# TyrLoc: A Low-cost Multi-technology MIMO Localization System with A Single RF Chain


Zhihao Gu
Fudan University
zhgu19@fudan.edu.cn

Taiwei He
Fudan University
twhe20@fudan.edu.cn

Junwei Yin
Fudan University
jwyin15@fudan.edu.cn

Yuedong Xu
Fudan University
ydxu@fudan.edu.cn

Jun Wu
Fudan University
wujun@fudan.edu.cn



## ABSTRACT

This work presents the design and implementation of TyrLoc, an accurate multi-technology switching MIMO localization system that can be deployed on low-cost SDRs. TyrLoc only uses a ***single RF Chain*** to switch on each antenna in an antenna array within the coherence time asynchronously, thus mimicking a MIMO platform to pinpoint the positions of WIFI, Bluetooth Low Energy (BLE) and LoRa devices. TyrLoc makes three key technical contributions. First, TyrLoc modifies the firmware of inexpensive PlutoSDR that controls the antenna switching pattern and tags the signal associated with each antenna. Second, it develops a two-stage fine-grained carrier frequency offset (CFO) calibration algorithm that harnesses the agile antenna switching pattern and is 10× more accurate than the baseline method. Third, TyrLoc employs an interpolated transform approach to facilitate angle-of-arrival (AoA) estimation in the presence of missing antennas. The AoA-based localization experiments in a multipath-rich indoor environment show that TyrLoc with eight antennas achieves the median errors of 63cm for WIFI, 39cm for BLE and 32cm for LoRa, respectively.



## CCS CONCEPTS

• **Networks** → **Location based services**.

## KEYWORDS

Switching MIMO, CFO Calibration, Localization, SDR

**ACM Reference Format:**
Zhihao Gu, Taiwei He, Junwei Yin, Yuedong Xu, and Jun Wu. 2021. TyrLoc: A Low-cost Multi-technology MIMO Localization System with A Single RF Chain. In *The 19th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '21), June 24–July 2, 2021, Virtual, WI, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3458864.3467677




*MobiSys '21, June 24–July 2, 2021, Virtual, WI, USA*



ACM ISBN 978-1-4503-8443-8/21/06…$15.00
https://doi.org/10.1145/3458864.3467677


| | WIFI [19–21] | BLE [26–29] | LoRa [31–33] |
|---|---|---|---|
| **Technique** | CSI | RSSI | RSSI / ToF |
| **Accuarcy** | $\sim 10^{-1}m$ | $\sim 10^{0}m$ | $10^{0} \sim 10^{1}m$ |
| **Advantage** | Ubiquity | Low power | Large scale |

**Table 1: Comparison of various protocols.**

## 1 INTRODUCTION

Indoor localization is playing a crucial role in many applications including shopping navigation, security surveillance [9, 10], augmented reality [11, 12, 20] and health monitoring [13–15]. In particular, RF-based localization systems become increasingly popular due to the pervasive usage of WIFI, Bluetooth Low Energy (BLE) and LoRa devices. For example, WIFI network has been deployed almost in every building, offering seamless network coverage; BLE has a variety of applications in household appliances such as laundry machine and portable devices such as wireless earphone; LoRa provides wireless communication capability for different kinds of sensors attached to industrial equipment in factories and smart electric meter at home. Many efforts have been dedicated to building localization systems based on WIFI [16–25], BLE [26–30] and LoRa [31–35]. Existing studies have mainly devoted to designing and implementing advanced signal processing methods in order to achieve higher accuracy of localization. Albeit their success in using commodity devices, several major issues still exist.

- **Absence of Multi-technology Functionality.** There lacks an inexpensive indoor localization system that provides universal positioning service for mainstream RF technologies including WIFI, BLE and LoRa.
- **Small Size of Antenna Array.** The accuracy of localization is largely determined by the size of the antenna array. The off-the-shelf devices are usually equipped with only a few RF chains, each of which connects to an antenna element, thus throttling the array size.

Each technique has its own strengths and suitable scenarios. The ubiquitous deployment of WIFI devices offers an easy access to WIFI-based localization service. Compared with WIFI, BLE is more suitable for low-power portable devices to extend their battery lifespan. LoRa is well-known for its long range transmission and strong penetration ability. In large-scale indoor environment, only a few anchor points based on LoRa can provide wide range positioning services. The necessity for multi-technology localization begins to

**Table 2: Comparison of off-the-shelf Software Defined Radios.**

| | PlutoSDR [1] | HackRF [2] | BladeRF x40 [3] | BladeRF-2.0 xA9 [4] | USRP B210 [5] | WARP v3 [6] |
|---|---|---|---|---|---|---|
| **RF Port** | SISO | SISO | SISO | 2 × 2 MIMO | 2 × 2 MIMO | 2 × 2 MIMO |
| **RF Coverage** | 70M~6GHz[1] | 1M~6GHz | 380M~3.8GHz | 47M~6GHz | 70M~6GHz | 2.4G/5G Band |
| **Bandwidth** | 56MHz | 20MHz | 28MHz | 56MHz | 56MHz | 40MHz |
| **ADC Resolution** | 12-bit | 8-bit | 12-bit | 12-bit | 12-bit | 12-bit |
| **Max Sample Rate** | 61.44 MSPS | 20 MSPS | 40 MSPS | 61.44 MSPS | 61.44MSPS | 100 MSPS |
| **Price** | $150 | $320 | $420 | $720 | $1282 | $5000 |

unfold as different types of RF signals coexist, thus creating an immersive multi-modal wireless environment. An intuitive solution is to employ one specialized localization system for each technology, yet bundling all of them together is cumbersome and cost inefficient. The favorable concept of localization with commodity devices ignores its potential drawbacks. For instance, accurate WIFI localization attributes to the acquisition of channel state information (CSI) that can be extracted from very few network interface cards via Intel 5300 CSI Tool [36] or Atheros CSI Tool [37]. As for BLE and LoRa, there does not exist a commodity device that offers the public functionality of acquiring channel information containing phase offset and amplitude attenuation. The lack of rich channel information restricts the their positioning accuracy. As shown in Tabel 1, for BLE and LoRa, the localization accuracy is markedly lower than WIFI if only utilizes the RSSI or ToF provided by commodity device. Hence, we advertise the use of software-defined radios (SDRs) for *universal* localization in which the receiver is capable of operating on a much wider spectrum and an agile channel bandwidth.

The popular SDRs with their performance parameters are listed in Table 2. The high-end SDRs are equipped with MIMO ports, the low-end SDRs are usually SISO, and they differ significantly in their prices. In general, RF positioning accuracy relies heavily on the size of antenna array [40]. To create a large array, we might have to synchronize multiple high-end MIMO SDRs such as USRP and WARP for more antennas (most of low-end SDRs do not support synchronization), thus pushing up the price of the universal localization system severalfold. One crucial question arises: *can we design a universal multi-technology localization system with inexpensive and portable SISO SDRs?*

To circumvent the limitation of small antenna array size, a promising approach is to employ an RF switch to create a large virtual antenna array with more antennas than RF chains. The basic idea is depicted in Fig. 1(a). By using an RF switch to connect an RF chain to different antennas asynchronously, then combining the signals received from different antennas to construct a virtual synchronous antenna array, one can utilize the received signals within the coherence time to refine the accuracy of AoA estimation. In SWAN, Xie *et al.* stitched twelve antennas to form a novel general-purpose antenna array with commodity MIMO WIFI using Atheros CSI tool [18]. This multi-functional and cost-efficient system is specialized in WIFI, yet not applicable to alternative ubiquitous Bluetooth and LoRa protocols. Phaser [22] utilizes a signal splitter to synchronize two Intel 5300 NICs to form an array of five antenna. In iArk, An *et al.* uses nine RF switches and a high-end MIMO SDR (USRP-2950) to implement a powerful 8 × 8 antenna array [38]. It supports multiple wireless IoT protocols and achieves high AoA accuracy, but the high cost of the SDR might restrict its large-scale deployment to some extent. More importantly, SWAN, Phaser and iArk all need multiple synchronous RF chains in which at least one RF chain connects to an antenna invariably to generate reference signals for carrier frequency offset (CFO) calibration. This single RF chain defect imposes great difficulties of transforming low-end SISO SDRs into powerful MIMO platforms.

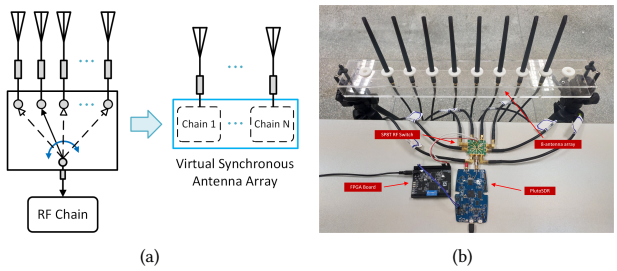



**Figure 1: (a) The basic idea of constructing a virtual synchronous antenna array based on RF switch. (b) The hardware demonstration of TyrLoc prototype.**

In this paper, we design TyrLoc using a low-end PlutoSDR with a single RF chain and an array of extended antennas. TyrLoc offers the virtual MIMO functionality that yields a high accuracy of indoor localization. Fig. 1(b) demonstrates the TyrLoc prototype built with a PlutoSDR (~ $150), an RF switch (~ $19) and an FPGA borad (~ $22, the FPGA chip inside is ~ $3.5), and the major challenges of designing and implementing TyrLoc are threefold.

**Challenges #1:** *How can we modify the firmware of low-end PlutoSDR to enable the MIMO functionality?*

In TyrLoc, an FPGA board together with a single-port-eight-throw (SP8T) RF switch is deployed to control the antenna switching mode. The FPGA module of PlutoSDR is modified to allow the unused six bits of ADC output to encode the identities of antennas. A serial-parallel conversion module is designed to address the inadequate GPIO problem, and synchronize the tagged data with the antenna switching.

**Challenges #2:** *How can we calibrate the phase offset caused by CFO without a reference RF chain?*

CFO represents the frequency mismatch of the oscillators between a transmitter and a receiver that introduces an additional term in the received signal phases, and this phase offset accumulates over time. With a reference antenna connected to an RF chain,

[1]The RF coverage marked in the technical document is 325M~3.8GHz, but it can actually work at 70M~6G.

the CFO induced phase offsets can be canceled out [18, 22, 38]. When such a reference antenna is absent, the phase offsets on asynchronously activated antennas will be dominated by the CFO, rather than the propagation distances from the signal source to the antenna array. We propose a novel two-stage CFO calibration approach for the single RF virtual MIMO system. The first stage utilizes the intra-packet symbols to narrow down the CFO to a few hundred Hertz. The second stage uses the inter-packet symbols to refine the CFO estimation, and exploits the switching pattern to cancel out the impact of the residual CFO on the signal phases received at different antennas.

**Challenges #3:** *How can we ensure the robustness of AoA estimation if no packet received in a switching interval?*

With the virtual MIMO provided by TyrLoc, we can estimate the AoAs of multipath propagation using the classic MUSIC algorithm [39]. The multipath signals are usually coherent so that the spatial smoothing method [41] is introduced to enhance the MUSIC algorithm. When TyrLoc switches to an antenna in the wild, it is highly possible that no packet transmission happens or the packet is lost at a slot. Then, some channel information is missing such that the virtual MIMO array becomes *non-uniform*, and the standard spatial smoothing is no longer applicable. We adopt the interpolated array transform [42] to convert a non-uniform array into a virtual uniform array that facilitates the operation of the MUSIC algorithm with spatial smoothing.

With TyrLoc's virtual MIMO capability, we estimate the angle of arrival (AoA) using the MUSIC algorithm with spatial smoothing for WIFI, BLE and LoRa devices in typical indoor environments, and further estimate their locations via the maximum likelihood method. Experimental results show that the median error of AoA estimation is 4.1° for WIFI, 2.9° for BLE, and 2.3° for LoRa in an $105m^2$ room. For localization, TyrLoc with eight-antenna array achieves the median errors of 63cm for WIFI, 39cm for BLE and 32cm for LoRa in multipath rich offices of $61m^2$ and $105m^2$. The tracking experiment also manifests the accuracy and consistency of Tyrloc's localization performance. The cross-comparisons show that LoRa is more resistant to long distance and Non-Line-of-Sight (NLoS) transmission than WIFI and BLE.

## 2 SYSTEM OVERVIEW

The TyrLoc system consists of three key components: antenna switching hardware module, signal processing software module and multi-technology localization module. The hardware and the software components work as a unity to transform a low-cost commodity SDR with a single RF chain into a multi-functional MIMO platform.

**1) Antenna Switching Hardware.** The hardware module transforms the commodity PlutoSDR equipped with a single pair of transceivers into a virtual MIMO platform with an array of eight antennas.

**- Switch Controller.** TyrLoc connects the RF chain of PlutoSDR to a single-port-eight-throw (SP8T) RF switch, and deploys an FPGA board to control the antenna switching.

**- Antenna Tagging.** TyrLoc takes advantage of the unused six bits of ADC output to encode each antenna and decode its identity.

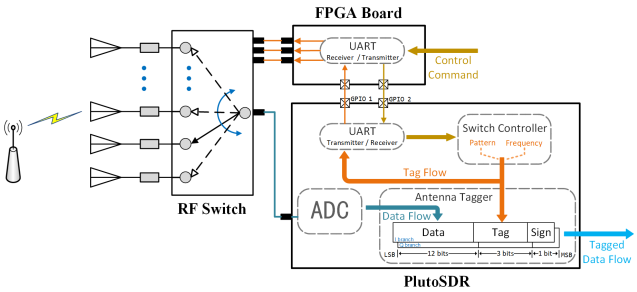



**Figure 2: The hardware architecture of TyrLoc.**

Theoretically, TyrLoc can support a large-scale array with up to 64 antennas.

**- UART Design.** TyrLoc implements a universal asynchronous receiver-transmitter (UART) module to convert the parallel control signal into the serial signal, and synchronize the tagged data with the antenna switching.

**2) Signal Processing Software.** In the software module, TyrLoc stitches the time asynchronous baseband signal samples received on different antennas so that the aligned signals can be utilized for channel parameter estimation therewith.

**- Packet Detection.** TyrLoc receives packets passively and detects the starting time of a WIFI packet through Schmidl-Cox algorithm [43]. For BLE and LoRa, the packet detection is performed according to their preamble structures. For each technology (i.e. WIFI, BLE and LoRa), a preamble detector is developed.

**- Asynchronous CFO Estimation.** TyrLoc designs a two-stage CFO calibration approach to mitigate the phase drift after antenna switching. This constitutes the major novelty of TyrLoc.

**- AoA Estimation for Non-uniform Array.** TyrLoc utilizes the beamsteering capability of virtual antenna array to obtain the direction of the WIFI, BLE or LoRa source using the MUSIC algorithm with interpolated array transform and spatial smoothing techniques.

**3) Multi-technology Localization.** TyrLoc makes use of multiple antenna diversity to enable accurate indoor localization. Two PlutoSDRs are used to perform the AoA-based localization for WIFI, BLE and LoRa devices. The algorithms of two-stage CFO calibration and building virtual antenna array are protocol independent. TyrLoc can provide indoor localization service based on more wireless protocols by adding corresponding preamble detectors.

## 3 TYRLOC HARDWARE DESIGN

In this section, we introduce the detailed hardware implementation of TyrLoc. Fig. 2 illustrates the hardware architecture of TyrLoc. It is composed of a vanilla ADALM-PLUTO SDR (PlutoSDR), a single-port-eight-throw (SP8T) RF switch and an FPGA board. PlutoSDR is a type of commonly used, off-the-shelf, low-cost and programmable SDR platform. Its detailed information is listed in Table 2. The SP8T extends the single receiving port of PlutoSDR to accommodate an array of eight antennas. The FPGA board is placed between PlutoSDR and SP8T, and connects them with dupont lines. It receives the serial signals from PlutoSDR and converts it into 3-bit parallel signals to enable the RF switch to work at pre-design switching frequency and pattern.

Implementing the switch controller is a very challenging task where we name a few difficulties below.

- How can we modify the PlutoSDR firmware to generate cyclic control signals?
- How can the PlutoSDR transmit parallel control signals to SP8T or receive control commands through only two unused general-purpose input/output (GPIO) ports?
- How can we eliminate the asynchronization between the received signal and the antenna switching?

The PlutoSDR uses Xilinx Zynq 7010 as the processing core. We exploit the remaining logic resources of Zynq 7010 to process the augmented functions.

**Switch Controller.** We design the switch controller based on a finite state machine, which works with the ADC synchronously. In Fig. 2, the brown line represents the transmission flow of control commands. The switch controller can decode control commands and generate cyclic control signals according to certain switching frequencies and patterns. The output of the switch controller, called tag flow, is used to tag the data flow from the ADC and transmitted to the UART module.

**Control Signal Conversion.** Only two GPIO ports remain unused in PlutoSDR, thus restricting us to directly control the SP8T RF switch which needs three control inputs in parallel. Besides, one or more control inputs are required to change the switching frequency or the pattern. The UART module is designed to transform the parallel control signal into serial signal so that we can send it to the FPGA board through GPIO Port #1. The FPGA board is also implemented with a UART module to recover the serial signal into 3-bit control inputs of the RF switch. With the UART module and GPIO Port #2, we can send control commands to the switch controller in order to change the switching pattern or frequency promptly.

**ID Tagging.** When the signals from different antennas are exported from the same RF chain, they cannot be differentiated so that the virtual antenna array cannot be constructed. Therefore, it is inevitable to modify the PlutoSDR firmware to tag the data collected from each antenna. In PlutoSDR, the programming part of Zynq 7010 is used to process the raw data from the ADC. As shown in Fig. 2, the ADC output includes the In-Phase (I) branch and the Quadrature (Q) branch. The output format of each branch is a 16-bit integer, while the accuracy of ADC is only 12 bits. Taking the I-branch as an example, the highest bit (i.e. the $15^{th}$ bit) is the sign bit, the lower 3 bits (i.e. the $12^{th}$~$14^{th}$ bits) are unused, and the remaining 12 bits (i.e. the $0^{th}$~$11^{th}$ bits) are the valid ADC data. It inspires us to turn these unused bits into antenna tags. We use the RF switch control signals generated by the switch controller to replace the $12^{th}$~$14^{th}$ bits of the data flow. Combining the I- and Q-branch together, we can convert 6 unused bits into antenna tags, thus supporting an extended array of up to 64 antennas. We implement the tagging function in the PlutoSDR firmware with Verilog codes.

**ID Extraction.** In the backend, each received sample point is represented by a 32-bit complex number, the first half of which represents the real part, and the remaining half represents the imaginary part. We can extract the $12^{th}$~$14^{th}$ bits of real and imaginary parts, then convert them into the antenna ID. TyrLoc stamps the $12^{th}$~$14^{th}$ bits of Q-branch with the antenna ID. The 3-bit signals from "000" to "111" correspond to eight antennas. Then, TyrLoc can easily distinguish the signals coming from different antennas.

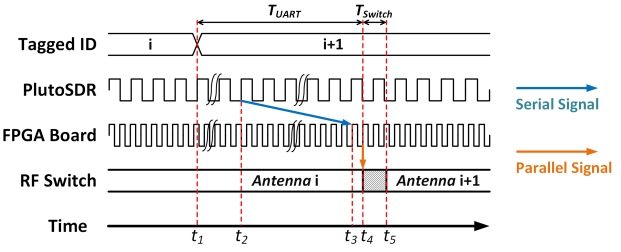



**Figure 3: The timing sequence of TyrLoc.**

**Data and Antenna synchronization.** UART is an asynchronous communication module. At the meantime, the RF switch also takes a little time to complete the switching. It will introduce some time delay, causing the switching of antennas to lag behind the ID tagging. Therefore, we need to eliminate this delay before processing the received signals. The time sequence of TyrLoc is illustrated in Fig. 3 and the delay can be expressed as:

$$\begin{aligned} T_{Delay} &= T_{UART} + T_{Switch} \\ &= (42T_{Pluto} + 10T_{Baud} + T_{FPGA}) + T_{Switch} \end{aligned} \tag{1}$$

The entire delay can be divided into UART transmission delay $T_{UART}$ and the switching time $T_{Switch}$ of the RF switch. In the first part, $T_{Pluto}$ and $T_{FPGA}$ represent one clock period of PlutoSDR and FPGA board respectively. $T_{Baud}$ is the time for UART to send one bit. At $t_1$, the antenna ID tagged to the data flow changes from $i$ to $i+1$. Then, it totally takes 42 clock periods to trigger the UART module from the idle state to sending state and update the voltage of GPIO. We choose the signal sample clock as the UART clock in the PlutoSDR, thus $t_2 - t_1 = 42T_{Pluto}$. From $t_2$ to $t_3$, PlutoSDR is sending the serial signal to the FPGA board. The serial signal consists of one start bit, eight data bits and one stop bit, thus taking $10T_{Baud}$ to transmit the signal. The FPGA board also takes one clock period to detect the beginning of serial data transmission, thus the parallel control signal of RF switch will not update until $t_4$. Then, the RF switch takes time to complete the switching from antenna $i$ to $i+1$. During this period, the received signal is regard as invalid and it will be discarded. In TyrLoc, $T_{Baud}$ is $4us$, $T_{Pluto} = 1/f_{sample\,rate}$ is decided by the sample frequency of PlutoSDR, $T_{FPGA}$ equals $20ns$ and the $T_{Switch}$ is typically $150ns$ [8].

## 4 CFO MODEL WITH ASYNCHRONISM

The phase offset caused by carrier frequency offset (CFO) is the major obstacle that hinders us from directly constructing an antenna array based on single RF chain. In this section, we describe the mathematical model of CFO and analyze its impact on an asynchronous antenna array.

### 4.1 Carrier Frequency Offset Model

CFO is an essential phenomenon in wireless communication systems, mainly attributed to the unaligned carrier frequency between the oscillator of the transmitter and that of the receiver. The oscillators are produced by different manufactures at various standards

so that CFO always exists and may drift over time [44, 47]. Existing CFO calibration algorithms are designed for communication purposes, pursuing extremely high time efficiency, while allows relatively large estimation errors (e.g. several hundred Hertz) that does not influence packet receptions but are *detrimental* to our AoA estimation. The influence of CFO on signal phase will be described in detail below.

Denote by $f_{tx}$ and $f_{rx}$ the carrier frequencies of *Tx* and *Rx* respectively, and denote by $\Delta f = f_{tx} - f_{rx}$ the CFO of the *Tx*-*Rx* pair. The mathematical model of signal transmission (ignoring noise) is given by

$$\begin{aligned} y(t) &= [(s(t)e^{j2\pi f_{tx}t}) * h_c(t)]e^{-j2\pi f_{rx}t} \\ &= e^{-j2\pi f_{rx}t}\int s(t-\tau)e^{j2\pi f_{tx}(t-\tau)}h_c(\tau)\,d\tau \\ &= e^{j2\pi\Delta f t}\int s(t-\tau)e^{-j2\pi f_{tx}\tau}h_c(\tau)\,d\tau \\ &= e^{j2\pi\Delta f t}\int s(t-\tau)h(\tau)\,d\tau \\ &= e^{j2\pi\Delta f t}[s(t)*h(t)] \end{aligned} \tag{2}$$

where $s(t)$ is the baseband signal, $h_c(t)$ represents the channel impulse response, $h(\tau) = e^{-j2\pi f_{tx}\tau}h_c(\tau)$, and $*$ is the convolution operator. The transmitter upconverts the baseband signal $s(t)$ to the carrier $f_{tx}$, then the receiver downconverts the signal from the carrier by multiplying $e^{-j2\pi f_{rx}t}$.

If two duplicated raw signals $s(t)$ and $s(t+T)$ (i.e. $s(t) = s(t+T)$) are transmitted with an interval $T$, the received signals $y(t)$ and $y(t+T)$ are expressed as

$$\begin{cases} y(t) = e^{j2\pi\Delta f t}[s(t)*h(t)] \\ y(t+T) = e^{j2\pi\Delta f(t+T)}[s(t+T)*h(t+T)] \end{cases} \tag{3}$$

During the coherence time, the channel impulse response is essentially invariant, thus $h(t) = h(t+T)$. Then, we obtain

$$y(t+T) = e^{j2\pi\Delta f T}y(t) \tag{4}$$

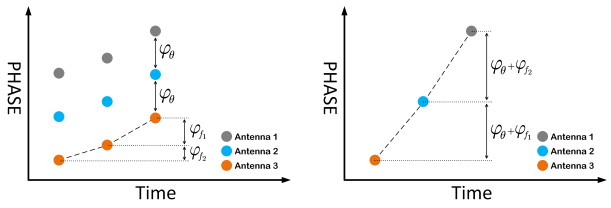
Notice that $y(t+T)$ is being rotated by $e^{j2\pi\Delta f T}$ on the basis of $y(t)$. As time interval $T$ increases, the phase shift accumulates over time. For instance, an 802.11n WIFI system operates at 5GHz band and its center frequency tolerance is ±20ppm [45] which means that the CFO may reach ±200kHz. If CFO is merely 10kHz, much smaller than the error boundary, time interval is $2ms$, the phase offset caused by CFO equals $40\pi$ which is intolerable for any phase related applications.

## 4.2 Model of Asynchronous Array

TyrLoc employs an asynchronous antenna array so that the signals on different antennas are received at different time slots. The phase distortion caused by CFO hinders us from directly grouping the phase of antenna array. To eliminate the influence of CFO, we define the phase model of the asynchronous uniform linear array with M antennas. Given the $i^{th}$ packet $pkt(i)$ is received by antenna $x_i$.

$$\varphi_i = (\varphi_{i-1} + 2\pi\cdot\Delta f_i\cdot T_i + 2\pi d\sin\theta/\lambda) \bmod 2\pi \tag{5}$$

where $\varphi_i$ is the phase of $pkt(i)$ received by antenna $x_i$, $\Delta f_i$ is the CFO while switching to $x_i$, $T_i$ represents the time interval between $pkt(i-1)$ and $pkt(i)$, and it is usually variable for different $i$, $\theta$ denotes the Angle of Arrival (AoA) of the signal source, $d$ is the spacing between two adjacent antennas and $\lambda$ is the signal wavelength.




(a) Synchronous array (b) Asynchronous array

**Figure 4: Signal phases of a 3-antenna array: synchronous vs asynchronous.**

We compare the phases of received signals by three antennas in Fig. 4. The left side is for the synchronous array and the right side is for the asynchronous one. The horizontal coordinate records the receiving times of three consecutive packets, and the vertical coordinate measures their phases. For the synchronous array, the relative phase differences $\varphi_\theta$ between antennas are caused by the different propagation distances from the signal source to the antennas, and the phase shift $\varphi_{f_i}$ between adjacent slots is caused by the CFO. The CFO does not distort the AoA estimation because it only uses the simultaneously received signals. While for the asynchronous array, only the phases in Fig. 4(b) can be measured, and the phase difference between pairwise antennas contains an additional unknowns $\varphi_{f_i}$, preventing the calculation of $\varphi_\theta$.

**Misunderstanding 1.** *Supposing $\Delta f_i$ to be similar, the M-element antenna array can establish $M-1$ equations in* (5)*. They can be used to estimate the parameter $\theta$.*

This approach does not work for three reasons. One is that CFO is not constant over time as the clocks drift [44, 47], as shown in Fig. 7. Another is only one arriving angle can be inferred in this way, while traditional AoA algorithms can estimate the angles of multipath signals. The third is that the equations are ill-conditioned if $T_i$ and $T_j$ are sufficiently close. Thus, the numerical calculation of CFO and $\theta$ might be wrong from time to time.

**Misunderstanding 2.** *We only use one antenna to receive signals at different time slots, thus $\theta = 0^\circ$ and Eq.* (5) *can be simplified as $\varphi_i = (\varphi_{i-1} + 2\pi\cdot\Delta f_i\cdot T_i) \bmod 2\pi$. Then, $\Delta f_i$ is calculated based on $\varphi_i$ and $\varphi_{i-1}$.*

CFO can be as high as 10kHz and the inter-packet delay $T_i$ is usually larger than $1ms$. Hence, the term $2\pi\cdot\Delta f\cdot T_i$ is much larger than $2\pi$ so that the CFO-induced phase shift has rotated $2\pi$ for many rounds. Besides, other factors such as IEEE 802.11 carrier sensing mechanism might cause $T_i$ inconsistent so that the CFO induced phase shift changes greatly. For a non-linear equation set, estimating the amount of rotations through trial-and-error does not work well.

# 5 TWO-STAGE CFO ESTIMATION

With the help of TyrLoc's hardware platform, the signals can be harvested by the virtual antenna array. In this section, we present a novel method for fine-grained CFO calibration.

## 5.1 Moose Algorithm.

TyrLoc employs Moose algorithm [46] to perform the CFO estimation. It relies on the duplicated training sequences contained in the preamble. The basic idea and main operations of Moose algorithm are as follows.

We transform Eq. (3) into its discrete form. Here, $s_n$ is the $n^{th}$ sample point of a symbol, and $s_{n+N}$ denotes the repeated point of $s_n$, where $N$ is the amount of intervals between the two identical symbols. Then, the received signals $y_n$ and $y_{n+N}$ are given by

$$\begin{cases} y_n = e^{j2\pi\Delta_f nT}(s_n * h_n) + w_n \\ y_{n+N} = e^{j2\pi\Delta_f (n+N)T}(s_{n+N} * h_{n+N}) + w_{n+N} \end{cases} \tag{6}$$

where $h$ is the weighted channel impulse response, $w$ is the zero-mean white Gaussian noise and $T$ is the sampling interval. For each point $s_n$, the received signal is $y_n$ that is modeled as a function with regard to $s_n$, $\Delta f$ and the channel impulse response. Then, using the fact $s_n = s_{n+N}$ and the assumption $h_n = h_{n+N}$ within the coherence time, there exists

$$\begin{aligned} y_{n+N} &= (y_n - w_n)e^{j2\pi\Delta fNT} + w_{n+N} \\ &= y_n e^{j2\pi\Delta fNT} - w_n e^{j2\pi\Delta fNT} + w_{n+N} \\ &= y_n e^{j2\pi\Delta fNT} + w'_{n+N} \end{aligned} \tag{7}$$

For $n = 1, 2, 3, ..., N$, we obtain

$$\begin{bmatrix} y_{N+1} \\ y_{N+2} \\ \vdots \\ y_{2N} \end{bmatrix} = e^{j2\pi\Delta fNT} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} + \begin{bmatrix} w'_{N+1} \\ w'_{N+2} \\ \vdots \\ w'_{2N} \end{bmatrix} \tag{8}$$

The maximum likelihood estimation of CFO is given by

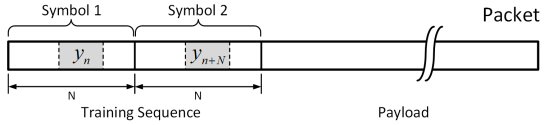
$$\Delta\hat{f} = \frac{1}{2\pi NT}\angle\left(\frac{\sum_{n=1}^{N}\bar{y}_n y_{n+N}}{\sum_{n=1}^{N}\bar{y}_n y_n}\right) = \frac{1}{2\pi NT}\angle\left(\sum_{n=1}^{N}\bar{y}_n y_{n+N}\right) \tag{9}$$

The variance of $\Delta\hat{f}$ is determined by

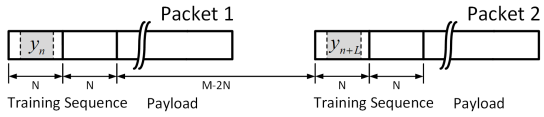
$$\mathrm{Var}(\Delta\hat{f}) = \frac{1}{4\pi^2 T_i^2 L \cdot SNR} \tag{10}$$

where $T_i = NT$ is the time interval between two identical symbols of training sequence, $L = N$ is the length of a training symbol in the preamble. The Moose algorithm is incapable to yield an accurate CFO estimate for the subsequent AoA estimation. Still taking 802.11n as an example, we can calculate the standard deviation of CFO estimation to be 197Hz when the SNR is 30dB, the length of training symbol is 64 and the symbol interval is 3.2$us$. Given the switching interval 2$ms$, the resulted calibration error is more than 2 $rad$, overwhelming the relative phase differences caused by the diverse $Tx$-$Rx$ signal propagation distances.

According to the Eq. (10), the variance of CFO estimation depends on time interval $T_i$ and length of training symbols. The classic Moose algorithm exploits two neighbouring training symbols in a preamble (e.g. Fig. 5(a)), while we perform the Moose algorithm on two training sequences of consecutive packets (e.g. Fig. 5(b)). To differentiate, we denote by $T_i = T_{sym}$ if two symbols come from the same packet, and by $T_i = T_{pkt}$ if they come from two consecutive packets. In general, $T_{sym}$ is at the $\mu s$ granularity, and $T_{pkt}$ is at the $ms$ granularity, i.e. $T_{pkt} \gg T_{sym}$. Therefore, the variance of $\Delta\hat{f}$ is relatively large (resp. small) when using intra-packet (resp. inter-packet) symbols.




(a) Intra-packet CFO estimation




(b) Inter-packet CFO estimation

**Figure 5: Moose algorithm: intra-packet and inter-packet.**

The CFO estimation range of Moose algorithm is determined by

$$|\Delta f|_{max} < \frac{1}{2T_i} \tag{11}$$

Intuitively, the intra-packet CFO estimation (i.e. $T_i = T_{sym}$) has a wide range but is less accurate, while the inter-packet CFO estimation (i.e. $T_i = T_{pkt}$) has a narrow range but is more accurate. In TyrLoc, the initial CFO may be very large (e.g. 10kHz for WIFI and BLE), which exceeds the estimation range of inter-packet method. Therefore, Moose algorithm cannot be directly used to estimate the CFO across the packets received on different antennas.

## 5.2 Two-stage Logic.

TyrLoc comes up with a two-stage CFO estimation approach. The basic idea of our solution is shown in Fig. 6.

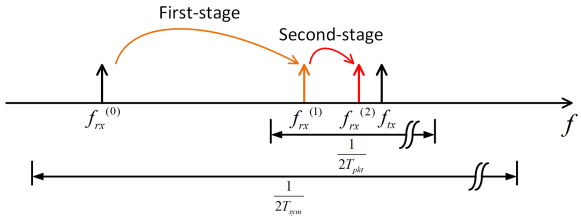



**Figure 6: Illustration of the two-stage CFO calibration.**

**Coarse Estimation: Intra-paket.** In the first stage, TyrLoc uses the short and long training symbols of WIFI, the entire preamble of BLE, and the consecutive symbols in the preamble of LoRa to perform the intra-packet CFO estimation. We estimate the CFO for twenty rounds and obtain preliminary CFO estimates. As shown in Fig. 6, in the first stage, the average of these CFO estimates is taken as the coarse CFO, and is used to adjust the carrier frequency of PlutoSDR. Repeating in this way several times, we can narrow down the carrier frequency gap between the transmitter and the receiver to satisfy the estimation range requirement.

**Fine-grained Estimation: Inter-packet.** The coarse calibration can reduce the CFO significantly to the range of a few hundred Hertz. Its accuracy is insufficient for the multi-antenna localization services, but it successfully drags down the CFO $|\Delta f|$ to be in the

range $\frac{1}{2T_{pkt}}$. In the second stage, we perform the inter-packet CFO estimation to the preambles of consecutive packets. We also take the average of fine-grained estimates to further shrink the CFO by adjusting the carrier frequency of PlutoSDR, ensuring the CFO locate in the estimation range. Limited by the PlutoSDR's minimum adjustment step of carrier frequency and the instability of CFO, residual CFO still exists, but it will not cause the phase shift more than $\pi$ within a switching period. Then we can get exact CFO estimation to calibrate the phase shift.

**Specialty in LoRa** LoRa is an emerging wireless technology designed for long range transmission. Its frame structure is much different from WIFI and BLE. The preamble of LoRa frame starts with a sequence of repeated up-chirp symbols (up to 65536 symbols), each of which may last from 256$us$ to 32.8$ms$ determined by different transmission parameters. Thus the transmission time of an entire frame may reach several hundred milliseconds or even longer, which is too large for inter-packet CFO estimation. We resolve this issue by executing the Moose algorithm on adjacent symbols in the preamble. Because the symbol interval can reach millisecond-level, this method can achieve the similar accuracy of inter-packet CFO estimation with WIFI and BLE. Due to the symbol interval is fixed, the phase offset caused by CFO is similar for each symbol in a short time. We can directly conduct the fine-grained CFO estimation without adjusting the center frequency of TyrLoc.

## 5.3 Building Virtual Synchronous Array

After performing two-stage CFO estimation, we obtain accurate CFO estimates to calibrate the phase shift based on Eq. (5). However, CFO is not constant over time as the oscillator slightly drifts [44, 47].

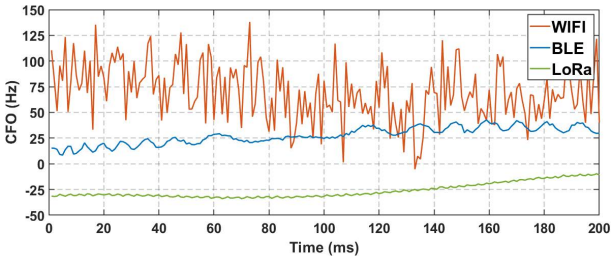



**Figure 7: CFO fluctuation over time.**

To evaluate the fluctuation of CFO, we use PlutoSDR to receive repeated packets without switching, then perform two-stage CFO estimation. In the experiment, the packet sending rate is 1000$pkt/s$ and we use high-frequency coaxial cable to connect the receiver and transmitter to ensure higher SNR. According to Eq. (10), the theoretical CFO estimation variance is small enough to server as a reasonable approximation of the true value. In Fig. 7, the CFO varies over time. Hence, for each switching round, we need to use inter-packet method to obtain fine-grained CFO estimates one or more times at the cost of a longer switching cycle.

**Switching pattern** To balance the accuracy of CFO estimation and the time efficiency, we enumerate three antenna activating sequences. In TyrLoc, the IDs of the antennas are numbered from 0 to 7 where we call the $0^{th}$ antenna the *Pivot Antenna*. The pivot antenna is the starting point in each round of switching, and serves as a "reference" for phase calibration. We exploit the packets received by the pivot antenna to perform inter-packet CFO estimation.

At Pattern-A, the pivot antenna only repeats once in a round to shorten the switching cycle as much as possible. To improve the of performance of CFO estimation, the pivot antenna repeats once for each two antennas at Pattern-B and every antenna at Pattern-C. For TyrLoc (8-antenna array), the numbers of packets needed to calculate a location are 9, 15 and 21 of Pattern-A, B and C.

**Table 3: Three switching patterns applied in TyrLoc.**

| Switching Pattern (One Cycle) | |
|---|---|
| Pattern-A | $x_0, x_0, x_1, x_2, x_3, ..., x_{n-1}$ |
| Pattern-B | $x_0, x_0, x_1, x_2, ..., x_0, x_0, x_{n-2}, x_{n-1}$ |
| Pattern-C | $x_0, x_0, x_1, x_0, x_0, x_2, ..., x_0, x_0, x_{n-1}$ |

**Virtual synchronous array** After calibrating the phase offset, we commence assembling the virtual synchronous antenna array. As shown in Fig. 8, the left part illustrates the phases received at Pattern-C, in which the blue dots and orange dots represent the average phases of the signal received by the pivot antenna $x_0$ and antenna $x_1 \sim x_7$ respectively. It is worth emphasizing that building virtual synchronous array does not require the assumption of fixed packet interval. The preamble detector can locate the beginning of each packet precisely. Hence, we can obtain the accurate time interval for each pair of adjacent packets. Then, we can calculate fine-grained CFO estimation according to Eq. (9).

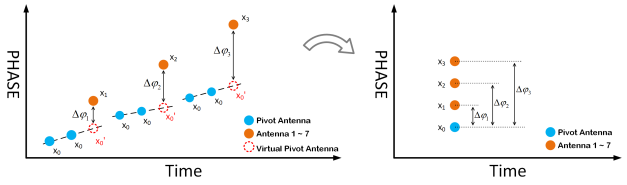



**Figure 8: Building virtual synchronous antenna array.**

Due to the inconstancy of CFO, the slopes between every two blue consecutive points are slightly different. The red cycle denotes phase of virtual pivot antenna $x_0'$, which is predicted based on the CFO estimates. $\Delta\varphi_i$ is the "actual" phase caused by the difference of propagation paths to $x_0$ and $x_i$. Then, aligning all phase offsets $\Delta\varphi_i$ to the pivot antenna, we can construct a virtual synchronous antenna array.

# 6 AOA ESTIMATION OF NON-UNIFORM ANTENNA ARRAY

The MUSIC algorithm performs well when the signal sources are uncorrelated. However, in the presence of multiple coherent signal sources, MUSIC algorithm encounters significant difficulties because of the collapse of the dimensionality of signal subspace [41, 49]. The multipath signals of indoor environment are usually correlated, especially when the signal strength of direct path is relatively weak due to obstruction, the classic MUSIC algorithm may merge the multipath signals from distinct directions as one superposed signal, leading to false peaks in the AoA spectrum [24]. MUSIC with spatial smoothing is an effective way to estimate the

AoAs of multipath signals accurately [19, 24]. However, the spatial smoothing operation requires a uniform linear array.

We call an array *uniform* if the spaces between any two adjacent antennas are identical (usually the half wavelength). We **narrowly** define that an array is *non-uniform* if one or more antennas are missing in the uniform array. To be noted, the spatial smoothing method is not applicable to non-uniform antenna arrays because the Vandermonde structure of steering matrix is not maintained. We hereby illustrate the need of designing a new AoA estimation method for the switching antenna array.

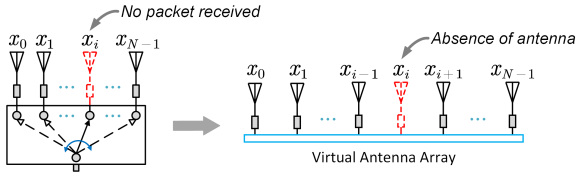



**Figure 9: No packet received when switching to antenna $x_i$, and results in the absence of antenna $x_i$ in the assembled virtual antenna array.**

In TyrLoc, an antenna might not receive an effective packet in its switching interval, possibly due to packet losses, no packet events or the preamble is split by the RF switch. As shown in Fig. 9, if a packet loss occurs while antenna $x_i$ is switched on, the assembled virtual antenna array will be "incomplete" or "non-uniform". Therefore, MUSIC with spatial smoothing does not work in our asynchronous antenna array robustly. We resort to the interpolated array transform [42] to tackle this problem. It designs a mapping matrix to convert the non-uniform array data into the virtual uniform array data that allows us to keep using the spatial smoothing approach.

The detail of the interpolated array transform is the following. Given $K$ narrow-band signal sources, $N$ antennas in the uniform linear array with $N > K$, and $L$ snapshots of signals, the received array data $\boldsymbol{Y} \in \mathbb{C}^{N\times L}$ can be written as

$$\boldsymbol{Y} = \boldsymbol{AS} + \boldsymbol{W} \tag{12}$$

where $\boldsymbol{S} \in \mathbb{C}^{K\times L}$ is the signal matrix, $\boldsymbol{W} \in \mathbb{C}^{N\times L}$ is the zero-mean white Gaussian noise with the variance of $\sigma^2$ and $\boldsymbol{A} \in \mathbb{C}^{N\times K}$ is the steering matrix formed as $\boldsymbol{A} = [\boldsymbol{\alpha}(\theta_1), ..., \boldsymbol{\alpha}(\theta_K)]$. Here, $\boldsymbol{\alpha}(\theta_k) = [1, e^{-j2\pi d \sin\theta_k}, ..., e^{-j2\pi(N-1)d\sin\theta_k}]^T$ corresponds to the channel response vector of the antennas $x_0$ to $x_{N-1}$ on the $k^{th}$ source. When a packet loss occurs on $x_i$, the element $e^{-j2\pi di\sin\theta_k}$ will be removed in $\boldsymbol{\alpha}(\theta_k)$. We substitute it by $\boldsymbol{\alpha'}(\theta_k) = [1, ..., e^{-j2\pi(i-1)d\sin\theta_k}, e^{-j2\pi(i+1)d\sin\theta_k}, e^{-j2\pi(N-1)d\sin\theta_k}]$ with only $N-1$ elements. Similarly, we replace the matrix $\boldsymbol{A}$ by its counterpart $\boldsymbol{A'} \in \mathbb{C}^{(N-1)\times K}$ that has $\boldsymbol{A'} = [\boldsymbol{\alpha'}(\theta_1), ..., \boldsymbol{\alpha'}(\theta_K)]$. Meanwhile, $\boldsymbol{Y}$ is replaced with $\boldsymbol{Y'} \in \mathbb{C}^{(N-1)\times L}$.

Now the antenna array is non-uniform so that the steering matrix $\boldsymbol{A'}$ doesn not satisfy Vandermonde structure. We need to design a mapping matrix to generate a virtual steering matrix complying with Vandermonde structure. There exists

$$\widetilde{\boldsymbol{A}} = \boldsymbol{MA'} \tag{13}$$

where $\widetilde{\boldsymbol{A}}$ is the virtual steering matrix, and $\boldsymbol{M} \in \mathbb{C}^{(N-1)\times(N-1)}$ is the mapping matrix. Then, select $P$ (usually $P > N$) sampling angles $\phi_1 \sim \phi_P$ to construct the matrix $\boldsymbol{A'_0} = [\boldsymbol{\alpha'}(\phi_1), ..., \boldsymbol{\alpha'}(\phi_P)]$. Thus, the least square solution of array mapping matrix $\boldsymbol{M}$ can be solved by

$$\boldsymbol{M} = \widetilde{\boldsymbol{A}}\boldsymbol{A'_0}^H(\boldsymbol{A'_0}\boldsymbol{A'_0}^H)^{-1} \tag{14}$$

Eq. (14) shows that the mapping matrix $\boldsymbol{M}$ can convert the non-uniform linear array data to the virtual uniform one. For the angular ranges in $(\phi_1, \phi_P)$, we acquire the approximated steering vector $\widetilde{\boldsymbol{\alpha}}(\theta_i) \approx \boldsymbol{M}\boldsymbol{\alpha}(\theta_i)$. The mapping accuracy depends on the selection of the sampling angles and the number of array elements.

We rewrite Eq. (12) after the interpolated array transform as

$$\widetilde{\boldsymbol{Y}} = \boldsymbol{MY'} = \boldsymbol{MA'S} + \boldsymbol{MW} \approx \widetilde{\boldsymbol{A}}\boldsymbol{S} + \boldsymbol{MW} \tag{15}$$

where $\widetilde{\boldsymbol{Y}} \in \mathbb{C}^{(N-1)\times L}$ is the array data matrix of virtual uniform array. It is the sum of the manipulated signal matrix $\boldsymbol{MA'S}$ and the weighted noise matrix $\boldsymbol{MW}$.

Then, the signal covariance matrix $\widetilde{\boldsymbol{R}} \in \mathbb{C}^{(N-1)\times(N-1)}$ can be expressed as

$$\widetilde{\boldsymbol{R}} = E[\widetilde{\boldsymbol{Y}}\widetilde{\boldsymbol{Y}}^H] = \widetilde{\boldsymbol{A}}\boldsymbol{S}\boldsymbol{S}^H\widetilde{\boldsymbol{A}}^H + \sigma^2\boldsymbol{M}\boldsymbol{M}^H \tag{16}$$

The weighted noise matrix $\sigma^2\boldsymbol{M}\boldsymbol{M}^H$ is harmful to the accuracy of the MUSIC algorithm. Hence, we should prewhiten the noise through the method described in [42]. Then, we can use the classic MUSIC algorithm with spatial smoothing to estimate the AoA of multipath signals.

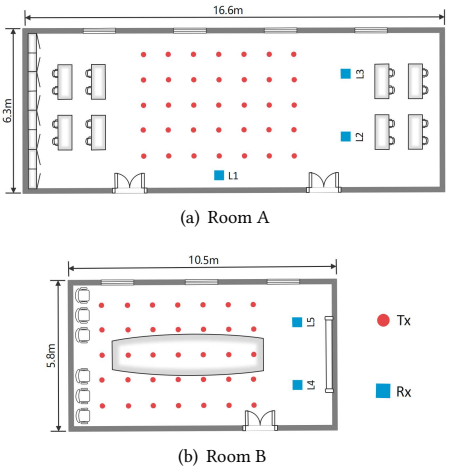
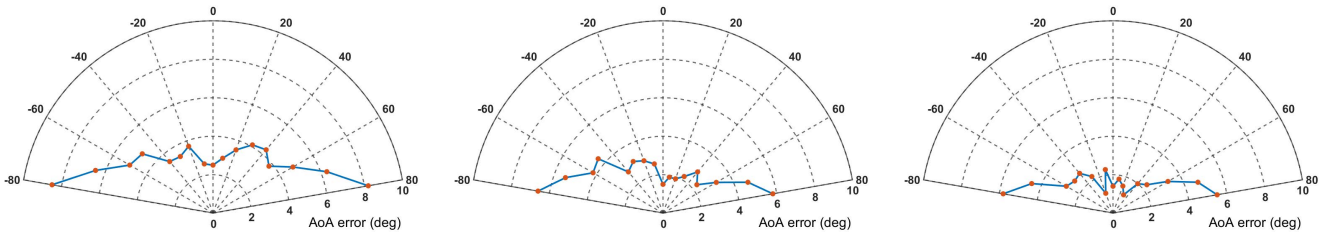



**Figure 10: Testbed environment. The locations of transmitter are marked as red dots and those of TyrLoc devices are marked as blue squares.**

## 7 EVALUATION

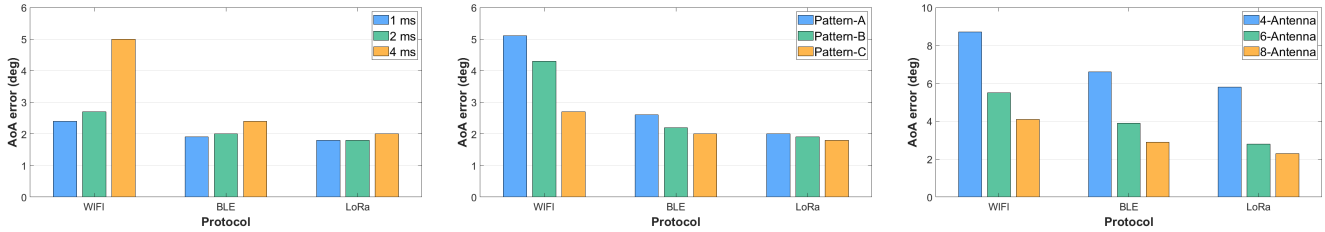
### 7.1 Experimental Setup

We evaluate the performance of TyrLoc in a rectangular office room with area of $105m^2$ and a smaller meeting room of $61m^2$. The layouts of the rooms are shown in Fig. 10, with some furniture, computers and cabinets inside, making each of them a rich multipath environment. Here, we deploy TyrLoc at $L1$ to evaluate the AoA microbenchmarks; $L2$, $L3$, $L4$ and $L5$ are used for evaluating the accuracy of AoA-based indoor localization and tracking in the




(a) WIFI (b) BLE (c) LoRa

**Figure 11: The median AoA estimation error of different signal's arriving angle.**




(a) Switching Interval (b) Switching pattern (c) Array size

**Figure 12: Factors affecting the AoA estimation accuracy. (a) Switching interval (b) Switching pattern (c) Array size**

LoS situation. For the NLoS scenario, we use two wooden cabinets (W:110$cm$ H:180$cm$ D:35$cm$, the total thickness of front board and back board is 7$cm$) to block the direct path signal and place a metal reflective surface in the room, and the other settings are the same as those of the LoS situation.

**WIFI.** We employ a Lenovo X200 laptop equipped with an Intel 5300 NIC [36] as the transmitter. The transmission power is the default setting of the CSI tool, 15dBm. The WIFI carrier frequency is set on channel 100 (5.5GHz) and the transmitter broadcasts 500 packets per second.

**BLE.** We implement the BLE v5.0 PHY layer on a PlutoSDR. We set the BLE transmitter working at advertising mode with the signal transmission fixed on channel 39 (2.48GHz), and it sends 500 advertising packets per second. The transmission power is set to the maximum, 7dBm.

**LoRa.** We use a wireless stick equipped with Semtech SX1276 [7] transceiver to send LoRa packets. The carrier frequency of the transmitter is 915MHz; the spread factor is 9 and the signal bandwidth is 250kHz. The transmission power of the node is 15dBm and we set the preamble length of LoRa packet as 128 symbols, where each symbol lasts 2.05$ms$.

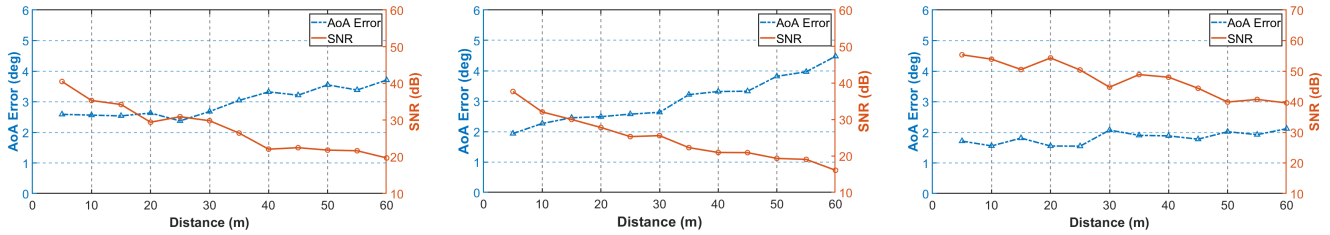
**Receiver.** The core component of TyrLoc is a PlutoSDR with a single $Tx$ and $Rx$. The SP8T RF switch used is HMC321ALP4E, a broadband non-reflective RF switch in low-cost surface mount packages, covering DC to 8GHz. We use an FPGA development board to control the RF switch, the FPGA chip inside is Spartan-6 XC6SLX25-2FTG256C. We build the 8-antenna uniform linear array for WIFI, BLE and LoRa respectively. The distance between two adjacent antennas equals to half of the wavelength (2.7$cm$ for WIFI, 6$cm$ for BLE and 16.4$cm$ for LoRa).

## 7.2 Microbenchmark

We now evaluate how the accuracy of TyrLoc's AoA estimation is affected by the antenna switching behaviors. The receiver is located at $L1$ in Fig. 10, and the transmitter is placed 4$m$ away from the receiver in line-of-sight. The ground-truth AoAs of test points range from $-80°$ to $80°$.

**Angular accuracy** To evaluate the AoA estimation capability of TyrLoc, we use the MUSIC algorithm with spatial smoothing to estimate the arriving angle of the signal. The ground truth is calculated based on the physical locations of the transmitter and TyrLoc. Fig. 11 plots the AoA results of all tested points. The median errors of WIFI, BLE and LoRa are 4.1°, 2.9° and 2.3°, respectively. The 90 percentile errors of them are 7.7°, 5.6° and 5.1°. Since we use a linear antenna array in the experiment, TyrLoc will achieve a better performance if the arriving angle is around the perpendicular direction to the antenna array.

**Impact of switching interval.** We study the impact of switching interval by setting it at 4$ms$, 2$ms$ and 1$ms$ for WIFI and BLE. For LoRa, we adjust the spread factor to control each symbol lasts 4.10$ms$, 2.05$ms$ and 1.02$ms$. In the experiment, TyrLoc operates with pattern-C and we test the AoA estimation performance at $-10°$, $0°$, $10°$ three angles. The result is shown in Fig. 12(a), for WIFI, the decrease in switching interval from 4$ms$ to 1$ms$ brings obvious enhancement. The AoA median error reduces from 5.0° to 2.4°. While for BLE and LoRa, decreasing from 4$ms$ to 1$ms$ brings slight improvement. The AoA median error reduces from 2.4° to 1.9° for BLE and 2.0° to 1.8° for LoRa. Longer switching interval may cause larger phase calibration errors, resulting in the degradation of AoA estimation accuracy. It's worth emphasizing that the transmission time of WIFI or BLE packets with long payload may exceed 1$ms$. To be compatible with variable packet length, we set the switching interval to 2$ms$ in the remaining experiments.




(a) WIFI (b) BLE (c) LoRa

**Figure 13: The median AoA estimation error of different distance between the transmitter and TyrLoc.**

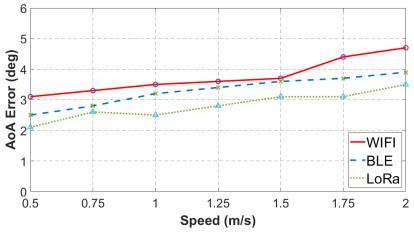



**Figure 14: Impact of moving speed on AoA estimation accuracy.**

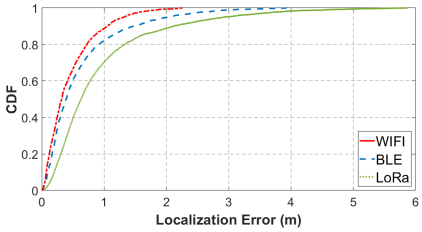



**Figure 15: CDF of localization error in LoS situation.**

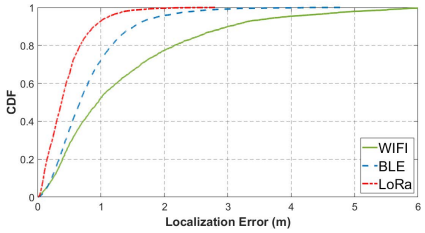



**Figure 16: CDF of localization error in NLoS situation.**

**Impact of switching pattern.** Switching pattern is a key factor in AoA estimation. We conduct experiments to test TyrLoc's AoA performance with pattern-A, B and C (illustrated in Table 3) to evaluate the influence of switching pattern. The ground truth of AoAs is $-10°$, $0°$ and $10°$. The AoA estimation errors of different protocols are plotted in Fig. 12(b). For WIFI, The median error is $5.1°$ with pattern-A, $4.3°$ with pattern-B and $2.7°$ with pattern C. For BLE, the median error is $2.6°$, $2.2°$, $2.0°$ with pattern-A, B and C. Meanwhile that of Lora is $2.0°$, $1.9°$, $1.8°$. Compared to Pattern-A and B, Pattern-C provides better AoA estimation accuracy. More frequent CFO estimation brings obvious accuracy improvement. So the remaining experiments are all conducted at pattern-C.

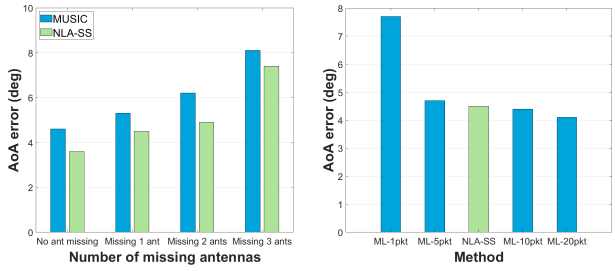
**Impact of array size.** To understand the impact of the array size on the AoA estimation accuracy, we repeat the AoA estimation experiments with four, six and eight antennas. In Fig. 12(c), the median AoA estimation errors are $8.7°$, $5.5°$, $4.1°$ with four, six and eight antennas for WIFI, meanwhile, $6.6°$, $3.9°$ and $2.9°$ for BLE. The median estimation errors of LoRa are $5.8°$, $2.8°$ and $2.3°$. One can clearly observe that more antennas bring the better accuracy of AoA estimation. Benefits from the switching based structure, Tyrloc can realize array extension at very low cost to achieve significant AoA performance improvement.

**Impact of distance.** We conduct experiments in a corridor to further study the impact of the distance on TyrLoc. We gradually increase the distance between the transmitter and the receiver from five meter to sixty meter. Fig. 13 shows that the SNR of the signal decreases with the increase of distance between the transmitter and antenna array. Meanwhile, the median AoA estimation errors of WIFI, BLE and LoRa increase from $2.6°$ to $3.7°$, $1.9°$ to $4.5°$ and $1.7°$ to $2.1°$ respectively. The accuracy of MUSIC algorithm greatly depends on signal's SNR [50]. With the increase of distance, WIFI and BLE's AoA performance declines obviously and the accuracy degradation of BLE is more serious. Compared with BLE and WIFI, LoRa remains higher SNR at the same distance and shows its stronger resistant to long distance.

**Impact of moving speed.** To evaluate the impact of moving speed on TyrLoc, we set the transmitter and receiver in a corridor, then move the transmitter away from the antenna array with a constant speed. According to Fig. 14, the performance of AoA estimation degrades slowly as the speed increases. For WIFI, the median error of AoA estimation increases from $3.1°$ with speed $0.5m/s$ to $4.7°$ with speed $2m/s$. Similarly, it increases from $2.5°$ to $3.9°$ for BLE and $2.1°$ to $3.5°$ for LoRa.

**Impact of antenna missing.** To evaluate the performance of interpolated array transform, we place a WIFI transmitter $4m$ away at the $0°$ angle of the receiver. A wooden board ($\sim 6cm$ thickness) is placed in the middle to create a gentle NLoS environment. To simulate antenna missing, we randomly discard certain antenna's data. Three sets of experiment are conducted to test its performance when missing one, two or three antennas. In Fig. 17(a), we compare the accuracy of AoA estimation using MUSIC directly with that of spatial smoothing MUSIC for the non-uniform antenna array (NLA-SS). The median errors of MUSIC are $4.6°$, $5.3°$, $6.2°$ and $8.1°$ in the situations where the number of lost antennas increases from 0 to 3. Applying the interpolated array transform and the spatial smoothing MUSIC, we obtain the median AoA errors $3.6°$, $4.5°$, $4.9°$ and $7.4°$ under the same setting. Thus, one can conclude that our approach outperforms the standard MUSIC algorithm in the presence of antenna missing.

**Comparison with maximum likelihood estimator.** We conduct experiments in gentle NLoS environment to compare the AoA estimation accuracy of NLA-SS with that of the maximum likelihood (ML) estimator employed in Widar 2.0 [23], which does not require a uniform antenna array. We randomly discard one antenna's data to generate non-uniform array. The results are shown in Fig. 17(b). The median error of the ML estimator using one set of




(a) NLA-SS vs MUSIC (b) NLA-SS vs ML

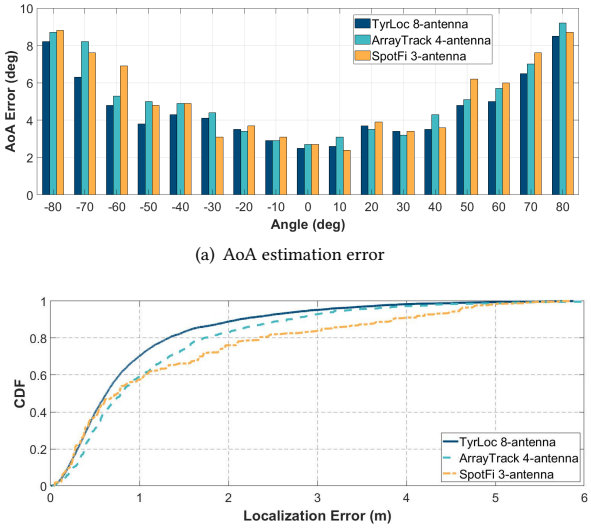
**Figure 17: Comparison: NLA-SS, MUSIC and ML.**

CSI (8-antenna array) is 7.7°, that of the ML estimator using the CSI of 5, 10 and 20 sets of CSI is 4.7°, 4.4° and 4.1°. The median error of NLA-SS algorithm is 4.5°. It only uses 1 set of data to achieve similar accuracy of the ML estimator using 10 sets of data. While in TyrLoc at least 21 packets are needed to harvest a set of CSI at pattern-C, which corresponds to 21 switching intervals. Given the packet sending rate $500pkt/s$, using 20 sets of data means the localization update rate is merely 1.19/s, which is insufficient to track moving targets.

## 7.3 Indoor Localization

**Performance in LoS and NLoS situations.** We use two PlutoSDR receivers, deployed at L2 and L3 (each with an 8-antenna ULA) in Room A, and at L4, L5 in Room B, to estimate the location of transmitters based on direct path AoAs. We choose 35 points of each room to examine the localization accuracy of TyrLoc. Fig. 15 plots the CDF of localization error in LoS situations. The median errors achieved are $63cm$ with WIFI, $39cm$ with BLE and $32cm$ with LoRa. We next measure the localization error in NLoS situation. We use two thick wooden cabinets as the shields to block the LoS signals from the transmitter, and place a metal reflective surface in the room to detect the performance of TyrLoc in the environment with strong reflective paths. Then the localization becomes more challenging because the direct path signal is relatively weak due to obstruction. Fig. 16 depicts the results of NLoS scenario where the median localization errors are $96cm$ for WIFI, $67cm$ for BLE and $40cm$ for LoRa. Compared with the LoS scenario, LoRa's performance slightly drops 25%, while the accuracies of WIFI and BLE degrade by 52% and 72% respectively. Due to the strong penetration ability of LoRa, it exhibits the great potential for localization in complex indoor environments.

**Comparison with synchronous array.** To compare the performance of TyrLoc with the high-end SDR based localization system with a synchronous antenna array. We use two WARP v3, each equipped with a 4-antenna array, to build a prototype of ArrayTrack [24]. We also compare TyrLoc with commodity WIFI-based system. We employ two laptops equipped with Intel 5300 NIC as the receivers and faithfully reproduce the algorithm of SpotFi [19]. We repeat the AoA and localization experiments based on WIFI in LoS situation. The carrier frequency is 5.5GHz and bandwidth is 20MHz, using the same setting of TyrLoc's "WIFI mode". Fig. 18(a) shows the comparison of AoA estimation error. The median error of TyrLoc is 4.1°, that of ArrayTrack and SpotFi is 4.9° and 4.8°.




(a) AoA estimation error

(b) CDF of localization error

**Figure 18: Comparison: TyrLoc, ArrayTrack and SpotFi.**

The localization result is depicted in Fig. 18(b), the median error achieved is $63cm$ with TyrLoc, $79cm$ with ArrayTrack and $75cm$ with SpotFi. Compared with the ArrayTrack system built with two WARP v3 ($cost \sim \$10000$), TyrLoc enables a larger antenna array with much lower cost ($cost \sim \$400$) and achieves higher localization accuracy. Compared with SpotFi, TyrLoc is multi-functional and flexible. It supports not only WIFI, but also BLE and LoRa-based localization services, both of which are more accurate than WIFI.

## 7.4 Device Trajectory

We further using TyrLoc to track the movement of a transmitter that is held in a person's hand. The transmitter is placed at around $3m$ away from two receivers. We ask a user to move the transmitter along the trajectory drawn on the ground to write letters in Room A. Fig. 19 depicts some examples of the recovered letters, in which the blue trajectories are estimated by TyrLoc, and the grey letters are the ground truths. Here, the trajectory "M","O" is obtained using WIFI, "B","I" is tracked by BLE and "S","Y","S" is conducted by LoRa.

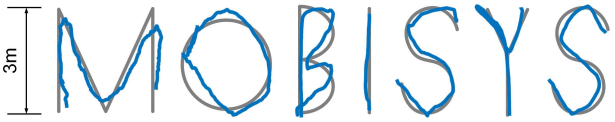



**Figure 19: Tracking devices with TyrLoc.**

# 8 RELATED WORK

**Localization based on various protocols.** There are many indoor localization system based on various wireless protocols. Due to the page limit, we just list part of the systems based on WIFI, BLE and LoRa. Since the release of CSI tool kit [36, 37], many indoor localization systems based on specific commodity WIFI devices have been presented [19–22, 25, 51, 53]. In these work, advanced phased-array signal processing techniques are applied to achieve high position accuracy. But the commodity devices for BLE, LoRa

cannot provide rich channel information, which results in relatively lower localization accuracy than those based on WIFI [26–29, 31–33]. To improve their accuracy, some attempts have been made to build the prototype based on SDR devices [30, 35, 52]. Those work process the raw signal data and achieve similar or higher precision than WIFI-based systems. TyrLoc exploits the flexibility of SDR to construct a general purpose platform that can easily switch to WIFI, BLE or LoRa mode as needed.

**Antenna array extension.** Many efforts have been made to expand the antenna array to improve the accuracy of localization. Previous wireless localization systems [24, 54] connect multiple clock-synchronized SDRs to obtain a larger antenna array. While the SDR that supports synchronization is usually expensive. Using multiple high-end SDRs results in severalfold hardware cost, which restricts its practical deployment. To reduce the overall cost of the system, some attempts have been made to combine multiple commodity WIFI device to extend the antenna array. Phaser [22] and 3D-WIFI [55] utilize a signal splitter to realize the synchronization of two WIFI NICs. Six RF chains are adapted for a five-antenna phased array, one radio chain is reserved for synchronization. To improve the utilization of the RF chain, antenna extension based on RF switch is a promising approach. SWAN [18] connects three RF switches (SP4T) to the three RF chains of a WIFI NIC correspondingly. It realizes a twelve-antenna array based on commodity WIFI devices. iArK [38] implements an large-scale antenna array based RF switches. These work have in common that one RF chain is used for synchronization or calibration purpose, thus at least two RF chains are required. We also notice the term "bandwidth stitching" [56] that merges CSI on multiple separate channels into a unified one, which is different from the term "antenna stitching". TyrLoc proposes a novel calibration method that enables single RF chain to build a virtual phased array with very low hardware cost.

## 9 CONCLUSION

TyrLoc empowers the inexpensive PlutoSDR with a large-scale antenna array only using a single receiving RF chain. The firmware of PlutoSDR is modified to enable an RF switch to control the antenna switching, and a novel two-stage CFO calibration algorithm is designed to make the received signal phases useful. The accurate localization results of TyrLoc on WIFI, BLE and Lora manifest its multi-technology functionality. TyrLoc's techniques are crucial to other low-cost programmable SDRs with a single RF chain, and are more widely applicable to other applications such as gesture recognition and motion tracking.

## 10 ACKNOWLEDGEMENTS

This work is supported in part by National Key R&D Program of China under Grant 2020YFA0711400; in part by Natural Science Foundation of China under Grant 61772139, 62072117; in part by Shanghai-Hong Kong Collaborative Project under Grant 18510760900; in part by Key-Area Research and Development Program of Guangdong Province under Grant 2020B010166003. Yuedong Xu is the corresponding author. The authors would like to thank the shepherd and anonymous reviewers for their great helps to improve the quality of this work.

## REFERENCES

[1] ADALM-PLUTO. https://wiki.analog.com/university/tools/pluto/
[2] HackRF One. https://greatscottgadgets.com/hackrf/one/
[3] bladeRF-x40. https://www.nuand.com/product/bladerf-x40/
[4] bladeRF-2.0 xA9. https://www.nuand.com/product/bladeRF-xA9/
[5] USRP B210. https://www.ettus.com/all-products/ub210-kit/
[6] WARP v3 Kit. https://mangocomm.com/products/kits/warp-v3-kit/
[7] Semtech SX1276. https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276.
[8] HMC321ALP4E Datasheet. https://www.analog.com/media/en/technical-documentation/data-sheets/hmc321a.pdf.
[9] F. Viani, G. Oliveri, M. Donelli, L. Lizzi, P. Rocca, and A. Massa, "WSN-based solutions for security and surveillance". In *Proc. of IEEE European Wireless Technology Conference*, 2010.
[10] C. Wang, J. Liu, Y. Chen, H. Liu, and Y. Wang, "Towards in-baggage suspicious object detection using commodity WiFi". In *Proc. of IEEE CNS*, 2018.
[11] U. Rehman and S. Cao, "Augmented-Reality-Based Indoor Navigation: A Comparative Analysis of Handheld Devices Versus Google Glass". *IEEE Trans. on Human-Machine Systems*, 2017.
[12] Y. Park, S. Yun, and K.-H. Kim, "When IoT met augmented reality: Visualizing the source of the wireless signal in AR view". In *Proc. of ACM MobiSys*, 2019.
[13] F. Adib, H. Mao, Z. Kabelac, D. Katabi, and R.C. Miller, "Smart Homes that Monitor Breathing and Heart Rate". In *Proc. of ACM CHI*, 2015.
[14] Y. Zeng, D. Wu, J. Xiong, J. Liu, Z. Liu, and D. Zhang, "MultiSense: Enabling multi-person respiration sensing with commodity wifi". In *Proc. of ACM IMWUT*, 2020.
[15] S. Yue, Y. Yang, H. Wang, H. Rahul, and D. Katabi, "Bodycompass: Monitoring sleep posture with wireless signals". In *Proc. of ACM IMWUT*, 2020.
[16] X. Li, D. Zhang, Q. Lv, J. Xiong, S. Li, Y. Zhang, and H. Mei, "IndoTrack: Device-Free Indoor Human Tracking with Commodity Wi-Fi". In *Proc. of ACM IMWUT*, 2017.
[17] S. Sen, B. Radunovic, R. Choudhury, and T. Minka., "You are facing the Mona Lisa: Spot localization using PHY layer information.". In *Proc. of ACM Mobisys*, 2012.
[18] Y. Xie, Y. Zhang, J. Liando, and M. Li, "SWAN: Stitched Wi-Fi ANtennas". In *Proc. of ACM MobiCom*, 2019.
[19] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter Level Localization Using WiFi". In *Proc. of ACM SIGCOMM*, 2015.
[20] M. Kotaru and S. Katti, "Position tracking for virtual reality using commodity WiFi". In *Proc. of IEEE CVPR*, 2017.
[21] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single WiFi access point". In *Proc. of USENIX NSDI*, 2016.
[22] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: Enabling phased array signal processing on commodity WiFi access points". In *Proc. of ACM MobiCom*, 2019.
[23] K. Qian, C. Wu, Y. Zhang, G. Zhang, Z. Yang and Y. Liu, "Widar2.0: Passive Human Tracking with a Single Wi-Fi Link". In *Proc. of ACM MobiSys* 2018.
[24] J. Xiong and K. Jamieson, "ArrayTrack: a fine-grained indoor location system". In *Proc. of USENIX NSDI*, 2013.
[25] Y. Xie, J. Xiong, M. Li, and K. Jamieson, "mD-Track: Leveraging multi-dimensionality for passive indoor Wi-Fi tracking". In *Proc. of ACM MobiCom*, 2019.
[26] Y. Zhuang, J. Yang, Y. Li, L. Qi, and N. El-Sheimy, "Smartphone-based indoor localization with bluetooth low energy beacons". *Sensors*, 2016.
[27] Y. Wang, Q. Ye, J. Cheng, and L. Wang, "RSSI-based bluetooth indoor localization". In *Proc. of IEEE MSN*, 2015.
[28] F.S. Dani and A.T. Cemgil, "Model-based localization and tracking using bluetooth low-energy beacons". *Sensors*, 2017.
[29] D. Chen, K. Shin, Y. Jiang, and K.-H. Kim, "Locating and tracking ble beacons with smartphones". In *Proc. of ACM CoNEXT*, 2017.
[30] R. Ayyalasomayajula, D. Vasisht, and D. Bharadia, "BLoc: CSI-based Accurate Localization for BLE Tags". In *Proc. of ACM CoNEXT*, 2018.
[31] K. Lam, C. Cheung, and W. Lee, "RSSI-Based LoRa Localization Systems for Large-Scale Indoor and Outdoor Environments". *IEEE Trans. on Vehicular Technology*, 2019.
[32] A. Mackey and P. Spachos, "LoRa-based localization system for emergency services in GPS-less environments". In *IEEE INFOCOM WKSHPS*, 2019.
[33] B. Islam, M.T. Islam, J. Kaur, and S. Nirjon, "LoRaIn: Making a Case for LoRa in Indoor Localization". In *Proc. of IEEE PeCom WKSHPS*, 2019.
[34] H. Zhu, K. Tsang, Y. Liu, Y. Wei, H. Wang, C. Wu and H. Chi, "Extreme RSS based Indoor Localization for LoRaWAN with Boundary Autocorrelation". In *IEEE Trans. on Industrial Informatics*, 2020.
[35] R. Nandakumar, V. Iyer, and S. Gollakota, "3D Localization for Sub-Centimeter Sized Devices". In *Proc. of ACM SenSys*, 2018.
[36] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: gathering 802.11n traces with channel state information". *ACM SIGCOMM CCR*, 2011.

[37] Y. Xie, Z. Li, and M. Li, "Precise Power Delay Profiling with Commodity WiFi". In *Proc. of ACM MobiCom*, 2015.
[38] Z. An, Q. Lin, P. Li, and L. Yang, "General-purpose deep tracking platform across protocols for the internet of things". In *Proc. of ACM MobiSys*, 2020.
[39] R. Schmidt, "Multiple emitter location and signal parameter estimation". *IEEE Trans. on Antennas and Propagation*, 1986.
[40] P. Stoica and A. Nehorai, "MUSIC, maximum likelihood, and Cramer-Rao bound", *IEEE Transactions on Acoustics, speech, and signal processing*, 1989.
[41] T.-J. Shan, M. Wax, and T. Kailath, "On spatial smoothing for direction-of-arrival estimation of coherent signals". *IEEE Trans. on Acoustics, Speech, and Signal Processing*, 1985.
[42] B. Friedlander and A. Weiss, "Direction finding using spatial smoothing with interpolated arrays". *IEEE Trans. on Aerospace and Electronic Systems*, 1992.
[43] T. Schmidl and D. Cox, "Robust frequency and timing synchronization for OFDM", *IEEE Trans. on communications*, 1997.
[44] C. Zucca and P. Tavella, "The clock model and its relationship with the Allan and related variances". *IEEE Trans. on ultrasonics, ferroelectrics, and frequency control*, 2005.
[45] IEEE Standard for Information technology, Part 11, Amendment 5, page 316, IEEE Std 802.11n-2009
[46] P. Moose, "A Technique for Orthogonal Frequency Division Multiplexing Frequency Offset Correction". *IEEE Trans. on Communications*, 1994.
[47] D.R. Brown, R. Mudumbai, and S. Dasgupta, Soura, "Fundamental limits on phase and frequency tracking and estimation in drifting oscillators". *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2012.
[48] S. Sen, J. Lee, K.-H. Kim, and P. Congdon, "Avoiding multipath to revive inbuilding WiFi localization". In *Proc. of ACM MobiSys*, 2013.
[49] A. Paulraj, V. Reddy, T. Shan, and T. Kailath, "Performance analysis of the MUSIC algorithm with spatial smoothing in the presence of coherent sources". *IEEE MILCOM*, 1986.
[50] Q. Zhang, "Probability of resolution of the MUSIC algorithm". *IEEE Trans. on Signal Processing*, 1995.
[51] E. Soltanaghaei, A. Kalyanaraman, and K. Whitehouse, "Multipath triangulation: Decimeter-level wifi localization and orientation with a single unaided receiver". In *Proc. of ACM MobiSys*, 2018.
[52] F. Zhang, Z. Chang, K. Niu, J. Xiong, B. Jin, Q. Lv, and D. Zhang, "Exploring lora for long-range through-wall sensing". In *Proc. of ACM IMWUT*, 2020.
[53] X. Li, S. Li, D. Zhang, J. Xiong, Y. Wang, and H. Mei, "Dynamic-music: accurate device-free indoor localization". In *Proc. of ACM UbiComp*, 2016.
[54] Z. Chen, Z. Li, X. Zhang, G. Zhu, Y. Xu, J. Xiong, and X. Wang, "AWL: Turning spatial aliasing from foe to friend for accurate WiFi localization". In *Proc. of ACM CoNEXT*, 2017.
[55] L. Zhang and H. Wang, "3D-WiFi: 3D localization with commodity WiFi". *IEEE Sensors Journal*, 2019.
[56] J. Xiong, K. Sundaresan, and K. Jamieson, "Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization". In *Proc. of ACM MobiCom*, 2015.