Notes on SDR

J.D. McCormack

2015-07-01

1 Introduction

The following document will contain information related to my efforts in software defined radio. From time to time, the document may include information on other topics as well. It will initially serve as a day to day journal of my activites. After a certain discovery phase, this document will be updated to create a manual or tutorial for future students to learn from. It is not recommended that the document be used for self study until a newer version is created. Many of the steps that are outlined will be dead ends or poor practices while the disocvery process takes place.

Starting from the bottom and working up may be useful.

2 7-1-2015

Currently working on using the RTL SDR.

What I have learned so far:

- This SDR is different than a FUNCUBE dongle
- It will work from around 500 Hz to 1700 Hz
- It can only RECIEVE

The fact that this can only recieve is by far the largest setback. This will ultimately not be what we can use for cognitive radio.

However, the tutorials still seem more widely available than those found for the BladeRF which is bi-directional. Therefore I will continue for a bit. It may serve a purpose as part of the larger sensor network at some point. We could still use it to relay information over a large distance.

There are "Cubelites" being sent out that are basically funcube dongle based satellites. These sound pretty cool.

I want to start taking notes in Latex so they will be more readable than a plain .txt file and still useable with version control.

I need to install texlive-full and texmaker.

Currently I am set back by needing to update ubuntu. I can't install anything else while the updates are installing.

Success So far I have made decent progress. The RTL is working with GNU SDR. I had trouble at first when the kernel was loading a separate driver that bogs it down.

I used this command to fix that problem:

```
# sudo rmmod dvb_usb_rtl28xxu rtl2823
```

There are more permanent ways of fixing the problem but I wanted to start with this as it is non-permanent and will default back to normal on a restart.

The new file in the RTL-SDR will allow you to hear FM stations. But they are extremely faint. I'm going to continue to play with the file settings to see if I can get a clearer transmission.

3 7-2-2015

I began the day with a quick interlude into learning LaTex. After about an hour and a half of studying I was able to produce the document you are currently reading. I'm not making use of many libraries but I believe it already seems more organized and official than my traditional notes. Also, it is much more portable than a normal word document and less prone to formating failures seen in google docs.

Yesterday I got the SDR to recieve FM stations. However, they were staticy and sounded slowed down. I'm not sure if this is an error in my demodulation values or just that the computer that I'm using is too slow. I tried using a different one but that ended up being slower than I remembered. I will try to get linux installed on my laptop later tonight when I'm done working, but I'm not confident it will work as I had trouble in the past.

Today I will try to replicate the results I had yesterday, but through the use of the python libraries instead of relying on the GNURadio GUI interface. A small note about the gui interface. I did learn that its possible to make variables, attach them to GUI widgets, and then alter then live. It appears that having more than 3 of these can severely impact performace. To use the GUI widgets, simple drag one onto your workspace (I used the Wx widgets) and then give it a unique name, and appropriate value range (if its a slider). Then in the blocks for different components, you can use these variable names instead of hardcoded values. This is useful for gains and frequencies.

/paragraphGNURadio in Python

I will be following the tutorial found here. I will begin with the dial tone generator.

Static I'm still only getting static when I run the RTL-SDR. I was able to use the GNURadio toolchain from just python no problem, however I still need to implent the RTL-SDR from the python toolchain. I used an additional tool put out by osmocom but that did not product better results. Automatic gain was on, so its possible I need to manually set the gain, but I am not sure. It could also be the poor quality of the antenna. the command was:

```
# rtl_fm -f 96.3e6 -M wbfm -s 200000 -r 48000 - | aplay -r 48k -f S16_LE
```

aplay is a command line utility for playing audio. I had to run that separately as piping the data did not seem to work. I got this command from osmocom's website

4 07-03-2015

I will not have much time to work today due to the holiday weekend. I will try to get Linux installed on my laptop in my free time. Either tomorrow or next week I will try to find a python example using the RTL-SDR driver. After that, I may switch gears back to the BladeRF.

5 07-04-2015

Happy 4th of July! No progress will be made today as I'll be busy all day.

6 07-05-2015

Didn't get a chance to work today either. Family event. Will continue progress tomorrow.

7 07-06-2015

Back to work today. I was attempting to install a program called Gqrx. Using the instructions from their github I added a repository and installed just the gqrx program. However, this created a massive conflict in my repositories. I uninstalled and figured I would just go back to working on the FM model to see if I could be sure its working right. However, installing that package messed up my installation of gnu radio. So now I must uninstall and reinstall evertyhing. At the time, I was following this tutorial On Gqrx. I found a person with a similar problem to mine here. There are instructions below on how to reinstall everything. I will be trying that next and will hopefully get back to where I was. It may also be time to start learning more about virtuan environments or just how to reimage a computer quickly.

Currently trying to use the following command to reset the broken packages. This is taking a long time so I will have to wait for it to finish in order to continue reinstalling gnuradio. The command is:

```
# sudo apt-get dist-upgrade
```

This did not end up working. Next I tried using aptitude, which as I have read, will work to fix these broken dependencies and packages. The command for that is:

```
# sudo aptitude install <packagename>
```

Still trying to get everything installed and working. The repository made GNURadio work again, but I lost the Osmocom packages. Still trying. I have been following the instructions direct from osmocom but I'm getting errors related to "Gruel" when I try to use cmake.

Success Finally remembered that the instructables I was using previously had the commands listed (although for arch). The three necessary components can be installed by using:

```
# sudo apt-get install gnuradio


# sudo apt-get install rtl-sdr


# sudo apt-get install gr-osmosdr
```

As a note, the instructable used arch linux and the final package was installed as gr-osmosdr-git. Debian/Fedora/Arch users may need to use this form of the package instead of gr-osmosdr. Another github was found here with plenty of examples. They may be out of date as the AM example did not compile correctly. Another useful site was found here this site had a single example, but it seemed to be working. I'm going to try to test to see if I can use my CB radio with this. I think it will be too low of a frequency, but this would make testing the blade very easy as I can control the transmission with just the hand held radio.

R820T So after trying to find a software solution for determining which tuner the device was using, I decided that the smarter solution was to just open the SDR up. The chip inside is the Rafael Micro R820T. This is GOOD. Next to the elusive E4000 this is the best possible tuner to have. Its range is 24-1766 MHz. Not quite as high as the E4000 but much lower than that one and much higher than any other tuner that it could have had. I'm pretty happy. The device came apart with no tools or fuss, everything was just snapped together. The device even went back together when it was done!

CB Radio After a bit of struggling it looks like I'm able to pick up CB signals. The main issue I have now is that without better knowledge of signal processing I can't properly adjust the FIR filter. So I am able to recieve CB signals but they are not specific to any channel. The antenna that comes with this RTL-SDR is also awful. If I transmit over wireless I recieve really garbled sounds. If I unscrew both antennas and connect by contact it is crystal clear but still not on any specific channel. I don't think I'll spend much more time on this however. The file is on github under the name airband_4.grc and airband_5.grc. The 5 was an attempt to fix some of the issues with the downloaded file. It was called airband_4 on the website because it was able to pickup 4 different AM broadcasts used by airplanes to communicate.

I found two resources to keep track of for general SDR and DSP information.

- http://complextoreal.com/tutorials/#.VZr6nKH7s_t
- http://greatscottgadgets.com/sdr/

8 07-07-2015

Today I will be taking a look at the bladeRF SDR. The first problem that comes up is it appears I forgot to bring a compatible antenna with me. I have to double check all my stuff to be sure, but due to the typically large size of these antennas I think it is likely that they got left behind. Anyway, despite not having an antenna I'm going to push on anyway and then see what I have lying around. I should be able to order something on Amazon fairly quickly if needed anyway. Nuand is nice enough to have a fairly detailed set of documents on their github account. It also looks like these may have been updated since the last time I went through this process. The github account is found here. I also just saw on this webpage that there is now matlab support for the bladeRF on windows. I'm not sure if this was always a feature or if this is indeed new to the program. Eitherway it is something to be aware of. It has support for Simulink too.

Following the tutorial, the first step is to add the appriproate repository so we can download the files. There is a snapshot section that allows you to get the most up to date releases but these are usually far from stable. The commands used are.

8.1 Install BladeRF

The commands are:

```
# sudo apt-get-repository ppa:bladerf/bladerf

# sudo apt-get update

# sudo apt-get install bladerf
```

Of course I immediately get an error saying "you have held broken packages." I should probably do more research into how to avoid this scenario, as it seems to come up quite a lot in working with GNURadio. This could be related to using the other PPA from before. I'm going to try to use aptitude to install this and see if that helps. Aptitude seems to be able to solve the problem, however it will be removing:

- gr-osmosdr (which I know I need)
- libbladerf0
- libgnuradio-osmosdr0.0

So I know that all three of these libraries are needed to run the blade and all but the libbladerf0 are needed to also run the RTL-SDR. I'll give it a shot and see what happens, I can always reinstall from the repository (I Hope). After running

```
# sudo aptitude install bladerf
```

and accepting their suggestions it seems to have installed properly. I also ran:

```
# sudo apt-get install libbladerf-dev
```

but it seemed to have already been installed. Now we can install the updated FPGA drivers.

8.2 Download new firmware

The commands are:

```
# sudo apt-get install bladerf-firmware-fx3

# sudo apt-get install bladerf-fpga-hostedx40

# sudo apt-get install bladerf-fpga-hostedx115
```

It's worth noting that we have the x40 not the x115 so we only need to install the x40.

8.3 Reinstall GNURadio

The next step seems to indicate that I should build the gnuradio from sources and not use the version found in the repository. Luckily, BladeRF links to a download script that pretty much puts cruise control on. Hopefully you have luck too. Here are the commands.

```
# mkdir -p  /software/gnuradio-build

# cd  /software/gnuradio-build

# wget http://www.sbrac.org/files/build-gnuradio

# chmod +x ./build-gnuradio
```

```
# ./build-gnuradio -m prereqs gitfetch
```

It took about 15-20 minutes to finish but everything downloaded successfully. Afterwards its necessary to actually build the downloaded programs. I followed the steps outlined to build GNURadio and the program halts halfway through with a cryptic error message. Hopefully I can diagnose the problem because it took roughly an hour to get that far.

Success! I ended up needing to use the Pybombs tool. It worked like a charm. This is linked to in the github wiki mentioned above and also found on the GNUiRadio webpage.

9 07-08-15

Today I will be traveling and not have much time to work. I spoke too soon on the success of pybombs. It looked like it worked and it did install the BladeRF software properly, however the GNURadio software did not. I tried several times and at one point got an error about the jdk which wasn't listed as a prereq. I tried the plain build again and got much further (89% vs 56% originally). I'll try running it again and see if it goes any further.

10 07-09-15

Today's focus switched to some open tasks I had with Dr. Integlia. The first is a comparison of various FPGA platforms available. After looking at everything, I am most excited by the offerings from digilent, especially the Zynq based boards. These have an onboard FPGA and a microprocessor onboard. I also prepared a comparison of SDR platforms. One board even had a Zynq SoC on board that was programmable. This could lead to interesting research down the line as students become better at using the FPGAs. The FPGA comparison is available in this repository but for now the SDR is not. I will try to migrate it here soon too.

11 07-10-15

Today I started the Literature review. There is a lot of ground to cover. I got through 14 sources. So far the general gist of what I've read is that the USRP is the go to SDR for research, but that people are excited by the RTL-SDR. GNU Radio seems to be very well recieved for both simulation and real world testing. I'm curious to see if some of the other software tools identified have a following in the academic world too.

I also learned how to use the IEEEtrans format for Latex and how to use Bibtex.

12 07-11-15

I won't have as much time to work today but I will try to get some amount done. I need to port the FPGA comparison to excel and continue the Lit Review. I will be trying to spend most of the afternoon working through Node.js and research graduate schools. I've been keeping up on Node.js fairly well but have been falling behind on Grad school searches.

13 07-12-15

Today I will be converting the Latex notes into an excel spreadsheet for sharing. I may not have much time to work today or tomorrow but I will put full days on Tuesday and Wednesday.

14 07-13-15

I'm going to try to make some more progress on the SDR today. I realized I may be more limited by this computer than I thought. It only has USB 2.0's at best and that could be throttling it too much as this is a USB3.0 boad. Regardless, I'll keep trying to build GNURadio for it to at least get the correct way to set that up.

First run:

```
# git clone https://github.com/Nuand/bladeRF.git
```

From there I followed the directions found on their github account here. In step four I switched to the directions here and was able to build the software without errors. You can check to make sure it worked by running

```
# bladeRF-cli -e info -e version
```

or

```
# bladeRF-cli -p
```

So now again I was back to the point where I needed to build GNURadio. I also need to load the drivers to allow for the expansion board, but one step at a time.

Here I would like to point out that it is possible to just use a live CD to run all of this without having to configure anything. However, the live CD does not come with the ability to install itself. I'm not sure what their thought process was for that, maybe to keep everything fresh and up to date, but it is a huge inconvience. If all else fails, the live CD combined with github would allow you to rebuild the environment pretty quickly each time. There is also direct support for bladeRF in Pentoo, a penetration testing varient of Gentoo. I can try this route if all else fails.

I am currently Running PyBombs again to try to get GNURadio to install. Hopefully it works this time, but it is unlikely that it will.

15 07-14-15

I don't want to speak too soon but it looks like GNURadio may have installed. I need to make a note of the following:

```
#  $prefix =  /software/BladeRF/bladeRF/build/target
```

I had been running the following without the sudo command, adding sudo seemed to work. I'm not sure why I didn't see a clearer error before:

```
#  sudo ./pybombs install gnuradio
```

For reference. Pybombs is located here:

```
#  /software/BladeRF/bladeRF/build/pybombs
```

The steps to open GNURadio were:

```
# : /software/BladeRF/bladeRF/build/pybombs$ ./pybombs env


#  /software/BladeRF/bladeRF/build/target$ source setup_env.sh


#  /software/BladeRF/bladeRF/build/target$ gnuradio-companion
```

After installing a few other modules and running an old test program, I can confirm that it is back up and running with the RTL-SDR. Now I am beginning the test with the BladeRF. One problem with the BladeRF is in order to easily test a signal I will have to use the transverter board. This is mostly because FM/CB Radio channels are below the normal operating range of the board. To activate the transverter board use the command:

```
# bladerf-cli -i


# xb 200 enable 200
```

Note the spaces in the command. The first command is just used to bring up the interactive inteface. This command was listed wrong on the wiki page, so I submitted a request to edit it accordingly.

A book to be aware of can be found here. This book's link was also incorrect so I fixed that on the wiki as well.

The biggest issue now is trying to remove the DC offset. Everytime I open the radio in the GNU Radio Companion there is a large spike in the center, and no audio is heard. Currently, my computer keeping freezing whenever I try to run anything using the BladeRF, I believe this may have to do with the limitations of this computer. I will begin trying to get Ubuntu running on my laptop tonight. First I have to clear off a lot of space on the harddrive. It may also have to do with the fact that I am using USB 2.0 ports on this computer. If thats the case, chaning to my laptop will not fix the problem.

16 07-15-15

Spent today trying to install Linux on my laptop. It still isnt cooperating. The problem is the laptop already has 4 partitions on it and HP did not make any of them extended by default as it should be with that many. I am currently trying to copy everything from a recovery partition, onto the main hard drive. I'll then wipe that partition and reformat it. Hopefully it doesn't corrupt my computer. After correspondance with Dr. Integlia, I am now aware of some other ongoing goals. These include:

- Preparing for next semester's courses
- Creating a short document
- Creating a longer more comprehensive document
- Identifying more conferences

I will continue spending today trying to install ubuntu and begin the transition tomorrow.

17 07-16-15

I ended up breaking my computer today while installing Ubuntu and corrupting the windows portion. I unloaded the documents I needed and then starting over with Windows 10 and Ubuntu. Everything works now and I can access google drive again.

18 07-17-15

Worked on the document for Harris corporation. The document can be found in this repository and on google drive.

19 07-18-15

I will not have much time to work today, and probably not much tomorrow. I should be able to make a bigger effort this upcoming week however.

20 07-19-15

Spent the day going over advanced MongoDB work in Node.js. I also had time to begin creating the example problems for the Circuits I class. I will be traveling tomorrow.

21 07-20-15

I will be traveling today with limited access to a computer until tomorrow.

22 07-21-15 to 07-24-15

I am traveling with limited access to SDR equipment. I have been continuing with the literature review list this week and hope to have 20 sources idenfitied by Monday

23 07-25-15

Today I will be working remotely from a friend's office for a few hours. Going to try either getting the SDR back online or to try to finsih up the literature review.

23.1 PyBombs

I still havent had luck with pybombs on the HP Laptop I am working from. It worked on the older computer no problem once I used sudo. I am currently reinstalling it. I have noticed that if I sudo whilte running PyBombs for the first time then the program is not able to be installed. The only chnanges I made this time were selecting "Force install" for everything I knew I would need ahead of time, and setting the number of threads that make could use to 8. I'm not sure if this will prove to be helpful at all. The 8 threads may have been too many as now I'm having trouble running other programs at the same time (music slows down and skips and even vim is noticeably less responsive).
It looks like everything is now installing correctly. The only changes were made were the ones specifed. After install gnuradio, I'm not installing RTL-SDR, BladeRF, and some other packages that sound useful. Once they are done installing its important to remember that you actually need to activate them within the environment you are using. They will not stay permanately active in linux. To do this we navigate to the "source" destination. For me, I just had to go one folder up, and then it was listed under target. If you cant find where it is, just install something else and pay attention to where it says it is writing the files . Then go to the appropriate folder. Once in there, run:

```
# source setup_env.sh
```

After testing it seems everything is back to working, at least with the RTL-SDR. Now I can begin testing with the BladeRF upon my return home. An important note is that I had a slowed down audio effect. It turned out I had miss matched sampling rates. One was being set manually, while another was being set by a variable. I hadn't noticed that there was a discrpency and now the audio sounds normal.

24 07-29-15

I was able to do a quick test once I got home to try out the BladeRF. It is working with GNU Radio now but still needs to get the DC offset fixed.

25 08-04-15

I'm back to working on the BladeRF after a brief hiatus. Currently, I am seeing if I had to reload the FPGA manually. To do this I use the command:

```
# bladeRF-cli -l <path/to/fpga/file>
```

In my case, the fpga file was stored in downloads. The FPGA file can be found on the Nuand website. I also learned that there are string arugments that allows GNURadio to add the xb200 as well as automatically load the FPGA firmware. More information can be found here.

25.1 09-14-15

Finally back at it. Today I will be focusing on the Ettus Research USRP B200 board. I'm going to try to follow the tutorial found at Ettus Research. I was able to use pybombs to install the first set of software. This was simply called "UHD" under the hardware tag in pybombs. As last time, make sure you start pybombs with sudo. There was another set of drivers called "Ettus" that would not install. I later saw this comand

```
# sudo apt-get install libuhd-dev libuhd003 uhd-host
```

It said the last two were already installed, but then installed libuhd-dev. I'm still getting errors that the device is not found in GNURadio. Typing in "lsusb" shows that Linux doesnt seem to recognize the device. I'm going to reboot and see if that helps.

That did not fix the issue. Next, I double checked that "apt-get" covered everything. As some part of the install may be from pybombs, which creates a virtual environment, I'm hoping that this does not cause a mismatch. Ok, so that had no effect. I'm going to google a bit more and see if I can figure out what I'm missing.

```
# uhd_find_devices
```

Can be used to locate the device. Originally, it was throwing an error message. Similar to the below:

```
# /usr/bin/uhd_find_devices:  symbol lookup error:


# /usr/bin/uhd_find_devices:  undefined symbol:


# _ZN3uhd6device4findERKNS_13device_addr_tENS0_15device_filter_tE
```

Which brought me here. Eventually, I discovered that the main issue was I had used the repositores to download the 3 files shown above (libuhd-dev, libuhd003, uhd-host) and then also done the commands shown below:

```
# sudo bash -c 'echo "deb http://files.ettus.com/binaries/uhd/repo/uhd/ubuntu/`lsb_release -cs` `lsb_release -cs` main" > /etc/apt


# sudo apt-get update


# sudo apt-get install -t `lsb_release -cs` uhd
```

When I went back and used

```
# sudo apt-get remove libuhd-dev libuhd003 uhd-host
```

and then ran

```
# sudo uhd_find_devices
```

I got the below message showing that it was now registerd:

– Loading firmware image: /usr/share/uhd/images/usrp_b200_fw.hex... done ——————————————————————————– UHD Device 0 ——————————————————————————– Device Address: type: b200 name: serial: 3087692 product: B200

However I'm still getting an "Empty device address" error in GNURadio. I did recently read that with out using USB 3.0 (my computer only has 2.0) It may be necessary to use either an external power adapter rated at 6 V, 3A or to use one of the 2 A to 1 B type connectors. I saw a brief document saying it may be an issue with not having root access, but running in a shell with root access via

```
# sudo -i
```

did not change anything.

Eventually I Came across the command

```
# uhd_usrp_probe
```

. This loaded the firmware and FPGA. After running this and returning to GNU Radio, I still am getting the errors as before. It looks like the problem may be in switching into the virtual envinronment created with pybombs. I ran the uhd_usrp_probe command again and it mentioned that there were no images installed. The error message provides a command to run which will download the images. The command for me was

```
#  /software/target/lib/uhd/utils/uhd_images_downloader.py
```

But make sure whatever you run is whats given to you in the error output. I then ran the uhd_usrp_probe command again but got errors about the compatibility error:

```
# Error:  RuntimeError:  Expected firmware compatibility number 8.0, but got 7.0:
```

With information saying to run the same image downloader python script.

At this point I realized I messed up more than I can probably recover from easily. I tried to delete the images but wasn't double checking the folder I was in and removed the entire target directory that pybombs outputs to. So I'm going to cut my losses and go back to the Ettus page and install GNU radio per their instructions instead of fighting pybombs to get everything to work.

While going through the documentation trying to find the GNU Radio section, I realized there is a post-download set of instructions found here. I'm going to go through those now which include

```
# uhd_images_downloader
```

.

Also changing a configuration so non-root users can access the radio:

```
# cd <install-path>/lib/uhd/utils

# sudo cp uhd-usrp.rules /etc/udev/rules.d/

# sudo udevadm control --reload-rules

# sudo udevadm trigger
```

For my case, ¡install-path¿ was simply "usr".

I was hoping to just use apt-get to install gnuradio but that installs otherfiles not compatible with the UHD drivers installed earlier. Using the same remove command we used the last time we got the error message worked (apt-get remove gnuradio was all that was really needed though). Back to square one.

26 09-15-15

Last night before class I ran the GNURadio build script found here. After it ran I was still having issues. I tried re-running it to just install the UHD Drivers, but I had to go to class. When I got back it was waiting for a user acknolowedgement (press the Y key). So I don't believe it actually ran. When I got in today I ran

```
# sudo apt-get remove gnuradio
```

again to see if that would remove the build script install. It clearly stated it was removing something, but when I got back to the terminal and ran the USRP Probe command and then gnuradio suddenly everything was working. I'm assuming the one from sources never uninstalled and was actually the one that ended up running. Its likely I forgot to uninstall the one from the repositories and that that was the one that was causing issues. Either way, there is now "appropriate sounding static" on the audio from the FM block. I'll have to run further testing once I finish with TA stuff for the day to make sure its working. I should be able to broadcast FM and pick it up on the spectrum analyzers. I assume I will be unable to get FM in the VTC due to the nature of the building. I could always bring it outside to test though.

I am currently following this tutorial to try to get a transmitter setup: HERE

27 09-16-15

Today I succesfully managed to send FM radio broadcasts out of the SDR. The blocks can be found in this github repository. I followed the tutorials from Ettus Research.

28 09-18-15

I found this helpful presentation from WPI.

There's also the main webpage found Here

They have a textbook available as well Here

I have success creating a python program that slowly ramps up the frequency it is outputting. Using my trusty Tivoli Audio PAL radio I was able to keep turning the dial to keep the signal in tune. The key was to put a separate thread to handle this task. I realized this when I saw that the gui function used a callback. This prevents the function that changes the frequency from blocking the flow of data through the other filter blocks. This file is saved as FMThread.py and will be shown below.

I also found this helpful website HERE which organizes many of the various out-of-tree modules for GNU Radio.

I am now following the install procedure for the gr-ieee802-11 block. This block can be found here.

The system seemed to install fine using te procedure outlined on the github page.

29 09-24-15

I'm going to try to take a deeper dive into some literature today, and hopefully identify some conferences/publications in the process.

first search term used is "mesh network gnu-radio", it returned 1 result

Next I searched for examples of Batman-adv with GNUradio, but recieved no results over the course of several command variants.

30 09-25-15

I found an interesting talk from a technology evangelist from Ettus research. His website is here. The talk can be found at this location.

He also discusses building a home made doppler system. Here is a presentation discussing this in more detail.

31 10-2-15

Found another useful ppt from Ettus here.

32 10-23-2015

Today I started playing around with the Ettus Research E310. Im so excited to get to work with this piece of cutting edge technology. I was able to start by connecting to the device over UART with the USB connector plugged into the "console" port. For Linux, this would probably work out of the box. For windows you'll need The FT230X driver from FTDI We'll be using our noble terminal emulator Putty to help too. We need to get an x-server setup on our computer so that we can view the GNU Radio GUI. To do that we'll use XMING. This can be found on sourceforge. Finally, we'll need to configure Putty properly as shown here. This let me acces GNU radio fine and I could see the window on my computer. If any of the links are dead, just try googling some of the keywords. Nearly all of the links I used were just the first or second result.

33 11-1-15

I have started researching TUN and TAP Adapters. These seem to be the key to what we are trying to do but I am not confident enough to say that. TUNs are virtual ports that accept IP packets and TAPs are ports that accept virtual ethernet packets. In theory I should be able to use a TAP to abstract out the MAC Address, but that doesnt seem the case. The way I understand it TAPs are the layer that connects PHY To MAC and TUNS connect MAC to layer 3. I'll continue to research these topics.

34 11-3-15

I found this link: http://www.wu.ece.ufl.edu/projects/wirelessVideo/project/GNU_Radio_USRP/ Example 3 provides some insight showing that my thought process is correct. I wish there was a flow graph for reference but it is just a python file. I will continue looking into this.

35 11-7-15

Need to look into how the Zigbee protocol is implemented. Basically it looks like the PHY layer needs to not only accept and transmist the complex signal, but also needs to convert complex to and from packets. These packets may then be able to be passed to Batman adv over a TUN interface.

- ask questions first posted to him directly
- post questions to github.
- ask for 802.11 traditional transciever
- run zigbee
- run 802.11p
- compare the implementations and look for differences

- identify questions about the differences.

Now trying to connect my linux laptop to the E310 using ssh -X root@192.168.1.100

36 11-14-15

Spent most of the day trying to build the UHD driver on the E310 itself. This took about four hours to do. There still seemed to be an issue. I'm going to continue orking tomorrow. The website I am looking at right now can be found here:

Link to the other person's website

37 11-15-15

This E310 is still giving me a ton of problems. I spent about 3 hours this morning trying to get everything to place nice. The issue seems to be that the E310 is running UHD version 3.08 and my PC is running 3.10. I'm not sure how this is happening is both should have been built from sources which makes me think I'm either missing something in the install process or I have a version installed from a different source and I'm not noticing. When I make uninstall on both the PC and E310 there are still versions of the _uhd_usrp_probe software. I found this message on the gnuradio mailing list that seemed to indicate I would have to roll back the PC version or reflash the SD card. I'll have to continue working for now as its going to be awhile until the B200 gets here. I may also continue looking into Vagrant tonight as it would be helpful for trying to switch back and forth between versions quickly.

38 11-17-15

So currently it appears that I have rolled back the PC to the proper version of UHD and it apears this may be simple to switch between the two versions should I have broken something. Basically, the repository version of UHD is version 3.008 and the sources version is 3.010. So a make install or make uninstall will add and remove 3.010. On the other hand a sudo apt-get install uhd or sudo apt-get remove will do the same for version 3.008. Hopefully when I try this tonight everything works out. This will also help when it comes time to fix the vagrant file.

Currently with vagrant I am unable to install UHD from the gnu radio sources. If we end up going with 3.008 I will just apt-get UHD. When I run GNU-Radio companion I get an error about the python path. If this goes away I wont discuss it further, but if it continues I'll include some screenshots and such to help with debugging.

39 11-19-15

This link may help clarify some issues: Here

40 11-20-15

Found a link to a washington state course. It has details about several lab exercises done out in both matlab and gnuradio http://courses.washington.edu/ee420/assignments.html

41 11-22-15

Almost forgot to save this webtie: http://aaronscher.com/$GNU_Radio_Companion_Collection/Packet_encode_decode.html$ It has a lot of useful information. I was able to use it to transmit an image through a flow graph, but so far I have been unabe to transmit over the air.

Some more useful links are below: http://www.trondeau.com/grcon15-presentations/

42 12-22-15

Finally got back to work on this after a mountain of finals and TA work. We have the B210 and I wanted to get a feel for working with the dual channels. The key is in the subboards sections. RF Block A needs to be set as A:A, and RF Block B needs to be set as A:B. I was successfully able to transmit and recieve on the TX/RX line of both sides.

43 12-23-15

Ran some more tests today. I was unable to get batman-adv working over zigbee following "the easy way" I had initially hoped. However, there are a LOT of variables and different settings that I have to confirm are all in sync before continuing on. I also am working off of just the TX/RX antennas and I am unsure if they automatically function in full duplex mode or if that needs to be managed. I ordered two additional antennas on amazon so that I can use separate TX and RX channels instead of one single channel for each.

44 12-29-15

Met with Mathworks yesterday to discuss options from available for working with SDR. I'm excited to begin working with Houman and the rest of the team on this part of the project. Hopefully things will go smoother using a full featured piece of software versus the open source software we have been using. I would like to continue working with GNURadio while I still have a chance however as I believe some things, such as interfacing into Unity, will be significantly easier being able to use python than having to use MATLAB.

45 1-5-16

I was finally able to test out my shell script that creates a GNU Radio Companion environment on a computer. It worked awesome but I forgot to design it to install the UHD drivers for GNURadio. I think I'll add a module that goes to the end and then downloads and opens PyBombs to allow for the rest of the modules to be installed as needed. This will make the system more robust to future changes to GNU Radio.

46 1-7-16

Found an interesting article today: http://www.schooner.wail.wisc.edu/tutorial/docwrapper.php3?docname=gnuradio.html
http://gnuradio.org/data/grcon11/02-ge-gr_network_layer.pdf
http://www.profheath.org/research/mimo-system-prototyping/hydra-mimo-ad-hoc-network-phase-2/
http://gnuradio.org/redmine/projects/gnuradio/repository/revisions/58bd4ceaee4884652a682297a49957137cafa56d/entry/gnurad
examples/python/digital/tunnel.py

47 1-11-15

Found this video:
https://www.youtube.com/watch?v=g3-SjnES0K8
He shows a demonstration of the tunnel.py program located in gr-digital -¿ examples -¿ ofdm -¿tunnel.py
I tried this out but was unncessful in pinging. It may have to do with configuring the gateway/iptables.
The docs say tunnel.py is a poor choice for projects and will be deprecated in favor of gr-mac.
After rewatching the video the commands he runs are:

```
# ./tunnel.py -f 910.0M -r 100k

# ifconfig gr0 192.168.200.1

# route add -net 10.10.10.0/24 gw 192.168.200.2
```

http://static1.1.sqspcdn.com/static/f/679473/25468067/1411397041210/Sep15_06_Malsbury_Applications.pdf?token=G00WxKm

48 1-12-16

So as far as I can tell it looks like the tunnel.py file is deprecated and sore spot as far as GNU Radio's community is concerned. I'm currently looking into gr-mac and pre-cog. Its unclear which of the two is currently the well supported file (if either). There is a video explaining how to use pre-cog below:
https://www.youtube.com/watch?v=f8emQ-TvD90

48.1 SUCCESS

Batman-adv was attached to two USRPs running on separate computers utilizing the gr-mac library fork made by Baliant Seeber. The fork can be found below: https://github.com/balint256/gr-mac.git

This will need to be setup on two different computers using the following process:

```
# git clone htt[s://github.com/balin256/gr-mac.git

# cd gr-mac

# mkdir build

# cd build

# cmake ..

# sudo make

# sudo make install

# sudo ldconfig
```

Balint's fork doesn't have a very good readme as of the time of this writing, but following the original jmalsbury repo the next steps are below. His fork can be found https://github.com/jmalsbury/gr-mac

```
# cd ..

# cd example

# sudo gnuradio-companion gmsk_radio.grc
```

Then Build and Run this flow chart. Then:

```
# sudo gnuradio-companion ofdm_radio.grc
```

Then Build and Run that flow char. Next:

```
# sudo gnuradio-companion simple_trx.grc
```

Now we need to go to the first computer and follow the below commands:

```
# sudo python simple_trx.py --port 12345 --radio-addr 85 --dest-addr 86
```

In a 2nd terminal type

```
# sudo ifconfig tun0 192.168.200.1
```

Then we will go to the other computer and run the following commands:

```
# sudo python simple_trx.py --port 12346 --radio-addr 86 --dest-addr 85
```

Again in a 2nd terminal type

```
# sudo ifconfig tun0 192.168.200.2
```

Back to computer 1, in the second terminal type:

```
# nc 192.168.200.2 12346
```

In computer 2, in the second terminal type:

```
# nc 192.168.200.1 12345
```

you should now be able to type messages and see them appear on the other radio, if not, check all your connections and ensure there are antennas.

Now to add batman-adv we will go back to the first computer:

```
# sudo modprobe batman-adv

# sudo ip link set mtu 1532 dev tun0

# sudo batctl if add tun0

# sudo ip link set up dev tun0
```

On the other computer, the same commands are issued, repeated in case they need to be changed later:

```
# sudo modprobe batman-adv

# sudo ip link set mtu 1532 dev tun0

# sudo batctlif add tun0

# sudo ip link set up dev tun0
```

Then if you run the below command on either computer you should see one other batman node active:

```
# sudo batctl o
```

49 01-15-16

Confirmed that the flowgraph we are working from only uses the TX/RX antenna. This will obviously slow down the transmission of packets but may also present opportunities for using the RX antenna for another use such as ambient energy detection or to scan for other active channels.

We could potentially have this scan the ISM band and if a primary user or other instance tells the radio to move off it could then wait for a signal from another node to tell it which channel to begin transmitting on.

50 01-22-16

Having trouble setting everything up on the new computers. Looks like the issue may be as simple as the distance between the transmitters is too far. These Antennas arent exactly great and I have to use the adapters with them so this is very possible. I'm going to keep working to confirm this. It still works on the first two we used so if anything I will just make an image and copy that to the new computers.

51 01-23-16

Ok so here is the state of affairs. We have successfully send batman-adv packets over SDR, as was noted before. However, after changing things to be "broadcast" under dest-addr in the virtual encoder and virtual decoder I was able to successfully ping bidirectionally through 3 devices with no problems whatsoever. We are currently seeing extreme range limiting issues for some reasons that are currently unclear to me. I tried adjusting the frequencies through the init part of the automatically generated python scripts but that does not seem to be working. I'm not 100sure why but would guess it has something to do with the fact that these files are automatically generated and are not created by a true programmer. I also think this may be the reason why we were having issues with the three new computers in the center of the lab. I'm hoping to run more tests before I go home today. Joe is currently running bat-vis to show me how to map topologies.

I will need to make a quick start guide or something soon for automating the process of setuping up each node. We are planning to expand to 16 nodes and this could become quite difficult. I believe learning one of the terminal multiplexers such as screen or tmux would be beneficial for the future.

Important progress/updates this morning:

1. The board I thought was broken was just an error, I was using a USB 2.0 cable not a 3.0 cable which meant it couldn't get enough board power to broadcast, but could get enough to turn on which explains the weird error. 2. So far it appears the 3 computers weren't working because the boards were too far apart from one another. I realized in the original setup they were under 1 ft from one another. This is probably an issue with transmit frequency as it was operating at 980 MHz and the antennas are rated for 2.5 GHz. I will run some more tests throughout the day to confirm. 3. I was able to successfully send packets between 3 radios today. I made three changes and now will figure out which of the changes mattered. The first change was that I noticed you could replace "dest-addr" (Destination address) with broadcast in the gnuradio blocks in question (virtual-channel-encoder/decoder). I also noticed that in the "Channel Multiplexer" it is possible to increase the "Channel count" number higher and it will allow for more outputs. I snaked these outputs to the same locations as the originals and this allowed for the transmission. Finally, I ensured all the boards were within a few inches of one another. I realized in the original setup we were seeing the middle board able to talk to the 2 edge boards, so wasn't sure if it was a proximity problem. Regardless, one of these should allow up to continue forward.

If I can't get the 3 new computers working by around 4-5 today, I will work with Pat/Cody tonight to image them off of the first computer.

52 01-26-16

Successfully switched frequencies around and managed to continue transmitting packets. I have generated two new radio flow graphs that may eventually get merged into one. The first is called: "BroadcastMAC.grc". This allows for the changing of TX/RX freq and gain. This also has the virtual channel encoder/decoder set to broadcast. I believe this needs to be running on at least one of the radios in the mesh to work. The second block has a much larger name unfortunately and is called: "nonbroadcastwithGreqAndMac.grc". The difference between this and the other block is that I did not change the virtual encoder/decoder to broadcast mode and added the additon of a spot to change the mac address on the fly. This is useful in cases where you forget to change the mac address before running.

Next steps are to try to see if we can bridge internet access over these usrps with batman, to see how batman reacts to the changing frequencies, and to take steps to allow for automation.

As always, a more indepth literature review will need to continue.

53 01-27-16

So after playing around with GNU Radio for a few hours I found a block called "selector" within the gr-misc category. This is essentially a multiplexer that can map n inputs to m outputs. A simple change of variables decides which input and which output are active. This should help us with our search for PHY layer changes we had discussed.

Unfortunately selector only works on streaming blocks so a different device will need to be created. I'm currently guessing I can make this work fairly simply by just mashing the OFDM and GMSK together.

54 01-28-16

Still trying to get the selector stuff to work, so far it just keeps crashing whenever I change sources. Here's an interesting side project that may be worth looking into at a later point in time: Follow the link

55 02-05-16

Today I finalized some target conferences and journals. The shortest deadline I can see is March 1st. A tight window but we may be able to push the gnu-radio/batman combination paper through assuming we can collect and process the data in time. The biggest hurtle will be getting everything done prior to spring break as I dont think I'll have much time to work over that week.

Today I will go through the Practical Evaluation of BATMAN Advanced paper with Pat to try to understand their test process so we can replicate some of their work with our environment. This should help speed up the test development phase. I would LOVE to have all testing down by friday of next week so we can spend the next week drafting and finishing up the paper but I don't think that will be feasible as we probably need more than the 4 nodes we currently have.

55.1 Test Plan Alpha

This is the initial draft of how we are hoping to test the system:

- The test plan we are basing this from mentions testing from one floor to another. I'm not sure this will be feasible as the layout of the school is not conducive to this. We will most likely have two-three setups where we can utilize the VTC Alone, and then several rooms adjacent. I like the floor plan included in their paper and would like to replicate that to show how the networks form. This is based on us being able to get more distance then we are currently seeing from the USRP Radios.

- Radio Conditions: Here we will profile the radio with and without Batman-adv running to measure the RSS using a tektronix spectrum analyzer. We can get distance measurements to quantitatively measure the RSS level when we lose the radio connectivity.

- Reachability and Packet Loss: From here we will ping from one node to all the other nodes and measure how many packets are dropped. We can set a number of "n" pings and count how many packets were dropped.

- Delay: Here we will use a test with "n" pings, but this time will measure the response time and find an average/std deviation to determine how slow the network is.

- Throughput: We will have to find a tool for properly measuring a throughput test. We could set one node up as a gateway and use a traditional internet speed test but I belive that would be creating unecessary overhead.

- Route Changes and Convergence: The paper is a little sparse on the description of how they benchmarked this. It looks like we would turn a node off and view how the network reacts, possibly one in the center.
- Frequency Based changes: I think it would be good to run all of these tests at several frequencies and examine the changes. This will obviously be dependent on the antenna used so we may need to either use a small band, mention this limiting factor, or switch antennas. I believe our antennas are also rated at 5 GHz but would have to check.
- Joe mentioned Using Alfred to make many of these graphs and I believe it would help strengthen the paper and provide useful visual aids.
- Link Decays: Possibly another way to organize the information and run a test would be to link more and more nodes and measure how the network degrades as more hops are added. We could measure up to 4 hops right now, and hopefully 7 once we recieve the next 3 radios. We could then test this at 3-4 frequency levels and view the results.
- Frequency Hopping: We still do not have an AI based frequency hopping algorithm in place. I'm not confident in my ability to have one in place by March 1st but can do my best. It may be better to write a first draft of the paper not involving frequency hopping and then re-evaluate closer to the deadline. We can then hope to have this in place for the next two papers

56 2-8-16

Still havent got to the testing phase. So much to do,so little time before the paper deadline. Anyway, finished the webhook stuff. Tried to see if we could use two channels on the B210 as part of the network, but the initial test was not promising. It said "node alive" for both nodes, but was filled with "D"'s which usually means theres errors in the stream and I wasn completely unable to ping back and forth.

57 2-10-16

Met with Brad yesterday to discuss everything in depth. I created a new shell script called raidseBatSignal.sh that should set up the batman-adv stuff automatically.

58 2-11-16

Meeting with Matlab today. Looks like Alfred is going to help us quickly develop the functionality we are looking for.

59 2-13-16

Still can't figure out how to configure Alfred. It looks like parts of it are built into batctl but we really need to figure out how to distribute the frequency information"

60 2-18-16

Alfred -c works, but will only run if the data was changed by someone other than the host. Essentially, the computer that updates Alfred will NOT have the command listed on Alfred -c run.

Additionally, the webinterface flowgraph is still running the older version. We need to update it to a broadcast flow graph. It is currently at a much older nonbroadcast flowgraph.

Furthermore, we need to create a better system for adjusting the MAC address on each node. The current system will be unusable once we want to work with more than 2 nodes and is annoying even then.

Tomorrow I need to go over how to set everything up with Joe, and possibly create a written testplan so that he can help with that the next week/this weekend.

START WRITING.

RESTRUCTURE Trello to be useable by others.

60.1 ESPEAK

Espeak is hilarious

61 2-20-16

After struggling for awhile trying to figure out what was going on it turned out that I did not actually have a functioning flowgraph until today. The problem was that though GNU Radio is happy to work in a thread, the GUI is not. I'm not sure why I didnt think of this before as Unity3D should have taught me that visuals and threads don't get along.

Anyway, now im going to keep working on adding the Alfred implementation. Hopefully tomorrow Brad will be in and I can work on the Fedora builds while he is helping to clean up the rest of this code. I'm still not against abandoning flask in favor of a MQ system which with the right MQ system may make for a more robust system. But, with the deadline approaching I'm not 100 percent sure I want to start porting to a new platform.

62 2-22-16

62.1 batctl source build

We are trying to upgrade batctl and will track the needed changes here:

- sudo apt-get install libnl-3-dev

Trying to test today. Still having trouble. We can see from nodes to their next hops but not beyond that.
Will continue to test and report back here as we learn more

63 2-23-16

Today we are going to continue testing. To begin, we are building batman-adv 2016.0 from sources. The file can be downloaded from batman's website and is installed by:

```
# sudo make

# sudo make install

# sudo depmod -a

# modprobe batman-adv
```

64 3-7-16

Helpful website for changing the hostnames of computerS:
`hostnames`http://askubuntu.com/questions/9540/how-do-i-change-the-computer-name

65 3-28-2016

Link To Tutorials

There is also a paper discussing the use of GNU Radio as a means of spectrum sensing. It is an IEEE paper titled "Experimental Spectrum Sensing Measurements using USRP Software Radio Platform and GNU-Radio." However, no code is provided, just psudocode/equations.

However, no code is provided, just psudocode/equations.

Another github to be aware of for spectrum sensing can be found here