SweepSense

Sensing 5 GHz in 5 ms using Low-cost Radios

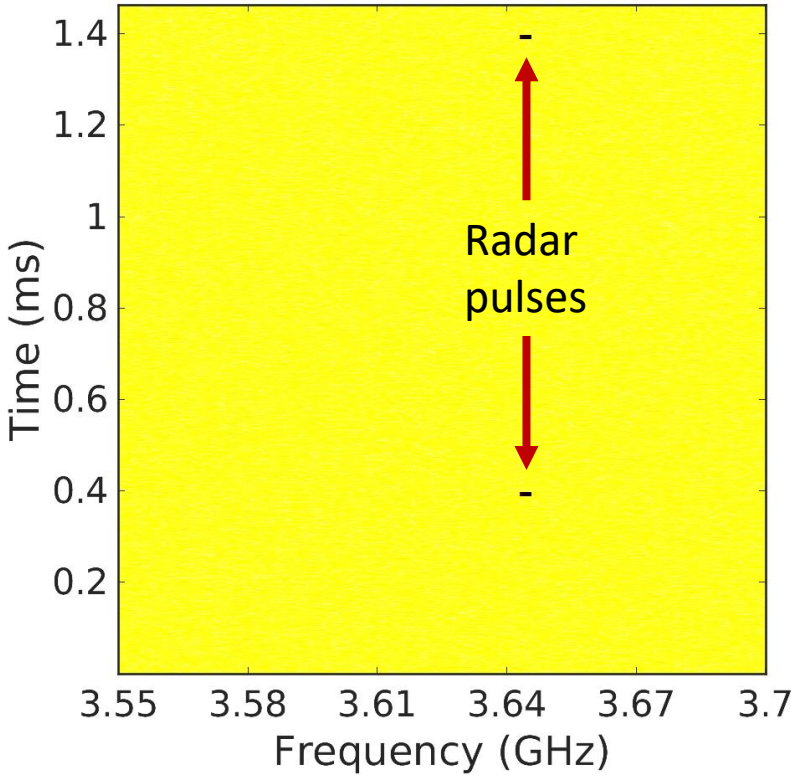
Yeswanth Guddeti, Raghav Subbaraman, Moein Khazraee,
Aaron Schulman, Dinesh Bharadia

UC San Diego

IIT MADRAS

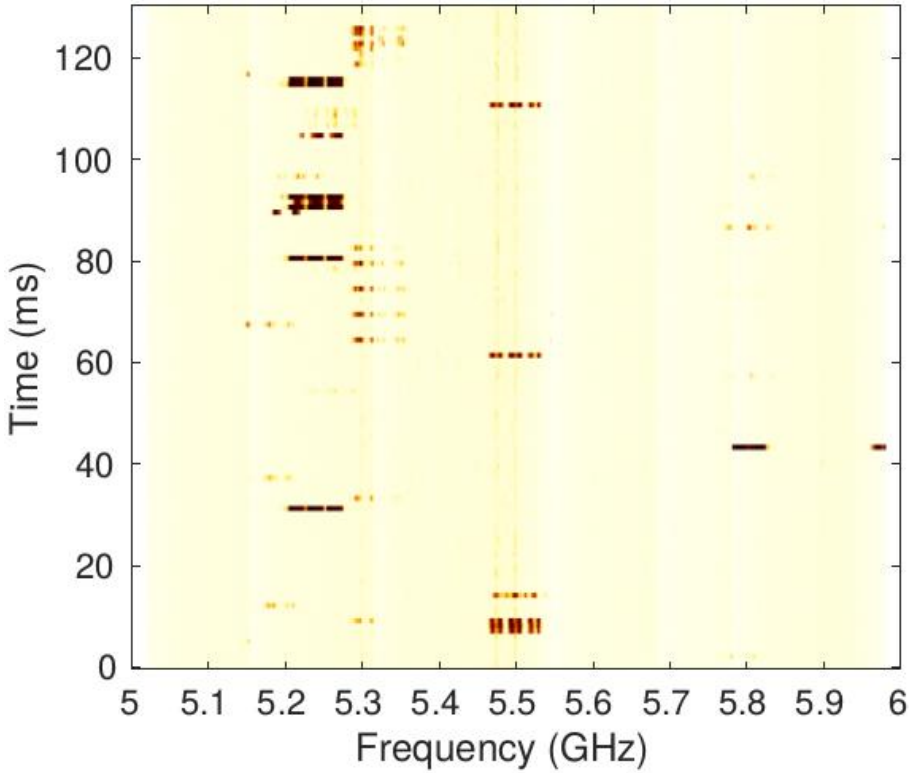
We need wide-bandwidth and high-time resolution sensing

CBRS Spectrum Sharing (3.5 GHz)



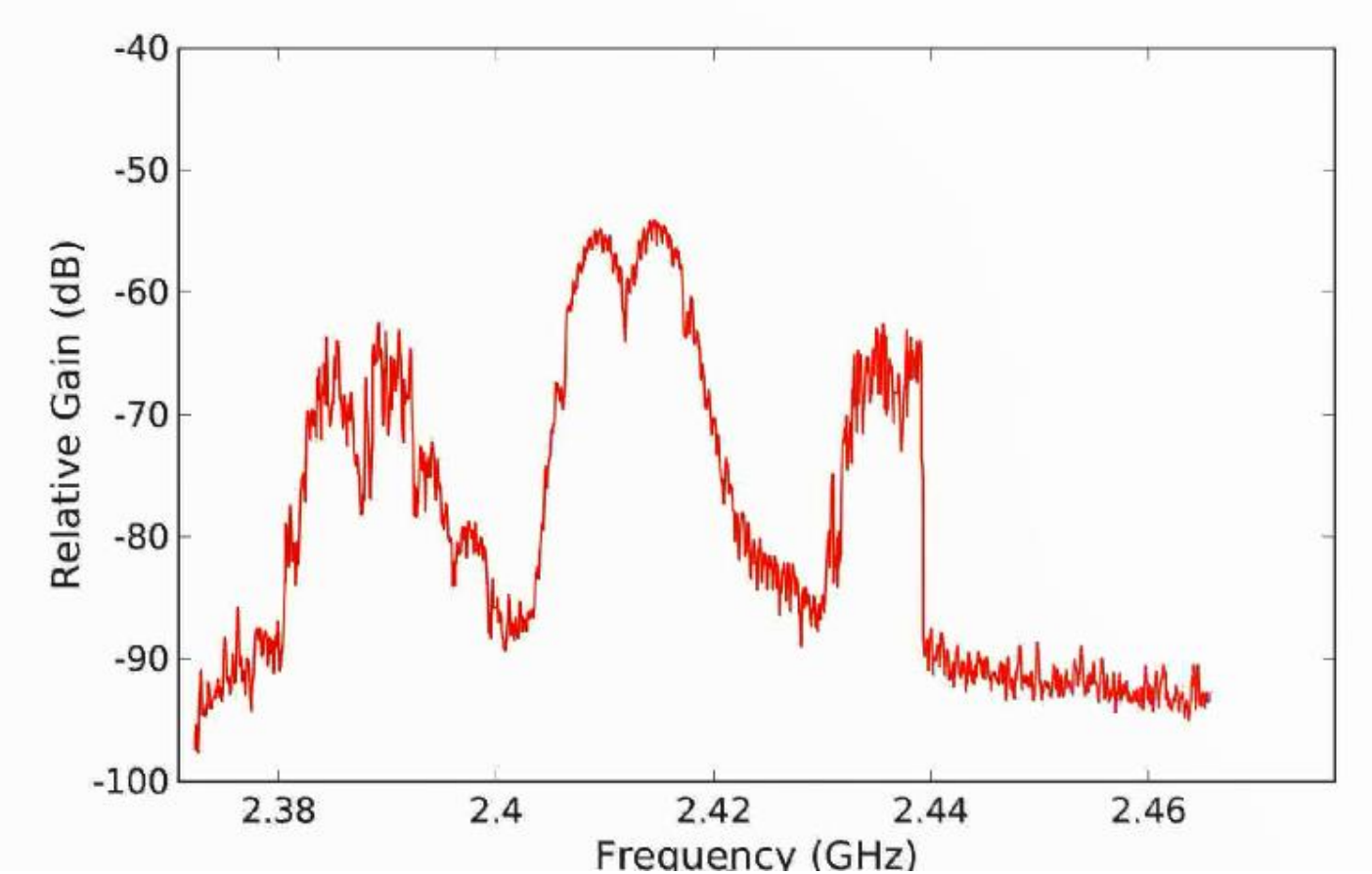
Requires sensing **150 MHz** for **1 ms** long radar pulses

LTE-Unlicensed co-existence (5 GHz)



Requires sensing **700 MHz** for **1 ms** long Wi-Fi frames

Spectrum analyzers sense with wide bandwidth



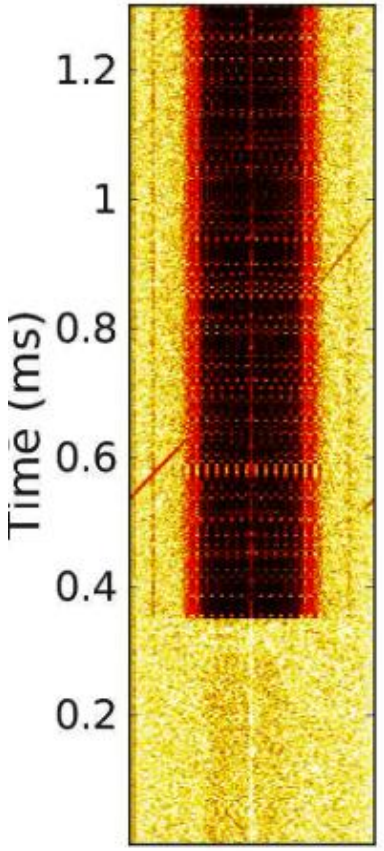




Keysight “RF Sensor”
(Government spectrum monitoring)

They have poor time resolution because they slowly sweep and only measure power

Radio receivers sense with high time resolution



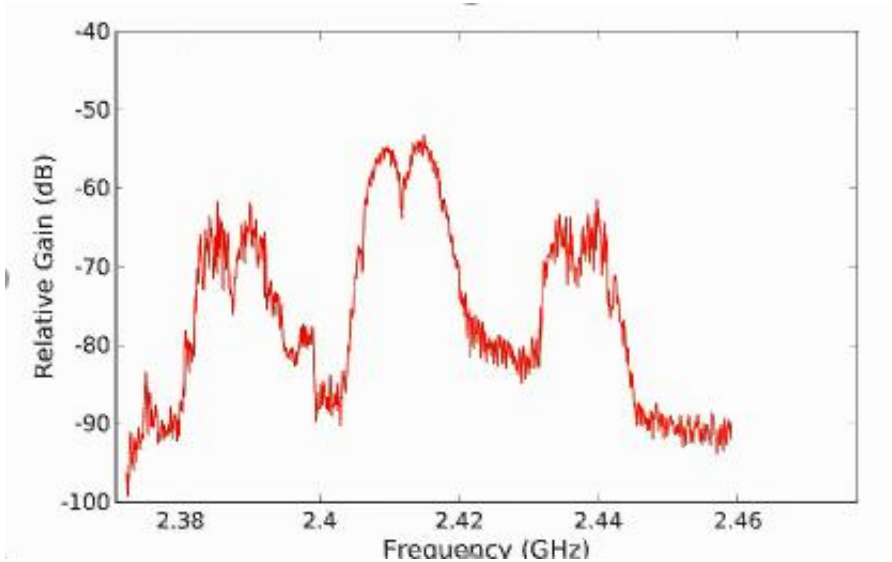


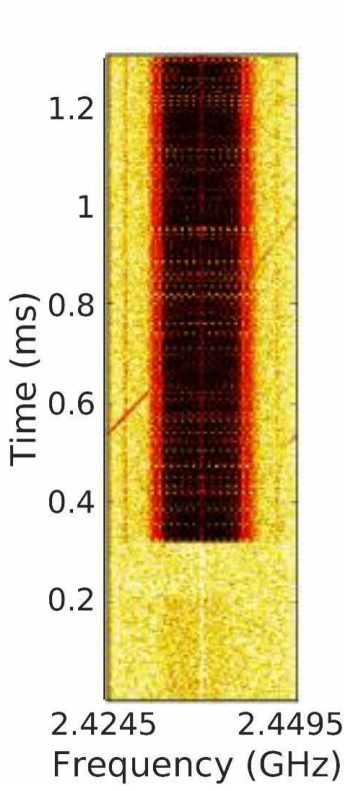
USRP N210 SDR
(Microsoft Spectrum Observatory)

They have poor bandwidth because their ADC has a limited sampling rate

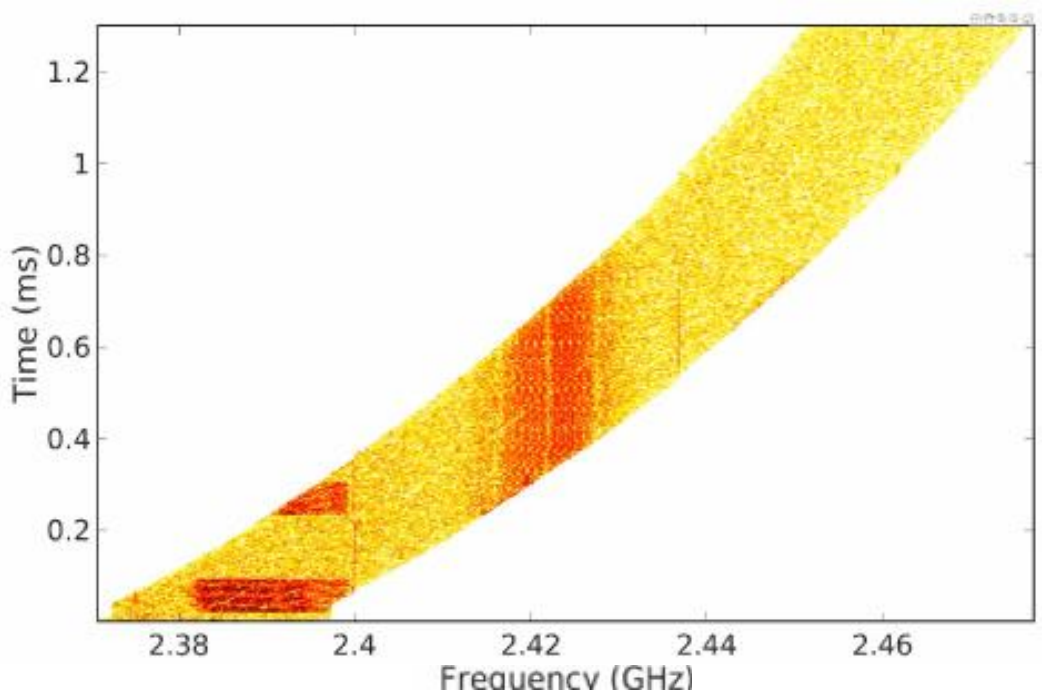
SweepSense: A new paradigm in spectrum sensing

Wide bandwidth + High resolution



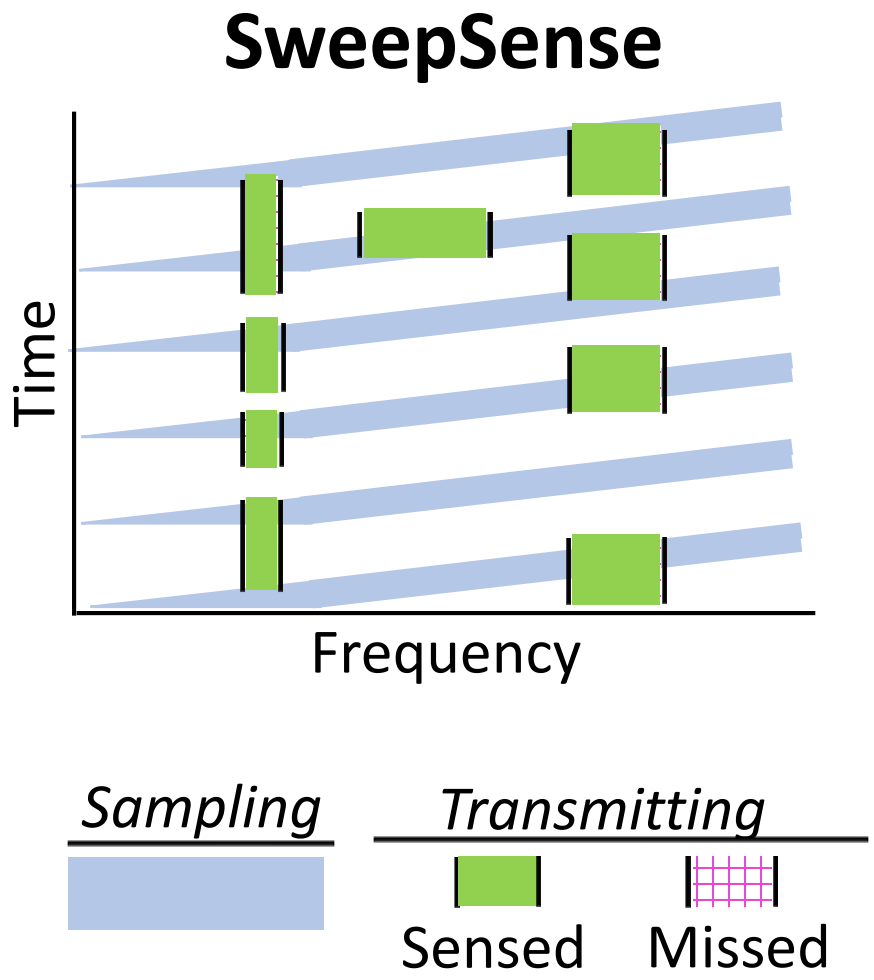


SweepSense



SweepSense combines the sensing capabilities of spectrum analyzers and radio receivers

Insight: Sweeping radio receivers capture a portion of every signal



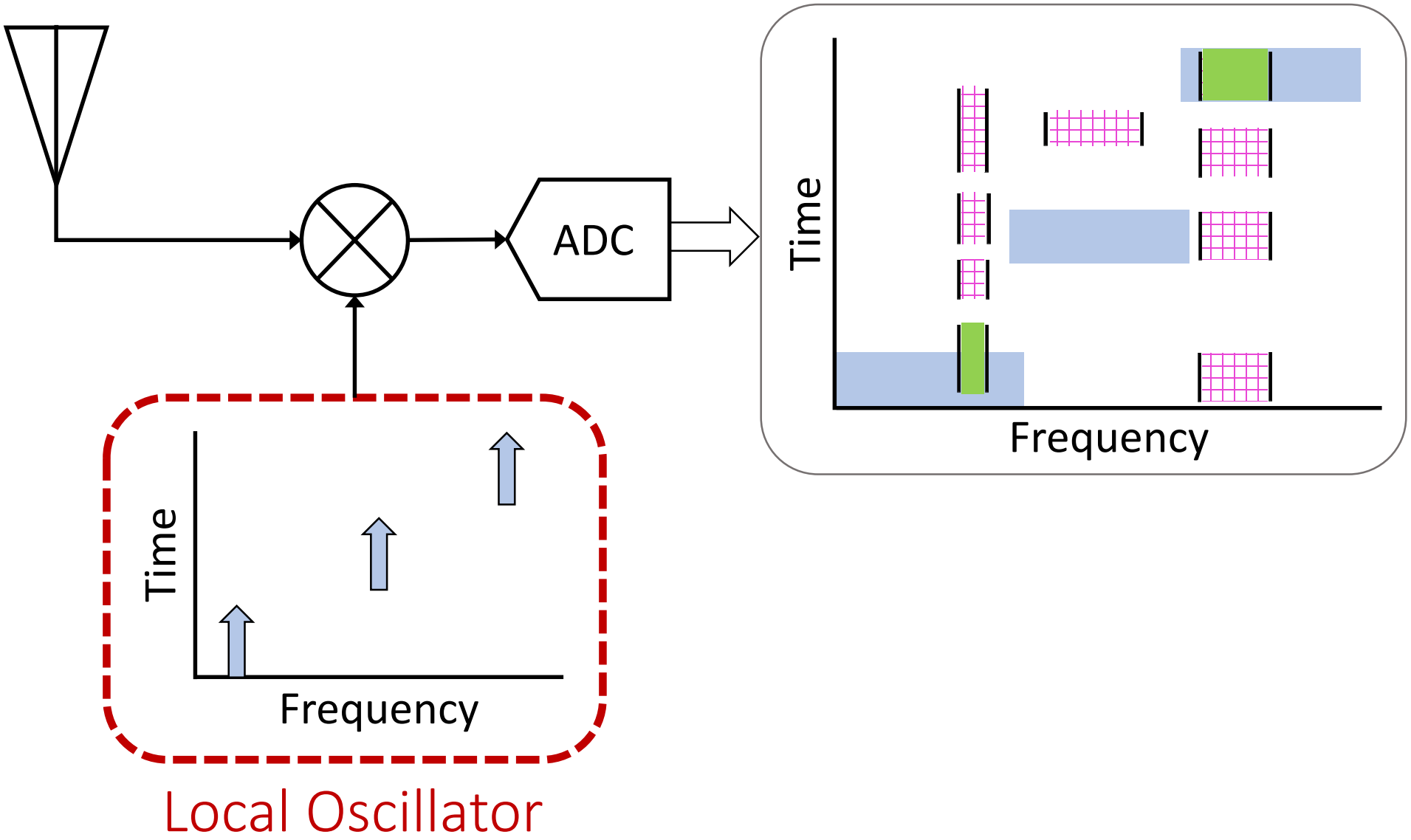
SweepSense Overview

1. Modifying off-the-shelf radio receivers to sweep the spectrum

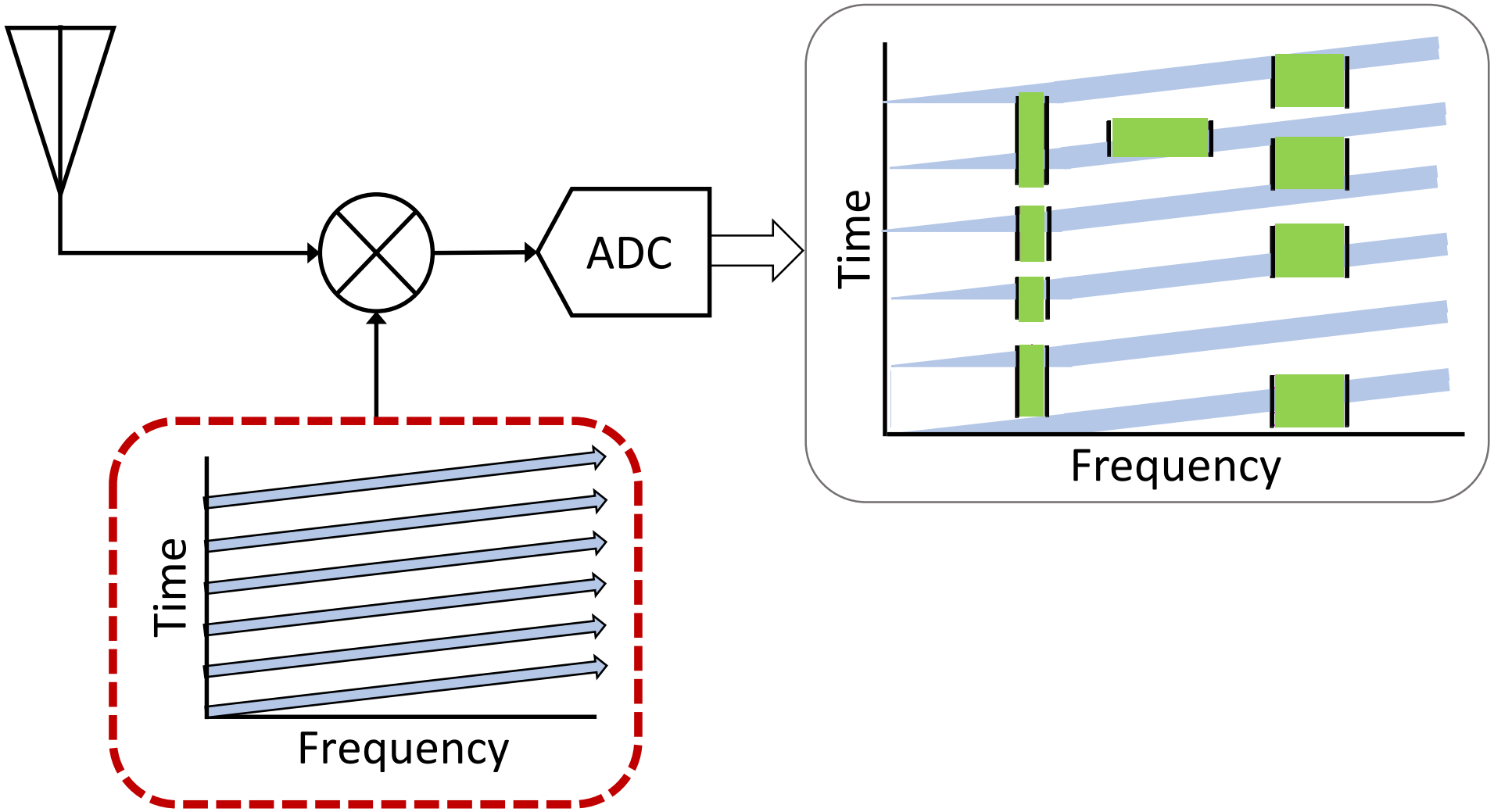
2. Unsweeping the distorted captures from sweeping receivers

3. Detecting the transmission protocol in unswept captures

Background: Radio receivers tune by generating a tone

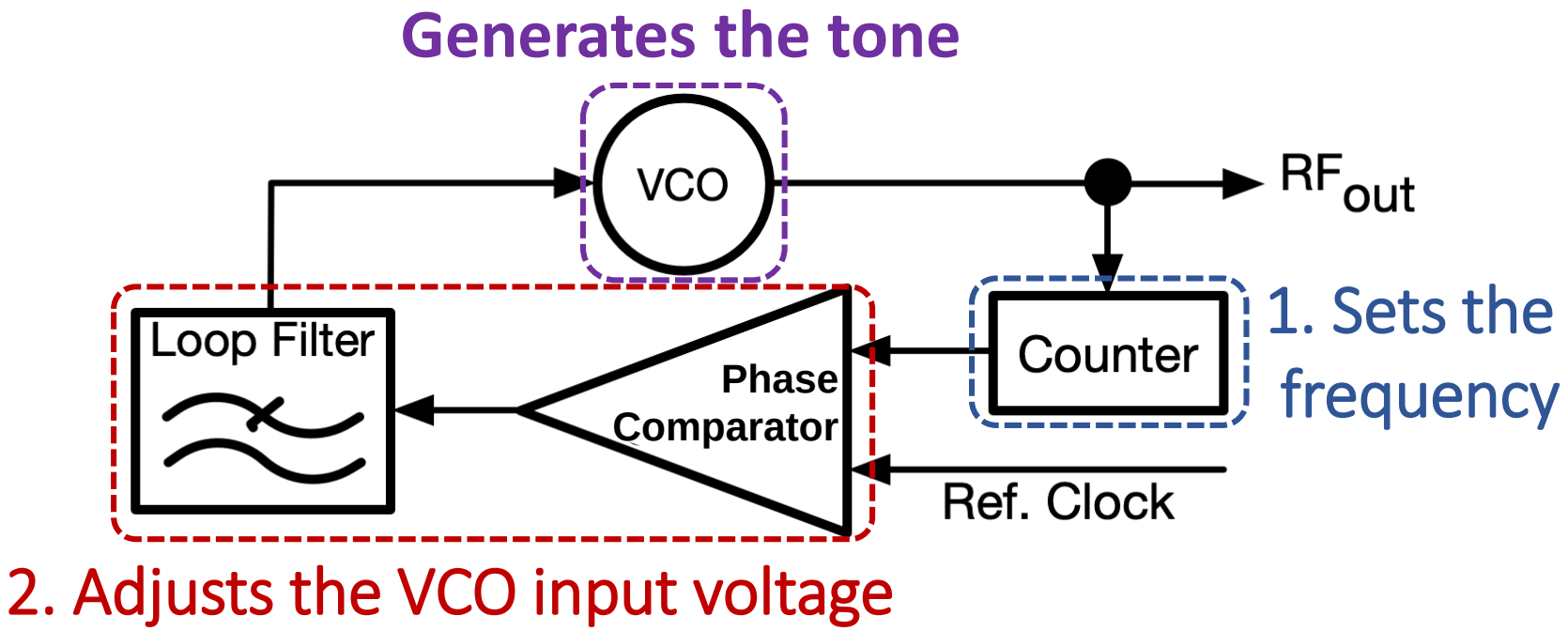


Generating a sweeping tone makes the receiver sweep



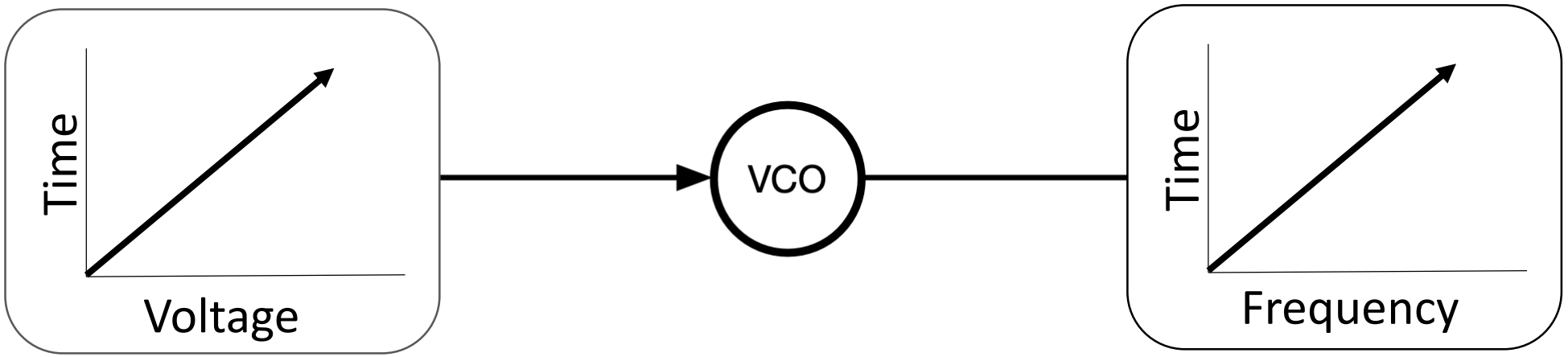
Sweeping Local Oscillator

A typical local oscillator is a VCO feedback loop

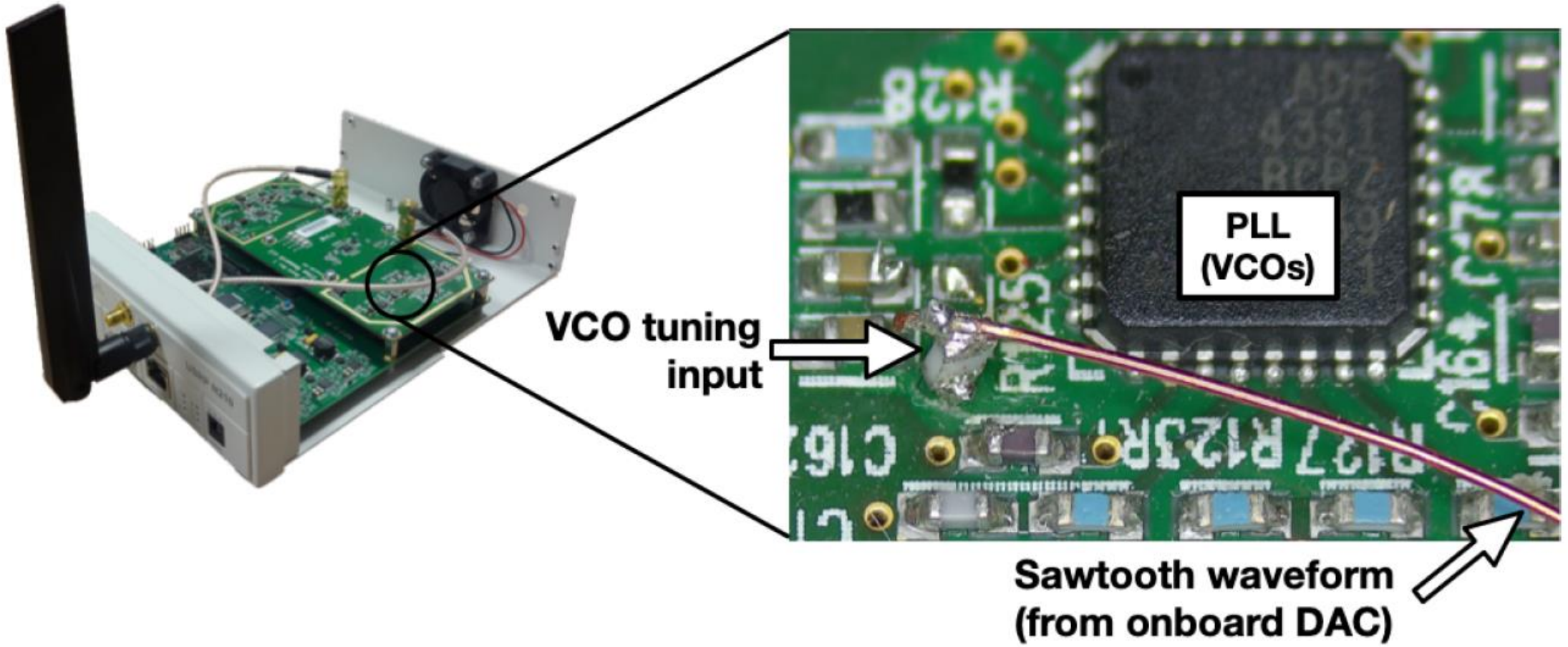


Problem: The feedback loop typically takes 10-100 µs to stabilize

SweepSense replaces the feedback loop with a ramp



Making the oscillator sweep only requires a single-wire mod



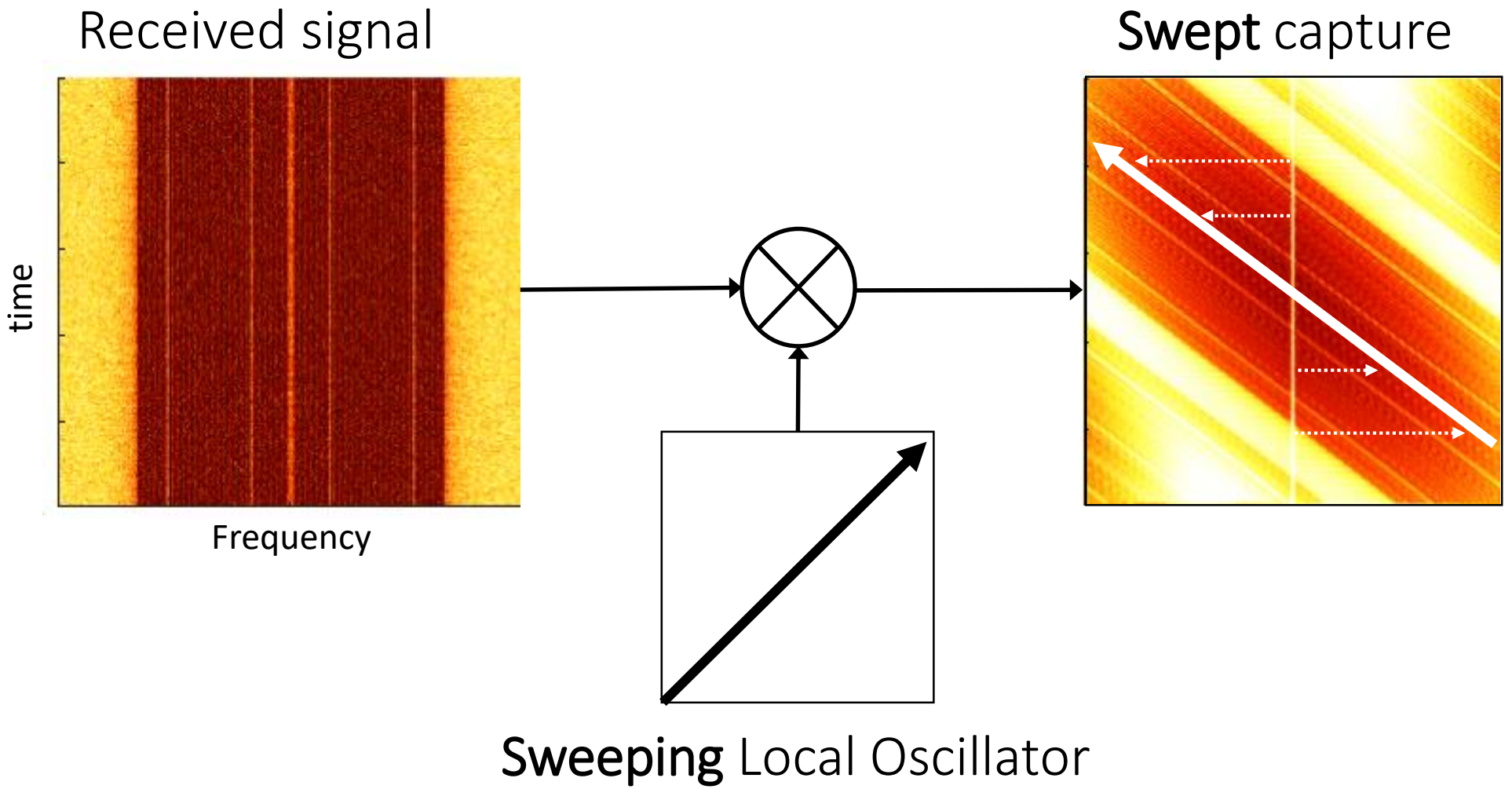
SweepSense Overview

1. Modifying off-the-shelf radio receivers to sweep the spectrum

2. Unsweeping the distorted captures from sweeping receivers

3. Detecting the transmission protocol in unswept captures

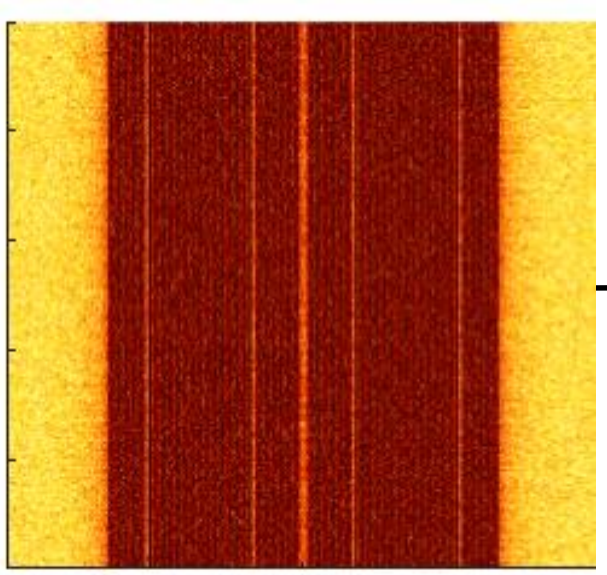
SweepSense captures have continuously changing center frequency

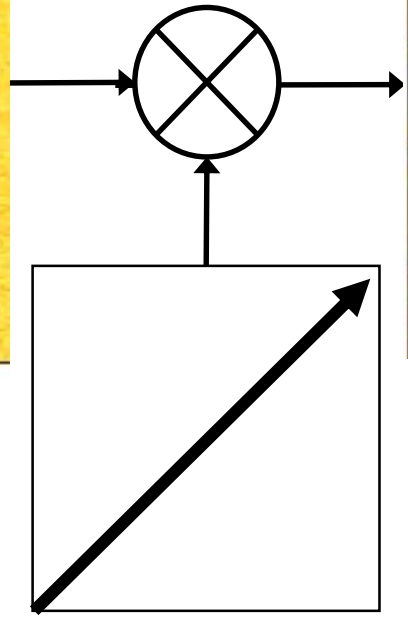


We need to unsweep the samples so they have a **fixed** center frequency

By applying a self-calibration signal, we can unsweep the samples

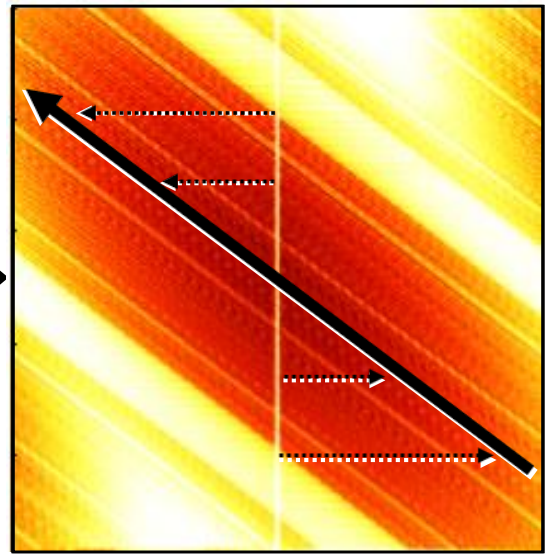
Received signal

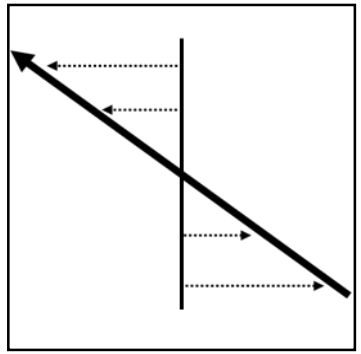




Sweeping Local Oscillator

Swept capture

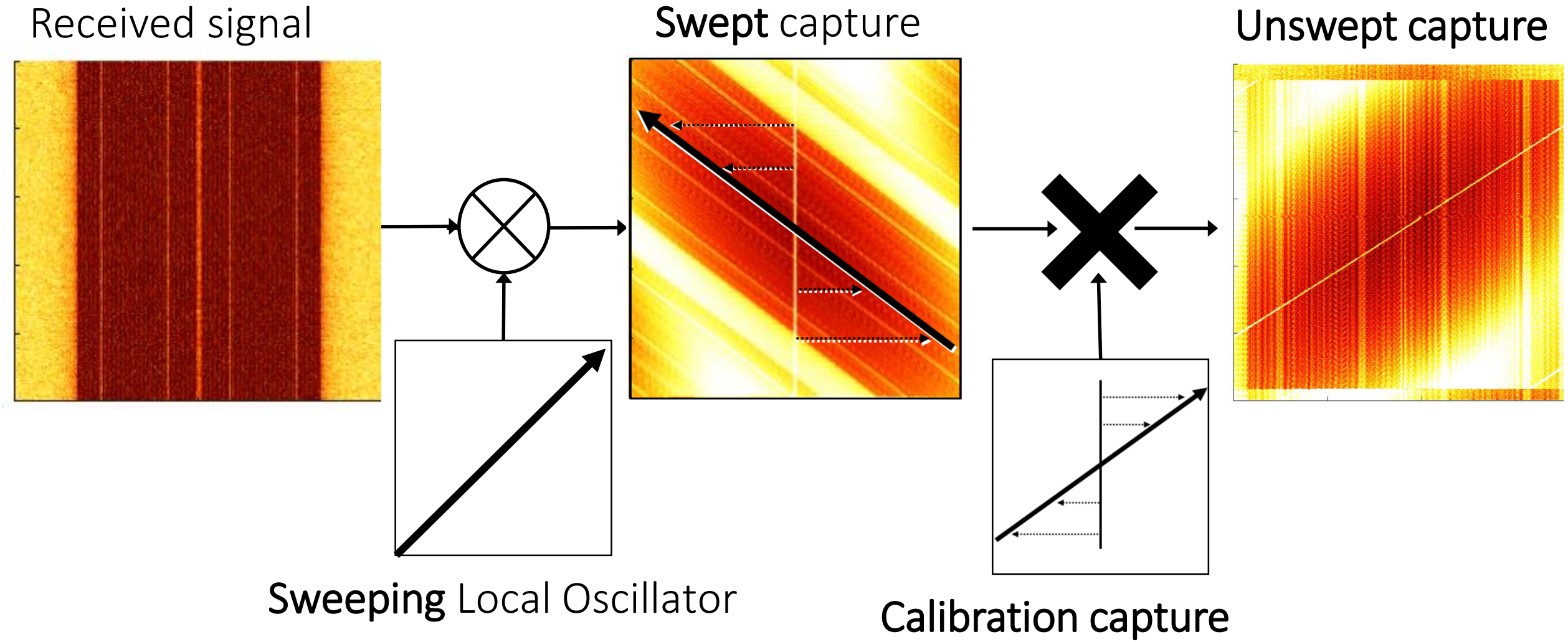




Calibration capture

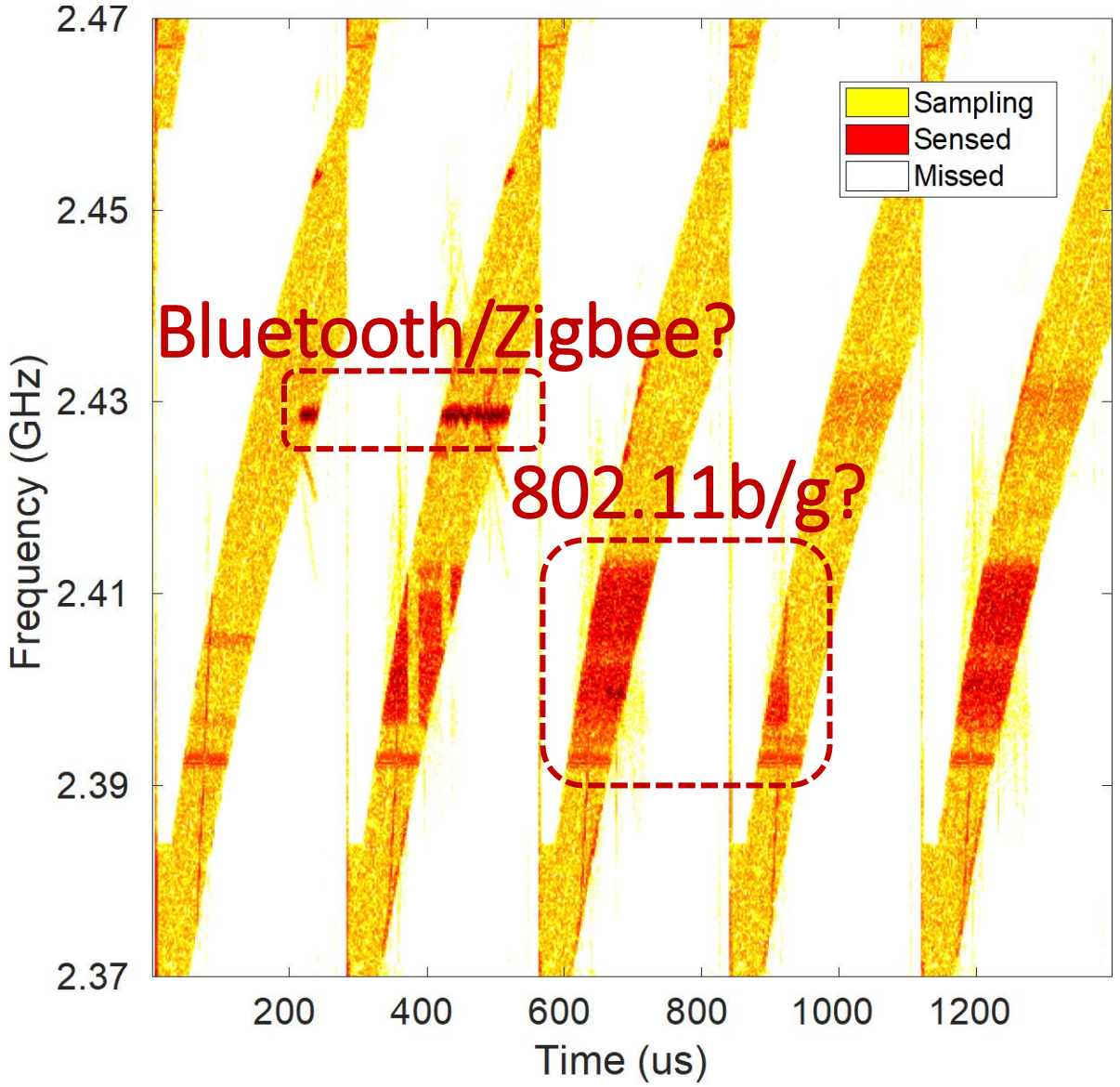
Unsweeping therefore creates a view of samples as if they are captured at a fixed frequency

By applying a self-calibration signal, we can unsweep the samples



Unsweeping therefore creates a view of samples as if they are captured at a fixed frequency

Swept captures contain significant portions of packets



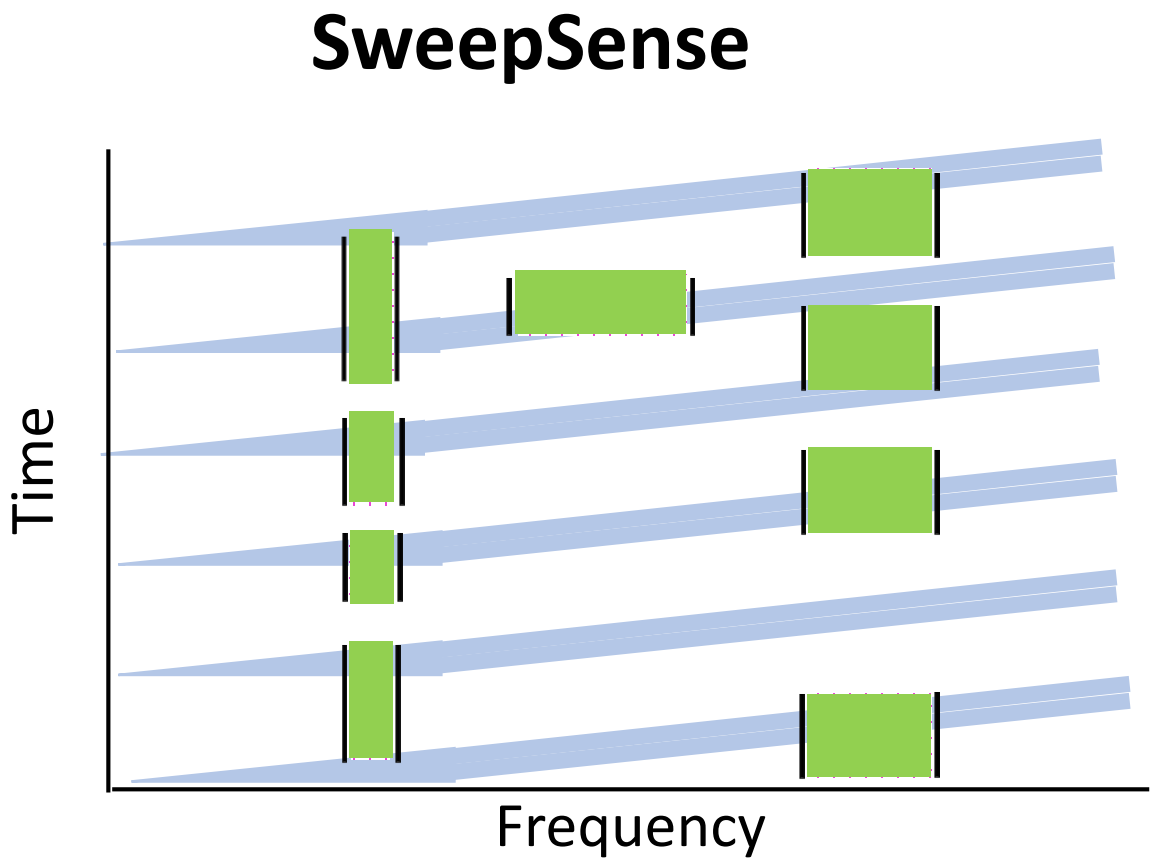
SweepSense Overview

1. Modifying off-the-shelf radio receivers to sweep the spectrum

2. Unsweeping the distorted captures from sweeping receivers

3. Detecting the transmission protocol in unswept captures

Challenge – We only capture a part of the packet

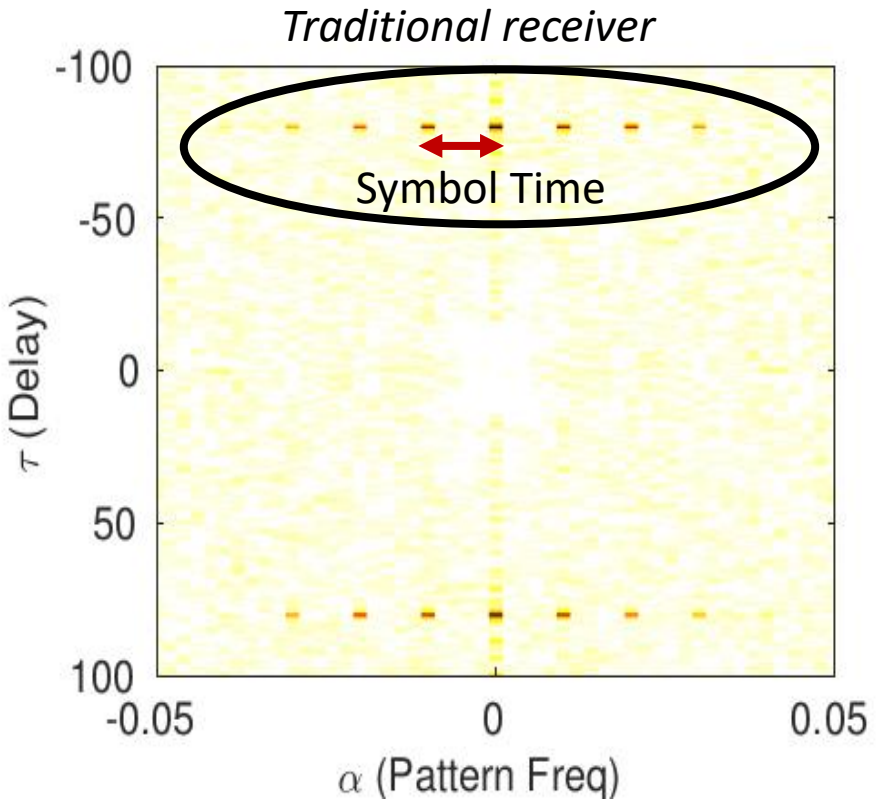


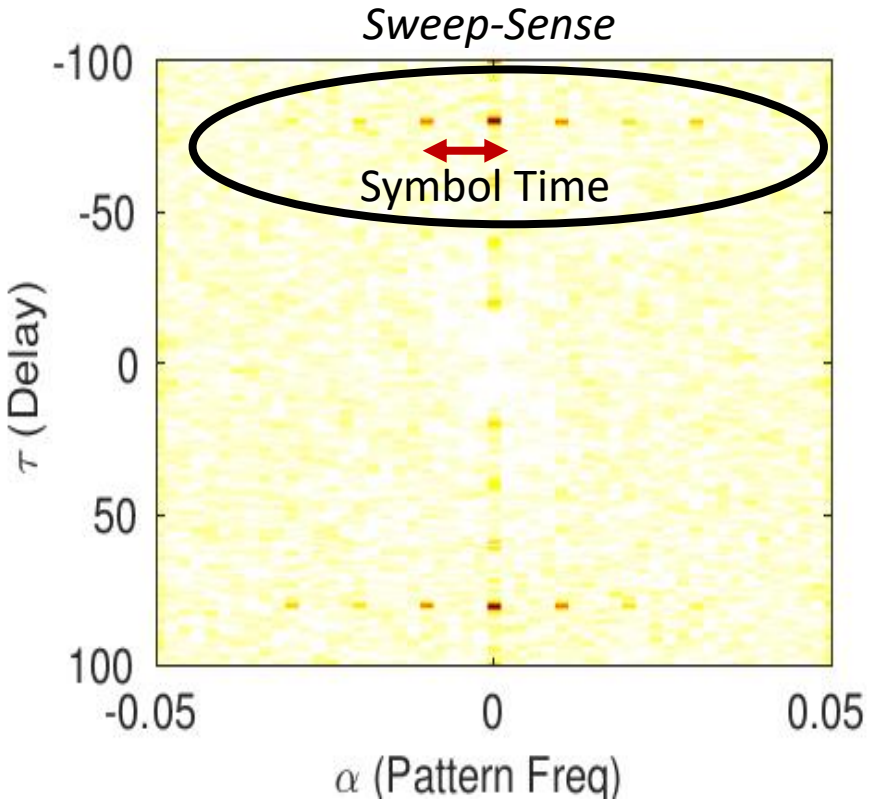
Standard decoding techniques can not detect the protocol using part of a packet

Protocol detection only requires short captures

Cyclo-stationary analysis captures repeated patterns in frequency and time.

- WiFi OFDM symbol time is captured by cyclic auto-correlation function (CAF).





Short Unswept captures retain Cyclostationary patterns

Cyclostationary patterns are distinct for each protocol

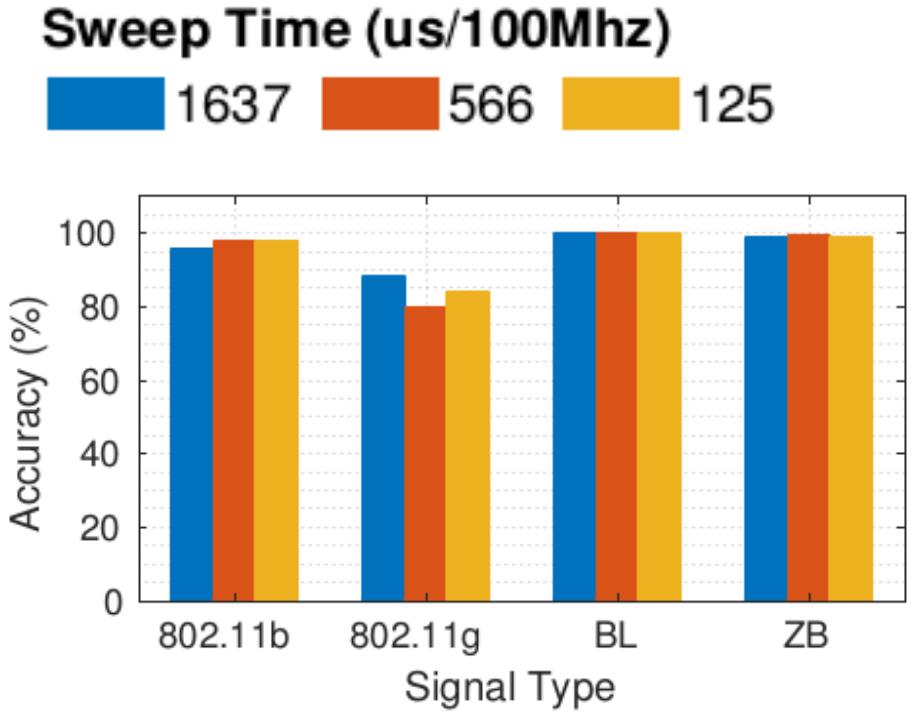
Bluetooth exhibit patterns in frequency and Zigbee exhibit patterns in time, which are distinguishable in Cyclo-stationarity analysis.

We use a Machine Learning-based model to classify the protocols:

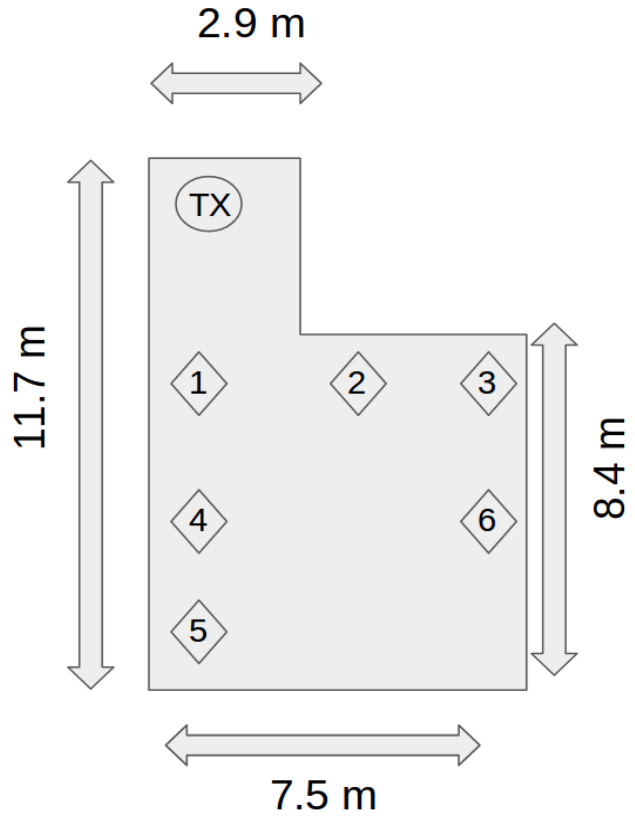
- Bluetooth (BLE)
- Zigbee (ZB)
- WiFi-OFDM (802.11g)
- WiFi-DSSS (802.11b)

Sensing protocols in Unlicensed band

Unlicensed band has OFDM, DSSS, BT, Zigbee.



Classification Accuracy



Layout of the room

SweepSense can sweep GHz wideband in a millisecond while still detecting protocols.

Radar detection in CBRS band

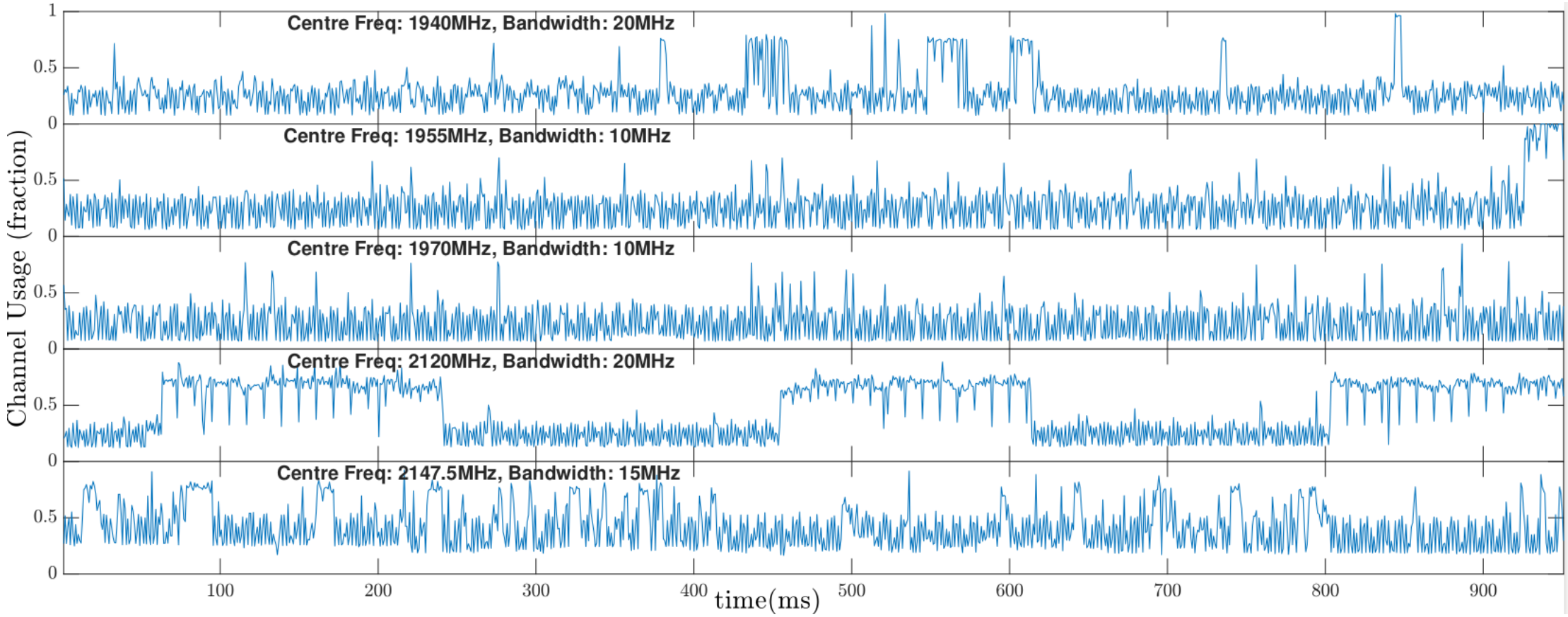
- Scans CBRS band **3.55 – 3.7 GHz** every **1.3 ms**.
- Use Vector Signal Generator (Keysight N5182B) to generate radar type “Bin 1 Lite” as per official testing and certification procedures for ESC sensors

Radar Type	Pulse width (us)	Pulses per second	Pulses per burst	Accuracy
Bin 1 Lite	0.8	1000	19	**99.5 % (398/400)**

SweepSense reliably detects maritime radar across 150 MHz

SweepSense creates new spectrum sharing opportunities

5 Downlink Channels spread across 200MHz are observed every 0.9 ms



SweepSense can detect loading across 200 MHz of LTE transmissions.

Conclusion

SweepSense can rapidly capture and classify the entire terrestrial spectrum.

Applications

- **Protocols detection for the ISM band**
- **Radar pulse detection in CBRS band**
- **LTE load pattern detection**

Future Applications:

- Interference Detection
- Transmitter localization

SweepSense begins!

Build your own applications using open-sourced SweepSense.



github.com/ucsdsysnet/sweepsense