International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 537-542 www.ijaem.net ISSN: 2395-5252

SDR base 4G network signal Analysis

Ali, Uche Egwu), Agbo, Levi .C Bassey, Kenneth Akpan
Department of Electrical/Electronic Engineering Technology, Akanu Ibiam Federal Polytechnic Unwana, Afikpo Ebonyi State.

Date of Submission: 15-10-2020 Date of Acceptance: 15-11-2020

ABSTRACT: LTE user equipment (UE) communicates with a base station (BS), when it has decoded some information about the BS. Such information reviews if the BS is accessible by UE. It also indicates the signal bandwidth, BS cell identity, and the identity of the network provider. The master information block (MIB) and the system information block type 1 (SIB1) of the 4G/LTE network holds these information. The information content of these blocks are extracted by capturing and analysing the captured 4Gsignal. This work presents a framework for extracting MIB and SIB1 messages using AD-FMCOMMS3-EBZ SDR kit. The 4G signal received with the kit is processed with Matlab software. We contributed by extending the matlab codes which extract the LTE channels carrying, transporting and broadcasting MIB and SIB1.

I. INTRODUCTION

Owing to numerous advantages of mobile communication network, the rate at which subscribers in this recent time subscribe to it have been of tremendous increase (Gerpott, May, & Nas, 2017). (ITU-D, 2017) shows that worldwide increase in number of subscribers from 2008 – 2017 is 47.9% (Figure 1). To accommodate this increase in subscription rate and to make communication easier, more mobile communication generations is being popped up. The generation have grown from first-fourth generation (1G - 4G). While Huawei just lunch 5G, 6G and 7G are under research (Gawas, 2015) aiming at improving performance and efficiency of mobile communication networks (Mshvidobadze, 2012).

1G being analog was only used for voice conversation. Improvement in 2G included text messaging as means of mobile communication and changed the technology from analog to digital. As it further improve to 3G, included multimedia with high data transmission rate and increased capacity (Mshvidobadze, 2012). Intergration of 3G is integrated with fixed internet formed 4G (LTE) which supports wireless internet. 4G increased the communication bandwidth, raised the quality of service and reduced cost of resources (Vora, 2015). LTE network provides low latency with high data rate and good quality of service. It also supports flexible bandwidth development. Network nodes and LTE systems interfaces are all IP base. 2G, 3G and new spectrumsare utilised by LTE network to It supports handover and roaming to existing networks and utilize 2G and 3G spectrum and new spectrums to work with EDGE, UTMS and GSM systems. It as well supports handover and roaming (Mustaqim, Khan, & Usman, 2012).

Wireless communication technology has reached a stage where exchanges of data between UE's are software defined. SDR technology supports in minimising network congestion. SDR being adaptive and modifiable makes this achievable (Vlachaki, Nikolaidis, Harms, Zhou, & Kunz, 2016). SDR tools are available both in field and academia. There are but not limited to universal software radio peripheral (USRP), HackRF, BladeRF and RTL-SDR.

High speed SDR systems are needed to carry out a combination of communication, data processing, and user interface tasks that have real-time constraint and different processing bandwidth (Cai, Zhou, & Huang, 2017). Such hardware platform must be scalable and robust at same time allowing for system future expansion and improvement. These requirements are fulfilled by Xilinx Zynq-7000 All Programmable SoCs families (eg. ZC706). It is versatile in connectivity, delivers real time data processing with fast speed. AD-FMCOMMS3 provides a configurable data interface to ZC706 by combining integrated frequency synthesisers with mixed signal baseband section and RF front end.FMCOMMS3 chip (AD9361) operates between 70MHz and 6GHz and covers both licensed and unlicensed band. It also supports a channel bandwidth of 200KHz or less to 56MHz through changing of sample rate, decimation and digital filters.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 537-542 www.ijaem.net ISSN: 2395-5252

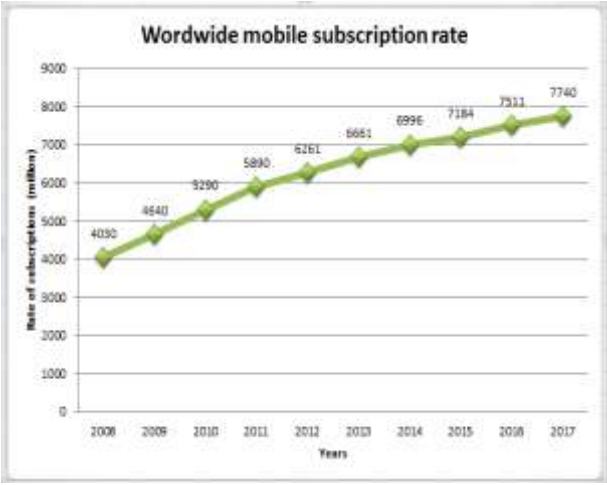

Figure 1: Mobile cellular subscription rate

Lte system information acquisition procedures (summarised)

UE camps on a given cell whenever it is turned ON. It receives system information messages from the cell BS. System information is made of master information block and system information block 1 to13 (SIB1-13). Information about UE camping with the cell and the cell configuration are message contents of MIB and SIB1 (Shi, Chen, & Huang, 2013).

As UE selects a cell, (PLMN) is selected first by non-access stratum layer. PLMN enables radio resource control layer (RRC) to select a cell from the selected PLMN (Labib, Marojevic, Reed, & Zaghloul, 2017).

For UE to select a particular cell, it scan sequentially the supported band to find the cell transmitting the highest signal strength in the supported LTE band. It use Primary and Secondary synchronisation signals (PSS and SSS) to acquire frequency and timing synchronisation. The camped cell ID is then established base on correlation results of locally generated primary synchronisation sequences. It as well acquires frequency and time synchronisations and also gets knowledge of the duplex mode and cyclic prefix type used by the cell (Labib et al., 2017).

At the end of synchronisation, reference signal (RS) is located. RS is used for channel equalisation and cell quality check before MIB is decoded and followed by SIB1 (Labib et al., 2017).

Hardware/receiver setup

The instruction for interconnecting ZC706/FMCOMMS3 and the host computer is given in (MathWorks, 2017). The IP address of ZC706/FMCOMMS3 used in this research is "192.168.1.1". The physical connection is as shown in figure 2. The set is configured based on the characteristics of LTE10 signal (the signal to be captured). Therefore, the signal should have a sampling rate of 15.36MHz and centre frequency of 816MHz (Prasad, Shukla, & Chisab, 2012). The gain is set to slow attack cause LTE signal have rapid change in power level.

Sampling frequency derivation

LTE OFDM symbol duration (T_{OFDM}) is approximated to 71.4µs. It does not change with transmission bandwidth or different FFT size if LTE signal is transmitted with normal cyclic prefix (Su, Lin, & Fan, 2013). That is FFT size of 128 and 1024 have same T_{OFDM}. Also duration of two samples of OFDM symbols varies with FFT size (Demel, Koslowski, & Jondral, 2014).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 537-542 www.ijaem.net ISSN: 2395-5252

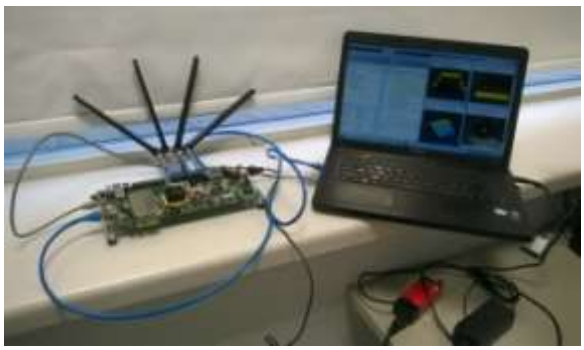

Figure 2: Hardware connection

So, if bandwidth is changed, the sampling frequencies (f_s) changes correspondence to the new bandwidth. LTE central RBs carrying synchronisation signal is within the central LTE bandwidth of 1.4 MHz. So, this central RBs is considered by UE when searching for signal. That is FFT size of 128 which is (N_{FFT}) for 1.4 MHz bandwidth is to be considered. In an OFDM based communication system, sampling frequency,

$$f_s = \Delta f \times N_{FFT} \quad (1)$$

Where the sub-carrier spacing $\Delta f = 15\text{KHz}$. Therefore for a bandwidth of 1.4MHz

$$f_s = 15 \times 128 = 1.92\text{MHz} \quad (2)$$

To retrieve MIB and SIB which is present in this central resource block, the captured signal have to be de-sampled with this rate not minding the actual/configured system bandwidth (Huang, Yongtao, Ying, & Shan, 2012).

Synchronisation

To decode the signal from a BS, its timing and frequency information have to be recovered. Estimation of symbol timing along with primary synchronisation signal (PSS) and secondary synchronisation signal detection are some of the steps taken in timing recovery (Sriharsha, Sreekanth, & Kiran, 2017). Then Fractional Frequency Offset (FFO) and Integer Frequency Offset (IFO) detection are the two types of frequency detection. It is worthy to note that PSS and SSS are not only for synchronisation but also for detecting number of cell ID (N_{ID}**).** BS is identified using its cell N_{ID}**.** Therefore, N_{ID} need to be recovered when synchronising to enable RBs within each frame to be calculated. N_{ID} is as well needed in descrambling and in channel demultiplexing.

Synchronisation process starts with coursing symbol clock recovery. It is completed when the signal redundancy introduced by cyclic prefix (CP) in each OFDM symbol is exploited. The receiver then recovers the symbol timing using a sliding window correlation with a length of N_{CP} and a fixed lag of N_{FFTL} to identify the CPs within the received signals.

$$\gamma(n) = \sum_{m=n}^{n+N_{CP}-1} r(m)r^*(m + N_{FFT}) \quad 3$$

If each symbol start at $n = (N_{CP} + \text{NFFTi}, i \in \mathbb{Z}$ then, correlation output γn peaks a linear slope around it. Coarse estimate of the received signal symbol timing results if magnitude peak detection is used within a search window of one OFDM symbol (Morelli & Moretti, 2017).

PSS and SSS embedded in the transmitter are important for frame recovery. PSS occurs in the transmitter from one out of the three Zadoff-Chu sequences with regard to the Cell Identity number (N_{ID}^2) which enables half frame timing recovery as it is send every 5ms. On the time-frequency grid, PSS is located within the central 6 RBs. It is detected by a correlation of the received signal with all Zadoff-Chu sequence send out by the transmitter (Huang et al., 2012).

Physical cell id determination

LTE system has 504 distinct cell IDs grouped into 168 cell ID groups with 3 unique sector numbers (Su et al., 2013). Thus, equation 4.3 uniquely defines a cell ID.

$$N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)} \quad 4$$

Where; $N_{ID}^{(1)} \in \{0, 1, 2, \ldots\ldots, 167\}$ is the cell ID group. It is identified through SSS sequence and $N_{ID}^{(2)} \in \{0, 1, 2\}$is IDs within a group and corresponds to ZC root indices (25, 29, 34). Once Z root index is identified through non-coherent detection, it will be used to identify the corresponding $N_{ID}^{(2)}$ (Sriharsha et al., 2017).

Pbch decoding and mib data identification

After synchronisation and Physical cell ID determination, PBCH which carries MIB data is decoded. PBCH being mapped to the central 72 subcarriers (corresponding to the minimum possible LTE system bandwidth (6 RBs) of the OFDM signal makes it possible for UE to detect

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 537-542 www.ijaem.net ISSN: 2395-5252

LTE network without having prior knowledge of the bandwidth (Demel et al.,
2015). The UE identifies centre frequency from PSS and SSS. Figure 3 is a block diagram showing PBCH signal processing procedures.

When SFN mod 4 = 0, MIB data is send in 40ms. If MIB is to be identified, data have to be extracted in 40ms time when decoding PBCH (Rupasinghe & Guvenc, 2015). With the 6 centre RBs sampling rate (1.92MHz), one slot duration samples ($N_{slot}^{samples}$) is

$$\left(N_{slot}^{samples}\right) = 1.92 \times 10^{6} \times 0.5 \times 10^{-3} = 960 \quad 5$$

Therefore samples needed to capture data at 40ms duration is

$$\left(N_{40ms}^{samples}\right) = 960 \times 2 \times 40 = 96800 \quad 6$$

$(N_{40ms}^{samples})$ is the amount of samples in the recorded data to be extracted for decoding MIB. For better reliability, 80ms of data was extracted in this paper. Therefore 153600 samples of data were extracted from collected data for analysis in MATLAB.

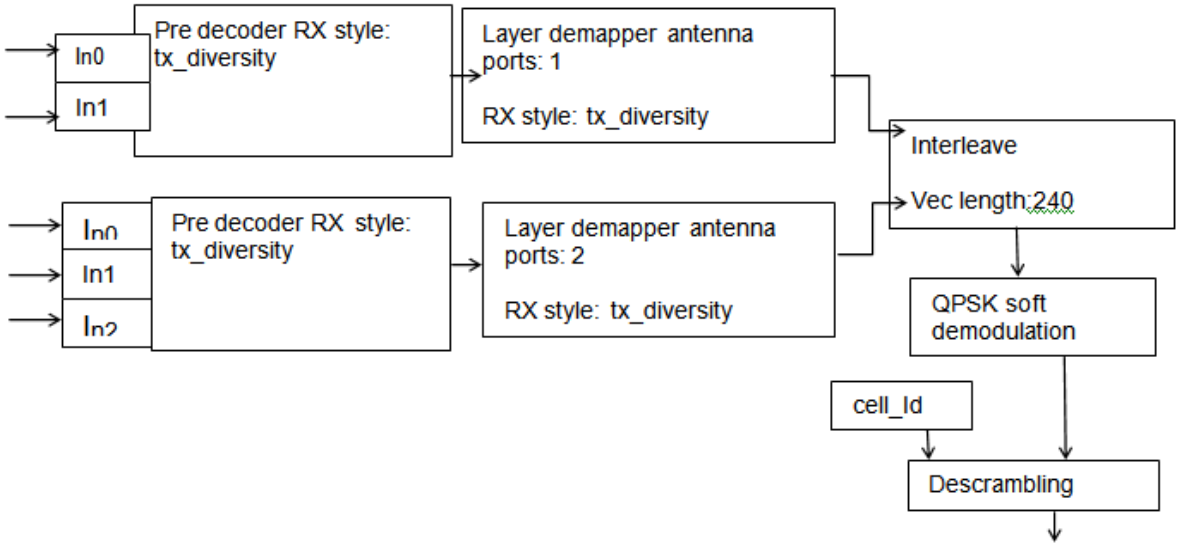

Figure 3: PBCH signal decoding procedures

Data analysis in matlab

The samples in the recorded data are down-sampled in order to analyse the sample contained at the central 6RBs. First cell search which enables cyclic prefix length and duplex mode detection is carried out on the down-sampled samples using the matlab function enb.CyclicPrefix and enb.DuplexMode respectively. Cell search continues across combination of the detected cyclic prefix length and duplex mode. The combination with highest correlation is recorded as it contains the cell identity number. The number of cell identity is extracted with the matlab function enb.NCellID (Sriharsha et al., 2017).

Timing synchronisation and frequency offset estimation/correction is further perform using the matlab function lteFrequencyOffset before OFDM demodulation and channel estimation. The matlab function lte OFDMD emodulation and lteDL Channel Estimation are use to perform these.

To recover MIB bit, the resource elements (REs) corresponding to the PBCH from first subframe across all receive antennas and channel estimates using the matlab function lteExtractResources. This is followed by PBCH decoding and MIB bits parsing (Demel et al., 2014).

MIB bit parsing enables the information content of MIB to be made known. One of the information is the system full bandwidth. To recover SIB1 information content, OFDM demodulation, frequency offset estimation and correction is repeated considering the system full bandwidth. Remember, SIB1 (Rupasinghe & Guvenc, 2015)

II. RESULT AND DISCUSSION

The downlink LTE signal with centre frequency 816MHz and sampling rate of 15.36MHz is captured using AD-FMCOMMS3-EBZ SDR as explained in section II. The signal was captured in Electronic CAD lab which is located in level three of sheaf building in Sheffield Hallam University City campus. Table 1

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 537-542 www.ijaem.net ISSN: 2395-5252

summarises the information obtained from the captured LTE signal.

Full correlation of PSS, SSS and MIB decoding is achieved with the developed Matlab program. It is worthy to note that if the signal to interference plus noise plus ratio (SINR) is unaccepted, MIB will not be decoded and the matlab program indicates error in matlab command window.

Figure 4 is the correlated PSS and SSS diagram showing first PSS sequence carrying OFDM symbol that can be identified. It shows that the value of the starting sample from 7th OFDM symbol in 0th slot of a sub-frame is 3627.

Table 1: Processed signal information content

Parameter	Value
Timing offset	3627 samples
Frequency offset	-1982.360Hz
MIB:	
No. of resource blocks	**50**
Duplex Mode	**FDD**
Cyclic Prefix	**Normal**
NCellID	**26**
Number of subframe	**0**
No. of antenna ports	**2**
PHICH duration	**Normal**
Ng	**one**
No. of frame	**369**

From the information in table 1 above, the captured signal was transmitted by a cell with cell ID 26. This cell is configured using FDD and normal cyclic prefix. The first detected PSS sequence of the cell carrying OFDM symbol is identified with the value 3627 samples (Figure 4). Frequency offset of the capture is -1982.360Hz which is less than the maximum amount possible to experience channel interference.

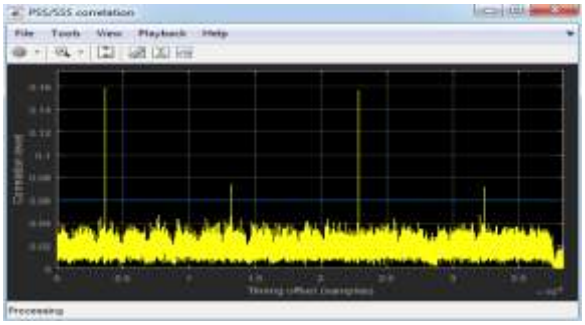

Figure 3: The correlated PSS and SSS diagram

Other MIB information as seen from table 1 above are the cell parameters such as the cell ID, cell bandwidth, cell duplex mode, cyclic prefix, number of sub-frame, number of antenna ports, PHICH duration, PHICH group (Ng) and number of frame These are necessary for the UE to camp to the base station and decode system information type 1 as well as other system information.

III. CONCLUSION

This work aim at capturing an LTE signal with software defined radio kit and process the signal in Matlab software. Fundamental idea on how data is transported from the base station to UE and how user equipment can gain access to the base station was given. This work gives better understanding of wireless network/LTE network to a student or professional embarking in a related research. The object of this research was achieved since the MIB information in the captured signal was deduced. The result shows that the captured signal is broadcasted by a cell with cell ID 26 and 50 resource blocks which indicates that it is an LTE10 signal.

RFERENCES

[1]. Cai, X., Zhou, M., & Huang, X. (2017). Model-Based Design for Software Defined radio on an FPGA. IEEE Access., 5, 8276-8283.

[2]. Demel, J., Koslowski, S., & Jondral, F. K. (2014). A LTE Receiver Framework Using GNU Radio. Journal of signal processing systems, 78(3), 313-320.

[3]. Demel, J., Koslowski, S., & Jondral, F. K. (2015). A LTE Receiver Framework Using GNU Radio. Journal of signal processing system, 313-320.

[4]. Gawas, A. U. (2015). An overview on evolution of mobile wireless communication networks: 1G-6G. International Journal on Recent and Innovation Trends in Computing and Communication, 3(5), 3130-3133.

[5]. Gerpott, T. J., May, S., & Nas, G. (2017). The impact of mobile Internet on mobile voice usage: A two-level analysis of mobile communications customers in a GCC country. Information & Management, 54(7), 958-970.

[6]. Huang, S., Yongtao, S., Ying, H., & Shan, T. (2012). Joint time and frequency offset estimation in LTE downlink. International ICST Conference on Communications and Networking (pp. 394-398). China: IEEE.

[7]. ITU-D. (2017, sept. 25). ICT facts and figures. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

[8]. Labib, M., Marojevic, V., Reed, J. H., & Zaghloul, A. I. (2017). Enhancing the robustness of LTE systems: Analysis and evolution of the cell selection process. IEEE communication magazine, 55(2), 208-215.

[9]. MathWorks. (2017). Guided Host-Radio hardware Setup (2017a). Retrieved 09 04, 2017,fromhttps://uk.mathworks.com/help/supportpkg/xilinxzynqbasedradio/ug/guided-host-radio-hardware-setup.html

[10]. Morelli, M., & Moretti, M. (2017). A maximum likelihood for SSS detection on LTE systems. IEEE Transactions on wireless communication, 2423-2433.

[11]. Mshvidobadze, T. (2012). Evolution mobile wireless communication and LTE networks. international Conference on Application of Information and Communication Technologies (AICT) (pp. 1-7). IEEE.

[12]. Mustaqim, M., Khan, K., & Usman, M. (2012). LTE-Advanced: Requirements and Technical Chanllenges for 4G Cellular Network. Journal of Emerging trends in Computing and Information Sciences, 3(5), 665-671.

[13]. Prasad, S. S., Shukla, c. k., & Chisab, R. F. (2012). Performance Analysis of OFDMA in LTE. Computing Communication & Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[14]. Rupasinghe, N., & Guvenc, I. (2015). Capturing, recording, and Analysing LTE Signals Using USRPs and Lab VIEW. IEEE SoutheastCon. Florida: IEEE.

[15]. Shi, Z., Chen, P., & Huang, L. (2013). A new efficient dynamic system information scheduling strategy in TDD-LTE. telkomnika, 11(9), 5480-5489.

[16]. Sriharsha, M. R., Sreekanth, D., & Kiran, K. (2017). A complete cell search and synchronisation in LTE. EURASIP Journal on wireless communication and networking., 1-14.

[17]. Su, S.-L., Lin, Y.-C., & Fan, Y.-J. (2013). Joint sector identity and integer part of carrier frequency offset detection by phase-difference in long term evolution cell search process. IET Journals & magazines, 7(10), 950-959.

[18]. Su, S.-L., Lin, Y.-C., & fan, Y.-J. (2013). Joint sector identity and integer part of carrier frequency offset detection by phase-difference in long term evolution cell search process. IET journals & magazines, 7(10), 950-959.

[19]. Vlachaki, A., Nikolaidis, l., Harms, J. J., Zhou, Y., & Kunz, T. (2016). Towards Dynamic Wireless Capacity management for the Masses. International conference on Ad Hoc Networks (ADHOCNETS) (pp. 155-166). EAI.

[20]. Vora, l. J. (2015). Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G. International Journal of Modern Trends in Engineering and Research, 2(10), 281-290.