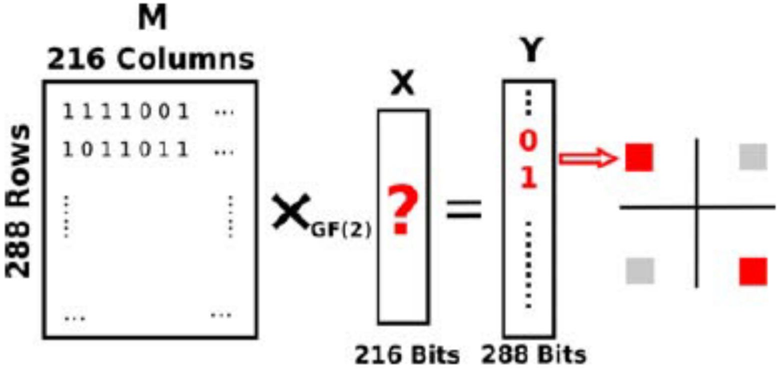
WEBee

Reverse Convolution Coding



$$M \times_{GF(2)} X = Y$$

Reverse Convolution Coding

- Convolutional encoding uses a 288-by-216 matrix M
  - M is not full row-rank (row:288 > column:216), the matrix equation is an overdetermined system
- ZigBee signals occupy only a 2MHz band, covering 7 WiFi subcarriers.
  - To emulate ZigBee signals, WEBee needs to control only 7 WiFi QAM points

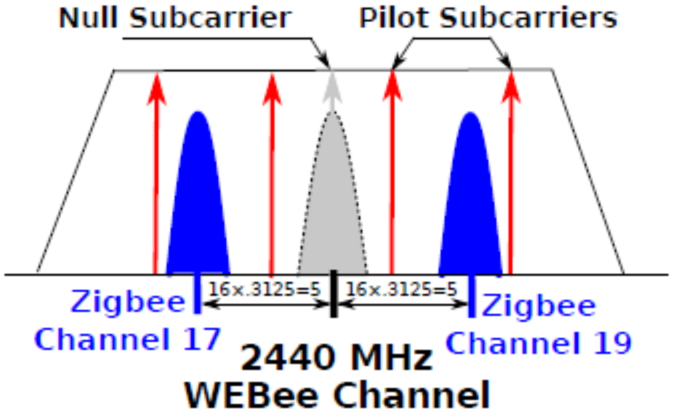
Reverse Convolution Coding

- WEBee needs to control only 84 bits (14 ×6 bits) of Y by manipulating the X

$$M' \times_{GF(2)} X = Y'$$

- M’ a full row-rank matrix (row:84 < column:216)
  - WEBee can emulate an arbitrary combination of 14 QAM points with 216 source bits in multiple ways.

NULL subcarrier Avoidance



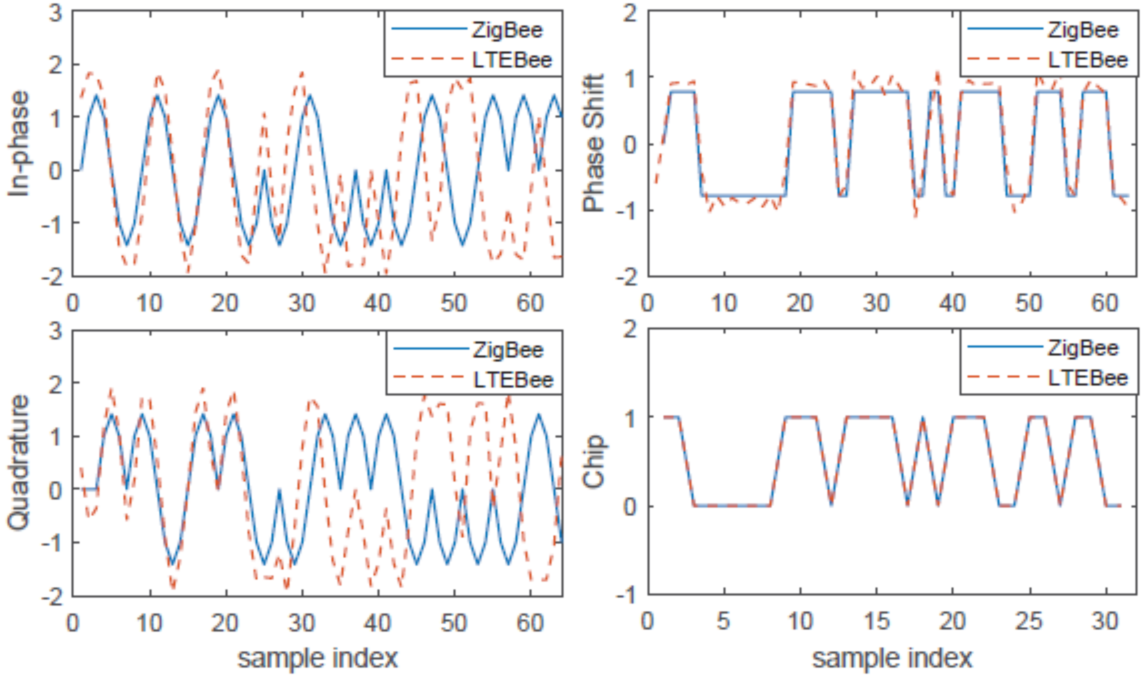
- Central frequency of a WEBee channel is set so there are ZigBee channels which do not overlap with the Null subcarrier

Cyclic Prefixing (CP):

- WiFi cyclic prefixing,
  - a technique to eliminate inter-symbol interference (ISI).
  - A guard interval lasting 0.8*μs in each WiFi symbol* is copied from the right of WiFi symbol and pasted into (overwrite) the left of the symbol
  - we have a segment of signals with 0.8*μs duration* which is *out of our control in signal emulation*
- Direct Sequence Spread Spectrum (DSSS)
  - Multiplying original bits with a pseudo random noise spreading code
  - ZigBee symbol (i.e., 4-bits) are mapped into a 32-chip sequence
  - 12 chip errors can be recovered by the Zig-Bee DSSS technique
- Due to the use of DSSS error due to CP can be tolerated by the ZigBee symbol

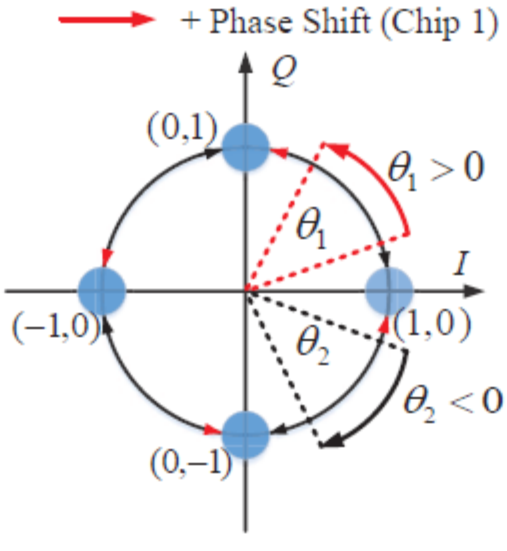
LTEBee

- Digital emulation vs analogue emulation
  - – do not need to generate the exact waveform in the time domain.



LTEBee

- ZigBee uses OQPSK,
  - phase shifts between two samples, instead of the values of these samples used to demodulate.
  - phase shifts quantized based on their signs



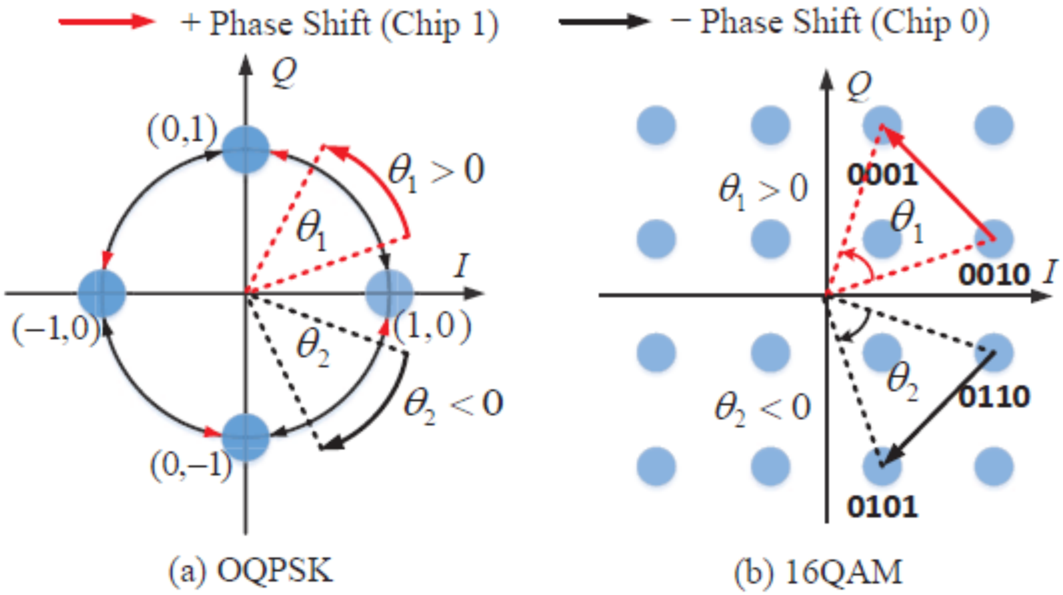
(a) OQPSK

LTEBee

- 16QAM can not generate exact 90 or -90 phase shifts
- It can generate the phase shifts with the right signs.

LTEBee

- Transition from ’0010’ to ’0001’ generates the phase shift of Q1
- Will be demodulated as chip 1 correctly,
  - despite not strictly following ZigBee’s analog signal.



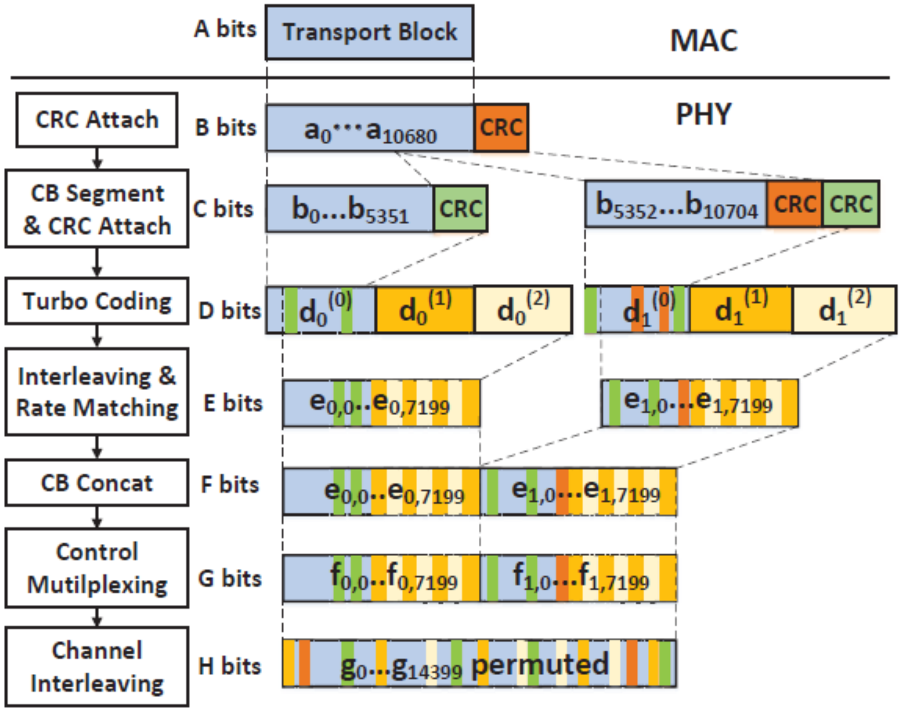
(a) OQPSK

(b) 16QAM

LTEBee

- Re-sample the entire target ZigBee signal with the LTE sample rate
- Calculate the phase shifts for these samples
- Allocate 16QAM constellation to these sample
    - generated LTE signal and target ZigBee signal have the same signs for phase shifts at all of these sample intervals.

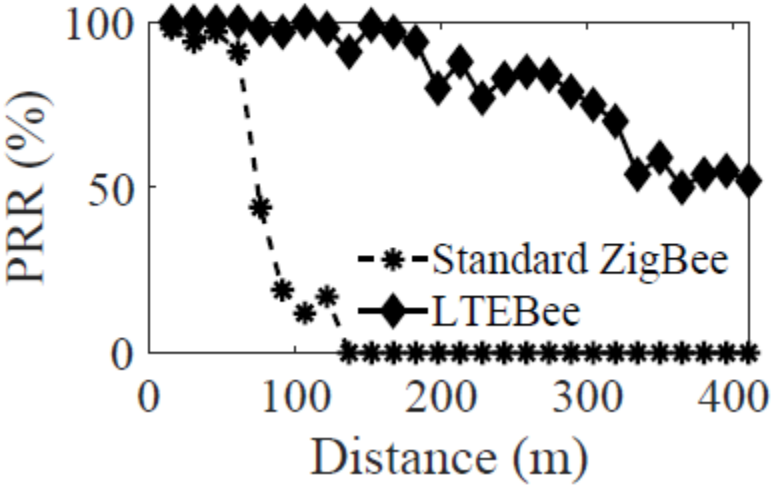
- Reverse engineer channel (Turbo) coding to get IP payload
  - Matrix Inversion



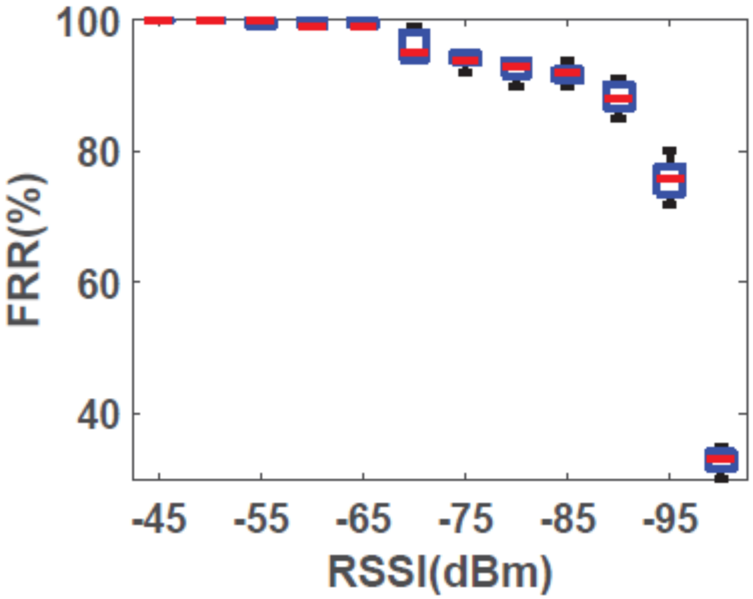
Sources of error

- Subcarrier Mapping
  - distorts original signal, and we cannot obtain desired phase shift pattern
  - pre-processes the sequence cancels out the impacts of the frequency exchange effects
- Uncontrollable CRC in turbo encoding
- Uncontrolled Header Bits

- Range Extension



- Robustness


FRR(%)
RSSI(dBm)