Enabling IoT Self-Localization Using Ambient 5G mmWave Signals

Junfeng Guan[†], Suraj Jog[†], Sohrab Madani[†], Ruochen Lu[*], Songbin Gong[†], Deepak Vasisht[†], Haitham Hassanieh[‡]
University of Illinois Urbana-Champaign[†], University of Texas at Austin[*], EPFL[‡]

ABSTRACT

The small cell size, wide bandwidth, and MIMO antenna arrays in 5G mmWave networks provide great opportunities for IoT localization. However, low-power and low-cost IoT devices are incapable of leveraging these benefits. We present *mm-ISLA*: a system that enables IoT nodes to localize themselves using ambient 5G mmWave signals without any coordination with the base stations. *mm-ISLA* leverages MEMS Spike-Train filters to access the wideband 5G signals and estimates the Angle of Departure from the base station MIMO antenna arrays to accurately localize the IoT nodes.

1 INTRODUCTION

Recent years have witnessed a tremendous growth in the number of IoT devices, with surveys projecting up to 31 billion deployed IoT nodes by 2030 [7]. Given such ubiquitous deployment of IoT nodes, the ability to localize and track these nodes with high accuracy is essential for many applications.

In this work, we present *mm-ISLA*, **I**oT **S**elf-**L**ocalization using **A**mbient 5G mmWave signals, a system that enables IoT devices to localize themselves in 5G networks by simply overhearing the *ambient* 5G mmWave signals without any coordination with the base stations, also known as gNBs. Leveraging ambient 5G signals, especially those in mmWave bands, for localizing IoT nodes is extremely appealing, because of two characteristics of 5G mmWave networks: 1) The small cell sizes lead to very dense deployments of base stations, up to 50 gNB per km^2 [3], resulting in more potential anchor points for accurate localization. 2) The unprecedentedly wide signal bandwidth, up to 400 MHz in mmWave eMBB channels, provides high Time of Flight (ToF) resolution. These two features together provide great opportunities for high-accuracy localization.

Enabling coordination-free self-localization using the ambient wideband 5G signals requires solving two fundamental challenges: (1) Power-constrained narrowband IoT devices, equipped with low-power and low-speed Analog-to-Digital Converters (ADC) [6], are incapable of capturing wideband 5G signals and reusing them for localization. (2) *mm-ISLA*'s IoT self-localization technique should not require any active participation of the gNBs, e.g., coordination or synchronization. Any needs for coordination and synchronization require modifying the 5G standards and dedicated gNB resource to function, so they cannot scale to the ubiquitous IoT nodes.

SIGCOMM '22 Demos and Posters, August 22–26, 2022, Amsterdam, Netherlands

ACM ISBN 978-1-4503-9434-5/22/08.
https://doi.org/10.1145/3546037.3546061

mm-ISLA is an extension of *ISLA*, a recent work of the authors [4], which focuses on IoT self-localization in sub-6 GHz bands. However, in this work, we try to extend *ISLA* to mmWave bands by resolving a limitation of *ISLA*. In this way, *mm-ISLA* can leverage the even wider bandwidth and smaller cell size.

Similar to *ISLA*, *mm-ISLA* overcomes the first challenge using MEMS (Micro-ElectroMechanical System) Spike-Train filters [2, 5], that is a novel RF filter with a spike-train-shaped frequency response, as shown in Fig. 1(b). When passing the wideband 5G signal through the Spike-Train filter, only the OFDM subcarriers in the spikes are kept while all the other subcarriers are filtered out as Fig. 1(c) illustrates. The filtered spectrum becomes sparse in the frequency domain, so *mm-ISLA* can sample the filtered signal below the Nyquist sampling rate, yet still be able to recover the wideband Channel Frequency Response (CFR). Eventually, the wideband CFR is translated into high-resolution Channel Impulse Response (CIR), as if *mm-ISLA* can access the entire bandwidth. This is the key enabler of *mm-ISLA*'s high localization accuracy.

However, adapting *ISLA*'s coordination-free localization protocol to mmWave bands would be impractical, because *ISLA* avoids coordination with the gNBs by measuring the Time Difference of Arrival (TDoA) between two antennas on the IoT node. Such IoT design requires two antenna front-ends with tightly synchronized RX chains, which is infeasible in mmWave frequencies because of the expensive and power-consuming mmWave front-ends. Therefore, *mm-ISLA* abandons the dual front-end IoT design and the TDoA-based localization algorithm of *ISLA*. Instead, *mm-ISLA* overcomes the coordination-free challenge by leveraging the additional degree of freedom provided by the MIMO antenna arrays at the 5G gNBs. *mm-ISLA* first resolves channels from multiple TX antennas at the gNBs leveraging a unique 5G-NR waveform – DeModulation Reference Signal (DMRS) in the Physical Downlink Shared Channel (PDSCH). The unique resource allocation pattern in the DMRS waveforms allows *mm-ISLA* to distinguish the OFDM subcarriers allocated to each antenna in the gNB MIMO antenna array. Therefore, *mm-ISLA* can then leverage the channel differences across the antennas to estimate the Angle of Departure (AoD) of the Line-of-Sight (LoS) path from the gNB to the IoT node. Finally, with the AoD measurements of three gNBs, an *mm-ISLA* node can localize itself using the standard triangulation localization algorithm.

2 *MM-ISLA* LOCALIZATION ALGORITHM

Figure 1 illustrates *mm-ISLA*'s system pipeline, and how it solves the two challenges of coordination-free IoT self-localization.

(1) Wideband Channel Estimation on Narrowband IoT Nodes: *mm-ISLA* mostly adopts the same approach as *ISLA* to overcome the challenge of capturing wideband 5G signals and estimating the wideband channel using low-speed ADCs on IoT devices. Since the sampling rates of IoT devices are significantly below the Nyquist

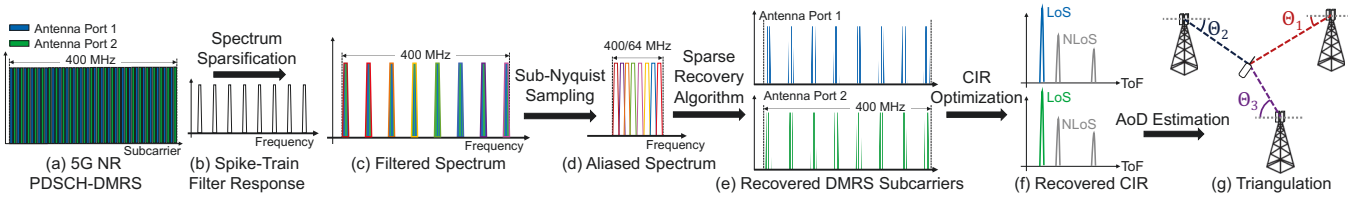

Figure 1: *mm-ISLA* **pipeline. (a) Wideband 5G PDSCH-DMRS Spectrum Allocated to 2 Antenna Ports. (b) MEMS Spike-Train Filter Frequency Response. (c) Filtered Sparse Spectrum. (d) Sub-Nyquist Sampled Spectrum Aliased to the Narrow ADC Bandwidth. (e) Recovered DMRS Subcarriers. (f) Recover Channel Impulse Response. (g) AoD-Based Triangulation Localization.**

sampling rate of wideband 5G signals, the wideband spectrum will alias to the narrow bandwidth of the ADCs, which leads to frequency collisions between subcarriers and makes them unresolvable. *mm-ISLA* utilizes the MEMS Spike-Train filter with periodic spike-shaped passbands to sparsify the wideband spectrum. The resulting spectrum becomes sparse with a periodic sparsity pattern, which allows us to reconstruct the wideband spectrum after sub-Nyquist Sampling. Moreover, the sparsity pattern of the filtered spectrum can be specifically designed by modeling the MEMS filter architecture [5]. Therefore, *mm-ISLA* adopts the filter hardware and sparse recovery algorithm co-design from *ISLA* to avoid frequency collisions and to maintain OFDM subcarrier orthogonality after aliasing.[1] After reconstructing the wideband spectrum, we estimate the CFR and translate it into super-resolution CIR by formulating an inverse optimization problem. Note that the ToF resolution of the reconstructed CIR is equivalent to that of the wide 5G bandwidth, and this is the key to achieve high localization accuracy.

(2) Coordination-Free Localization using a Single Antenna Front-End: Towards solving the coordination-free challenge, *mm-ISLA* however, takes a completely different approach than *ISLA*. The TDoA-based localization algorithm of *ISLA* is abandoned, because it requires two tightly synchronized RF front-ends, RF chains, and ADCs. The additional RF circuitry and ADC doubles the cost and power-consumption of the IoT nodes, which is even more infeasible in the mmWave frequencies than in the sub-6GHz bands. Restricted to a single antenna front-end, *mm-ISLA* enabled IoT nodes still manage to localize themselves without any coordination with the gNBs. To do so, *mm-ISLA* leverages another unique opportunity in 5G networks – the spatial diversity of the MIMO antenna arrays at the 5G gNBs. *mm-ISLA* tries to measure the ToF differences across antennas in the gNB MIMO antenna array, from which *mm-ISLA* can infer the AoD of the LoS path from the gNB to the IoT node. With AoD estimates of three or more gNBs along with the gNB locations and antenna array orientations, *mm-ISLA* enabled IoT nodes will be able to apply the standard triangulation algorithm to localize themselves. However, to do so, *mm-ISLA* has to first be able to estimate the CIR from each gNB MIMO antenna separately.

The question becomes how can *mm-ISLA* isolate concurrent transmissions from TX MIMO antennas at the 5G gNB and estimate them corresponding CIR separately? Note that signals from different TX antennas has to be transmitted at the same time, otherwise, the transmitting time offset will corrupt the AoD estimation. To overcomes this challenge, *mm-ISLA* leverages another unique opportunities in the 5G-NR standards, that is the resource allocation pattern in the 5G-NR PDSCH-DMRS waveforms. PDSCH-DMRS is a specific type of 5G-NR waveform used for decoding the PDSCH

[1]We refer interested readers to [4] for hardware-software co-design details.

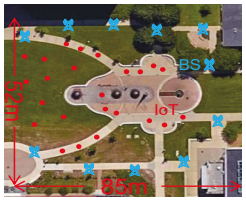

Figure 2: Testbed

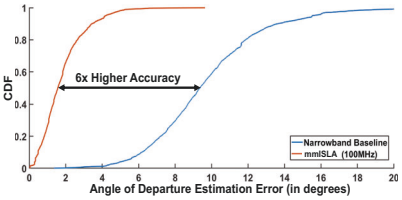

Figure 3: AoD Estimation Accuracy

data, so it's a preamble-like waveform one can leverage to estimate the channel. When MIMO is enabled at the gNB, to decode the channels from the MIMO antennas, different antenna ports are allocated with a different set of interleaved subcarriers in the resource block [1], as shown in Fig. 1(a). Therefore, we can identify the DMRS subcarriers corresponding to each TX antenna and estimate their channels separately. Since the interleaved subcarrier allocation pattern ensures that the DMRS waveform from all TX antennas covers the entire bandwidth of the resource block, we can still achieve wideband CFR estimations for all TX antenna. Therefore, we can estimate the super-resolution CIRs corresponding to each TX antenna with a small modification to the inversion optimization problem to incorporate the subcarrier allocation in the PDSCH-DMRS waveform. Finally, we compare the ToF differences across the TX antennas to estimate the AoD of the LoS path.

3 PRELIMINARY RESULTS AND DISCUSSION

We conducted preliminary experiments in a outdoor testbed as shown in Fig. 2 to evaluate *mm-ISLA*'s AoD estimation accuracy. Due to the lack of MIMO-enabled mmWave frond-ends, we evaluated *mm-ISLA*'s AoD estimation technique in sub-6GHz bands. We emulated a dual-antenna 5G gNB and a *mm-ISLA* enabled IoT node equipped with the MEMS spike-train filter using X310 USRPs. The dual-antenna base station prototype transmits 100 MHz OFDM waveform that mimics the 5G-NR DMRS waveform in the vacant 950 to 1050 MHz spectrum. The *mm-ISLA* IoT prototype emulates the MEMS spike-train filter in digital and then downsamples the signal by 16×, so that the effective ADC sampling rate is 6.25 MHz.

We compare the AoD estimation accuracy of *mm-ISLA* after reconstructing the 100 MHz wideband CIR against a baseline using a 6.25 MHz narrowband receiver without the spike-train filter. As shown in Fig. 3, *mm-ISLA* can achieve a median AoD error of only 1.56°, which is 6× lower than the 9.37° of the narrowband baseline. This result shows that *mm-ISLA* is able to leverage wideband 5G signals to estimate the AoD of the LoS path with high accuracy.

In practice, due to the directionality of mmWave gNBs, IoT nodes might not be able to receive PDSCH signals from three gNBs at a given location. However, *mm-ISLA* can potentially jointly leverage PDSCH signals and narrowband Synchronization Signal Block (SSB) used in beam sweeping to get three anchor points for triangulation.

REFERENCES

[1] 3GPP. 2020. *5G; NR; Physical channels and modulation.* Technical Specification (TS) 138.211. 3rd Generation Partnership Project (3GPP). Version 16.2.0.

[2] Junfeng Guan, Jitian Zhang, Ruochen Lu, Hyungjoo Seo, Jin Zhou, Songbin Gong, and Haitham Hassanieh. 2021. Efficient Wideband Spectrum Sensing Using MEMS Acoustic Resonators. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. USENIX Association, 809–825.

[3] Yixue Hao, Min Chen, Long Hu, Jeungeun Song, Mojca Volk, and Iztok Humar. 2017. Wireless fractal ultra-dense cellular networks. *Sensors* 17, 4 (2017), 841.

[4] 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)*. USENIX Association, Renton, WA, 1011–1026. https://www.usenix.org/conference/nsdi22/presentation/jog

[5] Ruochen Lu, Tomás Manzaneque, Yansong Yang, Jin Zhou, Haitham Hassanieh, and Songbin Gong. 2018. RF filters with periodic passbands for sparse Fourier transform-based spectrum sensing. *Journal of Microelectromechanical Systems* 27, 5 (2018), 931–944.

[6] Parvathanathan Subrahmanya and Amir Farajidana. 2020. 5G and Beyond: Physical Layer Guiding Principles and Realization. *Journal of the Indian Institute of Science* 100 (2020), 263–279.

[7] Adam Thierer and Andrea Castillo. 2015. Projecting the growth and economic impact of the internet of things. *George Mason University, Mercatus Center, June* 15 (2015).