Available online at www.worldscientificnews.com

World Scientific News

WSN 54 (2016) 27-39 EISSN 2392-2192

Evolutionary Analysis of GSM, UMTS and LTE Mobile Network Architectures

Paschal A. Ochang[1,a], **Philip J. Irving**[2,b]

[1]Department of Computer Science, Federal University Lafia, Nasarawa State, Nigeria

[2]Department of Computing, Engineering and Technology, University of Sunderland, Sunderland, SR6 0DD, United Kingdom

[a,b]E-mail address: pascosoft@gmail.com , phil.irving@sunderland.ac.uk

ABSTRACT

The Global System for Mobile Communications (GSM) which is a standard for 2G (second generation) cellular networks has created an avenue for the development of 3G (third generation) and 4G (fourth Generation) cellular network standards such as Universal Mobile Telecommunications System (UMTS) and long term evolution (LTE). With the deployment of new technologies still on the way, the era beyond 3G and 4G requires that cellular and radio technologies need to work together forming highly heterogeneous networks, therefore this paper analyses already existing cellular network technologies such as LTE, GSM and UMTS in order to give a general understanding of their architectures, functional and evolutional dependencies and also to provide an evolutionary trend and a clear overview of the support provided for other telecommunications infrastructure.

***Keywords*:** GSM; UMTS; LTE; Network Achitecture; Security; Bandwidth

1. INTRODUCTION

Mobile communication and wireless technologies have seen a major significant growth over the recent years (Gu and Peng, 2010) due to the numerous advantages they contribute not only to the economic sector but to other sectors as well. This significant evolution of mobile communications technologies can be categorised into generations respectively which include 1G, 2G, 3G and 4G (Poole, 2006). Section 2 of this report discusses the GSM architecture,

while section 3 discusses the UMTS architecture. Section 4 gives an overview of the LTE architecture, while section 5 gives an overview of the comparison between all architectures

2. GSM

The introduction of mobile communications can be traced back to the early 1980s when the first analogue systems where being implemented in the US, this led to the development of advance mobile phone system (AMPS) which commenced operation in Chicago with the major objectives of interstate roaming and handset compatibility (Fuentelsaz et al., 2008). Development also took place in Europe with the introduction of the total access communication system (TACS) and in 1985 two companies were give operational licences namely British Telecommunications and Racal Vodaphone (Poole, 2006). Most of these systems were analogue systems that consisted of mixed technologies which differ between countries and had many drawbacks such as continental roaming could not be achieved also the analogue systems could not handle the increase in capacity of users. In 1982 a committee of technical personnel referred to as Group Special Mobile (GSM) was set up by the European Conference of Postal and Telecommunications Administrations (CEPT) to implement a mobile communications technology that was digital, pan-European in nature and allowed roaming throughout the whole European continent while providing improved capacity when compared to analogue systems. In 1991 the GSM standard was deployed using the 900 MHz band (Gu and Peng, 2010).

2. 1. GSM SYSTEM ARCHITECTURE

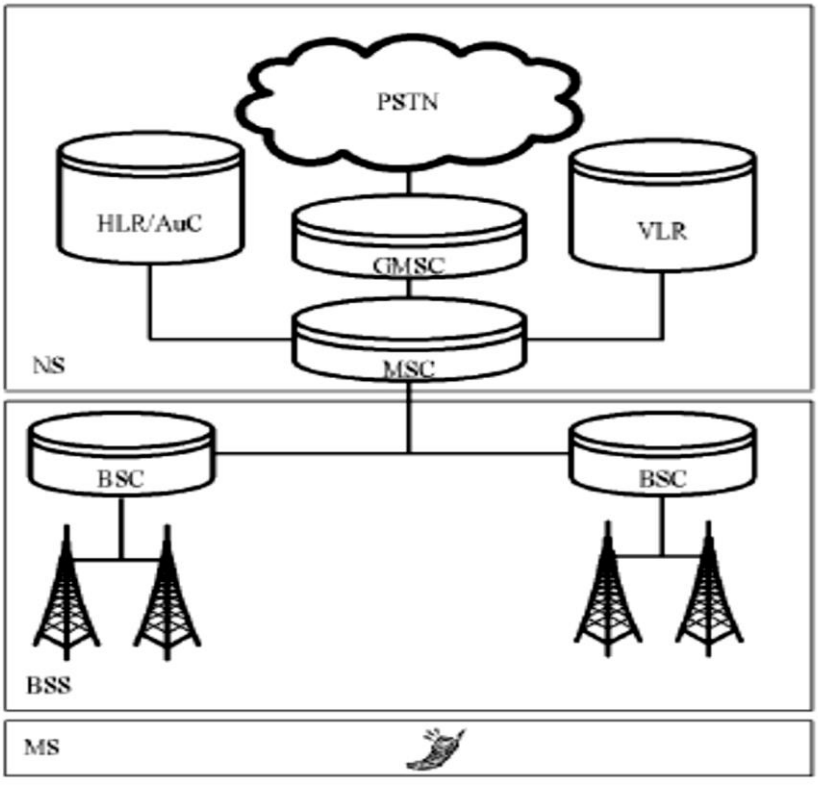

Figure 1. GSM Network Architecture.

The GSM architecture is made up of majorly three subsystems which include the Mobile Station, Network and Switching Subsystem (NNS), and the Base Station Subsystem (BSS) (Gu and Peng, 2010). The GSM architecture also contains an intelligent network subsystem (IN) which adds more functionality to a network in terms of prepaid services whereby a subscriber can fund his or her account for making calls and sending short message services (SMS) (Sauter, 2011).

2. 2. MOBILE STATION

The mobile station consists of all the equipment or software required by a subscriber to communicate with the network. It consists of the mobile equipment (ME) and the subscriber identity module (SIM). The ME which is also referred to as the mobile phone consists of a unique international mobile equipment identity (IMEI) which is used to validate and identify it on the network. The SIM is a memory module which contains all the details of a user on a network; it contains an international mobile subscriber identity (IMSI) which identifies it uniquely. It also consist of Authentication key (Ki) used for authentication (Qureshi and Usman, 2011).

2. 3. BASE STATION SUBSYTEM (BSS)

The BSS which is also known as the radio network or the radio subsystem manages all the radio transmission paths between the mobile stations (MS) and other subsystems in the GSM architecture (Sauter, 2011).The BSS consist of base station controllers (BSC) and the base transceiver stations (BTS).

2. 3. 1. Base Transceiver Station

The base transceiver station contains the facilities for transmitting and receiving radio signals. The transmission path between the mobile station and the base station is referred to as the Um interface.

2. 3. 2. GSM Air Interface

GSM employs two methods in other to allow simultaneous communication between a BTS and multiple subscribers, this include the frequency division multiple access (FDMA) which enables subscribers to communicate with the BTS using multiple frequencies, while the other method is the TDMA which enables subscribers to be multiplexed using time by dividing carriers into frames. Each of the frames contains eight time slots that are physically independent, and each of the time frames is referred to as a burst. If a subscriber was allocated a timeslot of 2 that meant the caller can only send and receive during this burst. The time slots are arranged into logical channels for the purpose of transmission of user data, some this logical channels include the traffic channel (TCH) which is used for the transmission of digitised voice, fast associated control channel (FACCH) which is used when urgent signalling messages are needed to be sent such as handover command, The Slow Associated Control Channel (SACCH) which is used for the measurement of signal quality and provides values for power control and handover decisions.

2. 3. 3. Base Station Controller (BSC)

The BSC carries out establishment, maintenance and release of connections that are established on a cell. The BSC also handles radio channel allocation and controls BTS to BTS handover. When a subscriber has an incoming call the BSC is paged by the MSC which in turns check its local database in other to determine the cell which a subscriber that needs to be paged belongs to. When a message is received by the mobile station, a channel assignment message is also sent by the mobile station. When the mobile station has exchanged necessary information with the MSC, a request is sent by the MSC to the BSC for a voice channel to be assigned to the mobile station. The BSC then checks if a traffic channel is available and activates it on the BTS then the mobile station switches to the TCH and the FCCH and uses the FCCH to notify the BTS that it is now on that TCH. When there is low signal reception by the mobile station, the BSC is responsible for sending power control messages to the BTS which in turn forwards it to the mobile station so that the mobile station can increase the power of the antennas.

2. 4. NETWORK AND SWITCHING SUBSYTEM (NSS)

The NSS is the core component of the GSM architecture which is responsible for call switching, end to end calls, mobility management of subscribers and communication with other networks such as PSTN and ISDN. The components of the NSS include the Mobile Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and Authentication Centre (AUC).

2. 4. 1. Mobile Switching Centre (MSC)

The MSC is a central part of the NSS which provides call set up, call routing, call switching and handoff. when there is no connection between the network and the mobile device, the MSC reports a change of location to the network so that the mobile station can be reachable by incoming calls, also when a subscriber changes location while a call is established, the MSC is part of the component that makes sure the call is rerouted to the next cell without interrupting the call. The MSC can be classified under different context depending on roles, for example a Gateway MSC is responsible for interfacing with the PSTN and it is also responsible for locating a currently called subscriber.

2. 4. 2. Home Location Register (HLR)

The HLR is a central database or subscriber database of all subscribers that are authorized to use the GSM network; it also contains the individual services that are associated with a subscriber. The HLR contains details of every SIM on the network and uses the IMSI of the SIM as a primary key for searching its records.

2. 4. 3. Visitor Location Register (VLR)

The VLR is a database of all subscribers who roam into an area served by an MSC but do not reside there (Chitrapu and Aghili, 2007). When a Subscriber roams into the area of an MSC, the subscriber details are copied into the VLR while the original details are stored in the HLR; this is used to reduce the amount of signalling done between the MSC and the HLR.

2. 4. 4. Equipment Identity Register (EIR)

The EIR contains a list of mobile phones that are either monitored, stolen or have been banned from the network the mobile phones are identified by their IMEI (international mobile equipment identity). When a mobile station tries to access a network the IMEI is compared with the register of the EIR and the response or status message can be (a) white-listed: in this case the mobile station is allowed to connect (b) grey-listed: in this case the mobile station is being monitored (c) black-listed: the mobile station is not allowed to connect because it has either been reported stolen or not approved.

2. 4. 5. Authentication Centre (AUC)

The Authentication Centre (AUC) is an element that is used to authenticate the SIM card of a subscriber on the network. The AUC contains the key per subscriber called Ki which is also contained in the SIM card in other to prevent SIM card cloning on the network.

2. 5. BANDWIDTH OFFERED BY GSM

GSM uses TDMA combined with a channel bandwidth of 200 kHz to provide a high level of spectrum efficiency (Poole, 2006).GSM uses Frequency division duplexing to pair channels for both uplink to the BTS and downlink to the mobile devices respectively. Initially in Europe, GSM was configured to use the 900MHz band with an uplink of 890 to 915 MHz and a downlink of 935 to 960 MHz to provide a bandwidth of 25MHz which can be split into 125 channels of 200 kHz each (Sauter, 2011). Due to the increase in demand for channels in the European countries the 1800 MHz band was introduced and had an uplink of 1710 to 1785 MHz and downlink of 1805 to 1880 MHz, this provided a bandwidth of 75 MHz which provided 375 channels. The 1900 and 850 MHz bands were also introduced in North America.

2. 6. AUTHENTICATION IN GSM

When a mobile station is switched on, it sends its IMSI after which it is assigned a TMSI. The MSC and VLR gets it's real IMSI and sends it to the AuC which then finds its authentication key (Ki). By using the Ki with ciphering key generation algorithm (A8) and Authentication algorithm (A3), a ciphering key (Kc) and a signed result (SRES) and random number (RAND) which is called an authentication triplet is generated (Qureshi and Usman, 2011). The triplet is sent back to the MSC and VLR who in turn send the SRES and the RAND to the mobile station while retaining the Kc. The mobile station uses the A3 and A8 algorithm to generate SRES and Kc using the Ki in the SIM and the received RAND, and then SRES is sent back to the VLR and MSC which in turn compares it with the SRES that was received from the AuC and HLR. Authentication is successful if the match between the SRES is successful

2. 7. ROAMING IN GSM

The roaming service allows a subscriber to travel out of his home network to a visited network and still use the services provided by his home network. When a subscriber moves to a visited network, the visiting network performs a location update (LU) through the Signalling Connection Control Part (SCCP) gateway which is part of the signalling system 7 (SS7)

(Assawaboonmee et al., 2004), then authentication is also carried out and the roaming subscriber profiles are stored in the VLR. The details of the subscriber will also be updated in the HLR of the subscriber's home network. This allows the subscriber to use the visited network as his home network.

2. 8. CALL SECURITY IN GSM

Call security and privacy in GSM is achieved by ciphering or encrypting each burst of data or voice stream using the A5/1 encryption algorithm (Gold, 2011). Data and speech encryption is only done on the air interface between the BTS and the Mobile station. To encrypt the data stream a Kc is calculated by the SIM card and AuC by using the Ki and RAND as input parameters for the A8 algorithm, then the A5 ciphering algorithm uses the Kc to generate a 114bit sequenced which is XOR with the data stream (Sauter, 2011). This 114 bit is changed for every burst in other to enhance security.

3. UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS)

UMTS is regarded as a third generation (3G) wireless communication system that acts as a successor to the second generation (2G) communication technologies and is an evolved version of GSM GPRS and EDGE (Poole, 2006). The GSM network was used to provide voice capabilities to subscribers but they was need to support the increasing number of subscribers while providing high speed data services. The Third Generation Partnership Programme (3GPP) was formed to oversee the implementation of a system that could offer support to those services.

3. 1. UMTS RELEASE 99 ARCHITECTURE

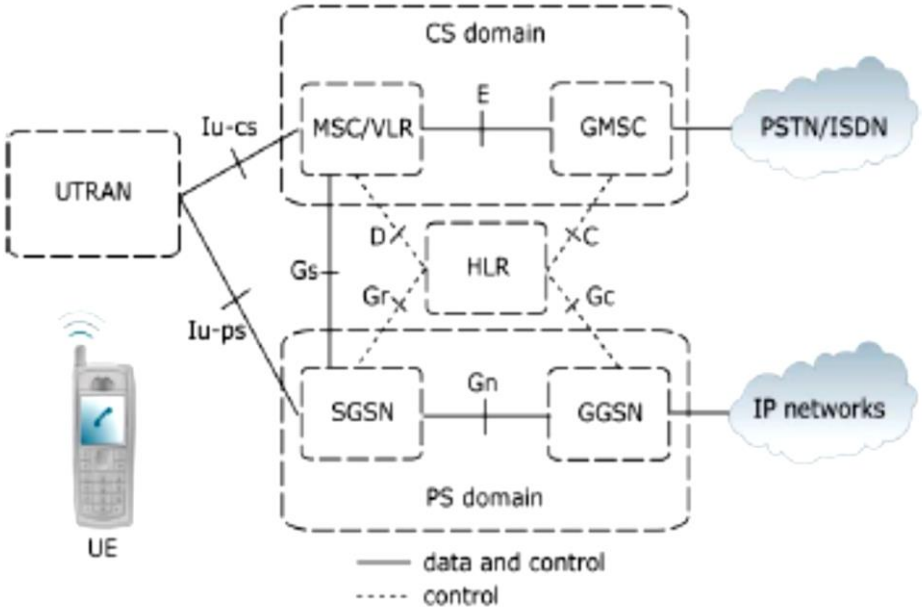

Figure 2. UMTS Release 99 Architecture

The first release of the UMTS system was called release 99 due to its year of release, and it was an enhancement to the GSM/GPRS architecture and consisted of three main portions: Core Network, User Equipment and the UMTS Terrestrial Radio Access Network (UTRAN) (Ouyang and Fallah, 2010)

3. 1. 1. User Equipment (UE)

This is the equivalent of the mobile station used in the GSM architecture.The UE also made use of a new SIM card called USIM which was given an access priority control feature whereby subscribers with high priority such as the police were still able to use the system even if it was close to its capacity (Poole, 2006).

3. 1. 2. Universal Terrestrial Radio Access Network (UTRAN)

The overall radio network access system of the UMTS is considered as the UTRAN (Britvic and Tesla, 2004). The UTRAN consist of multiple Radio Network Subsystems (RNSs) which is equivalent to the base station subsystem (BSS) in the GSM architecture, also the RNS consists of radio transceivers referred to as Node B which are equivalent to the BTSs in the GSM architecture and are controlled by Radio Network Controllers (RNCs) which is the equivalent of a base station controller (BSC) via an interface known as the Iub interface.

3. 1. 3. Core Network (CN)

The CN is similar to the network and switching subsystem (NSS) of the GSM architecture. The main function of the CN is to perform packet routing, connection of users, security, billing and the connection of UMTS to external packet switched and circuit switched networks (Neruda and Bestak, 2008). The CN elements can be categorised into a packet and circuit switched domain depending on the type of traffic and functions they handle. Some of the elements in the circuit switched domain include:

- The Mobile Switching Centre (MSC)/Visitor Location Register (VLR): these elements still retain their functions used in the GSM architecture
- The Gateway MSC (GMSC): it connects the UTMS standard to Circuit switched networks and assist in the termination of PSTN signalling. It also converts Circuit Switched network formats to protocols meant for mobile networks

While some of the elements in the packet switched domain include:

- Serving GPRS Support Node (SGSN): this performs access control, security functions and keeps track of the location of a UE. It is the equivalent of the MSC and VLR meant for packet switched networks.
- Gateway GPRS Support Node (GGSN): this is an equivalent of the GMSC meant for packet switched networks. It handles the task of an internet protocol router meant for packet switched networks that are external to the UMTS. The GGSN also handles billing functions and protects the core network by carrying out filtering and firewall functions.

Other elements such as the HLR, EIR, AuC retain the same functions carried out in the GSM architecture and are shared by both domains.

3. 2. UMTS RELEASE 4 ARCHITECTURE

The release 4 of UMTS presented major enhancements in the data and circuit switched voice services, with the major aim of merging the packet and circuit switched core networks into a unified network with the ability to handle all types of traffic. A new concept was implemented called Bearer-Independent Core Network (BICN) whereby traffic was inside IP packets rather than 64Kbp/s time slots (Sauter, 2011). For this to be achieved the MSC was divided into an MSC server, which is responsible for mobility management and call control, and a Media Gateway which is responsible for handling user traffic (Neruda and Bestak, 2008). The Media Gateway is capable of receiving voice streams via a GSM E-1 64Kbp/s timeslot and then covert the stream into an IP packet connection and transported to the destination Media Gateway.

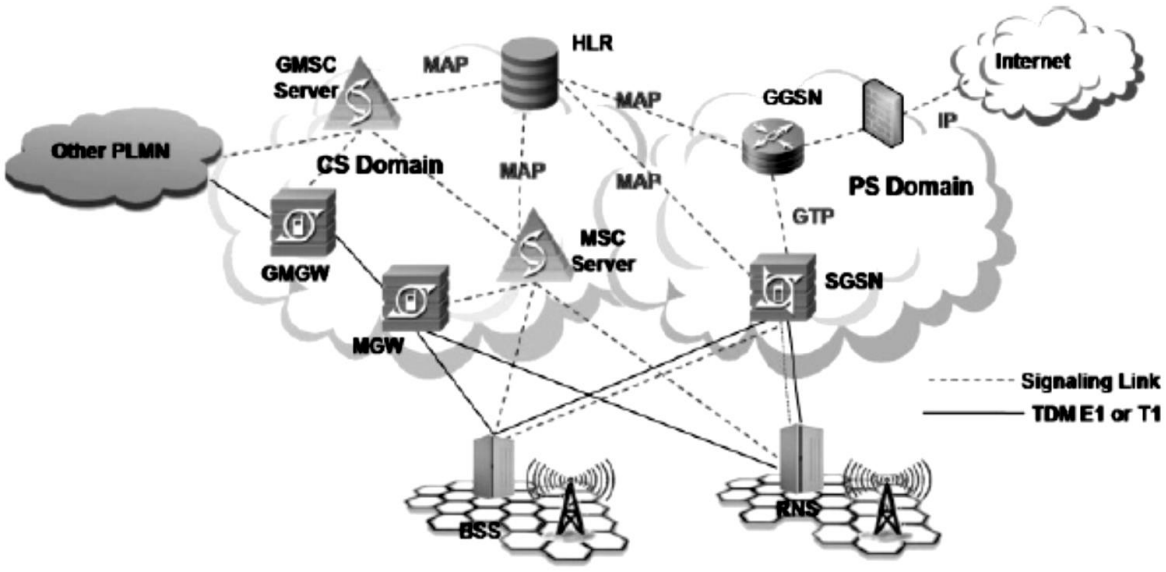

Figure 3. UMTS release 4 Core Network Architecture

3. 3. UMTS BANWIDTH

The UMTS uses WCDMA (Wideband Code Division Multiple Access) unlike the GSM which uses FDMA and TDMA to separate users into different timeslots and frequencies; this gives UMTS the ability to place multiple users on the same frequency with unique codes and high bandwidth is achievable. In other to achieve high data transmission rate per user, UMTS uses 5MHz bandwidth per carrier frequency, therefore the Carrier frequencies which are designated by a UARFCN (UTRA Absolute Radio Frequency Channel Number) can be calculated as 5* frequency in MHz (Poole, 2006).

3. 4. AUTHENTICATION AND SECURITY IN UMTS

In addition to the authentication triplet used in the GSM architecture, the UMTS makes use of two more values called Integrity Key (IK) and Authentication Token (AUTN), these

five are referred to as authentication vector (Sauter, 2011).The AUTN is used by the mobile devise to determine if the authentication procedure was initialised by an authorised network. When the UE respond to the authentication message, the SGSN and the MSC/VLR compares the SRES value to the response value received from the AuC/HLR and if it matches authentication is successful. The authentication and key agreement is used by UMTS for ciphering after successful authentication. The RNC handles ciphering and integrity of calls by using a security mode command message which contains a 128 bit ciphering key.

4. LONG TERM EVOLUTION (LTE)

Long Term Evolution (LTE) is a fourth generation wireless communication standard developed by the 3GPP (Setiawan and Ochi, 2009), although the standard was first publish in 2005 by the 3GPP in its release 6 (Mustaqim et al., 2012) it has been under development and was fully published in 2008 in the release 8 documentation of the 3GPP. The LTE is often referred to as 4G but the LTE-Advanced which was defined in the release 10 is considered as the true 4G network and release 8 is considered as 3.9G. LTE was implemented as a solution to solve the high demand for data rates by services such as gaming, streaming and web browsing which have increased the data rates from Mbit/s to Gbit/s. Another reason for the implementation of LTE was to reduce delay and latency in network services while increasing the spectral efficiency of the network.

4. 1. LTE ARCHITECTURE

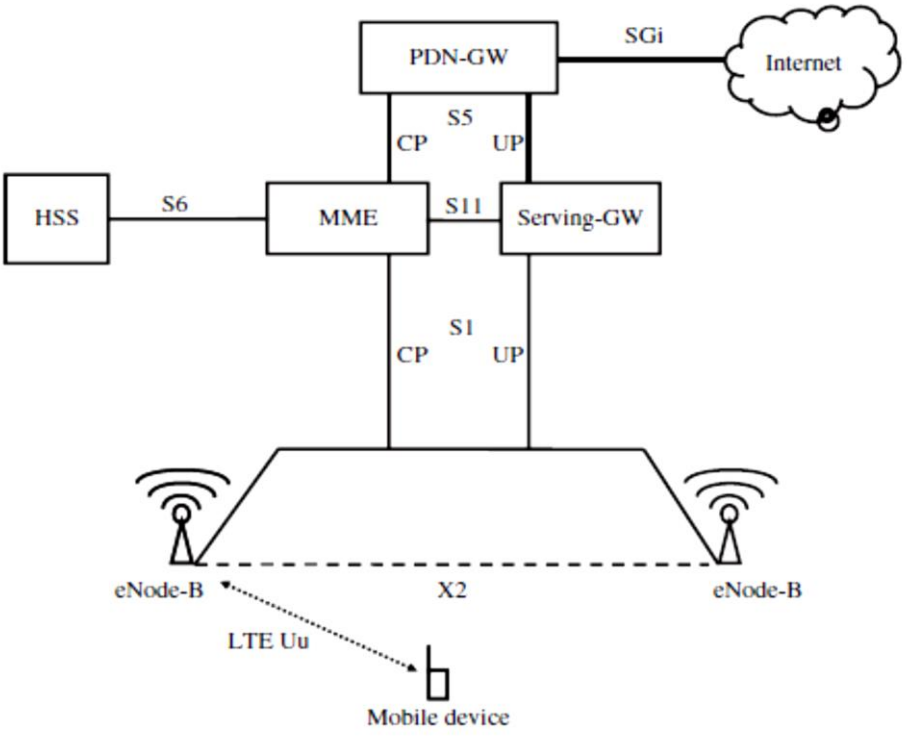

Figure 4. LTE Network Overview

LTE has a flat architecture which was developed in a work by the 3GPP known as the System Architecture Evolution (SAE) (Dahlman et al., 2011) this lead to an evolved core network referred to as Evolved Packet Core (EPC) and a flat LTE Radio Access Network (RAN). Both the EPC and the LTE RAN can be referred to as the Evolved Packet System (EPS) (Rinne and Tirkkonen, 2010).

4. 2. LTE RADIO ACCESS NETWORK (RAN)

The LTE RAN has also been evolved and is known as Evolved Universal Terrestrial Radio Access Network (EUTRAN) (Sauter, 2011). The LTE RAN consists of single radio access points referred to as eNode B, where the e stands for evolved. The eNode B handles all air interface communications, radio resource management, header compression, security, modulation, interleaving, handover and retransmission control. The eNode Bs in an an LTE RAN are connected together by an interface known as the X2 interface, while the S1 interface handles transport of user and control plane traffic and connects the eNode Bs to the EPC.

4. 3. EVOLVED PACKET CORE (EPC)

The The EPC in the LTE technology supports only access to the packet switched domain only and provides no support for the circuit switch domain (Dahlman et al., 2011). The EPC functions include: policy control, interconnection to external networks, subscriber charging and QoS provisioning. The elements of the EPC are discussed below.

4. 3. 1. Mobility Management Entity (MME)

The MME is the control plane node responsible for handling of security keys and transitions between idle to active state mobility. It operates in the control plane and is responsible for sending paging messages to the eNode Bs and also bearer procedures in terms of setup. MME is responsible for contacting the Homer Service Subscriber (HSS) for information of subscribers and is capable of storing the mobility context of UE (Rinne and Tirkkonen, 2010).

4. 3. 2. Serving Gateway (S-GW)

The S-GW is the user plane node in the EPC which is responsible for connecting the LTE RAN to the EPC. The S-GW also functions as a mobility anchor when UEs move from one eNode B to another and also handles user data tunnels between the eNode B and the Packet Data Network Gateway (PDN-GW) which act as the gateway router to the internet.

4. 3. 3. Packet Data Network Gateway (PDN-GW)

The PDN-GW handles the connection of the EPC to the internet and is also responsible for giving IP addresses to terminals. The PDN-GW is sometimes used by network operators to interconnect to the intranet of large companies via an encrypted tunnel in other to offer employees direct access to their private internal networks (Sauter, 2011).

4. 3. 4. The Home Subscriber Server (HSS)

This is the equivalent of the HLR in the GSM architecture and contains the database for the subscribers on the network and is combined physically with the HLR to allow seamless

roaming between two different radio networks, it also connects to the MME via the S6 interface.

4. 4. LTE BANDWIDTH

The LTE uses OFD modulation which enables bandwidths to be easily adjusted by changing the number of carries without making changes to the parameters of the system.LTE operates on lower bandwidths of 1.4 and 3 MHz and higher bandwidths of 15 and 20MHz, it can also operate on the 10 and 5 MHz it operates on the following bands in Europe: 1900-1920, 2010-2025, 2570-2620, 2300-2400.

4. 5. AUTHENTICATION AND SECURITY IN LTE

The algorithms used for authentication are stored and executed in the SIM and the HSS; this prevents eavesdropping because the key remain in a protected environment. After authentication integrity and ciphering checks are carried out between the MME and the UE, the eNode B also carries out ciphering and integrity checks, therefore integrity and ciphering is double. After integrity and ciphering is complete, the UE, MME and the eNode B can select an appropriate integrity an encryption algorithm (Sauter, 2011).

5. COMPARISON OF GSM, UMTS, AND LTE

GSM, UMTS and LTE are similar in many ways in the sense that they inherit most of the elements implemented in the GSM/GPRS and EDGE architecture while changing the names of the elements. A Major similarity is the fact that they all implement radio access points and they use cellular technology; another similarity is that they all employ the use of the HLR as the subscriber database although it is called the Home Subscriber Server (HSS) in LTE. The differences between most of the technologies are based on the evolvement of the core elements and the access methodologies, bandwidths and modulation types. The table below is used to give a better comparative analysis between the technologies.

Table 1. Comparison of GSM, UMTS and LTE features.

	GSM	UMTS	LTE
Access Methodology	TDMA/FDMA	WCDMA	OFDMA/ SC-FDMA
Maximum downlink speed	10-150Kbps	384Kbps	100Mbps
Maximum uplink speed	10-150Kbps	128Kbps	50Mbps
Bandwidth	200 KHz	5 MHz	1.4 to 20 MHz
Modulation types supported	GMSK	QPSK	QPSK, 16QAM, 64QAM
Core Network type	Circuit Switched	Circuit/packet Switched	Fully IP based

6. CONCLUSIONS

Mobile cellular technologies have experienced a tremendous growth and change in their architectural design and this change has been very significant in the core of the network. The network core has fully evolved from a circuit switched core to an all IP based core which means that with the advent of future cellular technologies, IP packets can be used to carry cellular network traffic therefore enhancing traffic management and providing better quality of service. Based on this analysis this means that they will be advanced support for services such as multimedia streaming. Integration with other telecommunication infrastructure such as Voice over Internet Protocol (VoIP) will provide an interesting area of research. Therefore further research can be carried out in other to provide a clear overview of how VoIP can be integrated into the IP core of advanced future cellular technologies.

References

[1] S. Assawaboonmee, 'Roamer Direct Dialing (RDD)', *2004 IEEE Region 10 Conference TENCON 2004*, 3 (2004) 41-43.

[2] V. Britvic, 'Steps in UMTS Network Design', *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, 2004. MELECON 2004*, 2 (2004) 461-464.

[3] P. Chitrapu, B. Aghili, 'Evoluton of GSM into the Next Generation Wireless World', in *IEEE Long Island Applications and Technology Conference, 2007. LISAT 2007*, 2007, 1-10.

[4] D. Erik, P. Stefan, S. Johan, *4G_LTE_LTE-Advanced* (Oxford: Elsevier, 2011)

[5] L. Fuentelsaz, J.P. Maícas, Y. Polo, 'The Evolution of Mobile Communications in Europe: The Transition from the Second to the Third Generation', *Telecommunications Policy*, 32 (2008) 436-449.

[6] S. Gold, 'Cracking GSM', *Network Security*, 2011, 12-15.

[7] G. Gu, G. Peng, 'The Survey of GSM Wireless Communication System', *2010 International Conference on Computer and Information Application (ICCIA)*, 2010, 121-124.

[8] M. Mustaqim, K. Khan, M. Usman, 'LTE-Advanced: Requirements and Technical Challenges for 4G Cellular Network', *Journal of Emerging Trends in Computing and Information Sciences*, 3 (2012) 665-671.

[9] M. Neruda, R. Bestak, 'Evolution of 3GPP Core Network', in *15th International Conference on Systems, Signals and Image Processing, 2008. IWSSIP 2008*, 2008, 25–28.

[10] Y. Ouyang, M. Fallah, 'A Study on Evolving the Architecture of Circuit Switched Domain in UMTS Core Networks', in *Wireless Telecommunications Symposium (WTS)*, 2010, 1-11.

[11] I. Poole, *Cellular Communications Explained: From Basics to 3G* (Oxford: Elsevier, 2006)

[12] A. Qureshi, M. Usman, 'An Optimal Mutual Authentication Scheme in GSM Networks', *Information and Communication Technologies (ICICT)*, 2011, 1-5

[13] M. Rinne, O. Tirkkonen, 'LTE, the Radio Technology Path towards 4G', *Computer Communications*, 33 (2010) 1894-1906.

[14] Sauter, M, *From GSM to LTE* (West Sussex: John Wiley & Sons, Ltd, 2010).

[15] H. Setiawan, H. Ochi, 'Study Feasibility of Common Wireless Communication Services Recognition for GSM, UMTS and LTE', *2009 International Conference on Advanced Technologies for Communications*, 2009, 253-256.

(Received 08 August 2016; accepted 24 August 2016)