Chapter 4
3G Communication Protocols

4.1 UTRAN Protocol Structure: The encryption mechanism is built into radio network protocols .The protocols in the RAN in UMTS are divided into three layers namely physical layer, data link layer and network layer. This division is according to OSI (Open systems Interconnection) model. Data link layer is further divided into several sublayers:

- MAC;
- RLC;
- Packet Data Convergence Protocol(PDCP);
- Broadcast/Multicast Control (BMC).

The physical layer and MAC support both user (U)plane and control (C) plane traffic in the same manner. Both the PDCP and BMC only exist in the U-plane whereas the RLC and layer 3 are divided into U-plane and C-plane.

Network layer is divided into several sublayers. The lowest sublayer RRC terminates in the UTRAN in the RNC. Higher sublayers terminate in the CN. The RRC protocol exist in the C-plane. The protocol structure is shown in figure 4.1.

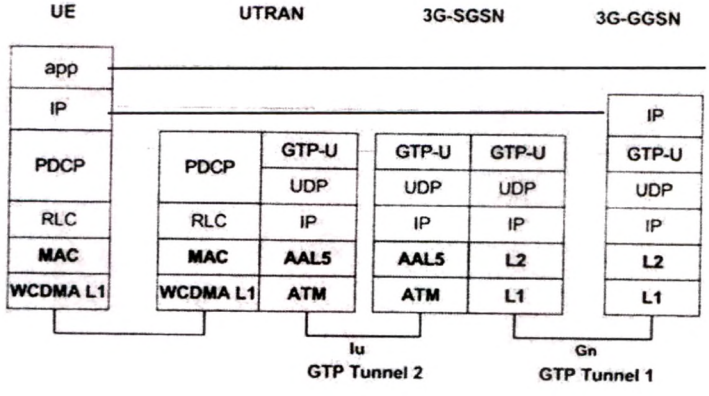

Figure 4.1 3G mobile communication protocol structure

4.2 Physical Layer: Physical layer services convert physical radio channels to transport channels. Layer 1 services include error detection and correction, frequency and time synchronization, multiplexing of transport channels, interleaving, modulation, power control , measurements and execution of soft handovers. The transport channels are divided into two main categories:

- Common channels- if only one particular UE(User Equipment) needs to be addressed, inband signalling is used;
- Dedicated channels(DCH)- the whole channel is reserved for one particular user.

Common channels include the Random Access channel (RACH) for transmitting short uplink messages (e.g. for initial access),the Forward Access channel (FACH) for short downlink messages, the Paging Channel(PCH) and the Broadcast Channel(BCH).

In GSM, encryption is done in the physical layer. As the physical layer terminates at the BS, an important target for improved security in UMTS was to move the termination point of encryption further back into the network. For this reason, encryption is not done in the physical layer in UMTS.

4.3 MAC Layer: The MAC layer converts transport channels into logical channels, which are characterized by what kind of data are transferred. There are two kinds of logical channels:

- Traffic channels –for U-plane information
- Control channels-for C-plane information

Logical channels include the broadcast control channel, paging control channel, common control channel (CCCH), dedicated control channel (DCCH), common traffic channels and dedicated traffic channels. These logical channels are mapped into transport channels.

The MAC layer contains the following functions:

- Mapping logical channels into transport channels;
- Choosing an appropriate transport format for each transport channel;
- Identification of an addressed UE in common channels;
- Multiplexing of upper layer PDUs;

- Traffic volume measurement.

The MAC layer also performs encryption in transparent RLC mode in the case of CS speech traffic. In this case the part that is encrypted is the MAC SDU (Signalling Data Unit) but the MAC header is not. The counter CFN (Connection Frame Number) consists of the least significant part of the encryption counter COUNT-C.

It is possible that several MAC PDUs are transmitted during the same Transmission Time Interval (TTI). In this case ciphering is not initialized in the middle of the TTI. Instead , the input parameter COUNT-C for the whole TTI is obtained from the CFN of the first radio frame in the TTI. Then a long mask bit stream is generated and used to encrypt all radio frames in the TTI.

4.4 RLC (Radio Link Control) Layer : The RLC layer provides the following services to upper layers:

- Transparent data transfer-upper layer PDUs are transmitted without any additional protocol information except possibly segmentation/reassembly of them
- Unacknowledged data transfer-upper layer PDUs are transmitted without guarantees of delivery, but with detection of transmission errors;
- Acknowledged data transfer-upper layer PDUs are transmitted with guaranteed delivery, potential retransmissions are used for error-free delivery and double transmissions are also detected
- Maintenance of Quality of Service(QoS) as defined by upper layers;
- Notification of irrecoverable errors to upper layers

The most important RLC functions are :segmentation and reassembly of upper layer PDUs; concatenation of the of the first segment of an RLC SDU with last segment of the previous RLC SDU into the same RLC PDU ,adding padding bits in case no concatenation is possible; data transfer; error correction; in-sequence delivery of upper layer PDUs, duplicate detection; RLC SQN check ; protocol error detection and recovery.

The RLC layer also provides encryption in unacknowledged and acknowledged RLC modes, when ciphering is applied to the whole RLC PDU except the PDU header. The header consists of a SQN(7 bits) and an extension bit (making one octet) in the UM (Unacknowledged Mode) case, and of a SQN(12 bits) and 4 other bits (making two octets)in the AM (Acknowledged Mode) case. In the former case, the extension bit of the header indicates whether a length indicator follows or the data. In the AM case, the 4 bits that are included in the header in addition to the SQN indicate:

- Whether the PDU contains control information or data;
- Whether a status report is requested from the receiver;
- Whether the length indicator follows or the data

4.5 PDCP : The PDCP provides header compression/decompression of IP (Internet Protocol) traffic, among other things.

4.6 BMC : The BMC provides transmission and scheduling of BMC messages and storage and delivery of cell broadcast messages.

4.7 RRC: The RRC provides such functions as :

- Broadcast of both NAS and Access Stratum(AS) information –for NAS information, the RRC provides scheduling, segmentation and repetition ;
- Establishment ,re-establishment, maintenance and release of RRC connections between the UE and RNC;
- Establishment, reconfiguration and release of (U-plane) radio bearers requested by upper layers;
- RRC connection mobility functions such as handovers, preparations for handovers to GSM, cell reselection;
- Paging and notification requested by upper layers;
- Control of requested QoS ;
- Control of UE measurements and related reporting

The RRC also provides encryption control as well as executing integrity protection of both RRC level signalling and higher layer signalling in the form of message authentication codes (MAC-I).

4.8 Mobile IP Network Architecture and Protocol Stack: The mobile IP protocols provide mobility to Internet access. Two methods have been proposed: (1) Internet access configuration using a mobile IP tunnel and (2) Intarnet access configuration using voluntary L2TP tunnels and mobile IP.

4.8.1 Internet Access Configuration Using a Mobile IP Tunnel: Figure 4.2 provides an overview. Mobility is provided through the mobile IP protocol. Forward traffic is routed between the home and foreign agents using a mobile IP tunnel. Reverse traffic is routed directly from the foreign agent to the remote server.

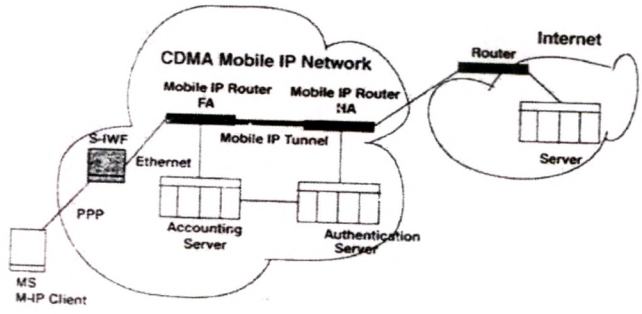

Figure 4.2 Internet Access Network Architecture

4.8.2 Functional Allocation : This configuration supports mobile IP as follows:

- A mobile IP capable router on the visited network provides the foreign agent (FA) function
- A mobile IP capable router on the home network provides the home agent(HA) function
- An external authentication server may be connected to the HA router to maintain subscriber information and perform mobile IP authentication.
- An external accounting server may be connected to interface with FA routers to collect and store accounting records. A single external server may perform both the authentication and accounting functions.
- The IWF in the serving system(S-IWF) and FA router reside on the same LAN are interconnected by Ethernet.

- The S-IWF terminates PPP protocol and relays IP datagrams received from the mobile to the designated mobile-IP FA router on the local network.
- The HA router is fixed, and its IP address is conveyed to the FA by the mobile in the mobile IP registration message.

4.8.3 Protocol Stack : Figure 4.3 shows the protocol stacks provided by each of the network elements in a mobile IP implementation.

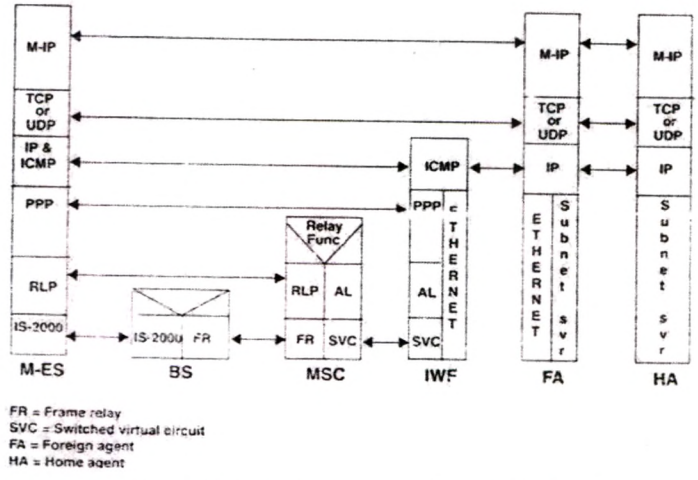

Figure 4.3 Protocol stacks in Mobile IP

4.8.4 Security:

- Three levels of authentication and authorization validation are provided :IS-41 service authorization validation (mandatory), IS-41 authentication (optional) and mobile HA authentication for mobile IP registration /reply messages(mandatory)
- Data privacy over the air link can optionally be provided by using RLP encryption between the mobile and packet switching unit(PSU).RLP encryption requires the IS-41 authentication feature to be activated.
- Identification inserted in the mobile IP registration request/reply provides antireply protection for registration messages.

4.8.5 Packet Routing:

- Datagrams sent by the mobile are delivered to the S-IWF for relaying to the FA. The FA routes datagrams from the mobile to the destination.
- The HA encapsulates datagrams destined for the mobile in another IP header and forwards them to the FA.
- The FA decapsulates the datagrams from the HA over the mobile IP tunnel and relays the original datagrams destined for the mobile to the S-IWF for delivery to the mobile.

4.8.6 Accounting: FA routers or IWFs collect accounting records and send them to designated accounting servers for storage.

4.8.7 Intranet Access configuration using voluntary L2TP Tunnels and Mobile IP: Figure 4.4 shows the intranet access network architecture using voluntary L2TP tunnels and mobile IP protocols. However a voluntary tunnel is established by the client between itself and an L2TP server. All forward and reverse traffic is sent through the L2TP tunnel. Voluntary tunneling is client-initiated tunneling in which the client encapsulates and encrypts the data to be transmitted right from his laptop. Mobile users initiate voluntary tunneling by invoking L2TP client software on the laptop, which directly interacts with L2TP server software on the L2TP network server (LNS) over the mobile IP connection.

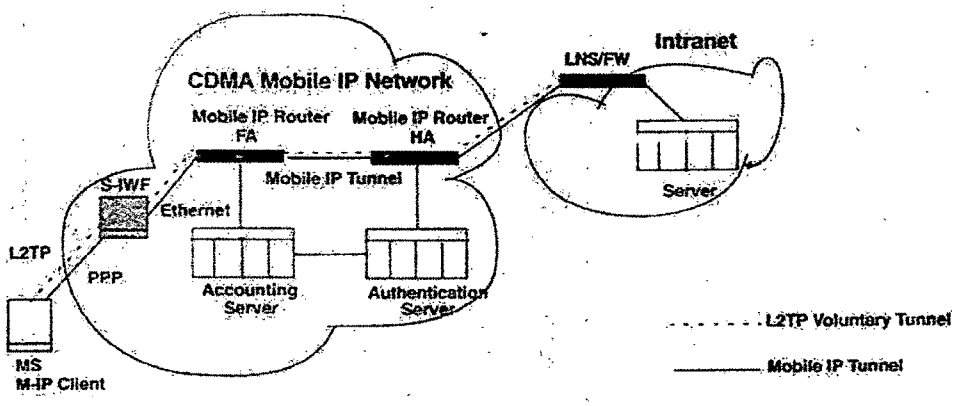

Figure 4.4 Intranet Access Network Architecture

4.8.8 Protocol Stack: Figure 4.5 shows the protocol stacks provided by each network element in a mobile IP implementation using a voluntary L2TP tunnel.

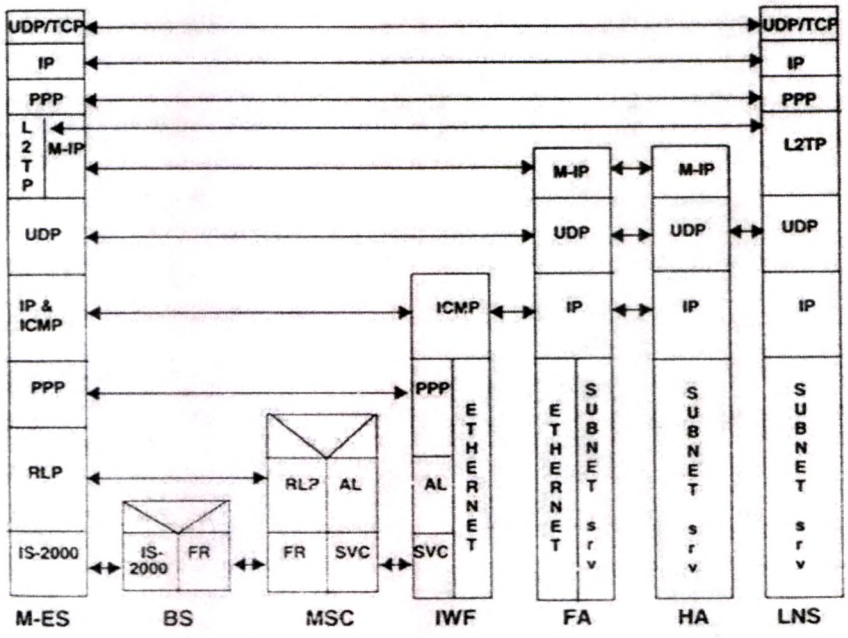

Figure 4.5 Protocol stack in Mobile IP using Voluntary L2TP Tunnel

4.8.9 Addressing:

- Private network assigns address to terminal by LNS using PPP contained within voluntary tunnel.
- Wireless session protocol (WSP) assigns IP address to user for link between mobile and wireless network

4.8.10 Security and Firewall Traversal:

- Two levels of authentication are provided:IS-41 authentication(optional) and mobile HA authentication during mobile IP registration (mandatory)
- Identification inserted in the mobile-IP registration request/reply provides antireply protection

- LNS authenticates terminals using PPP authentication integrity such as challenge handshake authentication protocol.
- Alternatively, end-to-end authentication, integrity and confidentiality can be provided if the terminal and LNS support IP.

4.9 Summary: This chapter describes communication protocols used in 3G communication systems as per OSI model . The encryption mechanism is built into these radio network protocols .The protocols are part of lowest three layers namely physical layer, data link layer and network layer. The chapter ends with discussion on mobile IP protocol and security issues related with it.