A Study of Network-Side 5G User Localization Using Angle-Based Fingerprints

Jiayi Meng†, Abhigyan Sharma⋆, Tuyen X. Tran⋆, Bharath Balasubramanian⋆, Gueyoung Jung⋆,
Matti Hiltunen⋆, Y. Charlie Hu†
Purdue University†, AT&T Labs Research⋆

***Abstract*—This paper explores network-side cellular user localization using fingerprints created from the angle measurements enabled by 5G. Our key idea is a binning-based fingerprinting technique that leverages multipath propagation to create fingerprint vectors based on angles of arrival of signals along multiple paths at each user. In network simulations that recreate urban environments with 3D building geometry and base station locations for a major city, our binning-based fingerprinting for 5G achieves significantly lower localization errors with a single base station than signal strength-based fingerprinting for LTE.**

I. Introduction

Cellular carriers perform user localization to infer the location of a user making an emergency call (as required by the Enhanced 9-1-1 system [2]) and optimize user performance in other potential use-cases such as handoff prediction [6]. Carriers must localize users purely using network-side techniques such as radio channel measurements since they do not have access to GPS information recorded by a user equipment (UE).

In LTE networks, the simplest and most coarse-grained network-side localization technique is called Tracking Area Update in which the base station (BS) that a user is connected to is reported [7]. LTE standards also include the Observed Time Difference of Arrival (OTDoA) technique, which uses BSes' locations and time difference of arrival of signals from different BSes at an user equipment (UE) to estimate the user's location. OTDoA is a form of a *geometric technique* that estimates the distances of a user from given reference points such as the surrounding BSes.

Fingerprinting techniques, in contrast, take a data-driven approach to localization. A fingerprint database is created from channel measurements such as the received signal strength from several BSes for each spatial grid (e.g., a 50m$\times$50m geographic area). Fingerprints for a user are matched to those in the database to estimate the grid the user is located in [8], [11], [13]. Fingerprinting techniques for LTE have been shown to outperform geometric techniques in a recent large-scale study using real LTE datasets [11] achieving a 300-1000m lower localization error than a geometric approach for a 50m$\times$50m grid size. This result is also suggestive of the difficulty of accurate geometric modeling of cellular networks.

In 5G, the use of antenna arrays enables measurements of angle of arrival of signals at the receiver (UE or BS). Such angle measurements have been used to localize WiFi users using geometric techniques that estimate the angles of a user with respect to multiple reference points such as WiFi access points [4], [9], [15], [17], [18], [22] and then use trilateration to localize the user. But, these techniques typically assume the existence of line-of-sight (LoS) transmissions to estimate the angle of a user with respect to a BS. Further, they assume availability of multiple reference points for trilateration.

But, applying angle-based geometric techniques to localize cellular UEs is challenging. First, a cellular UE may not have LoS transmissions from a BS in indoor or outdoor environments due to blockage by buildings or other objects. Second, a UE may only be in the range of a single BS, e.g., in sub-urban or rural environments with a sparse deployment of BSes. Third, multipath propagation makes it hard to accurately determine the angle of the UE with respect to a BS based on the angles of arrival of signals at the receiver.

Given the limitations of geometric techniques, we ask if angle measurements can localize users through a fingerprinting technique. Our intuition is that a high degree of multipath with distinct angles of arrival along each path could be used to create a unique location fingerprint. Based on this intuition, this paper addresses two main questions:

(1) How to create fingerprints from angle measurements in presence of multipath propagation? Multipath propagation results in multiple copies of the signal arriving at the receiving antenna with different angle, power, and delay. With distinct angles measured for each of the paths, which angle do we treat as a fingerprint? In case of an unequal number of paths at two locations, how do we compare angle measurements? Even if the number of paths is identical, how do we order the paths in a consistent manner across measurements in the absence of any metadata about each path?

(2) How does the accuracy of angle-based fingerprinting in 5G compare to RSRP-based fingerprinting available in LTE? Since 5G deployments are in early stages with limited availability, it is challenging to conduct a large scale comparative study between LTE and 5G. Further, our efforts to measure angle information on available 5G smartphones such as Samsung Galaxy S10 show that well-known diagnostic tools such as MobileInsight [10] do not reveal angle information even when connected to a 5G BS. Hence, we need an experimental setup that enables both RSRP and angle-related channel measurements needed for localization.

Our key idea is a *binning-based fingerprinting technique* that outputs a constant-size vector based on the zenith angle, the azimuth angle, and the received power along all the observed paths. Each element in the vector indicates whether the power received in an angular bin is above or below a threshold value. This technique has several advantages. First, fingerprints are of the same form independent of the number of paths, which makes it straightforward to compare fingerprints using standard distance metrics. Second, the uniqueness of angle measurements in the fingerprint can be maintained by choosing a sufficiently long vector. Third, the fingerprint only uses power as a binary indicator, hence it is robust to the higher variations in received power resulting from the use of millimeter wave (mmWave) radios in 5G. Finally, the technique is useful in creating fingerprints even if a single BS is observed by a UE. While our technique can be applied to any wireless network where angle measurements can be performed, we explore its feasibility in 5G networks.

Our comparative study uses a novel simulation methodology in that it recreates outdoor cellular environments with 3D building geometry data in a given area, actual LTE BS locations from a cellular carrier, and potential 5G BS locations selected among locations available to that cellular carrier. To our knowledge, this is a first study that evaluates localization approaches by combining realistic building geometries and BS locations. We use the ns-3 network simulator to collect extensive measurements for UEs with dual-stack radios (LTE and 5G mmWave). Our experiments cover geographic area in and around Atlanta, USA.

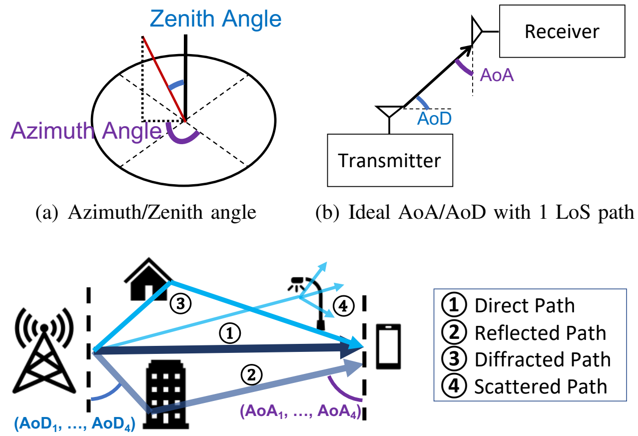
We present the first comparison of localization techniques for LTE and 5G, which respectively use the signal strength measurements and angle measurements for fingerprinting. These are our key findings in this exploratory work:

- Our binning-based localization using azimuth and zenith angles from one 5G mmWave BS has more than 70m lower median error than RSRP-based localization with one LTE BS due to the directionally insensitive nature of RSRP.
- Channel measurements from multiple BSes significantly reduce errors for both binning-based and RSRP-based localization, albeit binning-based localization has a 1.7m higher median error than RSRP-based localization in this case.
- A baseline angle-based technique, using mean angle as a fingerprint for localization, has up to 22.5m higher median error than binning-based localization, thereby showing the value of our binning-based fingerprinting technique.

II. Background

In this section, we provide background on angle measurements in wireless networks and on emerging 5G networks.

Angle measurements: In a three-dimensional space, the direction is specified by an *azimuth angle* in the horizontal plane and a *zenith angle* in the vertical plane as shown in Figure 1(a). For a directional wireless communication along a line of sight (LoS) between a trasmitter and a receiver, the 3D angle at which the transmitter sends a wireless signal is called the angle of departure (AoD), and then angle at which the receiver receives the signal is called the angle of arrival (AoA).



(a) Azimuth/Zenith angle (b) Ideal AoA/AoD with 1 LoS path

(c) Multipath propagation causes UE to receive signals from LoS and NLoS paths with different AoA and power.

Fig. 1. Illustration of azimuth, zenith, AoA, AoD.

Figure 1(b) shows AoA and AoD for LoS communication. Due to a combination of factors such as reflection and diffraction, wireless signals arrive at the receiver along multiple paths. Hence, a receiver typically observes multiple signal paths with distinct angles of arrival as shown in Figure 1(c).

The estimation of angle of arrival depends on the availability of antenna arrays in the receiver radio. The basic idea is to measure the phase shift in the arriving signal at consecutive antennas, and combining it with the space separation between these antennas to estimate the angle of arrival of signal. The phase shift can be obtained by reading the channel state information (CSI) matrix reported by radios. The CSI matrix can then be used by well-known high resolution AoA estimation algorithms such as MUSIC and ESPIRIT to estimate the AoA of not just one, but multiple paths at the same time [14], [16].

5G cellular networks: 5G operates in sub-6GHz as well as mmWave frequency ranges. In part to support the higher mmWave frequencies that are susceptible to interference, 5G BSs and UEs employ 8×8 phased-array antennas for transmit and receive beamforming, respectively, in order to improve the SNR while minimizing co-channel interference. Further, due to the shorter range of mmWave communication, such 5G BSs will need to be deployed with high density with inter-cell distance of a few hundred metres.

For UE localization, deployment of smaller cells can already help estimate user location to within a few hundred meters simply based on the tracking area update of the BS a UE is connected to. Hence, more sophisticated UE localization strategies (e.g., geometric or fingerprinting based strategies) would need to provide location accuracy within few 10s of meters for them to be effective. While a 5G network can continue to use localization techniques developed for LTE networks such as RSRP-based fingerprinting, the use of antenna arrays at the 5G transceivers potentially enables estimation of AoA and its use for UE localization [1].

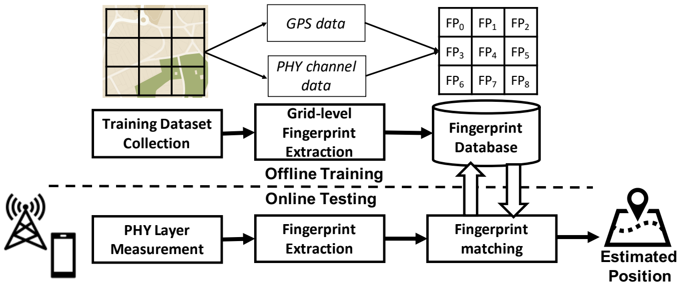


Fig. 2. Fingerprinting localization architecture

III. Angle-Based Localization Design

We first describe the components of our overall localization system (Section III-A), followed by a description of its key technique of binning-based fingerprint using angle measurements (Section III-B).

A. System Architecture

We consider a deployment of 5G BSes alongside existing LTE BSes and 5G UEs supporting dual connectivity with both LTE and 5G radios.[1] A UE collects radio channel measurements with respect to both LTE and 5G BSes, and reports them to the serving BS through the reference signal. The serving BS uses these measurements to estimate the channel quality and can also forward them in real-time to a controller server, typically owned and deployed by the carrier, for localization.

A UE collects channel measurements that are used by LTE localization techniques (e.g., RSRP and RSRQ), as well as the following 5G-specific measurements for any 5G BSes it observes. The UE records the BS identifier for all 5G BSes in range, and on each of the observed paths from those BSes, it measures (1) the *azimuth angle* of arrival of signal in the horizontal plane, (2) the *zenith angle* of arrival in the vertical plane, and (3) the *power* of the received signal for the path. Techniques to measure azimuth and zenith AoAs are covered in this survey [20]. The power values can be obtained from the power-delay profile, which characterizes arrival times of different signal paths versus their received power [21].

Offline localization training: The workflow for the training phase of localization is shown in Figure 2. During the offline training phase, first, the geographic area is partitioned into square grids of size $g \times g$ (unit: meters). Second, s locations are sampled within each grid to collect geographical location as well as localization-related channel measurements from the all BSes observed at a location. For each location, the fingerprint is extracted using our fingerprinting technique. Then, the database records the fingerprint for the grid by averaging the fingerprints of the s locations, while the grid's geographic location is represented by its center.

There are two broad methods to populate such a fingerprinting database. In the drive test approach, a test device is attached to a moving vehicle that records the radio measurements and geographic locations (e.g., using GPS) for all possible streets [5]. In the crowd-sourcing approach [11], which is used in a production Tier-1 ISP, the geolocation of a UE is reported by a smartphone application on the UE and the fingerprint for the same UE at the same time is obtained using ongoing radio channel measurements.

Online fingerprint matching: Figure 2 also shows the steps of the online matching phase. First, a UE measures and reports localization-related channel measurements to the serving BS. Next, a fingerprint is computed by the localization controller based on reported measurements using our fingerprinting algorithm. Finally, the fingerprint is matched to the existing fingerprints in a database. The closest fingerprint based on Euclidean distance is selected and the geographic location associated with that fingerprint is the final output.

B. Binning-Based Fingerprinting

Consider a UE that observes one or more BSes at a location. For each BS r, the UE measures a channel vector c_r of (azimuth angle, zenith angle, power) for each path from that BS. We convert this channel vector c_r into a constant-sized vector fingerprint f_r using the technique described below. Our overall fingerprint F at one location is a key-value map from each BS r to its fingerprint vector f_r.

We next describe how fingerprint f_s is obtained from its channel vector c_r. The challenge here is an unequal number of paths across locations because of non-uniform distribution of buildings and other objects which cause reflections/diffractions of signals. It presents major challenges of (1) selecting proper paths as the fingerprint and (2) comparing angles across multiple paths at different locations. The technique below creates fingerprints f_r as constant-sized vectors independent of the number of paths from a BS or their ordering or any other path characteristics (e.g., LoS vs. non LoS paths).

To compute f_r, we divide each plane (azimuth or zenith) in b bins such that the i-th bin, where $0 < i < (b-1)$, represents the range of angles from $\frac{360}{b} \times i$ to $\frac{360}{b} \times (i+1)$ in that plane. We construct the fingerprint $v\_azimuth = (v_1, v_2, ..., v_b)$, where v_i represents the total power received in the i-th bin for the azimuth angle. Each v_i in is defined as the sum of the power received along any path whose azimuth angle falls in the i-th bin. If no such paths exist, v_i is set to zero. Similarly, we construct the vector v_zenith for the zenith angles. Our preliminary fingerprint f_r is a concatenation of $v\_azimuth$ with v_zenith.

Unlike LTE, 5G also operates in millimeter wave frequencies that attenuate more easily resulting in a high variance of power. In our experiments, the variance leads to inaccurate fingerprints due to noise in the measurements. To mitigate the noise, we propose to discretize aggregate power in a bin into a binary value when building the fingerprint for each location. We define a threshold value t of the aggregate power in a bin. A value in the fingerprint vector f_r above the threshold t is set to 1, and below it set to 0. The default value for this threshold t is set to 0 based on the experiment in Section

[1] In dual connectivity, when both 5G and LTE are available, a UE is actively connected to both but preferentially uses the 5G radio for transmissions. When 5G is unavailable, the system falls back to an LTE-only mode.

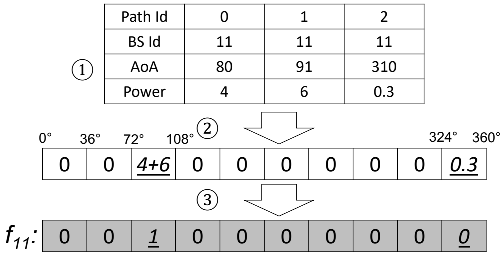


Fig. 3. Example of fingerprint construction for azimuth plane: 1. measure azimuth AoAs from BS 11; 2. fill power into bins based on AoAs for paths ($b = 10$); 3. discretize aggregate power into binary value as fingerprint f_{11}.

IV-B. This final step produces the fingerprint vector f_r. We empirically determine the value of parameters used by our approach (Section IV-B).

Fig. 3 shows an example of constructing a fingerprint for the azimuth angle only. The first step is to measure the azimuth angles of arrival for multiple paths from the serving base station $r = 11$ at location A where there are 3 measurable paths with different azimuth angles and power. The second step is to divide the plane for azimuth angles into $b = 10$ bins, for example, and fill the power of paths to corresponding bins. In the third step, we discretize the aggregate power of each bin into a binary value to output the fingerprint f_{11}.

Fingerprint matching: We match fingerprints by computing the distance among them as follows. Consider fingerprints F_1 and F_2 and the set of BSes R common to these fingerprints. If no BSes are common, i.e., R is null, then F_1 and F_2 have infinite distance among them. Otherwise, for each BS r in R, we compute the euclidean distance between the corresponding fingerprint vectors. Here, we depend on the our fingerprinting algorithm, which outputs uniform sized vectors as fingerprints. Finally, the distance between F_1 and F_2 is the sum of fingerprint distances for each BS r in R.

IV. Evaluation

We evaluate our localization technique using network simulations of urban environments constructed using real-world maps (Section IV-A). We first tune the parameters of our binning-based fingerprinting technique (Section IV-B) and compare it to other LTE and 5G fingerprinting techniques (Section IV-C, IV-D) in terms of their localization errors.

A. Experimental Setup

We use ns-3 to perform network-level simulations of cellular networks with dual connectivity of LTE and 5G mmWave radios. ns-3 mmWave module models several scenarios such as rural, urban, outdoor, and indoor [12]. We start with a scenario named Urban Macro, which simulates BSes located above roofs of buildings and UEs present in an outdoor environment. The probabilities of LoS and NLoS paths are set and paths with lower power are ignored according to 3GPP's recommendation [1]. 5G BSes are equipped with 64 (8×8) antennas with the height of 25m. UEs are equipped with 16 (4×4) antennas with the height of 1.6m. We simulate a UE moving linearly from the left edge to the right edge in each area, and recording a channel measurement every 0.5m. For each experiment, we repeat this process until 600×600 samples are collected in an area, which are equally divided between the training and test datasets.

We use three external data sources in ns-3 simulations. (1) We recreate the urban landscape in Atlanta, USA using the building location and geometry (length, breadth and height) from OpenStreetMap [3]. We randomly pick two $300m \times 300m$ areas referred to as AreaLo and AreaHi, which respectively have 1% and 35% building occupancy, i.e., the ratio of floor area of all buildings to the total area. (2) We add LTE BSes, known as eNodeBs, at the actual eNodeB locations for a major carrier in the US. AreaLo and AreaHi covered by 1 eNodeB and 3 eNodeBs respectively. (3) Since 5G BSes with mmWave are in early stages of deployment, we consider locations that are co-located with existing poles (a pole is a potential deployment site) and place 5G mmWave BSes with an equal spacing of 100m in x- and y-dimensions.

B. Configuring Binning-Based Technique

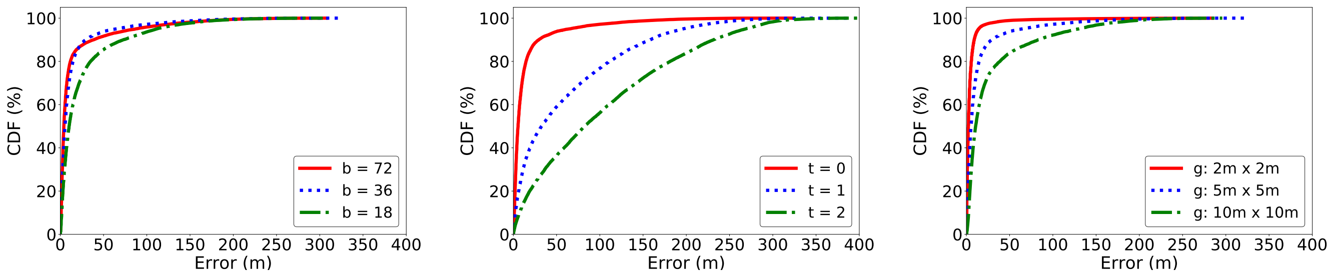
To choose the parameters of our binning-based technique, we evaluate the sensitivity of each parameter's values on localization error, while keeping the other parameters at their default values of $b = 36, t = 0, g = 2m \times 2m, s = 5$. Figure 4 presents the CDFs of localization errors for these experiments for AreaHi. We have similar findings for AreaLo.

Number of bins: A greater number of bins b improves the resolution and can result in unique fingerprints for each location. But, more bins could also make the fingerprints more susceptible to noise due to variations in angle at the same location. We experiment by setting the number of bins b to 72, 36, and 18, which correspond to an angular range of 5°, 10° and 20° respectively. Figure 4(a) shows that 36 bins and 72 bins have a smaller median error (4.8m) than 18 bins (10.2m), and 72 bins has a higher error than 36 bins at the tail. Thus, we pick 36 as the number of bins.

Threshold to discretize power: Figure 4(b) shows that the median localization errors for $t = 0$, $t = 1$ and $t = 2$ are 5.5m, 32.6m and 82.4m respectively. Thus, we select $t = 0$.

Grid size: We experiment with grid sizes g of $2m \times 2m, 5m \times 5m$ and $10m \times 10m$. Location samples per grid s is proportional to the grid size. Figure 4(c) shows that median localization error decreases from 10.7m to 5.5m and 2.3m when the grid size decreases from $10m \times 10m$ to $5m \times 5m$ and $2m \times 2m$. In practice, training data comes from GPS, which typically achieves an accuracy of 5m [19]. Hence, we present results for the $5m \times 5m$ grid size in later experiments. We note that a smaller grid size of $2m \times 2m$ improves accuracy for all techniques but does not alter the relative ordering among them.

Number of samples: While the above parameters are internal to our binning-based localization, the number of samples is an external parameter that affects the overhead of training data collection in our simulations as well as in practice. We experiment by setting the number of sampled locations per grid s for training to 2, 5, and 10 for a grid size of



(a) Number of bins (b) Threshold (c) Grid size

Fig. 4. Configuring parameters of the binning-based localization in AreaHi.

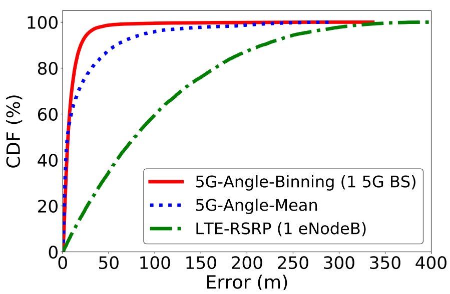


Fig. 5. Localization error in AreaLo (1 BS)

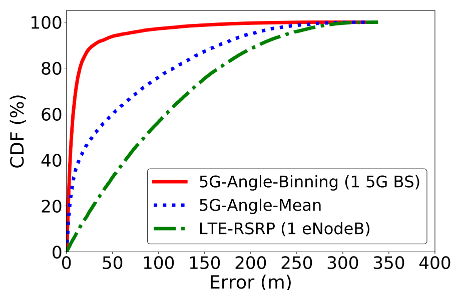


Fig. 6. Localization error in AreaHi (1 BS)

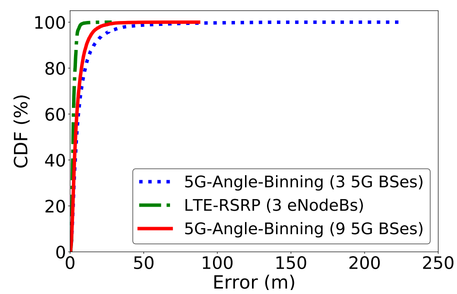


Fig. 7. Localization error in AreaHi (multiple BSes)

$5m \times 5m$. We find that 5 and 10 samples per grid have a similar median error as well as average error (median: 5.0m; average: 13.4m), both smaller than those of 2 samples (median: 12.0m; average: 23.7m). Because of the higher overhead of collecting 10 samples per grid, we choose 5 samples for $5m \times 5m$ grids.

C. Lower Density Area

We compare our binning technique, referred to as **5G-Angle-Binning** against two techniques. **5G-Angle-Mean** is a baseline that uses the average of azimuth angles and the average of zenith angles across all paths received from the serving BS as the fingerprint. It helps us quantify the benefit of our binning-based technique over simply using the mean angle as the fingerprint. **LTE-RSRP** uses RSRP measurements for the serving LTE BS and neighboring BSes similar to Margolies et al [11]. In the following description, parentheses after a technique's name shows the type and the number of BSes whose signals are used for fingerprinting.

We first show results for AreaLo where channel measurements from the serving LTE eNodeB or the serving 5G BS are used for localization. Comparing 5G-Angle-Binning (1 5G BS) with LTE-RSRP (1 eNodeB) in Figure 5, their median errors are 5.8m and 78.2m respectively. The reason LTE-RSRP (1 eNodeB) has a higher error is because signal strength is a directionally insensitive metric. Thus, localization errors are high when RSRP from only one eNodeB can be measured. But, a binning-based approach leverages multipath propagation due to physical objects (*e.g.,* buildings) in an outdoor environment. In this experiment, ns-3 reports 7.5 paths on average from the 5G BS to each location. These paths help create unique angle-based fingerprints across grids, thereby improving the accuracy of 5G-Angle-Binning (1 5G BS).

How does our binning-based fingerprinting compare to a simple angle-base fingerprinting? In Figure 5, the median error of 5G-Angle-Binning (1 5G BS) (5.8m) is close to the median error of 5G-Angle-Mean (5.1m) but 5G-Angle-Binning (1 5G BS) has a much smaller average error (9.5m) than 5G-Angle-Mean (21.1m). This is because taking the average of of the AoA's from different paths loses path-specific angle information while the binning-based technique preserves it in the form of unique fingerprints.

D. Higher Density Area

Figure 6 shows results from AreaHi using channel measuring from the serving BS. 5G-Angle-Binning (1 5G BS) achieves a median error of 5.5m and a mean error of 14.2m, which is similar to its results in the lower density area. While a binning-based fingerprinting uses multipath to its advantage, a higher density area which creates additional paths (19.0 signal paths on average in this experiment) does not necessarily improve its accuracy. 5G-Angle-Mean performs worse in a higher density area and its median error increases to 28.0m, which shows the value of our binning-based fingerprinting over simple techniques for angle-based fingerprinting. LTE-RSRP (1 eNodeB) still has a high median localization error of 80.0m, which shows the advantage of our binning-based technique when only 1 BS is available.

Figure 7 shows results from experiments in AreaHi but using channel measurements from multiple BSes. 5G-Angle-Binning (3 5G BSes) and 5G-Angle-Binning (9 5G BSes) use angle measurements from three neighboring 5G BSes or all nine 5G BSes in AreaHi to construct the fingerprint. LTE-RSRP (3 eNodeBs) considers RSRP measurements from all three eNodeBs present in AreaHi.

In Figure 7, the median (mean) localization errors of LTE-RSRP (3 eNodeBs), 5G-Angle-Binning (9 5G BSes) and then by 5G-Angle-Binning (3 5G BSes) are 2.0m (2.4m), 3.7m (5.3m) and 4.4m (7.7m) respectively. While all techniques achieve low localization errors comparable to our grid dimensions of $5m \times 5m$, LTE-RSRP achieves better results than 5G-Angle-Binning in this experiment. One explanation is that the RSRP measurements are more stable than angle measurements, which are affected more easily by the changing environment. Multiple angle measurements at short time intervals may help improve the robustness of binning-based fingerprinting.

Next, we compare the performance of localization schemes using multiple BSes against the previous experiment using 1 BS only. Comparing Figure 7 with Figure 6, we find that both LTE-RSRP (3 eNodeBs) and 5G-Angle-Binning (3 5G BSes) substantially improve their accuracy over LTE-RSRP (1 eNodeB) and 5G-Angle-Binning (1 5G BS) respectively. Thus, both schemes benefit from a trilateration-like effect as they consider measurements from three base stations. While 5G-Angle-Binning performs better with 1 BS, LTE-RSRP performs better with multiple BSes. Based on this result, it may be useful to explore a hybrid of angle-based and RSRP-based localization based on the density of BS deployments.

V. Conclusions and future work

We explored the use of angle-based measurements for UE localization in 5G. Our binning-based fingerprinting technique used angle measurements and received power from the serving base station as well as neighboring base stations across multiple paths. Using experiments for a major city and BS locations of a tier-1 carrier in the US, we showed that (1) our 5G binning-based localization using angle measurements from 1 5G BS outperforms LTE localization technique using RSRP measurements from 1 eNodeB in both lower density and higher density areas; (2) multiple base stations improve the accuracy of both LTE RSRP-based and our 5G binning-based localization because of a trilateration-like effect, which results in comparable accuracy of the two techniques.

The accuracy of angle-based localization could be improved, especially in dense urban environments by collecting and using *multiple measurements at short time intervals* for mobile UEs, and further by exploring a *hybrid of RSRP-based and angle-based techniques*. A longer-term challenge is to build a system for angle-based localization in 5G. To that end, first, we have to extend software such as MobileInsight [10] with *techniques to collect angle measurements* at UEs. Next, the azimuth and zenith angles are measured relative to the direction of the UE's antenna array, which depends on UE's orientation. Sensors embedded on a UE (e.g., gyroscope) can help with *derivation of absolute azimuth/zenith angles* in the global coordinate system. Finally, we need to quantify *trade-off between location accuracy and the volume of data collected* so that a localization service to collect and analyze measurements can scale of billions of 5G devices.

References

[1] 3gpp protocol rel. 15. https://www.3gpp.org/release-15, 2019.

[2] Enhanced 9-1-1. https://en.wikipedia.org/wiki/Enhanced_9-1-1, 2019.

[3] Openstreetmap. http://www.openstreetmap.org, 2019.

[4] Paramvir Bahl, Venkata N Padmanabhan, Victor Bahl, and Venkat Padmanabhan. Radar: An in-building rf-based user location and tracking system. 2000.

[5] Ayon Chakraborty, Luis E Ortiz, and Samir R Das. Network-side positioning of cellular-band devices with minimal effort. In *INFOCOM*, pages 2767–2775. IEEE, 2015.

[6] Ahlam Ben Cheikh, Mouna Ayari, Rami Langar, Guy Pujolle, and Leila Azouz Saidane. Optimized handoff with mobility prediction scheme using hmm for femtocell networks. In *ICC*, pages 3448–3453. IEEE, 2015.

[7] Michelle M. Do. Lte: Tracking area (ta) and tracking area update (tau). https://www.netmanias.com/en/post/blog/5930/lte-tau/lte-tracking-area-ta-and-tracking-area-update-tau, 2019.

[8] Mohamed Ibrahim and Moustafa Youssef. Cellsense: An accurate energy-efficient gsm positioning system. *IEEE Trans. on Vehicular Technology*, 61(1):286–296, 2011.

[9] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. Spotfi: Decimeter level localization using wifi. In *SIGCOMM*, volume 45, pages 269–282. ACM, 2015.

[10] Yuanjie Li, Chunyi Peng, Zengwen Yuan, Jiayao Li, Haotian Deng, and Tao Wang. Mobileinsight: Extracting and analyzing cellular network information on smartphones. In *MOBICOM*, pages 202–215. ACM, 2016.

[11] Robert Margolies, Richard Becker, Simon Byers, Supratim Deb, Rittwik Jana, Simon Urbanek, and Chris Volinsky. Can you find me now? evaluation of network-based localization in a 4g lte network. In *INFOCOM*, pages 1–9. IEEE, 2017.

[12] Marco Mezzavilla, Menglei Zhang, Michele Polese, Russell Ford, Sourjya Dutta, Sundeep Rangan, and Michele Zorzi. End-to-end simulation of 5g mmwave networks. *IEEE Communications Surveys & Tutorials*, 20(3):2237–2263, 2018.

[13] Avik Ray, Supratim Deb, and Pantelis Monogioudis. Localization of lte measurement records with missing information. In *INFOCOM*, pages 1–9. IEEE, 2016.

[14] Richard Roy and Thomas Kailath. Esprit-estimation of signal parameters via rotational invariance techniques. *IEEE Trans. on acoustics, speech, and signal processing*, 37(7):984–995, 1989.

[15] Andreas Savvides, Chih-Chieh Han, and Mani B Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *MOBICOM*, pages 166–179. ACM, 2001.

[16] Ralph Schmidt. Multiple emitter location and signal parameter estimation. *IEEE Trans. Antennas Propag.*, 34(3):276–280, 1986.

[17] Souvik Sen, Jeongkeun Lee, Kyu-Han Kim, and Paul Congdon. Avoiding multipath to revive inbuilding wifi localization. In *MOBISYS*, pages 249–262. ACM, 2013.

[18] Adam Smith, Hari Balakrishnan, Michel Goraczko, and Nissanka Priyantha. Tracking moving devices with the cricket location system. In *MOBICOM*, pages 190–202. ACM, 2004.

[19] Frank van Diggelen and Per Enge. The worlds first gps mooc and worldwide laboratory using smartphones. In *Proceedings of the 28th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2015)*, pages 361–369, 2015.

[20] Fuxi Wen, Henk Wymeersch, Bile Peng, Wee Peng Tay, Hing Cheung So, and Diange Yang. A survey on 5g massive mimo localization. *Digital Signal Processing*, 2019.

[21] Yaxiong Xie, Zhenjiang Li, and Mo Li. Precise power delay profiling with commodity wi-fi. *IEEE Trans. on Mobile Computing*, 18(6):1342–1355, 2018.

[22] Jie Xiong and Kyle Jamieson. Arraytrack: A fine-grained indoor location system. In *NSDI*, pages 71–84, 2013.