ELINT: Communications

Kyle A. Davidson, M.A.Sc.

This lab serves as an introduction to the Agilent 89600 Vector Signal Analysis software, and how it can be used as a tool for analyzing communications signals for the purposes of gathering Electronic Intelligence (ELINT). This will occur in two parts, the first is a progressive walk-through of a signal analysis for three different cases. Then, a series unknown signals will be presented for study and analysis.

1 Introduction

The Agilent 89600B Vector Signal Analysis (VSA) software provides signal analysis tools, to measure and analyze various forms of communications, radar and other signals. Although it can run on signals acquisition instrument, including the Agilent PXA, it will be used in this lab to conduct post-processing analysis of recorded signals.

1.1 Loading and Viewing a Signal

To get started we'll need to load a signal into the VSA. To do so

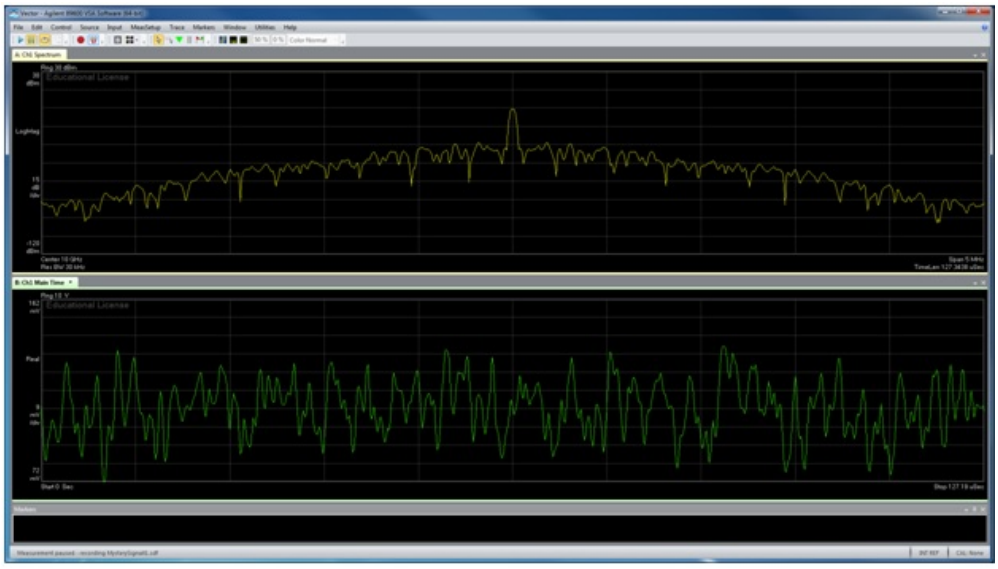

Figure 1: *Agilent 89600 VSA Display of mystery signal 1.*

- Select `File` → `Recall Recording` then select `MysterySignal1.sdf`

(Note — at any point if you would like to reset the VSA software to its initial conditions, select `File` → `Preset All`.)

Two displays should now be showing on the screen, the upper one shows the frequency spectrum, and the lower one the real portion of the signal, in mV. To adjust the scale for a better view of the time domain signal,

- right click anywhere on the `Main Time` graph, then left click `Auto Scale`.

The screen should now show the image seen in Fig. 1. At this point the recording can be paused.

- Press the symbolic pause or play buttons in the upper left portion of the display.

Once the signal has been paused a few controls should be adjusted.

- Go to `MeasSetup` → `Time` then adjust `Max Overlap (Avg Off)`, changing it from 90 % to 99.5 %

After this, press play again. Note, that the signals speed has been drastically reduced. Further increasing this value, for example to 99.9 %, will decrease the speed even more.

2 Analog Communications Signal Analysis

At this point we need to answer a few simple questions regarding the signal:

- What is the centre frequency?
- What is the signal power?
- What is the bandwidth?
- What type of modulation is occurring?

2.1 Spectrum

The first two, spectrum and power, can be answered easily using the spectrum plot. The centre frequency can be read directly from the `Ch1:Spectrum` trace. Located at the lower left corner of the trace the centre frequency is clearly 10 GHz. (This value is technically arbitrary, if the instrument is evaluating the signal after conversion to baseband, and not while still operating at the RF frequency.)

The signal power can be determined either at individual frequency points, or over a selected band. We will examine individual frequencies first, to do so a marker can be added to the `Ch1:Spectrum` plot by doing the following:

- `Right click` on the `Ch1:Spectrum` trace and left click on the green + symbol.
- Then `left click` on the marker and drag it to the desired location.

At this point the power for each marker, will be shown along with the related frequency point at the bottom of the VSA window.

Next, we need to measure the bandwidth and the power contained within it. Two methods exist for this:

- `Right click` on the `Ch1:Spectrum` trace, and then `left click` on `Show OBW` which stands for "show occupied bandwidth"; or
- `Right click` on the `Ch1:Spectrum` trace, and then `left click` on `Show Band Power`, which can be dragged to the desired centre frequency, and the vertical bars spread over the band of interest.

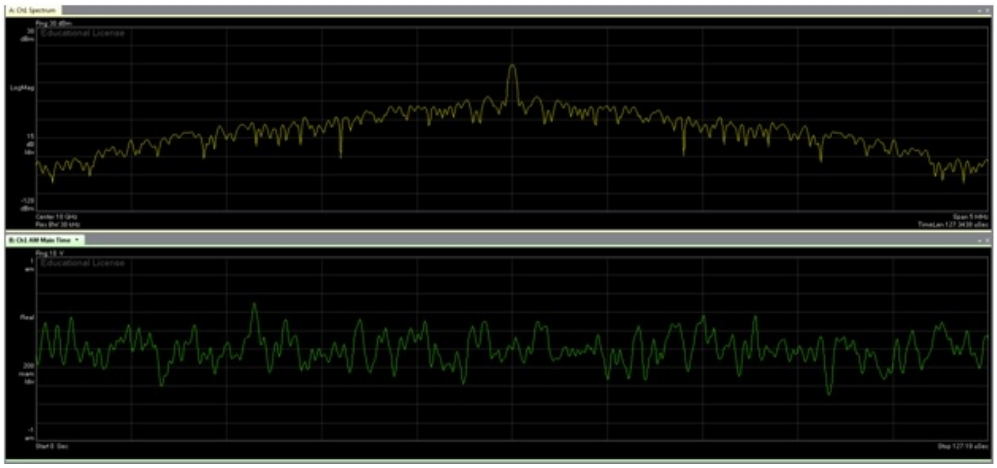

Figure 2: *VSA display of mystery signal 1 amplitude modulation analysis.*

The first method automates the process of determining the signal bandwidth, by displaying the spectrum containing 99 % of the observed power (this exact figure can be adjusted in the options). The second method allows the user to examine portions of the signals spectrum in isolation. In both cases the measured results are displayed in the marker section at the bottom of the VSA window.

2.2 Amplitude Modulation

Now that the basic characteristic of the signal have been determined, the details of its modulation need to be evaluated. This generally means the symbol rate, and type of modulation.

The first step here is to determine if the signal has any amplitude modulation.

- Select `MeasSetup` → `Measurement Type` → `Analog Demod`.
- Then `MeasSetup` → `Analog Demod Properties` followed by the demodulation you are interested in AM, FM, or PM. We want to select AM first.
- On the drop down menu of the lower display, `B`, select `Demod Channel 1` → `Inst Main Time`.

The displays, shown in Fig. 2, should be seen in the VSA window.

After this, go back and try demodulating the signal with FM or PM. The results should show little to no phase or frequency modulation in the `Main Time` window. At this point we've analyzed most of the parameters of Mystery Signal 1. However, it's a relatively simple communications signal (analog amplitude modulation over a single carrier), and we'll need some more tools to evaluate modern communications signals.

2.3 Frequency Modulation

Now, as previously described, recall the file `MysterySignal2.sdf` and analyze it in the same manner as `MysterySignal1`. In order to do so you'll need to answer the following questions: What is its centre frequency? What is its bandwidth? Is it frequency, phase or amplitude modulated?

You'll notice at this point the signal has almost no amplitude modulation, but is significantly modulated in phase or frequency. Once you've explored Mystery Signal 2's operation in detail, we're ready for digital signals, modulated in quadrature.

3 Vector Modulated Signal Analysis

Now, recall the file `MysterySignal3.sdf` and analyze it in the same manner as signals 1 and 2. However, it should quickly become apparent that the signal is vector modulated, that is modulated in both amplitude and frequency/phase. To further analyze this signal a number of steps are required, do the following:

- Select `File` $\rightarrow$ `Preset` $\rightarrow$ `All` (this returns the VSA to its initial configuration).
- Reload the recording `MysterySignal3.sdf`.
- Right click on the spectrum plot, and then left click on `Show OBW`.

This last step will act as a marker, shown in Fig. 3, superimposing a blue square over the portion of the spectrum containing 99 % of the signals power. The numeric results from the OBW filter are shown at the bottom of the window in the markers section,

This occupied bandwidth is approximately $(1 + \alpha)(symbol\ rate)$, where α is the describes the shape of the Nyquist(cosine) filter (this is also referred to as the roll-off or excess bandwidth factor). Communications theory states that the minimum bandwidth required to transmit a symbol is half the symbol rate. In order to realize this though, you would need a perfect filter, which would have

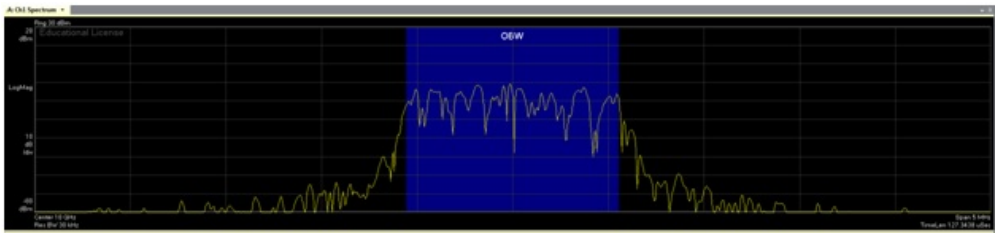

Figure 3: *VSA display of the occupied bandwidth of Mystery Signal 3.*

an alpha of zero. In most cases an alpha of 0.3, or 30 % more bandwidth than the theoretical minimum is required. In this case, that means a bandwidth of roughly 1 MHz is being used, which is a rough estimate of the symbol rate.

3.1 Symbol Rate through FFT of AM Demodulation

The problem with this initial method of estimating the symbol rate is its inaccuracy. A precise knowledge of the symbol rate is key to effectively receiving the signal of interest, so we need another technique.

The general process to apply in this case is to run the time domain waveform through a non-linear function and then evaluate the spectrum of the result. This method will indicate a significant energy spike in the frequency spectrum at the symbol rate. For a signal without constant amplitude, an approach would be to perform the fourier transform of an AM demodulated signal.

- Adjust the span of the measurements to at least three times the symbol rate, as determined by the occupied bandwidth.
- Change the measurement type to `Analog Demod`
- Change the `Analog Demod Properties` to `AM` selected
- Change the trace `B` data to `Demod Channel1` → `Spectrum`.
- Go to `MeasSetup` → `Average` then select the drop down menu below `Average` and pick `RMS Video Exponential` with a count of 10.

At this point the spectrum in trace `B` should be showing a clear spike around 1 MHz, indicating the symbol rate. However, we can get an even better result by increasing the frequency resolution.

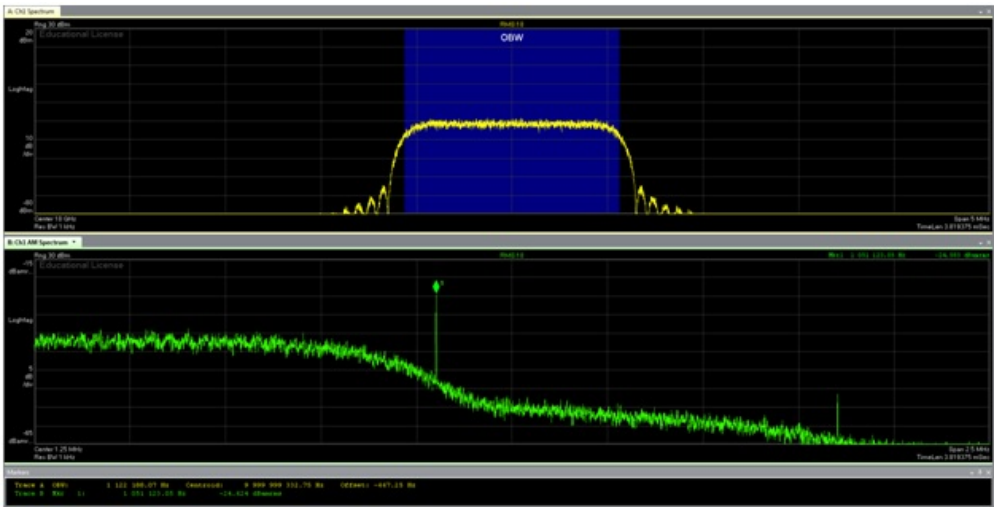

Figure 4: *VSA display of the symbol rate analysis of Mystery Signal 3.*

- Go to `MeasSetup` → `Frequency`, then select the tab for `ResBW`, and finally un-check `Auto` next to the `Frequency Points:` option.

The number of frequency points can now be increased to allow for more precise analysis, for example 204801. At this point a marker can be used to precisely measure the symbol rate.

- Right click on the `B:Ch1 AM Spectrum` trace and left click on the + to add a marker, and then adjust its position to that of the symbol rate spike.

The final results for the symbol rate should be very close to 1.05 MHz, and look similar to Fig. 4.

3.2 Modulation Format Recognition

Now that we've found the symbol rate, we need to determine how the signal is modulated. While we know it's some combination of amplitude and frequency/phase, this covers a large class of Quadrature Amplitude Modulation (QAM) and Quadrature Phase Shift Keying (QPSK) modulation.

The simplest method to apply here is to assume the signal is digitally modulated using QAM and a large number of levels, for example 256 QAM. Through picking the worst case, we will then be able to see simpler modulations, as

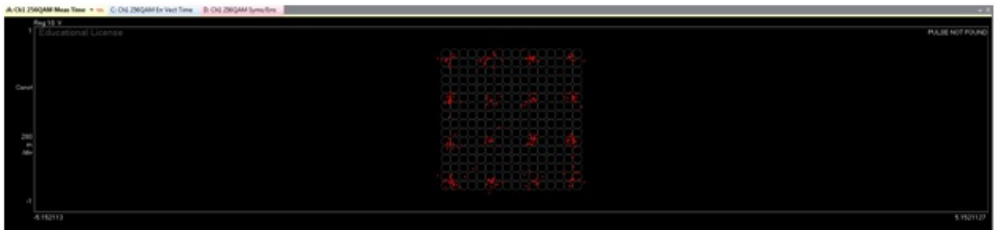

Figure 5: *VSA display of the modulation analysis of Mystery Signal 3.*

they're essentially the same format, like 16 QAM, but with fewer levels. To do this, follow these steps:

- Change the measurement type to `Digital Demodulation`.
- Adjust the `Digital Demod Properties` to the following:
  - Format: 256 QAM
  - Symbol Rate: 1.05 MHz
  - Measurement Filter: Root Raised Cosine (under the `Filter` tab)
  - Alpha: 0.35 (under the `Filter` tab)
  - Result Length: 200 (sets the number of symbols to display)
- Set Trace A to `Ch1: IQ Meas Time`.
- Select `Trace` → `Format` and set `Format` to `Constellation`

Based on the entered data you should have the same display as shown in Fig. 5, with four distinct levels for I and Q. This clearly implies the signal is a 16QAM. Based on this data, we can adjust the digital demodulation properties back to 16 QAM.

3.3 Symbol Rate Refinement

At this point we need to refine the symbol rate, which as will be seen, will drastically increase the accuracy of the receiver.

- Left click on the trace layout symbol button, in the upper left corner, and select a 2 x 2 set of windows, with the following displays:
  - `Constellation diagram`;

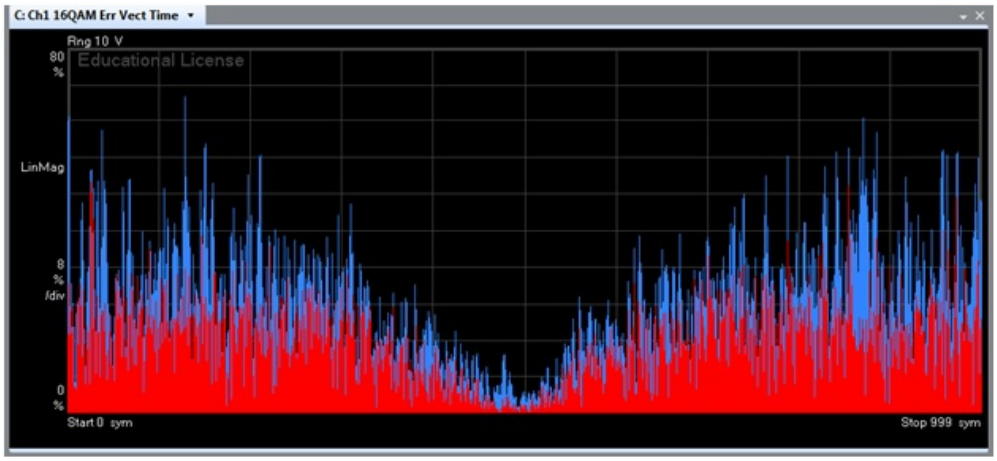

Figure 6: *VSA display of the error vector magnitude of mystery signal 3.*

  - `Spectrum`;
  - `Ch1:Error Vector Time`; and
  - `Syms/Errs`.

- Increase the number of symbols analyzed until a "V" pattern becomes obvious in the error vector magnitude plot.

This pattern can be seen in Fig. 6. The symbol rate can now be adjusted in very small increments (think kHz or hundreds of Hz), until the EVM plot flattens out. This reduction in EVM indicates the estimated symbol rate is becoming much closer to the actual rate. The final EVM should average around 2 %.

4 Unkown Signals

For the final signals, youre on your own. Using the tools presented for the other signals, analyze the `MysterySignal4.sdf` and `MysterySignal5.sdf` files and provide a complete report on their spectral and modulation characteristics.

The report should provide sufficient information for an analyst to demodulate the signal with no further signal characterization required. Ensure figures are included to substantiate your results.