Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

Maestría en Diseño Electrónico

Analysis of Indoor Localization Methods with Bluetooth Low Energy

TRABAJO RECEPCIONAL que para obtener el **GRADO** de **MAESTRO EN DISEÑO ELECTRÓNICO**

Presenta: **RICARDO ZAMORA DÁVALOS**

Director **JORGE ARTURO PARDIÑAS MIR**

Tlaquepaque, Jalisco. 24 de junio de 2025.

Acknowledgments

First and foremost, I thank God for granting me the strength, clarity, and perseverance to complete this academic journey. His presence has been my foundation in times of challenge and uncertainty.

I dedicate this work to my parents, whose love, sacrifices, and unwavering support have made this achievement possible. Their example continues to guide me every step of the way.

To Dr. Jorge Pardiñas, my advisor for this master’s degree project, thank you for your valuable guidance, constant support, and for always encouraging me to strive for deeper understanding and technical excellence.

I am also grateful to ITESO for providing not only a solid academic formation, but also for inspiring in me a commitment to work toward a more just and humane society through engineering.

To my colleagues and leaders at NXP Semiconductors, thank you for your mentorship, your technical insight, and for creating an environment where innovation and collaboration flourish. Your support was essential throughout this process.

To all those who have walked alongside me—family, friends, professors, and peers—this work is for all of you.

Summary

This case study presents a technical analysis of indoor distance estimation using Bluetooth Low Energy (BLE), with a particular focus on its integration into embedded systems. The study evaluates four key methodologies—Received Signal Strength Indication (RSSI), Time of Flight (ToF), Angle of Arrival (AoA), and Channel Sounding (CS)—highlighting their theoretical underpinnings, implementation characteristics, and practical performance. A primary contribution of this work lies in its comparative framework, which helps identify the most suitable BLE-based method depending on system requirements such as accuracy, power consumption, and hardware complexity.

The study includes experimental implementations of RSSI and ToF using NXP's MCX W71x platform, allowing for practical observations of BLE behavior under real-world conditions. Limitations in hardware accessibility restricted direct experimentation with AoA and CS; however, their inclusion is supported through publicly available demonstrations and validated references. These insights enable a balanced discussion between theoretical potential and real-world feasibility.

The main contribution of this work is the structured comparison and contextual application of BLE-based distance estimation techniques. This allows system designers to make informed decisions aligned with application constraints and performance goals. The study also serves as a technical guide for those developing BLE localization systems in domains such as smart buildings, asset tracking, and IoT deployments.

Overall, this work bridges the gap between theoretical methodologies and practical implementation, providing a foundation for future enhancements and hybrid approaches in BLE-based indoor localization systems.

Content

Introduction

Indoor localization has emerged as a critical enabling technology for a wide range of modern applications, including smart buildings, asset tracking, context-aware services, industrial automation, and healthcare monitoring. As society becomes increasingly interconnected, the need to locate objects, devices, and people within enclosed spaces—where satellite-based positioning systems such as GPS are ineffective—has led to the development of diverse methods and systems. Among these, Bluetooth Low Energy (BLE) has gained prominence due to its widespread adoption, low power requirements, and growing support for localization features in modern embedded platforms.

The principal goal of this study is to investigate and compare different BLE-based distance estimation methods for indoor localization. Four main techniques are considered: Received Signal Strength Indication (RSSI), Time of Flight (ToF), Angle of Arrival (AoA), and Channel Sounding (CS). Each method is analyzed with regard to its theoretical basis, technical implementation, and practical performance in embedded systems.

This document is structured into six chapters, each building upon the previous to provide a comprehensive and technical exploration of BLE-based positioning.

Chapter 1, titled "**Overview of Localization Methods Based on Distance Determination**," introduces the foundational concepts of indoor localization. It discusses key principles such as trilateration and triangulation, the role of anchors and tags, and the physical and technological constraints that affect positioning accuracy. The chapter also defines essential performance metrics—accuracy, precision, and resolution—which serve as evaluation criteria throughout the rest of the study.

Chapter 2, "**Basic Methodologies for Distance Estimation**," delves deeper into the physical principles that underlie distance measurement techniques in wireless systems. It classifies these methods into range-based (e.g., RSSI, ToF, AoA) and range-free (e.g., fingerprinting), and provides detailed technical explanations of how signal strength, propagation delay, and angle of arrival can be used to infer position. This chapter serves as a theoretical framework for understanding how BLE, as a communication protocol, can support distance estimation.

Building on this foundation, Chapter 3, "**Description of BLE and Elements for Distance Measurement**," offers a detailed breakdown of the BLE protocol stack. It covers both the host and controller architectures, highlighting critical components such as the Generic Attribute Profile (GATT), Link Layer, PHY layer, and emerging features like Channel Sounding and Direction Finding. This chapter establishes the technical context for integrating BLE with the estimation techniques previously introduced.

Chapter 4, "**Distance Estimation Methods with BLE**," presents a focused examination of how BLE enables each of the four selected methodologies: RSSI, AoA, ToF, and CS. Each section addresses the hardware and software considerations required for implementation, as well as the advantages and limitations in terms of precision, resource consumption, and environmental robustness. For example, while RSSI is widely available and easy to implement, it suffers from significant signal variability. In contrast, Channel Sounding offers sub-meter accuracy but requires advanced hardware support, currently limited to the latest BLE 6.0 platforms.

Chapter 5, "**Applications for Different Methodologies**," provides both experimental and referential validation. Practical experiments are conducted for RSSI and ToF using the NXP MCX W71x development platform. These results illustrate how environmental factors, hardware limitations, and signal processing techniques affect measurement accuracy in real-world scenarios. For AoA and CS, public third-party demonstrations are analyzed to compensate for the lack of compatible hardware. This balanced approach provides a practical dimension to the theoretical work, highlighting implementation challenges and real-use potential.

Chapter 6, "**Comparison Methodologies**," consolidates the information gathered in earlier sections into a structured comparative analysis. Each technique is evaluated based on six criteria: accuracy, hardware requirements, power consumption, implementation cost, robustness to environmental factors, and processing complexity. This comparison allows for an objective understanding of each method's strengths and limitations, guiding readers toward informed decisions in system design. The chapter concludes by referencing real-world deployments for each method, demonstrating their relevance across various domains such as logistics, industrial tracking, and access control.

The final section of the document presents concluding remarks, summarizing key findings and offering recommendations for future development. Depending on the application context—

ranging from low-power, low-cost solutions to high-precision systems—this study provides insights into choosing the most appropriate BLE-based distance estimation method.

In summary, this case study aims to bridge the gap between theoretical research and embedded system implementation in the context of BLE localization. It offers a technical yet practical approach, grounded in experimentation and enriched by state-of-the-art analysis, providing valuable guidance for researchers, engineers, and system integrators working in the field of wireless localization.

1. Overview of localization methods based on distance determination

This chapter gives an overview of localization systems that are based on distance estimation. The goal here is to explain the main concepts that guide localization and position estimation. It starts by talking about what localization is, what devices are involved, and how distance measurements help to figure out where things are located. These descriptions are not tied to any specific technology, as this chapter is meant to build the foundation for what's coming later.

1.1. Localization

Localization is about estimating the position of a device or an object in a space, in two or three dimensions. Most of the time, the position is estimated by figuring out how far the device is from known reference points. Those reference points, or anchors, are important because they help us make sense of where things are in the environment.

The ideal objective of Localization techniques is to determine the exact position of a tag or node of interest with zero error. However, we all know that's not always possible due to the cost constraints in terms of technology or the complexity needed, and other limitations. Instead, we aim to get the best estimate possible given the data we can measure.

A good localization system needs a reference framework. Usually, this involves having some anchors, which are devices that have known positions. The tag is the device whose position we need to find. A tag is typically a device that doesn't know where it is, but can send or receive signals to and from nearby anchors.

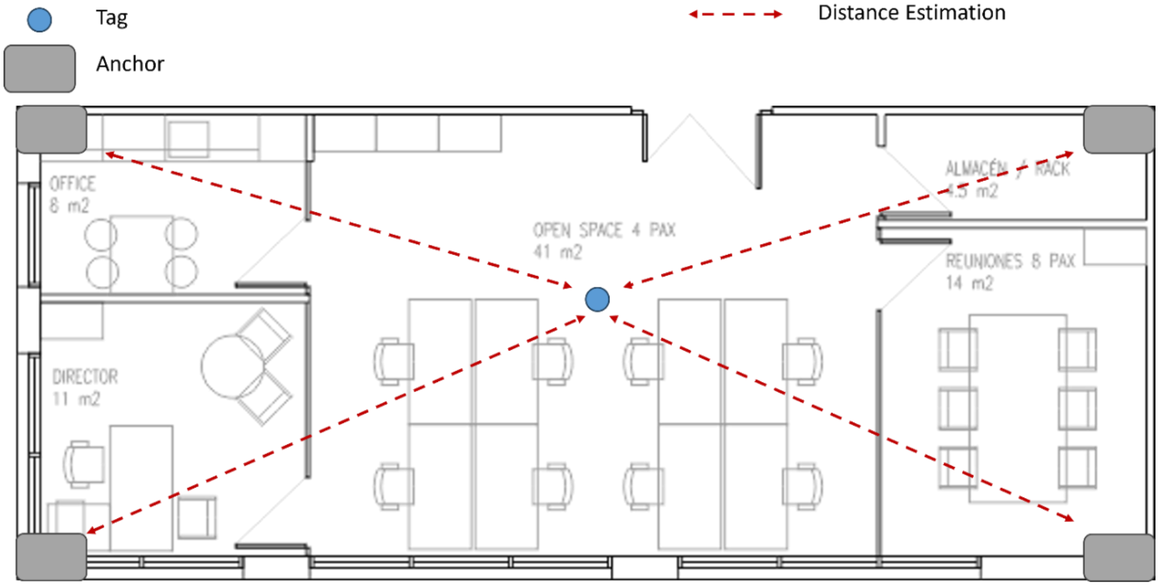


Fig. 1-1 Localization Indoor System

Typically, a tag refers to a device with an unknown position that can either send or receive signals to or from nearby anchors within its communication range. The nature of these signals depends on the application, but they are commonly based on radio frequency, optical, ultra-wideband (UWB), or acoustic technologies. [1].

Some tags are capable of measuring certain parameters of those signals — things like RSSI (Received Signal Strength Indicator), Time of Flight (TOF), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), or just proximity.

Based on this, the principle of localization is measuring or estimating the distance of a tag an several anchors, and made calculus to obtain an estimation of position in a known and delimited space, getting the localization.

One of the key insights in this field is that localization can be reduced to a problem of distance estimation. Thanks to geometrical methods such as trilateration or triangulation, it is not necessary to have full navigation data—knowing the distances to at least three anchors (in 2D) or four (in 3D) is enough to estimate a position.

Trilateration involves calculating the position of the tag based on known distances to three or more anchors. Using the intersection of circles (in 2D) or spheres (in 3D), the system calculates a position that satisfies all measured distances.

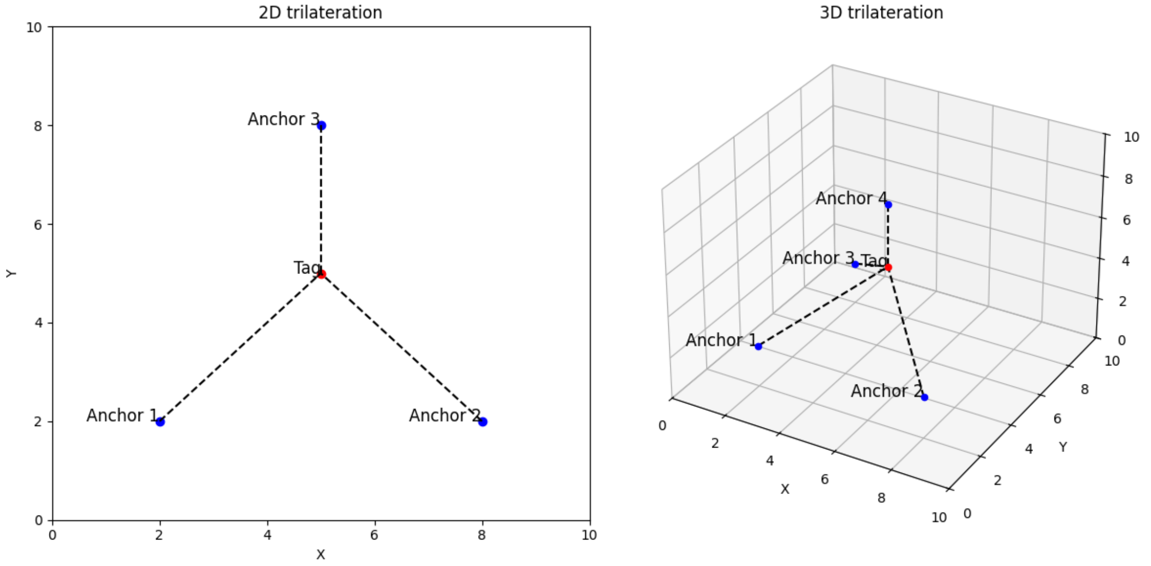


Fig. 1-2 2D and 3D trilateration

1.2. Accuracy, Precision and Resolution

Because these methods rely so heavily on distance the entire localization system depends on how well we can estimate distances. To evaluate a localization system, we need to understand three fundamental performance metrics: accuracy, precision, and resolution.

Accuracy refers to how close a measured position is to the actual (true) position. If the true position of a tag is (2.00 m, 3.00 m), and the estimated position is (2.10 m, 3.05 m), the error is about 11 cm. This system would have an accuracy of ±11 cm.

Precision refers to the repeatability or consistency of measurements under the same conditions. If repeated measurements of a static tag yield positions like (2.50 m, 3.50 m), (2.51 m, 3.49 m), and (2.49 m, 3.50 m), the results are precise.

Resolution is the smallest positional change that the system can detect. If the system can detect movement from (2.00 m, 3.00 m) to (2.02 m, 3.00 m), then the resolution is 2 cm. High-end systems might achieve resolutions as fine as 1 mm.

This chapter has introduced the basic concepts and metrics needed to understand localization systems based on distance. The following chapters will build on this by analyzing specific estimation techniques, especially those using Bluetooth Low Energy, which has become increasingly relevant due to its low cost and wide availability in embedded systems.

2. Basic methodologies for distance estimation

In the previous chapter, we introduced the idea that the main goal of localization is to determine the position of an object or tag by measuring its distance from reference points or anchors in a known space. Now, we will focus on the different approaches and techniques that make these distance measurements possible, offering a more detailed exploration of how these methods can be implemented in real-world systems.

When discussing about distance, the objective is to define a relative or absolute physical separation between two points in the space. This can be achieved using direct or indirect methods.

Direct methods are a “real” physical direct measurement of the distance between two points or objects, using a measurement instrument, or comparing it with a standardized distance or known pattern. On the other hand, indirect methods are estimations or deductions based on other physical measurements, like angles, time of propagation of a signal, strength of a signal, and geometry. These are the methodologies that will be explained on this chapter.

2.1. Physical concepts involved

Distance estimation in wireless systems is based on the behavior of certain physical parameters that change as a function of distance. Two fundamental concepts form the basis of these techniques: Power and Propagation speed.

Power is the rate at which energy is transferred or converted. It is the amount of energy used or generated per unit of time. The formal definition of power is:

$$P = \frac{dE}{dt} \tag{2-1}$$

The unit of measurement is the watt (W).

In distance estimation based on signal power, the transmitted signal power represents the electromagnetic energy emitted by the antenna per unit time. As the signal propagates through space, it experiences attenuation. The received power at the antenna corresponds to the amount of electromagnetic energy that arrives at the receiver per unit time.

The power could be described as the measure of how quickly energy is used or transmitted. In the context of radio signals, is the measure of the “strength” of the signal at a given time.

Speed of light is a fundamental physical constant that describes the speed at which light travels through vacuum. Its exact value is 299,792,458 meters per second.

Since the speed of light is a well-known and highly precise constant, if we can accurately measure the time it takes for light to travel a certain distance, we can determine that distance using the kinematic formula:

$$Distance\ = Speed * Time \tag{2-2}$$

Having defined these physical concepts, we can start with the methodologies for distance estimation, that can be classified in two categories: Range-based and Range-free methods. The main difference lies in whether the distance between nodes is directly estimated or other properties are used to infer location.

2.2. Ranged-Based methods

These methods attempt to estimate the current physical distance (or range) between two points using direct measurements or inferences based on signal properties that are modified with distance. Among the most common approaches are Received Signal Strength (RSS), Time of Flight (ToF), Time Difference of Arrival (TDoA), and Angle of Arrival (AoA).

As mentioned in Chapter 1, once the distance between a target tag and at least three anchors is known, localization can be achieved through trilateration (in 2D) or multilateration (in 3D with four or more anchors).

2.2.1 Received Signal Strength Indication (RSSI)

RSSI (Received Signal Strength Indicator) is the earliest technique used for estimating distance at the radio level. Its core concept is simple: the distance between two radio devices is inferred from the reduction in signal strength—specifically, the amplitude—as it travels through space. Although RSSI provides only rough distance estimates, it can still offer a general sense of proximity between two transceivers. It is also widely adopted, as it is supported by virtually all smartphones [2].

RSSI-based systems require only minimal hardware—typically just a power detector—which is commonly integrated into technologies like WiFi, Zigbee, and Bluetooth chipsets. These methods are also advantageous because they do not rely on synchronization between devices.

RSSI-based localization systems heavily rely on the propagation model used to estimate distance. Moreover, the accuracy of distance estimation tends to degrade as the separation between the transmitter and receiver increases. Despite this limitation, RSSI performs reliably in short-range environments [1].

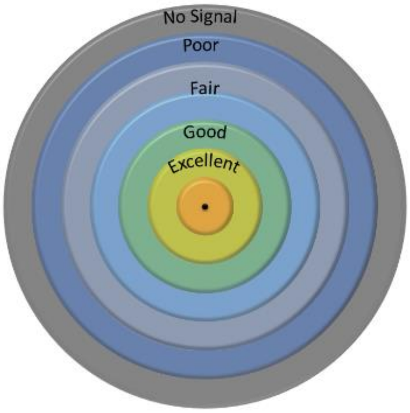


Fig. 2-1 RSSI performance

However, the inherent accuracy of RSSI is relatively low—typically within a range of three to five meters. Its performance is highly dependent on the surrounding environment, as RSSI is vulnerable to external influences such as signal absorption and diffraction. Even something as simple as holding the device in your hand can significantly affect the signal strength and, consequently, the distance estimation [2].

The Received Signal Strength Indicator (RSSI)-based localization algorithm offers a simple and cost-effective approach to positioning. It estimates the distance between sensor nodes and a reference transmitter by analyzing RSSI measurements [3].

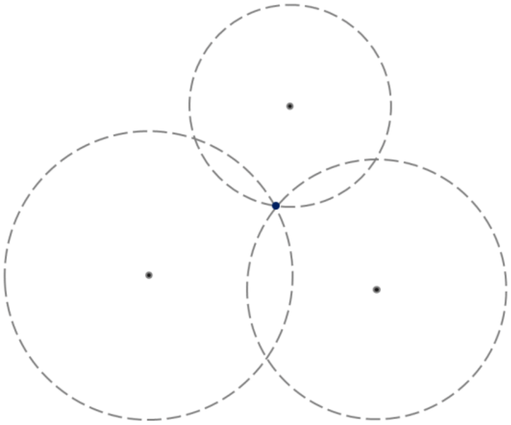


Fig. 2-2 Localization with RSSI

While RSSI-based localization has certain limitations—particularly its susceptibility to environmental interference—advancements in machine learning and statistical modeling are helping to enhance its accuracy. Consequently, RSSI-based localization remains a vibrant and promising area of research, with significant potential across various applications, including asset tracking, inventory management, healthcare, and emergency response [3]

In telecommunications engineering, a widely used model for estimating the received power at the terminals of a receiving antenna is the Friis Transmission Equation. This equation relates the received power to the power density of the incident wave and the effective aperture of the receiving antenna, assuming idealized free-space conditions. When a transmitting antenna emits a known amount of power, the Friis equation provides a theoretical estimate of the power that will be received at a given distance.

This model incorporates essential parameters that influence signal propagation, including antenna gains, signal wavelength, and the distance between the transmitter and receiver. It serves as a foundational tool for line-of-sight wireless communication systems and is widely applied in radio link budget calculations. The equation is named after Danish engineer Harald T. Friis, who introduced it in the 1940s.

The Friis equation is expressed as follows:

$$P_r = P_t \times G_t \times G_r \times \left(\frac{\lambda}{4 \times \pi \times d}\right)^2 \tag{2-3}$$

Where:

P_r: Power Received at the receiving antenna (watts).

P_t: Power Transmitted from the transmitting antenna (watts).

G_t: Gain of the transmitting antenna (unitless).

G_r: Gain of the receiving antenna (unitless).

λ: Wavelength of the signal (meters).

d: Distance between the transmitting and receiving antennas (meters).

π: Mathematical constant (approximately 3.1416).

This formula assumes ideal free-space conditions, meaning it does not account for obstacles, reflections, diffraction, or multipath propagation. Nonetheless, it remains a foundational tool in wireless communications and is often used as a starting point for more complex channel models.

2.2.2 Time of Flight (ToF)

Time of Flight localization methods utilize the time it takes for signals to travel between transmitter and receiver nodes to estimate distances and subsequently determine the location of objects or devices in a given environment. These methods are commonly used in various applications such as indoor positioning systems, asset tracking, and robotics.

ToF measurement relies on Round-Trip-Time (RTT). It is based on a precise measurement of the time difference between the transmission of a signal by object A and its return to the object A after being reflected by an object B.

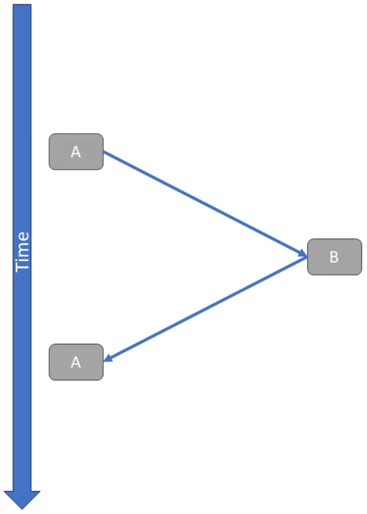


Fig. 2-3 Round-Trip Time

In wireless communication systems, RTT-based localization methods measure the time it takes for signals to travel between a device and multiple access points (e.g., Wi-Fi routers). By measuring the round-trip time of signals, the device can estimate its distance from each access point and determine its location through trilateration or multilateration.

The Time-of-Flight (ToF) technique is applicable to localization because the time it takes for an electromagnetic wave to travel from the transmitter to the receiver is directly proportional to the distance between them [4]

In a localization context, once the distances between a target node and at least three reference nodes (anchors) are known, the position of the target can be determined on a two-dimensional plane. For localization in three-dimensional space, a minimum of four anchors is required to accurately compute the target's position.

ToF is a method of measuring the distance between a sensor and an object, based on a precise measurement of the time difference between the transmission of a signal by the sensor and its return to the sensor after being reflected by an object.

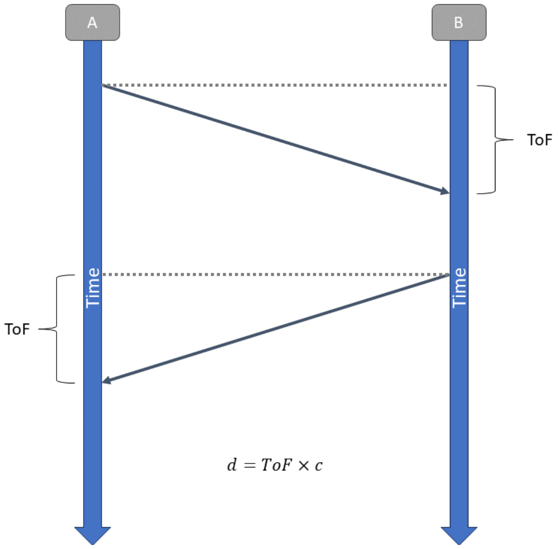


Fig. 2-4 Time of Flight

Based on a record of times at which the initial packet was transmitted by the Measuring Device (A) and the time at which a response packet is received from the Reflector Device (B) by A, A can calculate a ToF of the packet exchange. Using the calculated ToF, a distance estimate (or range) between the two devices can be computed. The determined distance d can be employed for a variety of functions, such as taking a specified action when the distance is above or below a threshold.

A method to capture the timestamps at which the packets are transmitted and received is required at both ends. Furthermore, these timestamps must be shared from Node B to Node A for ToF calculation. Node A records a count from a timer, designated T1, in response to initiating transmission of the ranging packet. In response to receiving the ranging packet, the Node B records a count from a local timer, designated T2. The Node B takes a certain amount of time to process the incoming packet and send a response packet. This time is designated as Processing Time, which is an overhead that needs to be eliminated to get an accurate ToF reading. In response to initiating transmission of the response packet the Node B stores a count designated T3. The response packet includes data payload indicating the timestamps to calculate the B processing time. Upon receiving the response packet, Node A records a count designated T4.

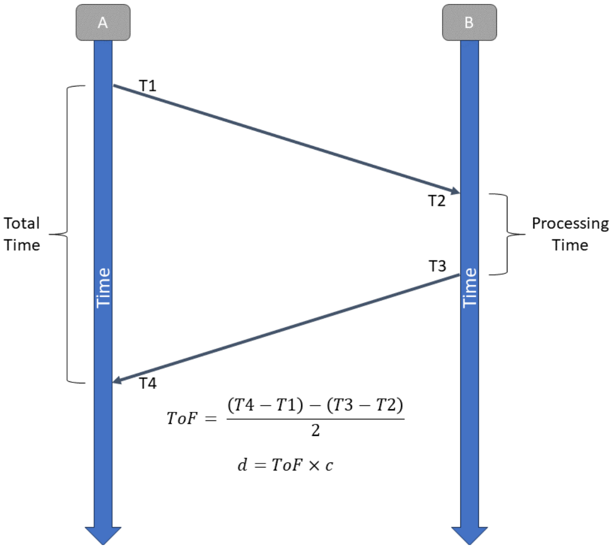


Fig. 2-5. ToF with Processing time calculation

T1: Sent from Node A

T2: Received at Node B

T3: Response sent from Node B

T4: Response received at Node A

$$ToF = \frac{(T4 - T1) - (T3 - T2)}{2} \tag{2-4}$$

2.2.3 Angle of Arrival (AoA)

The angle of arrival (AoA) refers to the direction from which a signal arrives at a receiver antenna array. It's a crucial parameter in various applications like radar, wireless communication, and radio astronomy.

AoA (Angle of Arrival)-based systems typically require an array of sensors to detect phase differences in the incoming signal at each element of the array, allowing the direction of arrival to be inferred. The accuracy of AoA measurements is influenced by the signal-to-noise ratio (SNR), the number of sensors in the array, and the spacing between them. The latter two factors determine the array's aperture, which directly affects angular resolution [1]

In radar systems, AoA helps in target localization and tracking. In wireless communication, it's used for beamforming, spatial multiplexing, and interference mitigation. Radio astronomy utilizes AoA for celestial object observation and imaging.

Angle of Arrival uses a single transmitter and a single receiver. The receiver is equipped with an antenna array. Small differences in the signal received by different antennas of the array can be used to estimate the angle of the receiver in relation to the transmitter. This technique uses no synchronization, which is a benefit in comparison to time based techniques. The location of the receiver can be calculated by triangulation.

For AoA estimation to work effectively, specific technical conditions must be met. First, the receiver must be equipped with a multi-element antenna array, where the spacing between antennas is typically a fraction of the signal's wavelength (commonly λ/2) to avoid spatial aliasing and achieve accurate phase difference measurements. The system also requires high-resolution analog-to-digital converters (ADCs) and signal processors capable of estimating the phase or time difference of arrival between signals received by the various antenna elements. Additionally, a precise calibration of the antenna array geometry and a well-characterized signal model are essential to reduce systematic errors and enhance direction-finding accuracy.

2.3. Range-Free Methods

These methods do not attempt to directly measure or estimate physical distance. They use information of a known environments or network (if several nodes are within communication range) and sometimes node density or movement patterns to estimate distance or position.

Fingerprinting. The range-free distance fingerprinting method estimates the distance of a device by comparing the current measurement with all the measurements in the fingerprint database.

To have this technique working, there is a pre-work needed before using it, called a Offline Phase, that includes:

1. Mapping of the area: The indoor area is divided into a grid of reference points with known and defined locations.

2. Data collection: at each reference point, measurements of the characteristics of available signals are collected/measured.
3. Database creation: For each reference point, a “fingerprint” is created, consisting of a vector of collected measurements.

After all this job done for the desired indoor environment, the Online Phase can be used:

1. Real-Time measurement: the device (tag) whose location is to be determined measures the same wireless signal characteristics collected during the offline phase, and creates the fingerprint of the device.
2. Database comparison: the fingerprint is compared with all the fingerprints stored in the database, and a comparison algorithm is used to find the fingerprints that are most similar to the current fingerprint.
3. Location estimation: the tags location is estimated based on the location of the reference points corresponding to the most similar fingerprints found on the database.

2.4. Comparison

The choice between range-based or range-free methods depend on the specific application requirements, such as needed localization accuracy, cost and power constraints, and the characteristics of the deployment environment.

Given the wide variety of distance estimation techniques available, this work will focus specifically on three range-based methods: Received Signal Strength Indicator (RSSI), Time of Flight (ToF), and Angle of Arrival (AoA). These techniques have been selected due to their relevance and applicability within Bluetooth Low Energy (BLE) systems, which will be introduced and discussed in more detail in the following chapters. The goal is to analyze their performance, constraints, and implementation considerations in the context of BLE-based positioning.

3. Description of BLE and elements for distance measurement

As the demand for high-accuracy location services continues to grow, Bluetooth Low Energy (BLE) has become a leading protocol for indoor positioning. BLE offers low-power, flexible communication, supporting topologies such as point-to-point, broadcast, and mesh, which makes it an ideal choice for large-scale device networks. Additionally, BLE includes features like Direction Finding, which enables devices to determine not only proximity but also the direction of other devices, offering the potential for centimeter-level location accuracy.

This chapter focuses on the BLE architecture, which is fundamental to understanding how BLE supports distance measurement techniques critical for precise positioning. BLE is particularly suited for systems that require real-time tracking and distance estimation due to its low power consumption, cost-effectiveness, and widespread adoption. The combination of these features makes BLE an ideal candidate for indoor location-based services, which are the focus of this work.

By understanding these key elements of BLE, we can better appreciate its applicability to the distance measurement methods discussed in earlier chapters, such as RSSI, ToF, and AoA. The following sections provide a detailed breakdown of the BLE components, their functionalities, and their relevance to positioning and distance estimation.

We will explore BLE in two main blocks: the BLE Host and BLE Controller. These components play a key role in enabling accurate distance measurement techniques which were introduced in previous chapters.

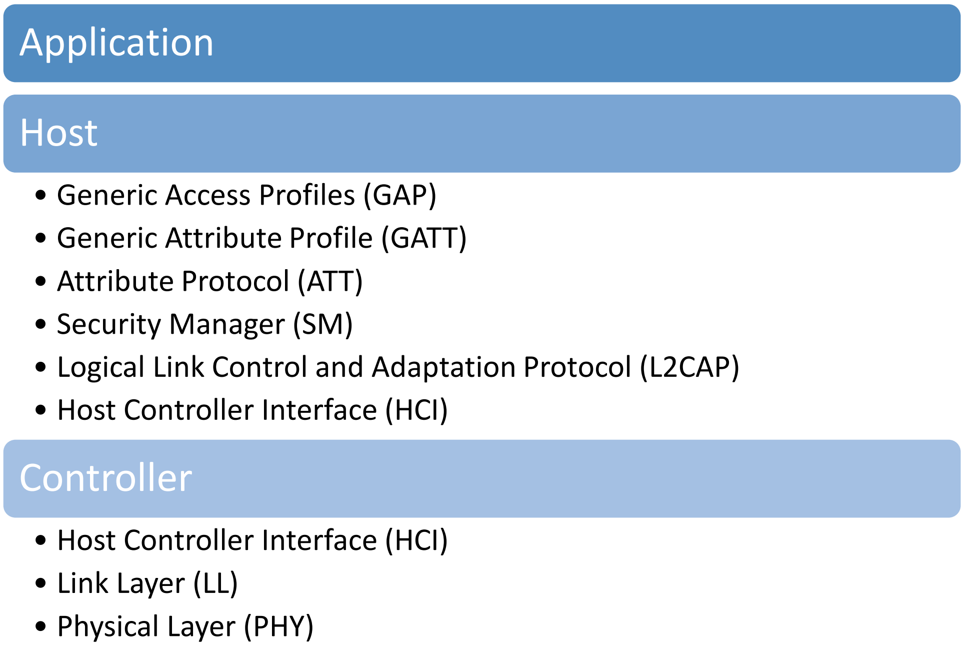

Application
Host
Generic Access Profiles (GAP)
Generic Attribute Profile (GATT)
Attribute Protocol (ATT)
Security Manager (SM)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
Host Controller Interface (HCI)
Link Layer (LL)
Physical Layer (PHY)

Fig. 3-1 BLE Architecture

3.1. BLE Host Architecture

Bluetooth Low Energy (BLE) operates through a layered architecture to enable efficient communication and functionality. The BLE host is responsible for managing communication between the host device and the connected BLE device. Key components include the Channel Manager, L2CAP Resource Manager, Security Manager Protocol, Attribute Protocol, Generic Attribute Profile, and Generic Access Profile, each serving specific roles to ensure smooth and secure data transmission.

3.1.1 Channel Manager

The Channel Manager is responsible for creating, managing, and closing L2CAP channels that enable data transport and application communication. It interacts with the L2CAP protocol to establish these channels, working with the remote device's channel manager to set up connections between endpoints. The Channel Manager also interacts with the local link manager to create logical links and configure them to meet the quality of service requirements for the data being transported.

For instance, in a BLE setup where a smartphone is connected to a Bluetooth sensor, the Channel Manager is tasked with creating and managing the L2CAP channel that ensures smooth communication. If the sensor sends temperature readings to the smartphone, the Channel Manager ensures that the connection maintains the required data quality and reliability, making real-time data transmission seamless.

3.1.2 L2CAP resource Manager

The L2CAP Resource Manager manages the ordering of data packet submission (PDU fragments) to the baseband and handles scheduling between channels to ensure that L2CAP channels receive fair access to the physical link. It ensures that limited resources (such as buffer space and bandwidth) are managed effectively so that no application or channel monopolizes the link, which is important because Bluetooth controllers have finite resources.

If having multiple BLE applications running on a device, like a fitness app sending real-time heart rate data and a background app syncing data with the cloud, the L2CAP Resource Manager ensures that both data streams are transmitted without interference, managing when and how each application's data is sent to ensure fair access and avoid congestion on the Bluetooth link.

3.1.3 Security Manager Protocol

The Security Manager Protocol (SMP) handles the generation of encryption and identity keys for secure device pairing. Operating over a dedicated L2CAP channel, the SMP ensures that encryption keys are stored securely and that random addresses are generated and resolved to known device identities. The protocol also interfaces with the Controller to authenticate devices during pairing and establish a secure connection.

When a pairing of a smartphone with a Bluetooth-enabled smart lock, the SMP ensures that encryption keys are exchanged securely between the devices. It also verifies that the devices are legitimate by authenticating the keys and establishing a secure channel, ensuring that no unauthorized devices can intercept or tamper with the data exchanged.

3.1.4 Attribute Protocol

The Attribute Protocol (ATT) enables communication between an ATT Server and an ATT Client. The ATT Client can request, send commands, and receive responses, which include reading or writing attributes on a remote device’s ATT Server. The protocol allows the devices to interact at the attribute level, providing a way to manage and exchange information like sensor readings or device status.

In a BLE-enabled heart rate monitor, the ATT protocol allows the smartphone (the ATT Client) to request the "Heart Rate" attribute from the heart rate monitor (the ATT Server). The monitor will then respond with the current heart rate data, which is used by the smartphone to display it to the user in real-time.

3.1.5 Generic Attribute Profile

The Generic Attribute Profile (GATT) represents the functionality of the ATT Server and Client by defining the hierarchy of services, characteristics, and attributes used in communication. GATT enables the discovery, reading, and writing of services and characteristics between devices. This profile is key to the structuring and organization of Bluetooth services.

A fitness tracker might expose services like "Heart Rate Measurement," "Battery Level," and "Device Information" through GATT. When a smartphone connects, it can discover these services, read the heart rate data, check the battery status, and retrieve device information—all thanks to the organization provided by the GATT profile. The GATT profile ensures that these services are well-structured and easy for the client to interact with.

3.1.6 Generic Access Profile

The Generic Access Profile (GAP) defines the basic functionality common to all Bluetooth devices, such as device discovery, connection modes, security, and service discovery. GAP specifies how devices discover one another and how they can connect securely, making it a fundamental component in all Bluetooth communications.

When the Bluetooth feature on a smartphone is turned on, the GAP is responsible for deciding whether the phone should be discoverable or connectable to other devices. For example, when increasing physical activity detected by the phone itself, the GAP can allows the phone to be discoverable by the heart rate monitor, enabling an automatic connection for data transfer. GAP ensures the process follows secure procedures, establishing a reliable link between devices.

The four main GAP modes—Central, Peripheral, Broadcaster, and Observer—are crucial for understanding the versatile nature of BLE communication, from simple point-to-point connections to one-to-many broadcasting.

Each of these modes serves a unique purpose and plays a significant role in the type of communication that can occur.

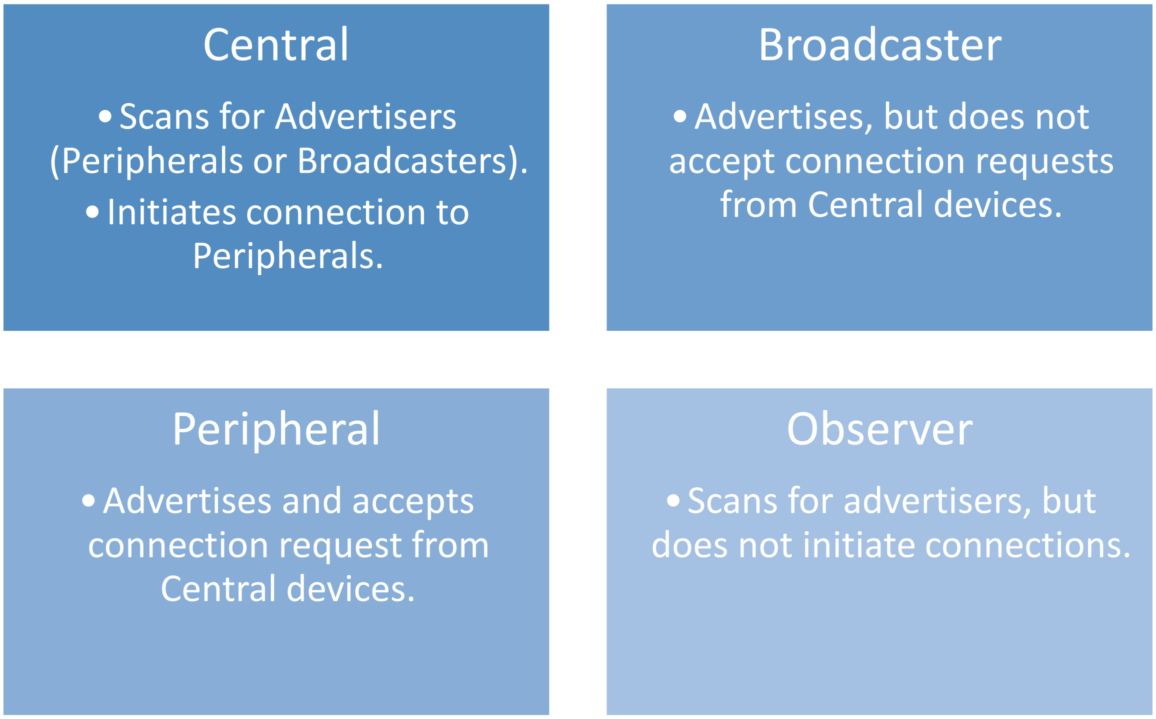

Central
• Scans for Advertisers (Peripherals or Broadcasters).
• Initiates connection to Peripherals.
Broadcaster
• Advertises, but does not accept connection requests from Central devices.
Peripheral
• Advertises and accepts connection request from Central devices.
Observer
• Scans for advertisers, but does not initiate connections.

Fig. 3-2 BLE Roles

3.2. BLE Controller Architecture

The BLE Controller handles the operations closest to the hardware, managing the essential functions for data transmission and reception on a Bluetooth device. This architecture is divided into several functional blocks that enable communication between devices and network efficiency. Below are the key blocks within the BLE controller.

3.2.1 Device Manager

The Device Manager is responsible for managing the general behavior of the Bluetooth device, but it is not directly involved in data transport. Its primary functions include discovering nearby Bluetooth devices, connecting to them, or making the local Bluetooth device discoverable or connectable by others.

When a Bluetooth device is powered on and wants to connect to another, the Device Manager is responsible for handling that connection request. If the device is set to be visible, the manager facilitates the connection process.

Additionally, the Device Manager interacts with the Baseband Resource Controller to request access to the transport medium for these operations. It also controls the local behavior of the device, such as managing the device's local name and any stored link keys.

3.2.2 Link Manager

The Link Manager (LM) handles the creation, modification, and release of logical links between devices, as well as the update of parameters related to physical links, such as enabling encryption or adjusting transmit power on the physical link.

For instance, if two Bluetooth devices are configured for secure communication, the Link Manager ensures that the logical links between them are properly encrypted. If the devices are at a longer distance, the Link Manager can adjust the transmission power to maintain a stable connection.

The LM is also responsible for creating new logical links between devices when required, utilizing the Link Layer (LL) protocol.

3.2.3 Link Controller

The Link Controller is in charge of encoding and decoding Bluetooth packets containing the data to be transmitted. It works directly with the physical and logical channels used for data transmission.

When a device sends a Bluetooth data packet, the Link Controller ensures that the packet is correctly formatted and transmitted over the appropriate physical channel. It also interprets the signals related to logical and physical links, which is essential for the correct data flow.

3.2.4 PHY

The Physical Layer (PHY) is responsible for transmitting and receiving packets of information over the physical communication channel. It controls the timing and frequency at which packets are transmitted, with the Baseband controlling it to ensure that the frequencies and timing used to transmit data between devices are correct.

A clear example of the PHY's role is when two devices are in relatively close proximity. The PHY ensures that the signal from one device is transmitted on the correct frequency and that the receiving device picks it up at the right moment.

3.2.5 Isochronous Adaption Layer

The Isochronous Adaptation Layer (ISOAL) enables the flexible sending and receiving of isochronous data (data requiring continuous, low-latency transmission) between the upper layer and the Link Layer. This layer adapts the data being sent, adjusting its size and intervals to meet the Link Layer’s protocol requirements.

A practical example of how the ISOAL works is in audio applications, where data needs to be transmitted at very specific intervals to ensure smooth playback. The ISOAL manages such data to ensure that audio packets are transmitted without loss or delay, even if the upper layers handle data in different packet sizes.

3.2.6 Channel Sounding

The Channel Sounding process enables Bluetooth devices to measure and adjust the quality of the communication channel between them. During this process, devices exchange information about the channel status, such as signal strength and other related parameters.

For instance, in an environment with interference, Channel Sounding can help devices adjust their transmission frequency or power to improve signal quality. Additionally, data collected during the process can be sent to the Host for distance estimation or to detect potential network attacks.

3.3. Bluetooth Range and Radio Spectrum Considerations

As Bluetooth Low Energy (BLE) becomes increasingly utilized in diverse applications, one of the critical factors that influence its performance is the communication range. Bluetooth technology offers a versatile range of communication distances, which can be tailored to meet the requirements of specific use cases. This flexibility is a significant advantage for system designers aiming to optimize their products for long-range or short-range communication, based on the unique needs of their application.

Bluetooth operates within the 2.4 GHz ISM (Industrial, Scientific, and Medical) spectrum band, a globally recognized frequency band that allows Bluetooth devices to be deployed worldwide without the need for additional regulatory compliance. The 2.4 GHz band strikes an ideal balance between communication range and throughput, making it well-suited for low-power wireless applications, including indoor location systems. Understanding how Bluetooth devices utilize this spectrum is crucial for ensuring efficient communication in systems where multiple devices are interconnected.

3.3.1 The Role of the Physical Layer (PHY) in Bluetooth Communication

The physical layer (PHY) plays a central role in the performance of Bluetooth communication. It defines the transmission techniques, channel utilization, and error correction methods that allow Bluetooth devices to effectively send and receive data. The PHY also impacts the range and clarity of the communication signal, much like how the speed and clarity of speech influence how well a message is understood. Bluetooth provides different PHY options, which can be selected based on the specific needs of a given application. These PHY choices allow developers to optimize their designs for varying trade-offs between range, data rate, and energy efficiency.

The selection of a suitable PHY is essential when designing systems that rely on precise distance measurements, such as those for indoor positioning systems. The PHY’s modulation techniques and its handling of environmental interference will directly affect the accuracy and reliability of distance estimates.

3.3.2 Path Loss and Environmental Considerations

Path loss, or the reduction in signal strength due to distance and obstacles, is another crucial factor when designing Bluetooth-based positioning systems. Just as sound gets muffled when passing through walls, radio waves can be attenuated by various environmental factors, including walls, buildings, and even weather conditions. Designers must consider these path loss effects when developing systems for indoor positioning or other Bluetooth-based services, ensuring that the system maintains reliable communication over the required distances.

By understanding and accounting for the effects of path loss, receiver sensitivity, transmit power, and antenna gain, designers can optimize Bluetooth-based systems to achieve the best performance in real-world environments. In the context of distance estimation for indoor positioning, such considerations are critical to achieving accurate and reliable results.

3.3.3 The Challenge of Interference

Unlike wired systems, where data is transmitted through dedicated physical media, wireless technologies must operate over shared radio frequency bands. This makes them inherently susceptible to conflicts when multiple devices attempt to transmit data simultaneously.

Bluetooth® technology operates in the 2.4 GHz ISM band, which is also used by other popular wireless protocols such as Wi-Fi and IEEE 802.15.4 (commonly used in Zigbee and Thread). Because of this overlap, Bluetooth devices can encounter interference from co-located networks or devices that operate on the same or adjacent frequency channels.

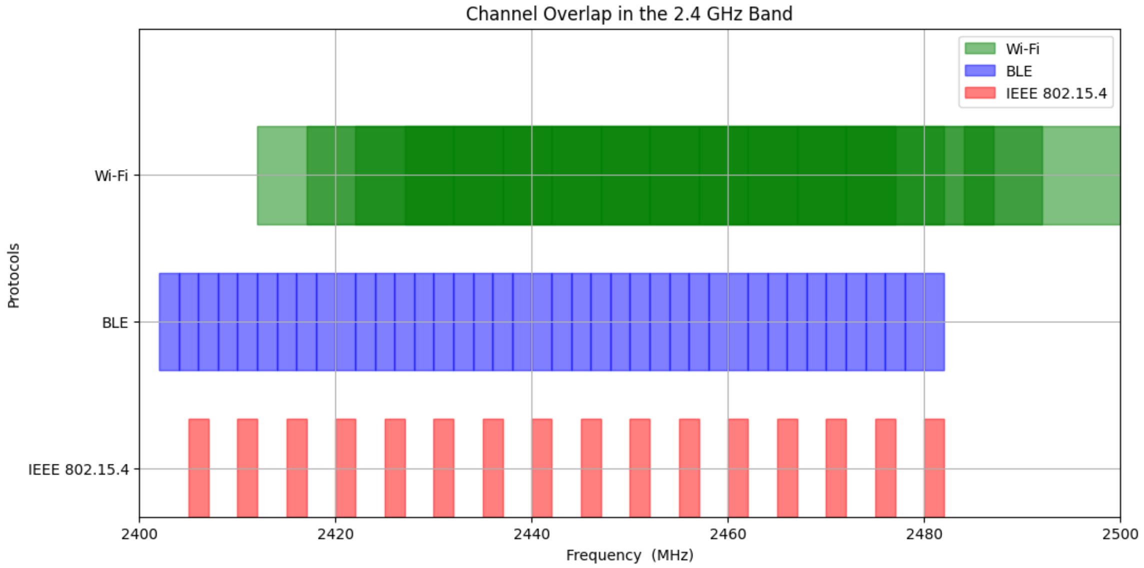


Fig. 3-3 Channel overlap in 2.4 GHz band

For instance, if two Bluetooth devices are communicating while a nearby Wi-Fi router transmits on the same channel, data packets may be disrupted or lost due to a collision. This can affect communication quality, reduce throughput, and in some cases, force retransmissions—leading to increased latency and power consumption.

To address this challenge, Bluetooth incorporates several mechanisms designed to minimize the impact of interference and packet loss. One of the core strategies is the use of adaptive frequency hopping (AFH), which dynamically avoids congested channels by monitoring the spectrum and excluding problematic frequencies from use. In this way, Bluetooth devices can maintain robust connections even in environments with high wireless traffic.

These strategies are essential for applications such as indoor positioning, where accurate and continuous communication between devices is necessary for real-time distance estimation. Understanding the sources of interference and how BLE mitigates them is crucial when designing systems for dense wireless environments like smart homes, industrial settings, or public spaces.

4. Distance estimation methods with BLE

After discussing the various methodologies for distance estimation and having explored the technical underpinnings of Bluetooth Low Energy (BLE), we are now in a position to integrate these concepts and examine specific BLE-based techniques in detail. This chapter presents an in-depth look at the most commonly used BLE distance estimation methods, including Angle of Arrival (AoA), Time of Flight (ToF), Received Signal Strength Indication (RSSI), and Channel Sounding. Each method offers different trade-offs in terms of complexity, accuracy, and implementation requirements, which will be discussed in their respective sections.

4.1. Received Signal Strength Indication (RSSI)

Received Signal Strength Indication (RSSI) is one of the most accessible and widely used methods for distance estimation in BLE systems. It relies on measuring the attenuation of signal power as it propagates from a transmitter to a receiver. Because BLE devices natively support RSSI readings, this method requires no additional hardware and is compatible with virtually all BLE-compatible platforms.

In the context of BLE, RSSI is typically reported by the radio after the reception of a packet and is expressed in dBm. The RSSI measurement includes both the signal strength and the ambient noise, which can vary significantly depending on the environment. It's important to highlight that the exact calculation and behavior of RSSI are highly dependent on the hardware implementation. Therefore, it is always recommended to consult the manufacturer's documentation to understand how RSSI is derived and what configuration or calibration steps are necessary to ensure reliable readings.

BLE specifications do not mandate a specific method for converting RSSI to distance; instead, developers must rely on empirical calibration or proprietary algorithms tailored to the particular BLE radio and use case. Several BLE SoCs include filtering or averaging features to stabilize RSSI measurements, and some allow configuration of the sampling interval or smoothing factor.

RSSI values are typically available in both connected and advertising modes, making it a flexible solution for a variety of BLE applications. However, its effectiveness is significantly reduced in dynamic or noisy environments, where signal fluctuations can introduce large errors in distance estimation.

4.2. Angle of Arrival (AoA)

Angle of Arrival (AoA) was introduced in the Bluetooth® Core Specification v5.1 as part of the Direction Finding feature. Together with Angle of Departure (AoD), it marked an important step forward in enabling more precise positioning capabilities with BLE.

As previously studied in chapter 2, AoA does not estimate distance directly. Instead, it determines the angle at which a radio signal arrives at the receiver. From this angle information, and with known reference points, it becomes possible to calculate distances using geometric relationships.

To perform AoA estimation, a Bluetooth device must be equipped with multiple antennas arranged in a known geometry, such as a Uniform Linear Array (ULA). In this configuration, the signal reaches each antenna at slightly different times, causing detectable phase shifts. These shifts are used to estimate the angle of arrival of the signal.

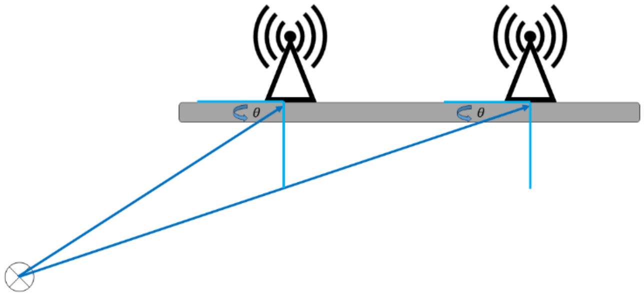


Fig. 4-1 AoA antenna principle

A key enabler of AoA functionality in BLE is the Constant Tone Extension (CTE). The CTE is an unmodulated signal appended to a standard Bluetooth LE packet, specifically designed to facilitate phase measurements across the antenna array. Since it maintains a constant frequency and phase, the receiver can sample the in-phase (I) and quadrature (Q) components of the signal over time, enabling accurate estimation of the angle of arrival. This mechanism is essential because the AoA method relies on very small phase differences between the received signals at each antenna.

AoA implementations often use Switch Antenna Arrays (SAA), where only one antenna receives the signal at a time. This configuration offers a good balance between implementation complexity and performance. More complex antenna arrangements may allow the estimation of multiple angles simultaneously but require additional hardware and signal processing.

It is important to note that the accuracy of AoA depends heavily on environmental conditions. In indoor scenarios, multipath propagation —where the signal reaches the receiver through multiple reflective paths— can interfere with the direct signal and lead to inaccurate angle estimation.

4.3. Time of Flight (ToF)

The Time of Flight (ToF) method estimates distance by measuring the time a radio signal takes to travel from one device to another and back. Applied to BLE, ToF involves the exchange of packets between two devices, where the elapsed time is calculated by considering radio processing delays and protocol-specific overheads, such as turn-around times. Since the inter-frame spacing (IFS) is defined by the Bluetooth specification, it becomes possible to determine the Two-Way ToF by measuring the delay between the end of transmission and the start of reception.

However, BLE radio signals propagate at the speed of light ($c \approx 3 \times 10^8$ m/s), meaning that a 1-meter distance corresponds to approximately 3.3 nanoseconds. Accurately capturing such small time intervals ideally requires timestamping mechanisms operating at gigahertz-scale clock speeds, which introduces complexity and cost. In practical BLE systems targeting consumer or IoT applications, low-power microcontrollers with integrated 2.4 GHz radios are often used. These platforms typically rely on a reference clock (Fref) such as 32 MHz, which translates into a raw ToF resolution of about 10 meters. While this level of precision may be insufficient for fine-grained localization, it can still serve to validate coarse estimates or supplement more accurate positioning techniques.

To improve distance estimation, multiple ToF measurements can be collected and averaged. When enough samples are taken, assuming they follow a normal distribution, statistical filtering techniques such as outlier removal, weighted averaging, or history-based smoothing can help mitigate the effects of environmental noise and multipath propagation—a common challenge in indoor scenarios. In such environments, reflected signals can arrive with different delays, skewing the average measurement and reducing accuracy.

The ToF method, therefore, introduces a trade-off between accuracy and measurement time. To reduce error margins and achieve accuracy within 1–2 meters, repeated measurements may be necessary, increasing latency and energy consumption.

A typical BLE-based ToF distance measurement system includes the following components:

a) A timestamp counter synchronized to the radio subsystem or reference clock (Fref).
b) A precise hardware-based timestamping mechanism to capture packet arrival and transmission times.
c) A measurement protocol that includes the steps of:
   a. Timestamp collection
   b. Preprocessing (e.g., initial filtering or validation)
   c. Postprocessing (e.g., statistical adjustment or smoothing)
   d. Generation of a measurement report

Although ToF is not natively supported in the Bluetooth Low Energy standard as a core feature, it remains a promising approach for BLE-based localization when combined with tailored firmware and dedicated timestamping logic.

4.4. Channel Sounding

Unlike Angle of Arrival (AoA) and Angle of Departure (AoD) techniques, which require multiple antennas and can suffer from performance degradation in multipath environments, Bluetooth Low Energy (BLE) introduces a promising method known as Channel Sounding (CS) to improve distance estimation accuracy. This method leverages phase-based ranging (PBR) and round-trip timing (RTT) measurements to characterize the radio propagation channel with high precision.

Phase-Based Ranging (PBR) is based on analyzing the phase shift of radio signals exchanged between two devices. Devices alternately transmit and receive coordinated unmodulated continuous wave tones over multiple frequency channels. This multi-frequency approach resolves phase ambiguities and reduces the impact of multipath propagation—especially important in indoor environments where reflections are prevalent—thereby enhancing the reliability and resolution of distance estimates.

The phase difference θ measured at frequency f relates to the distance d between devices by:

$$\theta = 2\pi \times d \times \frac{2f}{c} \tag{4-1}$$

where c is the speed of light (~3 × 10^8 m/s). Due to the periodicity of the phase, distances exceeding the wavelength require accounting for an integer number n of full cycles, yielding:

$$d = \frac{c}{2f}\left(\frac{\theta}{2\pi} + n\right) \tag{4-2}$$

To overcome the cycle ambiguity, BLE Channel Sounding measures phase shifts at multiple frequencies (multi-carrier phase ranging). By combining phase data across frequencies, the exact distance can be determined without explicitly tracking n.

In parallel, Round-Trip Timing (RTT) measurements complement PBR by measuring the time a signal takes to travel from the initiator device to the responder and back. Since radio waves propagate at the speed of light, the RTT multiplied by ccc provides the total travel distance, which divided by two yields the device separation:

$$2r = c \times t_{RTT} \tag{4-3}$$

For example, a round-trip time of 20 nanoseconds corresponds to an approximate one-way distance of 3 meters.

4. DISTANCE ESTIMATION METHODS WITH BLE

BLE’s Channel Sounding feature integrates these measurement techniques within the protocol stack by defining specific Link Layer procedures and a dedicated air interface protocol. This allows two devices to exchange a tightly synchronized series of RF signals across multiple channels, referred to as CS procedures. Each procedure is composed of multiple CS events, subevents, and steps, orchestrated to precisely time and measure the phase and timing characteristics of the communication channel.

Four CS step modes (mode-0 through mode-3) support distinct operations:

- Mode-0: Frequency and timing calibration between devices to synchronize clocks and oscillators.
- Mode-1: Exchange of RTT packets for round-trip time measurements.
- Mode-2: Transmission of phase-based ranging tones to measure channel phase and amplitude.
- Mode-3: A combined mode exchanging both RTT and phase/amplitude data for comprehensive channel characterization.

Devices equipped with antenna arrays can leverage antenna switching during CS tone exchanges to measure channel characteristics from different spatial perspectives, similar to AoA techniques but within the CS framework, further improving accuracy without the complexity of full direction-finding hardware.

This approach enhances BLE’s capability for indoor localization applications, where multipath effects and non-line-of-sight conditions complicate traditional methods such as RSSI or ToF. Channel Sounding’s multi-frequency, multi-step measurement process offers a scalable path to sub-meter accuracy in realistic deployment scenarios.

Overall, BLE Channel Sounding represents a significant advance in BLE-based distance estimation, combining precise physical layer measurements with protocol-level coordination, making it highly suitable for emerging applications in asset tracking, secure access control, and smart environment interaction.

5. Applications for different methodologies

This chapter presents an overview of the experimental work conducted using RSSI and Time-of-Flight (ToF) distance estimation techniques. Performing these experiments firsthand was essential to evaluate the behavior of these methods under real-world conditions, understand their practical limitations, and assess how environmental factors influence performance. Working directly with the development tools also allowed for the identification of integration challenges that may arise in embedded applications, particularly regarding timing precision and environmental noise.

In contrast, direct experimentation with Angle of Arrival (AoA) and Channel Sounding (CS) was not feasible due to hardware availability and confidentiality constraints. Implementing AoA requires a dedicated antenna array and a radio capable of controlled switching and phase sampling—resources that were not accessible during this project. As for Channel Sounding, this technique is part of the Bluetooth 6.0 specification, which, at the time of this work, is not yet supported by commercially available microcontrollers from NXP. Preliminary software and hardware support are under active development and subject to NDA restrictions, making it impossible to conduct or disclose direct experimentation results in this document.

To ensure a comprehensive and balanced analysis, this section incorporates third-party studies and publicly available demonstrations that validate the use of AoA and CS in practical scenarios. These references provide relevant technical insights and help contextualize the expected performance and limitations of each method, even in the absence of direct experimentation.

5.1. Experimental Results Overview

For the demonstrations of these methods when applicable is taking as a development resource from NXP Semiconductors. The MCX W71x series integrates a 96 MHz ARM Cortex-M33 core with a versatile radio subsystem that supports multiple wireless protocols, including Matter, Thread, Zigbee, and Bluetooth LE. This radio subsystem operates independently with its own dedicated core and memory, relieving the main CPU to focus on application tasks and enabling future-proofing through firmware updates. Additionally, the MCX W71x features robust security through the built-in EdgeLock Secure Enclave Core Profile and is compatible with NXP's EdgeLock 2GO cloud platform for secure credential provisioning and management [5].

Taking as a base a basic application provided on the MCUXpresso Software Development Kit (SDK), the needed changes in the applications can be easily replicated. The Bluetooth LE Host Stack component provides an implementation for a Bluetooth 5.3 mandatory and some optional, proprietary, and experimental features. The Bluetooth LE Host Stack component provides application examples, services, and profiles. Depending on the method, a dedicated application will be used and described, based on the needs in terms of Hardware or Software.

As described on section "3.1.5 Generic Attribute Profile", the Generic Attribute Profile (GATT) establishes in detail how to exchange all profile and user data over a BLE connection. GATT deals only with actual data transfer procedures and formats.

The GATT (Generic Attribute Profile) database defines a hierarchical structure to organize Bluetooth Low Energy (BLE) attributes. This hierarchy includes Profiles, Services, Characteristics, and Descriptors. A Profile is a high-level specification that outlines how one or more services can be used to support a specific application. A Service is a collection of related Characteristics, which represent individual data points or features. Each Characteristic may include one or more Descriptors, which provide additional information about the characteristic's value, such as format, range, or user description [6]

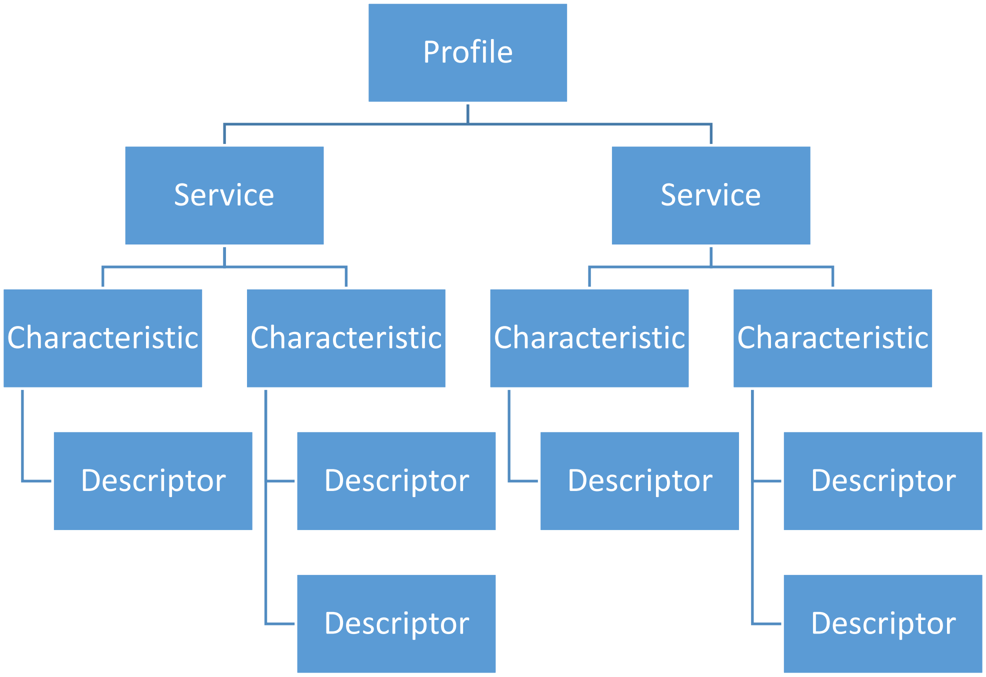


Fig. 5-1 BLE profile hierarchy

5.1.1 RSSI Experiment

An experimental demo was done based on “Appendix A. DEMO FOR RSSI BASED DISTANCE ESTIMATION”. Based on that demo, some criteria can be obtained to analyze this method.

To evaluate the performance of distance estimation using the RSSI method, a series of controlled experiments were conducted across three different environments: a large, open room with minimal electromagnetic interference (controlled), a typical office with multiple BLE devices and physical obstructions (office), and a high-interference environment with additional sources of electromagnetic noise and physical clutter (interference).

Fig. 5-2 RSSI vs Distance presents the measured RSSI values as a function of distance, ranging from 1 to 50 meters. The data clearly illustrates a non-linear, logarithmic relationship between distance and signal strength, consistent with theoretical models. In the controlled environment, the RSSI degradation is relatively smooth and gradual, making it suitable for estimation using simple path loss models. However, in the office and interference

environments, the signal strength decays more rapidly and exhibits greater fluctuations. For example, at 8 meters, the RSSI dropped to approximately -16 dB in the controlled environment, while in the interference setup it reached -106 dB. This highlights how multipath propagation and environmental obstructions can drastically impact signal quality and reliability.

Additionally, the collected data demonstrates the limited scalability of RSSI for long-range or high-density deployments, especially under non-ideal conditions. Notably, in the high-interference environment, the RSSI values plateaued beyond 35 meters, indicating a floor in detection sensitivity and increased uncertainty in distance estimation.

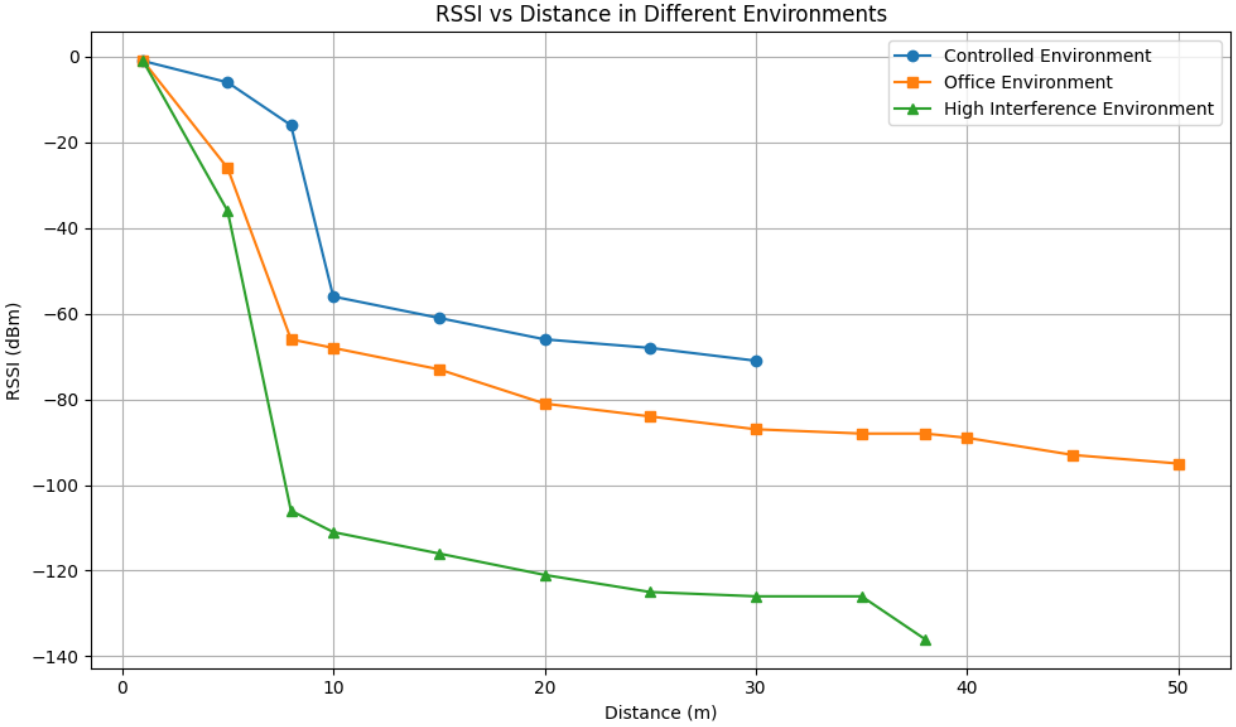


Fig. 5-2 RSSI vs Distance

To complement these findings, an estimation of power consumption was performed using NXP’s Current Consumption Estimator tool. A BLE advertising scenario with parameters matching the experimental setup (advertising at 1 Hz, 0 dBm TX power, default PHY) was simulated. The results indicate an average current draw well below 100 µA, confirming that RSSI-based ranging requires minimal energy. This reaffirms its value for battery-operated devices, such as beacon tags, wearables, and wireless sensors in large-scale IoT deployments.

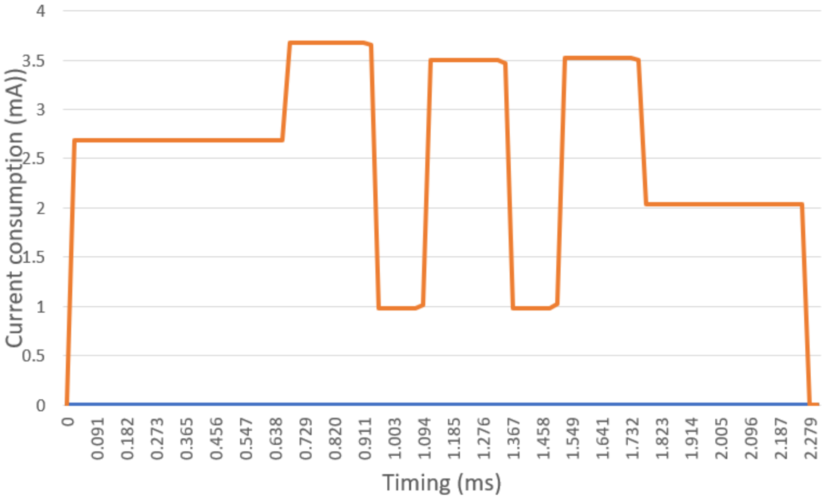


Fig. 5-3 Advertising Profile. Peripheral Device

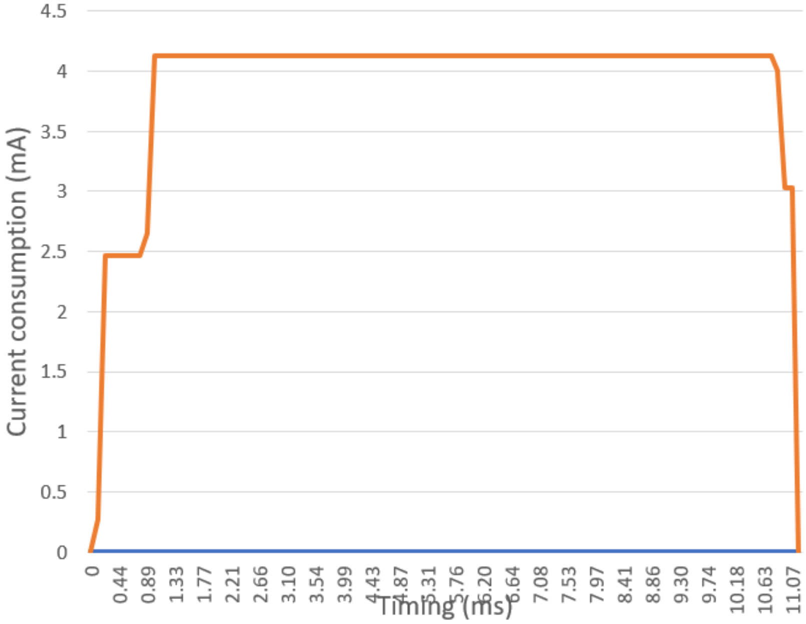


Fig. 5-4 Scan Profile. Central Device

5.1.2 ToF Experiment

During the experimental evaluation of the Time of Flight method, measurements were conducted using the same development board previously used for the RSSI-based experiments.

This board integrates BLE capabilities and allows the use of the LPIT (Low-Power Periodic Interrupt Timer), which provides microsecond-level resolution. This precision enables the system to theoretically resolve distances as small as approximately 1.5 meters, considering the speed of light and the round-trip time (RTT) model. Due to this limitation, measurements below 2 meters were not considered.

In practice, tests were performed in an office environment, which introduced considerable electromagnetic interference and physical obstructions. In the range between 2 and 8 meters, results showed relative consistency, and distance estimations were coherent with the expected values. However, even within this initial range, a small number of incorrect time measurements began to appear, likely due to transient radio interference or reflections. These erroneous values should be identified and filtered out to recover a more reliable estimation. As distance increased, these anomalies became more frequent and pronounced, making filtering and post-processing essential to maintain accuracy in a final application. Beyond 8 meters, instability became more significant, with a rise in packet loss and time values that were far from the expected RTT, making consistent measurement more difficult.

One of the contributing factors to this behavior is the shared use of the same clock domain for both the BLE radio subsystem and the LPIT. This architectural constraint may introduce timing conflicts at the application level, particularly during transmission and reception events, which are sensitive to clock phase alignment. In high-interference environments, such interactions can further distort ToF measurements. It is worth noting that this BLE radio also supports the use of an alternate timestamping mechanism that operates independently from the radio clock domain. However, this alternative provides timestamps with millisecond resolution, which corresponds to a theoretical distance resolution of approximately 150 kilometers. While useful for certain low-speed timing applications, this granularity is clearly unsuitable for short-range ranging tasks. Moreover, maintaining a BLE connection over such large distances is not physically feasible, as BLE is typically limited to tens of meters even under optimal conditions.

Complementing the evaluation, a power consumption estimate was performed using the same tool, simulating a BLE connection scenario with regular RTT exchanges. The current consumption profile showed a significant increase compared to the advertising-only case, with peaks occurring during packet transmission and reception. Despite this, the average current remained within reasonable bounds for typical BLE-connected devices, indicating that while ToF introduces greater energy demands, it remains viable for mid-power applications requiring improved accuracy.

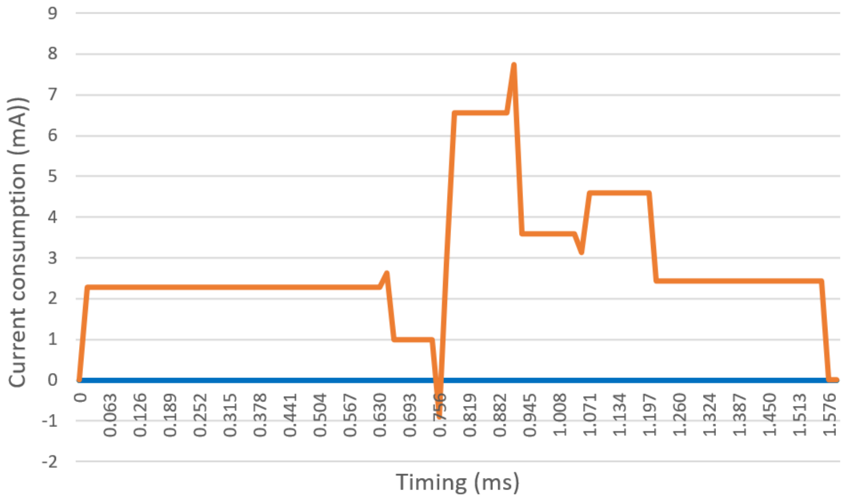


Fig. 5-5 Connection Profile. Peripheral Device

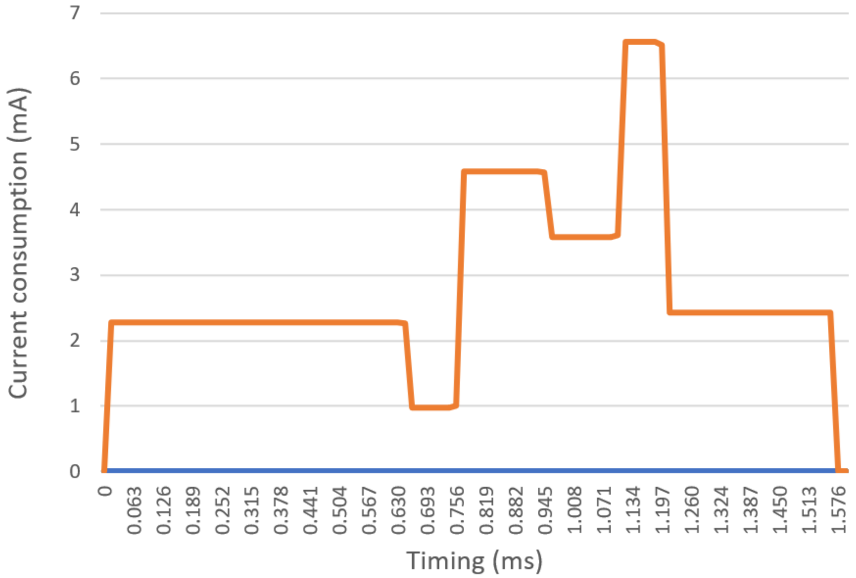


Fig. 5-6 Connection Profile. Central Device

These observations highlight the challenges of implementing precise timing-based distance estimation in constrained embedded systems and reinforce the importance of careful clock configuration and post-processing. For more details regarding the software implementation and hardware configuration used in this demonstration, please refer to “Appendix B. DEMO FOR TOF BASED DISTANCE ESTIMATION”.

5.1.3 Angle of Arrival (AoA) Reference

Due to hardware constraints, direct experimentation with Angle of Arrival (AoA) was not feasible in this study. Instead, this section summarizes findings from a related implementation that illustrates the practical use of AoA with BLE for localization.

The referenced system employs a circular antenna array composed of eight evenly spaced elements arranged at 45° intervals. Using BLE 5.1 Direction Finding capabilities, the receiver cycles through these antennas during the Constant Tone Extension (CTE) of a BLE packet. This sequential sampling allows the collection of phase information used to compute the angle of arrival based on phase differences between neighboring antennas.

The system operated with a 4 µs switching period and a 500 ns sampling rate, capturing eight samples per antenna per CTE. However, tests revealed that only a subset of these samples provided reliable phase data. Consequently, only the second through fourth samples were used for further analysis to reduce the impact of switching artifacts.

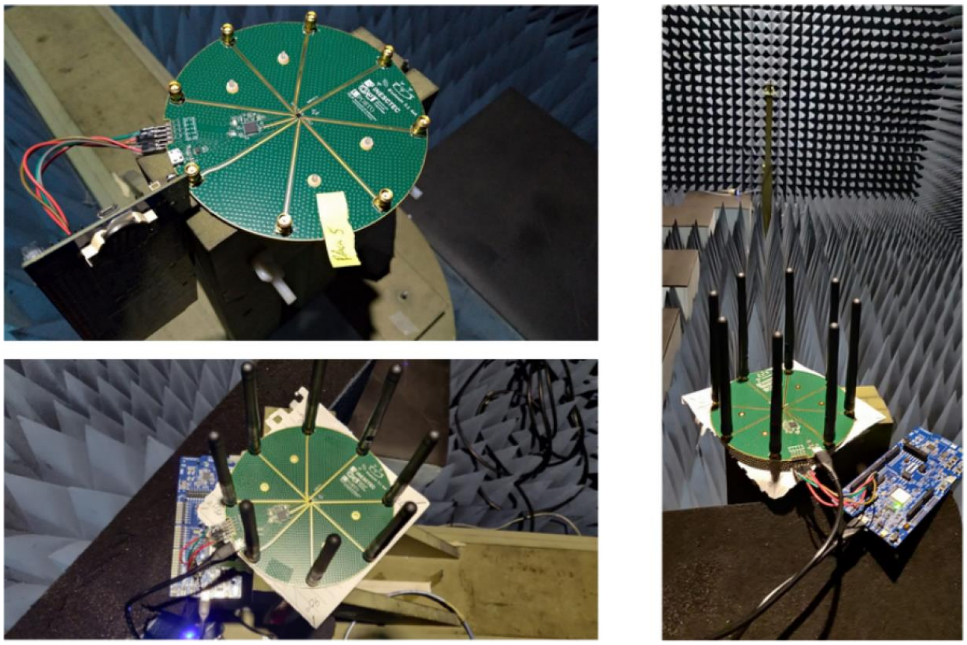


Fig. 5-7 Third Party Fabricated board design and setup [7]

Initial validation in a controlled environment confirmed the expected behavior of the system. The sinusoidal profile of phase differences was consistently observed across multiple orientations, demonstrating the accuracy and stability of the approach under ideal conditions.

In real-world field tests, the AoA estimation showed greater variability due to environmental factors such as multipath propagation and signal noise. Even so, it was possible to extract meaningful phase difference profiles by applying statistical processing techniques like averaging and histogram filtering. These approaches helped isolate the dominant values and mitigate the effects of measurement noise.

The evaluation demonstrated that accurate AoA estimation is achievable when the receiver remains stationary and a sufficient number of packets are collected. This highlights the importance of temporal data aggregation and the limitations of single-packet localization attempts, particularly in outdoor or reflective environments.

Ultimately, this external implementation confirms that AoA techniques in BLE systems are effective under the right conditions and with appropriate processing strategies. It also reinforces the need for careful consideration of signal quality and processing constraints when deploying AoA for indoor or context-aware localization applications.

5.1.4 Channel Sounding (CS) Reference

Due to the current limitations on sharing experimental results from ongoing internal tests involving Channel Sounding (CS), this section presents evidence from a public demonstration released by NXP Semiconductors. In this demonstration, part of NXP's Smarter World Video Series, project manager Donnie Garcia introduces BLE Channel Sounding technology as implemented in early versions of the MCXW and KW47 MCU platforms. [8]

The demonstration features two setups. The first uses NXP's Localization SDK to evaluate different embedded localization algorithms. The SDK enables developers to quickly run localization experiments and record data for offline analysis. The second setup is a more curated scenario with five localization boards, where four act as initiators performing round-robin channel sounding exchanges with a reflector board. This arrangement enables measurement updates every 0.25 seconds and supports high-throughput distance estimation. The speaker emphasizes how this approach facilitates triangulation and directional estimation due to the increased number of measurement perspectives.

These demonstrations validate the feasibility and performance potential of BLE Channel Sounding, particularly in complex indoor environments. All tests were conducted on early hardware and software versions, with references to the upcoming MCXW72 platform, which is expected to provide production-ready support for CS.

In addition to the previously discussed demonstration, NXP has released another video showcasing the practical application of Bluetooth Channel Sounding using their MCX W series microcontrollers. This demonstration illustrates how two devices equipped with MCX W MCUs can accurately measure the distance between them using Bluetooth Channel Sounding technology. The video emphasizes the MCX W's capability to perform precise distance measurements, highlighting its potential in various applications such as smart home devices and building automation systems. [9]

The demonstration underscores the MCX W's integration of a dedicated Localization Compute Engine, which enhances the efficiency and accuracy of distance measurements by offloading complex calculations from the main processor. This architectural design not only improves performance but also reduces latency, making it suitable for real-time applications.

5.2. Summary

The experimental evaluation of RSSI and ToF methods allowed for a practical analysis of their performance under realistic conditions. RSSI, while simple and broadly compatible, showed high variability and sensitivity to environmental noise. In contrast, ToF offered more consistent results at short ranges but encountered timing instability and increased packet loss with distance, especially in noisy environments.

Indirect references to third-party studies demonstrated the feasibility and potential of AoA and CS under favorable hardware and environmental conditions. AoA can deliver precise angular localization with appropriate filtering, while CS stands out for its high accuracy and robustness in complex scenarios.

These findings reinforce the notion that each BLE-based distance estimation method serves distinct applications. The choice depends on accuracy needs, hardware availability, and operational environment. The next chapter presents concluding remarks and recommendations based on the insights gained throughout this work.

6. Comparison methodologies

When designing location systems, selecting the most suitable distance estimation method is a critical decision that directly affects the system's accuracy, efficiency, and feasibility. Several technical approaches are available, each with its own strengths, limitations, and operational requirements. This section presents a comparison of the methods discussed previously, in the context of Bluetooth Low Energy (BLE).

The second part of this chapter explores real-world applications where different BLE-based distance estimation methodologies are employed. For each method, examples of practical deployments are presented, highlighting the suitability of the technique depending on factors such as accuracy requirements, power consumption, hardware complexity, and environmental conditions.

6.1. Evaluation Criteria

6.1.1 Accuracy

Accuracy refers to how close the estimated distance is to the actual distance between two devices. Among the evaluated methods, Received Signal Strength Indicator (RSSI) offers the lowest accuracy among the evaluated methods. Its estimates can deviate by several meters and are highly susceptible to environmental factors such as signal attenuation, interference, and the presence of dynamic obstacles.

Angle of Arrival (AoA) also provides high accuracy, potentially reaching centimeter-level estimations when implemented with a well-calibrated antenna array and in controlled environments. However, its performance can degrade in the presence of multipath interference or if the antenna geometry is suboptimal.

Time of Flight (ToF) is theoretically capable of accurate measurements, but in practice, its precision often depends on the resolution of internal timers and the implementation's ability to handle short time intervals reliably. Commonly, ToF systems can achieve an accuracy within 1–2 meters.

Channel Sounding (CS) demonstrates the highest accuracy, primarily due to the use of Channel State Information (CSI) and advanced techniques like Round-Trip Time (RTT) and Phase-Based Ranging (PBR). Under optimal conditions, CS can achieve sub-meter or even centimeter-level precision.

TABLE I
ACCURACY COMPARISON

Method	Comparison
RSSI	Low, several meters, highly affected by environment.
AoA	High, centimeters under ideal conditions and good antenna design.
ToF	Moderate, typically 1-2 meters depending on timer resolution.
CS	Very high, sub-meter or centimeter.

6.1.2 Hardware Requirements

Hardware requirements reflect the complexity and specificity of components needed to implement each method. These directly affect cost, integration effort, and feasibility, especially in resource-constrained embedded systems.

Received Signal Strength Indicator (RSSI) stands out as the least demanding in hardware. It leverages standard BLE radios, which typically provide RSSI readings without requiring additional circuitry or calibration. This makes RSSI suitable for simple, low-cost applications, although with a trade-off in performance.

Angle of Arrival (AoA) requires antenna arrays at the receiver side (e.g., access point or anchor node), allowing it to detect phase or time differences between multiple antennas. The transmitter (e.g., a mobile tag) typically only needs a single antenna, which simplifies its design.

However, the receiver must support real-time signal processing and antenna switching, increasing hardware complexity and size.

Time of Flight (ToF) demands precise timing capabilities at both the transmitting and receiving devices. High-resolution clocks, synchronized timers, and low-jitter RF chains are often required, adding to the cost and design constraints. This limits its implementation in ultra-low-power devices.

Channel Sounding (CS), on the other hand, introduces advanced requirements. It depends on Bluetooth LE 6.0-compliant hardware, supporting new physical layer features such as precise phase and timing measurements. These capabilities are typically only available in the latest generation of BLE chipsets, which may not yet be widely deployed.

TABLE II
HARDWARE REQUIREMENTS COMPARISON

Method	Comparison
RSSI	Minimal; supported by standard BLE radios.
AoA	High; requires antenna arrays and signal processing at receiver.
ToF	Moderate to high; requires precise timers and synchronized clocks at both ends.
CS	Very high; needs BLE 6.0 hardware with phase and RTT support.

6.1.3 Power Consumption

Power consumption is a critical factor in the design of location systems, especially for battery-powered devices. Each method has different requirements that affect the energy efficiency of the solution. RSSI has the lowest additional power consumption since it uses passive signal readings. AoA is efficient on the tag side but consumes more power on the anchor due to processing overhead. ToF requires more energy for repeated transmissions and precise timing. Channel Sounding exhibits the highest power demand due to its intensive signal exchange and processing operations.

TABLE III
POWER CONSUMPTION COMPARISON

Method	Comparison
RSSI	Very Low (passive measurement).
AoA	Low on tag, moderate on anchor (processing).
ToF	Moderate to High (timing operations).
CS	High (channel sweeping and processing).

6.1.4 Implementation Cost

Implementation cost plays a key role when selecting a method for commercial or large-scale deployments. RSSI offers the most cost-effective option as it leverages existing BLE capabilities without additional hardware. AoA systems can be more expensive, particularly on the anchor side, due to the need for multiple antennas and additional processing units, although the tag cost remains low. ToF generally increases the system cost as it demands high-precision timers at both the anchor and tag. Channel Sounding is the most expensive in terms of both hardware and software due to its complexity and advanced requirements.

TABLE IV
IMPLEMENTATION COST COMPARISON

Method	Comparison
RSSI	Very Low (uses standard BLE hardware)
AoA	Moderate to High (due to anchor complexity)
ToF	High (requires specialized timing hardware)
CS	Very High (advanced hardware and software)

6.1.5 Robustness to Environmental Conditions

Environmental robustness is critical in real-world deployments where obstructions, multipath propagation, and interference can degrade performance. AoA, although still susceptible to multipath effects, tends to be more robust than RSSI-based methods because it derives position estimates from phase and angular information rather than relying solely on signal amplitude, which is more easily distorted in complex environments.

ToF can suffer in environments lacking a clear line-of-sight, where multipath effects can distort the measured time. Channel Sounding is inherently more resistant to such disturbances, as it analyzes channel characteristics in depth, providing more stable estimates in challenging conditions.

TABLE V
ROBUSTNESS TO ENVIRONMENTAL CONDITIONS COMPARISON

Method	Comparison
RSSI	Low (sensitive to obstructions and interference)
AoA	Moderate (affected by multipath but more robust to signal strength changes)
ToF	Moderate (susceptible to LOS issues and multipath)
CS	High (resistant to interference and multipath)

6.1.6 Implementation and Processing Complexity

Regarding implementation and processing complexity, RSSI stands out as the simplest method to deploy, relying on straightforward propagation models and moderate algorithmic processing for localization. AoA involves more sophisticated signal processing algorithms to calculate the angle of arrival and subsequent position estimation, requiring higher computational resources. ToF implementations demand precise timing measurements and more advanced distance calculation algorithms, making it moderately complex compared to RSSI. Channel Sounding presents the highest complexity level, as it requires the development and integration of advanced algorithms to process detailed channel state information, including phase and timing data.

TABLE VI
IMPLEMENTATION AND PROCESSING COMPLEXITY COMPARISON

Method	Comparison
RSSI	Low (simple propagation models, moderate algorithms)
AoA	High (complex signal processing and angle calculation)
ToF	Moderate (precise timing and distance algorithms)
CS	Very High (advanced channel data processing)

6.2. Method Analysis Summary

Each technique presents unique advantages and trade-offs in terms of accuracy, hardware requirements, power consumption, implementation cost, and processing complexity. While RSSI stands out for its simplicity and cost-effectiveness, it suffers from lower accuracy and environmental sensitivity. AoA improves accuracy significantly but demands more complex hardware and algorithms. ToF offers promising precision but at the expense of specialized hardware and power consumption. Channel Sounding, the most recent advancement, achieves the highest accuracy by leveraging phase and timing measurements but requires advanced BLE 6.0 hardware and sophisticated processing. Ultimately, the choice of method depends on the specific application requirements, balancing system performance, cost, and complexity.

6.3. Real-World Applications of Distance Estimation Methods

6.3.1 RSSI Applications

RSSI-based distance estimation is widely used in asset tracking and inventory management systems where cost-efficiency and low power consumption are critical. Its simplicity allows integration with standard BLE devices without additional hardware, making it suitable for large-scale deployments with moderate accuracy requirements.

In retail and warehouse environments, BLE beacons using RSSI can help locate pallets or individual items, improving inventory accuracy and streamlining logistics. In smart homes and buildings, RSSI can enable presence detection and basic localization for automation tasks like lighting control or energy optimization.

In healthcare, RSSI is often applied in patient tracking or equipment location systems within hospitals. These deployments prioritize low-power operation and scalability over fine-grained accuracy, making RSSI a natural fit.

Several commercial and research solutions leverage RSSI for Bluetooth-based localization due to its simplicity, low power consumption, and compatibility with widely available BLE hardware.

One example is Kontakt.io, which provides BLE-based asset tracking and proximity alert systems, particularly in healthcare and logistics environments. Their solution includes mobile SDKs and a location engine to process RSSI values from BLE beacons [10].

In the research domain, IndoorAtlas offers hybrid localization techniques combining BLE RSSI and ambient magnetic field mapping. Their platform is used in airports and museums to guide visitors and improve location-based services [11].

These examples demonstrate that RSSI-based methods, though less accurate than phase- or time-based techniques, are still widely adopted in applications where cost, battery life, and deployment scalability are more critical than sub-meter accuracy.

6.3.2 ToF Applications

ToF is favored in indoor navigation and robotic applications that demand higher accuracy than RSSI can provide. The need for precise timing hardware and increased power consumption is justified by the performance gains.

Autonomous mobile robots (AMRs) in industrial settings often rely on ToF to maintain precise location awareness while navigating dynamic environments. Similarly, drones use ToF for safe flight in GPS-denied environments such as indoor warehouses or tunnels.

Consumer electronics, such as smart door locks or security cameras, may use ToF to estimate distance to users or objects for improved contextual behavior. In augmented reality (AR), ToF can contribute to spatial mapping and accurate gesture tracking.

Time-of-Flight (ToF) techniques are increasingly used in indoor navigation and automation systems where BLE alone might be insufficient. Companies like Minew and Qorvo have explored localization solutions that include ToF as a complement to BLE to improve accuracy in industrial and healthcare environments [12] [13].

6.3.1 AoA Applications

AoA is gaining traction in use cases requiring precise directional information, such as proximity-based services, indoor positioning systems, and location-aware marketing.

In retail, AoA enables hyper-localized promotions—detecting which product a shopper is approaching. In museums or event spaces, AoA can drive interactive experiences that adapt based on the visitor's direction and location. Hospitals and smart buildings benefit from AoA by guiding staff or visitors with real-time directions based on high-resolution localization.

Logistics and warehouse automation systems use AoA to track assets or mobile robots with fine granularity, enabling optimal resource planning and rapid response to system changes. Quuppa is one of the most prominent commercial solutions leveraging BLE AoA, offering centimeter-level positioning for sports analytics, industrial safety, and healthcare asset tracking [14].

AoA is particularly well suited for applications such as visitor analytics in museums, worker positioning in smart factories, and proximity detection in access control systems.

6.3.2 CS Applications

CS methods are particularly advantageous in high-interference environments or security-critical applications. For example, passive keyless entry systems in the automotive industry use CS to achieve centimeter-level accuracy and robust performance.

6. COMPARISON METHODOLOGIES

In building access control, CS can verify the proximity of authorized personnel with high confidence, even in environments crowded with wireless signals. In industrial monitoring, CS supports the real-time tracking of equipment or materials in RF-dense facilities.

Emerging use cases include augmented reality headsets and gaming platforms, where CS enables precise motion tracking. Smart cities can also benefit from CS through infrastructure monitoring and intelligent traffic flow estimation.

Although BLE 6.0's Channel Sounding (CS) has been standardized—with many semiconductor manufacturers (NXP Semiconductor, Silicon Labs, etc.) providing dev kits and stacks—commercial consumer devices explicitly incorporating CS (e.g., trackers, smart keys, mice) have not yet been released as of mid-2025.

Conclusions

This case study explored the application of Bluetooth Low Energy (BLE) for indoor distance estimation, focusing on four key methodologies: Received Signal Strength Indication (RSSI), Time of Flight (ToF), Angle of Arrival (AoA), and Channel Sounding (CS). By integrating theoretical analysis, BLE protocol architecture, and practical evaluations, the study provided a structured and comprehensive view of how these techniques function and perform in embedded systems for localization.

Each method was thoroughly analyzed in terms of implementation complexity, accuracy, hardware requirements, and environmental sensitivity. The experimental results obtained using NXP's MCX W71x platform validated the behavior of RSSI and ToF under real-world conditions. These tests highlighted the simplicity and low energy consumption of RSSI, as well as the improved precision but increased complexity of ToF. On the other hand, the inclusion of AoA and CS was supported through referenced third-party demonstrations, offering evidence of their potential in high-accuracy positioning applications, albeit with more demanding hardware and processing needs.

A comparative analysis revealed that no single method is universally optimal; rather, the choice of technique must be based on specific application requirements such as accuracy, range, cost, and energy constraints. For instance, RSSI remains attractive for low-cost and low-power scenarios, while CS shows promising capabilities for next-generation precision systems where sub-meter resolution is essential.

Some limitations were identified during the development of this study. The inability to perform direct testing with AoA and CS due to hardware constraints limited the scope of hands-on experimentation. Moreover, the early-stage nature of CS support in BLE 6.0 platforms restricted the ability to validate its full performance in practical deployments.

Despite these limitations, the study achieves its primary goal: to provide a deep and practical understanding of BLE-based distance estimation techniques. It serves as a guide for designers and researchers who aim to implement indoor positioning systems using BLE, offering a clear view of the trade-offs involved in each approach.

Future work may involve the implementation of AoA or CS in real scenarios as soon as commercial hardware becomes available, as well as the exploration of hybrid approaches that combine multiple estimation techniques to improve robustness and precision. Additionally, the integration of machine learning algorithms for signal filtering and error correction presents an attractive opportunity for enhancing localization accuracy in complex environments.

In conclusion, this work underscores the versatility of BLE as a platform for indoor localization and highlights the richness of technical options available to address the growing demand for accurate, efficient, and cost-effective positioning systems.

Appendix

A. DEMO FOR RSSI BASED DISTANCE ESTIMATION

The demo application was made taking as a base the Wireless UART FreeRTOS from the SDK (MCUXpresso SDK Builder) version 25.03.00

The Wireless UART service is a custom service that implements a custom writable ASCII Char characteristic that holds the character written by the peer device.

This application was made to support multiple connections, as GAP central or peripheral mode, and this is the reason of taking this example as a base.

Board that can used:

- KW45-EVK
- KW45-LOC
- FRDM-MCXW71

Software

The main changes that were make are related to the call of "requesting" the RSSI of a radio connection. This is made through an API that reads the power level of the controller's radio. (Gap_ReadRadioPowerLevel(gRssi_c, (deviceId)))

Calling this API, the response is contained in the gConnEvtTxPowerLevelRead_c connection event when reading connection TX power level, the gAdvTxPowerLevelRead_c generic event when reading gConnEvtRssiRead_c connection event when reading the RSSI.

Because of the handling of the Wireless UART application, we are calling this API every time we are receiving a message from the Client, specifically on the gEvtAttributeWrittenWithoutResponse_c event.

Then, the BLE stack will process the request, and we can have the RSSI value when having a gConnEvtRssiRead_c event on the BleApp_ConnectionCallback. We read the RSSI value on the pConnectionEvent->eventData.rssi_dBm.

Hardware

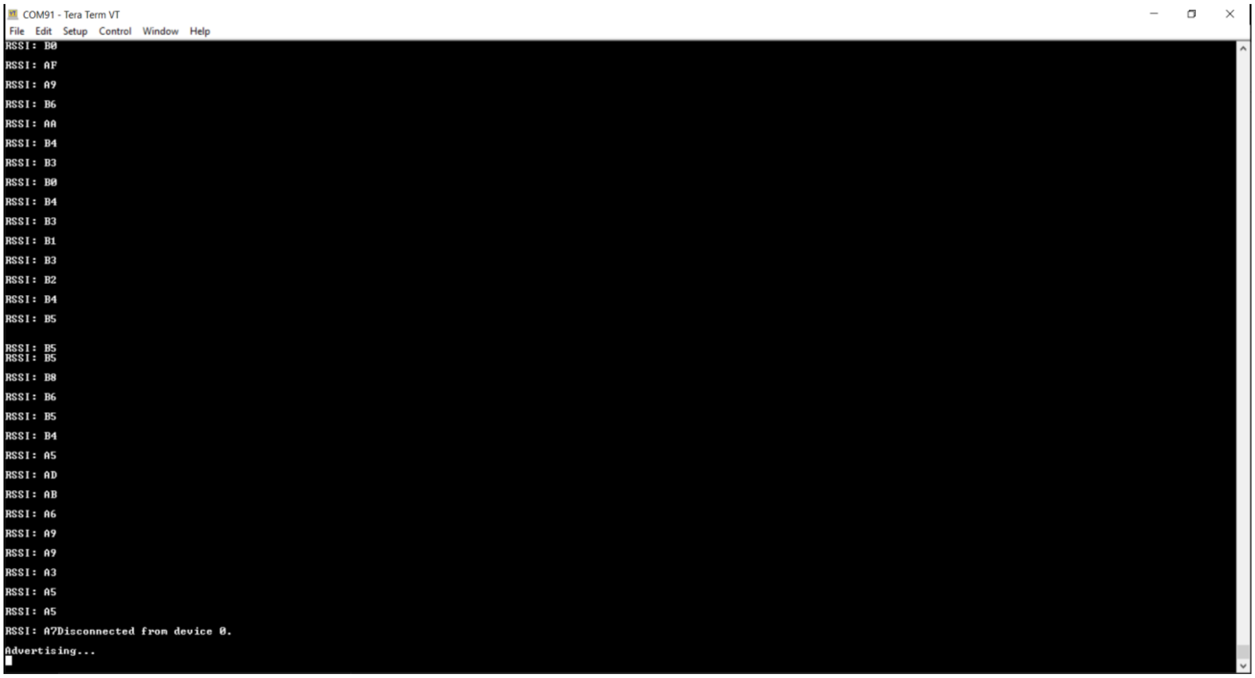
No special hardware change is required when working with the mentioned boards.

Setup

For the test, one board is used as GAP Peripheral that is advertising for stablishing a connection, and a smartphone is used as GAP Central that is scanning for stablishing a connection.

Every time the smartphone sends a character, a RSSI measurement will be triggered.

Results



```
RSSI: B0
RSSI: AF
RSSI: A9
RSSI: B6
RSSI: AA
RSSI: B4
RSSI: B3
RSSI: B0
RSSI: B4
RSSI: B3
RSSI: B1
RSSI: B3
RSSI: B2
RSSI: B4
RSSI: B5

RSSI: B5
RSSI: B5
RSSI: B8
RSSI: B6
RSSI: B5
RSSI: B4
RSSI: A5
RSSI: AD
RSSI: AB
RSSI: A6
RSSI: A9
RSSI: A9
RSSI: A3
RSSI: A5
RSSI: A5
RSSI: A7Disconnected from device 0.
Advertising...
```

Fig. A-6-1 Results for RSSI demo

B. DEMO FOR TOF BASED DISTANCE ESTIMATION

The demo application was made taking as a base the Wireless UART FreeRTOS from the SDK (MCUXpresso SDK Builder) version 25.03.00

The Wireless UART service is a custom service that implements a custom writable ASCII Char characteristic that holds the character written by the peer device.

This application was made to support multiple connections, as GAP central or peripheral mode, and this is the reason of taking this example as a base.

Board that can used:

- KW45-EVK
- KW45-LOC
- FRDM-MCXW71

Software

The first step was to enable the Controller Adv/Scan/Connection Notification, defining the gUseControllerNotifications_c macro.

With this, we are able to receive "extra information" on the Function handling the Bluetooth Controller notification events: BleApp_HandleControllerNotification.

After enabling this, depending on the role the application is running (Central or Peripheral), the corresponding notifications are enabled.

When this function is called, we can "react" depending on the specific notification. For this demo, we are focusing on the "gNotifConnRxPdu_c". Here we are able to check a specific value that is needed for ToF, the Timestamp in microseconds, valid for Conn Rx event and Conn Created event.

To "measure" the ToF, we need to modify the application, so the node can send/respond just after receiving an specific message.

To have the good measurements, we need to integrate the LPIT (Low Power Interrupt Timer) module to enable high-resolution timing, and with it measure the time on the

BleApp_HandleControllerNotification, and calculate de time between the time T1 (Sent from Node A), and the T4 (Response received at Node A).

Hardware

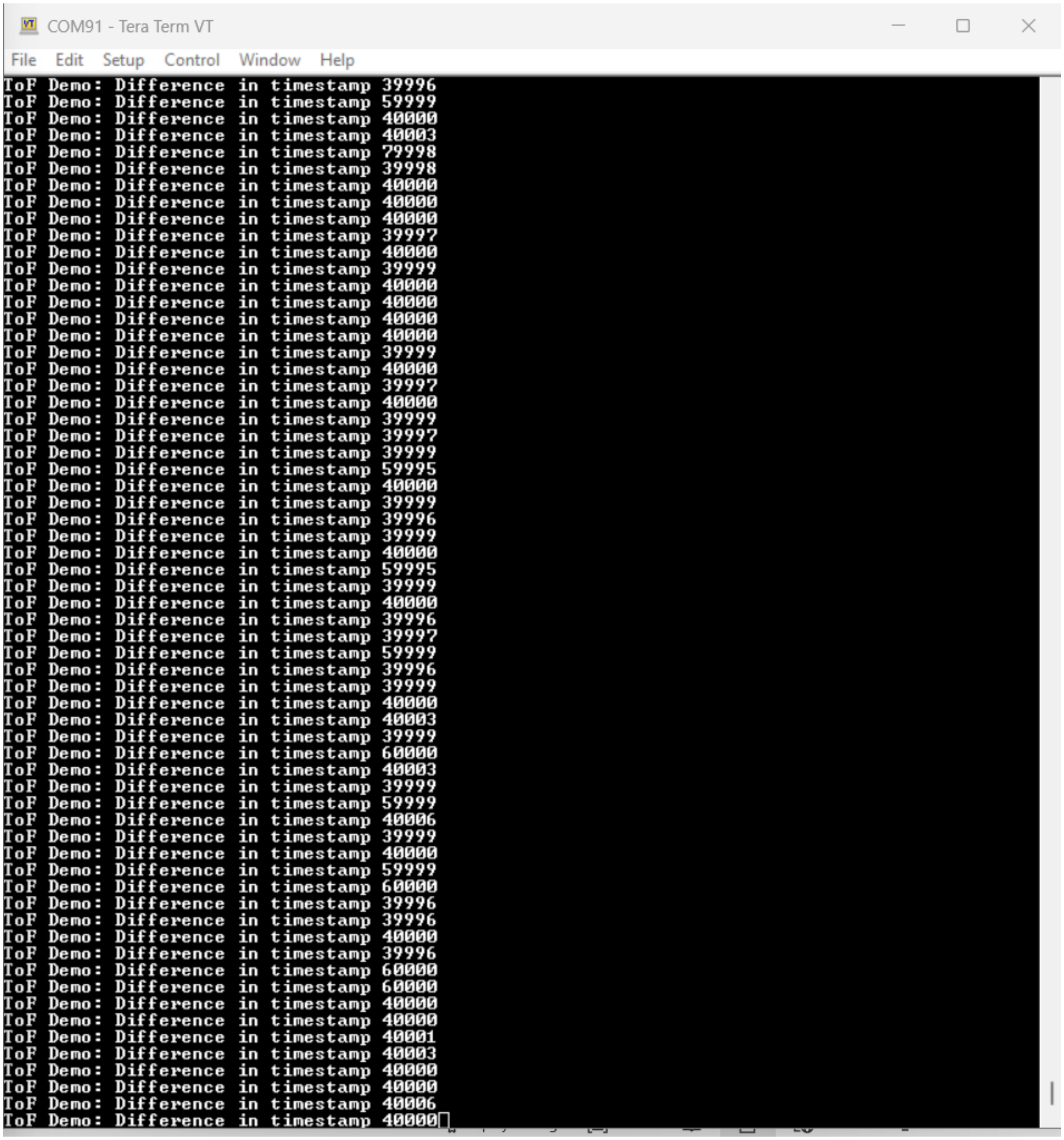
No special hardware change is required when working with the mentioned boards.

Setup

For the test, one board will be the Central device (Anchor) and the other will be the Peripheral (Tag). After stablishing the connection, the Anchor will send a message to the Tag, and will respond to this message, so the Anchor can measure the time between his transmission, and the reception of the response.

Results

With the setup, we can see a periodic measurement of time for the connection between the anchor and the tag:



```
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 59999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40003
ToF Demo: Difference in timestamp 79998
ToF Demo: Difference in timestamp 39998
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39997
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39997
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 39997
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 59995
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 59995
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 39997
ToF Demo: Difference in timestamp 59999
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40003
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 60000
ToF Demo: Difference in timestamp 40003
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 59999
ToF Demo: Difference in timestamp 40006
ToF Demo: Difference in timestamp 39999
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 59999
ToF Demo: Difference in timestamp 60000
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 39996
ToF Demo: Difference in timestamp 60000
ToF Demo: Difference in timestamp 60000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40001
ToF Demo: Difference in timestamp 40003
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40000
ToF Demo: Difference in timestamp 40006
ToF Demo: Difference in timestamp 40000
```

Fig. B-1 Results for ToF demo

Based on this, we can estimate the distance between one anchor and the tag.

References

[1] D. Munoz, F. B. Lara, C. Vargas and R. Enriquez-Caldera, Position Location Techniques and Applications, 2009.

[2] J. Hillyard, C. Bachmann and L. Huang, "Bluetooth® Channel Sounding – A Step Towards 10-cm Ranging Accuracy for Secure Access, Digital Key, and Proximity Services," 2023. [Online]. Available: https://www.bluetooth.com/blog/bluetooth-channel-sounding-a-step-towards-10-cm-ranging-accuracy-for-secure-access-digital-key-and-proximity-services/.

[3] R. Rathnayake, M. Maduranga, V. Tilwari and M. Dissanayake, "RSSI and Machine Learning-Based Indoor Localization Systems," 2023.

[4] D. Giovanelli, "Bluetooth Low Energy based proximity detection," 2019.

[5] NXP Semiconductors, "MCX W71x Secure and Ultra-Low-Power MCUs for Matter, Thread, Zigbee and Bluetooth LE," [Online]. Available: https://www.nxp.com/products/MCX-W71X.

[6] R. Zamora, "KW38 Custom Profile," 2021. [Online]. Available: https://community.nxp.com/t5/Wireless-Connectivity-Knowledge/KW38-Custom-Profile/ta-p/1269874.

[7] N. Paulino, L. M. Pessoa, A. Branquinho and E. Goncalves, "Design and Experimental Evaluation of a Bluetooth 5.1 Antenna Array for Angle-of-Arrival Estimation".

[8] D. Garcia, "Channel Sounding - the Latest in Bluetooth 6," NXP Semiconductors, 2024. [Online]. Available: https://www.nxp.com/company/about-nxp/smarter-world-videos/CHANNEL-SOUNDING-VID.

[9] O. Usturoi, "KW45 Based CS 1 to Many Demo," 2024. [Online]. Available: https://www.youtube.com/watch?v=y0MF0UTj4Ks.

[10] Kontakt.io, "Kontakt.io BLE Beacons and IoT Location Engine," [Online]. Available: https://kontakt.io/.

[11] IndoorAtlas, "Magnetic and BLE-based Indoor Positioning," [Online]. Available: https://www.indooratlas.com/.

[12] Minew, "RTLS Indoor Positioning," [Online]. Available: https://www.minew.com.

[13] Qorvo, "Ultra-Wideband and BLE Solutions for Asset Tracking," [Online]. Available: https://www.qorvo.com.

[14] Quuppa, "Intelligent Real-Time Locating Systems," [Online]. Available: https://www.quuppa.com.

[15] Z. Wang, "Securing Bluetooth Low Energy: A Literature Review," Harbin University of Science and Technology, 2017.

[16] C. Gentner, D. Gunther and P. H. Kindt, "Identifying the BLE Advertising Channel for Reliable Distance Estimation on Smartphones".

[17] G. F. Hatke, M. Montanari, S. Appadwedula, M. Wentz, J. Meklenburg, L. Ivers, J. Watson and P. Fiore, "Using Bluetooth Low Energy (BLE) Signal Strength Estimation to Facilitate Contact Tracing for COVID-19," MIT Lincoln Laboratory,.

[18] G. Retscher, P. Zariqi, A. O. P. Pachon, J. P. C. Cantu and S. Madawalagama, "Bluetooth Distance Estimation for COVID-19 Contact Tracing," Vienna University of Technology, 2021.

[19] B. Etzlinger, B. Nußbaummüller, P. Peterseil and K. A. Hummel, "Distance Estimation for BLE-based Contact Tracing – A Measurement Study," Johannes Kepler University.

[20] "Bluetooth LE eChannel Sounding Content," NXP Community, 2025. [Online]. Available: https://community.nxp.com/t5/Wireless-Connectivity-Knowledge/Bluetooth-LE-eChannel-Sounding-Content/ta-p/2050341.