KAIST Smile LAB

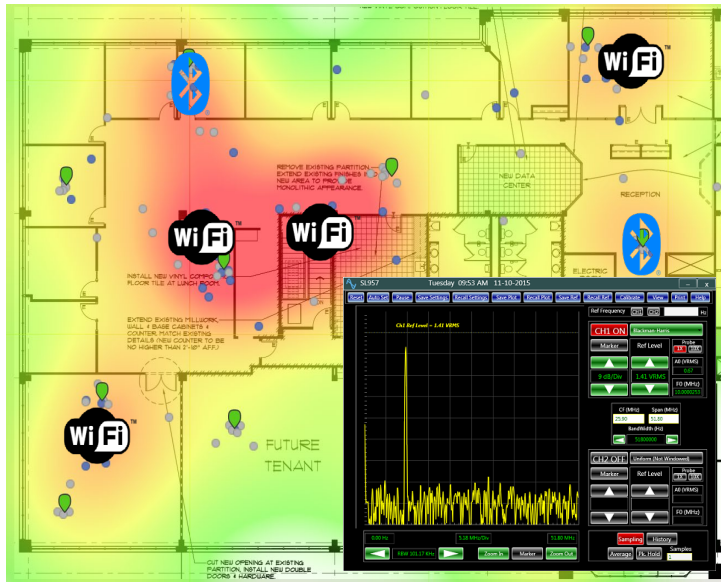
SDR Receiver Using Commodity WiFi via Physical-Layer Signal Reconstruction

Woojae Jeong, Jinhwan Jung, Yuanda Wang, Shuai Wang, Seokwon Yang, Qiben Yan, Yung Yi, and Song Min Kim

in collaboration with MICHIGAN STATE UNIVERSITY GEORGE MASON UNIVERSITY

Everything is going wireless

PHY signal analysis is crucial



Network management and operation

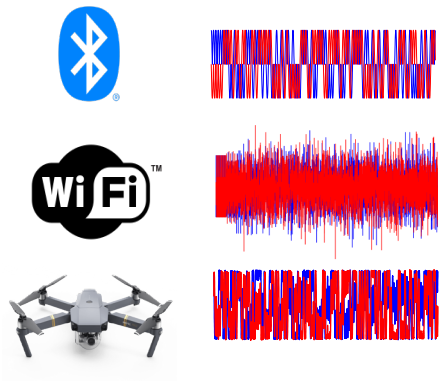
Security and privacy protection

IoT data collection

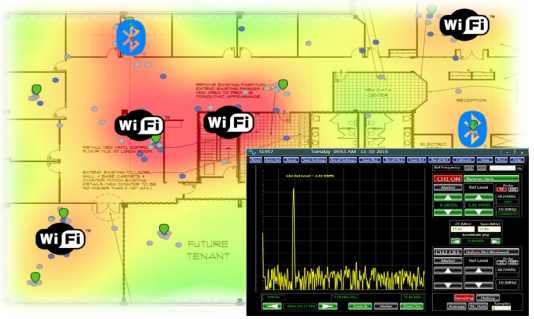
SDR is current de facto solution!

Why SDR?

1. Receive ambient signal in the air

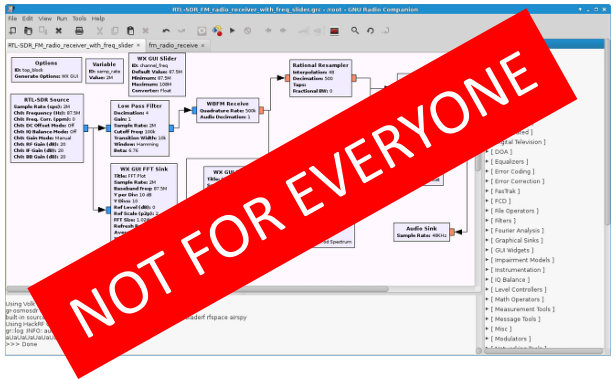


2. Software processing and applications



SDR is rarely used

	NI USRP	HackRF One
Price	$ 1100~	$ 300
Hard to use	Gnuradio	



SDR-Lite

A new design to use commodity WiFi as a SDR receiver

Beneficial WiFi

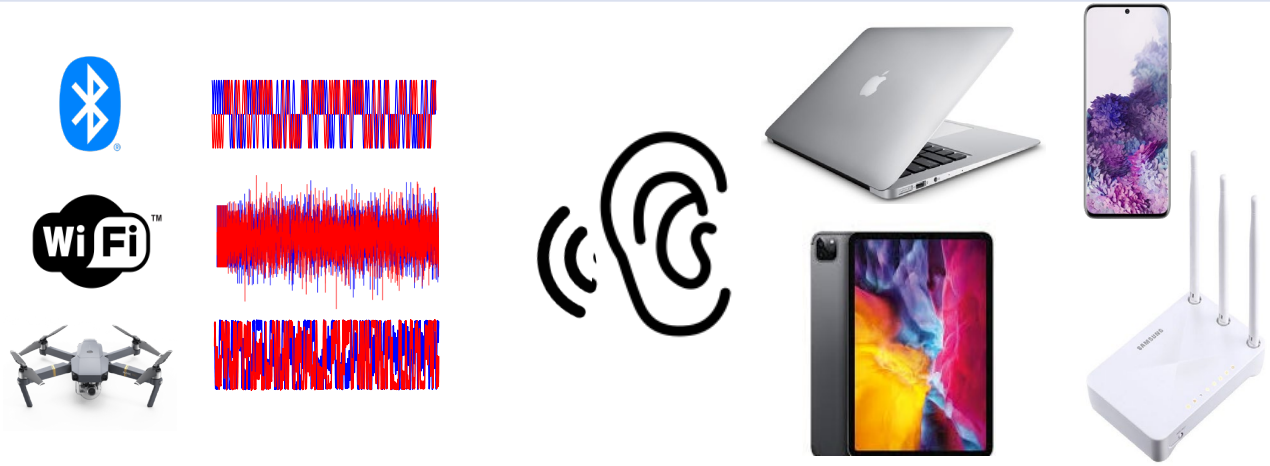
WNIC is Cheap

AR 9380: $14

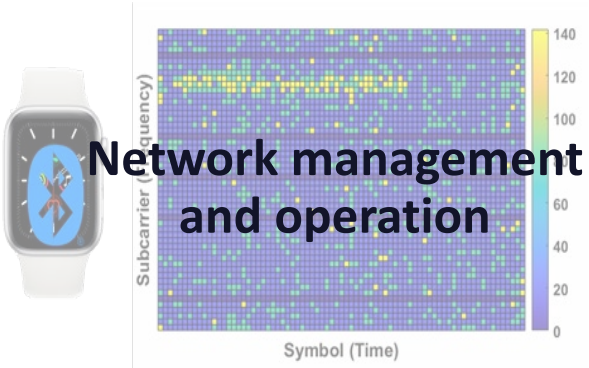
Billions of users

SDR-Lite: SDR Receiver Using Commodity WiFi

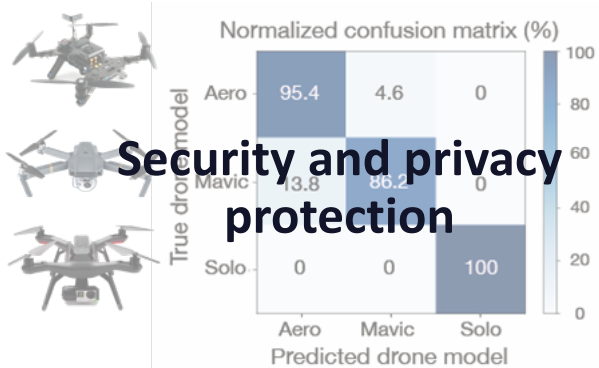
1. Receive ambient signal in the air



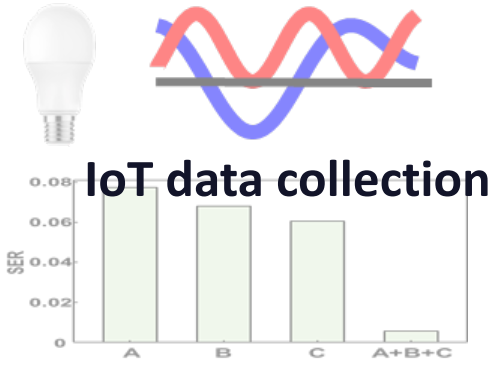
2. Software processing and applications



Network management and operation



Security and privacy protection



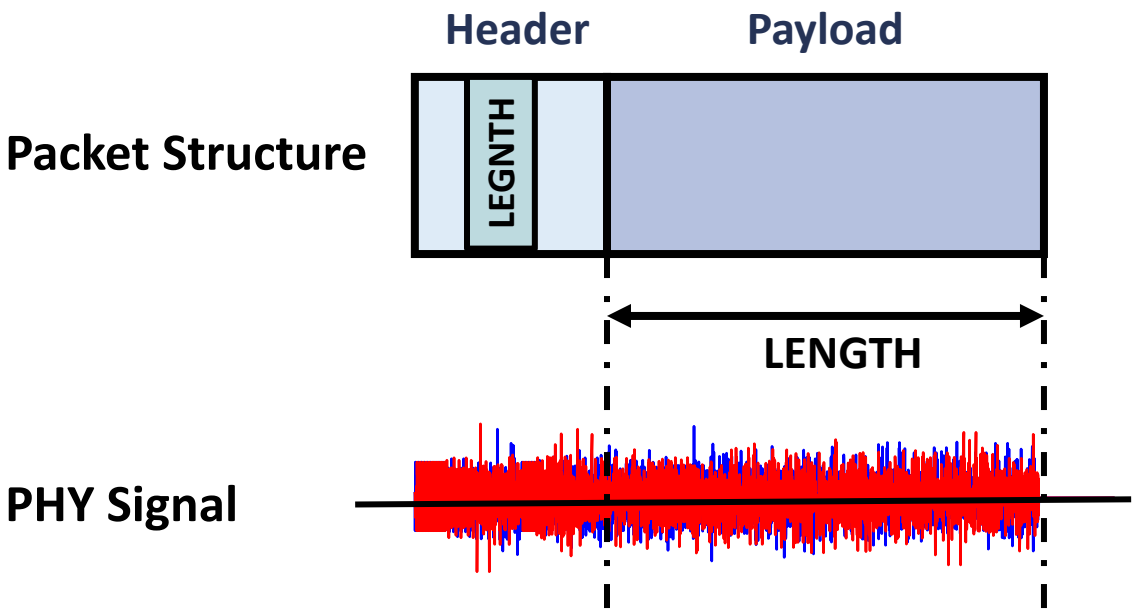
IoT data collection

Design Overview

1. Receive ambient signal in the air

2. Software processing and applications

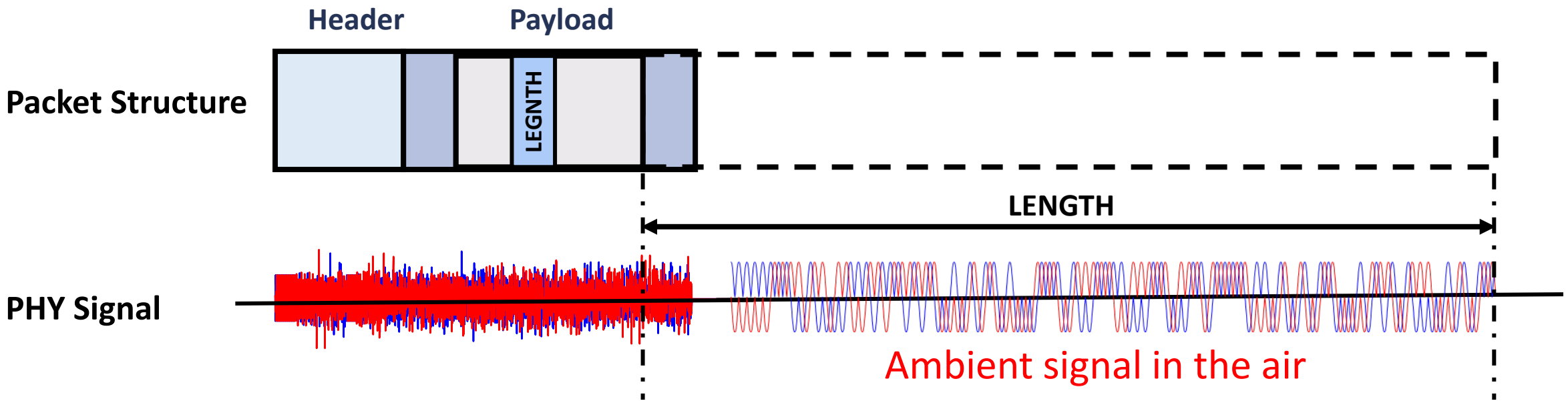
Signal reception of typical WiFi



WiFi decodes a packet during time corresponding LENGTH

How to receive ambient signal

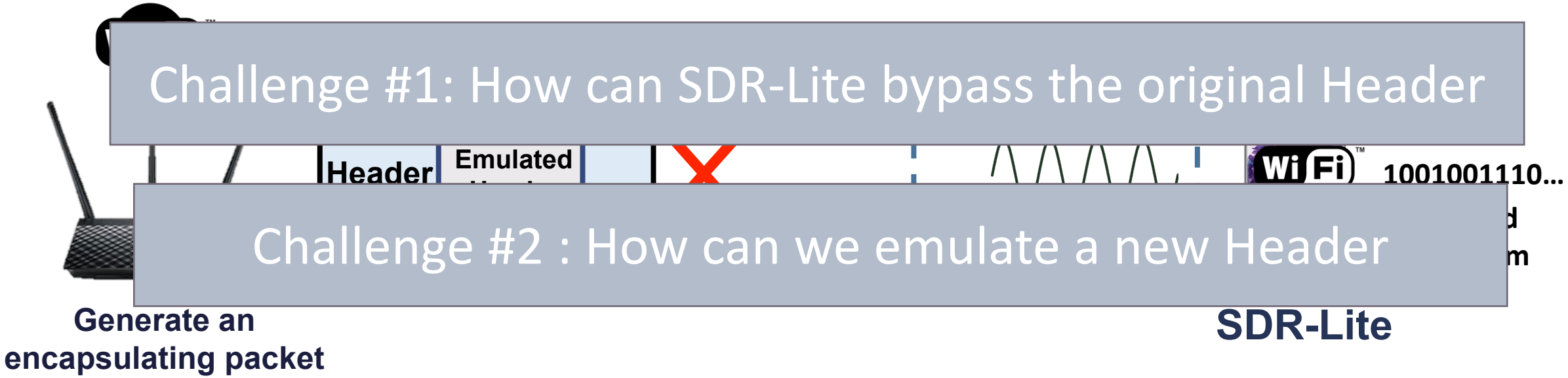
Q: What if a WiFi packet contains another header in the payload?



Construct a new WiFi Header in Payload through emulation

How SDR-Lite works?

WiFi transmitter sends an encapsulating packet that contains Emulated Header

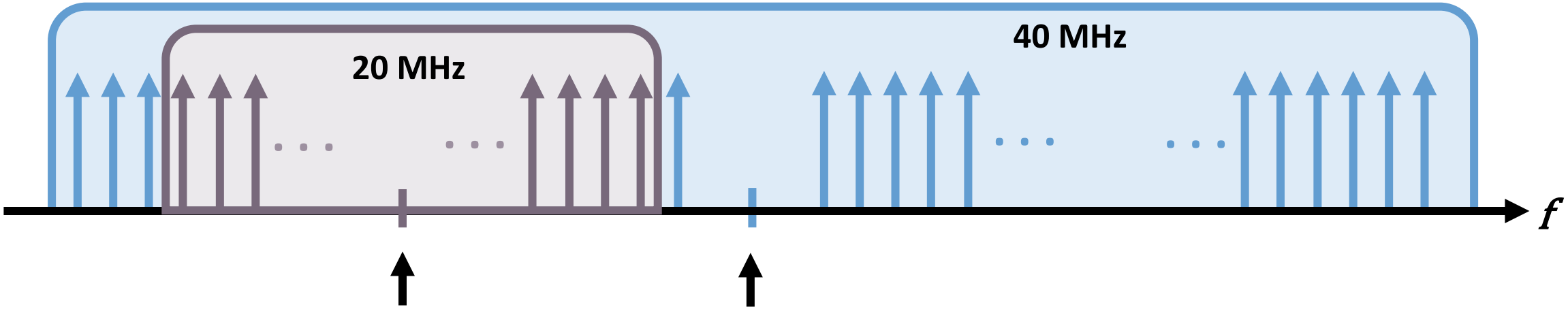


Challenge #1: How can SDR-Lite bypass the original Header

Challenge #2 : How can we emulate a new Header

Challenge #1: How can SDR-Lite bypass the original Header

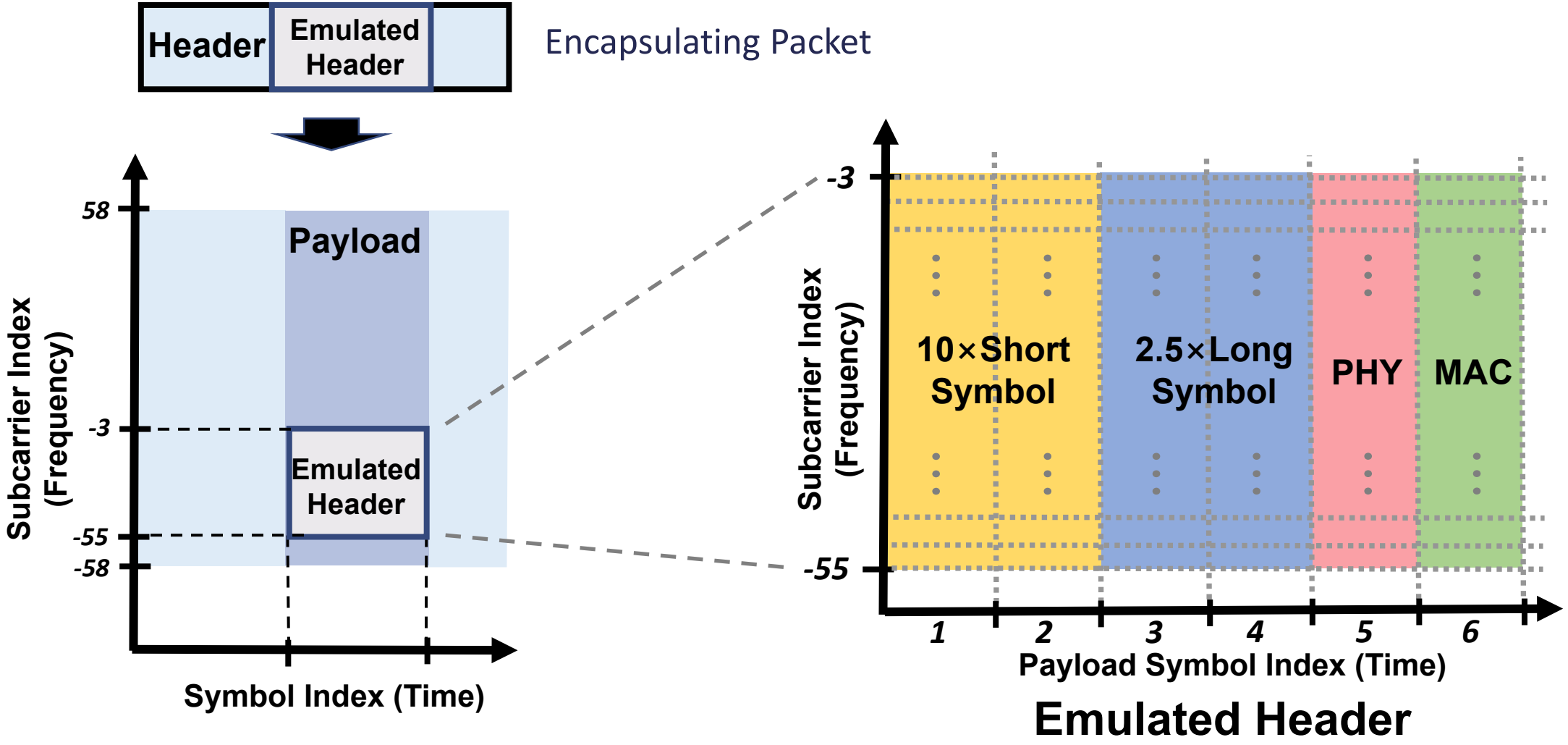
Encapsulating Packet



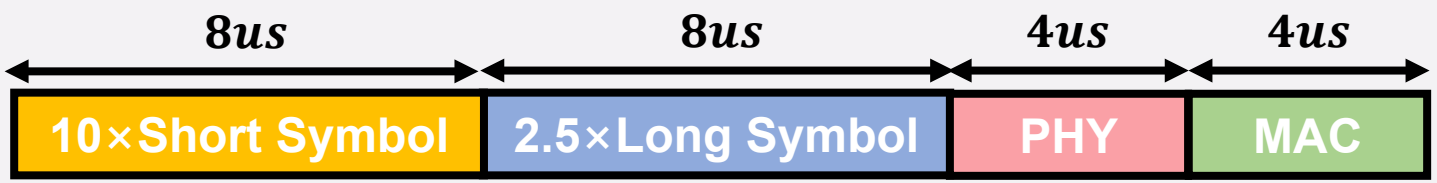
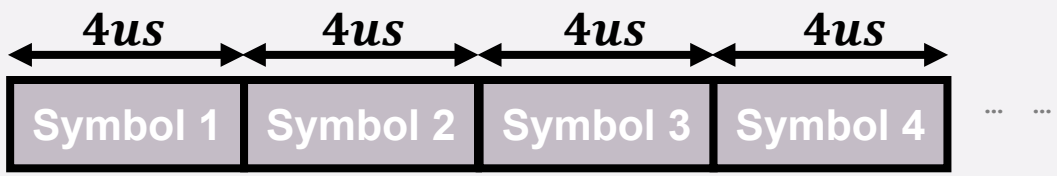
20MHz center frequency ≠ 40MHz center frequency

SDR-Lite channel

Challenge #2 : How can we generate an emulated Header

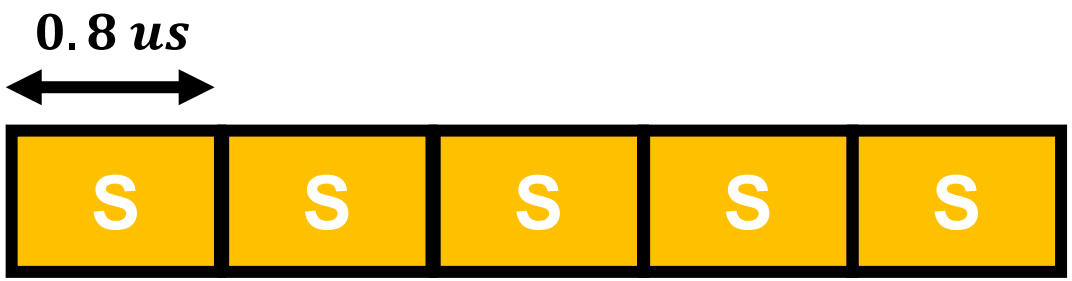


Header emulation using Payload

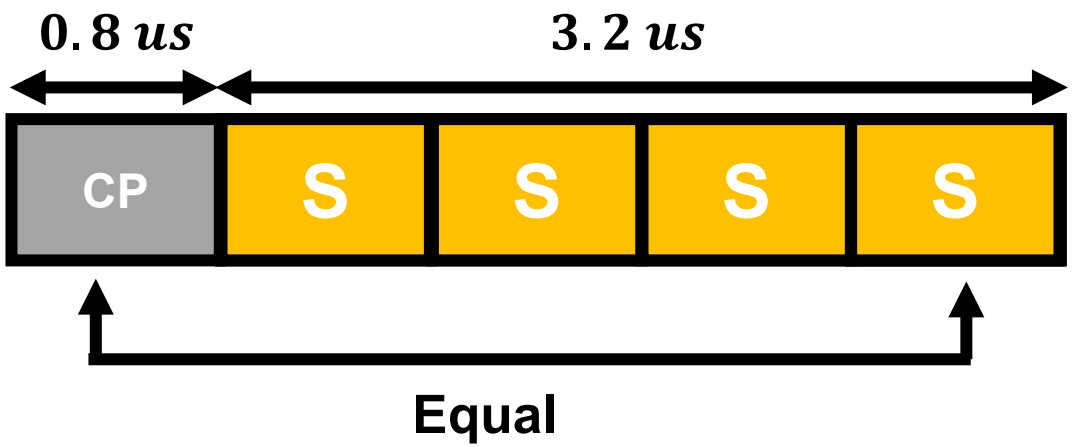
	Symbol format	Modulation
Header		BPSK/16 QAM
Payload		64 QAM

Addressing the discrepancy in the symbol format

5 x Short symbols
(in Header)



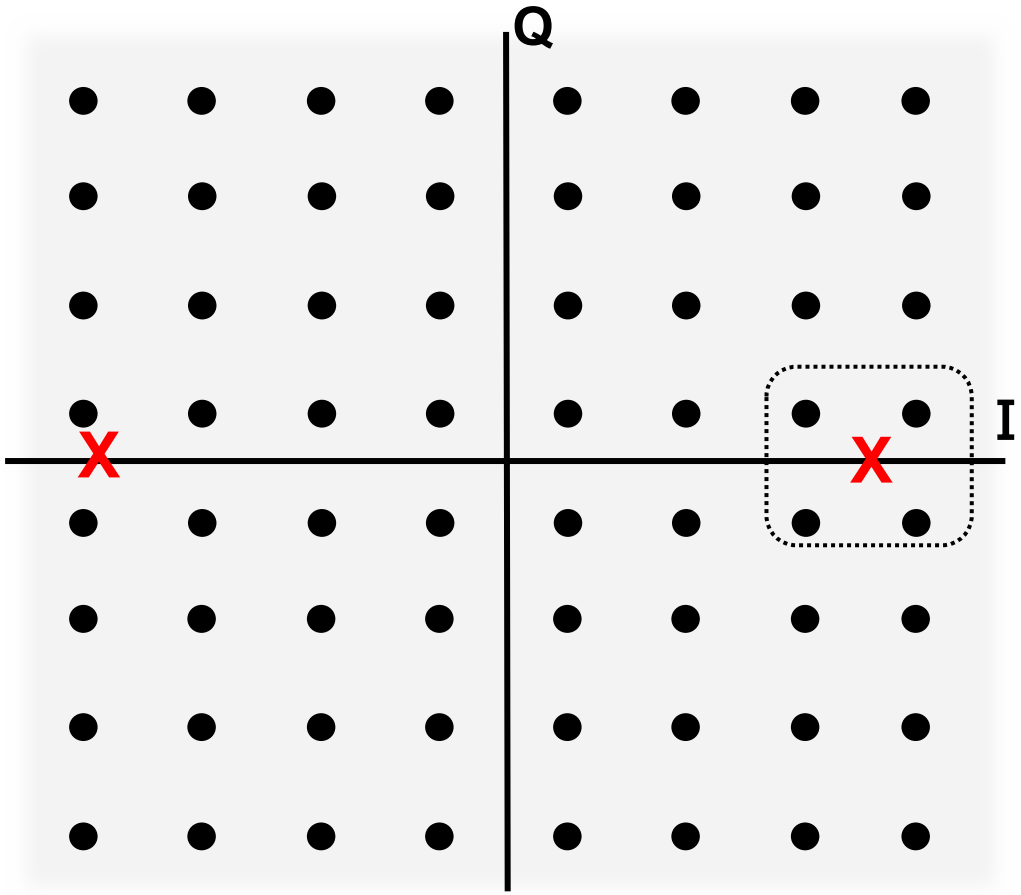
Payload Symbol

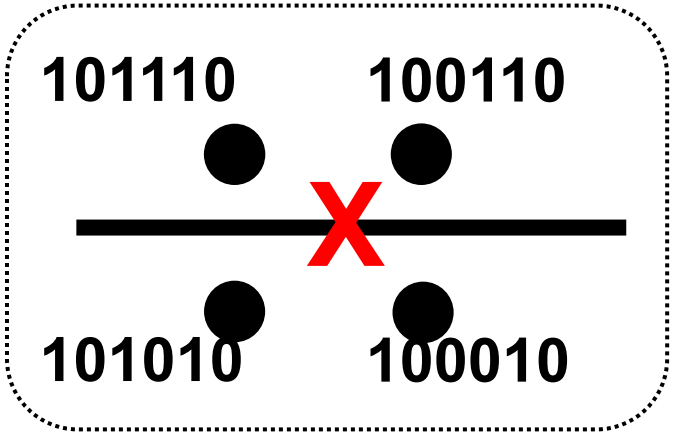


Subcarrier Constellation Mapping (Modulation)

- Encapsulated Packet (64 QAM)

X Long Symbol/PHY (BPSK)

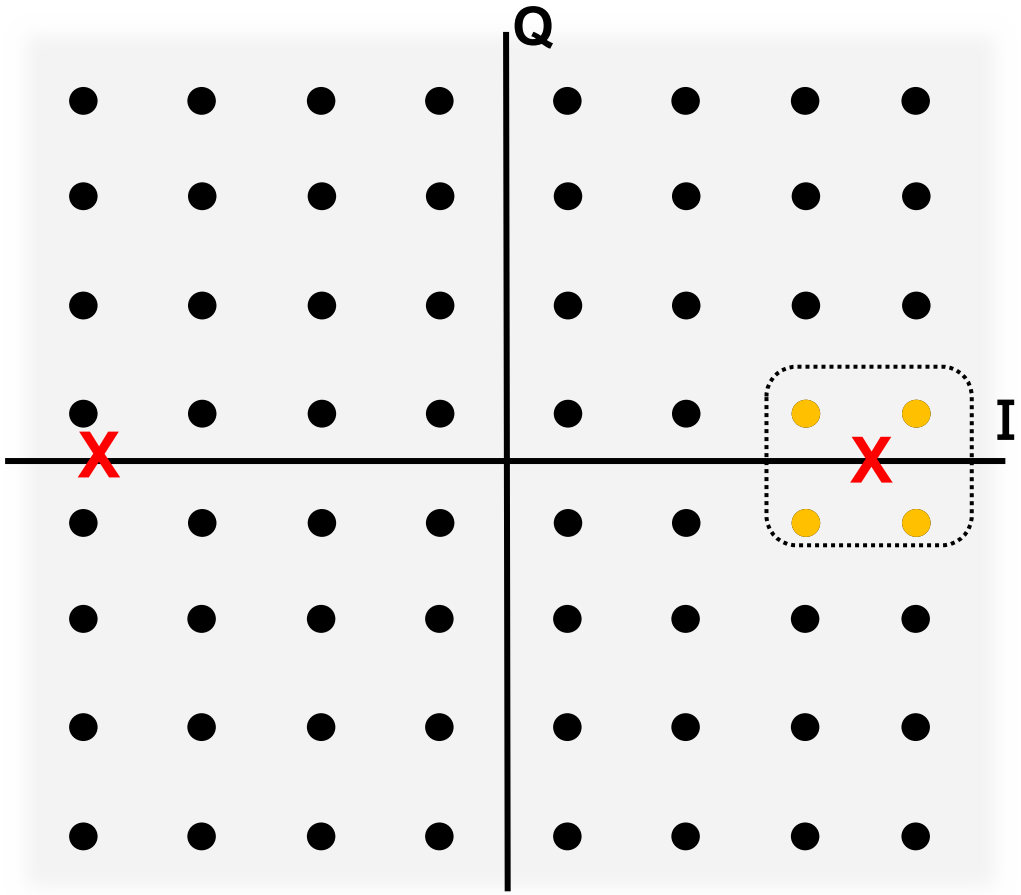


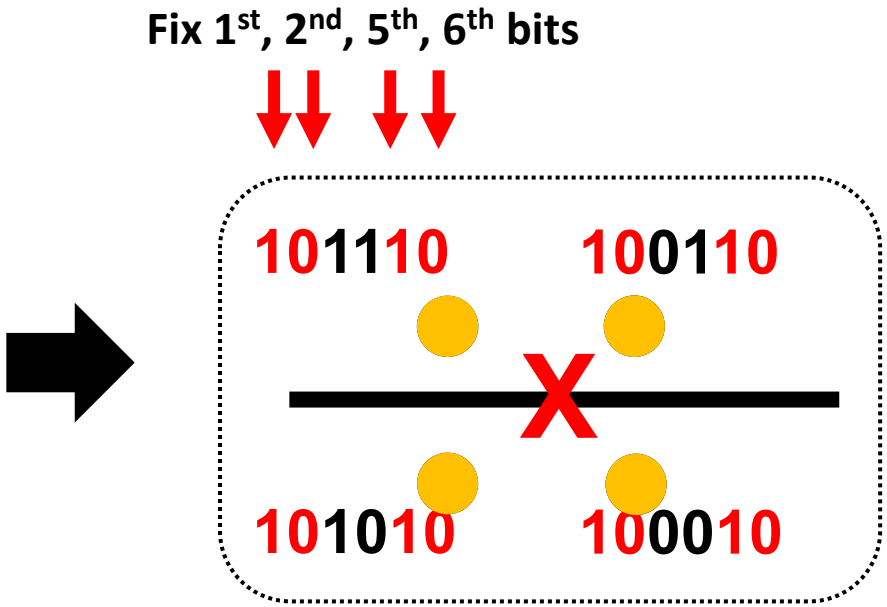


Subcarrier Constellation Mapping

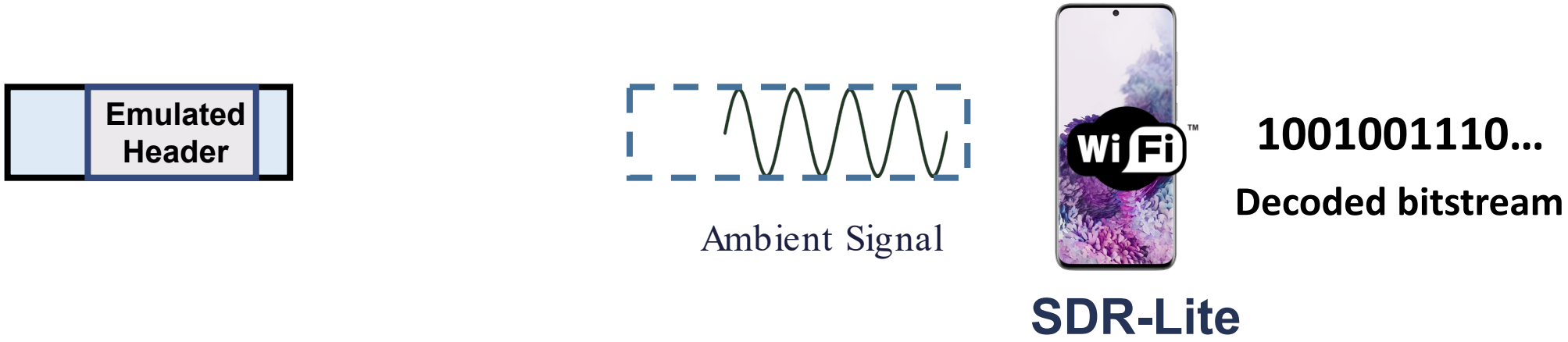
- Encapsulated Packet (64 QAM)

X Long Symbol/PHY (BPSK)





SDR-Lite receives an ambient signal



Reconstructing an ambient signal and enabling application

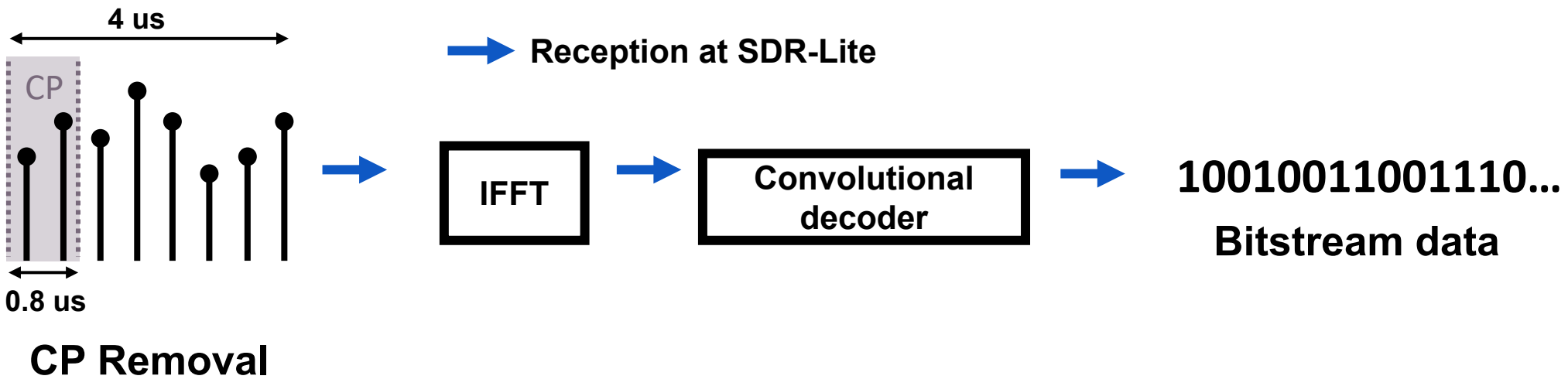
→ Software processing

SDR-Lite Design

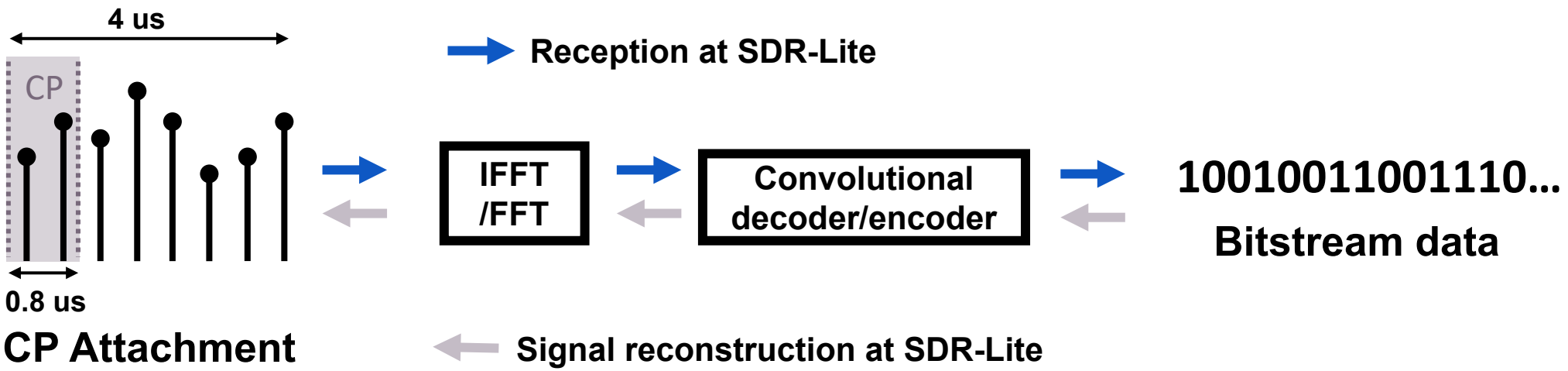
1. Receive ambient signal in the air

2. Software processing and applications

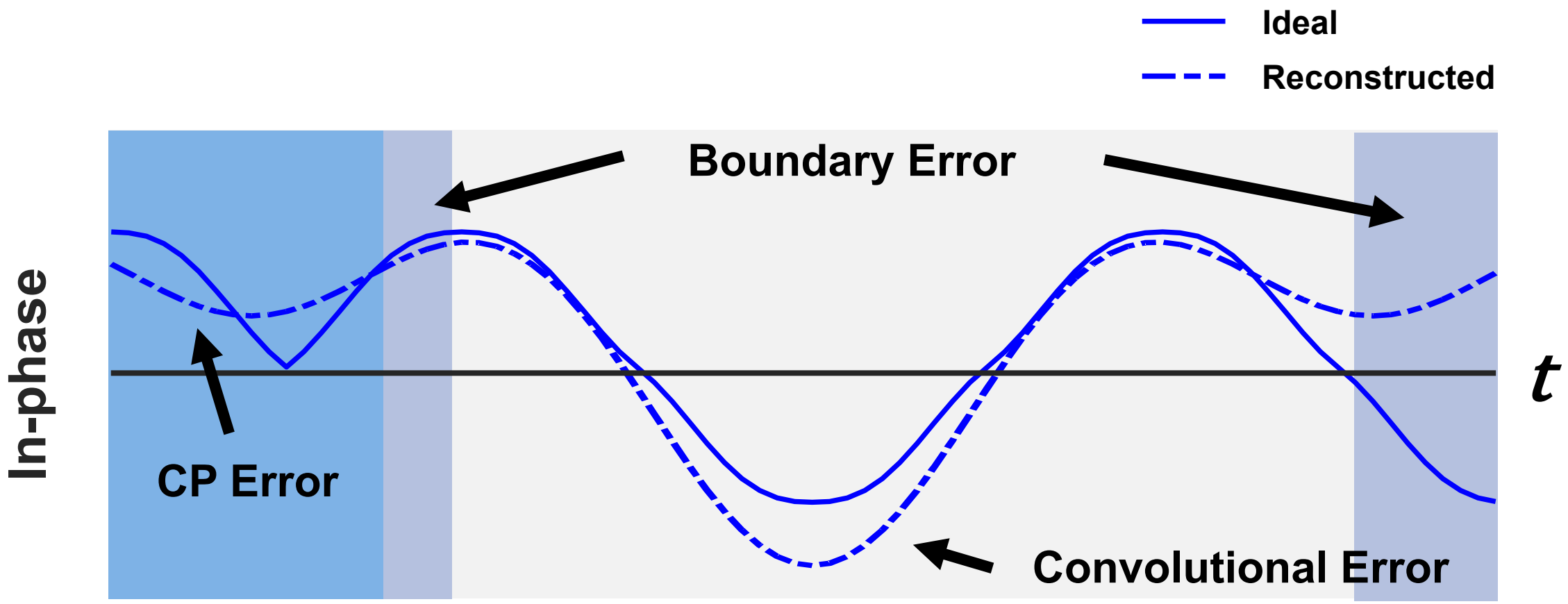
Reconstructing ambient signal from received bits



Reconstructing ambient signal from received bits



Reconstructed In-phase signal



Phase compensation through cross-correlation

Time-domain filtering

SDR-Lite Design

1. Receive ambient signal in the air

2. Software processing and applications

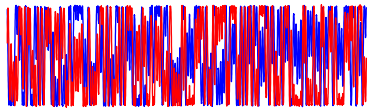
RF Fingerprinting

Spectrum Monitoring

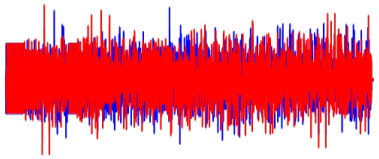
ZigBee Decoding

RF Fingerprinting

Reconstructed signal closely mimics the original ambient signal

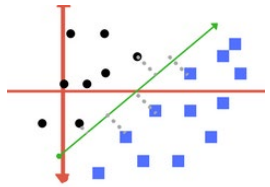


Drone

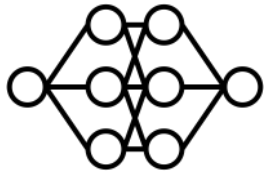


WiFi router

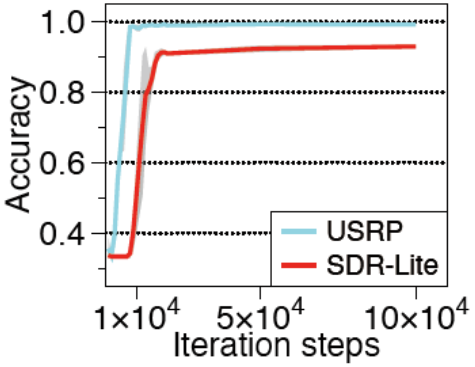
SDR-Lite



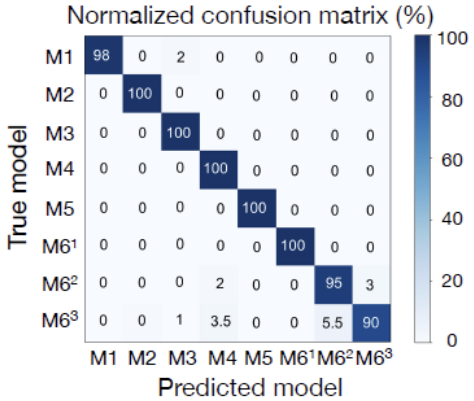
SVM



DNN



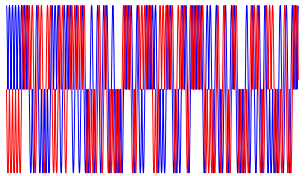
Drone Detection



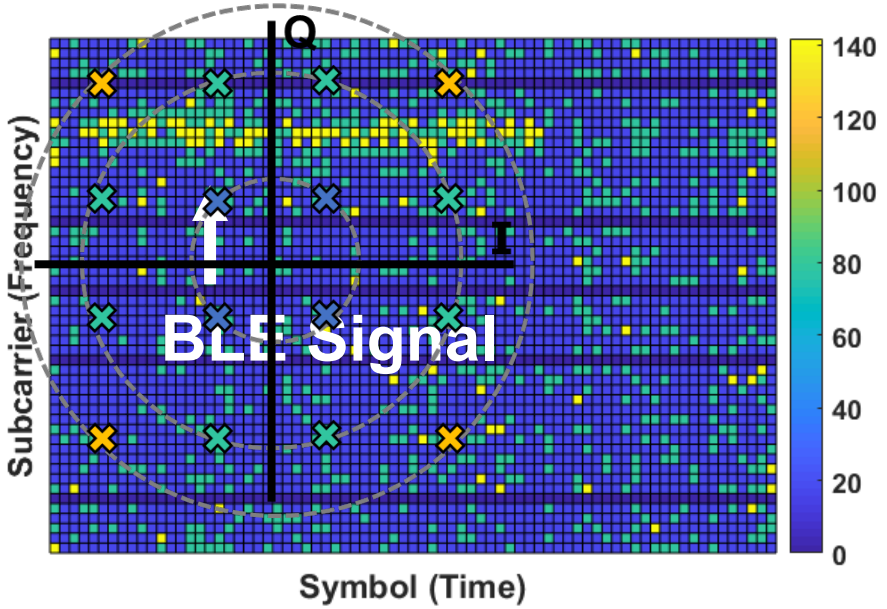
WiFi Device Identification

Spectrum Monitoring

Reconstructed signal could be used for spectrum analyzing



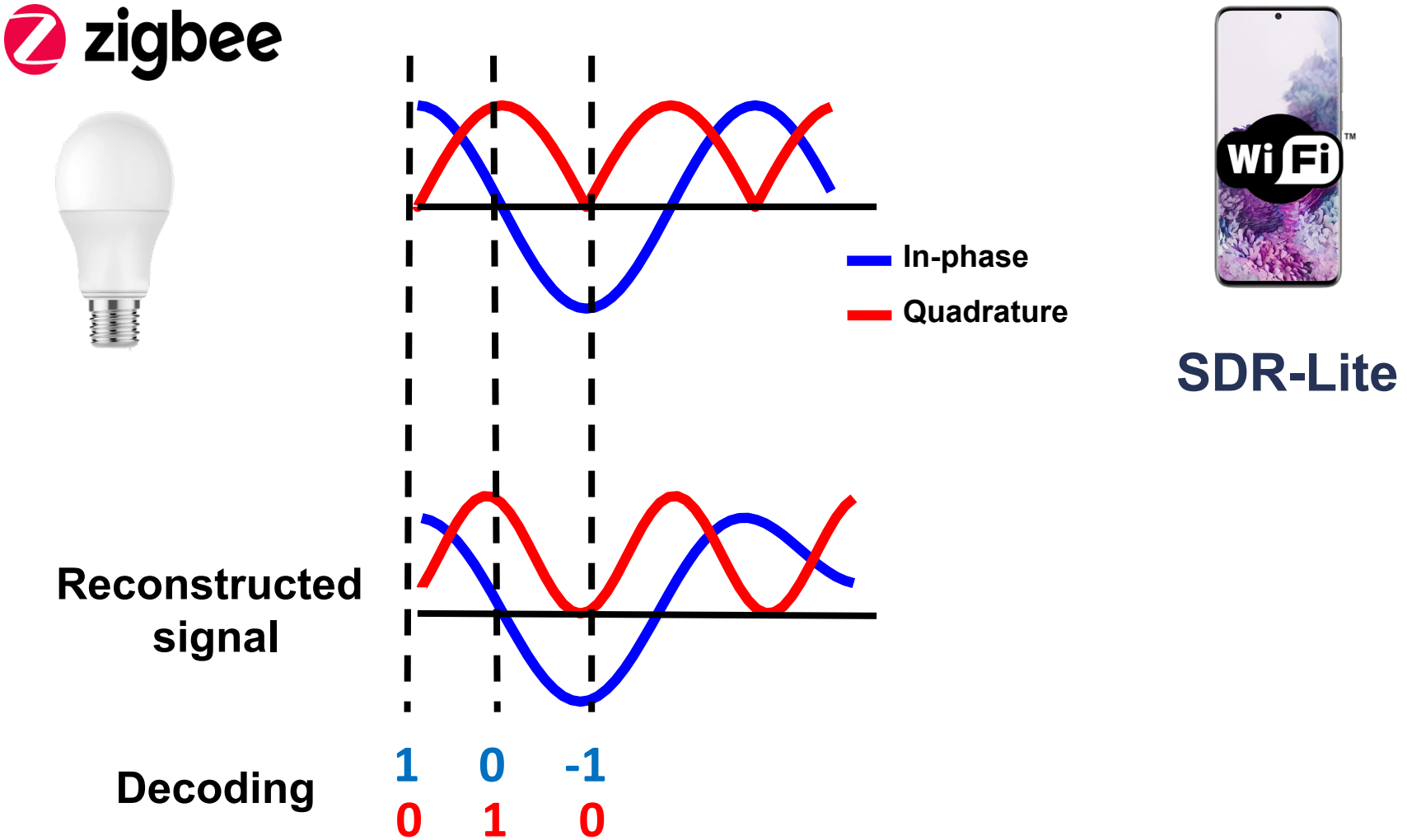
FFT



BLE device

SDR-Lite

ZigBee Decoding



Experiment Setup

AR 9380

Alfa AWUS036ACM

D-link DWA-192

USRP B210

(SDR-Lite)

Intel Aero

DJI Mavic pro

3DR Solo

TP-link Archer A7

TP-link WR841N

Netgear R7000

Honor View 10

iPad Pro

RC Car

Microwave

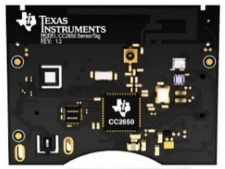
Raspberry Pi 0

Raspberry Pi 3

iPhone 5s

Moto G4

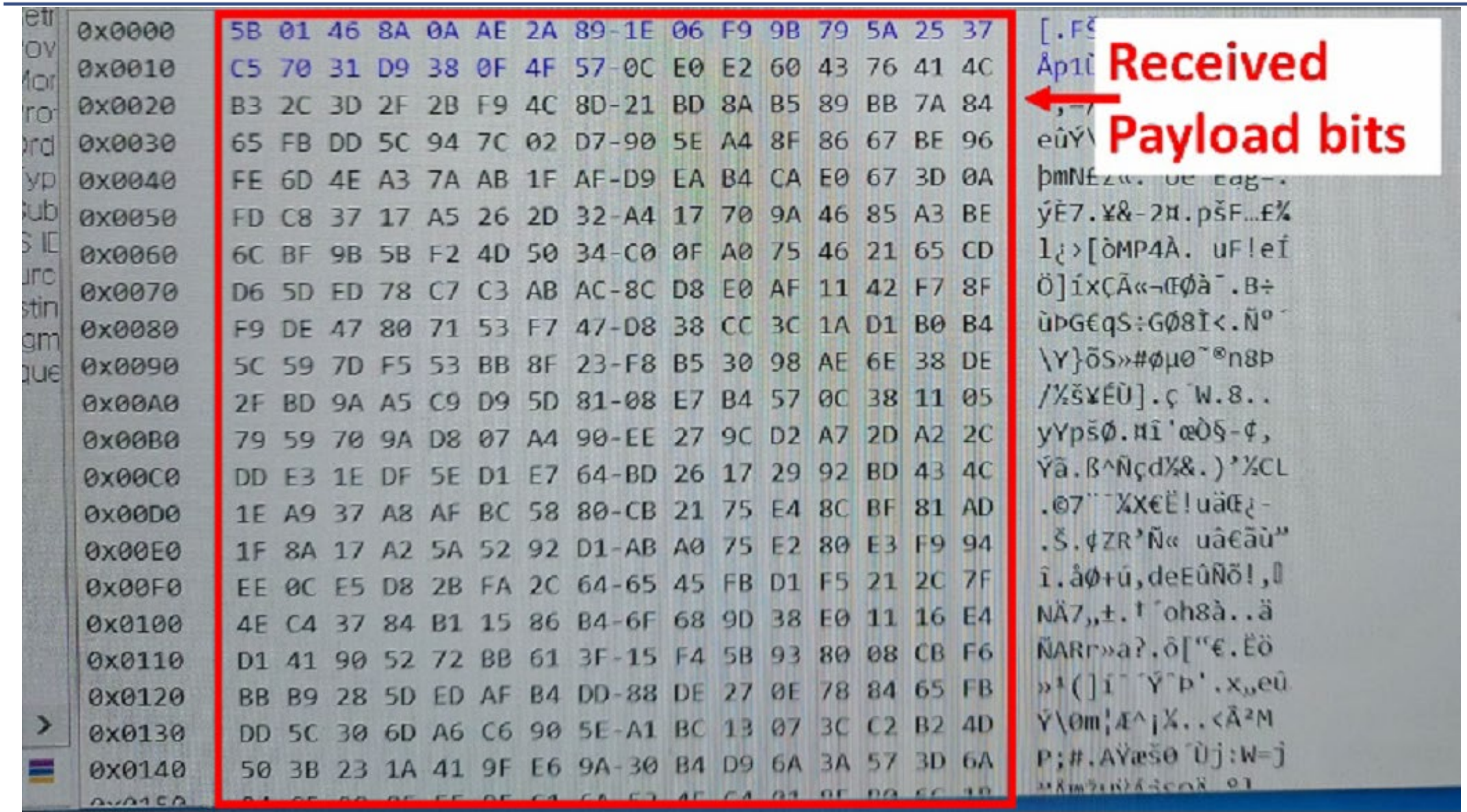
Xiaomi 8



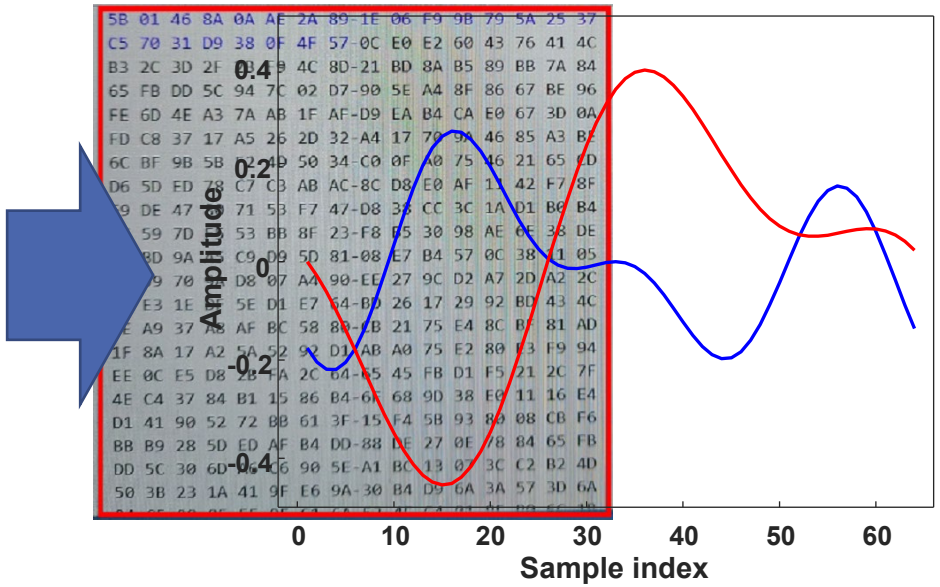
TI CC2650 (ZigBee & BLE)

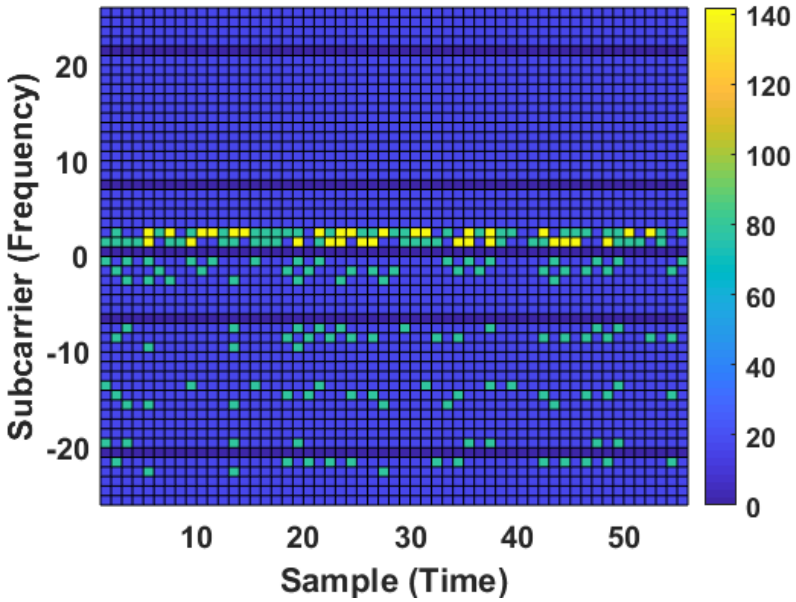
SDR-Lite in action

SDR-Lite in action



SDR-Lite in action





Received Payload bits

Reconstructed drone signal

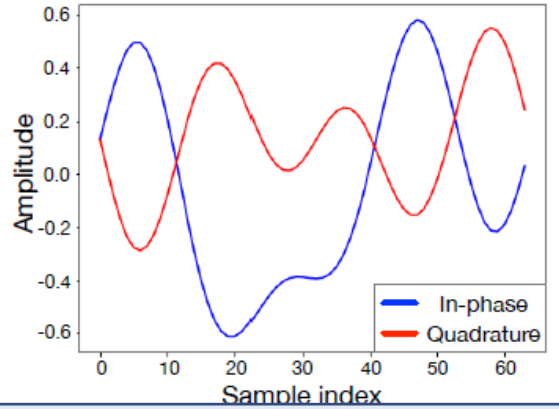
Waterfall

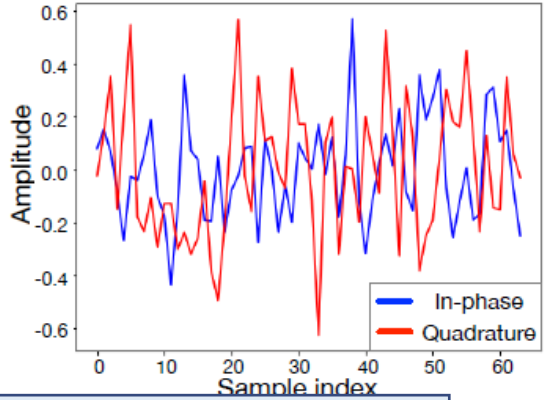
Can be used for unauthorized UAV detection

App. #1: Drone Detection

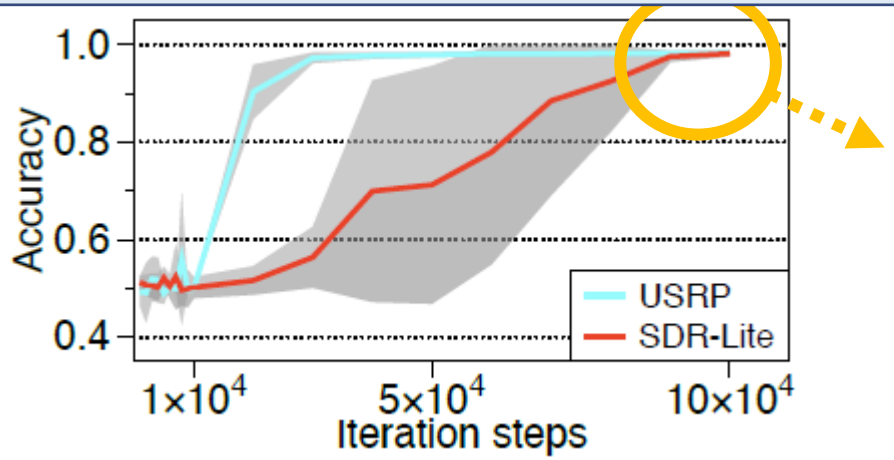
Intel Aero

DJI Mavic pro





SDR-Lite can detect drones' signal with high reliability

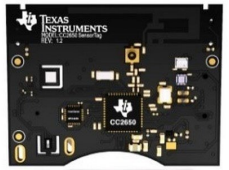


Accuracy

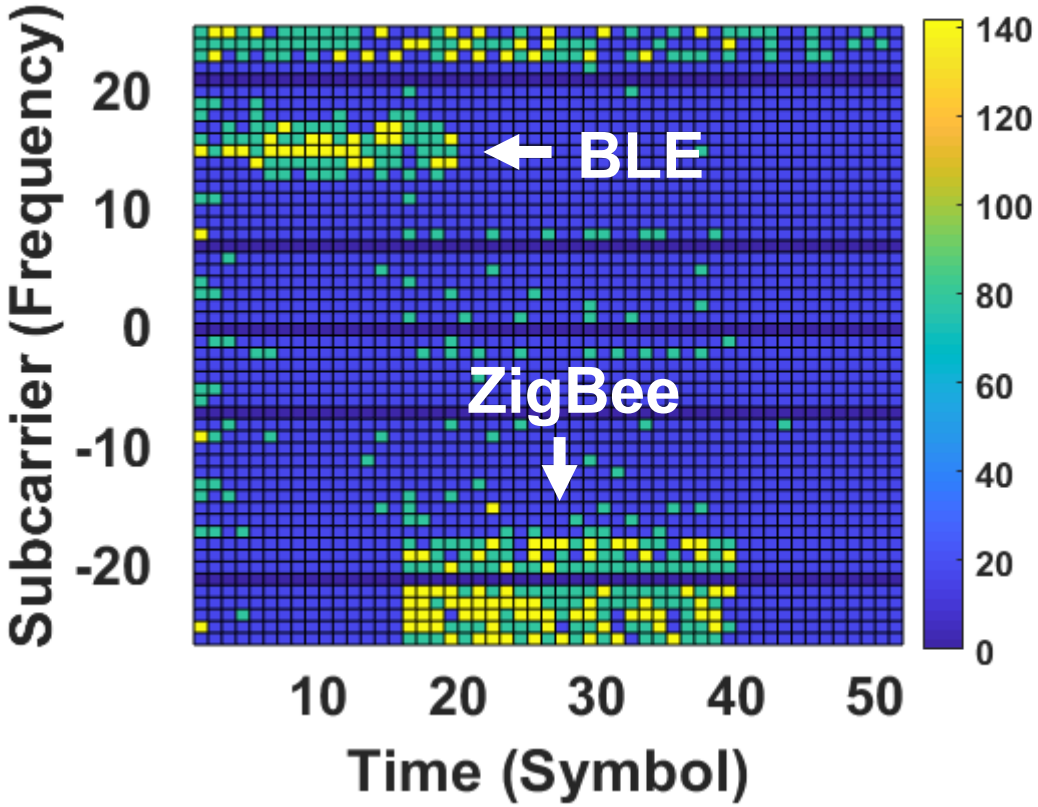
SDR-Lite: 98 %

USRP: 98.2 %

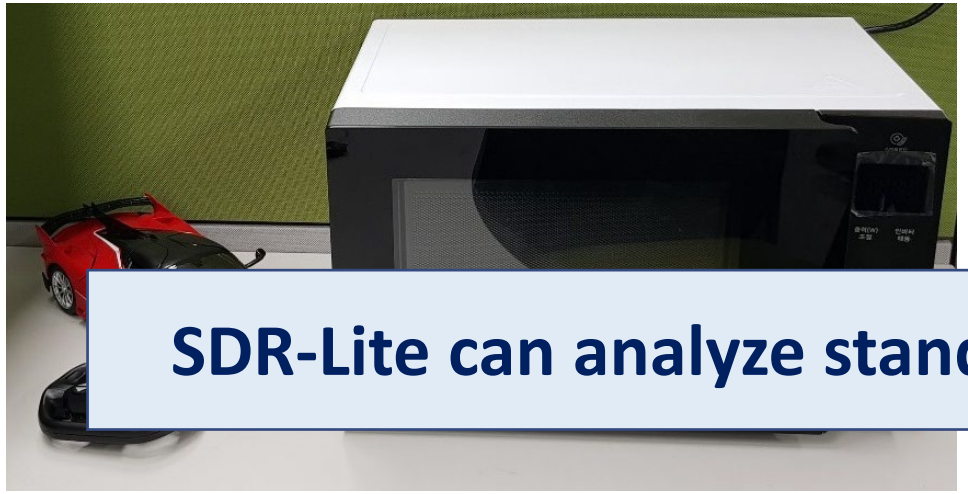
App #2 Spectrum Analysis: Standardized wireless signals



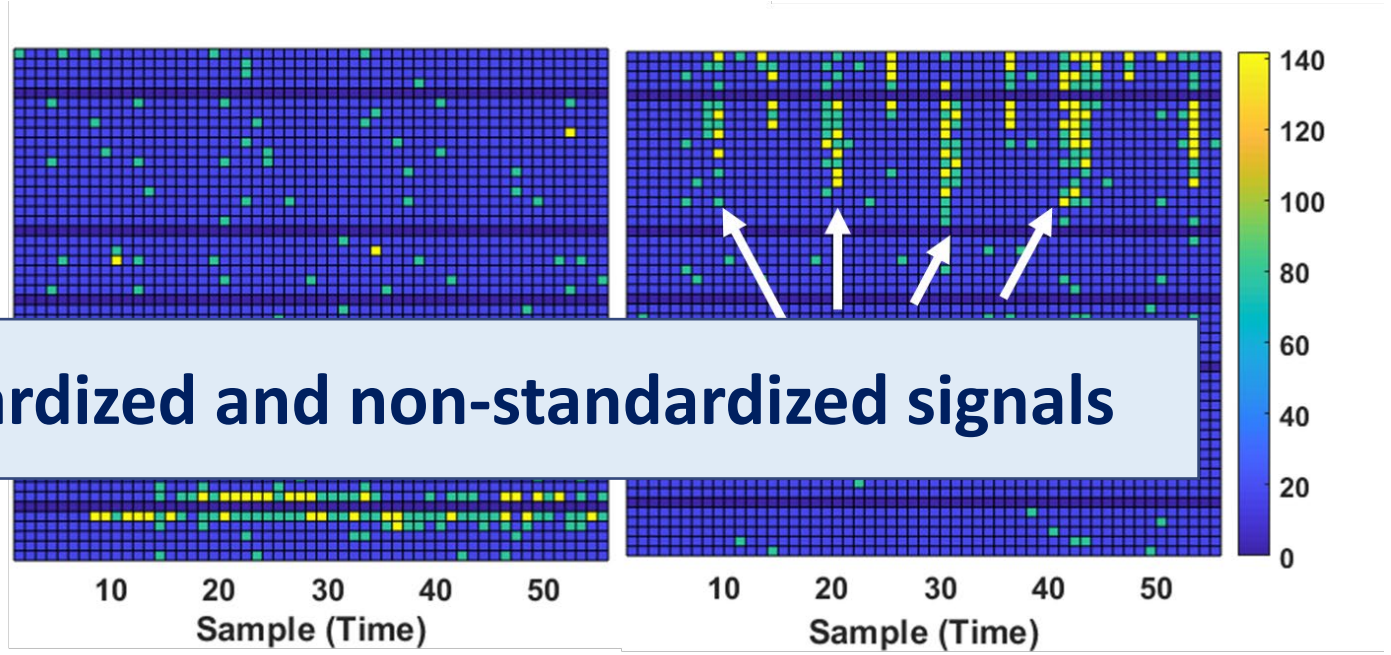
Bluetooth® zigbee



App#2 Spectrum Analysis: Non-standardized RF signals



RC car and microwave

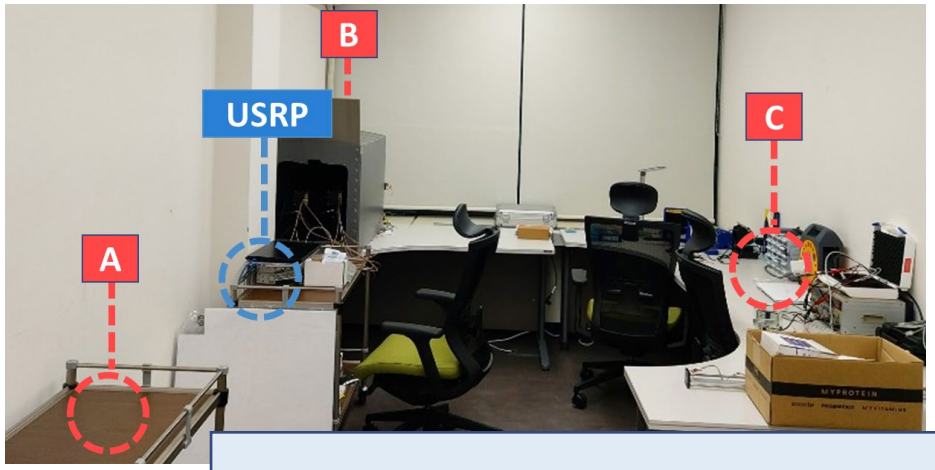


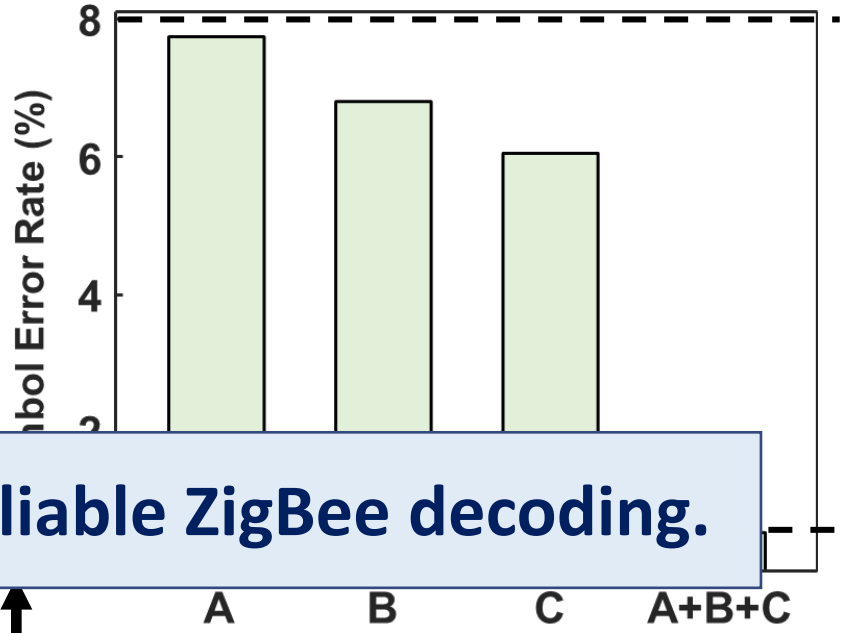
Radio Controlled Car

Microwave Oven

SDR-Lite can analyze standardized and non-standardized signals

App #3: ZigBee decoding

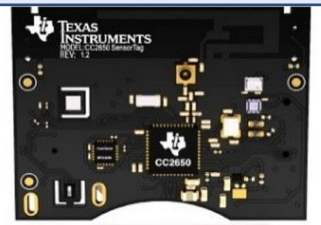




SDR-Lite enables high reliable ZigBee decoding.

Multiple SDR-Lite

zigbee



TI CC2650 (ZigBee & BLE)

Conclusion

- SDR-Lite is the first zero-cost and software-only SDR receiver built on commodity WiFi
- Ambient signal reception with emulated header and signal reconstruction
- Demonstrated three major applications:
  - Unauthorized UAV detection (Drone detection)
  - Network management (Spectrum monitoring)
  - IoT mobile data collection (ZigBee decoding)
- SDR-Lite spreads the blessing of SDR receiver to billions of WiFi devices and households to enhance our everyday lives

Thank you!