PACKETCRAFT®
WORLD-LEADING WIRELESS

Analysis of Bluetooth Channel Sounding

A New Bluetooth Feature for High Accuracy Distance Measurement

John Yi | CEO | Packetcraft

Agenda

- Intro
- Use Cases
- Concepts
- Link Layer
- Analysis
- Summary

Intro

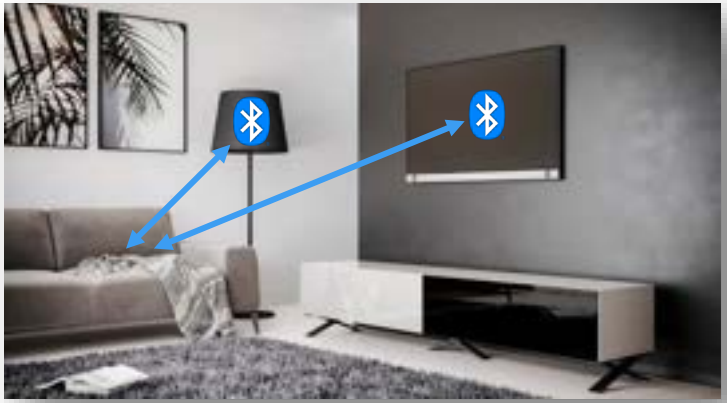
John Yi architected and implemented the Bluetooth LE Link Layer since v4.0 and participates in the Bluetooth Core Working Group for about 15 years.

Use Cases

- Applications
  - Secure Access, e.g., car, building
  - Real-Time Location System (RTLS), e.g., asset management, warehouse
  - Indoor Positioning System (IPS)

- Device Requirements
  - Single antenna, but works better with more paths
  - Low complexity reflector (initiator runs algorithm)
  - Operates at typical walking speed

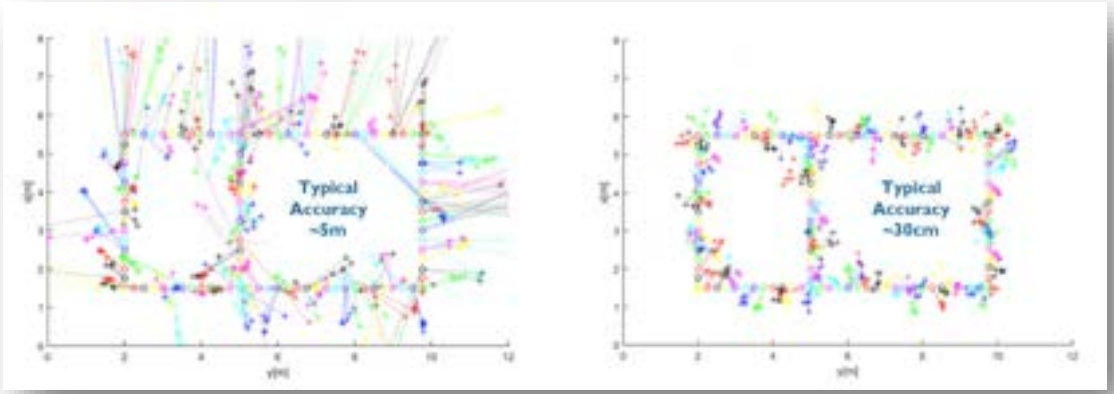
"Hey Siri, Where are my keys?"



"It's in the living room,"
"7 feet from the TV."

Use Cases – Accuracy

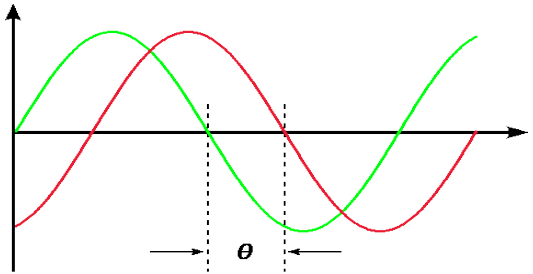
- Proximity Detection
- Accuracy ~30-cm



Credit: Imec

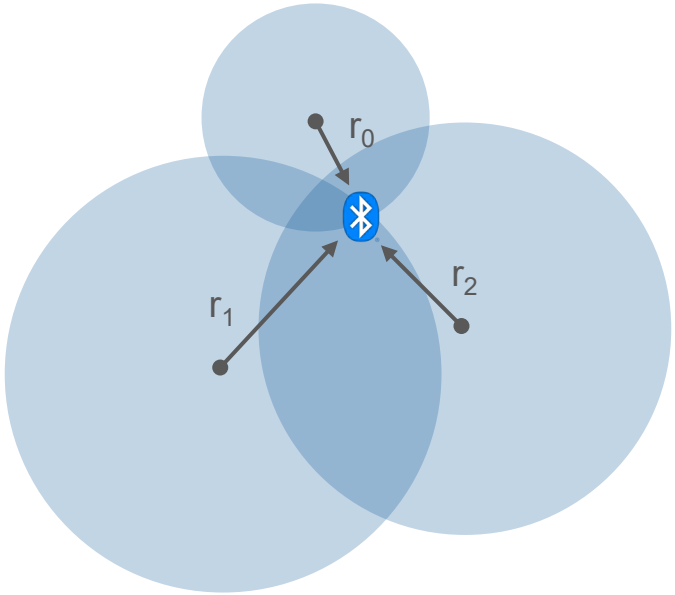
Concepts – Multipath

- RF impairment due to signal reflections, diffractions, and scattering
- Arrival at the receiver appears to have a longer path
- Dependent on frequency



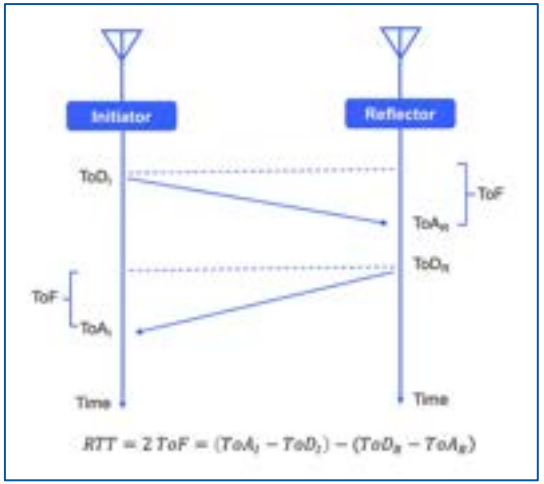
Concepts – Trilateration

- A moving device calculates is position using distance (r_x) from three fixed location devices
- Example: mobile devices can find indoor position using Bluetooth Beacons today with an accuracy of 4 meters under certain environmental conditions



Concepts – Round Trip Time (RTT)

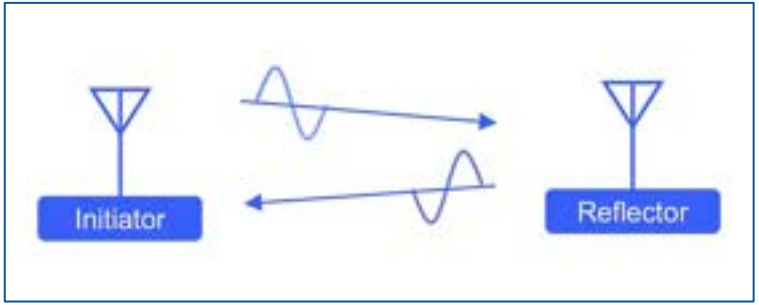
- Time of Flight (ToF)



Credit: Silicon Labs

Concepts – Phase-Based Ranging (PBR)

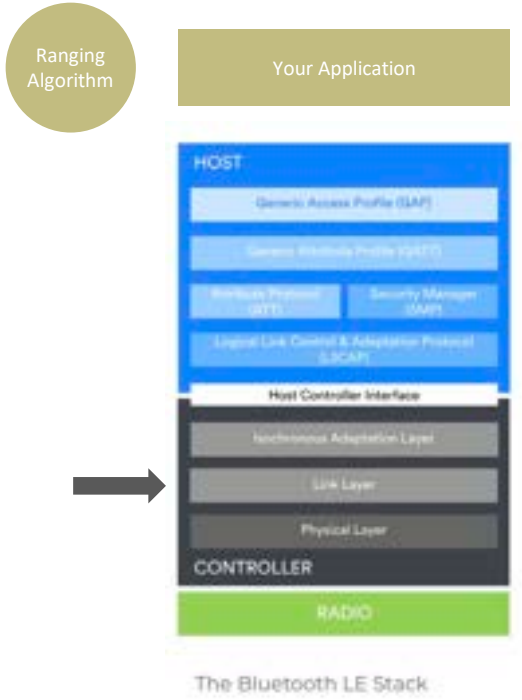
- Phase differences
- Amplitude
- More accurate than RTT



Credit: Silicon Labs

Link Layer – Context

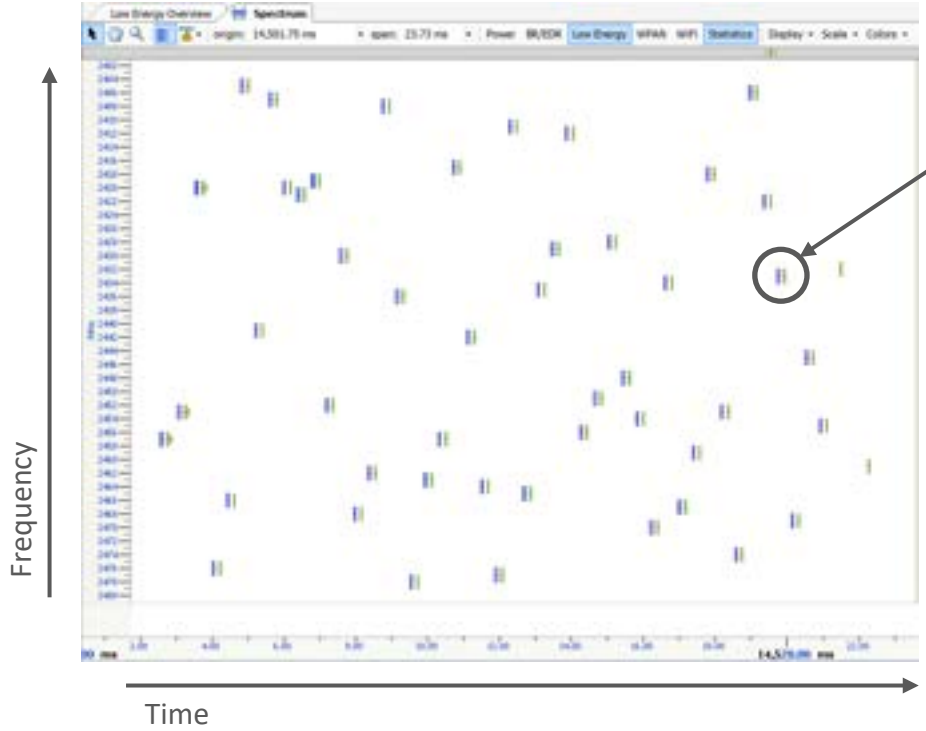
- Transports
  - Connectionless (Broadcast): ADV, PA, PAWR, BIS
  - Connection Oriented (Peer-to-Peer): ACL, CIS, CS
- Medium Access
- State Machines



The Bluetooth LE Stack

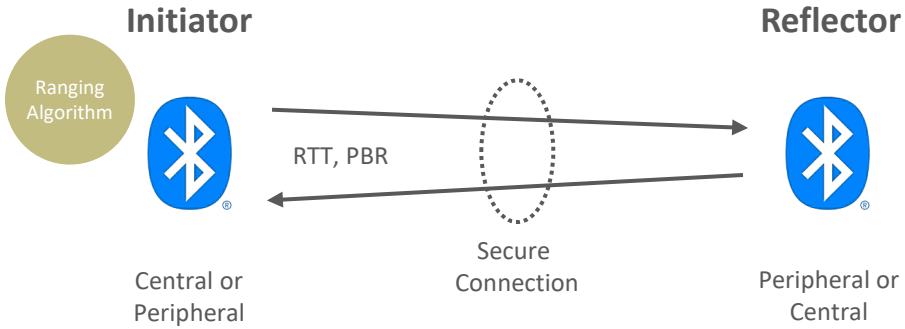
Link Layer – Communication Fundamentals

- Time
- Space – Frequency
- Coding – Access Address
- Modulation – PHY



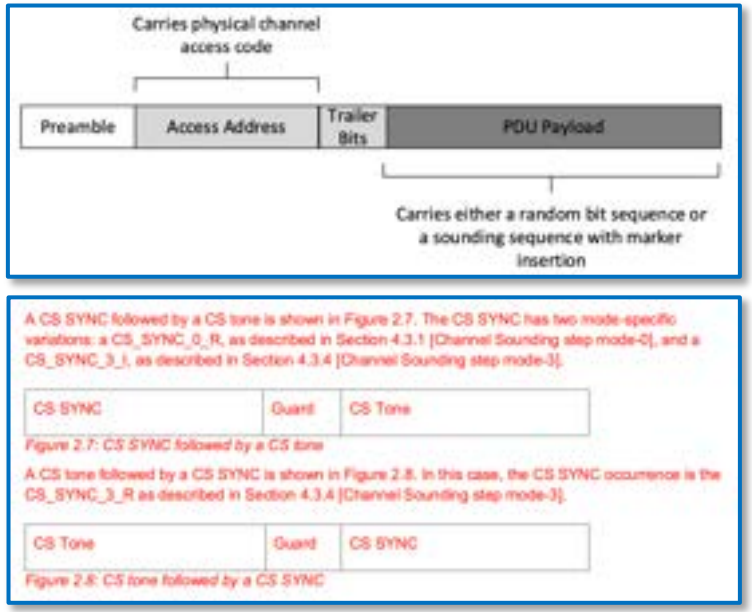
Link Layer – Roles and Modes

- Mode 0 - Calibrate
- Mode 1 – RTT
- Mode 2 – PBR
- Mode 3 – RTT + PBR (optional)



Link Layer – Packet Structure

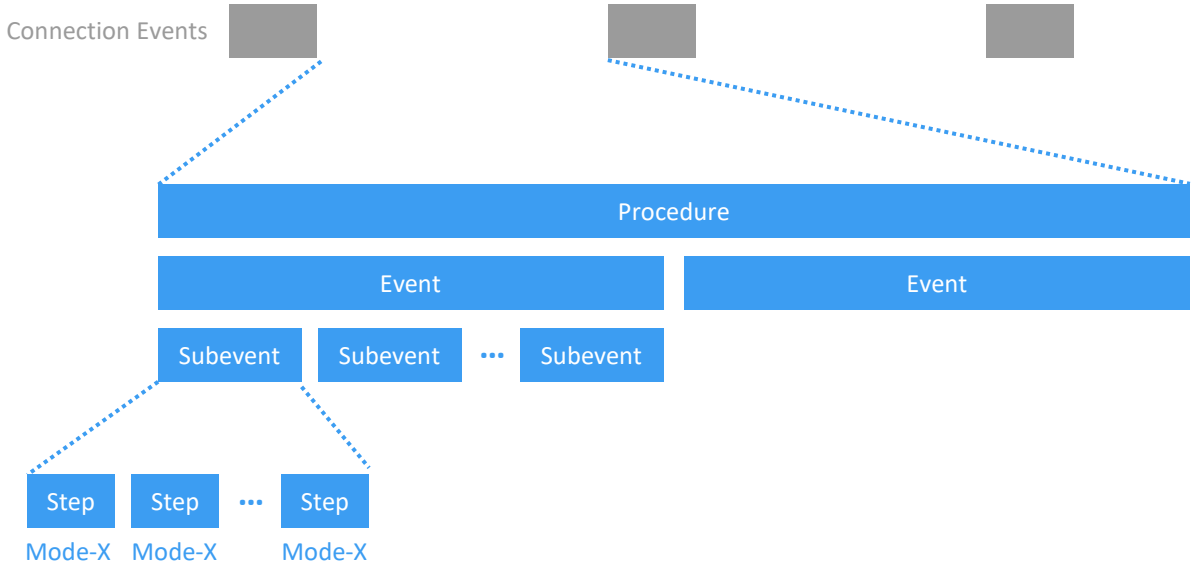
- Compared to ADV and ACL
  - Preamble – no change
  - Access Address – cryptographically generated
  - Trailer – 4 bits
  - Payload – nibble multiple
  - CRC – not present
  - Whitening is disabled



Source: Bluetooth Channel Sounding CR_PR, 2023-06-22

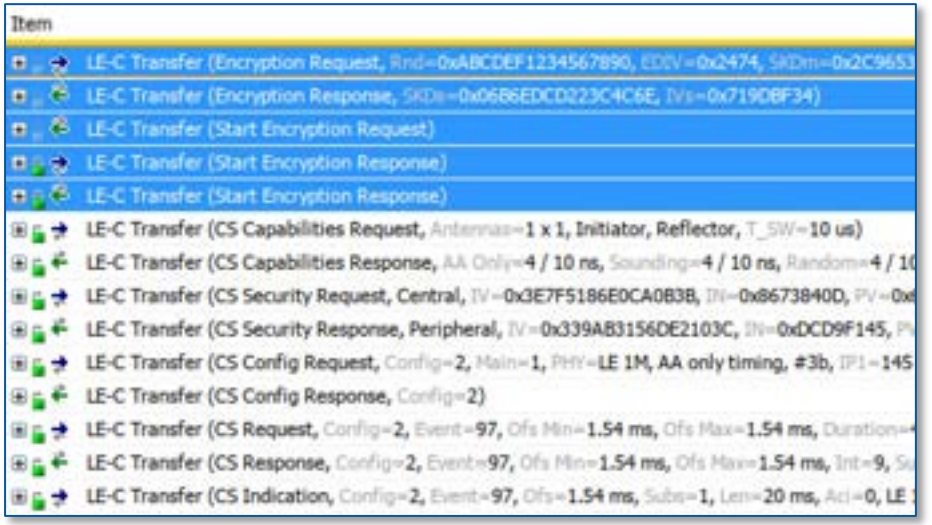
Link Layer – Packet Organization

- Procedure
- Event
- Subevent
- Steps



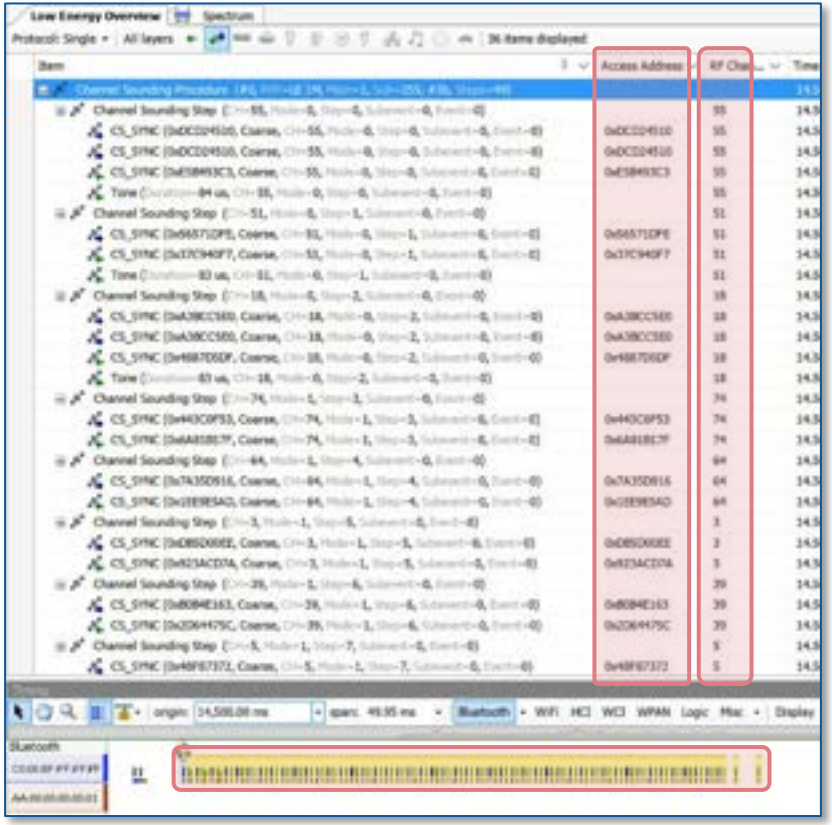
Analysis

- Secure Connection prerequisite required
- Channel Sounding Procedure
  - Exchange Capabilities
  - Exchange Security
  - Negotiate Configuration
  - Exchange Measurements (repeats)



Analysis

- Anti Spoofing
  - Pseudorandom Channel (CSA #3)
  - Pseudorandom AA generation
  - Subevent sub-mode insertion
  - Tone Extension Slot present
  - Antenna path permutation index
  - Pseudorandom Sounding Sequence markers
  - Random Bit Sequence
- Normalized Attack Detector Metric (NADM)



Summary

- High accuracy – about 30-cm with specialized algorithms
- Ubiquity of Bluetooth
  - Beacons can add fine ranging
  - Your phone is your Digital Key
- Highly secure with built in anti-spoofing
- Channel Sounding air trace available for download – *coming soon*
  Sign up for Packetcraft's newsletter: www.packetcraft.com

References

- Channel Sounding CR_PR (Draft)
  https://www.bluetooth.com/specifications/specs/channel-sounding-cr-pr/
- Bluetooth Core Specification 5.4 (Adopted)
  https://www.bluetooth.com/specifications/specs/core-specification-5-4/
- Introducing: The Bluetooth Low Energy Primer
  https://www.bluetooth.com/blog/introducing-the-bluetooth-low-energy-primer/
- Bluetooth Channel Sounding – A Step Towards 10-cm Ranging Accuracy for Secure Access, Digital Key, and Proximity Services
  https://www.bluetooth.com/blog/bluetooth-channel-sounding-a-step-towards-10-cm-ranging-accuracy-for-secure-access-digital-key-and-proximity-services/
- Trilateration
  https://en.wikipedia.org/wiki/Trilateration
- Multipath propagation
  https://en.wikipedia.org/wiki/Multipath_propagation
- How Does Channel Sounding Work?
  https://www.silabs.com/wireless/bluetooth/channel-sounding

John Yi | Packetcraft
sales@packetcraft.com

Thank you!

Questions?