Software Defined Radio

Ramsey Doany
Texas State University

Raise your hand if you have little/no background in communication

Stop me and ask questions, please!

Outline

- What is a Software Defined Radio?
- How is a Software Defined Radio Used?
- Common Hardware types/Examples
- How to pick an SDR
- HackRF One
- GNURadio
- Brief Review of Communication Theory
- Tutorials

What is a Software Defined Radio?

- SDR
- Wireless Communication System
- Hardware
  - RF Front End
  - Antenna
  - ADC/DAC
  - Connects to PC

- Software
  - Mixers
  - Modulators
  - Amplifiers
  - Comparators
  - Scopes
  - Etc.

How is an SDR Used?

- Hacking
  - Garage door opener
  - Vehicle Remote Spoofer
  - RFID Spoofing
  - Penetration Testing
- Research
  - RFID Interrogator
  - Cellular Communication SImulation
  - Packet Transmission/Reception
  - Analog Transmission/Reception

Common SDRs

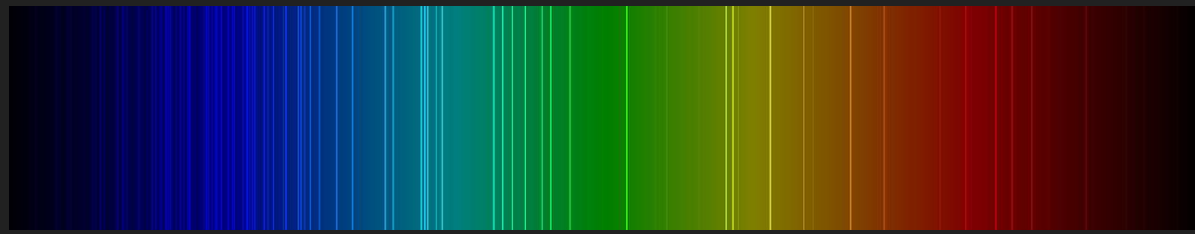
- USRP
  - National Instruments
  - Extremely High Performance
  - Several Thousand Dollars
- RTL-SDR
  - Hobbyist Grade
  - RX Only
  - ~$20
- LimeSDR
  - Research Grade
  - Several Hundred Dollars
- HackRF One
  - Simple Research Grade
  - Several Hundred Dollars

How To Pick an SDR

- Most Important Considerations
  - Application
  - Half/Full Duplex
  - Frequency Range
  - Built-in FPGA
  - Available Software Tools
  - Sample Rate
  - Range
  - Number of Antennas
  - Build your Own!

Considerations when using SDR

- Legality of Application
  - Don’t make a cell phone jammer
    - Up to $10k fine and 15 years prison
  - General Rules:
    - Only test on what you own
    - Be aware of your frequency range
- “Be a good RF spectrum neighbor”
  - Wifi
  - Cell Phone
  - Other Researchers



HackRF One

- $300
- Half Duplex
- 1 MHz to 6 Ghz Operating Freq
- Up to 20 Million Samples/Sec
- 8-bit quadrature samples
- SW configurable RX/TX gain and passband filter
- Open source

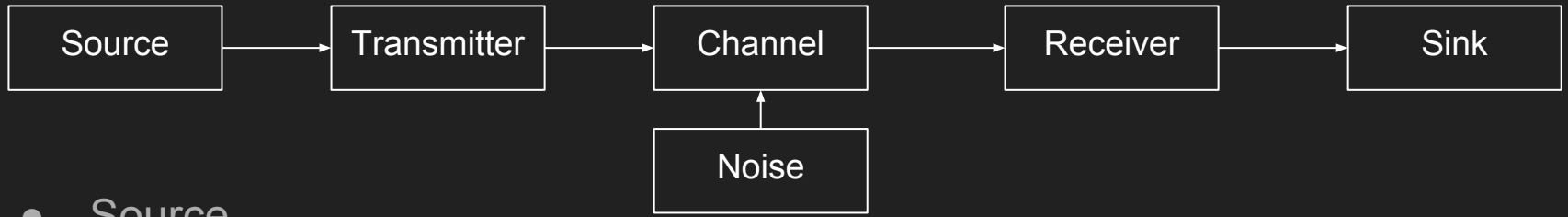
Software Tools

- LabView
  - National Instruments
  - Graphical Programming
  - Ideal when using multiple NI tools
  - Windows/Mac
  - Not all HW works with LV Mac
- GNURadio

GNURadio

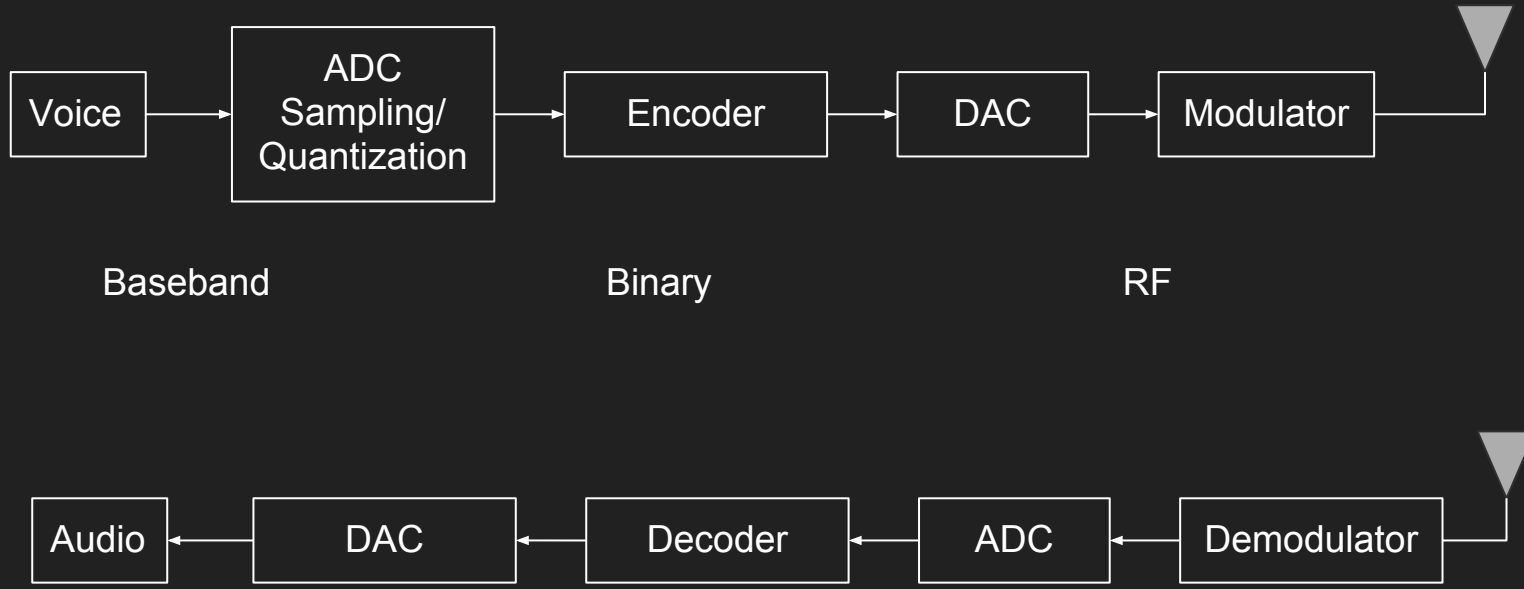
- Based On SoapySDR
  - Python
- Graphical Programming
- Mac and Linux (Windows not officially supported)
- wiki.GNURadio.org

A Brief Review of Communication Theory



- Source
  - Generation of information
- Transmitter
  - Encoding/Modulation
- Channel
- Receiver
- Decoding/Demodulation
- Sink
  - Receiver of Information

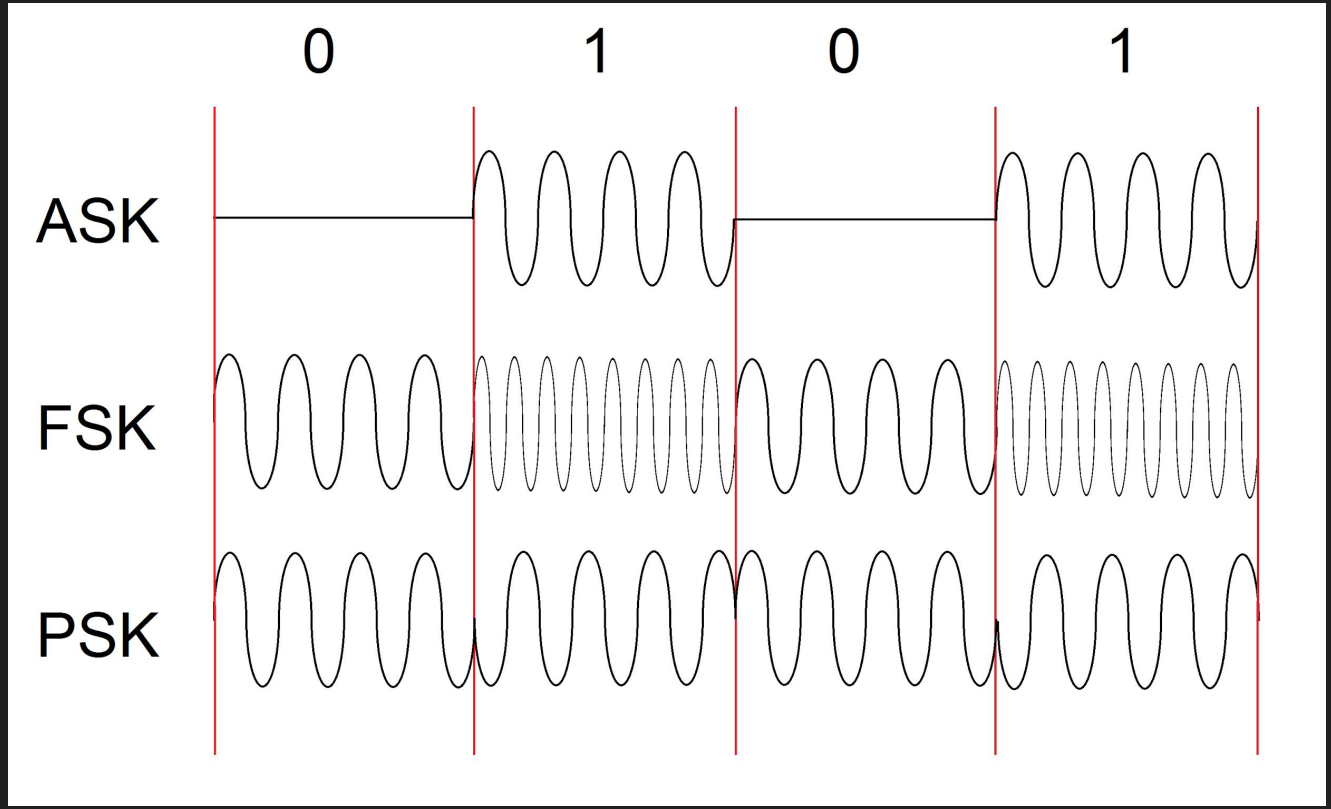
Speech Communication - Simple Block Diagram



Analog/Digital Modulation

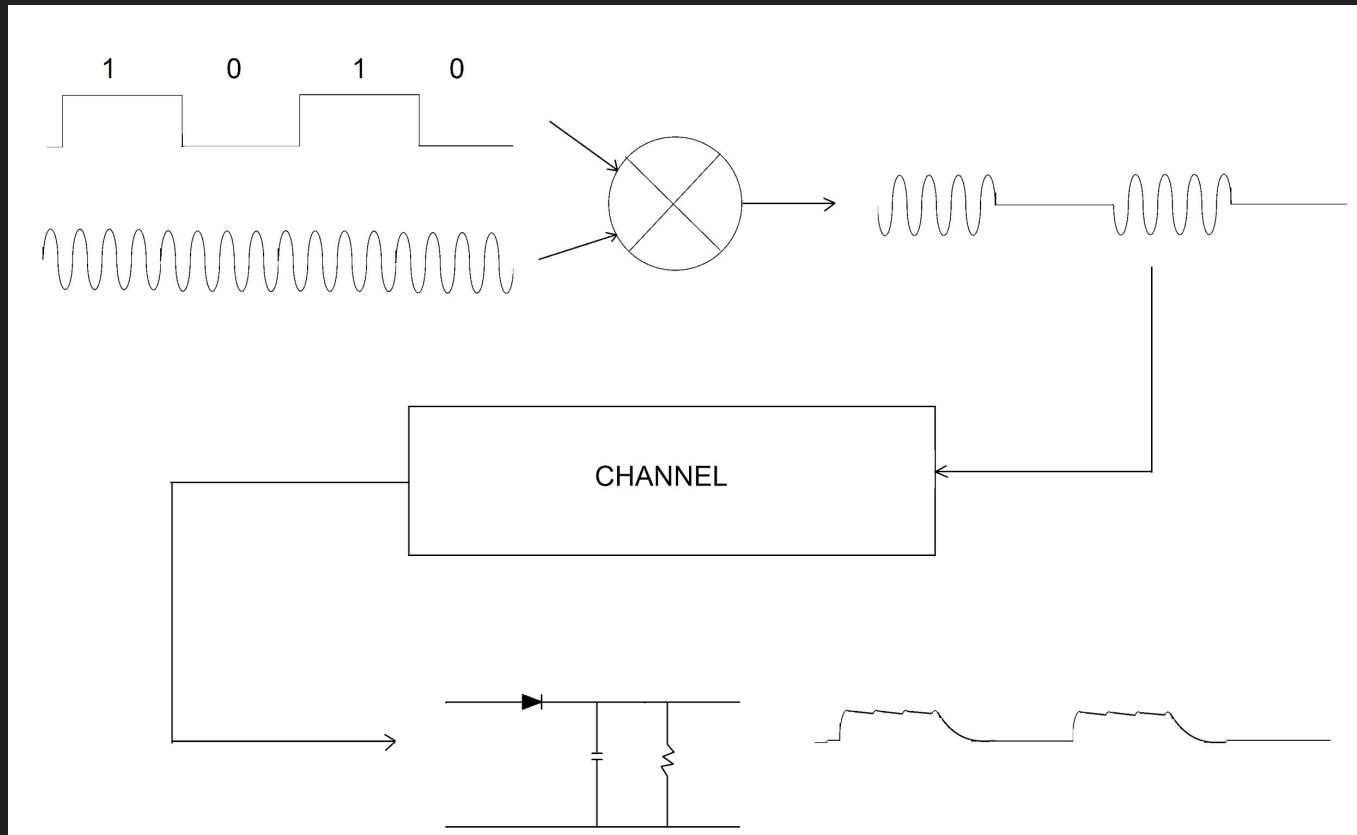
- Wireless Communication
- Analog Communication
- Digital Communication
  - Modulation - 3 possible variables to change
    - Amplitude Shift Keying (ASK)
    - Frequency Shift Keying (FSK)
    - Phase Shift Keying (PSK)

ASK/FSK/PSK



Modulation/Demodulation Example

ASK



Note On Sampling

- Nyquist Rate
  - Any signal can be recreated so long as the sampling frequency is at least twice the maximum frequency in the original signal
- Sampling and data playback frequencies must be consistent
- Aliasing
  - Sampling at a lower frequency creates copies of original signal at lower frequencies
  - Allows for sampling frequency to be lower than Nyquist Rate
  - Requires high performance filters
- Signal Sampling v Data Sampling
  - Many SDRs have a listed maximum sample rate significantly lower than its frequency range
    - Example: HackRF Sample Rate = 2MSPS Max Frequency: 6GHz
  - This is the data sampling rate
    - The SDR hardware converts RF signals to baseband signals, converts to digital, and communicates via USB

Tutorials

- Basics of GNURadio
  - Frequency Generation
  - FFT, Scope, Audio Sink
- Real Applications
  - Reception
    - FM Receiver
  - Reception and Transmission
    - Hack an RC Car