Positioning in 5G Networks: Emerging Techniques, Use Cases, and Challenges

Mohammad Abuyaghi, Samir Si-Mohammed, George Shaker, Catherine Rosenberg

Positioning in 5G Networks: Emerging Techniques, Use Cases, and Challenges

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

***Abstract*—As 5G networks proliferate globally, the need for accurate, reliable, and scalable positioning solutions has become increasingly critical across industries such as IoT, healthcare, and autonomous systems. This paper comprehensively reviews current and emerging positioning techniques within 5G, exploring the advancements enabled by sidelink communication, Reconfigurable Intelligent Surfaces (RIS), machine learning, and massive MIMO. We examine the evolution of 5G positioning as defined by key 3GPP releases, and provide a comparative analysis of the techniques in terms of accuracy, cost, and robustness. The review also highlights key challenges, including non-line-of-sight (NLOS) environments, real-time data processing, and security concerns, which must be addressed for widespread adoption. Finally, we discuss future directions for 5G-Advanced and 6G positioning technologies, offering insights into potential improvements and the ongoing evolution of the field.**

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

I. Introduction

RECENT years have seen 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 showcases how connectivity is revolutionizing various aspects of our daily lives. This paper focuses on positioning in 5G and beyond, discussing emerging technologies and their applications.

Positioning has been extensively studied over the past thirty years, driven by the demand for location-based services across various applications. Researchers have proposed various techniques for precise positioning, considering both accuracy requirements and device capabilities. For 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. Moreover, several industries such as healthcare and autonomous driving are increasingly dependent on accurate positioning. In healthcare, real-time location data is crucial for monitoring equipment, patients, and staff, improving efficiency and safety. In autonomous driving, precise and low-latency positioning is essential for ensuring safety and operational efficiency.

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. However, GNSS struggles with providing accurate indoor positioning, especially within buildings, while Wi-Fi and Bluetooth exhibit limited performance outdoors and with moving devices, making them less suitable for dynamic environments. More recently, employing 5G New Radio (NR) cellular networks for positioning has become a topic of significant interest. 5G cellular technology seems to offer the ideal tradeoff both indoors and outdoors, even with mobile objects. Furthermore, 5G is designed to accommodate high device density and global needs, which are beneficial for massive IoT. Advanced techniques such as Massive MIMO, Reconfigurable Intelligent Surfaces (RIS), and machine learning (ML)-aided positioning are contributing to substantial improvements in accuracy, efficiency, and reliability, especially in complex environments.

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 several positioning methods. Still, this domain is in constant evolution, and researchers have directed their attention toward proposing novel positioning solutions in complex scenarios, especially where a direct line-of-sight (LOS) between the device and the interconnected node is unavailable. Nevertheless, its challenges such as achieving low latency, providing real-time data, and ensuring the security and privacy of positioning information remain critical challenge obstacles that need to be addressed. Techniques like sidelink positioning or Reconfigurable Intelligent Surface (RIS)-aided positioning, or even hybrid techniques that combine multiple technologies to enhance positioning performance in complex environments, have also been extensively explored in the literature, for a

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).

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 too specific to a particular technology (e.g., Massive MIMO). The paper most closely aligned with our objectives is [12]. It is a recent and very valuable survey on cellular positioning, with a strong focus on machine learning-aided techniques for localization. However, it does not include the latest release of 3GPP (Rel-18), and it misses out on important information about recent positioning techniques (*e.g.,* Sidelink). Finally, several recent surveys are claiming to be on 6G positioning [13]–[15]. Since 3GPP has not yet published a release on 6G, all those surveys are exploratory.

To address these gaps, this paper offers a thorough and current examination of 5G cellular positioning, emphasizing a diverse array of use cases, including several in IoT. It 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. It is worth noting that for each emerging positioning technique, we designate one already published survey as a reference point. Then, we specifically focus on papers not covered by that survey, to ensure that we minimize redundancy and that we contribute original information to the existing body of knowledge. Specifically, the major contributions of this paper are the following:

- Summarize the latest advancements in 3GPP releases for positioning, with a focus on the characteristics of the different types of devices and the positioning requirements of the different 5G use cases.
- Provide a comprehensive review of the 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 and the state-of-the-art literature trying to address them.

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. In Section IV, we review emerging positioning techniques such as carrier phase, sidelink, RIS-aided, and ML-aided positioning, followed by emerging use cases in Section V. Finally, we discuss the practical challenges of implementing IoT positioning techniques in commercial and private 5G networks in Section VI. Section VII concludes the paper, followed by a list of abbreviations and acronyms.

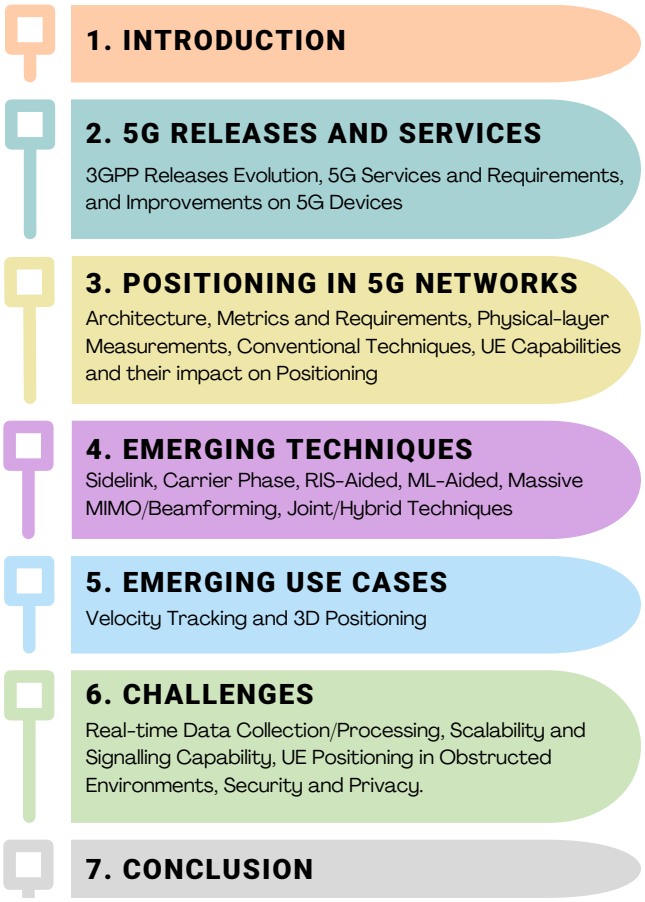

Fig. 1. Article Outline.

II. 5G Releases and Services

This section offers a general overview of the 5G landscape, covering key developments and advancements. It starts with the 3GPP Releases Evolution, outlining the milestones in standardization that have shaped 5G. Next, it discusses 5G service requirements, highlighting the performance requirements needed to support diverse applications. Finally, it explores Improvements on 5G Devices in Rel-18, detailing recent enhancements in devices' capabilities.

A. 3GPP Releases Evolution

The 3rd Generation Partnership Project (3GPP) is an organization that creates technical standards for mobile technologies, organized into releases, which include study items and work items. A study item involves feasibility studies or technical analyses focused on specific topics. Its purpose is to explore new ideas, technologies, or requirements and identify potential areas for standardization. A work item refers to a set of tasks focused on addressing specific features, improvements, or changes as part of the continuous standardization process. These activities lead to the creation of technical specifications [16].

We first provide a brief description of each of the releases 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 focus on non-standalone (NSA) 5G architecture, where the control plane is 5G and the data plane is Long Term Evolution (LTE). 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. Rel-16 introduced standalone (SA) 5G architecture, sidelink communication, 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 2022, the completion of Release 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 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). Rel-18 was completed in Q2 2024.

The plan for Rel-19 started in Q2 2021, 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 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 [17]. The Rel-20 plan, which kicked off in Q3 2024, continues the study of 6G planning by introducing new capabilities such as efficient multi-user MIMO and dynamic spectrum sharing, improving network performance, and supporting cutting-edge applications like XR and cloud gaming. It also uses AI and ML to improve mobility and reduce latency [18]. Fig. 2 shows a timeline for the 5G releases.

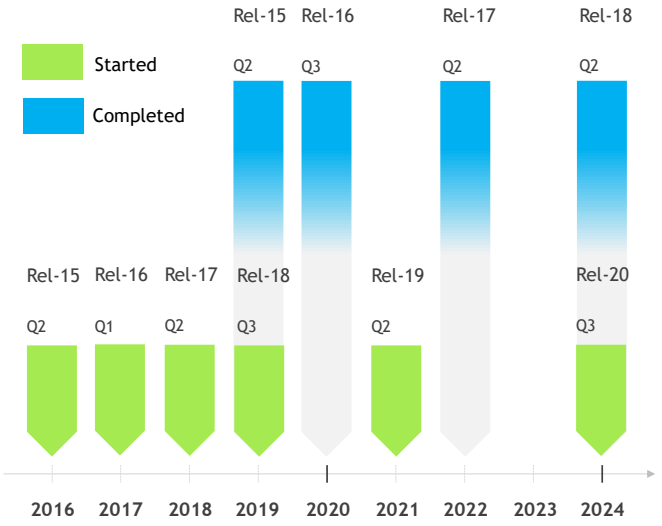

Fig. 2. Timeline of 5G Releases.

B. 5G Service Requirements

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

The Enhanced Mobile Broadband (eMBB) service was introduced in 3GPP Rel-15. It offers 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.

Ultra-Reliable Low Latency Communications (URLLC) was also introduced in Rel-15. It offers extremely low latency and high reliability to relatively low-rate mission-critical applications such as autonomous driving, remote surgery, and drone 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.

Massive Machine Type Communications (mMTC) supports 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 subcategories: (i) Long Term Evolution for Machines (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. Rel-15 recognized that NB-IoT and LTE-M would continue evolving as part of the 5G specifications due to their support for unique use cases [19].

As 5G networks developed further, 3GPP continued to support a range of 5G devices in a variety of usage scenarios. 3GPP Release 18 attempts to investigate and apply customized functionalities in this regard to improve and expand 5G capabilities. In addition to supporting conventional smartphones, the focus also encompasses a wide range of various 5G devices, such as cloud gaming consoles, low-complexity UEs, vehicle-to-everything (V2X), unmanned aerial vehicles (UAVs), and extended reality (XR) systems.

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 category of 5G devices, referred to as Reduced Capability (RedCap), has been introduced in 3GPP Rel-17 to accommodate these use cases [20]. RedCap devices are characterized by reduced throughput and bandwidth, relaxed latency requirements, and varying battery life (from days to years), depending on the specific use case. For example, RedCap devices can operate

TABLE I
5G SERVICES, CHARACTERISTICS, USE CASE, AND POSITIONING ACCURACY REQUIREMENT EXAMPLES

Characteristic	5G Services				
	URLLC	eMBB	RedCap	mMTC	
				LTE-M	NB-IoT
Maximum Data Rate (downlink)	100 Mbps	20 Gbps	150 Mbps	4 Mbps	250 kbps
Maximum Data Rate (uplink)	Not defined	10 Gbps	50 Mbps	1 Mbps	180 kbps
Minimum Latency	1 ms	4 ms	100 ms	10 ms	1.6 sec
Maximum Bandwidth (Frequency Range 1)	100 MHz	100 MHz	20 MHz	5 MHz	200 kHz
Maximum Bandwidth (Frequency Range 2)	2 GHz	2 GHz	100 MHz	-	-
Coverage (Maximum Coupling Loss)	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
Use Case Example	Remote Surgery	Augmented Reality	Wearables	Asset Tracking	Smart Metering
Positioning Accuracy *	20 cm	1 m	3 m	-	-

* Horizontal requirement for commercial use case based on 3GPP Rel-18.

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 [21]. This suggests that RedCap may potentially replace LTE-M in the coming years. FR2 uses a millimeter wavelength and operates above 24 GHz. Currently, mMTC only operates with FR1 because the minimum channel bandwidth specified for FR2 is 50 MHz [22].

Table I outlines the most recent requirements for the different 5G services. It also provides an example of a use case for each service, listing their key characteristics. 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, and long battery life, and can tolerate 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 a 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 [23]. As it is a premature service, there is no clear view of its characteristics. Thus, we chose not to include it in Table I.

C. Improvements on 5G Devices in Rel-18

3GPP Rel-18 focuses on significant enhancements for 5G devices, including enhancing support for cloud gaming and XR on 5G NR networks, requiring high data rates and low latency. Ongoing research is exploring scheduling and resource allocation systems, as well as UE power-saving techniques tailored for cloud gaming and XR services. To effectively handle the traffic from these applications, 3GPP is exploring ways to enhance RAN's awareness of XR, optimizing network parameters, adapting to varying traffic loads, and ensuring uninterrupted connectivity [24].

III. POSITIONING IN 5G NETWORKS

The demand for accurate positioning has grown due to the need for location-based services in sectors such as industrial IoT and autonomous driving. The introduction of 5G technology offers an opportunity to provide precise positioning for applications requiring robust, flexible, and cost-effective solutions globally. This section presents the basics of 3GPP 5G positioning.

A. Positioning Architecture in 5G Networks

The 5G location service architecture comprises four main components across all releases (see Fig. 3): (i) User Equipment (UE), which is capable of receiving the positioning reference signal (PRS) and/or transmitting the sounding reference signal (SRS). In addition, some UEs are capable of conducting physical-layer measurements, reporting them to the 5G core network (5GC), and computing their location. (ii) The Radio Access Network (NG-RAN), where the serving gNodeB (gNB) allocates the physical resources of the corresponding positioning reference signal, receives SRS and/or transmits PRS, conducts physical-layer measurements and reports them to the

location server. (iii) The location server, which is an entity in the 5GC called Location Management Function (LMF), its function is to initiates the positioning process communicates with the UE or the RAN, receives the reported physical-layer measurements, and computes the UE's location. (iv) Location Service Client (LSC), which connects third-party applications to the core network and provides customers with location service through open Application Programming Interfaces (APIs), such as real-time location push, map management, track query, and location data analysis [25].

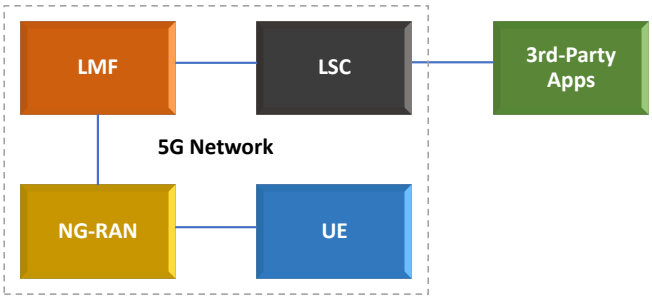

Fig. 3. High-Level Architecture of the 5G Location Service in 3GPP.

Every positioning technique follows a standard procedure that includes the request, signal transmission, physical-layer measurement, reporting, and computation. Network-based techniques such as UL-TDOA and AOA have similar procedures, differing only in the type of measurement used (time versus angle). These procedures are thoroughly outlined in 3GPP TS 38.305 [26].

B. Positioning Metrics and Requirements in 3GPP

The two key metrics 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 focus on reducing both positioning error and latency. In this subsection, we identify the accuracy and latency requirements set 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 (3D). As with most existing research in the literature, this paper focuses on two-dimensional (horizontal) positioning. 3D positioning is addressed separately in Section V.

For baseline devices (i.e., eMBB service), the desired level of accuracy for horizontal positioning in Rel-16 is set in the commercial use case to below three meters for indoor settings and below ten meters for outdoor settings, to achieve this level of accuracy for 80% of the estimation attempts for that UE, assuming several estimates are made [27]. In Rel-17, the target accuracy for the same service is set to below one meter for 90% of the estimation attempts 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 estimation attempts. Vertical positioning requirements are more relaxed than horizontal ones in most use cases [28].

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 meters for 90% of the estimation attempts in both settings (indoor and outdoor). This relaxation is primarily due to the smaller available bandwidth for RedCap UEs. Indeed, localizing a device with limited capabilities in different environmental settings is challenging due to multiple factors, including the low bandwidth and power-saving mode of the device. Rel-18 also sets the requirements of sidelink positioning, which utilizes other UEs to estimate a UE's location, these requirements include vehicles, public safety, commercial, and Industrial IoT use cases with specific accuracy and latency thresholds for each use case [29].

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 [27] 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 [28].

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 UE) and angle accuracy (the error of the direction measure in degrees) [29].

A metric that is rarely discussed and evaluated is the maximum number of UEs that can be accurately positioned simultaneously within a cell. Despite its significance, this topic remains relatively under-explored in existing literature. We briefly discuss it in Section VI.

In summary, a given 5G service does not adhere to specific positioning requirements. These requirements are tailored to specific use cases, and a given 5G service may serve multiple use cases.

C. Physical-Layer Measurements for Positioning

One fundamental component of positioning algorithms is the collection of physical-layer measurements from the transmitted or received signal, a process that can be carried out by the User Equipment (UE), the gNB (gNodeB), or both entities. The following are some key measurements [30] required for the 5G positioning methods which will be discussed in the following subsection.

- Reference Signal Time Difference (RSTD), is a UE measurement that refers to the difference in timing between the start of a DL-PRS subframe received by

a UE from gNB_1 and the start of the closest subframe received from gNB_2.

- Relative Time of Arrival (RToA), is a gNB measurement that refers to the beginning of a received UL-SRS subframe relative to the broadcast signal reference time. Where all gNBs transmit a broadcast signal simultaneously over the same frequency channel to synchronize the UE to the network.
- Reference Signal Received Power (RSRP), measures the average received power of a reference signal, to identify the main received beam index which is used to estimate the change in angle compared to a reference direction. This can apply to DL and UL signals such as CSI-RS, PRS, SRS, and Synchronization Signal (SS).
- Angle of Arrival (AoA), is a gNB measurement that estimates the azimuth and elevation angles of a UE with respect to a reference direction.
- gNB Rx-Tx Time Difference measures the difference in time between the received (Rx) uplink subframe containing SRS associated with UE, and the transmit (Tx) downlink subframe that is closest in time to the subframe received from the UE. The case is the opposite for UE Rx-Tx Time Difference, where the PRS is involved. These measurements define the round-trip time which can be used to estimate the distance between a gNB and a UE. MC-RTT positioning method uses multiple gNB to increase the accuracy.
- Timing Advance (TA), is a gNB measurement that indicates the time required by the UE to advance its transmission so that gNB can transmit and receive the subframes at the same time. This measurement is beneficial to estimate the distance between the UE and the gNB.

D. Conventional Positioning Techniques

In the following section, we present a summary of the conventional techniques used for positioning in wireless networks. They are typically classified into the following categories: (i) Range-based, (ii) Direction-based, and (iii) Fingerprinting-based [12], [31]. Note that, unlike the first two categories, fingerprint-based methods are not standardized in 3GPP. These distinct methods depend on the aforementioned physical layer measurements.

1) Range-based techniques: Estimate positions based on time 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 [8]. According to the traffic direction, we distinguish two types of TDoA [12]:
  - UL-TDoA, where the serving and neighboring gNBs measure the time difference of the received UL-SRS, and the resulting RToA measurements are used to estimate the location of the UE by the LMF.
  - DL-TDoA, where the UE measures the RSTD of DL-PRS from multiple gNBs and computes its location.
- Multi-Cell Round-Trip Time (MC-RTT): This technique involves sending signals from the UE to multiple gNBs and measuring the round-trip time for each of these signals. By estimating the RTT for each gNB, the distance between the UE and the gNBs can be calculated. MC-RTT, like other ranging-based techniques (e.g., DL-TDoA), uses a trilateration/multilateration estimation algorithm to calculate the UE's position [32]. The accuracy of Rx-Tx time difference measurements is contingent upon factors such as gNBs synchronization, carrier frequency, and unobstructed environment, potentially achieving precision at the centimeter level.

2) Direction-based techniques: Estimates the angle of the transmitted or received reference signal with relation to a reference angle. Beamforming, which is a technique used to focus the transmitted or received signal in a specific direction, is not a necessary component for these methods; nonetheless, it has been shown to enhance the precision of the measurements. The most common direction-based techniques are the following [12]:

- Angle of Arrival (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 serving and neighboring gNBs measure the angle of received SRS based on the beam in which the UE is located. These AoA measurements are then reported to the LMF for computing 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, which is a numerical identifier linked to a specific beam within a beamforming system, indicating the beam currently in use for communication with a particular user or device. 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.

3) Fingerprinting-based techniques: Rely 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, 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 related to the closest match in the database, allowing the system to determine the user's location based on the best match. This database, also known as a radio map or fingerprint database, stores the locations along with their associated fingerprints [12].

E. UE Capabilities and their Impact on Positioning

An important distinction among 5G services lies in the capabilities of the UEs that can use them. As a result, there are expected variations in positioning performance across different 5G services. It is worth noting that according to [7], positioning techniques such as UTDoA, OTDoA, fingerprinting, and E-CID have already been standardized for 4G and 4G-Advanced networks. These techniques have laid the groundwork for positioning capabilities in earlier generations of mobile networks. However, the advent of 5G has unlocked another level of options for positioning techniques. Indeed, 5G devices are known to have enhanced capabilities (compared to 4G devices), including support for a wider range of frequency bands, advanced beamforming, and MIMO (Multiple Input Multiple Output) technologies, and improved processing power. These advancements enable more precise and reliable localization, even in challenging environments such as dense urban areas or indoors where GPS signals may be limited. These enhancements have made the requirements for localization technologies evolve from merely meeting basic accuracy and reliability standards to supporting real-time and high-precision positioning for a diverse range of applications.

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. These states are CONNECTED, IDLE, and INACTIVE, and are all part of the RRC protocol (see Fig. 4) [33].

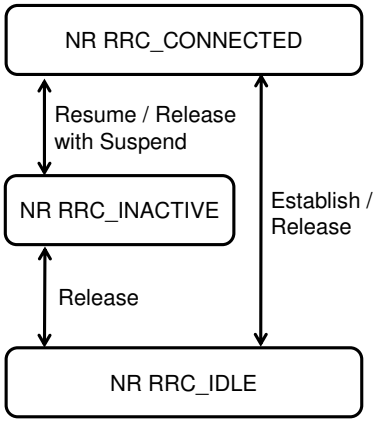

Fig. 4. UE Transition States in 5G.

The 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. RRC_INACTIVE state is designed to reduce network signaling load as well as the latency associated with transitioning to RRC_CONNECTED state. Furthermore, the UE in the RRC_INACTIVE state is allowed to behave similarly to the RRC_IDLE state to save power.

Regarding positioning, 3GPP states that some physical-layer measurements can be carried out when the UE is INACTIVE [30]. On the other hand, other measurements 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. 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 to the network. Therefore, NR functionality based on the existing RRC states may not be valid and it may need new device state definitions [23].

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 on the network side), low bandwidth can significantly affect the positioning accuracy. For example, the 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 [34]. While eMBB/URLLC UEs can transmit on the maximum bandwidth (i.e., 100 MHz in FR1), RedCap and mMTC UEs can transmit on up to 20 MHz and 5 MHz, respectively. As a result, the frequency hopping technique can be used to transmit the reference signal over multiple time slots to overcome the limited channel bandwidth and consequently achieve better accuracy. 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 [29].

3) UE Mobility: Mobile networks rely on mobility support to ensure seamless communication for a UE as it moves across different cell coverage areas. When a UE transitions from one cell to another, a handover process is initiated to switch the serving cell. Currently, this handover decision is based on layer 3 (L3) measurements and radio resource control (RRC) signaling [24]. However, to address latency, overhead, and interruption challenges associated with L3-based mobility management, 3GPP Rel-18 introduces mechanisms and procedures for layer 1/layer 2 inter-cell mobility. Additionally, Rel-18 aims to enhance conditional handover support, where the UE receives a handover command but defers its application until specific conditions are met. Moreover, inter-frequency mobility is supported [35]. This approach promises improved mobility robustness and service continuity in evolving mobile

networks. Still, and to the best of our knowledge, only a few works in the literature focus on the use of localization for handover management. In [36], a wireless testbed is introduced for evaluating ultra-dense networks and related mobility schemes. A mobility management scheme is provided in the testbed to track UE location proactively, enabling uninterrupted handover (HO) service. UE positions are tracked using SRSs transmitted by the UE, reducing signaling expenses for HO but increasing computational complexity. In [37], the authors propose a deep learning model for user localization and proactive HO management as well. The model utilizes received signal measurements to minimize unnecessary HOs and predict user location while maintaining network throughput.

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 [38]. 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).

IV. Emerging Positioning Techniques in 5G

In this section, we review the state of the art of the emerging 5G positioning techniques (*i.e.,* the techniques which have not been standardized in 3GPP yet), to improve accuracy and latency, which are: (i) Sidelink positioning, (ii) Carrier Phase positioning, (iii) RIS-aided positioning, (iv) Machine Learning-aided positioning and (iv) Hybrid positioning.

Before delving into the state-of-the-art, we provide a macro-level comparison of these emerging techniques in terms of complexity, accuracy, robustness, cost, and signal direction. This comparison is shown in Table II.

A. Sidelink Positioning

Sidelink communications refer to the direct exchange of data between two or more UEs, without the need for relaying through a centralized base station (BS). Unlike traditional positioning systems, sidelink positioning leverages direct Device-to-Device (D2D) communication within the 5G ecosystem, enabling UEs to exchange location-related information. This enables precise and real-time positioning even with dynamic and intricate mobility patterns. To the best of our knowledge, no comprehensive survey in the literature 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:

This paper [39] provides an overview of the evolution of sidelink communications in 5G and its positioning application.

According to [40], uncertainties in anchor positions can compromise positioning accuracy in industrial environments. They propose a joint estimation of vehicle and anchor positions using location-related measurements (LRMs) such as RSS and ToA. Devices function as anchor-agents, and vehicles are target-agents. The anchor-agents use sidelink measurements from target-agents to estimate LRMs, which are then used with a Kalman filter-based method to estimate the positions of both anchor- and target-agents. Simulations indicate that utilizing LRMs collectively, combining time- and angle-domain LRMs, yields enhanced performance in both 2D and vertical planes.

The study in [41] 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 involves the clustering of users, where NR-sidelink is harnessed for ranging users within each cluster, effectively mitigating overhead. The method is validated through an extensive mobility model, specifically tailored for a stadium entry use case. User clusters are derived from individual mobility patterns. Simulation-based analyses are conducted, revealing substantial signaling overhead reduction, approximately 75%, across a wide range of SINR conditions. The NR sidelink-based ranging attains 1.5-meter accuracy, and 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. Specifically, the wide-band Sidelink PRS (SL-PRS), which demands the maximum number of physical resource blocks, and which is used for positioning, could conflict with NR sidelink transmissions occurring within the same resource pool or sidelink carrier. The study in [42] addresses this to allow efficient scheduling between communication and positioning. They 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 utilize the same time and frequency resources for sidelink communication. Consequently, both UEs synchronize their transmissions within the same slot and subchannel. However, this synchronization introduces significant challenges related and security, as malicious entities could spoof the ”skip-preemption” messages, causing UEs to incorrectly synchronize their transmissions.

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 that integrate different aspects, including multiple QoS classes, to accommodate varying accuracy requirements to enable tailored solutions for different scenarios, and efficient scheduling mechanisms to

TABLE II
MACRO-LEVEL COMPARISON OF EMERGING 5G POSITIONING TECHNIQUES

Technique / Criteria	Complexity	Accuracy	Robustness	Cost	Signal Direction
RIS-Assisted	Computing: High	cm-level	Moderate, depends on a few key challenges, such as accurate CSI estimation, multipath interference, and environmental sensitivity.	High, deployment and maintenance	Mostly DL
ML-Assisted	Algorithmic: High	cm-level to meter-level	High, assuming enough accurate data	Moderate	DL / UL
Sidelink	Moderate, depends on devices	meter-level	Moderate	Moderate	SL
Carrier Phase	High algorithmic complexity	cm-level	High in LOS, low in NLOS	Moderate	Mostly DL
MIMO / Beamforming	High, real-time processing required	cm-level	High	High	DL / UL
Hybrid	Moderate to High, depends on the technique	cm-level to meter-level	High	Moderate to High	DL / UL

address distinct resource demands.

B. Carrier Phase Positioning

Carrier phase positioning, widely utilized in GNSS systems for its high accuracy, is now being explored for use in 5G NR systems. This technique involves multiplying a received reference signal with a replica signal generated at the receiver, calculating distance based on the phase difference between these signals [43]. Carrier phase positioning can utilize various 5G reference signals, such as the Demodulation Reference Signal (DMRS) [44] and PRS [45]–[47], to improve positioning accuracy.

A key challenge in carrier phase positioning is resolving the integer ambiguity parameter, which represents the total number of complete phase cycles that the reference carrier signal must travel between the UE and the gNB to generate the same observed phase at the UE. The study in [48] utilized the phase difference of arrival (PDoA) and OFDM subcarriers to handle the integer ambiguity of carrier phase, while [45] propose a technique for clock offset determination through carrier-phase measurements to achieve precise clock synchronization among base stations. The authors employ a fusion approach that combines UE positions estimated using Time Difference of Arrival (TDoA) and temporal variations of carrier phase measurements to provide interim position estimates, aiding in linearizing measurements and resolving integer ambiguities, and accordingly achieving centimeter-level accurate UE positioning. The study in [46] introduces the double-difference carrier phase measurements method to address the integer ambiguity issue by continuously transmitting PRS from two gNBs to accurately track carrier phase and prevent ambiguity problems in LOS environments. Additionally, they employ another UE to observe the same signals and eliminate measurement errors caused by clock offset between the two gNBs, achieving sub-meter accuracy. Further research is needed to explore the robustness of these methods in noisy or multipath conditions, evaluate trade-offs between different information sources, and assess computational complexities associated with the fusion process.

In their work, the authors of [47] 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.

The authors of [49] extend carrier phase positioning to UAV navigation. Their framework allows UAVs to achieve sub-meter accuracy in multipath-free environments by leveraging “loose” synchronization between the clocks of serving and neighbor gNBs. Their work, based on extensive experimental data, models gNB clock deviations using a stable Auto-Regressive Moving Average (ARMA) process, reducing both position estimation error and computational complexity.

Additionally, the authors in [50], propose a method to address multipath fading challenges in indoor environments. Their two-step approach combines sequential component cancellation (SCC) and multiple signal classification (MUSIC) algorithms to estimate the parameters of multipath components. This method has shown robust performance in real-world experiments, enabling accurate relative positioning in indoor environments.

In conclusion, recent research efforts in carrier phase positioning for 5G NR systems have addressed critical challenges, particularly the estimation of the 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 enhance the applicability of the widely used carrier phase technique in 5G positioning. 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) are engineered materials that can be reconfigured dynamically to improve coverage by controlling scattering, absorption, reflection, and diffraction properties. This control over propagation channels allows innovative radio positioning solutions, even in severe LOS obstruction scenarios. [15] provides a valuable review of recent works using RIS to improve positioning. We complete it with the following recent works:

In [51], Popoola et al. introduce a novel positioning model for Airborne Networks (i.e., where UAVs are used as aerial mobile base stations), leveraging RIS. The system includes an RIS, a 5G small cell, and a ToA/RSS positioning algorithm. According to the authors, one of the key open challenges for RIS-based positioning is pilot contamination, arising from the use of pilot symbols for the identification of individual RISs. They argue that it 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. [52] consider positioning in 5G networks by leveraging multiple passive RISs. The proposed method 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 show that the method effectively estimates the UE position, also quantifying the estimation uncertainty through the LSE error metric.

Zhang et al. [53] propose to use an RSS fingerprinting-based method for positioning in a RIS-assisted environment, to address the impact of noise on RSS measurements, particularly in indoor settings. They gather multiple RSS values under different configurations and use an optimization method based on Cramér-Rao Lower Bound (CRLB) to find the RIS configurations that yield the most accurate positioning. Note that CRLB is used to assess the accuracy of a given parameter estimation. These RSS values are used as fingerprints to train neural networks, enabling the estimation of target locations based on these fingerprints. Simulations show that the method can achieve positioning in an NLOS scenario with an accuracy of 0.5 meters.

Lu et al. [54] argue that the assumption of perfect knowledge of the RIS's location and orientation may not be valid in practical scenarios due to factors like deployment faults, external disturbances, or improper installation. Thus, they propose a Joint RIS Calibration and User Positioning method, JrCUP, where they use Fisher Information to derive analytical lower bounds for both user and RIS states and propose an iterative algorithm to estimate these parameters based on AoA and AoD measurements. Simulations show that multi-user scenarios generally outperform single-user cases due to the additional information obtained from a greater number of measurements, enhancing the accuracy of the RIS state.

Wang et al. [55] introduce the concept of Continuous Intelligent Surfaces (CISs), a specific type of RIS, which are planar structures that can be electronically controlled to manipulate electromagnetic waves. Unlike conventional RISs with discrete elements, CISs exhibit a continuous phase response function across the entire surface, enabling precise reflection, refraction, or scattering of incident waves. Fisher's information analysis demonstrated that strategically configured CISs can significantly enhance positioning accuracy, with carefully designed phase responses providing substantial improvements in positioning performance compared to random phase responses or a simple scattering plane.

Unlike most existing works on RIS positioning that rely on simulations, the authors in [56] present a demo of a real-world deployment using RIS equipment for indoor localization of UEs. They also introduce a novel weighting scheme for RSS fingerprints collected from various environments. The process involves two phases: a meta-learning phase, where a generalized Convolutional Neural Network (CNN) meta-model is built using data collected at different times, and an online learning phase, where the meta-model is fine-tuned using only 20% of the data from a new environment. However, it's worth noting that this approach has been used with Wi-Fi connectivity at 5.5 GHz. It would thus be interesting to see how it generalizes to 5G.

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. However, integrating RIS into existing 5G infrastructure poses challenges due to the need for installation and the high cost of maintenance.

D. Machine Learning-Aided Positioning

Machine Learning (ML) is transforming 5G positioning, particularly in complex scenarios like NLOS multipath. By creating signal fingerprints, leveraging crowdsourced data, and predicting device locations based on historical patterns, ML can significantly enhance location accuracy. Mogyorosi et al. [12] provides a comprehensive review of ML-based positioning methods. Building upon this, we present recent advancements in the field.

Zhao et al. [57] address the challenge of assessing the uncertainty in positioning methods. 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 and lead to a predicted uncertainty that is highly correlated with the actual positioning error.

In a similar vein, Albanese et al. [58] introduce the concept of "pseudo-multilateration," which involves a single UAV anchor obtaining 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 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, which can be mitigated by the usage of RISs to complement existing ground networks. Finally, the authors advocate the use of CNN for determining the UE position by treating the collected measurements as a single-channel image. This approach enables CNN to effectively handle the channel shadowing caused by obstacles in the scenario. However, to the best of our knowledge, no actual implementation has been proposed in the paper.

Ruan et al. [59] introduce iPos, an indoor positioning system that leverages fingerprinting and incorporates both supervised and unsupervised learning techniques. The system starts with preprocessing channel state information (CSI) and an unsupervised autoencoder extracts critical CSI features. The Gaussian Radial Basis Function (RBF) kernel is used to quantify the similarity between input and reconstructed features. An amplitude-phase probability fusion function is used 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. Since the system does not need complex convolutional operations it is particularly suitable for future deployment of UEs with limited computing power and storage capacity.

Torsoli et al. [60] introduce the concept of Blockage Intelligence (BI), which consists of a probabilistic description of wireless propagation conditions, especially in case of NLOS to reduce the biases in measurements estimates (*e.g.,* ToA). They process the cross-correlation between the transmitted and the received reference signals (PRS/SRS). Then, a two-class supervised classification problem is considered, representing either NLOS or LOS propagation conditions, and the vector of the statistical features is used as input. An exponential loss function is employed to obtain a classification model, which can be used to get 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. They also use in [61] a similar modeling approach by introducing a machine learning-based reference BS selection method. To do so, they propose a method utilizing the AdaBoost algorithm for classification. Based on signal statistical features, the model is trained to predict both the channel quality and the LOS posterior probability. Subsequently, the BS with the best channel quality is selected as the Reference Base Station (RBS), which is used to compute the TDoA by subtracting the ToA of that RBS from the ToA of all other BSs involved in localization. Simulation results show improvement in positioning accuracy when utilizing TDoA measurements compared to the common methods using the SNR to select the RBS.

Liu et al. [62] propose a ToA estimation method based on 5G downlink signals. The method leverages ML algorithms combined with a Kalman Filter (KF) to achieve high-precision and stable signal tracking, all within a Software Defined Receiver (SDR) framework, without requiring any changes to the existing hardware structure. The method is tested using real field deployment, and the results indicate that the 95% Cumulative Distribution Function (CDF) of the measurement error using commercial 5G signals in the indoor environment is 0.50 m. Furthermore, the results also show that the ML-based tracking method can achieve equal or even higher accuracy compared to traditional carrier phase-ranging tracking methods.

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 improving location accuracy by employing methods such as signal fingerprinting, crowdsourced data utilization, and historical pattern-based predictions. Still, the use of ML for 5G positioning faces a major challenge which is dataset availability. Indeed, comprehensive datasets representative of diverse 5G environments are needed for accurate model training, requiring significant resources for collection.

E. Massive MIMO & Beamforming Positioning

Massive MIMO [63] and beamforming have emerged as essential technologies for next-generation wireless networks. Massive MIMO utilizes large arrays of antennas at the base station to communicate with multiple users simultaneously, significantly improving spectral and energy efficiency. Beamforming, on the other hand, enables directional focusing of radio frequency signals, enhancing targeted communication and reception. These technologies offer opportunities to refine position estimation accuracy in complex environments by directing focused beams toward devices. Alamu et al. [64] offers a valuable overview of positioning with massive MIMO, though recent developments require an updated review, especially for beamforming positioning in 5G networks. We provide in what follows an overview of key recent advancements in both massive MIMO and beamforming positioning.

Sellami et al. [65] [66] use a neighbor-assisted algorithm to estimate distances between the UE and its two closest Anchor UEs through reference signal power measurements, and resolve ambiguity using beamforming over limited angular intervals. Their results consistently achieve sub-meter accuracy, even in challenging environmental conditions (low SNR).

The study of Singh et al. [67] estimates the ToA from multiple BSs through the application of the Estimation of Signal Parameters via Rotational Invariant Technique (ESPRIT) [68], achieving a 20 cm positioning accuracy for 90% of UEs in indoor factory scenarios.

Gante et al. [69] investigate the capabilities of low-power 5G positioning systems using machine learning in millimeter wave (mmWave), 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 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. [70] employed AoD in a mmWave indoor massive multiple-input single-output (MISO) scenario. 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, even in the presence of multiple users.

Abu et al. [71] 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. The proposed method for mmWave wireless networks utilizes time delay and angle information, employing beamforming for both UL and DL performance evaluation. The results show that it is more beneficial to have more antennas at the BS than at the UE, which can help minimize interference by directing signals more precisely to a specific UE.

Seo et al. [72] use beam sweeping, 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. By refining the estimated UE position based on beam direction, their method distinguishes closely located UEs and improves positioning accuracy as the beam width narrows, benefiting massive MIMO systems.

Koivisto et al. [73] propose a direction-of-arrival (DoA) and ToA estimation method using analog radio frequency (RF) beamforming-based observations, enhanced by an extended Kalman filter. Their CRLB-based analysis shows less than two meters of positioning accuracy with minimal computational overhead, making it a promising solution for RF multi-beam systems.

Wang et al. [74]explore deep convolutional Gaussian processes (DCGP) for outdoor mmWave positioning, using a large dataset of beamforming images. Their approach improves positioning accuracy while estimating uncertainty, highlighting the potential of DCGP in mmWave environments.

Pucci et al. [75] examine the sensing capabilities of 5G NR under the Joint Sensing and Communication (JSC) paradigm, Their results reveal the ability to detect tens of targets with submeter-level accuracy, confirming the viability of integrating sensing functionalities into communication systems through multi-beam designs.

Hu et al. [76] present a wideband SRS-based AoA estimation method for 5G, combining a Multiple signal classification (MUSIC) [77]-like algorithm with a novel focusing technique for high accuracy positioning with reduced computational complexity. Their method improves estimation accuracy by up to 30%, outperforming traditional narrow-band and wideband methods.

Chu et al. [78] propose a hybrid analog and digital beamforming (HBF) method for positioning enhancement in cellular MIMO systems. Resource allocation across power, beam, and frequency dimensions, improves positioning performance and robustness against multipath clutters.

In summary, recent advancements in Massive MIMO and beamforming have demonstrated their potential to significantly enhance positioning accuracy in 5G networks, even in obstructed environments with low SNR. These technologies leverage advanced methods such as ESPRIT, beam sweeping, and deep learning to refine position estimation. However, challenges remain regarding the complexity of deploying extensive antenna arrays, maintaining synchronization, and managing the high computational demands for real-time beamforming optimization.

F. Joint and Hybrid Positioning Techniques

The combination of signals from different technologies for positioning has garnered significant interest within the research community. By integrating multiple techniques, positioning accuracy can be greatly enhanced. This subsection reviews recent developments in joint positioning techniques within 5G and hybrid techniques that incorporate 5G with other technologies, such as GNSS, Bluetooth, and more.

In their study, Zhang et al. [79] use carrier phase with ToA to address the challenge in carrier phase positioning techniques 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. [80] propose a hybrid method to improve accuracy in indoor positioning by integrating 5G, Bluetooth Low Energy (BLE), and a terminal motion sensor. Their approach combines UL-TDoA from 5G, AoA from BLE, and sensor data using an optimization algorithm. This method achieves centimeter-level accuracy for distances of 3 meters and maintains less than 3 meters of error for longer distances.

In their work, Alghisi et al. [81] tackle the limited satellite visibility for GNSS positioning in urban areas by combining 5G technology with GNSS. Using ToA and TDoA with multiple 5G base stations, their findings reveal that 5 base stations are optimal for aiding GNSS positioning. Both ToA and TDoA yielded similar performance, with TDoA showing a slight advantage, particularly in challenging urban scenarios.

To address the challenges of unstable multi-signal estimation in GNSS-5G hybrid networks, Liu et al. [82] introduce the

Square Root Unscented Stable Filter (SRUSF) for joint positioning in GNSS and 5G. Their method stabilizes positioning accuracy by maintaining positive covariance in estimation errors and reducing the risk of divergence in hybrid networks. Simulation results show that SRUSF outperforms five other joint techniques, providing improved accuracy and reliability. This advancement paved the way for mass-user terminals to deliver more reliable positioning services in GNSS-5G environments.

Li et al. [83] tackle the issue of 5G clock synchronization error in hybrid GNSS/5G systems. Their method introduces double-differenced observations to mitigate the impact of clock errors, improving accuracy between terminals and base stations, as well as between base stations themselves. The study also examines 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.

Finally, Liu et al. focus in [84] on improving smartphone positioning accuracy by proposing a GNSS/5G hybrid positioning model, particularly for challenging urban environments where building interference diminishes the reliability of GNSS signals. They introduce a 5G observation model based on unit vectors, which addresses the shortcomings of the traditional angle of departure (AOD) method by reducing linearization errors. The unit vector model minimizes the nonlinearity of the observation process, leading to substantial gains in the 5G system's performance, especially in the presence of increased noise. Furthermore, the study highlights the importance of BS height and geometric distribution in positioning accuracy. The method offers a robust solution for seamless indoor and outdoor positioning, achieving decimeter-level precision even in occluded areas.

In summary, hybrid and joint techniques offer significant advantages in improving positioning accuracy and handling complex environments, such as indoors. However, these improvements may come at the cost of real-time updates, due to the time taken for the data fusion from different sources [85]. Nevertheless, there are certain use cases (such as asset tracking) where this trade-off is acceptable.

V. Emerging Positioning Use Cases

Positioning is not only a critical enabler in the 5G landscape but also an integral part of our daily lives, shaping how we interact with technology and our environment. From navigating cities to ensuring the efficient delivery of goods, accurate and real-time positioning enhances convenience, safety, and productivity. In everyday scenarios like commuting through dense urban areas, precise location data allows for better navigation and smarter traffic systems, reducing delays and improving public safety. Beyond logistics and transportation, positioning plays a vital role in emergencies, where the ability to quickly and accurately locate individuals can save lives.

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 additional complexities and challenges, especially for positioning. Two notable positioning extensions that are gaining momentum are velocity tracking and 3D positioning. We provide the following description of the two extensions and the related use cases and review the existing works that address these two extensions or the related use cases in the literature.

1) Velocity Tracking: Accurately localizing fast-moving vehicles, such as high-speed trains (HSTs) or fleets of vehicles, presents significant challenges. High mobility introduces complexities like Doppler shifts, rapidly changing propagation conditions, and the need for extremely low-latency position updates. Traditional positioning systems often struggle with precision in these dynamic environments, yet interest in addressing these challenges has surged in recent years. Technologies like Massive MIMO and beamforming offer potential solutions by improving propagation conditions and positioning accuracy, which is essential for channel estimation and enhancing wireless access in railway communications [86]. The following section reviews recent works addressing fast-moving vehicle positioning using 5G.

Shi et al. [87] 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 neural network 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. However, it is worth noting that 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 only 8 meters. The authors argue that there is still an interest in using their method as an alternative positioning method for HST in complex environments.

In [86], Shi et al. also consider a positioning problem of HST in railway wireless networks 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. 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 [88], linearizes the RDoA equations to pseudo-linear ones and is then utilized to obtain the train position. The simulation results illustrate that a centimeter-level accuracy can be achieved for small PRS intervals, velocities, and base station distances.

In [89], Trivedi et al. present a sensing-based 5G positioning

method for the positioning and tracking of HST. 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's performance. The proposed algorithm, implemented and tested in a 3GPP specified HST scenario [90], 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.

Wen et al. [91] introduce an Improved Extended Kalman Filter (IEKF) algorithm that utilizes the Least Squares of Undermeasurement (LSU) technique for HST localization. The IEKF method involves expanding nonlinear functions through higher-order statistical features, enhancing positioning accuracy. Simulation results show that the IEKF, when expanded to the second order, achieves over 20% performance improvement compared to traditional algorithms such as EKF (Extended Kalman Filter). Notably, at the third order, the IEKF demonstrates over 85% improvement, which reflects the additional accuracy gained from incorporating even more detailed statistical information and higher-order terms in the model. This illustrates the IEKF's effectiveness in high-speed train scenarios and its capability to manage high-dimensional systems with significant nonlinearity.

Besides localizing HSTs, some works focus on localizing fleets of vehicles. In [92], 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. Results show 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 critical use cases, such as logistics, emergency services, and UAV navigation, necessitate accurate 3D positioning. As 5G networks advance, 3D positioning becomes more achievable through a variety of innovative approaches. This section reviews recent developments in 3D positioning techniques within 5G networks.

Lin et al. [93] propose a tensor-based approach for 3D positioning using a wideband mmWave massive MIMO system. They introduce a multidimensional interpolation method to suppress frequency-dependent components in the antenna array steering vectors, critical for maintaining beamforming accuracy across the wideband spectrum. By leveraging the high temporal resolution of mmWave signals, they effectively decouple parameters across temporal, spatial, and frequency domains. Their approach computes 3D coordinates by exploiting the quasi-optical nature of mmWave signals, showing superior performance over traditional methods like the 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 [94] 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 show that the positioning accuracy in all dimensions is within 20 cm.

In their study, Afifi et al. [95] 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.

Nazari et al. [96] explore the 3D positioning and orientation of an unsynchronized multi-antenna UE using downlink MIMO-OFDM signals. They apply Fisher information analysis to show the problem is generally identifiable, as long as there is at least one multipath component. They formulate a maximum likelihood estimation problem to estimate the UE's position and orientation, along with several nuisance parameters like the UE clock offset and incidence points. The problem involves high-dimensional non-convex optimization over Euclidean and non-Euclidean manifolds. Then, they propose an initial geometric estimate of all parameters, which reduces the problem to a 1-dimensional search over a finite interval. Their results illustrate the effectiveness of this method, which narrows the gap to the Cramér-Rao bound using the maximum likelihood estimation.

Chel et al. [97] tackle multi-RIS enabled 3D SISO sidelink positioning, where at least two RISs act as passive anchors with known positions and orientations. It demonstrates that, through sidelink communication between two unsynchronized UEs, their absolute 3D positions and clock offset can be estimated, even in the absence of base stations (BSs). To achieve this, a low-complexity channel parameter estimation

method is developed to estimate delays and spatial frequencies. Using these estimates, a 3D-search algorithm is proposed to further refine the 3D positioning and clock offset calculations, supported by maximum likelihood estimators.

The reviewed studies present a range of innovative solutions for 3D positioning in 5G networks. 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 show that these approaches efficiently overcome these challenges, through improved accuracy and reliability in 3D positioning.

VI. Challenges in 5G Positioning

In this section, we discuss some challenges that need to be addressed to unlock the full potential of 5G for location-based services and applications. These challenges lie around the latency requirements of location-based services, massive signaling, scalability, and privacy concerns. We provide a detailed explanation of each challenge below.

A. 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 period. However, this type of tracing has a major drawback. It is challenging to differentiate the UEs due to a privacy policy that masks 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 traces 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 the International Mobile Subscriber Identifier (IMSI) to distinguish the UEs.

One suggested approach for achieving real-time network-based positioning in commercial RAN involves using Mobile Edge Computing (MEC) [98] 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 save storage space and enables simultaneous tracking of more UEs.

B. 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. 5. 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 [99].

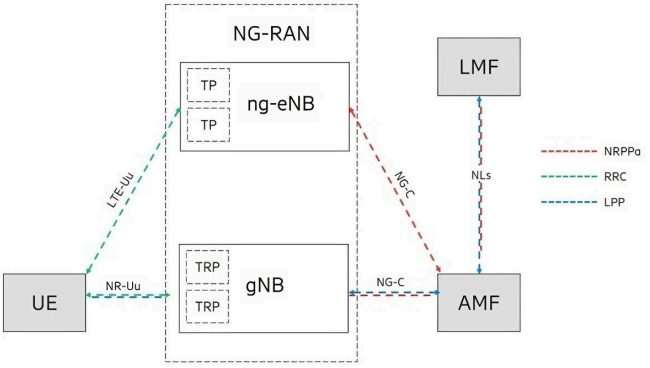

Fig. 5. 5G Positioning Signaling Protocols [26].

In the downlink positioning (UE-based) for mMTC service, Chen et al. [44] employ the DMRS instead of PRS for localizing a massive number of UEs using the 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 configuration is flexible so that the gNB can receive signals from multiple UEs at the same time. The maximum number of UE has not yet been determined, though, as this could compromise accuracy. More investigation is required as there may be a trade-off between accuracy and scalability that has not been examined in prior studies.

Due to the intended low complexity of mMTC service, the hardware capabilities are limited. In network-based positioning, as per 3GPP [26], 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 the subscriber identity module (SIM), which makes it important to establish a simplified form of AIoT UE identification in a 3GPP network [23].

C. 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.6). 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 [100].

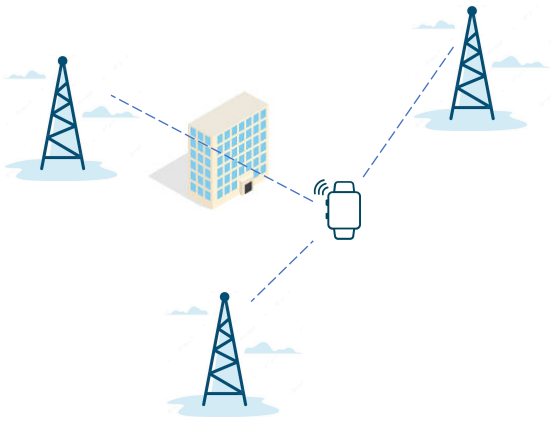

Fig. 6. An Example of Obstructed Line-of-Sight.

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 to get a target location estimation [101].

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. 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 [102].

D. Security and Privacy

Security is one of the 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 [103], two distinct categories of security-related vulnerabilities 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 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 [104].

In response to these vulnerabilities, several efforts have been made by the research community. [103] identifies the following as the most important approaches to enhance the security of 5G positioning:

- **Physical Layer Measurements:** Employing physical layer attributes to enhance security by validating device authenticity and integrity. For instance, [104] 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 a Service Enabler Architecture Layer (SEAL) to enable key management in 5G networks [105].

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 toward 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 us 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].

VII. Conclusion

As the deployment of 5G networks continues to expand globally, the demand for accurate, scalable, and reliable positioning solutions is increasingly critical across a broad spectrum of industries. This paper has reviewed the current landscape of 5G positioning technologies, focusing on both conventional and emerging techniques, including sidelink positioning, Reconfigurable Intelligent Surfaces (RIS), Machine Learning (ML)-aided positioning, and massive MIMO. Each of these technologies offers unique advantages, addressing various challenges faced by previous generations of positioning systems, such as poor indoor accuracy and high-latency data processing.

The discussion of use cases, such as industrial IoT, autonomous vehicles, and healthcare, highlights how 5G positioning capabilities are revolutionizing these fields, enabling real-time tracking, improved process automation, and enhanced safety. However, while significant progress has been made, several challenges remain unresolved. Real-time data collection, scalability in dense urban environments, and security concerns surrounding location-based data are critical hurdles that must be addressed for widespread commercial deployment.

Future research must continue to focus on improving accuracy in non-line-of-sight (NLOS) scenarios, especially in urban and indoor environments. Additionally, as 5G-Advanced and 6G technologies are developed, further exploration of hybrid positioning methods, which combine multiple signal types (e.g., GNSS, Bluetooth, and 5G), will be key to enhancing both accuracy and reliability. The integration of AI and machine learning holds promise for tackling these challenges, enabling more adaptive and intelligent positioning solutions that can respond to the dynamic nature of real-world environments.

In conclusion, while 5G offers transformative potential for positioning technologies, realizing its full capabilities will require continued innovation and collaboration between industry, academia, and standardization bodies. By addressing the existing challenges and embracing emerging technologies, the future of 5G and beyond will deliver unprecedented levels of precision, reliability, and scalability for positioning systems across the globe.

Acknowledgements

This work was funded in part by Rogers Communications Inc., Canada, and in part by the Natural Sciences and Engineering Research Council of Canada (NSERC). The authors gratefully acknowledge their support and contribution to this research.

List of Acronyms

The list of acronyms is provided in Table III.

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.

TABLE III
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	**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

[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] "What is a Work Item — 3gpp.org," https://www.3gpp.org/specifications-technologies/3gpp-work-plan/what-is-a-work-item, [Accessed 06-03-2024].

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

[18] Ericsson, "The Next Wave of Advanced 5G – 3GPP Release 19," 2024, accessed: August 20, 2024.

[19] 3GPP, "Release 15 Description; Summary of Rel-15 Work Items," 3rd Generation Partnership Project, Technical Report (TR) 21.915, September 2019, version 15.0.0.

[20] 3GPP, "Study on support of reduced capability NR devices," 3rd Generation Partnership Project, Technical Report (TR) 38.875, March 2021, version 17.0.0.

[21] 3GPP, "Study on further NR RedCap UE complexity reduction," 3rd Generation Partnership Project, Technical Report (TR) 38.865, September 2022, version 18.0.0.

[22] 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.

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

[24] X. Lin, "An Overview of 5G Advanced Evolution in 3GPP Release 18," *IEEE Communications Standards Magazine*, vol. 6, no. 3, pp. 77–83,

2022.

[25] 3GPP, "5G System Location Services," 3rd Generation Partnership Project, Technical Specification (TS) 23.273, September 2023, version 18.3.0.

[26] 3GPP, "User Equipment Positioning in NG-RAN," 3rd Generation Partnership Project, Technical Specification (TS) 38.305, March 2023, version 17.4.0.

[27] 3GPP, "Study on NR Positioning Support," 3rd Generation Partnership Project, Technical Report (TR) 38.855, March 2019, version 16.0.0.

[28] 3GPP, "Study on NR Positioning Enhancements," 3rd Generation Partnership Project, Technical Report (TR) 38.857, March 2021, version 17.0.0.

[29] 3GPP, "Study on Expanded and Improved NR Positioning," 3rd Generation Partnership Project, Technical Report (TR) 38.859, December 2022, version 18.0.0.

[30] 3GPP, "5G NR Physical Layer Measurements," 3rd Generation Partnership Project, Technical Specification (TS) 38.215, March 2023, version 17.3.0.

[31] 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.

[32] R. Keating, M. Säily, J. Hulkkonen, and J. Karjalainen, "Overview of positioning in 5G new radio," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2019, pp. 320–324.

[33] 3GPP, "NR Radio Resource Control (RRC) Protocol Specification," 3rd Generation Partnership Project, Technical Specification (TS) 38.331, March 2023, version 17.4.0.

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

[35] 3GPP, "5G-Advanced and Rel-18 Completion," https://www.3gpp.org/technologies/ran1-rel18, 2024, [Accessed 16-04-2024].

[36] N. Malm, L. Zhou, E. Menta, K. Ruttik, R. Jäntti, O. Tirkkonen, M. Costa, and K. Leppänen, "User localization enabled ultra-dense network testbed," in *2018 IEEE 5G World Forum (5GWF)*. IEEE, 2018, pp. 405–409.

[37] R. Klus, L. Klus, D. Solomitckii, M. Valkama, and J. Talvitie, "Deep learning based localization and HO optimization in 5G NR networks," in *2020 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2020, pp. 1–6.

[38] 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.

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

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

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

[47] 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.

[48] 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.

[49] 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.

[50] P. P. Hassan, I. Marsland, R. Smith, R. Kerr, S. H. R. Naqvi, and I. Lambadaris, "Carrier Phase Based Relative Positioning Using MUSIC-Based ToA Estimation with High Resolution," in *2024 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE, 2024, pp. 1–6.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] Q. Luo, Z. Yang, B. Di, and C. Xu, "Meta2Locate: Meta Surface Enabled Indoor Localization in Dynamic Environments," in *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, 2023, pp. 312–313.

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

[58] 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.

[59] 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.

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

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] "Accurate positioning using beamforming, author=Seo, Hyunmin and Kim, Hyunsoo and Kim, Taehyung and Hong, Daesik," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2021, pp. 1–4.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

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

[78] X. Chu, Z. Lu, J. Kang, Y. Zou, H. Zhang, and X. Qiu, "Hybrid Beamforming towards Positioning Enhancement under Cellular MIMO Systems," *IEEE Transactions on Wireless Communications*, 2024.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] Q. Liu, C. Gao, A. Xhafa, W. Gao, J. A. López-Salcedo, and G. Seco-Granados, "Performance Analysis of GNSS+ 5G Hybrid Positioning Algorithms for Smartphones in Urban Environments," *IEEE Transactions on Instrumentation and Measurement*, 2023.

[85] 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.

[86] 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.

[87] 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.

[88] 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.

[89] 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.

[90] 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.

[91] T. Wen, H. Jiang, B. Cai, and C. Roberts, "High-Speed Train Positioning Using Improved Extended Kalman Filter With 5G NR Signals," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] H. Chen, P. Zheng, M. F. Keskin, T. Al-Naffouri, and H. Wymeersch, "Multi-RIS-enabled 3D sidelink positioning," *IEEE Transactions on Wireless Communications*, 2024.

[98] 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.

[99] 3GPP, "NR and NG-RAN Overall Description," 3rd Generation Partnership Project, Technical Specification (TS) 38.305, March 2023, version 17.4.0.

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

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] 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.

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 researching 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. Before 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 with 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 (WSDL) at the University of Waterloo-Schlegel Research Institute for Aging. He is an (Adjunct + Research) professor at the University of Waterloo in the Department of Electrical and Computer Engineering as well as the Department of Mechanical and Mechatronics Engineering. Previously, he was an NSERC scholar at the Georgia Institute of Technology. Dr. Shaker also held multiple roles with RIM (BlackBerry). With close to twenty years of industrial experience in technology, and more than eight years as a faculty member leading projects related to the application of wireless sensor systems for healthcare, automotive, and unmanned aerial vehicles, Prof. Shaker has many design contributions to 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 has been the Canada Research Chair in the Future Internet. She was elected an IEEE Fellow for contributions to resource management in wireless and satellite networks in 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.