Law enforcement and position locating in LTE network (status and challenges)

Mustafa Abbas Shobar, Rami Tawil
Computer Sciences, Higher Institute for Doctorate in Science and Technology, Lebanese University, Beirut, Lebanon

Article Info

Article history:

Received May 25, 2023
Revised Jul 8, 2023
Accepted Aug 15, 2023

Keywords:

Artificial intelligence/machine learning
GSM
Location-based services
LTE
Radio frequency fingerprint

ABSTRACT

Since the advent of cellular networks represented by the first-generation GSM to the current generations (4G, 5G) represented by the LTE network. This brought about a qualitative revolution in cellular networks in terms of quality, speed, and efficiency. The emergence of cellular networks accompanied by the need to locate the user for commercial and marketing purposes, therefore emerge need for the concept of location-based services (LBS). However, with the increased reliance on cellular networks by users, there appeared a second trend to locate the user for security purposes and emergency. This was the first system established in the United States of America, called federal communication commission (FCC) 911. Position locating has also penetrated the military, security, and police investigations fields to locate criminals. Therefore, we review the methods of determining location in LTE networks. We evaluate each method and identify its weaknesses. In addition, we determine the most appropriate method for law enforcement. Based on the evaluation that showed the most effective way to determine the location used by law enforcement authorities is the radio frequency (RF) fingerprint. Then employment of artificial intelligence (AI)/machine learning (ML) to obtain an optimal method.

Corresponding Author:

Mustafa Abbas Shobar
Computer Sciences, Higher Institute for Doctorate in Science and Technology, Lebanese University
Beirut, Lebanon
Email: mustafa.shober@ul.edu.lb

1. INTRODUCTION

The increasing demand for mobile phone networks is due to the services provided by these networks, and because of the momentum of demand for cellular networks, a qualitative revolution occurred in them, which we are currently witnessing in the LTE network (4G and 5G). At the same time, the need to locate the user appeared in order to achieving financial gains as it invested in commercial marketing and location services (LCS), which called location-based services (LBS) for example the nearest shopping mall, restaurant, commercial show, gas station, cinema, and fast food. The other reason, which is to benefit from locating the user in emergency situations, as the United States of America was a pioneer in this field by establishing the 911 federal communication commission (FCC) system, which depends on locating emergency callers [1]. It should note that every service that provided has two uses. First, which known as normal use, for example, the regular user who benefits from these services to communicate with friends, relatives, and the outside world. Second, which is known as abnormal use, for example, the use of these services by organized crime gangs, terrorist organizations, and local criminals to perform their illegal actions, so there was an urgent need to employ methods of determining the location of the user in military operations and police investigations. Recently, criminal activity has evolved and greatly diversified in the performance of criminal acts, this in itself represents a major obstacle and challenge to the law enforcement authorities.

Because of these reasons, there was a challenge for researchers and developers to find the best method characterized by high accuracy, rapid response, and low cost [2]. Therefore, the solutions offered varied as well as their efficiency and method of work, but it is limited to providing solutions for the field related to LBS. In this research, we review the methods used to locate the user, evaluate each method, and determine the best approach that can used. In addition to the possibility of using these methods by law enforcement authorities.

2. LTE NETWORK

Before going into the details of the methods used to locate the user in the LTE network, we must first know the additions and improvements that the LTE network brought and formed a qualitative revolution in cellular networks. As the revolutionary change in the LTE network included all aspects (hardware components, software, structure, and way of working), as the LTE network consists of two main parts (core network and access network) with a lot of interfacing and signaling messages to ensure quality of service, speed of response, and ensuring that the call does not drop as showing in Figure 1 [3]. In addition to that, in the LTE network, there is a part for determining the location called positioning architecture, which is a precedent in cellular networks due to the absence of this part in previous cellular networks. This makes the handling of LTE positioning better and smoother when determining the location [3], [4]. The new positioning architecture in LTE networks is promising for user equipment (UE) location, as well as other areas like unmanned aerial vehicles (UAV) based cellular networks and LBSs.

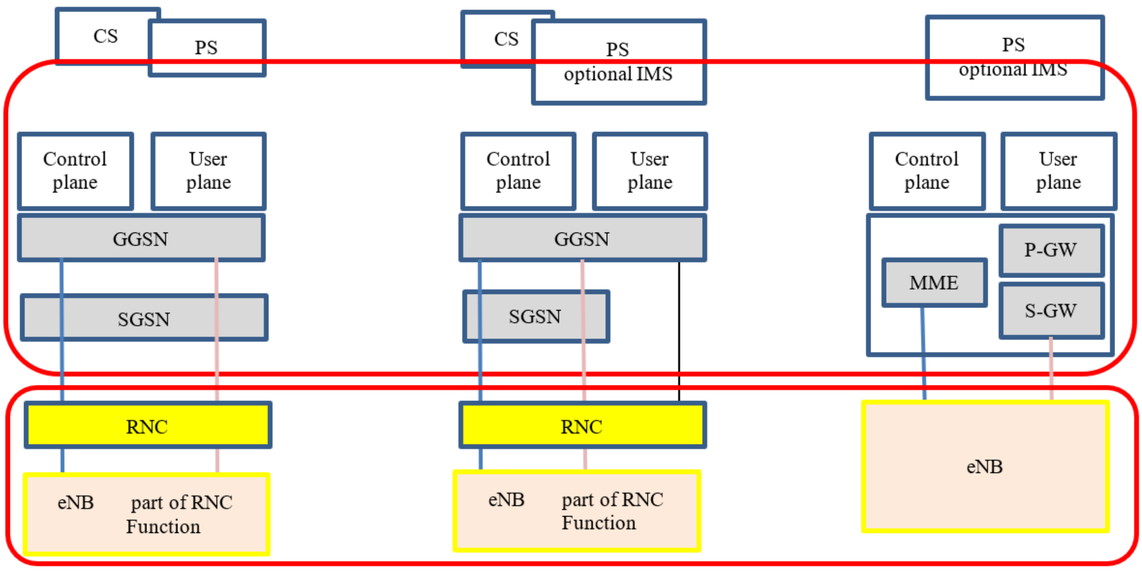

Figure 1. LTE architecture [3]

2.1. Positioning architecture

The position architecture in LTE contain three main components: i) LCS client, ii) LCS server, and iii) LCS target. Each of these elements has its own function, as the LCS server work as an existence that deals with the location of the LCS target device and collects some location information data, which in turn helps the UE to locate the data when needed and gauge the LCS target location [3]–[5]. An LCS client includes a component (hardware and software) and the LCS server to acquire the location data, as well as the LCS server to process the instance and send the outcomes. In turn, the LCS client quickly appreciates it [3]–[7].

2.2. Control plane positioning

To conquer possible network crowding in a contingency scenario, control plane positioning is fast, credible, and immune. LBS sessions established using the C-plane protocol, and assistance messages exchanged using the 'control' channels LTE positioning protocol (LPP). There are three ingredients which called (network initiated location request (NILR), mobile terminated location request (MTLR), mobile originated location request (MOLR)) is responsible for characterized the call flows of control plane [5]–[8].

2.3. User plane positioning

The data link is used to send location information in user plane location determination of the LTE network, where enabled by secure user plane location (SUPL). For the purpose of obtaining ancillary data and processing SUPL messages, the SUPL must be eligible to interact with the evolved serving mobile location center (E-SMLC). Relying on the data link, the LTE packet data network gateway (P-GW) and serving gateway (S-GW) elements forward SUPL messages. In addition, the SUPL supports both key positioning and emergency positioning [7]–[9].

2.4. Positioning techniques in LTE

In the LTE network, there are five standard ways to determine the location; each technique differs from the other in its working and mechanism. Where researchers and developers tried to find a technique characterized by high accuracy, speed of response, and low cost, so the technique varied to find an ideal way to determine the location. However, the results were not satisfactory, so the hybrid methods and radio mapping methods adopted. In this section, we debate the species of standard technique in LTE for positioning, in addition to the hybrid methods and radio map methods.

2.4.1. Enhanced cell ID

It is one of the oldest methods used to locate the UE in cellular networks (3G). The principle of this method is to identify the tower to which the UE connected, as well as the scoter within the coverage range of the tower, where this method called cell ID (CID) [10]. As for the LTE network and the revolutionary developments associated with this network, there have been improvements to this method and for this reason, it called enhanced cell ID (E-CID). The difference between the E-CID method and its predecessors is the calculation of by which the UE and the evolved NodeB (eNB) are separated measuring round trip time (RTT) [11]. This method contains three steps: first, it depends on the duration of sending a message in real time, where the eNB measures the duration of sending a message in real time sent by a recipient as in (1) [12]:

$$eNBx - Tx = T_{eNBRx} - T_{eNBTx} \tag{1}$$

Secondly, eNB then issues a time advance (TA) command to the UE; the purpose of this command is to correct the uplink timing. Third, as a result, the UE measures the RTT and sends it back to the eNB as in (2):

$$UERx - Tx = T_{UERx} - T_{UETx} \tag{2}$$

The E-CID method has some benefits such as low cost, easy development does not require any user interaction, and works with all types of phones. At the same time, it contains disadvantages first; the accuracy is restricted and does not have stable results. Second, it affected by external factors. Third, it needs a complete database and it needs to install an antenna array in the eNB. Final, it depends on at least three cell towers to locate the UE, i.e. the method cannot implemented in remote areas [13]–[15].

2.4.2. Observed time difference of arrival

The main idea of this method is that the signal send from the UE more than tow eNBs can locate the overlapping point [15]. The UE measures the reference signal time difference (RSTD) of sundry eNBs, then statements these variations to the enhanced serving mobile location centre (ESMLC). Thus, the EMLC is responsible for calculating the location of the UE by relying on the reported time differences and the location of the eNBs [6]. It should note that when the UE linked to one eNB for a certain period, it is at the same time exchanging data with other eNBs. The meaning of data trading with other eNBs is to ensure the quality of the call as well as not to drop the call while withdrawing from the eNB broadcast field to which it connected, in addition to easily distributing it while leaving the coverage area [1]–[3]. Therefore, depending on the different receiving time of the signal sent from three cell towers to the UE, the relative distance of the UE from each eNB can measured. The location of the UE specified by the interchange of the distance of each eNB [12], [16]. This method has advantages such as it does not need any interaction by the user or the device and good accuracy). Nevertheless, at the same time, this method suffers from an increase in cost due to the addition of equipment to the network. Where additional devices called location measurement unit (LMU) added, where they synchronize eNBs because they not synchronized with each other. The method also needs to change the structure of the network to suit the nature of its work to operate with the required efficiency. The process of developing the method is very complex and needs a long period. In addition, the method is not effective in remote areas [9], [12], [17]–[19].

2.4.3. Assisted global navigation satellite systems
With the help of an independent global navigation satellite systems (GNSS) system, mobile devices can receive satellite signals and determine their location. GNSS is also able to receive signals from various satellite systems like the United States global positioning system (GPS), the European Union's Galileo, the Russian GLONASS, and the Chinese BeiDou. The technology also suffers from many difficulties, including difficulty receiving data, energy consumption, processing speed, and time to first fix (TTFF) response time. Therefore, there was an urgent need to address these shortcomings by developing or establishing an auxiliary system for GNSS. As a result, assisted global navigation satellite systems (AGNSS) technology introduced. It works initially by adding GNSS equipment to the network independently. Its purpose is to speed up the transmission and reception of satellite signals [8]. The main difference between the work of GNSS and AGNSS is that the latter improves several parameters, including reducing energy consumption, enhancing the positioning process, and enhancing the sensitivity of the receiver. With all these improvements in AGNSS technology, it still suffers from location determination in urban cities with the presence of tall buildings, in addition to its limited use in smart devices, meaning that it does not work with old devices [17]–[19].

2.4.4. Radio frequency fingerprint
The radio characteristics of the cell serve as a basis for this positioning technology in the LTE network. Where the UE sends the measurements periodically every 20 ms to the eNB, where the E-SMLC is responsible for checking them. These measurements are CID, received signal strength indicator (RSSI), reference signal received power (RSRP), reference signal received quality (RSRQ), angle of arrival (AOA), observed time difference of arrival (OTDOA), and AGNSS. These measurements sent from UE to all nearby eNBs in the area Figure 2. The method include two phases, the first called the offline phase and the second called the online phase, each of these phases contains many operations [3], [20], [21].

a. The offline phase: in this phase, it contains many steps that must implemented to ensure that the method works perfectly. They can summarized in [20]–[23]:
   - Selecting the region in which the UE is to be located.
   - Implementation of the partition model according to the nature of the area and the idea of the developer, the partition model determines the accuracy of the method (i.e., whenever the partition model is integrated, the results are ideal).
   - The process collecting measurements or a measurements campaign, the measurements campaign can take a long time depending on the specific region.
   - Measurements integration in this step, it ensured that all measurements have collected according to the partition model without any loss of measurements.
   - The process of storing the measurements for the selected area after completing step d in a database.
   - According to the purpose of the method, several operations can be performed on the database, such as classification and distribution in accordance with the work of the method Figure 2.

b. The online phase: this method contains two steps [21]–[23]:
   - Choosing one of the matching algorithms or a proposed algorithm for matching the measurements sent from UE to eNB through E-SMLC with the database.
   - Returns the match result as the location of the UE from step a Figure 2.

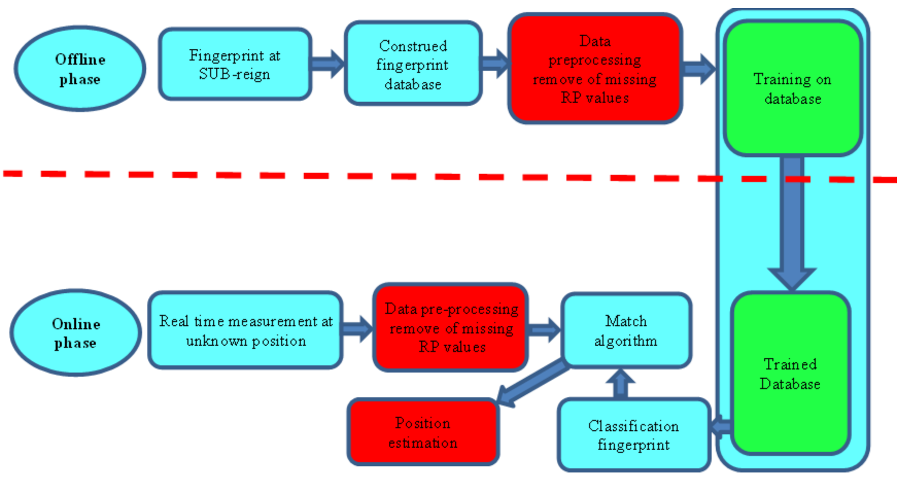

Figure 2. Fingerprint structure

2.4.5. Hybrid

In this method, two or more positioning techniques combined to obtain better results. For example, to avoid the defects in AGNSS technology in cities when there are tall buildings, OTDOA technology used to correct errors resulting from AGNSS technology [24]. In another case, three technologies collected such as CID, AGNSS, and OTDOA [25]. Common disadvantages of this method are delay, cost, energy consumption, and computational consumption.

3. LITERATURE REVIEW

In this section, we review the works and methods for UE positioning technologies that have employed in LTE network. In addition to the improvements and developments to determine location, also the problems encountered and how to overcome them. These solutions and developments added to the positioning techniques because the results obtained from the standard methods were not satisfactory and need to develop to keep up with the requirements facing the positioning technologies for many reasons. Each method's defects also identified, by comparing the methods used and the approach taken. In addition, identify the requirements for their works and drawbacks.

Research by Vaghefi and Buehrer [26], the UE positioning approach follows a collaborative approach based on radio frequency pattern matching (RFPM). Well arranged to achieve this, the device-to-device (D2D) communication protocol used to ensure that the UE communicates with other UEs in the eNB service area. In increment to communicating with eNB. The basic idea of this method is to rely on communication of the UE with other UE in addition to the eNB. This is to collect measurements. This collaborative approach enabled using D2D that allows the UE to transmit signals with each other without the need for another medium such as eNB. A localization algorithm has also developed to estimate UE location by relying on direct measurements between UEs and eNB. Key features (cooperative radio frequency (RF), D2D, and localization algorithm) and drawbacks (measurements taken from a single path lead to errors in measurements and similarity problems, medium accuracy, computational complexity, long response time, and requires at least three towers to work perfectly). Using a collaborative localization approach, the researcher attempted to locate the UE in [27]. The collaborative approach uses a D2D communication protocol with OTDOA and RTT measurements as well as a maximum likelihood estimator. Key features (cooperative localization, D2D, OTDOA, RTT, and machine learning (ML)) and drawbacks (high cost, requires synchronization of UE with each other in addition to eNB, computational complexity, and requires at least three towers to work perfectly). Li and Lei [28] proposed converting the UE measurements into grayscale images and applying deep learning (DL) to solve the problem of locating the UE. As well as creating a fingerprint base based on grayscale images resulting from UE measurements conversion. Three main steps adopted to achieve this. First, the deep residual network (DRN) loss function is calculated using interrupt entropy. Secondly, DNN's dynamic learning rate is used. Third, finding the most appropriate fingerprint to locate the UE, utilizing data optimization techniques. Finally, a hierarchical training model based on DNN and transfer learning. The resent network used to obtain the improved fingerprint by training the image fingerprint database. Transfer learning based on the feed-forward neural network (FFNN) employed to obtain an ideal positioning model. Key features (deep neural network (DNN), resent, FFNN, DL, transfer learning, and multilayer perceptron (MLP)) and drawbacks (high cost, high computing, response time, computational complexity, suboptimal partition model, and requires at least three towers to function properly).

Sivers and Fokin [29] suggested relying on the OTDOA technique in addition to the positioning reference signal (PRS) to locate the UE. Three algorithms also used to determine the location, linear least squares (LLS), nonlinear Gauss-newton (GN), and Levenberg-Marquardt (LM), in addition to the Cramer-Rao lower bound (CRLB) algorithm. Each algorithm's performance compared with CRLB. The results show that the LLS algorithm has results close to LM in a specific case. Key features (LLS, GN, LM, OTDOA, and CRLB) and drawbacks (high cost, high computing, response time, computational complexity, requires at least three towers to function properly, and need to synchronize the UE with eNB). Gadka *et al.* [30] proposed a method based on the OTDOA technique with cell specific reference signal (CSRS) instead of PRS. This reliance came about because PRS loads radio network resources. In addition, an appropriate algorithm used inside the receiver, to gauge the time of arrival (TOA) of the signal depending on the decision sample of the cross-correlation function. The proposed algorithm determines the engagement threshold amidst the received signal and the reference mode signal. Key features (OTDOA, CSRS, and software defined radio (SDR)) and drawbacks (modified receiver, computational complexity, least three towers to function properly, need to synchronize the UE with eNB, increased cost, and longer response time).

Research by Ma *et al.* [31] a method based on the multidimensional scaling (MDS) algorithm proposed to remove the UE RSRP divergence. Where the MDS algorithm depends on the relative difference in RSPR between two UE. In addition, the method uses minimization of drive tests (MDT) reports creating a fingerprint database. In addition, the method uses a chip set added to UE to extract reports. Key features

(MDS, RSRP, and MDT) and drawbacks (weakness of the proposed partition model, high computing, relatively accurate, at least three towers are needed to function properly, relying on MDT reports to create a fingerprint, adding devices to receive reports, and high cost). Zhu *et al.* [32] proposed a method based on TA technology and OTDOA in addition to RSRP and RSTD. A fingerprint formed using TA, E-CID, PRS, and cell specific reference signal (CRS). These two technologies combined to create an accurate fingerprint. After completing the fingerprint database formation, the ML algorithm used to give a unified model for estimation. This done by relying on values that produce an ideal distribution that makes the target data more likely. Key features (OTDOA, TA, RSTD, RSRP, ML, and E-CID) and drawbacks (weakness of the proposed partition model, high computing, relatively accurate, at least three towers are needed to function properly, high cost, and need to synchronize the UE with all eNB in the service area).

Research by Han *et al.* [33] another approach taken through a mobile application running in the android environment. This based on the relationship between the distances from the UE to the eNB. In this application, this relationship analyzed to re-locate the UE. By analyzing measurements of received signal strength (RSS) in addition to mobile country code (MCC), mobile network code (MNC), location area code (LAC), and cell ID (CID). Key features (RSS, LAC, MNC, MCC, and E-CID) and drawbacks (need to UE user intervention, need at least three towers to work properly, the accuracy is estimated, and the application is only available for phones running on android). Research by Celik *et al.* [34] of the research an improvement on E-CID technology based on RSRP, azimuth parameters, and COST 231 Walfish-Ikegami path loss model presented. The method implemented in two different ways as the first method depends on RSRP and azimuth parameters. The second depends on the bandwidth, RSRP, and azimuth parameters. By comparing the results, the second method excels at determining the location. Key features (RSRP, azimuth parameters, COST 231 Walfish-Ikegami path loss model, and E-CID) and drawbacks (medium accuracy, need at least three towers to work properly, and response time).

Research by Mondal *et al.* [35], relies on a cluster-based RF fingerprinting approach, where the fingerprint database formed based on LTE and Wi-Fi signals. The selected area scanned through a smartphone that uses the Nemo Handy application in addition to the MDT to save time extracting measurements. The fingerprint database is formed using E-CID and Wi-Fi technology, by three measurements from each technology. Furthermore, in this approach, no preliminary training of the data takes place, because it depends on reducing the search space through the cluster. Key features (E-CID, Wi-Fi, grid-based RF fingerprinting, and hierarchical clustering, MDT) and drawbacks (medium accuracy, need at least three towers to work properly, smart phones only, and partitioning model is not ideal). Ryden *et al.* [36] proposes a new OTDOA technique based on RSTD to locate the UE. An iterative method hired to characterize the first channel tap in the channel impulse response (CIR). Iterative methods used to obtain the time delays associated with the first channel tap. After obtaining the results and comparing them with the non-iterative methods, it found that the iterative methods had better results in determining the location. Key features (OTDOA, TOA, RSTD, CIR, and iterative) and drawbacks (high cost, need at least three towers to work properly, and synchronize the UE and all eNBs in the service area).

Wigren *et al.* [37] proposes a new OTDOA technique based on RSTD to locate the UE. This approach synchronizes the uplink when creating a radio access (RA) for a UE wireless link. In addition to the arrival time of the signal, it selected with high accuracy by sampling at a higher frequency. Moreover, the Zadoff-Chu (ZC) sequence correlation method used in three cases (direct autocorrelation, autocorrelation using additive white Gaussian noise (AWGN), and autocorrelation using multipath fading channel). Key features (OTDOA, UTDOA, preamble detection, and passive positioning) and drawbacks (high cost, need at least three towers to work properly, and synchronize the UE and all eNBs in the service area). Research by Wigren *et al.* [37], an approach based on multi-RAT positioning nodes used to locate the UE. With the use of OTDOA technology to create the fingerprint database, after forming the fingerprint database, one of the cluster algorithms implemented to create clusters. In each cluster the cell ID and RTT are stored, and then a polygon contraction algorithm used to calculate the cluster limits. Furthermore, in this method, no data training takes place. It relies on defining cluster boundaries to reduce the search area. Through the analysis of the results, it found that the proposed method improves the UE location. Key features (OTDOA, RTT, polygon, multi-RAT positioning nodes, and cluster) and drawbacks (high cost, need at least three towers to work properly, synchronize the UE and all eNBs in the service area, and response time).

Shakir *et al.* [38] proposes a hybrid approach that combines RSRP and cell service area in addition to a simple prediction model. The method also depends on GPS measurements, antenna location, and antenna direction. Then the root mean square error calculated to ensure the method's accuracy. The results showed a relative improvement in the UE location accuracy. Key features (RSRP, GPS, simple prediction model, and cell service area) and drawbacks (need at least three towers to work properly, not effective on older devices, and response time). Research by Panchetti *et al.* [39], the OTDOA technique used to solve the synchronization problem in which a proposed synchronization algorithm is implemented. This approach used

PRS and precise timing. The algorithm results compared with AWGN, multipath channels, and the derivation of theoretical bounds. The basis for the proposed algorithm is to assume that the synchronization has already occurred for the server cell in addition to the neighboring cell with less error. Thus, the algorithm expands the exact time synchronization depending on the signal model and enhances it when the SNR decreases. Key features (OTDOA, PRS, proposed synchronization algorithm, and time synchronization) and drawbacks (need at least 3 towers to work properly, synchronize the UE and all eNBs in the service area, assuming synchronization causes a problem with knowing the exact time and is it compatible with other devices, and response time).

According to Rosado *et al.* [40], a hybrid approach used for the UE location combining an appreciation model founded on equispaced taps with a time-delay appreciation based on joint maximum likelihood (JML) time-delay appreciation and PRS. The effect of multithreading is addressed through a combined time delay and channel estimator. The multipath can distinguished by random tapping between the first two taps. Thus, the range performance in multipath improved, which reflected in the improvement in UE location estimation. Key features (joint time-delay and channel estimation, PRS, multipath channel modelling, and JML) and drawbacks (need at least three towers to work properly, synchronize the UE and all eNBs in the service area, cost increase, medium accuracy, and response time). McDermott *et al.* [41] proposed a collaborative approach based on uplink time difference of arrival (UTDOA) and RTT measurements in addition to applying the ML algorithm to locate the UE. The basis of the proposed approach is to allow the UE to communicate not only with the eNB in the service area but with neighboring eNBs as well as with the UEs in the same service area using the D2D protocol. D2D used to create a synchronization state between UE and eNBs. After extracting the measurements, the ML algorithm estimates the UE location. Key features (UTDOA, RTT, collaborative approach, and ML) and drawbacks (need at least three towers to work properly, synchronize the UE and all eNBs in the service area, cost increase, medium accuracy, and response time).

Chen *et al.* [42] proposed a hybrid method that combines TOA and AOA techniques, by collecting seven TOA measurements and one AOA. The reason for suggesting these measurements is to mitigate non-line-of-sight (NLOS). The method locates the UE by interrupting the seven reads of the TOA measurements plus to one AOA. This is without the need to know the initial information about the NLOS. By comparing the results with both the Taylor series algorithm (TSA) and the hybrid lines of position algorithm (HLOP), the hybrid approach is superior in UE positioning. Key features (TOA, AOA, NLOS, and hybrid method) and drawbacks (need at least three towers to work properly, synchronize the UE and all eNBs in the service area, and cost increase). Li *et al.* [43] proposed a hybrid method that combines time difference of arrival (TDOA) and GPS technology to locate the UE. This method founded on the Kalman filtering and least squares method. Kalman filtering is used to process data in a dynamic environment. This reflected in a state vector where it refreshed without prediction in real time through an iterative process. A Z transform and baseline restraint also used to ameliorate the traditional features from accelerated segment test (FASF algorithm). Key features (TDOA, GPS, Z transform, and Kalman filtering) and drawbacks (need at least three towers to work properly, synchronize the UE and all eNBs in the service area, cost increase, power consumption, and only works with smartphones).

Liu *et al.* [44] suggested relying on protocol 11.802, in addition to the K-nearest neighbor (KNN) algorithm with the development of some control parameters to define the location of the UE. According to this proposed method, a database of fingers formed based on Wi-Fi signals, where the data collected in a single path line. On the matching stage, the KNN used to match the UE measurements in real time with the fingerprint database to locate the UE. Key features (11.802, Wi-Fi, and fingerprint) and drawbacks (need at least three towers to work properly, the proposed partition model is not ideal, and only works with smartphones). Mondal *et al.* [45] propose a multi-objective genetic algorithm (MOGA) to obtain independent standardization of the grid cell layout (GCL) to locate the UE. The fingerprint database is formed using OTDOA and MDT technology to extract RSRP. The method also improved in two stages. The first stage is array-wise standardization of grid-cell units employing non-overlapping GCL. The second stage is creating an overlapping GCL. Through the results, it found that the proposed method improved accuracy. Key features (OTDOA, MDT, RSRP, and MOGA) and drawbacks (need at least 3 towers to work properly, the proposed partition model is not ideal, expensive, needs to synchronize UE and all eNBs in the service area, computational complexity, and medium accuracy).

Wigren [46] suggested relying on AOA, TA, and E-CID techniques in addition to RTT to locate the UE. The fingerprint database formed founded on the measurements of the above techniques, the path of loss, and RTT. The proposed method also shows how to create improved algorithms in order to increase accuracy and reduce learning time. After forming the fingerprint database, one of the segmentation algorithms used to form the cluster. The proposed algorithm calculates a point of contraction calculated better than the center of the cluster, to deal with cases where the center of weight of the cluster is far of bounds. Polygon angles calculated iteratively, and learning time reduced through a self-learning algorithm. Key features (E-CID, TA, AOA, RTT, and cluster) and drawbacks (need at least 3 towers to work properly, the proposed partition model is not ideal, needs to synchronize UE and all eNBs in the service area, computational complexity, and medium accuracy). He and So [47] proposed a hybrid method that combines TDOA technology with fingerprinting based on the uplink sounding reference signal (SRS). Since the SRS contains information about the time and strength of the received signal, it facilitates the formation of a fingerprint database. The proposed method divided into two steps that facilitate the identification of the UE location. The first step is to place sensors in the eNBs to estimate the TDOA. This procedure detects the peak in the SRS devices by using the least squares calculation of a rough target location. The second step is to create a database of fingerprints from sub-regions based on a DNN to get an appreciation of the final location of the UE. Key features (TDOA, SRS, fingerprinting, DNN, and RSS) and drawbacks (need at least 3 towers to work properly, the proposed partition model is not ideal, needs to synchronize UE and all eNBs in the service area, computational complexity, and cost increase).

Alhafid and Younis [48] relied on OTDOA and RSTD technology in addition to the ML algorithm based on reference correlation. In addition, this paper, the effect of many factors on UE location accuracy known. Measurements from six adjacent cells used to prevent interference. Parameters such as PRS bandwidth, PRS periodicity, PRS sequence, consecutive sub frames, and power distribution used to locate the UE. Key features (OTDOA, RSTD, and ML) and drawbacks (need at least 3 towers to work properly, the proposed partition model is not ideal, needs to synchronize UE and all eNBs in the service area, computational complexity, and cost increase). Research by Fang and Ran [49] an approach based on a collaborative filtering algorithm proposed to produce a real-time commercial positioning system. Strong fingerprints generated based on TA and RSRP as well as GNSS MDT and KNN algorithm used for fast matching. After creating the fingerprint database, a collaborative filtering algorithm used to remove abnormal GNSS MDT measurements to increase UE location accuracy. Key features (TA, RSRP, collaborative filtering algorithm, KNN, and fingerprint) and drawbacks (need at least 3 towers to work properly, the proposed partition model is not ideal, needs to synchronize UE and all eNBs in the service area, computational complexity, cost increase, and only works with smartphones).

4. DISCUSSION CHALLENGES AND DIFFICULTIES

According to the previous literature review, there have been many attempts to locate the UE. Unfortunately, these attempts were limited to LBS to gain financial benefits or in emergency or disaster situations. With these attempts and methods proposed in the literature, suffer from shortcomings in work. In addition, no consideration given to what law enforcement authorities need to apprehend criminals.

4.1. Synchronize methods

Most of the methods employed (TA, AOA, TOA, TDOA, OTDOA, UTDOA, and collaborative approach) are of fairly significant accuracy, but they suffer from [26], [27], [29], [30], [32], [36], [37], [39], [41]-[43], [45]–[49]: i) need to synchronize the UE with the eNBs or the UEs in the cell's service area, ii) cost increases, iii) computational complexity, iv) power consumption, and v) if three towers not achieved, their work will significantly affected. Most methods that adopt these techniques are difficult to implement by law enforcement authorities. It requires full access to the cellular network to know the required synchronization time between the UE and the eNBs. This cannot achieved due to the policy of protecting user privacy. In addition, it requires adding devices to the cellular network. This in turn increases the cost and the time it takes to build the system.

4.2. Connectivity methods

In the case of other methods such as RSS, RSRP, and E-CID, they are low cost, do not need synchronization, and have no computational complexity. However, at the same time, it suffers from low accuracy and its reliance on three towers to function as required [31], [34], [35], [38]. It considered one of the most used methods by law enforcement authorities because it relies on the UE's communication with the eNBs. Through this method, the cell tower to which the UE is connected known, in addition to the sector through which the UE is covered. However, the main problem is determining the exact location of the UE. This is because the sector coverage area is large and difficult to determine based on this method alone.

4.3. Satellite methods

It is one of the most widely used technologies in smart phones, characterized by quick response, and easy location identification. Nevertheless, at the same time, it requires line of sight (LOS) between the device and the satellite. When this condition not met, it leads to a deviation in location determination. In addition, this technology is one of its biggest disadvantages, its large energy consumption. Therefore, law enforcement authorities cannot use this technology since it is limited to smart phones. In addition, the location determination process is for a limited period. Therefore, we see a trend to integrate AGNSS technology with another technology such as TA, which known as hybrid, to bypass energy consumption [17], [24], [29], [43].

4.4. Radio frequency Fingerprint

As for the methods that take RF fingerprinting as an approach, they also vary in accuracy, cost, computational complexity, and the need for synchronization. This is due to the technology used in fingerprint formation. In addition to the existence of shortcomings in the proposed partition model for the specified area, it was not at the required level with regard to dividing the area into sub-zones, the location of reference points, and the process of taking measurements. However, the fingerprint represents a promising area to invest in because it represents an open field, where more than one technology can be combined or rely on one technology to form a fingerprint. However, the shortcomings must be addressed in partition model like must be ideal in terms of the size of the sub-region and the distribution of reference points in it [22], [28], [32], [35], [37], [44]–[47]. By reviewing, the previous literature that tried to address most positioning technologies shortcomings or that provided a solution to a specific problem. This is shown in Tables 1 and 2. Added to it from the point of view of law enforcement authorities is the development of these criminal organizations in carrying out their illegal actions.

Table 1. Proposal work and the aim

Ref	Cell tower	Area	Proposal work	Aimed of work
[26]	At least three	Cities	Collaborative approach	Communication of the UE with other UE in addition to the eNB
[27]	At least three	Cities	Collaborative localization approach	Communication of the UE with other UE
[28]	At least three	Cities	Converting the UE measurements into grayscale images	Applying DL to solve the problem of locating the UE
[29]	At least three	Cities	OTDOA technique in addition to the PRS	Enhanced the OTDOA with PRS
[30]	At least three	Cities	OTDOA technique with CSRS	Correlation threshold of the received signal and the reference mode signal
[31]	At least three	Cities	MDS algorithm	Remove the UE RSRP variation
[32]	At least three	Cities	OTDOA in addition to RSRP and RSTD	Create an accurate fingerprint
[33]	At least three	Cities	Mobile application	The relationship between the distance from the UE to the eNB
[34]	At least three	Cities	Improvement on E-CID technology	The bandwidth, RSRP, and azimuth parameters to locate the UE
[35]	At least three	Cities	Cluster-based RF fingerprinting approach	The fingerprint database is formed using E-CID and Wi-Fi
[36]	At least three	Cities	OTDOA technique based on RSTD	An iterative method is used to distinguish the first channel tap in the CIR
[50]	At least three	Cities	Boot sequence capture approach and OTDOA	Synchronizes the uplink when creating a RA for a UE wireless link
[37]	At least three	Cities	Multi-RAT positioning nodes and OTDOA fingerprinting	Calculate the cluster limits
[38]	At least three	Cities	Hybrid approach that combines RSRP and cell service area	Ensure the method's accuracy
[39]	At least three	Cities	Synchronization algorithm	Synchronization has already occurred for the server cell in addition to the neighboring cell with less errors
[40]	At least three	Cities	JML time-delay estimation and PRS	Combining an appreciation model founded on equispaced taps with a time-delay appreciation
[41]	At least three	Cities	Collaborative approach based on UTDOA and RTT	To create a synchronization state between UE and eNBs
[42]	At least three	Cities	Hybrid method that combines TOA and AOA	Located the UE by interrupting the seven reads of the TOA measurements plus to one AOA
[43]	At least three	Cities	A hybrid method that combines TDOA and GPS	State vector it is refreshed without prediction in real time through an iterative process
[44]	At least three	Cities	Relying on protocol 11.802 and KNN	A database of fingerprint is formed based on Wi-Fi signals
[45]	At least three	Cities	MOGA Algorithm to obtain independent calibration of the grid cell layout GCL	Improved accuracy of located UE
[46]	At least three	Cities	Relying on AOA, TA, and E-CID	Increase accuracy and reduce learning time
[47]	At least three	Cities	A hybrid method that combines TDOA with fingerprinting based on the uplink SRS	DNN to get an estimate of the final location of the UE
[48]	At least six	Cities	Relied on OTDOA and RSTD	Measurements from six adjacent cells were used to prevent interference
[49]	At least three	Cities	Collaborative filtering algorithm	Produce a real-time commercial positioning system

Table 2. Comparison of positioning techniques depending on several criteria

Problem	Response time	Solution approach	Cost	Power	Hardware change	Complexity	Accuracy		Ref
							Rear	City	
UE communicates with other UEs in the eNB service area	High	Collaborative based RFPM	Medium	Medium	Yes	Yes	Poor	Medium	[26]
	Low	Collaborative based OTDOA AND RTT	High	High	Yes	Yes	Poor	Good	[27]
	Medium	Collaborative approach based on UTDOA and RTT, ML algorithm	High	Medium	Yes	Yes	Poor	Good	[41]
Bypassing radio signal interference	High	Converting the UE measurements into grayscale images	High	High	No	Yes	Poor	Good	[28]
Choosing the best algorithm among (LLS, GN, LM, CRLB)	Medium	OTDOA technique and PRS	High	High	No	Yes	Poor	Good	[29]
Avoid loads radio network resources	High	OTDOA technique with CSRS	High	Low	Yes	Yes	Poor	Good	[30]
Eliminate the UE RSRP difference	Medium	MDS algorithm	High	Medium	Yes	No	Poor	Medium	[31]
Unified model for estimation	Low	Fingerprint based OTDOA, TA, E-CID, RSRP, RSTD, PRS, CRS	High	High	No	Yes	Poor	Good	[32]
Located UE	Low	Mobile application running in the Android environment.	Medium	High	Yes	No	Poor	Relative	[33]
Improvement E-CID	Medium	Bandwidth, RSRP and azimuth parameters	Medium	Low	No	No	Poor	Medium	[34]
Reducing the search space	Medium	Cluster-based RF fingerprinting	Low	Low	No	No	Poor	Medium	[35]
Identify the first channel tap	Medium	Iterative method on OTDOA with RSTD, CIR	High	High	No	Yes	Poor	Good	[36]
Synchronizes the uplink when creating a RA for a UE wireless link	Medium	Sampling at a higher frequency	High	High	No	Yes	Poor	Good	[50]
Calculate the cluster limits	High	Fingerprint based OTDOA, RTT, E-CID	High	High	No	Yes	Poor	Good	[37]
Ensure the method's accuracy	High	Hybrid approach combines RSRP and cell service area	Medium	High	No	No	Poor	Good	[38]
Synchronization problem	Low	OTDOA, proposed synchronization algorithm	High	High	Yes	Yes	Poor	Good	[39]
The effect of multithreading	Low	Hybrid approach combining an appreciation model based on equispaced taps and time-delay appreciation based on JML time-delay estimation	High	Medium			Poor	Good	[40]
Mitigate NLOS	Low	A hybrid method combines TOA and AOA	High	High	No	No	Poor	Good	[42]
Process data in a dynamic environment	Medium	hybrid method combines TDOA and GPS	High	High			Poor	Good	[43]
Determine the location of the UE	High	Fingerprint based on protocol 11.802, in addition to KNN algorithm	Medium	Medium	No	No	Poor	Good	[44]
Independent calibration of the grid cell layout GCL	Medium	Fingerprint based OTDOA and MDT, MOGA Algorithm	High	Low	No	Yes	Poor	Medium	[45]
Reduce learning time	Low	Fingerprint based AOA, TA, and E-CID, RTT	High	Medium	No	Yes	Poor	Good	[46]
Detects the peak in the SRS devices	Medium	Hybrid combines TDOA fingerprint based on uplink SRS	High	Medium	Yes	Yes	Poor	Good	[47]
Prevent interference	High	OTDOA and RSTD technology in addition to the ML algorithm	High	Medium	No	Yes	Poor	Good	[48]
A real-time commercial positioning system	Medium	Collaborative filtering algorithm, fingerprints are based on TA, RSRP, GNSS MDT, KNN	High	High	No	Yes	Poor	Good	[49]

Most of these organizations well aware of the shortcomings in locating methods and trying to exploit these shortcomings to their advantage. First, for example, smart phones are not used by these organizations, but rather they rely on old-fashioned phones that are not equipped with GPS or any smart application, so any method that relies on smart phones becomes ineffective. In addition to methods that depend on user intervention to determine location. Secondly, these organizations avoid densely populated residential areas or cities to refuge, knowing that most of the roads depend on three towers to determine their location. That is why they resort to remote areas (countryside, desert, and mountain) to take them as a refuge because the condition of three towers not met in those areas, which is the basis for locating methods. Finally, researchers and developers not address these problems and support law enforcement authorities to perform their duties is due to the lack of financial returns. That is, remote areas have a small percentage of the population, so there is no financial sense in establishing a positioning system such as LBS. Furthermore, companies that provide cellular service are looking for profit gains, so we see a focus on the city by covering the city with the largest number of cellular towers to withstand the momentum on the network and ensure quality of service (QoS). In remote areas, the percentage of the population is low and the financial returns are low, so those areas only served by one cell tower. However, with an amendment the strength of the transmitted signal is high to cover the largest possible area. In addition, the researchers see that it is not feasible to invest in those areas with the presence of the GPS navigation system, as it is not very effective and accurate due to LOS between the device and its satellites.

4.5. Law enforcement requirements for locating UE

Through what has discussed to establish a method that assists law enforcement authorities in carrying out their duties. Keep in mind that the requirements for creating a method to assist law enforcement authorities differ from the requirements for LBS-based or emergency situations. These requirements include:

- Response time: time is a crucial factor when dealing with any accident or crime, so the response time between the time of the accident and the time it takes to locate the site should be as short as possible.
- Cost: the cost of establishing and implementing the method should be as low as possible since we are not anticipating financial returns.
- Computational complexity: the computational complexity must be reasonable to ensure response speed in addition to not increasing the cost.
- User interaction: the method should not require user interaction to locate the user's phone.
- Phone type: in order for the method to work effectively, it must encompass all types of phones, not just a specific type of phone.
- Added devices: the method must not need to add any devices to the network or the phone, because this increases the cost and time of creation. In addition, there is no guarantee that criminals will use the modified phone.
- Accuracy: the method must be accurate in determining the phone's location, to reduce search space.
- Energy consumption: the method should consume the least amount of energy.
- Number of cell towers needed: the method should work best with one cell tower. This is to ensure that the phone is located in remote areas.
- Remote area

5. CONCLUSION

In this paper a survey was proposed in which a revision was made for the positioning technologies and the main process done to accomplish the positioning requirements. As well as, a discussion of the main improvements made to these technologies in order to obtain the required satisfactions. In addition to the deficiency of the law enforcement authorities used to define the location of a UE, one of the biggest challenges of the localization procedure that can occur is locating in remote areas, especially areas covered by a single cell tower, this survey concludes that the best reliable approach to be adopted is the RF fingerprint of a mobile device. As result, the survey provide the importance of the discussed field in order to invest in, for the following reasons; first, it provides the reasons to avoid the technologies that need synchronization, second, give advantage of relying on communication between the UE and the eNBs to exchange information in order to take measurements, third, how to avoid relying on collecting measurements from one track to localize mobile devices by creating a clustering model for the target area, finally, we discussed the use of artificial intelligence techniques such as reinforcement learning (RL), DL, and deep reinforcement learning (DRL) for classification and matching points in order to have better localization process. So far, according to what has seen and reviewed of the works related to locating the phone in the LTE network, no addressing has done or addressing the locating of the cell phone through a single cell tower.

ACKNOWLEDGEMENTS

The authors would like to thank University of Babylon, College of Information Technology, Department of Information Networks (it.uobabylon.edu.iq) Babylon, Iraq and Lebanese University, Higher Institute for Doctorate in Science and Technology (ul.edu.lb) Beirut, Lebanon for its support in the present work.

REFERENCES

[1] M. F. M. Mahyuddin, A. A. M. Isa, M. S. I. M. Zin, M. A. H. Afifah, Z. Manap, and M. K. Ismail, "Overview of positioning techniques for LTE technology," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 2–13, pp. 43–50, 2017.

[2] M. A. Shober and S. B. Sadhkan, "A developed method to locate a mobile phone in remote areas," in *2019 2nd International Conference on Engineering Technology and its Applications (IICETA)*, 2019, pp. 179–184, doi: 10.1109/IICETA47481.2019.9012993.

[3] A. Elnashar, M. A. El-saidny, and M. R. Sherif, *Design, Deployment and Performance of 4G-LTE Networks*. West sussex, UK: Wiley, 2014, doi: 10.1002/9781118703434.

[4] D. Kakadia, J. Yang, and A. Gilgur, "Evolved Universal Terrestrial Radio Access Network (EUTRAN)," in *Network Performance and Fault Analytics for LTE Wireless Service Providers*, New Delhi: Springer, 2017, pp. 61–81, doi: 10.1007/978-81-322-3721-1_3.

[5] M. Thorpe and E. Zelmer, "LTE Location Based Services Technology Introduction," *Rohde & Schwarz*, pp. 1–22, 2015.

[6] A. Kaushal, A. Malhotra, and H. Vohra, "Location-based services & positioning technique using SUPL (Secure User Plane Location)," *L&T Technology Services*, pp. 1–11, 2015.

[7] A. Kangas, I. Siomina, and T. Wigren, "Positioning in LTE," in *Handbook of Position Location*, Hoboken, New Jersey: John Wiley & Sons, 2019, pp. 1165–1218, doi: 10.1002/9781119434610.ch32.

[8] "An overview of LTE Positioning," *Spirent Communications*, pp. 1–12, 2012.

[9] S. Fischer, *Observed Time Difference Of Arrival (OTDOA) Positioning in 3GPP LTE*. California, USA: Qualcomm Technologies, 2014.

[10] P. Skeffington and S. Vant, *Assessment of Mobile Location Technology*. London, UK: Mot MacDonald, 2010.

[11] J. Willaredt, "WiFi and Cell-ID based positioning-protocols, standards and solution," *SNET Project WT*, 2011.

[12] 3GPP LTE, *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements*. France: ETSI, 2016.

[13] S. M. Razavi *et al.*, "Positioning in cellular networks: Past, present, future," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6, doi: 10.1109/WCNC.2018.8377447.

[14] C. H. Chen and K. T. Feng, "Enhanced distance and location estimation for broadband wireless networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2257–2271, 2015, doi: 10.1109/TMC.2015.2398419.

[15] R. S. Campos and L. Lovisolo, *RF Positioning: Fundamentals, Applications, and Tools*. Boston, MA: Artech House, 2015.

[16] A. S. -Dannert, "Positioning Technologies and Mechanisms for mobile Devices," in *Seminar Master Module SNET2 (TU-Berlin, ed.)*, 2010, pp. 1–11.

[17] J. R. Rufa and E. M. Atkins, "OTDOA/GPS Fusion for Urban UAS Navigation using Particle Filtering Techniques," in *AIAA Guidance, Navigation, and Control (GNC) Conference*, 2013, pp. 1–18, doi: 10.2514/6.2013-4878.

[18] A. Clarkson, S. McCallum, N. Solhjoo, and S. Velentzas, "Hybridised Positioning Algorithms in Location Based Services," in *proceedings of the 1st workshop on positioning navigation and communication(WPNC'04)*, 2004, pp. 101–106.

[19] 3GPP LTE, *Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN*. France: ETSI, 2017.

[20] B. Singh, S. Pallai, and S. K. Rath, "A Survey of Cellular Positioning Techniques in GSM Networks," in *National Conference in Mobile Computing*, 2011, pp. 1–16.

[21] S. A. Hussain *et al.*, "Positioning a Mobile Subscriber in a Cellular Network," *IAENG International Journal of Computer Science*, vol. 34, no. 2, pp. 1–6, 2007.

[22] B. Abdelghani and G. Qiang, "A novel fingerprinting positioning approach in urban cellular networks," in *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, 2016, pp. 155–159, doi: 10.1109/ICCSN.2016.7586639.

[23] G. Ding, J. Zhang, L. Zhang, and Z. Tan, "Overview of received signal strength based fingerprinting localization in indoor wireless LAN environments," in *2013 5th IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, 2013, pp. 160–164, doi: 10.1109/MAPE.2013.6689973.

[24] C. Mensing and S. Sand, "Performance enhancement of GNSS positioning in critical scenarios by wireless communications systems," in *2008 IEEE/ION Position, Location and Navigation Symposium*, 2008, pp. 334–340, doi: 10.1109/PLANS.2008.4570053.

[25] G. D. Angelis, G. Baruffa, and S. Cacopardi, "GNSS/cellular hybrid positioning system for mobile users in Urban scenarios," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 313–321, 2013, doi: 10.1109/TITS.2012.2215855.

[26] R. M. Vaghefi and R. M. Buehrer, "Cooperative RF pattern matching positioning for LTE cellular systems," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, 2014, pp. 264–269, doi: 10.1109/PIMRC.2014.7136172.

[27] R. M. Vaghefi and R. M. Buehrer, "Improving positioning in LTE through collaboration," in *2014 11th Workshop on Positioning, Navigation and Communication (WPNC)*, 2014, pp. 1–6, doi: 10.1109/WPNC.2014.6843292.

[28] D. Li and Y. Lei, "Deep learning for fingerprint-based outdoor positioning via LTE networks," *Sensors*, vol. 19, no. 23, pp. 1–15, 2019, doi: 10.3390/s19235180.

[29] M. Sivers and G. Fokin, "LTE Positioning Accuracy Performance Evaluation," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Cham: Springer, 2015, pp. 393–406, doi: 10.1007/978-3-319-23126-6_35.

[30] P. Gadka, J. Sadowski, and J. Stefanski, "Detection of the First Component of the Received LTE Signal in the OTDoA Method," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–12, 2019, doi: 10.1155/2019/2708684.

[31] L. Ma, N. Jin, Y. Cui, and Y. Xu, "LTE user equipment RSRP difference elimination method using multidimensional scaling for LTE fingerprint-based positioning system," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6, doi: 10.1109/ICC.2017.7997470.

[32] J. Zhu, X. Luo, and D. Chen, "Maximum likelihood scheme for fingerprinting positioning in LTE system," in *2012 IEEE 14th International Conference on Communication Technology*, 2012, pp. 428–432, doi: 10.1109/ICCT.2012.6511256.

[33] S. Han, T. Kang, and J. Seo, "Smartphone Application to Estimate Distances from LTE Base Stations Based on Received Signal Strength Measurements," in *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, 2019, pp. 1–3, doi: 10.1109/ITC-CSCC.2019.8793365.

[34] G. Celik, H. Celebi, and G. Tuna, "A novel RSRP-based E-CID positioning for LTE networks," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 1689–1692, doi: 10.1109/IWCMC.2017.7986538.

[35] R. U. Mondal, J. Turkka, and T. Ristaniemi, "An efficient cluster-based outdoor user positioning using LTE and WLAN signal strengths," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2015, pp. 2182–2186, doi: 10.1109/PIMRC.2015.7343659.

[36] H. Ryden, A. A. Zaidi, S. M. Razavi, F. Gunnarsson, and I. Siomina, "Enhanced time of arrival estimation and quantization for positioning in LTE networks," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1–6, doi: 10.1109/PIMRC.2016.7794634.

[37] T. Wigren, A. Kangas, Y. Jading, I. Siomina, and C. Tidestav, "Enhanced WCDMA Fingerprinting Localization Using OTDOA Positioning Measurements from LTE," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, 2012, pp. 1–5, doi: 10.1109/VTCFall.2012.6398973.

[38] Z. Shakir, J. Zec, and I. Kostanic, "Position location based on measurement reports in LTE cellular networks," in *2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*, Apr. 2018, pp. 1–6, doi: 10.1109/WAMICON.2018.8363501.

[39] M. Panchetti, C. Carbonelli, M. Horvat, and M. Luise, "Performance analysis of PRS-based synchronization algorithms for LTE positioning applications," in *2013 10th Workshop on Positioning, Navigation and Communication (WPNC)*, 2013, pp. 1–6, doi: 10.1109/WPNC.2013.6533292.

[40] J. A. d. P. -Rosado, J. A. L. -Salcedo, G. S. -Granados, F. Zanier, and M. Crisci, "Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, p. 33, 2014, doi: 10.1186/1687-6180-2014-33.

[41] K. McDermott, R. M. Vaghefi, and R. M. Buehrer, "Cooperative UTDOA Positioning in LTE Cellular Systems," in *2015 IEEE Globecom Workshops (GC Wkshps)*, 2015, pp. 1–6, doi: 10.1109/GLOCOMW.2015.7414171.

[42] C. -S. Chen, Y. -J. Chiu, and J. -M. Lin, "Hybrid TOA/AOA Schemes for Mobile Location In Cellular Communications Systems," *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, vol. 1, no. 2, pp. 54–64, 2010, doi: 10.5121/ijasuc.2010.1205.

[43] C. -X. Li, W. -M. Liu, and J. -W. Wu, "High-precision positioning algorithm based on GPS," in *2010 2nd International Conference on Advanced Computer Control*, 2010, pp. 364–368, doi: 10.1109/ICACC.2010.5487145.

[44] X. Liu, S. Zhang, J. Quan, and X. Lin, "The experimental analysis of outdoor positioning system based on fingerprint approach," in *2010 IEEE 12th International Conference on Communication Technology*, 2010, pp. 369–372, doi: 10.1109/ICCT.2010.5689160.

[45] R. U. Mondal, T. Ristaniemi, and J. Turkka, "Genetic algorithm optimized grid-based RF fingerprint positioning in heterogeneous small cell networks," in *2015 International Conference on Location and GNSS (ICL-GNSS)*, 2015, pp. 1–7, doi: 10.1109/ICL-GNSS.2015.7217160.

[46] T. Wigren, "Fingerprinting localisation using round trip time and timing advance," *IET Communications*, vol. 6, no. 4, pp. 419–427, 2012, doi: 10.1049/iet-com.2011.0410.

[47] J. He and H. C. So, "A Hybrid TDOA-Fingerprinting-Based Localization System for LTE Network," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13653–13665, 2020, doi: 10.1109/JSEN.2020.3004179.

[48] A. K. Alhafid and S. Younis, "Observed time difference of arrival based position estimation for LTE systems: Simulation framework and performance evaluation," *Eastern-European Journal of Enterprise Technologies*, vol. 3, no. 9–105, pp. 20–28, 2020, doi: 10.15587/1729-4061.2020.201382.

[49] W. Fang and B. Ran, "An Accuracy and Real-Time Commercial Localization System in LTE Networks," *IEEE Access*, vol. 8, pp. 120160–120172, 2020, doi: 10.1109/ACCESS.2020.3004490.

[50] Y. Gao, Z. Deng, Y. Zhang, S. Sun, and Z. Li, "Mobile Phone Passive Positioning Through The Detection of Uplink Signal," in *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 2019, pp. 367–371, doi: 10.1109/SmartIoT.2019.00064.

BIOGRAPHIES OF AUTHORS

Mustafa Abbas Shobar received the B.Sc. degree in computer sciences from Shatt Al-Arab University College, Department of Computer Science, Basrah, Iraq in 2003, and the master's degree in information networks from the University of Babylon, College of Information Technology, Iraq, Babylon in 2020. He is Ph.D. student in computer sciences from the Higher Institute for Doctorate in Science and Technology, Lebanese University, Beirut, Lebanon. He is currently a student in computer sciences from the Higher Institute for Doctorate in Science and Technology, Lebanese University, Beirut, Lebanon. His current research interests include cellular networks, location technologies in cellular networks, UAV based cellular networks, and machine learning. He can be contacted at email: mustafa.shober@ul.edu.lb, shober@itnet.uobabylon.edu.iq, or shober_79@yahoo.com.

Rami Tawil is an associate professor at the Lebanese University; In 2009. He received his Ph.D. degree from Pierre et Marie Curie University, France in mobile networks. Since 2009, Rami Tawil is interested in research in several fields; fixed and mobile networks, quality of service (QoS), network security, trust and reputation, cloud computing, sensor networks, machine learning, computer vision, computer forensics, and risk management. He can be contacted at email: rami.tawil@ul.edu.lb.