R.I.C.E

February 1, 2019

Jacob Fletcher, Emil Mathew,
Matthew Sumpter

Overview -R.I.C.E(name in development)

- Radio frequency
- Interception
- Classification
- Exploitation

- Small operator carried system, that can work with long term missions and shorter DA operations.

Background – Why?

- Environments where current EW capabilities are limited
  - Dense Urban Environments
  - Subterranean Combat Environments
  - Operations where Near Peer A2/AD capabilities that limit the deployment air/ground assets
- Increasing global usage of IoT and RF main medium of wireless communication
  - 5.4 billion IoT
  - ~5 billion cellphones

Background – Why?

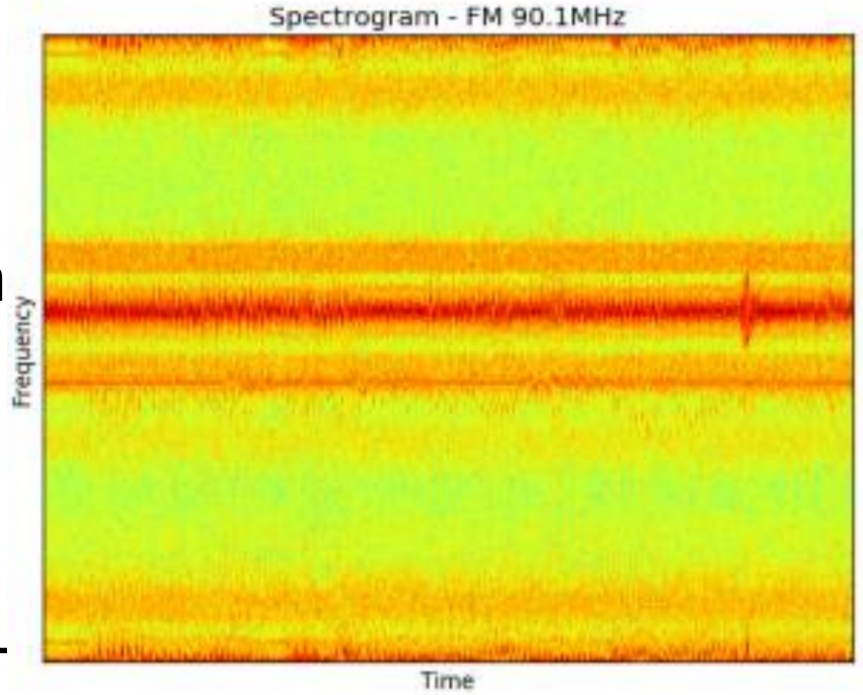
- In dense urban areas, signal traffic is high and difficult to identify
  - RF “Forensics”
    - What signals are present?
    - What signals are important?
    - What signals aren’t following the rules?
      - Security concern – may be intended to hack or “spoof” devices

Background – Why Machine Learning?

- RF sampling rates can exceed 200 GB/s
- Machine Learning:
  - Eliminates human error
  - Proper signals captured
  - ANd storage of interesting data

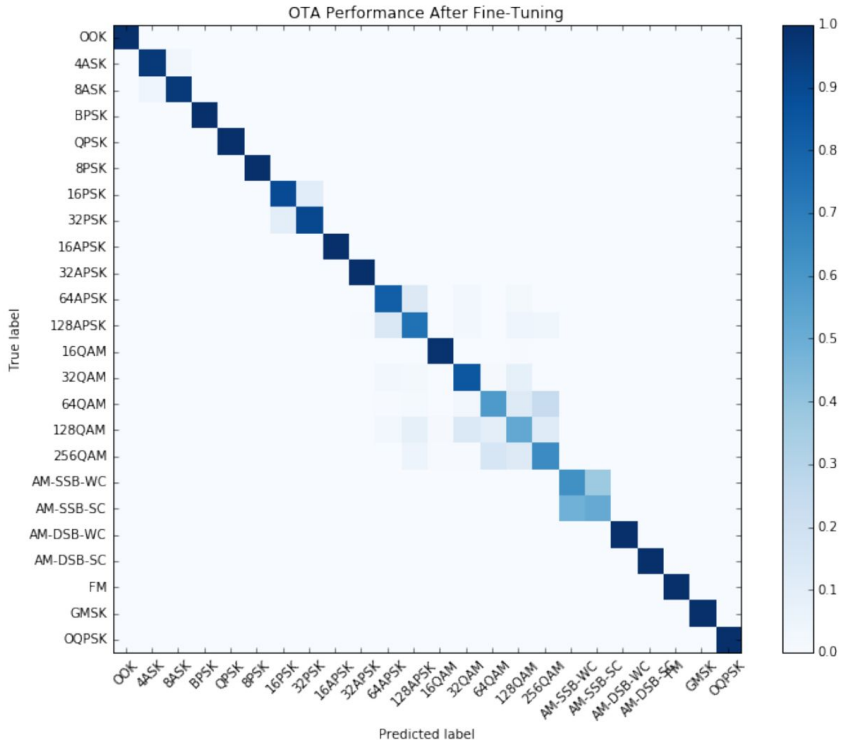
Background – Previous Work

- Spectrogram Approach
  - Discards phase info
  - Can be ~99% success at signal identification with expensive and heavy equipment
  - Pros:
    - Utilizes well-established tools for ML
    - Effective at signal identification
  - Cons:
    - Extra level of processing required to generate image



Background – In-phase/quadrature (IQ) Domain

- Uses DeepSig generated dataset and Convoluted Neural Network
- Pro: Facilitates real time decisions ~94/87% success (simulated/OTA)



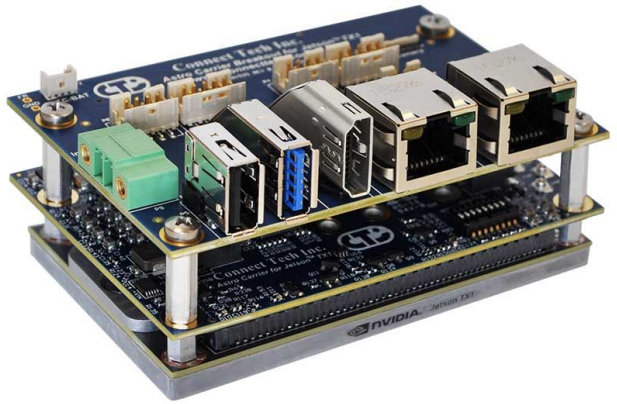
SOFWERX DEFENSEWERX

Background – Challenges

- Preprocessing and machine learning on data of this complexity not well explored in non-proprietary sources
- Practical application:
  - Classifying RF in real-time proven successful
  - Can it be made portable?

Tools for Approach – Hardware

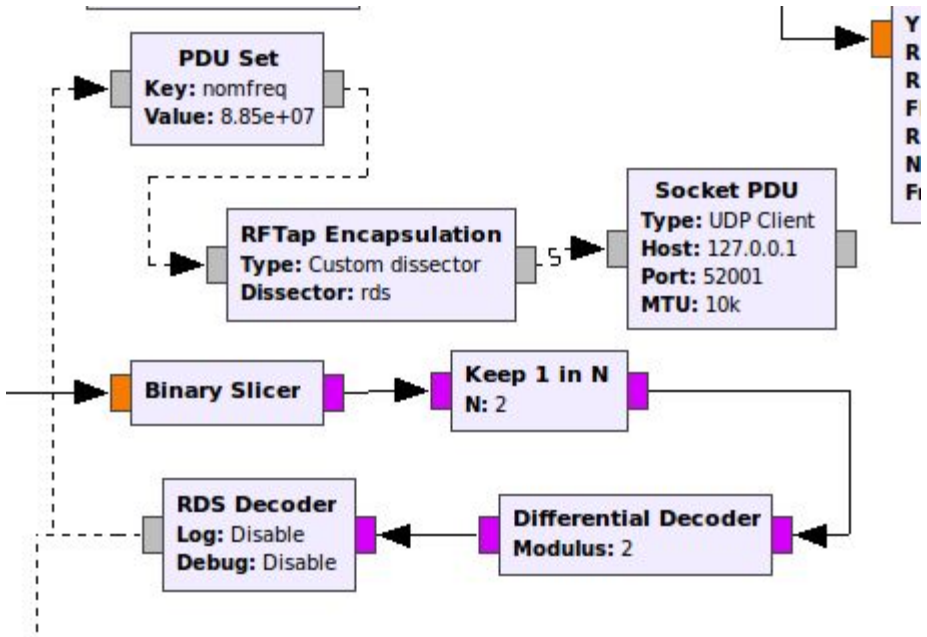
- Software-Defined Radio Devices
  - RTL-SDR
  - LimeSDR/Mini
- TX2
  - Portability allows for easy carry by operators
  - Capable of computational demands

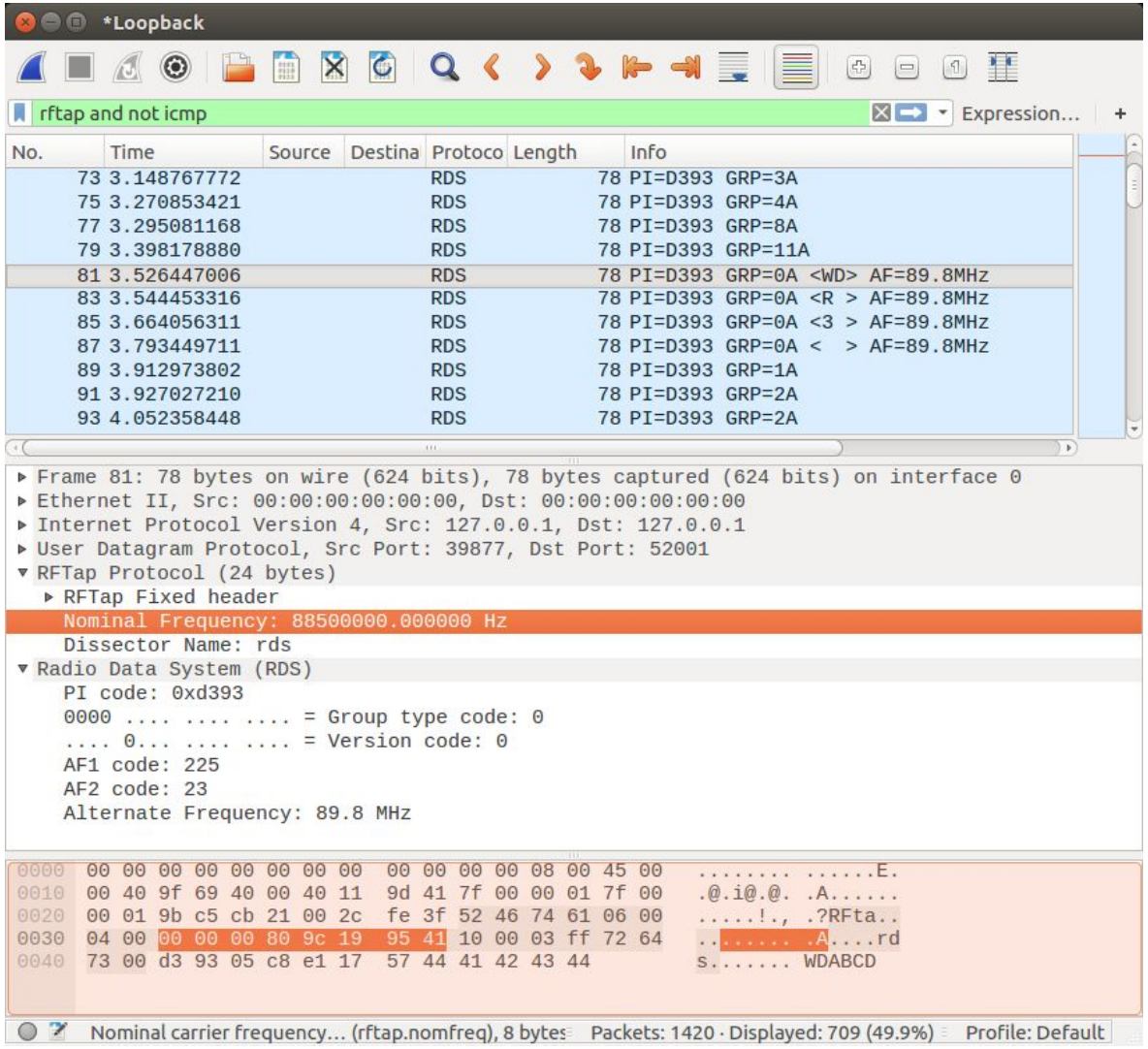


Tools For Approach – Software

- GNURadio
- RFTAP
- Wireshark

Current Interception Format





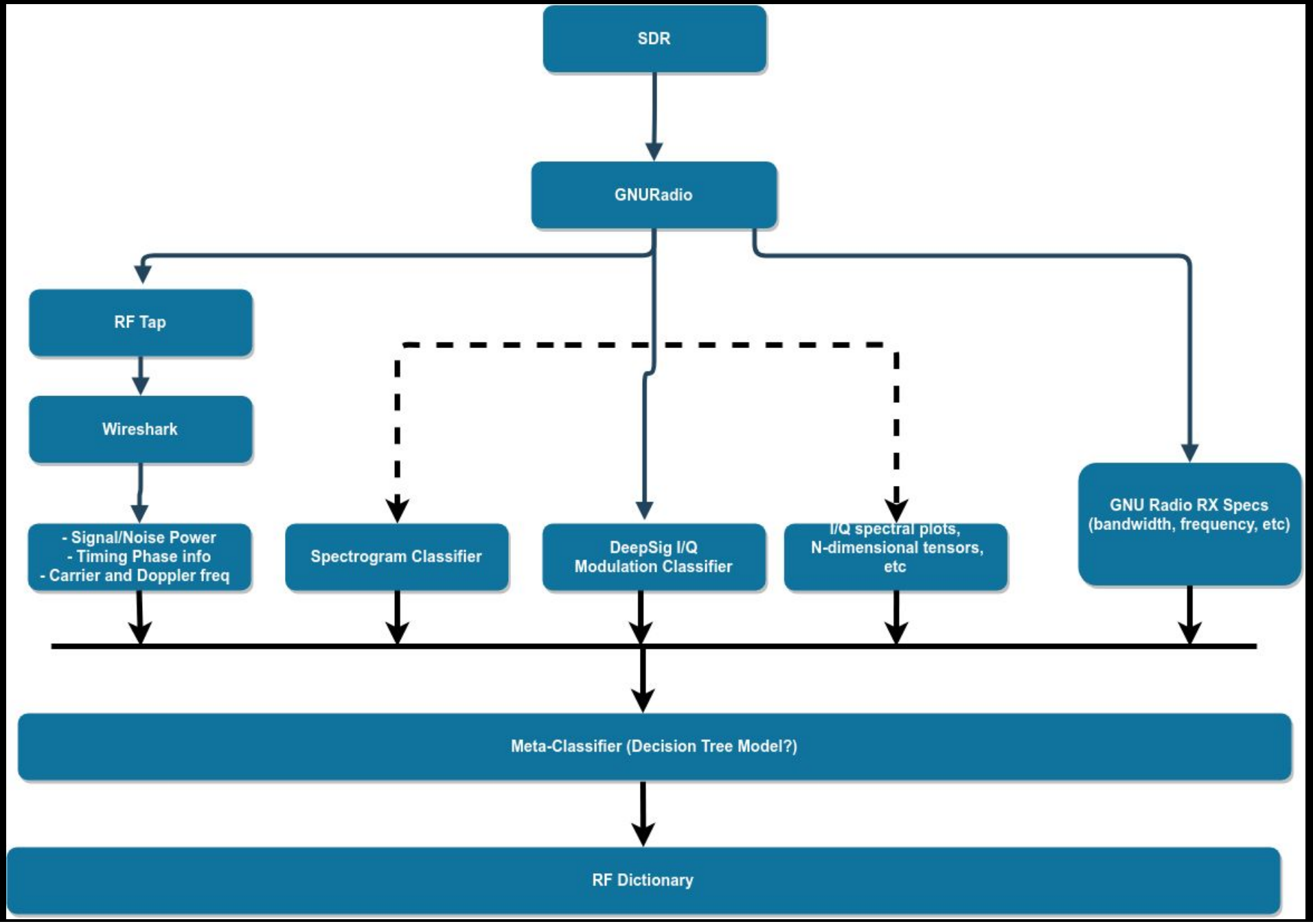
SOFWERX DEFENSEWERX

Generating Data – Processing RF signals

- GNU Radio config. provides initial insight
- GNU Radio Modules
  - RFTap
    - Allows wireshark to view RDS packet headers and look for metadata flags
  - Data “grooming”
    - Trim focus to specific bandwidth/frequency/modulation
    - Eliminate noise

Classification – Ensemble Classification

- I/Q currently best standard for real-time analysis
- Stacking
  - Weight predictions from various classifiers
  - Design meta-classifier that determines final classification from all garnered meta data


SDR
GNURadio
RF Tap
Wireshark
- Signal/Noise Power
- Timing Phase info
- Carrier and Doppler freq
Spectrogram Classifier
DeepSig I/Q
Modulation Classifier
I/Q spectral plots,
N-dimensional tensors,
etc
GNU Radio RX Specs
(bandwidth, frequency, etc)
Meta-Classifier (Decision Tree Model?)
RF Dictionary

Future Work – RF Dictionary

- There is still a need for an open, collected dataset
- Incoming signals can be quickly identified and assessed
- New signals can be incorporated
- SQLLite DB with metadata used to build reference library

Future Work

- Build multiple schemas for detection
  - Automate movement between schemas with python
- Explore other classification methods
- Need for transfer learning
  - Training is expensive
  - Classify real-time data, feed back into classifier training model
- Focus on UHF and VHF for interception and recording

Resources

https://www.darpa.mil/news-events/2017-08-11a
https://www.thinkmind.org/download.php?articleid=data_analytics_2015_8_30_60114
http://on-demand.gputechconf.com/gtc/2018/presentation/s8826-deep-learning-applications-for-radio-frequency-rf-data.pdf
https://arxiv.org/pdf/1712.04578.pdf
https://blog.kickview.com/deep-learning-meets-dsp-ofdm-signal-detection/