802.11数据包分析4：Matlab读取WiFi抓包结果（Pcap2Matlab)

Wi-Fi研习者
Wi-Fi话题下的优秀答主

序言

Matlab是常用的数据分析平台之一，本文我们介绍用Matlab来读取802.11的抓包文件（即Pcap）文件，并抽取其中的几个元素。将这些元素提取入Matlab后，我们才可以进一步扩展一些应用，比如说对数据应用一些机器学习算法之类。

Pcap2Matlab安装

首先我们要安装一个插件-Pcap2Matlab，该插件可以让Matlab读取Pcap的内容。有两种安装方法：

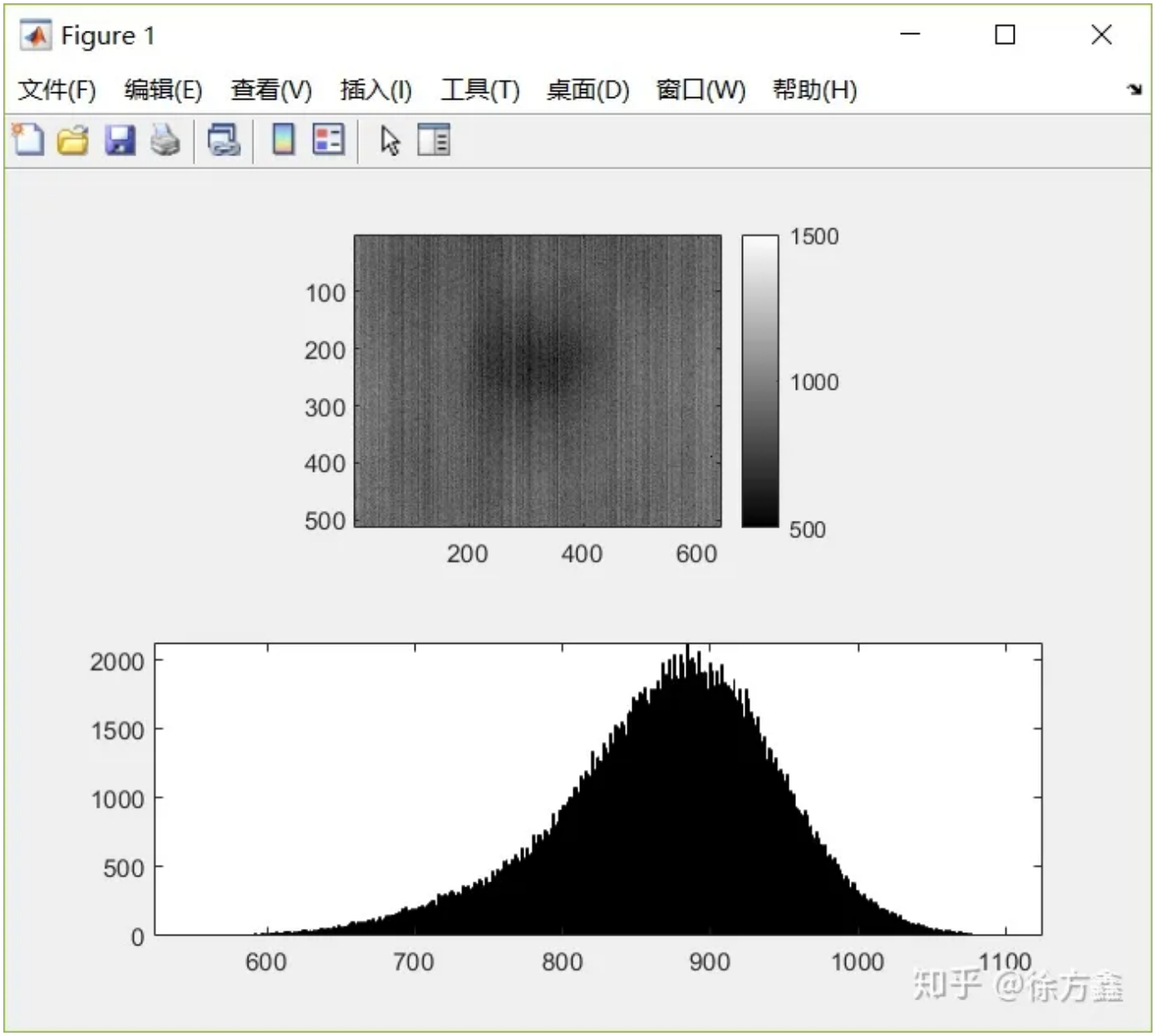
直接从Github上面下载：Pcap2Matlab
从Matlab的菜单栏→附加功能→获取附加功能→里面搜索Pcap2Matlab，然后安装也可以

安装完成之后，由于这个插件是基于tShake的，所以我们需要在其的目录下补充一些文件才可以使用。补充的文件是为了让tShake可以独立在Pcap2Matlab的文件夹下工作，但是不同版本Wireshark里面的dll文件不同，建议一个简单办法，就是把wireshark下面所有的dll都复制到Pcap2Matlab的文件夹下面，以及tshark.exe。

Remark：Wireshark不建议版本太新。

Pcap2Matlab的使用

首先是在下载Pcap2Matlab的文件下内有一个pcap2matlab_example.m，先运行这个看环境有没有配置正确，运行获得下面的图就是配置成功了



我们可以简单看下这个example程序的前28行

```
function pcap2matlab_example()
isRead = true;

CAPTURE_FILE = 'gigE_image.pcapng';
%% Set up the capturing/reading parameters:        %%VIP: 这里是设置要读取的字段
dissector = {'gvsp.status',...
             'gvsp.blockid16',...
             'gvsp.format',...
             'gvsp.packetid24',...
             'gvsp.fieldid',...
             'gvsp.fieldcount',...
```

```
                'gvsp.timestamp',...
                'gvsp.pixel.color','gvsp.pixel.occupy','gvsp.pixel.id',...
                'gvsp.sizex','gvsp.sizey',...
                'gvsp.offsetx','gvsp.offsety',...
                'gvsp.paddingx','gvsp.paddingy',...
                'gvsp.payloaddata','gvsp.payloadtype'};

capture_filter = 'udp and src port 20202';
read_filter = 'gvsp';
%% Capture/read:
if isRead
    % Read:
    pcap_result = pcap2matlab(read_filter,   dissector, CAPTURE_FILE, [], '-2');
else
    % Capture:
    pcap_result = pcap2matlab(capture_filter,dissector, 4, 700);                    %
end

%--------example程序以下就是分析以及过滤的部分了，上面的内容就已经把Pcap读取完成并保存到Pcap_r
```

其实简化以下就4行左右

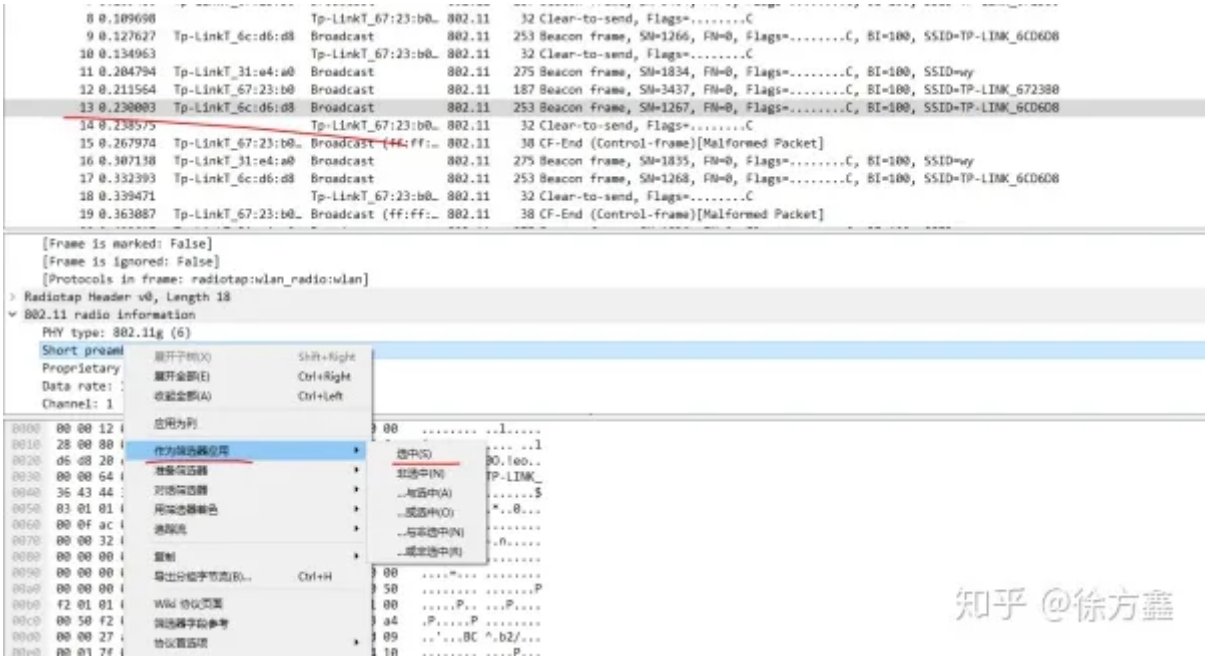
```
read_file        = 'xxxxx.pcap';
wifi_dissector   = {'frame.number', .....);
read_filter      = 'wlan';
pcap_result      = pcap2matlab(read_filter, wifi_dissector, read_file);
```

这里实际上要设置的就是readfile文件，然后过滤器类型read_filter，这个过滤器类型实际上是tshake -Y的内容，为了读取802.11的数据帧，我们设置成read_filter='wlan'，然后最后一个就是wifi_dissector，实际上是参数提取器，这里需要对wireshake解析的字段名有所了解，然后一个个填上去。

wifi_dissector字段名的获取

综上，整个读取pcap的架构已经有了，最后一步比较困难的就是知道属性的名字就行了。笔者花了不少时间探索方法，最终总结了下面这个方式应该是最简单的：

第一步，用wireshark打开我们所需要解析的pcap文件，选取一帧数据帧
第二步，鼠标选取某一个具体的属性，比如说选区PHY Type这个属性，选取后该行会被标注
第三步，右键这一行属性，选择作为筛选器应用→选中



第四步，此时在上面的筛选属性显示这一行，就会显示我们所选属性对应的dissector名字了

第五步，在matlab中设置对应的dissector即可

```
wifi_dissector = {'frame.number',...
                  'frame.time_relative',...
                  'frame.len',...
                  'wlan_radio.data_rate',...
                  'wlan.fc.type_subtype',...
                  'wlan.fc.ds'};
```


本文为原创文章，如需转载须注明出处和原文链接。