User Localization using Random Access Channel Signals in LTE Networks with Massive MIMO

Aleksei Fedorov, Haibo Zhang, Yawen Chen

Department of Computer Science, University of Otago, Dunedin 9016, New Zealand,

Emails: {aleksei, haibo, yawen}@cs.otago.ac.nz

***Abstract*—Recent studies show that real-time precise user localization enables to deliver accurate beamforming in MIMO systems without the need for channel estimation. This paper presents new solutions for accurate user localization in massive MIMO LTE systems. A key novelty of the developed schemes is the ability to locate users during LTE's random access channel synchronization procedure before they are connected to the network, by which the obtained location information can be immediately used to optimize the allocation of radio resource and perform accurate beamforming. To achieve this, the developed solutions leverage the advantages of spherical wave propagation since it allows simultaneously estimating the angle of arrival and the propagation distance from the user equipment to each antenna element in the base station. We design solutions for both single-path line-of-sight communication and multi-path propagation environments. The developed schemes were evaluated through both simulations and proof-of-concept experiments. Simulation results show that both algorithms can achieve decimeter-level localization accuracy using 64 and more antenna elements for the distances up to 300 meters. The proof-of-concept experiment justifies the feasibility of user localization based on the estimation of the shape of the incoming wavefront.**

***Index terms*—** User localization, random-access channel, spherical wave propagation, massive MIMO, phase noise

I. Introduction

Beamforming allows the creation of focused beams towards User Equipments (UEs), by which energy consumption and interference can be significantly reduced and radio resources can be reused to increase capacity [1]–[4]. In most existing beamforming schemes, beams are created based on the estimation of the Downlink (DL) channels via reference signals, which brings large overhead to DL data communications. For example, to maintain 25 UEs, the per-antenna reference signals used to measure the DL channels for a Base Station (BS) with 100 antenna elements consume more than 50% of the traffic generated by the BS [5]. Recently, it was demonstrated in [1] that, with information on UE locations, accurate beamforming can be performed without any channel feedback overhead. Hence, it is worth developing accurate UE localization schemes to support efficient beamforming in massive Multiple Input Multiple Output (MIMO) systems.

Limitations of existing works: Existing GPS-based solutions cannot provide precise locations for accurate beamforming using the commodity mobile devices. Moreover, the location information is available at the user side instead of the BS. To use location information for beamforming, the BS has to frequently pull it for the UEs. Several schemes [1], [6] have been proposed to locate UEs using LTE's Uplink (UL) signals based on the reference symbols carried in data communication. However, such schemes can locate UEs after radio resources have been allocated. If UEs can be located before radio resource allocation, the location information can be immediately used to optimize resource allocation and beamforming. Another limitation of existing schemes is lack of consideration for phase noise caused by non-ideal synchronization between antenna elements, which can significantly deteriorate the accuracy of UE localization [7].

Proposed approach: We focus on developing efficient solutions to localize users in areas with high population density (e.g. urban areas in business time and airports), where it is challenging to provide high-quality mobile communication due to the need to serve a large number of UEs using limited radio resources. Such areas are typically covered by many small cells with distances between adjacent BSs less than a few hundred meters [8], [9]. In such scenarios, the Spherical Wave Propagation (SWP) model can be adopted to locate UEs more accurately in massive MIMO systems because the linear dimensions of a massive MIMO array are large enough to distinguish the spherical shapes of the incoming wavefronts. Fig. 1 compares the SWP model with the conventional Plane Wave Propagation (PWP) model. Experiments conducted at the Universities of Bristol and Lund using massive MIMO prototypes have confirmed the necessity to use spherical propagation in the massive MIMO procedures [2], [4].

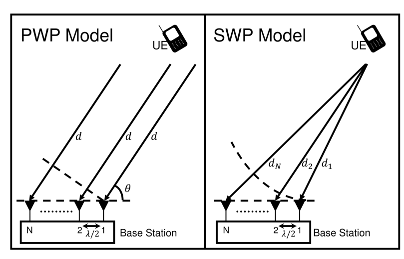


Fig. 1. All paths from UE antenna to BS's antenna elements cover the same distance with the same angle of arrival in (a), but cover different distances and have different angles of arrivals in (b).

In this work, we propose SWP-based solutions that use the Randon Access Channel (RACH) signals in Long Term Evolution (LTE) networks to locate UEs. In LTE, the communication between a UE and a BS starts from RACH synchronization where the UE broadcasts special signals to show the intention to connect to the network. Since UE locations are obtained based on RACH signals, our schemes enable the BS to get the location of a connecting UE before allocating radio resource to it, thereby enabling the use of UE locations to optimize radio resource allocation and perform accurate beamforming.

Challenges and our solutions: The first challenge is to accurately estimate the distance between each element in the massive MIMO antenna array and the UE without the need of precise time synchronization between UEs and the BS. Based on SWP, the difference in time delay experienced at different antenna elements can be described through small phase shifts between antenna measurements, as illustrated in Fig. 1(b). In case there is a single dominant Line-of-Sight (LoS) path to each antenna element, the phase shifts can be obtained by analyzing the angles of the RACH correlation spikes that are already computed during the RACH procedure. In case there are multiple communication paths, the proposed scheme leverages the Orthogonal Frequency Division Multiplexing (OFDM) nature of RACH signals to obtain more measurements for joint estimation of the shapes of all the incoming wavefronts via nonlinear data-fitting approach.

The second challenge is to deal with the phase noise caused by non-ideal synchronization between massive MIMO antenna elements. Even though all antenna elements at a BS are synchronized using a reference clock [3], there are still small phase deviations which can have a big impact on the estimation of the wavefront of the incoming signals. Using our testbed with two Ettus USRPs N210 and one 10 MHz reference NI OctoClock, we measure the phase noise in angle estimation of the RACH correlation spikes. We observed that the phase noise cannot be simply approximated by Gaussian noise. We define statistical properties of the noise distribution and use the system identification approach to deal with such phase noise.

Contributions: To the best of our knowledge, the proposed schemes are the first to locate users through phase shift estimation from LTE RACH synchronization based on the more realistic spherical-wave propagation model. Simulation results show that the single-path solution can provide decimeter-level localization accuracy for massive MIMO with 64 or more antenna elements within the region of 100 meters and sub-meter-level localization accuracy for massive MIMO with 80 or more elements up to 300 meters. For the multipath solution, the same results can be achieved using massive MIMO with no less than 48 antenna elements. We have implemented the single-path solution on the testbed by emulating MIMO systems with 8, 12 and 16 antenna elements. The results of the proof-of-concept experiments justify the feasibility of the proposed approach.

II. SWP-based Channel Modeling

As illustrated in Fig. 2, we assume that an LTE BS is equipped with a massive MIMO antenna with N spatially separated antenna elements Elm_i $(i = 1, 2, \cdots, N)$. Suppose the LTE network has an operating frequency $\mathbf{F}$ and a sampling duration Δt. To broadcast an uplink signal $s(t)$, a UE emits an electromagnetic wave $e^{\mathbf{j}2\pi\mathbf{F}t}$ [10] to carry the symbols to be transmitted as follows: $s(t) = \sum_{m=1}^{M} b_m(t)\, e^{\mathbf{j}2\pi\mathbf{F}t}$, where symbol $b_m(t)$ is nonzero in the period $[(m-1)\Delta t, m\Delta t]$, and 0 in other periods. M is the number of transmitted symbols.

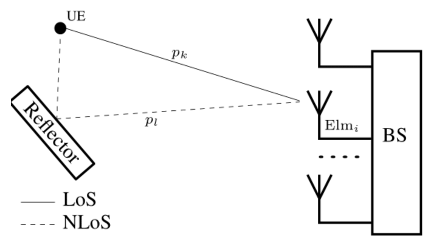


Fig. 2. Communication between a UE and an LTE BS with massive MIMO.

Considering a single path p_j from the UE to antenna element Elm_i, we use d_{ij} to represent the distance that path p_j traverses. All the symbols received at Elm_i along path p_j are delayed by $t_{ij} = d_{ij}/c$ where c is the speed of light. Let $s'_{ij}(t)$ be the signal received at Elm_i along path p_j as follows:

$$s'_{ij}(t) = a_{ij} \sum_{m=1}^{M} b_m(t - t_{ij})\, e^{\mathbf{j}2\pi\mathbf{F}(t-t_{ij})} + \eta_i(t), \qquad (1)$$

where a_{ij} is the path attenuation, and $\eta_i(t)$ is the noise. We define $a_{ij} = f(d_{ij}, \mathbf{F}, \mathrm{Env})$, indicating that path attenuation depends on not only the traveled distance and the carrier's frequency but also the propagation environment Env [11].

In a real environment, the radio signal may reach each antenna element along multiple paths due to signal reflection, scattering, diffraction and refraction, which is known as multipath propagation. Let $s'_i(t)$ be the signal received at Elm_i via multipath propagation, and L_i be the number of paths traversed by the signals received at Elm_i. $s'_i(t)$ can be modeled as

$$s'_i(t) = \sum_{j=1}^{L_i} a_{ij} s(t - t_{ij}) + \eta_i(t), \qquad (2)$$

where $t_{ij} = d_{ij}/c$ is the time delay to cover the distance d_{ij} along path j from UE to Elm_i.

In the following, we extend our model for multi-carrier signals. Let $s'_i(t, f_k)$ represent the signal received at Elm_i with frequency f_k, where $k \in [1, N_s]$ and N_s is the number of subcarriers. Then Eq. (2) can be extended for OFDM signals as follows:

$$\begin{pmatrix} s'_i(t,f_1) \\ s'_i(t,f_2) \\ \vdots \\ s'_i(t,f_{N_s}) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{L_i} a_{ij}(f_1) s_i(f_1, t - t_{ij}) \\ \sum_{j=1}^{L_i} a_{ij}(f_2) s_i(f_2, t - t_{ij}) \\ \vdots \\ \sum_{j=1}^{L_i} a_{ij}(f_{N_s}) s_i(f_{N_s}, t - t_{ij}) \end{pmatrix} + \begin{pmatrix} \eta_i(t,f_1) \\ \eta_i(t,f_2) \\ \vdots \\ \eta_i(t,f_{N_s}) \end{pmatrix}. \qquad (3)$$

While the single carrier approach has the limitation in closely relating a physical environment with the corresponding wireless channel due to the limited amount of measured information, the multi-carrier approach overcomes the drawback as the path attenuation $a_{ij}(f_k)$ depends on frequency. This dependence is vital in connecting the environment with the corresponding channel. In the following sections, we will show that this effect gives a significant benefit in UE localization.

III. Localization for the single LoS path case

The aim of our work is to localize LTE users at the BS side using UL signals, particularly the RACH signals. In this section, we explain the theory for the single path case. The solution for the multipath case will be presented in section IV.

A. Phase estimation

Let us start the derivation of the localization problem from the assumption of ideally synchronized antenna elements in the BS. We address the challenge stemming from non-ideal synchronization in section III-C.

In the case of a single path and RACH signals, the notation a_{ij} becomes a_i, t_{ij} becomes t_i and the symbols b_m become RACH symbols in Eq. (1). To recover each received symbol b_m, the BS removes the carrier wave $e^{\mathbf{j}2\pi\mathbf{F}t}$. Then the symbols received at Elm_i in Eq (2) can be represented as follows:

$$s_i''(t) = \frac{s_i'(t)}{e^{j2\pi\mathbf{F}t}} = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} \sum_{m=1}^{M} b_m(t - t_i) + \xi_i(t), \quad (4)$$

where $\xi_i(t)$ is a modified noise. As can be seen from Eq. (4), the channel change (i.e. $a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i}$ in Eq. (4)) is also reflected by t_i, which can be directly measured by phase shift. Our idea is to estimate the t_i through phase shift of the channel change.

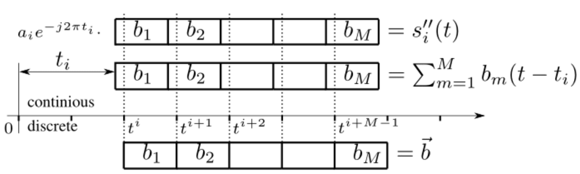


Fig. 3. Illustration of signal shifting in continuous and discrete time domains.

A key challenge here is to retrieve the phase shift from the incoming signal in the digital domain. As illustrated in Fig. (3), if we simply take the scalar product of the incoming signal $s_i''(t)$ with the one shifted by t_i symbols $\sum_{m=1}^{M} b_m(t - t_i)$, we could obtain the pure channel change h_i'':

$$h_i'' = \frac{1}{||b||^2}(s_i''(t), \sum_{m=1}^{M} b_m(t - t_i)) = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} + \varsigma_i, \quad (5)$$

where the notation $(*, *)$ means scalar product, $||b||$ is the norm of vector $\vec{b} = (b_1, b_2, .., b_M)$, and ς_i is the modified noise. The phase shift of $s_i''(t)$, denoted by φ_i, is simply the argument of the channel change since the attenuation coefficient a_i for a LoS path is a real number, i.e.,

$$\varphi_i = -\arg(h_i'') = (2\pi\mathbf{F}t_i + \delta\varphi_i) \bmod 2\pi, \quad (6)$$

where $\delta\varphi_i$ is noise caused by the modified noise, mod is the Modulo operator. However, we do not know the exact value of t_i. Thus, we estimate t_i based on the discrete measurements from antenna elements during RACH synchronization procedure. Suppose the synchronization is performed with a sampling period of Δt. The BS can measure an incoming signal only in discrete time at $t^l = l\Delta t$ as follows:

$$s_i''(t^l) = \frac{s_i'(t^l)}{e^{j2\pi\mathbf{F}t^l}} = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} \sum_{m=1}^{M} b_m(t^l - t_i) + \xi_i(t^l). \quad (7)$$

As illustrated in Fig. 3, the shifted symbol $b_m(t^l - t_i) = b_m$ if $t^l \in [(m-1)\Delta t + t_i, m\Delta t + t_i]$. Accordingly, starting from the time moment $t^i = \Delta t\lceil \frac{t_i}{\Delta t} \rceil \in [t_i, \Delta t + t_i]$ at which $\sum_{m=1}^{M} b_m(t^i - t_i) = b_1$, antenna element Elm_i measures the values that contain useful signal as follows:

$$\begin{aligned} t^i, \quad & s_i''(t^i) = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} b_1 + \xi_i(t^i); \\ t^{i+1}, \quad & s_i''(t^{i+1}) = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} b_2 + \xi_i(t^{i+1}); \\ \dots \quad & \dots \\ t^{i+M-1}, \quad & s_i''(t^{i+M-1}) = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} b_M + \xi_i(t^{i+M-1}). \end{aligned} \quad (8)$$

During all previous moments t^l before the moment t^i, Elm_i measures noise $s_i''(t^l) = \xi_i(t^l)$ as no symbol is sent. The received signal can also be written using vector representation:

$$\vec{s}_i = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i} (0, \dots, 0, b_1, \dots, b_M) + \vec{\xi}_i. \quad (9)$$

In order to calculate scalar product in Eq. (5), the BS needs to shift symbols $\sum_{k=1}^{M} b_m(t)$, i.e. the RACH symbols vector $\vec{b} = (b_1, b_2, .., b_M)$, by $\lceil \frac{t_i}{\Delta t} \rceil$ integer steps in discrete time and calculates the scalar product with $\vec{s}_i$.

In this way, the BS can measure the channel change at each antenna element and estimate phases of the incoming signals. Fortunately, the RACH synchronization procedure calculates a correlation vector between the incoming signal with the discrete shifted RACH vector, which is exactly the same operation as the scalar product in Eq. (5) [12]. Once a shift is the proper shift as in Eq. (9), a spike occurs in the correlation vector, and the BS can then measure the argument of the spiking element and estimate the phase of the incoming signal according to Eq. (6). This means that our scheme can take the values of correlation spikes directly from the RACH procedure and, consequently, it does not introduce additional complexity in the correlation spikes calculation.

The main issue of the phase estimation is that the argument of the spiking element can only be measured in modulus 2π, which adds ambiguity since the quotient (i.e. how many 2π's in the phase shift) is unknown. The following presents a phase sorting scheme to overcome this issue. We assume that the coordinates of each antenna element relative to the position of the MIMO antenna array are precisely known and the distance between any two neighboring elements is no larger than a half of the wavelength $\lambda/2$ where $\lambda = c/\mathbf{F}$ [10]. This guarantees that the difference in phase changes of the received signals between two neighboring antenna elements is no larger than π. Consequently, for any two neighboring antenna elements, the signal with the smallest phase can be always found except in the situation where the difference is equal to π. This case is not considered because in practice, such situation is very unlikely since a BS maintains a particular area, which cancels situations with phase shifts close to π radians. The influence of noise $\delta\varphi_i$ can also be neglected in the phase sorting scheme since even in the situation with zero SNR RACH signals, the standard deviation is less than 0.03 radians. Hence, for any two neighboring antenna elements, the signal with smaller phase can be always found based on the following two rules: if $|\varphi_{i+1} - \varphi_i| < \pi$, the smaller one remains to be smaller than the bigger one; if $|\varphi_{i+1} - \varphi_i| > \pi$, the smaller one becomes bigger since the difference between them cannot be bigger than π, and 2π should be added to the smaller phase.

To compute the actual phase for the signal received at each antenna element, we need to find the minimum phase for the signals received at all antenna elements, which can be done by performing a pairwise comparison between neighbouring antenna elements based on the above two rules. Suppose the signal received at antenna element Elm_i has the minimum phase φ_i. For each neighbour of Elm_i denoted by Elm_j, if $|\varphi_j - \varphi_i| \leq \pi$, φ_j remains unchanged, otherwise $\varphi_k = \varphi_k + 2\pi$ for any Elm_k in the direction from Elm_i to Elm_j. We repeat the same operation for the neighbours of Elm_j and so on until all φ_is have been corrected.

B. LoS localization during RACH synchronization

Because of the use of SWP, each phase shift φ_i corresponds to a certain distance $R_i = \lambda \times \frac{\varphi_i}{2\pi}$. As shown in Fig. 4, for

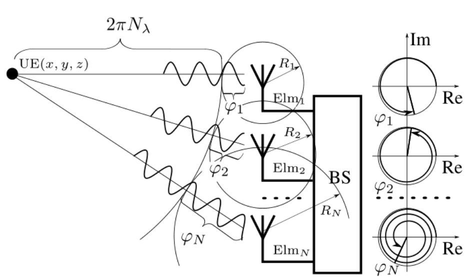


Fig. 4. Phase shift at antenna elements alongside the antenna array.

each Elm_i, we draw a sphere centered at Elm_i with radius of R_i. We draw a sphere centred at the UE with radius of $R = 2\pi N_\lambda$ so that this sphere is tangent to each sphere centered at Elm_i where $i \in [1, N]$. It can be seen that the LoS distance from the UE to antenna element Elm_i can be rewritten by $d_i = R + R_i, i = 1, \ldots, N$. By representing d_i with the coordinates of the UE (x, y, z) and Elm_i (x_i, y_i, z_i), we have

$$\sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} = R + R_i. \tag{10}$$

To localize the UE, the BS needs to jointly estimate the UE's coordinates and the common parameter N_λ. Since the number of unknown parameters is four (x, y, z, R), the coordinates of the UE can be calculated if there are no less than 4 antenna elements, which is not a problem for BS with Massive MIMO [2], [4]. Once the BS has enough antenna elements, the above formulated localization problem transforms to the classical GNSS positioning problem that can be solved using the Bancroft's algorithm [13].

C. Combating with phase noise

To understand how big is the phase noise between antenna elements in massive MIMO, we conduct experiments with two Ettus USRPs N210 synchronized via a NI OctoClock-G. One USRP periodically sends RACH signals to the other USRP that calculates correlation between the incoming and local signals and measures the phase of a correlation spike as in Eq. (6). The testbed is operating with a carrier frequency of 2.6 GHz and a sampling rate of 5.12 MS/s. We connect the two antenna ports with a 1-meter long SMA-SMA cable to minimize wireless channel effects and guarantee a constant distance between the transmitter and receiver. We run around 2900 rounds to measure the phase shifts.

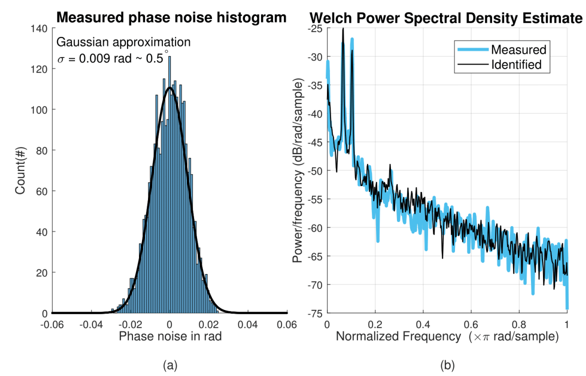


Fig. 5. (a) Histogram of the measured phase noise; (b) Power Spectral Density of the measured phase noise.

As illustrated in Fig. 5(a), the phase noise is too small to have a big impact on the phase sorting. However, it cannot be ignored for the estimation of phase shift which has a big impact on the localization accuracy. Fig. 5(b) shows the phase noise spectral density that has a number of significant spikes. In the presence of such phase noise, the estimated phase after sorting can be represented as follows:

$$\varphi_i' = \varphi_i + \Delta\varphi_i + \delta\varphi_i, \tag{11}$$

where $\delta\varphi_i$ comes from the modified noise in Eq. (5) and has Gaussian noise characteristics, while $\Delta\varphi_i$ is the phase noise that has to be estimated during the localization procedure.

To take into account the phase noise, we model the phase noise as a response of a state space model to white noise [14]:

$$\begin{aligned} \eta_{i+1} &= A\eta_i + Ke_i, \\ y_i &= C\eta_i + e_i, \end{aligned} \tag{12}$$

where matrices A, K, C define the model, y_i is the output that has the same statistical properties as $\Delta\varphi_i$, e_i is the disturbance of the model that has white noise properties and η_i is the vector of the model's states. In our experiments, the best number of states is 6. The identified process y_i is illustrated in black line in Fig. 5 (b). In order to retrieve the pure φ_i from Eq. (11), we use Kalman filter approach where φ_i's are measurements and the state space model given in Eq. (12) is the filter's dynamic part [15]. The output of Bancroft's algorithm is used as the initialization for the Kalman filter. After the filtering, the output of the Kalman filter (i.e. φ_is) is put back to Bancroft's algorithm to compute the refined UE location.

D. Eliminating CFO and initial phase offset

There are always a Carrier Frequency Offset (CFO) $\delta\mathbf{F}$ and an initial phase offset ϕ that are caused by independent work of local oscillators of a UE and a BS. This non-ideality can be counted at the BS side in Eq. (7) as follows:

$$s_i''(t^l) = \frac{s_i'(t^l)}{e^{\mathbf{j}\left[2\pi(\mathbf{F}-\delta\mathbf{F})t^l-\phi\right]}} = \\ = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i}\left[e^{\mathbf{j}\phi}\sum_{m=1}^{M} b_m(t^l-t_i)e^{\mathbf{j}2\pi\delta\mathbf{F}\,t^l}\right] + \xi_i(t^l). \quad (13)$$

In the same way as in Eq. (8), the useful signal starts to reach Elm_i at moment t^i, and the vector representation of the received signal given in Eq. (9) can be rewritten as follows:

$$\vec{s}_i = K_i e^{\mathbf{j}\phi}\left(0,\ldots,0,b_1\mathrm{f}^i,\ldots,b_M\mathrm{f}^{i+M-1}\right) + \vec{\xi}_i, \quad (14)$$

where $\mathrm{f}^i = e^{\mathbf{j}2\pi\delta\mathbf{F}\,t^i}$ and $K_i = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i}$. Hence, the spiking value in the correlation vector between the incoming signal and RACH preamble vector $\vec{b}$ can be represented as:

$$h_i' = a_i e^{-\mathbf{j}2\pi\mathbf{F}t_i}\left[e^{\mathbf{j}\phi}\frac{1}{\|b\|^2}\sum_{m=1}^{M} f^{i+m-1}\right] + \varsigma_i. \quad (15)$$

The CFO impact, inside of square brackets in Eq. (15), depends on the starting moment t^i, which can be different for different antenna elements. However, in LTE RACH synchronization, the maximum difference is no more than one sample, i.e. for any two antenna elements $\mathrm{Elm}_i, \mathrm{Elm}_j$, the difference in the first receiving moment $|t^i - t^j| \leq \Delta t$ where Δt is the length of the sampling period. This is because the sampling rate of RACH preamble vector $\vec{b}$ is 1.28 MHz, which is 24 times smaller than LTE conventional sampling rate 30.72 MHz. Hence, to make it possible for the situation when $|t^i - t^{i_2}| > \Delta t$, the size of a massive MIMO antenna has to be bigger than $\frac{3\cdot 10^8 m/s}{1.28MHz} \approx 234$ meters.

In case that $|t^i - t^j| = \Delta t$, we take the moment (t^i or t^j) for which the maximum number of antenna elements have spiking values. In this way, all elements of the massive MIMO antenna obtain the same impact from CFO and phase shift provided that all antenna elements are well-synchronized [2]. In the same way, we can estimate the phases of the incoming signals at different antenna elements. All spiking values are divided by the spiking value with the minimum phase as follows:

$$h_i'' = \frac{h_i'}{h_*'} = a_i e^{-\mathbf{j}(2\pi\mathbf{F}t_i - \varphi^*)} + \nu_i, \quad (16)$$

where h_*' is the spiking value with the minimum phase φ^*, and ν_i is the modified noise. Let r^* be the radius that corresponds to φ^*. From Eq. (16), it is well seen that h_i'' has a phase shift relative to φ^*. It means that the relative phase shift for the antenna element with φ^* becomes zero and its region has a zero radius, whereas the radii of the rest regions are reduced by r^*. Consequently, the radius of the common sphere centered at the UE is increased on r^*. The localization problem now can be rewritten as follows:

$$\sqrt{(x-x_i)^2+(y-y_i)^2+(z-z_i)^2} = R + r^* + (r_i - r^*), \quad (17)$$

and can be solved in the same way as Eq. (10). Please note, the operation in Eq. (16) change the noise properties in Eq. (11), however, the model in Eq. (12) stays the same except the doubled variance of the disturbance e_i.

IV. Localization for the multipath case

For the jth path from UE to antenna element Elm_i, we can represent its attenuation coefficient a_{ij} in the form of a complex number as $a_{ij} = a_{ij} + b_{ij}i = r_{ij}e^{\mathbf{j}\theta_{ij}}$. Since the attenuation for a LoS path is usually considered as a free-space loss, its attenuation coefficient commonly has a real value, that is, $\theta_{ij} = 0$. This makes it possible for our solution to localize a UE owing to the unnecessity to estimate the attenuation coefficients since real valued attenuation does not introduce any phase rotation (θ_{ij}). However, the attenuation coefficients for multipath propagation are generally considered as complex values [16], and localization algorithm has to estimate these attenuation coefficients too. Hence, the parameters to be estimated include the UE's coordinates (x, y, z), the radius of the common sphere R, and the attenuation coefficients for all paths that are different for each antenna element. Suppose the total number of paths is L. The number of parameters to be estimated becomes $4 + LN$ that is larger than the number of antenna elements N, thus, the proposed single-path solution cannot be simply extended for the multipath case. In this section, we solve the localization problem for the multipath scenario by exploiting the OFDM nature of RACH signals.

Unlike the solution for the LoS path case, we analyze channel influence in the frequency domain, which makes it easier to understand the channel influence on OFDM signals. Our algorithm first constructs a model of the radio channel based on the known environment and then optimizes it based on OFDM measurements using the nonlinear data-fitting approach. Since RACH signals are OFDM based and the received signal is known due to RACH synchronization, the channel influence can be always estimated in the frequency domain.

A. Channel model in frequency domain

The frequency response of a multipath channel (Eq. (2)) at Elm_i, denoted by H_i, can be represented as follows [16]:

$$H_i = \sum_{j=1}^{L_i} a_{ij} e^{-\mathbf{j}2\pi\mathbf{F}t_{ij}}, \quad (18)$$

where L_i is the number of paths for UE to Elm_i, and t_{ij} is the time for the signal to traverse distance d_{ij} along path j.

At first, it is worth explaining how the Non-Line-of-Sight (NLoS) signals are originated. The transmitted signal during its propagation may interact with the objects in the environment. Once an interacted signal is received by BS, we call it as an NLoS signal. The interactions can be in general grouped into

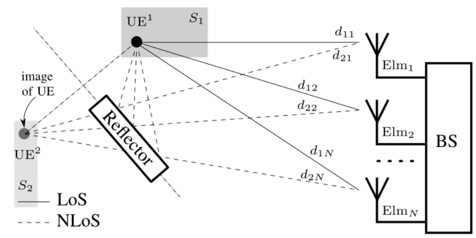


Fig. 6. Reception of multipath signal where S_1 and S_2 are search areas.

physical phenomena such as reflection, scattering, diffraction and refraction/penetration [11]. Regardless of the physical phenomena, NLoS signals cover different distances and have different angles of arrival. Consequently, from the BS perception, it looks like that the NLoS signals come from different sources. Let us call these sources as images of the original source as illustrated in Fig. 6, where the black circle is the real position of UE with coordinates UE^1 and the gray circle is the UE's image with coordinates UE^2.

The distance d_{ij} from $UE^j(x^j, y^j, z^j)$ to Elm_i is represented as an Euclidean distance: $d_{ij} = \|\mathrm{Elm}_i - \mathrm{UE}^j\|$. The attenuation coefficient $a_{ij} = f(d_{ij}, \mathbf{F}, \mathrm{Env})$ is a function of distance d_{ij}, frequency and the physical properties of the interacting objects:

$$a_{ij} = \frac{c^2}{(4\pi\mathbf{F})^2} \frac{\Gamma_j(\mathbf{F}, \mathrm{Elm}_i, \mathrm{UE}^j, \mathrm{Env})}{\|\mathrm{Elm}_i - \mathrm{UE}^j\|}, \tag{19}$$

where $\Gamma_j = C_j \cdot g(\mathbf{F}, \mathrm{Elm}_i, \mathrm{UE}^j, \mathrm{Env})$ is the Fresnel coefficient, which is a combination of constant C_j uniquely defined by path j, and a function g of carrier's frequency, the positions of transmitter and receiver, and physical properties of the interacting objects [11], [17]. To simplify the model, we use $\Gamma_j = C_j$ as constant coefficients that depends on the physical properties of the objects. Note that, for LoS path, $\Gamma_1 = 1$.

The model of a multipath channel given by Eq. (18) can then be refined by incorporating Eq. (19) as follows:

$$H_i = \sum_{j=1}^{L_i} \left[\frac{c^2 \Gamma_j}{(4\pi\mathbf{F})^2} \frac{1}{\|\mathrm{Elm}_i - \mathrm{UE}^j\|^2} \right] e^{-\mathbf{j}2\pi \frac{\mathbf{F}}{c} \|\mathrm{Elm}_i - \mathrm{UE}^j\|}. \tag{20}$$

This is a system of N equations $i = 1, \ldots, N$ as the antenna array has N elements. Since the number of unknown parameters (Γ_j and UE^j) is bigger than N, we expand it by exploiting the OFDM nature of RACH signals as follows:

$$\vec{H_i} = \begin{pmatrix} H_{i1} \\ H_{i2} \\ \vdots \\ H_{iN_s} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{L_i} \frac{c^2 \Gamma_j}{(4\pi f_1)^2} \frac{e^{-\mathbf{j}2\pi \frac{f_1}{c} \|\mathrm{Elm}_i - \mathrm{UE}^j\|}}{\|\mathrm{Elm}_i - \mathrm{UE}^j\|^2} \\ \sum_{j=1}^{L_i} \frac{c^2 \Gamma_j}{(4\pi f_2)^2} \frac{e^{-\mathbf{j}2\pi \frac{f_2}{c} \|\mathrm{Elm}_i - \mathrm{UE}^j\|}}{\|\mathrm{Elm}_i - \mathrm{UE}^j\|^2} \\ \vdots \\ \sum_{j=1}^{L_i} \frac{c^2 \Gamma_j}{(4\pi f_{N_s})^2} \frac{e^{-\mathbf{j}2\pi \frac{f_{N_s}}{c} \|\mathrm{Elm}_i - \mathrm{UE}^j\|}}{\|\mathrm{Elm}_i - \mathrm{UE}^j\|^2} \end{pmatrix}, \tag{21}$$

where $f_k = \mathbf{F} + k\Delta f$ is the kth subcarrier's frequency [12].

RACH symbols are carried by $N_s = 839$ subcarriers, which means that the number of unknown parameters becomes much less than the number of equations. For each antenna element Elm_i, the number of unknown parameters is $L_i + 3L_i$ according to Eq. (21), where L_i is the number of unknown Fresnel coefficients and $3L_i$ is the number of unknown coordinates of L_i image sources. In practice $L_i \ll N_s$. It has been reported that the number of observed paths is no more than 15 when the distance to UE is more than 20 meters [11], [18].

Incorporating phase noise $\Delta\varphi_i$ adds one more unknown element and the total number of unknown elements becomes $4L_i + 1 \ll N_s$ in eq. (21), and the influence of phase noise can be represented as follows: $\vec{H_i}^* = q_i \vec{H_i}$, where $q_i = e^{-j\Delta\varphi_i}$. Hence, the phase noise can be counted in the multipath case.

B. RACH OFDM measurements

In the same way, as in the single-path solution, all required operations have been already calculated during the RACH synchronization procedure including channel estimation. In fact, the BS calculates correlation vectors between incoming signals and local sequences based on the Fourier transform where multiplication operations are done in the frequency domain [19]. Since the amplitudes of RACH symbols are equal to one, the conjugated multiplication of incoming symbols with RACH symbols becomes equivalent to the corresponding division of incoming symbols to RACH symbols. This means that the BS can obtain the channel measurements without introducing additional complexity during the multiplication operation in the frequency domain. The channel measurement $\vec{H_i}'$ at Elm_i can be derived by: $\vec{H_i}' = \vec{H_i}^* + \vec{r_i}$, where $\vec{r_i}$ is the N_s dimensional vector of noise.

Now, the channel is well derived based on the positions of antenna elements, UE and its images, and the surrounding environment. However, a single antenna by itself can only resolve the distances d_{ij} and the combined effect of Fresnel and the phase noise coefficients, but not the coordinates of images UE^j. Hence, the measurements from all antenna elements have to be combined together to jointly estimate all the unknown coordinates UE^j. The combined measurements for N elements can be written in vector form as follows:

$$\begin{pmatrix} \vec{H_1}' \\ \vec{H_2}' \\ \vdots \\ \vec{H_N}' \end{pmatrix} = \begin{pmatrix} \vec{H_1}^* \\ \vec{H_2}^* \\ \vdots \\ \vec{H_N}^* \end{pmatrix} + \begin{pmatrix} \vec{r_1} \\ \vec{r_2} \\ \vdots \\ \vec{r_N} \end{pmatrix}.$$

Let us denote the $N \cdot N_s$ dimensional vectors as follows

$$\vec{H}' = \vec{H} + \vec{r}. \tag{22}$$

C. Localization as an optimization problem

Our goal is to find the position of UE. We formulate the multi-path localization problem as the following optimization problem with the objective to minimize the squared difference between the measurements and the channel.

$$\text{minimize} \quad ||\vec{H}' - \vec{H}||^2 = \sum_{i=1}^{N} \sum_{k=1}^{N_s} (H'_{ik} - H^*_{ik})^2 \tag{23a}$$

$$\text{s.t.} \quad UE^j \in S_j, \forall p_j \in \bigcup_{k=1}^{N} L_k. \tag{23b}$$

Here $H^*_{ik} = q_i H_{ik}$. The objective function given in (23a) is nonlinear due to the nonlinearity of the channel model (Eq. 21). The constraints in (23b) restrict the regions where the UE and its images can locate. We assume the BS has the knowledge of its surrounding environment due to the availability of Google maps, Openstreetmaps, and the heatmaps generated based on the statistics of cellular and Internet traffic. The search regions can be restricted to the areas that are accessible to human beings. The RACH synchronization procedure can also help reduce the size of the search area. It can provide a rough estimation of the time delay based on the position of the correlation spike, by which the distance from UE to BS can be estimated with the accuracy of ~ 200 meters [12]. The intersection of the area maintained by the BS and the ring defined based on the estimated time delay (RACH ring area) can be employed to further decrease the search area.

Since the objective function is nonlinear and non-convex, it is vital to start the optimization from a good initialization as an improper starting point may cause early convergence to a local minimum. A straightforward approach to estimate the global optimal location is to split the area maintained by the BS into small pieces and performed optimization within each small area. However, the complexity of such a naive approach is very high. Our idea is to use the output of the LoS localization algorithm as the initialization for the optimization problem.

V. Performance Evaluation

A. Simulation setup

The carrier frequency $\mathbf{F}$ is set to 2.6 GHz, which is typical for LTE systems. The RACH signals occupy 864 subcarriers including 25 guard/empty subcarriers with subcarrier spacing of $\Delta f = 1250$ Hz. We simulate the preambles of format zero, which is set for a network cell with a radius of approximately 14 km. According to the RACH performance report in [20], for a single-antenna receiver, the SNR is set to -17 dB for the signals sent from the edge of a cell. We use this SNR to generate background additive white Gaussian noise by considering the distance of 14 km and the UE transmitter power of 100 mW.

Our setup includes one UE and one BS. The UE has one transmitting antenna element, whereas the number of antenna elements at the BS is varied from 16 to 100 in the single-path case, and from 8 to 64 in the multi-path case. The antenna elements at the BS is simulated as a uniformly distributed array alongside a line. The distance between two neighboring elements is configured to be half of the wavelength $\lambda/2 \approx 6$ cm [10]. We use the coordinates of the BS as the center of the MIMO antenna array, and the coordinates of the UE as the coordinates for its single antenna. Each antenna element receives a signal mixed with the background noise that is -17 dB. The power of the received signal is modeled based on the propagation distance and free space loss [17]. We use the following two scenarios for evaluating our scheme in single-path and multi-path cases.

1) Single-path case: The UE is located in a sector with a 120 degree angle. The distance from the UE to the BS is varying from 10 to 500 meters. We test our algorithm for the single-path case to localize a UE in the following five regions: $10m-50m$, $50m-100m$, $100m-150m$, $150m-300m$, and $300m-500m$. The $10m-50m$ region is used to evaluate the performance for the near field, the next three scenarios are used for the transition regions between the near and far field regions, and the last scenario is for far field. The both measured and modeled phase noises are incorporated in the simulation. Results presented in Fig. 7 are calculated based on the results of 500 rounds for each configuration.

2) Multi-path case: The position of the UE is varying inside of the same sector as for single-path but the distance is limited to 200 meters. The NLoS signals are simulated to be specular reflections from concrete walls. The Fresnel coefficients of reflection Γ_j are taken from experimental measurements provided in [11]. Since we evaluate the localization performance, we take the angle of incidence as 45 degrees for all reflections and calculate the average reflection coefficient $\Gamma_j = 0.3$ for the operating frequency 2.6 GHz. To simulate reflections, we randomly place two walls within the simulated area as long as they do not block the LoS path. The images of the UE are calculated relative to the walls using the Householder transformation [21]. The phase noise is not incorporated to the multipath simulation. Results presented in Fig. 7 are calculated based on the results of 100 rounds for each configuration.

B. Simulation results

1) Single-path scenario: We evaluate our scheme for the single-path case using the following two metrics:

- Localization Error: the Euclidean distance between the estimated location and the real UE location;
- Angle Error: the difference on Angle-of-Arrival (AoA) between the estimated location and the real location.

Fig. 7(a) shows the Root Mean Square (RMS) of the localization error with the variation of the number of antenna elements, respectively. The errors higher than 2.5 meters are not drawn on the plot. Blue lines represent the results of Bancroft's algorithm, and black lines represent the results of Bancroft's algorithm after taking into account the phase noise using Kalman filter. Fig. 7(b) shows the RMS of the angle error with the variation of the number of antenna elements.

A key observation from the two figures is that the SWP assumption is correct and desirable for large massive MIMO since localization and angle errors decrease with the increase of the number of antenna elements. Even for the region of 300m-500m, the achievable accuracy with 100 antenna

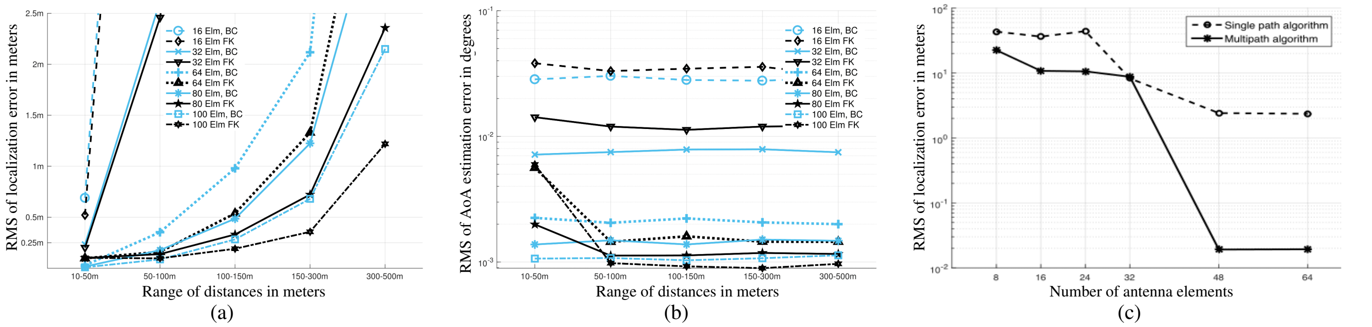


Fig. 7. Single-path: (a) RMS of localization error for Bancroft (BC) and for the refined (FK) results; (b) RMS of AoA estimation error for Bancroft (BC) and for the refined (FK) results. Multipath: (c) RMS of multipath localization error.

elements is around one meter after taking into account the phase noise. This enables the user separation in crowded open areas such as sports matches in stadiums and open-air events.

Another observation is that in the SWP model the phase noise can significantly deteriorate the localization performance. This is why it is necessary to take into account the phase noise in localization procedures. The results confirm the necessity in general because the refined results (i.e. FK results) are better than the results of standard Bancroft's algorithm. The exceptional situation occurs when the number of antenna elements is higher than 64 and the distances are closer than 100 meters. The reason for this effect is that we approximate the trends of the pure phases φ_i from (11) using parabolic shapes in Kalman filter. In other words, using Kalman filter, we are looking for a parabolic shape in the phase measurements (11) by taking into account the phase noise and then feed the resulting parabolic shape to Bancroft's algorithm. Obviously, a small portion of a sphere can be well approximated by parabolic shape but if the portion is big enough, the approximation becomes worse. In the case of small distances and large massive MIMO, we can see the same effects when comparatively big portions of spheres are captured by big antenna arrays and the refinement using Kalman filter only deteriorates the measurements.

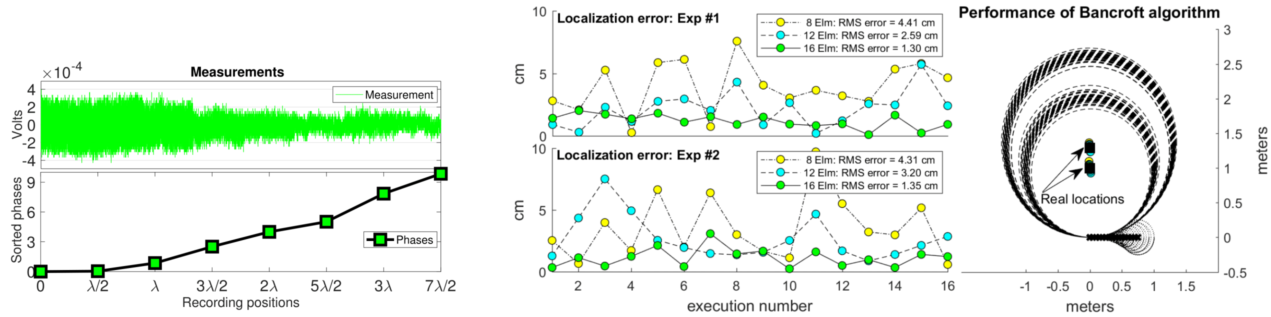
It is worth noting that the AoAs can be estimated with accuracy less than one degree. However, it can be well seen that the constructed Kalman filter converges slowly, and it starts to converge after 32 iterations. This effect is observed in Fig. 7(b) where the AoA estimation accuracy for 16 and 32 elements is deteriorated by the refinement while it is improved by the refinement for the higher number of antenna elements.

2) Multi-path scenario: We first run the single-path solution to estimate the initial position. Once the single path algorithm gives a solution which is behind walls, we set the initial point near the intersection of the walls. This can be done because we assume that the environment is known. Empirically, we found that the single-path algorithm gives an unpredictably big error when it loses the correct solution. Due to this fact, we take an initial position based on the information about the surrounding environment (environmental initialization). We use the standard Matlab function `lsqnonlin` to solve the formulated non-linear optimization problem. Instead of defining a restricted searching area, we use the following stopping policy to terminate the running of `lsqnonlin`: if the difference between two adjacent steps is smaller than 10^{-19}, the Matlab function `lsqnonlin` aborts.

Fig. 7(c) compares the RMS with those of the single-path algorithm. It is well seen that the multipath algorithm gives slightly better results in comparison with the single paths algorithm when the number of antenna elements is no larger than 32. This is because the ability to choose slightly better initializations in overall has a positive impact. Significant improvement occurs when the number of antenna elements reaches 48. This means that starting from 48 elements, the amount of measurements becomes enough for the multipath algorithm to resolve the localization problem even if the initialization is not accurate. The proposed algorithm for the multipath case becomes robust and the achieved accuracy is within several centimeters. The accuracy of the scenarios with a small number of antenna elements is worse due to the impact of weak initialization. If a good initial point is chosen, the result becomes good, otherwise, the algorithm may be trapped in a local minimum, and the Matlab solver does not have a good performance. Please note that the phase noise is not considered in the multipath scenario. Our future work is to incorporate non-ideality of synchronization and investigate other non-linear optimization solvers to address this problem.

C. Proof-of-Concept experiment

We implemented our single-path solution on our testbed and emulated a MIMO BS with 8, 12 and 16 antenna elements. The experimental setup is the same as in III-C except the two radios are communicating through the air. The ranges of experiments are limited by the lengths of available SMA cables that synchronize the radios. The transmitter repetitively sends RACH signals over the air, and the receiver changes its position according to the required number of times to emulate antenna arrays with 8, 12 and 16 elements. Once the receiver captures a signal, it performs the RACH synchronization and estimates the correlation spike's phase. Since the radios know the transmission moments due to the reference clock, the time alignment has been performed to emulate simultaneous reception by all antenna elements. The sorted phases are illustrated in Fig. 8(a). It can be seen that the phase changes consistently



(a) (b)

Fig. 8. Experimental results: (a) sorted phases obtained from RACH measurements; (b) estimation of two locations with different number of antenna elements.

accordingly to the positions of the antenna elements, thereby justifying the feasibility of our solution.

We perform our experiments in an indoor office environment with moving objects and people. For each position, the testbed executes 16 RACH procedures. Hence, for each antenna configuration, we run the localization algorithm 16 times as illustrated in Fig. 8(b). Centimeter-level accuracy is achieved since the emulated antenna array can easily capture the spherical shape of the wavefront for such limited distances.

VI. Conclusion

In this paper, we propose two algorithms to localize LTE UEs during the RACH synchronization procedure. The first algorithm is designed to localize UEs in the single path case using phase rotations of incoming signals, which can be captured by the antenna elements of a massive MIMO at the BS. The second algorithm works in the multipath case, in which the multipath channel is modeled using the spherical wave propagation assumption and linked to the propagation environment. We evaluate our schemes in both simulations and experiments, and results show that the localization algorithms can achieve decimeter-level accuracy for massive MIMO with a big number of antenna elements. The further development of the research lays in the extensive experimental validation of the algorithms and the enhancement of the optimization methods.

References

[1] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, "Eliminating channel feedback in next-generation cellular networks," in *Proceedings of the 2016 Conference on ACM SIGCOMM 2016 Conference*, ser. SIGCOMM '16. New York, NY, USA: ACM, 2016, pp. 398–411.

[2] J. Vieira, F. Rusek, O. Edfors, S. Malkowsky, L. Liu, and F. Tufvesson, "Reciprocity calibration for massive mimo: Proposal, modeling, and validation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3042–3056, May 2017.

[3] S. Malkowsky, J. Vieira, L. Liu, P. Harris, K. Nieman, N. Kundargi, I. C. Wong, F. Tufvesson, V. wall, and O. Edfors, "The world's first real-time testbed for massive mimo: Design, implementation, and validation," *IEEE Access*, vol. 5, pp. 9073–9088, 2017.

[4] S. Zhang, P. Harris, A. Doufexi, A. Nix, and M. Beach, "Massive mimo real-time channel measurements and theoretic tdd downlink throughput predictions," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2016, pp. 1–6.

[5] E. Bjrnson, E. G. Larsson, and T. L. Marzetta, "Massive mimo: ten myths and one critical question," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 114–123, February 2016.

[6] D. Vasisht, S. Kumar, and D. Katabi, "Sub-nanosecond time of flight on commercial wi-fi cards," *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 4, pp. 121–122, Aug. 2015.

[7] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "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*, ser. MobiCom '14. New York, NY, USA: ACM, 2014, pp. 237–248.

[8] E. Bjornson, J. Hoydis, and L. Sanguinetti, *Massive MIMO Networks:Spectral, Energy, and Hardware Efficiency*. Now Foundations and Trends, 2017.

[9] M. H. Alsharif, J. Kim, and J. H. Kim, "Green and sustainable cellular base stations: An overview and future research directions," *Energies*, vol. 10, no. 5, 2017.

[10] S. J. Orfanidis, *Electromagnetic Waves and Antennas*. Rutgers University New Brunswick, NJ, 2014.

[11] L. Raschkowski, P. Kyösti, K. Kusume, and T. Jämsä, "METIS Channel Models," Tech. Rep., 2015.

[12] S. Sesia, I. Toufik, and M. Baker, *LTE - The UMTS Long Term Evolution: From Theory to Practice*. Chichester: John Wiley & Sons Ltd, 2011.

[13] S. Bancroft, "An algebraic solution of the gps equations," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-21, no. 1, pp. 56–59, Jan 1985.

[14] L. Ljung, *System Identification: Theory for the User*, ser. Prentice Hall information and system sciences series. Prentice Hall PTR, 1999.

[15] W. S. Agee and R. H. Turner, "Optimal estimation of measurement bias," National Range Operations Directorate White Sands Missile Range Nm Analysis and Computation Div, Tech. Rep., 1972.

[16] D. Tse and P. Vishwanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[17] A. Fedorov, H. Zhang, and Y. Chen, "Geometry-based modeling and simulation of 3d multipath propagation channel with realistic spatial characteristics," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1458–1464.

[18] K. Mahler, W. Keusgen, F. Tufvesson, T. Zemen, and G. Caire, "Propagation of multipath components at an urban intersection," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–5.

[19] A. Fedorov, V. Lyashev, and L. Rapoport, "Fast algorithm of lte rach detection based on sparse fourier transform," in *2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC)*, Feb 2015, pp. 77–82.

[20] "ETSI TS 136 104 V10.2.0," ETSI, 650 Route des Lucioles,F-06921 Sophia Antipolis Cedex - FRANCE, Standard, May 2011.

[21] A. S. Householder, "Unitary triangularization of a nonsymmetric matrix," *J. ACM*, vol. 5, no. 4, pp. 339–342, Oct. 1958.