PHYSICAL LAYER TEST TRIALS AND ANALYSIS OF CALL DROPS AND REAL TIME THROUGHPUT VERSUS CHANNEL CAPACITY OF THE LONG TERM EVOLUTION (4G) TECHNOLOGY

by

SANIL FULANI

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT ARLINGTON

Spring 2011

ACKNOWLEDGEMENTS

It is an honor for me to show my sincere gratitude for my loving parents and sister for their consistent support and encouragement to make it possible for me to complete my thesis successfully.

I owe my deepest thanks to my advisor, Dr. Qilian Liang, for guiding on the thesis. I also owe my sincere gratitude to engineers from the companies Ericsson, Accuver, Ascom and 3S Network for allowing me to work on the tools and software for my educational purpose and providing me necessary guidance. I am very thankful to my thesis defense committee members, Dr. Alan Davis and Dr. Steven Gibbs, for their time for attending and reviewing my defense.

I am also thankful to my friends and everyone who supported me either directly or indirectly to prove my thesis and even God who made this possible.

January 28, 2011

ABSTRACT

PHYSICAL LAYER TEST TRIALS AND ANALYSIS OF CALL DROPS AND REAL TIME THROUGHPUT VERSUS CHANNEL CAPACITY OF THE LONG TERM EVOLUTION (4G) TECHNOLOGY

Sanil Fulani, MS

The University of Texas at Arlington, 2011

Supervising Professor: Dr. Qilian Liang

Wireless communication has evolved rapidly in recent years and demand for mobile devices with new and higher services is increasing. The 3G standard, Universal Mobile Telecommunication System (UMTS) is already upgraded with High Speed Packet Access (HSPA) to meet current demands, but this is not sufficient considering the current needs of high speed services. Considering the demand for high speed service, 3rd Generation Partnership Project (3GPP) has come up with a technology called Long Term Evolution (LTE) technology called as 4G with an objective of a radio access technology with higher data rates, lower latencies and packet services such as multimedia and games to offer better quality.

LTE is designed with a goal of evolving the radio access technology under the assumption that all services would be packet-switched, rather than following the circuit-switched model of earlier systems. Moreover, LTE is accompanied by an evolution of the non-radio aspects of the complete system, under the term ‘System Architecture Evolution (SAE) which includes the Evolved Packet Core (EPC) network. Together, LTE and SAE comprise the Evolved Packed System (EPS), where both the core network and the radio access networks are fully packet-switched. This thesis mainly emphasizes on Physical layer and a proof for the physical layer message sequence.

The main purpose of this master thesis is to study, analyze and implement a proof of Physical layer process in control plane of LTE system. The focus is on physical layer between the UE and eNB. Test trials were performed and screenshots for the analysis of call drops were taken and included. Results show the achievable Downlink and Uplink throughput in multi user and single user environment compared with the channel capacity of 10MHz channel. The thesis is mainly based on 3GPP LTE specifications and discussions.

The methodology undertaken was divided into five parts. First, the studies part which was mainly based on 3GPP LTE specifications and real time work. Second, the testing part which was performed in a real scenario of LTE system deployed specifically for this test. Third, the analysis part, where the call setup procedure and physical layer message proof is implemented. Also, the call drops incurred during the test and its valid reason is analyzed. Fourth,, the results part whereby the Average and Peak Achievable Downlink and Uplink Throughput for LTE is shown meeting the 4G requirements. Last part shows the conclusion that all the specifications mentioned by 3GPP is followed and proven that LTE is one of the best wireless communication technology of recent time.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview of 4G

4G stands for the fourth generation of cellular communications. It offers speeds that are about 10 times faster than the current third-generation (3G) networks. Its higher data speeds could make smart phones much more comparable to PCs, giving them better multimedia and gaming capabilities. The maximum theoretical data transfer with 3G technology is 2 Mbps. In practice, it will not give more than 500 Kbps to 1.5 Mbps, depending on the carrier, the location of the cell tower, congestion, etc.

LTE is a standard evolved by a group called the 3rd Generation Partnership Project. It is an all-IP network based upon the same core protocol of the internet, TCP/IP. Both LTE and WiMax use the principle of Orthogonal Frequency-Division Multiple Access, which conceptually has been around since the 1960s. OFDMA is based on the idea o1f frequency-division multiplexing, which is a method to transmit multiple data streams over a channel. In case of OFDMA, a digital data stream that needs to be transmitted is split into multiple pieces, each of which is modulated onto a separate carrier. These sub-carriers are combined together at the end. LTE splits the channel into two parts using frequency-division multiplexing, so the download and upload speeds are better balanced.

As shown in Figure 1.1, the uppermost evolution track is that developed in the 3GPP, which is currently the dominant standards development group for mobile radio systems. The second path of evolution has emerged from the IEEE 802 LAN/MAN standards committee, which created the ‘8002.16’ family as a broadband wireless access standard. This family is also fully packet-oriented often referred to as WiMAX. There's quite a bit of debate on whether LTE and WiMax meet all the technical requirementsto be classified 4G technologies. The International Telecommunications Union suggests that

WiMax, the standard that Sprint calls 4G, is actually part of the 3G family, though Sprint markets WiMax as 4G and its speeds are comparable to current LTE speeds. WiMax requires a new network to be built whereas LTE is an evolution of existing CDMA/HSPA networks. The third evolution track shown is led by 3GPP2. Based on the American 'IS95' standard, standardization in 3GPP2 has continued with parallel evolution tracks towards data-oriented systems (EV-DO). Likewise LTE, 3GPP2's latest evolution is a new OFDM-based system called Ultra-Mobile Broadband (UMB). In short the overall evolution pattern is of mobile radio towards flexible, packet-oriented, multiservice systems. More details are given in reference [30].

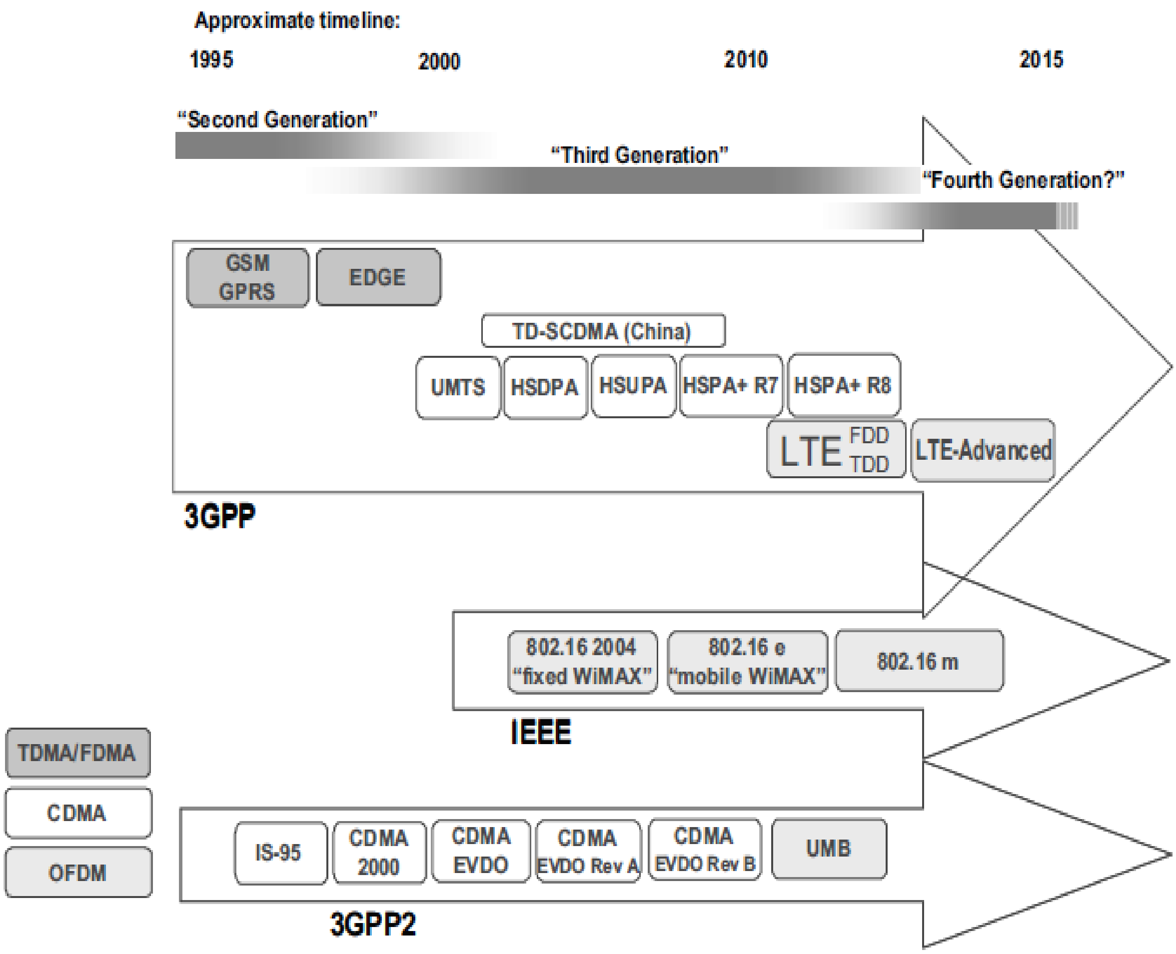


Figure 1.1 Timeline of Mobile Wireless Communication Standards [30]

Table 1.1 Evolution Track for Wireless/Multiple Access Technologies [30]

Generation	**Technologies**	**Multiple Access Technology**
2G	GSM (supports mainly voice)	TDMA/FDMA
2.5G	GPRS/EDGE (Packet Services added)	TDMA/FDMA
3G	UMTS	CDMA, WCDMA
4G	LTE	OFDMA (Downlink) SC FDMA (Uplink)

Within the 3GPP evolution track, some of the multiple access technologies are evident. Second Generation GSM/GPRS/EDGE was based on Time – and Frequency Division Multiple Access (TDMA/FDMA); the Third Generation UMTS technology marked the entry of a new Code Division Multiple Access (CDMA) into the 3GPP evolution track which is also known as Wideband CDMA (due to its 5MHz wide carrier bandwidth). Finally LTE has adopted Orthogonal Frequency Division Multiple Access (OFDMA) which is dominating the latest evolution of all mobile radio standards.

1.2 Motivations for Long Term Evolution

The target in 3GPP Release 8 is to improve the network scalability for increase in the traffic in existing networks and at the same time minimize the end-to-end latency by reducing the number of network elements.

- Need for Reduced latency (transmission and call connection establishment)
- Need for optimized system

  Evolve UMTS towards packet only system
- Potential network and traffic cost reduction
- Improved system capacity and coverage

- Need for increased cell edge bit rate
- Need for cheaper simplified architecture

  More data users
- Need for higher user data rates
- Need for lower power consumption for the mobile terminal
- Need for high quality of services

  Always on experience – reduce control plane latency

  Reduced RTT (Round Trip Time delay)
- Optimized inter-working with other 3GPP and wireless access networks

1.2.1 Key Performance targets for LTE

E-UTRA is expected to support different types of services including video streaming, VoIP, online gaming, real time video, push-to-talk and push-to-view. Hence, LTE is being designed to be a high data rate and a low latency system as given by key performance criteria as given in Table 1.2. The standard bandwidth capability of a UE is expected to be 20MHz for both transmission and reception. However, the service providers are given flexibility to use the bandwidth as given in the table depending on the requirements.

- Data Rate:
  - Instantaneous DL peak data rate of 100Mbps in a 20MHz DL spectrum (i.e. 5 bps/Hz)

    Instantaneous UL peak data rate of 50Mbps in a 20MHz UL spectrum (i.e. 2.5 bps/Hz)
  - Reduced latency to 10 msec round-trip time between user equipment and base station
- Cell Range:
  - 5 km – optimal size

    30 km sizes with reasonable performance

- Cell Capacity:
    - Up to 200 active users per cell (5MHz) (i.e. 200 active data users)
    - larger number of non-active users may also be present in each cell
- Mobility:
    - Optimized for low mobility (0-15 miles/h) even supports high speed
- Multiple Access Scheme:
    - DL: OFDMA (Orthogonal Frequency Division Multiple Access)

      UL: SC-FDMA (Single Carrier Frequency Division Multiple Access)
- Latency:
    a. User plane < 5ms

    It is calculated based on signaling analysis of an unloaded system. It is defined as the average time between the first transmission of a data packet and the reception of a physical layer Acknowledgement (ACK). The calculation should include typical HARQ retransmission rates.

    b. Control plane < 50ms

        i. Call setup delay is required to be significantly reduced compared to existing systems. This significantly affects battery life of terminals, since a fast transition of system from an idle state to an active state enables terminals to spend more time in the low-power idle state.
        ii. Control Plane Latency is measured as the time required for performing the transitions between two main LTE states: 'RRC_IDLE' and 'RRC _CONNECTED' (i.e., 'ACTIVE'). The LTE system should support transition from idle to active in less than 100ms (excluding paging delay and Non-Access Stratum (NAS) signaling delay).
- Inter-Working with other Radio Access Technologies:

  LTE relies on a evolved packet core network which allows interoperation with various access technologies like 3GPP (GSM/EDGE and UTRAN) as well as non-3GPP technologies

(WiFi, CDMA2000 and WiMAX). The continuity of service can only be guaranteed if measurements of signals from other systems and fast handover mechanisms are integrated in the LTE radio access design.

Table 1.2 LTE Performance Requirements

Parameter Metric	**Requirement**
Peak Data Rate	DL:100Mbps UL:50Mbps (for 20MHz Spectrum)
Mobility Support	Upto 400mph but optimized for low speeds from 0 to 10mph
User Plane Latency	Less than 5ms
Control Plane Latency (Transition time from idle to active)	Less than 100ms (transition from idle to active)
Control Plane Capacity	More than 200 users per cell for a 5MHz Spectrum
Coverage (cell size)	5-100km with slight degration after 30km
Spectrum flexibility	1.25, 2.5, 5, 10, 15 and 20MHz Used 10MHz for testing
Carrier frequency	2.6GHz used for testing
Number of antennas (downlink)	e-NB: 1, 2 or 4, UE: 2 or 4
LTE duplex mode	TDD or FDD (Used FDD for testing)
Receiver	Minimum Mean Square Error (MMSE) receiver for testing

1.3 Technologies for Long Term Evolution

1.3.1 Multicarrier Technology

The candidate scheme for Downlink is OFDMA and that for uplink is SC-FDMA. OFDMA subdivides the available bandwidth for signal transmission into a multitude of narrowband subcarriers, arranged mutually orthogonal, which either individually or in groups can carry independent information streams. When a high data stream is transmitted serially, it incurs a problem in having a symbol period Ts much smaller than the channel delay spread Td. This results into Inter-Symbol Interference (ISI). It is possible to overcome this interference only by means of a complex equalization procedure.

In OFDM, the high rate stream of data symbols is first converted from serial to parallel for modulation onto M parallel subcarriers as given in Figure 1.2. This results in an increase of symbol duration on each subcarrier by a factor of approximately M so that it becomes significantly longer than the channel delay spread. In telecommunications, the delay spread is a measure of the multipath richness of a channel.

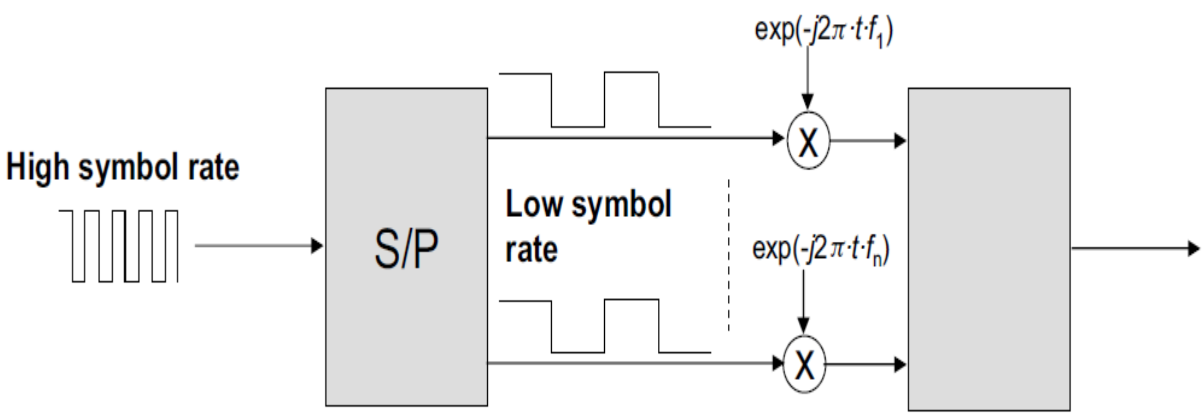


Figure 1.2 Serial-to-parallel conversions in OFDMA [30]

In OFDM, the sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, so that cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required. This greatly simplifies the design of both the transmitter and the receiver; unlike conventional FDM, a separate filter for each sub-channel is not required.

The orthogonality allows high spectral efficiency, with a total symbol rate near the Nyquist rate for the equivalent baseband signal (i.e. near half the Nyquist rate for the double-side band physical passband signal). Almost the whole available frequency band can be used. OFDM generally has a nearly 'white' spectrum, giving it benign electromagnetic interference properties with respect to other co-channel users.

OFDMA requires very accurate frequency synchronization between the receiver and the transmitter; with frequency deviation the sub-carriers will no longer be orthogonal, causing inter-carrier interference (ICI) (i.e., cross-talk between the sub-carriers). Frequency offsets are typically caused by mismatched transmitter and receiver oscillators, or by Doppler shift due to movement. While Doppler shift alone may be compensated by the receiver, the situation is degraded when combined with multipath, as since reflections will appear at various frequency offsets, which is much harder to correct. This effect typically gets worse as speed increases, and is an important factor limiting the use of OFDMA in high-speed vehicles. Several techniques for ICI suppression are suggested, but they may increase the receiver complexity [30].

1.3.1.1 Advantages of OFDMA

- Utilization of different spectrum bandwidths without changing basic system parameters or equipment design
- Possible to allocate different users the transmission resources of variable bandwidth and schedule them freely in the frequency domain
- low complexity of receivers
- In broadcast networks, simple combining of signals from multiple transmitters possible

1.3.1.2 Disadvantages of OFDMA

Since, the Peak-to-Average Power Ratio (PAPR) of an OFDM signal is relatively high, it results in a need for highly linear RF power amplifier and hence in turn the cost of transmitter design for OFDM rises. Use of OFDM for downlink transmissions does not suffer from this limitation as low-cost implementation has a lower priority for the base station than for the mobile terminal. In Uplink, The high PAPR of OFDM is difficult to tolerate for the transmitter of the mobile terminal, since it is necessary to compromise between the output power required for good outdoor coverage, power consumption, and the cost of the power amplifier.

SC-FDMA has a significantly lower PAPR, it therefore benefits from the advantages of multicarrier technology while at the same time avoiding excessive cost for the mobile terminal transmitter and retaining reasonable degree of commonality between uplink and downlink technologies. The other candidate for LTE was WCDMA but since LTE needs to remain competitive for many years, the initial benefits of technology reuse from UMTS become less advantageous in the long-term; as it would deprive from using OFDM with its flexibility, low receiver complexity and high performance in time dispersive channels [30].

1.3.2 Multi-Antenna Technology

- Diversity Gain: Improve robustness of transmission against multipath fading.
- Array Gain: Gives concentration of energy in one or more directions via pre-coding or beam forming. This gives multi-user MIMO capability to serve multiple users located in different directions to be served simultaneously.
- Spatial multiplexing gain: Supports transmission of multiple signal streams to a single user on multiple spatial layers created by combinations of the available antennas.

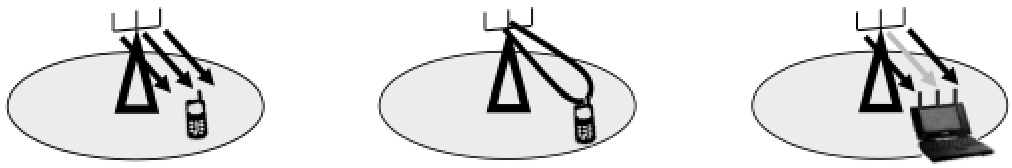


Figure 1.3 Multi-Antenna Scheme (a) Diversity Gain, (b) Array Gain and (c) Spatial multiplexing gain [30]

1.3.3 Adaptive Modulation and Coding Scheme

LTE supports different modulation techniques for both Uplink and Downlink. It supports 64QAM that is 6 bits per radio symbol for Downlink modulation and 16QAM that is 4 bits per radio symbol for Uplink modulation.

The OFDM signal used in LTE contains a maximum of 2048 different sub-carriers having a spacing of 15 kHz. Although it is mandatory for the mobiles to have the capability to be able to receive all 2048 sub-carriers, not all need to be transmitted by the base station which only needs to be able to support the transmission of 72 sub-carriers. In this way all mobiles will be able to talk to any base station. The exact format is chosen depending upon the prevailing conditions. The lower forms of modulation, (QPSK) do not require such a large signal to noise ratio but are not able to send the data as fast. Only when there is a sufficient signal to noise ratio can the higher order modulation format be used. Due to orthogonality between signals and also only two reference signals are present per Resource Block there is will be hardly any interference.

The channel coding scheme for transport blocks in LTE is Turbo Coding with a coding rate of R=1/3, two 8-state constituent encoders and a contention-free internal inter-leaver. Trellis termination is used for the turbo coding. Before the turbo coding, transport blocks are segmented into byte aligned segments with a maximum information block size of 6144 bits. Error detection is supported by 24 bit CRC.

CHAPTER 2

LTE NETWORK ARCHITECTURE

One of the major architectural changes as seen in Figure 2.1 is that in the core network area, the EPC does not contain a circuit switched domain and no direct connectivity to traditional circuit switched networks such as PSTN or ISDN is needed in this layer. LTE being the only all packet switched service model, follows the non-radio aspects of the system in terms called ‘System Architecture Evolution’ (SAE) that includes Evolved Packet Core (EPC) network. LTE encompasses the evolution of radio access and non radio aspects under Evolved- UTRAN (EUTRAN) and System Architecture Evolution (SAE) respectively. Together, LTE and SAE are called Evolved Packet System (EPS) where both the core network and radio access fully support packet switched services. UE, EUTRAN and EPC are connected with each other via the Internet Protocol (IP) connectivity layer. All our eNB are directly connected to each other via X2 interface. Hence, we observe that it does not having anything equivalent to RNC like in UMTS or 1XEVDO or BSC as in GSM. In core network, there are primarily four key nodes. Comparing MME and S-GW node with UMTS node than it is similar to SGSN GW and Data GW as in UMTS. And HSS could be compared to HLR in UMTS. EUTRAN is directly connected to each of these blocks in order to deliver traffic.

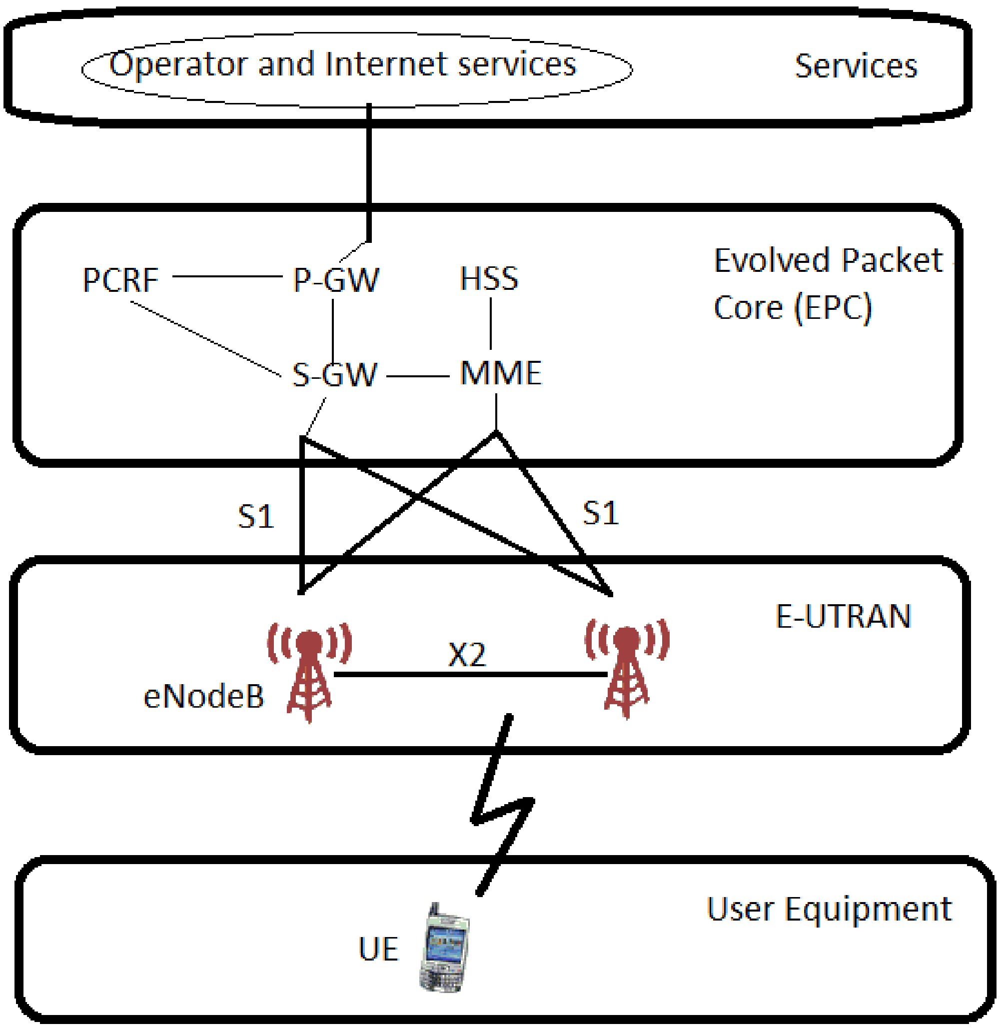


Figure 2.1 LTE Architecture System. Reproduced from different references

Figure 2.2 show the functional split between EUTRAN and EPC. As seen different entities in EPC is responsible for particular function which makes the functionality of LTE unique from other existing networks. EUTRAN and EPC are connected via S1 interface.

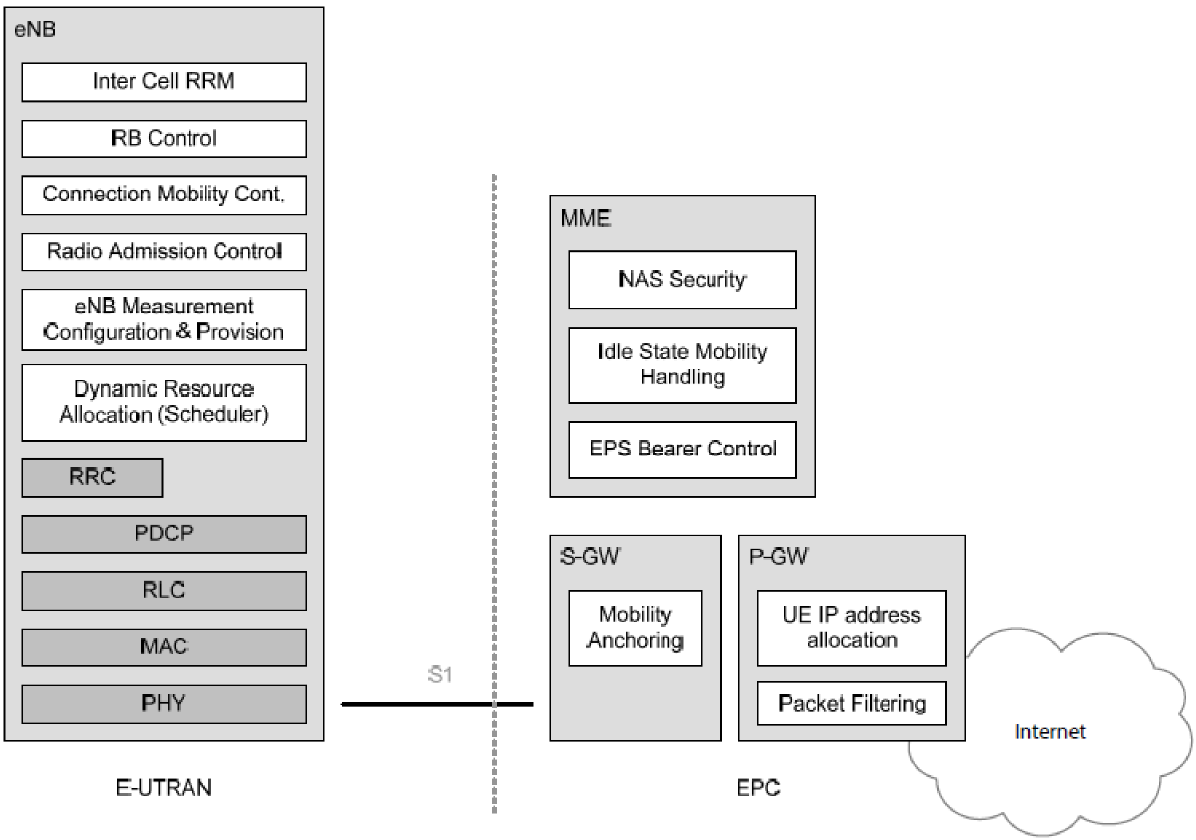


Figure 2.2 Functional split between EUTRAN and EPC. Reproduced from the copyright of 3GPP specifications [30]

2.1 Logical Elements in Basic System Architecture Configuration

2.1.1 User Equipment (UE)

UE is the device that the end user uses for communication. Typically it is a handheld device such as a smart phone or a data card as shown in Figure 2.3.(a) and Figure 2.3 (b) such as those used currently in 2G and 3G or it could be embedded to a laptop. It contains Universal Subscriber Identity Module (USIM) that is a different module from the rest of the UE which is also called the Terminal Equipment (TE). USIM is a type of application placed into a removable smart card called the Universal Integrated Circuit Card (UICC) and hence USIM is used to identify and authenticate the user and derive and possess security keys for protecting the radio interface transmission.

(a)

(b)

Figure 2.3 UE types, (a) Example of Data Card type of UE (b) Example of Smart Phone type of UE
Source: www.google.com

Functions: UE signals with the network for setting up, maintain and remove the communication links for end user needs. The functions includes mobility management functions such as handovers and reporting the terminals location and the parameter details that UE possess and uses during the process of call setup.

2.1.2 Access Network (EUTRAN)

EUTRAN consists of a network of e-NBs as shown in Figure 2.4. The protocols running between e-NBs and the UE are known as the Access Stratum (AS) protocols. Functionally eNodeB acts as a layer 2 bridge between UE and the EPC as it's the termination point of all the radio protocols towards the UE and relaying data between the radio connection and the corresponding IP based connectivity towards the

EPC. When a new UE activates under an eNodeB and requests for a connection setup to the network, the eNodeB routes this request to the MME that previously served that UE or selects a new MME, if a route to the previous MME is not available or routing information is absent. The eNodeB controls and analyses radio signal level measurements carried out by the UE, make similar changes itself and based on those makes decisions to handover UEs between cells. This even includes exchanging handover signaling between other eNodeBs and the MME. Hence, eNodeB plays an important role in Mobility Management.

There are two types of interfaces in EUTRAN. First is the X2 Interface. The e-NBs are inter-connected with each other by means of X2 interface. Second is called the S1 Interface: The e-NBs are normally inter-connected with EPS by means of S1 interface. Specifically, to MME by means of the S1-MME interface and to the S-GW by means of the S1-U interface.

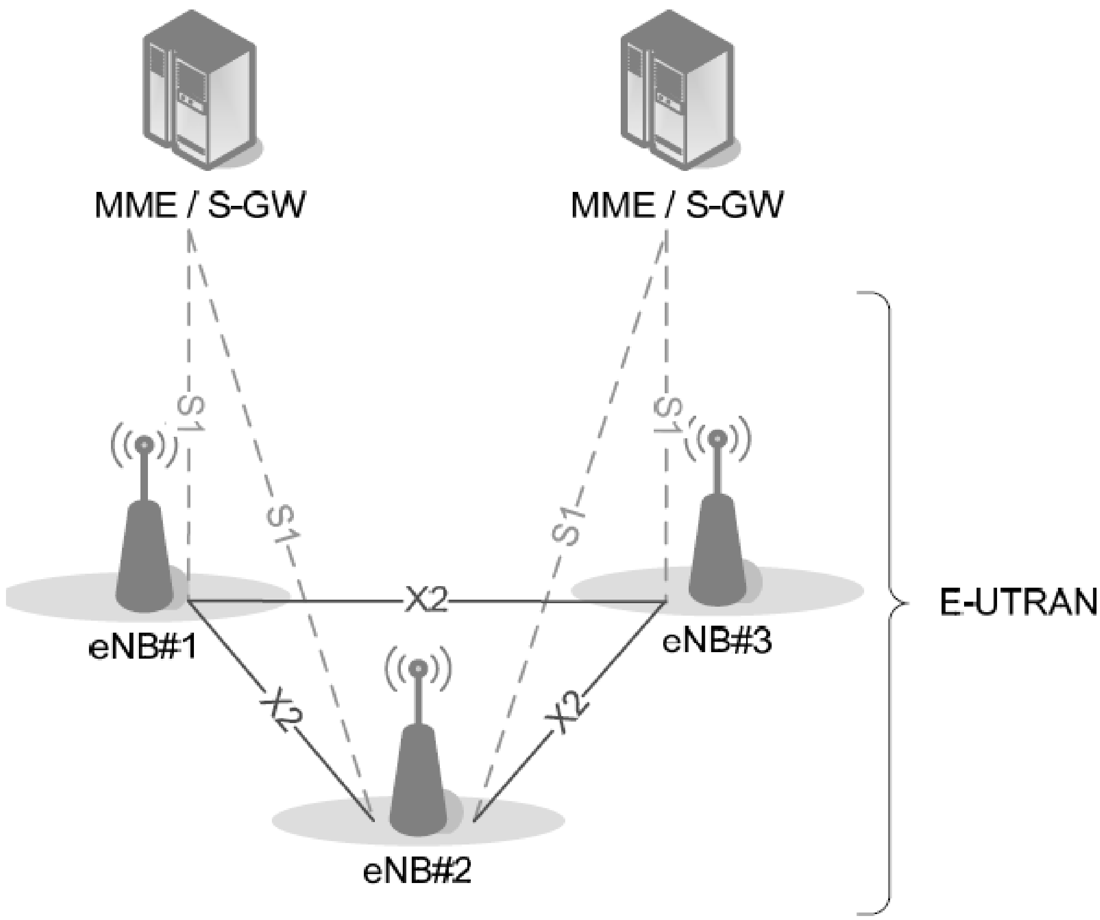


Figure 2.4 EUTRAN Architecture [30]

2.1.2.1 Functions of EUTRAN

- **Radio Resource Management.** Includes functions like radio bearers, such as radio bearer control, radio admission control, radio mobility control and dynamic allocation of resources to UEs in both uplink and downlink.
- **Header Compression.** Ensuring efficient use of radio interface by compressing the IP packet headers. As VoIP has small packets
- **Connectivity to the EPC.** Consisting of the signaling towards the MME and the bearer path towards the S-GW.

Unlike previous generation technologies, LTE integrates the radio controller function into the e-NB. Hence, allowing tight interaction between the different protocol layers of the radio access network. This results in reduction of latency and improving efficiency. This type of distributed control eliminates the need for a high availability which in turn has the potential to reduce costs and avoid ‘single points of failure’.

Also, since LTE does not support soft handover, there is no need for a centralized data-combining function in the network. As a consequence, as the UE moves, the network must transfer all information related to a UE, i.e. ‘UE context’ together with any buffered data, from one e-NB to another. A bearer is an IP packet flow with a specific defined Quality of Service (QoS) between the gateway and the UE. Based on application requirements, the bearers are set up and released by EUTRAN and EPC together. EPS provides the user with IP connectivity to a PDN for accessing the Internet, as well as for Voice over IP (VoIP) services. Multiple bearers can be established for a user to provide different QoS streams. Example is when user is engaged in voice (VoIP) call and at the same time web browsing or FTP (File Transfer Protocol) download.

At a higher level, the network is comprised of CN (EPC) and the access network (EUTRAN). CN consists of many logical nodes, while the access network is made up of essentially one node that is Evolved NodeB (eNB) which connects to the UEs.

2.1.3 Core Network (EPC)

EPC in SAE controls the UE and establishment of bearers. It has the following logical nodes:

- Serving Gateway (S-GW);
- PDN Gateway (P-GW);
- Mobility Management Entity (MME)

2.1.3.1 Serving Gateway (S-GW)

The Serving Gateway serves as the local mobility anchor for the data bearers when the UE moves between e-NBs. For all the data flows belonging to a UE in connected mode, the S-GW relays the data between eNodeB and P-GW. It retains the information about the bearers when the UE is in the idle state known as ECM IDLE and temporarily buffers downlink data while the MME initiates paging of the UE to re-establish the bearers.

One S-GW may serve only a particular geographical area with a limited number of eNodeBs and MMEs. S-GW should be able to connect to any P-GW in the whole network because P-GW will not change during mobility, while the S-GW may be relocated when the UE moves. If one UE is allowed to connect to multiple PDNs through different P-GWs, then the S-GW needs to connect to those separately. It also serves as the mobility anchor for inter-working with other 3GPP technologies such as GPRS and UMTS.

2.1.3.2 Paging Gateway (P-GW)

The Packet Data Network Gateway (P-GW also PDN-GW) is the edge router between the EPS and the external packet data networks. It is the highest level mobility anchor in the whole system that allocates IP address to the UE which in turn is used by the UE to communicate with other IP hosts in external networks e.g. the internet. The IP address is allocated when the UE requests PDN connectivity either during the time of UE attachment to the network or when a new PDN connectivity is needed. The connectivity of the UE to external packet data networks is provided by PDN GW by being the point of entry and exit of traffic for the UE. A single UE may have more than one PDN GW for simultaneous connectivity for accessing multiple PDNs. It performs the required Dynamic Host Configuration Protocol (DHCP) functionality and delivers the address to the UE. It is responsible for filtering of downlink user IP packets into different QoS based bearers and packet screening. When a UE moves from one S-GW to another, the bearers have to be switched in the P-GW. Each P-GW may be connected to one or more PCRF, S-GW and external network. For a given UE that is associated with the P-GW, there is only one S-

GW, but connections to many external networks and respective PCRF is supported, if multiple PDN connectivity is supported through one P-GW. Another important key function of P-GW is to serve as the mobility anchor for inter-working with non-3GPP technologies such as WI-MAX and CDMA2000 networks.

2.1.3.3. Mobility Management Entity (MME)

The Mobility Management Entity is a control node processing signaling between the UE and the CN. It is actually Brain of the EPC that makes all the decisions. It gives key instructions directly to S-GW and indirectly to P-GW for interaction with other nodes. Thinking this way it looks like a router but it's not but actually it's a call processing piece. Main function of MME includes Authentication and Authorization.

Authentication, Security and Connection Management: When any UE registers to the LTE network for the very first time, the MME creates a UE context and initiates the authentication and finds the UE's permanent identity from UE itself or from the previously visited network. It requests from the Home Subscription Server (HSS) in UE's home network, the authentication parameters and compares it with the one received from UE to assure that UE is who it claims to be. The MME calculates UEs ciphering and integrity protection keys from the master key received in the authentication vector from the home network to protect the communication from any unauthorized parties. MME allocates each UE a temporary identity called the Globally Unique Temporary Identity (GUTI), which minimizes the need to send the permanent UE identity that is The International Mobile Subscriber Identity (IMSI). The MME may periodically repeat authentication and may re-allocate GUTI to prevent unauthorized UE tracking. It includes the establishment of the connection and security between the network and UE, and is handled by the connection or mobility management layer in the NAS protocol layer.

Mobility Management: MME keeps track of the location of all UEs in its service area. When a UE registers to the network for the first time, the MME signals the location of the UE to the HSS in the UE's home network, and hence it requests the appropriate resources to be setup in the eNodeB and S-GW selected for the UE. Hence, keeping track of UE at the eNodeB when the UE is in connected mode or at the Tracking Area (TA) level that is a group of eNodeB in case of UE goes into Idle Mode. It is actively involved in the bearer activation/deactivation process and selection of SGW for a UE at the initial attach and at the time of intra-LTE handover involving The Core Network (CN) node relocation. The Non-Access Stratum (NAS) signaling terminates at the MME and then it is responsible for generation and allocation of temporary identities to UEs. It enforces UE roaming restrictions by checking the authorization of the UE to camp on the service provider's Public Land Mobile Network (PLMN). The MME being the termination point in the network for ciphering for NAS signaling handles the security key management.

Non-Access Stratum (NAS) Procedures: The protocols functioning between UE and CN are known as Non-Access Stratum (NAS) protocols. There is faster establishment of the connection and the bearers in LTE. A bearer is an IP packet flow with a defined Quality of Service between the gateway and the UE.

The MME creates a UE context when a UE is turned on and attaches to the network. It assigns a unique short temporary identity, the SAE-Temporary Mobile Subscriber Identity (S-TMSI) to the UE which identifies the UE context in the MME. This UE context holds user subscription information downloaded from the HSS. The local storage of subscription data in the MME allows faster execution of procedures such as bearer establishment since it removes the need to consult the HSS every time. UE context also holds dynamic information such as the list of bearers that are established and the terminal capabilities.

All UE-related information in the access network is released during long periods of data inactivity to reduce EUTRAN overhead and processing in the UE. This state is called EPS Connection Management IDLE (ECM-IDLE). The UE context and the information about the established bearers is retained by MME during these idle periods. To allow the network to contact an ECM-IDLE UE, the UE updates the networkwith its new location whenever it moves out of its current Tracking Area (TA). This procedure is called a 'Tracking Area Update'. It is the responsibility of MME to keep track of the user location while the UE is in ECM-IDLE.

When there is a need to deliver downlink data to an ECM-IDLE UE, the MME sends a paging message to all the e-NBs in its current TA, and the e-NBs page the UE over the radio interface. The UE performs a service request procedure on receipt of a paging message which results in moving the UE to the ECM-CONNECTED state. Hence the UE related information is thereby created in the EUTRAN and the bearers are re-established. The MME here is responsible for the re-establishment of the radio bearers and updating the UE context in the e-NB. This transition between the UE states is called an idle-to-active transition. To speed up the idle-to-active transition and bearer establishment, EPS supports concatenation of the NAS and AS procedures for bearer activation. Some procedures such as the bearer establishment procedure can be executed by the network without waiting for the completion of the security procedure, run simultaneously rather than sequentially for fast execution.

Security functions is the responsibility of MME for both signaling and user data. A mutual authentication of the UE and the network is performed between the UE and the MME/HSS.

2.1.3.4 Policy Control and Charging Rules Function (PCRF)

PCRF is the network element responsible for Policy and Charging Control (PCC). It is also responsible for policy control decision making, controlling flow-based charging functionalities in the Policy Control Enforcement Function (PCEF) which resides in P-GW. The PCRF provides information called PCC rules to the PCEF whenever a new bearer is to be set up. The PCRF provides QoS authorization that decides how a certain data flow will be in treated in PCEF.

2.1.3.5 Home Location Register (HLR)

HSS is a database server that is maintained centrally in the home operator's premises and records the location of the user in the level of the visited network control node, such as MME. HSS stores the master copy of the subscriber profile containing information about the PDNs to which the user can connect which could be in Access Point Name (APN) form or a PDN Address form (indicating subscribed

IP). HSS uses Diameter Protocol to interact with MME. It stores the master copy of the subscriber profile containing information about the PDNs to which the user can connect, identity of MME to which user is presently attached or registered.

Holds dynamic information such as identity of the MME to which user is presently attached or registered generating the vectors for authentication and security keys. The HSS is needed to be able to connect with every MME in the whole network, where its UEs are allowed to move. The HSS records will point to one serving MME at a time for each of the UE and when a new MME reports it is serving a UE, the HSS will cancel the location from the previous MME.

CHAPTER 3

LTE PROTOCOL ARCHITECTURE

3.1 User Plane Protocol

3.1.1 Packet Data Convergence Protocol (PDCP) layer

The main functions of PDCP layer are header compression, security (includes integrity protection and ciphering) and support for retransmission during handover. This layer also includes processing of Radio Resource Control (RRC) messages and Internet Protocol packets in control plane and user plane respectively.

3.1.2 Radio Link Control (RLC) layer

The main function of RLC layer includes segmentation and reassembly of upper layer packets so as to adapt the packets to size which can be transmitted. It also performs retransmission to recover from packet losses in an error free transmission and performs reordering of out of order packets received due to Hybrid Automatic Repeat request (HARQ) operation in the layer below it.

3.1.3 Medium Access Control (MAC) layer

The task of multiplexing data from different radio bearers is performed by the MAC layer. There is only one MAC entity per UE. At the transmitting side, each layer receives a Service Data Unit (SDU) from a higher layer, for which the layer provides a service and outputs a Protocol Data Unit (PDU) to the layer below. For example, the packets received by RLC layer from PDCP layer are called PDCP PDUs from PDCP side and represent RLC SDUs from RLC side.

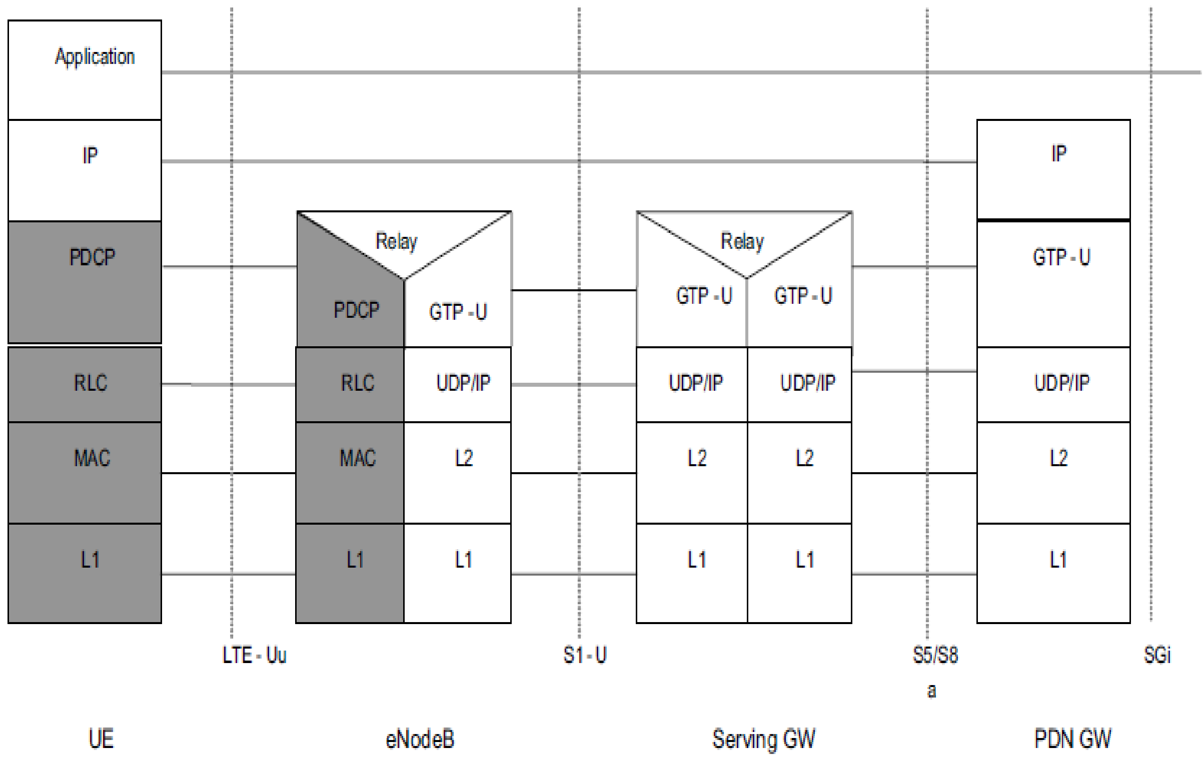


Figure 3.1 User Plane Protocol Stack [30]

3.2 Control Plane Protocol

The protocol stack for the control plane between the UE and MME is shown in the figure 3.2. The Access Stratum Protocols in Figure 3.1 are indicated by grey region. Lower layers in control plane perform the same functions as in user plane but the only exception is that there is no header compression function for the control plane. The main controlling function in the access stratum protocol stack is the RRC protocol also known as 'Layer 3'. It is responsible for configuring all the lower layers using RRC signaling between the e-NB and the UE, and it is also responsible for establishing the radio bearers. Control Plane of the Access Stratum (AS) handles radio-specific functionality. The AS interacts with NAS, also called 'upper layers'. The NAS control protocols handle PLMN selection, tracking area update, paging, authentication and Evolved Packet System (EPS) bearer establishment, modification and release.

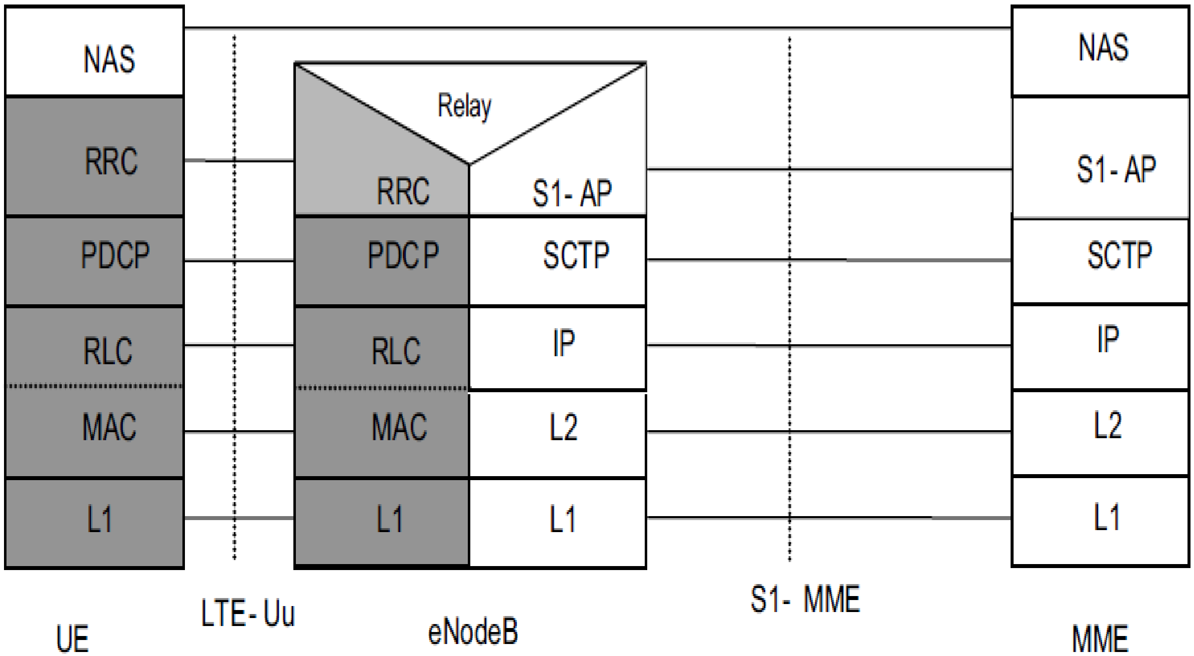


Figure 3.2 Control Plane Protocol Stack [30]

The Access Stratum (AS) control protocol depends on the Radio Resource Control (RRC) state of the UE which is either RRC_IDLE or RRC_CONNECTED. A UE in RRC_IDLE performs cell selection and reselection as discussed earlier, and decides on which cell to camp. An RRC_IDLE UE monitors a paging channel to detect incoming calls, and also acquires system information which mainly consists of parameters by which E-UTRNA can control the cell (re)selection process. RRC is a protocol by which the EUTRAN controls the UE behavior in RRC_CONNECTED mode. RRC protocol supports transfer of two NAS information namely common NAS information that is applicable to all UEs and dedicated NAS information that is applicable to only a specific UE. It supports the following functions.

- **System Information:** This includes the broadcasting of system information that includes NAS common information that is applied to UEs in RRC_IDLE and in RRC_CONNECTED.
- **RRC Connection Control:** It covers all the procedures related to call establishment, modification and release of an RRC connection. It also includes information of paging, initial security

activation, information of establishment of Signaling Radio Bearers (SRBs) and of Data Radio Bearers, that is the bearers carrying user data information and information of radio link failure.

- **Network controlled inter-RAT mobility.** This includes security activation procedures and transfer of UE RRC context information and also mobility procedure information.
- **Measurement configuration and reporting.** This includes information for inter-frequency, intra-frequency, inter-RAT mobility configuration and activation of measurements.

3.3 Channel Structure of LTE

To efficiently support various QoS classes of services, LTE adopts a hierarchical channel structure. There are three different channel types defined in LTE. They are give below:

- Logical channels (What to Transmit)
  - Logical Control Channels
  - Logical Traffic Channels
- Transport channels (How to Transmit) and
  - Downlink Transport Channel
  - Uplink Transport Channel
- Physical Channels (Actual Transmission)
  - Downlink Physical Channel
  - Uplink Physical Channel

As shown in Figure 3.3, the RLC layer passes data to the MAC layer as logical channels. The MAC Layer formats and sends the logical channel data as transport channel. And the Physical layer encodes the transport channel data to physical channels. Each of these channels is associated with a service access point (SAP) between different layers. These channels are used by the lower layers of the protocol stack to provide services to the higher layers. The radio interface protocol architecture and the SAPs between different layers are shown in Figure 3.3. Logical channels provide services at the SAP between MAC and RLC layers, while transport channels provide services at the SAP between MAC and

PHY layers. Physical channels are the actual implementation of transport channels over the radio interface. LTE is based entirely on shared and broadcast channels and contains no dedicated channels carrying data to specific UEs. This improves the efficiency of the radio interface and can support dynamic resource allocation between different UEs depending on their traffic/QoS requirements and their respective channel conditions. In this section, we describe in detail the various logical, transport, and physical channels that are defined in LTE.

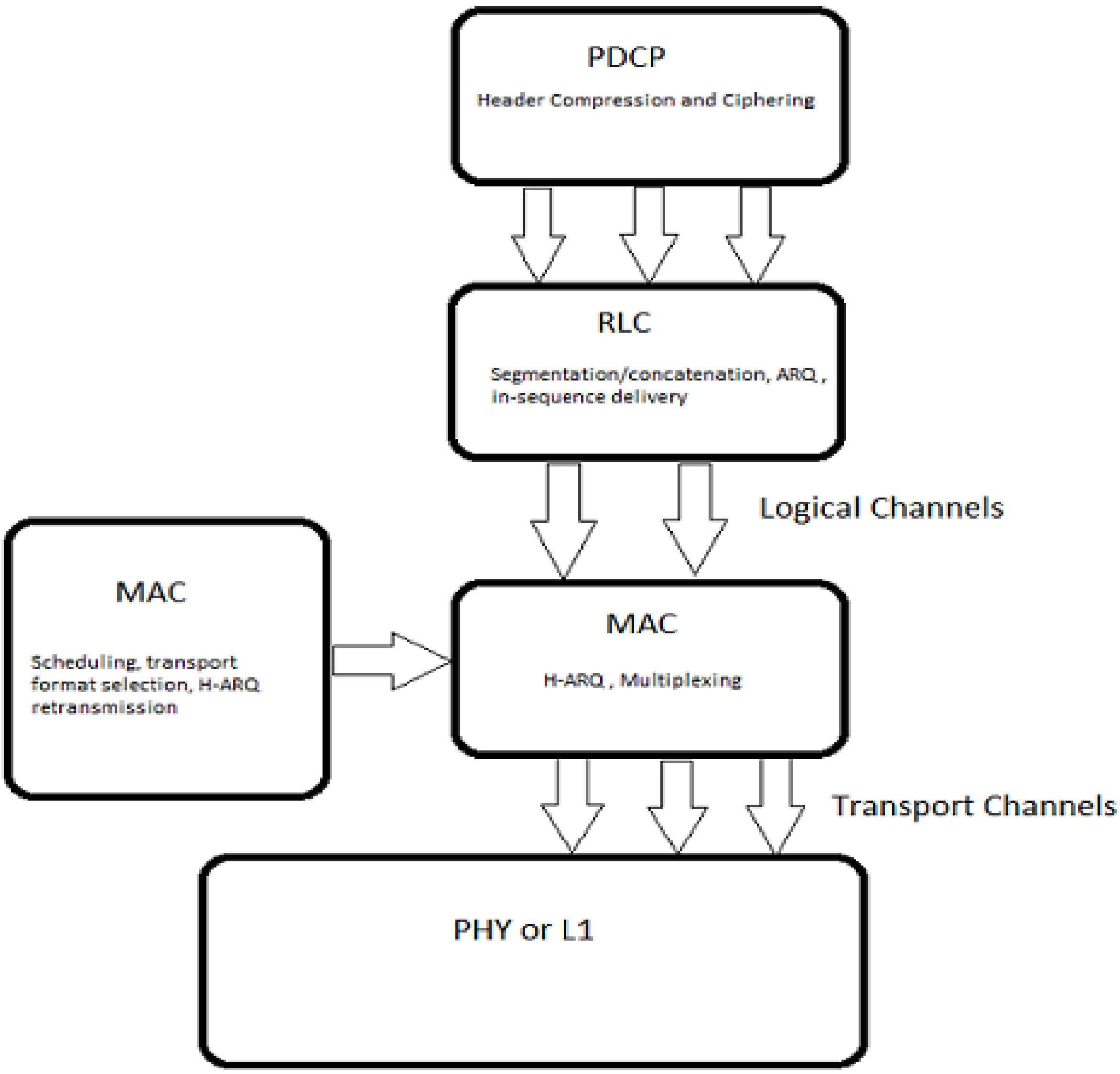


Figure 3.3 LTE Channel Structure. Reproduced from different references

3.3.1 Logical Channels: What to Transmit

Logical channels are used by the MAC to provide services to the RLC. Each logical channel is defined based on the type of information it carries. In LTE, there are two categories of logical channels depending on the service they provide: logical control channels and logical traffic channels. The logical control channels, which are used to transfer control plane information, include the following types:

- **Broadcast Control Channel (BCCH):** This control channel provides system information to all mobile terminals connected to the eNodeB. A downlink common channel used to broadcast system control information like downlink system bandwidth, antenna configuration, and reference signal power to the mobile terminals in the cell. Due to the large amount of information carried on the BCCH, it is mapped to two different transport channels: the Broadcast Channel (BCH) and the Downlink Shared Channel (DL-SCH).
- **Paging Control Channel (PCCH):** A downlink channel that transfers paging information to registered UEs in the cell, for example, when searching a unit on a network.
- **Common Control Channel (CCCH):** A bi-directional channel for transmitting control information between network and UEs when no RRC connection is available, implying the UE is not attached to the network such as in the idle state. Mostly, CCCH is used during the random access procedure, e.g. for actions including setting up a connection.
- **Multicast Control Channel (MCCH):** A point-to-multipoint downlink channel used for transmitting control information to UEs in the cell. It is only used by UEs that receive multicast/broadcast services.
- **Dedicated Control Channel (DCCH):** A point-to-point, bi-directional channel that transmits dedicated control information between a UE and the network. This channel is used when the RRC connection is available, that is, the UE is attached to the network. This control channel is used for carrying user-specific control information, e.g. for controlling actions including power control, handover, etc.

The logical traffic channels, which are to transfer user plane information, include:

- **Dedicated Traffic Channel (DTCH):** A point-to-point, bi-directional channel used between a given UE and the network. It can exist in both uplink and downlink and used for the transmission of user data.
- **Multicast Traffic Channel (MTCH):** A unidirectional, point-to-multipoint data channel that transmits traffic data from the network to UEs. It is associated with the multicast/broadcast service.

3.3.2 Transport Channels: How to Transmit

The transport channels are used by the Physical layer to offer services to the MAC layer. The LTE transport channels vary between the uplink and the downlink since each has different requirements and operates in a different manner. A transport channel is basically characterized by how and with what characteristics data is transferred over the radio interface, that is, the channel coding scheme, the modulation scheme, and the antenna mapping. Compared to UTRA/HSPA, the number of transport channels in LTE is reduced since no dedicated channels are present. LTE defines two MAC entities: one in the UE and one in the EUTRAN, which handle the following downlink/uplink transport channels.

3.3.2.1 Downlink Transport Channels

- **Downlink Shared Channel (DL-SCH):** This transport channel is the main channel for downlink data transfer. It is used by many logical channels. Used for transmitting the downlink data, including both control and traffic data, and thus its associated with both logical control and logical traffic channels. By sharing the radio resource among different UEs the DL-SCH is able to maximize the throughput by allocating the resources to the optimum UEs.
- **Broadcast Channel (BCH):** A downlink channel associated with the BCCH logical channel and is used to broadcast system information over the entire coverage area of the cell.

- **Multicast Channel (MCH):** Associated with MCCH and MTCH logical channels for the multicast/broadcast service. It supports Multicast/Broadcast Single Frequency Network (MBSFN) transmission, which transmits the same information on the same radio resource from multiple synchronized base stations to multiple UEs.
- **Paging Channel (PCH):** Associated with the PCCH logical channel. It is mapped to dynamically allocate physical resources, and is required for broadcast over the entire cell coverage area. It is transmitted on the Physical Downlink Shared Channel (PDSCH), and supports UE discontinuous reception.

3.3.2.2 Uplink Transport Channels

- **Uplink Shared Channel (UL-SCH):** It is associated with the CCCH, DCCH, and DTCH logical channels. It supports H-ARQ, dynamic link adaption, and others. The uplink shared channel is counterpart of the DL-SCH.
- **Random Access Channel (RACH):** A specific transport channel that is not mapped to any logical channel. It transmits relatively small amounts of data for initial access or, in the case of RRC, state changes.

The data on each transport channel is organized into transport blocks, and the transmission time of each transport block, also called the Transmission Time Interval (TTI), is 1 ms in LTE. TTI is also the minimum interval for link adaptation and scheduling decision. Without spatial multiplexing, at most one transport block is transmitted to a UE in each TTI and with spatial multiplexing, up to two transport blocks can be transmitted in each TTI to a UE. Besides transport channels, there are different types of control information defined in the MAC layer, which are important for various physical layer procedures. The defined control information includes as shown on the next page.

- **Downlink Control Information (DCI):** It carries information related to downlink/uplink scheduling assignment, modulation and coding scheme, and Transmit Power Control (TPC) command, and is sent over the Physical Downlink Control Channel (PDCCH).
- **Control Format Indicator (CFI):** It indicates how many symbols the DCI spans in that sub frame. It takes values CFI = 1, 2, or 3, and is sent over the Physical Control Format Indicator Channel (PCFICH).
- **H-ARQ Indicator (HI):** It carries H-ARQ acknowledgment in response to uplink transmissions, and is sent over the Physical Hybrid ARQ Indicator Channel (PHICH). HI = 1 for a positive acknowledgment (ACK) and HI = 0 for a negative acknowledgment (NAK).
- **Uplink Control Information (UCI):** It is for measurement indication on the downlink transmission, scheduling request of uplink, and the H-ARQ acknowledgment of downlink transmissions. The UCI can be transmitted either on the Physical Uplink Control Channel (PUCCH) or the Physical Uplink Shared Channel (PUSCH).

3.3.3 Physical Channels: Actual Transmission

Each physical channel corresponds to a set of resource elements in the time-frequency grid that carry information from higher layers. The basic entities that make a physical channel are resource elements and resource blocks. A resource element is a single subcarrier over one OFDM symbol, and typically this could carry one (or two with spatial multiplexing) modulated symbol(s). A resource block is a collection of resource elements and in the frequency domain this represents the smallest quanta of resources that can be allocated.

3.3.3.1 Downlink Physical Channels

- **Physical Downlink Control Channel (PDCCH):** It carries information about the transport format and resource allocation related to the DL-SCH and PCH transport channels, and the H-ARQ information related to the DL-SCH. It also informs the UE about the transport format, resource allocation, and H-ARQ information related to UL-SCH. It is mapped from the DCI transport channel.

- **Physical Downlink Shared Channel (PDSCH):** This channel carries user data and higher-layer signaling. It is used for unicast and paging functions.
- **Physical Broadcast Channel (PBCH):** It corresponds to the BCH transport channel and carries system information for UEs requiring access to the network.
- **Physical Multicast Channel (PMCH):** It carriers multicast/broadcast information for the MBMS service.
- **Physical Hybrid-ARQ Indicator Channel (PHICH):** This channel carries H-ARQ ACK/NAKs associated with uplink data transmissions. It is mapped from the HI transport channel.
- **Physical Control Format Indicator Channel (PCFICH):** It informs the UE about the number of OFDM symbols used for the PDCCH. It provides information to enable the UEs to decode the PDSCH and is mapped from the CFI transport channel.

3.3.3.2 Uplink Physical Channels

- **Physical Uplink Control Channel (PUCCH):** It carries uplink control information including Channel Quality Indicators (CQI), ACK/NAKs for H-ARQ in response to downlink transmission, and uplink scheduling requests.
- **Physical Uplink Shared Channel (PUSCH):** It carries user data and higher layer signaling. It corresponds to the UL-SCH transport channel.
- **Physical Random Access Channel (PRACH):** This channel carries the random access preamble sent by UEs.

Besides physical channels, there are signals in the downlink and uplink physical layer, which do not carry information from higher layers. The physical signals defined in the LTE specifications are

- **Reference signal:** It is defined in both downlink and uplink for channel estimation that enables coherent demodulation and for channel quality measurement to assist user scheduling. There are three different reference signals in the downlink. First is the Cell specific reference signals that are associated with non-MBSFN transmission. Second is the MBSFN reference signals that is associated with MBSFN transmission and third is the UE specific reference signals. There are two types of uplink reference signals. First is the Demodulation reference signals that are associated with transmission of PUSCH or PUCCH and second is the Sounding reference signal that are used to support uplink channel-dependent scheduling.

- **Synchronization signal:** It is split into a primary and a secondary synchronization signal, and is only defined in the downlink to enable acquisition of symbol timing and the precise frequency of the downlink signal.

The Figure 3.4 and Figure 3.5 show mapping of each of these channels with each other to transfer information from the upper layers.

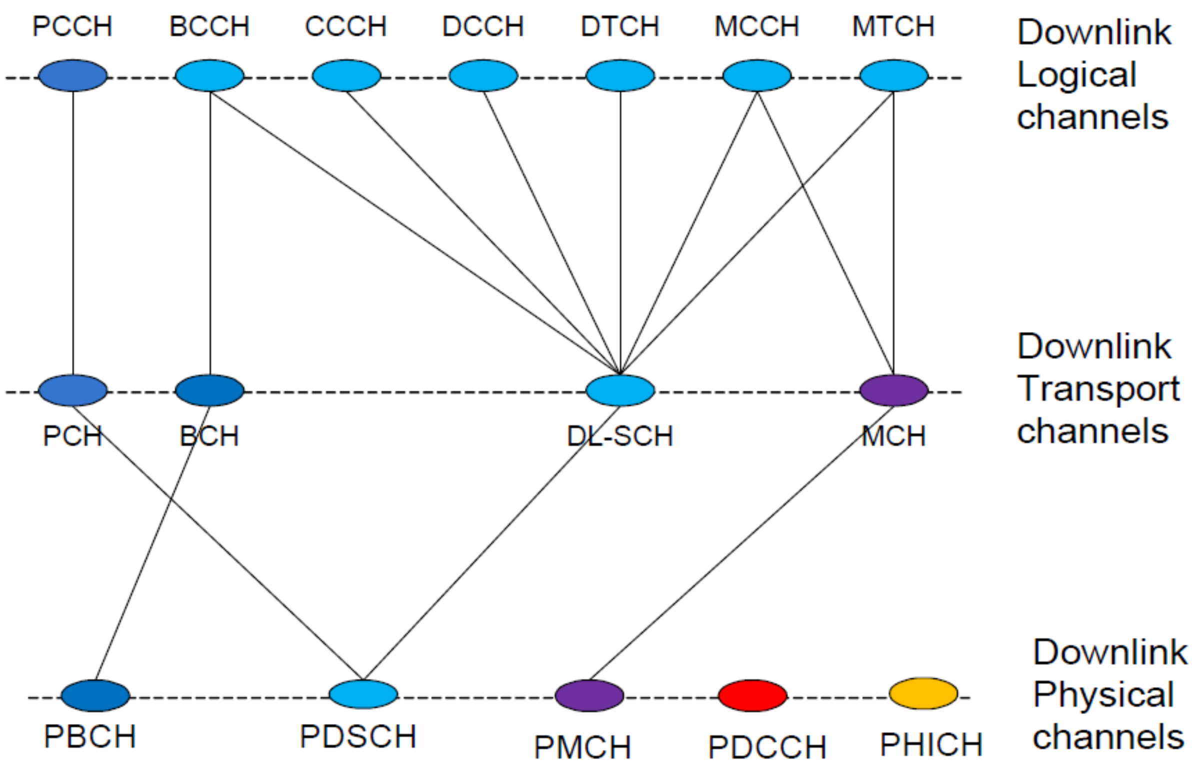


Figure 3.4 Mapping of Downlink LTE channels. Source: EventHelix.com Inc.

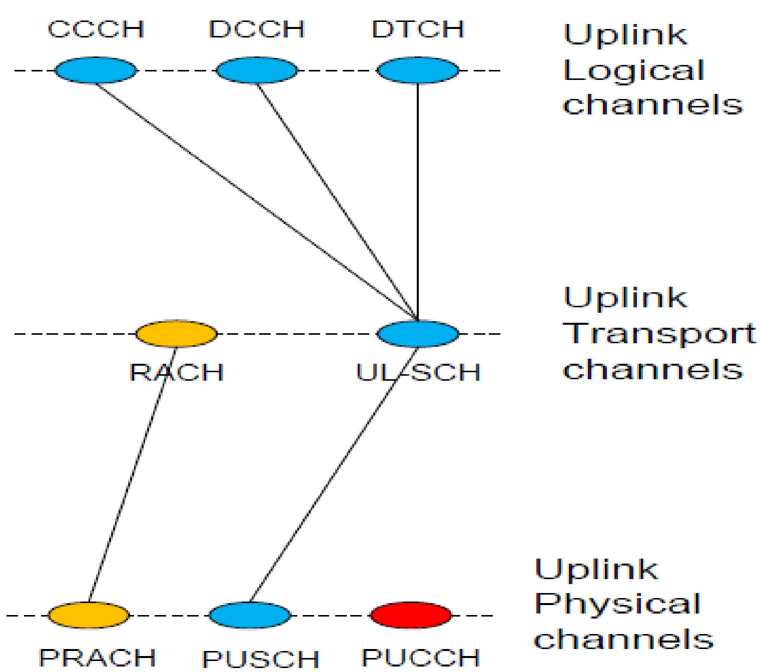


Figure 3.5 Mapping of Uplink LTE channels. Source: EventHelix.com Inc.

CHAPTER 4

PLMN SELECTION

4.1 Mobility States

From mobility perspective, the UE can be in one of the three states LTE_DETACHED, LTE_IDLE and LTE_ACTIVE or RRC_DETACHED, RRC_IDLE and RRC_ACTIVE. When a UE is powered-on and is in the process of searching and registering with the network then the UE is said to be in the LTE_DETACHED STATE. In the LTE_ACTIVE STATE, the UE is registered with the network and has RRC connection with the e-NB. In this state, the network knows the cell to which the UE belongs and can transmit/receive data from the UE. In the LTE_IDLE STATE, the UE is not transmitting or receiving any packets and no context about the UE is stored in the e-NB. The location of the UE is only known at the MME and in the Tracking Area (TA) that consists of multiple e-NBs. The MME has the information about the Tracking Area (TA) in which the UE last registered and the Paging which is necessary to locate the UE to a cell. UE Mobility or Handover takes place only in two modes.

4.2 Categories of Cells in LTE

The cells are categorized according to which services they offer,

- Acceptable Cell. A UE can always attempt an emergency call on an Acceptable Cell. The acceptable cell satisfies certain criteria.
  1. The cell is not barred
  2. Cell selection criteria are fulfilled
- Suitable Cell. This is a cell on which UE can camp on to provide normal service. Suitable cell satisfies some criteria:
  1. The cell should be part of the selected PLN or registered PLMN or equivalent PLMN.

2. The cell should not be barred
3. The cell is part of at least one LA which is not part of the forbidden LA list.
4. The cell selection criteria are full filled.

- Barred Cell. The UE is not allowed to camp on a barred cell. System information 3 indicates whether a cell is barred or not.
- Reserved Cell. This is a cell on which camping is not allowed. Only particular UE are allowed to camp on a reserved cell.

4.3 Service type in Idle and Connected Mode

The action of camping on a cell is necessary to get access to some services. Three levels of services are defined for UE. They are Limited service (emergency calls on an acceptable cell), Normal service (for public use on a suitable cell) and Operator service (for operators only on a reserved cell)

The idle mode procedure of a UE can be classified as four different processes:

- PLMN (Public Land Mobile Network) selection
- Cell selection and reselection
- Location registration
- Support for manual CSG ID selection

The PLMN area is the geographical area in which a PLMN provides communication services according to the specifications to mobile users. In the PLMN area, the mobile user can set up calls to a user of a terminating network. The terminating network may be a fixed network, the same PLMN, another PLMN or other types of PLMN. Terminating network users can also set up calls to the PLMN. The PLMN area is allocated to a PLMN. It is determined by the service and network provider in accordance with any provisions laid down under national law. In general the PLMN area is restricted to one country. If there are several PLMNs in one country, their PLMN areas may overlap. In border areas, the PLMN areas of different countries may overlap. Administrations have to take precautions to ensure that cross border coverage is minimized in adjacent countries unless otherwise agreed.

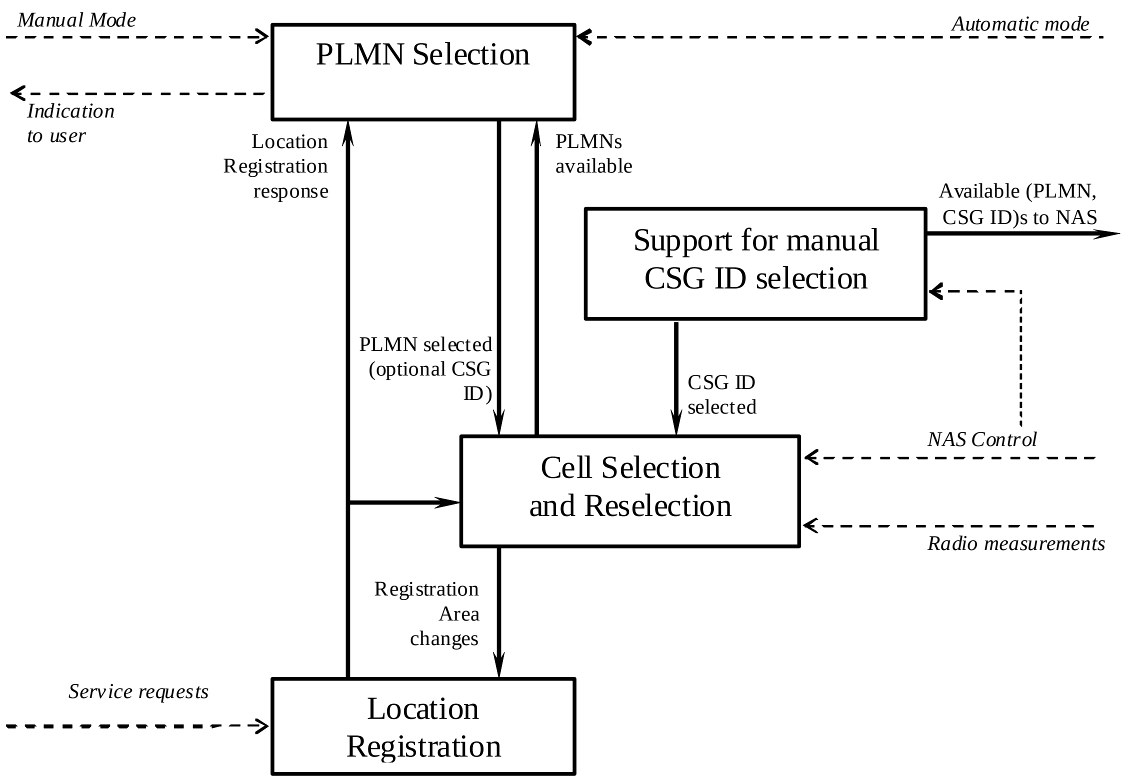


Figure 4.1 Idle Mode process [3]

When a UE is switched on, a Public Land Mobile Network (PLMN) is selected and the UE searches for a suitable cell of this PLMN to camp on. The UE searches for a suitable cell of the selected PLMN and chooses that cell to provide available services, and tunes to its control channel which is known as “camping on the cell”. The UE then registers its presence by means of a NAS registration procedure. After successful Location Registration the selected PLMN becomes a registered PLMN.

If the UE finds a more suitable cell, it reselects that cell and camps on it. If the new cell is in a different registration area, location registration is performed. If necessary, the UE searches for higher priority PLMNs at regular time intervals and search for a suitable cell if another PLMN has been selected by NAS. If the UE loses coverage of the registered PLMN, either a new PLMN is selected automatically (automatic mode), or an indication of which PLMNs are available is given to the user, so that a manual selection can be made (manual mode). Registration is not performed by UEs only capable of services that need no registration. If the UE is unable to find a suitable cell to camp on, or the Universal Subscriber Identity Module (USIM) is not inserted, or if the location registration failed, it attempts to camp on a cell irrespective of the PLMN identity, and enters a "limited service" state in which it can only attempt to make emergency calls. Search of available CSG IDs may be triggered by NAS to support manual CSG ID selection. If the UE loses coverage of the registered PLMN, either a new PLMN is selected automatically (automatic mode), or an indication of which PLMNs are available is given to the user, so that a manual selection can be made (manual mode).

The purpose of camping on a cell in idle mode is that it enables the UE to receive system information from the PLMN. When registered and if the UE wishes to establish an RRC connection, it can do this by initially accessing the network on the control channel of the cell on which it is camped. If the PLMN receives a call for the registered UE, the registration area of the cell in which the UE is camped. It can then send a "paging" message for the UE on control channels of all the cells in the registration area. The UE will then receive the paging message because it is tuned to the control channel of a cell in that registration area and the UE can respond on that control channel. It enables the UE to receive cell broadcast services. The relationship between these processes is illustrated in Figure 4.1

CHAPTER 5

SYNCHORNIZATION, CELL SEARCH AND SELECTION

Before functioning and system performance evaluation are done and after the UE has camped on one PLMN, two important physical layer procedures must be evaluated and validated they are Cell Search and Cell Selection procedures.

Cell Search procedure is necessary since it ensures that the UE's receiver is synchronized in both the frequency and time domain to a downlink LTE signal. The Test Device (TD) is than enabled to receive important parameters via broadcasted system information on a broadcast channel. These parameters are essential to establish uplink synchronization as well as to perform initial access to network. This procedure is called Random Access Procedures which includes functionality from higher layers like the MAC and RRC layers. Before understanding the synchronization and cell search and selection process, we need to understand some basic LTE measurements that play an important role in all three procedures.

5.1 LTE Measurements

Different parameters like power parameters and the parameters that are included in the System Information Broadcasts decide the cell selection. It is responsible for selecting the most suitable cell to camp on for the UE. In a LTE network, a UE measures two parameters on the Reference Signal: RSRP (Reference Signal Received Power) and RSRP (Reference Signal Received Quality). Reference signal is similar to Pilot Signal in UMTS or WiMAX. RSRP is applicable in both RRC_IDLE and RRC_CONNECTED modes, while RSRP is only applicable in RRC_CONNECTED mode.

5.1.1. Reference Signal Received Power (RSRP)

RSRP measurement provides cell-specific signal strength metric. It measures average received power over the resource elements that carry cell-specific reference signal within certain frequency bandwidth. In the procedure of cell selection, cell reselection in idle mode and handover in connected mode, RSRP is used. This measurement is used mainly to rank different LTE candidate cells according to the signal strength and is used as an input for handover and cell reselection decisions. RSRP can be compared to Received Signal Strength Indication (RSSI) in GSM technology and Received Signal Code Power (RSCP) in UMTS technology.

5.1.2. Reference Signal Received Quality (RSRQ)

RSRQ is the quality of the Reference signals. It is not a quality with respect to QoS or bit error rate or packet rate. But, it is quality with respect to noise or interference. It is a Signal to Interference Noise Ratio (SINR).

5.2 Cell Search

For cell selection UE can use one of the following search procedures that is Initial Cell Selection procedure or Stored Information Cell Selection procedure.

5.2.1 Initial Cell Selection

This procedure requires no prior knowledge of which RF channels are required in EUTRA carrier. The UE scans all RF channels in the EUTRA bands according to its capabilities to find a suitable cell. On each carrier, the UE need only search for the strongest cell. Once a suitable cell is found, it is selected. The UE tries to find a cell (not necessarily the best cell, but a usable cell) and camp on it. Once the UE is successfully camped on the cell, UE can get the neighbor list from the system information and tries to camp on the best cell.

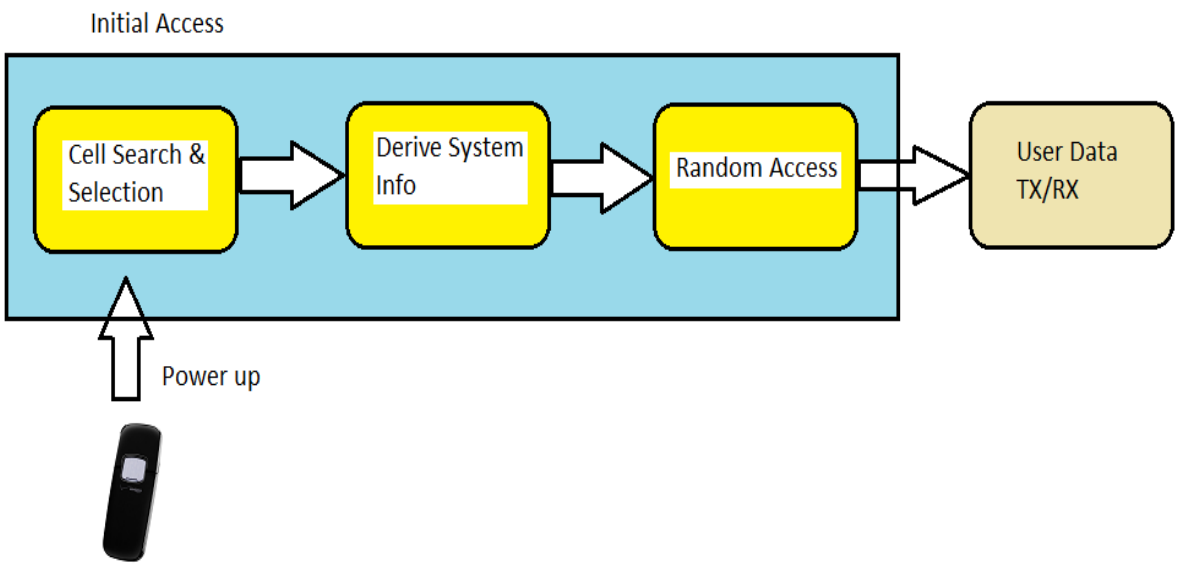


Figure 5.1 Initial Access Process. Reproduced from source [14]

For a given frequency, the UE follows the four steps for initial cell selection as given below:

a. Search for primary synchronization channel (P-SCH): chip and slot synchronization is done
b. Frame synchronization via secondary synchronization channel (S-SCH):
c. Find the primary scrambling code from the common pilot channel (CPICH):
d. Tune to Primary common control physical channel (P-CCPCH) and decode the system information; check whether it is a suitable cell for camping (PLMN code is broadcast)

5.2.2 Stored Information Cell Selection

This procedure requires stored information of carrier frequencies and optionally also information on cell parameters, e.g. scrambling codes, from previously received measurement control information elements. Once the UE has found a suitable cell the UE shall select it. If no suitable cell is found the Initial cell selection procedure shall be started. Frequency and scrambling code may be saved on the phone. The UE may try to synchronize to cell after switching on and on fail starts initial cell selection as above.

5.3 Initial Cell Synchronization

LTE uses a hierarchical cell-search procedure where an LTE radio cell is identified by a cell identity, which is comparable to the scrambling code that is used to separate base stations and cells in WCDMA. When the UE is powered up it needs a network to attach itself. The first towards it is Cell search. Cell Search is a procedure by which a terminal can find a potential cell to attach too. As a part of cell search procedure the terminal obtains the identity of cell and estimates the frame timing of the identified cell. LTE supports 510 different cell identifiers divided into 170-cell identity group of 3 identities each. LTE provides two signals in downlink, the Primary Synchronization Signal and the Secondary Synchronization signal. The process of cell search, cell selection, fetching the system information and random access is known as the LTE Initial Access procedure. In short, mobile terminal or UE acquires time and frequency synchronization with cell and detects the cell ID of that cell based on BCH (Broadcast Channel) signal and hierarchical SCH (Synchronization Channel) signals. The Primary Synchronization signal carries physical layer identity and Secondary Synchronization signal carry physical layer cell identity, and hence, in this way there cell search consists of two steps to identify the cell's identity.

5.3.1 Primary Synchronization Signal (PSS)

In first step of cell search, UE uses primary sync signal to find the timing on 5 ms basis. This signal is transmitted twice in each frame (as LTE frame is of 10 ms). Terminal can use this signal to identify the frame timing with a 5 ms ambiguity. Here terminal locks its local oscillator frequency to the base station carrier frequency. The terminal also finds an identity within the cell. It also obtains partial knowledge about reference signal structure.

5.3.1.1 Zadoff-Chu Sequence

The type of signal used for primary synchronization is a Zadoff-Chu (ZC) sequence. They are CAZAC sequences, which stands for Constant Amplitude Zero Auto Correlation and describes characteristic of ZC sequences. A Zadoff–Chu sequence is a complex-valued mathematical sequence which, when applied to radio signals, gives rise to an electromagnetic signal of constant amplitude, whereby cyclically shifted versions of the sequence comprising the signal do not cross-correlate with each other when the signal is recovered at the receiver. A generated Zadoff–Chu sequence that has not been shifted is known as a "root sequence. The sequence then exhibits the useful property that cyclic-shifted versions of itself remain orthogonal to one another, provided, that is, that each cyclic shift, when viewed within the time domain of the signal, is greater than the combined propagation delay and multi-path delay-spread of that signal between the transmitter and receiver. With constant amplitude, a low peak-to-average power ratio is achieved as zero auto correlation results in good time domain response. The complex value at each position (n) of each root Zadoff–Chu sequence (*u*) given by

$$x_u(n) = e^{-j\pi n(n+1)/Nzc}$$

Where,

Nzc – length of sequence and

$$0 \leq n \leq N_{zc} - 1$$

The Root indices 'u' in the equation determines a ZC sequence from a set of ZC sequences available with the required sequence length Nzc. The root index u depends on the selected physical layer identity and indicates the maximum number of sequences available with a certain length Nzc. Six resource blocks (RB) around the DC subcarrier are reserved for transmission of the synchronization signals in the frequency domain. RB is formed by 12 subcarriers with a spacing of 15 kHz between the subcarriers. Hence, a bandwidth of 180 kHz (12 x 15 kHz) is occupied, reserving a frequency range of 1.08 MHz (6 x 180 kHz) around the center frequency for transmission of synchronization signals (that is, 72 subcarriers). With a use of only

62 of the 72 reserved subcarriers in the primary synchronization signal, the required length, Nzc, of the Zadoff-Chu sequence is given as Nzc=63 including one unused DC subcarrier which is punctured. The reason 62 rather than 72 of the reserved subcarriers are used is because it enables the UE to use a 64 Fast Fourier Transform (FFT) and lower sampling rate. This approach helps to approximate the vendor-specific implementations of an estimation algorithm and simplifies the entire procedure.

5.3.2 Secondary Synchronization Signal (SSS)

In the next step, the terminal then detects the cell identity group and determines the frame timing using a secondary synchronization signal. After the mobile has found the 5 ms time, the second step is to obtain the radio frame timing and the cells' group identity, this can be found from the SSS which also has 5 ms period. The SSS is transmitted in the symbol before the PSS. It is transmitted in the first and sixth subframes (subframes 0 and 5) due to 5 ms periodicity. Like the PSS, the SSS is transmitted on 62 of the 72 reserved subcarriers around the DC subcarrier. The SSS is represented by an interleaved concatenation of two length-31 binary sequences that are scrambled with a sequence that depends on the physical layer identity as the PSS. It is always transmitted as a pair of sequences in a subframe.

5.4 Cell Selection

In the Idle mode the UE performs the following tasks in order to select a cell:

1. When a PLMN is selected the cell selection is made through one of the cell selection procedures.
2. If suitable cell is found the UE camp normally on the cell.

3. In camp normally state the cell reselection is made depending upon the triggers described

4. If no suitable cell found in 2, the UE searches for an acceptable cell and enters the camp on any cell state.

5. In camp on any state the cell reselection is made depending upon the triggers, if no suitable cell found the UE move to any cell state.

6. If suitable cell found in 5 the UE move to the camp normally state.

7. In either state i.e. camped normally or camped on any whenever the UE returns from the connected mode to the idle mode the UE tries to camp on the last cell used for camping in the connected mode.

8. In case last cell in 5 is not a suitable or acceptable cell, procedure 1 and 4 are repeated depending upon the camped state.

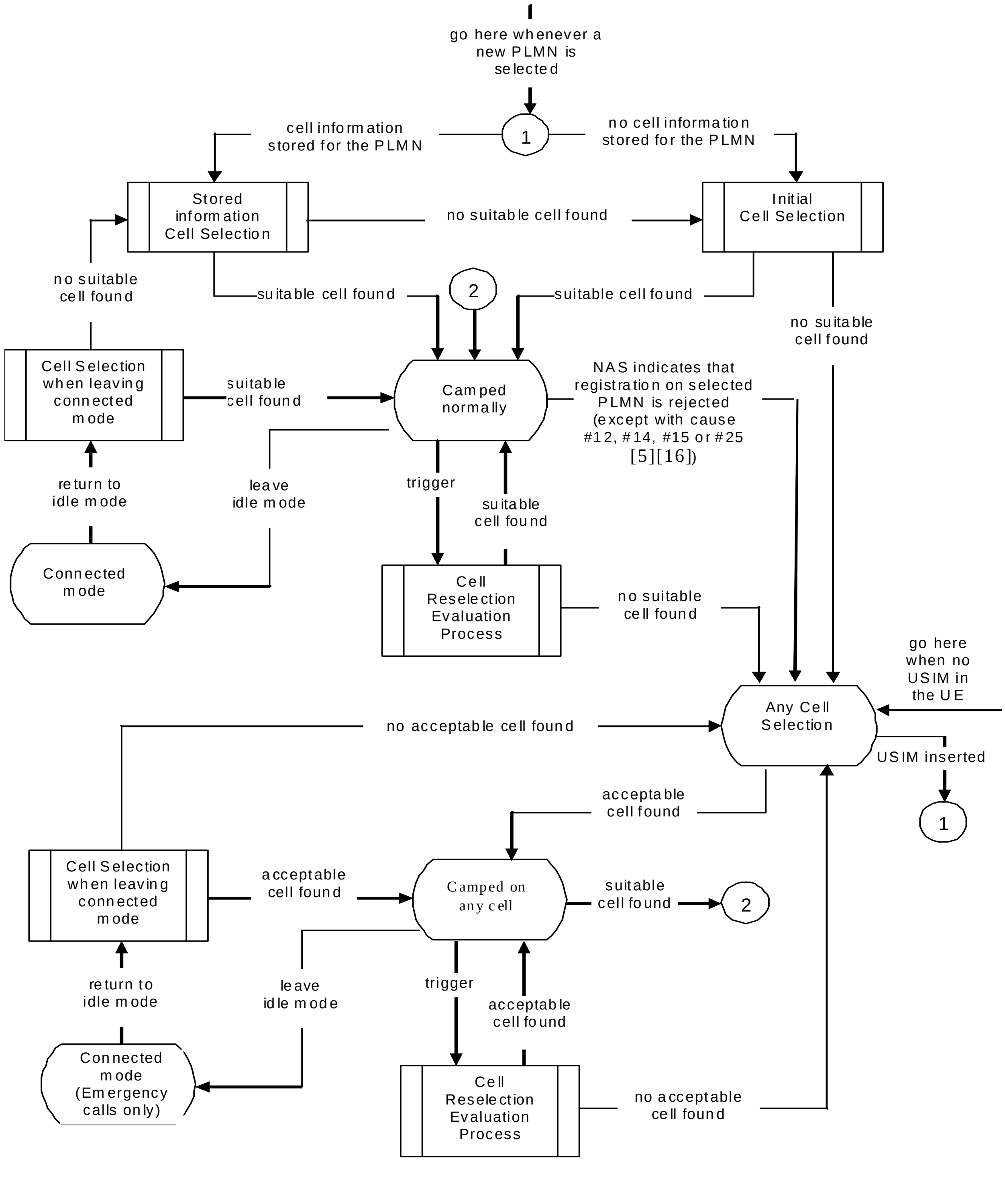


Figure 5.2 Idle Mode Cell Selection and Reselection [3].
In any state, a new PLMN selection causes an exit to number 1 Source 3GPP TS25.304 Specification

5.4.1 Cell Selection Criteria

In order for a cell to be a candidate for a suitable or acceptable cell, the criteria needed to be satisfied is Srxlev > 0 where *Srxlev = Qrxmeasured – Qrxlevmin – Qrxlevminoffset – Pcomposition*

where:

- Srxlev – Cell Selection RX level value (dB)

  Ratio of energy per modulating bit to the noise spectral density the quality. Gives the quality of the cell and is reported from physical layer
- Qrxlevmeas – Measured cell RX level value i.e. Received Signal Received Power (RSRP). This measured value is the linear average over the power of the resource elements that carry the cell-specific reference signals over the considered measurement bandwidth.
- Qrxlevmin – Minimum required RX level in the cell (dBm)
- Qrxlevminoffset – It is an offset to Qrxlevmin that is only taken into account as a result of a periodic search for a higher priority PLMN while camped normally in a Visitor PLMN (VPLMN). This offset is based on information provided within SIB Type 1. The offset is defined to avoid "ping-pong" between different PLMN. If not available then Qrxlevminoffset is assumed to be 0dB.
- Pcompensation – max(UE_TXPWR_MAX_RACH-P_MAX,0) (dB)
  - UE_TXPWR_MAX_RACH – Maximum TX power level UE may use when accessing the cell read in system information message. (dBm)

P_max – Maximum RF output power of the UE (dBm). It is UE dependent value

5.4.2 Cell Reselection Criteria

Cell reselection is performed on the basis of the ranking of the current and the neighboring cells. The ranking is performed on the basis of the following R values [3]

$R_s = Q_{meas,s} + Qhyst_s$

$R_n = Q_{meas,n} – Qoffset_{s,n}$

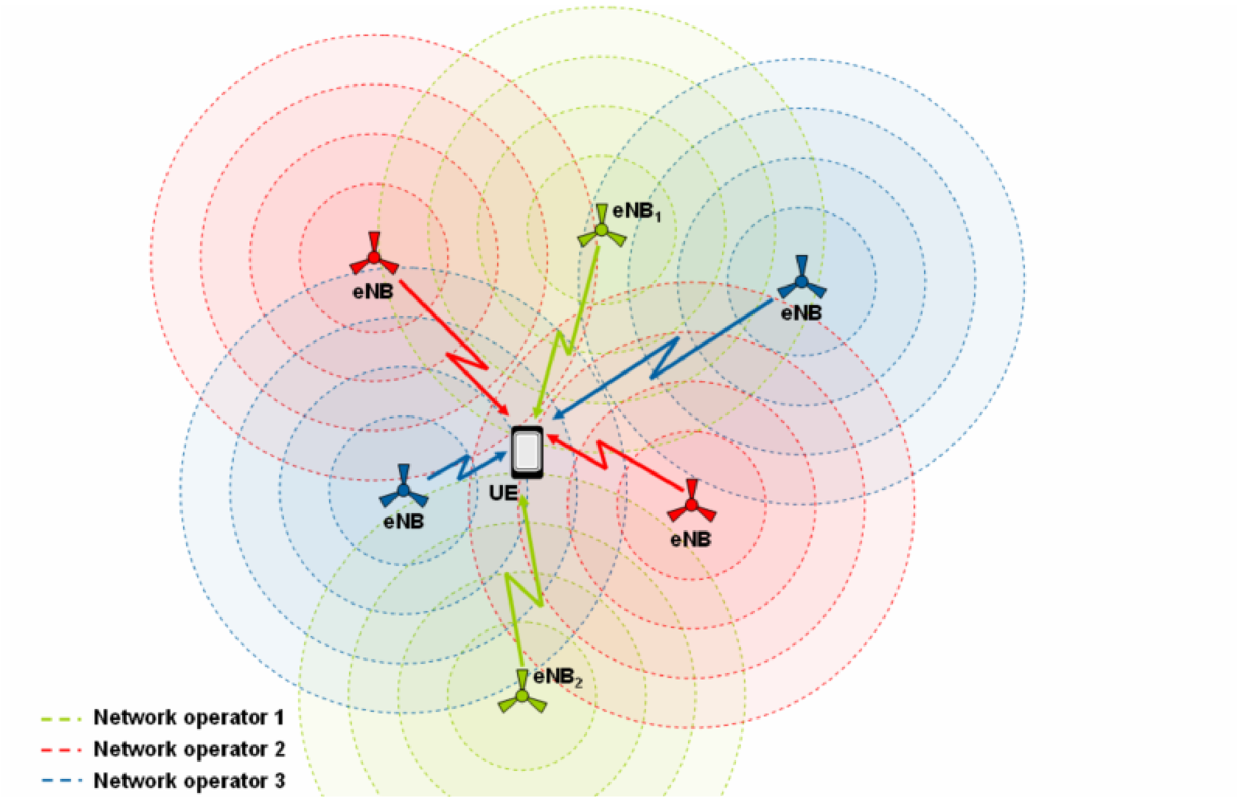


Figure 5.3 Example of Cell Selection Source: Cell search and cell selection in UMTS LTE [14]

Figure 5.3 shown here is a cell selection scenario in a real network. Assume that the UE belongs to network operator 1 (green) and two other carriers also operating in the same LTE network but at different frequencies. The UE receives all eNodeBs at different power levels and based on the definition, the UE will select the strongest cell with network operator 3 and soon finds out after decoding SIB1 that the PLMN saved on the USIM does not match to the transmitted one. It will then stop with its attempt and proceed to the next strongest signal, of operator 2 red and the PLMN will match. The UE uses the information in SIB1 and SIB2 to compute the cell selection criteria. Once the criteria S>0 is fulfilled, UE starts camping on this cell.

CHAPTER 6

CONTRIBUTION – PERFORMANCE ANALYSIS AND PROOF FOR MESSAGE TRANSFER SEQUENCE BETWEEN PHYSICAL LAYER AND EPC

6.1 Drive Test Trials

In this chapter is shown my contribution and here I have shown the study of control plane. The screenshots shows the real time study of control plane messaging taking place between different entities in LTE/SAE architecture. The control plane study involves starting from UE power on that is Detached state and its transition to Idle and Attached state. It also includes study of messages that are exchanged between UE and eNB during the whole process of Connection Establishment, UE Mobility, Handover and Connection Release and tested the cell selection and reselection based on the predefined parameters like SNR, RSRP (Received Signal Reference Power) and others and study how they effect in the performance of the UE in terms of Throughput. This chapter also includes the study results and analysis of drop call that were faced during the time of test and cause for the same.

A predefined route was driven where the LTE eNB is already installed and LTE software is installed on the eNB. During the whole drive, data is collected using software like TEMS Investigation or XCAL. This data will include diverse information of parameters such as LTE frequency, RSRP, SNR, Call setup, Call Establishment, Call Drops, Uplink and Downlink Physical layer Throughput, Handover, and Packet Latency (Round Trip Delay). After the data is collected next step is to process them using software like TEMS Discovery or XCAP. Data is imported into the software, layer 3 messages are studied and studied where exactly in the sector or cell the UE performance is not up to the KPI's (Key Performance Indicator) expectations. Finding the location in the cell or sector where exactly the above mentioned parameters did not meet KPI's and studying how each parameters is significant for cell selection and reselection, handover and throughput for the performance of the LTE system.

The tests were designed and performed to demonstrate the following

- LTE works stable under realistic initial LTE deployment in typical urban and suburban areas, wide and different environmental areas
- The transmission performance inside and at the cell edge of LTE is acceptable
- The achievable data rates in different location and near line of sight of propagation and in multipath conditions in urban areas
- The optimal and achievable throughput rates in a single and multi-user environment
- An important goal of the field testing was to measure throughput and effect of different parameters like RSRP and SNR on cell selection and reselection procedure. And also at the same time to measure and test the relative performance of different antenna setups at the Enhanced Node B (e-NB)

Here, I have carried out experimental results of the working of the real time LTE network and measured the performance of LTE radio systems under real network deployment conditions. A series of drive tests were performed in the vicinity of installed LTE test beds in the center of three major US cities. Analysis of the resulting data helped me to study the performance of Control Plane in LTE and optimize the related LTE sites. All this results were carried out with the help of companies such as Ericsson, Alcatel Lucent, Nokia Siemens Networks and 3S Networks. My drive test results show that the design goals of LTE can be met with an acceptable certainty and reliability as currently incorporated in the 3GPP specifications. The UEs were driven along different diverse routes in three sectors at a speed ranging from 0 – 25miles/h. The routes included Clockwise route, Anti-clockwise route and specific selected routes.

The data collected is stored in a log file for further post process analysis. The results for the stationary tests are shown in the screen shots and graph. The tests were performed with 2x2 MIMO antenna configurations which are commercially deployed in present existing 3G networks. 4x4 MIMO systems will be added in future to handle the increasing traffic in commercial LTE networks. Such a system will require innovation to integrate 4 RX antennas in terminals. The application level performance, measurement results were taken using UDP and TCP traffic over a 2x2 20MHz MIMO at a specific stationary position with good RF condition having SNR in the range of 25 to 30 and RSRP between -65 to -69. LTE system is required to support communication with terminals moving at speeds of up to 200 miles/h depending on band of frequency. These requirements are to be achieved in typical cells of radius up to 3.5 miles up to 70 miles.

6.1.1 Drive test kit setup

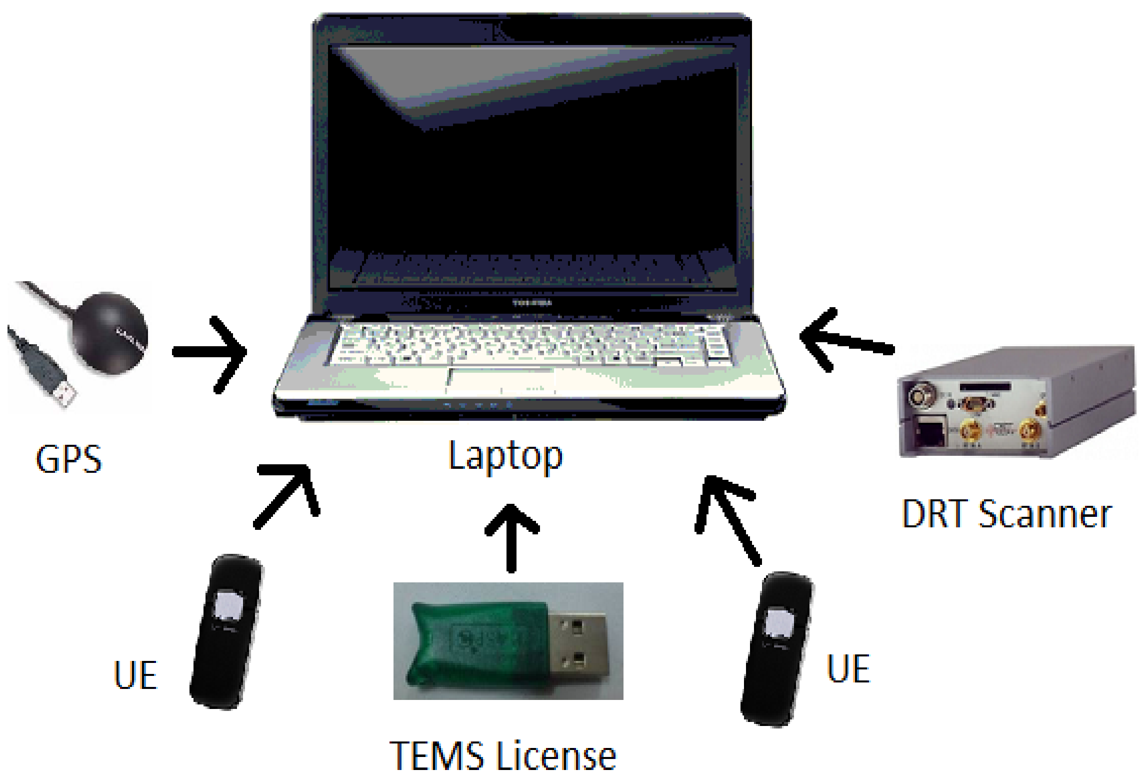


Figure 6.1 Hardware kit setup

All the hardware and software were connected which will be shown in figure in the report and the equipments were mounted inside a driving vehicle like a van.

a) Hardware:

LG UE – User Equipment

DRT and PCTEL scanner - Scanning LTE frequency, RSRP and SNR values

GPS – Driving predefined routes

Laptop - collecting data and interface between UE, e-NB and Scanner

TEMS License

b) Software:

TEMS Investigation 11.0.4 P1J (Ascom) – Data collection

TEMS Discovery (Ascom) – Data processing and Analysis

XCAL (Accuver) – Data Collection

XCAP (Accuver) – Data processing and Analysis

Netpersec – Throughput Measurement

6.1.1.1 Scanner Settings

Check the network connection for Ethernet port which was connected to the laptop Set PC static IP address to 192.168.5.1

- Verify to ping scanner IP address: 192.168.5.2
  Ping reply messages indicate that the connection has been established successfully.

- Filtering Mode – Selects the type of filtering to be used for decoding. TopN returns up to N sets of data where N is the number entered in the TopN Value field.

- TopN Value – The maximum number of data sets that will be returned. The largest entry is 127.

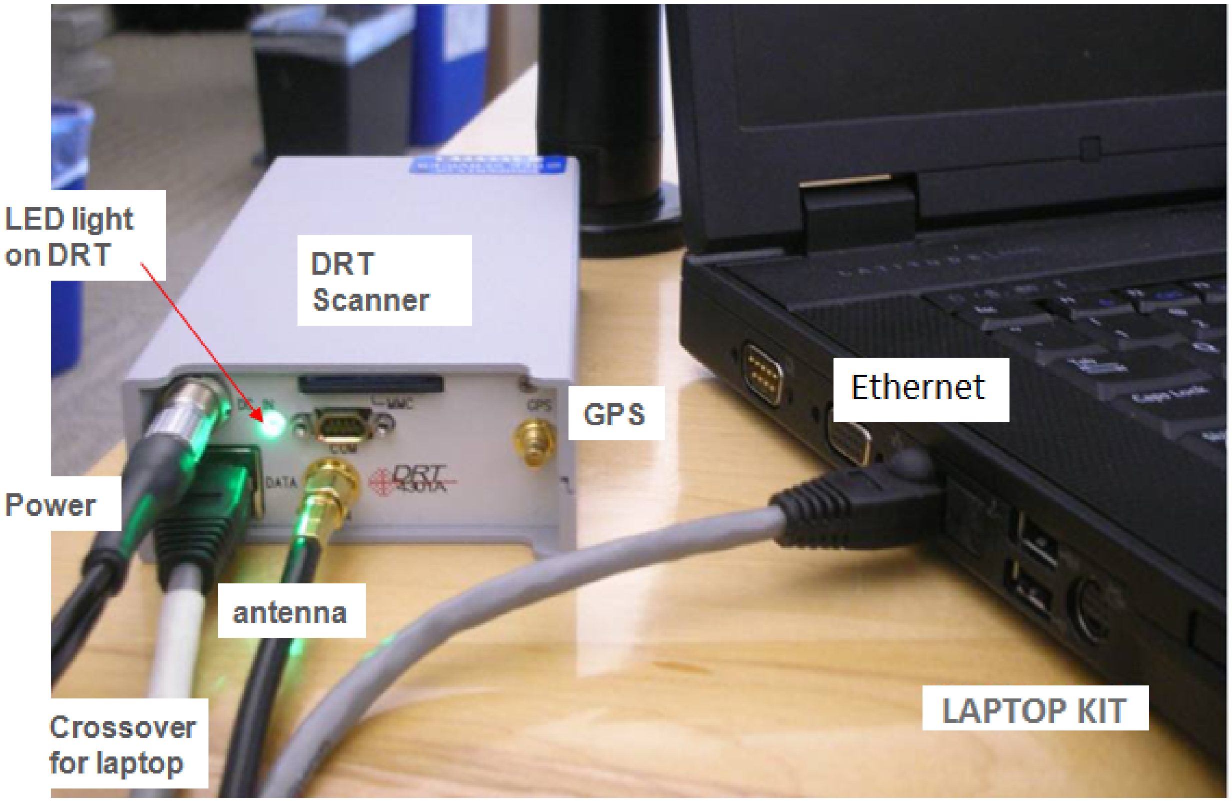


Figure 6.2 DRT Scanner Connection [Courtesy: 3S Network Inc.]

Figure 6.2 shows the connection of the scanner with the laptop kit. The LED on scanner has three colors specifying different specific states corresponding to the color. When a scanner is turned on, Red color of the scanner LED shows the power up mode of scanner followed by blue color specifying the search state of the scanner and last green color states the network frequency scanning mode of the scanner.

Antenna port as shown in Figure 6.2 scans the required LTE frequency needed for the UE and displays it in the software. The antenna is mounted on top of van for scanning signals with low interference. Scanner is connected to the laptop kit using an Ethernet port as shown in figure. The display seen in the software is shown in the figure 6.3 below. Click on the frequency displays the properties of the signal as shown in figure below.

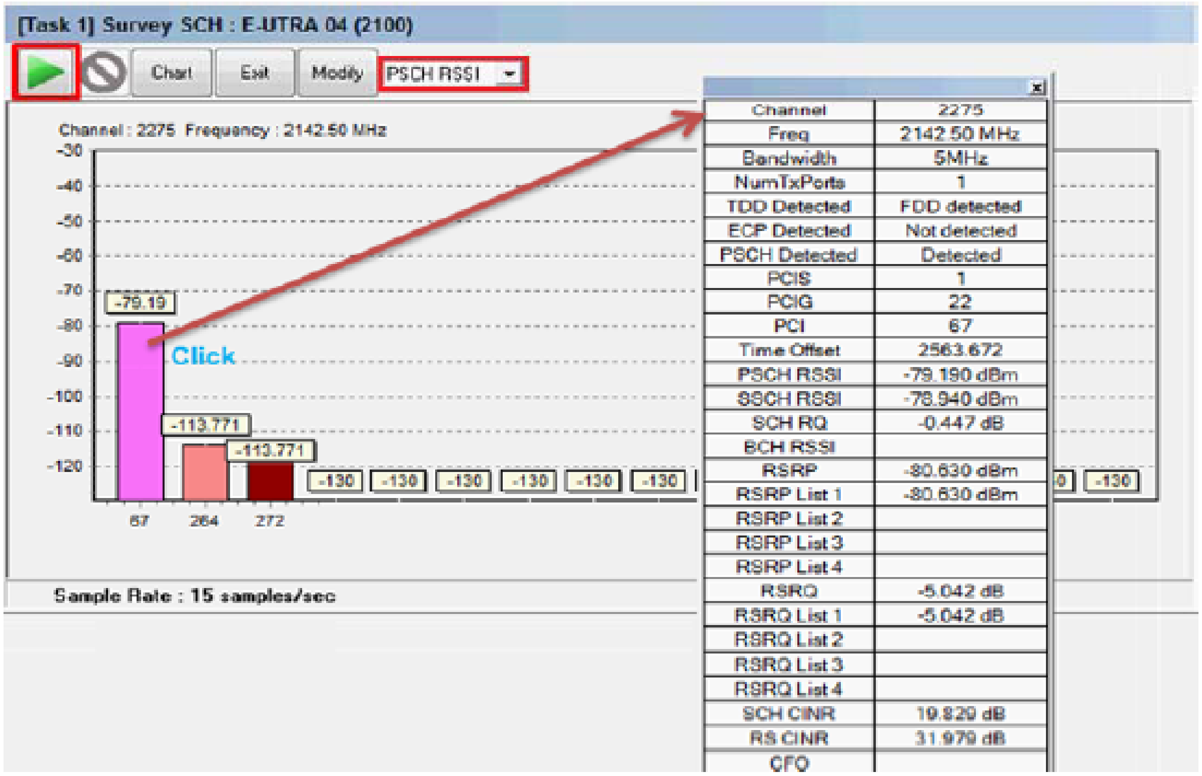


Figure 6.3 Scanned values from scanner Source: www.accuver.com

6.1.1.2 User Equipment Information

Figure 6.4 Test UE Source: www.google.com

The Figure 6.4 shows the UE that is used for test trials. These UE is a data which is used only for data calls and does not support a voice call. My tests were based on data calls and study of data calls. The LED on UE has different colors specifying different specific states of UE corresponding to the color. The specific color and the respective state of UE are shown in the Table 6.1.

During the whole test we are mainly interested in three main states of UE that are Detached, Idle and Connected mode specified by Red, Blue and Green respectively. These main states are mainly encountered during the whole test.

Table 6.1 UE LED Info Courtesy: 3S Network Inc.

<table>
<tr><th colspan="2">Device Status</th><th>Color</th></tr>
<tr><td colspan="2">No Service (Detached/Power up)</td><td>Red</td></tr>
<tr><td rowspan="3">Idle (System Acquired)</td><td>Legacy CDMA</td><td rowspan="3">Blue (blink)</td></tr>
<tr><td>eHRPD</td></tr>
<tr><td>LTE</td></tr>
<tr><td colspan="2">Internet PDN connection (Connected Mode)</td><td>Green (blink)</td></tr>
<tr><td colspan="2">PIN Locked</td><td>Yellow</td></tr>
<tr><td colspan="2">Invalid USIM card / No USIM</td><td>Yellow (blink)</td></tr>
<tr><td colspan="2">Emergency Download</td><td>MAGENTA</td></tr>
<tr><td colspan="2">CDMA S/W assert (for developer)</td><td>White</td></tr>
<tr><td colspan="2">LTE S/W assert (for developer)</td><td>Cyan</td></tr>
</table>

6.2 Drive Route and Test Sites

As shown in figure 6.5, the overall scenario consists of couple of base station sites, each of them with three sectors having different azimuths that are placed in order to cover the defined area. The distance between the sites is approximately 600 meters which corresponds to typical setup of commercial UMTS antennas. All sites are synchronized using a defined GPS-clock. The cell diameter is approximately 350 meters.

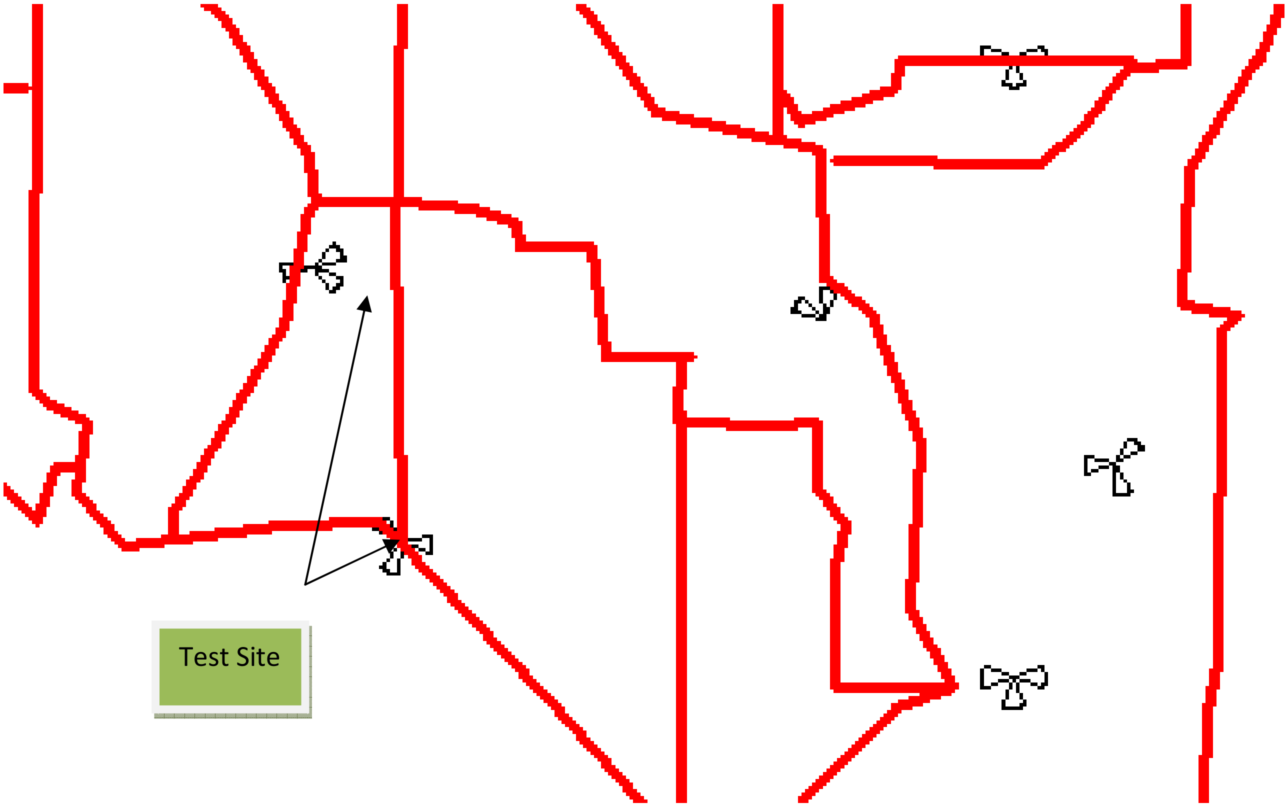


Figure 6.5 Driven Route for the test [Courtesy: 3S Network Inc.]

6.3 Analysis of Physical layer message sequence for Call Procedure

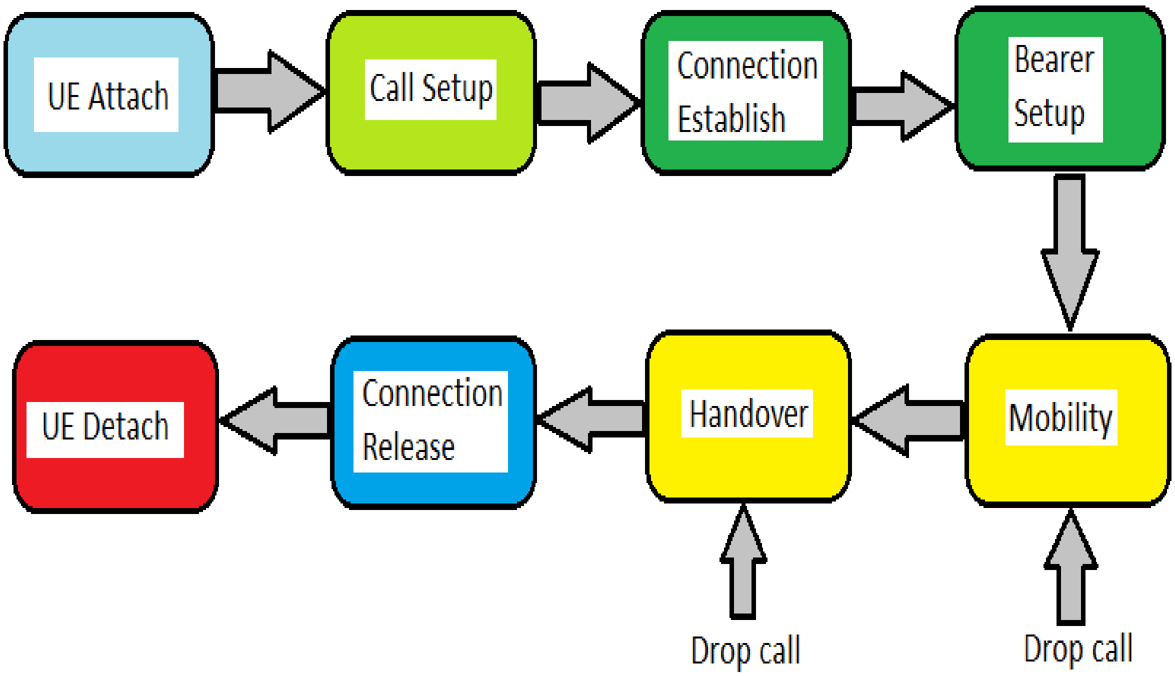


Figure 6.6 Control Plane Call Procedure

The Figure 6.6 shows the call procedure and the analysis of message sequence for each of the blocks. The experimental analysis was carried out for each of the blocks in a real call scenario near the site having LTE network. After analysing message sequence of each stage, Drop call analysis was carried out. Drop call analysis was done by studying where exactly in the area call faced a drop and hence specific reason for the drop and also the suggested solution of the same. After analyzing the whole call scenario, average throughput and peak throughputs for both UL and DL were measured and proved that LTE definitely meets the requirements for deployment and it's the fastest network till date. The study of each of the blocks mentioned here is given in the subtopics.

6.3.1 UE Attach and Call Setup

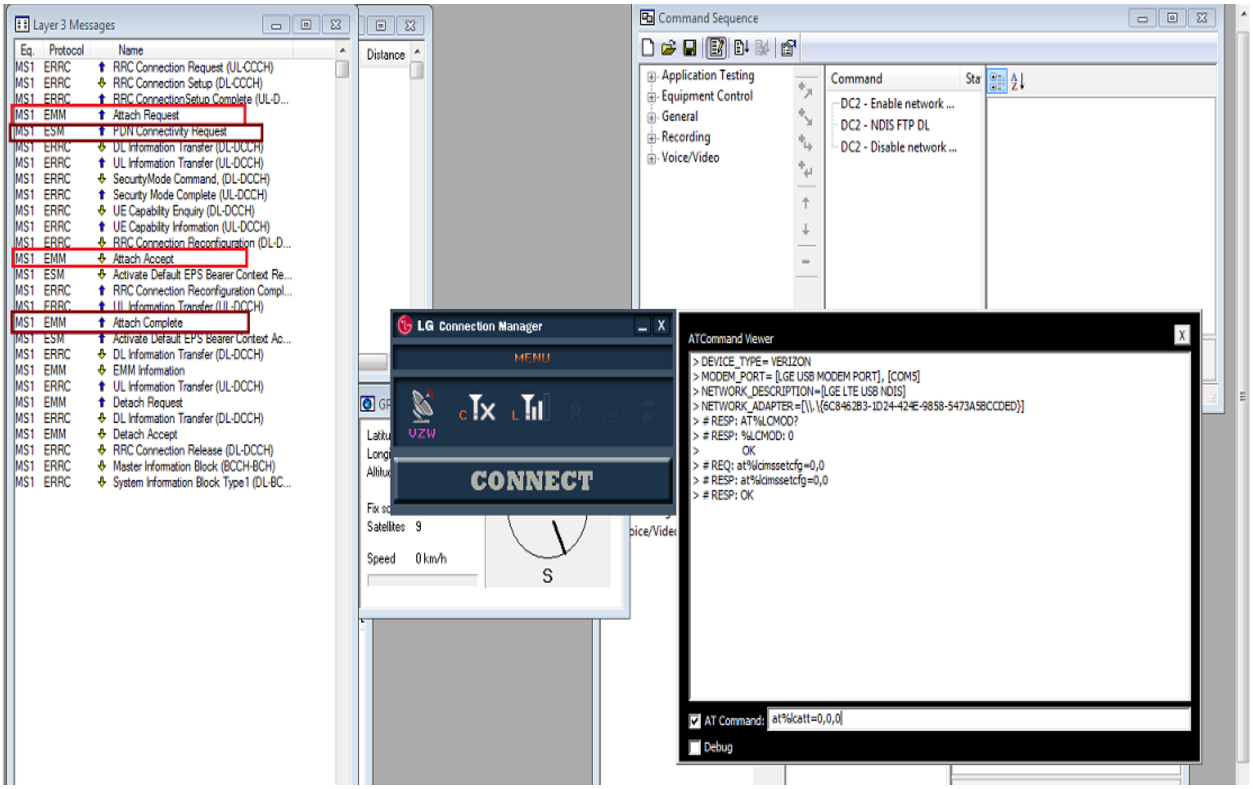


Figure 6.7 UE Attachment to Network [Courtesy: 3S Network Inc.]

In this stage, once the UE is powered on, it scans the frequency and checks which PLMN it belongs to which can be shown as the Attach process. Attach Process is a process where UE tries to connect to an eNB and hence in turn with a network. It sends an Attach Request message followed by PDN connectivity on the DL channel to connect to the end PDN-GW. Once the UE gets the authentication, it gets the back the Attach Accept message on the DL channel. During the attach process the UE is asked for an Identity and Authentication request as shown in the Figure 6.8.

During this entire process, UE sends the AT Commands to connect to the network. These commands are specific for attach and detach process or can be said as the language of UE to connect to a network. This process is preceded by cell selection process as discussed earlier in the paper. Once the UE is attached, it gets into idle mode and monitors the necessary parameters like RSRP, SNR and others and hence decides the handover decisions. If any of the messages are missing the UE will not be able to attach to the network. In case, the UE is not able to attach to the network. It will send an attach reject message with the cause shown in the respective message.

Figure 6.8 Identity and Authentication message sequence [Courtesy: 3S Network Inc.]

6.3.1.1 UE Parameter Measurement and Monitoring

For a continuous service as a user moves, UEs must not only be connected to a serving cell but also monitor their neighbor cells which is a continuous activity, since conditions of propagation to different eNodeBs change rapidly at any time as can interference levels. The UE has to meet specified minimum performance requirements that are scenario-specific such as for cell search, measurement accuracy, measurement periodicity, handover, signal quality and others. These requirements are mainly specified in 3GPP Technical Specification 36.133, 'Evolved Universal

Terrestrial Radio Access (EUTRAN); Requirements for Support of Radio Resource Management (Release 8) www.3gpp.org. The UE has to follow the below steps in order to keep continuous connectivity.

- **Serving cell quality monitoring and evaluation.** This is monitored and evaluated periodically and if the serving cell quality is satisfactory that is above the required threshold then no further action is taken. However, if the serving cell quality is below the configured threshold, the next step is taken.
- **Initiate periodic cell search activity for candidate neighbor cells.** Monitored neighbor cells can be any of intra-frequency, inter-frequency and inter-RAT cells and the search is performed in a defined order of priority. Cell search needs to be periodic as new cells may appear and disappear at any time. Hence, even if a UE has identified a neighbor cell successfully it will continue performing cell search activity until the serving cell quality becomes satisfactory again or the UE moves to another serving cell through handover, cell reselection or a cell change order. If some neighbor cells are identified successfully, the following step is taken.
- **Neighbor cell measurement.** In this step the signal strength for the neighbor cells identified in the previous step is measured periodically (since the signal strength and quality may vary). To avoid the effect of short-term fluctuations due to fast fading in the radio channel, any measurements for mobility is averaged over a number of evenly spaced measurement samples. The measurement period is specified already example, intra-frequency LTE Reference Signal Received Power (RSRP) measurements have a period of 200ms and the next step is performed whenever measurements are available.
- **Mobility evaluation.** Decision regarding whether or not a UE should move to another serving cell is made here. Mobility evaluation is done within a network entity i.e. eNodeB decides on handover or within the UE in case of cell reselection. If the criteria to trigger UE mobility are fulfilled then a mobility procedure to move towards a better cell is executed.

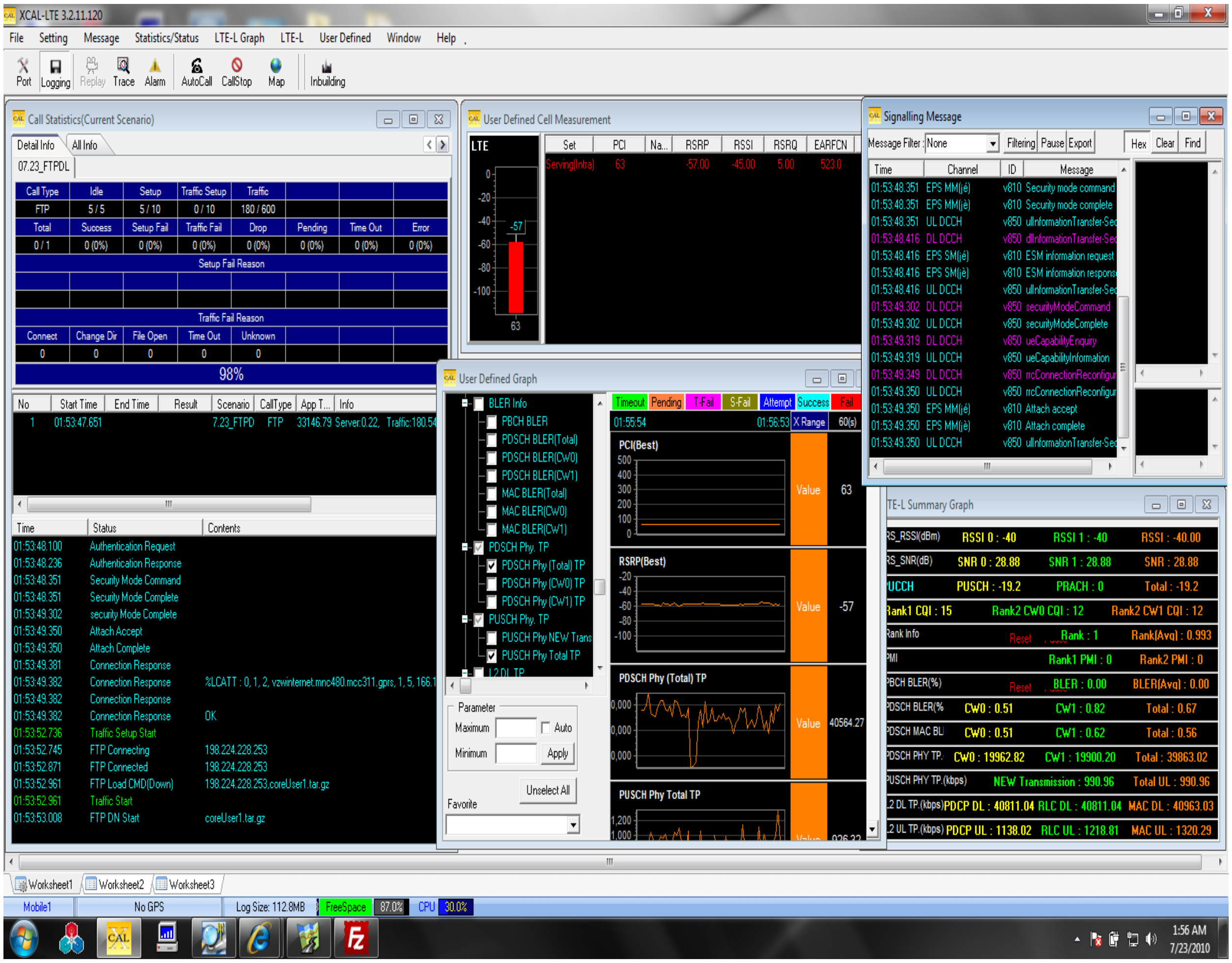


Figure 6.9 Parameter Monitoring of UE [Courtesy: 3S Network Inc.]

The above Figure 6.9 shows the monitoring of different parameters by UE as discussed above. As shown in figure 6.10, the call parameters are setup before making a test call. During the whole test to avoid user interruption, 20 test calls were made automatic and continuous with the idle time of 5 seconds between the call. Traffic time was kept as 1000 seconds so if there arose any traffic for more than 1000 seconds, the call gets disconnected. The total time kept for the establishment of a call was kept as 100 seconds and if the call was unable to establish due to reason like network attach failure then the UE gets detached from the network.

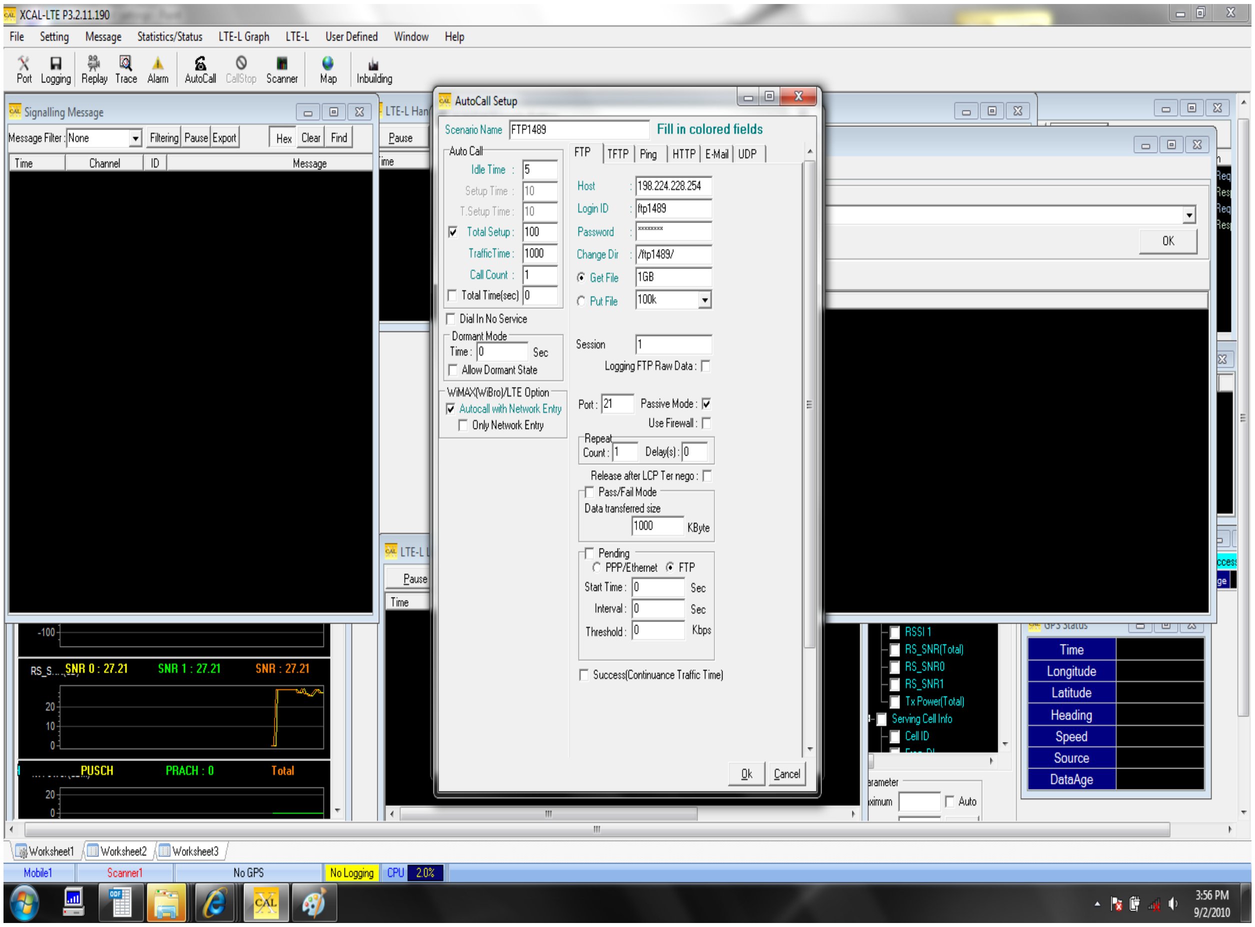


Figure 6.10 Test Call Setup Parameters [Courtesy: 3S Network Inc.]

6.3.2 Bearer Establishment

Connection Establishment and Bearer Establishment process is executed very close to each other and hence goes hand in hand. When a call is made, connection is established and hence a Bearer is establishment for a particular service to execute.

EPS uses the concept of EPS bearer to route IP traffic from a gateway in the PDN to the UE. A bearer is an IP packet flow with a defined Quality of Service (QoS) between the gateway and the UE. The EUTRAN and EPC together set up and release bearers as required by applications. EPS bearer is an end-to-end connection between UE and P-GW. P-GW is the gateway to the outside network and it forwards messages to IP networks, Internet or private networks. When IP packets come into gateway, it's going to forward it all the way to UE.

There are two main types of bearers:

1) Default Bearer

This bearer is the first bearer to be setup per APN network and an IP address is assigned to the UE by the P-GW and at least one bearer is established called default bearer that remains established throughout the cycle of PDN connection in order to provide the UE with always-on IP connectivity to that PDN. The default bearer always has to be a non-GBR bearer since it is permanently established. That means Non-GBR bearers do not guarantee any particular bit rate. These can be used for applications like web-browsing or FTP transfer and hence for these bearers no bandwidth resources are allocated permanently to the bearer. Depending on the subscription data retrieved from the HSS, the MME assigns the QoS profile associate with it. As this bearer provides end-to-end connectivity between UE and P-GW for connecting to a specific network, there could exists Multiple Default bearers one per APN. For example: for IMS signaling.

2) Dedicated Bearer

At anytime during or after completion of the attach procedure, additional bearers called dedicated bearers can also be established. A dedicated bearer can be either a GBR or a non-GBR bearer. These dedicated bearers could be established by the network, or they could be requested by the UE. This dedicated bearer will have new QoS profile for different application. For example: for VoIP or Video application. This bearer is established depending on the need for particular application.

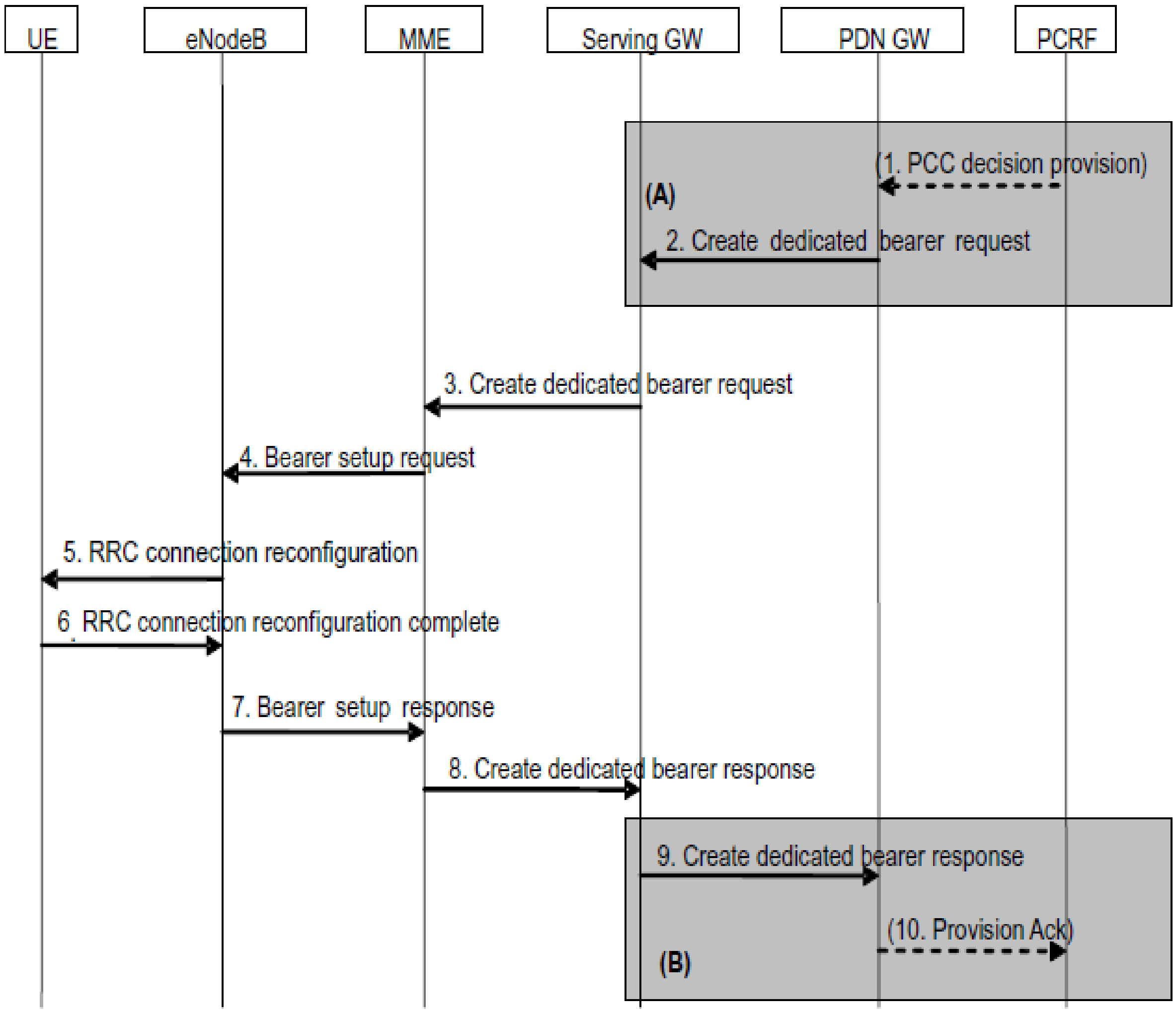


Figure 6.11 Example of message flow for a LTE/SAE bearer establishment. Reproduced by permissoin from copyright 3GPP specifications [30]

In the procedure of end-to-end bearer establishment, when a bearer is established, the bearers across each of the interfaces are established.

- The PCRF sends a 'PCC (Policy Control and Charging) Decision Provision' message indicating the required QoS for the bearer to the P-GW that uses QoS policy to assign the bearer-level QoS parameters.
- The P-GW then sends a 'Create Dedicated Bearer Request' message including the QoS and UL TFT to be used in the UE to the S-GW.

- The S-GW forwards the Create Dedicated Bearer Request message (including bearer QoS, UL TFT and S1-bearer ID) to the MME. (message 3)
- A set of session management configuration information including the UL TFT and the EPS bearer identity is build by the MME which includes it in the 'Bearer Setup Request' message which it sends to the e-NB (message 4)
- The session management configuration being the NAS information is therefore sent transparently by the e-NB to the UE.
- The Bearer Setup Request provides the QoS of the bearer to the e-NB, this information is used by the e-NB for call admission control and also to ensure the necessary QoS. The e-NB then maps the EPS bearer QoS to the radio bearer QoS.
- Then 'RRC Connection Reconfiguration' message (including the radio bearer QoS, session management configuration and EPS radio bearer identity) is sent to the UE to set up the radio bearer (message 5). The RRC Connection Reconfiguration message contains all the configuration parameters for the radio interface. This is mainly for the configuration of the Layer 2 (RLC, MAC and PDCP parameters) and also the Layer 1 initialization parameters.
- Messages 6 to 10 are the corresponding response messages to confirm that the bearers have been set up correctly.

This message sequence was analyzed and studied in the test trials and the Figure 6.12 shows the message sequence performed on the real time scenario. Followed by the Figure 6.13(a) and Figure 6.12 (b), shows the details of messages RRC Connection Reconfiguration and RRC Connection Reconfiguration Completse, respectively.

Figure 6.12 shows that the RRC Connection Reconfiguration received on DL logical channel DL-DCCH. This message includes the UE unique identity assigned to it, also the target Cell-Id and other power parameter information that is needed by the UE in order to establish a connection. In response to RRC Connection Reconfiguration message, the UE responds with the message RRC Connection Reconfiguration Complete that is sent on the UL-DCCH uplink logical Channel.

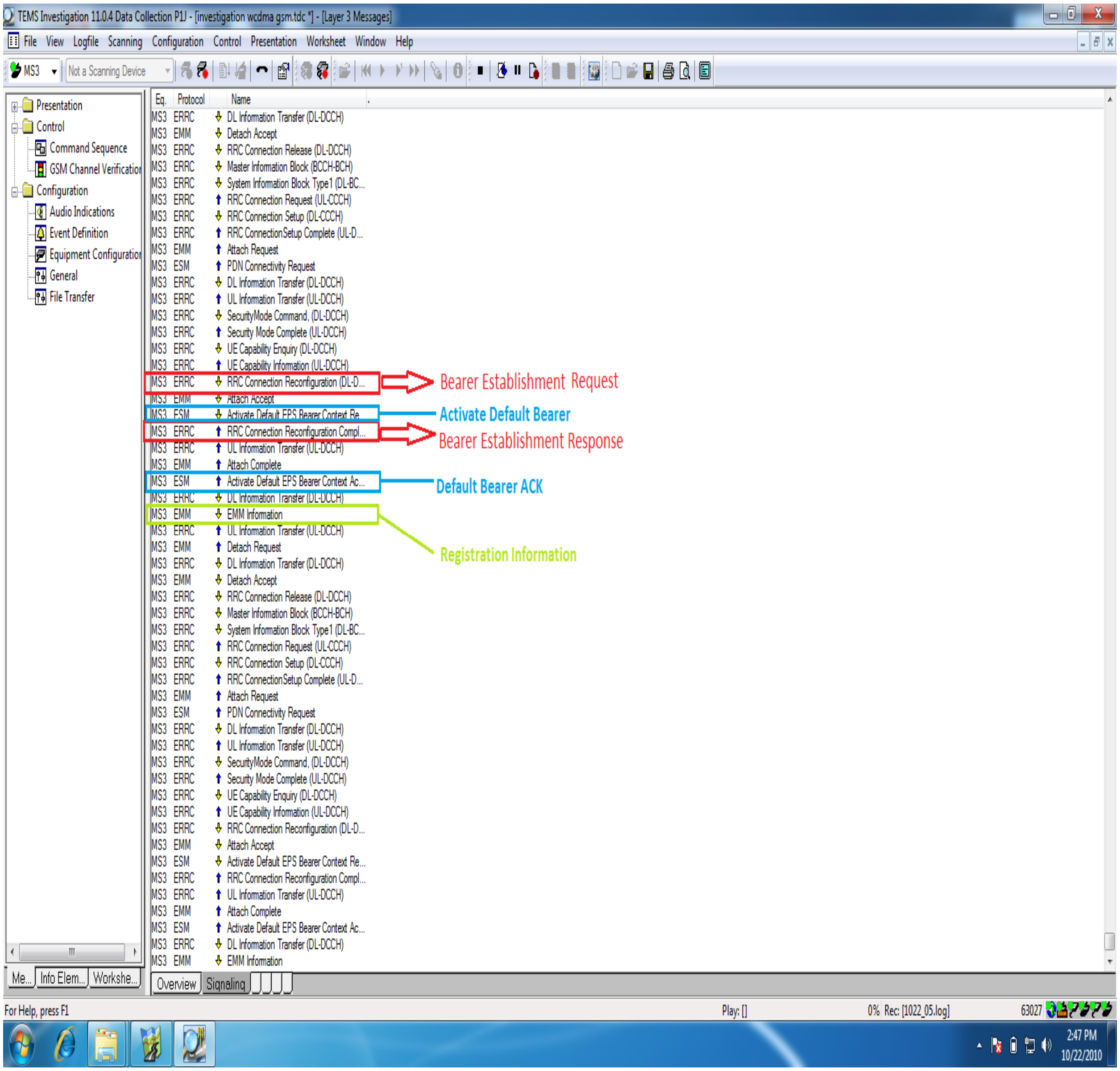
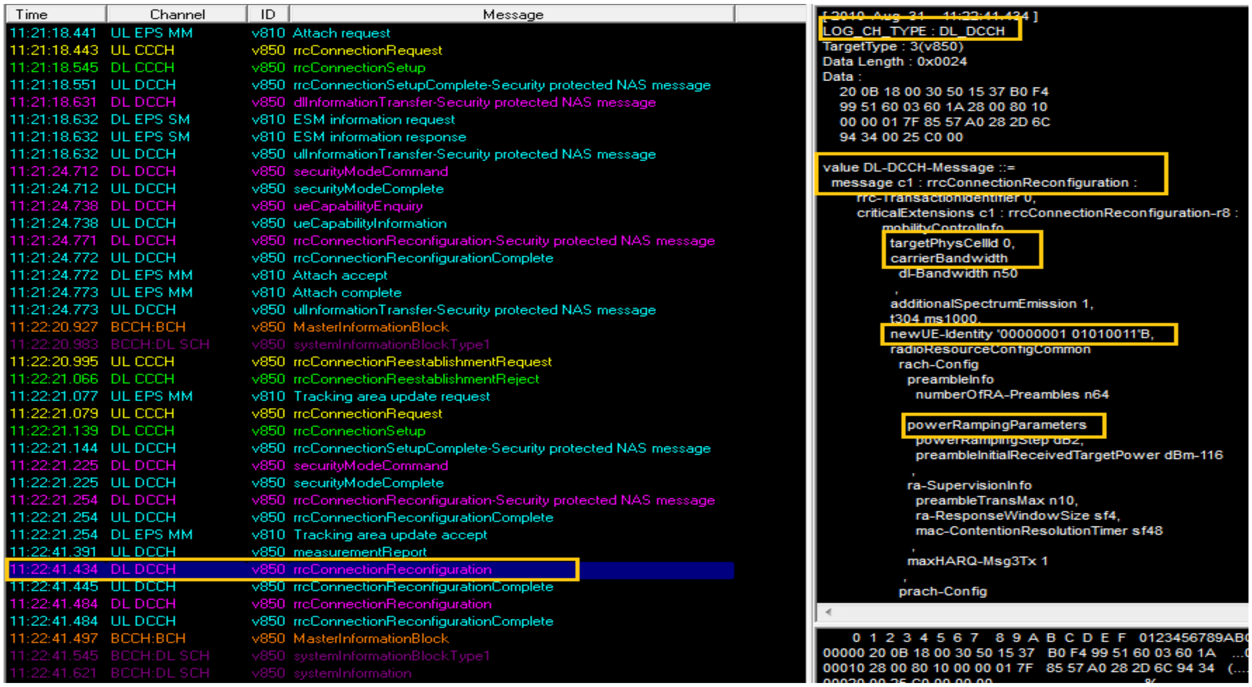
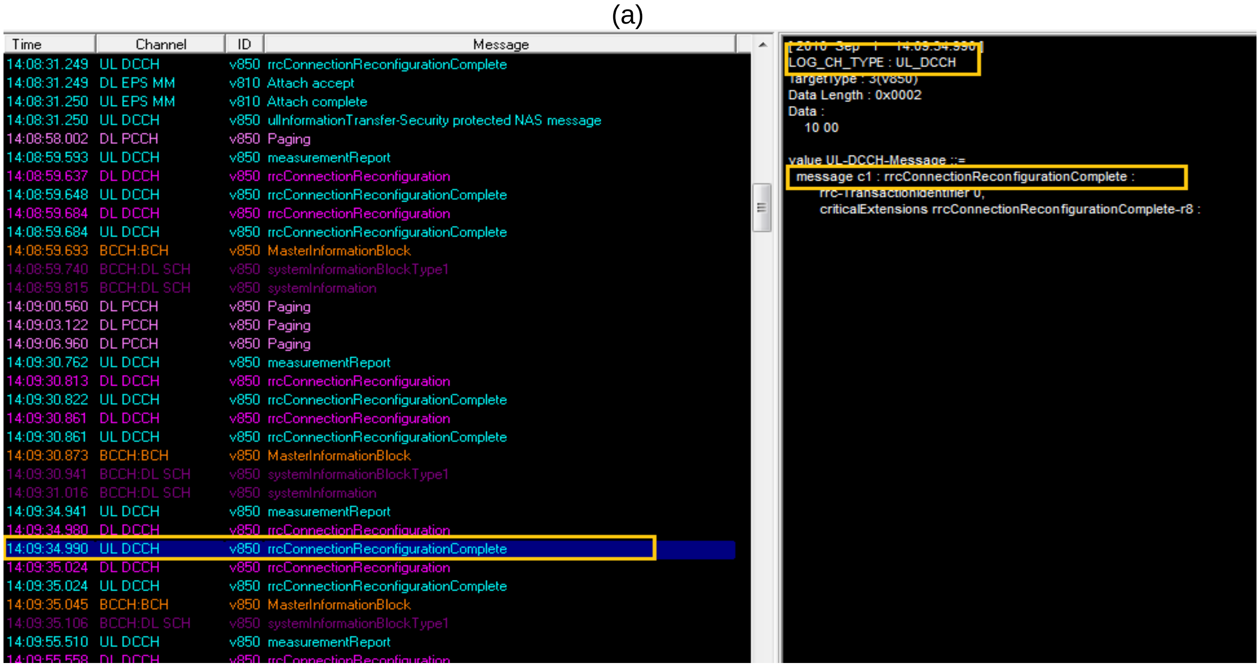


Figure 6.12 Test Analysis of Bearer Establishment Message [Courtesy: 3S Network Inc.]



(a)



(b)

Figure 6.13 (a) Test Analysis of RRC Connection Reconfiguration Message, (b) Test Analysis of RRC Connection Reconfiguration Complete Message

6.3.3 Connection Establishment

Two mechanisms of NAS states explain the state of a UE with respect to connection establishment:

- EPS Mobility Management (EMM) state (EMM-REGISTERED OR DEREGISTERED). This gives the information whether or not a UE is registered in MME
- EPS Connection Management (ECM) state (ECM-IDLE or ECM-CONNECTION). This gives the information status of the connectivity of the UE with the Evolved Packet Core

<table>
<tr><th></th><th>1: Off</th><th>Attaching</th><th>2: Idle / Registered</th><th>Connecting to EPC</th><th>3: Active</th></tr>
<tr><td>EMM</td><td colspan="2">DEREGISTERED</td><td colspan="3">REGISTERED</td></tr>
<tr><td>ECM</td><td colspan="4">IDLE</td><td>CONNECTED</td></tr>
<tr><td>RRC</td><td>IDLE</td><td>CONNECTED</td><td>IDLE</td><td colspan="2">CONNECTED</td></tr>
</table>

Figure 6.14 Possible combinations of NAS and AS states [30]

When a UE undergoes transition of states from ECM-IDLE to ECM-CONNECTED, it involves establishment of the RRC connection and establishment of S1-connection. RRC connection establishment is initiated by NAS and completed prior to S1-connection establishment. UEs move to ECM-CONNECTED when they become active. This LTE transition from ECM-IDLE TO ECM-CONNECTED takes place within 100ms. RRC connection release is initiated by the e-NB which is followed by the release of the S1 connection between the e-NB and the Core Network.

6.3.3.1 Connection establishment message sequence

RRC connection establishment procedure involves the establishment of SRB1 and the transfer of the initial uplink NAS message which triggers the establishment of the S1 connection that follows the establishment of SRB2 and one or more DRBs.

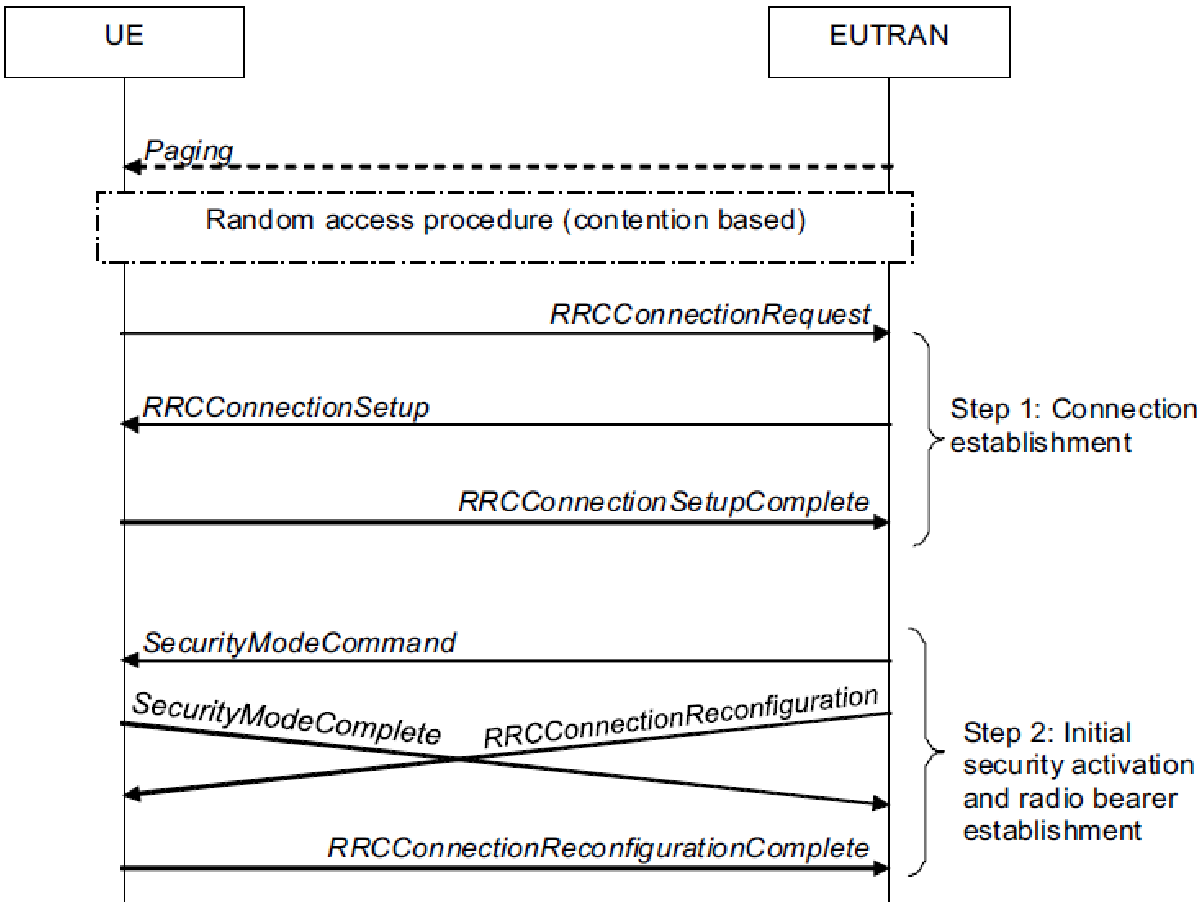


Figure 6.15 RRC Connection Establishment Message sequence [30]

STEP 1: Connection Establishment

- Upper layers in the UE trigger connection establishment in response to paging. The UE checks if the access is blocked and if not then the lower layers in the UE perform a contention-based random access procedure and the UE starts a timer known to be as T300 and sends the RRCConnectionRequest message that includes an initial identity (S-TMSI or a random number) and an establishment cause.
- If the connection is accepted by EUTRAN, it returns the RRCConnectionSetup message that includes the initial radio resource configuration including SRB1.

- The UE in return sends the RRCConnectionSetupComplete message and includes the NAS message, an identifier of the selected PLMN used to support network sharing and an identifies of the registered MME that is provided by upper layers. Based on identifier of both selected PLMN and registered MME, the e-NB decides on the CN node to which it should establish the S1-connection further.

STEP 2: Initial security activation and radio bearer establishment

- To activate integrity protection and ciphering, the EUTRAN sends the SecurityModeCommand message. This message indicates which algorithms shall be used as it is integrity-protected but not ciphered.
- The UE verifies the integrity protection of the SecurityModeControl message and on verification success, it configures lower layers to apply integrity protection and ciphering to all subsequent messages. Ciphering is not applied to the response message i.e. the SecurityModeComplete or SecurityModeFailure message.
- EUTRAN then sends the RRCConnectionReconfiguration message including a radio resource configuration used to establish SRB2 and one or more DRBs. This message may be sent prior to receiving the SecurityModeComplete message in which case the release of the connection is needed by EUTRAN in which case the two procedures result from a single S1-procedure does not support partial success.
- The UE finally responds the RRCConnectionReconfigurationComplete message.

The message flow during the Connection Establishment process is analyzed and studied in the test trials and the message flow in actual scenario is shown in the figure 6.16. There is minute delay in the messages sent and received and hence the sequence order of the messages is not displayed in sequence.

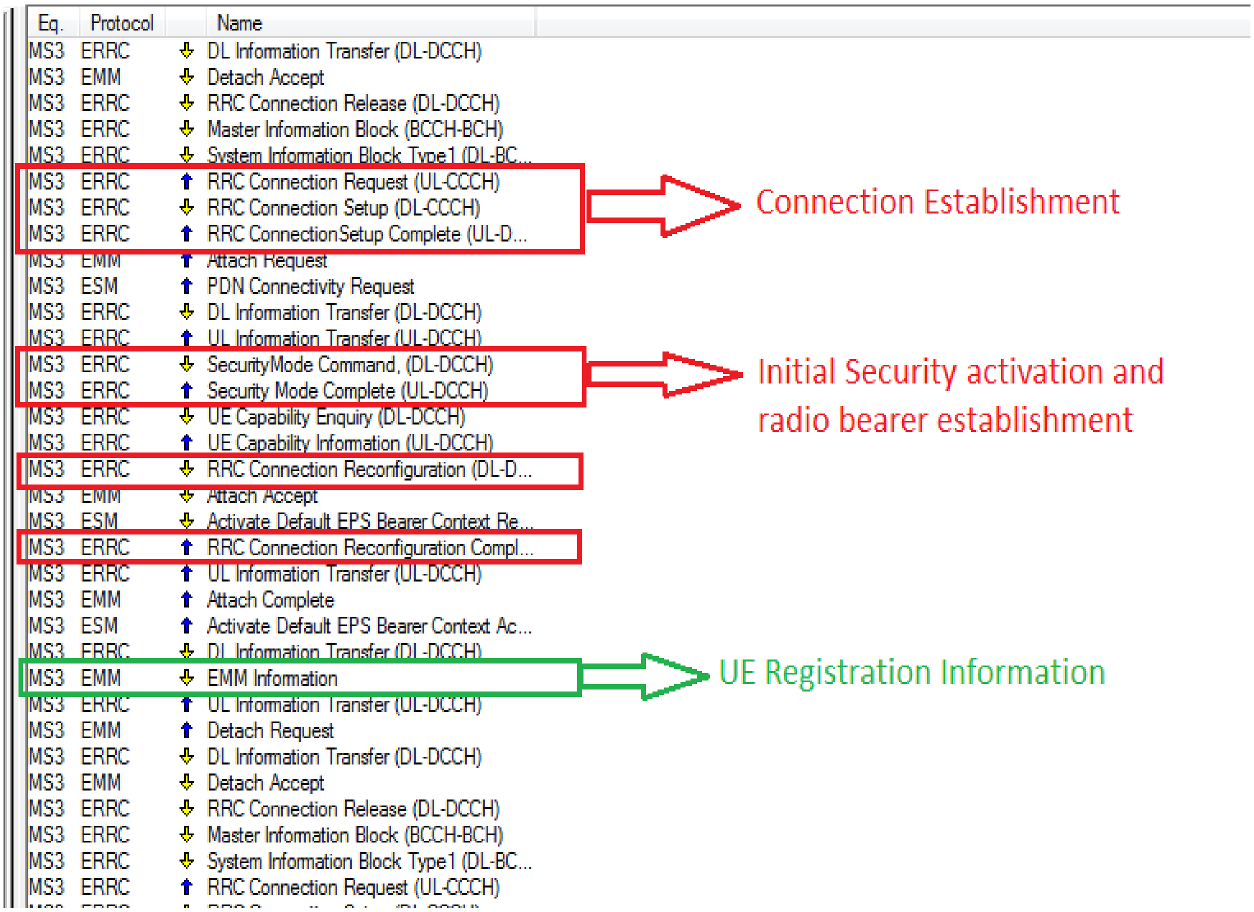


Figure 6.16 Test Analysis of RRC Connection Establishment Message Sequence
[Courtesy: 3S Network Inc.]

A connection establishment may fail due to many reasons as described below:

- Access to the network may be blocked
- EUTRAN may temporarily reject the connection establishment by including a wait timer, in which case the UE rejects any connection establishment request till the wait is ongoing and not elapsed.
- The UE aborts the connection establishment procedure and informs upper layers of the failure to establish the connection in case cell re-selection occurs during connection establishment.
- The NAS may abort an ongoing RRC connection establishment, for example is upon NAS timer expiry.

6.3.4 Mobility within LTE

The Control Plane of the Access Stratum (AS) handles radio-specific functionality depending on the Radio Resource Control (RRC) states of the UE. This state of UE can also be designated as Mobility Management States that depends on the source and target cells and mobility state of the UE.

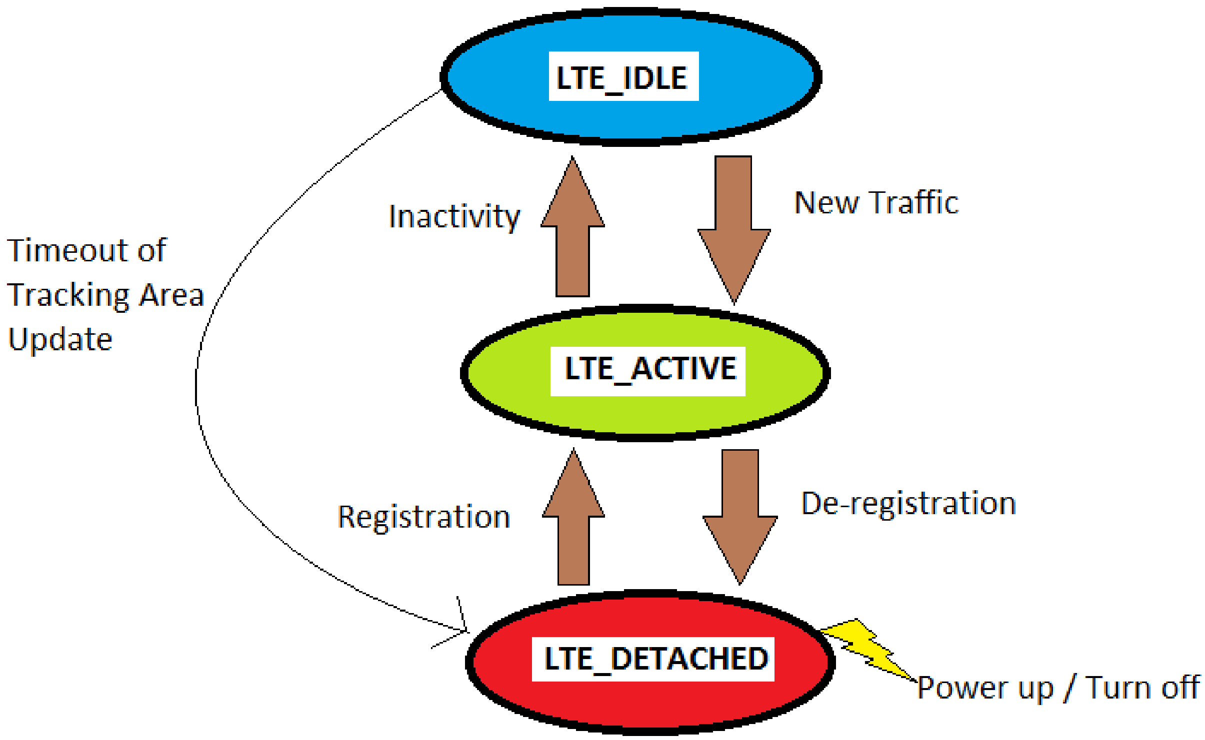


Figure 6.17 Mobility states of the UE in LTE. Reproduced from [24]

6.3.4.1 Idle State Mobility

In this RRC_IDLE mode the UE performs cell selection and reselection by monitoring a paging channel to detect incoming calls and acquires system information consisting of parameters by which the EUTRAN can control the cell selection-reselection process. In this mode, the UE does not inform the network of the cell change and is in a power-conservation mode type. The location of the UE is known by the Tracking Area (TA). During the time of UE-terminated call, the UE is paged in its last reported TA. It has been agreed in 3GPP that TAs for LTE and other RATS i.e. an e-NB and a UMTS Node-B will belong to separate TAs for network handling simplification of mobility of the UE crossing 3GPP RAT boundaries.

UE being capable of transmitting/receiving in multiple RATs, when moves across different RAT technologies in idle mode, the objective will be to keep the UE camped in idle state of different technologies i.e. LTE_IDLE in LTE and PMM-IDLE in UMTS/GPRS. Here UE is not supposed to perform Tracking Area (TA) updates in LTE or Routing Area (RA) updates in UTRAN/GERAN when UE moves between these technologies. For this reason, the UE is assigned to both TA and RA and as long as UE is moving among the cells broadcasting one of these TA or RA update, the UE does not send TA or RA update in idle mode. Whenever a new traffic arrives for the UE, the UE immediately is paged in both the technologies and data is forwarded through the particular RAT in which the UE responds.

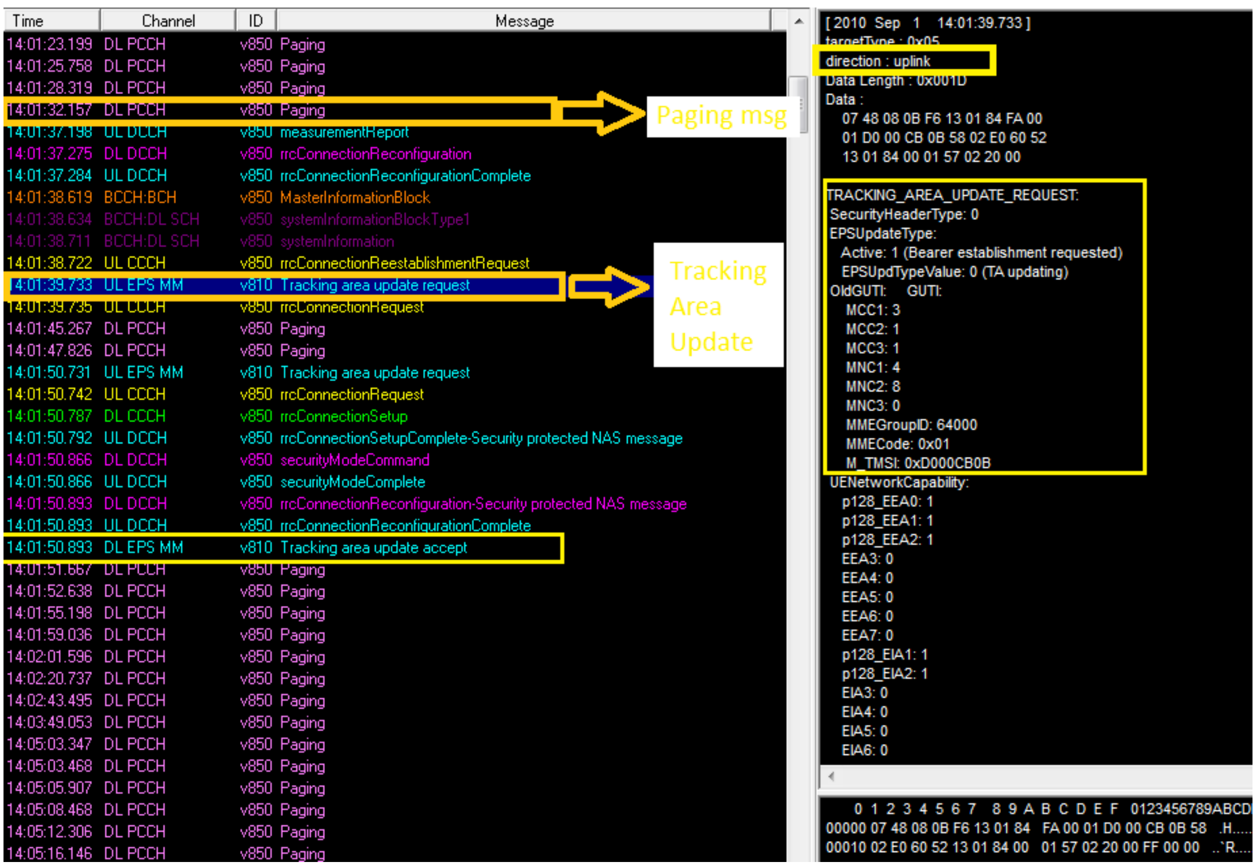


Figure 6.18 Test Analysis of Tracking Area Update Message for Idle Mode Mobility
[Courtesy: 3S Network Inc.]

LTE has two mechanisms for indicating system information change.

1. A paging message including a flag indicating whether or not the system information has changed.
2. A value tag in SIB1 which is incremented every time one or more SI messages change.

UEs in RRC_IDLE mode use the first mechanism and UEs in RRC_CONNECTED mode can use any of the above mentioned mechanism particularly when a UE is unable to receive the paging messages.

UEs in RRC_IDLE needs no additional wake-ups to detect changes of system information as they are only required to receive paging message at their normal paging periods or occasions. To ensure reliability of reception, the notification change paging message is repeated a number of times during the BCCH modification period preceding that in which the new system information is first transmitted.

UEs in RRC_CONNECTED receive paging message the same number of times per modification period as UEs in RRC_IDLE using the default paging cycle. The notification of change of system information is infrequent, that is once every few hours, and overheads for the messages could be considered negligible. Whenever a UE received a notification of a system information change, it then considers all the system information to be invalid from the start of the next modification period. Hence, the UE operations may be restricted until the UE has re-acquired the most essential information specifically in RRC_CONNECTED. And hence the information change is assumed to be infrequent. If the UE re-enters a cell, it considers the SI previously acquired from the cell to remain valid if it was received previously within the 3 hours.

6.3.4.2 Connected State Mobility

In RRC_CONNECTED, the EUTRAN decides to which cell a UE should handover in order to maintain the radio link connection. In RRC_CONNECTED, the EUTRAN in order to facilitate the transfer of data via a shared data channel, it assigns substantial radio resources to the UE. The UE monitors an associated control channel and provides the network with measurement reports of downlink channel quality, its buffer status and also neighboring cell measurement information to allow EUTRAN to select the most suitable cell for the UE to camp on. This report contains information of cells using other frequencies. The UE receives System Information report mainly including information required to use the transmission channels. In LTE technology, the UE always connects to a single cell only, hence the connection of UE from a source cell to a target cell is a 'hard handover'.

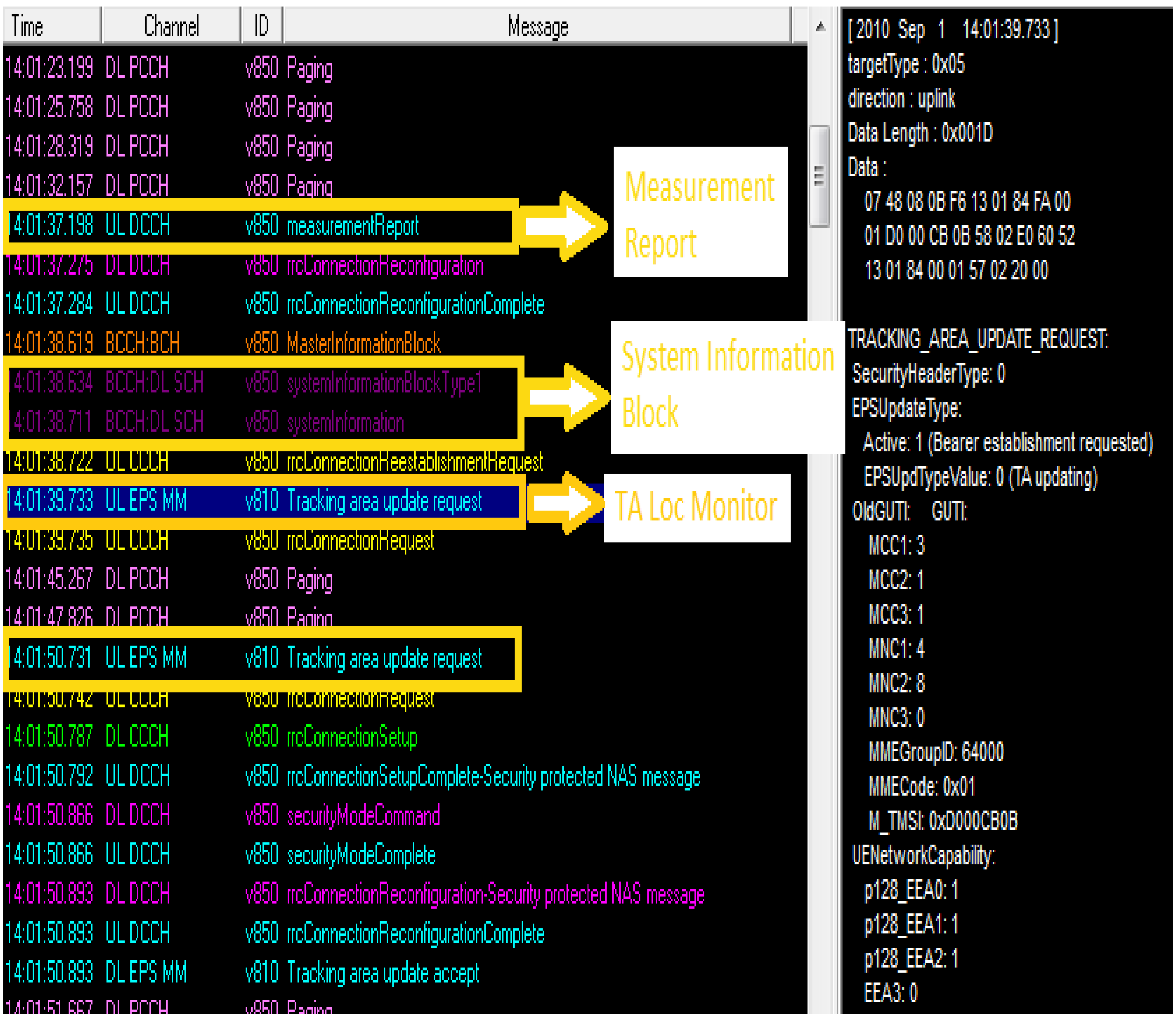


Figure 6.19 Test Analysis of Message Sequence for Connected Mode Mobility
[Courtesy: 3S Network Inc.]

Figure 6.19 and Figure 6.20 is the test analysis of message sequence for connected mode mobility. Mainly measurement report, SIB and TA update message are involved in the connected mode mobility process. In this MeasurementReport message, the UE includes measurement results related to a single measurement. If multiple cells triggered the report, the UE includes the cells in a decreasing value of reporting quantity that is the best cell is reported first. A parameter ‘maxReportCells’ in MeasurementReport message includes the information regarding the number of cells.

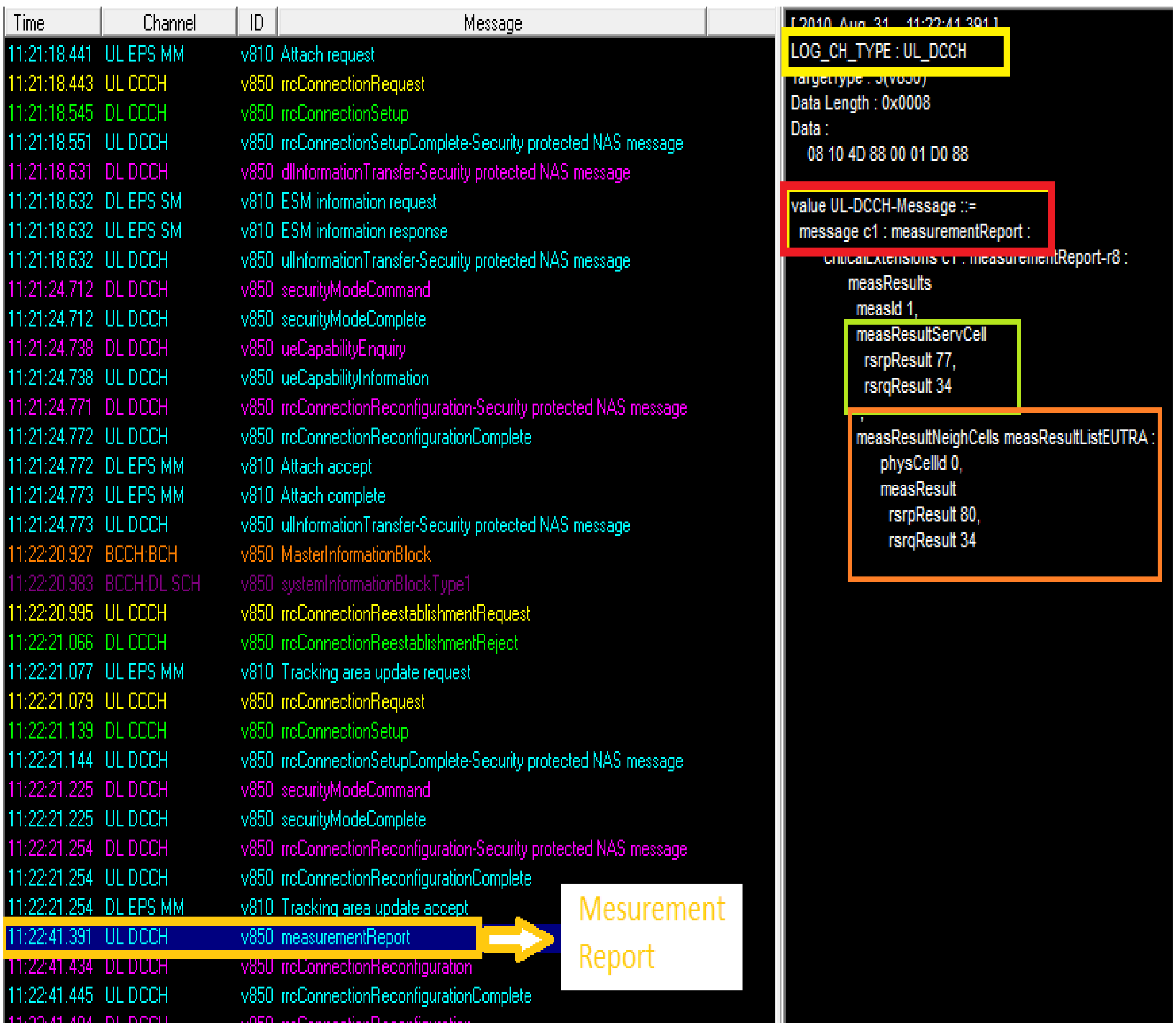


Figure 6.20 Test Analysis of Measurement Report message sequence for Connected Mode Mobility [Courtesy: 3S Network Inc.]

6.3.4.3 Measurement Configuration

To support the control of the UE mobility, The EUTRAN can configure UE to report measurement information. The following measurement configurations can be reported via the RRCConnectonRecongifuration message.

- Measurement object parameter: This defines on what the UE should perform the measurements such as a carrier frequency. It may even include a list of cells to be considered as well as parameters such as frequency or cell specific offsets.
- Reporting configuration parameter: This reporting configuration consists of the criteria which cause the UE to send a measurement report and the information the UE is suppose to report such as Received Signal Code Power (RSCP) for UMTS or Reference Signal Received Power (RSRP) for LTE.
- Measurement Identities. These identify and define the applicable measurement object and reporting configuration.
- Quantity parameters. The quantity configuration parameter defines the filtering to be used on each measurement.
- Measurement gaps. They define time periods when no uplink or downlink transmissions will be scheduled so that the UE may perform the measurements.

6.3.4.4 System Information

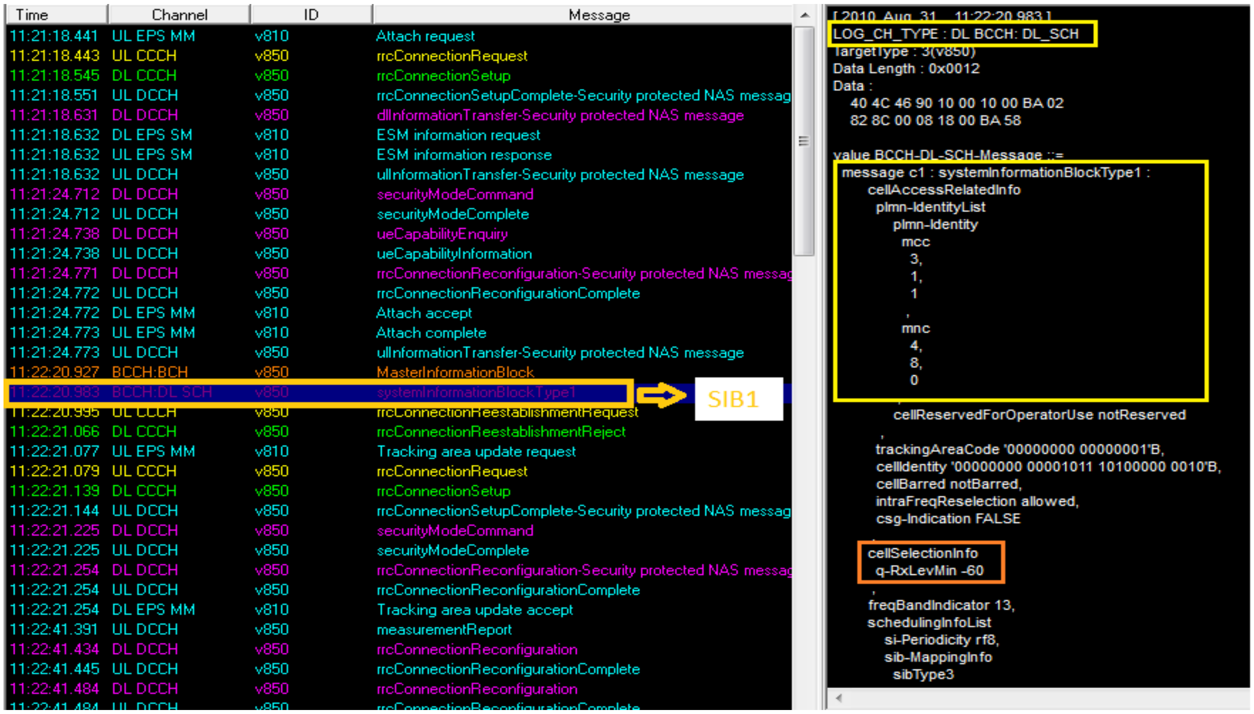
System information is established by means of System Information Blocks (SIBs), which contains different necessary parameters. Three types of RRC message are used to transfer system information. These messages are described below.

- **Master Information Block (MIB).** This message contains a limited number of most frequently transmitted parameters which are important for a UE to get initial access to the network.

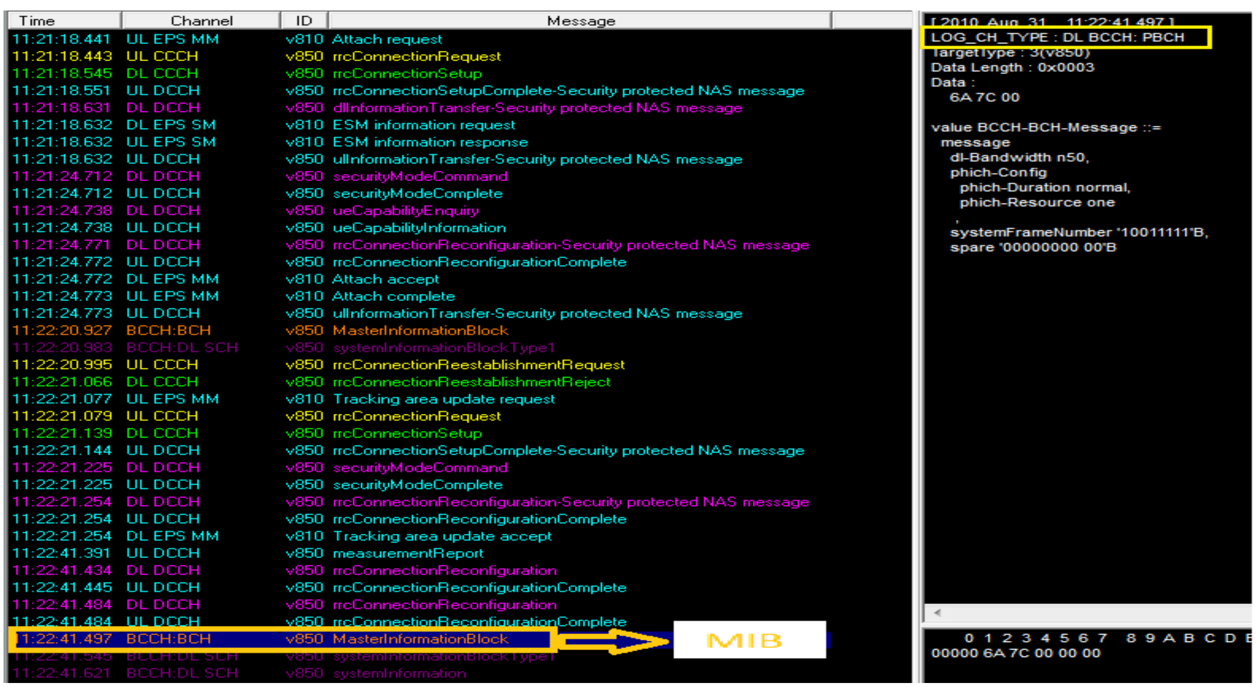
- **System Information Block Type 1 (SIB1).**This message contains parameters that are essential to determine if a cell is suitable for cell selection-reselection and about the time domain scheduling of the other SIBs.
- **System Information Block Type 2 (SIB2).**This message includes shared and common channel information.
- **SIB3 – SIB8.** This message contains parameters used to control intra-frequency, inter-frequency and inter-RAT cell reselection.

Table 6.2 System Information Block Message Details [30]

Message	**Content**	**Period (ms)**	**Applicability**
MIB	Most Essential parameters	40	Idle and Connected
SIB1	Cell access related parameters, scheduling information	80	Idle and Connected
1st SI	SIB2: Common and shared channel configuration	160	Idle and Connected
2nd SI	SIB3: Common cell reselection information and intra-frequency cell reselection parameters other than the neighboring cell information SIB4: Intra-frequency cell reselection information	320	Idle only
3rd SI	SIB5: Inter-frequency cell reselection information	640	Idle only
4th SI	SIB6: UTRA cell reselection information SIB7: GERAN cell reselection information	640	Idle only, depends on UE support of UMTS or GERAN



(a)



(b)

Figure 6.21 (a) Test Analysis of System Information Block Message (b) Test Analysis of Master Information Block (MIB) message, [Courtesy: 3S Network Inc.]

Figure 6.21 (a) and Figure 6.21 (b) shows the analysis details that are present in SIB1 and MIB messages. As seen in the figure theses SIB1 and MIB are received on logical channel DL-BCCH, type DL-SCH and PBCH channels respectively.

6.3.5 Handovers in LTE

In LTE_ACTIVE mode handover taking place when a UE moves between two LTE cells, the source cell, based on measurement reports from the UE, determines the target cell and queries it for the available resources to accommodate the UE. Handover in LTE are 'hard handovers, that means at the time of handover there is a short interruption in service even during both the intra-e-NB and inter-e-NB handovers.

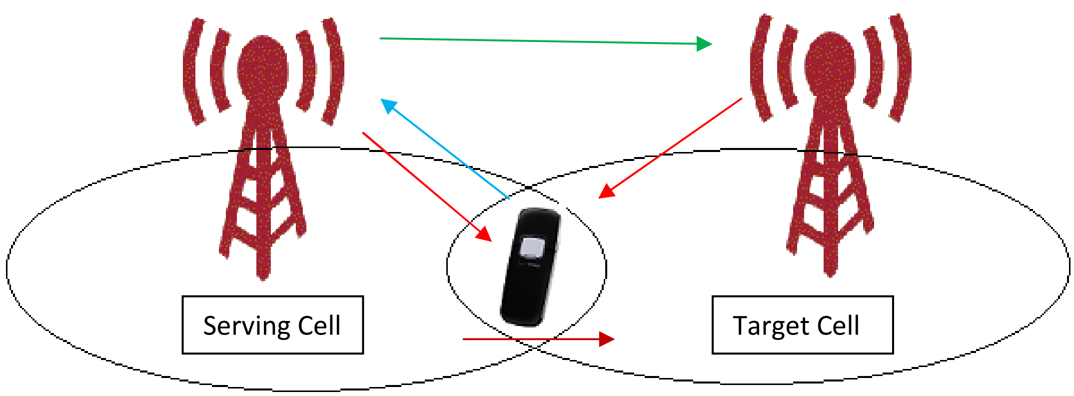


Figure 6.22 Red – DL handover measurements, Brown – Processing of DL measurements, Blue – UL reporting, Green – handover decision & execution. Reproduced from [16]

In RRC_CONNECTED, the EUTRAN controls mobility by ordering the UE to perform handover to another cell, which may be on the same frequency ('intra-frequency') or a different frequency ('inter-frequency'). The EUTRAN may use the handover procedures for purposes such as change of security keys to a new set or to perform a ‘synchronized reconfiguration’ in which the EUTRAN and the UE together apply the new configurations.

The handover procedure message sequence is described below:

1. The UE sends the MeasurementReport message.
2. Before sending the handover command to the UE, the source e-NB requests one or more target ccells to prepare for the handover. During this ‘handover preparation request’, the source e-NB provides UE RRC context information about the UE capabilities, UE-specific Radio Resource Management (RRM) information and the current AS- configuration. In this response, the e-NB controlling the target cell generates the ‘handover command’. The source e-NB forwards this to the UE in the RRCConnectionReconfiguration message.
3. The source e-NB sends the RRCConnectionReconfiguration message to the UE to inform UE to perform handover and this includes mobility control information (that is identity and frequency of the target cell) and the radio resource configuration information which is common to all the UEs in the target cell. This also includes dedicated radio resource configuration, the security configuration and The Cell Radio Network Temporary Identifies (C-RNTI) used by a given UE while it is in a particular cell. In order to avoid the RRCConnectionReconfiguration message becoming excessively large, the EUTRAN uses another reconfiguration procedure for re-activating measurements. The UE stops any inter-frequency and inter-RAT measurements and deactivates the measurement gap configuration, if no measurement configuration information is included in the message used to perform inter-frequency handover.
4. If the UE is able to act with the configuration included in the received RRCConnectionReconfiguration message, the UE starts a timer, known as T304 and initiates a random access procedure using the received RACH configuration, to the target cell at the first available occasion. The target cell does not specify when the UE need to initiate access in that cell. Hence, the handover process is sometimes described as asynchronous. The UE does not need to acquire system information directly from the target cell prior to initiating random access

and resuming data communication. The UE here derives new security keys and applies the received configuration in the target cell.

5. Once the random access procedure is successful, the timer T304 is stopped by the UE. The AS informs the upper layers in the UE about any uplink NAS message for which transmission might not have completed successfully, so that the NAS can take appropriate action before detach.

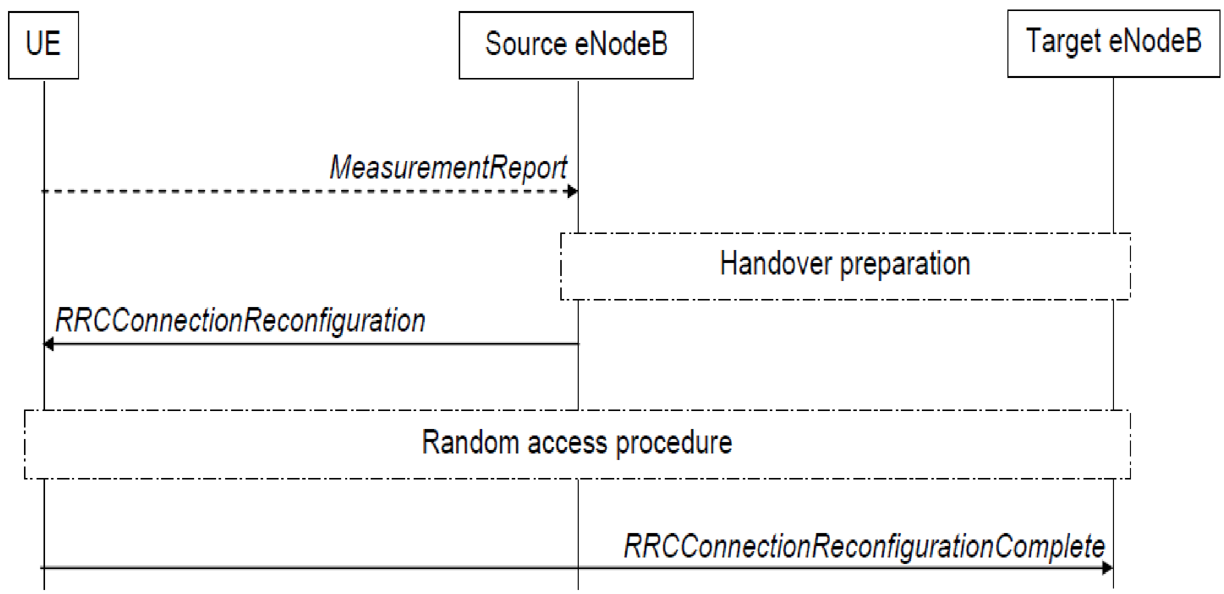


Figure 6.23 Handover Message Sequence [30]

In LTE technology, data buffering/storage during the DL occurs at the e-NB due the termination of RLC protocol at the e-NB which is different than UMTS architecture where data buffer occurs at the centralized Radio Network Controller (RNC) and inter-RNC handovers occurring less frequently. In LTE two mechanisms were proposed to minimize data loss during handovers. They are Buffer Forwarding and Buffer Bi-casting.

In buffer forwarding, the source e-NB forwards the buffered data for the UE to the target e-NB once the handover decision is taken. While in Buffer Bi-casting, the S-GW bi-casts or multi-casts the data to a set of e-NBs which are suppose to be candidates for being the next serving e-NB.

The issue with bi-casting is the determination of when to start bi-casting, because if bi-casting starts too early, there will be significant bandwidth backhaul requirement increase and if bi-casting starting too late results in packet loss. Hence, according to 3GPP, buffer forwarding mechanism was chosen to avoid packet loss for intra-LTE handovers that is source e-NB decides whether or not to forward traffic. To avoid reorder of packets, Packet Data Control Protocol (PDCP) sequence numbers are continued at the target e-NB to help UE to determine order of delivery of packets to higher layers. Buffer and context will be transferred between e-NBs through a new interface called X2 interface.

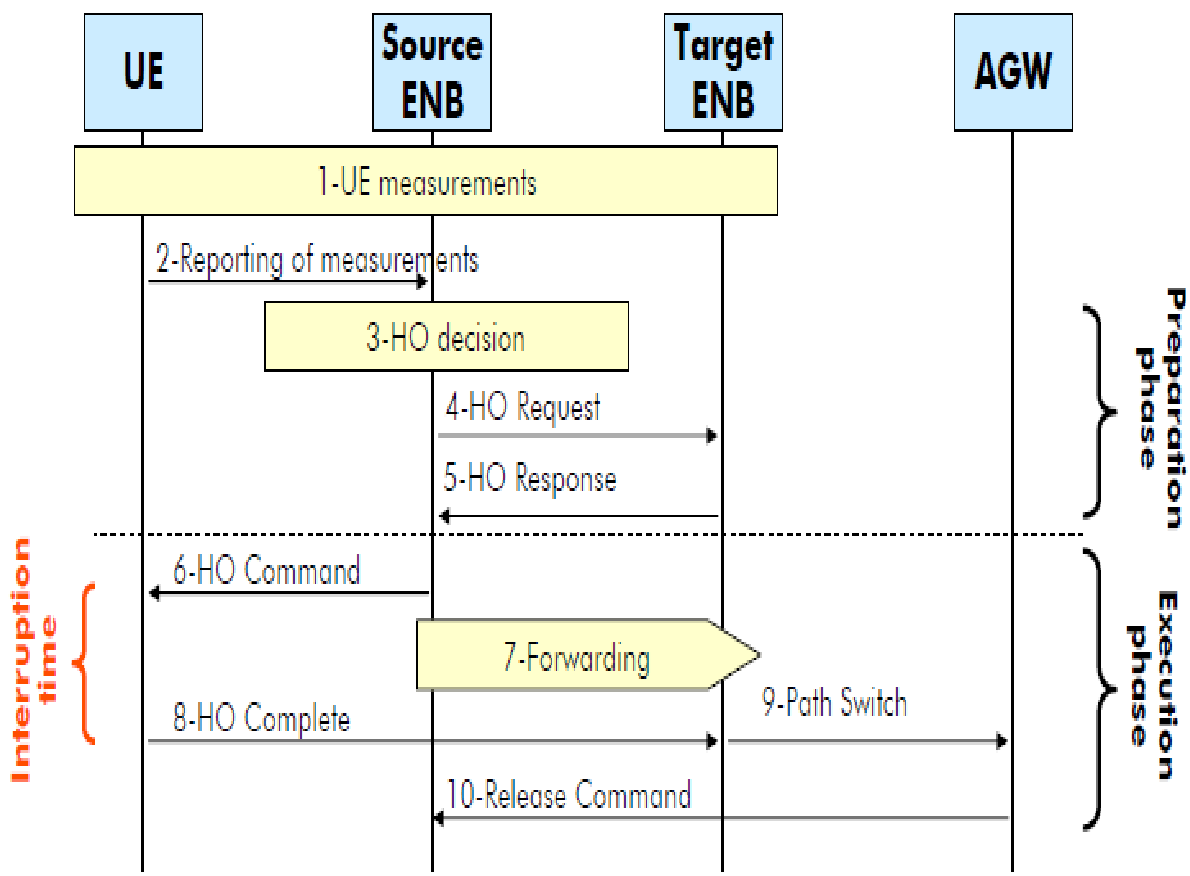


Figure 6.24 Intra- LTE Handover Procedure [26]

6.3.5.1 Types of Handovers

1. eNodeB Initiated Handover
    a. **Backward Handover** whereby the eNodeB controls the source cell requests the target eNodeB to prepare for handover
    b. **RLC Handover** or **Radio Link Failure Handover** that takes place when backward handover failure occurs or reconfiguration compliance failure occurs
    c. **NAS Recovery** occurs when target eNodeB is not prepared for handover
2. UE Initiated Handover
    a. **Forward Handover** whereby the UE by itself decides to connect to the target cell, where it then requests that the connection be continued

Before the source cell commands the UE to handover to target cell, the target cell also prepares the respective radio resources for handover. If the resources are not reserved then the UE transitions to idle-state where it again attempts to complete the handover procedure by transitioning back to connected-state using Non-Access Stratum (NAS) recovery procedure. The target cell for handover may belong to either the source e-NB i.e. intra-e-NB handover or a target e-NB i.e. inter-e-NB handover.

a) Backward Handover

In this hard handover process, the e-NB controlling the source cell requests the target e-NB to prepare for the handover. The target e-NB subsequently generates the RRC message to order the UE to perform the handover and the message is transparently forwarded by the source e-NB to the UE.

It can be described as network-controlled/UE-assisted mobility. In order for e-NB to be able to decode the Measurement Report from the UE and subsequently prepare the target cell for handover, the radio conditions need to be good enough and also for the UE to be able to decode the Handover Command from the source e-NB.

There is a short interruption in service between the time that the UE decodes the Handover Command from the source eNodeB and the time that the target eNodeB decodes the Handover Confirm from the UE. However, none of the data buffered in the source eNodeB is lost due to data forwarding and in-order deliver in LTE.

b) RLF Handover or RRC Connection Reestablishment

This handover procedure is also known as RRC Connection Reestablishment procedure in 3GPP Release 8 specifications. RLF handover is UE-based mobility and it provides a recovery mechanism whenever a backward handover signaling with source cell partially fails because of poor radio conditions provided that the security is active. The RLF handover takes place when though the radio conditions are sufficient for the source e-NB to be able to decode the Measurement Report from the UE and prepare the target cell for handover but the conditions is not sufficient enough for the UE to be able to decode the Handover Command from the source e-NB.

When a UE interprets any Radio Link defects, it will start the RLF timer called T311 timer, which is approximately 500ms or 1000ms but in the real time field trials that are performed it is kept to be 640ms and upon expiration of the RLF timer, the UE again starts searching for a suitable target cell frequencies and upon finding a suitable cell on an LTE frequency, the UE stops the timers T311 and starts the timer T301 and initiates a contention based random access procedure to enable the RRCConnectionReestablishmentRequest message and hence attempts to re-establish its connection with the target cell while remaining in connected-state. This re-establishment is successful if the source eNodeB has prepared the target cell for handover.

The UE in this message includes the identity of the cell and the identity used in the cell in which the failure occurred, a short Message Authentication Code and a cause. The EUTRAN carries out the re-establishment procedure to continue SRB1 and re-activate security without changing algorithms. An RRC connection reconfiguration procedure is executed to resume operation to re-activate measurements. If the cell in which the UE initiates the re-establishment is not prepared or in other words the cell does not have a context for that UE, the EUTRAN will subsequently reject the procedure, causing the UE to move to RRC_IDLE.

The RLF handover procedure results in additional delay and a longer interruption in service as compared to the backward handover but it also guarantee that none of the buffered data in the source e-NB is delivered and not lost.

c) NAS Recovery Handover

It is a UE-based mobility which is triggered if the target eNodeB is not prepared when the UE attempts re-establishment i.e. when the security is not active. This conveys that the radio conditions are not good enough for the source eNodeB to be able to decode the MeasurementReport from the UE. This results into the source eNodeB not able to prepare the target eNodeB for handover. In this NAS recovery procedure, the UE does not remain in connected-state. Upon re-establishment failure, the UE transitions into idle-state from connected state and attempts to establish a new connection.

Disadvantage

- Additional delay occurs compared to RLF handover procedure and longer interruption in service.
- Data forwarding and in-order delivery cannot be performed and all the data buffered in the source eNodeB is lost.
- Hence, TCP retransmissions needed, impacting throughput performance and consume valuable core network resources triggering retransmissions.

d) Forward Handover

LTE also supports a kind of 'forward' handover, in which the UE by itself decides to connect to the target cell, where it then requests that the connection be continued. The UE applies this connection re-establishment procedure only after loss of the connection to the source cell; the procedure only succeeds if the target cell has been prepared in advance for the handover. Here, handover related information is exchanged between the UE and target eNodeB.

This type of handover is possible even if the radio conditions are not good enough for source eNodeB to be able to decode the MeasurementReport from the UE and prepare the target cell or even with complete failure of signaling with the source eNodeB. Here the UE searches for a suitable target cell and attempts to re-establish its connection with the target cell while remaining in connected-state. If the target cell is not prepared, the target eNodeB fetches the UE's context from the source eNodeB. This will still include an additional delay versus the backward handover procedure and hence interruption in service but is less compared to RLF handover and NAS recovery procedure.

6.3.6 Connected Mode Inter-RAT Mobility

For handovers between LTE and other non-3GP technologies will take place using S2 interface.

6.3.6.1 Handover to LTE network

The handover procedure to LTE is similar to the handover procedure within LTE. The only difference is that upon handover to LTE network, the entire AS-configuration needs to be signaled where on the other hand within LTE it is possible to use 'delta signaling' where only the changes to the configuration are signaled. If the ciphering is not being activated yet in the previous RAT then the EUTRAN activates ciphering as part of the handover procedure.

6.3.6.2 Mobility from LTE network

This mobility procedure from LTE to another RAT includes both handover and Cell Change Order (CCO). Mobility from LTE is performed only after security has been activated. The procedure is described below:

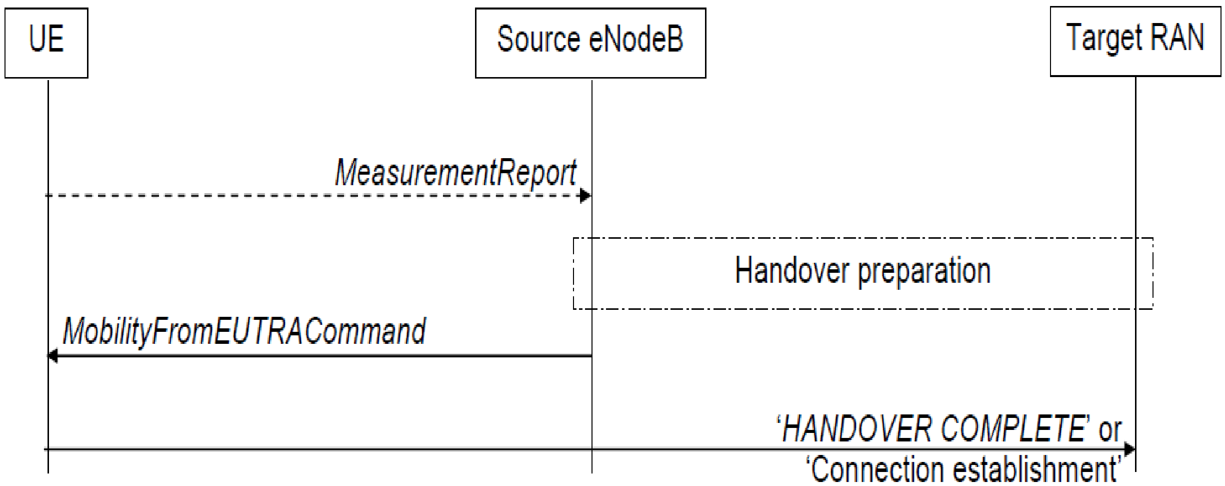


Figure 6.25 Mobility from LTE [30]

- The UE may send a MeasurementReport message.
- Whenever there is a handover, the source e-NB requests the target RAN node to prepare for the handover and hence as part of the 'handover preparation request' the source e-NB provides information about the UE capabilities of the applicable inter-RAT and also the information regarding the currently-established bearers. In response, to the source e-NB message, the target RAN gerates the 'handover command' and returns this to the source e-NB.
- The source e-NB sends a MobilityFromEUTRACommand message to the UE. This message includes either the inter-RAT message received from the target during handover or target cell/frequency and a few inter-RAT parameters.
- Upon receiving the above message, the UE starts the T304 timer. The UE then connects to the target node, by using received radio configuration or by initiating connection establishment.

6.4 Drop Call Analysis

Drop Calls are of two types happening in respective call scenarios. They are (1) Drops when not able to attach to an eNodeB (Mainly happens in short call), (2) Drops when UE not able to properly handover from source eNodeB to target eNodeB (Mainly happens in long call).

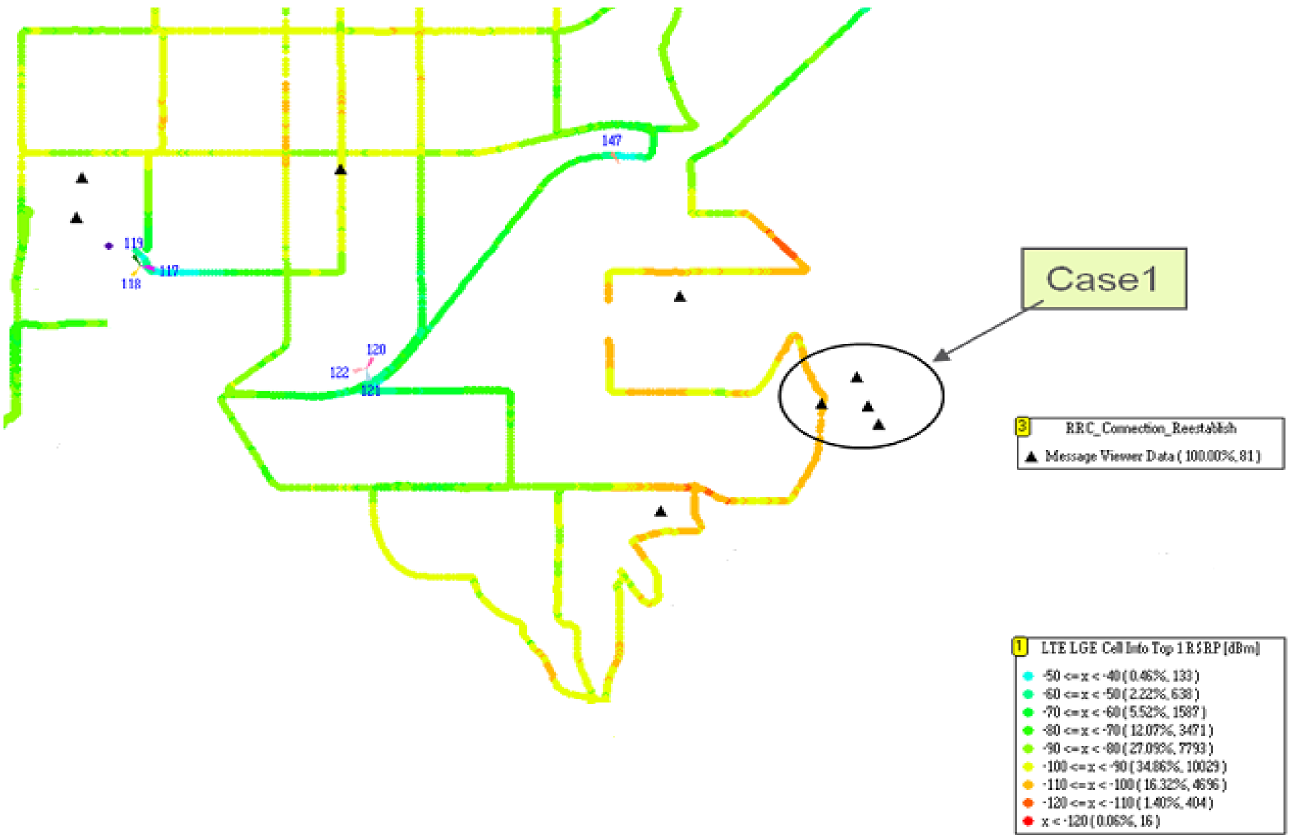


Figure 6.26 Drop Call Spots during the test trials [Courtesy: 3S Network Inc.]

Figure 6.26 shows the three cases of call drop that were due to three different reasons that are analyzed later in the paper. There could be many reasons for a drop call like failure due to poor RF conditions, timing out of LTE Timers, handover, failure due to other network, authentication failure and others. The few of the drop call reasons are highlighted later in the paper. Over here, I have just focuses only on one case of call drop that is caused due to handover.

6.4.1 Case 1 Analysis

To better understand case 1, I have first explained the cause of call drop.

Important parameters involved during handover:

- Control Parameters:
  - Hysteresis (dB) and Time to Trigger (TTT) (s)
- Measurement Parameters:
  - RSRP and SINR

Measurement Report Triggering

On the basis of measurement type, the UE measures and report any of the following:

- The serving cell and listed cells indicated as part of the measurement object.
- Detected cells on a listed frequency that are not listed cells but are detected cells by the UE.

For LTE, the below LTE event-triggered reporting criteria are specified:

- Event A1: Serving cell becomes better than absolute threshold
- Event A2: Serving cell becomes worse than absolute threshold
- Even A3: Neighbor cell becomes better than an offset relative to the serving cell
- Event A4: Neighbor cell becomes better than absolute threshold
- Event A5: Serving cell becomes worse than one absolute threshold and neighbor cell becomes better than another absolute threshold
-

For inter-RAT mobility, the following event-triggered reporting criteria are specified:

- Event B1: Neighbor cell becomes better than absolute threshold
- Event B2: Serving cell becomes worse than one absolute threshold and neighbor cell becomes better than another absolute threshold

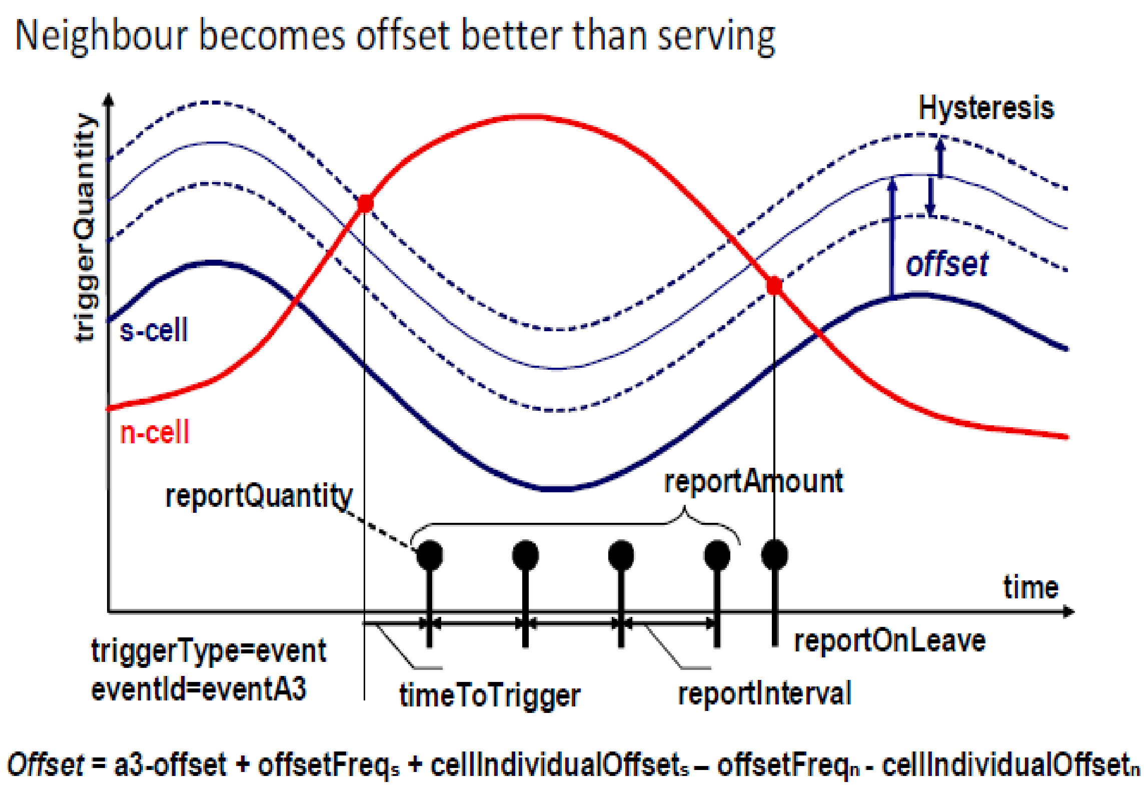


Figure 6.27 Event A3 [32]

The UE triggers an event when one or more cells meets a specified ‘entry condition’. The EUTRAN can impact the entry condition by setting the value of some configurable parameters used in conditions like one or more thresholds, an offset and a hysteresis. These entry conditions must meet for at least a duration corresponding to a ‘TimeToTrigger’ parameter configured by the EUTRAN in order for the event to be triggered. The UE scales the TimeToTrigger parameter depending on its speed.

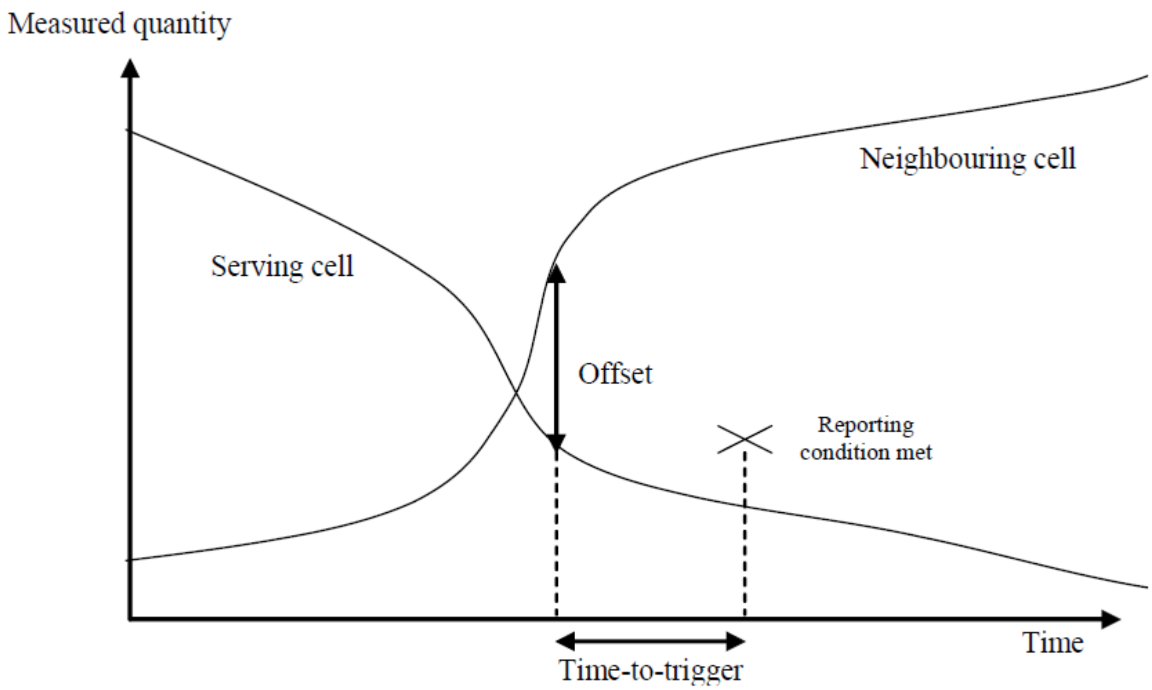


Figure 6.28 Event Triggered Report Condition (Event A3) [30]

The UE is configured to provide a number of periodic reports after having triggered an event. This 'event-triggered periodic reporting' is configured by means of parameters 'reportAmount' and 'reportInterval' that specify the number of periodic reports and the time period between them respectively. If this even-triggered periodic reporting is configured, the UE's count of the number of reports sent is reset to zero, whenever a new cell meets the entry condition. And the same cell cannot then trigger a new set of periodic reports unless it first meets a specified 'leaving condition'. Also to event-triggered reporting, the UE may be possibly configured to perform periodic measurement reporting rather than reporting only after the occurrence of an event.

The Figure 6.26 shows the analysis for the drop call case 2. The reason due to occurrence of EventA3 but the UE was not able to properly handover as the hysteresis and timetotrigger was not enough to trigger handover at a proper time. And hence the UE was executing ping-pong between the sites that is time to trigger Event A3 was happening late. RRC Drop occurred in good RF condition where server RSRP was decreasing and Neighbor RSRP was increasing rapidly and UE was not able to handover properly, the handover timer gets expired and the call was dropped. The reason is still better explained in this topic.

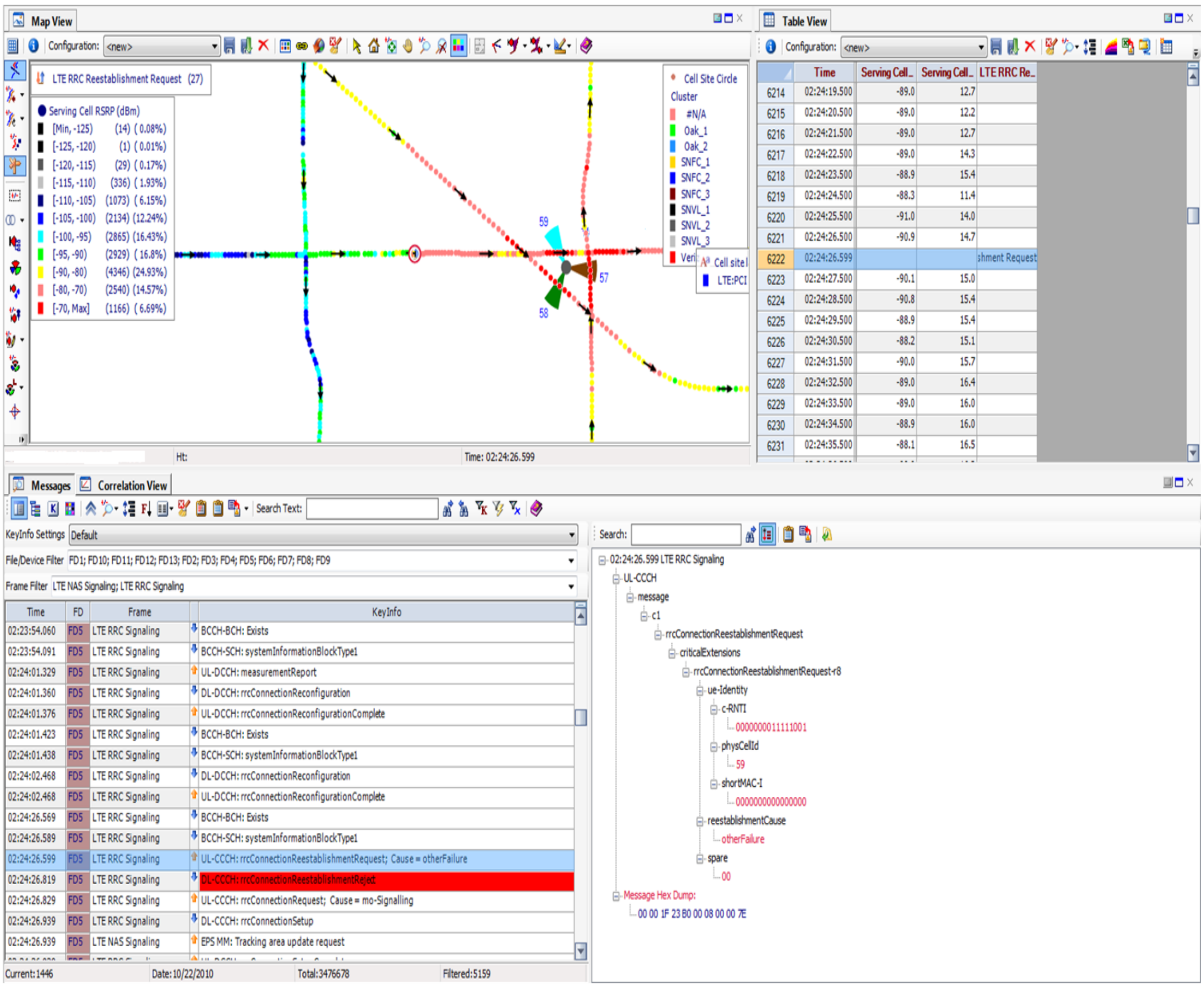


Figure 6.29 Analysis of Case 2 Drop Call due to Handover failure [Courtesy: 3S Network Inc.]

The recommended solution to avoid the drop was to change A3 time to trigger to 40ms on PCI 100 and 101 and change the hysteresis A3 to 5dB. A quicker HO fixed the drop in this area.

To allow the network to release the NAS signalling connection, the UE shall start the timer T3440 in the following cases: a) UE receives any of the EMM cause values, and b) UE receives a TRACKING AREA UPDATE ACCEPT message and the UE has not set the "active" flag in the TRACKING AREA UPDATE REQUEST message and the tracking area updating or combined tracking area updating procedure has been initiated in EMM-IDLE mode. Upon expiry of T3440, the UE shall locally release the established NAS signalling connection.

In case b,

- upon an indication from the lower layers that the user plane radio bearers are set up, the UE shall stop timer T3440 and may send uplink signalling via the existing NAS signalling connection or user data via the user plane bearers; or

- upon receipt of a DETACH REQUEST message, the UE shall stop timer T3440 and respond to the network initiated detach.

6.4.2 Other Cases for Call Drops

There were many different reasons for call drops couple of them are explained here. The reasons for drop calls are given below.

- Every RRC Connection request requires response within 1s, otherwise the T300 timer will expire. UE was unable to successfully RACH when trying to send the RRC Connection request within this 1s time. T300_Expiry is generally found in poor RF area. If found in good downlink RF then it is indicative of site issue or UL interference. UE does not reselect a better cell. For example, the UE sends measurement report to add PCI 121, a neighbor RSRP of serving cell being -105 dBm.

- Solution sites were awaiting turn up, these sites will increase coverage in a majority of the areas where the Setup Failures were found.

- RRC Setup failure rate (1.27%)

CHAPTER 7

CONCLUSION

Concluding the test analysis, my thesis results prove that LTE meets the requirement specifications and meets all the respective Key Performance Indicators that I needed to launch LTE technology. Also, the results show how different parameters affect throughput and connectivity of the User Equipment in a 4G networks. A 10MHz bandwidth at 2.6 GHz with a 2x2 MIMO antenna system was used in all the tests. While running in adaptive MIMO mode, the BTS switched automatically between single-stream transmission (transmit diversity) and multi-stream transmission (spatial multiplexing), depeding on the reported SNR of the UE. Also, adaptive modulation using QPSK, 16 QAM and 64 QAM was applied depending on the actual channel condition, or the reported SNR.

Test cases

a) A stationary test about 100 meters away from eNodeB site using multi UE's at the same measuring the UL and DL throughput.
b) Measuring the peak UL and DL Throughput using one single UE and full bandwidth applied to a single UE stationary around 200 meters away from the eNodeB site.
c) Measuring the control plane latency test
d) Analysis of Call Drops and solution for the same.

7.1 Test Trials Throughput Results

7.1.1 Average Throughput Result

Before showing the results, Channel capacity is calculated and simulated for a 10MHz bandwidth and graph is plotted for maximum channel capacity that could be achieved with it. Also, the results show the throughput meeting the channel capacity criteria.

Channel capacity is the tightest upper bound on the amount of information that can be reliably transmitted over a communications channel. Shannon–Hartley theorem states the channel capacity *C*, meaning the theoretical tightest upper bound on the information rate of clean data that can be sent with a given average signal power *S* through an analog communication channel subject to additive white Gaussian noise of power *N*, is:

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

where

- *C* - channel capacity in bits per second;
- *B* is the bandwidth of the channel in hertz;
- *S* is the total received signal power over the bandwidth measured in watt or $volt^2$;
- *N* is the total noise or interference power over the bandwidth, measured in watt or $volt^2$; and
- *S/N* is the signal-to-noise ratio (SNR) or the carrier-to-noise ratio (CNR)

By the noisy-channel coding theorem, the channel capacity of a given channel is the limiting information rate (in units of information per unit time) that can be achieved with arbitrarily small error probability. Figure 7.1 shows the channel capacity for a 10MHz bandwidth, the achieved information rate is 80 Mbits/second.

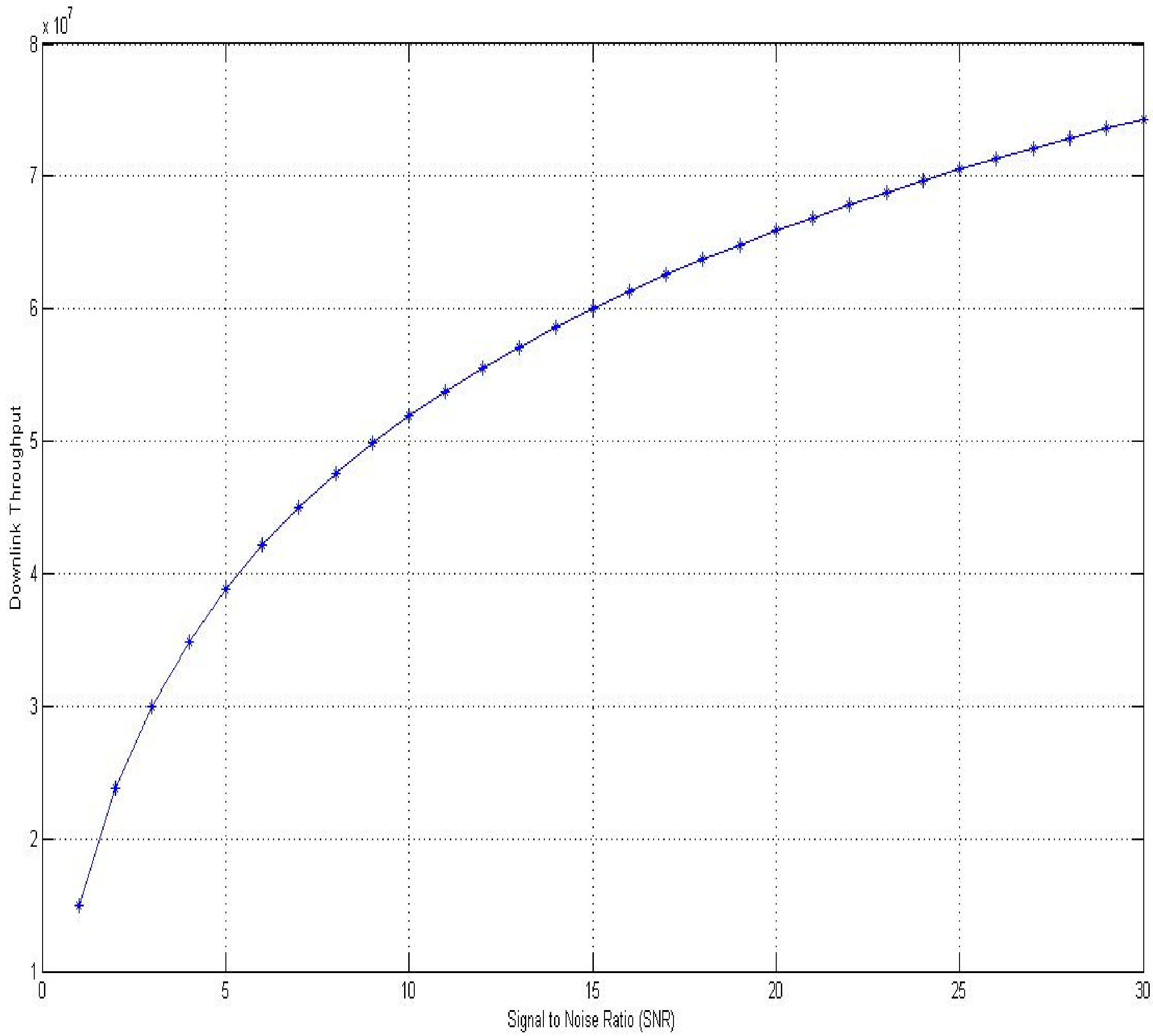


Figure 7.1 Channel Capacity graph for test trials

7.1.2 Peak Downlink Throughput Result

The Figure 7.2 shows the achieved peak downlink throughput and as seen from the figure, the peak throughput reached was 52 Mbps. This throughput is achieved at a Bandwidth of 15MHz. Also, as seen the RF conditions were good having an SNR of approximately 24 and signal strength RSRP -53 and BLER 0%. This result shows that the LTE does achieve the promised data rates. This shows that the achieved data rate is well under the upper bound of channel capacity.

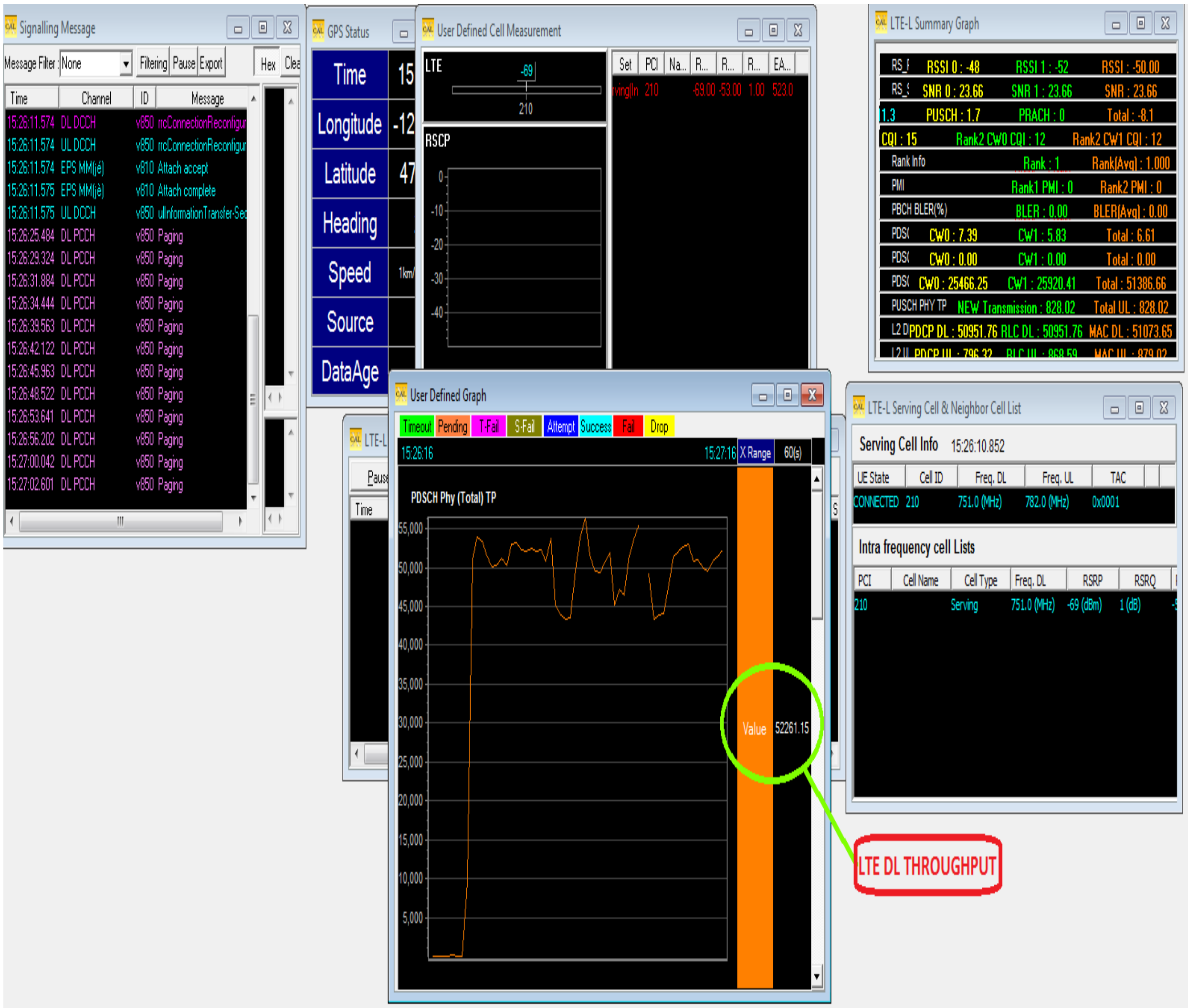


Figure 7.2 Peak Downlink Throughput for two user [Courtesy: 3S Network Inc.]

Figure 7.3 shows the effect of different parameters like RSRP and SINR on the achievable downlink throughput. As seen in the figure, the highest throughput rate is reached when mobile is in a good RF conditions with low interference and high signal strength. But in LTE as seen from the graph in Figure 7.3, show that even at cell edge where the RF conditions are not good still the it is possible to achieve acceptable throughput rates and hence results in a reduced call drops.

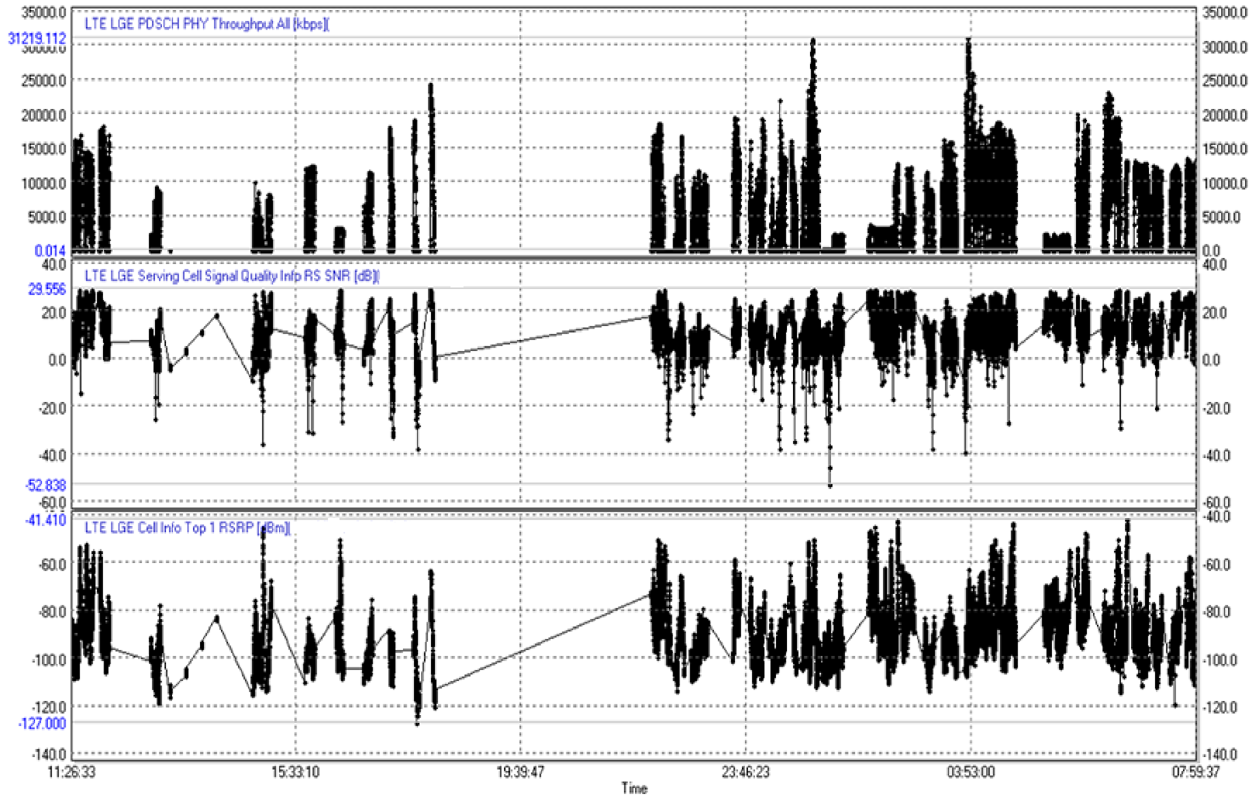


Figure 7.3 Average Downlink Throughput versus SINR and RSRP [Courtesy: 3S Network Inc.]

7.1.3 Peak Uplink Throughput Result

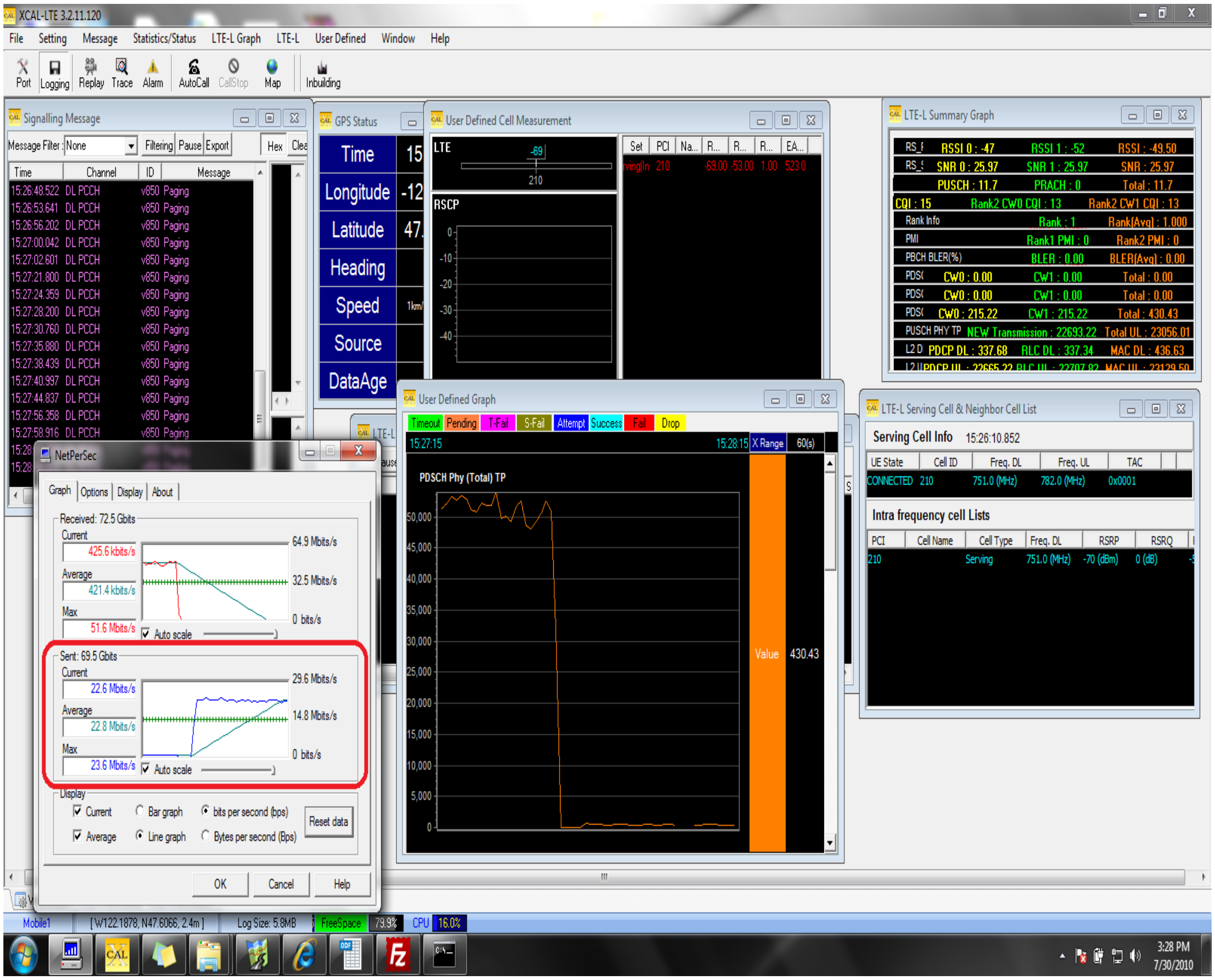


Figure 7.4 Peak Uplink Throughput for two user [Courtesy: 3S Network Inc.]

The above figure 7.4 shows the achieved peak uplink throughput that was achieved during the whole test. As seen from the figure, the peak throughput reached was 22.6 Mbps. This throughput is achieved at a Bandwidth of 15MHz.

Also, as seen the RF conditions were good having an SNR of approximately 25.97 and signal strength RSRP -53 and BLER 0%. This result shows that the LTE does achieve the promised data rates.

7.2 Latency Test Results

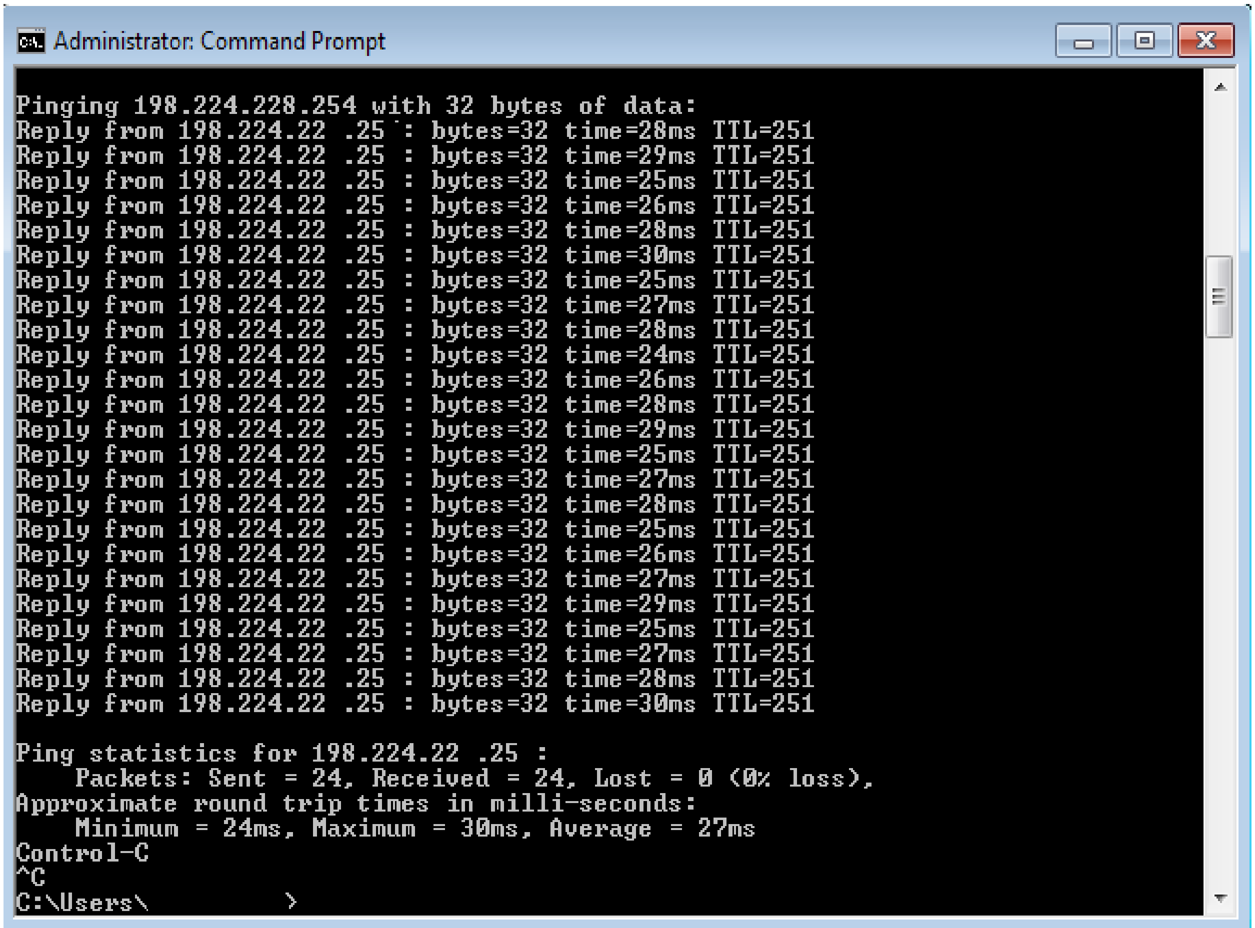


Figure 7.5 Control Plane Latency Test [Courtesy: 3S Network Inc.]

The Figure 7.5 shows LTE meeting the control plane latency criteria. The standards had set a control plane latency of 100ms that is the time from idle to connected mode. The result here shows the average latency of 27ms with a 0% loss. This shows the how fast LTE network can be. Also, the minimum latency reached was 24ms and the peak latency period was calculated as 30ms.

7.3 Test Trials Drop Call Results

Figure 7.6 shown above gives the distribution of different call drops with respect to the cause responsible for the drop. As seen from the pie chart maximum drops occurred due to other network. But in real world this is not a big issue as it can be solved easily by changing the antenna tilt and azimuth of antenna that is transmitting where it is supposed not to. Second largest drop is caused due to RRC Connection Failure by network itself. This category includes all drops that are due to poor RF condition, handover failure and others reasons that are related to the network itself where the UE is attached. But during the test this drops though high but not large enough that it cannot meet the specifications of 3GPP. Total of 42 drops out of 2000 calls that were made during the entire test, which is less than 2.5% of the drop.

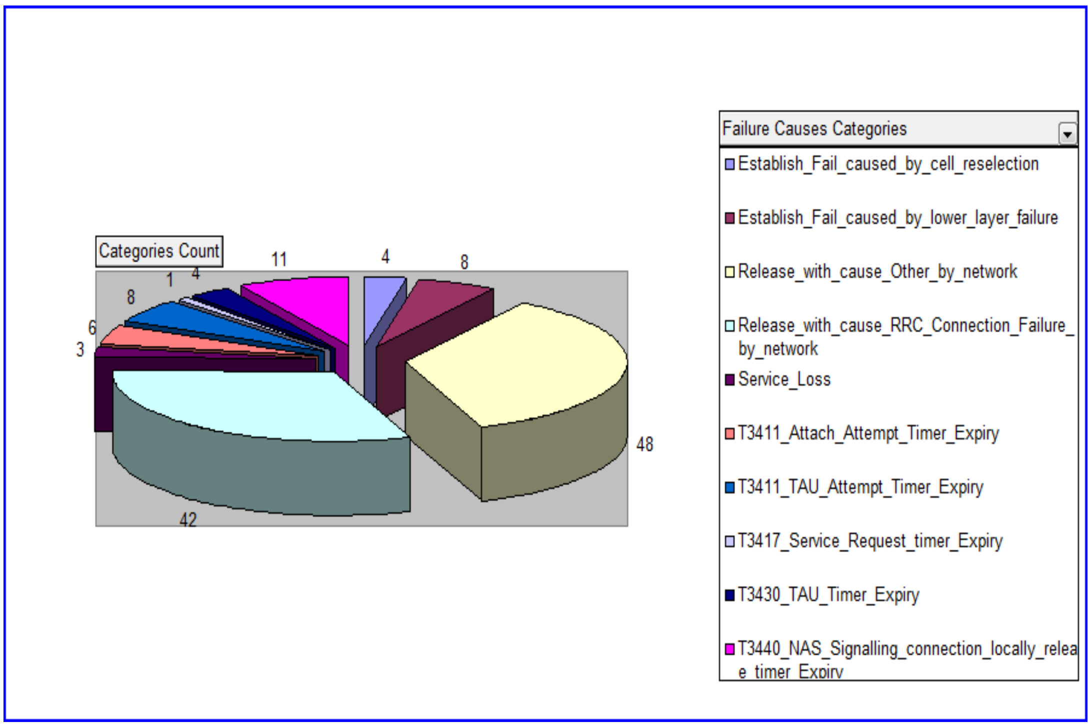


Figure 7.6 Pie Chart mentioning Drop Call categories [Courtesy: Ericsson and 3S Network Inc.]

7.4 Conclusion

Table 7.1 Results of Key Performance Indicators measured during the test

Category	Sub-Category	Target Value	Actual Value	Test UE configuration
Short Call Performance Accessibility	**Access Failure Rate**	**4%**	**1.19%**	**UE with 100KB DL**
Long Call Performance Accessibility	**Access Failure Rate**	**4%**	**1.24%**	**UE with 1GB DL**
Long Call Performance Retainability	**Session Failure Rate**	**4%**	**1.4%**	**UE with 1GB DL**
	RRC Drop	**5%**	**1.5%**	**UE with 1GB DL**
DL/UL Physical layer Throughput	**PDSCH Phy Throughput**	**20Mbps**	**52 Mbps 10Mbps Average for 4 user**	**SNR 24.6 RSRP -53**
	PUSCH Phy Throughput	**8Mbps**	**22.5 Mbps 10 Mbps Average for 2 user**	**SNR 25 RSRP -53**
RF-SINR	**Percent included Area>13dB**	**10%**	**46.70%**	**N/A**
Control Plane Latency	**Latency**	**100ms**	**27ms 24ms min 30ms max**	**N/A**

Table 7.1 shows the results for the target performance that are needed to show that the performance of LTE technology meets the preset Key Performance Indicator parameters. LTE had to meet the minimum criteria in order for it to prove the fastest network. The above calculated results of test show that LTE does meet the preset criteria.

APPENDIX A

LTE AND UMTS TERMINOLOGY AND CONCEPT COMPARISON

LTE Term	UMTS Term	1xEVDO	Meaning
		Air Interface Terms	
OFDMA	WCDMA	CDMA	Orthogonal Frequency Division Multiple Access, Physical layer of LTE Downlink
SC-FDMA	WCDMA	CDMA	Single Carrier Frequency Division Multiple Access, Physical layer of LTE Uplink
Subcarrier	Radio Channel	Radio Channel	A single 15kHz radio channel
Symbol	Chip (0.26µs)	Chip	A single 66.67µs time period
Resource Block	N/A	N/A	The smallest block of resources that can be allocated
Resource Element	N/A	N/A	The smallest unit of radio resources, one subcarrier for one symbol
Timeslot	Slot	Slot	7 consecutive symbols
Subframe	N/A	N/A	2 consecutive symbols
Radio Frame	Frame	Frame	10 consecutive subframes
Reference Signal	Common Pilot Channel (CPICH)	Pilot Channel	Periodic signal for transmission quality measurements

Access Network Terms			
EUTRAN	UTRAN	AN	Evolved Universal Terrestrial Radio Access Network
eNodeB	Node B	Base Station (BTS)	Evolved Node B
Physical Layer Cell ID	Scrambling Code	Pilot PN Offset	Unique cell identifier
X2	Iub and Iur	A13/A16/A17/A18	eNodeB to eNodeB interface
S1	Iu	A10/A11/A12	eNodeB to Core Network interface
LTE-Uu	Uu		LTE Air Interface
Core Network Terms			
EPC	Packet Switched Core Network (PS-CN)	Packet Data Network (PDN)	Evolved Packet Core
MME	Serving GPRS Support Node (SGSN)	RNC+PDSN	Mobility Management Entity
S-GW	Serving GPRS Support Node (SGSN)	PDSN	Serving Gateway
P-GW	Gateway GPRS Support Node (GGSN)	HA	Packet Data Network Gateway

HSS	Home Location Register (HLR)	HAA	Home Subscriber System
PCRF	PCRF	PCRF	Policy Charging Rule Function
EPS Bearer Service	PDP Context	PPP+MIP	A configured end-to-end traffic path between the UE and the PDN-GW (Radio Bearer + S1 Bearer)

APPENDIX B

LIST OF ACRONYMS

3GPP – 3rd Generation Partnership Project

3GPP2 – 3rd Generation Partnership Project 2

ACK – Acknowledgment

AMPS – Analogue Mobile Phone System

APN – Access Point Name

ARFCN – Absolute Radio Frequency Channel Number

ARQ – Automatic Repeat request

AS – Access Stratum

BCH – Broadcast Channel

BCCH – Broadcast Control CHannel

BLER – BLock Error Rate

CAZAC – Constant Amplitude Zero AutoCorrelation

CCCH – Common Control CHannel

CDMA – Code Division Multiple Access

CN – Core Network

CPICH – Common PIlot CHannel

CQI – Channel Quality Indicator

CRC – Cyclic Redundancy Check

dB – deci-Bel

DCCH – Dedicated Control Channel

DL – Downlink

DL-SCH – Downlink Shared CHannel

eNodeB – evolved Node NodeB

EPC – Evolved Packet Core

EPS – Evolved Packet System

EUTRAN – Evolved UTRAN

FDD – Frequency Division Duplex

FDMA – Frequency Division Multiple Access

GPRS – General Packet Radio Service

GTP – GPRS Tunneling Protocol

HARQ – Hybrid Automatic Repeat request

HLR – Home Location Register

HSDPA – High Speed Downlink Packet Access

HSUPA – High Speed Uplink Packet Access

IMSI – International Mobile Subscriber Identity

MBSFN – Multimedia Broadcast Single Frequency Network

MBMS – Multimedia Broadcast/Multicast Service

MCCH – Multicast Control CHannel

MCH – Multicast CHannel

MIB – Master Information Block

MIMO – Multiple Input Multiple Output

NACK – Negative ACKnowledgement

NAS – Non Access Stratum

PAPR – Peak-to-Average Power Ratio

PBCH – Physical Broadcast CHannel

PCC – Policy Control and Charging

PCCH – Paging Control CHannel

PCI – Physical Cell Identity

PDN – Packet Data Network

PDU – Protocol Data Unit

PLMN – Public Land Mobile Network

PRACH – Physical Random Access CHannel

PSS – Primary Synchronization Signal

QAM – Quadrature Amplitude Modulation

QCI – QoS Class Identifier

RA – Random Access

RAN – Radio Access Network

RNC – Radio Network Controller

SAE – System Architecture Evolution

SSS – Secondary Synchronization Signal

REFERENCES

[1] 3GPP TS 36.213 3rdd Generation Partnership Project, Technical Specification Group Radio Access Network: Evolved Universal Terrestial Radio Access (E-UTRA), Physical Layer Procedures. Release 8.

[2] 3GPP TS 36.213 3rdd Generation Partnership Project, Technical Specification Group Radio Access Network: Evolved Universal Terrestial Radio Access (E-UTRA), Physical Channels and Modulation. Release 8.

[3] 3GPP TS 25.304: User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode

[4] 3GPP TR 25.913: Technical Specification Group Radio Access Network; Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (EUTRAN)

[5] 3GPP TR 36.331: Technical Specification Group Radio Access Network; Requirements for Evolved UTRA (E-UTRA); Radio Resource Control (RRC); Protocol Specification; Release 9

[6] 3GPP TR 36.300: Technical Specification Group Radio Access Network; Evolved UTRA and Evolved UNTRAN; Overall Description State 2; Release 8

[7] 3GPP Technical Specification 36.133, ‘Evolved Universal Terrestrial Radio Access (EUTRAN); Requirements for Support of Radio Resource Management. Release 8.

[8] UMTS overview by K.W. Richardson

[9] Impact of Intra-LTE Handover with Forwarding on the User Connections by Lajos Bajzik, Peter Horvath, Laszlo Korossy, Csaba Vulkan.

[10] Technical Overview of 3GPP LTE by Hyung G. Myung, May 18, 2008.

[11] LTE Whitepaper by Santosh Kumar Dornal

[12] E-UTRA RACH within the LTE system by Romain Masson

[13] Public Safety Communication over 3GPP LTE, Master's Thesis by Stefan Sundkvist, Lulea University of Technology, February 7, 2008.

[14] Cell search and cell selection in UMTS LTE, Application Note by Rohde and Schwarz

[15] Field trials of LTE with 4x4 MIMO by Johan Furuskog, Karl Werner, Mathias Riback and Bo Hagerman.

[16] Nokia Siemens Networks and Aalborg University, "Performance Analysis of Handover Measurements and Layer 3 Filtering for UTRAN LTE".

[17] Moray Rumney, "3GPP LTE: Introducing Single-Carrier FDMA", Agilent Review.

[18] Robertson, P.; Kaiser, S. "The effects of Doppler spreads in OFDMA mobile radio systems", Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS.

[19] H.G. Myung et al., "Single Carrier FDMA for Uplink Wireless Transmission," IEEE Vehic. Tech. Mag., vol. 1, no. 3, Sep. 2006

[20] Long Term Evolution – 3GPP LTE Radio and Cellular Technology by Borko Furht and Syed A. Ahson.

[21] Yngve Selen and Henrik Asplund, "3G LTE Simulations Using Measured MIMO Channels", Ericsson Review.

[22] Riback, M & Karlsson, J., 2008. Initial field performance measurements of LTE. Ericsson Review.

[23] LTE Performance for Initial Deployments: Technical White Paper from Nokia Siemens Networks.

[24] LTE Mobility Enhancements, Qualcomm Incorporated, February 2010.

[25] Long Term Evolution (LTE): A Technical Overview, Technical White Paper from Motorola Inc.

[26] 3GPP Long-Term Evolution/System Architecture Evolution Overview, September 2006, Ulrich Barth, Alcatel.

[27] Fundamentals of LTE by Arunabha Ghosh, Jun Zhang, Rias Muhamed.

[28] Evolved Packet System,The LTE and SAE Evolution of 3G UMTS by Pierre Lescuyer and Thierry Lucidarme.

[29] LTE for UMTS, OFDMA and SC-FDMA Based Radio Access by Harri Holma and Antti Toskala,

[30] UMTS – The Fundamentals by B. Walke, P. Seidenberg and M.P. Althoff.

[31] LTE- The UMTS Long Term Evolution from Theory to Practice by Stefania Sesia, Issam Toufik and Matthew Baker.

[32] LTE Measurement Events by Jakub Bluszcz, Leliwa Technical Bulletin.

WEBSITES

[1] www.wikipedia.com

[2] www.google.com

[3] http://www.3glteinfo.com/umts/umts-cell-selection-procedure

[4] http://wirelessoom.wordpress.com/2009/06/23/what-is-happening-when-you-switch-on-your-phone/

[5] www.radio-electronics.com

[6] www.eventhelix.com

[7] www.3g4g.co.uk

[8] www.umtsworld.com

[9] http://wired-n-wireless.blogspot.com

[10] http://3g4g.blogspot.com/2009/08/simplicity-of-lte-and-its-differences.html

[11] http://lte-epc.blogspot.com/2009/11/lte-control-plane-protocol-stacks.html

[12] http://bandarupallivenu.blogspot.com/2010/12/hierarchical-channel-structure-of-lte.html

[13] www.polarisnetworks.net/lte_functional_testers

[14] http://jawadsblog.wordpress.com/2009/12/14/idle-cell-selection-in-lte/

BIOGRAPHICAL INFORMATION

Sanil Hajibhai Fulani was born on August 15th, 1986 in Rajkot, Gujarat, India. He received his Bachelor of Engineering in Electronics and Communication Engineering from Gujarat University, India in June 2008. Prior to pursuing his Masters, he took software training at L&T InfoTech, Mumbai, India. In Spring 2009, he started his Master's studies in Electrical Engineering Department with a focus of Wireless Communication and Networking at The University of Texas at Arlington, United States. He received his Master's in Electrical Engineering from the University of Texas at Arlington in May 2011. His research interests include wireless communication, digital communication and computer networks.