REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11/18/2020	Conference Briefing	

4. TITLE AND SUBTITLE
Software Defined Radio Discovery

5a. CONTRACT NUMBER
W15P7T-13-C-A802

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Curtis M Watson

5d. PROJECT NUMBER
0718D420SD

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-20-2934

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Department of Defense

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Software Defined Radio Working Group hosted by Army Research Lab

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		14	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

Software Defined Radio Discovery

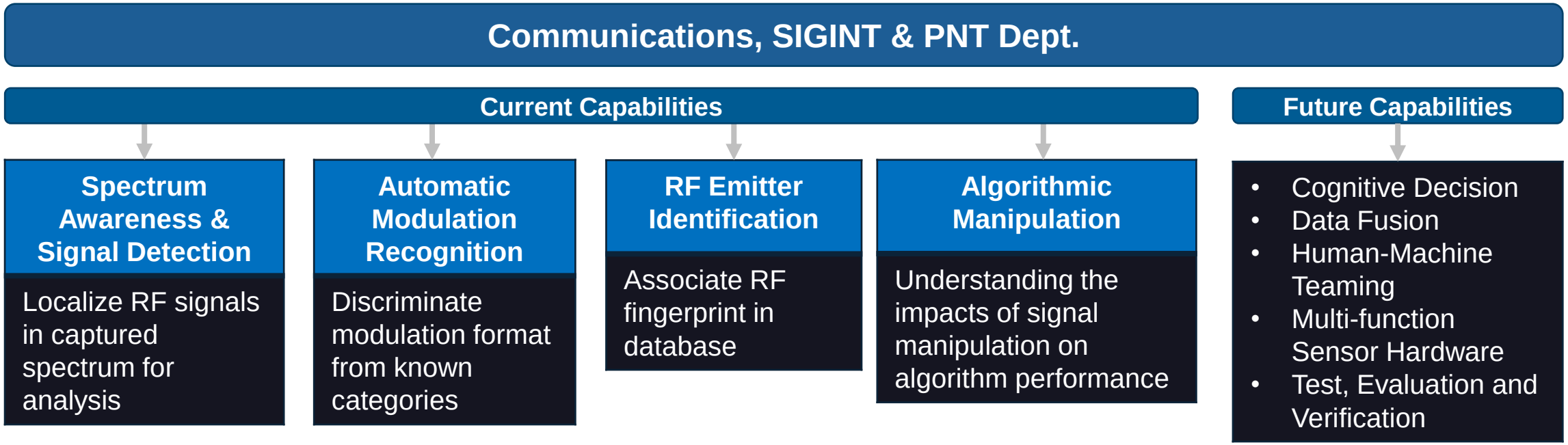
Curtis Watson, PhD (cmwatson@mitre.org)

18 November 2020

Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2934

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Signal Analysis Technologies



Software Defined Radio (SDR) Enables Rapid Capability Comm Systems & Can Challenge Identification

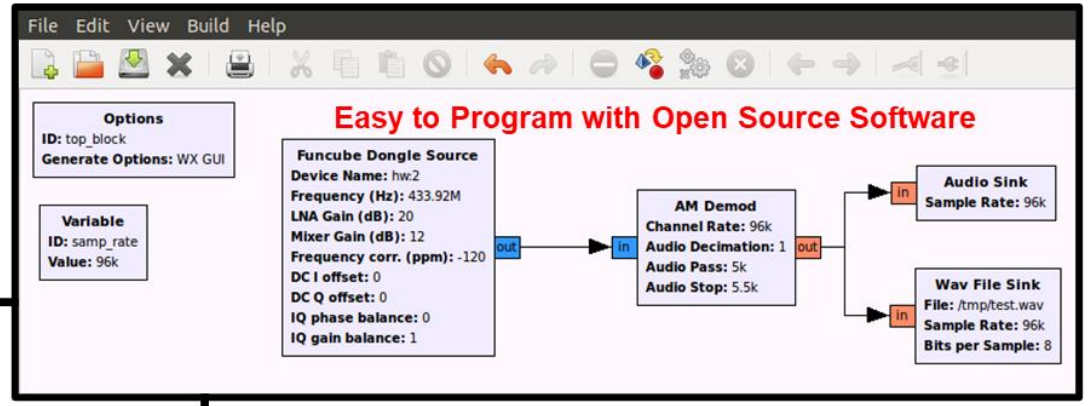
Conventional Approach to Develop Waveform Characterization is Time-Intensive

Discovery → Identification → Exploitation

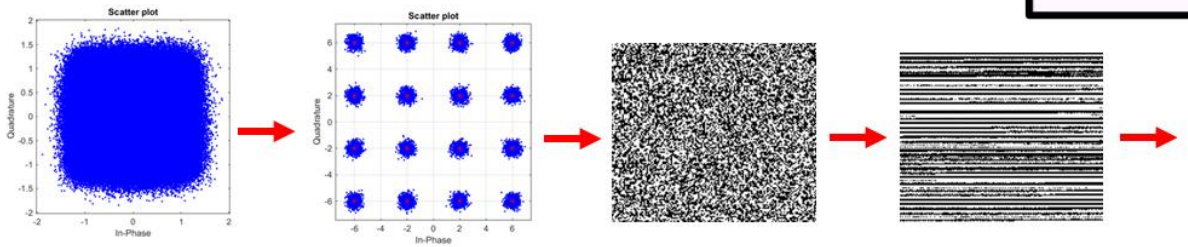
Conventional Characterization Lifecycle: months to years

Software Defined Radio (SDR) is enabling our adversaries with non-traditional communication systems

Current Waveform Characterization Development Cannot Achieve *Seconds to Minutes* Time-Scales

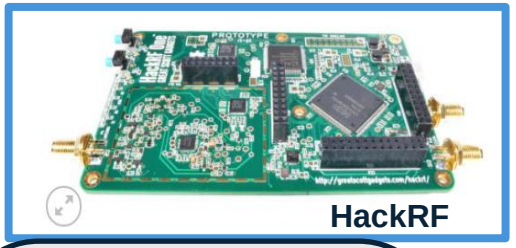


Example of Characterization Process



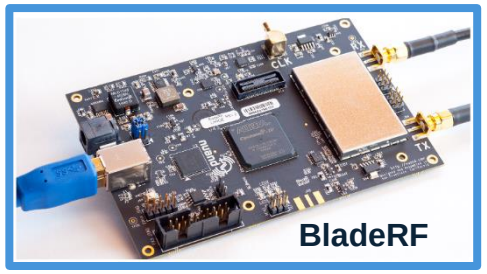
Desired Outcome: to create an automated system to rapidly identify and characterize RF waveforms

Low Cost Hardware & Open Source, Off-the-Shelf Waveform Protocols : Specific Types for our Effort



$299

$299

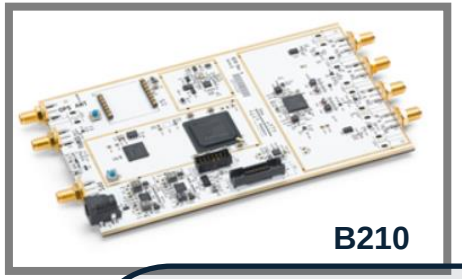


$420

python™

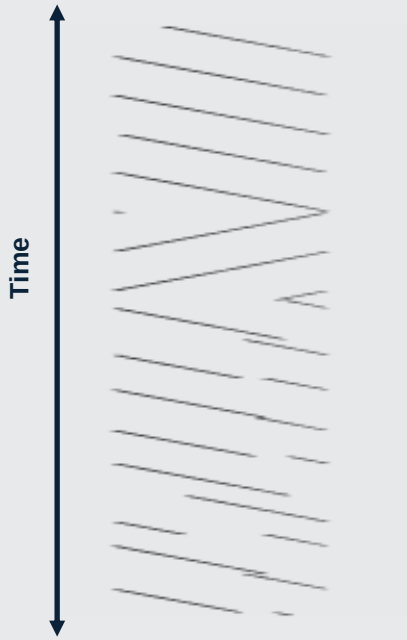
$2500

$1500



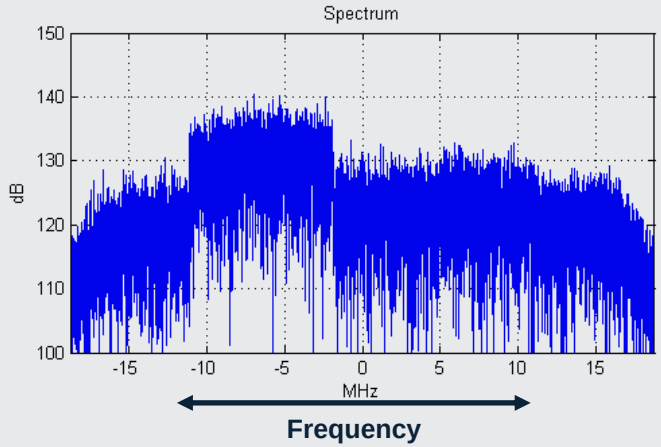
GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

LoRa

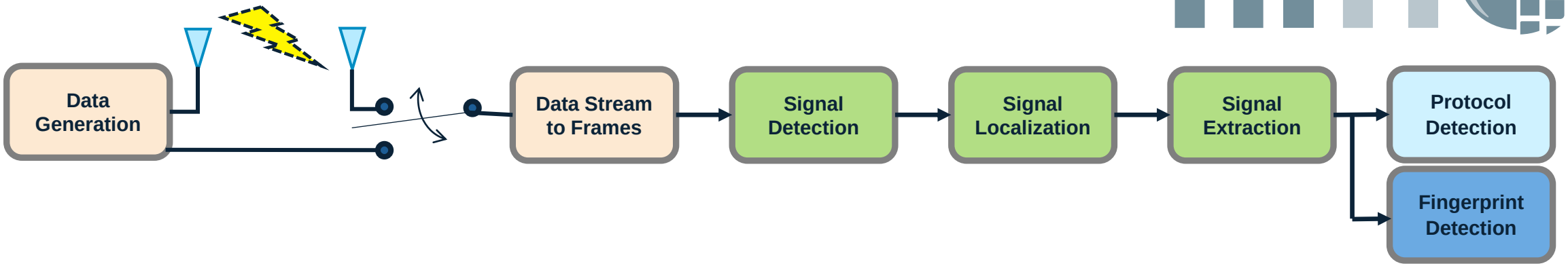


802.15.4

WiFi



SDR Emitter Identification Architecture



Data Generation creates the stimulus data which could be wirelessly transmitted or through wire and channel emulation

Data Stream to Frames is the conversion from streaming processing to block processing

Signal Detection finds activity in the data collection

Signal Localization isolates the signal detection in time and frequency

Note: signal detection and localization could occur within the same algorithm

Signal Extraction takes the localized signal from wider band signal and passband filters, moves to baseband and downsamples the data

Protocol Detection processes a set of algorithms to rapidly identify common waveform protocols

Currently implemented detection for: IEEE 802.15.4 & LoRa

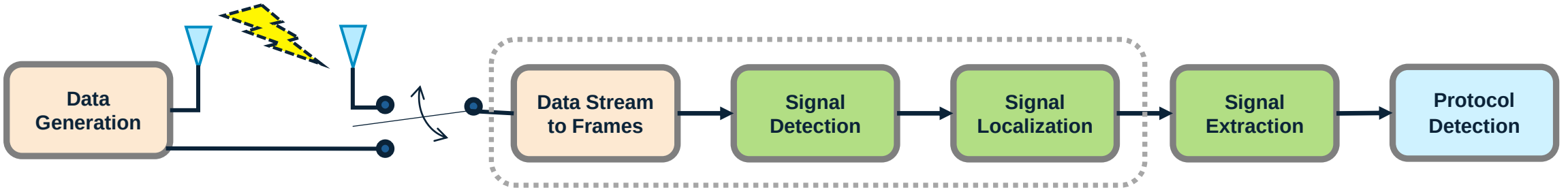
In development: IEEE 802.11

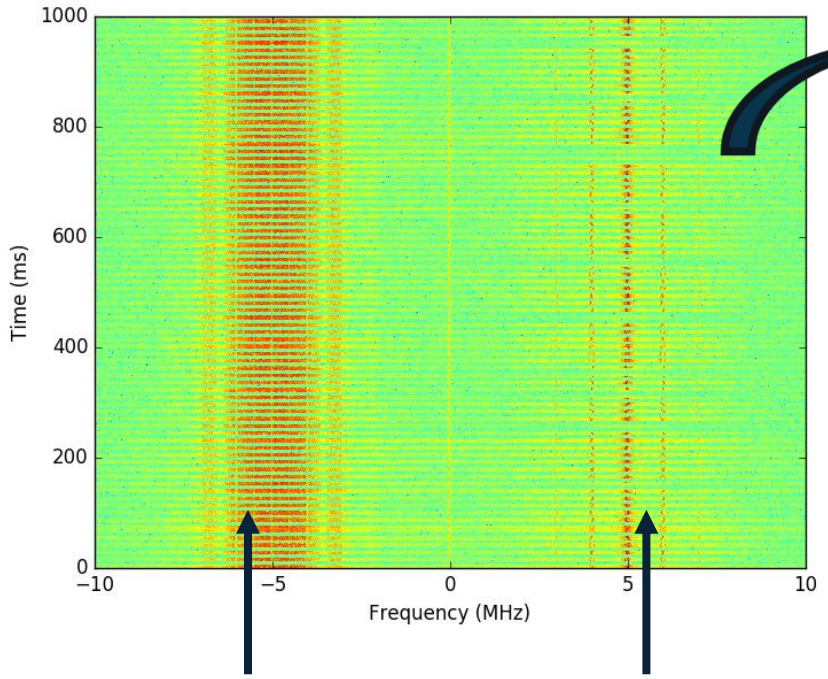
Future: Bluetooth

Fingerprint Detection rapidly identify characteristics unique to the emitter hardware.

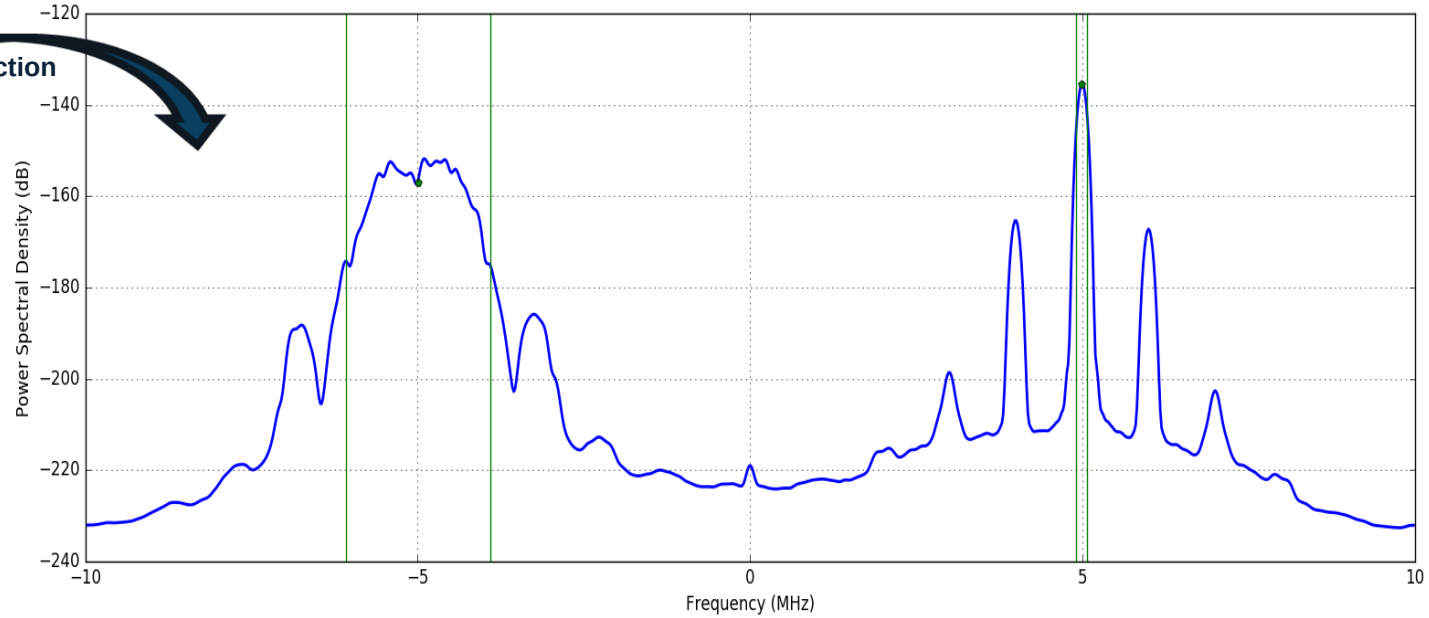
MITRE

Illustrative Example of Processing (1)





detection



IEEE 802.15.4
@ -5 MHz with
2 MHz BW

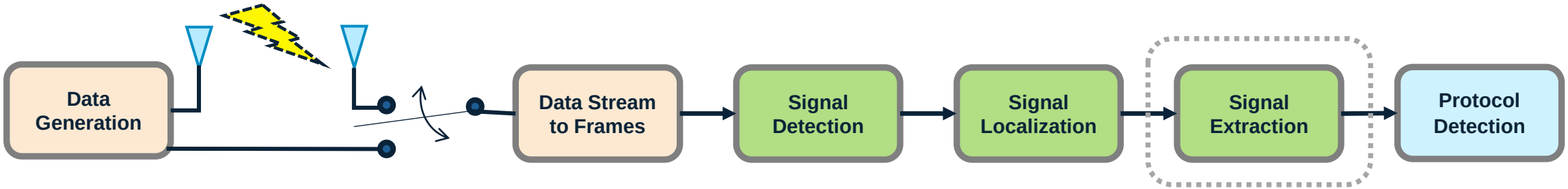
LoRa
@ +5 MHz with
125 kHz BW

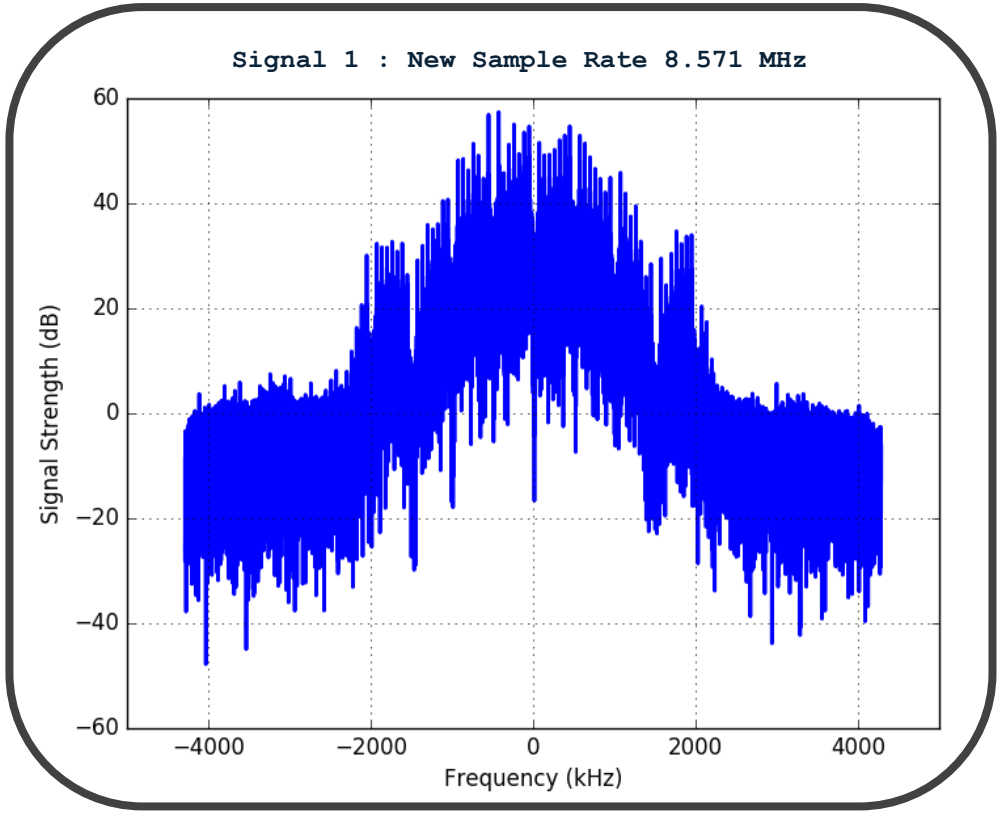
localization

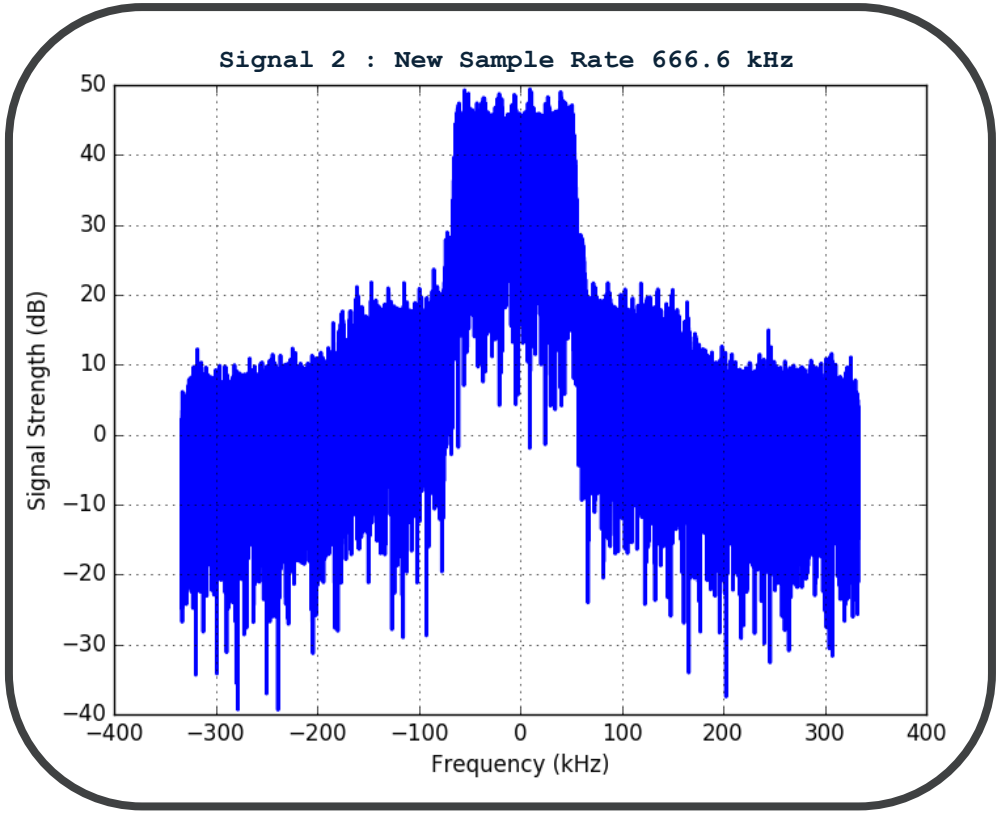
```
Signal 1
Center Frequency -4.990234 MHz
Bandwidth         2.168863 MHz
```

```
Signal 2
Center Frequency +4.990234 MHz
Bandwidth         161.8554 kHz
```

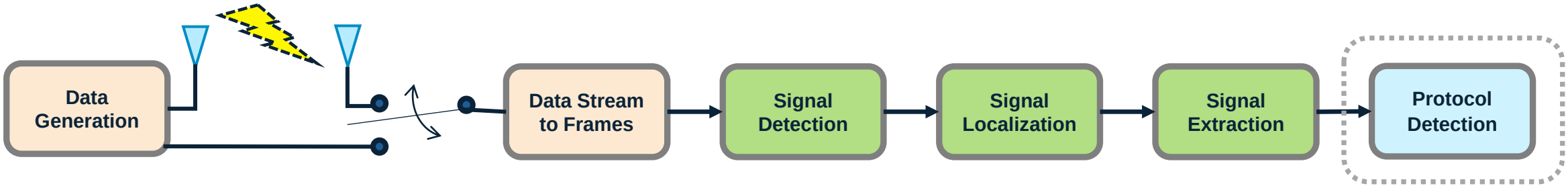
Illustrative Example of Processing (2)



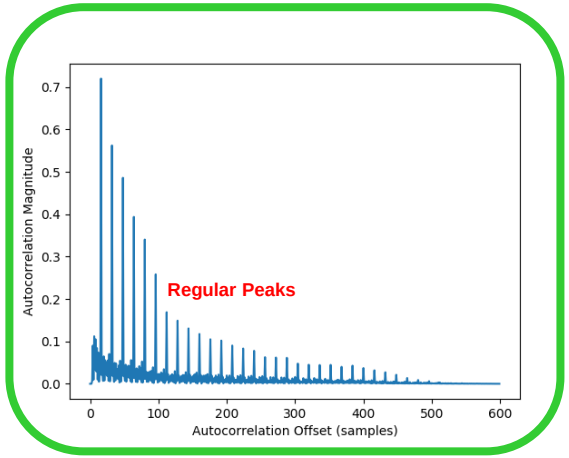




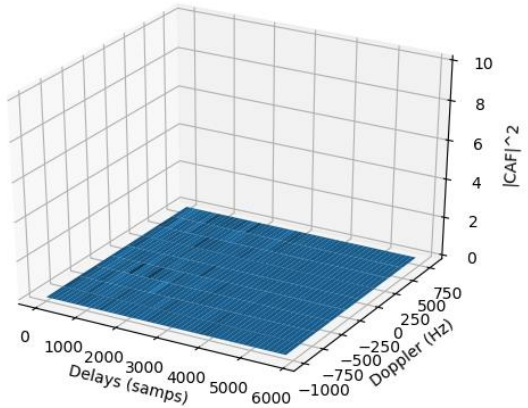
Illustrative Example of Processing (3)



Signal 1 is IEEE 802.15.4

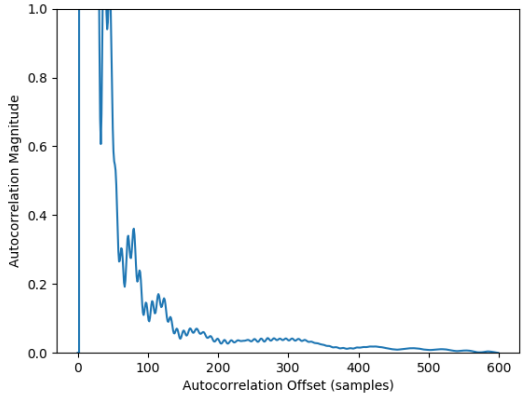


802.15.4 Test ✓

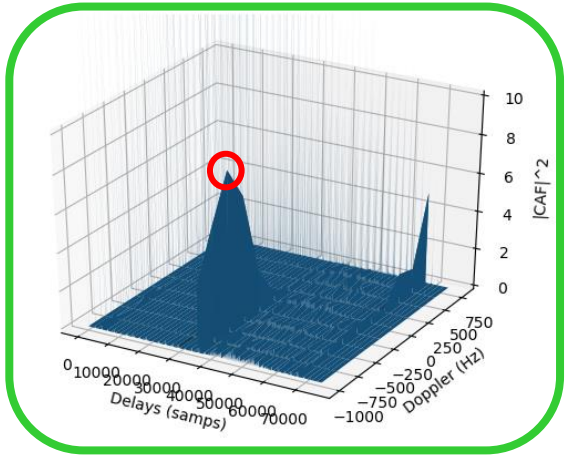


LoRa Test ✘

Signal 2 is LoRa

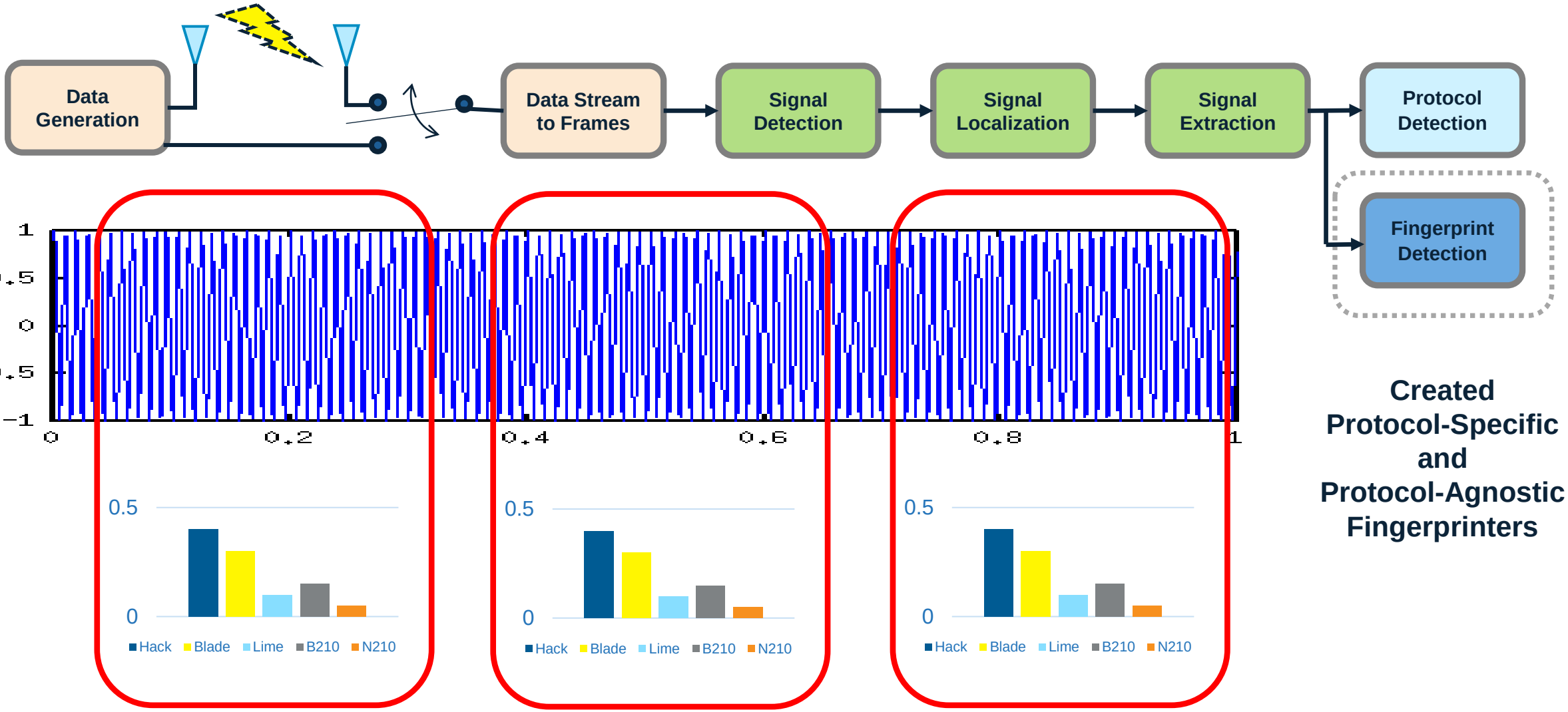


802.15.4 Test ✘



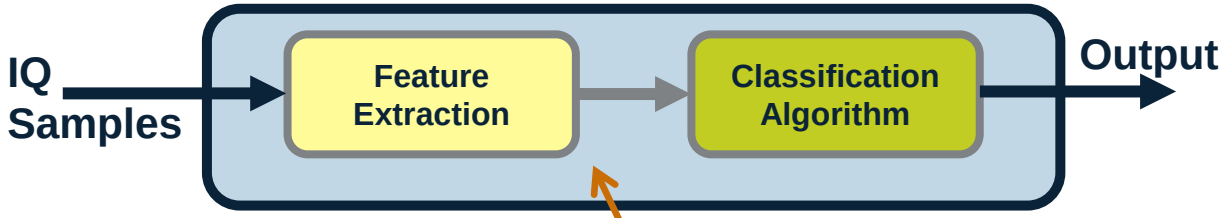
LoRa Test ✓

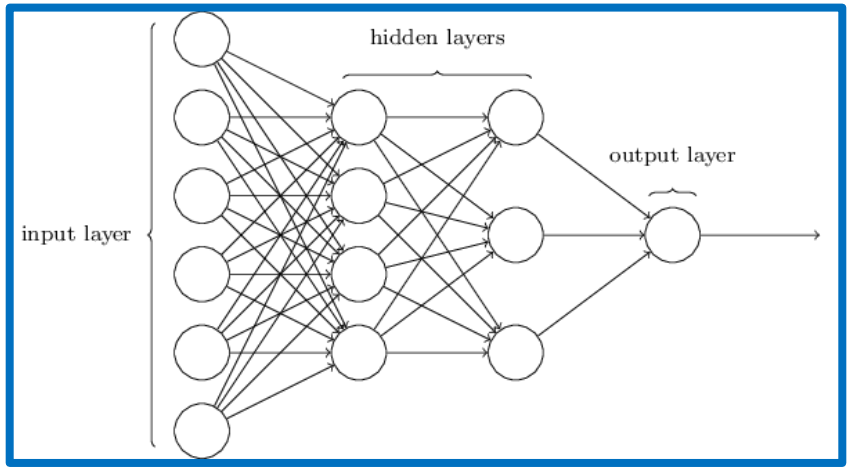
Illustrative Example of Processing (4)



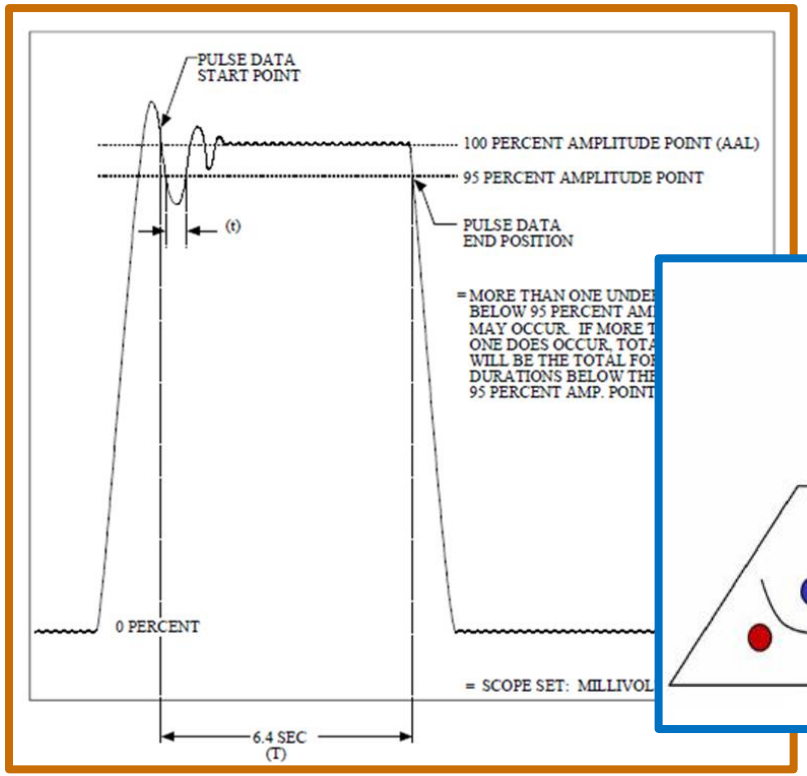
Created Protocol-Specific and Protocol-Agnostic Fingerprinters

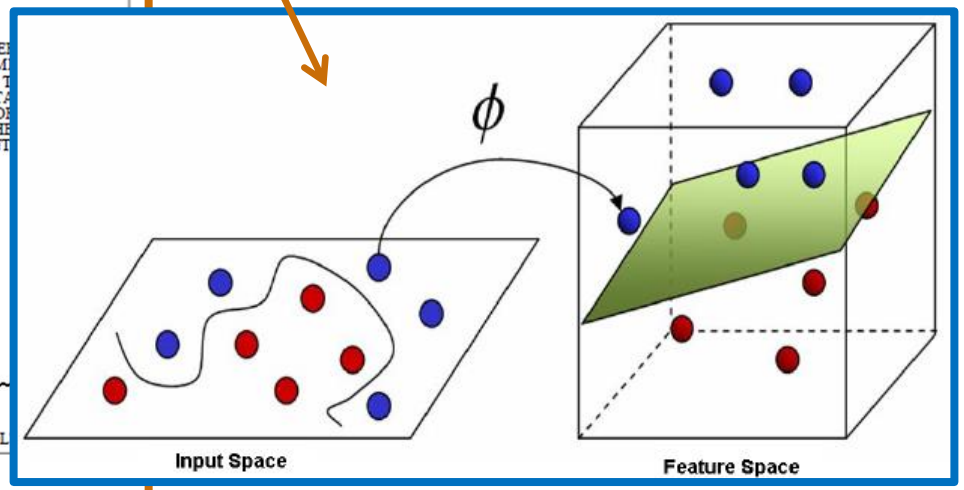
Machine Learning Approaches to Classification

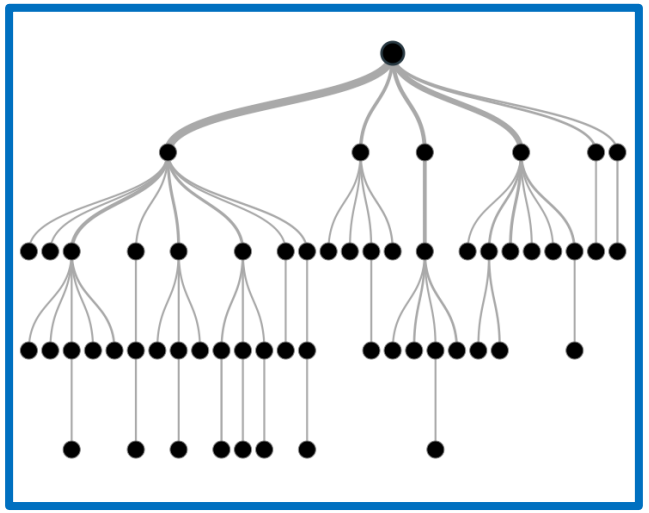




Human Designed Features Based on Domain Knowledge

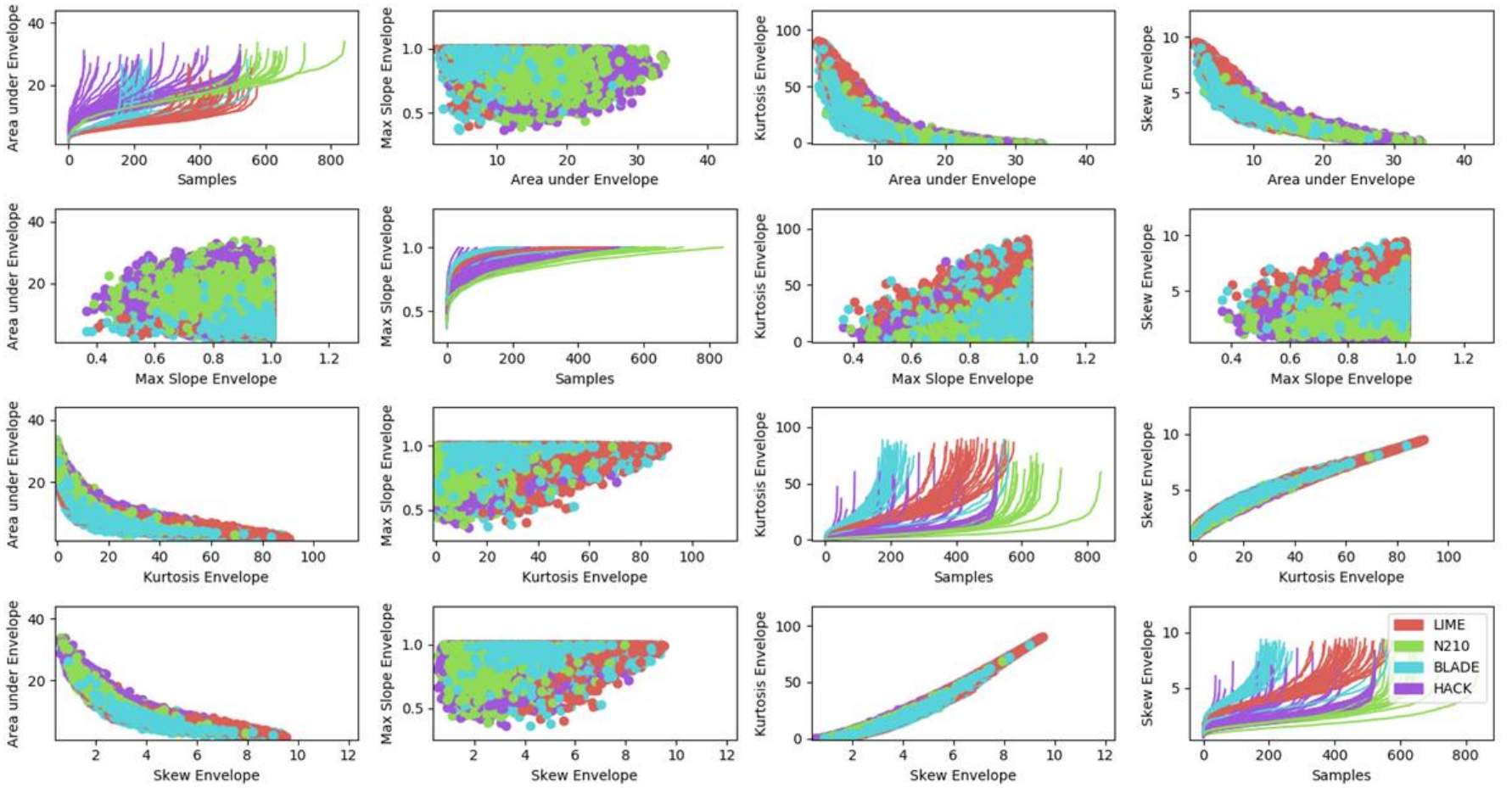






WiFi Fingerprinter using Energy Envelope Features

Energy Envelope is calculated from the spectrogram by finding the envelope of the signal and normalizing such that the maximum has a unit-magnitude



Random Forest Classification Confusion Matrix

	LIME	N210	BLADE	HACK
LIME	99.1%	0.3%	0.3%	0.3%
N210	0.5%	80.5%	0.1%	19.0%
BLADE	0.3%	0%	99.3%	0.2%
HACK	0%	7.6%	0%	92.4%

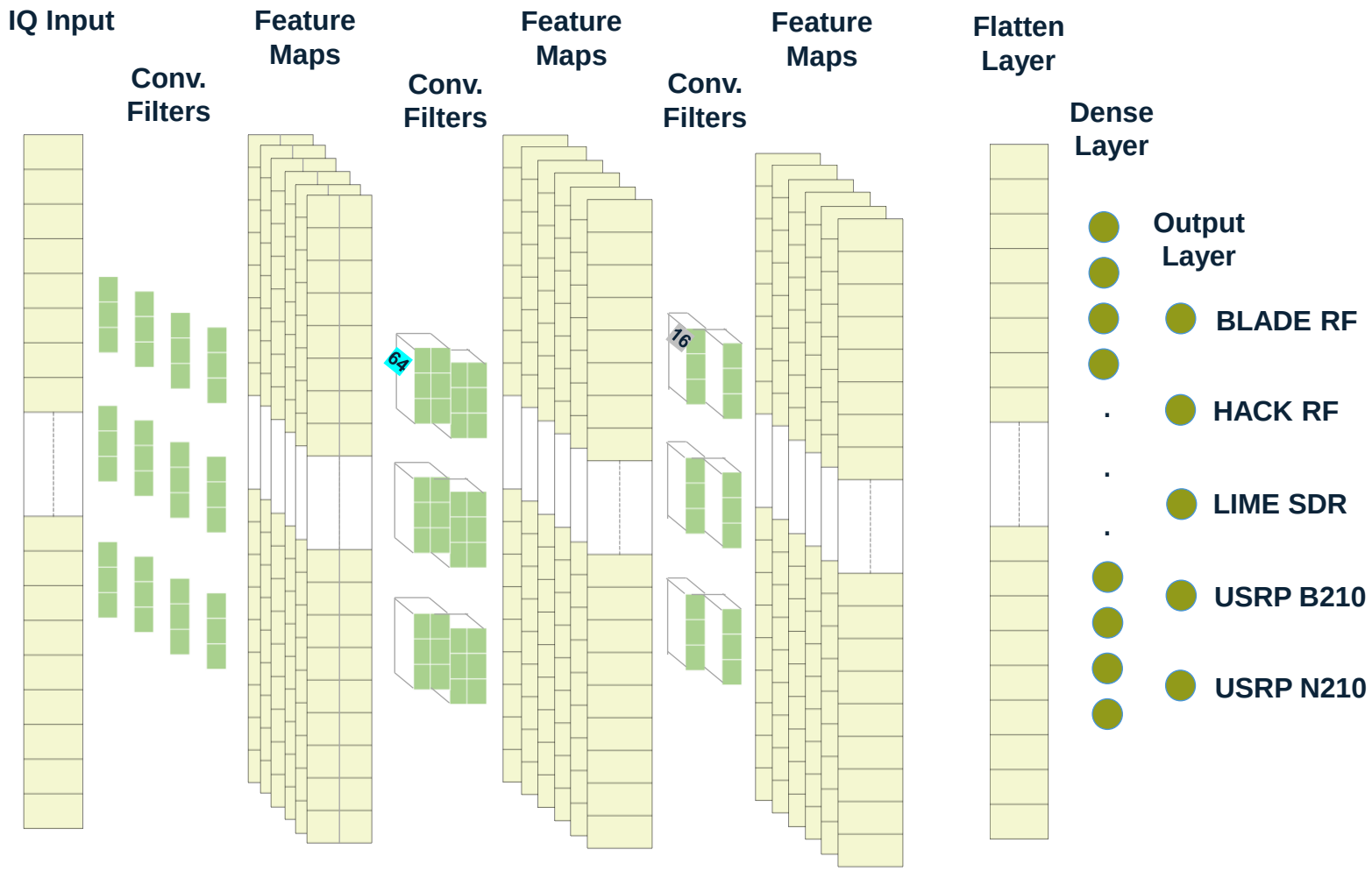
Average Accuracy: 93.11%

Average Precision: 93.05%

Easily Extendable to Other Protocols

Neural Network (NN) Fingerprinter Architecture: Protocol Agnostic

TensorFlow



BLADE RF	HACK RF	LIME SDR	B210	N210
100%	0%	0%	0%	0%
0%	67%	0%	33%	0%
0%	0%	100%	0%	0%
0%	0%	0%	100%	0%
0%	0%	0%	0%	100%

Average Accuracy: 93.33%

Average Precision: 95.00%

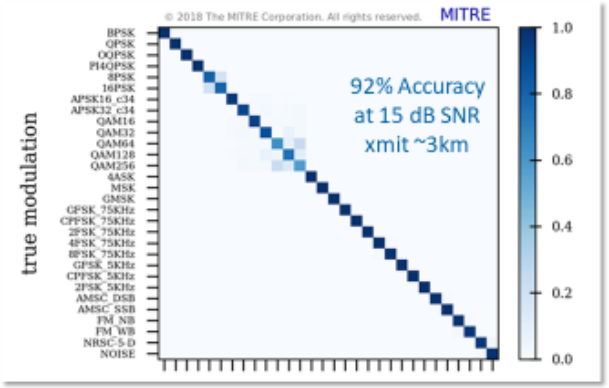
MITRE

Going Forward

Automatic Modulation Recognition

Data Generation

Architecture to iterate design cycle

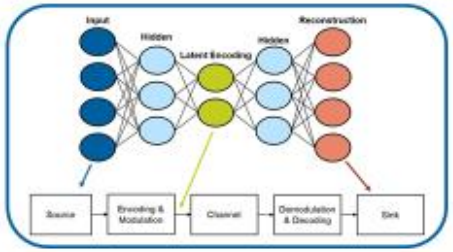


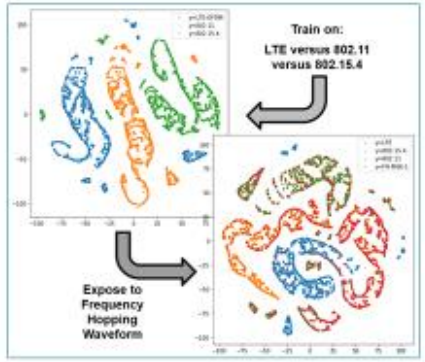
Over-the-air Results

Developed ability to recognize the modulation format of communication waveform
Architecture enables rapid algorithm development & improvement – also extendable to other RF modalities

MITRE

RF Emitter Identification

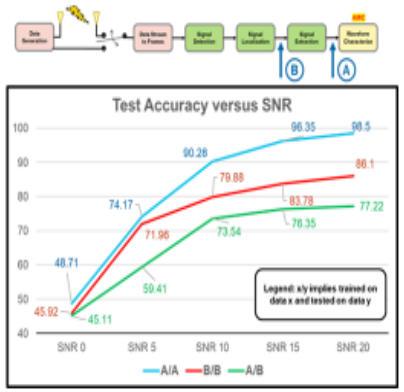




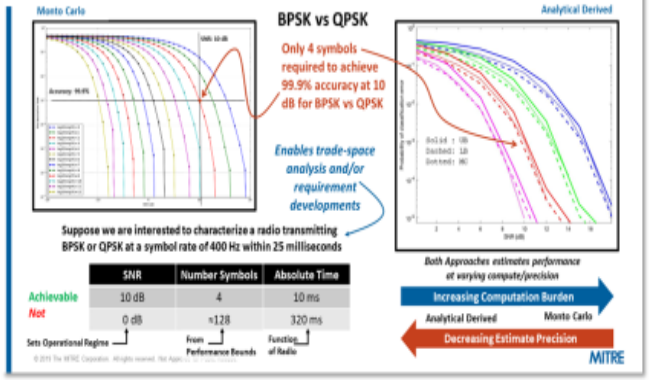
Performance Analysis of Data-Driven Algorithms

Machine Learning algorithms cannot be developed in a vacuum

We studied the affects on performance due to signal processing functions



Computing Modulation Classification Performance Bounds



Mathematically derived performance bounds allows us to better: (1) set algorithmic expectations (2) derive realistic requirements (3) understand operational trade-off space

MITRE

- How much data is needed to achieve requirements?
- Is there a connection to Information Theory?

The view, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation

This technical data deliverable was developed using contract funds under Basic Contract No. W15P7T-13-C-A802.

Curtis Watson, PhD

cmwatson@mitre.org

MITREcorp

linkedin.com/in/curtis-w-b71008123

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™