INL/EXT-16-39259-Revision-0

# Data Acquisition in Wireless Router Link Testbed using GNU Radio Companion

Christian W. Hearn, Andrew Kuznicki, Christopher Becker, Kurt W Derr, Samuel Ramirez

September 2016


The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-16-39259-Revision-0

# Data Acquisition in Wireless Router Link Testbed using GNU Radio Companion

**Christian W. Hearn, Andrew Kuznicki, Christopher Becker, Kurt W Derr, Samuel Ramirez**

**September 2016**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Office of Nuclear Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

# Data Acquisition in Wireless Router Link Testbed using GNU Radio Companion GNU Radio Conference (GRCON 2016)

**Christian Hearn** christianhearn@weber.edu
**Andrew Kuznicki** andrewkuznicki@mail.weber.edu
Weber State University 1447 Edvalson Drive , Ogden, UT 84403-1802 USA

**Christopher Becker** cbecker@cs.utah.edu
University of Utah, 50 S. Central Campus Drive, SLC UT 84112 USA

**Kurt Derr** kurt.derr@inl.gov
**Samuel Ramirez** samuel.ramirez@inl.gov
Idaho National Laboratory, 2525 Freemont Ave, Idaho Falls, ID 83415, USA

## Abstract

A IEEE802.11g WLAN wireless-router link testbed is under development at the Idaho National Laboratory-Wireless Research Center. The project objective is to generate repeatable, high-quality, controlled-noise wireless transmissions for software-defined radio (SDR) analysis and research. Signal acquisition for the data link will include both an USRP X310 (with GNU Radio Companion) in parallel with a Tektronix RSA 306a Spectrum Analyzer. The integration and validation of the the SDR is described. Preliminary results indicate the router test-bed comprised of readily-available Wi-Fi and RF hardware will provide low-noise, and repeatable signal captures.

## 1. Introduction

The Idaho National Laboratory (INL) cyber security and wireless research centers collaborate with federal agencies to develop, test, and validate technologies that protect national infrastructure. Current research areas include monitoring spectrum for wireless security and protecting long-term evolution (LTE)-enabled mobile communication devices from cyber-attack.

Low-cost radio hardware and open source software-defined radio (SDR) emerging technologies create opportunities for both constructive research and malicious behavior in security for wireless communications. In response to emerging threats to wireless security, the INL wireless cyber research scientists are interested in the means to acquire a database of wireless signal captures in interference-controlled environments. The signal capture or measurement process must also be repeatable.

A signal capture database of actual signals in known conditions would be a useful tool in the field of cyber-security. Existing databases (e.g CRAWDAD at Dartmouth University) will be valuable in future comparisons [1]. Channel models for generating simulation scenarios are effective tools for initial research, but real signals transmitted from commercial-off-the-shelf (COTS) devices were the focus of this effort.

The project goals of measurement repeatability and reliability directed interest toward the creation of a link testbed. Two system features were implemented as a result. Repeatability would be addressed with the ability to isolate outside interference. Reliability would potentially be achieved with a second redundant measurement for verification.

It is anticipated the database would be used to train SDR signal classifiers. Replay attacks and spoofing are additional examples of relevant cyber-scenarios to be investigated with the link testbed. Flexibility in terms of hardware configurations would be advantageous in a rapidly-changing environment.

## 2. Background

A test plan from the International Telecommunications Union (ITU) for the evaluation of digital terrestrial television broadcasting systems was the basis for the link testbed [2]. The ITU evaluation recorded a noise free signal in parallel with the noise-interference channel evaluated by the viewer.

A WLAN link testbed could be fabricated with existing hardware similar to the ITU structure. The wireless router

testbed would implement a redundant measurement for comparison and validation. Two computer-linked wireless routers generate message traffic. Antennas and the wireless channel are replaced with coaxial cable to minimize external interference and allow for controlled measurements. A pick-off tee and splitter create a sampling path for instrumentation. Antennas may replace one section of the coaxial transmission line between the router and pick-off tee. Future modifications will include a combiner to introduce a controlled noise source to the channel.

## 2.1. Measurement Configuration

A schematic illustrating the Wi-Fi Link Testbed is shown in Figure 1. Two Linux-based Linksys Wireless-G Broadband Routers (model no. WRT54GL) were configured for transmit and receive. The diversity antenna ports on the wireless routers [3] were modified using terminations and coaxial cable to establish a minimum-interference measurement channel. Attenuators were initially configured around a resistive-load 6-dB pick-off tee that sampled the channel. The sampled signal is routed through a 1x2 power divider to both a PC-based digital spectrum analyzer (Tektronix RSA 306a) and a software-defined radio (USRP X310).

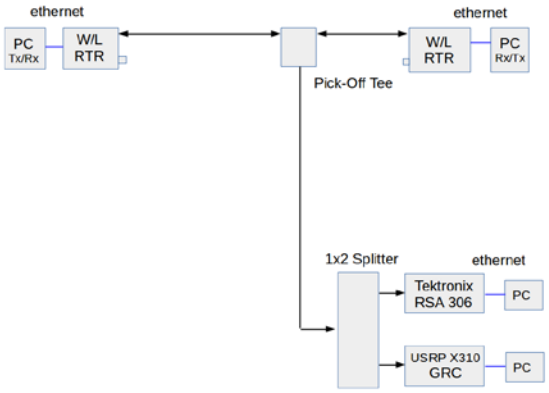


**Fig. 1.** Wi-Fi Router Link Testbed.

The Wireless routers shown in Figure 1 are designed for WLAN IEEE 802.11b/g protocols. IEEE 802.11g operates in a frequency range $2.412<f<2.462$ GHz. The IEEE 802.11 standard supports twelve overlapping *20* MHz channels which allows speeds up to *54* Mbps. Transceivers in the link automatically adjust data rate to maintain reliability. Different speeds available depend upon the encoding. Examples include BPSK (*6* and *9* Mbps), QPSK (*12* and *18* Mbps) and QAM for speeds greater than *18* Mbps (up to *54* Mbps).

The two Linux-based wireless routers were configured with DD-WRT utility software. One router operated as a repeater-bridge. The second router was set up as a standard access point. With correct settings, the computers attached to the routers 'pinged' in either direction.

In a laboratory setting with a range less than six feet, the routers would transmit and receive pings with antennas removed and ports terminated. The DD-WRT utility software was subsequently installed on the second router for transmit power control. Sufficient shielding was achieved with aluminum foil to isolate spurious router RF radiation.

## 2.2. Measurement Validation

The pick-off tee shown in Figure 1 allows for a sampled signal from the communication channel to be recorded. A 1x2 power divider allows two instruments to record simultaneously. A Tektronix PC-based RSA 306 spectrum analyzer is attached in parallel with a USRP X310 software-defined radio.

Figure 2 is an illustration of the first measurement. The *50* Ω port for the SDR is terminated to isolate Tektronix RSA 306 spectrum analyzer measurement. For the second measurement, the Tektronix port was terminated to isolate the USRP X310 software-defined radio configured to record (not shown).

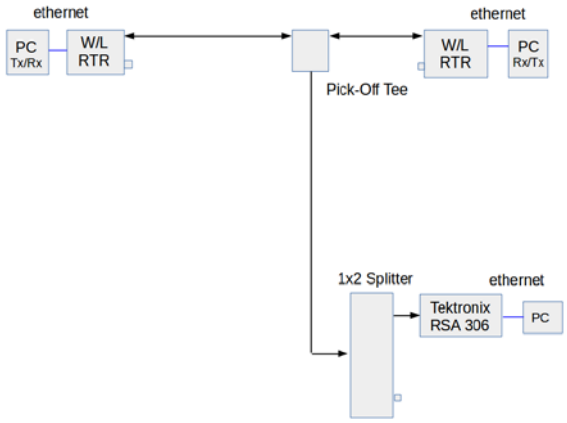


**Fig 2.** Wi-Fi Router Link Testbed configured for single-measurement with PC-based spectrum analyzer.

### 2.2.2 SIGNAL CAPTURE WITH SPECTRUM ANALYZER

The Tektronix RSA-306a PC-based spectrum analyzer was configured with *Signal-Vu* software to record router communication. The RSA-306 has digital recording capability and a frequency range from *9 kHz – 6.2 GHz* The measurement was facilitated with a setup option to write-to-file with a set trigger-level threshold. The screen capture shown in Figure 3 is nearly synchronized with the

data written to file. Improvement of the synchronization is an objective for future measurement campaigns.

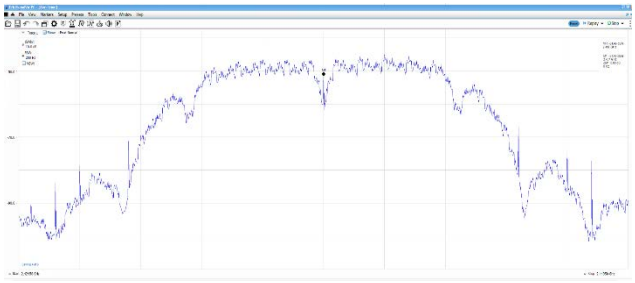

**Fig. 3.** Tektronix *Signal-Vu* screen capture of router bridge link spectral response. Spectral amplitude range is approximately *-50* dBm with a noise floor at *-100* dBm.

Several file formats are available in the *Signal-Vu* software. The MATLAB-specific binary file (**.mat*) was chosen for this example. **.mat* files may be directly imported to the MATLAB command line. In-phase and Quadrature (I+Q) quantities are recognized as variables and stored as complex data vectors.

The header file contains recording parameters and may be read as a string. For example, the Tektronix record of the 'ping' for the example recorded a sample period of approximately *18* ns with a corresponding sample rate of *56* MHz.

Meta-file data sample period = *1.7857e-8 - fs=56 MHz*

The raw data I+Q records for the spectrum analyzer measurement is shown in Figure 4. The raw data file contained over *724,000* samples stored as complex numbers. The router ping may be seen as a transient burst between sample numbers *150-200* k.

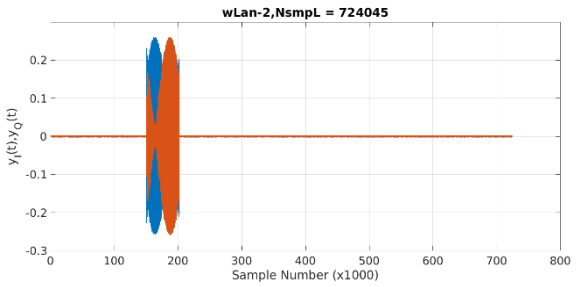


**Fig 4.** Raw data IQ records for spectrum analyzer measurement example.

Amplitudes and locations of the I+Q maximums within the router 'burst' were identified. The post processing index is the center point between the I+Q maximums. Time domain sequences (with dimensions typically *N=64, 128,256*) are centered around the post-processing index. Normalized FFT frequency domain amplitude responses are calculated from the finite time domain sequences.

Figure 5 is an illustration of the in-phase and quadrature time-domain responses for the PC-based spectrum analyzer measurement. Both I+Q data records are aligned, and time-domain responses appear as smooth waveforms.

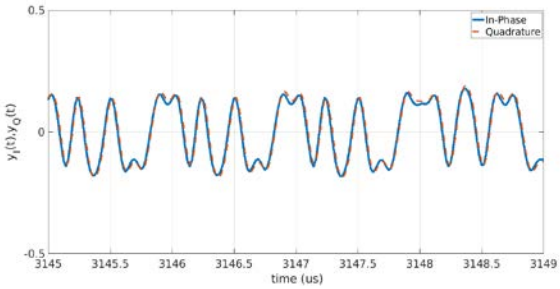


**Fig. 5.** I+Q time domain responses for spectrum analyzer measurement example. *N=256* for the example shown.

Figure 6 is the FFT-processed, normalized amplitude spectral response for the PC-based spectrum analyzer measurement. The frequency scale was halved to facilitate a visual comparison of the MATLAB-calculated FFT with the Tektronix screen-capture shown in Figure 3. Overall agreement with some differences in smoothing is observed.

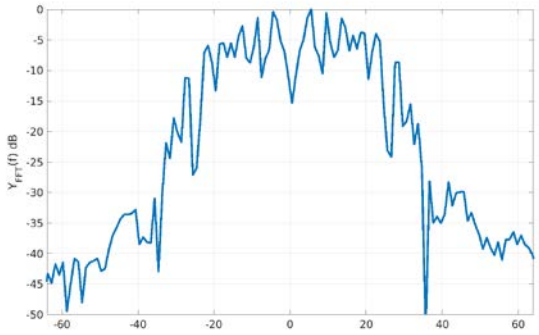

**Fig. 6.** FFT processed normalized frequency domain responses for spectrum analyzer measurement example. *N=256* for the example shown. The scale was zoomed-in for clarity.

## 2.2.2. SIGNAL CAPTURE WITH SDR

A USRP X310 SDR controlled with GNU Radio Companion (GRC) PC software was attached to record router communication. A file-sink model was created within GRC. A block diagram of the GRC file sink model is shown in Figure 7. The data was stored as complex format; the sample rate was *25* MHz. Software was written to record data for a maximum of thirty seconds. A screen capture of the router-bridge link spectral response is shown in Figure 8.
The maximum *25* MHz sample rate for the USRP X310 is bound by the ethernet connection limitation. The *64*-bit samples (*32*-bit for I , *32*-bit for Q) are stored in two, *4*-byte blocks. The GRC file sink samples are stored as complex

values. In-phase and quadrature quantities are stored as real and imaginary parts respectively.

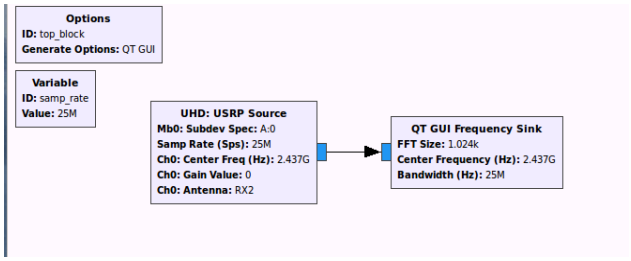


**Fig. 7.** GNU Radio Companion File Model

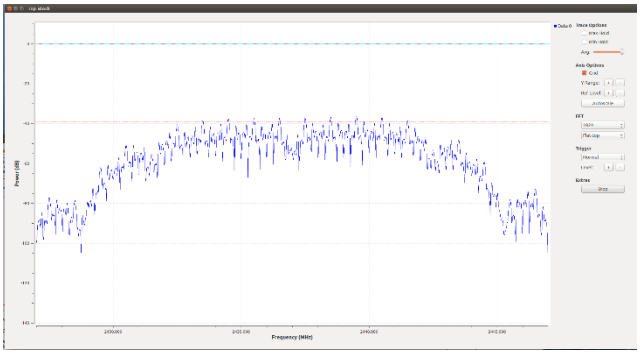

**Fig. 8.** GNU Radio Companion screen capture of router-bridge link spectral response. Spectral amplitude range is approximately *-45* dBm with a noise floor at *-95* dBm.

The memory requirement for the SDR file sink recording I+Q will be *2x4 =8* bytes/sample. The estimated files size for a *30* second SDR file-sink recording:

$$N_{SAMP} = 25 \text{ MHz x } 30 \text{ sec x } 8 \text{ bytes/sample} = 6 \text{ GB}$$

Some care was required to process the GRC binary file in MATLAB. Figure 9 illustrates the raw data I+Q records for the GRC measurement. The binary data file contained well over the 1.5 million count shown, however the router burst can be seen.

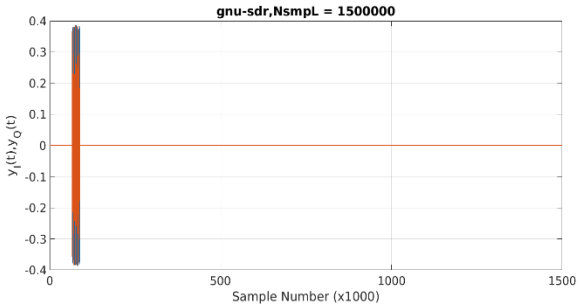


**Fig. 9.** Raw data I+Q records for GNU Radio Companion measurement example.

The MATLAB post-processing algorithm for Figures 10 and 11 was identical to the method outlined in the previous section. The location of the router burst was identified, an average index between the I+Q maximums was determined. The time- and frequency-domain window sequence was centered around the averaged index.

Figure 10 is an illustration of the in-phase and quadrature time-domain responses for the GRC measurement example. Comparison of the time-domain waveforms recorded from the spectrum analyzer illustrate the different sample rates, where the spectrum analyzer sample rate is roughly twice the SDR sample rate.

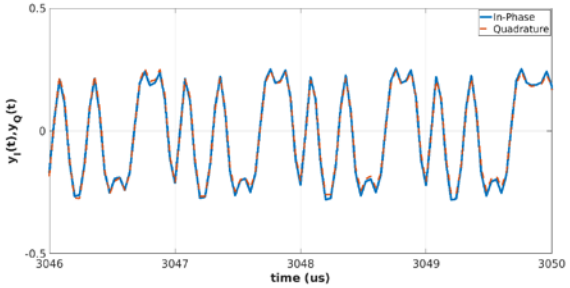


**Fig. 10.** I+Q time domain responses for GNU Radio Companion measurement example. *N=256* for the example shown.

Figure 11 is the FFT-processed, normalized-amplitude spectral response for the GRC measurement example. Aside from the scaling of the two spectrums due to the different sample rates, the FFT amplitudes responses are similar.

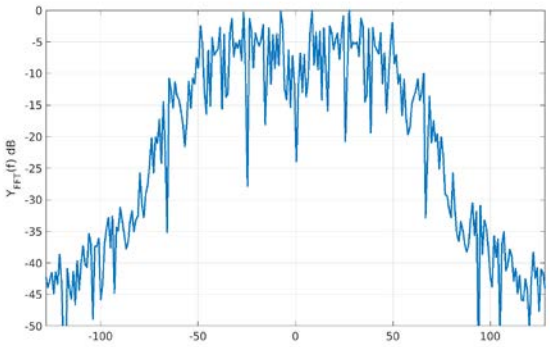


**Fig. 11.** FFT processed normalized frequency domain responses for GNU Radio Companion measurement example. *N=256* for the example shown.

## 3. Discussion

Preliminary results indicate the router test-bed comprised of readily-available wireless routers, coaxial cable, connectors, pick-off tee and divider will provide low-noise, and repeatable signal captures. The encouraging low-noise floors shown in both recordings will be useful in the development of SDR-based receivers. Preliminary playback tests of recorded data have been successful and will be developed as

a means to assess quality of the recorded signal. Unexpected challenges included containment of wireless-router spurious RF emissions, and prohibitively large data files.

### 3.1.1 SIGNAL CAPTURE PLAYBACK

Recent access to the INL anechoic chamber allowed a signal capture playback test in an ideal low-noise environment. Figure 12 is an illustration of the playback test geometry. A data record stored on a USRP X310 is played back in transmit mode. The long-range WiFi adapter receives packets from a recorded signal played-back or transmitted from the USRP X310.

Once a better laptop became available for the project, the recording times were increased to *90* seconds. The corresponding file size was approximately *18* GB. The DD-WRT default beacon rate is *10* beacons/sec. Under ideal conditions, the long-range WiFi adapter would receive approximately *900* beacons per recording.

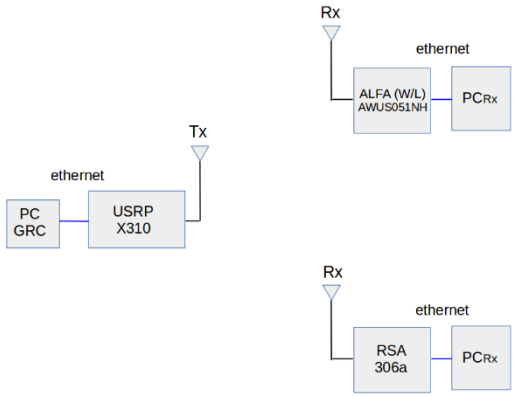


**Fig. 12**. USRP X310 configured for playback test of recorded data.

Preliminary results indicate a recorded signal played back in the configuration shown has a beacon receive rate greater than *90*%. Work is underway to utilize the playback test as a metric to quantitatively assess captured-signal quality.

### 3.1.2. CHALLENGES

The visual results and preliminary playback test results discussed in the previous sections are encouraging. However, the project objective to focus on a hardware-based signal generation has presented challenges. For example, preliminary results indicate the transmit and receive gain settings for the USRP X310 signal recording affect the number of packets received for a playback test. In addition, a preamplifier in the spectrum analyzer affects the dynamic range of the recorded data. Efforts continue to identify previously unknown parameters and to establish a reliable calibration procedure before completing signal captures.

A second laboratory challenge encountered was due to the use of low-cost commercial-off-the-shelf (COTS) wireless routers. In short-range laboratory environment, spurious RF emission coupled with adaptive software created a curious result. Successive antenna ports would be terminated with *50 Ω* loads where ultimately, all four ports were terminated. With a point-to-point range of approximately six feet and no shielding, the repeater link would remain intact. In-situ shielding with aluminum foil isolated spurious router RF radiation in most cases.

Recorded data files sizes are prohibitively large in non-binary formats. For example, thirty seconds of recorded data for the SDR generated a 6 GB binary file. Converting the entire record in binary to **.csv* text format resulted in a 34 GB unmanageable file. Post-processing required care to manage and should be considered when assembling a data base of signal captures for research.

Future experimentation with the spectrum analyzer will focus on the control of the sampling frequency to compare with the ethernet-limited sample rate for the USRP X310.

## 4. Conclusions and Future Work

Preliminary measurements of a WLAN wireless router link testbed under development at the Idaho National Laboratory Wireless Research Center have been successful. Repeatable, minimal noise wireless transmission for SDR analysis and research are easily obtained using COTS equipment.

The testbed was created at minimal cost. Modifications to future technologies (e.g., LTE) and field tests should be straightforward. Examples of near-term future work implementing the testbed include:

- Replace one of the routers with a second SDR to simulate a 'replay attack'.
- Reinstate a wireless link between one router and the pick-off tee to measure/characterize noise environments. One benchmark measurement in this configuration will be at the outdoor wireless range (low-noise, desert setting).
- Noise source modification: A schematic of proposed future modifications to the Wi-Fi Link Testbed is shown in Figure 13. Modifications could include a combiner to introduce a controlled noise source to the channel. Bandwidth control could be facilitated with a band-pass filter at the noise input to simulate partial band interference environments.

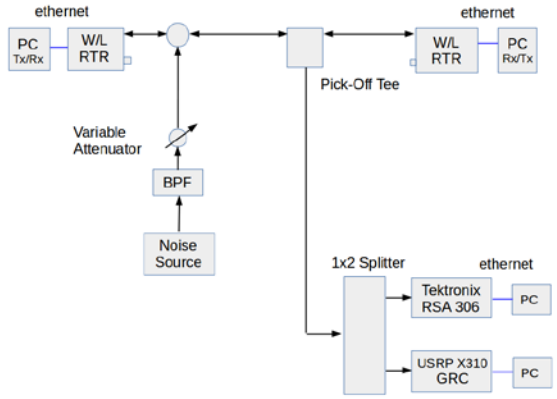


**Fig. 13.** Future configuration for Wi-Fi Router Link Testbed. A noise source with variable attenuation and narrow band pass filter response will be integrated to the testbed channel.

## Acknowledgements

The work was completed at the Idaho National Laboratory, cyber security and wireless research laboratory. Support was provided through the Department of Energy Visiting Faculty Program.

## References

[1] CRAWDAD. http://www.crawdad.org/

[2] ITU-R BT.2035, *Guidelines and techniques for the evaluation of digital terrestrial television broadcasting systems*,

[3] FCC-ID: Q87-WT54GV40 CCS, *EUT:Wireless-G Broadband Router with Port Switch*,