# Chapter 2
# Network Architecture and Protocols

The Third Generation Partnership Project (3GPP) Long-Term Evolution/System Architecture Evolution (LTE/SAE) seeks to take mobile technology to the next level through the realization of higher bandwidths, better spectrum efficiency, wider coverage, and full interworking with other access/backend systems. LTE/SAE proposes to do all this using an all-IP architecture with well-defined interworking with circuit-switched systems. Additionally, the evolved 3GPP system introduced a hybrid mobile network architecture supporting radio access technologies and several mobility mechanisms. We begin this chapter by introducing the LTE network reference model and define its various functional entities and its interconnection possibilities. Next, we discuss the end-to-end protocol layering in a LTE network, network selection and discovery, and IP address allocation. Finally, we describe in more detail the functional architecture and processes associated with security, QoS, and mobility management.

## 2.1 Architecture Model and Concepts

The network architecture of LTE is based on functional decomposition principles, where required features are decomposed into functional entities without specific implementation assumptions about physical network entities. This is why 3GPP specified a new packet core, the Evolved Packet Core (EPC), network architecture to support the E-UTRAN through a reduction in the number of network elements, simpler functionality, improved redundancy, and most importantly allowing for connections and hand over to other fixed line and wireless access technologies, giving the service providers the ability to deliver a seamless mobility experience.

## 2.2 Architecture Reference Model

Figure 2.1 shows the LTE network reference model, which is a logical representation of the network architecture. The network reference model identifies the functional entities in the architecture and the reference points between the functional entities

T. Ali-Yahiya, *Understanding LTE and its Performance*,
DOI 10.1007/978-1-4419-6457-1_2, © Springer Science+Business Media, LLC 2011

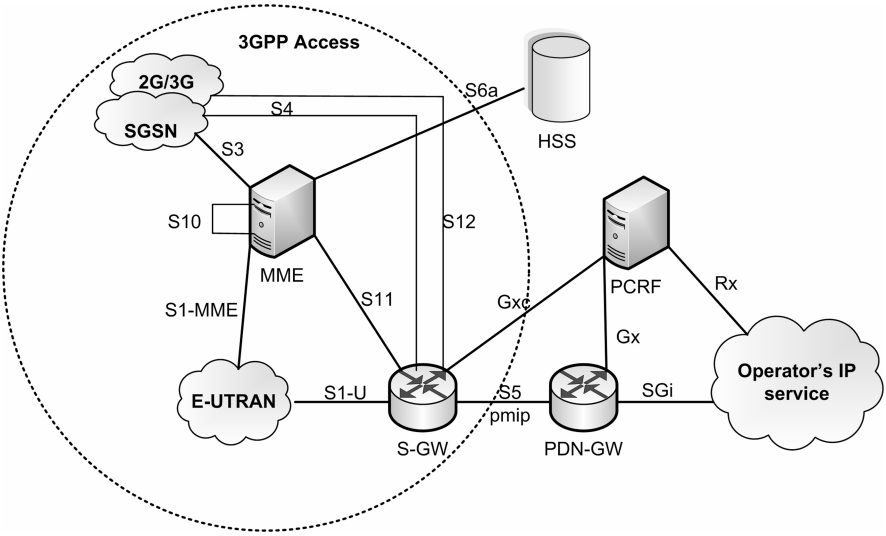


**Fig. 2.1** LTE reference model

over which interoperability is achieved. The overall architecture has two distinct components: the access network and the core network. The access network is the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The core network is all-IP core network and is fully Packet Switched (PS). Services like voice, which are traditionally Circuit Switched (CS), will be handled using IP Multimedia Subsystem (IMS) network. The core network is called the Evolved Packet Core (EPC). Network complexity and latency are reduced as there are fewer hops in both the signaling and data plane. The EPC is designed to support non-3GPPP access supports for mobile IP. To improve system robustness security, integrity protection, and ciphering have been added and represented by Non-Access Stratum (NAS) plane, which is an additional layer of abstraction to protect important information like key and security interworking between 3GPP and non-3GPP network [3]. Apart from the network entities handling data traffic, EPC also contains network control entities for keeping user subscription information represented by Home Subscriber Server (HSS), determining the identity and privileges of a user and tracking his/her activities, i.e., Authorization, Authentication and Accounting (AAA) server, and enforcing charging and QoS policies through a Policy and Charging Rules Function (PCRF). Note that E-UTRAN and EPC together constitute the Evolved Packet System (EPS).

Both radio access network and core network could achieve many functionalities including

- Network Access Control Functions
- Packet Routing and Transfer Functions
- Mobility Management Functions
- Security Functions

- Radio Resource Management Functions
- Network Management Functions

## *2.2.1 Functional Description of LTE Network*

We highlight in this section the functional description of the most important part of the LTE network architecture which is divided into radio access network and core network.

### 2.2.1.1 Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

E-UTRAN is the air interface of 3GPP's Long-Term Evolution (LTE) upgrade path for mobile networks. It is a radio access network standard meant to be a replacement of the UMTS, HSDPA, and HSUPA technologies specified in 3GPP releases 5 and beyond. LTE's E-UTRAN is an entirely new air interface system, which provides higher data rates and lower latency and is optimized for packet data. It uses OFDMA radio access for the downlink and SC-FDMA for the uplink. The E-UTRAN in LTE architecture consists of a single node, i.e., the eNodeB that interfaces with the user equipment (UE). The aim of this simplification is to reduce the latency of all radio interface operations. eNodeBs are connected to each other via the X2 interface, and they connect to the PS core network via the S1 interface (see Fig. 2.2).

A general protocol architecture of E-UTRAN (Fig. 2.3) splits the radio interface into three layers: a physical layer or Layer 1, the data link layer (Layer 2), and the network layer or Layer 3. This hierarchical stratification provides a complete vision of the radio interface, from both the functionality associated with each of the structured layer to the protocol flow between them. The purpose of the protocol

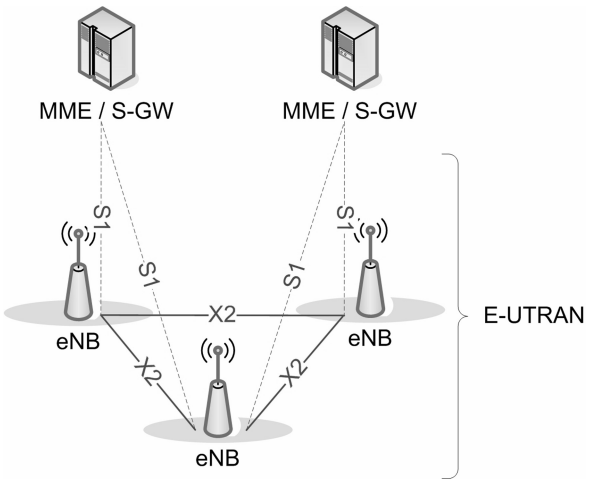


**Fig. 2.2** E-UTRAN architecture

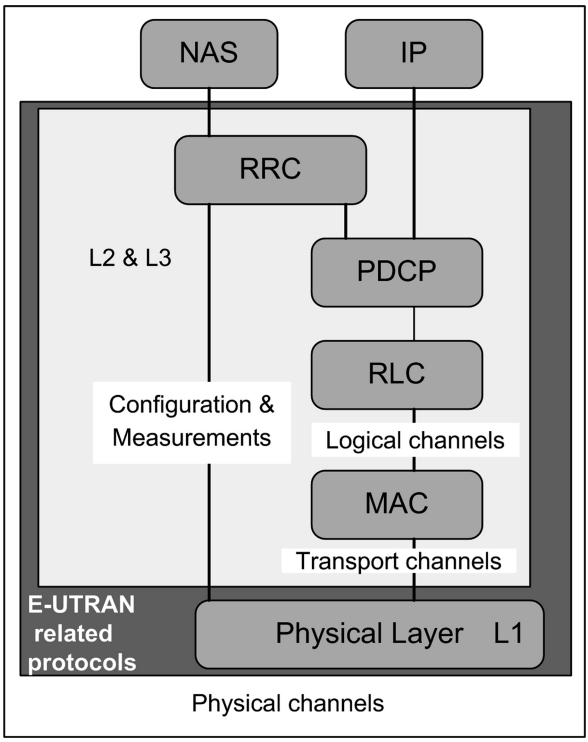


**Fig. 2.3** LTE protocol layers

stack is to set the services to organize the information to transmit through logical channels whose classifying parameter is the nature of the information they carry (i.e., control or traffic information) and map these logical channels into transport channels whose characteristic is how and with what characteristic the information within each logical channel is transmitted over the radio interface. This how and with what characteristic means that for each transport channel there is one or more transport formats associated, each of them defined by the encoding, interleaving bit rate, and mapping onto the physical channel. Each layer is characterized by the services provided to the higher layers or entities and the functions that support them as follows:

- Physical layer: Carries all information from the MAC transport channels over the air interface. Takes care of the link adaptation (AMC), power control, cell search (for initial synchronization and handover purposes), and other measurements (inside the LTE system and between systems) for the RRC layer.
- MAC: The MAC sublayer offers a set of logical channels to the RLC sublayer that it multiplexes into the physical layer transport channels. It also manages the HARQ error correction, handles the prioritization of the logical channels for the same UE and the dynamic scheduling between UEs, etc.

- RLC: It transports the PDCP's PDUs. It can work in three different modes depending on the reliability provided. Depending on this mode it can provide ARQ error correction, segmentation/concatenation of PDUs, reordering for in-sequence delivery, duplicate detection, etc.
- PDCP: For the RRC layer it provides transport of its data with ciphering and integrity protection and for the IP layer transport of the IP packets, with ROHC header compression, ciphering, and depending on the RLC mode in-sequence delivery, duplicate detection, and retransmission of its own SDUs during handover.
- RRC: Between others it takes care of the broadcasted system information related to the access stratum and transport of the Non-Access Stratum (NAS) messages, paging, establishment and release of the RRC connection, security key management, handover, UE measurements related to inter-system (inter-RAT) mobility, QoS, etc.

On the other hand, interfacing layers to the E-UTRAN protocol stack are

- NAS: Protocol between the UE and the MME on the network side (outside of E-UTRAN). Between others performs authentication of the UE and security control and generates part of the paging messages
- IP layer

#### 2.2.1.2 System Architecture Evolution (SAE)

The main component of the SAE architecture is the Evolved Packet Core (EPC) which consists of the following functional elements:

- *Serving Gateway (S-GW)*:
  The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and PDN-GW) [4]. For idle state UEs, the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, e.g., parameters of the IP bearer service and network internal routing information. It also performs replication of the user traffic in case of lawful interception.
- *Mobility Management Entity (MME)*:
  The MME is the key control node for the LTE access network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. It is responsible for authenticating the user. The Non-Access Stratum (NAS) signaling terminates at the MME and it is also responsible for generation and allocation of temporary identities to UEs. It checks the authorization of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE

roaming restrictions. The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management. Lawful interception of signaling is also supported by the MME. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN. Finally, the MME also terminates the S6a interface toward the home HSS for roaming UEs.

- *Packet Data Network Gateway (PDN-GW)*:
  The PDN-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PDN-GW for accessing multiple packet data networks. The PDN-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the PDN-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1x and EV-DO).

Table 2.1 gives the logical functions performed within this architecture. Several functions are defined and each encompasses a number of individual functions (see Fig. 2.4).

### *2.2.2 Reference Points*

The LTE defines a reference point as a conceptual link that connects two groups of functions that reside in different functional entities of the E-UTRAN and EPC. Figure 2.3 shows a number of reference points defined by the 3GPP. These reference points are listed in Table 2.2. Note that these reference points are based on release 8 of the standardization and there may exist more reference points that are dependent on the type of network architecture.

## 2.3 Control and User Planes

The radio interface in LTE is characterized through its protocols where it can be defined by two main groupings according to the final purpose service: the user plane protocols and the control plane protocols. The first carries user data through the access stratum and the second is responsible for controlling the connections between the UE and the network and the radio access bearers. Even though separation of the control plane and the user plane was maybe one of the most important issues of LTE design, full independence of the layers is not feasible because, without interaction between the user plane and the control plane, operators are not able to control QoS, the source/destination of media traffic, and when the media starts and stops.

**Table 2.1** Functional decomposition of the EPS

| EPS entity name | Function |
|---|---|
| eNodeB | Radio resource management<br>IP header compression and encryption of user data stream<br>Selection of an MME at UE attachment when no routing to an MME can be determined<br>Routing of user plane data toward serving gateway<br>Scheduling and transmission of paging messages<br>Scheduling and transmission of broadcast information and measurement and measurement reporting<br>Scheduling and transmission of PWS messages |
| MME | NAS signaling<br>NAS signaling security<br>AS security control<br>Inter-CN node signaling for mobility between 3GPP access networks<br>Idle mode UE reachability<br>Tracking area list management (for UE in idle and active modes)<br>PDN-GW and serving GW selection<br>MME selection for handovers with MME change<br>SGSN selection for handovers to 2G or 3G 3GPP access networks<br>Roaming<br>Authentication<br>Bearer management functions including dedicated bearer establishment<br>Support for PWS message transmission |
| S-GW | The local mobility anchor point for inter-eNodeB handover<br>Mobility anchoring for inter-3GPP mobility<br>E-UTRAN idle mode downlink packet buffering and initiation of network-triggered service request procedure<br>Lawful interception<br>Packet routing and forwarding<br>Transport level packet marking in the uplink and the downlink<br>Accounting on user and QCI granularity for interoperator charging<br>UL and DL charging per UE, PDN, and QCI |
| PDN-GW | Per-user-based packet filtering<br>Lawful interception<br>UE IP address allocation<br>Transport-level packet marking in the downlink<br>UL and DL service-level charging, gating, and rate enforcement |

### *2.3.1 User Plane*

Figure 2.5 shows the user plane protocol stack including the E-UTRAN and the S1 interface of a conventional, i.e., non-self-backhauled, system. The radio access uses the protocols MAC, RLC, and PDCP. The user plane part of the S1 interface is based on the GPRS Tunneling Protocol (GTP), which uses a tunneling mechanism ensuring that IP packets destined to a given UE are delivered to the eNodeB where the UE is currently located. GTP encapsulates the original IP packet into an outer IP packet which is addressed to the proper eNodeB. The S1 interface can be operated

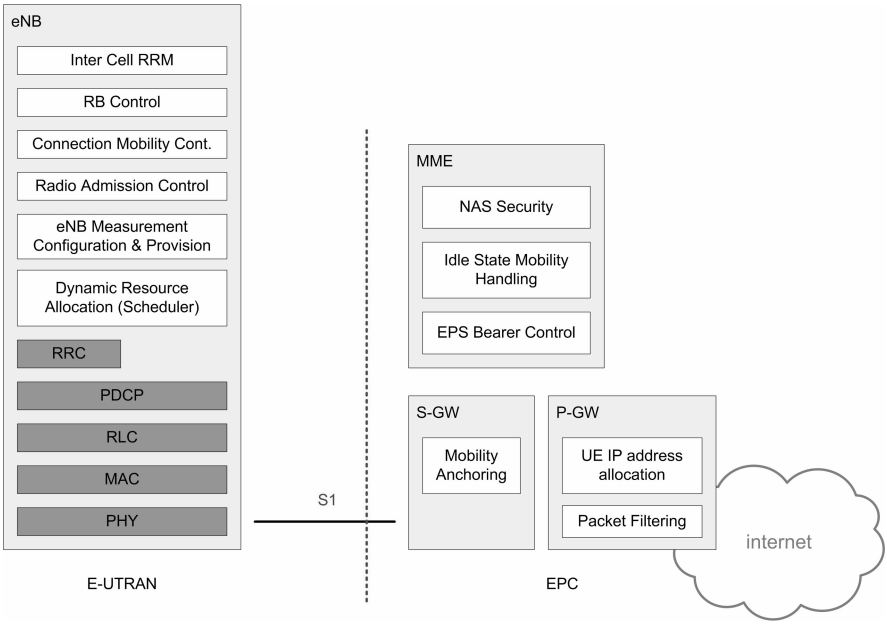


**Fig. 2.4** Functional split between E-UTRAN and EPC

**Table 2.2** LTE reference points

| Reference point | End point | Description |
|---|---|---|
| S1-U | E-UTRAN and S-GW | For the per-bearer user plane tunneling and inter-eNodeB path switching during handover |
| S3 | MME and SGSN | It enables user and bearer information exchange for inter-3GPP access network mobility in idle and/or active state |
| S4 | S-GW and SGSN | It provides related control and mobility support between GPRS core and the 3GPP anchor function of S-GW |
| S5 | S-GW and PDN-GW | It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated PDN-GW for the required PDN connectivity |
| S6a | MME and HSS | It enables transfer of subscription and authentication data for authenticating and authorizing user access between MME and HSS |
| S10 | MME and MME | For MME relocation and MME to MME information transfer |
| S11 | MME and S-GW | |
| S12 | UTRAN and S-GW | For user plane tunneling when direct tunnel is established |
| Gx | PCRF and PDN-GW | It provides transfer of QoS policy and charging rules to Policy and Charging Enforcement Function (PCEF) in the PDN-GW |
| SGi | PDN-GW and PDN | PDN may be an operator – external public or private packet data network or an intra-operator packet data network, e.g., for provision of IMS services |
| Rx | PCRF and PDN | The Rx reference point resides between the AF and the PCRF |

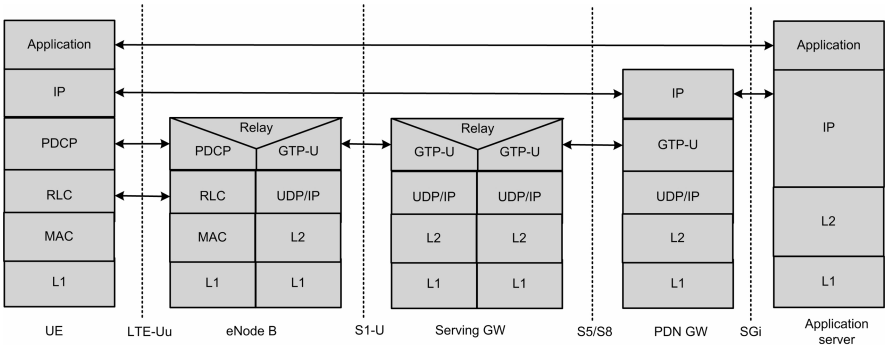


**Fig. 2.5** User plane end-to-end protocol stack

over various Layer 1/Layer 2 technologies, e.g., fiber optic cables, leased (copper) lines, or microwave links.

Figure 2.5 shows also an example TCP/IP-based application, such as web browsing. The corresponding peer entities operate in the UE and at the server hosting the web application. For simplicity, peer protocol entities of the server are drawn in the Serving Gateway (S-GW); however, in general they are located somewhere in the Internet.

All information sent and received by the UE, such as the coded voice in a voice call or the packets in an Internet connection, are transported via the user plane. User plane traffic is processed at different hierarchical levels, from eNodeB up to the core network (EPC). Also, control traffic is strictly tied to the user plane. Irrespective of the reasons behind the current hierarchical architecture, for the transmission backbone it means the higher the level of network hierarchy the greater the amount of accumulated traffic generated. Therefore, higher level network elements will readily become the bottleneck of the network. Therefore, transmission capacity should be fitted to the network hierarchy; at higher levels high-capacity transmission means, such as fiber, are needed, but when it comes to the edge of the network microwave transmission becomes a more flexible and cost-effective substitution, particularly in terms of capacity extending.

#### 2.3.1.1 GPRS Tunneling Protocol (GTP)

GPRS Tunneling Protocol (GTP) is a collection of protocols central to IP mobility management within 3GPP packet core networks (GPRS/UMTS/EPC) comprising of GTP-C, GTP-U, and GTP′ variants. The protocol stack for GTP is as depicted in Fig. 2.6.

GTP-C is the control part of GTP and is used in control plane mechanisms in GPRS, UMTS, and LTE/SAE/EPC networks. GTP-C is standardized as version 0, version 1, and version 2 by 3GPP. All the GTP-C versions use UDP as transport protocol. GTP v2 offers fallback to GTP v1 via the earlier “Version Not Supported” mechanism but explicitly offers no support for fallback to GTP v0.

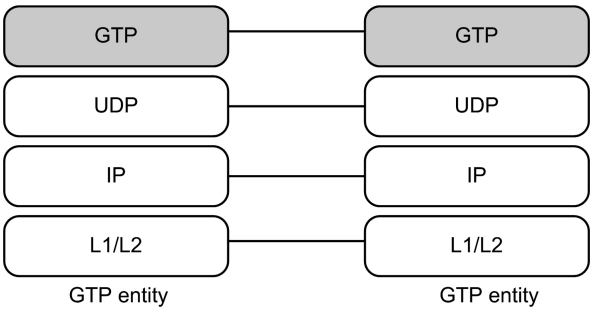


**Fig. 2.6** GTP stack

GTP-U is the bearer part of GTP and is used in user plane mechanisms in GPRS, UMTS, and LTE networks. GTP-U is standardized as version 0 and version 1 by 3GPP. All the GTP-U versions use UDP as transport protocol. GTP′ or GTP Prime is used for interfacing with CGF in GPRS and UMTS networks. LTE MME, S-GW, and PDN Gateway nodes use GTP-C for control plane signaling on S11/S5 interfaces, while S-GW and PDN-GW nodes use GTP-U for user plane on S1-U and S5 interfaces primarily. LTE/SAE/EPC network uses only GTP version 2 also known as evolved GTP unless backward compatible to 3G UMTS/HSPA networks.

After the downlink path is switched at the S-GW downlink packets on the forwarding path and on the new direct path may arrive interchanged at the target eNodeB. The target eNodeB should first deliver all forwarded packets to the UE before delivering any of the packets received on the new direct path. The method employed in the target eNodeB to enforce the correct delivery order of packets is outside the scope of the standard.

In order to assist the reordering function in the target eNodeB, the S-GW shall send one or more "end marker" packets on the old path immediately after switching the path for each UE. The "end marker" packet shall not contain user data. The "end marker" is indicated in the GTP header. After completing the sending of the tagged packets the GW shall not send any further user data packets via the old path. Upon receiving the "end marker" packets, the source eNodeB shall, if forwarding is activated for that bearer, forward the packet toward the target eNodeB.

On detection of an "end marker" the target eNodeB shall discard the end marker packet and initiate any necessary processing to maintain in-sequence delivery of user data forwarded over X2 interface and user data received from the S-GW over S1 as a result of the path switch. On detection of the "end marker," the target eNodeB may also initiate the release of the data forwarding resource (see Fig. 2.7).

### *2.3.2 Control Plane*

The control plane protocol function is to control the radio access bearers and the connection between the UE and the network, i.e., signaling between E-UTRAN and EPC (Fig. 2.8). The control plane consists of protocols for control and support of the user plane functions:

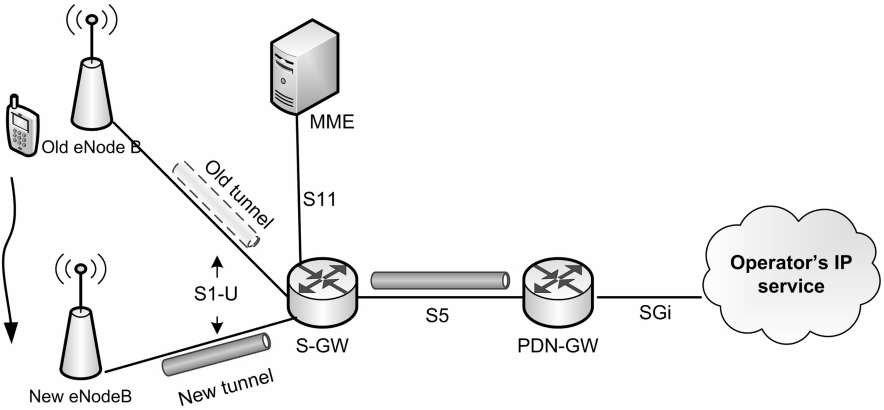


**Fig. 2.7** GTP tunneling

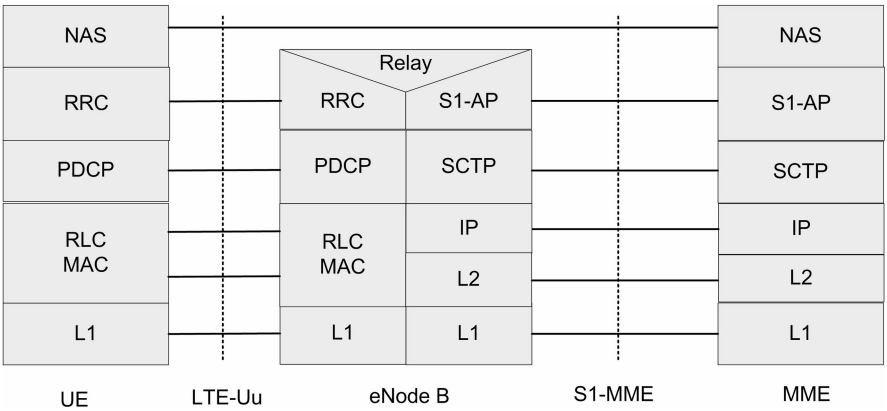


**Fig. 2.8** Control plane end-to-end protocol stack

- controlling the E-UTRAN network access connections, such as attaching to and detaching from E-UTRAN;
- controlling the attributes of an established network access connection, such as activation of an IP address;
- controlling the routing path of an established network connection in order to support user mobility;
- controlling the assignment of network resources to meet changing user demands.

In the control plane, the NAS protocol, which runs the MME and the UE, is used for control purposes such as network attach, authentication, setting up of bearers, and mobility management. All NAS messages are ciphered and integrity protected by the MME and UE. The Radio Resource Control (RRC) layer in the eNodeB makes handover decisions based on neighbor cell measurements sent by the UE, pages for the UEs over the air, broadcasts system information, controls UE measurement

reporting such as the periodicity of Channel Quality Information (CQI) reports, and allocates cell-level temporary identifiers to active UEs. It also executes transfer of UE context from the source eNodeB to the target eNodeB during handover and does integrity protection of RRC messages. The RRC layer is responsible for the setting up and maintenance of radio bearers.

### 2.3.3 X2 Interface in User and Control Planes

The X2 user plane interface (X2-U) is defined between eNodeBs. The X2-U interface provides non-guaranteed delivery of user plane PDUs. The user plane protocol stack on the X2 interface is shown in Fig. 2.9a. The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs.

The X2 control plane interface (X2-CP) is defined between two neighbor eNodeBs. The control plane protocol stack of the X2 interface is shown in Fig. 2.9b. The transport network layer is built on Stream Control Transmission Protocol (SCTP) on top of IP. The application layer signaling protocol is referred to as X2-AP (X2 Application Protocol).

### 2.3.4 S1 Interface in User and Control Planes

The S1 user plane interface (S1-U) is defined between the eNodeB and the S-GW. The S1-U interface provides non-guaranteed delivery of user plane PDUs between the eNodeB and the S-GW. The user plane protocol stack on the S1 interface is shown in Fig. 2.10a. The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the eNodeB and the S-GW.

The S1 control plane interface (S1-MME) is defined between the eNodeB and the MME. The control plane protocol stack of the S1 interface is shown in Fig. 2.10b. The transport network layer is built on IP transport, similarly to the user plane,

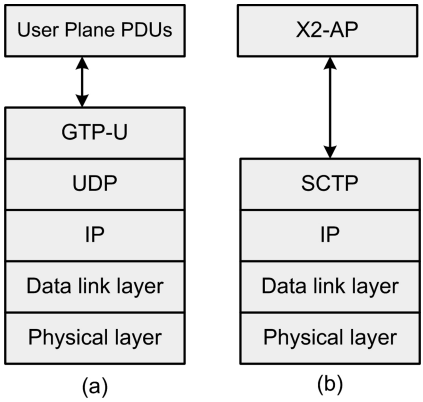


**Fig. 2.9** (**a**) X2 interface in user plane, (**b**) X2 interface in control plane

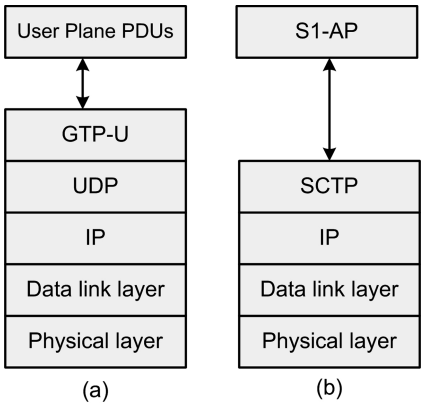


**Fig. 2.10** (**a**) S1 interface in user plane, (**b**) S1 interface in control plane

but for the reliable transport of signaling messages SCTP is added on top of IP. The application layer signaling protocol is referred to as S1-AP (S1 Application Protocol).

## 2.4 Multimedia Broadcast and Multicast Service (MBSM)

MBMS is a point-to-multipoint service in which data is transmitted from a single source to multiple destinations over radio network. Transmitting the same data to multiple recipients allows network resources to be shared. MBMS is realized by addition of existing and new functional entities of the 3GPP architecture [5].

MBMS in real provides two different services: (i) broadcast and (ii) multicast. The broadcast service can be received by any subscriber located in the area in which the service is offered and multicast services can only be received by users having subscribed to the service and having joined the multicast group associated with the service. Both services are unidirectional point-to-multipoint transmissions of multimedia data and can be highly applied to broadcast text, audio, picture, video from Broadcast Multicast Service Center to any user located in the service area. For such a service, only the broadcast service providers can be charged possibly based on the amount of data broadcasted, size of service area, or broadcast service duration. Multicast is subject to service subscription and requires the end user to explicitly join the group in order to receive the service. Because it is subject to subscription, the multicast service allows the operator to set specific user charging rules for this service [4].

### *2.4.1 MBMS Service Architecture*

The MBMS service architecture is based on the packet core domain and is compatible with EPS, as well as 2G/GSM or 3G UMTS packet core nodes like the SGSN and

GGSN. In EPS networks, there are two additional logical network entities: MCE, MBMS GW.

1. The Multi-cell/multicast Coordination Entity (MCE) is a new logical entity, responsible for allocation of time and frequency resources for multi-cell MBMS transmission. The MCE actually does the scheduling on the radio interface. The MCE is a logical node which may be integrated as part of the eNodeB (in which case, the M2 interface becomes an internal eNodeB interface).
2. The MBMS Gateway (MBMS GW) is a logical entity – this does not preclude the possibility that it may be part of another network element – that is present between the BMSC and eNodeBs whose principal function is the sending/broadcasting of MBMS packets to each eNodeB transmitting the service. The MBMS GW uses IP Multicast as the means of forwarding MBMS user data to the eNodeB. The MBMS GW performs MBMS Session Control Signaling (session start/stop) toward the E-UTRAN via MME.
3. The M1 interface, associated with the MBMS data (or user plane), makes use of IP multicast protocol for the delivery of packets to eNodeBs.
4. The M2 interface is used by the MCE to provide the eNodeB with radio configuration data.
5. The M3 interface supports the MBMS session control signaling, e.g., for session initiation and termination.

## *2.4.2 MBMS Service Deployment*

LTE is quite flexible and offers many possible options for MBMS service deployment. In MBMS, the operator has the possibility of reserving a frequency layer to MBMS transmissions. In this case, the cells belonging to this layer only offer MBMS service. In those dedicated cells, there is no support for unicast (or point-to-point) service. In contrast, when no specific frequency is reserved for MBMS, mixed cells provide simultaneous unicast and MBMS services [6]. In parallel, there may be two types of MBMS data transmission in LTE: (i) single-cell transmission – in this case, MBMS data is only provided and available over the coverage of one single cell. (ii) Multi-cell transmission – in this case, the MBMS data sent in the different cells is tightly synchronized. This allows the receiving terminal to recombine the signals received from various cells and improve the signal-to-noise ratio, as compared with conventional point-to-multipoint transmission.

### 2.4.2.1 MBMS on Single Frequency Network

The MBMS that is going to be used in LTE is called as Evolved MBMS (E-MBMS) and it is considered as an important component in the EPS architecture (Fig. 2.11). MBMS should be supported in paired or unpaired spectrum. E-MBMS provides a transport feature to send the same content information to a given set of users in a cell to all the users (broadcast) or to a given set of users (multicast) for which a notion

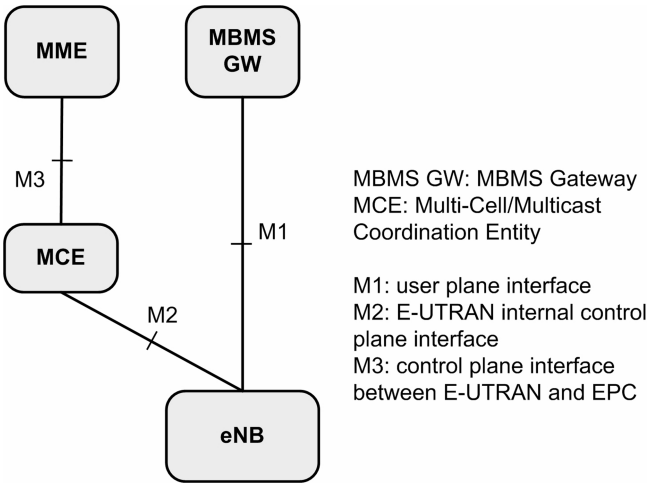


**Fig. 2.11** E-MBMS logical architecture

of subscription applies in order to restrict the multicast services to a given set of users [7].

As EPS is based on Flat IP architecture, and we have already IP multicast feature available, how can a end user visualize this on EPS? it is thus very important to not mix up IP multicast with MBMS. In IP multicast there is no sharing of a given radio resource in between the user as it is purely a way of duplication of IP packets on some routers on the network [8].

E-MBMS (which is the evolved version of the legacy MBMS system) will be using some MIMO open loop scheme. In E-MBMS, there will be single (single-cell broadcast) or multiple transmitting eNodeBs and multiple receiving UEs. E-MBMS is a good application to demonstrate what MIMO can bring to the system. Indeed, in the case of broadcast of the same signal on the same frequency band the transmission power has to be chosen so that the far mobiles should receive the signal with good quality. To reduce the required power, increasing the number of transmit and receive antennas is a good solution [9]. MIMO options, like spatial multiplexing, are possible in the MBMS context.

In E-UTRAN, MBMS transmissions may be performed as single-cell transmissions or as multi-cell transmissions. In the case of multi-cell transmission, the cells and content are synchronized to enable for the terminal to soft-combine the energy from multiple transmissions. The superimposed signal looks like multipath to the terminal. This concept is also known as Single Frequency Network (SFN). The E-UTRAN can configure which cells are parts of an SFN for transmission of an MBMS service. A MBMS Single Frequency Network is called a MBSFN. MBSFN is envisaged for delivering services such as mobile TV using the LTE infrastructure and is expected to be a competitor to DVB-H-based TV broadcasts.

In MBSFN, the transmission happens from a time-synchronized set of eNodeBs using the same resource block (Fig. 2.12). The Cyclic Prefix (CP) used for MBSFN

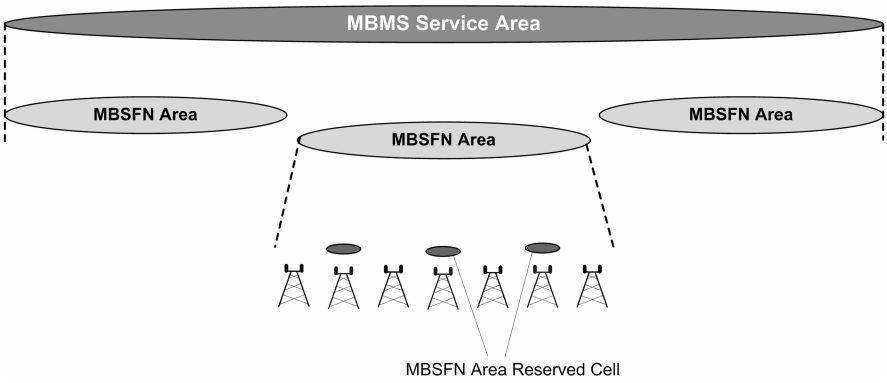


**Fig. 2.12** MBSFN visualization

is slightly longer, and this enables the UE to combine transmissions from different eNodeBs located far away from each other, thus somewhat negating some of the advantages of SFN operation [10].

## 2.5 Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) is a Transport Layer protocol, serving in a similar role to the popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. SCTP is used in LTE to ensure reliable, in-sequence transport of messages.

LTE uses SCTP, which we view as a layer between the SCTP user application and an unreliable end-to-end datagram service such as UDP. Thus, the main function of SCTP amounts to reliable transfer of user datagrams between peer SCTP users. It performs this service within the context of an association between SCTP nodes, where APIs exist at the boundaries. SCTP has connection-oriented characteristics but with broad concept. It provides means for each SCTP endpoint to provide the other during association startup with a list of transport addresses (e.g., address/UDP port combinations) by which that endpoint can be reached and from which it will originate messages. The association carries transfers over all possible source/destination combinations, which may be generated from two end lists. As result SCTP offers the following services:

- application-level segmentation;
- acknowledged error-free non-duplicated transfer of user data;
- sequenced delivery of user datagrams within multiple streams;
- enhanced reliability through support of multi-homing at either or both ends of the association;
- optional multiplexing of user datagram into SCTP datagrams.

SCTP assumes that it is running over an IPv4 or IPv6 network. Even more importantly, it assumes it is running over a well-engineered IP network. This, in practice, means that there is a diverse routing network underneath so as to avoid a single point of failure. In LTE, SCTP handles the communications between the eNodeB and the MME. This communication connection is very important and fragile since it must be able to detect dropouts very quickly. TCP does not do this, whereas SCTP detects that immediately and recognizes when a packet is dropped or a link goes down. LTE providers specifically and telecom networks in general need this ability to insure a high quality of service.

Additionally SCTP has, as a default, "selective ACK," which is optional in TCP. What this means is that a packet will *never* be resent if it has already been acknowledged as sent. In the LTE world, where every bit counts, using SCTP means no wasted data. The purpose of the use of SCTP in LTE is to provide a robust and reliable signaling bearer. To achieve this, SCTP provides appropriate congestion control procedures, fast retransmit in the case of message loss, and enhanced reliability. It also provides additional security against blind attacks and will be used to increase security in connecting the LTE networks of different operators.

## 2.6 Network Discovery and Selection

The Dynamic Host Control Protocol (DHCP) is used as the primary mechanism to allocate a dynamic Point-of-Attachment (PoA) IP address to the UE. Note that the EPS bearer supports dual-stack IP addressing, meaning that it is able to transport both native IPv4 and native IPv6 packets. In order to support DHCP-based IP address configuration (both version IPv4 and IPv6), the PDN-GW shall act as the DHCP server for HPLMN-assigned dynamic and static and VPLMN-assigned dynamic IP addressing. When DHCP is used for external PDN-assigned addressing and parameter configuration, the PDN GW shall act as the DHCP server toward the UE and it shall act as the DHCP client toward the external DHCP server. The serving GW does not have any DHCP functionality. It forwards all packets to and from the UE including DHCP packets as normal.

In the case of IPv6 address allocation mechanism, the IPv6 Stateless Address autoconfiguration is the basic mechanism to allocate /64 IPv6 prefix to the UE. Alternatively shorter than /64 IPv6 prefix delegation via DHCPv6, RFC 3633 [11] may be provided, if it is supported by the PDN-GW. When DHCPv6 prefix delegation is not supported the UE should use stateless address autoconfiguration RFC 4862 [12].

## 2.7 Radio Resource Management

The purpose of Radio Resource Management (RRM) is to ensure the efficient use of the available radio resources and to provide mechanisms that enable E-UTRAN to meet radio resource-related requirements like (i) enhanced support for

end-to-end QoS, (ii) efficient support for transmission of higher layers and (iii) support of load sharing and policy management across different radio access technologies. In particular, RRM in E-UTRAN provides means to manage (e.g., assign, re-assign, and release) radio resources taking into account single- and multi-cell aspects. The RRM functions are represented by the following aspects.

### *2.7.1 Radio Bearer Control (RBC)*

The establishment, maintenance, and release of radio bearers involve the configuration of radio resources associated with them. When setting up a radio bearer for a service, Radio Bearer Control (RBC) takes into account the overall resource situation in E-UTRAN, the QoS requirements of in-progress sessions, and the QoS requirement for the new service. RBC is also concerned with the maintenance of radio bearers of in-progress sessions at the change of the radio resource situation due to mobility or other reasons. RBC is involved in the release of radio resources associated with radio bearers at session termination, handover, or at other occasions. RBC is located in the eNodeB.

### *2.7.2 Connection Mobility Control (CMC)*

Connection Mobility Control (CMC) is concerned with the management of radio resources in connection with idle or connected mode mobility. In idle mode, the cell reselection algorithms are controlled by setting of parameters (thresholds and hysteresis values) that define the best cell and/or determine when the UE should select a new cell. Also, E-UTRAN broadcasts parameters that configure the UE measurement and reporting procedures. In connected mode, the mobility of radio connections has to be supported. Handover decisions may be based on UE and eNodeB measurements. In addition, handover decisions may take other inputs, such as neighbor cell load, traffic distribution, transport, and hardware resources, and operator-defined policies into account. CMC is located in the eNodeB.

### *2.7.3 Dynamic Resource Allocation (DRA) – Packet Scheduling (PS)*

The task of Dynamic Resource Allocation (DRA) or Packet Scheduling (PS) is to allocate and de-allocate resources (including buffer and processing resources and resource blocks (i.e., chunks)) to user and control plane packets. DRA involves several sub-tasks, including the selection of radio bearers whose packets are to be scheduled and managing the necessary resources (e.g., the power levels or the specific resource blocks used). PS typically takes into account the QoS requirements associated with the radio bearers, the channel quality information for UEs, buffer

status, interference situation, etc. DRA may also take into account restrictions or preferences on some of the available resource blocks or resource block sets due to inter-cell interference coordination considerations. DRA is located in the eNodeB.

### 2.7.4 Inter-cell Interference Coordination (ICIC)

Inter-Cell Interference Coordination (ICIC) has the task to manage radio resources (notably the radio resource blocks) such that inter-cell interference is kept under control. ICIC is inherently a multi-cell RRM function that needs to take into account information (e.g., the resource usage status and traffic load situation) from multiple cells. The preferred ICIC method may be different in the uplink and downlink. ICIC is located in the eNodeB.

### 2.7.5 Load Balancing (LB)

Load Balancing (LB) has the task to handle uneven distribution of the traffic load over multiple cells. The purpose of LB is thus to influence the load distribution in such a manner that radio resources remain highly utilized and the QoS of in-progress sessions is maintained to the extent possible and call dropping probabilities are kept sufficiently small. LB algorithms may result in handover or cell reselection decisions with the purpose of redistributing traffic from highly loaded cells to underutilized cells. LB is located in the eNodeB.

### 2.7.6 Inter-RAT Radio Resource Management

Inter-RAT RRM is primarily concerned with the management of radio resources in connection with inter-RAT mobility, notably inter-RAT handover. At inter-RAT handover, the handover decision may take into account the involved RAT resource situation as well as UE capabilities and operator policies. The importance of inter-RAT RRM may depend on the specific scenario in which E-UTRAN is deployed. Inter-RAT RRM may also include functionality for inter-RAT load balancing for idle and connected mode UEs.

### 2.7.7 Subscriber Profile ID for RAT/Frequency Priority

The RRM strategy in E-UTRAN may be based on user-specific information. The Subscriber Profile ID for RAT/Frequency Priority (SPID) parameter received by the eNodeB via the S1 interface is an index referring to user information (e.g., mobility profile and service usage profile). The information is UE specific and applies to all its radio bearers. This index is mapped by the eNodeB to locally defined

configuration in order to apply specific RRM strategies (e.g., to define RRC_IDLE mode priorities and control inter-RAT/inter-frequency handover in RRC_CONNECTED mode).

## 2.8 Authentication and Authorization

The trust model in LTE (Fig. 2.13) is similar to that of UMTS. It can roughly be described as a secure core network while radio access nodes and interfaces between the core network and the radio access nodes are vulnerable to attack. The system architecture for LTE is flatter than that of UMTS, having no node that corresponds to the Radio Network Controller (RNC) in UMTS. Therefore, the UE user plane security must be terminated either in the LTE eNodeB or in a core network node. For reasons of efficiency, it has been terminated in the eNodeB. However, because eNodeBs and backhaul links might be deployed in locations that are vulnerable to attacks, some new security mechanisms have been added. Security over the LTE air interface is provided through strong cryptographic techniques. The backhaul link from the eNodeB to the core network makes use of Internet Key Exchange (IKE) and the IP Security Protocol (IPsec) when cryptographic protection is needed. Strong

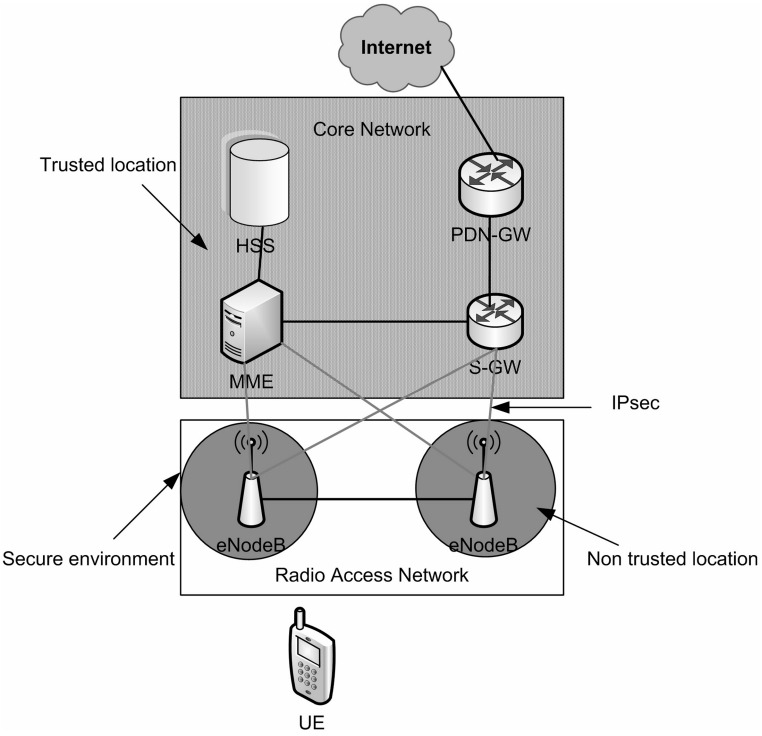


**Fig. 2.13** LTE trusted model

cryptographic techniques provide end-to-end protection for signaling between the core network and UE. Therefore, the main location where user traffic is threatened by exposure is in the eNodeB. Moreover, to minimize susceptibility to attacks, the eNodeB needs to provide a secure environment that supports the execution of sensitive operations, such as the encryption or decryption of user data and the storage of sensitive data like keys for securing UE communication, long-term cryptographic secrets, and vital configuration data. Likewise, the use of sensitive data must be confined to this secure environment. Even with the above security measures in place, one must consider attacks on an eNodeB, because, if successful, they could give attackers full control of the eNodeB and its signaling to UEs and other nodes. To limit the effect of a successful attack on one eNodeB, attackers must not be able to intercept or manipulate user and signaling plane traffic that traverses another eNodeB – for example, after handover.

### *2.8.1 User Authentication, Key Agreement, and Key Generation*

The subscriber-authentication function in LTE/3GPP Evolved Packet System (EPS) is based on the UMTS Authentication and Key Agreement (UMTS AKA) protocol. It provides mutual authentication between the UE and core network, ensuring robust charging and guaranteeing that no fraudulent entities can pose as a valid network node. Note that GSM Subscriber Identity Modules (SIMs) are not allowed in LTE because they do not provide adequate security.

EPS AKA provides a root key from which a key hierarchy is derived. The keys in this hierarchy are used to protect signaling and user plane traffic between the UE and network. The key hierarchy is derived using cryptographic functions. For example, if key2 and key3 (used in two different eNodeBs) are keys derived from key1 by a mobility management entity (MME), an attacker who gets hold of, say, key2, still cannot deduce key3 or key1, which is on a higher layer in the key hierarchy. Furthermore, keys are bound to where, how, and for which purpose they are used. This ensures, for example, that keys used for one access network cannot be used in another access network, and that the same key is not used for multiple purposes or with different algorithms. Because GSM does not have this feature, attackers who can break one algorithm in GSM can also compromise the offered security when other algorithms use the same key. Further, the key hierarchy and bindings also make it possible to routinely and efficiently change the keys used between a UE and eNodeBs (for example, during handover) without changing the root key or the keys used to protect signaling between the UE and core network.

### *2.8.2 Signaling and User-Plane Security*

For radio-specific signaling, LTE provides integrity, replay protection, and encryption between the UE and eNodeB. IKE/IPsec can protect the backhaul

signaling between the eNodeB and MME. In addition, LTE-specific protocols provide end-to-end protection of signaling between the MME and UE. For user-plane traffic, IKE/IPsec can similarly protect the backhaul from the eNodeB to the serving gateway (S-GW). Support for integrity, replay protection, and encryption is mandatory in the eNodeB. The user-plane traffic between the UE and eNodeB is only protected by encryption as integrity protection would result in expensive bandwidth overhead. Notwithstanding, it is not possible to intelligently inject traffic on behalf of another user: attackers are essentially blind in the sense that any traffic they try to inject would almost certainly decrypt to garbage.

## 2.9 Summary and Conclusions

We described previously the overall EPS network architecture, giving an overview of the functions provided by the core network and E-UTRAN. The protocol stack across the different interfaces is explained, along with an overview of the functions provided by the different protocol layers. The end-to-end bearer path along with QoS aspects are also discussed, including a typical procedure for establishing a bearer. The remainder of this chapter presents the network interfaces in detail, with particular focus on the E-UTRAN interfaces and the procedures used across these interfaces, including those for the support of user mobility.

It has been seen that LTE architecture is designed to be simple to deploy and operate, through flexible technology that can be deployed in a wide variety of frequency bands. The LTE/SAE architecture reduces the number of nodes, supports flexible network configurations, and provides a high level of service availability. In parallel with the LTE radio access, packet core networks are also evolving to the SAE architecture. This new architecture is designed to optimize network performance, improve cost efficiency, and facilitate the uptake of mass market IP-based services.

## References

1. 3GPP TR 25.913: Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (EUTRAN).
2. Motorola, Long Term Evolution (LTE): A Technical Overview, Technical White Paper.
3. 3GPP TS 24.301: Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS): Stage 3.
4. 3GPP TS 22.246: Multimedia Broadcast/Multicast Service (MBMS) User Services: Stage 1.
5. 3GPP TS 22.146: Multimedia Broadcast/Multicast Service (MBMS): Stage 1.
6. 3GPP TS 23.246: Multimedia Broadcast/Multicast Service (MBMS): Architecture and Functional Description.
7. 3GPP TS 26.346: Multimedia Broadcast/Multicast Service (MBMS): Protocols and Codecs.
8. 3GPP TS 33.246: 3G Security: Security of Multimedia Broadcast/Multicast Service (MBMS).
9. 3GPP TS 32.273: Multimedia Broadcast and Multicast Service (MBMS) Charging.

10. 3GPP TS 36.440: General Aspects and Principles for Interfaces Supporting Multimedia Broadcast Multicast Service (MBMS) within E-UTRAN.
11. IETF RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.
12. IETF RFC 462: IPv6 Stateless Address Autoconfiguration.

http://www.springer.com/978-1-4419-6456-4

Understanding LTE and its Performance

Ali-Yahiya, T.

2011, XXV, 250 p., Hardcover
ISBN: 978-1-4419-6456-4