

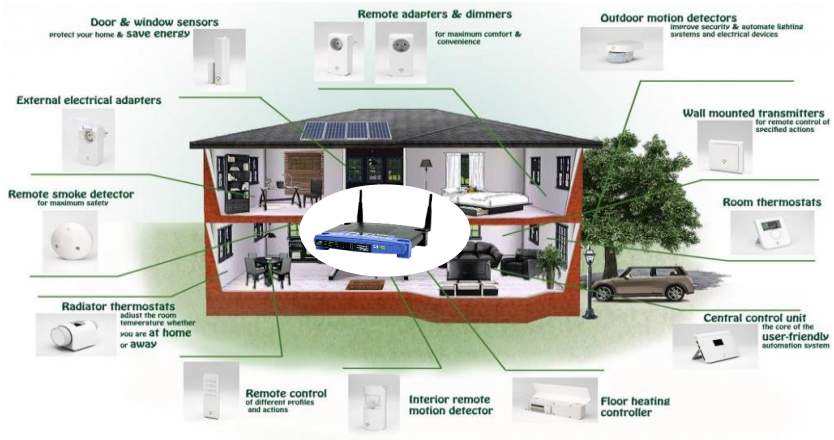

ZigFi:

Harnessing Channel State Information for Cross-Technology Communication

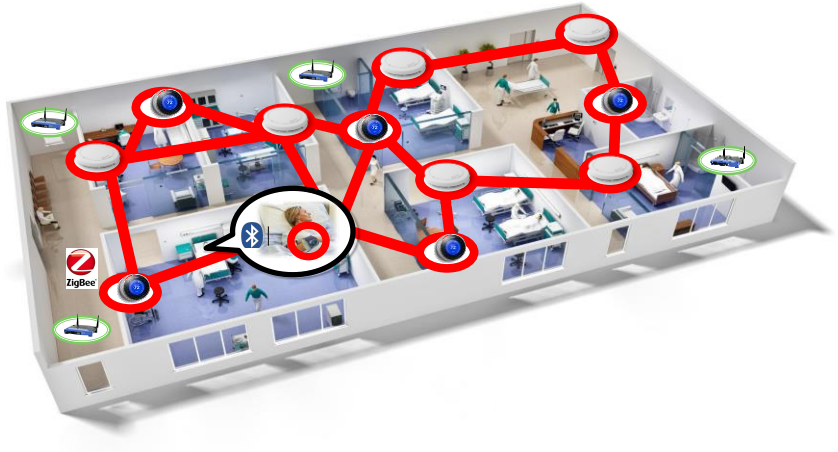
Xiuzhen Guo[1], Yuan He[1], Xiaolong Zheng[1],
Liangcheng Yu[2], Omprakash Gnawali[3]

[1]Tsinghua University
[2]KTH Royal Institute of Technology
[3]University of Houston

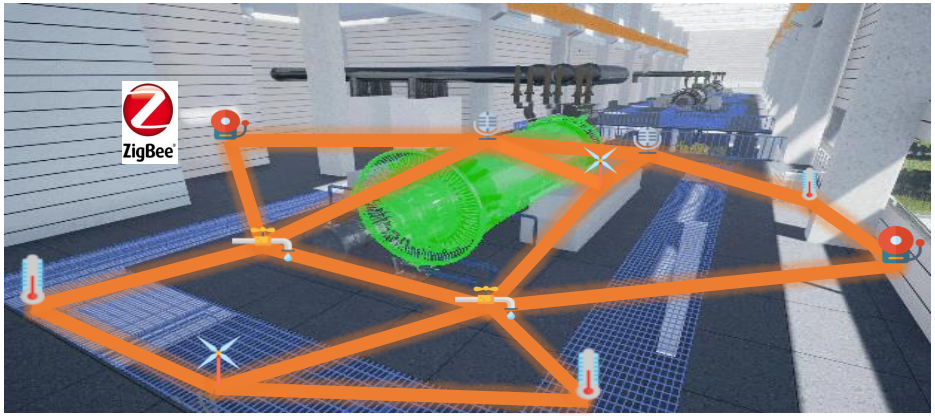
Wireless is everywhere



Smart Home

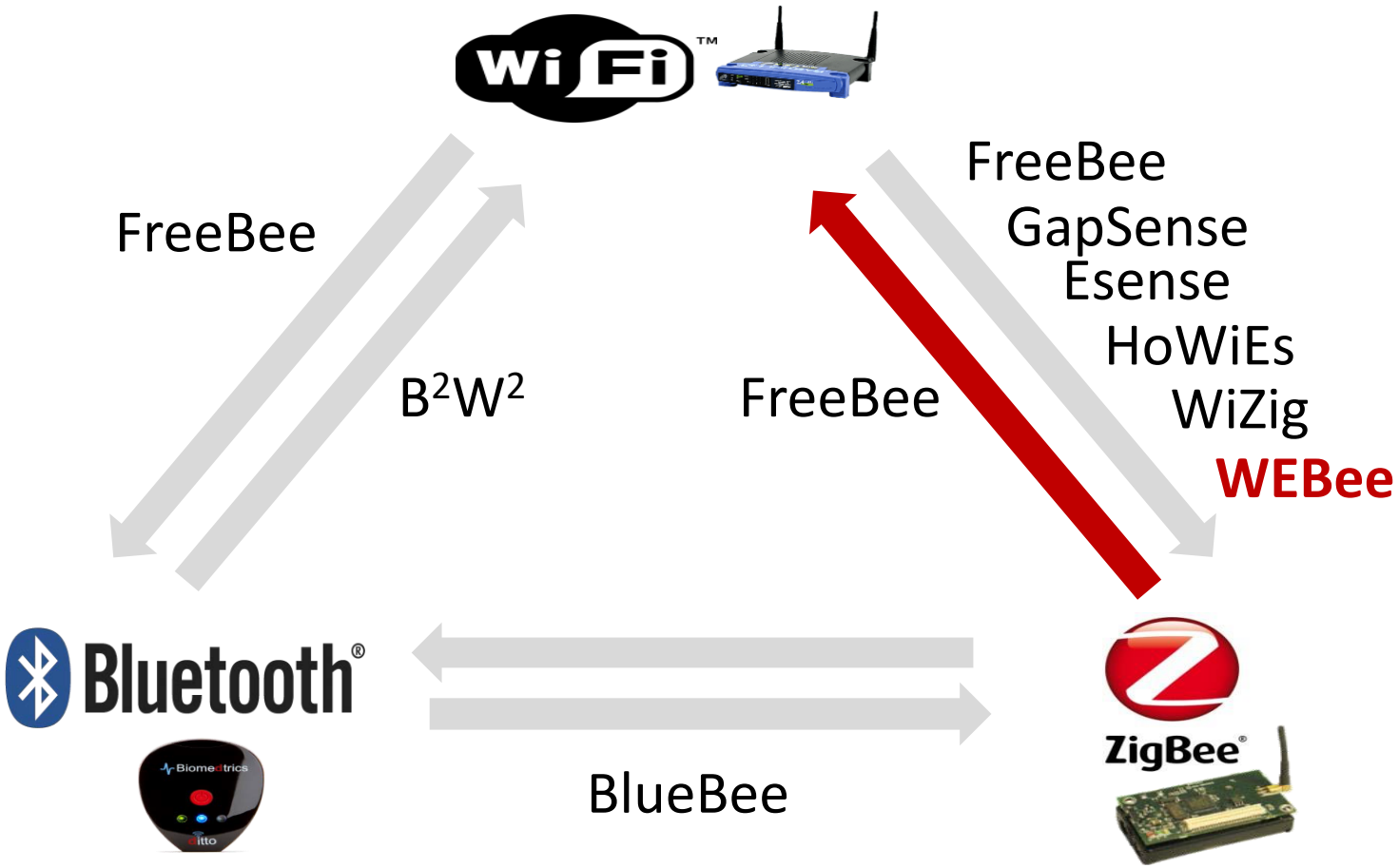


Smart Hospital



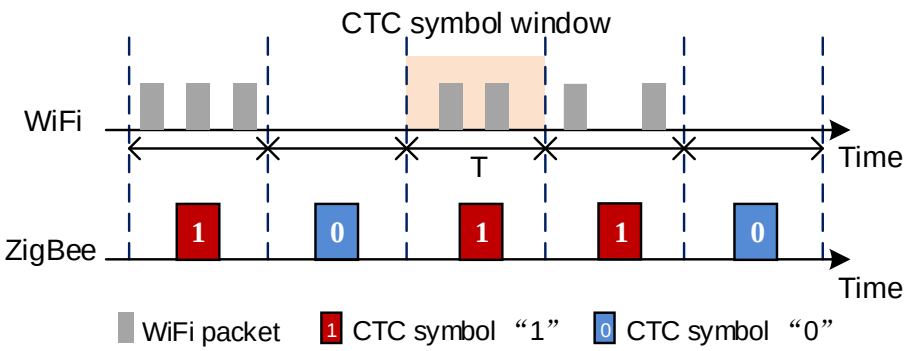
Smart Factory

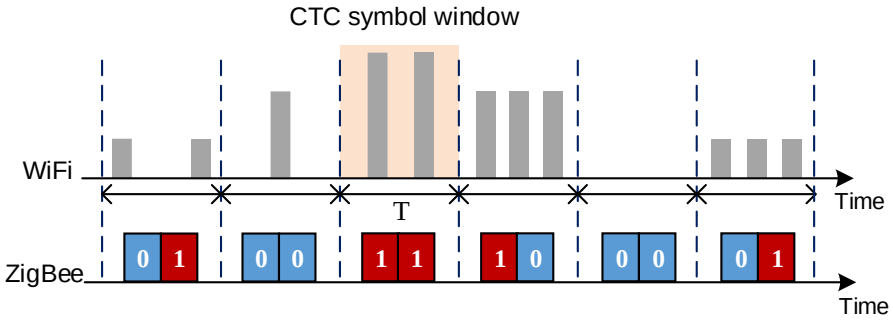
CTC among different technologies



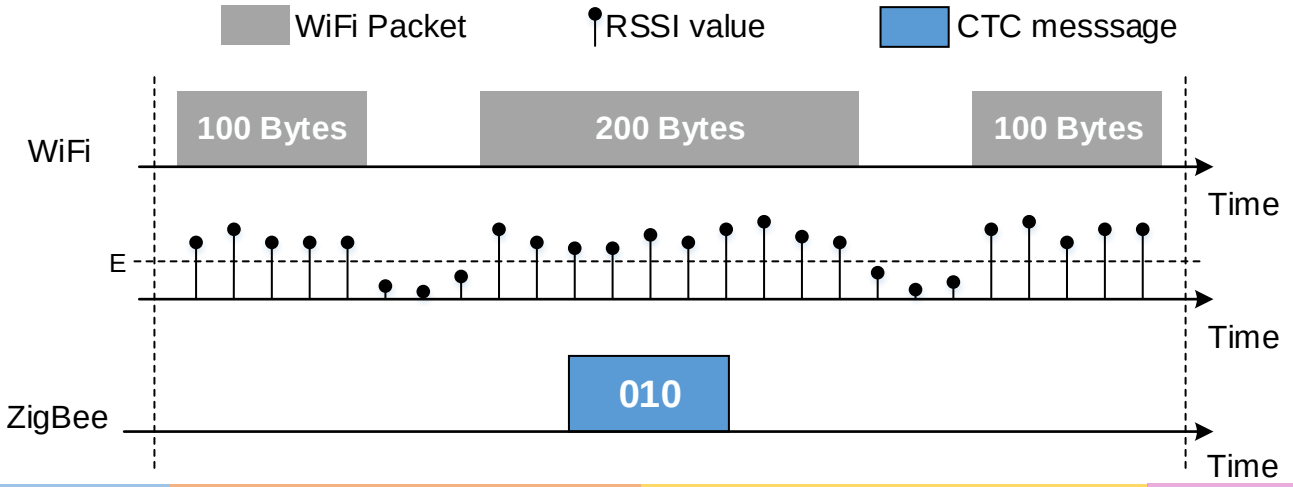
The state of the art

- Packet Energy: WiZig [Infocom'17]



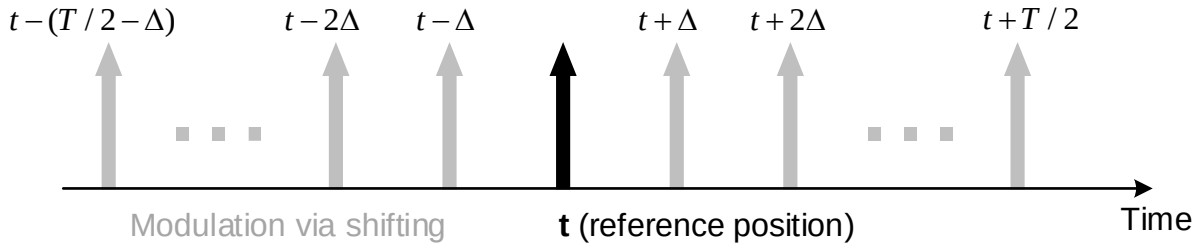


- Packet Size: Esense [MobiCom '09], HoWiEs [Infocom '13]

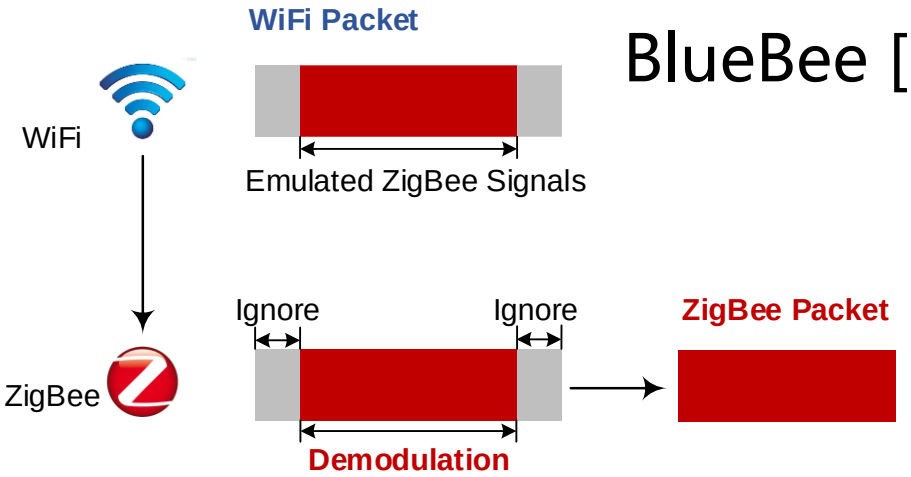


The state of the art

- Packet Transmission Timing: FreeBee [MobiCom ’15], Gap Sense [Infocom ’13]



- Physical Signal Emulation: WEBee [MobiCom ’17], BlueBee [SenSys ’17]

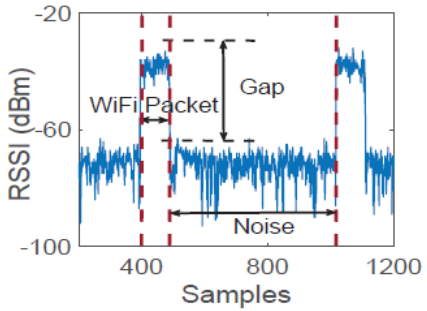


Challenges

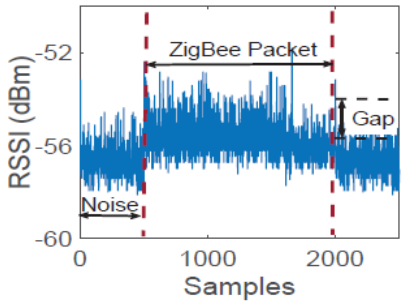
ZigBee

Bandwidth: 2M
Rate: 250Kbps
Modulation: OQPSK, DSSS
Tx: 0dBm

Using RSSI is inefficient

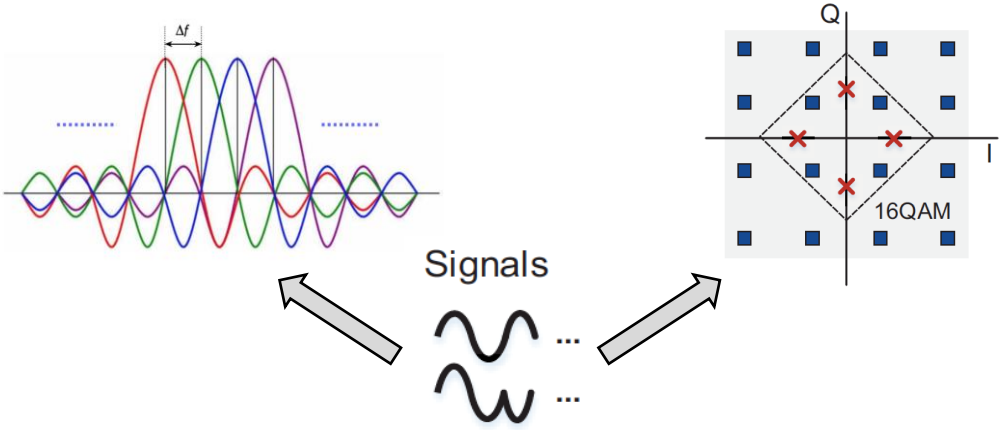


(a) WiFi RSSI



(b) ZigBee RSSI

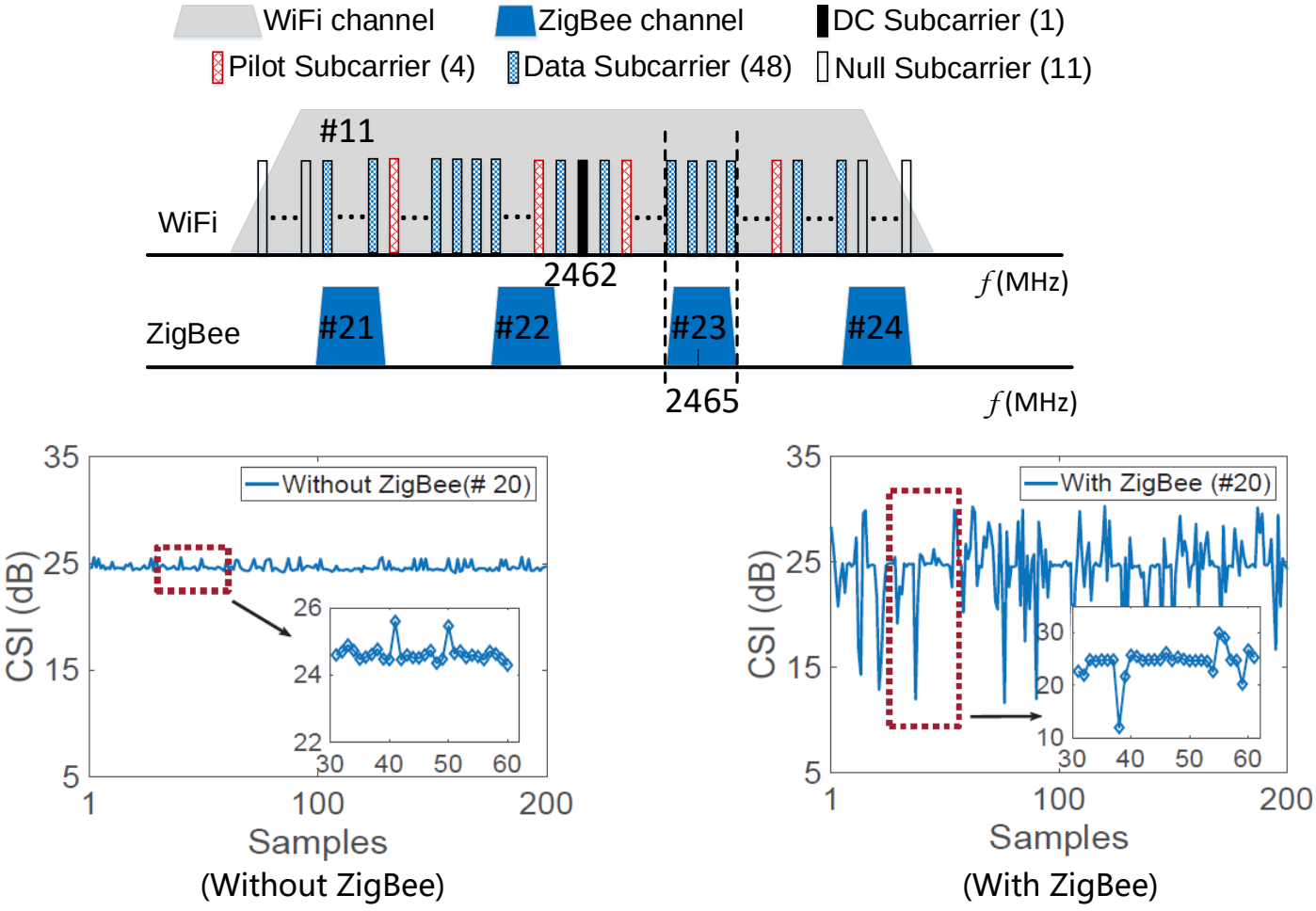
Directly decoding is difficult



Bandwidth: 20M
Rate: 54Mbps
Modulation: QAM, OFDM
Tx: 20dBm

Physical emulation is infeasible

Feasibility of using CSI



(Without ZigBee)

(With ZigBee)

The transmission of ZigBee packets affects the CSI significantly

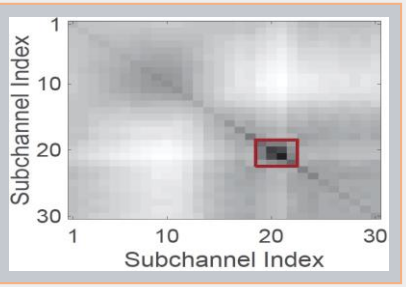
Challenges of using CSI

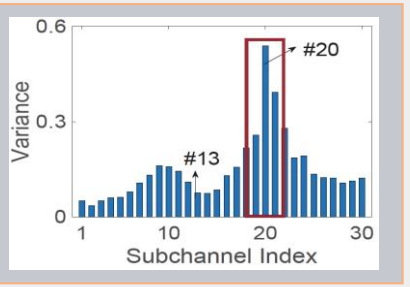
- **Frequency** domain:
  Select a proper subchannel

- **Time** domain:
  ZigBee length satisfies a threshold

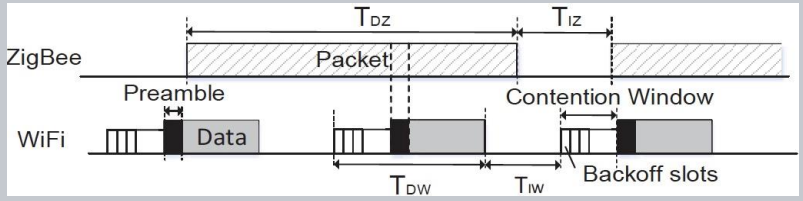
- **CSI** sequence:
  Choose an appropriate ZigBee power

#Subchannel

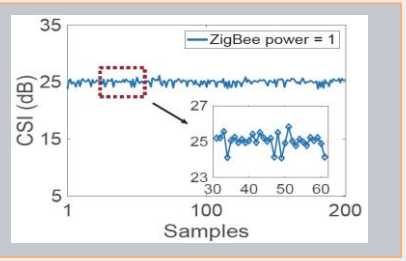


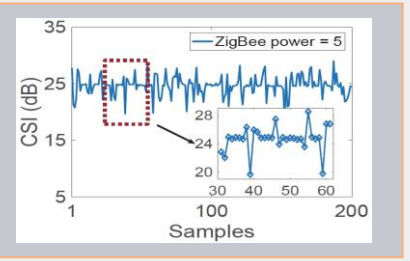


#Packet Length



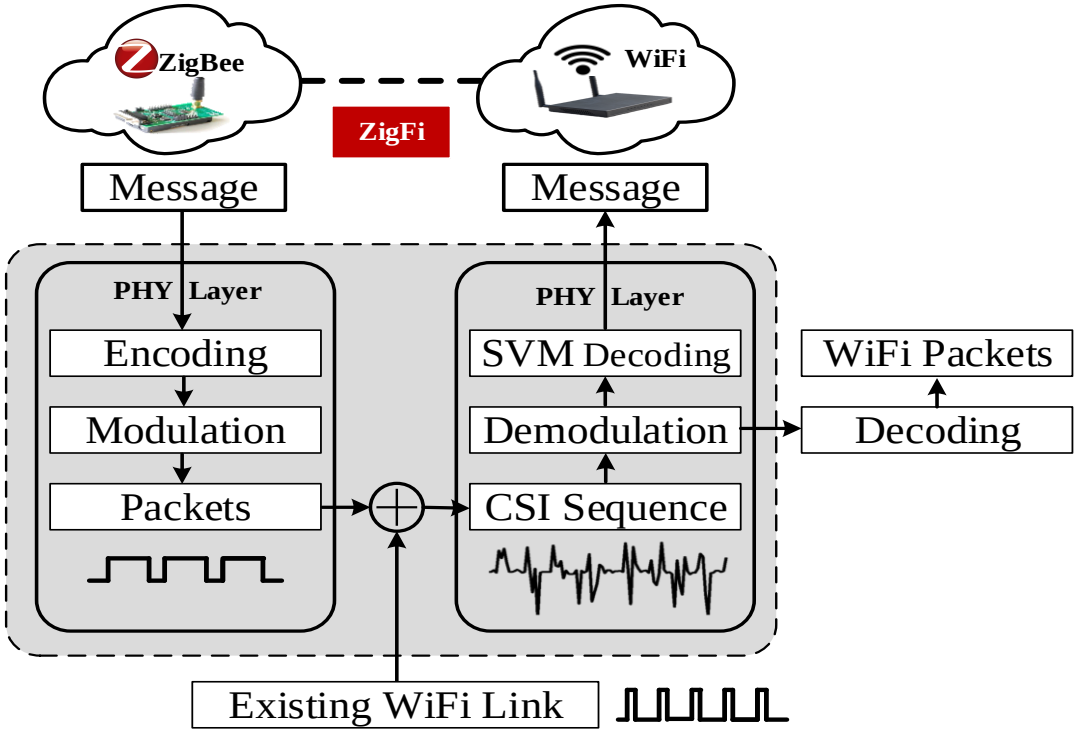
 # Transmission Power





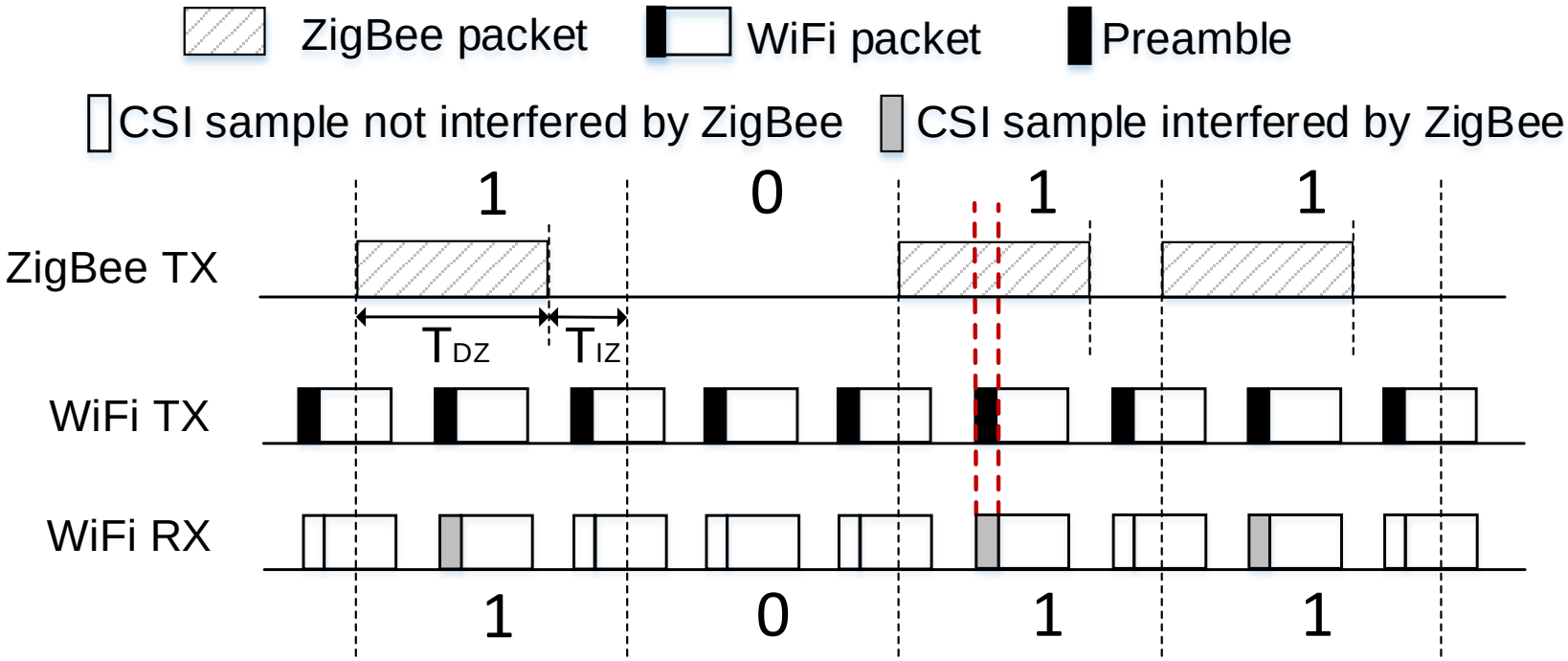
ZigFi: Harnessing CSI for CTC

- ZigBee packets piggy-backed to the existing WiFi link
- WiFi receiver collects two sets of information
- SVM classification



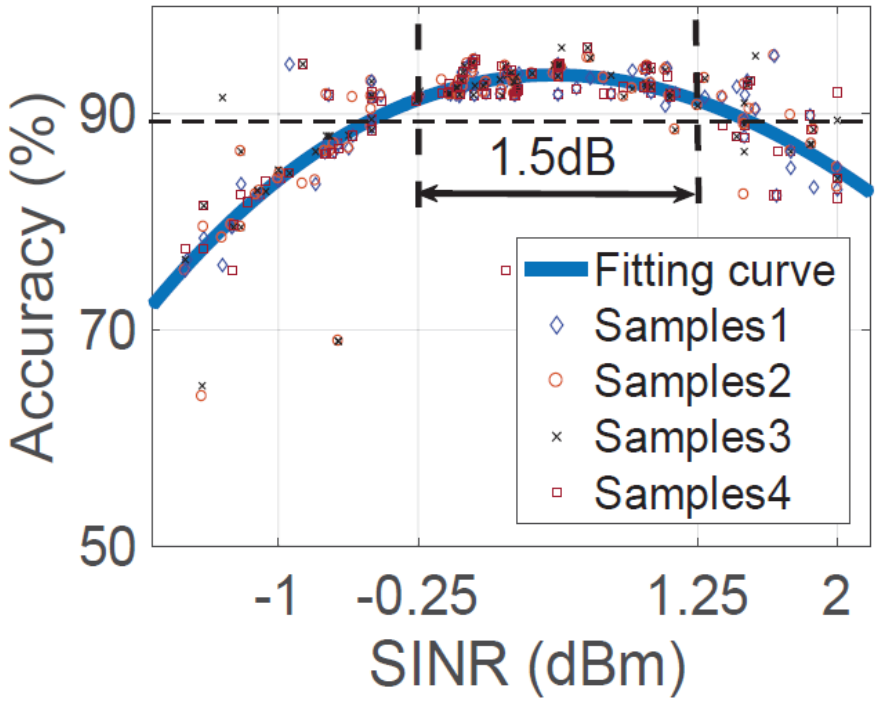
Encoding and decoding

- Encoding: Presence or absence of ZigBee packets
- Decoding: SVM identifies the interfered CSI sequence



SINR in ZigFi

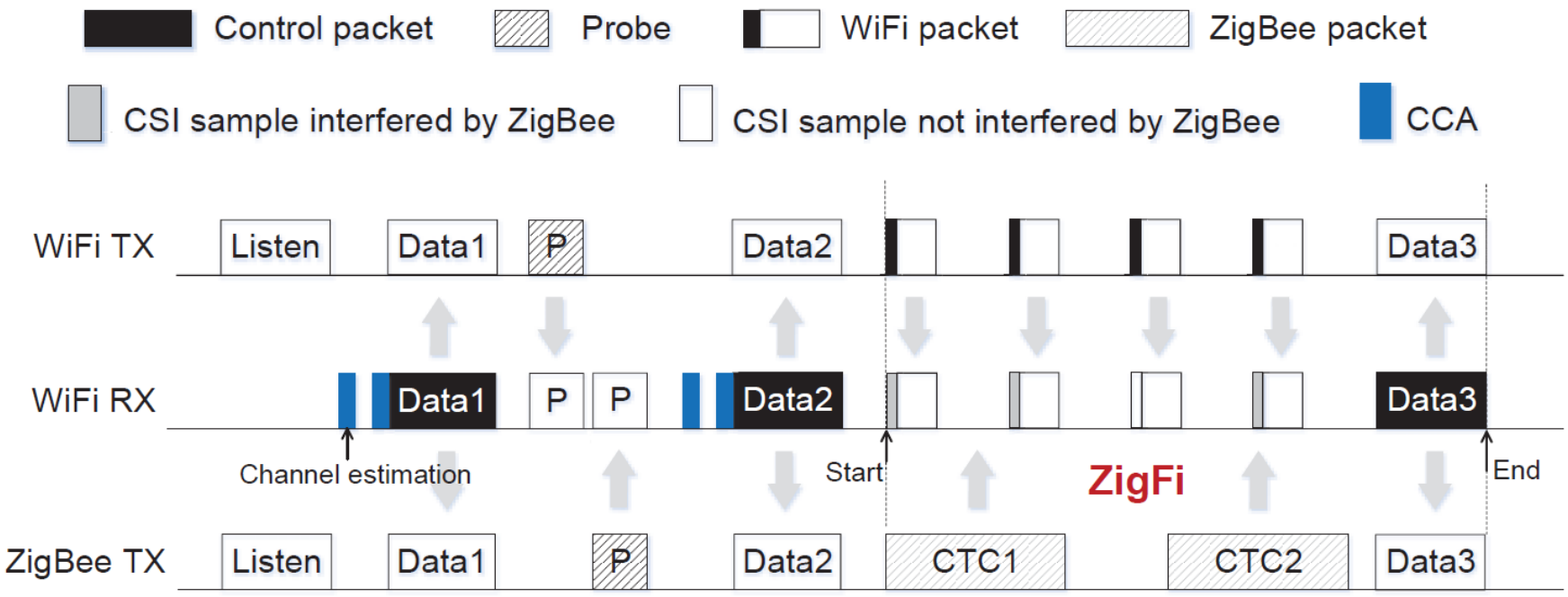
$$SINR = 10lg\frac{S_Z}{I_W + N}$$



SINR in range [-0.25,1.25], decoding accuracy > 0.9

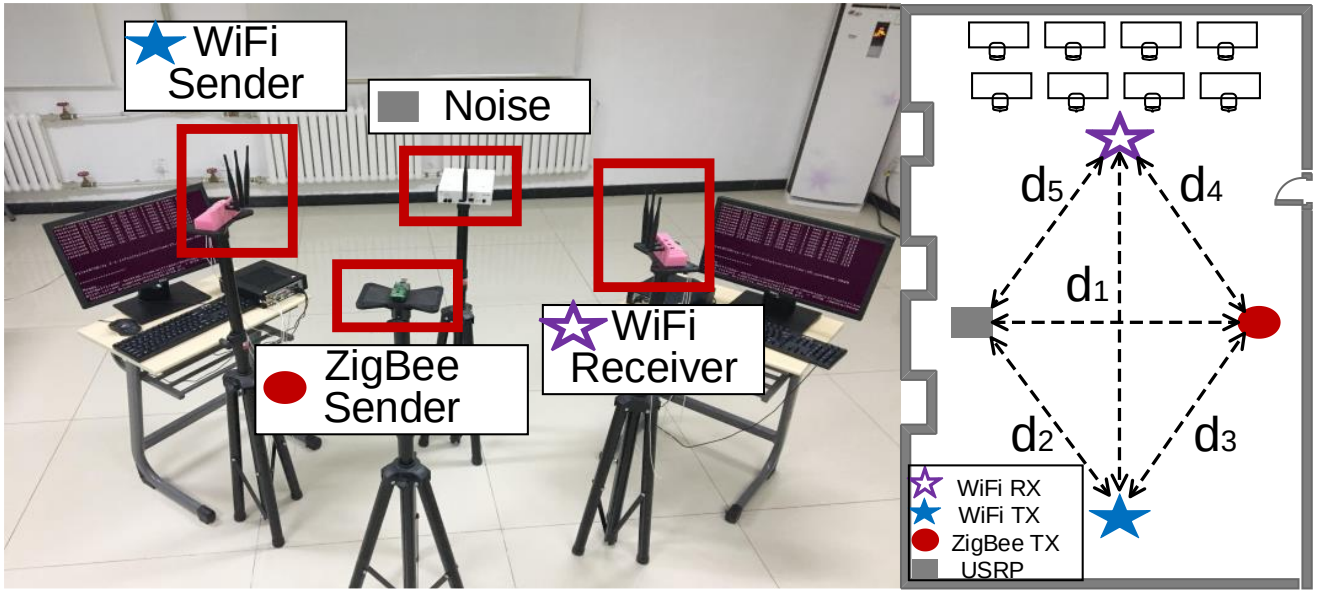
The Receiver-initiated mechanism

- Establish a **WiFi link**
- Obtain an appropriate **SINR**

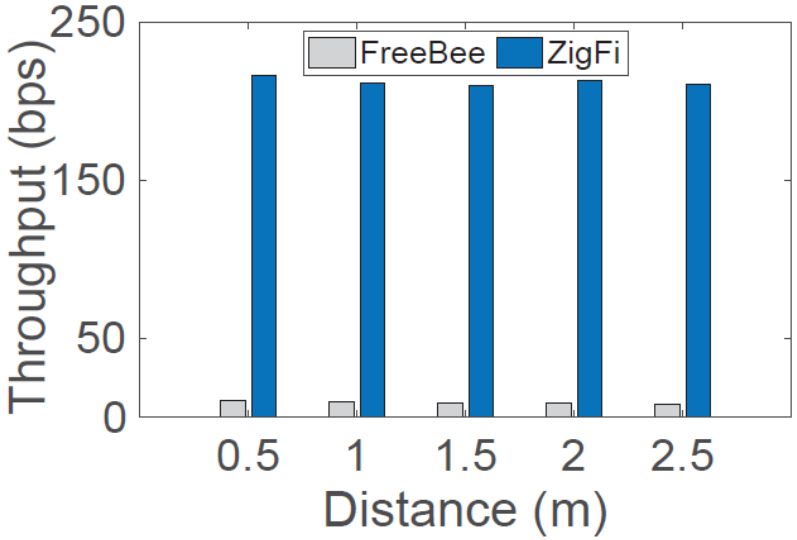


Evaluation

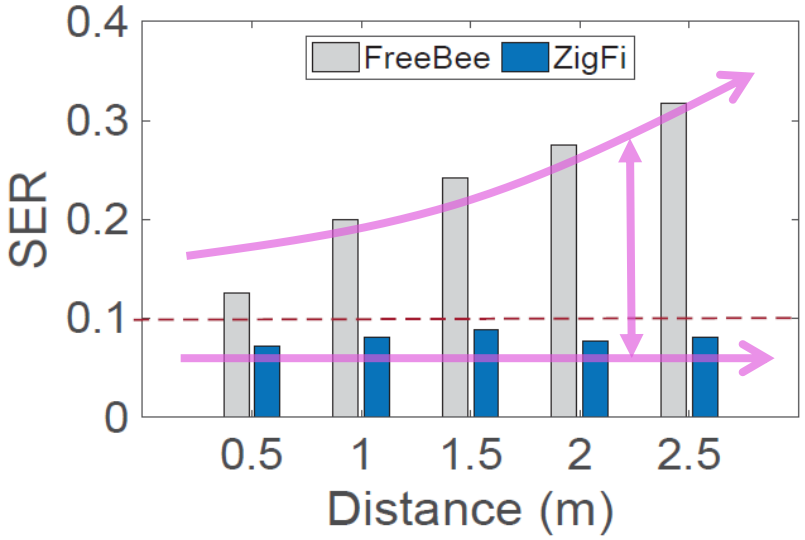
- WiFi: Commercial WiFi device + CSITool, channel 11
- ZigBee: TelosB mote, channel 23
- Noise: USRP generator
- Metrics: Throughput and SER



ZigFi vs. FreeBee



(a) Throughput

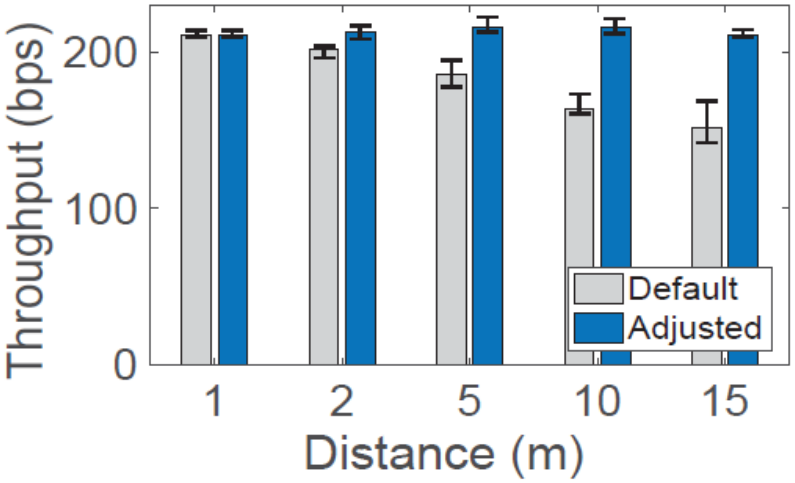


(b) SER

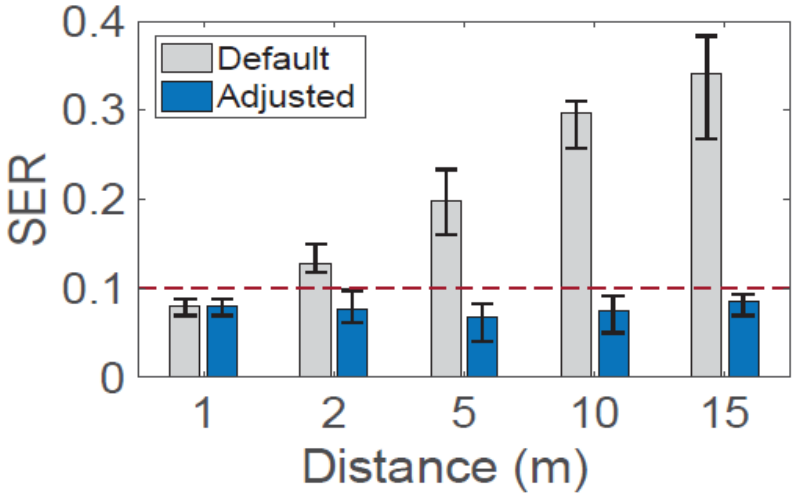
ZigFi shows significant enhancement over FreeBee in terms of throughput and SER.

Distance

- The ZigBee Tx and the WiFi Rx



(a) ZigFi Throughput

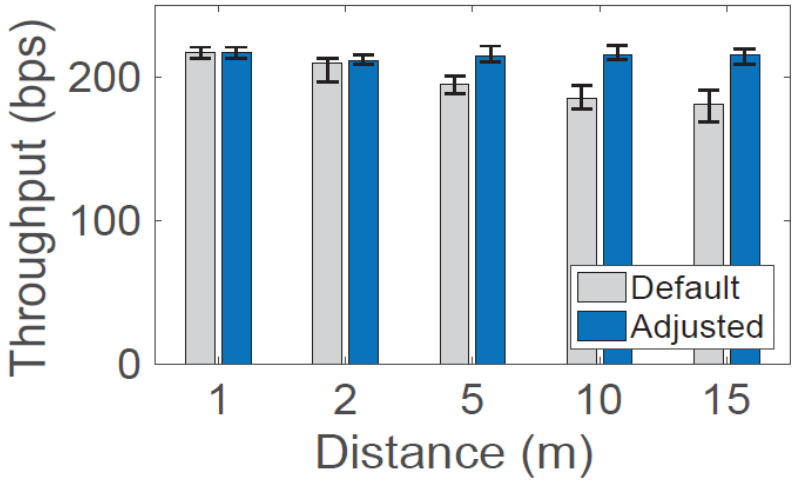


(b) ZigFi SER

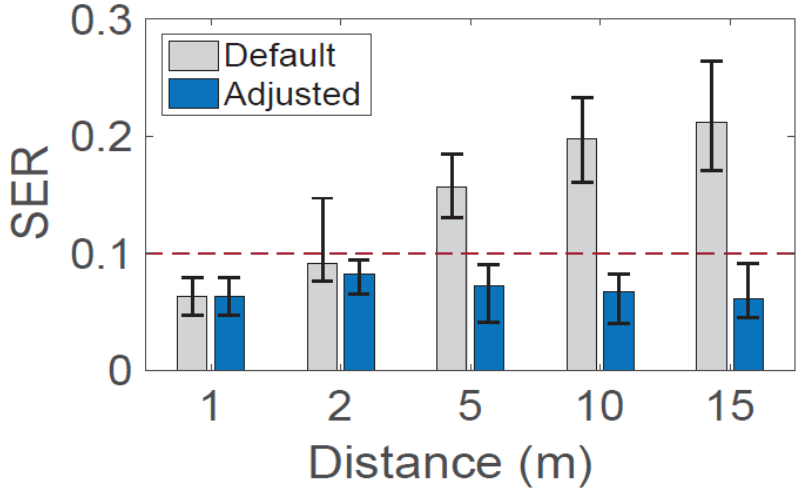
Adaptive is better than default.
ZigFi performs well under the adaptive mode.

Distance

- WiFi Tx and the WiFi Rx



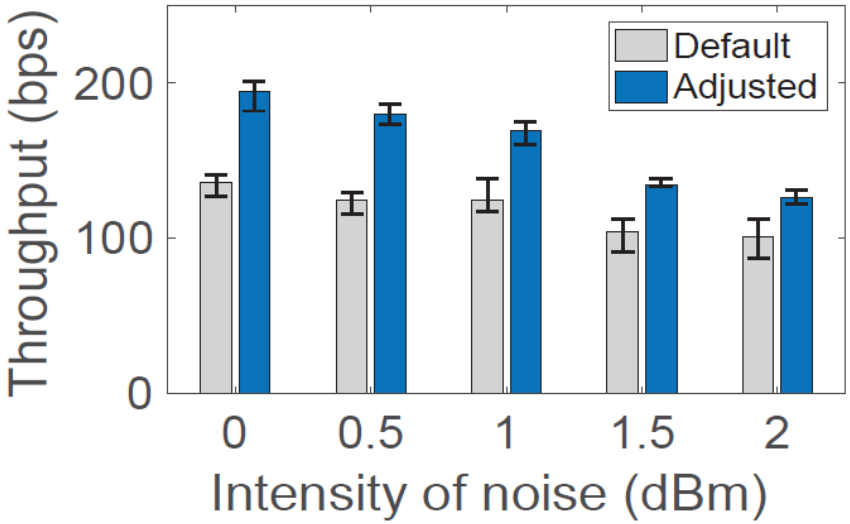
(a) ZigFi Throughput



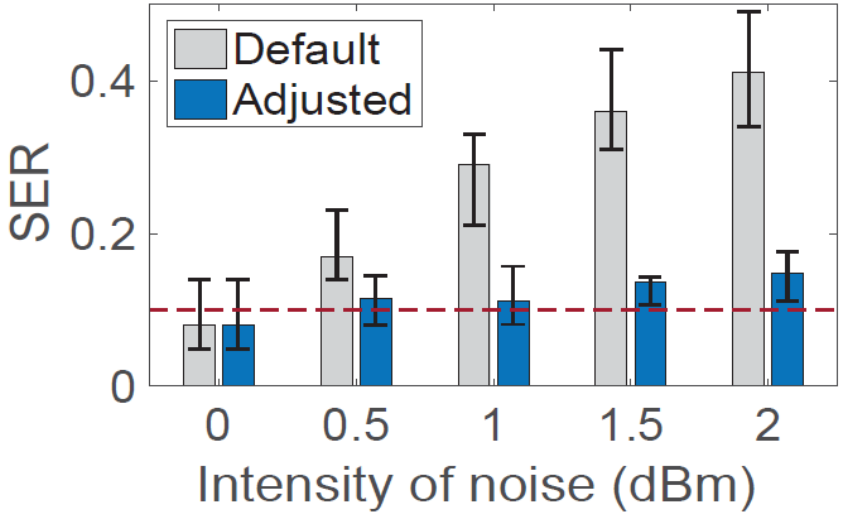
(b) ZigFi SER

Adaptive is better than default.
ZigFi in the adaptive mode performs well.

Noise



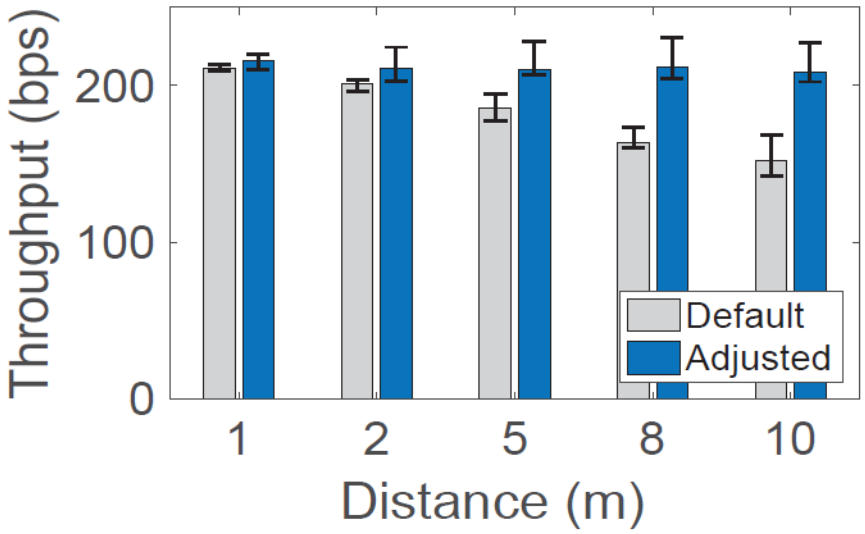
(a) ZigFi Throughput



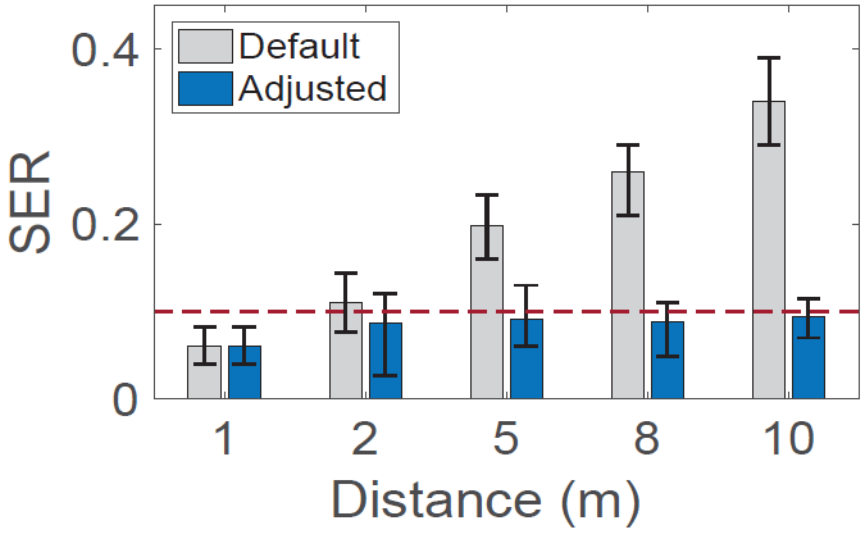
(b) ZigFi SER

Throughput of ZigFi degrades with noise intensity increases. ZigFi in the adaptive mode is more resilient to noise.

NLoS Scenario



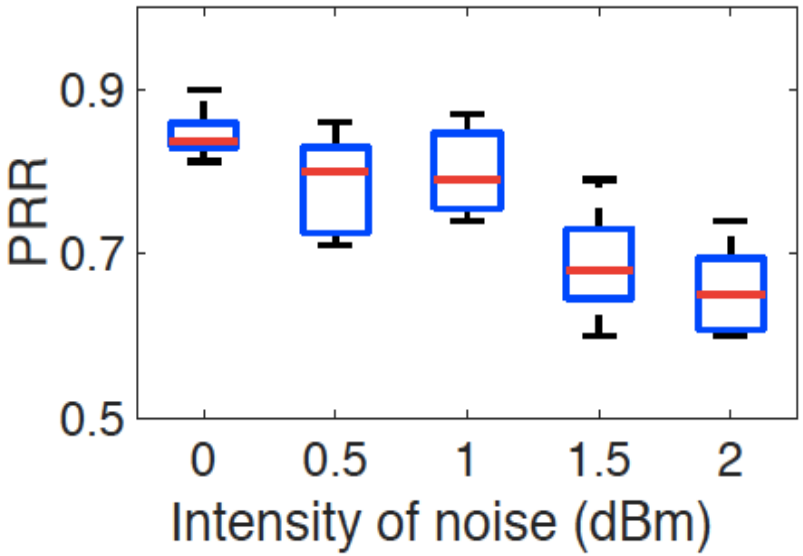
(a) ZigFi Throughput



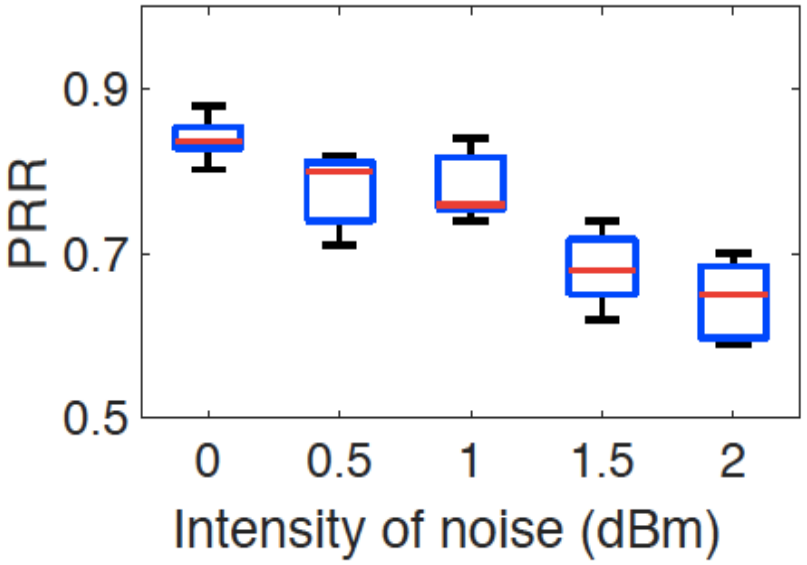
(b) ZigFi SER

ZigFi in the adaptive mode is robust under NLoS scenario

The impact on the WiFi communication



(Without ZigFi)



(With ZigFi)

ZigFi has limited impact on the WiFi communication

Summary

- We harness **CSI as a side channel** to achieve CTC from ZigBee to WiFi and translate the decoding problem into a CSI classification problem.
- We design a **receiver-initiated protocol** for practical application of ZigFi.
  - Proper subchannel
  - Appropriate packet length
  - Suitable transmission power
- Experimental results show that ZigFi achieves **efficient and robust CTC**.


Q&A

Thanks

guoxz16@mails.Tsinghua.edu.cn