Qualcomm

Using *Bluetooth*® Channel Sounding to improve Indoor Positioning

Mayank Batra,
Principal Engineer,
Bluetooth Standards Lead

Evolution of Bluetooth positioning

What is Bluetooth Channel Sounding?

Core principles

How phase-based ranging works

How round-trip time works

Security measures

Conclusions

Evolution of Bluetooth positioning

Bluetooth LE (2010): Enabled presence detection and basic item finding (Find Me Profile).

Beacons & RSSI (2013): First-generation distance estimation using signal strength (TX Power & RSSI).

Direction Finding (2019): Bluetooth SIG introduced Angle of Arrival (AoA) and Angle of Departure (AoD) for direction calculation using phase measurements and antenna arrays.

Channel Sounding (2024): Next step for accurate, secure distance measurement.

Limitations of Previous Methods

RSSI-based distance estimation not accurate enough for many applications.

No indication of direction or robust security safeguards.

Direction finding improved accuracy but still had limitations for fine-ranging.

What is Bluetooth Channel Sounding?

- A new feature in the Bluetooth Core Specification enabling secure, accurate distance measurements between Bluetooth devices.
  - Fundamentally, it enables a device to characterize the propagation path to a remote device.
  - Released as part of Bluetooth Core Specification 6.0* in August 2024. Enhancements already being developed.
- Designed to improve accuracy and security in device positioning applications.
  - Line of sight: ± 50 cm accuracy for distances up to 5 meters, ± 10% of actual distance for higher distances.
  - Multiple antennas can be used on one or both devices to counter the effects of multi-path indoors.
- Use cases:
  - Find My solutions: More accurate item location.
  - Digital keys: Enhanced security for access control.
  - Asset tracking & navigation: Reliable, fine-grained positioning.
  - Developer flexibility: Prioritize accuracy, security, or latency as needed.
    - Can enable distance measurements typically at 10 Hz (one measurement every 100 milliseconds).
- Limitation: A point-to-point connection is required between the two devices.

* https://www.bluetooth.com/specifications/specs/core-specification-6-0/

Core principles

Radio wave properties: amplitude, wavelength, frequency, phase.

Two main methods:

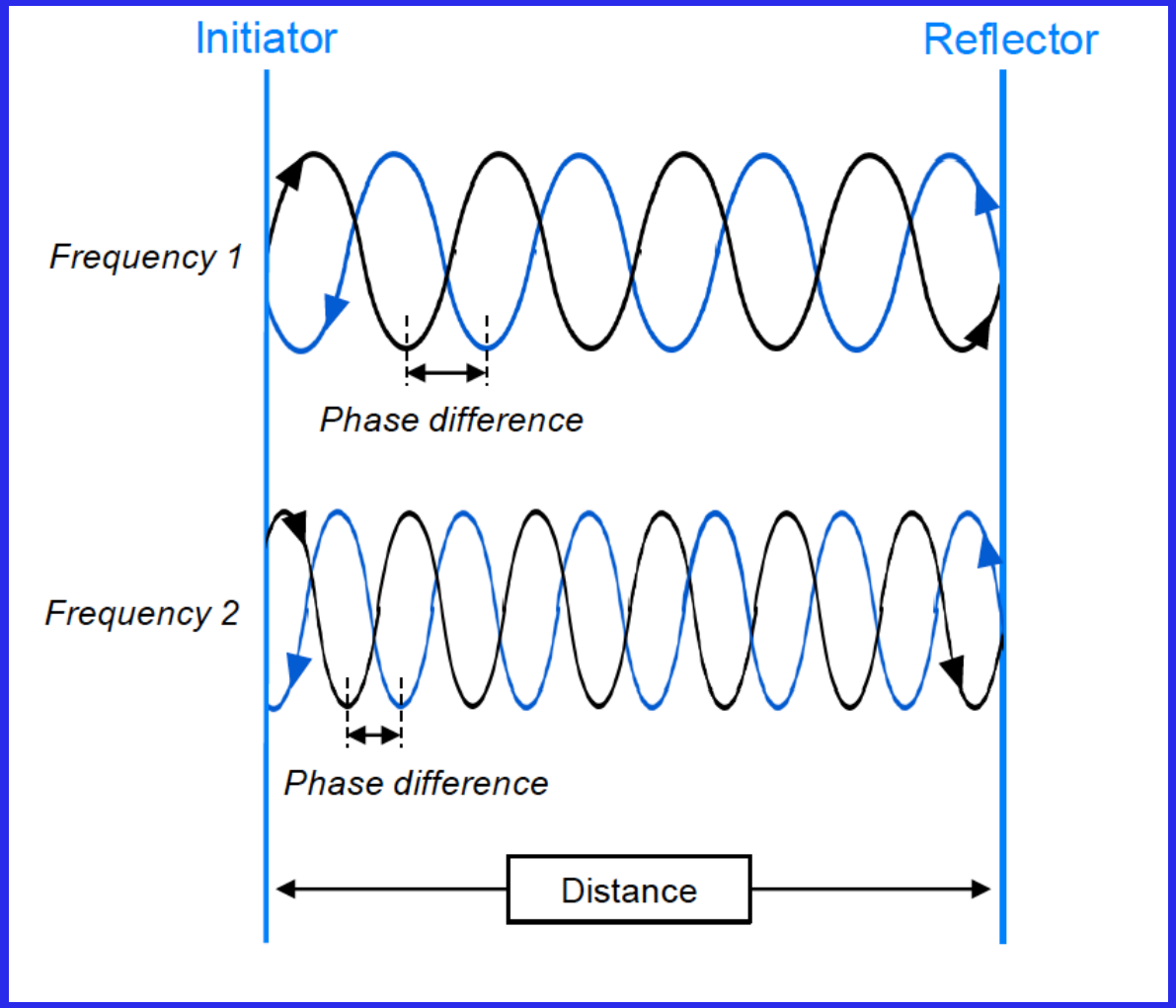
Phase-Based Ranging (PBR): Measures phase differences across frequencies to calculate distance.

Round-Trip Time (RTT): Measures time-of-flight for signals between devices. Also provides different levels of security.

Both PBR and RTT supported; PBR is primary for accuracy, RTT adds security and resolves ambiguity.

How Phase-based Ranging works

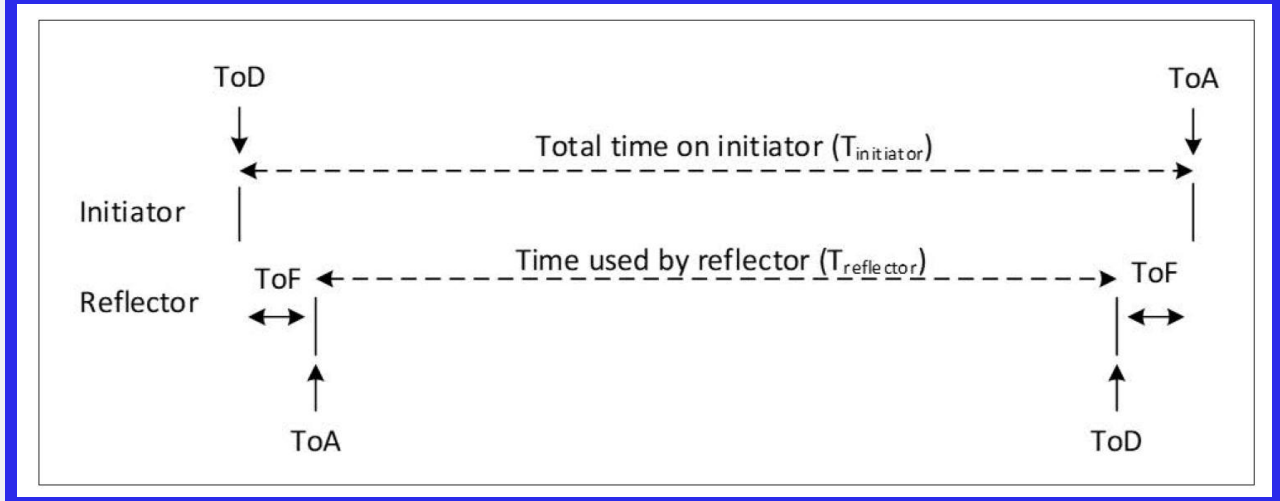
- Frequency f1:
  - Initiator sends a tone at frequency f1.
  - Reflector performs a phase measurement.
  - Reflector sends a tone at frequency f1, calculates PCT*.
  - Initiator performs a phase measurement, calculates PCT.
- Reflector sends its PCTs to Initiator.
- Total phase shift $\Delta\phi$ is the sum of two PCTs.
  - $distance = c \times \Delta\phi / 4\pi \times f$
- To resolve phase ambiguity (wrap every 2π), tones are exchanged at multiple frequencies.
- Slope of phase vs. frequency gives a linear estimate of distance.
- Ambiguity can arise due to periodic phase values; RTT helps resolve this.



* Phase Correction Term: Difference between the phases of the received and transmitted tones

How Round-Trip Time works

- Measures time taken for a signal to travel from Initiator to Reflector and back.
- Reflector sends its ToD – ToA measurements to Initiator.
- Distance = $((T_{initiator} - T_{reflector})/2) \times c$.
- Requires precise timestamping and compensation for device processing delays.



Security features

- RTT with Sounding or Random Sequence
  - Mitigate replay attacks and timing-based exploits by introducing unpredictability in the signal pattern.
- Combined PBR & RTT:
  - Hard to attack both simultaneously. Phase and time attacks require different techniques.
- Deterministic Random Bit Generator (DRBG):
  - Generates cryptographically secure random bits for randomizing bit streams, access addresses, antenna paths.
  - Reduces predictability in patterns, making it harder for attackers to guess or inject malicious data.
- Attack detection:
  - Normalized Attack Detector Metric (NADM) to monitor anomalies in signal behavior and report likelihood of attack.
- SNR control:
  - Injects noise into the channel making it harder for attackers to extract useful information from signals.
- LE 2M BT=2.0 PHY (BT=time-bandwidth product in GFSK):
  - Improves physical layer security by making it harder for an attacker to inject a fake signal without matching exact waveform.

Conclusions

- Previous positioning methods were less reliable:
  - RSSI-based distance estimation could be affected by environmental factors, leading to variability in accuracy.
    - Also impacted by variations in TX output power (±2 dB) and variations in RSSI accuracy (±2 dB) leading to uncertainty.
  - Typically confirmed presence, not precise location/direction; performance could degrade with obstacles/signal attenuation.
  - Direction finding (AoA/AoD) improved accuracy but still faced challenges with fine-ranging and robust security.

- Channel Sounding: A notable improvement in reliability
  - Uses phase-based ranging and round-trip timing to deliver more accurate distance measurements
  - Reduces (but does not entire eliminate) the impact of RSSI limitations and multipath effects.
  - Built-in security features (randomization, attack detection, SNR control) to help protect against spoofing and relay attacks.

- Indoor positioning revolution:
  - In challenging indoor environments, Channel Sounding enables more precise, secure, and reliable location determination.
  - Enables new applications for navigation, asset management, and “Find My” solutions in offices, hospitals, airports, etc.

Thank you

Follow us on:

For more information, visit us at qualcomm.com & qualcomm.com/blog