LCS Capable GSM Network

TEJAS OZA
Abstract

LCS Capable GSM Network

TEJAS OZA

This thesis is about Location Based Services which intends to acquire the location of the mobile phone. The goal of our thesis project is to extend the Mobile Switching Centre and Base Station Controller with location based support which is a part of the Global System for Mobile Communications that follows the 3rd Generation Partnership Project standards and integrate with the Mobile Arts Home Location Register, Gateway Mobile Location Centre and Serving Mobile Location Centre. To achieve this goal the prototype of LCS capable GSM network will be implemented using the functional programming language Erlang/OTP and C programming language. Further for testing and verification, tests will be performed until in the final result the location of mobile phone is obtained.
Acknowledgments

I am glad to have this opportunity to express my gratitude to all who assisted during the entire course of my thesis project.

I would like to express special gratitude to my supervisor Christian Rohner of Uppsala University for his patience and motivation. His aspiring guidance helped me in writing and completion of this thesis.

I appreciate Mobile Arts AB for giving this opportunity by having belief in us and we are glad to finish our thesis at MA with all testing needed for proof of concept. I am grateful to Mobile Art’s AB supervisors Hao Zhang and Robert Andersson who provided their great support, encouragement and thoughtful feedback during thesis work. They helped us for setting up lab environment and different GSM components.

I would like to thank my thesis partner Tobias Vehkajärvi for working with me as good team mate. He provided his support and guidance whenever required.
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station Controller</td>
</tr>
<tr>
<td>BSS</td>
<td>Base Station System</td>
</tr>
<tr>
<td>BSSAP</td>
<td>BSS Application Part</td>
</tr>
<tr>
<td>BSSMAP</td>
<td>BSS Management Application Part</td>
</tr>
<tr>
<td>BTS</td>
<td>Base Transceiver Station</td>
</tr>
<tr>
<td>CC</td>
<td>Connection Confirm</td>
</tr>
<tr>
<td>CM</td>
<td>Connection Management</td>
</tr>
<tr>
<td>CR</td>
<td>Connection Request</td>
</tr>
<tr>
<td>CREF</td>
<td>Connection Refuse</td>
</tr>
<tr>
<td>DA</td>
<td>Destination Address</td>
</tr>
<tr>
<td>DTAP</td>
<td>Direct Transfer Application Part</td>
</tr>
<tr>
<td>DT1</td>
<td>Data form 1</td>
</tr>
<tr>
<td>DT2</td>
<td>Data form 2</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communication</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IT</td>
<td>Inactivity Test/Timer</td>
</tr>
<tr>
<td>LM</td>
<td>Location Management</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobile Application Part</td>
</tr>
<tr>
<td>MO</td>
<td>Mobile Originating</td>
</tr>
<tr>
<td>MM</td>
<td>Mobility Management</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Centre</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Terminating</td>
</tr>
<tr>
<td>OA</td>
<td>Originating Address</td>
</tr>
<tr>
<td>OTP</td>
<td>Open Telecom Platform</td>
</tr>
<tr>
<td>RLC</td>
<td>Release Complete</td>
</tr>
<tr>
<td>RLSD</td>
<td>Released</td>
</tr>
<tr>
<td>RR</td>
<td>Radio Resource</td>
</tr>
<tr>
<td>SCCP</td>
<td>Signalling Connection Control Part</td>
</tr>
<tr>
<td>SMS</td>
<td>Short message Service</td>
</tr>
<tr>
<td>SMSC</td>
<td>Short Message Service Centre</td>
</tr>
<tr>
<td>SS7</td>
<td>Signaling System 7</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary Mobile Subscriber Identity</td>
</tr>
<tr>
<td>UDT</td>
<td>Unitdata</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor Location Register</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Subscriber Integrated Services Digital Network</td>
</tr>
<tr>
<td>MTP</td>
<td>Message Transport Part of SS7</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switch Telephone Network</td>
</tr>
</tbody>
</table>
## Contents

1 **Introduction** .................................................. 3  
   1.1 Project Overview ........................................... 3  
   1.1.1 Location Based Services ................................. 3  
   1.1.2 Types of location estimate methods .................... 3  
   1.1.3 Cellular Systems ....................................... 4  
   1.2 Project Background ......................................... 5  
   1.3 Project Scope ............................................... 6  
   1.4 Problem Statement ......................................... 6  
   1.5 Goals and Motivation ....................................... 6  
   1.6 Planning .................................................. 7  
   1.7 Contributions ............................................... 7  

2 **Technical Background** ....................................... 8  
   2.1 Introduction to GSM Network ................................ 8  
   2.1.1 Mobile Station (MS) .................................... 8  
   2.1.2 Base Station Subsystem (BSS) ........................... 8  
   2.1.3 Network Switching Subsystem (NSS) .................... 8  
   2.1.4 Serving Mobile Location Centre (SMLC) ............... 9  
   2.1.5 Gateway Mobile Location Centre (GMLC) ............. 9  
   2.1.6 Proxy Mobile Location Centre (XMLC) ............... 9  
   2.2 GSM Network Background .................................. 10  
   2.2.1 GSM - Protocol Stack ................................... 10  
   2.2.2 Interface between GSM Components ..................... 11  
   2.3 Related Work ............................................ 12  

3 **Technical Solution** .......................................... 14  
   3.1 Methodology ............................................... 14  
   3.2 System Design ............................................. 14  
   3.2.1 Network Architecture .................................. 15  
   3.2.2 System Architecture .................................... 18  
   3.2.3 Provide Subscriber Location Procedure ................ 19  
   3.2.4 State Machine for Provide Subscriber Location in MSC 30  
   3.2.5 Location Update Procedure ............................. 31  
   3.2.6 State Machine for Location Update Procedure in MSC 33  

4 **System Deployment and Testing** ............................. 34  
   4.1 Deployment of nanoBTS .................................... 34  
   4.1.1 Configuration steps for connecting nanoBTS with your Computer 34  
   4.2 Deployment of TCP Server/Client .......................... 35  
   4.3 Deployment of OpenMSC .................................... 36  
   4.4 Deployment of GMLC, SMLC, HLR .......................... 36  
   4.5 Deployment of SS7 Stack ................................... 36  
   4.6 Testing Methods (BLACK BOX Testing) ................... 37  
   4.7 Results .................................................. 47  

5 **Future Work** ................................................ 48  
   5.1 Voice Call ................................................ 48  
   5.2 AGPS functionality ......................................... 48  

6 **Conclusion** .................................................. 49  

7 **References** .................................................. 50
Appendices

8.1 Deployment of OpenBSC
1 Introduction

1.1 Project Overview

This thesis is about Location Based Services (LBS) in Mobile Cellular Networks where this service provides the current location of the user or Mobile Phone by various methods e.g. Cell-ID, TA-NMR, TOA, E-OTD and AGPS. In this thesis Cell-ID based method is used to obtain the location of mobile phone.

1.1.1 Location Based Services

LBS provides information about the location of an entity and is widely used in social networking and emergency services. These services are easily integrated in the mobile applications of Smart phones and Tablets, where it is used for entertainment, social networking etc. In real-time systems it is used for vehicle tracking, stolen assets tracking, finding position for criminal, emergency services etc.

Some real-time applications of location-based services are:

- Sending alerts for social gathering and events in a city
- Finding nearest service, e.g. restaurant, bank, food store, cinema etc
- On-line games where you can find friends from different locations
- To navigate address and also current position with distance from the current address
- Finding people from mobile applications via LBS Service and display position on the same mobile.
- Up to date information for temperature, traffic services etc
- Stolen phones, computers etc can be tracked.

1.1.2 Types of location estimate methods

Location or distances between two devices, can be estimated using different technologies including beacon information or following basic physical laws such as velocity and attenuation of electromagnetic waves.

- **Cell Global Identity (CGI)**: This parameter gives the current cell location of the target MS. The format shall either be the cell global identification or the Location Area Code (LAC) plus Cell Identity (CI) form. LAC indicates the Cell Identity of the particular Base Transceiver Station (BTS). The purpose of the Cell Identity value is to identify a BTS/cell within a location area. Cell Identifier message may also contain Mobile Country Code (MCC) plus Mobile Network Code (MNC). These parameters of Cell ID received in early classmark3 message is used by SMLC to calculate the estimate position of Mobile Phone.

- **Timing Advance (TA)**: This is one of the known methods to calculate the location of MS where the time is calculated for the signal transfers from MS to the base station. TA values are generally between 0 to 63. To fetch the TA value, a TA-request is sent to MS where MS is unaware of it i.e no ringing tone or any alert and in response Cell-ID of serving cell and TA value is returned.

- **Time of Arrival (TOA)**: This method requires three LMU (Location Measurement Unit) where the main logic is that the signal is sent from MS to three measurement units, when MS enters the region of LMU’s (where the geographical co-ordinates in LMU is already known) and after receiving the signals at LMU’s the position is calculated on the basis of hyperbolic triangulation method.

- **E-OTD**: The E-OTD method needs at least three BTS’s where the main logic is to calculate position with Observed Time Difference. The signal received from BTS in case of the synchronized networks normal and dummy bursts can be used and for the unsynchronized networks the RTD real time difference is calculated from at least 3 BTS’s where the MS measures relative time of arrival of these signals.
• **Assisted GPS**[^4] AGPS provides the most accurate position of an entity which is approximate in 10 meters range but depends on several conditions like MS compatibility, clear sky visibility with healthy satellites in range etc. where the basic logic is to calculate the position from radio signals sent by satellite to receiver and in our case the MS. During assistance data delivery to get more accurate position the MS could ask additional assistance data like differential GPS correction, approximate handset location or cell based location from SMLC. If the position is calculated at a network where in our case SMLC then it is called as MS-Assisted Method and when the position is calculated at MS then it is called as MS-Based method. For extended part of the thesis both MS-Assisted and MS-Based have been tested and later in the chapters detail description can be found.

1.1.3 **Cellular Systems**

This thesis is done by two students where my colleague was from Göteborg University. Therefore the thesis was divided into 2 parts a) MAP[^9] part and b) BSSMAP[^3] part. This report is based on the BSSMAP part of GSM network architecture which is shown in Fig 1 with dotted line. Later when my thesis partner left then I had to do some development at MAP part also to finish the thesis.

![Fig 1 Basic GSM Architecture](image)

By referring to the figure above to locate a subscriber or a mobile phone, the SLIR (Standard Location Immediate Request) in xml format is triggered from XMLC and after converting it to Erlang[^11] record, it is forwarded to the GMLC. The GMLC then sends Send Routing Info for LCS-REQ to HLR[^9] to ask which MSC the MSISDN[^9] belongs to and after receiving the MSC address, the GMLC sends Provide Subscriber Location Request(PSL) to the MSC. The MSC after recognizing the PSL, sends a paging request to the Mobile Station via BSC and waits for the paging response. After the MSC recieves the paging response, it encapsulates the Cell Identity parameters which is received in an early classmark3 message from Mobile Station plus mandatory parameters received in PSL like MSISDN or IMSI[^9], Location Type, Location Age etc. into BSSMAP Perform Location Request and sends to the BSC. When the BSC receives request from MSC for Location Information about a specific mobile station, then BSC recognize if the received information is BSSMAP Location Request and if so then transmits the data to/from SMLC from/to Mobile.
Station (handset) and receives the location response from the SMLC to send it back to the MSC which forwards it to the GMLC via SS7 communication. Then finally XMLC Client gets the location estimation of Mobile Station. In real time system the Location Request can be triggered by the client or Network Initiated and after the position of Mobile Station is calculated either by Cell-ID, Timing Advance (TA Method), TOA, E-TOD, AGPS and for our case the Cell-ID method was used where the final result in form of XML format can be seen on XMLC node. The result will be displayed with longitude and latitude coordinates which can be verified by putting these values in Google maps and cross check the result, which is explained in detail later in this report.

1.2 Project Background

During the thesis work Mobile Arts had provided nodes such as XMLC, GMLC, SMLC, HLR in the GSM (Global Systems for Mobile Communication) network. The thesis goal was to extend the OpenMSC which was built during Project CS 2010 course held at Uppsala University and OpenBSC which is open source project available on web is used as BSC where both systems need to be integrated to enable the Location Services. Also in the previous Project CS we used CNODE for communication between OpenBSC written in C and OpenMSC written in Erlang. But in the current thesis we replaced previously used CNODE with connecting node written in Erlang which is used to accept data from OpenBSC and forward it to OpenMSC and vice a versa. Hardware such as nano-BTS, ex-jobb laptops and mobile phones were provided by Mobile Arts as well. Also some systems like HLR, GMLC etc resided in Mobile Arts secured network premises so for these reasons the system developed for thesis which needed integration with Mobile Arts specified system’s, most of the work was done mainly at Mobile Arts AB premises in Stockholm.

Since Mobile Arts current LCS products (XMLC, GMLC, SMLC) and student project CS built MSC are all based on Erlang/OTP, this thesis shall also be mainly based on Erlang/OTP. In addition, some C coding was needed as the BSC is from an open source project called OpenBSC which is developed using C.
1.3 Project Scope

The scope of this thesis project is to build a LCS capable GSM radio network to provide the location estimate of a Mobile Station (MS) either through cell-based, Timing Advance (TA) and Assisted Global Positioning System (A-GPS) positioning methods that should communicate with already existing SMLC and GMLC with BSSAP-LE, BSSLAP, RRLP[5] protocols over the SS7. The SMLC node after receiving BSSAP-LE LCS message, calculates the position of MS and returns back the result to the MSC. The scope of the thesis can be described in sub goals as below:

- Support for Mobile Terminating Location Request (MT-LR[4])
- Support for Mobile Originating Location Request (MO-LR[4])(Optional)
- GSM CGI Location (CGI + TA(Optional) + NMR(Optional))
- GSM A-GPS[4] Location (MS-based, MS-assisted)(Optional)

1.4 Problem Statement

Location Based Services are becoming very popular now a days and are widely used in real life. Mobile Arts AB provides the solution for 2G, 3G and 4G Location Based Services where accuracy and quality of location estimate is directly co-related to mobile handsets. This thesis was proposed to basically implement LBS solution by extending existing Mobile Switching Center(MSC), Open Base Transceiver Station(OpenBSC), Application Program Interface(API) towards Gateway Mobile Location Center(GMLC) and Home Location Register(HLR). Also to implement Erlang node for communication between OpenBSC and Serving Mobile Location Centre(SMLC) and when implementation is done then tests are performed until we get the current location of the mobile phone.

1.5 Goals and Motivation

Main Goals

- Implementing additional functionality of existing MSC from previous Project CS course to support for Location Based Services in core GSM network.
- Extending existing open-source OpenBSC to support RRLP (Radio Resource Location Services Protocol) for communication between SMLC and Mobile Station.
- Adapt OpenBSC to support for BSSAP-LE (Base Station System Application Part – LCS Extension) protocol to communicate with SMLC.
- Implementing protocol stack for Location Based Services.
- Perform single test for the prototype built to achieve the location of the target mobile phone.

Others

- Understanding MA’s current exiting products GMLC, SMLC, HLR, SS7 communication. Encoding and decoding libraries for protocol parameters conversion and modify them to adapt the current traffic flow.
- SS7 stack support for communication between all nodes.
1.6 Planning

The thesis was structured into the following steps:

- Start-up period: (2 weeks) a. Studying relevant material b. Familiarizing with Mobile Arts development environment
- Approval of Requirement Specification: (2 weeks) Approval of Implementation Proposal: (2 weeks)
- Presentation of Intermediate University Report: (1 week)
- BSC support for BSSAP-LE: (2 weeks)
- BSC support for RRLP: (2 week)
- Integration with GSM core network and start testing prototype: (3 weeks)
- Verify Location Services OK in the GSM network prototype: (1 week)
- Remaining and any optional features: (1 week)
- Approval of Technical Report: (2 weeks)
- Approval of Final University Report: (2 week)

1.7 Contributions

Our solution for 2G helped a lot for testing of SMLC and different mobile phones, especially when AGPS functionality was added. This solution was also useful to see different behavior of the mobile phones during RRLP traffic flow and we can see how hardware and firmware of mobile phones affects the performance. Without this solution it was impossible to test SMLC behavior for LBS services. This is the complete network in box solution for 2G Location Based Services where it is currently used and will be used in the future where there are multiple opportunities to test old mobile phones and newly releasing mobile handsets for AGPS functionality.
2 Technical Background

2.1 Introduction to GSM Network

GSM stands for Global System for Mobile Communication which is a global standard used for communications in mobile networks. This standard was defined and developed by European Telecommunications Standards Institute (ETSI). GSM describes the protocols for digital cellular networks used by mobile phones, where in early days it was mainly defined as circuit-switched network optimized for full duplex voice telephony. Since year 2014 it has become the default global standard for mobile communications and expanded over period of time in cellular networks where it is widely used in several countries. The complete GSM network constitute of Base Station Subsystem(BSS), Network Switching Subsystem(NSS) and Mobile Station (MS) where details of these entities is described in following subsections.

2.1.1 Mobile Station (MS)

Mobile Station comprises of:

- **Mobile Equipment (ME):** The Mobile Equipment in general terms called as mobile phone, manufactured by several different companies now a days and each mobile phone is uniquely identified by an IMEI (International Mobile Equipment Identity).

- **Subscriber Identity Module (SIM):** Small smart card or chip which has unique International Mobile Subscriber Identity (IMSI) is used for identification and authentication in network topology worldwide. The function includes to send and receive calls or data and receive other subscribed services. While communicating with the network all data is encoded in binary form and send via air interface to the network. Usually the SIM is protected by PIN or password.

2.1.2 Base Station Subsystem(BSS)

Base Station Subsystem(BSS\(^9\)) constitute of Base Transceiver Station (BTS) and Base Station Controller (BSC) which together forms the cellular subsystem and is responsible for radio signal traffic handling and management between mobile station and network switching subsystem(NSS\(^9\)).

- **BTS\(^9\) (Base Transceiver Station):** BTS is responsible for transmitting and receiving of radio signals from MS through air interface and on other-side towards the BSC, forwards these signals after encryption and after receiving data from BSC responsible for decryption and forwards to MS.

- **BSC\(^9\) (Base Station Controller):** BSC is the main controller for radio signals between BTS and NSS. In general a single BSC can handle from few to hundreds of BTS. BSC is responsible for handling voice call, roaming, SMS transfer etc services. A single MSC can handle several BSC’s.

2.1.3 Network Switching Subsystem(NSS)

- **MSC \(^9\) (Mobile Switching Center):** MSC is the main component of GSM structure which acts as an switching center for MS. Whenever MS roams in inter and intra cellular area then via handover, MSC knows the details of MS. MSC’s are connected to outbound other MSC’s via GMSC(Gateway MSC). Generally MSC is connected to VLR, BSC, HLR and to PSTN\(^{15}\) (Public Switch Telephone Network) via ISDN\(^{15}\) (Integrated Services Digital Network).

- **HLR\(^9\) (Home Location Register):** HLR is the functional entity which is responsible for management of mobile subscribers. The main function of HLR is to store the latest location of each MS in need of routing of data. The HLR also stores IMSI, MSISDN, VLR number, MSC number etc.

- **VLR\(^9\) (Visitor Location Register):** A VLR can have control over one or more MSC areas and whenever the MS is roaming in particular area it sends location update request, then MSC sends this details to the VLR. VLR then stores IMSI, MSISDN, TMSI, classmark info, location of MS and supplementary services.
2.1.4 Serving Mobile Location Centre (SMLC)

An SMLC can be called as calculation engine and processing entity which has database to store cell data for specified area and by means of which SMLC is responsible for calculating geographic location of MS covered by respective BSC’s. While managing the location procedure, SMLC decides the positioning method e.g. cell-id based, TA-method, A-GPS depending on client request as shown below:

1. Cell-ID based:
   (a) Falls into low level accuracy
   (b) Default fallback method
   (c) Always works
2. TA- method:
   (a) Falls into medium level accuracy
   (b) Second level fallback method
   (c) Always works
3. AGPS:
   (a) Falls into high level accuracy
   (b) Most preferred method
   (c) Works under certain circumstances

An SMLC may be either BSS based SMLC or NSS based SMLC but our system in current thesis uses BSS based SMLC where BSC is connected to the MSC and SMLC. When MSC sends Location Request to the BSC, it forwards to the SMLC. If quality is satisfied by the parameters then SMLC sends location response otherwise fallback to cell-id based method and sends back location response.

2.1.5 Gateway Mobile Location Centre (GMLC)

The Mobile Arts GMLC is an advanced network positioning system, providing mobile operators with the ability to use a range of location techniques. The LCS clients sends location service (LCS) request to the GMLC and GMLC in turn asks HLR, to which MSC the MS is connected and then forwards it to that MSC. After receiving the LCS result the GMLC sends back this result to the LCS Client.

2.1.6 Proxy Mobile Location Centre (XMLC)

The Proxy Mobile Location Centre (XMLC) provides OMA (Open Mobile Alliance) and 3GPP compliant location and messaging gateway functionality. It supports the OMA Mobile Location Protocol (MLP 3.2), including Mobile Terminating (MT), Network Induced (NI) and Mobile Originating (MO) location methods, as well as Triggered Location reports. Furthermore, the XMLC supports the OMA Roaming Location Protocol (RLP) for location of subscribers roaming into and out of the operators’ network. The XMLC supports the definition of subscriber’s privacy data with regards to which 3rd party content providers and/or end-users are allowed to locate a subscriber. Finally, the XMLC provides functionality for message proxy.
2.2 GSM Network Background

This section describes the GSM protocols used in our thesis.

2.2.1 GSM - Protocol Stack

• IPA ip.access (Internet Protocol Access)
  IPA protocol ip.access,
  type: SCCP
  DataLen: 60
  Protocol: SCCP (0xfd)
  Internet Protocol Access (IPA) is used as a base for simple transfer of packets used for acknowledgment and connection management over Internet. When you start the OpenBSC with specifying the target MSC IP address and port, it continuously sends ping request to connect to the MSC. When MSC replies with pong then both systems are interconnected. BSC sends the next packet Identity Request and so on. For all this simple communication, binary packet is sent with IPA header. For our thesis as mentioned earlier we used TCP nodes written in Erlang to communicate and it sends all the packets with IPA as top layer header.

• SCCP
  SCCP stated as Signaling Connection Control Part resides at network layer with respect to OSI Model. The main role of SCCP is to provide control over the connections while keeping into consideration routing of packets using point code and global titles, flow control and segmentation of the packets. All these features of SCCP are extended provisions. As I discussed previously about BSSMAP protocol, SCCP is the main building block for communication of BSSMAP and DTAP messages, where in protocol layer SCCP comes above DTAP and BSSMAP. In Fig 2.2.1.a you can see detail SCCP message flow for Lb interface.

![Fig 2.2.1.a SCCP Message Flow on Lb Interface](image-url)
• BSSMAP-LE
The location request procedure which is applicable to the Lb interface makes use of SCCP connection oriented signaling. The main purpose of this procedure includes providing location estimate for target MS in dedicated mode and also LCS assistance data transfer which depends on the demand of Qos(Quality Of Service) and accuracy of coordinates. This request can be initiated by either serving BSC or the visited MSC for the MS, where the request is sent as an BSSMAP-LE Perform Location Request via Lb interface to the SMLC, where in response SMLC can send either BSSMAP-LE Perform Location Response or Perform Location Abort.

• BSSLAP
This protocol is used at Lb interface when SMLC sends BSSLAP TA- Request to MS and in response receives TA-Response or TA Layer 3.

• MAP (Mobile Application Part)
This Protocol resides at higher level and for our thesis this protocol is used to send MAP Provide Subscriber Location Request and MAP Provide subscriber Location Response towards MSC.

• SS7(Signaling System no. 7)
SS7 is the main backbone of the core network where it is widely used in wired and wireless communications. SS7 is mainly used for authentication, roaming facility, call setup and tear down. It also provides services as call forwarding, calling and called party information etc. In GSM network different network elements use SS7 signaling where they communicate over 56 or 64 kbps bidirectional channels called signaling links.

2.2.2 Interface between GSM Components

• Interface between BTS and BSC (Abis)
This is interface between Base Transceiver Station(BTS) and Base Station Controller(BSC) and for our thesis project we used nanoBTS where it connects with OpenBSC via Ethernet and communicates over IP.

• Interface between MSC and BSC(A-interface)
The main roles of this interface are BSS management, call handling and location management. For our system we support following services and in further section you will find more details of these functions.

- Communication with BSC via SCCP and BSSAP-LE over IPA and later SCCP.
- Support Mobile Terminating Location Request (MT-LR)
- (Optional) Support Mobile Originating Location Request (MO-LR)
- Support Location Update (LU)
- (Optional) Support Authentication
- (Optional) Support Ciphering
- (Extended) AGPS(RRLP Protocol)

• Interface between HLR and MSC (C interface)
When a subscriber makes a call and fixed network fails, then via respective interrogation procedure Gateway MSC retrieves the roaming number from the HLR. During mobile terminated short message service the SMS Gateway MSC retrieves serving MSC(where the MS is located) to forward the SMS. In our system we used this interface for location update where subscriber tries to connect to the network and subscriber management services like insert subscriber data and delete subscriber data. In following sections we will discuss more details about this interface.

• Interface between SMLC and BSC (Lb interface)
This interface is used when the network uses BSS based SMLC and same is used for our system. BSC
and SMLC uses this interface for location service procedure or handling location assistance data for targeted MS. Details on this interface and location procedure is specified in 3gpp documentation GSM 03.71 and GSM 09.31. Also this interface is used by SMLC for operation and management services as well as location measurement message transfer.

- **Interface between GMLC and MSC (Lg interface)**
  GMLC sends location request to the MSC via this interface and in the same way MSC uses this interface to send the location response to the GMLC.

- **Interface between GMLC and HLR (Lh interface)**
  When GMLC receives the location request from XMLC, the first step for GMLC is to find the respective MSC serving the target MS and to find this, GMLC uses Lh interface to ask the HLR about respective MSC number.

2.3 Related Work

Since early 2001 researchers were doing lot of work to improve location based services in 2G. Which included MS-Based/MS-Assisted AGPS, E-OTD and focus was to lower the number of messages and parameters in stand alone SMLC with smart intelligence in SMLC. During that time Cell ID and timing advance methods were still under study in GERAN LCS[19]. The GERAN LCS was concerned with changes to the overall architecture of LCS architecture of 3GPP Release 4.

They were discussing several scenarios for AGPS method as this method was providing faster time to radio-locate, higher signal sensitivity and better performance e.g. assistant data delivery during roaming of MS i.e. if MS can fetch the data from home or visiting network, mandatory fields at protocol level in network and MS side, roaming networks must support AGPS.

There were also some discussions[20] on comparing different Location estimate methods in GSM (2G) and UMTS (3G) where advantages and drawbacks for all the methods were compared. The new location estimate methods AOA and OTDOA (similar to GSM E-OTD method) were introduced in UMTS at that time, where the BTS was replaced with Node-B. The SRNC includes the required functionality of BSS/SMLC. It was found that the performance of both E-OTD and OTDOA was consistent and accuracy was better than CID but can lead to errors due to unfavorable BTS configurations and multipath. The AOA is expensive method and required installation of directional antennas[20]. The location of MS is calculated based on triangulation where MS should know at least two Node-B’s.

In this paper[20] it was found that Cell ID method is cost effective where the performance is limited. E-OTD/OTDOA is expensive to implement due to major changes in infrastructure. AGPS method has compatibility GSM and UMTS with good performance and much lower cost than E-OTD/OTDOA. To improve accuracy the hybrid method can be used e.g. AGPS with Cell-ID can provide better results in accuracy but requires smart logic in SMLC.

Wireless Local Area Networks is becoming very popular and widely used for Internet access for wireless enabled clients. In another research[21] for localizing in wireless network stated that this could lead to better accuracy concerning indoor scenario because there was always problem to get location estimate in indoor scenarios. The access point is the base station of Wi-Fi network. In wireless network the location of MS can be retrieved based on characteristics of the wireless signals received, power, time or angle of arrival[21]. This positioning i.e. positioning using Wi-Fi were considered to be cost efficient and highly useful for indoor positioning. In Cell-ID method client can estimate the closer access point by scanning the received radio beacons. Similarly TOA and TDOA perform the time measurements to calculate distance between Wi-Fi access points and client/user. One of the most common location techniques used for locating a client in Wi-Fi network is Received Signal Strength Indication (RSSI). Some of them are based on propagation model to translate signal power into distance i.e. to approximating the distance between Wi-Fi clients and access points as briefed earlier. Other method[21] is to store RSSI measurement in database where it is defined as empirical model. In general case the grid is created by dividing localizing area into smaller parts where each point in grid specify as several Wi-Fi signals from the neighboring access points this positioning technique is defined as RSSI fingerprinting[21].

The parameters such as time, interference, load in RSSI measurements, validity of mean RSSI measurement stored in database, number of access point involved can directly affect the location accuracy[21]. My
goal in this thesis work was more focused towards proof of concept i.e. system development, integration and testing for location services in GSM (2G). The approach I chose had been a part of previous studies/papers, however my thesis work is a specific solution that would fit to Mobile Arts product range with building complete LCS capable GSM network where it can be used for testing purposes.
3 Technical Solution

3.1 Methodology

In most of the software projects selection of proper software development methodology plays a vital role which directly affects the total software development process of project where there are several methodologies like Extreme, Scrum, Rapid Prototype Model, Agile etc., which are more suitable for small and agile projects having limited number of people. Generally in most of the big project’s in companies waterfall model methodology is widely used to increase efficiency of software development process.

Our thesis project comes under the category of small project which has project life cycle of 4 months and 1 month for final university report writing and two persons are assigned to work for this thesis project. By considering these factors we required rapid prototyping without spending extensive time in planning and designing. So keeping these requirements in mind we chose RAD\textsuperscript{18} (Rapid Application Development) methodology.

During complete life cycle of project development the progress was continuously supervised by assigned skilled developers of Mobile Arts by scheduling weekly meeting and discussions. This helped a lot to make perfect software design where initially we started with minimal rough design of system and after review from Mobile Arts colleague it had been modified as per the requirements.

3.2 System Design

For GSM network architecture there are some basic modules which are core part of network like MSC, HLR, BSC and BTS. In our implementation we are going to use mentioned modules and some additional modules required for location services i.e GMLC, SMLC. The details of availability of modules are given as below.

1. Mobile Art’s Products: XMLC, GMLC, SMLC, HLR, MSC
2. Sourced: TE SS7 Stack
3. Hardware: nanoBTS, Cell Phones
4. Open source: OpenBSC

The motivation behind LCS capable GSM Network is to provide the location of mobile station by processing cell-id, TA-NMR or Assistance Data provided to the SMLC which performs some calculation related to location services and sends response to the target mobile station or upper network layers. At present 3 different types of position technologies are used i.e Network based, Handset based and Hybrid. GMLC which is provided by Mobile Arts is a Gateway Location Server which uses network-based/handset based technology or combination of both for location services. For position calculation Mobile Arts SMLC is used which is BSS based SMLC, where goal is to make successful connection and traffic flow towards to BSC (OpenBSC ).
3.2.1 Network Architecture

In this section we are emphasizing on network and system architecture of LCS Capable GSM Network. Below is the basic architecture where it shows the connection between all the nodes along with the type of interface.

![Network Architecture Diagram]

Fig 3.2.1.a Network Architecture

1. Communication Between Modules

   (a) **GMLC - HLR Communication (Lh interface)**
       Protocol: MAP
       Interaction phase: Location service.
       Functionality: Retrieve subscriber information.

   (b) **GMLC - MSC Communication (Lg interface)**
       Protocol: MAP
       Interaction phase: Location service.
       Functionality: Request updated subscriber location.

   (c) **MSC - HLR Communication (C interface)**
       Protocol: MAP
       Interaction phase: Subscriber management.
       Functionality: Keeping the VLR and HLR up-to-date with subscriber information.
(d) **MSC - BSC Communication (A interface)**  
Protocol: BSSAP  
**Interaction phase:** Subscriber management and Location services.  
**Functionality:** Conveying information to and from the subscriber.

(e) **SMLC - BSC Communication (Lb interface)**  
Protocol: BSSAP-LE / BSSLAP  
**Interaction phase:** Location Services  
**Functionality:** Calculate MS Location.

2. **Network Protocols**  
All previously described LCS capable GSM components e.g GMLC, MSC, SMLC etc., convey messages to each other via data wrapped under protocol headers. This Network Protocol stack is defined by 3GPP and must be followed by different entities of LCS capable GSM components. Different protocols used for our thesis project are described as below:

(a) **MAP:** Higher layer protocol used for communication between GMLC and MSC over SS7.  
(b) **BSSAP:** Layer 3 Protocol used for communicating between MSC and BSC.  
(c) **BSSLAP:** This protocol is used for transferring of TA data in case where SMLC originates the TA request to BSC.  
(d) **BSSAP-LE:** Layer 3 Protocol used for communication between BSC and SMLC over SS7.  
(e) **SCCP:** Layer 2 protocol used for connection management between MSC, BSC and SMLC.  
(f) **RRLP:** This protocol is used to transfer the position measurement data or location estimate from/to the MS and SMLC where the main goal is to provide the location estimate of MS.

![Fig 3.2.1.b Protocol Stack between MSC-BSC-SMLC](image-url)
Fig 3.2.1.c Protocol Stack between MS-BSC-SMLC
3.2.2 System Architecture

Figure 3.2.2 illustrates the different modules which can be stated as a) protocol modules which are basic implementation of protocols required for GSM functionality and follows 3gpp standards b) other modules which are designed to handle messages to and fro from the modules and work together with protocol modules to make a complete infrastructure of a system needed for LCS capable GSM Network.

1. **Location Management Module:** When a subscriber enters the network, this module determines whether MS is allowed to attach and provides a valid TMSI to MS. Also when subscriber leaves the network area it will get detached and subscriber information is removed from VLR.

2. **Subscriber Management Module:** As part of location updating procedure, insertion and deletion of subscriber information in the VLR database, which on requirement might be invoked by the HLR.

3. **Location Service Module:** This module is responsible for providing location services: a) Handling Location request from GMLC b) Sending paging request on arrival of Location request and after getting paging response, sending the location data request to the SMLC with classmarkinfo over SCCP connection to the BSC.

Fig 3.2.2 System Architecture

The functionalities of all the modules in figure 3.2.2 are explained in detail with their working and responsibilities are explained as below.
4. **Database Access Module**: Implements different database query functions against the VLR Database.

5. **VLR**: Database used to store temporary information about currently visiting subscribers in the network, store location information of each subscriber and keep it updated. CouchDB\(^\text{[14]}\) is used as database and our choice because of document database and user friendly GUI.

6. **OpenBSC**: Open source project implementing BSC component. For our project we are using OpenBSC as BSC and where it is extended to support Location based services.

7. **Erlang Node - Server**: We have developed the Erlang Server to convey the network packets between OpenBSC and SMLC needed for Location services and also to make use of existing protocols developed by Mobile Arts. The Erlang Server is connected to OpenBSC via TCP/IP and we used our own protocol in OpenBSC for LCS communication. Suggestion for protocol structure is simple:

\[
\langle\text{PacketID:} 8, \text{Length:} 16, \text{PacketData:binary}\rangle
\]

Table 3.2.2 shows what PacketID corresponds to which BSSAP-LE packet.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Packet ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAC_MSGT_TA_REQ</td>
<td>0x07</td>
</tr>
<tr>
<td>IPAC_MSGT_LOC_RESP</td>
<td>0x08</td>
</tr>
<tr>
<td>IPAC_MSGT_LCS</td>
<td>0x09</td>
</tr>
</tbody>
</table>

Fig 3.2.2 Protocol Structure for Internal use

### 3.2.3 Provide Subscriber Location Procedure

General Network Positioning for a MT-LR (Mobile Terminating Location Request), Figure 3.2.3/a represents a Mobile Terminating scenario where MS is identified by MSISDN or IMSI. The below scenario describes the full call flow for MT-LR where the SLIR is triggered from XMLC (MA’s Proxy Mobile Location Centre) client and for our case we used the Linux terminal to trigger the SLIR in XML format. This XML format has client specific and location specific details. After we trigger SLIR, XMLC in turn forward’s this request to GMLC and rest can be seen in the figure and explained in detail after the figure. The final result appears either in MA’s GUI or we can see the result on Terminal from where we triggered the SLIR.

![MT-LR Message Sequence Diagram](image)

Fig 3.2.3/a MT-LR Message Sequence Diagram
Description:
The message flow shown in Fig 3.2.3/a shows communication via 2 different types of Protocols i.e MAP and BSSMAP-LE.

- **MAP**
  - MAP Provide Subscriber Location (PSL)
  - MAP Provide Subscriber Location Response(PSL-R)

- **BSSMAP-LE**
  - BSSMAP-LE Perform Location Request(PLreq)
  - BSSMAP-LE Perform Location Response(PLrsp)

- **BSSLAP**(optional)
  - BSSLAP TA Layer 3
  - BSSLAP TA Request
  - BSSLAP TA Response

All these messages are described with their packet info as below.-

1. **Send routing info for LCS Request (SLIR):** After we trigger SLIR from MA’s XMLC, then XMLC forwards this request to GMLC and GMLC requests the HLR for information regarding which MSC the MS is currently connected to. The below Table 3.2.3/1 shows the message content.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Request</th>
<th>Indication</th>
<th>Response</th>
<th>Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoked id</td>
<td>M</td>
<td>M(=)</td>
<td>M(=)</td>
<td>M(=)</td>
</tr>
<tr>
<td>MLC Number</td>
<td>M</td>
<td>M(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSISDN</td>
<td>C</td>
<td>C(=)</td>
<td>C</td>
<td>C(=)</td>
</tr>
<tr>
<td>IMSI</td>
<td>C</td>
<td>C(=)</td>
<td>C</td>
<td>C(=)</td>
</tr>
<tr>
<td>LMSI</td>
<td></td>
<td></td>
<td>C</td>
<td>C(=)</td>
</tr>
<tr>
<td>Network Node Number</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>GPRS Node Indicator</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Additional Number</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Supported LCS Capability Sets</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Additional LCS Capability Sets</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>MME Name</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>AAA Server Name</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>V-GMLC Address</td>
<td>U</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Additional V-GMLC Address</td>
<td>U</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>H-GMLC Address</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>PPR Address</td>
<td>U</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>User error</td>
<td>C</td>
<td></td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Provider error</td>
<td></td>
<td></td>
<td></td>
<td>C</td>
</tr>
</tbody>
</table>

2. **Send routing info for LCS ACK (SLIA):** If the MS information resides in HLR then it replies to GMLC with ACK containing MSC address. The above Table 3.2.3/1 shows the message content of Send routing info for LCS ACK which can be seen in Response column.
3. **Provide Subscriber Location REQ (PSL):** When GMLC gets the MSC address where the request MS is connected, then GMLC requests the respective MSC for current location of MS along with IMSI, LCS QoS information and other optional message parameters by sending Provide Subscriber Location Request. This message can also contain client information which is optional where Invoke ID, Location Type, MLC Number and LCS Client ID are mandatory. Other parameters with optional and conditional type can be seen in Table 3.2.3/2.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Request</th>
<th>Indication</th>
<th>Response</th>
<th>Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoke id</td>
<td>M</td>
<td>M(=)</td>
<td>M(=)</td>
<td>M(=)</td>
</tr>
<tr>
<td>Location Type</td>
<td>M</td>
<td>M(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLC Number</td>
<td>M</td>
<td>M(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCS Client ID</td>
<td>M</td>
<td>M(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Override</td>
<td>U</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td>C</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSISDN</td>
<td>C</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMSI</td>
<td>C</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCS Priority</td>
<td>C</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCS QoS</td>
<td>C</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td>U</td>
<td>C(=)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location Estimate</td>
<td></td>
<td>M</td>
<td>M(=)</td>
<td></td>
</tr>
<tr>
<td>Age of Location Estimate</td>
<td></td>
<td>C</td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>User error</td>
<td></td>
<td>C</td>
<td>C(=)</td>
<td></td>
</tr>
<tr>
<td>Provider error</td>
<td></td>
<td></td>
<td></td>
<td>O</td>
</tr>
</tbody>
</table>

4. **Paging, Authentication, Ciphering:**

- **Paging:** The MSC sends PAGING messages to MS as an encapsulated BSSMAP connectionless message which includes the IMSI of MS, where the message content of PAGING request can be seen in Table 3.2.3/3. The channel needed field in message content is optional and might be used to define combination of channels required for paging transaction. It should be noted that each PAGING message sent is dedicated to only one MS and BSS encapsulates this page message according to the radio interface message defined in 3GPP 04.08 and as shown in Table 3.2.3/3.

<table>
<thead>
<tr>
<th>INFORMATION ELEMENT</th>
<th>DIRECTION</th>
<th>TYPE</th>
<th>LEN (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>MSC-BSS</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>IMSI</td>
<td>MSC-BSS</td>
<td>M</td>
<td>3-10</td>
</tr>
<tr>
<td>TMSI</td>
<td>MSC-BSS</td>
<td>O</td>
<td>6</td>
</tr>
<tr>
<td>Cell Identifier List</td>
<td>MSC-BSS</td>
<td>M</td>
<td>3 to 3+7n</td>
</tr>
<tr>
<td>Channel Needed</td>
<td>MSC-BSS</td>
<td>O</td>
<td>2</td>
</tr>
<tr>
<td>eMLPP Priority</td>
<td>MSC-BSS</td>
<td>O</td>
<td>2</td>
</tr>
</tbody>
</table>
• **Role of paging in MT-LR:** When MSC gets the Provide Subscriber Location Request from GMLC, it first checks for authentication of GMLC and barring restrictions for MS in VLR. On success MSC will send paging request to BSC which in turn try to page the subscriber. In request of this procedure, the MS will send PAGING RESPONSE to BSS which in turn will forward it to MSC. The message content of paging response can be seen in Table 3.2.3/4.

<table>
<thead>
<tr>
<th>INFORMATION ELEMENT</th>
<th>PRESENCE</th>
<th>LEN (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RR management Protocol Discriminator</td>
<td>M</td>
<td>1/2</td>
</tr>
<tr>
<td>Skip Indicator</td>
<td>M</td>
<td>1/2</td>
</tr>
<tr>
<td>Paging Response Message Type</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>Ciphering Key Sequence Number</td>
<td>M</td>
<td>1/2</td>
</tr>
<tr>
<td>Spare Half Octet</td>
<td>M</td>
<td>1/2</td>
</tr>
<tr>
<td>Mobile Station Classmark</td>
<td>M</td>
<td>4</td>
</tr>
<tr>
<td>Mobile Identity</td>
<td>M</td>
<td>2-9</td>
</tr>
</tbody>
</table>

Table 3.2.3/4 Paging Response

The current cell ID in Cell Identifier field and certain location information that includes the TA value in complete Layer 3 Information can be seen in Table 3.2.3/5 which is message content of COMPLETE LAYER 3 INFORMATION. If target MS supports any MS based or MS assisted positioning method, it provides the information to BSC and MSC via early classmark sending.

<table>
<thead>
<tr>
<th>INFORMATION ELEMENT</th>
<th>DIRECTION</th>
<th>TYPE</th>
<th>LEN (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>BSS-MSC</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>Cell Identifier</td>
<td>BSS-MSC</td>
<td>M</td>
<td>3-10</td>
</tr>
<tr>
<td>Layer 3 Information</td>
<td>BSS-MSC</td>
<td>M</td>
<td>3-n</td>
</tr>
<tr>
<td>Chosen Channel</td>
<td>BSS-MSC</td>
<td>O</td>
<td>2</td>
</tr>
<tr>
<td>LSA Identifier List</td>
<td>BSS-MSC</td>
<td>O</td>
<td>3-3n</td>
</tr>
<tr>
<td>PADU</td>
<td>BSS-MSC</td>
<td>O</td>
<td>3-n</td>
</tr>
</tbody>
</table>

Table 3.2.3/5 COMPLETE LAYER 3 INFORMATION

The detail procedure of MS attached and detached to the network is shown on flow chart in Fig 3.2.3/b.
5. **BSSMAP-LE Perform Location Request**: After MSC gets paging response from BSC(OpenBSC) then as described earlier our SMLC is BSS based, MSC sends BSSMAP-LE Perform Location Request to the BSC and in our case OpenMSC sends this request to OpenBSC. In OpenBSC we made changes so that it will detect LCS packet and then forward it to SMLC that may contain some measurement data related to positioning. If requested location information and accuracy within QoS is satisfied by obtained cell Id and if available TA value, the SMLC may compute a location estimate and sends back Perform Location Response to BSC. Otherwise for higher accuracy the SMLC can invoke AGPS procedure e.g. MS based position method. In this case the SMLC follows assistance data procedure which is shown in Fig 3.2.3/c. The below Table 3.2.3/6 shows the message content of BSSMAP-LE Perform Location Request.
Position Measurement Procedure: This procedure is used between SMLC and MS to get positioning data. This procedure is used to get more accurate position when is requested from network. During this procedure of delivering components, SMLC uses pseudo-segmentation procedure to send data where data is sent in small chunks of 242 octets so that this segmentation can be avoided at lower levels to get higher reliability for delivering of data to MS. If not then there are chances of loosing data during RR management even like Handover. Fig 3.2.3/c shows the sequence diagram for RRLP communication. Further after the figure there is brief description of each sequence of messages.

Later this thesis is extended to support AGPS and RRLP extension is added to OpenBSC. Several mobile phones are tested to check support of AGPS and to get more accurate position. In favorable condition like at least four satellites are visible, mobile phone successfully accepts all assistance data sent from SMLC, so in this case the final position of MS calculated with accuracy within 10 meters.
**Assistance Data Delivery Procedure:** The Assistance Data procedure takes around 15-20 seconds to transfer complete assistance data to MS which is around 6-8 segments. The Fig 3.2.3/d describes the message flow for Assistance Data Delivery Procedure. During this procedure the known issues are: a) Timer expired i.e sometimes MS never replies to assistance data and timer expires in SMLC, which in turn sends final location response where position is calculated based on cell-id or MS after 16 seconds cut off the radio connection towards BSC and BSC sends abort to SMLC, b) Data rejected by MS i.e. it is noticed during testing that some MS do not accept assistance data and never replies to Assistance Data Ack or sends Assistance Data Ack with reference number 0, which means either MS do not support RRLP protocol or something is not right in mobile handset e.g for IPhone 5 when tested in local lab with 2G AGPS, the phone sends Assistance Data ACK with Ref=0 which means it ignores/rejects/does not want to provide location but when we tried same while dialing 112 emergency number in Sweden then Iphone 5 replies with correct Assistance Data Ack, completes the RRLP traffic flow and finally provides the position.

![Fig 3.2.3/d Assistance Data Delivery Procedure](image)
These messages are RRLP components which are sent from the network to the MS. It is generally used by the network to provide assistance data to enable MS-based E-OTD or MS-based Assisted GPS capabilities in the MS. The message mainly consists of chunk of data with below respective fields. The Table 3.2.3/7 shows the Assistance Data Component.

**Table 3.2.3/7 Assistance Data Component**

<table>
<thead>
<tr>
<th>Element</th>
<th>Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-OTD Reference BTS for Assistance Data</td>
<td>C</td>
</tr>
<tr>
<td>E-OTD Measurement Assistance Data</td>
<td>C</td>
</tr>
<tr>
<td>E-OTD Measurement Assistance Data for System Information List</td>
<td>C</td>
</tr>
<tr>
<td>GPS Assistance Data</td>
<td>C</td>
</tr>
<tr>
<td>GPS Time Assistance Measurement Request</td>
<td>O</td>
</tr>
<tr>
<td>GPS Reference Time Uncertainty</td>
<td>O</td>
</tr>
</tbody>
</table>

- **RRLP(Measure Position Request):** After all assistance data is delivered to MS, SMLC finally sends Measure Position Request to MS where the message content is shown in Table 3.2.3/8. From assistance data provided by SMLC, MS calculate its position and sends Measure Position Response to SMLC with position coordinates.

**Table 3.2.3/8 Measure Position Request**

<table>
<thead>
<tr>
<th>Element</th>
<th>Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positioning Instructions</td>
<td>M</td>
</tr>
<tr>
<td>E-OTD Reference BTS for Assistance Data</td>
<td>O</td>
</tr>
<tr>
<td>E-OTD Measurement Assistance Data</td>
<td>O</td>
</tr>
<tr>
<td>E-OTD Measurement Assistance Data for System Information List</td>
<td>O</td>
</tr>
<tr>
<td>GPS Assistance Data</td>
<td>O</td>
</tr>
<tr>
<td>GPS Time Assistance Measurement Request</td>
<td>O</td>
</tr>
<tr>
<td>GPS Reference Time Uncertainty</td>
<td>O</td>
</tr>
</tbody>
</table>

- **RRLP(Protocol Error):** During RRLP traffic flow there might be a case where SMLC or MS can send Protocol Error to indicate the sender that there is some problem in receiving a complete and understandable component. e.g. We discovered in Iphone 5 where after receiving each assistance data it sends back ACK with reference number '0' and after 3 attempts SMLC sends RRLP (Protocol Error) with type of Protocol Error which has the following one of the indicator field.
  - '0': Undefined
  - '1': Missing Component
  - '2': Incorrect Data
  - '3': Missing Information Element or Component Element
• **RRLP (Measure Position Response):** In response of Measure Position Request this message is sent from MS to the network as an RRLP component. It is the response to the Measure Position Request. In the Measure Position Response which is received from BSC and sent from the MS the location estimate can be contained in one of the element i.e E-OTD Measurement Information, Location Information or GPS Measurement Information otherwise in fail case Location Information Error element must be included. In Table 3.2.3/9 the complete message contents of Measure Position Response is shown.

**Table 3.2.3/9 Measure Position Response**

<table>
<thead>
<tr>
<th>Element</th>
<th>Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Sets</td>
<td>O</td>
</tr>
<tr>
<td>Reference BTS Identity</td>
<td>O</td>
</tr>
<tr>
<td>E-OTD Measurement Information</td>
<td>O</td>
</tr>
<tr>
<td>Location Information</td>
<td>O</td>
</tr>
<tr>
<td>GPS Measurement Information</td>
<td>O</td>
</tr>
<tr>
<td>Location Information Error</td>
<td>C</td>
</tr>
<tr>
<td>GPS Time Assistance Measurements</td>
<td>O</td>
</tr>
</tbody>
</table>

In case of MS is not able to perform location request or network cannot determine the position estimate then Location Information Error must be included where it describes the Error Reason and this field is mandatory. Error Reason can be defined by string value from 0 to 10 which is described as below:

- '0': Undefined error.
- '1': There were not enough BTSs to be received when performing mobile based E-OTD.
- '2': There were not enough GPS satellites to be received, when performing GPS location.
- '3': E-OTD location calculation assistance data missing.
- '4': E-OTD assistance data missing.
- '5': GPS location calculation assistance data missing.
- '6': GPS assistance data missing.
- '7': Requested method not supported.
- '8': Location request not processed.
- '9': Reference BTS for GPS is not the serving BTS.
- '10': Reference BTS for E-OTD is not the serving BTS.

6. **BSSMAP-LE Perform Location Response:**

After successful procedure when BSC forwards location co-ordinates to SMLC then SMLC encapsulate this content in form of Perform Location Response and sends to the BSC and which in turn forwards it to MSC. The Table 3.2.3/10 describes content of Perform Location Response message where message type field is Mandatory and Location Estimate, Deciphering Keys and LCS cause are conditional. This means they can appear on some specific event. The positioning data field is optional where it depends upon Quality Of Service parameter.
7. **Provide Subscriber Location ACK:** As soon as the OpenBSC sends BSSMAP-LE Perform Location Response to MSC then MSC first decodes the BSSMAP-LE message and again encodes into MAP Provide Subscriber Location Response (PSL-R) and sends it to GMLC which contains the location information and location age where the message content can be seen in Table 3.2.3/11. At last GMLC sends this response to the XMLC and we can see the output in Terminal with X and Y coordinates as shown in Fig 3.2.3/e. To verify the position, paste these coordinates to [https://maps.google.com/](https://maps.google.com/) and current position of subscriber can be seen.

### Table 3.2.3/10 BSSMAP-LE Perform Location Response

<table>
<thead>
<tr>
<th>INFORMATION ELEMENT</th>
<th>TYPE</th>
<th>LEN (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>Location Estimate</td>
<td>C</td>
<td>2-22</td>
</tr>
<tr>
<td>Positioning Data</td>
<td>O</td>
<td>2-n</td>
</tr>
<tr>
<td>Deciphering Keys</td>
<td>O</td>
<td>17</td>
</tr>
<tr>
<td>LCS Cause</td>
<td>O</td>
<td>3</td>
</tr>
</tbody>
</table>

### Table 3.2.3/11 Provide Subscriber Location ACK

<table>
<thead>
<tr>
<th>INFORMATION ELEMENT</th>
<th>TYPE</th>
<th>LEN (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>Location Estimate</td>
<td>C</td>
<td>2-22</td>
</tr>
<tr>
<td>Positioning Data</td>
<td>O</td>
<td>2-n</td>
</tr>
<tr>
<td>Deciphering Keys</td>
<td>O</td>
<td>17</td>
</tr>
<tr>
<td>LCS Cause</td>
<td>O</td>
<td>3</td>
</tr>
</tbody>
</table>
Fig 3.2.3/e Final Output in Terminal at XMLC
3.2.4 State Machine for Provide Subscriber Location in MSC

OpenMSC is developed using Erlang OTP (Open Telecom Platform) where state machine plays vital role to create the stable system with efficient methods. State machines for OpenMSC can be seen in Fig 3.2.4/a and explanation of whole procedure with points which represents state and brief description for the same is mentioned after the figure.

![State Machine for Provide Subscriber Location in MSC](image)

**Fig 3.2.4/a State Machine for Provide Subscriber Location in MSC**

- **init:**
  - When GMLC sends MAP Provide Subscriber Location Request to OpenMSC, it goes into init state.
  - The Black dot in figure represents stop/End state.
  - In init state it checks from VLR the status of subscriber if
    1. user_error then directly terminates the state.
    2. error, detached: Go to check_last_location state.
    3. MS-Idle then send paging request and to go wait_for_page_rsp state.
    4. MS-Dedicated means channel is assigned to MS then go to wait_for_location_rsp state.

- **check_last_location:** This state checks for last location stored in database, if found then go to send_location state otherwise user_error then goes to stop/end state.

- **wait_for_page_rsp:** If OpenMSC gets:
  - paging response then OpenMSC extracts cell info and encodes cell info into packet BSSMAP-LE Perform Location Request and sends it to OpenBSC which in turn forwards it to SMLC and OpenMSC goes into wait_for_location_rsp state.
  - error, mnrf then goes into check_last_location state.

- **wait_for_location_rsp:** While being in this state if OpenMSC gets:
  - Location response then it goes to send_location state.
  - error_positioning then goes to check_last_location state.
3.2.5 Location Update Procedure

Figure 3.2.5/a illustrates general network positioning for Location Update where TMSI of MS is not known. This is the procedure when MS tries to attach to network. The whole call flow is explained briefly as below:

1. **Location Update Request**: This is the step when MS tries to get attached to the network and it sends Location Update Request to the BSC via BTS which in turn forwards it to the MSC.

2. **Identification REQ/RSP**: If in the Location Update Request, the MS send its TMSI the MSC sends Identification Request to MS and in turn MS sends Identification response which contains the IMSI.

3. **Update Location**: MSC sends Update Location to the HLR along with IMSI of MS and if the user exists in HLR with provided IMSI, HLR replies with Update Location ACK. Otherwise HLR tells MSC to insert subscriber data in VLR via Insert Subscriber Data request.

4. **Insert Subscriber Data/ACK**: This message is shown with dotted arrow as HLR sends it in parallel with update location ACK and in turn MSC/VLR will insert information of MS in database and sends Insert Subscriber Data ACK back to the HLR.

5. **Location Update CNF**: After successful operation the MSC sends Location Update CNF to the MS and which now gets attached (connected) to the network.

6. **TMSI Reallocation Complete**: After it updates the latest TMSI provided by the MSC, it sends TMSI Reallocation Complete to the MSC.

![Fig 3.2.5/a General Location Update Procedure for MS](image-url)
In below Fig 3.2.5/b you can see the flow chart where detail procedure for Location Update can be seen when TMSI is not known.

![MSC-LU-Flowchart](image-url)
3.2.6 State Machine for Location Update Procedure in MSC

As discussed earlier that we used Finite State Machines (FSM) to develop our product and Fig 3.2.5/c shows the FSM diagram for location update procedure.

![State Machine Diagram](image)

**Fig 3.2.5/c State Machine for Location Update Procedure in MSC**

All states are described in form of points as below:

- **init**: MS tries to attach to the network by sending Location Update request to OpenBSC and OpenBSC sends this request to OpenMSC. This will make it enter init state in OpenMSC. In this state it will check:
  - If IMSI is present in Location Update request if yes, then go to update_lai state where MSC tells VLR to update the same.
  - If IMSI is not present then it will ask MS for Id_req for IMSI and goes into wait_for_id_rsp state.

- **Update_lai**: In this state MSC checks:
  - If subscriber status is present in VLR if yes, then goes to subscriber present status.
  - Otherwise go to wait_for_update_loc_cnf

- **wait_for_update_loc_cnf**: In this state MSC waits to get Update location confirm from HLR and if MSC gets:
  - error, then ends the traffic case
  - Otherwise go to the subscriber_present state.

- **Subscriber_present_state**: In this state MSC sends TMSI re-allocation command to mobile station and goes to wait_for_tmsi_realloc.

- **wait_for_tmsi_realloc**: When MSC gets TMSI re-allocation complete then traffic case ends.
4 System Deployment and Testing

4.1 Deployment of nanoBTS

In mobile communication networks, a base transceiver station (BTS) is hardware or can be a cell tower which sends and receives the radio signals from the user equipment i.e UE which could be mobile phones.

Usually the normal size BTS are huge in size like a tower but ip.access nanoBTS are very small BTS, we can consider about the size of Wifi which supports an A-bis interface over IP. Below figure represents the nanoBTS used during thesis work.

![Fig 4.1 nanoBTS used during thesis work](image)

The nanoBTS are wonderful and makes picocells with complete GSM base stations and provides standard Um interface to the handset and another Abis interface over IP to the BSC. For our thesis work we connect the nanoBTS to internal GSM network components of Mobile Arts so that any machine running OpenBSC can connect to nanoBTS.

Nano-BTS has following features:-:

- Supporting frequency bands 900, 1800 or 1900MHz
- Indoor coverage up to several hundred meters
- Very simple deployment where one can connect nano-BTS by a single Ethernet connection for power, traffic and signaling.
- Output power Up to 200mW

4.1.1 Configuration steps for connecting nanoBTS with your Computer

Before connecting the nano BTS to a computer machine one needs to install DHCP server and ubuntu for our case we followed the below steps:

- `sudo apt-get install dhcp3-server`
- **Configuring DHCP server:** One can use two network cards where one dedicated for nanoBTS and in Ubuntu it is needed to configure the interface which is wanted to be used for DHCP server listening. By default it listens to eth0. One can change this by editing `/etc/default/dhcp3-server` file.
  - `sudo vim /etc/default/dhcp3-server`
  - Find this line `INTERFACES="eth0"` and replace with the following line `INTERFACES="eth1"`. Save and exit.
- `sudo /etc/init.d/dhcp3-server restart`

The non configured ip.access nanoBTS needs to be configured as follows:\[12\]:

---

[12]: Refer to the original text for the details of the configuration steps.
• When nanoBTS is connected to the network for the first time it will automatically obtain an IP address via DHCP

• OpenBSC has some features to configure/find nanoBTS. When one runs the following command
  /openbsc/openbsc/src/ipaccess/ipaccess-find eth0 below output can be seen:
  Trying to find ip.access BTS by broadcast UDP...
  MAC Address='00:02:95:00:16:48' IP Address='192.168.1.85' Unit ID='1801/0/0'
  Location 1='BTS_NBT131G' Equipment Version='139_029_31'
  Software Version='120a002_v209b24d0' Unit Name='nbts-00-02-95-00-16-48' Serial Number='00065049'

• The BTS is listening on TCP port 3006 for incoming Abis-over-IP connections. This is called Secondary OML Link.

• The BTS has non configured or default Unit ID (65535/0/0) and will refuse to work until a Unit ID has been set. One can set the Unit ID and Primary OML IP using ipaccess-config as follows:
  $ ./ipaccess-config -u 1801/0/0 -o 192.168.1.1 -r 192.168.1.85 Where 192.168.1.1 is your OpenBSC IP and 192.168.1.85 is nanoBTS's IP.

NOTE:- When nanoBTS has powered-on then at initial stage it will blink with orange light which states that nanoBTS is waiting to get connected with BSC and after successful connection with OpenBSC one will see the constant green light.

4.2 Deployment of TCP Server/Client

Initially when we started our thesis when the main question arising in our mind was how to make efficient reliable connection between OpenBSC and our product, because in *Student Project CS* we used CNODE concept to connect our system to OpenBSC but later we decided to make use of Erlang.

Erlang itself has support for TCP and UDP connections so in the beginning we created TCP server and TCP client and made some dummy tests so we could verify the stability and performance of the system. As from previous experience while working with OpenBSC we already knew that when we start the OpenBSC then it sends IPA Ping and waits for IPA pong, we extended the TCP server to Erlang gen_server and made changes to adopt to the ping signal from OpenBSC and responds with pong. The loop of ping and pong was successful and the connection was stable. We added sccp and bssmap packet handling in TCP gen_server. During traffic flowing there are lot of GSM packets flow back and forth where TCP gen_server/client parse the incoming packets from OpenBSC and sends to MSC and vice versa.

We used similar Erlang TCP gen_server for connection between OpenBSC and SMLC. During the initial development this TCP gen_server was designed to handle basic IPA packet flow towards the OpenBSC and SCCP, BSSMAP packet flow towards SMLC. Later when the thesis was extended to add support for AGPS functionality then SCCP protocol was used for connection between

\[ MSC \xleftarrow{sccp} OpenBSC \xrightarrow{sccp} SMLC \]

Initially TCP gen_server was designed to start manually from shell as shown below. Later after the thesis was extended then both openmsc and openbsc(erlang node) were changed to become complete application and all nodes became part of it, so from single command

`. /openmsc start`

OR

`. /openbsc start`

all dependent nodes and applications could be started.
At openmsc:

```
./openmsc shell
(openmsc@msc)tcp_child_sup:start_link().
{ok,<0.936.0>}
(openmsc@msc)tcp_gen_server:start_link(5000).
{ok,<0.938.0>}
```

At openbsc:

```
./openbsc shell
(openbsc@bsc)tcp_child_sup:start_link().
{ok,<0.952.0>}
(openbsc@bsc)tcp_gen_server:start_link(5001).
{ok,<0.954.0>}
```

Then OpenBSC connects to openmsc and openbsc (erlang node).

4.3 Deployment of OpenMSC

In previous project CS from Uppsala University we already developed MSC named as OpenMSC which was SMS capable and we had implemented respective required protocols. During this thesis project we used the same OpenMSC which is now extended for LCS support. During implementation we did not found any problems as our system design was good enough to follow and we stick to the design. We used some old libraries from project CS OpenMSC and implemented protocol libraries while encoding and decoding BSSMAP and other packets. We also developed SCCP Library in Erlang to encode and decode SCCP packets. As discussed earlier that we used tcp gen_server based in Erlang, so we needed to implement IPA protocol also so that we can communicate with OpenBSC. Mobile Arts has their own internal applications to run GMLC, HLR, SMLC so we also made our OpenMSC as part of Mobile Arts application, so that it works and behaves same as other Mobile Arts applications. This helped us to understand MA’s application process and how to maintain stability in the system by using system alarm etc.

4.4 Deployment of GMLC, SMLC, HLR

All other components of GSM network which were needed to create LCS capable GSM network were mostly covered by MA’s products as GMLC, HLR, SMLC and we made use of these existing systems. First MA colleagues helped us to install and configure GMLC, HLR, SMLC on virtual server so that we can access it via IP network. After this installation and configuration we started all nodes but most important thing was to deploy ss7 stack and configure it for communication between nodes. We had used stack for OpenMSC also. GMLC and HLR was communicating with OpenMSC via Lg and Lh api.

4.5 Deployment of SS7 Stack

In GSM network all network modules or systems communicates via SS7 stack which is the heart of GSM network because it is the main source to route traffic via global titles. In telecommunication network Global Title is used to specify an address which is used in SCCP Protocol for routing signaling messages. These addresses are unique and refers to only one destination where in practice destinations can change over time. For our thesis work we used SS7 stack for HLR, GMLC ,SMLC and MSC where all systems were communicating via global titles. After we deployed the stack with help of Mobile Arts colleagues we needed to change map_dialog and respective api to make communication with our OpenMSC. After making the changes in map_dialog at GMLC, OpenMSC started communicating via TCAP and successfully encoded and decoded the PSL request or we can say that we made the changes so that GMLC and OpenMSC both can encode and decode the PSL parameters via API.
4.6 Testing Methods (BLACK BOX Testing)

Testing is very crucial part in Telecom Platform, as one need to modify the product as per different 3gpp standard used by other operators. Of course this was internal testing and most important thing was to test the system built within the scope of the thesis.

The testing results explained below are shown for a) MAP Interface b) BSSMAP Interface. The below figure shows the output in MA OAM(Operation and Management) GUI where one can see the details.

- MAP Interface
  To obtain the current location of subscriber, the SLIR request is triggered from shell command and results can be seen in Fig 4.7.a. The snap shot is taken from MA’s OAM GUI where one can see the complete successful traffic flow for LCS SLIR request.

Fig 4.7.a MT-LR PSL message flow on MA’s OAM GUI
Message Contents

1. XML Request Content of SLIR: The yellow box in the figure below shows the XML content of SLIR request where the location type, maximum location age and horizontal accuracy fields mainly affect the results.

**Verification:** The mandatory attributes of SLIR request i.e. MSISDN, Location Type, Location Age and Horizontal Accuracy can be seen. The successful delivery of this message shows the continuation of message flow.

Fig 4.7.a/1 SLIR request content in XML format at XMLC
2. **PSL Request Content**: When GMLC gets the MSC number in response of SRI-SM from HLR, then GMLC sends PSL request to MSC and in the figure below contents of PSL request can be seen, where the contents are represented as Erlang records.

**Verification**: In PSL message content we can clearly see the mandatory attributes of SLIR such as Location Type, MLC Number, LCS Client ID, Privacy Override, IMSI, MSISDN, LCS Priority, LCS QoS, which were sent from XMLC. The successful delivery of this message shows the continuation of message flow.
3. **PSL Response Content:** After successful traffic flow when MSC gets BSSMAP Perform Location Response from OpenBSC, then MSC encapsulates co-ordinates into MAP Provide Subscriber Location Response and sends it to the GMLC. Message contents can be seen in the below figure.

**Verification:** In PSL response we can see the location estimate which shows the PSL was successful and location of mobile phone is returned. The successful delivery of this message shows the continuation of message flow.

![Fig 4.7.a/3 PSL Response Content](image-url)
4. **PSL Response Content at XMLC**: On receiving of MAP Provide Subscriber Response from MSC, GMLC forwards it to the XMLC where message content at XMLC is shown in below figure.

**Verification**: In PSL response at XMLC we can see the location estimate in human readable form i.e latitude(X) and longitude(Y), which shows the PSL was successful and location of mobile phone is returned.

![Fig 4.7.a/4 PSL Response Content at XMLC](image-url)
- **BSSMAP Interface**
  When MSC gets PSL request then it sends paging request to MS via OpenBSC. If the MS replies with paging response then MSC encapsulates Cell ID Info in previously received Classmark Info from MS into BSSMAP Perform Location Request and sends it to OpenBSC and which recognizes the request and forwards it to openbsc erlang node over IPA Protocol. It then initiates SCCP connection request towards SMLC and after receiving SCCP Connection Confirm from SMLC it forwards PLR to SMLC. In turn the SMLC calculates the position based on Cell ID info and in the final result, replies back with the position co-ordinates in BSSMAP PERFORM LOCATION RESPONSE. The complete successful traffic case is shown in below Fig 4.7.b. In extension of the thesis with AGPS support the communication between OpenBSC and openbsc erlang node is done over SCCP protocol.

![Fig 4.7.b PLR message flow between openbsc Erlang Node and SMLC](image_url)
Message Contents

1. SCCP Connection Request: When OpenBSC sends PLR to OpenBSC erlang node then it initiates SCCP connection towards SMLC. In below figure one can see the message content of SCCP Connection Request sent by openbsc erlang node to SMLC.

Verification: The mandatory attributes of SCCP Connection Request i.e connection id, source address and destination address can be seen in message content. The successful delivery of this message shows the continuation of message flow.

Fig 4.7.b/1 SCCP Connection Request Message Content

2. SCCP Connection Confirm: On receiving of SCCP Connection Request, SMLC sends SCCP Connection Confirm to OpenBSC erlang node, where message contents can be seen in below figure.

Verification: The matching connection id in SCCP Connection Confirm message from SMLC proves the establishment of SCCP connection from BSC. The successful delivery of this message shows the continuation of message flow.

Fig 4.7.b/2 SCCP Connection Confirm Message Content
3. **BSSMAP Perform Location Request**: On receiving of SCCP Connection Confirm, openbsc erlang node sends BSSMAP Perform Location Request to SMLC and waits for BSSMAP Perform Location Response where message content shown in below figure.

**Verification**: The required attributes i.e Cell ID received in paging response from mobile phone is sent to SMLC to calculate the position of mobile phone. The successful delivery of this message shows the continuation of message flow.

![Fig 4.7.b/3 BSSMAP Perform Location Request Message Content](image-url)
4. **BSSMAP Perform Location Response**: After SMLC calculates the position co-ordinates it will forward it to OpenBSC erlang node and encapsulates the co-ordinates in BSSMAP Perform Location Response and sends to OpenBSC. The message contents of BSSMAP Perform Location Response can be seen in the below figure.

**Verification**: In BSSMAP Perform Location Response one can see the latitude and longitude values which shows that SMLC successfully calculated the position of mobile phone.

![BSSMAP Perform Location Response Message Content](image)

**Fig 4.7.b/4 BSSMAP Perform Location Response Message Content**
5. **SCCP Release**: After SMLC sends BSSMAP PERFORM LOCATION RESPONSE to OpenBSC erlang node, it sends SCCP Release message to SMLC node to terminate SCCP connection where message content can be seen in below figure.

**Verification**: In SCCP Release message one can see the same connection id used in SCCP Connection request sent by BSC to SMLC, which verifies the complete message flow of one transaction.

![SCCP Release Message Content](image-url)
4.7 Results

The co-ordinates we received in shell terminal in response of the SLIR request, we cross verified the location of MS by putting x and y co-ordinates in Google maps. The result is shown in Fig 4.7.c and the estimated location of MS is around 500 meters as we used cell based method. This is the expected result from the Cell-ID method and the limited cell data loaded into SMLC. In real practice this scenario can easily occur. It could have been better results with Cell ID and AGPS method if it would had been possible to bring the mobile phone out of test network but the bottle neck was network coverage.

![Fig 4.7.c MS Position Result in Google Maps](image)
5 Future Work

In this thesis we have concentrated on building GSM network with support of location based services and main focus was on developing & integration of respective GSM components with CGI method working. Other methods have been omitted to keep the work self-contained and considering time limitations. For future work we suggest to look closer into other features of GSM network i.e Voice Call, Voice Mail, Missed Call Alert and TA, TOA, E-TOD, AGPS functionality for location based services.

5.1 Voice Call

Currently the main function of Global MSC is voice call handling, SMS, and also Location based services is getting more popular. If we combine our student project CS OpenMSC which supports for SMS and current LCS capable OpenMSC which supports for LCS then only major thing left is to make complete MSC that is to include voice call. Voice call has more dealing with switching, session handling, handover, billing/charging etc. Our current OpenMSC supports Location Update and to obtain the subscriber position. We are keen to implement voice call facility in our OpenMSC which might be included in our future work.

5.2 AGPS functionality

After we tested our system and when we verified the location co-ordinates of the subscriber, we realized that in real time system it is so important to give location co-ordinates which gives subscriber’s location in few meters e.g. 10 meters. But this accuracy depends on many factors but of course the method chosen for locating a subscriber also plays major role. Because of time constraint we did not implement AGPS functionality initially which is very vast in itself and might have taken much more time since we had to update the OpenBSC also.

Later when my thesis partner left, I started working with Mobile Arts and extended our thesis to add support for AGPS. We tested many phones and this helped a lot to make SMLC, MSC more robust.
6 Conclusion

The aim of this thesis project was to design and implement a prototype of the LCS capable GSM network using Erlang and C programming language which was successfully attained. The test environment was built using nanoBTS, OpenMSC, OpenBSC, GMLC, SMLC and HLR where the integration of these components required to implement the API's as well as the basic IPA protocol and other sccp, bssmap protocol using C and Erlang programming languages. The Erlang node was implemented for communication between OpenBSC written in C and SMLC written in Erlang.

For validation of the built prototype the mobile phone was attached to the test network using nanoBTS, OpenBSC, OpenMSC and HLR which proved the integration of respective components and successful encoding/decoding of the required messages. While the mobile phone was attached to the test network, the location request was sent from the XMLC to find out the current location of the mobile phone. The location of the mobile phone in form of latitude and longitude was achieved. This proved the complete integration of the GSM network components including X/G/SMLC and successful parsing of messages required for LCS capable GSM network.

The implementation phase during the project was quite engaging as OpenBSC is a complex system with more than 80,000 lines of code in 'C' language. To understand the OpenBSC code required extensive efforts and skills to integrate OpenBSC with OpenMSC and SMLC. I had used gdb tool to back trace the segmentation faults during the implementation and testing in OpenBSC for support of the location based request and response. The implementation of basic IPA protocol with other sccp and bssmap protocol to support for LCS in the OpenBSC required extensive study of 3GPP documents and other network protocols. As the implementation was done in 'C' and Erlang programming language, good skills were required in both. We also acquired knowledge of CouchDB and protocol sniffing tools like Wireshark.
7 References

1. 3GPP GSM 04.08, Mobile radio interface layer 3 specification, 1998
2. 3GPP GSM 08.06, Signalling transport mechanism specification for BSS - MSC interface, 1999
3. 3GPP GSM 08.08, MSC - BSS interface layer 3 specification, 1999
4. 3GPP TS 03.71 "Location Services (LCS); (Functional description) - Stage 2"
5. 3GPP TS 04.31 "Location Services (LCS); Mobile Station (MS) – Serving Mobile Location Center (SMLC); Radio Resource LCS Protocol (RRLP)."
6. 3GPP TS 04.71 "Location Services (LCS); Mobile radio interface layer 3 Location Services (LCS) specification"
7. 3GPP TS 08.71 "Location Services (LCS); Serving Mobile Location Center – Base Station Subsystem (SMLC-BSS) interface Layer 3 specification."
8. 3GPP TS 09.31 "Location Services (LCS); Base Station System Application Part; LCS Extension (BSSAP-LE)"
9. 3GPP GSM 09.02, Mobile application part specification, 1998
11. Erlang Programming, A concurrent approach to software development, Francesco Cesarini and Simon Thompson, O'Reilly, 2009
15. TietoEnator Internal SS7 course material.
20. Location Services in GSM and UMTS Networks
21. A Survey of Positioning Techniques and Location Based Services in Wireless Networks
8 Appendices

8.1 Deployment of OpenBSC

OpenBSC is a free software which has GSM BSC Implementation but not BSS based SMLC support. At current state OpenBSC supports either whole GSM network in a box or we can connect external HLR, MSC and nanoBTS. Below are the simple steps to deploy OpenBSC in your system.

- First step is to start installing dependencies for OpenBSC where following Debian packages need to be installed before you start
  - libdbi0
  - libdbi0-dev
  - libdbd-sqlite3
  - libortp-dev
  - build-essential
  - libtool
  - autoconf
  - automake
  - git-core
  - pkg-config

(While installing OpenBSC, you might need to install some additional dependent packages)

- Building libosmocore
  - Checkout libosmocore from git using git clone git://git.osmocom.org/libosmocore.git
  - cd libosmocore
  - Rebuild the configure script using autoreconf -fi
  - Run the configure script using: ./configure
  - Build the actual software using: make
  - Install the library by using: make install
  - Do not forget ldconfig: sudo ldconfig

- Building libosmo-abis
  - Check out libosmo-abis from git using git clone git://git.osmocom.org/libosmo-abis.git
  - Change into the right directory using
  - cd libosmo-abis
  - Rebuild the configure script using: autoreconf -fi
  - Run the configure script using: ./configure
  - Build the actual software using: make
  - Install the library by using: make install
  - Do not forget ldconfig: sudo ldconfig

- Building libosmo-sccp
  - Check out libosmo-sccp from git using: git clone git://git.osmocom.org/libosmo-sccp.git
  - Change into the right directory using: cd libosmo-sccp
  - Rebuild the configure script using: autoreconf -fi
– Run the configure script using: `./configure`
– Build the actual software using: `make`
– Install the library by using: `make install`
– Do not forget `ldconfig`: `sudo ldconfig`

**Building OpenBSC**

– Check out OpenBSC from git using: `git clone git://git.osmocom.org/openbsc.git`
– Change into the right directory using: `cd openbsc/openbsc`
– Rebuild the configure script using: `autoreconf -i`
– Point OpenBSC to the installation of libosmocore: `export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig`
– Run the configure script using: `./configure --enable-osmo-bsc` (this option needed to configure OpenBSC with osmo-bsc)
– Build the actual software using: `make`

To add configuration parameters so that OpenBSC reads these parameters to know the network settings, you need to add the following lines in `openbsc.cfg`

**vim openbsc/openbsc/src/osmo-bsc/openbsc.cfg** and change the value as:

– mobile network code (MNC) 28
– short name OpenMSC
– long name OpenMSC
– auth policy accept-all
– auth policy closed: (Do not allow anyone who is not marked as authorized=1 in the HLR database)

Add following configuration of MSC to end of `openbsc.cfg` file. As OpenBSC team keep updating software so these configuration might get change. You need to adopt according to the software version.

– msc
– ip.access rtp-base 4000
– timeout-ping 20
– timeout-pong 5
– mid-call-timeout 0
– destination address of msc IP PORT: dest 192.168.211.242 5000 0
– Run `./osmo-bsc`