

Sniffer 使用手册

本文档描述了 Sniffer 程序的使用方法。Sniffer 是一个无线传感器网络监听分析程序，目前发布版需要在安装 Windows 系统的 PC 上使用；使用时要配合一个被监听网络节点相同的硬件节点（以下称为 Sniffer 节点），该节点烧录了特殊的固件可以接收任意节点发送的数据包并转发到 PC。

需注意的是，**Sniffer 节点只能监听到通讯范围内的节点的数据**，如果某些节点距离过远，其数据将不能被接收到，需要诊断这样的节点时，需将 Sniffer 节点移动到其通讯范围内。此外，如果网络中短时间内有过多的数据收发，Sniffer 节点可能无法接收并转发所有的数据。

一. 硬件准备

- 准备一个 WVDS 系统 VD 节点和一个 USB 转 TTL 模块（建议使用可给节点供电的模块，Sniffer 节点一直处于射频接收状态，用电池供电时间久了经常需要更换）；
- 使用 IAR 编译烧录 apps\sniffer 应用程序，或者用其他软件直接烧录对应的.d43/.txt 文件；
- 将 VD 节点和串口模块类似图 1 进行连接，USB 端再接网络监视用的 PC；

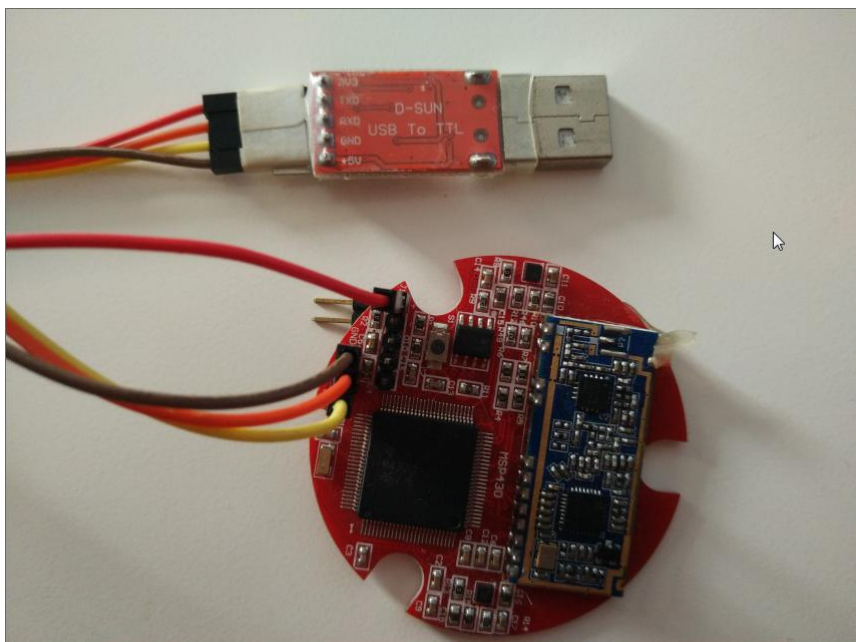


图 1 Sniffer 节点连接

二. 软件使用

2.1. 启动软件

解压缩 Sniffer GUI 软件后，包含的文件如图 2 所示，双击 sniffer.vbs 或 sniffer.exe 启动软件。如果想查看控制台输出或诊断无法正常运行问题，可双击 sniffer.bat 启动软件。

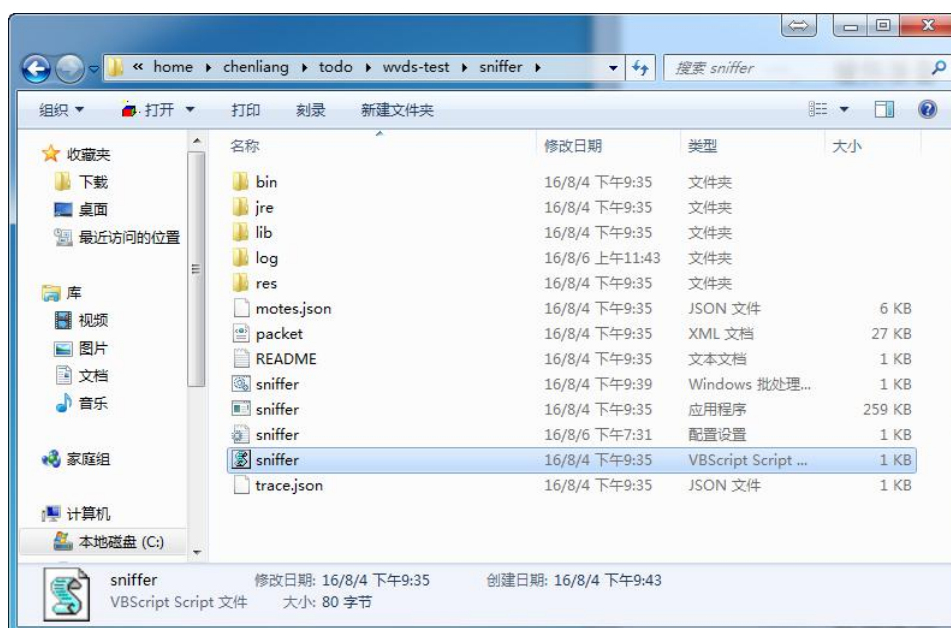


图 2 Sniffer GUI 文件列表

软件启动后出现如图 3 的选择窗口，请查看“设备管理器”确定前述串口模块对应的串口号并正确选择。波特率应保持为 115200。



图 3 Sniffer 串口选择

2.2. 软件使用

Sniffer GUI 软件启动后出现如图 4 的主界面：

- 菜单栏【帮助】-【帮助】，点击后将打开帮助手册 pdf 文件；
- 菜单栏【帮助】-【关于】，点击后显示 GUI 程序版本和 Sniffer 节点固件版本；
- 工具栏【编辑】，点击后将用记事本打开消息解析定义文件 packet.xml；
- 工具栏【重载】，点击后重新加载经修改的消息解析定义文件 packet.xml；
- 工具栏【清除】，点击后清除各标签页中的当前显示数据；
- 工具栏【重放】，点击后将弹出文件选择对话框，选择某个日志文件后将重放显示其中的数据；
- 工具栏【管理】，点击后可编辑各节点的名称；
- 工具栏【退出】，点击后退出 Sniffer GUI 程序。

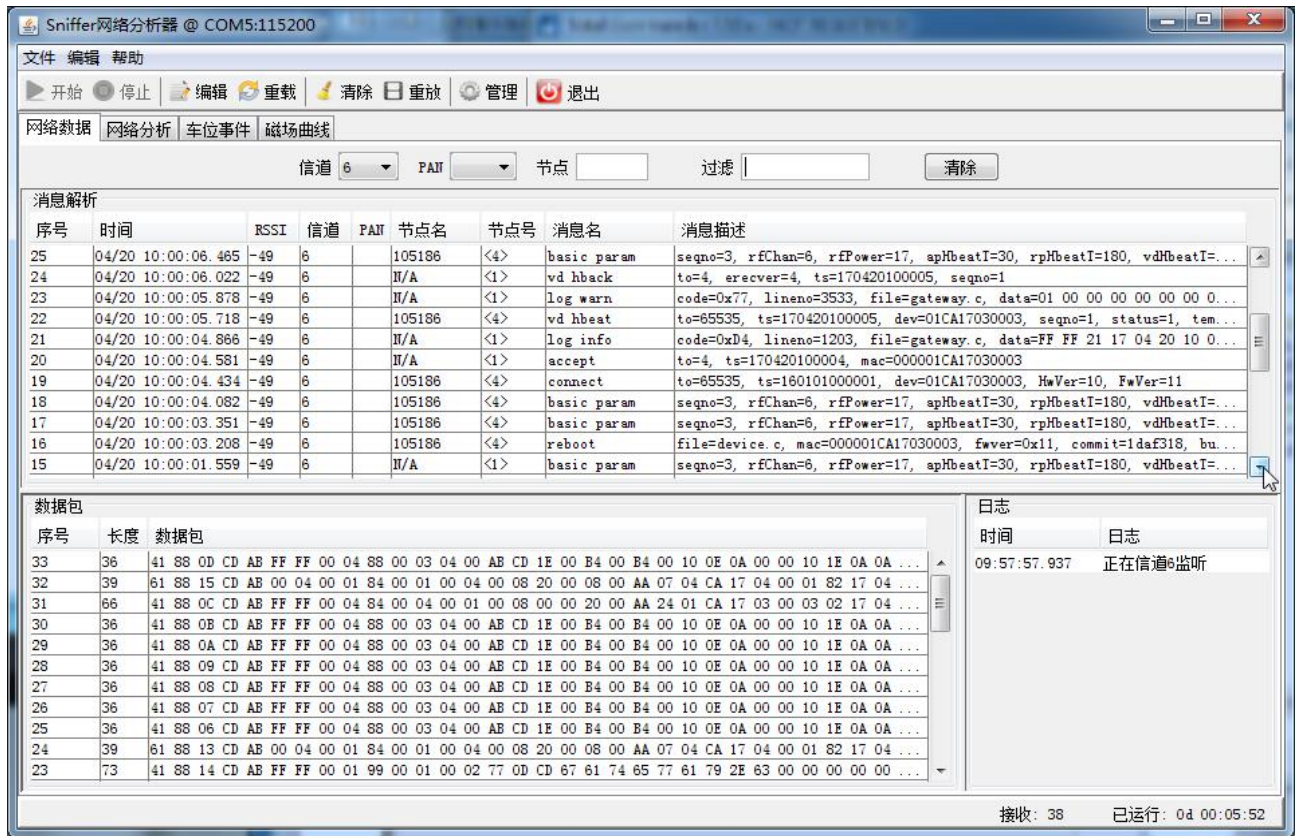


图 4 Sniffer 主界面

主界面中主要是两个数据表格，上方是经过解析后的数据包，以易读形式展示了重要的消息字段的取值，下方是原始数据包，以字节串的形式展示，是有效载荷部分经过 AES 解密后的 802.15.4 数据帧。右下角是 Sniffer 程序本身相关的控制台输出，例如 Sniffer 节点重启或改变信道将在该表格中有提示。

2.2.1. 消息解析表

上方“消息解析”表格是使用中需主要关注的，它的数据列见表 1 说明。

列名称	说明
序号	数据包的接收序号。与下表一一对应，点击上表某行可查看对应下表的原始数据包行。
时间	数据包的接收时刻。准确来说是 GUI 软件的接收时刻，与监听节点的准确接收时刻一般差别不大。
RSSI	监听节点接收该行对应的数据包时测得的信号强度，以 dBm 为单位。
信道	当前行数据包所属的射频信道号。
PAN	子网(PAN)号，区分不同的子网。目前未使用。
节点名	网络节点的名称，比节点号易于对应到相应的节点。
节点号	网络节点的短地址。节点使用该 16 位短地址进行数据收发和中转。
消息名	当前行对应的网络消息的名称。由该无线网络系统的协议定义，便于根据名称快速了解该消息的类型和作用。
消息描述	当前行对应的网络消息的具体内容。具体显示的内容是根据下表中的原始数据包和对应的消息定义自动解析出来的，所有的消息定义在 packet.xml 中。

表 1 “消息解析”表的数据列

2.2.2. 网络协议分析

无线网络协议分析的主要方法就是根据“消息解析”表格中的内容判断网络节点的工作状态，需要掌握各消息的含义和相关的流程。目前使用到的消息列表如下：

消息名	关键字段	说明
connect	VD 和 RP 向 AP 发送以请求加入其管辖的子网	
	dev	该节点的设备编码
	HwVer	硬件版本号
	FwVer	软件版本号
accept	AP 向某 VD 或 RP 发送允许其加入自己的子网	
	ts	时间戳，供节点修正本地时间
	MAC	允许加入的节点的 MAC 地址
assign	AP 向某 VD 或 RP 发送让其更改短地址为所分配的值	
	MAC	被分配新地址的节点的 MAC 地址
	addr	新分配的短地址
reject	AP 向某 VD 或 RP 发送拒绝其加入网络	
	MAC	被拒绝入网的节点的 MAC 地址
	reason	拒绝入网的原因
park evt	VD 检测到其所在泊位的状态改变时向 AP 发送	
	status	泊位状态
park ack	AP 接收到某 VD 的 park evt 消息后向该 VD 发送	
vd hbeat	VD 每隔一个心跳周期向 AP 发送，未收到 ACK 短时间后再发送	
	ts	时间戳
vd hback	AP 接收到某 VD 的 vd hbeat 消息后向该 VD 发送	
rp hbeat	RP 每隔一个心跳周期向 AP 发送，未收到 ACK 短时间后再发送	
	ts	时间戳
rp hback	AP 接收到某 RP 的 rp hbeat 消息后向该 RP 发送	
basic param	AP/RP/VD 不定期发送，包括节点当前使用的网络参数	
	apHbeatT	AP 节点的心跳周期，以秒为单位
netcmd req	VD 节点每隔一个下行命令轮询周期发送，向父节点询问是否有对应命令	
	to	下行命令请求的目标节点
netcmd cmd	AP 或 RP 缓存有给某 VD 的命令时向该 VD 发送	
	more	后续是否还有更多给该 VD 的数据
	seqno	下行命令序列号
	dest	下行命令的目标地址
netcmd ack	VD 接收到下行命令时向父节点发送，告知已成功接收	
	seqno	下行命令序列号，与接收的 netcmd cmd 相同
alarm	VD/RP 检测到节点存在硬件故障或电压低等问题时向 AP 发送	
	battery	电池电压是否正常
log info	AP/RP/VD 程序运行到某些关键正常代码时发送，用于了解生产环境网络情况	
	lineno	行号，该行调试代码所在行
	file	该行调试代码所在的源码文件名
	data	该行调试代码附带的一些变量值

log warn	AP/RP/VD 程序运行到警告代码时发送，有些情况需要对程序进行修正
log error	AP/RP/VD 程序运行到错误代码时发送，需要对程序进行相应修正

表 2 网内无线消息列表

根据表 2 和相关的流程，我们可以形成下表的一些网络诊断结论：

现象	可能问题	解决操作
某节点上电后未监听到任何数据	上电有问题	重新上电
	射频损坏	返厂测试
某节点总在发送 connect 消息，AP 已发送对应的 accept 消息	VD 射频接收存在问题，可能和天线或信道有关	1. 检查天线 2. 用 sniffer 监听测试该 VD 所在位置是否下行通信存在问题
有车辆驶入或离开时未发送 park evt 消息	算法检测或程序运行出错	再次尝试，如果多次均未检测到，为程序运行出错，尝试重新上电
	传感器故障	后台应收到对应报警消息
周期性发送的消息如 vd/rp hbeat、netcmd req、basic param 长时间未发送	程序运行出错	重新上电
某节点之前在正常工作，某个时刻后长时间再无任何消息收发	电池已用完或供电故障	重新上电仍然无法正常工作，更换电池
	程序运行出错死机	重新上电，上电后能正常工作则确认是软件死机

2.2.3. 消息过滤

当网络中有较多的节点和较多的数据收发时，消息解析表格中不断滚动的最新数据无法让人查看关心的节点或消息，此时可以在“过滤”文本框中输入某些关键字查看特定消息。一些常用的关键字列表如下供参考：

关键字	作用
消息名如 park evt	过滤出特定类型的消息，比如输入 park evt 关键字后，可以方便地查看某节点在车辆出入时是否发送了对应的消息
设备编码或其一部分如 01CA16080006 或 80006	查看特定节点的相关消息。注意不是所有消息均显示 dev 字段，因此可能有些消息过滤后未显示。
时间戳如 160808222653	查看某个时间戳的消息。可用于检查是否有对应 ACK 消息等
warn 或 error	查看运行中出错的情况
lineno=xxx	查看某些行的运行调试消息

特别地，在“节点”文本框中输入某个节点的节点号如 10，则表格中只显示该节点发送的相关数据。

2.3. 自动网络分析

2.3.1. 节点管理

点击工具栏“管理”按钮会弹出如图 5 的界面，可以配置某个设备编码对应的车位号，便于在其他标签页中查看某车位对应的数据。



图 5 节点管理

在“车位号”列点击某一行按 F2，可以编辑对应的车位号，改后按“保存”按钮。

2.3.2. 网络分析

切换到“网络分析”标签页时，将会出现如图 6 的界面，在该界面中将会随着监听的网络数据的输入更新相关的状态指示和统计数据等。目前只支持简单的统计分析。各表格均可以点击表格头按某列进行排序。在 VD 表格中，对车位事件和射频状态特别使用不同的颜色来显示，便于快速识别其状态变化。



图 6 网络分析标签

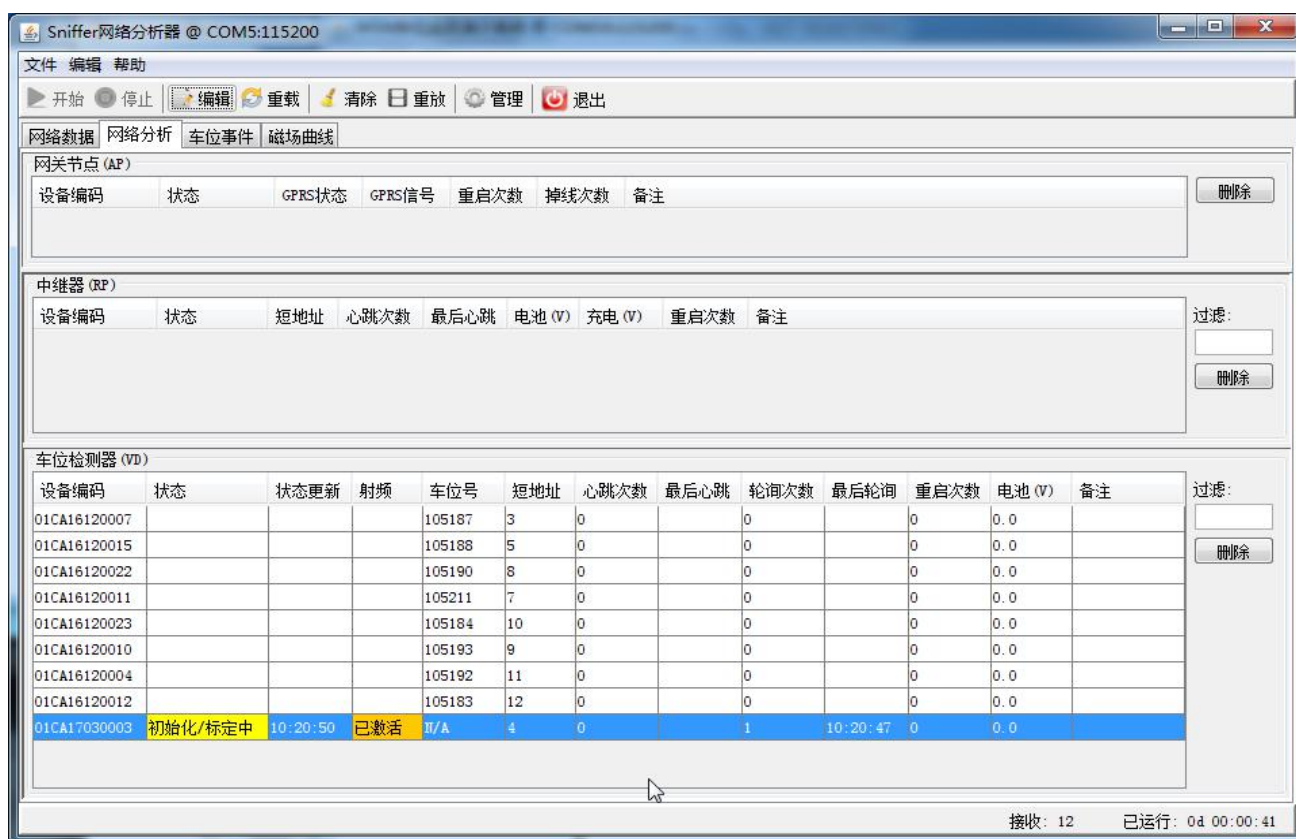


图 7 VD 正在重新标定

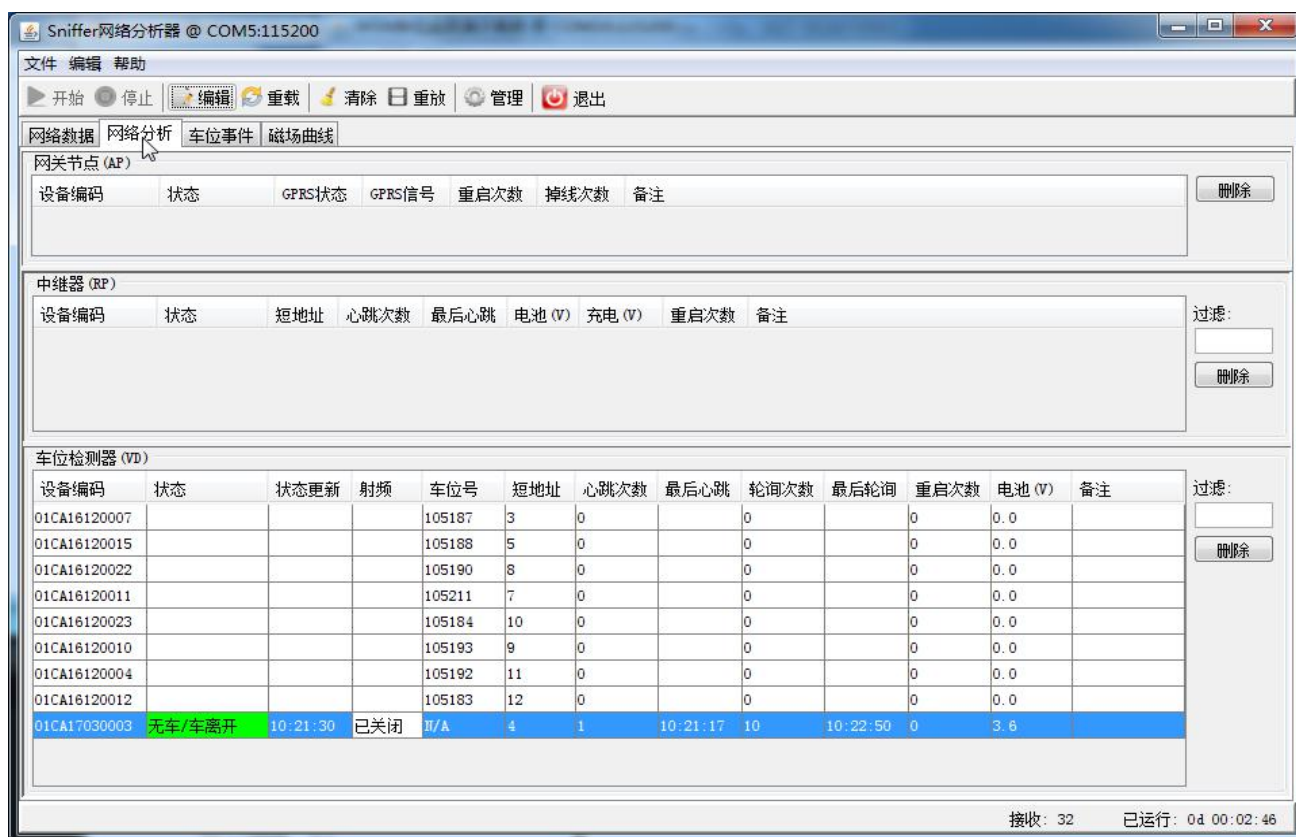
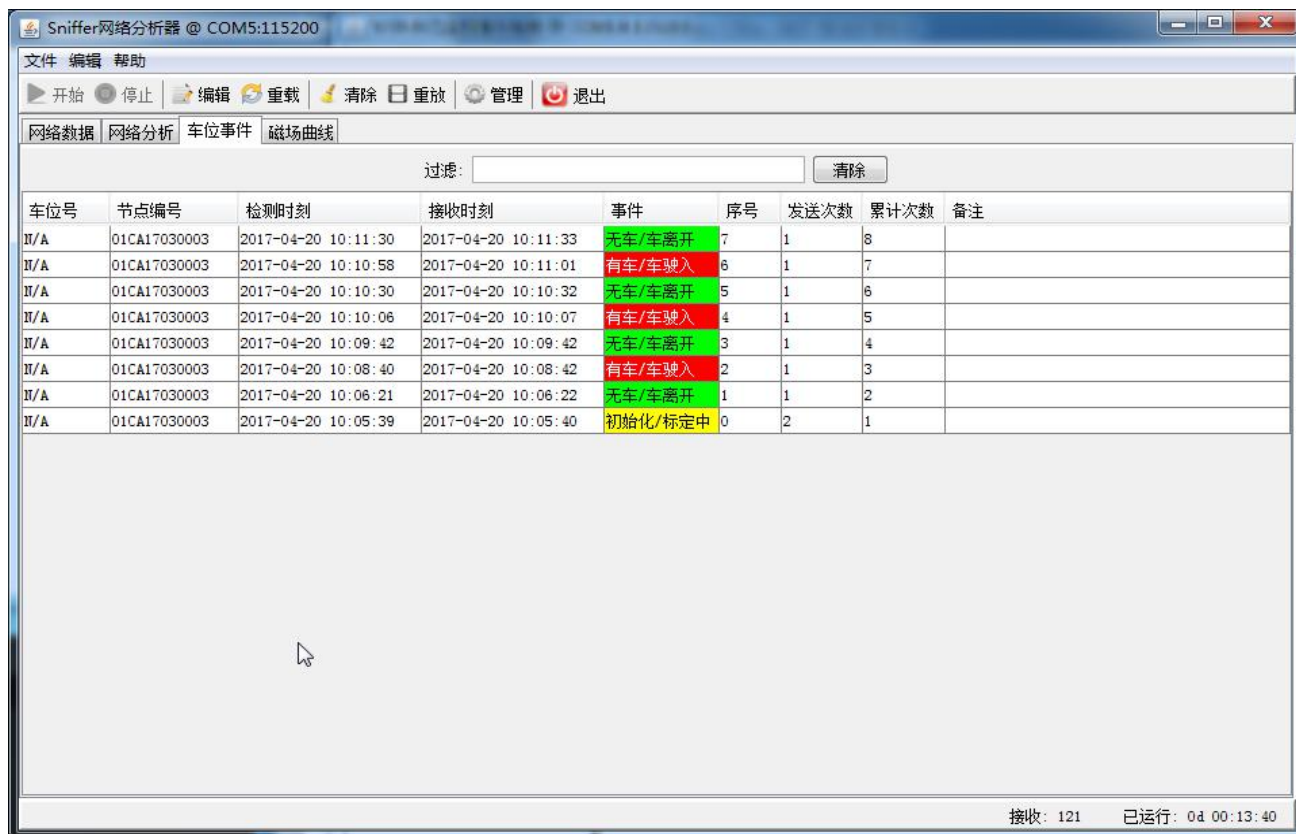


图 8 VD 完成标定且关闭射频

2.3.3. 车位事件

“车位事件”标签页将对监听到的泊位事件消息（即前述消息列表中的 `park evt` 消息）进行统计，以便

了解车辆出入的次数和时间等统计数据。通过颜色显示更能快速识别各行数据对应的车位状态。



车位号	节点编号	检测时刻	接收时刻	事件	序号	发送次数	累计次数	备注
II/A	01CA17030003	2017-04-20 10:11:30	2017-04-20 10:11:33	无车/车离开	7	1	8	
II/A	01CA17030003	2017-04-20 10:10:58	2017-04-20 10:11:01	有车/车驶入	6	1	7	
II/A	01CA17030003	2017-04-20 10:10:30	2017-04-20 10:10:32	无车/车离开	5	1	6	
II/A	01CA17030003	2017-04-20 10:10:06	2017-04-20 10:10:07	有车/车驶入	4	1	5	
II/A	01CA17030003	2017-04-20 10:09:42	2017-04-20 10:09:42	无车/车离开	3	1	4	
II/A	01CA17030003	2017-04-20 10:08:40	2017-04-20 10:08:42	有车/车驶入	2	1	3	
II/A	01CA17030003	2017-04-20 10:06:21	2017-04-20 10:06:22	无车/车离开	1	1	2	
II/A	01CA17030003	2017-04-20 10:05:39	2017-04-20 10:05:40	初始化/标定中	0	2	1	

图 9 车位事件列表

该表格中各列的作用如下：

- “序号”列是 park evt 数据包的序号，如果出现跳跃，如 8 后就是 10，是 sniffer 没有监听到 9，应该是 VD 进行了对应的发送；
- “发送次数”列是该序号的数据包发送了多少次，在通信较差或冲突情况下可能发送多次；
- “累计次数”列是 Sniffer 启动后该节点到该行为止事件消息的累计个数（不含重复发送）。

2.3.4. 磁场曲线

“磁场曲线”标签页根据接收到的多种类型消息绘制磁场数据的曲线，以便直观了解某点磁场 3 轴数据的变化情况。

标签页上方有以下控制组件：

- “节点下拉框”中选择某个节点，则曲线图中将切换显示该节点的数据；
- “节点过滤文本框”中输入设备编码或车位号的部分数字，会自动以该输入为过滤关键字更新节点下拉框中的节点列表，以便在节点较多时快速查找到并查看某节点的数据；
- 对某些消息，“状态”将显示当前查看节点的车位状态；
- “数据系列”有 3 轴对应的复选框组，选中或不选中某复选框将切换对应轴磁场数据在曲线中的显示。

标签页下方有对曲线图的控制组件：

- “标识”复选框切换是否显示曲线图上的数据点；
- “实心”复选框切换是否填充数据点；
- “X 滚动”复选框切换 X 轴超过当前显示范围时自动调整，右侧文本框可改变 X 轴的显示时长范围；
- 当“X 滚动”不选中时，在“X 下限”和“X 上限”文本框中修改可直接设置查看数据的时长范围；

- 在“Y 下限”和“Y 上限”文本框中修改可调整 Y 轴的数据范围；
- 在曲线图内可以通过鼠标拖动来放大或缩小曲线图，在缩放之后可以按“重置”按钮根据 X 上下限、Y 上下限恢复到未缩放前的视图。

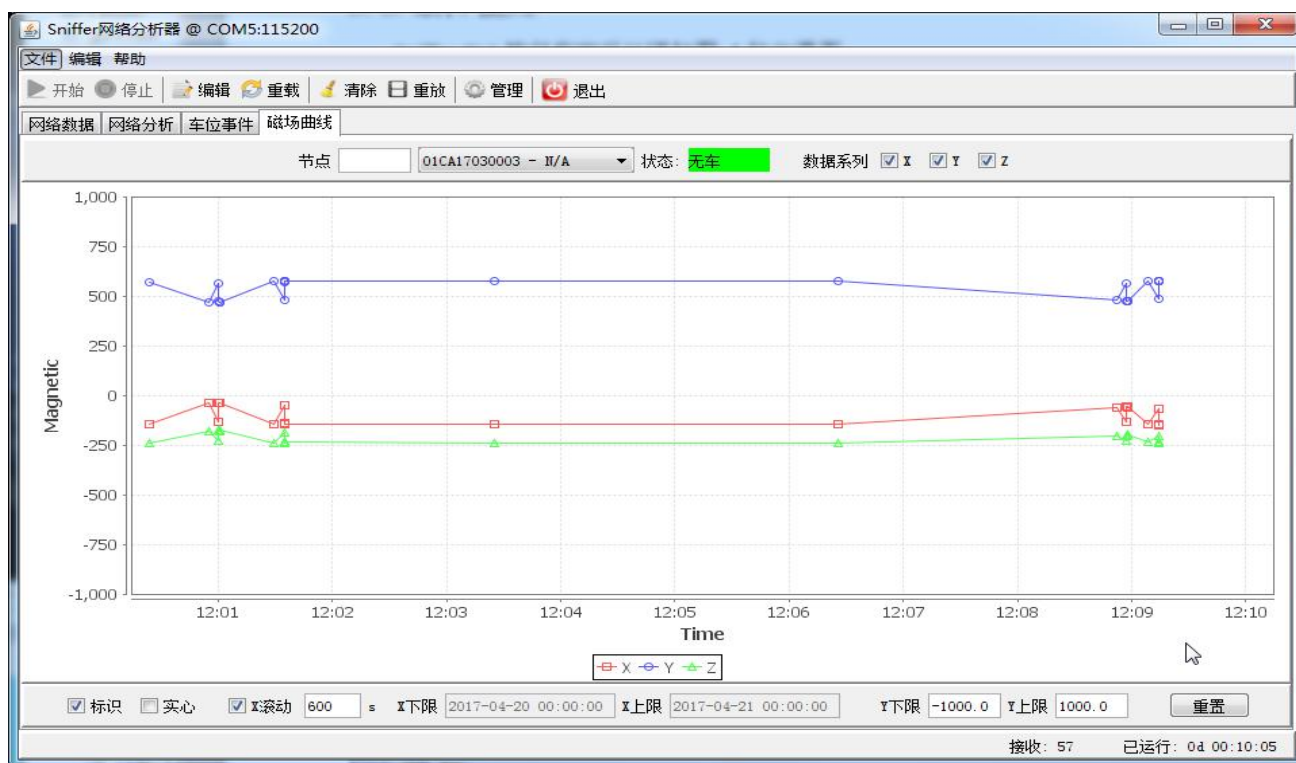


图 10 磁场曲线图

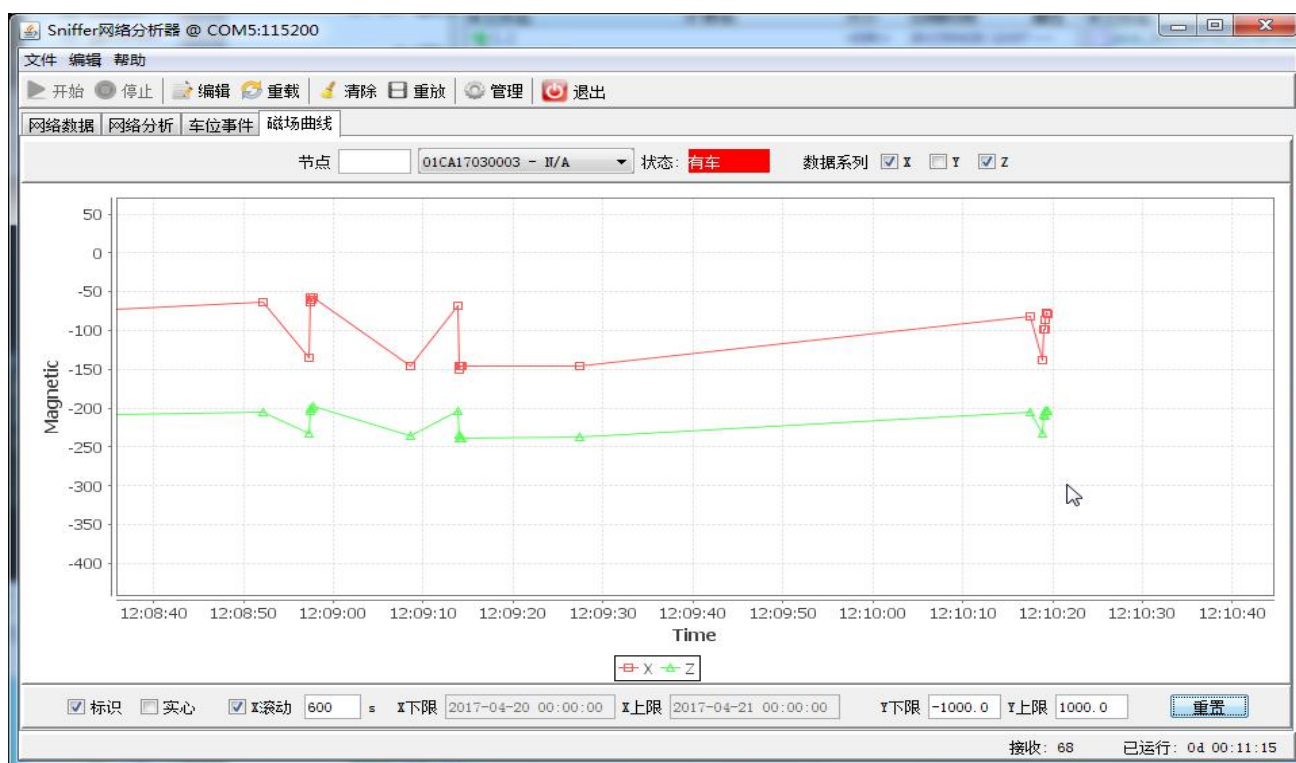


图 11 磁场曲线缩放