University of Piraeus

DEPARTMENT OF DIGITAL SYSTEMS

POSTGRADUATE STUDY PROGRAM
IN TECHNO-ECONOMIC MANAGEMENT AND SECURITY OF INFORMATION SYSTEMS

Direction: Security of Information Systems

Security Analysis for 3G Radio Interface

Chrysoula P. Sklia

MTE/0927

Supervisor Professor: Prof. Christos Xenakis

ATHENS

DECEMBER 2012

DIPLOMA THESIS

Security Analysis of 3G Radio Interface

Chrysoula P. Sklia

MTE/0927

SUPERVISOR:

Christos Xenakis

December 2012

ABSTRACT

As the GSM technology evolved and mobile cellular technology has become very popular, security threats that exploited the main drawbacks of GSM have made their appearance. GSM was designed with a moderate level of security, where the subscriber is authenticated in the network.

The Universal Mobile Telecommunication System (UMTS) in one of the Third Generation mobile cellular communication systems. UMTS in build on the success of the Second Generation GSM system, and also improves its security features. In the UMTS networks not only the user is authenticated to the network, but also the network is authenticated to the user.

Despite the fact that some important security issues of GSM are addressed in UMTS, there are still some points of vulnerability. The TMSI and sometimes the IMSI is still transmitted over the network, making it possible to an attacker to collect various IMSIs and TMSIs using an IMSI catcher, and thus impersonate the user in the network. When this info is appropriately used by an adversary, denial of Service attacks may occur. Using the specific TMSIs an adversary can initiate a number of RRC Connections, which is the primary step for authenticating to the network. If the number of RRC Connections initiated is more than the limit that the network infrastructure can handle, this can cause a break down of the Node B and potentially the HLR, thus not being able to serve more calls.

The object of study in this diploma thesis is the UMTS Network Security Architecture, specifically in the Radio Access Network (UTRAN). After analyzing the architecture of the UMTS Network and the UTRAN Security Architecture, we attempt to make an estimation of the max number of RRC connections that can be transmitted in the UTRAN Interface.

SUBJECT AREA: Security in 3G Network Interface

WORD KEYS: Security, 3G Networks, UMTS, UTRAN, RRC Connections, Capacity of UTRAN RRC Connections

Acknowledgments

This thesis was produced as part of the Post graduate program "Digital Systems Security" of University of Piraeus. However, the realization would not have been possible without the help of some people.

I would like to express my gratitude to the Direct Supervisor of my thesis Christos Xenakis for giving me the opportunity to work on such a modern and interesting object. His guidance and patience was very important for concluding this thesis.

Finally I would like to thank my family and my friends who always stood beside me, supported me and filled me with courage throughout the course of my studies.

December 2012

Chrysoula P. Sklia

Table of Contents

Table of Figures

1 Introduction

1.1 Objective of this Diploma Thesis

The UMTS Technology offers its success in its predecessor the GSM. Since the GSM was not built to have very strong security, the UMTS should address the security issues of the GSM. One important security feature of the GSM is the double authentication of the user and the Network. This means that in UMTS, not only the user is authenticated to the Network, but also the network is authenticated to the user.

During this authentication process of the user towards the network, an RRC Connection is established between the User Equipment (UE) and the Radio Network Controller (RNC).

The RRC Connection is a handshake process consisting of three messages, the RRC Connection Request, the RRC Connections Setup and the RRC Connection Setup Complete. After the last message is exchanged, the RRC Connection is established, and the authentication process begins.

One important observation is that the TMSI of the subscriber is used in the RRC Connection request and is transferred unencrypted over the Radio Network Interface.

So if an adversary can have a way of obtaining a large number of TMSIs, he could initiate a large number if RRC Connections, thus flooding the RNC with more requests that it can handle. Such an attack could lead to a Denial of Service attack, causing the Node Bs, the RNC and potentially the HLR, not to be able to serve any more authentication requests, since they will be overloaded.

So in this Diploma Thesis we present the overall security architecture of the UMTS Radio Network Interface, paying special attention in the way an RRC Connection is established. At the last chapter, we initiate an attempt of calculating the maximum capacity of RRC Connections that can be initiated towards an RNC. Based on this formula, an adversary could initiate an attack, by flooding the RNC with more RRC connection request than the node can handle.

1.2 Organization of the Thesis

This Thesis is organized in six chapters. The present chapter is the Introduction.

In Chapter 2 we present the Architecture or the UMTS Network, examining the tree key concepts of the UMTS, the User Equipment (UE), the Access Network (UTRAN), and the Core Network (CN). In this chapter also a presentation of the basic addresses and identifiers used in the UMTS Network

In Chapter 3 we present the UMTS Security Architecture by examining possible attacks in the UMTS Networks and the Authentication and Key Agreement protocol.

In Chapter 4 we are making a thorough analysis of the UMTS Radio Access Network, presenting the UTRAN Architecture and the concepts of the Access and Non Access Stratum. Further we present the Radio Interface Protocol, and we examine in details the Radio Resource Control Interface.

In Chapter 5 we present the way of calculating the capacity of the RRC Connection in the Uplink Interface.

In Chapter 6 we present the conclusions that are derived from this Thesis.

In Chapter 8 we present the Abbreviations used throughout the thesis.

In Chapter 8 we present the Bibliography and the References used.

2 UMTS Network

The UMTS Network is consisted of 3 basic subsystems, the User Equipment (UE), the Access Network (AN) and the Core Network (CN)

UMTS is a mobile cellular third generation system used from mobile devices around the world which has as main characteristic high traffic rates of data transmission. The UMTS technology offers a large set of services to end users around the world, no matter where they are located.

The UMTS network architecture as well as the network architecture that support roaming in 3G is consisted of tree parts as shown in Figure 1:

1. The User Equipment (UE)
2. The UMTS Terrestrial Radio Access Network (UTRAN)
3. Core Network

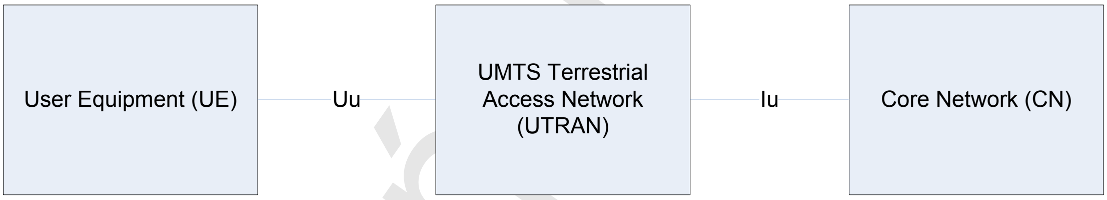


Figure 1: UMTS basic network structure

The User Equipment is used by a subscriber/ user to access the services provided by the network. To connect to the network, a UE interfaces with the Access Network using the WCDMA air interface which is referenced as the Uu interface. Two modes of operation are used by the Uu interface: the Frequency Division Duplex (FDD) for the paired spectrum and the Time Division Duplex (TDD) for the unpaired spectrum.

The UMTS Terrestrial Radio Access Network (UTRAN) allows connectivity between the User Equipment (UE) and the Core Network (CN). The UTRAN is consisted of a number of base stations, called Node Bs, and controlling nodes, which are called Radio Network Controllers (RNC). The Radio Network controllers are connected to the Core Network.

The Core Network performs the core functions of the network which include mobility management, call control, switching and routing. The core network also manages the subscription information of a subscriber and provides services based on the information.

2.1 User Equipment

The UMTS User Equipment (UE) is not a simple mobile phone but rather, a mobile multimedia terminal able to provide simultaneously voice, video and data services.

The UMTS standards do not impose the physical aspect of the UE (size, weight, type of display/keyboard, etc.). The look-and-feel of the UE depends on each mobile equipment manufacturer. The difference between UEs may come from their capability to provide a certain number of services – there is no mandatory set of services imposed by the UMTS standards either.

Therefore, in the mobile market we can find UEs offering: speech-only, video-telephony only, Internet-access only, streaming-only, or a combination of all above. The UEs may also differ from each other according to their radio access capability. They can be dual-mode and allow seamless service provision across 2G and 3G networks. Examples are GSM + UTRA/FDD, GSM + GPRS + UTRA/FDD, GSM + EGPRS + UTRA/FDD, GSM + EGPRS + UTRA/FDD + HSDPA. This possibility shall take into consideration the bearer limitation of each technology (e.g. an active video-telephony call cannot be maintained when roaming from UMTS to GSM). [1]

2.1.1 Components of User Equipment

The User Equipment is divided into two components:

1. Mobile Equipment (ME)
2. Universal Integrated Circuit Card (UICC)

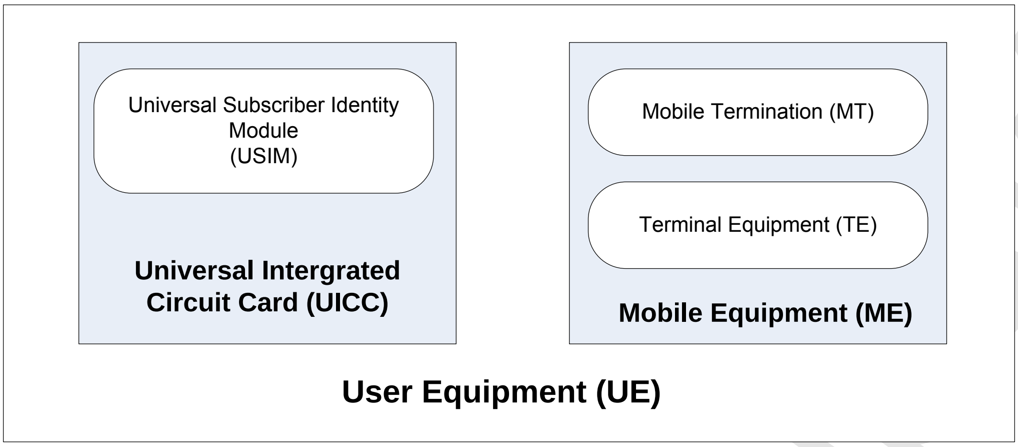


Figure 2: User Equipment Components

The UICC is a smart card that contains an application called Universal Subscriber Identity Module (USIM). The USIM contains the logic required to unambiguously and securely identify the user. Thus the USIM is the user dependent part of the UE and is provided from the Service Provider.

The ME equipment on the other part is the user independent part of the UE. The ME is usually manufactured by an equipment manufacturer who is usually a different identity than the service provider. The ME is further divided in two entities, the Mobile Termination (MT) and the Terminal Equipment (TE) [2]

2.1.2 USIM

The UMTS user service identity module (USIM) shall contain sufficient information to identify the user and service provider. USIM is a UMTS specific application residing on a removable IC card and is required for service provision. Authentication and ciphering functionality may be part of USIM or some other application on the same or different IC card. The UMTS IC card could also support applications other than UMTS USIM application in order to allow more versatile UMTS IC card functionality such as access to value-adding services.

The mandatory requirements for IC Cards used for holding USIM application are related to the need to have one USIM application on the IC card, as well as to the security issues [3]

Every UE may contain one or more USIM simultaneously (100% flexibility). Higher layer standards like MM/CC/SM address 1 UE + 1 (of the several) USIM when they mention a MS.

The main difference between a USIM and a GSM-SIM is that the USIM is downloadable (by default), can be accessed via the air interface, and can be modified by the network. The USIM is a Universal Integrated Circuit Card (UICC), which has much more capacity than a GSM SIM. It can store Java applications. It can also store profiles containing user management and rights information and descriptions of the way applications can be used. [4]

2.2 UTRAN

The Access Network (AN) resides between the UE and the Core Network. It performs the functions related to the access technique. Specifically for the UMTS the Access Network performs functions specific to the access of WCDMA air interface.

The Access Network is called Base Station Subsystem (BSS) for GSM and Radio Network Subsystem (RNS) for UMTS. The Radio Network subsystem is also known as the Universal Terrestrial Access Network (UTRAN)

Both types of Access Systems – the BSS and RNS- have a similar structure. They comprise of a Base Station Controller (BSC) and one or more Base Transceiver Station (BTS). The BTS terminates the radio connection with the UE. The BSC controls one or more BTS. In Radio Network Subsystem (RNS), the BTS is referred to as Node B, while the BSC as Radio Network Controller.

A Radio Network Controller (RNC) is a network component in the PLMN that executes functions for controlling of one or more Node B.

A Node B is a logical network component which serves one or more cells. [5]

The UTRAN architecture is examined in details in Section 4.1

2.3 Core Network

When a UMTS subscriber originates (or terminates) a call to access circuit- or packet-switched services, the connection is controlled by the core network. If the desired service is provided by an external network, the core network further provides interworking functionality. The core network also manages the mobility of the UE within its home network (i.e. the network where the subscription data is stored) and within a visited network in the case where the UE is roaming. Finally, the core network performs high-level security functions such as location updating and authentication, and controls charging and accounting aspects.

Overall the functions supported from the Core Network are:

- Mobility Management
- Call Control
- Switching
- Session Management
- Routing
- Authentication
- Equipment Identification

The logical structure of the Core Network can be found in the Figure below:

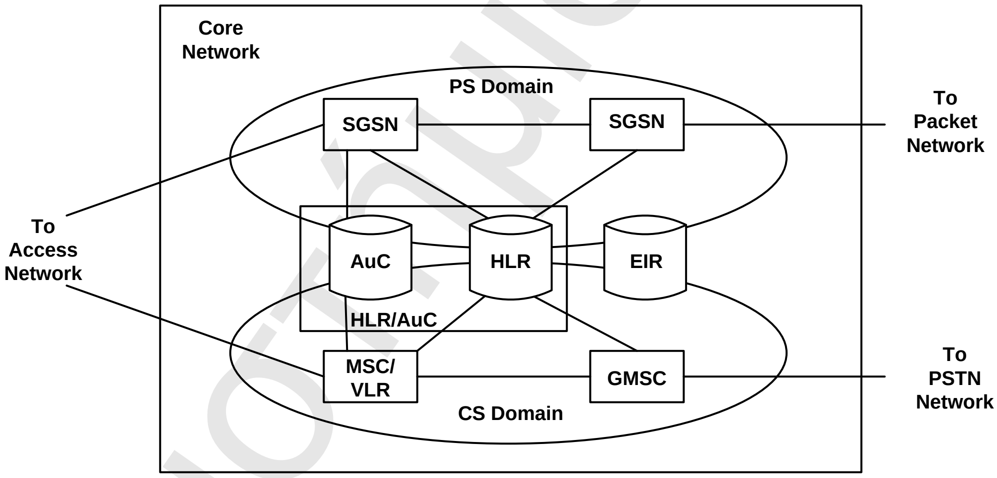


Figure 3: Logical Structure of Core Network

The CN is constituted of a Circuit Switched (CS) domain and a Packet Switched (PS) domain. These two domains differ by the way they support user traffic, as explained bellow.

These two domains are overlapping, i.e. they contain some common entities. A PLMN can implement only one domain or both domains.

2.3.1 Circuit Switched Domain

The CS domain uses Circuit switched connections for communication between UE and the destination. A CS connection is defined as a connection for which dedicated network resources are allocated at the time the connection is established and are freed when the connection is released. An example of CS connection is the connection established in the PSTN network during a telephonic conversation.

To establish/release CS connection and to switch voice streams a switching entity is required. For this the CS network has the Mobile Switching Center (MSC). Alongside the MSC there is the Visit Location Registry (VLR) which contains the subscribers profile obtained from the Home Location Registry (HLR). MSC requires from the VLR the subscriber information and provides services to the subscriber based on this information.

Apart from the MSC/VLR the CS has the Gateway Mobile Switching Center (GMSC) for providing connectivity to external CS networks, including the CS domain of other UMTS and PSTN networks)

2.3.2 Packet Switched Domain

The PS domain uses the Packet Switched (PS) connections for communication between the UE and the destination. A PS connection is defined as a connection that transports the user information using autonomous concatenation of bits called packets; each packet is routed independently of the previous one. An important aspect of PS connections is that resources are not reserved for a connection, but they are shared between various communication entities. This sharing of resources results in better resource utilization. An example of PS connection is the connectionless transfer of IP datagrams in the Internet.

To route packets in the PS domain, a routing entity is required and for this the PS domain has the Serving GPRS Support Node (SGSN). Unlike CS domain, where one entity holds the database (VLR) and another switch the connections (MSC), in PS domain the SGSN performs both functions. Apart from the SGSN the PS domain has the Gateway GPRS Support Node (GGSN) which performs functions similar to the GMSC, meaning that GGSN provides connectivity to external PS networks.

Also there are entities that are common both the CS and the PS domain. Among these id the HLR that is located in the subscriber’s home network. The HLR holds permanent and subscribed information of the subscriber. The permanent information includes the permanent identity of the subscriber, called IMSI. The subscribed information includes information about the services that are provisioned in the HLR, for example if the used is prepaid, or has Number Portability enabled.

Apart from the HLR, one important common node is the Authentication Center (AuC) which holds authentication information. This information is used for authentication and other security related functions. Usually the AuC is presented as part of the HLR. One more common entity between the CS and the PS domain is the Equipment Identity Register (EIR). The EIR monitors the legitimacy of a User Equipment (UE) used in the UMTS Network.

2.4 Addresses and Identifiers

In UMTS a number of identifiers are used for the purpose of addressing and identification. Each identifier serves a specific purpose. First is the International Mobile Subscriber Identity (IMSI) that uniquely identifies a subscriber. An IMSI may be associated with multiple Mobile Subscriber ISDN (MSISDN) numbers. The MSISDN can be viewed as the mobile phone numbers or the service identity. Apart from these identifiers there is a temporary identifier, TMSI, which is used to hide the IMSI.

While MSISDN is relevant in the CS domain, the equivalent entity in the PS domain is the Packet Data Protocol (PDP) address. In simple terms the PDP address identifies the network address using which identities outside the PS domain communicate with the MS.

Also there is the International Mobile Equipment Identity (IMEI) which uniquely identifies the MS.[6]

Then there are also E.164 addresses, used to identify network entities.

2.4.1 Subscriber Identity

A subscriber is uniquely identified by its International Mobile Subscriber Identity (IMSI). The IMSI is stored in the USIM and kept hidden from ordinary access. As shown in Figure 4, the IMSI is divided in three distinct parts.

The first three digits of the IMSI form the Mobile Country Code (MCC). The MCC identifies the country of domicile of the mobile subscriber.

The next two or three digits form the Mobile Network Code (MNC). The MNC identifies the home PLMN of the subscriber. The last field of IMSI is the Mobile Subscriber Identification Number (MSIN). The MSIN uniquely identifies the subscriber within a PLMN. The combination of MNC and MSIN is called the National Mobile Subscribed Identity (NMSI)

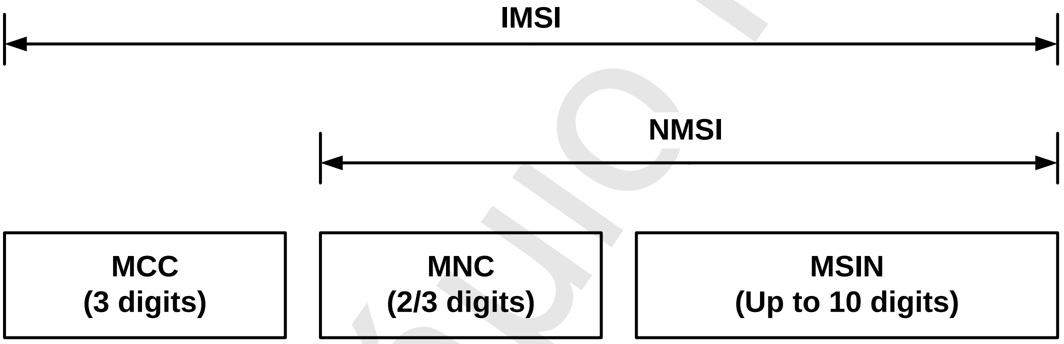


Figure 4: Structure of IMSI

2.4.2 Service Identity

The mobile number used to contact a person is the Mobile Subscriber ISDN (MSISDN) number and not the IMSI. Thus, an MSISDN, can be viewed as a service identity because a subscriber may have multiple MSISDN, where each MSISDN identifies a particular service.

The MSISDN numbers are based in the ISDN numbering plan and are allocated in such manner that fixed lines ISDN or PSTN subscriber can call any mobile subscriber. The ISDN numbering plan is based in ITU specification E.164.

Figure 5 shows the architecture of and MSISDN. Like IMSI, the MSISDN is made up to three distinct parts:

1. Country Code (CC)

2. National Destination Code (NDC)
3. Subscriber Number (SN).

There is a one to one analogy between the elements of an IMSI and an MSISDN. The basic difference between the two is the number of digits allocated to individual elements. The CC is from one to three digits.

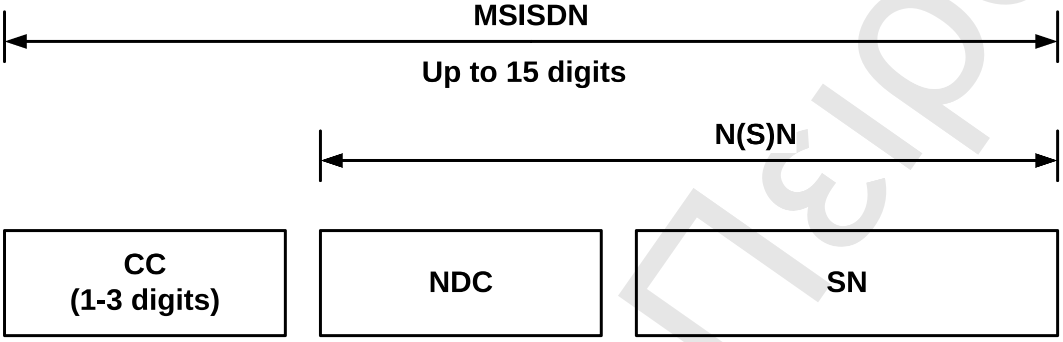


Figure 5: Structure of MSISDN

The MSISDN can have a maximum of 15 digits. The size of National (Significant) Number depends upon the size of the CC and can be of a maximum of 14 digits. (when CC is one digit).

2.4.3 Temporary Identities

Apart from the IMSI and the MSISDN there are also temporary identities used for specific purposes. These temporary identities are as follows:

- Temporary Mobile Subscriber Identity (TMSI)
- Local Mobile Station Identity (LMSI)
- Mobile Station Roaming Number (MSRN)
- Radio Network Temporary Identity (RNTI)

2.4.3.1 Temporary Mobile Subscriber Identity (TMSI)

From a security point of view there is the nee to hide the permanent identity IMSI of a subscriber. For this, a temporary identity TMSI is used on the air interface. The TMSI, or Temporary Mobile Subscriber Identity, is allocated by the VLR of the SGSN. It is also possible that two temporary identities are used, one for the CS and one for the PS domain. Under such circumstances, the identities are called TMSI and

P-TMSI for CS and PS domain respectively. The TMSI has only logical significance and is applicable within the area controlled by VLR (or SGSN).

The TMSI consists of four octets. The exact encoding of TMSI is chosen by agreement between the network operator and equipment manufacturer to suit loca needs.

2.4.3.2 Local Mobile Station Identity (LMSI)

For the purpose of optimizing database search, a VLR may use a local identifier called the Local Mobile Station Identity (LMSI). The VLR sends the LMSI to the HLR during message exchange along with IMSI/MSISDN in its database. In all further correspondence with the VLR, the HLR includes the LMSI sent earlier from the VLR. The VLR them uses the LMSI to optimize database search.

The LMSI consists of four octets and is allocated by the VLR.

2.4.3.3 Mobile Station Roaming Number (MSRN)

To facilitate Roaming, a VLR allocates a roaming number called the Mobile Station Roaming Number (MSRN). The MSRN is used to route calls directed to a MS. When a mobile terminated call is received by the GMSC, it queries the VLR (via HLR) for a number, using which, it can route the call. The VLR allocates a MSRN for the MS and passes it to HLR, which in turn forwards it to GMSC. The GMSC then used the MSRN to route the call to the MS via MSC/VLR.

The MSRN is the same format as the MSISDN, but it is not the same as the MSISDN. The MSRN is allocated by the visited network according to the numbering plan of the visited PLMN. In certain cases the MSRN may be the same as the MSISDN (for example when the subscriber is in the Home Network).

2.4.3.4 Radio Network Temporary Identity (RNTI)

While TMSI, LMSI and MSRN are allocated by Core Network, there are temporary identities allocated by the UTRAN. One such temporary identity is the Radio Network Temporary Identity (RNTI). The RNTI is used as a UE identifier to exchange signaling messages between UE and UTRAN. There are various types of RNTI.

The s-RNTI is allocated by the Sewing RNC, which is in charge of the radio connections between the UE and UTRAN. The Serving RNC allocates the s-RNTI for those UE that have a RRC connection. The s-RNTI is used by the UE to identify itself to the Serving RNC and is used by the Serving RNC, which in turn uses it (s-RNTI) to address a particular UE.

Apart from s-RNTI, there are d-RNTI, c-RNTL and few other identifiers.[7]

More details can be found on Section Mobility Handling 4.1.2

2.4.4 PDP Adress

For an MS to communicate with entities of a Packet Data Network (PDN), it must have an address appticable in the PDN. Note that the PDN lies outside the PLMN which implies that the addresses in the PLMN (like IMSI) are alone not sufficient for communication with PDN entities. Since the most common PDN is based on the Internet Protocol (IP), a MS must have an [P address for co1nmu.n.icating with other entities in the PDN. The IP address may be an lI’v4 or an IPv6 address. In either case, the MS must have an address, called the Packet Data Protocol (PDP) address, to communicate with entities in a PDN.

The PDP address is assigned either statically or allocated dynamically by the GGSN. A static PDP address is allocated by the network operator of the home PLMN. Since the allocation is static, it is of permanent nature.

However, network addresses are a scarce resource and it does not make sense to allocate them on a permanent basis, more so because a subscriber may not need to use one all the time. Hence, the addresses are generally allocated dynamically, so that a small set of these may be shared between a large number of subscribers.

A dynamic PDP address is allocated during the activation of PDP context. A PDP context can be viewed as a set of information maintained by UE, SGSN and GGSN. It contains a PDP type (that identifies the type of PDN, for example IPv4); the PDP address [say a dynamically allocated IPv4 address); Q05 information; and other session information. Activating a PDP context refers to creating the PDP context at the UE, SGSN and GGSN so that the UE can communicate with an entity in PDN using the PDP address maintained in the PDP context. After the communication is over, the PDP context is deactivated.

2.4.5 Equipment Identity

A MS is identified by its International Mobile Equipment Identity (IMEI). The IMEI is a 15-digit identifier (its structure is shown in Figure 6). The first eight-digits are the Type Allocation Code (TAC). The next six-digits are the Serial Number (SNR). The last digit is spare and is set at 0.

The IMEI is used to track stolen a MS. The IMEI of a handset can be known by typing the string #06# on the MS.

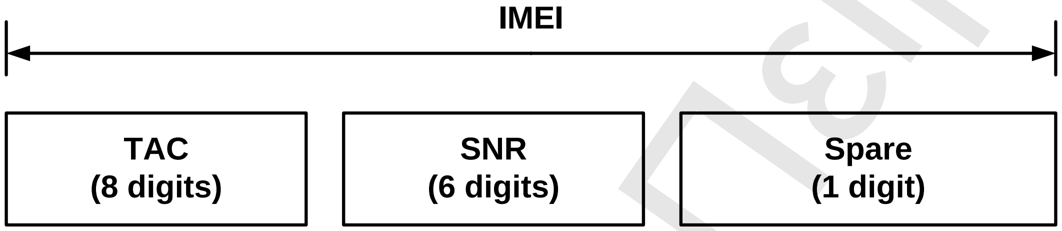


Figure 6: Structure of IMEI

3 UMTS Security Architecture

Staring from the first generation analogue mobile phone and moving to the GSM and now days on UMTS, communication security has always been a vital point.

As the UMTS was build upon the GSM, the former inherits some characteristics of the later in terms of security.

UMTS security builds on the success of GSM by retaining the security features that have proved to be needed and that are robust. As in GSM, a smart card is used in UMTS to store all the identification and security related data that the subscriber needs to make or receive a call [8]. Although GSM security has been very successful, an objective of the UMTS security design was to improve on the security of second generation systems like GSM by correcting real and perceived weaknesses [9].

Some of these weaknesses are the following [10], [11], [12]

- active attacks using a "false base station"
- cipher keys and authentication data are transmitted in clear between and within networks
- encryption does not extend far enough towards the core network and data is transmitted in clear on the microwave links
- data integrity is not provided
- user authentication on a previously generated cipher key and channel hijack depends on the use of encryption
- fraud and legal interception were not considered in the design phase but came only as after-thoughts
- 2G systems do not have the flexibility to upgrade and improve security functionality over time.

In addition to the removal of above observed deficiencies, 3G security offers new security features and services. It should be noted that the main objective of 3G security architecture is not to provide a completely secure system, but to build a system that is flexible to adapt to new challenges [13]

3.1 Possible attacks in UMTS Protocols

As the computational capabilities are increasing and new equipment becomes available, the possible intruders have more means to perform an attack in the UMTS network. [14]

In order to be able to carry out these attacks, the intruder has to possess one or more of the following capabilities:

- Eavesdropping. This is the capability that the intruder eavesdrops signaling and data connections associated with other users. The required equipment is a modified MS.
- Impersonation of a user. This is the capability whereby the intruder sends signaling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The required equipment is again a modified MS.
- Impersonation of the network. This is the capability whereby the intruder sends signaling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. The required equipment is modified BS.
- Man-in-the-middle. This is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signaling and user data messages exchanged between the two parties. The required equipment is modified BS in conjunction with a modified MS.
- Compromising authentication vectors in the network. The intruder possesses a compromised authentication vector, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signaling messages on network links.

The possible attacks identified for the UMTS network are the following:

Denial of service

The following will result in complete or partial denial of services to the target user.

1) User de-registration request spoofing: If the network cannot authenticate messages then an attacker with a modified MS can send a de-registration request to the network, which is complied by the network and simultaneously sends instructions to the Home Location Register (HLR) to do the same.
2) Location update request spoofing: Instead of sending requests for de-registration, the attacker sends a location update request from a different area from the one in which the user is presently located. As a result the user is paged in the new area.
3) Camping on a false BS/MS: The attacker with a modified BS/MS puts himself in-between the Serving Network (SN) and the target user.

Identity catching

Mobile users are identified by temporary identities, but there are cases where the network requests the user to send its permanent identity in clear text.

1) Passive identity catching: The attacker with a modified MS waits passively for a new registration or a database crash as in such cases the user is requested to send its identity in clear text.
2) Active identity catching: In this case, the attacker with a modified BS entices the user to camp on his BS and then asks him to send his International Mobile Subscriber Identity (IMSI).

Impersonation of the network and thereby eavesdropping

In this sub-section we cover attacks where the intruder masquerades as a genuine network towards the user.

1) By suppressing encryption between the target user and the intruder: An attacker with a modified BS entices the user to camp on his false BS and when the service is initiated, the intruder does not enable encryption.
2) By suppressing encryption between the target user and the true network: In this case, during call setup the ciphering capabilities of the MS are modified by the intruder and it appears to the network that there is genuine mismatch of the ciphering and authentication algorithms. After this the network may decide to establish an un-enciphered connection: The intruder cuts the connection and impersonates the network to the target user.

3) By forcing the use of a compromised cipher key: The attacker with a modified BS/MS and a compromised authentication vector entices the user to setup a call while camped on his false BS/MS. The attacker then forces the use of a compromised cipher key.

Impersonation of the user

1) By the use of a compromised authentication vector: The attacker with a modified MS and a compromised authentication vector impersonates the target user towards the network and the other party.
2) By the use of an eavesdropped authentication response: The intruder with a modified MS uses an eavesdropped authentication response if the same challenge is used again.
3) Hijacking outgoing calls in networks with encryption disabled: The intruder with a modified BS/MS pages the target user for an incoming call, who then sets up a call which it allows to occur. The intruder modifies the signalling elements and it appears to the serving network that the user wants to set-up a mobile originated call. The intruder then cuts the connection with the target user, and makes fraudulent calls on the user’s subscription.
4) Hijacking outgoing calls in networks with encryption enabled: In this case the intruder also modify the ciphering capabilities of the MS to suppress encryption.
5) Hijacking incoming calls in networks with encryption disabled: An associate of the intruder makes a call to the target user, which is relayed by the intruder until authentication and call setup has been done. If the network does not enable encryption the intruder releases the target user, and uses the connection to answer the call.
6) Hijacking incoming calls in networks with encryption enabled: In such instances, apart from the method used in subsection 5, the intruder suppresses the encryption as well.

3.2 UMTS Security Architecture

According to specifications, the security architecture is made up of a set of security features and security mechanisms [15]. A security feature is a service capability that meets one or several security requirements. A security mechanism is an element or process that is used to carry out a security feature. Figure 6 shows the way security features are grouped together in five different sets of features, each one facing a specific threat and accomplishing certain security objectives. The following is a description of these groups of features:

Network access security (I): Provides secure access to 3G services and protects against attacks on the radio interface link.

Network domain security (II): Allows nodes in the operator's network to securely exchange signalling data and protects against attacks on the wireline network.

User domain security (III): Secures access to mobile stations.

Application domain security (IV): Enables applications in the user and in the provider domain to securely exchange messages.

Visibility and configurability of security (V): Allows the user to get information about what security features are in operation or not and whether provision of a service depends on the activation or not of a security feature.

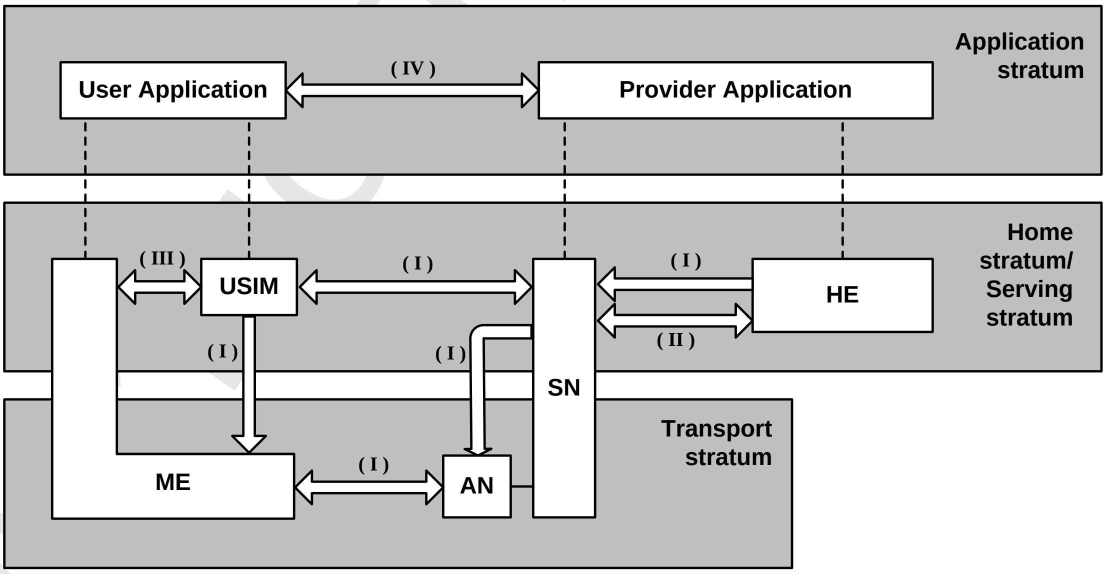


Figure 7: Overview of the security Architecture

3.2.1 Network Access Security Features

Network access security features can be further classified into the following categories: entity authentication, confidentiality and data integrity.

The following is a description of the security features classified into the category of entity authentication:

User authentication: The property that the network that provides the service (serving network) corroborates the identity of the user.

Network authentication: The property that the user corroborates that he is connected to a serving network that is authorized by the user’s home network to provide him services; this includes the guarantee that this authorization is recent.

The following security features deal with the confidentiality of data on the network access link:

Cipher algorithm agreement: The property that the mobile station and the serving network can securely negotiate the algorithm that they shall use subsequently.

Cipher key agreement: The property that the mobile station and the serving network agree on a cipher key that they may use subsequently.

Confidentiality of user data: The property that user data can not be overheard on the radio interface.

Confidentiality of signalling data: The property that signalling data can not be overheard on the radio interface.

The features provided to achieve integrity of data on the network access link are the following:

Integrity algorithm agreement: The property that the mobile station and the serving network can securely negotiate the integrity algorithm that they shall use subsequently.

Integrity key agreement: The property that the mobile station and the serving network agree on an integrity key they may use subsequently.

Data integrity and origin authentication of signalling data: The property that the receiving entity (mobile station or serving network) is able to verify that signalling has not been modified in an unauthorized way since it was sent by the sending entity (serving network or mobile station) and that the origin of the signalling data received is indeed the one claimed. [16]

3.3 Authentication and Key Agreement (AKA)

UMTS AKA is a security mechanism used to accomplish the authentication features and all of the key agreement features described above. This mechanism is based on a challenge/response authentication protocol conceived in such a way as to achieve maximum compatibility with GSM's subscriber authentication and key establishment protocol, in order to make easier the transition from GSM to UMTS. A challenge/response protocol is a security measure intended for an entity to verify the identity of another entity without revealing a secret password shared by the two entities.

The key concept is that each entity must prove to the other that it knows the password without actually revealing or transmitting such password.

The UMTS AKA process described in this subsection is invoked by a serving network after a first registration of a user, after a service request, after a location update request, after an attach request and after detach request or connection re-establishment request. In addition, the relevant information about the user must be transferred from the user's home network to the serving network in order to complete the process. The home network's HLR/AuC provides serving network's VLR/SGSN with Authentication Vectors (AVs).

The authentication and key agreement process is summarized in the following algorithm and illustrated in Figure 8:

Stage 1:

1. Visited network's VLR/SGSN requests a set of AVs from the HLR/AuC in the user's home network.

2. HLR/AuC computes an array of AVs. This is done by means of the authentication algorithms and the user's private secret key K, which is stored only in the home network's HLR/AuC and the USIM in the user's mobile station.

3. Home network's HLR/AuC responds by sending n authentication vectors AV1 ? AVn back to the visited network's VLR/SGSN.

Stage 2:

1. Visited network's VLR/SGSN chooses one AV and challenges mobile station's USIM by sending the RAND and AUTN fields in the vector to it.

2. The mobile station's USIM processes the AUTN. With the aid of the private secret key K, the user is able to verify that the received challenge data could only have been constructed by someone who had access to the same secret key K. The USIM will also verify that the AV has not expired by checking its sequence number (SEQ) field. Provided that the network can be authenticated and that the AV is still valid, the USIM proceeds to generate a confidentiality key (CK), an integrity key (IK) and a response for the network (RES).

3. The user responds with RES to the visited network.

4. Visited network's VLR/SGSN verifies that response is correct by comparing the expected response (XRES) from the current AV with the response (RES) received from the mobile station's USIM.

Mutual authentication is performed in step 5 of the former algorithm. Both the USIM and the VLR/SGSN have authenticated each other after two conditions have met: First, that the USIM has verified that the MAC field in AUTN equals a value computed internally using the key K and the fields SQN, RAND and AMF. Second, that the VLR/SGSN has verified that the RES value transmitted by user's mobile station equals the internal XRES value.

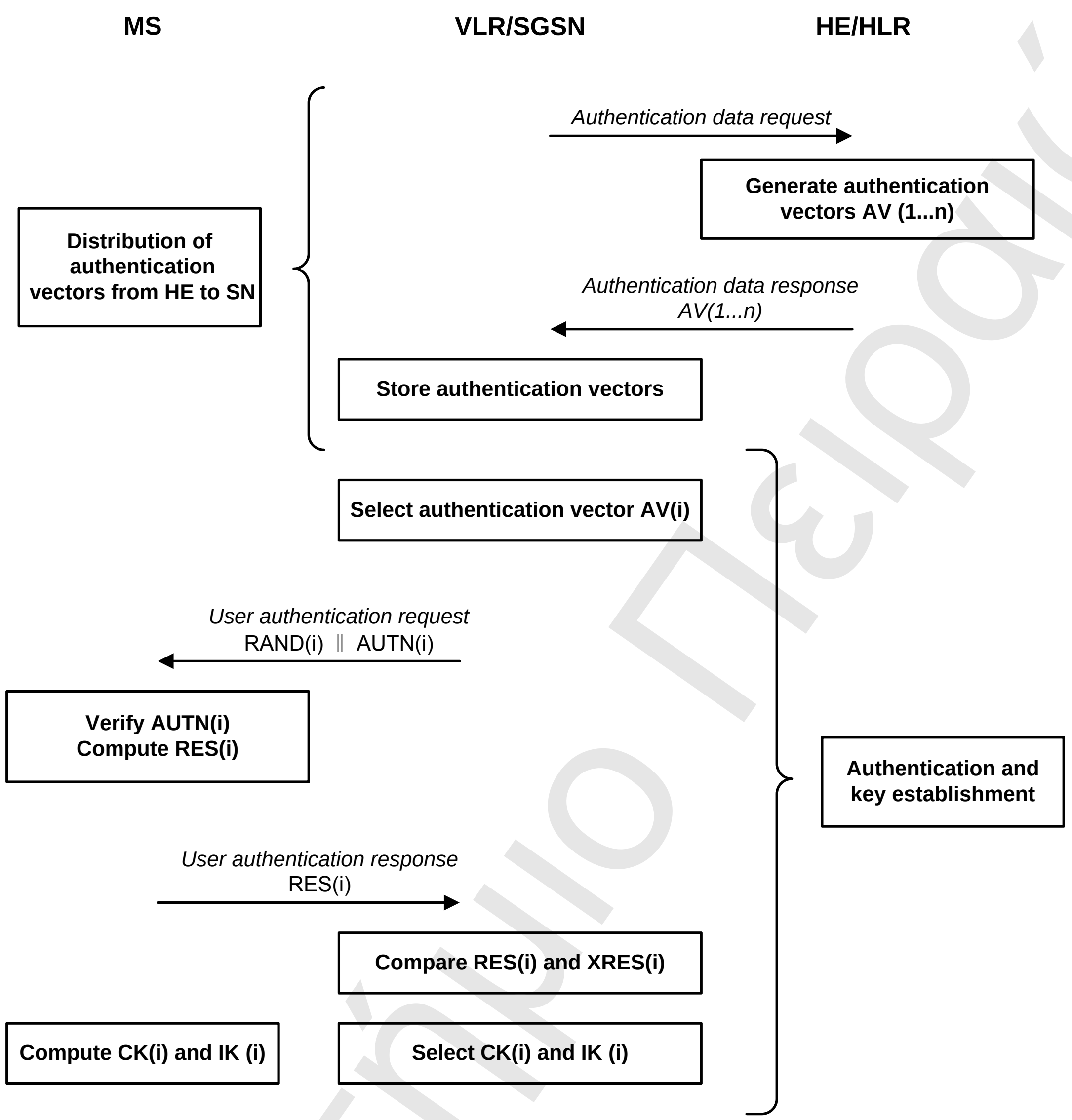

MS
VLR/SGSN
HE/HLR
Authentication data request
Generate authentication vectors AV (1...n)
Distribution of authentication vectors from HE to SN
Authentication data response AV(1...n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i) Compute RES(i)
Authentication and key establishment
User authentication response RES(i)
Compare RES(i) and XRES(i)
Compute CK(i) and IK (i)
Select CK(i) and IK (i)

Figure 8: Authentication and Key Agreement

3.3.1 Generation of Authentication Vectors

Upon receipt of an authentication data request, the HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND. For each user the HE/AuC keeps track of a counter $SQN_{HE.}$

Subsequently the following values are computed by the HE/AuC by using the user-specific key K and an operator-specific Authentication Management Field (AMF):

- A message authentication code MAC = f1K(SQN || RAND || AMF) where f1 is a message authentication function

- An expected response XRES = f2K(RAND) where f2 is a (possibly truncated truncated)
- message authentication function
- A cipher key CK = f3K(RAND) where f3 is a key generating function
- An integrity key IK = f4K(RAND) where f4 is a key generating function
- An anonymity key AK = f5K(RAND) where f5 is a key generating function

Finally the authentication token AUTN = SQN ⊕AK || AMF || MAC is constructed. Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The authentication token AUTN is sent to the user together with the random challenge RAND by the SN. Its purpose is twofold: Firstly, it authenticates the Home Environment (HE) to the user, since AUTN can only be computed by an entity in possession of K. It cannot be replayed, because the time-variant parameter SQN is included in the computation of AUTN. Secondly, by verifying that AUTN is correct, the user is also assured that the serving network is trusted by the user's HE The parameters (RAND, XRES, CK, IK, AUTN) together form the UMTS authentication vector sent to the SN by the HE. [17]

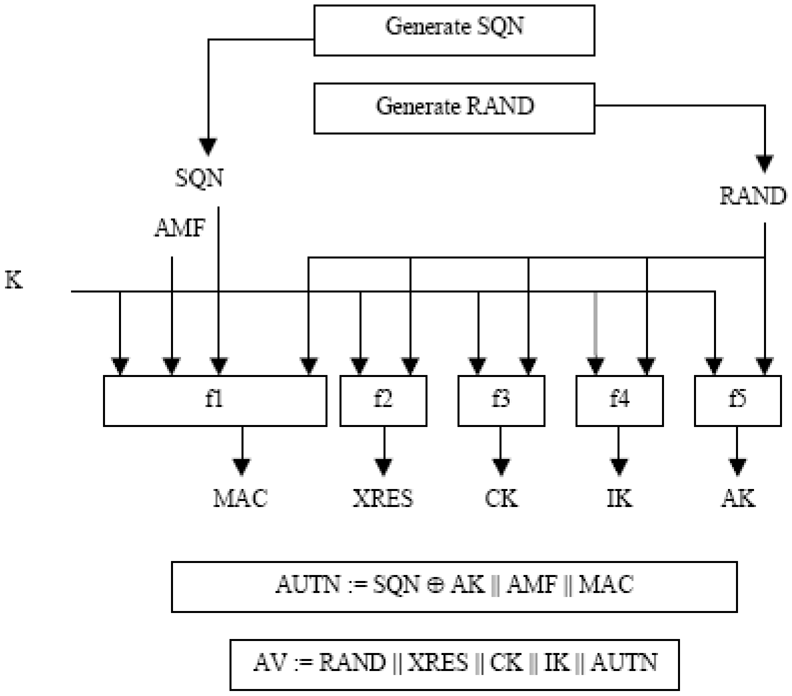

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 9: Generation of Authentication Vectors

4 UMTS Terrestrial Radio Access Network (UTRAN)

The UTRAN is responsible for call setup, routing and switching operations. It is responsible for exchanging data and signaling traffic between the User Equipment (UE) and the Core Network (CN). Further more the UTRAN handles functions related to UE network access and mobility and also control the allocation and withdrawal of radio bearers required for the traffic support

The functioning of the UTRAN is based in the UTRA/FDD and UTRA/TDD modes of the WCDMA technology.

4.1 UTRAN Architecture

As shown in Figure 1 the UTRAN is the connection between the UE and the CN through the Uu and the Iu interfaces respectively.

Compared with GSM radio access network, the UTRAN brings the following innovations:

1. specification of four new interfaces: “Uu”, “Iub”, “Iur” and “Iu”, the latter being declined into two interfaces “Iu-CS” and “Iu-PS” with respectively the CS and the PS core network domains. These interfaces presented in Table 6.1 are open and should allow interworking between equipments from different manufacturers, and therefore offer more flexibility to operators on the choice of equipment providers
2. use of CDMA access mode. The use of (wideband) CDMA as multiple-access technique in the UTRAN requires supporting the macrodiversity procedure, nonexistent in radio access systems based on TDMA access mode;
3. use of Asynchronous Transfer Mode (ATM) for the transport layer of “Iu”, “Iub” and “Iur” interfaces. This transfer mode is particularly appropriate for transport in the network of information with variable bit rate while respecting the requested transmission delay
4. handling of the mobility in the UTRAN. The UTRAN handles mobility at cell and URA (UTRAN Registration Area) levels independently from the mobility management handled by the CN. This enables efficient radio resources management and less signaling exchange between the mobile station and the

CN. Temporary identities for UTRAN mobility management purposes were also specified.

The UTRAN interfaces are shown in the table below

Interface	Location
Uu	UE – UTRAN
Iu	UTRAN – CN
Iur	RNC – RNC
Iub	Node B - RNC

Table 1: UTRAN interfaces

The overall UTRAN architecture is shown in the Figure below

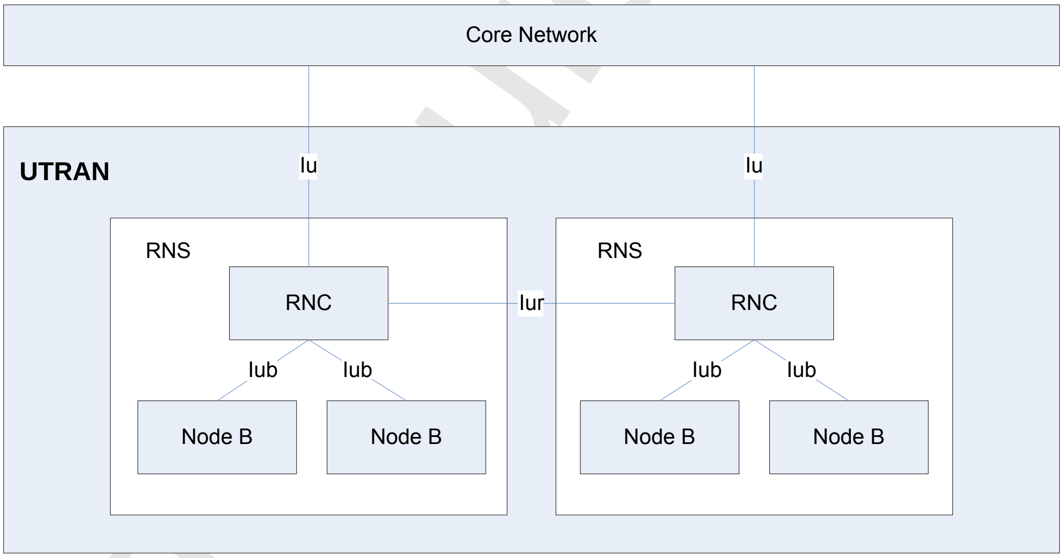


Figure 10: UTRAN Architecture

4.1.1 The radio network sub-system (RNS)

The UTRAN is composed of one or several radio sub-systems called Radio Network Sub-system (RNS) and equivalent to the GSM BSS functional sub-system. A RNS consists of a Radio Network Controller one or more Node Bs. A Node B is connected to the RNC through the Iub interface

Node B

Node B is the exchange node between the UTRAN and all the UEs located in the cell or sectors covered by Node B. It mainly assures physical layer functions such as interleaving, channel coding and decoding, rate matching, spreading, QPSK modulation, etc.

A Node B can support FDD mode, TDD mode or dual-mode operation.

There are three chip-rate options in the TDD mode: 7.68 Mcps TDD, 3.84 Mcps TDD and 1.28 Mcps TDD. Each TDD cell supports one of these options.

A Node B which supports TDD cells can support one chip-rate option only, or more than one option.

The radio network controller (RNC)

The RNC enables radio resource management in the UTRAN. Its main functions are:

– outer loop power control;

– handover control;

– mobile stations admission and traffic load control;

– channelization and scrambling code allocation handling;

– data transmission scheduling in packet transfer mode;

– combining/distribution of signals from/to different node Bs in a macrodiversity situation.

Inside the UTRAN, the RNCs of the Radio Network Subsystems can be interconnected together through the Iur. Iu(s) and Iur are logical interfaces. Iur can be conveyed over direct physical connection between RNCs or virtual networks using any suitable transport network.

Depending on the role it plays for a given UE, the RNC is called

- Controlling RNC (CRNC),
- Serving RNC (SRNC) or

- Drift RNC (DRNC).

One RNC equipment is generally able to play each of these three logical roles.

The CRNC role is not dependent on whether the UE has established or not an RRC connection. It handles radio resources for all Node Bs under its control – each Node B is controlled by a unique CRNC. The CRNC is also responsible for admission control of UEs in the cells it covers, and control of resources allocation during for instance a handover execution towards its controlling area.

The SRNC is the RNC that handles radio resources for a given UE that has already established an RRC connection. It is thus responsible for the handling of radio connection with the UE and some associated procedures such as handover, radio bearer allocation, SRNS relocation and outer loop power control. The SRNC is also responsible for selecting the best frame out of those received from different Node Bs involved in a macrodiversity scenario.

The DRNC is any RNC different from the SRNC but involved in a connection between a UE and the UTRAN. It is linked to the SRNC by the Iur interface. When an RNS runs out of radio resources or if a soft handover procedure has been decided, the SRNC could request an RNC belonging to another RNS to support it in terms of radio resources (spreading codes). This other RNC is called DRNC. The RNS containing the SRNC is designated as the Serving RNS (SRNS), whereas the one containing the DRNC is called Drift RNS (DRNS).

4.1.2 Mobility Handling

Beside the temporary identifiers TMSI and P-TMSI allocated to the UE by the CN for security purpose, a set of temporary identifiers are also used in the UTRAN for identification of a UE related data in common channel and mobility management in the UTRAN level.

The following four types of these identifiers called Radio Network Temporary Identifiers (RNTI) have been specified:

Four types of RNTI exist:

1. Serving RNC (s-RNTI)
2. Drift RNC (d-RNTI)

3. Cell RNTI (c-RNTI)
4. UTRAN RNTI (u-RNTI)

The sRNTI is used by UE to identify itself to the Serving RNC and also by the serving RNC for addressing to the U. The s-RNTI is allocated for all UEs having a RRC connection, it is allocated by the Serving RNC and it is unique within the Serving RNC/BSS. The s-RNTI is reallocated always when the Serving RNC for the RRC connection is changed.

The dRNTI is allocated in Drift RNC upon drift UE context establishment. The dRNTI is umique withing the drift RNC and the mapping between the sRNTI and the dRNTI should be known ti the serving RNC. Drift RNC/BSS shall know the s-RNTI and SRNC-ID related to existing d-RNTI within the drift RNC/BSS It is possible to have at the same time both an S-RNTI and a D-RNTI allocated to a given UE, and in this case the related SRNC and DRNC should be capable of handling both these identifiers

The cRNTI is allocated by a controlling RNC to the UE when the UE eneres a new cell that it is under its control. The C-RNTI shall be unique within the accessed cell. Controlling RNC shall know the d-RNTI associated to the c-RNTI within the same logical RNC (if any).

The u-RNTI is used to identify the the UE inside the UTRAN and is allocated to a UE having an RRC connection. Each RNC has a unique identifier within the UTRAN part of the PLMN, denoted by RNC identifier (RNC-ID). This identifier is used to route UTRAN interface messages to correct RNC. RNC-ID of the serving RNC together with the s-RNTI, they compose the uRNTI which is a unique identifier of the UE in the UTRAN part of the PLMN.

4.2 Access Stratum & Non Access Stratum

Dividing the UMTS in Access Stratum (AS) and Non Access Stratum (NAS) is another way of modeling the UMTS, than separating it to User Equipment (UE), Access Network and Core Network.

The Access Stratum serves in managing resources of the air interface as well as providing the means to carry information over the air interface.

On the other hand, the Non Access Stratum protocols are applied between UE and CN and rely on the functions of the AS.

The architecture of the Access Stratum and the Non Access Stratum is depicted in the pisture below:

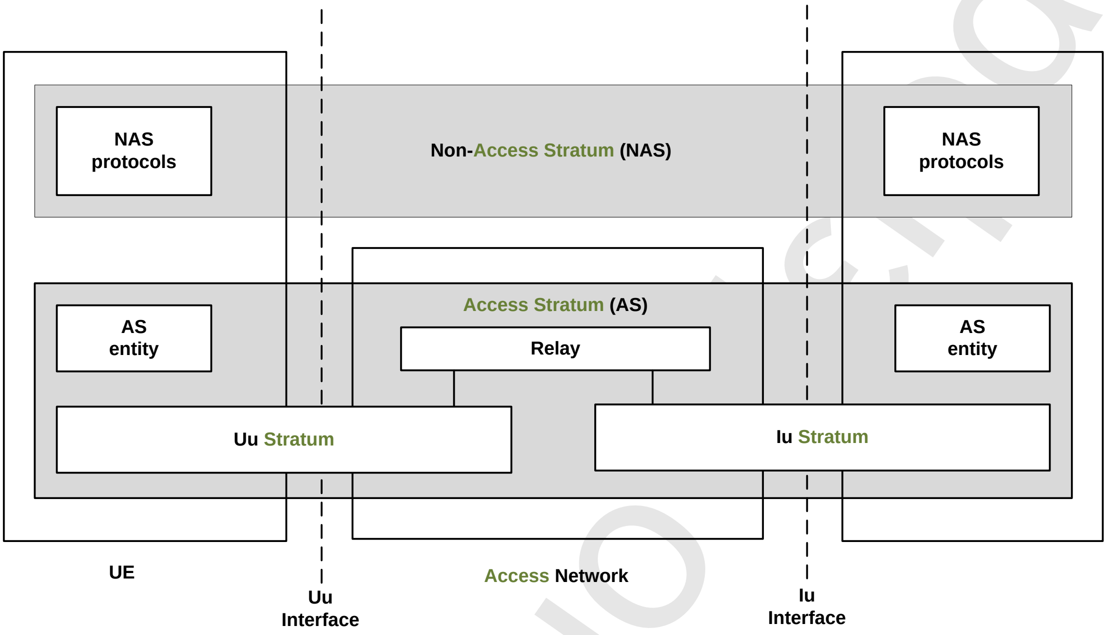


Figure 11: AS and NAS architecture.

4.2.1 Access Stratum

The Access Stratum is shared in the UE level and Access and Core Network Level. It provides the way of carrying information over the air interface and groups together the protocols and functions for the transport of user data as well as the network control signaling generated by the Non access Stratum.

The Access Stratum is further divided in the Uu stratum and the Iu stratum. The AS protocols that apply in the Uu and Iu are used for transporting information between the UE and the CN.

The Uu stratum is used for carrying information between the UE and the UTRAN. More specific the Uu is used to manage the radio resources between the UE and the UTRAN. The protocols used from the AS in the Uu stratum are responsible for the set up and the control of the radio bearers and are referred to as “radio protocols”.

The Uu stratum protocols are consisted of the following controls:

1. Medium Access Control (MAC)
2. Radio Link Control (RLC)
3. Broadcast/Multicast Control (BMC)
4. Packet Data Convergence Control (PDCP)
5. Radio Resource Control (RRC)

The RRC layer is of great interest as it is the main signaling protocol for the communication between the UE and the RNC.

The Iu stratum is used for carrying information between the UTRAN and the CN. More specific the Iu is used for transferring data and signaling information from the UTRAN to the CN serving access node (MSC or SGSN). The protocols used from the AS in the Iu stratum are responsible for the setup and the control of Iu bearers and are referred to as “Iu Protocols”. The Radio Access Network Application Part (RANAP) in the main Iu Protocol used between the UTRAN and the MSC/SGSN.

Simply said the Access Stratum provides services to the Non Access Stratum, with the most important being the transportation of NAS messages between the NAS entities.

The realization and the control of the radio access bearers is performed through the set of AS protocols in Uu and Iu stratum. These protocols are divided in two planes:

– *User plane* that includes the data stream(s) and the data bearer(s) for the data stream(s). The upper application layers generate data stream(s) that are adapted to the physical media by applying AS functions such as data formatting, error correction and recovery. So the user plane is materializing the radio access bearers.

– *Control plane* which includes the Application protocols that generate control signalling messages (i.e RANAP, RNSAP or NBAP) and the Signalling Bearer for transporting the Application Protocol messages. The control plane performs the establishment, the modification and release of radio access bearers within the user plane.

4.2.2 Non Access stratum

The Non access stratum protocols are applied between the UE and the CN and independent of the radio access technology implemented within the UMTS network. These protocols are not related to the transport of user data or network signaling. For these protocols the UTRAN acts as a carrier terminating the signaling in the Core Network. The UTRAN does not perform any analysis in the NAS messages but only acts as a relaying function.

The NAS protocols are as well divided in two planes

--User Plane that comprises basically user application protocols generating data streams to be transported by AS, that may or not adhere to GSM/UMTS standards

--Control Plane that encompasses all the protocols associated to Connection Management (CM) and Mobility Management (MM) functions for circuit-switched services, and Session Management (SM) and GPRS Mobility Management (GMM) functions for packet switched services.

In the figure below the protocols for the AS and NAS are shown

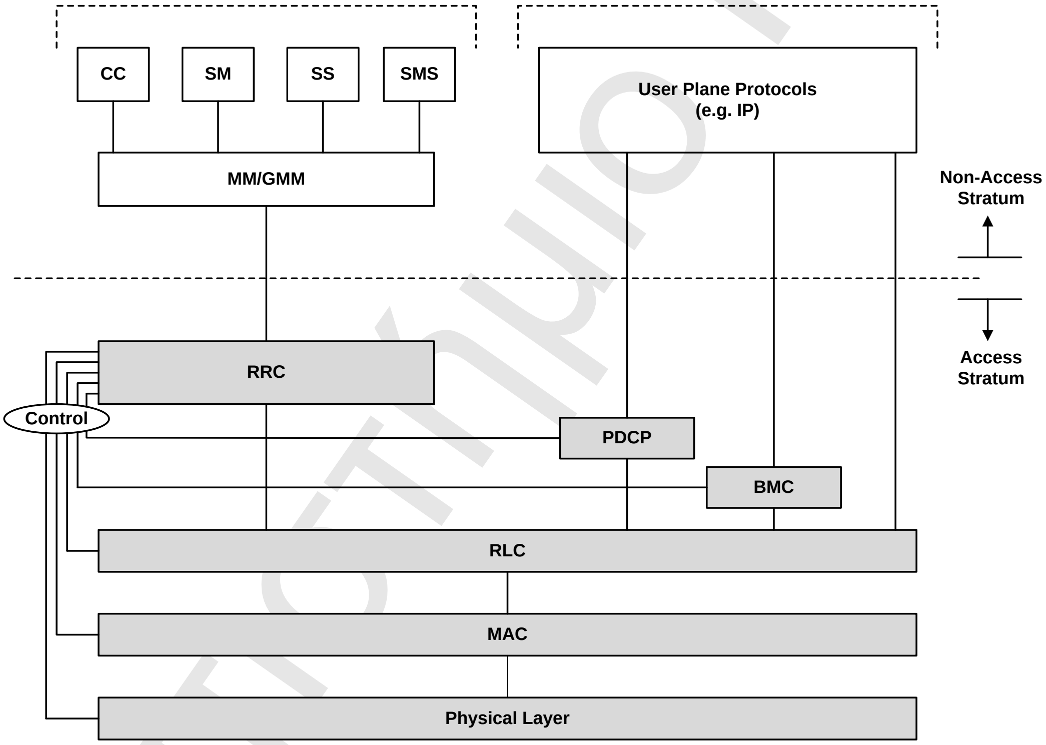


Figure 12: AS and NAS Protocols

4.2.3 Mobility Management/ GPRS mobility management (MM/GM)

Call Establishment in a mobile network follows a different procedure than the call establishment in a fixed network. The case of a mobile network is more complex for the following reasons:

– the user equipment is neither permanently attached to the network nor always localized by the network;

– the user equipment is a mobile equipment and therefore, in order to be reachable at any time, it must keep its localization up-to-date;

– a geographic area could be covered by several different mobile operator networks and, in this case, a user equipment shall perform the selection of an authorized network. The selected network shall in turn perform admission control on mobile equipments attempting attachment to it.

So in wireless network in order to make call establishment possible the following conditions must be fulfilled:

– a successful selection of a mobile network

– a successful attachment to the selected network

– updating of the user equipment location.

All the above functions are responsibility of the Non Access Stratum protocols.

MM (*Mobility Management*) is in charge of all the functions related to the mobility of the UE with regard to the core network (PLMN selection, network attachment, location update, etc.). It is composed of the protocol entities MM (Mobility Management) and GMM (*GPRS Mobility Management*) respectively responsible for the mobility management of the CS and the PS network domains

The CM (*Connection Management*) is composed of four types of entities:

1. CC (Call Control) for the handling of calls in the CS domain
2. SM (Session Management) for the handling of sessions in the PS domain
3. SS (Supplementary Service) used for the activation of supplementary services
4. SMS (Short Message Service) for the sending and receiving of text messages

4.2.3.1 Call Control (CC)

The call control (CC) protocol is one of several protocols in the connection management (CM) sublayer. This protocol includes the control functions for the call establishment and release.

A CC entity must support the following elementary procedures:

- Call-establishment procedures
- Call-clearing procedures
- Call-information-phase procedures
- Miscellaneous procedures

A call can be either a mobile-originated call (MOC) or a mobile terminated call (MTC); that is, it can be initiated by either the mobile or by the network. Optionally the UE can also support a network-initiated MOC. This functionality can be used with the completion of calls to busy subscriber (CCBS) supplementary service.

The call-clearing procedure can be initiated either by the UE or by the network. Note, however, that this means the logical CC-level connection clearing. The actual radio connection (RRC level) is always released by the UE. A radio connection and a CC connection are separate concepts. One can use the radio connection for many other things besides the circuit switched call, such as SMS and for packet-data applications. Therefore, releasing a call connection does not necessarily mean that the radio connection should also be released. There may be other applications that still need the radio connection. While the call is active, the CC can perform various procedures. The user-notification procedure informs the user about call-related events, such as user suspension or resume. Support of multimedia calls will be an important procedure especially in UMTS. The dual-tone multifrequency (DTMF) control procedure enables the user to send DTMF tones toward the network. Key presses in the UE containing digit values (0–9, A, B, C, D, *, #) are signaled over the air interface to the MSC, which converts them into DTMF tones and sends them onward to the remote user. Typical applications of the DTMF include various automated information services (e.g., telephone banking: "Press 1 if you want to hear your bank account balance; Press 2 if you want to settle your bills; Press 3 if you want to talk to the operator," and so forth). The support of DTMF is described in [18]. The support for the in-call modification procedure is optional for the UE. This procedure means that the same connection can be used for different kinds of information transfer during the same call, but not at the same time. In practice, this procedure is used for alternating the call between speech and fax services or between speech and data.

Miscellaneous CC procedures include in-band tones and announcements, status inquiry, and call reestablishment. The in-band tones and announcements procedure is used when the network wants to make the mobile station attach the user connection (e.g., in order to provide in-band tones/announcement) before the UE has reached the “active” state of a call. In this case, the network may include a progress indicator (IE) indicating user attachment in a suitable CC message. The status-inquiry procedure can be used to inquire about the status of the peer entity CC. This is a useful procedure in error handling. The call-reestablishment procedure is mostly an RRC-layer matter, as it involves setting up a new radio connection in place of the lost one. Within the CC level, however, this procedure includes provisions for the UE to make a decision as to whether a reestablishment should be attempted. The network-side CC must also identify and resolve any call states or an auxiliary state mismatch between the network and the UE.

The CC protocol is defined in [19]

4.2.3.2 Session Management (SM)

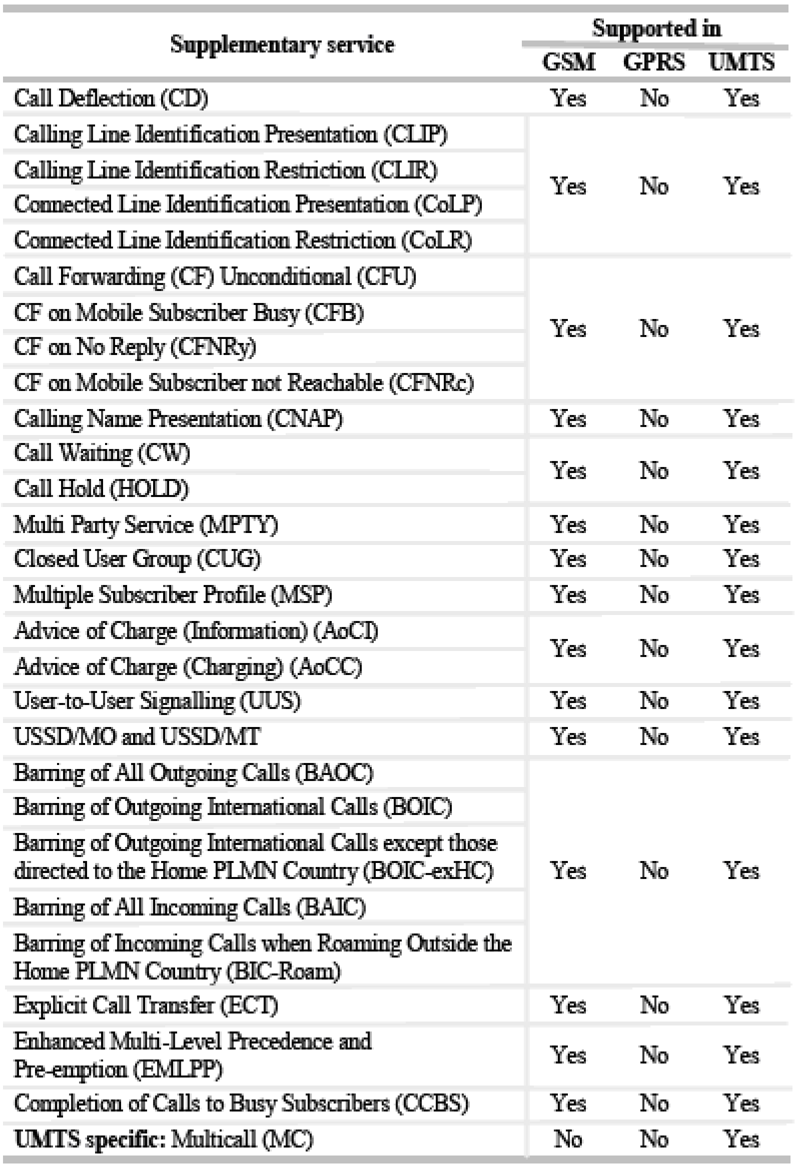
The main function of the SM protocol is to support packet data protocol (PDP) context handling of the user terminal. Note that there is no “connection” concept in a (IP) packet-switched system as we know it in a circuit- switched system. However, the communicating entities do need to know about the characteristics of the data to be transferred. This task is performed by the PDP context-activation procedure. Other functions this task must perform include PDP deactivation and PDP modification.

The SM procedures for identified access can only be performed if a GMM context has already been established between the UE and the network. If no GMM context has been established, the MM sublayer must initiate the establishment of a GMM context by use of the GMM procedures. After GMM context establishment, the SM uses services offered by GMM. Ongoing SM procedures are suspended during GMM procedure execution.

The SM protocol is defined in [TS-SCDMA Standards, http://www.cwts.org/].

4.2.3.3 Supplementary Services (SS)

Supplementary services bring out additional features to the aforementioned teleservices, including video-telephony and other applications [20]. They are not offered to a customer as a stand alone service but as a complement to a service –the supplementary services the network may offer are indicated in the user’s service subscription. As shown in Table 2, all GSM Release 99 supplementary services are also supported in UMTS. An exception is the multi-call supplementary service that is only available in UMTS networks [21]. This service enables users to dynamically control parallel network connections in the CS domain – each connection using its own dedicated bearer.



Supplementary service	Supported in		
	GSM	GPRS	UMTS
Call Deflection (CD)	Yes	No	Yes
Calling Line Identification Presentation (CLIP)	Yes	No	Yes
Calling Line Identification Restriction (CLIR)			
Connected Line Identification Presentation (CoLP)			
Connected Line Identification Restriction (CoLR)			
Call Forwarding (CF) Unconditional (CFU)	Yes	No	Yes
CF on Mobile Subscriber Busy (CFB)			
CF on No Reply (CFNRy)			
CF on Mobile Subscriber not Reachable (CFNRc)			
Calling Name Presentation (CNAP)	Yes	No	Yes
Call Waiting (CW)	Yes	No	Yes
Call Hold (HOLD)			
Multi Party Service (MPTY)	Yes	No	Yes
Closed User Group (CUG)	Yes	No	Yes
Multiple Subscriber Profile (MSP)	Yes	No	Yes
Advice of Charge (Information) (AoCI)	Yes	No	Yes
Advice of Charge (Charging) (AoCC)			
User-to-User Signalling (UUS)	Yes	No	Yes
USSD/MO and USSD/MT	Yes	No	Yes
Barring of All Outgoing Calls (BAOC)	Yes	No	Yes
Barring of Outgoing International Calls (BOIC)			
Barring of Outgoing International Calls except those directed to the Home PLMN Country (BOIC-exHC)			
Barring of All Incoming Calls (BAIC)			
Barring of Incoming Calls when Roaming Outside the Home PLMN Country (BIC-Roam)			
Explicit Call Transfer (ECT)	Yes	No	Yes
Enhanced Multi-Level Precedence and Pre-emption (EMLPP)	Yes	No	Yes
Completion of Calls to Busy Subscribers (CCBS)	Yes	No	Yes
UMTS specific: Multicall (MC)	No	No	Yes

Table 2: UMTS Supplementary Services

4.2.3.4 Short Message Service (SMS)

Short Message services is a service that provides the ability to send a short message from a UE to the SMS Service Centre (SMS-SC), where this is stored and then forwarded to the final destination. This variant is referred to as SMS-MO/PP (Mobile Originated/Point-to- Point), to be compared with variant SMS-MT/PP (Mobile Terminated/Point-to-Point) where it is the UE which receives a short message forwarded by the SMS-SC. SMS is a non-real-time service The size of the message is limited to 160 characters.

The term SMS-MO refers to a mobile-originated SMS message; SMS-MT refers to a mobile-terminated SMS message.

In the evolution path of SMS, there is also the Enhanced Messaging Service (EMS), where white and black images or sounds are associated to the short messages [22], [23]. EMS relies on the concatenation of as much as 255 short messages to create a single message stream.

A more important step in the enhancement of SMS is the introduction of the Multimedia Messaging Service (MMS). This non-real-time service (“store and forward” mechanism) is already available in GPRS networks and will be preserved in UMTS [23] – this is a bearer independent service. MMS enables users to send and receive messages including text (ASCII, UCS2, etc.), audio (MP3, MIDI, WAV, etc.), still-images (JPEG, GIF, PNG, etc.), video (H.263, MPEG4), and optionally, streaming. It uses IP data path and IP protocols (WAP, HTML, HTTP, etc.) and supports different addressing modes (MSISDN, Email, etc.).

4.3 Radio Interface Protocol Structure

The radio interface is layered into three protocol layers:

- the physical layer (L1);
- the data link layer (L2);
- network layer (L3).

Layer 2 is split into following sublayers: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP) and Broadcast/Multicast Control (BMC).

Layer 3 and RLC are divided into Control (C-) and User (U-) planes. PDCP and BMC exist in the U-plane only.

In the C-plane, Layer 3 is partitioned into sublayers where the lowest sublayer, denoted as Radio Resource Control (RRC), interfaces with layer 2 and terminates in the UTRAN.

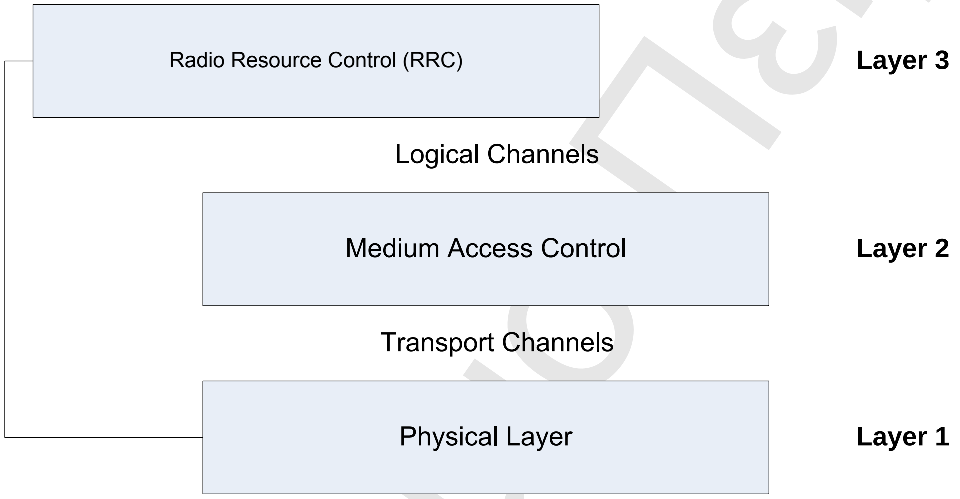


Figure 13: UTRAN Protocol Structure

4.4 Radio Resource Control

The Radio Resource Control is the most important of the radio interface protocols. It is used for sigalling between the UE and the UTRAN. The physical layer, the MAC, the RLC, the PDCP and the BMC are controlled by the RRC. The RRC is used in the control plane and not in the user plane.

4.4.1 RRC Functions

The Radio Resource Control (RRC) layer handles the control plane signalling of Layer 3 between the UEs and UTRAN. The RRC performs the following functions:

Establishment, re-establishment, maintenance and release of an RRC connection between the UE and UTRAN. The establishment of an RRC connection is initiated by a request from higher layers at the UE side to establish the first Signalling Connection for the UE. The establishment of an RRC connection includes an optional cell re-selection, an admission control, and a layer 2 signalling link establishment. The release of an RRC connection can be initiated by a request from higher layers to release the last Signalling Connection for the UE or by the RRC layer itself in case of RRC connection failure. In case of connection loss, the UE requests re-establishment of the RRC connection. In case of RRC connection failure, RRC releases resources associated with the RRC connection.

Assignment, reconfiguration and release of radio resources for the RRC connection. The RRC layer handles the assignment of radio resources (e.g. codes) needed for the RRC connection including needs from both the control and user plane. The RRC layer may reconfigure radio resources during an established RRC connection. This function includes coordination of the radio resource allocation between multiple radio bearers related to the same RRC connection. RRC controls the radio resources in the uplink and downlink such that UE and UTRAN can communicate using unbalanced radio resources (asymmetric uplink and downlink). RRC signals to the UE to indicate resource allocations for purposes of handover to GSM or other radio systems.

4.4.2 RRC States

The UTRA radio access interface has been specified in a way that enables a flexible usage of radio resources. The principle consists of adapting at any time resources allocated to a UE to its traffic needs. Figure 14 presents the different service states of the RRC protocol. According to whether an RRC connection is established or not, the mobile station operates in two different modes:

– *idle mode* in which there is no RRC connection established between the UE and the UTRAN;

– *connected mode* in which an RRC connection has been established. This mode is subdivided in four states: CELL_DCH, CELL_FACH, CELL_PCH and URA_PCH.

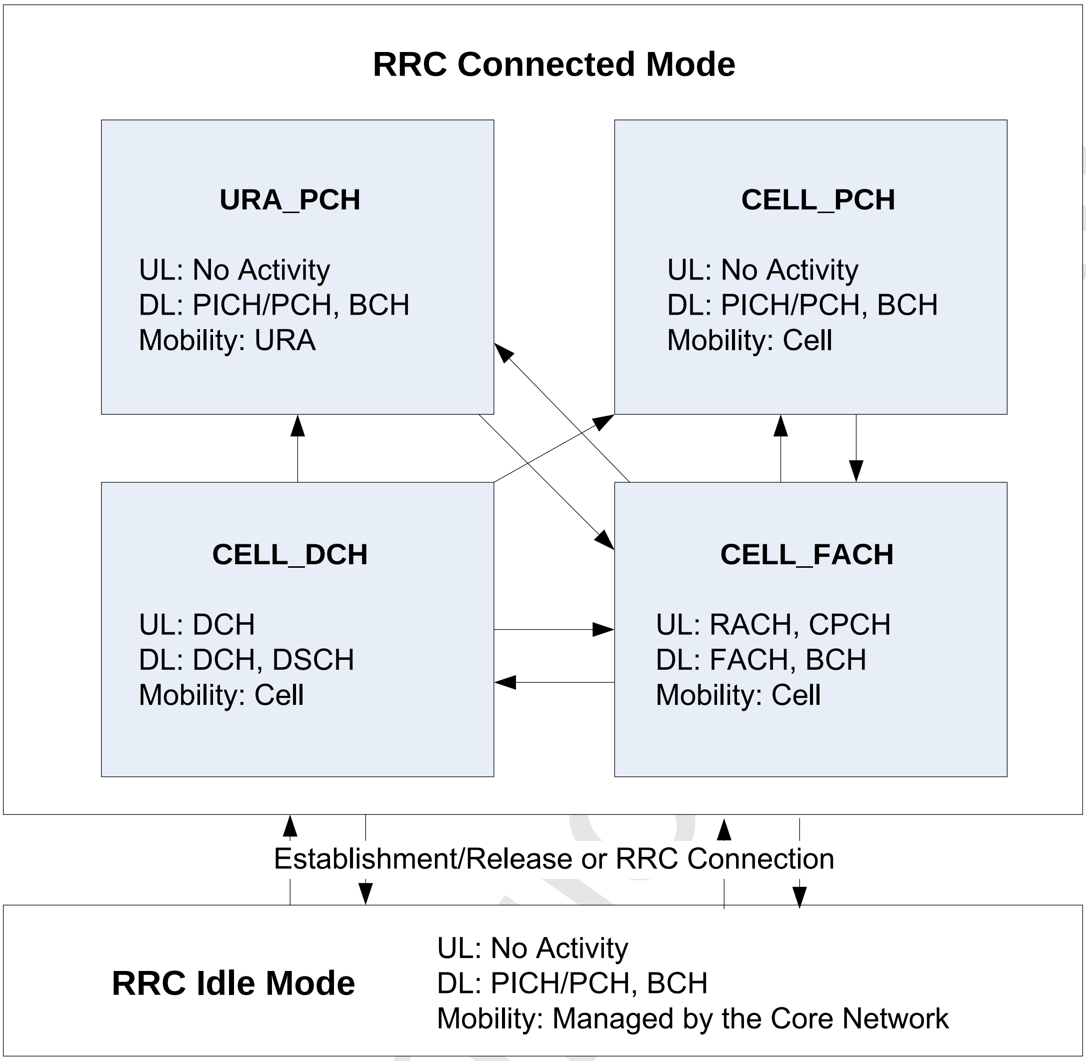


Figure 14: RRC Service states: mobility and transport channels involved

CELL_DCH state

UE enters the CELL_DCH state from idle mode or CELL_FACH state when dedicated radio resources (one or several transport channels of type DCH or DSCH) are allocated to it. Dedicated resources are used for real-time traffic or transfer of a huge amount of data in packet mode. In CELL_DCH the UE receives RRC messages sent on DCCH, and with regard to the UE capabilities, system information could be received on BCH or FACH. Transitions to states CELL_FACH, CELL_PCH or URA_PCH are triggered by using signalling messages between the UE and the UTRAN. For instance, in a packet mode session, if there is no user data exchange for a while, UTRAN could ask UE to move to CELL_PCH or URA_PCH state. Upon release of the RRC connection, the UE is automatically in idle mode.

CELL_FACH state

In CELL_FACH state, no dedicated resources are allocated to the UE. Common transport channels RACH, FACH or CPCH are used for the exchanges between the UE and the network, and the UE mobility is handled at the cell level. This state is suitable for transfer of small amount of non-real-time user data and signalling messages. In CELL_FACH the UE listens to RRC messages sent on BCCH, CCCH or DCCH. Transition to CELL_PCH or URA_PCH is done when explicitly requested by the UTRAN. Upon release of the RRC connection, the UE moves to idle mode.

CELL_PCH and URA_PCH states

CELL_PCH and URA_PCH are states with very low activity in the radio interface and without transmission/reception of user traffic. In these states, UE is in DRX mode: its activity being reduced to PICH/PCH monitoring and cell reselection process. Transitions to these states are ordered by the UTRAN, for instance, when there is a long period without any user traffic exchange in CELL_DCH or CELL_FACH.

Before resuming user traffic, RRC shall move to CELL_FACH state and perform the UTRAN location update process (Cell Update or URA Update). Indeed, in CELL_PCH or URA_PCH:

– when the UTRAN receives downlink user traffic, it sends to the UE a paging message indicating traffic resumption. The UE then moves to the CELL_FACH state and performs a Cell Update procedure with a cause set to paging response.

Upon completion of this procedure user traffic can then be resumed

– for uplink traffic, the RRC entity in UE moves to the CELL_FACH state and performs a Cell Update procedure with a cause set to uplink traffic resumption.

After successful completion of the procedure, the user traffic is resumed.

The main difference between CELL_PCH and URA_PCH is that the UE position is known for the former at cell level and for the latter at URA level. Moving from CELL_PCH to URA_PCH state will reduce the location update activity by performing the procedure upon URA change instead of cell change. The importance of this URA_PCH state can be easily understood if we consider for example a fast moving UE in CELL_PCH without traffic in an area composed of several micro cells.

4.4.3 RRC Connection Establisment

The RRC Connection Establishment is a procedure initiated from the UE towards the UTRAN but can be triggered also from the network. It starts when an RRC Connection Request message is sent over the RACH/PRACH channel. Since there is no previous RRC Connection established, the network is not aware of the UE presence, so the UE must perform a Random access procedure over the shared uplink channel.

The RRC Connection establishment makes the transition from RRC Idle mode to RRC connected mode. The UE must be in RRC connected mode in order to transfer any application data or completing any signalling procedure.

For example the UE triggers and RRC connection establishment when there is an attempt from the UE application to make a data call, or to send an email. Also an RRC Connection establishment can take place when the UE moves into a new Area and has to complete Location Update procedure.

The RRC Connection procedure can be triggered from the network when the latest sends a Paging message. This could be done in order to deliver an incoming SMS or a notification of an incoming voice call.

As shown in the picture below the RRC connection starts with the UE sending and RRC CONNECTION REQUEST over the RACH.

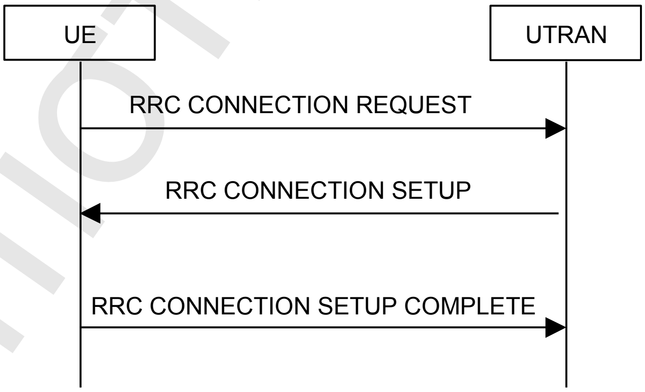


Figure 15: RRC Connection Establishment

The RRC CONNECTION REQUEST message sent to the RNC, ransfers among others the current UE identity (TMSI) and the connection establishment cause (Mobile Originating Signalling, Mobile Terminting Access, Mobile Originating Data etc).

The RRC connection request information element is shown in the table below:

Information Elements	
UE Identity	CHOICE
	S-TMSI
	Random Value
Establishment Cause	CHOICE
	Emergency
	High Priority Access
	Mobile Terminating Access
	Mobile Originating Signaling
	Mobile Originating Data

Table 3: Content of RRC Connection Message

The RNC then replies with an RRC connection setup message which contains information about the Signalling Radio Bearers (SRB) to be used on the connection and the indication of the RRC state. The UE acknowledges a successful RRC connection establishment using the RRC CONNECTION COMPLETE message.

5 Capacity in the UMTS

Unlike the GSM system, where the capacity is considered deterministic, which means is has a single value, in UMTS, the capacity does not have a single fixed value.

Capacity in UMTS depends on a number of factors, such as

- multi-path propagation
- orthogonality in UL/DL
- thermal noise
- received interference at the mobiles and Node B

In the following chapters we are going to examine some of the main factors that affect the UMTS capacity, giving focus on the capacity of the system to establish RRC Connections.

5.1 RRC Capacity

In order for the network to be able to serve new RRC Connections request a number of conditions must be fulfilled. [24], [25], [26], [27]

In the UMTS the capability of establishing new RRC Connections is depended upon a number of parameters. The parameters that we are going to examine here are

1. Number of Channel Element
2. Power
3. Iub Capacity
4. Code used

Channel Element

Channel Element Resource is the pool resource of the NodeB. This means that all cells connected to the NodeB will share the same CE pool resource. If the pool resource threshold is reached then we have congestion and the RRC connection fails to be established.

The CE Congestion can happen both in the DL and the UL.

In terms of hardware the number or CEs can vary upon the model of the card. Each manufacturer defines a given number of channel elements per each Radio Access Bearer, and the number of channel elements is also an indicator of how many Hardware Boards is required per Node B.

The values of the CE may vary depending on the vendor.

In the below table we can see the average number of CE for UL and DL per Node B for Ericsson model of Radio Base Station.

Part Number	# of CE in DL per Node B	# of CE in UL per Node B
RBS3106	153	133
RBS3116	102	102
RBS3206	258	172
RBS3216	341	203
RBS3308	192	117
RBS3418	195	139
RBS6102	384	384
RBS6201	384	384

Table 4: Number of CE in DL and UL for Ericsson Node Bs

According to HUAWEI [26] if the number of uplink or downlink CEs are more than 20 then it is considered a traffic overload which can cause failure in establishing the RRC connection.

Power

Incrementing the load in the uplink can cause service rejection since there is high radio load within the cell. In this case the RRM (Radio Resource Management) can not establish any new RRC connection due to the call admission control (cac). The call admission control uses the RTWP (Received Total Wideband Power) value in order to decide if there is power congestion or not. If this value is over a specified limit (for Ericsson it is iFcong+iFOffset during a time longer than iFHyst) [27] then the RRC connection can not be stabled.

Iub Capacity

According to Huawei [24] typical configuration bandwidth of Iub is between 10 and 20 Mbps. If the Iub capacity is not enough to accept the RRC connection then this can be rejected.
According to [29] a physical capacity of IuB in the downlink direction is equal to V_{IuB}= 13,36 Mbps

Code resource

Code resource fails to be allocated during RRC connection establishment. Code congestion is generally caused by too many network users. According to HUAWEI if the effective utilization of codes is lower than 30%, it is possible that the code distribution algorithm is abnormal.

Also there are other reasons that can lead to RRC rejection such as no response received from the UE.

In case the number of RRC connection establishment failures or the rater of failed RRC connection establishment failures exceed a vendor specific limit then statistics and metrics must be collected in order to understand where the problem lies.

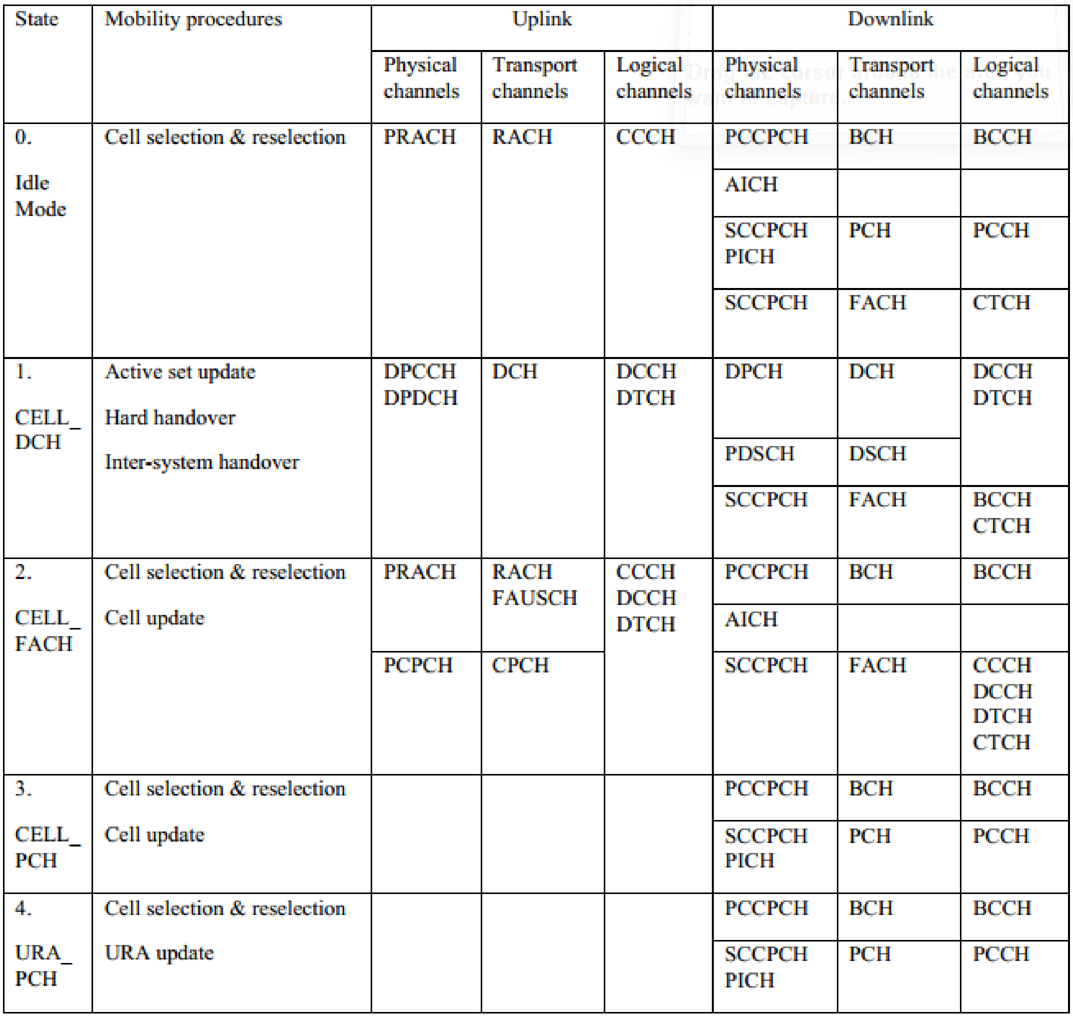
5.2 RRC Connection Uplink Capacity

In this section we are going to proceed to an attempt to calculate the Uplink and Downlink capacity while establishing an RRC connection. It is important that the Layer architecture of the UTRAN is understood in order to proceed to such estimation.

According to [30] for each logical channel, a transport and a physical channel is assigned. For each transport channel, possibility to use it depends on whether the physical channel related to it is available. Also, transport channels that are not possible to use in a given state, may be allocated to the UE, for usage in other states when physical channels supporting those are available

Table 5 shows the correspondence between the several Channels for the Uplink and the Down link, depending on the mobility procedure.

For our study we will attempt an estimation for the the Uplink and the Downlink Capacity during RRC connection establishment procedure.



State	Mobility procedures	Uplink			Downlink		
		Physical channels	Transport channels	Logical channels	Physical channels	Transport channels	Logical channels
0. Idle Mode	Cell selection & reselection	PRACH	RACH	CCCH	PCCPCH	BCH	BCCH
					AICH		
					SCCPCH PICH	PCH	PCCH
					SCCPCH	FACH	CTCH
1. CELL_ DCH	Active set update Hard handover Inter-system handover	DPCCH DPDCH	DCH	DCCH DTCH	DPCH	DCH	DCCH DTCH
					PDSCH	DSCH	
					SCCPCH	FACH	BCCH CTCH
2. CELL_ FACH	Cell selection & reselection Cell update	PRACH	RACH FAUSCH	CCCH DCCH DTCH	PCCPCH	BCH	BCCH
					AICH		
		PCPCH	CPCH		SCCPCH	FACH	CCCH DCCH DTCH CTCH
3. CELL_ PCH	Cell selection & reselection Cell update				PCCPCH	BCH	BCCH
					SCCPCH PICH	PCH	PCCH
4. URA_ PCH	Cell selection & reselection URA update				PCCPCH	BCH	BCCH
					SCCPCH PICH	PCH	PCCH

Table 5: RRC States - Uplink, Downlink layers correspondence

As it is shown in Figure 16 RRC Connection Establisment is a signal sent over the Common Control Channel (CCCH) logical channel. Therefore according to Table 5 for the Uplink, when the Logical Channel is the Common Control Channel (CCCH), the relevant Transport Channel is the Random Access Channel (RACH) and the relevant Physical Channel is the Physical Random Access Channel (PRACH)

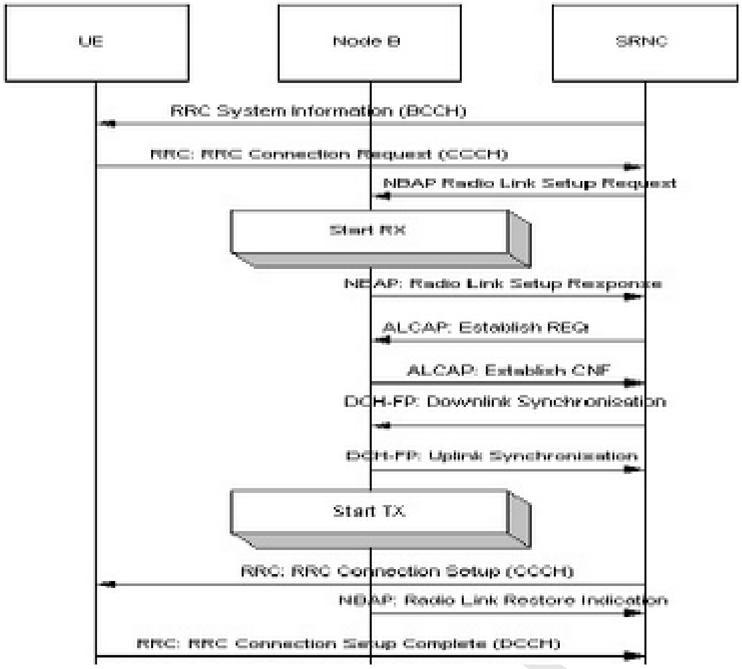

UE
Node B
SRNC
RRC System Information (BCCH)
RRC: RRC Connection Request (CCCH)
NBAP Radio Link Setup Request
Start RX
NBAP: Radio Link Setup Response
ALCAP: Establish REQ
ALCAP: Establish CNF
DCH-FP: Downlink Synchronization
DCH-FP: Uplink Synchronization
Start TX
RRC: RRC Connection Setup (CCCH)
NBAP: Radio Link Restore Indication
RRC: RRC Connection Setup Complete (DCCH)

Figure 16: RRC Connection Establishment - Logical Channels

So actually the question of calculating the uplink capacity for the RRC Connection establishment does down to the question of calculating the capacity of the Random Access Channel (RACH).

In order to be able to attempt such an estimation, the RACH procedure should be analysed.

RACH is a common transport channel in the uplink and is always mapped one-to-one onto physical channels (PRACHs). In one cell, several RACHs/PRACHs may be configured. If more than one PRACH is configured in a cell, the UE performs PRACH selection randomly.

The parameters for RACH access procedure includes: access slots, preamble scrambling code, preamble signatures, spreading factor for data part, available signatures and subchannels for each Access Service Class (ASC) and power control information. The Physical channel information for PRACH is broadcasted in SIB5/6 and the fast changing cell parameters such as uplink interference levels used for open loop power control and dynamic persistence value are broadcasted in SIB7.

RACH access procedure follows slotted-ALOHA approach with fast acquisition indication combined with power ramping in steps.

Maximum of 16 different PRACHs can be offered in a cell, in FDD, the various PRACHs are distinguished either by employing different preamble scrambling codes or by using common scrambling code with different signatures and subchannels. With in a single PRACH, a partitioning of the resources between the maximum 8 ASC is possible, thereby providing a means of access prioritization between ASCs by allocating more resources to high priority classes than to low priority classes.ASC 0 is assigned highest priority and ASC 7 is assigned lowest priority. ASC 0 shall be used to make emergency calls which has got more priority. The available 15 access slots are split between 12 RACH subchannels.

The RACH transmission consists of two parts, namely preamble transmission and message part transmission. [31]

RACH preamble is of length 4096 chips and consists of 256 repetitions of a signature of length 16 chips. There are a maximum of 16 available signatures. All 16 preamble signature codes available in every cells.

The 10 ms RACH message part radio frame is split into 15 slots, each of length Tslot = 2560 chips. Each slot consists of two parts, a data part to which the RACH transport channel is mapped and a control part that carries Layer 1 control information. The data and control parts are transmitted in parallel. A 10 ms message part consists of one message part radio frame, while a 20 ms message part consists of two consecutive 10 ms message part radio frames.

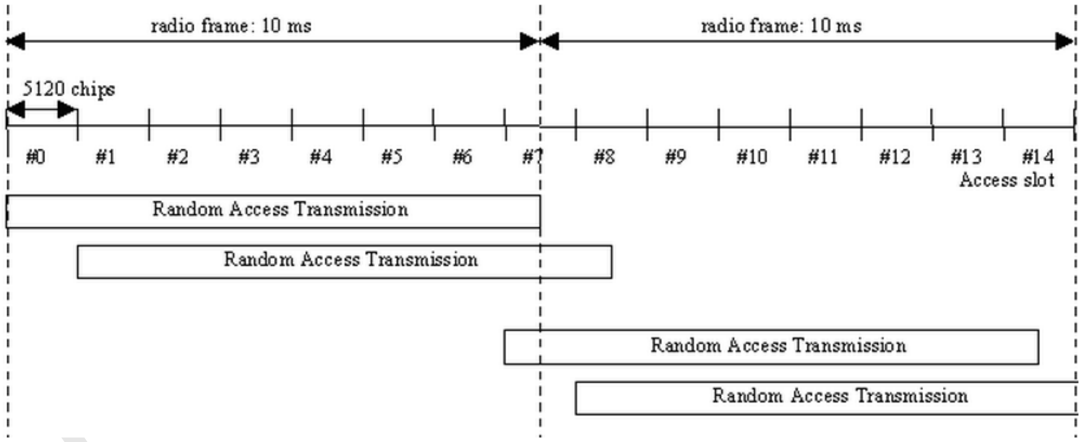

radio frame: 10 ms
radio frame: 10 ms
5120 chips
#0
#1
#2
#3
#4
#5
#6
#7
#8
#9
#10
#11
#12
#13
#14
Access slot
Random Access Transmission
Random Access Transmission
Random Access Transmission
Random Access Transmission

Figure 17: RACH access slot numbers and their spacing

The number of UE per sec that the RACH channel can support can be calculated from the below formula:

$$\boxed{\text{Number of UE per sec} = \text{Number of UE per Frame} * \text{Number of Frames per sec}}$$

Assuming that we have frames for 10 ms then the second part of the above equation becomes

$$\text{Numbers of Frames per sec} = 100$$

Also assuming that we have 1UE per Frame then the first part of the above equation becomes, [32]

$$\text{Number of UE per Frame} = 1$$

So at the end we have that

$$\mathbf{Number\ of\ UE\ per\ sec = 100}$$

The above value was calculated based in the assumptions made for the number of users per frame and the number of frames per sec.

According the vendor, the RRC capacity may vary. For example, the specification for Alcatel Lucent LTE eNodeB Digital Module, indicate [33]:

- 600 RRC-connected users per modem (1800 RRC-connected users per eNodeB)
- 115 Mbps for the Uplink
- 172,8 Mbps for the downlink.

In general the computation of the RRC capacity is rather complicated and depends on the vendor of the equipment. The RRC capacity is part of the procedure for estimation of UMTS Network Capacity in which also the number of users that will access the network should also be considered.

6 Conclusion

In this thesis, a detailed analysis was made in the UMTS technology. UMTS Network Architecture, as long as with the functions established within it were thoroughly examined. Particular attention was made to the part of the RRC Connection Establishment procedure.

Also a research was made for deriving values for the parameters that influence the RRC Capacity such as the Number of Channel Elements, Power, Iub capacity and Code, among different vendors, specifically Huawei, Ericsson and Alcatel Lucent.

Furthermore, an attempt to calculate the number of UE that can initiate an RRC connection was performed. Based on this value it is possible to generate denial of service attacks in the RNC part of the network, in case there is a flood of RRC requests more than the max limit.

Nevertheless, the number of RRC Capacity, can not be calculated as a single number, since it is depended upon many factors that may vary from vendor to vendor.

7 Abbreviations

3G	Third Generation
3GPP	Third Generation Partnership Project
AuC	Authentication Center
AKA	Authentication and Key Agreement
AS	Accesss Stratum
AV	Authentication Vector
BSS	Base Station Subsystem
BSC	Base Station Controller
BTS	Base Transceiver Station
CE	Channel Elements
CC	Country Code
CCCH	Common Control Channel
CDMA	Code Division Multiple Access
CM	Connection Management
CN	Core Network
CRNC	Controlling Radio Network Controller
CS	Circuit Switched service
DL	Downlink
DRNC	Drift Radio Network Controller
DTMF	Dual Tone Multi Frequency
EIR	Equipment Identity Register
FACH	Forward Access Channel
FDD	Frequency Division Duplex
GGSN	Gateway GPRS Support Node

GMM	GPRS Mobility Management
GMSC	Gateway Mobile Switching Centre
GSM	Global System for Mobile telecommunications
GPRS	General Packet Radio Service
HLR	Home Location Register
HSDPA	High-Speed Data Packet Access
IMEI	International Mobile Station Equipment Identity
ITU	International Telecommunication Union
LMSI	Local Mobile Station Identity
MAC	Medium Access Control
ME	Mobile Equipment
MM	Mobility Management
MO	Mobile Originating
MS	Mobile Station
MSISDN	Mobile Subscriber ISDN
MSRN	Mobile Station Roaming Number
MT	Mobile Termination/Terminal
NAS	Non Access Stratum
NDC	National Destination Code
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
PS	Packet Switched service

PSTN	Public Switched Telephone Network
RACH	Random Access Channel
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RNTI	Radio Network Temporary Identity
RRC	Radio Resource Control
RTWP	Received Total Wideband Power
SGSN	Serving GPRS Support Node
SM	Session Management
SN	Subscriber Number
SRNC	Serving Radio Network Controller
s-RNTI	Serving Radio Network Temporary Identity
SS	Supplementary services
TE	Terminal Equipment
TDD	Time Division Duplex
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visit Location Registry
WCDMA	Wideband - Code Division Multiple Access

8 References

[1] UMTS, Javier Sanchez and Mamadou Thioune, ISTE

[2] 3G Networks: Architecture, Protocols and Procedures, By Sumit Kasera, Nishit Narang, Tata McGraw-Hill Education

[3] http://www.hexazona.com/nexwave/docs/training/UMTS%2008%20User%20Equipment.pdf

[4] UMTS Signalling, UMTS Interfaces, Protocols, Message Flows and Peocedures analyzed and explained, R.Kreher, T. Rudebusch, WILEY

[5] 3GPP TS 123002 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Network architecture

[6] 3GPP TS 23.003 Numbering, addressing and identification

[7] 3GPP TS 25.401 UTRAN overall description

[8] UMTS Security, K.Boman, G.Horn, P.Howard and V.Niemi, Elecronics & Communication engineering Journal, October 2002

[9] 3GPP TS 33.120 (4.0.0), “3G Security; Security principles and objectives”, Release 4, March, 2001

[10] C. J. Mitchell, “Security for Mobility”, Institute ofElectrical Engineers, December, 2004

[11] G. M. Køien, “An introduction to access security in UMTS”, IEEE Wireless Communications, Volume 11, Pages: 19-25, 2004

[12] C. Xenakis, L. Merakos, “Security in third Generation Mobile Networks”, Computer Communications, Vol.27, pp. 638-650, 2004

[13] Evaluation of UMTS security architecture and services, Abdul Bais, Walter T. Penzhorn, Peter Palensky, 2006 IEEE

[14] 3GPP TR 33.900 (1.2.0), “A Guide to 3G Security” January, 2000.

[15] 3rd Generation Partnership Program. Security Architecture. Technical Specification 33.102. Release 5.Version 5.2.0

[16] Security Architecture in UMTS Third Generation Cellular Networks, Tomas Balderas-Contreras Ren´e A. Cumplido-Parra, Coordinaci´on de Ciencias Computacionales, Instituto Nacional de Astrof´ısica, ´ Optica y Electr´onica, Luis Enrique Erro 1, Sta. Ma. Tonantzintla, 72840, Puebla, MEXICO

[17] Security Mechanisms in UMTS Stefan Pütz, Roland Schmitz, Tobias Martin, DuD • Datenschutz und Datensicherheit 25 (2001) X

[18] Prasad, R., W. Mohr, and W. Konhäuser, Third Generation Mobile Communication Systems, Norwood, MA: Artech House, 2000, pp. 243–248.

[19] TS-SCDMA Standards, http://www.cwts.org/.

[20] 3GPP TS 22.004 General on supplementary services

[21] 3GPP TS 22.135 Multicall; Service description; Stage 1

[22] 3GPP TS 23.040 Technical realization of the Short Message Service (SMS)

[23] 3GPP TS 22.140 Multimedia Messaging Service (MMS); Stage 1

[24] http://www.scribd.com/doc/76667295/18/RRC-Setup-Congestion-Monitor

[25] UMTS Capacity simulation study Andrés Felipe Cosme Hurtado Master of Science in Telematics Thesis

[26] http://www.scribd.com/doc/99892559/36/Observation-Point-and-Analysis-Examples-of-Typical-Problems

[27] http://www.finetopix.com/archive/index.php/t-9216.html

[28] UMTS Capacity simulation study Andrés Felipe Cosme Hurtado Master of Science in TelematicsThesis

[29] MODELING AND DIMENSIONING OF THE IUB INTERFACE IN THE UMTS NETWORK M. Stasiak, J. Wiewióra, P. Zwierzykowski Poznan University of Technology, Chair of Communication and Computer Networks

[30] TSGR2#6(99)807, RRC protocol states, Ericsson

[31] Random Access Channel (RACH) Procedure, Senthil Kumar http://www.3g4g.co.uk/Tutorial/SK/sk_rach_procedure.html

[32] RACH Capacity (Part 1 of 2) http://lteuniversity.com/get_trained/expert_opinion1/b/lauroortigoza/archive/2012/03/21/rach-capacity-part-1-of-2.aspx]

[33] Alcatel-Lucent LTE eNodeB Digital Module