Applications for RTL based Software Defined Radios

Presented by Stan Frady
WNC IEEE
Abstract

Due to recent advances in software and the discovery of lower cost hardware, Software Defined Radios (SDRs) are becoming very common. The fact that no communication license is required to use these devices allows easy access into this field. Different applications will be discussed to provide a brief introduction on what can be done with these wireless devices.
Topics

- What is SDR?
- RTL based SDR and related hardware/software
- Applications of RTL based SDR
What is SDR?

• There is a fair amount of debate about what SDR means.
  o Definition 1: Any signal processing function done in software
  o Definition 2: SDR is one where the RF signal is converted to a digital bit stream and all of the modulation and demodulation of the signal is done with digital signal processors (DSPs)
  o Definition 3: A radio that includes a transmitter in which operating parameters of the transmitter, modulation type or conducted output power can be altered by making a change in software with no hardware changes
Benefits from SDR include

- Digital modes are seamless as they can be done without intervening hardware and cables
- Remotely run SDR interface with the internet/wifi
- You can visually see what is going on in the RF Spectrum besides hearing it
- Software can make it easier to navigate radio controls than buttons with multiple settings and hidden menus
GNU Radio – adding FFT features

Options
- ID: top_block
- Title: AM Receiver us spectrum
- Author: Marcus Leech
- Description: gnu Radio...ow graph
- Generate Options: WX GUI

Variable
- ID: samp_rate
- Value: 32k

Variable Slider
- ID: current_freq
- Default Value: 1.42G
- Minimum: 1.415G
- Maximum: 1.425G
- Converter: Float

Variable Slider
- ID: volume_control
- Default Value: 1
- Minimum: 0
- Maximum: 100
- Converter: Float

Variable
- ID: bw
- Value: 500k

Audio Sink
- Sample Rate: 32kHz
- Device Name: plughw:0,0

FFT Sink
- Title: Hydro Spectrum
- Sample Rate: 100k
- Baseband Freq: 1.42G
- Y per Div: 10 dB
- Y Divs: 10
- Ref Level (dB): 50
- FFT Size: 1024k
- Refresh Rate: 2
- Average: On
- Average Alpha: 250m

Band Pass Filter
- Decimation: 128
- Gain: 1
- Sample Rate: 300k
- Low Cutoff Freq: 40
- High Cutoff Freq: 14k
- Transition Width: 100
- Window: Hamming
- Beta: 6.76

Multiply Const
- Constant: 1m

Complex to Mag^2
That’s great, but I want something easier!

- In Q1 2012, Antti Palosaari discovered that the $20 USB dongles used for digital video broadcast-terrestrial (DVB-T) reception had a really wide range radio receiver in them. He teamed up with developers at Open Source Mobile Communications (Osmocom) to build drivers and utilities to couple these dongles with SDR software commonly used by licensed amateurs to receive radio transmissions of all kinds.
DVB-T features

• Have limited reception in the 64 – 1700 MHz range
  o This includes the 2 and 1.25 meter and 70, 33 and 23 cm amateur radio bands
  o Also includes FM broadcast, marine, public service and commercial 2-way services

• With an inexpensive RF upconverter developed by Opendous ($40), reception can be extended to 300 KHz
  o Covers 160 to 6 meter amateur radio bands
  o Also includes CB, AM and shortwave broadcast
Which DVB-T to buy?

- Want a DVB-T dongle with a Realtek RTL2832u control chip
- The tuner on the dongle will often vary
- Most common is the R820T but Elonics E4000 chips will also work
- Difference in the tuners is the actual tuning range and price
Newsky TV28T v2 USB DVB-T

Ham It Up

Ham It Up

- [http://www.nooelec.com/store/software-defined-radio/ham-it-up-v1-0-rf-upconverter-for-software-defined-radio.html](http://www.nooelec.com/store/software-defined-radio/ham-it-up-v1-0-rf-upconverter-for-software-defined-radio.html)
DC to daylight receiver

- For about $60 plus laptop, free software, antennas, feedline coax and connectors
- Monitor anything:
  - All the ham bands
  - CB Radio
  - AM & FM broadcast channels
  - MURS, FRS, GMRS
  - Public Service/Police/Fire/Emergency
  - Commercial 2 way radio
  - Shortwave
  - Marine
  - Intercom systems
What about software?

- I like using SDR#
  - Based on C# and is a fully featured SDR
  - Source code is free so it is possible to find new plugins for it
  - Runs on Windows and Linux

Important note for RTL-SDR users

You can use this quick installation script to test the latest development version:
http://sdrsharp.com/downloads/sdr-install.zip
SDR# v0.0.0.0 - IQ Imbalance: Gain = 1,001 Phase = -0,057*

Radio
- NFM
- AM
- LSB
- USB
- WFM
- DSB
- CW-L
- CW-U
- Filter type: Blackman-Hams
- Filter bandwidth: 14110
- Filter order: 400
- Squelch
- CW Shift
- Snap to grid: 1 kHz
- Correct IQ
- Swap I & Q
- FM Stereo
- Mark Peaks

Audio
- AGC
- Use AGC
- Threshold (dB): -100
- Decay (ms): 100
- Slope (dB): 0

FFT Display
- Frequency Manager (Plugin)
- Recording (Plugin)

VFO: 0.000.250.000
Center: 0.000.000.000
Zoom
Contrast
Speed
RADIO PANEL

- **NFM** – Narrow FM
- **AM** – Amplitude Modulation
- **LSB** – Lower Side Band
- **USB** – Upper Side Band
- **WFM** – Wide FM
- **DSB** – Double Side Band
- **CW-L** – Continuous Wave Lower CW-U – Continuous Wave Upper

**Frequency** – The current tune frequency

**Center** – The current frequency of the center of the FFT display when NOT zoomed in. (NOTE: If a frequency is entered that is outside the current frequency range displayed by the FFT, the frequency will not change. Select a new Center that is the same or near the desired new Frequency)

**Shift** – This is to input an offset if an upconverter or downconverter is used so that the selected frequency is corrected to display the actual tuned frequency. Simply check the Shift box and enter your offset.

**Front End / Input Select** – The input select will allow you to choose your desired input device. A properly installed program will show:

- **RTL-SDR / TCP** – RTL2832u device via TCP connection
- **RTL-SDR / USB** – RTL2832u device via USB connection
- **FUnCube Dongle**
- **SoftRock / Si5570**
- **Other**

**Filter Type** – This is to select the desired filtering type. Different filters will cause changes in the demodulated signal audio response curve due to differing envelopes and filtering profiles.

**Filter Bandwidth** – This is the effective width of the signal being processed for the mode selected. You can see the affected area in both the FFT and Waterfall area of the display when zoomed in, and you can either change the filter width here, or by dragging the outer edge of the grayed out area in either live display.

**Filter Order** – A modifier for the selected filter. The default setting works for most applications.

**Squelch** – Turn squelch on, and select the level with the box below it. Squelch levels may change depending on filtering type and mode selected.

**CW Shift.** – Changes the frequency shift in either CW mode. Similar to changing a BFO (Beat Frequency oscillator).

**Snap To Grid** – Forces frequency to snap to frequency steps selected when drag tuning.

**Correct IQ** – Enables SDR#’s exclusive Automatic IQ Correction.

**Swap I & Q** – Swap I & Q inputs. Useful when using sound card input devices. Swaps L/R inputs to I/Q

**FM Stereo** – Select FM Stereo demodulation when using WFM with broadcast FM radio

**Mark Peaks** – Displays a marker on detected peaks above the noise floor.
Alternatives to laptop

- **Newer Android tablet**
  - Nexus7, Kindle Fire, Samsung Galaxy Tab
  - Software is SDR Touch
  - Android tablet has to be running at least Android 4.0 (ICS) and rooted
  - Uses On the Go (OTG) usb cable to connect SDR dongle to tablet

- **Use network connection (wired or wireless)**
  - Dongle connected to Remote Server such as Raspberry Pi
  - Using TCP server, allows you to send data from home computer to remote PC
Raspberry Pi as Remote Server

- **Raspberry Pi features:**
  - Credit card size computer with ARM chipset
  - Uses 2.5 or 3.5W based on model used
  - Place program on it using SD Card
  - Runs Linux

- **Raspberry Pi not powerful enough to run current programs to decode/process SDR data but does a good job of running the rtl_tcp server**

- **Plug SDR dongle into Raspberry Pi and you have a very small and powerful SDR radio server**
Raspberry Pi
Raspberry Pi SDR Server

- Cost of Raspberry Pi is $25 or $35
- Add SD/SDHC Card (1 GB or larger)
RTL Applications
Sniffing/Decoding 2.4ghz

- This is impossible using any version of the rtl-sdr as the highest you can buy reach 2.2Ghz just shy of the 2.4Ghz we need.
- MMDS is a digital broadcast system used in some countries for digital TV, and the LNB is part of the antenna. The MMDS LNB can be found for a variety of frequencies and LO frequencies.
- The base frequency defines the filters on the device and the LO frequency defines by how much will it reduce the input frequency.
- Based on the specification, it would do EXACTLY what we need - take 2.2-2.4Ghz signal and down convert it to around 400Mhz. Then we can use the rtl-sdr and some code to decode packets off the air.
RTL Applications
Sniffing/Decoding 2.4ghz
RTL Applications
Sniffing/Decoding 2.4ghz

- Tuning to 2,405Mhz (or 407Mhz after down conversion using LO of 1998Mhz) clearly show a strong signal when I move my mouse.
Everyday multiple NOAA weather satellites pass above you. Each NOAA weather satellite broadcasts an Automatic Picture Transmission (APT) signal, which contains a live weather image of your area.

The rtl-sdr dongle combined with a good antenna, SDRSharp and a decoding program can be used to download and display these live images several times a day.

Audio piping method installed and set up. Audio piping will allow the audio from SDRSharp to be passed to a decoding program. You can use either windows stereo mix, VB-cable (free) or virtual audio cable (paid with trial version).
Everyday multiple NOAA weather satellites pass above you. Each NOAA weather satellite broadcasts an Automatic Picture Transmission (APT) signal, which contains a live weather image of your area.

The rtl-sdr dongle combined with a good antenna, SDRSharp and a decoding program can be used to download and display these live images several times a day.

Audio piping method installed and set up. Audio piping will allow the audio from SDRSharp to be passed to a decoding program. You can use either windows stereo mix, VB-cable (free) or virtual audio cable (paid with trial version).
RTL Applications
Weather Satellites

- NOAA APT weather satellites broadcast their signal at about 137 MHz, and their signals are also right hand circularly polarized (RHCP), which means you will need a right hand circularly polarized antenna to properly receive the signals. This is because as the satellites broadcast their signal, they also rotate, rotating the signal polarization.
RTL Applications
Weather Satellites
The NOAA satellites only pass overhead at certain times of the day, broadcasting a signal. These signals appear at around ~137 MHz, and only when a satellite is passing overhead. Each satellite has a different frequency. Currently only NOAA satellites 15, 18 and 19 are operational, their frequencies are shown below.

- NOAA 15 - 137.6200 MHz
- NOAA 18 - 137.9125 MHz
- NOAA 19 - 137.1000 MHz
RTL Applications
Weather Satellites

• WXtoImg is a free weather satellite decoding program, which can decode the APT signal, and also tell you the times and frequencies of the satellites passing overhead. There is also a paid version of WXtoImg which can unlock more features, however it is not required for use with rtl-sdr.
RTL Applications
Weather Satellites
RTL Applications

ADS-B

• RTL-SDR can be used as a super cheap real time air radar
• Modern planes use something called an ADS-B (Automatic Dependent Surveillance-Broadcast) Mode-S transponder, which periodically broadcasts location and altitude information to air traffic controllers.
• Compared to dedicated commercial ADS-B receivers which can go for between $200 – $1000, the $20 RTL-SDR is very attractive for the hobbyist in terms of price. However, note that the RTL-SDR probably shouldn’t be used for ADS-B in a real aircraft for safety reasons.
RTL Applications

ADS-B

- ADS-B broadcasts at a frequency of 1090 MHz. It has been discovered by the RTL-SDR community, that the R820T tuner has the best sensitivity at this frequency. The E4000 and other tuners perform poorly in comparison.
- Software used is ADSB# and Virtual Radar Server.
- The stock antenna that comes with the dongle may already be able to pick up ADS-B signals, depending on how far away you are from the aircraft and what your local RF interference is like.
- However a properly tuned antenna is required to get decent range. ADS-B uses a vertically polarized signal, so only certain types of antennas will work.
RTL Applications

ADS-B

- ADS-B broadcasts at a frequency of 1090 MHz. It has been discovered by the RTL-SDR community, that the R820T tuner has the best sensitivity at this frequency. The E4000 and other tuners perform poorly in comparison.
- Software used is ADSB# and Virtual Radar Server.
- The stock antenna that comes with the dongle may already be able to pick up ADS-B signals, depending on how far away you are from the aircraft and what your local RF interference is like.
- However a properly tuned antenna is required to get decent range. ADS-B uses a vertically polarized signal, so only certain types of antennas will work.
RTL Applications ADS-B

- Collinear Coax Antenna
RTL Applications
ADS-B
RTL Applications
ADS-B

- FM Receiver
- Spectrum Analyzer
- Analogue TV decoder
- Trunking / Scanning
- Wireless devices such as temperature sensors
- Ham Digital modes and Morse Code
- LTE signals
- Matlab
- Pager decoding
- Sonde – Weather Balloon
- Ship / Trains
- Satellite Tracking
Any Questions?