Wideband cellular signaling system simulator

Master's Thesis

Juha Sipilä

5. November 1998

Helsinki University of Technology

Department of Computer Science

ABSTRACT

Author:	Juha Sipilä
Date of birth:	4.9.1972
Student number:	43979R
Department:	Computer Science / Telecommunication software and multimedia laboratory
Major:	Telecommunication software
Minor:	Software systems
Subject:	Wideband cellular signaling system simulator
Instructor:	Ari Ahtiainen / Nokia research Center
Inspector:	Professor Olli Martikainen
Keywords:	WCDMA, signaling, radio interface, CVOPS

Description:

The success of the current 2nd generation mobile communications systems has created a worldwide interest towards the development of a 3rd generation mobile-communication-systems. One of the most promising radio access technologies currently is Wideband Code Division Multiple Access (WCDMA), which is under major research activities around the world.

This Master's thesis describes a control plane trial WCDMA signaling specification initiated by Japanese telecommunication operator NTT/DoCoMo and implementation of the specification done by Nokia Research Center. The Implementation was done with CVOPS protocol development tool. There is also a short introduction to 3rd generation-mobile-communication-systems in general and to the current standardization situation. GSM system is used as a reference in suitable places.

To keep the length of this presentation reasonable, only OSI layer-3 specific radio interface signaling is described.

TIIVISTELMÄ

Tekijä:	Juha Sipilä
Syntymäaika:	4.9.1972
Opiskelijanumero:	43979R
Osasto:	Tietotekniikka/Tietoliikenneohjelmistojen ja multimediatekniikan laboratorio
Pääaine:	Tietoliikenneohjelmistot
Sivuaine:	Ohjelmistojärjestelmät

Työn nimi:	Laajakaistaisen soluverkon signalointijärjestelmän simulaattori
Ohjaaja:	FK Ari Ahtiainen / Nokia Research Center
Valvoja:	Professori Olli Martikainen
Hakusanat:	WCDMA, Signalointi, radiorajapinta, CVOPS

Kuvaus:

Toisen sukupolven matkapuhelinjärjestelmien menestys on luonut maailmanlaajuisen kiinnostuksen kolmannen sukupolven matkapuhelinjärjestelmän kehittämiseen. Yksi lupaavimmista ehdokkaista kolmannen sukupolven radiosaantitekniikaksi on tällä hetkellä Wideband Code Division Multiple Access (WCDMA), jota tällä hetkellä tutkitaan voimakkaasti.

Tämä diplomityö kuvaa japanilaisen matkapuhelinoperaattorin NTT/DoCoMo:n WCDMA signalointi spesifikaation ja Nokia Research Center:n tekemän toteutuksen spesifikaatiosta. Implementaatio on tehty CVOPS protokollakehitys työkalulla. Diplomityössä on myös lyhyt yleiskuvaus kolmannen sukupolven järjestelmistä ja tämän hetkisestä standardointitilanteesta. GSM järjestelmää käytetään esimerkkinä joissain kohdissa.

Jotta esityksen laajuus säilyisi kohtuullisena, ainoastaan OSI-mallin kolmatta kerrosta vastaava radiorajapinnan signalointi on kuvattu.

PREFACE

This master's thesis has been written in Nokia Research Center/Mobile Networks laboratory as a part of MCC-SIM project. It has been interesting to work in this project among people truly dedicated to their work. Special thanks to Sami Virtanen and Marko Teittinen for helping me out with the numerous technical details.

I would like to thank my instructor Ari Ahtiainen for patience and understanding. Without his help this master's thesis would never been finished. Also thanks to Marko Teittinen who, despite his duties, had time to read through this master's thesis and gave valuable comments.

Furthermore I would like to thank Prof. Olli Martikainen for his participation as a supervisor.

I would like to thank Sari Männynsalo and Petri Grönberg about their spiritual support and all the help concerning the language. Sari is better than the syntax checker...

Special thanks to Atte Artamo and Juha Kärnä for helping me to understand the essence of CDMA and to Tuomo Sipilä and Juho Laatu for their invaluable help concerning the standardisation.

In addition, I would like to express my gratitude to my parents for supporting my studies. Finally, I would like to thank Minna for her patience and understanding during this work.

Helsinki, 5. November, 1998

Juha Sipilä

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

A3	GSM authentication algorithm
A5	GSM ciphering algorithm
A8	GSM ciphering key computation algorithm
ACCH	Associated Control CHannel
ADP	Adapter for Data Transmission
ANSI	American National Standards Institute
ARIB	Association of Radio Industries and Business
ASCII	American national Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
ASN2C	Abstract Syntax Notation to C-language
ATM	Asynchronous Transfer Mode
AUX	AUXilary
BCCH	Broadcast Control CHannel
BER	Basic Encoding Rules
BPSK	Binary Pulse Shift Keying
BS	Base Station
BSC	Base Station Controller
BSS	Base Station System
CASN	C to Abstract Syntax Notation
CC	Call Control
CCSP	Common Channel Signaling Protocols
CDG	CDMA Development Group
CDMA	Code Division Multiple Access
CONN_ID	Connection IDentifier
CR	Call Reference
CVOPS	C-based Virtual OPerating System
DHO	Diversity HandOver
DoCoMo	NTT Mobile Communications Network, Inc.
DSP	Digital Signal Processing
DTCH	Dedicated Traffic CHannel
EFR	Enhanced Full Rate
EFSA	Extended Finite State Automaton
EIA	Electronic Industries Association
ETSI	European Telecommunication Standards Institute
FACH	Forward Access Control CHannel
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FPLMTS	Future Public Land Mobile Telephone System
GDB	GNU Debugger
GPRS	General Packet Radio System
GSM	Global System for Mobile Communication
HHO	Hard HandOver
HLR	Home Location Register
HSCSD	High-Speed Circuit Switched Data
IMSI	International Mobile Subscriber Identity
IMT-2000	International Mobile Telephone 2000

IMUI	International Mobile User Identity
IP	Internet Protocol
IS	Interim Standard
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
JDC	Japan Digital Cellular
k_c	Ciphering key
LAC	Link Access Control
LAI	Location Area Identifier
LU	Location Update
MAC	Medium Access Control
MAP	Mobile Application Part
MCC	Mobile Country Code
MCC-SIM	Mobile Control Center-Subscriber Identity Module
MM	Mobility Management
MNC	Mobile Network Code
MOC	Mobile Originated Call
MS	Mobile Station
MSC	Mobile services Switching Center
MS-Sim	Mobile Station Simulator
MS-Tester	Mobile Station Tester
MTC	Mobile Terminated Call
NCDMA	Narrowband Code Division Multiple Access
NMP	Nokia Mobile Phones
NRC	Nokia Research Center
NTT	Nippon Telegraph and Telephone
PCH	Paging CHannel
PCS	Personal Communication Services
PDC	Personal Digital Cellular
PDU	Protocol Data Unit
PHYS	PHYSical
PID	Process IDentifier
PLMN	Public Land Mobile Network
QoS	Quality of Service
QPSK	Quadrate Pulse Shift Keying
RACH	Random Access CHannel
RAND	RANDom
RBC-id	Radio Bearer Control - identifier
RIM	Radio Interface Management
RNC	Radio Network Controller
ROSE	Remote Operations Service Element
RRC	Radio Resource Control
SDCCH	Stand-alone Dedicated Control CHannel
SDL	Specification and Description Language
SF	Spreading Factor
SoHO	Softer HandOver
SHO	Soft HandOver
SRES	Signed RESult
SSCOP	Service Specific Connection Oriented Protocol
TAC	Terminal Association Control

TC-info	Terminal Capabilities-information
TCP	Transmission Control Protocol
TD-CDMA	Time Division Multiple Access/Code Division Multiple Access
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TMSI	Temporary Mobile Subscriber Identity
TMUI	Temporary Mobile User Identity
TN	TraNsparent
TTC	Telecommunication Technology Committee
UMTS	Universal Mobile Telecommunication System
UPCH	dedicated User Packet CHannel
UWCC	Universal Wireless Communications Consortium
WARC	World Administrative Radio Conference
WCDMA	Wideband Code Division Multiple Access
VLR	Visitor Location Register
VTT	Valtion teknillinen tutkimuskeskus (Technical Research Centre of Finland)

1. INTRODUCTION

During the 1990's the usage and importance of mobile communications has increased substantially. Mobile communication has become an important part of our everyday lives and society in general. The essential reason for this development has been the new digital mobile-communication-systems, which have provided more capacity, better speech quality, advanced services, and light and portable terminals.

These currently used mobile-communication-systems are called 2nd generation mobile-communication-systems. The difference between the 1st and 2nd generation is that the 1st generation systems are based on analog technology. Due to economical, political, and occasionally also for technical reasons, there are several competing 2nd generation mobile-communication-systems.

Current mobile-communication-systems are constantly evolving, but it has still been long known that they will not be sophisticated enough in the next millennium. Already during the 2nd generation specification phase, the first projects for drafting 3rd generation mobile-communication-systems were initiated. After years of specification work, these systems are now becoming a reality and the first test systems are under implementation. The first commercial networks should be ready already in 2001.

During the project, which this master's thesis is part of, a signaling testing system for 3rd generation mobile station has been implemented. The system is based on a specification made by Japan's leading mobile telecommunication operator *NTT/DoCoMo*. The specification is based on WCDMA (*Wideband Code Division Multiple Access)* radio access technology. The concept '*wideband*' refers to the fact that the capacity of the system is lower than in the current fixed networks, which are broadband systems, but it is higher than in the current 2nd generation mobile-communication-systems, which are narrowband systems.

The objective of the work was to implement required protocols and assist in the development of a fully operational tester system required by the customer. During the implementation and integration phase, a lot of information about protocol programming, development tools, and signaling procedures specific to WCDMA was gained.

This master's thesis has five chapters excluding the Introduction and Conclusion. Chapter 2 introduces the current standardization status of 3rd generation mobile-communication-systems, which is by no means a simple matter. Chapter 3 describes the basic architecture of the trial system. Also short descriptions about the basic WCDMA concepts are included.

Chapter 4 describes the radio interface specific layer-3 signaling. Layer-2 specific signaling was left out in order to keep the length of this presentation reasonable. The internal interfaces of the network were also left out, since they are not needed when a mobile station is tested.

Chapter 5 describes experimental part of this master's thesis. It describes the implementation of the Mobility Management protocol and partly the Terminal Association Control protocol. The integration process of the whole stack is also been described. Short descriptions are also provided about the tracing methods, tools used, and tester usage.

2. STANDARDISATION OF 3RD GENERATION SYSTEMS

2.1 Background

Already in the middle of 1980's during the ongoing regional 2nd generation standardization work, the first international research projects for sketching 3rd generation mobile-communication-systems and standards were initiated by ITU *(International Telecommunication Union)* under the name FPLMTS *(Future Public Land Mobile Telephone System)* [LEK97].

All the ITU specific work was intended to be unified to the FPLMTS, renamed later on to IMT-2000 *(International Mobile Telephone 2000)*, which in the ideal case was intended to be the totally new, one and only 3rd generation mobile-communication-system throughout the world. However, the current development seems to be leading to a situation, where the ITU specifications will work more as a framework and there will be multiple 3rd generation mobile-communication-system standards. The ITU has accepted the situation and recently designed a so-called *'family concept'*, which allows this type of development. Multiple competing system may exist, but they are specified by the ITU to be interoperable [ETR1201] [Cl98].

One of the most important issues in 3rd generation mobile-communication-system development work has been the allocation of required frequency bands, which are very limited natural resource. After years of preliminary work, the agreement was made in the WARC-92 -conference (*World Administrative Radio Conference*) in 1992. Conference decided, that there will be two worldwide frequency bands for 3rd generation mobile-communication-systems: 1885-2025 MHz and 2110-2200 MHz. The national regulators were requested to 'clean' these bands, but some parts of the frequency bands are still in use (see Chapter 2.2.2). There have been some doubts, whether the reserved frequency bands will be adequate for expected traffic rates or not. It is possible, that further allocations will be done in the future [LEK97][CHB97].

2.2 Regional situation

2.2.1 General

The ITU is not the only organization doing 3rd generation mobile- communication-system standardization and development work. In addition, the regional standardization organizations in Europe, Japan and the United States are doing the corresponding work.

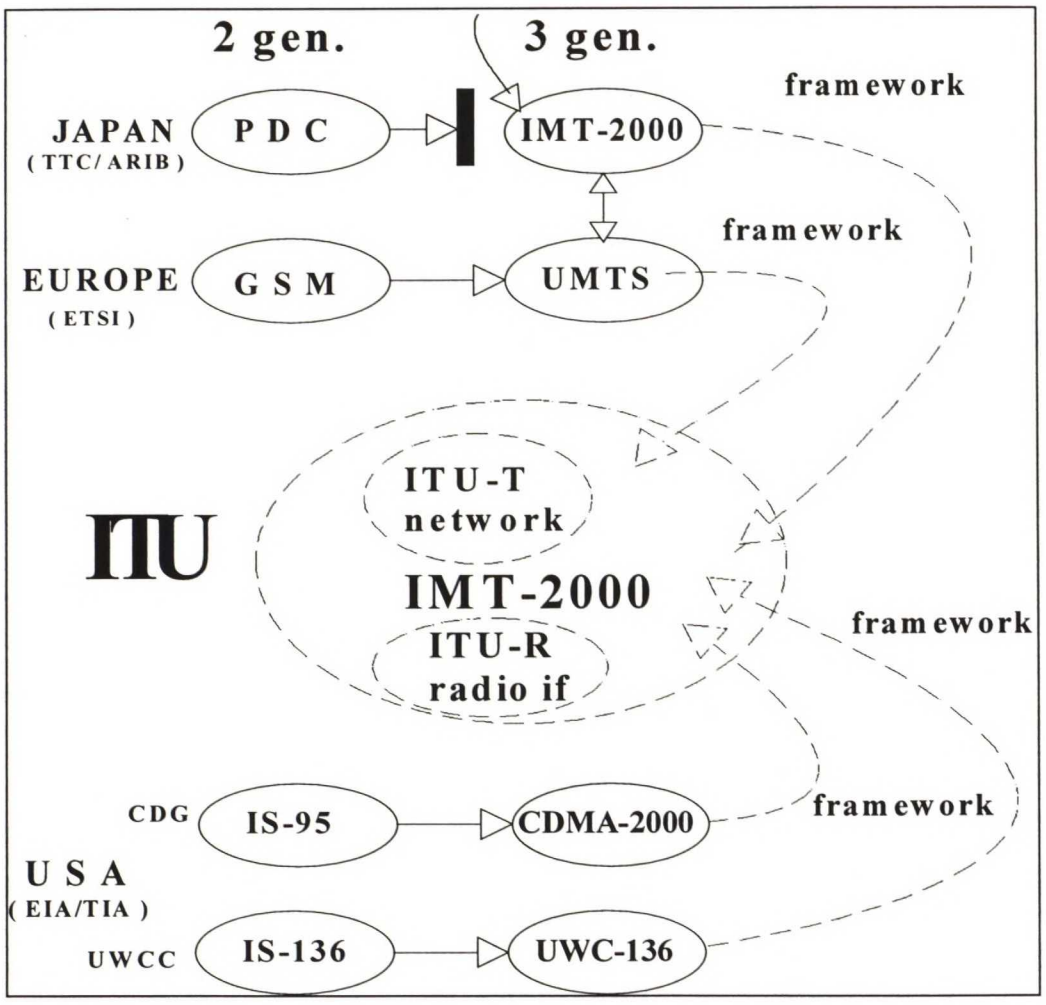


Figure 1: The global standardization status

2.2.1 Europe

Telecommunication standardization in Europe is centralized to the ETSI *(European Telecommunication Standards Institute)*. The ETSI 2nd generation mobile-communication-system is called GSM *(Global System for Mobile communications)* [GSM0102] [MB92]. GSM has been very successful and it is in use around the world. There exists three different variants of GSM in three different frequency bands: 900 MHz, 1800 MHz, and 1900 MHz (USA). The development of the GSM standard is still ongoing. New features like the packet data system GPRS (*General Packet Radio System*), the improved circuit switched data HSCSD (*High Speed Circuit Switched Data*), and the improved speech coding technology EFR (*Enhanced Full Rate*) have been specified and partly implemented. The extended GSM standard with these new features is called GSM phase 2+.

The ETSI 3rd generation mobile-communication-system is called UMTS *(Universal Mobile Telecommunication System)*. Initially UMTS was designed to be a totally new system. However, due to economical and political reasons, certain parts of UMTS, for example mobility management and packet data services, will be based on GSM phase 2+. According to the decision made in the ETSI meeting on 29.1.1998, UMTS will have two different radio access technologies: WCDMA and TD-CDMA *(Time Division Multiple Access/Code Division Multiple Access)*. More information about the decision and the differences between the two technologies can be found in [EPR1702].

2.2.2 USA

The standardization in the USA has traditionally been less formal than in Europe. The companies make contributions and proposals to the standardization organizations and some of them are accepted as official standards.

The national standardization organization is the ANSI *(American National Standards Institute)*, which is the USA's official representative in the global standardization.

Most of the standards in the USA are accredited by the ANSI, but specified by the special organizations focused on a certain problem area.

Currently the USA has two major organizations doing mobile-communication-system standardization. The TIA/EIA *(Telecommunications Industry Association/Electronic Industries Association)* is a member-driven trade organization, which also does telecommunication standardization. All IS-series *(Interim Standard)* standards are made by the TIA/EIA. The TIA/EIA has been accredited by the ANSI since 1992.

The ANSI Committee T1 is more formal and traditional standardization organization than the TIA/EIA. The ANSI Committee T1 creates all types of telecommunication standards and takes care of the USA's technical contributions to the ITU. The GSM-1900 standard, which is the USA's version of GSM, has been designed by the T1 [CHB97].

Currently the USA has three major competing 2nd generation mobile-communication- system standards:

1. **IS-95 (TIA/EIA)**

- Based on the narrowband CDMA-technology
- Support group is the CDG *(CDMA development group)*
- Operates in both the 800 MHz and the 1900 MHz frequency band

2. **IS-136/IS-54 (TIA/EIA)**

- Based on the narrowband TDMA-technology
- Older versions are called D-AMPS
- Support group is the UWCC *(Universal Wireless Communications Consortium)*
- Operates in both the 800 MHz and the 1900 MHz frequency band

3. **GSM-1900 (T1)**

- ETSI's GSM specification customized to 1900 MHz frequency band
- Supported group is the GSM alliance
- Operates only in the 1900 MHz frequency band

The mobile-communication-systems operating on the 1900 MHz frequency band are called PCS-systems *(Personal Communication Services)*. The 1900 MHz frequency band was allocated by the FCC *(Federal Communications Commission)*, which is the USA's official frequency band regulation authority, due to the several request from the different authorities. The older 800 MHz frequency band was full and there were no *frequency band licenses* (a permission to use the certain frequencies in a certain geographical area) available for the new operators. The lack of the frequency band licenses limited the growth of cellular markets in the USA.

The PCS-systems generally provide more services and better speech quality than the mobile-communications-systems operating on the 800 MHz frequency band. The wideband PCS markets are currently developing rapidly. The major problem has been the FCC's policy to sell the frequency band licenses in an auction. The prices have been too high and therefore many operators have been unable to build the actual network or they have gone to bankruptcy. General information about the PCS-systems can be found in [Me97].

All the TIA-standards are using their own network standard called IS-41. Network standard specifies the network components and their interfaces. GSM-1900 uses GSM core network. GSM core network uses different specification and is a competitor to the IS-41 network standard.

Both IS-95 and IS-136 will be evolved into a 3rd generation mobile communication standards. The next generation IS-95 is based on the wideband CDMA technology and is called *CDMA-2000*. Next generation IS-136 is based on the wideband TDMA technology and is called *UWC-136*. The Development from 2nd to 3rd generation mobile-communication-system will happen in several phases and the enhanced networks stay compatible with the older mobiles. Both systems are contributed to the ITU and according to their support groups, they are planned to be part of the ITU's family concept. The GSM-1900 evolution is very likely going to follow the ETSI's UMTS path [CDGCONT] [UWCCCONT] [Me97] [UWCCPR2302] [CDGPR0406].

Unfortunately the 1900 MHz frequency band used by the wideband PCS-systems is located in the area allocated for 3rd generation systems, and hence the USA has

already used part of the radio resources dedicated for 3rd generation mobile-communication-systems. How this situation affects to the commercialization of 3rd generation mobile-communication-systems remains to be seen.

2.2.3 Japan

Japanese telecommunication markets have been very closed. The Japanese standardization organizations the TTC *(Telecommunication Technology Committee)* and the ARIB *(Association of Radio Industries and Business)* have a 2nd generation mobile-communication-system-specification called PDC *(Personal Digital Cellular)* [RCR27F]. The older name for PDC was JDC *(Japan Digital Cellular)*. PDC has not been sold outside Japan, and the Japanese companies, which have supported PDC, have had only moderate market shares with the mobile-communication-systems based on the other standards. Due to the closed standardization policy, the foreign companies have also had major difficulties in implementing PDC terminals and networks.

Japan has been very active in 3rd generation mobile-communication-system development for many reasons. The Japanese companies have had very low market shares in the very profitable global telecommunication markets and there is a national project to improve the situation when the next generation systems are sold. The Japanese customers require new services that are more advanced and these require more transfer capacity. The frequency capacity in Japanese 2nd generation mobile-communication-system networks is also running out and there is an urgent need for the new and more spectrum efficient radio access technology.

Instead of creating completely own system like PDC, the Japanese are counting on openness in 3rd generation mobile-communication-system standardization. The Japanese standardization organizations have been contributing material to the ITU for a long time and nowadays they also have close contacts to the ETSI. The goal is to have a trial network ready in the year 1999 and a commercial network in the year 2000. The radio access technology in the Japanese system is going to be WCDMA.

The Japan's biggest telecommunication operator, NTT/DoCoMo, has been actively supporting the standardization. NTT/DoCoMo has implemented an own trial specification and done agreements with the major mobile-communication-system manufactures for implementing a trial system according to the specification.

Nokia was chosen to implement a trial mobile station to this system. The simulator described in this master's thesis has been used to test signaling of this produced mobile station within Nokia [NPR0304] [DPR0304].

2.3 Requirements

Currently the name 3rd generation mobile-communication-system is used when talking about a mobile communication system specification, which meets certain requirements (see table 1). The requirements for the satellite systems are different than for the terrestrial systems, but in this master's thesis, the satellite systems are excluded. More information about 3rd generation mobile-communication-satellite-systems can be found in [ETR1201] (the ETSI perspective) and in [Me97].

The current 3rd generation mobile-communication-system specifications are at least in some scale contributed to the local standardization bodies such as the ETSI and the international ones such as the ITU. The ITU specifications differ from the regional ones by being intended to be more frameworks than actual 'bit-level' specifications.

The ITU and the ETSI have both tried to specify some requirements for describing a 3rd generation mobile-communication-system and for separating it from 2nd generation mobile-communication-systems. Requirement lists are very long and are more advisory than exact. Some of the key issues are listed in the table 1. Longer lists can be found in [UMTS3001] and in [ETR1201].

1. Higher bit rates (ITU-T + ETSI)
• 144 kbit/s Rural Outdoor
• 384 kbit/s Suburban Outdoor
• 2048 kbit/s indoor/low range Outdoor
2. Wideband and multimedia services
• Possibility to provide the QoS services (ITU-T + ETSI)
• Internetworking with the IP + the other existing networks (ITU-T + ETSI)
• Independent service creation (ETSI)
• Virtual Home Environment – concept (ITU-T + ETSI)
3. International roaming (ITU-T + ETSI)
• Roaming between all 3rd generation mobile-communication-systems worldwide
• Interoperability to 2nd generation networks
4. Efficient spectrum usage (ITU-T + ETSI)
5. Operates in 3rd generation frequency band (ITU-T + ETSI)

Table 1: The major requirements for 3rd generation mobile-communication-systems.

The main difference between the 3rd generation and 2nd generation mobile-communication-systems are the bit-rates, which are considerably higher in the 3rd generation mobile-communication systems. The general concept of the service standardization is also modernized. The service capabilities are standardized instead of the fixed services. The service capabilities consist of the bearers (see Chapter 3.3.4) defined with the QoS parameters, and the mechanisms needed to realize the services. The standard will provide mechanisms for the service operators and the providers to create their own supplementary services, teleservices, and end-user-applications [UMTS3001].

The advanced services and the higher bit-rates will require more frequency band and more sophisticated infrastructure. This naturally increases the cost of the provided services. How the users are going to react to the new systems and are they willing to pay the price of the new technology remains to be seen.

The other important issue is the international roaming. The 1st generation mobile-communication-systems were designed to be national or allowing roaming in limited number of countries. The 2nd generation mobile-communication-systems were continental (initially) and the 3rd generation mobile-communication-systems are designed to be global. The roaming must be possible anywhere without changing the terminal. In addition, the interoperability to 2nd generation mobile-communication-systems must be guaranteed for providing the sufficient initial coverage and service level.

The efficient spectrum usage and usage of the 3rd generation frequency bands are very self-evident requirements and are strongly dependent on the used radio technology. The radio technology in 3rd generation mobile-communication-systems is intended to be wideband differing from the narrowband used in 2nd generation mobile-communication-systems.

3. A WIDEBAND CODE DIVISION MULTIPLE ACCESS TRIAL SYSTEM

3.1 General

Due to the reasons described in Chapter 2.2.3, The Japanese mobile network operators and telecommunication authorities have had an interest to develop a new more efficient mobile communication standard. Among many possible radio access technologies, WCDMA was found to be the most promising one. Before the final decision can be made, the new technology must anyhow be tested in a complete mobile-communication-system environment.

The leading Japanese mobile network operator NTT/DoCoMo took the first initiative and decided to build a WCDMA trial system. NTT/DoCoMo had no intention to build the system by itself, but instead they did a specification and requested proposals about the implementation from the leading mobile-communication-system manufacturers. According to given proposal, NTT/DoCoMo chose the manufacturer to implement the mobile station and/or the network side.

The purpose of the trial system is to provide a multifunctional experimental environment, which can be used to test and gain experience from WCDMA, both from the viewpoint of radio technology and functionality of the complete system. Due to the experimental nature of the system, the specification has been designed with a tight time schedule. General idea seems to have been, to take the all the suitable parts from the current 2nd generation standards, and redesign only those entities that are affected by the new WCDMA radio technology.

3.2 Architecture

The architecture of the WCDMA trial system consists of MS *(Mobile Station)*,BS (Base Station), and MCC-SIM *(Mobile Control Center – Subscriber Identity Module)*. The MCC-SIM is divided to DHO (*Diversity HandOver unit/TransCoder)*, ADP *(Adaptor for Data Transmission)*, and MCC-CNT (*Mobile Control Center – Controller*). Transmission method between the network elements and within MCC-SIM is *Asynchronous Transfer Method* (ATM).

MCC-CNT is a base station controller simulator. It corresponds BSC (*Base Station Controller*) of GSM. Since the WCDMA trial system does not have a separate MSC *(Mobile switching Center)*, MCC-CNT also takes care of needed MSC functions.

The DHO/TC is a unit, which takes care of macrodiversity handling of one MS. It also converts digital speech data into analog form. The ADP is an adapter unit between the external data interfaces and the rest of WCDMA trial system.

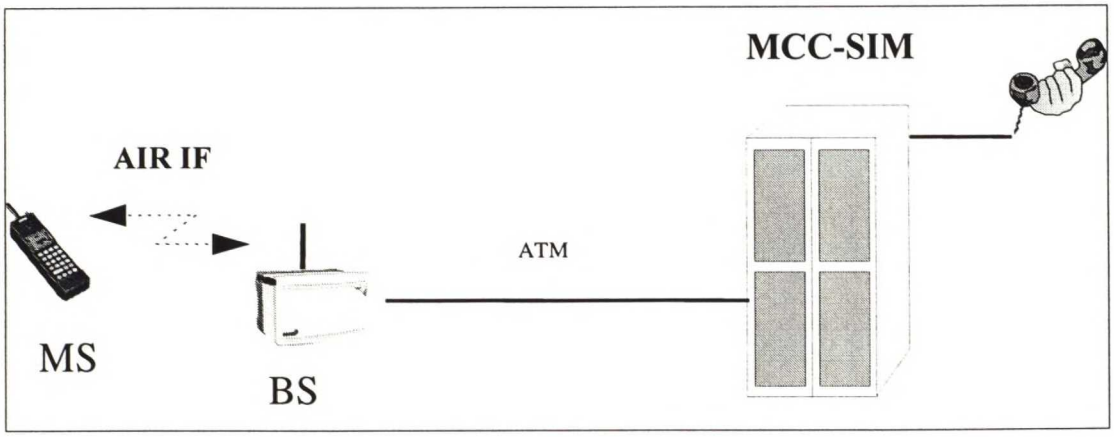


Figure 2: The architecture of the WCDMA trial system

The WCDMA trial system should include at least one MCC-SIM and a few BSs, so all the different handover types could be tested. Every BS should be able to have multiple sectors. Every sector covers certain angle around the BS.

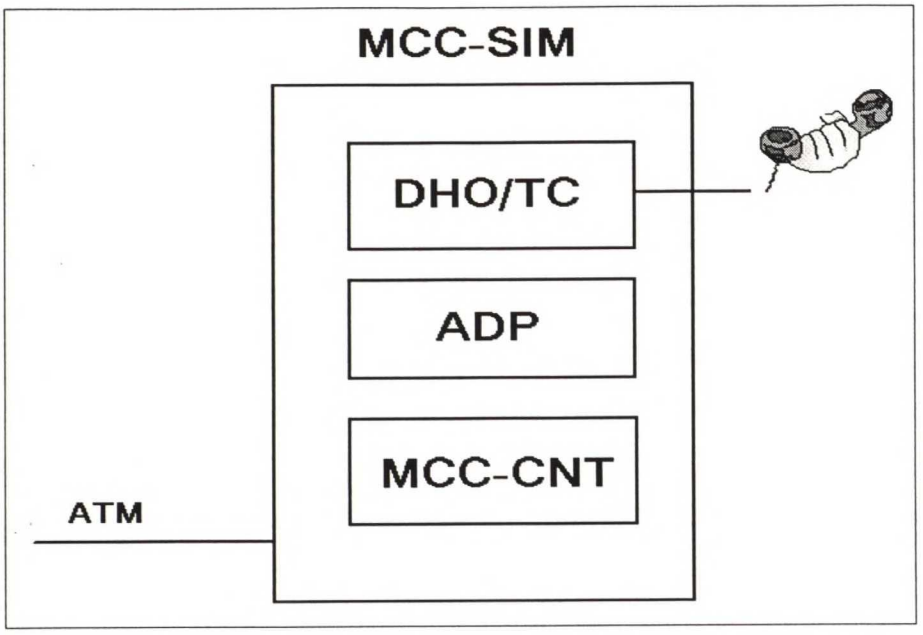


Figure 3: The logical structure of the MCC-SIM

There should be a possibility to have multiple MSs in one sector. Maximum of two simultaneous calls to an MS should be supported. This property is called *Multicall*.

3.3 Basic concepts

3.3.1 CDMA

3.3.1.1 Introduction

Mobile-communication-systems have a certain fixed amount of radio band available and multiple users use it simultaneously. This creates a requirement to somehow divide the band, so that it would be possible for all users to exploit the common resource without interfering others. The methods used to divide the common resource are called *access methods*. This Chapter is based on [OP98].

The most common currently used access methods are FDMA *(Frequency division multiple access)*, TDMA *(Time division multiple access)* and the narrowband version of CDMA *(Code division multiple access)*. FDMA technology divides one major frequency band to a group of smaller bands and dedicates one frequency to each user. FDMA is the only possible multiplexing scheme to be used in analog systems. TDMA technology multiplexes the information stream to multiple time slots. The traffic specific for a user is sent in a certain time interval. TDMA technology requires that sent information is converted to digital form before the transmission and multiplexing. TDMA and FDMA techniques are often combined so, that the entire available frequency band is divided with FDMA between cells and one frequency is divided to timeslots with TDMA. This is the case for example in GSM.

CDMA is an access method based on the *spread spectrum* radio technology. Spread spectrum technology permits all the users of the system to transmit simultaneously to the whole available frequency band and extracts the sent message from the frequency chaos by using special operations. The idea can be compared to a restaurant where all the people are simultaneously talking different languages with approximately the same volume. First everything sounds like a pure noise, but after a short while you can distinguish discussion done with the language you understand. If somebody speaks much louder than everybody else, then nobody hears a thing...

3.3.1.2 WCDMA and NCDMA

There exist two variants of CDMA: NCDMA *(Narrowband CDMA)* and WCDMA *(wideband CDMA)*. Both are spread spectrum technologies.

Most significant of the NCDMA standards is the TIA/EIA IS-95, which has been developed by an American telecommunication company Qualcomm. The NCDMA transmission rates are roughly equal to the ones used in the other 2nd generation mobile-communication-systems (9.6 kbps etc.) and the used frequencies are situated on the frequency bands dedicated for 2nd generation mobile-communication-systems.

As mentioned earlier the final WCDMA standards are not yet ready. WCDMA technology will anyhow provide transmission rates up to 2Mbps and the used frequency bands will be situated in an area allocated for the 3rd generation mobile-communication-systems (see Chapter 2.1). Basic technology is similar in NCDMA and WCDMA systems, but the higher bit rates and the 'newness' of WCDMA brings some differences.

3.3.1.3 CDMA Transmission

The transmission of user data in CDMA technology can be divided into three phases: Modulation/demodulation, spreading/de-spreading and transmitting/receiving.

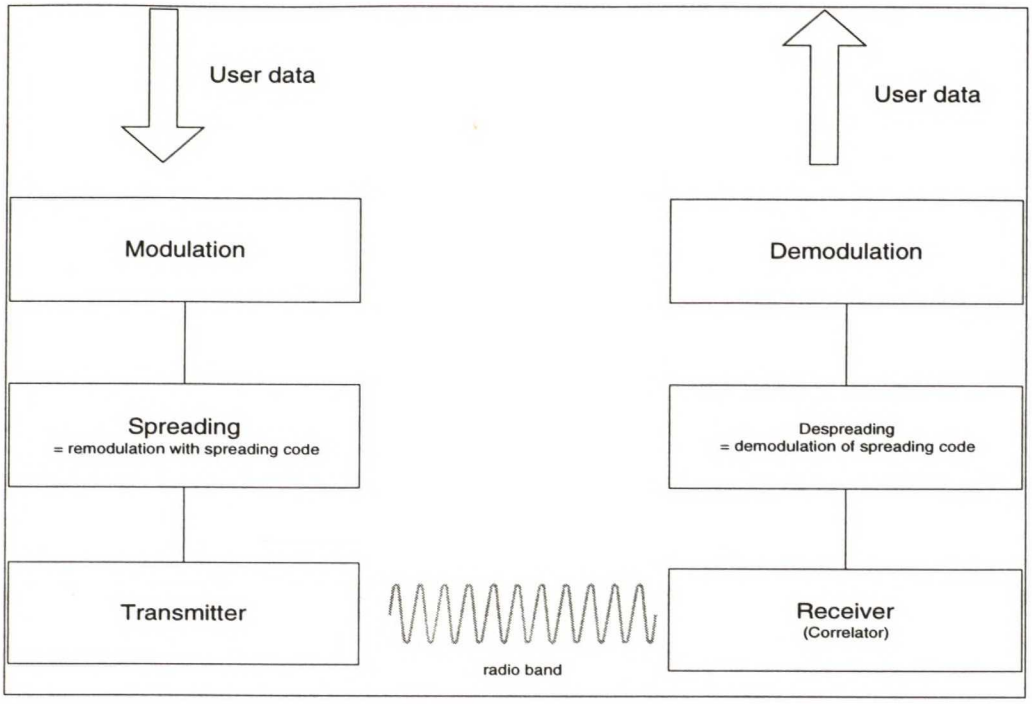


Figure 4: CDMA transmission

3.3.1.4 Modulation

A stream of bits carrying information from the user is called *user data.* Before user's data is ready to be sent, it has to be *modulated.* Modulation means conversion of the information to the form, where it is possible to send over the transmission media. An example of such is sine wave. Because the waves can have different phases, frequencies, and/or amplitudes, a wave period can include multiple bits of information. The amount is dependable on the used *modulation method.* BPSK *(Binary pulse shift keying)*, for example, includes one bit information per period and QPSK *(Quadrate pulse shift keying)* includes two bits per period.

3.3.1.5 Spreading

When the user transmits to the radio interface, the transmission requires certain amount of frequency band. Spread spectrum technology allows everybody to use the whole available frequency band. This requires that the transmission of each communicating party is be *spread* to the whole available frequency band. This reduces interference and makes it possible for multiple users to exploit the frequency

band. In reception, the power levels should be the same among all the transmitting parties.

Spreading is made with a random bit sequence called *spreading code*. Spreading can be considered as a re-modulation of the modulated user data with the spreading code. Spreading code has a two-way functionality: it is needed for the radio technical reasons, as described earlier, but it is also a unique identification of a certain user. Spreading code is a combination of two different codes: *long code* and *short code*. They are both cyclic bit sequences.

Long code is used for identification. Long code is allocated with some static method. When the transmission is done in *downlink* (from network to mobile) direction, the long code identifies the sector. When the transmission is done in *uplink* (from mobile to network) direction, the long code identifies the transmitting mobile station. Every mobile station and sector has only one long code.

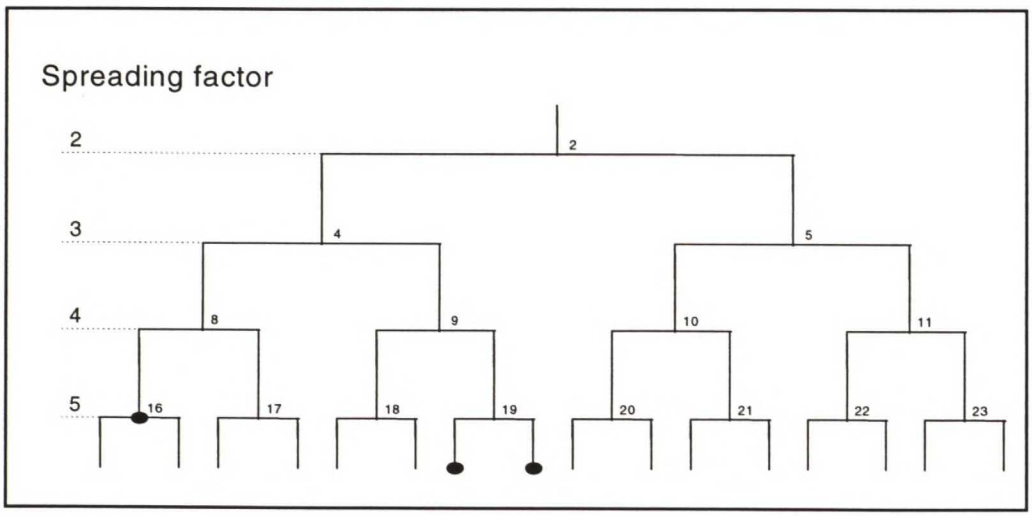


Figure 5: Short code allocation

As the name indicates, short codes are a considerably shorter than long codes. The network dynamically allocates short codes with a specific algorithm (see Figure 5). The usage of short codes is dependable on the transmission direction. In downlink direction, every sector has an own long code and short code is used to identify mobile station. When multiple calls are active to one terminal short code is also used to separate the calls. In uplink direction, every mobile station has an own long code

and short code identifies simultaneous calls from one terminal. Different types of short codes provide different amount of transfer capacity and when the transmission rate of a call is changed, quite often the short code has to be changed. This can be done in two-ways: either more efficient short code can be allocated or multiple less efficient short codes can be used for one call (=*multicode*).

Both long codes and short codes should be chosen so, that the combined codes have a good *cross-correlation* and *auto-correlation* capabilities. Auto-correlation is a measurement of similarity between a certain code and the time-shifted version of itself. Cross-correlation is a measurement of similarity between two separate codes. Auto-correlation properties are required due to *macrodiversity* for initial synchronization and combination of different signals (see Chapter 3.3.1.9). Cross-correlation properties are needed to separate codes in the reception. All short codes have to be *orthogonal*. Orthogonality means that the cross correlation is 0.

Short codes are hard to allocate due to the orthogonality requirements and length. Limited amount of possible short codes restricts the transfer capacity of the CDMA system. Opposed to the short code allocation, the long code allocation is a very easy task and there exist an almost infinite number of possible long codes. Long codes are partly used to solve the short code allocation problem. In downlink direction, which requires more codes, every sector has its own long code and because short codes and long codes are combined, every sector can reuse the short codes.

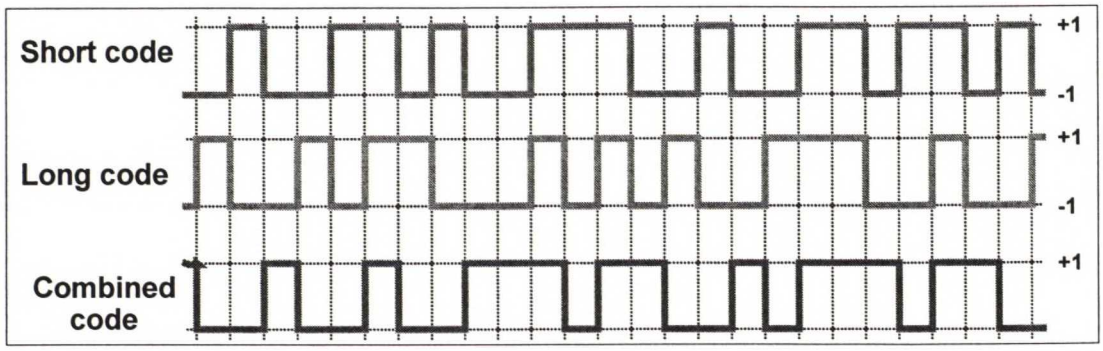


Figure 6: Combination of short and long code

It is very hard to find combined codes that would have both good auto-correlation and cross-correlation capabilities. Usually some sort of compromise has to be made. Usually cross-correlation is seen as a more favorable property.

3.3.1.6 User identification

In CDMA technology, all the transmitting parties are using the whole available frequency band, which creates huge frequency chaos. This raises a justified question about the methods for extracting a specific user's information from the frequency band. The solution lies in the correlation properties of the combined code, which is used as a 'fingerprint' for the user.

The transmitting side re-modulates modulated data with the 'fingerprint'. This 'fingerprint' spreads the data to the whole available frequency band and makes it identifiable. Due to certain procedures, the receiving sides knows the 'fingerprint' of the transmitting side and it can correlate the frequency 'chaos' and find out if the transmission modulated with the 'fingerprint' is included or not.

3.3.1.7 Chip rate

The CDMA system using a certain fixed frequency band has a constant transmission capacity. This constant transmission capacity is called *chip rate* and one capacity unit is called a *chip*. The capacity is dependable on the width of the used frequency band. When the width is for example 5 MHz, then the transmission capacity of the frequency band is 4.096 Mcps *(Mega chips per second)*. The chip rate and the user bit rate are two different things (see Chapter 3.3.1.8).

The amount of chips reserved for a short code is called *spreading factor*. Due to the orthogonality requirements of short codes, there is only a certain amount of suitable codes. Because the number of chips is constant, the capacity of the channel is dependable on the size of spreading factor. The amount of short codes can be calculated with the following equation:

$$N = 2^{SF-1}$$

Where,

N = Amount of short codes

SF = spreading factor

High spreading factor means more short codes, but the capacity per short code is lower. One short code is equal to one symbol of modulated user data, so capacity per short code is represented *symbols per second* instead of chips per second. As an example, if the spreading factor is 2 it is possible to have two simultaneous short codes, which both have the capacity of 4.096 Mcps/2 = 2.048 *Msps*. If the spreading factor is 4 it is possible to have four channels, which all have the capacity of 4.096 Mcps/4 = 1.024 Msps.

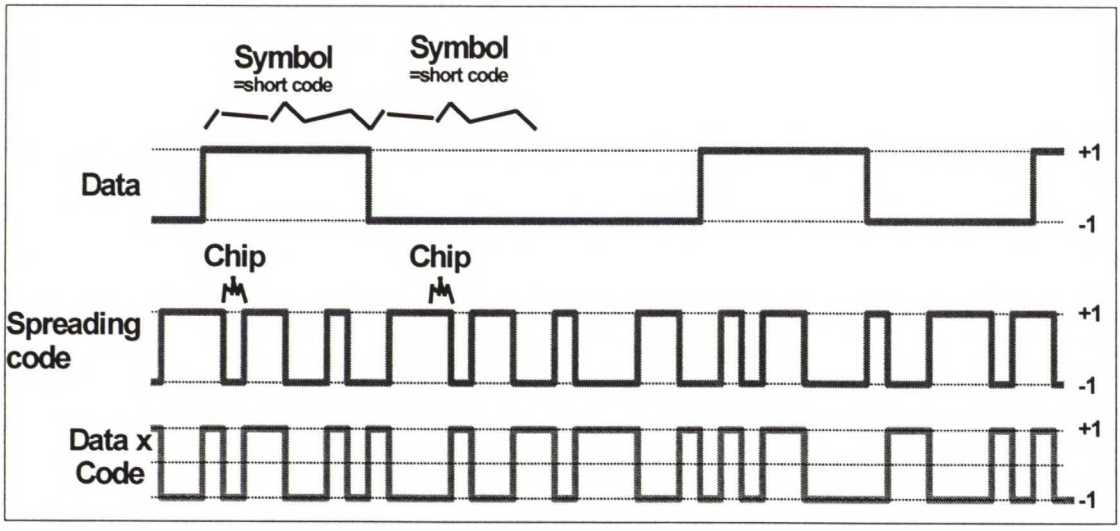


Figure 7: Spreading and chip rate

3.3.1.8 Bit rate of short code

Length of a short code is always one symbol as described earlier. This means that if the modulation method is known, the user bit rate of a short code can be calculated with the following equation:

$$R = CR / SF * N * M$$

R = User bit rate of a short code
CR= Chip rate
SF= Spreading factor
N = number of codes dedicated for a user
M = Bits per symbol

If CR = 4.096 Mcps, SF=4, N=1 and M=2 (QPSK used), then user bit rate of a short code is 2.048 Mbps.

3.3.1.9 CDMA specialties

Due to sensitivity to interference, CDMA-technology has some special problems. A transmitting mobile, which uses too much transmission power can block the whole system. This requires that the transmission power levels have to be set very sophisticatedly. This is not easy, because mobile stations require different amount of transmission power due to the different distances from the base station. This is called 'near-far' problem.

The CDMA cell range is dependent on the amount of users in the cell. When the amount of users increases, the range of cell decreases and some of the users may drop out. When the amount of users decreases, the cell range again increases and the new users are included. This is very undesirable property. It is called 'cell breathing' and it can be solved with centralized load control.

Because mobile stations and base stations in a CDMA system are using the same frequency, it is possible to transmit simultaneously through multiple base stations. This property is called *macrodiversity*. Against the 'TDMA-thinking' this is not consuming any resources, instead it improves the transmission quality. Macrodiversity makes it possible to use smaller power levels, because the received signals can be diversity combined and the transmission power of one base station can be lower.

3.3.2 Handovers of WCDMA Trial

The mobile communication system must be able to maintain the active call between the mobile station and the base station subsystem even if there is a need to change the frequencies or the base station serving the mobile station. The procedure, which makes this operation possible, is called *handover* procedure.

Handover procedures in mobile-communication-systems based on CDMA-technology differ remarkably from the ones used in mobile-communication-systems based on FDMA/TDMA technology, because the fundamentals of the radio technologies are different. Normally all the CDMA mobile stations broadcast on the same frequency. It is also possible to use different frequencies if the network planning requires this. The use of different frequencies is anyhow a totally different issue than in TDMA/FDMA -based mobile-communication-systems (like GSM), where there are multiple frequencies in each cell.

Due to macrodiversity, all the CDMA mobile stations usually transmit and receive simultaneously through multiple sectors, which may all belong to multiple BSs. The traffic is sent and received through all the sectors, but the data received only from the best sector is forwarded frame-by-frame basis to BSC. This decision is done either in the BTS or in a special unit called DHO.

The set of the sectors, which are transmitting to the mobile station and receiving from the mobile station, is called the *active set* of a mobile station. The sectors may be part of different base stations. The CDMA handover procedures modify the active set by adding and removing sectors depending on, for example, their transmission quality. There exists four types of handovers: HHO *(Hard handover)*, FHHO *(Fast hard handover),* SHO *(Soft handover),* and SoHO *(Softer handover)*. Soft handover and softer handover are often called with a common name *Diversity handover* (DHO).

Hard handover is needed when the active set has to be totally emptied due to, for example, change of frequency. Fast hard handover is similar to HHO, except that the

old MCC-SIM/BS connection is not released and it is possible to quickly toggle between new and old active set. This property is required, for example, during fast packet transmission. Softer handover is a situation, where a new sector is added into the base station, which is already existing in the active set *(intra BTS handover)*. Soft handover is a situation where such a sector is added, which belongs to a base station not previously existing in the active set *(inter BTS handover)*.

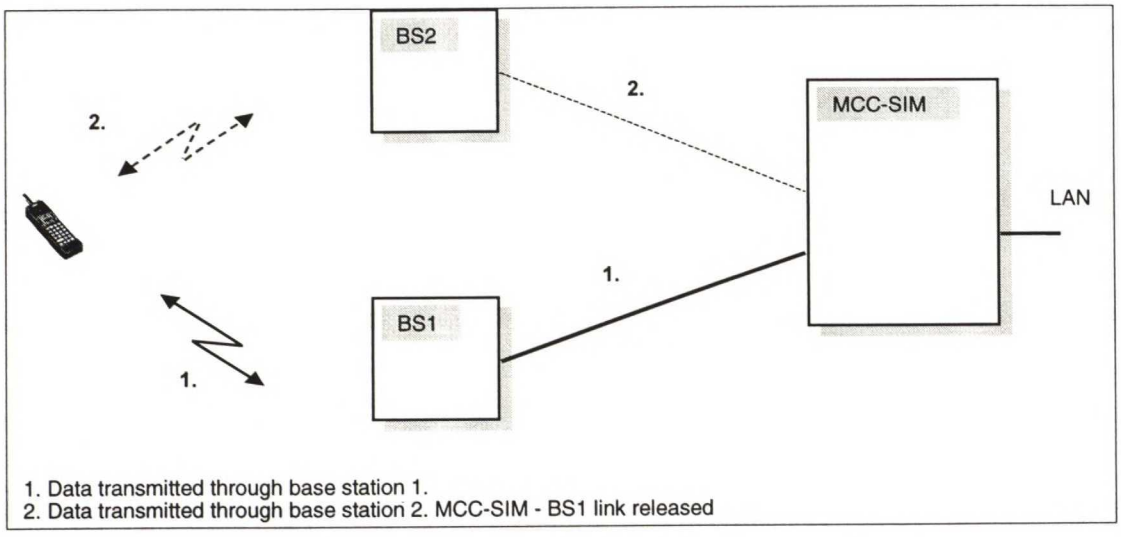


Figure 8. Hard handover

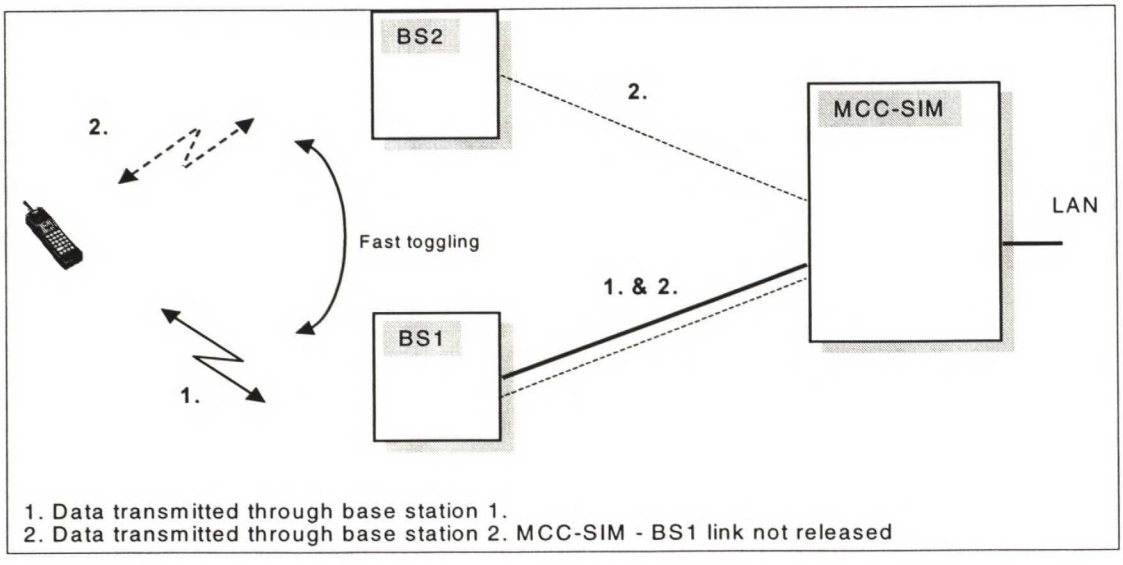
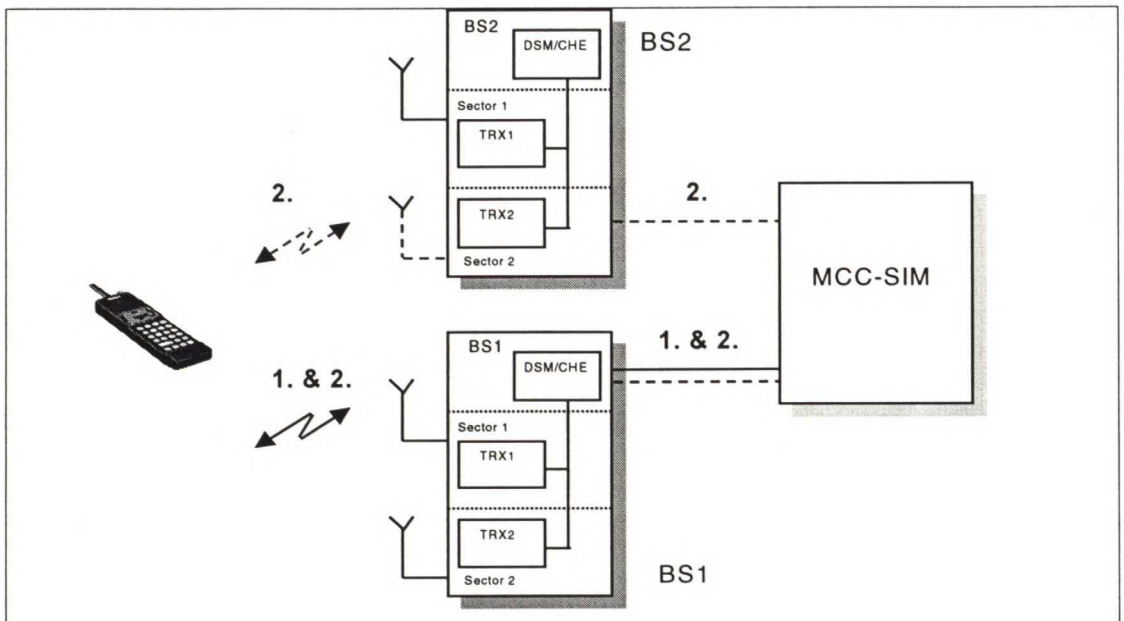


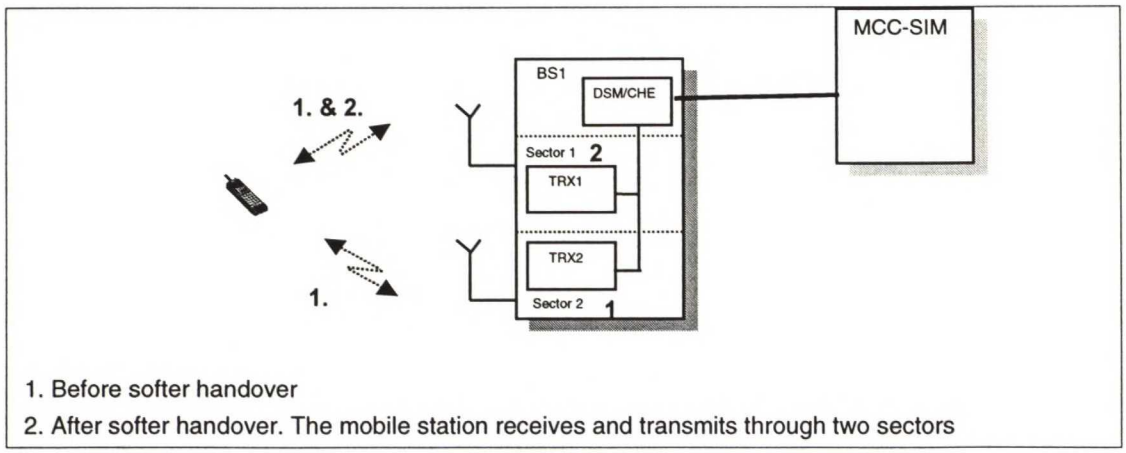
Figure 9: Fast hard handover

Diversity handover is conceptually separated to SHO and SoHO, because after Soft handover case the MCC-SIM has to route the traffic also to the new base station. The system has to actually do multicasting to all base stations of the active set. CDMA technology consumes fixed line resources quite heavily due to this reason.



1. Before soft handover. MCC-SIM routes traffic only to base station 1.
2. After soft handover. MCC-SIM routes traffic both to base station 1 and base station 2.

Figure 10: Soft handover



1. Before softer handover
2. After softer handover. The mobile station receives and transmits through two sectors

Figure 11: Softer handover

3.3.3 Radio channel structure of the WCDMA trial

3.3.3.1 Introduction

In mobile-communication-systems, an interface consists of a certain amount of radio or fixed line resources. The ITU officially defines *a channel* as "an identified portion of an interface". Then it can be said, that channel is a certain amount of resources dedicated to a certain use and collected under one identifier. Depending on the used abstraction level, we can talk about physical or logical channels.

Physical channel is a channel defined with the physical layer specific parameters like frequency, long and short code, used power level, and timing advance. *Logical channel* is a higher level abstraction for a channel and it is defined with a certain unique identifier. Certain types of procedures are usually executed in a certain logical channel. A physical channel may include multiple logical channels. The user of a logical channel usually does not know how the channel is mapped to a physical channel.

Because this representation is about higher level protocols, we focus on logical channels and skip physical channels. More information about the physical channels of the WCDMA Trial system can be found in [Do98]. The logical channels can be divided into the three categories: *common signaling channels*, *dedicated signaling channels* and *traffic channels*.

A common signaling channel transmits the signaling traffic only to one direction and it is listened by all the parties connected to it (broadcast transmission). A dedicated signaling channel transmits the signaling traffic bi-directionally between the two dedicated parties (point-to-point transmission). A traffic channel is used to transmit user data and is bi-directional.

Common signaling channels are used to establish dedicated signaling channels and to transmit information specific to all the users of a mobile-communication-system. Dedicated signaling channels are used to transmit the information dedicated to a

certain mobile station. The transfer capability in a dedicated signaling channel is considerably higher than what it is in the common signaling channel. A dedicated signaling has to be established for a traffic channel specific signaling.

Traffic channels are used to transmit user data. The user data may consist of digitized voice, circuit switched digital data or packet data. Traffic channels may have different capabilities depending on the physical layer specific parameters like used short codes etc.

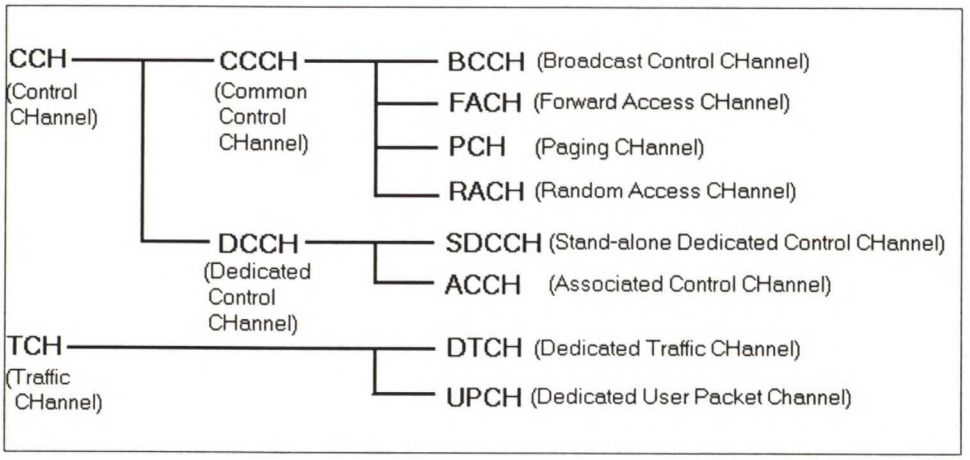


Figure 12: Logical channels of the WCDMA trial system

3.3.3.2 PCH

PCH *(Paging Channel)* is a common signaling channel and it is used to transmit so called *paging messages*, which are messages informing the mobile stations about the incoming calls, from the network to the mobile station. All the mobile stations listening to a certain BS are constantly monitoring its PCH, and if they find a paging message intended for them, they start an establishment of a dedicated signaling channel. The PCH is separated to *paging groups*. The paging group of a mobile station is calculated from the IMUI value (see Chapter 3.2.5) according to a certain formula and the mobile station is required to listen the PCH only during the time intervals specified by its paging group.

3.3.3.3 BCCH

BCCH *(Broadcast Control Channel)* is a common signaling channel used to transmit network configuration and radio transmission specific information of a BS to the listening mobile stations. When a mobile station switches to new base station, first channel it begins to monitor is the BCCH. The BCCH channel provides the required information about the short codes of the other common channels, the initial transmission power levels and the identity of the network.

3.3.3.4 RACH + FACH

As described earlier the PCH is used to transmit paging messages and the BCCH is used to transmit information about the network configuration. These channels can only be used to transmit information from the network to the mobile station. There exists anyhow a need for bi-directional and more generic common signaling channels. The two special common signaling channels dedicated for this purpose are RACH *(Random Access Channel)* and FACH *(Forward Access control channel)*.

RACH is used to transport messages from the mobile station to the network and FACH is used to transport messages from the network to the mobile station. Maybe the most common signaling situation is the establishment of a SDCCH channel (see Chapter 3.3.3.5). The RACH + FACH combination has also a special use in the packet data transmission. If there is a small amount of packet data to be sent, the RACH and FACH channels are used instead of the dedicated packet channel UPCH (see Chapter 3.3.3.8).

3.3.3.5 SDCCH

The capacity of a common signaling channel is limited, so there is a need to establish a dedicated signaling channel as soon as possible. The dedicated signaling channel that is established by using the common channel signaling (RACH+FACH) is called SDCCH *(Stand-alone Dedicated Control CHannel)*. SDCCH is used as long as there is no traffic channel. After the traffic channel allocation, the signaling of a call is switched to ACCH (see Chapter 3.3.3.6) and the SDCCH is released. There exists

some signaling situations, where a traffic channel is not established. This kind of situation is for example the location update. In those cases, the signaling channel is the SDCCH during the whole procedure.

3.3.3.6 ACCH

ACCH *(Associated Control CHannel)* is a dedicated signaling channel, which is established simultaneously with the traffic channel. ACCH and the traffic channel are multiplexed to use the same physical channel. ACCH is used to carry all the call specific signaling, while the traffic channel is active. In the multicall situation, it is possible to use one ACCH channel for the several traffic channels.

3.3.3.7 DTCH

DTCH *(Dedicated traffic channel)* is a traffic channel used to transmit all types of user data except packet data. Data can consist of digitized voice, open digital data etc. There exist multiple types of DTCHs depending on their transmission capacity. The capacity is depending on the used short code (see Chapter 3.3.1.5). It is also possible to combine several short codes for establishing a very fast transmission channel. As described in the previous Chapter, signaling channel for DTCH is ACCH and it is multiplexed to be a part of DTCH.

3.3.3.8 UPCH

UPCH *(User packet channel)* is used to transmit user packet traffic in those cases where the FACH and the RACH does not have an adequate capacity. The UPCH is established similarly than the DTCH and it uses the ACCH for signaling. The WCDMA-trial specification for a packet data transmission is not yet completely finished and in the first version, UPCH is similar to DTCH except that it carries packet data. This is against the connectionless nature of the packet data. It is very likely, that the future specifications will have a something more sophisticated.

3.3.4 Bearer

The mobile-communication-systems must be able to transmit many types of traffic: normal voice traffic, different type of open digital traffic, and packet data traffic. The different traffic types require a different amount of transfer capacity and this creates demand for different types of physical radio channels. The network level radio transfer connection between the mobile station and the network is called as a *radio bearer*. In the CDMA-based mobile communication systems, the transfer capacity of the radio bearer is depending on the type and the amount of the short codes reserved for a single connection.

3.3.5 The identifiers of WCDMA trial system

Traditionally mobile-communication-systems have required a different type of numbering system, than what is used in the fixed-line communication systems. In addition to the subscriber identification, the mobile communication system needs many internal numbers for providing the mobility, the security aspects etc.

The WCDMA trial specification has very limited roaming and subscriber management capabilities, because the MSC-to-MSC interfaces are not specified and the system is intended to experimental use. This is also seen in the numbering. Many of the internal identifiers familiar from GSM are missing. Only the basic ones are included.

The IMUI *(International Mobile User Identity)* is equal to the GSM IMSI *(International mobile subscriber identity)*. It is a 15-digit unique identifier of a mobile user, including also the country and network identifiers.

The TMUI *(Temporary mobile user identity)* is equal to the GSM TMSI *(Temporary mobile subscriber identity)*. It is a 32-bit identifier, which is allocated by the MSC and used instead of the IMUI for providing identity protection for the user. Except

the error situations, after the initial location update the TMUI is always used in the signaling messages instead of the IMUI.

The TMUI assignment source id is a 6-octet identifier including the country code, the network code, and the location area identifier of a mobile user. It is used in the location update for informing the used location area and identifying the MSC, which allocated the used TMUI.

The RBC-id *(Radio Bearer Control identifier)* is one-octet identifier used by the radio resource control and the call control. It identifies the logical channel of a call. The logical channel may consist of multiple different types of bearer combinations and the RBC-id makes it possible to handle this group with single identifier.

3.4 Technical data

This Chapter describes some of the key technical characteristics of the WCDMA trial system. Some liberties have been taken for choosing the parameters, which are essential to this representation. The parameters are divided to two groups: general and radio technical [Do98].

GENERAL PARAMETERS:

Maximum transfer rate (air interface)	384 Kbps
Services provided	- Voice service - Open digital - Packet communication
Maximum number of calls to one MS	2
Maximum number of simultaneous calls	6

RADIO TECHNICAL PARAMETERS:

Radio access method	Direct sequence CDMA FDD
Frequency	2 GHz band (3rd generation band)
Carrier frequency interval	5 MHz
Chip rate	4.096 Mcps (chips per second)
Number of carriers	4
Symbol rate	32 to 256 ksps

4. A WIDEBAND CODE DIVISION MULTIPLE ACCESS TRIAL SIGNALING SPECIFICATION

4.1 General

The WCDMA trial specification is a mobile-communication-system specification designed for gaining experience about the WCDMA radio access technology. The specification describes interfaces between different system components. The control plane protocol stack of the specification can be seen from figure 13.

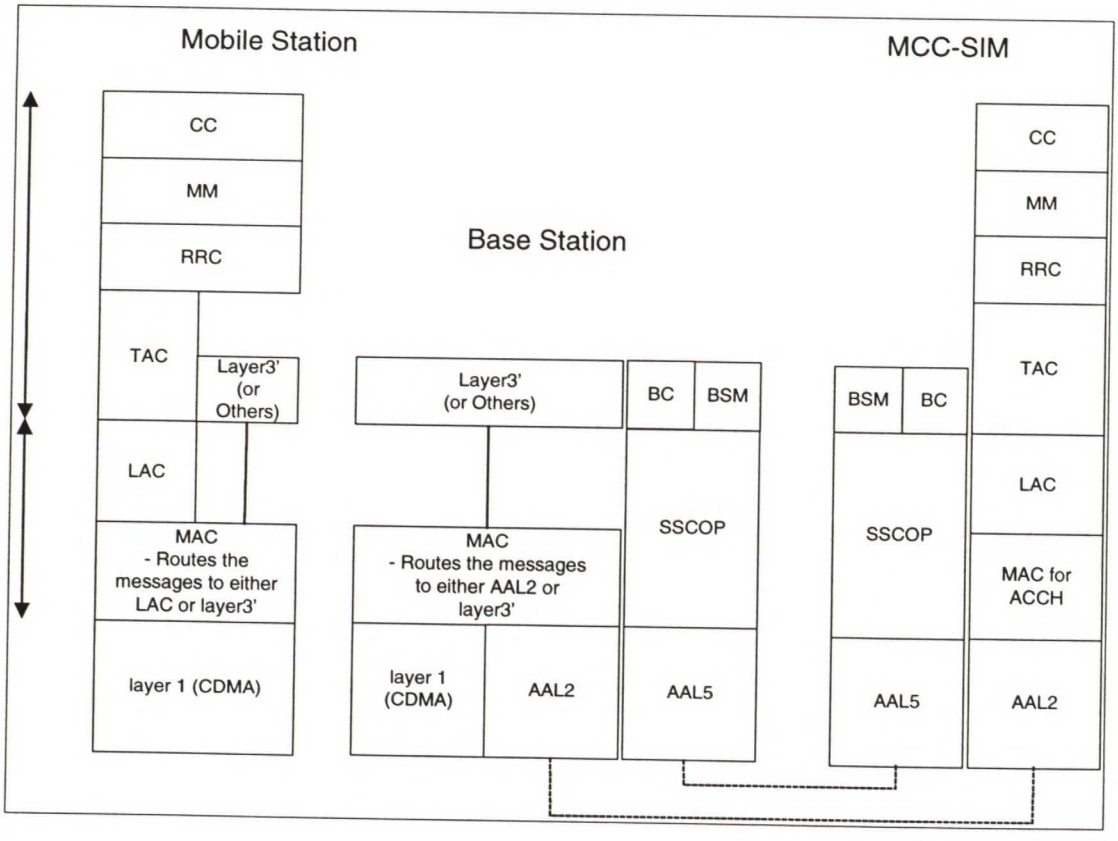


Figure 13: The signaling protocol stack of the WCDMA trial specification

The specification is not yet completely finished. The system is operational, but the management of network faults and the special situations occurring in the commercial networks under major load are left out. Furthermore, the specification does not include any MSC-to-MSC interfaces (MAP-protocols in GSM) and hence this is a

closed system. The specification should be considered as a draft, which will be a base for the more sophisticated future specifications.

This presentation describes only the layer-3 protocols of the WCDMA Trial specification and among the layer-3 protocols only those, that are needed in the air interface. The interface between the BS and the BSC, which is called *Abis* in the GSM terminology, is left out. This is due to fact that the tester implemented in this master's thesis is a mobile station tester and the abis interface is not visible to the mobile station. The lower layer protocols, like the LAC (layer-2), were left out for keeping the length of presentation reasonable. All the control plane layer-3 air interface messages are listed in Appendix A.

In this presentation the terms MTC *(Mobile Terminated Call)* and MOC *(Mobile Originated Call)* are used. MTC is a situation, where someone is calling to the user of the mobile station (incoming call). MOC is a situation, where the user of the mobile station is calling someone (outgoing call). This Chapter is based on [MB92] and [Do98].

4.2 Call Control

4.2.1 Introduction

Before the called and the calling user can communicate, some kind of end to end signaling must take place. The quality requirements, the bearer capabilities, and the transfer rates of the connection must be negotiated. The called user must also be informed about the incoming call. When the call is successfully established, there must be some means to change its properties like the type of sent information (data, voice etc.) and inform the system about the changes. After the users have released the call, the used resources must be released. In the case of multicall, where a multiple connections exist to a terminal, the establishment and the release of the simultaneous connections must be handled.

Traditionally in mobile-communication-systems, these procedures are considered as a part of the communication management, which includes a protocol called CC *(Call Control)*-protocol. The communication management is a task of the MSC and in addition to what was said previously, it includes also other call management related procedures. These are for example routing, call transfers and handling of connections to external networks. It is obvious that, these are complicated tasks with a many possible exceptional cases. This is the reason why for example in GSM the communication management specific program blocks are very extensive.

The WCDMA trial specification is intended to be a description of an experimental system instead of a commercial one. This is the reason why many of the exceptional situations occurring in the communication management could have been left out and the communication management consists mainly from the CC-protocol.

The CC-protocol only includes few things specific to mobile communication systems. These are the management of the radio bearer properties and the internetworking functions. The CC is implemented according to the corresponding fixed-line-communication-system specifications. For example, the GSM CC is very

close to the narrowband ISDN CC (*Integrated Services Digital Network)* and the WCDMA trial specification CC is based on the broadband ISDN CC.

In the early versions of WCDMA trial CC specification, there were very many information elements for a single message. Most of information elements were different than the ones used in the ISDN CC specifications. This was due to the intentions for implementing a complicated internetworking to the various types of fixed line communication systems. The recent specification versions have anyhow left these elements out and the current CC is quite close to ISDN CC.

4.2.2 Call establishment

The call establishment procedures are similar both in MTC and MOC. This is the reason why they are described simultaneously.

The signaling is initiated by sending the SETUP-message on the SDCCH channel to the called user. The message includes the information about the required radio resources and protocols, transfer rates, and ATM specific Quality-of-Service requirements. In addition, the calling and called user identification information is (naturally) included. The SETUP-message can include information about multiple bearers and information transfer rates.

The call establishment procedure continues with the CALL PROCEEDING – message, which confirms, that the SETUP-message has been received and that a call establishment procedure towards the called user is ongoing. If multiple bearer information elements and information transfer rate elements were sent in the SETUP message and only one type of bearer and rate is supported by the called user, then this message includes information about that bearer and rate. If there is a multiple possibilities, then the bearer and the rate is negotiated by using the CONNECT-message.

When the mobile station of the called user is alerting, the calling user is informed with the ALERTING-message. This message contains no bearer specific information

elements. Before the ALERTING-message was sent, a traffic channel was established and the dedicated signaling channel was switched from the SDCCH to the ACCH.

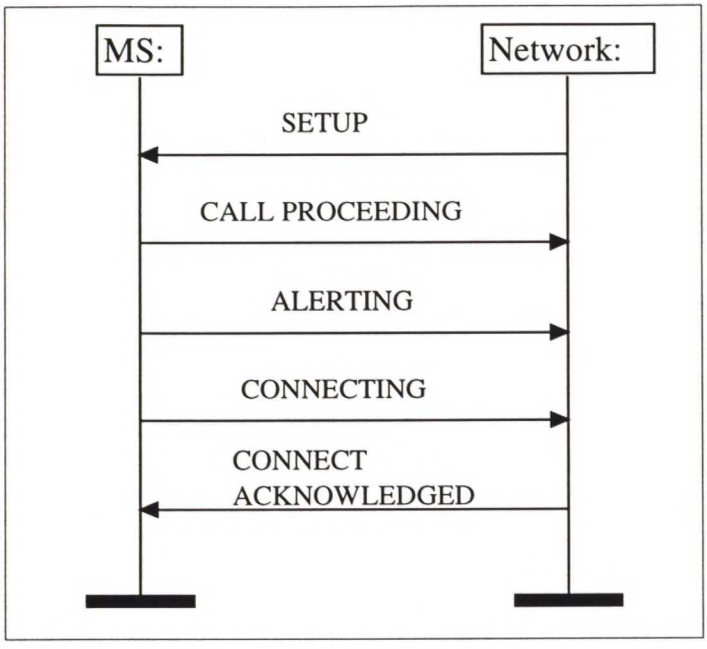


Figure 14: CC signaling for call establishment

After the called user has answered the call, the calling user is informed with the CONNECT-message. This message includes the mobile bearer and transfer rate information if this was not previously sent in the CALL PROCEEDING-message.

The calling user confirms the established call by sending a CONNECT ACKNOWLEDGE-message. This is, like the ALERTING-message, a pure signaling message and includes no bearer specific information elements.

4.2.3 Call release

Either the called or the calling user, depending on which side hangs up the line first, initiates the releasing procedure. The releasing procedure may also be initiated automatically by the network in a different type of error situations. Such cases are for example problems in the bearer negotiations or in the connection management.

The releasing is initiated with a RELEASE-message. After reception of this message the receiving side responds by sending a RELEASE COMPLETE message and CC – connection is now released.

The RELEASE-message has an information element, which includes the cause of the release. The RELEASE COMPLETE-message can also have a corresponding field, which is used in a situation where the RELEASE COMPLETE-message has been the initial release message. This type of procedure may occur during some error situations.

4.2.4 Multicall handling

The WCDMA trial specification offers a possibility to have a multiple simultaneous calls to a mobile station. The WCDMA multicall feature is different than the conference call feature of 2nd generation mobile-communications-systems, since every call has an own radio bearer. This makes possible, for example, a simultaneous voice and data calls to the same mobile station. Every call has an own traffic channel, but the used ACCH signaling channel is shared. Only a single voice call is allowed at a time.

The multicall feature involves two protocol entities: CC and RRC (*Radio resource Control)*. The RRC has the most complicated task, since it has to route the signaling of all the traffic channels to a dedicated signaling channel and to handle the multicall handovers. Task of the CC is easier. It has to find out, if the call is initiated to a mobile station, which already has a call ongoing and in such a case initiate the

multicall specific signaling. The multicall specific CC-signaling is similar to the CC-signaling of a normal call, except to some minor differences in the contents of the information elements. The SDCCH is also not established, because the ACCH is already active and it can be used to transmit all the signaling traffic. This includes also SETUP and CALL PROCEEDING -messages. In the multicall situation, the release of a CC-connection is done similarly than the release of a CC-connection during normal call.

In the whole signaling of a call, the most significant differences between the multicall specific signaling and the signaling of a normal call are on the RRC and common channel protocols. This is due to fact, that the SDCCH is not established and that in the MTC paging is not required. By using the RBC-id, the RRC can hide the complexity of the multicall bearers quite efficiently.

4.3 Mobility Management

4.3.1 Introduction

One of the main differences between fixed networks and mobile networks is the concept of user mobility. In mobile networks, the user can be located anywhere in the home network or possibly in the other operator's network if there is a roaming agreement. This property creates a group of problems.

A mobile-communication-system must have methods for locating the user when this is requested. Such requests are made, for example, during every MTC. For providing this property, the mobile-communication-system must maintain some type of database, where the user location information can be requested.

Theoretically, mobile network can be accessed by anyone who has a correct type of terminal. Because only the paying users are the good users, there must be a method for assuring that the user is the one who he claims to be and she/he is allowed to use the network. In other words, the user has to be authenticated. This procedure is not needed in the fixed networks, where the authentication is based on to a specified cable connection. Everybody who has an access to the cable connection is an authorized user from the fixed network point of view. This point of view may differ from the point of view of the user who pays the bills of the cable connection.

Mobile-communication-systems can be accessed from any geographical location inside the network's coverage area. Because the radio transmission can be received by anyone who uses a correct frequency, there is a risk of eavesdropping. If the mobile networks should have the same service level than the fixed networks, which has been the idea already on 2nd generation mobile-communication-systems, then some procedure must exist for providing the confidentiality. A solution to this problem is the use of ciphering.

A part of confidentiality is the user privacy management. The traffic and signaling channels are both ciphered, but still there is a slight possibility that the identity of a

user could be revealed. Inside a mobile network, the user is identified, with the IMUI value. If an eavesdropper finds out the IMUI, he knows the identity of the user. Due to this, the transmission of the IMUI over the unreliable radio interface is limited to a minimum and the TMUI is used instead. The management of TMUI values is the most important task of the privacy management.

The protocol designed to handle the user mobility and the mobility-originated problems is typically called MM *(mobility management)*. In GSM, the mobility management includes the MM-protocol and a lot of external functions. Reason for this is mainly the considerable amount of exceptional cases that may occur in the network. As the name states, the WCDMA trial system is not intended to be a commercial system, so it does not have to handle all the possible error situations. This is the reason why the WCDMA mobility management has only a few functions in addition to the MM protocol. The WCDMA mobility management also does not have the actual ciphering and authentication algorithms. The corresponding messages are included in the MM-protocol and they are sent according to the correct procedure, but the contents of the messages are not used.

The mobility management in GSM also includes a multiple operations between the MSCs, which use so called MAP-protocols. The WCDMA trial specification does not specify the MSC-to-MSC interfaces, which makes the WCDMA trial mobility management even simpler.

4.3.2 Message structure

The WCDMA trial MM-protocol has gone through remarkable changes between the different specification versions. The first draft specification requested that the MM-protocol should be implemented by using the OSI ROSE-protocol *(Open System Interconnection Remote Operation Service Element)* [ISO13712]. The ASN.1 *(Abstract Syntax Notation One)* definitions were not included, but the external representation of messages was similar to the BER (*Basic Encoding Rules*), which is the most common ASN.1 encoding rule [X690]. Later versions removed the BER-based representation of messages and changed the external representation to use the

encoding rules defined by NTT/DoCoMo. In this new solution, some features of ROSE were anyhow left and this new solution was called a 'slimmed ROSE'.

Due to the ROSE origin, the MM has only one message, which is called the MOBILITY FACILITY. This message has five *operations*: TERMINAL LOCATION REGISTRATION, AUTHENTICATION CHALLENGE, START CIPHERING, TMUI ASSIGNMENT and IMUI RETRIEVAL. The specification status of the last operation is still unclear. It has a very logical use but in the latest specification version (version 1.12), it was removed. It is possible, that in the future implementations it will return.

Every operation has four *primitives: Invoke, Return Result, Return Error,* and *Reject.* The execution of an operation is requested with invoke-ROSE-primitive and the result is sent with return-result-ROSE-primitive. When compared to the standard service primitives, invoke-ROSE-primitive is equal to the request-primitive and return-result-ROSE-primitive is equal to the response-primitive. The Error and Reject-ROSE-primitives are used in a different type of error situations. They are explained in the Chapter 4.3.6.

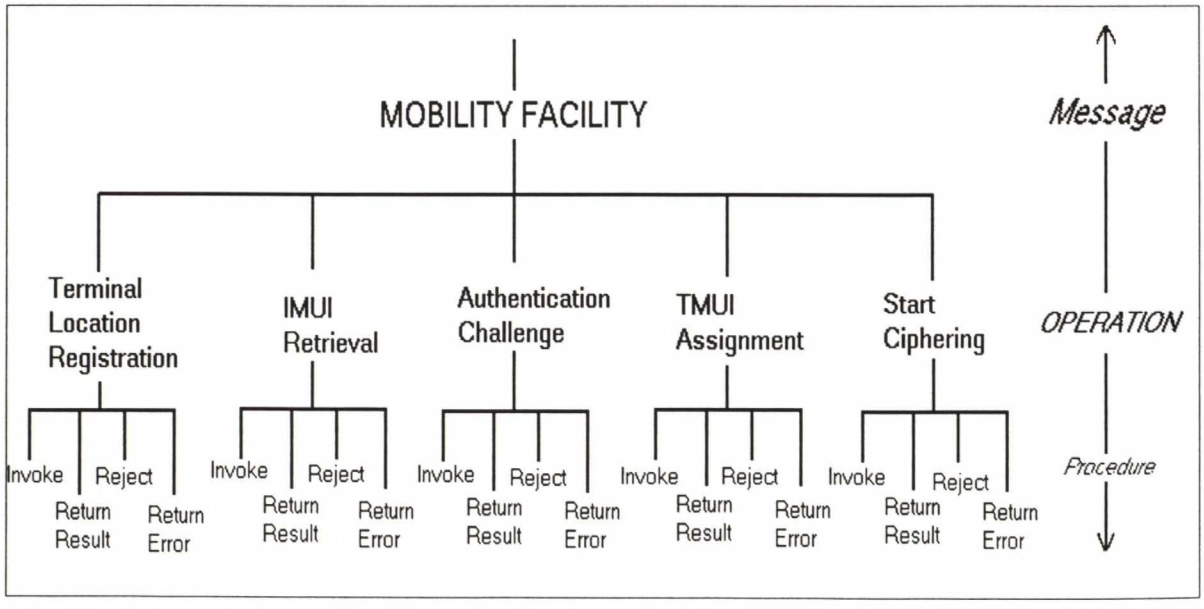


Figure 15: MM message structure

The use of this type of message structure creates some problems in message decoding. Instead of a single message identifier field, three fields are needed. First field identifies a message, second an operation and third a primitive. Three octets are needed to carry the information of one.

Due to the ROSE origin every message has an *'invoke identifier'* -field, which is used as an operation identity in the case of multiple simultaneous invokes of the same operation type. This field is not needed in all implementation environments, since the system can separate simultaneous invokes with some specific routing mechanisms.

4.3.3 Location management

The location update operation is executed, when the mobile station is initially registered to the network or when the location area of the mobile station changes. The mobile station constantly listens to the location area information, which is broadcasted on BCCH. When it realizes, that the location area is changed, the mobile station executes a location update procedure.

The signaling required by location update procedure is initiated when the mobile station sends MOBILITY FACILITY - TERMINAL LOCATION REGISTRATION – Invoke message. The message contains the user identifier and optionally the mobile station characteristics, which are coded to a special structure called *TC-info*. The user identifier is IMUI, when the message is sent for first time, and TMUI + TMUI assignment source id after that. The specification does not say, when the TC-info structure should be included, but very likely it should be sent with the IMUI in the initial location update. This way the initial location update message would work in a similar way than the TAC-messages used as initial messages (see Chapter 4.6).

Opposite to what could be expected, it is not a task of MM to provide the actual user information. Instead, it provides a pointer to the place where the user data can be fetched and maintains the validity of this pointer. The IMUI identifies the user's HLR (*Home Location Register*) and provides an index to be used inside HLR. The

TMUI is an index to the user data inside a VLR (*Visitor Location Register*). The TMUI-assignment-source-id is for situations where the VLR changes between the location updates. It identifies the VLR that allocated the used TMUI value. When the network receives the location update message, it first checks from the TMUI-assignment-source-id is the TMUI value allocated by it or should the data be fetched from some other VLR.

When the user data is found and the required authentication and ciphering procedures have been done, the location update procedure is terminated. The mobile network responds to the mobile station by sending a MOBILITY FACILITY - TERMINAL LOCATION REGISTRATION - Return Result message. The location update is complete.

4.3.4 Authentication and ciphering management

Before the subscriber is allowed to use the mobile network she/he must be authenticated and ciphering must be started. The specification of authentication and ciphering procedures is incomplete in the current specification versions. The authentication and ciphering messages exist, and they include logical information elements. The usage of the information elements is anyhow completely unspecified.

The GSM authentication is based on to a comparison of two values calculated independently by both the mobile station and the network. The authentication algorithm is called A3. The authentication procedure is straightforward. The network sends a random number called RAND to the mobile station, which calculates value by using the RAND and an authentication key. The result, which is called SRES, is sent to the network, which also calculates SRES. If the results match, then the user is authenticated.

The specified authentication messages and the used information elements are quite similar both in the GSM specification and in the WCDMA Trial specification. In the WCDMA trial, the authentication is initiated by network, which sends a MOBILITY FACILITY - AUTHENTICATION CHALLENGE – Invoke message. The message

contains an information element called *Authentication random pattern.* This could be similar to RAND. The mobile station responds by sending a MOBILITY FACILITY –AUTHENTICATION CHALLENGE - Return result. This message includes only one information element called *Authentication calculation result.* This information element is very similar than the SRES.

The GSM ciphering is initiated with message RR CIPHERING MODE COMMAND, which includes an identifier of the used algorithm. The information is needed because the specification provides a possibility to use multiple algorithms. The most common GSM ciphering algorithm is called A5. The A5 takes frame number and a special ciphering key called k_c as input and outputs a bit sequence, which is then combined with the traffic stream.

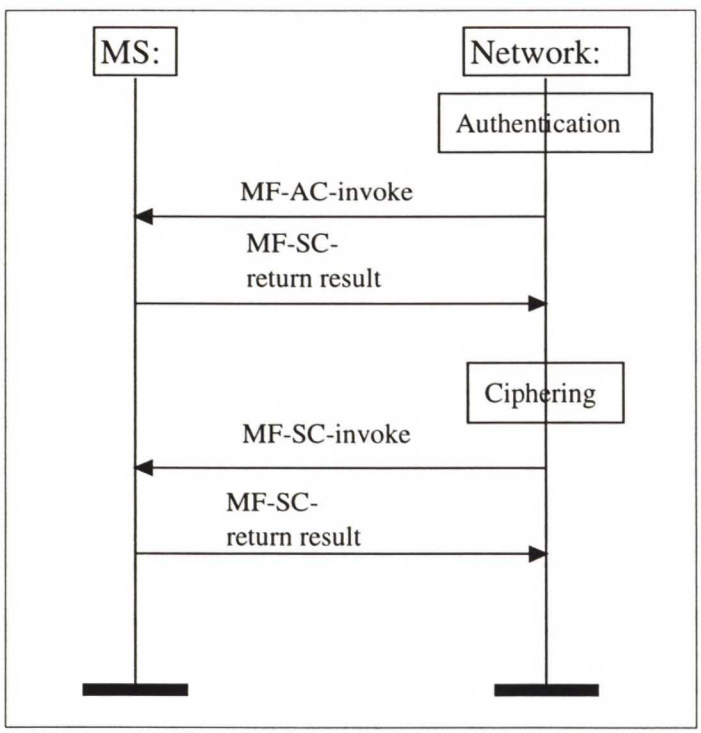


Figure 16: MM authentication and ciphering

In the WCDMA Trial specification, the ciphering is initiated similarly than in GSM. The network sends a MOBILITY FACILITY – START CIPHERING – Invoke message, which contains an information element called *Execution ciphering pattern for signaling channel.* This information element includes the information about which ciphering algorithm should be used if the mobile station supports multiple

ciphering algorithms. Currently this means just ciphering or not ciphering, but the information element has 7 bits reserved for the future extensions. The mobile station responds by sending a MOBILITY FACILITY – START CIPHERING – Return Result message and ciphering is activated. This message does not contain any information elements.

When comparing the ciphering procedures of GSM and the WCDMA trial specification, a noticeable difference is the location of the message, which initiates the ciphering. In GSM, it is a RR message, but in the WCDMA Trial, it is a MM message. Due to this new location, it could be possible that the ciphering in the WCDMA trial is used between the mobile station and the MSC. In GSM, the ciphering is used only in the air interface.

4.3.5 Identity privacy management

After the initial location update, the identification of a mobile station should always be done with TMUI instead of IMUI. The TMUI is allocated by the VLR, where the mobile station is currently registered. If the VLR changes, the new VLR should be able to allocate the new TMUI without requesting IMUI from the mobile station. This is possible with the internal network operations.

Due to security reasons, TMUI should be reallocated time to time. The specification keeps this as an implementation specific matter. Only required thing is, that TMUI should be reallocated after every location update. The reallocation is done by the network, which executes the operation by sending a MOBILITY FACILITY – TMUI ASSIGNMENT – Invoke message. The mobile station confirms the new TMUI value by sending a MOBILITY FACILITY – TMUI ASSIGNMENT – Return Result message.

In some error situations, the network and the mobile station may have different TMUI value and the mobile station can not be identified. The network can request the IMUI value of the mobile station by sending a MOBILITY FACILITY – IMUI RETRIEVAL – Invoke message. The mobile station responds by sending IMUI in a

MOBILITY – IMUI RETRIEVAL – Return Result message. After the user identification, the TMUI is reallocated with the TMUI reallocation procedure.

4.3.6 Error handling

The management of the different exceptional situations is usually the most complicated phase of protocol design. Due to the ROSE origin, the Mobility Management protocol has relatively large set of error messages. Every operation has two different error primitives: *Return Error and Reject.* For example, the TERMINAL LOCATION REGISTRATION specific error messages are the MOBILITY FACILITY – TERMINAL LOCATION REGISTRATION – Reject and the MOBILITY FACILITY - TERMINAL LOCATION REGISTRATION – Return Error. A reject primitive is used, when a non-system-based error has occurred. This is the case, when there are for example an unmatched information element. A Return Error primitive is used, when there are system-based errors like application errors etc. The Reject is less critical than the Return Error, which creates a situation where the active calls of the mobile station have to be released.

Due to the lower layers, it should not be possible for a message to disappear without the sending protocol layer to be informed about it. It may anyhow be possible that the peer entity for some reason does not understand the received message. There are two possibilities in this situation: the peer entity does not send anything back or the peer entity sends a Reject or Return Error message.

The first case is handled by using the timers. When a message is sent, the sender starts a timer and if the answer does not come within a certain time, a retransmission is done. The retransmission is done 10 times, and if the correct answer is still not received, the call is released.

The second case is similar than the first if a Reject message is received. After ten consecutive Reject-messages, the call is released. The protocol stack is released immediately, if a Return Error –primitive is received in any phase.

4.4 Radio Resource Control

4.4.1 Introduction

One of the most important things in a mobile-communication-system is the management of radio resources. Due to the new WCDMA radio technology, the radio resource management has come even more complicated than in 2nd generation-mobile-communication-systems. Macrodiversity, multicall, multiple bearers, and several types of fast power control and handover algorithms demand a lot of new features. It can be said that most of the changes between 2nd generation-mobile-communication-systems and 3rd-generation-mobile-communication-systems will be in the radio resource management.

The radio resource management in WCDMA trial system is done by a protocol called RRC *(Radio Resource Control)*. The RRC operates together with the common channel signaling protocols. The RRC does not have very many messages, actually only eight, but they include a great variety of information elements and one message is used in multiple situations.

4.4.2 RRC Signaling channels

RRC-protocol does not use the common signaling channels and hence for each RRC signaling session, a dedicated signaling channel must be established. This can be either ACCH or SDCCH. ACCH is used during active call and SDCCH otherwise.

The establishment of SDCCH is done with the Common channel signaling protocols (see Chapter 4.5.3). The establishment of ACCH is done during the DTCH/UPCH establishment, since ACCH uses the same physical channel than DTCH/UPCH. When the ACCH is in use, then the SDCCH will be released and instead of the Common channel protocols, this is done with the RRC-protocol. Usually it is done as a last phase of call establishment. In some cases, the SDCCH release can also be done locally and no messages are needed.

The release of the SDCCH signaling channel is done with three RRC messages. Releasing is initiated by the network, which sends a SDCCH RELEASE message to the mobile station. The mobile station releases the resources and confirms the release by sending a SDCCH RELEASE COMPLETE message, which is the last message sent in the SDCCH channel. When the network receives the message, all the remaining SDCCH resources are released.

The internal release of SDCCH is used in MTC and MOC. When the SDCCH is no more needed, both the network and the mobile station release the channel locally and no specific release messages are needed.

4.4.3 Radio bearer management

The radio bearer management consists of initialization, maintaining, and allocation of radio bearers. A radio bearer provides a certain transfer rate. All the different transfer rates require a different type of short codes and some rates may even require multiple short codes.

The radio bearer establishment signaling is rather straightforward. The network must have information about the radio environment of the active set before it can allocate a new bearer. The mobile station sends the information in an ACCESS RADIO LINK FACILITY message with *Origination/termination-candidate-zone-assignment* -information element. The network performs an internal bearer allocation (BTS/BSC-interface etc.) and sends an ACCESS RADIO LINK SETUP -message to the mobile station including the short codes of a bearer. The mobile station does required initializations and establishes a bearer. The radio bearer is ready.

It is possible to change the properties of a radio bearer during the connection by sending an ACCESS RADIO LINK FACILITY- messages with *code-alternation-set, bearer-integration-cancel-set* ,and *bearer-integration-set* -information elements. New type of short codes can be allocated, short codes can be changed, and multiple bearers can be combined to use one short code. This message is bi-directional, so

both the mobile station and the network can change the properties of a bearer if required. The network anyhow always does the final allocation decision.

When the bearer is no more needed, the network releases the connection by sending an ACCESS RADIO LINK RELEASE - message to the mobile station. The mobile station releases the bearer and sends an ACCESS RADIO LINK RELEASE COMPLETE -message to the network. Remaining network side connections (BTS/BSC interface) are released by using the internal signaling of the network.

4.4.4 Handovers

The handover specific signaling is done with two messages, which both have different types of information elements. The signaling can be done either separately during the call or it can be part of the call establishment phase. The handover requests can include requests for deletion of a sector and/or addition of a sector from/to active set. Multiple sectors can be added or removed with a single message, which makes it possible, for example, to initiate the SHO and the SoHO simultaneously.

The addition of a sector is always suggested by the mobile station, but confirmed by the network. This is due to the fact, that only the network is aware of available resources. Either the mobile station or the network can do the deletion of a sector, but the opposite side must be informed about this matter. The negative addition decision is not signaled to the mobile station, but the negative deletion decision has to be signaled to the opposite side for keeping the both sides consistent.

All the handover signaling during a call is done with an ACCESS RADIO LINK FACILITY -message. Different handover cases have different information elements. When the handover consist of addition, the mobile station sends either *DHO-additional-candidate-zone-assignment* -information element for suggesting a DHO or *HHO-candidate-zone-assignment* –information element for suggesting an HHO. The sent information elements include measurement information about the current active set and the suggested new active set members. The values are given to a special

handover algorithm, which does the final decision. If a positive handover decision is made, the network responds with an ACCESS RADIO LINK FACILITY –message. If the handover type is DHO a *DHO-addition-setting* –information element is included. In the case of HHO, an *HHO-set* -information element is included. The mobile station does the required modifications to the active set and if the handover type was DHO, it sends the confirmation with a *DHO-additions-setting-respond* – information element. The HHO is not confirmed with the RRC signaling, instead the layer1-signaling is used.

During a call establishment phase, it is also possible to do an instant handover by sending a *DHO-addition-setting* or a *DHO-deletion-setting* –information element in the ACCESS RADIO LINK SETUP-message. The mobile station informs the network about the success of the handover with an ACCESS RADIO LINK SETUP RESPONSE –message including a *DHO-addition-setting-response* and/or a *DHO-deletion-setting-response* –information element.

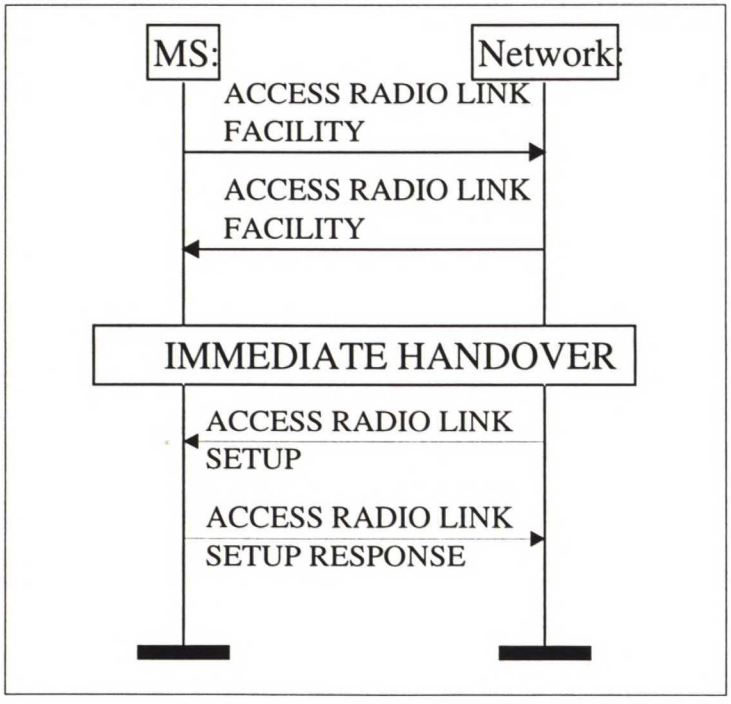


Figure 17: Handover signaling of RRC

As mentioned earlier it is also possible to remove sectors from the active set. The used message is ACCESS RADIO LINK FACILITY. When the mobile station does the deletion a *DHO-deletion-notification* –information element is sent and the network responds with a *DHO-deletion-notification-response* –information element. If the network does the deletion a *DHO-deletion-setting* -information element is sent and the mobile station responds with a *DHO-deletion-setting-respond* –information element.

4.4.5 Power Control

The coverage area of a base station is dependable on the transmission power of both the mobile station and the base station. If the transmission power is increased also the coverage area will grow, but this creates more interference to the whole network.

CDMA-technology requires a very sensitive interference control mechanism, since all the mobile stations are on the same frequency. A mobile station using too high transmission power can do a severe damage to the whole network. A sudden increase of transmission power may easily occur due to the landscape properties. When a moving mobile station is behind, for example, a building it needs to use reasonably high transmission power. After the obstacle has disappeared the transmission power is too high and the mobile station must be able to quickly lower the transmission level for preventing undesired interference.

As described in the Chapter 3.3.1.9, the range of a CDMA-cell is dependable on the load of the network. After a certain limit, every new mobile shrinks the planned range of a base station. When the range shrinks, then some of the mobile stations will drop out and possibly lose connection.

This fundamental difficulty between the interference and the used transmission power makes the power control a complicated task, which has to adapt quickly to different type of situations. Quick response requires a lot of signaling in the lower protocol levels. There exists a dedicated radio specific signaling channel embedded to a traffic channel which, among other things, is used for transmission of power

control bits. Since the messages sent in this channel are layer 1 specific matters they are not covered in this presentation.

The power control consist of an uplink power control and a downlink power control. Both of them include three phases: *initial power control*, *closed loop power control,* and *outer loop power control.*

Initial power control, which is sometimes called open loop power control, is used to set the initial transmission power values for different channels. Closed loop power control is used to adjust the power values of the dedicated channels according to a constant measurement information. It calculates the transmission characteristics and orders the transmitting side to either increase or decrease the transmission power in a feedback-loop. It is very fast and it can adapt to different type of situations in milliseconds. Outer loop takes care of higher-level power control. It sets the limits and requirement values for the closed loop and takes care of power control balance between cells.

The RRC power control signaling is intended for setting up the parameters of outer loop power control. The used message is the ACCESS RADIO LINK FACILITY and it is sent from the mobile station to the network. The information elements involved with the power control are *Active-zone-report*, *Low-speed-transmission-power-control-information-report*, *DHO-additional-candidate-zone-assignment,* and *HHO candidate-zone-assignment*. The first one is used to inform the network about the new power level ranges of the current active set. The ranges may change, for example, due to diversity handover. The second one is used to inform the network about the need to change the reception quality requirements, when the reception quality decreases. The last two are handover specific information elements, which also include the initial power levels for the new sectors.

4.4.6 Multicall handling

Interaction of different traffic types is an interesting question. Should it be possible to receive a data call while a speech call is ongoing? Should a speech call be

accepted while a data call is active? In GSM, the answer is currently no. Only one type of traffic is allowed at a time, but in the near future, the GPRS will change the situation. A speech call and a packet data call may be active simultaneously.

The WCDMA trial system has been designed to provide multiple types of simultaneous connections right from the start. This property is called multicall. It is a different thing than the possibility to make multiple simultaneous speech calls, which is called 'conference call' in GSM. The conference call is achieved by multiplexing the different traffic streams in the MSC to a single traffic channel. The principle is similar to as having several loudspeakers and one microphone in the MSC. One loudspeaker is reserved for every participant and the microphone captures the conversation for the listener. The multicall feature of the WCDMA Trial system provides a separate traffic channels for every connection. As a restriction there can be only one speech channel, so if the conference call is required it has to be made similarly than in GSM.

The assignment of multiple traffic channels is complicated, since the idea is to use only one signaling channel (ACCH). The different traffic channels require also different type of short codes due to the different capacity requirements.

There are different possibilities to allocate the short codes. Two active data calls can be multiplexed to one fast short code, which then includes two logical DTCHs and one ACCH signaling channel. It is also possible to allocate two slower short codes. In this case, the both DTCHs have an own short code and the ACCH is multiplexed to either one of those. It may even be possible to allocate multiple short codes for a very fast DTCH.

This type of complexity creates problems, because one call may be consisted of multiple short codes. The problem is solved with a unique call specific identifier called RBC-id. It is calculated by adding together the CC-connection identifier values CONN_ID *(Connection Identifier)* and CR *(connection reference)*. If the call consist of multiple short codes, they can be references with one identifier.

The protocol elements involved with the multicall are CC and RRC. The radio bearer is allocated by the RRC according to the radio bearer requirements provided to it by the CC. The CC also provides the connection identification information (CR and CONN ID), that can be used to calculate the RBC-id.

After a normal MOC or MTC is established, the multicall can be initiated by sending a normal call establishment message including the same IMUI or TMUI that is used in currently active call. The CC identifies the multicall situation and requests the RRC to allocate a multicall specific radio bearer. The RRC allocates the bearer and informs the mobile station by sending an ACCESS RADIO LINK SETUP message.

All the multicall specific signaling is sent on one ACCH. This is a problem in the call release, because the ACCH is multiplexed to one of the traffic channels. If this traffic channel is released, then also the signaling channel disappears. A special operation called ACCH switching solves the problem. A new ACCH channel is established before the old one is released and signaling is switched to it. If the ACCH switching is not needed, the signaling of the release is similar to a non-multicall situation.

Actually, there is very little multicall specific air interface signaling in the RRC. The complexity of multicall is in the routing and internal handling of different types of short codes. The handover situations during a multicall can also be complicated, if the active set needs to be optimized somehow.

4.5 Common Channel Signaling protocols (Others)

4.5.1 Introduction

This Chapter describes a group of small protocols, which manage the common channels. In the specification they are gathered under the name Others. Their functionality is part of the radio resource management and they co-operate with the RRC protocol. Some similarity can be found to the GSM's RR'-protocol.

4.5.2 Broadcasting of the network status

The mobile station needs several types of information about the network for being able to establish and maintain a connection. This information must be available to all mobile stations before and after a dedicated signaling channel is established. A special channel called BCCH is reserved for this purpose as described in Chapter 3.3.3.3.

The WCDMA trial signaling specification has a special protocol called *Radio Interface BCCH protocol* for broadcasting the network information on the BCCH. The protocol includes two messages: a BROADCAST INFORMATION 1 and a BROADCAST INFORMATION 2.

The BROADCAST INFORMATION 1 includes information, which is not dependent on the ongoing traffic. This type of information is for example the decision of handover zone, the zone information, the restriction information, and the information related to the control channel structure.

The BROADCAST INFORMATION 2 includes information, which is dependent on the ongoing traffic.

4.5.3 SDCCH setup

When the mobile station initiates signaling with the network or vice versa when the network initiates signaling with the mobile station, they have to use a common signaling channel. The mobile station uses RACH and the network FACH. Since resources on the common signaling channels are limited and the signaling between the network and a certain mobile station is not relevant to the other mobile stations, there is a need to establish a dedicated signaling channel for the further interchange of messages. The initial dedicated signaling channel is called SDCCH and it is established by using a special protocol called *SDCCH setup protocol.*

The mobile station initiates signaling by sending a SIGNAL CHANNEL SETUP REQUEST –message on RACH. If the establishment succeeded, the network sends a SIGNALING CHANNEL SETUP RESPONSE on FACH. This message includes the parameters required for the establishment of SDCCH. If the network is not able to establish the SDCCH, the request is rejected with a SIGNALING CHANNEL SETUP FAILURE message.

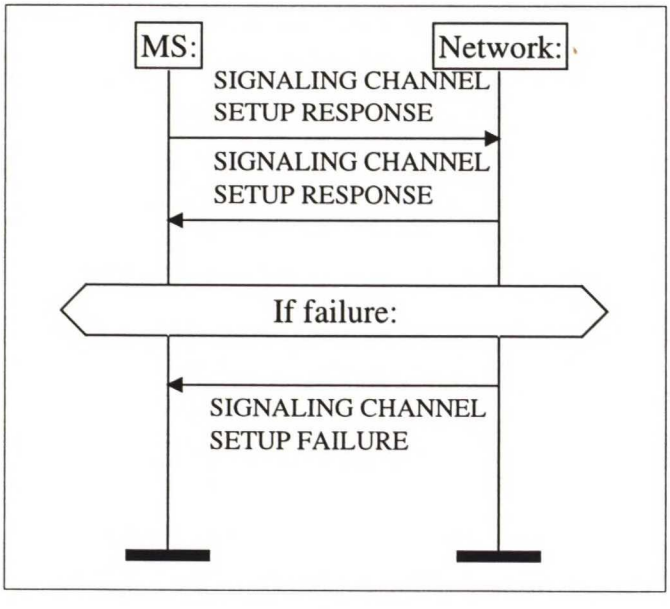


Figure 18: SDCCH establishment

It may be possible, that when multiple mobile stations are simultaneously trying to establish their SDCCH, reply messages are mixed up. For preventing this situation, mobile stations can be differentiated by using a random value called PID *(Protocol IDentifier)* on MAC *(Medium Access Control)*, which is a layer-2 protocol. The accessing mobile station allocates the PID and it is sent to the network, which sends it back with the reply message. If the sent and received PID values match, then the mobile station knows that the reply message was headed for it. Otherwise a collision has occurred and the establishment procedure is restarted.

This mechanism is similar to the one used in GSM. PID is called *random discriminator*, but it is used for the same purpose. Instead of layer-2, in GSM the random discriminator in sent with a layer-3 message RR CHANNEL REQUEST, which is equal to a WCDMA Trial message SIGNALING CHANNEL SETUP REQUEST.

4.5.4 Initial paging

During MTC, the network has to find out the location area of the mobile station. This information has been stored to the internal registers of the network, when the mobile station has done a location registration or updating procedure. When the location area is found, the network has to inform the correct mobile station with a special message, which is sent on a common channel. This procedure is called *paging.*

The common channel dedicated for paging messages is PCH. Since it would be a very power-consuming task for the mobile station to constantly listen to the PCH, mobile stations are grouped to *paging subgroups* according to their IMUI value. Messages to a certain paging group are sent in a certain time slot. The mobile station monitors the PCH only during its own timeslot. The paging subgroup of the mobile station is calculated by using the following equation:

PSG = (IMUI % (pch_n * 256)) % pch_n

where,

PSG = Paging subgroup,
pch_n = number of PCH groups,
IMUI = The IMUI value of mobile station

The specification has an own protocol defined for paging, which is called the *radio interface PCH protocol.* It includes only one message: PAGING. The PAGING message can contain paging information for a maximum of three mobile stations. When a mobile station receives a paging message, which includes its own IMUI or TMUI value, it begins the establishment of SDCCH channel according to procedure described in Chapter 4.5.2. In addition to IMUI or TMUI value, the PAGING message includes a special information element called *paging id*, which is used to separate multiple simultaneous paging messages sent to the same mobile station.

4.5.5 Packet data control

In addition to speech, mobile networks must also be capable of transmitting data. There exist two data transmission methods: Circuit switched and Packet.

The circuit switched data is similar to a normal voice transmission. An end-to-end transmission channel is established and the data transmission is started as a continuous bit flow, just like a stream of digitized voice. An adapter unit in the mobile network/fixed network interface takes care of the required internetworking operations like a PSTN rate adaptation.

The packet data is similar to sending of a letter. The data is divided into small units, which are extended with header information. One unit is called a packet. The packets have a certain fixed length and usually they are all routed separately. No end-to-end connection is needed, since a special common channel is used. The receiving party

monitors the channel constantly and identifies its own packets from the header information.

The WCDMA Trial system supports the circuit switched data and packet data. However, the nature of packet data transmission is such, that it is sent on top of a circuit switched connection. This bit strange solution is intended for simplifying the implementation of packet data services in the trial phase. A normal traffic channel is allocated between the mobile station and the network. The packet data to/from the mobile station is sent through this channel. Inside the channel, there may exist multiple virtual connections. This solution is against the idea of connectionless services and the final 3rd generation packet data concept are very likely implemented by using methods that are more sophisticated.

The WCDMA trial system packet data can be sent through two different types of channels: RACH/FACH and UPCH. RACH/FACH is used if the amount of transmitted data is limited. If the amount of transmitted data is higher then a special circuit switched packet data traffic channel called UPCH is established. UPCH is called a dedicated packet data channel and RACH/FACH a common packet data channel.

The management of packet data in the air interface is done by a special protocol called *Packet control protocol*. The protocol includes two types of messages: common packets channel management messages and dedicated channel management messages.

The initialization of a common packet channel is started when the mobile station sends a COMMON PACKET ACCESS RADIO LINK ACTIVATION REQUEST-message. The network does the required preparations and responds with a COMMON PACKET ACCESS RADIO LINK ACTIVATION SETUP -message. The mobile station confirms the setup by sending a COMMON PACKET ACCESS RADIO LINK ACTIVATION RESPONSE. All these messages are sent on RACH and FACH.

If the transmission rate exceeds a certain limit, or there are is no more data to be sent, the mobile station has to deactivate the common packet channel. The deactivation is initiated when the mobile station sends a PACKET ACCESS RADIO LINK DEACTIVATION REQUEST. When the network has deactivated the common channel, it responds by sending a PACKET ACCESS RADIO LINK DEACTIVATION SETUP -message. The mobile station confirms the deactivation and sends a PACKET ACCESS RADIO LINK DEACTIVATION RESPONSE message. All these messages are sent on RACH and FACH. If a dedicated packet channel is established during a common packet channel release, it is also possible to send the last message on UPCH.

The dedicated packet channel is activated with a DEDICATED PACKET ACCESS RADIO LINK ACTIVATION REQUEST –message, which is sent from the mobile station to the network on RACH. The network allocates the channel and responds with a DEDICATED PACKET ACCESS RADIO LINK ACTIVATION SETUP – message, which is sent on FACH. The channel is now allocated and ready for the traffic.

During the transmission, it is also possible to change the dedicated channel properties like the type and amount of used short codes. This property may be needed if the traffic increases substantially. The network allocates the new resources and informs the mobile station with a CODE ALTERNATION REQUEST -message. The mobile station executes the required modifications and responds by sending a CODE ALTERNATION message. Both of these messages are sent on UPCH.

The packet data is a relatively new feature in the mobile-communication-systems. GSM has GPRS, which is recently specified and is waiting for the first implementations. There are very little experiences about the subject. The immaturity can also be seen in the WCDMA packet data specification, which is very much under construction. The future will show how the specification will evolve.

4.6 Terminal association control

4.6.1 Introduction

After the SDCCH has been established, the mobile station has to send the user identity and the terminal characteristics to the network. In GSM terminology, the message used for this purpose is called an "initial message". The message contains the user identity and a special structure, which contains some essential parameters of the terminal. Such parameters are for example the maximum transmission power levels, the short code requirements, and the ciphering requirements. The structure is called *classmark* in GSM and *TC-info* in WCDMA trial.

The WCDMA trial specification has a three different initial messages: MOBILITY FACILITY - TERMINAL LOCATION REGISTRATION - Invoke, TERMINAL ASSOCIATION SETUP and PAGING RESPONSE. The first one is a MM – message and it is used in location update. The last two messages are part of a special protocol called TAC *(Terminal Association Control)* and they are used during the establishment of MTC and MOC.

The purpose of the TAC protocol is to send the initial messages and to receive their responses. In GSM, there is no TAC protocol and the initial messages are part of MM and RRC protocols. This could also be the case in the WCDMA trial but for some reason, they were separated to an own protocol during the specification phase.

In the Japanese 2nd generation system (PDC), the roaming of the mobile terminal and the mobile user are separated. An initial message, which includes both the user and terminal information, does actually an initial association between the user and the terminal, which is required in PDC. The existence of a TAC-like protocol in the WCDMA trial specification may be explained against this background.

4.6.2 Mobile Originated call

In first phase of MOC, the SDCCH is established by using the common channel signaling protocols. The next phase would be the MM-procedures authentication of the user and ciphering. The network cannot anyhow execute these, since it does not know the identity of the user and the ciphering algorithms supported by the mobile terminal. In addition, the RRC requires more information about the mobile terminal capabilities for the traffic bearer allocation.

As described in the previous Chapter, TAC sends the required information in a TERMINAL ASSOCIATION SETUP -message. The terminal characteristics are in the TC-info structure and the user identification is done with TMUI. If the TMUI is unidentified, which normally should not be possible due to the location update procedure, the MM requests the IMUI of the mobile station with a specific MM -message and after that executes a TMUI reallocation procedure.

After the MM procedures authentication, ciphering, and possibly TMUI reallocation are done, the network sends a TERMINAL ASSOCIATION CONNECT message and the association procedure between the terminal and the user is ove.

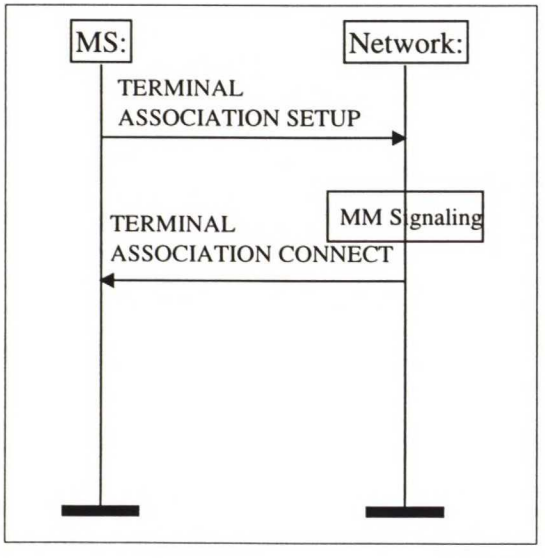


Figure 19: TAC specific signaling during MOC

TAC does not have any specific release messages for MOC and hence, the association is released during the general release procedure.

4.6.3 Mobile Terminated call

The first phase of MTC is naturally the paging, which is done with a special paging protocol. The paging is done with either IMUI or TMUI. When the paged mobile station is found, SDCCH is established for further signaling.

Similarly than in MOC, the TAC message is the first layer-3 message to be sent. In MTC, the used message is called a PAGING RESPONSE and it has two purposes: inform the network about the success/failure of the paging and to provide the required user and terminal information. If the paging is done with IMUI also the PAGING RESPONSE includes IMUI and the MM reallocates TMUI. The PAGING RESPONSE -message must also to include the paging id, which was sent in PAGING. This element is used to separate simultaneous paging messages sent to the same mobile station.

After MM procedure authentication, ciphering, and possibly TMUI reallocation are performed, the network sends a PAGE AUTHORIZED message and association procedure between the mobile terminal and the user is accomplished.

TAC does not have any specific release messages for MTC and hence, the association is released during the general release procedure.

4.7 CASE: Mobile Terminated Call

4.7.1 Introduction

Previous Chapters have described the signaling of the different protocol layers in different situations. The accomplishment of a certain procedure is anyhow result of interaction between different protocol layers. The purpose of this Chapter is to demonstrate the end-to-end signaling of one task and to show how the different protocol layers co-operate. The demonstrated task is MTC, which was chosen, since it is an example of a task, which involves all the layer-3 protocol layers. This includes also CC and TAC, which are not used, for example, during the location update.

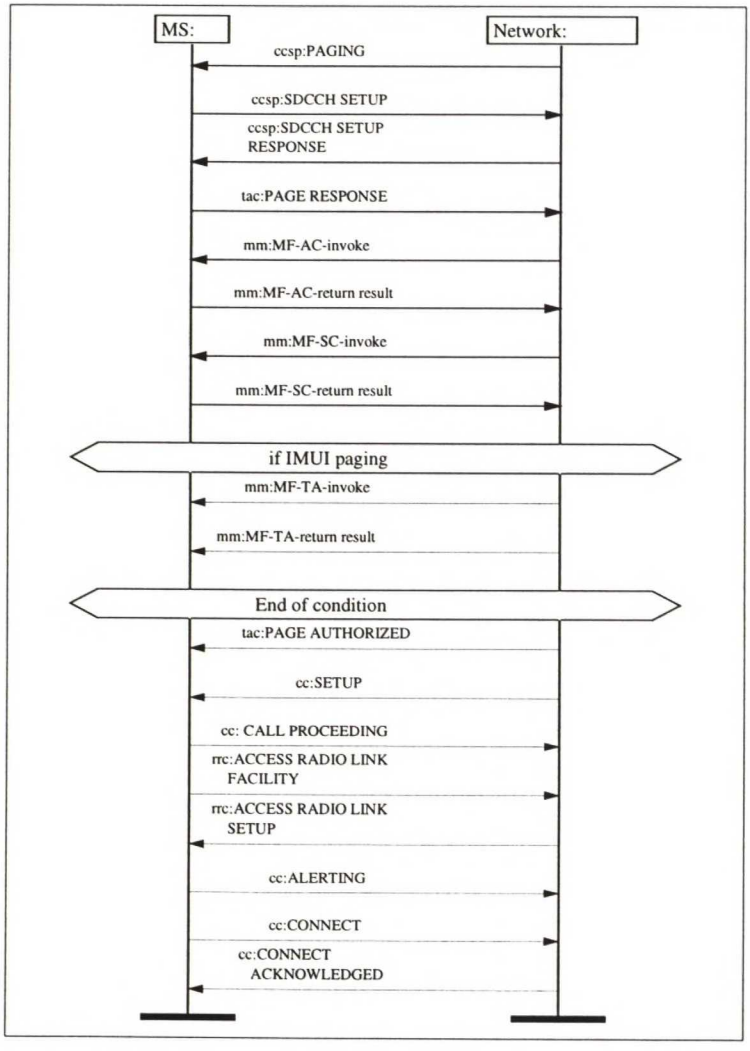


Figure 20: Layer-3 MTC signaling

4.7.2 Paging

When the network CC receives the information about an incoming call it has to initiate the paging procedure. CC is able to use only a dedicated signaling channel and the paging message must be sent in a common signaling channel. Common channels are controlled by the CCSPs *(common channel signaling protocol)*, so CC has to request paging with an internal request primitive. After the request has been received, the paging protocol (one of the CCSPs) sends a PAGING message on PCH to mobile stations. The message includes the identity of the called user and the paging id. Multiple mobiles can be paged with the same message.

The paging can be done with IMUI or TMUI, but for security reasons, IMUI should be used only in the exceptional cases. The mobile station is constantly monitoring the PCH and when it identifies a message including its own identifier, it executes the SDCCH establishment procedure.

4.7.3 SDCCH establishment

The SDCCH establishment is done by SDCCH setup protocol, which is one of the CCSPs. The signaling is initiated with a SIGNALING CHANNEL SETUP message. The network receives the message, allocates required resources (a lot of internal signaling between BTS and BSC) and informs the mobile station with a SIGNALING CHANNEL SETUP RESPONSE -message. This message includes the uplink and downlink short codes of the SDCCH. The network initializes the downlink SDCCH by constantly sending specific layer 1 messages called SDCCH IDLE PATTERN FRAME. When the mobile station receives these, it establishes the layer-2 connection and begins to send similar messages to uplink direction. The paging and the SDCCH establishment procedures are confirmed with a PAGING RESPONSE –message, which is sent from the mobile station to the network by TAC. This message includes the identification of the paged user and a terminal specific information, which is required for the further call establishment procedures.

4.7.4 MM procedures

After the network has received the PAGING RESPONSE – message, a dedicated signaling channel is established and the MM procedures are initiated for authentication of the user and preventing the eavesdropping of further signaling. The authentication is initiated with a MM message MOBILITY FACILITY – AUTHENTICATION CHALLENGE – invoke. After the authentication value is calculated, the mobile station sends it to the network with a MOBILITY FACILITY – AUTHENTICATION CHALLENGE –Return Result –message. If the values calculated by the mobile station and the network match, then the authentication was successful and the ciphering may be initiated.

The ciphering is initiated by the network, which informs the used ciphering algorithm to the mobile station with a MOBILITY FACILITY – START CIPHERING – invoke –message. The mobile station initiates the ciphering and sends the confirmation to the network with a MOBILITY FACILITY – START CIPHERING – Return Result -message. A two-way ciphering is started and the further signaling and traffic is encrypted.

The MM procedures also include the reallocation of TMUI value. The specification requires reallocation of TMUI after every location update and IMUI paging. It is also possible to reallocate TMUI after every MOC or MTC, but this is an implementation specific matter and is not mandatory.

If the TMUI reallocation procedure is needed, it is done after the ciphering is started. The used message is MOBILITY FACILITY – TMUI ASSIGNMENT – invoke. It is sent from the network to the mobile station and it includes the new TMUI value. The mobile station updates the new TMUI value to its database and informs the network by sending a MOBILITY FACILITY – TMUI ASSIGNMENT – return result - message. The new TMUI is now in use.

The network has now assured that it is possible to establish a call to the requested mobile station. TAC finalizes the paging and MM procedures by sending a PAGE AUTHORISED -message. The call establishment procedure can be started.

4.7.5 CC setup

Before the call can be established, the network must inform the mobile station about the call requirements and assure that the mobile station is capable of supporting the type of call requested. This is a CC-procedure and CC sends the information to the mobile station with a SETUP message. The message includes a list of possible bearer types and information transfer rates.

The mobile station confirms the SETUP –message by sending a CALL PROCEEDING message. If the mobile station can support only one type of bearer and information transfer rate, these are sent in this message. Otherwise the negotiations are done later with a CONNECT –message and the message is empty.

4.7.6 DTCH/ACCH establishment

When the CALL PROCEEDING is sent, the mobile station is ready for the establishment of DTCH. The DTCH requires a radio bearer. The radio bearer allocation is a RRC task and the network executes it. Before the network can do the allocation, it requires information about the radio channel properties of the current active set. The mobile station sends this information with an ACCESS RADIO LINK FACILITY –message including an *Origination/Termination-Candidate-Zone-Designation* –information element.

The network establishes ACCH and DTCH and begins to send layer 1 message ACCH SYNC on ACCH to the downlink direction. The network informs the mobile station about the ACCH configuration by sending an ACCESS RADIO LINK SETUP -message on SDCCH channel. When the RRC receives this message it begins to send ACCH SYNC –message on ACCH to the uplink direction and

switches the further signaling traffic from the SDCCH to the ACCH. When the network receives the first ACCH SYNC then the ACCH is completely established.

4.7.7 Call connection

After the DTCH is allocated, the mobile station starts alerting the called user and informs the calling users with an ALERTING -message. When the user answers, the mobile station informs the calling user with a CONNECT -message. If the used bearer and information transfer rate were not negotiated with the CALL PROCEEDING- message, then the required information is included to this message.

When the calling user has received the CONNECT -message, it replies with a CONNECT ACKNOWLEDGE –message. The call is now established.

4.7.8 SDCCH release

When the ACCH has been established, the SDCCH channel becomes obsolete and it has to be released. The RRC signaling for the SDCCH release is not used during MTC. Instead, the SDCCH is released internally after the network has received the CONNECT –message and the mobile station the CONNECT ACKNOWLEDGE – message.

5. MS-TESTER

5.1 General

5.1.1 Introduction

MS-Tester is a software-based emulator operating in a UNIX-workstation. It emulates network side of the WCDMA trial layer-2 and layer-3 signaling protocols and it is used to test the corresponding control plane protocols of the WCDMA trial mobile station. The layer-1 WCDMA radio interface is replaced with a UNIX-socket, which is extended with some additional proprietary protocols. All communication between the MS-Tester and the mobile station is done through the socket interface.

MS-Tester includes the required protocols from all the network components (BS, BSC, and MSC/HLR/VLR). The protocols are collected to a single protocol stack, so there is no need for Abis (BS to RNC) and A-interfaces (BSC to MSC). MS-Tester supports number of BSs, which makes it possible to test different types of handovers. The protocol architecture of MS-Tester can be seen in Appendix C.

MS-Tester was implemented in the CVOPS protocol development environment. During all the phases of the implementation project nine programmers were involved and 70000 lines of C-code was written. This amount includes both MS-Sim and MS-Tester. The comments and the code generated with the CodeTool encoding/decoding function generator are also included. Due the incomplete specifications, the code has been rewritten several times. One protocol, which was already implemented, was found out to be useless since it was removed in the later versions of the specification.

The experimental part of this master's thesis includes the implementation of the MM –protocol, the integration of the MS-Tester protocol stack, and the modification of TAC-protocol.

5.1.2 MS-Sim

Protocols operate in peer-to-peer direction, so before a protocol can be executed also the opposite party must exist. Without the execution, the protocol cannot be tested. Since the system under testing cannot be used for testing the tester, also corresponding peer entity must be implemented during the implementation of the tester.

This was the reason, why during the MS-Tester implementation also another simulator called MS-Sim *(Mobile Station Simulator)* was implemented. MS-Sim simulates the signaling stack of a WCDMA trial mobile station. MS-Sim was also implemented with the CVOPS protocol development environment and it was connected to MS-Tester through a socket interface. The MS-Sim protocol architecture can be seen in Appendix D.

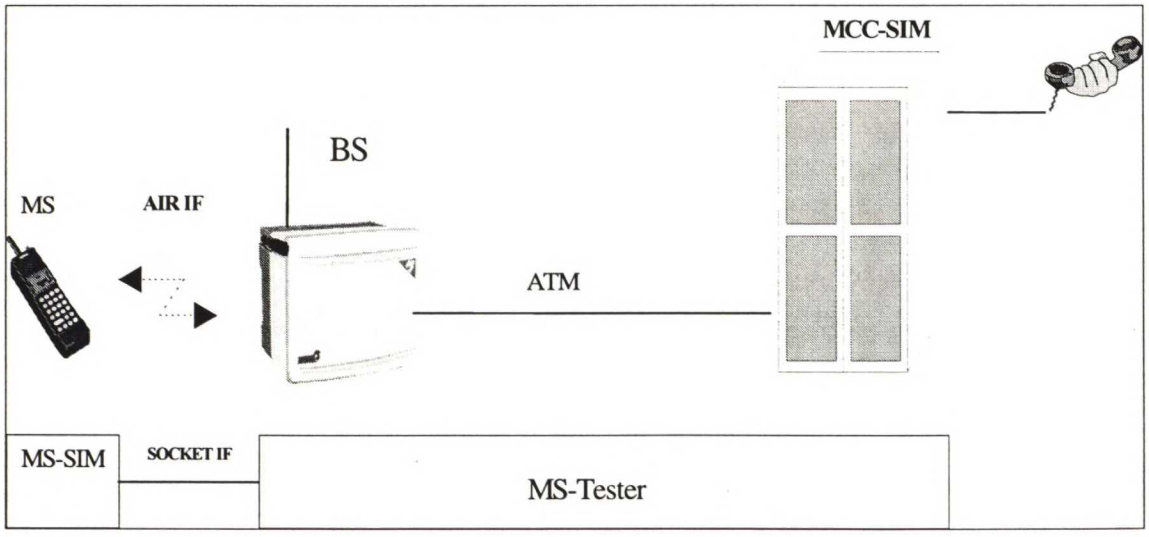


Figure 21: The physical architecture and the simulator architecture

5.1.3 Structure

The software architecture of MS-Tester consists of protocols, which are described in figure 22. All the protocols were implemented during the project. The protocols marked with gray color are completely or partly implemented by the author. The Dat-files are ASCII-files, which are read during the system initialization and can be edited either manually or using a special parameter editing tool.

- 'Physical'-layer consists of multiple CVOPS vtask. See chapter 5.1.4
- 'Others' -layer takes care of common channel signaling.
- LAC implements the LAC-protocol specific signaling.
- TAC implements the TAC-protocol specific signaling. Partly implemented by the author.
- RRC implements the RRC-protocol specific signaling.
- MM implements the MM-protocol specific signaling. Implemented by the author.
- CC implements the CC-protocol specific signaling.
- Management is used to simulate the HLR, VLR, and external networks. See chapter 5.1.5
- Vlr.dat includes all the mobile terminal and user specific information
- Bts.dat includes information specific to a certain base station
- Sector.dat includes information specific to a certain sector

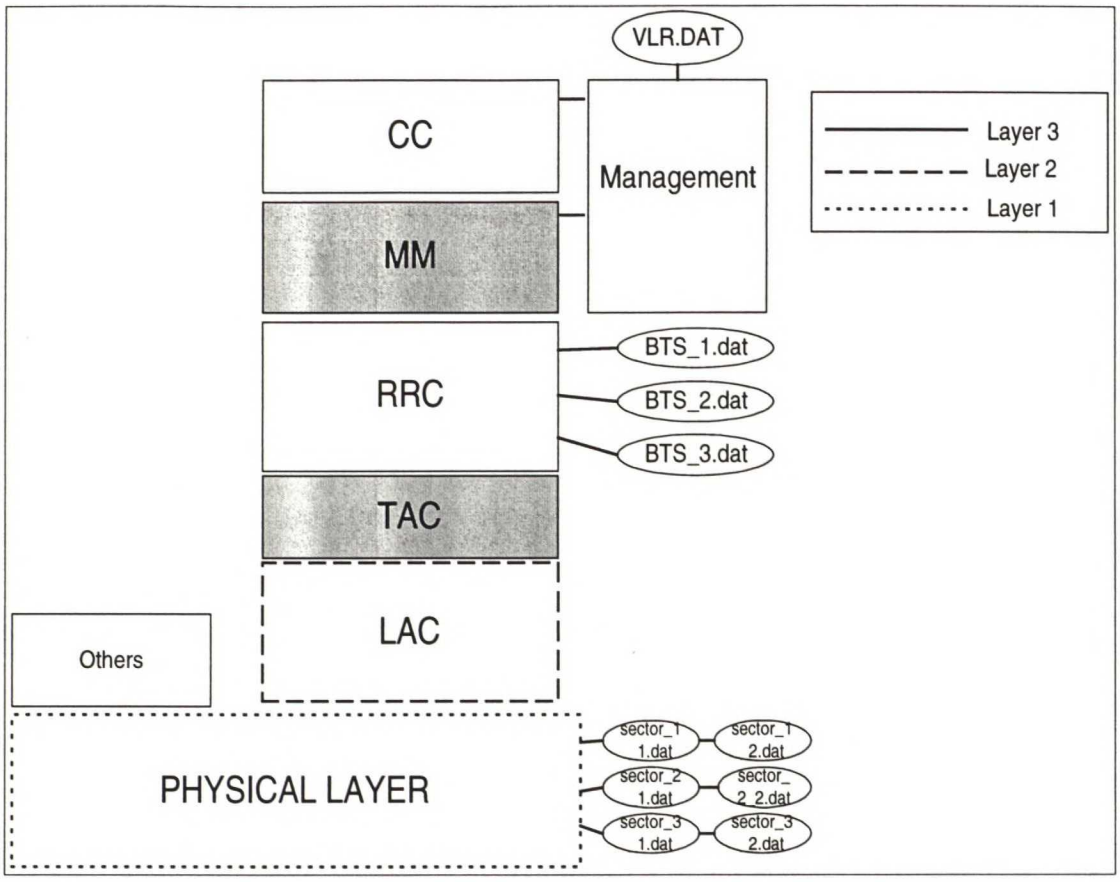


Figure 22: MS-Tester's software architecture

5.1.4 Physical layer

Due to fact that the protocol software needs to be tested as early as possible, real air interface needs to be replaced with something else. In MS-Tester, the physical layer is replaced with a physical layer emulator.

The emulator consists of five different entities: socket driver, multiplexer, phys, AUX, and diversity. It takes care of message passing over the socket interface and routes the message to the correct sector on uplink direction and to the correct mobile station on downlink direction. The routing between the entities is based on a special layer-1 specific PDU header called RIM *(radio interface management)*. All the entities were implemented in the CVOPS protocol development environment.

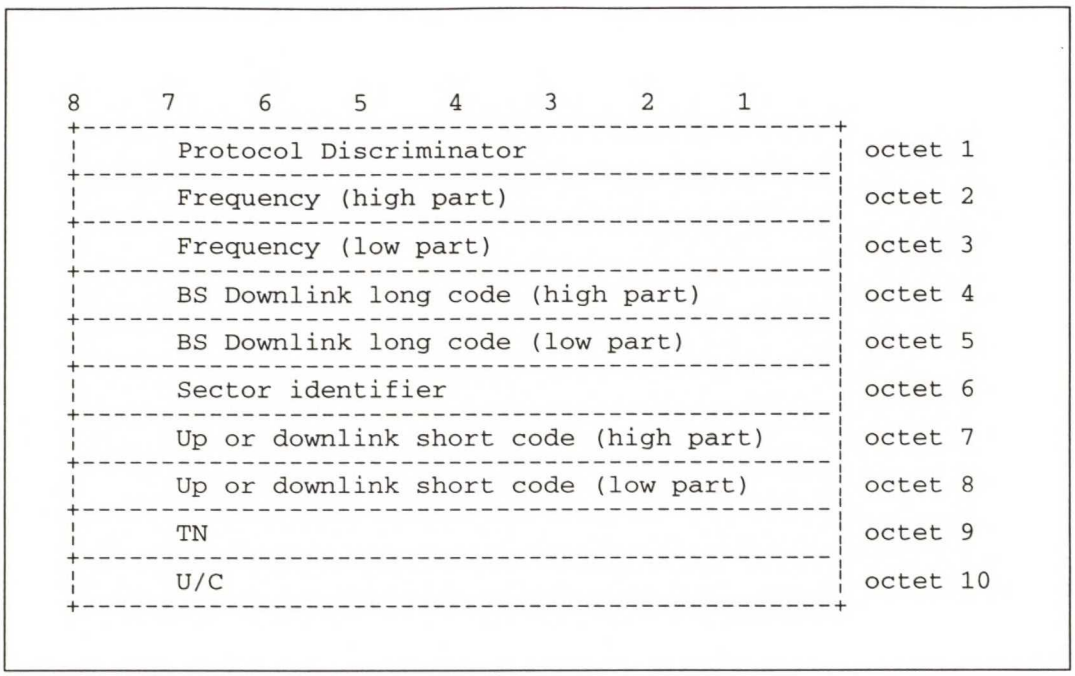


Figure 23: The Radio Interface Management header

The socket driver is a UNIX-socket implementation for CVOPS. The sockets are used to transmit the physical layer information.

The multiplexer chooses a correct PHYS-entity, which is equal to a sector. The routing is done by using the frequency, the BS long code, and the sector identifier fields of the RIM-header.

The PHYS, which is used to simulate a sector, is used to route messages to either common channel protocols, if the message was sent in a simulated common channel, or to LAC, if the message was sent in a simulated dedicated channel. The routing is done with the TN *(transparent)* field of the RIM header. If the message is sent to LAC, the correct PHYS connection is chosen with the short code field of RIM-header.

The AUX simulates the layer-3 signaling protocols of the Abis interface. It multiplexes the signaling channels and the traffic channels to separate connections. This is done with the information provided in the RIM-header.

The DHO simulates a dedicated Abis interface connection for the ACCH, SDCCH, and UPCH channels. The DHO also maintains the active set of a certain MS.

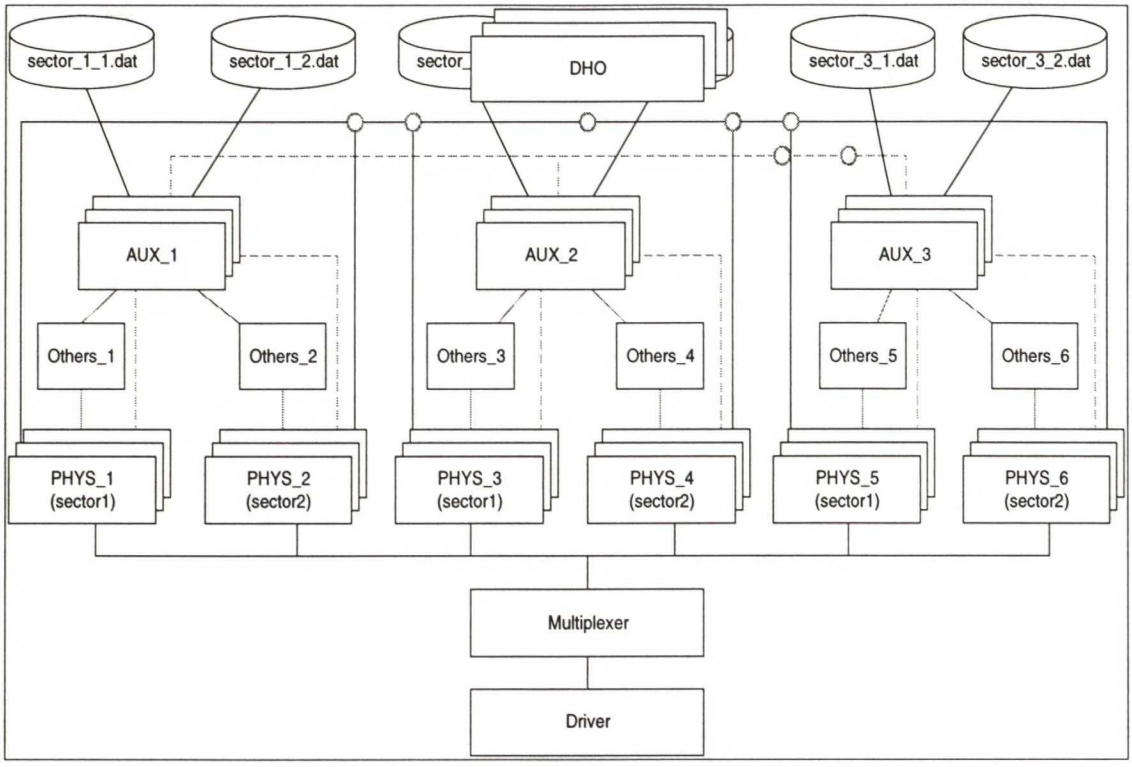


Figure 24: The architecture of physical layer simulator

5.1.5 MSC/HLR/VLR

There exist a lot of mobile station specific information, which must be maintained by the network. This type of information is for example location information, authentication specific information, and ciphering specific information. The network also has to take care of internetworking between the system and several types of external networks. In GSM, these operations execute in MSC. The WCDMA trial specification includes a very few MSC-functions and the previously mentioned operations are not in this group.

A special vtask called *Management* has been specified and implemented during the project for maintaining the user information and handling the connections to external networks. Management is a connectionless vtask. It receives requests and outputs

responses according to the given parameters. During the system initialization, it reads the parameter values of all the mobile stations from the vlr.dat file to a special internal data structure. If the data is modified during the system execution, it is updated to this structure. When the system is turned off all the modifications are lost and by the next time the system is turned on, it returns to the initial state.

Management simulates the requests coming to the system from the external networks. The external requests are sent from the CVOPS user interface. MTC, for example, can be initiated with a special 'MTC' macro. Management also simulates the external networks for CC during the call establishment phase.

Among other things, Management handles TMUI allocation, which is a VLR procedure in GSM. Management receives an internal TMUI reallocation primitive from MM, which includes the old TMUI. It responds to MM with an internal primitive including the new TMUI. The TMUI is updated to the mobile station with the MM-signaling.

5.2 TOOLS

5.2.1 CVOPS

5.2.1.1 Introduction

A protocol stack consists of multiple protocols. As known the implementation, testing, and simultaneous execution of multiple protocols is a complicated task. A good execution and implementation environment is an essential requirement for a successful project.

CVOPS *(C-based virtual operating system)* is a tool and run-time environment for implementing communication protocol stacks. It has been developed by the VTT *(Valtion Teknillinen Tutkimuskeskus – Technical Research Center of Finland)*. CVOPS is based on C-language and it has been used by the telecommunication industry for over 10 years.

CVOPS includes basic mechanisms for protocol development like scheduling, message passing, timers, frames, and execution environment. It also has a special EFSA *(Extended finite state automaton)* language for implementing the protocol logic.

A CVOPS system consists of several protocols, which may all include multiple instances (connections). One instance from a protocol implemented with CVOPS is called vtask *(virtual task)*. A CVOPS protocol stack is implemented by connecting the vtasks together through their external interfaces. CVOPS has special names for these interfaces: UP, DOWN, RES, PEER, and TIMEOUT. A CVOPS protocol stack to be run consists of the protocol stack implementation and the CVOPS run-time environment. The whole CVOPS system is executed as one process of the host operating system.

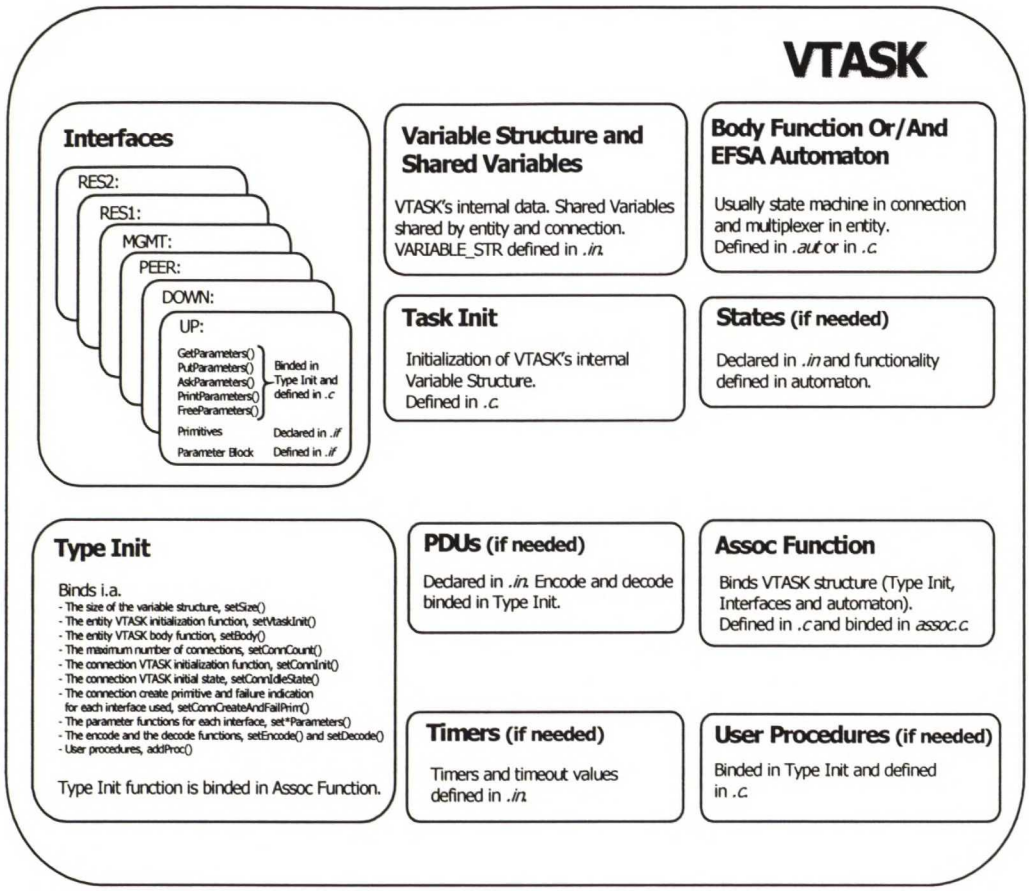


Figure 25: CVOPS architecture

CVOPS supports automatic management of internal connections. Every user can have an own stack instance. Certain service primitives can be specified to be as connection create primitives, which create new instance from the receiving protocol. The routing table is automatically updated and all the following messages coming from the sender are going to the newly created receiver.

The instantiated vtask is called as a *connection vtask*. The vtask responsible for routing the messages to the correct connection vtask is called as an *entity vtask*. In a vtask, there can only be one entity vtask, but several connection vtasks. However, it is not necessary to use the connection vtasks if there is no need for that. All the messages coming to a protocol can be handled in the entity vtask. Entity and connection vtasks can have different EFSAs, if so required.

CVOPS can be considered as a quite old-fashioned protocol development tool. Nevertheless during the years it has become a relatively stable and reliable environment and there exists many experienced users. Because CVOPS is based on C-language, it is easy to add external code and in some special situations, it is even possible to modify the CVOPS run-time environment. The external C-programming tools can be used to debug possible errors.

More information about CVOPS can be found in [MO96A][MO96R] [MO96U].

5.2.1.2 CVOPS implementation

A vtask is implemented by writing a group of protocol dependent description files and C-files. These files are compiled and linked with the CVOPS-core, which creates an executable run-time file. The CVOPS command line based user interface can be included, if so required. The following files have to be created:

1. ***.if** describes the interface between two protocols. Defines the primitives and variables used in this interface.
2. ***.in** describes the internal symbols of vtask. These symbols include PDU identifiers, vtask specific variables, and list of timers. The vtask specific variables are collected to a structure, which is called VARIABLE_STR.
3. ***.aut** contains the logical state description of the protocol. It's implemented with the CVOPS EFSA language.
4. **<protocol>.c** includes all the C-functions of the vtask, which can be called from CVOPS-automaton. It also includes some initialization functions (like TypeInit) and the functions for managing the primitive parameters. Implemented with C-language.
5. **<protocol>cod.c** contains the encoding/decoding functions of the protocol specific PDUs. It is implemented with C-language.
6. **struct.str** is used to describe the structure of the whole protocol stack. Includes information about which vtasks are connected together and through which interfaces. There is one struct.str for every CVOPS protocol stack. It is written according to certain rules and is not compiled.
7. **assoc.c** describes the bindings between the vtasks and their symbolic names. The symbolic names are used in struct.str.

5.2.1.3 CVOPS data flow

Vtasks communicate with asynchronous messages. The scheduling of different protocols is based on a message driven scheduling algorithm. A vtask sends a message to other vtask by putting it to the message queue. The scheduling algorithm notifies the inserted message and executes the protocol where the message was targeted. The execution of the protocol means the execution of the EFSA or a special function called body. The executed vtask takes the message as input and produces an output. The next execution turn is given to a vtask, which is the recipient of the next message in queue and so on.

Vtasks usually execute so rapidly that a more sophisticated scheduling algorithm is not needed. CVOPS has anyhow possibility to use the prioritized message queues and in this case, the scheduling algorithm first passes the messages, which are in the queue with the highest priority.

5.2.2 Purify

Purify is a third party software development tool, which is used to find out run-time programming errors. These kinds of errors are uninitialised memory reads and writes, memory leaks, array bound violations etc. Purify is instrumented to object files and it is used during the execution of a program. Purify is a commercial tool and it has been developed by the Rational software.

Purify has a graphical user interface, which makes it possible to monitor the occurring errors during the program execution. Some errors like memory leaks and potential memory leaks can be seen after the program execution has finished. Purify can be combined with GDB (*Gnu debugger*), which makes it possible to automatically debug the code if a Purify-specific error occurs.

5.2.3 CodeTool

A protocol includes a lot of information, which has to be sent peer-to-peer. This information is stored to the internal data structures of the protocol. These structures cannot be used to transmit the included data to the peer entity and therefore some external representation format has to be used instead. Such a format is for example an octet string. A peer-to-peer message including identifier and user data in the external representation format is called a PDU *(Protocol Data Unit)*.

Functions, which carry out the conversion from the internal representation to the external representation, are called *encoding functions*. The functions, which do the opposite, are called *decoding functions*.

CodeTool is an encoding/decoding function generator developed by Nokia Research Center. It has a graphical user interface, which makes it possible to describe the messages and their information elements graphically. The CodeTool can generate the encoding and decoding functions according to descriptions. The generated C-functions can be compiled and linked to either CVOPS or used as stand-alone. This depends on the code generator settings. The CodeTool also generates the print- and ask-functions, which can be used for tracing purposes.

The CodeTool can be used with protocols, which have non-formal external representation format for data. If some formal representation, like ASN.1, is used then the other tools are more convenient. The CodeTool has certain limitations and due to the complexity of many information elements, there is sometimes a need to manually edit the generated code. This makes it difficult to update the generated functions later. In such situations, CodeTool is anyhow worth using, because a lot of code can still be generated and it is error free.

5.3 Integration of MS-Tester stack

5.3.1 Introduction

The implementation of the MS-Tester was done during April 1997 – November 1997. Because the MS-Tester consists of protocol layers, the implementation could be done modularly. Every programmer implemented one or more vtasks. MSCs *(Message Sequence Chart)*, were used to define the interaction and interfaces between the different protocol layers.

After the implementation was done, the programmers did the module testing in their own module test environments and gave the code for integration. The integration work was separated to two parts: RRC + the lower layers and the layers above the RRC (done by author). The integration was done during the December 1997 – January 1998.

5.3.2 Integration

The integration had to be done in a down-to-top fashion, because the upper layer protocols require the services of lower layer protocols. Because the integration of the lower layers and the upper layers was done simultaneously, the RRC module test enviroment was initially used for emulating the lower layers. This gave more time for the lower layer integration.

The integration was done layer-by-layer. As a first phase, the global compilation preparations were extended so, that it included also the new vtask. The first compilation attempt was never successful. Some dependence files were needed for replacing the ones used in the module test environments.

After the compilation was successfully done, the first execution attempt was usually a failure. The most common explanation was a null pointer. Usually the null pointers

were due to differences between the primitive parameter handling in the module test enviroment and in the integration environment. Purify and GDB were found out to be valuable tools in this phase.

When the system was operational, it was often found out that there had been some misunderstanding concerning the interaction between two layers despite of careful planning. Usually some piece of information was missing and a new primitive had to be added for providing that. Some concepts were also understood differently by different people and this created a problem. Actually, this was expected due to the draft status of the specification.

A major problem was routing and the use of connections. Because the module test environments had usually been very simplified, the routing properties had not been thoroughly tested. This was clearly seen during the integration. For some vtasks, the whole routing system had to be rewritten and almost all vtasks required some modifications.

Version management system was also developed. It was made according to previous systems, which have been used in NRC. A special script was implemented for every vtask. This script fetches the correct file versions from the version control system. The script can be updated automatically, so the programmer does not have to type in the absolute version numbers. The system has one main level script, which creates the directory structure and fetches vtask specific scripts from the version control. After the scripts are fetched, they are executed.

The version number of the main script is also the version number of the whole MS-Tester. The version number is shown during the initialization of the system. It is also possible to show it with **version** –macro.

The integration work also included some modifications to the internal tracing mechanism and installation of the message editor tool to all vtasks.

5.3.3 Experiences

During the integration work several things were learnt about big software projects and protocol programming:

- The interfaces can never be defined too well
- It should be assured that all the programmers understand the basic concepts exactly in the same way.
- Physical distances decrease the software quality. If possible, all the programmers and designers should be situated in a same physical location.
- A proper requirement analysis should be done, so there is a doubtless mutual understanding what should be done.
- Good MSC-charts are invaluable
- The properly done and thorough module tests save a lot of time.
- Purify-like tool is required. No Purify-errors should be allowed.
- The main designer should have limited amount of actual implementation work. An experienced technical coordinator is required.

5.4 Implementation of Mobility Management

5.4.1 General

The WCDMA trial MM-protocol has gone through multiple changes between the different specification versions as described in Chapter 4.3.2. The differences between the first specifications and the current ones are huge.

Usually the protocol should be implemented tightly according to the specification, which should provide the exact and unambiguous implementation instructions. Because the schedule of the project was very tight, the implementation work had to be started although the specification was merely a draft. This meant, that some guesses had to be made, which were based on previous experiences from similar systems. Sometimes these guesses were right and sometimes wrong. This was also the case with MM-protocol.

A wrong guess was to use ROSE and BER coding. The encoding/decoding functions were written with ASN.1 and compiled with CASN/ASN2C. The later specification versions changed the external representation of data, and the encoding/decoding functions had to be rewritten. Luckily, the CodeTool could be used and situation was not a disaster.

The new codecs still included some ROSE specific features. One of these was the usage of three octets for identification of message instead of one. This property made impossible to code the message identification with CodeTool and it had to be implemented manually.

An interesting feature was also the lack of proper state machine descriptions. All the existing SDL-charts were mere drafts and gave very little real information about the protocol. The protocol logic had to be implemented by using the general MSCs of MS-Tester.

A major problem was also the language. All the new specifications were released in Japanese and in the worst case the translation to English took weeks. Luckily the Japanese specifications had some English words in the message descriptions and some work could be done. Naturally, the more detailed explanations were unreadable so they had to be guessed before the translation was available.

5.4.2 Structure

The MM-protocol consists of an entity vtask and an connection vtask. The connection vtask would not have been obligatory, but it was implemented since in the future there may be multicall features, which require multiple MM instances. Both the connection and entity vtasks have similar state machines. The encoding and decoding functions were written with CodeTool and the generated code was modified manually to provide properties, which were impossible to implement with CodeTool.

The MM routing was implemented to be simple. All the primitives from RRC are routed directly to CC entity vtask, which chooses the correct connection and binds the MM/CC interface for the next incoming message. During a multicall, a special MM routing table is used to calculate the correct CC or RRC connection and the interface binding is done in MM by using additional routing services of CVOPS.

The MM does not have any databases. The initial subscriber information is read and updated by Management and it is provided to and from MM by using the CVOPS internal primitives.

5.4.3 Encoding/decoding

Due to ROSE origin, there exist three types of MM information elements: Operation-, Procedure-, and Singleton information elements (see Figure 15). The Singleton – type information elements are used to store data and the Operation and Procedure – type information elements are used for encoding and decoding.

There are separate data structures for all information element types, but the data is only on the bottom, singleton level. The reason for this solution is the code generation structure of CodeTool. An own structure is specified for every information element and because in MM there is only one message, there are lots of information elements. Since most of the information elements do not include any data and they are used for structural reasons, it would be useless to copy the data to their leaf nodes. Instead, the data is stored to the main level of the variable structure (Singleton-type element) and the substructure pointers of the higher-level information elements are set to these elements.

As an example we can take the encoding procedure of the MM message MOBILITY FACILITY – TMUI ASSIGNMENT – invoke. The message requires TMUI and TMUI assignment source id –values, which are sent to MM by Management. The data is copied from the internal primitives to the corresponding information elements in the variable structure. For example, the TMUI is copied to a TMUI structure, which includes a node called TMUI.

The TMUI ASSIGNMENT–invoke –structure (Procedure-type element) consists of a TMUI -structure and a TMUI assignment source id –structure. The pointers of the substructures are now set to the corresponding structures on the top level of the variable structure. For example, the TMUI structure pointer is set to the previously mentioned TMUI structure.

The operation level structure, TMUI ASSIGNMENT -basic information element – structure, includes a pointer to Invoke, Return Result, Reject, or Return Error type of procedure level information element. Since in this example, the procedure is Invoke, the pointer is set to a TMUI ASSIGNMENT–invoke –structure. The procedure type is given as a parameter of the encoding function and the pointer is set with a switch-case structure.

The pointer chain from top-to-bottom is now ready and the data can be encoded. The result of the encoding is an octet string, which is stored to a frame-type variable. The variable is a part of the variable structure.

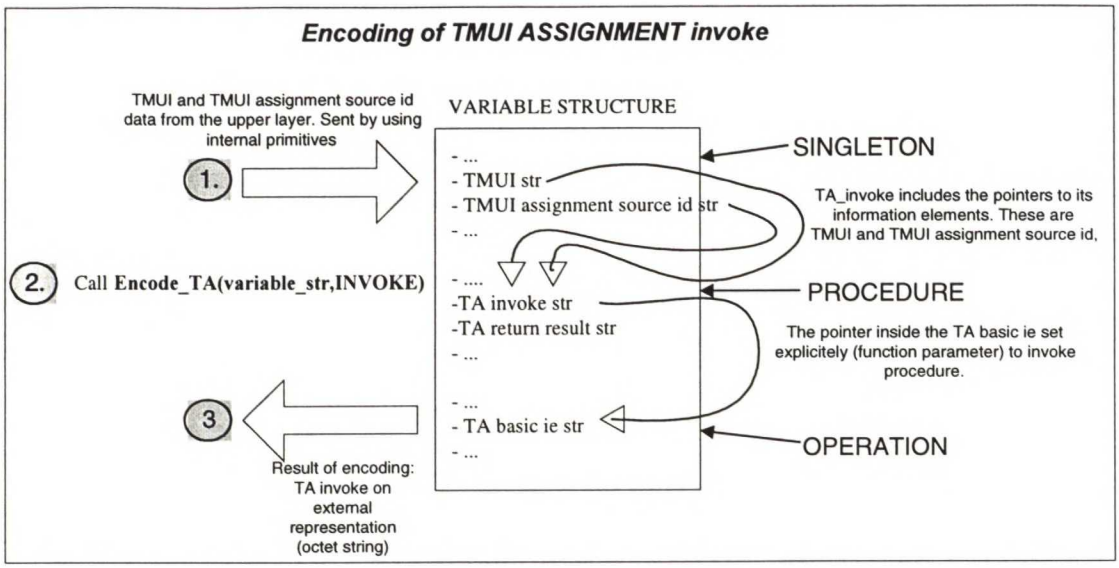


Figure 26: The encoding procedure of TMUI ASSIGNMENT –invoke.

The decoding procedure uses same principles, but works the opposite way. The result of decoding is set to similar singleton level information elements, than from where it was encoded.

5.4.4 State machine

A simplified MM state machine consists of eight different states: IDLE, AUTHENTICATE, START_CIPHERING, WAIT_TMUI, INITIATING, TMUI_ASSIGNMENT, RESOLVE_IMUI, and ACTIVE.

IDLE is the initial state. The next state is INITIATING. In MTC and MOC, the transition is triggered by RRC, which sends an internal primitive. In LU, the transition is triggered with a MOBILITY FACILITY-TERMINAL LOCATION REGISTRATION – invoke message, which is sent by the mobile station.

During the INITIATING -state, the user is identified. MM requests Management to check the validity of TMUI or IMUI (initial LU). If the TMUI was known the management replies with a *mgtMm_MsidFound* – primitive, otherwise a *mgtMm_IMUIreq*- primitive is sent and the IMUI has to be requested.

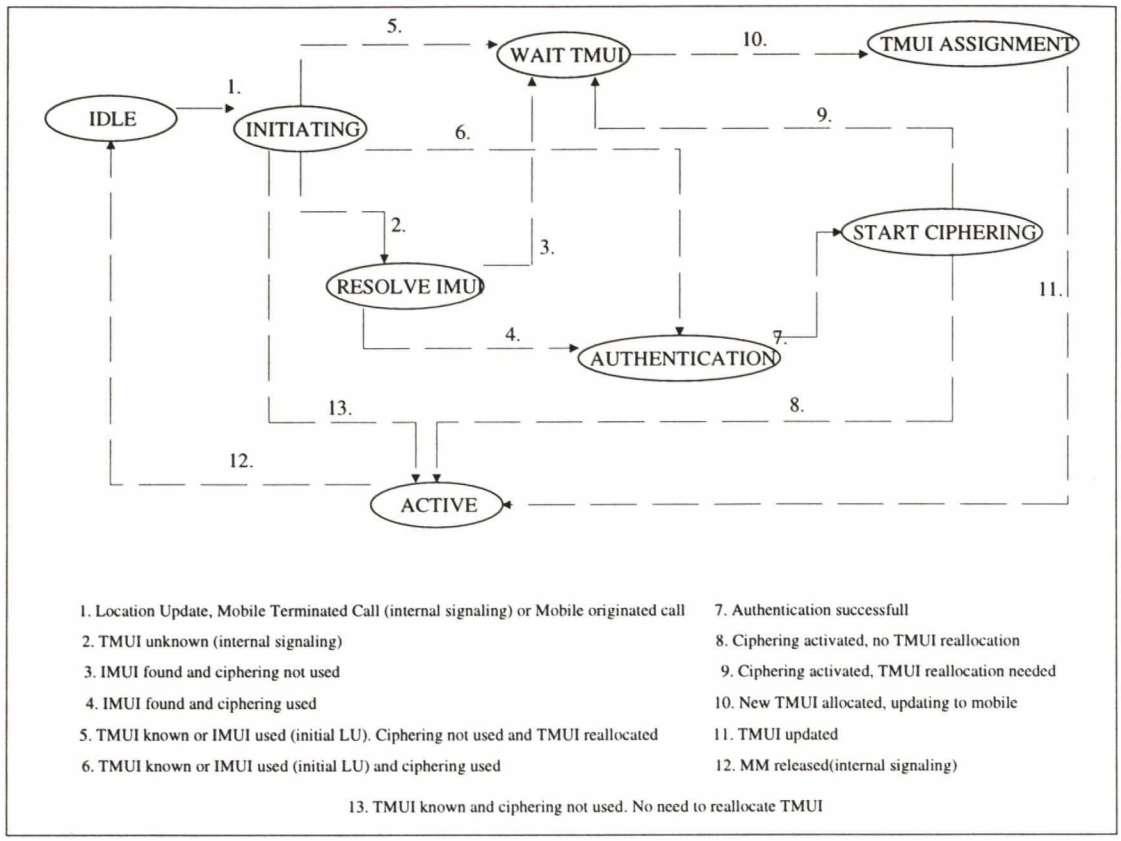


Figure 27. The simplified state machine of the Mobility Management

If the TMUI was unidentified, the IMUI value of the mobile station has to be requested. A MOBILITY FACILITY – IMUI REQUEST – invoke -message is sent to the mobile station and the state is switched to RESOLVE_IMUI. After the mobile station has sent its IMUI with a MOBILITY FACILITY – IMUI REQUEST –Return Result –message, the procedure continues.

The next state depends on the status of the NO_CIPHERING flag. If the flag is not set the mobile station has to be authenticated and ciphering must be activated. A MOBILITY FACILITY – AUTHENTICATION CHALLENGE –invoke –message is sent and the state is switched to AUTHENTICATE. After a MOBILITY FACILITY – AUTHENTICATION CHALLENGE –Return Result is received, the state is switched to START_CIPHERING and a MOBILITY FACILITY – START CIPHERING – invoke -message is sent. The mobile station answers with a MOBILITY FACILITY – START CIPHERING –Return Result –message. the mobile station is authenticated and the ciphering is active.

The next state depends on TMUI. If the TMUI has to be reallocated due to usage of IMUI or LU, a reallocation procedure has to be initiated. Otherwise the state is switched to ACTIVE and the following procedure is skipped.

The new TMUI value is requested from the Management with a *mmMgt_TMUIreq* – primitive and the state is switched to WAIT_TMUI. When Management responds, the state is switched to TMUI_ASSIGNMENT and the new TMUI value is sent to the mobile station with a MOBILITY FACILITY – TMUI ASSIGNMENT –Invoke –message. After the mobile station has answered with a MOBILITY FACILITY – TMUI ASSIGNMENT -Return Result –message, the procedure is finished and the state is switched to ACTIVE.

When the state is switched to ACTIVE, MOC and MTC require now further messages to be sent, but LU must be confirmed with a MOBILITY FACILITY – TERMINAL LOCATION REGISTRATION –Return Result -message.

MM is released with the internal primitives during the general call release or after the LU. During the release procedure, the state is switched to IDLE.

All operations also have reject and error messages. A Reject -message is sent if there is a decoding problem, authentication failure etc. The Return Error -message is used with the fatal errors like unidentified IMUI or application error. All the messages also have retransmission timers. After a Reject or time-out has been received, ten retransmission attempts are made before giving up from trying and switching the state to IDLE. If a Return Error is received, the state is switched immediately to IDLE.

5.5 Implementation of Terminal Association Control

5.5.1 General

As described in the Chapter 4.6, Terminal Association Control (TAC) is a protocol used to send so-called initial. The first draft version of TAC was implemented according to the first specification version. Author made the modifications required by the later specifications.

The modifications consisted of the removal of two messages (confirmation messages) and the updating of encoding/decoding functions to correspond to specification changes. Some bug fixes and modifications, which were required by the internal signaling, were also made.

5.5.2 State machine

A simplified TAC State machine consisting of five different states: IDLE, LAC_CONNECTED, AWAIT_TA_CONNECT, AWAIT_PAGE_AUTH, and TA_CONNECTED.

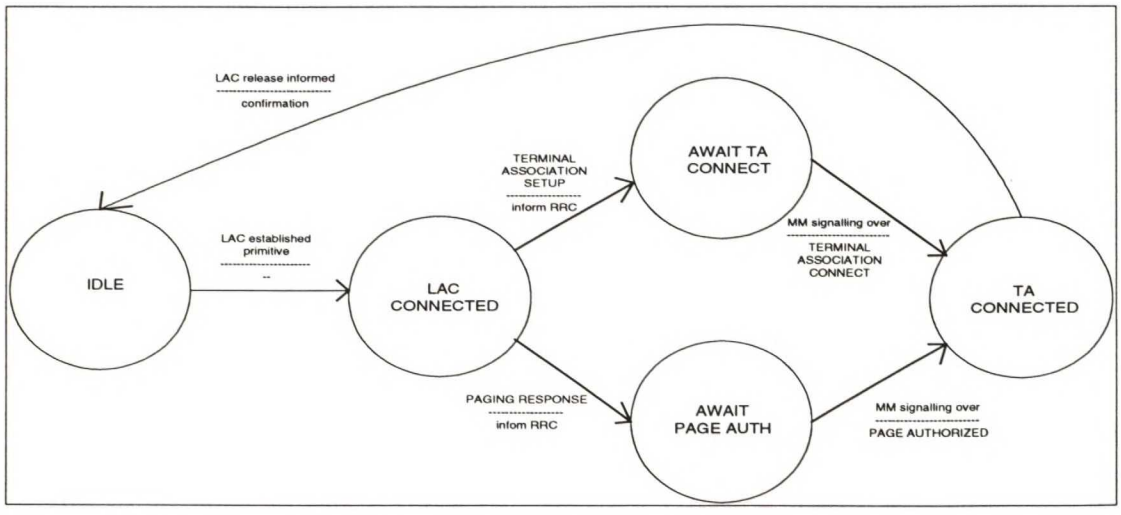


Figure 28: A simplified state machine of TAC.

IDLE is the initial state. After the lower layer (LAC) is established, it is signaled to TAC with an internal primitive, and TAC switches its state to LAC_CONNECTED. The procedure continues, when an initial TAC message is received from the mobile station. When MOC is established the received message is a TERMINAL ASSOCIATION SETUP and state is switched to AWAIT_TA_CONNECTED. When MTC is established the received message is a PAGING COMPLETED and the state is switched to AWAIT_PAGE_AUTH.

When the MM specific MTC/MOC signaling is over, MM informs this to RRC, which in turn informs TAC. TAC sends a reply message to the mobile station, which is a PAGE AUTHORIZED during MTC and a TERMINAL ASSOCIATION CONNECT during MOC. In both cases, the state is switched to TA_CONNECTED and a TAC-connection is established.

TA CONNECTED -state is switched to IDLE after the LAC-connection is released. The release is signaled to TAC with an internal signaling primitive.

Previously TAC had also two confirmation messages for the release: one for MTC and one for MOC. Both messages required a state before the TA_CONNECTED – state could be switched to IDLE. In the latest specification versions, these were removed.

5.5.2 Encoding/Decoding

Re-implementation of encoding and decoding functions consisted of updating the CodeTool definitions and modification of the already generated code due to some complicated information elements.

The TC-info information element was completely updated. The first specification version defined it as an octet field, with the length of one, but in the later specification versions it was changed to be a complicated variable length data structure.

The coding rules for IMUI were changed. The IMUI coding was changed to be BCD *(Binary Coded Decimal)*. Usually this type of coding is easy to implement with CodeTool, but in this case, the first BCD digit was changed to be the last 4 bits of the first octet, where the first 4 bits were used for a identification and length information. This type of structure was impossible for CodeTool and the generated code had to be manually modified.

5.6 Use of MS-Tester

5.6.1 General

MS-Tester is controlled through the CVOPS command line user interface. The user interface makes it possible to send primitives to all vtasks, enter primitive parameters, set values for the CVOPS internal variables, and execute macros. It is also possible to set the tracing level either for each vtask separately or for the whole system.

5.6.2 Execution

A signaling procedure is used to execute a certain mobile-communication-situation like location update (LU), Mobile Terminated call (MTC), Mobile originated call (MOC), Soft Handover (SHO) etc. A signaling procedure is initiated by sending a primitive with certain parameters to the correct vtask.

Since there are multiple types of primitives, which may include a huge amount of different types of parameters, specific CVOPS macros are written to simplify the situation. For example, MTC can be initiated with a single command (MTC).

Here is an example of an execution of SHO using tracing level 3 (see Chapter 5.6.3.). Before the SHO can be executed, either MOC or MTC must be active. We assume that this has already been done.

The tracing level is changed to 3:

```
:
 Alternative commands:
 <macro> <vtask> aboutCvops Clear debug Exit log macro memory path production
  Reinitialize run send set show system? .

: set trace allV sp i3

:
```

The macro **t3** could also have been used.

The SHO is initiated by sending a correct primitive to RRC protocol:

```
:
 Alternative commands:
 <macro> <vtask> aboutCvops Clear debug Exit log macro memory path production
  Reinitialize run send set show system? .

: nwRRC.con_.1 outputRrc_handoverReq
```

The macro **sho_add** could also have been used.

5.6.3 Tracing

5.6.3.1 Introduction

When a protocol stack is executed, there must be a way to observe its operation. The amount of information, which can be displayed from the stack is huge. Therefore there must be some means to filter the information and according to the given parameters provide only the requested details. This observation of the stack is called

tracing and the information that is provided by the tracing system, is called *tracing information.*

Already during the project establishment phase it was decided, that the existing CVOPS tracing could not be used as it is. The CVOPS tracing does not provide protocol specific information, instead it traces the internal functions of CVOPS.

CVOPS provides a mechanism called *internal tracing* for implementing an external tracing. The information included by the message and the internal state of a vtask can be given as a parameter to an external function, which can then decide what information should be printed and how.

5.6.3.2 Usage

The MS-Tester tracing is based on an external tracing function called *trace_msg.* This function is called by the vtask immediately after it has received a message. The function traces the contents of a message in a certain tracing level. The direction of the message can also be seen. High level means, that more information is shown. If the tracing level is such, that it requires the contents of an information element to be printed, it calls a vtask specific print function for the information elements of the vtask.

5.6.3.3 Tracing levels

There exist seven possible tracing levels:

1. PDU name + direction, protocol layer.
2. PDU name + direction + contents in hex, protocol layer
3. PDU name + direction + contents in hex, protocol layer, primitive name
4. PDU name + direction + contents in hex, protocol layer, information element contents (field by field)
5. PDU name + direction + contents in hex, protocol layer, primitive name, information element contents (field by field)
6. PDU name + direction + contents in hex, protocol layer, primitive name, information element contents (field by field), timer time-outs
7. PDU name + direction + contents in hex, protocol layer, primitive name, information element contents (field by field), timer time-outs, primitive parameters

The level seven is not used in the current system. It is reserved for the future purposes. Examples from the different tracing levels can be seen in Appendix B.

5.6.4 Message editor

5.6.4.1 Introduction

The message editor is a testing tool for CVOPS developed by Nokia Research Center. It allows the modification of the contents of a certain message, or to replace the content of a message with a totally different one. This makes possible to test different types of decoding and signaling errors.

The installation of the message editor requires come minor modifications to the code of the encoding/decoding functions and the parameter functions. The new message must be written to a special file from where it is read by CVOPS, when time for sending comes. The new message can be written either as a sequence of bytes, which replaces the old one, or it can be modified by using certain simple editing commands.

The message file is read with a special primitive called *msgedit*, which is sent to the corresponding vtask. After the primitive is received, the message editor requests the name of the file. The message data is read to a special data structure from where it is read by the CVOPS when a corresponding message is sent.

5.6.4.2 Example

As an example, editing of the fictitious "PAGING COMMAND"-message:

The original message as encoded by the Network simulator:

```
0c 15 01 90 0e 02 0c 08 11 32 54 76 98 10 32 f4
```

Editing command (*paging.msg*-file):

```
! This is example of case 1 (BTSM means BTSRR-layer)
BTSM PAGING_CMD 0c 15 01 90 0e 02 0c 08 11 32 54 76 98 10 32 f4
```

Or alternatively (*paging.msg*-file):

```
! this is example of case 2 (BTSM means BTSRR-layer)
@BTSM PAGING_CMD S:5 D:1 I:1;02 S:1 DL I:9;08;11;32;54;76;98;10;32;f4
```

In both above cases the sent message will be:

```
0c 15 01 90 0e 02 0c 08 11 32 54 76 98 10 32 f4
```

The message editing files are loaded to the simulator in the following way:

```
send to arb msgedit
< Give a name of the file containing the Edited msg's:> "file"
```

5.6.4 Example

Here is an example of MTC signaling procedure on a tracing level 1. The operation of MM and TAC state machines are also partly shown.

MTC is initiated from the CVOPS user interface with a special primitive, which is sent to the Management vtask:

```
:

Alternative commands:
<macro> <vtask> aboutCvops Clear debug Exit log macro memory path production
Reinitialize run send set show system? .

: mtc
```

Signaling is started. Tracing is edited to contain only the layer-3 signaling messages (-> = Incoming message, <- = outgoing message):

```
NWLAYER3M_1        PEER-> : PAGING
NWLAYER3M_1        PEER<- : SIGNALING_CHANNEL_SETUP
NWLAYER3M_1        PEER-> SIGNALING_CHANNEL_SETUP_RESPONSE
NWTAC.CON_.1       PEER<- : TAC_PAGE_RESP
```

After TAC has received the PAGING RESPONSE, it signals internally the user identifier to Management. The user identifier is either IMUI or TMUI. The MM state machine receives an internal primitive from Management, which confirms the identification of the user. If ciphering is used, then an authentication message is sent. Otherwise MM executes an **after_ciphering** () –macro, which executes few operations and switches the state of MM to ACTIVE.

```
INITIATING        mgtMm_MSidFound        {
                                         if (NO_CIPHERING == 1)
                                         {
                                            after_ciphering()
                                         }
                                         else
                                         {
                                            start(TIMER_5)
                                            RT_COUNTER = 0
                                            Comp_type = 1 (* INVOKE *)

                                            Encode(MM_AC)
                                            MmRrc_dtr
                                            To(AUTHENTICATE)
                                          }
                                          }
```

The signaling continues according to the signaling procedure. The sent authentication message can be seen as the first in the sequence:

```
MMNWS.CON_.1        PEER-> : MF_AC_INVOKE
MMNWS.CON_.1        PEER<- : MF_AC_RESULT
MMNWS.CON_.1        PEER-> : MF_SC_INVOKE
MMNWS.CON_.1        PEER<- : MF_SC_RESULT
MMNWS.CON_.1        PEER-> : MF_TA_INVOKE
MMNWS.CON_.1        PEER<- : MF_TA_RESULT
```

After MM procedures are over TAC receives an internal primitive from RRC and sends a PAGE AUTHORIZED message:

```
AWAIT_PAGE_CMP      rrcTac_pageAuthReq  {
                                          TacLac_idtr(TAC_PAGE_AUTH)
                                          to (TA_ACTIVE)
                                        }
```

The signaling continues. The Sent TAC message can be seen as the first in the sequence:

```
NWTAC.CON_.1        PEER-> : TAC_PAGE_AUTH
CC.CON_.1           PEER-> : CC_SETUP
NWRRC.CON_.1        PEER<- : ACCESS_RADIO_LINK_FACILITY
NWRRC.CON_.1        PEER-> : ACCESS_RADIO_LINK_SETUP
CC.CON_.1           PEER<- : CC_ALERTING
CC.CON_.1           PEER<- : CC_CONNECT
CC.CON_.1           PEER-> : CC_CONNECT_ACKNOWLEDGE

:
 Alternative commands:
 <Macro> <vtask> aboutCvops Clear debug Exit log macro memory path production
  Reinitialize run send set show system? .

:
```

The procedure is finished. The call is active and the CVOPS user interface is waiting for further commands.

6. CONCLUSIONS

The success of the current 2nd generation mobile-communications-systems has created a worldwide interest towards the development of the 3rd generation mobile-communication-system. One of the most promising radio access technologies currently is WCDMA, which is under major research activity around the world. One of the major players in the development and standardization is the leading Japanese mobile-communication-operator NTT/DoCoMo. For supporting the WCDMA development, NTT/DoCoMo has created a trial specification for a complete WCDMA system. The system is called a WCDMA trial system.

This master's thesis describes the layer-3 radio interface specific signaling parts of the WCDMA trial system specification and the Nokia Research Center's implementation of the specification. In addition, a short description about the status and future of the 3rd generation mobile-communication systems is given. The implementations of Mobility Management and Terminal Association Control protocols are described in more detailed level, because the author was responsible of them. The author also participated to the stack integration process, which is described and analyzed here.

Implementation was done with CVOPS protocol development tool. During the implementation process, CVOPS was found to be flexible and straightforward to implement, but a bit old fashioned. Nokia Research Center's long experience in CVOPS implementations was found out to be a benefit, because it was always possible to get support from the more experienced CVOPS programmers. Due to fact that CVOPS is based on C-language, more complicated programming errors could be debugged by using the standard external C-programming tools like symbolic GDB-debugger and Purify-analyzer. The information element structures used in the specification were simple, so Nokia Research Center's CodeTool- code generator could be used to automatically generate the error sensitive encoding and decoding functions.

Nokia Research Center has a long experience in the development of workstation based signaling testing environments. Software based testing has been found out to be very usable before the final integration tests. The correct functionality of the system under testing can be verified and modifications to the software under testing can be done easily in a good software development environment. Well-tested software speeds up the integration testing of the system because one source of errors is eliminated and most of the system parameters could have been chosen and tested.

A specification should be an unambiguous description of a system. Unfortunately, the current development cycle has become so rapid, that there is less and less time to do specifications. This creates a situation, where specifications are not finished before they are released. During this project, it was found out that the product development process must adapt to this situation and the implementation work must be initiated immediately when the first specification drafts are available. The development team must make good guesses and use common sense to fill the gaps. Some of the guesses may turn out to be incorrect, but it does not matter if most of them are right and the rough guidelines stay the same.

The principles of protocol programming stay the same despite of the system. CDMA technology has anyhow some specialties, which add complexity. The most remarkable of these is the macrodiversity. The proper handling of multiple simultaneous transmission paths to one mobile station is a complicated task and makes the implementation of Radio Resource Control quite hard. WCDMA is also a new system and there are very few non-radio-technological books about the subject. This increases the importance of information spreading inside the project. It must be assured that all the members of the project understand the basic concept similarly.

Generally, the MS-Tester project succeeded well. The customer of the project, Nokia Mobile Phones, was very satisfied and the WCDMA trial mobile station was delivered to NTT/DoCoMo in time. According to NMP, this would have been impossible without workstation testing. Recent news from NTT/DoCoMo laboratories in Tokyo announced, that the first successful layer3 call was made with the Nokia's mobile station. Nokia was the first non-Japanese manufacturer providing functional prototype mobile station.

REFERENCES

[CDGCONT] ITU-R U.S. TG8/1: *The cdma2000 ITU-R RTT Candidate Submission.* ITU-R, June 1998

[CDGPR0406] CDG Press Release: *Wideband cdmaOne Technology Endorsed by Telecommunications Industry Association (TIA) groups*, CDG, Costa Mesa, 6.Apr.1998

[CHB97] Gibson J.D : The Communications Handbook , CRC press, 1997, ISBN 0-8493-8349-8

[Cl98] Clarke P.: *Air Interface choice could dictate divergence or global harmony*, Electronic Engineering Times, p 16, January 1998

[Do98] NTT/DoCoMo: *W-CDMA System Description for Experimental W-CDMA Mobile Station,* NTT/DoCoMo, Japan, January 1998

[DPR0304] NTT/DoCoMo Press Release: *A Next-Generation mobile communications system meeting the needs of mobile multi-media.* NTT/DoCoMo, 3.Apr.1998

[EPR1702] ETSI press release: *Agreement reached on radio interface for third generation mobile system, UMTS (Universal Mobile Telecommunications System)*, ETSI,17.Feb.1998

[ETR1201] ETR 12-01 version 2.0.0: *Special Mobile Group (SMG); Framework for satellite integration within the Universal Mobile Telecommunications system (UMTS).* ETSI, 1994

[GSM0102] ETSI. European digital cellular telecommunications system (Phase 2): *General Descriptions of a GSM PLMN* (GSM 01.02). ETSI, Sophia Antipolis, 1993

[ISO13712] ISO 13712-1,ISO 13712-2, ISO-13712-3: *Information technology - Remote operations,* ISO/IEC, April 1995

[LEK97] Leite F., Engelman R., Kodama S., Mennenga H., Towaij S.: *Regulatory Considerations Relating to IMT-2000,* IEEE Personal Communications, pp. 14-19, August 1997

[MB92] Mouly, M., Pautet, M-B., *The GSM system for Mobile Communications. Published by the authors. France, 1992. ISBN 2-9507190-0-7*

[Me97] Mehtora A.: *GSM system engineering.* Artech House Publishers, 1997, ISBN 0-89006-860-7

[MO96A] Malka J., Ojanperä E.: *Advanced User's Guide for CVOPS 6.1.* Technical Research Centre of Finland, Helsinki, December 1996

[MO96R] Malka J., Ojanperä E.: *Reference Manual for CVOPS 6.1.* Technical Research Center of Finland, Helsinki, December 1996

[MO96U] Malka J., Ojanperä E.: *User's Guide for CVOPS 6.1.* Technical Research Center of Finland, Helsinki, December 1996

[NPR0304] Nokia Press Release: *Nokia to participate in Japanese 3rd generation Digital Cellular Development.* Nokia, Helsinki, 3.Apr.1998

[OP98] Ojanperä T., Prasad R.: *Wideband CDMA for third generation mobile communications.* Artech House, Boston, 1998. ISBN 0-89006-735-X

[Pa98] Parker T.: *US forges its own road into Third Generation,* Mobile Communications International, pp. 39-41, June 1998

[Q1701] ITU-T Recommendation Q.1701 Version 4.2 – *Framework for IMT-2000 Networks,* ITU, Geneva, May 1998

[RCR27F] ARIB RCR STD-27F: *Personal Digital Cellular Telecommunication System ARIB Standard – Revision F.,* ARIB, Japan, Feb 1997

[UMTS3001] UMTS 30.01 draft version 3.2.0: *Positions on UMTS agreed by SMG*, ETSI, Sophia Antipolis, December 1997

[UWCCCONT] ITU-R U.S. TG8/1: *TR-45 Proposed RTT Submission (UWC-136)*. ITU-R, June 1998

[UWCCPR2302] UWCC Press Release: *Universal Wireless Communications Consortium (UWCC) Announces UWC-136, the TDMA IS-136 Solution for Third Generation*, UWCC, Atlanta, 23.Feb.1998

[X690] ITU-T X.690: *Information technology – ASN.1 Encoding rules: Specification of basic encoding rules (BER), canonical encoding rules (CER) and distinguished encoding rules (DER).*ITU-T, December 1997

APPENDIX A: LAYER 3 MESSAGES

Radio Resource Control:

RRC establish and manages the radio bearer connections. Management is a broad concept, which includes power control, handovers, and bearer capability handling. There are only a few messages, but multiple different types of information elements.

Radio bearer management, handover, power control, and multicall handling specific messages

Purpose	Establishment and modification of radio bearer, handover, power control, and multicall signaling. These messages are used after SDCCH signaling channel has been established.
Messages	ACCESS RADIO LINK SETUP (RNC->MS) *L3 RR Assignment command* ACCESS RADIO LINK SETUP RESPONSE (MS->RNC) *L3 RR Assignment complete* ACCESS RADIO LINK RELEASE (RNC->MS) *L3 RR Channel release* ACCESS RADIO LINK RELEASE COMPLETE (MS->RNC) *L2 LAPDM DISC/UA* ACCESS RADIO LINK FACILITY (MS->RNC) *L3 RR Measurement report* *L3 RR Channel Mode Modify Acknowledge* ACCESS RADIO LINK FACILITY (RNC->MS) *L3 RR Handover Command* *L3 RR Channel Mode Modify* *L3 RR Frequency Redefinition*

SDCCH release specific messages:

Purpose	Release SDCCH signaling channel
Messages	SDCCH RELEASE (BTS -> MS)
	L3 RR Channel release
	SDCCH RELEASE COMPLETE (MS -> BTS)
	L2 LAPDM DISC / UA

Common Channel Signaling Protocol (Others)

Others consist of a number of protocols, which do not have protocol discriminators. They work together with RRC by preparing the mobile station for radio communication.

BCCH channel

Broadcast messages *(Radio Interface BCCH protocol)*

Purpose	Inform mobile station from different system parameters.
Messages	BROADCAST INFORMATION 1 (BTS -> MS)
	L3 RR System Information Type 1 to 4
	BROADCAST INFORMATION 2 (BTS -> MS)
	L3 RR System Information Type 1 to 4

RACH/FACH channel

SDCCH establishment messages *(SDCCH Setup protocol)*

Purpose	Setup and release SDCCH signaling channel
Messages	SIGNALING CHANNEL SETUP REQUEST (MS -> BTS)
	L3 RR Channel Request
	SIGNALING CHANNEL SETUP RESPONSE (BTS -> MS)
	L3 RR Immediate Assignment
	SIGNALING CHANNEL SETUP FAILURE (BTS -> MS)
	L3 RR Immediate Assignment Reject

Packet data control messages *(Packet Control protocol)*

Purpose	Packet control within radio interface
Messages	PACKET ACCESS RADIO LINK DEACTIVATION REQUEST (MS -> BTS) --- PACKET ACCESS RADIO LINK DEACTIVATION SETUP (BTS -> MS) --- PACKET ACCESS RADIO LINK DEACTIVATION SETUP RESPONSE (MS -> BTS) – *possible also on UPCH* – --- COMMON PACKET ACCESS RADIO LINK ACTIVATION REQUEST (MS-> BTS) --- COMMON PACKET ACCESS RADIO LINK ACTIVATION SETUP (BTS -> MS) --- COMMON PACKET ACCESS RADIO LINK ACTIVATION RESPONSE (MS -> BTS) --- DEDICATED PACKET ACCESS RADIO LINK ACTIVATION REQUEST (MS->BTS) --- DEDICATED PACKET ACCESS RADIO LINK ALTERNATION SETUP (BTS->MS) ---

PCH-channel

PCH messages *(Radio Interface PCH protocol)*

Purpose	Page user for the 1st incoming call
Messages	PAGING (BTS -> MS) *L3 RR Paging Request Type 1-3*

UPCH-channel

Code alternation messages *(Packet Control protocol)*

Purpose	Modification of dedicated packet access channel code
Messages	CODE ALTERNATION REQUEST (BTS->MS) --- CODE ALTERNATION RESPONSE (MS->BTS) ---

Terminal Association Control

TAC is used to establish an association between the mobile user and the mobile terminal during MOC and MTC. TAC also sends the initial layer 3 messages and receives their responses.

Mobile Originated Call specific messages:

Purpose	Terminal association in mobile originated call
Messages	TERMINAL ASSOCIATION SETUP (MS -> MSC) *L3 MM CM Service Request* TERMINAL ASSOCIATION CONNECT (MSC -> MS) *≈ L3 MM CM Service Accept*

Mobile Terminated Call specific messages:

Purpose	Terminal association in mobile terminated call
Messages	PAGING RESPONSE (MS -> MSC) *L3 RR Paging Response* PAGE AUTHORIZED (MSC -> MS) ----------

Mobility Management

Mobility Management takes care of user privacy protection and location management. Privacy protection consists of authentication, ciphering, and identity privacy management.

Location management specific messages:

Purpose	Location update messages
Messages	MOBILITY FACILITY – TERMINAL LOCATION REGISTRATION – Invoke *L3 MM Location Update Request* MOBILITY FACILITY – TERMINAL LOCATION REGISTRATION – return result *L3 MM Location Update Accept*

Authentication and ciphering management specific messages:

Purpose	Authentication of user and initiation of ciphering.
Messages	MOBILITY FACILITY – AUTHENTICATION CHALLENGE – Invoke *L3 MM Authentication Request* MOBILITY FACILITY – AUTHENTICATION CHALLENGE – return result *L3 MM Authentication Response* MOBILITY FACILITY – START CIPHERING – Invoke *L3 RR Ciphering Mode Command* MOBILITY FACILITY – START CIPHERING – return result *L3 RR Ciphering Mode Complete*

Identity privacy management specific messages:

Purpose	User privacy protection
Messages	MOBILITY FACILITY – TMUI ASSIGNMENT – Invoke *L3 MM TMSI Reallocation Command* MOBILITY FACILITY – TMUI ASSIGNMENT – return result *L3 MM TMSI Reallocation Complete* MOBILITY FACILITY – IMUI RETRIEVAL – Invoke *L3 MM Identity Request* MOBILITY FACILITY – IMUI RETRIEVAL – return result *L3 MM Identity Response*

Error handling messages:

Purpose	Handling of different type of error situations.
Messages	MOBILITY FACILITY – <OPERATION> – reject ---------- MOBILITY FACILITY – <OPERATION> – return error ----------

Call Control

Call Control negotiates the quality requirements, bearer capabilities, and transfer rate of a connection. Call Control can also change properties of connection, handle multiple connections to the same terminal, and release call.

Call establishment and multicall handling specific messages:

Purpose	Establishment of call, bearer negotiations and multicall handling.
Messages	SETUP (MS<->MSC)
	L3 CC Setup
	CALL PROCEEDING (MS<->MSC)
	L3 CC Call Proceeding
	ALERTING (MS<->MSC)
	L3 CC Alerting
	CONNECT (MS<->MSC)
	L3 CC Connect
	CONNECT ACKNOWLEDGE (MS<->MSC)
	L3 CC Connect acknowledge

Call release specific messages:

Purpose	Release of call.
Messages	RELEASE (MS<->MSC)
	L3 CC Release
	RELEASE COMPLETE (MS<->MSC)
	L3 CC Release Complete

APPENDIX B: TRACING LEVELS

Level 1.

```
....

 : send to mmnws mgtMm_MSidFound

dstCEPid :1

: r
  MMMS.CON_.1              PEER<- : MF_AC_INVOKE
  MMNWS.CON_.1             PEER<- : MF_AC_RESULT
  MMMS.CON_.1              PEER<- : MF_SC_INVOKE
  MMNWS.CON_.1             PEER<- : MF_SC_RESULT

....
```

Level 2.

```
...

: send to mmnws mgtMm_MSidFound

dstCEPid :1

: r

  MMMS.CON_.1              PEER<- : MF_AC_INVOKE
                                01 00 22 02 10 05 A1 0E 02 01 01 02
                                01 03 31 06 80 01 2A 81 01 2A

  MMNWS.CON_.1             PEER<- : MF_AC_RESULT
                                01 00 22 02 0B 05 A2 09 02 01 02 02
                                01 03 04 01 2A

  MMMS.CON_.1              PEER<- : MF_SC_INVOKE
                                01 00 22 02 0B 05 A1 09 02 01 01 02
                                01 04 04 01 2A

  MMNWS.CON_.1             PEER<- : MF_SC_RESULT
                                01 00 22 02 08 05 A2 06 02 01 02 02
                                01 04
...
```

Level 3.

```
...

: send to mmnws mgtMm_MSidFound

dstCEPid :1

: r
  MMNWS.CON_.1              RES3<- : mgtMm_MSidFound

  MMMS.CON_.1               DOWN<- : rbcMm_dti

  MMMS.CON_.1               PEER<- : MF_AC_INVOKE
                                 01 00 22 02 10 05 A1 0E 02 01 01 02
                                 01 03 31 06 80 01 2A 81 01 2A
  MMNWS.CON_.1              DOWN<- : rbcMm_dti

  MMNWS.CON_.1              PEER<- : MF_AC_RESULT
                                 01 00 22 02 0B 05 A2 09 02 01 02 02
                                 01 03 04 01 2A
  MMMS.CON_.1               DOWN<- : rbcMm_dti

  MMMS.CON_.1               PEER<- : MF_SC_INVOKE
                                 01 00 22 02 0B 05 A1 09 02 01 01 02
                                 01 04 04 01 2A

  MMNWS.CON_.1              DOWN<- : rbcMm_dti

  MMNWS.CON_.1              PEER<- : MF_SC_RESULT
                                 01 00 22 02 08 05 A2 06 02 01 02 02
                                 01 04
```

Level 4

```
...

: send to mmnws mgtMm_MSidFound

dstCEPid :1

: r


  MMMS.CON_.1               PEER<- : MF_AC_INVOKE
                                 01 00 22 02 10 05 A1 0E 02 01 01 02
                                 01 03 31 06 80 01 2A 81 01 2A
```

```
--- Message found: AC_INVOKE --

AC-Invoke (SET, header)
{
 execution-authentication-type (OCTET STRING) =
 2A
 authentication-random-pattern (OCTET STRING) =
 2A
}

--- End of AC_INVOKE ---------


  MMNWS.CON_.1              PEER<- : MF_AC_RESULT
                                01 00 22 02 0B 05 A2 09 02 01 02 02
                                01 03 04 01 2A

--- Message found: AC_RESULT --

AC-result (OCTET STRING) =
2A

--- End of AC_RESULT ---------


  MMMS.CON_.1               PEER<- : MF_SC_INVOKE
                                01 00 22 02 0B 05 A1 09 02 01 01 02
                                01 04 04 01 2A

--- Message found: SC_INVOKE --

SC-Invoke (OCTET STRING) =
2A

--- End of SC_INVOKE ---------


  MMNWS.CON_.1              PEER<- : MF_SC_RESULT
                                01 00 22 02 08 05 A2 06 02 01 02 02
                                01 04


--- Message found: SC_RESULT --

 NO INFORMATION ELEMENTS

--- End of SC_RESULT ---------

...
```

Level 5 and Level 6

```
...

: send to mmnws mgtMm_MSidFound

dstCEPid :1

: r
  MMNWS.CON_.1              RES3<- : mgtMm_MSidFound


  MMMS.CON_.1               DOWN<- : rbcMm_dti


  MMMS.CON_.1               PEER<- : MF_AC_INVOKE
                                01 00 22 02 10 05 A1 0E 02 01 01 02
                                01 03 31 06 80 01 2A 81 01 2A

--- Message found: AC_INVOKE --

AC-Invoke (SET, header)
{
 execution-authentication-type (OCTET STRING) =
 2A
 authentication-random-pattern (OCTET STRING) =
 2A
}

--- End of AC_INVOKE ---------

  MMNWS.CON_.1              DOWN<- : rbcMm_dti


  MMNWS.CON_.1              PEER<- : MF_AC_RESULT
                                01 00 22 02 0B 05 A2 09 02 01 02 02
                                01 03 04 01 2A

--- Message found: AC_RESULT --

AC-result (OCTET STRING) =
2A

--- End of AC_RESULT ---------

  MMMS.CON_.1               DOWN<- : rbcMm_dti


  MMMS.CON_.1               PEER<- : MF_SC_INVOKE
                                01 00 22 02 0B 05 A1 09 02 01 01 02
                                01 04 04 01 2A

--- Message found: SC_INVOKE --

SC-Invoke (OCTET STRING) =
2A

--- End of SC_INVOKE ---------
```

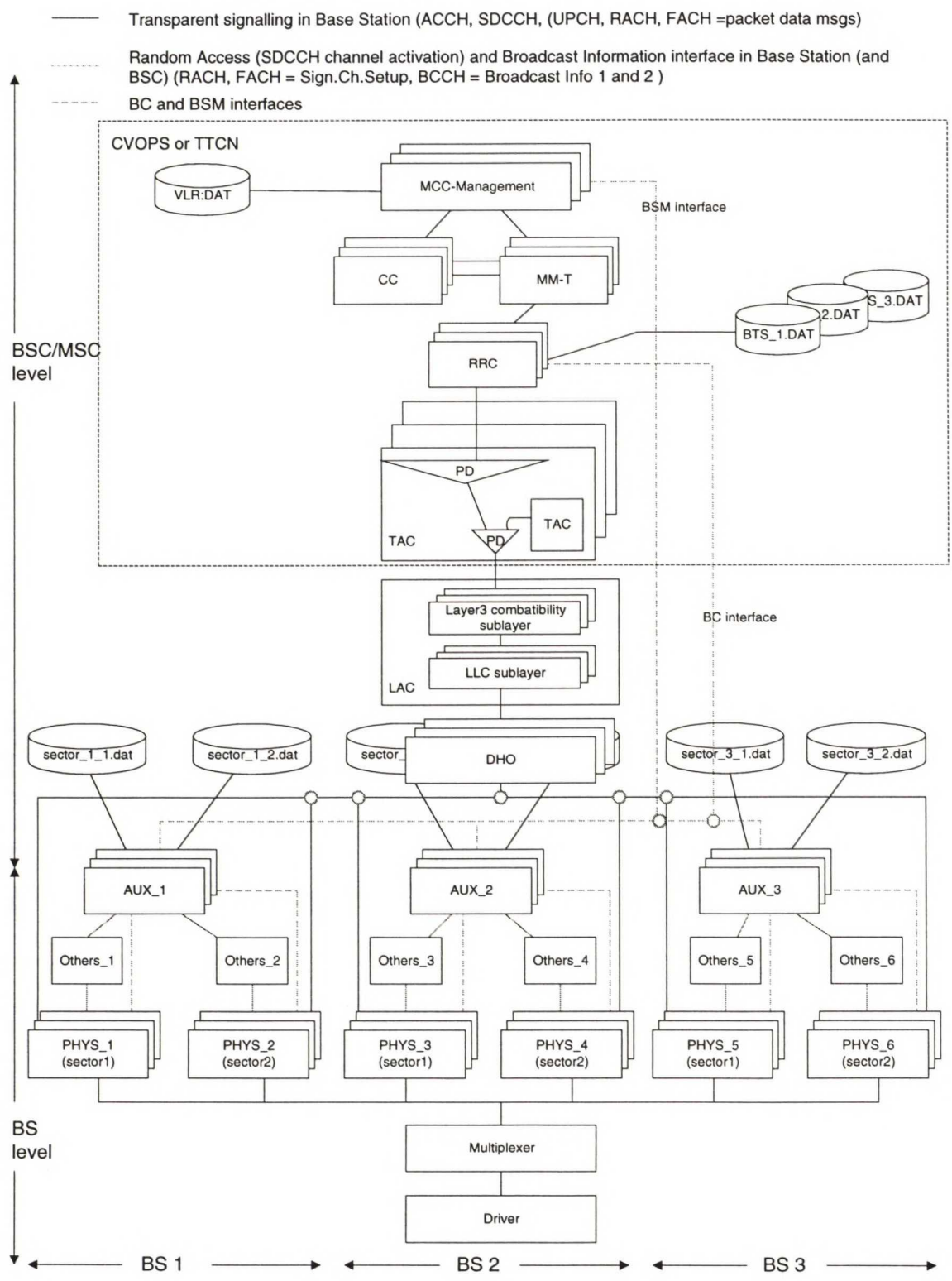
```
  MMNWS.CON_.1              DOWN<- : rbcMm_dti


  MMNWS.CON_.1              PEER<- : MF_SC_RESULT
                                  01 00 22 02 08 05 A2 06 02 01 02 02
                                  01 04


--- Message found: SC_RESULT --

 NO INFORMATION ELEMENTS

--- End of SC_RESULT ---------

...
```

Level 7

```
...

: send to mmnws mgtMm_MSidFound

dstCEPid :1

: r
  MMNWS.CON_.1              RES3<- : mgtMm_MSidFound

--- PRIMITIVE PARAMETER TRACE ON --

  MMMS.CON_.1               DOWN<- : rbcMm_dti

--- PRIMITIVE PARAMETER TRACE ON --

  MMMS.CON_.1               PEER<- : MF_AC_INVOKE
                                  01 00 22 02 10 05 A1 0E 02 01 01 02
                                  01 03 31 06 80 01 2A 81 01 2A

--- Message found: AC_INVOKE --

AC-Invoke (SET, header)
{
 execution-authentication-type (OCTET STRING) =
 2A
 authentication-random-pattern (OCTET STRING) =
 2A
}

--- End of AC_INVOKE ---------

  MMNWS.CON_.1              DOWN<- : rbcMm_dti

--- PRIMITIVE PARAMETER TRACE ON --

  MMNWS.CON_.1              PEER<- : MF_AC_RESULT
                                  01 00 22 02 0B 05 A2 09 02 01 02 02
                                  01 03 04 01 2A
```

```
--- Message found: AC_RESULT --

AC-result (OCTET STRING) =
2A

--- End of AC_RESULT ---------

  MMMS.CON_.1              DOWN<- : rbcMm_dti

--- PRIMITIVE PARAMETER TRACE ON --

  MMMS.CON_.1              PEER<- : MF_SC_INVOKE
                               01 00 22 02 0B 05 A1 09 02 01 01 02
                               01 04 04 01 2A

--- Message found: SC_INVOKE --

SC-Invoke (OCTET STRING) =
2A

--- End of SC_INVOKE ---------

  MMNWS.CON_.1             DOWN<- : rbcMm_dti

--- PRIMITIVE PARAMETER TRACE ON --

  MMNWS.CON_.1             PEER<- : MF_SC_RESULT
                                01 00 22 02 08 05 A2 06 02 01 02 02
                                01 04


--- Message found: SC_RESULT --

 NO INFORMATION ELEMENTS

--- End of SC_RESULT ---------

...
```

APPENDIX C: MS-TESTER PROTOCOL ARCHITECTURE

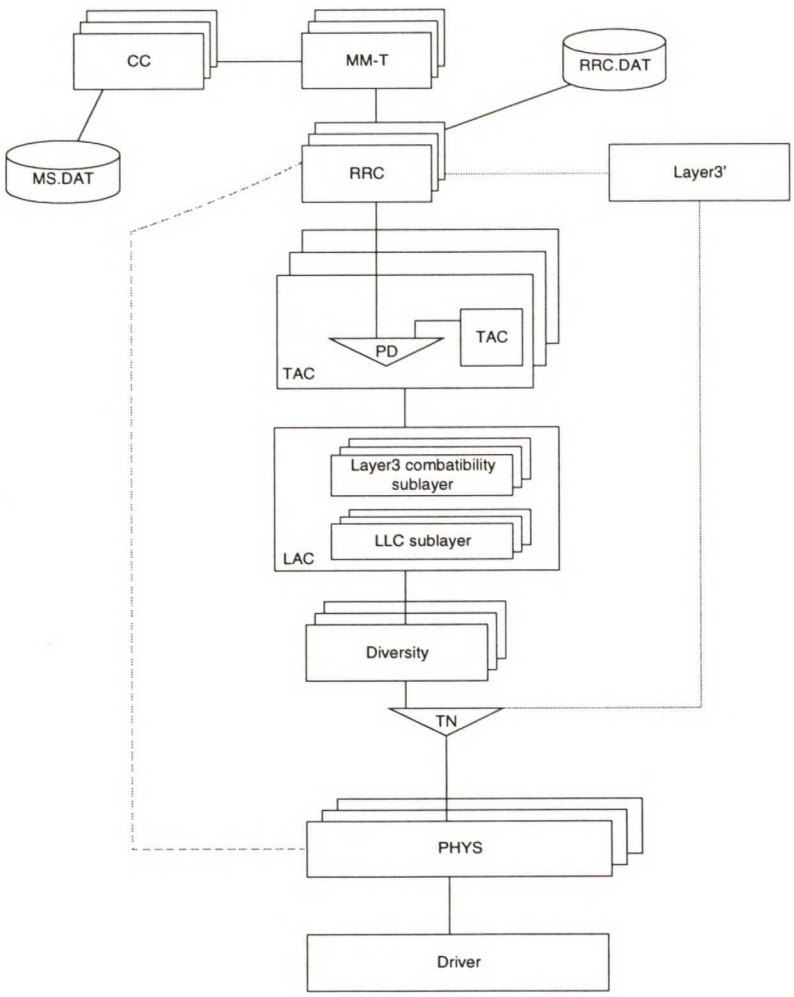


APPENDIX D: MS-SIM PROTOCOL ARCHITECTURE

——— Transparent signalling through Base Station (ACCH, SDCCH, (UPCH, RACH, FACH =packet data msgs)

..... Semi-Transparent signalling in Base Station (RACH, FACH = Sign.Ch.Setup, PCH = Paging, BCCH = Broadcast Info 1 and 2)

- - - - - Channel Allocation requests




TEKNILLINEN OSASTO