Bridge: Enabling BLE Direction Finding Feature Compatible with All Bluetooth Devices

Runting Zhang[1†], Yijie Li[2†], Dian Ding[1*], Yi-Chao Chen[1*], Yida Wang[1], Dongyao Chen[1], Jingxian Wang[2], Jiadi Yu[1], Ling Ma[1], Guangtao Xue[1,3]

[1]Shanghai Jiao Tong University, [2]National University of Singapore, [3]Shanghai Key Laboratory of Trusted Data Circulation and Governance, and Web3

johnson_zrt@sjtu.edu.cn,yijieli@nus.edu.sg,{dingdian94,yichao,yidawang,chendy}@sjtu.edu.cn,wang@nus.edu.sg,{jiadiyu,maling920827,gt_xue}@sjtu.edu.cn

ABSTRACT

Bluetooth-based location services have experienced significant growth over the past decades. RSSI-based techniques using beacons only provide meters-level accuracy. Angular-based approaches rely on customized antenna arrays, introducing high costs and limited usability. In 2020, Bluetooth Special Interest Group (Bluetooth SIG) released version 5.1, integrating Angle of Arrival (AoA) estimation to enable direction finding capabilities, which has the potential to improve localization across various fields, including logistics and industry. However, more than 4.1 billion devices (68% of the total) still do not support the direction finding feature. To address this issue and ensure backward compatibility, we proposed Bridge, a solution that leverages an additional trigger node (referred to as Trigger) to make the direction finding feature compatible with all Bluetooth devices without requiring modifications to existing hardware or firmware. The Trigger mimics communication behaviors with both locators and targets simultaneously by sending a nesting packet. Subsequently, processes and algorithms are delicately designed to estimate AoA. Bridge also supports large-scale deployment through dynamic packet flow switching, enabling it to handle concurrent targets and manage handover with a consistent operation pattern. We implemented and evaluated Bridge in real-world scenarios. The system achieved an average localization error of 33.4*cm* while extending the direction-finding feature to 10 target devices of different Bluetooth versions, indicating the effectiveness of Bridge.

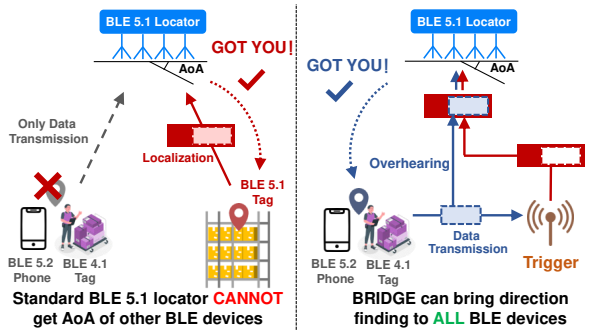


Figure 1: Bridge utilizes an additional trigger node to make the official direction finding feature in BLE v5.1 compatible with other versions of Bluetooth devices. It enables the localization of any Bluetooth device through deployed BLE v5.1 locators.

CCS CONCEPTS

• **Networks** → **Location based services**;

KEYWORDS

BLE Direction Finding, Localization

ACM Reference Format:

Runting Zhang[1†], Yijie Li[2†], Dian Ding[1*], Yi-Chao Chen[1*], Yida Wang[1], Dongyao Chen[1], Jingxian Wang[2], Jiadi Yu[1], Ling Ma[1], Guangtao Xue[1,3]. 2025. Bridge: Enabling BLE Direction Finding Feature Compatible with All Bluetooth Devices. In *The 31st Annual International Conference on Mobile Computing and Networking (ACM MOBICOM '25), November 4–8, 2025, Hong Kong, China.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3680207.3723466

1 INTRODUCTION

Indoor localization techniques have long attracted attention to enable location-based services. Numerous approaches

†Authors contributed equally to this research. * Corresponding author.

ACM MOBICOM '25, November 4–8, 2025, Hong Kong, China

ACM ISBN 979-8-4007-1129-9/2025/11…$15.00
https://doi.org/10.1145/3680207.3723466

based on wireless protocols have been proposed including WiFi [28, 34, 44, 45, 77, 88, 93, 94], Bluetooth [4, 10, 12, 46, 50], ZigBee [38], Ultra Wide Band (UWB) [3, 95], and Radio Frequency Identification (RFID) [25]. Among these, Bluetooth and WiFi technologies stand out due to their broad infrastructure deployment and widespread support. WiFi can achieve high-precision performance through integrated channel state information (CSI) tools in commercial access points (APs), however, few products support this feature, and continuous scanning requires significant power consumption.

In comparison, Bluetooth, particularly with the advent of Bluetooth Low Energy (BLE), offers lower power consumption. Traditional BLE localization approaches are primarily divided into two categories. One leverages received signal strength (RSSI) propagation models [4, 10, 46, 50] or fingerprints [24, 65, 66, 81] with pre-deployed beacons (e.g., ibeacon [4]), which typically achieve only meter-level accuracy. With the growing demand for high accuracy in IoT scenarios, especially in industrial asset tracking and automation applications, researchers are devoted to using multi-input and multi-output (MIMO) capable software-defined radio (SDR) [18, 54] or SDR with customized antenna arrays [31, 67, 79] to measure angle-of-arrival (AoA) for improved localization precision (i.e., decimeter-level accuracy). However, these methods incur high additional costs and reduce usability. In summary, BLE has historically lacked an integrated high-precision localization solution.

To address this problem, the Bluetooth SIG introduced an updated version (v5.1) in 2020, which includes a novel feature termed "**direction finding**" [6, 80]. This feature leverages a switched antenna array integrated into locators to estimate AoA, offering benefits such as high integration, ease of deployment, and enhanced accuracy. Since its release, numerous indoor positioning systems based on BLE 5.1 direction finding have been widely implemented across various sectors, including logistics [22, 29, 40, 43, 53, 78, 84, 86], industry [1, 5, 19, 23, 39, 41, 56, 83, 90], healthcare [36, 37, 63], retail [20, 82], events [57, 58, 89], and other areas [9, 18, 27, 64, 70, 96]. However, over 4.1 billion BLE devices, constituting approximately 68% of the market [7], remain incompatible with BLE direction finding due to the new packet structure updates [6]. These devices, spanning both older and newer BLE versions, cannot adapt to direction finding service through software or firmware updates [52, 61]. The substantial costs and impracticalities associated with replacing either the existing infrastructure of these localization systems or the chips pose significant challenges. This leads to a crucial question: *"Can we make direction finding compatible with all BLE devices without modifying or replacing the existing hardware or firmware?"*

To answer this question, we present Bridge, a novel system that employs an additional node (named Trigger) to enable the already deployed *locators* with the direction finding feature to locate unsupported BLE *targets*, shown as Fig. 1. Trigger is a fully controlled device with BLE signal sending and receiving capabilities (e.g., SDR with limited antennas or BLE development board) that can communicate with both the locator and target, breaking through the limitation of direction finding function. In practice, we have overcome the following **challenges** to realize Bridge:

#1. How to imitate the direction finding process without modifying the hardware or firmware of existing locators and targets across different BLE versions?

To enable direction finding capabilities for originally unsupported devices, Trigger must facilitate communication with both locators and targets. It allows locators to concurrently receive direction finding packets from Trigger and sample signals from targets. This simultaneous communication, however, presents a significant challenge due to the temporal overlap caused by the strict time constraint inherent in the direction finding process. To address this issue, we designed the **nesting packet** (Sec. 5), aiming to carry out payloads for different receivers simultaneously. Nesting packet involves two features: 1) it embeds two distinct packets into a single transmission, thereby ensuring the preservation of all necessary content and structural integrity of the original packets. 2) it should follow BLE bit stream processing to guarantee error checking and time alignment. Through the implementation of nesting packets, we facilitate a process known as **overhearing**, where the signal sampled by the locator will be partially substituted by the packet from the target during the sampling period. This mechanism effectively supports a "bridged" direction finding functionality.

#2. How to achieve AoA estimation via overhearing in a "bridged" direction finding feature?

Although overhearing is established, conventional AoA estimation fails due to several factors: First, the arrival time of the overhearing deviates, and overhearing only occurs within a specific period (not the entire CTE period as normal). Second, the phase of the signal from the target differs from the standard CTE (with constant frequency) in traditional direction finding, hindering the execution of standard reference cancellation and carrier frequency offset (CFO) estimation. Third, the "bridged" direction finding process is prone to mutual RF interference and multi-path effects, raising system robustness issues.

To address the above issues, we first proposed an amplitude difference-based dynamic threshold to perform preliminary screening, followed by a differential phase derivative correlation to eliminate spatial variations and achieve accurate arrival time estimation (Sec. 6.1.1). Next, reference cancellation is conducted through a generated ideal signal with known phase information (Sec. 6.1.2). For CFO estimation, we proposed a 2-stage process to handle arrival fluctuations

relative to the reference period (Sec. 6.2). Finally, we introduced an antenna-level multi-packet combination along with a sampling control algorithm to mitigate the interference and ensure robust communication (Sec. 6.3).

#3. How to achieve large-scale deployment?

A single Trigger can cover up to 20 locators, allowing for large-scale deployment with minimal additional hardware installation. To enhance scalability, we first propose a dynamic packet flow switching mechanism to support concurrent targets based on the Trigger threshold and target quantities. Additionally, we apply an identical operation pattern across all Trigger to handle the handover problem (Sec. 7). We implemented Bridge in real-world scenarios, and saves up to 53.3% cost compared to existing SDR solutions.

To the best of our knowledge, Bridge is the first system to make the official direction finding feature compatible with every Bluetooth device. Extensive real-world experiments show a 33.4cm average localization error. The results indicate that Bridge empowers high-precision localization, not limited to officially supported devices, with performance close to that of standard systems.

Our contributions can be summarized as follows:

- We proposed Bridge, the first system that makes the BLE official direction finding feature compatible with every Bluetooth device without requiring any hardware or firmware modifications by using a trigger node.
- We carefully designed a nesting packet for the trigger node to carry out necessary payloads to mimic communication behaviors with both locators and targets.
- We developed a series of processes and algorithms to accurately estimate AoA in the presence of dynamic packet arrival and interference.
- We introduced approaches to support concurrent targets, address handover issues, and enable cost-effective large-scale deployment.
- We implemented Bridge in real-world scenarios, demonstrating that it can achieve a 33.4cm localization accuracy.

2 RELATED WORK

Radio Frequency (RF) Based Localization. The increasing demand for location-aware services has spurred proposals for numerous RF-based localization techniques, utilizing WiFi [28, 34, 44, 45, 77, 88, 93, 94], Bluetooth [4, 10, 12, 46, 50], ZigBee [38], UWB [3, 95], and RFID [25]. Due to its ubiquity, WiFi-based techniques [28, 34, 44, 45, 77, 88, 93, 94] are flourishing, leveraging commercial APs and using channel state information (CSI) [34, 93] to realize high-precision by specific network interface tools (e.g., Intel WiFi Link 5300 radios [34]). However, only a few commercially available products possess such chipsets. Some effort [30, 69] attempts to implement CSI for other chipsets, but the hardware needs to be modified. Moreover, continuous WiFi scanning causes more power consumption [60].

In contrast, BLE's low cost and power efficiency led to its widespread integration across numerous devices. Conventional BLE localization methods fall into two categories: *1) RSSI-based model:* this type of works use BLE beacons (e.g., iBeacons [4]) to obtain RSSI and establish propagation models [10, 46, 50] or fingerprint [24, 65, 66, 81], achieving poor localization accuracy of 3m and 1.3m, respectively. *2) Angular-based model:* Angular-based model aims for higher precision by employing AoA, relying on MIMO capable SDRs [18, 54] or SDRs with customized antenna array [31, 67, 79]. While more precise, these works entail higher costs.

In 2020, Bluetooth SIG released a new BLE standard (5.1), introducing **direction finding** [6, 80] that integrated AoA estimation. Many subsequent localization works [18, 27, 64, 70] and applications [1, 5, 19, 22, 23, 29, 39–41, 43, 53, 56, 78, 83, 84, 86, 90] have been proposed based on BLE 5.1 or higher version. However, only a few commercial hardware can support the directional finding feature, which limits wider deployment [18]. To overcome this issue, we proposed Bridge, expanding the direction finding feature to every off-the-shelf Bluetooth device without modifying any existing device, thereby elevating the applicability of BLE localization.

Cross-Technology Communication. Cross-technology communications (CTC) [35] breaks down the communication barriers between different wireless protocols. Several works [13, 14, 26] need hardware modification for message exchange. Recent works focus on signal emulation for cross-protocol communication like WiFi to ZigBee [11, 32, 48, 49] and WiFi to BLE [15–17, 47]. A series of Cho, Hsun-Wei's works [15–17] enables bi-directional communication between WiFi and BLE. However, all these works need hardware modifications or firmware updates on transmitter or receiver sides and fail to implement high-precision localization capability. WiBeacon [51] emulates BLE beacons by modifying WiFi APs to expand BLE location-based services, but its localization accuracy approximates RSSI-based approaches (around 1m). So far, high-precision localization is still an urgent need, especially for industry or logistics needs.

Since the BLE direction finding feature can offer high-precision localization capability, we attempt to break the limitation that the BLE direction finding feature is only supported on a few BLE targets. Unlike most CTC techniques, the premise of our work is not to modify existing devices due to substantial costs for replacing existing infrastructure or Bluetooth chips.

3 BACKGROUND

3.1 Bluetooth Low Energy (BLE)

BLE is booming in compact IoT devices for its low power consumption and over 5.4 billion BLE-enabled devices were

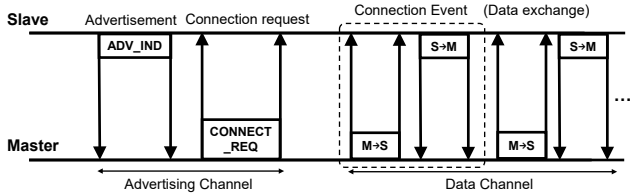


Figure 2: Packet flow of BLE v4.0 connection process.

shipped in 2023. Report [7] claims that over 97% of Bluetooth devices will include BLE by 2027, indicating the wide availability of BLE in the future. BLE operates in $2.4GHz$ unlicensed band which is equally divided into 40 channels [92], including 3 advertising channels for connection establishment and 37 data channels for exchanging data. Specifically, BLE modulates digital data by employing Gaussian Frequency Shift Keying (GFSK) to confront noise.

Link layer characteristics. Fig. 2 depicts the packet flow of the old-version (BLE v4.0) connection-establishment process. When not being connected, the slave (peripheral device in later-version specifications) device continues to broadcast a protocol data unit (PDU) named *ADV_IND* through 3 **advertising channels** to wait for a connection request. The master (central device) in the scanning state listens to the advertising packets and sends the connection request packet (*CONNECT_REQ*) back to a particular device, and the link layer enters the Connection State.

The connection event is considered opened while the link layer (LL) data PDU is transmitted through the remaining 37 **data channels** from both devices, named $M \rightarrow S$ (packets from master to slave) or $S \rightarrow M$ (packets from slave to master).

Bit stream processing. In BLE communication, every transmitted PDU needs to go through error-checking and whitening. The transmitter encrypts the payload, generates Cyclic Redundancy Check (CRC), whitens it and the receiver dewhitens, checks CRC, and decrypts the payload, respectively.

3.2 BLE Direction Finding Feature

To address the growing demand and increase the localization accuracy of Bluetooth location services, Bluetooth SIG integrated **direction finding** capability in version 5.1. With this new feature, the BLE device (*locator*) can determine the direction of a message being transmitted from another device (*target*), significantly enhancing localization solutions.

Direction finding feature update. Several updates appear on newly BLE after v5.1 comparing to previous BLE [6]. First, the data channels can also be used in the Advertising State, offering the opportunity to achieve direction finding before entering the Connection State. Second, the protocol added an extended advertising payload to exchange necessary data. Periodic advertising mode achieves direction finding by transmitting three PDUs (*ADV_EXT_IND*, *AUD_ADV_IND*,*AUD_SYNC_IND*), shown as Fig. 3. Particularly, additional fields named Constant Tone Extension

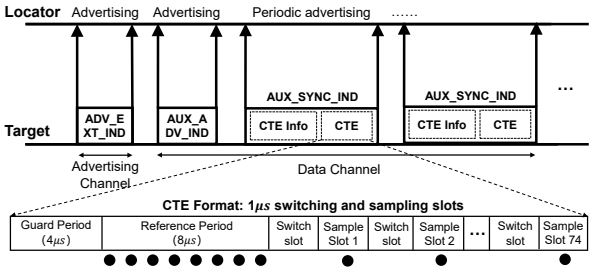


Figure 3: Packet flow of BLE v5.1 for direction finding feature and the structure format of newly added CTE.

(CTE) and CTE info in *AUX_SYNC_IND* are used to indicate whether the packet supports direction finding.

CTE for AoA estimation. If the packet supports AoA detection, a specific CTE structure has a variable length ranging from $16\mu s$ to $160\mu s$, shown as Fig. 3. As a standard, the first $4\mu s$ are termed the guard period and the next $8\mu s$ are termed the **reference period**, following an alternating sequence of **switch slots** and **sample slots**. The switching antenna in the locator can parse the IQ samples that will be used to calculate the phase difference in different elements of the antenna array, which in turn realize the AoA estimation.

With the help of the newly direction finding feature, BLE devices can integrate high-precision localization functions internally. Numerous companies [21, 42, 68, 85, 87] have introduced positioning systems based on BLEv5.1 tags to serve industrial [1, 5, 19, 23, 39, 41, 56, 83, 90], logistics [22, 29, 40, 43, 53, 78, 84, 86], medical [36, 37, 63], retail [20, 82], events [57, 58, 89], and other scenarios.

Limitation. Unfortunately, the direction finding has not been widely supported in commercial BLE devices until now. It is because such a feature significantly relies on CTE structures proposed after BLE v5.1. Lower-version BLE devices cannot generate necessary CTE info to be recognized by locators. Higher-version devices (e.g., phones of BLE v5.2) may not necessarily support this feature due to cost considerations. It is unrealistic to modify the hardware or firmware of off-the-shelf devices, thereby preventing the direction finding feature from being deployed on a large scale.

An intuitive solution to this issue is to enable the target to send the specific packet to cheat CTE structure (somewhat similar to CTC), however, facing severe difficulties of generating CTE info and channel alignment. According to BLE protocol [6], channel number (essential for signal modulation and channel alignment) changes due to the channel hopping mechanism and stays unavailable on most commercial BLE devices, making it hard to cheat CTE structure successfully.

■ **Key idea of Bridge.** This motivates us to propose Bridge, which tends to locate every Bluetooth device using the direction finding feature integrated with deployed locators. The key idea of Bridge is to introduce an additional Trigger node. In a nutshell, Trigger will function as a bridge to synchronize time and channels as well as providing CTE

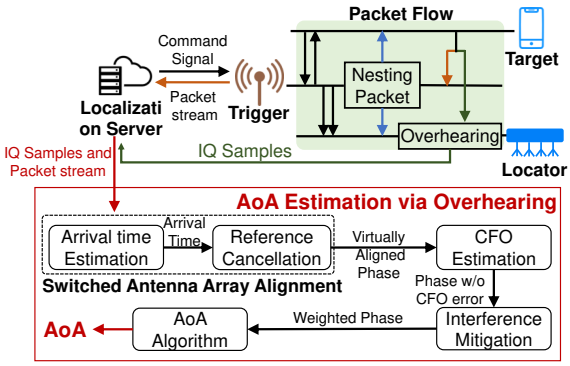


Figure 4: System overview of BRIDGE.

info so that the locator can recognize and sample the specific packet ($S \rightarrow M$) broadcasted by targets at the appropriate time. BRIDGE helps extend the official direction finding feature to have the potential to be widely applied and deployed.

4 SYSTEM DESIGN

4.1 Technical Assumptions

The goal of BRIDGE is to extend direction finding features to all Bluetooth devices without modifying existing hardware or firmware. In this work, we make the following assumptions:

- **Already deployed locators supporting direction finding protocol.** We assume that there are already locators that support direction finding in the scenario. These locators are originally prepared for BLE devices over v5.1. We aim to make these locators available for lower versions or direction finding unsupported BLE devices.
- **Target devices should act as slave roles.** We assume that the target devices are in an advertising state, ready to establish connections. This is not a strong assumption since slave (peripheral) roles are widespread, commonly for devices without visible interfaces or control consoles (e.g., earphones). Smart devices like smartphones and smartwatches can also act as connection slaves after operations, which will not conflict with regular use.
- **IQ samples are available during CTE periods.** Core specification [6] claims locators with switched antenna arrays should be able to sample IQ data during CTE period. Most direction finding solutions provide direct access to IQ samples from locators [61, 72] and allow users to customize their angular solutions. For rare cases, IQ samples can still be accessed on direction finding localization servers during the intermediate process of AoA estimation.

Following by above assumptions, the **design objective** of BRIDGE goes to utilizing the existing Bluetooth direction finding locators to accurately locate every Bluetooth device with minimum cost of deploying additional hardware.

4.2 System Overview

The intuition behind BRIDGE is to introduce an additional node called TRIGGER, which directly talks to both targets and

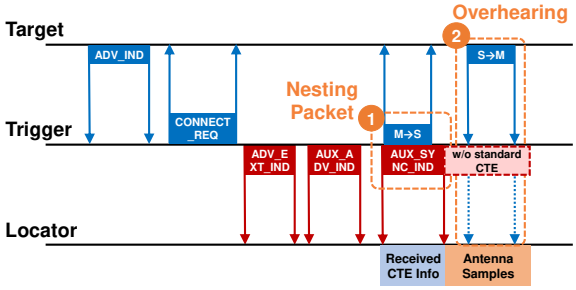


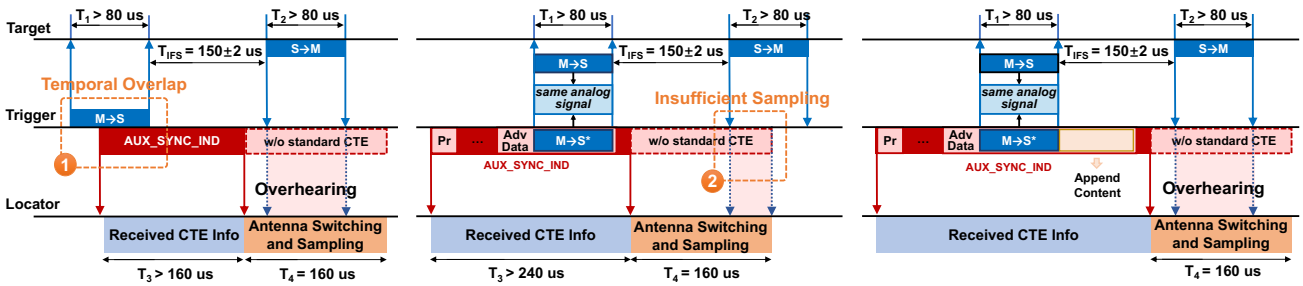
Figure 5: Packet flow design of BRIDGE.

locators separately. The TRIGGER will serve as a bridge to form a "bridged" direction finding feature between the locator and the unsupported target. Fig. 4 shows the system overview of BRIDGE, comprising four core components: trigger node, locator, target, and localization server. Below, we introduce the definition and functionality of each character:

- **Trigger node:** TRIGGER is a fully controlled device with capabilities to send or receive Bluetooth signals, which can be implemented using SDR, full stack BLE development board, and so on. Once received AoA estimation command from the server, TRIGGER will: 1) serve as connection master to establish a connection with targets; 2) serve as a virtual tag to send necessary CTE info packets to locators; 3) synchronize the time and channel between the target and locator using well-designed **nesting packet** (details shown in Sec. 5), aligning the target's signal with the locator's IQ sampling during the CTE period. Note that one TRIGGER can cover 20 locators, allowing for large-scale deployment with limited additional cost.
- **Locator:** As already deployed to locate direction finding supported devices (tags), the locator will receive multiple packets from TRIGGER, mirroring the reception process typical of BLE 5.1 tags. The signal received by the locator during the CTE period will be partially replaced by the signal from the target, which is called **overhearing**.
- **Target:** The target represents a device that needs to support direction finding features (e.g., lower version tags, smartphones, controllers, etc). It should act as a slave role, ready to establish connections. BLE device address is used to determine a specific location target.
- **Localization Server:** The server (e.g., personal computer) is physically connected to locators and TRIGGER, commanding TRIGGER as well as receiving IQ samples from locators. IQ data is afterwards processed through AoA estimation via overhearing including steps of switched antenna array alignment, CFO estimation, and interference mitigation.

4.3 Packet Flow Design

To communicate with both locators and targets, TRIGGER must act as a master to establish a connection to the target as well as to imitate direction finding behavior to locators. Since the protocol cannot be modified, the BRIDGE's packet flow is specially designed as it should obey the original flow



(a) Inevitable temporal overlap (b) Insufficient sampling (c) Temporal adjustment by appending content

Figure 6: Synchronization via nesting packet. (a) Temporal overlap occurs when achieving synchronization; (b) If only execute packet insertion and encoding, *S→M* will be insufficiently sampled and further influence AoA estimation; (c) Meaningless content is appended for temporal adjustment to maximize the sampling of overhearing.

for both parties. Specifically, below walks through the packet flow as shown in Fig. 5.

- **Communication between Trigger and target:** The target advertised *ADV_IND* to be ready for connection establishment. Once Trigger scanned *ADV_IND*, it should send *CONNECT_REQ* and *M→S* packets to the target and later hear a response packet (*S→M*) from the target. This process is the connection event.
- **Communication between Trigger and locator:** The Trigger should send *ADV_EXT_IND*, *AUX_ADV_IND*, and *AUX_SYNC_IND* packets to locator for activating the direction finding event and providing essential CTE Info. Note that the original CTE is removed.
- **Synchronization and overhearing:** To imitate direction finding behavior, *M→S* and *AUX_SYNC_IND* packets should be transmitted within a strict temporal constraint to achieve signal substitution in CTE period. This process inevitably causes temporal overlap. Once successful, the locator receives both CTE info from Trigger, followed by a response (*S→M*) from the target just in time to substitute sampling signals in CTE period (called overhearing). The locators further obtained IQ samples for AoA estimation.

The following sections will present the details of Bridge, and are committed to answering the following questions: 1) How to achieve packet flow by precisely synchronizing channel and timing under condition of temporal overlap? (Sec. 5). 2) How to accurately estimate AoA via overhearing that differs from original direction finding feature? (Sec. 6)

5 SYNCHRONIZATION VIA NESTING PACKET

5.1 Temporal Overlap in Alignment

Trigger serves as a bridge to provide CTE info as well as time and channel synchronization, enabling locators to sample the transmitted *S→M*. For **channel alignment**, since Trigger is fully controlled, it can apply specific segments (channel number) in packet *CONNECT_REQ* and *AUX_ADV_IND* to determine which data channel to be used. For **time alignment**, it may similarly control the time offset and when to send the packets. Note that the CTE part transmitted in *AUX_ADV_IND* by Trigger is removed in advance. The goal of synchronization is that the *S→M* packet exactly replaces the removed original CTE part in *AUX_ADV_IND* when being received by the locators (called **overhearing**)

Unfortunately, the synchronization inevitably suffers from a ***temporal overlap*** for Trigger to send packets, as shown in Fig. 6(a). The synchronization requires the arrival time of *S→M* (with a length of $T_2 > 80\mu s$ enough to cover multiple cycles of antenna switching) exactly falls within the CTE period T_4, and occupies as long as possible for the locator to sample as much data of overhearing for later AoA estimation. According to the communication process, the interval between *S→M* and *M→S* is $T_{IFS} = 150 \pm 2\mu s$, which is less than the length of received CTE info containing in *AUX_SYNC_IND* ($T_3 > 160\mu s$). It means that no matter how to adjust the arrival time of *S→M*, the transmission of *M→S* and *AUX_SYNC_IND* must overlap in time, which will result in transmission error or system failure when utilizing the same channel in Trigger. To this end, we proposed a meticulously crafted packet (named **Nesting Packet**) to transmit the corresponding payload for each side in the next section.

5.2 Nesting Packet

The main function of a nesting packet is to carry out a blended payload for different receivers through a crafted packet design. The design objectives of the nesting packet are listed below:

- Nesting packet should ensure all necessary original contents and structures are unchanged.
- Nesting packet must obey the BLE bit stream processing procedure for passing error checking and time alignment when being received.
- The packet flow should maximize the occupying time of *S→M* in the CTE period for sufficient sampling for later AoA estimation.

Specifically, the structure and generating method of the nesting packet is composed of four steps:

Algorithm 1: Nesting Packet

Input: PDU X for original $M \rightarrow S$ packet, insert position T, corresponding CRC initial value K, and physical channel no. N.
Output: Updated content Y of $M \rightarrow S^*$ in nesting packet satisfying $modulate(Pr + AA + whiten((X + CRC(X,K)),1,N),N) = modulate(whiten(Y,T,N),N)$.

```
// Pr and AA: Preamble and Access Address
   for the original M→S.
```

After *GFSK* demodulation:
$\longrightarrow Pr + AA + whiten((X + CRC(X,K)),1,N) = whiten(Y,T,N)$;
$\longrightarrow dewhiten(Pr + AA + whiten((X + CRC(X,K)),1,N),T,N) = dewhiten(whiten(Y,T,N),T,N)$;
$\longrightarrow Y = whiten(Pr + AA + whiten((X + CRC(X,K)),1,N),T,N)$;

```
// Whiten and dewhiten process are the same.
```

return Y;

Packet insertion. Nesting packet should contain the contents for both locator and target. According to official advertising payload format [6], a segment named "Adv Data" offers a large reserved space which is enough for inserting $M \rightarrow S$ packet. This modification will not interfere with the transmission of necessary CTE Info content. As shown in Fig. 6(b), the $M \rightarrow S$ packet will be appended to the "Adv Data" segment in the nested *AUX_SYNC_IND*.

Packet encoding. It is crucial to ensure that the received payload from the analog signal of the nesting packet for both the locator and target exactly matches the original packets. The pipeline of encoding $M \rightarrow S$ to newly $M \rightarrow S^*$ in nesting packet is shown in Algo. 1, considering the BLE packet format of $M \rightarrow S$ as well as necessary bit stream process for TX and RX including CRC generation and checking, (de)whitening.

Temporal adjustment. When a nesting packet is formed, the packet length for TRIGGER to send will become longer. Since the insertion position is near the end of *AUX_SYNC_IND*, the locator can overhear only a small part of the front of $S \rightarrow M$, as shown in Fig. 6(b). This ***insufficient sampling*** significantly influences the accuracy of AoA estimation. To address this issue, we append meaningless content (multiple 0s) just after newly encoded $M \rightarrow S^*$ to maximize the occupying time of $S \rightarrow M$ in the CTE period, as shown in Fig. 6(c). At this point, $S \rightarrow M$ is finally adjusted to arrive as soon just after the end of *AUX_SYNC_IND* (with a minimum interval in between). In addition, the length of meaningless content can also be used to control antenna sampling to improve performance, which will be discussed in Sec. 6.3.2.

CRC update. Considering the full payload in the nesting packet including original contents, encoded $M \rightarrow S^*$, and appended contents for temporal adjustment, the CRC value of *AUX_SYNC_IND* will be regenerated accordingly.

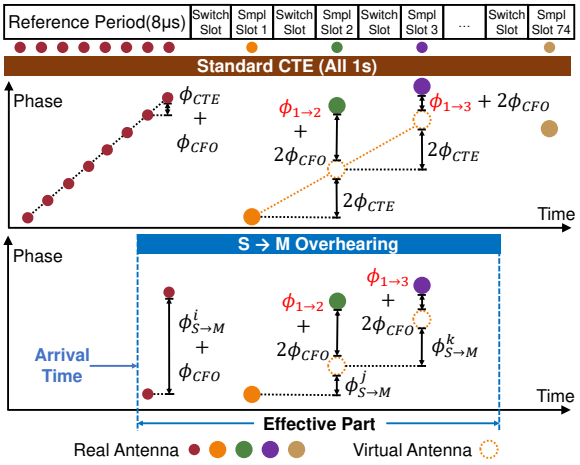


Figure 7: Comparison of phase alignment between standard CTE and overhearing. AoA estimation in overhearing mainly faces two challenges: 1) The arrival time of $S \rightarrow M$ is uncertain; 2) The phase difference is related to the content of $S \rightarrow M$ (unique phase shift $\phi^j_{S\to M}$ not constant) and hard to eliminate.

6 AOA ESTIMATION VIA OVERHEARING

Once our synchronization via nesting packet successfully aligns the time and channel in CTE period, the locator will then sample IQ data of overhearing. However, AoA estimation through overhearing mainly faces two challenges compared to using original CTE signals: 1) **Uncertain arrival time**: although the synchronization ensures the overhearing occurs in CTE period, unexpected arrival time deviation still appears due to hardware delay and temporal calibration; 2) **Unstable phase difference:** The phase difference in overhearing is significantly related to the content of $S \rightarrow M$, which fluctuates instead of being a constant tone (standard CTE).

Specifically, as shown in Fig. 7, the phased difference between the sampling slots (initial phase difference across antennas are automatically normalized and eliminated) consists of three parts: phase shift due to antenna spatial separation ($\phi_{1\to i+1}$), phase difference in modulated $S \rightarrow M$ signal ($\phi^j_{S\to M}$), and phase error caused by carrier frequency offset (ϕ_{CFO}). The part $\phi^j_{S\to M}$ is relevant to the content of $S \rightarrow M$, which is different from the constant phase difference (ϕ_{CTE}) in standard CTE. AoA estimation requires clean extraction of phase difference from antenna spatial structure ($\phi_{1\to i+1}$). In this section, we introduce our detailed AoA estimation process with the newly overhearing characteristics, including switched antenna array alignment (Sec. 6.1), CFO estimation (Sec. 6.2), and interference mitigation (Sec. 6.3).

6.1 Switched Antenna Array Alignment

We applied virtual reference antenna (VRA) to firstly remove $\phi^j_{S\to M}$ related to $S \rightarrow M$ packet. For such purpose, we first estimate the signal arrival time to determine the effective

overhearing proportion in CTE, then achieve reference cancellation with the generated phase for VRA.

6.1.1 Arrival Time Estimation. Unlike the standard CTE period with a known duration of signal persistence, arrival time deviation brings the uncertainty of where the overhearing lies in the CTE sampling period. It leads to an indefinite effective length of IQ samples from each $S \rightarrow M$ overhearing (Fig. 7). We propose an algorithm for accurate arrival time estimation including a preliminary amplitude judgment and a μs-level differential phase correlation.

Preliminary amplitude judgment. Conventionally, the amplitude of the signal can be used to determine the arrival time based on a constant threshold. However, it fails in our case because: 1) antenna switching and various polarization patterns may cause amplitude drops suddenly; 2) the time interval between samples is too large for μs-level accuracy.

Therefore, we propose a preliminary amplitude judgment with a dynamic amplitude threshold to detect the existence of a signal within each CTE. Specifically, as shown in Fig. 8(a), it involves a dynamic amplitude threshold (empirically $0.35\times$ average amplitude). To avoid outliers, 3 adjacent samples as a group are calculated average. Through the above process, a preliminary scope of overhearing has been determined.

Differential phase correlation. To accurately estimate the signal arrival time in μs-level, it is essential to utilize the phase information, which remains stabler than amplitude during antenna switching. The corresponding ideal phase can be generated from the decoded content of $S \rightarrow M$. Among existing techniques, phase correlation approach benefits from its high robustness and phase consistence characteristics on samples from the switching antenna array.

Unlike the proposed phase correlation method used in SDR-based packet detection, in our case, the phase generated from the collected IQ samples cannot be directly used to determine characteristics or calculate correlation peaks due to the rapid antenna switching of the locator (causing additional phase shift and sampling rate mismatch). Therefore, in our differential phase correlation process, phase from the same antenna, with a time interval of a complete antenna switching round t_c, is subtracted correspondingly to remove the phase changes from the antenna spatial structure. Within the preliminary scope from amplitude judgment, phase differential with an interval of t_c is generated for both real and ideal phases separately (Fig. 8(c)(e) from (b)(d)). 0s are added to the real phase differential to compensate for the insufficient sampling rate. These phase differential are then convoluted to find the correlation peak, and the arrival time can be derived as $T_{arrival} = t_0 + t_{ideal} - t_{corr}$, where t_0, t_{ideal}, and t_{corr} represent the beginning time of preliminary scope, temporal length of ideal phase differential, and temporal length to the convolution peak, respectively (Fig. 8(f)).

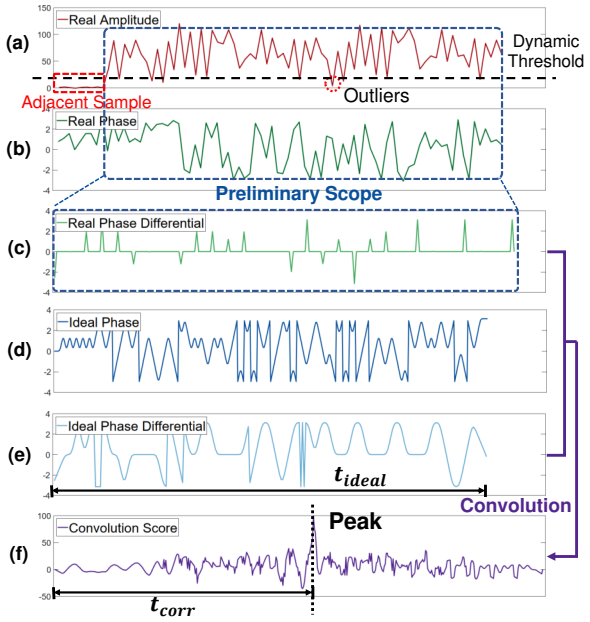


Figure 8: Process of arrival time estimation. A preliminary amplitude judgment is conducted to determine a preliminary scope of effective overhearing (Fig. (a)). Phase differential is generated from both real and ideal phases (Fig.(c)(e) from Fig. (b)(d)) to calculate correlation peak (Fig. (f)) and determine the exact arrival time.

6.1.2 Reference Cancellation. Conventional reference cancellation in standard CTE remains unchanged because the original CTE transmits a series of modulated 1s without whitening, leading to a constant signal frequency. However, BRIDGE leverages overhearing to sample the packet in the CTE period. Since the target transmits $S \rightarrow M$ with varying frequency through overhearing, the conventional reference cancellation fails. To address this issue, the phase of the virtual reference antenna is generated by using the ideal phase of $S \rightarrow M$. Specifically, given the μs-level arrival time of $S \rightarrow M$ ($T_{arrival}$), the phase difference of adjacent slots (T_i and T_{i+1}) caused by reference signal is then calculated by $\phi^i_{S\rightarrow M} = \hat{\phi}^{T_{i+1}-T_{arrival}}_{S\rightarrow M} - \hat{\phi}^{T_i-T_{arrival}}_{S\rightarrow M}$, where $\hat{\phi}^T_{S\rightarrow M}$ represents ideal phase of $S \rightarrow M$ at time T. Here, the aligned phase $\phi_{1\rightarrow 2}$ is still combined with multiplications of carrier frequency offset phase error (ϕ_{CFO}), which will be addressed in Sec. 6.2.

6.2 CFO Estimation

Due to manufacturing imperfections and changes in the environment, a slight frequency difference exists between the oscillators in the transmitter and the receiver called carrier frequency offset (CFO). CFO estimation is crucial to estimating this frequency deviation for accurate AoA estimation. In this section, we propose a CFO estimation algorithm suitable for overhearing to strip ϕ_{CFO} part.

Challenge in overhearing. For a standard direction finding solution, the effective part must contain the complete

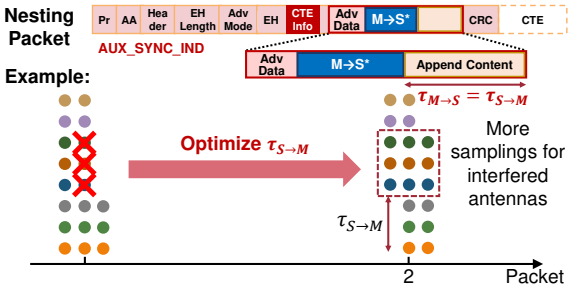


Figure 9: Antenna sampling control.

reference period ($8\mu s$). This time is adequate to use linear regression to estimate the CFO precisely. However, the arrival time deviation of overhearing may result in the effective part only partially or even not falling within the reference period (Fig. 7). In this case, the standard estimation approach produces large estimation errors and leads to failure. To address this issue, we propose a 2-stage CFO estimation method:

Coarse-grained estimation. There are two conditions according to the arrival time derived from Sec. 6.1.1: 1) If the $S\to M$ packet arrives within the reference period, a linear regression can still be applied to the aligned phase using effective reference period samples. 2) If the $S\to M$ packet arrives completely after the reference period, an empirical CFO estimation ($0.01rad$) will be applied. This coarse-grained estimation ϕ_{CFO_c}, though only obtaining a rough estimation, will be further used in the next stage.

Fine-grained estimation. For effective samples beyond the reference period, we take the differential of the time of each complete antenna switching round to eliminate the influence of $\phi_{1\to i+1}$. Assuming a sampled phase sequence containing m complete switching rounds with N antennas, which can be denoted by $[\phi_1^1, \phi_1^2, \cdots, \phi_1^N, \cdots, \phi_m^1, \phi_m^2, \cdots, \phi_m^N]$, the fine-grained CFO estimation can be calculated as:

$$\phi_{CFO\_f} = \frac{\sum_{j=1}^{N}\sum_{i=1}^{m-1}(\phi_{i+1}^j - \phi_i^j + 2k\pi)}{2N^2(m-1)}$$

Note that $\phi_{i+1}^j - \phi_i^j$ may exceed a cycle (2π), we used the coarse-grained estimation ϕ_{CFO_c} to determine the exact number k of cycle passed for a complete antenna switching rounds. Specifically, $k = \lfloor (2N \times \phi_{CFO\_c})/(2\pi) \rfloor$. Therefore, the fine-grained CFO estimation is more accurate than the coarse-grained estimation due to its longer time interval according to Moose algorithm [55].

6.3 Interference Mitigation

After above process, BRIDGE can extract phase difference in antenna spatial separation ($\phi_{1\to i+1}$) for AoA estimation. However, BLE direction finding is prone to interference with other $2.4GHz$ RF signals and multi-path effects under complex environments. To mitigate the interference, packet-level combination integrates data from multiple packets for higher accuracy [44]. It applies the AoA algorithm to each packet, and then filters across multiple AoA estimations, requiring a large number of packets. To use fewer packets to improve the update rate while achieving high precision, we propose an antenna-level combination for intra-packet phase calibration and apply an antenna sampling control algorithm.

Algorithm 2: Arrival Time Optimization

Input: A set X of all interfered antennas. Number of all antennas N, sampling slots before, within, and after the effective overhearing N_b, N_w, N_a. Currently the first sampling antenna A_f.
Output: Delay of the overhearing $\tau_{S\to M}$.

```
Max = 0 for −N_b ≤ i ≤ N_a do
    S_i = 0, Y = {A|A ∈ [A_f+i, (A_f+N_w−1)+i], A ∈ ℤ}
        mod N // Modulo ∀A ∈ Y
    foreach A_j ∈ X do
        if A_j ∈ Y then S_i = S_i + 1;
    end
    if S_i > Max then Max = S_i, Sol = i ;
end
return τ_{S→M} = Sol × 2μs;
```

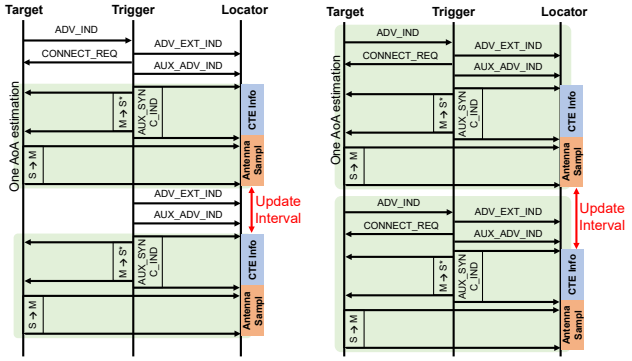
6.3.1 Antenna-level combination. Our proposed antenna-level combination first filters out the phase outliers of antenna elements and applies a weighted average to the phase of the virtually aligned antenna array.

Filter outliers. The anomalous pattern of phase derivative for a specific antenna array with known spatial structure is generated and compared to our sampled data. In a standard antenna switching sequence, the phase derivatives remain the same within each row and varies between rows. To determine the bad readings of certain antenna samples, we set a dynamic error ratio threshold of phase derivative (empirically 15%) for the adjacent antennas to filter outliers.

Apply weighted average. The weighted average is applied to phase using Maximal Ratio Combining (MRC) [8] algorithm based on the SNR of the received signal, since the amplitude of samples indicates the relative signal strength within the same CTE period, MRC is then applicable to better calibrate the intra-packet phase.

6.3.2 Antenna sampling control algorithm. To mitigate the interference coming in a burst, phase from adjacent antennas may suffer from great error. As shown in Fig. 9, to have antennas with bad readings (samples with red crosses) sampling more in subsequent cases for efficient and accurate AoA estimation results, we propose an antenna sampling control algorithm as follows:

Antenna sampling arrangement. Notice that some antennas may experience one more sampling slot than others. After detecting antennas with phase bad readings (interfered antennas), the overhearing can be advanced or postponed to rearrange the first antenna sampling within the overhearing period. We then determine to introduce a $\tau_{S\to M}$ delay in



(a) The number of concurrent targets is within Trigger's threshold. (b) The number of concurrent targets surpasses Trigger's threshold.

Figure 10: Dynamic packet flow switching.

the next overhearing to maximize the number of interfered antennas that can be sampled more in the next CTE event.

Arrival time optimization. Once given the effective overhearing in the sampling period, we can calculate the number of sampling slots before, within, and after overhearing, as well as the first sampling antenna index. After detecting interfered antennas, we are then able to derive the set of antennas with more samplings, and advance/postpone the set within the calculated range to maximize the intersection with interfered antennas. Details of deriving the delay $\tau_{S\to M}$ is shown in Algo. 2, and we may achieve the case by appending $n = \tau_{S\to M}/8\mu s$ more bytes in *AUX_SYNC_IND*.

7 SCALABILITY

Concurrent Targets Support. Facilitating positioning for multiple concurrent targets is crucial for scalability. The standard direction finding feature allows locators to support tens of concurrent Bluetooth v5.1 targets under connectionless CTE mode. Therefore, the increased number of other Bluetooth devices by Bridge will not exceed the capability of the locator. However, the Trigger can cover up to 20 locators, and the increase of concurrent targets in this area may cause channel blocking of Trigger, interfering with the stability of the AoA update rate.

To maintain the update rate for concurrent targets, we introduce a **dynamic packet flow switching** strategy (Fig. 10). This method adjusts Trigger's operational mode by comparing the number of concurrent targets N_c and the connection number threshold N_{th}. N_{th} is dictated by Trigger's hardware performance and latency considerations, and we set N_{th} to 4 to enable the latency of 35 *ms*.

1) $N_c < N_{th}$: Trigger keeps a connection with each target after an AoA estimation. Without repeated procedure for establishing connections, the following nesting packet (*AUX_SYNC_IND* and $M\to S$) is transmitted in a shorter interval, allowing a higher AoA update rate (Fig. 10(a)).

2) $N_c >= N_{th}$: Trigger fails to maintain all connections for latency considerations. As a trade-off between stability and update rate, we command Trigger to establish a new connection for each AoA estimation, shown as Fig. 10(b), to stably support a large number of concurrent targets.

Table 1: Comparison of cost and coverage

System	Coverage (m^2)	Cost	Cost per m^2
TyrLoc [31]	105	\$1200	\$11.4
Dead on Arrival [18]	25	\$5000	\$250
Su et al. [79]	72	\$564	\$7.83
Monfared et al. [54]	18	> \$20000	> \$1111.1
Bridge	**875**	**\$3198**	**\$3.65**

Trigger Handover. The large-scale deployment may result in targets being overlapped by multiple Trigger and cause handover problems. Due to the nature of connection establishment, the target can only connect to the first Trigger sending *CONNECT_REQ* rather than the closest Trigger. If the target is unexpectedly connected to a far-away Trigger (due to the uncertainty of hardware latency), locators near the target might not be successfully activated, which leads to a lower AoA accuracy or even localization failure.

The traditional methods for selecting Trigger based on packet RSSI [91] or target trajectory [97] are prone to errors due to environmental interference. In our Bridge, we apply a uniform operation pattern for all Trigger to handle the handover problem. Each Trigger uses the same device address in *CONNECT_REQ* and $M\to S$, and maintains consistent time intervals for corresponding packets. This uniformity allows all triggers to do synchronization in the same way, and all triggers covering the target can activate locators within their coverage area to overhear from the target. Locators in the vicinity of the target are all able to localize on the target, thus improving localization accuracy.

System Cost. To reduce system cost, Trigger can be implemented using general-purpose SDRs with only single-input single-output capability. Nevertheless, strict latency demand ($150\mu s$ for BLE) filters out extremely low-cost SDRs (e.g., PlutoSDR [2]). Despite this, Bridge still maintains competitive cost (especially against angular-based SDR systems [18, 31]) for two reasons: 1) No requirement of customized antenna arrays: our Bridge utilizes the existing direction finding locators equipped with unified antenna arrays, saving extra cost and effort to design and customize special antenna arrays; 2) Easy deployment: our Trigger can cover more than 20 locators (supporting a large area of 875 m^2), reducing the number of required Trigger for fixed coverage area. As shown in Table. 1, our Bridge using Trigger can save up to 53.3% cost compared to other SDR-based angular localization systems with the same coverage condition.

8 IMPLEMENTATION

This section presents a prototype implementation of Bridge, comprising four parts, shown as Fig. 11.

Trigger node: We use Ettus USRP N210 [59] as Trigger, with two antenna RF slots (TX/RX, RX2) enabling TX and

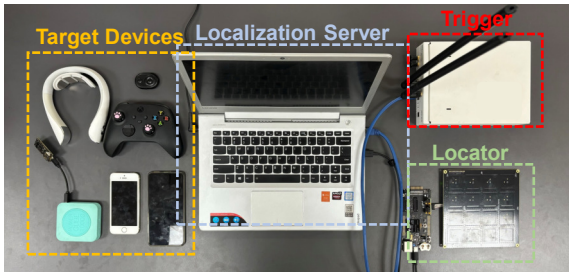


Figure 11: Implementation of Bridge.

Table 2: Target devices

Appliance	Model	Company	BLE version
Smartphone	iPhone 5s	Apple	4.0
Smartphone	iPhone 15	Apple	5.3
Smartphone	Mate30	Huawei	5.1
Smartphone	Note 12 Pro	Redmi	5.1
Smartphone	P40	Huawei	5.1
Speaker	L07A	Xiaomi	4.2
Controller	Xbox	Microsoft	4.0
Remote control	YK10	Tiktok	5.0
Neck massager	K5-2	SKG	5.0
Thunderboard Tags	BG22	Silicon labs	5.2

RX simultaneously. The gains of TX and RX are set to $20dB$ and $25dB$ respectively, for performance tradeoff between coverage and packet error rate. Two identical bidirectional antennas with $12dBi$ and $2300 - 2400MHz$ are used for TX and RX. N210 is directly connected to the localization server via GB Ethernet and controlled by the server.

Locator: The locator is developed using Silicon Labs Pro Kit [75], comprising a radio board coupled with a Wireless Starter Kit [74]. The BG22 radio board [73] features a dual-polarized antenna array with 4×4 antenna slots.

Tracking targets: 10 common BLE devices of various BLE version (from v4.0 to v5.3) are tested as targets (Tab. 2). **None of them originally supported standard direction finding features.** The targets include devices already in the advertising state (remote, tags, etc.) that can be directly used, and devices that require additional operations like initiating pairing mode (e.g., smartphone, controllers, etc.) to begin advertising. During experiments, all targets serve as slave roles (peripheral), ready for connection establishments.

Localization server: We use a common Lenovo laptop with a 4-core CPU @$2.3GHz$ as the localization server. It is connected to Trigger via Ethernet and to locators via USB, receiving IQ samples from locators and applying further AoA estimation algorithms.

9 EVALUATION

9.1 Experiment Setup

Environment and deployment. The following experiments are conducted in a reading room ($35m \times 25m$ area) of a school library, including, opening space, tables and chairs, and crowded bookshelves (floor plan depicted in Fig. 12). Locators are deployed on the ceiling, and targets are carried

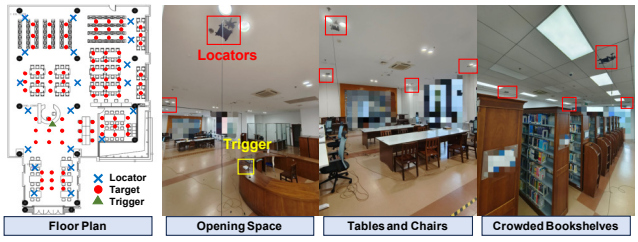


Figure 12: Experiment environments.

on human hands to simulate everyday usage. All evaluated targets remain stationary to simplify the experiments, and mobility issues can be solved by existing post filters (similarly to current direction finding systems). One Trigger is put on a table in the central area to fully cover the whole area. Ground truth data for the locations of targets is collected manually. Unless in Sec. 9.4 discussing the impact of concurrent targets, experiments are all conducted with only one device being localized, at each target point in turn.

Comparison schemes. The comparison schemes include the following localization systems: standard BLE direction finding, iBeacon, RSSI-based fingerprint, and our proposed Bridge. For standard BLE direction finding, a direction finding tag acts as a target, and for iBeacon and fingerprint, the existing beacons are utilized with slightly different arrangements on the ceiling.

9.2 Microbenchmark

In this section, we evaluate the impact of system components. Here, 4 devices (Huawei P40, Thunderboard tags, remote controller, iPhone 5s) are tested for microbenchmarks.

Nesting packet. To determine the packet success rate of nesting packet, the success Rx rate is compared when transmitting: 1) $M \rightarrow S$ only; 2) *AUX_SYNC_IND* only with the same length of nesting packet; 3) nesting packet with Rx for two packets individually. After 2000 times of TX for each case, Fig. 13 shows that our nesting packet slightly affects TX and Rx, where a slight decrease (only 2.5%) of Rx $M \rightarrow S$ possibly results from the signal interference ahead and after.

Switched antenna array alignment. An AoA estimation error performance is compared for following three cases: our switched antenna array alignment with arrival time estimation and reference cancellation, reference cancellation with an amplitude threshold-based arrival time estimation, and without phase alignment. Fig. 14 shows that our method performs the best, amplitude threshold-based method suffers from large error when wrongly estimating the arrival time, with 90% AoA error below 3.1°, 15.8°, and 61.9° respectively.

CFO estimation. The AoA error is compared with different CFO estimation methods including our coarse-grained and fine-grained method, coarse-grained only, and without CFO estimation. Fig. 15 shows that the fine-grained CFO leads to a higher AoA accuracy, while coarse-grained suffers from

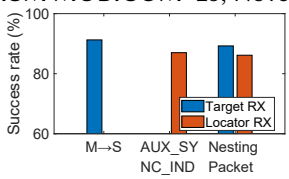


Figure 13: Success rate using nesting packet.

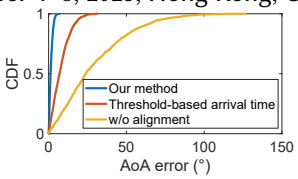


Figure 14: AoA error in alignment.

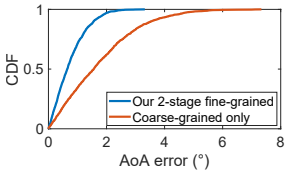


Figure 15: AoA error in CFO estimation.

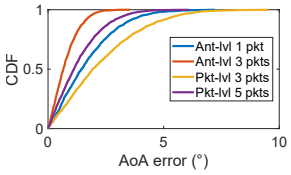


Figure 16: AoA error in interference mitigation.

large error when it lacks an effective reference period, with 90% AoA error below 1.64° and 3.77° respectively.

Interference mitigation. The AoA error is compared using various interference mitigation methods: packet-level combination with 3 or 5 packets, and antenna-level with 1 or 3 packets, enabling our antenna sampling control algorithm. Fig. 16 shows our antenna-level combination with 3 packets achieves the best AoA accuracy performance (90% error below 1.63°), and even a single packet achieves higher accuracy than 3 packets with packet-level (90% error below 3.54°over 4.76°), proving the efficacy of mitigating interference.

Handover. To evaluate Bridge's ability to handle the handover problem, we introduce another Trigger put in the corner of the reading room to emulate the handover process. The target is put in the coverage of both 2 Trigger, and the successful CTE sampling events from nearby 4 locators are collected, with 500 CTE rounds in total. The following handover solution is compared including trajectory prediction, RSSI based determination, and our method, Fig. 17 shows that our method achieves over 90% success rate for all 4 nearby locators, successfully dealing with the handover problem.

9.3 Overall Performance

For overall performance, all schemes in our Bridge are enabled to achieve the best overall performance. Notice that, for those SDR-based BLE AoA localization systems with customized antenna array [31, 67, 79], their angular/localization error perform inferior to (or close to) the standard direction finding system. We, therefore, adopt standard direction finding system as our localization system performance baseline.

Localization accuracy. The overall localization accuracy is compared with four schemes (listed in Table. 3): our system, standard direction finding, iBeacon, and RSSI fingerprint method. The results indicate that our system achieves a localization error of decimeter level (33.4cm), which is close to the standard direction finding system (20.9cm) and far better than methods utilizing RSSI (meter-level accuracy). The slight accuracy gap between Bridge and the standard

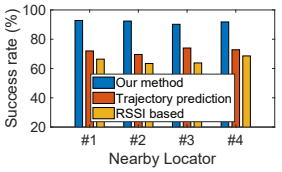


Figure 17: Handover

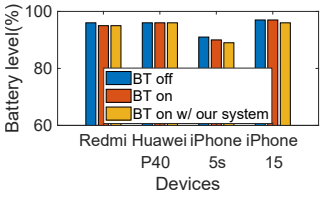


Figure 18: Phone battery

Table 3: Overall localization error (cm) and power consumption (average current (mA))

Schemes	Average	Median	90%	Current
iBeacon [4]	223.1	188.5	460.4	2.72
RSSI-based fingerprint [91]	100.9	83.8	200.9	2.73
Standard direction finding	20.9	18.1	42.1	2.81
Bridge	**33.4**	**28.3**	**72.0**	2.71
(Idle)				2.66

method rises from the shorter effective overhearing than standard CTE length and its frequency changes.

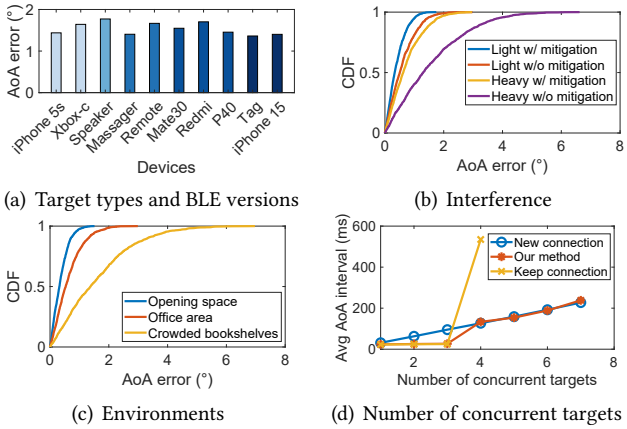
Power consumption. We measure the power consumption of the same target (thunderboard tag) under different schemes: idle, iBeacon, RSSI-based fingerprint, standard direction finding and our Bridge. The advertising or periodic advertising intervals are all set to 100ms to ensure the same update rate. The real-time power is monitored using the Energy Profiler in Simplicity Studio [76]. Given the same voltage (3.3V), the average current within 1min is monitored (Table. 3) to compare the real-time power consumption. Our Bridge achieves a similar power consumption performance (2.71mA) to other beacon modes, which is slightly lower than the standard direction finding power consumption (2.81mA) since the Trigger shares the alignment tasks with locators.

In addition, we conduct a real-scenario power consumption test for mobile phones. Four smartphones are tested for power consumption (battery level) under several conditions: Bluetooth off, Bluetooth on, and Bluetooth on with our Bridge localizing. They undergo an hour test, all staying in standby mode with a full battery at the beginning. Also, when being localized by our system, they keep BLE advertising with the same interval (150ms) and TX power (−8dBm) to control the variables of power consumption. Fig. 18 shows that our localization system does not cause a considerable additional power consumption to the targets.

9.4 Impact of Factors

Impact of target types and BLE version. All listed devices are tested, though within a subspace (not the whole reading room), and Fig. 19(a) shows that all the median AoA errors are less than 2°. For different BLE versions (darker color indicates a higher BLE version), the AoA accuracy does not perform a trend, proving that our system has consistent effectiveness for devices of various types and BLE versions.

Impact of interference. To test our interference mitigation method under different interference levels, tests are conducted in the library under different periods: daytime around



(a) Target types and BLE versions (b) Interference

(c) Environments (d) Number of concurrent targets

Figure 19: Impact of different factors.

2 pm with heavy interference, and late evening around 10 pm with light interference. Fig. 19(b) shows the results that for both light and heavy interference, our method improves the performance by 0.4° and 1.7° of 90% AoA error, respectively. The highest interference level in our evaluated scope is limited that the standard direction finding system works fine. Given the ability to detect the channel congestion and dynamically select the idle channel when establishing connections in lower version BLE devices [71], BRIDGE can ensure its robustness under complex RF interference.

Impact of environments. Three representative areas are specially analyzed with different environments, named as opening spaces, areas with tables and chairs, and crowded bookshelves. Fig. 19(c) shows that our system has the 90% AoA error below 0.8°, 1.3°, and 3.4° under these environments, respectively. Crowded bookshelves will bring more occlusion, thereby causing a relatively large error.

Impact of concurrent targets. Three different work modes are tested: establish a new connection for each AoA estimation round, keep connection, and our dynamic packet flow switching method (maximal connection threshold set to 3), with the number of concurrent targets increasing from 1 to 7. The average AoA interval for all targets is collected to evaluate system latency. Fig. 19(d) shows that: always establishing new connections suffers from a relatively low update rate with a small number of concurrent targets compared to other methods while keeping connection experiences system failure with ≥ 5 concurrent targets. In addition, the average localization accuracy can still be maintained (35.7cm with 7 concurrent targets), indicating a well-balanced performance with a considerable update rate and strong system robustness.

10 DISCUSSION AND CONCLUSION

TRIGGER selection. For those SDRs satisfying latency requirements (e.g., USRP N210 in our prototype system), their multifaceted proficiency surpasses the stipulated demands by a considerable margin. One possible solution to lower the SDR cost is to combine several low-cost SDRs (e.g., HackRF One [33]) to achieve parallel Tx and Rx, which may reach the latency demands (after coding or programming optimization) for our BRIDGE. Another choice is to use the Bluetooth development board with an open Bluetooth Stack (e.g., Kinetis KW41Z [62]) that can be modified by uploading firmware to run our system program, which greatly economizes costs.

Also, the function of TRIGGER may be merged into the deployed locators to further reduce the extra cost. Currently, we establish our BRIDGE without modifying the existing locators (either software or hardware). Given locators with open permissions (or through firmware modifications) to activate the antenna switching function manually, the locators can take the response of TRIGGER to synchronize the time and channel for overhearing, similarly to our BRIDGE.

Multi-protocol support. BRIDGE is now available for Bluetooth devices. Particularly, direction finding feature has potential to be expanded to various wireless protocols (Zigbee, WiFi, etc.). Similar to CTC, once TRIGGER is designed to synchronize multi-protocol devices and achieves overhearing, our system can support multiple protocols in the future. A multi-protocol support will greatly benefits the direction finding systems, providing a universal paradigm for hign-precision indoor wireless positioning.

Practicality. BRIDGE is not aim to replace or alternate the established direction finding systems, but to act as a role of making up the compatibility for a large number of existing and unsupported devices. The newly proposed Bluetooth 5.1 direction finding only covers a limited number of BLE devices, urging backward compatibility updates to expand its versatility. Our BRIDGE provides an integrated solution that makes the high-accuracy direction finding system compatible with all BLE devices, even without their original manufacturer's software or firmware updates. When Bluetooth SIG reveals a new version of the core specification (e.g., v4.x to v5.0), devices of the old version cannot support new features unless they make a hardware replacement (SoC). Our BRIDGE can still function with a high value, since it is impossible to replace all existing Bluetooth devices at once.

Conclusion. We propose BRIDGE, leveraging an additional trigger node TRIGGER to bring BLE official direction finding feature compatible with every Bluetooth device without modifying existing hardware or firmware. Extensive results indicate the effectiveness of BRIDGE, reporting an average 33.4cm localization error in real scenarios.

ACKNOWLEDGMENTS

We are grateful to all anonymous reviewers and the shepherd (Jie Xiong) for their constructive comments. This work is supported in part by National Natural Science Foundation of China (No. 61936015), Natural Science Foundation of Shanghai (No. 24ZR1430600) and Shanghai Key Laboratory of Trusted Data Circulation and Governance, and Web3.

REFERENCES

[1] AAE. Optimisation of order processing in discrete manufacturing through automatic transparency and movement histories, 2023.

[2] ADALM-PLUTO. https://www.analog.com/ADALM-PLUTO, 2024.

[3] Abdulrahman Alarifi, AbdulMalik Al-Salman, Mansour Alsaleh, Ahmad Alnafessah, Suheer Al-Hadhrami, Mai A Al-Ammar, and Hend S Al-Khalifa. Ultra wideband indoor positioning technologies: Analysis and recent advances. *Sensors*, 16(5):707, 2016.

[4] Apple Developer. iBeacon. https://developer.apple.com/ibeacon/, 2024.

[5] ATLA. Atla soars above bottlenecks: Rtls unlocks efficiency in production, 2023.

[6] Bluetooth SIG. Core specification v5.1. https://www.bluetooth.com/specifications/specs/core-specification-5-1/, 2019.

[7] Bluetooth SIG. Bluetooth 2023 market update. https://www.bluetooth.com/2023-market-update/, 2023.

[8] D.G. Brennan. Linear diversity combining techniques. *Proceedings of the IEEE*, 91(2):331–356, 2003.

[9] French Army CENZUB Centre. French army cenzub centre improves multi-unit military cooperation through location technology-powered combat simulation, 2023.

[10] Dongyao Chen, Kang G Shin, Yurong Jiang, and Kyu-Han Kim. Locating and tracking ble beacons with smartphones. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, pages 263–275, 2017.

[11] Yongrui Chen, Zhijun Li, and Tian He. Twinbee: Reliable physical-layer cross-technology communication with symbol-level coding. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 153–161. IEEE, 2018.

[12] Kenneth C Cheung, Stephen S Intille, and Kent Larson. An inexpensive bluetooth-based indoor positioning hack. In *Proceedings of UbiComp*, volume 6, 2006.

[13] Zicheng Chi, Zhichuan Huang, Yao Yao, Tiantian Xie, Hongyu Sun, and Ting Zhu. Emf: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous iot devices. In *IEEE INFOCOM 2017-IEEE conference on computer communications*, pages 1–9. IEEE, 2017.

[14] Zicheng Chi, Yan Li, Hongyu Sun, Yao Yao, Zheng Lu, and Ting Zhu. B2w2: N-way concurrent communication for iot devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 245–258, 2016.

[15] Hsun-Wei Cho and Kang G Shin. Bluefi: bluetooth over wifi. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, pages 475–487, 2021.

[16] Hsun-Wei Cho and Kang G Shin. Flew: fully emulated wifi. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pages 29–41, 2022.

[17] Hsun-Wei Cho and Kang G Shin. Unify: Turning ble/fsk soc into wifi soc. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pages 1–15, 2023.

[18] Marco Cominelli, Paul Patras, and Francesco Gringoli. Dead on arrival: An empirical study of the bluetooth 5.1 positioning system. In *Proceedings of the 13th international workshop on wireless network testbeds, experimental evaluation & characterization*, pages 13–20, 2019.

[19] Mitsubishi Materials Corporation. Mitsubishi materials corporation tracks 80,000 tonnes of copper products in its challenging metal-heavy environment, 2023.

[20] Dusun. Bluetooth technology empowers dusun iot to build a new smart iot ecosystem, 2023.

[21] Dusun. Iot gateway hardware. https://www.dusuniot.com/, 2023.

[22] EJOT. Ejot enjoys operational transparency through the simultaneous tracking of over 8000 orders, 2023.

[23] Dyer Engineering. Dyer engineering's location tracking system has cut costs by up to to £10,000 per month through improved workflow procedures, 2023.

[24] Ramsey Faragher and Robert Harle. Location fingerprinting with bluetooth low energy beacons. *IEEE journal on Selected Areas in Communications*, 33(11):2418–2428, 2015.

[25] Zahid Farid, Rosdiadee Nordin, Mahamod Ismail, et al. Recent advances in wireless indoor localization techniques and system. *Journal of Computer Networks and Communications*, 2013, 2013.

[26] Piotr Gawlowicz, Anatolij Zubow, and Adam Wolisz. Enabling cross-technology communication between lte unlicensed and wifi. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 144–152. IEEE, 2018.

[27] Michele Girolami, Francesco Furfari, Paolo Barsocchi, and Fabio Mavilia. A bluetooth 5.1 dataset based on angle of arrival and rss for indoor localization. *IEEE Access*, 2023.

[28] Jon Gjengset, Jie Xiong, Graeme McPhillips, and Kyle Jamieson. Phaser: Enabling phased array signal processing on commodity wifi access points. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 153–164, 2014.

[29] LOXX Lagerlogistik GmbH. Loxx lagerlogistik gmbh ensures punctual and damage-free delivery to worldwide customer base, 2023.

[30] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. Free your csi: A channel state information extraction platform for modern wi-fi chipsets. In *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, pages 21–28, 2019.

[31] Zhihao Gu, Taiwei He, Junwei Yin, Yuedong Xu, and Jun Wu. Tyrloc: a low-cost multi-technology mimo localization system with a single rf chain. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, pages 228–240, 2021.

[32] Xiuzhen Guo, Yuan He, Jia Zhang, and Haotian Jiang. Wide: Physical-level ctc via digital emulation. In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, pages 49–60, 2019.

[33] HackRF One. https://greatscottgadgets.com/hackrf/one/, 2024.

[34] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. Tool release: Gathering 802.11 n traces with channel state information. *ACM SIGCOMM computer communication review*, 41(1):53–53, 2011.

[35] Yuan He, Xiuzhen Guo, Xiaolong Zheng, Zihao Yu, Jia Zhang, Haotian Jiang, Xin Na, and Jiacheng Zhang. Cross-technology communication for the internet of things: A survey. *ACM Computing Surveys*, 55(5):1–29, 2022.

[36] Heidelberg University Hospital. Personnel tracking during mci training at heidelberg university hospital (ukhd), 2023.

[37] Stavanger University Hospital. Haltian's empathic building hospital solution, 2023.

[38] Chih-Ning Huang and Chia-Tai Chan. Zigbee-based indoor location system by k-nearest neighbor algorithm with weighted rssi. *Procedia Computer Science*, 5:58–65, 2011.

[39] ILR Industries. Ilr industries reduces spread of covid infection and increases productivity through rtls based approach to worker safety, 2023.

[40] Mitsuboshi Metal Industry. Mitsuboshi metal industry has reduced truck driver waiting time by 1,000 hours per year and enabled better transparency of logistics processes, 2023.

[41] INDUTRAX. Deploy location aware solutions quickly and easily, 2023.

[42] INDUTRAX. Location aware software. https://www.indutrax.net/en/, 2023.

[43] K-Hansen. K-hansen relies on cargovis with quuppa intelligent locating system, 2023.

[44] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. Spotfi: Decimeter level localization using wifi. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pages 269–282, 2015.

[45] Manikanta Kotaru and Sachin Katti. Position tracking for virtual reality using commodity wifi. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 68–78, 2017.

[46] Xiangjie Li, Dan Xu, Xuzhi Wang, and Rizwan Muhammad. Design and implementation of indoor positioning system based on ibeacon. In *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, pages 126–130. IEEE, 2016.

[47] Zhijun Li and Yongrui Chen. Bluefi: Physical-layer cross-technology communication from bluetooth to wifi. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pages 399–409. IEEE, 2020.

[48] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 2–14, 2017.

[49] Zhijun Li and Tian He. Longbee: Enabling long-range cross-technology communication. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 162–170. IEEE, 2018.

[50] Xin-Yu Lin, Te-Wei Ho, Cheng-Chung Fang, Zui-Shen Yen, Bey-Jing Yang, and Feipei Lai. A mobile indoor positioning system based on ibeacon technology. In *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 4970–4973. IEEE, 2015.

[51] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Wibeacon: Expanding ble location-based services via wifi. In *Proceedings of the 27th annual international conference on mobile computing and networking*, pages 83–96, 2021.

[52] Martin Woolley. Bluetooth direction finding: A technical overview. https://www.bluetooth.com/wp-content/uploads/Files/developer/RDF_Technical_Overview.pdf, 2025.

[53] Kloeckner Metals. Kloeckner metals achieved 15-20,000 usd more shipments per day as well as better delivery rates and improved operational efficiency through rtl, 2023.

[54] Shaghayegh Monfared, Trung-Hien Nguyen, Luca Petrillo, Philippe De Doncker, and François Horlin. Experimental demonstration of ble transmitter positioning based on aoa estimation. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 856–859. IEEE, 2018.

[55] P.H. Moose. A technique for orthogonal frequency division multiplexing frequency offset correction. *IEEE Transactions on Communications*, 42(10):2908–2914, 1994.

[56] Morita. Morita addressed intricate fire truck production challenges by adopting kokusai kogyo's innovative solution, 2023.

[57] Mizkan Museum. Mizkan museum introduces a seamless, self-guided tour experience, 2023.

[58] Sydney Living Museums. Sydney living museums unveils immersive, technology-based visiting experience, 2023.

[59] USRP N210. https://www.ettus.com/all-products/un210-kit/, 2024.

[60] Azin Neishaboori and Khaled Harras. Energy saving strategies in wifi indoor localization. In *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems*, pages 399–404, 2013.

[61] Nordic Semiconductor. Direction finding white paper. https://docs.nordicsemi.com/bundle/nwp_036/page/WP/nwp_036/intro.html, 2025.

[62] NXP. Mkw41z/31z/21z data sheet. https://www.nxp.com/docs/en/data-sheet/MKW41Z512.pdf, 2018.

[63] University of Fukui Hospital. The university of fukui hospital improves hand hygiene procedures by 300%, 2023.

[64] Giovanni Pau, Fabio Arena, Yonas Engida Gebremariam, and Ilsun You. Bluetooth 5.1: An analysis of direction finding capability for high-precision location services. *Sensors*, 21(11):3589, 2021.

[65] Yiran Peng, Wentao Fan, Xin Dong, and Xing Zhang. An iterative weighted knn (iw-knn) based indoor localization method in bluetooth low energy (ble) environment. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pages 794–800. IEEE, 2016.

[66] Kanyanee Phutcharoen, Monchai Chamchoy, and Pichaya Supanakoon. Accuracy study of indoor positioning with bluetooth low energy beacons. In *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*, pages 24–27. IEEE, 2020.

[67] Xinyou Qiu, Bowen Wang, Jian Wang, and Yuan Shen. Aoa-based ble localization with carrier frequency offset mitigation. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–5. IEEE, 2020.

[68] Quuppa. Quuppa intelligent locating system. https://www.quuppa.com/, 2023.

[69] Fabio Ricciato, Savio Sciancalepore, Francesco Gringoli, Nicolò Facchi, and Gennaro Boggia. Position and velocity estimation of a non-cooperative source from asynchronous packet arrival time measurements. *IEEE Transactions on Mobile Computing*, 17(9):2166–2179, 2018.

[70] Pradeep Sambu and Myounggyu Won. An experimental study on direction finding of bluetooth 5.1: Indoor vs outdoor. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1934–1939. IEEE, 2022.

[71] Bluetooth SIG. Core specification 4.2 of the bluetooth system, 2023.

[72] Silicon Labs. An1297: Custom direction-finding solutions using the silicon labs bluetooth stack. https://www.silabs.com/documents/public/application-notes/an1297-custom-direction-finding-solutions-silicon-labs-bluetooth.pdf, 2021.

[73] Silicon Labs. Bg22 dual polarized antenna array radio board. https://www.silabs.com/documents/public/schematic-files/BRD4191A-A02-schematic.pdf, 2024.

[74] Silicon Labs. Efr32xg22 wireless gecko starter kit. https://www.silabs.com/development-tools/wireless/efr32xg22-wireless-starter-kit, 2024.

[75] Silicon Labs. Silicon labs bg22 bluetooth dual polarized antenna array pro kit. https://www.silabs.com/development-tools/wireless/bluetooth/bgm22-pro-kit, 2024.

[76] Silicon Labs. Simplicity studio. https://www.silabs.com/developer-tools/simplicity-studio, 2024.

[77] Elahe Soltanaghaei, Avinash Kalyanaraman, and Kamin Whitehouse. Multipath triangulation: Decimeter-level wifi localization and orientation with a single unaided receiver. In *Proceedings of the 16th annual international conference on mobile systems, applications, and services*, pages 376–388, 2018.

[78] KISSEL Spedition. The pke solutions provides a new dimension to the fast paced-logistics environment, 2023.

[79] Yang-Hsi Su, Chouchang Jack Yang, Euiseok Hwang, and Alanson P Sample. Single packet, single channel, switched antenna array for rf localization. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(2):1–25, 2023.

[80] Nitesh B Suryavanshi, K Viswavardhan Reddy, and Vishnu R Chandrika. Direction finding capability in bluetooth 5.1 standard. In *Ubiquitous Communications and Network Computing: Second EAI International Conference, Bangalore, India, February 8–10, 2019, Proceedings 2*, pages

53–65. Springer, 2019.

[81] Xiaohua Tian, Ruofei Shen, Duowen Liu, Yutian Wen, and Xinbing Wang. Performance analysis of rss fingerprinting based indoor localization. *IEEE Transactions on Mobile Computing*, 16(10):2847–2861, 2016.

[82] Tigros. Tigros achieves maximised operational efficiencies within 18 months of rtls implementation, 2023.

[83] Ltd. Toshin Industry Co. Toshin industry co., ltd. reduces product search times from 20 minutes to 2 minutes, 2023.

[84] DGS Transports. Optimising logistics handling – cargovis indoor positioning at dgs transports, 2023.

[85] Traxmate. Tracking everything everywhere. https://traxmate.io/, 2023.

[86] traxmate. Warehouses and logistics, 2023.

[87] U-blox. Bluetooth indoor positioning. https://www.u-blox.com/en/technologies/bluetooth-indoor-positioning, 2023.

[88] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 165–178, 2016.

[89] Liiga & Veikkaus. Liiga & veikaus deliver engaging results through rtls to hockey spectators, 2023.

[90] VEO. Veo – technicians' daily work made easier by modern indoor positioning, 2023.

[91] Yixin Wang, Qiang Ye, Jie Cheng, and Lei Wang. Rssi-based bluetooth indoor localization. In *2015 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pages 165–171, 2015.

[92] Martin Woolley. The bluetooth low energy primer. *Bluetooth Blog*, 15:2022, 2022.

[93] Yaxiong Xie, Zhenjiang Li, and Mo Li. Precise power delay profiling with commodity wifi. In *Proceedings of the 21st Annual international conference on Mobile Computing and Networking*, pages 53–64, 2015.

[94] Yaxiong Xie, Jie Xiong, Mo Li, and Kyle Jamieson. md-track: Leveraging multi-dimensionality for passive indoor wi-fi tracking. In *The 25th Annual International Conference on Mobile Computing and Networking*, pages 1–16, 2019.

[95] Mohammadreza Yavari and Bradford G Nickerson. Ultra wideband wireless positioning systems. *Dept. Faculty Comput. Sci., Univ. New Brunswick, Fredericton, NB, Canada, Tech. Rep. TR14-230*, 40, 2014.

[96] YMCA. The ymca has improved customer experience while simultaneously improving safety standards through the tracking of swimmers fitness, 2023.

[97] Yuan Zhuang, Chongyang Zhang, Jianzhu Huai, You Li, Liang Chen, and Ruizhi Chen. Bluetooth localization technology: Principles, applications, and future trends. *IEEE Internet of Things Journal*, 9(23):23506–23524, 2022.