*Application Note*

# *使用蓝牙信道探测实现高精度、低成本且安全的测距*

*Bhargavi Nisarga*

**摘要**

即将推出的蓝牙信道探测功能扩展了基于蓝牙的距离测量，超越了对接收信号强度指示 (RSSI) 和方向发现 (DF) 功能的支持范围，因而能够实现高精度、低成本和安全的测距设计。

本应用手册介绍了蓝牙通道探测技术的基础知识，该技术使用基于相位的测距来提高准确性，同时利用随机调制数据包的往返时间来增强安全性。本文档还概述了使用低功耗蓝牙器件执行测距操作的信道探测程序。

## 内容



## 商标

# 1 引言

测距是确定两个地点或位置之间距离的过程或方法。目前，基于蓝牙的测距技术在许多应用中广泛使用，这些应用通过使用接收信号强度指示 (RSSI) 来确定通信范围内两个蓝牙设备之间的距离。此外，通过使用三边测量方法，可以通过从多个（至少三个）已知固定位置（也称为锚节点）的蓝牙设备进行距离测量来实现对蓝色设备的定位。

支持测距和定位功能的应用有多种，其中包括：

- 智能门禁设计，包括遥控免钥匙进入、无钥匙进入及启动 (PEPS) 和数字钥匙门禁设计，广泛应用于汽车门禁
- 物品查找
- 资产跟踪
- 定位
- 室内导航
- 接近服务

为了将该技术广泛应用于各种测距应用，优化的测距设计需要考虑以下关键因素：

- 高精度
- 远距离
- 低功耗
- 增强安全性
- 实时用户体验
- 低系统成本
- 易于在广泛市场中进行推广和采用

即将推出的蓝牙信道探测 (CS) 功能考虑了所有这些因素，为测量两个蓝牙设备之间的距离提供了一种新的高精度方法。

自问世以来，蓝牙规范一直在不断发展，通过增添新的功能，不仅推动了新的市场和应用，还能够解决现有应用中的挑战或限制，以利用现有的蓝牙生态系统来提升用户体验并降低总体系统成本。同样，即将推出的蓝牙信道探测功能有望改进现有的测距设计并推动新的应用。

低功耗蓝牙采用窄带技术，实现了远距离和低功耗的无线数据通信。蓝牙信道探测功能使用基于相位的多频音调测距来执行高精度距离测量和往返飞行时间测量，以应对基于中间人的安全威胁，防范距离篡改。此外，低功耗蓝牙无线电技术已广泛应用于大多数智能手机，并在越来越多的物联网设备中得到采用，因此相较于其他无线测距技术，它为实现广泛的市场推广和采用提供了便捷路径。

以下各节介绍了信道探测功能的基础知识以及执行安全测距的程序。

## 2 蓝牙信道探测的基础知识

蓝牙信道探测使用一种称为基于相位的测距 (PBR) 的常见技术来执行高精度距离测量。在 PBR 技术中，两个设备通过估算接收到的未调制信号与本地振荡器 (LO) 之间的相位偏移或相位差来测量它们之间的距离。请参阅节 附录 A：基于相位的测距和多载波相位测距的基础知识，了解基于相位的测距技术的基础知识以及实际系统中需要多载波相位测距系统的原因。多载波相位测距系统通过在多个射频频率下测量接收到的未调制信号与 LO 信号之间的相位差，以生成所测相位差与频率之间的关系曲线，从而用于确定两个设备之间的距离。

根据蓝牙信道探测，如果设备 A（发起者）正在测量到设备 B（反射者）的距离，则发起者通过发送未调制的音调开始测距。反射者测量传入信号相对于本地振荡器的相位，然后向发起者发送未调制的音调。随后，发起者测量传入信号相对于本地振荡器的相位。请参阅图 2-1。

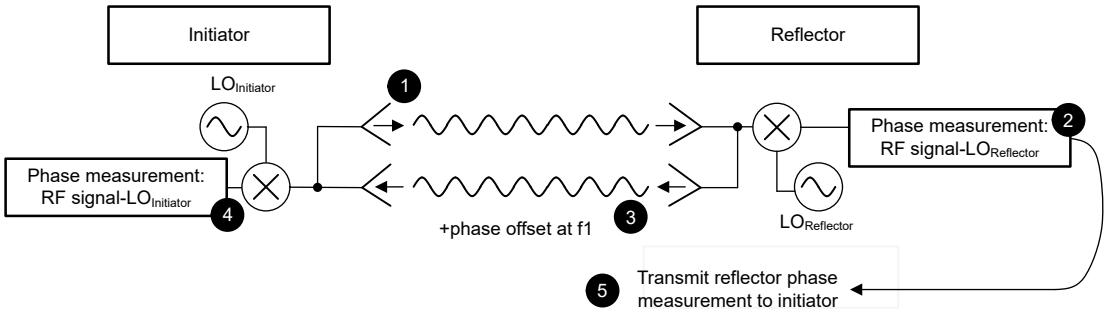



**图 2-1. 蓝牙信道探测、基于相位的测距**

**备注**

蓝牙信道探测并不要求反射者设备是真正的反射器，即不需要设备将 LO 锁定到传入射频信号并将设备传回给发起者。相反，它采用双向相位差测量来消除发起者和反射者 LO 引起的相对相位偏移。

该技术会在 2.4GHz 蓝牙频段（1MHz 频率步长）的多个频率下执行音调交换（发起者和反射者之间）和相位测量（在发起者和反射者上）。借助发起者和反射者的相位测量，在所有频率下对相对相位和设备本地振荡器之间的差异进行校正。经过相位校正后，将每个频率下测量的实际相位偏移/相移绘制为所测相位差与频率之间的关系曲线。在理想条件下，绘制相位差测量值与频率间的曲线会得到一条直线，其斜率代表发起者和反射者之间的距离。测得的相位差环绕在 2π 周围，因此需要进一步校正相位差，以计算有效斜率并确定发起者和反射者之间的距离。

然而，在现实世界中，从发起者的天线到发射者的天线，无线电信号可能会经过多条路径。这被称为多路径传播，可能会影响相位差测量，进而影响测距的分辨率和准确性。在存在通道损失的情况下，通过在增加的频率或音调下跨多条天线路径进行相位测量，并使用 IFFT、MUSIC（多信号分类）算法等高级信号处理，可以实现高精度的距离估算。

下一节详细介绍了*信号探测规范草案*中概述的信道探测过程，用于收集相位测量数据以进行距离测量。

# 3 蓝牙信道探测过程

信道探测过程可以分为一个或多个 CS 事件。CS 事件可以由一个或多个 CS 子事件组成。子事件是一组预定义的时隙和频隙，其中两个蓝牙设备同意进行通信并交换一组射频信号。这些交换是双向的，因为两个设备轮流发送和接收射频信号。在 CS 子事件中，使用一个或多个 CS 步骤来执行实际的测距音调和安全数据包的交换（有关蓝牙 CS 安全性的更多详细信息，请参阅节 5）。蓝牙 CS 规范定义了四种 CS 步骤类型：模式 0 到模式 3。每种模式都用于特定用途。

**表 3-1. CS 步骤类型：模式 0 至模式 3**

| 模式 | 说明 |
|---|---|
| 模式 0 | 用于交换同步信息，以便使一方的时序与另一方的时序对齐并进行两方频率校准 |
| 模式 1 | 用于交换往返时间 (RTT) 数据包 |
| 模式 2 | 用于交换基于相位的测距 (PBR) CS 音调，以测量通信通道的相位和振幅 |
| 模式 3 | 用于交换 RTT 和 PBR CS 音调 |

图 3-1 展示了 CS 过程、CS 事件、CS 子事件和 CS 步骤之间的关系。

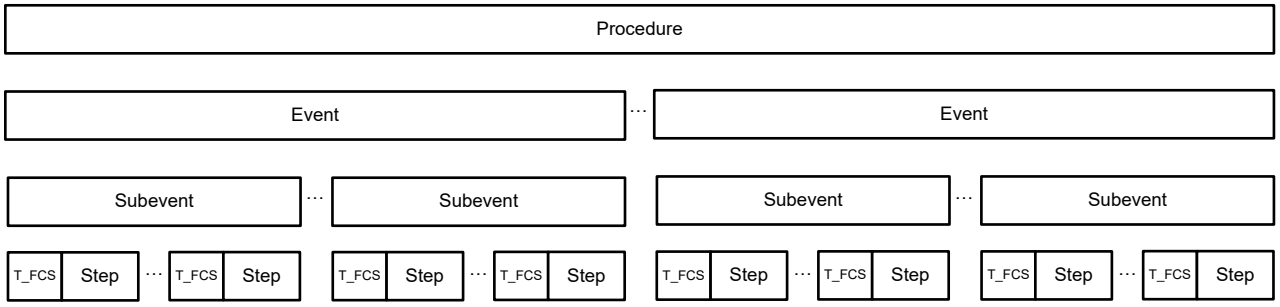



**图 3-1. CS 过程、事件、子事件、步骤层次结构**

**备注**

T_FCS 是指发送两个 CS 步骤之间的频率变化间隔时间周期

为了在其他正在进行的低功耗蓝牙连接中灵活调度 CS 过程，可以调度多个 CS 子事件，使其与单个低功耗连接事件错开。CS 子事件偏移用于在时间上分隔多个 CS 子事件。LE 连接事件之间允许的 CS 子事件数量是可选的。

信道探测事件和子事件的一般结构从 LE ACL（异步连接逻辑传输）连接事件锚点的时间偏移处开始，如图 3-2 所示。

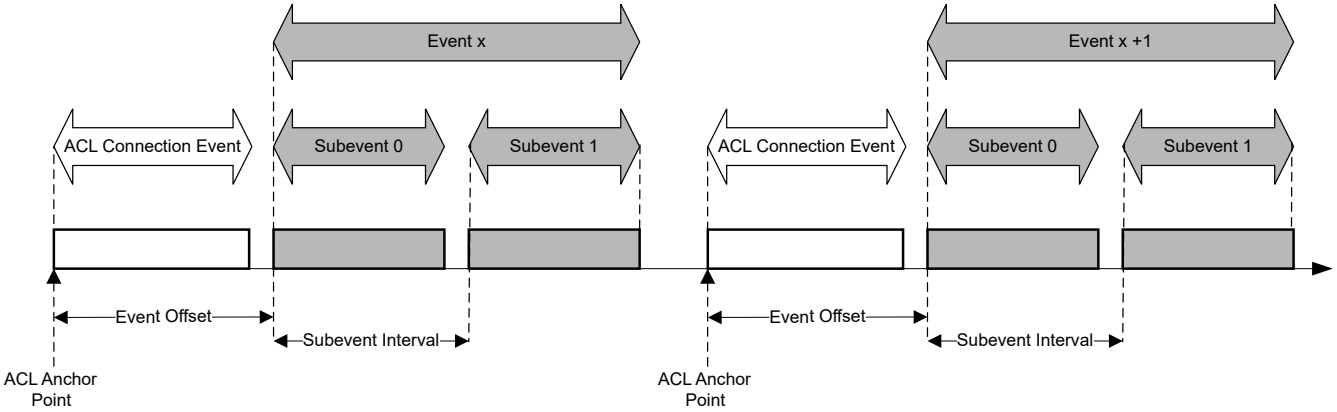



**图 3-2. 信道探测事件和子事件调度**

# 4 基于相位的蓝牙信道探测测距流程

在 CS 上下文中，发起者是启动（发起）CS 过程的蓝牙设备，反射者是响应（反射）CS 过程的蓝牙设备。在启动 CS 过程之前，通过链路层控制消息交换该过程的运行参数。

图 4-1 展示了在 CS 发起者和反射者之间执行基于相位的测距的大致 CS 流程。

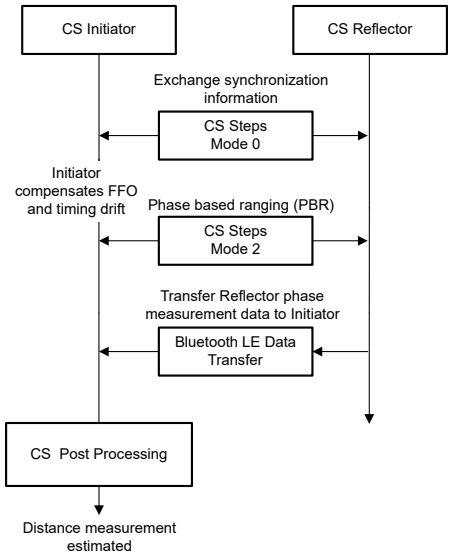



**图 4-1. 基于相位的信道探测测距概要流程**

在 CS 子事件开始时，必须执行 CS 模式 0 步骤，以便提供 CS 发起者和反射者之间的频率和定时同步，以供该 CS 子事件内的其余 CS 步骤使用。

多载波相位测距涉及在不同频率下进行相位差测量，而在生成这些频率时发生的任何相对误差（发起者和反射者设备之间）都可能会干扰这些相位测量并在总体距离估算中引入误差。因此，在每个单独的测量过程中，发起者和反射者设备需要保持其载波频率对齐，这一点很重要。根据蓝牙信道探测规范草案，发起者设备需要与发射者保持时间和载波频率对齐。该设备使用初始的模式 0 步骤，通过估算和补偿设备之间的分数频率偏移 (FFO) 来实现此步骤。

CS 模式 0 步骤之后是模式 2 PBR 步骤，其中发起者和反射者设备以不同的通道频率交换未调制的 CS 音调。

在 2.4GHz 无许可证 ISM 频段中的 79 个指定蓝牙信道中，具有 1MHz 信道间隔的 72 个信道可用于低功耗蓝牙、CS PBR（注意：低功耗蓝牙广播通道不适用于 CS PBR）。发起者和反射者都按照频率的函数测量传入音调的相位和振幅。完成所有 PBR 模式 2 步骤后，发起者和反射者设备都可以获得同相和正交相位（I 和 Q）测量形式的相位和振幅信息。接下来，反射者可以在低功耗蓝牙连接事件期间将该测量信息传达给发起者。注意：反之亦然，即发起者也可以将测量结果发送回反射者，以进行进一步处理。

接下来，发起者将来自两个设备的相位和真毒测量结果组合在一起，并执行后处理以估算距离测量值。蓝牙信道探测没有指定特定的算法来计算距离估算值，而是提供了一些使用相位测量值进行距离估算的数学表示。可以使用先进且高效的后处理算法来消除多路径和衰减效应，从而提供可靠的距离估算值。此外，可以使用音调质量信息来过滤因信号干扰和噪声而产生的异常值。可以使用具有不同复杂度和效率的后处理算法来计算距离近似值，同时考虑精度、功耗和计算延迟要求方面的权衡。

## 5 信道探测安全性

蓝牙信道探测规范草案已添加了不同的安全功能，以侦测或防止一种攻击，该攻击可以操纵测距过程，使两个有效 CS 设备之间的距离看起来比实际距离更近。有关安全功能的完整列表，请参阅信道探测规范草案。

用于距离估算的 PBR 过程可能受到中间人攻击的影响，通过执行中间人攻击，可以延迟或操纵正在进行的信号传输的相位，从而使得两个有效设备之间的距离测量值偏小。为了缓解这些攻击，蓝牙信道探测规范规定了 PBR 期间的频率随机跳频，并另外增加了往返时间 (RTT) 测量，这是测量两个设备之间距离的另一种方法。由于使用 1MHz 跳频的 PBR 最大不模糊可测量距离为 150m（有关计算方式，请参阅方程式 1），因此 RTT 飞行时间测量尽管不如 CS PBR 机制精确，但仍然是识别翻转攻击的可行选项。

**备注**

使用 PBR 时的最大可测量距离取决于两个频率信号之间的最大可测量相位差。由于任意两个音调之间的最大相位差为 2* $\pi$，而 CS 音调相隔 1MHz，因此最大可测量距离 dmax 可通过以下公式得出：

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

使用 RTT 飞行时间测量数据进行距离估算如图 5-1 所示。

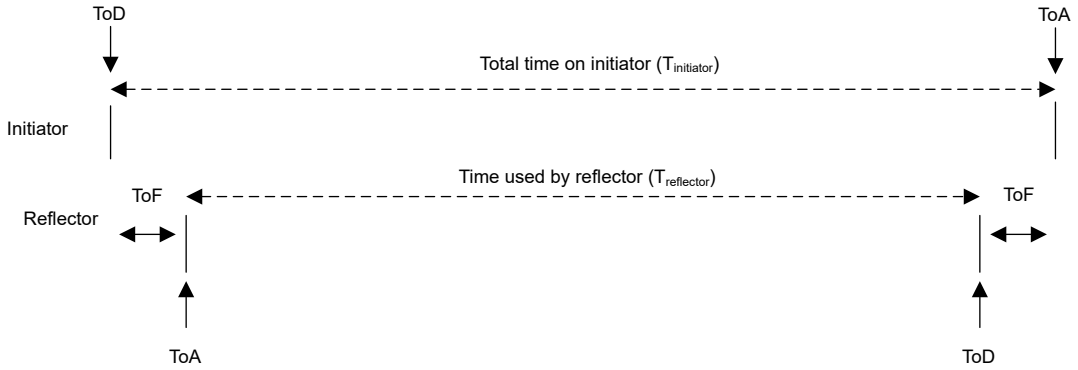



**图 5-1. 用于 RTT 估算的到达时间 (ToA)、离开时间 (ToD) 和飞行时间 (ToF)**

发起者和反射者之间进行 RTT 数据包交换。这些 RTT 数据包在发起者和反射者处的离开时间 (ToD) 和到达时间 (ToA) 用于估算飞行时间。CS 步骤模式 1 和模式 3 允许进行 RTT 数据包交换。

蓝牙 CS 规范还支持使用随机序列（仅发起者和反射者知道）的 RTT 数据包进行通信，因此越来越有可能测量接收到的 GFSK 调制数据包和预期数据包信号（参考）之间的差异。此测量表示为标准化攻击检测指标 (NADM)，它是一个范围，表明中间人攻击者试图转发 RTT 数据包（通过操纵信号使其提前）以执行 ECLD（提前提交/延迟检测）和 EDLC（提前检测/延迟提交）类型攻击的机会是增加还是减少。NADM 算法用于确定链路两侧每个 CS 设备中接收到的 RTT 数据包的 NADM 值。NADM 算法定义和实现超出了蓝牙 CS 规范的范围。

## 6 总结

即将推出的蓝牙信道测深功能可满足定位服务解决方案的关键要求，包括相对于先前蓝牙解决方案对更远距离的高精度测量以及更高的安全性。这些关键因素与低功耗蓝牙技术的低功耗属性以及在智能手机、消费类物联网、工业和汽车应用中的广泛应用相结合，使该技术成为一种面向高精度、低成本、安全测距解决方案的超有前途的技术。

作为蓝牙 SIG 的会员，德州仪器 (TI) 正在与 SIG 积极合作，共同推动信道探测技术的规范制定。TI CC2340R5 和即将推出的 TI 低功耗蓝牙器件在器件的射频内核以及软件开发套件 (SDK) 的蓝牙堆栈中支持即将推出的蓝牙信道探测技术。所有信道探测模式（包括模式 3 基于相位的测距和 RTT 数据包交换）均受到支持。要获得与即将推出的 TI 信道探测演示、工具和示例有关的更多信息，请发送电子邮件至 connectivity_auto_marketing@list.ti.com，或联系您当地的 TI 销售办事处。

**备注**

蓝牙信道探测规范仍处于草稿状态。在最终发布之前，本应用手册将按照规范草稿的更新按需进行更新。

## 7 参考资料

1. Bluetooth，*信道探测规范草案*。
2. *On the Security of Carrier Phase Based Ranging*, Hildur Ólafsdóttir è s, Aanjhan Ranganathan, Srdjan Capkun, ETH Zurich.

# 附录 A：基于相位的测距和多载波相位测距的基础知识

基于相位的测距 (PBR) 系统涉及测量两个实体之间传播的无线电信号的相位变化，从而确定它们之间的距离。

下面来看看一个测距例子，其中实体 A（发起者）正在测量其与实体 B（反射者）的距离。在理想的 PBR 系统中，实体 A 通过在特定频率 f 下发送未调制连续波音调启动测试过程。实体 B 接收到此射频信号后，会充当真正的反射者，将本地振荡器锁定到传入射频信号并将其传回给发起者。最后，发起者通过测量接收信号与自身本地振荡器信号之间的相位差来确定距离。图 8-1 展示了射频信号处于特定频率时基于相位的测距。实体 A 是发起者，实体 B 充当真正的反射者，将其 LO 锁定到传入射频信号并将其传回给发起者。

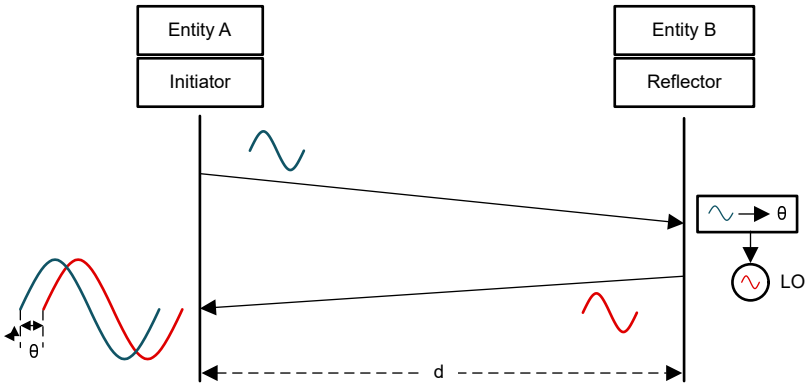



**图 8-1. 射频信号处于特定频率时基于相位的测距**

如果发起者和反射者之间的距离 d 小于信号的波长（即 $\frac{2 \times f}{c}$ ，其中 f 是 RF 音调的频率，c 是光速），那么测得的相位偏移或相位差 $\theta$ 是：

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

然而，在实际应用中，需要测量的距离可能长于信号波长。为了做到这一点，必须追踪射频音调在两个实体之间传播时所经过的完整周期数量。假设 n 是经过的完整周期数（整数），则距离 d 的测量公式为：

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

为了消除追踪经过的完整周期数的需求，采用了多载波相位测距方法。在多载波相位测距系统中，会在多个射频音调频率上进行相位测量（接收到的信号与其自身本地振荡器信号之间的相位差）。在相同距离（因此具有相同的传播时间）传输不同频率的射频信号可能会有不同的相位偏移或相移。

举例来说，假设发起者和反射者设备之间的距离为 d，它们在两个频率 f1 和 f2 上执行 PBR（具体如图 2-1 中所述）。也就是说，设备首先在射频信号频率 f1 上执行 PBR，然后在射频信号频率 f2 上再次执行 PBR。在 f1 和 f2 上测得的相位差如下所示：

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

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

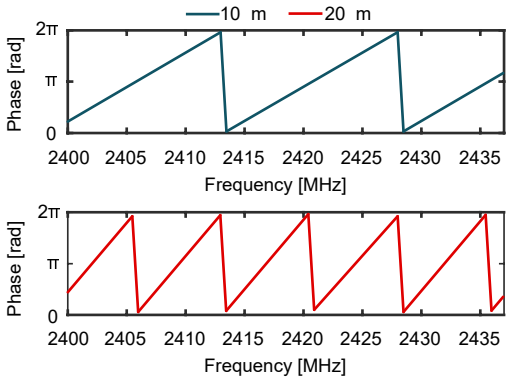
通过结合方程式 4 和方程式 5 以消除完整周期数 (n) 的不确定性，距离 d 现在表示为：

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

为了在实际应用中获得更高的测距精度和分辨率，需要在两个以上频率下进行相位偏移测量。此外，如果将相位偏移测量数据绘制为相位与频率间的关系曲线，则曲线的斜率就代表着发起者和反射者之间的距离 d。请参阅图 8-2 和图 8-3。方程式 6 可以视为一条直线，其斜率与距离成正比：

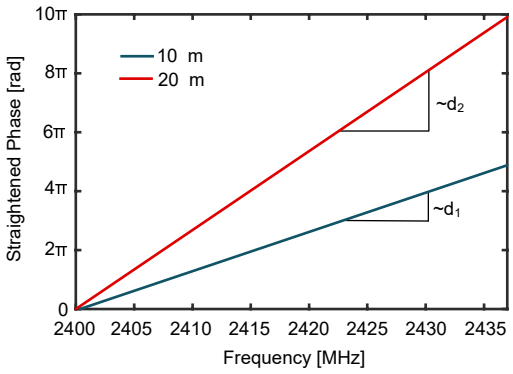
$$d = \frac{c}{4\pi} \times slope \tag{7}$$

参考资料 [2] - 图 8-2 展示了发起者和反射者之间两个不同距离 d1 = 10m 和 d2 = 20m 下测得的相位差与频率之间的关系。这些相位差环绕在 2 π 周围，可以按照图 8-3 所示进行展开，以计算有效相位斜率并估算发起者和反射者之间的距离。




(a) The phase of the received signal.

**图 8-2. 测得的相位与音调频率间的关系（环绕 2 π ）**




(b) The straightened phase of the received signal.

**图 8-3. 测得的相位与音调频率间的关系（展开后的相位）**

# 重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265