Application Note

High Accuracy, Low Cost, Secure Ranging with Bluetooth Channel Sounding

Bhargavi Nisarga

ABSTRACT

The upcoming Bluetooth Channel Sounding feature extends Bluetooth based ranging beyond the supported received signal strength indication (RSSI) and direction findings (DF) capabilities to enable high-accuracy, low-cost, secure ranging designs.

This application note presents the basics of Bluetooth channel sounding technology – using phase based ranging to enhance accuracy and round trip time (RTT) of random modulated data packets to enhance security. The document also provides an overview of the channel sounding procedures using Bluetooth LE devices to perform the ranging operations.

Table of Contents

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

Ranging is a process or method to determine the distance from one location or position to another. Bluetooth based ranging is currently used in many applications wherein distance between the two Bluetooth devices in range is determined by using the received signal strength indication (RSSI). Additionally, Bluetooth devices can be localized with distance measurement from multiple (at least three) Bluetooth devices in known fixed locations (also known as anchor nodes) using trilateration methods.

There are several ranging and localization enabled applications including:

- Smart access designs involving remote keyless entry, passive entry passive start (PEPS), and digital key access designs with broad adoption in automotive car access
- Item finding
- Asset tracking
- Localization
- Indoor navigation
- Proximity services

Optimum ranging designs address the following key factors to enable broad proliferation and adoption of the technology in a wide range of distance measurement applications:

- High accuracy
- Long range
- Low power
- Increased security
- Real time user experience
- Low system cost
- Easy for broad market scalability and adoption

The upcoming Bluetooth Channel Sounding (CS) feature considers all of these factors to provide a new high-accuracy distance measurement method between two Bluetooth devices.

The Bluetooth specification has been evolving since the inception by adding new features to not only enable new markets and applications but also, address challenges or limitations in existing applications to make use of the Bluetooth ecosystem that already exists to enhance user experience and lower the overall system cost. On the same lines, the upcoming Bluetooth Channel Sounding feature is expected to enhance existing ranging designs and enable new applications.

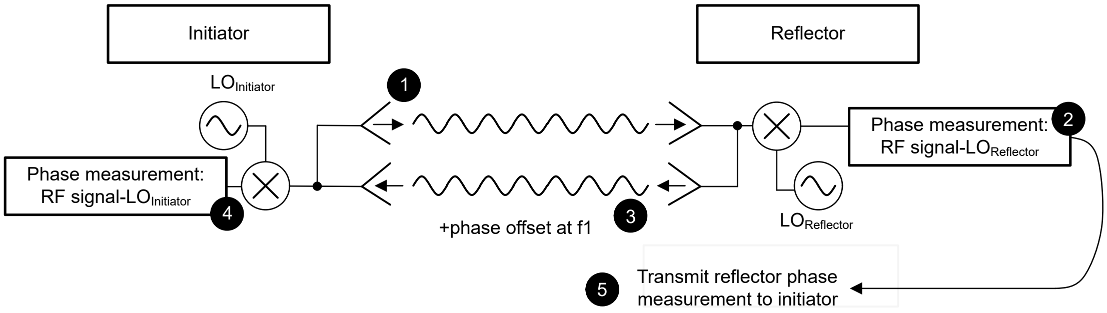
Bluetooth LE uses narrow band technology that supports long range and low power wireless data communication. The Bluetooth channel sounding feature uses phase-based ranging across multiple frequency tones to perform high accuracy distance measurement and round-trip time of flight measurements to mitigate man-in-the-middle based security threats against distance manipulation. Additionally, the Bluetooth LE radio technology has been adopted in majority of the smart phones and in a growing number of IoT devices, thereby, paving an easy path to broad market scalability and adoption compared to other wireless ranging technologies.

The following sections include the basics of Channel Sounding feature and procedure for performing secure ranging.

2 Basics of Bluetooth Channel Sounding

Bluetooth Channel Sounding uses a known technique called phase-based ranging (PBR) to perform high accuracy distance measurement. In PBR, two devices measure the distance between them by estimating the phase offset or phase difference between a received unmodulated signal and a local oscillator (LO) signal. See Section Appendix A: Basics of Phase Based Ranging and Multi-Carrier Phase Ranging for the basics of phase-based ranging and the need for multi-carrier phase ranging systems in real world systems. Multi-carrier phase ranging systems measure the phase difference between the received unmodulated signal and the LO signal at multiple RF frequencies to generate measured phase difference vs. frequency curve, that is in turn used to determine the distance between the two devices.

Per Bluetooth CS, if device A (initiator) is measuring the distance to device B (reflector), then, the initiator begins ranging by transmitting an unmodulated tone. The reflector measures the phase of incoming signal relative to the local oscillator and then, transmits an unmodulated tone back to the initiator. Next, the initiator measures the phase of incoming signal relative to the local oscillator. See Figure 2-1.


Initiator
Reflector
$LO_{Initiator}$
1
2
Phase measurement: RF signal-$LO_{Reflector}$
Phase measurement: RF signal-$LO_{Initiator}$
4
3
+phase offset at f1
$LO_{Reflector}$
5
Transmit reflector phase measurement to initiator

*Two way phase difference measurement at frequency f1
No impact from Initiator/Reflector LO as their relative phase is subtracted out

Figure 2-1. Bluetooth Channel Sounding, Phase Based Ranging

Note

Bluetooth CS does not require the reflector device to be a true reflector requiring the device to lock the LO to the incoming RF signal and transmit the device back to the initiator. Instead, two-way phase difference measurements are used to remove the relative phase offsets due to the initiator and reflector LO.

The tone exchange (between the initiator and reflector) and phase measurements (at both the initiator and reflector) are performed at multiple frequencies in the 2.4GHz Bluetooth band (1Mhz frequency steps). With the phase measurements from both initiator and reflector, the differences in the relative phases and the devices' local oscillators are corrected across all frequencies. After the phase correction, the actual phase offset/shift measured at each frequency is plotted as the measured phase difference vs. frequency curve. In optimal conditions, plotting the phase difference measurements vs. each frequency yields a straight line with a slope that represents the distance between the initiator and the reflector. Since the measured phase differences wrap around 2pi, the phase differences are required to be further straightened to calculate the effective slope and determine the distance between the initiator and reflector.

In the real-world though, the radio signals travel from the initiator's antenna to the reflector's antenna by more than one path. This is referred to as multipath propagation and can impact the phase difference measurements and in turn, the ranging resolution and accuracy. In presence of channel impairments, collecting phase measurements at increased the number of frequencies or tones, across multiple antenna paths and using advanced signal processing like IFFT, MUSIC (MUltiple SIgnal Classification) algorithms enable high accuracy distance estimation.

The next section details the channel sounding procedure outlined in *Channel Sounding Draft Specification* for collecting phase measurements to perform distance measurement.

3 Bluetooth Channel Sounding Procedure

A channel sounding procedure can be divided into one or more CS events. CS events can be comprised of one or more CS subevents. Subevents are a set of predefined time and frequency slots in which the two Bluetooth devices agree to communicate and exchange a combination of RF signals. These exchanges are bidirectional, as both devices take turns sending and receiving RF signals. Within a CS subevent, one or more CS steps are used perform the actual exchanges of ranging tones and security packets (see Section 5 for further details regarding Bluetooth CS security). Bluetooth CS specification defines four CS step types: mode 0 through mode 3. Each mode is used for a specific purpose.

Table 3-1. CS Step Types: Mode 0 to Mode 3

Mode	Description
Mode 0	Used to exchange synchronization information to align on timing and calibrate frequency of one side w.r.t. the other
Mode 1	Used to exchange a Round Trip Timing (RTT) packets
Mode 2	Used to exchange phase-based ranging (PBR) CS tones, to measure phase and amplitude of the communication channel
Mode 3	Used to exchange both RTT and PBR CS tones

Figure 3-1 shows the relationship between CS procedures, CS events, CS subevents, and CS steps.

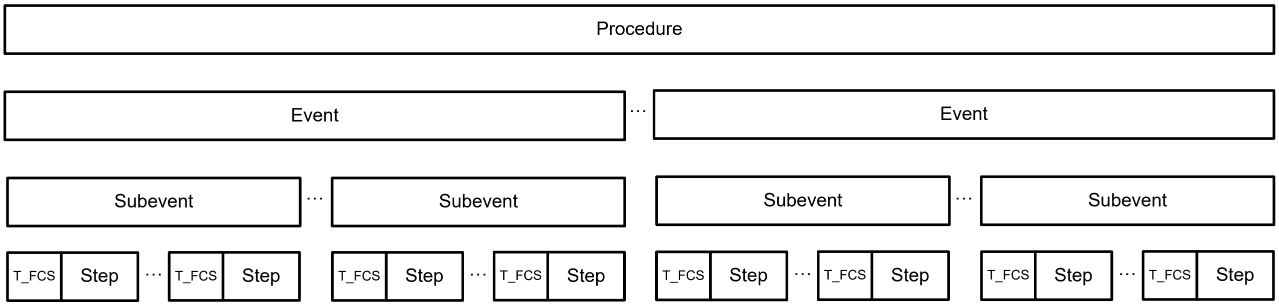


Figure 3-1. CS Procedure, Event, Subevent, Step Hierarchy

Note

T_FCS refers to frequency change spacing time period between transmitting two CS steps

To allow for flexible scheduling of CS procedure amidst other ongoing Bluetooth LE connections, multiple CS subevents can be scheduled to be offset from a single LE connection event. A CS subevent offset is used to separate the multiple CS subevents in time. The number of CS subevents allowed in between LE connection events is selectable.

The general structure of Channel Sounding events and subevents started at an offset from the timing of LE ACL (asynchronous connection logical transport) connection event anchor points is as shown in Figure 3-2.

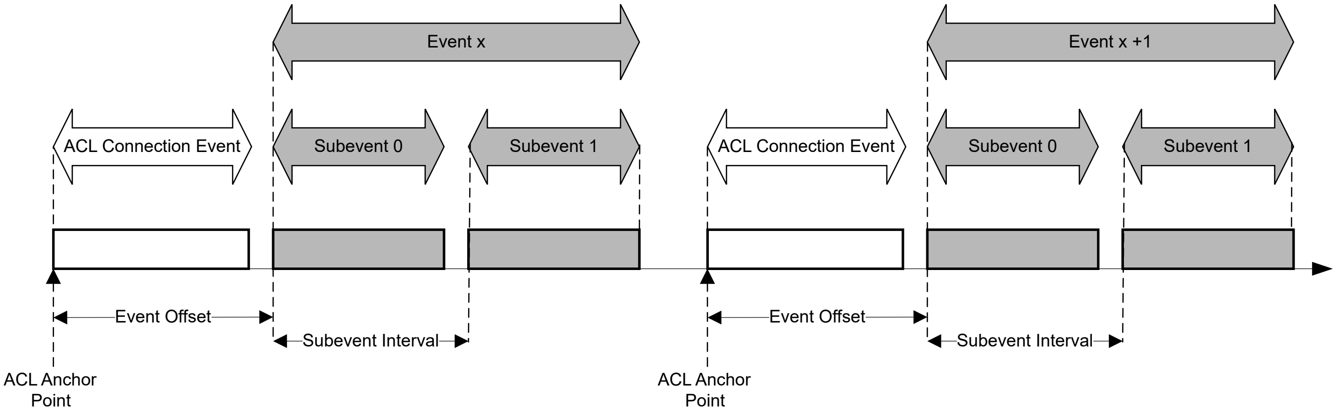


Figure 3-2. Channel Sounding Events and Subevent Scheduling

4 Bluetooth Channel Sounding Flow for Phase-Based Ranging

In the context of CS, an initiator is the Bluetooth device that starts (initiates) the CS procedure and a reflector is the Bluetooth device that responds to (reflects) the CS procedure. The procedure's operating parameters are exchanged through Link Layer control messages prior to starting the CS procedure.

Figure 4-1 shows the high-level CS flow to perform phase-based ranging between a CS initiator and reflector.

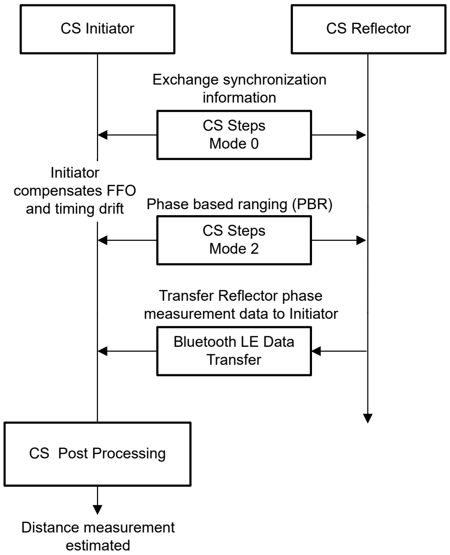

CS Initiator
CS Reflector
Exchange synchronization information
CS Steps Mode 0
Initiator compensates FFO and timing drift
Phase based ranging (PBR)
CS Steps Mode 2
Transfer Reflector phase measurement data to Initiator
Bluetooth LE Data Transfer
CS Post Processing
Distance measurement estimated

Figure 4-1. High-Level Channel Sounding Phase-Based Ranging Flow

At the beginning of CS subevent, the CS Mode 0 steps are mandatory to provide frequency and timing synchronization between CS initiator and reflector, for the remaining CS steps within that CS sub-event.

Multi-carrier phase ranging involves phase difference measurements at different frequencies, and any relative error (between the initiator and reflector devices) in the generation of the frequencies can disrupt those phase measurements and introduce errors in the overall distance estimation. Therefore, it is important that the initiator and reflector devices keep their carrier frequencies aligned during the entire duration of each individual measurement. Per Bluetooth Channel Sounding draft specification, the initiator device is required to align its timing and carrier frequencies to the reflector. The device uses the initial Mode 0 steps to do this step by estimating and compensating the fractional frequency offset (FFO) between the devices.

The CS Mode 0 steps are then followed by Mode 2 PBR steps which involves both the initiator and reflector devices exchanging the unmodulated CS tones at different channel frequencies.

Out of the 79 designated Bluetooth channels in the 2.4GHz unlicensed ISM band, 72 channels with 1MHz channel spacing can be used for Bluetooth LE, CS PBR (Note: Bluetooth LE advertising channels are not prescribed for CS PBR). Both the initiator and the reflector measure the phase and amplitude of the incoming tone as a function of frequency. Once all the PBR Mode 2 steps are complete, both the initiator and reflector devices can have the phase and amplitude information in the form of in-phase and quadrature-phase (I and Q) measurements. Next, the reflector can communicate this measurement information to the initiator as part of the Bluetooth LE connection events. Note: vice-versa wherein the initiator can send back the measurements to the reflector for further processing is also possible.

Next, the initiator combines the phase and amplitude measurements from both the devices and performs post processing to estimate the distance measurement. The Bluetooth CS does not specify a specific algorithm to compute a distance estimate, but provides some mathematical representation towards distance estimation using the phase measurements. Advanced and efficient post processing algorithms can be used to eliminate multipath and fading effects to provide robust distance estimation values. Additionally, tone quality information can be used filter outliers due to signal interference and noise. Post processing algorithms with varying complexity and efficiency can be used to compute distance approximation with tradeoff consideration with respect to accuracy, power consumption and computational latency requirements.

5 Channel Sounding Security

The Bluetooth channel sounding draft specification has added different security features to either detect or to prevent an attack that can manipulate the ranging procedure to make the distance between two valid CS devices appear closer than they actually are. Refer to the Channel Sounding draft specification for full list of security features.

PBR procedures used for distance estimation can be attacked by performing man-in-the-middle attacks that can either delay or manipulate phase of the ongoing signal transmissions to measure a shorter distance between the two valid devices. To mitigate these attacks, the Bluetooth CS specification specifies random hopping of frequencies during PBR and additionally, has added round trip time (RTT) measurements that is yet another ranging measurement between the two devices. Since the maximum unambiguous measurable distance for PBR with 1MHz frequency hops is 150m (see Equation 1 for calculation), the RTT time-of-flight measurements, although not as accurate as the CS PBR mechanism is still a viable option to identify roll over attacks.

Note

The maximum measurable distance using PBR, depends on the maximum measurable phase difference between the two frequency signals. With maximum phase difference between any two tones being 2**π* and the CS tones being 1MHz apart, the maximum measurable distance dmax is given by:

$$d_{\max} = \frac{c}{4\pi} \times \frac{(\Delta\theta_{max})}{(\Delta f)} = 150m \qquad (1)$$

The distance estimation using RTT time-of-flight measurements is as shown in Figure 5-1.

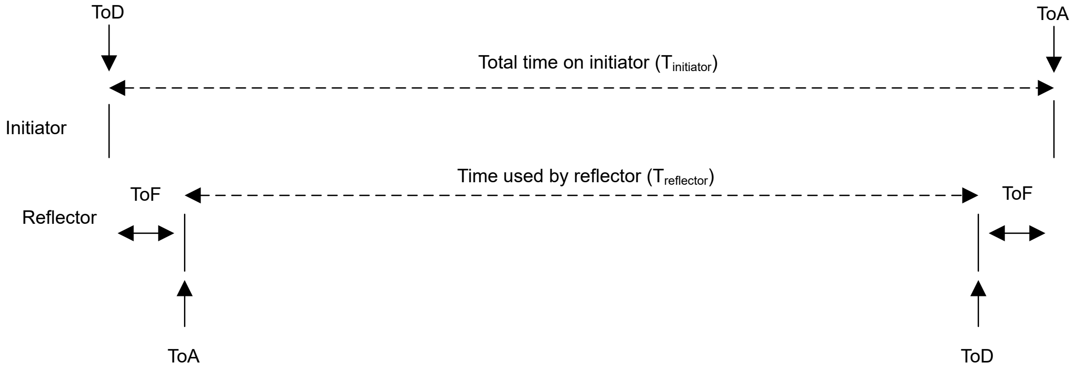

ToD
ToA
Total time on initiator ($T_{initiator}$)
Initiator
Time used by reflector ($T_{reflector}$)
ToF
ToF
Reflector
ToA
ToD

Figure 5-1. Time of Arrival (ToA), Time of Departure (ToD), and Time of Flight (ToF) for RTT Estimation

RTT packets are exchanged between initiator and reflector. The time of departure (ToD) and time of arrival (ToA) of these RTT packets at both the initiator and reflector are used to estimate the time-of-flight. The CS step mode 1 and mode 3 allow for RTT packet exchanges.

Bluetooth CS specification also supports RTT packets with random sequence (known to only the initiator and reflector) to be communicated, so that it is increasingly possible to measure difference between the received GFSK modulated packet and the expected packet signal (reference). This measurement is represented as a normalized attack detector metric (NADM) which is a range that indicates if there is an increased or decreased chance of a man-in-the-middle attacker trying to relay the RTT packets by manipulating the signal to appear earlier to perform ECLD (early commit, late detect) and EDLC (early detect, late commit) type of attacks. NADM algorithms are used to determine the NADM value for the received RTT packets in each CS device on both sides of the link. The NADM algorithm definition and implementation is beyond the scope of Bluetooth CS specification.

6 Summary

The upcoming Bluetooth Channel Sounding feature addresses the key requirements of Location Services solutions, including high accuracy measurement across longer ranges and increased security compared to the prior Bluetooth solutions. These key factors combined with Bluetooth LE technology's low power attribute and the ubiquitous adoption in smart phones, consumer IoT, industrial and automotive applications, makes it an ultra-promising technology for high-accuracy, low cost, secure ranging solutions.

As a Bluetooth SIG associate member, Texas Instruments (TI) is actively working with the SIG on the specification of the Channel Sounding technology. TI CC2340R5 and upcoming TI Bluetooth LE devices support the upcoming Bluetooth Channel Sounding in the device's RF core and as part of the Bluetooth stack in the Software Development Kit (SDK). All the Channel Sounding modes including Mode 3 phase-based ranging and RTT packet exchange are supported. To get more information regarding the upcoming TI channel sounding demos, tools and examples, please contact connectivity_auto_marketing@list.ti.com or your local TI sales office.

Note

The Bluetooth channel sounding specification is still in draft state. This application note will be updated as needed, depending on the updates to the draft specification before the final release.

7 References

1. Bluetooth, *Channel Sounding Draft Specification*.
2. *On the Security of Carrier Phase-based Ranging*, Hildur Ólafsdóttir, Aanjhan Ranganathan, Srdjan Capkun, ETH Zurich.

Appendix A: Basics of Phase Based Ranging and Multi-Carrier Phase Ranging

Phase Based Ranging (PBR) systems involve measuring the changes to the phase of the radio signal propagating between two entities to determine the distance between them.

Consider a ranging example, wherein Entity A (initiator) is measuring its distance from Entity B (reflector). In an ideal PBR system, Entity A initiates ranging by transmitting an unmodulated continuous wave tone, at a specific frequency f. Entity B receives this RF signal and acts as a true reflector by locking the local oscillator to the incoming RF signal and transmits it back to the initiator. Finally, the initiator measures the difference in the phase of the received signal and its own local oscillator signal and determines the distance based on this phase measurement. Figure 8-1 shows phase based ranging with RF signal at a specific frequency. Entity A is the initiator and Entity B is acting as a true reflector by locking its LO to the incoming RF signal and transmitting it back to the initiator.

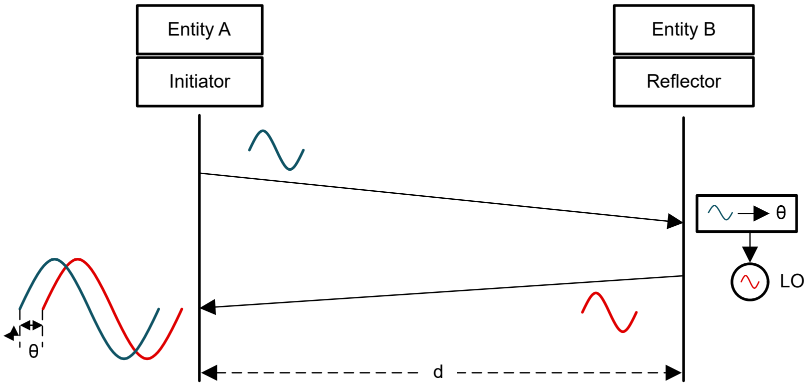


Figure 8-1. Phase Based Ranging with RF Signal at a Specific Frequency

If the distance d, between the initiator and the reflector is less than the signal's wavelength, that is, $\frac{2 \times f}{c}$, where f is the frequency of the RF tone and c is the speed of light, then, the measured phase offset or phase difference θ is:

$$\theta = 2\pi \times d \times \frac{2 \times f}{c} \tag{2}$$

However, in real-world applications, there is a need to measure distances longer than signal's wavelength and to do this, there is a necessity to keep track of the number of whole cycles that have elapsed when the RF tone is propagating between the two entities. Considering n is the number of whole cycles (integer) that have elapsed, then, distance d is measured as:

$$d = \frac{c}{2 \times f}\left(\frac{\theta}{2\pi} + n\right) \tag{3}$$

To eliminate the need for tracking the number of whole cycles elapsed, multi-carrier phase ranging is considered. In multi-carrier phase ranging systems, the phase measurements (difference in the phase of the received signal and its own local oscillator signal) are taken at multiple RF tone frequencies. RF signals at different frequencies traveling the same distance (and in turn, the same propagation time) can have a different phase offset or shift.

For example, consider that the initiator and reflector devices with distance d between them, perform PBR (as described with Figure 2-1) at two frequencies: f1 and f2. That is, the devices first perform PBR at RF signal frequency f1 and then at RF signal frequency f2. The phase differences measured at f1 and f2 is shown as:

$$\theta_1 = 2\pi \times \left(d \times \frac{2 \times f_1}{c} + n\right) \tag{4}$$

$$\theta_2 = 2\pi \times \left(d \times \frac{2 \times f_2}{c} + n\right) \tag{5}$$

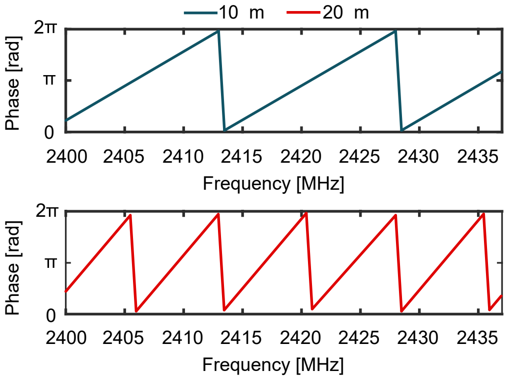
Combining Equation 4 and Equation 5 to remove number of whole cycles (n) ambiguity, the distance d is now represented as:

$$d = \frac{c}{4\pi} \times \frac{(\theta_2 - \theta_1)}{(f_2 - f_1)} \tag{6}$$

To get better ranging accuracy and resolution in real-world, the phase offset measurements at more than two frequencies is required. Further, if the phase offset measurements are plotted as a phase vs. frequency curve, then, the slope of the curve represents the distance d between the initiator and the reflector. See Figure 8-2 and Figure 8-3. Equation 6 can be seen as a straight line with the distance proportional to the slope of the line:

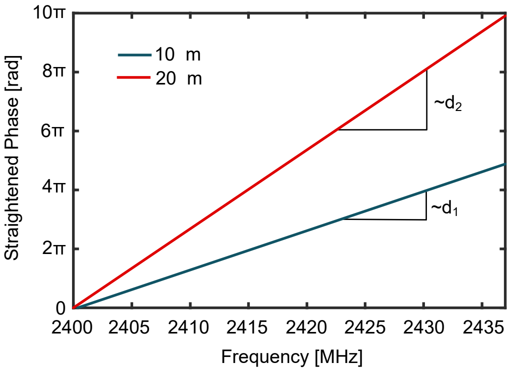
$$d = \frac{c}{4\pi} \times slope \tag{7}$$

Referenced from [2] - Figure 8-2 shows the measured phase differences vs. frequency for two different distances d1 = 10m and d2 = 20m between the initiator and reflector. The phase differences wrap around 2π and can be straightened as shown in Figure 8-3 to calculate the effective phase slope and estimate the distance between the initiator and the reflector.



(a) The phase of the received signal.

Figure 8-2. Measured Phase vs. Tone Frequencies (Wrapping Around 2π)



(b) The straightened phase of the received signal.

Figure 8-3. Measured Phase vs. Tone Frequencies (Straightened Phase)

IMPORTANT NOTICE AND DISCLAIMER

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265