



蓝牙核心规范 v5.1

功能概述

蓝牙核心规范 v5.1 包含对蓝牙®核心规范的一系列更新。本文档总结并解释了每项更改。

请参阅蓝牙核心规范 v5.1 以了解完整详情。

作者: 马丁·伍利

版本: 1.0.1

修订日期: 2020 年 12 月 9 日

修订历史

版本	日期	作者	更改
1.0.0	2019 年 1 月 28 日	马丁·伍利	初始版本
1.0.1	2020 年 12 月 9 日	马丁·伍利	语言变化



表 内容

1.0 测向.....	4
1.1 概述	4
1.2 技术细节	5
2.0 GATT 缓存增强功能.....	6
2.1 背景 2.2 改进的缓存策略 2.3 更好的状态管理	6
2.3 更好的状态管理	7
2.3 更好的状态管理	8
3.0 广告增强1:随机广告	
频道索引.....	9
3.1 背景 3.2 改进的数	9
据包冲突避免	9
4.0 广告增强功能2:定期广告	
同步传输.....	10
4.1 背景	10
4.2 二的力量	10
5.0 小幅增强.....	11
5.1 HCI 对 LE 安全连接中的调试密钥的支持	11
5.2 休眠时钟精度更新机制 5.3 扫描响应数据中的ADI字段 5.4	11
QoS与流规范的交互	11
5.5 主机通道分类	11
二次广告	12
5.6 允许 SID 出现在扫描响应报告中 12	
5.7 指定违反规则时的行为	12

1.0 测向

概述

蓝牙近距离解决方案和定位系统目前使用信号强度来估计距离。蓝牙核心规范 v5.1 中的新测向功能使蓝牙设备能够确定蓝牙信号传输的方向。

此新功能提供两种不同的方法,可高精度地确定蓝牙信号的发射角度。这两种方法称为到达角 (AoA) 和出发角 (AoD)。

每种技术都要求两个通信设备中的一个具有多个天线阵列,当使用 AoA 方法时,天线阵列包含在接收设备中,当使用 AoD 时,天线阵列包含在发送设备中。

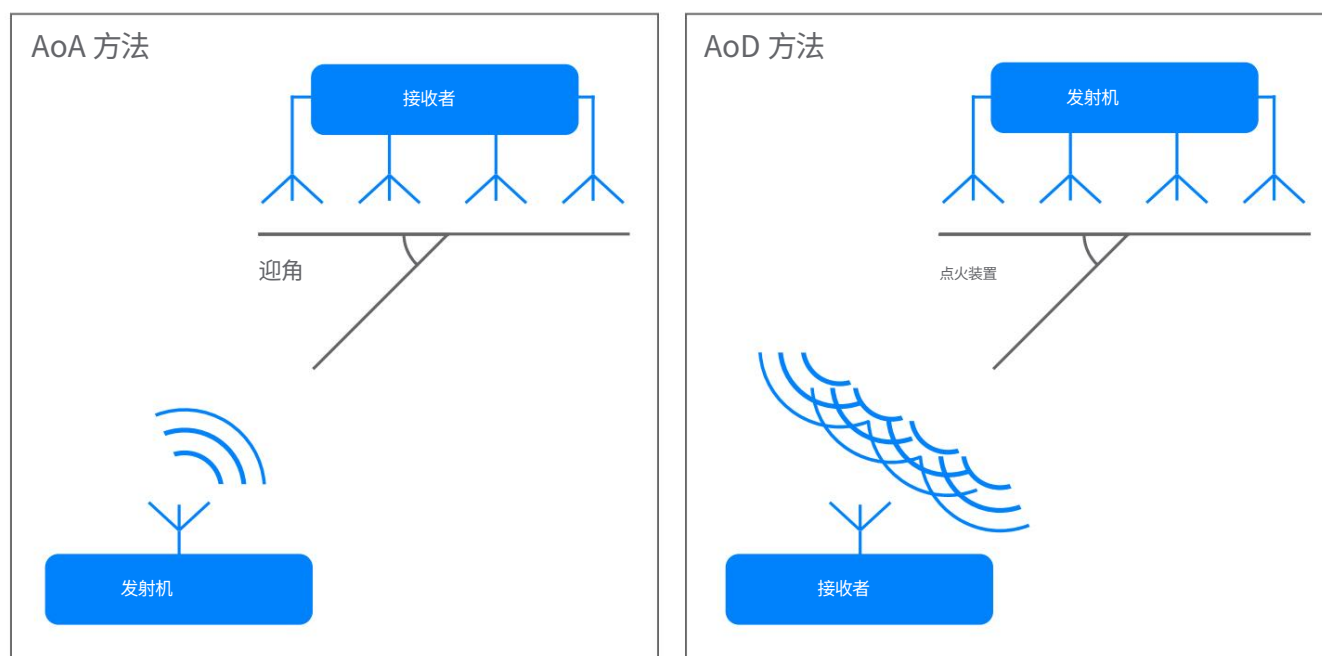


图 1 - 到达角 (AoA) 和出发角 (AoD)

蓝牙核心规范 v5.1 使接收设备中的蓝牙低功耗 (LE) 控制器能够生成数据,然后可以使用该数据来计算与发射设备的方向角。

此次发布的蓝牙核心规范中加入了测向功能,这是蓝牙发展路线图中的几个步骤中的第一步,最终将实现蓝牙定位服务的关键增强。相关配置文件发布后,蓝牙开发人员将能够利用新的测向控制器功能来创建高精度、可互操作的定位系统,例如实时定位系统 (RTLS) 和室内定位系统 (IPS)。

新的测向功能还可以通过确定设备方向来增强蓝牙近距离解决方案,特别是在定向项目查找和兴趣点信息解决方案中。

技术细节

蓝牙测向功能使用同相和正交 (IQ) 采样来测量特定时间入射到天线的无线电波的相位。在 AoA 方法中,采样过程将逐个应用于阵列中的每个天线,并根据阵列的设计以某种合适的顺序进行。

采样数据通过主机控制器接口 (HCI) 向上传递到堆栈,然后可以对采样数据应用合适的算法来计算一个设备相对于另一个设备的方向。此核心规范版本未定义从 IQ 样本计算角度的算法。一旦相关配置文件可用,应用程序开发人员将有机会实现适合预期用例的算法。

为了支持 IQ 采样以及堆栈中较高层对 IQ 样本的使用,链路层 (LL) 和 HCI 都进行了相应的更改。

在链路层,定义了一个称为恒定音调扩展 (CTE) 的新字段 (见图 2)。CTE 字段的目的是提供恒定频率和波长信号材料,以便执行 IQ 采样。此字段包含一系列 1,不受通常的白化过程的影响,也不包括在 CRC 计算中。

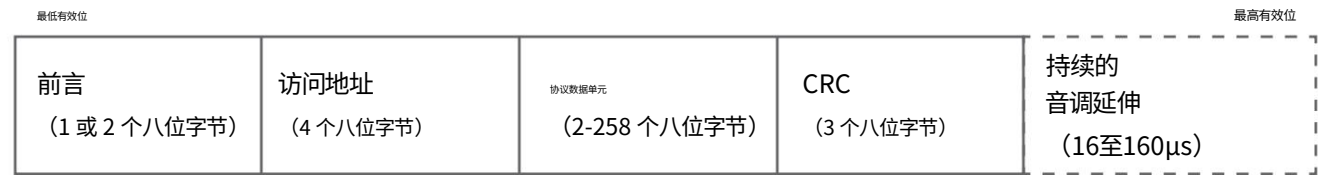


图 2 - 恒定音调扩展

CTE 既可用于无连接场景,也可用于面向连接场景。对于无连接使用,需要定期广告功能 (因为采样过程中的确定性定时很重要),并且 CTE 附加到 AUX_SYNC_IND PDU。对于面向连接使用,已定义新的 PDU LL_CTE_REQ 和 LL_CTE_RSP。无论哪种情况,都有新的 HCI PDU 允许配置 CTE PDU 的各个方面,例如 CTE 长度、天线切换模式的长度和天线 ID。

2.0 GATT 缓存增强功能

背景

所有低功耗蓝牙连接设备均使用通用属性配置文件 (GATT)。因此,GATT 缓存这一主题与多种设备类型相关。

GATT 设备包含一个称为属性表的数据库。属性表包含 GATT 服务、特性和描述符结构详细信息和值,是 GATT 低功耗蓝牙设备工作方式的核心。属性表中的条目由属性句柄标识。

GATT 客户端必须执行称为服务发现的过程,以获取客户端所连接的远程 GATT 服务器设备上的属性表的详细信息。然后,客户端可以在与服务器的后续属性协议 (ATT) 交互中使用这些详细信息 (包括识别属性句柄)。

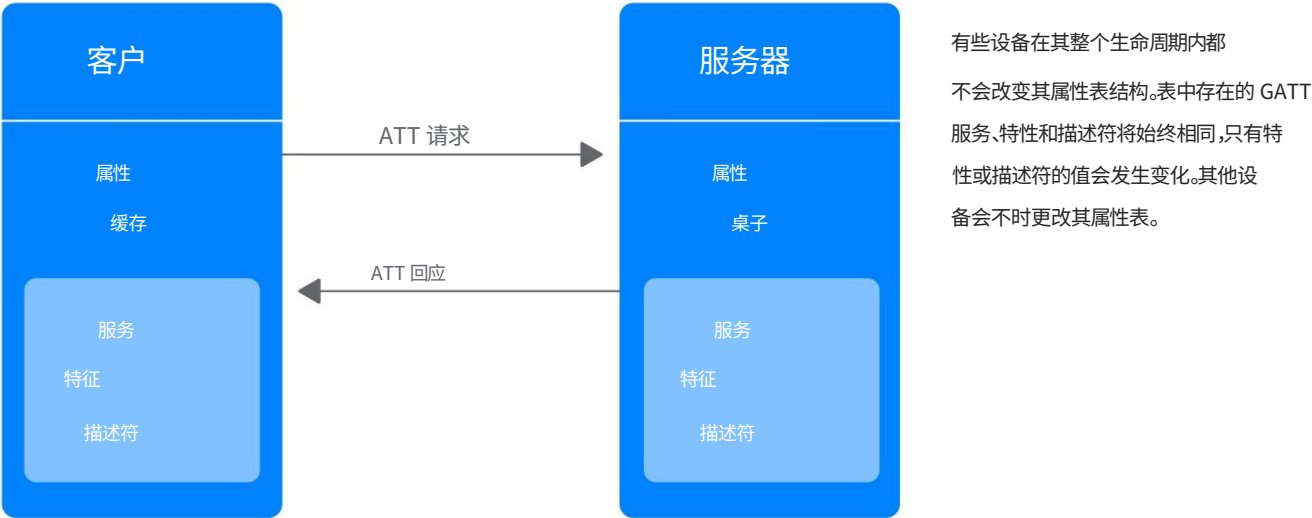


图 3 - 服务发现和属性缓存

服务发现需要时间并消耗能源。因此,蓝牙核心规范 v5.1 定义了一种属性缓存策略,旨在允许客户端在没有任何变化时跳过服务发现。

以前,缓存和客户端/服务器属性表同步仅使用通用属性服务中可能存在的服务更改特性进行控制。GATT 服务器可以通过向客户端发送 ATT 指示来通知连接的客户端其属性表已更改。客户端回复 ATT 确认并执行服务发现以将其属性缓存与服务器的属性缓存同步。

为了避免 GATT 服务器需要跟踪每个连接到它的客户端,以及每个客户端是否已获悉最新的属性表更改,以前核心

规范规定,没有信任关系(即未绑定)的客户端和服务端每次连接时都必须执行服务发现。这条规则可能会导致某些类型的产品的能源效率和用户体验问题。

此外,除了尝试使用 ATT 服务更改指示通知客户端属性表已更改之外,没有针对客户端对属性表的视图与服务端对属性表的视图进行进一步的状态管理。该方法允许客户端和服务端之间的通信中存在竞争条件,就属性表更改和一般 ATT 交互而言,客户端在连接到服务端后等待服务更改指示时可能会超时,继续发送一般 ATT PDU,然后接收服务更改指示。

改进的缓存策略

此版本对 GATT 客户端和服务端处理属性缓存和缓存同步的方式进行了更改。它允许与服务端没有信任关系的客户端在连接之间保留其属性缓存,从而显著改善了用户体验并提高了能效,并解决了上述竞争条件问题。

引入了两个新特性,每个特性都是通用属性服务的成员:数据库哈希和客户端支持的功能。如果客户端支持新的数据库哈希特性(如客户端更新服务端的客户端支持的功能特性中的标志所示),则与服务端没有信任关系的客户端现在可以跨连接缓存属性表。

数据库哈希特性允许客户端询问服务端是否有任何变化,而不是依赖服务端使用服务更改指示来告知它。服务端负责维护数据库哈希特性的值,该值是根据属性表的相关方面计算得出的哈希值。客户端在建立连接后立即读取其值。客户端可以缓存数据库哈希值,然后使用它来确定远程属性表是否已更改。如果已更改,客户端将再次执行服务发现。如果没有,则不需要。这为某些类型的设备提供了巨大的用户体验和能效优势。

此外,客户端现在可以推断出它所连接的设备与之前连接的设备属于同一类型,并且其属性表已被客户端缓存。如果来自连接设备的数据库哈希与与客户端的属性缓存相关联的数据库哈希相同,并且设备制造商等其他详细信息相同,则客户端可以得出结论,无需为连接的设备执行服务发现,因为从另一个设备获得的属性缓存已经包含等效数据。

对于某些应用来说,这一变化具有相当大的价值。例如,考虑蓝牙智能锁,智能手机或其他客户端设备与建筑物的门交互,以便在用户接近时进行身份验证并为其开门。服务发现只需要在用户第一次尝试通过带有智能锁的门时执行。用户可能会感觉到延迟

在第一次使用时,门不会解锁,但随后当用户接近楼宇服务发现中的任何门时,将不需要服务发现,并且用户将体验到智能锁的近乎即时的响应。

更好的状态管理

状态机定义属性表的客户端视图与其属性表的服务器视图是否同步,以及客户端是否需要执行服务发现。

属性缓存的修订规范引入了严格定义的强大缓存概念,该概念形式化了该状态机并引入了使用它的机制。

客户端可分为感知变化状态和不感知变化状态。规范列出了转换到适当状态的精确规则,以及在这两种状态下应如何表现。

特别值得注意的是,如果服务器认为客户端属性表缓存与服务器的缓存不同步,则服务器可能会返回新的“数据库不同步” ATT 错误响应。当服务器处于更改不感知状态时,它将忽略从客户端收到的所有 ATT 命令。许多事件可以将客户端的状态转换为更改感知状态,包括服务器收到对其之前发送的服务更改指示的 ATT 确认,或者服务器使用 <<数据库不同步>> 错误通知客户端并随后从客户端收到其他 ATT PDU。

从客户端的角度来看,如果它进入了更改不可感知状态,它将不会使用其属性缓存,并将其视为无效。它将继续被视为无效,直到客户端的属性缓存和服务器再次同步。

3.0 广告增强功能1:随机化广告渠道索引

背景

在蓝牙核心规范 v5.0 中,广告事件被定义为“在主广告渠道上发送的一个或多个广告 PDU,从第一个使用的广告渠道索引开始,到最后使用的广告渠道索引结束”。

实际上,这意味着当所有三个渠道都在使用时(通常情况下),广告会严格按照 37、38、39 的顺序使用渠道。

为了减少持续数据包冲突的可能性(两个或多个设备在重叠的时间段内在同一信道上进行广告宣传),蓝牙核心规范 v5.0 规定连续广告事件之间的时间必须包括 0 到 10 毫秒之间的随机延迟。

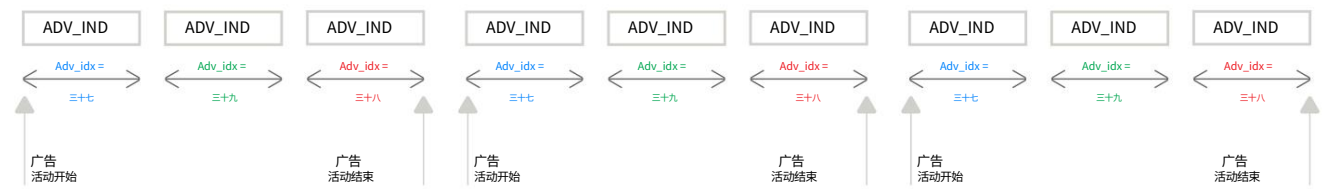


图 4 - 按照蓝牙核心规范 5.0 使用广告频道,固定顺序为 37、38、39

改进的数据包防冲突功能

在此版本中,处于广告状态的设备不再需要按照严格且不变的顺序选择广告渠道,从使用的最低渠道索引开始,到最高的渠道索引结束。现在可以随机选择渠道索引。广告渠道索引的随机化进一步降低了发生广告数据包冲突的可能性。

通过对广告信道索引选择实施这一改变,使用广告进行无连接通信的应用程序将受益于繁忙无线电环境中更高的可扩展性和可靠性。

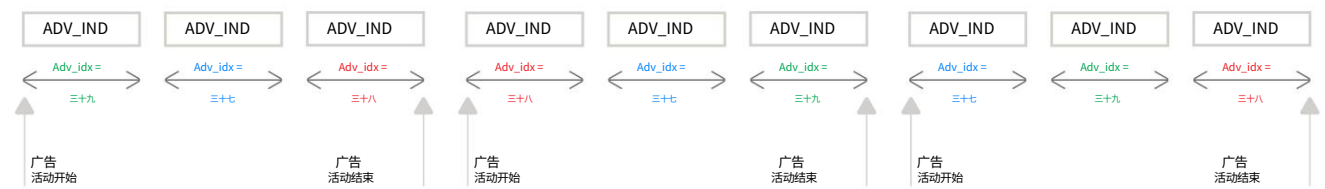


图 5 - 按照蓝牙核心规范 5.1 使用随机信道索引序列的广告信道

4.0 广告增强功能2:定期广告同步传输

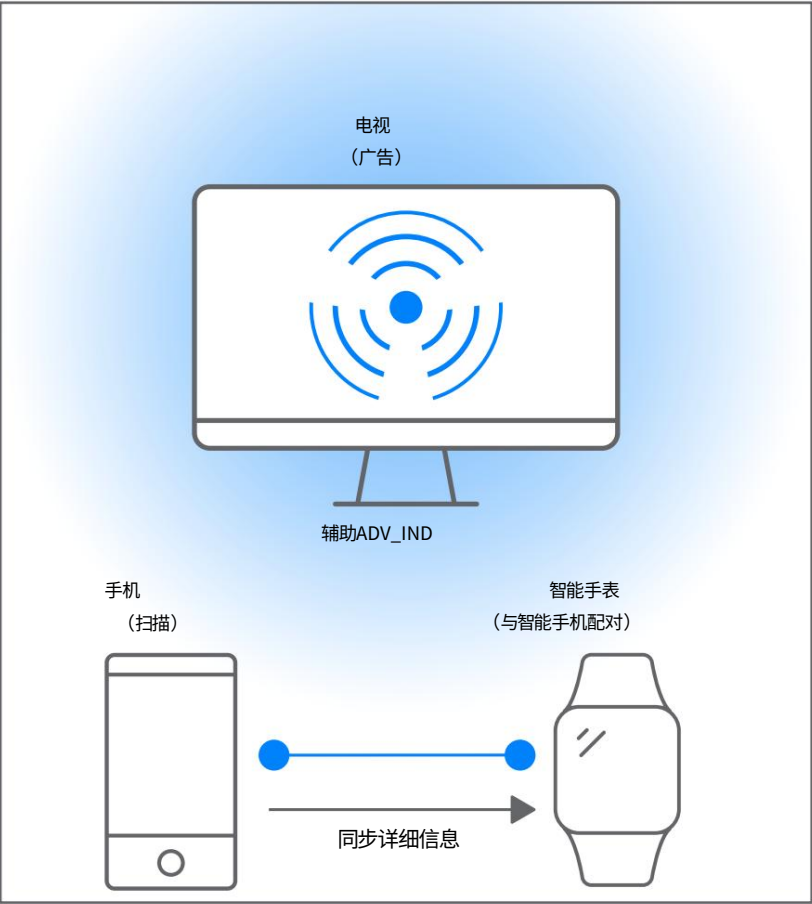
背景

蓝牙核心规范 v5.0 引入了定期广告,它使用确定性广告事件调度,并提供了一个程序,设备可以使用该程序将其扫描与另一台设备的广告调度同步。扫描和广告时间的同步可以使扫描设备更加节能,并且可以实现一些需要精确计时数据交换的用例。

为了与远程设备的定期广告同步,远程设备会广告包含名为 SyncInfo 的字段的 AUX_ADV_IND PDU.SyncInfo 包含接收设备需要知道的所有内容,以便从此时起与远程设备执行的 AUX_SYNC_IND PDU 定期广告同步。但是,这种定期广告同步过程可能是一项相对昂贵的操作。

两人的力量

某些类型的设备由于功率有限,可能无法承担与定期广告同步程序相关的能源成本,或者可能存在工作周期或扫描时间限制,从而阻止其工作。



新的定期广告同步传输 (PAST) 功能允许另一个限制较少的设备执行同步过程,然后通过点对点低功耗蓝牙连接将获取的同步详细信息传递给另一个限制设备。例如,智能手机可以扫描 AUX_

SYNC_IND 数据包从电视机发送,然后通过连接将它们传递到相关的智能手表,这样

手表可以受益使用定期广告和扫描从电视获取数据。

图 6 - 定期广播同步传输使用示例

细微改进

此版本的核心规范包含许多小的增强功能。

HCI 对 LE 安全连接中的调试密钥的支持

增强

LE 安全连接是一种蓝牙配对程序,它使用 Diffie Hellman 密钥协商协议来确保配对期间共享安全密钥的交换安全。Diffie Hellman 使用非对称椭圆曲线加密技术,包含一个公钥和一个私钥。这使得在开发和测试期间无法获取共享密钥并将其用于跟踪和调试连接。

在蓝牙核心规范 v4.2 中,定义了用于测试目的的硬编码密钥值。但是,如果在控制器中实现椭圆曲线算法,主机就无法表明它想要使用这些算法。最新版本的核心规范添加了一个 HCI 命令,让主机告诉控制器使用调试密钥值。如果主机本身实现椭圆曲线算法,则不会受到此更改的影响。

睡眠时钟精度更新机制

增强

目前,在建立 LE 连接时,中央设备会使用休眠时钟精度 (SCA) 字段通知外围设备其时钟的精度。但精度要求可能会根据控制器处理的并发用例而变化。例如,它可能从一个值开始,但在建立另一个具有更高时钟精度要求的连接时需要提高。

蓝牙核心规范 v5.1 提供了新的链路层 PDU,LL_CLOCK_ACCURACY_REQ,可用于将新的时钟精度值通知给连接的外围设备。此 PDU 可由中央设备传输给外围设备,也可由外围设备传输给中央设备,以便外围设备可以使用它来通知连接中的中央设备其时钟精度。

在某些情况下,此功能可能会降低功耗。

扫描响应数据中的 ADI 字段

错误纠正

AdvDataInfo (ADI) 字段用于扩展广告包。以前,扫描响应包中不允许使用此字段。在最新发布的核心规范中,允许在扫描响应包中包含 ADI。

QoS 与流量规范之间的交互

信息丰富

此变化澄清了与蓝牙基本速率/增强数据速率 (BR/EDR) 相关的服务质量 (QoS) 和流相关规则。



二次广告主播频道分类

错误纠正

HCI 命令 LE_Set_Host_Channel_Classification 允许将无线电信道分类为“坏”。以前,该命令仅适用于连接,但现在也适用于次要广告信道。

允许 SID 出现在扫描响应报告中

错误纠正

广告集 ID (SID) 字段用于扩展广告包。以前,扫描响应包中不允许使用此字段。在蓝牙核心规范 v5.1 中,允许在扫描响应报告中包含 SID。

指定违反规则时的行为

信息丰富

最新核心规范版本中添加了“响应无效行为”这一新部分,以明确处理行为不当的蓝牙设备时可遵循的规则。