GSM Navigation Techniques

Technical Report · March 2015

DOI: 10.13140/RG.2.1.4585.7369

Nizar Zarka
Higher Institute for Applied Sciences and Technology

Higher Institute for Applied Science and Technology
Communication Department
Fourth Year

HIAST

GSM NAVIGATION

Submitted by

Mohammed Alebrahim

Supervisors

Scientific Supervisor

Dr. Nizar Zarka

Eng. Mousaab Orabi

Language Supervisor

Mr. Sameeh Dlaikan

Organizer Supervisor

Dr. Nizar Zarka

31/3/2015

For My Parents

Acknowledgments

I am grateful to the department of Communication, HIAST Damascus for giving me the opportunity to conduct this paper, which is an integral part of the curriculum in Communication Engineering.

I would like to take this opportunity to express heartfelt gratitude for my scientific supervisor Eng. Mousab Orab, who provided me with valuable input at various stages of this paper writing.

I would also like to acknowledge the support of every individual who assisted me in making this paper a success, and I would like to thank Dr. Nizar Zarka, the organizer supervisor for his guidance, support and direction without which, paper and presentation would not have taken shape.

I am also thankful to the language supervisor Mr. Sameh Dilekan for helping me.

Table of Contents

List of Figures

List of Tables

List of abbreviations

GSM	Global System For Mobile communication
BTS	Base Transceiver Station
RSSI	Received Signal Strength Information
MS	Mobile Station
GPS	Global Positioning System
API	Application Program Interface
UMTS	Universal Mobile Telephone System.
CI SI	Cell Identity with cell Sector
RSS	Received Signal Strength
CI-TA	Cell Identity-Timing Advanced
E-CL	Enhanced Cell Identity
RTT	Round Trip Time
AOA	Angle of Arrival
ID	Identification

Abstract

Research in positioning in GSM (Global System for Mobile communication) phones has gained interest recently as it enables a wide set of location based services.

RSSI (Received Signal Strength Information) based technique has been the preferred method for GSM localization on the handset as RSSI information is available in all cell phones. Although the GSM standard allows for a MS (Mobile Station) to receive signal strength information from up to six BTSs (Base Transceiver Stations), many of today's cell phones are low-end phones, with limited API (Application Program Interface) support that give only information about the associated cell tower. In addition, in many places in the world, the density of cell tower is very limited. This raises the challenge of accurately determining the cell phone location with very limited information, mainly the RSSI of the associated cell tower.

This paper argues that localization solution based on cellular phone technology, specifically GSM phones, is a sufficient and attractive option in terms of coverage and accuracy for a wide range of indoor, outdoor, and place based location-aware applications. This paper will be presented preliminary results that indicate that GSM-based localization systems have the potential to detect the places that people visit in their everyday lives, and can achieve median localization accuracies of 50 meter for indoor and outdoor environments. Respectively I'll discuss in this paper many topics about positioning by GSM. In the beginning, this paper will presented the structure of GSM network, and then compare between positioning in GSM and GPS (Global Positioning System).

Then, the methods used in determining the location will be discussed. Finally, this paper will be cited some applications based on positioning using GSM network.

Introduction

Generally, positioning technologies can be defined in terms of:

- **Performance.** This is based on the accuracy of the positioning method that gives different levels of accuracy and hence aims at different market sectors. For example, fleet managers do not require a high level of accuracy, so this method can simply find the nearest antenna to the device. However, emergency services, such as determining the distance that the device is away from several antennas.
- **Complexity.** Sometimes combining and deploying two or more location technologies gives results that are more accurate. These positioning technologies can be grouped under complexity, and are commonly known as hybrid systems.
- **Implementations requirements**. Some implementations require extra applications in the existing system to achieve some degree of accuracy, such as in the software requirements of the handsets, or in the hardware requirements of the mobile network.
- **Investment.** This a major factor, and it depends on the amount of additional services that the network can provide for in the future, and their required level of accuracy.
  For example: a person is in an accident but precise location is unknown.

How can the rescue team find location of this person?

On possible solution: localize the mobile phone of this person via GSM positioning.

Chapter 1: Principals and Definitions

1- Definition

GSM positioning: is positioning technology that depends on mobile network. There for to understand GSM positioning system we need a basic understanding of how the network cells structures are built. Let us ponder of the following figure1.

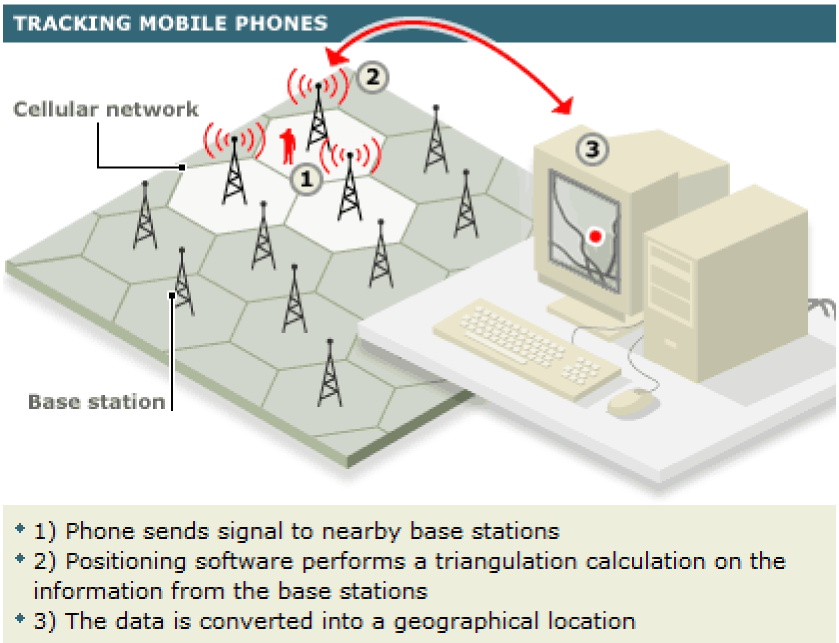


Figure 1: Steps of Positioning.

2- The architecture of GSM system

Each mobile contains a number of base stations including the respective antennas that serve the nearby cell phones or mobile phone. These base stations are located throughout the country and are called Base Transceiver Stations (BTS) and it almost has direction coverage. Figure 2.

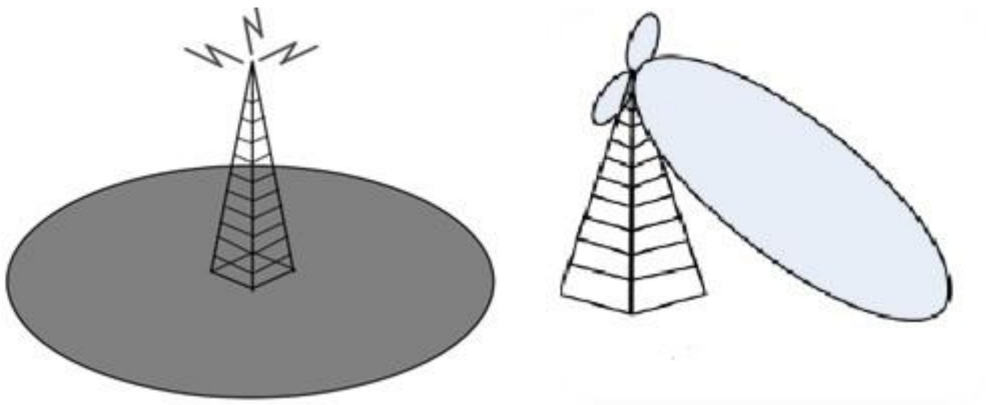


Figure 2: Base Transceiver Stations (BTS).

Some BTSs are pooled and are controlled by a Base Station Controller (BSC). The next higher hierarchy is the Mobile Switching Center (MSC) that routes calls between MSs and between MSs and fixed-line network phones. The region controlled by an MSC is frequently identical to the so-called Location Area (LA) that plays an important role for positioning techniques, as will be seen later on. The number of BSCs controlled by one MSC as well as the number of BTSs controlled by one BSC may vary from one provider to another as well as from one region to another. Data, and not only positioning relevant data, may be acquired at different interfaces. Between the BTS and the BSC the so-called Abis-interface is defined. The data available at one of these interfaces are restricted to all BTS assigned to this one BSC, but it is more detailed than on the higher level interfaces. The next hierarchy is the A-interface that is defined between the BSC and the MSC. All data of the BSC assigned to one MSC may be acquired at one of these interfaces. Figure 3 gives an overview about the GSM network structure and the respective interfaces relevant for the positioning task.

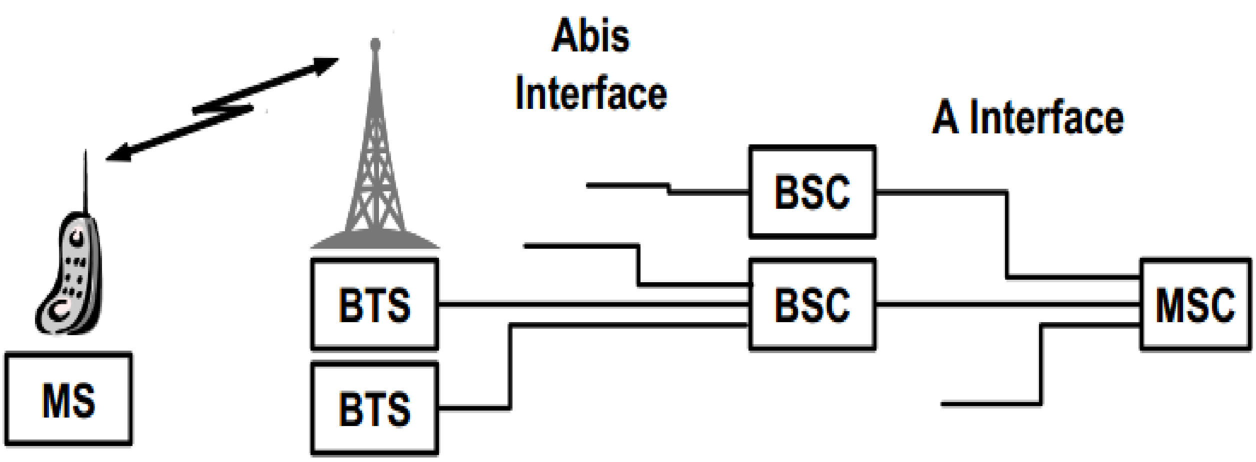


Figure 3: Structure of GSM network interfaces.

Every BTS has a coverage reach that we often call a cell. Figure 4

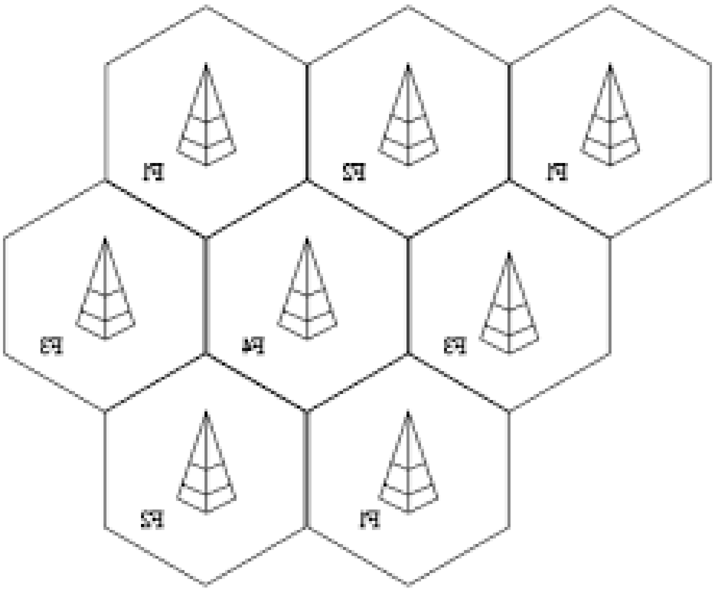


Figure 4: Cells of BTSs.

3- Different types of cells:

There are three different types of cells:

3- 1- Omni cell:

If the demand for capacity in a certain area is low, it is common to place the base station in the middle of the cell, and let the antenna be omnidirectional, covering 360°. This gives the widest geographical coverage.

3- 2- Sector cell:

In urban areas, sector cells are often used. One base station is then placed where three smaller cells meet, with 120° coverage for each antenna. Many small cells together give higher capacity than a few big cells.

3- 3- Polygon cells:

In UMTS (Universal Mobile Telephone System) radio access networks the cells are shaped as polygons. The polygon can be built with a number of corners between 3 and 15 [1]. Figure 5 shows these three types.

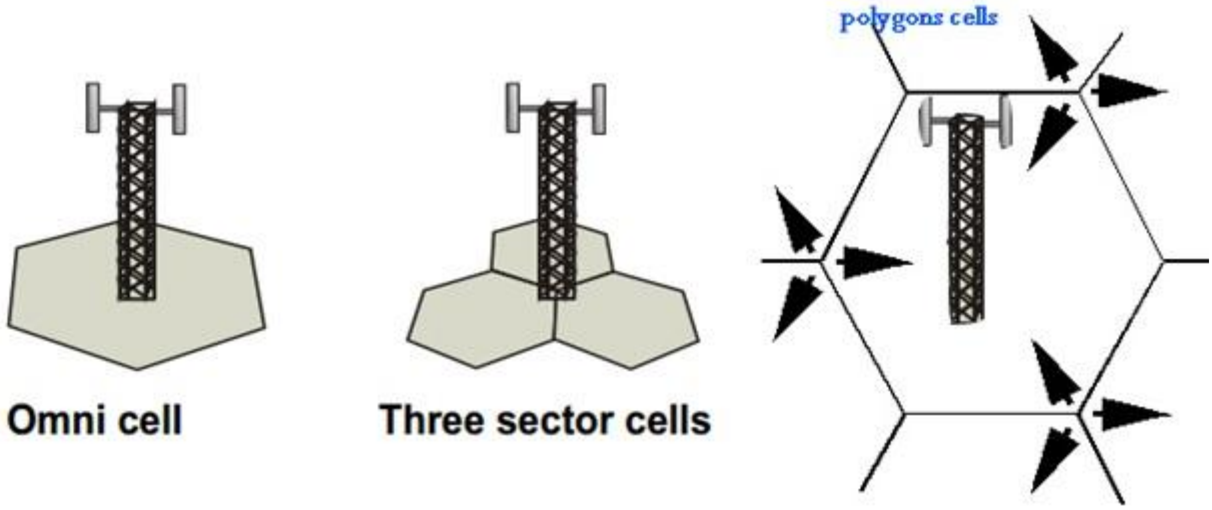


Figure 5: Three different types of cells.

The size of the cell normally depends on the population. Actually, cells that are in the countryside are the largest and those in big cities are the smallest.

GSM positioning is possible by knowing which base station a mobile device is connected to, the accurate of positioning is generally connected to the cell size.

4- Comparison between GSM and GPS navigation:

We know that we can use GPS for navigation so why GSM is used widely nowadays. To answer this query we need to compare between these two methods. Figure 6 show the simple graph for them.

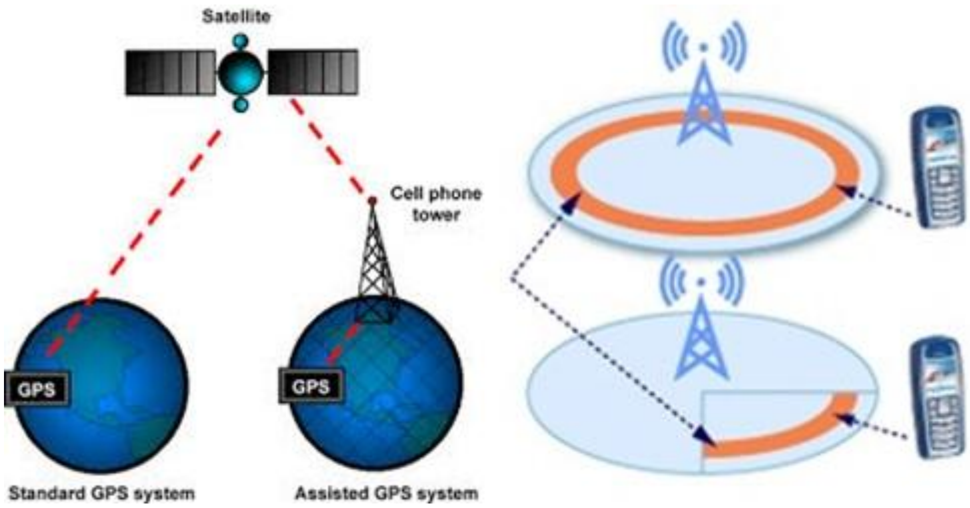


Figure 6: GSM and GPS positioning.

The GSM positioning system continues the movement of the positioning technologies from the sky to ground bases by replacing completely the satellites from the picture. In developed countries, there are many GSM towers in urban areas. This is what we call existing infrastructure but in GPS we need satellites. This is added to the fact that this technology doesn't consume more power [2]. Figure 7 compares between many technologies in consumption of power.

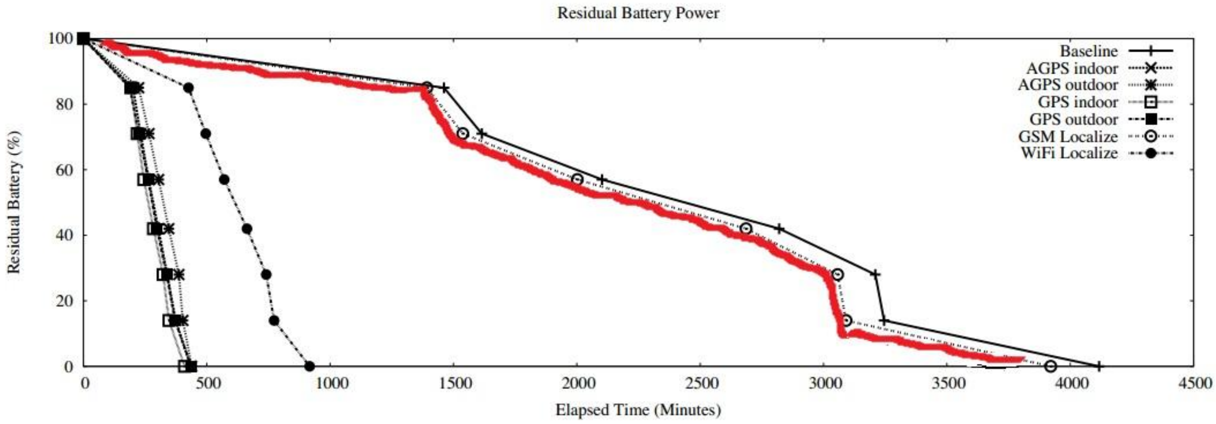


Figure 7: Energy consumption due to GPS, A GPS, WiFi, and GSM based localization in comparison to a baseline scheme. Experiment performed on Nokia N95 phone platform.

And since the phone knows by default how to measure and get the tower's id, there is just a software issue to get the ids, match them to a table with geographical positions and triangulate, based on the strength of signal the user's position. However, if you are in a remote area, like in mountains, where there are few emitters the quality of location falls dramatically. [2]

GPS is an outdoor device and you cannot use it indoor unlike GSM which you can use anywhere you have a signal coverage. [3]

Above all, in GPS you are the only person who can access this data so you are the sole beneficiary unless you send them to others, but in GSM localization positioning system can get your position data immediately.

Therefore, we can summarize these differences in the following table

Table 1: Difference between GSM and GPS.

GSM positioning	GPS positioning
Utilize the GSM network	Uses satellites to find position
Gives us an approximate location	Give us good accuracy
Works inside buildings, within cargo, in garage	Doesn't work inside and in covered places. Need to "see" the satellites
Consume low power	Consume high power
Works inside mobile system	Doesn't work without GSP chip

Chapter 2: Methods of GSM positioning and Applications

There are several methods for this purpose. I will present some of them:

- CI SI (cell Identity with Cell Sector)
- RSS (Received Signal Strength)
- Handover event
- CI-TA (Cell Identity-Timing Advanced)
- E-CL (enhanced cell identity)
- RTT (Round Trip time)
- AOA (Angle of Arrival)

The backbone in all cellular positioning systems is the cell ID (Identification) method, so this method identifies the cell which the mobile is connected to and give a geographical description of the boundary of the this cell. [4]However, notice that low accuracy depends on the size of cell in figure 8.

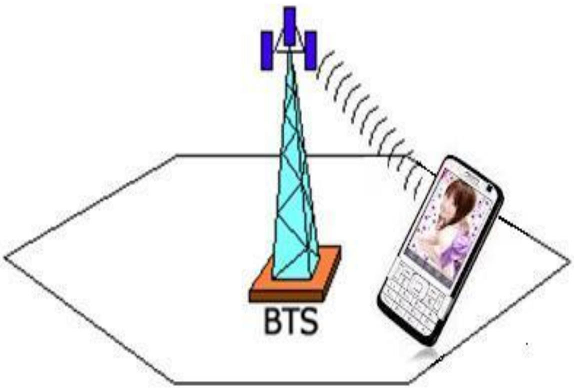


Figure 8: accuracy depends on the size of cell.

However, when we come to the accuracy the level of the uncertainty, “the uncertainty area” is as big as the cell itself. Therefore, the cell ID method is available wherever there is cellular coverage. It does not rely on any radio measurements and the response time is therefore very low. The problem is of course the accuracy that is limited by the size of the cell. [5]

1- CI SI (cell Identity with Cell Sector):

This is an extension of IC method and the position of the mobile phone is the position of the cell and sector in which the mobile phone is registered. Mostly there are three sectors each one covers 120 degree. When we come to the accuracy it is form hundred meters to hundred kilometers according to the sector size. Notice figure 9.

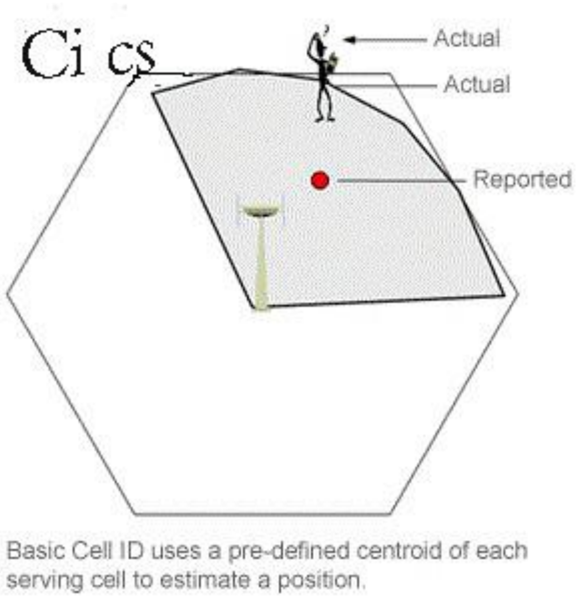


Figure 9: CI -CS Method.

2- RSS (Received Signal Strength):

This is an extension of IC CS method by measuring the signal strength of mobile phone in the sector. Notice figure 10.

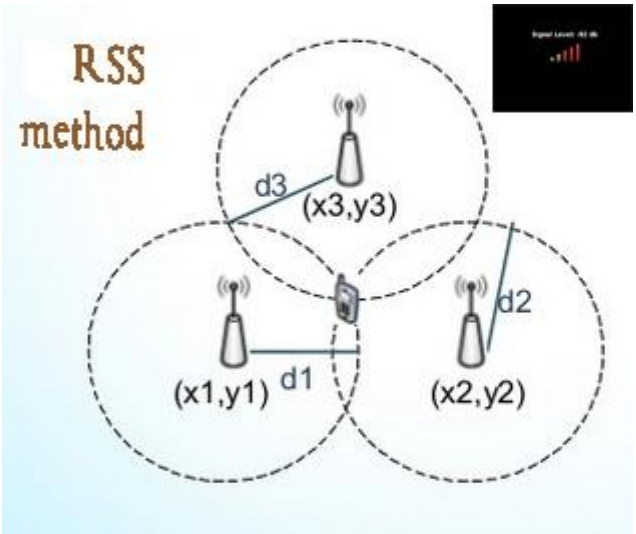


Figure 10: RSS Method.

The received signal strength at the mobile station is important information for e.g. **handover** decisions. (When MS move from BTS to another neighboring one). Therefore, the MS can measure the signal strength of the serving cell and up to six neighboring BTS. The MS transmits these measurements to the network during communication. The accuracy of the signal strength is subject to fluctuations, since it depends on metrology multipath propagation, shadowing effects (moving and fixed objects).

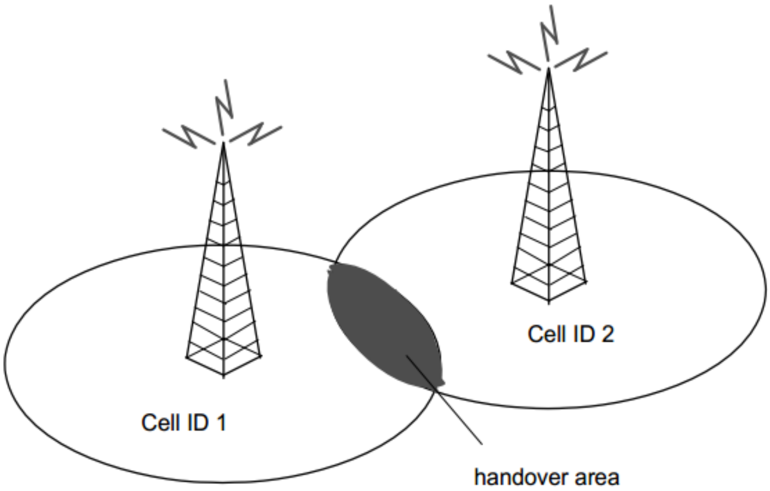
The signal strength is measured between-110dB m and 48dB m. The unit dB m is transmission power related to 1mW. The difference between two transmission levels is given in dB (up to -70dB m) respectively 6 dB .The accuracy decreases, in other words the standard deviation gets higher, with increasing distance.

The problem in this method is that the received signal in the mobile isn't necessarily the signal transmitted from the BTS, where it can be reflected several times before reaching the MS. [6]

There is also of the problem of damping in the transmission area which measure by dB m. When we come to the accuracy, it is from (100 m to 20Km).

3- Handover Event:

The next possibility to position mobile phones is the handover event. This occurs when a mobile phone switches from one BTS to the next one due to low quality communication e.g. indicated by a low RSS value. The advantage of this method is the availability of two cell IDs at the moment of handover, thus defining the borderline of the two cells as position. The restriction is that this increased accuracy is not available all the time. Again the accuracy depends on the size of the cell areas. Figure 11 presents an exemplary geometry for a handover event. The same principle may be used, if a mobile switches from one LA to the next one. In this case the accuracy is decreased, because the LAs are larger than the cells. For the new LA the respective cell ID is delivered too, thus compensating the decrease of accuracy partially. [7]



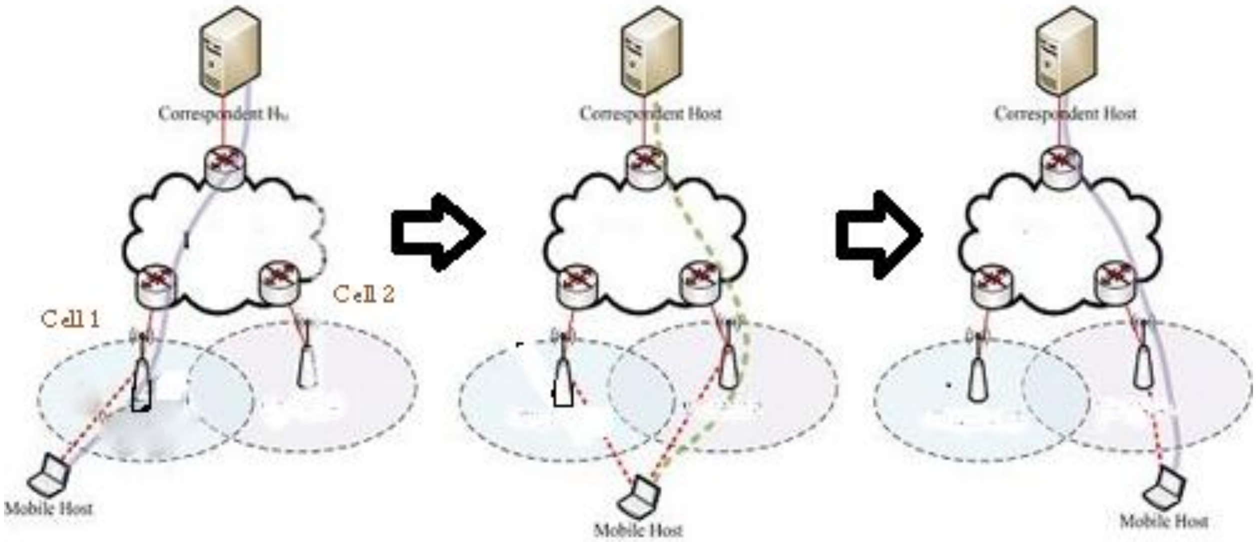


Figure 11: Positioning during handover event.

4- CI-TA (Cell Identity-Timing Advanced):

The method measures the time difference between the base station and the mobile device, the positioning system then calculates the distance between them [8]

This method gives the same accuracy as CI method in big cities but highly improves accuracy in countryside. The time difference between the base station and the mobile is that time which a signal takes to reach the mobile from the base station and goes back to the station. Measuring the propagation time –the time of travel of signal between BTS and MS BTS sent a signal and wait for a response from MS. After measuring the time difference the positioning system divides the cells area into several disks, each one has TA value according to its distance from the BTS. Timing advanced value- when MS sends the signal to BTS value is divided from 0-1-…to 63 (equates 0 m -55 m -…to 35km) [3] For example: in TA0 disk the time difference equals 3,69 µs equates 550 m Figure 12.

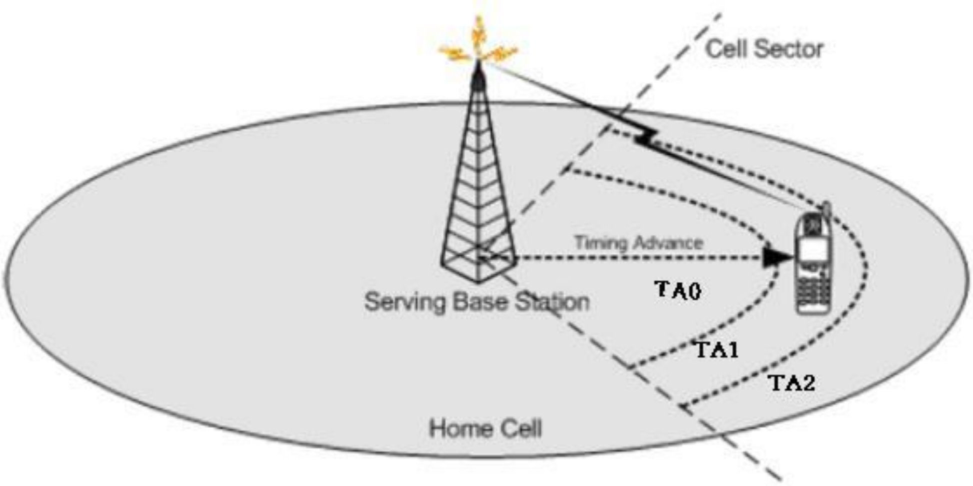


Figure 12: Timing advance value.

The signal's travel time can be computed in a completely synchronized network. Usually, the MS clock is not synchronized, so its clock bias must be treated as a nuisance parameter. This is the case in GPS where only the satellites are synchronized. Travel time can be measured in many different ways. [9]

For example, it is estimated in the uplink to GSM at multiple BSs upon the request of the network. The performance depends mainly on the synchronization accuracy, which in turn is limited by the chip rate. GPS typically features an accuracy of about 10 m in unobstructed environments, while 2G and 3G system have an achievable accuracy in the neighborhood of 100m.

GSM system intrinsic measurement quantities are the TA-value, and RSS value for the measurement of the signal strength at the MS with respect to the serving BTS and up to six neighboring BTS. Both may be convert into distance that may be used for positioning using arc sections.

5- E-CL (enhanced cell identity):

This is an extension of CI-TA method which gives a smaller uncertainty area by reduction in cell sectors angle, the mobile device measures the signals strength from near sector cells. This method has no effect in Omni cell in rural areas but gives much higher accuracy in small Omni cells in the cities. Figure 13.

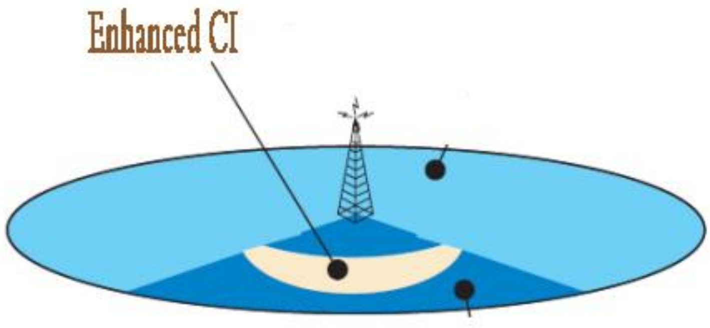


Figure 13: E-CI method.

6- RTT (Round Trip time):

This is an extension of CI-TA method, and in this method MS sent simultaneous signals to two or more BTS, each BTS computes the time difference and converts this to distance to MS. [4] Figure 14.

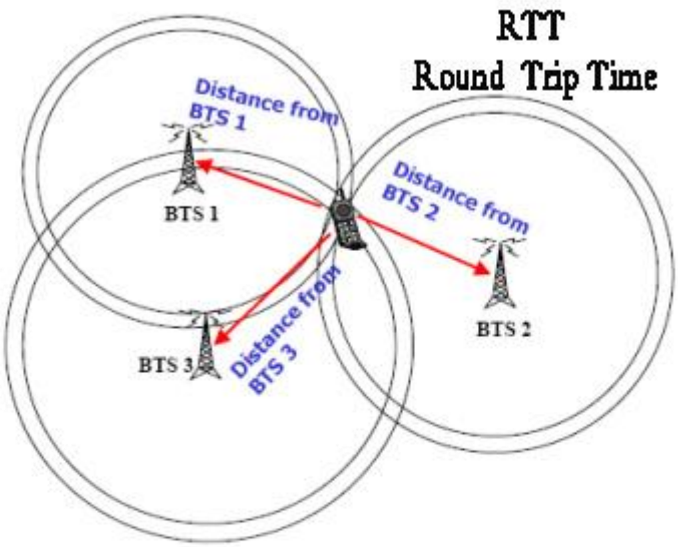


Figure 14: RTT method.

In general, this method is called Time-of- Arrival (TOA). Due to the fact that more than three distance are available, the solution is not unique and may be solved by e.g. least square adjustment. [4] In this method, we should know that BTS must be exactly synchronized. Time delay of one (microseconds) involves 150 m inaccuracy. Bias error is possible when unsynchronized. Passive positioning is possible. [10]

7- AOA (Angle Of Arrival):

This method depends on measuring the AOA of a signal from BTS at MS or the AOA of a signal from MS at BTS. However, it needs extension (antenna with angle measurement unit) Signal angle of arrival (AOA) information, measured at the BS using an antenna array, which can be used for positioning. Assuming two-dimensional geometry, angle of arrival measurement at two BSs is sufficient for unique location. This is illustrated in Figure 15, where the user location is determined as the point of intersection of two lines drawn from the BSs. It is seen that AOA technique requires line of sight between the MS and the BSs for accurate results. In addition, the uncertainty in AOA measurement causes a position uncertainty that increases with MS-BS distance. Achieved accuracy depends on the number of available measurements, geometry of BSs around the MS and multipath propagation too.

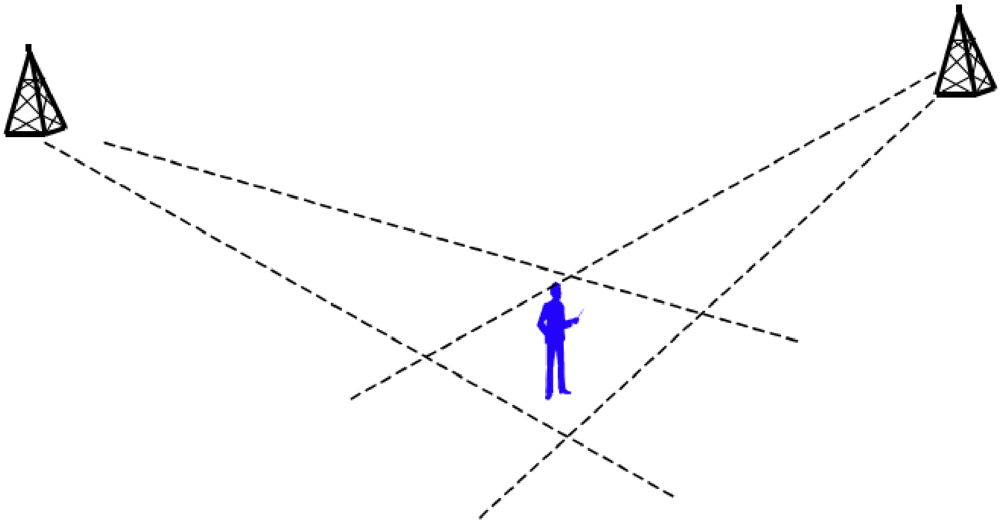


Figure 15: Positioning with angle of arrival measurements.

Since AOA method needs line-of-sight propagation conditions to obtain correct location estimates, clearly, it is not the method of choice in dense urban areas, where line of sight to two BSs is seldom present. In [11], an rms location error of approximately 300 m with 2 BSs and 200 m with 3 BSs in an urban environment was observed. However, the AOA technique could be used in rural and suburban areas where the attainable accuracy is better and it is an advantage to be able to locate a MS which can only be measured by two BSs. A major barrier to implement AOA method in existing 2G networks is the need for an antenna array at each BS. It would be very expensive to build an overlay of AOA sensors to existing cellular network. However, since it is a network-based method and supports legacy handsets, it is developed by several companies as an E911 solution. In 3G systems AOA measurements may become available without separate hardware if adaptive BS antennas (arrays) are widely deployed. In addition to financial issues, AOA method may have a capacity problem. Multilateral measurement principle (measurement at several BSs) requires the co-ordination of almost simultaneous measurements at several BS sites, and it is difficult to serve a large number of users.

Accuracy:

As we saw previously, each method has different accuracies and the following table shows us the precision of GSM-positioning methods.

Table 2: Precision of GSM-Positioning. [3]

Precision of GSM-Positioning	
Method	Precision
Cell ID	100 m -35km
CI with Cell Sector	100 m -35km
CI with CS and Received Signal Strength	100 m -20km
Angle Of Arrival (AOA)	50 m -150m
Round-Trip-Time (RTT)	50 m -150m
Time Difference Of Arrival (TDOA)	50 m -150m
Enhanced Time Difference (ETD)	50 m -150m

Applications:

- This technique is used in emergencies to see places of people injured.
- In cases of natural disasters.
- In security applications to track criminals.
- Observers also used to track wild animals and monitor their movement.
- Commercial application. [10]
- Drive Test - The method of GSM signal testing:
  Drive test implies testing the GSM network quality and checking the range of the signal with the help of a moving vehicle. The testing is carried out using special equipment installed on a car. The main part of the equipment is a GSM standard mobile phone, a lap top and special equipment connected to it which identifies the geographical location.
  Drive Test or a programme for measuring and data analysis allows for assessing the area covered by the GSM signal, its level, quality, functioning of the main stations and the quality of separate elements and units.
  The equipment measures the level of the signal in any given location.

  Below you is map of Tbilisi covered by Magti GSM signal
  (See figure 16).
  Different colours show different levels of signal in the streets of Tbilisi.

The green colour indicates high level of the received signal, blue shows its normal level, yellow – is a medium level and red shows the lowest level. There are certain factors which determine different types of the signal: the distance to the nearest base station, specificity of the relief, and the construction characteristics of the building.
The closer the mobile phone is from the base station, the stronger is the level of the signal. The range covered by the main station is 35 km. [12]

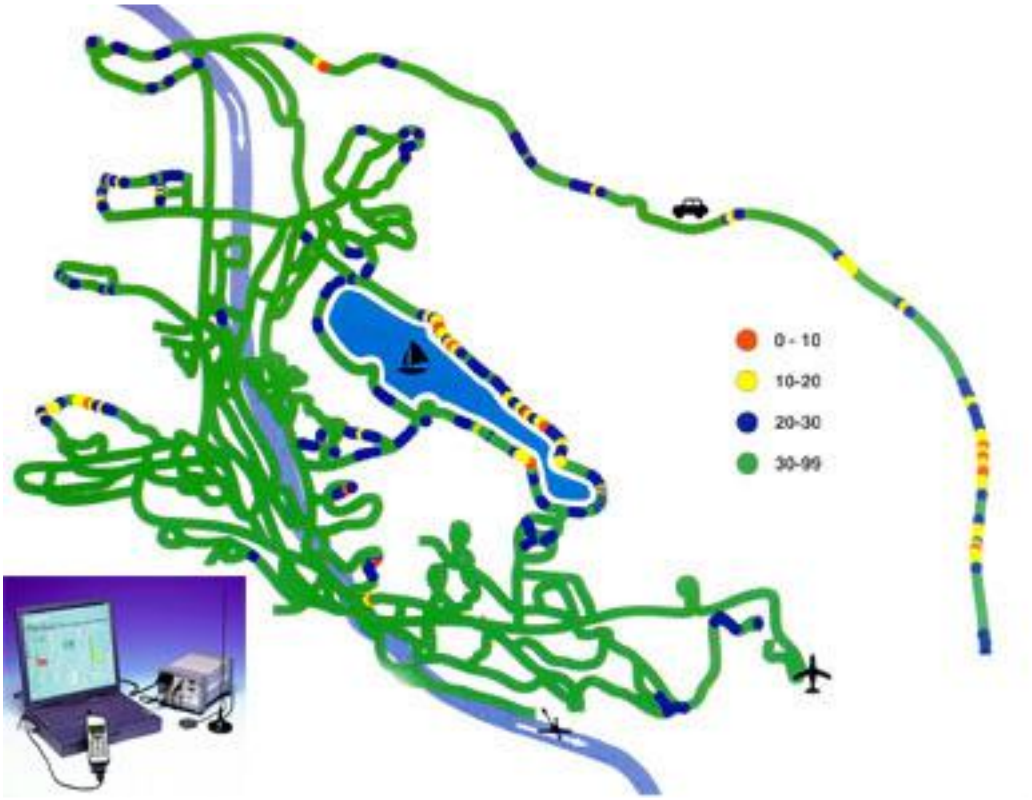


Figure 16: map of Drive Test - The method of GSM signal testing

Conclusion:

In this paper, the comparison between GSM and GPS positioning is presented and the methods used in GSM positioning and the measurement these methods depend on are studied. In addition, we compared between these methods according to the accuracy of each one. We ended this paper by presenting some of the applications where this technology is used. GSM positioning is of increasing importance for safety, gaming, and commercial services, so the question remains where there is a more accurate method, and if it is possible to implement this method in practice.

Works Cited

[1] GoFinder INTERNATIONAL, "Positioning Handsets on a Telstra GSM network," [Online]. Available: www.gofinder.net/. [Accessed 22 February 2015].

[2] Radu Poenaru, "GPS vs aGPS vs WiFi vs GSM localization," Agile and Ruby Lab , 26 August 2009. [Online]. Available: http://radupoenaru.com/?p=784. [Accessed 23 February 2015].

[3] J. Kushwaha, "Location Estimation of GSM user Using Enhanced Tringularisation Method with Implementation of RF Fingure Printing," *International Journal of Engineering Science and Innovative Technology (IJESIT),* vol. 3, no. 6, pp. 347-351, 2014.

[4] Department of Information Technology, "Location technology for cellular systems," Uppsala University, 2014. [Online]. Available: http://www.it.uu.se/katalog/tw/research/LocationTechnology.

[5] D. L. Dirk Gerstenberger, "Method and arrangement for dl-otdoa (downlink observed time difference of arrival) positioning in a lte (long term evolution) wireless communications system". Stockholm, Sweden Patent WO2010104436 A1, 16 Septemper 2010.

[6] J. V. Stoep, "Design and Implementation of Reliable Localization Algorithms using Received Signal Strength," University of Washington, Washington, 2009.

[7] Wikipedia, "Handover," Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Handover. [Accessed 23 February 2015].

[8] "TS-80 positioning and measurement within the GSM network," in *6th FIG regional Conference*, San Jose, 2007.

[9] F. G. Fredrik Gustafsson, "Mobile Positioning Using Wireless Networks," *IEEE SIGNAL PROCESSING MAGAZINE,* pp. 41-53, July 2005.

[10] M. F. L. K. J. N. J. K. I. G. J. r. D. Katerina Dufková, "Active GSM Cell-ID Tracking: "Where Did You Disappear?"," Charles University, Prague, 2009.

[11] A. K. S. a. A. Sakagami.S, "Vehicle position estimates by multibeam antennas in multipath environments," *IEEE Trans. Veh. Technol,* vol. 41, no. 1, pp. 63-68, 1992.

[12] D. Kurtskhalia, " Drive Test - The method of GSM signal testing,". [Online]. Available: http://www.magticom.ge/magazine/1999-3/1999-3-4.html.