LOCATION AWARE SYSTEM
USING MOBILE STATION IN GSM NETWORK

ABDUL MUEED KHALID

FACULTY OF COMPUTER SCIENCE
AND INFORMATION TECHNOLOGY

UNIVERSITI MALAYA
KUALA LUMPUR

OCTOBER 2007
LOCATION AWARE SYSTEM USING MOBILE STATION IN GSM NETWORK

ABDUL MUEED KHALID

DESSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF COMPUTER SCIENCE

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

UNIVERSITI MALAYA KUALA LUMPUR

OCTOBER 2007
IN THE NAME OF THE GOD, THE MOST GRACIOUS AND THE MOST MERCIFUL
ABSTRACT

Ever since humans first started travelling, people have developed technologies to locate their position. Today locating a mobile device is considered easy, thanks for the remarkable location technology developed by US military called GPS. GPS has become the standard for location technology. But now it is time to look beyond GPS technology. It is time to look in to technologies that is affordable to every one, like mobile cellular telephone system.

Mobile phone service is a service that is affordable to every one. Similar to GPS, mobile phone also uses electromagnetic waves to communicate. Mobile phone industry is a potentially huge market and service like location service not only benefits the users but also generate huge revenue to the networks. This research concentrates on providing a cheap solution to implement and provide location service in mobile phone.

An in-depth study of location technologies and its possible services has been carried out. The proposed solution has been developed by concentrating on the needs of reducing the cost of implementing location service. Developed solution is based on signal strength which is already available in the network. This solution propose method of using propagation models to find the distance between mobile user and the base station and use triangulation method to calculate the location. It also propose a location processing model which gives an improved result compared with Time advance and cell sector. This thesis also proposes methods of implementing location service in the network including the methods of presenting location service in the mobile devices.
An experimental investigation was carried out to find out the reliability of location technology proposed. It is shown that proposed location method can be used in most of the location service. Accuracy of the location technology proposed shows improved results and can cater old and new handsets. It is also noted that the proposed methods of providing location service will minimise the cost of implementing location technology.
ACKNOWLEDGEMENT

Praise is to God who has made it possible for me to undertake this research work.

I would like to express my deepest gratitude to my supervisor, Dr. Rosli Salleh for his invaluable guidance, encouragement, faith and advice during this research work and from whom I have learned enormously. In the mean time I would like to thank Ms. Rafidah Md Noor for her support and Dr. Ibrahim Mohamed from Institute of Mathematical Sciences for his support in mathematics related works.

I would also like to express my special thanks to Maldives telecommunication company “Dhiragu” for providing information necessary for this research. I would also like to greatly appreciate and thank all the staffs from Dhiragu who helped me in getting the information I requested knowing that the requested information is confidential information of the company.

I sincerely thank all family members and friends for helping me and providing me support and encouraged me throughout the study. Last but by no mean the least, I would like to thank from bottom of my heart to my wife for the help and effort she has taken during the course of this studies. Finally I would like to thank my mother for her constant prayers.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>v</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xiii</td>
</tr>
<tr>
<td><strong>1. INTRODUCTION</strong></td>
<td></td>
</tr>
<tr>
<td>1.1. GENERAL INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.2. MOTIVATION BEHIND MOBILE LOCATION SERVICES</td>
<td>5</td>
</tr>
<tr>
<td>1.3. RELATED WORK</td>
<td>7</td>
</tr>
<tr>
<td>1.4. OBJECTIVE OF THE STUDY</td>
<td>9</td>
</tr>
<tr>
<td>1.5. SCOPE OF THE STUDY</td>
<td>11</td>
</tr>
<tr>
<td>1.6. OUTLINE OF THE THESIS</td>
<td>12</td>
</tr>
<tr>
<td><strong>2. GSM MOBILE COMMUNICATION NETWORK</strong></td>
<td></td>
</tr>
<tr>
<td>2.1. HISTORY</td>
<td>14</td>
</tr>
<tr>
<td>2.2. ARCHITECTURE OF GSM NETWORK</td>
<td>15</td>
</tr>
<tr>
<td>2.2.1. Mobile Station (MS)</td>
<td>16</td>
</tr>
<tr>
<td>2.2.2. Base Station System (BSS)</td>
<td>16</td>
</tr>
<tr>
<td>2.2.3. Network Switching Subsystems (NSS)</td>
<td>17</td>
</tr>
<tr>
<td>2.2.4. Cell and Location Area (LA)</td>
<td>18</td>
</tr>
<tr>
<td>2.2.5. Addressing and identification</td>
<td>20</td>
</tr>
<tr>
<td>2.2.5.1. Identification of mobile subscriber</td>
<td>20</td>
</tr>
<tr>
<td>2.2.5.2. Identification of location area and base station.</td>
<td>21</td>
</tr>
<tr>
<td>2.2.6. The radio link interface</td>
<td>22</td>
</tr>
<tr>
<td>2.2.7. Protocol and signalling</td>
<td>23</td>
</tr>
<tr>
<td>2.2.8. Handover</td>
<td>24</td>
</tr>
<tr>
<td><strong>3. MOBILE LOCATION SERVICE</strong></td>
<td></td>
</tr>
<tr>
<td>3.1. INTRODUCTION</td>
<td>26</td>
</tr>
</tbody>
</table>
3.2. LOCATION BASED SERVICES 26
   3.2.1. Public Safety Services 27
      3.2.1.1. Emergency Services 27
      3.2.1.2. Emergency Alert Services 27
   3.2.2. Location Based Charging 28
   3.2.3. Fleet and Asset Management Services 28
   3.2.4. Location Based Information Services 28
      3.2.4.1. Navigation 29
      3.2.4.2. City Sightseeing 29
   3.2.5. Location Dependent Content Broadcast 29
3.3. MOBILE LOCATION TECHNIQUES 29
3.4. TYPE OF RADIO LOCATION SYSTEMS 32
   3.4.1. Network information based 32
      3.4.1.1. Using CI / CGI and TA for MS Location 32
   3.4.2. Signal strength based 33
   3.4.3. Angle of arrival based 34
   3.4.4. Time based 36
      3.4.4.1. Uplink Time of Arrival (TOA) 36
      3.4.4.2. Time Differences of Arrival (TDoA) 37
      3.4.4.3. Enhanced Observed Time Difference (E-OTD) 39
   3.4.5. GPS Based Positioning 40
      3.4.5.1. Assisted GPS (A-GPS) 40
3.5. CONCLUDING REMARKS 42

4. NETWORK INFORMATION BASED POSITIONING METHODS 45
   4.1. INTRODUCTION 46
   4.2. CELL 47
      4.2.1. Cell identity 47
      4.2.2. Using Cell Identity and Cell Sector to locate Mobile Stations 49
   4.3. TIMING ADVANCE 50
      4.3.1. Using Timing Advance to locate Mobile Stations 51
   4.4. OBSERVED TIME DIFFERENCE 54
      4.4.1. Time Difference of Arrival (TDoA) 55
4.4.1.1. TDOA location algorithm 56
4.4.2. TDOA using GSM 58

5. SIGNAL STRENGTH AS A METHOD OF LOCATING
5.1. INTRODUCTION 59
5.2. PROPAGATION PATH LOSS 60
   5.2.1. Indoor Propagation Path Loss 61
   5.2.2. Outdoor Propagation Path Loss 62
5.3. CALCULATING MS – BS LOCATION USING HATA MODEL 62
5.4. TRIANGULATING MS LOCATION 65
5.5. FACTORS CONTRIBUTING TO LOCATION ERROR 67
   5.5.1. Multipath propagation 68
   5.5.2. NLOS propagation 69
5.6. CONCLUDING REMARK 70

6. IMPLEMENTING LOCATION SERVICE IN GSM
6.1. INTRODUCTION 71
6.2. LOCATION PROCESSING MODULE (LPM) 72
6.3. METHODS OF IMPLEMENTING 78
   6.3.1. Network Based 78
      6.3.1.1. Subscriber tracking in GSM 78
   6.3.2. Hand Phone assisted network based 81
   6.3.3. SIM Application Toolkit 82
   6.3.4. SIM API for Java Card 84
6.4. MOBILE LOCATION SERVER (MLS) 84
   6.4.1. Subscriber Authorization Function (SAF) 85
   6.4.2. Subscriber Tracing Function (STF) 85
   6.4.3. Location Calculation Function (LCF) 86
   6.4.4. Formatting and Presentation Function (FPF) 86
6.5. PRESENTING LOCATION INFORMATION 88
6.6. LOCATION SERVICE STANDARD DEFINED BY UMTS 89
6.7. LCS COMMUNICATION PROTOCOLS 89
   6.7.1. LIF Mobile Location Protocol 89
7. EXPERIMENTAL RIG AND MEASUREMENT TECHNIQUES

7.1. INTRODUCTION
7.2. SELECTION OF AREA TO CARRY THE TEST
7.3. DEVELOPMENT OF TESTING TOOLS AND THE TESTING SETUP
   7.3.1. Engineering function in Nokia Mobile phone.
7.4. SOFTWARE DEVELOPMENT AND METHOD OF DATA GATHERING
   7.4.1. Implementation of Software Tool
      7.4.1.1. Protocol Implementation
      7.4.1.2. Commands Used
      7.4.1.3. Pseudocode
      7.4.1.4. Flow chart

8. RESULTS AND DISCUSSION

8.1. INTRODUCTION
8.2. EFFECT OF SIGNAL STRENGTH IN DIFFERENT SPEED
8.3. TIMING ADVANCE MEASUREMENTS
   8.3.1. Reliability of timing advance
   8.3.2. Possible applications using Timing Advance
8.4. SIGNAL STRENGTH
   8.4.1. Distance calculating using signal Strength
   8.4.2. Triangulating MS Location using the MS-BS distance
8.5. PROPOSED LOCATION PROCESSING MODEL

9. CONCLUSION

9.1. PROPOSED SOLUTION
9.2. EXPERIMENT
   9.2.1. Proposed Location Processing Model
9.3. CONTRIBUTIONS
9.4. PROBLEMS FACED
9.5. RECOMMENDATION FOR FUTURE WORK

REFERENCES
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Mobile Phone and Fix Line Subscribers Compared with Population (3rd Quarter 2004)</td>
</tr>
<tr>
<td>Figure 1.2</td>
<td>Growth Rate for Mobile Phone and Fix Line Subscribers</td>
</tr>
<tr>
<td>Figure 1.3</td>
<td>Some of the NTT DoCoMo’s location-dependent screen</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>General architecture of a GSM network</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Cell Configuration within a location area.</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>Structure of IMSI</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>Structure of Cell Global Identification (CGI)</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>Structure of Base Station Identity Code (BSIC)</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>Signalling protocol structure in GSM</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Cell ID and Timing Advance positioning method.</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>The geometry of the rang-based signal strength location method</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>The angle of arrival method for MS location. The line of position are straight lines whose intersection provides the location of MS.</td>
</tr>
<tr>
<td>Figure 3.4</td>
<td>TDoA Implementation</td>
</tr>
<tr>
<td>Figure 3.5</td>
<td>E-OTD Implementation</td>
</tr>
<tr>
<td>Figure 3.6</td>
<td>A-GPS Implementation</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>(a) 60° Sectoring; (b) 120° Sectoring</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>60° Sectored Cell</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Sectored Cells</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>TA and Cell Sector method used in positioning MS</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>Locating MS using TA from three BTS</td>
</tr>
</tbody>
</table>
Figure 4.6  TDoA method of MS location. The lines of location are hyperbolas whose intersection provides the location of the MS.

Figure 5.1  Typical MS -BS arrangement

Figure 6.1  Over all processes of LPM.

Figure 6.2  Processes of Identifying neighbouring Cells.

Figure 6.3  Processes of calculating MS location

Figure 6.4  Typical location processing scenario.

Figure 6.5  Tracking Activity

Figure 6.6  Functions of MLS

Figure 6.7  GSM network entity arrangements with LCS server

Figure 7.1  Male’, Capital of Maldives and its surrounding

Figure 7.2  Nokia Net monitor screen as seen on the mobile phone screen.

Figure 7.3  Setup and data recording screen of our MAGIC program.

Figure 7.4  Equipments used

Figure 7.5  Flow char showing main functions to receive data from hand phone and GPS.

Figure 8.1  Signal strength variation measured in different speed.

Figure 8.2  Comparison with Time Advance with actual MS location.

Figure 8.3  Percentage of TA values recorded.

Figure 8.4  Actual distance compared with the distance calculated using Hata model.

Figure 8.5  Error compared with actual distance and distance calculated with Hata Model and the average error.

Figure 8.6  Actual Error after triangulation using three BS and average error

Figure 8.7  Accuracy of MS location after processing using the proposed model for different number of MS-BS measurements
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Different cell type and its coverage</td>
<td>19</td>
</tr>
<tr>
<td>5.1</td>
<td>Average Signal loss for Radio Path Obstructed by Building Material</td>
<td>61</td>
</tr>
<tr>
<td>6.1</td>
<td>List of commands available in SIM Application Toolkit.</td>
<td>82</td>
</tr>
<tr>
<td>6.2</td>
<td>Parameters for each cell</td>
<td>86</td>
</tr>
<tr>
<td>8.1</td>
<td>Signal Strength measurements at different speed</td>
<td>110</td>
</tr>
<tr>
<td>8.2</td>
<td>TA Readings and Actual GPS location of MS</td>
<td>112</td>
</tr>
<tr>
<td>8.3</td>
<td>Percentage of TA value recorded in different areas.</td>
<td>113</td>
</tr>
<tr>
<td>8.4</td>
<td>Actual distance and the calculated distance with error measurements using Hata model.</td>
<td>116</td>
</tr>
<tr>
<td>8.5</td>
<td>Actual GPS location compared with calculated location using three BTS and its location error.</td>
<td>118</td>
</tr>
<tr>
<td>8.6</td>
<td>Actual GPS location compared with calculated location using three BTS and its location error.</td>
<td>120</td>
</tr>
<tr>
<td>8.7</td>
<td>Actual GPS location compared with calculated location using five BTS and its location error.</td>
<td>120</td>
</tr>
<tr>
<td>8.8</td>
<td>Actual GPS location compared with calculated location using seven BTS and its location error.</td>
<td>121</td>
</tr>
</tbody>
</table>
LIST OF ABBREVIATIONS

A-GPS  Assisted GPS
AOA  Angle of arrival
API  Application programming interface
AuC  Authentication Centre
BCC  Base Station Colour Code
BCCH  Broadcast Control Channel
BS  Base station
BSC  Base Station Controller
BSIC  Base Station Identity Code
BSS  Base station subsystem
BSSAP  BSS Application Part
BTS  Base Transceiver Station
BTSM  BTS Management protocol
CEPT  Conference of European Posts and Telegraphs
CGI  Cell Global Identification
CI  Cell Identity
CM  Circuit Mode Connection
DNS  Decca Navigation System
DTAP  Direct Transfer Application Part
EKF  Extended Kalman Filter
E-OTD  Enhanced Observed Time Difference
ETSI  European Telecommunication Standards Institute
FCC  Federal Communications Commission
FDMA  Frequency Division Multiple Access
GLONASS  Global Navigation Satellite System
GMLC  Gateway Mobile Location Centre
GMLS  Gateway Mobile Location Server
GPS  Global Positioning System
HLR  Home Location Register
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>JRC</td>
<td>Joint Radio Committee</td>
</tr>
<tr>
<td>KLIA</td>
<td>Kuala Lumpur International Airport</td>
</tr>
<tr>
<td>LA</td>
<td>Location area</td>
</tr>
<tr>
<td>LAC</td>
<td>Location Area Code</td>
</tr>
<tr>
<td>LAI</td>
<td>Location Area Identification</td>
</tr>
<tr>
<td>LBS</td>
<td>Location Based Services</td>
</tr>
<tr>
<td>LCS</td>
<td>Location Service</td>
</tr>
<tr>
<td>LIF</td>
<td>Location Interoperability Forum</td>
</tr>
<tr>
<td>LMSI</td>
<td>Location Mobile Station Identity</td>
</tr>
<tr>
<td>LMU</td>
<td>Location Measurement Unit</td>
</tr>
<tr>
<td>LORAN</td>
<td>Long Range Navigation</td>
</tr>
<tr>
<td>LOS</td>
<td>Line of sight</td>
</tr>
<tr>
<td>LPM</td>
<td>Location Process Mode</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobile Application Part</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobile Application Protocol</td>
</tr>
<tr>
<td>MCC</td>
<td>Mobile Country Code</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>MLP</td>
<td>Mobile Location Protocol</td>
</tr>
<tr>
<td>MM</td>
<td>Mobility Management</td>
</tr>
<tr>
<td>MM</td>
<td>Mobility Management</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Message Service</td>
</tr>
<tr>
<td>MNC</td>
<td>Mobile Network Code</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile stations</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Centre</td>
</tr>
<tr>
<td>MSIN</td>
<td>Mobile Subscriber Identification Number</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International ISDN Number</td>
</tr>
<tr>
<td>MSRN</td>
<td>Mobile Station Roaming Number</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Termination</td>
</tr>
<tr>
<td>NCC</td>
<td>Network Colour Code</td>
</tr>
<tr>
<td>NLOS</td>
<td>Non line of sight</td>
</tr>
<tr>
<td>NSS</td>
<td>Network Switching Subsystems</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>OMC</td>
<td>Operations and Maintenance Centre</td>
</tr>
<tr>
<td>OTD</td>
<td>Observed Time different</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RNC</td>
<td>Radio Network Controller</td>
</tr>
<tr>
<td>RR</td>
<td>Radio Resources Protocol</td>
</tr>
<tr>
<td>RTD</td>
<td>Real Time Difference</td>
</tr>
<tr>
<td>SAT</td>
<td>SIM Application Toolkit</td>
</tr>
<tr>
<td>SCH</td>
<td>Synchronization Channel</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SMLC</td>
<td>Serving Mobile Location Centre</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service</td>
</tr>
<tr>
<td>TA</td>
<td>Timing Advance</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time-Division Multiple Access</td>
</tr>
<tr>
<td>TDOA</td>
<td>Time difference of arrival</td>
</tr>
<tr>
<td>TE</td>
<td>Terminal Equipment</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary Mobile Station Identity</td>
</tr>
<tr>
<td>TOA</td>
<td>Time of arrival</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>VLF</td>
<td>Very low frequency</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor Location Register</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 GENERAL INTRODUCTION

One of the examples of a mobile location application is Navigation Systems. Centuries ago people have been developing systems of navigations, mostly for sea transportation. Some of the early navigation systems include measurement of angle above the horizon of the sun and stars to determine latitude. In 13th Century sailors started developing tools like magnetic compass, lead line, Portolan Charts, cross-staff for the navigation purpose. But most of these tools are very inaccurate until introduction of electromagnetic navigation systems in 20th century. There were many accurate navigation systems born in World War II. That includes DECCA, OMEGA and LORAN Navigation systems.

Current navigation systems are based on signals from satellites. Among the satellite based navigation system, GPS or Global Positioning System is the most used system at the moment. GPS is based on 24 satellites and 5 monitoring stations around the world that enable the satellites to broadcast a signal that can be used as a reference in determining the position of users (Johan Hjelm, 2002).

All the mentioned navigation systems use electromagnet waves to measure the distance between the transmitter and the receiver. Similar arrangement of transmitter and receivers are used in mobile phone systems. Therefore if it is possible to use mobile
phone system to locate the user, a new generation of mobile application can be provided to the users. It is obvious by providing such applications in mobile phone, the revenue of mobile phone operators will boost to a greater extend.

It is estimated that total annual revenue potential for all location-based services will be over USD 8 billion dollars per year. Mobile phone subscribers are growing at an average rate of 40% per year in the world. It is estimated that in 10 years the demand for mobility will make wireless technology the primary source for voice communication, with a total market penetration rate of 50-60% (James J. Caffery, Jr, 2000).

As shown in Figure 1.1 & Figure 1.2 in Malaysia mobile phone subscribers are more than half the population with an annual growth rate of 44.06% (Facts & Figures, 2005). Location service for mobile phone is fairly new for Malaysia at the moment. If mobile location service can be introduced, it can be an attractive service and there is a potentially huge market for such service in Malaysia. Service like Short Messaging Service (SMS) has been extremely popular all over the world including Malaysia.

In Malaysia, at the end of 3rd quarter of 2004 there were 6,585.3 million SMS message sent and its 504.93 messages per subscriber. SMS message service had a growth rate of 46.17% at the end of 3rd quarter of 2004 (Facts & Figures, 2005).
Writing SMS using a mobile phone key pad needs lots of patience for the most users. It still has become a very popular service. Service like location service will attract huge amount of potential customers. It is expected that majority of the mobile phone subscribers will subscribe location service if this service is available.
By knowing mobile phone subscribers location, it is possible to use this information in
many location based services. Like

- Public Safety Services
- Location Sensitive Charging
- Tracking Services
- Traffic Monitoring
- Enhanced Call Routing
- Location Based Information Services

There are not many location-dependent services worth the name in the world at the
moment. Among those networks that provide location dependent services, Japan has the
most successfully implemented service providers. Japanese cellular phone service
provider Jphone, has a service that gives the local map of the user position. This is
based on the cell that he/ she is connected. They charge this service USD 25-30 cent
(Johan Hjelm, 2002).

Similar service is provided by the Japanese cellular phone service provider NTT
DoCoMo. They provide this service in their iMode menu as iArea. This service is also
based on the user connected cell and do not imply any modification of either the
network or the mobile telephone. They have four functions at the start: weather forecast
including rain-alert; local guides with shops, restaurants and hotels in maps which
changes as the user moves, Train Connections and Traffic information. Among these
services some of them are free (Johan Hjelm, 2002). Figure 1.3 shows some of the
screens that are available in iMode menu.
The idea of mobile phone was first born in 1947. Since then mobile phone service has grown to majority of the world cities. Mobile phone service is provided in such a way that it requires information from the mobile devices and the network in order for it to work successfully. It is this information that makes it interesting for researchers to explore in order to create other services like location of the mobile users.

One of the driving forces of mobile location service is 1996 US Federal Communications Commission (FCC) ruling requiring that all cellular service providers to provide location information for the support of E-911 safety service (Pi-Chun Chen A, 1999). This requirement from FCC is because of the increase in number of emergency calls placed by mobile telephones. Over 20% of 911 calls were made by wireless users and that one-fourth of those callers could not identify their location (CC Docket No. 94-102, 1997). Even though this statistic was published by the United States, it is believed emergency calls called from mobile phone will be as similar as this in other countries.

Apart from emergency service, location information can be used in developing other services. These services can be developed to generate additional revenue for the
networks. Currently some of the well known hardware manufacturers have started
developing solutions for the location-dependent application using mobile phones. Those
include Nokia's mPosition, TruePosition and Ericsson’s mobile location solution (Nokia
mPosition, 2005; TruePosition, 2005; Ericsson, 2005)

One question that everyone asks is, “Why not we integrate GPS receiver to locate the
location on the mobile user in to the mobile phone”. The answer is that there are lots of
advantages in developing the mobile phone network to locate its user rather than using
GPS receivers in the mobile devices. Here are some of the advantages:

- Most of the time GPS receivers are not suitable for the working environment of
  the mobile phone. Because mobile phone users most of the time operates in

- To get the location information using GPS receivers, users have to on the GPS
device. Mobile phone is always on and users do not need to do any thing to get
the information.

- GPS technology is expensive to build and more complicated than a Mobile
television. Integrating GPS receives with mobile phone will make mobile

- Privacy of GPS device is not guaranteed because GPS system is owned and
controlled by US military. On the other hand Mobile hand phone networks are
built and maintained by companies. Even though degradation of the GPS signal
no longer exists (White House, 2000), there are chances that US military might impose degradation again or stop the service for commercial use.

- When using GPS devices there are no history of the location request recorded. Only the handheld device keep track of where it has been. In Mobile network base location systems the network keeps track of the location of the device. Which means the users can request for the history of their location.

- As its name describes GPS receiver is a receiver. It doesn’t transmit any data. This makes it difficult to monitor, record history and track the GPS receiver remotely. On the other hand mobile hand phone transmit and receive information between the networks.

1.3 RELATED WORKS

Many studies have been done to identify the location of the MS in the network. There were many methods used in identifying the location of the MS. Some of these methods are very accurate but the investments needed to implement these methods are very high. This is because it requires some changes to network and MS itself.

There are basically three method of estimating the location of mobile users (James J. Caffery, Jr 2000; Johan Hjelm, 2002). That is using the time for signal to travel between the sender and receiver, the angle of the signal receiving to the antenna and the signal strength attenuation when traveling between the antennas or path loss. Most commonly researched method is the time based method. This is because it’s the most accurate method. There are many hurdles that have to be to over come in order to successfully
locate the MS location using these methods. Some of the problems include Non-Line of sight (NLoS) and Multipath Propagation.

Pi-Chun Chen A (1999) describes a model that can be used to estimate MS location using Time of arrival (ToA) measurements. In this method NLoS mitigation algorithm and sector information are used on ToA measurements. A Kalman Filter is also proposed in this model in order to make the location of the MS accurate.

Spirito, M.A. & Mattioli (1998, p.173 -177);  Pi-Chun Chen A (1999);  Montse Najar & Josep Vidal (2001) and Montse Najar & Josep Vidal (2003) also proposes Kalman Filters to improve the accuracy of MS location when using Time of arrival or Time difference of arrival (TDoA). Results of these methods do give a very promising results, the accuracy varies between few meter. In order to implement time based methods network or MS needs some changes.

Angle of arrival (AoA) is also another method that has been studied by many researchers. Soren Anderson et al (1991) described a method of using an antenna array. In this method antenna arrays are employed in base station to identify the direction of receiving and transmitting signal. It also describes mathematical models and simulation results. Similar method has been described by Yuan-Hwang & Jiann-Yan (1993) and Shuji Sakagami et al (1992). AoA also suffers from multipath propagation. It is believed that to implement AoA methods the initial investment will be much higher than any other methods because of the hardware changes needed in the network and in the mobile devices.
Karim & Jinane (2003) describes a method using signal strength measurements from seven surrounding base station and comparing these measurements with a database that contains prerecorded signal strengths of each base station in different location around the base station. The result of this is used with a Kalman filter to minimize the location error. Yamamoto et al (2001) proposed an algorithm based on signal measurements. It considers the fluctuation in received signal strength due to shadowing, and obtains probability density function (PDF) of the propagation distance. An overall PDF, obtained by combining the PDF's is used to determine MS location. Xuemin Shen et al (2000) propose a fuzzy inference system with a smoothing device. The computer simulation result of this system demonstrates an improvement in MS location.

Among these three methods, time based method provides the most accurate result. AoA based methods seems to be a distanced solution because of the changes needed in the current mobile network. Signal strength based methods in its row form produce very inaccurate results. But it is possible to get a better result with signal strength after doing additional processing. It is also noted that signal strength based methods are the cheapest solution to implement since it does not require any changes to the network nor mobile device.

1.4 OBJECTIVES OF THE STUDY

Mobile telephone is one of the remarkable technologies that mankind has developed during the last century. It has become part of day to day life, even for an average person.

Development of mobile telephone has passed two generation and we are at the beginning of the third generation. Even though mobile telecommunication has reached
and achieved extraordinary achievements, development of mobile phone based location service has been very slow. There are some reasons for this too. Location based services described in section 1.1 is mainly for the air and sea navigation. Most of the time in such environment the transmitter and receiver has line of sight. Mobile telephone environment is very different than this. Mobile telephone environment is with lots of objects (trees, buildings, people and etc) which obstruct the signal and most of the time line of sight between the transmitter and receiver will not be possible. The other difference is that mobile phone system is not designed for the purpose of locating the users. Bellow states the objectives of this research work:

- To identify a method that will locate the MS with a reasonable accuracy and with a minimum implementation cost. In order to minimize the cost, this research work will concentrate on reducing the changes to the network or to the MS. This is achieved by concentrating on the already available resources in the network and MS to find the MS location.

- This research also intends to develop a model to calculate the MS location and proposes a method to implement location service using already available resources in the system.
1.5 SCOPE OF THE STUDY

In order to achieve the above objectives, the following scope has been identified as the scopes of this research.

- A thorough study of the mobile telephone network (GSM network) and identify the possible sources available in the network that can help in developing a solution.

- Study the possible location technology and methods in the market and identify the advantages and disadvantages in each method.

- Since Mobile telephone system uses electromagnetic waves to communicate, the best candidate to be used in locating MS location is properties of electromagnetic waves. One of the properties which are closely monitored in mobile phone network is the signal strength. For this reason signal strength behaviour in the field is studied in detailed.

- To study the signal strength of the mobile network, collect signal strength and GPS data from the field and compare the location information that can be derived from the signal strength with the GPS location.

- Develop a software tool that can record the signal strength from a hand phone and the GPS location from a GPS receiver attached to a computer.
Based on the collected signal strength measurements from the field and the network information provided by the service provider, this research develop a method to locate the MS location and compare the result of this method with the GPS location.

In order to use this location processing model it is very important to identify a way to implement location service using this model. For this reason this research identifies the tapping point of the system for the information which is needed for this model to work.

This research also proposes a location service implementation method that uses existing mobile infrastructure with minimum changes.

1.6 OUTLINE OF THE THESIS

GSM network being the most popular cellular network represents more than 43% of the total cellular market (Siegmund et al, 1998). Chapter 2 describes a brief description of the GSM network and detail description of its components that can be used in developing location aware service.

In developing a location aware service, it is important to identify the services that can be provided and the techniques that can be used to identify the location of the mobile equipment. There are several methods developed to identify the location of mobile equipments using radio frequencies. In Chapter 3 possible services using location of the users has been discussed together with different techniques in locating mobile equipment in GSM mobile network environment.
Because this research concentrate in developing a solution using the resources available in the network, Chapter 4 discusses in detail the network resources that can be used in developing a solution for locating mobile equipments.

Chapter 5 discusses the mobile location method using the signal strength. In this chapter a thorough study of distance measuring using signal strength will be discussed. This chapter also discusses sources of location error and steps needed to mitigate the impact of each error source.

Chapter 6 discusses aspects of implementing location services in GSM network. Its discussion includes ways to acquire location information from the network and changes to the network. This chapter also proposes a location processing model that can minimize the location error.

In Chapter 7, description of the experiment rig and the measurement techniques used will be outlined.

Results are discussed in Chapter 8 which is obtained from the experiments conducted to identify the accuracy of the proposed location models. Finally in Chapter 9, the thesis is concluded with recommendation for future work.
CHAPTER 2

GSM MOBILE COMMUNICATION NETWORK

2.1 HISTORY

During the early 1980s, analogue cellular telephone systems were experiencing rapid growth in Europe. Each country develops its own system, which was not compatible with each other (Theodore, 2002; Hernando & Perez-Fontan, 1999). Because it was incompatible, each network was limited to its boundaries. These networks were also limited to a limited market and it was not possible to extend their market to other countries.

In early 1982 Conference of European Posts and Telegraphs (CEPT) formed a study group called the Group Special Mobile to study and develop a European public land mobile system. In 1989 GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990 (Theodore, 2002; Hernando & Perez-Fontan, 1999). Commercial service was started in mid 1991 and by 1993 there were 36 GSM networks in 22 countries.

Although standardised in Europe, GSM is not only a European standard. Over 200 GSM networks were operational in 110 countries around the world at the end of 1990’s. In the beginning of 1994, there were 1.3 million subscribers worldwide which had grown to more than 350 million by 2001 (Theodore, 2002).
2.2 ARCHITECTURE OF GSM NETWORK

GSM network consist of several entities, which includes Mobile Station (MS) which is carried by the subscriber, Base Station System (BSS) controls the radio link between the MS and Network Switching Subsystems (NSS). Figure 2.1 shows a generic GSM network.

Figure 2.1 General architecture of a GSM network
2.2.1 Mobile Station (MS)

Mobile station consists of the physical equipment used by a Public Land Mobile Network (PLMN) subscriber; it comprises the Mobile Equipment (ME) and the Subscriber Identity Module (SIM). The ME comprises the Mobile Termination (MT) and Terminal Equipment (TE) (ETS GSM 03.02, 1996). Each ME is uniquely defined by the International Mobile Equipment Identity (IMEI) which is 15 digits long (ETS GSM 03.03, 1995). SIM provide the subscribers identification so that user can get the subscribed services irrespective of a specific terminal. The SIM card contains the International Mobile Subscriber Identity (IMSI), a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility.

2.2.2 Base Station System (BSS)

The Base Station System (BSS) is the system of base station equipment which is viewed by the Mobile Switching Centre (MSC) through a single A-interface. BSS is responsible for communication with Mobile Station in a certain area. The radio equipment of a BSS supports one or more cells. A BSS may consist of one or more base stations controller and one or more Base Transceiver Stations (BTS), where an Abis-interface is implemented (ETS GSM 03.02, 1996). The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers.
2.2.3 Network Switching Subsystems (NSS)

One of the main components of Network Switching Subsystem is Mobile Switching Centre (MSC). It acts like a switch node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber (ETS GSM 03.02, 1996).

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. Home Location Register is a database in charge of the management of the mobile subscribers (ETS GSM 03.02, 1996). A PLMN contain one or several HLRs depending on the number of mobile subscribers.

Two kind of information are stored in HLR they are: the subscription information, some location information enabling the charging and routing of call towards the MSC where the MS is located (eg: MS Roaming Number, VLR address, MSC address, Local MS Identity) (ETS GSM 03.02, 1996). HRL holds two number for each mobile subscription they are International Mobile Station Identity (IMSI) and Mobile Station International ISDN Number(s) (MSISDN).

Visitor Location Register (VLR) is a database that holds information about the MS location. When MS moves from one Location Area (LA) to another, MSC in charge of that particular area notice the VLR and register this information (ETS GSM 03.02, 1996). A mobile station roaming in a MSC area is controlled by the VLR in charge of this area. A VLR may be in charge of one or several MSC area. VLR also contains
information needed to handle the call set-up or received by the MSs registered in its database. The following elements are included in VLR: International Mobile Subscriber Identity (IMSI), Mobile Station International ISDN number (MSISDN), Mobile Station Roaming Number (MSRN), Temporary Mobile Station Identity (TMSI), Location Mobile Station Identity (LMSI) and Location area where the mobile station has been registered (ETS GSM 03.02, 1996).

The Authentication Centre (AuC) is associated with HLR, and store an identity key for each mobile subscriber registered with the associate HLR. AuC communicates only with its associated HLR over an interface denoted the H-interface (ETS GSM 03.02, 1996).

2.2.4 Cell and Location Area (LA)

In GSM Cell, Location Area and Service area have different meaning. Cell is the area which is covered by a particular base station. Location Area (LA) is defined as an area in which a mobile station may move freely without updating the location register (ETS GSM 03.02, 1996).

Figure 2.2 Cell Configuration within a location area.
In GSM the cell arrangement has an umbrella approach as shown in Figure 2.2. Use of small cell within one large cell operating in different frequency is typical cell arrangement in GSM networks. Most of the traffic load will be taken by the smaller cells and the bigger cell will be used to cover the “Holes” in between the smaller cells. Different cell type can have different coverage dimension (Siegmund et al, 1998). Table 2.1 shows the coverage dimension for each type of cell.

<table>
<thead>
<tr>
<th>Cell Type</th>
<th>Antenna Location</th>
<th>Cell Dimension (km)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large macrocell</td>
<td>Above rooftop level</td>
<td>3-30</td>
</tr>
<tr>
<td>Small macrocell</td>
<td>Above rooftop level</td>
<td>1-3</td>
</tr>
<tr>
<td>Microcell</td>
<td>Below or about rooftop level</td>
<td>0.1-1</td>
</tr>
<tr>
<td>Picocell</td>
<td>Below rooftop level</td>
<td>0.01-1</td>
</tr>
<tr>
<td>Nanocell</td>
<td>Below rooftop level</td>
<td>0.01-0.001</td>
</tr>
</tbody>
</table>

Each cell is allocated with a predetermined set of frequencies from the cellular frequency band. The allocation is typically made in accordance with a certain frequency plan. Because only a limited number of frequencies are available in the cellular frequency band, the same frequencies that are allocated to one cell are also allocated to (reused by) other cells in distant parts of the service area. Adjacent cells are not allocated to use the same frequency by the frequency plan. The power levels of the signal transmissions on any given frequency are limited in strength, this is to limit propagation beyond the cell area. For frequency planning process, software tools are used for predicting each frequency and the interference resulting from concurrent use of that frequency by other cells. The interference predictions made by the frequency planning software tools rely on certain wave propagation models and other theoretical considerations (Theodore, 2002).
2.2.5 Addressing and identification

In GSM specification there are number of different addressing and identification specified (ETS GSM 03.03, 1995). Therefore it is necessary to learn about the addressing since it will help in identifying the MS and its location.

2.2.5.1 Identification of mobile subscriber

A unique International Mobile Subscriber Identity (IMSI) is given to each mobile subscriber in the GSM network. This identification number is 15 digits long and consists of numeric characters (0 to 9). This number contains: Three digits of Mobile Country Code (MCC), two digits of Mobile Network Code (MNC) and Mobile Subscriber Identification Number (MSIN) (ETS GSM 03.03, 1995).

MCC identifies uniquely the country of the mobile subscriber. The MNC identifies the home GSM Public Land Mobile Network (PLMN) of the mobile subscriber. Each and every network in the country is given a unique identification number in GSM that is the MNC code. Allocation of Mobile Subscriber Identification Number (MSIN) depends on the individual network. Nation Mobile Subscribers Identity is MNC + MSIN (ETS GSM 03.03, 1995). Figure 2.3 shows the structure of Mobile Subscriber Identification Number.
2.2.5.2 Identification of location area and base station.

Location Area Identification (LAI) consists of MCC, MNC and Location Area Code (LAC). MCC and MNC are same as the three and two digit codes used in IMSI. LAC is a fixed length code of 2 Octets identifying a location area within a GSM network. As shown in Figure 2.4 Cell Global Identification (CGI) consists of Location Area Identification and the Cell Identity (CI). CI is of fixed length with 2 octets and it can be coded using a full Hexadecimal representation (ETS GSM 03.03, 1995).

Base Station Identity Code (BSIC) comprises of Network Colour Code (NCC) and Base Station Colour Code (BCC) which has a 3 bit in each. Figure 2.5 shows the structure of BSIC. BSIC is a local colour code a mobile station uses to distinguish between different neighbouring base stations. Each cell has an allocated BSIC, in each burst BSIC will be broadcasted on the Synchronisation Channel (SCH). BSIC are used to avoid ambiguity.
or interference which can arise when a mobile station in a given position can receive two cells using the same Broadcast Control Channel (BCCH) frequency. The BCCs of each base station is assigned by the network operator, and it’s assigned such that no neighbour stations have equal BCC and thus equal BSIC. Figure 2.5 shows the structure of BSIC (ETS GSM 03.03, 1995).

![Figure 2.5 Structure of Base Station Identity Code (BSIC)](image)

BSIC is a value between 0 to 63 and for each cell a BSIC is allocated. In each cell its BSIC is broadcasted in every burst. When in idle mode, the mobile station identifies a cell according to the cell identity broadcast on the BCCH and not by BSCI (ETS GSM 03.03, 1995).

### 2.2.6 The radio link interface

The International Telecommunication Union (ITU) allocated the bands 890-915 MHz for the uplink and 935-960 MHz for the downlink for mobile networks. Radio interface in GSM uses a combination of Time-Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA). FDMA divides the frequency by 25MHz in to 124 carrier frequencies with a guard band of 200 kHz. Each of these carrier frequencies are divided in to time slots by TDMA and one or more frequencies are assigned to each base stations (George Aggelou, 2005; Hernando & Perez-Fontan, 1999).
Since the TDMA is used in communication between MS and BTS, MS has to be synchronised to the current servicing cell. In order to achieve this, BS sends to each MS a “Timing Advance (TA)” parameter according to the perceived round trip propagation delay BS-MS-BS. From the TA value received from the BS, the MS knows when to send the frame, so that it can arrive at the BS in synchronised form. The values of the TA is continuously calculated and transmitted to the MS. The resolution is one GSM bit, which has the duration of 48/13 μs. This is the round trip propagation delay from BS-MS-BS. Therefore one way propagation is defined as (48/13)/2 = 1.846 μs. The Timing Advance value is a value between 0-63 (ETS GSM 05.10, 1996; Henry, 2000).

2.2.7 Protocol and signalling

As in other networks, GSM networks use signalling protocols between MS, BSS and MSC. Therefore it is important to understand the protocol in order to develop Mobile Location Service. A GSM mobile can seamlessly roam nationally and internationally, which requires that registration, authentication, call routing and location updating functions. These functions are handled by the handover mechanism. Handover functions are performed by the Network Subsystem, mainly using the Mobile Application Part (MAP) built on top of the Signalling System No. 7 protocol (ETS GSM 80.08, 1998). Figure 2.6 shows the basic structure of GSM signalling protocol.
Radio Resources Protocol (RR) deals with the allocation, un-allocation and parameters of the radio-channel and is crucial in the setup of all communication with the MS. Above this is Mobility Management (MM) and Circuit Mode Connection (CM). The MM deals with handover and CM deals with setup and termination of calls. Other protocols used between different entities in the network are BTS Management protocol (BTSM) across the Abis interface and the BSSAP (BSS Application Part) across the A interface (ETS GSM 80.08, 1998).

All the function of signalling uses mobile application protocol (MAP). MAP is defined in ETS GSM 09.02 (1997) and contains 1067 pages. It includes all the function required for GSM to be compatible with all the other external networks.

**2.2.8 Handover**

Mobile Station is a mobile device that will be moving from one BS to another. Handover is the term used to switch ongoing call from one channel to another channel or switch calls from one cell to another cell. There are four different handovers.
• Channels (time slots) in the same cell,
• Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
• Cells under the control of different BSCs, but belonging to the same Mobile services Switching Centre (MSC), and
• Cells under the control of different MSCs.

First two type of handover is called internal handover. In this kind of handover there will not be any MSC involvement. Internal handover occurs between channels on the same cell or between channels pertaining to different cell of the same BSS. It is decided and executed autonomously by the BSS, so that no message is generated at the BSS-MSC interface, until the completion of the handover execution (ETS GSM 80.08, 1998). In Internal Intra-Cell handover, if the handover measurements show a low Received Signal Quality (RXQUAL) it will handover the call from one channel/timeslot in the servicing cell to another channel/timeslot in the same cell. Main reason for such a handover is because of the poor signal quality of the interference. Internal inter-cell handover can occur either to a timeslot on a new carrier or to a different timeslot on the same carrier (ETS GSM 05.08, 1997).

In the last two types of handovers the MSC will be involved. This type of handover is called External handover or Inter MSC handover. At any given time during a call MS will be measuring the signal quality from 16 different neighbouring cells. Among that 16, the best 7 Cell identity (BSIC) will be transmitted back to the network. This information will be passed to BSC and MSC for handover decision at least once each and every second (ETS GSM 05.08, 1997).
CHAPTER 3

MOBILE LOCATION SERVICE

3.1 INTRODUCTION

The idea of locating mobile users using GSM mobile hand sets seems to be very new but location service has been around for decades. First location service was targeted to sea navigation and the next generation of location services was targeted for sea and air navigation. It was very recently location services were developed targeting land navigation. One of the most successful and efficient sea, air and land location service developed was GPS system developed by U.S military (James J. Caffery, Jr 2000).

Location service using mobile hand phone network is still very new and emerging technology. There are several advantages of using mobile hand phone signals for location services. Navigation service is only one application among many location based service that can be developed using mobile hand phone network.

3.2 LOCATION BASED SERVICES

Here are some of the possible location based services that can be implemented using mobile hand phone users location:

- Public Safety Services
- Location Based Charging
- Tracking Services
• Enhanced Call Routing
• Location Dependent Content Broadcast
• Mobile Yellow Pages
• Location Based Information Services

3.2.1 Public Safety Services

Location information can be used for the safety of the public. This kind of services can be categorised as Emergency Services and Emergency Alert Services.

3.2.1.1 Emergency Services

Location of the mobile hand phone users can be used in search and rescue operation. In case of emergency, the emergency service providers can trace back the caller location and coordinates the rescuer operation more effectively and faster. United States E-911 can be taken as an example. It requires all networks to facilitate locating emergency callers for search and rescue (CC Docket No. 94-102, 1997). Location of the user can be provided directly from the network to the emergency departments to rescue the people in need.

3.2.1.2 Emergency Alert Services

Emergency Alert Services may be enabled to notify wireless subscribers within a specific geographic location or geographic area of emergency alerts. This may include such alerts as tornado warnings, pending volcano eruptions, tsunami alert, etc. This is a service that can be implemented easily since it does not require pinpoint accuracy. Since
most of these emergencies affect huge areas, location of the users can be located within hundreds of meters.

3.2.2 Location Based Charging

Location Based Charging allows a subscriber to be charged different rates depending on the subscriber's location or geographic zone, or changes in location or zone.

For example, when the mobile user uses the hand phone at home, the mobile call charges can be reduced to the same price as the house fixed line charges. This will encourage the mobile users to use mobile phone instead of house phone.

3.2.3 Fleet and Asset Management Services

Fleet and Asset Management services allow the tracking of location and status of specific service group users. Examples may include a supervisor of a taxi service who needs to know the location and status of taxis, parents who need to know where their children are, animal tracking, and tracking of assets.

3.2.4 Location Based Information Services

This type of location can also be categorised as two different services. They are: Navigation, City Sightseeing.
3.2.4.1 **Navigation**

The purpose of the navigation application is to guide the handset user to his/her destination. The destination can be input to the terminal, which gives guidance how to reach the destination. The guidance information can be e.g. plain text, symbols with text information or symbols on the map display.

3.2.4.2 **City Sightseeing**

City Sightseeing would enable the delivery of location specific information to a sightseer. Such information might consist of combinations of the historical sites, providing navigation directions between sites, facilitate finding the nearest restaurant, bank, airport, bus terminal, restroom facility, etc.

3.2.5 **Location Dependent Content Broadcast**

The main characteristic of this service is that the network automatically broadcasts information to terminals in a certain geographical area. An example of such a service may be localized advertising. A detail description of location based advertising is found in (Yunos et al, 2003 p.30-37)

3.3 **MOBILE LOCATION TECHNIQUES**

Heart of mobile location problem is finding a location technology to calculate the precise location of the mobile devices. Since the medium of communication in mobile devices are radio signals which is unguided and have no control over the signal after it
gets transmitted. There are several factors that can affect the accuracy of the location technologies like Multipath Propagation, Non-Line of Site (NLoS) propagation and many more. In-depth studies of factors that affect the accuracy of the location are discussed in Chapter 5.

Computing the distance that the signal travels in a guided medium like wire can be easier than computing the distance that the radio signal travels after its been transmitted. The other problem is the direction that it travels to reach the destination. When the radio signal gets transmitted, it does not travel in a selected path like in wire. Most of the time it gets transmitted to a very large area, among those signals some will reach its destination and some does not. In mobile radio system it is the signal and its property that can be used to calculate the distance from the source and destination. In mobile radio location it attempts to locate the MS by measuring the radio signal travelling between the MS and a set of fixed stations. There are three fundamental types of radiolocation systems: those based on signal strength, Angle measurements, Time measurements and GPS based measurements (James J. Caffery, Jr 2000).

Each type of radiolocation method has to measure the signal very accurately in order to achieve reasonable position information. Even if the signal strength is measured with very little error in signal strength or angle of the signal or the propagation time, the final outcome of the location information might result in hundreds of meters of error. For example the radio wave travels in light speed (300,000 kilometre per second) through air (ETS GSM 03.03, 1995). At this speed an error of one millionth of a second will result in an error of 300 meter.
In order to achieve high accuracy in location estimation it is necessary that line-of-sight (LoS) paths exist between the MS and the BSs that are utilized in the location process. Locating a MS in two-dimension requires a minimum of three BSs in order to resolve ambiguities arising from multiple crossings of the lines of position (James J. Caffery, Jr 2000).

Apart from the above mentioned radiolocation systems, there are few other methods to locate the mobile users in a GSM system. They are by using Cell Identity (CI) or Cell Global Identification (CGI) together with Timing Advance (TA). The key purpose of this research is to find the MS location using an inexpensive way. By using the signal properties like angle of arrive or time, the investment in implementing such systems are very high due to the changes to the system. If the time based radiolocation technology is used, the hardware cost of MS or the whole system will increase. If the angle of arrival is used, the hardware cost of the base station will increase because an adaptive array antenna is needed to measure the angle of arrival (Yamamoto et al, 2001). On the other hand the signal strength or CGI together with TA will minimise the implementation cost since these measurements are already available in the system. The only disadvantages in using these measurements over the angle and time measurement is that the angle and time measurements can give much more accurate MS location than signal strength and TA measurements.
3.4 TYPE OF RADIO LOCATION SYSTEMS

3.4.1 Network information based

3.4.1.1 Using CI / CGI and TA for MS Location

GSM network allocate identification codes for Cell, Base Stations and Location Area which are parts of Cell Global Identity (CGI). CGI consist of Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC) and Cell Identity (CI). All four parts of CGI can be used to locate the MS with a level of accuracy.

If CGI is used as the mean of locating MS, CI can be used in identifying the servicing area of the particular Cell. Operators know where their antennas or BS are located geographically. By using their cell coverage database it will be possible to locate the BS servicing the MS at any given time. The accuracy of this type of locating depends on the Cell size.

To improve the accuracy of this type of location Cell sectors can be used. Normally in cell arrangement there is more than one antenna radiating different direction. Separate antennas radiate in different direction around the base station to cover the full circle around it. Therefore if the antenna that the MS is connected is known then it will be possible to narrow down the MS location to one sector of the cell coverage area.

The other thing that can be used to improve the accuracy of this method is the Timing Advance (TA). Timing advance is a number between 0-63. Since the TA defined as 1.846 milliseconds which is 554 meter (ETS GSM 03.03, 1995), by multiplying the TA value by 554 we can estimate the distance between the MS and BTS. If the TA value is used together with the Cell sector it will be possible to narrow down the sector to a
narrow band of 554 meter width in the selected sector. Figure 3.1 shows how MS can be located using CI, Cell sector and TA.

Since CGI and TA values are available in the network, this location method does not need any modification of mobile phone or network. Therefore this method will support all the current handsets and the roaming subscribers. Currently this method is been used in different applications by different network operators (like Jphone and NTT DoCoMo Japan) (Johan Hjelm, 2002).

3.4.2 Signal strength based

Signal strength or power level from servicing and neighbouring cell can be used to calculate the distance between the MS and the each neighbouring BS. Since the signal strength measurement represent a distance between MS and BS, the MS must lie on a circle centered at the BS. By using multiple BS the location of MS can be calculated. The intersection of circles from multiple BS will give the MS location. Figure 3.2 shows how MS can be located using the signal strength measurements from multiple BS.
Chapter 3, Methods of Mobile Positioning

3.4.2 Range-based signal strength location method

For this method accurate BS location has to be known, at least within 10 meters. The distance calculated using propagation model for each BS can be used in triangulating MS location. The precision of this method varies with the cell density. This method is expected to give more accurate location than Cell ID and TA.

This method can also be implemented without any major investment since signal strength from servicing and neighbouring cells are always available in GSM network. GSM system transmits this information about the signal in each and every timeslot using BCCH carrier (ETS GSM 05.08, 1997). Each timeslot is 0.577 milliseconds (Hernando & Perez-Fontan, 1999).

3.4.3 Angle of arrival based

Angle of Arrival (AoA) or Direction of Arrival is a method that uses the angle of the signal arriving to the MS from different BS or vice versa. This is achieved by using antenna arrays (Krizman et al, 1997 p.919-923; Lopes et al, 1999 p.1-7). In mobile radio systems, the antenna arrays are typically located only at the BSs, since it is difficult to

Figure 3.2 The geometry of the rang-based signal strength location method
place an array in a MS handset (James J. Caffery, Jr 2000). The biggest advantage in this method is that the MS location can be calculated using the measurement from two BS. After measuring the angle of the signal arriving to each BS, a line can be drawn to meet each other to identify the location of the MS. The figure 3.3 illustrates the AoA method.

![Figure 3.3 The angle of arrival method for MS location. The line of position are straight lines whose intersection provides the location of MS.](image)

A simple geometric relation can be used in the angles detected from both BS to find the MS location. The method described by Shuji Sakagami, et al (1992) can be one simple solution for AoA method. Problem with this method is the angle measurements. A slight error in measuring the angle will cause a big error in MS location. For example an error of 3° with a MS which is 200 meters away will give an error of 10 meter but if the MS is 1000 meters away the MS will be located 52 meters away from the actual point. This means a slight miscalculation in AoA will give a big error.
3.4.4 Time based

This type of position involves measuring the time that the signal takes to travel from source to destination or time it takes to travel to destination and returning back to source. Since the radio signal travels at the speed of light (300,000 kilometres per second) the timing mechanism in either source and destination or both has to be very perfect. At this speed an error of a millisecond can’t be ignored since in one millisecond, signal can travel 300 meters. All the time based methods also suffers from multipath fading and NLoS propagation. But Time based methods suffers lesser than the others. This is because of the speed of the signal, even though the signal reflects and diffract it does not get slowed, though it takes a bit longer time to reach the BS.

3.4.4.1 Uplink Time of Arrival (TOA)

In this method, signal from MS are detected in multiple BS. Propagation delay of the signal is calculated in each BS, this information is used in estimating the MS location using triangulation. Like in signal strength ToA measurement will provide a circle, centred at the BS, on which MS must lie (Estrada, et al, 1999 p.1166-1171). Figure 3.3 illustrates this method. In this method an additional hardware called Location Measurement Unit (LMU) is used to handle the ToA measurement in each BS. When an application request for location measurement the MS is forced to perform an asynchronous hand over. Under such circumstances, the MS is transmitting up 70 access burst (ETS GSM 03.71, 1998). The ToA measurements from LMUs are sent to a new network entity called Serving Mobile Location Centre (SMLC) for the location calculation. The SMLC utilizes the ToA measurements in combination with information about the coordinates of the measurement units and the Real Time Difference (RTD)
values to produce a position estimate. The SMLC delivers the position estimate together with an uncertainty estimate to the application (ETS GSM 03.71, 1998). This method does not require changes in existing handsets, therefore it works well with the current handsets. Only changes that has to be made is on network side.

The problem with this method is that all the LMUs and the MS must share a common clock reference with each other. There is a capacity limit because several receivers must be assigned simultaneously. The more traffic there is on the network, the lower the performance (mainly because of interference). Positioning itself creates interferences by the positioning request and the forced handover. This problem may not arise if this method is going to be used for services like emergency services alone. But if this system is going to be used for services like root guidance then it will overload the network. For example if one thousand tourists are making positioning request every few minutes, the network will get overloaded with handovers.

### 3.4.4.2 Time Differences of Arrival (TDoA)

TDoA are calculated by calculating the time difference of arrival of the signal to two different BS from MS. This measurement will give a hyperbola. This hyperbola is a curve of constant time difference of arrival from two BSs. The lines of position are given by hyperbolas which foci at the BSs on which the MS must lie. Figure 3.4 shows the TDoA method.
The branch of the hyperbolas chosen for the lines of position is determined from the sign of the TDoA measurement. If the sign is negative, the hyperbola branch furthest from the BS with respect to which the TDoA measurement was made, will be chosen. If it is positive, the branch nearest the reference BS is chosen (James J. Caffery, Jr 2000).

In this method all the BSs has to have a common time reference but MS need not refer the same time reference. The timing reference for the BS can be achieved by using a GPS receiver or a LMU unit. This device can be installed in all the BS or it can be in a fixed position so that the BS can refer it (Johan Hjelm, 2002; James J. Caffery, Jr 2000).

This method can be implemented in the current GSM networks. In GSM networks for pseudo Synchronised Handover, the system maintains the record of Observed Time difference (OTD) which is denoted as the time difference of two BS as measured by MS and values for Real Time Difference (RTD) which is the value of the local time in one BS minus that of the other BS. These two values are used in handover decision and get updated in every bit period. Pseudo Synchronisation is optional in GSM networks.
These two values can be used to calculate the TDoA by using the method introduced in (Spirito, M.A. & Mattioli, 1998).

3.4.4.3 **Enhanced Observed Time Difference (E-OTD)**

Unlike other time based methods E-OTD is a MS based method. This means the current handsets can’t be used if this method is implemented. In this method handsets should be capable of making E-OTD measurements. MS calculates the position itself using the assisted data from the network, the position information can then be send to the SMLC using a special LCS signal. Even in this method the network has to be synchronised, this can be achieved by installing LMUs in every BS or in a fixed place for all the BSs to refer.

For MS to compute the position, each BS has to provide its geographical location information. This method can also be implemented in current GSM network but need some changes in the MS handsets (James J. Caffery, Jr 2000). Figure 3.5 shows E-OTD method.

![Figure 3.5 E-OTD Implementation](image-url)
3.4.5 GPS Based Positioning

GPS or Global Positioning System was developed by the United States Government for its military. GPS is based on 24 satellites and 5 monitoring station around the world. The satellites are position to cover entire earth surface and at any given point on the earth surface there will be five satellites in view.

Until May 2000 the GPS signal was degraded for the civilian use. Originally, GPS was provided with 1.5 meter accuracy for military use and 50 meter for civilians. This was done by using signal encoding and only the U.S military has the key to decode it. On May 2000 President Clinton announced that U.S will stop the international degradation of the GPS signals available to the public beginning at midnight. Actual release of degrading of GPS signal was schedule for 2006 (White House, 2000).

Start up of GPS system is bit slow because the receiver does not know where it is when it starts measuring, it has to search for satellite signals first before it provides any location information. Unless the receiver has an almanac, it takes approximately 12 minutes to provide location. If receiver is equipped with almanac it takes 15 seconds to 2 minutes (Johan Hjelm, 2002).

3.4.5.1 Assisted GPS (A-GPS)

Like E-OTD this method is also fully handset based method. Adding GPS receiver to handsets will have a big impact on handsets hardware and software. On the other hand the network has a very low impact. Only support of a SMLC is needed on network side.
As mentioned in previous section GPS takes 12 minute to 15 second to get position information. When using mobile phone even 15 second seems to be too long to a mobile user and two minute will be unacceptable. Normally GPS receivers come with all the necessary information about the satellite and it has the capability of processing location information. The problem with this is that it will consume lots of battery life and can be expensive. When GPS receivers are asked to give position information it scans all the satellite and find out the best satellite to use in position calculation.

In A-GPS when the mobile is asked for position information the network can give the satellite information that can be used in positioning. This can be done by identifying the Cell the mobile is in and finding the satellite that are best viewed by that cell coverage area. By providing the satellite information the receiver need not look for any other satellite, it can straight use the satellite that are suggested by the network for the position calculation. This will definitely speed up the processes and can save the battery power. This will also help in developing small GPS receivers that can be fitted in a mobile phone. Figure 3.6 shows the A-GPS method.

Figure 3.6 A-GPS Implementation
The advantage in this method is that it can be very accurate especially when the degradation of the GPS signal has been removed. The other thing is that it needs only one BS instead of three BS.

The problem with this system is that it will be expensive to implement GPS receiver in mobile handsets. A-GPS gives very high accurate positioning information in open area but it performs very badly indoor. This is because GPS receivers need to have direct link with the satellite in order to calculate the position information.

### 3.5 CONCLUDING REMARKS

Each and every method discussed above has its advantages and disadvantages. To implement Network information based method there is not much work to do. This is because this information is already available in the system but it is designed for the network operation purposes and not for locating its users. For this reason the location information that can be generated using this information will be very in accurate and do not have much option to improve the accuracy using this information. But because the investment of implementing location service using this method is not much compared to other methods, we can see some applications in the current market using this method for example Maxis and DiGi’s Friend Finder service.

Similar to network information based method signal strength measurement information is also recorded in the system. This measurement in its row form does not make much difference in locating MS. But this information when processed, it improves location of MS very much when compared to network information method. This method also requires minimum investment because it does not require any changes to the network or
to the hand phone. Location service using this method can provide location service to
new and old hand phones.

As mentioned above, AOA based method is the most expensive method. This is because
it requires major hardware changes to network. Even though it requires only two BS to
locate a MS, it requires MS and BS to have line of sight. If both MS and BS have a line
of sight, accuracy of MS location is very much accurate compared to any other method.
But because most of the time MS and BS does not have a line of sight, this method
performs very poorly and can be considered in appropriate unless a better solution is
developed using this method.

Time based methods can be considered the best method when developing location
service but it definitely is not the cheapest method. Time based methods have the
advantage of signal travelling speed. The disadvantage of time based method is that it
requires changes to network or both network and hand phone which will result in a
higher investment.

Assisted GPS method is a better solution than implementing GPS in the hand phone.
Even though there are hand phones in current market with GPS receiver, it dose not
work together with the hand phone network. Instead it work as a standalone GPS
receiver. As mentioned above implementing GPS in hand phone will result in expensive
hand phone and hand phone battery used by the GPS. For this reason implementing
GPS in the hand phone does not seems to be a solution.
A-GPS can be a good positioning method but because it performs poorly in indoor and mobile handsets are usually used in indoor, even if this method is implemented, it has to be implemented together with another method which performs well in indoor.

Among all the above methods, Cell ID is the only method that is 100% error free. This is because the GSM handset always knows the cell that it is communicating and the network operators know where their BSs are. If in case of any failure of the positioning method, the position on the MS will fall back to Cell ID level.
CHAPTER 4

NETWORK INFORMATION BASED POSITIONING METHODS

4.1 INTRODUCTION

The most economic way of implementing the location service is to use what is available in the mobile network. For the operation of mobile network, it maintains network and its subscriber’s information.

The purpose of this information was not initially designed for the purpose of locating the MS accurately. This information was used in the operation of the network. Therefore it has to be processed in order to make the MS location accurate. Each of this information can give the location of MS with certain accuracy but cannot be used to generate pinpoint location information. Below is some of the information from the network that can be used to identify the location of the MS.

- Mobile Country Code (MCC)
- Location Area Code (LAC)
- Cell Identity (CI)
- Timing Advance (TA)
- Observed Time Difference (OTD)
MCC is used to identify the country that the mobile is in. LAC identifies an area of the network. Most of the time LAC covers a huge area like a state or a part of a state. CI identifies the Cell that is been servicing the mobile. Location of the mobile depends on the type of the cell [Table 2.1]. TA identifies the distance of the mobile from the cell. The distance identified using TA is a range and it is identified within 550 meter range.

Even though the above mentioned information from the network identifies the location of the mobile, it is not accurate enough to be used in a commercial location dependent application. In order to keep the investment of implementing the location service low, it will be important to identify the information from the network that can be used in processing reasonable location information.

MCC, LAC identifies a very huge area and it cannot be processed to produce the location information any accurate than it does. Cell ID gives a better result than MCC and LAC. Cell ID based location depends on the Cell Type but Cell ID and TA together will give a better result. Therefore in this chapter Cell ID and TA will be discussed in detail.

### 4.2 CELL

The Cell is an area of radio coverage identified by a base station. In cellular networks, in order to increase the frequency reuse each cell is sectored and each cell sector uses different frequency. This is achieved by using directional antennas. When sectoring is employed, the channels used in a particular cell are broken down to sector groups and are used only within a particular sector (Theodore, 2002; Henry, 2000). A cell is
normally partitioned in to three 120° sectors or six 60° sectors as shown in Figure 4.1 and Figure 4.2.

![Figure 4.1 (a) 60° Sectoring; (b) 120° Sectoring](image)

4.2.1 Cell identity

In GSM network, two identification codes are used in identifying the cell. Base Station Identify Code (BSIC) identifies the base station or the Cell and Cell Identity (CI) identifies the antenna of the Cell, none of these two repeats in the network within a local area.
Even on idle mode CI, BSIC and LA of the MS parked cell will be transmitted in BCCH carrier (ETS GSM 05.08, 1997). In idle mode MS monitors the BCCH carriers and decode the BA list (BCCH Allocation list) from the servicing cell and monitor the frequencies listed in the BA list. The BCCH allocation is the list of BCCH carriers in use by a given PLMN in a given geographical area. It indicates the RF channels that have to be monitored by MS while camped on a cell (ETS GSM 03.22, 1997).

Using this BA list MS will measure the signal strength of each frequency and identifies the strongest six cells and report the readings back to the network for hand over decision. BA list does not contain the BSIC of the neighbouring BS that uses the frequency. Therefore in idle mode it is not possible to identify the neighbouring BSS that uses the frequency listed in BA.

In connection mode there is another BCCH carrier list, called BA (SACCH), which is sent on the SACCH. This also contains the list of BCCH carriers to be monitored by the MS for hand over purposes. This information is also not enough to uniquely identify the surrounding cells therefore in connection mode MS synchronise and demodulate surrounding BCCH carriers and identify the BSIC (ETS GSM 03.22, 1997). Even though MS identifies BSIC of the neighbouring BSS in connection mode it does not identify the CI.

By identifying neighbouring BS it does not give an advantage in finding the MS location but if it is possible to identify the CI of the neighbouring cells, it can be used to narrow down the location of the MS.
It is possible to identify the neighbouring CI from the frequency information provided by BCCH and SACCH. Since no neighbouring cells use the same frequency, frequency can be used to identify the cell and its ID. This can be done by referring the information from the network service provider database of frequencies. Even in the cases of cell having frequency hopping implemented, it will not have any effect in identifying the cell since frequency hopping is implemented among the different frequencies within a single cell.

### 4.2.2 Using Cell Identity and Cell Sector to locate Mobile Stations

As discussed above CI, BSIC and LA of the servicing cell is available to the MS at any given time (including idle time). This information can be used in identifying mobile location. Mobile location based on this method will depend on the cell size. By using this information location of the Cell can be identified. Operator’s maintains database of network information. Some of the information that is recorded includes geographical location of the BS, Cell Sector coverage angle for each antenna (Sector Size) and its azimuth. This information can be used to narrow down the MS location from the entire cell site to just one sector of the cell site. Figure 4.3 shows the basic concept of using the CI and cell sector information to narrow down the MS location.

In case of omni-directional antennas, cell sector method will not be applicable since it is one single antenna that covers 360°. In such cases this method can locate MS within the whole cell coverage area.
Cell sector information may not give better location information but it can limit the scope of the location information to just one sector of the cell. Though it does identify the MS within a huge area, it still can be used in some of the location based services like Location Based Charging, Weather reports, Traffic information, Local news, and Prayer time for Muslims.

Accuracy of this method can vary between the cell sizes. It is expected that this method will give better accurate information in urban area than in rural area because of the size of the cell in urban area is smaller compared with rural area.

Cell ID is the only guaranteed location method that will not fail. Even though the accuracy of Cell ID method is low, it will be always available even all the other methods fails to locate the MS, making it the last resource when all the other means of location method fails.

### 4.3 TIMING ADVANCE

This is a method used in order to get the TDMA scheme to work. In TDMA schemes all the time frames from MS’s connect to BS should reach BS in sequence. For this MS must be synchronised when received by the BTS. This synchronisation is done by the

---

**Figure 4.3 Sectored Cells**

A. Cell site

B. Sectored cell

50m – 30km

Cell Sector Size

Azimuth
concept of Timing Advance. The degree of synchronization is measured by the base station on the uplink, by checking the position of the TSC (Training Sequence Code). A 26 bit training sequence is sent in the middle of each burst which is used by the receiver to synchronise and estimate the propagation characteristics. Training sequence is mandatory in all frames transmitted from the mobile. From these measurements, the base station calculates the TA and sends this information to the mobile (ETS GSM 05.08, 1997).

TA value is a value between 0 to 63 (Henry, 2000) which mean that the actual distance represented by TA is between 550 meters to 35 kilometres. TA value is always available for the servicing BS that is even during the idle mode.

### 4.3.1 Using Timing Advance to locate Mobile Stations

TA can be used to calculate the location of the MS within a band of 550 meter around the BS. When TA is used together with the Cell sector, the 550 meter band around the BS can narrow down to one sector of the Cell site. Figure 4.4 demonstrate the use of TA together with CI and cell sector.

![Figure 4.4 TA and Cell Sector method used in positioning MS](image)

In calculating TA, BS uses first arrived propagation path (ETS GSM 03.03, 1995). Therefore we can assume that the TA calculation is most of the time for the line of sight
path or the path closed to the line of sight path. Since TA value represents distance between MS and BS, the distance \( d \) is:

\[
550(TA - 0.5) \leq d \leq 550(TA + 0.5)
\]

As mentioned above TA value can be obtained only for the servicing BS. But if it is possible to get the TA value of the neighbouring BS, it will be possible to reduce the position identified by the TA to just a 550 meter band around the BS for each BS. The area common to all TA band will be the position of MS. Figure 4.5 shows this method. For this method to work MS should be able to get the TA from each of the neighbouring BS. One way is to force the network to handover the MS to at least two of its neighbouring BS and get the TA from each of them.

![Figure 4.5 Locating MS using TA from three BTS](image)

In GSM there is no command defined to force handover a MS to another BS. But there are BSS management commands like forcehHO and adjacentCellHandOver to do similar function (ETS GSM 12.20, 1996). The purpose of these function are to shutdown the BTS or RTX for maintenance. When forcehHO command is executed all the traffic in the BTS will be handed over to other BTS or RTX’s within the same BTS.
It is possible that this command might hand over the MS to another RTX in the same BTS. In such cases the purpose of handover will not be served. The purpose of executing this command in this case is to handover MS to another BTS and to get its TA value. Therefore the forcehHO command alone will not serve the purpose. Handover to another BTS will be possible by changing adjacentCellHandOver attribute, so that handover within the BTS will be not allowed (ETS GSM 12.20, 1996). However this will result in handing over all the MSs camping in the RTX to another BTS. But in this case there will be some MS loosing its connection because the MS being moved might be in a place where there is no BTS to handover.

In GSM, force handover is possible but it is not appropriate to execute the commands available in the GSM to handover the MS since the consequences of using these commands are too high. This is because these commands are not designed for this purpose.

On the other hand even if new commands for force handover are available, it will not be suitable to use these commands for MS location in some of the applications. If MS force handover method is adopted for applications like route guidance, it will create a massive load of handover command signalling on the network which will reduce the performance of the network. This is because application like Route Guidance requires MS to be located as frequently as possible and for a longer period (period possibly for the duration of the journey). But this method can be adopted in application like Weather, Localised Advertising, where location information is generated once in a while.
4.4 OBSERVED TIME DIFFERENCE

Observed Time Difference (OTD) is used in GSM network for synchronised and pseudo-synchronised handover. For pseudo-synchronised handover there are three different quantities defined (Henry, 2000):

- $t_0$ denotes the one way line of sight propagation delay between the MS and BTS.
- RTD (Real Time Difference) denotes the value of the local GSM time in BTS1 (servicing BTS) minus that of BTS2 (new BTS)
- OTD denotes the timing difference between BTS1 and BTS2 as measured by the MS

The relationship between the above mention quantities are:

$$OTD = RTD + t_1 - t_2 \quad \text{..........................}(4.2)$$

In synchronised and pseudo-synchronised handover the RTD is known to the BTS1 and MS. BTS1 may order pseudo-synchronised handover to BTS2, including RTD in the “HANDOVER COMMAND” message (Henry, 2000).

The use of this kind of handover method is to estimate the Timing Advance of the new BTS without receiving it from the new BTS. Under normal operation the $t_1$ is closely related to the Timing Advance sent from the BTS1 to the MS, since MS gets synchronised to BTS2 before performing handover, OTD, RTD and $t_1$ is available to MS, hence value of $t_2$ can be calculated using (4.2) that can be used to set the new Timing Advance parameter without receiving it from the BTS2 (Henry, 2000). In the
non synchronised handover, the Timing Advance is directly evaluated by the new BTS and transmitted to MS.

RTDs are estimated by each BTS from comparison with the time-bases of the neighbouring BTSs. If the network is synchronised, MS is able to obtain RTDs from OTDs, through the following formula (Henry, 2000):

\[
RTD = 2500 \cdot \text{int}\left(\frac{OTD}{2500} + 0.5\right)
\]  

...................................................................(4.3)

In order to find the location of the MS this information can be used to estimate the TDoA measurements between the MS and BTSs.

4.4.1 Time Difference of Arrival (TDoA)

TDoA is the difference of time of arrival of signal from two different BS. This approach would require the BSs to be synchronised to some common time reference if the time of transmission was unknown. TDoA method produces a hyperbola which is a curve of constant time different of arrival from two BSs. The line of position is given by hyperbolas which foci at the BSs on which the MS must lie. The location of the MS is at the intersection of the hyperbolas. Since the branches of hyperbola intersect in two different places, the branches chosen for the lines of position are determined from the sign of the TDoA measurement. If the sign is negative, the hyperbola branch furthest from the BS with respect to the TDoA measurement was made will be chosen. If it is positive, the branch nearest the reference BS is chosen. Figure 4.6 demonstrate the concept of TDoA.
4.4.1.1 **TDoA location algorithm**

For location in two dimensions, three BSs are required which produce two TDoA pairs. Since distance and time are directly related by the speed of light, a hyperbolic equation can be derived for the measured time difference of arrival between BS \( i \) and \( j \).

\[
p_{i,j} = \frac{D_i(x_i) - D_j(x_j)}{c}
\]

Where \( p \) is the TDoA, \( D \) is the range measurements and \( c \) is the speed of light (\( c = 3 \times 10^8 \) m/s is the electromagnetic wave propagation speed). By rearranging equation (3.4) and squaring yields. Where \( i = 2,3 \) and \( j = 1 \).

\[
2cp_{i,j}D_i(x_i) = D_i^2(x_i) - D_j^2(x_j) - c^2 p_{i,i}^2
\]

\[
= \|x]\|^2 - \|x_i\|^2 + 2x_i(x_i - x_j) + 2y_i(y_i - y_j) - c^2 p_{i,i}^2
\]
Solving the equation for \( D_i(x_i) \) for \( i = 2,3 \), \( j = 1 \) and equating the result can be shown as

\[
y_i = mx_i + b
\]

...............(4.7)

Where

\[
m = \frac{p_{3,1}(x_2 - x_1) - p_{2,1}(x_3 - x_1)}{p_{2,1}(y_3 - y_1) - p_{3,1}(y_2 - y_1)}
\]

...............(4.8)

\[
b = \frac{p_{2,1}\|x_3\|^2 - p_{3,1}\|x_2\|^2 + p_{3,2}\|x_1\|^2 + c^2 p_{3,1} p_{2,1} p_{3,2}}{2 [p_{2,1}(y_3 - y_1) - p_{3,1}(y_2 - y_1)]}
\]

...............(4.9)

By substituting \( y_i \) back into (4.6) and solving for \( x_i \) yields the quadratic equation:

\[
A x_i^2 + B x_i + C = 0
\]

...............(4.10)

Where

\[
A = 4 c^2 p_{2,1}^2 (1 + m)^2 - u^2
\]

...............(4.11)

\[
B = -4 c^2 p_{2,1}^2 [2 x_1 - 2 m(y_1 - b)] + 2 u
\]

...............(4.12)

\[
C = 4 c^2 p_{2,1}^2 (\|x_1\|^2 - 2 y_2 b + b^2) - v^2
\]

...............(4.13)

And

\[
u = 2 [x_1 - x_2 + m(y_1 - y_2)]
\]

...............(4.14)

\[
v = \|x_2\|^2 - \|x_1\|^2 - 2 b(y_1 - y_2) - c^2 p_{2,1}^2
\]

...............(4.15)

Which can then be used to compute the \( y_i \) by equation (4.7). The solution for (4.10) will result in two values for \( x_i \), leading to ambiguity. These two solutions are the two branches of the hyperbola. This ambiguity can be resolved by noting the signs of one of
the TDoAs. By plugging both solutions into (4.4) and noting the sign, the correct solution can be found (James J. Caffery, Jr 2000).

4.4.2 TDoA using GSM

Information available in the GSM network can be used to derive TDoAs. The OTDs and RTSs can be used to compute the TDoAs. OTDs are estimated by the MS from time bases of the servicing and the neighbouring BTSs while in the connected mode. The RTDs are estimated by each BTSs. If the network is synchronised, MS can derive the RTDs from OTD by using (4.3)

\[ p_{i,j} = (RTD_j - OTD_j)T_b / 2 \quad (j = BTS1,2) \quad \ldots \ldots \ldots \ldots (4.16) \]

Where \( T_b \) is defined as \( 48/13 \mu s \) (Henry, 2000) and \( i \) as BTS1. This TDoA measurement can be together with the algorithm described in 4.4.1.1 to identify the location of the MS. It is assumed that this method will not give any better accurate information than AT method described in 4.3 since OTD is a method used to calculate the AT value for the new BTS without receiving it from the BTS. Also the timing of GSM which is \( 48/13 \mu s \) needs to be reduced in order to get an accurate OTD. With current GSM bit period the Mobile can be located at least with an accuracy of 550m.
CHAPTER 5

SIGNAL STRENGTH AS A METHOD OF LOCATING

5.1 INTRODUCTION

Apart from network information based location methods, signal properties can be used to identify the location of the MS. Signal strength has been studied by various researchers to calculate the distance between transmitter and receiver.

Even though signal strength depends on many environment factors, it still can be used to calculate distance. Because its performance depends on the environment, it is expected that the accuracy of the location information using signal strength will vary depending on the environment. The field strength of a signal can be represented as a function of distance in space or as a function of time (William C.Y. Lee, 1993). As discussed in Chapter 2 at any given time MS will be monitoring the signal quality of the neighbouring cells and reports back the best 6 cell (excluding servicing BTS) to the network for hand over decision. This information can be used to identify the distance between the MS and the 6 neighbouring BSs and servicing BS.

In this chapter a detailed discussion of calculating distance using different signal strength model will be discussed together with its feasibility in a real environment.
5.2 PROPAGATION PATH LOSS

Propagation path loss is the difference between the effective power transmitted and the average field strength of the received signal. Apart from the distance between the transmitter and receiver there are many factors that contribute to propagation path loss. They are (William C.Y. Lee, 1998; Hernando & Perez-Fontan, 1999):

- Frequency
- Height of the base station antenna
- Height of the mobile station antenna
- Height of the base station relative to the surrounding terrain (effective height)
- Terrain irregularity
- Land usage in the vicinity of the mobile terminal.

When calculating propagation path loss, all the above factors have to be taken into account. The environment at which mobile phone operates is also one of the factor that affect propagation path loss. Mobile phone environment can be categorised as two. They are; Indoor and Outdoor environment.

Path loss can occur in indoor within floors of a building or with different rooms of the same floor. There is no good propagation path loss model available when the transmitters and receivers are located indoors. In case of out door propagation path loss, there are number of good models available (Hernando & Perez-Fontan, 1999).
5.2.1 Indoor Propagation Path Loss

Factors affecting path loss in indoor can be identified as Floors and Partitions. In the same floor, signal can attenuate mainly because of the partitions. In partition attenuation, signals are obstructed by wide variety of partition materials. Partitions vary widely in their physical and electrical characteristic, making it difficult to apply general model to identify the path loss. Table 5.1 shows attenuation as a function of common building materials:

Table 5.1
Average Signal loss for Radio Path Obstructed by Building Material

<table>
<thead>
<tr>
<th>Material Type</th>
<th>Loss (dB)</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concrete block wall</td>
<td>13-20</td>
<td>1300 MHz</td>
</tr>
<tr>
<td>Concrete floor</td>
<td>10</td>
<td>1300 MHz</td>
</tr>
<tr>
<td>Dry plywood (3/4 in)</td>
<td>1</td>
<td>9.6 GHz</td>
</tr>
<tr>
<td>General Machinery</td>
<td>5-10</td>
<td>1300 MHz</td>
</tr>
<tr>
<td>Aluminium sheets (1/8 in)</td>
<td>47</td>
<td>9.6 GHz</td>
</tr>
</tbody>
</table>

A complete tables of materials used in indoor partitions and radio path obstructed by materials is listed in (Theodore, 2002).

Signal Attenuation between floors depends on many factors, that include external dimensions, material of the building, type of construction used to create the floors and the external surroundings. Even the number of windows and the presence of tinting can impact the loss between floors.

It is reported that the signal receiving inside the building due to an external transmitter increases with height. This is mainly because at the lower floors of the buildings signal...
attenuate because of the surrounding obstruction especially in urban. At higher floors a
LOS path may exist, thus causing a stronger incident signal at the exterior walls of the
building (Theodore, 2002).

5.2.2 Outdoor Propagation Path Loss

Below state some of the propagation path loss model available:

- Okumura Model
- Hata Model
- JRC Model
- Walfish-Ikegami Model
- COST 231 – Hata Model

JRC (Joint Radio Committee) Model and Walfish-Ikegami uses detail train profile in
calculating the propagation path loss. COST 231-Hata Model is a modified version of
Hata model and it is developed to be used in computerised coverage calculation
application (Hernando & Perez-Fontan, 1999). For this reason Hata Model will be
discussed and used when calculating MS-BS distance.

5.3 CALCULATING MS – BS DISTANCE USING HATA MODEL

Hata Model is an improved version of Okumura model. Okumura model was developed
by Yoshihisa Okumura in 1968 is the model of choice for analysing mobile-radio
propagation. His model is a fully empirical method developed from a series of

The Okumura model was described in (Yoshihisa Okumura, et.al, 1968). The application of that model involves the use of numerous curves to determine adjustment factors to be applied to field strength. M. Hata, (1980) reduced many of Okumura’s adjustment to equations (James J. Caffery, Jr 2000; Hernando & Perez-Fontan, 1999; Theodore, 2002). These equations can be used in calculating path loss in macrocells.

\[
L_p = \begin{cases} 
A + B \log_{10}(d) & \text{Urban area} \\
A + B \log_{10}(d) - C & \text{Suburban area} \\
A + B \log_{10}(d) - D & \text{Open area}
\end{cases}
\]  

(5.1)

Where

\[
A = 69.55 + \log_{10}(f_c) - 13.82 \log_{10}(h_b) - a(h_m) 
\]  

(5.2)

\[
B = 44.9 - 6.55 \log_{10}(h_b) 
\]  

(5.3)

\[
C = 5.4 + 2[\log_{10}(f_c/28)]^2 
\]  

(5.4)

\[
D = 40.94 + 4.78[\log_{10}(f_c)]^2 - 19.33 \log_{10}(f_c) 
\]  

(5.5)

And

\[
a(h_m) = \begin{cases} 
(1.1 \log_{10}(f_c) - 0.7)h_m - (1.56 \log_{10}(f_c) - 0.8) & \text{Urban area} \\
8.29(\log_{10}(1.54h_m))^2 - 1.1 & \text{Suburban area} \\
3.2(\log_{10}(11.75h_m))^2 - 4.97 & \text{Open area}
\end{cases}
\]  

(5.6)
Where \( L_p \) is the path loss, \( f_c \) is frequency, \( h_b \) is the height of the base station antenna and \( h_m \) is the MS antenna’s height above the ground.

The European Cooperation for Scientific and Technical research (EURO-COST) formed the COST-231 working committee to develop an extended version of Hata model. COST-231 proposed the following formula to extend Hata’s model to 2GHz (Theodore, 2002; Hernando & Perez-Fontan, 1999). This model is specially used in calculating path loss in outdoor microcells.

\[
L_p = E + B \log_{10}(d) + C_M
\]

\[E = 46.3 + 33.9 \log_{10}(f_c) - 13.82 \log_{10}(h_b) - a(h_m)
\]

Where \( a(h_m) \) is defined in (5.6) and

\[C_M = \begin{cases} 
0 \text{ dB} & \text{for medium size city and suburban areas} \\
3 \text{ dB} & \text{for metropolitan centers}
\end{cases}
\]

The above equations can be used together with the information available in the mobile network to calculate the distance between MS and BS. The variables required in these equations are already available in the network as explained in Chapter 2. MS report to the network the details of the neighbouring BS for hand over decision. The information reported back to the network includes the frequency and signal strength of the
neighbouring BS. This information will be enough to compute the distance between MS and BS using equation 5.7.

5.4 TRIANGULATING MS LOCATION

By using the path loss models it is possible to calculate the distance between MS and BS. Distance from three different MS can be used to locate the MS location coordinates.

![Figure 5.1 Typical MS -BS arrangement](image)

A typical MS – BS arrangement is shown in Figure 5.1. MS is located at point M and the corresponding BSs are located at A, B and C. The coordinates of M, A, B and C are \((x_0, y_0)\), \((x_a, y_a)\), \((x_b, y_b)\) and \((x_c, y_c)\). The estimated distance between M and three BS are \(d_{0a}\), \(d_{0b}\) and \(d_{0c}\) respectively. Relation between the MS coordinates and its distance between BSs can be expressed as
Each equation will produce a circle centring at the BS. The MS lies on the circumference of the circle. The point at which all the circle meets is the location of MS. In order to find this point, pairs of equation can be combined to form a linear equation which will produce a straight line between the two intersection points of circles. This will produce three straight lines passing through the intersection points of the circles and meeting it in one or more points as shown in Figure 5.1.

To identify the MS location, the meeting points of these lines can be calculated. Thus by combining any two of the above lines and solving it for \( x_0 \) and \( y_0 \) will give the MS location. It is possible to get three different values for MS location when three pairs of these are solved i.e. \( (x_0', y_0') \), \( (x_0^2, y_0^2) \) and \( (x_0^3, y_0^3) \). This is because of the measurement errors while measuring and calculating the distance between MS and BS. To find the best possible MS location these three values for MS location can be averaged to form the \( x_0 \) and \( y_0 \).
\[ x_0 = \frac{x_0^1 + x_0^2 + x_0^3}{3} \quad \text{and} \quad y_0 = \frac{y_0^1 + y_0^2 + y_0^3}{3} \] ..........(5.16)

This method of triangulating MS location can also be used even in Time of Arrival method discussed in Chapter 3.

In GSM, information reported back to the network by MS contains signal strength of six strongest neighbouring BS (ETS GSM 03.22, 1997). Thus, distance between MS and BS for six BS can be calculated and triangulated to find MS location more accurately.

### 5.5 FACTORS CONTRIBUTING TO LOCATION ERROR

Inaccurate signal strength measurement, Time measurement or angle of arrival measurement due to environment and signal propagation properties can cause errors in calculating MS location.

In time based methods, a small inaccuracy in time measurements can cause huge error in distance calculation. This is because radio waves travels at the speed of light and at that speed a millisecond of error will result in three hundred meters. For the Angle based methods, a very minor error in the angle measurement can result in showing the MS location far away from the actual MS location specially when calculating the location of MS from a far away BS. Similarly error in signal strength can cause very inaccurate MS location.

Method of improving the accuracy of measuring equipment is out of the scope of this thesis. Thus, the rest of the chapter will consider the factors contributing the location error due to the propagation. In this regard, factors contributing the location error in
wireless communication system include multipath propagation and non-line-of-sight propagation.

5.5.1 Multipath propagation

Multipath propagation is caused when signal from transmitter receives to its receiver in multiple signals. This phenomenon is known as fading. Generally this variation of signal can be broken down to two types (Henry, 2000; William C.Y. Lee, 1993).

- The slow or long-term variations
- The fast or short-term variations

Long-term variation or shadow fading is due to blockage by natural or man-made structures along the propagation path and in vicinity of the mobile. There are other factors influencing long term fading that includes speed of the mobile, speed of the surrounding objects and transmission bandwidth of the signal (Theodore, 2002).

Short-term variations are due to a number of multipath echoes reaching and combining at the receiver antenna. These echoes are generated by diffuse reflections from environmental features (Hernando & Perez-Fontan, 1999).

The multipath signal that receives makes it hard to actually determine the signal strength, time and angle in wireless system. High variation in received signal strength in mobile radio system makes it difficult to use path loss models for location.

To minimise the effect of Multipath effect on mobile location, measurements of signal strength can be average for a period and used in calculating the distance between the
MS and BS. There are more advance methods developed to mitigate the effect of multipath including high regulation frequency estimators (Krizman, et al, 1997 p.919-923) and least-means-square (LMS) technique. Super-regulation techniques such as the MUSIC and Root-MUSIC have been utilized to detect multipath components that conventional detectors are unable to detect (James J. Caffery, Jr 2000).

5.5.2 NLOS propagation

Non-line-of-sight (NLoS) propagation occurs when the direct, or line of sight (LoS) path between MS and BS gets blocked by some structure in between. When this happens the signal reaching the receiver takes longer path than LoS to reach it. The signal transmitted reaches the receiver by reflection or diffraction resulting in a longer path. Because it takes longer path to reach to the destination, all mobile location methods suffer.

When signal gets reflected or diffracted signal looses its power since it travels longer distance than the direct path resulting higher path loss. When propagation path loss models are used in such situation the MS location will result in huge error. Typical ranging error introduced by NLoS propagation has been measured in the GSM system which indicates that NLoS error can average between 500-700 meters (James J. Caffery, Jr 2000) when calculating location using time based methods. For angle based locations systems, large error can be introduced if the reflected path is measured.

To mitigate non-line of sight (NLoS) error many solutions have been proposed by researchers. Some of it includes models to distinguish LoS and NLoS signals. P. Wylie and J. Holtzam propose a method to identify LoS by using time history of its range measurements for each BS combining with a prior knowledge of the standard deviation.

5.6 CONCLUDING REMARK

As it can be seen the errors introduced by the multipath and non-line of sight propagation will definitely reduce the accuracy of the MS location no matter which method is employed. There are many ways to mitigate the effect of these errors. In order to do so, the above mentioned models should be utilised in the signal receiving hardware. In mobile telephone system these error mitigation models has to be implemented in the hand set or in the base station hardware.

ETSI standards does not propose any method to mitigate error introduced by multipath and NLoS single for GSM. Thus, the only possible way to minimise the effect of measurement error introduced buy the multipath signal is to average the signal measurements which is available in the current mobile hardware.

In the case of NLoS error, the signal that arrives first at the receiver has the minimum NLoS error. This is because first arrived propagation path will be most of the time for the line of sight path or the path closed to the line of sight path. Since GSM uses first arrived propagation path when calculating TA value (James J. Caffery, Jr 2000), it is assumed that the MS also uses the arrived propagation path when calculating the signal strength.
CHAPTER 6

IMPLEMENTING LOCATION SERVICE IN GSM

6.1 INTRODUCTION

The main focus of this chapter will be to provide outline for implementation of location service in GSM network. Suggested scheme is mainly focused in providing commercial location services with minimum changes to network and mobile devices.

The measurements used in calculating the location of the MS discussed in chapter 4 and Chapter 5 need to be gathered in to central location in order to process and forward the location of the MS when requested by the clients. This chapter proposes and discuss a new model that can be used when processing the MS location. This model is called Location Processing Model (LPM). Proposed model of processing MS location minimise the error level and maximise the accuracy. Even though this method requires additional processing of data, it provides a very simple and efficient solution of processing MS location based on the data from the network.

This chapter also proposes a server based solution in order to implement location service in an existing GSM network.
6.2 LOCATION PROCESSING MODEL (LPM)

The proposed model to process and estimate the MS location is called Location Processing Model (LPM). This is a simple but effective model that uses information from the network and the mobile station to process MS location.

As mentioned in Chapter 4 (4.2.1), even though the MS receives the frequencies to monitor in BCCH Allocation list (BA list) it does not identify the neighbouring cell. This is because in idle mode it receives only the servicing BSIC and its CI, and in connection mode it receives all the neighbouring BSs BSIC but not the CI of neighbouring cells.

Neighbouring CI can be identified with additional processing of BA list information. Figure 6.1 shows an overall process of LPM.
In order to mitigate the effect of errors discussed in 5.5 it’s important to use additional measurements. To minimise the effect of Multipath variation, signal from each monitoring channel needs to be averaged at least for five second (Karim & Jinane, 2003). The result of the average for each frequency channel together with the additional information from BA list is used in identifying the neighbouring CI. Figure 6.2 explains the processes of identifying the BS with the help of frequency.
In order to identify the MS location it will be very important to identify the CI of servicing and neighbouring cells. This is because CI will be the key to uniquely identify the geographical location of BS. In idle and connection mode the servicing cell and its CI are known to MS, it’s the neighbouring CI that has to be identified. As discussed in chapter 2.2.4 no two adjacent cells are allowed to use the same frequency. This property of frequency plan can be used to identify the CI of neighbouring cells that uses the particular frequency. This can be done with the help of the network information database.

Averaged signal strength from each frequency can be used to calculate the MS – BS distance using the method discussed in Chapter 5. To minimise the error on MS location MS – BS distance calculated from all the frequency can be used.
Figure 6.3 Processes of calculating MS location

In most of the cases MS will report frequency from six neighbouring BS excluding servicing BS (ETS GSM 03.22, 1997), this means MS – BS distance for seven BS can be used in calculating the MS location. In order for MS location to be uniquely identified, at least three distances from three BS should be known. It is expected that the accuracy of MS location will improve if more BSs are used in calculating MS location. As explained in Chapter 5 MS location is identified as the meeting point of all the lines and it is expected that the lines are not going to be meeting in one single point due to the signal strength measurement error. Thus the location of MS can be calculated by averaging the X and Y coordinates of resulting meeting points of lines.
If signal strength from all seven BS are used it will be possible to get distances from seven BS which will result in seven or more MS locations. Since this method uses signal strength to identify the location of MS and signal strength is very dependent on the environment, it will be important to identify the MS locations that have most errors and not to use those when averaging the MS locations. In order to do that TA band and the sector of the servicing cell can be identified and those MS locations that fall in and around this TA sector band can be used in averaging MS location.

After average MS location is calculated, accuracy of MS location can be given as the distance between averaged MS location and the furthest MS location used in averaging. In case if there is not enough neighbouring BS available and the service is provided only based on the servicing BS, MS location can be identified as the area that is covered by the TA band of the sector. If the servicing BS is an omni-directional antenna, in such cases MS location can be identified by the area covered by the Cell which can be identified by the CI. Figure 6.3 explains the MS location calculation process and Figure 6.4 explains the concept of MS location processing.
If calculated accuracy of MS location is more than the area identified by the Cell sector and TA band then the MS location can be Cell sector and TA band instead of calculated MS Location. This could be a very unlikely scenario but it is possible in a situation such as:

- When MS has less than two BS as neighbouring BS
- Signal strength measurements are extremely bad so that none of calculated MS location falls in or around the TA band identified for that sector.

Figure 6.4 Typical location processing scenario.
6.3 METHODS OF IMPLEMENTING

There are two methods of implementing Location based services (LBS) in GSM network (Cristopher Drane, et al, 1998).

1. Network based

2. Hand Phone assisted network based

Network based methods totally process the location of MS using the information provided by the network entities and functions. In Hand Phone assisted method, hand phone provides the network measurements to the network for further processing of MS location.

6.3.1 Network Based

Subscriber and equipment tracking procedures in ETS GSM 12.08 (1998) can be used in gathering the required details for location calculation. The main purpose of these procedures is for administration and for network management to trace the activities of various entities when specific events occur within the Public Land Mobile Network (PLMN). This facility also enables the tracking of all the information that is available to the PLMN connecting the cell path by associated entity.

6.3.1.1 Subscriber tracking in GSM

There are many types of subscriber tracking defined in (ETS GSM 12.08, 1998). That includes; tracking of a native subscriber in home network, tracking of a native
subscriber roaming in other networks, tracking of a foreign subscriber in home network and tracking of equipment based on International Mobile Equipment Identity (IMEI).

Operators can activate tracking by invoking the management function “Active Home Subscriber Trace” in the HLR. HLR then forward this message to the VLR where subscriber is registered via a MAP message (MAP-ACTIVATE-TRACE-MODE). VLR then forward the tracking activation command to MSC. From MSC, tracking is invoked by sending a MAP message to BSS (MSC_INVOKE_TRACE). When BSS receives this message it starts tracking the necessary fields in the BSS Record. This tracking activity is explained in Figure 6.5.

Resulting reports will be reported back to the Operations and Maintenance Centre (OMC). Detail contents of the reports are available in (ETS GSM 12.08, 1998). Some of the important fields available in these reports are:

- Cell ID, Location ID, BSIC
- Timing Advance value
- MS power, BS power
- MSC Address, VLR Number, Service Centre Address, BTS ID
- All radio measurements.
Subscribers tracking procedures can be useful in implementing location service in GSM network. Reports provided by the tracking activity provide all the necessary information to calculate the MS location using the location technology discussed in Chapter 4 and 5.

With this method there will not be any changes to the hand phone or to the network. Only additional network entity will be a location server. Location server will be needed which ever the implementation method is used.

For this reason, a single additional entity to the system called Mobile Location Server (MLS) is proposed. This will act as a location service provider to the clients. MLS proposed in this thesis outlines only the major functions necessary for such application. Complete functional description of such application server is out of the scope of this thesis.
6.3.2 Hand phone assisted network based

As discussed in Chapter 4, MS measure the signal strength of frequencies listed in BA list (BCCH Allocation list) and identify six strongest cells and report the readings back to the network for hand over decision. This information can be retrieved and send to MLS through a SMS gateway as SMS. This will be an additional function that has to be built to the hand phone. There are two ways to implement this function in hand phones.

1. Java application running in hand phones
2. SIM Application tool kit (SAT)

A java application can be developed to retrieve all the necessary information from the hand phone and to send it back to MLS for further processing of MS location. This application can be made available to be downloaded and install via WAP protocol in to handsets. The problem with this approach is that not all hand phones has the capacity to run the java application and not all the subscribers who has java enabled hand phones are familiar with the procedure of downloading application over WAP.

A better solution than java application is SAT application. SAT applications are installed and run in SIM itself. The other advantage of SAT is that almost all the hand phones support SAT applications. Some of the SIM based value added services provided in Malaysia includes Restaurant Bookings, Cinema Bookings, Stock Exchange and Muslim Prayers time. Location service can also be included as SIM based service.
6.3.3 SIM Application Toolkit

The SIM Application Toolkit described in 3GPP TS 11.14 (1999) provides mechanisms which allow SAT applications to interact and operate with any ME. Table 6.1 shows some of the Commands available in the SIM application tool kit. The detail description of these commands is available in 3GPP TS 11.14 (1999)

<table>
<thead>
<tr>
<th>Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CLOSE CHANNEL</td>
<td>PROVIDE LOCAL INFORMATION</td>
</tr>
<tr>
<td>DISPLAY TEXT</td>
<td>RECEIVE DATA</td>
</tr>
<tr>
<td>GET CHANNEL STATUS</td>
<td>REFRESH</td>
</tr>
<tr>
<td>GET INKEY</td>
<td>RUN AT COMMAND</td>
</tr>
<tr>
<td>GET INPUT</td>
<td>SELECT ITEM</td>
</tr>
<tr>
<td>GET READER STATUS</td>
<td>SEND DATA</td>
</tr>
<tr>
<td>LANGUAGE NOTIFICATION</td>
<td>SEND DTMF</td>
</tr>
<tr>
<td>LAUNCH BROWSER</td>
<td>SEND SHORT MESSAGE</td>
</tr>
<tr>
<td>MORE TIME</td>
<td>SEND SS</td>
</tr>
<tr>
<td>OPEN CHANNEL</td>
<td>SEND USSD</td>
</tr>
<tr>
<td>PERFORM CARD APDU</td>
<td>SET UP CALL</td>
</tr>
<tr>
<td>PLAY TONE</td>
<td>SET UP IDLEMODE TEXT</td>
</tr>
<tr>
<td>POLL INTERVAL</td>
<td>SET UP MENU</td>
</tr>
<tr>
<td>POWER OFF CARD</td>
<td>TIMER MANAGEMENT</td>
</tr>
<tr>
<td>POWER ON CARD</td>
<td></td>
</tr>
</tbody>
</table>

These commands can be used to setup a menu driven application. One important command that can be used in providing location service is “PROVIDE LOCAL INFORMATION”. This command requests ME to send current local information to the SIM. This information includes (3GPP TS 11.14, 1999):

- Location information: the mobile country code (MCC), mobile network code (MNC), location area code (LAC) and cell ID of the current servicing cell.
- The IMEI of the ME;
• The Network Measurement Results and the BCCH channel list;
• The current date, time and time zone;
• The current ME language setting;
• Timing Advance.

Information provided by this command can be used to processes the MS location since it gives cell ID and the measurements of signal strength, frequencies of servicing and neighbouring BS.

In order to implement location service, a SIM application toolkit based application can be developed. This application can be a menu driven application. Class 0 SMS messages can be used in communicating between MLS and the MS.

Class 0 messages are messages that can be sent or received by the MS but does not get stored in the SIM or ME. When this kind of message receives to the MS no “message received” message will be displayed and no alert sound gets triggered. But the message appears on the display of the MS (ETS GSM 3.38, 1998).

The message sent from the MS can contain the details provided by the “PROVIDE LOCAL INFORMATION” command. In this case subscriber tracking activity can be eliminated and use the information provided by the “PROVIDE LOCAL INFORMATION” command to calculate the location of MS by the Location Server. Currently in Malaysia market all the operators use “GEMPLUS” SIM cards (Gemplus, 2005) which supports SAT. Gemplus also provides a development tools called GemXplore it is a plug-in for Borland's JBuilder. It enables Java Card and SIM Toolkit
aplet development capabilities within JBuilder, providing additional wizards, project management and custom menus.

6.3.4 SIM API for Java Card

SIM API for Java cards is a technology described in (ETS GSM 03.19, 1998). It describes an API for the GSM SIM. This API allows application to access the functions and data described in (3GPP TS 11.11, 1999) and (3GPP TS 11.14, 1999), such that SIM based services can be developed and loaded onto SIMs, quickly.

Great advantage of this API is that it can be loaded in to SIM even after issuing the SIM to the subscribers, this can be done remotely. This API can be of important use in developing location based application but at the moment not many mobile phone support this API.

6.4 MOBILE LOCATION SERVER (MLS)

MLS will be a new physical entity proposed to GSM system. MLS will consist of four main functions. Subscriber Authorization Function (SAF), Subscriber Tracking Function (STF), Location Calculation Function (LCF) and Formatting and Presentation Function (FPF). Figure 6.6 shows the basic concept of MLS.
6.4.1 Subscriber Authorization Function (SAF)

The Subscriber Authorization Function (SAF) is responsible for providing access and subscription authorization to Location Service (LCS) Server.

6.4.2 Subscriber Tracking Function (STF)

Subscriber Tracking Function (STF) is responsible for requesting and receiving tracking information from Operations and Maintenance Centre (OMC) or from HLR. STF will also identify the necessary fields from track report and forward it to location calculation unit for calculation.
6.4.3 Location Calculation Function (LCF)

Location Calculation Function (LCF) receives the tracking data from STF and uses those data to calculate the location of MS. It is also responsible in determining which location technology it is going to use based on the data provided by STF. This function also holds the details about network.

The database holding the network details includes the cell details needed in calculating the location information. The information listed in Table 6.2 needs to be stored in the database for each cell in this function.

<table>
<thead>
<tr>
<th>Parameters data needed for each cell</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell ID</td>
<td>Cell Identity number</td>
</tr>
<tr>
<td>Azimuth</td>
<td>Cell direction (RTX)</td>
</tr>
<tr>
<td>Cell Sector Type</td>
<td>Type of cell used (4 or 6 sectored cell)</td>
</tr>
<tr>
<td>BTS position</td>
<td>BTS position (latitude/longitude) of the BTS</td>
</tr>
<tr>
<td>CGI</td>
<td>Cell global identity.</td>
</tr>
<tr>
<td>BS TX value</td>
<td>Base Station Transmitter power</td>
</tr>
<tr>
<td>BSIC</td>
<td>Base station identity code</td>
</tr>
<tr>
<td>BCCH</td>
<td>Frequency of the broadcast carrier.</td>
</tr>
</tbody>
</table>

6.4.4 Formatting and Presentation Function (FPF)

Formatting and presentation function (FPF) produce output of the location and forward it to the client. Output of the location can be presented by many means, which includes: Voice Messages, SMS text message, MMS Picture Message or as an interactive object. More detail discussion of Formatting and Presentation functions are discussed later in this chapter. Typical proposed network arrangement with MLS is shown in Figure 6.7.
In this scenario, subscriber can request LCS through home SMS gateway and get the reply as an SMS.

Figure 6.7 GSM network entity arrangements with LCS server

MLS provides the interface between a mobile user and an external Content Provider. The interface may support one or more technologies such as voice, SMS or WAP. The MLS also provides firewall, authentication and authorisation features to control access to the Gateway from 3rd parties.
6.5 PRESENTING LOCATION INFORMATION

Current mobile phone system has four different ways of providing such services they are: Voice, Short Message Service (SMS), Multimedia Messaging Service (MMS) and Wireless Application Protocol (WAP). These services are available to all subscribers at a very minimal cost. Majority of the handsets in the current market now support MMS.

It is possible to use these services to provide the subscribers with location service. If we consider voice as a means of providing location services, operators can setup location service call centres to answer subscribers call regarding their location. Queries may vary depending on the service provided. In such arrangement location subscribers will query by voice to an operator and it is the operator who will be interacting with the MLS.

The other way is to use SMS service to send query to location server. In this way users can SMS commands to MLS that will process the command and invoke necessary procedures in order to get the required result from MLS. The result of the query can be delivered back to the user by means of an SMS. This can be an effective means of providing location service since SMS is a very convenient and easy service available in all the handsets. If the location service provided requires maps or other kind of visual guides. The maps can be rendered and sent to the user as a MMS message.

In location service like location based information service, maps can be provided as a MMS message. Based on the location of the subscriber, maps can be generated and formatted as a MMS message and sent to subscriber. For map service the content
service provider to MLS server should be able to provide the maps with additional information based on the requested location.

6.6 LOCATION SERVICE STANDARD DEFINED BY UMTS

Universal Mobile Telecommunications System (UMTS) defines its standard of location service in (3GPP TS 23.171, 1999). It describes major changes to the hardware and new entities to the network. Some new entities that are proposed are Location Measurement Unit (LMU), Servicing Mobile Location Centre (SMLC) and Gateway Mobile Location Centre (GMLC).

6.7 LCS COMMUNICATION PROTOCOLS

ETSI nor UMTS defines protocol to communicate between LCS client and server. It is very important to adopt a common protocol for the communication in order to make the location interoperable among the networks. For this purpose there is a third party forum called Location Interoperability Forum (LIF) which has developed a protocol for the purpose of communication between LCS client and server.

6.7.1 LIF Mobile Location Protocol

The Location Interoperability Forum (LIF) is an initiative established jointly by Ericsson, Motorola and Nokia to define and promote a common solution for determining the location of mobile devices across different wireless network boundaries (LIF TS 101, 2002; Andrew Jagoe, 2003).
The Mobile Location Protocol (MLP) is an application-level protocol for getting the position of mobile stations independent of underlying network technology. The MLP serves as the interface between a Location Server and a Location Services (LCS) Client. This specification defines the core set of operations that a Location Server should be able to perform.

This specification covers the core of a Mobile Location Protocol that can be used by a location-based application to request MS location information. The API is based on existing and well-known Internet technologies as HTTP, SSL/TLS and XML, in order to facilitate the development of location-based applications (LIF TS 101, 2002).
CHAPTER 7

EXPERIMENTAL RIG AND MEASUREMENT TECHNIQUES

7.1 INTRODUCTION

Detail method used in carrying the experiments will be discussed in this chapter. This chapter also describes the tools used and developed when carrying on the experiments. The main purpose of these experiments is to implement the measurement techniques described in Chapter 4, 5 & 6 in a real environment. To carry out the experiments based on the theoretical work done in this research, a program was developed and a mobile telephone network and an area were identified.

The information and test results produced in this work was based on the mobile network information received from the telecommunication company based in Republic of Maldives called Dhiraagu (www.dhiraagu.com.mv).

Dhiraagu has been the national telecommunications carrier of the Maldives since 1988 (Dhiraagu, 2005). The information provided by Dhiraagu was very limited due to the nature of the information. Thanks for the help provided by the company, this research was able to test some of the theories discussed in this thesis.
The information provided by Dhiraagu includes:

- BTS Name
- Latitude
- Longitude
- Cell Name
- Antenna Height
- Location Area Code
- Cell ID
- BCCH
- NCC
- BCC
- Transmitter power (TX)
- Frequencies used by Cell
- Azimuths of the antenna
- Neighbours cells

The above information was provided for 29 different BS.

7.2 SELECTION OF AREA TO CARRY THE TEST

As mentioned above the information provided by the service provider was very limited and was willing to give minimum information required to carry out the test. Since these tests were to carry out in Urban, Sub-urban and Rural area, we requested to get the information from the network in and around the capital Male’ (Capital of Maldives).
Maldives is located in Indian Ocean near the equator. It consists of 26 atolls and has 1190 islands and among these islands 200 are inhabited and the rest are 87 tourist resorts and uninhabited islands. Male' is the capital and its located in the middle of the atoll chain, a small island buzzing with the sounds and activities of about 75,000 people which is about one third of the population with an area of 1.77 sq.kms (VisitMalsives, 2005).

For this research, we have selected Male’ as a city or urban area and area around Male’ as the Sub-Urban area. No tests were conducted for the rural area because of the limitation of the network information.

![Figure 7.1 Male’, Capital of Maldives and its surrounding](image)

Male’ being the capital of Maldives and the home for 75,000 people with a small area it has a very complex road system with narrows roads and lots of buildings. Figure 7.1 shows the map of Male’ and its complex rode structure. Because of the demand of the
mobile phone service in the capital (1 in 2 adults in the country use a GSM phone (Dhiraagu, 2005)) the mobile antennas are all around the capital.

7.3 DEVELOPMENT OF TESTING TOOLS AND THE TESTING SETUP

A software tool was developed to receive the information from a mobile phone and GPS receiver connected to a computer. The program was designed to use in Microsoft Pocket PC (PDA) and to connect the mobile phone and GPS receiver to the PDA wire Bluetooth connection. But because we could not locate a mobile phone that is capable of making Bluetooth connection and that give access to retrieve network information, the program was redesigned to run in Microsoft Windows environment.

The program developed for the purpose of retrieving network information from the mobile phone and information from GPS receiver was developed using Microsoft Visual C++ and Microsoft Visual Basic. Mobile Phone used for the purpose of retrieving network information was Nokia 8120. Program uses Nokia Netmonitor or engineering function which is built to Nokia DCT3 family phones. The GPS receiver used in the test was Gamin eTrex GPS receiver.

7.3.1 Engineering function in Nokia Mobile phone.

![Nokia Net monitor screen as seen on the mobile phone screen.](image-url)
Nokia Netmonitor menu is a hidden menu found in old Nokia Mobile phones. This is an engineering menu that gives information about the Network and the state of the mobile phone. Figure 7.2 shows sample output screens of Nokia Netmonitor screen. The new generation of the Nokia phone (DCT4) does not provide any details about the way to activate this menu. It is assumed that even the DCT4 mobile phone has this hidden menu but Nokia does not reveal the activation procedures. Some of the information provided in this additional menu includes:

- **Servicing Cell Information**
  - Channel number of channel used
  - RXLev parameter value
  - TX level of the transmitted signal
  - Time slot
  - Timing Advance
  - Rate of transmission errors
  - Radio Link Timeout
  - C1 & C2 parameter
  - Type of channel currently used by the phone
  - BSIC value for current cell
  - Hopping Sequence Number

- **7 Neighbouring Cell Information**
  - Channel number of channel used
  - C1 parameter & BSIC
  - RXLev parameter value
• **Identification of the currently used network**
  - Mobile Country Code
  - Mobile Network Code
  - Location Area Code
  - Channel number of channel used in communication with cell
  - Cell Identifier

• **Change Phone settings**
  - Turn on constant backlight of the screen and keyboard
  - Information about battery and phone charger mode
  - Phone battery Charging parameters
  - Charging parameters and indicators
  - Information about the battery

• **Other Information**
  - Information about FBUS connection between phone and computer
  - Reason of last rebooting internal firmware of phone.
  - Reason of last connection end
  - Information about handover
  - Information about SIM card
  - Reads/ write data field from SIM card
  - Test connected with SMS messages

Hidden engineering menus are available in many of the other mobile phone brands. The reason to pick Nokia for this research is because of the availability of necessary resources about this function and the procedure to access this function.
7.4 SOFTWARE DEVELOPMENT AND METHOD OF DATA GETHERING

Software developed for the purpose of data gathering is called “THE MAGIC”. Figure 7.3 shows the screen output of “The Magic” program in connection mode. It communicates with the Mobile phone and GPS receiver using serial connection. Since the setup needs the mobility, the program was installed in a laptop and both Mobile phone and GPS receiver was connected to the laptop.

Figure 7.3 Setup and data recording screen of our MAGIC program.

Information from Mobile Phone and the GPS receiver is stored in a Microsoft Access Database. Software records measurement each an every half a second. The information recorded in each measurement includes:

- Status
- Altitude
- East Position Error
- North Position Error
- Type of position fix
- Date and Time
- Latitude
- Longitude
- Velocity
- Record Count
- Record Status
- Information from Mobile Phone
- Information from GPS
• **Network Information**
  
  o Country code
  
  o Network Code
  
  o Location Area Code

• **Servicing Cell information**
  
  o Cell ID
  
  o Channel Number
  
  o Signal Strength (RXLevel)
  
  o Transmitted signal strength
  
  o Timing Advance
  
  o Transmission Error
  
  o Radio Link Timeout
  
  o Path-loss (C1 & C2)
  
  o Channel Type
  
  o BSIC

• **Neighbouring cell information**
  
  o Channel
  
  o C1 / BSIC
  
  o RXLevel
  
  o C2
GPS receiver information includes:

- Altitude
- Date Time
- Latitude
- Longitude
- Speed

In order to record the required measurements, both GSM hand phone and the GPS receiver were installed outside the vehicle. The reason for it to be placed outside the vehicle is to maximise the possibility of receiving line of sight signal both from mobile antennas and from satellites. Both GPS receiver and Mobile phone was wired to the laptop using serial connection. GPS receiver was used to get the reference MS position to be compared with the estimated one. Figure 7.4 shows the equipment used.

![Equipment Image](image.png)

**Figure 7.4** Equipments used

The information recorded were retrieved from the stored Microsoft Access file and used for further processing.
7.4.1 Implementation of Software Tool

Almost all the major mobile hand phone manufacturers provide engineering mode or network monitoring mode. But there is very little technical information available in the market for these functions. Especially activating procedure and programming procedures. Among all the hand phones available in the current market, Nokia hand phones “netmonitor” function is most widely discussed over the internet forums and blogs. There are no official documents about this functions published by Nokia or any other manufacturer. This function is an additional hidden menu that can be activated in Nokia old phones (DCT3 generation). Sadly the option of activating this menu in new Nokia hand phones (DCT4 generation phones) is yet not known.

There are 1 to 132 sub menus (in some Nokia hand phones) in this function. These sub menus provides information ranging from cell, signal, power, phone memory, phone security and many more information. Among these submenus for this research only submenu 1, 2, 3, 4, 5 and 11 were used. These menus provide cell information and signal strength information.

In order to read this informs using a software tool there were three things that need to be studied. That includes:

- Communication between hand phone and the computer
- Protocol used in communication
- Commands used in reading and writing to hand phone.

The hand phone that was used in this experiment was a Nokia 8210 and it was connected to the computer using a serial cable. For this reason serial communication
was the first thing that needs to be studied. Since serial communication procedure is
something very simple and well published procedure, it will not be further detailed in
this document.

There are two kinds of protocols used by Nokia when communicating with its hand
phone. These are FBUS and MBUS. MBUS is a very slow half-duplex protocol which
can have maximum bit rate of 9600bps and only used in very old Nokia hand phones.
FBUS is a full duplex protocol with bit rate of 115200bps and used in new hand phones
that use serial cable to communicate. Sadly Nokia also has not yet published any official
document explaining these protocols. Only available information is from individual
researchers and forums from the internet. In this research only FBUS protocol was
implemented and used because the hand phone used supports only this protocol.

In general most of the time to communicate with a mobile hand phone modem it is
possible to use AT commands which is defined by ETS GSM 07.07 (1999). To
communicate using AT commands it is not necessary to use the FBUS protocol. AT
commands can be send to the modem of mobile hand phone using a serial connection
and the hand phone respond to the command. But this command set does not have any
command to access Nokia netmonitor menus, thus the only solution will be to use Nokia
FBUS communication protocol.

There was no implementation done for the GPS receiver protocol because the GAMIN
hardware that was used in this research was provided with an ActiveX component
(OCX file).
7.4.1.1 Protocol Implementation

When writing the date to hand phone the protocol header consists of 6 Byte.

- Byte 0: F-Bus frame ID. This id is 0x1e for cable and 0x1c for infra read.
- Byte 1: Destination address. When sending data this is always 0x00
- Byte 2: Source address. When sending data it is always 0x0c
- Byte 3: This is the message type. For net monitor message type is 0x40
- Byte 4 & 5 is the length of the message.
- Byte 6 : Data segment starts

If the data segment ends at an odd bit, then a padding bit (0x00) has to be added to end at a even bit. Second last bit is the odd check sum and the last bit is the even check sum.

The checksum is calculated by XORing all the odd bytes and placing the result in odd check sum location and then XORing the even bytes and placing the result in even checksum location.

Below shows a sample implication of protocol using C++

```c++
EncodeFBUSFrame(int s, unsigned char *buffer, int length, unsigned char type)
{
    unsigned char  outbuffer[130];
    unsigned char  checksum=0;
    int   count, current=0;
    int   sent;

    /* message header. */
    outbuffer[current++] = 0x1e;  /* fbus cable */
    outbuffer[current++] = 0x00;  /* Destination */
    outbuffer[current++] = 0x0c;  /* Source */
    outbuffer[current++] = type;   /* Type */
    outbuffer[current++] = length / 256;  /* Length */
    outbuffer[current++] = length % 256;  /* Length */

    /* Copy in data */
    memcpy(outbuffer + current, buffer, length);
    current+=length;
}
```
/* If the message length is odd we should add pad byte 0x00 */
if (length % 2) outbuffer[current++] = 0x00;

/* calculating checksums over entire message
   and append to message. */

/* Odd bytes */
checksum = 0;
for (count = 0; count < current; count += 2)
    checksum ^= outbuffer[count];
outbuffer[current++] = checksum;

/* Even bytes */
checksum = 0;
for (count = 1; count < current; count += 2)
    checksum ^= out_buffer[count];
outbuffer[current++] = checksum;

/* Send it out... */
sent = s.DeviceWrite (outbuffer, current);
}

When receiving data from the hand phone similar byte arrangement is followed accept
that the source and destination byte get swapped.

7.4.1.2 Commands Used

To receive the netmonitor menu information from the hand set there is a very simple
command that needs to be sent to the mobile hand set. A byte array of four with the
following byte arrangement can be sent to the hand set to get the netmonitor menu
information.

Byte 0: 0x00
Byte 1: 0x01
Byte 2: Number of the netmonitor menu.
Byte 3: 0x00
The following codes explain the implementation in C++

```c++
NetmonitorCommand(int testnumber)
{
    unsigned char  req[4];
    req[0] = 0x00;
    req[1] = 0x01;
    req[2] = testnumber;      /* Add menu number */
    req[3] = 0x00;
    return req;
}
```

### 7.4.1.3 Pseudocode

The following pseudocode explains the mains functions that was implemented in order to receive and record the information from the hand phone and GPS receiver.

```plaintext
RecordingProcess()
    Recording = true
    /* Loop the recording process until the process if shutdown */
    Loop until Recording = false
        If port.IsOpen = false
            port.open(port number)
        end if
        if port.IsOpen
            /* Get netmoniter command code for 1 menu */
            command = netmonitor(1)
        /* Encode netmoditer command code in FBUS protocol format*/
        EncodeFBUSFrame(p, command, command.length, 0x40)
        WaitforRespond(inputbuffer)
        /* Decode the receive respond from the hand phone and
        Split the respond string according to its field value and displays
        in its appropriate field */
        DecodeInputBuffer(inputbuffer)
        Display servicing cell fields
            Channel = substring(inputbuffer,2,3)
            RxLevel = substring(inputbuffer,6,3)
            TxLevel = substring(inputbuffer,10,3)
            TA = substring(inputbuffer,17,2)
```
DTX active = substring(inputbuffer,20,1)
Rtimeout = substring(inputbuffer,22,4)
C1 = substring(inputbuffer,28,3)
C2 = substring(inputbuffer,36,3)
CHtype = substring(inputbuffer,44,4)

End

Inputbuffer= empty

/* Get netnomiter command code for 2 menu */

command = netmonitor(2)
EncodeFBUSFrame(p, command, command.length, 0x40)
WaitforRespond(inputbuffer)
DecodeInputBuffer(inputbuffer)

Display servicing cell fields
    BSIC = substring(inputbuffer,11,2)
    TDX disable = substring(inputbuffer,20,1)
End

Inputbuffer= empty

/* Get netnomiter command code for 3 menu */

command = netmonitor(3)
EncodeFBUSFrame(p, command, command.length, 0x40)
WaitforRespond(inputbuffer)
DecodeInputBuffer(inputbuffer)

Display 1st & 2nd neighbouring cell fields
    Channel = substring(inputbuffer,14,3)
    BSIC/C1 = substring(inputbuffer,18,2)
    RxLevel = substring(inputbuffer,20,3)
    C2 = substring(inputbuffer,23,3)

    Channel = substring(inputbuffer,27,3)
    BSIC/C1 = substring(inputbuffer,31,2)
    RxLevel = substring(inputbuffer,33,3)
    C2 = substring(inputbuffer,36,3)
End

Inputbuffer= empty

/* Get netnomiter command code for 4 menu */

command = netmonitor(4)
EncodeFBUSFrame(p, command, command.length, 0x40)
WaitforRespond(inputbuffer)
DecodeInputBuffer(inputbuffer)
Display 3rd, 4th & 5th neighbouring cell fields
   Channel = substring(inputbuffer,1,3)
   BSIC/C1 = substring(inputbuffer,5,2)
   RxLevel = substring(inputbuffer,7,3)
   C2 = substring(inputbuffer,10,3)

   Channel = substring(inputbuffer,14,3)
   BSIC/C1 = substring(inputbuffer,18,2)
   RxLevel = substring(inputbuffer,20,3)
   C2 = substring(inputbuffer,23,3)

   Channel = substring(inputbuffer,27,3)
   BSIC/C1 = substring(inputbuffer,31,2)
   RxLevel = substring(inputbuffer,33,3)
   C2 = substring(inputbuffer,36,3)

End

Inputbuffer= empty

/* Get netnomiter command code for 5 menu */

command = netmonitor(5)
EncodeFBUSFrame(p, command, command.length, 0x40)
WaitforRespond(inputbuffer)
DecodeInputBuffer(inputbuffer)

Display 6th 7th & 8th neighbouring cell fields
   Channel = substring(inputbuffer,1,3)
   BSIC/C1 = substring(inputbuffer,5,2)
   RxLevel = substring(inputbuffer,7,3)
   C2 = substring(inputbuffer,10,3)

   Channel = substring(inputbuffer,14,3)
   BSIC/C1 = substring(inputbuffer,18,2)
   RxLevel = substring(inputbuffer,20,3)
   C2 = substring(inputbuffer,23,3)

   Channel = substring(inputbuffer,27,3)
   BSIC/C1 = substring(inputbuffer,31,2)
   RxLevel = substring(inputbuffer,33,3)
   C2 = substring(inputbuffer,36,3)

End

Inputbuffer= empty

/* Get netnomiter command code for 11 menu */

command = netmonitor(11)
EncodeFBUSFrame(p, command, command.length, 0x40)
WaitforRespond(inputbuffer)
DecodeInputBuffer(inputbuffer)
Chapter 7, Experimental rig and measurement techniques

Display Network information fields
  Countrycode = substring(inputbuffer,4,3)
  NetworkCode = substring(inputbuffer,10,2)
  LocatinArea = substring(inputbuffer,18,5)
  CID = substring(inputbuffer,40,5)
End

ReadGPSData()     /* read the GPS to get the location */
/* save the phone recording and GPS readings to a database */
SaveDataInDatabase()
End if
End loop
End RecordingProcess

WaitforRespond(inputbuffer)
/* waiting to receive the data from the hand phone */

StartTickTime = CurrentTickCount     /* read the current CPU tick time */
bufferLocation = 0
Loop until (notDataToRead)
  /* if the current tick time subtract from the started tick time is greater than the time out time than raise error */
  If CurrentTickCount- StartTickTime > TimeOutTime
    Return error
  End if
  /* read data from input buffor */
  Readcount = readDatafromPort(tempbuffer)
  If Readcount > 0
    /* if any data is read then change the start tick timer to current tick counter to */
    StartTickTime = CurrentTickCount
    /* add all receive data to input buffer variable */
    i=0
    Loop While i=0
      Inputbuffer(bufferLocation+i) = tempbuffer(i)
      bufferLocation = bufferLocation+1
      i = i + 1
    End Loop
  End if
End loop
End WaitforRespond
7.4.1.4 Flow chart

The following flow chart explains the main functions that were implemented in order to receive and record the information from the handphone and GPS receiver.

Figure 7.5 Flow chart showing main functions to receive data from handphone and GPS.
CHAPTER 8

RESULTS AND DISCUSSION

8.1 INTRODUCTION

To identify the reliability of the methods discussed in this thesis, experiments were carried in real mobile network environment. Experiments were also carried out to find the effect on the mobile signal in different speed and the effect of speed on the accuracy of the MS location. In this chapter we also discuss the possible ways to increase the accuracy of the results.

8.2 EFFECT OF SIGNAL STRENGTH IN DIFFERENT SPEED

Experiment is carried in highway at the speed of 120 km/h, 80 km/h and 40 km/h. Measurements are taken by driving a car in between Subang Jaya and Kula Lumpur International air port (KLIA). Figure 8.1 shows the results for all three speeds.

At speed 120 km/h and 80 km/h similar signal fluctuation can be seen but at the speed of 40km/h the signal fluctuation is relatively smooth compared to signal fluctuation in 120 and 80 km/h.
Table 8.1
Signal Strength measurements at different speed.

<table>
<thead>
<tr>
<th>Sec.</th>
<th>120 Km/h</th>
<th>80 Km/h</th>
<th>40 Km/h</th>
<th>Sec.</th>
<th>120 Km/h</th>
<th>80 Km/h</th>
<th>40 Km/h</th>
<th>Sec.</th>
<th>120 Km/h</th>
<th>80 Km/h</th>
<th>40 Km/h</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>-73</td>
<td>-62</td>
<td>-68</td>
<td>5</td>
<td>-46</td>
<td>-60</td>
<td>-70</td>
<td>6</td>
<td>-46</td>
<td>-60</td>
<td>-74</td>
</tr>
<tr>
<td>7</td>
<td>-46</td>
<td>-60</td>
<td>-76</td>
<td>8</td>
<td>-46</td>
<td>-60</td>
<td>-76</td>
<td>9</td>
<td>-54</td>
<td>-59</td>
<td>-76</td>
</tr>
<tr>
<td>17</td>
<td>-68</td>
<td>-60</td>
<td>-69</td>
<td>18</td>
<td>-68</td>
<td>-60</td>
<td>-69</td>
<td>19</td>
<td>-68</td>
<td>-61</td>
<td>-58</td>
</tr>
<tr>
<td>20</td>
<td>-47</td>
<td>-61</td>
<td>-58</td>
<td>21</td>
<td>-47</td>
<td>-60</td>
<td>-58</td>
<td>22</td>
<td>-47</td>
<td>-60</td>
<td>-58</td>
</tr>
<tr>
<td>29</td>
<td>-55</td>
<td>-61</td>
<td>-55</td>
<td>30</td>
<td>-57</td>
<td>-61</td>
<td>-55</td>
<td>31</td>
<td>-57</td>
<td>-60</td>
<td>-55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sec.</th>
<th>120 Km/h</th>
<th>80 Km/h</th>
<th>40 Km/h</th>
<th>35</th>
<th>-44</th>
<th>-57</th>
<th>-53</th>
<th>36</th>
<th>-44</th>
<th>-57</th>
<th>-53</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>-46</td>
<td>-60</td>
<td>-70</td>
<td>41</td>
<td>-47</td>
<td>-63</td>
<td>-71</td>
<td>42</td>
<td>-48</td>
<td>-63</td>
<td>-71</td>
</tr>
<tr>
<td>43</td>
<td>-48</td>
<td>-64</td>
<td>-70</td>
<td>44</td>
<td>-52</td>
<td>-60</td>
<td>-70</td>
<td>45</td>
<td>-52</td>
<td>-60</td>
<td>-70</td>
</tr>
<tr>
<td>46</td>
<td>-54</td>
<td>-60</td>
<td>-80</td>
<td>47</td>
<td>-54</td>
<td>-61</td>
<td>-80</td>
<td>48</td>
<td>-58</td>
<td>-60</td>
<td>-80</td>
</tr>
<tr>
<td>55</td>
<td>-61</td>
<td>-50</td>
<td>-62</td>
<td>56</td>
<td>-64</td>
<td>-49</td>
<td>-62</td>
<td>57</td>
<td>-64</td>
<td>-48</td>
<td>-63</td>
</tr>
<tr>
<td>58</td>
<td>-67</td>
<td>-47</td>
<td>-68</td>
<td>59</td>
<td>-71</td>
<td>-47</td>
<td>-68</td>
<td>60</td>
<td>-74</td>
<td>-47</td>
<td>-68</td>
</tr>
<tr>
<td>64</td>
<td>-81</td>
<td>-45</td>
<td>-57</td>
<td>65</td>
<td>-81</td>
<td>-45</td>
<td>-57</td>
<td>66</td>
<td>-82</td>
<td>-44</td>
<td>-57</td>
</tr>
<tr>
<td>67</td>
<td>-82</td>
<td>-43</td>
<td>-57</td>
<td>68</td>
<td>-83</td>
<td>-42</td>
<td>-69</td>
<td>69</td>
<td>-75</td>
<td>-42</td>
<td>-69</td>
</tr>
<tr>
<td>70</td>
<td>-75</td>
<td>-41</td>
<td>-69</td>
<td>71</td>
<td>-77</td>
<td>-41</td>
<td>-69</td>
<td>72</td>
<td>-58</td>
<td>-42</td>
<td>-69</td>
</tr>
<tr>
<td>79</td>
<td>-49</td>
<td>-40</td>
<td>-56</td>
<td>80</td>
<td>-49</td>
<td>-41</td>
<td>-56</td>
<td>81</td>
<td>-48</td>
<td>-44</td>
<td>-56</td>
</tr>
<tr>
<td>82</td>
<td>-48</td>
<td>-50</td>
<td>-55</td>
<td>83</td>
<td>-45</td>
<td>-50</td>
<td>-55</td>
<td>84</td>
<td>-45</td>
<td>-53</td>
<td>-56</td>
</tr>
<tr>
<td>85</td>
<td>-45</td>
<td>-44</td>
<td>-56</td>
<td>86</td>
<td>-48</td>
<td>-44</td>
<td>-56</td>
<td>87</td>
<td>-53</td>
<td>-44</td>
<td>-56</td>
</tr>
<tr>
<td>91</td>
<td>-63</td>
<td>-50</td>
<td>-57</td>
<td>92</td>
<td>-68</td>
<td>-50</td>
<td>-57</td>
<td>93</td>
<td>-72</td>
<td>-52</td>
<td>-57</td>
</tr>
<tr>
<td>94</td>
<td>-72</td>
<td>-54</td>
<td>-57</td>
<td>95</td>
<td>-46</td>
<td>-54</td>
<td>-57</td>
<td>96</td>
<td>-46</td>
<td>-54</td>
<td>-57</td>
</tr>
<tr>
<td>100</td>
<td>-50</td>
<td>-56</td>
<td>-56</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 8.1 Signal strength variation measured in different speed.

High signal fluctuation can be a problem when using signal strength to calculate the distance between MS and BS. As explained in Chapter 6, averaging the signal strength for a fixed time period can improve the signal strength measurement. If the signal strength varies too much, the average signal strength calculated will have errors. As it can be seen from Table 8.1 and Figure 8.1, signal measurements measured at 40 Km/h has acceptable signal variation but at 120 and 80 Km/h signal variation is too high and will produce inaccurate signal measurements specially when averaged. In this research no experiment was conducted in Maldives to find out the error introduced by the speed of the MS on its location. This is because in Maldives the speed limit is 30Km/h.

Based in the speed test conducted in Malaysia, it can be concluded that the accuracy of the MS location will depend on the speed of the MS. It can also be concluded that most accurate MS location can be calculated when MS has less motion or with no motion.
8.3 TIMING ADVANCE MEASUREMENTS

8.3.1 Reliability of timing advance

Measurements were taken to test the reliability of TA. The measurement of TA from servicing BS and the actual location of the MS was recorded. The actual distance calculated is compared with the distance calculated by TA in Figure 8.2.

TA value calculated by the network is meant to be accurate. As it can be seen from the Table 8.2 & Figure 8.2 the actual distance measured by the GPS falls in to the TA band identified by the TA measurement. It is also noticed that even though TA value is a value between 0 and 63, in all measurements that were taken during the experiment TA remains below 22. In order to study the behaviour of TA within the areas that are poorly covered or areas which has higher TA value more experiments need to be conducted.

<table>
<thead>
<tr>
<th>Actual Timing Advance (TA) value</th>
<th>Distance Represented by TA Value</th>
<th>Actual (Kilometer) measured by GPS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From Base Station (Km)</td>
<td>To Base Station (Km)</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>2</td>
<td>0.825</td>
<td>1.375</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>1</td>
<td>0.275</td>
<td>0.825</td>
</tr>
<tr>
<td>3</td>
<td>1.375</td>
<td>1.925</td>
</tr>
<tr>
<td>3</td>
<td>1.375</td>
<td>1.925</td>
</tr>
<tr>
<td>2</td>
<td>0.825</td>
<td>1.375</td>
</tr>
<tr>
<td>2</td>
<td>0.825</td>
<td>1.375</td>
</tr>
</tbody>
</table>
In highway and urban area there is a dominating TA value. In highway TA value 2 is roughly 60% and in urban area TA value 1 is 75%. In sub-urban area TA values up to 22 was measured and there is no major dominating value. This shows in sub-urban areas cells are bigger than urban areas and highways. This is possibly because of the less population in sub-urban. Table 8.3 & Figure 8.3 shows percentage of TA values measured during the experiment.

Table 8.3
Percentage of TA value recorded in different areas.

<table>
<thead>
<tr>
<th>Timing Advance (TA) Value</th>
<th>Highway (%)</th>
<th>Sub-Urban (%)</th>
<th>Urban (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>75</td>
</tr>
<tr>
<td>2</td>
<td>58</td>
<td>18</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>31</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>30</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Figure 8.3 Percentage of TA values recorded.

If TA is used to locate MS location, the accuracy of MS location will depend on the cell size. The TA band identified within each cell sector gets bigger as it moves away from the BS. Since highway and urban area records average TA value of 1 and 2 respectively, accuracy of MS location will be better in these two areas than sub-urban area.

8.3.2 Possible applications using Timing Advance

Timing advance can locate MS with an accuracy of 550 meters band within the cell sector. Since TA is part of GSM network operation and it will be always available as long as the connection between MS and BS exist, TA can be the last resort to calculate MS location when every other location means fails.

Location calculated using TA method can still be used in many applications. From the services described in Chapter 3, few need very accurate location. Service like Location Based Charging, Enhanced Call Routing, Location Dependent Content Broadcast, Mobile Yellow Pages and Location Based Information Services can still be implemented using TA method mentioned.
8.4 SIGNAL STRENGTH

Signal strength was recorded for urban and sub-urban area in Maldives as discussed in Chapter 7. In all areas the average number of neighbouring antennas is seven. The speed at which the measurement was taken is 30 km/h.

8.4.1 Distance calculating using signal Strength

Distance between MS and BS were calculated offline after measuring the signal strength in selected roots in Male’. Measurements were also taken in sub-urban area around Male. Calculations were very limited since the network service provider provided only information about 29 BS.

Hata model discussed in Chapter 5 is used in calculating the distance between MS- BS. Table 8.4 and Figure 8.4 shows the actual distance and the calculated distance using this model. The distance calculated using this model has an average error of about 250 meters. As it can be seen in Figure 8.5 distance error varies between 0 to 600 meters.
Table 8.4
Actual distance and the calculated distance with error measurements using Hata model.

<table>
<thead>
<tr>
<th>Samples</th>
<th>Distance (Meter) From Base station</th>
<th>Error in Meter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actual</td>
<td>Calculated</td>
</tr>
<tr>
<td>1</td>
<td>767.45</td>
<td>555.00</td>
</tr>
<tr>
<td>2</td>
<td>732.03</td>
<td>900.00</td>
</tr>
<tr>
<td>3</td>
<td>318.17</td>
<td>253.91</td>
</tr>
<tr>
<td>4</td>
<td>723.20</td>
<td>502.00</td>
</tr>
<tr>
<td>5</td>
<td>850.00</td>
<td>640.00</td>
</tr>
<tr>
<td>6</td>
<td>824.28</td>
<td>720.00</td>
</tr>
<tr>
<td>7</td>
<td>648.37</td>
<td>880.00</td>
</tr>
<tr>
<td>8</td>
<td>650.47</td>
<td>465.06</td>
</tr>
<tr>
<td>9</td>
<td>261.71</td>
<td>110.00</td>
</tr>
<tr>
<td>10</td>
<td>307.97</td>
<td>742.24</td>
</tr>
<tr>
<td>11</td>
<td>727.09</td>
<td>726.80</td>
</tr>
<tr>
<td>12</td>
<td>727.09</td>
<td>568.91</td>
</tr>
<tr>
<td>13</td>
<td>644.54</td>
<td>1,010.00</td>
</tr>
<tr>
<td>14</td>
<td>644.54</td>
<td>910.00</td>
</tr>
<tr>
<td>15</td>
<td>257.86</td>
<td>665.00</td>
</tr>
<tr>
<td>16</td>
<td>662.43</td>
<td>445.10</td>
</tr>
<tr>
<td>17</td>
<td>307.97</td>
<td>850.00</td>
</tr>
<tr>
<td>18</td>
<td>725.78</td>
<td>303.19</td>
</tr>
<tr>
<td>19</td>
<td>1,600.00</td>
<td>950.00</td>
</tr>
<tr>
<td>20</td>
<td>1,700.00</td>
<td>1,500.00</td>
</tr>
<tr>
<td>21</td>
<td>900.00</td>
<td>1,020.00</td>
</tr>
<tr>
<td>22</td>
<td>1,200.00</td>
<td>990.00</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.4 Actual distance compared with the distance calculated using Hata model.
Figure 8.5 Error compared with actual distance and distance calculated with Hata Model and the average error.

8.4.2 Triangulating MS Location using the MS-BS distance

Experimental result of distance between MS and BS calculated using signal strength measurement was used to triangulate MS location. The method described in chapter 5 is used to triangulate MS location. As described in chapter 5, to triangulate MS location it is necessary to have distance from three BS. Because of the limitation of information, among the nine hundred measurements taken on the field there were only eight measurements that has all the information necessary to perform triangulation. These eight measurements have information for all the neighbouring base stations and the servicing base stations.
Table 8.5
Actual GPS location compared with calculated location using three BTS and its location error.

<table>
<thead>
<tr>
<th>Samples</th>
<th>Latitude (GPS Location)</th>
<th>Longitude (GPS Location)</th>
<th>Latitude (Calculated Location)</th>
<th>Longitude (Calculated Location)</th>
<th>Location Error (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.876</td>
<td>73.198</td>
<td>4.760</td>
<td>73.400</td>
<td>232.938</td>
</tr>
<tr>
<td>2</td>
<td>4.837</td>
<td>73.198</td>
<td>4.890</td>
<td>73.180</td>
<td>55.846</td>
</tr>
<tr>
<td>3</td>
<td>4.162</td>
<td>73.198</td>
<td>4.400</td>
<td>73.300</td>
<td>259.094</td>
</tr>
<tr>
<td>4</td>
<td>4.830</td>
<td>73.202</td>
<td>4.700</td>
<td>73.400</td>
<td>236.863</td>
</tr>
<tr>
<td>5</td>
<td>4.122</td>
<td>73.186</td>
<td>4.220</td>
<td>73.400</td>
<td>234.883</td>
</tr>
<tr>
<td>6</td>
<td>4.980</td>
<td>73.277</td>
<td>5.200</td>
<td>73.270</td>
<td>220.108</td>
</tr>
<tr>
<td>7</td>
<td>4.759</td>
<td>73.237</td>
<td>4.950</td>
<td>73.400</td>
<td>250.838</td>
</tr>
<tr>
<td>8</td>
<td>4.760</td>
<td>73.235</td>
<td>5.000</td>
<td>73.420</td>
<td>303.271</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>224.230</td>
</tr>
</tbody>
</table>

As it can be seen in Figure 8.6 and Table 8.5, accuracy of MS location is within 300 meter or less than one housing block and average error is about 225 meter. The accuracy provided by using only three BS is still accurate enough to be used in many applications described in Chapter 3 and it is much more accurate than TA method.
8.5 PROPOSED LOCATION PROCESSING MODEL (LPM)

The result after calculating MS-BS distance using the Hata Model for each neighbouring and servicing BS for the above mentioned eight measurements from the field is used to test the performance of the model proposed in Chapter 6.

Among the seven distances calculated from the signal strengths for each measurement, three most accurate MS-BS distances is first used in processing MS location. Similarly the five most accurate MS-BS distances is used in processing MS location. Finally all seven MS-BS distance is used in processing MS location. The result after processing MS location using three, five and seven MS-BS distance is shown in Figure 8.7. Table 8.6, Table 8.7, Table 8.8 shows the MS location from GPS and calculated MS location together with its location error using 3, 5, 7 base station. As it can be seen in Figure 8.7 most of the time the accuracy of the MS location improves when more base stations are used. In some measurements the accuracy improves 60% when seven BS are used compared to three. There are also measurements that increase error after processing with seven BS but this increase in error is very minor.
Table 8.6
Actual GPS location compared with calculated location using three BTS and its location error.

<table>
<thead>
<tr>
<th>Samples</th>
<th>Lat</th>
<th>Long</th>
<th>Lat</th>
<th>Long</th>
<th>Location Error (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS Location</td>
<td>Calculated Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4.876</td>
<td>73.198</td>
<td>4.760</td>
<td>73.400</td>
<td>232.938</td>
</tr>
<tr>
<td>2</td>
<td>4.837</td>
<td>73.198</td>
<td>4.890</td>
<td>73.180</td>
<td>55.846</td>
</tr>
<tr>
<td>3</td>
<td>4.162</td>
<td>73.198</td>
<td>4.400</td>
<td>73.300</td>
<td>259.094</td>
</tr>
<tr>
<td>4</td>
<td>4.830</td>
<td>73.202</td>
<td>4.700</td>
<td>73.400</td>
<td>236.863</td>
</tr>
<tr>
<td>5</td>
<td>4.122</td>
<td>73.186</td>
<td>4.220</td>
<td>73.400</td>
<td>234.883</td>
</tr>
<tr>
<td>6</td>
<td>4.980</td>
<td>73.277</td>
<td>5.200</td>
<td>73.270</td>
<td>220.108</td>
</tr>
<tr>
<td>7</td>
<td>4.759</td>
<td>73.237</td>
<td>4.950</td>
<td>73.400</td>
<td>250.838</td>
</tr>
<tr>
<td>8</td>
<td>4.760</td>
<td>73.235</td>
<td>5.000</td>
<td>73.420</td>
<td>303.271</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>224.230</td>
</tr>
</tbody>
</table>

Table 8.7
Actual GPS location compared with calculated location using five BTS and its location error.

<table>
<thead>
<tr>
<th>Samples</th>
<th>Lat</th>
<th>Long</th>
<th>Lat</th>
<th>Long</th>
<th>Location Error (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS Location</td>
<td>Calculated Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4.876</td>
<td>73.198</td>
<td>4.866</td>
<td>73.400</td>
<td>202.247</td>
</tr>
<tr>
<td>2</td>
<td>4.837</td>
<td>73.198</td>
<td>4.800</td>
<td>73.180</td>
<td>40.973</td>
</tr>
<tr>
<td>3</td>
<td>4.162</td>
<td>73.198</td>
<td>4.310</td>
<td>73.200</td>
<td>148.019</td>
</tr>
<tr>
<td>4</td>
<td>4.830</td>
<td>73.202</td>
<td>4.800</td>
<td>73.400</td>
<td>200.260</td>
</tr>
<tr>
<td>5</td>
<td>4.122</td>
<td>73.186</td>
<td>4.180</td>
<td>73.300</td>
<td>127.414</td>
</tr>
<tr>
<td>6</td>
<td>4.980</td>
<td>73.277</td>
<td>4.800</td>
<td>73.270</td>
<td>180.132</td>
</tr>
<tr>
<td>7</td>
<td>4.759</td>
<td>73.237</td>
<td>4.800</td>
<td>73.380</td>
<td>148.377</td>
</tr>
<tr>
<td>8</td>
<td>4.760</td>
<td>73.235</td>
<td>4.700</td>
<td>73.400</td>
<td>175.946</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>152.921</td>
</tr>
</tbody>
</table>
Table 8.8
Actual GPS location compared with calculated location using seven BTS and its location error.

<table>
<thead>
<tr>
<th>Samples</th>
<th>GPS Location</th>
<th>Calculated Location</th>
<th>Location Error (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Latitude</td>
<td>Longitude</td>
<td>Latitude</td>
</tr>
<tr>
<td>1</td>
<td>4.876</td>
<td>73.198</td>
<td>4.872</td>
</tr>
<tr>
<td>2</td>
<td>4.837</td>
<td>73.198</td>
<td>4.800</td>
</tr>
<tr>
<td>3</td>
<td>4.162</td>
<td>73.198</td>
<td>4.250</td>
</tr>
<tr>
<td>4</td>
<td>4.830</td>
<td>73.202</td>
<td>4.800</td>
</tr>
<tr>
<td>5</td>
<td>4.122</td>
<td>73.186</td>
<td>4.150</td>
</tr>
<tr>
<td>6</td>
<td>4.980</td>
<td>73.277</td>
<td>4.900</td>
</tr>
<tr>
<td>7</td>
<td>4.759</td>
<td>73.237</td>
<td>4.800</td>
</tr>
<tr>
<td>8</td>
<td>4.760</td>
<td>73.235</td>
<td>4.700</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.7 Accuracy of MS location after processing using the proposed model for different number of MS-BS measurements

It is also noted during the calculation, MS location that are 50m off the TA sector band of servicing BS should be considered when calculating averagMS location. By doing so it improves the accuracy of MS location specially those MS location that falls around the boundaries of TA sector. If all seven neighbouring BS are available, by using this method it is possible to get the MS location with in 100 meter.
As explained in Chapter 6, this method works with a minimum neighbouring BS of two but accuracy varies depending on the number of neighbouring BS. During this experiment it has been recorded that all the measurements has seven neighbouring BS and it is assumed that there will be at least two neighbouring BS available most of the time. Thus MS can be located within 250 meter in the rural or badly covered area.
CHAPTER 9

CONCLUSION

In this research mobile hand phone network was thoroughly studied with the intention of identifying the ways of implementing location service in the current mobile network with minimum investment. Possible features and functions which are already available in the networks which can facilitate the mechanism of location service were identified.

Method of location techniques was studied. It includes techniques that use the signal travelling time, angle of the receiving signal and signal attenuation factor when travelling between mobile station and base stations. Because signal strength measurements are already measured by the network and the mobile stations, it is been concluded that the signal attenuation factor is the only method that can minimise the implementation cost compared to other methods.

9.1 PROPOSED SOLUTIONS

In order to locate MS location, distance between MS and BS has to be calculated. Since signal attenuation factors have been selected as the method to calculate the MS–BS distance. Various propagation path loss models were studied. Hata model, a model evolved from Okumura Model was selected as the best propagation model to calculate the MS–BS distance. Using these MS-BS distance, a mathematical triangulation model was introduced to identify the location of MS. This model identifies the MS location with certain accuracy.
In order to make the calculated location of MS accurate and reliable a new model to process the location was proposed. This model is called Location Processing Model (LPM). This model uses the result from the triangulation combined with the additional information available in the network to produce a much improved result compared to non-processed result and network based location results. Final result of MS location from this model can also estimate the accuracy level.

This work also highlights the possible techniques to implement and present location service to the users. Proposed implementing method is a client server based system with an additional location server at the network side as a server and MS as the client. In order to minimise the changes to the network this work identifies and propose an information collecting point in the system. The proposed collecting point is the Operations and Maintenance Centre (OMC) and identifies the possible useable commands in the GSM system that can be used in gathering necessary information to process the location of MS.

Since the proposed method does not require changes to the network except an additional server, the initial investment can be very minimum.

In order to test the work discussed in this research, an experimental investigation was carried out. Data gathered from the experiment was processed to find out the effect of mobile station speed on location method. This data was also used to investigate the location error when using proposed location method and the effectiveness of the proposed location processing model.
9.2 **EXPERIMENT**

Experiments were conducted on real mobile network and data were gathered. The result of this data was used to calculate the MS–BS distance using the path loss model.

Result from path loss model based on Hata model found to be in good agreement with the theoretical work. The MS location using the triangulation models together with the resulting MS-BS distance calculated using Hata model produce an accuracy of 300 meter. This is a better result than using TA and CI. Resulting MS location using triangulation when used with proposed LPM produce an accuracy of 100 meter. This result is considered as a very promising result.

9.2.1 **Proposed Location Processing Model (LPM)**

The result produces by location processing model out perform TA, TA sector and CI method. From the experiments performed it is clearly seen accuracy of this model improves by the number of neighbouring BSs used.

The drawback of this model will be the processing that it required in order to come up with the best possible location of MS. Depending on the number of neighbouring BS available, this process will require comparing and processing lots of information in order to get the best possible solution.
9.3 CONTRIBUTIONS

As explained in Chapter 1, the main objective of this research is to propose a method that can locate any GSM mobile hand phone with minimum implementation cost. This research has explained detail step by step method that is needed to locate the MS and implement location service in current mobile network.

This work also proposes a completely new approach in processing MS location. The proposed model produces an accuracy of 100 meter. The result from this model can give the accuracy level together with the MS location. This model is not only applicable for processing MS location using signal strength but it can also be used in processing MS location using TOA method too.

Accuracy of 100 meter can be considered very promising result when compared with other similar works based on signal strength.

9.4 PROBLEMS FACED

Getting the required information from the mobile service providers was very difficult because of the nature of the information. The required information seems to be confidential and this information is kept as a secret among the networks. This was one of the reasons why the network service providers rejected our request for the information. Among the networks approached for this information were all the networks from Malaysia.
After months of correspondence and requests to various mobile telecommunication companies, only one company accepted our request to provide the much needed information. It was a telecommunication company from Maldives called Dhiraagu who was willing to share some limited information from their network with us. Information provided by Dhiraagu was just enough to complete part of the experiments that was initially planned.

In order to do a complete test on the theoretical work discussed in this research, much more help will be needed from the service provider.

9.5 RECOMMENDATION FOR FUTURE WORK

As mentioned in Chapter 6, this thesis outlines the foundation method of implementing location service in GSM network. Using signal strength to locate MS location is the cheapest method since the information required is already available in the network. But signal strength has lots of limitations; there are many ways to improve the accuracy of the method, specially using filtering techniques. Result from the location processing model can still be improved by using these filters. These techniques need to be studied to improve the accuracy of the location technologies.

Presentation of location information in hand sets is also needed to be investigated further. It is not an option to ask mobile users to change the hand sets to subscribe for the service therefore it is very important to find ways to provide the location service to every mobile device in the network. Currently almost all the handsets in the market cater for WAP service. Studies on how to implement location service over WAP
protocol needs to be studied, especially a way to implement geographical information service (GIS) over WAP.

Implementing LBS will only be a part of the overall problem. Location security, location inter operability among different networks and location roaming are also needs to be addressed and studied before any commercial implementation of LBS.


ETS GSM 03.02 (1996). Digital cellular telecommunications system (Phase 2); Network architecture.
ETS GSM 03.03 (1995). Digital cellular telecommunications system (Phase 2); Numbering, Addressing and Identification.

ETS GSM 03.19 (1998). Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™. Version 7.1.0 Release 1998

ETS GSM 03.22 (1997). Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode. Version 6.0.0 Release 1997

ETS GSM 03.71 (1998), Digital cellular telecommunications system (Phase 2+), Location Services (LCS), (Functional description) - Stage 2; (GSM 03.71 version 7.4.0 Release 1998)


ETS GSM 05.10 (1996). Digital cellular telecommunications system (Phase 2); Radio subsystem synchronization. Version 4.9.0 Release November 1996

ETS GSM 07.07 (1999). Digital cellular telecommunications system (Phase 2); AT command set for GSM Mobile Equipment (ME) (GSM 07.07 version 4.4.1)

ETS GSM 09.02 (1997). Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) version 6.8.0 Release 1997

ETS GSM 12.08 (1998). Digital cellular telecommunications system (Phase 2); Subscriber and equipment trace. February 1998

ETS GSM 12.20 (1996). Digital cellular telecommunications system (Phase 2); Base Station System (BSS) Management Information.

ETS GSM 3.38 (1998). European digital cellular telecommunications system (Phase 2); Alphabets and language-specific information.

ETS GSM 80.08 (1998). Digital cellular telecommunications system (Phase 2+); Mobile-service Switching Center – Base Station System (MSC – BSS) interface; Layer 3 version 4.12.1, October 1998


References


White House (2000). press release on 1 May 2000 “Statement by the president regarding the united states decision to stop degrading global positioning system accuracy”


