



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**

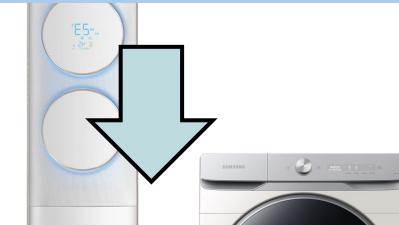
in collaboration with



Everything is going wireless

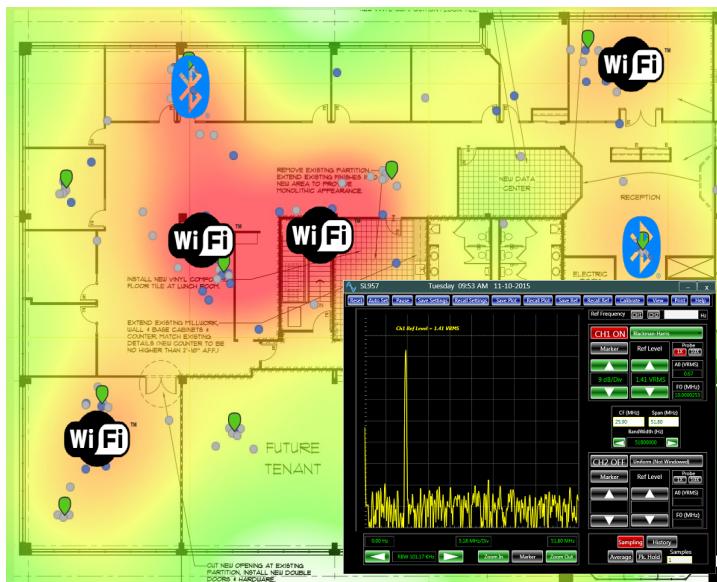


Wireless signals are increasing



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



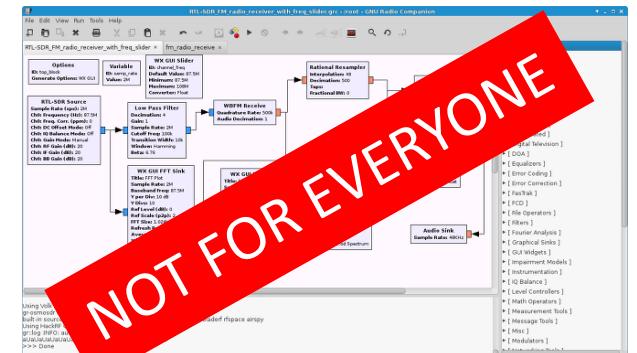
2. Software processing and applications



SDR is rarely used



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



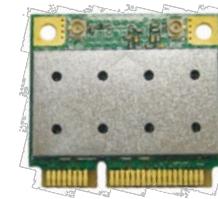
SDR-Lite

A new design to use commodity WiFi
as a SDR receiver

Beneficial WiFi



WNIC is Cheap

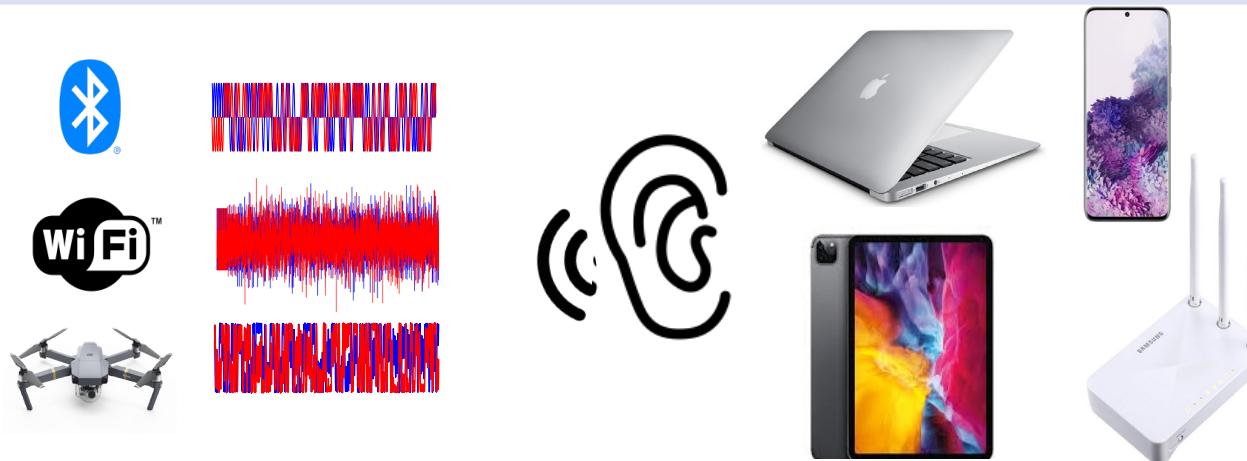


AR 9380: \$14

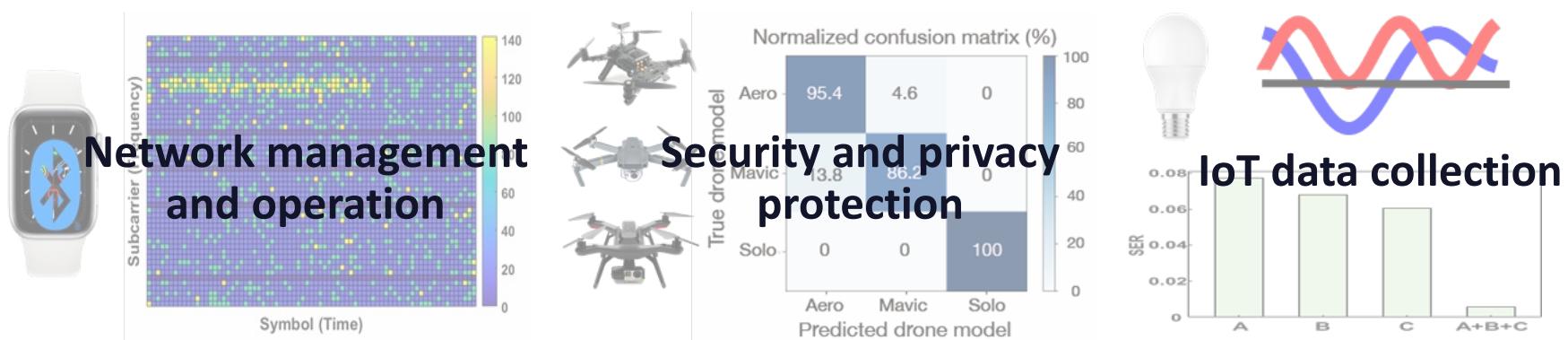
Billions of users

SDR-Lite: SDR Receiver Using Commodity WiFi

1. Receive ambient signal in the air



2. Software processing and applications



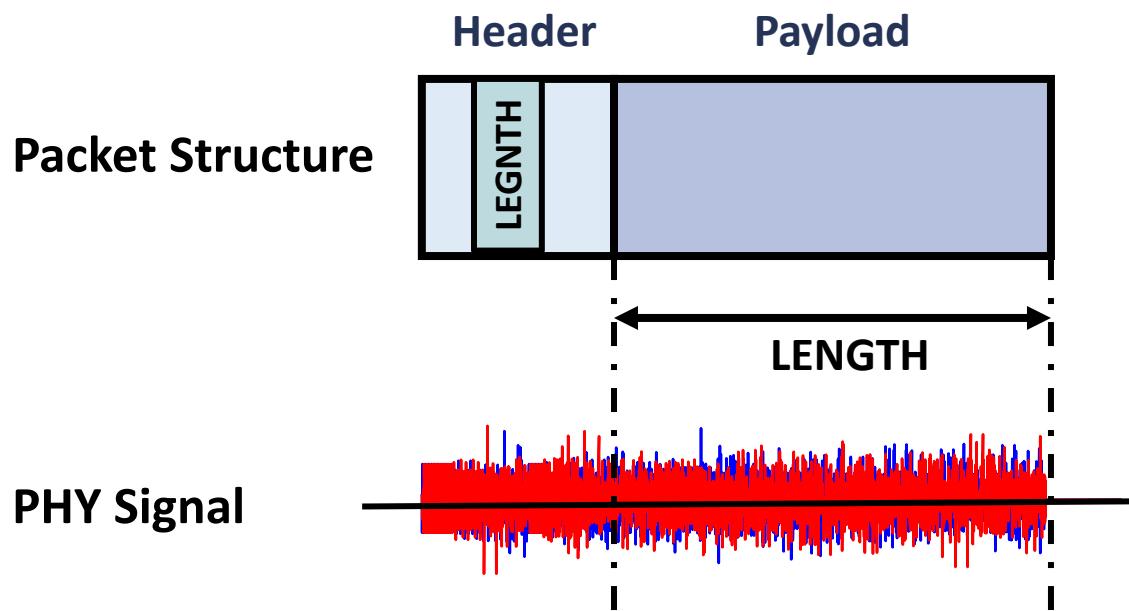
Design Overview

1. Receive ambient signal in the air



2. Software processing and applications

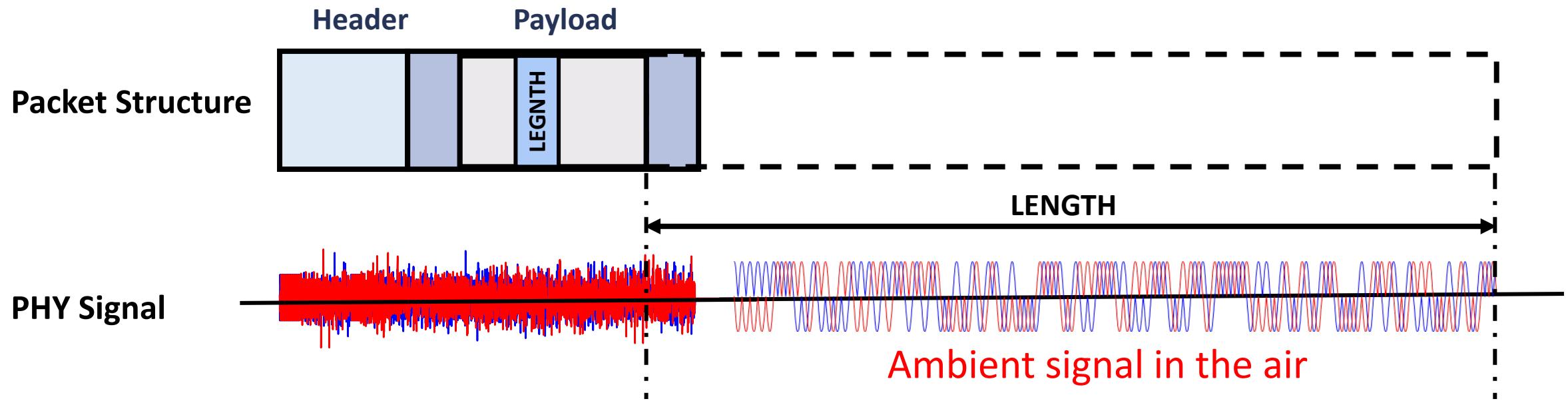
Signal reception of typical WiFi



WiFi decodes a packet during time corresponding LENGTH

How to receive ambient signal

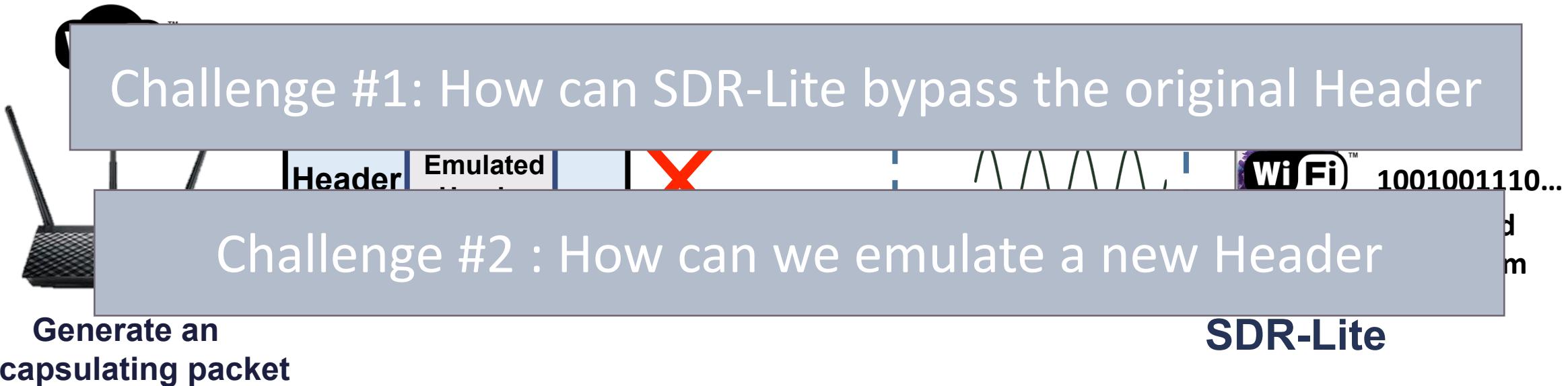
Q: What if a WiFi packet contains another header in the payload?



Construct a new WiFi Header in Payload
through emulation

How SDR-Lite works?

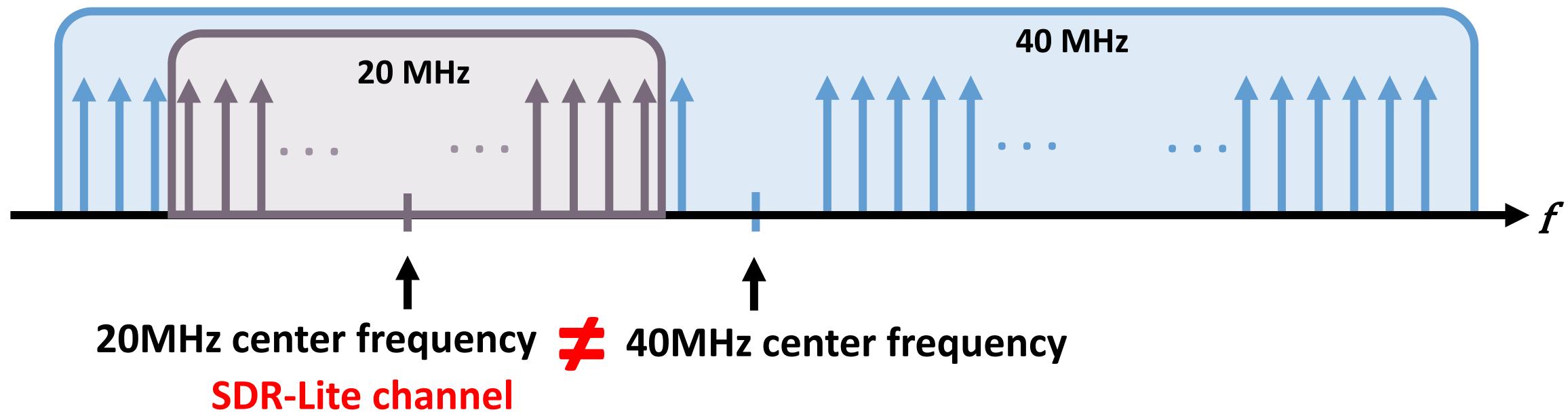
WiFi transmitter sends an encapsulating packet that contains Emulated Header



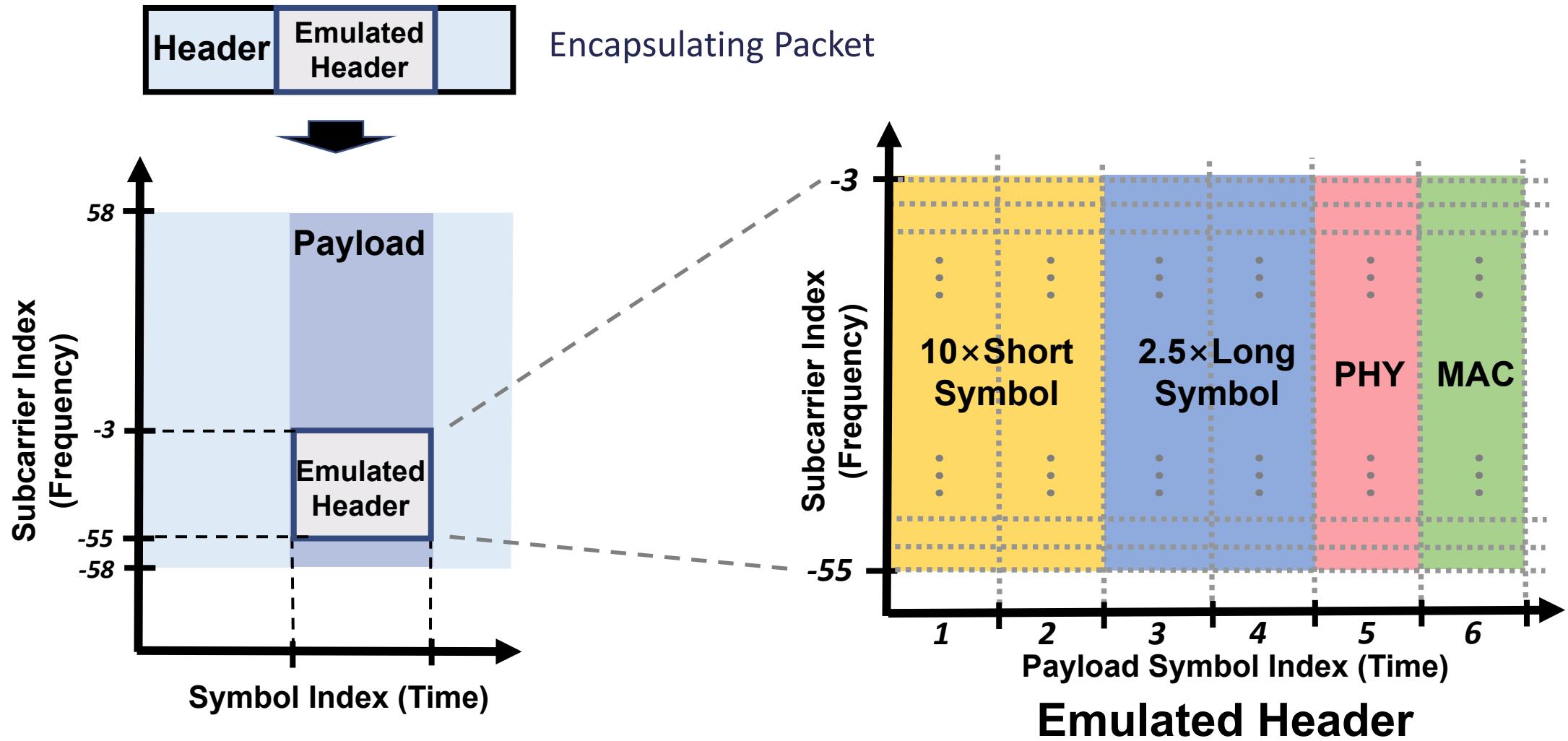
Challenge #1: How can SDR-Lite bypass the original Header



Encapsulating Packet



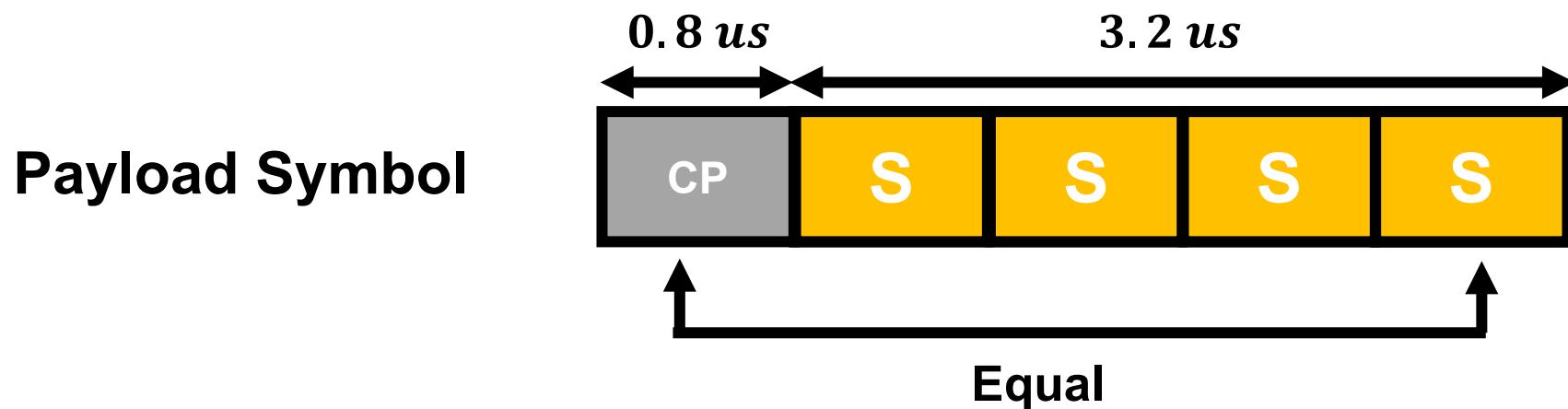
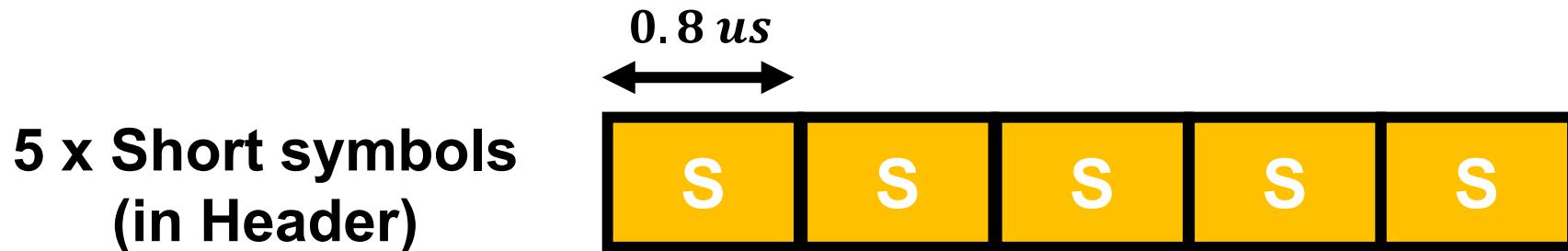
Challenge #2 : How can we generate an emulated Header



Header emulation using Payload

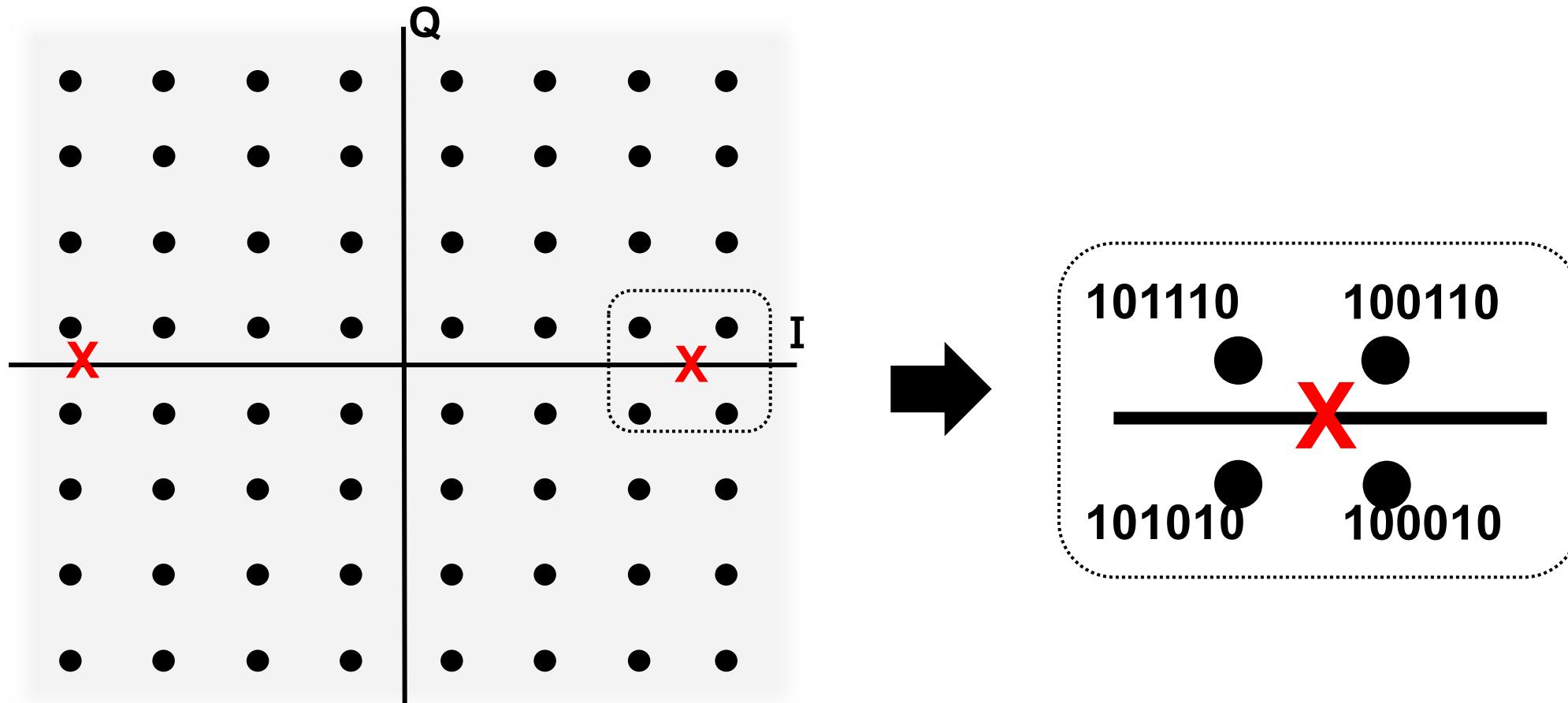
	Symbol format	Modulation
Header	<p>The diagram shows the symbol format for the header. It consists of four main components: 10× Short Symbol (yellow), 2.5× Long Symbol (blue), PHY (pink), and MAC (green). The total duration is 24 microseconds, divided into four 4μs intervals by double-headed arrows above the bars.</p>	BPSK/16 QAM
Payload	<p>The diagram shows the symbol format for the payload. It consists of four symbols labeled Symbol 1, Symbol 2, Symbol 3, and Symbol 4, followed by an ellipsis indicating repetition. The total duration is 16 microseconds, divided into four 4μs intervals by double-headed arrows above the bars.</p>	64 QAM

Addressing the discrepancy in the symbol format



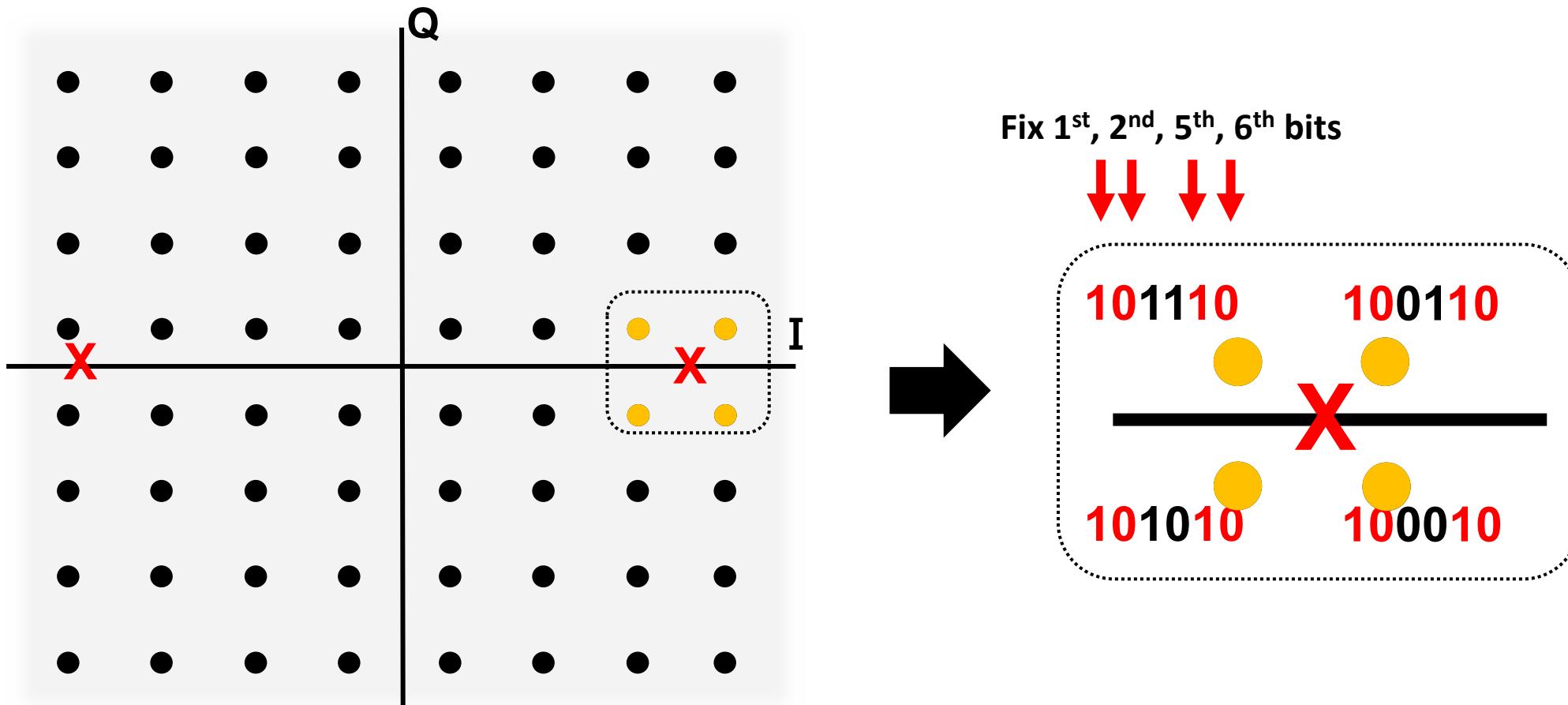
Subcarrier Constellation Mapping (Modulation)

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

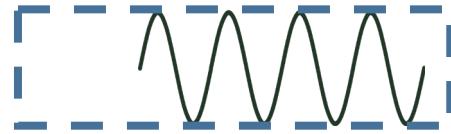


Subcarrier Constellation Mapping

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



SDR-Lite receives an ambient signal



Ambient Signal



1001001110...
Decoded bitstream

Reconstructing an ambient signal and enabling application
→ Software processing

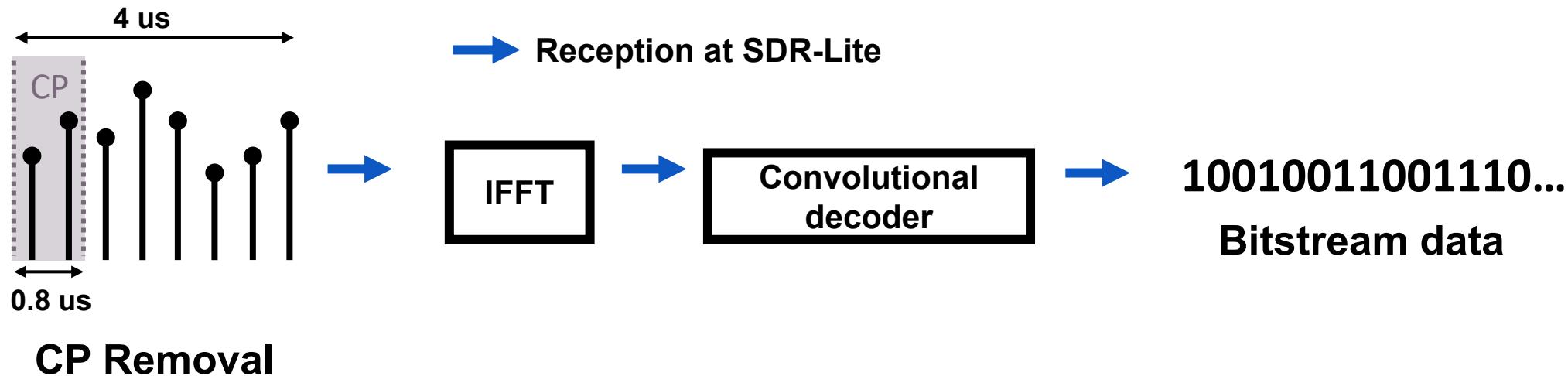
SDR-Lite Design

1. Receive ambient signal in the air

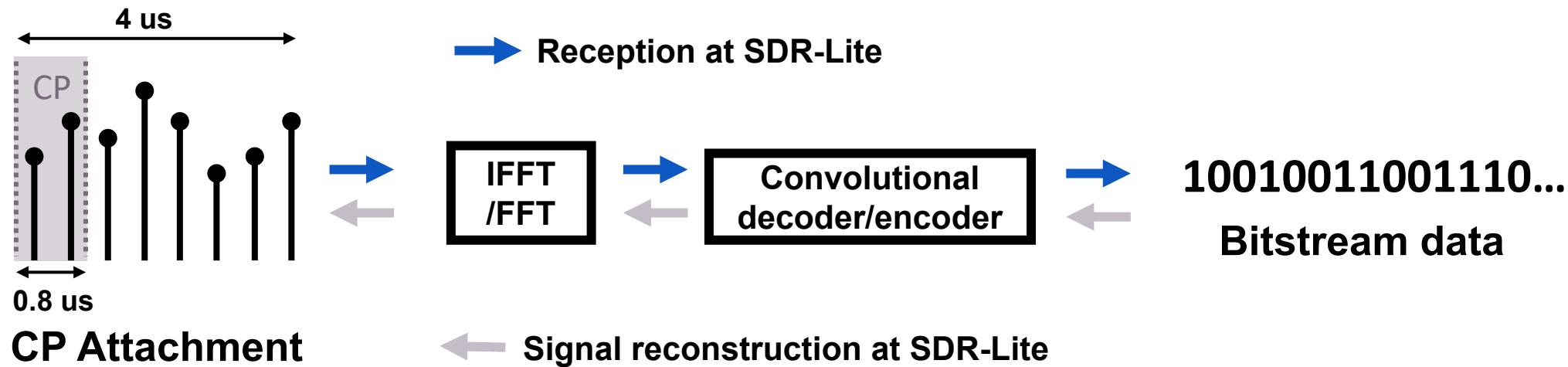


2. Software processing and applications

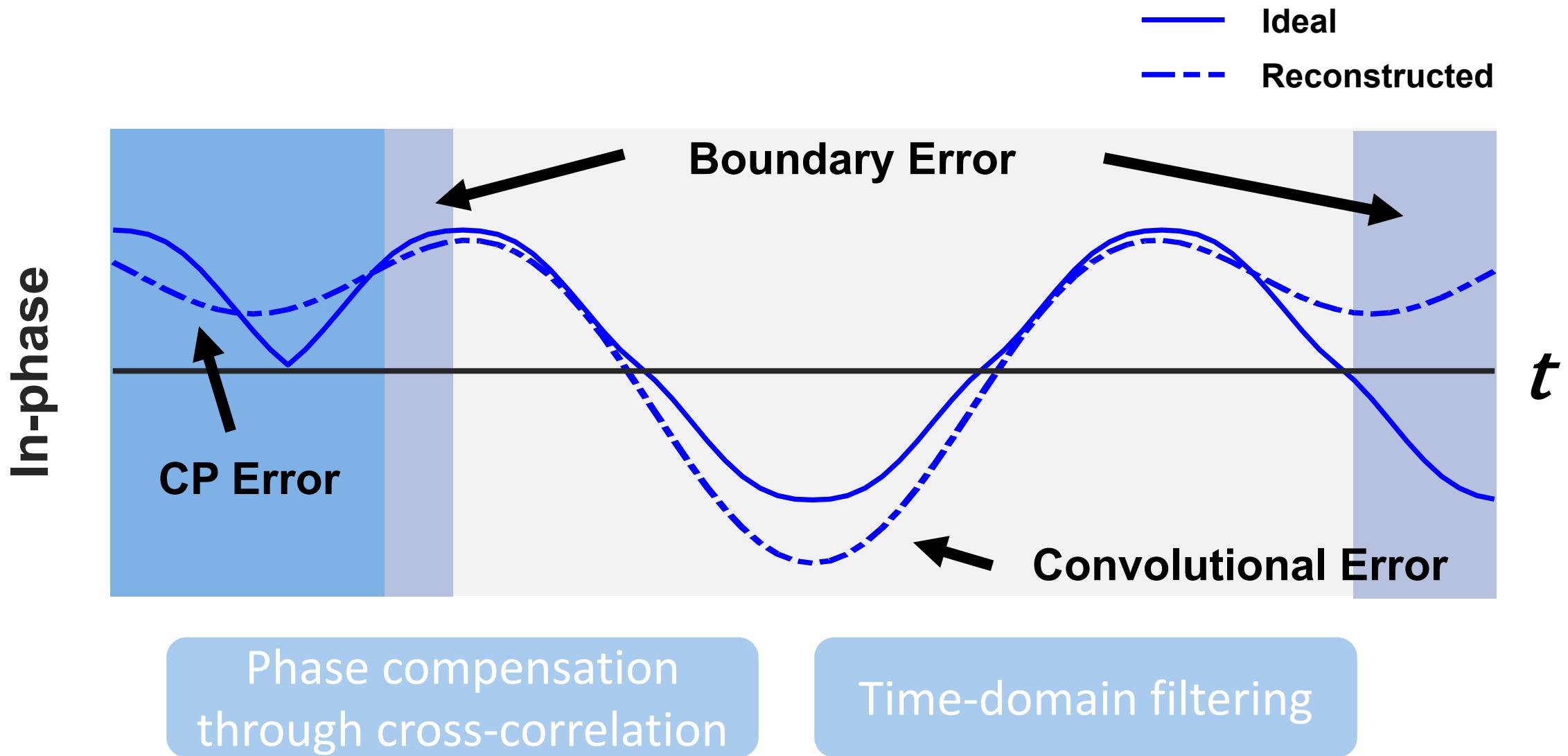
Reconstructing ambient signal from received bits



Reconstructing ambient signal from received bits



Reconstructed In-phase signal



SDR-Lite Design

1. Receive ambient signal in the air



2. Software processing and applications

RF Fingerprinting

Spectrum Monitoring

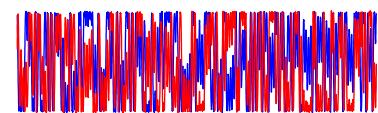
ZigBee Decoding

RF Fingerprinting

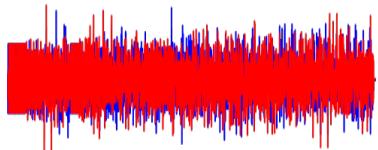
Reconstructed signal closely mimics the original ambient signal



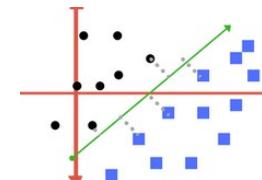
Drone



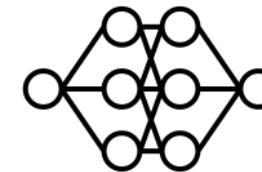
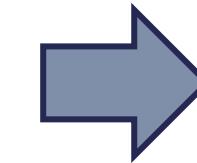
WiFi router



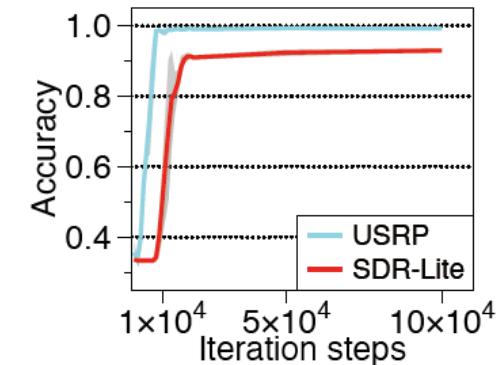
SDR-Lite



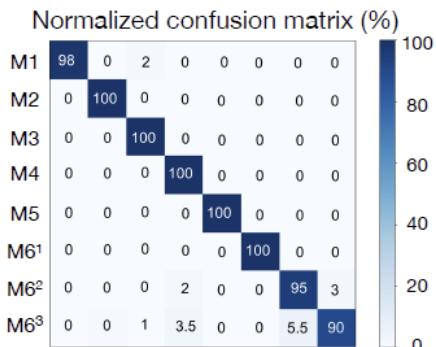
SVM



DNN



Drone Detection



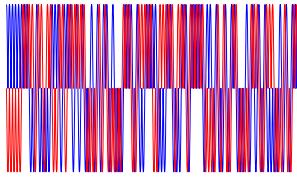
WiFi Device Identification

Spectrum Monitoring

Reconstructed signal could be used for spectrum analyzing

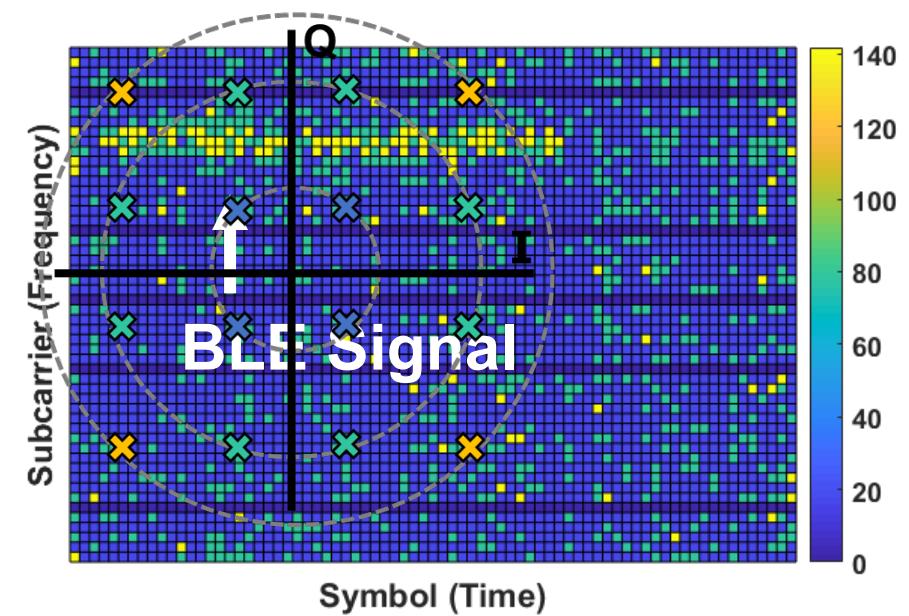


BLE device

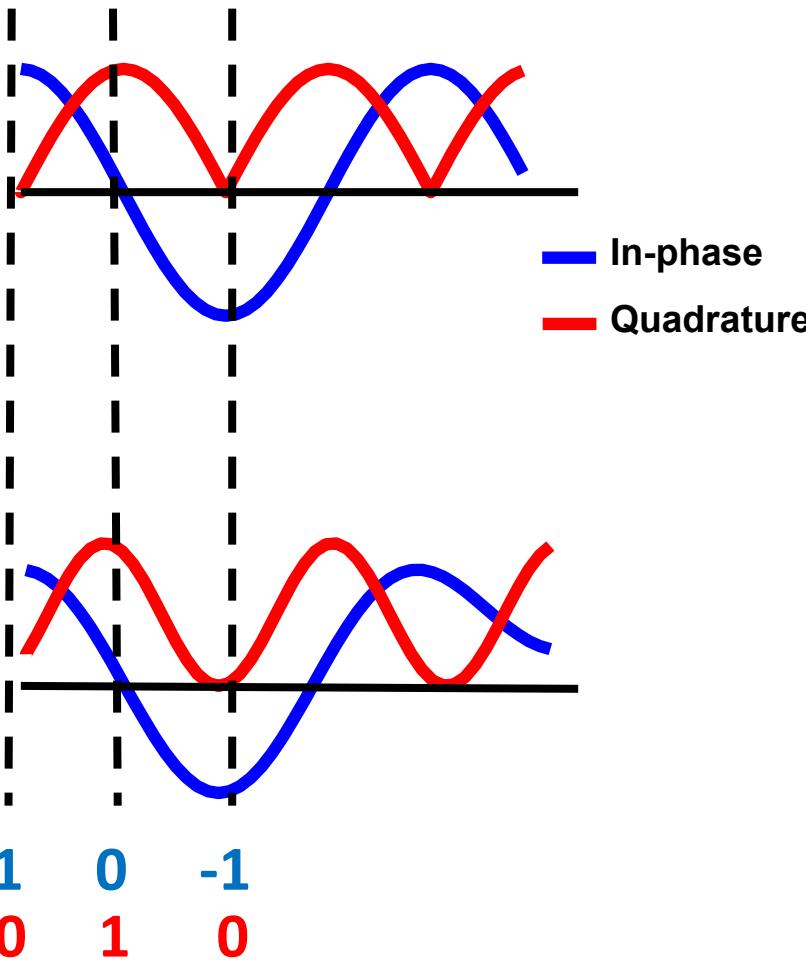


SDR-Lite

FFT
→

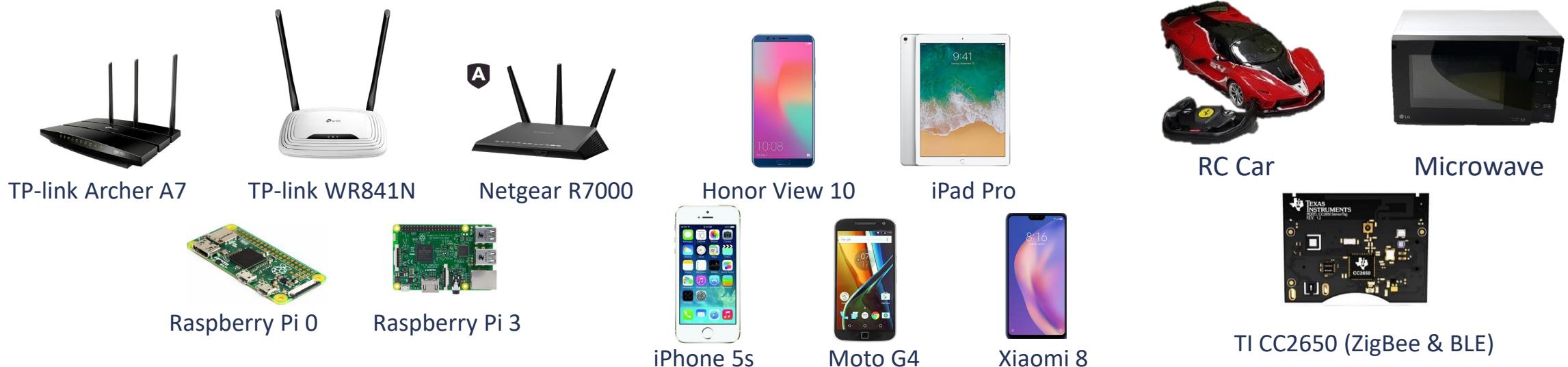


ZigBee Decoding



SDR-Lite

Experiment Setup



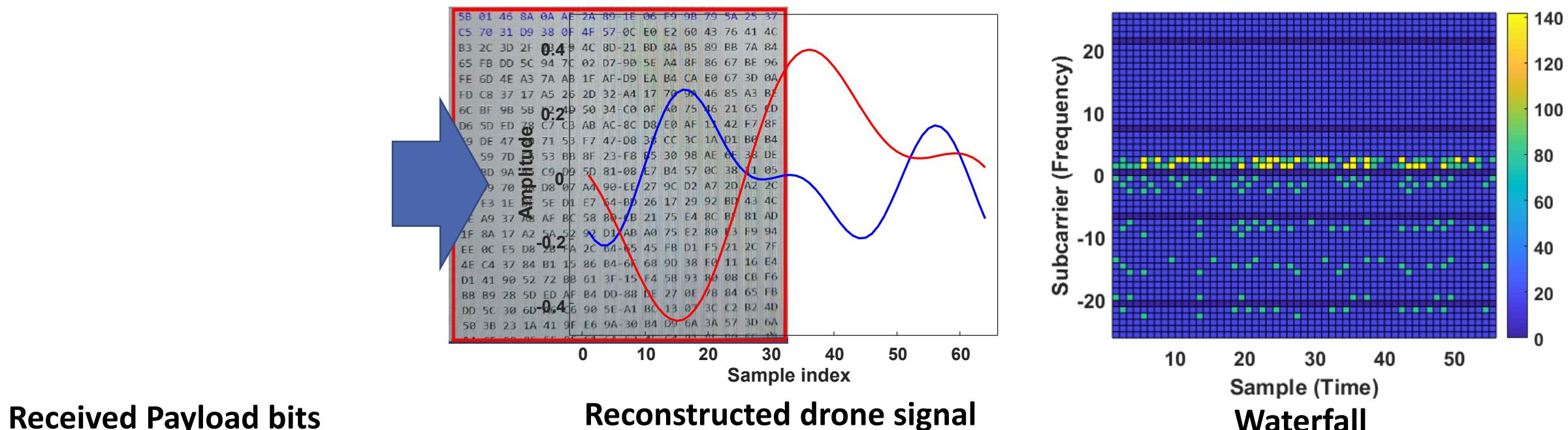
SDR-Lite in action



SDR-Lite in action

etn	0x0000	5B 01 46 8A 0A AE 2A 89-1E 06 F9 9B 79 5A 25 37	[.F\$
Ov	0x0010	C5 70 31 D9 38 0F 4F 57-0C E0 E2 60 43 76 41 4C	Ap1L
for	0x0020	B3 2C 3D 2F 2B F9 4C 8D-21 BD 8A B5 89 BB 7A 84	,-
ro	0x0030	65 FB DD 5C 94 7C 02 D7-90 5E A4 8F 86 67 BE 96	eūY\
rd	0x0040	FE 6D 4E A3 7A AB 1F AF-D9 EA B4 CA E0 67 3D 0A	Received
yp	0x0050	FD C8 37 17 A5 26 2D 32-A4 17 70 9A 46 85 A3 BE	Payload bits
Sub	0x0060	6C BF 9B 5B F2 4D 50 34-C0 0F A0 75 46 21 65 CD	↓
S IE	0x0070	D6 5D ED 78 C7 C3 AB AC-8C D8 E0 AF 11 42 F7 8F	pmNEz". uc eag-.
uro	0x0080	F9 DE 47 80 71 53 F7 47-D8 38 CC 3C 1A D1 B0 B4	ýÈ7.¥&-2¤.pšF...£%
stin	0x0090	5C 59 7D F5 53 BB 8F 23-F8 B5 30 98 AE 6E 38 DE	lç>[òMP4À. uF!ef
gm	0x00A0	2F BD 9A A5 C9 D9 5D 81-08 E7 B4 57 0C 38 11 05	Ö]ixÇÀ«→øΦà".B÷
gue	0x00B0	79 59 70 9A D8 07 A4 90-EE 27 9C D2 A7 2D A2 2C	ùDG€qS:GØ8I<.Ñ°
	0x00C0	DD E3 1E DF 5E D1 E7 64-BD 26 17 29 92 BD 43 4C	\Y}ōS»#øμ0~®n8P
	0x00D0	1E A9 37 A8 AF BC 58 80-CB 21 75 E4 8C BF 81 AD	/%š¥ÉÙ].ç W.8..
	0x00E0	1F 8A 17 A2 5A 52 92 D1-AB A0 75 E2 80 E3 F9 94	yYpšØ.mí'øØ§-¢,
	0x00F0	EE 0C E5 D8 2B FA 2C 64-65 45 FB D1 F5 21 2C 7F	Ýä.ß^Ñçd%&.)'%CL
	0x0100	4E C4 37 84 B1 15 86 B4-6F 68 9D 38 E0 11 16 E4	.@7" "XX€Ë!uä€ç-
	0x0110	D1 41 90 52 72 BB 61 3F-15 F4 5B 93 80 08 CB F6	.š.¢ZR'Ñ« uâ€äù"
	0x0120	BB B9 28 5D ED AF B4 DD-88 DE 27 0E 78 84 65 FB	i.åø+ü,deEûÑö!,
	0x0130	DD 5C 30 6D A6 C6 90 5E-A1 BC 13 07 3C C2 B2 4D	NÄ7,,±. t'oh8à..ä
	0x0140	50 3B 23 1A 41 9F E6 9A-30 B4 D9 6A 3A 57 3D 6A	ÑARR»a?.ö["€.Ëö
	0x0150	51 3E 30 0F FF 0E C1 5A F2 4F C4 91 0F D9 EC 39	»¹(]í" "Ý"p'.x,eú

SDR-Lite in action



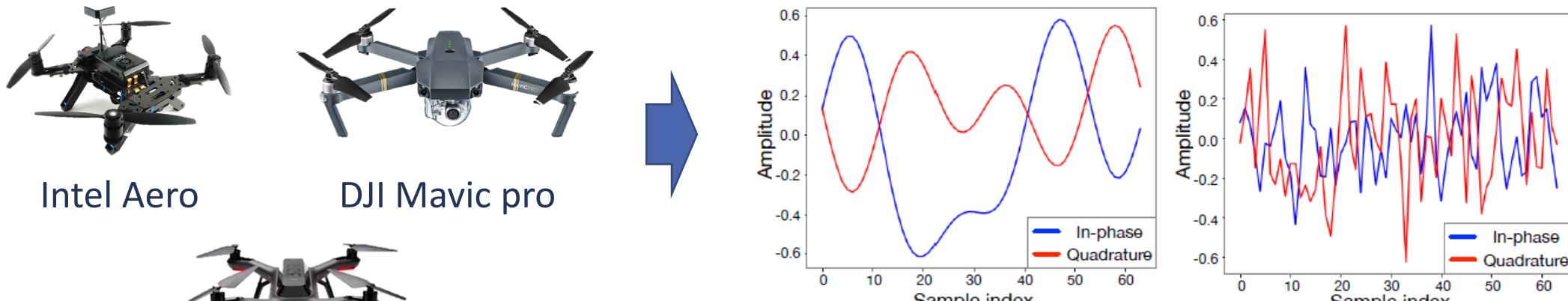
Received Payload bits

Reconstructed drone signal

Waterfall

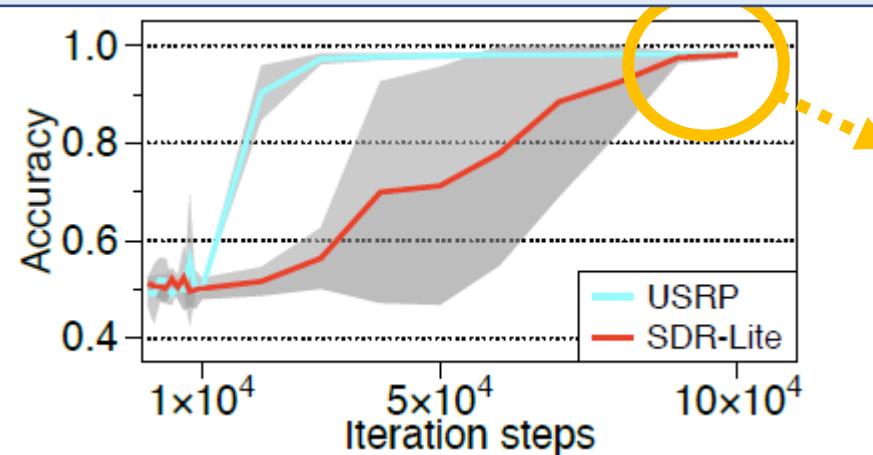
Can be used for unauthorized UAV detection

App. #1: Drone Detection



SDR-Lite can detect drones' signal with high reliability

SDR-Lite

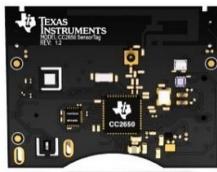


Accuracy

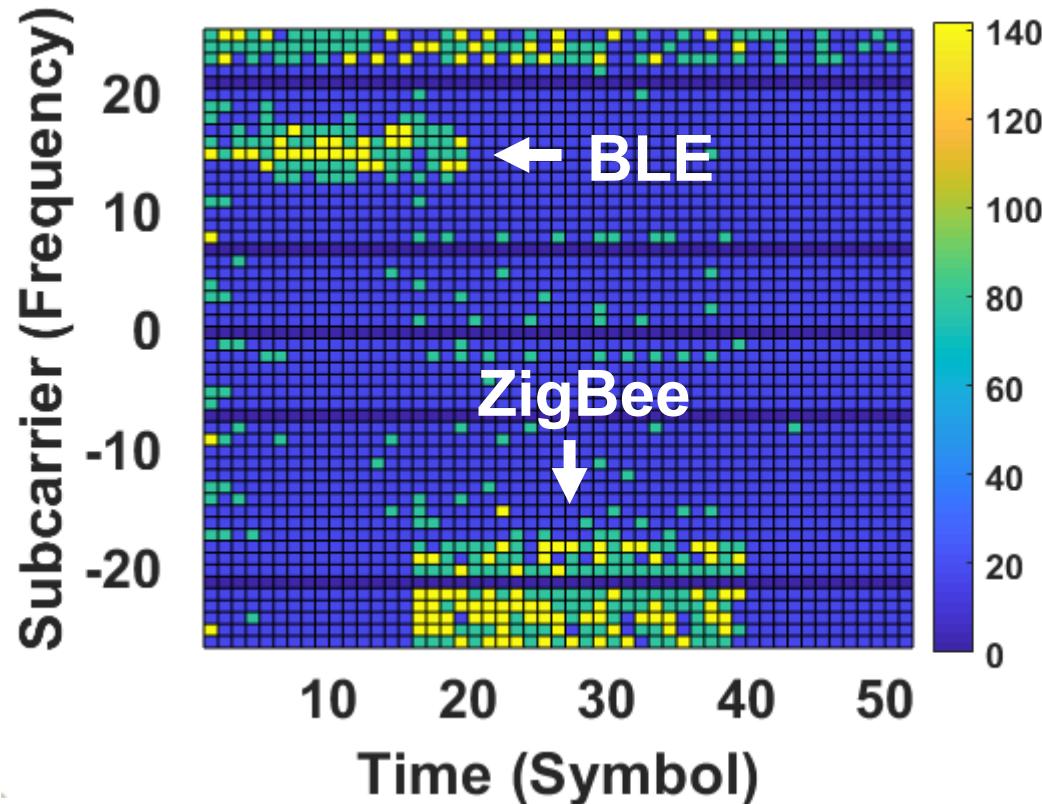
SDR-Lite: 98 %

USRP: 98.2 %

App #2 Spectrum Analysis: Standardized wireless signals



Bluetooth®  zigbee

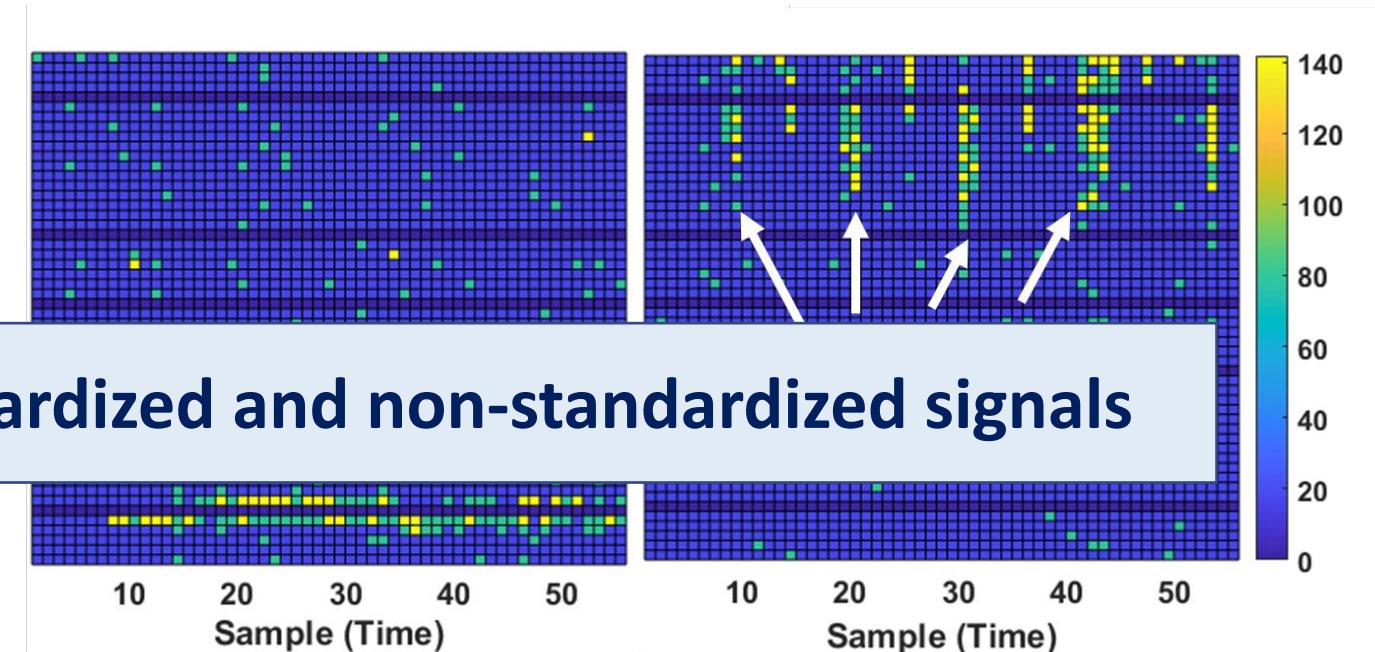


App#2 Spectrum Analysis: Non-standardized RF signals

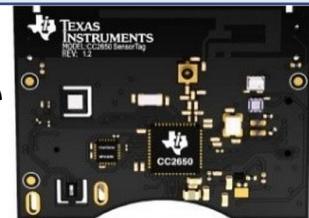
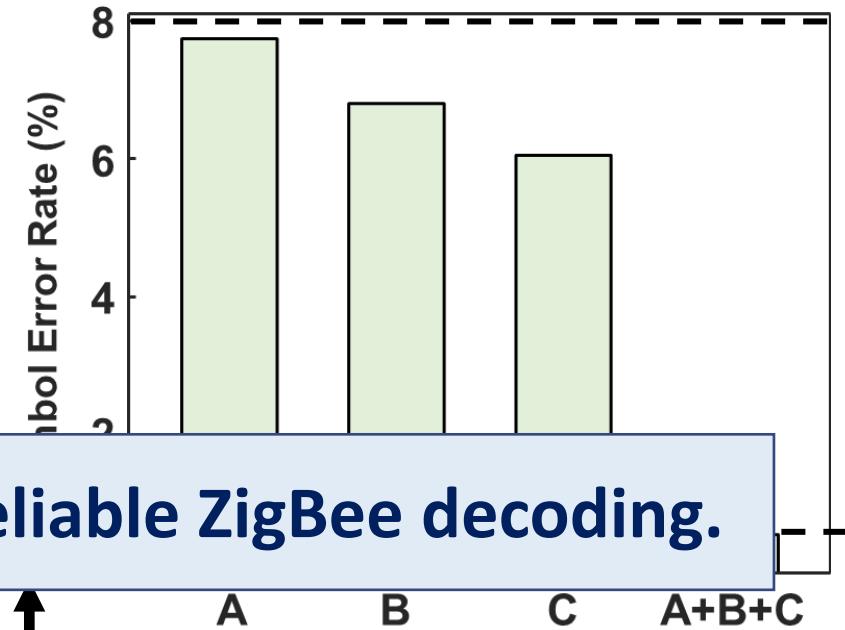
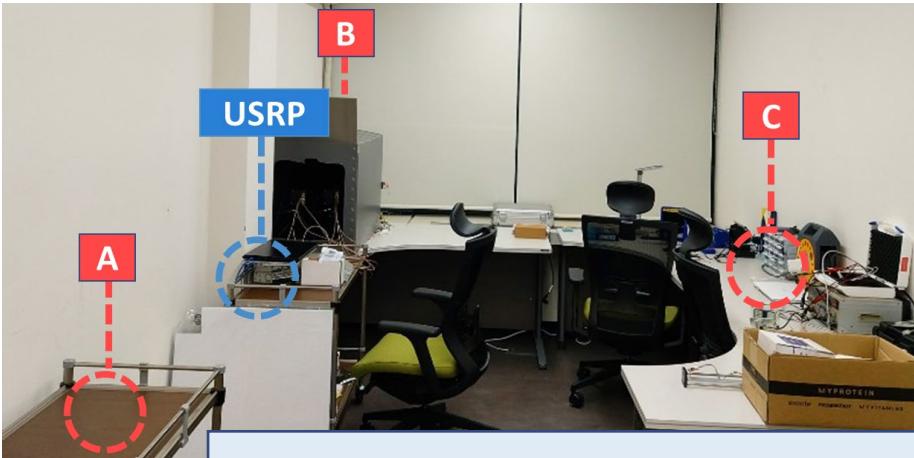


SDR-Lite can analyze standardized and non-standardized signals

RC car and microwave



App #3: 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!