A Systematic Review on Positioning in 5G and beyond Cellular Networks: Overview, State-of-the-art and Deployment Challenges

Mohammad Abuyaghi, *Graduate Student Member, IEEE,* Samir Si-Mohammed, George Shaker, *Senior Member, IEEE,* Catherine Rosenberg, *Fellow, IEEE*

***Abstract*—The integration of 5G services into our daily lives has created a high demand for accurate and reliable positioning solutions. With the widespread deployment of 5G networks, there is a growing interest in utilizing their advanced capabilities for positioning. This article provides an overview of the 5G services and discusses how positioning can be tailored to meet specific requirements and device capabilities. It presents 5G positioning architecture, standardized techniques and requirements outlined in different 3GPP 5G releases. It also surveys the literature for the latest advancements in 5G and beyond positioning techniques such as sidelink positioning, carrier phase, RIS-aided, machine learning-aided, massive MIMO, beamforming and hybrid techniques, by reviewing the most recent literature on the subject. Lastly, the article addresses the practical challenges associated with implementing positioning solution in 5G networks.**

***Index Terms*—5G, Positioning, RIS, Machine Learning, Massive MIMO, Beamforming, Hybrid Techniques, Internet of Things.**

I. Introduction

THE last few years have witnessed a remarkable proliferation of cellular communication technologies and new devices, some with very sophisticated capabilities while others are very simple, giving rise to a plethora of use cases. This proliferation is indicative of the innovative ways in which connectivity is revolutionizing various aspects of our daily lives. This paper is on 5G (and beyond)) positioning, discussing emerging technologies enabling more precise and efficient location-based services in a variety of use cases.

The topic of positioning has been extensively studied in the past thirty years, largely due to the widespread demand for location-based services in several use cases and for different wireless technologies. Researchers have proposed and utilized various positioning techniques to enable precise positioning taking into account not only the varying accuracy requirements of the location-based services, but also the capabilities of the targeted devices. An an example, in the Internet of Things (IoT) domain, use cases such as asset tracking, smart cities, and industrial automation have different requirements. Asset tracking relies on accurate and real-time positioning for streamlined logistics. Smart cities leverage location data for intelligent traffic management, waste disposal or public safety, with a focus on accuracy and scalability. In industrial automation, the emphasis is on precise location data to enhance process optimization and ensure personnel safety. Beyond the IoT realm, several use cases, like emergency services or consumer navigation, also showcase diverse positioning requirements. While emergency services prioritize rapid and precise location data for swift response times, consumer navigation relies on accurate positioning for delivering precise directions and location-based services, with an added emphasis on security and privacy.

To satisfy the requirements of the different positioning use cases, researchers have explored the use of multiple wireless technologies, such as GNSS (Global Navigation Satellite system), cellular, Wi-Fi and Bluetooth. More recently, employing 5G New Radio (NR) cellular networks for positioning has become a topic of huge interest. Indeed, traditional technologies like Bluetooth or Wi-Fi can offer satisfactory accuracy indoors, but their performance is poor outdoors, especially when the device is in motion. In contrast, GNSS has difficulty penetrating buildings, making it challenging to provide accurate positioning information indoors. 5G cellular technology seems to offer the ideal tradeoff both indoor and outdoor, even with mobile objects. Furthermore, 5G is designed to accommodate high device density which is beneficial for massive IoT.

5G is regulated by the 3rd Generation Partnership Project (3GPP) which periodically publishes Releases (i.e., sets of standards), the first one being Rel-15 and the current one Rel-18. 3GPP has standardized (among many other things) several methods for positioning. Still, this domain is in constant evolution, and researchers have directed their attention towards proposing novel positioning solutions in complex scenarios, especially where a direct line-of-sight (LOS) between the device and the interconnected node is unavailable. Techniques like sidelink positioning or Reconfigurable Intelligent Surface (RIS)-aided positioning have also been extensively explored in the literature, for a possible standardization by the 3GPP in a near future either in 5G-Advanced or 6G.

Given the current trendiness of the topic, numerous surveys on positioning have been proposed in the literature. First, surveys like [1]–[6] provide comprehensive insights into localization but notably lack a focus on 5G NR. On the other hand, references such as [7]–[9] while focusing on 5G, may be considered outdated. Other surveys such as [10], [11], are

Mohammad Abuyaghi, George Shaker, and Catherine Rosenberg are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada (E-mails: mohammad.abuyaghi@uwaterloo.ca; gshaker@uwaterloo.ca; cath@uwaterloo.ca).

Samir Si-Mohammed is with the ICube lab of University of Strasbourg, France (E-mail: simohammed@unistra.fr).

too specific to a particular technology (e.g., Massive MIMO). The paper that is closer to ours in objectives is [12]. It is a recent and very valuable survey on cellular positioning, that strongly focuses on Machine learning-aided techniques for localization, and does not include the latest release of 3GPP (Rel-18). Finally, several recent surveys are claiming to be on 6G positioning [13]–[15], it is essential to note that 3GPP has not yet published a release on 6G and hence, all those surveys are exploratory.

This paper offers a thorough and current examination of 5G cellular positioning, emphasizing a diverse array of use cases, including IoT. It also reviews the latest progress on 3GPP 5G positioning including requirements for different use cases, the supported positioning techniques, and the items under study at 3GPP. Specifically, the major contributions of this paper are the following:

- Summarize the latest advancements in 3GPP releases for positioning, with a focus on the requirements of the different 5G services.
- Provide a systematic review of the state-of-the-art works on emerging positioning techniques in 5G networks, namely sidelink, carrier phase, RIS-aided, ML-aided, massive MIMO, beamforming and hybrid techniques. Some of those techniques could be adopted by 3GPP for 5G-Advanced or 6G.
- Present the major challenges hindering the usage of 5G positioning techniques in practice.

The paper is structured as follows (see Fig. 1): Section II provides a summary of the latest releases from 3GPP and presents the landscape of 5G services. In Section III, 5G positioning architecture, requirements, and common techniques are presented. We provide a comprehensive review of the state-of-the-art for emerging techniques like carrier phase, sidelink, RIS-aided, and ML-aided positioning in Section IV. Finally, we discuss the practical challenges of implementing IoT positioning techniques in commercial and private 5G networks, and emerging use cases in Section V. The paper is concluded in Section VI. The list of the abbreviations and acronyms is provided in Table II.

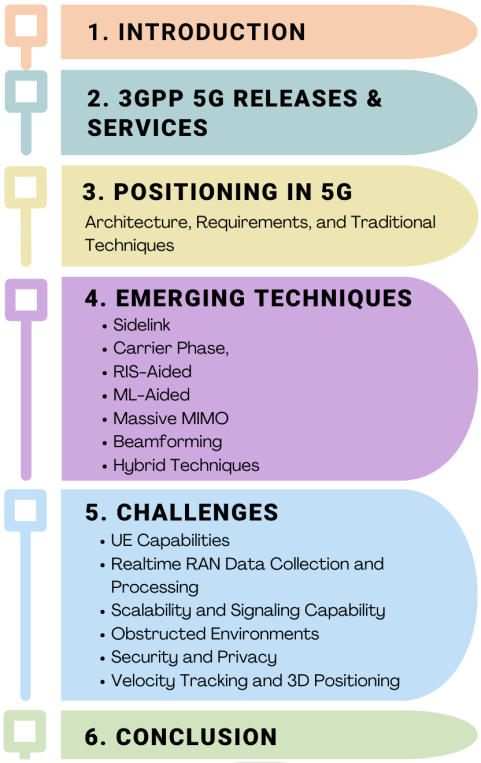

Fig. 1. Article Outline.

II. Latest 3GPP Releases and 5G Services

A. 3GPP Releases Evolution

The 3rd Generation Partnership Project (3GPP) is an organization that collaborates on creating technical standards for mobile technologies, organized into releases, which include agreed-upon features and work items. A work item represents a set of tasks which aim at developing new or improved functionalities of a system in 3GPP (*e.g.,* the 3GPP summary of Rel-17 Work Items [16] contains a set of tasks dedicated to the enhancement of 5G NR positioning).

As 5G positioning techniques and 5G services are imbedded into tied to these releases, we provide a brief description of each of them in this section, highlighting their respective key milestones.

In 2015, the work on 5G NR began, aiming to create a new radio access technology and incorporating non-standalone (NSA) 5G architecture, where the existing Long Term Evolution (LTE) radio access and Evolved Packet Core (EPC) serves as an anchor for mobility management and coverage to incorporate the 5G carrier. The completion of the Rel-15 NR specifications occurred in Q4 2018.

Rel-16 further advanced the development of NR to meet all the requirements of 5G. Important aspects of Rel-16 include the introduction of standalone (SA) 5G architecture, advancements in industrial IoT and vehicle-to-everything (V2X) communication, improvements in multiple-input multiple-output (MIMO) technology, positioning, and power-saving features for user equipment (UE). Rel-16 was finalized by Q2 of 2020.

In Q2 of 2022, the completion of Rel-17 brought several important updates. These updates include improvements to sidelink communication, reduced capability devices for NR, expanded NR operation up to 71 GHz, Radio Access Network (RAN) slicing, improvements in coverage, support for private networks, and advancements in positioning technology.

The commencement of work on 5G Advanced was initiated by Re.18 which includes artificial intelligence (AI) and machine learning (ML) technologies, device complexity reduction, positioning improvement, and NR Support for unmanned aerial vehicles (UAV). The completion of Rel-18 is anticipated to occur by 2024.

The plan for Rel-19, unveiled in 2023, is a significant step for 5G Advanced, aiming to improve 5G capabilities and lay the foundation for a smooth transition to 6G. The main goal of

TABLE I
5G SERVICES, REQUIREMENTS, AND USE CASE EXAMPLES

Service / Aspect	URLLC	eMBB	RedCap	mMTC	
				LTE-M	NB-IoT
Max. Data Rate (DL)	100 Mbps	20 Gbps	150 Mbps	4 Mbps	250 kbps
Max. Data Rate (UL)	Not defined	10 Gbps	50 Mbps	1 Mbps	180 kbps
Min. Latency	1 ms	4 ms	100 ms	10 ms	1.6 sec
Max. Bandwidth (FR1)	100 MHz	100 MHz	20 MHz	5 MHz	200 kHz
Max. Bandwidth (FR2)	2 GHz	2 GHz	100 MHz	-	-
Coverage (MCL)	Not defined	144 dB	140 dB	156 dB	164 dB
Battery Lifetime	Varies	Days	Days to Years	5+ Years	10+ Years
Mobility	Supported	Supported	Supported	Supported	Not Supported
Transmission Mode	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex	Half Duplex
Device Complexity	Medium to High	High	Medium	Low	Low
Use Case Examples	Remote Surgery	Augmented Reality	Wearables	Asset Tracking	Smart Metering

Rel-19 is to build a flexible and robust mobile network, with a specific focus on extended reality (XR) and virtual reality (VR) applications. It is expected to strengthen data security, improve mobility, and prioritize the use of AI and ML to optimize network management and configuration, among other aspects. Additionally, it will also potentially integrate sensing and communication in 6G networks [17].

B. 5G Services Landscape

5G services encompass a diverse range of use cases, which are characterized by a set of different requirements. The 3GPP has proposed to categorize these requirements into different classes (along with their operating devices' types), that we summarize in the following:

The Enhanced Mobile Broadband (eMBB) service was introduced in 3GPP Rel-15. It necessitates high data rates to cater to data-intensive applications such as virtual reality and ultra-HD video streaming. The key factors to consider in this service are augmented bandwidth, low latency and high throughput.

The concept of Ultra-Reliable Low Latency Communications (URLLC) was also introduced in Rel-15. It is characterized by the need for extremely low latency and high reliability in mission-critical applications such as autonomous driving, remote surgery and drones control. The primary goals to consider in this service are the achievement of extremely low latency and high reliability, all of which are essential for ensuring real-time responsiveness and uninterrupted connectivity.

The evolution of massive Machine Type Communications (mMTC) necessitates the provision of support for a vast number of devices concurrently, thereby facilitating the implementation of low-power, wide-area IoT (LPWA) applications such as smart metering and environmental monitoring. The focus of this service which was also introduced in Rel-15, is on low power consumption, extended coverage and the ability to support a significant number of devices with limited capability. mMTC service comprises two sub categories: (i) Long Term Evolution Machine Type Communication (LTE-M), introduced in Rel-13 and (ii) Narrowband IoT (NB-IoT), introduced in Rel-14. These two sub-categories differ in many aspects such as mobility, coverage, bandwidth and transmission mode.

The emergence of devices such as wearables and industrial wireless sensors, presents a challenge in categorizing them under the legacy mMTC service. As a result, a new 5G service, referred to as Reduced Capability (RedCap), has been introduced in 3GPP Rel-17 to accommodate these use cases [18]. The RedCap service is characterized by reduced throughput and bandwidth, relaxed latency requirement and varying battery life (from days to years), depending on the specific use case. For example, RedCap devices can operate with a maximum bandwidth of 20 MHz in the carrier frequency range 1 (FR1) below 7 GHz. In comparison, eMBB and URLLC devices can have a maximum bandwidth of 100 MHz, while mMTC devices can have a maximum bandwidth of 5 MHz. In Rel-18, 3GPP has requested the industry groups to examine a bandwidth limit of 5 MHz for RedCap [19]. This suggests that RedCap may potentially replace LTE-M in the coming years. FR2 uses millimeter wavelength and operates above 24 GHz. Currently, mMTC only operates with FR1 because the minimum channel bandwidth specified for FR2 is 50 MHz [20].

Table I outlines the common requirements for different 5G services. It comes with updated requirements based on recent 3GPP releases. This table is designed to assist readers with an updated overview of the different characteristics of each service, according to several criteria. It also provides examples of trendy use-cases for each service, highlighting their requirements. For example, critical applications such as remote surgery and autonomous vehicles require extremely low latency and high speed mobility but can tolerate lower throughput. On the other hand, smart metering use cases require extensive coverage, long

battery life, and can tolerate the latency and mobility. Note that the coverage requirement in Table I is determined by the Maximum Coupling Loss (MCL), which is a metric measured in decibels (dB), that indicates the maximum attenuation of the radio signal between transmitting and receiving nodes. A higher MCL value indicates a larger area of coverage.

3GPP has recently started discussion about Ambient IoT (AIoT), which encompasses the very low-end IoT use cases with requirements for ultra-low complexity UEs, ultra-low power consumption, and small form factor. These requirements can be fulfilled by battery-less (zero-energy) UEs or UEs with limited energy storage capability. However, current cellular technologies are unable to meet AIoT power consumption and UE cost/complexity criteria, necessitating the development of new technologies under NR in Rel-19 or later and 6G [21]. As it is a really premature service, there is no clear view about its characteristics. Thus, we chose not to include it in Table I.

III. Positioning in 5G Networks

The demand for accurate positioning has increased due to the need for location-based services in multiple verticals such as industrial IoT and autonomous driving. The advent of 5G technology presents an opportunity to provide precise positioning for applications that requires robust, flexible, and cost-effective positioning solutions. This section presents basic architecture of positioning in 5G networks, the requirements and improvements in 3GPP standards, and the common techniques used for positioning in 5G.

A. Positioning Architecture in 5G Networks

The location service architecture in 5G framework, across all releases, comprises four main components (see Fig. 2): (i) User Equipment (UE), which receives positioning reference signal (PRS) and sends sounding reference signal (SRS), conducts physical-layer measurements, reports them to the 5G core network (5GC), and in some cases computes its own location, (ii) 5G Radio Access Network (NG-RAN), where the serving gNodeB (gNB) allocates the physical resources for the UE positioning process, receives SRS and sends PRS, conducts physical-layer measurements and reports them to location server in the core network, (iii) Location Management Function (LMF) in the 5GC, which initiates the positioning request based on a third-party inquiry, receives the reported physical-layer measurements, and computes the UE's location and (iv) Location Service (LCS) Clients, which connect third-party applications to the core network and provide customers with LCS through open Application Programming Interfaces (APIs), such as real-time location push, map management, track query, and location data analysis [22].

B. Positioning Requirements in 3GPP Standards

The two key measures of performance in positioning are accuracy and latency. Accuracy commonly denotes the difference between the calculated location and the actual one, while latency indicates the time required for end-to-end positioning. Consequently, 3GPP studies and research work in

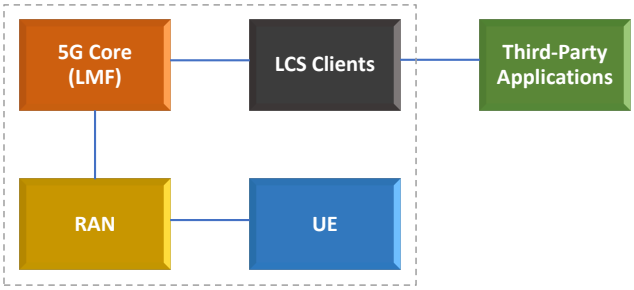

Fig. 2. 5G Location Service High Level Architecture in 3GPP

the field concentrate on reducing the error in positioning and the latency. In this subsection, we identify the accuracy and latency requirements specified by 3GPP for various use cases across consecutive releases. It is important to note that when assessing the accuracy of a positioning system, the 3GPP standard differentiates between two types: horizontal and vertical. Horizontal positioning pertains to latitude and longitude, encompassing two dimensions, while vertical positioning incorporates altitude to achieve three dimensions.

For baseline devices (i.e., eMBB service), the desired level of accuracy for horizontal positioning in Rel-16 is set in commercial use case to below three meters for indoor settings and below ten meters for outdoor settings, with the goal of achieving this level of accuracy for 80% of the UEs [23]. In Rel-17, the target accuracy for the same service is set to below one meter for 90% of the UEs in both settings (indoor and outdoor). For the industrial IoT use case, the requirement is stricter; the target accuracy is set to less than 20 centimeters for 90% of the UEs. Vertical positioning requirements are more relaxed than horizontal ones in most use cases. Rel-17 also sets the requirements of sidelink positioning, which includes V2X, public safety, commercial, and Industrial IoT use cases with specific accuracy and latency thresholds for each use case [16].

In Rel-18, 3GPP defines a set of requirements for more use cases in different positioning scenarios. For instance, the target accuracy for horizontal RedCap service positioning is set to below three metres for 90% of the UEs in both settings (indoor and outdoor) [24]. This relaxation is mainly due to the less available bandwidth for RedCap UEs. Indeed, localizing a device with limited capabilities in different environmental settings is challenging due to multiple factors, including low bandwidth and power saving mode of the device. Researchers suggested some solutions like use of frequency hopping in uplink transmission [25] and the use of external trigger to wake-up the device [26].

Latency is another performance metric that indicates if a positioning method can calculate the location in real time or not. End-to-end latency requirements for 5G positioning have evolved with the new releases as well, from less than one second in Rel-16 [23], to less than 100 milliseconds in Rel-17. To further decrease latency, several enhancements have been proposed, including (i) reducing the number of samples for each

measurement, (ii) triggering measurement via low layer signals to save some processing time, (iii) conducting measurement when there is no data transmission, and (iv) transmitting the PRS/SRS signals when the UE is inactive [16]. In Rel-18, the latency requirement for RedCap/Sidelink is not defined yet. Nevertheless, two new requirements are defined for sidelink positioning; relative speed (the speed of a moving UE with respect to another one) and angle accuracy (the error of the direction measure in degrees) [24].

C. Traditional Positioning Techniques

In the following section, we present a brief summary of the conventional techniques commonly used for positioning in wireless networks. They are typically classified into four categories [12], [27]: (i) Proximity-based, (ii) Range-based, (iii) Direction-based and (iv) Fingerprinting-based. Note that, unlike the three first categories, fingerprint-based methods are not standardized in 3GPP. These distinct approaches offer diverse strategies for accurately determining the location of devices in various scenarios.

1) Proximity-based techniques: Estimate the position of an object based on whether it is present within a specific radio coverage area or not. These techniques rely on detecting the proximity of the object to predefined radio signal ranges or boundaries to infer its location. The most common proximity-based technique is E-CID (Enhanced Cell-ID). In this method, the location of the UE is estimated based on the information provided by the gNB it is connected to. The gNB Cell ID is used to identify the geographical area covered by that gNB. The E-CID method enhances the accuracy of the traditional Cell ID-based positioning by incorporating additional information, such as the Received Signal Strength Indicator (RSSI) or timing measurements, which are used to estimate the distance between the UE and the gNB antenna array. NR E-CID method incorporate angle measurement to further enhance the accuracy.

2) Range-based techniques: Estimate positions based on range measurements between transmitters and a receiver or vice versa. The most common range-based techniques are:

- Time Difference of Arrival (TDOA): It is a technique used to estimate the location of a UE based on the time difference at which signals travel between the UE and multiple gNBs, using trilateration or multilateration. According to the traffic direction, we distinguish two types of TDOA:
  - UL-TDOA, where gNBs measure the time difference of the received UL-SRS, and the resulting measurements are used along with other configuration information to estimate the location of the UE by the LMF.
  - DL-TDOA, also previously called Observed TDOA in LTE, where the UE measures the time difference of DL-PRS from multiple gNBs and computes its location.
- Multi-Cell Round-Trip Time (MC-RTT): This technique consists in sending multiple signals from the UE to multiple gNBs and measuring the round-trip time for each of these signal. By estimating the RTT for each gNB, the distances between the UE and the gNBs can be determined. Then, similar to other ranging-based techniques (e.g., DL-TDOA), MC-RTT uses a trilateration/multilateration estimation algorithm to calculate the position of the UE.

3) Direction-based techniques: Uses signal angles for position estimation. The most common direction-based techniques are the following:

- Angle of Arrival (AOA): Also called UL-AOA, this technique is used to determine the location of a UE based on the direction from which a wireless signal is coming. Specifically, the gNBs measure the azimuth and zenith angles of the received UL-SRS from the UE. These measurements are then reported to the location server (LMF) in Core Network (CN) for computation to estimate the UE's position.
- Angle of Departure (AOD): Also called DL-AOD, the UE measures in this technique the received signal strength of the DL-PRS and identifies the received beam index. With the azimuth information of the gNB provided by the LMF and knowing the angle difference of the identified beam index, the UE can compute the angle of departure.

4) Fingerprinting-based techniques: Relies on various measurements collected and employed to predict the position of a UE. It involves conducting on-site surveys in a specific area to create a database of signal strength patterns at different locations. During these surveys, specific signal attributes are measured at known locations, such as received signal strength, timing information (e.g., Timing Advance or RTT), device orientation, and floor number (if indoors). These measurements are collected and stored in the database as fingerprints. When a UE needs to be localized in the same area, it measures its signal attributes and compares them with the fingerprints in the database. The device's signal attributes are then matched to the closest match in the database, allowing the system to determine the user's location based on the best match. his database, also known as a radio map or fingerprint database, stores the locations along with their associated fingerprints.

IV. Emerging Positioning Techniques in 5G

In this section we review the state of the art of the emerging 5G positioning techniques that recently caught researchers' attention to improve the accuracy, which are: (i) Sidelink positioning, (ii) Carrier Phase positioning, (iii) RIS-aided positioning, (iv) Machine Learning-aided positioning and (iv) hybrid positioning. In fact, and as mentioned in Section I, several surveys about positioning in 5G have recently been published (*e.g.,* [9], [12]–[15]). They provide valuable information about the different positioning techniques employed in the literature. However, due to the dynamic nature of this research area, there is a constant need for update. Newly introduced techniques, such as sidelink positioning, necessitate a comprehensive literature review to provide readers with a holistic understanding of the domain. To achieve this, we use the PRISMA method [28]; a systematic and comprehensive

literature reviewing approach, to explore papers not covered in the aforementioned surveys. This method ensures a thorough and up-to-date analysis of the evolving landscape of positioning methods in 5G. Note that we chose to focus on papers published after 2020.

A. Sidelink Positioning

Also known as Device-to-Device (D2D) communications, Sidelink communications refer to the direct exchange of data between two or more UEs, without the need for routing through a centralized base station (BS). Unlike traditional positioning systems that rely on external infrastructure, sidelink positioning harnesses the power of direct D2D communication within the 5G ecosystem, allowing UEs to exchange location-related information with one another. This enables precise and real-time positioning in a variety of scenarios, even with dynamic and intricate driving conditions. Ganesan et al. [29] provide an overview of the evolution of sidelink communications in 5G, and its application for positioning. To the best of our knowledge, there is no comprehensive survey in the literature that reviews the techniques for sidelink positioning in 5G. We aim to bridge this gap by providing a thorough analysis and overview of the state-of-the-art of these works, presented in the following:

According to the Lu et al. [30], the accuracy of positioning in industrial environments can be compromised due to uncertainties in the positions of anchors. To enhance accuracy, a joint estimation of vehicle and anchor positions is proposed, leveraging location-related measurements (LRMs) such as RSS and TOA. In this approach, devices function as anchor-agents, and vehicles are target-agents. The anchor-agents use sidelink measurements from target-agents to estimate LRMs. These LRMs are then transmitted to a radio unit. The final step involves employing a proposed Kalman filter-based method to estimate the positions of both anchor- and target-agents. Simulations involving two sets of anchor-agents with different geometric configurations indicate that utilizing LRMs collectively, combining time- and angle-domain LRMs, yield enhanced performance in both 2D and vertical planes. This collaborative approach outperforms using LRMs individually and improves the positioning accuracy in complex industrial environments.

Hunukumbure et al. [31] put forth a novel approach to positioning utilizing NR-sidelink and the recently introduced Multiple Quality-of-Service (QoS) class within the 5G framework. This method aims to meet the requirements of scenarios demanding both high data volume and reduced latency. It involves the clustering of users, where NR-sidelink is harnessed for ranging users within each cluster, effectively mitigating overhead. The Multiple QoS class innovation introduces varying levels of accuracy (primary, intermediary, and minimum) under the QoS requirements. This hierarchical approach streamlines latency in location privacy protocol messaging. To validate their approach, an extensive mobility model is developed, specifically tailored for a stadium entry use case. User clusters are derived from individual mobility patterns. Simulation-based analysis are conducted, revealing substantial signaling overhead reduction, approximately 75%, across a wide range of SINR conditions, through user clustering and the integration of NR-sidelink. The presented outcomes also showcase the system's ability to achieve high precision. The gNB-based lead UE tracking achieves sub-meter level accuracy, while NR-sidelink-based ranging attains 1.5 meter accuracy. Furthermore, the Multiple QoS class implementation leads to notable latency reductions ranging from 30% to 45%.

It is worth noting that sidelink communications and positioning are distinct processes that employ different mechanisms. As a matter of fact, Panzner et al. [32] address the distinct resource demands of sidelink communication and positioning, necessitating efficient scheduling between the two. To tackle this, the authors introduce a scheme aiming at selectively bypassing the preemption mechanism typically applied to sidelink communications. Their proposed approach involves a UE that sends a wideband SideLink Positioning Reference Signal (SL-PRS). This UE also transmits a "skip-preemption" message to another UE detected to be utilizing the same time and frequency resources for sidelink communication. Consequently, both UEs synchronize their transmissions within the same slot and subchannel.

In summary, recent developments in 5G sidelink positioning strategies emphasize collaborative and innovative approaches to overcome challenges in accuracy and efficiency. These advancements include joint estimation techniques which integrate different aspects, including multiple QoS classes, which accommodate varying accuracy requirements to enable tailored solutions for different scenarios, and efficient scheduling mechanisms to address distinct resource demands.

B. Carrier Phase Positioning

Due to its ability to provide high accuracy positioning in the GNSS, the carrier phase positioning method is being extensively evaluated in 5G NR system. Carrier phase is a technique used for positioning in the downlink. It involves multiplying the received reference signal with a replica signal generated at the receiver. After filtering out the high frequency component, the method calculates the distance by measuring the phase difference between the two signals [33]. More than one 5G reference signal can be used for carrier phase measurement such as Demodulation Reference Signal (DMRS) [34] and PRS [35] [36] [37]. The authors of [33] provide an overview of this technique. However, to the best of our knowledge, there is no survey about carrier phase positioning in the literature. We discuss in the following the recent works tackling carrier phase positioning.

In their work, Kim et al. [38] tackle one of the main challenges of carrier phase, which is the estimation of the unknown integer ambiguity parameter. It represents the total number of complete phase cycles that the reference carrier signal has travelled between the UE and the gNB to produce the same observed phase at the UE. To do so, similar to TDOA, they calculate the phase difference of arrival (PDOA) to discard the local clock error. They also used the OFDM subcarriers to solve the integer ambiguity of the carrier phase.

The same challenge is tackled by Fan et al. [35], who propose a technique for determining clock offset by utilizing carrier-phase measurements. They devise a fusion approach that combines estimated positions of a UE using TDOA and the temporal variations of carrier phase measurements. This fusion method offers interim position estimates for the UE, which can be employed to linearize the measurements and resolve integer ambiguities. As a result, accurate UE positions can be obtained using the carrier phase measurements. Numerical simulations illustrate that the method can achieve centimeter-level accuracy.

Jin et al. [36] propose to overcome the integer ambiguity issue through a method called double-difference carrier phase measurements. This method involves transmitting PRS continuously over time from two gNBs to accurately track carrier phase and prevent ambiguity issues in line-of-sight environments. Additionally, they used another UE to observe the same signals and eliminate measurement errors caused by clock offset between the two gNBs. This experimental approach achieves sub-meter accuracy.

Li et al. [37] introduce a technique for multi-frequency carrier phase ranging that addresses the issue of Antenna Reference Point (ARP) position error in gNBs. The proposed method achieves a positioning accuracy of 2 centimeters.

Khalife et al. [39] propose a framework that enables Unmanned Aerial Vehicles (UAVs) to navigate horizontally with sub-meter accuracy in multipath-free environments using cellular carrier phase measurements. This framework takes advantage of the ”loose” synchronization between the clocks of serving and neighbor gNBs. Extensive experimental data shows that the deviations in gNB clocks can be modeled as a stable Auto-Regressive Moving Average (ARMA) process. This loose network synchronization is used to cluster the clock deviations in a way that minimizes position estimation error and reduces computational complexity.

In conclusion, recent research efforts in carrier phase positioning for 5G NR systems have addressed critical challenges, particularly the estimation of unknown integer ambiguity parameter. Various techniques, such as PDOA calculations, fusion approaches, and double-difference measurements, have been proposed to enhance the accuracy and reliability of carrier phase positioning. These methods contribute to refining the practicality of carrier phase techniques. Moreover, the exploration of multi-frequency ranging and applications in UAV navigation further expands the possibilities of leveraging carrier phase measurements for high-precision positioning in 5G networks.

C. RIS-Aided Positioning

Reconfigurable Intelligent Surfaces (RIS) [40] are composed of specially engineered materials capable of dynamic reconfiguration of their properties, such as scattering, absorption, reflection, and diffraction, all of which can be controlled through software. RISs hold significant potential for enhancing positioning accuracy by providing greater control over the channel through the manipulation of RIS elements. This control over propagation channels offers innovative solutions to challenges in radio positioning. Specifically, RISs can assist positioning systems in establishing robust communication links between base stations and mobile UEs, even in scenarios with severe LOS obstructions. [15] is a valuable review of some of the recent works that leverage RIS to improve positioning. We propose to complete it with the following works:

Basar et al. [41] introduce a comprehensive and versatile RIS channel model that is specifically designed for mmWave frequencies. Alongside the model, they introduce the SimRIS Channel Simulator, an open-source tool for simulating RIS channels. The proposed channel model is applicable in a wide range of scenarios, encompassing both indoor and outdoor environments, and it can accommodate various frequency bands, including the mmWave band. The model takes inspiration from the 3GPP cluster channel model, integrating crucial factors such as LOS probabilities between terminals, RIS array responses, and gains of Tx/Rx units and RIS elements. Additionally, it incorporates realistic path loss and shadowing models, along with environmental characteristics that are specific to different scenarios and frequency bands.

In [42], Popoola et al. introduce a novel positioning model for Airborne Networks (i.e., where UAVs are used as aerial mobile base stations), leveraging RIS. They present a mathematical modeling of the proposed system, which comprises an RIS, a 5G small cell, and a TOA/RSS positioning algorithm. The primary objective of the proposed system model is to enhance the positioning accuracy of users and mobile base stations in mobile networks. By employing RIS technology, the authors aim to optimize the positioning capabilities in the airborne network context. The paper also addresses the challenges associated with implementing RIS-based positioning. One of the key challenges discussed is pilot contamination, arising from the use of pilot symbols for the identification of individual RISs. Pilot contamination can impact the accuracy and reliability of positioning in RIS-based systems, and mitigating this issue is crucial to achieving precise positioning.

In their study, Liu et al. [43] tackle the challenge of positioning in 5G networks by leveraging multiple passive RISs. The proposed method is based on TDOA and is applicable to both downlink and uplink scenarios. It involves estimating the UE position by considering all plausible positions in conjunction with various choices of RISs. For each combination, the UE position is estimated based on the measured TDOA, and the resulting position with the Least Squares Error (LSE) is selected as the final estimation. The method is tested through simulation, and the results demonstrate that the method effectively estimates the UE position while providing the LSE error as a metric.

Zhang et al. [44] propose to use a RSS fingerprinting-based method for positioning in a RIS-assisted environment. The motivation behind incorporating RIS is to address the impact of noise on RSS measurements, particularly in indoor settings. To overcome this, they suggest to gather several measurements of RSS values under different RIS configurations. Then, they use an optimization method based on Cramér-Rao Lower Bound (CRLB) to find the RIS configurations that yield the most

accurate positioning. It is worth noting that CRLB is used to assess the accuracy of a given parameter estimation. These measured RSS values are then used as fingerprints to train Neural Networks, enabling the estimation of the target location based on these fingerprints. Simulations results indicate that the method is able to achieve positioning in NLOS scenario with an accuracy of 0.5 meters.

Lu et al. [45] address a significant limitation in existing research on RIS-assisted positioning, where an assumption is commonly made regarding the perfect knowledge of the RIS's location and orientation. The authors argue that such an assumption may not hold in practical scenarios due to factors like deployment faults, external disturbances, or improper installation of RIS. To overcome this limitation, they propose a Joint RIS Calibration and User Positioning method, namely JrCUP, which is designed to enable user positioning even when the state of the RIS is not perfectly known. To model this uncertainty, they use the concept of Fisher Information, which allows them to derive analytical lower bounds for the states of both the user (clock offsets and 3D positions) and the RIS (array orientation and 3D position). Then, they propose an iterative algorithm to estimate these parameters based on AOA and AOD measurements. The simulations show that the geometric impact can be detrimental and therefore needs extra attention and evaluation in the network planning phase. More importantly, they have found and shown that multi-user scenario in general outperforms the single-user case.

Wang et al. [46] present a comprehensive signal model for source positioning with RISs and establish a theoretical framework based on electromagnetic theory. They also introduce the concept of Continuous Intelligent Surfaces (CISs), a specific type of RIS. CISs are planar structures that can be electronically controlled to manipulate electromagnetic waves passing through them. The controlled phase response of CISs enables precise reflection, refraction, or scattering of incident waves according to desired specifications. Unlike conventional RISs with discrete elements, CISs exhibit a continuous phase response function across the entire surface. By performing Fisher information analysis, the authors demonstrate that strategically configured CISs can significantly enhance positioning accuracy. The study reveals that the position information intensity in CIS-aided positioning is directly proportional to the fourth power of the carrier frequency. As a result, superior positioning performance can be achieved with CIS assistance, particularly at high frequencies compared to scenarios without CISs. Moreover, they show that CISs with carefully designed phase responses can provide substantial improvements in positioning performance compared to CISs with random phase responses or a simple scattering plane. The simulation results show that optimal-configured CISs can significantly improve positioning accuracy.

To summarize, recent advancements in 5G positioning strategies involving RIS technologies have showcased innovative methods. These include the utilization of multiple passive RISs for TDOA-based positioning, RSS fingerprinting in RIS-assisted environments, joint RIS calibration and user positioning techniques, the application of CISs, etc. Moreover, studies highlight the potential of RISs in diverse scenarios, including airborne networks, demonstrating the versatility of RIS-assisted positioning in 5G networks.

D. Machine Learning-Aided Positioning

Machine Learning (ML) is poised to revolutionize positioning within 5G networks, particularly in challenging scenarios like NLOS multipaths. ML is expected to play a pivotal role in complex positioning applications, especially where indirect, noisy observations and nonlinear signal characteristics are involved. ML can enhance location accuracy by creating signal fingerprints, leveraging crowdsourced data, and predicting device locations based on historical patterns. [12] provides a comprehensive review and comparison of method featuring ML for positioning. Nevertheless, due to the active nature of this field, there is a need for an updated review, that we provide in the following:

Zhao et al. [47] address the challenge of assessing the uncertainty in positioning methods. To tackle this issue, they introduce the use of Gaussian processes (Bayesian optimization) and Random Forests (Classification methods) for both the estimation of UE positions and the quantification of uncertainty. The models are trained using TOA measurements of PRS from multiple BSs. Their results demonstrate that their proposed methods achieve satisfactory positioning accuracy. Additionally, the uncertainty assessment provides valuable indications of the reliability of the position predictions.

In [48], Albanese et al. address the limitations of traditional positioning approaches and introduce a novel concept called "pseudo-multilateration". This concept involves a single UAV anchor obtaining a set of distance measurements over time while following a specific motion trajectory. These distance measurements then undergo a processing phase, which results in the determination of the target trajectory (if it is moving) within the considered time frame. The paper emphasizes the flexibility of UAVs in providing connectivity even in challenging conditions. However, it also acknowledges the high deployment complexity associated with UAVs. To overcome this, the authors propose a fully deployed ubiquitous scenario empowered by RISs to complement existing ground networks. RISs are chosen for their low-complexity and low-cost properties, making them a promising solution for enhancing wireless connectivity. Finally, the authors advocate the use of Convolutional Neural Network (CNN) for determining the UE position by treating the collected measurements as a single-channel image. This approach enables the CNN to effectively handle the channel shadowing caused by obstacles in the scenario, leading to improved positioning accuracy.

Ruan et al. [49] introduce iPos, an indoor positioning system that leverages fingerprinting, and incorporates both supervised and unsupervised learning techniques. The system's process begins with channel state information (CSI) preprocessing. Then, an unsupervised autoencoder extracts critical CSI features. To further enhance the system's probability estimation, a supervised learning model optimizes a Radial Basis Function (RBF) model. Finally, the amplitude-phase probability fusion

function efficiently combines amplitude and phase probabilities derived from the processed CSI data to deliver positioning estimations. The method's performance is evaluated in both an office and a corridor environment, yielding average indoor positioning errors of 2.14 m and 2.81 m, respectively. Notably, the system's novelty lies in its ability to achieve accurate positioning using only one base station while avoiding the need for complex convolutional operations, which makes it particularly suitable for future deployment on smart terminals with limited computing power and storage capacity.

Torsoli et al. [50] introduce the concept of Blockage Intelligence (BI), which consists in a probabilistic description of wireless propagation conditions, especially in case of NLOS. To do so, they process the cross-correlation between the transmitted and the received reference signals (PRS/SRS), in order to calculate statistical features containing positional information used by the BI. Then, a two-class supervised classification problem is considered, where a binary random variable is used to represent NLOS and LOS propagation conditions, and the vector of the statistical features is used as input. An exponential loss function is employed to obtain a model for classification, which can be used to obtain a probabilistic characterization of NLOS propagation conditions. They show how BI can enhance location awareness using simulation in 3GPP indoor factory scenarios for different ranging methods, including TOA, RTT and AOD.

In [51], Torsoli et al. also use a similar modeling approach, and they introduce a machine learning-based reference BS selection method. The authors argue that to select an appropriate BS can greatly impact the positioning accuracy. To do so, they propose a method utilizing the AdaBoost algorithm for classification. The model is trained to predict both the channel quality and the LOS posterior probability based on signal statistical features. Subsequently, the BS with the best channel quality is selected for positioning. Simulation results demonstrate the method's efficacy, as it achieves a notable improvement in positioning accuracy when utilizing TDOA measurements.

Liu et al. [52] propose a ML-based method for estimating TOA of 5G signals. They employ classification algorithms (SVM, KNN, Classification Tree, and Cross Entropy) for predicting TOA accurately in the following way: The classification models are trained using labeled data, allowing them to learn the relationship between the input features (S-curve of 5G signals) and the output variable (TOA). The method is tested using real field deployment, and the results show that support vector machine (SVM) achieves the most accurate pseudorange measurements. The results indicate that the 95% Cumulative Distribution Function (CDF) of the pseudorange measurement error using commercial 5G signals in the indoor environment is 0.50 m. Furthermore, in comparison experiments, it was demonstrated that the ML-based tracking method can achieve an equal or even higher level of accuracy compared to the traditional carrier phase ranging tracking method.

To conclude, the incorporation of ML models within 5G networks holds significant promise for addressing positioning challenges, especially in scenarios characterized by NLOS paths. The presented studies showed that ML techniques can contribute to strongly improve location accuracy by employing methods such as signal fingerprinting, crowdsourced data utilization, and historical pattern-based predictions.

E. Massive MIMO

Massive MIMO [53] has emerged as a key technology for next generation wireless networks. It involves the deployment of an extensive array of antennas at the base station, enabling simultaneous communication with multiple users, and enhancing spectral and energy efficiency. Massive MIMO harnesses numerous antennas to detect subtle signal variations, enabling precise device positioning, particularly in dense urban settings. Alamu et al. [54] provides a valuable overview of the existing works featuring Massive MIMO for positioning. However, their survey is starting to get obsolete due to the very active nature of this field. To address this, the following sections present an updated review of recent developments and findings in the realm of Massive MIMO positioning.

Sellami et al. [55] introduce an innovative approach for localizing a stationary Target UE within a challenging massive MIMO environment. Leveraging the capabilities of 5G wireless networks, including features like D2D links, massive MIMO and beamforming, the proposed algorithm relies on distance measurements between the UE and its two closest neighbor Anchor UE. These Anchor UEs assist the BS in accurately determining the UE's position. The method involves estimating distances through reference signal power measurements, identifying potential Target UE positions by intersecting circles derived from distance estimates, and resolving ambiguity using beamforming over limited angular intervals. Simulation results demonstrate that the proposed solution is able to achieve an accuracy of less than 1 meter in challenging environmental conditions.

Sellami et al. [56] also propose a neighbor-assisted positioning algorithm designed for determining the position of a stationary UE in outdoor scenarios utilizing Massive MIMO systems. The algorithm leverages two neighbouring UEs that maintain LOS components with the base station based on reference signal power measurement, aiding in scenarios with obstructed channel conditions. The BS performs beamforming over an angular interval determined by the calculated distance and AOA of the first neighbour to discover two candidates for the UE post. Finally, a bilateration is performed exploiting the second neighbour to cope with the ambiguity problem. Simulation results showcase that the algorithm achieves sub-meter positioning accuracy, with an estimation error consistently below 1 meter, even at SNR values as low as 10 dB.

The study of Singh et al. [57] outlines an approach for achieving highly precise positioning in 5G massive MIMO systems. The method utilizes a massive MIMO system within cellular networks to estimate the TOA from multiple BSs through the application of the Estimation of Signal Parameters via Rotational Invariant Technique (ESPRIT) [58]. The target UE position is determined based on multilateration using a

subset of accurate TOA measurements. Simulation results indicate an enhancement in positioning accuracy compared to conventional methods, achieving a 20 cm positioning accuracy for 90% of UEs in indoor factory scenarios.

The highlighted studies in this section contribute to the advancement of positioning techniques in 5G massive MIMO environments. The proposed algorithms utilize distance measurements, reference signal power measurements, and advanced techniques such as ESPRIT to accurately determine the position of stationary UEs. They address challenges in both indoor and outdoor scenarios, improving accuracy even in environments with obstructed channels and low SNR conditions.

F. Beamforming

Beamforming, which is a key component that allows for the directional focusing of radio frequency signals, thereby facilitating targeted communication and reception. Beamforming can also allow to refine position estimation accuracy in complex environments through directing focused beams to devices. Despite its increasing significance, there seems to be a gap in surveys dedicated to the utilization of beamforming to enhance positioning in 5G networks. The following review aims to fill this void by summarizing the latest works in this domain.

Gante et al. [59] investigate the capabilities of low-power, accurate 5G positioning systems using machine learning. The study focuses on a deep learning-based millimeter-wave positioning method and compares it with state-of-the-art outdoor positioning systems, considering energy consumption and estimation errors. The proposed method exhibits notable energy efficiency gains and reduced estimation errors. Particularly effective in NLOS scenarios, it surpasses existing approaches in both accuracy and energy efficiency. Evaluation results reveal that the deep learning-based millimeter-wave positioning method achieves remarkable energy efficiency, requiring as little as 0.4 mJ per position fix. This translates to energy efficiency gains of 47× and 85× for continuous and sporadic position fixes, respectively, compared to the latest assisted-GPS implementations.

Fascista et al. [60] introduce a positioning scheme for mobile devices in an indoor mmWave massive multiple-input single-output (MISO) scenario. The two-fold approach leverages coarse-grained AOD information from mobile clients with a single antenna to estimate each client's position. Emphasizing the advantages of Downlink (DL) signals over Uplink (UL) signals in terms of signal-to-noise ratio (SNR), the study suggests that well-designed transmit beamforming enhances position estimation accuracy in DL compared to UL, assuming realistic power conditions. The proposed two-step algorithm incorporates adaptive beamforming to achieve highly accurate positioning in DL, even in the presence of multiple users.

Abu et al. [61] address the challenge of communication systems lacking synchronization for effective positioning. The paper focuses on two-way positioning protocols, namely the round-trip positioning protocol (RLP) and collaborative positioning protocol (CLP). It delves into single-anchor positioning, deriving the Cramer-Rao bound (CRB) for position and orientation from a single transmitter and demonstrating the feasibility of estimating the user's position. The proposed single-anchor positioning method for mmWave wireless networks utilizes time delay and angle information, employing beamforming for both uplink and downlink performance evaluation. The results show that it is more beneficial to have more antennas at the BS than at the UE.

Seo et al. [62] propose the use of beamforming to update the estimated position of DL-TDOA. Precisely, they employ beamsweeping, which is a technique involving the identification of the strongest beam directed toward the UE through the measurement of Reference Signal Received Power (RSRP). The latter helps in estimating the angle between the serving gNB and the UE. Subsequently, they refine the initial estimated position of DL-TDOA to a new position aligned with the virtual line derived from this estimated angle. Their simulation shows enhanced positioning as well as a capability to distinguish closely located UEs with overlapped estimated positions. Furthermore, the results indicated that a narrower beamwidth corresponded to improved performance in the proposed method. This characteristic bodes well for massive Multiple MIMO environments characterized by a substantial number of antennas.

Koivisto et al. [63] introduce a novel estimation and tracking solution for DOA and TOA using only analog/radio frequency (RF) beamforming-based observations. The proposed approach employs an extended Kalman filter for estimation and tracking and establishes Cramér-Rao lower bounds for the RF multi-beam system. An information-based criterion is suggested for selecting beams, ensuring highly accurate performance with manageable computational complexity. The theoretical estimation performance, evaluated through CRLBs, demonstrates positioning accuracy better than 2 m in most cases.

Wang et al. [64] propose a novel approach for mmWave positioning in outdoor environments using Deep Convolutional Gaussian Process (DCGP)-based regression in a fingerprinting framework. The study leverages an open-source mmWave dataset, comprising beamforming images from 160,801 bidimensional positions, to conduct simulations. By employing DCGP, this method enhances accuracy in millimeter-wave communication-based positioning while also enabling uncertainty estimation.

Pucci et al. [65] conduct an assessment of the sensing capabilities within the 5G NR framework. The analysis encompasses the performance capabilities of the 5G OFDM waveform under the Joint Sensing and Communication (JSC) paradigm, considering scenarios involving fully digital arrays and multi-beam designs for the judicious allocation of spatial resources between communication and sensing purposes. Results reveal the ability to detect tens of targets with submeter-level accuracy, affirming the viability of integrating sensing functionalities into communication systems.

Hu et al. [66] present an innovative method for AOA estimation in 5G systems utilizing wideband SRS. The approach

incorporates a pre-estimation step employing a Multiple signal classification (MUSIC) [67]-like algorithm for coarse AOA estimation, followed by a fine-estimation step using a novel focusing algorithm to achieve high accuracy with reduced computational complexity. The MUSIC-like algorithm is applied in the pre-estimation step to obtain the coarse estimation of AOA and N within the framework of beamforming. Outperforming traditional narrow-band and wideband methods, the proposed technique enhances estimation accuracy by up to 30%.

The presented works showcase diverse applications of beamforming techniques for positioning, ranging from refining position estimation accuracy using beamsweeping in DL-TDOA, to utilizing deep learning-based millimeter-wave positioning and adaptive beamforming for indoor scenarios demonstrate the versatility and potential of beamforming in enhancing positioning accuracy, even in complex environments.

G. Joint and Hybrid Positioning Techniques

Combining signals from different technologies for positioning has always been of particular interest to the community. For fact, as presented in the following, multiple studies have demonstrated that combining two or more techniques can enhance positioning accuracy. This subsection reviews the recent work on joint techniques withing 5G and hybrid technique incorporating 5G and other technologies such as GNSS, Bluetooth, etc.

In their study, Zhang et al. [68] use carrier phase with TOA to address the challenge in carrier phase positioning technique such as, continuous phase tracking, accurate integer ambiguity resolution, and positioning error caused by NLOS. They propose a two-step position estimator based on Bayesian theory, i.e. Maximum Likelihood Estimation (MLE) and Maximum A Posteriori (MAP) estimation, besides NLOS identification and suppression scheme to further enhance the accuracy.

Liang et al. [69] proposed a hybrid method to improve accuracy in indoor positioning by integrating 5G, Bluetooth Low Energy (BLE), and a terminal motion sensor. This method involves utilizing UL-TDOA from 5G, AOA from BLE, and sensor data using an optimization algorithm. The approach successfully achieved centimeter-level accuracy for distances shorter than 3 meters and less than 3 meters of error for longer distances.

In their work, Alghisi et al. [70] tackle the limited satellite visibility for GNSS positioning in urban areas by combining 5G technology with GNSS. The study utilized both TOA and TDOA methods to assist GNSS positioning using multiple 5G base stations. The findings indicated that 5 base stations could effectively resolve the positioning issue, while configurations with fewer 5G base stations were not as effective. Additionally, the results suggested that TOA and TDOA processing yielded similar quality, with TDOA showing a slight advantage over TOA.

The existing algorithms for combining multiple signals from different technologies face challenges in dealing with rapid fluctuations in signal sources, and the unstable estimation of multi-scale multi-type signals in GNSS-5G hybrid networks. To address this, Liu et al. [71] introduce the Square Root Unscented Stable Filter (SRUSF) for joint positioning in GNSS and 5G. This filter utilizes a compact coupled filter group architecture in a reliable spatio-temporal network and includes a stabilized coefficient to ensure positive covariance of the estimation error. By doing so, it reduces the risk of filtering results diverging due to signal source variations and discrepancies between the system model and the actual situation. Simulation results demonstrate that the SRUSF method significantly improves positioning accuracy and reliability compared to five other joint estimation methods for multiple signals. This advancement has the potential to enable mass user terminals to offer timing and positioning services with unparalleled accuracy and dependability within the architecture of a GNSS and 5G-based spatio-temporal network.

Another approach for GNSS/5G hybrid method is presented by Li et al. [72]. Their algorithm is proposed to address the issue of 5G clock synchronization error affecting positioning by involving using double-differenced observations and introducing reference terminals to mitigate the impact of clock errors on positioning accuracy between terminals and base stations, as well as between base stations themselves. The study then examine the dynamic positioning performance of various combined positioning models in different obstructed environments by integrating 5G double-differenced observations with undifferenced/double-differenced GNSS observations and comparing the results with GNSS-only positioning. The findings indicate that the combined positioning model outperformed a single system in different positioning modes, particularly in obstructed environments.

As presented in this subsection, hybrid and joint techniques may allow to have an improved accuracy, and the ability to deal with complex environments (*e.g.,* indoor). However, these improvements may come at the cost of real-time updates, due to the time taken for the data fusion from different sources [73]. Nevertheless, there are certain use cases (such as asset tracking) where this trade-off is acceptable.

V. Challenges in 5G Positioning

In this section, we address the main challenges that need to be overcome to unlock the full potential of 5G for location-based services and applications. These challenges lie around the capabilities of 5G service devices and the network to run positioning algorithms, the latency requirements of location-based services, massive signaling, scalability, privacy concerns, and emerging use cases such as velocity tracking and 3D positioning. We provide a detailed explanation of each challenge below.

A. UE Capabilities

The primary distinction among 5G services lies in the capabilities of the UE. As a result, there are expected variations in positioning performance across different 5G services. In this subsection, we examine the positioning performance of the UEs according to their operations modes (or states), their bandwidth, and their mobility.

1) UE States: In 5G cellular networks, the UE can be in three different modes of operation, referred to as state transitions. These state transitions include CONNECTED, IDLE, and INACTIVE, and are all part of the Radio Resource Control (RRC) protocol [74].

As illustrated in Fig. 3, RRC_CONNECTED state is designed for efficient data transmission, allowing the UE to keep its transmitter and receiver constantly active. The RRC_IDLE state is a power-saving mode in which the UE does not exchange data and only monitors the paging and broadcast channel to maintain connectivity. When there are no active data transmissions, the UE enters the idle state to conserve battery. To check for new data, the network sends a paging message to the UE. The UE uses Discontinuous Reception (DRX) to periodically wake up and monitor downlink signals, allowing it to turn off its receiver. Two main enhancements to the paging procedure are implemented in 5G: (i) it can be controlled by the RAN, and (ii) a third state is introduced. The RRC_INACTIVE state is designed to decrease the amount of signaling and delay in transitioning from the RRC_IDLE state to the RRC_CONNECTED state. It keeps the Core Network connection active between the 5GC and NG-RAN for both control and user planes, while also minimizing power consumption.

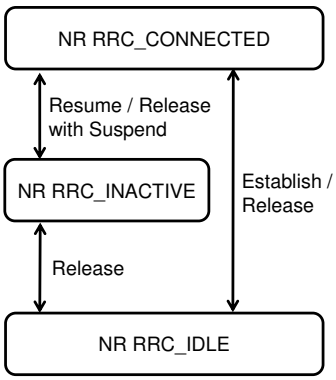

Fig. 3. UE Transitions

Regarding positioning, 3GPP states that some physical-layer measurements can be carried out when the UE is INACTIVE [75]. On the other hand, there are other measurements that can only be conducted when the UE is CONNECTED. This information is important for determining the most suitable positioning method for a certain 5G service. Nevertheless, modern UEs are typically equipped with accelerometers that can detect motion and wake-up the UE from IDLE or INACTIVE state. This capability allows for measurements to be taken regardless of the UE's state. In situations where there is no motion, the last known location of the UE should still be accessible. Ultra low-complexity UEs (i.e., Ambient IoT) are not always connected with the network. Therefore, NR functionality based on the existing RRC states may not be valid and it may need new device state definitions [21].

2) UE Bandwidth: Low bandwidth capability is not a major issue in UE-based positioning (i.e., downlink PRS), as 3GPP introduced Narrowband PRS (NPRS) for NB-IoT with only 180 kHz bandwidth. However, for network-based positioning (i.e., location is computed in the network side), low bandwidth can significantly affect the positioning accuracy. For example, UL-TDOA technique requires that the UE transmits UL-SRS with a certain bandwidth to achieve the desired accuracy. It was observed that at least 10 MHz bandwidth for SRS is required to have fair accuracy [76]. While eMBB/URLLC UEs can transmit the maximum bandwidth (i.e., 100 MHz in FR1), RedCap and mMTC UEs can transmit the signal with up to 20 MHz and 5 MHz, respectively. As a result, frequency hopping technique can be used to transmit the signal over multiple time slots. The idea behind frequency hopping is to continuously switch subcarrier frequencies during the radio transmission in a specific pattern. The main goal of this technique is to minimize the chances of unauthorized interception or jamming of telecommunications. It was evaluated through simulation by industry partners of 3GPP, who found that transmitting 100 MHz SRS from a RedCap UE over 5 hops can achieve similar accuracy to transmitting 100 MHz SRS without frequency hopping [24].

3) UE Mobility: When a UE is not actively communicating and is in motion, real-time positioning and precise accuracy are challenging. The 3GPP has established a specific procedure for selecting a new cell while in the RRC_INACTIVE state [77]. The UE will perform cell re-selection to access the cell that has the strongest radio signal quality. The network provides the UE with a whitelist of neighboring cells that should be considered during signal measurements for potential cell re-selection. Additionally, the network uses various parameters, such as priorities, signal quality thresholds and UE capabilities, to assist the UE in the cell re-selection process.

For network-based positioning, calculating the location after each measurement can result in extra noise. However, if calculations are done after a group of measurements, then selecting the most repetitive values for these measurements can reduce the error. The accuracy here improves at the cost of real-time updates. This approach is suitable for various scenarios like asset tracking, where you can achieve reasonable accuracy and nearly real-time updates (e.g., every 5 minutes).

B. Real-Time RAN Data Collection and Processing

In commercial RAN nowadays, physical-layer measurements are collected and aggregated every 15 minutes to be reported/processed for network-based positioning. Two main types of tracing are used to capture the logs of specific UEs: (i) Cell trace and (ii) User trace. In cell trace, all UEs within a cell site are logged for a specific time period. However, this type of tracing has a major drawback. It is challenging to differentiate the UEs due to a privacy policy that mask certain digits of the International Mobile Equipment Identity (IMEI). This makes it nearly impossible to distinguish UEs from the same manufacturer. Alternatively, an identifier called "UE-Trace-ID" can be used, but it is not practical for more than two UEs due to the large number of "UE-Trace-ID"s generated for each UE every few minutes. On the other hand, user trace can capture data for a single UE across multiple cell

sites. However, the number of UEs that can be traced using this method is limited due to design and cost constraints. The user trace uses International Mobile Subscriber Identifier (IMSI) to distinguish the UEs.

The suggested approach for achieving real-time network-based positioning in commercial RAN involves using Mobile Edge Computing (MEC) [78] to increase the available resources for user tracing and promptly process the reported measurements. The positioning system can also limit the trace to the necessary events (i.e., measurements) only, which helps saving storage space and enables simultaneous tracking of more UEs.

C. Scalability and Signaling Capability

The signaling flow of messages for positioning between the UE and the 5GC currently follows standard signaling protocols established by 3GPP, namely LTE Positioning Protocol (LPP) and NR Positioning Protocol A (NRPPa) over NG Control Interface (NG-C) between 5GC and NG-RAN, and RRC protocol between the NG-RAN and the UE as illustrated in Fig. 4 [79]. NG-C introduces new capabilities to the conventional LTE control plane including network slicing. This enables operators to create dedicated networks for specific applications, improving performance for critical tasks like self-driving cars and virtual reality [80].

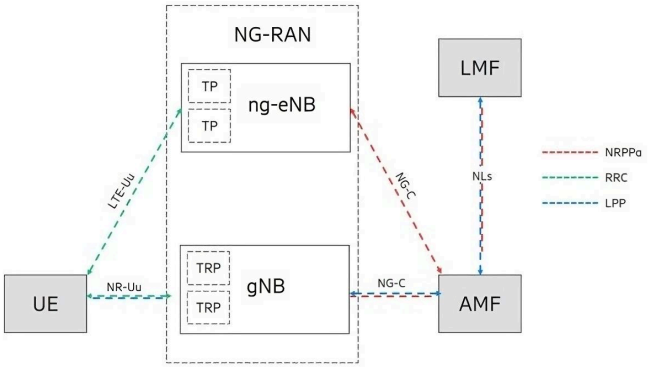

Fig. 4. Involved Protocols in 5G Positioning

In the downlink positioning (UE-based) for mMTC service, Chen et al. [34] employ the DMRS instead of PRS for localizing massive number of UEs using carrier phase technique. The rationale behind using DMRS is that it is a broadcast signal that is received by every UE within the gNB's coverage.

In uplink positioning (network-based), SRS is designed to allow the gNB to receive simultaneously from twelve UEs at each antenna port (up to four antenna ports). Therefore, the gNB can receive up to 48 SRS signals at the same time without any collision, thanks to the cyclic shift configuration in SRS [81]. However, this upper limit has not been tested in previous studies, and further research is needed to determine how to enable simultaneous positioning in a massive network.

Due to the intended low complexity of mMTC service, the hardware capabilities are limited. In network-based positioning, as per 3GPP [79], the UE is required to provide various pieces of information to the LMF to assist in positioning computation such as Reference signal received power and quality, UE Rx-Tx time difference measurement, and LOS/NLOS information. In the context of low-capability 5G services such as RedCap or mMTC, two challenges arise: (i) low-complexity devices may not be capable of transmitting this information, and (ii) the ability to send such a large amount of information to the LMF through uplink signaling is uncertain. Consequently, the standardized signaling for positioning may not be suitable for mMTC positioning and may require modification.

In 3GPP networks, all the NR UE access mechanisms are handled by the gNB. For ultra low-cost UEs (i.e., AIoT), low-complexity 3GPP network illuminators, readers, and/or smartphones are needed, requiring more coordination between network devices to service AIoT UEs which requires a new network protocol design. In addition, due to their small form factor and low-cost requirement, AIoT UEs cannot support full stack access protocol. Thus, simplified protocol design is a key requirement for these devices. Moreover, it will be difficult to register such UEs with the network through subscriber identity module (SIM), which makes it important to establish a simplified form of AIoT UE identification in a 3GPP network [21].

D. UE Positioning in Obstructed Environments

UEs in nomadic mobility frequently encounter obstructed line-of-sight (OLOS), leading to reduced positioning accuracy. Various methods have been suggested to address this issue. This section will present both conventional techniques and the latest advancements in this area.

Range-based positioning methods are more affected by inaccuracies in distance measurements when the line of sight from the UE to the BS is obstructed by an object (see Fig.5). As a result, range-free methods are sometimes employed instead. One such method involves using Multiscale Radio Transmission Power (MRTP), which involves incrementally increasing the level of transmission power and determining the distance based on the smallest scale of received signals based on empirical RSS-distance pairs. This method assumes the presence of multiple gNBs, with at least one being obstructed [82].

Another conventional technique using RSS involves identifying OLOS by using Maximum Likelihood Estimation (MLE) to estimate a preliminary Path Loss Exponent (PLE) parameter for all reference nodes (i.e., gNBs). This is followed by calculating the signal attenuation for each link and determining the average signal attenuation. The next step involves comparing the calculated signal attenuation on each link with the average to determine which link(s) are obstructed. These obstructed links are then removed, and MLE is reapplied to obtain a more accurate PLE parameter. This new PLE parameter is used to repeat the process in order to get a target location estimation [83].

A recent algorithm has been proposed for accurate sequential positioning in environments with multiple signal paths. This algorithm involves using a factor graph formulation and a particle-based sum-product algorithm (SPA) to capture the delay and amplitude statistics of the multi-path radio channel.

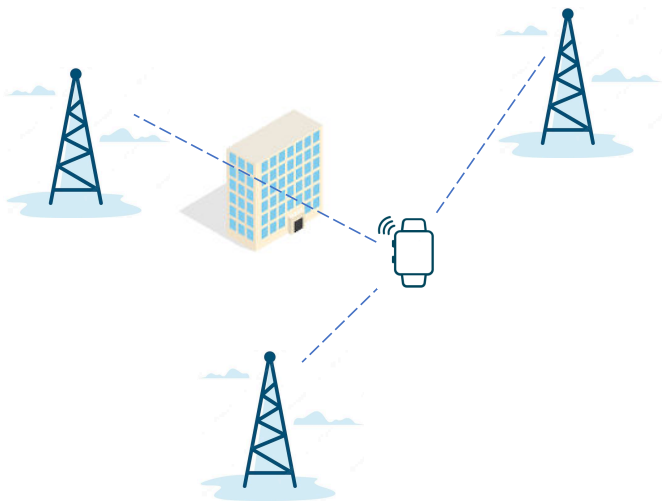

Fig. 5. An Example of Obstructed Line-of-Sight

By doing so, the algorithm can indirectly exploit position-related information from the multi-path components (MPCs) to estimate the UE's position without relying on prior information like floorplan data or training data. This algorithm is capable of providing precise position estimates even in obstructed line-of-sight scenarios [84].

E. Security and Privacy

Security is one of major challenges that are hurdling the development of positioning in general. This can be explained by the numerous threats that it can provoke. According to [85], there are two distinct categories of security-related vulnerabilities that have implications for 5G positioning:

1) **Security Threats:** These vulnerabilities manifest as a spectrum of concerns such as interference, attacks, and errors. Threats like Man-in-the-Middle (MiM) attacks and Distributed Denial-of-Service (DDoS) attacks pose significant risks. Typically, the accuracy of positioning assumes critical significance, particularly for applications that hinge on precise data. Data corruption or manipulation becomes then a tangible threat for these very applications.
2) **Privacy Concerns:** Alongside security threats, privacy is a paramount concern. This dimension unfolds in multifaceted ways. Unauthorized tracking and sharing of user locations can be very harmful. Equally crucial is the concept of the "right to be forgotten", where users have the prerogative to erase location data that has been collected about them. Moreover, the positioning of certain UEs has the potential to unveil user behavior patterns, presenting a unique challenge to uphold user privacy and anonymity. This threat also extends beyond individual users to industrial settings, where the disclosure of operational methodologies through the positioning of the IoT devices can have profound implications for companies.

In particular, 5G positioning methods have their own sets of vulnerabilities. For instance, several ranging/direction techniques, including NR E-CID, AOA, and AOD, present vulnerabilities due to radio signal interference. These vulnerabilities stem from the potential manipulation of the ranging process through various types of attacks, including relay, replay, and amplitude-based attacks. In contrast, TDOA and MC-RTT techniques offer heightened resilience against relay attacks. However, these methods are not immune to distance manipulation vulnerabilities. Challenges such as early detection, late commitments, and overshadowing can introduce inaccuracies in distance estimation, compromising the overall positioning accuracy [86].

In response to these vulnerabilities, several efforts have been made from the research community. [85] identifies the following as the most important approaches to enhance security of 5G positioning:

- **Physical Layer Measurements:** Employing physical layer attributes to enhance security by validating device authenticity and integrity. For instance, [86] propose V-Range as a secure alternative to PRS/SRS, through a distance bounding protocol using shortened OFDM symbols and integrity checks. The receiver layer detects the correctness of the data, and checks for power level consistency.
- **Trustworthiness Metrics:** Metrics that evaluate the trustworthiness of devices and data sources can aid in identifying potential threats.
- **Cryptography:** The deployment of encryption techniques, digital signatures and secure communication protocols can shield against unauthorized access and data tampering. For example, 3GPP has proposed Service Enabler Architecture Layer (SEAL) to enable key management in 5G networks [87].

Amid these efforts, it's noteworthy that various legal frameworks have emerged to address these security and privacy challenges. Legislative measures span diverse jurisdictions and serve as a crucial step towards instilling confidence in the IoT positioning landscape.

Interestingly, the role of positioning encompasses security enhancements. Indeed, it can serve as a safeguard against compromised devices, theft, or unauthorized usage. For instance, it can allow to know if a device has been altered or stolen, according to its position evolution. Moreover, positioning can wield proximity-based authentication, bolstering security protocols and access controls [6].

F. Positioning for Emerging Use Cases

As 5G technology continues to advance, it brings forth a multitude of emerging use cases that extend beyond traditional communication capabilities, and that come along with addition complexities and challenges. Two notable applications gaining momentum are velocity tracking and 3D positioning. We provide in the following a description of the two use cases,

and we review the existing works which tackle these two applications in the literature.

1) Velocity Tracking: Localizing moving trains, or vehicles in general, is a challenging task. The high mobility introduces complexities such as signal Doppler shifts, fast-changing propagation conditions and the requirement for extremely low latency in position updates. Traditional positioning systems may struggle to keep pace with the speed and may lack some precision in the position estimation. Yet, this kind of use-cases is gaining a lot of interest in the last couple of years. 5G, with all its promises in terms of reliability and latency, is naturally a major candidate to fulfil this role. Using technologies like Massive MIMO or beamforming can help to solve the fast-changing propagation conditions issue, or to improve the accuracy of the positioning. We examine in the following recent works tackling the positioning of moving vehicles using 5G.

Shi et al. [88] present a two-stage location-aware beamforming technique for localizing highs-speed trains (HST). The first stage involves a deep learning-based positioning method to determine the positions of train carriages. They train a Back Propagation Neural Network (BPNN) to implement the positioning function, on a large amount of historical data with latitude and longitude information (paired). The second stage involves a hybrid precoding system employed for beamforming with a reduced number of RF chains. QoS considerations with optimizing the power allocation for each carriage are addressed through the formulation of a difference of two convex programming problems. According to the authors, while current GPS positioning accuracy stands at approximately 5 meters, the designed positioning algorithm in their work achieves an accuracy of nearly 8 meters. The authors argue that their method can be used as an alternative positioning method for HST in complex environments.

In [89], Shi et al. also consider a positioning problem of HST in railway wireless network by utilizing the 5G NR PRS. They assume that the train runs along the railroad at a fixed velocity, and receives PRS signals from the BSs deployed on the side of the railroad. To deal with the positioning problem, an Iterative Two-phase Weighted Least Squares (I2WLS) method based on range difference of arrival (RDOA) measurements is proposed. RDOA measurements determine the position of the mobile source by detecting the range difference between the arrival of the signal transmitted by the two BSs. The I2WLS, which is based on a widely used algorithm for estimating regression coefficients [90], linearizes the RDOA equations to pseudo-linear ones, and is then utilized to obtain the train position. The accuracy gap between Root Mean Squared Error (RMSE) of the proposed approach and Cramer-Rao lower bound (CRLB) is small when the RDOA measurements noise level is sufficiently small. Furthermore, the simulation results illustrate that a centimeter-level accuracy can be achieved for small PRS intervals, velocities and base station distances.

In [91], Trivedi et al. present an innovative compressed sensing-based 5G positioning method for the positioning and tracking of HST. They advocate that employing compressed sensing techniques in 5G positioning, combined with an Extended Kalman Filter (EKF), enables precise positioning of HSTs. The proposed method utilizes the Distributed Compressed Sensing Simultaneous Orthogonal Matching Pursuit (DCS-SOMP) algorithm to extract AOD, AOA, and TOA of the LOS path based on received signals. The positioning results are integrated with an EKF for train tracking. The EKF prediction outputs are utilized for beamforming and outlier detection, enhancing the algorithm performance. The proposed algorithm, implemented and tested in a 3GPP specified HST scenario [92], achieves sub-meter positioning accuracy with 4-6 Remote Radio Heads, and an accuracy of 0.34 meters with 95% availability when using 2 Remote Radio Heads.

Beside localizing HSTs, some works focus on localizing fleets of vehicles. In [93], Liu et al. showcase the application of cloud-based cooperative positioning for localizing a vehicle platoon. The objective is to enhance the positioning accuracy of convoy vehicles by leveraging correlated random features such as speed and distance. Employing the Gamma-Markov-Group-Sparse (GMGS) model to capture the stochastic nature of these correlated features, they introduce a collaborative road profile estimation method with Gaussian Processes. This method integrates crowd-sourced local vehicle predictions to refine onboard estimates through the Kalman Filter. Then, they formulate the vehicle platoon cooperative positioning as a sparse Bayesian inference (SBI) problem, that they propose to solve using a Turbo Vehicle Platoon Cooperative positioning (Turbo-VPCL). Results demonstrate improved accuracy and resilience in road profile estimation, compared to GPS and its model uncertainties.

In summary, the presented works address the challenge of precise positioning in dynamic scenarios, particularly focusing on HST and vehicle platoons. The proposed methods involve a range of techniques, including location-aware beamforming, compressed sensing and cloud-based cooperative positioning. In a general way, these approaches aim to overcome limitations associated with GPS accuracy, environmental complexity and stochastic features inherent in high-speed transportation. The results suggest that the proposed methodologies offer a reliable positioning in various operational conditions.

2) 3D Positioning: Many use cases, such as logistics and emergency applications, necessitate 3D positioning. In this section, we examine the latest advancements in 3D positioning within 5G networks.

Lin et al. [94] propose a tensor-based approach for 3D positioning using 5G wideband mmWave massive MIMO system. They initially introduce an extended multidimensional interpolation method to mitigate the frequency-dependence of the array steering vectors. This allows for joint processing of data across the entire frequency band and takes advantage of the high temporal resolution of wideband mmWave signals. Subsequently, they propose a parameter decoupling-based tensor multiparameter estimation algorithm to effectively suppress noise in temporal, spatial, and frequency domains, enabling precise parameter estimation. After that, they present a simplified perturbation term-based method to match the estimated parameters with low complexity. Finally they leverage

the quasi-optical nature of mmWave signals to compute the 3D coordinates of the target. Simulation results show that their proposed approach outperformed ESPRIT algorithm.

Due to the challenge of meeting the Nyquist sampling rate in 5G hardware devices, traditional subspace methods can result in significant false peaks during parameter estimation, leading to a sharp decrease in accuracy. To address this issue, Wu et al. in [95] propose a sparse parameter estimation and 3D positioning approach using the orthogonal matching pursuit algorithm. They first create an L-shaped sparse antenna to form a sparse array manifold. Utilizing 2D AOA and time of flight (ToF), they establish a 3D parameter estimation model and a 3D positioning method based on the direct path. Subsequently, they transform the 3D parameter coupling estimation into two 2D parameter coupling estimations. Simulation results demonstrate that the positioning accuracy in all dimensions is within 20 cm.

In [96], Afifi et al. approach the positioning of UAVs by framing it as an optimization problem. They suggest that the drone can use RSSI measurements from nearby 5G base stations to determine its location without direct interaction with these stations. They address this positioning problem using an appropriate optimization method to find the best solution. Additionally, they introduce a deep supervised learning method to offer a positioning solution with similar accuracy for real-time dynamic applications.

In their work, Nazari et al. [97] focus on solving the problem of localizing a single base station and expand it to estimate the 3D position and orientation of an unsynchronized multi-antenna UE using downlink MIMO-OFDM signals. They use Fisher information analysis to demonstrate that the problem is generally identifiable, as long as there is at least one multipath component in addition to the line-of-sight, even if the position of the corresponding incidence point is initially unknown. They then formulate a maximum likelihood estimation problem to simultaneously estimate the 3D position and orientation of the UE, as well as several nuisance parameters such as the UE clock offset and the positions of incidence points corresponding to the multipath. This maximum likelihood problem involves a high-dimensional non-convex optimization over a combination of Euclidean and non-Euclidean manifolds. To simplify the complex search process, they propose an initial geometric estimate of all parameters, which reduces the problem to a 1-dimensional search over a finite interval. Their numerical results demonstrate the effectiveness of this ad-hoc estimation method, which narrows the gap to the Cramér-Rao bound using the maximum likelihood estimation.

The presented works address the intricate challenge of 3D positioning in 5G scenarios. They encompass different approaches such as tensor-based parameter estimation, sparse antenna design, optimization-based UAV positioning, and a complex optimization framework for 3D UE positioning. These diverse methods aim to overcome challenges related to hardware limitations, false peaks in traditional subspace methods, and the identification of parameters in complex non-convex optimization problems. Results that these approaches efficiently overcome these challenges, through an improved accuracy and reliability in 3D positioning.

VI. Conclusion

With the extreme widespread of 5G networks deployment, an important interest has been put into using it for positioning. This article presents the various 5G services and explores how positioning strategies can be customized to cater to distinct requirements and device capabilities. It delves into the intricacies of 5G positioning architecture, techniques, and requirements as defined in recent 3GPP releases. It also delves into emerging positioning methodologies like sidelink positioning, carrier phase, RIS-aided, machine learning-aided, massive MIMO, beamforming, and hybrid techniques, drawing insights from recent literature. Finally, it highlights both the practical challenges entailed in implementing positioning within 5G networks, and on emerging use cases such as velocity tracking and 3D positioning.

The surveyed articles show that these different techniques can allow to overcome serious challenges in positioning, especially NLOS paths and indoor environments. However, each one has its own set of pros and cons. Typically, sidelink positioning facilitates direct device-to-device communication, minimizing latency but sacrificing range and accuracy, while carrier phase offers high precision but demands sophisticated hardware and is sensitive to signal reflections. RIS enhance coverage through passive beamforming, yet their require a complex deployment of a large number of controllable elements, which can be a significant barrier to widespread adoption, particularly in cost-sensitive applications. Machine learning-aided techniques adapt to dynamic environments, handling NLOS scenarios, but require substantial training data and time as well. Massive MIMO boosts spectral efficiency but relies on complex processing and hardware. Beamforming directs signals for improved coverage but is susceptible to interference. Finally, hybrid techniques, combining the strengths of various methods, aim to strike a balance between accuracy, coverage, and cost, though at the expense of increased complexity. From that, we see that the choice of technique depends on the specific application needs and deployment considerations in the targeted use case.

To conclude, unlocking the full potential of 5G for positioning faces serious challenges that demand innovative solutions. The variability in UE capabilities require advancements in device technologies and standardized protocols for consistent and accurate positioning across diverse devices. Also, overcoming signal propagation challenges in obstructed environments, like urban canyons or indoor spaces, calls for innovative signal processing and adaptive algorithms. Scalability is a pivotal challenge, requiring solutions that can efficiently manage the increasing number of connected devices within the expansive 5G network. Finally, security also emerges as a critical concern, necessitating robust encryption, secure protocols, and stringent access controls to safeguard location data.

List of Acronyms

The list of acronyms is provided in Table II.

TABLE II
LIST OF ACRONYMS

3D	Three Dimensions	**3GPP**	The Third Generation Partnership Project	**5G**	Fifth Generation
5GC	5G Core Network	**AI**	Artificial Intelligence	**API**	Application Programming Interface
ARMA	Auto-Regressive Moving Average	**ARP**	Antenna Reference Point	**AOA**	Angle of Arrival
AOD	Angle of Departure	**BLE**	Bluetooth Low Energy	**BPNN**	Back Propagation Neural Network
BS	Base Station	**CDF**	Cumulative Distribution Function	**CIS**	Continuous Intelligent Surface
CLP	Collaborative Localization Protocol	**CNN**	Convolutional Neural Network	**CRB**	Cramer-Rao Bound
CRLB	Cramer-Rao Lower Bound	**CSI**	Channel State Information	**D2D**	Device to Device
DCGP	Deep Convolutional Gaussian Process	**DDoS**	Distributed Denial-of-Service	**DL**	Downlink
DMRS	DeModulation Reference Signal	**DRX**	Discontinuous Reception	**E-CID**	Enhanced Cell ID
eMBB	Enhanced Mobile Broadband	**EKF**	Extended Kalman Filter	**ESPRIT**	Estimation of Signal Parameters via Rotational Invariant Technique
FR1	Frequency Range 1	**GMGS**	Gamma-Markov-Group-Sparse	**gNB**	5G NodeB
GNSS	Global Navigation Satellite System	**GPS**	Global Positioning System	**HST**	High-Speed Train
I2WLS	Iterative Two-phase Weighted Least Squares	**IMEI**	International Mobile Equipment Identity	**IMSI**	International Mobile Subscriber Identifier
IoT	Internet of Things	**JSC**	Joint Sensing and Communication	**kNN**	K-Nearest Neighbors
LCS	Location Service	**LMF**	Location Management Function	**LOS**	Line of Sight
LPP	LTE Positioning Protocol	**LPWA**	Low Power Wide Area	**LRM**	Location-Related Measurement
LSE	Least Squares Error	**LTE-M**	Long Term Evolution Machine Type Communication	**MAP**	Maximum A Posteriori
MC-RTT	Multi-Cell Round-Trip Time	**MCL**	Maximum Coupling Loss	**MEC**	Mobile Edge Computing
MIMO	Multi-Input Multi-Output	**MISO**	Multi-Input Single-Output	**ML**	Machine Learning
MLE	Maximum Likelihood Estimation	**mMTC**	Massive Machine Type Communication	**mmWave**	Millimeter Wave
MPC	Multi-Path Component	**MRTP**	Multiscale Radio Transmission Power	**MUSIC**	Multiple Signal Classification
MiM	Man-in-the-Middle	**NB-IoT**	Narrowband IoT	**NG-C**	Next Generation Control Plane
NG-RAN	Next Generation Radio Access Network	**NLOS**	Non Line of Sight	**NPRS**	Narrowband Positioning Reference Signal
NR	New Radio	**NRPPa**	NR Positioning Protocol A	**NSA**	Non Stand Alone
OFDM	Orthogonal Frequency Division Multiplexing	**OLOS**	Obstructed Line of Sight	**PDOA**	Phase Difference of Arrival
PLE	Path Loss Exponent	**PRISMA**	Preferred Reporting Items for Systematic Reviews and Meta-Analysis	**PRS**	Positioning Reference Signal
QoS	Quality of Service	**RAN**	Radio Access Network	**UAV**	Unmanned Aerial Vehicles
RDOA	Range Difference of Arrival	**RF**	Radio Frequency	**RIS**	Reconfigurable Intelligent Surface
RLP	Round-trip Localization Protocol	**RMSE**	Root Mean Squared Error	**RRC**	Radio Resource Control
RSRP	Reference Signal Received Power	**RSSI**	Received Signal Strength Indicator	**RedCap**	Reduced Capability
SA	Stand Alone	**SEAL**	Service Enabler Architecture Layer	**SNR**	Signal to Noise Ratio
SPA	Sum-Product Algorithm	**SRS**	Sounding Reference Signal	**SRUSF**	Square Root Unscented Stable Filter
SVM	Support Vector Machine	**TDOA**	Time Difference of Arrival	**UE**	User Equipment
UL	Uplink	**URLLC**	Ultra-Reliable Low Latency Communication	**V2X**	Vehicle to Everything
VPCL	Vehicle Platoon Cooperative Localization	**Wi-Fi**	Wireless Fidelity		

REFERENCES

[1] P. S. Farahsari, A. Farahzadi, J. Rezazadeh, and A. Bagheri, "A survey on indoor positioning systems for iot-based applications," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7680–7699, 2022.

[2] Y. Li, Y. Zhuang, X. Hu, Z. Gao, J. Hu, L. Chen, Z. He, L. Pei, K. Chen, M. Wang *et al.*, "Toward location-enabled iot (le-iot): Iot positioning techniques, error sources, and error mitigation," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4035–4062, 2020.

[3] G. Bhatia and N. Jain, "A survey on localization in internet of things: Techniques, approaches, technologies and challenges," in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*. IEEE, 2022, pp. 596–604.

[4] P. S. Varma and V. Anand, "Indoor localization for iot applications: review, challenges and manual site survey approach," in *2021 IEEE Bombay Section Signature Conference (IBSSC)*. IEEE, 2021, pp. 1–6.

[5] T. Janssen, A. Koppert, R. Berkvens, and M. Weyn, "A survey on iot positioning leveraging lpwan, gnss and leo-pnt," *IEEE Internet of Things Journal*, 2023.

[6] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[7] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo, and G. Seco-Granados, "Survey of Cellular Mobile Radio Mocalization Methods: From 1G to 5G," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2017.

[8] C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola, and C. Fischione, "A survey of enabling technologies for network localization, tracking, and navigation," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3607–3644, 2018.

[9] J. A. del Peral-Rosado, G. Granados, R. Raulefs, E. Leitinger, S. Grebien, T. Wilding, D. Dardari, E. Lohan, H. Wymeersch, J. Floch *et al.*,

"Whitepaper on new localization methods for 5g wireless systems and the internet-of-things," in *White Paper of the COST Action CA15104 (IRACON)*. COST Action CA15104, IRACON, 2018, pp. 1–27.

[10] N. Saeed, H. Nam, T. Y. Al-Naffouri, and M.-S. Alouini, "A state-of-the-art survey on multidimensional scaling-based localization techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3565–3583, 2019.

[11] F. Wen, H. Wymeersch, B. Peng, W. P. Tay, H. C. So, and D. Yang, "A survey on 5g massive mimo localization," *Digital Signal Processing*, vol. 94, pp. 21–28, 2019.

[12] F. Mogyorósi, P. Revisnyei, A. Pašić, Z. Papp, I. Törös, P. Varga, and A. Pašić, "Positioning in 5G and 6G Networks-A Survey," *Sensors*, vol. 22, no. 13, p. 4757, 2022.

[13] S. E. Trevlakis, A.-A. A. Boulogeorgos, D. Pliatsios, J. Querol, K. Ntontin, P. Sarigiannidis, S. Chatzinotas, and M. Di Renzo, "Localization as a key enabler of 6G wireless systems: A comprehensive survey and an outlook," *IEEE Open Journal of the Communications Society*, 2023.

[14] A. Behravan, V. Yajnanarayana, M. F. Keskin, H. Chen, D. Shrestha, T. E. Abrudan, T. Svensson, K. Schindhelm, A. Wolfgang, S. Lindberg *et al.*, "Positioning and sensing in 6G: Gaps, challenges, and opportunities," *IEEE Vehicular Technology Magazine*, 2022.

[15] T. Ma, Y. Xiao, X. Lei, L. Zhang, Y. Niu, and G. K. Karagiannidis, "Reconfigurable Intelligent Surface Assisted Localization: Technologies, Challenges, and the Road Ahead," *IEEE open j. Commun. Soc.*, 2023.

[16] 3GPP, "Study on NR Positioning Enhancements," 3rd Generation Partnership Project, Technical Report (TR) 38.857, March 2021, version 17.0.0.

[17] A. Toskala and Y. Lair, "5G-advanced shifts to the next gear with release 19," Jun 2023.

[18] 3GPP, "Study on support of reduced capability NR devices," 3rd Generation Partnership Project, Technical Report (TR) 38.875, March 2021, version 17.0.0.

[19] 3GPP, "Study on further NR RedCap UE complexity reduction," 3rd Generation Partnership Project, Technical Report (TR) 38.865, September 2022, version 18.0.0.

[20] 3GPP, "NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone," 3rd Generation Partnership Project, Technical Specification (TS) 38.101-2, September 2023, version 18.3.0.

[21] M. M. Butt and N. R. Mangalvedhe, "Ambient IoT: A missing link in 3GPP IoT Devices Landscape," 11 2023.

[22] 3GPP, "5G System Location Services," 3rd Generation Partnership Project, Technical Specification (TS) 23.273, September 2023, version 18.3.0.

[23] 3GPP, "Study on NR Positioning Support," 3rd Generation Partnership Project, Technical Report (TR) 38.855, March 2019, version 16.0.0.

[24] 3GPP, "Study on Expanded and Improved NR Positioning," 3rd Generation Partnership Project, Technical Report (TR) 38.859, December 2022, version 18.0.0.

[25] W. S. Jeon, S. B. Seo, and D. G. Jeong, "Effective Frequency Hopping Pattern for ToA Estimation in NB-IoT Random Access," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 10 150–10 154, 2018.

[26] H. Bello, Z. Xiaoping, R. Nordin, and J. Xin, "Advances and opportunities in passive wake-up radios with wireless energy harvesting for the internet of things applications," *Sensors*, vol. 19, no. 14, 2019.

[27] W. Y. Al-Rashdan and A. Tahat, "A Comparative Performance Evaluation of Machine Learning Algorithms for Fingerprinting-Based Localization in DM-MIMO Wireless Systems Relying on Big Data Techniques," *IEEE Access*, vol. 8, pp. 109 522–109 534, 2020.

[28] A. Liberati, D. G. Altman, J. Tetzlaff, C. Mulrow, P. C. Gøtzsche, J. P. Ioannidis, M. Clarke, P. J. Devereaux, J. Kleijnen, and D. Moher, "The PRISMA Statement for Reporting Systematic Reviews and Meta-analyses of Studies that Evaluate Health Care Interventions: Explanation and Elaboration," *Annals of internal medicine*, vol. 151, no. 4, pp. W–65, 2009.

[29] K. Ganesan, "5G Advanced: Sidelink Evolution," *IEEE Commun. Stand. Mag.*, vol. 7, no. 1, pp. 58–63, 2023.

[30] Y. Lu, M. Koivisto, J. Talvitie, E. Rastorgueva-Foi, M. Valkama, and E. S. Lohan, "Cooperative positioning system for industrial IoT via mmWave device-to-device communications," in *2021 IEEE 93rd VTC2021-Spring*. IEEE, 2021, pp. 1–7.

[31] M. Hunukumbure, O. Y. Kolawole, and D. M. Gutierrez-Estevez, "Optimising UWB based Location Tracking in Smartphones through the Support of 5G," in *2022 IEEE ICCE*. IEEE, 2022, pp. 1–6.

[32] B. Panzner, T. Şahin, and P. Keshavamurthy, "Coexistence of 5G Sidelink Communication and 5G Sidelink Positioning," in *2022 Inter. Symp. ELMAR*. IEEE, 2022, pp. 77–80.

[33] A. Fouda, R. Keating, and H.-S. Cha, "Toward cm-Level Accuracy: Carrier Phase Positioning for IIoT in 5G-Advanced NR Networks," in *2022 IEEE 33rd Annual Intern. Symp. on PIMRC*, 2022, pp. 782–787.

[34] L. Chen, X. Zhou, F. Chen, L.-L. Yang, and R. Chen, "Carrier Phase Ranging for Indoor Positioning With 5G NR Signals," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10 908–10 919, 2022.

[35] S. Fan, W. Ni, H. Tian, Z. Huang, and R. Zeng, "Carrier Phase-Based Synchronization and High-Accuracy Positioning in 5G New Radio Cellular Networks," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 564–577, 2022.

[36] C. Jin, W. P. Tay, K. Zhao, K. Voon Ling, J. Lu, and Y. Wang, "A Sub-meter Accurate Positioning using 5G Double-difference Carrier Phase Measurements," in *2023 IEEE/ION PLANS*, 2023, pp. 1176–1183.

[37] J. Li, M. Liu, S. Shang, X. Gao, and J. Liu, "Carrier Phase Positioning Using 5G NR Signals Based on OFDM System," in *2022 IEEE 96th VTC2022-Fall*, 2022, pp. 1–5.

[38] W. Kim, J. Park, and J. Cho, "Implementation of Carrier Phase Positioning for 5G OFDM System," in *2022 13th Intern. Conf. on ICTC*, 2022, pp. 2058–2061.

[39] J. Khalife and Z. M. Kassas, "On the Achievability of Submeter-Accurate UAV Navigation With Cellular Signals Exploiting Loose Network Synchronization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4261–4278, 2022.

[40] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE transactions on wireless communications*, vol. 18, no. 8, pp. 4157–4170, 2019.

[41] E. Basar, I. Yildirim, and F. Kilinc, "Indoor and outdoor physical channel modeling and efficient positioning for reconfigurable intelligent surfaces in mmWave bands," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8600–8611, 2021.

[42] O. Popoola, S. Ansari, R. I. Ansari, L. Mohjazi, S. A. Hassan, N. Aslam, Q. H. Abbasi, and M. A. Imran, "IRS-Assisted Localization for Airborne Mobile Networks," *Autonomous Airborne Wireless Networks*, pp. 141–156, 2021.

[43] R. Liu, M. Jian, and W. Zhang, "A TDoA based Positioning Method for Wireless Networks assisted by Passive RIS," in *2022 IEEE GC Wkshps*. IEEE, 2022, pp. 1531–1536.

[44] Z. Zhang, L. Wu, J. Dang, B. Zhu, and L. Wang, "Multiple RSS Fingerprint Based Indoor Localization in Ris-Assisted 5g Wireless Communication System," *ISPRS Archives*, vol. 46, pp. 287–292, 2022.

[45] Y. Lu, H. Chen, J. Talvitie, H. Wymeersch, and M. Valkama, "Joint RIS Calibration and Multi-User Positioning," in *2022 IEEE 96th VTC2022-Fall*. IEEE, 2022, pp. 1–6.

[46] Z. Wang, Z. Liu, Y. Shen, A. Conti, and M. Z. Win, "Source Localization with Intelligent Surfaces," in *ICC 2022*. IEEE, 2022, pp. 895–900.

[47] Y. Zhao and D. Shrestha, "Uncertainty in position estimation using machine learning," in *2021 Inter. Conf. on IPIN*. IEEE, 2021, pp. 1–7.

[48] A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "First responders got wings: UAVs to the rescue of localization operations in beyond 5G systems," *IEEE Commun. Mag.*, vol. 59, no. 11, pp. 28–34, 2021.

[49] Y. Ruan, L. Chen, X. Zhou, Z. Liu, X. Liu, G. Guo, and R. Chen, "iPos-5G: Indoor Positioning via Commercial 5G NR CSI," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8718–8733, 2022.

[50] G. Torsoli, M. Z. Win, and A. Conti, "Blockage intelligence in complex environments for beyond 5G localization," *IEEE J. Sel. Areas Commun.*, 2023.

[51] G. Torsoli, M. Z. Win, and A. Conti, "Selection of reference base station for TDOA-based localization in 5G and beyond IIoT," in *2022 IEEE GC Wkshps*. IEEE, 2022, pp. 317–322.

[52] Z. Liu, L. Chen, X. Zhou, Z. Jiao, G. Guo, and R. Chen, "Machine learning for time-of-arrival estimation with 5G signals in indoor positioning," *IEEE Internet Things J.*, 2023.

[53] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive mimo for next generation wireless systems," *IEEE communications magazine*, vol. 52, no. 2, pp. 186–195, 2014.

[54] O. Alamu, B. Iyaomolere, and A. Abdulrahman, "An overview of massive mimo localization techniques in wireless cellular networks: Recent advances and outlook," *Ad Hoc Networks*, vol. 111, p. 102353, 2021.

[55] A. Sellami, L. Nasraoui, and L. Najjar, "Neighbor-assisted localization for massive MIMO 5G systems," in *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*. IEEE, 2021, pp. 503–509.

[56] A. Sellami, L. Nasraoui, and L. Najjar, "Outdoor neighbor-assisted localization algorithm for massive mimo systems," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–5.

[57] V. Singh, A. A. Masal, J. K. Milleth, and B. Ramamurthi, "High Precision Positioning using Multi-cell Massive MIMO system for 5G and beyond," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2021, pp. 1234–1240.

[58] R. Roy, A. Paulraj, and T. Kailath, "Esprit–a subspace rotation approach to estimation of parameters of cisoids in noise," *IEEE transactions on acoustics, speech, and signal processing*, vol. 34, no. 5, pp. 1340–1342, 1986.

[59] J. Gante, L. Sousa, and G. Falcao, "Dethroning GPS: Low-power accurate 5G positioning systems using machine learning," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 2, pp. 240–252, 2020.

[60] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "Low-complexity accurate mmwave positioning for single-antenna users based on angle-of-departure and adaptive beamforming," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 4866–4870.

[61] Z. Abu-Shaban, H. Wymeersch, T. Abhayapala, and G. Seco-Granados, "Single-anchor two-way localization bounds for 5G mmWave systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6388–6400, 2020.

[62] H. Seo, H. Kim, T. Kim, and D. Hong, "Accurate positioning using beamforming," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2021, pp. 1–4.

[63] M. Koivisto, J. Talvitie, E. Rastorgueva-Foi, Y. Lu, and M. Valkama, "Channel parameter estimation and TX positioning with multi-beam fusion in 5G mmWave networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3192–3207, 2021.

[64] X. Wang, M. Patil, C. Yang, S. Mao, and P. A. Patel, "Deep convolutional gaussian processes for mmwave outdoor localization," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 8323–8327.

[65] L. Pucci, E. Paolini, and A. Giorgetti, "System-level analysis of joint sensing and communication based on 5G new radio," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2043–2055, 2022.

[66] K. Hu, W. Li, Q. Lu, C. Shi, B. Zhao, and Y. Shen, "SRS-based Wideband AoA Estimation Method in 5G New Radio," in *2023 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2023, pp. 1–5.

[67] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE transactions on antennas and propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[68] Z. Zhang, S. Kang, and X. Zhang, "High precision positioning algorithm based on carrier phase and time of arrival," *IET Communications*, vol. 15, no. 20, pp. 2575–2585, 2021.

[69] Y. Liang, L. Li, T. Pang, P. Cao, and X. Zhu, "Hybrid positioning solution combining 5G, bluetooth, and terminal motion sensor," in *5th International Conference on Information Science, Electrical, and Automation Engineering (ISEAE 2023)*, T. Lei, Ed., vol. 12748, International Society for Optics and Photonics. SPIE, 2023, p. 127480I.

[70] M. Alghisi and L. Biagi, "Positioning with GNSS and 5G: Analysis of Geometric Accuracy in Urban Scenarios," *Sensors*, vol. 23, no. 4, p. 2181, Feb. 2023.

[71] J. Liu, Z. Deng, E. Hu, Y. Huang, X. Deng, Z. Zhang, Z. Ding, and B. Liu, "GNSS-5G Hybrid Positioning Based on Joint Estimation of Multiple Signals in a Highly Dependable Spatio-Temporal Network," *Remote Sensing*, vol. 15, no. 17, p. 4220, Aug. 2023.

[72] F. Li, R. Tu, L. Zeng, S. Zhang, M. Liu, and X. Lu, "Integrated positioning with double-differenced 5G and undifferenced/double-differenced GPS," *Measurement*, vol. 218, p. 113114, 2023.

[73] L. Bai, C. Sun, A. G. Dempster, H. Zhao, J. W. Cheong, and W. Feng, "GNSS-5G hybrid positioning based on multi-rate measurements fusion and proactive measurement uncertainty prediction," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–15, 2022.

[74] 3GPP, "NR Radio Resource Control (RRC) Protocol Specification," 3rd Generation Partnership Project, Technical Specification (TS) 38.331, March 2023, version 17.4.0.

[75] 3GPP, "5G NR Physical Layer Measurements," 3rd Generation Partnership Project, Technical Specification (TS) 38.215, March 2023, version 17.3.0.

[76] T. A. H. Bressner, "Development and Evaluation of UTDoA as a Positioning Method in LTE," Master's thesis, KYH, Sweden, 2015.

[77] 3GPP, "UE procedures in Idle mode and RRC Inactive state," 3rd Generation Partnership Project, Technical Specification (TS) 38.304, April 2023, version 17.4.0.

[78] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, 2020.

[79] 3GPP, "User Equipment Positioning in NG-RAN," 3rd Generation Partnership Project, Technical Specification (TS) 38.305, March 2023, version 17.4.0.

[80] 3GPP, "NR and NG-RAN Overall Description," 3rd Generation Partnership Project, Technical Specification (TS) 38.305, March 2023, version 17.4.0.

[81] B. Ghimire, E. Eberlein, and M. Alawieh, "Reference Signal Enhancement in 5G for Extended Coverage in Multi-User Scenarios," in *2022 IEEE 96th VTC2022-Fall*, 2022, pp. 1–6.

[82] W. Chen, X. Li, and J. Rong, *Sensor Localization in an Obstructed Environment*. Springer Berlin Heidelberg, 2005, p. 49–62.

[83] K. Tong, X. Wang, A. Khabbazibasmenj, and A. Dounavis, "RSS-Based Localization in Obstructed Environment with Unknown Path Loss Exponent," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, 2014, pp. 1–5.

[84] A. Venus, E. Leitinger, S. Tertinek, and K. Witrisal, "A graph-based algorithm for robust sequential localization exploiting multipath for obstructed-los-bias mitigation," *IEEE Transactions on Wireless Communications*, p. 1–1, 2023.

[85] E. S. Lohan, A. Alén-Savikko, L. Chen, K. Järvinen, H. Leppäkoski, H. Kuusniemi, and P. Korpisaari, "5G Positioning: Security and Privacy Aspects," *A Comprehensive Guide to 5G Security*, pp. 281–320, 2018.

[86] A. K. Dutta and M. Singh, "Challenges and Opportunities in Enabling Secure 5G Positioning," in *2023 15th Inter. Conf on COMSNETS*. IEEE, 2023, pp. 498–504.

[87] 3GPP, "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows," 3rd Generation Partnership Project, Technical Specification (TS) 23.434, June 2023, version 18.5.0.

[88] X. Shi, Y. Ma, L. Liu, and Y. Han, "A location-aware hybrid beamforming system for high speed trains," in *2021 13th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2021, pp. 1–5.

[89] J. Shi, G. Zhang, Y. Lin, F. Li, and C. Shen, "Positioning of high-speed trains based on prs," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2022, pp. 578–583.

[90] P. W. Holland and R. E. Welsch, "Robust regression using iteratively

reweighted least-squares," *Communications in Statistics-theory and Methods*, vol. 6, no. 9, pp. 813–827, 1977.

[91] M. A. Trivedi and J. H. van Wyk, "Localization and Tracking of High-speed Trains Using Compressed Sensing Based 5G Localization Algorithms," in *2021 IEEE 24th International Conference on Information Fusion (FUSION)*. IEEE, 2021, pp. 1–8.

[92] E. TR, "5G: Study on scenarios and requirements for next generation access technologies (3GPP TR 38.913 version 14.2.0 release 14)," *ETSI TR 138 913*, 2017.

[93] A. Liu, L. Lian, V. Lau, G. Liu, and M.-J. Zhao, "Cloud-assisted cooperative localization for vehicle platoons: A turbo approach," *IEEE Transactions on Signal Processing*, vol. 68, pp. 605–620, 2020.

[94] Z. Lin, T. Lv, J. A. Zhang, and R. P. Liu, "Tensor-based High-Accuracy Position Estimation for 5G mmWave Massive MIMO Systems," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[95] X. Wu, S. Gui, L. Zhou, Y. Wu, F. Yan, and Z. Tian, "Indoor Single Station 3D Localization Based on L-shaped Sparse Array," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–5.

[96] G. Afifi and Y. Gadallah, "Unmanned Aerial Vehicles 3-D Autonomous Outdoor Localization: A Deep Learning Approach," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2022, pp. 908–913.

[97] M. A. Nazari, G. Seco-Granados, P. Johannisson, and H. Wymeersch, "mmWave 6D Radio Localization With a Snapshot Observation From a Single BS," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 7, pp. 8914–8928, 2023.

AUTHORS' BIOGRAPHY

Mohammad Abuyaghi (Graduate Student Member, IEEE) is a PhD student in Electrical and Computer Engineering at the University of Waterloo, Canada. He is currently conducting research on 5G IoT positioning at the Wireless Sensors and Devices Laboratory. Mohammad holds a B.Sc. degree from the University of Jordan, which he received in 2007, and an M.A.Sc. degree from Dalhousie University, which he obtained in 2021. Prior to pursuing his master's degree, he worked for 12 years in the telecom industry as a network engineer in the capacity of planning, design, project management, and operation at Shaw Communications, Eastlink, Huawei Technologies, and Umniah. His research interests include IoT, 5G, Wireless Networks, and Physical-Layer Security.

Samir Si-Mohammed is a Postdoctoral Researcher at the ICube lab of University of Strasbourg (France). He graduated as a PhD in Computer Science from École Normale Supérieure (ENS) de Lyon (France) in 2023, and as a Computer Science Engineer from the Higher National School of Computer Science (ESI) of Algiers (Algeria) in 2020. He did his final year internship at EURECOM in Sophia-Antipolis (France). He was a visiting scholar at the Electrical and Computer Engineering department of the University of Waterloo (Canada) during Summer 2023. His research interests include IoT, 5G, Wireless Networks, Digital Twins and Machine Learning.

George Shaker (Senior Member, IEEE) is the lab director of the Wireless Sensors and Devices Laboratory at the University of Waterloo-Schlegel Research Institute for Aging. He is an (Adjunct + Research) professor with University of Waterloo at the Department of Electrical and Computer Engineering as well as the Department of Mechanical and Mechatronics Engineering. Previously, he was an NSERC scholar at Georgia Institute of Technology. Dr. Shaker also held multiple roles with RIM's (BlackBerry). With close to twenty years of industrial experience in technology, and more than eight years as a faculty member leading project related to the application of wireless sensor systems for healthcare, automotives, and unmanned aerial vehicles, Prof. Shaker has many design contributions in commercial products available from startups and multinationals. A sample list includes Google, COM DEV, Honeywell, Blackberry, Konka, DBJ, Enice, Spark Tech Labs, China Mobile, TriL, Bionym, Lyngsoe Systems, ON Semiconductors, Ecobee, Medella Health, NERV Technologies, Novela, Thalmic Labs, North, General Dynamics Land Systems, General Motors, Toyota, Maple Lodge Farms, Rogers Communications, and Purolator.

Catherine Rosenberg (Fellow, IEEE) is a Professor in Electrical and Computer Engineering at the University of Waterloo since 2004. Since June 2010, she holds the Canada Research Chair in the Future Internet. She was elected an IEEE Fellow for contributions to resource management in wireless and satellite networks on 2011 and was elected a Fellow of the Canadian Academy of Engineering in 2013. In April 2018, she became the Cisco Research Chair in 5G Systems. Additionally, Professor Rosenberg was on the Scientific Advisory Board of the Orange Group (France-Telecom) from 2007 to mid 2015. She became its president from January 2013 to mid 2015. She also became the president of the Scientific Advisory Board of the French IRT (Research and Technology Institute) BCOM on multimedia and networking in 2014. Her research expertise lies in wireless networks, multimedia, traffic engineering and energy systems. Her work in wireless networks includes 5G, IoT, and generally resource management. Professor Rosenberg's multimedia research encompasses CDN, peer-to-peer, and real-time streaming. Her research in traffic engineering focuses on quality of service, network optimization and game theory and pricing. Prof. Rosenberg's research in energy systems includes smart grid design, storage modeling, renewable integration, and data analysis.