PassiveBLE: Towards Fully Commodity-Compatible BLE Backscatter

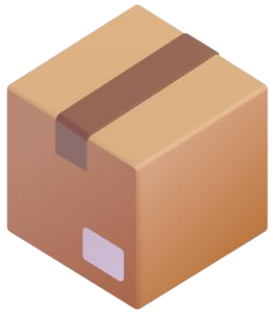
Huixin Dong, Yijie Wu , Feiyu Li , Wei Kuang ,
Yuan He , Qian Zhang , Wei Wang

華中科技大學
HUAZHONG UNIVERSITY SCIENCE AND TECHNOLOGY

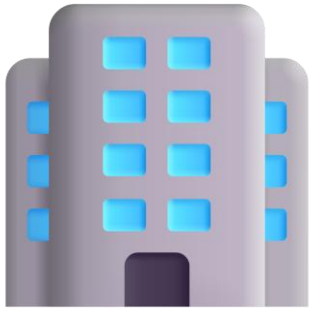
香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

清華大學

BLE backscatter facilitates uW-level BLE communications



Logistics & Tracking



Smart Infrastructures

Wearable Electronics

BLE Backscatter facilitates ultra-low-power and compatible communication with wide-deployed BLE devices.

Problem： BLE backscatters' bottleneck for industry data collection

One-shot communication based on BLE advertising packets

Excitation Source
(Provide carriers)

Backscatter Tag
(Upload data)

Commercial BLE Receiver
(Receive data)

Limited throughput

Only tens of kbps, cannot support data collection applications

High delay

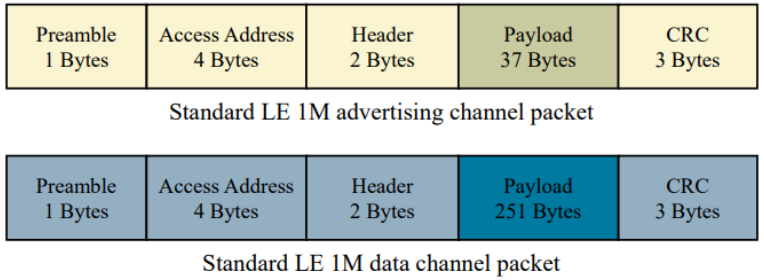
Delay of advertising packets > 20ms

InPrivate broadcasting

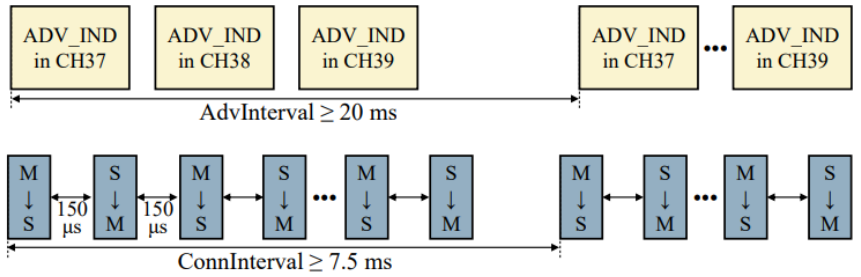
Transparent broadcasting, cannot apply to any security methods

Motivation: enabling BLE connection compatible becomes crucial

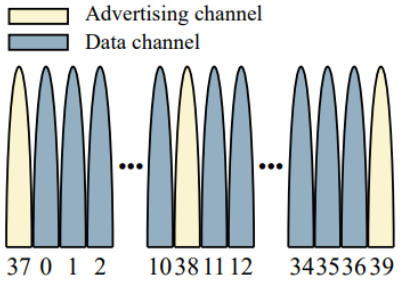
Communication capability of connected communications



Higher Coding Efficiency (78.7% vs 96.2%)



Less Transmission Interval (6.67ms/packet vs 150us/packet)



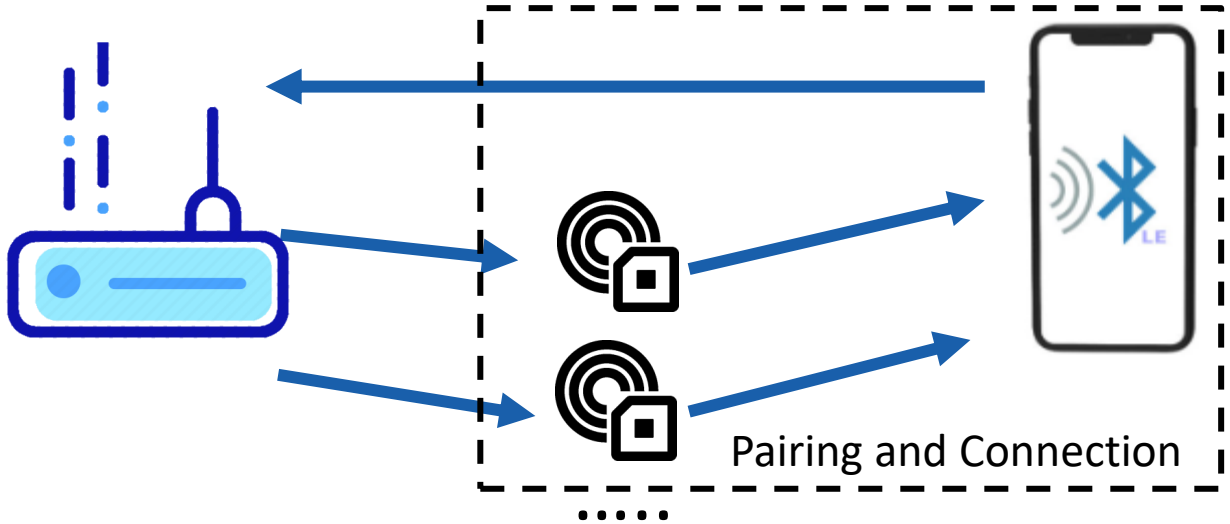
More Data Channels (3 Adv channels vs 37 Data channels)

Pushing the BLE backscatter from advertising packets compatible to BLE connection compatible is promising to provide 2 orders of improvement

Can we further leverage the capability of backscatter to fully support BLE connections

Our target: Support the commodity BLE Connection

Communication with Pairing and Connection (same as active BLE)



Advantages

Higher throughput

Up to Mbps-level throughput, can support multiple types of sensing data

Lower delay

us-level packet delay (150us) the same as commercial BLE devices

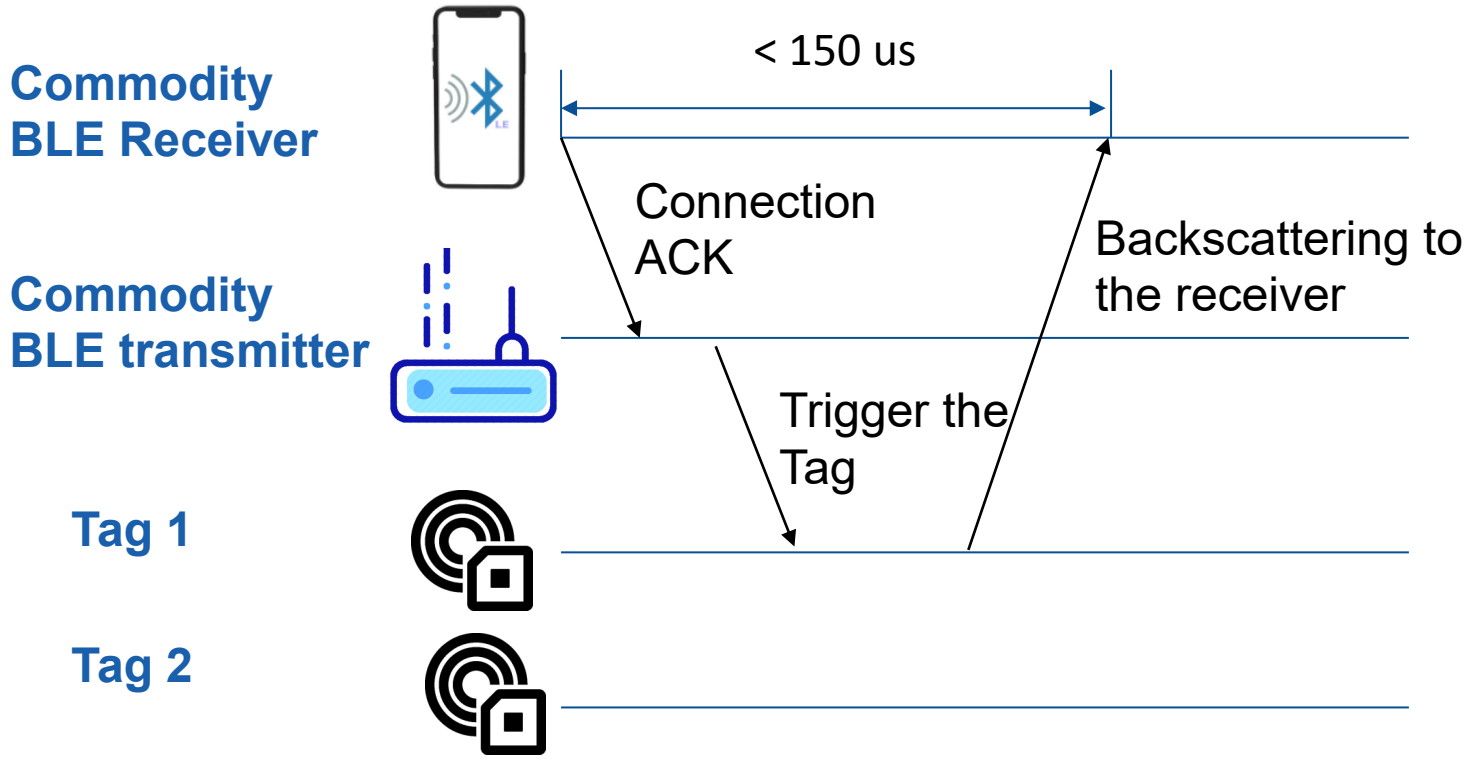
Private connection

Achieve data packet connections the same as commercial BLE devices.

Challenges and Solutions

Challenge 1: High-performance synchronization on tag

BLE Connection under a connection event



Sync requirements

Short wake-up time
< 150 us

Symbol-level accuracy
< 0.5 us

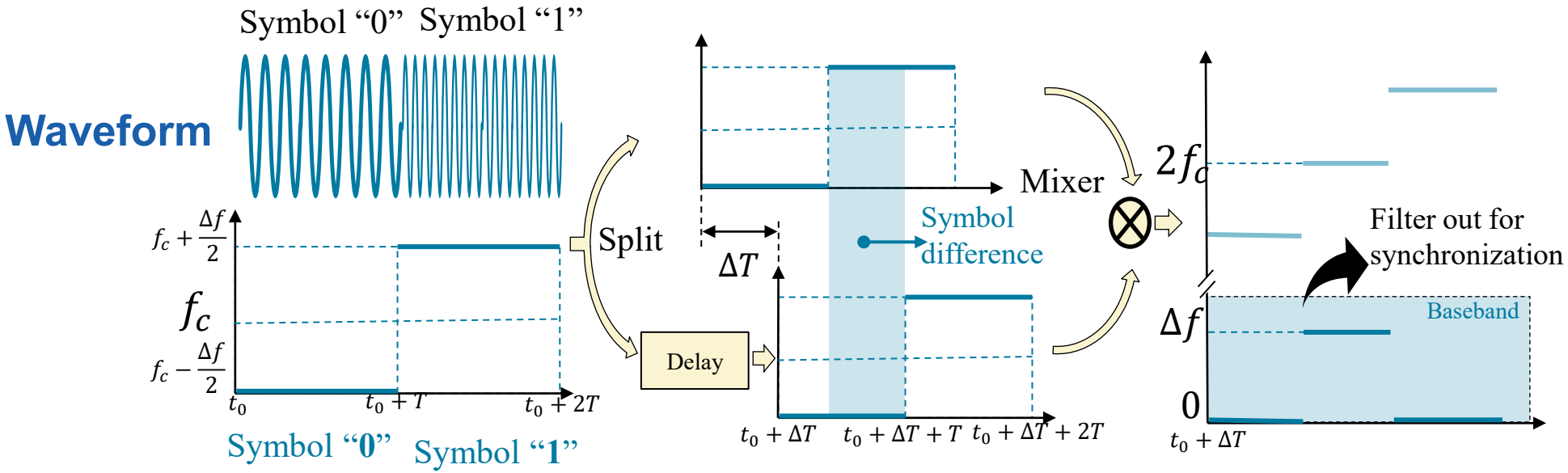
Envelop detectors cannot extract symbols

LO-based demodulator are power hungry

Solution 1: Extract the difference between symbols

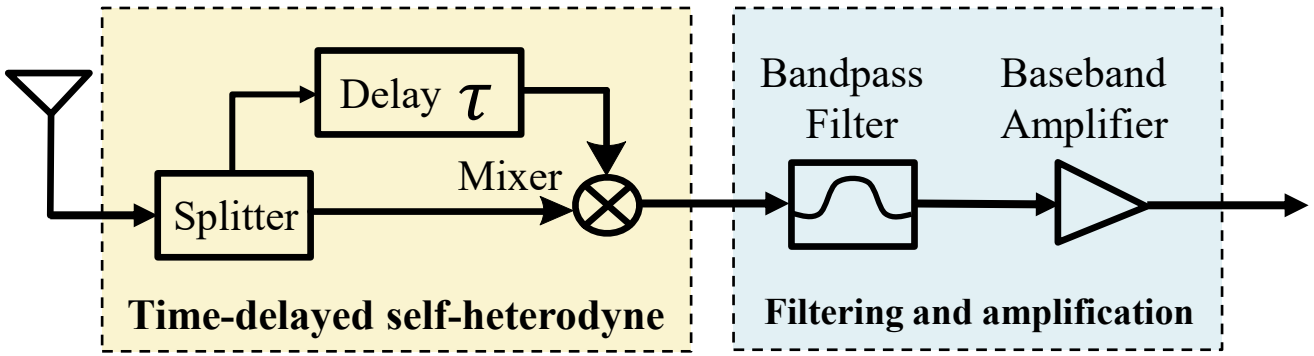
Key insight

Extract the difference between symbols rather than demodulate them for synchronization

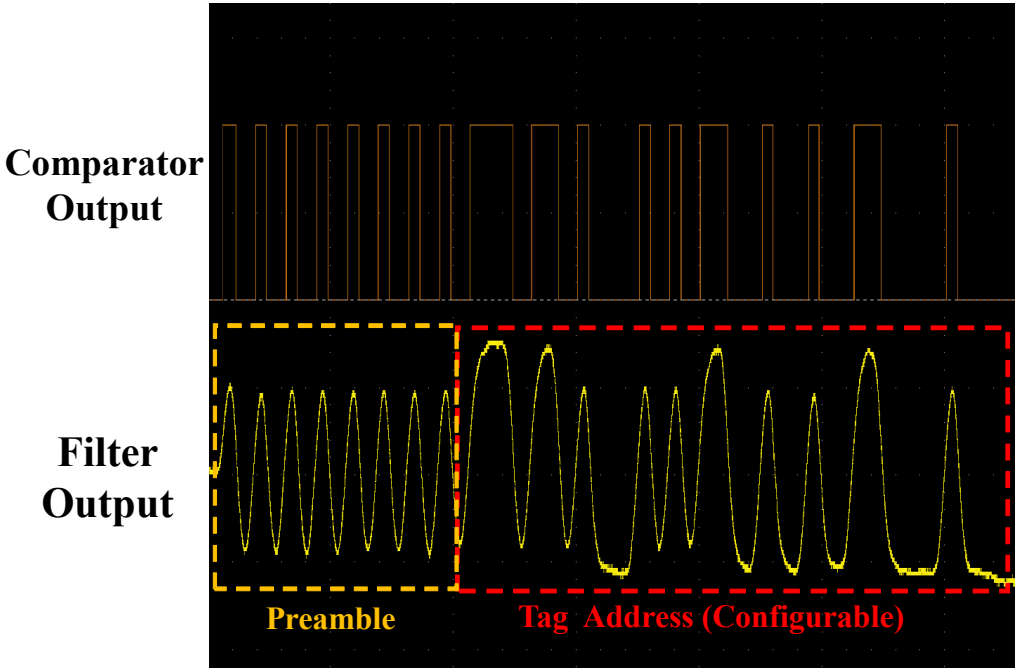


Solution 1: Delayed Self-heterodyne circuit

Circuit diagram

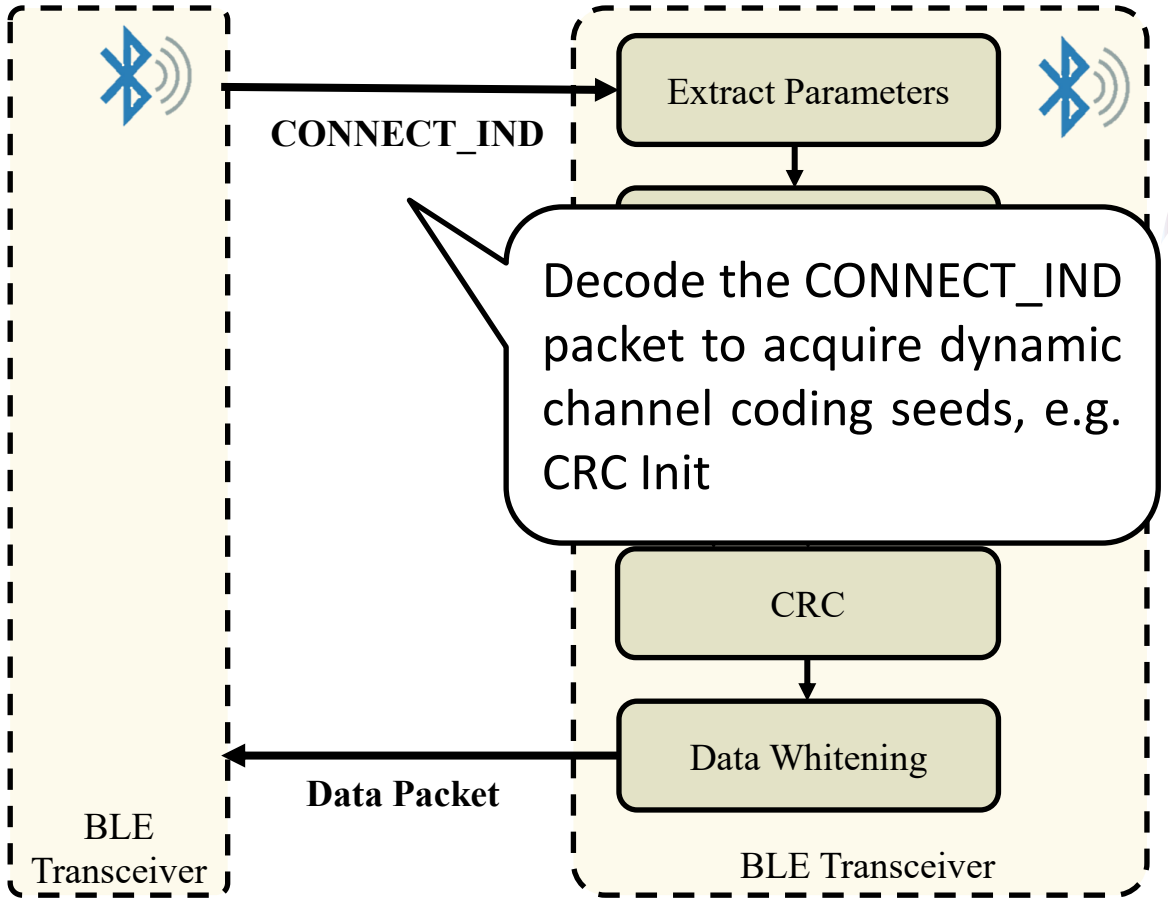


Output on oscilloscope



Challenge 2: Dynamic coding seeds for BLE packets

Commodity BLE devices



Commodity BLE packets encoding

Whitening

$$(Data \ \mathbf{XOR} \ w(C\_index)) \times f_c$$

Data on tag — Need extract from BLE packets

CRC

$$(Data \ \mathbf{XOR} \ CRC_{Init}) \ \mathbf{MOD} \ g(x)$$

Data on tag — **Need extract from BLE packets**

All need completed on one BLE device

Tag cannot decode BLE packets to obtain these seeds

Will it possible for the tag to generate commodity-compatible BLE packets without obtaining these seeds?

Solution 2: XOR Operations on RF Signals

Observation

The encoding process using XOR operation to combine data and the dynamic seed, and XOR operations are independent of operation order.

Commodity BLE packets encoding

Whitening $(Data\ \mathbf{XOR}\ w(C\_index)) \times f_c$

Data on tag

Need extract from BLE packets

CRC $(Data\ \mathbf{XOR}\ CRC_{Init})\ \mathbf{MOD}\ g(x)$

Data on tag

Need extract from BLE packets

All need completed on tags

Change the order of XOR operation

Equal results

PassiveBLE packets encoding

$Data$

Data on tag

$\mathbf{XOR}\ (w(C\_index)) \times f_c$

Can we construct XOR operations outside tags?

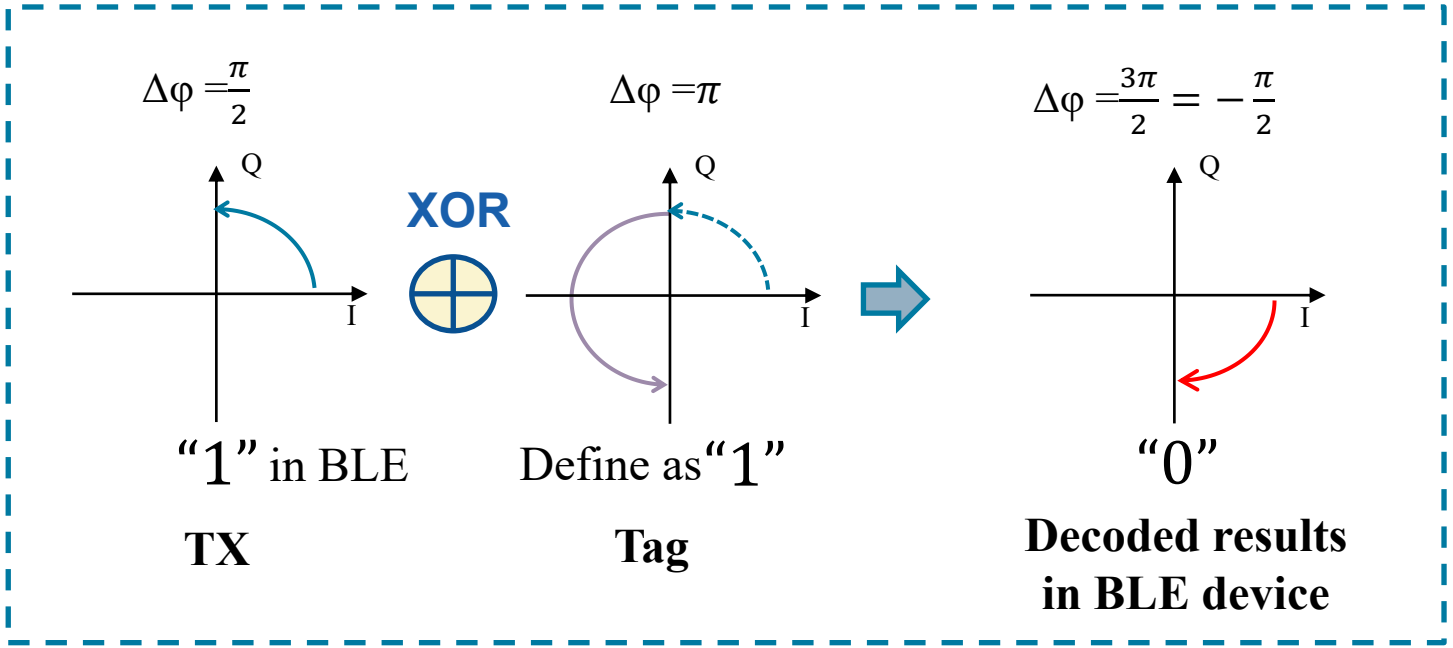
$(Data\ \mathbf{MOD}\ g(x))\ \mathbf{XOR}\ (CRC_{Init}\ \mathbf{MOD}\ g(x))$

These must completed on tags only contain static parameters

Solution 2: XOR Operations on RF Signals

Our idea

Constructing XOR operations with RF signals' phase changes by backscattering

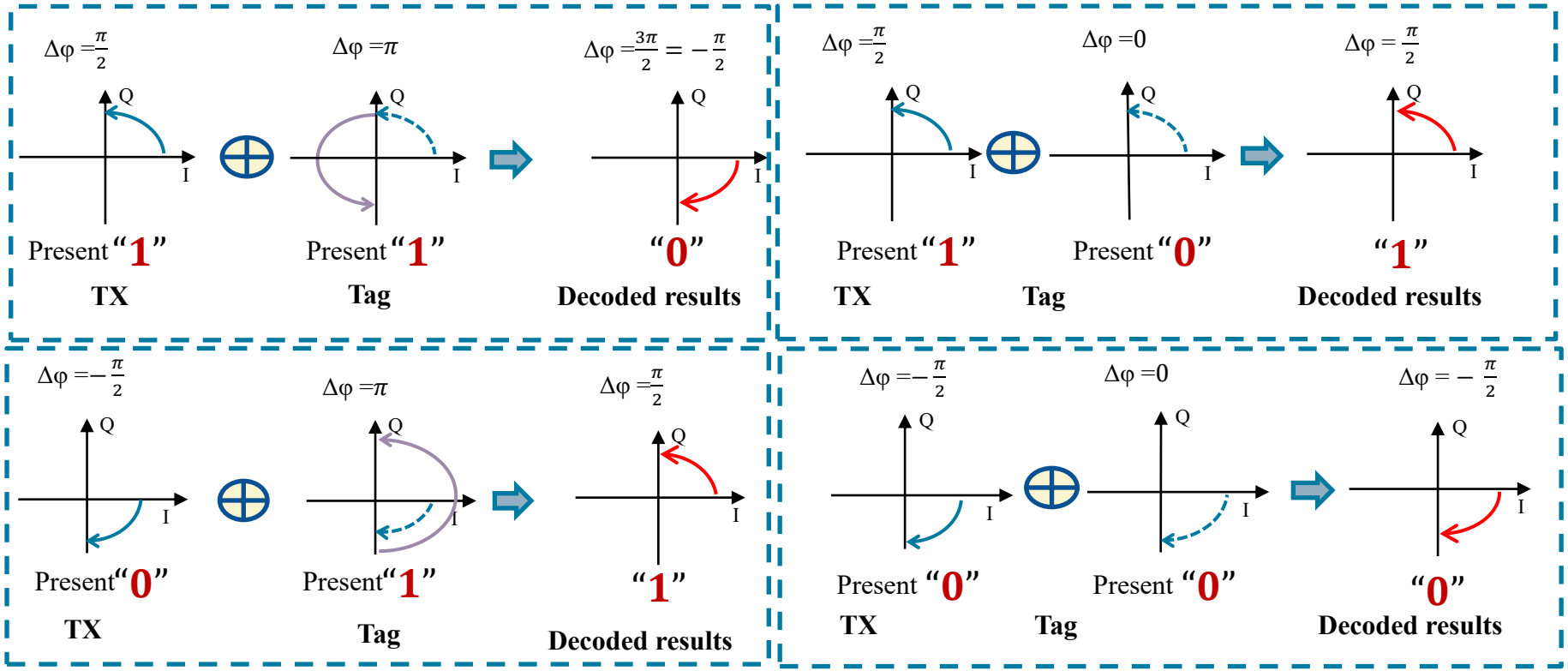


XOR operation "1" ⊕ "1" = "0"

Solution 2: XOR Operations on RF Signals

Our idea

Constructing XOR operations with RF signals' phase changes by backscattering



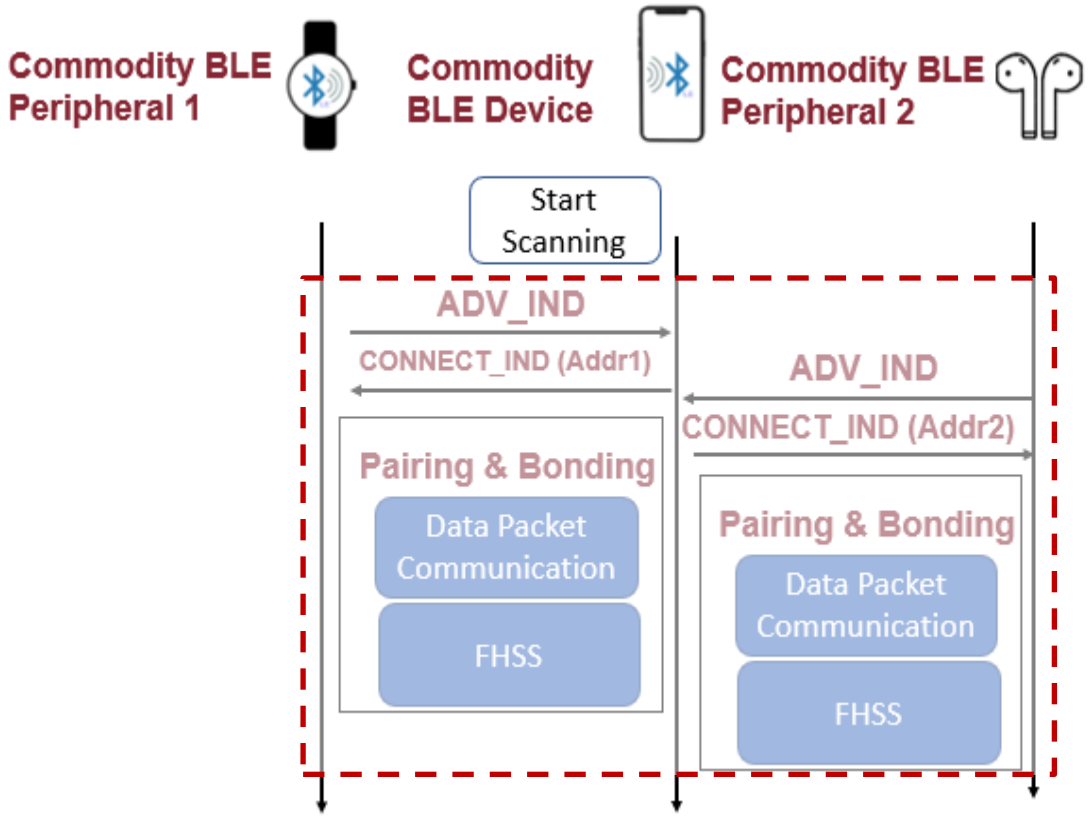
Truth Table

Input (TX)	Input (Tag)	Output (RX)
1	1	0
1	0	1
0	1	1
0	0	0

Equal to XOR operation

Challenge 3: Building Commodity-level Connection on Passive BLE Tag

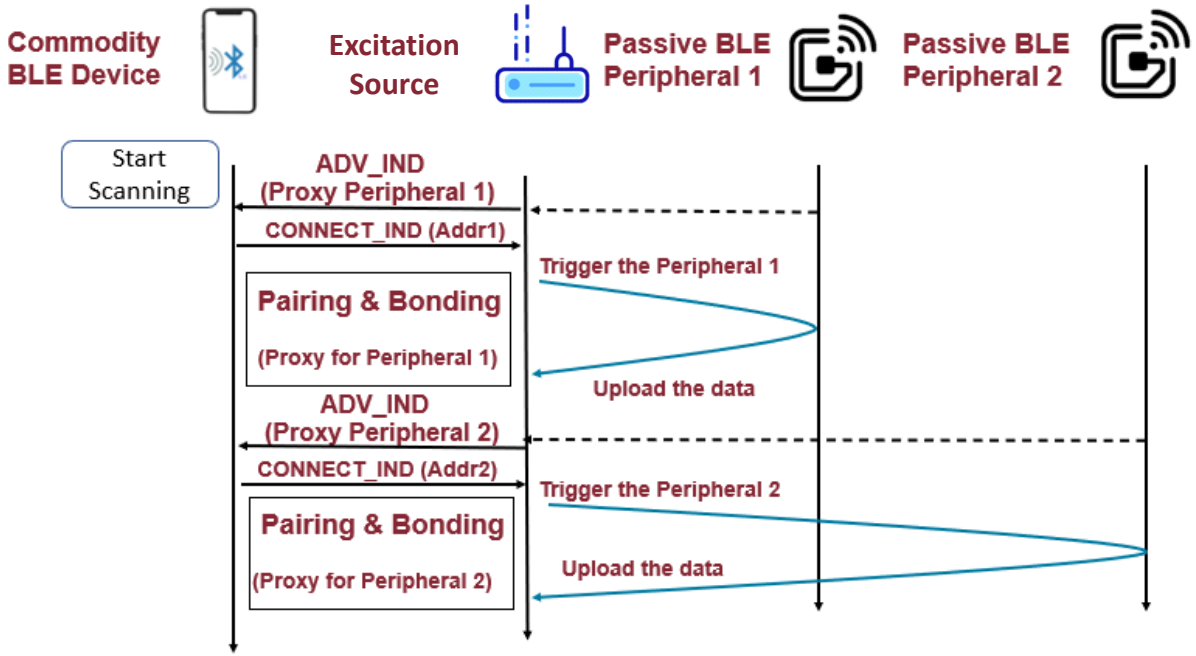
Commodity Active BLE Connection Example



Too complex for a backscatter tag

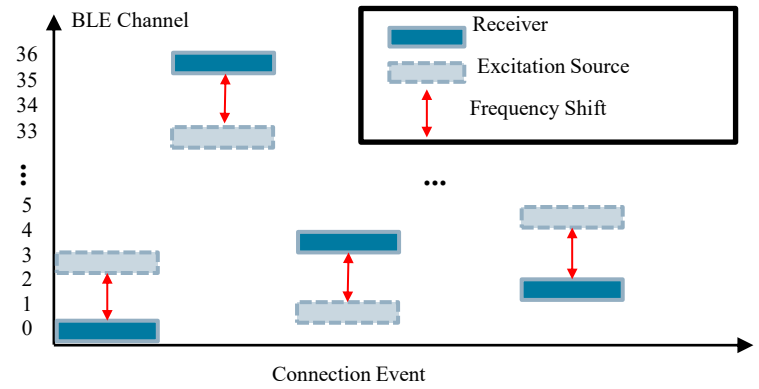
Solution 3: Excitation-source proxy connection

Commodity BLE Connection on PassiveBLE



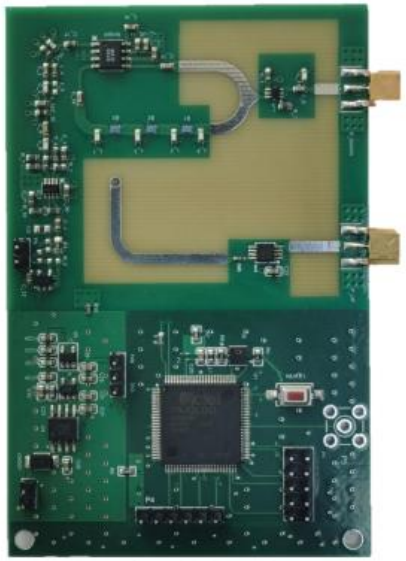
One commodity BLE helps to build and maintain multiple BLE connections with passive BLE peripherals.

FHSS Proxy

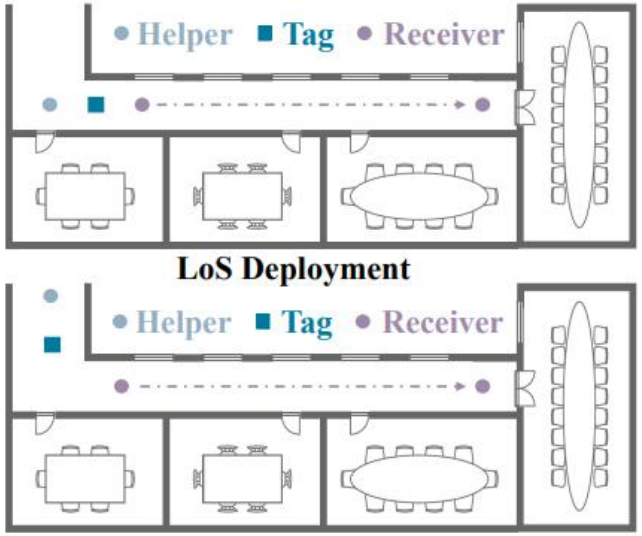


Frequency hopping on the carrier provided for PassiveBLE tags to save energy.

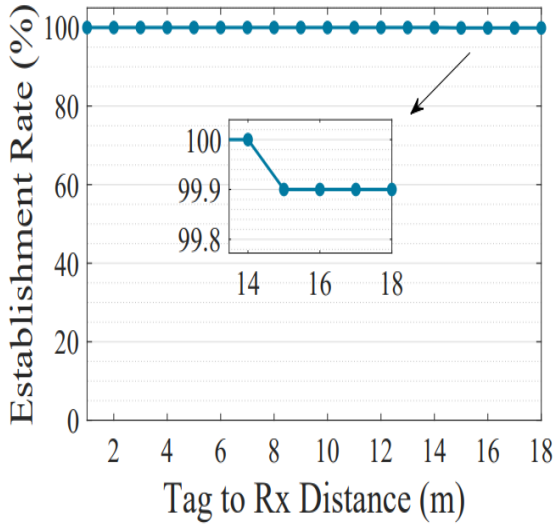
Evaluation

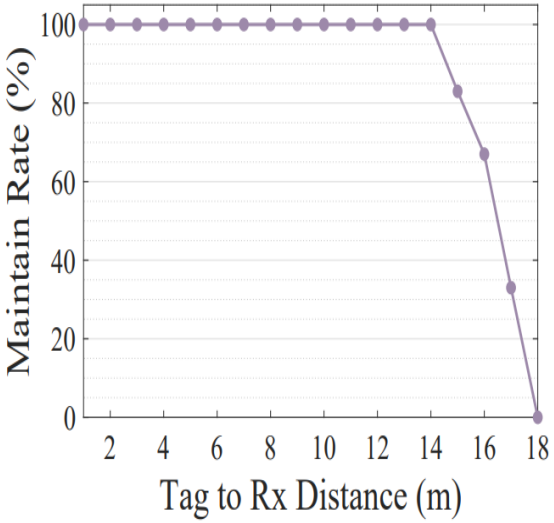


PassiveBLE Tag



NLoS Deployment

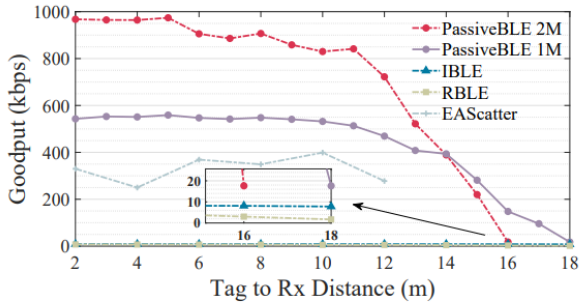




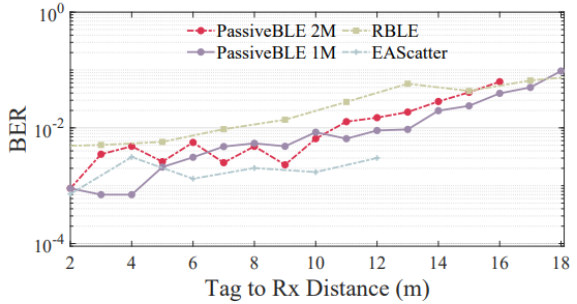
Implementation and experiment setup

PassiveBLE achieves overall 100% BLE connection establishment and maintain within 14 meters

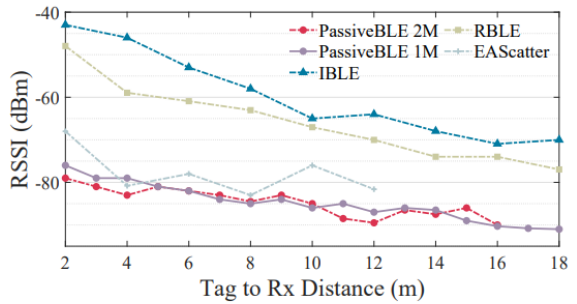
Evaluation



(a) Goodput.

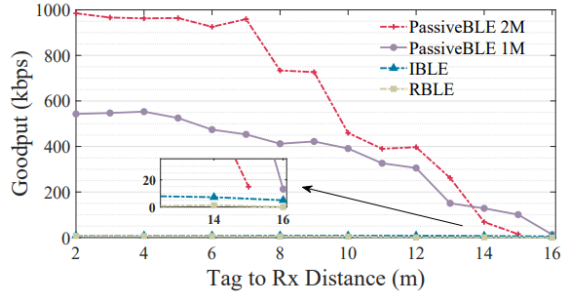


(b) BER.

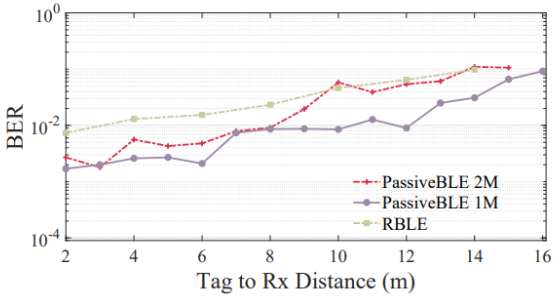


(c) RSS.

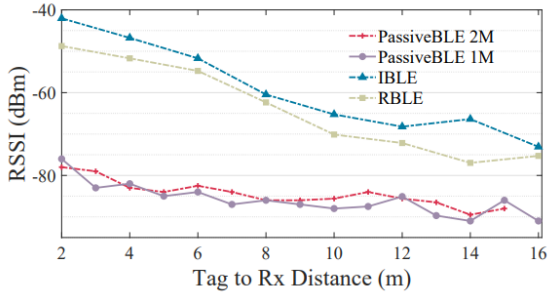
End-to-end communication performance in the LoS condition



(a) Goodput.



(b) BER.



(c) RSS.

End-to-end communication performance in the NLoS condition

PassiveBLE achieves SOTA communication performance with measured goodput up to 974kbps while maintaining BLE protocol compatible

Summary

1

Precision Synchronization Circuit

Using off-the-shelf components, our implementation achieves a sensitivity of -33 dBm with a synchronization accuracy of approximately 93 nanoseconds.

2

Distributed XOR Coding Scheme on RF signals

Enabling backscatter tags to generate standard-compliant BLE data packets without requiring knowledge of dynamic transmission parameters.

3

BLE connection compatible backscatter

We designed a specialized BLE connection scheduler that enables backscatter tags to establish and maintain BLE connections with unmodified consumer devices.

Thanks!