

探索蓝牙信道探测

高精度距离测量及其用例

Wayne Wang – 芯科科技中国区高级现场应用工程师

tech talks



BLUETOOTH

议程大纲

- 01** 信道探测(**Channel Sounding**)协议概述
- 02** 应用案例
- 03** 性能数据
- 04** 芯科科技解决方案
- 05** **Q&A**

信道探测协议概述

信道探测综合介绍

- 测量两个设备之间的距离
 - 基于相位的测距 (Phase-based Ranging, PBR)
 - 往返时间 (Round Trip Time, RTT)
- **RTT和PBR在2.4 GHz频段上工作**
 - 标准规定了多达**72**个通道
 - 随机切换模式 (Random hopping pattern)
- 面向连接的两种测距方法和角色
 - 启动器 (Initiator) : 希望计算自身到另一个设备的距离的设备
 - 反射器 (Reflector) : 对启动器进行响应的设备
- 设备间最多支持**4**条天线路径
 - **8**种可能的天线组合
- 标准中包含多项安全功能
- 可与到达角/离开角(**AoA/AoD**)结合使用
 - 允许单对启动器/反射器的位置估算
- 预计将于**2024**年纳入蓝牙技术联盟规范
 - 初版信道探测规范草案:
<https://www.bluetooth.com/specifications/specs/channel-sounding-cr-pr/>

规范中包含的内容

- 射频和链路层的定时和功能要求
- 强制性 **vs.** 可选特性和模式
- 天线配置和安全特性指南

规范中尚未包含的内容

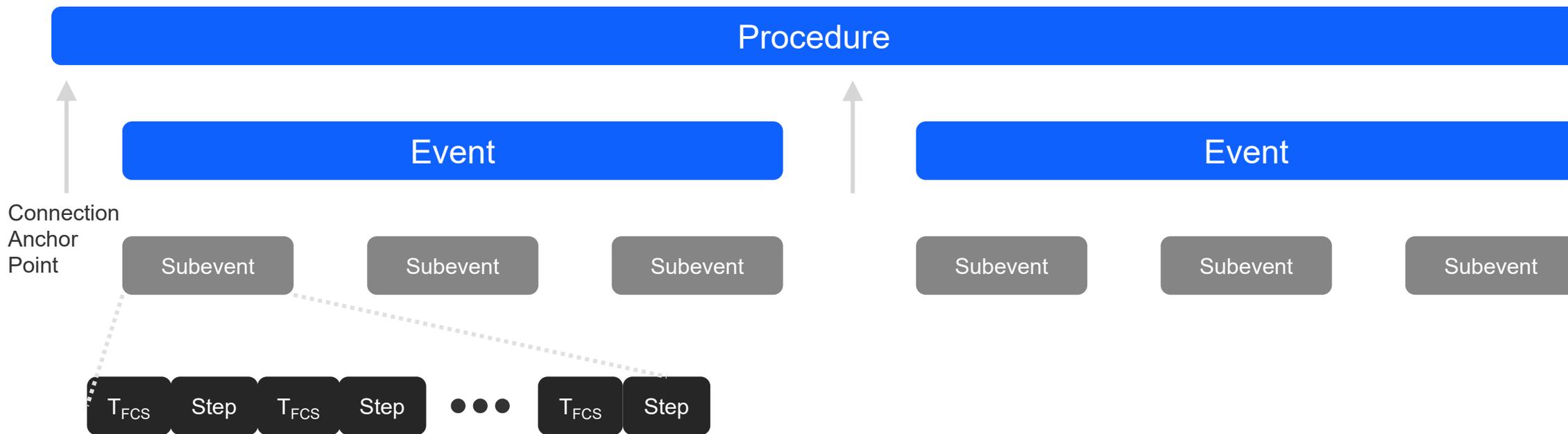
- 距离测量算法的建议和优化

中心和外设设备的信道探测设置



注意：虽然这种交换发生在每个信道探测过程开始之前，但如果之前已经缓存了信息，则可以在设置期间跳过其中一些步骤

信道探测程序 -> Event -> Subevent -> Step



- 由事件组成的**Procedure**可以跨越多个连接间隔
- **Subevent**需要在单个连接间隔内完成
- **Step**对应于设置、PBR或RTT测距，定义为4种模式

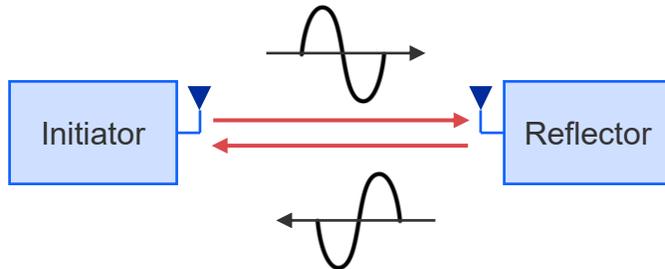
信道探测 Step Modes

Mode-0: 校准 (Calibration)

- 补偿时钟漂移和频率偏移
- 结果在分数频率偏移表

Required

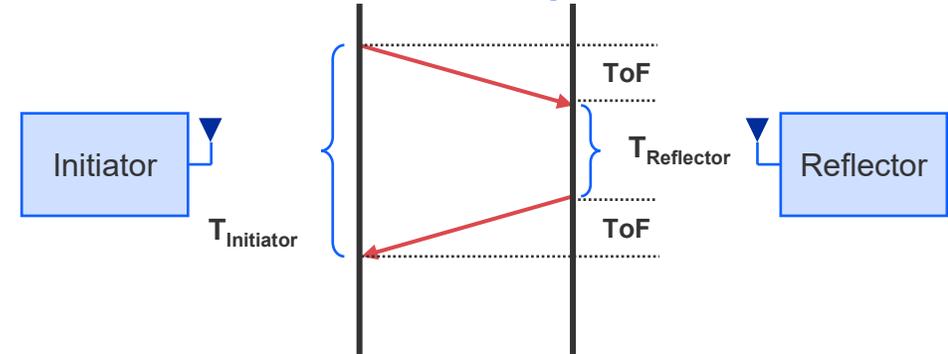
Mode-2: 相位测距 (Phase based ranging)



- 启动器和反射器之间的CS Tone交换
- 在每个步骤中执行每个天线路径

Required

Mode-1: 往返时间 (Round trip time)



- 在启动器和反射器之间交换的CS SYNC数据包

Required

Mode-3: PBR+RTT

- 在每个步骤中结合PBR和RTT
- RTT距离测量可以与PBR结果交叉核对
- 提供更高的安全性，因为距离估计中的不匹配可能间接指向中继攻击

Optional

信道探测安全特性

- 潜在的漏洞
 - 假冒（**Spoofing**）
 - 中间人攻击（**MITM**）或中继攻击
- **Deterministic random bit generator (DRBG)**
 - 在安全启动数据交换期间初始化
 - 搅乱启动器和反射器之间的位序列
 - 在**tone extension**，天线路径选择和更多部分的随机有效载荷
- 交叉检查**PBR**和**RTT**
 - 可以在**Mode 1** 步骤中使用**Mode 2** 作为子模式或使用**Mode 3**来完成
 - 距离估算不匹配指明为中继攻击
- **Normalized Attack Detector Metric (NADM)**
 - 检测接收信号中意外的位转换或相位变化
 - 标准不包括实施要求
 - 目前规定的规模异常是分类的
 - 可选特性

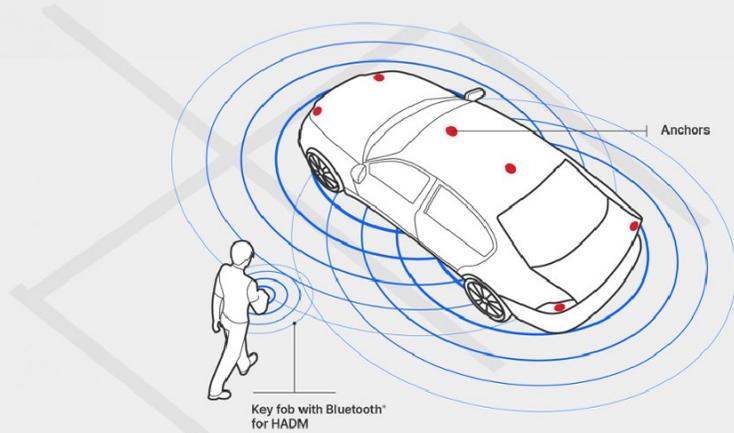
低功耗蓝牙定位服务比较

	RSSI	到达角 (Angle of Arrival)	信道探测 (Channel Sounding)
本地化指标	解决距离估算发射机信号强度	解决两点之间的相对夹角	使用飞行时间和基于相位的测距来解决两点之间的距离
天线要求	单天线	规格要求多天线	不需要多天线，但对最佳位置分辨率有用
低功耗蓝牙连接性	面向连接和无连接	面向连接和无连接	面向连接
性能指标	+/- 5 m, 对多径干扰的敏感性高	+/- 3 度精度—方位角 +/- 5 度精度—仰角	+/- .3 m < 5m 带PBR测距 +/- 0.5 m > 5m 带PBR测距
解决方案的优势	<ul style="list-style-type: none"> 在现有的低功耗蓝牙产品中普遍支持RSSI测量 	<ul style="list-style-type: none"> 实时位置跟踪的可扩展解决方案 支持5-10年的电池寿命 	<ul style="list-style-type: none"> 外形小巧，天线设计灵活 通过邻近传感增加安全功能

应用案例

—

信道探测—地理围栏（Geo-Fencing）应用



接近时解锁：

- 远程无钥匙进入
 - ▶ 通过测距的区域检测以确保安全车辆进入
 - ▶ 用户体验增强，如唤醒/欢迎响应
- 基于邻近传感的锁定和解锁
 - ▶ 在一定的距离自动门锁和开锁
- 预防丢失
 - 零售防盗
 - ▶ 跟踪商店内高价值物品的位置，如果它们被移出指定区域，就会触发警报。
 - 未经授权移动的地理围栏通知
 - ▶ 在检测到未经授权的移动或在特定边界外移动的货物时发送警报。

信道探测—室内设施应用

访问控制

- 限制未经授权人员进入
- 如果有人停留在该地区太长时间，将发送警报到本地服务器/云

入口访问

当被授权的员工接近门时，对他们进行认证并允许他们进入

资产管理

- 工厂内库存的粗略定位
- 帮助工作人员提高效率



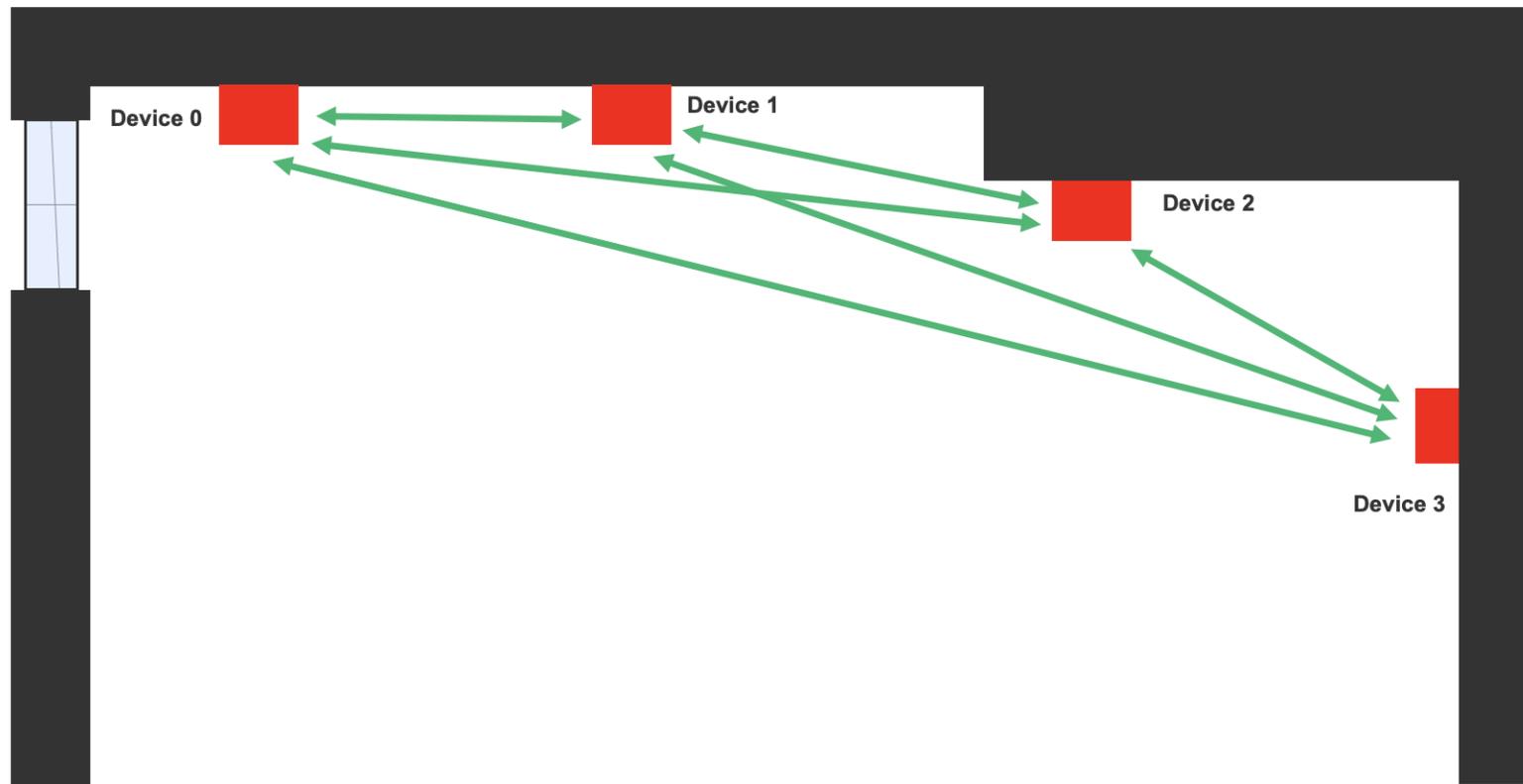
距离测量演示



Distance Measurement Demo



信道探测—静态设备定位



- 使设备定位静态设备，如灯具或接入点。
- 这些装置作为启动器和反射器来计算彼此之间的距离，从而创建一个几何地图。

静态设备定位演示



Static Device Positioning



性能数据

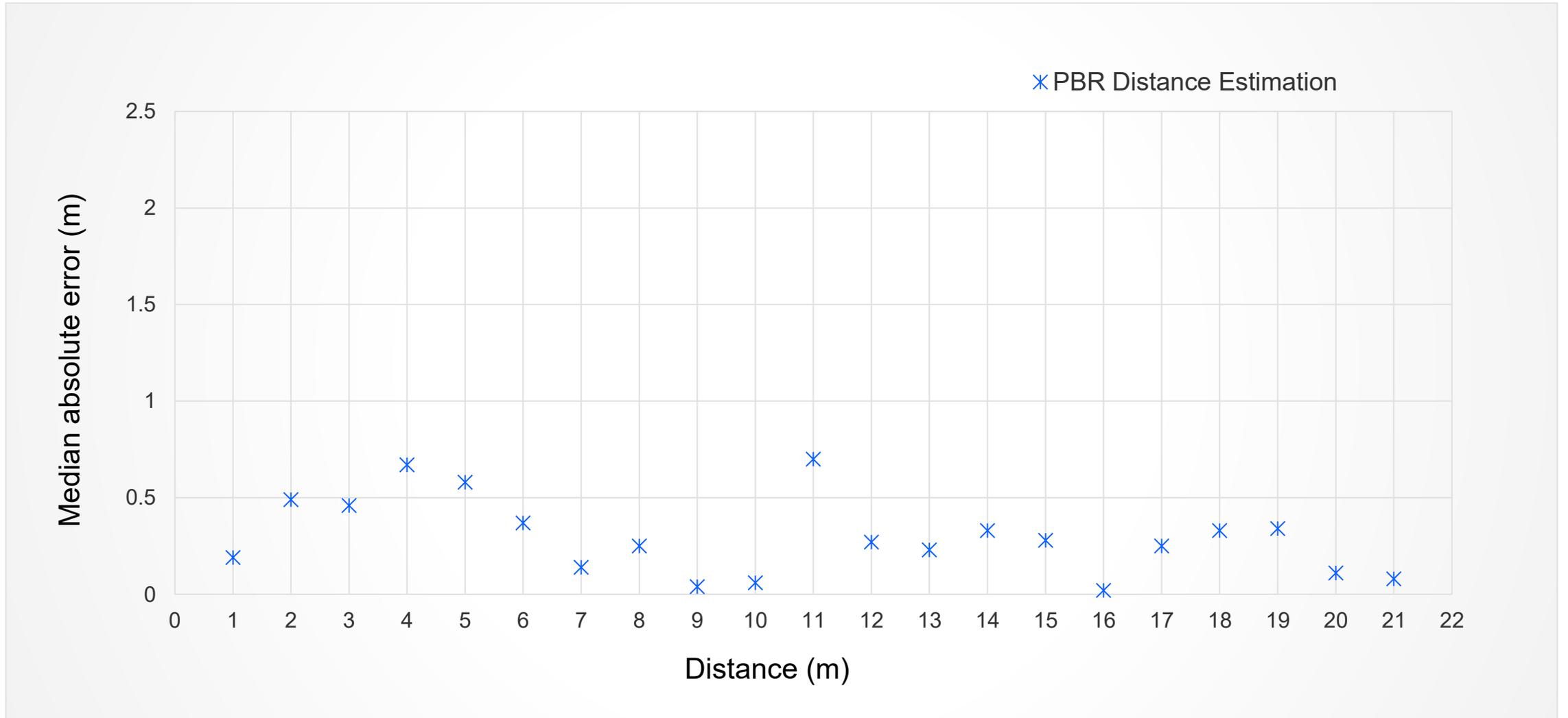
—

在室内办公环境的性能表现

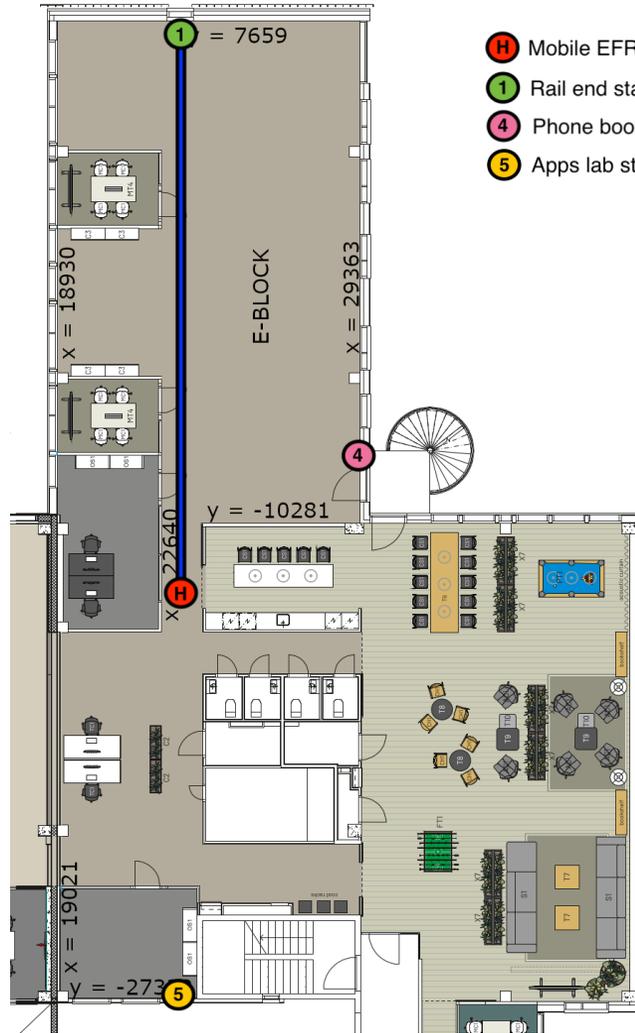


- 天花板轨道设施
 - 内部测试环境
 - 多个固定的**EFR32**设备放置在不同位置
 - 用于控制测量的移动**EFR32**装置(可重复)
- 挑战一在室内办公室环境有严重的多径效应
- 统计分析
 - 静态测量在多个距离可达**30**米
 - 每距离数百次测量，以确定最小/最大，平均值，中位数，标准，绝对误差

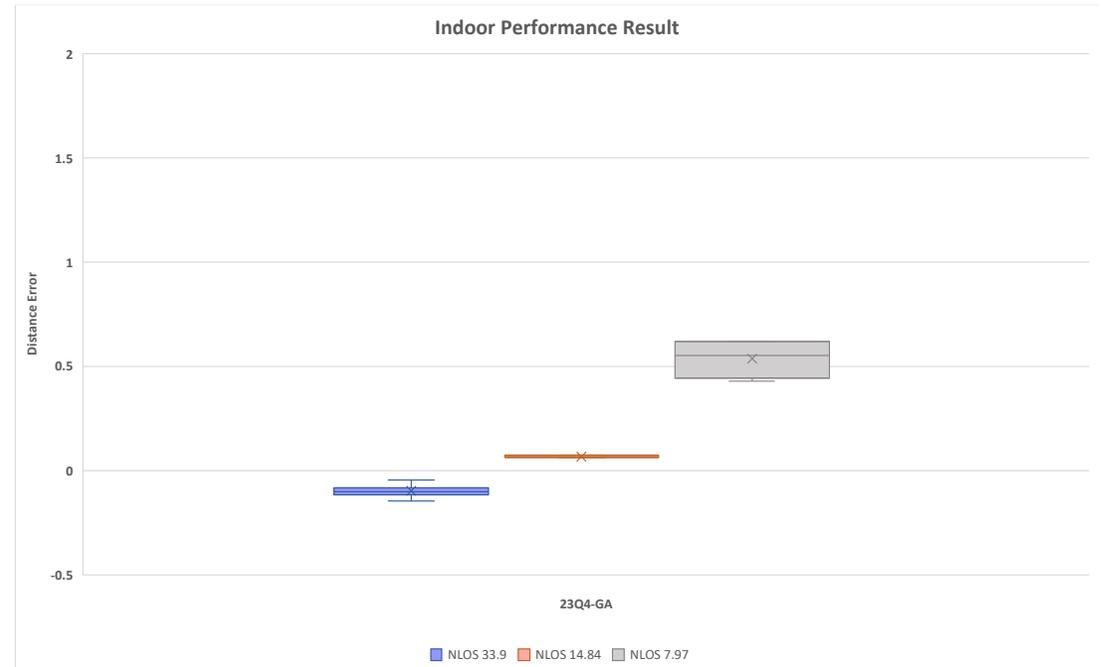
室内表现结果—Line of Sight



室内表现结果—Non-Line of Sight



1 – 5 = NLOS
 33.9m
 1 – 4 = NLOS
 14.84m
 H – 4 = NLOS 7.9m



芯科科技解决方案

—

BG24: 针对电池供电，支持信道探测的物联网设备进行了优化



- 5x5 QFN40 (26 GPIO)
- 6x6 QFN48 (32 GPIO)
- 3.1x3.0 WLCSP42

差异化特性

- 极小外型
 - 3.1 x 3.0 WLCSP package
- **+20 dBm**输出功率
 - Eliminates need for external power amplify
- **AI/ML**硬件加速器
 - Accelerates inferencing while reducing power consumption
- **Secure Vault High**
 - Protects data and device from local and remote attacks
- **20-bit ADC**
 - 16-bit ENOB for advance sensing
- 优化的共存
 - Ideal for gateways and hubs
- **PLFRCO**
 - Eliminates need for 32 KHz xtal

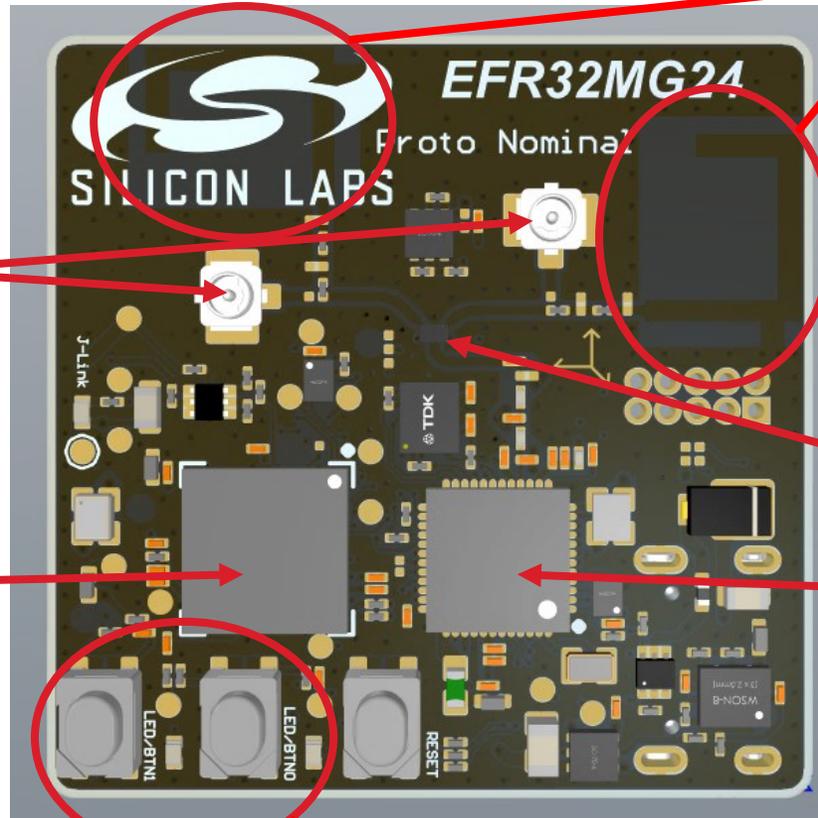
设备规格

- 高性能射频
 - Up to +19.5 dBm TX
 - -97.6 dBm RX @ BLE 1 Mbps
- **Efficient ARM® Cortex®-M33**
 - Up to 78 MHz
 - 1536kB Flash, 256kB RAM
- 低功耗
 - 49.1 μ A/MHz (CoreMark)
 - 5.0 mA TX @ 0 dBm
 - 5.1 mA RX (802.15.4)
 - 4.4 mA RX (BLE 1 Mbps)
 - 1.3 μ A EM2 sleep
- 多协议支持
 - Bluetooth 5.4 (1M/2M/LR), Bluetooth mesh, Proprietary 2.4 GHz

双天线信道探测板一正面

2x U.FL connector 可选的外部
天线支持

On-board debugger 便于编
程和调试



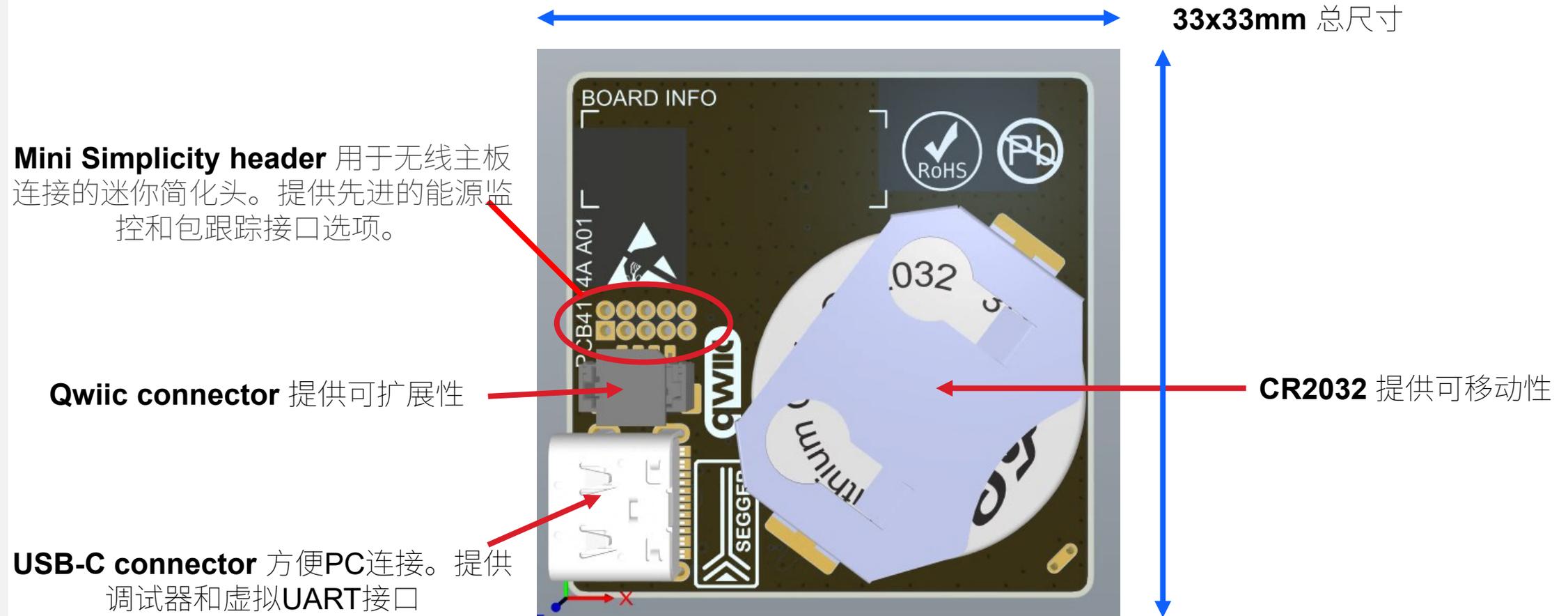
2x PCB antenna 用于天线分
集和双极化

1-to-2 RF switch

EFR32MG24B210F1536IM48-B
我们功能最强的xG24系列
(带1.5MB闪存, 信道探测, MVP, Secure
Vault High, +10dBm)

User buttons and LEDs
固件演示支持

双天线信道探测板一背面



可视化工具



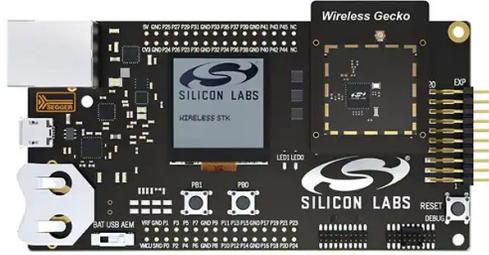
可视化工具显示实时数据

- 信道探测数据与RSSI读数进行比较
- 信道探测接口SDK

即将到来的新特性

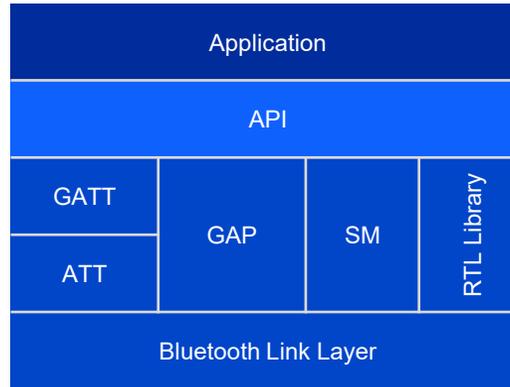
- 数据记录 (Date logging)
- 信心度显示 (Confidence metric display)
- 信道映射选择 (Channel map selection)

芯科科技提供全方位的信道探测解决方案



开发套件

BRD4198A with Single Antenna
Wireless Pro Kit
EFR32MG24 + 10dBm OPN
BRD2606A with Dual Antennas



软件协议栈

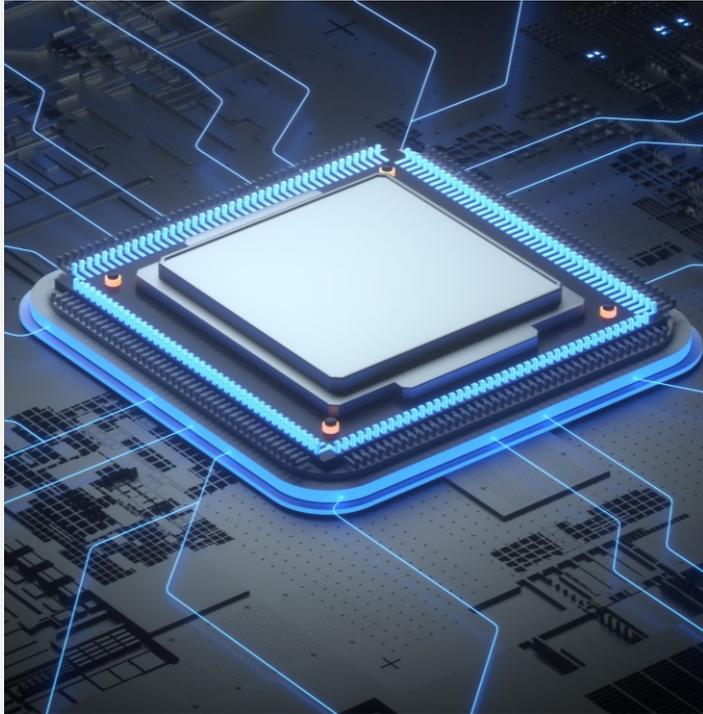
In-house developed stack
Supports Bluetooth 5.4 features + Channel
Sounding
New and improved Ranging features



开发工具

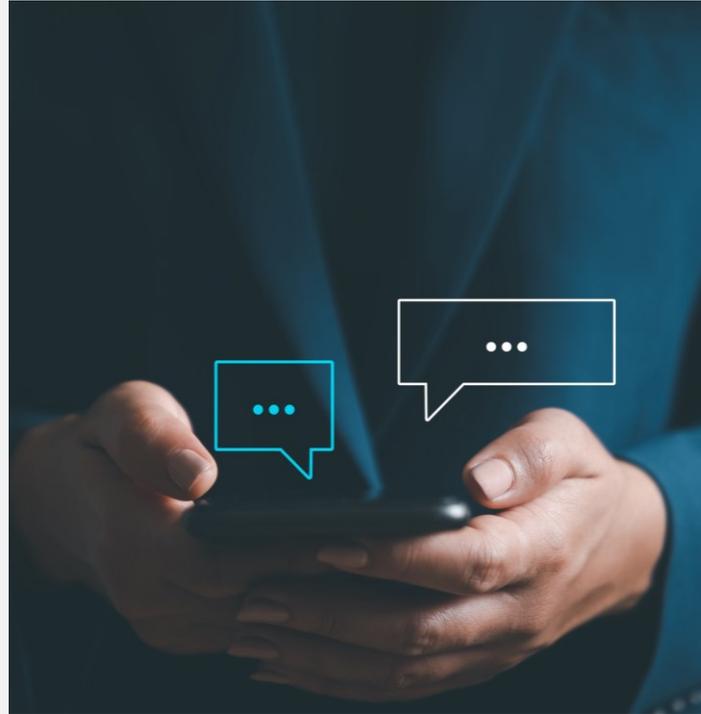
Real-time visualization tool
PBR, RTT modes
CS Sample projects
CS Analyzer + Energy Profiler +
Network Analyzer
App note + Salesforce Support

即刻开始设计



早期访问

成为我们正在进行的信道探测的早期访问计划的一部分，以获得我们的开发工具。



联系我们

如有任何问题或欲加入我们的抢先体验计划，请联系本地销售团队。



更多信息

欲了解更多有关信道探测和芯科科技的产品，请访问官网：

<https://www.silabs.com/wireless/bluetooth/channel-sounding>

Q&A

