2. REVIEW OF LITERATURE

2.1 INTRODUCTION

This chapter introduces the evolution of wireless communication procedures and the different type of architectures. This also briefly discusses about the handover mechanisms adapted in the different types of wireless communication network over the different period of time. The advances in handover mechanism and the corresponding review are discussed in the following chapters.

2.2 WIRELESS COMMUNICATION

Electromagnetic wave was discovered during 19th century, as the communication media. The communication through public mobile telephone began after the World War II. In 1948 the fully automated mobile telephone service began operating. In 1969 the frequency reuse technology was introduced by Bell System in a small zone. The introduction of VLSI (Very-Large-Scale Integration) technology made low-power application of signal processing algorithms and coding techniques to progress rapidly [5][6]. This lead to huge interest among people towards wireless connectivity, which paved the path for more research activities in wireless communication technology.

In wireless network, high frequency radio waves are used instead of wires. There are two types of wireless networks namely Infrastructure-less and infrastructure-based wireless network. Infrastructure-less wireless network, otherwise known as peer-to-peer or ad-hoc network [7] is again classified into two classes as Mobile Ad-hoc Network (MANET) and Wireless Sensor Network (WSN). In Infrastructure-less wireless network, the MNs are connected with wireless links and without using pre-existing communication infrastructure or central control. It is an autonomous system [8].
In infrastructure-based wireless network the Access Point (AP) or BS acts like a hub, providing connectivity for the wireless devices. The AP or BS provides the way to access the MN to the backbone wired network. The Network control functions are performed by the BSs. BS coordination in infrastructure-based networks provide a centralized control mechanism for transmission scheduling, dynamic resource allocation, power control, and handoff. The cellular phone systems, wireless LANs, and paging systems are some of the examples of infrastructure-based wireless networks [9].

2.3 THE GENERATIONS OF CELLULAR PHONE SYSTEMS

Since last few decades cellular phone system has faced several generations of evolution and revolutions namely zero to 4G which are discussed below in some detail.

2.3.1 Zero Generation (0G)

Zero generation refers to pre-cellular mobile telephony technology in 1970s. These mobile telephones were usually mounted in cars or trucks, later briefcase models were also introduced. Technologies used in 0G systems included PTT (Push to Talk), MTS (Mobile Telephone System), IMTS (Improved Mobile Telephone Service), AMTS (Advanced Mobile Telephone System), OLT (Norwegian abbreviation - Offentlig Landmobile Telefoni, meaning - Public Land Mobile Telephony) and MTD (Swedish abbreviation - Mobiltelefoni system D, meaning - Mobile telephony system D)[10]. The handover feature is not available with 0G [11].

2.3.2 First Generation (1G)

In first generation, the analog cellular mobile communication was used which was in use till 1990s for some government and very few industries, all over the world [12]. The first generation mobile communication Nordic Mobile Telephone (NMT) System was developed in Europe in 1981
Advanced Mobile Phone System (AMPS) was deployed in U.S. cellular telephone system in 1983, TACS (Total Access Communication System) was deployed in England in 1982 [14]. The foremost technology used in 1G was Frequency Division Multiple Access (FDMA) [15].

2.3.2.1 Architecture of 1G

Figure 2.1 shows the architecture of 1G wireless communication system. The MN refers to cell phones. MN is usually connected with any one of the BS at a time. Antennas available inside BS consist of transmitter/receiver. BSs are connected with first level Mobile Telephone Switching Office (MTSO). The first level MTSO is connected with second level MTSO. MTSO is in turn connected with Public Switched Telephone Network (PSTN) [16].
2.3.2.2 Handover

Each mobile device is assigned with a Mobile Identity Number (MIN) which includes area code, exchange number and subscriber identity number. Each mobile device also has a permanent electronic serial number assigned by manufacturer to secure the mobile device. The control channels, forward and reverse channel are used to initiate the call and to initiate handover process [17].

In handover, the BS measures the signal strength from the MN and passes it to the second level MTSO through first level MTSO. When the signal strength falls below the threshold value, the nearby BSs also measure the signal strength and inform it to MTSO. Among the neighbouring BSs MTSO allots BS which has best signal strength as the new BS to MN. The second MTSO instruct the new BS to allocate a channel for MN. The new BS allocates a channel and then the channel information is given to second MTSO. The second MTSO generates the handover instruction and sends it over the FOCC (Forward Control Channel) to MN through existing BS. The handover instruction has the information of new channel to be used along with SAT (Supervisory Audio Tone). The MN receives the FOCC. After 50ms the MN sends a signaling tone as acknowledgement to existing BS. MN retunes to the new channel from the existing channel and transmits the SAT to new BS for confirmation of new channel establishment. When the new BS receives this information, it forwards this to second MTSO, thereby handover gets completed. Then the Second MTSO informs existing BS to release the previous channel for further usage. The sequence of handover steps are given in Figure 2.2. The voice path is then re-routed via new BS. The operation of first generation cellular system was closed before 2007 due to poor voice quality, no security, limited capacity and poor handover reliability.
2.3.3  Second Generation (2G)

Digital modulation formats were introduced in 2G networks. In second generation, Time Division Multiple Access (TDMA)/ Frequency Division Duplexing (FDD) [18] and CDMA/FDD (Code Division Multiple Access/ Frequency Division Duplexing) [19] were introduced. GSM (Global System for Mobile Communication) utilizes TDMA with FDD variation. GSM was the first fully digital system using the 900 MHz frequency band. GSM became popular very quickly because it provided better speech quality and, through a uniform international standard, made it possible to use a single telephone number and mobile device around the world. The European Telecommunications Standardization Institute (ETSI) adopted the GSM standard in 1991, and GSM is now used in 140 countries [20]. IS-136 (Interim standard 136) is used in North America and PDC (Pacific Digital Cellular) in
Japan. Interim Standard 95 (IS-95) is also a North American digital cellular standard based on CDMA/FDD technology. It is also known as CDMAOne (Code Division Multiple Access One) or TIA (Telecommunication Industry Associations)-EIA (Electronic Industries Alliance)-95 [21].

According to market data supplied by the GSM Association, which promotes GSM worldwide, about 80% of the global mobile market uses this GSM standard. The user had the ability to roam worldwide with the certainty of being able to operate on GSM networks in exactly the same way with proper billing agreement which lead to major success of the GSM standard.

2.3.3.1 GSM Architecture

The GSM architecture is given in Figure 2.3. GSM consists of various components like MN, Base Transceiver Station (BTS), BSC, MSC, Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AuC) and Equipment Identity Register (EIR)[22]. A MN is a communication device with varied capabilities, communication and computing, which can move freely keeping the communication on. The MN is connected to the one of the nearby BTS with high signal strength and considerable range. BTS is a piece of equipment that facilitates the wireless communication between MN and the network. The BTS mainly consists of transmitter, receiver equipment and few components for signal and protocol processing. The BTS regularly broadcast its own identification numbers as Location Area Identifier (LAI), Cell Identifier (CI) and Base Transceiver Station Identity code (BTS - Id) through Broadcast Control Channel (BCCH) so as to introduce it to the new MNs [22]. BTS is connected with BSC. The control and protocol intelligence required for channel allocation, channel management and handover management are managed by BSC. The functions of BSC include radio network management (such as radio frequency control), BTS handover management and call setup. Both BTS and BSC form the Base Station Subsystem (BSS). BSC is connected with a switch called the MSC and all the MNs are routed through MSC [23]. The MSC performs all of the switching functions such as path search, data
forwarding and service feature processing of a switching node in a fixed telephone network. Since the MSC also considers the allocation and administration of radio resources and the mobility of the users, it has to provide additional functions for location registration of users and the handover of a connection in the case of changing from cell to cell (within the MSC). MSC has HLR, VLR, EIR and AuC. MN registration is done by VLR and HLR whereas authentication is done by AuC and EIR checks the validity with the IMEI. The four databases namely HLR, VLR, AuC, EIR along with MSC constitute Network and Switching Subsystems (NSS). Both BSS and NSS combine together, to form Operations Support Subsystem (OSS). Subscriber Identity Module (SIM) has the information about International Mobile Subscriber Identity (IMSI) number which is used to provide the MN home address. Whenever MN enters into a new network, the Temporary Mobile Subscriber Identity (TMSI) is assigned by the new network, like Care of Address (CoA) [24][25][26].

![GSM Architecture](image)

**Figure 2.3: GSM Architecture**

During a connection MN operates either Traffic Channel (TCH) or Stand-alone Dedicated Control Channel (SDCCH). The TCH is used for user payload data transmission. But it does not carry control information. SDCCH
is especially applied for call setup, authentication, ciphering location update and Short Message Service (SMS). Received Signal Level (RXLEV) and the Received Signal Quality (RXQUAL) are the two parameters to describe the quality of existing TCH/SDCCH channel. RXLEV is measured in decibel-milliwatts (dBm). RXLEV threshold values for handover initiation (varies with respect to MN) and termination (about -110 dBm) should be chosen accurately for proper handover process. Handover termination belongs to final signal level of existing BTS, i.e., thereafter there is no communication with existing BTS. RXQUAL measured as Bit Error Rate (BER) in percent before error correction. Table 2.1 shows the measurement range of BER. RXQUAL_0 level indicates zero level BER whereas RXQUAL_7 corresponds to seventh level (from 12.8% BER), in which signal cannot be filtered. RXQUAL threshold level for handover initiation varies from one MN to other, which mainly depends on transceiver quality.

<table>
<thead>
<tr>
<th>RXQUAL Level</th>
<th>Bit error rate in percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From</td>
</tr>
<tr>
<td>RXQUAL_0</td>
<td>-</td>
</tr>
<tr>
<td>RXQUAL_1</td>
<td>0.2</td>
</tr>
<tr>
<td>RXQUAL_2</td>
<td>0.4</td>
</tr>
<tr>
<td>RXQUAL_3</td>
<td>0.8</td>
</tr>
<tr>
<td>RXQUAL_4</td>
<td>1.6</td>
</tr>
<tr>
<td>RXQUAL_5</td>
<td>3.2</td>
</tr>
<tr>
<td>RXQUAL_6</td>
<td>6.4</td>
</tr>
<tr>
<td>RXQUAL_7</td>
<td>12.8</td>
</tr>
</tbody>
</table>

If RXLEV or RXQUAL is below the initial threshold value, then MN reads the BCCH channel of all the neighboring BTS. The BTS regularly broadcast for every 480ms its own identification numbers as LAI, CI and Base transceiver Station Identity Code (BSIC) through BCCH. The LAI is
hierarchically assigned to each BS by the mobile network. This LAI is used for location updation of MN. Format of LAI structure is given in Figure 2.4. LAI consist a three digit Country Code (CC), two digits Mobile Network Code (MNC) and a five digits or a maximum of $2 \times 8$ bits Location Area Code (LAC). Within a location area, the individual cells are uniquely identified with a CI, a maximum of $2 \times 8$ bits. In order to distinguish neighboring base stations, a BSIC is used which consists of two components namely Network Color Code (NCC) and Base transceiver station Color Code (BCC). NCC of size 3 bits act as a color code within a mobile network and a BCC is of size 3 bits. Directly adjacent mobile networks have different NCCs and neighboring base stations of a mobile network have different BCCs.

![Figure 2.4: LAI Format](image)

### 2.3.3.2 GSM handover

If a handover is initiated by the network, then it is known as network initiated mobile assisted handover and if the handover is initiated by the MN then the handover is known as mobile initiated network controlled handoff. Based on the mobility of MN, the GSM handover is classified into intra MSC and inter MSC handover. If handover takes place within a MSC then it is called as Intra-MSC handover. If handover occurs between different MSCs then it is called as Inter-MSC. Intra MSC is classified again into intra BSC and inter BSC. If the new BTS and existing BTS are under the same BSC then it is called as intra BSC handover and if they are under different BSCs then it is called as inter BSC. If the existing BTS and new BTS are under the different MSCs, then it is known as inter MSC handover [27]. The schematic information is given in Figure 2.5.
Figure 2.5: GSM Handover types

There are two types of MSCs namely anchor MSC and relay MSC. Anchor MSC is otherwise called as home MSC, which remain constant throughout its lifetime of connection. Relay MSC otherwise called as foreign MSC, may belong to homogeneous network or heterogeneous network. Inter-MSC handover is further divided into three types [28] namely 1) anchor to relay  2) relay to anchor  and 3) relay to relay. The structure for the above said types are shown in Figure 2.6, Figure 2.7, Figure 2.8 respectively.

Figure 2.6: Anchor to relay Inter-MSC handover
2.3.3.3 GSM Inter MSC Authentication procedure

In GSM whenever a MN requests to access a foreign network, the home-network must authenticate the MN [23]. The schematic is given in Figure 2.9. The GSM authentication algorithms A3/A8 and COMP-128 are discussed in the following sub sections.
(1) **A3/A8 Algorithm:-**

The process of authenticating a MN is based on the A3/A8 algorithm, which is performed at the network side as well as at the MN side [29]. MN sends the authentication request with its IMSI number to MSC. MSC/HLR (MSC’s HLR) checks whether the IMSI number belongs to its network. When the MN enters into a territory of foreign network, this foreign network will not have the IMSI information of that MN. Hence the IMSI of MN is forwarded to VLR. Then VLR identifies the home network from the IMSI number. The information in IMSI number is shown in Figure 2.10.

![Figure 2.9: GSM authentication](image)

![Figure 2.10: IMSI number format](image)

**MCC** - Mobile Country Code

**MNC** - Mobile Network Code: It identifies the home GSM Public Land Mobile Network (PLMN) of the mobile subscriber as a unique identification code.
MSIN  -  Mobile Station Identification Number: It uniquely identifies the mobile subscriber within a GSM PLMN. The first 3 digits identify the Home Location Register identification (HLR-id) of the MN.

NMSI  -  National Mobile Station Identity: The MNC and MSIN together called as NMSI.

VLR sends the authentication request to the HLR of the MN’s home network. HLR verifies its database about the MN’s identity. If MN belongs to its network then the request is forwarded to AuC. AuC has 128 bit authentication key Ki of MN. Using random number generation algorithm, AuC generates a Random number RAND [30]. This RAND number and Ki are given as inputs to A3 algorithm, which generates 32 bit Signed Response (SRES) as an output. A8 algorithm takes both RAND and Ki as an input and generates 64-bit Ciphering Key Kc as an output [31]. The RAND, SRES and Ki are together called as Triplet. AuC sends the triplet message as an authentication reply to foreign network’s VLR. VLR stores SRES and Kc values and then sends RAND to MN. MN executes A3 algorithm with RAND and key Ki and produces SRES. Also MN executes A8 algorithm to produce Kc. MN sends SRES to VLR for the verification. VLR compares received SRES with the SRES of AuC. If it matches then MN is an authenticated user. Figure 2.11 illustrates the concept of this model with the sequence of steps and various parameters involved in the exchange during authentication.

(2) Comp128 algorithms:

COMP-128 algorithm is proposed to replace the A3/ A8 algorithms with increased number of bits for calculation of SRES and Kc[30]. COMP-128 produces SRES and Kc through the single keyed hash function by taking RAND and Ki as an input. In COMP-128 version-1 produces 54-bit Kc. The COMP-128 version-2 produces 64-bit Kc [32]. Figure 2.12 shows the COMP128 version 2 protocol.
Comp-128 algorithm takes both RAND (128 bit) and Ki (128 bit) as inputs. This algorithm performs eight rounds of functions. Each round
consists of 5 layer operation and a permutation. Each layer performs 16 combination operations by taking a pair of inputs and produces a pair of outputs [33]. Figure 2.13 illustrates the sequence of operation involved. After the completion of round operation, 32 bits SRES and 64 bits Kc are obtained as outputs.
2.3.3.4 IS-95 Architecture

Interim Standard 95 (IS-95) is the first CDMA-based digital cellular standard in 2G mobile communication standards. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95. IS-95, developed by Qualcomm, is based on spread spectrum technology. The IS-95 architecture is shown in Figure 2.14. The main elements are MN, BS, MSC, HLR, VLR, AuC and EIR. BS consists of BTS and BSC. BTS consists of radio equipment (transmitter and receiver = transceivers) and provide radio coverage for a given cell or sector. The channels are classified into forward link (the link from the BS to MN) and reverse link (the link from MN to BS). The forward link has four coded channels namely pilot, synchronization, paging and traffic. The reverse link has two types of channels namely access and reverse traffic [34][35].

![Figure 2.14: IS-95 Architecture](image)

The Pilot Channel (PC) sends the beacon continuously to the MN carrying the information such as timing, phase reference and signal strength for power control. Using this information and based on the measurement of Signal-to-Noise Ratio (SNR) of the pilot signal the MN identifies the BSs which are surrounding it and the strongest BS among them helps to initiate
the handoff operation. The Synchronization Channel (SC) provides the MN with critical time synchronization data. The MN uses the SC to discover the network and its parameters. SC provides pilot PN offset. The paging channel contains messages (system parameters, access parameters, and the neighbor list) that the MN requires for access and paging. Paging channel (PCH) can be used to locate a mobile device. In reverse link the access channel is used to communicate with the BS when no traffic channel has been set up, reverse traffic channel is used to send data and control signals to the BS. IS-95 supports analog and CDMA network.

2.3.3.5 IS-95 Handover

IS-95 supports three main types of handovers namely soft handover, softer handover and hard handover which is shown in Figure 2.15. Soft handover involves an inter-cell handover and is a make-before-break connection. MN has a RAKE receiver, with an ability to operate on three paths (i.e. three BTS) [34][36]. Therefore during handover MN is allocated with a forward link channel at each of the BSs. The information transmitted on each channel is the same, operating on the same CDMA frequency channel, but the channels may use different Walsh codes and different power control bits.

Softer handoff (make-before-break) is an intra-cell handoff, which occurs between the sectors of a BS. Hard handoff (break-before-make type) occurs when the continuity of radio link is not maintained. Hard handover mainly takes place when the mobile device is switched between two BSs using different radio channels. Hard handover is implemented in the area where a MN is a handover from a CDMA network to non-CDMA network [37].
2.3.3.6 IS-95 inter MSC authentication algorithm

In IS-95 network the MN’s authentication algorithm is called Cellular Authentication and Voice Encryption (CAVE) algorithm. In IS-95 network instead of IMEI number, 32 bits Electronic Serial Number (ESN) is shared by both MN and home network MSC/EIR (MSC’s EIR). The first 8 bits of the ESN was the original manufacturer code, leaving 24 bits for the manufacturer to assign up to 16,777,215 codes to mobile devices [38]. In IS-95, AuC generates a 64 bits A-key value and this key shared by both MN and AuC. To execute CAVE algorithm, home MSC generates a random number (RANDSSD).

The ESN, A-key and RANDSSD as input, the MSC processes and executes the CAVE algorithm [39][40] and generates a 128-bit sub-key called the Shared Secret Data (SSD). The SSD has two parts: SSD_A (64 bit), for creating authentication signatures and SSD_B (64 bit), for generating keys to encrypt voice and signaling messages [41]. MSC sends the RANDSSD to MN. Since MN has ESN and A-key, with the help of RANDSSD MN executes CAVE algorithm and produces SSD-A and SSD-B. MN sends SSD-A to MSC. MSC verifies the MN generated SSD-A and MSC generated SSD_A are equal. If it is equal then MN is genuine user otherwise is an intruder.
2.3.4 2.5 Generation (2.5G)

To support higher data rate transmission for web browsing and e-mail traffic support, 2.5 generation (2.5G) was introduced. The major applications of 2.5G are Wireless Application Protocol (WAP), General Packet Radio Service (GPRS), High Speed Circuit Switched Data (HSCSD), Enhanced Data rates for GSM Evolution (EDGE) etc. [42].

2.3.4.1 GPRS Architecture

GPRS applies a packet switching principle, where the data is split into packets and they are transmitted separately and finally assembled at the receiver end. The components of GPRS are MN, BTS, BSC, Serving GPRS Support Node (SGSN) and Gateway GPRS support node (GGSN). In a BSC, upgradation of both software and hardware is required. The hardware upgrade consists of adding a Packet Control Unit (PCU). This PCU differentiates data destined for the standard GSM network (Circuit Switched Data) and GPRS network (Packet Switched Data). The architecture of GPRS is shown in Figure 2.16. GPRS Support Nodes (GSN) are used to integrate GPRS into the existing GSM architecture. GSN also takes care of the delivery and routing of data packets between the MNs and the external Packet Data Networks (PDN). There are two new GSN functional elements namely SGSN and GGSN. SGSN delivers data packets from and to the MNs within its service area. Its function also includes packet routing and transfer, mobility management (attach/detach and location management), logical link management, authentication and charging functions. The location register of the SGSN stores location information and user profiles of all GPRS users registered with the SGSN. GGSN acts as an interface between the GPRS and the external packet data networks. GGSN converts the GPRS packets coming from the SGSN into the appropriate Packet Data Protocol (PDP) format (e.g., Internet Protocol (IP) or X.25) and sends them out on the corresponding packet data network. PDP addresses of incoming data packets are converted to the GSM address of the destination user and the re-addressed packets are sent to the responsible SGSN. Same as MSC in
GSM, GGSN also has HLR (It also acts as a authentication centre), VLR and EIR registers [43][44].

![GPRS Architecture Diagram](image)

**Figure 2.16: GPRS Architecture**

The Packet Broadcast Control Channel (PBCCH) is a unidirectional point-to-multipoint signaling channel used by the BSS to broadcast specific information about the organization of the GPRS radio network to all GPRS MNs of a cell. The PBCCH also broadcasts circuit switched services along with system information about GPRS. The Packet Common Control Channel (PCCCH) is a bidirectional point-to-multipoint signaling channel that conveys signaling information for network access management. It consists of four sub-channels which are described below.

(i) The Packet Random Access Channel (PRACH) - used by the MN to request one or more PDTCH.

(ii) The Packet Access Grant Channel (PAGCH) - used to allocate one or more PDTCH to a MN.
(iii) The Packet Paging Channel (PPCH) - used by the BSS to find out the location of a MN (paging) prior to downlink packet transmission.

(iv) The Packet Notification Channel (PNCH) - used to provide information to a mobile node of incoming PTM (Point to Multipoint) messages (multicast or group call).

The dedicated control channel is a bidirectional point-to-point signaling channel which also has the channels, Packet Associated Control Channel (PACCH) and Packet Timing Advance Control Channel (PTCCH). The PACCH is allocated along with one or more Packet Data Traffic Channel (PDTCH) assigned to one MN. It transports signaling information regarding one specific MN. The PTCCH is used for adaptive frame synchronization. The PDTCH is employed for the transfer of user data [45].

2.3.4.2 GPRS Handover

Both GSM and GPRS share the same radio access network, making some handover functionalities common to both. Cell reselection process takes place during the handover process. The GPRS follows the Network Assisted Cell Change (NACC) procedures to reselect the cell [46]. If MN decides that there is a need of reselecting new BTS, then MN starts to read the system information of other BTS. If MN finds better BTS, then it sends the cell change notification and channel request message to SGSN. It performs the handover process [47][48].

2.3.5 Third Generation (3G)

Third generation (3G) is based on the International Telecommunication Union (ITU) family under the International Mobile Telecommunications-2000 (IMT-2000). ITU lounged IMT-2000 for global frequency band for all countries. An organization called 3rd Generation
Partnership Project (3GPP) has continued that work by defining a mobile system that fulfills the IMT-2000 standard. This system is called Universal Mobile Telecommunications System (UMTS). ITU also has approved Wideband CDMA (W-CDMA), CDMA2000 and Time Division Synchronous Code Division Multiple Access (TD-SCDMA) as the 3G standards which are part of the 3G framework [49]. Some of the applications of 3G are symmetric and asymmetric data transmission, circuit and packet switching based services, voice, multimedia and high speed data communication, global roaming [50].

2.3.5.1 WCDMA Architecture

The WCDMA architecture is shown in Figure 2.17. The WCDMA has 5 MHz channel to support data and voice at a rate of 2 Mb/s. WCDMA based 3G has two major parts namely Radio Access Network (RAN) and Core Network (CN). The RAN consists of BS and Radio Network Controller (RNC). The BS takes care of channel coding, interleaving, rate adaptation and processing the air interface. BS (node B in 3G) acts as an interface between the network and WCDMA air interface. RNC acts as an interface between CN and BS. The Circuit Switching (CS) domain and Packet Switching (PS) domain are the two domains of CN. Circuit switching is based on GSM model, in which communication occurs via MSC and Gateway MSC (GMSC). Packet switching is based on GPRS model; here communication occurs through SGSN and GGSN [51].
2.3.5.2 WCDMA Handover

Each MN has a TMSI and a permanent IMSI. Each time when MN changes its network, it receives a new TMSI. RNC monitors the signal quality of the MN. Whenever the quality of the signal received from a particular MN fall below the threshold value, immediately the RNC suggests another channel with better quality. Similar to IS-95, in WCDMA also handover is categorized as soft handover, softer handover and hard handover [51][52].

2.3.5.3 CDMA 2000 Architecture

CDMA2000 supports high-speed data services has peak data rate of 2.45 Mb/s on the downlink. To support packet based services more efficiently, CDMA 2000 is upgraded with Packet Data Serving Node (PDSN), Authentication, Authorization and Accounting (AAA), and Home Agent (HA) along with the existing network elements of IS-95, namely BTS and BSC which is shown in Figure 2.18. BSC has additional IP routing functionality, new PDSN establishment and it initiates AAA for the MN. In addition, it also
does the functionalities of HLR and VLR. MN usually initiates a data call via BTS, BSC to PCF (Packet Control Function). The PCF selects a PDSN, based on certain unique characteristics of the MN [59] and establishes a GRE (Generic Routing Extension) tunnel with the PDSN. Now the MN initiates a Point-to-Point protocol (PPP) session which gets terminated at the PDSN. This results in single hop IP connectivity between the MN and the PDSN [52][53].

![CDMA 2000 Architecture](image)

**Figure 2.18: CDMA 2000 Architecture**

### 2.3.5.4 CDMA 2000 Handover

A mobility of a node is taken care at each level of the hierarchy as BTS level, PCF level, and PDSN level. When the MN moves between two BTSs, as long as the movement is confined to the PDSN the MN does not need to set up a new PPP session. But if the MN moves between two BTSs that are controlled by two different PCFs, then each PCF chooses a new PDSN in the hierarchy. This results in the termination of the PPP session and starts a new one for which the MN chooses a new PDSN to re-establish a new PPP session. During packet-based communication, a MN is identified with a simple IP addressing scheme or mobile IP. In case of simple IP addressing scheme, the mobile device obtains the IP address from a Dinamic
Host Configuration Protocol (DHCP) server that usually co-locates with the PDSN. Thus the identifier changes as the MN moves between the PDSNs. However, if the MN uses mobile IP-based approach, this IP address does not change. In case of IP address change, layer 3 mobility can be taken care of by mobility protocols like Mobile IP at PDSN layer [52][54][53].

2.3.6 Fourth Generation (4G)

Fourth Generation (4G) introduced LTE (Long Term Evolution). LTE achieved high data rates through carrier aggregation, spectrum aggregation and additional antennas (up to 8 antennas downlink, 4 antennas uplink), achieving 3Gbps (Gigabits per second) peak data rate uplink and 1.5Gbps downlink. LTE supports both IPv4 and IPv6 and it also uses Orthogonal Frequency Division Multiplexing (OFDM) technology, Multiple Input Multiple Output (MIMO) technology, Flash-OFDM, Single Carrier-FDMA (SC-FDMA), Multi-carrier CDMA (MC-CDMA) and LTE SAE (System Architecture Evolution). LTE-CoMP (LTE Co-ordinated multipoint) refers to the dynamic coordination of transmission and reception among different base stations. In 4G lot of researches are going on today for standardization. The 4G supports applications like Mobile TV, Multimedia Messaging Service (MMS), Digital Video Broadcasting (DVB), Video on demand, Video conferencing etc., [55]. The latest evolution of UMTS standard is Evolved Packet System (EPS) in 4G.

2.3.6.1 Evolved Packet System Architecture

EPS consists of two parts, namely LTE and System Architecture Evolution (SAE) as shown in Figure 2.19. LTE looks after the radio interfaces and SAE takes care on core network architecture evolution. LTE is also known as Enhanced UMTS Terrestrial Radio Access Network (E-UTRAN). LTE is a packet optimized access network which supports IP-based real-time and non-real time services. Its performance is comparable to circuit switching parameters. It has fully shared radio resource allocation scheme thereby maximizes resource usage by combining all the radio bearers on a shared high bit rate radio channel. The goal is to provide reduced latency, higher
data rates, improved system capacity, coverage as well as reduced cost for the operator. There is no separate RNC (BSC), but RNC is functionality integrated into eNode-B (BS is represented as eNode-B in 4G) [56].

SAE, also known as EPC (Evolved Packet Core) is composed of several functional entities, namely MME (Mobility Management Entity), Serving Gateway (S-GW), Packet Data Network Gateway (PDN-GW) and Home Subscriber Server (HSS). All the control plane functions, security procedures, terminal-to-network session handing, idle terminal location management are done by MME with the help of HSS database. The S-GW, the termination point of the packet data, act as an interface towards E-UTRAN and serves as a local mobility anchor thereby supports intra E-UTRAN mobility and mobility with other 3GPP technologies. PDN-GW (Packet Data Network Gateway), is the termination point of the packet data interface towards the packet data network. It supports policy enforcement features, packet filtering and enhanced charging support. PDN-GW also acts like a home agent. LTE supports mobility with both 3GPP and non-3GPP access systems (UTRAN).

![Figure 2.19: EPS Architecture](image-url)
2.3.6.2 EPS Handover

Intra-MME and Inter-MME are the two types of handovers defined for LTE. LTE supporting Mobility with 3GPP (trusted) access system is called local mobility and mobility with non-3GPP (untrusted) access system is called global mobility [57][58]. Both GTP-based (GPRS Tunneling Protocol) mobility and mobile-IP-based mobility are used to support local mobility. However, only mobile IP-based mobility is used to support global mobility [59].

2.4 CONCLUSION

The various developments in wireless communication procedures have been discussed upto present 4G status. The handover mechanisms with different type of architectures have also been discussed. The signaling channel used by various networks are also discussed. The next chapter introduces a new authentication algorithm which deals authentication and identity verification during inter MSC handover. It also gives performance improvements obtained through the new authentication algorithm in various networks.