Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 2315036, 17 pages
https://doi.org/10.1155/2017/2315036

WILEY | Hindawi

Review Article

Evolution of Positioning Techniques in Cellular Networks, from 2G to 4G

Rafael Saraiva Campos

Department of Computer Engineering, CEFET/RJ, Campus Petrópolis, Petrópolis, RJ, Brazil

Correspondence should be addressed to Rafael Saraiva Campos; rafaelsaraivacampos@gmail.com

Received 29 June 2016; Revised 3 October 2016; Accepted 18 October 2016; Published 12 January 2017

Academic Editor: Mauro Femminella

This review paper presents within a common framework the mobile station positioning methods applied in 2G, 3G, and 4G cellular networks, as well as the structure of the related 3GPP technical specifications. The evolution path through the generations is explored in three steps at each level: first, the new network elements supporting localization features are introduced; then, the standard localization methods are described; finally, the protocols providing specific support to mobile station positioning are studied. To allow a better understanding, this paper also brings a brief review of the cellular networks evolution paths.

1. Introduction

At first, the main drive behind the development of positioning techniques to support location services (LCS) in cellular networks was the need to locate any mobile station (MS) originating emergency calls. The Federal Communications Commission (FCC) issued the first regulation concerning the availability and accuracy of the localization of such calls in the USA, as far back as 1996 [1, 2]. In 2002, the European Union adopted a similar approach, but without defining minimum precision requirements for the estimated positions [3]. With the advances in both the cellular radio access networks (RANs) and core networks—particularly with the introduction of packet-switching—the mobile telephony operators and vendors devised a myriad of new commercial LCS applications. Those included location-based billing, location-based marketing, and location-based social networks.

This paper starts explaining the intrinsic positioning capabilities available in any cellular system and then describes the functions that have been added by the Third-Generation Partnership Program (3GPP) in the RAN and core networks through the generations—from the second generation (2G) to the fourth generation (4G)—to support enhanced LCS applications. To allow a better comparison, the same structure is used for all generations: we describe, first, the new network elements, then the standard localization methods, and finally the most important protocols supporting enhanced LCS functions.

1.1. Brief Review of Cellular Technologies Evolution, from 2G to 4G

1.1.1. 2G: Digital Voice and Circuit-Switched Data—GSM and IS-95. There were several 2G cellular systems, but the most important ones—as they were the starting points of two families of digital technologies, as shown in Figure 1—were the Global System for Mobile Communications (GSM) and IS-95, also known as cdmaOne. Both are fully digital and support voice and circuit-switched (CS) data at low rates (up to 14.4 Kbps) (1 Kbps = 1024 bits per second). Their most important difference lies in the multiple access technique employed in the RAN: GSM uses Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA)—200 kHz carriers with 8 time slots per frame—while IS-95 uses FDMA and Code Division Multiple Access (CDMA)—1.23 MHz carriers with multiple pseudonoise codes.

1.1.2. 2.5G: Introduction of Packet-Switched Data—GPRS and IS-95B. Along the years, data traffic on cellular networks kept increasing and new technologies supporting higher rates

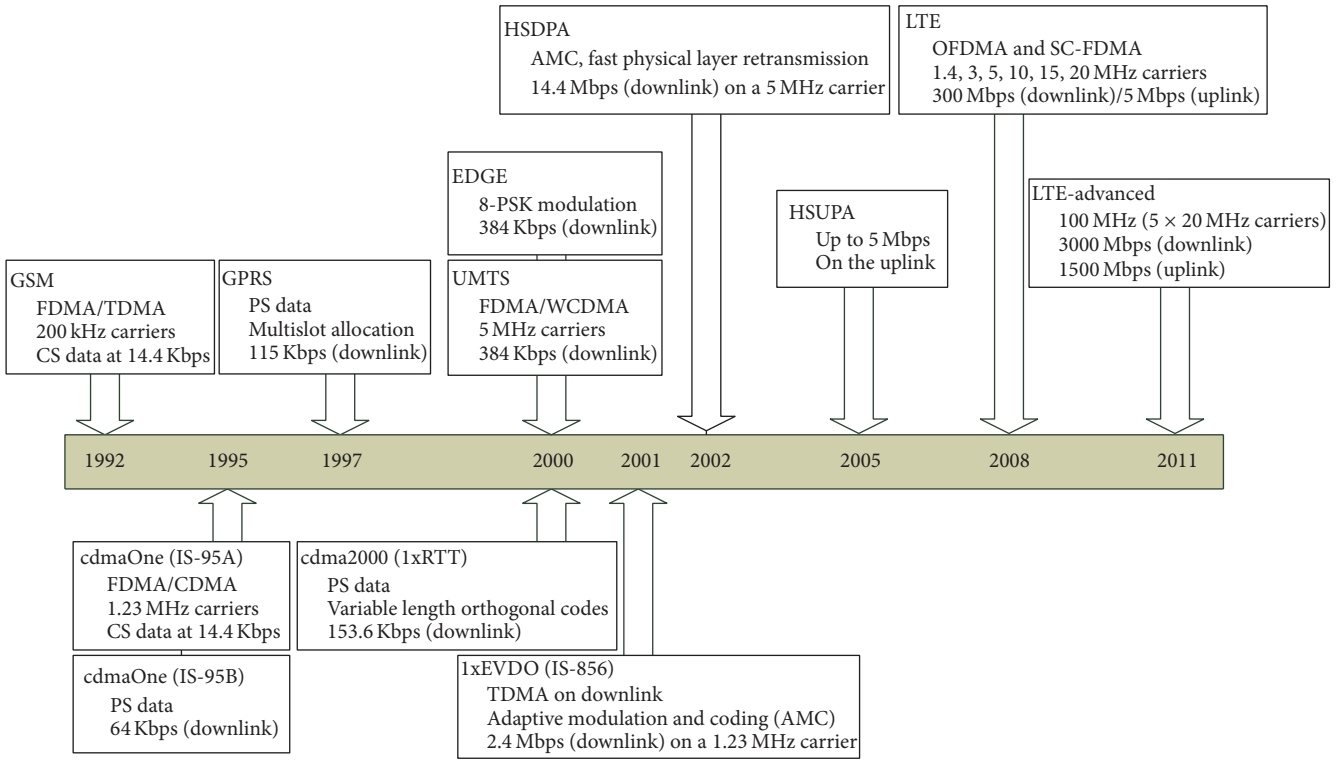

Figure 1: Evolution path of the two cellular technologies families: GSM (above) and CDMA (below). This timeline is greatly simplified; many intermediary standards have been ruled out. Only the evolution cornerstones are represented. The figure also brings some key features introduced by each standard, such as maximum achievable data rates, multiple access, and modulation techniques.

were demanded. Obviously, something beyond CS data was required. The General Packet Radio Service (GPRS) technology introduced the packet-switched (PS) domain in the GSM core network. GPRS uses the same modulation scheme of GSM in the RAN—Gaussian Minimum-Shift Keying (GMSK)—but, by assigning multiple time slots per user and using more efficient coding schemes, reaches higher data rates: up to 170 Kbps in the downlink [4]. On the cdmaOne family, packet-switching was introduced by IS-95B, with downlink rates of up to 64 Kbps. IS-95B networks were first deployed in September 1999 in South Korea and after that only in another four countries [5].

1.1.3. 3G: Improving the Data Rates—EDGE, 1XRTT, and UMTS. Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), and cdma2000 1xRTT (1x Radio Transmission Technology) were the first third-generation (3G) systems. While EDGE and UMTS belong to the GSM evolution path, 1xRTT is part of the cdmaOne family.

EDGE improved GPRS rates by using a modulation scheme of higher spectral efficiency, 8-PSK (phase-shift keying), which transmits three bits per symbol, while GMSK transmits only one bit per symbol. Theoretically, EDGE data rates would be three times higher compared to GPRS. In practice, EDGE peak downlink data rate is 384 Kbps [6].

UMTS shares essentially the same core network of GSM/GPRS/EDGE systems. However, the UMTS RAN is completely different from the GSM/GPRS/EDGE RAN (GERAN). While the GERAN uses 200 kHz carriers with 8 time slots per frame—that is, both FDMA and TDMA—the UMTS RAN uses Wideband Code Division Multiple Access (WCDMA) on a 5 MHz carrier [7]. Initially, UMTS download rates reached up to 384 Kbps, which is the same peak downlink rate of its predecessor, EDGE.

On the cdmaOne evolution path, cdma2000 1xRTT, defined by IS-2000, reached downlink rates of up to 153.6 Kbps by using variable length orthogonal codes and Quadrature Phase-Shift Keying (QPSK) modulation [8].

1.1.4. 3.5G: 1xEVDO and HSDPA. The next step on the evolution path of the cdmaOne family was 1xEVDO (1x Evolution Data Optimized), defined by IS-856. 1xEVDO uses adaptive modulation and coding (AMC), assigning forward error correction (FEC) codes with lower redundancy—that is, with higher code rates—and modulation schemes of higher spectral efficiency (e.g., QAM (Quadrature Amplitude Modulation) with 16 and 64 symbols) to users with higher signal-to-noise ratios (SNRs). This feature, coupled with sophisticated scheduling algorithms, allows 1xEVDO to achieve a peak downlink rate of 2.4 Mbps on a 1.23 MHz carrier. The 1xEVDO carrier has the same bandwidth of IS-95 and IS-2000 carriers but, unlike those earlier systems, supports only PS data. On the downlink, 1xEVDO uses TDMA with variable length time slots (whose length is dynamically determined by the scheduling algorithm) [9].

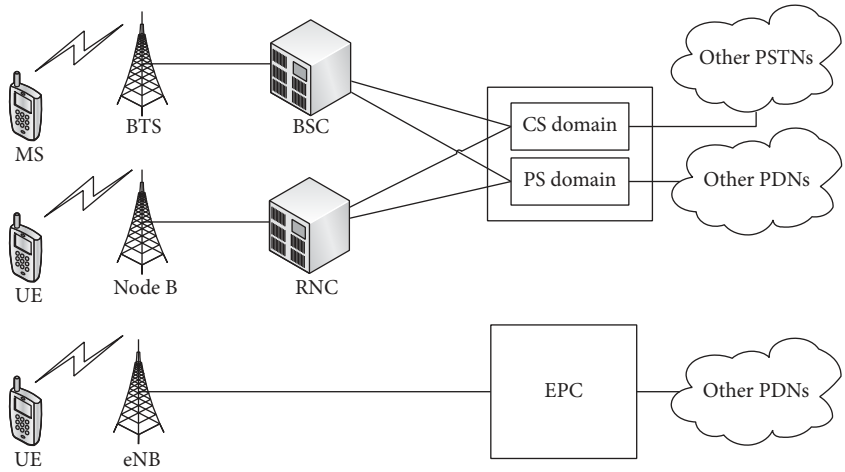

Figure 2: Schematic representation of the GSM/GPRS/EDGE, UMTS, and LTE networks. The figure shows that GSM and UMTS share the same core network. In GSM network, the BTS is connected to the core network through the Base Station Controller (BSC). In the UMTS network, Node B is connected to the core network through the Radio Network Controller (RNC). The evolved Node B (eNB) in the LTE network has both Node B and RNC functions and is directly connected to the EPC. GSM and UMTS core network CS domain connects to other Public Switched Telephone Networks (PSTNs), while the PS domain connects to other Packet Data Networks (PDNs). The EPC in LTE has only the PS domain. In both UMTS and LTE, the MS is referred to as User Equipment (UE).

On the GSM family, High-Speed Downlink Packet Access (HSDPA) significantly improved UMTS downlink data rates, using fast physical layer retransmission and other techniques similar to those already adopted in 1xEVDO, such as AMC and improved scheduling algorithms to increase cell throughput [10]. However, as HSDPA runs on UMTS systems with 5 MHz carriers, the maximum achievable rate is much higher than that in the 1.23 MHz 1xEVDO carrier: up to 14 Mbps (note that even though the HSDPA downlink rate is 6 times the 1xEVDO downlink rate, the HSDPA spectral efficiency (2.88 bits/Hz) is only 48% higher than 1xEVDO's (1.95 bits/Hz); however, this comparison is not taking into account the fact that HSDPA runs on a UMTS carrier shared by PS data and CS voice, while the 1xEVDO carrier is reserved for PS data). High-Speed Uplink Packet Access (HSUPA), using similar techniques [11], does the same thing to the UMTS uplink, reaching data rates of up to 5 Mbps in microcells [10].

1.1.5. 4G: LTE and LTE-Advanced. Originally, the 3GPP 4G system was referred to as System Architecture Evolution (SAE), with a core network known as Evolved Packet Core (EPC) and RAN called Long-Term Evolution (LTE). However, the LTE acronym ended up being used to designate the whole system. LTE has RAN and a core network that are completely different from previous UMTS systems. LTE core network—the EPC—has only the PS domain, so CS voice service is not supported, as shown in Figure 2. Instead, voice is carried as data using Voice-Over-IP (VoIP). LTE RAN uses Orthogonal Frequency Division Multiple Access (OFDMA) and carriers with up to 20 MHz of bandwidth on the downlink, achieving peak data rates of up to 300 Mbps. With a 20 MHz bandwidth, LTE spectral efficiency is 15 bits/Hz, which is approximately 5 times the WCDMA HSDPA Release 5 spectral efficiency. LTE-Advanced pushes the data rates even higher. It achieves up to 3000 Mbps in the downlink by combining five 20 MHz carriers, using a total bandwidth of 100 MHz [12].

1.2. 3GPP Technical Specifications Organization. The 3GPP is an ensemble of six standardization groups: ARIB (Association of Radio Industries and Businesses), ATIS (Alliance for Telecommunications Industry Solutions), CCSA (China Communications Standards Association), ETSI (European Telecommunications Standard Institute), TTA (Telecommunications Technology Association), and TTC (Telecommunication Technology Committee). Those groups are referred to as 3GPP Organizational Partners, and they work together to issue technical specifications (TSs) and technical reports (TRs) regarding the radio access network, the core network, and services of GSM/GPRS/EDGE, UMTS, and LTE mobile telephony cellular systems.

The 3GPP specifications are grouped into releases, series, and stages, as follows:

(i) *Releases.* Each new release marks the introduction of new technologies—like UMTS in Release 99 or LTE in Release 8—or important enhancements—such as LTE-Advanced in Release 10. Table 1 lists 3GPP releases from 1995 to 2013. Several versions of the same TS might be issued within the same release to implement new features (a list of features per release, from Release 1999 to Release 13, is available in [13]), until the release is frozen. There is a parallelism between adjacent releases development (until the previous release is frozen), which provides time for the vendors and operators to adapt to the new release.

(ii) *Series.* Each series refers to a particular subject and might span one or more releases. For example, the

Table 1: Frozen 3GPP releases from 1997 to 2013.

Release	Spec. version number	Freeze date
Rel-11	11.w.u	June 2013
Rel-10 (LTE-Advanced)	10.w.u	June 2011
Rel-9	9.w.u	December 2009
Rel-8 (LTE)	8.w.u	December 2008
Rel-7	7.w.u	December 2007
Rel-6 (HSUPA)	6.w.w	March 2005
Rel-5 (HSDPA)	5.w.u	June 2002
Rel-4	4.w.u	March 2001
R99 (UMTS/EDGE)	8.w.u (GERAN) 3.w.u (UTRAN)	March 2000
R98	7.w.u	Early 1999
R97 (GPRS)	6.w.u	Early 1998
R96	5.w.u	Early 1997

GSM RAN features before Release 4 are defined in the 05 series. From Release 4 onwards they are defined in the 45 series. In the case of 3G (and beyond) network, the RAN characteristics are defined in the 25 series. A table showing all 3GPP specification series is available in [14] (this table is too large and therefore is not reproduced here due to lack of space.)

(iii) *Stages.* Stage 1 specifications define services under a user point of view; general requirements are defined, without providing details about the implementation. Stage 2 specifications provide overall information about technical implementation of the services/features defined in Stage 1. Stage 3 specifications bring highly detailed technical information that is used by network operators and hardware manufacturers/vendors. Stages 1 and 2 specifications are grouped into series $X2$ and $X3$, respectively, where $X = 0$ (GSM before Release 4), 4 (GSM from Release 4 onwards), and 2 (3G and 4G networks).

The title of each TS shows the series, release, and version. The general format of a 3GPP specification title is TS xx.yyy Vzz.w.u, for series 21 to 55, or TS xx.yy Vzz.w.u, for series 01 to 13. The "TS" shows that it is a technical specification. The two-digit number "xx" shows the series that this specification belongs to. The following three-digit number "yyy"—or two-digit number, for series 01 to 13—identifies the TS within that series. The letter "V" stands for "version." The two-digit number "zz" shows the release the TS applies to. The one-digit numbers "w" and "u" identify the TS version within release "zz." A full list of 3GPP specifications grouped by release is available in [15].

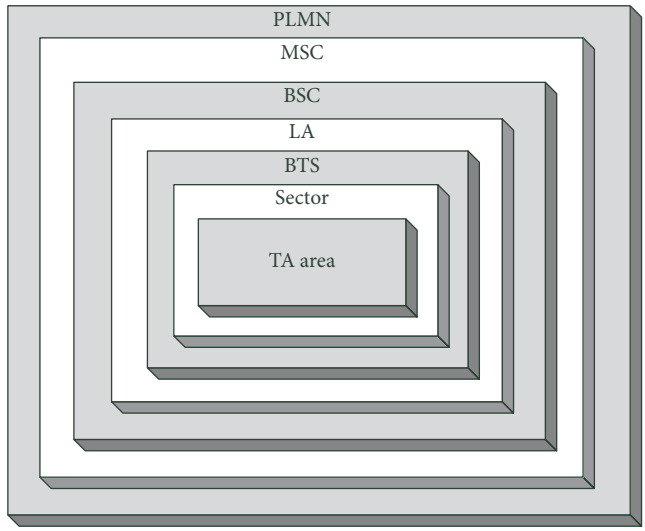

Figure 3: Location resolution hierarchy within a GSM cellular network.

2. Cellular Networks Intrinsic Positioning Capabilities

Different levels of location awareness are inherent to any metropolitan area network (MAN) with wireless radio access, to allow call forwarding and packet routing to any MS and call and session continuity when the MS moves from one base station transceiver (BTS) coverage area to another [16]. These built-in location capabilities can be extended to support added value LCS applications [17].

Figure 3 depicts the location resolution hierarchy within a GSM cellular network. At the highest level, it is possible to have a very coarse MS location estimate as the geographic area covered by the Public Land Mobile Network (PLMN) is known. A PLMN comprises a set of mobile switching centers (MSCs). Each MSC provides service to part of the geographic area covered by the PLMN. Consequently, knowing the MSC to which the target MS is connected allows a less coarse position estimate. Within each MSC, one or more base station controllers (BSCs) manage groups of BTSs. So, the geographic area served by an MSC might be divided into smaller zones, each associated with a different BSC. Within each BSC, one or more location areas (LAs) can be defined [18]. When an MS must be paged, the paging message is sent to all BTSs within the LA where the MS is located. When the MS crosses LAs boundaries, it notifies the network, so that the BSC knows, at all times, within which LA the MS is located [19]. Within each LA there are groups of BTSs. A BTS has one or more sectors. A sector covers a restricted area whose size and format depend on some factors, such as the propagation environment, the transmitter output power, the type and height of the antennas, and the losses at the transmitter station. As GSM uses TDMA in the radio access network, some time alignment between different MSs transmissions within the same sector must be implemented. This is achieved using the Timing Advance (TA) parameter, which is proportional to the signal round-trip time (RTT) between the MS and the serving sector

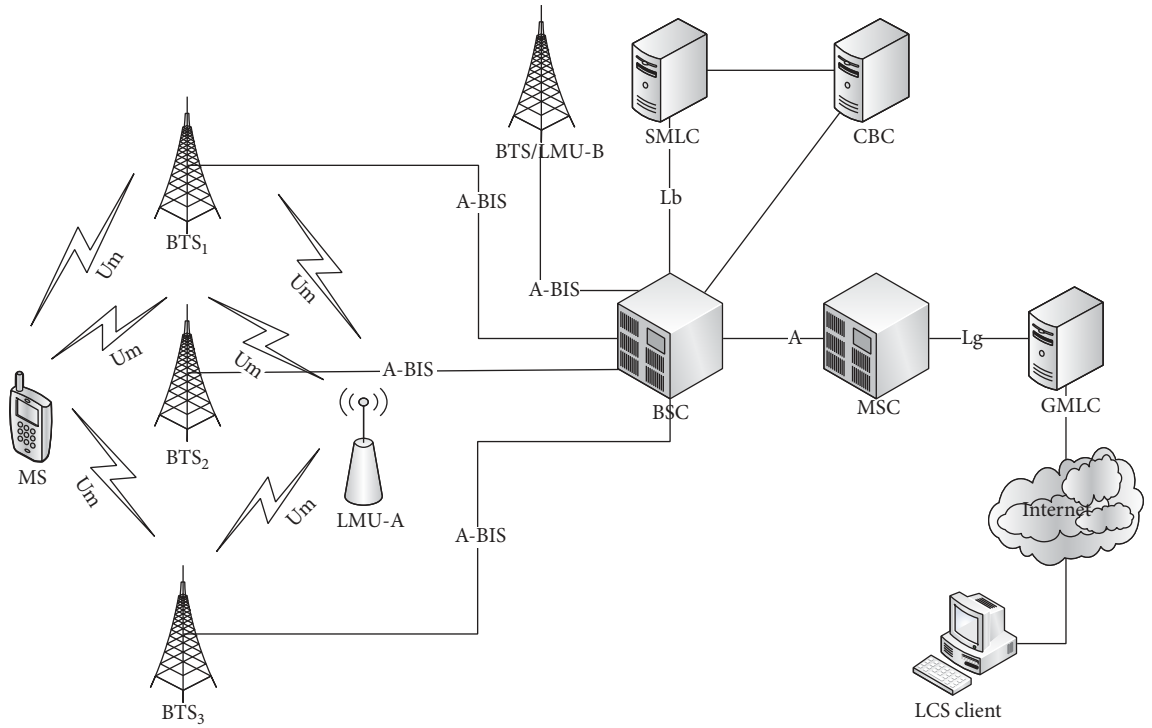

Figure 4: MS-assisted EOTD position fix: the SMLC uses RTD and OTD measurements sent by the LMU and the target MS, respectively. This scenario represents a mobile terminated location request (MT-LR) [22].

antenna. The TA parameter subdivides the serving area of each sector into smaller areas (TA areas). A TA area provides the highest achievable resolution for an MS position estimate in active mode within a GSM network, using only the parameters ordinarily applied to mobility management [20]. For an MS in idle mode, the highest achievable accuracy would be the geographic zone covered by the current LA.

The cellular networks intrinsic positioning capabilities can be enhanced with specific measurements and signals that are used as support data for the position calculation. The following sections show how it is achieved in 2G, 3G, and 4G cellular networks.

3. GSM/GPRS/EDGE LCS Architecture

3.1. Network Elements. In the GERAN LCS architecture two network elements have been added to provide specific support to LCS [21]: the Serving Mobile Location Center (SMLC) and the Location Management Unit (LMU). A third element, the Gateway Mobile Location Center (GMLC), has been added to the core network [22]. Figures 4 and 5 illustrate how those elements are interconnected in two different positioning scenarios.

3.1.1. SMLC. The SMLC is part of the GSM Base Station Subsystem (BSS) and can be either a standalone element or integrated into the BSC. The SMLC manages the position fix process. It receives and relays position location requests to (in the case of network initiated location requests) and from (in the case of MS initiated location requests) the MS. It also receives measurements made by the target MS and by LMUs, as well as Global Navigation Satellite Systems (GNSS) signals, which might assist the target MS positioning. The SMLC selects the localization technique to be used, based on the availability of LMUs and cells and on the specific positioning service requirements, like accuracy and position fix delay, as defined by the LCS client [23] (an LCS client is a logical functional entity (e.g., a software application) which queries the SMLC for one or more target MS locations; the LCS client might reside in a network element—e.g., the MS, the SMLC, or the GMLC—inside the PLMN or in an external entity; the GMLC is part of the GSM core network and establishes the communication between the SMLC and an LCS client located outside the PLMN). The SMLC also sends LCS assistance data to the Cell Broadcast Center (CBC), so that these data can be broadcasted to support MS-based localization methods [24].

3.1.2. LMUs. 3GPP technical specifications define two types of LMUs [21]: type A and type B. A type A LMU (LMU-A) is a standalone mobile unit equipped with a GNSS receiver that communicates directly with the BTSs through the Um interface (the air interface). A type B LMU (LMU-B) is integrated with the BTS and communicates directly with the BSC through the A-BIS interface. BTSs are not synchronized in the GERAN; therefore, the LMUs measure the real-time differences between their transmissions. These measurements are required in hyperbolic multilateration positioning (in multilateration positioning, the MS location is estimated using distance estimates from several fixed reference stations; those

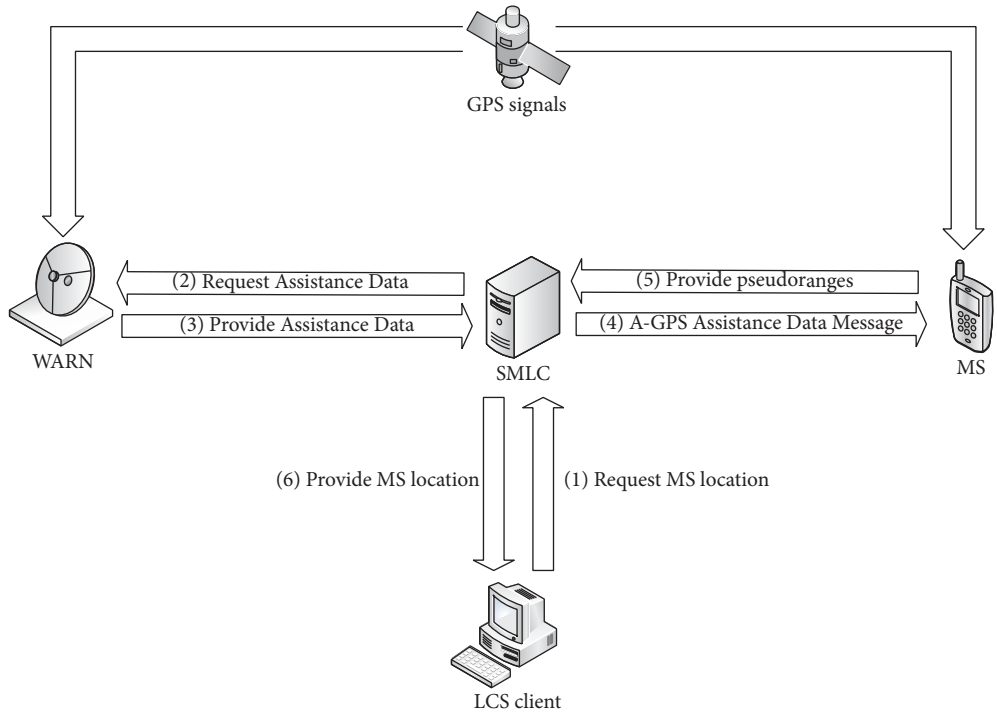

Figure 5: Simplified scenario of an MS-assisted A-GPS position fix. The message flow shown here is a higher layer abstraction. Some specific position related protocols and messages are described in Sections 3.3, 4.3, and 5.3.

distance estimates are derived from receiver signal strength or round-trip time measurements; multilateration can be circular or hyperbolic [25]). To ensure the highest possible localization accuracy, the LMU coordinates must be known at all times with high accuracy level. In the case of type A LMUs, this is provided by the built-in GNSS receivers.

LMUs time measurement accuracy for positioning methods supported in GSM networks, under different channel conditions, is specified in [26]. The measurement accuracy of the LMU is defined as the standard deviation of the 90% most accurate time measurements (this is also referred to as RMS_{90}). Measurements are performed at two carrier-to-noise (C/N) ratios (0 dB and 20 dB) for two different channel conditions (static and mobile with Rayleigh fading). The lowest RMS_{90} value—which is obtained for a static MS with $C/N = 20$ dB—is 0.1 μs.

3.1.3. GMLC. The GMLC allows communication of the SMLC with LCS clients external to the PLMN. The GMLC implements functions like charging and billing data for LCS, coordinate system transformation (between the coordinate system adopted at the SMLC and the one used by the external LCS client), and verification and authorization (i.e., it verifies if the LCS client is allowed to locate the client) [22].

3.2. Standard LCS Methods. GSM/GPRS/EDGE LCS architecture has four standard positioning methods [21]: TA (Timing Advance), EOTD (Enhanced Observed Time Difference) [27], UTDOA (Uplink Time Difference of Arrival), and GNSS based (autonomous and assisted modes) method.

3.2.1. TA. TA positioning is also called E-CID (Enhanced Cell Identity) [28]. It is classified as a centroid method called *centroid of the angular ring section*. Pure CID (Cell Identity) localization returns the coordinates of the serving sector as the target MS location estimate. The use of the TA parameter—which is proportional to RTT and originally applied to align the MS transmissions within a sector, avoiding overlapping of transmissions of MSs on adjacent slots at the reception—allows reducing the uncertainty area, therefore improving the positioning accuracy. The TA parameter can be used to restrict the uncertainty area of all the other supported localization methods [21].

3.2.2. EOTD. EOTD is a hyperbolic multilateration positioning method. Hyperbolic methods rely on time difference of arrival (TDOA) measurements to estimate the target MS position. There is a TDOA measurement for each pair of reference nodes, yielding a hyperbolic line-of-position (LOP) (a LOP is the loci of all points (coordinates) where the MS can be located; i.e., the LOP is the set of all candidate solutions for the MS positioning problem), with the two reference stations as focuses. As two hyperbolas might intercept at two points, at least three hyperbolic LOPs—and therefore four reference nodes—are required to yield an unambiguous position fix. If available, more than four reference nodes might be involved in an EOTD position fix, to improve accuracy. Two types of EOTD localization are supported in the GERAN [28]:

(i) MS-assisted type: the MS sends measurements to the SMLC, which then calculates the MS position.

(ii) MS-based type: the MS calculates its position using assistance data broadcasted by the network.

Unlike the cdmaOne RAN, whose BTSs transmissions are kept tightly synchronized using Global Positioning System (GPS) signals as a time reference, the GERAN is asynchronous. So, time corrections are required before using TDOA measurements. These time corrections are provided by the LMUs and are called Real-Time Differences (RTDs). Consider that bursts sent from BTS_1 and BTS_2 are received at a nearby LMU at instants t_1 and t_2, respectively. The BTSs and LMU coordinates must be known with high level of accuracy (type B LMUs are fixed, as they are integrated with BTSs, so their precise coordinates might be obtained directly from a map; type A LMUs are mobile, so the most accurate available positioning method—typically GPS—must be used to obtain their coordinates; inaccuracies in the coordinates of the reference nodes and LMUs, used in the position fix, might severely impair the position location accuracy [28]). The RTD between BTS_1 and BTS_2, as measured by the LMU, is given by $RTD_{12} = OTD_{12} - GTD_{12}$, where OTD_{12} is the Observed Time Difference (OTD) between the reception of bursts from BTS_1 and BTS_2; that is, $OTD_{12} = (t_1 - t_2)$, and GTD_{12} is the Geometric Time Difference (GTD) between the reception of bursts from BTS_1 and BTS_2. The GTD is calculated assuming line-of-sight (LOS) paths between the LMU and each BTS. It is given by $GTD_{12} = (d_{L1} - d_{L2})/c$, where c is the speed of light in free space and d_{L1} and d_{L2} are the LOS distances (i.e., the Euclidean distances) between the LMU and BTS_1 and BTS_2, respectively.

Let us consider an example of an MS-assisted EOTD position fix, as shown in Figure 4 [21]. An external LCS client sends a location request (LR) to the SMLC through the GMLC. The SMLC based on an initial coarse estimated position of the target MS—for instance, its current LA—selects which BTSs and LMUs will be used in the position fix. The SMLC then orders the selected BTSs to send bursts, which are received by the selected LMUs (in the example, for the sake of simplicity, just one LMU-A is used, but more LMUs might be involved in the position fix) and by the target MS. The LMUs measure the RTD between the BTS transmissions. The target MS measures the OTD between the BTS transmissions. The RTD and OTD values are sent back to the SMLC, which then uses theses values to calculate the target MS position. Each pair of reference BTSs yields a hyperbolic LOP [29]. At the SMLC, a system of at least three hyperbolic LOPs is obtained. Such a system does not have a closed form solution, due to non-line-of-sight (NLOS) propagation and system inaccuracies [30]. Approximation methods (e.g., Least Squares) might be used to calculate the target MS position, $(\widehat{x}, \widehat{y})$, which is then sent by the SMLC back to the external LCS client, through the GMLC. The LMUs do not need to measure and report RTD values to the SMLC at every position fix—the SMLC might use previously reported values. However, an RTD update rate must be defined, as RTDs between BTSs tend to vary along time, due to the time drift between the clocks of asynchronous BTSs [24].

To support MS-based EOTD position fixes, the SMLC broadcasts through the CBC assistance data to allow the MS to calculate its position. Some of the contents of the broadcast EOTD assistance message include neighbor cells RTD values; RTD drift factor values; and serving cell and neighbor cells geographic coordinates [24].

3.2.3. UTDOA. Like EOTD, UTDOA is also a hyperbolic multilateration positioning technique [31, 32]. However, unlike EOTD—which requires software updates at the MS, so that it can measure and report OTD values—UTDOA does not require any modification at the MSs [22]. Accordingly, at least theoretically, it is capable of locating any MS within the network. The ability to locate any terminal, regardless of any built-in hardware features or software updates, is particularly important in scenarios like emergency call localization [33]. Nevertheless, UTDOA requires the deployment of more LMUs (to improve positioning accuracy in EOTD, more geographically dispersed BTSs are required; in the case of UTDOA, more geographically dispersed LMUs are necessary for that same purpose), a common clock reference for the LMUs (which means that all of them need a GPS receiver), and generates extra signaling load in the network, due to the exchange of coordination messages between the serving BTSs and the LMUs [28].

In UTDOA, LMUs measure the time of arrival (TOA) of bursts ordinarily generated by the MS while in dedicated mode (circular multilateration [29, 34] is not viable in this scenario, as the instant when the MS transmitted its burst cannot be known; there is no synchronization between LMUs and MSs) [35]. As the LMUs share the same clock reference, it is possible to calculate the TDOA between pairs of LMUs, each one yielding a hyperbolic LOP whose focuses are located at the LMUs coordinates (which are known). With at least three TDOA measurements—and therefore four LMUs—it is possible to obtain an unambiguous position estimate [36].

3.2.4. GNSS Based Positioning. The most widespread GNSS currently in use is GPS. The GPS system comprises three segments [37]:

(i) The space segment, composed of a constellation of up to 32 medium-altitude Earth orbit (MEO) satellites (MEO satellites have circular orbits with an altitude ranging between 5000 and 20000 km [38]).

(ii) The control segment, comprising all the nine ground stations involved in the system monitoring.

(iii) The user segment, composed of all military and civilian GPS receivers.

The satellites are equipped with highly precise atomic clocks and transmit at two carrier frequencies, $L1$ and $L2$, at 1575.42 MHz and 1227.6 MHz, respectively. Those carriers are modulated by long pseudonoise (PN) code sequences and a navigation message. Each satellite transmits this long PN code sequence with a different offset to allow satellite identification at the GPS receiver. The navigation message contains data about the satellite orbit and a series of parameters, such as ionospheric delay [39] and clock synchronization correction factors, which are used by the GPS receiver in the position calculation. GPS localization is a three-dimensional (3D)

circular multilateration technique where the GPS receiver must have a clear view to at least four GPS satellites to be able to yield an unambiguous position fix (in fact, four GPS satellites do not give a unique position fix for three space dimensions plus time, since four second-order equations with four unknowns can have two solutions; however, one of the solutions can be discarded by dead reckoning, and an unambiguous position estimate over the Earth surface is obtained). The number and geometric disposition of the visible satellites affect the positioning accuracy.

GPS enabled MSs might operate in autonomous or assisted mode [40]. In autonomous mode, the MS calculates its position using the GPS signals, without any interaction with the PLMN. In assisted mode, also referred to as Assisted GPS (A-GPS), the MS receives assistance data from the PLMN and calculates its position (MS-based) or sends measurements back to the SMLC (MS-assisted). The assistance data might enable the use of combined signals from other GNSS constellations as well, such as GLONASS (Global Navigation Satellite System) and Galileo [21].

In autonomous mode, the MS is equipped with a fully functional GPS receiver and is capable of calculating its position without any communication with the cellular network. However, this mode has some disadvantages. Without assistance data from the PLMN, the MS has to scan the entire code phase (from 0 to 1023 chips, which is the PN code length) and frequency (from −4 kHz to +4 kHz around the carrier frequencies, to account for the Doppler shift) spaces to identify which satellites are visible at its current location. This increases the time-to-first-fix (TTFF) in conventional GPS receivers, as well as the handset power consumption, reducing the MS battery lifetime.

In assisted mode, or A-GPS positioning, the MS receives assistance data from the cellular network. The GPS Assistance Data Message includes the list of satellites that are visible at the target MS current location; the network is capable of starting with a coarse estimate of the MS location, as explained in Section 2, as well as Doppler shift corrections for each satellite. With that information, the MS can greatly reduce the code phase and frequency search window, reducing the TTFF to only a few seconds [22]. This also increases MS battery lifetime. The assistance data also helps the MS demodulating satellites signals that would be unusable in autonomous mode, increasing LCS availability—even, in some cases, to indoor environments. The GPS Assistance Data Message also includes Differential GPS (DGPS) corrections. DGPS data must be transmitted frequently to the MS (approximately every 30 seconds). The full contents of the GPS Assistance Data Message are listed in [24].

The operation of A-GPS requires the establishment of a GPS reference network, also known as a wide-area reference network (WARN)—whose receivers are placed at fixed known locations and with clear view of the sky, so that they can operate continuously [22]. Each fixed GPS receiver uses the satellites signals to estimate its position and compare this estimate with its ground-truth position, which has been previously surveyed to a high degree of accuracy. This comparison yields differential correction factors that are provided to the SMLC when requested. DGPS improves the positioning accuracy to under 5 meters. The WARN also provides information such as which satellites are visible over a given area at a given time, Doppler shifts, and ionospheric delays.

Figure 5 shows a simplified diagram of the information flow between the LCS client, the SMLC, the WARN, and the target MS during an MS-assisted A-GPS position fix. Initially, the SMLC receives a location request originated from an LCS client, via the GMLC (which is not shown in the diagram). The SMLC then requests and receives DGPS corrections and assistance data (e.g., list of visible satellites, Doppler shift corrections, and code phase search window) [22] from the WARN. The SMLC broadcasts the assistance data in the A-GPS Assistance Data Message, through the CBC (which is also not shown in the diagram). The target MS uses this information to calculate the pseudoranges to the visible satellites. The pseudoranges are sent to SMLC, where the MS position is calculated using the DGPS corrections previously provided by the WARN. Then, the estimated MS coordinates are sent back to the LCS client. The information flow between the LCS client, the SMLC, the WARN, and the target MS during an MS-based A-GPS position fix could also be depicted by Figure 5, with a minor correction: in step (5), instead of sending back satellite pseudoranges, the target MS calculates its own position and reports it back to the SMLC.

3.3. Radio Resource LCS Protocol (RRLP). RRLP is the specific LCS protocol in GSM/GPRS/EDGE networks. RRLP is part of Layer 3 of the GSM protocol stack and allows the exchange of LCS related messages between two entities: the SMLC and the MS. RRLP supports three procedures (Position Measurement Procedure, Assistance Data Delivery Procedure, and Error Handling Procedure), implemented with five message (or component) types [41]:

(i) Measure Position Request: used by the SMLC to request location measurements (in MS-assisted positioning) or location estimates (in MS-based positioning) from the MS.

(ii) Measure Position Response: used by the MS in response to a Measure Position Request; it contains location measurements, location estimates, or an error indicator.

(iii) Assistance Data: used by the SMLC to send EOTD or A-GPS assistance data to the MS.

(iv) Assistance Data Acknowledgment: used by the MS to acknowledge the correct reception of a complete Assistance Data component.

(v) Protocol Error: used by the receiving entity to notify the sender entity that there is a problem that prevents the completion of a requested procedure.

The Assistance Data Delivery Procedure allows the SMLC to send assistance data to the MS for location measurements (in MS-assisted mode) or location calculation (in MS-based mode). The message flow between the two entities (SMLC and MS) in this procedure is shown in Figure 6. First, the SMLC sends one or more Assistance Data Messages to

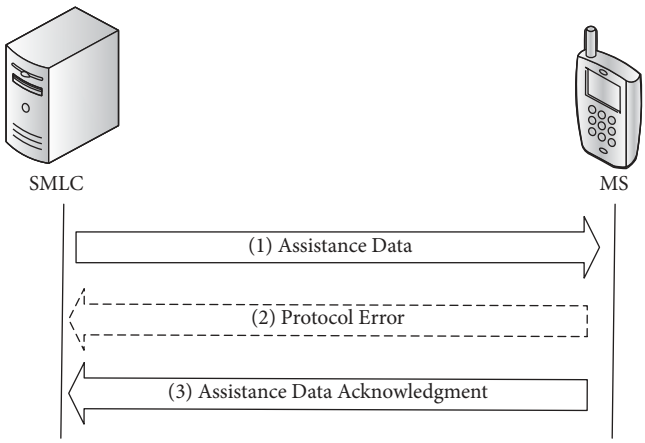

Figure 6: RRLP Assistance Data Delivery Procedure.

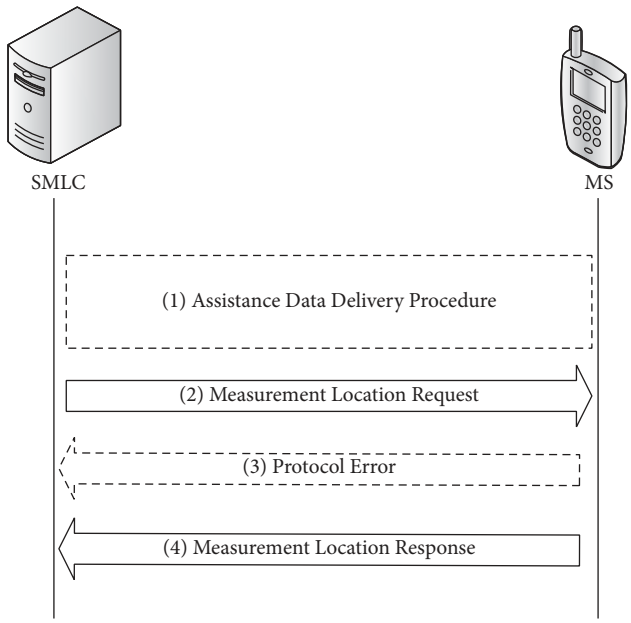

Figure 7: RRLP Position Measurement Procedure.

the MS. If there is any error in the received messages, or any condition that prevents the MS from sending back the requested information, a Protocol Error message is sent to the SMLC. Otherwise, the MS sends an Assistance Data Acknowledgment message, to confirm correct reception of the Assistance Data Message.

The Position Measurement Procedure allows the SMLC to request and receive location measurements and location estimates from the MS (according to the 3GPP definition of this procedure [41], only mobile terminated location requests (MT-LRs) are supported by RRLP [22]). The message flow between the two entities (SMLC and MS) in this procedure is shown in Figure 7. First, the SMLC sends a Measurement Position Request, which might be preceded by an Assistance Data Delivery Procedure. The MS receives the request and tries to provide the required information. If any problem occurs, a Protocol Error message is generated. If not, the MS sends a Measurement Location Response, containing the requested data.

When a receiving entity—either the SMLC or the MS—detects that some data is missing or receives erroneous data, a Protocol Error message is sent with an error code indicating the error type, as listed in Table 2.

Table 2: RRLP error codes.

Error code	Description
0	Undefined
1	Not enough BTSs
2	Not enough satellites
3	EOTD Location Assistance Data missing
4	EOTD Assistance Data missing
5	A-GPS Location Assistance Data missing
6	A-GPS Assistance Data missing
7	Method not supported
8	Not processed
9	Ref. BTS for GPS not serving BTS
10	Ref. BTS for EOTD not serving BTS

3.3.1. RRLP Privacy Issues. In MS-based positioning, upon reception of a Measure Position Request, the MS replies with a Measure Position Response message containing its location. However, no authentication is used. As a result, a third party might act as the SMLC, send a Measure Position Request message, and obtain the target MS coordinates. It is not an identity privacy violation in itself, because, to send the RRLP messages to the MS, the eavesdropper already has the target MS unique identifier (the IMSI—International Mobile Subscriber Identity). However, this is a violation of location privacy. It is even more serious as the subscribers may not even be aware that an RRLP session is taking place. The RRLP location privacy weaknesses were exposed during a large GSM field test carried at the 2009 HAR (Hacking at Random) conference [42]. The GSM test network comprised two microcells connected through an E1 trunk to a server running the OpenBSC software (OpenBSC is an open source software implementation of the GSM network side protocol stack [43]).

4. UMTS LCS Architecture

4.1. Network Elements. GSM/GPRS/EDGE and UMTS networks have completely different RANs but share most core network elements. As a result, the same elements defined for 2G networks remain in the 3G LCS implementation: the LMUs, the GMLC, and the SMLC—which in 3G networks is incorporated into the RNC [44]. Only one new network element was added, the Positioning Element (PE), to improve the accuracy and availability of hyperbolic multilateration in WCDMA networks. PEs are used in the OTDOA-PE method, which is described in the following section.

4.2. Standard LCS Methods. UMTS LCS architecture has four standard positioning methods [45]: Cell ID based, Observed Time Difference of Arrival with Idle Period in

the Downlink (OTDOA-IPDL), and UTDOA and GNSS based (autonomous and assisted modes) methods. Some other methods were indicated for further development in Release 4 [46], such as angle of arrival (AoA), Observed Time Difference of Arrival with Positioning Elements (OTDOA-PEs) and almanac-based DGPS method (DGPS-A), which is an improvement to previous A-GPS positioning.

4.2.1. Cell ID Based Positioning. Cell ID (CID) positioning, also known as cell of origin (COO), is a proximity-based method, as it returns as the MS location estimates the geographic coordinates associated with the serving cell (which is assumed to be the closest to the target MS) [47]. These coordinates might be the location of the antennas—and not that of Node B equipment—or the centroid of the cell coverage area. Additional parameters, such as RTT or RSS, can be used to enhance the positioning accuracy of CID.

One of the E-CID alternatives, CID + RTT, achieves a much higher precision in UMTS than in GSM networks, due to the much higher bandwidth in WCDMA. This improves the spatial resolution of RTT values: from 554 meters in GSM to 78 meters in WCDMA. This better spatial resolution helps reducing the confidence region, which results in higher positioning accuracy. RTT spatial resolution in UMTS can be further improved with oversampling. Oversampling factors down to 1/16 of the chip period are supported [48].

4.2.2. OTDOA-IPDL. CDMA and WCDMA might suffer from a condition referred to as the "near-far" problem: the reception at the User Equipment (UE) of strong signals from a nearby BTS might make it impossible to detect and demodulate the signals from more distant BTS. This happens because, as all cells share the same downlink frequency, in the reception of the signals of a given cell the energy sum of signals from all other cells acts as noise. If one cell—the near one—is received with a very high energy, the SNR of a distant cell—the far one—will be very low.

In downlink hyperbolic multilateration methods, such as EOTD, the UE must detect the TOA of signals from at least four geographically dispersed cells. The near-far problem might prevent the UE from achieving this minimum number of measurements required to obtain an unambiguous position fix. In fact, EOTD would be usable only at the border of each cell coverage area [46].

To prevent this problem in UMTS, 3GPP has proposed OTDOA-IPDL, which is an adaptation of EOTD positioning to WCDMA networks [49, 50]. OTDOA-IPDL uses idle periods in the downlink. The idle periods of different cells might be time aligned or randomly distributed. During an idle period, a cell will transmit only the synchronization channel or nothing at all, depending on the idle period configuration—continuous mode or burst mode. A UE will use the idle periods of its serving cell to obtain TOA measurements from other cells. OTDOA-IPDL improves the hearability of OTDOA, minimizing the near-far problem. OTDOA-IPDL with time aligned idle periods has another advantage: as the UE is making TOA measurements during periods where all neighbor cells are transmitting only the Common Pilot Channel (CPICH), the method's availability is not affected by the RAN traffic (the energy sum of signals from cells with heavy downlink traffic would overcome the weaker signals of cells with low traffic) [46].

Even though OTDOA-IPDL improves OTDOA availability, it is still hard to obtain measurements from at least four cells in a UMTS network. In fact, this is caused by one of the most fundamental aspects of WCDMA networks planning—that each cell must have a dominant area, where its signal overcomes the signals from neighbor cells. Simulations indicate that OTDOA-IPDL improves OTDOA availability from 31% (when no idle periods are used) to 74%, which is a significant improvement but whose final result is still insufficient. To improve accuracy, OTDOA positioning must be used in conjunction with other methods, such as E-CID [7].

4.2.3. UTDOA. UTDOA positioning in 3G networks is done the same way as in 2G networks. Please refer to Section 3.2.

4.2.4. GNSS Based Positioning. GNSS based positioning in 3G networks is done the same way as in 2G networks. Please refer to Section 3.2.

4.2.5. AoA. AoA positioning is also known as multiangulation. Its deployment in cellular networks requires the installation of antenna arrays at Nodes B [51–54], which might be quite expensive and time-consuming. As previously mentioned, this positioning method suffers heavily from NLOS propagation [55], being of little use in dense urban environments. However, to improve positioning accuracy, some hybrid techniques have been proposed, combining AoA with other methods, such as UTDOA [56] or TOA [57].

4.2.6. OTDOA-PE. A further improvement to OTDOA was proposed by 3GPP, which is the introduction of positioning elements (PEs) that transmit short three-symbol identifier codes during Node B idle periods. OTDOA-PE is therefore OTDOA-IPDL with the use of PEs. PEs are handheld-sized elements accessible only through the air interface. They are registered in the network just like other UE and some operators reserve IMSI ranges to be assigned to them. PEs coordinates must be accurately known. They must be placed at reference points other than Nodes B locations. Each PE is attached to a Node B—from now on referred to as its serving Node B—and is synchronized with it. PEs transmit in the downlink channel and their signals, upon reception at the UE, provide TOA measurements to be used in the hyperbolic multilateration [46].

The greater advantage of OTDOA-PE upon EOTD is that as the PEs are synchronized with the serving Node B, there is no need to measure RTD values with LMUs. As previously mentioned in Section 3.3, RTD values are broadcasted by the SMLC through the CBC as positioning assistance data. However, RTD values between pair of BTSs must be periodically updated, due to the clock drift between different BTSs. This LMU and RTD complication is eliminated with OTDOA-PE. For a better understanding and comparison of EOTD and OTDOA-PE, consider Figures 8 and 9.

Figure 8(a) shows the geometry of an EOTD positioning, with four BTSs (for the sake of simplicity, let us assume that

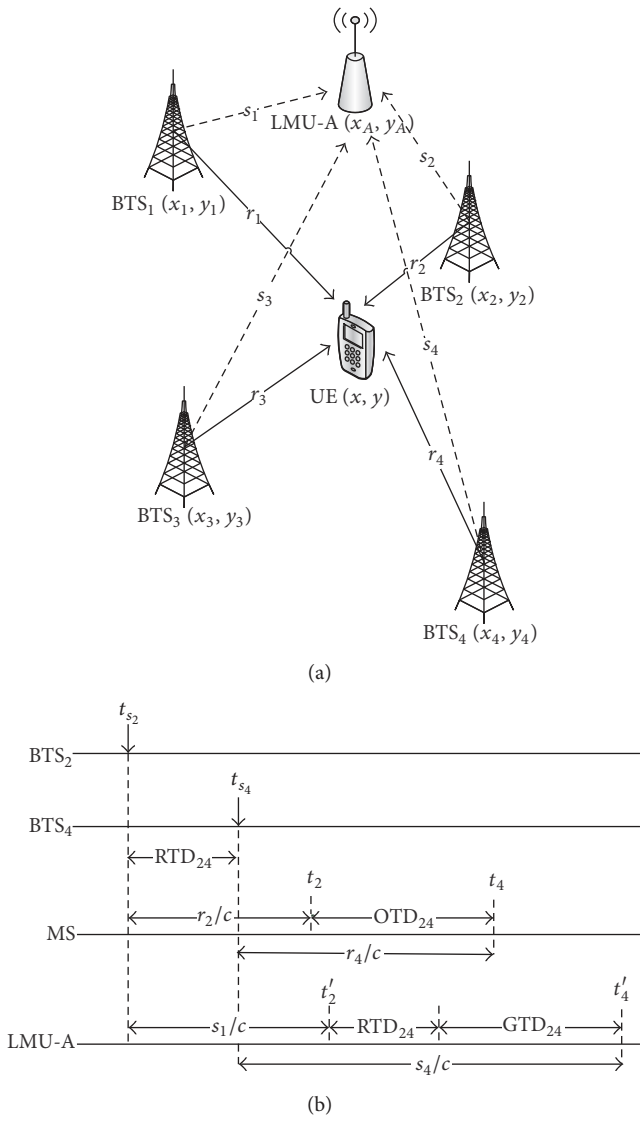

Figure 8: (a) EOTD positioning scenario, with four single-cell geographically dispersed BTSs and LMU, all placed at known coordinates. Note that r_i, i = 1, 2, 3, and 4, indicate the distance between BTS_i and the MS and that s_i, i = 1, 2, 3, and 4, indicate the distance between BTS_i and the LMU. (b) Timeline of the EOTD positioning scenario, assuming LOS between all elements.

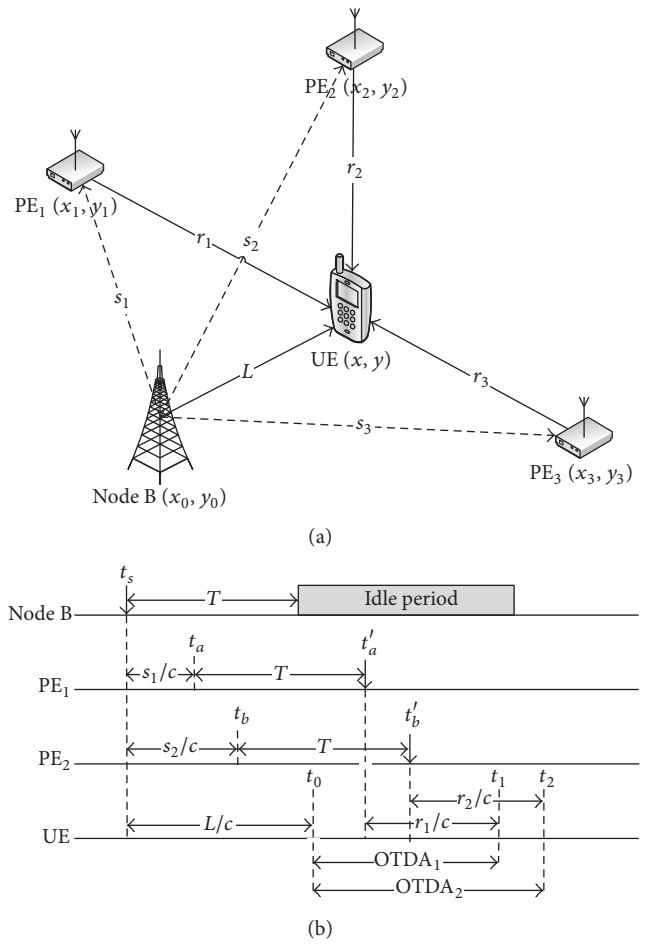

Figure 9: (a) OTDOA-PE positioning scenario, with one single-cell Node B and three geographically dispersed PEs, all placed at known coordinates. Note that r_i, i = 1, 2, 3, and 4, indicate the distance between PE_i and the UE and that s_i, i = 1, 2, 3, and 4, indicate the distance between PE_i and Node B; L is the distance between Node B and the UE. (b) Timeline of the OTDOA-PE positioning scenario, assuming LOS between all elements.

they all have just one sector, so each BTS corresponds to a cell) and LMU, all placed at known coordinates. To obtain an unambiguous position estimate, the TDOA between at least three pairs of cells must be calculated (and therefore a minimum of four geographically dispersed cells is needed). Figure 8(b) shows this calculation along a timeline for BTS_2 and BTS_4. Their transmissions are not synchronous, so the control channel frames transmission at BTS_2 and BTS_4 start at instants t_{s_2} and t_{s_4}, respectively. The RTD between BTS_2 and BTS_4 is $RTD_{24} = (t_{s_4} - t_{s_2})$. The signal from BTS_2 takes r_2/c seconds to reach the MS, where r_2 is the distance between the MS and BTS_2 and c is the speed of light in free space. It is detected at the MS at instant t_2. The signal from BTS_4 takes r_4/c seconds to reach the MS, being received at instant $t_4 = (r_4/c + RTD_{24})$. The MS then obtains the OTD between the reception of the signals from BTS_2 and BTS_4, $OTD_{24} = (t_4 - t_2)$. At the LMU, signals from BTS_2 and BTS_4 are detected at instants $t'_2 = s_2/c$ and $t'_4 = (s_4/c + RTD_{24})$. So, the LMU obtains $RTD_{24} = (t'_4 - t'_2) - GTD_{24}$, where $GTD_{24} = (s_4 - s_1)/c$. Distances s_4 and s_1 are known, as the coordinates of both BTSs and the LMU are known. OTD_{24}, measured by the MS, and RTD_{24}, measured by the LMU, are then reported back to the SMLC.

Figure 9(a) shows the geometry of an OTDOA-PE positioning, with one single-cell Node B and three PEs (as a minimum of four reference points is needed to provide three hyperbolic LOPs), all placed at known coordinates. The TDOA measurements are made between the serving Node B and each PE. Figure 9(b) shows this calculation along a timeline for Node B, PE_1 and PE_2. The control channel frame transmission at Node B starts at instant t_s and is received at

PE_1 and PE_2 at instants t_a and t_b, respectively, where $t_a = s_1/c$ and $t_b = s_2/c$. Then, T seconds after detecting Node B start-of-frame (SOF), each PE starts the transmission of its identifier code, at instants t'_a and t'_b. Node B signal is detected at the UE at instant t_0 and the codes of the PEs are received at the UE at instants t_1 and t_2, where $t_0 = L/c$, $t_1 = (s_1/c + T + r_1/c)$, and $t_2 = (s_2/c + T + r_2/c)$. The UE then obtains $OTDOA_1 = (t_1 - t_0)$ and $OTDOA_2 = (t_2 - t_0)$. As the PEs are synchronized with the serving Node B, it is not necessary to calculate RTD values, so LMUs are not needed. Note that the PEs transmissions are carried out during the serving Node B idle period.

4.2.7. DGPS-A. As already mentioned in Sections 3.2 and 3.3, A-GPS assistance data on 2G systems already included DGPS corrections. Those are ephemeris-based DGPS (DGPS-E) corrections that are used to compensate for deviations in satellite orbits, clock drift, and atmospheric perturbations. 3GPP recommends the augmentation of these DGPS assistance data, providing to the UE also almanac-based DGPS (DGPS-A) corrections. The combination of DGPS-E and DGPS-A corrections results in a lower assistance data update rate [46], which results in less additional network load and longer UE battery lifespan.

4.3. Radio Resource Control (RRC) Protocol. RRC is a UMTS Layer 3 protocol that handles control plane signaling between the UE and the UTRAN (Universal Terrestrial Radio Access Network, i.e., the UMTS RAN). RRC supports the exchange of position related messages, such as assistance data and position measurements, of EOTD and A-GPS methods. However, RRC is not a protocol designed solely for positioning. It includes many other functions, such as outer loop power control and paging notification. As it is not a positioning specific protocol, we are not going to get into details of RRC here. For further information, please refer to [58].

5. LTE LCS Architecture

5.1. Network Elements. Support to LCS in LTE networks was introduced only from Release 9 [12]. Essentially, the same specific positioning related network elements introduced in 2G and 3G networks are also present in 4G networks. However, the SMLC in LTE is called Evolved SMLC (E-SMLC). It has the same basic functions of the 2G and 3G SMLC, but with support to enhanced positioning features, such as hybrid localization and geofencing [59].

5.2. Standard LCS Methods. The standard LCS methods in LTE are E-CID, Assisted GNSS (A-GNSS), OTDOA (also referred to in LTE as downlink positioning), and UTDOA (also referred to in LTE as uplink positioning). LTE also supports A-GNSS + OTDOA hybrid positioning [60].

5.2.1. E-CID. As already stated in Sections 3.2 and 4.2, E-CID enhances CID accuracy by adding reference data to the position fix, such as RSS levels (RSS levels can also be used to provide distance estimations in circular multilateration positioning [61]) and RTT values. In LTE networks, E-CID might also use angle-of-arrival (AoA) information in the uplink. However, this requires the installation of antenna arrays in the eNBs. Besides that, AoA is too sensitive to multipath propagation, which is predominant in the heavily NLOS conditions in dense urban areas. E-CID might also work as a fallback method, when more precise positioning provided by other techniques, such as A-GNSS, is inaccessible, either due to UE limitations (no built-in GNSS receivers) or due to unavailability of GNSS signals (e.g., the target UE is indoors). The role of E-CID as a fallback positioning technique is particularly relevant for emergency call locating (it was considered so relevant in 4G that the LTE Positioning Protocol (LPP), unlike RRLP (in 2G networks) and RRC (in 3G networks), supports E-CID). A discussion on the FCC Enhanced 911 (E911) [1] emergency call locating regulations and possible related applications can be found in [62]. Some aspects of the E911 evolution to accommodate Voice-over-Internet Protocol (VoIP) emergency calls, which will certainly increase with the widespread deployment of 4G networks (no support to circuit-switched voice calls), are explored in [63].

5.2.2. A-GNSS. LTE A-GNSS effectively is not just A-GPS: it also supports the Russian GLONASS [64] and is designed to be forward-compatible with future constellations (e.g., Galileo, still not fully operational). The possibility of using signals from different constellations improves both positioning availability and precision. LTE supports two types of A-GNSS: UE-based type, where the UE receives assistance data from the network and calculates its location, and UE-assisted type, where the UE receives assistance data from the network, makes position related measurements (e.g., satellite pseudoranges), and reports those measurements back to the E-SMLC [60].

5.2.3. OTDOA with Position Reference Signals. LTE OTDOA uses position reference signals (PRS) transmitted on antenna port (an antenna port is a logical mapping of OFDMA channels, rather than a physical antenna) 6 [12]. Reference signals in LTE do not convey any higher layer information, existing only at the physical layer. The use of specific positioning-purpose signals in LTE OTDOA improves its availability and precision. To improve the hearability (i.e., the ability to detect weak signals from more distant cells, even in the presence of stronger signals from the serving and closer cells) of the positioning reference signals by the UE, orthogonal sequences are used to isolate PRS of neighbor cells in the code domain [65].

5.2.4. Hybrid A-GNSS + OTDOA. Hybrid positioning combines the TDOA measurements obtained from the LTE network with GNSS pseudorange measurements. Thereby, the hybrid method is expected to improve positioning availability and accuracy, particularly in environments where GNSS signal reception might be impaired, such as inside building or in urban "canyons" (i.e., streets in dense urban areas which are sided by skyscrapers) [66]. The techniques to combine those measurements are open to different implementation [40].

5.3. LTE Positioning Protocol (LPP). LPP is the positioning protocol in LTE networks. It is designed to be forward-compatible with future access networks to prevent piling

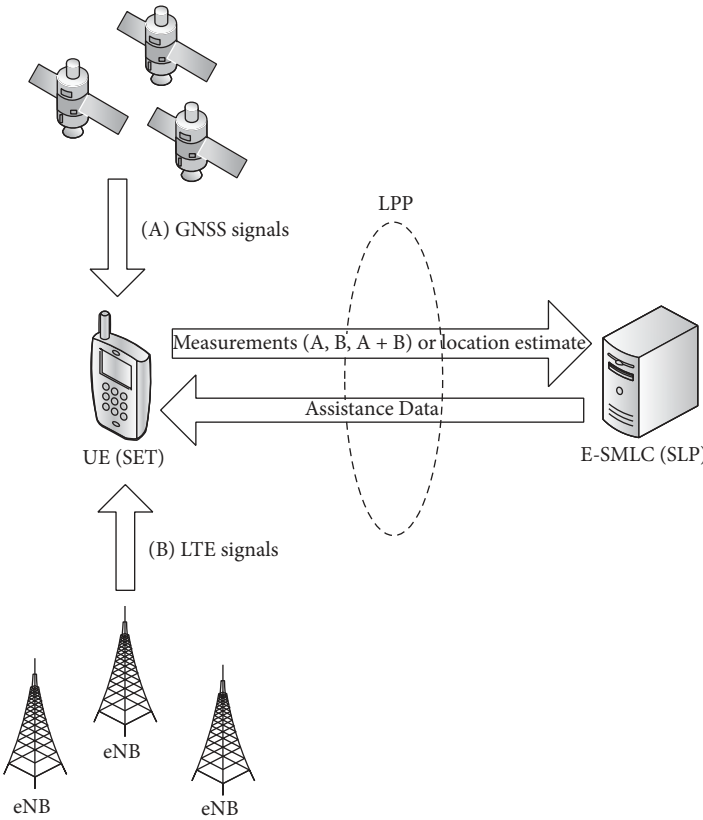

Figure 10: LPP conveying location related information between the UE and E-SMLC (or between the SET and the SLP, in user plane positioning). In the case of UE-based positioning, the UE sends its location estimate to the E-SMLC; in the case of UE-assisted positioning, the UE sends measurements (from GNSS constellations, from the LTE network, or form both, in the case of A-GNSS + OTDOA hybrid positioning).

up several positioning protocols through the generations to come. It supports E-CID, A-GNSS, and OTDOA, as well as hybrid localization to improve accuracy. And, unlike previous protocols, such as RRLP and RRC—which support only control plane positioning—LPP also can be used in user plane positioning [60, 64]. Control plane positioning uses dedicated control channels to convey location related information (assistance data and position estimates). It is considered more reliable and fast, so it is used in emergency call location [67]. Control plane positioning can be carried out without user intervention or even without user awareness (refer to Section 3.3, in the subsection about RRLP privacy issues). User plane positioning transfers location data into IP (Internet Protocol) datagrams using end-user applications. In LTE, user plane positioning is implemented by version 2.0 of the Secure User Plane Location (SUPL) protocol. SUPL 2.0, however, does not reinvent the wheel. It is built upon control plane protocols, such as LPP, RRC, and RRLP.

LPP is a point-to-point protocol between the UE and the E-SMLC. However, it has an extension, the LPP Annex (LPPa), which is specified only for control plane procedures between the evolved Node B (eNB) and the SMLC [68]. Referring to the OSI (Open Systems Interconnection) network model, LPP is an application layer protocol, while LPPa is a network layer protocol. LPPa has two modules: Location Information Transfer Procedures and Management Procedures (error handling). LPPa supports E-CID, OTDOA, and UTDOA [69]. Section 5.3.1 details LPPa a little further.

As shown in Figure 10, LPP conveys position related data between the UE and the E-SMLC in control plane positioning or between the SET (SUPL Enable Terminal) and the SLP (SUPL Location Platform) in user plane positioning. LPP uses six types of procedures or transactions, grouped into three groups [64]:

(i) Procedures related to capabilities exchange: Capabilities Transfer and Capabilities Indication Procedures.

(ii) Procedures related to assistance data exchange: Assistance Data Transfer and Assistance Data Delivery Procedures.

(iii) Procedures related to location information exchange: Location Information Transfer and Location Information Delivery Procedures.

LPP is also capable of detecting and reporting several specific error conditions, mostly in the positioning assistance data.

An example of a full LPP session is shown in Figure 11. It shows a control plane network initiated location request (NI-LR). The first procedure is the Capabilities Transfer, which

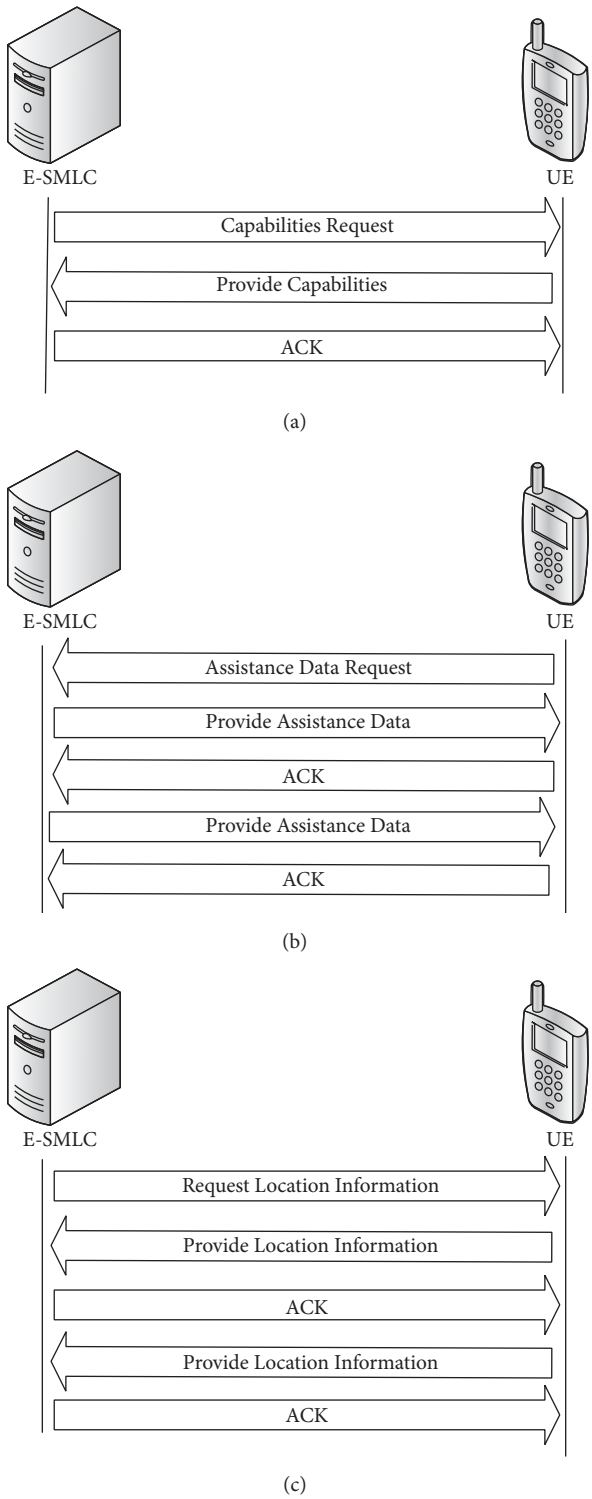

Figure 11: Example of a NI-LR LPP session: (a) Capabilities Transfer Procedure; (b) Assistance Data Transfer Procedure; and (c) Location Information Transfer Procedure.

starts with the server (in the case of NI-LR, the SMLC) sending a Request Capabilities Message, requesting the target UE to report the positioning methods it supports. The UE replies with a Provide Capabilities Message. The server then ends this transaction with an acknowledgment (ACK) message. Following that, the UE starts an Assistance Data Transfer Procedure, sending a Request Assistance Data Message. The server must then reply with one or more Provide Assistance Data Messages. After correctly receiving and decoding each Provide Assistance Data Message from the server, the UE replies with an ACK message. After sending all necessary assistance data to the UE, the E-SMLC commences a Location Information Transfer Procedure, sending a Request Location Information message. The UE then replies with one or more Provide Location Information Messages, containing its estimated coordinates (in the case of UE-based positioning) or position related measurements (in the case of UE-assisted positioning).

In the case of a UE initiated LR (the UE wants to locate itself), the UE starts the LPP session with a Capabilities Indication Procedure, sending a Provide Capabilities Message. Note that, unlike in the previous NI-LR example, the Provide Capabilities Message is sent autonomously by the target device and not as a response to a Request Capabilities Message sent by the E-SMLC. The same applies to the Location Information Delivery Procedure, when the UE sends unsolicited location information to the server. On the other hand, in the Assistance Data Delivery Procedure, the server sends unsolicited Provide Assistance Data to the UE.

5.3.1. LPPa. LPPa is an extension of LPP design to provide specific support to E-CID and OTDOA positioning in LTE networks. LPPa has the following functions:

(i) *E-CID Location Information Transfer.* It enables the exchange of location related information (information that will be used to improve CID positioning, e.g., RTT and RSS) between the eNB and the E-SMLC.

(ii) *OTDOA Information Transfer.* It enables the exchange of OTDOA assistance data (e.g., positioning reference signals code and frequency offsets and the list of neighbor eNBs whose positioning reference signals the target UE shall monitor) between the eNB and the E-SMLC.

(iii) *Reporting of General Error Situations.* It is reporting error situations for which no specific error message is defined.

Each of these functions comprises one or more elementary procedures, which in turn encompass a set of messages that define the information exchange. Table 3 maps the LPPa functions to its elementary procedures [69].

6. Summary

This review paper has presented the positioning capabilities in cellular networks, starting with the intrinsic localization support, inherent to any cellular system, and then passing through the specific features added by 3GPP—network elements (supported functions and interconnection with other elements of the architecture), supported positioning methods (position calculation details, related air interface

Table 3: LPPa functions and elementary procedures.

Function	Elementary procedure
E-CID Location Information Transfer	E-CID Measurement Initiation
	E-CID Measurement Failure Indication
	E-CID Measurement Report
	E-CID Measurement Termination
OTDOA Information Transfer	OTDOA Information Exchange
Report of General Error Situations	Error Indication

parameters, autonomous and assisted operation modes, and assistance data provided by the network), and protocols (functions, elementary procedures and more relevant message exchanges)—from the second until the fourth generation. It has also brought a section explaining the organization of 3GPP Technical Specifications and provided a quick review on the cellular networks evolution path.

Competing Interests

The author declares no competing interests.

References

[1] Federal Communications Commission, *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket no. 94-102, Federal Communications Commission, Washington, DC, USA, 1997.

[2] J. W. Reed, K. J. Krizman, B. D. Woerner, and T. S. Rappaport, "An overview of the challenges and progress in meeting the E-911 requirement for location service," *IEEE Communications Magazine*, vol. 36, no. 4, pp. 30–37, 1998.

[3] European Commission, "Commission recommendation 2003/558/EC," Official Journal of the European Union, 2003, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:189:0049:0051:EN:PDF.

[4] ETSI, "General Packet Radio Service, GPRS," May 2014, http://www.etsi.org/technologies-clusters/technologies/mobile/gprs.

[5] CDG, "cdmaOne," May 2014, http://www.cdg.org/technology/cdmaone.asp.

[6] ETSI, "EDGE," May 2014, http://www.etsi.org/technologies-clusters/technologies/mobile/edge.

[7] P. Muszynski and H. Holma, "Introduction to WCDMA," in *WCDMA for UMTS—Radio Access for Third Generation Mobile Communications*, H. Holma and A. Toskala, Eds., chapter 3, pp. 43–49, John Wiley & Sons, 3rd edition, 2004.

[8] CDG, "CDMA2000," May 2014, http://www.cdg.org/technology/cdma2000.asp.

[9] E. Simo, *EV-DO Rev-0 and Rev-A: The Physical Layer Explained*, BookSurge Publishing, 2007.

[10] A. Toskala, H. Holma, T. Kolding, P. Mogensen, K. Pedersen, and K. Ranta-Aho, "High-speed downlink packet access," in *WCDMA for UMTS—Radio Access for Third Generation Mobile Communications*, H. Holma and A. Toskala, Eds., chapter 11, pp. 307–344, John Wiley & Sons, 3rd edition, 2004.

[11] 3GPP, "FDD enhanced uplink; overall description; stage 2," 3rd Generation Partnership Project (3GPP) TS 25.309, 2006, http://www.3gpp.org/ftp/Specs/html-info/25309.htm.

[12] C. Cox, *An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications*, John Wiley & Sons, New York, NY, USA, 1st edition, 2012.

[13] 3GPP, "3GPP Features and Study Items," May 2014, http://www.3gpp.org/DynaReport/FeatureListFrameSet.htm.

[14] 3GPP, "Specification numbering," May 2014, http://www.3gpp.org/specifications/79-specification-numbering.

[15] 3GPP, "3GPP specification status report," May 2014, http://www.3gpp.org/DynaReport/status-report.htm.

[16] Y. Xiao, Y. Pan, and J. Li, "Design and analysis of location management for 3G cellular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 4, pp. 339–349, 2004.

[17] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," *IEEE Communications Magazine*, vol. 36, no. 4, pp. 46–59, 1998.

[18] K. Kyamakya and K. Jobmann, "Location management in cellular networks: classification of the most important paradigms, realistic simulation framework, and relative performance analysis," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 2, pp. 687–708, 2005.

[19] A. Roy, A. Misra, and S. K. Das, "Location update versus paging trade-off in cellular networks: an approach based on vector quantization," *IEEE Transactions on Mobile Computing*, vol. 6, no. 12, pp. 1426–1440, 2007.

[20] M. Pent, M. A. Spirito, and E. Turco, "Method for positioning GSM mobile stations using absolute time delay measurements," *Electronics Letters*, vol. 33, no. 24, pp. 2019–2020, 1997.

[21] 3GPP, "Functional stage 2 description of Location Services (LCS) in GERAN," 3rd Generation Partnership Project (3GPP) TS 43.059, 2008, http://www.3gpp.org/ftp/Specs/archive/43_series/43.059/.

[22] 3GPP, "Location Services (LCS); Functional description; Stage 2," 3rd Generation Partnership Project (3GPP), TS 03.71, June 2004, http://www.3gpp.org/ftp/Specs/html-info/0371.htm.

[23] 3GPP, "Location services (LCS); service description; stage 1," 3rd Generation Partnership Project (3GPP) TS 22.071, 2007, http://www.3gpp.org/ftp/Specs/html-info/22071.htm.

[24] 3GPP, "Location Services (LCS); broadcast network assistance for Enhanced Observed Time Difference (E-OTD) and Global Positioning System (GPS) positioning methods," 3rd Generation Partnership Project (3GPP) TS 04.35, 2002, http://www.3gpp.org/ftp/Specs/html-info/0435.htm.

[25] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *Computer*, vol. 34, no. 8, pp. 57–66, 2001.

[26] 3GPP, "Radio transmission and reception," 3rd Generation Partnership Project (3GPP) TS 05.05, 2005, http://www.3gpp.org/ftp/Specs/html-info/0505.htm.

[27] M. A. Spirito, "On the accuracy of cellular mobile station location estimation," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 3, pp. 674–685, 2001.

[28] M. Weckstrm, M. Spirito, and V. Ruutu, "Mobile station location," in *GSM, GPRS and EDGE Performance—Evolution towards UMTS*, T. Halonen, J. Romero, and J. Melero, Eds., chapter 4, pp. 119–139, John Wiley and Sons, 2nd edition, 2003.

[29] S. Gezici, "A survey on wireless position estimation," *Wireless Personal Communications*, vol. 44, no. 3, pp. 263–282, 2008.

[30] L. Chen, S. Ali-Löytty, R. Piché, and L. Wu, "Mobile tracking in mixed line-of-sight/non-line-of-sight conditions: algorithm and theoretical lower bound," *Wireless Personal Communications*, vol. 65, no. 4, pp. 753–771, 2012.

[31] Y. T. Chan and K. C. Ho, "A simple and efficient estimator for hyperbolic location," *IEEE Transactions on Signal Processing*, vol. 42, no. 8, pp. 1905–1915, 1994.

[32] K. C. Ho, "Bias reduction for an explicit solution of source localization using TDOA," *IEEE Transactions on Signal Processing*, vol. 60, no. 5, pp. 2101–2114, 2012.

[33] M. A. Spirito and A. G. Mattiolli, "Preliminary experimental results of a GSM mobile phones positioning system based on timing advance," in *Proceedings of the 1999 VTC-Fall IEEE VTS 50th Vehicular Technology Conference 'Gateway to 21st Century Communications Village'*, pp. 2072–2076, Amsterdam, The Netherlands, September 1999.

[34] R. Bill, C. Cap, M. Kofahl, and T. Mundt, "Indoor and outdoor positioning in mobile environments—a review and some investigations on WLAN-positioning," *Geographic Information Sciences*, vol. 10, no. 2, pp. 91–98, 2004.

[35] X. Wang, Z. Wang, and B. O'Dea, "A TOA-based location algorithm reducing the errors due to non-line-of-sight (NLOS) propagation," *IEEE Transactions on Vehicular Technology*, vol. 52, no. 1, pp. 112–116, 2003.

[36] J. Bull, "Wireless geolocation: advantages and disadvantages of the two basic approaches for E-911," *IEEE Vehicular Technology Magazine*, vol. 4, no. 4, pp. 45–53, 2009.

[37] A. El-Rabbany, *Introduction to GPS: The Global Positioning System*, Artech House, Norwood, Mass, USA, 2nd edition, 2006.

[38] F. Vatalaro, G. E. Corazza, C. Caini, and C. Ferrarelli, "Analysis of LEO, MEO, and GEO global mobile satellite systems in the presence of interference and fading," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 291–300, 1995.

[39] M. Imae, E. Kawai, and M. Aida, "Long term and long distance GPS time transfer corrected by measured ionospheric delay," *IEEE Transactions on Instrumentation and Measurement*, vol. 42, no. 2, pp. 490–493, 1993.

[40] G. De 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.

[41] 3GPP, "Location Services (LCS); Mobile Station (MS)—Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)," 3rd Generation Partnership Project (3GPP) TS 04.31, 2007, http://www.3gpp.org/ftp/Specs/archive/04_series/04.31/.

[42] H. Welte, "Report of OpenBSC GSM field test August 2009, HAR2009, Vierhouten, The Netherlands," Tech. Rep., HAR2009, 2011, https://openbsc.osmocom.org/trac/raw-attachment/wiki/FieldTests/HAR2009/har2009-gsm-report.pdf.

[43] Osmocom, "Welcome to Osmocom OpenBSC," May 2014, http://openbsc.osmocom.org/trac/.

[44] 3GPP, "Location Services (LCS); Functional description; Stage 2 (UMTS)," 3rd Generation Partnership Project (3GPP), TS 23.171, April 2004, http://www.3gpp.org/ftp/Specs/archive/23_series/23.171/.

[45] 3GPP, "User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN); stage 2," 3rd Generation Partnership Project (3GPP) TS 25.305, 2008, http://www.3gpp.org/ftp/Specs/html-info/25305.htm.

[46] 3rd Generation Partnership Project (3GPP), "UE positioning enhancements," Tech. Rep. TR 25.847, 2001.

[47] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Robust tracking in cellular networks using HMM filters and Cell-ID measurements," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 3, pp. 1016–1024, 2011.

[48] J. Borkowski and J. Niemelä, "Enhanced performance of Cell ID+RTT by implementing forced soft handover algorithm," in *Proceedings of the IEEE 60th Vehicular Technology Conference (VTC '04)*, pp. 3545–3549, September 2004.

[49] S. Kong and B. Kim, "Error analysis of the OTDOA from the resolved first arrival path in LTE," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6598–6610, 2016.

[50] D. Porcino, "Performance of a OTDOA-IPDL positioning receiver for 3G-FDD mode," in *Proceedings of the 2nd International Conference on 3G Mobile Communication Technology*, pp. 221–225, March 2001.

[51] S.-F. Chuang, W.-R. Wu, and Y.-T. Liu, "High-resolution AoA estimation for hybrid antenna arrays," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 7, pp. 2955–2968, 2015.

[52] J. Caffery and G. L. Stiiber, "Subscriber location in CDNA cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 2, pp. 406–416, 1998.

[53] S. Sakagami, S. Aoyama, K. Kuboi, S. Shirota, and A. Akeyama, "Vehicle position estimates by multibeam antennas in multipath environments," *IEEE Transactions on Vehicular Technology*, vol. 41, no. 1, pp. 63–68, 1992.

[54] P. M. Grant, J. S. Thompson, and B. Mulgrew, "Adaptive arrays for narrowband CDMA base stations," *Electronics and Communication Engineering Journal*, vol. 10, no. 4, pp. 156–166, 1998.

[55] R. Klukas and M. Fattouche, "Line-of-sight angle of arrival estimation in the outdoor multipath environment," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 1, pp. 342–351, 1998.

[56] C. Li and Z. Weihua, "Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems," *IEEE Transactions on Wireless Communications*, vol. 1, no. 3, pp. 439–447, 2002.

[57] Y. Fu and Z. Tian, "Cramer-Rao bounds for hybrid TOA/DOA-based location estimation in sensor networks," *IEEE Signal Processing Letters*, vol. 16, no. 8, pp. 655–658, 2009.

[58] 3GPP, "Radio Resource Control (RRC); protocol specification," 3rd Generation Partnership Project (3GPP) TS 25.331, 2013, http://www.3gpp.org/ftp/Specs/html-info/25331.htm.

[59] 3rd Generation Partnership Project (3GPP), "Functional stage 2 description of Location Services (LCS)," TS 23.271, 2007.

[60] 3GPP, "Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN," 3rd Generation Partnership Project (3GPP) TS 36.305, 2014, http://www.3gpp.org/ftp/Specs/html-info/36305.htm.

[61] 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.

[62] J. M. Zagami, S. A. Parl, J. J. Bussgang, and K. D. Melillo, "Providing universal location services using a wireless E911 location network," *IEEE Communications Magazine*, vol. 36, no. 4, pp. 66–71, 1998.

[63] R. S. Campos and L. Lovisolo, *RF Positioning: Fundamentals, Applications and Tools*, Artech House, Norwood, Mass, USA, 1st edition, 2015.

[64] 3GPP, "LTE Positioning Protocol (LPP)," TS 36.355, June 2014.

[65] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation," TS 36.211, 2014.

[66] C. Mensing and S. Sand, "Performance enhancement of GNSS positioning in critical scenarios by wireless communications systems," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS '08)*, pp. 334–340, May 2008.

[67] Spirent, "An overview of LTE positioning," Spirent, White Paper, 2012, https://www.spirent.com/Assets/WP/WP_LTE_Positioning_Overview.

[68] I. S. Ari Kangas and T. Wigren, "Positioning in LTE," in *Handbook of Position Location: Theory, Practice, and Advances*, S. A. Zekavat and R. M. Buehrer, Eds., chapter 32, pp. 1087–1089, John Wiley & Sons, 2011.

[69] 3GPP, "LTE Positioning Protocol A (LPPa)," 3rd Generation Partnership Project (3GPP) TS 36.455, 2013, http://www.3gpp.org/ftp/Specs/html-info/36455.htm.