Direction Finding using Software-Defined Radio

Beth Flippo

TELEGRID Technologies, Inc.
Florham Park, NJ

Who is this girl?

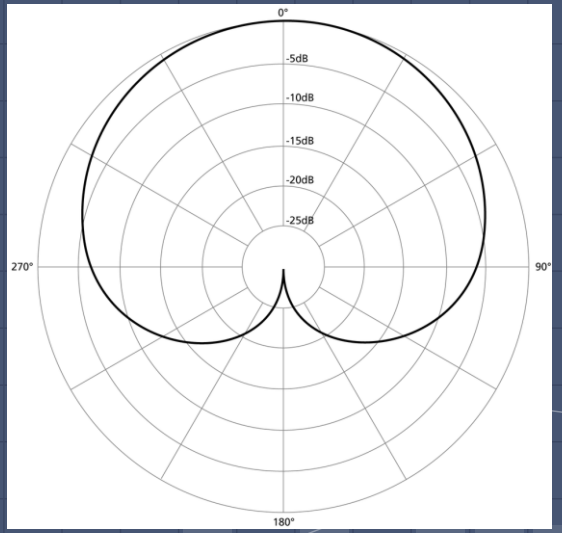
- Bachelor of Science in Computer Science from the Watson School of Engineering at SUNY Binghamton.
- VP Embedded Software Dev. at TELEGRID since 2006.
- Previously worked in IT at Goldman Sachs and Cantor Fitzgerald.
- Member of the Internet Engineering Task Force (IETF) Security Area Advisory Group (SAAG).
- Member of the West Essex Amateur Radio Club.
- Volunteer computer science teacher at a local high school.
- Tinkerer, hobbyist and lover of RF, LINUX and all things open source.

Beth Flippo
W2QNB

Direction Finding

What is Direction Finding?

- Direction finding refers to the measurement of the direction or bearing from which an RF signal was transmitted.
- The location can be stationary or mobile.
- Available since World War I
- WWII Battle of the Atlantic – British “Huff-Duff” System responsible for 24% of u-boats sunk.
- Identify variations in the received RF signal
  - Frequency
  - Time
  - Amplitude
  - Phase



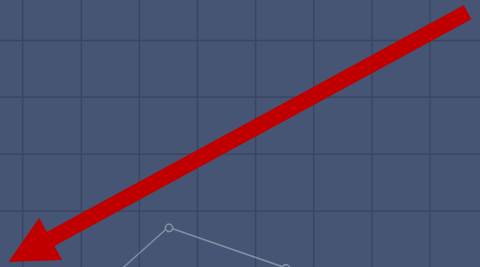
Active vs Passive DF

Active DF

- Signals are transmitted in order to identify location.
  - Radar measures the time between the transmission of a wave and the return of its reflection in order to determine the distance to the target

Passive DF

- Receive and analyze signals from external emitters.
- By not transmitting it allows users to obtain information without revealing themselves.



Our focus for today

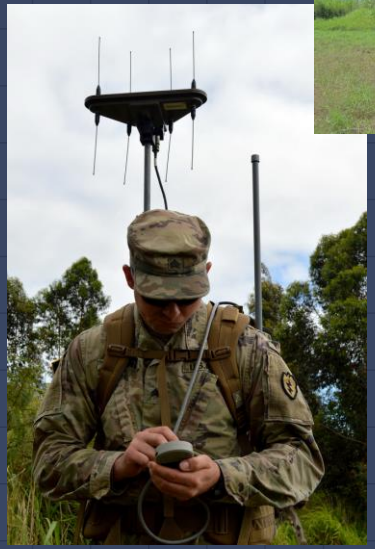
Why perform DF?

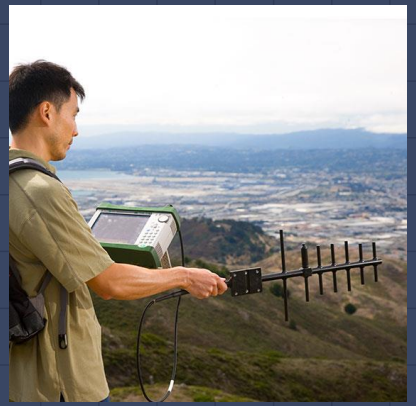
Portable 4G lte 3G + GPS + Wifi Signal Blocker Jammer
$228.60

- Intentional transmissions
  - Broadcasts
  - Radar
  - Jammers
- Unintentional transmission
  - Spurious Emissions
  - Stuck Mic

Who does direction finding?

- Military
  - Signal Intelligence
  - Electronic Warfare
  - Enemy Location Identification
- Law Enforcement
  - Vehicle Tracking
- Government
  - Emergency & Rescue
  - FCC Spectrum Enforcement
- Amateur Radio
  - Fox hunting

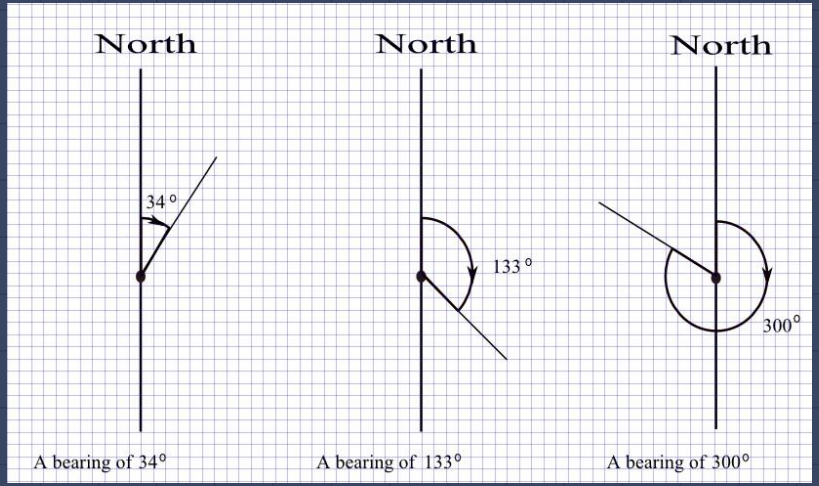




What is a bearing?

- Direction-finding systems generate a bearing (azimuth) that point in the direction of a signal.
- Measured in degrees, relative to our current position.
- Multiple bearings taken from different locations can be used for signal direction accuracy.
- Accuracy is primarily a function of the methodology used to calculate the bearings.
- Need to know the location the bearing was taken.

A bearing is defined as "a positive angle from 0 to 360 measured clockwise with respect to the north."

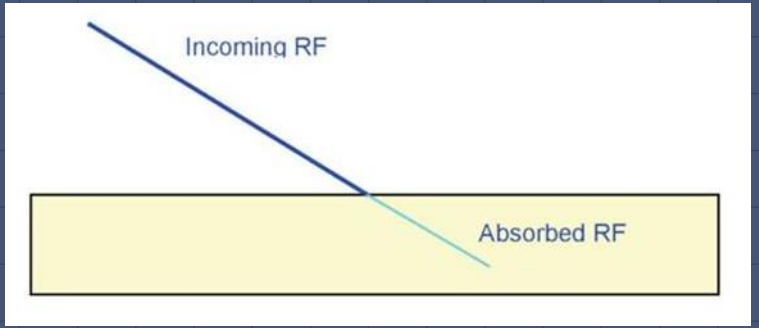


RF Propagation Issues

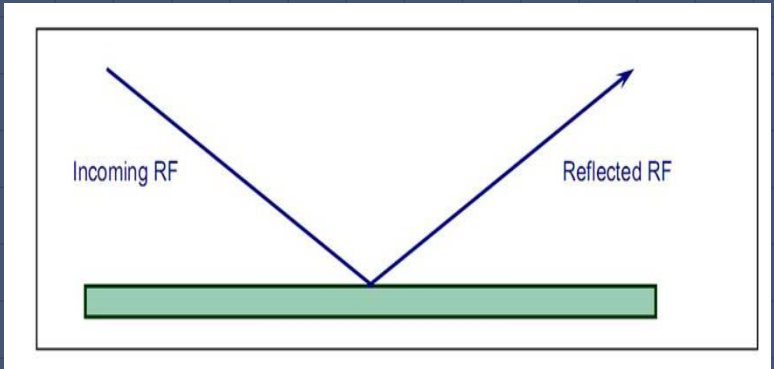
2

Attenuation/Absorption

- The absorption of RF signals by intermediary objects.
- The rate of absorption depends on
  - Frequency of the signal
  - Object composition
    - Low attenuation
      - Wood, plastic, glass
    - Medium attenuation
      - Bricks, liquids, organic material
    - High attenuation
      - Soil



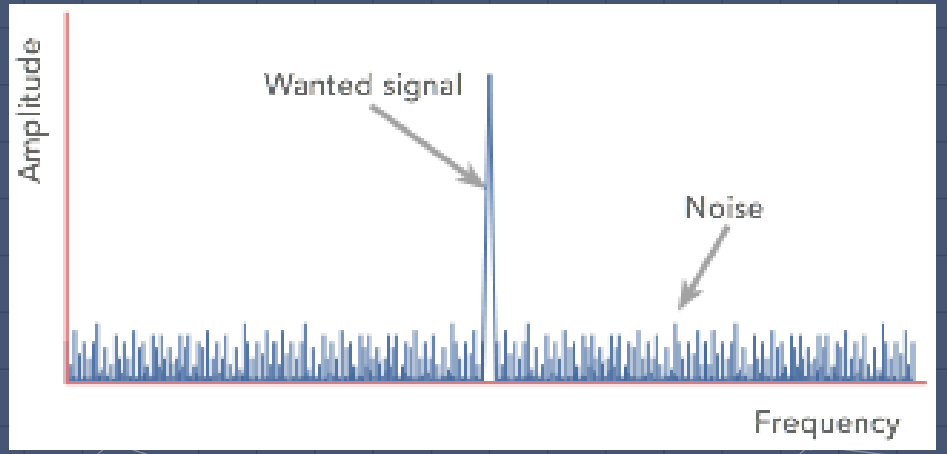
Reflections



- RF signals are reflected by intermediary objects such as tinted windows, concrete and metal.
- Signals may appear to be coming from the point of reflection rather than the actual transmission source.

Noise

- The “noise floor” is the level of ambient noise at a given location.
- High noise levels mask the RF signal making it unable to detect and therefore unable to generate bearings.
- Constant or intermittent noise may be mistaken for the RF signal.



What is Multipath?

- Multipath is defined as simultaneously receiving a signal from different directions
- Multiple reflection points in urban area cause a high multipath environment
- Frequency is a factor

Multipath is the single biggest issue in direction finding!!

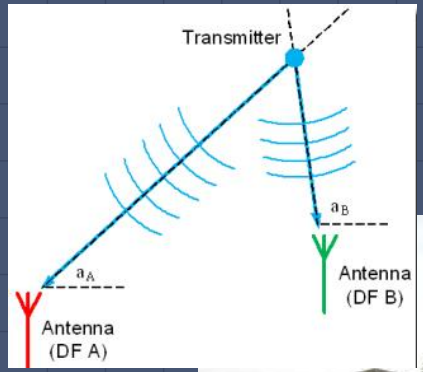
DF Methodologies

3

There is no “right way” to perform DF

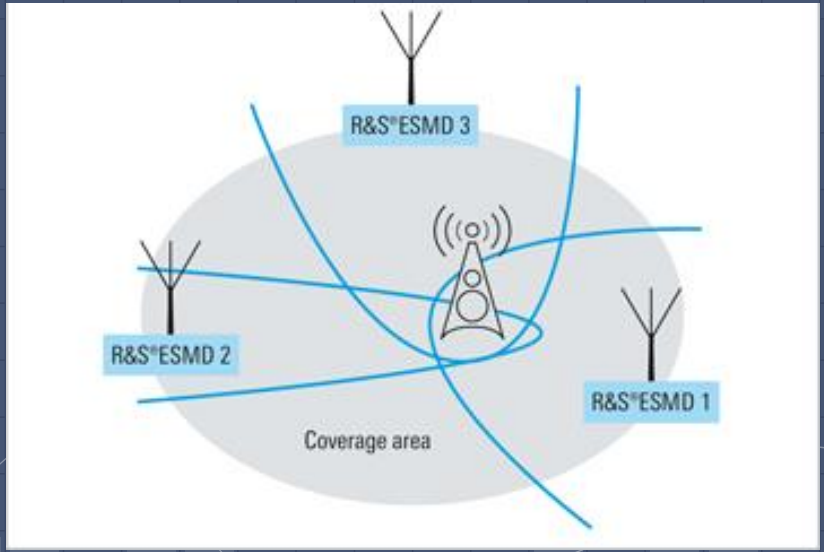
Manual Direction Finding

- Manual direction finding involves the use of a receiver and hand-held directional antenna like a yagi
- Rotate the antenna until maximum signal strength is determined.
- Large number of bearings from different locations to perform triangulation.
- Can be mobile with mounted antennas on vehicles.



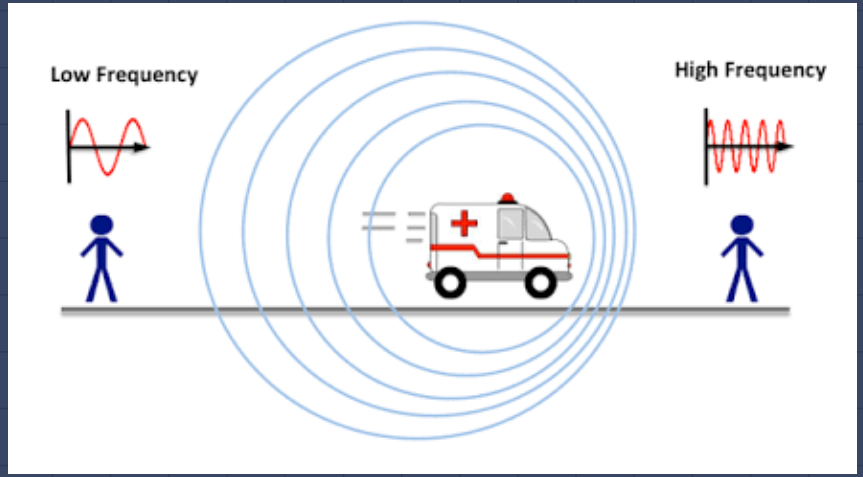
Time Difference of Arrival (TDOA)

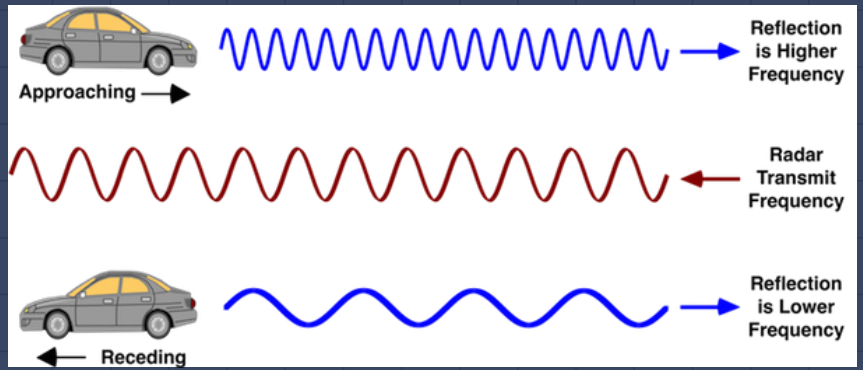
- Time of arrival of an RF signal at physically separate receiving stations with precisely synchronized time references.
- The time differences can be represented as hyperbolae which cross at the location of the transmitter.
- Sensors are usually in fixed locations
- Requires a control computer and cannot be used standalone.
- Requires network, GPS and power.
- Good accuracy over large distances.
- Sensors can have lower accuracy due to having multiple units.



Doppler Effect

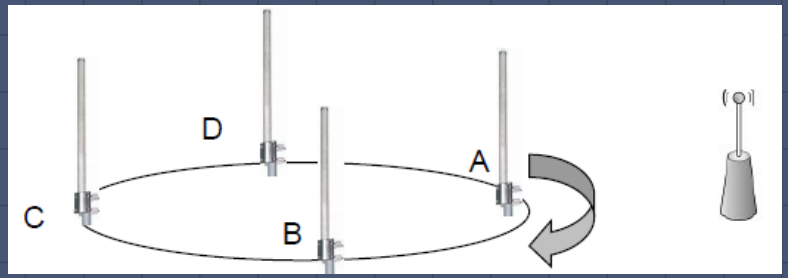
- Objects moving towards each other causes the observed frequency to increase and objects moving away from each other causes the frequency to decrease.
- The received frequency will shift upward as you approach the signal and downward as you move away.
- This shift can be detected and used to determine if we are moving in the right direction.
- For DF we move the receiver relative to the transmitter so that we can measure the Doppler shift.

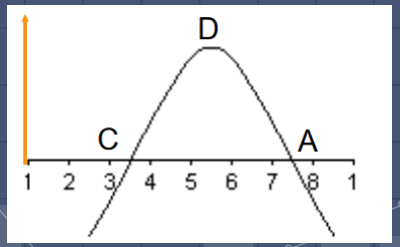




Doppler Shift

- A circular antenna array is rotated so the antennas will move closer and farther from the RF transmitter.
- Continuous measurement of the shift will produce a Doppler sine wave.
- The wave has the same frequency as the rotation of the antenna.
- The wave has 2 zero crossings at A and C because they are stationary to the transmitter.
- The second zero crossing (downwards slope) is the point closest to the transmitter





Pseudo-Doppler

- To capture the doppler shift the antenna would need to be rotated at unrealistic speeds.
- Pseudo-doppler simulates the rotation by electronically switching a set of fixed antennas.
- Each antenna generates a series of Doppler pulses and the system uses them to synthesize the Doppler sine wave.
- To produce sufficient shift the switching must be fast!

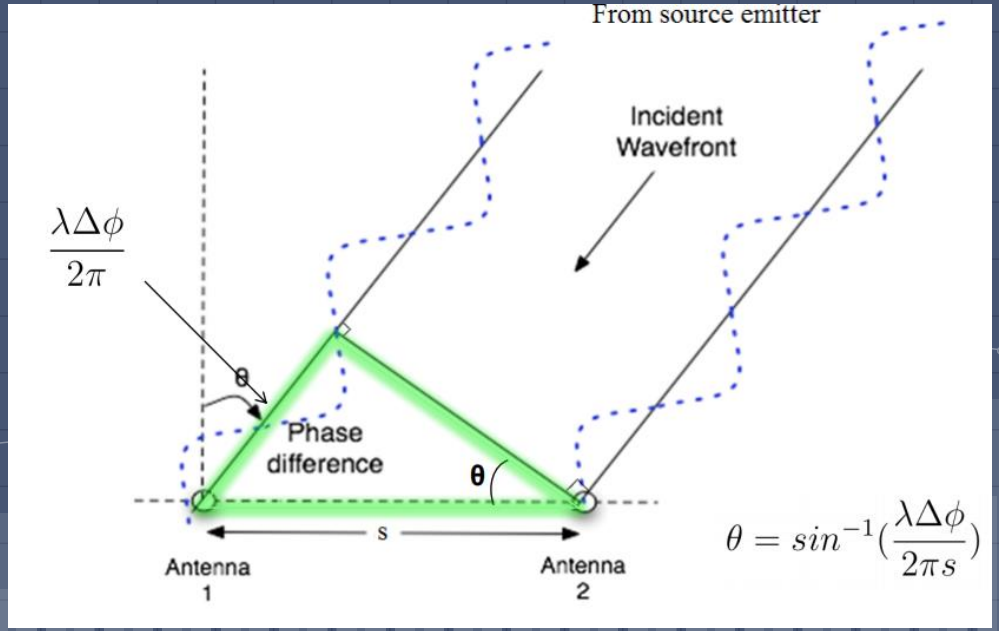
Watt-Watson

- Developed by Sir Robert Alexander Watson-Watt who also co-invented radar.
- Amplitude variation DF methodology.
- Uses Adcock (or crossed loop) antennas to compare the level of the signal received at each antenna. It then computes bearing based on the differences between them.

Phase Interferometry

- Relies on the time delay of the arrival of a signal between two or more antennas.
- Measures the difference in signal phase between antennas.
- Unlike the time difference the phase difference can be measured accurately over short distances.
- At least 3 antennas to resolve bi-directional ambiguity.

Interferometry *is a family of techniques in which waves, usually electromagnetic waves, are superimposed causing the phenomenon of interference in order to extract information.*



Current Direction-Finding Devices

- Mobile DF Platforms
- Large backpack style units
- Expensive
  - excess of $100,000 per unit
- Individual stand-alone units
- Not networked

Praemittias Systems
Wolfhound System

R&S®MP007
Portable Direction Finding System

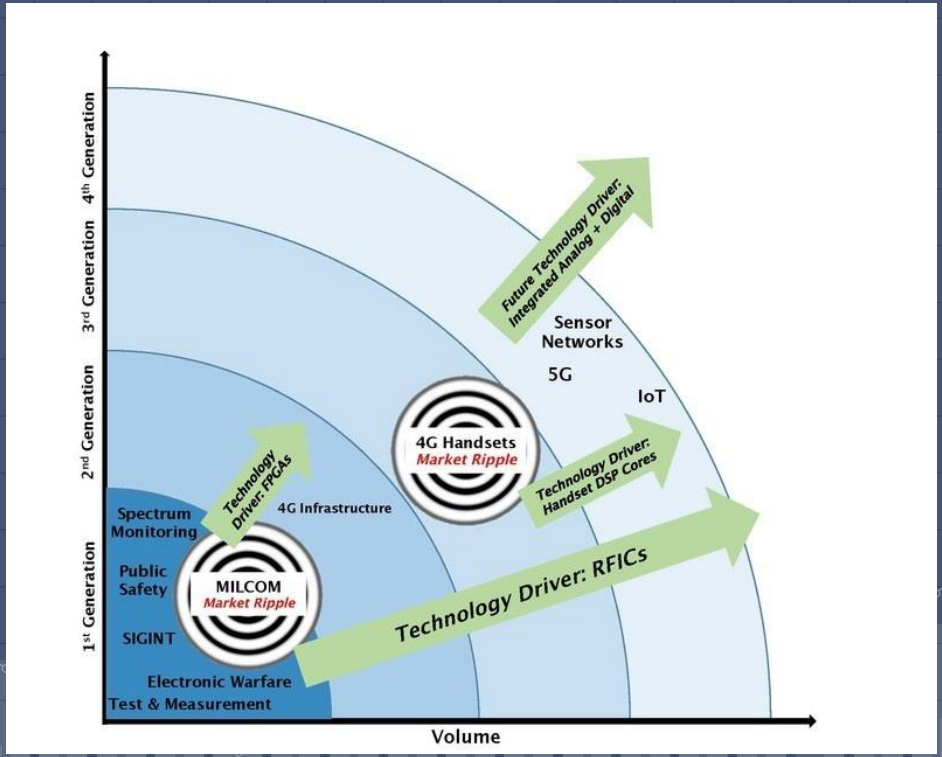
Software Defined Radio

4

Software Defined Radio (SDR)

- A radio where some or all of the radio's operating functions are implemented through software.
- Potentially tune to any frequency band and receive any modulation across a large frequency spectrum
- Allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware.

Evolution of SDR



- First Wave
  - Analog Devices RFIC and Xilinx DSP intensive FPGAs
  - Joint Tactical Radio System (JTRS) program funded the development and productization of SDR for military radios.
- Second Wave
  - The low-cost advancement of RFICs, FPGAs, and EDA tools
- Third wave
  - 4G LTE handsets moved consistently to SDR architectures enabled by low-power, high-performance DSP cores optimized for handsets
- Now de facto industry standard for radios

Cheap SDR

- RTL-SDR
  - Released in 2012
  - Small USB SDR dongle
  - DVB-T TV tuner dongles based on the RTL2832U chipset
  - 64 and 1700 MHz frequency range
  - Receive Only
  - Open Source
  - Approx. $20

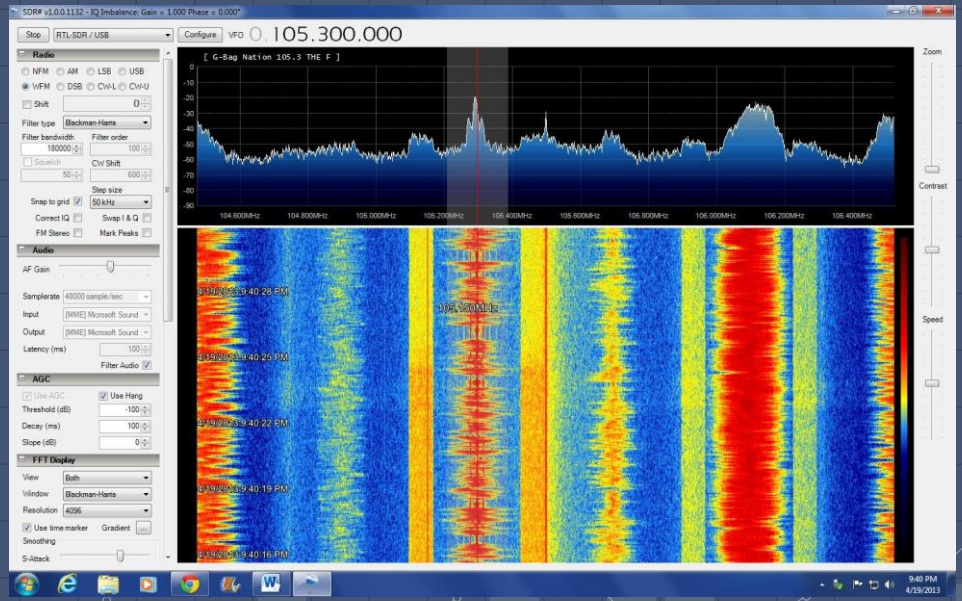
Cheap SDR

- SUP-2400
- In 2016 it was discovered a very cheap $5 DirecTV Upconverter which can be converted into a 2.4 GHz Downconverter can be used with the RTL-SDR.
  - 1 sup-2400 - UP to 4100 MHz (4.1 GHz)
    - [4100-2400=1700MHz]
  - 2 sup-2400's - UP to 6500 MHz (6.5 GHz)
  - 3 sup-2400's - UP to 8900 MHz (8.9 GHz)
  - 4 sup-2400's - UP to 10368 (10GHz)

HackRF One

- Released in 2014
- 10MHz to 6GHz frequency range!
- Developed by Michael Ossmann a who was given a development grant from DARPA
- Receive and Transmit (still need a license)
- Open Source
- Approx. $300

SDR#



- PC-Based Application for SDR
- Supports Multiple SDRs
- RF Scanner & Waterfall
- Heat-Mapping
- Plug-ins for multiple features
- Open Source

Benefits of SDR DF

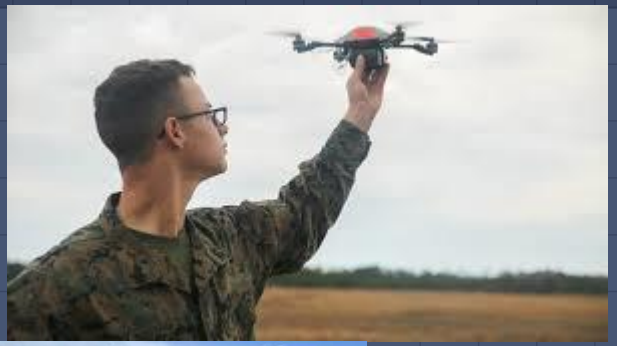
5

Cheap SDR and DF

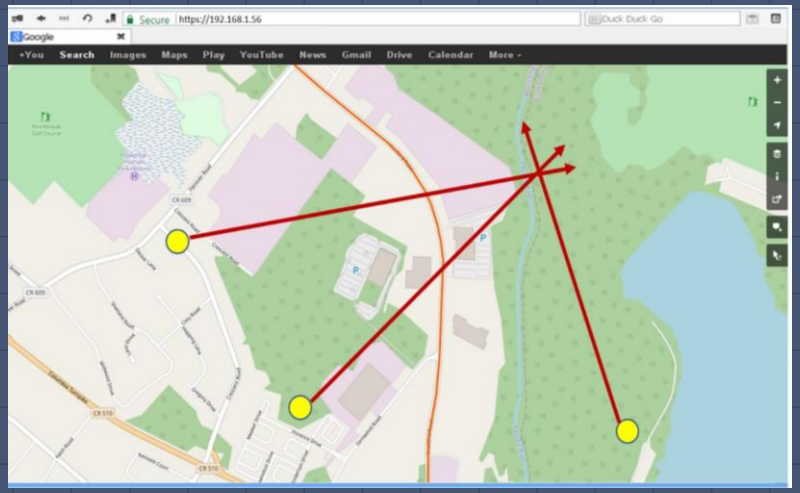
- Small Footprint
- Inexpensive
- Frequency Spectrum Sweep
- IOT Potential
  - Sensors
  - Camera/Video recording
- Mobility
- Digital Applications

Mobility

- Drones
- Robotics
- Smart Phones Accessory
- Autonomous Navigation
- Manned/Un-Manned (MUM-T)
- Freedom of movement
- Overcome current land navigation limitations
- Emergency response



Data Analytics



- Advanced Triangulation
  - Low-cost allows more units
- Combination of multiple DF Methodologies
- Multiple Frequency Analysis
  - Do not even need to know what frequency you are looking for!

IoT

- Remote Accessibility
- RF Spectrum Analysis
- Smart Phone Applications
- Cloud Data Storage
  - Save large amounts of historical data for robust applications.
- AI/machine learning algorithms

THAT'S IT!

Beth Flippo
VP Embedded Software Development
TELEGRID Technologies, Inc.
beth.flippo@telegrid.com
973.994.4440

Thank you to:
Rohde and Schwarz
Spench.net
RTL-SDR
HACKRF

More Information