:7f:10:f3:77", //嗅探器设备自身 WiFi mac  
    "rate": "1", //发送频率  
    "wssid": "kaituo", //嗅探器设备连接的 WIFI 的 ssid  
    "wmac": "a8:57:4e:c0:d4:8c", //嗅探器设备连接的 WIFI 的 mac 地址  
    "time": "Sat Jun 04 22:45:28 2016", //时间戳，采集到这些 mac 的时间  
    "lat": "30.748093", //北半球，纬度  
    "lon": "103.973083", //经度  
    "addr": "四川省成都市郫县犀浦镇两河新街;围城南路与兴业南街路口东 581 米", //地址信息  
    "data": [{  
        "mac": "9a:21:6a:7b:62:6a", //采集到的手机 mac 地址  
        "rssi": "-75", //rssi，手机的信号强度，如 rssi=-75,则信号强度为-75dbm  
        "ts": "hello", //目标 ssid，手机连接的 WIFI 的 ssid  
        "tmc": "00:01:02:03:04:05", //目标设备的 mac 地址，手机连接的 WIFI 的 mac  
        "tc": "Y", //是否与路由器相连  
        "ds": "N", //手机是否睡眠  
        "ssid0": "七天连锁_wifi", //手机用户 9a:21:6a:7b:62:6a 曾经连接过的 WIFI 的  
        "ssid1": "工商银行", //手机用户 9a:21:6a:7b:62:6a 曾经连接过的 WIFI 的 SSID  
        "ssid2": "东方明珠",  
        "ssid3": "home",  
        "ssid4": "abcd",  
    }]  
}
```

DS-003 WIFI 嗅探设备说明书

```
        "ssid5":"xiong",
        "ssid6":"XX 会馆"
    }, {
        "mac": "1c:31:72:5c:83:6b",
        "rssi": "-65",
        "ts": "world",
        "tmc": "00:01:02:03:04:06",
        "tc": "Y",
        "ds": "Y",
        "ssid0": "七天连锁_wifi">//手机用户 9a:21:6a:7b:62:6a 曾经连接过的 WIFI 的
SSID
        "ssid1": "工商银行">//手机用户 9a:21:6a:7b:62:6a 曾经连接过的 WIFI 的 SSID
        "ssid2":"东方明珠",
        "ssid3":"home",
        "ssid4":"abcd",
        "ssid5":"xiong",
        "ssid6":"XX 会馆"
    }
}
```

另外为了减少不必要的流量浪费，特别对上述数据结构进行了优化，**特别说明如下**：

1，**ts、tmc、tc 三个字段**表示手机连接的 WIFI ssid,手机连接的 WIFI 的 mac 地址，手机是否连接此 wifi，如果手机没有连接 WIFI，之前的处理方法是 ts 为空，后面的 tmc 为空，tc 为 N，这样实际造成了数据浪费，现在做如下优化，如果手机没有连接 WIFI，则不发送 ts,tmc 和 tc 字段。服务器收到此三个字段为空，则表示手机没有连接路由器 WIFI

2，**ds 字段**表示手机是否睡眠，之前设计如果睡眠则为 Y，否则为 N，现在优化为如果睡眠为 Y，否则不发送 ds 字段，服务器收到此字段为空，则表示手机没有处于睡眠状态。

3，**ssid 字段**(early wifi ssid)表示手机曾经连接过的 WIFI 名称，如果有一个则增加字段 ssid0,如有 7 个则增加字段 ssid0,ssid1,ssid2,ssid3,ssid4,ssid5,ssid6。目前强制最多有 7 个 ssid。所以服

务在收到 json 后，如果没有 essid0 字段则表示没有获取到此手机曾经连接的 WIFI，服务器可通过遍历 essid0-ssid6 来判断有几个 ssid

4, 经纬度和地址信息, 这三个字段, lat 表示纬度, lon 表示经度, addr 表示对应的地址, 地址为中文显示, 编码格式为 UTF-8, 这三个字段也有可能为空(当探针没有找到位置时), 定位精度实测在 0-50 米范围内。

5, 为了节省流量尽可能的传输数据, JSON 格式是 unformatted 格式。

4.3.2. PHP 接收 API 程序实例

```
<?php
require ('connect.php');

/*
本例用到的数据:
data={"id":"0029c591","mmac":"5e:cf:7f:29:c5:91","rate":"1","wssid":"datasky1","wmac":"00:0c:43:76:20:59","time":"Tue Feb 21 08:13:31 2017",
"lat":"30.747988","lon":"103.973152","addr":"四川省成都市郫县犀浦镇两河新街;围城南路与兴业南街路口东","data":[{"mac":"a4:56:02:61:7f:57","rssi":"-91",
"range":"91.5"},{"mac":"8c:a6:df:62:2d:3d","rssi":"-93","range":"108.5"},{"mac":"a4:56:02:71:be:b3","rssi":"-96","range":"140.1"},{"mac":"cc:34:29:97:4d:0d",
"rssi":"-95","range":"128.6"},{"mac":"44:33:4c:aa:71:82","rssi":"-94","range":"118.1"},{"mac":"b0:48:7a:5a:10:f8","rssi":"-86",
"range":"59.7"},{"mac":"a8:57:4e:9d:ca:d8","rssi":"-96","range":"140.1"},{"mac":"5e:cf:7f:93:3d:0e","rssi":"-56","range":"4.6"},{"mac":"5e:cf:7f:93:3d:0f",
"rssi":"-58","range":"5.5"},{"mac":"5e:cf:7f:93:3d:10","rssi":"-63","range":"8.4"},{"mac":"5e:cf:7f:93:3d:0b","rssi":"-68",
"range":"12.9"},{"mac":"5e:cf:7f:93:3d:0c","rssi":"-53","range":"3.5"},{"mac":"5e:cf:7f:93:3d:0d","rssi":"-69","range":"14.0"},{"mac":"e4:f3:f5:24:2c:d8",
"rssi":"-89","range":"77.1"},{"mac":"14:cf:92:8a:8f:f0","rssi":"-96","range":"140.1"}]}POST /dsky HTTP/1.0*/
$ddata=$_POST['data'];

/--解析 Json, 获取对应的变量值
$obj=json_decode($data, json_unescaped_unicode);
$id = $obj['id'];
$mmac = $obj['mmac'];
$rate = $obj['rate'];
$wssid = $obj['wssid'];
$wmac = $obj['wmac'];
$time = $obj['time'];
$lat = $obj['lat'];
$lon = $obj['lon'];
$addr = $obj['addr'];
$detail_data = $obj['data'];

$i=0;//循环变量

/--得到 Json_list 数组长度
$num=count($obj["data"]);

/--遍历数组, 将对应信息输出
for ($i;$i<$num;$i++)
{
    $mac=$detail_data [$i]["mac"];
    $rssi=$detail_data [$i]["rssi"];
    $range=$detail_data [$i]["range"];
    $ts=$detail_data [$i]["ts"];
    $tmc=$detail_data [$i]["tmc"];
    $tc=$detail_data [$i]["tc"];
    $ds=$detail_data [$i]["ds"];
}
```

```
$ssid1=$detail_data [$i] ["ssid1"];  
$ssid2=$detail_data [$i] ["ssid2"];  
$ssid3=$detail_data [$i] ["ssid3"];  
$ssid4=$detail_data [$i] ["ssid4"];  
$ssid5=$detail_data [$i] ["ssid5"];  
$ssid6=$detail_data [$i] ["ssid6"];  
}  
  
?>
```

4.4. 探测技术

The screenshot shows a configuration window for the DS-003 WIFI sniffing device. It is divided into two main sections: 'WIFI参数区' (WIFI Parameter Area) and '系统升级' (System Upgrade). The 'WIFI参数区' contains several input fields: 'WIFI SSID', 'WIFI 密码' (WIFI Password), 'MAC上报周期' (MAC reporting period) with a value of 0, 'IP' (IP address) with a value of 0.0.0.0, '域名' (Domain), '端口号' (Port number) with a value of 0, '路径' (Path), and six 'VSSID' fields (VSSID1 through VSSID6). There is a checkbox labeled '选用IP (选中表示使用IP, 否则使用域名)' (Select IP (selected means use IP, otherwise use domain)). Below these fields are two buttons: '读参数' (Read Parameters) and '写参数' (Write Parameters). The '系统升级' (System Upgrade) section includes a text box for the upgrade file, a button labeled '选择固件所在目录' (Select the directory where the firmware is located), and a button labeled '升级' (Upgrade).

DS-003WIFI 嗅探设备可配置多达 6 个伪基站，这六个伪基站可以采用主动探测的方式，将不主动发送 WIFI 报文的设备(如苹果)唤醒，诱导手机主动连接伪基站，实现主动探测的功能，通过主动探测技术和被动探测相结合的方式，再加上我司独有的探测算法，经过一年多的市场检验，产品稳定性达到 99.999%，探测效率达到 98%。

成都数据天空科技有限公司专注大数据传感设备设计，为客户提供性能可靠稳定的软硬件设备，致力于探测端的数据深度挖掘，为客户提供更多更有价值的数据信息，线下大数据传感设备专业供应商，专业的才是精品的！！请认准 DataSky 成都数据天空科技有限公司！！！！

5. 产品试用

- (1) 淘宝店铺：DataSky
- (2) 技术支持邮箱：742227326@qq.com ；电话：13708042153

DS-003 WIFI 嗅探设备说明书

(3) 本文档适用于本公司所有使用 WIFI 传输数据的设备