SweepSense
Sensing 5 GHz in 5 ms using Low-cost Radios

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

They have poor time resolution because they slowly sweep and only measure power.
Radio receivers sense with high time resolution

They have poor bandwidth because their ADC has a limited sampling rate
SweepSense: A new paradigm in spectrum sensing

Wide bandwidth + High resolution

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

**Diagram:**

Time

Frequency

ADC

**Graph:**

Time

Frequency

Sweeping Local Oscillator
A typical local oscillator is a VCO feedback loop

1. Sets the frequency
2. Adjusts the VCO input voltage

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

Received signal

Swept capture

Sweeping Local Oscillator

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

Frequency (GHz)

Time (us)

2.37

2.39

2.41

2.43

2.45

2.47

Sampling
Sensed
Missed

Bluetooth/Zigbee?

802.11b/g?
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

SweepSense

Time

Frequency

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.

Sweep Time (us/100Mhz)

- Blue: 1637
- Red: 566
- Yellow: 125

### Classification Accuracy

<table>
<thead>
<tr>
<th>Signal Type</th>
<th>802.11b</th>
<th>802.11g</th>
<th>BL</th>
<th>ZB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy (%)</td>
<td>100</td>
<td>80</td>
<td>90</td>
<td>70</td>
</tr>
</tbody>
</table>

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

### Layout of the room

- TX
- Nodes 1, 2, 3, 4, 5, 6
- Dimensions: 11.7 m x 8.4 m x 7.5 m
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.

<table>
<thead>
<tr>
<th>Radar Type</th>
<th>Pulse width (us)</th>
<th>Pulses per second</th>
<th>Pulses per burst</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bin 1 Lite</td>
<td>0.8</td>
<td>1000</td>
<td>19</td>
<td><strong>99.5 %</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><em>(398/400)</em></td>
</tr>
</tbody>
</table>

SweepSense reliably detects maritime radar across 150 MHz.
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