
Department of Information Technology

# Mobility Management in Packet Switched Mobile Networks

The Department Council of the Department of Information Technology confirmed the topic of this Master's Thesis on 12th of March 2003.

| | |
|---|---|
| Examiners: | Professor Jan Voracek,<br>Vladimir Botchko, Ph. D |
| Supervisor: | Tatiana Issaeva, M. Sc. |


| | |
|---|---|
| Author: | Marina Lishchina |
| Address: | Ajurinmäki 5A 18,<br>02600, Espoo, Finland |
| Mobile: | +358 50 4860452 |


April 10, 2003

# ABSTRACT OF MASTER'S THESIS

**LAPPEENRANTA UNIVERSITY OF TECHNOLOGY**
Department of Information Technology

| | |
|---|---|
| Author: | Marina Lishchina |
| Title of the thesis: | Mobility Management in Packet Switched Mobile Networks |
| Date: | 10th April 2003 |
| Original language: | English |
| Number of pages: | 87 |
| Number of figures: | 37 |

| | |
|---|---|
| Examiners: | Professor Jan Voracek<br>Vladimir Botchko, Ph. D |
| Supervisor: | Tatiana Issaeva, M. Sc. |

Nowadays mobile networks became part of everyday life. One of the main differences between fixed networks and mobile networks is user mobility, that can be defined as ability to make and receive calls anywhere and anytime the user wants. This thesis explains term mobility and specifies the problems, which must be solved to provide mobility and the ways it is done in cellular networks. It gives an overview of mobility procedures: paging, location updating, roaming and handover.

Thesis concentrates on mobility in packet switched domain of third generation (3G) mobile networks, as an example mobility management in Universal Mobile Telecommunications System (UMTS) is described. Differences between mobility in packet switched and circuit switched domains are given and explained.

To make mobility of users and theirs terminals possible, the communication between different parts of network is needed. Signalling exchange between network elements and execution of mobility procedures is done with help of protocols. Master's thesis describes protocols involved in mobility provision. The main attention is paid to GPRS Mobility Management (GMM) protocol.

The implementation of executable prototype of GMM protocol is presented as a practical part of this thesis.

Keywords: mobility management, UMTS, protocol, GMM, location updating

# DIPLOMITYÖN TIIVISTELMÄ

**Lappeenrannan teknillinen yliopisto**
Tietotekniikan osasto

| | |
|---|---|
| Tekijä: | Marina Lishchina |
| Otsikko: | Liikkuvuuden hallinta pakettikytkentäisissä matkaviestinverkoissa |
| Päiväys: | 10.04.2003 |
| Kieli: | englanti |
| Sivujen lukumäärä: | 87 |
| Kuvien lukumäärä: | 37 |
| Tarkastajat: | Professori Jan Voracek<br>Vladimir Botchko, FT |
| Ohjaaja: | Tatiana Issaeva, DI |

Nykyisin matkaviestinverkot ovat osa jokapäiväistä elämää. Merkittävimpiä eroja kiinteiden ja matkaviestinverkkojen välillä on käyttäjän liikkuvuus, joka voidaan määritellä mahdollisuudeksi soittaa ja vastaanottaa puheluita missä ja milloin tahansa. Työ selittää termin liikkuvuus ja määrittää ongelmat, jotka täytyy ratkaista liikkuvuuden aikaansaamiseksi sekä tavat, joilla nämä ongelmat on ratkaistu matkaviestinverkoissa. Työ luo yleiskatsauksen liikkuvuuden aikaansaamisessa käytettäviin menetelmiin, joita ovat haku, sijainnin päivitys, sijainnin seuranta ja kanavan vaihto.

Työ keskittyy liikkuvuuteen kolmannen sukupolven matkaviestinverkkojen pakettikytkentäisessä osassa, esimerkkinä liikkuvuuden hallinta UMTS:ssa (Universal Mobile Telecommunications System). Erot paketti- ja piirikytkentäisen osan välillä tuodaan esille ja selitetään.

Jotta käyttäjät ja heidän päätteensä voisivat liikkua, tiedon täytyy kulkea verkon eri osien välillä. Merkinanto verkkoelementtien välillä ja liikkuvuuden mahdollistavien toimenpiteiden suoritus tehdään yhteyskäytännön avulla. Työ kuvaa yhteyskäytännöt, jotka ovat osallisena liikkuvuuden tarjontaan. Painopiste on GPRS:n liikkuvuudenhallintayhteyskäytännössä, GMM:ssä.

GMM protokollan prototyypin toteutus on esitetty työn käytännön osassa.

Hakusanat: liikkuvuuden hallinta, UMTS, yhteyskäytäntö, GMM, sijainnin päivitys

## ACKNOWLEDGEMENTS

This Master's thesis has been written in the Mobile Networks Laboratory of Nokia Research Center, Helsinki; and I would like to thank all the people who made it possible. Special thanks to my supervisor Tatiana Issaeva for the valuable comments and ideas about some figures content and to Ari Ahtiainen for the suggestions about the structure of the thesis.

I also would like to express my gratitude to all people in Lappeenranta University of Technology who organised International Master's Program in Information Technology and gave me the opportunity to study in Finland. This personally concerns professor Jan Voracek and Nina Kontro-Vesivalo.

Finally, I would like to thank my parents and my boyfriend Alexander Salamov for their love and everyday support.

Helsinki, April 10th, 2003

Marina Lishchina

# ABBREVIATIONS

| | |
|---|---|
| 1G | The First Generation Mobile Communication Systems |
| 2G | The Second Generation Mobile Communication Systems |
| 3G | The Third Generation Mobile Communication Systems |
| 3GPP | 3rd Generation Partnership Project |
| AMPS | Advanced Mobile Phone System |
| ASN.1 | Abstract Syntax Notation One |
| AuC | Authentication Center |
| BS | Base Station |
| CASN | Compiler for ASN.1 |
| CC | Country Code |
| CGI | Cell Global Identity |
| CID | Cell ID |
| CN | Core Network |
| CS | Circuit Switched |
| EIR | Equipment Identity Register |
| GGSN | Gateway GPRS Support Node |
| GMM | GPRS Mobility Management |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| GTP | GPRS Tunnelling Protocol |
| HLR | Home Location Register |
| IMEI | International Mobile Equipment Identity |
| IMEISV | IMEI Software Version |
| IMSI | International Mobile Subscriber Identity |
| ITU | International Telecommunication Union |
| ITU-T | Telecommunication Standardisation Sector of ITU |
| LA | Location Area |
| LAI | Location Area Identity |
| MAP | Mobile Application Part |
| MCC | Mobile Country Code |
| ME | Mobile Equipment |

| | |
|---|---|
| MM | Mobility Management |
| MNC | Mobile Network Code |
| MSISDN | Mobile Subscriber ISDN Number |
| MSIN | Mobile Subscriber Identification Number |
| MSRN | Mobile Subscriber Roaming Number |
| NDC | National Destination Code |
| NMSI | National Mobile Subscriber Identity |
| NMT | Nordic Mobile Telephone systems |
| P-TMSI | Packet Temporary Mobile Subscriber Identity |
| PDC | Pacific Digital Communications |
| PDP | Packet Data Protocol |
| PDU | Protocol Data Units |
| PID | Process Identifier |
| PLMN | Public Land Mobile Network |
| PS | Packet Switching |
| QoS | Quality of Service |
| RA | Routing Area |
| RAC | Routing Area Code |
| RAI | Routing Area Identification |
| RANAP | Radio Access Network Application Part |
| RED | Routing/ Encoding/Decoding |
| RNC | Radio Network Controller |
| RRC | Radio Resource Control protocol |
| SDL | Specification and Description Language |
| SGSN | Serving GPRS Support Node |
| SIM | Subscriber Identity Module |
| SM | Session Management |
| SMS | Short Message Service |
| SN | Subscriber Number |
| SRN | Serial Number |
| TAC | Type Allocation Code |
| TACS | Total Access Communication System |

| | |
|---|---|
| TMSI | Temporary Mobile Subscriber Identity |
| UE | User Equipment |
| UMTS | Universal Mobile Telecommunications System |
| URA | UTRAN Registration Area |
| UTRAN | UMTS Terrestrial Radio Access Network |
| VLR | Visitor Location Register |

# 1. INTRODUCTION

People are becoming more and more mobile than ever before. They communicate in a number of different ways: by voice (directly or using voice mail) or by data exchange (e-mail, short message service, file transfer). Mobility is a feature of a mobile network that makes this communication possible.

Second generation (2G) mobile systems are currently most widely used all over the world. Most successful example of 2G cellular systems is Global System for Mobile communications (GSM). Rapid growth of requirements, supporting of different types of information exchange and needs for more global system, then 2G networks, entail the intensive research in this area and new third generation (3G) mobile systems were created. Universal Mobile Telecommunications System (UMTS) is an example of 3G mobile networks. UMTS can be structured as consisting of two domains: circuit switched domain that is used for voice communication and packet switched domain that is responsible for data transfer.

Big research work was done in area of mobile communications and many books were written that make an overview of cellular systems, some of them also give general description of mobility and how it is supported. One of goals of this thesis is to give detailed description of mobility and mobility procedures – actions, which should be executed for providing users mobility. The data in packet switched domain and circuit switched domain is transmitted using different techniques. This leads changes in mobility also. The research in this area was done as a part of this thesis work. Provision of mobility involves a lot of interactions between network elements, which are done by a number of protocols. Another purpose of this thesis is to study and present the functionality of GPRS Mobility Management (GMM) protocol in depth.

This thesis consists of theoretical and practical parts and structured as follows. Chapter 2 explains term “mobility”, describes the procedures that are executed to support user mobility and gives some background information about cellular systems and evolution of mobility. Chapter 3 shows main differences between mobility in packet and circuit switched domains. Mobility management functionality is handled with help of protocols, and Chapter 4 provides an overview of them. The main attention in the thesis is paid to

GMM protocol, in details it is presented in Chapter 5. Chapter 6 represents the practical part of this thesis work. It describes implementation of GMM protocol. Chapter 7 gives conclusion of the thesis.

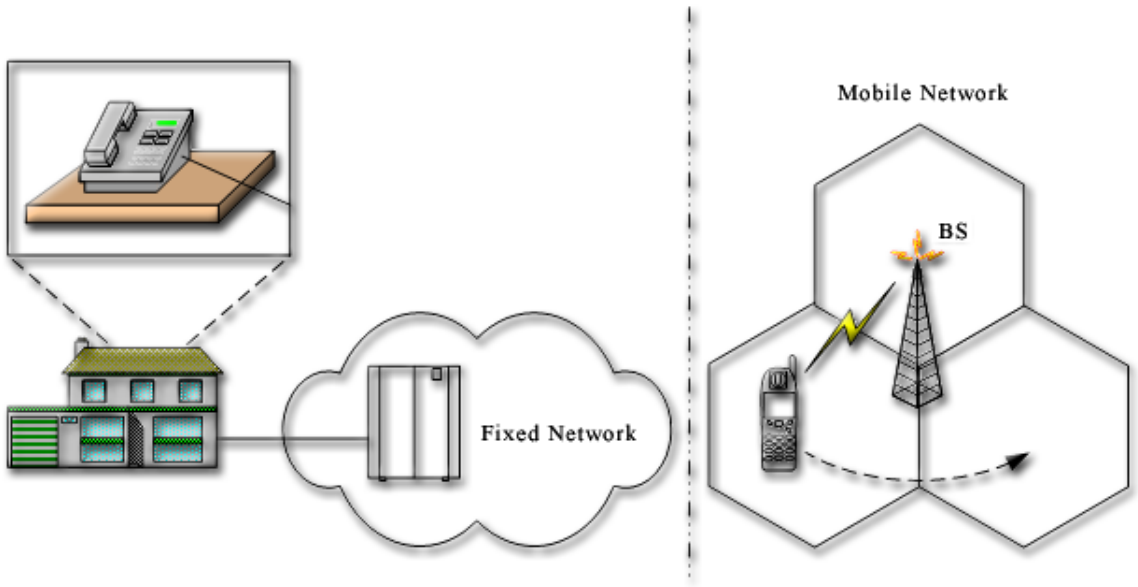
# 2. CONCEPTS OF MOBILITY MANAGEMENT

This chapter gives main definitions in area of mobile communications, explains term "mobility" and takes a close look at mobility management responsibilities. History of mobile networks allows understanding of the changes from generation to generation of cellular networks and makes emphasis to evolution of mobility.

## 2.1. Definition of mobility

After introduction of electromagnetic waves as a communication medium at the end of 19th century, this technique was used in radiotelegraphy and military service before became a part of public telephony. Over the last twenty years, there has been rapid growth of mobile communication market, what makes cellular network the most successful communication system.

Figure 2.1 helps to understand the principles of mobility. In fixed network the location of phone is always the same and there is permanent wire connection between the phone and the network. Thus the network always knows where to deliver calls.




**Legend:**
BS = Base Station

**Figure 2.1:** Concept of mobility

The opposite situation is in the mobile network. There is no wire connection between the phone and the network and the location of the mobile phone is changing from time to time. We will refer mobile phone as User Equipment (UE) in this thesis. The area controlled by one mobile service operator is divided into cells. Base Station (BS) provide radio transmission and reception for the cells it covers. BS is a network element, which performs cellular coverage. To deliver a call to the UE Base Station should know the cell where the UE is. Because the UE can move around the BS from one cell to another special mechanisms need to be introduced for controlling the location of each phone in the network. These mechanisms are supported in cellular networks and give the user a possibility to move anywhere.

Thus one of the main differences between fixed networks and mobile networks is user mobility. For fixed networks the location of user terminal is permanent and the services are always provided by the one network operator. Otherwise, in mobile networks, the user can be located and use services anywhere in the home network and possibly in the other operators' networks. So, mobility allows people to communicate with people, not with place. Mobility can be defined as ability of a user to originate and receive calls anywhere in home network and, if possible, in other mobile networks.

The continuous progress in the area of wireless technology and communication networks has enabled the creation of scenarios where users can access several information and services independently from their location. Specific mechanisms need to be implemented, that can adequately support the user's mobility and assure him/her to remain connected even if the user is moving. In next subsections I will describe which problems must be solved to provide mobility and how it is done in mobile networks.

Now, when term "mobility" was defined, let us take a look at evolution of mobility to clarify what changes were made from generation to generation and understand future developments in mobility.

### *2.1.1. Evolution of mobility from 1G to 3G mobile networks*

The first systems offering mobile telephone service were introduced in 1946 in St. Louis in the USA [11]. These first mobile phones were car-phones and they were heavy, bulky and expensive. Similar phones were set up in Europe in the early 1950s. At first with this

phone was not possible to talk and listen simultaneously, but in the 60's it was improved to a two-channel system. The system could support very limited number of users and characterized by poor speech quality, limited services and restricted mobility.

The introduction of cellular systems in late 1980s allowed increasing in capacity and mobility. These cellular systems could transmit only analog voice information, and was named as first generation (1G) mobile networks. Nowadays there are three different generations of networks in mobile communication. First generation networks offered basic mobility; it means that 1G networks were developed with national scope and they were incompatible with each other so that subscribers could not use any services outside the home network. The most popular 1G systems are Advanced Mobile Phone System (AMPS), Nordic Mobile Telephone systems (NMT), and Total Access Communication System (TACS).

As mobile networks became more and more popular, the need for more global mobile communication system increased. The main advantages of second generation (2G) networks comparing to 1G networks are compatibility and international transparency. Second generation networks introduced concept of advanced mobility, when the subscriber is reachable in other operators' networks and can receive and originate calls there. This feature was named as roaming. Possibility to roam between networks belonging to different operators makes 2G networks regional (like European-wide).

The development of 2G cellular systems was also driven by the need of transmission quality and system capacity improvement and for introduction of new services. 2G systems are based on digital transmission technologies and offer not only speech service, but also support of simple non-voice services like Short Message Service (SMS). Supplementary services such as swindle prevention and encrypting of user data became standard features.

Most successful example of 2G cellular systems is Global System for Mobile communications (GSM), supported mostly in European countries. Another examples are Japanese Pacific Digital Communications (PDC) and IS 95 used in North America. In spite of big success of GSM and other 2G networks they still have some limitations, one of them is that the concept of globalisation did not succeed completely and there are

different 2G technologies that do not interoperate. The third generation (3G) was expected to complete the globalisation process of the mobile communication, but in reality it is not so.

Universal Mobile Telecommunications System (UMTS) is an example of 3G mobile networks. Figure 2.2 illustrates general structure of UMTS system.


**Legend:**
ME = Mobile Equipment
SIM = Subscriber Identity Module
UE = User Equipment
UMTS = Universal Mobile Telecommunications System

**Figure 2.2:** UMTS system structure

UE is a device that the subscriber uses to access the mobile network. User Equipment consists of two elements: Mobile Equipment (ME) that contains hardware and software enabling radio communication, and Subscriber Identity Module (SIM) - a smart card that identifies the subscriber in the network.

UMTS Terrestrial Radio Access Network (UTRAN) is a part of UMTS network that is responsible for all radio related activities. It also provides access for UE to the functionality of the Core Network (CN). CN is a part of UMTS system that handles routing, switching, service provision and also provides possibility to connect external networks. Mobility management issues are mostly handled in UE and CN parts of UMTS network. In Core Network the node responsible for handling mobility functions is called Serving GPRS Support Node (SGSN). In more details the UMTS system structure as well as the description of network elements involved in mobility provision are given in Section 4.1 of this Master's thesis.

In 3G there can be distinguished three different types of mobility [12]:

- Terminal mobility,
- Personal mobility, and

- Service provider portability (or service mobility).

Terminal mobility refers to the ability of the network to route calls to the UE regardless of its location in the network. This type of mobility is similar to those that we have in 2G systems. Personal mobility can be defined as the ability of the user to access their personal services independent of their location or terminal. This means that the user is globally reachable and can originate and receive sessions by using different terminals. Service provider portability allows the user to receive his personalized end-to-end services regardless of current network. Subscribed services are personalised by user profiles, and they are provided regardless of user's location.

In UMTS UTRAN level mobility management was introduced, which takes into account the user's mobility within UTRAN. In UMTS different types of traffic: voice, video, packet data, etc., can be transmitted. To share radio resources efficiently and to meet Quality of Service (QoS) requirement UTRAN mobility management is needed. More details about this feature will be given in Section 3.2.2. Other benefits of 3G networks are high bit rate up to 2Mbit/s, multi-media messaging, video streaming, etc.

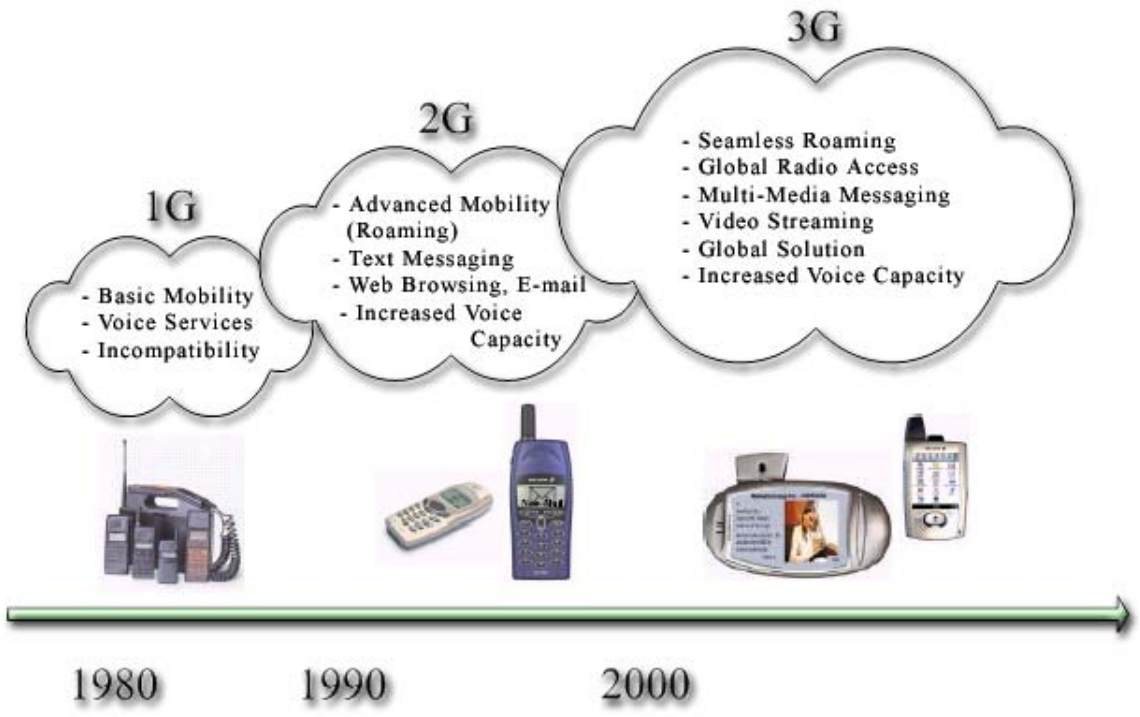



**Figure 2.3:** Mobile networks evolution [4]

Figure 2.3 summarizes the evolution path of mobile communication systems. Future development can be seen as introduction of new ways to handle and combine all kinds of data and mobility.

## 2.2. What mobility management is

Supporting of users' mobility creates very strict requirements for the cellular network. The set of procedures that were implemented to provide mobility can be combined under common name of *Mobility Management* (MM).

To make possibility for users of being reachable anywhere and any time four basic procedures were introduced: paging, location updating, roaming and handover operations. These features are presented in more details in the next section. In addition, the MM handles permanent and temporary identities and addressing information of the subscribers and theirs terminals as well as network elements. Mobility management includes functions that protect the confidentiality of the identities. Finally, MM appears in the role of provider for connection management and session management services.

Mobility management includes function to support mobility in both circuit-switched networks and in packet-switched networks. This thesis states the peculiarity of mobility management in packet-switched domain.

## 2.3. Mobility management responsibilities

The following sections give detailed overview of mobility management functions, such as location updating, paging, roaming and handover. The description starts with close look at location updating procedure and paging that are used to determine the user position in the network. Handover function is described next. Handover implements the possibility to move during the active call and keep good radio connection to the network. At the end of this subsection such feature as roaming is described. The section specifies differences between national, international and regional roaming and introduces the concept of global roaming.

### *2.3.1. Location management*

In the fixed networks the services available for the subscribers depend on the network that the subscriber's telephone line is connected to, and hence on the location. The services can be provided any time after subscriber is connected to the network. As the location of the terminal is permanent, it is known where the network has to deliver incoming calls. In mobile networks the situation is different because the UE is moving. It is necessary for the network to know where every registered UE is within the network in order to connect it on request. These functions are the part of mobility management named location management.

Location management procedures enable the GSM or UMTS network to determine the location of the mobile subscribers' phones. Location management is the two-stage process; the first stage is location registration, and the second is call or other request delivery. During the location registration stage the UE notifies the network about its current location. In circuit switched (CS) networks (like GSM) location update procedure is used; in packet switched (PS) networks (like UMTS) the same functions are executed by routing area updating procedure. These procedures are similar, but there are some differences. In CS networks cells are grouped into location areas (LA), while in PS domain they form routing areas (RA). Typically RA is a subset of an LA. More details about RAs and LAs can be found in Section 3.2.1. By reporting information about current LA/RA UE gives the network the information about its current location.

LA/RA update procedure is initiated by the UE and can occur when:

1. The UE is first switched on.
2. UE detects that the location has been changed. This type of update procedure is called normal LA/RA update.
3. A location update timer expires. That is, the UE periodically reports its presence to the network.

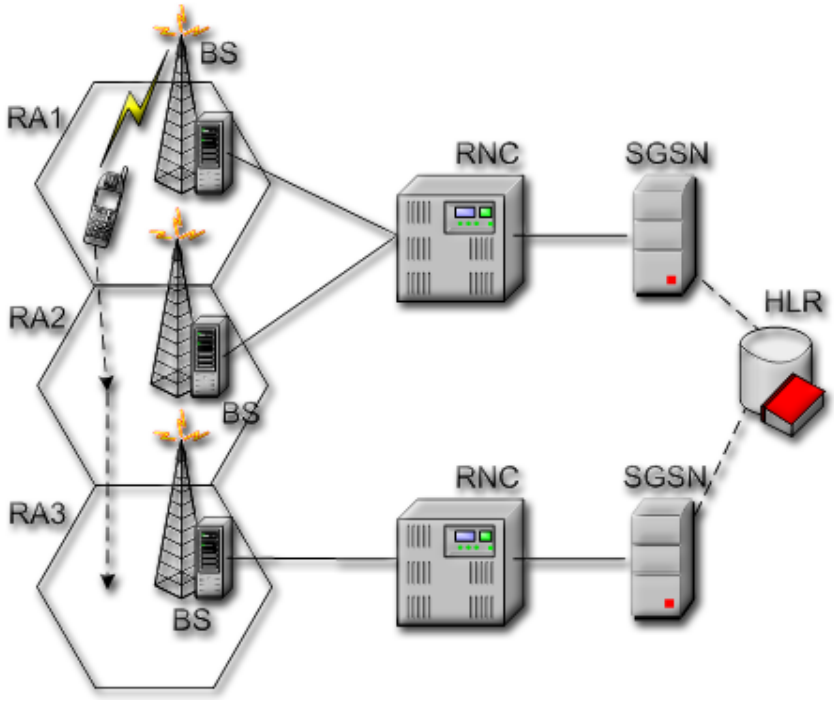
The location registration takes place whenever a UE is switched on. It makes the UE visible for the network. When the mobile phone is switched off, deregistration from the

network is made, after which the network knows that the UE is not reachable and does not try to establish any sessions.

Normal location/routing area update is performed when the UE detects a location/routing area change. It will notify the network that it is now located in a different area. Detection of location change is done as follows:

1. There is a special channel that UE can listen and that is used by the network to broadcast cell identity;
2. The UE periodically listens to the identities and compares it with the cell identity stored in the UE;

If the comparison indicates that the location has been changed, UE initiates location update procedure or routing area update procedure. Let us see an example on Figure 2.4.




**Legend:**

BS = Base Station
HLR = Home Location Register
RA = Routing Area
RNC = Radio Network Controller
SGSN = Serving GPRS Support Node

**Figure 2.4:** Routing Area Updating example

Before explaining the Figure 2.4 let us clarify some definitions. As you can see from the picture all the BSs are connected to the node, called Radio Network Controller (RNC). RNC is the main element of the UTRAN, which performs management of radio resources. Home Location Register (HLR) is database that is used to store and manage the permanent data about subscribers. When the user buys the subscription from the network operator, the subscriber's data is inserted into the HLR.

Figure 2.4 helps to understand how the Routing Area Updating procedure is performed. UE could move within the routing area RA1, from one cell to another, without the need for a routing area updating. If it moves from RA1 to RA2 the SGSN must be notified about this change by RA update procedure. If the UE moves from RA1 or RA2 into routing area RA3, then the HLR must be also notified of the change to know the address of new SGSN, and the SGSN in area 3 will store the mobile's new routing area information.

Periodic location update is used to inform the network about UE availability. If this procedure has not been performed in some period of time, the network assumes that the user equipment is not reachable. Periodic update is performed at certain time intervals, which is specified by a network operator.

In UMTS periodic RA update timer is controlled as in the UE as in SGSN. The value of timer is set in SGSN and the UE receives it every time it visits RA. When the timer of the UE expires, the UE initiates a periodic Routing Area Update. After this both, the UE and the SGSN, reset their timers.

In order to be able to route the incoming calls, the network keeps track of the location of the UE, as it was explained earlier. But the location information is needed to be stored. For this purpose the functional units called location registers are used. The two main types of location registers are:

- Home Location Register (HLR), which was already mentioned above.

- Visitor Location Register (VLR), where subscriber data is stored as long as the UE is within the area controlled by this VLR. In UMTS VLR is usually combined with SGSN in one physical node.

More detailed information about registers is given in Section 4.1.1 of this master's thesis.

### *2.3.2. Paging*

The paging procedure is needed whenever network has a call that should be delivered to the UE. Since the connection with network is only established at initiative of the UE, the network needs some mechanism to trigger this establishment; this role is fulfilled by the paging procedure.

When the RA update is performed, the network knows the location area or routing area where the UE is. In order to make the call delivery, the system must determine in which cell the UE is. When the call arrives, a paging message is send to all cells in the RA where the user is known to be (see Figure 2.5). UEs are listening to the special channel through which the paging message is delivered. All the UEs in the RA listen to the same channel, and the paging message contains the ID using which the UE can check if the message was sent to this UE or not.

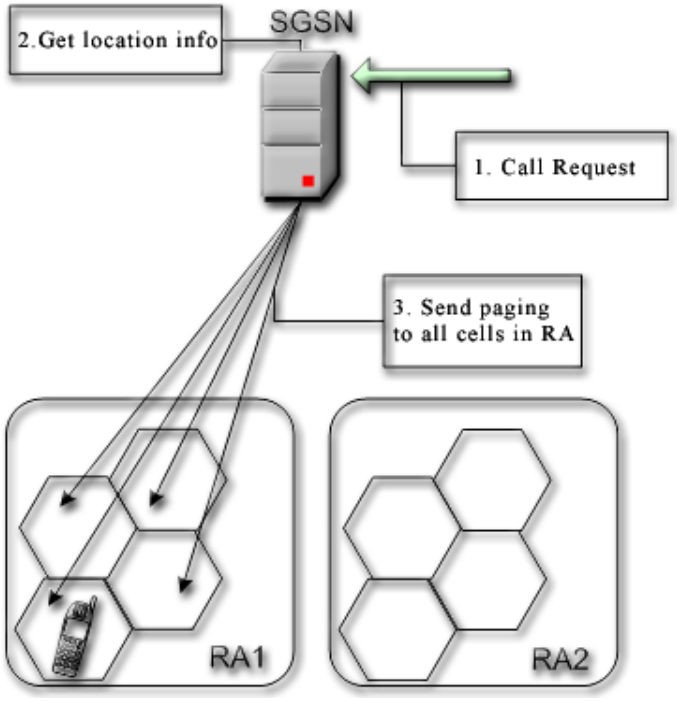



**Figure 2.5:** Paging procedure

In UMTS two types of paging are specified: Paging Type 1 and Paging Type 2. Paging Type 1 is the conventional way to use paging. Paging Type 1 procedure commands the

UE being idle to invoke the establishment of packet switched radio connection to the network. UMTS terminals are able to handle various connections simultaneously. When the UE already has a connection with the core network and one more connection is needed the Paging Type 2 is sent to the UE. Paging Type 2 message is always addressed to the one UE only.

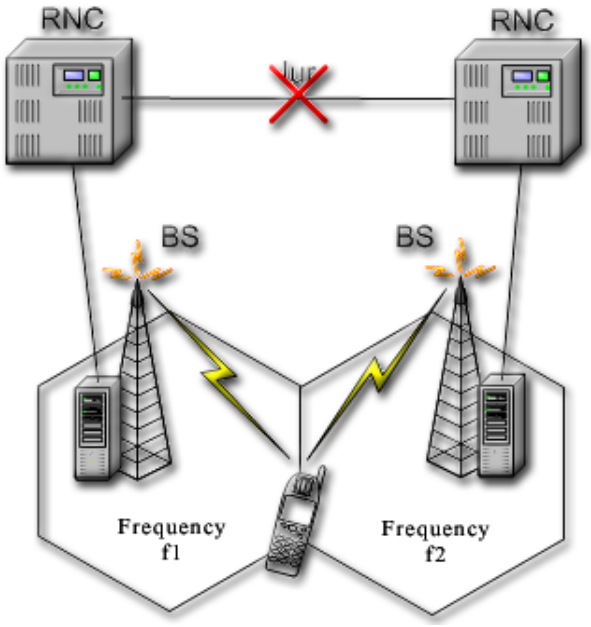
### *2.3.3. Handover*

Another feature that makes mobility possible is handover. Handover enables the network to maintain a user's connection when the user continues to move and change his/her location. The main reason behind the handover is that due to a movement a user can be served more efficiently in another cell (for example with less power or better connection quality), so the mobile station or network initiates actions in order to improve the connection. Handover mechanism gives the user possibility to move while having an active call or session.

The basic concept of handover is simple: when the subscriber moves from the coverage area of one cell to another, a new connection with the target cell is set up and the connection with the old cell is released. The number of handovers is straightforward dependent on the degree of user's mobility. If the user keeps on moving into the same direction then it can be said that the faster the user is moving the more handovers to be made.

Classification defines three categories of handover mechanisms: hard handover, soft handover and softer handover. If the during handover process, the old connection is released before establishing new one, it called as a hard handover. The hard handover can be further divided into intra-frequency and inter-frequency hard handovers. In case of intra-frequency hard handover the carrier frequencies of radio access before and after handover performed are the same. On the other hand, if the new carrier and the old carrier differ then inter-frequency handover is made. Inter frequency handover may happen between two different radio access networks, for example, between GSM and UMTS, so it also can be classified as inter-system hard handover.

Figure 2.6 shows an example of hard handover – inter-frequency hard handover. In practice a handover that requires a change of the carrier frequency is always performed as hard handover [16].



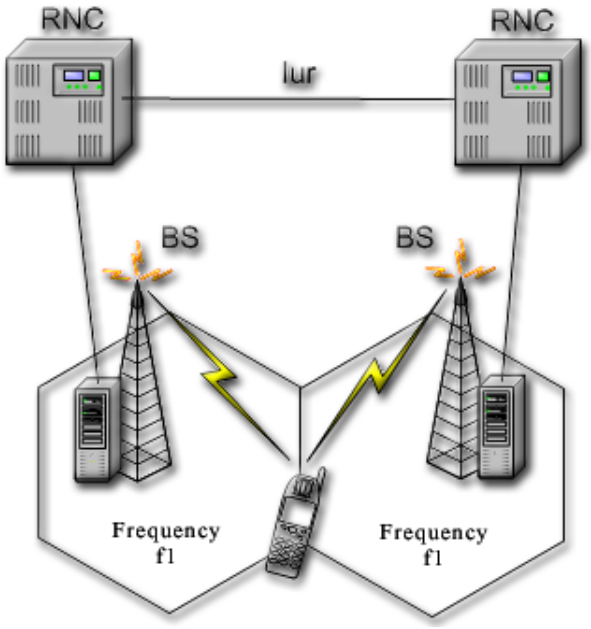

**Legend:**
BS = Base Station
RNC = Radio Network Controller

**Figure 2.6:** Inter-frequency Hard Handover [4]

Unlike in hard handover, when the soft handover is performed a new connection is established before the old connection is released, so the UE always keeps at least one radio link to the UTRAN. Soft handover is a feature of UMTS network, and it was not possible in GSM. This is so, because the interface, named Iur, exists between two RNCs.

For better understanding of difference between hard and soft handovers let us see a simple analogue that was given as en example on 3G System course in Nokia Learning Center. Imaging Tarzan in jungle that is standing on a tree and hold a liana. When he decides to jump to new tree, he starts jumping, leaves the liana, and only after that holds a new one. He can also jump by another way: when jumping Tarzan holds new liana, so that he is holding two lianas simultaneously, and after that he leaves the old one. The same situation is happens in hard and soft handover respectively. In soft handover the UE always have connection to the network.

Soft handover is performed between two cells, controlled by different Base Stations, but not necessary belonging to the same RNC. All RNCs involved into a soft handover must coordinate the work over the Iur interface.




**Legend:**
BS = Base Station
RNC = Radio Network Controller

**Figure 2.7:** Intra-frequency Soft Handover [4]

In soft handover the neighbouring cells involved in the handover process use the same frequencies. Most of handovers in the UMTS system are intra-frequency soft handovers (Figure 2.7).

Softer handover is a special case of soft handover and it is also UMTS specific feature. In case of softer handover the radio links that are added and removed always belong to the same BS. UTRAN is able to perform soft and softer handovers at the same time. When it happens, the term soft-softer handover is used.

Performing the handover needs radio resources control, so in spite that the handover increase user mobility it is related to Radio Resource Management, not Mobility Management and we will leave further considerations about this topic out of the thesis.

### *2.3.4. Roaming*

Another function of mobility management is roaming. The MM functions inside a home network allow a user to move freely within the coverage area of this single network. Roaming is an ability, which makes it possible for the users to move from one network to another that is operated by a different operator company and possibly even in a different country. Roaming can be provided only when some administrative and technical constraints are met, and there is some agreement between operators. Issues like terms and conditions of payments, subscription agreements, and etc. must be solved between operators. In addition it requires a user to have a UE enabling him/her to access different networks. If different network operators co-operate, they can offer their subscribers a coverage area that much wider then any of them could do on its own.

There can be categorised three different types of roaming: national roaming, international roaming, and regional roaming. In national roaming the UE can use services within a network of the same country from that of user's home network. The UE makes a periodic search for the home PLMN (Public Land Mobile Network) while roaming nationally, thus it automatically returns to the home network when this is possible.

National roaming allows the operator in a certain national network to differentiate between an area where roaming from neighbouring networks is allowed, and another where it is denied. This subtype of national roaming is called regional roaming. By another words, regional roaming allows the network operator to control subscriber roaming. In this case the roaming area can be a single location/routing area, several location/routing areas or the whole PLMN.

In international roaming subscribers can use their UEs in network of a different country from that of the home network. Due to roaming agreements between different operators in different countries, subscribers can be offered service in these operators' networks.

In addition to these roaming in 3G networks, it should be possible to change the network from the third generation to the second generation system. This should provide seamless basic service even when there is no 3G network coverage available.

At the end of this section I would like to define term *global roaming*. Global roaming can be divided into two types, subscriber and mobile phone roaming. The mobile phone roaming means that the same piece of equipment works in the same way in all the networks. For example, a mobile phone that was bought in Finland should work correctly in the USA, Japan or any other part of the world.

With subscriber roaming it is possible to use services you have in the home network within the other networks by changing the SIM card from one mobile phone to another. For example, when travelling to the USA you can take with you only the SIM card and plug it in a mobile phone rented in the USA. Both subscriber and mobile phone roaming is planned to be implemented in the 3G systems. Nowadays mobile systems do not support global roaming and it can be seen as a goal for future developments.

### 2.4. Identities of users and their terminals

To control user mobility the network has to somehow separate users and their terminals from each other. For identification, service separation, routing purposes and security different types of identities are used, as summarised below:

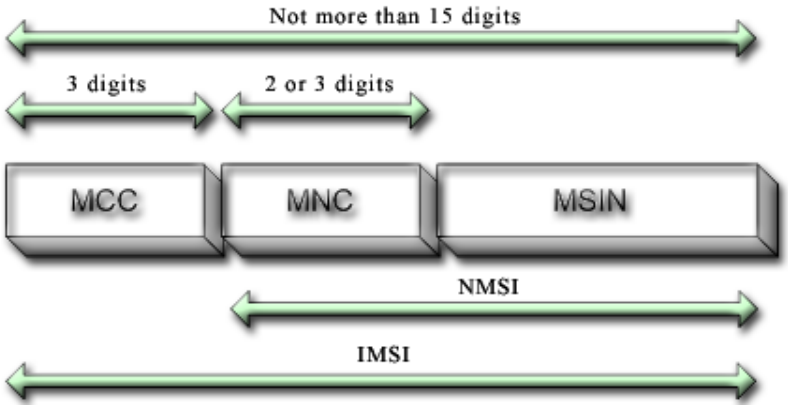
- International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) are used for identification purposes.

- Mobile Subscriber ISDN Number (MSISDN) is needed for service separation to recognise the service to be.

- In order that routing process being not fixed to any network it uses Mobile Subscriber Roaming Number (MSRN).

- For security provision it is recommended to use Temporary Mobile Subscriber Identity Number (TMSI) and Packet Mobile Subscriber Identity (P-TMSI).

IMSI provides global identification for a subscriber and shall be allocated to each subscriber. This value acts as primary search key for all registers to maintain subscriber information and charging. IMSI shall not exceed 15 digits, and can be composed of three main parts as shown on Figure 2.8.

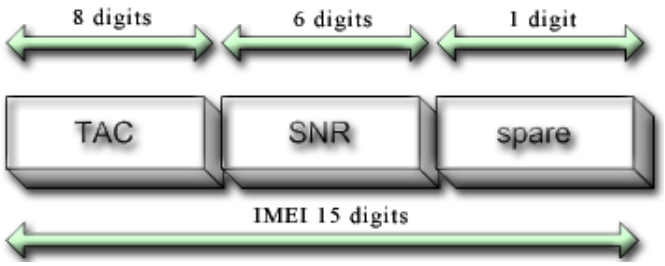



**Legend:**
MCC = Mobile Country Code
MNC = Mobile Network Code
MSIN = Mobile Subscriber Identification Number

**Figure 2.8:** Structure of IMSI [6]

Mobile Country Code (MCC) consists of three digits and identifies subscriber's home country. All country codes can be found in Appendix A to CCITT Blue Book Recommendation E.212. Mobile Network Code (MNC) uniquely identifies home PLMN and can consist of two or three digits. The length of MNC depends on mobile country code and differs for all network operators within one country. The network operator gives to the user on subscription Mobile Subscriber Identification Number (MSIN) consisting of 9-10 digits. MNC and MSIN make together National Mobile Subscriber Identity (NMSI). The IMSI number is the identity used by network, not by other subscribers, so it is not number you dial.

IMEI uniquely identifies ME (see Figure 2.9). It consists of the following elements: Type Allocation Code (TAC) and Serial Number (SRN). There is separate register handles this value – Equipment Identity Register (EIR). All the IMEI numbers are handled in three categories that represented as lists in EIR: White List, Grey List and Black List.

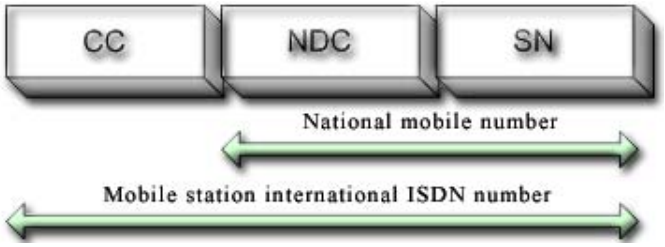



**Legend:**
TAC = Type Allocation Code
SNR = Serial Number

**Figure 2.9:** Structure of IMEI [6]

IMEIs listed in White list are normal identities, which do not have any limitations. Grey-listed IMEI numbers are under observation and network controls each transaction with this UE in use. If the UE is on the Black list any transactions are rejected except emergency calls. The network may or may not perform IMEI checking procedure.

Because one subscriber can have more then one service activated, MSISDN is used as a separator between them. Thus the mobile user can have one MSISDN for speech service and another number for facsimile service and so on.




**Legend:**
CC = Country Code
NDC = National Destination Code
SN = Subscriber Number

**Figure 2.10:** Number Structure of MSISDN [6]

There are three parts in a MSISDN (Figure 2.10):

- Country Code (CC) of the country in which UE is registered,
- National Destination Code (NDC) of the network, and
- Subscriber Number (SN).

MSISDN is a number you dial to call another subscriber.

MSRN - Mobile Subscriber Roaming Number - is used to route calls to the UE. MSRN and MSISDN have the same structure even if they are used for different purposes.

In order to support the subscriber identity confidentiality temporary identities are used instead of IMSI. These identities are called Temporary Mobile Subscriber Identity (TMSI) and Packet Temporary Mobile Subscriber Identity (P-TMSI), which is allocated in circuit switched (CS) and packet switched (PS) domains respectively. These temporary identities have time and area limited validity. TMSI is allocated by the VLR and valid until the UE performs next transaction. P-TMSI is generated by the SGSN and it is valid in area, which is controlled by this SGSN. TMSI and P-TMSI are random generated numbers, which length is less then 4 octets. The network shall not allocate the number with all 32 bits equal to 1, because when the number is stored in SIM card this means that no valid TMSI (P-TMSI) is available.

### 2.5. Location structures and identities

To determine the location and differentiate one area form another, each location structure should also have an identity.

Location is one of the main terms in mobility management and it is refers to the location of the end-user within the logical structure of the network. The network uses location information in order to reach the users when it is needed.

In UMTS network four types of logical structures are defined:

- Location Area (LA),
- Routing Area (RA),
- UTRAN Registration Area (URA), and
- Cell.

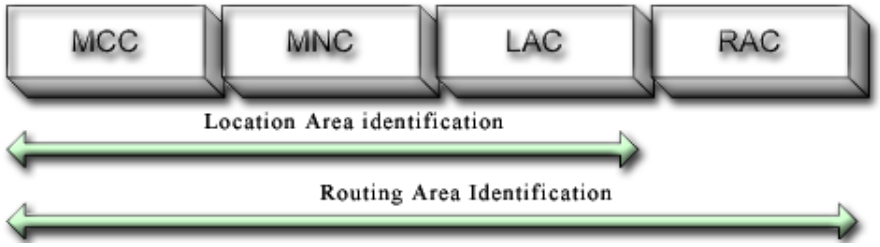
Location Area is the area where the user can move without performing the Location Updating Procedure. It consists of Cells, the smallest logical entity in the mobile network. LA can consist of one Cell or group of Cells up to all the Cells under the VLR. LA is

defined in circuit switched domain. To make it possible to distinguish one LA from another each location area has unique identity – Location Area Identity (LAI). The LAI is composed of the following elements:

$$LAI = MCC + MNC + LAC.$$

MCC and MNC have the same format as in the IMSI number (see Section 2.4). LA code is a fixed length of two octets number that cannot be repeated within the PLMN. Thus there are cannot be found two location areas with the same LAI; this identifier is unique number throughout the world.

For the same role as LA plays in CS domain packet switched domain has RA, which is very similar to LA. The UE may move inside routing area without performing RA update procedure. One LA may have several RAs within it, but not vice versa, so RA is a kind of subset of LA and what is more one RA cannot belong to two location areas. Routing Area Identification (RAI) and LAI structures are shown on Figure 2.11.




**Legend:**
MCC = Mobile Country Code
MNC = Mobile Network Code
LAC = Location Area Code
RAC = Routing Area Code

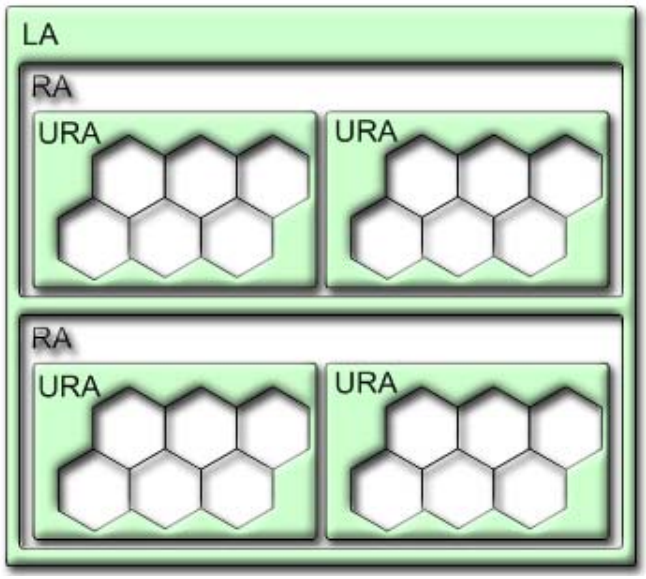
**Figure 2.11:** Structures of Location Area Identification and Routing Area Identification [6]

Routing Area Code (RAC) has fixed length of one octet and should not be duplicated within a location area.

In GSM network the mobility management functions is completely handled by the UE and the Core Network, but in UMTS the UTRAN is also involved in MM. UTRAN Registration Area (URA) is one of the key elements in UTRAN mobility. A URA is

defined as an area covered by a number of cells. It is not visible in the Core Network and known only within the UTRAN. Like in case of LA and RA, when the UE is entered to the new UTRAN Registration Area URA update procedure shell be made.

The Cell is the smallest location structure entity having its own publicly visible identity called Cell ID (CID). CID number can be coded using full hexadecimal representation and has length of two octets. To globally separate cells from each other the Cell Global Identity (CGI) is used. CGI consists of the Location Area Identification and Cell Identity. CI must be unique within a location area.




**Legend:**
LA = Location Area
RA = Routing Area
URA = UTRAN Registration Area

**Figure 2.12:** Mobility Management logical entities relationships [4]

Figure 2.12 summarises all the writing above in a way of showing the relationships between different mobility management logical entities.

# 3. COMPARING OF MOBILITY MANAGEMENT IN PS DOMAIN TO MOBILITY MANAGEMENT IN CS DOMAIN

## 3.1. Overview of switching methods

Mobility management in packet switched domain differs from mobility in circuit switched domain. This is so because transmission techniques used for data sending are not the same and requires different solutions for providing mobility.

There are two main switching methods for data transmission: packet switching and circuit switching. The following sections make overview of these switching techniques and help to understand the reasons for changes made in PS mobility compared to mobility in CS networks.

### *3.1.1. Circuit switching*

Circuit switching is the most familiar technique used to build a communications network nowadays. This is the process that establishes connections on demand and allows exclusive use of the connections until they are released.

Figure 3.1 considers an example of communication between two points A and D in a network. Let us assume that the direct connection between A and D is not possible and using of two other transit nodes, B and C, is required.

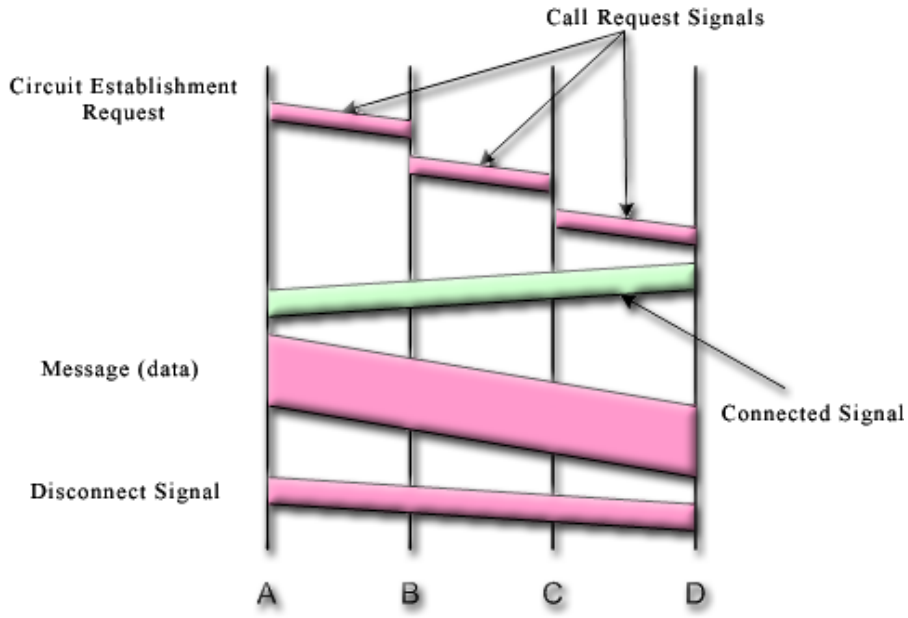



**Figure 3.1:** Circuit switched connection between A and D (Information flows in two directions. Information sent from the calling end is shown in darker colour and information returned from the destination is shown in light colour)

Circuit switching is composed of three phases:

- Connection phase, during which a circuit between source and destination is set up. When establishing a connection, each switching node is looking for a trunk available for connecting to the destination and reserves resources that will be used, thus searching delay is appeared. Delay during the setting up process can be high. After completion of the connection, a signal confirming circuit establishment is returned; it flows directly back to node A with no search delays since the circuit has already been established. After that the second phase starts.

- Transfer of the data.

- Termination phase. After data transfer has been finished, the connection is disconnected and resources should be released.

In circuit switching a network resources are reserved for the call, and no other call can use those resources until the original connection is closed. As you can see the usage of network resources are not rational, and they even reserved if long silence is between two users.

Circuit-switching systems are ideal for communications that require data to be transmitted in real-time, such as voice or video.

### *3.1.2. Packet switching*

The other common communications method is packet switching, which main concept is to divide messages into packets and send each packet individually. For routing purpose each packet has a header that contains information about the source, destination, packet numbering, etc.

In packet switching the packets belonging to different messages can share one line that makes usage of network resources very efficient.

There are two basic approaches in packet switching:

- Connection-oriented, and
- Connectionless.

In the connection-oriented packet switching the first initiating message is sent to set up a route between the intermediate nodes for all the packets passed during the session between two end-nodes. In each node, an entry is registered in a table to indicate the route for the connection that has been set up. Every packet belonging to the session goes through the same path as first initial message and can have only short header, containing a session identifier, and not their destination. In this way, packets arrive to the destination in the correct order.

It seems that this approach quite similar to circuit switching despite the message is spitted to the packets, but there are much more differences. In case of connection-oriented no actual channel is set up, so different virtual circuits may compete over the same resources. Connection-oriented packet switching is slower than circuit switching, but it makes efficient use of network resources.

This method can be used as alternative to circuit switching, but in this case some additional actions should be done to guarantee the constant transmission delay or needed capacity.

Connectionless approach uses more dynamic scheme to determine the route through the network links. There is no initial phase and packets are transmitted independently from each other. Its headers must contain full information about the destination for routing. The intermediate nodes examine the header, and decide to which node the packet should be sent to reach its destination. In the decision two factors are taken into account:

- The shortest path to the destination;
- Finding an available destination from alternate routes.

Thus, in this method, the packets do not follow a pre-established route and can be sent by different ways. Due to the nature of this method, the packets can reach the destination in a different sequence than they were sent, thus they must be sorted at the destination and reordered.

Packet switching is better suites for sending data that is not time-critical, such as file transfer, e-mail messages, and Web pages.

UMTS network is packet switched network and because of this some differences exists between UMTS mobility and mobility in circuit switched networks, such as GSM. Section 3.2 takes a look at this topic.

## 3.2. Features of mobility in PS mobile networks

This section points an attention on features of mobility in packet-switched mobile networks. Most of procedures are very similar in both domains, but packet nature of UMTS network cause making some changes. I would like to focus on new feature in UMTS – UTRAN level mobility management, and to describe changes in location management.

### *3.2.1. Specials in location management*

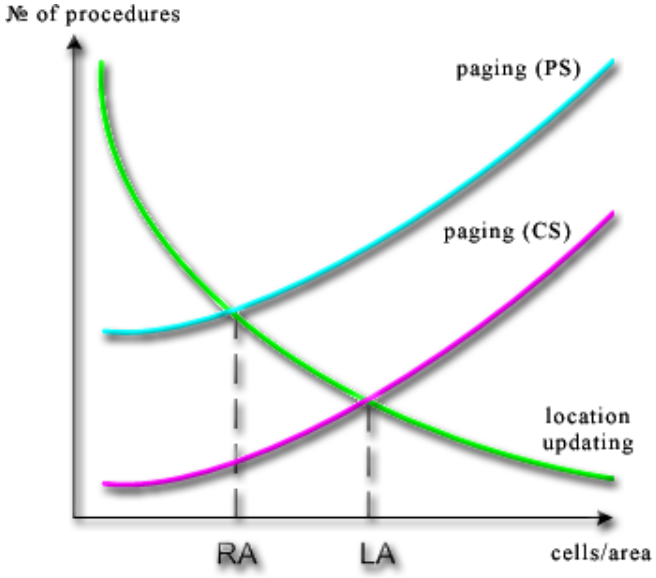
Handling the UE's location is one of the main responsibilities of mobility management. In circuit switched domain it is done with help of Location Update procedure, and in packet switched domain Routing Area Updating procedure is used. Both procedures are executed in similar ways, but there are some differences.

First of all, the RA updating is performed each change of routing area, so it is executed more often than location updating procedure. In this section I will try to explain the reason for this change.

The main task of location management is to keep track of the user's current location, so that incoming packets can be routed to his or her UE. For this purpose, the UE periodically sends routing area update messages to the current SGSN. If the UE sends updates rather rare, its location is not known exactly, and it is necessary to page the UE each time the network has a downlink packet. As a result a significant delivery delay appears. On the other hand, if location updates happen very often, the UE's location is well known, and the data packets can be delivered without any additional paging delay, but in this case quite many of uplink radio capacity and battery power is consumed.

Thus for a good location management a compromise between these two methods should be found. Similar situation is in case of circuit switched domain, despite of difference that the message is not divided into the packets.

Figure 3.2 shows the dependency of amount of procedures (location updating and paging) performed from LA/RA size. Updating procedure is performed each change of area and does not depend from the domain where it is done. Paging procedure is executed every time the network has data to transmit. In packet domain one message is spited into the packages and paging is performed each time the packet is sent, so to sent a whole message the network makes paging a few times, while in CS domain paging is done only one time per message.




**Legend:**
LA = Location Area
RA = Routing Area

**Figure 3.2:** Determining of LA and RA size

As you can see from the Figure 3.2 for efficient mobility management it is needed that the size of area in PS domain is smaller than the size of area in CS domain, thus RA updating in packet networks need to be performed more often than LA updating in circuit networks.

While performing routing area updating procedure it is also possible to update the information about the current location area, because RA is a subset of LA, thus for this purpose it is needed to make a possibility for transmission parameters of both domains. It is not necessary to make location update every time when RA update is performed, but such feature helps to avoid performing of two updating procedure in time the RA and LA are both changed.

### *3.2.2. UTRAN mobility management*

As was described earlier, in the packet networks the same radio resources can be used for transmutation packages from different sources, and thus to transmit different types of traffic. Therefore new mechanisms need to be introduced for more efficient sharing of the

radio resources. To respond to this demand, new type of mobility management – UTRAN level MM – was introduced.

UTRAN level mobility management refers to those functions that keep the UE in touch with the UTRAN radio cells, control the user's mobility within UTRAN and take into account the type of traffic it is using. This is one of differences between circuit switched mobility management in GSM, where mobility management took care of CN subsystem only, and packet switched MM, where controlling of radio resources and user's mobility within UTRAN is needed because of packet nature of sending data.

Because the UTRAN mobility management is close to radio related details that are not covered by this master's thesis, I will not go to more concrete description of the feature. If you interested in this topic please refer to the book "UMTS Networks" [4].

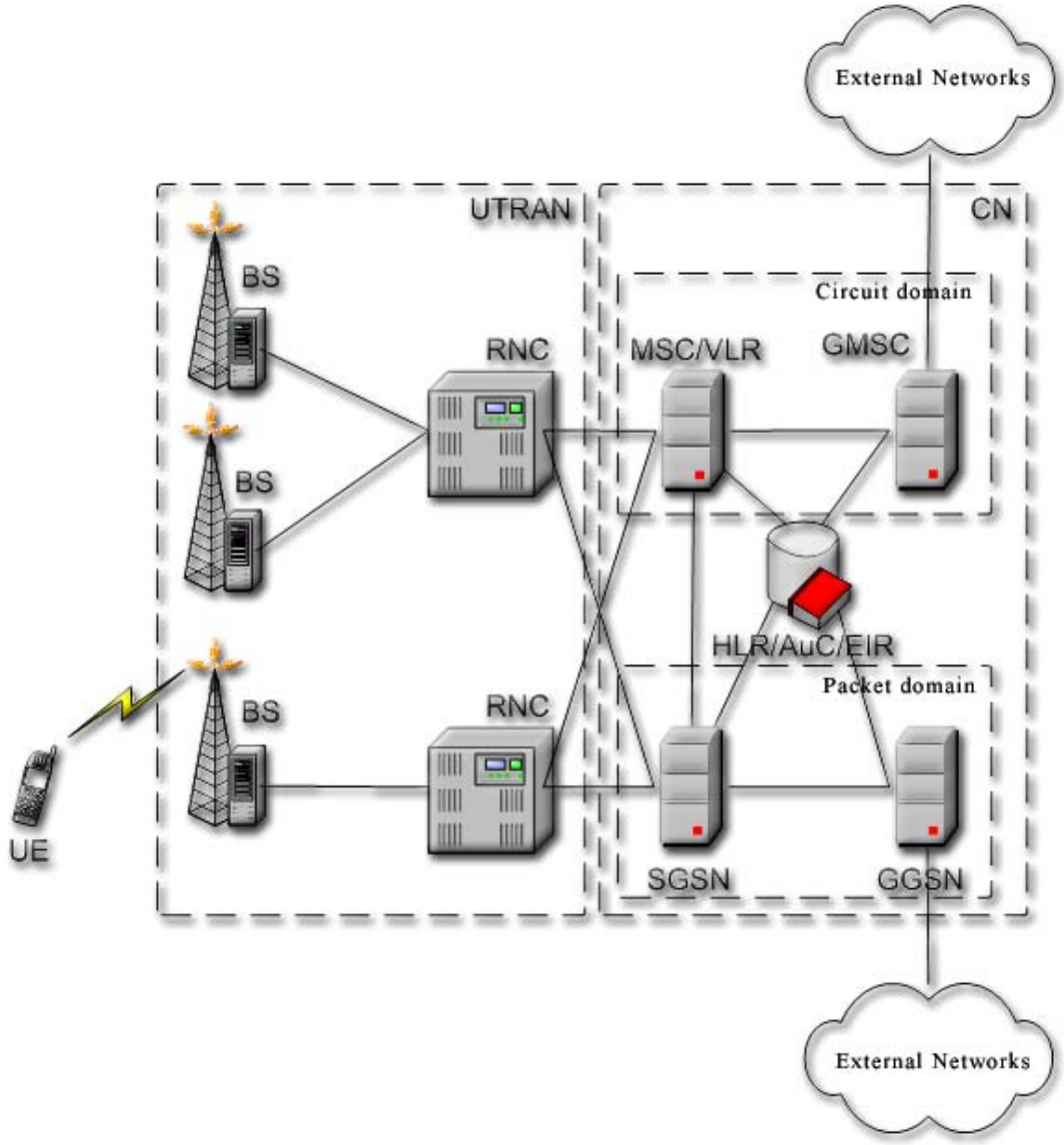
# 4. MOBILITY MANAGEMENT PROTOCOLS

## 4.1. Network elements involved into mobility management

Figure 4.1 illustrates the architecture of the UMTS network. The UMTS network can be split into two main parts: Core Network and UMTS Terrestrial Radio Access Network (UTRAN). Mobile equipment of the end user is referred as User Equipment (UE) in UMTS. UTRAN handles all radio related procedures and provides a mechanism for UE to access the functionality of the Core Network. The packet switched domain of the CN is responsible for providing packet switched services, connection and access to the external networks, switching and routing. Packet domain of CN consists of the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). Another important part of CN is registers. Registers do not belong to any of the domains and used as databases of different types of subscriber's information.

To make mobility of users and theirs terminals possible, the communication between different parts of network is needed. Mobility management issues are mostly handled in UE and CN parts of UMTS network. Signalling exchange is done with help of protocols that will be described bellow, but to clarify the purposes of different mobility management protocols it is needed to explain functionality of network elements involved into mobility.

The SGSN is the node that serves the UE. It is mainly handles the functionality related to mobility management. It responsible for the maintenance of location information of UEs, controls security functions. It is also combined with a database (VLR) where user’s identities, such as IMSI or P-TMSI are stored, and there is also information about the identity of current RA for each user, that is registered in this SGSN area. Similar functions in CS domain are performed by node named Mobile Services Switching (MSC). In practice MSC is usually combined with VLR in one physical device. In this thesis we will refer the node that combines SGSN and VLR functions to SGSN to distinguish it from the CS domain device.




**Legend:**

AuC = Authentication Center
BS = Base Station
CN = Core Network
EIR = Equipment Identity Register
GGSN = Gateway GPRS Support Node
GMSC = Gateway Mobile Services Switching Center
HLR = Home Location Register
MSC = Mobile Services Switching Center
RNC = Radio Network Controller
SGSN = Serving GPRS Support Node
UE =User Equipment
UTRAN = UMTS Terrestrial Radio Access Network
VLR = Visitor Location Register

**Figure 4.1:** UMTS architecture

The main task of GGSN is to provide communication with external networks. The external network sees GGSN as a router, which hides UMTS network detail. It maintains

routing information for the registered UE and routes packets from external networks to SGSN. Procedures of GPRS Tunnelling Protocol (GTP) are used for achieving this result. The SGSN and GGSN functionalities may be combined in the same physical node, or they may reside in different physical nodes. GMSC provides similar to GGSN functionality for CS network domain.

### *4.1.1. Registers of Core Network*

The part of core network named registers contains addressing and identity information for both CS and PS domains. This information is used for performing mobility management procedures. There are four main registers: Home Location Register (HLR), Authentication Center (AuC), Equipment Identity Register (EIR) and Visitor Location Register (VLR).

HLR is the database where permanent information of subscriber, such as IMSI, MSISDN, current SGSN address, information about permitted services and etc., is stored. One subscriber can be registered into only one HLR. The subscriber information is permanently placed into HLR of a network's operator in time the user is subscribed to this operator services. The information stored in HLR is used by both, an MSC and SGSN.

The VLR database contains temporary information about subscribers, for example, TMSI, LAI of location area where the subscriber was registered last time. Every time a mobile phone moves into a new MSC area, the VLR covering that area informs the HLR about the new location of the UE using the LAI. The information stored in VLR is related only to those subscribers that are currently within the area controlled by the MSC, and the information is removed when the subscriber leaves this area. VLR participates in mobility management for CS domain. In packet domain the same functions that VLR executes in CS domain are performed by SGSN.

The Equipment Identity Register maintains the information related to mobile phones hardware. The International Mobile Equipment Identities (IMEIs) are stored in this database. All the IMEI numbers in the EIR are grouped into three categories: White List, Grey List and Black List. The different classifications determine whether a UE is allowed to receive services or not. Stolen UEs can be registered in Black List, in this case no calls

can be made from the UE and because the location of switched-on phone is known it is easier to find the UE.

AuC is a database that handles security parameters needed to provide confidentiality, verify user's identity. It is stores an authentication key used to check the authenticity of the subscriber and calculate the parameters for providing cipher communication. Typically the AuC, HLR and EIR are integrated together in one physical device.

### *4.1.2. User Equipment*

To be able to use services provided by the UMTS network the user needs special device called User Equipment. The UE connects to the network via the radio interface. User Equipment consists of two main elements: Mobile Equipment that is hardware and software enabling radio communication, and Subscriber Identity Module that is a smart card identifies the subscriber in the network. SIM contains subscriber information such as IMSI, TMSI (P-TMSI), services available and security parameters. SIM is a very important in mobility management. If SIM is removed from the ME, mobility cannot be provided. Thus the user cannot make calls or receive calls if SIM is removed.

A UE can operate in one of three modes of operation, which allow using different services. The different UMTS mobile station operation modes are defined as follows [2]:

- PS/CS mode of operation: Operating in this mode the UE is attached to both the PS domain and CS domain, and it is capable of simultaneously access to PS services and CS services.

- PS mode of operation: The UE is attached to the PS domain only and may only use services of the PS domain. In this case CS-like services, such as voice calls, can be offered over the PS domain.

- CS mode of operation: The UE is attached to the CS domain only and only services of the CS domain can be offered. However, this does not prevent PS-like service to be offered over the CS domain.

## 4.2. Overview of the protocols

Due to the mobile nature of the subscribers there is needed to transport subscriber related information between different parts of the UMTS system. Mobility management protocols described below provide interfaces for information transfer.

### *4.2.1. GPRS Mobility Management protocol (GMM)*

GMM handles users' mobility management issues that are specific for packet switched domain. It operates within the signaling plane of UMTS. One peer entity of GMM resides in UE and the other is in SGSN. The main function of GMM is to keep a User Equipment attached to the network and ready for data transmission and receiving until otherwise requested either by the user or the network. Controlling the location of the UE makes possible to deliver calls at any time the mobile phone is within the coverage area and powered on. GPRS Mobility Management also takes care of the identification of the subscriber and his/her equipment and performs the security functions between the UE and CN.

Similar functions in circuit switched domain are done by Mobility Management protocol (MM). When functioning, GMM continuously co-operate with MM that is done for supporting both packet-switched and circuit-switched domains. GMM also forwards Session Management (SM) layer data from the UE side to network side and backwards.

In more details GMM functionality is described in Chapter 5 of this Master's Thesis.

### *4.2.2. Summary of Mobile Application Part protocols*

Mobile Application Part (MAP) is the protocol responsible for information exchange within the fixed part of the mobile network. MAP version for 3G networks is responsible for controlling the following network interfaces:

- The interface between SGSN and HLR;
- The interface between GGSN and HLR;
- The interface between SGSN and EIR; and

- The interface between SGSN and MSC/VLR.

Supporting of these interfaces makes MAP important part of many mobility management procedures, such as Routing Area updating and roaming.

More details concerning MAP protocol can be found in 3GPP TS 29.002 [19].

### *4.2.3. Role of GTP protocol in roaming and handovers*

Serving GPRS Support Node is used to communicate with UE. SGSN is a Core Network element that is responsible for providing mobility. If the data, either signalling or user should be transferred to outside networks, SGSN needs to communicate with GGSN that controls outside connections. This communication is implemented using GPRS Tunnelling Protocol (GTP). Thus GTP is responsible for interaction of two GPRS Support Nodes, such as SGSN and GGSN.

GTP is defined as for interface between two GSNs within the one network, as for interface between two GSNs in different networks. Such connections are very important to provide roaming and perform handovers.

GTP is divided into two different planes: signalling plane (GTP-C) and transmission, or user plane (GTP-U). The main concept in GTP is *GTP tunnels*, that is the virtual connections between two GSNs. In the signalling plane, GTP defines a tunnel management and control protocol that allows the SGSN to provide UE access to the network. Signals are used for creating, modifying and deleting of tunnels. In the user plane, GTP uses a tunnelling mechanism to provide possibility for carrying user data.

GTP protocol is specified by 3GPP organization and the details could be found in technical specification 3GPP TS 29.060.

### *4.2.4. Mobility functions of RRC and RANAP protocols*

Radio Access Network Application Part (RANAP) and Radio Resource Control protocol (RRC) provide the services for transporting MM layer messages. RRC takes care of establishing and maintaining of connections between the RNC and UE, and RANAP is responsible for controlling connections between RNC and SGSN. Together RRC and

RANAP provide end-to-end connection for mobility management layer. Thus these protocols are used as transport while performing such mobility management procedures as Routing Area Updating procedure, registration to the network and deregistration from the network and many others. Performing of paging, handover and UTRAN level mobility needs using of RRC and RANAP as well.

In technical specifications 3GPP TS 25.331 and 25.413 can be found more detailed descriptions of functionality of RRC and RANAP protocols respectively.

# 5. ROLE OF GMM PROTOCOL

This chapter explains in details GPRS Mobility Management (GMM) protocol. The functionality of GMM is presented by describing GMM services and procedures.

## 5.1. Services and interfaces of GMM layer

GMM is a protocol, which main function is to support user's mobility. GMM is an asymmetric protocol, what means that GMM on UE side and CN side has different functionality.

The main function of GMM sublayer is to support the mobility of users' terminals. This goal is achieved by executing of elementary procedures. Term "elementary procedure" can be defined as some kind of actions that is taken in order to confirm the request from the protocol operational environment [15]. Elementary procedures and timers are the basic "building blocks" of protocol functionality.

The set of GMM elementary procedures is defined in technical specification 24.008 that was written by 3GPP organization [1]. Depending on how these procedures can be initiated they divided into two groups: GMM common procedure and GMM specific procedures.

GMM specific procedures can be initiated either by the network or UE to attach or detach the IMSI in the network and to establish GMM context. There are GPRS attach or combined GPRS attach procedures, and GPRS detach and combined GPRS detach. The GMM context is considered to be established when GPRS attach procedure was completed successfully. Another examples of GMM specific procedures are normal routing area updating, combined routing area updating and periodic RA updating. The UE initiates these procedures when a GMM context has already been established. And, finally, last type of specific procedure is Service Request that is initiated by the UE in order to establish secure connection to the network or to request resource reservation. This procedure is used, for example, when the UE replies to paging message from the UMTS network or when the UE attempts to request resource reservation.

GMM common procedures can only be initiated when peer-to-peer UMTS connection between UE and CN packet domain node is exists and GMM context is established, while

specific procedures are usually make this PS signalling connection by needs to be executed. GMM common procedures are always initiated by the network and can be started during the performing of any specific procedure. GMM common procedures are: P-TMSI re-allocation, GPRS authentication and ciphering, GPRS identification and GPRS information.

You probably noticed that all the GMM procedures are presented in two types normal and combined GPRS procedures. Normal procedures are performed only within the PS domain, when the UE is attached or will be attached for using GPRS services only. In case the UE is attached or will attach as for GPRS as for non-GPRS (GSM) services combined procedures will be used to support both circuit switched and packet switched domains. Combined procedures can only be used if the network and UE support them. In more details GMM procedures are described bellow in this chapter.

Both common and specific GMM procedures also include error handling mechanism and functions to control abnormal cases.

GMM protocol offers its services to the upper layers and uses services of the underlying layers. The logical level can also communicate with its peer entity via messages called Protocol Data Units (PDU). To make it possible interfaces of GMM with other layers is defined. Figure 5.1 clarifies the GMM interfaces on the UE part, and Figure 5.2 shows the CN part GMM interfaces.

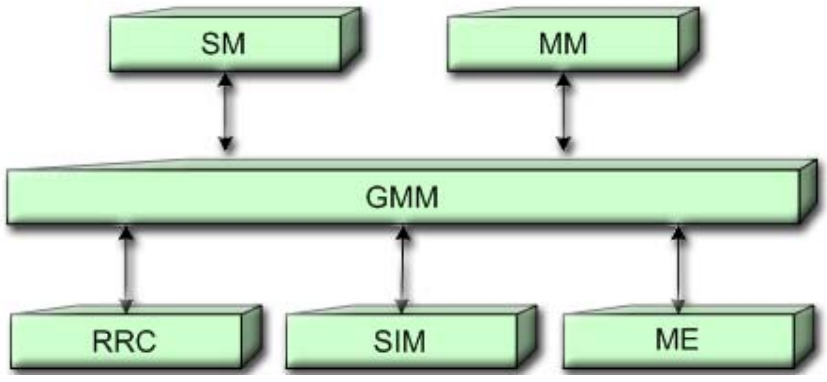



**Figure 5.1:** GMM main interfaces on the UE side

GMM protocol on the UE part has three main interfaces to other layers which are RRC, SM and MM. GMM also has two functional to UE information storage: SIM and ME.

The SIM is a detachable information storage element where all the subscriber information, security information and some other parameters are stored. ME includes information about the Mobile Equipment, such as the International Mobile Equipment Identifier (IMEI) and IMEI Software Version (IMEISV). The information from both the SIM and ME are used in execution of most of the GMM procedures. Interface with RRC layer provides transport functionality. On the UE side RRC protocol is used to transmit GMM PDU to peer entity in the Core Network Session management protocol uses GMM for transmit its PDUs. Communication with MM syblayer provides a possibility for the user to use CS and PS services simultaneously.

On the Core Network side three interfaces with other protocols (RANAP, MM, SM) and one functional interface to the network information storage (SGSN/VLR) are defined.

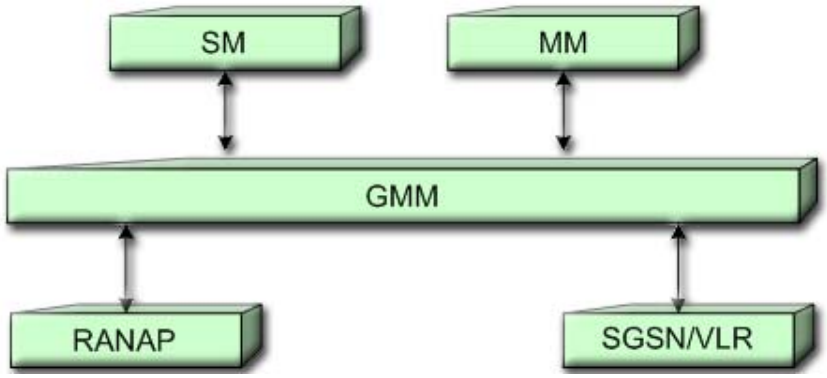



**Figure 5.2:** GMM main interfaces on CN side

The purposes of the interfaces are similar to those on the UE side. For transmitting of the GMM PDUs RANAP protocol is used in similar way as RRC on the UE. SGSN/VLR contains subscriber information, as well as location information and security parameters. These parameters are needed in most of the procedures performed by the GMM.

Before the description of GMM elementary procedures will be done in more details I first want to introduce concept of GMM state model. It will help to understand the GMM protocol behaviour and role of different procedures.

### 5.2. GMM State model

In this chapter the GMM protocol is described by means of two different state machines: state machine in the UE side of protocol, and state machine in the CN part of protocol.

### *5.2.1. GMM states in UE part*

Figure 5.3 illustrates the main states in which GMM entity in the UE operates.

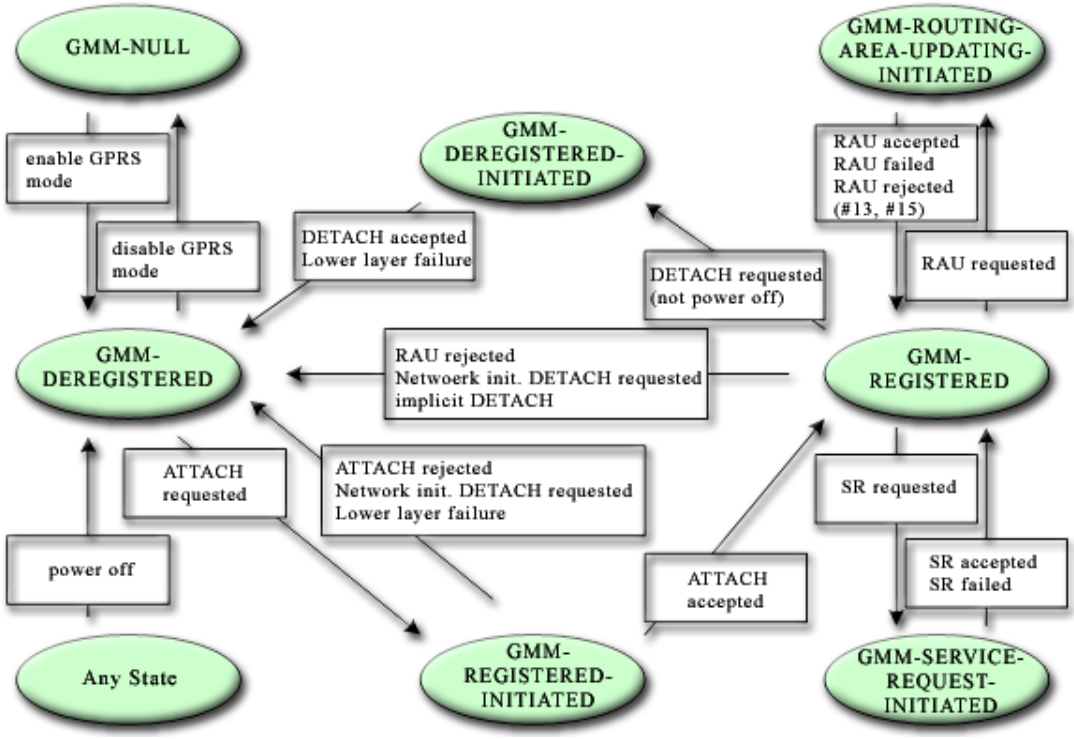



**Figure 5.3:** GMM main states in the UE [1]

When the UE is powered off or the user has not selected to use the GPRS feature UE is in the GMM-NULL state. In this state the GPRS capability is disabled and no GPRS mobility management functions may be performed.

After the user equipment is powered on, the UE is entering the GMM-DEREGISTERED state, where the GPRS capability has already been enabled, but no GMM context has yet been established. To use services of the GPRS mobility management entity GMM context must be set up by starting a GPRS attach or combined GPRS attach procedure (see Section 5.4.2).

The state GMM-DEREGISTERED is entered not only by switching on the UE. This is also happened when [1]:

- GPRS capability has been enabled in the UE after not been used;
- GPRS detach or combined GPRS detach procedure has been performed; or

- GMM procedure has failed (except routing area updating).

While performing GPRS attach or combined GPRS attach procedure the UE is in the GMM-REGISTERED-INITIATED state. In this state the mobile station is waiting for a response from the network and depending from the results enters state GMM-REGISTERED in case of success or state GMM-DEREGISTERED otherwise.

In the GMM-REGISTERED state the GPRS attach or combined GPRS attach procedure has been successfully performed and a GMM context has been established. When the UE is in this state, it may activate PDP (Packet Data Protocol) context, send and receive user data and signalling information. For sending and receiving data packets PDP context must be created. Context creation resembles opening or creating a connection. Context creation is one of the functions of SM layer so I will not include detailed explanation about this process to the Master's thesis and refer the reader to 3GPP specification TS 24.008 [1].

In this state the mobile station is able to response to paging messages and perform routing area updating.

If the routing updating procedure has been started, the UE is entered the GMM-ROUTING-AREA-UPDATING-INITIATED state. The UE is in this state while the response from the network will not be received; and it is returns to the GMM-REGISTERED in most cases after getting the answer.

When the UE receive paging message or any data from upper layer (SM layer) Service Request procedure is initiated in order to make resources reservation. By starting the Service Request GMM entity enters GMM-SERVICE-REQUEST-INITIATED state and awaiting a response from the network.

In the GMM-DEREGISTERED-INITIATED state the user equipment has started GPRS detach or combined GPRS detach procedure to requested the release of the GMM context. This state is only entered if the UE is not being switched off. Power-off detachment is always handled independently of the current state of GMM and can be performed in any state, because the user can turn off the power at any time from the GMM point of view.

In addition to the GMM states described above, the behaviour of the UE depends on a GPRS update status. The influence of update status while executing GMM elementary

procedures is explained in Section 5.4 for each procedure, but here I would like to give main description of the GMM update status and explain the differences in its values.

Update status is defined even if SIM is removed or connected to a switched off UE. The value of the GPRS update status can only be changed after execution of a GPRS ATTACH, network initiated GPRS DETACH, AUTHENTICATION PROCEDURE, or ROUTING AREA UPDATING procedure. Specification (see 1, pp. 46 - 47) defines three different values of the update status:

- GU1: UPDATED – this value is set up if the last GPRS attach or routing area updating was successful;
- GU2: NOT UPDATED – if for last GPRS attach or routing area updating no answer was received from the network, the value of the GPRS update status is NOT UPDATED;
- GU3: ROAMING NOT ALLOWED – in this case the last GPRS attach or routing area updating failed by receiving negative answer from the network.

### *5.2.2. GMM states in Core Network part*

On the network side of the GMM protocol four main states can be defined (Figure 5.4): GMM-DEREGISTERED, GMM-COMMON-PROCEDURE-INITIATED, GMM-REGISTERED and GMM-DEREGISTERED-INITIATED.

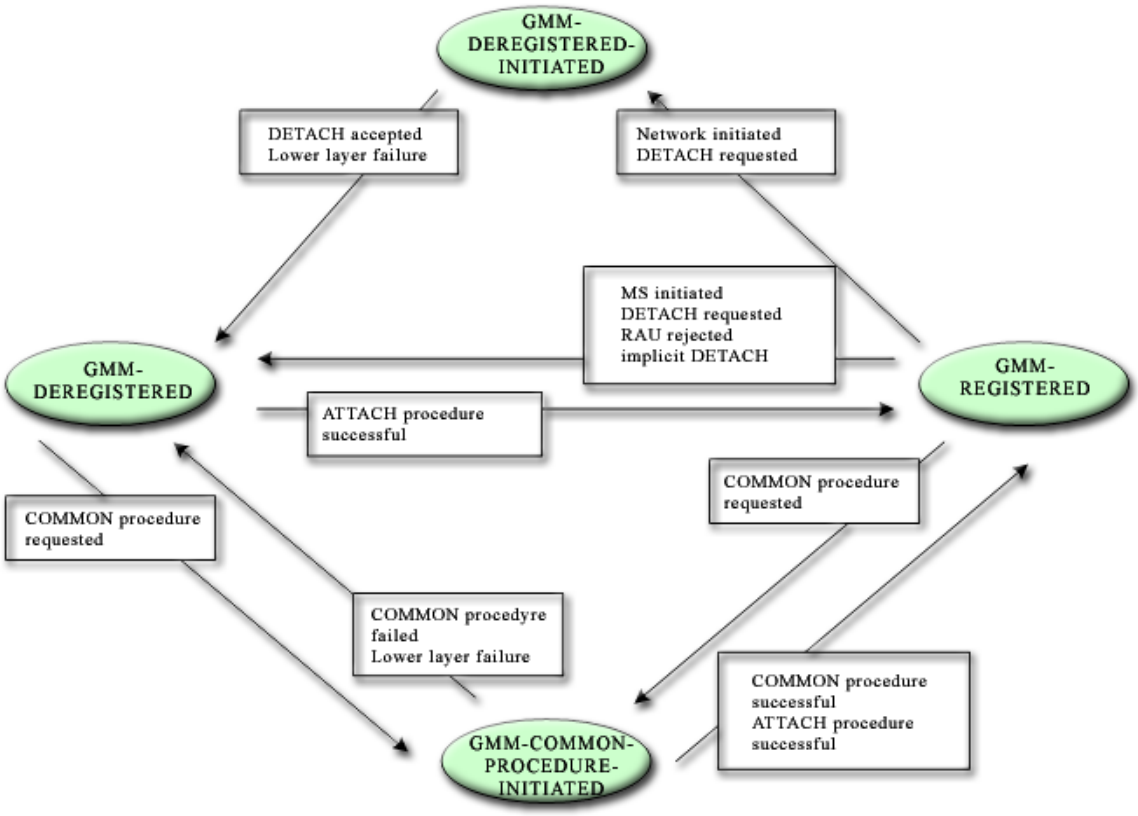



**Figure 5.4:** GMM main states on the network side [1]

These four states and transactions between them give an overview of the behaviour of the network part of the GMM protocol. Initial state of the GMM network part is GMM-DEREGISTERED. In this state the network does not know about the UE, because it is detached in this moment and registration of the mobile station in the network has not been performed yet. In GMM-DEREGISTERED state GMM context is not exist, but the network may answer to a GPRS attach or combined GPRS attach procedure initiated by the UE.

After the attach procedure has been successfully finished GMM protocol is enters to GMM-REGISTERED state. In this state GMM context has already been established and the network can reach the mobile station to send incoming call request and can receive user data.

When the network initiates common procedure execution the state GMM-COMMON-PROCEDURE-INITIATED is entered independent of state in which GMM was before. Common procedures can be initiated as in state GMM-REGISTERED as in state GMM-

DEREGISTERED during performing attach procedure. The state GMM-COMMON-PROCEDURE-INITIATED can be left when the answer from the UE has been received.

Finally, the last possible state of the network part of GMM is GMM-DEREGISTERED-INITIATED. Here the network has started a GPRS detach procedure and is awaiting the answer from the UE side.

## 5.3. GMM procedures

In the following section GMM procedures are described. Specific GMM procedures, such as attach, detach and routing area updating can be performed as normal procedures for packet switched domain as combined procedures, if the UE wants to use CS an PS services.

In UEs that can operate in both CS and PS domains the communication between GMM and MM entities should be done. But this communication is implementation-dependant and not specified in 3GPP technical specification, so it is not included in this thesis.

### *5.3.1. Attachment and detachment procedures*

Before a mobile station can send any data, it has to register to the UMTS network. Registration is accomplished by one of the main procedures of GMM – the attach procedure.

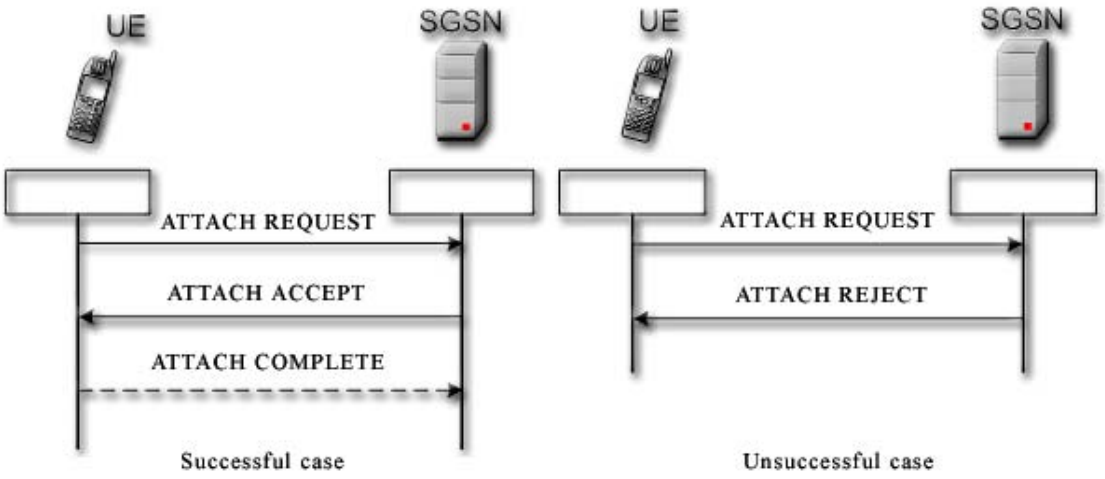
The GPRS attach procedure can be used for two purposes [1]:

- Normal GPRS attach, performed by the UE to IMSI attach to GPRS services only.

- Combined GPRS attach procedure, used by the UE to attach the IMSI to GPRS and non-GPRS services.

To make it possible to use GPRS services, the mobile station must support packet-switched operations. While performing attach the UE provides its identity and an indication of attach type (normal or combined attach) that is to be executed. The identity provided to the network is the UE's Packet TMSI (P-TMSI) or IMSI.

In the attach procedure the network checks if the user is authorised, copies the user profile from the HLR to the SGSN, and assigns a P-TMSI to the user. Optionally the equipment identity checking can also be performed. Figure 5.5 shows GMM signalling between the UE and SGSN of successful and unsuccessful cases of attach procedure at the PDU level.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.5:** GPRS attach procedure [1]

PDUs are transmitted from the UE to the SGSN and vice versa. On this figure and on the other figures bellow the solid arrows means mandatory PDUs of GMM and the dashed lines are sent only in some cases. The attach procedure is always initiated by the mobile station and started by sending of an ATTACH REQUEST PDU to the network. If the network accepts the ATTACH REQUEST, it sends an ATTACH ACCEPT message to the UE. In case if the network decided to give the UE new temporary identity (P-TMSI) and ATTACH ACCEPT message contains it, the mobile station sends an ATTACH COMPLETE PDU to the network. ATTACH REJECT message is sent by the network to the UE to indicate that the corresponding ATTACH REQUEST has been rejected, and considered as unsuccessful completion of the attachment procedure.

The network may initiate GMM common procedures, e.g. the GMM identification and GMM authentication and ciphering procedure (see Section 5.4.4), depending on the received information such as IMSI, old RAI, and P-TMSI.

It is also possible to perform a combined GPRS/IMSI attach and its execution is similar to shown above within GMM level.

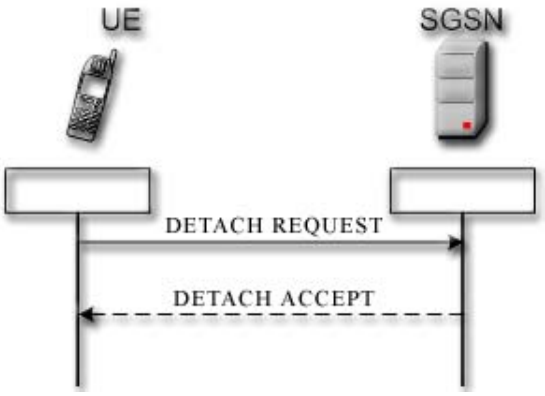
When the Attach procedure was successfully completed, the location of the mobile is known and tracked, communication between the UE and SGSN is secured, and the SGSN knows what the subscriber is allowed to do and the HLR knows which SGSN the UE uses.

After attaching the UE can send and receive GPRS SMS (Short Message Service) messages but no other data.

When the user wants to leave UMTS network or stop using GPRS services, the user has to close the connection and "log out" from the network. The connection is closed by the PDP Context Deactivation procedure of the SM layer, after which no other data than SMS can be sent or received. The user can "log out" from the UMTS network using the Detach procedure of the GMM layer, after which no packet data services are available. In a similar way to the attachment procedure, detachment can also be normal or a combined detach that is used for detachment form GPSR services only and from both GPRS and GSM services respectively.

In UMTS the detachment can be initiated either by the UE or the network (SGSN or HLR). Figures 5.6 and 5.7 show how the UE and network initiate detachment respectively.

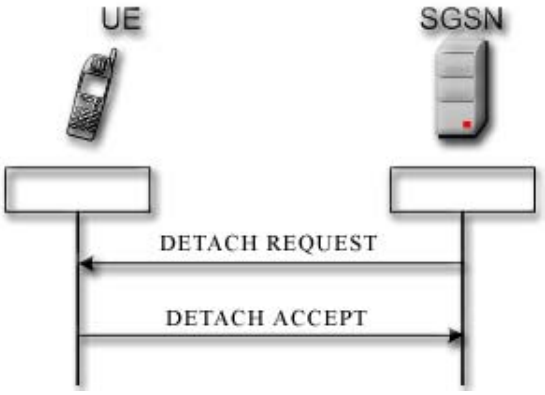
A UE initiated detach happens, for example, when the power is switched off or when the SIM is removed. The mobile station detaches by sending Detach Request PDU to the SGSN. In the Detach Request message there is an indication that point if the detach is made due to switch off or not. This indication is needed to know whether a Detach Accept message should be returned or not.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.6:** UE initiated Detach procedure [1]

The network may perform initiation of detach procedure to inform an UE that it does not have access to the SGSN-based services any more. Figure 5.7 shows PDU signalling of the GMM layer in case of detach initiated by the network.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.7:** CN initiated Detach procedure [1]

The network can also command the user equipment to re-attach immediately after the detach procedure using an information element called Detach Type, which is sent in the DETACH REQUEST.

To summaries all written above let us make some conclusions. The GPRS detach procedure is used in the following cases [1]:

- to detach the IMSI from GPRS services only;

- as a combined GPRS detach procedure used by UE to detach the IMSI for GPRS and non-GPRS services or for non-GPRS services only; or

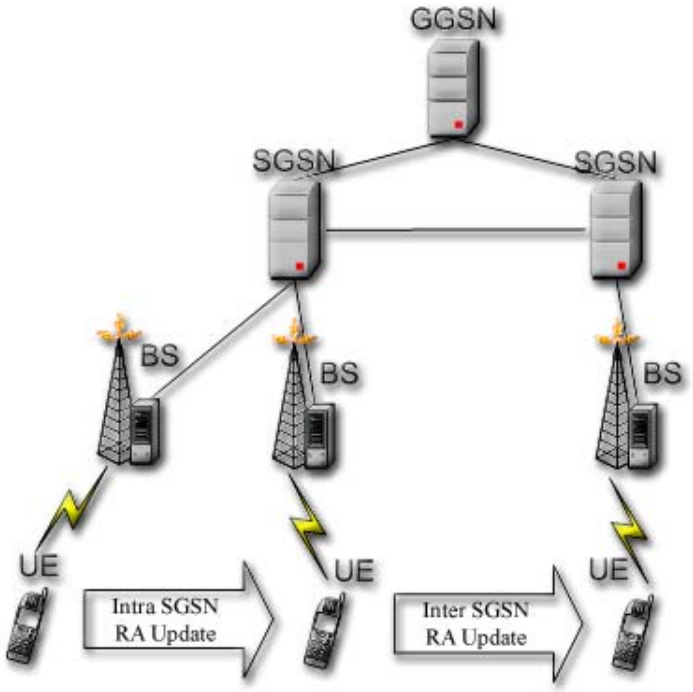
- in case of a network failure condition to indicate to the UE that a re-attach with successive activation of previously active PDP contexts shall be performed.

After completion of a GPRS detach procedure or combined GPRS detach procedure for GPRS and non-GPRS services the GMM context is released and no any data can be sent or received. The GPRS detach procedure causes the UE to be marked as inactive in the network for GPRS services, non-GPRS services or both services.

### *5.3.2. Routing area updates*

One of the main functions of the GMM layer is to inform the network of the current location of the UE. This is done using a Routing Area Updating procedure. The Routing Area Updating procedure is always initiated by the UE, and can be invoked only in state GMM-REGISTERED.

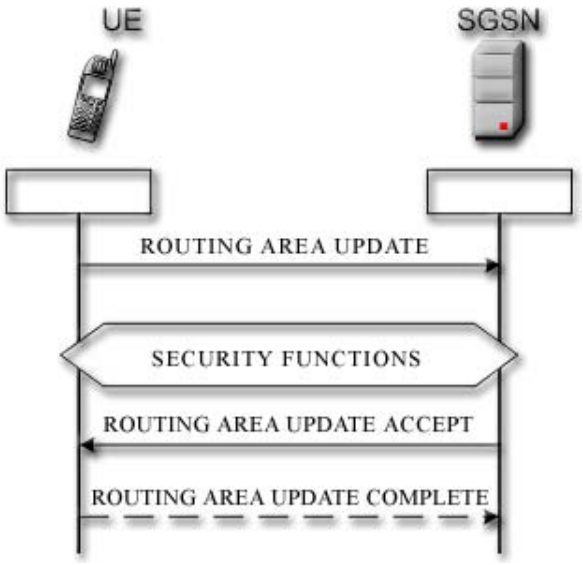
There are can be defined two different types of routing area updates: Inter-SGSN RA update and Intra-SGSN RA update. Figure 5.8 clarifies the difference between them. In Inter-SGSN updating the UE moves from the RA controlled by one SGSN to RA, controlled by another SGSN, thus SGSN area changes. In Intra-SGSN RA updating, the routing areas changes inside the same SGSN area.




**Legend:**
BS = Base Station
GGSN = Gateway GPRS Support Node
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.8:** Intra SGSN and Inter SGSN Routing Area updating

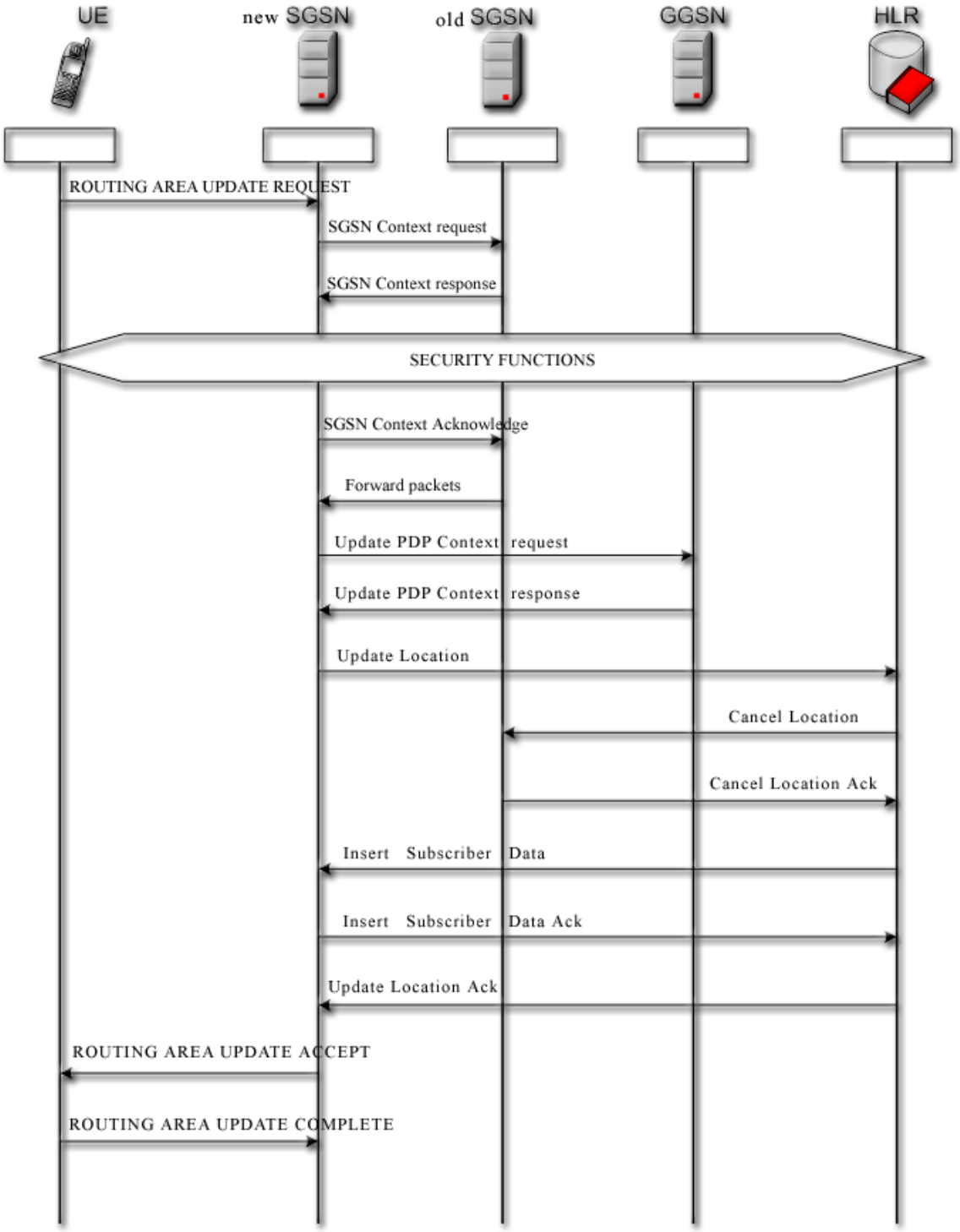
Whenever the UE moves to a new RA, it sends a ROUTEING AREA UPDATE REQUEST to its assigned SGSN. This message contains the Routeing Area Identifier (RAI) of its old routing area. If the UE has moved to an RA that is belong to the same SGSN as the old RA, the SGSN has already the necessary user profile and can assign a new P-TMSI to the user with the ROUTING AREA UPDATE ACCEPT message. In case of Intra-SGSN routing area update there is no need to inform other network elements, such as GGSN or HLR, about the UE's movements. This case is shown on Figure 5.9.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.9:** Intra SGSN Routing Area Updating [1]

When the UE moves to the RA administered by a different SGSN than the old RA, the new SGSN requests the old SGSN to send the user's profiles (see Figure 5.10). After that, the new SGSN informs the HLR and, if needed, the MSC/VLR about the user's new SGSN. Example on Figure 5.10 also shows the usage of other mobility protocols involved in performing of RA updating. The messages between new SGSN and old SGSN as well as between SGSN and GGSN are GTP-C protocol messages. To SGSN communication with HLR MAP protocol is used.




**Legend:**
GGSN = Gateway GPRS Support Node
HLR = Home Location Register
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.10:** Inter SGSN Routing Area Updating [5]

In the GMM level three types of Routing Area Updating procedure are specified [1]:

- Normal routing area updating procedure;
- Combined routing area updating procedure;
- Periodic routing area updating procedure.

Normal and combined RA update is performed when the UE detects that the routing area has been changed. The difference between them is that while performing RA updating, the location area update for CS domain is also performed. In this case the PDUs ROUTING AREA UPDATE ACCEPT and ROUTING AREA UPDATE COMPLETE carry information as for the routing area updating as for the location area updating.

Periodic routing area updating is used to periodically report the "presence" of the UE to the network. This allows the network to detect if an UE is still attached to the network or not. A periodic RA update timer is maintained in both the UE and the SGSN. Every time this timer expires, the UE performs periodic RA update. The periodic RA update timer value is set/changed by the SGSN, and is sent to the UE through the ROUTING AREA UPDATE ACCEPT or the ATTACH ACCEPT messages when the UE visits an RA, and this value cannot be changed before the UE leaves the routing area.

Signalling exchange for all these types of RA updating is similar and the difference only in information elements carried inside the PDUs. The value of the information element named *Update Type* specifies if normal update, combined RA/LA updating or periodic update is to be performed.

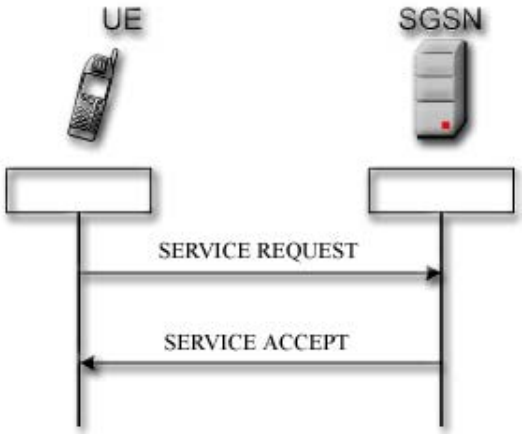
### *5.3.3. Service request procedure*

Service request procedure is used by the UE in case the establishment of a secure connection between SGSN and the UE is needed, so that the UE can send uplink signalling messages or user data. This procedure is used in the following cases [1]:

- In the UE side there is the initiation of CM layer service (e.g. SM or SMS) procedure, thus there is a message need to be sent to the network and UE has not connection to it;

- The network want to transfer downlink signalling or user data, and paging procedure is used to notify about this.

Information element (IE) named *service type* is used to indicate the reason for the initiation of Service Request procedure. This IE can take either of the following values: "signalling", "data" or "paging response". It transferred in SERVICE REQUEST message (see Figure 5.11).




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.11:** Successful case of SERVICE REQUEST procedure [1]

Let us see the PDUs exchange while performing Service Request procedure. In order to establish secure peer-to-peer connection (PS signalling connection) between UE and core network (CN), the UE sends the SERVICE REQUEST message to the SGSN. If connection with RRC layer is not exists, it has to be established to make it possible to send SERVICE REQUEST PDU.

After receiving the SERVICE REQUEST, the SGSN may perform authentication, and it shall perform the ciphering procedure. After the establishment of the secure PS signalling connection to the SGSN, the network response with SERVICE ACCEPT message and the UE may send signalling message or used data, or the SGSN may start the resource reservation for the active PDP contexts.

SERVICE REJECT message is sent by the network to the UE in order to reject Service request procedure.

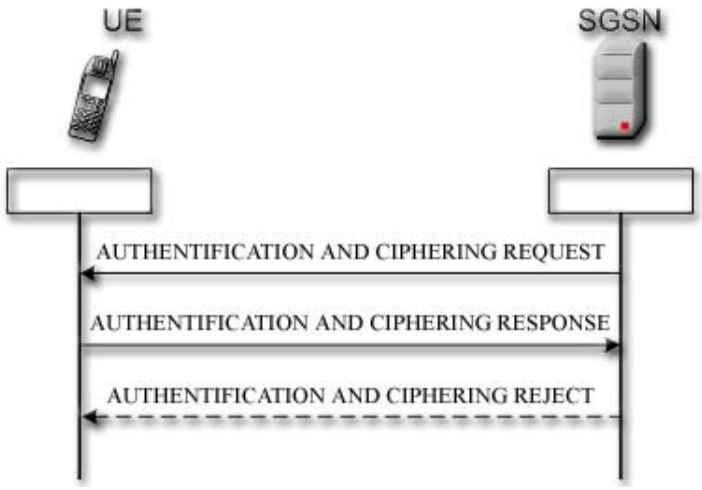
### *5.3.4. Security procedures*

GMM is also responsible for handling such issues as authentication and ciphering, identification of the subscriber and mobile equipment, and P-TMSI reallocation. All these procedures are named as common elementary procedures. They are always initiated by the network.

Main purposes of the authentication and ciphering procedure are [1]:

- to check if identity provided by UE can be accepted or not;
- to provide UE with parameters which needed for calculating new GPRS UMTS ciphering key and a new GPRS UMTS integrity key;
- to let network set algorithm and ciphering mode; and
- to permit the user equipment to authenticate the network.

Authentication and ciphering procedure is always initiated and controlled by the network, but there is a possibility for the UE to reject the network. Figure 5.12 illustrates PDUs exchange for this procedure execution.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.12:** Authentication and ciphering procedure [1]

The network initiates Authentication and Ciphering procedure by transferring the AUTHENTICATION AND CIPHERING REQUEST PDU across the radio interface. This message contains all parameters needed to calculate response parameter when authentication is performed. These parameters are: authentication parameter RAND () and authentication parameter AUTN (). RAND and AUTN are transferred into the USIM, which contains the special master key K. Parameter RAND is a non-predictable number and the AUTN is authentication token. Using permanent key K with parameters RAND and AUTN as inputs, USIM can verify validity of parameter AUTN to check if it was generated in AuC or some false network trying to attack the mobile station. In a positive case calculated authentication response parameter RES is sent back to the network in the AUTHENTICATION AND CIPHERING RESPONSE message.

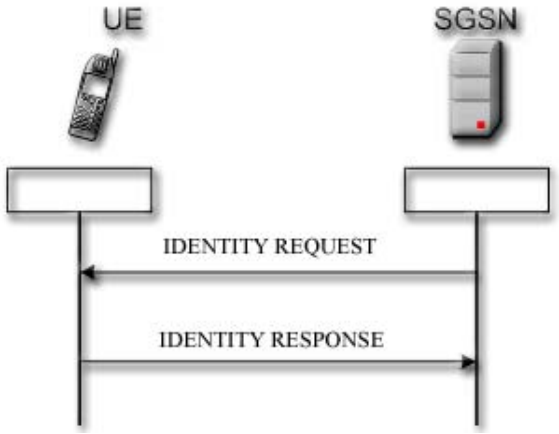
AUTHENTICATION AND CIPHERING FAILURE PDU may be sent by the UE to indicate that the authentication of the network has failed.

After receiving parameter RES the network is able to check validity of the UE. In positive case the procedure ends successfully, otherwise the network answers with AUTHENTICATION AND CIPHERING REJECT PDU. Upon receiving this PDU, the UE sets the GMM Status to " ROAMING NOT ALLOWED " and changes the state to GMM-DEREGISTERED.

Authentication and Ciphering procedure is also responsible for providing secure connection between the UE and the network. Ciphering is one of the security functions defined to protect subscriber identity and data. When ciphering is active, all information exchanged between the UE and the network on the dedicated radio channels is encrypted. The key previously set between the network and the UE is used to encipher and to decipher the encrypted information. In UMTS for this purpose UMTS ciphering key and UMTS integrity keys are calculated using GPRS ciphering key sequence number, which is transmitted inside the AUTHENTICATION AND CIPHERING REQUEST PDU.

This thesis mostly considers the mobility management issues, thus such security aspects as process of calculation of different security parameters is out of scope of this Master's thesis. If you are interested in such details you can find some useful information in [4].

Another security procedure provided by GMM is identification. It is used to provide network with specific identification parameters such as IMSI, IMEI, and IMEISV (International Mobile Equipment Identity SW version). Figure 5.13 contains a sequence diagram for an Identification procedure.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.13:** Identification procedure [1]

This procedure consists of only two steps:

Step 1: The network initiates the identification procedure by transferring an IDENTITY REQUEST message to the UE, where the requested identification parameters are specified.

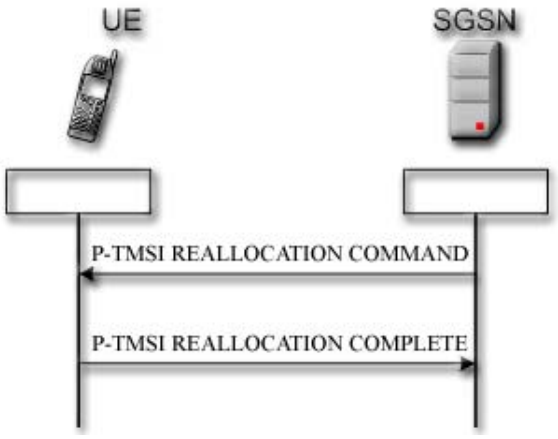
Step 2: Mobile station sends back an IDENTITY RESPONSE PDU, which contain the requested identity.

This procedure is invoked whenever the user cannot be identified by means of a temporary identity. For example, it should be used when the user registers in a serving network for the first time, or when the network cannot retrieve the IMSI from the P-TMSI by which the user identifies itself on the radio path.

Finally, GMM is responsible for identity confidentiality. This is done by using of temporary identity for GPRS services, the Packet-TMSI (P-TMSI). This temporary identity is set with help of P-TMSI reallocation procedure. Thus the purpose of the P-

TMSI reallocation procedure is to provide identity confidentiality, i.e. to protect a user against being identified and located by an intruder.

The SGSN may initiate P-TMSI re-allocation procedure at any time when the UE is in the GMM-REGISTERED state. P-TMSI can also be implicitly reallocated in the attach or routing area updating procedures. The P-TMSI re-allocation procedure is usually performed at least at each change of routing area, because the P-TMSI is valid only inside the one RA.




**Legend:**
SGSN = Serving GPRS Support Node
UE = User Equipment

**Figure 5.14:** P-TMSI re-allocation procedure [1]

The P-TMSI REALLOCATION COMMAND (see Figure 5.14) message contains a new combination of P-TMSI, RAI and optionally P-TMSI Signature. The network does not send any user data during the PTMSI reallocation procedure.

Upon getting this PDU the mobile station stores received P-TMSI, RAI and P-TMSI signature for future usage and responses with P-TMSI REALLOCATION COMPLETE message. After this new temporary identity shall be used instead of permanent IMSI.

### *5.3.5. GMM Information and GMM Status*

GMM Information procedure support is optional. The network may invoke this procedure at any time when the GMM context is established. There is only one message for this procedure – GMM INFORMATION that is sent from the network to the UE.

When the UE, which supports the GMM Information procedure, receives the GMM INFORMATION message, it accepts the message and optionally may use the contents to update the appropriate information stored within the mobile station (e.g. time zone, name for network). If the UE does not support this procedure, it should ignore the contents of the message and return a GMM STATUS message with cause " Message type non-existent or not implemented".

GMM STATUS message can be sent either by the UE or by the network to report about error condition. If the UE receives a GMM STATUS message no state transition and no specific action shall be taken, but local actions are possible. The actions to be taken on receiving a GMM STATUS message in the CN side are an implementation dependent option.

### 5.4. GMM timers

In GMM protocol to work more effectively, several important timers are specified. Main timers are:

- Periodic RA Update Timer;
- Mobile Reachable Timer.

The Periodic RA Update Timer monitors execution of Periodic Routing Area update procedure in the UE. The value of the timer is set in each visit of new routing area and messages ROUTING AREA UPDATE ACCEPT and ATTACH ACCEPT are used for this purpose. Thus the periodic RA update timer is unique within an RA. Each time the timer expires, the UE starts a periodic ROUTING AREA UPDATE procedure.

If when the periodic RA update timer expires the UE is out of packet domain coverage, but within the CS domain and it is CS-attached to a network, then the Periodic Location Update procedure is started immediately. In addition, the periodic RA update procedure is started once the UE returns to packet domain coverage.

The network supervises the periodic ROUTING AREA UPDATE procedure by means of the Mobile Reachable timer. The mobile reachable timer should be longer than the periodic RA update timer. The Mobile Reachable timer is reset and started when the UE has released PS signalling connection between the UE and the network and stopped when

the connection to network is established. When the Mobile Reachable timer expires, typically the network stops sending paging messages to the mobile and may take other appropriate actions.

In UE and CN side some other timers are specified. All these timers are listed in the Appendix I. Such timers are used to control the execution of GMM procedures (except the GMM Information and GMM Status). In the UE side a timer is started when the mobile is waiting for a response from the core network. In similar way, on network part the timers are started after sending message to the UE in order to monitor the time of response.

# 6. IMPLEMENTATION OF GMM

## 6.1. Project overview

Rapid growth in usage of mobile networks has made a number of difficulties when writing specifications and creation of mobile telecommunications software.

The work on UMTS standardisation was finished in year 2000, but changes are still made. The large size and real-time nature of mobile communication systems originate some problems, which are not possible to solve without early implementation. UMTS system is only start to become a part of real life and mostly it is still on paper only, so nobody can guarantee that there are no bugs.

This thesis was done as a part of 3G SDL library project, which goal is to implement executable prototype versions of UMTS protocols to see if everything writing in specifications really works. It was found out that the implementation results could be also used for more concrete purposes, like testers and trial systems for supporting standardisation process. A secondary objective for the project was to develop protocol implementation methodologies using SDL and ASN.1. [9]

In practical part of the thesis I would like to describe implementation of GMM protocol that was done by me as a part of 3G SDL library project.

The following subsections describe protocol development stages and issues, point on which parts were more difficult while implementing the GMM, make an overview of tools used in implementation process and testing. The last subsection summarises an experience obtained by the author from the project and gives some reflections for future work.

## 6.2. Software development issues

Over the years, various models of software development process have emerged to support the development of high-quality software products. The primary function of process model is to determine the order of software development stages to help to understand what to do next. In my opinion the most suitable model for GMM system implementation is spiral model. This type of development process has iterative nature and divided into some basic activities. It was needed to get working version with limited functionality in a

short time, so most important procedures, such as attachment, detachment and routing area updating, needed to be implemented first. Then new procedures were added gradually. Every time new feature is added all the development phases is repeated. Thus spiral model is the best choice in this case. Figure 6.1 shows development process model for GMM system.

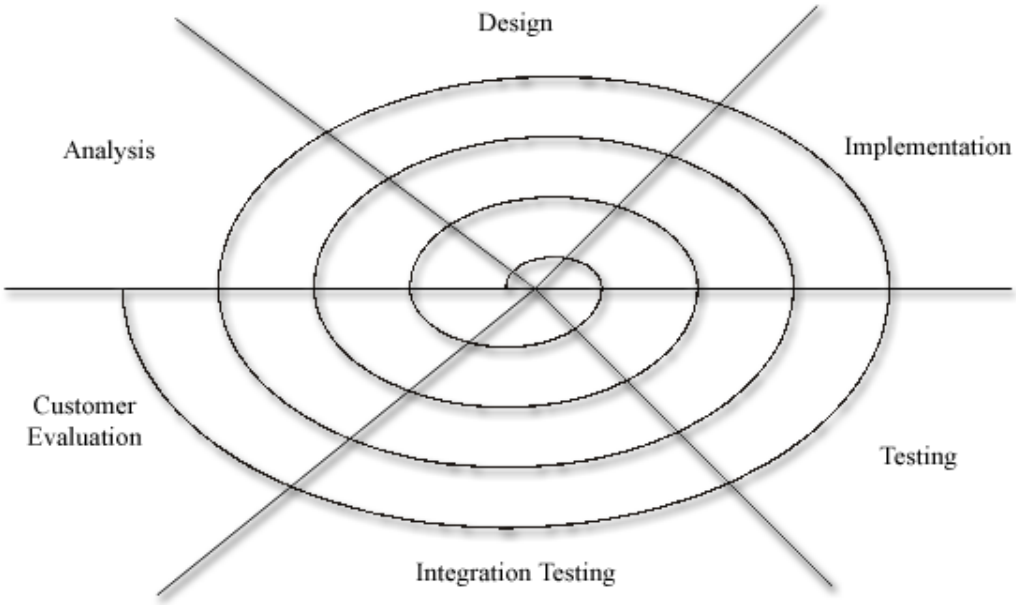



**Figure 6.1:** Development process model

Each cycle is started from analysis phase. In my point of view it is one of the hardest parts of development. This phase includes analysis of system requirements. In the project requirements developed by 3GPP organization are used. The specific feature of this documents that is each protocol described in stand-alone manner, detailed description of each procedure is given, but it is very difficult to understand how the protocol is communicate with another layers. At the analysis stage the behaviour of the protocol should be understood and the interfaces of the protocol to its operational environment should be identified, after this the design phase can be started.

At the design phase the behaviour of the system is fully specified. In protocols most of actions are triggered by external events, so the definition of signals, that is needed to specify the interfaces are very important. When designing the system it should be taken into account that the system specifications periodically change and one of the project purposes is to have implemented latest version of the protocol. Thus system has to

support easy updating. What more it should be possible to reuse designed system, so the modularity principles should be supported.

To meet these requirements the formal description methods are used. It is widely used technique in telecommunication area and especially in protocol design. In 3G SDL Library project Specification and Description Language (SDL) and Abstract Syntax Notation One (ASN.1) are used. Using SDL behaviour of protocol is specified. The Abstract Syntax Notation One (ASN.1) language is used for definition of protocol data types, which is also defined at the design stage. Protocols are implemented in SDL by using development environment of Telelogic SDL Design Tool (SDT). More detailed description of tools, languages and techniques used in GMM protocol development are specified in the next subsection.

After the clear high-level structure and interface definitions have been done, the representation of the actual system functionality can be started. The functional behaviour is used to mean SDL processes. Processes describe how the signals and the data are handled.

After the design phase has been finished, the SDL processes and data are described in a very detailed level, and this is time for implementation stage. In SDT environment it is possible to generate executable application from designed SDL system.

Finally, the SDL description is simulated using Simulator at SDT tool. The role of the simulations is to ensure that the system works as specified and uses data correctly.

Once the protocol is thoroughly tested, it is integrated to the 3G SDL library and integration testing of whole system is performed. The integration means that all the protocols are connected together and form the UMTS protocol stack. Integration testing helps to find any shortages in the interface definitions and protocol design. Once integration testing has been completed the protocol or whole library is delivered to the customers for evaluation. 3G SDL library models are used by other projects, so the customers' feedback is very valuable, because allows the developers to better meet customer's requirements.

## 6.3. SDL implementation of GMM protocol

This section was written to give a brief overview of the techniques and tools used in the project. It also provides a detailed description of practical part of the thesis.

### *6.3.1. Tools and languages used*

In last years, a number of formal description techniques and tools have been developed to replace the natural language specification techniques. The main benefits of using the formal description techniques are increased reliability of the system and decreased design time. This is the reason why the usage of formal techniques has been increased in the telecommunication area

**SDL**

Nowadays, there are many different techniques to be chosen for different design purposes. Specification and Description Language (SDL) is a method for specification and description of telecommunications systems. SDL was standardised by ITU-T (International Telecommunication Union, Telecommunication Sector) organization and is specified in ITU-T Recommendation Z.100 [8].

With SDL, we may specify many different levels of abstraction, from overview to very specific details. There are four main hierarchical levels: system, block, process and procedure (see Figure 6.2).

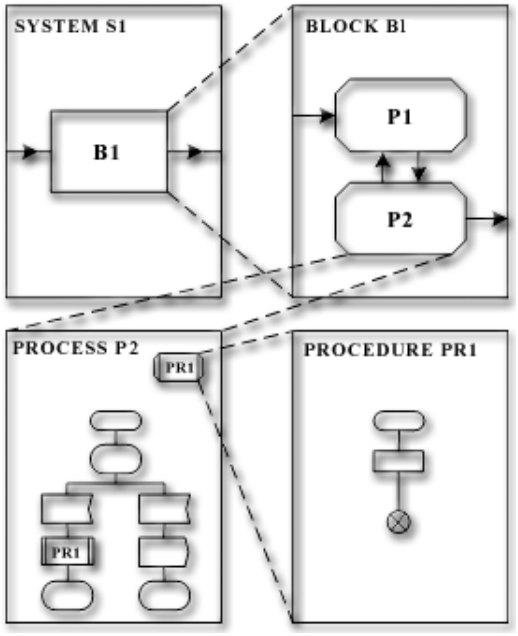



**Figure 6.2:** Hierarchical structure in SDL [17]

System and block levels give the static description of the system, and process and procedure refer to dynamic behaviour. System is a top layer, and everything that is not included in the system is considered to be a part of the environment. System is decomposed into blocks, which in turn consists of one or several processes. The SDL process is defined in terms of Extended Finite State Machine, that is the set of states and transactions between them. The SDL process has finite number of states. Process may be created at the start time or dynamically by response to some event. The communication between processes or process and environment is done by signals exchange.

**Telelogic SDL Design Tool (SDT)**

Since the SDL became very popular in telecommunication industry, the variety of tools supporting this language was developed. One of such tools is Telelogic SDL Design Tool (SDT). SDT is an integrated software environment for the development of real-time systems using SDL. SDT contains build-in components for analysis, code generation, simulation and validation of SDL models. Let me in a few words describe those ones that were used in GMM system development.

SDL Editor is a design tool, which is used to create and edit SDL diagrams. This is the tool I used to build the whole GMM system.

MSC Editor is a tool for creating and editing of Message Sequence Charts. MSCs help to understand the behaviour of the system, and represented as a number of signals sent in defined order. It can be used at the specification phase for when requirements for the system are created, and during the testing phase for tracing and controlling the simulation process.

SDL Analyzer carries out syntax and semantic analysis, and it is always started before code generation can be performed. Code generator produces C-code from the given SDL models. The process of code generation is presented on the Figure 6.3.

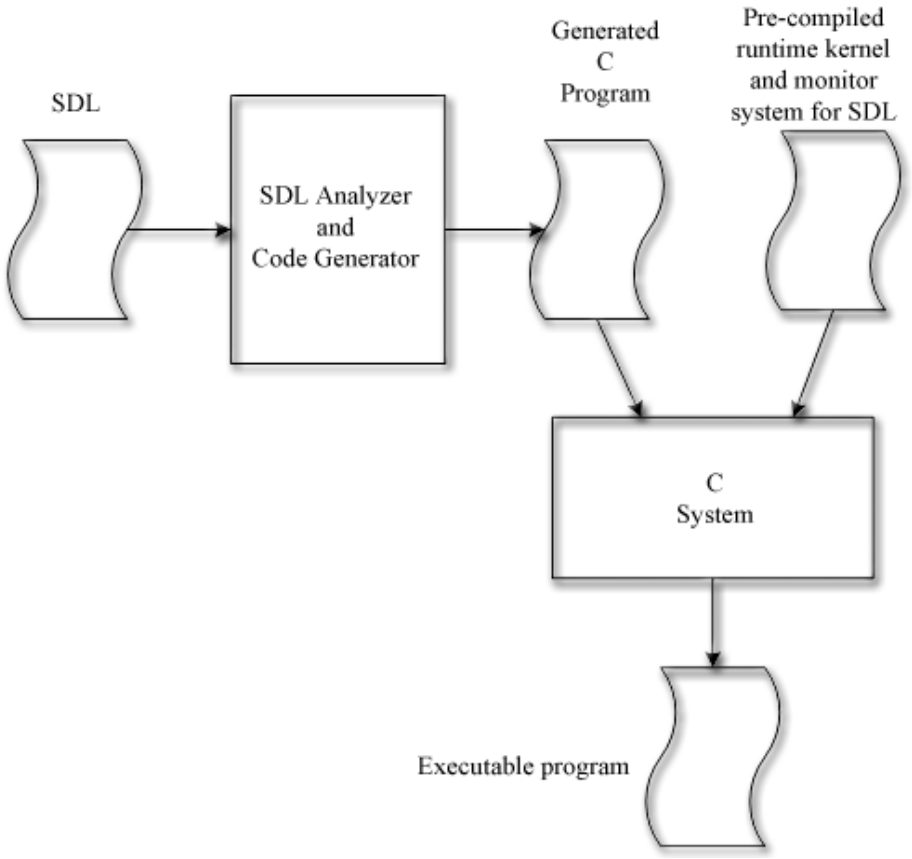



**Figure 6.3:** Code generation [17]

For executing the generated program Simulator is used. In GMM protocol development the main function of simulator was to help in debugging process.

The newest version of the Telelogic SDT is version 4.4, but in this thesis work SDT 3.5 was used.

**Abstract Syntax Notation One (ASN.1)**

There is one problem in SDL that must to be solved for success of 3G SDL library project. SDL language does not include the concept of PDU. This problem can be solved by defining all the data types and values in ASN.1 (Abstract Syntax Notation One) language. ASN.1 is an international standard, which aim is to specify data used in communication protocols. ASN.1 is standardised in ITU-T recommendation X.680.

ASN.1 describes the *abstract syntax* of data, i.e. such way when the data are equal for all systems, and the methods how the information is represented in transmission media (*transfer syntax*). The encoding and decoding rules define how the abstract syntax is converted to transfer syntax. There are ASN.1 encoding and decoding rules, but for GMM system was decided to use own once. The process of implementation of the encoding and decoding functions is described in Section 6.4 of the thesis. Bellow the example of usage ASN.1 language is shown:

```
RoutingAreaUpdateRequest ::= SEQUENCE {
  updateType                    UpdateType,
  cipheringKeySequenceNumber    CipheringKeySequenceNumber,
  oldRAI                        RoutingAreaIdentification,
  radioAccessCapability         RadioAccessCapability,
  oldPTMSIsignature     [25]    PTMSIsignature          OPTIONAL,
  readyTimer            [23]    GPRStimer               OPTIONAL,
  drxParameter          [39]    DRXParameter            OPTIONAL,
  tmsiStatus            [9]     TMSIstatus              OPTIONAL,
  pTMSI                 [24]    MobileIdentity          OPTIONAL,
  msNetworkCapability   [49]    MSNetworkCapability     OPTIONAL,
  pdpContextStatus      [50]    PDPcontextStatus        OPTIONAL
}
```

The example gives a definition of ROUTING AREA UPDATE ACCEPT PDU. Most of PDUs are usually defined as a sequence of components. There are two kinds of terms here: names and types. The PDU is really only defined as a structure built out of types, and the names are given only for better usage and understanding. In this example we have message type named *RoutingAreaUpdateRequest.* This type of message has eleven components, seven of which are optional in the message. All the optional elements have a number placed between the square brackets, this is the tag, and it is used in decoding

process as will be shown in Section 6.4.3. All the other types, such as MobileIdentity are defined in similar way. When making a definition built-in types (for example INTEGER) or another defined type can be used.

Nokia Research Center has developed a family of internal software for ASN.1 support. These tools were widely used in the project and will be briefly described below.

**CASN**

CASN is used to validate ASN.1 definitions for a back-end. It checks if there are any errors in definition of data types and if not then produce binary syntax tree file (*.stx). Back-ends for different environments use binary syntax tree as an input (see Figure 6.4).

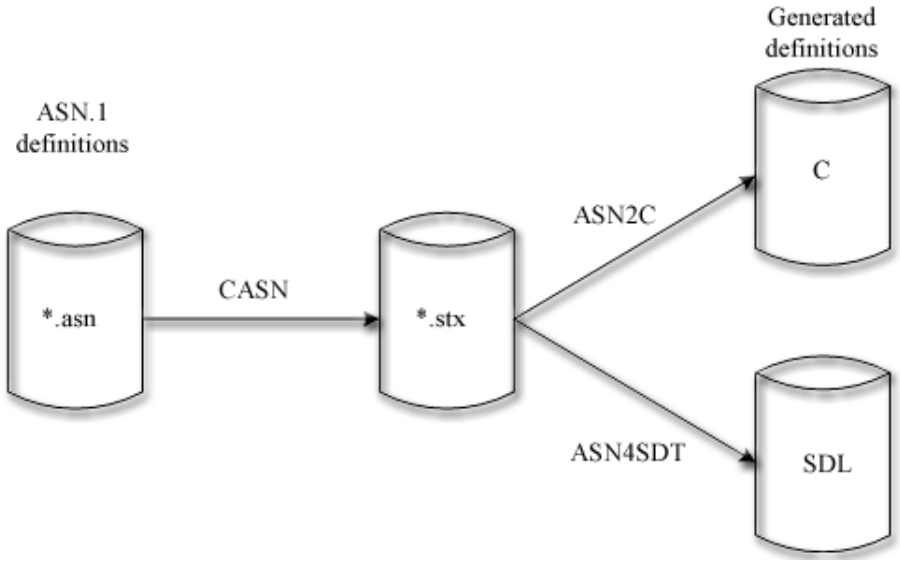



**Figure 6.4:** CASN tool usage [7]

**ASN2C**

ASN2C is one of the back-ends for the CASN Compiler. It generates C definitions from ASN.1 definitions. As the input this tool accepts the syntax tree file from CASN and as an output it produces a number of C files and header files:

- *.typ – header files that contains C type definitions;
- *.def – header files, which contains C constants and macros;
- *tst.ext – header file that contains of test function prototypes;

- *tst.c – C file contained test functions.

**ASN4SDT**

ASN4SDT is also a back-end tool for CASN Compiler. It was developed for integrating of ASN.1 data types with SDT. ASN4SDT generates from ASN.1 specifications SDT type definitions and C-language functions that are needed for integration.

All of the tools mentioned here were used in the project. The last sections of the thesis explain the design process of GMM protocol.

### *6.3.2. Structure of GMM system*

The GMM protocol implementation is made according to 3GPP Technical Specification 24.008 [1]. The implementation includes all the functionality that is described in specification, but some features, such as timers handling and error cases, are out of this implementation and should be added latterly.

GMM is asymmetric protocol, what means that GMM on UE side and CN side has different functionality and requires different implementation. The protocol implementations are defined in packages as block types, so it is possible to reuse the same code by instantiating the block types in different locations. Thus the block type has the same meaning as class in object-oriented programming [14]. GMM implementation has two block types: GMM_UE and GMM_CN, they are incorporated in a separate packages, what makes possible to use instances of these block types in other SDL models by simply including the package to a desired system.

The implementation is started from the highest level of the system and gradually to be expanded to the lower level blocks. The SDL System GMM_Bench was created for testing of GMM protocol implementation. It consists of two blocks: GMM_UE and GMM_CN, which are instances of the corresponding block types.

The services that the protocol offers to higher level protocol are defined in external interfaces of a protocol. As can be seen from the Figure 6.5 the system has several external interfaces:

- Interfaces to the transport layer protocols RRC (Radio Resource Control protocol) and RANAP (Radio Access Network Application Part protocol), which

are used by GMM for transportation of GMM PDUs between entities on the UE and CN parts;

- Interface to the Session Management (SM) protocol, that is uses GMM for transport purposes;

- Interface with SIM card to be able to get the UE identities, change update status and calculate security parameters;

- The GMM_CN entity has interface with SGSN register, that is needed to get needed identities on the CN side, and to control procedures execution;

- There is also interface with environment for testing purposes.

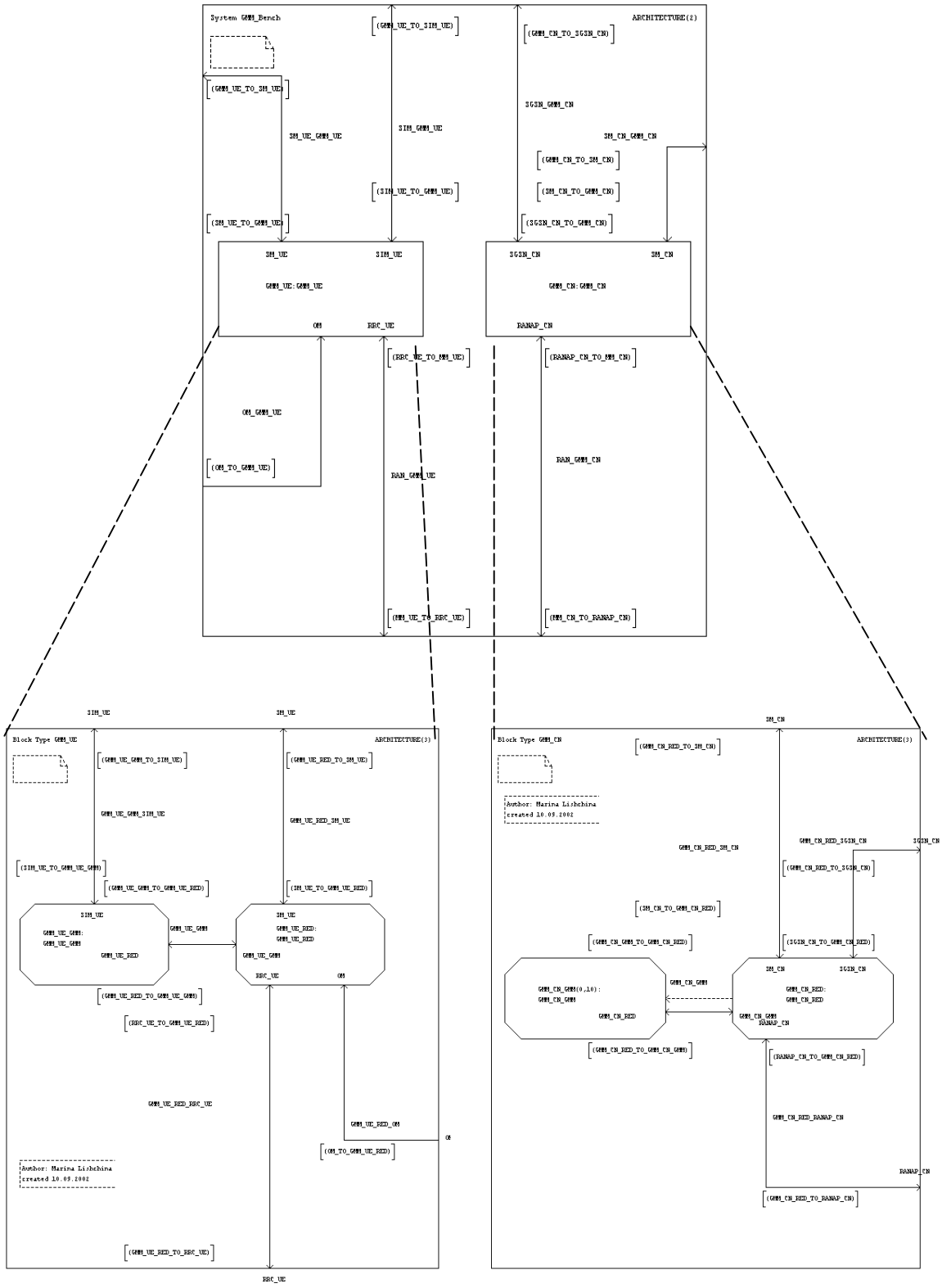



**Figure 6.5:** System GMM_Bench, Blocks GMM_UE and GMM_CN

Figure 6.5 also shows further decomposition of GMM_UE and GMM_CN blocks. Because many things are done in parallel, the functionality of GMM is divided into

processes. GMM_UE block consists of two SDL processes that are implemented as entities of process types. GMM_CN also consists of two processes. Processes are communicated with each other sending and receiving signals that creates internal interface.

GMM external and internal interfaces are stored in a separate package for increasing modularity and reusability. As you can see from the Figure 6.5 each interface is defined by name of *Signal List* written in square brackets (for example [GMM_UE_TO_SIM_UE]). Signal List contains a set of signals that can be sent or received trough the interface.

### *6.3.3. Process level implementation*

Processes in the SDL model define the functionality of the protocol. GMM_UE block consists of two processes: GMM_UE_GMM and GMM_UE_RED, and GMM_CN block is constructed from GMM_CN_GMM and GMM_CN_RED processes (see Figure 6.5).

The process architecture of GMM protocol is based on the so-called Routing/ Encoding/Decoding (RED) architecture. The idea is to separate behaviour functionality of the protocol from the interface related functions, such as routing, encoding and decoding. [9]

GMM_UE_RED handles routing and data conversions between internal and external presentations (encoding and decoding) on the UE side, and GMM_CN_RED represents the same functionality on the CN part of the protocol. In addition GMM_CN_RED is responsible for creation of GMM_CN_GMM process. GMM_CN_GMM is only the process that is created dynamically, all the other SDL processes in the system are created at system initialisation. On the Figure 6.5 the creation of the process is shown as dashed arrow.

GMM_UE_GMM and GMM_CN_GMM processes perform the main functionality of the protocol. All the external signals coming to GMM_UE block are first processed by the GMM_UE_RED and routed to the GMM_UE_GMM or to the upper SM layer. Because the GMM_UE_GMM process is only one and it is not possible to delete it or create new one, there is easy to route signals to this process. The opposite situation is on the CN part.

Signals coming from outside the GMM_CN block are first coming to GMM_CN_RED process and then should be routed to the corresponding process. As was written above, the GMM_CN_GMM is created dynamically, and there is a possibility to create more than one process, for this implementation up to ten processes can be created. To distinguish one process from another each process in SDL has Process Identifier (PID) assigned to it at the process creation. Routing table that is based on association of the PID with different protocol parameters has been defined. It is maintained by the GMM_CN_RED with help of special procedures for adding, removing, searching and editing of entities in the routing table. These procedures are grouped into separate package.

To clarify the principles of RED architecture and to show how it is done in GMM protocol implementation I would like to give some examples from SDL code of performing routing, encoding and decoding.

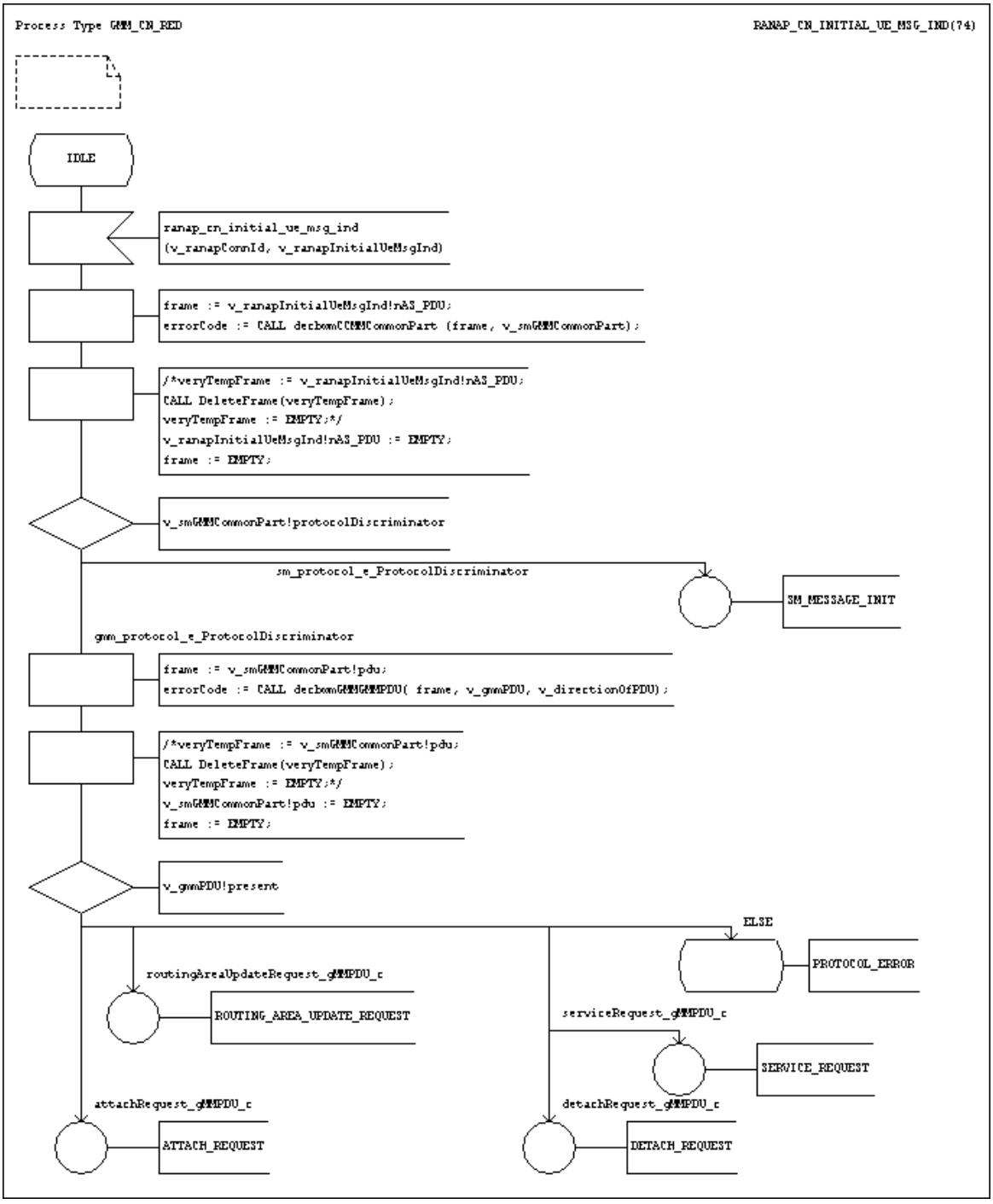



**Figure 6.6:** Example of decoding in GMM implementation

Let us see an example on Figure 6.6. It demonstrates the behaviour of GMM_CN_RED process on arrival of ranap_cn_initial_ue_msg_ind primitive. This message is sent from the transport layer in case the GMM peer entity wants to initiate procedure execution and sends request PDU. The PDUs are transported across the network, as encoded fields of transport layers PDUs, so upon arriving PDU must be decoded. This is done by calling

function decbwmCCMMCommonPart. This function was written using C language and SDL definition was made to be possible to use it inside the SDL model. In more details the process of encoding and decoding as well as description of encoding and decoding functions is given in the next section. When the data has been successfully decoded GMM_CN_RED checks to which protocol this PDU was send. This check is needed because the GMM layer is used as transport by Session Management protocol, and SM layer PDUs can be received by the GMM_CN_RED. The same reason makes decoding process contains two phases. GMM layer does not know how to decode SM layer PDUs and this is not needed, but before we know exactly which protocol PDU we have received it is not possible to decode it completely. Thus after call of decoding function decbwmCCMMCommonPart we will be able to see protocol identification. If GMM PDU has been received, decoding of it is made by decbwmGMMGMMPDU function. After decoding it is known which PDU was received.

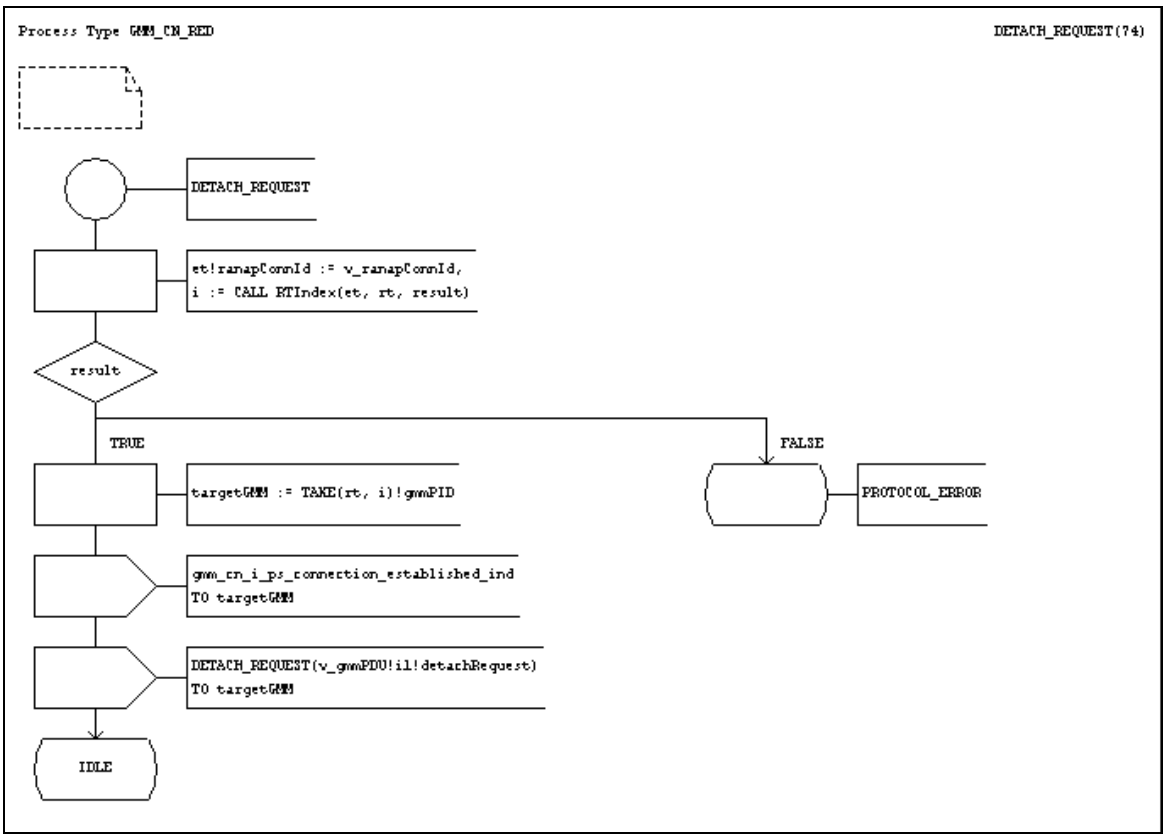



**Figure 6.7:** Example of routing in GMM implementation

Let us assume that it is DETACH REQUEST. The PDU should be forwarded to the corresponding process as shown on Figure 6.7. For that purpose the PID of

GMM_CN_GMM process (targetGMM) should be defined from the routing table. It is done based on RANAP Connection ID, which is associated with targetGMM in the routing table. After targetGMM has been found DETACH REQUEST PDU is sent to the corresponding GMM_CN_GMM process.

Third example demonstrates encoding process, when the AUTHENTICATION RESPONSE arrives to GMM_UE_RED. This case is shown on Figure 6.8.

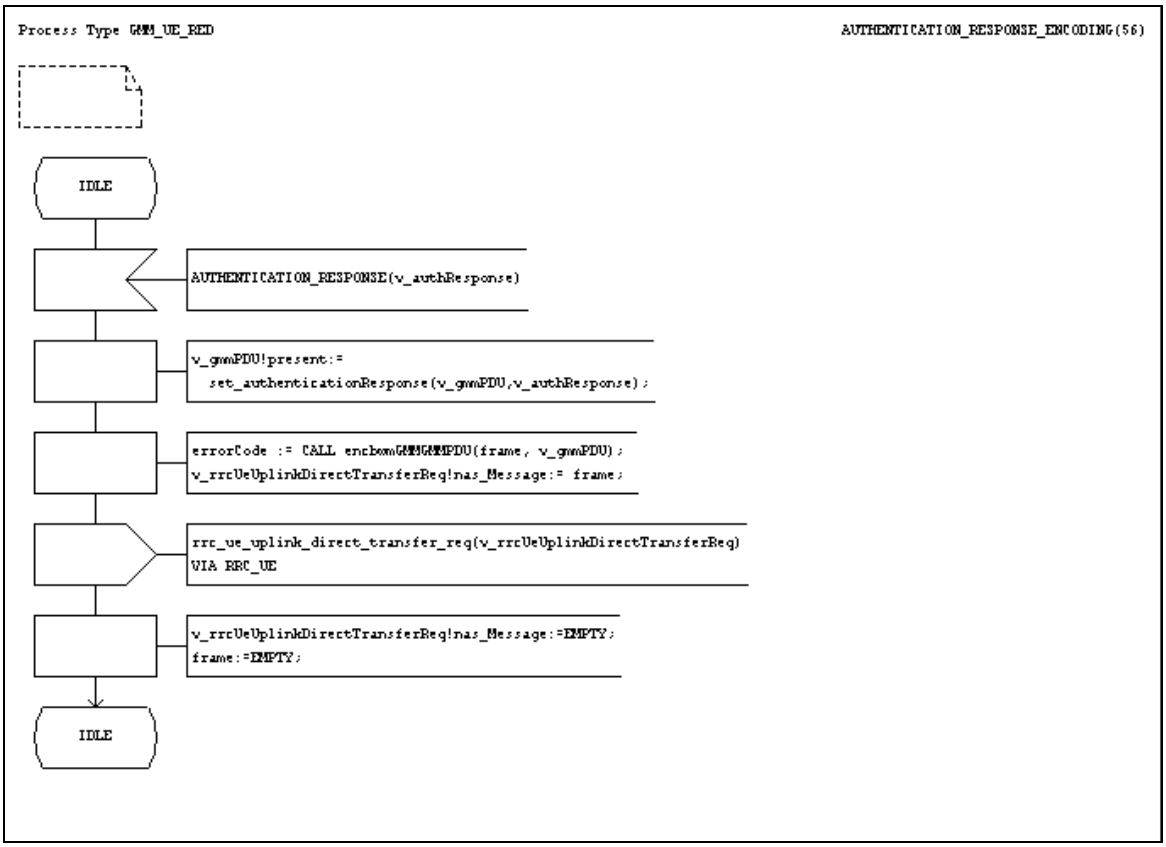



**Figure 6.8:** Example of encoding in GMM implementation

The encoding of PDU is done with encbwmGMMGMMPDU. The encoded PDU is sent to the transport layer in rrc_ue_uplink_direct_transfer_req primitive as one of fields of the primitive's parameter.

Finally I would like to briefly go through the encoding and decoding functions implementation process. Next section gives this description.

### 6.4. GMM encoding and decoding functions implementation

As was described earlier the GMM PDUs must be encoded before transition to peer entity and decoded when received. For this purposes encoding and decoding functions are used.

These functions were generated from the ASN.1 definitions using Asn2bwm tool and then manually corrected. Asn2bwm was developed in Nokia Research Center. Using ASN.1 definitions it is possible to write most of the information needed for encoding and decoding to the type specified in ASN.1. To make it possible some changes needed to be done in ASN.1 files. Mostly it is just an adding of CASN Compiler options.

Asn2bwm User's Guide defines four steps that are needed to be executed in order to produce encoding and decoding functions and to be able to use them [28]:

- Define the encoding rules for the protocol;
- Write the ASN.1 definitions according to the generic and protocol-specific encoding rules;
- Produce the encoding and decoding functions (codecs) using the Asn2bwm tool. Before Asn2bwm tool can be used, ASN.1 definitions have to be compiled with CASN Compiler;
- Link the produced codecs together with the rest of the code;

The produced codecs will be in *.c and *.ext source files. The *.ext file contains the codec function prototypes. The *.c file has to be linked into the program that uses encoding and decoding functions.

Finally, I would like to give an example of encoding and decoding of a GMM data type. Bellow an example of encoding and decoding of *RoutingAreaIdentification*:

```
void ebwmGMMRoutingAreaIdentification (BitVector v0,
  GMMRoutingAreaIdentification *home)
{
  bvPutInteger(v0, home->mcc2, 4);
  bvPutInteger(v0, home->mcc1, 4);
  bvPutInteger(v0, home->mnc3, 4);
  bvPutInteger(v0, home->mcc3, 4);
  bvPutInteger(v0, home->mnc2, 4);
```

```
  bvPutInteger(v0, home->mnc1, 4);
  bvPutString(v0, home->lac.st, 16);
  bvPutString(v0, home->rac.st, 8);
}

void dbwmGMMRoutingAreaIdentification (BitVector v0,
  GMMRoutingAreaIdentification *home)
{
  bvGetInteger (v0, &bwmLong,4);
  home->mcc2 = bwmLong;
  bvGetInteger (v0, &bwmLong,4);
  home->mcc1 = bwmLong;
  bvGetInteger (v0, &bwmLong,4);
  home->mnc3 = bwmLong;
  bvGetInteger (v0, &bwmLong,4);
  home->mcc3 = bwmLong;
  bvGetInteger (v0, &bwmLong,4);
  home->mnc2 = bwmLong;
  bvGetInteger (v0, &bwmLong,4);
  home->mnc1 = bwmLong;
  bvGetString (v0, home->lac.st, 16);
  bvGetString (v0, home->rac.st, 8);
}
```

When encoding a data type, its elements just putted one by one into bit vector, and get on decoding. The size of each field should be carefully checked, and the order of elements while encoding and decoding has to be the same.

To conclude the practical part of the thesis I would like to write a few words about the experience I have received while working on this project in Mobile Networks Laboratory, Nokia Research Center.

### 6.5. Experience

As a practical part of the Master's thesis a prototype implementation of GMM protocol was done. Different tools and languages were used for this work, such as Telelogic SDT tool, ASN.1 languages and CASN tools developed in Nokia Research Center. In this section I would like to express my experience of working with these tools.

Main work was done under the Telelogic SDT environment. The overall attitude to this SDL tool is good, and there were much more positive features than negative ones. In my opinion, the couple of important things have to be remembered before design of SDL models can be started:

- One of advantages of SDT is supporting of modularity. Such things as packages and types make the possibility of reusing SDL code in different models. The naming policy has to be agreed for better understanding of used code and the signals purposes. In my work 3G SDL Library Style Guide [9] was very helpful.

- The definition of data types was written on ASN.1 language. With help of Nokia CASN tools it is possible to use them in SDL model and to produce codecs. Thus this definition should be written properly before starting the real implementation work. Some definitions could have complex structure that follows difficult conversions in SDL. Little experience of SDL and ASN.1 programming helps to avoid this situation and to create more simple definitions for PDUs keeping their structure invariable.

- The one of main disadvantages of Telelogic SDT that it is not possible to control the code generation process.

- ASN.1 Nokia CASN tools and Telelogic SDT are quite powerful tools and fairly easy to use. With some experience it is possible to understand the behaviour of another SDL system in a short period of time. Even more the SDT gives a lot of assistant during the testing phase.

This thesis tried to provide a deep overview to the subject and I hope it will be useful to someone, who interested in mobility management problems of packet switched networks.

# 7. CONCLUSION

Mobility is a main difference between fixed networks and mobile networks. In this paper term mobility was defined as an ability of users to originate and receive calls and possibly use other services of the network anytime and anywhere.

Providing mobility is not an easy task, and specific mechanisms need to be implemented to support this feature. The aim of this thesis was to indicate different mobility procedures and then to find what modifications should be done when transmission technique is changed (there are two transmission techniques: circuit switching and packet switching). The work was concentrated on the overview of mobility management tasks performed by different protocols in packet switched domain.

As was indicated in this paper the main mobility management functions are location updating, paging procedure, handover and provision of roaming. Location updating is used to notify the network about the current location of the UE. Paging is needed whenever a call should be delivered to the UE. Handover gives the user a possibility to move while having an active call. Roaming was defined as ability to use the UE within networks controlled by different operators.

As was shown on the thesis if packet switching is used when transmitting a message, this message is divided into small packages and then each of them is sent to the destination. Therefore some modifications should be done while performing mobility management functions.

The overview of mobility management protocol was presented in this paper to help the reader to understand how mobility is supported. The functionality of GMM protocol was studied in derails. A prototype implementation of GMM was given in the thesis as a practical part of the work.

This thesis tried to provide a deep overview of the subject, and hopefully it will be useful to someone interested in mobility details.

# REFERENCES

[1] Technical Specification 24.008 version 4.7.0: Mobile radio interface Layer 3 specification; Core network protocols, 3GPP, 2002.

[2] Technical Specification 23.060 version 4.6.0: Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS), 3GPP, 2002.

[3] Technical Specification 24.007 version 4.2.0: Technical Specification Group Core Network; Mobile radio interface signalling layer 3, 3GPP, 2002.

[4] H.Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi, *UMTS Networks*, John Wiley & Sons, 2001.

[5] NOKIA 3G System course, Training materials, Nokia Networks Oy, Finland 2002

[6] Technical Specification 23.003 version 4.4.0: Technical Specification Group Core Network; Numbering, addressing and identification, 3GPP, 2002.

[7] 3G SDL Library implementation framework course materials, Nokia Research Center, Mobile Network Laboratory, Finland, 2002

[8] ITU-T Recommendation Z.100, 1993. Programming languages, CCITT Specification and Description Language (SDL). Geneva: International Telecommunication Union (ITU)

[9] Juhä Sipilä, Vesa Luukkala, An SDL Implementation Framework for Third Generation Mobile Communication System, Nokia Research Center, Mobile Network Laboratory, 2001.

[10] LO Walters, PS Kritzinger, Cellular Networks. Past, Present and Future, Article, 2000.

[11] Mouly Michel, Pautet Marie-Bernadette: The GSM System for Mobile communications, Published by the authors, 1992

[12] Ian F. Akyildiz, Janise McNair, Joseph Ho, Huseyin Uzunaloglu, Wenye Wang, Mobility in Next Generation Wireless Systems, Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology

[13] Siitari H.-L., Workstation Testing of GPRS Mobility Management, Master's Thesis, University of Oulu, Department of Electrical Engineering, Finland, 2000

[14] Issaeva Tatiana, Radio Subsystem Management in 3G Mobile Communications, Master's Thesis, Lappeenranta University of Technology, 2000

[15] Andrei Zimenkov, Transport Resource Management within UMTS Radio Network Subsystem, Master's Thesis, Lappeenranta University of Technology, 2002

[16] http://www.umtsworld.com/

[17] Introduction to SDL course training materials, Telelogic AB, 2001

[18] www.telelogic.com

[19] Technical Specification 29.002 version 4.8.0: Technical Specification Group Core Network; Mobile Application Part (MAP) specification, 3GPP, 2002.

[20] Technical Specification 29.060 version 4.4.0: Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface, 3GPP, 2002.

[21] Technical Specification 25.331 version 4.6.0: Technical Specification Group Radio Access Network, Radio Resource Control (RRC) Protocol Specification, 3GPP, 2002.

[22] Technical Specification 25.413 version 4.5.0: Technical Specification Group Radio Access Network, UTRAN Iu interface RANAP signalling, 3GPP, 2002.

[23] www.3gpp.org

[24] Location Registration, Nokia internal document, Nokia Corporation, 2002

[25] Pressman Roger s., Software Engineering. A practitioner's Approach, Forth Edition, The McGraw-Hill Companies, USA, 1997.

[26] ISO 8824(90)/X.208(88) Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)

[27] Marina Lishchina, GMM protocol presentation slides, Nokia Research Center, Mobile Network Laboratory, 2002.

[28] Antti Kuosmanen, Asn2bwm User's Guide, Nokia Research Center, 2002

[29] Qi Wang, Mosa Ali Abu-Rgheff, Towards a Complete Solution to Mobility Management for Next-Generation Wireless System, The University of Plymouth/Department of Communication and Electronic Eng., 2002

[30] Telelogic AB: SDT 3.5 Reference Manual, 2000

# APPENDIX I. Timers of GPRS mobility management

| **UE side** | | | | |
|---|---|---|---|---|
| Timer Num. | Timer Value | State | Cause of Start | Normal Stop |
| T3310 | 15s | GMM-REG-INIT | ATTACH REQ sent | ATTACH ACCEPT received<br>ATTACH REJECT received |
| T3311 | 15s | GMM-DEREG or GMM-REG | ATTACH REJ received (depending of cause value)<br>ROUTING AREA UPDATE REJ received (depending of cause value)<br>Low layer failure | Change of the routing area |
| T3316 | 30s | GMM-REG-INIT<br>GMM-REG<br>GMM-DEREG-INIT<br>GMM-RA-UPDATING-INT<br>GMM-SERV-REQ-INIT | Authentication parameters stored after receipt of a UMTS authentication challenge | Security mode setting<br>AUTHENTICATION & CIPHERING REJECT received<br>Enter GMM-DEREG or GMM-NULL |
| T3318 | 20s | GMM-REG-INIT<br>GMM-REG<br>GMM-DEREG-INIT<br>GMM-RA-UPDATING-INT<br>GMM-SERV-REQ-INIT (UMTS only) | AUTHENTICATION & CIPHERING FAILURE (cause='MAC failure' or 'GSM authentication unacceptable') sent | AUTHENTICATION & CIPHERING REQUEST received |
| T3320 | 15s | GMM-REG-INIT<br>GMM-REG<br>GMM-DEREG-INIT<br>GMM-RA-UPDATING-INT<br>GMM-SERV- | AUTHENTICATION & CIPHERING FAILURE (cause=synch failure) sent | AUTHENTICATION & CIPHERING REQUEST received |

| | | | | |
|---|---|---|---|---|
| | | REQ-INIT (UMTS only) | | |
| T3321 | 15s | GMM-DEREG-INIT | DETACH REQ sent | DETACH ACCEPT received |
| T3330 | 15s | GMM-ROUTING-UPDATING-INITIATED | ROUTING AREA UPDATE REQUEST sent | ROUTING AREA UPDATE ACC received<br>ROUTING AREA UPDATE REJ received |
| T3302 | Default 12 min | GMM-DEREG or GMM-REG | At attach failure and the attempt counter is greater than or equal to 5.<br>At routing area updating failure and the attempt counter is greater than or equal to 5. | At successful attach<br>At successful routing area updating |
| T3312 | Default 54 min | GMM-REG | In UMTS, when peer-to peer connection is released. | When entering state GMM-DEREG |
| T3317 | 10s | GMM-SERVICE-REQUEST-INITIATED | SERVICE REQ sent | Security mode control procedure is completed,<br>SERVICE ACCEPT received, or<br>SERVICE REJECT received |
| **Network side** | | | | |
| T3322 | 6s | GMM-DEREG-INIT | DETACH REQ sent | DETACH ACCEPT received |
| T3350 | 6s | GMM-COMMON-PROC-INIT | ATTACH ACCEPT sent with P-TMSI and/or TMSI<br>RAU ACCEPT sent with P-TMSI and/or TMSI<br>P-TMSI REALLOC COMMAND sent | ATTACH COMPLETE received<br>RAU COMPLETE received<br>P-TMSI REALLOC COMPLETE received |
| T3360 | 6s | GMM-COMMON-PROC-INIT | AUTH AND CIPH REQUEST sent | AUTH AND CIPH RESPONSE received<br>AUTHENT-AND CIPHER-FAILURE received |
| T3370 | 6s | GMM- | IDENTITY REQUEST | IDENTITY |

| | | | | |
|---|---|---|---|---|
| | | COMMON-PROC-INIT | sent | RESPONSE received |
| T3313 | Network dependent | GMM_REG | Paging procedure initiated | Paging procedure completed |
| Mobile Reachable | Default 4 min greater than T3312 | All except GMM-DEREG | In UMTS, change to IDLE mode. | PDU received |