

# UNIVERSIDAD POLITÉCNICA DE CARTAGENA

Escuela Técnica Superior de Ingeniería de  
Telecomunicación

## Estudio de la capacidad de estimación del ángulo de llegada usando BLE 5

**TRABAJO FIN DE GRADO**

GRADO EN INGENIERÍA EN SISTEMAS DE  
TELECOMUNICACIÓN



**Autor: SÁNCHEZ DÍEZ DE REVENGA, JULIO**

Director: Gómez Tornero, José Luis

Cartagena, Enero 2024



# Preámbulo

“Encontraré la canción, u otro encontrará la canción, pero la canción será cantada de nuevo en este año o en un año que aún está por venir. Como una vez fue, así será de nuevo, en un mundo sin fin.”

- Pueblo Errante.



# Agradecimientos

Llega el momento de cerrar este capítulo de mi vida, mi paso por el grado universitario. Quiero aprovechar este momento para expresar mi gratitud a todas las personas con las que he compartido camino, porque ha sido gracias a ellas he llegado hasta donde me encuentro ahora. He aquí un intento intento, tras múltiples ediciones, de ponerle palabras a este sentimiento.

Mi familia merece la primera mención. A mis padres, por su apoyo en cada paso de este camino. Gracias por vuestros consejos y la confianza que habéis depositado en mí. A mis hermanos por su humor y su capacidad de traer ligereza a los momentos más estresantes de mi vida.

A Ana, gracias por estar a mi lado, compartiendo alegrías y desafíos. Ha sido un placer realizar toda esta etapa acompañado de ti, teniéndote como ejemplo de perseverancia y entereza. Estoy deseando descubrir lo próximo que nos depara el destino.

A mis amigos, compañeros de estudios y de aventuras, han sido una parte integral de esta experiencia. Juntos hemos compartido risas, desvelos, éxitos y desafíos. Gracias en especial a aquellos con los que he compartido aventuras extracurriculares. Juntos hemos luchado para que las máquinas sigan funcionando en [Makers of Murcia \(MOM\)](#), peleando por que las máquinas hagan nuestra voluntad en el [Free Open Source Club \(FOSC\)](#) y el [Radio Club Errante \(RCE\)](#), y compartido los momentos en los que íbamos ganando durante la [Teleco Lan Party \(TLP\)](#) y [Murcia Lan Party \(MLP\)](#). Aunque estoy seguro de que por vosotros he seguido un camino más largo para llegar a este momento, cada paso extra que hemos dado ha dejado una buena huella en mí.

Un agradecimiento especial a mi tutor José Luis Gómez Tornero, por supervisar este trabajo y a Ángel Torrecillas por su confianza y la oportunidad de explorar esta tecnología con él. Agradecido también a los buenos profesores que he tenido en etapas pasadas, ya que gracias a ellos comencé a estudiar teleco. Y a mis profesores durante la carrera, he aprendido mucho de muchos de vosotros. Gracias por desafiarme, por inspirarme y por brindarme las herramientas necesarias para crecer tanto académica como personalmente. Espero no romper lazos con todos ustedes, ya que parafraseando a un anciano hobbit: "No conozco a la mitad de ustedes la mitad de lo que desearía, y lo que deseo es menos de la mitad de los que la mitad merecéis. Ahora tengo otros asuntos que atender, los he pospuesto ya demasiado. Lamento anunciar que ha llegado el final. Os dedico mi más sentida despedida."



# Índice general

<b>1</b>	<b>Introducción</b>	<b>1</b>
1.1	Motivación	2
1.2	Objetivos y Métodos	2
<b>2</b>	<b>Sistemas de Posicionamiento</b>	<b>5</b>
2.1	Técnicas de Posicionamiento	5
2.1.1	Métodos basados en potencia	6
2.1.2	Métodos basados en tiempo	8
2.1.3	Métodos basados en fase	11
2.1.4	Métodos híbridos	12
2.2	Redes para Construir un Sistemas de Posicionamiento	13
2.2.1	Global Navigation Satellite System (GNSS)	13
2.2.2	Redes móviles	13
2.2.3	Wireless Local Area Networks (WLAN)	14
2.2.4	Ultra Wide Band (UWB)	14
2.3	Bluetooth	15
2.3.1	Bluetooth Low Energy	15
<b>3</b>	<b>Estado del arte</b>	<b>17</b>
3.1	Bluetooth	17
3.1.1	Capa física de BLE	18
3.1.2	Mecanismo de Anunciado	19
3.1.3	BLE Direction Finding	20
3.2	Agrupaciones de Antenas para Angle of Arrival (AoA)	23
<b>4</b>	<b>Objetivos e implementación</b>	<b>29</b>
4.1	Transmitir con CTE	31
4.2	Muestrear y conmutar entre antenas	32
4.3	Procesado de las muestras	33
4.3.1	Implementación del procesado de muestras	34
4.3.2	Texas Instruments (TI) Real Time Location System (RTLS) Toolbox	35
<b>5</b>	<b>Experimentos</b>	<b>37</b>
5.1	Validación Transmisión con CTE	38
5.2	Validación del sistema en cámara anecoica	43
5.3	Pruebas en entornos reales	47
5.3.1	Campaña de medidas en el Palacio de los Deportes	48
5.3.2	Campaña de medidas en el Makers of Murcia	52

<b>6 Conclusiones y vías futuras</b>	<b>55</b>
<b>Bibliografía</b>	<b>59</b>
<b>Lista de Acrónimos y Abreviaturas</b>	<b>73</b>

---

# Índice de figuras

2.1	Representación geométrica de un problema de Multilateración (MLAT) en 2D [1]	6
2.2	Problema de Triangulación 2D con incertidumbre en los ángulos [2]	7
2.3	Uso de Leaky Wave Antenna (LWA) para barrer el espacio con haces digitales. [3]	8
2.4	Visualización de las hipérbolas que cumplen cierto Time Difference of Arrival (TDoA).	9
2.5	Concepto de Two Way Ranging (TWR) [4]	10
2.6	Fundamento de la estimación de AoA midiendo la fase en dos puntos del espacio [5]	11
3.1	Pila del protocolo Bluetooth Low Energy (BLE) [6]	17
3.2	Canales de Bluetooth Low Energy (BLE) según su uso. [7]	18
3.3	Simulación del consumo de corriente de un dispositivo Bluetooth Low Energy (BLE) en sus distintos estados. [8]	20
3.4	CTE packet format from docs simplelink-cc13x2-26x2-sdk	21
3.5	Ventanas de conmutación de antenas, de 1us y 2us (TIDA029)	23
3.6	Estimación del AoA con un Uniform Linear Array (ULA) [9]	25
4.1	Arquitectura del TI CC2640R2F	30
4.2	Modificación del necesaria LAUNCHXL-CC2640R2 para conectar el BOOSTXL-AOA [10]	30
4.3	Estructura del Constant Tone Extension (CTE) en Bluetooth Low Energy 5 [11]	34
5.1	LAUNCHXL-CC2640R2 (abajo) y bladeRF (arriba) con antena log-periodica (derecha).	38
5.2	Configuración de Sigdigger para abrir la grabación que contiene los paquetes con CTE	39
5.3	Selección del canal 2 de BLE para su análisis	40
5.4	Sigdigger mostrando dos paquetes BLE capturados. El segundo con CTE.	40
5.5	Medida de la duración del CTE usando los cursores de Sigdigger	41
5.6	Medida de la frecuencia del CTE usando la selección periodica de Sigdigger	42
5.7	Montaje en la cámara anecoica	43
5.8	Sistema de medida del AoA con 3 dispositivos [10]	44
5.9	Medidas de ángulo en la cámara anecoica	45
5.10	Visualización del error en las mediciones de la cámara anecoica	46
5.11	Visualización de la varianza en las mediciones de la cámara anecoica	46
5.12	Montaje del BOOSTXL-AOA en el motor NEMA17 con la controladora GRBL.	47
5.13	Foto durante la campaña de medidas en el Palacio de los Deportes	48
5.14	Esquema de la localización de los dispositivos en el Palacio de los Deportes	49
5.15	Medidas de ángulo en el Palacio de los Deportes	50

5.16 Error en las medidas tomadas en el Palacio de los Deportes . . . . .	50
5.17 Visualización de la variancia y supervivencia de paquetes durante la MLP . . . . .	51
5.18 Foto de el hackerspace de Makers of Murcia . . . . .	52
5.19 Medidas de ángulo en Makers of Murcia . . . . .	53
5.20 Error en las medidas tomadas en Makers of Murcia . . . . .	54
5.21 Visualización de la variancia y supervivencia de paquetes en MOM . . . . .	54

---

# 1 Introducción

En el campo del **Internet of Things (IoT)**, la localización de dispositivos móviles desempeña un papel fundamental en el desarrollo de aplicaciones innovadoras que no solo potencian la eficiencia energética, sino que también promueven un enfoque más eficiente y sostenible en nuestras soluciones tecnológicas. [12] [13]. Dentro de este contexto, el estándar **BLE** se presenta como una opción ventajosa para llevar a cabo la localización de dispositivos móviles en entornos interiores, especialmente donde las tecnologías de posicionamiento por satélite como el **Global Positioning System (GPS)** no funcionan de manera óptima. En este proceso, se emplean dispositivos emisores conocidos como "beacons," que desempeñan el papel de radio balizas, emitiendo señales que permiten la identificación y posicionar de forma precisa de los dispositivos. Los beacons **BLE** son especialmente atractivos debido a su bajo costo y su eficiente consumo de energía, lo que facilita la implementación de un gran número de estos dispositivos, con intervalos de mantenimiento largos. [14]. Su simplicidad les permite ser emulados también en el dispositivo móvil del usuario, eliminando los costes en muchos casos de uso. En los sistemas de posicionamiento actuales basados en **BLE** 4.0, se emplea la potencia recibida (medida a través del **Received Signal Strength Indicator (RSSI)**) para estimar la distancia que separa al beacon del receptor. [15]. En la nueva versión del estándar **Bluetooth Low Energy (Version 5) (BLE5)** se añaden características para mejorar la precisión de los sistemas de posicionamiento, usando agrupaciones de antenas e información de fase. [16] [17]

El **Grupo de Electromagnetismo Aplicado a las Telecomunicaciones (GEAT)** de la UPCT, ha desarrollado en los últimos años sistemas de radio-localización basados antenas **Leaky Wave Antenna (LWA)**. Estas antenas pueden realizar un barrido espacial al cambiar la frecuencia de operación [13] [18]. Esta técnica se ha aplicado a una gran variedad de redes inalámbricas en bandas centimétricas [19–26] y en bandas milimétricas para RADAR [18, 27, 28]. También se

han usado las **LWA** para la localización de beacons **BLE** 4.0 [29–32].

## 1.1 Motivación

Los avances en sistemas de posicionamiento han desencadenado una profunda transformación en nuestra vida cotidiana. Los sistemas de posicionamiento por satélite, conocidos como **Global Navigation Satellite System**, se han convertido en una herramienta ampliamente utilizada para el posicionamiento y navegación en exteriores, impactando tanto a individuos como a empresas y gobiernos. Estos sistemas han revolucionado la logística y las operaciones en una amplia gama de sectores; Desde el sector primario como la agricultura y la pesca, la construcción o toda una industria de servicios de entrega rápida entre otros.

Existe la necesidad de el desarrollo de sistemas específicos de posicionamiento para interiores, fruto de las limitaciones que tienen los sistemas que cubren grandes extensiones. Estos sistemas nos permitirán desarrollar soluciones tecnológicas que, al igual que las aplicaciones de posicionamiento en exteriores, mejorarán la eficiencia, la comodidad y la seguridad en nuestra vida cotidiana, pero dentro de espacios cerrados. Por ejemplo, podríamos tener aplicaciones de navegación detallada en centros comerciales, hospitales o aeropuertos, gestionando activos de manera eficiente en almacenes o fábricas, o incluso mejorando la experiencia en eventos y conferencias a través de la ubicación precisa de dispositivos y participantes. En resumen, los sistemas de localización en interiores nos ofrecen un vasto campo de posibilidades para optimizar y enriquecer nuestra interacción con el entorno en espacios cerrados.

## 1.2 Objetivos y Métodos

En este proyecto se investigará el uso de tecnología Bluetooth para la localización en interiores. Sobre cómo podemos utilizar las funcionalidades avanzadas de localización introducidas en **Bluetooth Low Energy (Version 5) (BLE5)**; **Constant Tone Extension (CTE)**, **Angle of Arrival (AoA)** y **Angle of Departure (AoD)**, para mejorar la precisión. Se estudiarán los detalles necesarios para su implementación y se implementará usando electrónica **Commercial Off-The-Shelf (COTS)**. Se analizará el desempeño del sistema de medida en condiciones ideales, las de una

---

cámara anecoica, para compararla con entornos de despliegue reales. El diseño del sistema de localización se realizará teniendo en cuenta la posibilidad de tomar ventaja de la amplia flota de dispositivos que ya tienen BLE.

Este documento está dividido en 5 capítulos. En este primer capítulo se introduce el documento. En el segundo capítulo se introducen distintas tecnologías que permiten el diseño de un sistema de radio-localización. El tercer capítulo es una introducción al estado del arte de las tecnologías involucradas en un sistema de localización Bluetooth por AoA. El cuarto capítulo establece los objetivos que debe satisfacer el sistema de medida de AoA y los detalles para su implementación. El quinto capítulo recoge los resultados experimentales de dicha implementación. Por último, el sexto capítulo contiene las conclusiones y futuras vías de investigación del trabajo.

En el futuro se podrán concebir técnicas de localización de dispositivos Bluetooth usando tanto la Received Signal Strength (RSS), como Time of Flight (ToF) o información de fase, incorporando las técnicas avanzadas de localización de BLE con los sistemas de antenas LWA desarrollados por el grupo GEAT anteriormente mencionadas. Particularmente, se pretende que en un futuro, los sistemas de antenas inteligentes permitan estimar la posición de los dispositivos BLE en tres dimensiones de forma precisa y con una baja complejidad en el despliegue; manteniendo los dispositivos a localizar en un coste mínimo. Para ello se podrían combinar las técnicas de medida propias de BLE5 como las desarrolladas por GEAT para la reducción de la incertidumbre en el posicionamiento y los costes de despliegue.

---



## 2 Sistemas de Posicionamiento

Este capítulo se presentan las bases de un sistema de radio-localización. Para llegar al objetivo de tener un sistema de localización y navegación en interiores, primero debemos de ser capaces de acotar la posición de los dispositivos en el espacio. A este proceso lo llamaremos posicionar el dispositivo, y la primera parte de este capítulo se recogen diversas medidas que pueden ser utilizadas para este fin. Seguidamente, se recopilan distintas tecnologías de comunicación inalámbricas que pueden ser utilizadas como base de un sistema de posicionamiento. Durante este capítulo se analizan las diferentes alternativas desde el punto de vista del diseño de un sistema de posicionamiento para interiores.

### 2.1 Técnicas de Posicionamiento

Existen múltiples estrategias de radio localización. Es decir, que nos permiten localizar un objeto mediante el uso de ondas de radio. En el contexto de los sistemas de posicionamiento, distinguimos cuatro estrategias principales. Estas estrategias varían la magnitud física que medimos para acotar la posición, partiendo de un sistema de referencia. La lista que se ha compilado a continuación no es exhaustiva, conteniendo únicamente los representantes más notables. Tampoco quedan limitadas estas técnicas a ondas de radio, pueden ser aplicadas en ondas que se propagan por otros medios como las acústicas. Asumiremos por simplicidad que el emisor es el móvil a localizar, y que el sistema de localización hace de receptor (Salvo que se especifique lo contrario). Por simplicidad, asumiremos que las condiciones de localización son **Line of Sight (LOS)**. Al final, podremos entender las ventajas e inconvenientes que tendrá **AoA**.

### 2.1.1 Métodos basados en potencia

#### Received Signal Strength (RSS)

Las técnicas de RSS consisten en medir la potencia con la que se recibe la transmisión. Podremos calcular la distancia entre el emisor y el receptor aplicando un modelo de pérdidas en el canal inalámbrico [1]. La simplicidad y el bajo coste la hacen posiblemente la técnica de localización más extendida. Está presente en la amplia mayoría de sistemas de comunicaciones inalámbricas, ya que el dato de la potencia recibida (generalmente conocido como RSSI) es necesario para su correcto funcionamiento. Cada medida que realicemos nos acotará la posición a un disco entorno al receptor de posiciones que cumplen el modelo de pérdidas. Realizando la medida desde varios receptores, podemos realizar MLAT y acotar la posición del dispositivo a la intersección de los discos. El ancho de estos disco vendrá dado por la incertidumbre de nuestro modelo de propagación y de si conocemos la potencia de transmisión inicial. En un entorno interior, el que el efecto multi-camino tiene una gran influencia, multipath reina, aumentando la incertidumbre de los modelos de propagación.

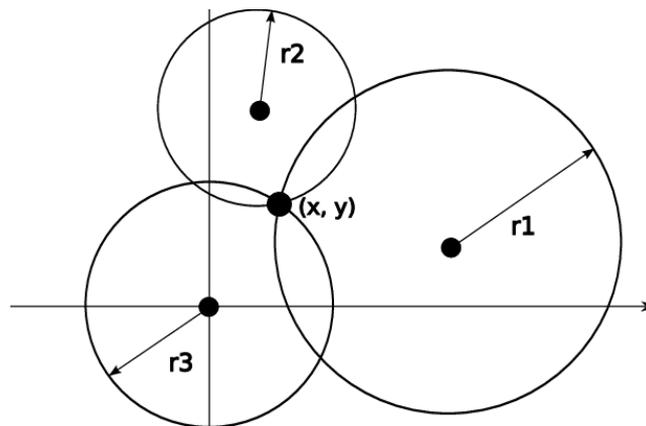


Figura 2.1: Representación geométrica de un problema de MLAT en 2D [1]

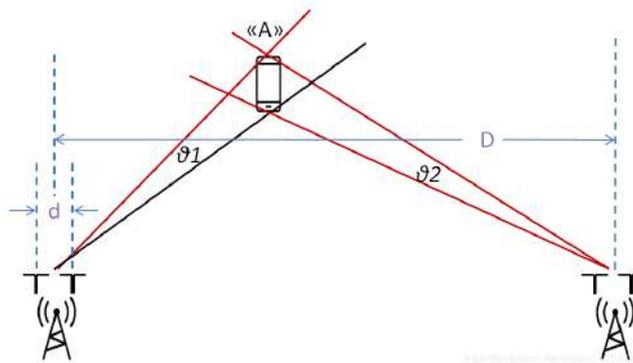
#### Puntos de Interés

El representante más simple de los sistemas de medida de potencia es el de los Puntos de Interés. En él, se establece un transmisor de baja potencia en el punto de interés. El receptor, normalmente el móvil del usuario busca este transmisor, y sabrá que se encuentra en las proximidades de un punto de interés al recibirlo. Disminuyendo la potencia de emisión (y por ende aumentando la duración de la batería) del transmisor, podemos reducir el radio de detección.

Esto se traduce en una menor área de incertidumbre, una mayor precisión a costa de tener que instalar más transmisores para cubrir el mismo área. Sin embargo, requiere que el receptor conozca la ubicación de todos los transmisores a fin de interpretar su recepción.

### Medidas de potencia dirigibles

La Radiogoniometría o "Búsqueda por Radio Dirección", del inglés **Radio Direction Finding (RDF)**, se refiere a la disciplina que permite determinar la dirección hacia la que se encuentra un emisor de radio. Para ello, existen múltiples técnicas que veremos a continuación. La más simple de ellas consiste en utilizar antenas con haces directivos. Se mide la potencia de la señal que recibimos apuntando estos haces en distintos ángulos. Barriendo el espacio, podemos encontrar el máximo de potencia recibida y estimar así la dirección hacia la que se encuentra el emisor. Esta dirección tendrá un arco de error que dependerá del paso con el que recorramos el espacio, la directividad de nuestro haz y la precisión con la que podamos medir la potencia recibida. Estas técnicas nos darán la dirección hacia la que se encuentra el emisor. Dados dos ángulos, y dos puntos a una distancia conocida, podremos construir el triángulo que también tiene como vértice el transmisor. A esta técnica se la conoce como triangulación.



**Figura 2.2:** Problema de Triangulación 2D con incertidumbre en los ángulos [2]

La implementación más simple de esta técnica sería la de físicamente apuntar una antena muy directiva en búsqueda de la señal. No es un método muy usado pese a su simplicidad. El problema principal es que requiere movimiento de partes mecánicas, cuyo tamaño debe de ser lo más grande posible para mejorar la directividad. Por otro lado, podemos hacer uso de antenas inteligentes [33] para realizar el barrido sin piezas móviles. Digital Beamformers o LWA pueden ser utilizados para barrer el espacio con nuestras antenas sin piezas móviles.

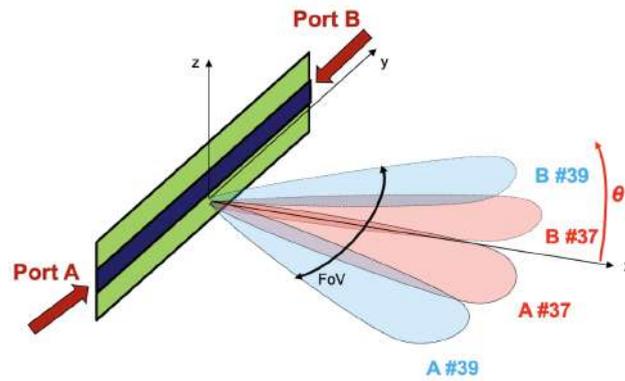


Figura 2.3: Uso de **LWA** para barrer el espacio con haces digitales. [3]

### 2.1.2 Métodos basados en tiempo

Las señales de radio, al desplazarse por el aire tienen una velocidad conocida,  $c$ , la velocidad de la luz. Conociendo el tiempo que ha pasado entre la emisión y la recepción del mensaje, podemos calcular la distancia que ha recorrido la onda. Si asumimos que la comunicación es **LOS**, obtendremos la distancia en línea recta entre emisor y receptor. Esto nos dará en tres dimensiones una esfera hueca centrada en el receptor cuyo grosor depende de la incertidumbre en la medida del tiempo, de nuevo estaremos ante un problema de **MLAT**. Aunque esta asunción no es necesaria si tenemos un modelo adecuado del comportamiento del entorno en el que ubiquemos nuestro **Indoor Positioning System (IPS)**. El reto principal de estas técnicas de medida, viene dado directamente de la velocidad de la luz. Para tener una resolución espacial de 30cm, el reloj interno debe de tener una frecuencia de 1 GHz o 10GHz para 3cm. [34]

#### **Time of Arrival (ToA)**

**Time of Arrival (ToA)** es la aproximación de primer orden, y consiste en medir el instante en el que se recibe la señal en distintos nodos. Para ello, primero se sincronizan con precisión el transmisor y los receptores. El transmisor hace envía su señal con una marca temporal, y los receptores pueden compararla con su reloj interno para estimar la distancia que ha recorrido la señal. Es la técnica mas utilizada en los sistemas basados en satélite (como los **Global Navigation Satellite System (GNSS)**), ya que con una sincronización precisa, es muy exacta. La complejidad de estos sistemas no escala bien hacia abajo. Mientras que en **GPS** damos cobertura a una gran

parte del planeta con un solo reloj atómico,<sup>1</sup> en el caso de un **IPS** necesitaríamos muchos por edificio, disparando los costes. Ya que, comparativamente, necesitaremos una mayor densidad espacial de estaciones receptoras en un **IPS**.

### Time Difference of Arrival (TDoA)

**TDoA** elimina el requisito de sincronización entre emisor y receptor. Los receptores se sincronizan entre sí y al reciben una transmisión con marca temporal. Calculando la diferencia del **ToA** de dos receptores, obtendremos la diferencia temporal de ambos caminos, eliminando así el desfase que pudiera existir con el emisor. Esa diferencia de tiempo, el **TDoA** nos permite calcular la distancia extra que ha viajado la señal al nodo más lejano.

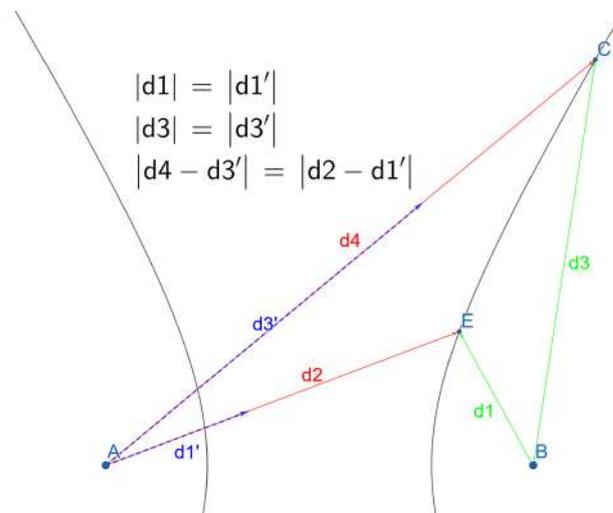


Figura 2.4: Visualización de las hipérbolas que cumplen cierto **TDoA**.

La posición del emisor estará limitada por tanto, a los puntos cuya distancia a ambos receptores tenga una diferencia igual al **TDoA**. Estos puntos estarán contenidos en un espacio geométrico, que en dos dimensiones, será una hipérbola (con los receptores en sus focos)<sup>2</sup>. Como los receptores están sincronizados, sabremos cual recibe la señal primero, y podremos reducir al semi-espacio que cumpla esta condición.

De nuevo, podremos acotar más la posición del emisor al realizar la intersección de espacios

<sup>1</sup>Los satélites de GPS orbitan a 20Mm de altitud, por lo que podrían dar una cobertura LOS a hasta el 38% de la superficie terrestre. [35]. Muchos órdenes de magnitud más que en cualquier sistema de localización en interiores. Este margen es muy pequeño para la demostración.

<sup>2</sup>El boceto de geogebra de la Figura 2.4 puede encontrarse en: <https://www.geogebra.org/calculator/za2dsmxa>

posibles, medidos desde múltiples parejas de receptores. El área de incertidumbre dependerá en este caso de la sincronización entre receptores y la resolución temporal que tengamos.

### Two Way Ranging (TWR)

Time of Flight (ToF) en el contexto de BLE, y Two Way Ranging (TWR) en el de Ultra Wide Band (UWB); se refieren a la misma técnica. El "transmisor" comienza a medir tiempo al enviar su señal. El "receptor" la recibe y contesta. Al ser recibida por el "transmisor", obtendrá el tiempo de ida y vuelta (two way). El error sistemático debido al tiempo de procesamiento puede eliminarse mediante calibración. Tanto el que transcurre entre la primera recepción y la respuesta, como tras la segunda recepción. Se elimina así por completo la necesidad de sincronización entre receptores y transmisor. En su lugar, se producen dos cambios significativos con respecto a las técnicas anteriores: Todas las partes (localizado y localizador) necesitan la capacidad de ser (al menos) half-duplex; y los "transmisores" deben de ser conocedores de las calibraciones de los "receptores". El valor de las calibraciones puede o bien propagarse aprovechando que todas las partes pueden emitir, o bien fijarse de antemano. El tiempo de ida y vuelta acota la posición del dispositivo a una esfera de radio conocido. [34] [4]

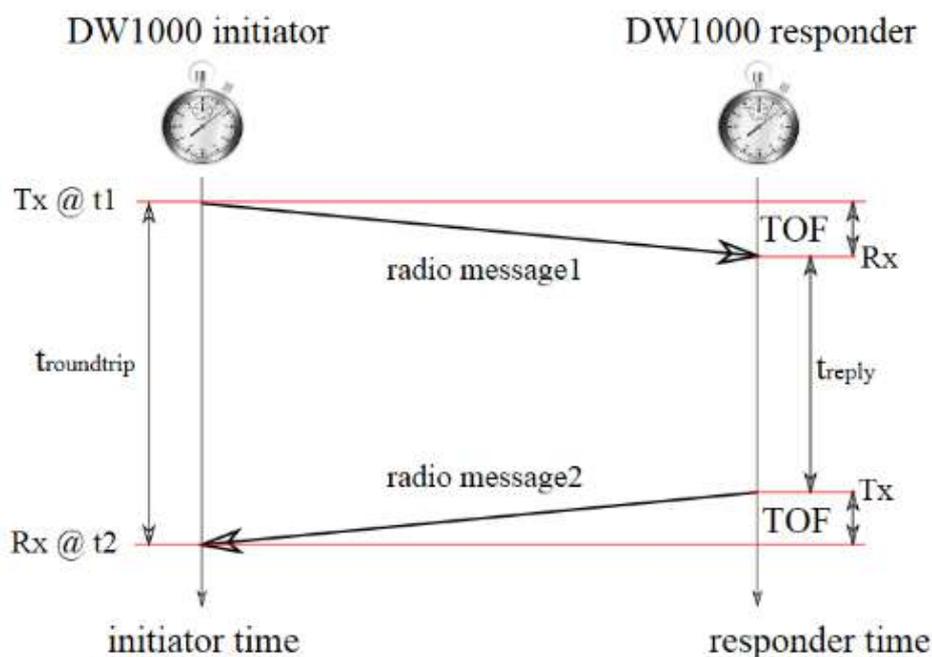


Figura 2.5: Concepto de Two Way Ranging (TWR) [4]

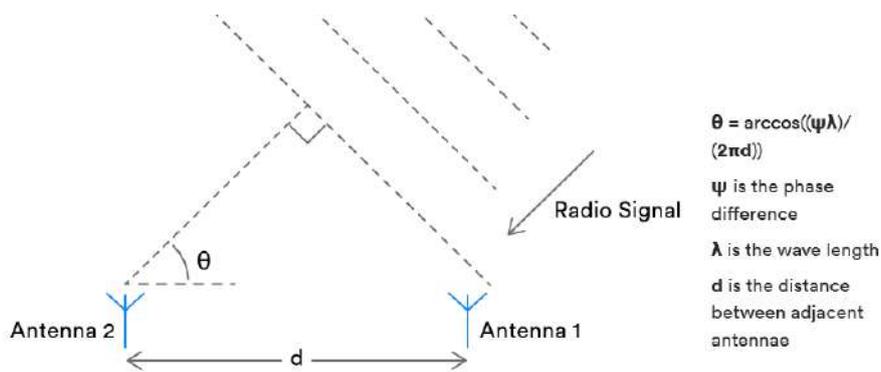


Figura 2.6: Fundamento de la estimación de **AoA** midiendo la fase en dos puntos del espacio [5]

### 2.1.3 Métodos basados en fase

Las señales de radio tienen una naturaleza ondulatoria al propagarse por el espacio. Un frente de onda es el lugar geométrico en el que todos los puntos tienen la misma fase. Estudiando como se desplaza espacialmente un frente de onda, podemos obtener en qué dirección y sentido se propaga. En otras ocasiones, podremos usar el dato de fase para reducir la incertidumbre de una medida de distancia, como es el caso de las medidas que utilizan interferometría. Una simplificación que puede ser muy útil en estos sistemas es la de asumir que el frente de ondas es una línea recta a pequeña escala, en lugar de arcos, debido a la distancia entre emisor y receptor en comparación al sistema receptor. Para estudiar la evolución del frente de ondas, se necesita recibir la señal desde distintos puntos del espacio.

#### Medidas de variación espacial de fase

Como veremos más adelante, **BLE** propone una primera aproximación a la medida del **Angle of Arrival (AoA)**. Midiendo la fase con la que recibimos una señal conocida en distintos puntos del espacio, podemos estimar la dirección de propagación del frente de onda. En distintos puntos del espacio recibiremos la señal con una fase diferente, y esta diferencia depende del ángulo que forme el frente de ondas con el segmento que une los puntos desde los que medimos. En el contexto de este trabajo, **AoA** se refiere a la medida del ángulo de llegada de una señal utilizando una sola radio y un conmutador para recorrer una agrupación de antenas. Analizaremos los puntos a favor y en contra de este tipo de sistemas en los siguientes capítulos.

## Medidas de coherentes

El campo del **RDF** está bien nutrido de distintas técnicas de procesado de señales haciendo uso de agrupaciones de antenas. [9] Típicamente, la señal es obtenida en cada antena de forma coherente. De esta manera, pueden procesarse de forma exhaustiva rechazando interferencias y minimizando el efecto multipath. Es un campo ampliamente explorado en los últimos años, en los que se han desarrollado diferentes aproximaciones al problema. Los máximos exponentes de estas aproximaciones son **Multiple Signal Classifier (MUSIC)** y **Estimation of Signal Parameters via Rotational Invariance Technique (ESPRIT)**. El increíble desempeño de estos sistemas viene acompañado de una gran complejidad computacional y un equipamiento de alto coste para el muestreo de las señales. Es por eso que no son un buen candidato para un **IPS**. Sin embargo, suelen verse con frecuencia en el mundo militar.

### 2.1.4 Métodos híbridos

Los métodos híbridos de posicionamiento se refieren a la combinación (a veces referida como fusión) de múltiples técnicas de posicionamiento para obtener resultados más precisos y confiables. Aprovechan las fortalezas de diferentes métodos para cubrir entre sí sus limitaciones. Además de combinar las distintas estrategias de localización con radio, puede combinarse el uso de acelerómetros, giroscopios, brújulas magnéticas, cámaras... El procesamiento de las medidas que acotan la posición del emisor queda fuera del alcance de este trabajo.

En este trabajo nos centraremos en técnicas que permitan delimitar la ubicación a través del ángulo desde el que se recibe la transmisión. En otras palabras, veremos cómo usar el **AoA** de comunicaciones **BLE** para localización precisa en interiores.

---

## 2.2 Redes para Construir un Sistemas de Posicionamiento

Las redes inalámbricas nos rodean en nuestro día a día, incluso cuando estamos en el interior de edificios. Por eso, resulta interesante utilizarlas como base de un **IPS**. Las redes inalámbricas pueden clasificarse en 4 grupos, en función de su área de cobertura. **Wireless Personal Area Networks (WPAN)**, **Wireless Local Area Networks (WLAN)**, **Wireless Metropolitan Area Networks (WMAN)** y **Wireless Wide Area Networks (WWAN)**. Esta división es interesante a la hora de caracterizarlas para su uso en sistemas de localización. Como **WWAN** tenemos redes como las de telefonía móvil o **GNSS**. Como **WMAN** encontramos otras como LoRa. Representando a las **WLAN** están WiFi y ZigBee. **WPAN** encontramos RFID, **BLE** o UWB. Salvo las redes GNSS, UWB, o RFID, las tecnologías no tienen como propósito principal la localización y por lo general tendrán un desempeño peor en situaciones comparables. A cambio, los costes de despliegue del sistema de localización serán compartidos con la red de comunicación correspondiente. En muchos casos, se podrá aprovechar que el usuario ya tiene hardware compatible y no supondrá un coste extra.

### 2.2.1 Global Navigation Satellite System (GNSS)

**GNSS**, en español, Sistema global de navegación por satélite es el nombre por el que se conocen el conjunto de sistemas de navegación a escala global. Debido a su impacto, se consideran infraestructura crítica y de importancia estratégica para las organizaciones que los operan. Esto ha llevado al despliegue del sistema americano, **Global Positioning System (GPS)**; ruso, **Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS)**, europeo Galileo, el chino **BeiDou Navigation Satellite System (BDS)**, Indio **Indian Regional Navigation Satellite System (IRNSS)** o japonés **Quasi-Zenith Satellite System (QZSS)**. Pese a ser el tipo de sistemas de posicionamiento más extendido, su desempeño en interiores se aleja del ideal por la dificultad de establecer un enlace de comunicación con los satélites. [36]

### 2.2.2 Redes móviles

Las redes celulares, en todas sus generaciones, han permitido la localización de clientes como funcionalidad extra. El área de incertidumbre que podemos esperar es de una fracción del

---

área de cobertura de un sector, que por lo general es demasiado grande para la navegación en interiores. Esto es debido a que tradicionalmente se utilizan técnicas de multilateración entre celdas y/o sectores. Con la aparición de 5G mmWave, el Massive **Multiple-Input and Multiple-Output (MIMO)**, medidas de canal mejoradas y las redes segmentadas en funciones (Lo que permitiría exponer estos datos provenientes de la red a terceros), podrían revolucionar los servicios de localización. Esta prometedora tecnología futura queda fuera del alcance de este estudio.

### 2.2.3 **Wireless Local Area Networks (WLAN)**

Redes **WLAN** como **IEEE 802.11 (Wi-Fi)** o Zigbee, por la densidad de redes que encontramos en entornos urbanos, permiten localizar con una precisión de algunos metros. Se utilizan habitualmente por aplicaciones como Google Maps para asistir la localización que se obtiene mediante **GNSS**. Existen repositorios como Wigle<sup>[37]</sup>, que podemos usar para ubicar un receptor en función de que redes (y con qué potencia) puede ver. Para mejorar la precisión del posicionamiento de los **Wi-Fi positioning system (WFPS)**, y competir en el mercado de los sistemas de localización, **Wi-Fi** introdujo **WiFi Fine Timing Measurement (WiFi-FTM)**. De momento, mantiene una incertidumbre de metros. También requiere cambios significativos en los módems de los dispositivos para soportar las medidas de tiempo de vuelo. Por lo que no es adecuada para este trabajo. <sup>[38]</sup>

### 2.2.4 **Ultra Wide Band (UWB)**

**UWB** es una tecnología de radio basada en IEEE 802.15.4a y 802.15.4z. Está diseñada desde el principio para ser la base de un sistema de posicionamiento. Consigue por tanto el menor consumo en operación y tiene una precisión del orden de centímetros. Usa **TDoA** y **TWR**, incluso puede llegar a hacer uso de la fase para aumentar la precisión (**Phase Difference of Arrival (PDoA)**). Las desventajas son, que requiere de hardware específico para el sistemas de localización y que requiere diseño de RF de banda ancha (más de 500MHz, localizados por lo general de 3 a 10GHz).

## 2.3 Bluetooth

Bluetooth (BT) es una tecnología inalámbrica de corto alcance, creado por el Bluetooth (BT) Special Interest Group (SIG). Diseñado para WPAN con la premisa de ser robusta, de bajo consumo y bajo coste. La penetración de mercado de BT es enorme, con más de 5.4 mil millones de nuevos dispositivos solo en 2023 [39]

Actualmente, el estándar se divide en dos formas de Bluetooth, el Bluetooth Basic Rate (BR) y el BLE. Nos centraremos en el segundo, siendo el más indicado como veremos para IPS. El sistema Bluetooth Low Energy Controller (LE) incluye las características diseñadas para reducir el consumo que le dan nombre, pero también introduce reducciones a la complejidad y el coste de implementación en comparación a BR. Está diseñado para aplicaciones que requieran un menor caudal de datos y se beneficien de ciclos de trabajo reducidos. El estándar contiene muchas capacidades opcionales, lo que permite cubrir las necesidades especializadas de algunos productos. Aprovecharemos algunas de ellas en este trabajo, tales como CTE, AoA y las extensiones de anuncio.

### 2.3.1 Bluetooth Low Energy

BLE es parte del estándar BT, un protocolo diseñado para WPAN, creado por el Bluetooth (BT) SIG. BLE fue incorporado en la especificación de BT 4.0 en 2010 con un coste inferior, además de la sustancial reducción en consumo que le da nombre.

BLE está diseñado para dispositivos IoT. Utiliza un modelo de datos cliente/servidor asíncrono, que permite a los dispositivos pasar largos periodos en modo de espera. Esto lo hace un sistema de comunicaciones inalámbricas ideal para dispositivos que requieran de larga duración de batería, ya que una pila de botón dura años en los dispositivos más simples.

En Diciembre de 2016 se publica la versión 5.0 del estándar Bluetooth (BT). La última actualización hasta la fecha de redacción de este trabajo es Bluetooth (BT) "Core Specification Version 5.4" del 31 de Enero de 2023. [16] BLE5 introduce mejoras significativas en las capacidades del protocolo, tales como aumento de la tasa de bit, comunicaciones de mayor alcance, un algoritmo de acceso a medio mejorado y mucho más. En BLE 5.1 [40] se introduce la posi-

bilidad de utilizar técnicas de posicionamiento avanzadas, facilitando la medida de el **AoA** o el **Angle of Departure (AoD)** como veremos más a delante. Este **Trabajo Final de Grado (TFG)** se desarrolla en el periodo de transición de **BLE** 5.1 a 5.4. Los dispositivos que hacen uso de las nuevas características de localización de **BLE5** no han llegado a las masas.

---

# 3 Estado del arte

## 3.1 Bluetooth

La arquitectura de los sistemas Bluetooth se descompone en 3 capas. Controlador, Host y Aplicación. En este trabajo nos centraremos en el Controlador, puesto que es el encargado directo de la interfaz de radio. Como es habitual en los modelos por capas, las aplicaciones se comunican a través de una pila de protocolos con las distintas capas. De las labores de interconexión se encarga el Host y la Aplicación de las funcionalidades de cara al usuario final.

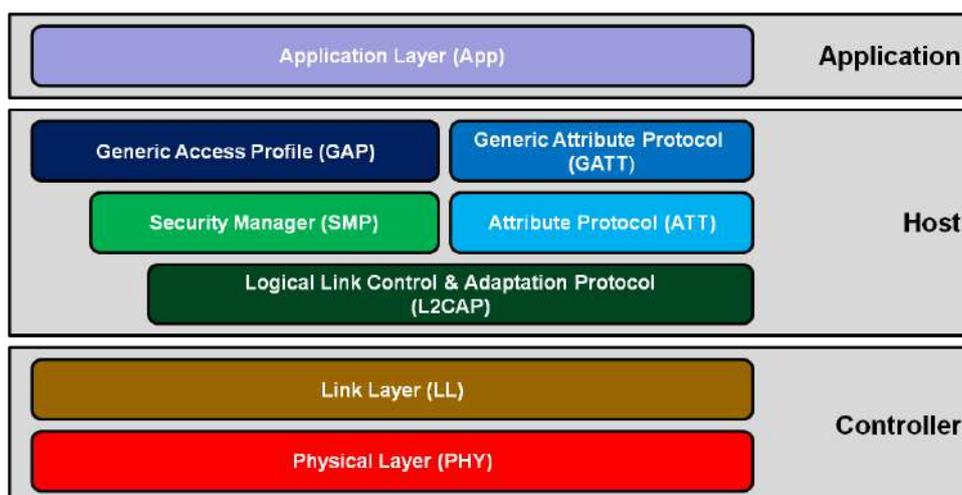
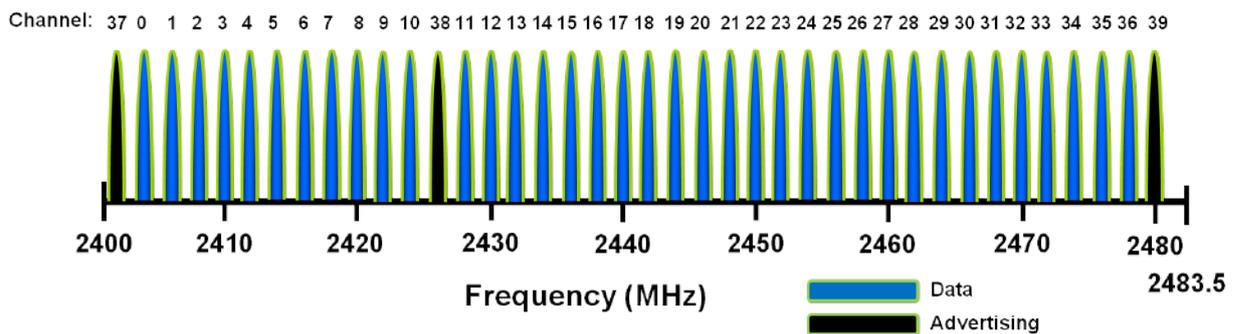


Figura 3.1: Pila del protocolo Bluetooth Low Energy (BLE) [6]

### 3.1.1 Capa física de BLE

Los sistemas Bluetooth Low Energy funcionan en la banda **Industrial, Scientific, and Medical (ISM)** de 2.4GHz, de 2.4 a 2.485GHz y la potencia de transmisión suele estar entre -20 y 10dBm. **BLE** divide este espacio en 40 canales con una separación de 2MHz. El sistema de descubrimiento de dispositivos **BLE** usa transmisión de paquetes de anuncio. Los anuncios se envían en canales dedicados, el 37, 38 y 39. El resto de canales se utilizan para la transmisión de datos durante las conexiones.



**Figura 3.2:** Canales de **Bluetooth Low Energy (BLE)** según su uso. [7]

BLE5 pone a disposición de los diseñadores cuatro **BLE Physical Layer (BLE)** entre los que elegir. Todos tienen en común la modulación, **Gaussian Frequency Shift Keying (GFSK)**. El **PHY LE 1M** viene de BLE4, transmite información a 1M baudio. Las tres nuevas opciones de capa física introducidas en BLE5, nos permite ajustar el desempeño a la aplicación. Los **PHY Coded** con **Error Correcting Code (ECC)** son S2 y S8, añadidos sobre el **PHY LE 1M**, disminuyendo la tasa de datos neta pero incrementando el rango. El **PHY LE 2M** de 2Mbps 1 bit por símbolo, modulando a 2M baudios. A cambio de la mayor tasa de transmisión, influirá negativamente en el rango y en el consumo de energía.

PHY	Tasa binaria	Distancia	Ventaja
LE 2M	2 Mb/s	×0.8	Velocidad
LE 1M	1 Mb/s	x1	Compatibilidad
LE Coded S2	500 kb/s	x2	Balanceado
LE Coded S8	125 kb/s	x4	Rango

**Tabla 3.1:** Tabla comparativa de PHY

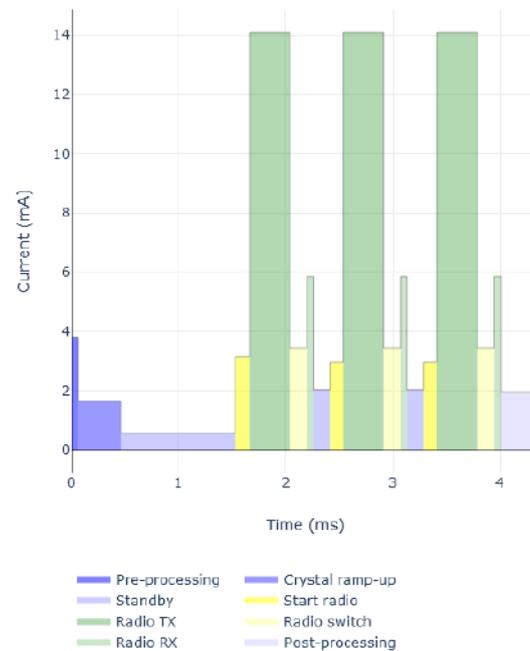
Cabe aclarar, que la tasa binaria de la tabla anterior se refiere a la máxima capacidad de

transmisión de la modulación, no a la transferencia de datos de aplicación. La transferencia de datos de aplicación dependerá también, entre otras cosas, de la relación entre la longitud de los paquetes y el tiempo entre saltos de canal. [41]

### 3.1.2 Mecanismo de Anunciado

El mecanismo de descubrimiento y emparejado de BLE está basado en la transmisión de anuncios. Tradicionalmente, en BT existen tres canales de anuncio: el 37, 38 y 39. El dispositivo anunciante se anunciará en al menos uno de los tres canales dedicados que podemos ver en la Figura 3.2. En el paquete de anuncio se detallan las capacidades del dispositivo, entre ellas, si es conectable. En caso de aceptar conexiones, cualquier dispositivo receptor podría iniciar el proceso. BLE v4.0 introduce la posibilidad de añadir hasta 37 bytes de información a estos paquetes. Esto permite mantener los ciclos de trabajo cortos, y maximizar el tiempo durante el que los dispositivos permanecen durmientes. Este mecanismo permite la transmisión de información de forma unidireccional, sin establecer sesiones, lo que mantiene al mínimo los tiempos de actividad. Un dispositivo que quiera maximizar la duración de su batería podrá permanecer a la espera hasta que tenga que transmitir. En la Figura 3.3, se puede observar que la transmisión es la acción que mas energía consume en estos dispositivos, mientras que el consumo durante el tiempo de espera es muchísimo inferior. A cambio, la contraparte deberá permanecer escaneado de manera continua los canales de anunciado. Como veremos más a delante, los diseñadores de sistemas de localización tienen la opción de desplazar el consumo al extremo en el que nos podamos permitir una batería más grande o incluso una conexión fija de alimentación.

---



**Figura 3.3:** Simulación del consumo de corriente de un dispositivo BLE en sus distintos estados. [8]

Bluetooth 5 amplía las posibilidades de los anuncios, introduciendo "Anuncios extendidos". Estas extensiones rompen la retro compatibilidad con BLE 4, a cambio, introducen nuevas capacidades. Cabe destacar que la información que se puede transmitir en un paquete se ve extendida de 37 a 255 bytes, se introduce la posibilidad de encadenar paquetes de anuncio entre sí para transmitir hasta 1650 bytes. Se introduce soporte oficial a la periodicidad conocida en los anuncios, permitiendo reducir el consumo del escáner una vez se sincroniza con un emisor (sin establecer una conexión). Además, con el fin de aumentar la resiliencia a interferencias, se puede señalar que la cadena de anuncios sigue en un canal de datos.

### 3.1.3 BLE Direction Finding

La versión 5 del estándar Bluetooth Low Energy (BLE) introdujo las funciones de AoA y AoD como características opcionales. Estas innovaciones fueron concebidas con el propósito de mejorar la resolución de los sistemas de localización basados en Bluetooth permitiendo realizar nuevas medidas. AoA permite determinar la dirección desde la que llega una señal Bluetooth, mientras que la AoD proporciona información sobre la dirección desde la que se emitió la señal. Ambas funciones requieren conmutar entre múltiples antenas (Switched Antenna Array

(SAA) durante la comunicación. Uno de los puntos más fuertes de BLE es su bajo coste y con la intención de mantenerlo, se buscó poder realizar las nuevas medidas sin introducir grandes gastos a la hora de implementarlo. Esto se ha traducido en poder realizar las medidas con un solo PHY e imponiendo unos requisitos a los conmutadores de las antenas modesto. Debido a estas limitaciones, surge la necesidad de la CTE. Además, necesitaremos que el receptor pueda muestrear y procesar la señal que recibe antes de pasar por el demodulador.

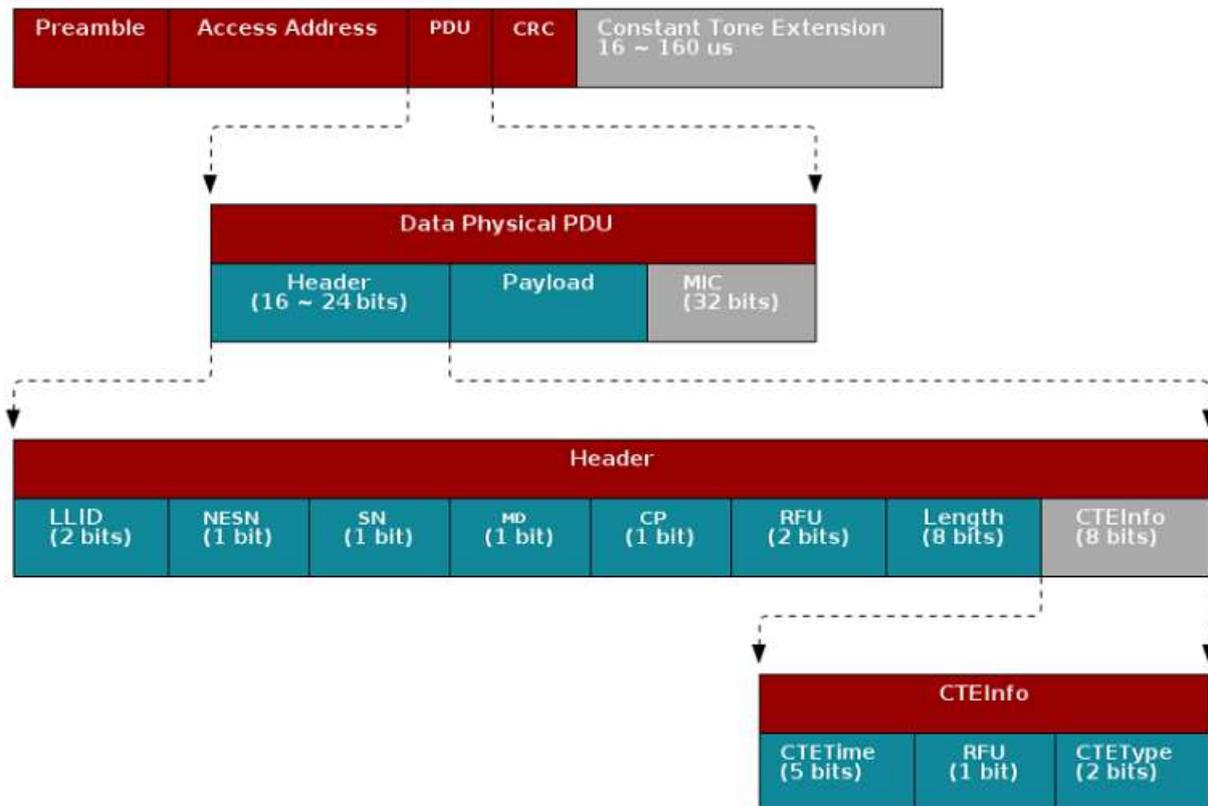


Figura 3.4: CTE packet format from docs simplelink-cc13x2-26x2-sdk

### Constant Tone Extension

El CTE (Constant Tone Extension) consiste en añadir un tono al final del paquete, detrás del Cyclic Redundancy Check (CRC)<sup>1</sup>, que lo dota de la capacidad de localización. Esto se consigue transmitiendo el mismo símbolo (se toma el 1) durante un tiempo de 16 a 160us, equivale a de 16 a 160 símbolos a 1 Mbaudio (de 2 a 20 octetos). Al usar GFSK como modulación, resultará

<sup>1</sup>Cabe destacar que el CTE no está protegido por ningún mecanismo de BLE. Ni el Chequeo Redundante Ciclico (CRC), ni la Comprobación de Integridad del Mensaje (MIC) en caso de estar emparejado. Por lo que no podremos detectar interferencias (CRC) ni autenticar la procedencia (MIC) del CTE.

en el tono constante que se buscaba, que quedará desplazado +250KHz de la frecuencia central del canal.

En dispositivos reales, es importante desactivar el mecanismo de Whitening de BLE para que el tono sea constante. El mecanismo de whitening impide que se transmitan secuencias largas de símbolos iguales, ya que esto podría introducir efectos no deseados sobre la distribución espectral de potencia y es un mecanismo común en muchos sistemas de comunicación inalámbrica, aunque los detalles de su implementación varían. En el caso de BLE se implementa pasando el paquete tras el cálculo del CRC por un Linear Feedback Shift Register (LFSR) con un polinomio generador  $y = x^7 + x^4 + 1$  [40].

### Direction finding

Según como se distribuyan las capacidades de CTE y Antenna Switching entre emisor y receptor, podremos medir AoD o AoA .

**AoD** En el caso de AoD , toda la complejidad queda concentrada en el transmisor. Su labor será realizar transmisiones con CTE, mientras realiza cambios de antena. El receptor podrá medir las discontinuidades en la fase para estimar el ángulo desde el que se transmitió.

**AoA** En AoA , las nuevas funcionalidades están repartidas. Por un lado, los transmisores envían paquetes con CTE y los receptores estiman el ángulo de llegada comparando la fase en distintas antenas.

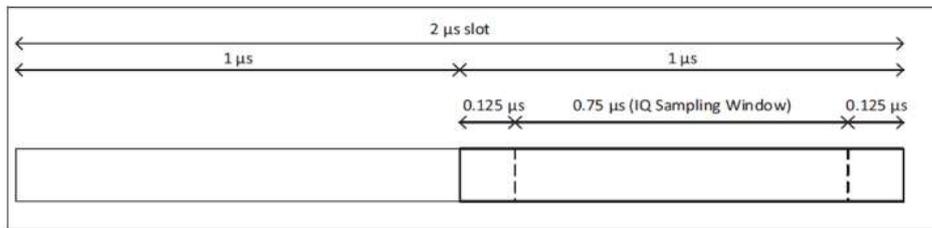
	Conmutación de antenas	Extensión de Tono Constante
AoA	Rx	Tx
AoD	Tx	Tx

**Tabla 3.2:** Tabla distribución de responsabilidades

Si cambiásemos los papeles de emisor y receptor, tendríamos funcionalmente el mismo esquema, aunque la información se generaría en el extremo opuesto.

## Antenna Switching

Como veremos en la sección sobre RDF, al cambiar de antena cambia también el camino que ha recorrido la señal recibida. Esto se traduce en un desfase en la señal que podemos medir. BLE opta por realizar las medidas en múltiples antenas con un solo receptor, lo que reduce el coste y la complejidad (al no necesitar coherencia entre múltiples receptores). Bluetooth 5 establece ranuras de 1 o 2  $\mu\text{s}$  de duración por antena y durante ese tiempo debemos de ser capaces de: Conmutar la antena, alcanzar un estado de equilibrio y realizar el muestreo de la señal. La ranura de 1  $\mu\text{s}$  establece una ventana de muestreo de 0.75  $\mu\text{s}$ , dando 0.25  $\mu\text{s}$  a los conmutadores para actuar y estabilizarse. La ranura de 2  $\mu\text{s}$  tiene la misma ventana de muestreo, pero da 1.25  $\mu\text{s}$  a los conmutadores. Podemos ver la distribución temporal de ambas ranuras en la siguiente figura:



**Figura 3.5:** Ventanas de conmutación de antenas, de 1  $\mu\text{s}$  y 2  $\mu\text{s}$  (TIDA029)

Por último, mencionar la importancia del aislamiento entre los distintos canales (antenas). Esta debe tenerse en cuenta a lo largo de todo el diseño del dispositivo. A la hora de elegir el conmutador de antenas, de enrutar las líneas de transmisión y de crear la agrupación de antenas. El diseño de este último se discute en [11]

## 3.2 Agrupaciones de Antenas para AoA

En esta sección se cubren las bases teóricas de la técnica utilizada para obtener la Direction of arrival (DoA) utilizando un SAA. Como se ha introducido anteriormente, estas técnicas utilizan la diferencia de fase recibida en una agrupación de antenas para obtener el ángulo de la comunicación. Una agrupación o *array* de antenas es un sistema radiante constituido de elementos radiantes (antenas) individuales. Por lo general estos elementos se usan simultáneamente, introduciendo desfases entre las antenas para controlar la dirección y forma de su patrón

de radiación conjunto. Los arrays de antenas aportan así una gran flexibilidad, lo que los ha llevado a formar parte de múltiples sistemas de radiocomunicaciones.

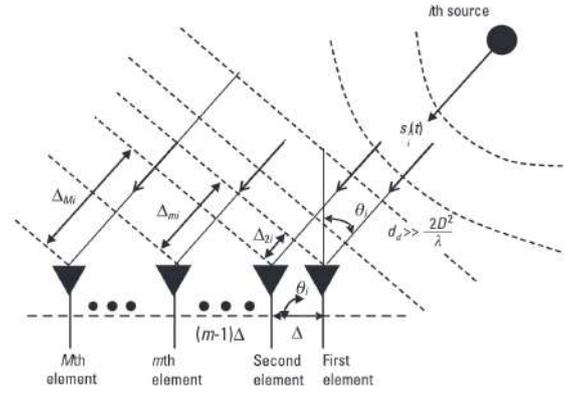
En este caso, nos centraremos en el uso de los arrays en receptores y empezaremos considerando que podemos recuperar la señal recibida por cada elemento individualmente. La disposición espacial de los elementos es determinante a la hora de establecer el marco de referencia sobre el que operaremos. Hay una multitud de posibilidades, nos quedaremos con un ULA [42]. Consideremos un ULA compuesto de  $M$  elementos idénticos y equiespaciados una distancia  $\Delta$  a lo largo de un segmento. Además, tendremos estas asunciones [9]:

1. Los elementos del array son antenas isotrópicas
2. Los elementos del array están equiespaciados, a una distancia  $\Delta < \lambda$
3. El medio de propagación es isotrópico y lineal.
4. El ruido es Additive White Gaussian Noise (AWGN) y está uncorrelado espacialmente. No hay fuentes de interferencia.
5. El array está estacionario y la fuente permanece estacionaria durante el tiempo de medida.
6. La distancia entre la fuente y el array será tal que podemos considerar los frentes de ondas como planos paralelos al incidir en el array.
7. La fuente es de banda estrecha, y solo se recibe una señal proveniente de ella.
8. La señal está uncorrelada con el ruido.

De la geometría que hemos establecido, que podemos ver en la Figura 3.6, obtenemos que el retardo de una antena a otra será:

$$\tau = \frac{d}{c} = \frac{\Delta \sin \phi}{c} \quad (3.1)$$

Asumiendo que  $\Delta$  es menor que una longitud de onda ( $\lambda$ ), este retardo entre las antenas se



**Figura 3.6:** Estimación del AOA con un ULA [9]

corresponde con un desfase ( $\delta$ ) en la señal menor a  $2\pi$ , tal que:

$$\delta = 2\pi \frac{\tau c}{\lambda} = 2\pi \frac{d}{\lambda} = 2\pi \frac{\Delta \sin \phi}{\lambda} \quad (3.2)$$

Podemos construir el vector de apuntado de la agrupación (Array Steering Vector). Este vector representa el desfase de la señal en los distintos elementos de la agrupación. Nótese que la distancia entre una antena número  $N$  y la primera (número 0) será  $(N-1)$  veces  $\Delta$ .

$$\mathbf{a}(\phi) = \left[ 1 \quad e^{-j\frac{2\pi\Delta}{\lambda} \sin \phi} \quad e^{-j\frac{4\pi\Delta}{\lambda} \sin \phi} \quad \dots \quad e^{-j2\pi\frac{(N-1)\Delta}{\lambda} \sin \phi} \right] \quad (3.3)$$

Por lo que la señal ideal  $y(t)$  recibida por la ULA en cada instante  $t$  vendrá dada por  $\mathbf{y}(t) = \mathbf{a}(\phi)s(t)$ . Donde  $s(t)$  representa la señal recibida en el primer elemento de la agrupación. Teniendo en cuenta el ruido (asunción 8), la señal recibida será  $\mathbf{y}'$ ,  $\mathbf{y}'(t) = \mathbf{y}(t) + \mathbf{n}(t)$ . Que al estar uncorrelado espacialmente  $\mathbf{n}(t)$ , el ruido en cada elemento tendrá forma:

$$\mathbf{n}(t) = \left[ n_0(t) \quad n_1(t) \quad n_2(t) \quad \dots \quad n_{N-1}(t) \right] \quad (3.4)$$

$$\mathbf{y}'(t) = \left[ s(t) + n_0(t) \quad s(t)a_1(\phi) + n_1(t) \quad \dots \quad s(t)a_{N-1}(\phi) + n_{N-1}(t) \right] \quad (3.5)$$

Podemos ir eliminando asunciones mediante un modelado más detallado. Por ejemplo, al sustituir los elementos por antenas no isotrópicas (asunción 1), tendremos una componente de ganancia que varía en función del ángulo. Si la asunción 2 no se cumple, y los elementos tienen distancias no homogéneas, deberemos de ajustar los desfases en nuestro vector  $\mathbf{a}(\phi)$ . Si existen

múltiples fuentes de señal que interfieren, podemos aplicar técnicas de **Successive Interference Cancellation (SIC)** para localizarlas una a una, etc.

En un sistema de **RDF**, nuestro objetivo será encontrar el valor de  $\phi$  que minimiza el error en la estimación. Para esto, existen múltiples técnicas de procesado. Los máximos representantes son las técnicas de barrido de haz y las de sub-espacios (como ESPRIT y MUSIC). Por lo general, estas técnicas requieren la recepción simultánea en todos los elementos de la agrupación. Además, requieren un preprocesado que puede llegar a ser muy costoso en entornos multi-camino. Este preprocesado es necesario para compensar el aumento en la correlación entre señales introducido por las replicas. [9, p. 34] Como hemos visto, con el fin de mantener el coste controlado solo tendremos un receptor y una capacidad de computo limitada.

$$\min_{0 < \phi < \pi} \left( \sum_{n=0}^N y_n(t) - y'_n(t) \right) \quad (3.6)$$

Al hacer AoA, en el estándar BLE solo se utiliza un receptor, que conmuta entre las diferentes antenas, en el conocido como **Switched Antenna Array (SAA)**, tomando muestras de la señal en cada una. Recordemos que podemos calcular el desfase de dos muestras  $IQ$  de esta manera:

$$\begin{aligned} IQ_0 &= a_0 + jb_0 & \& \quad & IQ_1 &= a_1 + jb_1 \\ z &= IQ_0 \cdot IQ_1^* = a_0a_1 + b_0b_1 + j(a_2b_1 - a_1b_2) \\ \theta &= \arctan \left( \frac{Im(z)}{Re(z)} \right) \end{aligned} \quad (3.7)$$

En nuestro sistema receptor, conoceremos la distancia entre los puntos en los que muestreamos la señal, la ubicación de las antenas y la longitud de onda de la señal a recibir. Dado que la señal recorre caminos diferentes para alcanzar cada antena, se introduce el desfase ( $\delta$ ). El desfase introducido por la diferencia de caminos puede calcularse como hemos visto en la ecuación 3.2. Despejando, obtenemos que el ángulo de llegada (con respecto a la perpendicular del **ULA**) podría calcularse como<sup>2</sup>:

$$\phi(AoA) = \arcsin \frac{\delta \lambda}{2\pi \Delta} \quad (3.8)$$

<sup>2</sup>En este caso tomamos el ángulo según la Figura 3.6. En la Figura 2.6, el ángulo se mide con respecto al segmento que contiene el **ULA**, por lo que utiliza el coseno.

---

Queda aclarar que el estándar BLE se enfrenta a un reto extra al muestrear las distintas antenas mediante conmutación. Esto implica que va a ser imposible el muestreo de dos antenas durante el mismo instante de tiempo, por lo que se introduce un desfase temporal. Sin embargo, esto se contrarresta gracias al CTE. Al ser un tono constante, no existirá desfase temporal si el tiempo entre muestras es igual a un periodo. En el siguiente capítulo se recogen los detalles de implementación de un sistema de medida de AOA.

---



## 4 Objetivos e implementación

En los capítulos anteriores hemos hecho un repaso de distintas técnicas de radio localización y cómo se han introducido en **BT**. Las ventajas de implementar un **IPS** utilizando las funcionalidades avanzadas de localización de **BLE5** lo hacen un candidato muy interesante, permitiendo reducir el número de estaciones de medida (o Anchors) mientras aumenta la precisión del sistema. Todo esto, sin imponer requisitos en los dispositivos a localizar que supongan un gran coste.

En este capítulo cubriremos el diseño de un sistema de medida de **AoA** utilizando dispositivos embebidos **BLE**. En el siguiente capítulo, evaluaremos el desempeño de este sistema de medida. Como vimos con anterioridad, para poder implementar este sistema tenemos requisitos especiales; Necesitamos que el dispositivo a localizar transmita paquetes con el **CTE** y que el dispositivo localizador sea capaz de realizar un muestreo IQ mientras conmuta entre las antenas.

Los dispositivos **BLE** que utilizaremos están basados en la placa de desarrollo LAUNCHXL-CC2640R2 de **TI**<sup>1</sup>. El CC2640R2 es un microcontrolador de bajo consumo con radio **BLE5** incorporada; su uso está enfocado a dispositivos restringidos en coste, ideal para desplegar de forma masiva en un sistema de localización. Se eligió ya que permite la transmisión de paquetes con **CTE**, muestreo IQ y la conmutación de antena tras detectar la presencia del **CTE**. El CC2640R2 solo tiene un puerto de antena, por lo que necesitaremos conmutadores externos. La agrupación de antenas utilizada es el BOOSTXL-AOA de **TI**, que incorpora los conmutadores de antena necesarios y se acopla a las placas de desarrollo elegidas.<sup>2</sup> Para poder

---

<sup>1</sup>La placa de desarrollo utilizada puede encontrarse en: <https://www.ti.com/tool/LAUNCHXL-CC2640R2>

<sup>2</sup>La placa con la agrupación de antenas puede encontrarse en: <https://web.archive.org/web/20210206210857/https://www.ti.com/tool/BOOSTXL-AOA>

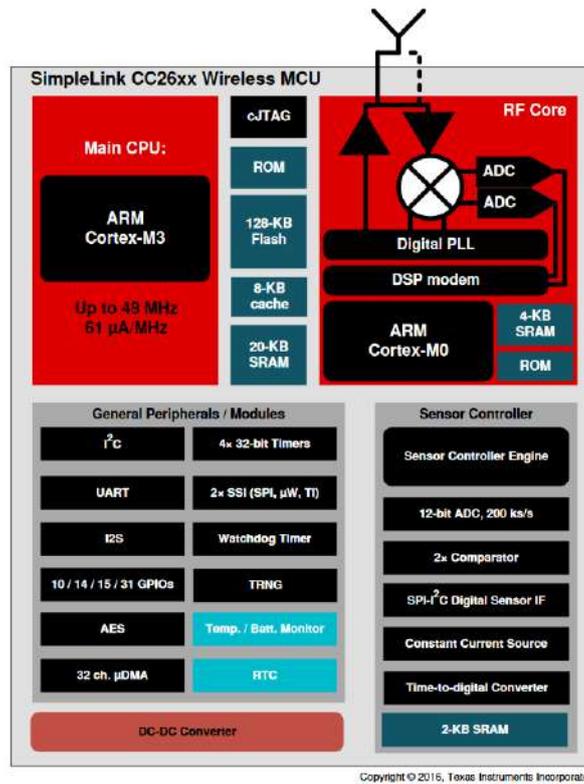


Figura 4.1: Arquitectura del TI CC2640R2F

utilizar antenas externas en el LAUNCHXL-CC2640R2, debemos de girar el condensador C51 a la posición C58 como se ve en la siguiente figura. De esta manera, desconectamos la antena impresa para terminar la línea con el conector de RF tipo JSC.



Figura 4.2: Modificación del necesaria LAUNCHXL-CC2640R2 para conectar el BOOSTXL-AOA

La arquitectura del CC2640R2 muestra que la radio depende de un componente conocido como

el RFCore. El RFCore del CC2640R2 es un ARM Cortex-M0 y está encargado del procesamiento de señal. [43] TI solo nos permite interactuar con el a través del **Command and Packet Engine (CPE)**, no permitiendo que modifiquemos su código; a diferencia de el procesador principal. [44, p. 1585] Esta situación es común entre la mayoría de fabricantes de microcontroladores que incorporan la radio, y supone la mayor barrera a la hora de experimentar con nuevas funcionalidades de los protocolos de radio, ya que no tenemos control directo sobre lo que transmitimos. A continuación, veremos los detalles de implementación que hacen posible este sistema.

## 4.1 Transmitir con CTE

En primer lugar, debemos transmitir paquetes **BLE** con **CTE**. Esto es, en principio, muy simple; Transmitir el paquete como haríamos habitualmente y añadir al finalizar una serie de unos. Estos unos, al ser transmitidos en el **GFSK** de **BLE**, resultarían en un tono a +250kHz del centro del canal; es decir, el **CTE**. En la práctica, no es tan simple. **BLE** tiene un mecanismo de whitening que evita las secuencias largas de bits repetidos y de usar un **PHY** codificado, se utiliza su respectivo codificador convolucional. Estos pasos, junto a otros como el cálculo del **CRC** [45] se realizan de manera automática en el RFCore antes de la transmisión, de forma transparente.

En la figura 3.4 vimos el formato de los paquetes con CTE. Observamos que también debemos de introducir cambios en la cabecera, tales como marcar el la presencia de un **CTE** con el bit de **CTE Presence bit (CTE)** y añadir el campo de **CTEInfo**. El **CTETime** se mide en número de octetos de "1" a transmitir como CTE, y va de 2 a 20, o lo que es lo mismo, de 16 a 160us. **CTEType** será 0 para indicar que es un **CTE** para **AoA**, podría usarse para configurar el periodo de muestreo en el caso de **AoD**. Además, hay un campo **Reserved for Future Use (RFU)**. Transmiremos los paquetes con el **CTE** de 160us. Es necesario usar un RFCore parcheado<sup>3</sup> para transmitir el **CTE** desactivando el whitening, los **ECC** y que permita extender la cabecera con el **CTEInfo**.

---

<sup>3</sup>Una copia de los parches puede encontrarse en: [https://github.com/contiki-ng/cc2640r2-sdk/tree/master/rf\\_patches](https://github.com/contiki-ng/cc2640r2-sdk/tree/master/rf_patches)

## 4.2 Muestrear y conmutar entre antenas

Para realizar las medidas de **AoA** utilizaremos también un CC2640R2 ya que permite la captura de muestras IQ de para su posterior procesado. Debemos de coordinarnos de nuevo con el RFCore, para obtener las muestras IQ y realizar la conmutación de antena en los momentos adecuados. Gracias al parche del firmware del RFCore, podemos obtener las muestras en bruto, sin ser procesadas por ninguna etapa del DSP, y también, ser notificados con una interrupción al recibir el CRC de un paquete; justo al comienzo del CTE. Sin embargo, aún nos encontramos con algunas limitaciones. Estas son que el RFCore no tiene acceso a los GPIO, y que el sistema de muestreo no está optimizado para este propósito.

El RFCore no tiene acceso a los GPIO, lo que dificulta la sincronización de la conmutación entre antenas con el inicio del CTE. La tarea de conmutación de antenas se realiza en el CPU principal, utilizando un GPTimer para realizar el cambio de antenas cada 4us. El RFCore produce una interrupción al terminar de recibir el paquete BLE, permitiendo iniciar el GPTimer durante el CTE. Este sistema tiene un retardo, desde que se lanza la interrupción hasta que se comienza la rutina de conmutación de antenas. Por suerte, mientras que el periodo de la conmutación sea constante (gracias al GPTimer) podemos calibrarlo. El RFCore lanza la interrupción 3.25us después de que comience el CTE, por lo que debemos dejar 0.75us extra para respetar el periodo de guarda antes de comenzar el muestreo, y después 8us más de periodo de referencia (tal y como se detalla en la Figura 4.3). Entonces, podemos empezar a recorrer el array antena a antena hasta que acabe el CTE.

Por otro lado, tenemos una limitación en el sistema de muestreo. No solo debemos de ser capaces de muestrear los paquetes, sino que debemos de mantener la funcionalidad **BLE** para detectar el final del paquete. Los ADC utilizados por el RFCore para muestrear la señal tienen una resolución de 13 bits, por lo que cada muestra de I o Q ocupará 16bits en memoria, 4 bytes cada pareja. La frecuencia de muestreo es de 4MHz y hay disponibles 2KB de SRAM de los 4KB dedicados al RFCore, donde almacenar las muestras IQ. Esto se traduce en que la memoria se llenará a una velocidad de 16 bytes/us, quedando completamente llena a los 127us. No podremos capturar un **CTE** de longitud completa usando el CC2640R2, ya que el **CTE** dura como máximo 160us. Además, necesitaremos tiempo para procesar las muestras de la ram del RFCore antes de poder recibir el siguiente paquete. Esto nos limitará la cantidad de paquetes

por segundo que podemos procesar a entorno 3 por segundo.

## 4.3 Procesado de las muestras

Una vez obtenidas las muestras, debemos de tener en cuenta varios factores durante el procesado. Factores como el tiempo de estabilización de los conmutadores, que los osciladores de transmisión y recepción pueden tener deriva durante el CTE o se produzcan cambios de fase en el sistema al cambiar la frecuencia a la que se envían los paquetes. Estas consideraciones se tienen en cuenta durante el procesado, por lo que solo impactan a la cantidad de paquetes por segundo que podemos localizar. Esto es debido a que debemos de liberar la memoria donde almacenamos las muestras antes de poder atender el siguiente paquete. El BOOSTXL-AOA que utilizamos está caracterizado en [11]. En esta calibración se incluyen los parámetros de calibración necesarios para compensar los desfases entre antenas (como variaciones entre las longitudes de las líneas de transmisión) y se almacena dicho valor por pares de antena dentro de cada ULA. Además, cada ULA tiene una lista de compensaciones de ángulo por canal. Estas calibraciones fueron medidas de forma empírica y son posiblemente fruto de múltiples efectos combinados.

Los conmutadores que utiliza el BOOSTXL-AOA, necesitan entorno a 2 $\mu$ s para estabilizarse. Esto nos obliga a descartar las primeras 8 muestras que obtengamos al cambiar de antena. Estaremos muestreando en realidad en una de cada dos ventanas de muestreo de 2 $\mu$ s, que al muestrear a 4MHz, resultará 8 muestras por ventana. De las cuales, podríamos desechar la primera y la última como se detalla en la Figura 3.5, aunque en este caso no es necesario.

Podemos utilizar el periodo de referencia para calibrar los osciladores de recepción y transmisión, ya que puede que el CTE no sea exactamente de 250 kHz. También podemos calcular la deriva que han tenido los osciladores comparando la diferencia de fase entre dos muestras (en tiempos distintos) en la misma antena. Supondremos que el emisor permanece estático durante la transmisión del CTE, y toda la diferencia de fase será debida a la deriva. Así podremos restar la contribución de la deriva. Tal y como vemos en el Algoritmo 1.

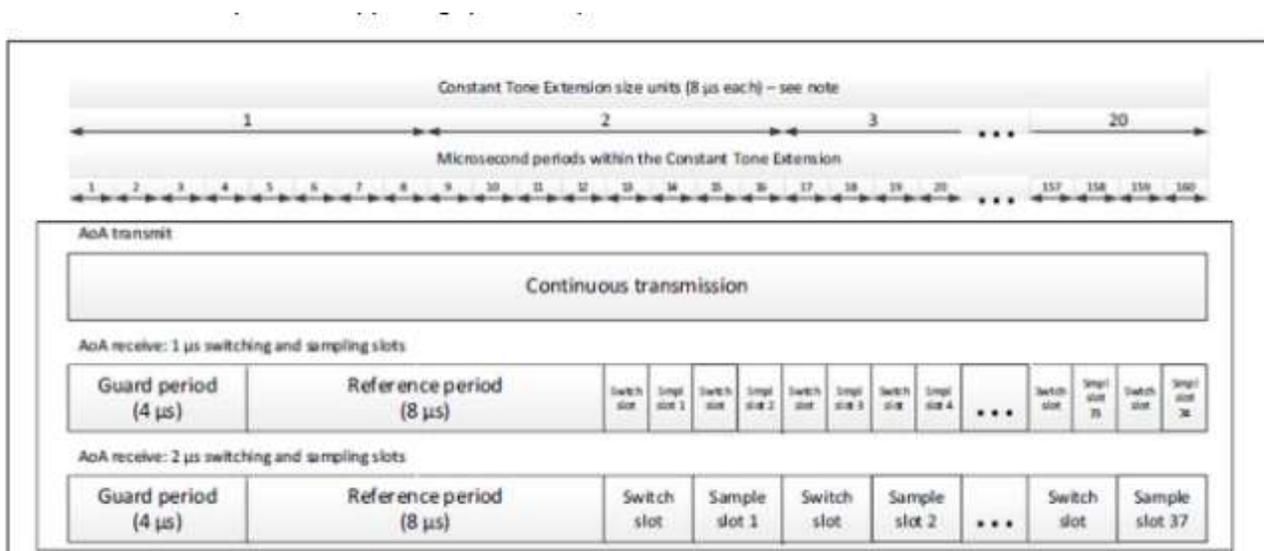


Figura 4.3: Estructura del CTE en Bluetooth Low Energy 5 [11]

### 4.3.1 Implementación del procesado de muestras

El BOOSTXL-AOA tiene dos agrupaciones de tres antenas, dispuestas a 90 grados. Utilizaremos para localizar el dispositivo la agrupación que reciba un mayor RSSI. El Algoritmo seguido para obtener el AoA dadas las muestras realizadas a un CTE se encuentra a continuación. Para realizar el cómputo del ángulo de llegada una vez muestreada la señal debemos asociar cada muestra con su correspondiente antena, por simplicidad operaremos con solo una muestra por antena en cada periodo de muestreo. El CC2640R2 es capaz de tomar más muestras como vimos anteriormente, por lo que solo tomaremos una<sup>4</sup>. Es importante destacar que en la implementación real las muestras estarán separadas periodos completos del CTE para ser comparables sin tener que compensar un desfase extra.

En lugar de calcular el ángulo de llegada por cada par de muestras, [1] en su implementación de referencia utiliza la optimización recogida en el Algoritmo [1]. En primer lugar, calcula el desfase de cada par de muestras utilizando el producto complejo conjugado de cada par de muestras tal y como vimos en la fórmula [3.7]. Esto permite calcular el desfase de la señal al ser recibida desde dos antenas con una única operación trigonométrica, la arco-tangente. Como vimos en la sección anterior, además es posible que exista un desfase acumulativo al que llamamos deriva. El efecto contribuido por la deriva se estima calculando el desfase entre dos muestras tomadas en la misma antena. Como vemos en el Algoritmo [1], línea 21, aplicaremos

<sup>4</sup>En general, esta es una aproximación de primer orden al cálculo del AoA. Se podría hacer un análisis más detallado de las muestras para tener en cuenta más efectos.

una compensación proporcional al tiempo entre ambas muestras. Esto se debe a que al tener más de 2 antenas en la agrupación, las muestras que comparemos estarán separadas entre sí distintas cantidades de tiempo, siendo afectadas más o menos por la deriva. Asumiremos que la deriva es constante en ese periodo entre las dos muestras en la misma antena que comparemos. Una vez calculados los desfases medios por cada par de antenas, deberíamos calcular el ángulo de llegada del frente de ondas utilizando la fórmula 3.8. Sin embargo, como se detalla en [11], es posible realizar este cálculo utilizando una transformación lineal. Esto evita realizar otra operación trigonométrica, el arco-seno. Este proceso está recogido en la línea 37 del Algoritmo 1. Por último, realizamos la media del AoA obtenido en cada par de antenas y ese será nuestro resultado final una vez compensemos la desviación asociada al canal (de nuevo, tal y como se detalla en [11]). Los valores de calibración del BOOSTXL-AOA y el patrón de conmutación entre antenas utilizados se encuentran en el Software Development Kit (SDK) en los archivos `ant_array1_config_boostxl_rev1v1.c` y `ant_array2_config_boostxl_rev1v1.c`

### 4.3.2 TI Real Time Location System (RTLS) Toolbox

Para facilitar la implementación de los sistemas de localización basados en BLE, Texas Instruments pone a disposición de sus clientes una librería para gestionar Real Time Location System (RTLS). Actualmente TI ha dejado de soportar las funcionalidades de localización avanzada en el CC2640R2 debido a las limitaciones del RFCore descritas anteriormente<sup>5</sup>. Utilizaremos la versión del SDK 3.40.00.10 para nuestras pruebas.

---

<sup>5</sup>Una nueva familia de MCUs, la cc26x2, utiliza un RFCore core que ha contemplado desde un primer momento este caso de uso. La última implementación a fecha de diciembre de 2023 puede encontrarse en: [https://software-dl.ti.com/simplelink/esd/simplelink\\_cc13xx\\_cc26xx\\_sdk/7.10.02.23/exports/examples/rtos/CC26X2R1\\_LAUNCHXL/ble5stack/rtls\\_coordinator/README.html](https://software-dl.ti.com/simplelink/esd/simplelink_cc13xx_cc26xx_sdk/7.10.02.23/exports/examples/rtos/CC26X2R1_LAUNCHXL/ble5stack/rtls_coordinator/README.html)

---

**Algorithm 1** Cálculo del AoA

---

```

1: patrón           // Objeto que define la agrupación de antenas y su patrón de muestreo
2: muestras[n]     // Lista de las muestras
3:
4:
5: procedure PROCESADO DE MUESTRAS(patrón, muestras)
6:   // Matriz de acumuladores de desfase entre antenas
7:   desfases = 0
8:
9:   for muestraA en muestras do
10:    if muestraA es valida then      // Tiene siguiente y anterior
11:      for par en patrón do
12:        // b y c son la distancias en muestras a muestraA
13:        // muestraC es la muestra siguiente, en la misma antena que muestraA
14:
15:        muestraB, b = patrón.Siguiente(muestraA)
16:        muestraC, c = patrón.Repeticion(muestraA)
17:
18:        // Calculamos la deriva que se ha producido por muestra desde muestraC
19:        // Calculamos cuanto se produciría de ser constante entre
20:        // que se tomó la muestraA y la muestraB
21:        deriva = desfase(muestraA, muestraC)
22:        derivaPorMuestra = deriva / b
23:        compensación = derivaPorMuestra * c
24:
25:        // Calculamos el desfase corregido y lo añadimos al acumulador
26:        desfase = desfase(muestraA, muestraB)
27:        desfases[par] += desfase - compensación
28:
29:    // Calculamos la media de cada acumulador
30:    medias = media(desfases)
31:
32:    // Aplicamos la calibración de cada par de antenas de la agrupación
33:    for par en patrón do
34:      // A cada par de antenas le corresponde una calibración de signo, ganancia y desfase
35:      (signo, desfase, ganancia) = par.calibración()
36:      dato = media[par]
37:      resultados[par] = signo * (dato + desfase) * ganancia
38:
39:    // Calcular la media de todos los pares del ángulo de llegada
40:    resultado = media(resultados)
41:    // Aplicar la corrección para el canal
42:    resultado += patrón.channelOffset
43:    return resultado

```

---

## 5 Experimentos

En este capítulo validaremos la implementación del sistema de medida de **AoA** haciendo uso del sistema **Real Time Location System (RTLS)** de **TI**. Usando, como vimos en el capítulo anterior, dispositivos basados en el LAUNCHXL-CC2640R2 y utilizando como agrupación de antenas el BOOSTXL-AOA. El **BT SIG** define en la especificación de **BLE5** [16] las pruebas a realizar durante el proceso de certificación y validación de los dispositivos. Estas incluyen un **Test Suite (TS)** referente a las propiedades físicas de la radio<sup>1</sup>. En este **TS** se recogen los procedimientos para comprobar características como el cumplimiento de la plantilla de potencia, medida de sensibilidad, o transmisiones espúreas. En el contexto de **BLE**, como vimos en la sección 3.1.1, el **PHY** está una capa por encima de estas propiedades. Es por eso que el **SIG** define un **RF-PHY-TS**<sup>2</sup>, en el que se detallan los casos de prueba pertinentes para la validación del **CTE** y el **Complex Sampling (IQ)**. En este caso, con CC2640R2F configurado como se expone en el capítulo anterior, nos interesan las siguientes pruebas:

- **RFPHY/TRM/BV-15-C**: Potencia de TX con **CTE** y **PHY** 1 MS/s.
- **RFPHY/TRM/BV-16-C**: Desplazamiento y deriva en frecuencia en TX con **CTE** y **PHY** 1 MS/s.
- **RFPHY/RCV/IQC/BV-05-C**: Coherencia de las muestras **IQ** con ranuras de 2us y **PHY** 1 MS/s.
- **RFPHY/RCV/IQDR/BV-11-C**: Rango dinámico de las muestras **IQ** con ranuras de 2us.

---

<sup>1</sup>El **RF-TS** puede encontrarse en:

[https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc\\_id=173655](https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=173655)

<sup>2</sup>El **RF-PHY-TS** puede encontrarse en:

[https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc\\_id=225827](https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=225827)

Sin embargo, por limitaciones materiales, en este trabajo no es posible la validación de la implementación del sistema siguiendo la metodología del SIG. A continuación se realizará la validación cualitativa de que el dispositivo a localizar transmite correctamente las CTE. Después, mediremos el desempeño del sistema al completo midiendo AoA en una cámara anecoica. Por último, comprobaremos el funcionamiento del sistema en entornos reales.

Se ha decidido utilizar todos los canales de BLE añadiendo el CTE a los paquetes que se transmiten una vez se ha realizado una conexión. De este modo, se utilizarán más canales dentro de los posibles en BLE, en lugar de estar limitados a los destinados al anuncio. Un comportamiento similar a nivel de radio podría conseguirse haciendo uso de las nuevas capacidades de anunciado de BLE5, los anuncios periódicos y extendidos. Esta decisión permitiría en un despliegue real disminuir el consumo de batería del dispositivo a localizar, ya que sería posible adaptar el plan de transmisión de forma dinámica. Como vimos en la Figura 3.3, el consumo al transmitir es mucho mayor que al recibir.

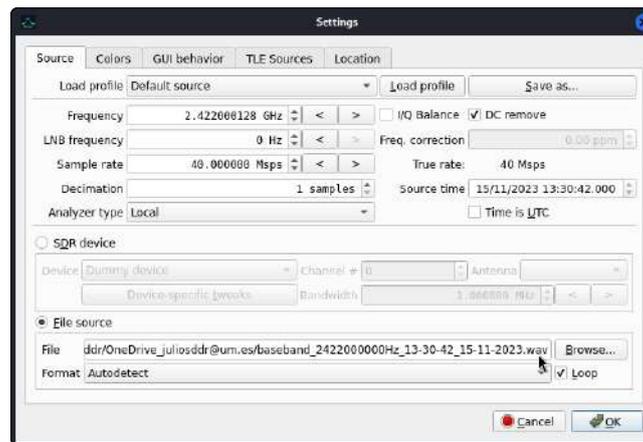
## 5.1 Validación Transmisión con CTE



**Figura 5.1:** LAUNCHXL-CC2640R2 (abajo) y bladeRF (arriba) con antena log-periodica (derecha).

Para confirmar que podemos transmitir correctamente los paquetes BLE que contienen un CTE, utilizaremos el montaje que puede verse en la figura 5.1. Los paquetes BLE se transmitirán con

un LAUNCHXL-CC2640R2, como detallamos en el capítulo anterior. Para capturar la señal utilizaremos un **Software Defined Radio (SDR)**, concretamente un Nuand bladeRF 1<sup>3</sup>. El bladeRF solo se utilizará como receptor, por lo que el puerto de TX quedará conectado a una carga de 50 Ohmios. En su puerto de RX, conectaremos una antena log-periodica (construida usando **Printed Circuit Board (PCB)**)<sup>4</sup>. Esta combinación de receptor y antena nos da la flexibilidad de poder analizar una amplia sección del espectro<sup>5</sup>, siendo adecuada para la exploración de la banda de 2.4GHz que utiliza **BLE**. Una de las limitaciones de este montaje es la ausencia de calibración, por lo que lo usaremos de forma cualitativa.



**Figura 5.2:** Configuración de Sigdigger para abrir la grabación que contiene los paquetes con CTE

Para grabar y analizar la señal utilizaremos el programa libre Sigdigger<sup>6</sup>, conectando el bladeRF por USB a un portátil corriendo Linux. SigDigger es un programa de análisis de señales digitales, que permite la captura directa de las mismas usando diversos SDR. Está enfocado al tratamiento de señales desconocidas e incorpora una gran variedad de estimadores y demoduladores para su análisis. En este caso lo utilizaremos para visualizar la señal de los paquetes **BLE** en el dominio del tiempo.

Realizaremos una captura con el bladeRF a 40 **IQ Mega Sample Per Second (MSPS)** sintonizado a una frecuencia central de 2.422GHz capturando una buena parte de la banda **ISM** de 2.4GHz. La captura irá de 2402 a 2442MHz, abarcando por completo los canales BLE del 0 al 17

<sup>3</sup>El bladeRF permite la captura de hasta 40MSPS de 12 bits, en el rango de 300MHz a 3.8GHz.

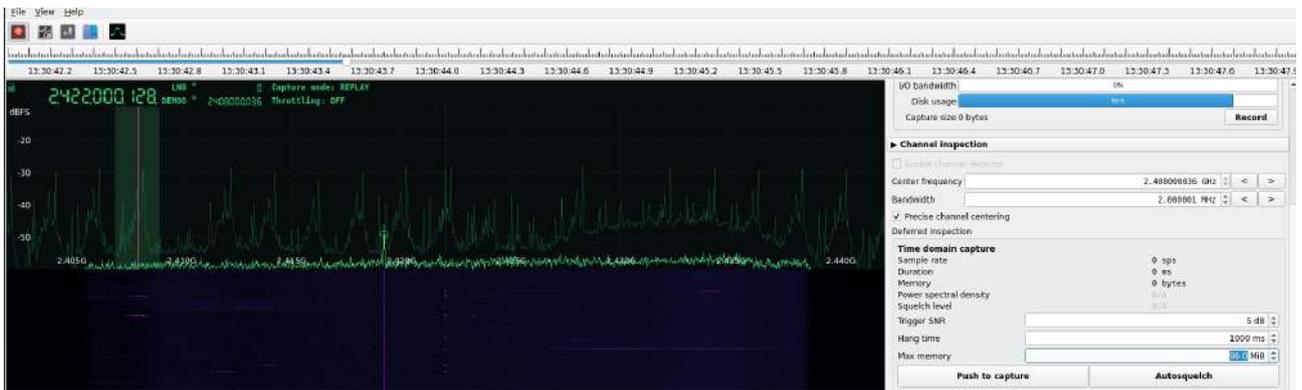
<https://www.nuand.com/bladerf-1/>

<sup>4</sup>La antena utilizada es la Log-Periodic 850-6500 MHz de Kent Electronics.Su hoja de datos se encuentra:

<https://www.wa5vjb.com/pcb-pdfs/LP8565A2.pdf>

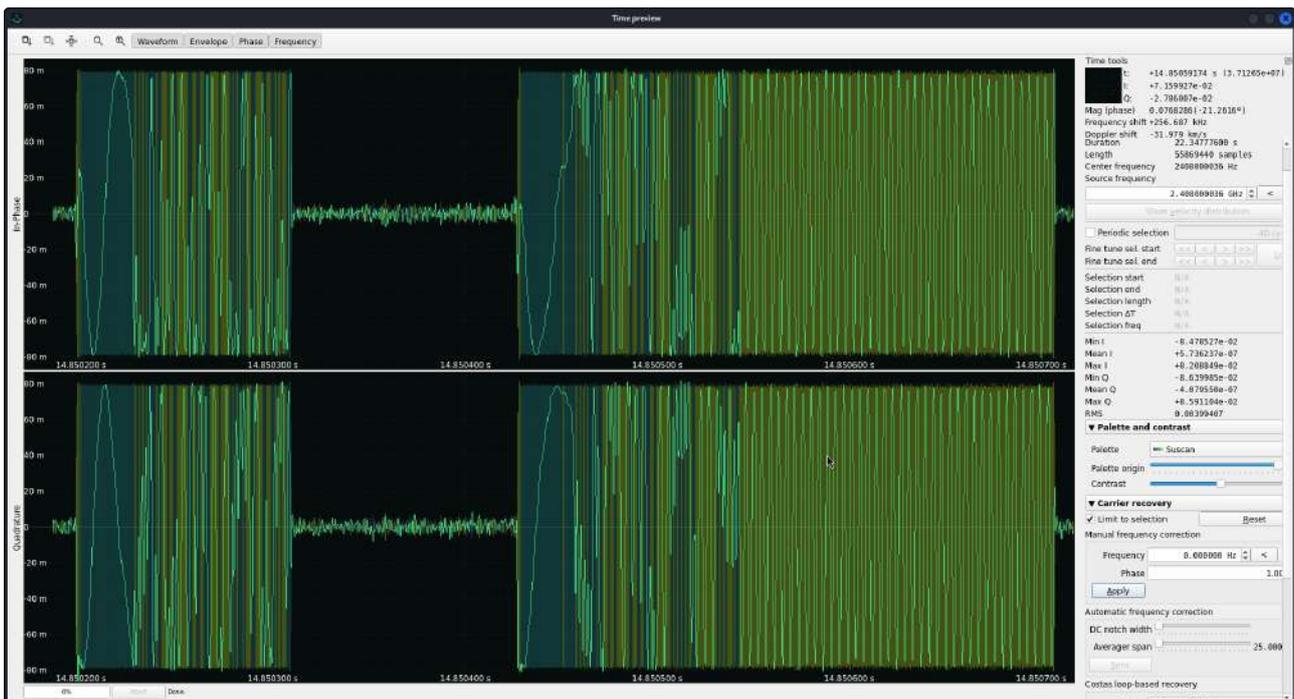
<sup>5</sup>Agradecer a Alejandro Aliaga del **RCE** su regalo. Gracias a él, esta combinación de dispositivos me acompaña en mis exploraciones del espectro.

<sup>6</sup>SigDigger es un programa libre que puede encontrarse en: <https://github.com/BatchDrake/SigDigger>



**Figura 5.3:** Selección del canal 2 de BLE para su análisis

incluyendo el 38 como muestra la Figura 3.2. Solo se capturará la mitad del ancho de banda del canal 37 y el 18. <sup>7</sup>. Configuraremos Sigdigger para sintonizar el canal 2 de BLE para su análisis, filtrando 2MHz entorno a 2408MHz como se ve en la Figura 5.3 y usando el LAUNCHXL-CC2640R2 transmitiremos 2 paquetes BLE, el primero sin CTE y el segundo con un CTE de 160us.



**Figura 5.4:** Sigdigger mostrando dos paquetes BLE capturados. El segundo con CTE.

En la Figura 5.4, se observan los dos paquetes BLE transmitidos por el CC2640R2. En la

<sup>7</sup>Para capturar todos los canales de BLE necesitaríamos cubrir de 2401 a 2481 MHz y no es posible capturar 80MHz de ancho simultáneo con el bladerf. Se necesitaría un SDR capaz de realizar 80MSPS IQ.

figura vemos superpuestos colores en la señal, representando su frecuencia instantánea. Cada frecuencia se corresponde con un 0 o 1 ya que BLE utiliza GFSK como modulación. En esta representación, la frecuencia correspondiente a un 1 tiene un tono amarillo, mientras que el 0 es verde. Para estudiar la Figura 5.4, utilizaremos como referencia la Figura 3.4. En ambos paquetes se distingue un preámbulo, seguido de información. Podemos distinguir que al final del segundo paquete, donde esperamos el CTE, el color no cambia. Podemos confirmar que el whitening está desactivado en ese periodo de tiempo, ya que con él, no sería posible la transmisión de tantos símbolos iguales. Utilizando los cursores podemos comprobar en la Figura 5.5 que la longitud de esta sección de símbolos iguales tiene una duración de 164us. Esto puede deberse a que el CTE tenga una duración ligeramente superior a la esperada, o que el último campo del paquete (que como vimos en la Figura 3.4 es el CRC) podría acabar en 4 '1' sucesivos.

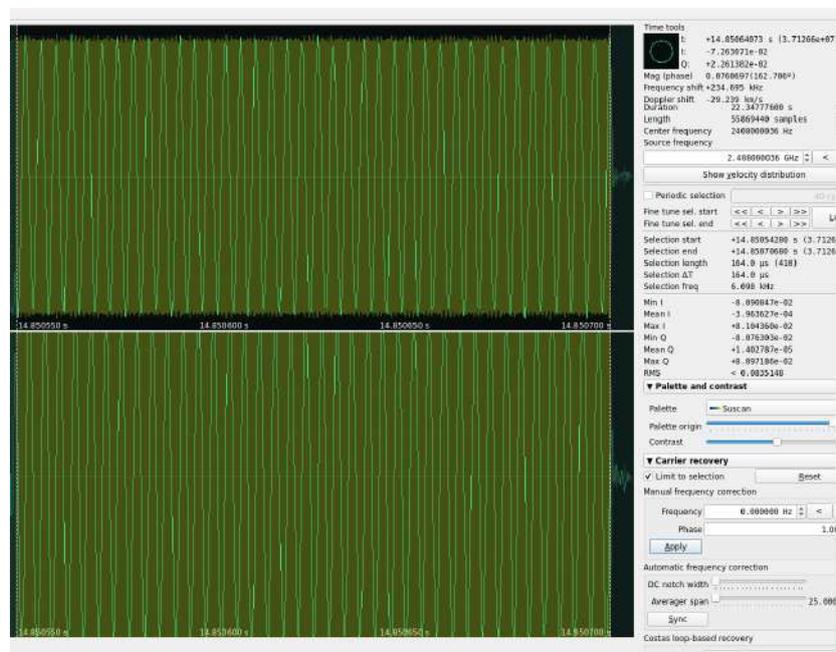
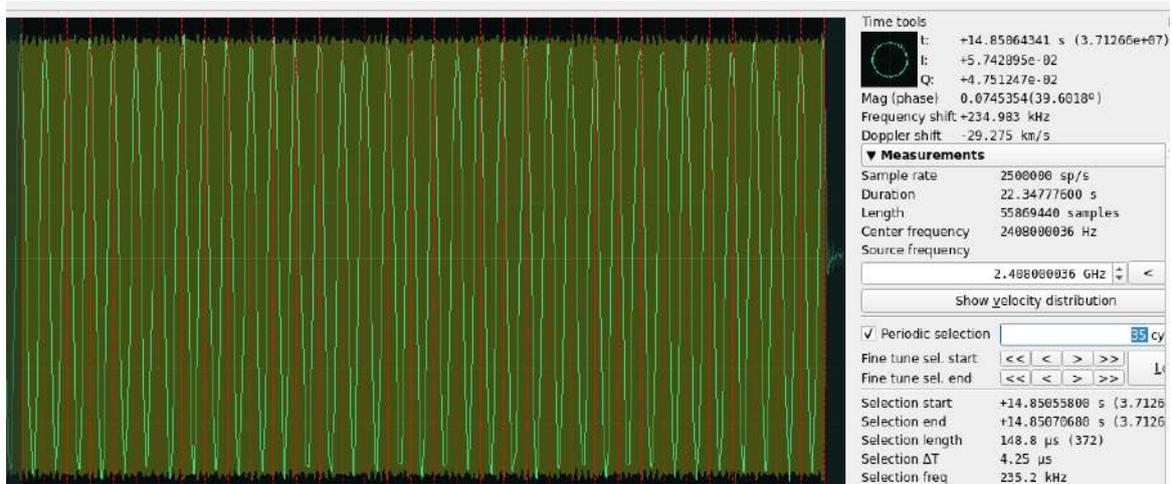


Figura 5.5: Medida de la duración del CTE usando los cursores de Sigdigger

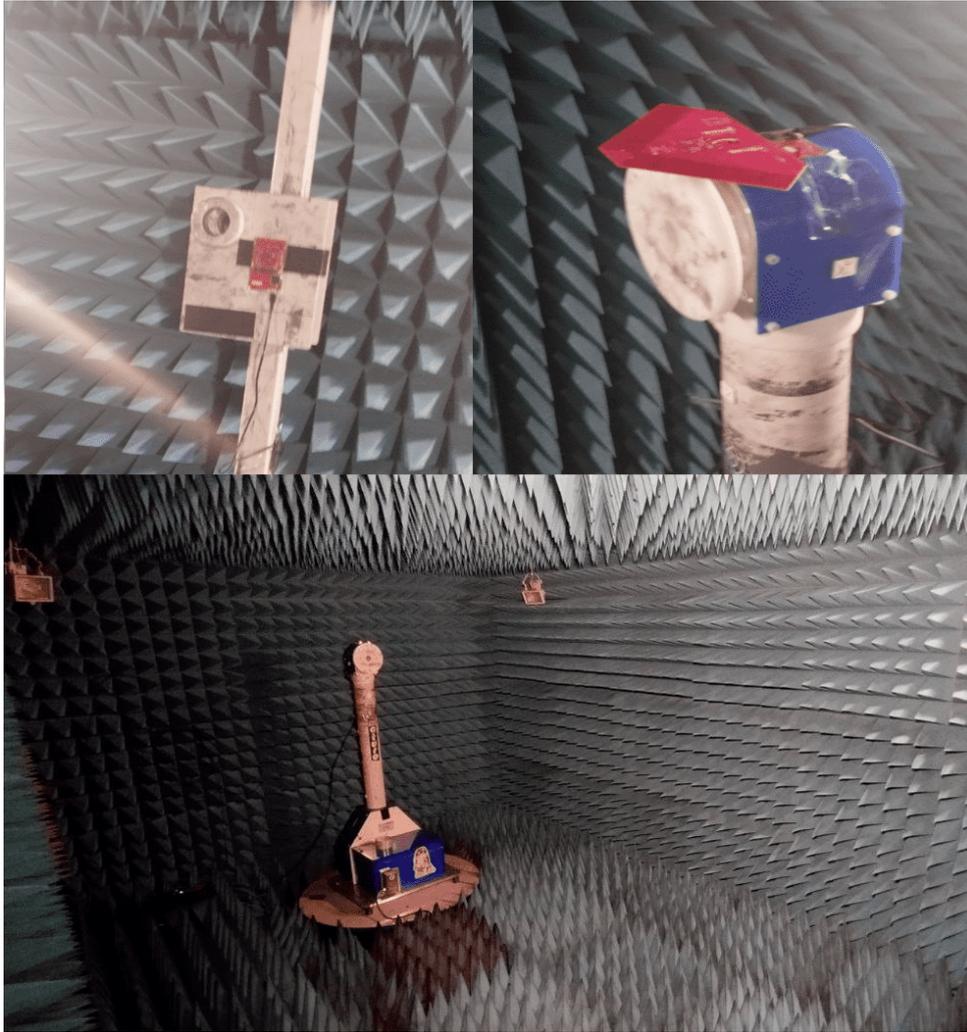
Por último, haciendo uso de la selección periódica podemos medir la frecuencia del CTE. Ajustamos los cursores de inicio y final en las crestas de la sinusoide y ajustamos el número de ciclos para que se corresponda con el de periodos de la señal entre los cursores. En la Figura 5.6 podemos comprobar que la frecuencia de la señal durante el CTE es de 235,2kHz. Midiendo en otros paquetes de la grabación, parecería que esta desviación es aproximadamente la misma en

todos los paquetes. Este error podría deberse al equipo de medida. La frecuencia esperada del **CTE** es de 250KHz, tal y como vimos en capítulos anteriores. Esta desviación en frecuencia, de no ser compensada, provocaría una medición errónea tal y como se explicó en la última sección del capítulo anterior.



**Figura 5.6:** Medida de la frecuencia del **CTE** usando la selección periodica de Sigdigger

## 5.2 Validación del sistema en cámara anecoica

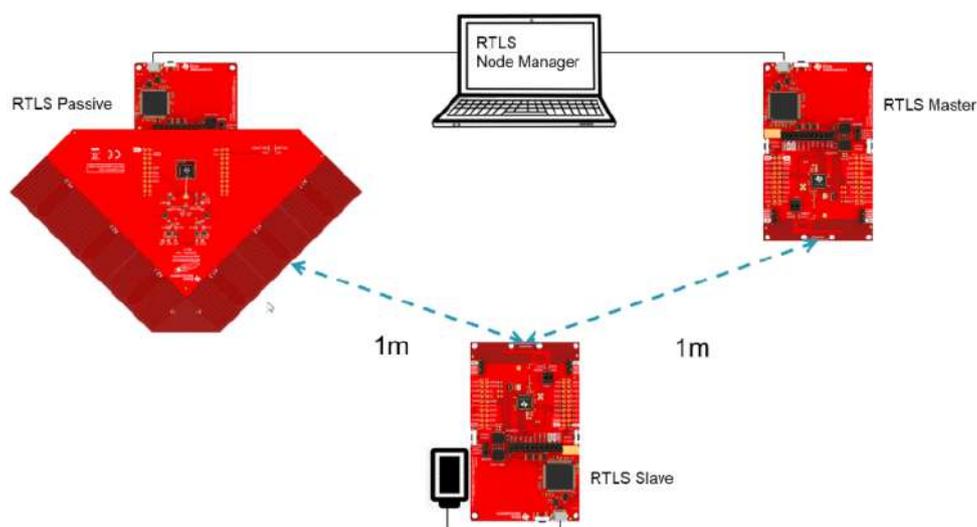


**Figura 5.7:** Montaje en la cámara anecoica

Para comprobar el correcto funcionamiento del sistema de medida de **AoA** descrito en el capítulo anterior, realizaremos una validación fin a fin en un entorno controlado. Esta validación consistirá en un barrido angular en la cámara anecoica de la Escuela Técnica Superior de Ingeniería de Telecomunicación de la **Universidad Politécnica de Cartagena (UPCT)**. Para realizar el barrido angular, utilizaremos el posicionador para girar la agrupación de antenas entre medidas. Mientras, el dispositivo a localizar permanece estático a una distancia fija de aproximadamente 3m. Detalles del montaje pueden verse en la Figura **5.7**. La cámara anecoica tiene un tamaño de 3x4x3m y un rango de operación en frecuencia de 0.5 a 6 GHz, siendo adecuada para este experimento con **Bluetooth Low Energy (BLE)**, ya que como hemos visto opera a 2.4GHz.

Los dispositivos utilizados son los descritos en el capítulo anterior, basados en el LAUNCHXL-

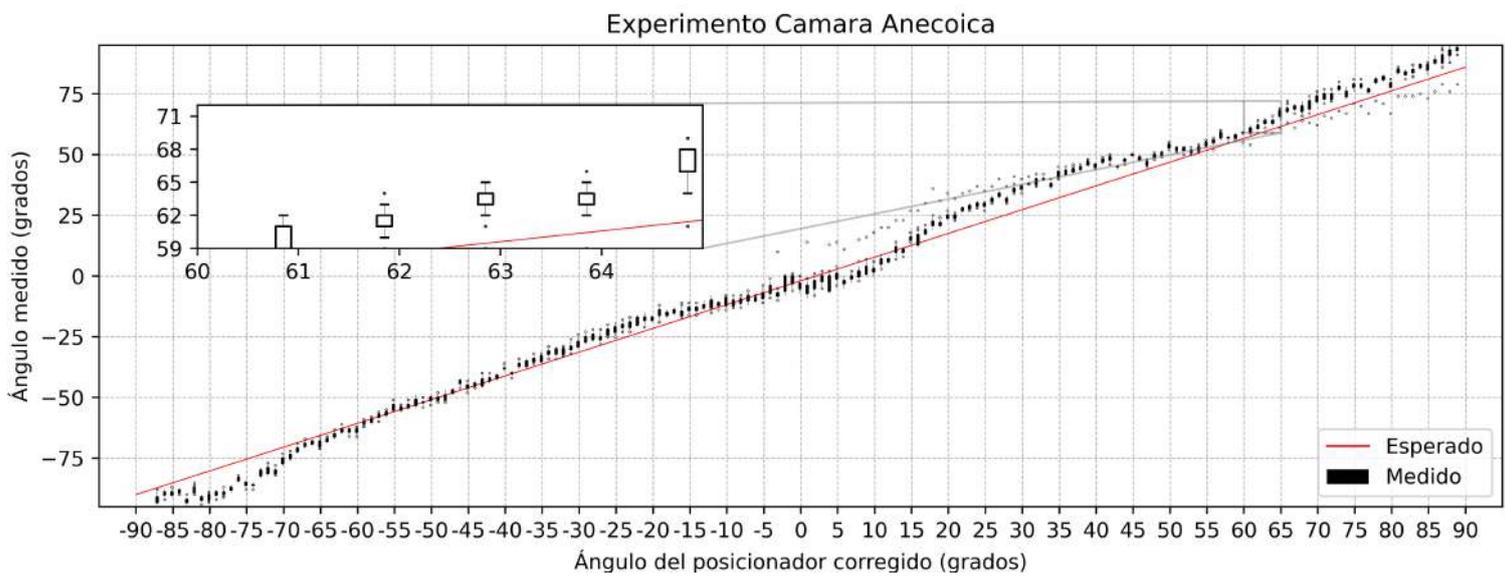
CC2640R2 y usando el BOOSTXL-AOA como agrupación de antenas. Siguiendo la arquitectura de toma y procesamiento de muestras descrita en el mismo. Sin embargo, tal y como se ve en la figura 5.8, aparece un tercer dispositivo, el maestro. Para los experimentos se ha dividido el dispositivo localizador, separando las labores de muestreo del CTE y la conmutación de antena en un dispositivo (el pasivo); mientras que el maestro se coordina con el dispositivo a localizar (esclavo). De esta manera, el pasivo solo deberá esperar la señalización del maestro, que contendrá el cuándo y dónde (en qué frecuencia) deberá de recibir el paquete con CTE. El maestro realizará las tareas de conexión y comunicación con el esclavo. Las tareas de procesamiento de la señal recibida se realizan en el pasivo, siendo el ordenador solo utilizado para facilitar la comunicación entre maestro y pasivo haciendo uso de la librería RTLS Node Manager de TI; además de almacenar los resultados de las medidas de AoA para su representación y análisis. El esclavo solo estará conectado a un alimentador (en sustitución de una batería) y al maestro de forma inalámbrica.



**Figura 5.8:** Sistema de medida del AoA con 3 dispositivos [10]

Realizaremos la medida del ángulo de llegada de 95 paquetes BLE con Constant Tone Extension (CTE) por posición. Y recorreremos el espacio comprendido de  $-90^\circ$  a  $90^\circ$  en pasos de  $1^\circ$  usando el posicionador. Dado que el alineamiento a  $0^\circ$  entre el pasivo en el posicionador y el esclavo se ha realizado a mano, los datos se han calibrado en el post-procesado. Todas las posiciones se han desplazado  $2.85^\circ$  en sentido horario, de tal modo que el error medio es cero. Los resultados de esta campaña de medidas pueden observarse en un diagrama de cajas y bigotes en la Figura 5.9.

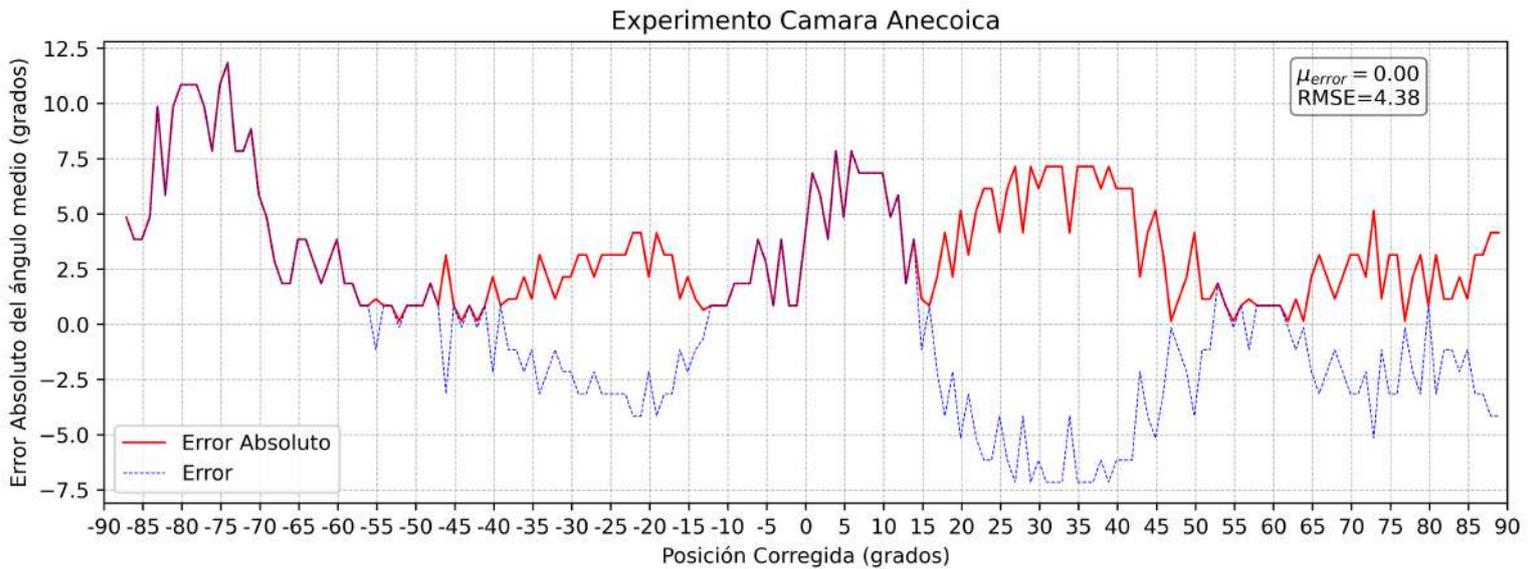
En este gráfico, y los sucesivos diagramas de cajas y bigotes en este capítulo, las cajas representan el rango intercuartílico de las medidas en cada posición, con el límite inferior y superior correspondiente al percentil 25 y 75, respectivamente. Los bigotes se extienden a los percentiles 5 y 95, y cualquier punto fuera de estos bigotes es considerado un valor atípico. Los puntos atípicos están representados como círculos. El diagrama de cajas y bigotes se ha elegido ya que permite visualizar de manera rápida la variabilidad y la tendencia de los datos; permitiendo un análisis cualitativo rápido y completo. Adicionalmente, se incluye una línea roja que muestra los valores esperados; esta línea representa los puntos en los que el ángulo medido coincidiría con el ángulo corregido del posicionador.



**Figura 5.9:** Medidas de ángulo en la cámara anecoica

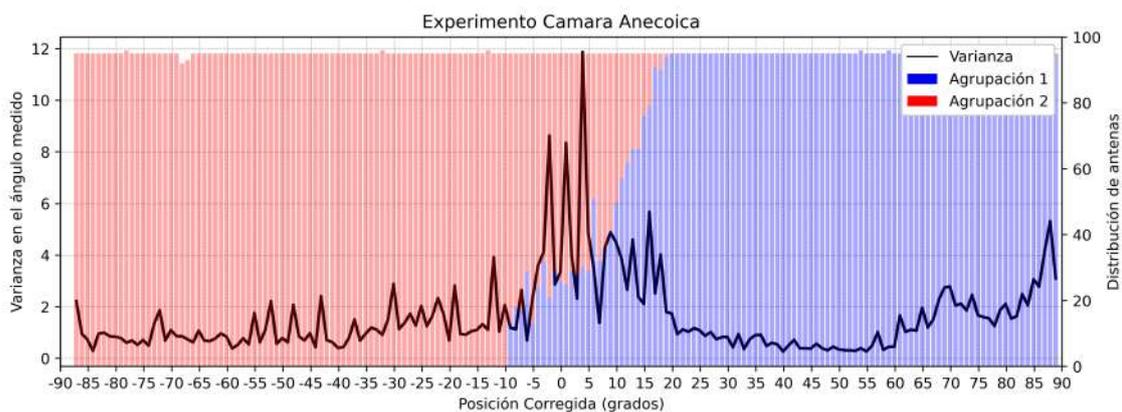
En la Figura 5.9, se puede observar que los valores medidos en cada posición se extienden en pocos grados y que los datos medidos siguen de cerca la línea de valores esperados. Sin embargo, su interpretación precisa es difícil dada la escala. Este resultado confirma que el sistema de medida de AoA implementado funciona. Para valorar su desempeño, nos apoyaremos en las Figuras 5.10 y 5.11. En la Figura 5.10 observamos el error cometido en cada posición entre la media de los valores medidos y su valor esperado. Se ha calculado también el RMSE, que fue de 4.38 grados.

En la Figura 5.11 se ven representados dos datos. Tenemos la varianza de los ángulos medidos y una representación de la proporción de medidas que se ha realizado con cada agrupación en



**Figura 5.10:** Visualización del error en las mediciones de la cámara anecoica

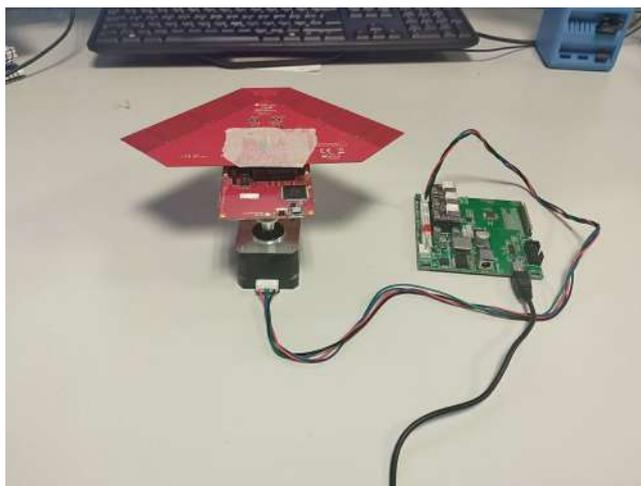
cada posición. Como se explicó en el capítulo anterior, el BOOSTXL-AOA está compuesto de dos agrupaciones y usaremos para medir la que mayor RSSI reciba en cada paquete. Esto está representado en el gráfico como un diagrama de barras, en el que se representa la proporción de medidas realizadas con cada agrupación por posición. Así vemos que el sistema de medidas mantiene una varianza de menos de 2, salvo en las posiciones entorno a  $0^\circ$ , que aumenta al realizarse medidas desde ambas agrupaciones. Esto refleja que podría existir una discontinuidad entre las medidas realizadas con una agrupación y la otra.



**Figura 5.11:** Visualización de la varianza en las mediciones de la cámara anecoica

## 5.3 Pruebas en entornos reales

Una vez validado el correcto funcionamiento del sistema en la cámara anecoica, podemos probar el desempeño del sistema en entornos reales. Utilizaremos los dispositivos en la misma configuración que en la sección anterior. En esta ocasión, no contamos con el posicionador de la cámara anecoica para variar el ángulo por lo que hemos construido uno utilizando piezas de una cortadora láser. El posicionador se compone de un controlador y un motor paso a paso como se ve en la Figura 5.12. El controlador del motor utilizado es una placa Woodpecker para máquinas CNCs de escritorio, corriendo GRBL<sup>8</sup>. El sistema nos permitirá realizar los barridos angulares que necesitamos de forma automática, coordinando la toma de datos desde el ordenador. En estos experimentos, recorreremos de  $-100^\circ$  a  $100^\circ$  en pasos de  $1^\circ$ . Realizaremos la medida de AoA siguiendo el esquema descrito en la sección anterior, transmitiendo 50 paquetes con CTE por posición. La principal desventaja de este montaje es la dificultad de alineamiento inicial, que deberemos de compensar en el post procesado.



**Figura 5.12:** Montaje del BOOSTXL-AOA en el motor NEMA17 con la controladora GRBL.

Se han seleccionado dos entornos fuera del laboratorio y en cada uno domina un efecto sobre el canal inalámbrico diferente. En ambos escenarios se ha ubicado el esclavo y el pasivo a 3m de distancia, manteniendo una línea de visión totalmente despejada entre ambos. El primer escenario pretende probar el sistema en un entorno con alta probabilidad de interferencias, mientras que el segundo representa un entorno con fuerte influencia del efecto multi-camino.

---

<sup>8</sup>GRBL es un firmware libre para CNCs, disponible en: <https://github.com/grbl/grbl>

Estas características son, como hemos visto en los capítulos anteriores, de esperar en los entornos en los que podría desplegarse un sistema de posicionamiento de las características que hemos seleccionado, por lo que interesa conocer su influencia. Se transmitirán 45 paquetes con CTE por posición para la medida del AoA.

### 5.3.1 Campaña de medidas en el Palacio de los Deportes



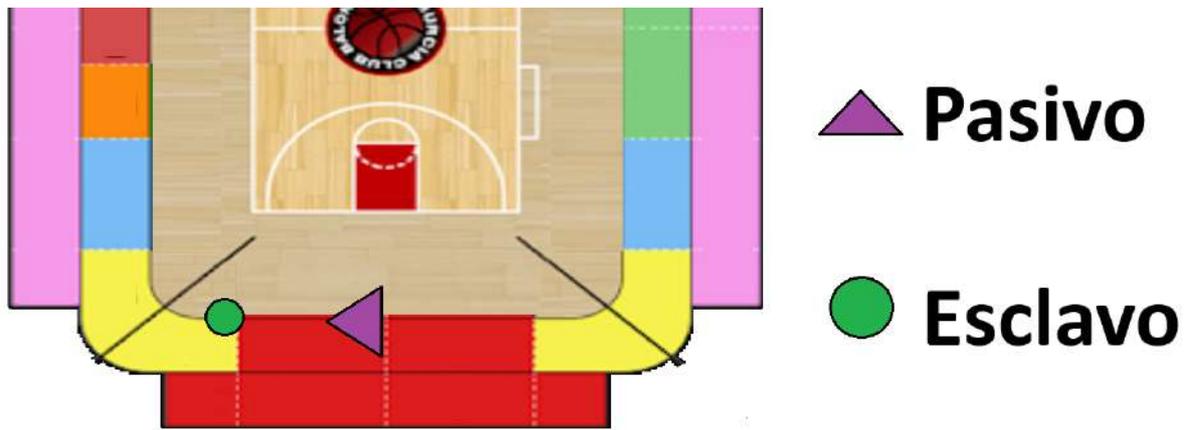
**Figura 5.13:** Foto durante la campaña de medidas en el Palacio de los Deportes

La primera localización es el Palacio de los Deportes <sup>9</sup> durante el evento de la Murcia Lan Party <sup>10</sup>. El experimento se realizó en la pista principal del polideportivo, un espacio muy amplio, que podría ser también representativo de un concierto o centro comercial. Realizar el experimento durante la MLP nos permite probar el comportamiento del sistema al estar expuesto a interferencias. Durante el evento, casi un millar de "gamers" se congregan para jugar en el Palacio de los Deportes de Murcia. El evento está infectado de dispositivos que hacen uso de la banda ISM de 2.4GHz, tanto con conexiones Wi-Fi como periféricos inalámbricos que dejan de funcionar al separarse más de un metro de sus receptores. Podemos ver la fuente de interferencias para este experimento en la Figura 5.13.

Como hemos visto en capítulos anteriores, las interferencias podrían afectar significativamente

<sup>9</sup>Ubicación del Palacio de los Deportes: <https://maps.app.goo.gl/5HavF5Ks8GvwpgjH9>

<sup>10</sup>Evento Murcia Lan Party (MLP): <https://www.murcialanparty.com/>

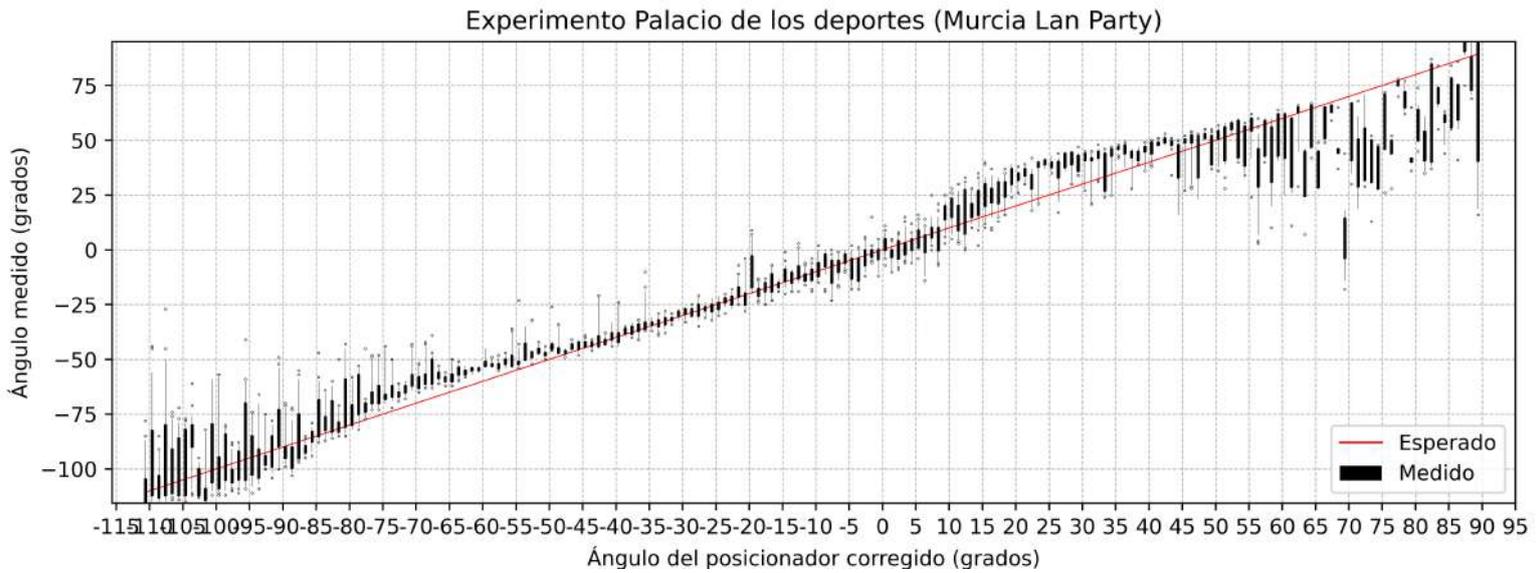


**Figura 5.14:** Esquema de la localización de los dispositivos en el Palacio de los Deportes

al sistema de medida de **AoA** usando **BLE**. Esto se debe a que el **CTE** no está protegido por los mecanismos de detección y corrección de errores que utilizan las conexiones **BLE**. Es decir, se descartarán los paquetes en los que se detecten errores no corregibles en los campos de datos, pero no podrán detectarse los errores provocados por las interferencias durante el **CTE**. Estos errores no detectados provocarían desfases entre las muestras que no podríamos compensar, desviando la medida de **AoA**.

Para el experimento, se colocaron los dispositivos tal y como se muestra en la Figura 5.14. El posicionador se ubicó en las gradas con el BOOSTXL-AOA, a 4.5m sobre la pista y unos 4m de distancia de los participantes del evento. El dispositivo a localizar se encontraba también en la grada, en la esquina de pista, a unos 3m de distancia del posicionador. El ordenador con el que se toman las medidas se encontraba debajo de las gradas.

Los resultados de la campaña de medidas de encuentran representados de nuevo en un diagrama de cajas y bigotes, en la Figura 5.15. El procesamiento de los datos es equivalente al realizado anteriormente, con la diferencia del cambio rango de ángulos barridos (de  $\pm 90^\circ$  a  $\pm 100^\circ$ ) y que en esta ocasión se han procesado 45 paquetes por posición. Además, en esta ocasión, se ha realizado una corrección de 10.6 grados en sentido anti-horario a las etiquetas del posicionador.



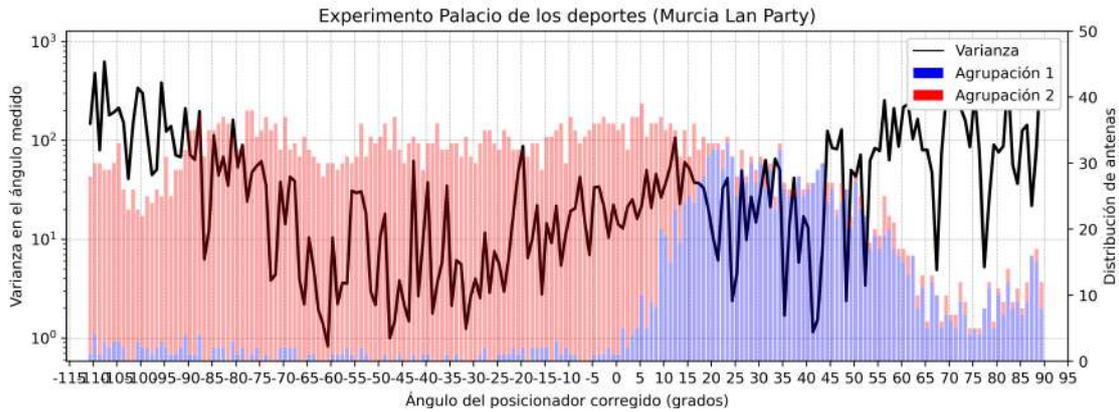
**Figura 5.15:** Medidas de ángulo en el Palacio de los Deportes

En la Figura 5.15, se puede comprobar que de nuevo las medidas siguen la tendencia de los valores esperados, tal y como veíamos en las medidas realizadas en la cámara anecoica en la Figura 5.9. A diferencia de las medidas realizadas en el caso ideal, podemos ver claramente que las medidas en los extremos del gráfico están contenidas en un intervalo más grande que en el tramo central. En el gráfico de la Figura 5.16, podemos ver con más detalle el error en las medidas con respecto al valor esperado. Podemos comprobar que el error aumenta significativamente a partir de los 60°, dirección hacia la que se encuentra la "fuente de interferencias" como vimos en la figura 5.14. El RMSE medio de la campaña de medidas ha sido 11.42 grados.



**Figura 5.16:** Error en las medidas tomadas en el Palacio de los Deportes

En la Figura 5.17 vemos la variancia de las medidas, esta vez en escala logarítmica. En esta ocasión no se aprecia el efecto provocado por la combinación de datos de ambas agrupaciones que veíamos en la Figura 5.11. Además, en este gráfico podemos observar claramente el efecto de las interferencias en la comunicación. Al descartarse los paquetes recibidos con errores no corregibles, podemos ver como la suma de los paquetes recibidos por las dos agrupaciones no suma los 45 paquetes que transmitimos y que el número de paquetes descartados aumenta al acercarse a la fuente de interferencias.



**Figura 5.17:** Visualización de la variancia y supervivencia de paquetes durante la MLP

Confirmamos así la hipótesis de que las interferencias tienen un impacto significativo en el proceso de medida de AoA. Sin embargo, un estudio más detallado sería necesario para la caracterización completa del comportamiento de un sistema de medidas BLE de AoA.

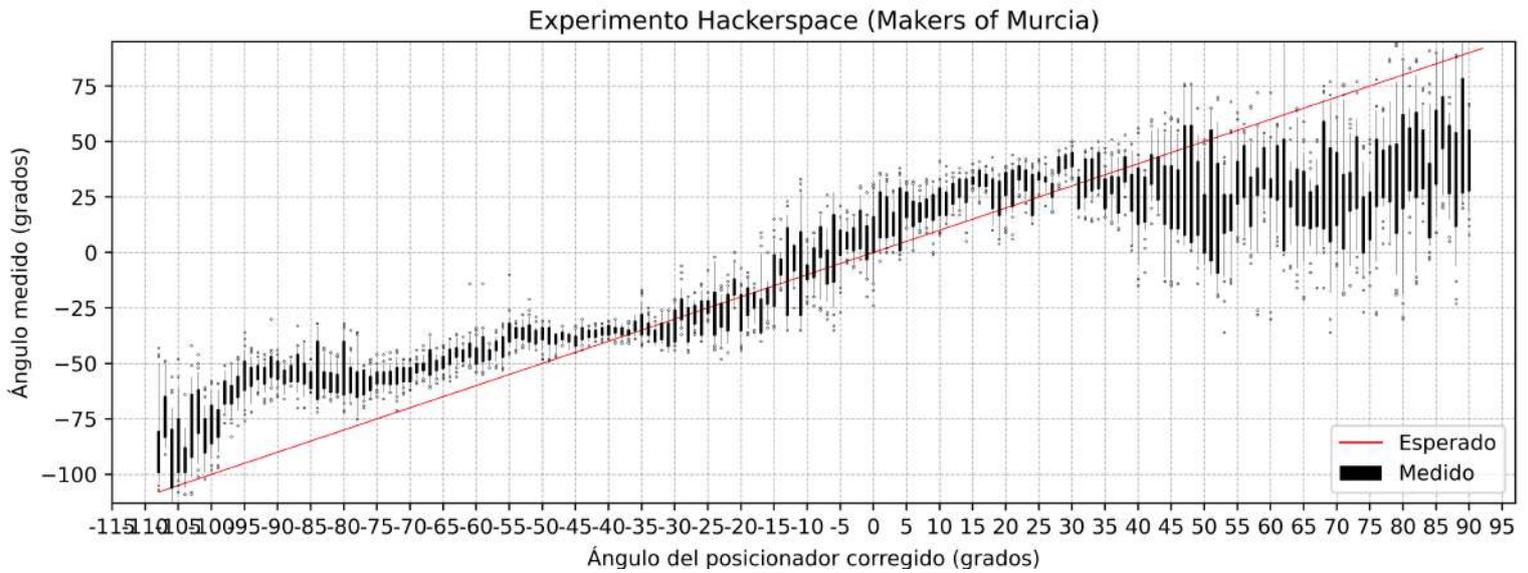
### 5.3.2 Campaña de medidas en el Makers of Murcia



**Figura 5.18:** Foto de el hackerspace de Makers of Murcia

La segunda localización es el Hackerspace de Makers of Murcia, ubicado en el Centro de Empresas e Innovación de Murcia (CEEIM).<sup>11</sup> Es un sótano de hormigón, con el techo a 4m de altura y un tamaño de la habitación de entorno a 15x5m. El edificio está lleno de oficinas, por lo que los canales WiFi de 2.4Ghz están todos en uso, como es de esperar de la mayoría de entornos urbanos. A diferencia del escenario anterior, este hecho no afecta al uso de dispositivos inalámbricos en la ubicación. Es representativo de las zonas comunes de un edificio de oficinas o un almacén, zonas de interior, con paredes próximas, pero que permiten mantener **LOS** entre emisor y receptor. En esta ocasión el posicionador se ubica a 3m de altura en el centro de la pared larga de la habitación, con el esclavo a 3m de distancia en línea recta en el centro de la habitación, a 1.5m de altura sobre el suelo. El punto de acceso **Wi-Fi** de la habitación está ubicado a aproximadamente 70° de la agrupación de antenas.

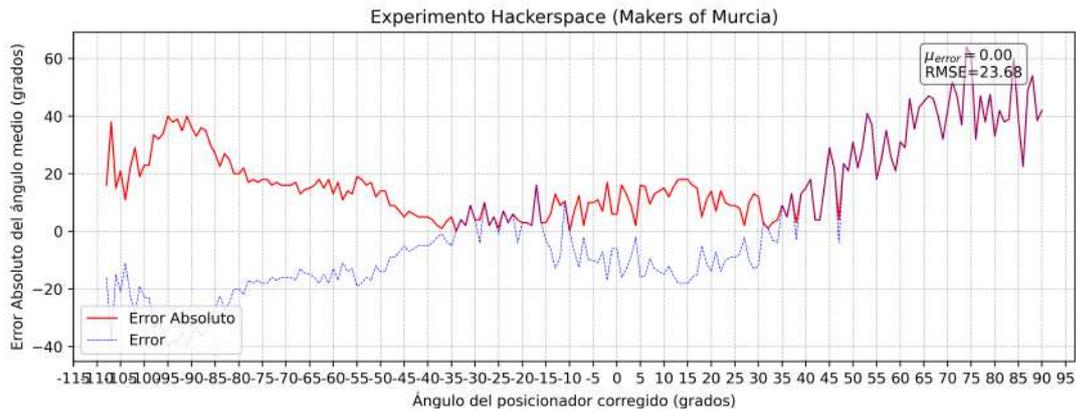
<sup>11</sup>Ubicación del Hackerspace: <https://maps.app.goo.gl/B3tEWTaEsk7mxsFy9>



**Figura 5.19:** Medidas de ángulo en Makers of Murcia

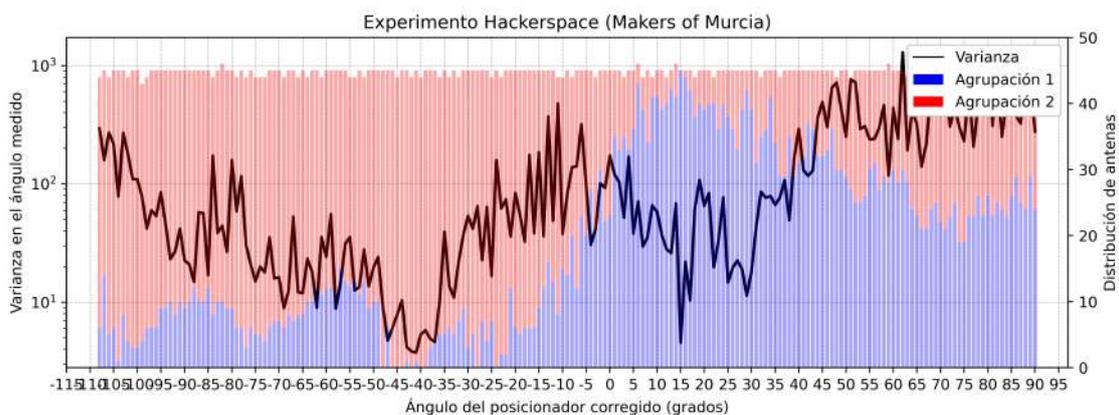
Los resultados de la campaña de medidas de encuentran representados de nuevo en un diagrama de cajas y bigotes, en la Figura 5.19. El procesamiento de los datos es equivalente al realizado en la sección anterior. Además, en esta ocasión, se ha realizado una corrección de 8.6 grados en sentido anti-horario a las etiquetas del posicionador.

En la Figura 5.19, se puede comprobar que en este caso, las medidas no siguen tan cercanamente la tendencia de los valores esperados. De nuevo, a diferencia de las medidas realizadas en el caso ideal, podemos ver claramente que las medidas en los extremos del gráfico están contenidas en un intervalo más grande que en el tramo central, y las medidas vuelven a tener una dispersión asimétrica en el extremo derecho e izquierdo. En el gráfico de la Figura 5.20, podemos ver de nuevo el error en las medidas con respecto al valor esperado. Podemos comprobar que el error aumenta significativamente a partir de los 65°, dirección hacia la que se encuentra esta vez el punto de acceso Wi-Fi de la habitación. El RMSE medio de la campaña de medidas ha sido 23.68 grados.



**Figura 5.20:** Error en las medidas tomadas en Makers of Murcia

En la Figura 5.21 vemos la varianza de las medidas de esta campaña de medidas, de nuevo, en escala logarítmica. En esta ocasión si parece verse el efecto provocado por la combinación de datos de ambas agrupaciones, aquel que veíamos en la Figura 5.11. Además, en este gráfico podemos observar que en esta ocasión el efecto de las interferencias en la comunicación no es tan pronunciado como en la MLP. Sin embargo, en esta ocasión vemos que la selección de la agrupación más cercana no es siempre el ideal. Esto se podría deber al canal inalámbrico con mucha influencia del efecto multi-camino.



**Figura 5.21:** Visualización de la varianza y supervivencia de paquetes en MOM

En este escenario se ha podido comprobar que existe un impacto no mitigado fruto del efecto multi-camino en el sistema de medidas BLE de AoA. Sería necesario un estudio más detallado para la caracterización completa del comportamiento de un sistema de medidas BLE de AoA en estas condiciones.

## 6 Conclusiones y vías futuras

En este trabajo se han recorrido las diferentes técnicas de medida que pueden utilizarse como base para diseñar un sistema de localización y diferentes tecnologías de comunicación inalámbrica disponibles para hacerlo. Este Trabajo Final de Grado (TFG) comenzó con el trabajo realizado para el proyecto Hospital Assets Indoor Location System (HAILS), en Visualtis S.L, y en el mismo se ha comprobado la capacidad de estimación del ángulo de llegada usando el estándar BLE 5. Se ha comprobado la efectividad del Constant Tone Extension (CTE), que puede ser una tecnología habilitante para aumentar la precisión de los sistemas de localización que hacen uso de tecnologías ya desplegadas. Como hemos visto en capítulos anteriores, podría añadirse capacidades extra de localización a un parque de dispositivos ya desplegado solo con una modificación de su firmware, una vez es posible la transmisión del CTE. Los operadores de los Indoor Positioning System (IPS) solo estarían obligados a reemplazar las estaciones base, donde se concentra la complejidad del sistema. Además, podrían usarse también los dispositivos móviles de los usuarios para localizar con alta precisión a personas. Sin embargo, Android no soporta todavía habilitar el CTE y Apple ha elegido añadir radios Ultra Wide Band (UWB) para aumentar la precisión de sus sistemas de localización.

Hemos comprobado que es posible medir el Angle of Arrival (AoA) de una transmisión Bluetooth Low Energy (Version 5) (BLE5) haciendo uso de un único receptor conmutando entre antenas. Texas Instruments (TI) nos provee de una librería de herramientas muy completa en su Real Time Location System (RTLS) Toolbox, que es suficiente para la implementación de sistemas de medida de AoA. Durante la realización de esta investigación, TI decidió dejar de soportar el RTLS Toolbox en el CC2640R2, reservando el soporte a sus microcontroladores de mayor potencia y coste. Esto ha aumentado la complejidad de la implementación, ya que eligió el CC2640R2 por ser un buen balance de coste y funcionalidades anunciadas. Tras tener que lidiar

con las limitaciones que presenta (discutidas en el Capítulo 4) entiendo la decisión de **TI** (pese a lo desafortunada que ha sido para i). Tras este trabajo, sigo considerando el CC2640R2 un buen candidato a dispositivo a localizar, ya que con él somos capaces de transmitir el **Constant Tone Extension (CTE)**.

El desempeño del sistema de medida en la cámara anecoica ha sido muy bueno, con una resolución espacial que podría llegar a ser inferior al paso angular que utilizamos para probarlo. Sin embargo, el desempeño del sistema de medida se degrada considerablemente en los entornos reales probados. Comparando los resultados del Hackerspace con los del Palacio de los deportes, podríamos llegar a la conclusión de que las interferencias reducen el campo de visión del sistema, mientras que los entornos con mucha influencia del efecto multi-camino reducen la repetibilidad de las medidas. Es necesaria más investigación para determinar el origen exacto del comportamiento observado y así poder buscar opciones para mitigarlo en el post procesado.

El hecho de que el **CTE** quede desprotegido de interferencias por el **Cyclic Redundancy Check (CRC)** o el **Message Integrity Codes (MIC)** provoca que no podamos detectarlas. Existe la posibilidad de aplicar técnicas de procesamiento más avanzadas. Se podría aprovechar que los radios de los dispositivos permiten muestrear más de una vez por símbolo, por lo que se podría tomar más de una muestra durante las ventanas de muestreo. Parece previsible que el estándar **BLE** se expanda en esta dirección, dando más libertad en el procesado de la señal recibida. Otra alternativa sería utilizar dos receptores simultáneamente, y de esta manera, en uno podríamos asegurar la integridad del **CTE**, mientras que el otro receptor lo muestra cambiando de antena. Esta solución intermedia permitiría mantener el coste de los receptores bajo, ya que no sería necesario que los receptores fueran coherentes.

Sería interesante seguir la investigación de las capacidades avanzadas de localización que ofrece **BLE5**. Además de las capacidades de medir **AoA/AoD**, se ha introducido otra nueva capacidad en **Bluetooth Low Energy (Version 5) (BLE5)**, la medida del **ToF**. Esta combinación abriría la puerta a métodos de localización híbridos, que con una sola estación base podría medir ángulo y distancia. Eliminando la necesidad de hacer multilateración o triangulación y reduciendo significativamente la complejidad del despliegue de la infraestructura, ya que disminuiría la densidad de sensores necesaria.

Tras comprobar la degradación de la calidad de las medidas en entornos reales, y la congestión inescapable de la banda de 2.4GHz, también puede ser interesante explorar los sistemas de localización usando otras tecnologías. **UWB** destaca sobre el resto para la implementación de sistemas de localización en entornos de interior.

Por último, destacar que ha sido especialmente interesante tener que lidiar con las limitaciones del RFCore. Ha sido necesaria la familiarización con los modos de "prueba" en los módem, especialmente los diseñados para pasar pruebas de certificaciones como RFPHY.TS.p20<sup>1</sup>. Estos modos de prueba dan acceso a de bajo nivel a la radio, que puede ser muy útil para la investigación de este tipo de mecanismos de localización.

---

<sup>1</sup>El Test Suite relevante al comportamiento del PHY de BLE5 se encuentra en:

[https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc\\_id=225827](https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=225827)

---



# Bibliografía

- [1] E. Goldoni, A. Savioli, M. Risi, and P. Gamba, “Experimental analysis of RSSI-based indoor localization with IEEE 802.15.4,” pp. 71–77, May 2010.
- [2] “BOOSTXL-AOA: How to calculate the coordinates.” <https://e2e.ti.com/support/wireless-connectivity/bluetooth-group/bluetooth/f/bluetooth-forum/856500/boostxl-aoa-how-to-calculate-the-coordinates-of-the-node-to-be-located-by-the-aoa>, Nov. 2019.
- [3] A. G. Martinez, M. P. Garcia, and J. L. Gomez-Tornero, “Direct Synthesis of Frequency-Scanned Monopulse Half-Width Microstrip Leaky-Wave Antennas,” in *2020 14th European Conference on Antennas and Propagation (EuCAP)*, (Copenhagen, Denmark), pp. 1–4, IEEE, Mar. 2020.
- [4] “Qorvo - Application Note APS013.” <https://www.qorvo.com/products/d/da008448>.
- [5] M. Woolley, “Bluetooth Direction Finding A Technical Overview.” <https://www.bluetooth.com/bluetooth-resources/bluetooth-direction-finding/>, Oct. 2021.
- [6] “Introduction to Bluetooth® Low Energy.” <https://microchipdeveloper.com/xwiki/bin/view/applications/ble/introduction/>.
- [7] “Bluetooth® Low Energy Channels - Developer Help.” <https://microchipdeveloper.com/xwiki/bin/view/applications/ble/introduction/bluetooth-architecture/bluetooth-controller-layer/bluetooth-link-layer/Channels/>.
- [8] “Online Power Profiler for Bluetooth LE - Nordic DevZone.” <https://devzone.nordicsemi.com/power/w/opp/2/online-power-profiler-for-bluetooth-le>.

- 
- [9] Z. Chen, G. Gokeda, and Y. Yu, *Introduction to Direction-of-Arrival Estimation*. Artech House Signal Processing Library, Boston: Artech House, 2010.
- [10] “Welcome to the Angle of Arrival BoosterPack.” [https://dev.ti.com/tirex/content/tirex-product-tree/cc26xx\\_devtools/.metadata/.tirex/project0\\_boostxl\\_aoa\\_bp/landing\\_page\\_index.h](https://dev.ti.com/tirex/content/tirex-product-tree/cc26xx_devtools/.metadata/.tirex/project0_boostxl_aoa_bp/landing_page_index.h)
- [11] “Application Note Bluetooth® Angle of Arrival (AoA) Antenna Design.” <https://www.ti.com/lit/an/tida029a/tida029a.pdf>, June 2023.
- [12] P. Spachos, I. Papapanagiotou, and K. N. Plataniotis, “Microlocation for Smart Buildings in the Era of the Internet of Things: A Survey of Technologies, Techniques, and Approaches,” *IEEE Signal Processing Magazine*, vol. 35, pp. 140–152, Sept. 2018.
- [13] Y. Guo and R. Ziolkowski, eds., *Smart Leaky-Wave Antennas for Iridescent IoT Wireless Networks*. Wiley, 2022.
- [14] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, “BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities,” *IEEE Internet of Things Journal*, vol. 5, pp. 811–828, Apr. 2018.
- [15] “Bluetooth Core Specification v4.2.” <https://www.bluetooth.com/specifications/specs/core-specification-4-2/>.
- [16] “Bluetooth Core Specification v5.4.” <https://www.bluetooth.com/specifications/specs/core-specification-5-4/>, Jan. 2023.
- [17] G. Pau, F. Arena, Y. E. Gebremariam, and I. You, “Bluetooth 5.1: An Analysis of Direction Finding Capability for High-Precision Location Services,” *Sensors (Basel, Switzerland)*, vol. 21, p. 3589, May 2021.
- [18] M. Poveda-García, D. Cañete-Rebenaque, and J. L. Gómez-Tornero, “Frequency-Scanned Monopulse Pattern Synthesis Using Leaky-Wave Antennas for Enhanced Power-Based Direction-of-Arrival Estimation,” *IEEE Transactions on Antennas and Propagation*, vol. 67, pp. 7071–7086, Nov. 2019.
- [19] M. Poveda-García, J. Oliva-Sanchez, R. Sanchez-Iborra, D. Rebenaque, and J. Gómez Tornero, “Dynamic Wireless Power Transfer for Cost-Effective Wireless Sensor Networks Using Frequency-Scanned Beaming,” *IEEE Access*, vol. PP, pp. 1–1, Jan. 2019.
-

- 
- [20] A. Gil Martínez, M. Poveda-García, J. A. Lopez Pastor, J. Sanchez-Aarnoutse, and J. Gómez Tornero, “Wi-Fi Direction Finding With Frequency-Scanned Antenna and Channel-Hopping Scheme,” *IEEE Sensors Journal*, vol. PP, pp. 1–1, Oct. 2021.
- [21] A. Gil Martínez, M. Poveda-García, J. García Fernández, M. Campo-Valera, D. Rebenaque, and J. Gómez Tornero, “Direction Finding of RFID tags in UHF band using a Passive Beam-Scanning Leaky-Wave Antenna,” *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 1–1, Jan. 2022.
- [22] J. A. Lopez Pastor, M. Poveda-García, A. Gil Martínez, D. Rebenaque, and J. Gómez Tornero, “Two-dimensional localization system for mobile IoT devices using a single Wi-Fi access point with a passive frequency-scanned antenna,” *IEEE Internet of Things Journal*, vol. PP, pp. 1–1, Sept. 2023.
- [23] A. Gil Martínez, M. Poveda-García, D. Rebenaque, and J. Gómez Tornero, “Metasurface Antenna for Fast Frequency Scanning With Application to Conical Direction Finding,” *IEEE Antennas and Wireless Propagation Letters*, vol. PP, pp. 1–5, July 2023.
- [24] A. Gil Martínez, J. A. Lopez Pastor, M. Poveda-García, A. Algaba-Brazalez, D. Rebenaque, and J. Gómez Tornero, “Monopulse Leaky Wave Antennas for RSSI-Based Direction Finding in Wireless Local Area Networks,” *IEEE Transactions on Antennas and Propagation*, vol. PP, pp. 1–1, Nov. 2023.
- [25] M. Campo-Valera, M. Poveda-García, J. García Fernández, A. Gil Martínez, D. Rebenaque, and J. Gómez Tornero, “Laboratory to Develop a Practical Hand-Made Monopulse Antenna for RFID Localization Systems,” *IEEE Access*, vol. PP, pp. 1–1, Jan. 2022.
- [26] J. Gómez Tornero, A. Gil Martínez, M. Poveda-García, and D. Rebenaque, “ARIEL: Passive Beam-Scanning Antenna terminal for Iridescent and Efficient LEO Satellite Connectivity,” *IEEE Antennas and Wireless Propagation Letters*, vol. 21, pp. 1–5, Nov. 2022.
- [27] D. Zelenchuk, A. Martínez Ros, T. Zvolensky, J. Gómez Tornero, G. Goussetis, N. Buchanan, D. Linton, and V. Fusco, “W-Band Planar Wide-Angle Scanning Antenna Architecture,” *Journal of Infrared, Millimeter, and Terahertz Waves*, vol. 34, pp. 127–139, Feb. 2013.
-

- 
- [28] L. F. Herrán, A. Algaba Brazalez, and E. Rajo-Iglesias, “Ka-band planar slotted waveguide array based on groove gap waveguide technology with a glide-symmetric holey metasurface,” *Scientific Reports*, vol. 11, p. 8697, Apr. 2021.
- [29] M. Poveda-García, A. Gomez-Alcaraz, D. Rebenaque, A. Martinez-Sala, and J. Gómez Tornero, “RSSI-Based Direction-of-Departure Estimation in Bluetooth Low Energy Using an Array of Frequency-Steered Leaky-Wave Antennas,” *IEEE Access*, vol. PP, pp. 1–1, Jan. 2020.
- [30] M. Poveda-García, A. Gil Martínez, and J. Gómez Tornero, “Frequency-Scanned Focused Leaky-Wave Antennas for Direction-of-Arrival Detection in Proximity BLE Sensing Applications,” pp. 1–4, Mar. 2020.
- [31] M. Poveda-García, E. Andreu-Garcia, J. García Fernández, D. Rebenaque, and J. Gómez Tornero, “Frequency-Scanned Leaky-Wave Antenna Topologies for Two-dimensional Direction of Arrival Estimation in IoT Wireless Networks,” pp. 1–5, Mar. 2021.
- [32] A. J. Martinez-Ros, J. L. Gomez-Tornero, and G. Goussetis, “Planar Leaky-Wave Antenna With Flexible Control of the Complex Propagation Constant,” *IEEE Transactions on Antennas and Propagation*, vol. 60, pp. 1625–1630, Mar. 2012.
- [33] “Bluetooth® Direction Finding Fundamentals (UG103.18).” <https://www.silabs.com/documents/public/user-guides/ug103-18-bluetooth-direction-finding-fundamentals.pdf>.
- [34] D. Giovanelli and E. Farella, “RSSI or Time-of-flight for Bluetooth Low Energy based localization? An experimental evaluation,” in *2018 11th IFIP Wireless and Mobile Networking Conference (WMNC)*, (Prague), pp. 1–8, IEEE, Sept. 2018.
- [35] “Since one satellite can see half of the earth, why do we need more than two satellites in a given network?.” <https://wtamu.edu/~cbaird/sq/2013/05/10/since-one-satellite-can-see-half-of-the-earth-why-do-we-need-more-than-two-satellites-in-a-given-network/>.
- [36] E. Dominguez, A. Pousinho, P. Boto, D. Gomez-Casco, S. Locubiche-Serra, G. Seco-Granados, J. A. Lopez-Salcedo, H. Fagner, F. Zangerl, O. Peña, and D. Jimenez-Baños, “Performance Evaluation of High Sensitivity GNSS Techniques in Indoor, Urban and
-

- Space Environments,” in *29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, (Portland, Oregon), pp. 373–393, Nov. 2016.
- [37] “WiGLE: Wireless Network Mapping.” <https://wiggles.net/>.
- [38] D. Schepers and A. Ranganathan, “Privacy-Preserving Positioning in Wi-Fi Fine Timing Measurement,” *Proceedings on Privacy Enhancing Technologies*, vol. 2022, pp. 325–343, Apr. 2022.
- [39] “2023 Bluetooth® Market Update.” <https://www.bluetooth.com/2023-market-update/>.
- [40] “Bluetooth Core Specification v5.1.” <https://www.bluetooth.com/specifications/specs/core-specification-5-1/>, Jan. 2023.
- [41] “What is Bluetooth 5 and When do I Use it?.” <https://www.ti.com/video/single.html>.
- [42] S. A. Schelkunoff, “A mathematical theory of linear arrays,” *The Bell System Technical Journal*, vol. 22, pp. 80–107, Jan. 1943.
- [43] T. Instruments, “Datasheet CC2640R2F (SWRS201B).” <https://www.ti.com/lit/ds/swrs201b/swrs201b.pdf?ts=1702146774896>.
- [44] “Technical Reference Manual: CC13x0, CC26x0 SimpleLink™ Wireless MCU (SWCU117I).” <https://www.ti.com/lit/ug/swcu117i/swcu117i.pdf>.
- [45] “Speeding up CRC calculations for Bluetooth Low Energy - Great Scott Gadgets.” <https://greatscottgadgets.com/2013/05-07-speeding-up-crc-calculations-for-bluetooth-low-energy/>.
- [46] S. Abielmona, H. V. Nguyen, and C. Caloz, “Analog Direction of Arrival Estimation Using an Electronically-Scanned CRLH Leaky-Wave Antenna,” *IEEE Transactions on Antennas and Propagation*, vol. 59, pp. 1408–1412, Apr. 2011.
- [47] A. Algaba-Brazalez and E. Rajo-Iglesias, “Design of a Butler matrix at 60GHz in inverted microstrip gap waveguide technology,” in *2015 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting*, pp. 2125–2126, July 2015.
-

- 
- [48] A. Algaba-Brazález, H. Wang, P. Castillo-Tapia, L. Manholm, M. Johansson, and O. Quevedo-Teruel, “Flexible 6G antenna systems based on innovative lenses combined with array antennas,” in *2023 17th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, Mar. 2023.
- [49] R. Archacki, K. Hogan, M. Fraser, and A. Georgi, “UNLOCKING VALUE WITH LOCATION INTELLIGENCE.” <https://web-assets.bcg.com/52/4a/f7d8a23a47d597f69e3b17b031d7/bcg-unlocking-value-with-location-intelligence-feb-2021.pdf>.
- [50] “Automotive Bluetooth® Low Energy CarAccess (TIDUE70A).” <https://www.ti.com/lit/ug/tidue70a/tidue70a.pdf>.
- [51] “Bluetooth Angle Estimation for Real-Time Locationing.” <https://www.silabs.com/whitepapers/bluetooth-angle-estimation-for-real-time-locationing>.
- [52] “Bluetooth® 5, Refined for the IoT.” <https://www.silabs.com/whitepapers/bluetooth-5-refined-for-the-iot>.
- [53] “From cable replacement to the IoT Bluetooth 5.1.” <http://www.rohde-schwarz.com/appnote/1MA108>, June 2019.
- [54] P. Castillo-Tapia, O. Zetterstrom, A. Algaba-Brazález, L. Manholm, M. Johansson, N. J. G. Fonseca, and O. Quevedo-Teruel, “Two-Dimensional Beam Steering Using a Stacked Modulated Geodesic Luneburg Lens Array Antenna for 5G and Beyond,” *IEEE Transactions on Antennas and Propagation*, vol. 71, pp. 487–496, Jan. 2023.
- [55] K. Cengiz, “Comprehensive Analysis on Least-Squares Lateration for Indoor Positioning Systems,” *IEEE Internet of Things Journal*, vol. 8, pp. 2842–2856, Feb. 2021.
- [56] M. Cominelli, P. Patras, and F. Gringoli, “Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System,” in *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization, WiNTECH '19*, (New York, NY, USA), pp. 13–20, Association for Computing Machinery, Oct. 2019.
-

- 
- [57] A. Comuniello, A. De Angelis, A. Moschitta, and P. Carbone, “Using Bluetooth Low Energy Technology to Perform ToF-Based Positioning,” *Electronics*, vol. 11, p. 111, Dec. 2021.
- [58] “Constant Tone Extension Service.” <https://www.bluetooth.com/specifications/specs/constant-tone-extension-service-1-0/>, Jan. 2021.
- [59] M. K. Emará, D. J. King, H. V. Nguyen, S. Abielmona, and S. Gupta, “Millimeter-Wave Slot Array Antenna Front-End for Amplitude-Only Direction Finding,” *IEEE Transactions on Antennas and Propagation*, vol. 68, pp. 5365–5374, July 2020.
- [60] M. Englund, “Evaluation of Angle of Arrival based positioning for keyless entry access control.” <https://www.diva-portal.org/smash/get/diva2:1317231/FULLTEXT01.pdf>.
- [61] “An Experimental Study on Direction Finding of Bluetooth 5.1: Indoor vs Outdoor.” <https://ieeexplore.ieee.org/abstract/document/9771930/>.
- [62] A. Foroozesh, R. Paknys, D. R. Jackson, and J.-J. Laurin, “Beam Focusing Using Backward-Radiating Waves on Conformal Leaky-Wave Antennas Based on a Metal Strip Grating,” *IEEE Transactions on Antennas and Propagation*, vol. 63, pp. 4667–4677, Nov. 2015.
- [63] M. Garcia-Vigueras, J. L. Gomez-Tornero, G. Goussetis, A. R. Weily, and Y. J. Guo, “Efficient Synthesis of 1-D Fabry–Perot Antennas With Low Sidelobe Levels,” *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 869–872, 2012.
- [64] M. Garcia-Vigueras, J. L. Gomez-Tornero, G. Goussetis, J. S. Gomez-Diaz, and A. Alvarez-Melcon, “A Modified Pole-Zero Technique for the Synthesis of Waveguide Leaky-Wave Antennas Loaded With Dipole-Based FSS,” *IEEE Transactions on Antennas and Propagation*, vol. 58, pp. 1971–1979, June 2010.
- [65] A. F. García, C. Gómez, T. Sánchez, A. D. Redondo, L. Betancur, and R. C. Hincapié, “Algoritmos de Radiolocalización basados en ToA, TDoA y AoA,” *Ingeniería y Región*, vol. 14, pp. 9–22, 2015.
-

- 
- [66] A. Gil Martínez, M. Poveda-García, D. Rebenaque, and J. Gómez Tornero, “Frequency-scanned monopulse antenna for RSSI-based direction finding of UHF RFID tags,” *IEEE Antennas and Wireless Propagation Letters*, vol. PP, pp. 1–1, Oct. 2021.
- [67] L. Goldstone and A. Oliner, “Leaky-wave antennas I: Rectangular waveguides,” *IRE Transactions on Antennas and Propagation*, vol. 7, pp. 307–319, Oct. 1959.
- [68] J. L. Gomez-Tornero, “Analysis and Design of Conformal Tapered Leaky-Wave Antennas,” *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 1068–1071, 2011.
- [69] J. Gómez-Tornero, *Antenna and Array Technologies for Future Wireless Ecosystems*. Wiley, 2022.
- [70] J. L. Gomez-Tornero, G. Goussetis, A. P. Feresidis, and A. A. Melcon, “Control of Leaky-Mode Propagation and Radiation Properties in Hybrid Dielectric-Waveguide Printed-Circuit Technology: Experimental Results,” *IEEE Transactions on Antennas and Propagation*, vol. 54, pp. 3383–3390, Nov. 2006.
- [71] J. Gomez-Tornero, D. Canete-Rebenaque, and A. Alvarez-Melcon, “Printed-circuit leaky-wave antenna with pointing and illumination flexibility,” *IEEE Microwave and Wireless Components Letters*, vol. 15, pp. 536–538, Aug. 2005.
- [72] J. L. Gómez-Tornero, A. Martínez-Ros, A. Álvarez-Melcón, F. Mesa, and F. Medina, “Substrate integrated waveguide leaky-wave antenna with reduced beam squint,” in *2013 European Microwave Conference*, pp. 491–494, Oct. 2013.
- [73] J. Gómez Tornero, D. Rebenaque, J. A. Lopez Pastor, and A. Martinez-Salas, “Hybrid Analog-Digital Processing System for Amplitude-Monopulse RSSI-based MiMo WiFi Direction-of-Arrival Estimation,” *IEEE Journal of Selected Topics in Signal Processing*, vol. PP, pp. 1–1, Apr. 2018.
- [74] J. Gómez Tornero, D. Rebenaque, and A. Melcón, “Microstrip Leaky-Wave Antenna With Control of Leakage Rate and Only One Main Beam in the Azimuthal Plane,” *Antennas and Propagation, IEEE Transactions on*, vol. 56, pp. 335–344, Mar. 2008.
-

- 
- [75] H. Guerboukha, R. Shrestha, J. Neronha, Z. Fang, and D. Mittleman, “Conformal leaky-wave antennas for wireless terahertz communications,” *Communications Engineering*, vol. 2, Apr. 2023.
- [76] R. Guzmán, A. Martínez-Sala, J. Gómez Tornero, and J. García-Haro, “Integration of Directional Antennas in an RSS Fingerprinting-Based Indoor Localization System,” *Sensors*, vol. 16, p. 4, Dec. 2015.
- [77] Z. Hajiakhondi-Meybodi, M. Salimibeni, K. N. Plataniotis, and A. Mohammadi, “Bluetooth Low Energy-based Angle of Arrival Estimation via Switch Antenna Array for Indoor Localization,” in *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*, pp. 1–6, July 2020.
- [78] K.-Y. Kim, E.-K. Kang, J.-W. Kim, and K.-W. Ra, “A Study and Design of Beam Scanning Array Antenna using IR-UWB,” *Journal of the Institute of Electronics and Information Engineers*, vol. 51, Mar. 2014.
- [79] H. Lee and D.-H. Kwon, “Conformal Metasurfaces on a Grounded Dielectric Substrate for Leaky-Wave Antennas,” in *2022 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (AP-S/URSI)*, pp. 451–452, July 2022.
- [80] Y. Lichen, *Bluetooth Direction Finding*. PhD thesis, Delft University of Technology, Delft, Sept. 2018.
- [81] J. A. Lopez Pastor, A. Gomez-Alcaraz, D. Rebenaque, A. Martínez-Sala, and J. Gómez Tornero, “Near-Field Monopulse DoA Estimation for Angle-Sensitive Proximity Wi-Fi Readers,” *IEEE Access*, vol. PP, pp. 1–1, June 2019.
- [82] J. A. Lopez Pastor, P. Arques, J. Franco-Penaranda, A.-J. Garcia-Sanchez, and J. Gómez Tornero, “Wi-Fi RTT-based active monopulse RADAR for single access point localization,” *IEEE Access*, vol. PP, pp. 1–1, Feb. 2021.
- [83] Y. Ma, X. Shi, J. Wang, Y. Zhang, F. Sun, and F. Wu, “Millimeter-Wave Conformal Directional Leaky-Wave Antenna Based on Substrate-Integrated Waveguide,” *Electronics*, vol. 12, p. 3111, July 2023.
-

- 
- [84] A. J. Martínez-Ros, J. L. Gómez-Tornero, and G. Goussetis, “Broadside radiation from radial arrays of substrate integrated leaky-wave antennas,” in *2012 6th European Conference on Antennas and Propagation (EUCAP)*, pp. 252–254, Mar. 2012.
- [85] A. J. Martínez-Ros, J. L. Gómez-Tornero, and G. Goussetis, “Conformal Tapered Substrate Integrated Waveguide Leaky-Wave Antenna,” *IEEE Transactions on Antennas and Propagation*, vol. 62, pp. 5983–5991, Dec. 2014.
- [86] A. J. Martínez-Ros, J. L. Gómez-Tornero, and G. Goussetis, “Frequency scanning leaky wave antenna for positioning and identification of RFID tags,” in *2011 IEEE International Conference on RFID-Technologies and Applications*, pp. 451–456, Sept. 2011.
- [87] A. J. Martínez-Ros, J. L. Gómez-Tornero, and G. Goussetis, “Multifunctional Angular Bandpass Filter SIW Leaky-Wave Antenna,” *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 936–939, 2017.
- [88] “nWP036 - Direction Finding.” [https://infocenter.nordicsemi.com/pdf/nwp\\_036.pdf](https://infocenter.nordicsemi.com/pdf/nwp_036.pdf), Aug. 2020.
- [89] A. A. Oliner, “Leakage from higher modes on microstrip line with application to antennas,” *Radio Science*, vol. 22, pp. 907–912, Nov. 1987.
- [90] A. Oliner and K. Lee, “Microstrip leaky wave strip antennas,” *1986 Antennas and Propagation Society International Symposium*, vol. 24, pp. 443–446, 1986.
- [91] H. Paaso, N. Gulati, D. Patron, A. Hakkarainen, J. Werner, K. R. Dandekar, M. Valkama, and A. Mämmelä, “DoA Estimation Using Compact CRLH Leaky-Wave Antennas: Novel Algorithms and Measured Performance,” *IEEE Transactions on Antennas and Propagation*, vol. 65, pp. 4836–4849, Sept. 2017.
- [92] Y. Pan, T. Ao, and Y. Dong, “Fully Planar Single/Fixed-Beam Ultrawideband Leaky-Wave Antenna Based on Leaky Grounded Coplanar Waveguide,” *IEEE Antennas and Wireless Propagation Letters*, vol. 22, pp. 606–610, Mar. 2023.
- [93] F. Pizarro Torres, D. Ramírez-Gil, A. Algaba-Brazalez, L. Herrán-Ontanón, and E. Rajo-Iglesias, “Comparison study of  $4 \times 4$  Butler matrices in microstrip technologies for Ka-
-



- 
- [103] M. L. Sollie, K. Gryte, T. H. Bryne, and T. A. Johansen, “Outdoor Navigation Using Bluetooth Angle-of-Arrival Measurements,” *IEEE Access*, vol. 10, pp. 88012–88033, 2022.
- [104] J. Tornero and A. Melcon, “Nonorthogonality relations between complex hybrid modes: An application for the leaky-wave analysis of laterally shielded top-open planar transmission lines,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 52, pp. 760–767, Mar. 2004.
- [105] “The Trilateration algorithm..” [https://www.researchgate.net/figure/The-Trilateration-algorithm\\_fig4\\_224144937](https://www.researchgate.net/figure/The-Trilateration-algorithm_fig4_224144937).
- [106] L. Urquhart, “An Analysis of Multi-Frequency Carrier Phase Linear Combinations for GNSS,” Jan. 2008.
- [107] F. V. Vidarsson, O. Zetterstrom, A. Algaba-Brazález, N. J. G. Fonseca, M. Johansson, L. Manholm, and O. Quevedo-Teruel, “Conformal Parallel Plate Waveguide Polarizer Integrated in a Geodesic Lens Antenna,” *IEEE Transactions on Antennas and Propagation*, vol. 70, pp. 10327–10337, Nov. 2022.
- [108] W. Wang, D. Marelli, and M. Fu, “Fingerprinting-Based Indoor Localization Using Interpolated Preprocessed CSI Phases and Bayesian Tracking,” *Sensors*, vol. 20, p. 2854, Jan. 2020.
- [109] L. Wang, J. L. Gómez-Tornero, E. Rajo-Iglesias, and O. Quevedo-Teruel, “Low-Dispersive Leaky-Wave Antenna Integrated in Groove Gap Waveguide Technology,” *IEEE Transactions on Antennas and Propagation*, vol. 66, pp. 5727–5736, Nov. 2018.
- [110] L. Wang, J. L. Gómez-Tornero, and O. Quevedo-Teruel, “Substrate Integrated Waveguide Leaky-Wave Antenna With Wide Bandwidth via Prism Coupling,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, pp. 3110–3118, June 2018.
- [111] F. Xu and K. Wu, “Guided-wave and leakage characteristics of substrate integrated waveguide,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, pp. 66–73, Jan. 2005.
-

- 
- [112] H.-Y. Yen, Z.-T. Tsai, Y.-C. Chen, L.-H. Shen, C.-J. Chiu, and K.-T. Feng, “I/Q Density-based Angle of Arrival Estimation for Bluetooth Indoor Positioning Systems,” in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–5, Apr. 2021.
- [113] I. Yoo and D. R. Smith, “Design of Conformal Array of Rectangular Waveguide-Fed Metasurfaces,” *IEEE Transactions on Antennas and Propagation*, vol. 70, pp. 6060–6065, July 2022.
- [114] O. Zetterstrom, P. Arnberg, F. V. Vidarsson, A. Algaba-Brazález, L. Manholm, M. Johansson, and O. Quevedo-Teruel, “V-Band Geodesic Generalized Luneburg Lens Antenna With High Beam Crossover Gain,” *IEEE Transactions on Antennas and Propagation*, vol. 71, pp. 7591–7596, Sept. 2023.
- [115] H.-J. Zhao, H. Chu, X. Zhu, and Y.-X. Guo, “A 1-D Electronic Beam-Scanning Monopulse Antenna Array Based on a Compact Stripline Phase-Shifter,” *IEEE Antennas and Wireless Propagation Letters*, vol. 19, pp. 2477–2481, Dec. 2020.
- [116] D. Zheng, G.-B. Wu, D. Wang, K. F. Chan, K. Wu, and C. H. Chan, “Planar Leaky-Wave Antenna Featuring Wideband Fixed-Beam Radiation and Tailorable Directional Angle for Millimeter-Wave Applications,” *IEEE Transactions on Antennas and Propagation*, vol. 71, pp. 3238–3250, Apr. 2023.
- [117] I. Ziskind and M. Wax, “Maximum Likelihood Localization of Multiple Sources by Alternating Projection,” *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 36, pp. 1553–1560, Nov. 1988.
-



# Lista de Acrónimos y Abreviaturas

## A

**AoA** Angle of Arrival. [vii](#), [ix](#), [2](#), [3](#), [5](#), [11](#), [12](#), [15](#), [16](#), [20](#), [22](#), [23](#), [25](#), [27](#), [29](#), [31](#), [32](#), [34](#)–[38](#), [43](#)–[45](#), [47](#)–[49](#), [51](#), [54](#)–[56](#)

**AoD** Angle of Departure. [2](#), [16](#), [20](#), [22](#), [31](#), [56](#)

**AWGN** Additive White Gaussian Noise. [24](#)

## B

**BDS** BeiDou Navigation Satellite System. [13](#),

**BLE** Bluetooth Low Energy. [ix](#), [1](#)–[3](#), [10](#)–[13](#), [15](#)–[23](#), [29](#), [31](#), [32](#), [35](#), [37](#)–[41](#), [43](#), [44](#), [49](#), [51](#), [54](#), [56](#), [76](#)

**BLE5** Bluetooth Low Energy (Version 5). [1](#)–[3](#), [15](#), [16](#), [29](#), [37](#), [38](#), [55](#), [56](#)

**BR** Bluetooth Basic Rate. [15](#)

**BT** Bluetooth. [15](#), [19](#), [29](#), [37](#)

## C

**COTS** Commercial Off-The-Shelf. [2](#)

**CP** [CTE](#) Presence bit. [31](#)

**CPE** Command and Packet Engine. [31](#)

**CRC** Cyclic Redundancy Check. [21](#), [22](#), [31](#), [41](#), [56](#)

**CTE** Constant Tone Extension. [ix](#), [2](#), [15](#), [21](#), [22](#), [27](#), [29](#), [31–34](#), [37](#), [38](#), [40–42](#), [44](#), [47](#), [49](#), [55](#),  
[56](#), [73](#)

## D

**DoA** Direction of arrival. [23](#)

## E

**ECC** Error Correcting Code. [18](#), [31](#)

**ESPRIT** Estimation of Signal Parameters via Rotational Invariance Technique. [12](#)

## F

**FOSC** Free Open Source Club. [v](#)

## G

**GEAT** Grupo de Electromagnetismo Aplicado a las Telecomunicaciones. [1](#), [3](#)

**GFSK** Gaussian Frequency Shift Keying. [18](#), [21](#), [31](#), [41](#)

**GLONASS** Global'naya Navigatsionnaya Sputnikovaya Sistema. [13](#),

**GNSS** Global Navigation Satellite System. [vii](#), [2](#), [8](#), [13](#), [14](#)

**GPS** Global Positioning System. [1](#), [8](#), [13](#)

## H

**HAILS** Hospital Assets Indoor Location System. [55](#),

---

**I**

**IEEE** Institute of Electrical and Electronics Engineers.

**IMU** Inertial Measurement Unit.

**IoT** Internet of Things. [1](#), [15](#)

**IPS** Indoor Positioning System. [8](#), [9](#), [12](#), [13](#), [15](#), [29](#), [55](#)

**IQ** Complex Sampling. [37](#), [39](#), [40](#)

**IRNSS** Indian Regional Navigation Satellite System. [13](#),

**ISM** Industrial, Scientific, and Medical. [18](#), [39](#), [48](#)

**K**

**KPI** Key Performance Indicator.

**L**

**LE** Bluetooth Low Energy Controller. [15](#)

**LFSR** Linear Feedback Shift Register. [22](#)

**LOS** Line of Sight. [5](#), [8](#), [52](#)

**LWA** Leaky Wave Antenna. [ix](#), [1–3](#), [8](#)

**M**

**MIC** Message Integrity Codes. [56](#),

**MIMO** Multiple-Input and Multiple-Output. [14](#)

**MLAT** Multilateración. [ix](#), [6](#), [8](#)

---

**MLP** Murcia Lan Party. [v](#), [48](#), [54](#)

**MOM** Makers of Murcia. [v](#)

**MSPS** Mega Sample Per Second. [39](#), [40](#)

**MUSIC** Multiple Signal Classifier. [12](#)

## P

**PCB** Printed Circuit Board. [39](#)

**PDoA** Phase Difference of Arrival. [14](#)

**PHY** [BLE](#) Physical Layer. [18](#), [21](#), [31](#), [37](#)

## Q

**QZSS** Quasi-Zenith Satellite System. [13](#),

## R

**RCE** Radio Club Errante. [v](#), [39](#)

**RDF** Radio Direction Finding. [7](#), [12](#), [23](#), [26](#)

**RFU** Reserved for Future Use. [31](#)

**RSS** Recived Signal Strength. [3](#), [6](#)

**RSSI** Received Signal Strength Indicator. [1](#), [6](#)

**RTLS** Real Time Location System. [vii](#), [35](#), [37](#), [44](#), [55](#)

## S

**SAA** Switched Antenna Array. [20](#), [23](#), [26](#)

---

**SDK** Software Development Kit. 35

**SDR** Software Defined Radio. 39, 40

**SIC** Successive Interference Cancellation. 26

**SIG** Special Interest Group. 15, 37, 38

## T

**TDoA** Time Difference of Arrival. ix, 9, 14

**TFG** Trabajo Final de Grado. 16, 55

**TI** Texas Instruments. vii, 29, 31, 34, 35, 37, 44, 55, 56

**TLA** Three Letter Acronym. 77

**TLP** Teleco Lan Party. v

**TMT** Too Many Three Letter Acronyms (TLAs).

**ToA** Time of Arrival. 8, 9

**ToF** Time of Flight. 3, 10, 56

**TS** Test Suite. 37

**TWR** Two Way Ranging. 10, 14

## U

**ULA** Uniform Linear Array. ix, 24–26, 33

**UPCT** Universidad Politécnica de Cartagena. 43,

**UWB** Ultra Wide Band. vii, 10, 14, 55, 57

---

**W**

**WFPS** Wi-Fi positioning system. [14](#)

**Wi-Fi** IEEE 802.11. [14](#), [48](#), [52](#), [53](#)

**WiFi-FTM** WiFi Fine Timing Measurement. [14](#)

**WLAN** Wireless Local Area Networks. [vii](#), [13](#), [14](#)

**WMAN** Wireless Metropolitan Area Networks. [13](#)

**WPAN** Wireless Personal Area Networks. [13](#), [15](#)

**WWAN** Wireless Wide Area Networks. [13](#)

---