# *LiTEfoot*: Ultra-low-power Localization using Ambient Cellular Signals

Nakul Garg*, Aritrik Ghosh*, Nirupam Roy
{nakul22, aghosh98, niruroy}@umd.edu
University of Maryland, College Park

## ABSTRACT

In this paper, we introduce a low-power wide-area cellular localization system, called *LiTEfoot*. The core architecture of the radio carefully applies non-linear transform of the entire cellular spectrum to obtain a systematic superimposition of the synchronization signals at the baseband. The system develops methods to simultaneously identify all the base stations that are active at any cellular band from the transformed signal. The radio front end uses a simple envelop detector to realize the non-linear transformation. We build on this low-power radio to implement a self-localization system leveraging ambient 4G-LTE signals. We show that the core system can also be extended to other cellular technologies like 5G-NR and NB-IoT. The prototype achieves a median localization error of 22 meters in urban areas and 50 meters in rural areas. It can sense a 3GHz wideband LTE spectrum in 10ms using non-linear intermodulation while consuming 0.9 mJ of energy for a PCB-based implementation and 40 $\mu$J for CMOS simulation. In other words, *LiTEfoot* tags can last for 11 years on a coin cell while continuously estimating location every 5 seconds. We believe that *LiTEfoot* will have widespread implications in city-scale asset tracking and other location-based services. The radio architecture can be useful beyond low-power self-localization and can find application in synchronization and communication on battery-less platforms.

## CCS CONCEPTS

• **Hardware → Wireless devices**; • **Networks → Cyber-physical networks**; • **Social and professional topics → Sustainability**.

## KEYWORDS

Asset tracking, Low-power sensing, NextG, Wideband, Ambient Computing, Sustainable, Scalable

**ACM Reference Format:**
Nakul Garg*, Aritrik Ghosh*, Nirupam Roy. 2024. *LiTEfoot*: Ultra-low-power Localization using Ambient Cellular Signals. In *The 22nd ACM Conference on Embedded Networked Sensor Systems (SENSYS '24), November 4–7, 2024, Hangzhou, China.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3666025.3699356

* Both authors contributed equally to this research.


*SENSYS '24, November 4–7, 2024, Hangzhou, China*

ACM ISBN 979-8-4007-0697-4/24/11.
https://doi.org/10.1145/3666025.3699356

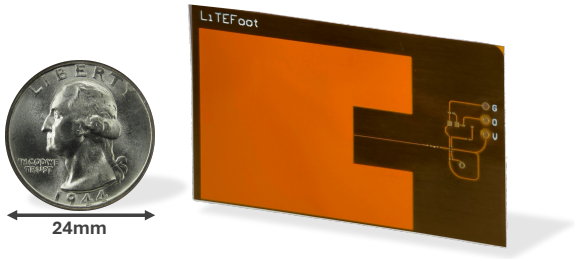



**Figure 1: *LiTEfoot*- an ultra-low-power wireless tracker next to a US quarter for scale.**

## 1 INTRODUCTION

Cargo theft is one of the major perils to supply chains accounting up to $30 billion in cost per year to transport and retail businesses [41, 105] adding to inflation and economic crisis. Existing asset tracking solutions, that focus on large containers or transport vehicles for cost-effectiveness [4, 63], remains mostly ineffective as the most common method is 'pilfering' or stealing a part of the cargo than the entire shipment. Organized crime proliferates in this space leveraging the gap in technology for long-distance asset tracking at smaller granularity and a lower cost. On the other hand, a diverse set of other applications await a maintenance-free solution for wide-area location tracking, including livestock monitoring, warehouse logistics, and locating children, pets, and people with mental illness [26, 77]. A location tracking tag of size of a coin cell that remains operational for years and capable of monitoring self-location across all roads in the country with little infrastructure cost seems to be a fitting technological answer. *But is it even possible to meet all these requirements in a practical asset tracking solution?*

Asset tracking, geofencing, and location-based services are a major part of the growing industry that targets smart commercial and personal application spaces [27]. The solutions generally consist of a tag that contains a localization module to estimate its current location and a communication module to periodically update the location status to the monitoring server [109]. A significant majority of the solutions relies on Global Positioning System (GPS) for location estimation for its infrastructure-free self-localization [17, 36]. However, GPS tracking over a long period of time is challenging due to its high power consumption. [9] A GPS-enabled tag, therefore, often comes with sizable battery pack making its overall form factor to be similar to a smartphone and weights over 200 gram [11], which makes it challenging to incorporate in a low-power device. Moreover, traditional GPS-based localization methods, while effective in open-sky environments, falter in urban canyons and dense cities with skyscrapers [14].

The need for small, low-cost, and low-power alternatives for asset tracking has led to the next dominant techniques for commercial tags which implements proximity-based localization [6, 94]. In this design the tag can not self-localize, rather it uses a short range communication with nearby infrastructure which in turn estimates the location of the tag [44]. For instance, location of an RFID-enabled tag can be predicted when it comes in range of RFID readers deployed at specific locations in a building [18]. Naturally, the infrastructure costs of such solutions are suitable for small controlled environments. Apple AirTag expands the scope of proximity-based location using the 'Find My' network of Apple as the infrastructure [42]. Here the tag basically functions as a Bluetooth Low Energy (BLE) beacon to interact with mobile device in range and the phone updates the tag's approximate location on the server using its own GPS. Unfortunately, its location fixes are unpredictable across long distances as it is conditioned on the presence of a GPS-enabled Apple device with in a few meters of range [44]. While the proximity-based location techniques can lead to a very low-power and small tags for the simplicity of functionality, it offloads the responsibility to infrastructure. The lack of standalone location estimate makes it infeasible for asset tracking over large geographic regions.

Global coverage of cellular infrastructure has opened an interesting possibility of wide-area localization without investing on dedicated infrastructure. Popularity of 4G-LTE and enthusiasm around 5G networks have led to a widespread cellular coverage around the world. In the United States, mobile networks cover more than 98% of the population and over 90% of road networks, as reported by the FCC [23]. Several research works [16, 24, 33] have explored this opportunity for nation-wide localization techniques [9] and multiple commercial products are available cellular localization on smartphones and with tags [22]. However, these systems encounter following two critical challenges in adapting cellular localization on a low-power platform.

(a) First challenge is the latency and computational overhead of scanning wide bandwidth. Active cellular bands are spread across several GHz of bandwidth and naturally, nearby cells use different bands. A self-localizing tag aiming to identify signals from all available cells will require to scan the entire bandwidth. Low-cost narrow-band radios operating in tune-and-capture mode can take tens of minutes to complete one round of scanning and not applicable to dynamic scenarios where the tag can move to different cells within that time [88]. A real-time localization of a tag moving on a vehicle in an urban area will require the tag to scan the spectrum within a few milliseconds. (b) The second challenge is the downconversion of the passband signal for synchronization and cell identification. Traditional radios require power-hungry local oscillators at high-frequencies and sophisticated mixing hardware to convert the signal to baseband before applying correlation on synchronization signals [39, 79]. This operation can itself takes tens of milliWatts of power, which makes the tag last for only a few hours on a battery source like a coin cell.

In this paper, we proposed an architecture for passive cellular localization within the power limit of 1 millijoule and with location update the latency of around 10 milliseconds. This radio architecture exploits the core opportunity from the non-linear transform of the cellular downlink broadcast signals. We explore the behavior of the subcarriers in the cellular synchronization signals under this transformation and show methods to recover cell identity from the systematic superposition of intermodulated frequencies, which we call spectrum folding. Our low-power radio frontend uses a simple envelope detector to realize spectrum folding and onboard algorithms can identify any number of cells operating at any part of the 3GHz spectrum. We build on radio to realize a localization system leveraging the ambient 4G-LTE signals. We call this system *LiTEfoot*. The prototype achieves a median localization error of 22 meters in urban areas and 50 meters in rural areas. It senses a 3GHz wideband LTE spectrum in 10ms using non-linear intermodulation, consuming 40 J of energy per location inference in CMOS simulation, and 0.8 mJ in our PCB prototype. This results in a 625× reduction in energy consumption for the CMOS design and a 27× reduction for the PCB prototype, compared to GPS, which consumes 25 mJ per location inference [95].

*LiTEfoot* presents a new class of low-power receivers tailored to cellular synchronization signals (see Fig 1). We aim to offer a solution that ensures broad coverage and operates on minimal energy, opening up possibilities for applications requiring extensive geographic reach and energy efficiency. The core ideas of spectrum folding and the low-power radio can be adapted for applications in various low-power location-based services and also for channel synchronization battery-less communication platforms.

The use of non-linearity for implicit signal mixing or passive downconversion is a proven technique. It has been explored extensively in various low-power applications to replace power-hungry oscillators in radio receivers [60, 61, 73, 98, 102]. Notably, *MIXIQ* [79] proposed a low-power 802.11ax receiver that modifies OFDM packets to send a helper signal, preserving IQ data for such implicit baseband downconversion. *Saiyan* [39] demonstrated a low-power, long-range receiver for frequency-modulated signals. These lines of work have shown remarkable power efficiency when custom base stations are available to broadcasting specially designed signals. Our work *LiTEfoot* is unique in leveraging non-linear transform with unmodified cellular signals. The core insight lies in a theoretical analysis of certain auto-/cross-correlation properties that survive non-linear intermodulation and baseband superimposition of a signal. *LiTEfoot*'s system design leverages this insight for identifying standard cellular synchronization signals (PSS and SSS) despite their noisy baseband mixture after the non-linear transformation. This novel architecture enables a single-antenna ultra-low-power radio, made from simple off-the-shelf components, to simultaneously detect multiple cell towers' identity without requiring to decode the cellular packets. By allowing non-linearity to intermodulate and fold the spectrum to baseband, *LiTEfoot* sacrifices IQ data but gains the ability to sense the entire 3 GHz LTE spectrum in just 10 ms, a capability crucial for low-power wide-area localization and wide-band spectrum monitoring as well.

While several opportunities exist in research and application, this paper focuses on developing the core capabilities and assessing the

limits of the systems. To this end, we have made the following three specific contributions at the current stage of this project:

- A novel method for signal searching over a wide frequency spectrum. We presented the theoretical foundation and the practical implementation for the non-linear transformation of spectrum and synchronization signal detection on the transformed narrow-band signal.
- Development of a signal strength multilateration-based localization with the low-power radio.
- Prototype development and evaluation of the system with real-world existing 4G-LTE infrastructure.

# 2 CELLULAR NETWORKS PRIMER

## A. Structure of a Cell

In cellular networks, "cells" are the fundamental geographic segments served by a stationary transceiver, called a base station or an eNodeB. In an LTE cellular network, base stations typically use 3-sector cells served by three antennas each covering 120° angular sectors of the cell for improved communication and capacity gain (see Fig. 2). While omnicells with single antennas covering 360° field are also common. LTE defines four types of base stations with different power and coverage areas – macro, micro, pico, and femtocells with up to 20 km, 2 km, 200 m, and 30 m of coverage respectively.

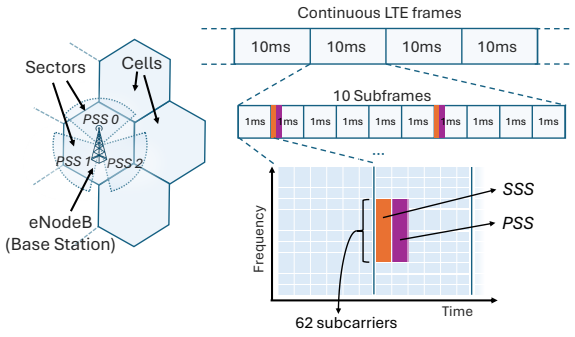



**Figure 2: LTE cells and frame structure.**

Cells are organization-level concepts and therefore different service providers can have overlapping regions of their cells. In fact, a physical cell site or cellular tower can be used by multiple service providers operating independent base stations each having one or more antennas serving different sectors of the corresponding cells. These base stations obviously operate on independent frequency bands and are non-interfering to each other while communicating with mobile clients called User Equipments (UE). However, signals from multiple base stations of the same or different service providers are often available at a physical location and can be observed by scanning across frequency bands.

**Operational frequencies:** LTE operational frequencies are organized in over 70 bands allocated with different bandwidths over a large spectrum ranging from 450 MHz to 3.8 GHz. Some service providers also use parts of their underutilized 3G bands for 4G LTE transmissions. Although, typical frequency bands used in the USA lie between the range of 700 MHz to 3.5 GHz. Within a frequency band, the bi-directional communication between the base station and the mobile device is defined by two different duplex modes – frequency and time division duplex (FDD and TDD). However, almost all service providers in the USA use frequency division duplex (FDD) modes where the uplink (i.e., transmission from the mobile device to the base station) and downlink (i.e., transmission from the base station to the mobile device) use separate frequencies predefined per band.

## B. Cell Identity

Each individual cell in LTE networks can identified using the Cell Global Identity (CGI) which is a globally unique identifier [106]. While the CGI is useful at the network-level operations and management, at the physical layer mobile devices rely on the Physical Cell Identity (PCI) for cell identification. The PCI is a 9-bit number ranging from 0 to 504 that locally identifies each sector antenna. Naturally, this limited number of PCI values are reused over different cells, but the numbers are carefully assigned to distant cells during LTE site planning to avoid confusion between nearby cells [52]. For practical purposes, the PCI numbers can be successfully used for cell selection and handoffs.

**Synchronization Signals:** The PCI numbers are created by combining two numbers between 0-2 and 0-167 which are in turn used as seeds to two pseudorandom sequences, called Primary and Secondary Synchronization Signals (PSS and SSS), used for synchronization and PCI number identification. The Primary Synchronization Signal (PSS) utilizes the frequency-domain Zadoff-Chu sequence and is numbered from 0 to 2, while the Secondary Synchronization Signal (SSS) is formed using maximum length sequences (m-sequences) and numbered from 0 to 167. Mobile devices utilize these synchronization signals, which are emitted by base station antennas, to determine their PCI values. The PCI is calculated using the formula $PCI = 3 * SSS + PSS$.

## C. Base Station Signal Format

The LTE physical layer maintains the continuous connection model, especially on the FDD downlink, which operates as a continuous stream. Apart from carrying user data, the downlink transmissions contain system information, network parameters, and control signals that are essential for connection establishment and handoffs, and maintaining synchronization. The communication stream is organized as a time-frequency grid of resources, called a radio frame. Along the time axis, a frame has a duration of 10 milliseconds as shown in Figure 2. Each frame is subdivided into 1-millisecond subframes, which are further divided into two slots, each lasting 0.5 milliseconds. One slot contains 7 or 6 Orthogonal Frequency Division Multiplexing (OFDM) symbols, depending on whether the normal or extended cyclic prefix is used. Along the frequency axis, the frame length is defined by the number of OFDM subcarriers placed at 15 kHz spacing. The total number of subcarriers depends on the bandwidth of the channel, ranging from 72 in 1.4 MHz to 1200 in 20 MHz channel bandwidth. For the FDD downlinks, the PSS signal is broadcasted at the central 62 subcarriers of the last symbol of time slots 0 and 10, and the SSS signal is broadcasted one symbol before PSS.

# 3 SYSTEM DESIGN

In this section, we will discuss in detail the design of *LiTEfoot* and the technical contributions.

## A. Intermodulated Spectrum Folding

Downconversion, a critical process in RF architecture, traditionally relies on a mixer to lower high-frequency signals to the baseband by multiplying them with a carrier wave generated by a local oscillator. However, an alternate approach involves utilizing a squaring operation-multiplying it by itself to achieve downconversion without the need for an external carrier. This technique facilitates simultaneous wideband mixing and eliminates the need for a traditional oscillator, which simplifies the overall RF design. By removing the oscillator, the system becomes less complex, making it an alternative to modern RF architectures.

We introduce a technique called "intermodulated spectrum folding" that is built upon the distinct properties of LTE synchronization signals (PSS and SSS), which consistently exhibit a narrow bandwidth of 1.4 MHz (1.08 MHz without guard bands) across all LTE frame bandwidths, ranging from 1.4 MHz to 20 MHz. By implementing a squaring operation, this method isolates and folds LTE signals from various bands into the baseband. This process results in a superimposition of signals through both in-band and cross-band mixing, as illustrated in Figure 3. These superimposed signals can then be selectively extracted using a narrowband filter.

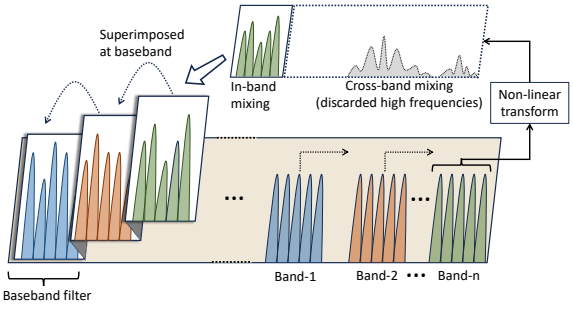



**Figure 3: Intermodulation and spectrum folding.**

Before reaping the benefits of intermodulated spectrum folding, it is pivotal to address its inherent challenges, notably the side effects of intermodulation and signal intermixing. For the effective implementation of spectrum folding in *LiTEfoot*, three critical properties must be ensured: (1) *Correlation Preservation Post-Intermodulation:* The technique must maintain the correlation characteristics of PSS and SSS after intermodulation, essential for accurate PCI estimation. (2) *Interference Mitigation:* The system must be designed to effectively withstand interference from adjacent carriers and bands that are folded into the baseband, ensuring that it can clearly distinguish the synchronization signals. (3) *Relative Signal Strength Extraction:* Despite signal squaring and superimposition, extracting relative signal strengths from overlapping base stations is crucial, enabling applications such as multilateration for precise location estimation.

Solving these challenges is fundamental to the success of intermodulated spectrum folding as a strategy for LTE. The subsequent system design section will explore how *LiTEfoot* builds upon spectrum folding, addressing these challenges.

**Envelop Detector as Non-linear Channel:** The envelope detector is an efficient way to introduce non-linearity in RF circuits using a simple passive diode. Consider two sinusoidal signals, $sin(2\pi f_1 t)$ and $sin(2\pi f_2 t)$, where $f_1$ and $f_2$ denote their respective frequencies. Let $y(t) = sin(2\pi f_1 t) + sin(2\pi f_2 t)$ be the incident signal at the envelope detector. The envelope detector subjects $y(t)$ to a non-linear squaring operation producing

$$y^2(t) = \frac{1}{2}[\cos(2\pi(f_1 - f_2)t) - \cos(2\pi(f_1 + f_2)t) + 2 - \cos(2\pi 2f_1 t) - \cos(2\pi 2f_2 t)] \quad (1)$$

The output signal $y^2(t)$ produces a baseband component $f_1 - f_2$, alongside the harmonics $2f_1, 2f_2$ and $f_1 + f_2$.

**Non-linearity in OFDM signals:** Extending $y(t)$ to an OFDM signal consisting of $N$ subcarriers, each centered around a carrier frequency $f_c$, we can write it as:

$$y(t) = \sum_{n=1}^{N} sin(2\pi(f_c + \Delta f_n)t), \quad (2)$$

where $\Delta f_n$ is the frequency offset of the $n$-th subcarrier from the carrier frequency. The squaring operation results in a sum of products of all pairs of subcarriers, which, when expanded, produces terms like:

$$y^2(t) = \frac{N}{2} + \frac{1}{2}\sum_{n=1}^{N}\sum_{m=1}^{N}[\cos(2\pi(\Delta f_n - \Delta f_m)t) - \cos(2\pi(2f_c + \Delta f_n + \Delta f_m)t)], \quad (3)$$

The output includes baseband components, $(\Delta f_n - \Delta f_m)$, independent of the carrier, and components at twice the carrier frequency, $2f_c$. To isolate the baseband components, we simply use a low-pass filter, eliminating all the higher frequency terms. Finally, the filtered output, $y^2_{lowpass}(t)$, retains only the baseband frequencies:

$$y^2_{lowpass}(t) = \frac{N}{2} - \frac{1}{2}\sum_{n=1}^{N}\sum_{m=1}^{N}\cos(2\pi(\Delta f_n - \Delta f_m)t), \quad (4)$$

The generation of baseband frequency components results from the non-linear intermodulation of the subcarriers. Essentially, it contains the frequency differences of the incoming signals, effectively downconverting or 'folding' the higher frequency elements into the baseband region.

## B. Signal Detection on Folded Spectrum

Mobile devices rely on correlation with the cell-specific synchronization signals, PSS and SSS, for initial cell identification and frame timing alignment. The pseudorandom sequences used in these signals show excellent auto-correlation for noise resilience and controlled cross-correlation property for robustness to the efficient separation of signals from different cells and support the unambiguous identification of the PCI. Spectrum folding intermodulates the subcarriers of the PSS and SSS signals and superimposes signals from different cells at the baseband. In this

section, we show that these signals sufficiently maintain these properties for successful cell identification in practice.

**Correlation properties of PSS$^2$:** After the non-linear operation, the number of unique PSS in LTE reduces from three to two. Specifically, the Zadoff–Chu sequences for $PSS_1$ and $PSS_2$, originally distinct due to their respective roots $q = 29$ and $q = 34$, selected for their good auto and cross-correlation properties under various timing and frequency offsets [82], become indistinguishable after undergoing the squaring operation. This is because these sequences, when squared, produce identical signals, effectively merging $PSS_1$ and $PSS_2$ into a single, non-distinguishable entity. This reduction, however, does not compromise *LiTEfoot*'s performance in PCI estimation. PSS signals are primarily utilized for synchronization offset estimation, while the SSS serves as the key determinant for actual PCI estimation. Therefore, despite the non-linear transformation's effect on PSS orthogonality, the integrity of PCI estimation remains unaffected, ensuring robust signal identification and time synchronization.

**Correlation properties of SSS$^2$:** An intriguing aspect of SSS signals is their resilience in maintaining excellent cross-correlation properties even after undergoing non-linear transformations. The SSS in LTE systems employs M sequences, renowned for their wide and flat spectrum due to their pseudorandom nature [113]. The non-linear transformation of SSS preserves the flatness and wideband characteristics which helps in maintaining good correlation properties even after the spectrum is intermodulated. This persistence of correlation is the key in *LiTEfoot* ensuring the robustness of our PCI estimation.

**PCI Estimation after Spectrum Folding:** To estimate PCI from intermodulated signals, we employ a time-domain correlation approach similar to a matching filter. This method extracts all the PCIs by correlating the received signal with squared versions of the predefined PSS and SSS:

$$PCI = \{i \mid \text{corr}\left(x, PSS_i^2 \oplus SSS_i^2\right) > thresh, i = 1, ..., N\} \quad (5)$$

Here, $\oplus$ is the concatenation operation and $x$ is the received signal. The PSS and SSS have a constant bandwidth of 1.08 MHz which is crucial for maintaining signal integrity across LTE's variable bandwidth scenarios.

We experimentally validate the correlation performance of the intermodulated signal ($SSS^2$) for all 504 PCIs in LTE across varying bandwidths, as shown in the confusion matrix in Figure 4. Our analysis confirms that the non-linear squaring operation preserves the orthogonal nature of the PSS and SSS signals, maintaining their unique cross-correlation and auto-correlation properties. Notably, we observe a *mod 4* ambiguity in the correlation spectrum, seen as secondary peaks at the ±4 indices relative to the original index. These secondary peaks, while present, exhibit significantly lower correlation amplitudes compared to the primary peaks. Importantly, this *mod 4* ambiguity does not compromise *LiTEfoot*'s ability to accurately estimate the PCI, as our evaluation confirms that the highest correlation values consistently align with the correct PCI.

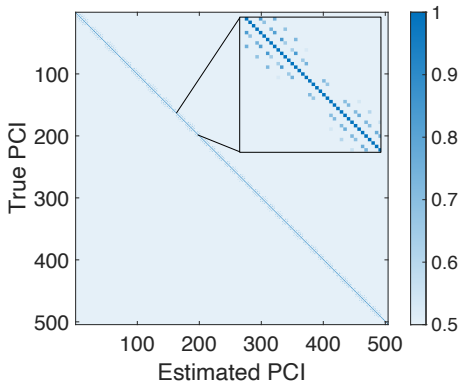



**Figure 4: Confusion matrix for PCI estimation using SSS$^2$ (i.e., the SSS signal after non-linearity).**

## C. Dealing with Folding Interference

Despite *LiTEfoot*'s efficient downconversion capabilities through passive intermodulation, its use of an envelope detector introduces notable challenges in frequency selectivity. Unlike active radios, which have the ability to distinguish and selectively filter frequencies before downconversion, the envelope detector indiscriminately processes every frequency that reaches the antenna. This broad, non-selective approach allows for intermodulation where multiple subcarriers mix with synchronization signals, as detailed in Equation 4. This intermodulation introduces unwanted signal components which degrade the overall signal quality. Such interference is particularly detrimental as it can significantly deteriorate SSS correlation. In this section, we outline the three primary sources of interference—inter-subcarrier, inter-band, and inter-synchronization signal interference—and propose specific strategies to mitigate these challenges and enhance system performance.

**(1) Inter-subcarrier interference:** In LTE networks, which have bandwidth options ranging from 1.4-20 MHz, a challenge emerges with the increase in bandwidth. Despite the constant bandwidth allocated for PSS and SSS, the use of higher bandwidth configurations by cell towers—aimed at supporting an increased user base and higher data rates—introduces inter-subcarrier interference.

As the bandwidth increases, the presence of data subcarriers also increases, leading to a scenario where these subcarriers begin to overshadow the PSS and SSS signals. The interference becomes problematic after non-linear transformation, when the data subcarriers fold on top of synchronization signals aggressively compromising the detectability of synchronization signals. For example, the correlation accuracy drops from 99.7% in a 1.4 MHz LTE frame to 1.5% in a 10 MHz frame.

To solve this challenge, we leverage the inherent periodicity of PSS and SSS (10 ms in LTE). Considering the variability of data subcarriers over frames, we model their amplitude distribution as Gaussian. This is our core intuition for frame stacking. As shown in Figure 5, we exploit the sync signal's periodic stability against the

background of fluctuating data subcarrier noise. By stacking just 100 frames—a span of 1 second—the Signal-to-Interference-and-Noise Ratio (SINR) of the sync signal is significantly enhanced, improving the accuracy of 95%.

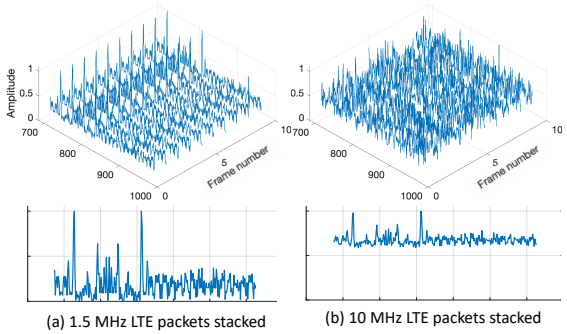



**Figure 5: LTE packets before and after stacking (a) 1.4 MHz bandwidth (b) 10 MHz bandwidth. After stacking the PSS and SSS strength increases in the 10 MHz case whereas the data fades into a DC bias.**

**(2) Inter-band interference:** Consider two cell towers operating at different bands with center frequencies $f_{c1}$ and $f_{c2}$ and bandwidths $\Delta f_1$ and $\Delta f_2$. According to Equation 4, the output signal will consist of frequency differences from inter-band subcarriers, causing interference.

In LTE, PSS and SSS occupy the central 62 subcarriers, spanning a bandwidth of 1.4 MHz. Except for the 1.4 MHz bandwidth option, which includes a 22.85% guard band, LTE bands typically incorporate a 10% guard band to mitigate interference. Given that the minimum frequency difference possible between sync signals from different cell towers will always exceed 1.4 MHz, we simply employ a low-pass filter with a cutoff frequency of $f_{cutoff} = 1.4$ MHz to remove all inter-band interference from the received signal.

**(3) Inter-synchronization signal interference:** PSS and SSS are designed with robust correlation characteristics, a feature that is preserved even after non-linear squaring operations. This resilience ensures that, despite the superposition of multiple synchronization signals, the accuracy of PCI estimation remains high. The squaring process, while introducing additional components into the signal, does not significantly disrupt the distinct correlation patterns of PSS and SSS. We also extensively evaluate *LiTEfoot* in the presence of multiple cell towers in the real world, which we discuss in the evaluation section.

## D. Recovering Base Station Signal Strength

**(1) Blind Separation of Weighted Superposition:** A key challenge in multi-cell environments is to independently extract each cell's Received Signal Strength Indicator (RSSI) from the composite received signal, where individual cell contributions are overlapped and intermodulated.

To address this challenge, we develop a blind source separation algorithm. Our approach iteratively isolates each cell's contribution to the composite signal, as illustrated in Figure **??**. The core idea is to reconstruct and subtract the time-domain PSS-SSS signal, for each identified PCI, from the received composite signal. We formulate this as an optimization problem:

$$E(A_i) = \frac{1}{N}\sum_{n=1}^{N}(x(n) - \alpha_i \cdot SyncSig_{PCI=i}(n - \delta t_i))^2$$

$$\begin{aligned} &\text{Minimize} \quad E(A_i) \\ &\text{subject to} \quad 0 \le A_i \le A_{\max} \end{aligned}$$

Here, $x(n)$ is the received signal, $SyncSig_{PCI=i}(n)$ is the PSS-SSS signal for the i-th PCI, $\alpha_i$ is the amplitude factor, $\delta t_i$ is the time delay in samples, $N$ is the total number of samples, and $A_{max}$ is the upper amplitude limit. Our objective is to minimize the residual energy $E(A_i)$ by adjusting $\alpha_i$. The minimum residual energy indicates the most accurate subtraction, corresponding to the best estimate of the cell's RSSI, as shown in Figure 6(a).

The accuracy of this separation largely depends on correctly estimating both the amplitude factor $\alpha_i$ and the time delay $\delta t_i$. Initially, we assume $\delta t_i$ is known from the correlation process used for PCI identification, though we next refine this with a super-resolution algorithm for phase-level synchronization.

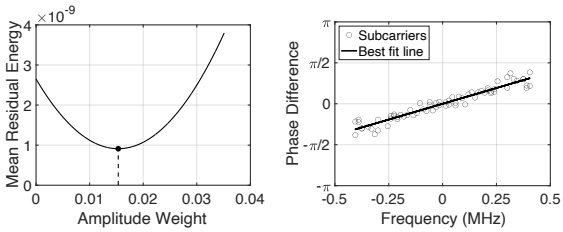



**Figure 6: (a) Blind Separation of weighted superposition (b) Linear phase change introduced due to sub-sample offset in the OFDM subcarriers.**

**(2) Sub-sample Offset Estimation:** Correlation-based synchronization can only provide sample level time-resolution [67, 100] which naturally depends on the sampling rate or the bandwidth of the receiver. Naturally, any sub-sample delay is missed out and results in poor amplitude estimation. We aim to resolve this sub-sample offsets to estimate the amplitudes accurately.

Fortunately, the cyclic prefix, with a duration of 4.7 microseconds for Frequency Division Duplexing (FDD) LTE, enables us to detect the sub-sample offsets by introducing a predictable phase change in the OFDM subcarriers of the signal. For a signal captured with $N = 62$ subcarriers, the frequency domain of the signal reveals this linear phase change across subcarriers. Figure 6(b) shows an example of linear phase changes in the subcarriers of PSS and SSS of a real-world LTE signal.

Let's say our wireless channel is $h = e^{-j2\pi f\tau}$, where $\tau$ represents the sub-sample delay, and $f$ corresponds to the frequency of each subcarrier. Given a received signal $X(f)$ and a known reference signal $S(f)$ in the frequency domain, the phase difference $\Delta\phi$ attributable to the sub-sample offset can be calculated as:

$$\Delta\phi = \angle\left(\frac{X(f)}{S(f)}\right)$$

where $\angle$ denotes the phase angle of the complex quotient, indicating the linear phase shift across subcarriers due to sub-sample offsets. This phase difference directly relates to the sub-sample delay $\tau = \frac{\Delta\phi}{2\pi\Delta f}$, where $\Delta f$ represents the frequency spacing between adjacent subcarriers. We correct for $\tau$ to accurately align the PSS and SSS in time before performing the amplitude estimation.

## E. Localization Algorithm

**(1) Multilateration with Relative Signal Strengths:** Our localization approach combines open-source databases (OpenCellID [47], Mozilla Location Services [66], and CellMapper [12]) for PCI-to-coordinate mapping of cell towers with a trilateration technique based on relative signal strengths. We formulate an optimization problem to determine the tag's position $(x, y)$ by minimizing the discrepancy between observed and expected signal strength ratios from multiple cell towers.

Given $n$ cell towers with known positions $(x_i, y_i)$ and estimated amplitudes $A_i$, we define our objective function as:

$$f(x,y) = \sum_{i=1}^{n} \sum_{j=i+1}^{n} \left( \frac{A_i}{A_j} - \frac{\sqrt{(x-x_i)^2 + (y-y_i)^2}}{\sqrt{(x-x_j)^2 + (y-y_j)^2}} \right)^2$$

This function compares the ratio of amplitudes $\frac{A_i}{A_j}$ to the ratio of Euclidean distances for each unique pair of cell towers, summing the squared differences. By using amplitude ratios rather than absolute values, we account for real-world signal propagation losses. We initialize the optimization with the centroid of all observed cell towers as our starting point.

*Eliminating False Positives.* Our system achieves near-perfect recall in PCI identification, leveraging the strong auto-correlation properties of PSS-SSS signals. However, this high sensitivity can lead to false positives. To address this challenge, we implement a refinement strategy that analyzes estimated PCIs along with their corresponding signal delays. We've observed that spurious peaks often cluster around delays associated with true cells, due to low-level correlations with other cells' signals. To filter these false positives, we group and sort signals by their estimated amplitude factors, selecting only those with non-zero amplitudes. This approach effectively balances high recall with improved precision in our PCI estimations, enhancing the overall accuracy of our localization system.

**(2) Optimization for On-Road Applications:** For applications such as vehicle tracking and urban mobility studies, we enhance our location estimation by incorporating road constraints. Our improved algorithm includes a road snapping technique [37], which aligns estimated positions with nearby drivable roads using OpenStreetMap [68] data as a sparse graph. We employ a sliding window optimization process that starts with an initial point mapped to the k-nearest road points. For each subsequent estimated point, we identify k candidate points on nearby roads and apply a distance constraint based on the maximum possible travel. This constraint is calculated as the product of the time interval between points and the road's speed limit ($\Delta t \times maxspeed$). We retain only the candidate points that satisfy this distance constraint, defaulting to the nearest point on nearby roads if no candidates meet the criteria. This optimization produces more realistic trajectories for on-road applications by leveraging the constraint that tags predominantly travel on known road networks.

## F. Extending *LiTEfoot* to Upcoming Standards

Dual sequence synchronization is a consistent feature in cellular networks that serves the basic two stage frame and slot synchronization used in standards starting from beginning (2G GSM Training Sequence[2], 3G UMTS P-SCH/S-SCH sequence[64], and PSS/SSS sequence for 4G[1] and 5G[1]). *LiTEfoot* relies on the uniqueness of these code sequences after the non-linear transformation, as described in Equation 4 (Section 3). We have shown that *LiTEfoot* architecture holds correct with other cellular standards and benchmarked its performance for 5G-NR and NB-IoT in the Evaluation section.

5G-NR expands the PCI range to 1008 values, using 3 PSS values (m-sequences of length 127) and 336 SSS values (gold sequences of length 127) [91]. Despite introducing diverse frame structures, 5G maintains key similarities with LTE. Firstly, the frame and sub-frame durations remain consistent [91]. Secondly, while 5G allows dynamic placement of synchronization signals, these signals maintain consistent location within subsequent frames and occupy 144 subcarriers with a 10ms repetition. After the non-linear transformation, the resulting baseband signal remains independent of the central frequency, requiring only an adjustment of *LiTEfoot*'s low-pass filter cutoff to accommodate 5G's subcarrier spacing.

NB-IoT, with its 15 kHz subcarrier spacing and 10ms frame length [85], is also supported by *LiTEfoot* by adjusting the filter cutoff and the wait-time for signal acquisition. The correlation properties of the code sequences naturally improve with each new standard to support denser deployment of the base stations. It leads to better post-transformation distinguishability of the sequences showing *LiTEfoot*'s potential as a universal, low-power localization system across current and NextG cellular standards.

# 4 *LITEFOOT* PROTOTYPE IMPLEMENTATION

Figure 7 illustrates the system overview, and Figure 8 presents the PCB prototype of *LiTEfoot*'s RF frontend. We've implemented a PCB prototype using low-cost COTS components and simulated a CMOS design to showcase *LiTEfoot*'s potential for further power reduction.

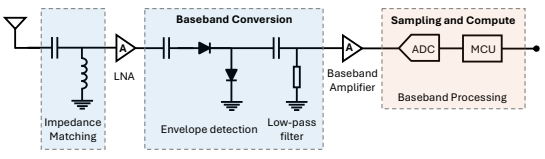



**Figure 7: The high-level circuit schematic of *LiTEfoot*.**

**RF Frontend:** We design a flexible patch antenna with a center frequency of 1.94 GHz covering LTE bands. Our RF frontend utilizes a tuned RF architecture [104], comprising of a low-noise amplifier (LNA), an envelope detector, and a high-impedance amplifier.

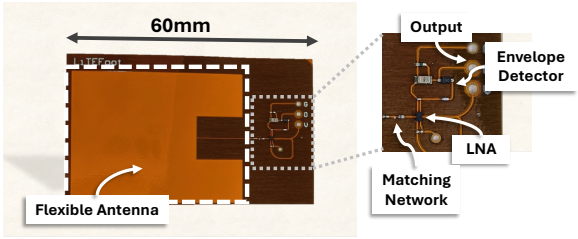



**Figure 8: *LiTEfoot* PCB tag prototype showing the low-power RF frontend.**

**Envelope Detector:** We implement a Greinacher voltage doubler circuit [43] using a Skyworks Schottky diode [87] for RF-to-baseband conversion. A $\pi$ matching network ensures 50Ω impedance matching. High Q-value capacitors and inductors minimize losses. The detector's output passes through a passive low-pass filter with a 1.4 MHz cutoff.

**Baseband Amplification:** The tuned RF 20dB amplifier boosts sensitivity to -70dBm. The high-impedance sub-MHz baseband amplifier uses a 10-stage cascaded common-source configuration, achieving 68 dB voltage gain.

**ADC:** We use an ultra-low-power successive approximation register (SAR) ADC by Texas Instruments [49]. This 12-bit ADC with SPI interface requires an external serial clock and consumes 585.7 $\mu$W offering the power efficiency required for our prototype.

**Baseband Processing:** We implement *LiTEfoot* using the Apollo3 Blue ultra-low-power ARM Cortex-M4 based MCU SoC [5]. It interfaces with the ADC via SPI and uses Direct Memory Access for efficient signal transfer. The SoC's flash stores the code with zero fetch overhead, while data resides in SRAM and Flash. We power-gate the unused SRAM banks during idle times. Overall, the SoC consumes less than 6$\mu$A/MHz at 3V during active processing and approximately 1$\mu$A/MHz in deep sleep mode. While we optimize for power efficiency using the COTS MCU, future ASIC implementations could further help in reducing the power consumption [38, 39, 79].

**Cost of Prototype:** We design the prototype using COTS components. It includes an Skyworks SMS7630 diodes [48] ($0.60), an Infineon BGA7M1N6 LNA [93] ($1.11), a TI ADS7042 ADC [49] ($2.79), and an Ambiq Apollo3 [5] ($3.98). Including additional passive components, the total material cost for a *LiTEfoot* prototype is $9.48. This low-cost design, combined with *LiTEfoot*'s long battery life and minimal maintenance requirements, enables economically viable large-scale deployments for wide-area asset tracking and various IoT applications.

**CMOS Simulation:** We designed and simulated an Application Specific Integrated Circuit (ASIC) using TSMC-45nm CMOS technology to explore further power efficiency. The ASIC layout, created using Electric VLSI software and simulated with PathWave Advanced Design System (ADS), demonstrates a potential power consumption reduction to 112 $\mu$W. For the LNA, we implemented a self-biased inverter architecture [90] optimized for 45nm CMOS, achieving 15 dB gain while consuming only 89 $\mu$W. The transistors are biased in the low-inversion region at 0.26V with a 25 $k\Omega$ self-biasing resistor. We simulated a 10-bit charge-redistribution ADC [97] capable of 2 Msps at 3.8 $\mu$W, significantly outperforming the COTS ADC (ADS7042) used in our PCB prototype. These improvements could enable years of battery life for small tags.

# 5 EVALUATION

## A. Localization Evaluation

We evaluate *LiTEfoot*'s localization performance through real-world experiments across urban and rural environments, comparing it against GPS ground truth. Our experiments cover multiple routes totaling 54km, with *LiTEfoot*'s tag mounted in a vehicle alongside an iPhone 15 running the Matlab mobile application for GPS data collection. Table 1 summarizes the key characteristics of our test routes: an urban route (Route 1) covering 1.80 km$^2$ with 35 cell towers (19.44 cells/km$^2$), and two rural routes (Routes 2 and 3) spanning 3.60 km$^2$ and 4.05 km$^2$ with 10 and 11 towers respectively (2.78 and 2.72 cells/km$^2$).

| Route | Area (km$^2$) | Number of Towers | Cell Density (cells/km$^2$) |
|---|---|---|---|
| Route 1 | 1.80 | 35 | 19.44 |
| Route 2 | 3.60 | 10 | 2.78 |
| Route 3 | 4.05 | 11 | 2.72 |

**Table 1: Key characteristics of evaluation routes.**

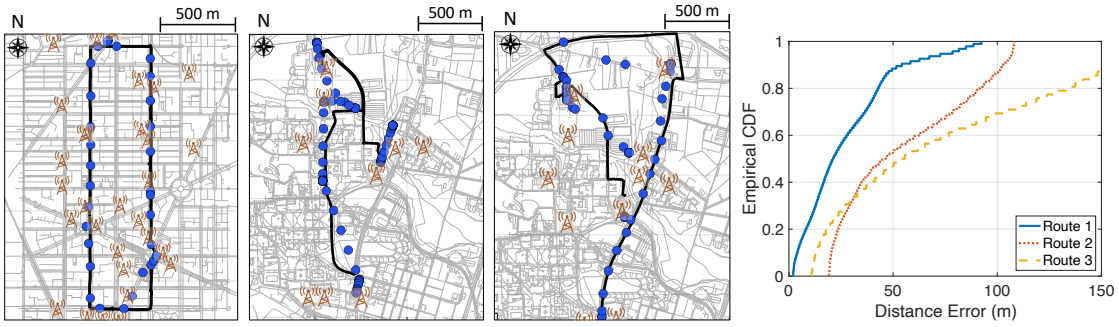
Figure 9 shows *LiTEfoot*'s estimated trajectories (blue) alongside GPS trajectories (black) for each route and presents the CDF of absolute location errors. Our results show a median error of 22 meters in the urban area and 50 meters in rural areas. These results correlates strongly with cell tower density, with the urban route consisting approx 7 times higher density compared to the rural routes, directly impacting the localization accuracy.

We note that existing baselines were not suitable for direct comparison, as many require prior information about cell towers (e.g., LTE Band, MNC, MCC) or are incompatible with real-world cell tower setups due to high latency demands, as demonstrated in next section. This evaluation validates *LiTEfoot*'s ability to provide accurate localization in the wild across varied environments.

## B. Latency Evaluation

We evaluate *LiTEfoot*'s sensing latency across LTE bands (spanning 450 MHz to 3 GHz) and compare its performance with existing localization techniques. The experiment was conducted on a predefined route in a challenging environment of rural area where we observed 8 unique LTE bands (2, 4, 5, 12, 13, 14, 41, and 71) with at least one serving cell each (see Fig. 10).

**Baselines:** In this experiment we compared *LiTEfoot* against four baseline methods: •GPS: Using a COTS module [95]. •Wideband SDR Search: Scanning the entire LTE band using frequency hopping. •Targeted Band SDR Search: Pre-selecting six frequencies based on prior knowledge. •RSSI Method: Implementing Crescendo [19] on targeted frequencies. Each baseline presents distinct trade-offs. GPS offers high accuracy but with relatively high latency and power consumption. SDR-based methods provide flexibility but suffer from long sensing times due to sequential frequency hopping. The RSSI




(a) Route1: Urban (b) Route2: Rural (c) Route3: Rural (d) Localization accuracy

**Figure 9: *LiTEfoot*'s estimated trajectories and localization errors for in (a) urban and (b), (c) rural environments. The black lines denote the GPS trajectory and blue markers denote *LiTEfoot*'s estimated trajectory. The cell towers that are detected during the route are shown in red. (d) The empirical CDF of the localization errors.**

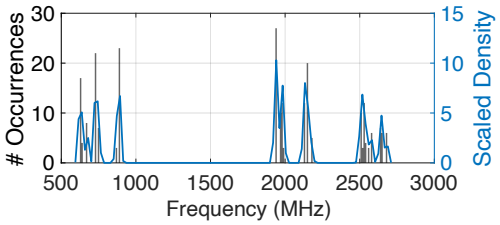



**Figure 10: Diversity in downlink center frequencies used by the cells in a 200-meter radius.**

method improves on SDR approaches but still requires pre-selection of frequencies.

**Results and Analysis:** Table 2 shows the comparison of latency, accuracy, and power consumption. The results show the fundamental challenge in cellular-based localization: the vast number of possible configurations (65,535 in LTE) necessitates either frequency hopping or prior knowledge of active bands, creating a significant latency bottleneck. *LiTEfoot* overcomes this bottleneck through its spectrum folding technique, enabling simultaneous sensing of all LTE bands. This approach eliminates the need for sequential frequency hopping, resulting in exponential reduction in latency.

| Method | Latency (s) | Error (m) | Energy (mJ) |
|---|---|---|---|
| SDR (Wideband search) | 66100 | 38 | $21 \times 10^4$ |
| SDR (Targeted search) | 0.66 | 38 | 210 [76, 92] |
| Crescendo [19] | 0.66 | 24 | 210 |
| GPS [95] | 1 | 2 | 25 |
| *LiTEfoot* | 0.01 | 19 | 0.039 |

**Table 2: Comparison between latency, accuracy, and power consumption.**

## C. Power Evaluation

**Measurements Methodology:** We implemented *LiTEfoot* on a custom PCB using low-power COTS components. Power consumption of individual modules was measured using a Keysight power monitoring unit [53] for high-precision readings. Additionally, we performed CMOS simulations to estimate potential power savings. The RF peripheral in our PCB prototype interfaces with an Apollo3 MCU.

**Power Consumption Analysis:** Tables 3, 4, and 5 show the overall power and energy per inference, along with a breakdown of power consumption for the RF chain (PCB and 45nm CMOS) and baseband computation, respectively. In our PCB prototype, the RF frontend consumes 8738.8 $\mu$W, with the LNA being the most power-intensive component at 8035.2 $\mu$W. The total energy consumption per inference is 902.37 $\mu$J, distributed between the RF frontend (873.88 $\mu$J) and baseband compute (28.49 $\mu$J). The baseband compute consumes 2035 $\mu$W of power and takes 14.52 ms per inference, with SSS correlations dominating the time consumption at 13.02 ms. Our CMOS simulation results demonstrate significant potential for power reduction. The simulated RF frontend consumes only 111.8 $\mu$W, representing a 98.7% reduction compared to the PCB prototype. Total energy consumption per inference in the CMOS simulation is 39.67 $\mu$J, a 95.6% reduction from the PCB prototype. The simulated RF frontend achieves high sensitivity (-70 dBm), while the ADC simulation shows a power consumption of 3.8 $\mu$W at 2 Msps, further contributing to the overall system efficiency.

**Battery Life:** We project that the CMOS implementation of *LiTEfoot* can operate continuously for 11 years on a standard CR20we32 coin cell battery (220 mAh) with location updates every 5 seconds.

| Module | Power ($\mu$W) | Time (s) | Energy ($\mu$J) |
|---|---|---|---|
| RF frontend (PCB) | 8738.8 | 0.10 (10 frames) | 873.88 |
| RF frontend (CMOS) | 111.8 | 0.10 (10 frames) | 11.18 |
| Baseband Compute | 2035 | 0.0145 | 28.49 |
| **Total (PCB)** | | **0.1145** | **902.37** |
| **Total (CMOS)** | | **0.1145** | **39.67** |

**Table 3: Overall power and energy per inference.**

## D. Micro-Benchmarks

**Comparison of 5G-NR, NB-IoT, and LTE Standards:** We evaluate *LiTEfoot*'s performance across LTE, 5G-NR, and NB-IoT, each employing distinct PCI encoding methods. LTE, our baseline, uses 504 unique PCI values from both PSS and SSS. NB-IoT simplifies

| Component | PCB prototype ($\mu$W) | CMOS sim ($\mu$W) |
|---|---|---|
| LNA | 8035.2 | 89 |
| Envelope Detector | 0 | 0 |
| High Imp. PA | 162.9 | 19 |
| ADC | 585.7 | 3.8 |
| **Total RF** | **8738.8** | **111.8** |

**Table 4: RF frontend power consumption.**

| Module | Power ($\mu$W) | Time (ms) |
|---|---|---|
| PSS Search (correlations) | 2035 | 0.66 |
| SSS Search (correlations) | 2035 | 13.02 |
| Amplitude Estimation | 2035 | 0.84 |
| Multilateration | 2035 | $2 \times 10^{-6}$ |
| **Total Baseband** | **2035** | **14.52** |

**Table 5: Baseband power and time per inference.**

this approach, using only the Narrowband SSS (NSSS) to encode 504 NCellID values. In contrast, 5G-NR expands to 1008 unique PCI values while retaining LTE's PSS and SSS structure. As we show in Figure 11, NB-IoT achieves the highest PCI estimation accuracy, exceeding 95%, due to its narrower bandwidth and simplified signal structure. 5G-NR initially shows lower accuracy but matches NB-IoT's performance with increased frame stacking, due to its broader bandwidths and fluctuating data subcarriers. LTE maintains consistent performance across frame stack above 20. These results demonstarte *LiTEfoot*'s adaptability across cellular standards, with frame stacking proving particularly effective in managing 5G-NR's dynamic resource allocation.

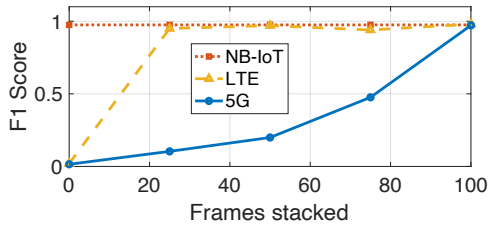



**Figure 11: PCI estimation accuracy (F1 score) vs. number of stacked frames for LTE, 5G-NR, and NB-IoT.**

**Sub-sample offset correction:** We evaluate the effect of sub-sample offsets due to clock drift or synchronization errors. Since we do not have any way to synchronize the tag with the base stations, there could be ground truth timing errors. Figure 12a shows the CDF of phase-offsets for all subcarriers before and after the sub-sample correction algorithm. As we see, before the offset correction, sub-sample shifts within ±0.5 sample can result in phase shifts of $\pm\pi$ radians. Whereas, after applying our sub-sample correction, most phase differences are reduced to 0. This benchmark uses 1000 real-world synchronization signals with varying signal strengths. We observe there are a few outliers in the CDF when the phase noise is large compared to the signal strength and the best-fit slope of the phase is incorrectly estimated.

**Impact of speed:** We evaluate *LiTEfoot*'s performance at varying vehicle speeds in both urban and rural environments, using GPS-measured ground truth speeds. As shown in Figure 12b, urban settings demonstrate the minimal impact of speed on

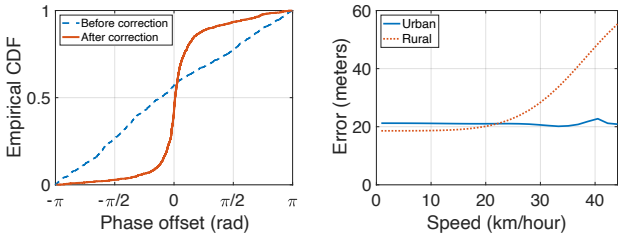



**Figure 12: (a) CDF of phase offsets in measurements before and after sub-sample offset correction. (b) Localization error for varying speed of vehicle.**

localization accuracy. In contrast, rural environments have increased localization errors at higher speeds. Urban environments typically feature a higher density of smaller cells and micro-cells, which change every few meters, contributing to more robust localization across various speeds.

## E. Ultra-low-power Geofencing

We also evaluate *LiTEfoot* for geofencing application, which can enable ultra-low-power tracking for elderly care monitoring and route enforcement. Our approach focuses on minimizing power consumption and evaluating continuous PCI monitoring for timely and accurate alert generations.

To reduce computational load, we implement a hierarchical search algorithm that leverages the reduced number of unique PSS signals post non-linear transformation and the periodic nature of synchronization signals. This algorithm first performs a PSS search to identify potential time indices, followed by selective SSS correlation, significantly narrowing the search scope. We further optimize by focusing on known base stations rather than continuously searching for new ones, reducing the search space from thousands to tens of samples in subsequent frames.

We evaluate the alert generation performance in four different scenarios: two for entry restrictions and two for exit restrictions. Geofencing boundaries are marked on maps, and the relevant PCI database is filtered onto the tag. The tag continuously monitors observed PCI values and generates alerts when entering or exiting marked locations. Figure 13a illustrates the PCIs detected over time and marks the event when the tag exits a designated region. Figure 13b shows the overall accuracy of alert generation distance from marked boundaries across urban and rural settings. Our results show alert generation within 24 meters of the defined boundaries in urban environments and 106 meters in rural environments due to lower cell tower density.

# 6 RELATED WORK

**Asset tracking:** Asset tracking applications span various domains, from supply chain management to healthcare [10, 32, 40, 62, 69, 75]. GPS and satellite-based systems [17, 36**?** ] offer global coverage but face power and indoor limitations. Cellular IoT technologies like NB-IoT and LTE-M [55, 70] improve on GPS's battery life and coverage for wide-area tracking. RFID [103, 108], BLE beacons

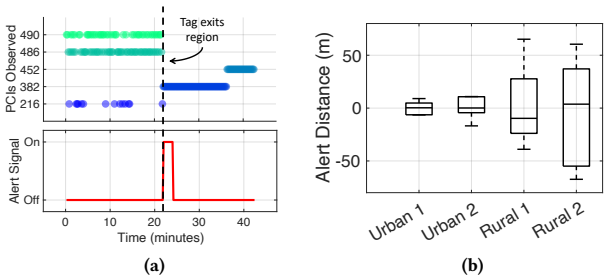



**Figure 13: (a) An alert is generated when the tag exits the boundary of the marked region. (b) Alert generation distance from the map boundaries.**

[6, 59], and acoustics [7, 8, 28, 29, 34, 57, 110] offer low-cost, short-range tracking solutions for controlled indoor environments, each with distinct advantages and limitations. *LiTEfoot* on the other hand leverages ambient cellular signals for low-power, wide-area asset tracking without custom infrastructure.

**Cellular localization:** Ambient cellular signals have been explored for localization and tracking [24, 25, 56, 71, 83, 84]. RSSI-based approaches [46, 58, 107] achieve 50-200 meter accuracy. Fingerprinting techniques [13, 21, 45, 54, 80] improve accuracy to sub-50 meters but require extensive wardriving. Notably, Crescendo [19] utilizes RSSI distributions within grid cells; and DeepLoc [86] and DeepFeat [65] use RSSI to train a deep learning model to achieve sub-20 meter accuracy. TransparentLoc [114] leverages crowdsourced data for both indoor and outdoor location estimation. However, these methods typically require power-intensive downconversion and frequency hopping, limiting IoT applicability. ISLA [51] offers cellular self-localization but faces form factor constraints due to multi-antenna requirements. In contrast, *LiTEfoot* enables wideband sensing and localization without power-intensive components, striking a balance between accuracy and energy efficiency for low-power IoT applications.

**Non-linearity based receivers:** Recent advancements in low-power RF receivers [20, 30, 31, 39, 73, 79, 98] have focused on replacing active components with non-linear envelope detectors to reduce power consumption in communication [3, 15, 72, 89, 99, 111, 112]. MIXIQ [79] introduced a low-power 802.11ax receiver by modifying OFDM packets to include a helper tone and preserve IQ data during downconversion. These systems primarily rely on the use of a secondary helper signal or changes in the transmitter. ReMix [101] leveraged non-linear backscatter circuits for in-body communication and localization. LivingIoT [50] and Sirius [31] use envelope detectors for direction of arrival estimation. In contrast to all these approaches, *LiTEfoot* operates on unmodified cellular networks, leveraging non-linear transformations of cellular synchronization signals to enable wideband sensing and PCI estimation without requiring helper tones or any protocol modifications. This approach allows *LiTEfoot* to achieve ultra-low power consumption while maintaining compatibility with existing cellular infrastructure.

# 7 DISCUSSION

**Scalable and Sustainable IoT:** This paper is a step toward a broader vision of sustainable ambient intelligence and scalable IoT. By leveraging existing cellular infrastructure for self-localization, *LiTEfoot* enables country-wide scalability without dedicated anchors. The system's ultra-low-power design allows tags to operate for years without battery replacement or maintenance, minimizing electronic waste and environmental impact. This substantially reduces the tag's embodied carbon footprint [74]. *LiTEfoot*'s wide-bandwidth sensing and low-latency inference capabilities enable tracking millions of objects across smart cities and supply chains. We believe this could revolutionize urban sustainability through real-time air quality monitoring or tracking personal belongings across vast distances. *LiTEfoot* paves the way for sustainable, large-scale tracking solutions that align technological progress with environmental consciousness.

**Communicating locations:** Localization trackers often need a communication module to periodically update location to a server or nearby hub. Standalone GPS trackers (e.g., [35] and [95]) often use cellular or satellite communications to do so. *LiTEfoot* can incorporate an NB-IoT module for relaying location data. Using a low-power NB-IoT transmitter [96], which consumes 76 mW to transmit a 140 kb packet in eDRX mode, the system can intermittently send updates hourly, daily, or monthly depending on the application. This enables *LiTEfoot* to operate for approximately 10 years on a coin cell. The same antenna frontend can be shared between *LiTEfoot* and the communication unit, maintaining a compact form factor while providing flexible communication capabilities.

**PCI Distribution:** 4G-LTE defines 504 unique PCI numbers to be used in base stations per network. Cellular networks are designed to ensure neighboring base stations get unique PCI numbers [81], while it may repeat in a non-adjacent base station. So, in theory, a PCI-based localization system can face ambiguity when a combination of PCI values from observable base station transmission repeats for two different geographic locations. However, the probability of such repeating combinations is significantly small. Moreover, *LiTEfoot* often senses multiple PCI values from each service provider operating in a region which makes the chances of location ambiguity negligible.

**PCI database updates:** In LTE networks, the PCI value typically changes infrequently under normal operating conditions. PCI values remain constant unless there is a network reconfiguration such as cell outages, recoveries, maintenance, or upgrades [25, 52, 78, 81]. However, *LiTEfoot* can maintain good accuracy even with infrequent database changes, as it relies on multiple PCI values per location. Moreover, the tags can be updated using the same NB-IoT module used for communication, ensuring long-term reliability with minimal overhead.

**Application scenarios of *LiTEfoot*:** The ultra-low-power design of the system enables a wide range of long-term tracking applications. In logistics, *LiTEfoot* can provide wide-area asset tracking to combat cargo pilfering, a major supply chain challenge. For smart cities, *LiTEfoot* can enable efficient management of

shared e-scooters and bikes by logging usage and location data, transmitting only when docked. In agriculture, it facilitates long-term livestock monitoring and geofencing of large industrial vehicles with minimal communication needs. Urban services can benefit from *LiTEfoot*-equipped smart waste bins or trucks that log positions and communicate only when necessary. The system's 20-meter accuracy suffices for these applications. With its ability to operate for years on a single cell, *LiTEfoot* opens up possibilities for persistent, wide-area monitoring across diverse domains, from supply chain management to environmental sensing.

**Limitations and Future Work:** Our work reveals opportunities for further refinement. Like GPS and other RF-based systems, *LiTEfoot*'s performance may be affected in metal-enclosed spaces due to signal attenuation. The system's accuracy, while sufficient for many applications, could be enhanced in areas with sparse LTE coverage. Our current PCB prototype, while functional, leaves room for optimization; VNA-tuned impedance matching could significantly improve sensitivity and power efficiency, especially for the LNA. The localization algorithm currently assumes uniform transmitting power from cell towers, which may not always hold true, affecting precision. Implementing time-of-flight based multilateration could potentially improve accuracy by reducing reliance on signal strength assumptions. Subtle effects of tag orientation and placement on signal reception could be mitigated with improved antenna design. Future ASIC implementations could further reduce power consumption and form factor.

## 8 CONCLUSION

*LiTEfoot* is a novel low-power cellular localization system leveraging non-linear spectrum transformation for efficient baseband signal superimposition. It senses a 3 GHz wideband LTE spectrum in 10 ms using non-linear intermodulation, while operating in the $\mu J$ energy regime and achieving median localization errors of 22 m.

## 9 ACKNOWLEDGEMENT

The authors would like to thank the anonymous shepherd and reviewers for their helpful comments. This work was partially supported by NSF CAREER Award 2238433. We also thank the companies that sponsors the iCoSMoS laboratory at UMD.

## REFERENCES

[1] 3GPP. 2024. 3GPP Specifications Per TSG Round. https://www.3gpp.org/specifications-technologies/specifications-by-series/specifications-per-tsg-round. Accessed: 2024-07-01.
[2] 3rd Generation Partnership Project (3GPP). 2024. *GSM/EDGE Physical layer on the radio path. General description.* Technical Specification 45.001. Technical Specification Group Radio Access Network. Available: 3GPP website.
[3] Mohamed R Abdelhamid, Ruicong Chen, Joonhyuk Cho, Anantha P Chandrakasan, and Fadel Adib. 2020. Self-reconfigurable micro-implants for cross-tissue wireless and batteryless connectivity. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.
[4] Fahim Ahmed, Mark Phillips, Stephen Phillips, and Kyoung-Yun Kim. 2020. Comparative study of seamless asset location and tracking technologies. *Procedia Manufacturing* 51 (2020), 1138–1145.
[5] Ambiq. 2024. Ultra-low power microcontroller Apollo3 Blue. https://ambiq.com/apollo3/.
[6] Roshan Ayyalasomayajula, Deepak Vasisht, and Dinesh Bharadia. 2018. BLoc: CSI-based accurate localization for BLE tags. In *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*. 126–138.
[7] Yang Bai, Nakul Garg, and Nirupam Roy. 2022. Spidr: Ultra-low-power acoustic spatial sensing for micro-robot navigation. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 99–113.
[8] Yang Bai, Nakul Garg, and Nirupam Roy. 2024. Microstructure-Assisted Vision: Adding New Senses to Low-Power Devices. *GetMobile: Mobile Computing and Communications* 27, 4 (2024), 15–20.
[9] Atul Bansal, Akshay Gadre, Vaibhav Singh, Anthony Rowe, Bob Iannucci, and Swarun Kumar. 2021. Owll: Accurate lora localization using the tv whitespaces. In *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)*. 148–162.
[10] Ygal Bendavid, Harold Boeck, and Richard Philippe. 2010. Redesigning the replenishment process of medical supplies in hospitals with RFID. *Business Process Management Journal* 16, 6 (2010), 991–1013.
[11] Willem Bouten, Edwin W Baaij, Judy Shamoun-Baranes, and Kees CJ Camphuysen. 2013. A flexible GPS tracking system for studying bird behaviour at multiple scales. *Journal of Ornithology* 154 (2013), 571–580.
[12] CellMapper. 2024. CellMapper. https://www.cellmapper.net/.
[13] Ayon Chakraborty, Luis E Ortiz, and Samir R Das. 2015. Network-side positioning of cellular-band devices with minimal effort. In *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2767–2775.
[14] Youjing Cui and Shuzhi Sam Ge. 2003. Autonomous vehicle positioning with GPS in urban canyon environments. *IEEE transactions on robotics and automation* 19, 1 (2003), 15–25.
[15] Farzan Dehbashi, Ali Abedi, Tim Brecht, and Omid Abari. 2021. Verification: can wifi backscatter replace RFID?. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 97–107.
[16] José A del Peral-Rosado, Ronald Raulefs, José A López-Salcedo, and Gonzalo Seco-Granados. 2017. Survey of cellular mobile radio localization methods: From 1G to 5G. *IEEE Communications Surveys & Tutorials* 20, 2 (2017), 1124–1148.
[17] DigitalMatter. 2024. DigitalMatter Asset Tracking. https://www.digitalmatter.com/our-devices/4g-gps-trackers/.
[18] Laura Dodds, Isaac Perper, Aline Eid, and Fadel Adib. 2023. A handheld fine-grained rfid localization system with complex-controlled polarization. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*. 1–15.
[19] Rizanne Elbakly and Moustafa Youssef. 2019. Crescendo: An infrastructure-free ubiquitous cellular network-based localization system. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6.
[20] Joshua F Ensworth, Alexander T Hoang, and Matthew S Reynolds. 2017. A low power 2.4 GHz superheterodyne receiver architecture with external LO for wirelessly powered backscatter tags and sensors. In *2017 IEEE International Conference on RFID (RFID)*. IEEE, 149–154.
[21] Sinem Coleri Ergen, Huseyin Serhat Tetikol, Mehmet Kontik, Raffi Sevlian, Ram Rajagopal, and Pravin Varaiya. 2013. RSSI-fingerprinting-based mobile phone localization with route constraints. *IEEE Transactions on Vehicular Technology* 63, 1 (2013), 423–428.
[22] Kelly R Evenson, Michelle M Goto, and Robert D Furberg. 2015. Systematic review of the validity and reliability of consumer-wearable activity trackers. *International Journal of Behavioral Nutrition and Physical Activity* 12, 1 (2015), 1–22.
[23] FCC. 2023. https://docs.fcc.gov/public/attachments/DA-15-1487A1.pdf.
[24] Yuda Feng, Yaxiong Xie, Deepak Ganesan, and Jie Xiong. 2021. Lte-based pervasive sensing across indoor and outdoor. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*. 138–151.
[25] Yuda Feng, Yaxiong Xie, Deepak Ganesan, and Jie Xiong. 2022. Lte-based low-cost and low-power soil moisture sensing. In *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*. 421–434.
[26] Raul Fernández-Garcia and Ignacio Gil. 2017. An alternative wearable tracking system based on a low-power wide-area network. *Sensors* 17, 3 (2017), 592.
[27] Attila Frankó, Gergely Vida, and Pal Varga. 2020. Reliable identification schemes for asset and production tracking in industry 4.0. *Sensors* 20, 13 (2020), 3709.
[28] Nakul Garg, Yang Bai, and Nirupam Roy. 2021. Microstructure-guided spatial sensing for low-power iot. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 503–504.
[29] Nakul Garg, Yang Bai, and Nirupam Roy. 2021. Owlet: Enabling spatial information in ubiquitous acoustic devices. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 255–268.
[30] Nakul Garg and Nirupam Roy. 2023. poster: Ultra-low-power Angle-of-Arrival Estimation Using a Single Antenna. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. 569–570.
[31] Nakul Garg and Nirupam Roy. 2023. Sirius: A self-localization system for resource-constrained iot sensors. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. 289–302.
[32] Nakul Garg, Irtaza Shahid, Karthik Sankar, Mallesham Dasari, Ramanujan K Sheshadri, Karthikeyan Sundaresan, and Nirupam Roy. 2023. Bringing AR/VR to Everyday Life-a Wireless Localization Perspective. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*. 142–142.

[33] Nakul Garg, Irtaza Shahid, Ramanujan K Sheshadri, Karthikeyan Sundaresan, and Nirupam Roy. 2023. Fast Localization and Tracking in City-Scale UWB Networks. *arXiv preprint arXiv:2310.02211* (2023).

[34] Nakul Garg, Harshvardhan Takawale, Yang Bai, Irtaza Shahid, and Nirupam Roy. 2023. Structure assisted spectrum sensing for low-power acoustic event detection. In *Proceedings of Cyber-Physical Systems and Internet of Things Week 2023*. 278–284.

[35] Global View. 2024. Buy GPS Tracking Devices. https://www.global-view.net/buy-gps-tracking-devices Accessed: 2024-07-01.

[36] GlobalStar. 2024. GlobalStar IoT Asset Tracking. https://www.globalstar.com/en-us/products/iot.

[37] Google. 2024. Google Snap to Roads. https://developers.google.com/maps/documentation/roads/snap.

[38] Xiuzhen Guo, Yuan He, Zihao Yu, Jiacheng Zhang, Yunhao Liu, and Longfei Shangguan. 2022. RF-transformer: a unified backscatter radio hardware abstraction. In *Proceedings of the 28th annual international conference on mobile computing and networking*. 446–458.

[39] Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. 2022. Saiyan: Design and implementation of a low-power demodulator for {LoRa} backscatter systems. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. 437–451.

[40] Hanhaa. Year. *Cold Chain Monitoring*. https://hanhaa.com/cold-chain/ Accessed: Month Day, Year.

[41] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. 2020. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal* 8, 8 (2020), 6222–6246.

[42] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. 2022. AirGuard-protecting android users from stalking attacks by apple find my devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 26–38.

[43] Hewlett-Packards. [n. d.]. https://www.hpl.hp.com/hpjournal/95dec/dec95a12.pdf.

[44] Hazem Ibrahim, Rohail Asim, Matteo Varvello, and Yasir Zaki. 2023. I Tag, You Tag, Everybody Tags!. In *Proceedings of the 2023 ACM on Internet Measurement Conference*. 561–568.

[45] Mohamed Ibrahim and Moustafa Youssef. 2011. CellSense: An accurate energy-efficient GSM positioning system. *IEEE Transactions on Vehicular Technology* 61, 1 (2011), 286–296.

[46] Mohamed Ibrahim and Moustafa Youssef. 2011. A hidden markov model for localization using low-end GSM cell phones. In *2011 IEEE International Conference on Communications (ICC)*. IEEE, 1–5.

[47] Open Cell ID. 2024. Open Cell ID. https://opencellid.org/.

[48] Skyworks Solutions Inc. Accessed 2024. SMS7630-079LF Schottky Diode - Single, 20V, 100mA, 2 pF @ 0V, 30 Ohm @ 5mA, SC-79 Package. https://www.digikey.com/en/products/detail/skyworks-solutions-inc/SMS7630-079LF/2052135. Available at Digi-Key Electronics.

[49] Texas Instruments. 2024. 12-Bit Ultra-Low-Power SAR ADC With SPI Interface. https://www.ti.com/product/ADS7042.

[50] Vikram Iyer, Rajalakshmi Nandakumar, Anran Wang, Sawyer B Fuller, and Shyamnath Gollakota. 2019. Living IoT: A flying wireless platform on live insects. In *The 25th Annual International Conference on Mobile Computing and Networking*. 1–15.

[51] Suraj Jog, Junfeng Guan, Sohrab Madani, Ruochen Lu, Songbin Gong, Deepak Vasisht, and Haitham Hassanieh. 2022. Enabling {IoT}{Self-Localization} Using Ambient 5G Signals. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. 1011–1026.

[52] Hakan Kavlak and Hakki Ilk. 2012. PCI planning strategies for long term evolution networks. In *NETWORKING 2012 Workshops: International IFIP TC 6 Workshops, ETICS, HetsNets, and CompNets, Held at NETWORKING 2012, Prague, Czech Republic, May 25, 2012. Proceedings 11*. Springer, 151–156.

[53] Keysight. 2024. Keysight E6313A Power Supply. https://www.keysight.com/us/en/assets/9018-04576/user-manuals/9018-04576.pdf.

[54] Heikki Laitinen, Jaakko Lahteenmaki, and Tero Nordstrom. 2001. Database correlation method for GSM location. In *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings (Cat. No. 01CH37202)*, Vol. 4. IEEE, 2504–2508.

[55] Christos Laoudias, Adriano Moreira, Sunwoo Kim, Sangwoo Lee, Lauri Wirola, and Carlo Fischione. 2018. A survey of enabling technologies for network localization, tracking, and navigation. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3607–3644.

[56] Da Li, Yingke Lei, and Haichuan Zhang. 2020. A novel outdoor positioning technique using LTE network fingerprints. *Sensors* 20, 6 (2020), 1691.

[57] Dong Li, Jialin Liu, Sunghoon Ivan Lee, and Jie Xiong. 2020. FM-track: pushing the limits of contactless multi-target tracking using acoustic signals. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 150–163.

[58] Ding-Bing Lin and Rong-Terng Juang. 2005. Mobile location estimation based on differences of signal attenuations for GSM systems. *IEEE transactions on vehicular technology* 54, 4 (2005), 1447–1454.

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

[60] Kai Lv, Xiaolong Pan, Junwen Zhang, Kaihui Wang, Dong Guo, Qi Zhang, ao Li Deng, and Xiangjun Xin. 2019. Envelope detection of 16QAM single carrier signal for IM/DD RoF system at Q-band. *IEICE Electronics Express* 16, 4 (2019), 20180986–20180986.

[61] Vivek Mangal and Peter R Kinget. 2019. A wake-up receiver with a multi-stage self-mixer and with enhanced sensitivity when using an interferer as local oscillator. *IEEE Journal of Solid-State Circuits* 54, 3 (2019), 808–820.

[62] Digital Matter. Year. *Cold Chain Monitoring*. https://www.digitalmatter.com/applications/cold-chain-monitoring/ Accessed: Month Day, Year.

[63] Kunal Maurya, Mandeep Singh, and Neelu Jain. 2012. Real time vehicle tracking system using GSM and GPS technology-an anti-theft tracking system. *International Journal of Electronics and Computer Science Engineering* 1, 3 (2012), 1103–1107.

[64] Ajay R Mishra. 2007. *Advanced cellular network planning and optimisation: 2G/2.5 G/3G... evolution to 4G*. John Wiley & Sons.

[65] Amel Mohamed, Mohamed Tharwat, Mohamed Magdy, Tarek Abubakr, Omar Nasr, and Moustafa Youssef. 2022. DeepFeat: Robust large-scale multi-features outdoor localization in LTE networks using deep learning. *IEEE Access* 10 (2022), 3400–3414.

[66] Mozilla. 2024. Mozilla Location Services. https://location.services.mozilla.com.

[67] Rajalakshmi Nandakumar, Vikram Iyer, Desney Tan, and Shyamnath Gollakota. 2016. Fingerio: Using active sonar for fine-grained finger tracking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 1515–1525.

[68] OpenStreetMap contributors. 2024. OpenStreetMap. https://www.openstreetmap.org.

[69] Asil Oztekin, Foad M Pajouh, Dursun Delen, and Leva K Swim. 2010. An RFID network design methodology for asset tracking in healthcare. *Decision support systems* 49, 1 (2010), 100–109.

[70] Stefano Parrino, Giacomo Peruzzi, and Alessandro Pozzebon. 2021. Lopatran: Low power asset tracking by means of narrow band iot (nb-iot) technology. *Sensors* 21, 11 (2021), 3772.

[71] Giovanni Pecoraro, Simone Di Domenico, Ernestina Cianca, and Mauro De Sanctis. 2018. CSI-based fingerprinting for indoor localization using LTE signals. *EURASIP Journal on Advances in Signal Processing* 2018 (2018), 1–18.

[72] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. 2018. PLoRa: A passive long-range data network from ambient LoRa transmissions. In *Proceedings of the 2018 conference of the ACM special interest group on data communication*. 147–160.

[73] Carlos Pérez-Penichet, Claro Noda, Ambuj Varshney, and Thiemo Voigt. 2018. Battery-Free 802.15. 4 Receiver. In *2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 164–175.

[74] Thibault Pirson and David Bol. 2021. Assessing the embodied carbon footprint of IoT edge devices with a bottom-up life-cycle approach. *Journal of Cleaner Production* 322 (2021), 128966.

[75] PowerFleet. Year. *Asset Tracking Solutions*. https://www.powerfleet.com/asset-tracking/ Accessed: Month Day, Year.

[76] Qorvo. 2024. RF2052 RF Frequency Converter, 30 - 2500 MHz, Integrated PLL/VCO, RF Mixer. https://www.rfmw.com/products/detail/rf2052-qorvo/326547/?gad_source=1&gclid=EAIaIQobChMI0LTFvrT_hgMVnWJHAR0uzQKnEAAYBCAAEgL_nfD_BwE. Accessed: 2024-06-28.

[77] Partha Pratim Ray, Dinesh Dash, and Debashis De. 2019. A systematic review and implementation of IoT-based pervasive sensor-enabled tracking system for dementia patients. *Journal of medical systems* 43 (2019), 1–21.

[78] RFAssurance. 2015. The Value of PCI Planning in LTE. https://main.rfassurance.com/?q=node/79. https://main.rfassurance.com/?q=node/79 Accessed: 2024-07-01.

[79] Mohammad Rostami, Xingda Chen, Yuda Feng, Karthikeyan Sundaresan, and Deepak Ganesan. 2021. MIXIQ: re-thinking ultra-low power receiver design for next-generation on-body applications. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 364–377.

[80] Hazem Sallouha, Alessandro Chiumento, and Sofie Pollin. 2017. Localization in long-range ultra narrow band IoT networks using RSSI. In *2017 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[81] J Salo, M Nur-Alam, and K Chang. 2010. Practical introduction to LTE radio planning. *A white paper on basics of radio planning for 3GPP LTE in interference limited and coverage limited scenarios, European Communications Engineering (ECE) Ltd, Espoo, Finland* 47 (2010).

[82] Stefania Sesia, Issam Toufik, and Matthew Baker. 2011. *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons.

[83] Kimia Shamaei and Zaher M Kassas. 2018. LTE receiver design and multipath analysis for navigation in urban environments. *Navigation* 65, 4 (2018), 655–675.

[84] Kimia Shamaei, Joe Khalife, and Zaher M Kassas. 2018. Exploiting LTE signals for navigation: Theory to implementation. *IEEE Transactions on Wireless Communications* 17, 4 (2018), 2173–2189.

[85] Aya Shimura, Mamoru Sawahashi, Satoshi Nagata, and Yoshihisa Kishiyama. 2018. Physical Cell ID Detection Performance Applying Frequency Diversity Reception to NPSS and NSSS for NB-IoT. In *2018 24th Asia-Pacific Conference on Communications (APCC)*. 514–519. https://doi.org/10.1109/APCC.2018.8633505

[86] Ahmed Shokry, Marwan Torki, and Moustafa Youssef. 2018. DeepLoc: A ubiquitous accurate and low-overhead outdoor cellular localization system. In *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. 339–348.

[87] Skyworks. 2024. https://store.skyworksinc.com/products/detail/sms7630006-skyworks/150612/.

[88] Raghav Subbaraman, Kevin Mills, Aaron Schulman, and Dinesh Bharadia. 2023. Crescendo: Towards Wideband, Real-Time, High-Fidelity Spectrum Sensing Systems. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*. 1–14.

[89] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. 2017. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 1, 3 (2017), 1–24.

[90] T. Taris, JB. Begueret, and Y. Deval. 2011. A 60µW LNA for 2.4 GHz wireless sensors network applications. In *2011 IEEE Radio Frequency Integrated Circuits Symposium*. 1–4. https://doi.org/10.1109/RFIC.2011.5940633

[91] Technical Specification Group Radio Access Network. [n. d.]. *NR; Physical channels and modulation.* Technical Specification 38.211. 3rd Generation Partnership Project (3GPP).

[92] Infineon Technologies. 2024. BGA7M1N6E6327XTSA1 RF MOSFET, Low Noise Amplifier. https://www.win-source.net/products/detail/infineon-technologies/bga7m1n6e6327xtsa1.html. Accessed: 2024-06-28.

[93] Infineon Technologies. Accessed 2024. BGA7M1N6E6327XTSA1 - RF Amplifier, LTE Band 7, 2.5GHz to 2.7GHz, 15.6dB Gain, 0.75dB Noise Figure, 20dBm OIP3, TSNP-6 Package. https://www.digikey.com/en/products/detail/infineon-technologies/BGA7M1N6E6327XTSA1/5959862. Available at Digi-Key Electronics.

[94] Amee Trivedi and Deepak Vasisht. 2020. Digital contact tracing: technologies, shortcomings, and the path forward. *ACM SIGCOMM Computer Communication Review* 50, 4 (2020), 75–81.

[95] u blox. 2023. Ultra-low power GPS with the u-blox M10. https://www.u-blox.com/en/blogs/tech/ultra-low-power-gps-u-blox-m10 Accessed: 2024-07-01.

[96] u blox. 2024. SARA-N310 Module. https://www.u-blox.com/en/product/sara-n310-module. https://www.u-blox.com/en/product/sara-n310-module Accessed: 2024-07-01.

[97] Michiel Van Elzakker, Ed Van Tuijl, Paul Geraedts, Daniel Schinkel, Eric Klumperink, and Bram Nauta. 2008. A 1.9 $\mu$W 4.4 fJ/conversion-step 10b 1MS/s charge-redistribution ADC. In *2008 IEEE International Solid-State Circuits Conference-Digest of Technical Papers*. IEEE, 244–610.

[98] Ambuj Varshney and Lorenzo Corneo. 2020. Tunnel emitter: Tunnel diode based low-power carrier emitters for backscatter tags. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.

[99] Ambuj Varshney, Oliver Harms, Carlos Pérez-Penichet, Christian Rohner, Frederik Hermans, and Thiemo Voigt. 2017. LoRea: A backscatter architecture that achieves a long communication range. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. 1–14.

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

[101] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi. 2018. In-body backscatter communication and localization. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. 132–146.

[102] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. 2017. {FM} backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*. 243–258.

[103] Jue Wang and Dina Katabi. 2013. Dude, where's my card? RFID positioning that works with multipath and non-line of sight. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. 51–62.

[104] David D Wentzloff, Abdullah Alghaihab, and Jaeho Im. 2020. Ultra-low power receivers for IoT applications: A review. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 1–8.

[105] Henry H Willis and David Santana Ortiz. 2004. Evaluating the security of the global containerized supply chain. (2004).

[106] Yi Wu, Hai Jiang, Ye Wu, and Dongmei Zhang. 2010. Physical cell identity self-organization for home eNodeB deployment in LTE. In *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*. IEEE, 1–6.

[107] Jie Yang, Alexander Varshavsky, Hongbo Liu, Yingying Chen, and Marco Gruteser. 2010. Accuracy characterization of cell tower localization. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 223–226.

[108] Lei Yang, Yekui Chen, Xiang-Yang Li, Chaowei Xiao, Mo Li, and Yunhao Liu. 2014. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. 237–248.

[109] Sooyoung Yoo, Seok Kim, Eunhye Kim, Eunja Jung, Kee-Hyuck Lee, and Hee Hwang. 2018. Real-time location system-based asset tracking in the healthcare field: lessons learned from a feasibility study. *BMC medical informatics and decision making* 18 (2018), 1–10.

[110] Sangki Yun, Yi-Chao Chen, Huihuang Zheng, Lili Qiu, and Wenguang Mao. 2017. Strata: Fine-grained acoustic-based device-free tracking. In *Proceedings of the 15th annual international conference on mobile systems, applications, and services*. 15–28.

[111] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. Freerider: Backscatter communication using commodity radios. In *Proceedings of the 13th international conference on emerging networking experiments and technologies*. 389–401.

[112] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. 2016. Enabling practical backscatter communication for on-body sensors. In *Proceedings of the 2016 ACM SIGCOMM Conference*. 370–383.

[113] Tao Zhang, Shuxing Li, Tao Feng, and Gennian Ge. 2014. Some New Results on the Cross Correlation of $m$-sequences. *IEEE transactions on information theory* 60, 5 (2014), 3062–3068.

[114] Shuli Zhu, Lingkun Li, Xuyu Wang, Changcheng Liu, Yuqin Jiang, Zengwei Huo, Hua Chai, Jiqiang Liu, Dan Tao, and Ruipeng Gao. 2023. Experience: Large-scale cellular localization for pickup position recommendation at black-hole. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*. 1–15.