



# 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



# Everything is going wireless

---

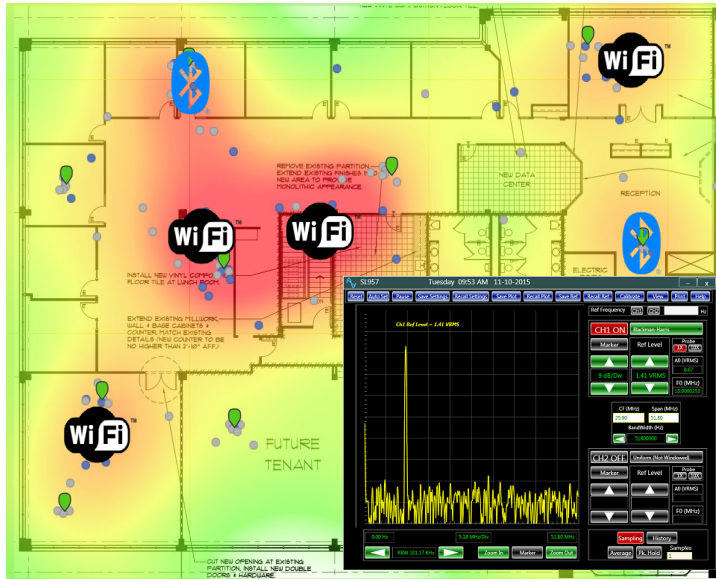


Wireless signals are increasing



PHY signal analysis is becoming more beneficial

# 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



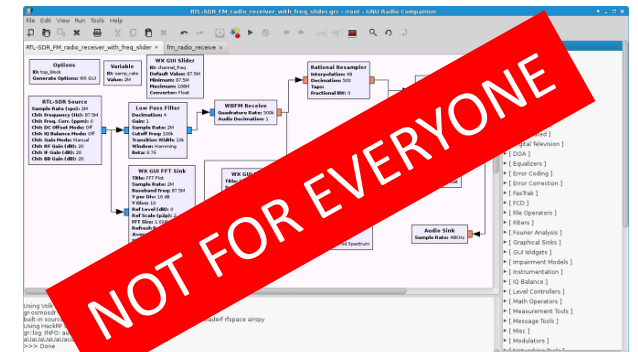
## 2. Software processing and applications



# SDR is rarely used



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



# SDR-Lite

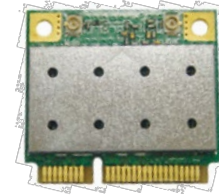
A new design to use commodity WiFi  
as a SDR receiver

# Beneficial WiFi

---

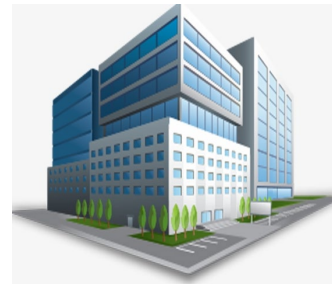


WNIC is Cheap



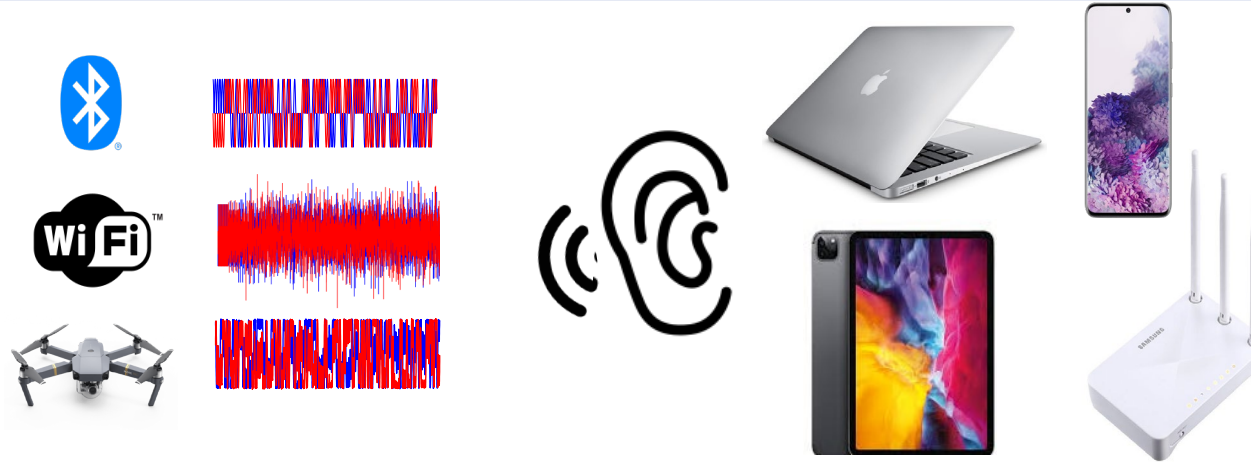
AR 9380: \$14

Billions of users

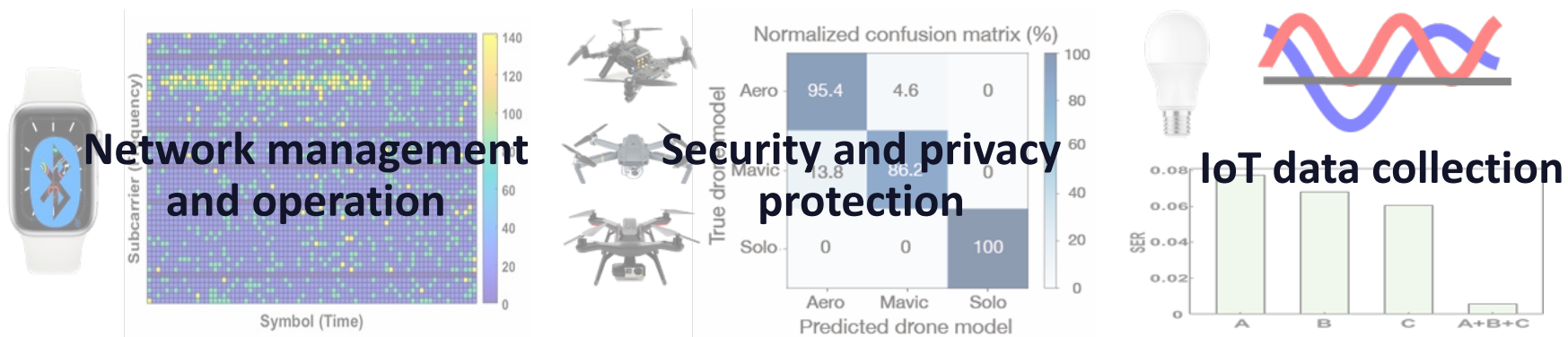


# SDR-Lite: SDR Receiver Using Commodity WiFi

## 1. Receive ambient signal in the air



## 2. Software processing and applications





# Design Overview

---

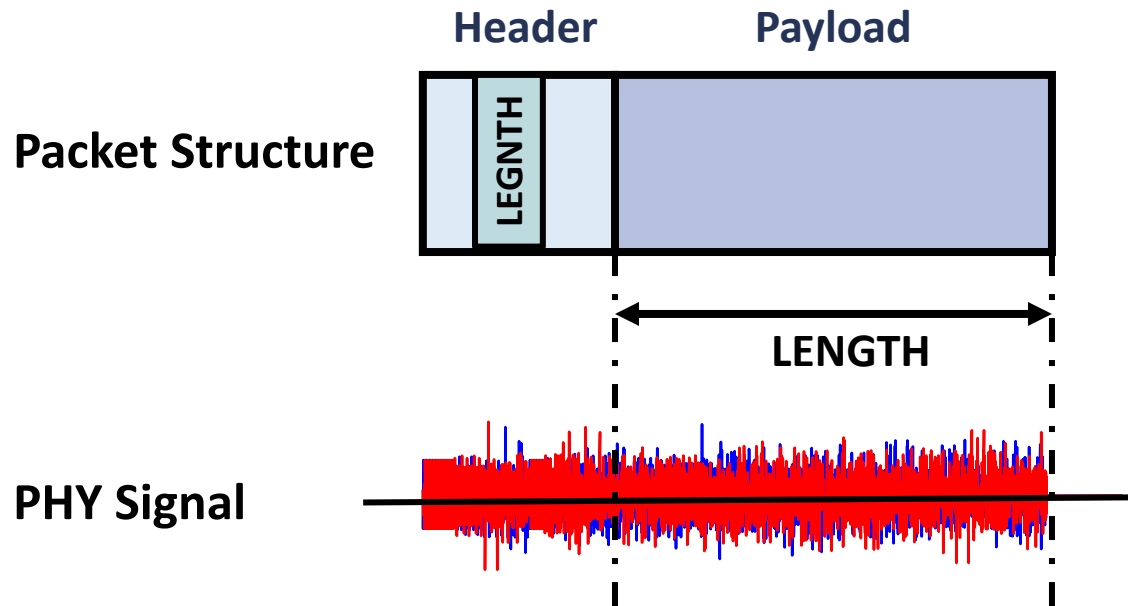
**1. Receive ambient signal in the air**

**2. Software processing and applications**



# Signal reception of typical WiFi

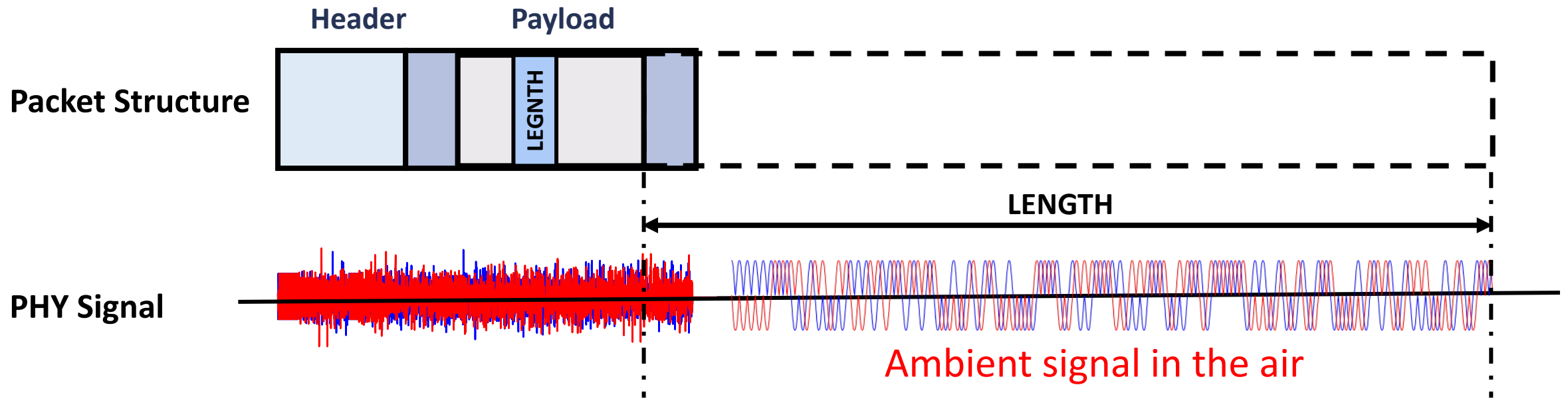
---



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

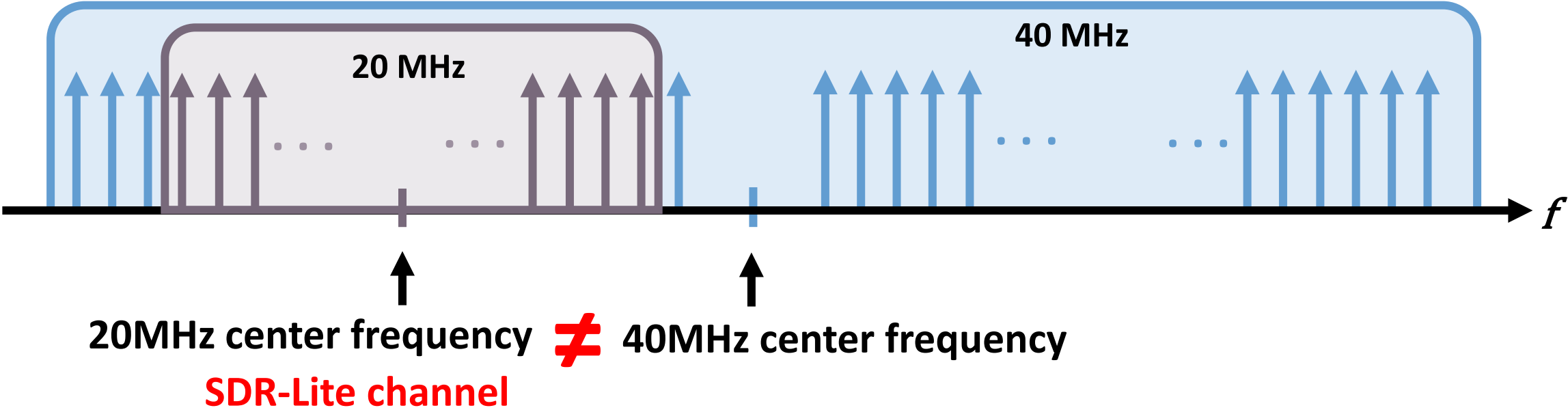


Challenge #2 : How can we emulate a new Header

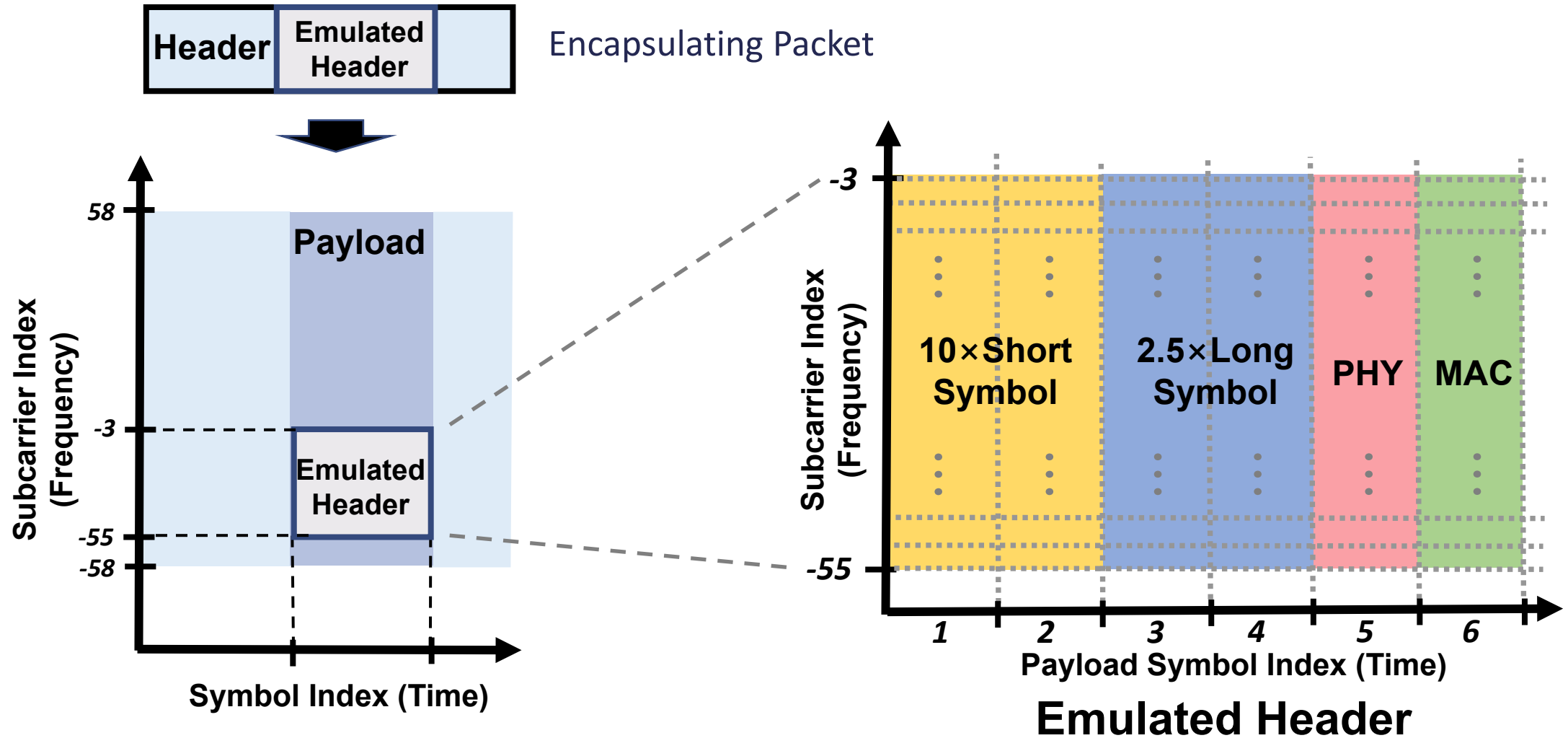
Generate an  
encapsulating packet

SDR-Lite

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

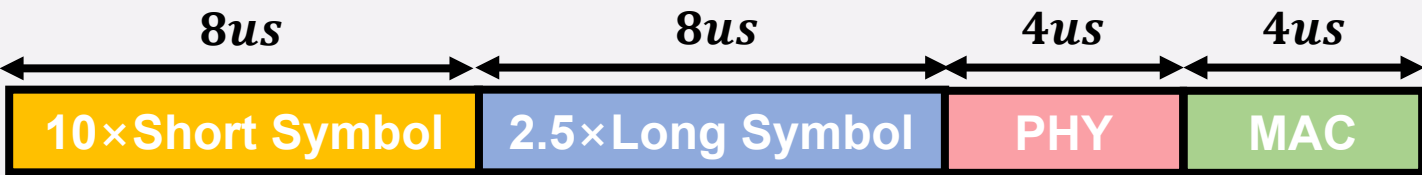
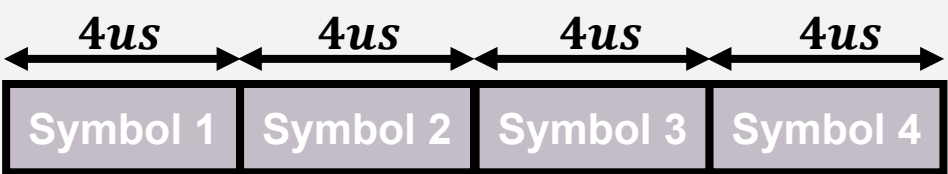


# Challenge #2 : How can we generate an emulated Header



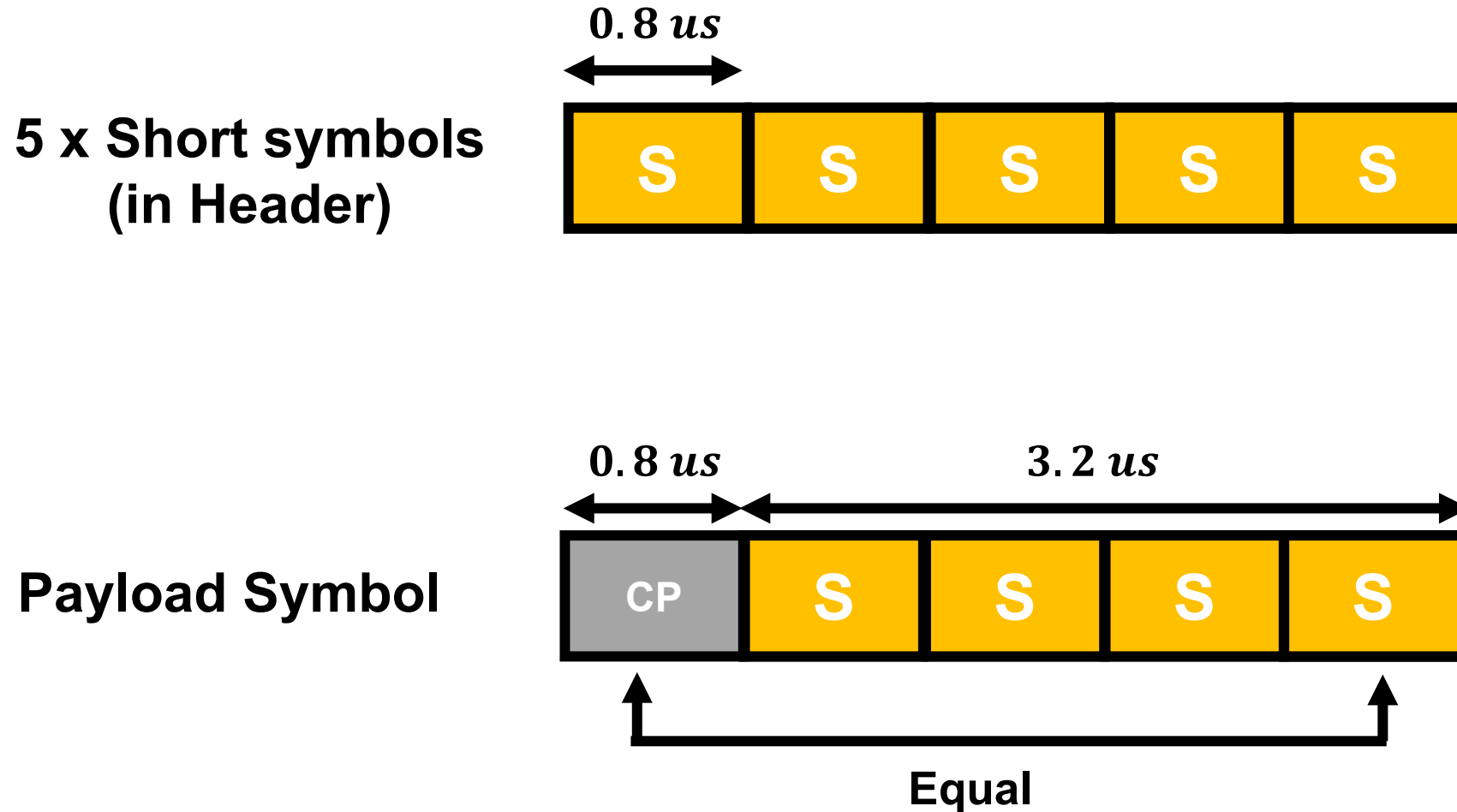
# Header emulation using Payload

---

	Symbol format	Modulation
Header		BPSK/16 QAM
Payload		64 QAM

# Addressing the discrepancy in the symbol format

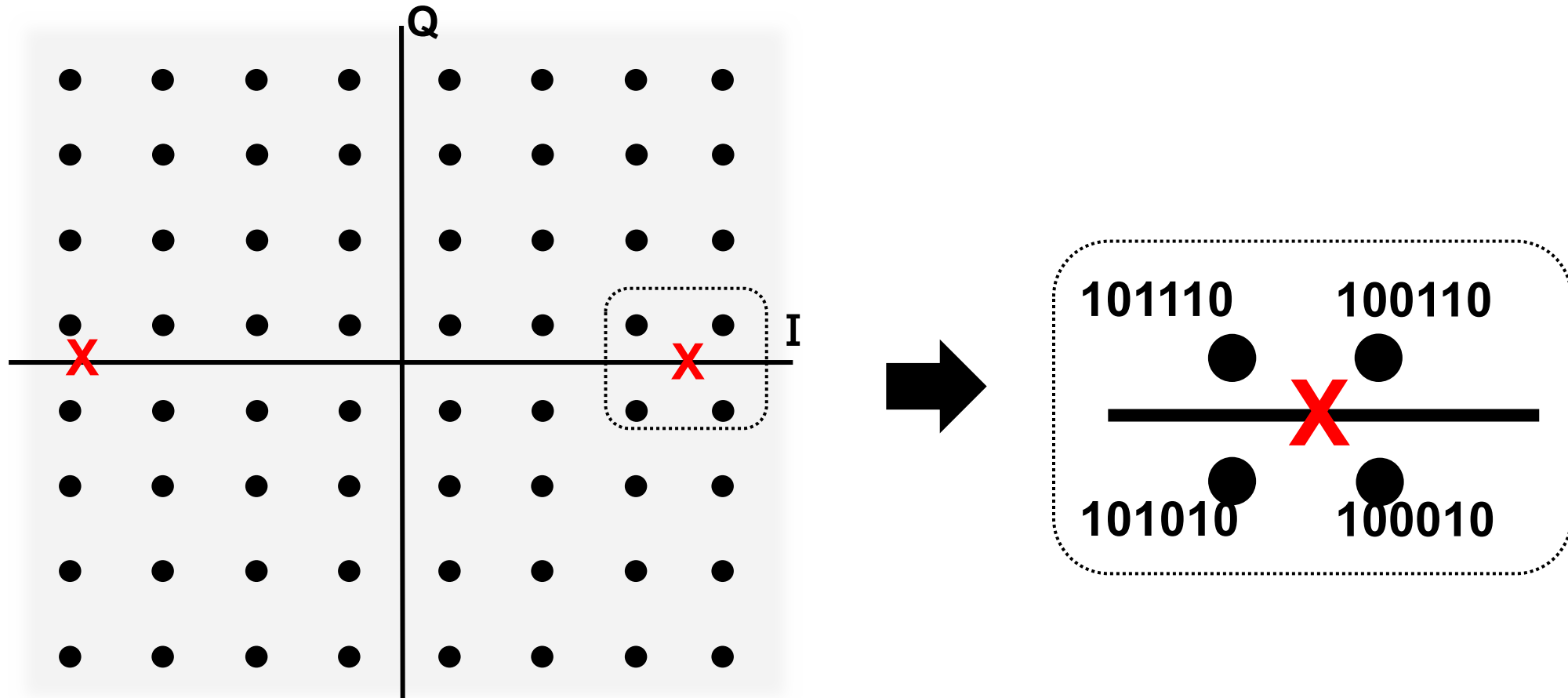
---





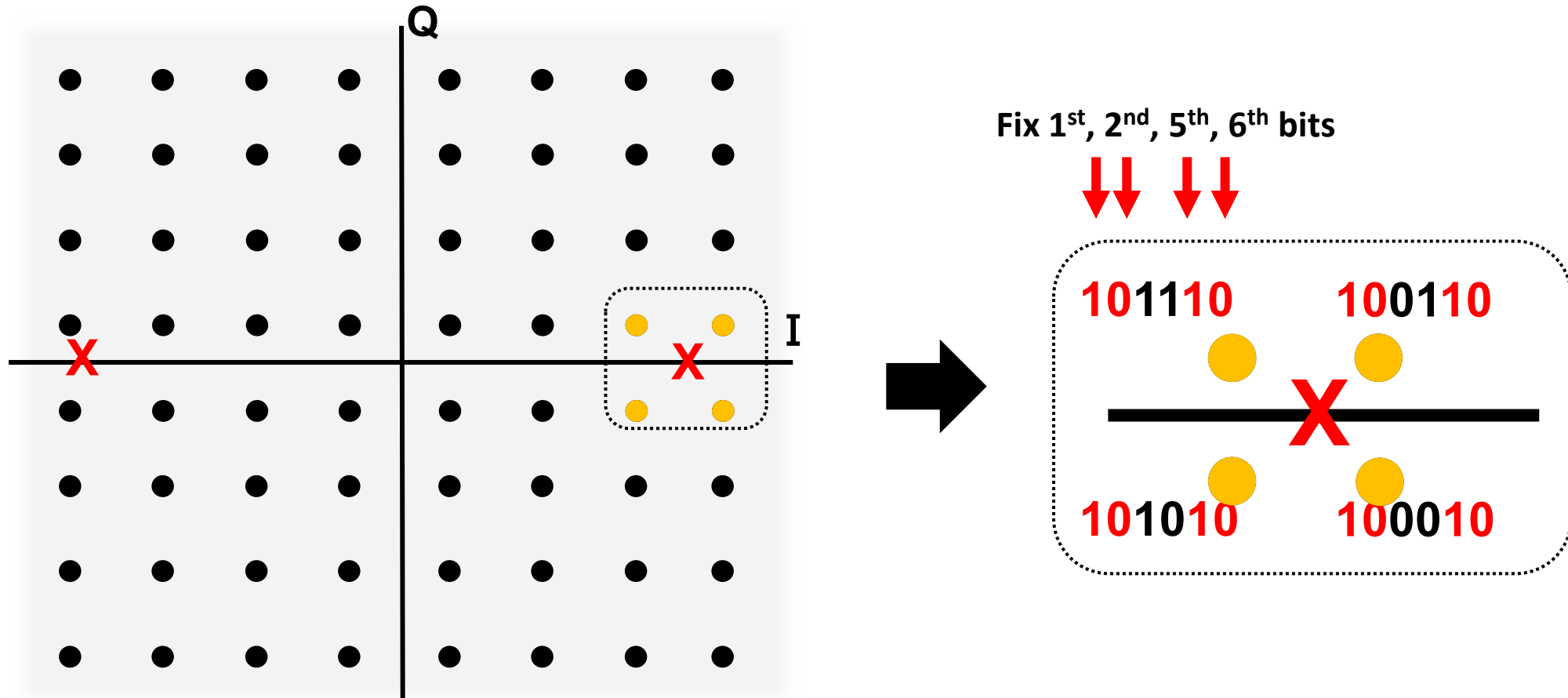
# Subcarrier Constellation Mapping (Modulation)

- Encapsulated Packet (64 QAM)      **X** Long Symbol/PHY (BPSK)



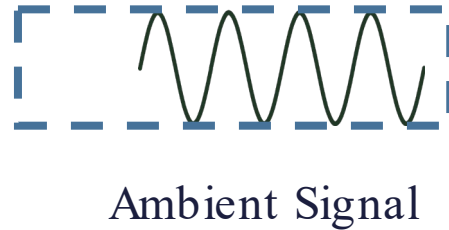
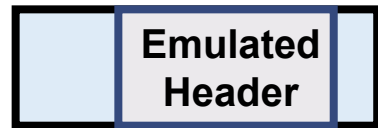
# Subcarrier Constellation Mapping

- Encapsulated Packet (64 QAM)
- **X** Long Symbol/PHY (BPSK)



# SDR-Lite receives an ambient signal

---



**1001001110...**  
**Decoded bitstream**

**SDR-Lite**

Reconstructing an ambient signal and enabling application  
→ Software processing

# SDR-Lite Design

---

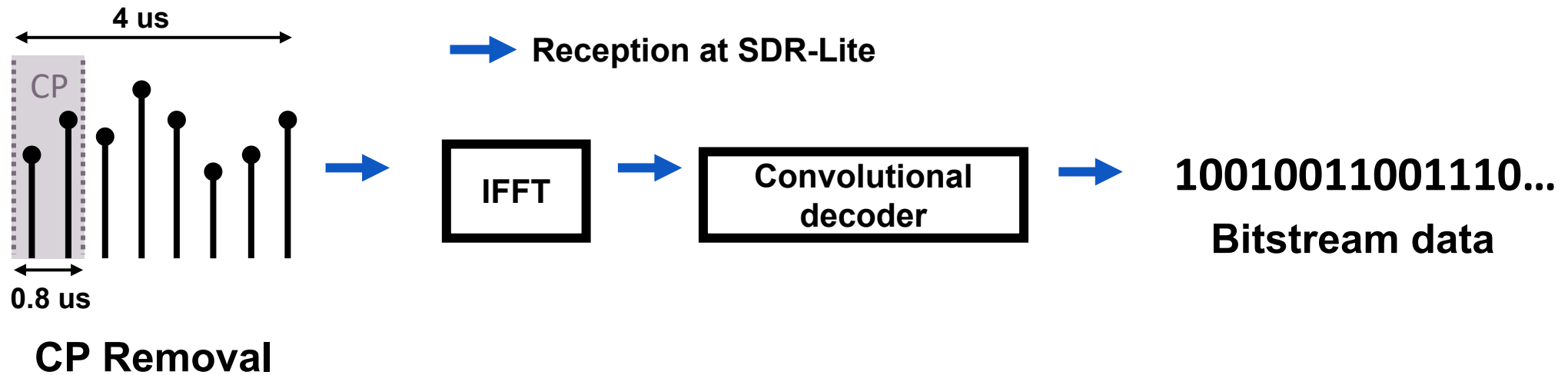
**1. Receive ambient signal in the air**

**2. Software processing and applications**



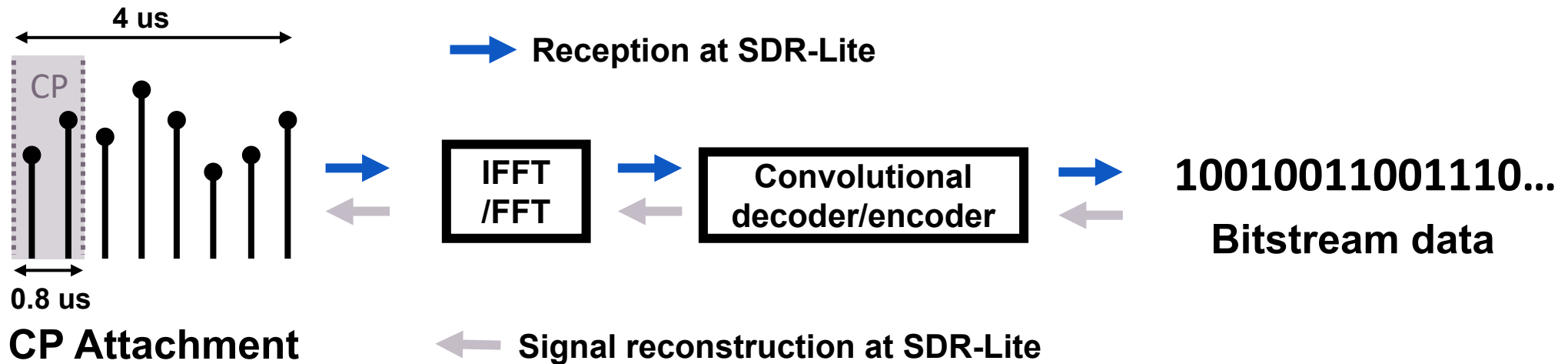
# Reconstructing ambient signal from received bits

---

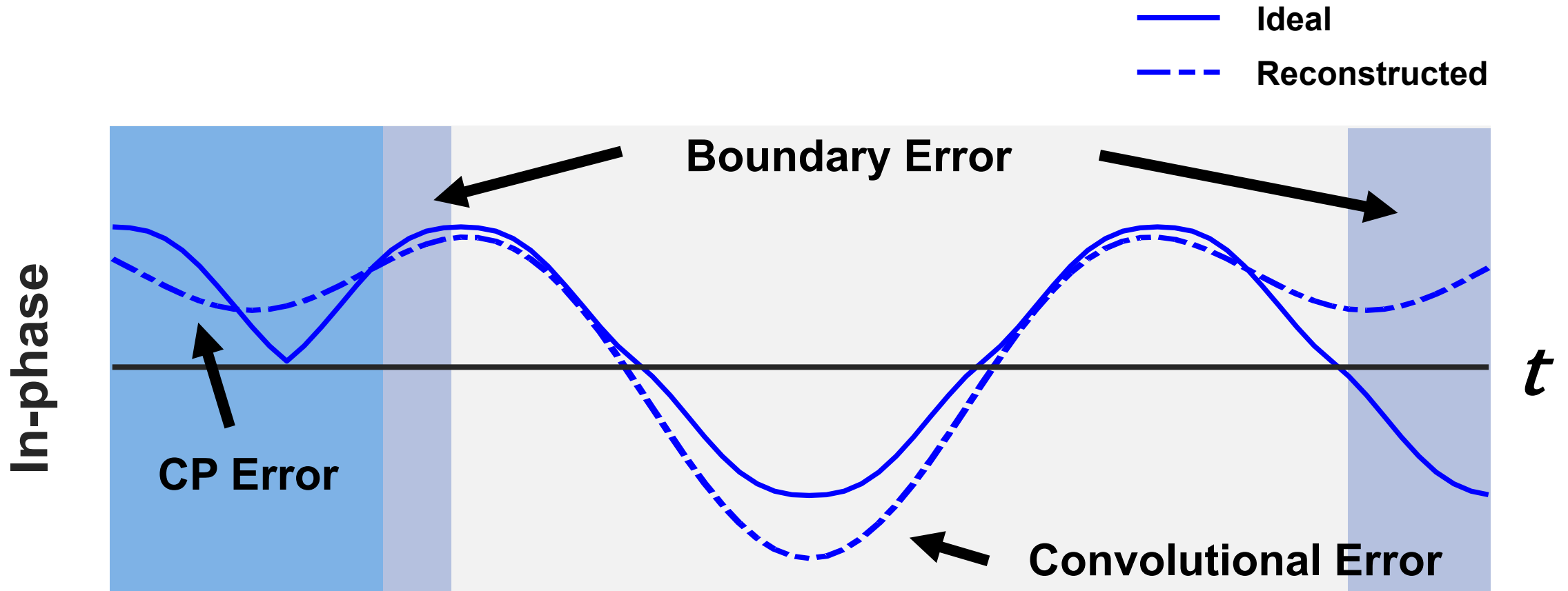


# Reconstructing ambient signal from received bits

---



# 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**



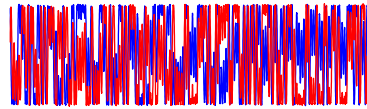


# RF Fingerprinting

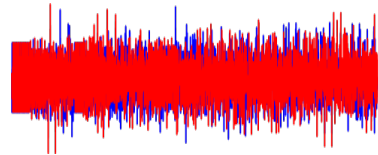
Reconstructed signal closely mimics the original ambient signal



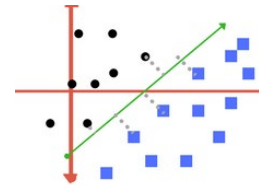
Drone



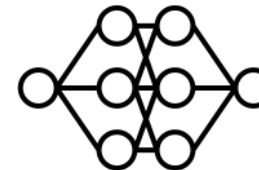
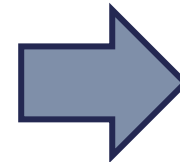
WiFi router



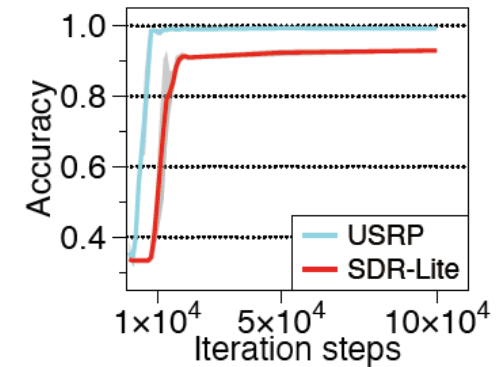
SDR-Lite



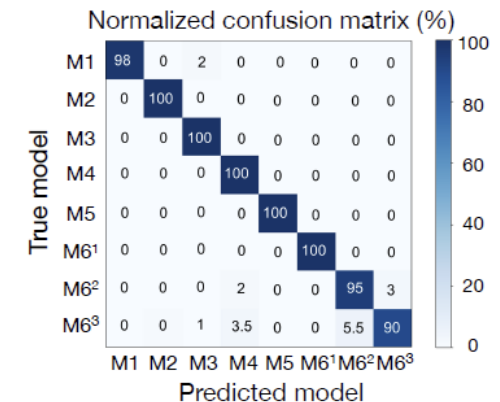
SVM



DNN



Drone Detection



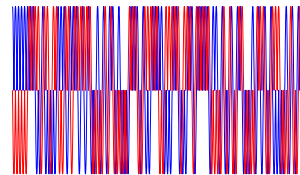
WiFi Device Identification

# Spectrum Monitoring

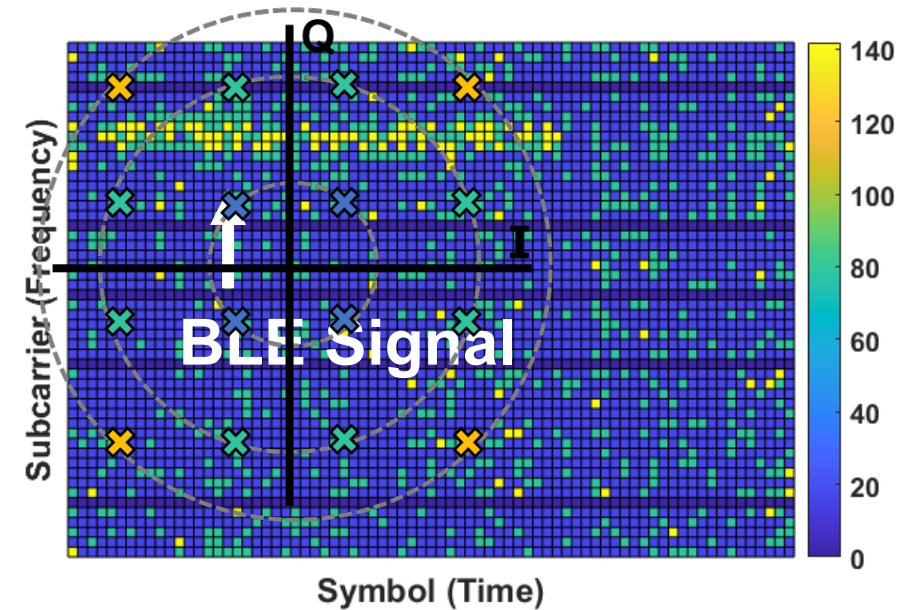
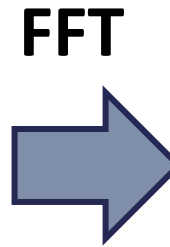
Reconstructed signal could be used for spectrum analyzing



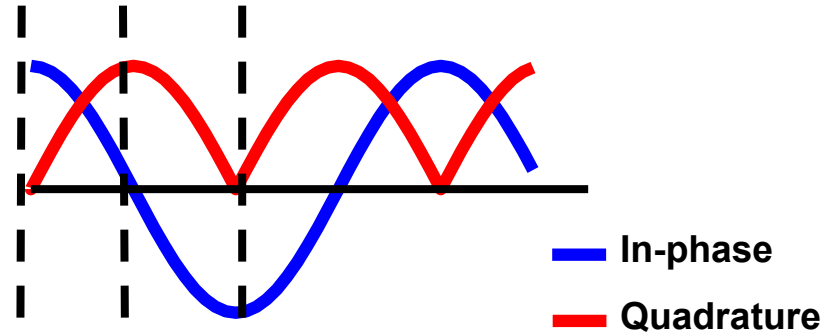
BLE device



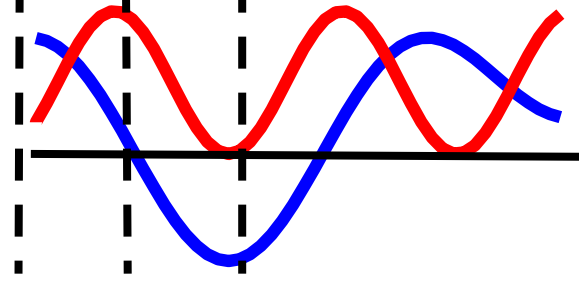
SDR-Lite



# ZigBee Decoding



Reconstructed  
signal



Decoding

1	0	-1
0	1	0



SDR-Lite

# 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



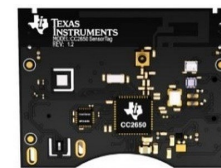
iPhone 5s



Moto G4



Xiaomi 8



TI CC2650 (ZigBee & BLE)

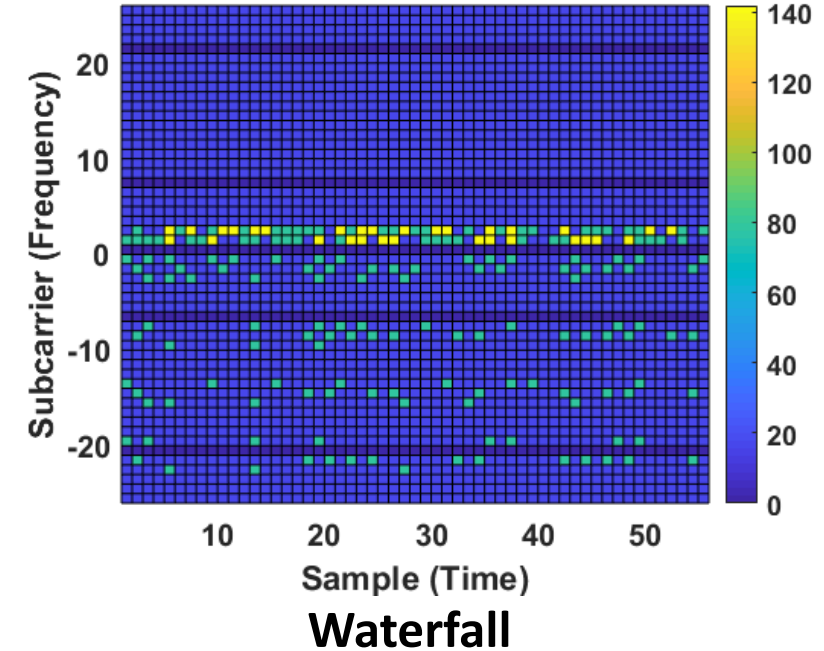
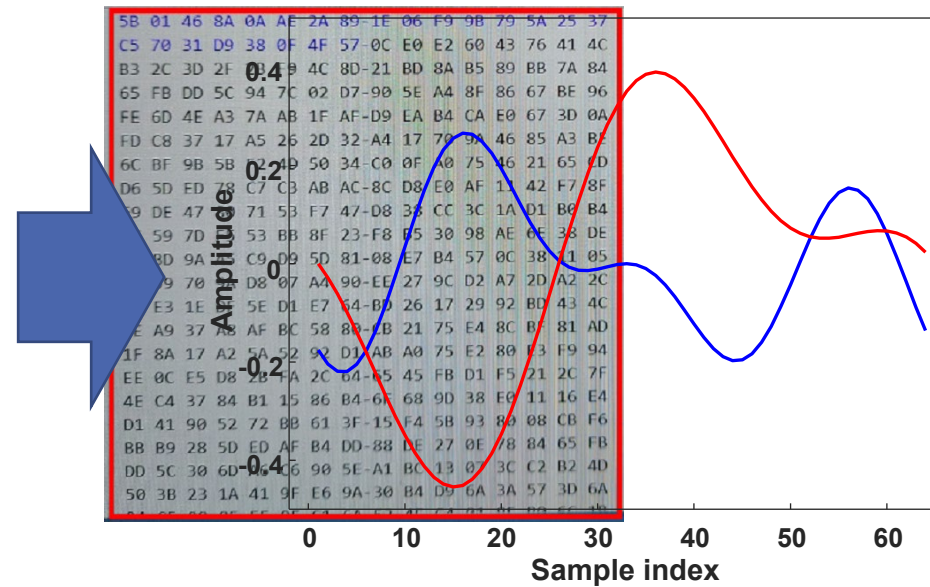
# SDR-Lite in action



# SDR-Lite in action

0x0000	5B 01 46 8A 0A AE 2A 89-1E 06 F9 9B 79 5A 25 37	[.FÉ
0x0010	C5 70 31 D9 38 0F 4F 57-0C E0 E2 60 43 76 41 4C	Äp1i
0x0020	B3 2C 3D 2F 2B F9 4C 8D-21 BD 8A B5 89 BB 7A 84	←
0x0030	65 FB DD 5C 94 7C 02 D7-90 5E A4 8F 86 67 BE 96	eüY\
0x0040	FE 6D 4E A3 7A AB 1F AF-D9 EA B4 CA E0 67 3D 0A	pmNÉzæ. be eag-
0x0050	FD C8 37 17 A5 26 2D 32-A4 17 70 9A 46 85 A3 BE	ÿË7.¥&-2µ.pšF..f%
0x0060	6C BF 9B 5B F2 4D 50 34-C0 0F A0 75 46 21 65 CD	lç>[òMP4À. uF!eİ
0x0070	D6 5D ED 78 C7 C3 AB AC-8C D8 E0 AF 11 42 F7 8F	Ö]ixCÃ«-æøà~.B÷
0x0080	F9 DE 47 80 71 53 F7 47-D8 38 CC 3C 1A D1 B0 B4	ùpG€qS:Gø8İ<.Ñ°
0x0090	5C 59 7D F5 53 BB 8F 23-F8 B5 30 98 AE 6E 38 DE	\Y}õS»#øµø~°n8p
0x00A0	2F BD 9A A5 C9 D9 5D 81-08 E7 B4 57 0C 38 11 05	/%š¥ÉÛ].ç`w.8..
0x00B0	79 59 70 9A D8 07 A4 90-EE 27 9C D2 A7 2D A2 2C	yYpšø.ñî'æòš-ç,
0x00C0	DD E3 1E DF 5E D1 E7 64-BD 26 17 29 92 BD 43 4C	ÿã.ß^Ñçd%&.)'¼CL
0x00D0	1E A9 37 A8 AF BC 58 80-CB 21 75 E4 8C BF 81 AD	.ø7`~%X€Ë!uäæç-
0x00E0	1F 8A 17 A2 5A 52 92 D1-AB A0 75 E2 80 E3 F9 94	.š.çZR'Ñ« uâeãü"
0x00F0	EE 0C E5 D8 2B FA 2C 64-65 45 FB D1 F5 21 2C 7F	î.âø+ú,deEûÑö!,
0x0100	4E C4 37 84 B1 15 86 B4-6F 68 9D 38 E0 11 16 E4	NÄ7,,±.†`oh8à..ä
0x0110	D1 41 90 52 72 BB 61 3F-15 F4 5B 93 80 08 CB F6	ÑARR»a?,.ø["€..Ëö
0x0120	BB B9 28 5D ED AF B4 DD-88 DE 27 0E 78 84 65 FB	»†(]i`~ÿ~p'.x,øeü
0x0130	DD 5C 30 6D A6 C6 90 5E-A1 BC 13 07 3C C2 B2 4D	ÿ\øm!æ^j%.<Ã²M
0x0140	50 3B 23 1A 41 9F E6 9A-30 B4 D9 6A 3A 57 3D 6A	P;#.AYæšø`Ûj:W=j
0x0150	01 0F 00 0F 0F 0F 01 0A 03 0F 0A 01 0F 00 00 10	MÄm?ü?äçøä`ø!

# SDR-Lite in action



Can be used for unauthorized UAV detection

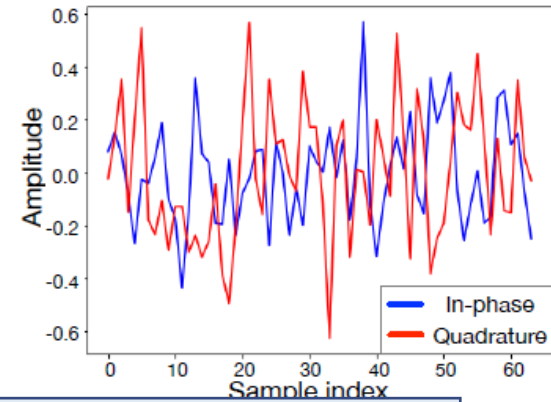
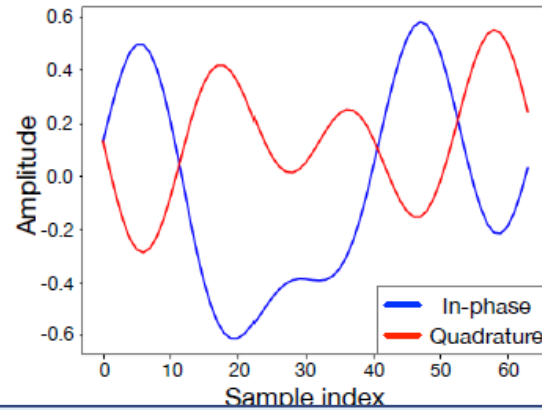
# App. #1: Drone Detection



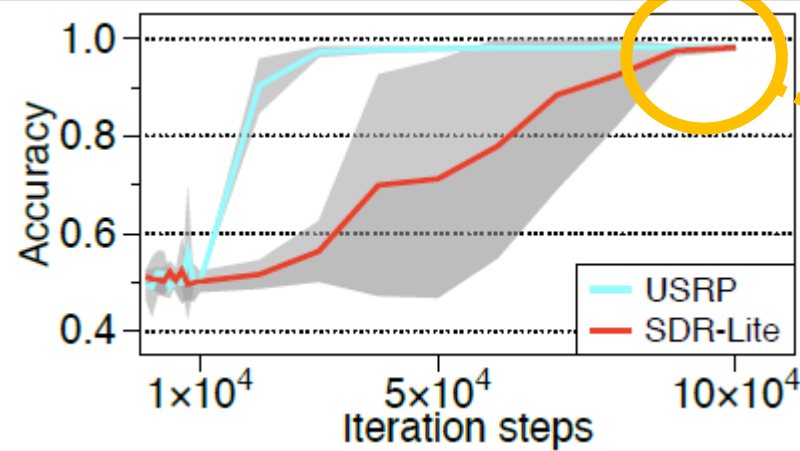
Intel Aero



DJI Mavic pro



**SDR-Lite can detect drones' signal with high reliability**



**Accuracy**

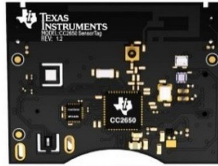
**SDR-Lite: 98 %**

**USRP: 98.2 %**

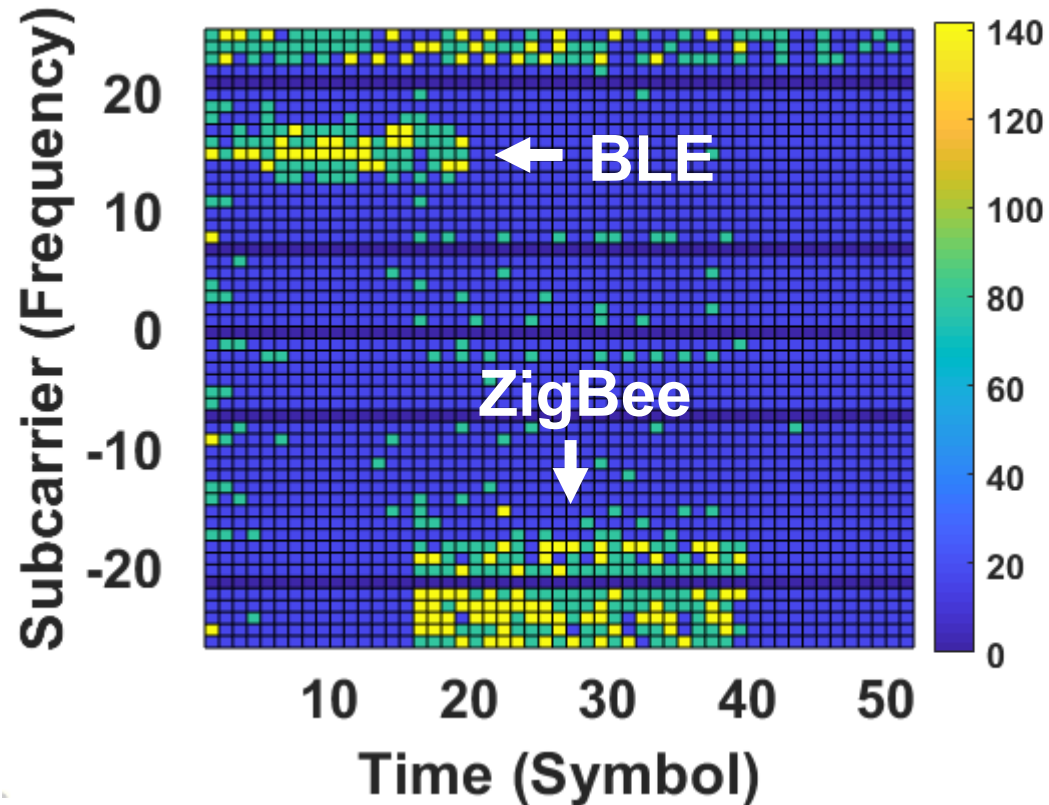


# App #2 Spectrum Analysis: Standardized wireless signals

---



 **Bluetooth**<sup>®</sup>  **zigbee**

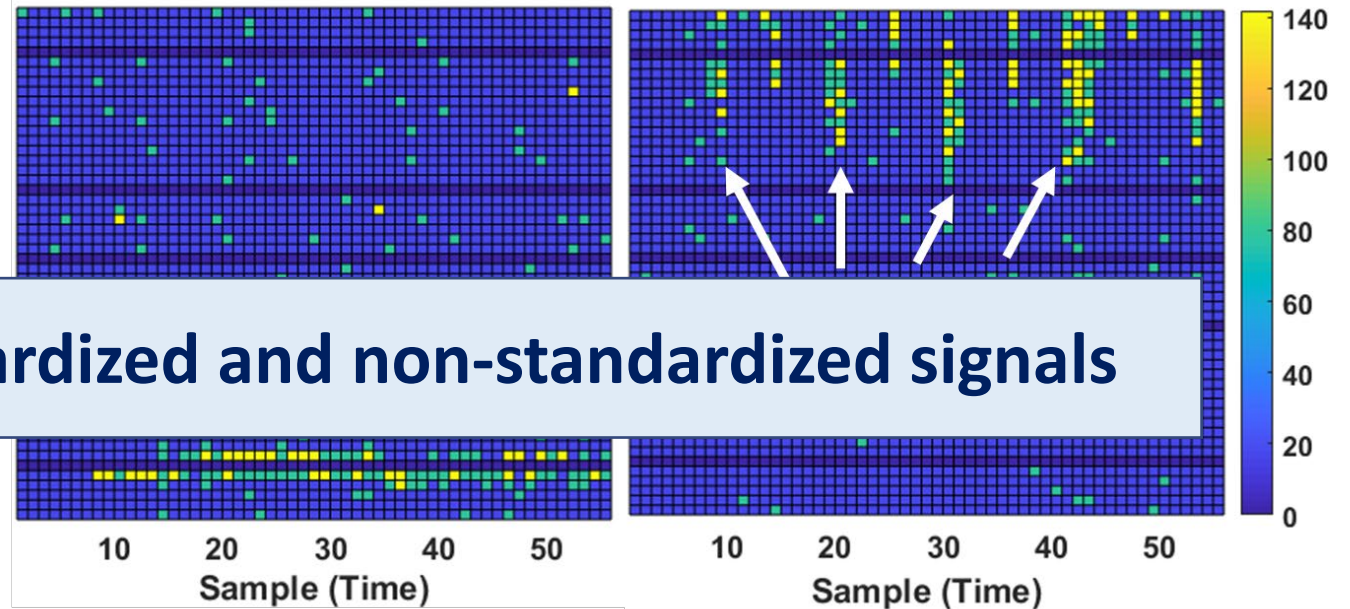


# App#2 Spectrum Analysis: Non-standardized RF signals



**SDR-Lite can analyze standardized and non-standardized signals**

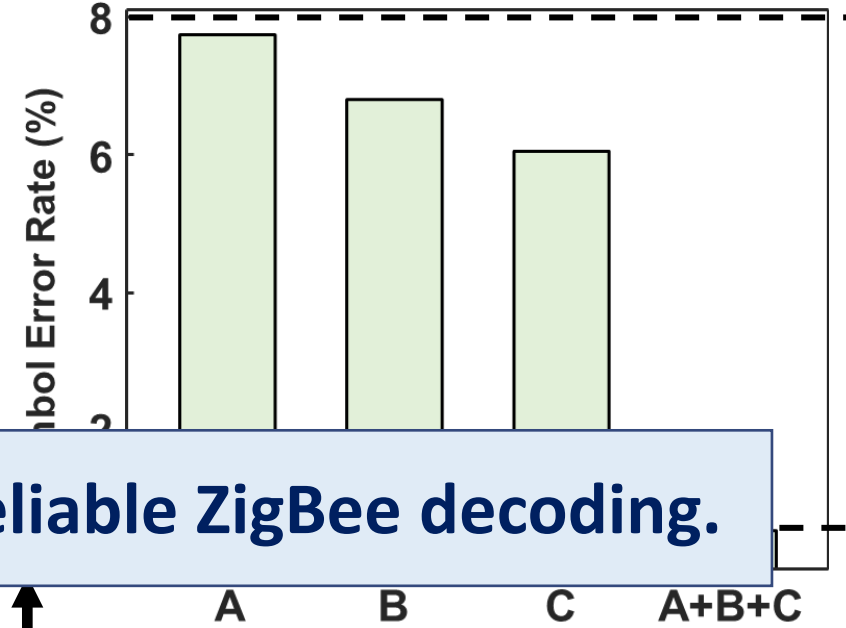
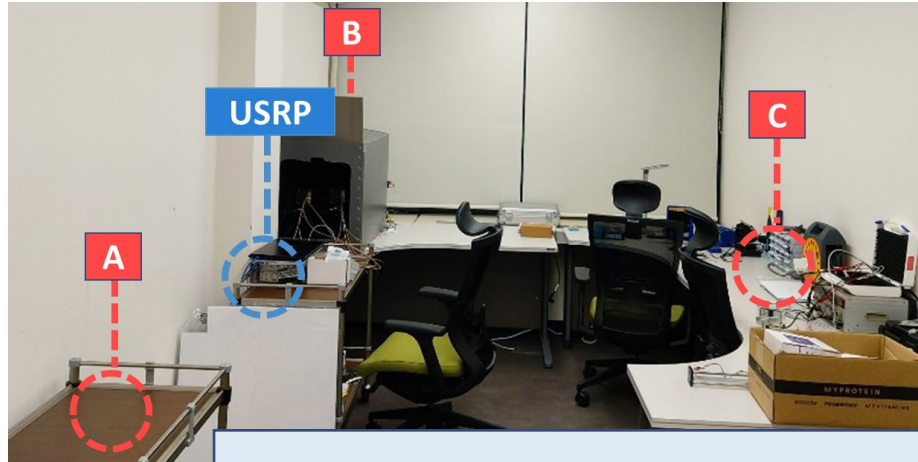
**RC car and microwave**



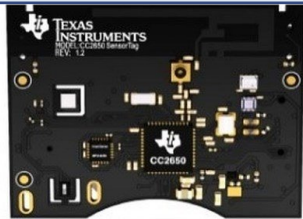
**Radio Controlled Car**

**Microwave Oven**

# App #3: ZigBee decoding



**SDR-Lite enables high reliable ZigBee decoding.**



TI CC2650 (ZigBee & BLE)

Multiple SDR-Lite

# 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!**