A New Location-Based Service Architecture with Efficient Transmission Method Using Control Channels

Mohammed I. A. Aal-Nouman

Submitted in partial fulfilment of the requirement for the degree of

Doctor of Philosophy

University of Salford

School of Computing, Science and Engineering

2017

Table of Contents

List of Tables

List of Figures

Publications

- “Location-Based Services by Clustering Distributed Databases in Mobile Networks” Poster abstract research showcase college of Science and Technology university of Salford, UK **2014**.
- Work-in-Progress: Design an Efficient Data Transmission for LBS Using Random Access Channel in UMTS” LBS conference, Augsburg, Germany **2015**.
- SPARC 2015 Salford postgraduate annual research conference “Location-Based Services for Mobile Network by Clustering Distributed Databases” Salford, **2015**.
- Full conference paper "Efficient Communications for Location-Based Services Using Spare Extensions of Control Channels in Mobile Networks," **2016** IEEE, 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus **2016**.
- Full conference paper “Efficient message transmission method for in-vehicle emergency service”, IEEE 6th International Conference on Information Communication and Management (ICICM). Hatfield, UK **2016**.
- Full conference paper “A new architecture for location-based services core network to preserve user privacy," IEEE 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, **2017**.
- Full journal paper “Disaster Early Warning Messages via Control Channels of the Mobile Network” published in Elsevier, Journal of Telematics and Informatics November **2017**
- Full journal paper “Transmission of Emergency Medical Messages for Patients Using Control Signal of Cellular Network ” submitted to Elsevier Journal of Computer Communications since November **2017**

Acknowledgements

While my name may be alone on the front cover of this thesis, I am by no means its sole contributor. Rather, there are a number of people behind this piece of work who deserve to be both acknowledged and thanked.

Firstly, many thanks to my parents for showing faith in me. I salute them all for the selfless love, care, pain and sacrifice you made to shape my life. I would never be able to pay back the love and affection shown to me by my parents, and thanks to all my family and friends who have supported and continue to support me in my life.

In addition, special thanks to my beautiful wife, Amenah, for her patience, constant support and unconditional love. She was always around at times I thought it impossible to continue, and she helped me to keep things in perspective. I greatly value her contribution and deeply appreciate her belief in me. And many thank for her parents for their support. Also, I do not forget my lovely daughter, Sara, and son, Ibrahim, whose smiles brightened the hardest days.

Also, many thanks to the University of Salford who offered help when needed and particularly to my supervisor, Professor Haifa Takruri-Rizk, for the valuable guidance, advice and non-stop support during my PhD journey.

Finally, I would like to thank the Ministry of Higher Education and Scientific Research of Iraq for funding the PhD study and Al-Nahrain University for nominating me for this scholarship, as well as the Iraqi Cultural Attaché in London for all their help throughout the study.

DEDICATED TO MY FAMILY

Abbreviations

2G	Second generation
3G	Third generation
3GPP	3rd Generation Partnership Project
AAL2	Adaptation Layer 2
AAL5	Adaptation Layer 5
A-GNSS	Assisted GNSS
AI	Acquisition Indicator
AICH	Acquisition Indicator Channel
ATM	Asynchronous Transfer Mode
AuC	authentication centre
BCH	Broadcast Channel
CCCH	Control channel
CID	channel identifier
CLP	Cell Loss Priority
CN	Core Network
CN	Core Network
CPICH	Common Pilot Channel
CPS	common part sublayer
CRC	cycle redundancy check
CSFB	circuit switched fallback
C-RNTI	Cell Radio Network Temporary Identities
DCH	The Dedicated Channel
DPCCH	Dedicated Physical Control Channel
DPCH	Dedicated Physical Channel
DPDCH	Dedicated Physical Data Channel
E-AGCH	E–DCH Absolute Grant Channel
E-DCH	enhanced dedicated channel
E-DPCCH	EDCH Dedicated Physical Control Channel
E-DPDCH	Dedicated Physical Data Channel
E-HICH	EDCH Hybrid ARQ Indicator Channel
EIR	Equipment identity register
EPS	Evolved Packet System

E-RGCH	the E-DCH Relative Grant Channel
ETSI	European Telecommunications Standards Institute
FACH	forward access channel
F-DPCH	the Fractional Dedicated Physical Channel
FTPICH	Fractional Transmitted Pre-coding Indicator Channel
GFC	Generic Flow Control
GGSN	Gateway GPRS Support Node
GMLC	Gateway location mobile centre
GMSC	Gateway MSC
GNSS	global navigation satellite system
GPS	Global poisoning system
GSM	Global System for Mobile Communications
HEC	Header Error Control
HLR	Home location register
HSDPCCH	Dedicated Control Channel associated with HS-DSCH transmission
HS-PDSCH	High Speed Physical Downlink Shared Channel
HS-SCCH	High Speed Shared Control Channel
PICH	Physical indicator channels
IE	information element
IE FI	information flags indicator
IMS	IP Multimedia Subsystem
ITU	International Telecommunication Union
LBS	Location-based service
LCS	Location service
LI	length indictor
LTE	Long term evolution
LTE-A	LTE Advance
M-FSK	Multiple frequency-shift keying
MME	Mobility Management Entity
MSC	Mobile switching centre server
NI	Notification Indicator
OTDOA	observed time difference of Arrival
OVSF	Orthogonal Variable Spreading Factor

P-CCPCH	Primary Common Control Physical Channel
PCH	Paging Channel
PI	Page Indicator
PICH	Paging Indicator Channel
PLMN	public land mobile network
POI	point of interest
PPT	packet payload type
PRACH	physical random access channel
PS	Packet Switch
PSAP	public safety answering point
PT	Payload Type
QoS	Quality of service
QPSK	quaternary phase shift keying
RACH	random access control channel
R-GMLC	requesting GMLC
RLC	Radio Link Control protocol
RNC	Radio Network Controller
RNS	Radio Network Subsystems
RRC	Radio Resource Control
SC	Circuit Switch
S-CCPCH	secondary common control physical channel
SCH	Synchronization Channel
SDH	Synchronous Digital Hierarchy
S-DPCCH	Secondary Dedicated Physical Control Channel
SF	spreading factor
SGSN	Serving GPRS Support Node
SMS	Short message system
SONET	Synchronous Optical Networking
SSCS	service specific conversion sublayer
TB	transport block
TFCI	Transport Format Combination Indicator
TFI	Transport Format Indicator
UE	User equipment

UMTS	Universal Mobile Telecommunications Service
U-RNTI	UTRA Radio Network Temporary Identities
USIM	Universal Subscriber Identity Module
USSD	unstructured supplementary service data
U-TDOA	Uplink-Time Difference of Arrival
UTRA	Universal Terrestrial Radio Access
UTRAN	universal terrestrial radio access network
UUI	user-to-user indication
V2I	vehicle to infrastructure
V2V	vehicle to vehicle
VCI	Virtual Channel Identifier
V-GMLC	visited GMLC
VLR	Visitor Location Register
VoLTE	Voice over LTE
VPI	Virtual Path Identifier
WCDMA	wideband code division multiple access
XML	Extensible Mark-up Language

Abstract

Location-based services (LBS) are services that are provided to users according to their location; these services can either be provided to the user when requested (pulled), for example, when the user asks, "Where is the nearest hospital?" or sent automatically (pushed) when the user's location changes, such as in commercial advertising.

The main components of the LBS needed to secure an end to end service are: mobile terminal, positioning system, communications network, and service and data provider. In general, the communication network used to transfer the data between the user and the data and service provider is the Internet. Therefore, if the user is offline because of the Internet connection is unavailable or damaged, the LBS cannot be completed, and the mobile operator cannot exchange data with the data and service provider.

There are some qualities of service that are essential to achieve a good service in LBS like security, privacy, response time, coverage and many others. In a standard architecture, the data and service provider are an external third-party company, but this raises some concerns regarding response time and user privacy, as the user information could be shared.

To solve the problem regarding disconnection, a solution is proposed to use the spare extension of the random access channel (RACH), which is carried by the physical random access channel (PRACH) for the uplink to send the user request to the core network. Then, the spare extension of the forward access channel (FACH) will be used, which is carried by secondary common physical control channel (S-CCPCH) for the downlink to send the location information from the core network to the user. Moreover, to solve the privacy and response time issues, a database is attached to the gateway mobile location centre (GMLC) in the core network of mobile operator to act as a data and service provider. Thus, there is no need for the request and the information to be sent to a third-party company anymore.

One of the main contributions of this research is the end to end connection between the user and the service provider being always available, even if the Internet is unavailable. Also, the user obtains the information faster in a secure and confidential way as this information are not being shared with other parties.

Matlab is used as a simulation tool in this research. The results show that the connection between the user and the data provider is used successfully; the request and the data are sent using the RACH and FACH; the response time has been reduced; and the user privacy is enhanced.

Chapter One: Introduction

Location-based services (LBS) are computer programme-level services that use the location of the users to provide some services to them. LBS can be accessed by mobile devices through the mobile network, which uses geographical information to find the user position. With the expansion of smartphone and tablet use, LBS have become more important, as they can be used in location finding, navigation, advertising, emergency service and more [1-4] LBS can be query-based and provide the user with useful information such as answers to "Where is the nearest hospital?" or they can be push-based and deliver marketing information or disaster warning messages to customers based on their location [5]. LBS architecture basically comprises the following components [4, 6-8]:

- **Mobile Devices**: where the request is sent by the user to the data provider, and back again from the service and data provider to the user via the communication network; the data could be presented to the user as speech, pictures, text or any other form.
- **Communication Network**: the mobile network, which carries the user request from the mobile device to the service provider and then carries the information back to the user.
- **Positioning Component**: the location of the user has to be found and determined before being serviced by LBS. The location can be found and calculated either by mobile network assistant or by using the Global Positioning System (GPS).
- **Service and Application Provider**: provides service request processing such as position calculation, route finding or searching specific information.
- **Data and Content Provider**: accesses data that the user has requested, like information or the location of a specific place. The data provider usually is a third-party company [9, 10].

So, for an LBS system to be successful, the user's position must be found, and a communication network to send and receive the user request and the location information must be available. In addition, the Location Services (LCS) server and services provider having to be available to provide the requested data to the user. Figure 1-1 shows an example of LBS components [3, 7].

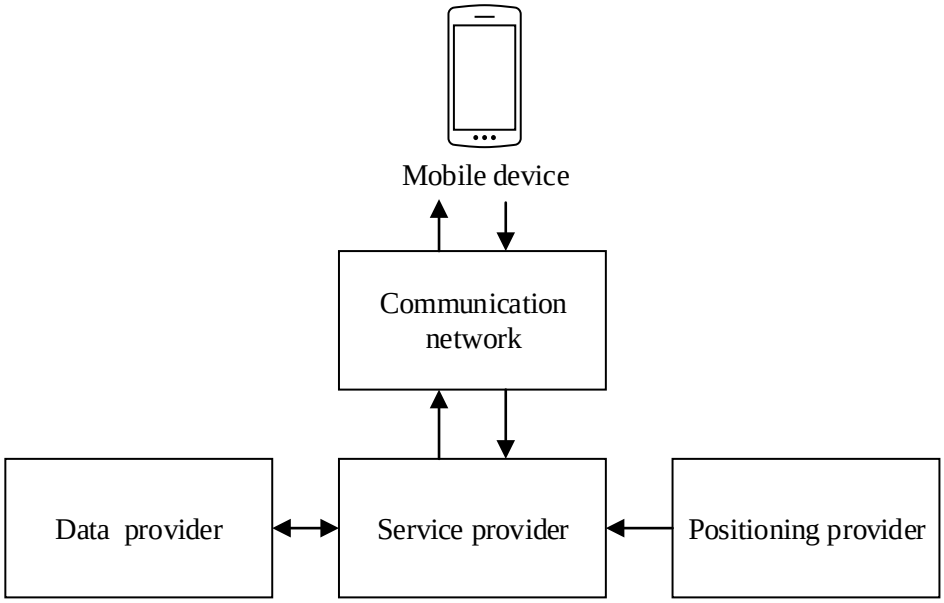


Figure 1-1 LBS components

In the 3GPP standard and majority of LBS systems, the communication network used between the user and the data provider is the Internet [11]. It could be transferred via the data channel of the mobile network to the core network and then sent to a third-party data provider which is external to the mobile operator network.

The size of the data sent from the user request is small, as the user usually searches or navigates on a point of interest like a specific hospital or a hotel. This also applies for the information coming from the data provider, as it is usually a coordinate i.e. latitude and longitude.

1.1 Research Problem

The location-based service, as aforementioned, uses the Internet to communicate between the user and the data provider. In some cases, like roaming abroad or in the case of rural areas or even on a motorway or rural areas, the Internet connection is unavailable or limited [12-14]. This leads to loss of the LBS service. Additionally, this can occur in a crowded place where the network is overloaded and the connection cannot be established even though the user is within the network coverage.

There is another problem in the LBS that this thesis solves, which is the user privacy invasion; because the LBS systems uses a third party data provider, the location and the user information will be shared and invaded. Moreover, the response time to send the data to an

external party will be increased and the possibilities of the packet drop or loss will be increased as well.

1.2 Research Motivation

There are many situations where the user has an urgent requirement to be connected to a service provider, like in an emergency service after an accident, monitoring an unwell patient remotely, or sending natural disaster information.

According to statistics from the World Health Organisation, the primary cause of death worldwide for those aged between 15 and 29 is from road traffic injuries, as can be seen in Figure 1-2 [15]. In fact, in 2013 around 1770 deaths in the United Kingdom alone were caused by traffic accidents, and that number is even higher in other countries. In some cases the numbers exceed 200,000 per year for large population countries like China and India [16, 17].

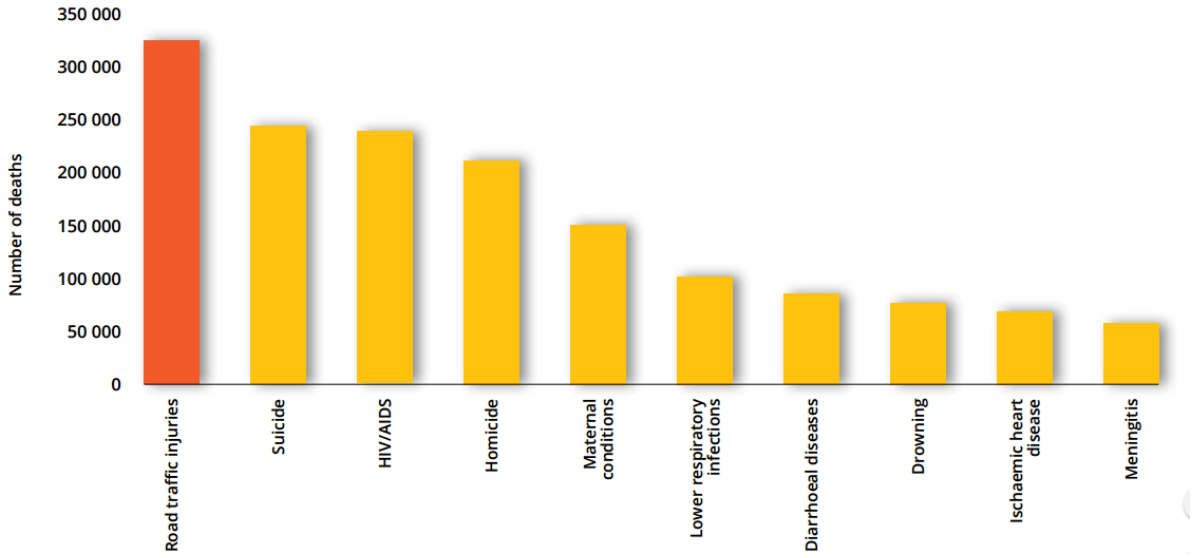


Figure 1-2 Top Causes of Death Among People Aged 15–29 Years Old, 2013

Therefore, it is very important that the person who is involved in an accident is able to communicate with the public safety answering point (PSAP) or at least find an emergency service nearby like a hospital.

Also, The World Health Organization (WHO) has given priority to eHealth systems since 2005. eHealth is any technology that uses secure information and communication to support any field related to health, like health monitoring and surveillance, health-care services, and health education [18].

One of the most important requirements for healthcare is that people can access and be provided with healthcare services anytime and anywhere [19]. One of the major challenges is to provide healthcare services to the patients at all times [20, 21]. That means the e-healthcare systems must secure a connection and communication line between the patient and the healthcare centre. Most of the applications and systems used in the healthcare services use the Internet to send the patient monitoring information to the hospital [19, 21-25].

In another aspect, according to UN office for disaster risk reduction (UNISDR), centre for research on the epidemiology of disasters (CRED): the average number of annual death from natural disasters is about 99,700 for the period between 2004 and 2013. While the average numbers of people affected by natural disasters annually is around 175 million per year for the same period and 260 million annually for the period between 1994 and 2003 [26].

To prevent the unnecessary death, countries around the globe now recognize that warning systems is one of the important part of risk management [27] which could help save more live in the future [26, 28].

Many meetings and agreements around the globe tried to set goals and targets to prevent or reduce the natural disaster effects on the human life [29] by making the early warning systems and disaster risk information available to all people whenever they are [30, 31]. These early warnings would help people to receive the disaster information in order to promote early evacuation [32]. These warning messages are not only used to warn people about the disaster but they could also be used after the disaster to provide or ask for support, like blood donations [32, 33] and shelter or any other resources [34].

The most common method used to send the warning messages is the Internet (Wi-Fi or packed channel of the mobile network). However, the Internet may not always be available in some areas like rural areas or motorways or in locations where there are many users like stadiums or concert theatres and the network could be overloaded. In the rural areas, where the communication network could be poor, the information and communication provider sector faces a number of problems, as in such areas there is really a need for warning systems and emergency services [35]. There are thus studies, which show that rural areas have lagged behind compared to the major cities with respect to Internet access and speed [12-14]. Some studies shows that rural and suburban areas cannot secure a fixed connection to the Internet, and in some cases they can only get a slow, unreliable connection [36]. Other study shows only 30% of rural and suburban areas can access to the Internet using the mobile network

[37]. Moreover, the coverage of the Internet serviced by mobile networks is focusing on the population not on the amount of area covered in LTE deployment; that leads to skipping areas with low population [38].

In a standard architecture, the data and service provider are an external third-party company, but this raises some concerns regarding response time and user privacy, as the user information could be shared. Studies show that many users have concern about their information to be shared and they believed that it is important to have their location information kept confidential, especially if it could be shared with commercial advertising agents [39-41].

Thus, it is clear there is a need for a solution to solve any problem that may occur in the communication between the user and the data and service provider whilst simultaneously protecting the user's information and privacy.

That would give a motivation to the governments to adopted the emergency service to the users and put some regulations and policies to the mobile operator to add a location-based service database into their core network to be used for emergency cases. And also enable disaster warning messages and emergency information to be sent over control channels when the user has no internet connection and wants to get an urgent service to save his/hers live.

1.3 Aim and Objectives

The aim of this research is to design an LBS that is able to complete the user request without using the Internet or the packet channel of the mobile network while preserving the user privacy by avoid using a third party to provide location information to the LBS.

To achieve the aim of the research the following objectives need to be fulfilled:

- Build a model for the uplink channel to send the user request to the core network via universal terrestrial radio access network (UTRAN) using a new method which use the spare extension of the random access control channel (RACH), which is carried by the physical random access channel (PRACH).
- Build a downlink model to send the location information that the user asked for from the core network to the mobile user using a new method that use the spare extension of the forward access channel (FACH), which is carried by the secondary common control physical channel (S-CCPCH).
- Mathematically modelling the uplink and the downlink channel.

- Build a backhaul connection between UTRAN and the mobile operator's core network in order to exchange the information between the data provider and the user.
- Build a database, which contains location information and attach it to the GMLC of the mobile network.
- Design a new architecture for the mobile core network to use a database that attached to the GMLC as a data provider instead of using a third party data provider.
- Design a solution for the core network architecture where the system has more than one GMLC in its core networks.
- Validate the results for the mathematical models with the simulation results and compare the simulation results with 3GPP standard architectures to evaluate it.

1.4 Research Contribution

In this thesis a new method is proposed to send the user request to the LBS service and data provider using the spare extension of the RACH, and then send the information back to the user from the core network using the spare extension of the FACH.

Furthermore, the mathematical model of the 3GPP standard and the proposed method for the RACH and FACH are presented in this thesis in order to compare between the two methods to validate the proposed method.

The new method will help the users to get an alternative channel to send their request to the LBS provider when the Internet is unavailable. Over and above, when the Internet is available the proposed solution will send the data faster than other systems

Also, the thesis proposed a new architecture by migrating the LBS database from a third party provider to the core network. By using the proposed architecture, the user information will be safe and the user privacy is protected. Moreover, the time between requesting and getting the information from the data provider will be reduced, as will the chance of interference.

1.5 Possible Research Application

The location-based service has no limit to its applications, as it could be any application as long as the user's location is involved. However, the research in this thesis focused on those applications where the user has no Internet connection and needs to find a specific point of interest, like emergency service, disaster warning messages or e-healthcare in rural areas. For example, if an accident happened on a motorway and the Internet coverage was unavailable, the request and location information would travel via the RACH and FACH.

Another possible application is when the user travels abroad and tries to find a hotel or any specific location. The visited mobile operator will serve the user as a roaming user and could charge an extra cost for the Internet, and in some cases it could serve with voice only service (no Internet). So, the solution will provide LBS over the control signals RACH and FACH. Additionally, the solution could be very useful in a crowded place like a stadium, where the network could be overloaded, but the use of the proposed solution will help to send and receive the data when needed and because the size of user request and location information are small the control signal will not be overloaded.

1.6 Research Roadmap

In order to achieve the aim and objectives of this research, the research takes many stages to reach its final form, these steps are (Figure 1-3):

1. **Identify the latest technology in LBS** by reading and investigating most recent published work to define what the location-based service is and what type of technology and methods are used in the communication network between the user and the data provider. Also, investigate what the LBS component and core network architecture are.
2. **Identify the problem of LBS;** the problem in the communication network was found to be when the user has no Internet connection or when there is an overload on the network. Also, user privacy has been found to be jeopardized, as information are shared with a third party companies.
3. **Doing the literature review** to check what are the latest available solutions to solve the problem mentioned in the previous step. There are new standards released by third general partnership project (3GPP) to solve the communication problem and many researchers have proposed various methods for solving the communication and the privacy issues.
4. **Propose a solution** to solve the issues mentioned above in the LBS; this can be divided into multiple stages:
    A. Solving the problem related to the communication between the user and the core network, which is also divided into two stages, including the uplink where the user sends the request to the data provider and the downlink where the data provider sends the information to the user.

B. Solving the problem related to the core network to solve the privacy issue by adding a database to the core network, and taking into consideration the network configuration where it could have more than one GMLC.

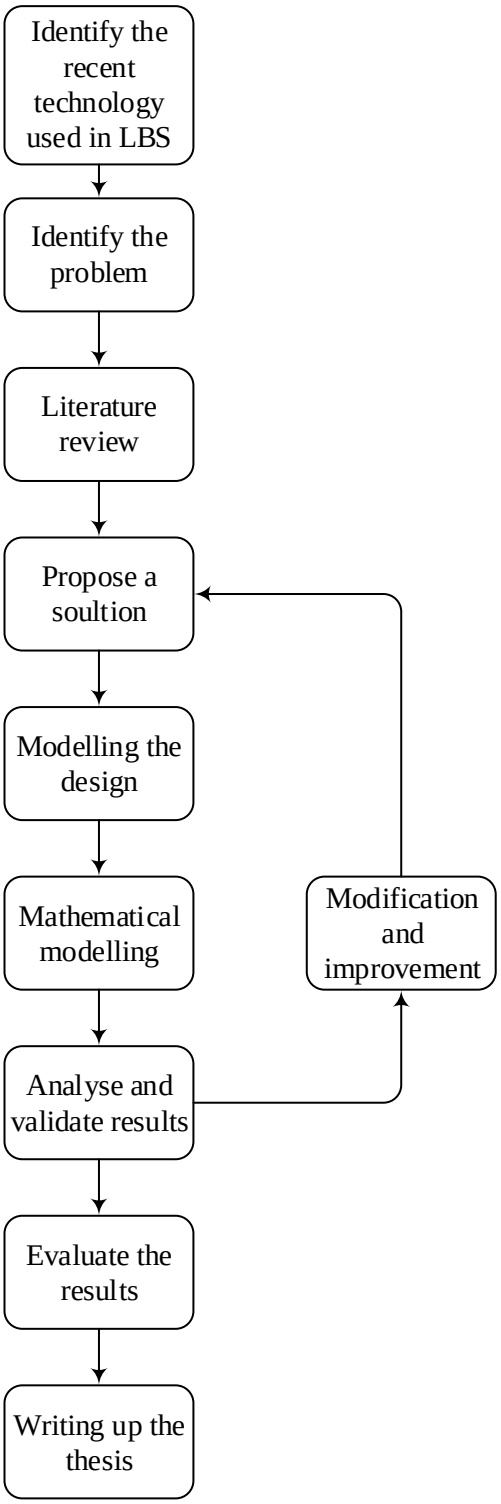


Figure 1-3 Research Roadmap

5. **Modelling the proposed design** in Matlab by building the frame structure of the control channel that is used to carry the information and the request to and from the user.
6. **Formulate the input and the output** by building the mathematical model for the frame structure of the uplink and the downlink in both after and before the proposed solution.
7. **Add finishing parameter and steps** like implementing the backhaul from the core network to the radio access network, and adding the required functions to calculate the cycle redundancy check (CRC) and modulate the signal.
8. **Publish the work in journals and present at conferences**; the results have been presented in three conferences: one for the uplink stage, another for the uplink and the downlink, and the final one for the new architecture for the core network. In addition, there are another two journal papers for evaluate and validate the transmission methods.
9. **Validate the design** by comparing the result from the simulation with the results obtained from the mathematical model, as well as comparing the system behaviour with the standard to validate it.
10. **Evaluate the result** by comparing the result from the proposed design with the results from other similar works, by simulating them with their selected parameter and design.
11. **Document and present the results** by writing up all the required theories from the background to the standard then present the results and discuss them.

1.7 Structure of the Thesis

In ***chapter one*** the motivation of the work is explained along with research problem, research contribution and possible applications that can be applied for the proposed solution.

To understand the proposed solution, ***Chapter two*** presents the background of the location-based service and components. The requirements of the LBS system to achieve good quality of service are also demonstrated in the chapter.

Also, ***Chapter three*** explains the mobile network background and system architecture, in addition to the channels and the frame structures of those channels. The procedure needed to complete the data transfer from the mobile is also described.

Chapter four constitutes the literature review and reviews the similar research in the location based service communication field, together with methods used to protect the user privacy.
The proposed solution is shown in ***Chapter five*** with its three main stages, namely the uplink stage, the downlink stage, and the core network stage, and finally, the backhaul to connect the whole network together is also presented in this chapter.
Chapter six introduces the mathematical channel model for the standard and for the proposed design for the uplink and downlink stages.
All the results and findings are shown in ***Chapter seven***, where the comparison between the proposed designs of other systems is shown. Furthermore, the comparison between the mathematical model results and the simulation results are shown in this chapter.
Finally, ***Chapter eight*** shows the conclusion for the system and the results with the possible extended future work.

Chapter Two: Location-Based Services

The development of smartphones and mobile devices has made these devices an essential everyday tool used in every aspect of our lives and making the life easier. One of the many is the services that are based on the user's location, known as location-based services (LBS). LBS are services that are provided to the user according to their location. These services can either be sent to the user when requested (pulled), or sent automatically by the service provider (pushed) [42].

A large range of LBS are currently provided by service providers, offering services like navigation when the user navigates a road, information about places, games that depend on the location, advertising to the user when they are near a shop or a market, giving the nearest location of specific points of interest such as a park or hospital, or even requesting or getting an emergency service [1, 2, 4, 17].

2.1 LBS Components

Technologically, the main component of LBS can be classified into four main tiers: *the user, Communication Network, Positioning Component, Service and data Provider* [43] as can be seen in Figure 2-1.

The user is the person who asks for the location service, such as navigation or looking for a point of interest, and to send the user's request to the service provider, a device like a mobile phone is needed. Of course, in order to obtain such a service, the network should know the user's location first, so *the positioning component* will find the location; there are many ways to find the user's location, but the most well-known is the GPS. Other methods use cellular network signals. Once the user's position is known to the system, a *communication network* is needed to transfer the user information such as the location along with the user request to the service and data provider. In a normal system and 3GPP standard where the user uses the mobile phone, the Internet is used to send the information [3, 17, 44, 45]. *The service provider* sends the user's request to the data provider who in turn checks its location service (LCS) database and sends the requested information back to the user via the communication network.

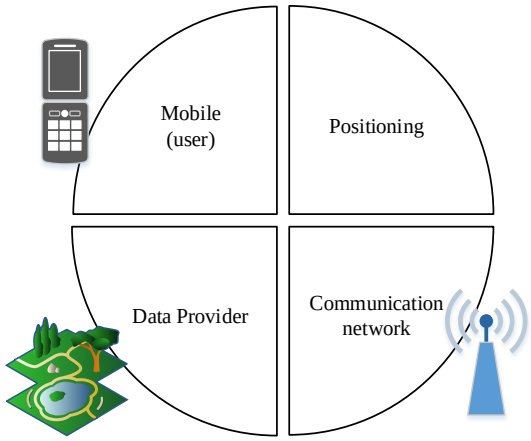


Figure 2-1 LBS Components

As aforementioned, there are many positioning techniques that are used to find the user location in GSM, UMTS and LTE. In a 3G network – similar to 2G - the UTRAN can use one of the positioning methods to locate the User Equipment (UE). To find the position of the UE, two main steps are taken: signal measurements, and then position estimate and computation based on the measurements [46].

There are many techniques used for UE positioning, namely: cell ID-based, observed time difference of arrival (OTDOA), global navigation satellite system (GNSS) and uplink-time difference of arrival (U-TDOA) [46]. While the positioning methods that are used in LTE are: OTDOA, assisted GNSS (A-GNSS) and enhanced cell ID positioning [47]. The ETSI/3GPP standardisation has defined a general LCS for UMTS architecture to be able to find the mobile phone's position even when the phone is not equipped with GPS.

2.2 LBS Architecture

The LBS, like any system, has a standard architecture even though many researchers have changed some of the architecture and standards. The standard architecture of any LBS system has many elements, which are merged with the mobile network elements. The GMLC and the LCS clients are the elements that are used in the LBS architecture and have information about user and service location [11]. The other elements and components that are part of the mobile network will be explained in the next chapter. Figure 2-2 shows the basic architecture of LBS within the mobile network [8].

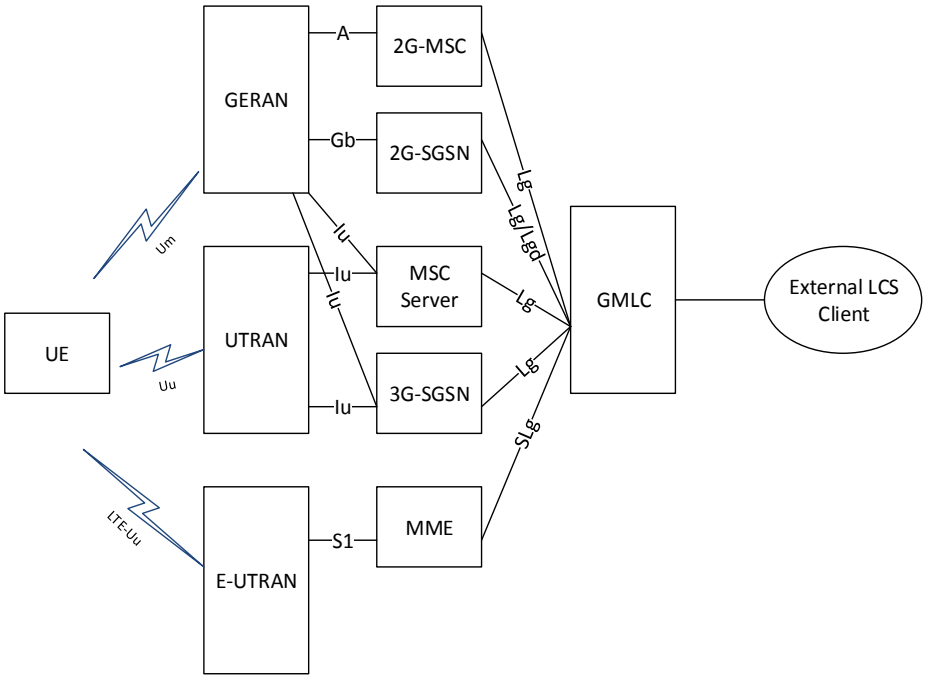


Figure 2-2 LBS Architecture

The LCS entities with the core network (CN) using the access network to communicate across interfaces like A, Gb, Iu and S1. Signals and messages are transmitted among the mobile network to and from the LCS elements in order to send and receive information.

The GMLC contains functionality required to support LCS. It could be one GMLC in a core network or could be more than one [4, 11]. The GMLC may also include a requesting GMLC (R-GMLC) which is the GMLC that receives the location request of the user, and home GMLC (H-GMLC) which is the GMLC to which the target user belongs, or a visited GMLC (V-GMLC) that is the GMLC where the user is currently located [11, 48].

The main functions of GMLC are that it interacts with location services (LCS) clients for location information, performs transaction management by managing the data flow between the core network and the location server and is an interface with other nodes in the core network via interfaces like Lh and Lg.

The LCS client is a third-party system that asks the mobile operator to provide a user position; it can obtain the information by requesting it from the mobile operator or can be given it when the user asks for certain information form the LCS client. The external LCS client can access the network via the GMLC and the GMLC may request routing information from the HLR or HSS. After the authorization process, the GMLC sends a request to check the user location to either a Mobile Switching Centre server (MSC), serving GPRS Support

Node (SGSN), or a Mobility Management Entity (MME) and receives the resultant location estimates from them.

LCS is a service concept in system standardisation. Functionalities, entities, interfaces and communication messages and all necessary network elements are specified by LCS. The main logical components of the LCS are the LCS client, LCS server and target UE. Logical reference model can be seen in Figure 2-3 [11, 49, 50].

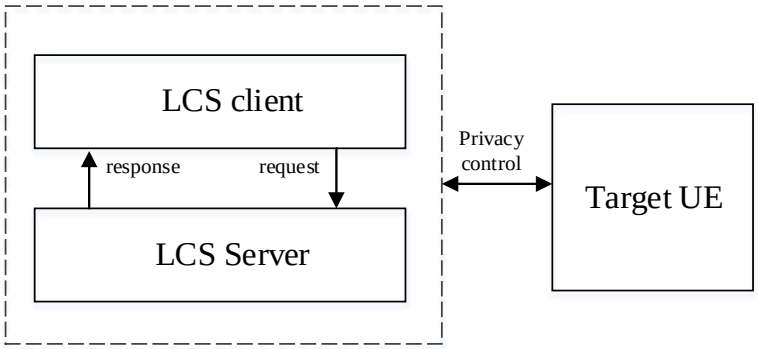


Figure 2-3 Logical Reference

The LCS client can ask for the user location from the LCS server. There may be one LCS client in the system or could be more. This depends on the network's architecture and technology if it is UMTS, LTE or EPS. The user uses applications to access the service through the Internet [11].

A certain target UE requests location information from an LCS server, which is resident in an LCS client. This means the target UE is a user who asks for a location based service, and the LCS server is where all the information about the location is stored to prepare the requested information for the LCS client [49]. The LCS server can be hardware, software or a combination of both. It sends back a location related information after receiving it from the LCS client [50].

In addition, the LCS Server could receive a request from the client or from more than one client and the LCS server could be one or more in a network.

2.3 LBS Requirements

According to 3GPP standards, LBS attributes vary from service to service but the primary distinguishing attributes that add value to a service are accuracy, coverage, privacy, and transaction rate. Moreover, to achieve a good quality of service in the LBS the system needs to demonstrate good performance in many aspects, such as accuracy and response time. When the LBS are used for emergency services, there may be insufficient time to respond

to the user request, so the network and data and server providers must respond as quickly as possible with minimum delay [4, 49].

It is difficult to achieve good performance and quality of all requirements in one system, as when a system has a quick response time, it may have less accuracy, because the system needs more time to calculate and estimate the user location. This is the situation for all the parameters and requirements, like accuracy, response time, complexity, privacy etc.

2.3.1 Accuracy

The accuracy parameter is an optional and negotiable quality of service parameter, there are two types of accuracy: the vertical accuracy and horizontal accuracy. The accuracy in general depends on many factors, such as environmental with weather conditions and signal attenuations, or network design such as network topology. Different types of service need different ranges of accuracy, so for navigation services the range would be ten metres, while kilometres are considered as an acceptable range for fleet management [49].

2.3.2 Response Time

The time needed to transmit the information between the LCS server and the LCS client is the response time. Depending on the LCS client requirement, the response time could be a negotiable parameter, but when considering emergency services, the response time is a very important parameter [4, 17, 49].

2.3.3 Reliability

Reliability gives an indication of how often the positioning and location information request that satisfies the system requirements are successful. For a tracking service like vehicle tracking the reliability is not critical, while for a service that tracks a child the reliability is more important [49].

2.3.4 Privacy

Even though the location based service provides a convenient service that helps us in our daily life, the server provider has to access some private information like user identity, type of service and user's location [51, 52]. In some cases, this might lead to potential privacy invasions, especially if the service provider is unknown or untrusted [53].

Therefore, a mobile operator must ensure that its subscriber privacy is confidential. However, this information still needs to be sent to the service and data provider, which might be an external LCS [49]. In this case, the user's information are shared with other parties.

2.3.5 Priority

When the location based service operator receives multiple requests at the same time, it should give priority for some of them and delay the others. The LCS server should always give the highest priority for emergency services, and the higher priority gets faster access to the resource and may get a faster, reliable and accurate location estimation [49].

2.3.6 Coverage

To get a good quality of service, the user should be able to access a location service anywhere within the operator's coverage area or within the roaming area. In some cases, the operator cannot guarantee the coverage for the users because of the network topology and environmental factors and user location like urban or rural area [12-14].

Furthermore, in the case of the roaming, the visited network may not accept localization methods and in some cases the network service may not be available in this roaming operator. Alternatively, the coverage problems may come from roaming contracts between network operators [49].

2.3.7 Security

User's location and information should be secured and provided in a reliable manner to ensure they are not going to be lost or delivered with error. The LCS server gives a grant to the LCS Client to access the location information and even though the access is granted to the LCS client, the existing security mechanisms must be used [49].

Before being allowed to access the LCS service, the target UE must be authenticated first, so that the user information can be stored on the LCS server, and only authorized LCS Clients to access the LCS Server and see that information. This ensures no unknown or untrusted third-party LCS can access the network [49].

2.4 Summary

The Location-Based Service is a service that provides a service by using user's location, with services like navigation, searching for a point of interest (POI), advertising, or even emergency service. The main component of the LBS are user, positioning, communication network, and service and data provider. In general, the Internet is used as a communication network in the LBS. In a standard 3GPP and normal systems a third-party data provider is used to provide the data and the services, and they are known as the LCS client. The LCS client interacts with the mobile's operator core network via the GMLC.

To achieve a good performance in the LBS there are many requirements that need to be realised, such as accuracy, security, privacy, time response, but not all these requirements can be achieved in just one system.

By using the new proposed methods the LBS will get better QoS parameter. The LBS after using the new architecture got better response time, reliability, privacy, priority and coverage.

Chapter Three: Mobile Network; Standards and Background

A communication network is needed in order to send the information from the user to the service and data provider, and then back again to the user. The location-based services (LBS) usually use the mobile network to send and receive the information. For this reason, an understanding of the mobile communication network is important to understand how the LBS communicates between the user and the service and data provider. In this chapter, as an example of the mobile network the UMTS architecture and standard are explained, as well as the types of channels used by the user to send the data to and from the core network. Also, in this chapter the types of protocols used to transfer these data over the channels to and from the core network are presented.

3.1 UMTS Architecture:

The UMTS is a third generation of mobile cellular network, and is presented and developed by the 3rd Generation Partnership Project (3GPP). The UMTS uses wideband code division multiple access (W-CDMA) radio access technology offering a good bandwidth and spectral efficiency to the mobile network operators [54].

The UMTS can be classified into two subsystems: radio network subsystems (RNS), also known as universal terrestrial radio access network (UTRAN), and the core network (CN), which can be divided into circuit switch (SC) and packet switch (PS). See Figure 3-1 for further details [54].

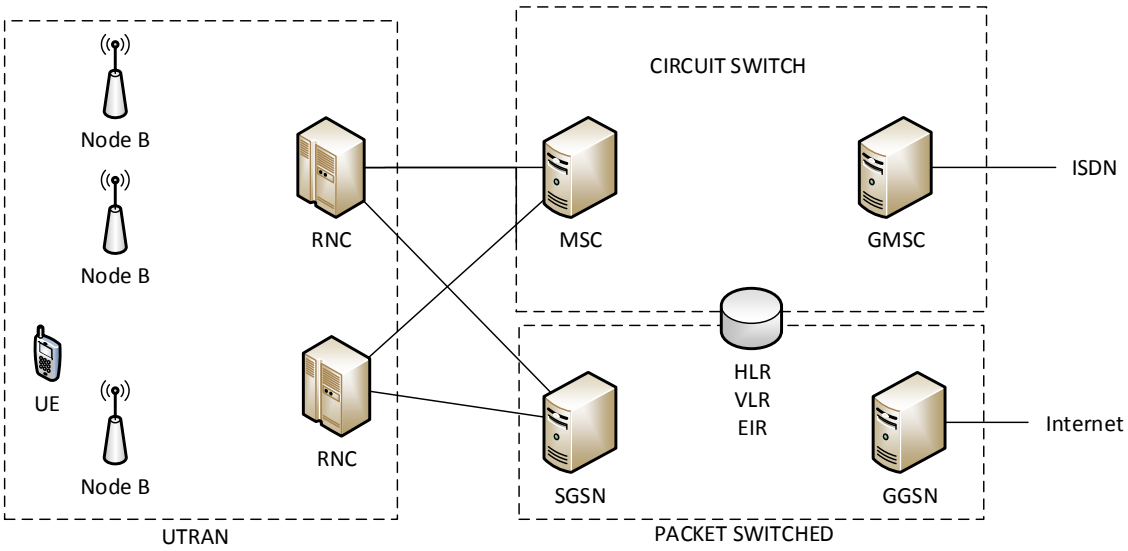


Figure 3-1 UMTS Architecture

3.1.1 UMTS Core Network

The UMTS core network can be classified into two domains: the circuit switched domain and the packet switched domain. Where the voice and video-telephony are supported at the CS, and the PS enables the user to connect to the Internet and be online.

3.1.1.1 Circuit Switched Components:

The main architecture elements of the UMTS circuit switched core network include: mobile switching centre (MSC) which basically works the same as that in GSM, and is considered the primary service node for the network, which is responsible for routing and managing the voice calls and video-telephony and other services [55]. The function of the MSC is setting up and releasing an end-to-end connection, handling mobility and handover requirements during the call [56].

Gateway MSC (GMSC) is an MSC, which accomplishes the routing function to the real location of the user when the network is delivering a call to the public land mobile network (PLMN). Effectively, the GMSC is the interface of the core network to external networks.

3.1.1.2 Packet Switched Components:

The basic packet switched (PS) domain of the UMTS core network architecture can be summarized into the following elements:

Serving GPRS support node (SGSN): this was first developed when general packet radio service (GPRS) was introduced and it is still being used in the UMTS network architecture. The SGSN provides many functions in the UMTS mobile network, such as managing mobility, managing session, and interaction with other areas of the network [56].

Gateway GPRS Support Node (GGSN) was first introduced into the GPRS network of the second generation network GSM. It is the central and main element in the UMTS PS network. It handles the internal network between the UMTS PS network and external PS networks, and can be considered as a router.

3.1.1.3 Shared Elements

The basic shared elements between the CS and the PS of the 3G network are: [55].

The Visitor Location Register (VLR) which is a database that saves the user information when he/she is located in the area covered by this VLR. It stores the roaming number of the user and the area where that user resisted, and it can be connected to one or more MSCs.

Home location register (HLR) is a database, which has all the administrative information about every user (subscriber) and their last known location in the network.

Equipment identity register (EIR), is the entity that decides whether the user (UE) is allowed to access the network or not.

The authentication centre (AuC) is a database, which constrains the secret keys. It also contains the user's Universal Subscriber Identity Module (USIM) card.

3.1.2 UTRAN

The UTRAN contains RNSs and each RNS has one radio network controller (RNC) and different numbers of base stations, which can be called Node B. RNSs and RNC are connected to each other by (Iur) interface [56].

The RNC acts as a switch to control the elements of the UTRAN, and the main function of the RNC are control functions and radio resource managements, which are a collection of many algorithms used to accomplish a good Quality of service (QoS) of radio connection and guarantee the stability of the radio path.

The Base Station (Node B) implements radio access physical channels of the WCDMA and transfers information to the physical channels from the transport channels based on the RNC arrangement [56].

Each element of the UMTS network communicates with other elements with signals, which are carried by the channel.

3.2 Transport and Physical Channels:

UMTS allocates a bandwidth for the users, and this bandwidth and its controlling functions are called channels. There are three layers of channels in UMTS, which are logical, transport, and physical channels. The types of information to be transmitted are described by the logical channels, while the transport channels describe how those logical channels are to be transferred, and the media that is used to transmit the information is the physical channels, Figure 3-2 shows the three channel layers [56].

The data generated at the higher layers in universal terrestrial radio access (UTRA) are carried by transport channels and mapped in the physical layer to be carried by physical channels. To enable multiplexing several services to one connection the physical layer is used.

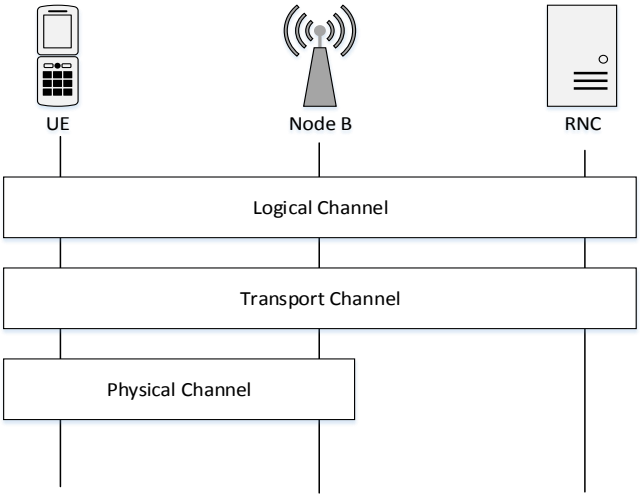


Figure 3-2 Channel Layers

When the data is expected to arrive at the specific transport channel from the higher layers, each transport channel is combined by a transport format indicator (TFI). The physical layer gathers the TFI information from different transport channels to the transport format combination indicator (TFCI). To inform the receiver which transport channels are active for the current frame, the physical control channels transmit the TFCI [57].

At the receiver, the resulting TFI is given to the higher layers after being decoded from the TFCI. Figure 3-3 shows two transport channels mapped to a single physical channel; if there are any errors for each transport block, it will be shown in the error indication. The transport channels may have a different number of blocks and not all the transport channels are necessarily active at the same time [58].

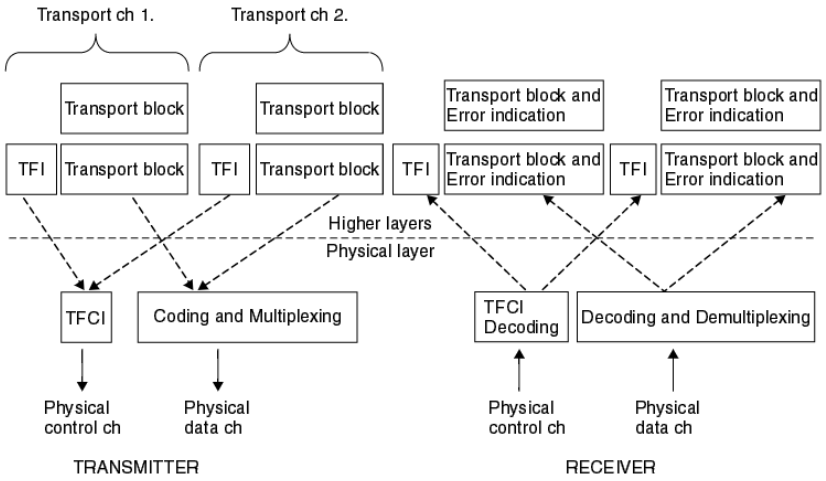


Figure 3-3 Interfaces Between Higher Layers and The Physical Layer

3.2.1 Transport Channels

To carry the required data in the air across the radio access network, the transport channel is used to carry the data. The transport channels are offered by the upper layer to provide services. The transport channels can be classified into two groups of channels: common channels and dedicated channels.

3.2.1.1 Dedicated Transport Channels

The dedicated channel (DCH) is a bidirectional channel, and can be a downlink (from the user to the core network) or uplink channel (from the core network to the user). It can be transmitted over part of the cell or can use the entire cell [59].

3.2.1.2 Common Transport Channels

There are six types of common transport channels: FACH, RACH, BCH, PCH, HS-DSCH and E-DCH [58, 59].

Broadcast Channel (BCH)

The Broadcast Channel (BCH) is a downlink channel that is used by the system to broadcast specific information related to the system. The entire cell is always used to transmit the BCH. For the cells configured with broadcast distribution, the first BCH is mapped to Primary Common Control Physical Channel P-CCPCH and one additional BCH is mapped to secondary Primary Common Control Physical Channel S-CCPCH.

Forward Access Channel (FACH)

The FACH is a downlink transport channel and it takes the entire cell to be transmitted. The FACH can transmit a small amount of data.

Paging Channel (PCH)

The Paging Channel (PCH) is a downlink transport channel. The transmission of the PCH is related to the transmission of the physical layer generated paging indicators to page the user when there is a call.

Random Access Channel (RACH)

The RACH is an uplink transport channel that is received from the entire cell. The RACH is used for initial access, connection setup and can carry a small amount of data.

Indicators

Indicators are fast and low level signals which are carried over transport channels and transmitted without using information blocks. These indicators are: Page Indicator (PI), Acquisition Indicator (AI) and Notification Indicator (NI).

Indicators can be Boolean (True or false). Physical indicator channels (ICH) are used to carry indicators that are transmitted.

3.2.2 Physical Channels

The physical channels are used to carry the payload data and information. They manage the physical characteristics of the signal. Physical channels can be defined by a specific carrier frequency, scrambling code, a channelization code, and time duration.

Each physical channel has one radio frame, which consists of 15 slots, and the length of a radio frame corresponds to 38400 chips. Physical channels can be classified into detected and common channels [59].

3.2.2.1 Dedicated Physical Channels

The dedicated channels can be either uplink or downlink according to their direction to or from the user equipment UE.

Dedicated uplink physical channels

There are many types of uplink dedicated physical channels in the UMTS, including the uplink Dedicated Physical Control Channel (uplink DPCCH), the uplink Secondary Dedicated Physical Control Channel (uplink S-DPCCH), the uplink Dedicated Physical Data Channel (uplink DPDCH), the uplink enhanced dedicated channel E-DCH Dedicated Physical Data Channel (uplink E-DPDCH), the uplink Dedicated Control Channel associated with HS-DSCH transmission (uplink HSDPCCH), and the uplink EDCH Dedicated Physical Control Channel (uplink E-DPCCH).

Dedicated downlink physical channels

There are five types of downlink dedicated physical channels in the UMTS: the Fractional Dedicated Physical Channel (F-DPCH), the E-DCH Relative Grant Channel (E-RGCH), Dedicated Physical Channel (downlink DPCH), the EDCH Hybrid ARQ Indicator Channel (E-HICH) and the Fractional Transmitted Pre-coding Indicator Channel (FTPICH).

In this thesis, the dedicated uplink and downlink channels will not be explained because it is not part of the design; for more information about the dedicated channels, please refer to the 3GPP standard 25.211.

3.2.2.2 Common Physical Channels

The common physical channels can be classified into either uplink to send information from the user, or downlink to send the information to the user.

Common uplink physical channels

As the proposed design uses the PRACH and S-CCPCH as common physical channels, the PRACH and S- CCPCH are only explained among other common physical channels.

Physical Random Access Channel (PRACH)

The Physical Random Access Channel (PRACH) is used to carry the RACH. It can be divided into a preamble part and a message part, as seen in Figure 3-4 [59]. The length of each preamble is 4096 chips' and has 256 signatures of 16 chips'.

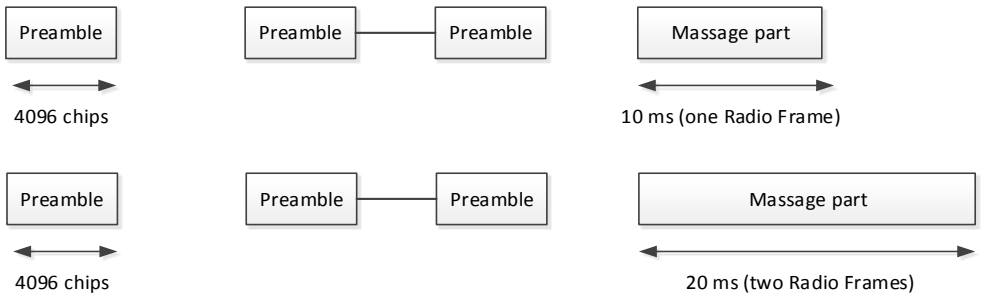


Figure 3-4 Structure of the RACH

The structure of the random-access message part radio frame can be seen in Figure 3-5, and the radio frame takes 10 ms or 20 ms in time depending on the number of a radio frame. Each 10 ms message part radio frame is split into 15 slots, each slot having a length of 2560 chips and with two parts: a control part that carries control information from the upper layer and a data part where the RACH is mapped [59].

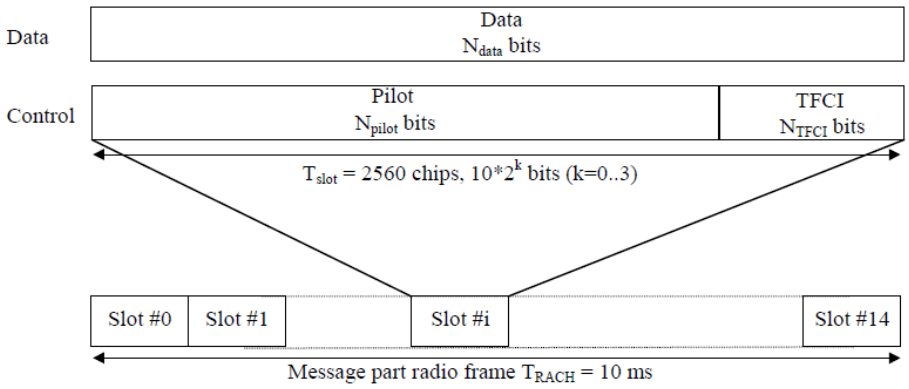


Figure 3-5 Frame Structure for RACH

The data part consists of $10*2^k$ bits, where k=0, 1, 2, 3. This is changeable according to the spreading factors, which are 256, 128, 64 and 32 for the RACH for the message data part. The radio frame message part usually has 10 ms message parts, while a 20 ms message part

consists of two 10 ms message part radio frames. Table 3-1 shows the characteristics of RACH for different slot formats [57].

On the other hand, the control part consists of eight known pilot bits to support channel estimation and two TFCI bits. This corresponds to only the spreading factor of 256 for the message control part [57].

Table 3-1 RACH Characteristics

Slot Format	SF	Channel Bit Rate (kbps)	Channel Symbol Rate (ksps)	Bits/ Slot	Bits/ Frame
0	256	15	15	10	150
1	128	30	30	20	300
2	64	60	60	40	600
3	32	120	120	80	1200

Common downlink physical channels

There are many downlink physical channels, which are: Common Pilot Channel (CPICH), Primary Common Control Physical Channel (P-CCPCH), Secondary Common Control Physical Channel (S-CCPCH), Synchronisation Channel (SCH), Acquisition Indicator Channel (AICH), Paging Indicator Channel (PICH), High Speed Physical Downlink Shared Channel (HS-PDSCH), High Speed Shared Control Channel (HS-SCCH), E–DCH Absolute Grant Channel (E-AGCH), E-DCH Rank and Offset Channel (E-ROCH), MBMS Indicator Channel (MICH) and Common E-DCH Relative Grant Channel [59].

S-CCPCH

The S-CCPCH is used to carry the FACH and PCH, and can also carry the BCH in some configurations. The S-CCPCH can have a TFCI in some configurations and cannot have it in other configurations and it is the UTRAN responsibility to determine whether a TFCI should be transmitted or not; for this reason the UEs should always support the use of TFCI. A 10 ms radio frame is used to carry 15 slots, and each slot has 2560 chips and can carry $20*2^k$ bits for k=(0-6), which is depend on the spreading factor 256,128,64,32,16,and 4. Figure 3-6 shows the S-CCPCH structure. Table 3-2 shows the different types of slot formats and its characteristics [59].

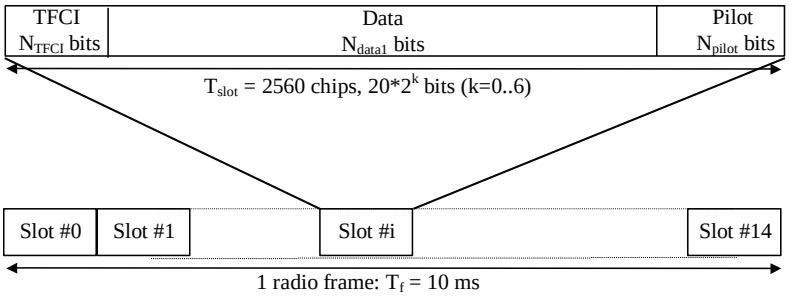


Figure 3-6 Radio Frame Structure of S-CCPCH

The size of TFCI can be 0,2,4 or 8 bits, and Npilot can be 0, 8 or 16 bits while the size of data will take the remaining fields after the Pilots and TFCI are filled. All the configuration will change depending on the slot format.

Table 3-2 S-CCPCH Characteristics

Slot Format	SF	Channel Bit Rate (kbps)	Channel Symbol Rate (ksps)	Bits/ Slot	Bits/ Frame
0	256	30	15	20	300
4	128	60	30	40	600
8	64	120	60	80	1200
11	32	240	120	160	2400
12	16	480	240	320	4800
15	8	960	480	640	9600
16	4	1920	960	1280	19200

3.2.3 Mapping of Transport Channel into Physical Channel

Each transport channel is mapped to a physical channel to be transmitted. In some cases, many transport channels may be mapped to one physical channel. Figure 3-7 shows the mapping of the transport channel into a physical channel [59].

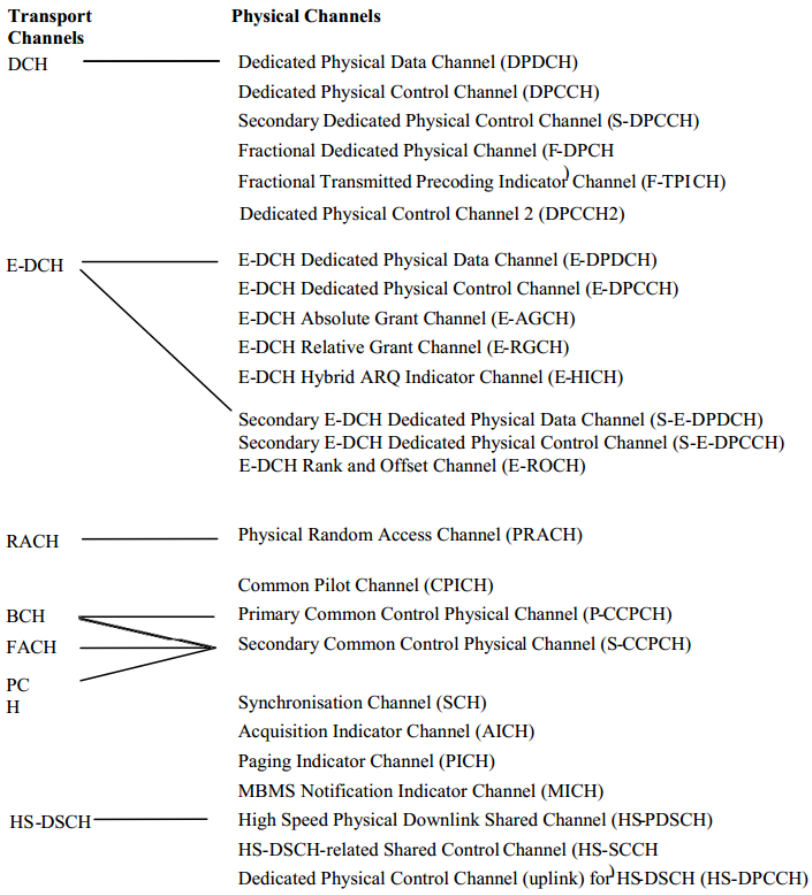


Figure 3-7 Transport Channels to Physical Channel Mapping

3.3 Frame Structure

The general structure of the frame comprises a header and a payload, where the header contains information related to the frame type and control field while the payload has the other information and data. The structure of the frames can be seen in Figure 3-8 [57].

On the Iub interface, within each byte, the bits are sent from the highest bit position (bit position 7 first) and the frame is transmitted starting from the lowest numbered byte (Byte 0). If the spare extension not being used by the transmitter it will be ignored by the receiver but it has to be set as zeros [57].

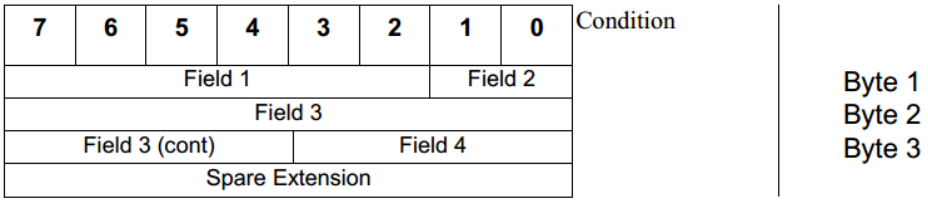


Figure 3-8 Frame Structure

The frame structure fields are different according to the channel type, but all are similar to a header and payload.

3.3.1 RACH

The RACH data frame has many fields like CFN, FT, TFI and CRC. The CFN corresponding to the first frame when receiving the data will indicate if the payload is received in several frames. Figure 3-9 shows the RACH frame structure [57].

CRC: is the cyclic redundancy checksum used to calculate and detect the error in the header of any data frame.

Transport Format Indicator (TFI): is used to show the transmission interval.

CFN: indicator to show which radio frame was used first in the uplink or which one will be transmitted first in the downlink.

TB: transport block.

IE: information element.

New IE FI: new information flags indicator can be used to change the frame configuration. It can take either 0 or 1. For example, if the Bit 1 from New IE IF is set to 0, Ext Propagation Delay IE is present.

Propagation Delay: it is used to measure radio interface delay in the RACH.

Ext. Propagation Delay: this is an extended part of the Propagation Delay; it is only activated when the bit 1 of New IE FI is true.

Cell Portion ID: indicates the best received quality signal in the RACH.

Rx Timing Deviation: it has the measurement of the received timing deviation. It has all measurements that are made for all slots and all frames that have a payload. It can be used only in TDD mode.

Received SYNC UL Timing Deviation: it is only used with TDD mode, and it is used for timing synchronization for the uplink.

Spare Extension Field length in RACH data frame is 28 octets and in normal cases it is set to zero.

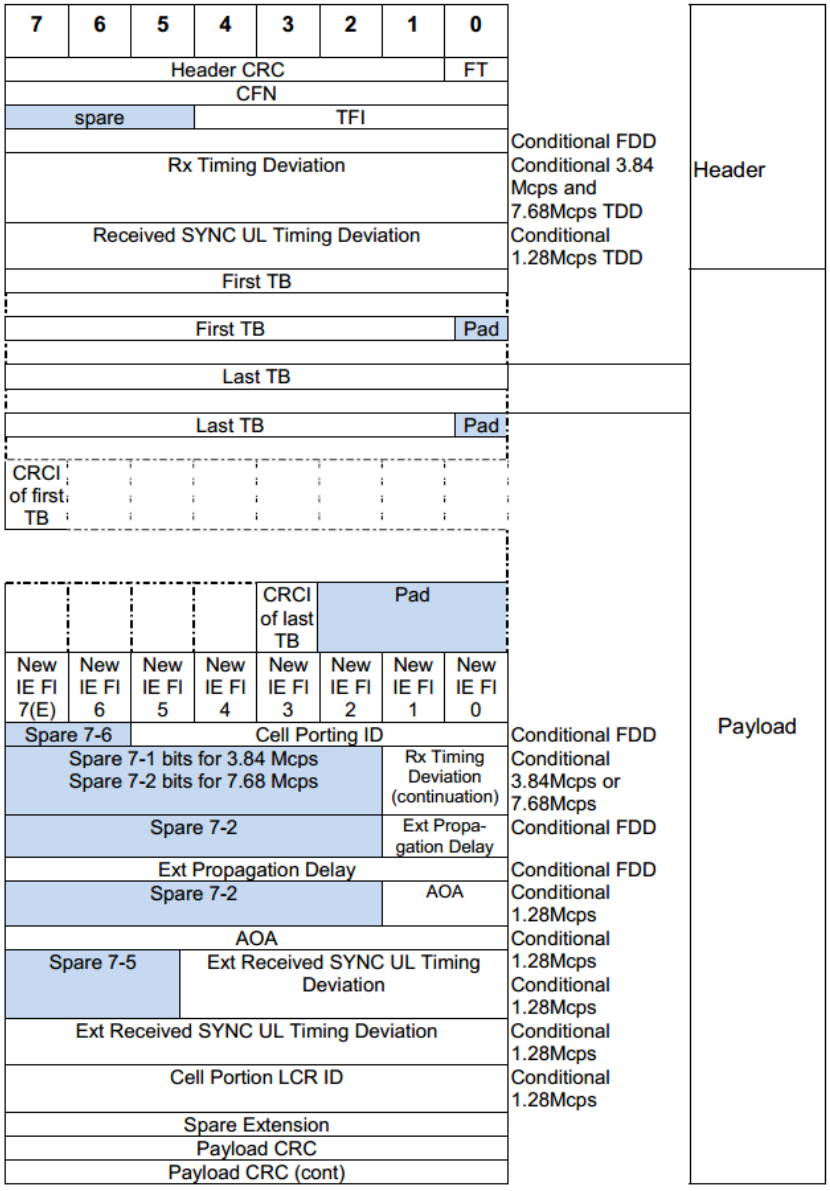


Figure 3-9 RACH Frame Structure

3.3.2 FACH

Like the RACH, the FACH frame has the CFN, which indicates which payload is to be transmitted first. The CFN of the first frame will indicate if the payload is to be transmitted more than one frame. Usually, the FACH is carried by the S-CCPCH. Figure 3-10 shows the FACH frame structure [57].

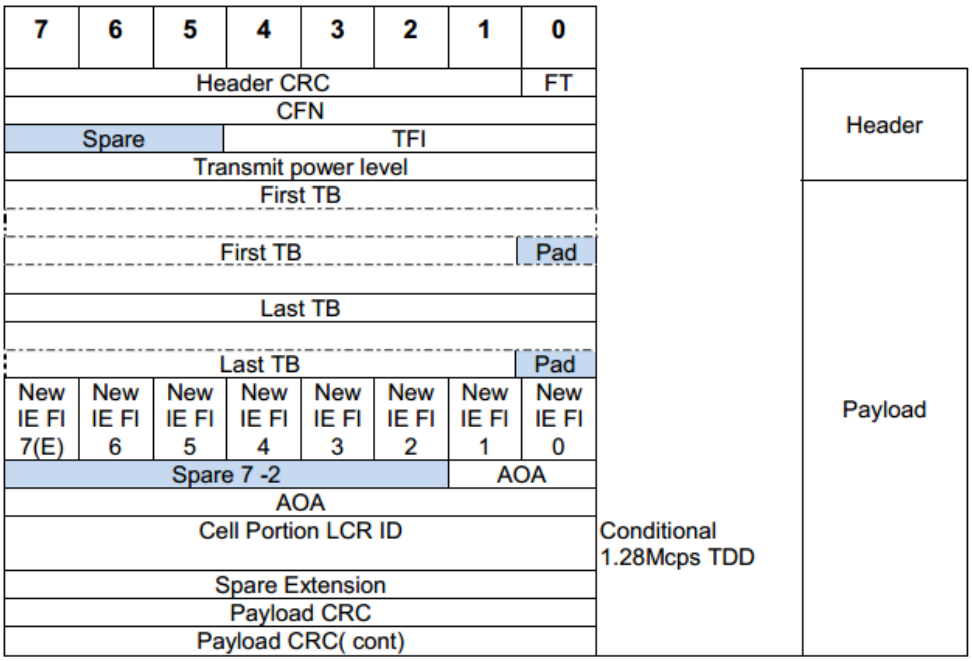


Figure 3-10 FACH Frame Structure

All the fields are defined in the RACH section. However, the length of spare extension in FACH can take up to 29 octets and it is sent as zero by the sender and neglected by the receiver as long as they are zeros.

3.4 Transmission Procedure

The physical channels and the transport channels use a sequence of signalling and messages to send the information to and from the network; these signals are used for different types of services like data, voice call or video calls. Each of these services and channels have the specific quality of service (QoS) like bit error rate, bit rate and delay. Based on the required QoS, there are several operations that can be applied to transport or physical channels. These operations are simplified and illustrated in Figure 3-11 [60].

3.4.1 Operations Applied to Transport Channels

The operation that is applied to the transport channels is the multiplexing and coding operation. After this, information are checked to see whether there are any errors and then they are sent to the physical channel.

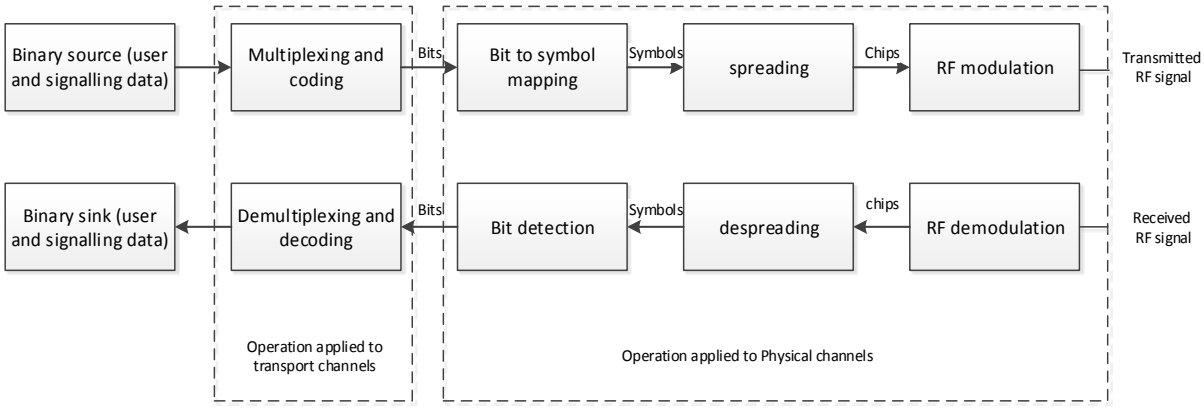


Figure 3-11 Simplified Transmission Chain in FDD Physical Channel

3.4.1.1 Multiplexing and Channel Coding

Many serviced transport channels can be mapped into one or more physical channels. The transport channels can be used to carry information with different data rates depending on the service; this flexibility can make the transport channels efficiently allocated to physical channels and use the same Radio Resource Control (RRC) connection. Similarly, common transport channels can use the same operations. There are many stages in multiplexing and channel codings, such as cyclic redundancy check (CRC), transport block segmentation, channel coding, turbo coding, frame segmentation, and rate matching [61]. Most of the operations can be applied to the uplink and downlink [60].

3.4.1.2 CRC

CRC is a method to detect errors in the code. It is commonly used in mobile, network communication, and storage devices to find accidental changes to the original data. It uses the remainder of a polynomial division of data block; the data entering the system gets a short check value attached. On the receiver this calculation is repeated and, if the check procedure finds an error where the values do not match, corrective action may be taken.

3.4.2 Operations Applied to Physical Channels

The most common operations that apply to physical channels are channelization codes, scrambling, and modulation.

3.4.2.1 Channelization Codes

The channelization codes are one of the spreading operations, where each symbol is transformed into a number of chips. Usually, the number of chips per data symbol is equal to the spreading factor.

The Orthogonal Variable Spreading Factor (OVSF) codes are another name of channelization code. It has a length of codes depending on its spreading factor (SF). It can be defined as $C_{ch,\,SF,\,k}$, where k is the code number such that $0 \leq k \leq SF-1$ and SF are the spreading factor of the code.

OVSF codes originate from the code tree, as shown in Figure 3-12. . If the system decides to assign one OVSF code to a user, the "sub-tree" cannot be used for other users, even when the orthogonal property is maintained across different symbol rates. Also, the smaller SF code on the root of the tree cannot be used. For example, if the code $C_{ch,4,2}$ is used by one user, the codes $C_{ch\ 8,4}$; $C_{ch,8,5}$; cannot be used by other users. This case is applicable for code $C_{ch,2,1}$ in the root path of $C_{ch,4,2}$ [61].

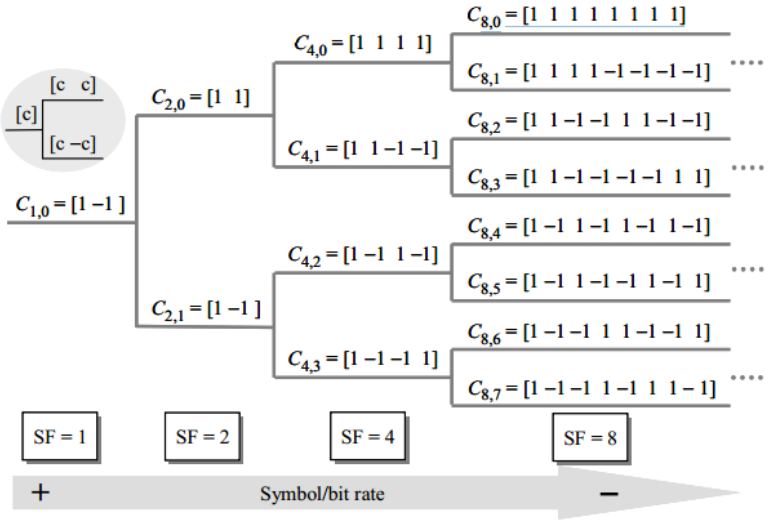


Figure 3-12 Tree Structure to Generate OVSF Codes

3.4.2.2 Scrambling Codes

Scrambling codes are used to separate the serving cell from other cells in the downlink and to separate the selected UE from others in the uplink. The OVSF code can be reused between the user and Node B within the same coverage and location when using the scrambling codes. Scrambling codes are used before the channelization codes so it cannot affect the channel bandwidth [60]

3.4.2.2.1 Uplink Scrambling Codes

The uplink signal of each UE is scrambled with a unique scrambling code, and this scrambling code will make the Node B to differentiate one UE from each other. Complex scrambling is used by rotating the constellation continuously to distribute the power evenly

between the two orthogonal I/Q branches. It is the RNC responsibility to assign different scrambling codes in the uplink to different UEs. A long scramble code is an example of scrambling code that is used in the uplink.

Long scrambling codes: The long scrambling codes are spread over one radio frame of 10 ms length, which give up to 38,400 chips. The long scrambling code is used in Node B when using the RAKE receiver, and the long scrambling sequence can be defined, as shown in Figure 3-13 [60].

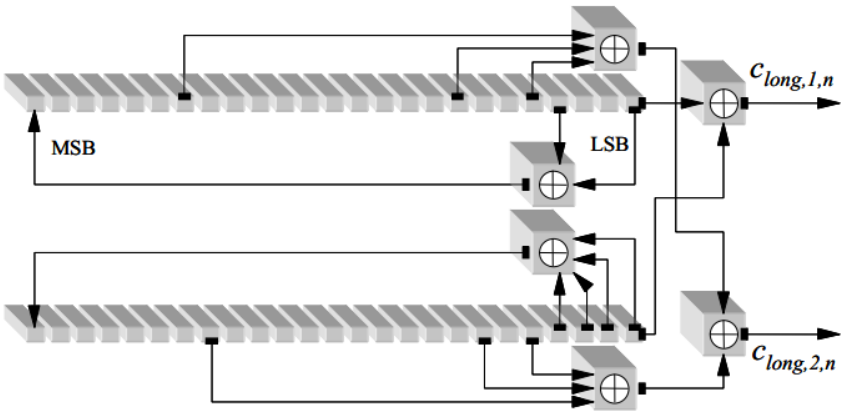


Figure 3-13 Long Scrambling Code for the Uplink

3.4.2.2.2 Downlink Scrambling Codes

In the downlink, only long scrambling codes can be used. All data channels are multiplied by a unique long scrambling code to form the signal from every Node B.

In general, there are $2^{18} - 1$ scrambling codes. For this reason, the search process is slow so in order to make the search procedure quicker, only 8,192 of these are used, that means n = (0-8191). These codes are divided into 512 sets; each set has only one primary scrambling code and 15 secondary scrambling codes.

In the downlink, it is possible to generate a complex value scrambling code from a combination of two real-valued sequences $C_{n,1}$ and $C_{n,2}$. Figure 3-14 shows the long scrambling code in the downlink.

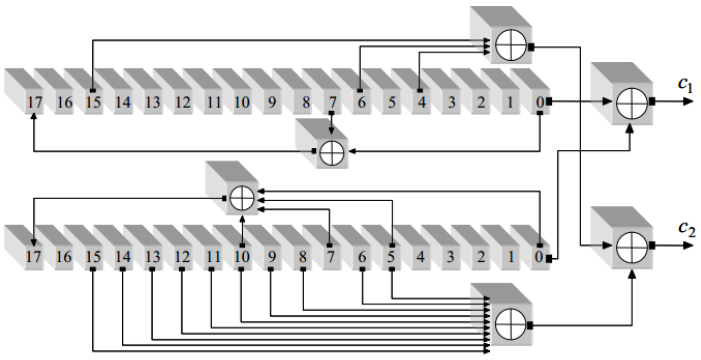


Figure 3-14 Long Scrambling Code in Downlink

3.4.2.3 Spreading and Modulation of Common Physical Channels

In this section, the PRACH and S-CCPCH are described and explained. Only the spreading of the common physical channel is taken into consideration (not the detected channels), as only these channels are used in the proposed design.

3.4.2.3.1 Spreading Factor of the Physical Random Access Channel (PRACH)

The PRACH mentioned earlier carries the RACH transport channel used by the UE to request RRC connection establishment. Each slot of the PRACH has two parts, a data part and the control part. The data part is used to carry the RACH transport channel. The OVSF codes SF = 256 (15 kbps), 128 (30 kbps), 64 (60 kbps) or 32 (120 kbps) are used for the data part to spread the signals. Note that in uplink the number of symbols are the same as the number of bits. The control part is used to carry transport upper layer control information and has a spreading factor of 256 with a fixed rate of 15 kbps and contains two TFCI bits and eight pilot bits.

The transmission begins with PRACH, and a short preamble pattern notifies the Node B that there is a RACH data message coming next. The PRACH preamble part comprises of 256 repetitions of a signature of 16 chips' length (16 * 256 = 4,096); that gives a maximum of 16 available signatures. The length of the message part can be either one radio frame (10 ms) or two radio frames (20 ms); the higher layer is defining a number of the radio frames. The large cells use the message part of 20 ms [57].

3.4.2.3.2 Spreading Factor of S-CCPCH

FACH and PCH are carried by the Secondary Common Control Physical Channel (S-CCPCH). They can either share the same frame (same physical channel) or can be

transmitted on different channels. The spreading factor of the S-CCPCH can be 256, 128, 64, 32, 16, 8 or 4 that causes the channel symbol rates to vary between 15- 960 ksps [57].

3.4.2.4 Modulation

UMTS uses a quaternary phase shift keying (QPSK) for its transmission modulation technique where two chips are transmitted in each symbol [62].

In QPSK, a group of two bits are grouped together as a symbol before it is sent to be modulated, and each of these symbol can be one of four possible values: 11, 10 01, or 00. During each symbol interval, according to the input symbol, there are four possible phase shift (angles) that the modulator shifts the carrier to. In an ideal case where there are no noise and loss, the phases are each 90 degrees apart, and the phase shift in ideal cases will draw a constellation diagram matching the configuration shown in Figure 3-15.

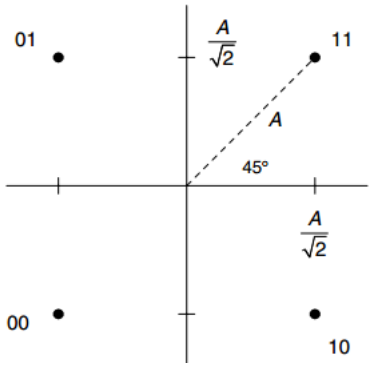


Figure 3-15 Ideal QPSK Constellation

As can be seen in the figure, the QPSK modulation can be presented by the following equations [63]:

$$I \cos w_c t + Q \sin w_c t = A \cos(w_c t + \theta) \qquad 3.1$$

$$A = \sqrt{I^2 + Q^2} \qquad 3.2$$

$$\theta = \tan^{-1}\left(\frac{Q}{I}\right) \qquad 3.3$$

$$Wc = 2\,\pi\, fc \qquad 3.4$$

Where A is the amplitude, and f is the carrier frequency, the complex signal x(t) is formed by simply using the in-phase baseband signal I (t) as the real part and the quadrature baseband signal Q(t) as the imaginary part.

If I and Q take on values of ± A / √2 (where A is the Amplitude) in all possible combinations, the angles of these signals will be on values of π /4, 3π/4, -π/4 and - 3π/4. To present the resulting signal in the form of complex value form referenced to the carrier frequency, the modulated signal can be as

$$x(t) = I(t) + jQ(t) \qquad 3.5$$

Where the complex signal is x(t) formed by using both the quadrature baseband signal Q(t) as the imaginary part and the in-phase baseband signal I (t) as the real part.

3.5 RRC Connection Establishment Procedure

This section presents a number of signalling procedures related to the UEs. Note that not all procedures nor the signalling are explained, as only procedures that are used in the proposed design are explained here.

The Radio Resource Control (RRC) protocol is used in UMTS on the air interface between the UE and Node B [64]. RRC is responsible for the control signalling that includes functions like radio bearer establishment, connection establishment and connection release, broadcast of system information, reconfiguration and release, paging notification and release, connection mobility procedures [64].

The RACH and FACH channels are used to establish and release the connection, so to understand the function of each channel, let us take an example that shows the establishment of an RRC connection on the RACH/FACH common transport channel. In this example, the data transport bearer for the RACH/FACH is considered as it is established before this procedure. Figure 3-16 shows the RRC connection establishment [65].

1. The user (UE) sends an initial signal to set-up an RRC connection; this signal is RRC Connection Request message, which is carried by CCCH using the RACH.
2. Cell Radio Network Temporary Identities (C-RNTI) and UTRA Radio Network Temporary Identities (U-RNTI) identifiers are both assigned by the SRNS and sent to the user along with a configuration message to the UE in order to give the permission to connect and join the network. The RRC message connection setup is sent on CCCH, which uses the FACH.
3. The UE sends RRC Connection Setup Complete using DCCH after receiving the configuration message from the RNC, and the RACH transport channel carries the DCCH logical channel.

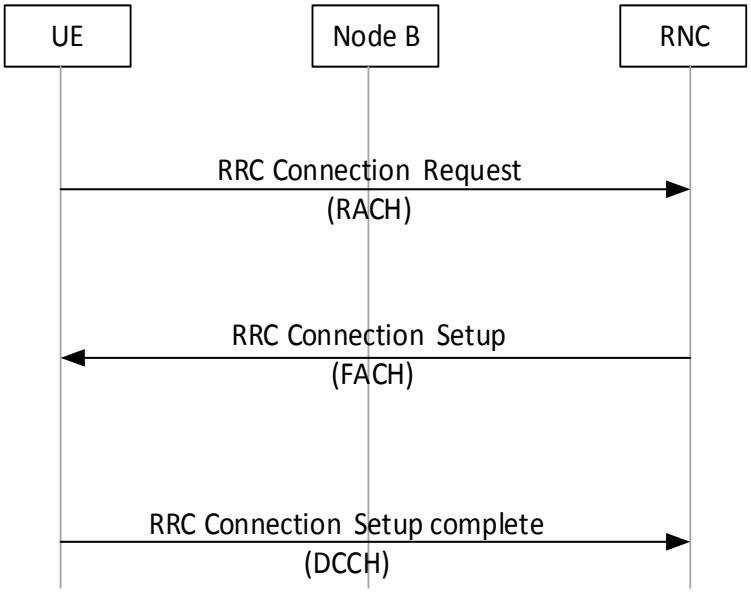


Figure 3-16 RRC Connection Establishment

So far the connection request and the information are in the UTRAN, and in order to send this information to the core network, the Iu interface is used. The Iu defines the protocols and characteristics of the air interface.

The Iu is the interface between the UTRAN and Core Network in the UMTS. The Iu interface can be either between the circuit switch domain and CN, which is called Iu-CS, or between the CN and the packet switch domain, which is called Iu-PS. Figure 3-17 shows the two logical types of Iu interface where the RNC is considered as the access point of the UTRAN. The Iu interface supports location services by carrying location information from UTRAN to CN and from the CN to UTRAN [66].

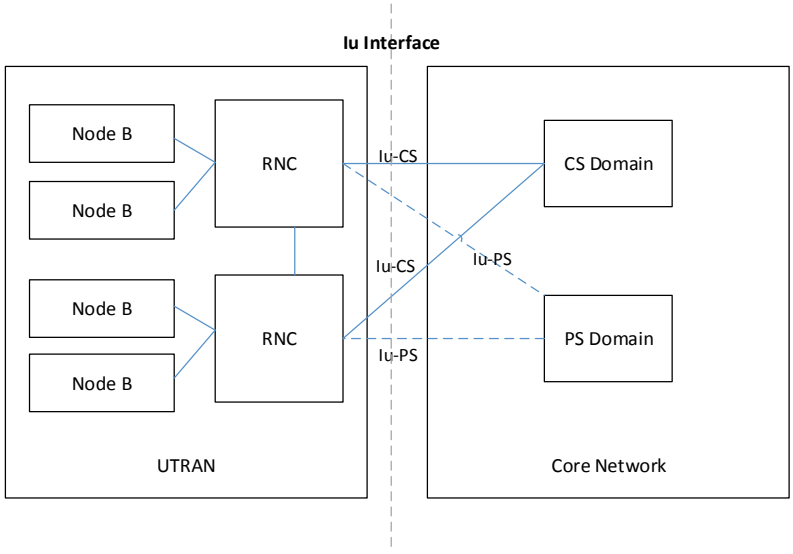


Figure 3-17 Iu Interface Between the Core Network and UTRAN

Each UTRAN can be connected to one or more CN Access Points in the Iu-cs. On other hand, the UTRAN Access Point shall not be connected to more than one CN Access Point in the Iu-PS [66].

The AAL2 protocol in the transport option ATM is used to carry the data toward the circuit switched domain in the core network [67].

3.6 Protocol Stack

The protocol stack is a term used to define the protocols used in a system for each element or stage, the UMTS protocol stack can be seen in Figure 3-18 [8, 64].

The user level uses the Radio Link Control protocol (RLC) and sends the information to the MAC layer and then to the WCDMA to be sent to the Node B. At Node B the ATM is used and AAL2 protocol to send the information to the RNC, which also can use the AAL2 to the core network. Sometimes the RNC uses the AAL5 to send the information to the Core network, but in the Iu-CS the most common protocol to send the information of the user plane is the AAL2 [64].

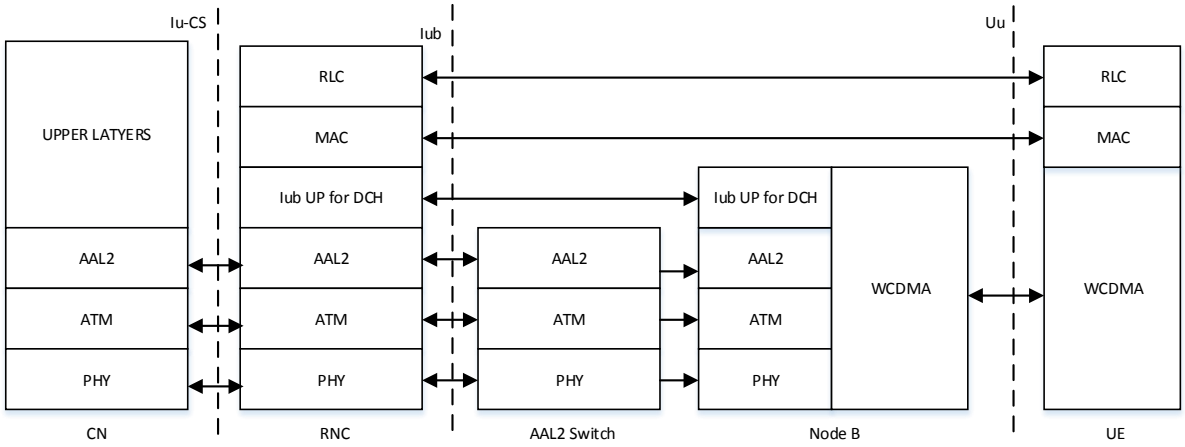


Figure 3-18 User Plane Protocol Stack for Circuit Switching [8, 68]

3.7 ATM

ATM is one of the options that can be used in the transport layer data stream in the Iu-CS and Iu-PS, according to ITU-T Recommendation I.361 [67, 69]. The AAL2 protocol improves on other ATM Adaptation Layers, by packing lots of small packets efficiently into one standard-sized ATM cell of 53 bytes.

The cell structure of the ATM has two main fields, the header which is 5 bytes and the information field, which has up to 48 bytes, as can be seen in Figure 3-19. The payload field

came from the upper layers, which are the service specific conversion sublayer SSCS and common part sublayer CPS.

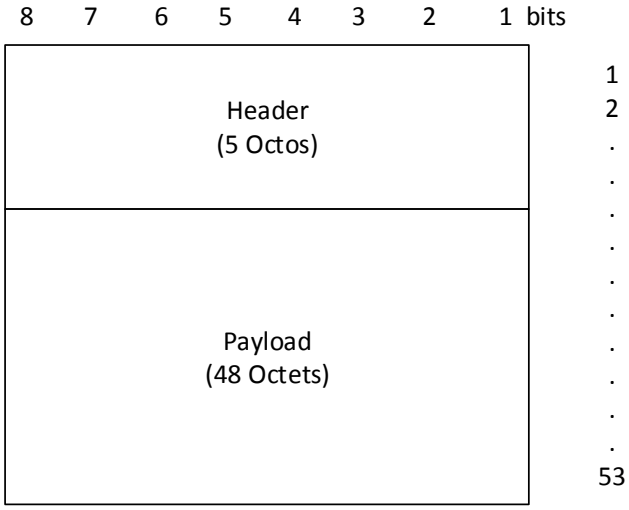


Figure 3-19 ATM General Structure

3.7.1 ATM Header

The header is 5 bytes long and contains the information of the payload and channel to be used to carry this information. Figure 3-20 below shows the header of the ATM.

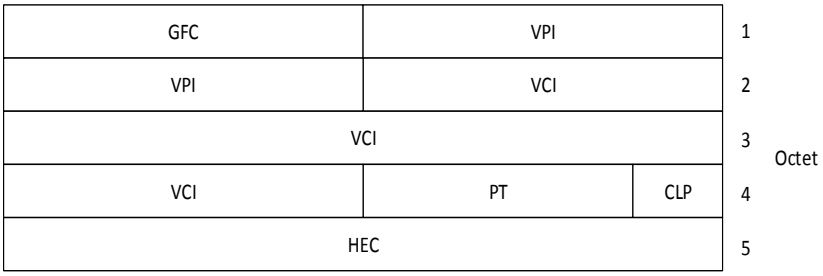


Figure 3-20 ATM Header

Where CLP Cell Loss Priority, GFC Generic Flow Control, PT Payload Type, HEC Header Error Control VPI, Virtual Path Identifier, VCI Virtual Channel Identifier.

3.7.2 Information Field

The information field or the payload field has information coming from the AAL2 upper layer, CPS and SSCS, and these sublayers help the mapping from upper layer services to ATM cells. Figure 3-21 shows the AAL2 and ATM layers [70].

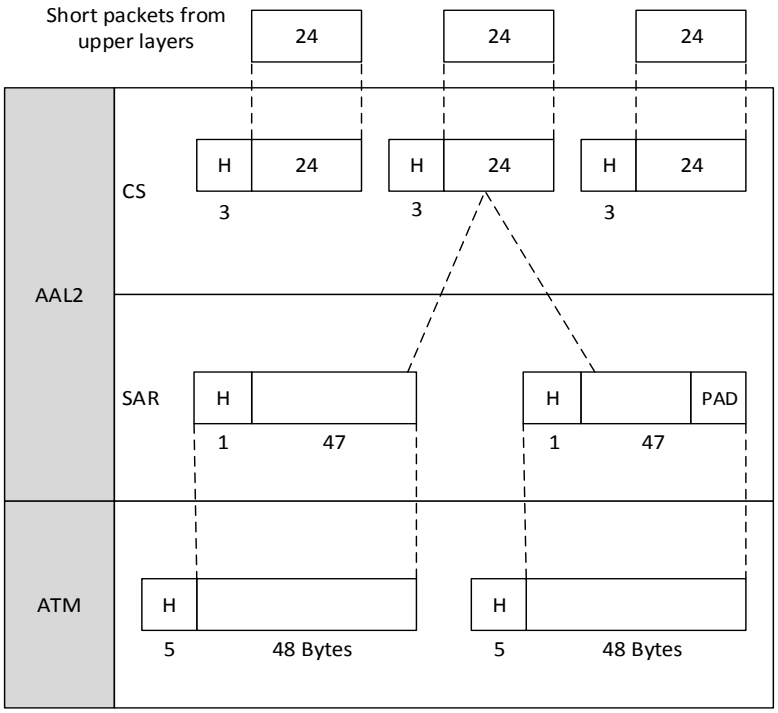


Figure 3-21 AAL2 and ATM Layers Structure

The CPS-Packet payload has a sub-field, which is CID: channel identifier, LI: length indictor, PPT: packet payload type, UUI: user-to-user indication, HEC: header error control while the SAR header has only SF Start Filed, which has OSF: offset field, SN: sequence number and a Parity bit.

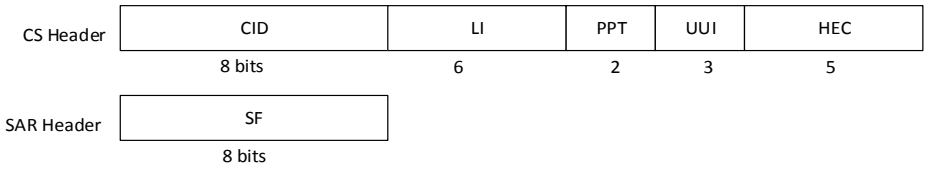


Figure 3-22 CS and SAR Headers

A 3-Byte header at the CS layer is added to each 24-Byte short packets that come from the upper layers. The SAR provides a mapping between CS and ATM layer by adding a header to receiving 47 byte packet from CS and passes to the ATM layer.

3.8 LTE and LTE-A Using 3G

In some providers the LTE uses the circuit switching of the UMTS to provide essential services, and the operator's roadmap to follow IP Multimedia Subsystem (IMS) is based on their business and economic requirements. So, while some operators will target initial

deployment of voice over LTE (VoLTE) services with IMS, there are other operators looking to leverage the LTE network for voice prior to investing in IMS, and using their 2G or 3G network for basic services like voice; this is called circuit switched fallback (CSFB) [71]. In fact, there are many options for LTE to provide basic services, especially voice services, and these options are SRVCC and CSFB.

3.8.1 SRVCC and CSFB

In general, there are two approaches to provide basic services while offering 4G PS data services: dual radio solutions and single radio solutions. For the dual radio solution, two always-on radios are used, one for PS LTE data and the other for CS telephony.

On the other hand, single radio solutions use only one radio to handle both types of traffic, using network signalling to determine when to switch from the PS network to the CS network. Consequently, there are two 3GPP standardised solutions:

1. CSFB provides a mechanism for basic services by switching to the 2G/3G CS domain without the need to deploy any dedicated infrastructure to support, such as voice in LTE. In this case, the LTE network can be viewed as a data-centric network.
2. IP multimedia subsystem single radio voice call continuity (IMS SRVCC) is based on IMS deployment to offer multimedia services to LTE end users (including voice) within LTE coverage and to hand over voice calls to the 2G/3G CS domain when the UE moves out of LTE coverage [72].

As shown in Figure 3-23, the 3GPP-based options for offering the VoLTE network are based on IMS SRVCC and CSFB.

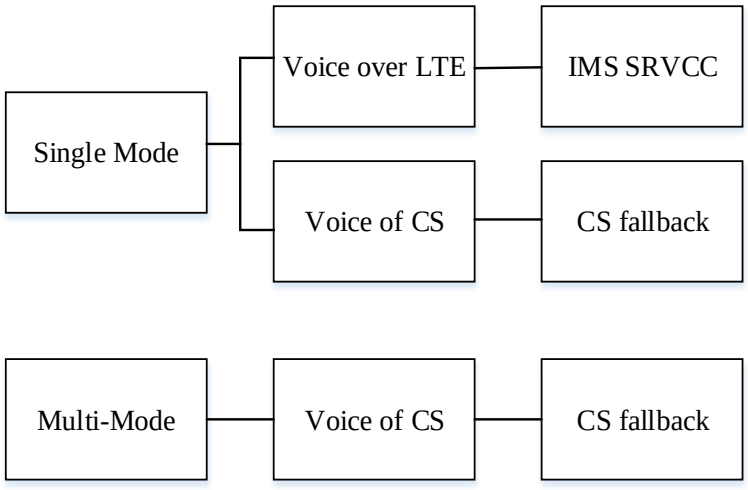


Figure 3-23 Voice Service over LTE

3.8.2 Circuit Switched Fallback (CSFB)

In general, the CSFB enables a device that is operating in LTE mode to use either 3G or 2G circuit-switched networks to receive or place essential services like voice call [73].

To clarify, let us take the example of a device on LTE that receives an incoming call while a data connection is enabled. The LTE network pages the device. The device responds with a service request message to the network, then the network asks the device to move (fallback) to 2G/3G to accept the incoming call. Similarly, for outgoing calls, the same service request is used to move the device to 2G/3G to place the outgoing call.

Control signals for connection establishment when using the CSFB are the same control signals that are used in the normal UMTS with some slight differences.

3.9 Summary

In this chapter, the basic architecture of the UMTS has been explained, as well as the channels that are used in the UMTS. In order to send informaton, the user shall send the information from the mobile to the core network via the UTRAN (Node B and RNC).

To send the information, there are several stages the data must go through, like multiplexing and coding, scrambling, and modulation. After the mobile first joined the network, it sent the information first via the control channel to the UTRAN using the RACH, and the access grant to join this network is sent back to the mobile using FACH.

The protocol that is used to send the inforamtion using the RACH/FACH is the RRC connection establishment, which is used to establish the connection between the user and the UTRAN, and then this information are sent to the core network via the ATM using the AAL2 protocol.

A new method is presented in this thesis that used the RACH and FACH to carry informattion in UMTS network, the ATM is used to carry those information between the UTRAN and the core network.

Chapter Four: Literature Review

LBS have a standard architecture but they still attract many inventions and researches to develop and evolve them in many aspects, such as (not limited to): the localization methods used to find the user, the method to transmit the information to the core network, preserving user privacy, and the applications in which the system may be used, such as navigation, tourism, health care, etc.

According to the proposed design in this thesis, two areas will be focused on during the literature review, which are: the methods used to transmit information between the user and the core network, and the architecture of the core network in terms of the LCS client and servers to reduce response time and protect users' privacy. Usually, the researchers - with some exemptions - use the Internet to communicate between the user and the core network, and use a third-party as a data and service provider in their design and assumptions.

4.1 Location-Based Services

Location-based services were first introduced by the active badge project by the University of Cambridge, which can be considered as the first research to use and develop the LBS [74]. It used sensors in the office to locate the users who wore a badge. Then Nokia in 1996 introduced a system that was used in the case of emergency to locate users within the GSM network [75].

Then the 3rd Generation Partnership Project (3GPP) published a system to transmit emergency call data from a vehicle to a PSAP, to be offered in all new cars, by sending fixed data at the same time as an emergency call using General Packet Radio Service (GPRS) or Wideband Code Division Multiple Access (WCDMA) [45, 76]. Their system developed and specified the eCall in-band modem, which is used for reliable transmission via the voice channel. The eCall system was first introduced by the European Commission and was prioritised within the mobile communication network completed in 2015 [44]. The European Commission had high-level requirements, recommendations and guidelines for eCall service and standards with the mobile telecommunication industry, automotive industry, public emergency authorities and any other industries related to the safety in the eSafety Forum [45, 77, 78].

The Internet is also used in Sukaphat design to track and find a lost mobile. It uses a cell identifier method to improve the accuracy of indoor localisation. Tracking information are

sent from the lost mobile to the recipient via the Internet mainly or using SMS messages. The results can be presented by either text or a GUI using Google Maps [79].

The Internet channel GSM/ GPRS is also used in a system that used to identify wheelchair location information, GPS and GSM network are used to find the location of the user, the Tian et al. system module is connected to a microcontroller, to the web-based management server. The server then receives the wheelchair's information and displays its location using Google Maps. The system overview is shown in Figure 4-1 [23].

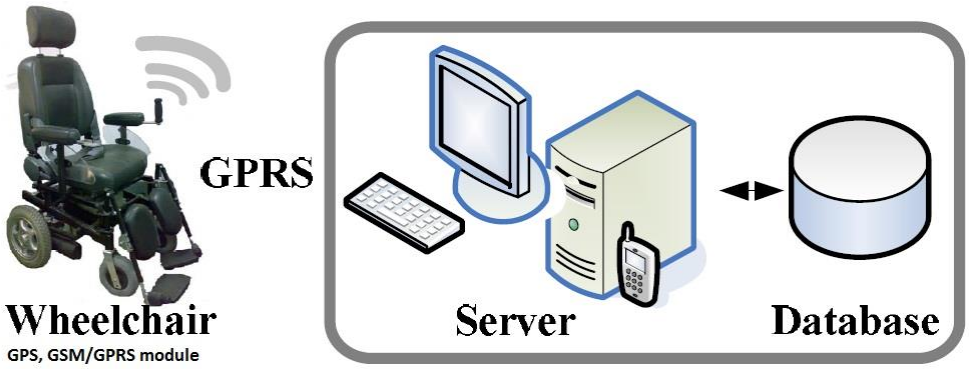


Figure 4-1 Wheelchair Positioning System [23]

Hasemann provided a method that dispatches the information request as an unstructured supplementary service data (USSD) code, so the incoming USSD code for LBS is identified by the mobile operator. The problem is that the user has to know which USSD code to use and what code stands for which service, so requested location-based information can be sent to the user graphically via SMS/MMS, and the user can select whether to receive the required information graphically, acoustically or in another way [80].

To find the location of the user, Panahi et al., used GPS to obtain a tourist's current location. The system also uses cellular networks and Wi-Fi to record any change in the user's position when GPS is unavailable. An XML file is used which contains information on the location requested by the user. The Internet is used for transmitted data. However, the system uses a cloud-based middleware server to store the data from the LBS provider, so when the user is not connected to the Internet, he/she can get the information from the middleware server instead of communicating with the end server. The middleware is used to provide service that generates XML output to be used to communicate with the mobile application. Figure 4-2 shows a diagram of the system [81].

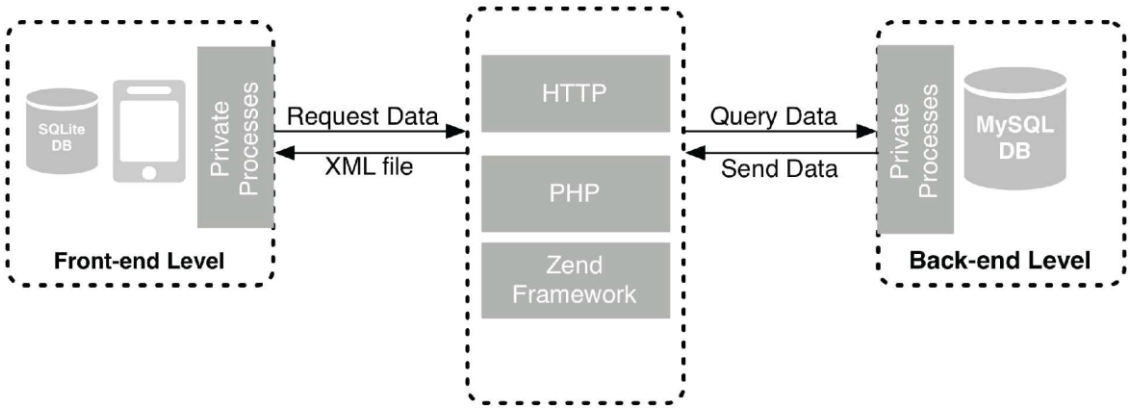


Figure 4-2 Middleware-Based LBS [81]

Fogue et al. proposed a design that can be placed in a car to send notifications to the PSAP when it is involved in an accident. The system has sensors all around the car that are activated when there is a collision. The communication network proposed in this solution is vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). Once the information from the sensors is collected, it is sent via the UMTS network data channel to the PSAP [82].

Chaklader et al. designed a system that is used in case of a car accident. A black box is placed in the vehicle, which collects its location when there is an accident, then sends notifications to the emergency rescue services using the Global System for Mobile Communications (GSM) text service [24].

Winston et al., use a random access channel (RACH), which is a control channel in the vehicular communication to send information and control signal to the data providers [83]. Instead of the usual standard packet channel, they use the data filed in the RACH structure to send the data. This system is close to our proposed system, but the main different is that our proposed system uses the spare extension in the RACH instead of the data field like in Winston system.

The transmission of the disaster warning messages is one important service offered by the LBS. Hongsheng used the digital audio broadcast (DAB) to send emergency warnings. The method used two DAB transmitters to establish a bidirectional multimedia communication. It can be used in an area where the disaster might happen, and it uses computers attached with dongles so that messages can be transmitted and received [84].

Another system called mKRISHI uses VHS transmission, satellite communication or mobile phones to warn fishermen about an upcoming disaster. It is used to warn the fishermen in the sea or near the coast if any disaster is coming, like a hurricane or tsunami. All the data are stored in the web based system and sent directly to the fishermen [85].

Jinggangshan's geological disaster prevention management information system uses the sensors to check the weather and land condition with video surveillance data based on wireless sensor network to predict and send early warnings. The sensors used the GPRS to send the early warning information to the cloud and then the monitoring system sends the warning messages to the users as a real-time video stream transmission via the Internet [86]. The Wireless Sensor Networks (WSN) are proposed along with Unmanned Aerial Vehicles (UAV) to collect information about the natural disaster in [87] where the Internet is the main communication between the WSN sink and the data centre.

Similarly, one system was designed and implemented using WSN with integrated ultrasound sensors to transmit an emergency data and the Internet is the main backhaul between the WSN and the data centre [88].

Also, mobile phones are used in another research study by Solmaz to act like a sensor and are used to evacuate visitors in a park in case of disaster or emergency. In this case, the sink mobile broadcasts a message to sensor nodes and the WSN is used to carry this message to all visitors [89].

Social media such as Twitter can also be used as a platform to warn people about disasters. Twitter in particular has been used in Tsunami Warning and Response Social Media System (TWRsms) to warn about incoming disaster [90]. Similarly, Twitter has been used by Carley in Indonesia to warn people about incoming tsunamis [91]. Social media like Facebook and WhatsApp can also be used after disasters to ask for support like shelter and blood donation [34].

The e-Health system is considereda one location-based service that attracts many researchers to improve its components and architecture to fulfil its requirements [20, 21]. like in AMMA system which uses the Internet of the code division multiple access (CDMA) cellular network to send patient information, which uses an agent based mobile middleware architecture from the ambulance Also, the packet channel in the third-generation (3G) mobile network is used in the Gallego system, which delivers biomedical information from the ambulance to the hospital [21]. Prakoso also used a secure system to preserve patient medical information when sending it to the doctor in hospitals at a distance for monitoring and diagnosis, and the connection used in this system is the Internet [25].

Another healthcare system framework is designed by Haung et al. to collect medical data from Wireless Body Area Network sensors, and send the information to a gateway in a

secure way to protect the user information and then send it to the hospital using the Internet or the packet channel of the CDMA [92].

vNurse system is presented by Rehunathan et al., which is based on a smartphone platform that makes a secure patient remote monitoring outside a clinic or hospital. It uses full Internet Protocol (IP) for the connection, and uses attached WBANs to check the patient situation while he/she is away [93].

In some situations, a quick medical response is needed. Patients being taken to hospitals by cars could get stuck in traffic [22]. For this reason, Misbahuddin et al. presented a new scheme to transfer patient health data to the hospital using ZigBee technology. If the ZigBee is not available the Wi-Fi will be used and if the Wi-Fi is not present the cellular network will be used after classifying patients based on their condition [22]. Brahmi et al. also proposed a similar enhanced scheme for IEEE 802.15.4 protocol to ensure fast transmission on the road in the event of a car accident for the emergency service. By using this scheme the time delay will be shorter for carrying important messages and information [94].

4.2 Data Transmission

Some works do not use location-based service, but rather new efficient methods to transmit data to the server or core network, and as our proposed design transmits data to the core network, a literature review of this type of system has been presented.

Shahbazi et al. presented a system where data modems are used to transmit data over the voice channel. The input data is converted from serial to parallel as blocks, and each K-bit of data are converted to a symbol and considered as an index of the codebook (database). At the receiver, the signal is decoded back to symbols, fed to the demodulator and converted back to blocks of K-bit data from the code book. The system needs a computer at each terminal as well as a mobile phone to complete the transmission of data [95]. Figure 4-3 shows Shahbazi system.

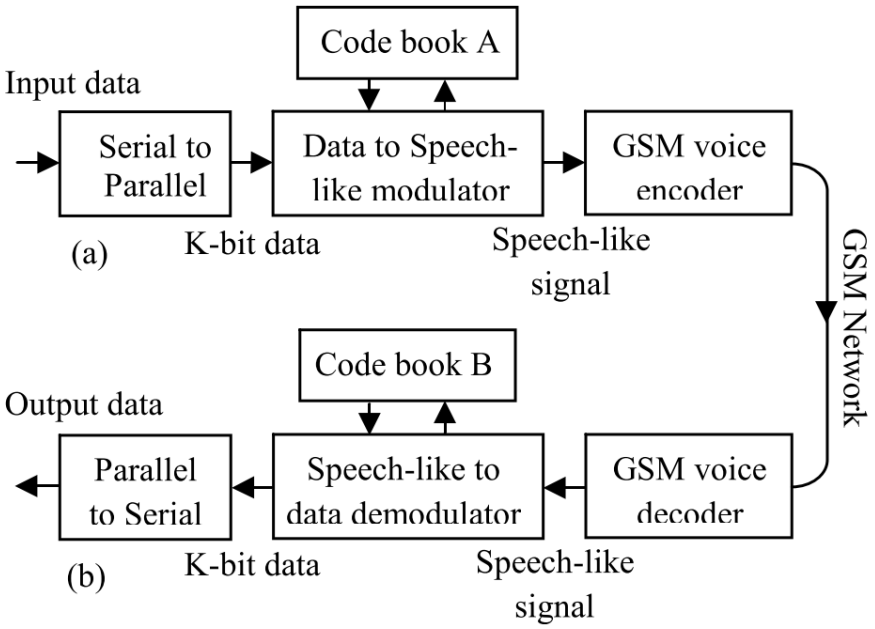


Figure 4-3 Overall Modem Structure (a) Transmitter (b) Receiver [95]

LaDue et al. also designed a system that transfers data by using a modem through a compressed speech medium. This modem is an addition to the existing GSM system (Figure 4-4). The modem converts input data to a pulse-code modulation stream and feeds it into a GSM mobile unit, which encodes and modulates this signal using GSM standards and sends it over the air [96].

Figure 4-4 LaDue et al.'s System

Anisette presented a solution based on received signal strength indication (RSSI) to locate a user, with the data collected and managed by GSM or 3G networks; so the transmission uses the Internet or packet channel just like the standard, and the data provider is any third-party server [9].

Ali et al. proposed and evaluated a system for data transmission over a mobile voice channel based on multiple frequency-shift keying (M-FSK) modulation with optimised parameters.

The parameters of the M-FSK modulation are tuned using real mobile communication voice channels. Figure 4-5 shows Ali et al.'s system [97].

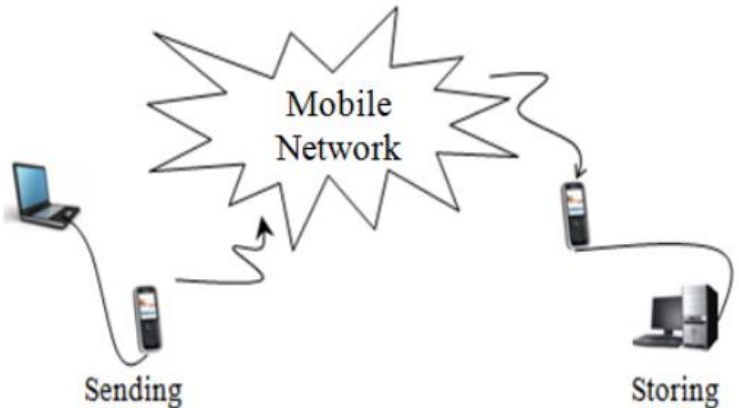


Figure 4-5 Ali et al.'s Test Bed [97]

Another system built by Ghosh et al. also uses the mobile communication voice channel to communicate and send the data to a central location centre for analysis [98].

Peric et al. designed a low bit-rate transmission over a voice channel in GSM using a modem to transmit small amounts of data [99].

4.3 Privacy Protection

In recent years, there have been many researchers working to protect user privacy in LBS while maintaining response time and accuracy. Even though there is a debate about the privacy of the user's location, some researchers claim the users are not concerned whether their location is being shared with other organizations and third parties [39, 41, 100-103], while others believe it is important to have their location kept confidential, especially if it could be shared with commercial advertising agents [39-41]. Lin et al. did a study about user concern about their privacy and showed that people also behave differently about their location if they are in work or at home [104].

There are many methods to protect this privacy such as adding anonymizer, spatial and temporal cloaking where an approximate location is sent to the server instead of the exact value or, for example, by sending the nearest neighbour location instead of the real one. This technique, however, has poor accuracy and a bad response time. Another approach is to transform the location so that the system sends a transformed user position to preserve user location privacy [4, 105]. Adding an anonymizer to the network will not solve the privacy issues, as the security and confidentiality risks are transferred from the data and service provider to the anonymizer [106].

The above methods are the most popular among researchers, but there are other methods available to protect user privacy.

Schlegel et al., present a dynamic grid system design that uses a query server between the user and the service provider. The request for the user and the cell identifier are encrypted before being sent to the third-party service provider to keep the user's privacy secured [107]. Figure 4-6 shows the system architecture.

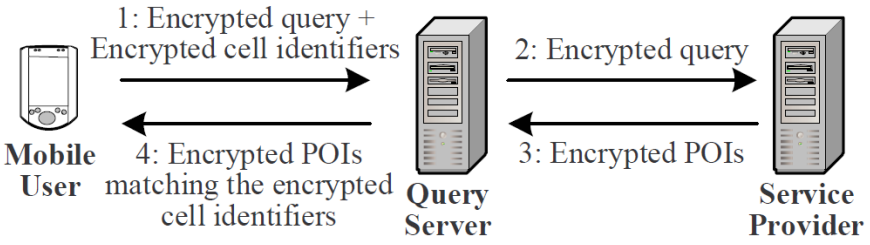


Figure 4-6 Schlegel et al.'s System Design [107]

An architecture to protect identity privacy in the LBS is proposed by Dewri et al., [108] whereby a user-centric design can share the user location just after the user has evaluated the impact of the service quality and accuracy.

A new framework, called KAWCR, to protect privacy in the LBS has been proposed. KAWCR use a centralised server, which must be a trusted third-party in the system as an anonymizer to hide and protect user privacy [109]. Other researchers like Gan et al. and Hyunjo et al. also used the anonymiser to hide the user information [110, 111].

A solution to preserve user location and privacy by obfuscating location information are presented by Ardagna et al. The research focuses on developing techniques to protect a single sample of a location [112].

A 3PULS system that used pseudo-location to preserve user's information are proposed by Niu et al. 3PLUS uses k-anonymity for user's location privacy with a higher probability. A set of pseudo-locations is kept in the server buffers, and these pseudo-locations contain two parts, namely part of a location obtained from previous user locations, and the other part is randomly exchanged with encountered users [113].

An enhanced-location-privacy-preserving scheme for the LBS environment has been proposed by Peng et al., where it distributes the spatial information periodically, and the real location is encrypted by the pseudo-location to preserve user's information [106].

Myungah et al. added a Post office box (POB) server to the LBS system architecture. The LBS server receives the user request from the POB server but the POB cannot access the

query and information. The answer will be generated by LBS server and sent back to the POB without knowing the user's identity. POB server in turn sends the request back to the requester without knowing its content [114]. Tang et al., also designed a similar system but with a different algorithm to anonymise the user data [115], as they proposed a decentralised privacy-preserving scheme with a two-phase forwarding method and a key management protocol. It first disconnects the user from the data provider when the server receives the request to protect the user identity and then adds an efficient pseudonym mechanism.

4.4 Summary

The location based service attracts the researchers to develop and improve its services and architecture. The literature review focuses on the location based service transmission method, but there are some cases where they have used a new and effective transmission method without using it in LBS.

In summary, most of the location based service systems use the Internet to send the information from the user to the core network or to the data and service provider, the disadvantage of using the Internet is that the user could have no Internet access. However, some projects have sent information to the core network using voice channel and a modem. The main disadvantage of this method is the need for additional hardware and/or software to complete the connection. Table 4-1 shows the transmission methods that could be used in the LBS systems.

Table 4-1 Comparison of Transmission Methods

System	Year	Data transmission methods	Disadvantage
3GPP eCall	2008	GPRS	The users will not have an LBS if they has no Internet connection.
Sukaphat	2011	Internet	
Tian et al.	2009	Internet	
Anisette	2011	Internet	
Panahi et al	2013	Internet	
Chaklader et al.	2014	GSM	
mKRISHI	2016	GPRS	
Jinggangshan's	2015	GPRS	
AMMA	2005	Internet	

Prakoso	2016	Internet	
Haung et al.	2017	Internet	
TWRsms	2016	Social media/Internet	
Carley et al	2016	Social media/Internet	
Basu et al	2017	Social media/Internet	
Fogue et al.	2012	V2V and mobile Internet.	The users will not have an LBS if they have no Internet connection and if the V2V or WSN is used, there should be a series of vehicles/sensors to carry the signal.
Erdelj	2017	WSN and Internet	
Erd et al	2016	WSN and Internet	
Solmaz et al	2017	WSN and Internet	
vNurse	2011	WBAN and Internet	
Misbahuddin et al	2012	zigbee and Internet	
3GPP eCall in-band modem	2017	Data over voice using modem	Additional hardware is needed (modem or and computers)
Shahbazi et al.	2010	Data over voice using modem	
LaDue	2008	Data over voice using modem	
Ali et al.	2013	Data over voice using modem	
Ghosh et al.	2015	Data over voice using modem	
Peric et al.	2015	Data over voice using modem	
Hongsheng	2017	Digital Audio Broadcast	
Winston et al.	2014	Data filed in the RACH	The data field of the RACH is used which is already has a control data and could cause bigger number of slots and frames which leads to higher delay

Hasemann	2012	USSD	The user needs to know which code to use when requesting a specific service

Also, in the related work and as privacy issues are one of the most important issues in the LBS, the selected work has been reviewed. There are many ways to protect the user information suggested by the researchers, such as adding a server to act like an anonymiser to encrypt the user information, the disadvantage of using a third party server as an anonymiser is the increment of the interferences between the core network and the data provider in addition to response time increment, another method to protect the user privacy is by using a cloaking method by giving a location nearby the user's location, the main disadvantage is the poor accuracy in addition to the disadvantage mentioned in the first method. Table 4-2 shows the summary of the methods used.

Table 4-2 Comparison Among Privacy Protection Methods

System	Year	Privacy protection methods	Disadvantage
Schlegel et al.	2015	server between the user and the service provider	increment of the interferences between the core network and the data provider in addition to response time increment
Dewri et al.	2014	server between the user and the service provider	
KAWCR	2010	use a centralised server as an anonymizer	
Gan et al.	2016	Server in the middle as anonymizer	
Hyunjo et al.	2012	Server in the middle as anonymizer	
Myungah et al	2017	Server in the middle as anonymizer	
Ardagna et al.	2011	In middle server for obfuscating location information	Poor accuracy.

3PULS	2013	In middle server for obfuscating location information	
Peng et al.,	2017	In middle server for obfuscating location information	
Tang et al.,	2017	decentralised privacy-preserving scheme with a two-phase forwarding method	Poor accuracy with complexity

In this thesis, the proposed method used the control channels to carry the information between the user and the core network, which gives the system a new connection that is always available even if the user has no Internet connection with faster data transfer. Moreover, the method used a new core network architecture to protect the user privacy without sharing the information with third-party servers.

Chapter Five: Proposed Design

As mentioned earlier in the previous chapters, LBS architecture is comprised of mobile devices, a communication network, positioning components, a service and data provider [6]. Generally, LBS use the Internet to send and receive information from the core network. In the proposed design, the control channels are used to transmit the data from the user to and from the mobile operator's core network instead of the Internet. A new architecture that uses the database(s) within the operator network is proposed to solve the privacy issues and to obtain a more efficient response time.

Usually, the LBS are operated by independent third-parties that provide services based on the location of mobile users [116], which leads to more interference between the operator and the service provider, costing the operator and the service provider money and time to maintain this connection between them. For this reason, in the proposed design, the mobile operator provides the LBS by adding one or more databases to the mobile CN containing the service information and location. The proposed design can be divided into three main stages. These stages are:

1- The uplink stage; where the user asks for a specific service like a location.
2- The database; which is located in the mobile operator core network, and could be one or more databases depending on the mobile operator architecture. This database has all the location and information of places that the user might ask for.
3- The downlink stage; where the mobile operator sends the information to the user who asked for this information. Figure 5-1 shows the top level of the proposed design architecture.

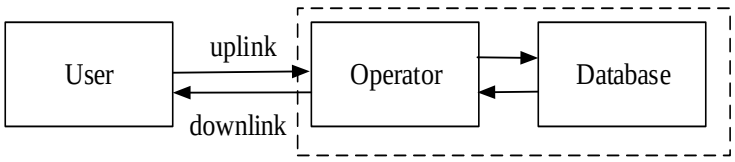


Figure 5-1 Top Level of The Proposed Design

5.1 The Uplink Stage

The uplink is the information transferred from the user to the core network or to the data and service provider. When the user requests a service, such as looking for the location of the nearest hospital, the request is sent to the mobile operator. However, when he/she asks the system to provide coordinates of a specific location, it is essential to find the location of the

user first, using one of the standard positioning techniques with the assistance of the mobile network or GPS. These techniques may be one of the following: cell origin, time of arrival, time difference of arrival, the angle of arrival or received signal strength [117].

The service provider then tries to find the nearest service that the user requested and locates its coordinates depending on the user's location, which is the next step.

In the uplink, the mobile sends the user information and the user's request to the mobile operator through several stages (Figure 5-2):

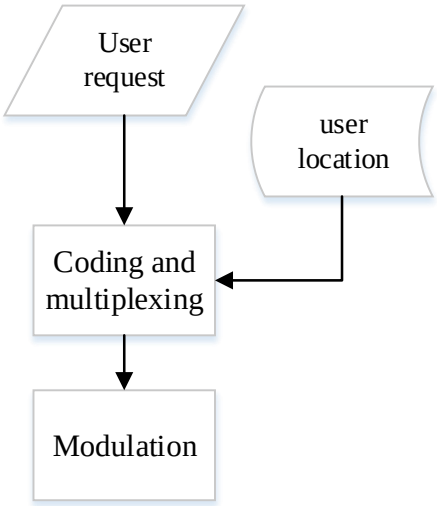


Figure 5-2 Uplink Stages

- In the beginning, the user asks for the coordinates of a location (for example, a hospital) using a mobile phone; the mobile network then locates the user and sends this information together to the service and data provider.
- The second step is to convert the user request to binary and then organise this information and insert it in the spare extension in the RACH frame. The data then separates into multiple slots and is mapped into the PRACH. If the data cannot fit in one slot it will take the next slot, and if all slots in one frame are filled, the data will take the second next frame, as shown in Figure 5-3. As the RACH, which is mapped into a PRACH, is used to transmit control information to perform location updates [118] and because the RACH is the first signal sent to the operator, the proposed design uses the RACH for the uplink to carry the user requests with the location update.

- Finally, those data are converted into symbols to be modulated and transmitted. The UMTS uses QPSK in the uplink and downlink channels and uses a root-raised cosine filter for pulse shaping [62].

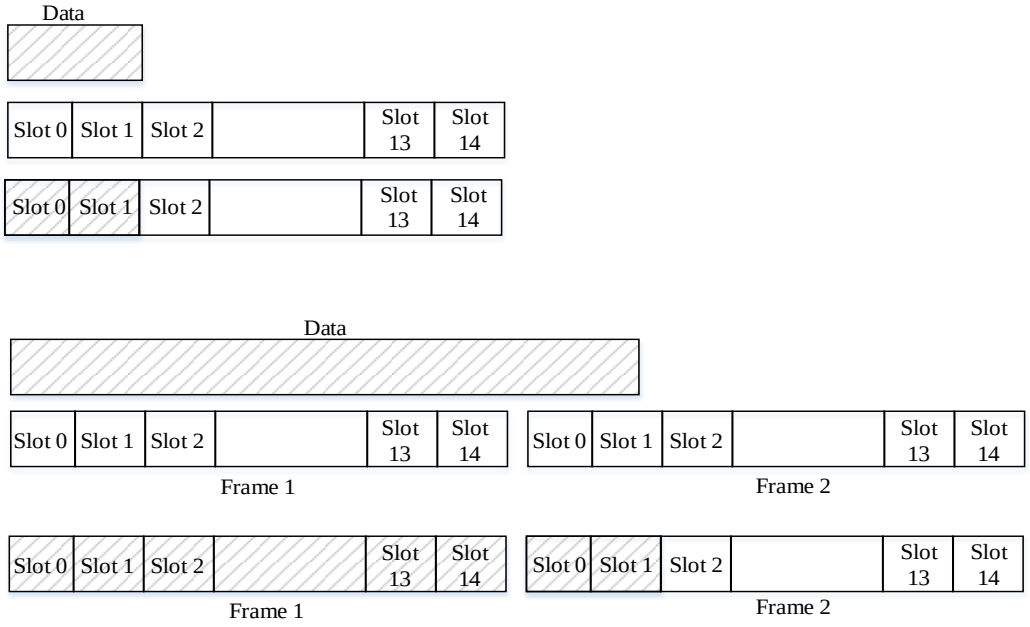


Figure 5-3 Data Mapped into Slots and Frame

The size of the frame is changeable depending on the spreading factors of the system and frame configuration; the NEW IEIF field in the payload can be configured to change the frame configuration where if bit 0 of New IEFI is set to one, the Cell Portion ID field is present. Otherwise, the field will not present. Moreover, if bit 1 of New IEFI is set to one the Ext Propagation Delay IE is present and when it sets to zero the field is not present [57]. Figure 5-4 shows the payload part or the RACH. The full description of the RACH frame can be found in previous chapters.

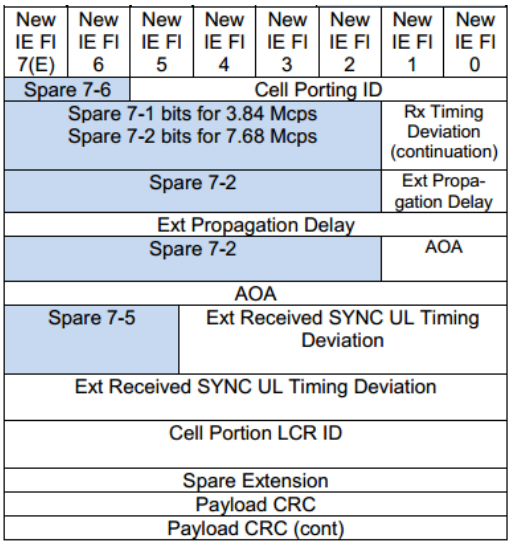


Figure 5-4 RACH Payload

The frame is divided into two main sections: header and payload. At the header the FT is set to 1 if the frame carries data, or 0 if it carries control signals. CFN and TFI are generated randomly for the first frame using functions, and the header's CRC is calculated and filled in its field after the header is filled with needed information, Figure 5-5 shows the RACH header. The spare extension at the payload in normal and standard systems is set to zeros and sent to the receiver. It can carry up to 28 bytes of information [57]. While in the proposed design the spare extension is used to carry the user request. Moreover, it depends on the size of the user request, as the spare extension can carry up to 28 characters, whilst if the user request is less than 28, padding will be added to fill the spare extension.

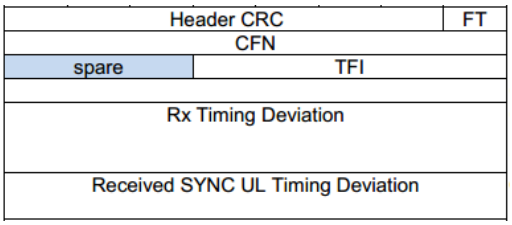


Figure 5-5 RACH Header

After the data payload is filled with all necessary information and the user request is converted into binary and put in the spare extension of the frame, the CRC calculation is resumed. The CRC is the calculation that uses polynomial division, and it is attached to the payload to check the payload error and to the header to check the header error. The polynom that is used in the header is [57, 119]:

$$X^7 + X^6 + X^2 + 1 \qquad 5.1$$

And the polynom used in payload is

$$X^{16} + X^{15} + X^2 + 1 \qquad 5.2$$

The CRC calculation starts from FT field to the last bit of the header and from the first bit to the end of the spare extension on the payload. It has two inputs and one output; the inputs are the number that we want to calculate the CRC for, and the "generator polynomial" in the form of bits is multiplied by the x^n. The generator polynomial can be presented in binary form like [1 1 0 0 0 1 0 1] for $X^7+X^6+X^2+1$.

$$1 * x^7 \ + 1 * x^6 + 0 * x^5 + 0 * x^4 + 0 * x^3 + 1 * x^2 + 0 * x^1 + 1 * x^0$$
$$= \ x^7 + x^6 + x^2 + 1$$

In the payload, the size of the Transport blocks (TB) are defined and generated randomly, and the spare extension is used to send the user request as mentioned before. The data in the spare extension can be obtained by calling a function, which gets the input from the keyboard then converts this value into binary and reshapes it to a matrix of 8 bits, as follows:

```
function UserRequest
      get the user request
      convert it to binary
      reshape it to the matrix of n by 8 bits
return
```

The next step is to convert the data in the frames from binary to the symbol to prepare it before it is sent to the next stages: channel coding, spreading and then modulating, where QPSK is used to modulate the signal that carries the information to the core network. The design procedure can be seen in Figure 5-6.

All the spreading factors for RACH are taken into consideration, so the spreading factors could be one of the following spreading factors (32, 64, 128 and 256). At the end of this stage, the data are transmitted from the terminal and will be managed to be forwarded to the core network by UTRAN.

5.2 Backhaul Connection

In order to send the information to the core network from the UTRAN, a backhaul protocol is implemented, which is the AAL2. In a network, the AAL2 is used to transfer data in IuCS domain [120]. Moreover, the mobile network can use many options to build the backhaul like E1/T1 connection, Ethernet or DSL. The media used can be either copper, which can

carry the E1/T1, fibre optics (SDH, SONET), or microwave, which is the best for the long distance and the most common among them [121].

This backhaul can be used in both directions from the core network to the UTRAN or vice versa. The standard design is used in the system, so no change has been made to this connection. However, in order to send the information to the core network, the backhaul has been implemented.

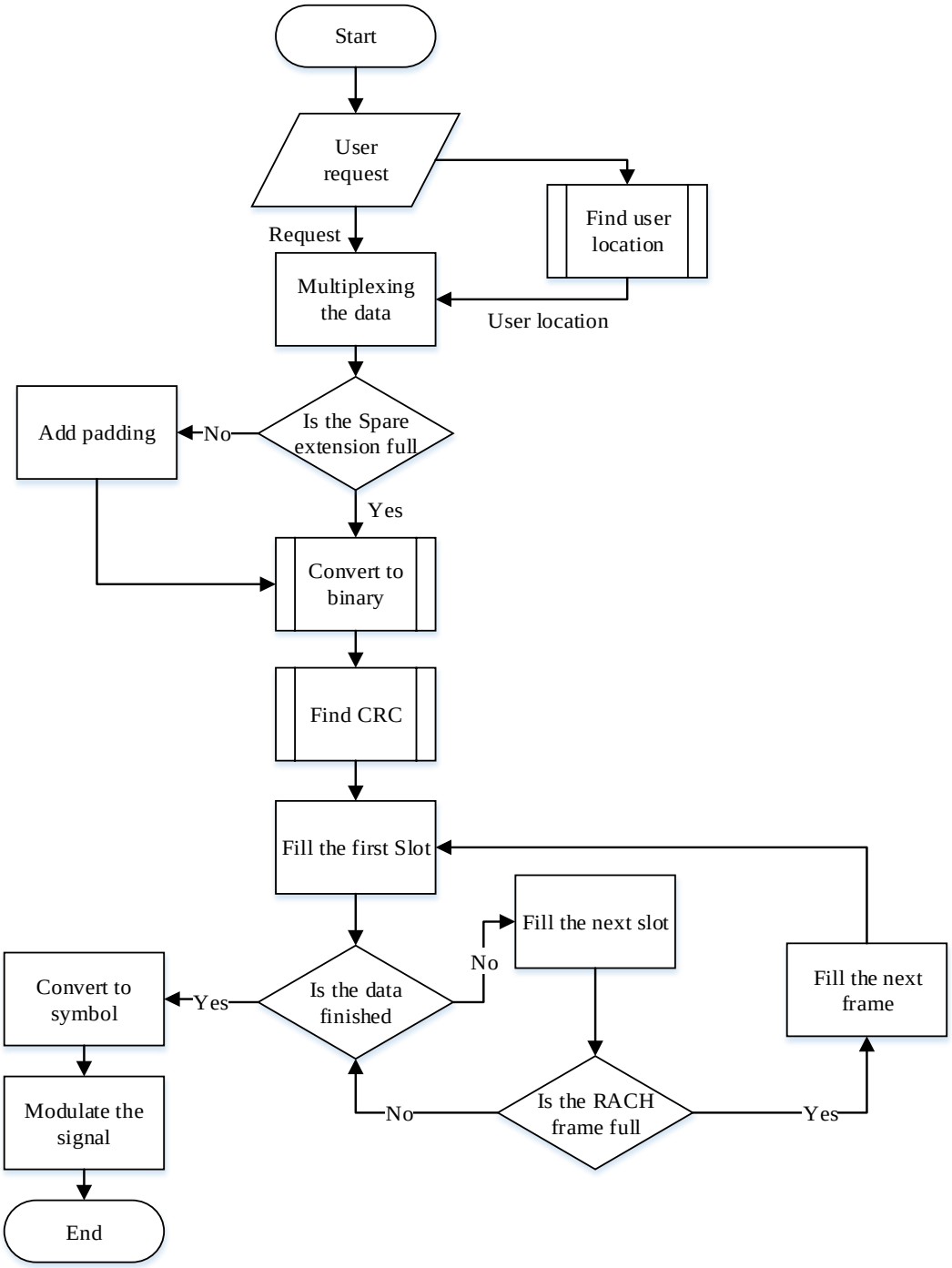


Figure 5-6 Uplink Flowchart

5.3 Core Network

The core network (CN) is used to connect the UTRAN with the data and service provider, and in the 3GPP standard system the data and service provider are a third party connected to the network through the GMLC. See Figure 5-7.

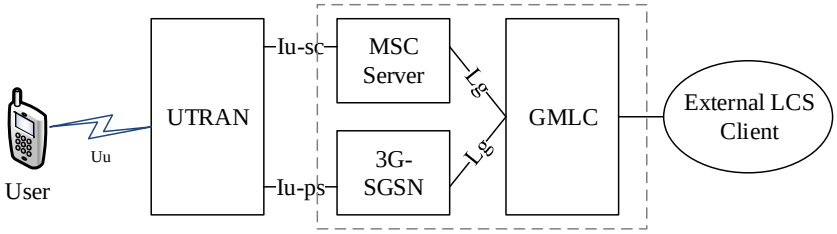


Figure 5-7 Simple Core Network

The use of a third party LCS client raises some concern related to the user privacy and response time. For this reason, in this thesis, some changes have been made to the core network in order to tackle the issues.

The new design in this thesis added a database to the core network attached to the GMLC; this database has all the location and information for interesting places that the network covers. Figure 5-8 shows the new core network with added database.

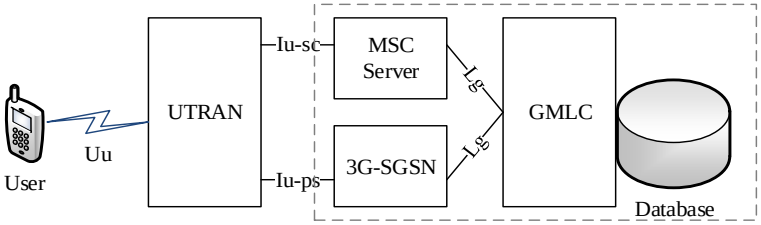


Figure 5-8 The New Design Core Network with One GMLC

In some cases, there will be more than GMLC in order to reduce the load in one GMLC, and the mobile operator can configure and change the number of GMLC depending on its requirement [11]. As there could be more than one option for the GMLC number, the proposed design considered the other option as well, and Figure 5-9 shows the core network with multiple GMLC and a database to each GMLC.

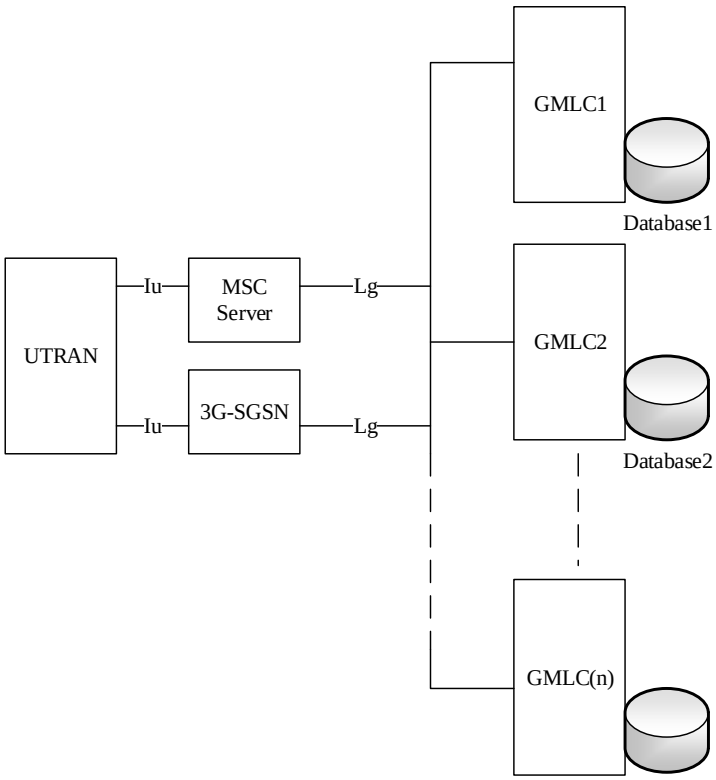


Figure 5-9 Core Network with Multiple GMLCs

So, if the request arrived from the MSC to the GMLC. The GMLC checks the attached database for the required information and sends the information back to the MSC which then forward it to the UTRAN. If the system architecture has more than one GMLC, the requested information will be checked if it is in the attached database of the H-GMLC, if not, it will forward it to another GMLC, and then send the information back to the user via UTRAN. The H-GMLC is the GMLC that the user belongs to. Figure 5-10 shows the Core network procedure.

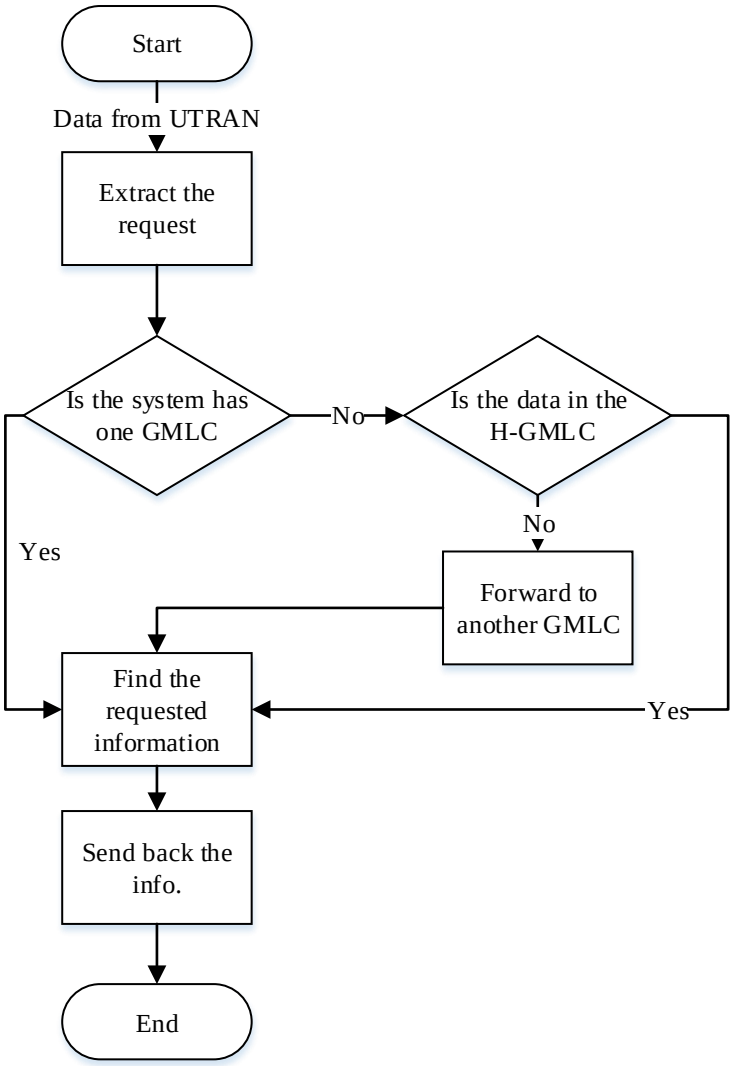


Figure 5-10 Core Network Flowchart

5.4 LBS Database

Each GMLC is attached to a database, which acts as the LCS client database, so the data no longer needs to be sent to a third part company, which after all might pose a threat to privacy and may not be trusted. Instead the mobile operator will provide the data and content to the system. As an example, in the thesis, a database is built with all the major hotels in the city of Manchester, with the coordinates of each hotel and some information, see Figure 5-11. The GMLC receives the user request to look for a specific named hotel; the GMLC then checks its database to fulfil the user's request, and when the user's request location is found, the coordinates are sent back to the MSC by the GMLC and then to the user via UTRAN.

2	247 hotel	53.507722	-2.359604	hotel
3	ascott	53.487234	-2.3418	hotel
4	beaucliffe hotel	53.489183	-2.325433	hotel
5	britannia inn	53.519526	-2.333594	hotel
6	citysuits	53.485474	-2.246396	hotel
7	copperheads	53.483511	-2.256611	hotel
8	copthorne hotel manchester	53.467987	-2.284395	hotel
9	fairways lodge	53.518431	-2.276768	hotel
10	hellohotel	53.5051	-2.346187	hotel
11	holiday inn express manchester salford quays	53.470129	-2.28871	hotel
12	holiday inn manchester mediacityul	53.473092	-2.299387	hotel
13	holiday inn manchester west	53.479758	-2.269377	hotel
14	hotel campanile manchester salford	53.476257	-2.263886	hotel
15	hotel extras	53.488053	-2.246837	hotel
16	hotel ibis budget manchester salford quays	53.469722	-2.282605	hotel
17	ibis manchester charles street	53.492619	-2.291799	hotel
18	ivy mount guest house	53.489167	-2.333795	hotel
19	lamb hotel	53.483419	-2.333451	hotel
20	lord nelson	53.518201	-2.331375	hotel
21	premier inn manchester city centre arena printworks hot	53.484986	-2.246789	hotel
22	premier inn manchester salford quays media city	53.471311	-2.28755	hotel
23	premier inn manchester swinton	53.58201	-2.312306	hotel
24	ramada manchester salford quays	53.469802	-2.282614	hotel
25	restaurant & hotel isis	53.512123	-2.322592	hotel
26	rockhouse hotel	53.474655	-2.356543	hotel
27	royal oak	53.481926	-2.340304	hotel
28	stay inn	53.486596	-2.254523	hotel
29	the ainscow	53.482479	-2.258226	hotel
30	the edgerton arm	53.483223	-2.25529	hotel
31	the grapes hotel	53.478695	-2.36478	hotel
32	the hazeldean	53.514437	-2.268258	hotel
33	the lowery	53.483108	-2.250521	hotel

Figure 5-11 Manchester's Hotel's Database

In the standard design, third party companies are used as an LCS client, which has a database with all the location information, so when the GMLC want to check the location of the point of interest, it will send the request via the Internet to the LCS client. In the proposed design, the database is built and attached to the same GMLC. Moreover, as mentioned earlier, there are some systems, which use multiple GMLC and thus, the proposed design also implemented this type of system with a database attached to them. This approach could improve the privacy but because there will be more connection and routes in the network it could take more response time, and the chance of packet drop may increase [122]. The proposed design implemented the following options and compared them to check the difference and calculate the response time from the request being sent by the GMLC to the database and getting the result back to the GMLC:

- A server acts like a GMLC attaching a database to it.
- More than one server acts like GMLCs with a database attached to each one; one GMLC will be the H-GMLC which the user belongs to, and the other GMLC will be R-GMLC that received the location request.

- A server acts like an LCS client with a database attached to it, and the GMLC communicates to this server via the Internet.

Figure 5-12 shows the three types of database attachement architecture where A shows a single GMLC, B is more than one GMLC, and C is the GMLC connected to a third party LCS client.

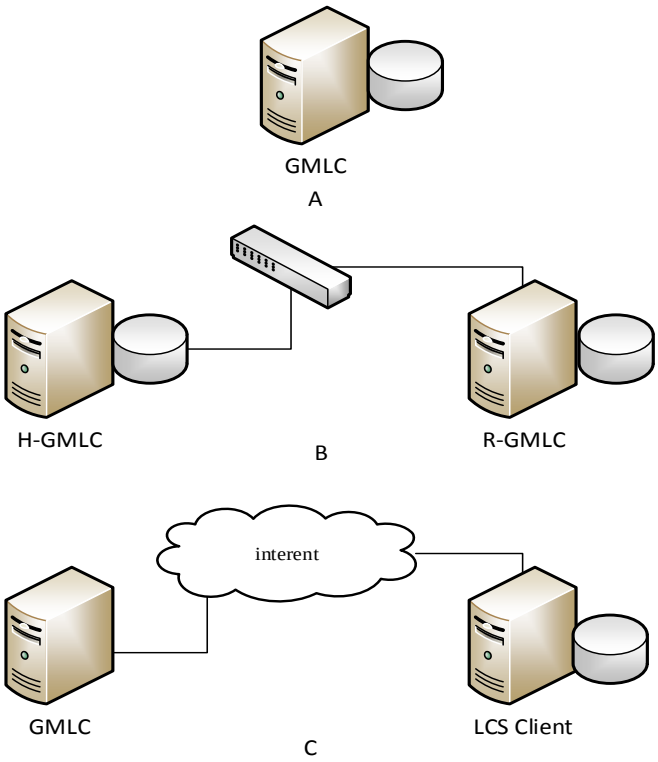


Figure 5-12 Three Different Types of Architecture

5.5 The Downlink

The downlink is similar to the uplink, but the operation is in the opposite order; the downlink is the information transfer from the core network to the user. The UTRAN receives the location or the information from the core network, and this information are obtained from the data provider. In the downlink the data goes through several stages (Figure 5-13):

- First, the data is transmitted by the core network carrying location information
- Then the location is converted to binary and organised, and inserted into the spare extension of the FACH frame
- The data are then separated into many slots to be carried by the S-CCPCH, if that data cannot be fitted into one slot, it will take the next slots, and also if the data cannot be fitted into one frame it could take more than one frame.
- At last, the information converted to symbols and sent to be modulated using QPSK

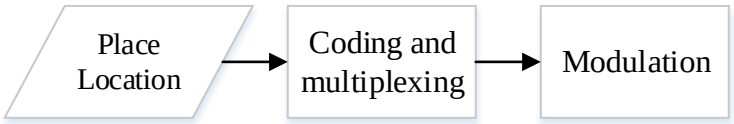


Figure 5-13 Downlink Stages

The frame header carries information like FT, CFN, and information about the power level. In the implementation the CFN, TFI and the power level for the first frame are obtained from functions to get random numbers. Figure 5-14 shows the FACH header.

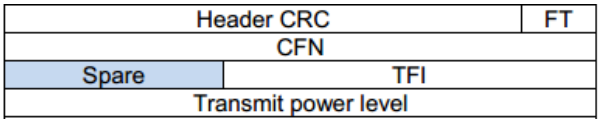


Figure 5-14 FACH Header

The other part of the frame is the payload, and just like the RACH in the uplink, the size of FACH frame is changeable according to many factors, like slot format, frame configuration and the spreading factors. The NEW IEFI also play a role in the frame size that if bit 0 of New IEFI in the payload is set to one, the AOA IE field is present, otherwise the field will not be present. Moreover, if bit 1 of New IEFI is set to one, the Cell Portion LCR ID IE is present and when it is set to zero, the field is not be present [57]. Figure 5-15 shows the FACH payload.

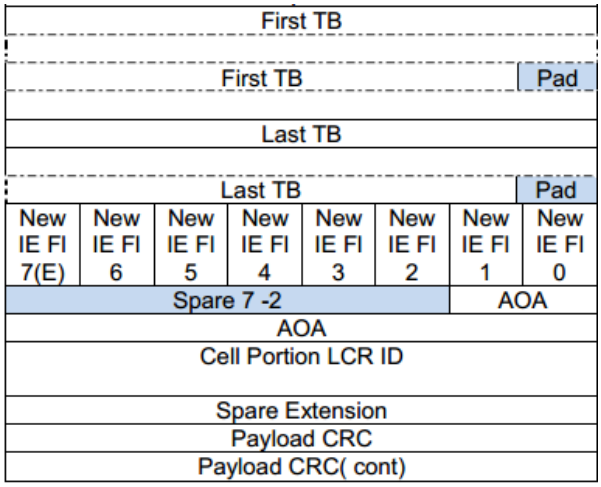


Figure 5-15 FACH Payload

The spare extension in the FACH payload in normal systems is filled with zeros and sent to the receiver, which then neglects the spare extension [57]. In the proposed design in this thesis, the spare extension of the FACH is used to carry the location information from the

data and service provider. The spare extension can carry up to 28 characters and when the data are less than 28 it will be filled with padding until it reaches 28. Usually, in LBS, the spare extension carries the coordinates of a location that the user asked for.

When the header is filled with the necessary information, the CRC will be calculated and added to the header, and this is the same situation for the payload but with the different polynom. The CRCs used in the downlink for the FACH are the same as those used in the uplink in the RACH [57, 119].

Now the FACH frame is ready to be mapped into the S-CCPCH. The data are separated into multiple slots depending on the data size. If the FACH frame is bigger than the slot, the next slot will be used, and if all slots in the first frame are filled, the next frame will be used. Then the data are converted to symbols and modulated using QPSK. Figure 5-16 shows the downlink flowchart.

In the end, when the data are received by the UE, it is extracted from the spare extension of the FACH frame and converted into something the user can understand, either text, image or points on the map.

All the possible spreading factors for S-CCPCH are taken into consideration in this thesis, so the spreading factors could be one of the following spreading factors (4, 8, 16, 32, 64, 128 or 256).

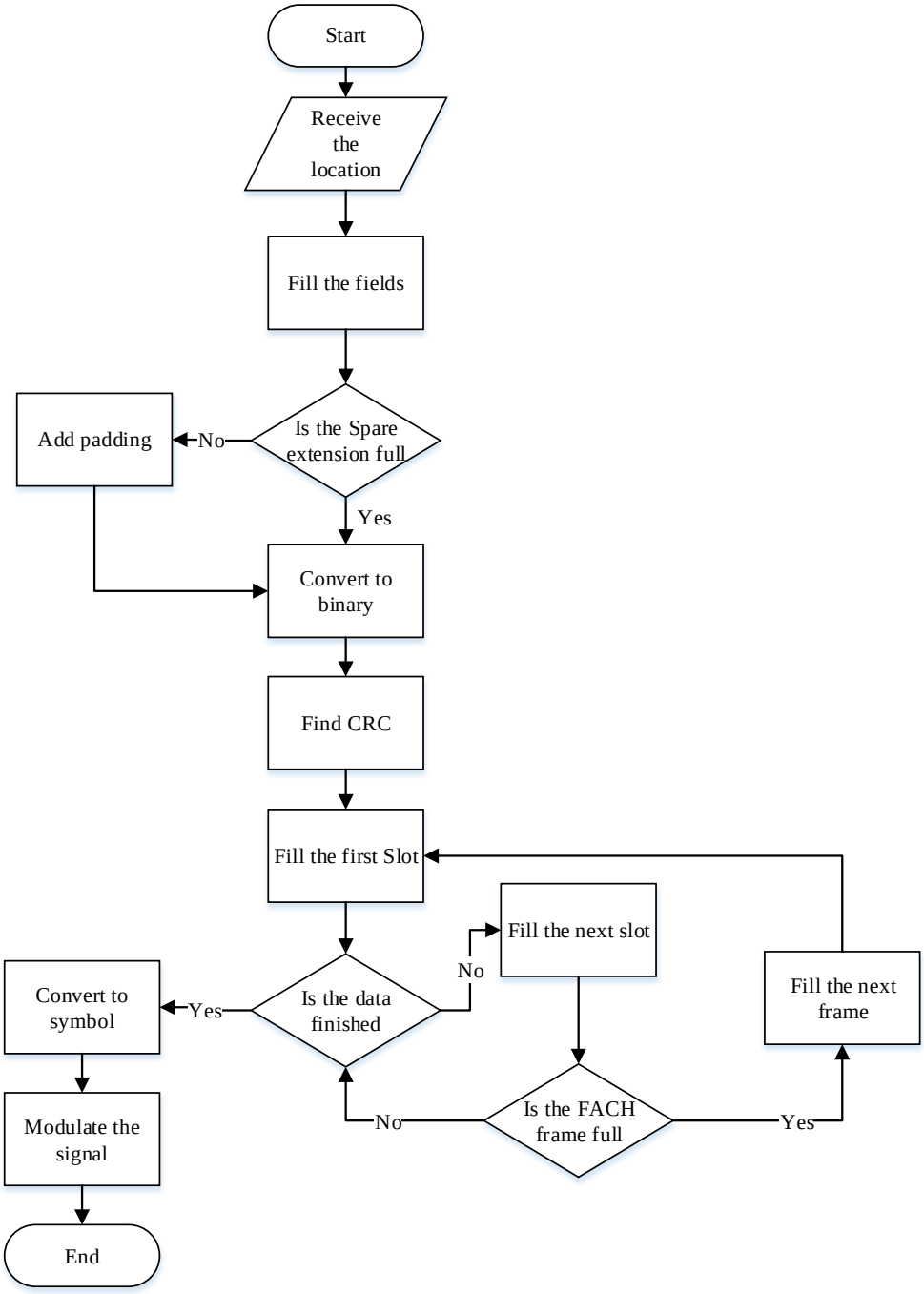


Figure 5-16 Downlink Flowchart

5.6 Summary

In this chapter the proposed design is introduced, and divided into three main sections: Uplink stage, core network, and the downlink stage.

In the uplink stage the user request is transmitted from the user side to the core network via the UTRAN, and the design uses the spare extension of the RACH to send this request. The RACH is carried by the PRACH and modulated using the QPSK.

In the core network, the request is received by the mobile operator and checks the database that is attached to the GMLC. In some networks, it could be more than one GMLC, and in this case, the mobile operator sends the request to the H-GMLC where the user is being serviced. If the data are not in this GMLC, it will be forwarded to the R-GMLC. After the needed information are obtained from the GMLC, it will be sent to the user in the downlink stage.

In the downlink stage, the information uses the spare extension of the FACH, which is mapped and carried by the S-CCPCH, and modulated using QPSK.

A standard AAL2 backhaul between the UTRAN and the core network is also implemented to carry the information between them.

To summarise the system procedure, an example is provided here to see how the system works. If, for example, the user is in a location near University of Salford and is looking for a hotel called Lamb Hotel, the following steps would be followed:

1- The user asks for the location of "Lamb Hotel".
2- The mobile operator finds the user location.
3- The request is converted into a binary level.
4- The binary number fills the spare extension of the RACH.
5- The header CRC and payload CRC are calculated, and the CRC fields in the RACH frame are filled.
6- The channel is spread using the spreading factor and modulated using QPSK.
7- The backhaul carries the information from the UTRAN to the Core network.
8- The MSC receives the signal, demodulates, decodes it and gets the user request along with the user location.
9- The MSC checks if "Lamb Hotel" is in the GMLC database, and if not, it will send to another GMLC.
10- After the location of the hotel has been found, the MSC sends the information back to UTRAN via the backhaul.
11- The FACH spare extension is filled with the hotel coordination.
12- After the CRC is calculated, the channel is spread and modulated.
13- The S-CCPCH is used to carry the FACH.
14- The UE receives the signal and demodulates it, getting the coordinates of the hotel.

Chapter Six: Mathematical Model

In this chapter the calculation and the mathematical model of the transmission part of the system is shown in term of the time needed to transmit the data for different types of spreading factors. The model can be divided according to the link direction: uplink and downlink. The mathematical models presented in this chapter are only for the frame structure of the transport channels and the physical channels, that means the environmental effect and other parameter that could affect the signal is not presented in the mathematical model but these parameter taken in to the consideration in the simulation model.

6.1 Uplink

In the uplink the data are filled in RACH message part and mapped into PRACH. The PRACH message part frame (A) has 15 slots (a) [59], which can be presented as

$$A = \{ a1, a2, \ldots, ai \} \quad 6.1$$

The maximum value in PRACH for i=15, the data size of each slot can be calculated as

$$Size_a = 10 * 2^k, \ \forall a \in A, k \in \{0,1,2,3\} \quad 6.2$$

Where k is a variable, its value depends on the spreading factor sf. k can be found from the spreading factor equation as

$$sf = \frac{256}{2^k} \Rightarrow k = \frac{(\log \frac{256}{sf})}{\log 2} \quad 6.3$$

The slot size then can be formulated as

$$Size_a = 10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}} \quad 6.4$$

Because of the frame in PRACH is a group of slots, where it can be up to 15 slots per frame size, the frame size can be calculated as

$$Size_A = \sum_1^m Size_a \ , \ bits \ where \ m \leq 15 \quad 6.5$$

$$Size_A \sum_1^m 10 * 2^k \ , \ bits \ for \ k \epsilon \{0,1,2,3\}, m \leq 15 \quad 6.6$$

$$Size_A = \sum_1^m 10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}} \ , \ bits \ for \ sf \epsilon \{32,64,128,256\}, m \leq 15 \quad 6.7$$

Where:

m is the number of the slots used

$Size_A$ is the frame size

$Size_a$ is the slot size

According to 3GPP, the time needed to transmit one frame is 10 ms in the RACH, so the channel bit rate can be calculated as:

$$Ch_{bitrate} = \frac{Size_A}{Time} \quad 6.8$$

$$Ch_{bitrate} = \frac{\sum_1^m 10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}}{10} \ Kbps \quad 6.9$$

$for\ sf\ \epsilon \{32,64,128,256\}, m \leq 15$

6.1.1 3GPP Uplink Mathematical Model

The data that will be transmitted by PRACH is mapped from the RACH frame. To find the size of this data, the number of slots and frames needed to transmit the data must be found first. According to 3GPP the RACH frame is divided into header and payload [57]:

$$Data_{size} = Header + Payload \quad 6.10$$

While

$$Payload = ctrl + TB + CRCI_{size} + Spare_{Ext} \quad 6.11$$

$$Data_{size} = Header + ctrl + TB + CRCI_{size} + Spare_{Ext} \quad 6.12$$

Where:

ctrl is the control field in the frame = 6 bytes

Header which is normally 4 bytes

TB is the Transport block each TB is 8 bits

CRCI is Cyclic Redundancy Checksum Indicator

$Spare_{Ext}$ is the Spare extension which has 28 bytes in the RACH

The Spare extension data size is 28 Octets. In the 3GPP standard it is sent as zeros by the transmitter and neglected by the receiver. Also, the Spare extension is trivial generally, while in the proposed design the spare extension of the RACH is used to transmit the user request in the uplink. The calculation will be made first for the 3GPP standard and then for the proposed design. The CRCI size depends on the number of the TB as follow:

$$CRCI_{size} = \left\lceil \frac{TB}{8} \right\rceil \quad 6.13$$

Substituted the new value in the equation, the payload size will be

$$Payload_{size} = 8 * (6 + 28 + TB + CRCI_{size}) \quad , \text{bit} \tag{6.14}$$

$$Payload_{size} = 8 * \left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil \right) \quad , bit \tag{6.15}$$

As the requested data may occupy one or more frame, the number of frames needed to transmit the information without the header should be calculated first. The data payload will be divided by the size of the frame with no header and then the header is added which is normally 4 bytes, the formula for the number of frames before adding the header will be:

$$N_{Frame} = \left\lceil \frac{Payload_{size}}{Size_A - Header} \right\rceil \tag{6.16}$$

Substitute the frame size and the payload size into the equation:

$$N_{Frame} = \left\lceil \frac{8*(6+28+TB+CRCI_{size})}{\sum_1^m (10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}) - 4*8} \right\rceil \tag{6.17}$$

$$N_{Frame} = \left\lceil \frac{8\left(34+TB+\left\lceil \frac{TB}{8} \right\rceil\right)}{\sum_1^m (10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}) - 32} \right\rceil \tag{6.18}$$

The data size to be transmitted can be found as the header size for one or multiple frames plus the payload size

$$Header_{size} = 4 * 8 * N_{frame} \, , bits \tag{6.19}$$

$$Data_{size} = Header_{size} + Payload_{size} \tag{6.20}$$

$$Data_{size} = 32 * \left\lceil \frac{8\left(34+TB+\left\lceil \frac{TB}{8} \right\rceil\right)}{\sum_1^m (10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8 * \left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right) \tag{6.21}$$

The number of slots needed to transmit this information will be

$$N_{Slots} = \left\lceil \frac{Datasize}{Size_a} \right\rceil \tag{6.22}$$

$$N_{slots} = \left\lceil \frac{32 * \left\lceil \frac{8\left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{\sum_{1}^{m} (10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8 * \left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}} \right\rceil \quad 6.23$$

Number of frames needed to transmit the whole data after adding the header size for one or multiple frames with the payload data will be

$$N_{frame} = \left\lceil \frac{N_{slots}}{15} \right\rceil \quad 6.24$$

$$N_{frame} = \left\lceil \frac{32 * \left\lceil \frac{8\left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{\sum_{1}^{m} (10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8 * \left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{15 * 10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}} \right\rceil \quad 6.25$$

Because of the time needed to transmit a frame is 10ms [59] the time needed for one slot will be 10ms/15 which is 0.667 ms. The time needed to transmit the whole data will be:

$$time = 0.666 * \left\lceil \frac{32 * \left\lceil \frac{8\left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{\sum_{1}^{m} (10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8 * \left(34 + TB + \left\lceil \frac{TB}{8} \right\rceil\right)}{10 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}} \right\rceil \quad 6.26$$

6.1.2 Proposed Design Uplink Mathematical Model

For the proposed method, the spare extension carries information which are the user request, and the size of the user request can be between 1-28 bytes, and then a padding is added to the spare extension to make it 28 byte again as it is always sent in this size, the spare extension size can found as

$$SES = \left(\left\lceil \frac{URS}{28} \right\rceil * 28 - URS\right), \ byte \quad 6.27$$

Where:

URS is user request size

SES is the spare extension size

When using the spare extension as the field to carry the user request, the TB fields are no longer needed, and any field related to the TB will be omitted. The payload and the frame size can be found as follow:

$$Payload = (6 + \text{SES} + \text{URS}),\ \text{byte} \quad 6.28$$

$$Payload = \left(6 + \left\lceil \frac{URS}{28} \right\rceil * 28\right),\ \text{byte} \quad 6.29$$

To find the number of the required frames, the payload is divided by the frame size without the header

$$N_{Frame} = \left\lceil \frac{Payload}{Size_A - Header} \right\rceil \quad 6.30$$

$$Header_{size} = 4 * N_{frame}\ ,\ byte \quad 6.31$$

$$Header_{size} = 8 * 4 * \left\lceil \frac{8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{\sum_1^m (10* 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil \quad 6.32$$

Now adding the header with payload to find the whole data size

$$Data_{size} = Header_{size} + Payload_{size} \quad 6.33$$

$$Data_{size} = 32 * \left\lceil \frac{8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{\sum_1^m (10* 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8 * \left(6 + \left\lceil \frac{URS}{28} \right\rceil * 28\right) \quad 6.34$$

The number of Slots needed to transfer the data

$$N_{Slots} = \frac{Data_{size}}{Size_a} \quad 6.35$$

$$N_{Slots} = \left\lceil \frac{32* \left\lceil \frac{8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{\sum_1^m (10* 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 32} \right\rceil + 8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{10* 2^{\frac{(\log \frac{256}{sf})}{\log 2}}} \right\rceil \quad 6.36$$

The time needed to transmit the information for the new design will be

$$time = 0.666 * N_{slot} \quad 6.37$$

$$Time = 0666 * \left\lceil \frac{32 * \left\lceil \frac{8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{\sum_1^m (10*2^{\frac{(\log\frac{256}{sf})}{\log 2}})-32} \right\rceil + 8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}} \right\rceil \quad 6.38$$

And the number of frame after adding the header size for one or multiple frames along with the payload will be

$$N_{frame} = \left\lceil \frac{N_{slots}}{15} \right\rceil \quad 6.39$$

$$N_{frame} = \left\lceil \frac{32 * \left\lceil \frac{8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{\sum_1^m (10*2^{\frac{(\log\frac{256}{sf})}{\log 2}})-32} \right\rceil + 8*\left(6+\left\lceil \frac{URS}{28} \right\rceil *28\right)}{10*2^{\frac{(\log\frac{256}{sf})}{\log 2}}} \right\rceil /15 \quad 6.40$$

6.2 Downlink

For the downlink the data are filled in the FACH and carried by the S-CCPCH, the S-CCPCH frame (A) has 15 slots (a), which can be presented as

$$A = \{ a1, a2, \ldots, ai \} \quad 6.41$$

For maximum value of i=15 in S-CCPCH, A is the frame that has a maximum of 15 slots, the data size of each slot can be calculated as

$$Size_a = 20 * 2^k - (N_{TFCI} + N_{Pilot}) \quad 6.42$$

$$Size_a = 20 * 2^k - 8 \quad 6.43$$

$N_{TFCI} + N_{Pilot} = 8$ as it is the most common configuration [59]. k value between 0, and 6 , for different spreading factor (SF) which can be one of the following in S-CCPCH (4, 8, 16, 32, 64, 128, and 265) . k can be calculated from the spreading factor equation as

$$sf = \frac{256}{2^k} \Rightarrow k = \frac{(\log\frac{256}{sf})}{\log 2} \quad 6.44$$

From the above equation the frame size can be found as

$$Size_A = \sum_1^m Size_a \ , \ bits, m \leq 15 \quad 6.45$$

$$Size_A = \sum_1^m (20 * 2^k) - 8 \ bits, for \ K\epsilon \{0,1,2,3,4,5,6\}, m \leq 15 \quad 6.46$$

$$Size_A = \sum_{i=1}^m (20 * 2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 8 \ bits, \quad 6.47$$

$for \ SF \ \epsilon \{4,8,16,32,64,128,256\}, m \leq 15$

The time needed to complete the whole transmission for one frame is 10 ms, to find the channel bit rate:

$$Ch_{bitRate} = \frac{Size_A}{Time} \quad 6.48$$

$$Ch_{bitRate} = \frac{\sum_1^m (20*2^{\frac{(\log \frac{256}{sf})}{\log 2}}) - 8}{10} \ Kbps \quad 6.49$$

$$for \ SF \ \epsilon \{4,8,16,32,64,128,256\}, m \leq 15$$

6.2.1 3GPP Downlink Mathematical Model

The data that is transmitted by S-CCPCH is mapped from the FACH. To find the size of this data, first, the number of slots and frames needed to transmit the data must be found. According to 3GPP the RACH frame is divided into header and payload [57]:

$$Frame_{FACH} = Header + Paylaod \quad 6.50$$

$$Frame_{FACH} = Header + ctrl + TB + SpareExtension \quad 6.51$$

Where

ctrl is the control field in the frame 5 bytes.

Header is 4 bytes.

TB is the Transport block, each TB is 8 bits (1 byte).

The *Spare extension* is 28 bytes long in the FACH.

The Spare extension will be sent by the transmitter as zeros and neglected by the receiver. In the standard the spare extension is not necessary and usually ignored while in the new design the spare extension is used to transmit the location information in FACH in the downlink and to be carried by the S-CCPCH

$$Payload_{FACH} = 8 * (5 + 28 + TB), \text{bit} \quad 6.52$$

$$Payload_{FACH} = 8 * (33 + TB), bit \quad 6.53$$

$$Header = 4 * 8 \ bit \quad 6.54$$

Number of S-CCPCH frames needed to transmit this information can be calculated by dividing the payload size over the frame size with no header as follow

$$N_{Frame} = \left\lceil \frac{Payload_{FACH}}{Size_A - Header} \right\rceil \quad 6.55$$

$$N_{Frame} = \left\lceil \frac{8*(5+28+TB)}{(\sum_1^m (20* 2^{\frac{(\log \frac{256}{sf})}{\log 2}} - 8)) - 4*8} \right\rceil \quad 6.56$$

$$N_{Frame} = \left\lceil \frac{8(33+TB)}{(\sum_1^m (20* 2^{\frac{(\log \frac{256}{sf})}{\log 2}} - 8)) - 32} \right\rceil \quad 6.57$$

The whole data size to be transmitted over the S-CCPCH is the header for one or multiple frames plus the payload

$$Header_{FACH} = 4 * 8 * N_{frame}, \ bits \quad 6.58$$

$$Data_{size} = Header_{FACH} + Payload_{FACH} \quad 6.59$$

$$Data_{size} = 32 * \left\lceil \frac{8(33+TB)}{(\sum_1^m (20* 2^{\frac{(\log \frac{256}{sf})}{\log 2}} - 8)) - 32} \right\rceil + 8 * (33 + TB) \quad 6.60$$

Number of slots needed to transmit this information are

$$N_{Slots} = \left\lceil \frac{Data_{size}}{Size_a} \right\rceil \quad 6.61$$

$$N_{slots} = \left\lceil \frac{32* \left\lceil \frac{8(33+TB)}{(\sum_1^m (20* 2^{\frac{(\log \frac{256}{sf})}{\log 2}} - 8)) - 32} \right\rceil + 8*(33+TB)}{20* 2^{\frac{(\log \frac{256}{sf})}{\log 2}} - 8} \right\rceil \quad 6.62$$

Time needed to transmit these slots is the number of the slots multiplied by the 10/15 ms which is the time for frame over the number of slot.

$$Time = 0.666 * \left\lceil \frac{32 * \left\lceil \frac{8(33+TB)}{\frac{(\log\frac{256}{sf})}{\log 2} - 8)) - 32} \right\rceil + 8*(33+TB)}{20 * 2^{\frac{(\log\frac{256}{sf})}{\log 2}} - 8} \right\rceil \quad 6.63$$

Number of frame after adding the header for multiple frames can be formulated as

$$N_{frame} = \left\lceil \frac{N_{slots}}{15} \right\rceil \quad 6.64$$

$$N_{frame} = \left\lceil \frac{32 * \left\lceil \frac{8(33+TB)}{\frac{(\log\frac{256}{sf})}{\log 2} - 8)) - 32} \right\rceil + 8*(33+TB)}{15*(20 * 2^{\frac{(\log\frac{256}{sf})}{\log 2}} - 8)} \right\rceil \quad 6.65$$

6.2.2 Proposed Design Downlink Mathematical Model

For the new transmission method in the proposed design, the spare extension carries the location information. the spare extension size SES is 28 bytes all and can be as

$$SES = \left(\left\lceil \frac{URS}{28} \right\rceil * 28 - URS \right), \ byte \quad 6.66$$

Where *URS* is the size of the user information which can be any data but usually it will be a coordinate of a location, The payload for the FACH is after omitting the TB as the spare extension will carry the information instead of the TB fields

$$Payload = (5 + \text{SES} + \text{URS}), \text{ byte} \quad 6.67$$

$$Payload = \left(5 + \left\lceil \frac{URS}{28} \right\rceil * 28 \right), \text{ byte} \quad 6.68$$

The number of the frame needed without the header will be

$$N_{Frame} = \left\lceil \frac{Payload}{Size_A - 32} \right\rceil \quad 6.69$$

$$Header_{size} = 4 * N_{frame}, byte \quad 6.70$$

$$Header_{size} = 8 * 4 * \left\lceil \frac{8*\left(5 + \left\lceil \frac{URS}{28} \right\rceil * 28 \right)}{\frac{(\log\frac{256}{sf})}{\log 2} - 8)) - 32} \right\rceil \quad 6.71$$

$$Data_{size} = Header_{size} + \quad Payload \tag{6.72}$$

$$Data_{size} = 32 * \left\lceil \frac{8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{(\sum_1^m(20*2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8))-32} \right\rceil + 8 * \left(5 + \left\lceil\frac{URS}{28}\right\rceil * 28\right) \tag{6.73}$$

The Slots needed to transfer this data can be calculated as

$$N_{Slots} = \left\lceil \frac{Data_{size}}{Size_a} \right\rceil \tag{6.74}$$

$$N_{Slots} = \left\lceil \frac{32*\left\lceil \frac{8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{(\sum_1^m(20*2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8))-32} \right\rceil + 8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{20*\ 2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8} \right\rceil \tag{6.75}$$

Time needed to transmit these slots is the number of slots multiplied by 0.666 ms

$$Time = \ 0.666 * \left\lceil \frac{32*\left\lceil \frac{8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{(\sum_1^m(20*2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8))-32} \right\rceil + 8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{20*\ 2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8} \right\rceil \tag{6.76}$$

Number of frame after adding the header size for multiple frames will be

$$N_{frame2} = \left\lceil \frac{N_{slots}}{15} \right\rceil \tag{6.77}$$

$$N_{frame2} = \left\lceil \left\lceil \frac{32*\left\lceil \frac{8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{(\sum_1^m(20*2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8))-32} \right\rceil + 8*\left(5+\left\lceil\frac{URS}{28}\right\rceil*28\right)}{20*\ 2^{\frac{(\log\frac{256}{sf})}{\log 2}}-8} \right\rceil / 15 \right\rceil \tag{6.78}$$

6.3 Summary

In this chapter the mathematical models of both 3GPP standard and proposed design have been introduced. The mathematical models for those systems are presented in two parts uplink and downlink. The comparison of results between those systems is included in the next chapter.

Chapter Seven: Results and Comparison

This chapter provides all the results of the thesis study, including results from the channel mathematical model and its comparison with the 3GPP standard mathematical model. Also, the simulation results are compared with the mathematical model for validation. Finally, the comparison between the results from the proposed system with 3GPP system to evaluate the proposed design results. Also, the results from the core network are shown in this chapter, which cover comparisons of the response time and the privacy for different architectures: one GMLS, multiple GMLCs and standard architecture.

7.1 Proposed Design and 3GPP Standard Mathematical Model Results

This section shows the comparison between the results obtained from the mathematical model of the 3GGP standard design and the results from the mathematical model of the proposed design. This section is divided into two subsections: uplink, which shows the mathematical results for the uplink and its comparison with the 3GPP standards, and the downlink; where the result from the downlink mathematical presentation and the comparison with the standard are shown.

7.1.1 Uplink

In this section, the comparison between the results obtained from the uplink equations are shown; the mathematical model has been presented and derived in the previous chapter with two different types of design: the standard design that presented by 3GPP and the proposed system design.

In the uplink, the spreading factor can take different values varying from 32 to 256, namely (32, 64, 128, and 256). The results for the different spreading factors have similar behaviour, and for that reason, only two different sets of results are shown for two different types of spreading factors. Other results and comparisons for the other spreading factors can be seen in appendix A.

The comparison between the mathematical uplink model of the 3GPP standard and the proposed system for the spreading factor = 64 is shown in Figure 7-1

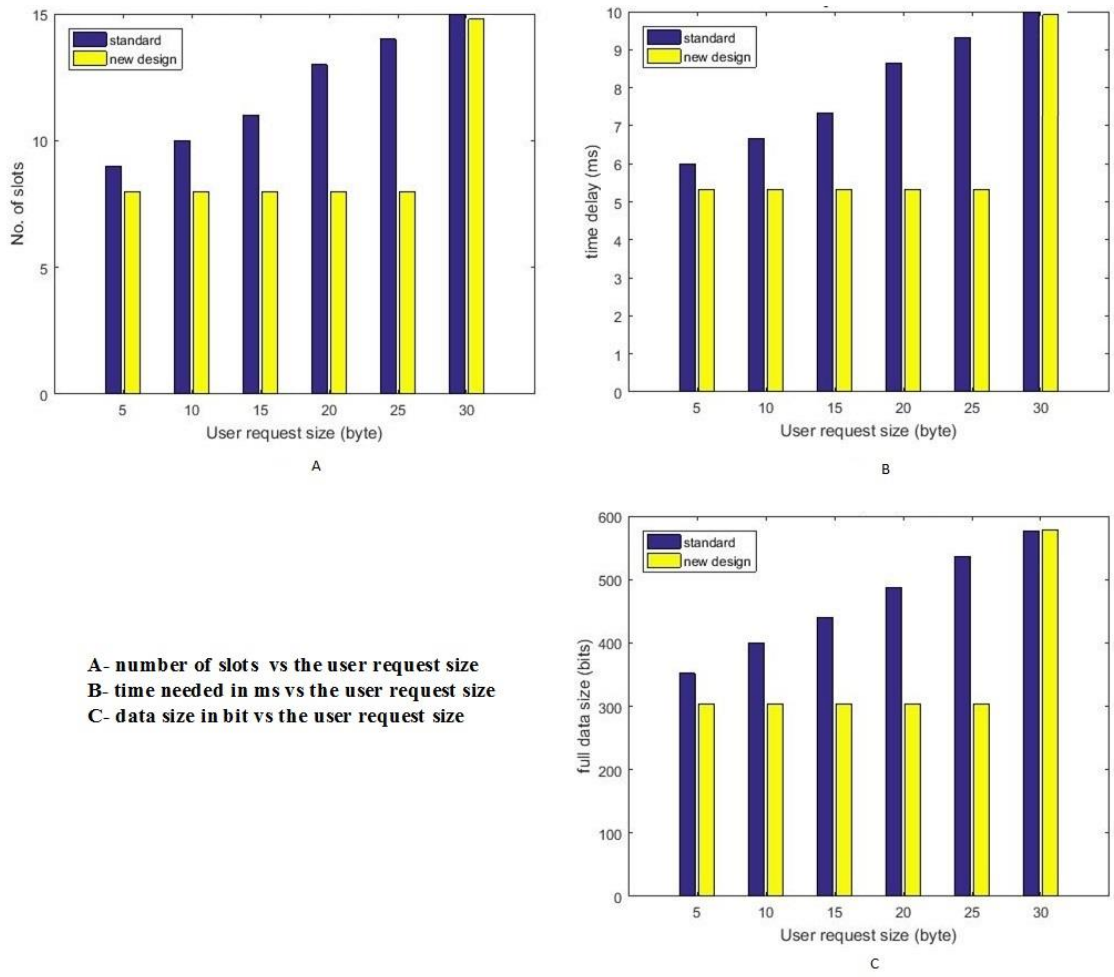


Figure 7-1 Mathematical Uplink Result for SF=64

As can be seen in the mathematical result (c), the standard design has a data size value, which increased gradually when increasing the user request size, while the proposed system has a value that is fixed until the user request size reached 28 bytes; this is because the spare extension of the RACH can take up to 28 bytes. In the same figure (A), the slots needed in PRACH, to carry this data are shown and it is evident that the slots number needed is increasing with the user request size in the 3GPP standard, while in the proposed system this number is fixed until it reaches the threshold of 28 bytes, which is the same case in (B) for the time needed to transmit these slots, that because the data are transmitted using the TB field in the 3GPP standard and every TB can take only one byte while the spare extension is used to transmit the data which can take 28 bytes. Figure 7-2 shows the same result of the uplink with spreading factor = 128.

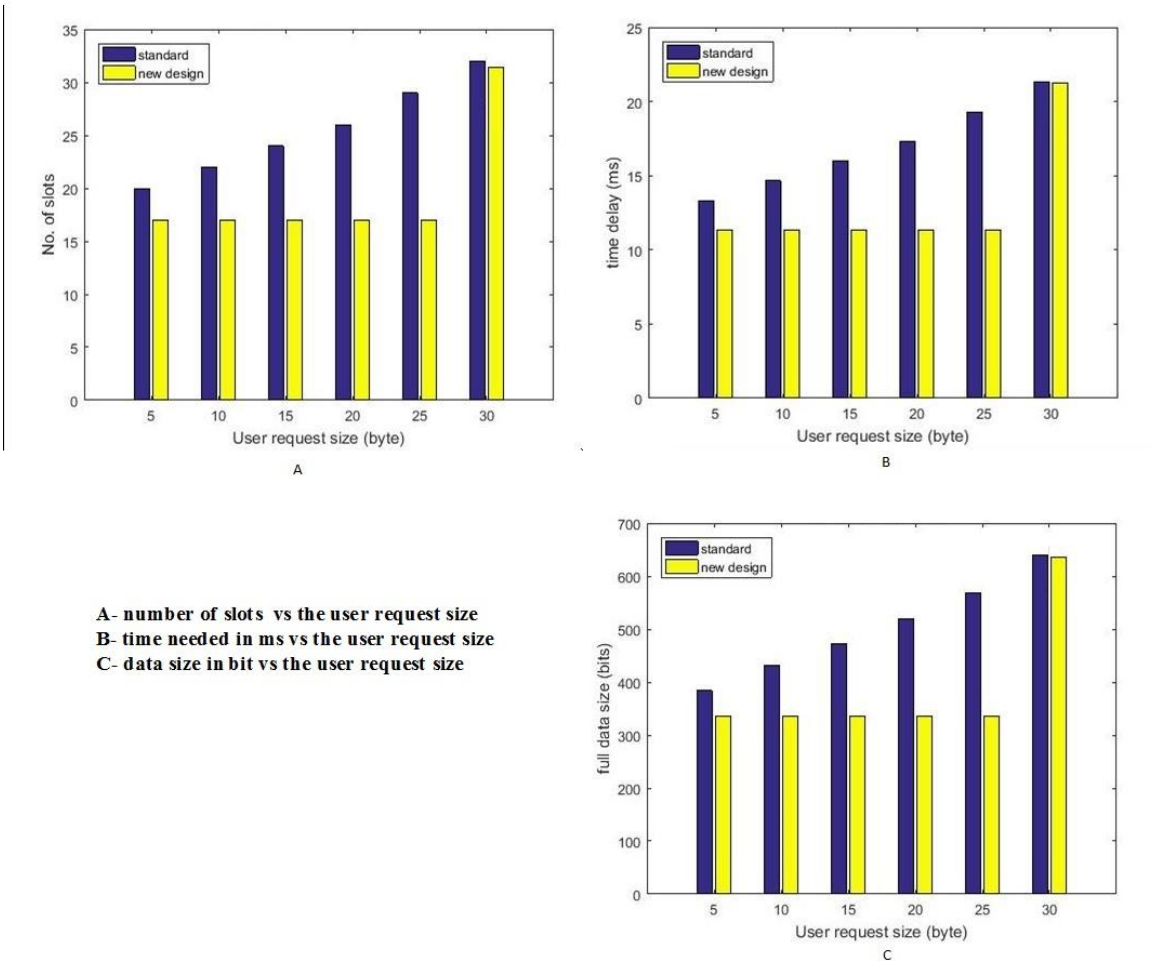


Figure 7-2 Mathematical Uplink Result for SF=128

As can be seen, the behaviour of the mathematical model is similar to that shown in the result for the spreading factor = 64 but with different numbers of slots, time and data size.

7.1.2 Downlink

The downlink mathematical results comparing between the 3GPP standard model and the system design is illustrated in this section. The mathematical equations for both the 3GPP standard and the proposed method are presented and derived in Chapter Six.

As in the uplink, the downlink has many options for the spreading factors, 4, 8, 16, 32, 64,128 and 256. In this chapter only the results from two spreading factors are shown, namely 64 and 128. Any other spreading factors' results are included in Appendix A.

The difference between the mathematical model presentation of the 3GPP standard design and the proposed design for the spreading factor = 64 can be seen in Figure 7-3.

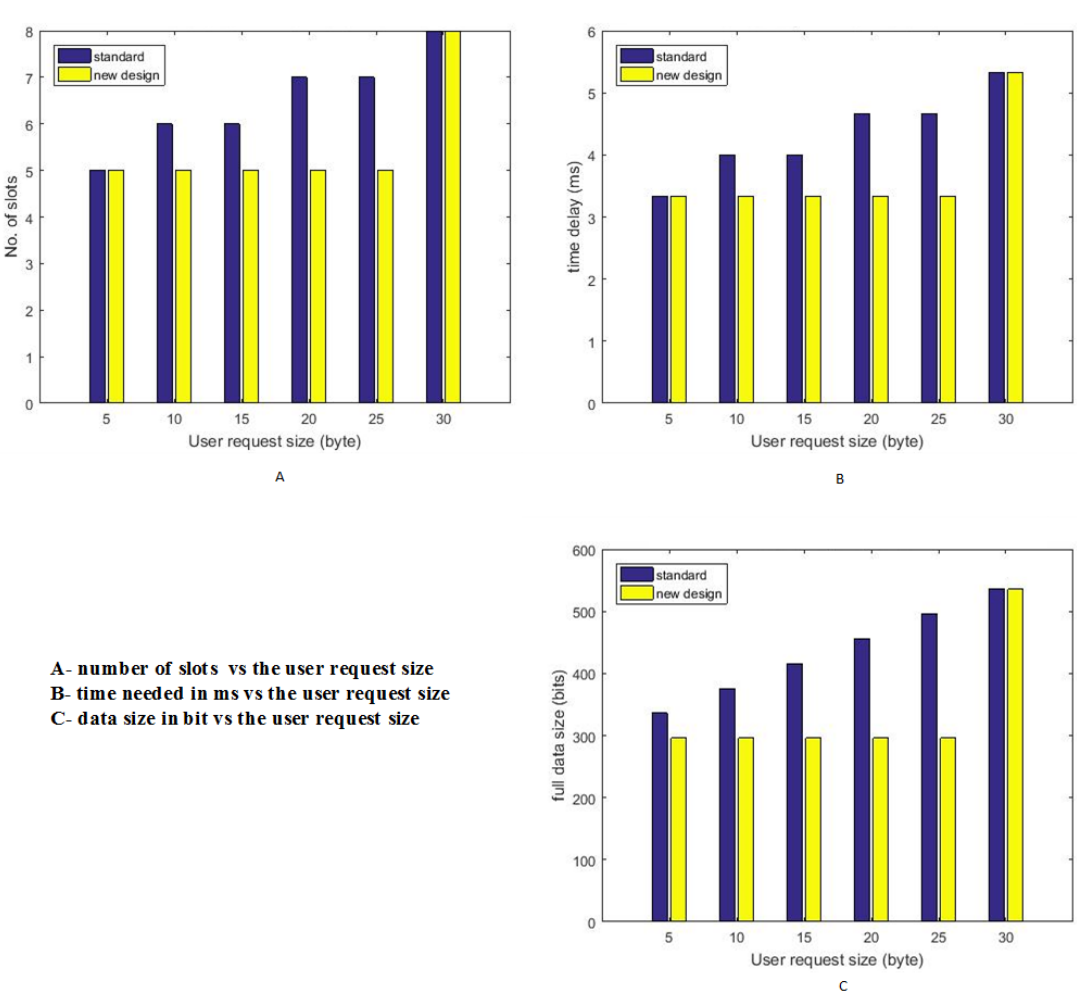


Figure 7-3 Mathematical Downlink Results for SF=64

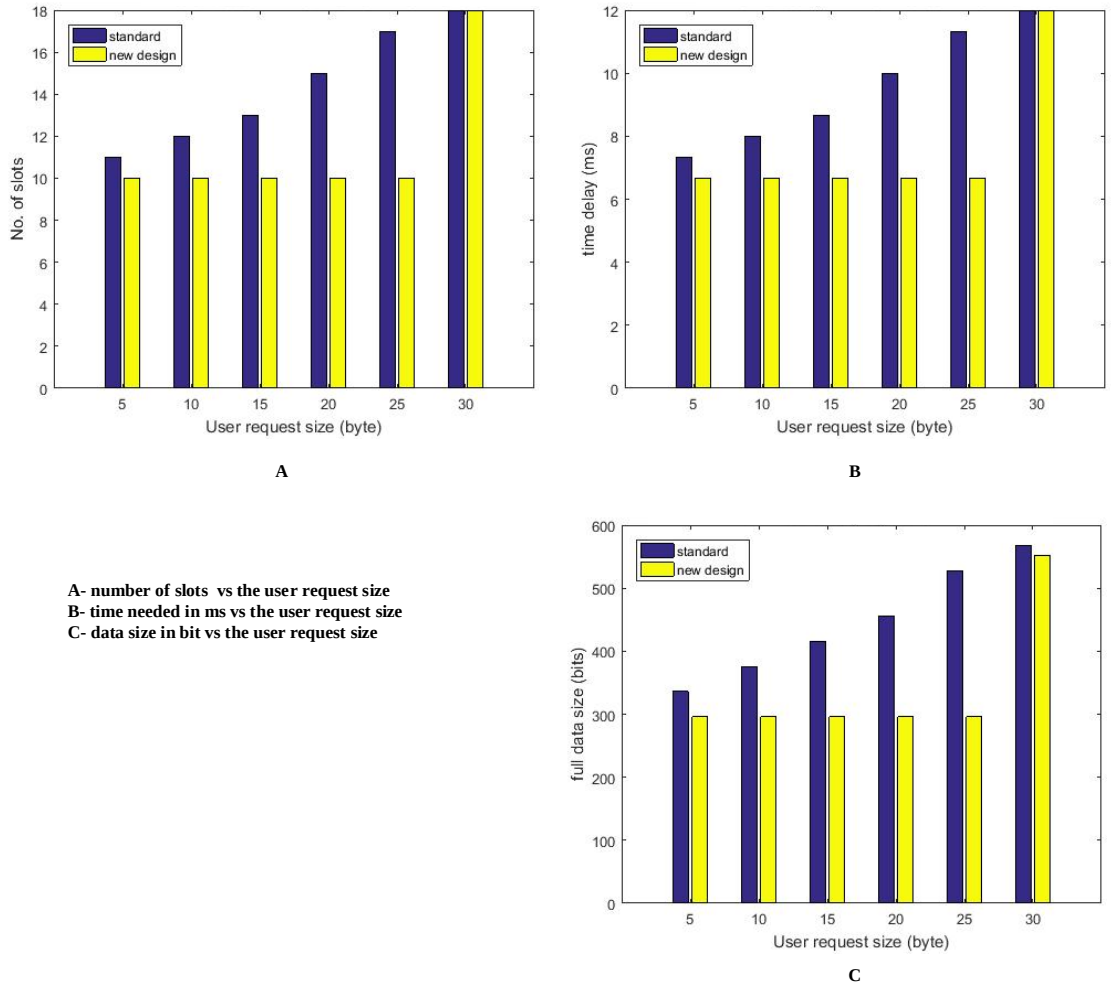
The figure shows the differences between the standard and the new design in regards to number of slots needed for the S-CCPCH to send the data (A), the time needed to send these slots (B) and the size of the data in the FACH that those slots carry (C).

The results show that the new design has less data size than the 3GPP standard to carry the user request, and needs less number of slots to send the information, which leads to less time needed transmit the data; that because the data are transmitted using the TB field in the 3GPP standard and every TB can take one byte while the spare extension is used to transmit the data which can take 28 bytes.

The behaviour of the different spreading factor is similar with some differences in the values, Figure 7-4 shows the mathematical model results for the spreading factor =128.

The spare extension of the FACH can carry up to 28 bytes, so for that reason the data can be carried in the same frame and with the same number of slots in the new design. The user

request is sent via the spare extension, while in the 3GPP standard and other systems the user request is sent via the TB fields.



A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

Figure 7-4 Mathematical Model Downlink Results for SF=128

7.2 Proposed Design Validation: Mathematical Model vs Simulation Results

The simulation results are shown in this section to highlight the differences and compare between the simulation results and the mathematical model in order to validate the results. The results are presents as uplink results and downlink results. The different between the simulation results and the mathematical results is because of the other parameters that could affect the signal, like the scrambling code, channelizing code and noise in the air. These stages could cause some differences in the results.

7.2.1 Uplink Validation

The simulation results obtained from the uplink channel using the RACH are compared with the mathematical model of the proposed design. As mentioned earlier in this chapter, the

uplink can use different spreading factors, which are 32, 64, 128 and 256. All the validation results for the different spreading factors can be seen in Appendix B. Figure 7-5 shows the comparison between the mathematical results and the simulation results for spreading factor 64.

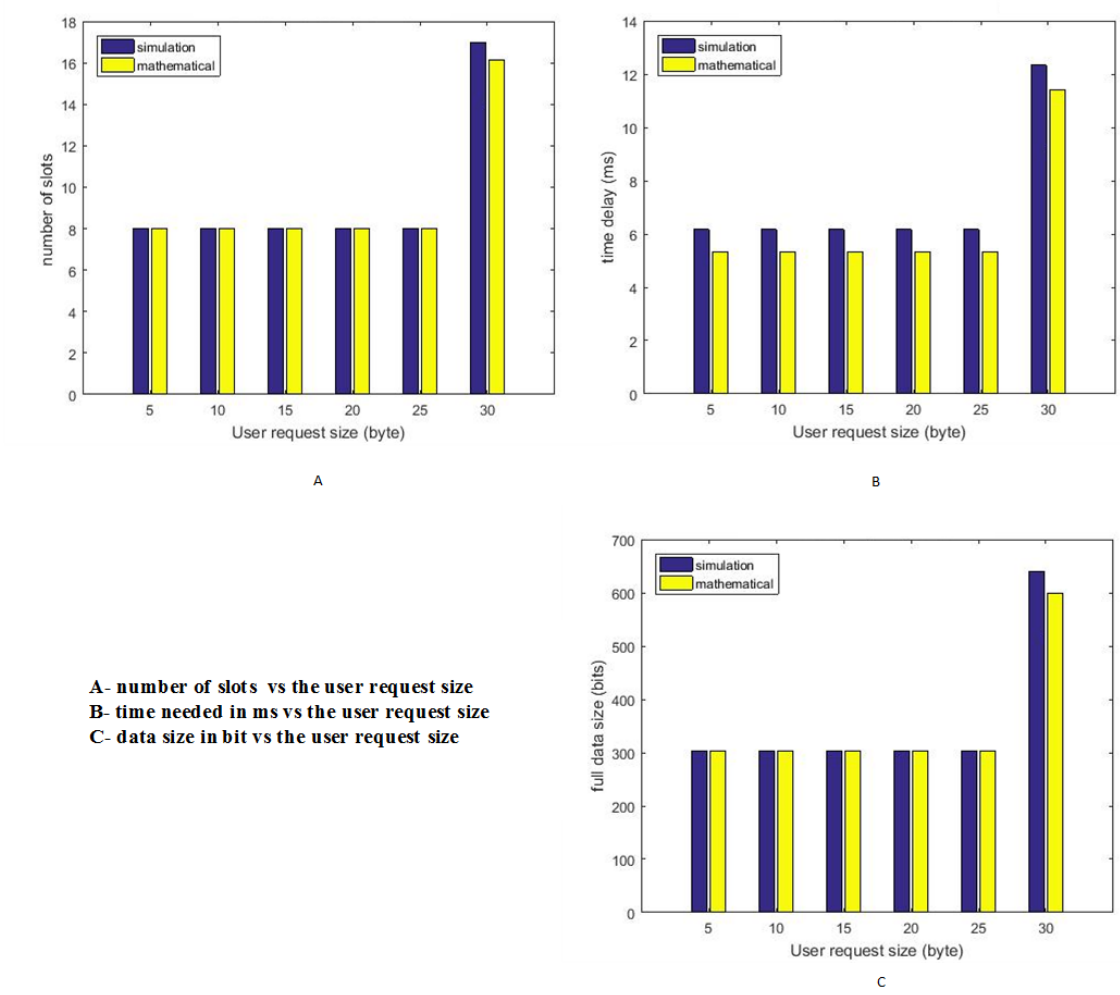


Figure 7-5 Comparison Between The Mathematical and Simulation Result for Uplink with SF= 64

The figure compares between the mathematical model results and the simulation results for the uplink channel in regards to number of slots needed for PRACH to send the data (A), the time needed to send these slots (B) and the size of the data in the RACH that those slots carry (C).

There are slight differences in the time needed to send the information (B), while the other results show a match between the mathematical and simulation results. Moreover, there are other mismatches when the user request exceeds 28 bytes. That is because when the user

request is above 28 bytes, the system will need another set of spare extension fields, and will add it up.

Figure 7-6 shows the results for the spreading factor = 128, which, it can be seen, has a similar behaviour to that of sf=64.

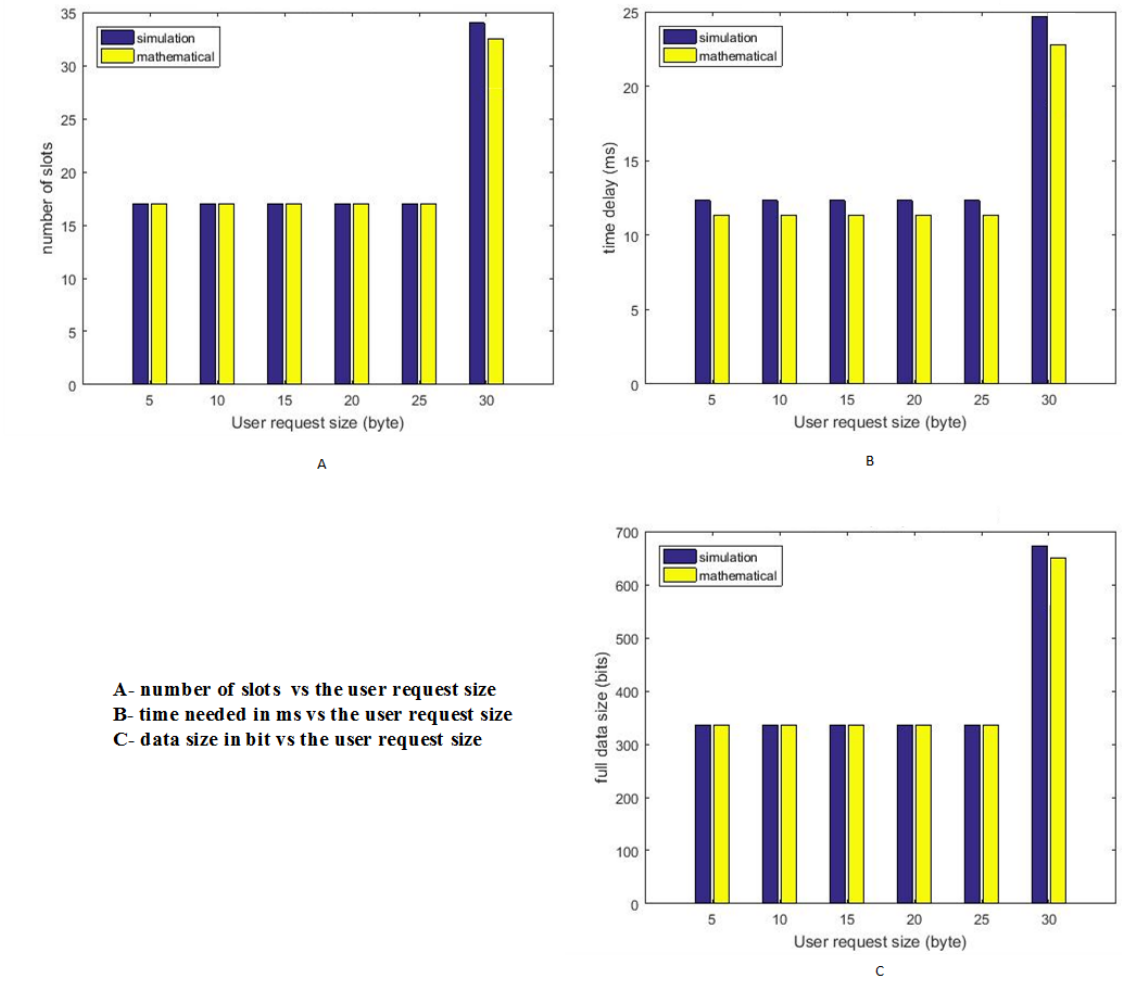


Figure 7-6 Comparison Between The Mathematical and Simulation Result for Uplink with SF= 128

7.2.2 Downlink Validation

A comparison between the simulation result for the downlink channel using the FACH and mathematical model are shown in this section to validate the downlink simulation results. The downlink channel can take different spreading factors, which are 4, 8, 16, 32, 64, 128 and 256. All these possible spreading factors are considered in the results to validate the downlink channel results and can be seen in Appendix B, as only two of them are shown and discussed in this section, which are the 32 and 64. Figure 7-7 shows the comparison between

the mathematical results and the simulation results for the downlink with a spreading factor = 32.

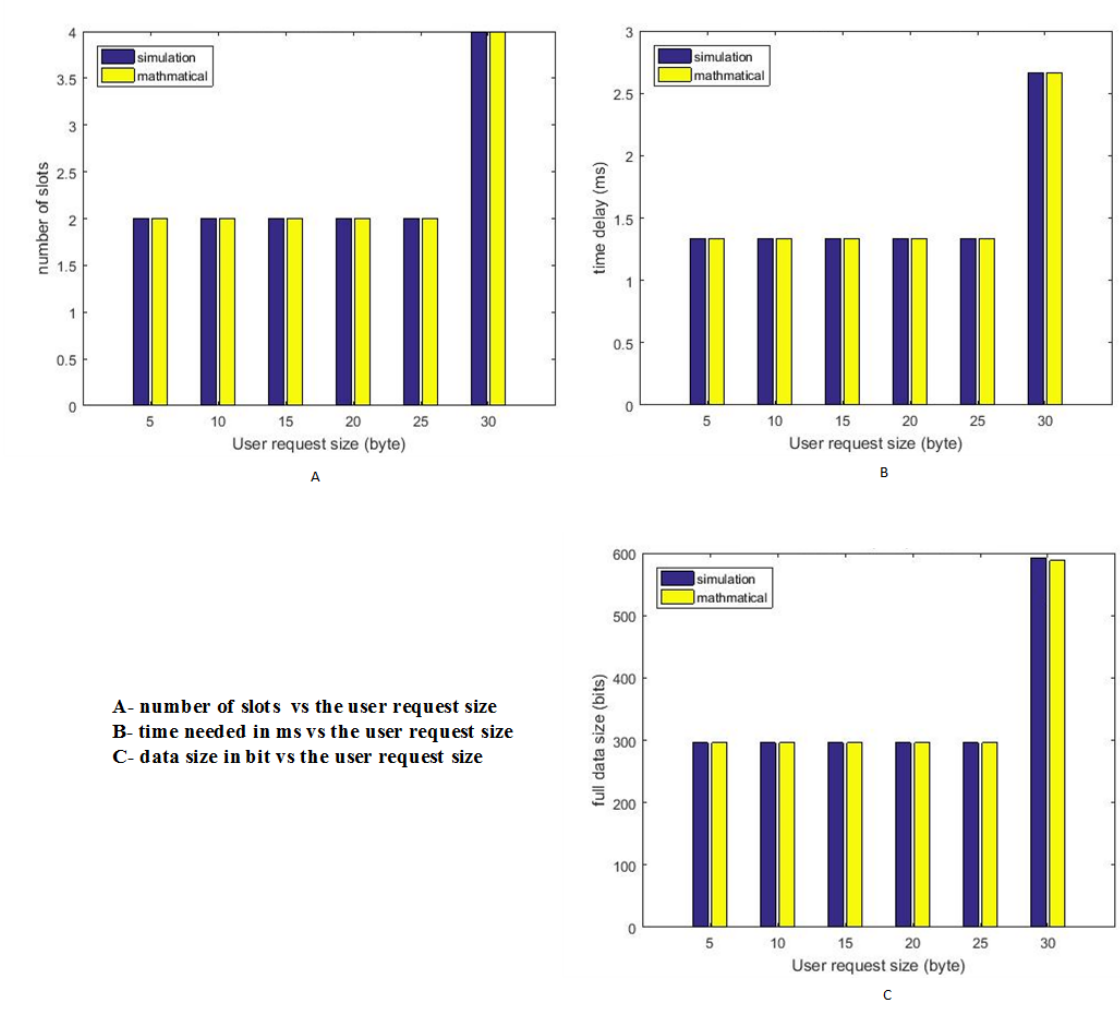


Figure 7-7 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF= 32

The figure compares between the mathematical model results and the simulation results for the downlink channel in respect to the number of slots needed for S-CCPCH to send the data (A), the time needed to send these slots (B) and the size of the data in the FACH that those slots carry (C).

The results are matched for all the results where the user request is under 28 bytes, and slightly different when the request is above 28 bytes. This difference can also be seen in the higher spreading factor like 64 and 128, as shown in Figure 7-8 where the shown spreading factor is 64.

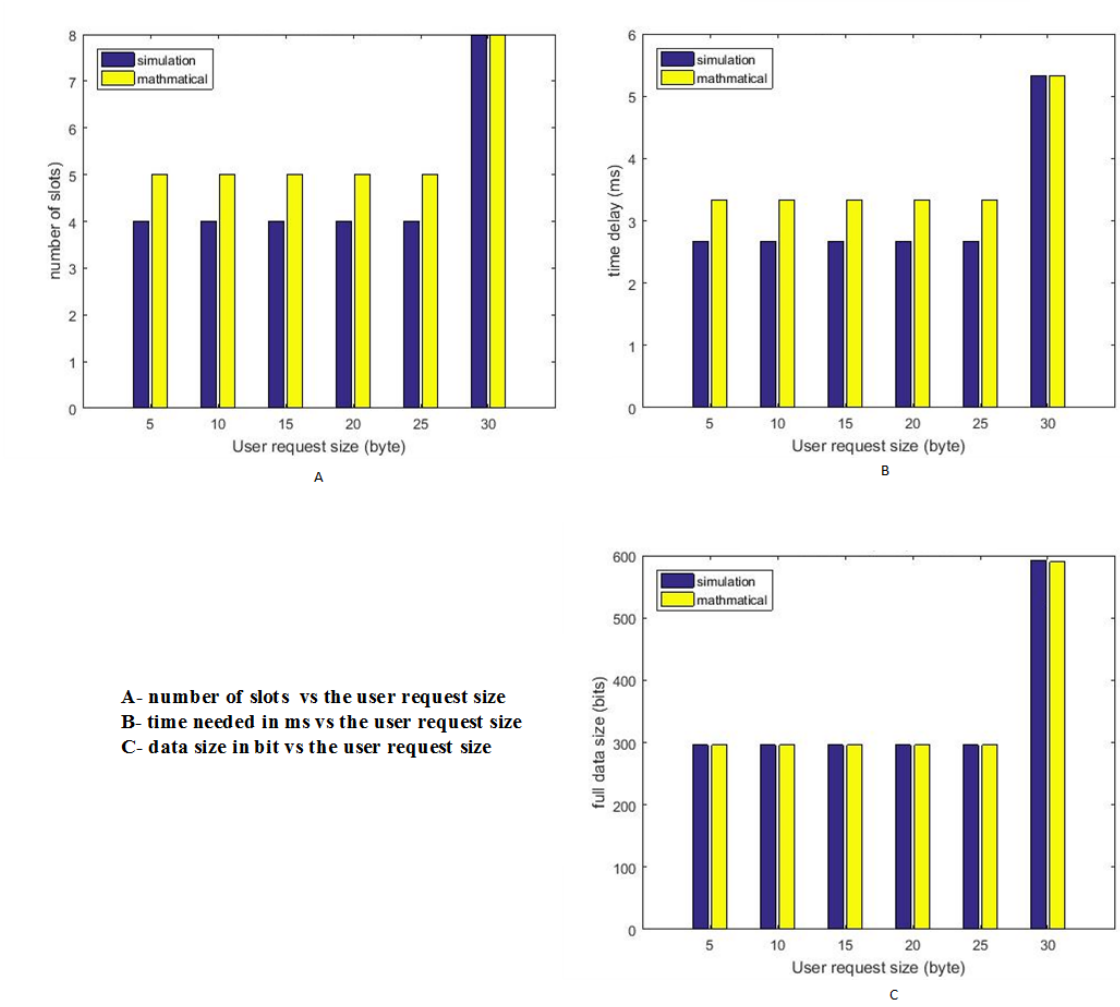


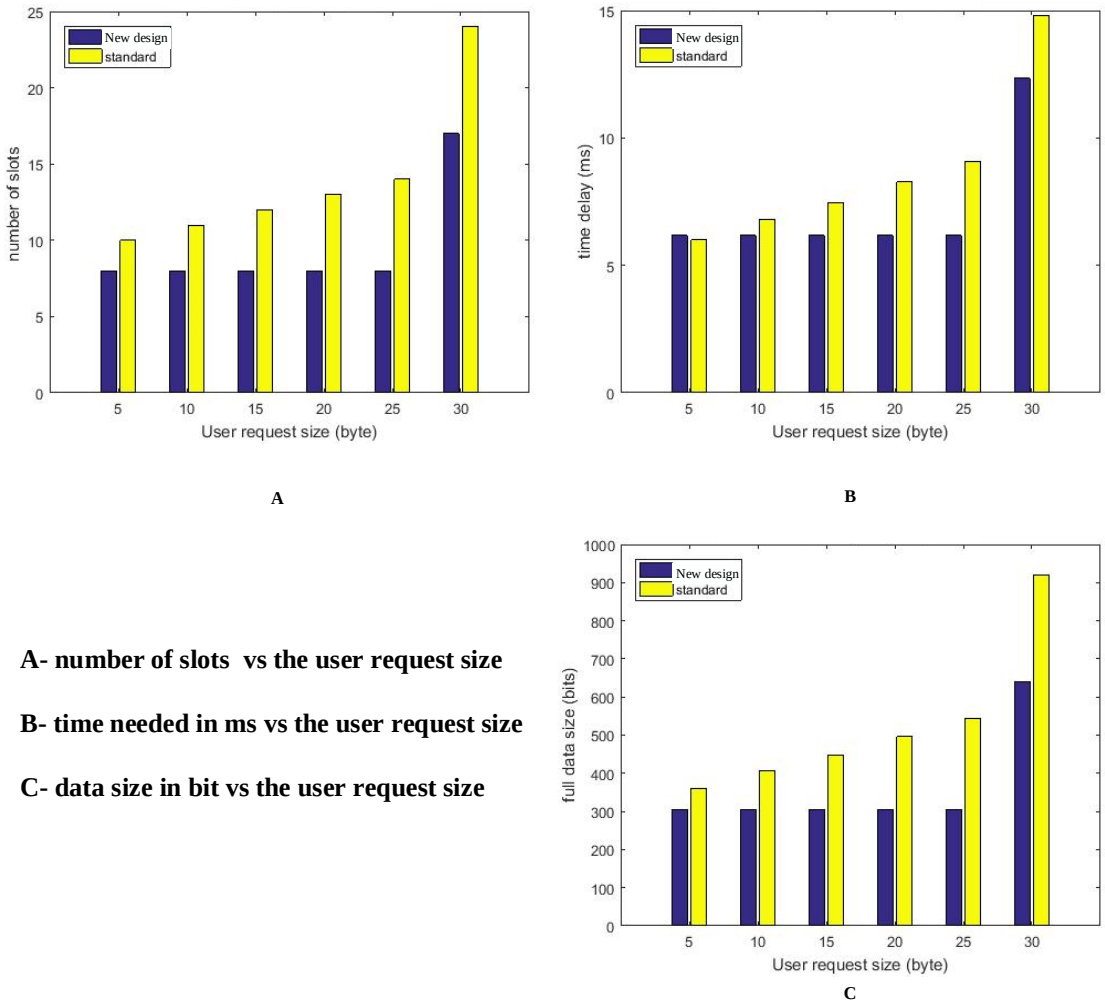
Figure 7-8 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF= 64

7.3 Proposed Design vs 3GPP Standard Simulation Results

After validating the simulation results by comparing them with the mathematical results, this section evaluates the achieved results against other systems. The 3GPP standard system design is used for the purpose of the evaluation as it is the nearest one to the proposed system design where the RACH can also be used to transmit a small amount of data. The results are presented in two parts; uplink and downlink. The simulator has been ran for five time and the average values has been shown in the results graphs. The reason why the simulation ran more than once is to add more accuracy to the results even though the result was very close and in many case are similar

7.3.1 Uplink Evaluation

The proposed system design utilises the spare extension in the uplink RACH to send the user request. The 3GPP standard does not use the spare extension for transmitting data, but uses another field in the frame structure to send the user information which is TB field. The results for two spreading factors are presented in this section, which are SF 64 and 128. Other spreading factor results can be found in Appendix C. Figure 7-9 illustrates a comparison between the proposed design and the 3GPP standard using spreading factor = 64; the figure shows the number of slots needed for PRACH to send the data (A), the time needed to send these slots (B) and the size of the data in the RACH that those slots carry (C).



A- number of slots vs the user request size

B- time needed in ms vs the user request size

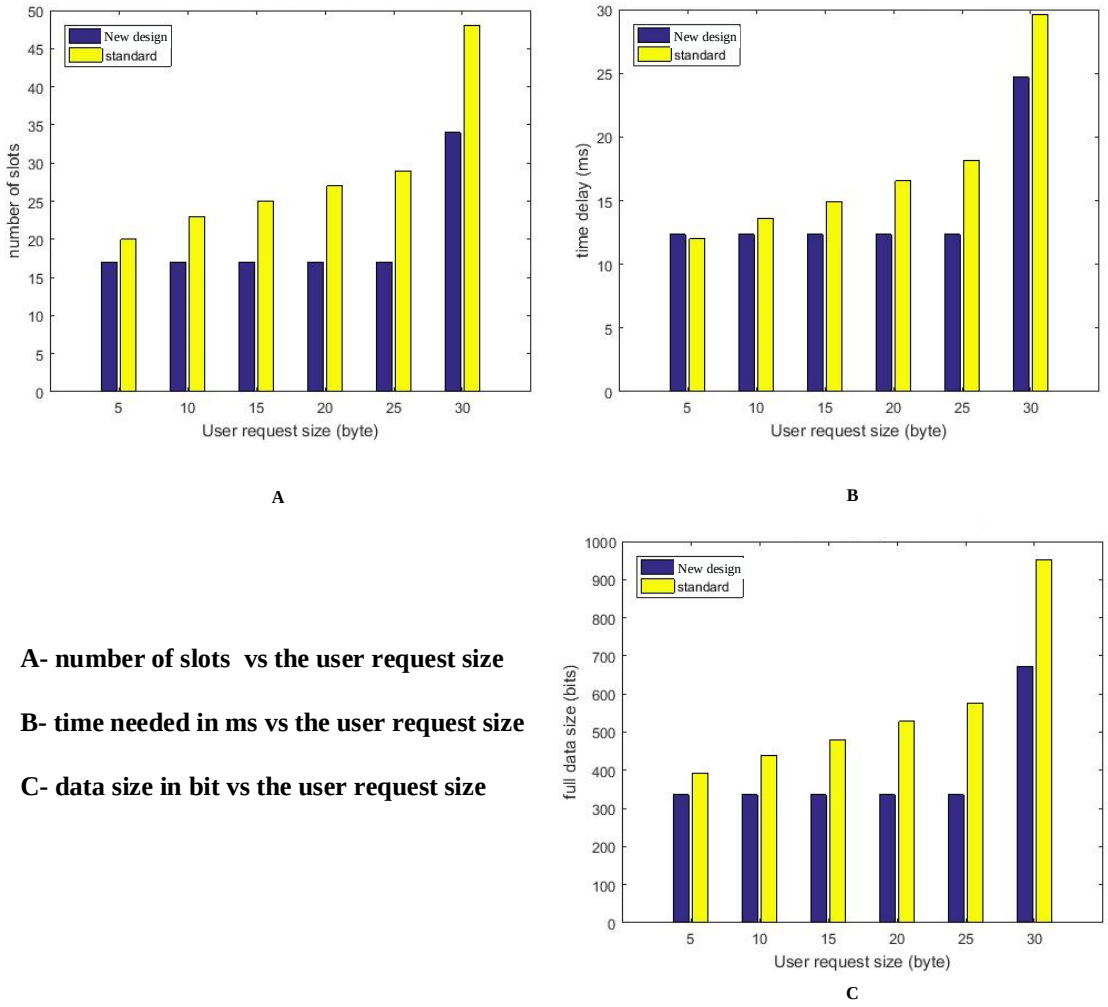
C- data size in bit vs the user request size

Figure 7-9 Comparison Between The Results of the 3GPP and The New Design for The Uplink SF= 64

It is obvious that the new design performs better than that in other systems, as the data size needed to send the user request is increasing continuously when using 3GPP standard (C),

while it keeps its size fixed until it reaches 28 bytes when using the proposed design. Consequently, the number of slots needed in PRACH to send this information are less in the proposed design (A), which leads to less time needed (B).

Figure 7-10 shows the results when using spreading factor 128 in the uplink. The results follow a similar trend to those of spreading factor 64.



A- number of slots vs the user request size

B- time needed in ms vs the user request size

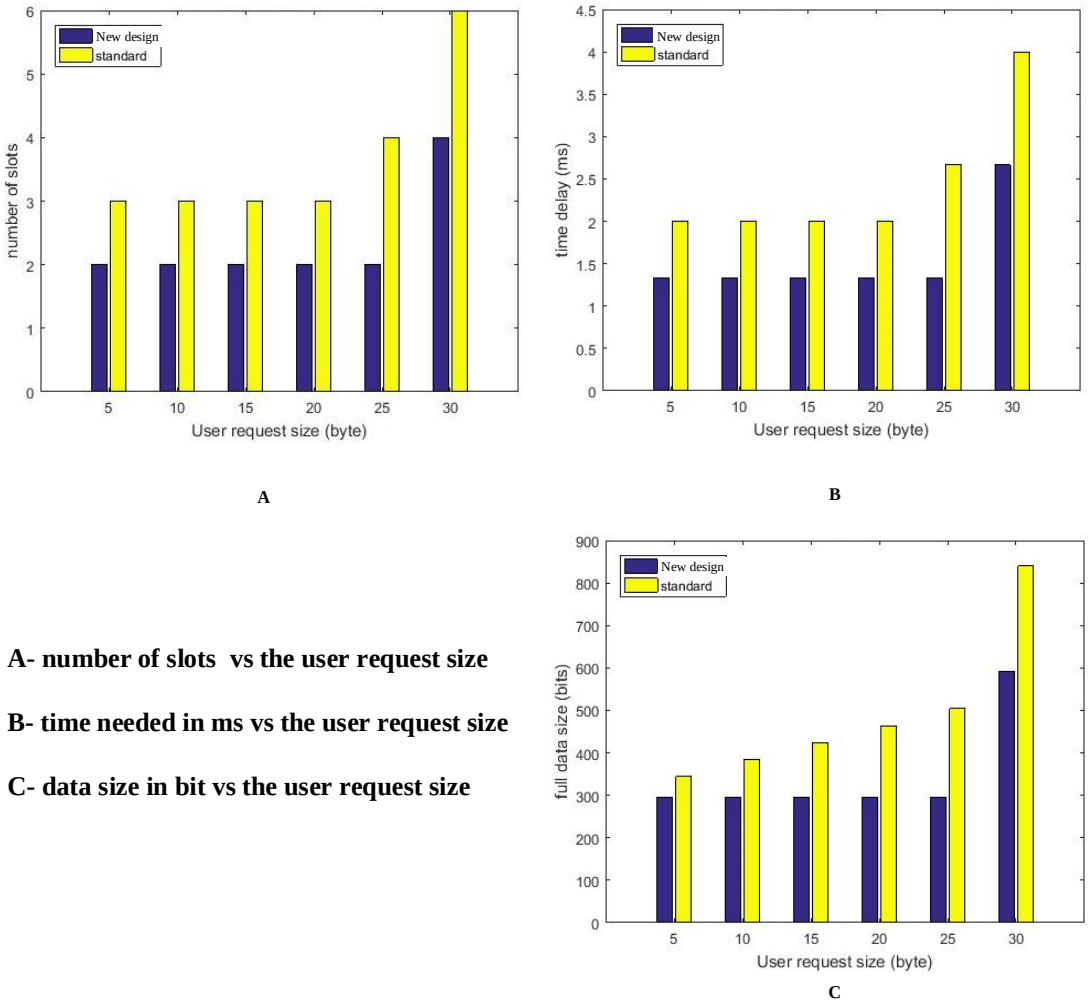
C- data size in bit vs the user request size

Figure 7-10 Comparison Between the Results of The 3GPP and The New Design for the Uplink SF= 128

7.3.2 Downlink Evaluation

A comparison between the simulation result obtained from the proposed system downlink channel using the FACH and the simulation result of the 3GPP standard to evaluate proposed system is shown in this section. The downlink channel can employ different spreading factors, all the possibilities are considered in the results and can be seen in Appendix C. Only two spreading factors are shown in this section, which are 32 and 64. Figure 7-11 illustrates

a comparison between the system design and the standard for the downlink with spreading factor = 32; the number of slots needed for S-CCPCH to send the data (A), the time needed to send these slots (B) and the size of the data in the FACH that those slots carry (C).



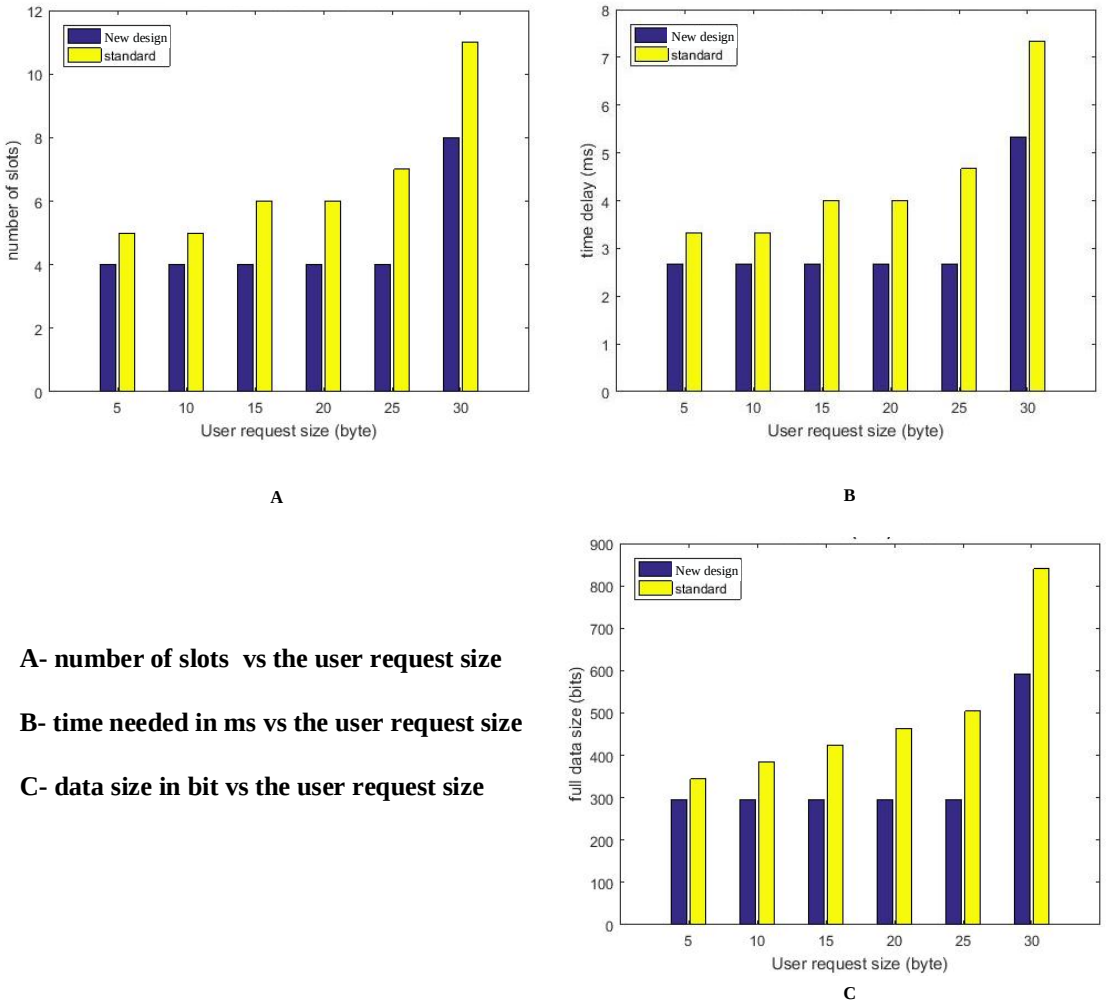
A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure 7-11 Comparison Between The Results of The 3GPP and The New Design for The Downlink SF= 32

The performance of the new design is better than that of the 3GPP standard requiring less time (B) when sending the same size of user request. The new design needs a lesser size of information to send the request (C), because the number of slots needed to send this information in S-CCPCH is less than those needed in the 3GPP standard (A). Figure 7-12 shows similar trend for spreading factor 64



A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure 7-12 Comparison Between The Results of The 3GPP and The New Design for The Downlink SF= 64

7.4 Critical Evaluation

To evaluate the proposed method we compared it with other methods that use the RACH and/or FACH to communicate between the user and the service and the data provider. However, many studies use other methods for the communication, like using the Internet or the voice channel. In this section a comparison among the proposed method and other methods is presented.

Methods that use data over voice are using a modem to transfer these data, and would need an extended extra hardware for the two sides of the network (transmitter and the receiver).

On the other hand, methods that use the WSN and/or the V2V would need a series of connections from the first user (node) who requested the service, to be carried by other users

(nodes) till it received by the data and service provider (sink). If there is any problem in this connection between the user and the final destination, the data will not be delivered.

Methods that use the Internet using the Wi-Fi would need a hotspot, and in case of emergency or if the user is a way from the hotspot coverage, the connection will be terminated and the user cannot send or receive from the data provider.

Moreover, methods that used the Internet via the packet channel of the mobile network (like GPRS or HSPA) will need the Internet channel to be active and available all the time, moreover if the user is out of allowance, he/she cannot connect to the service provider.

In the proposed method, users can communicate with the data and service provider everywhere as long as there is a mobile network coverage, even if the user has no direct Internet connection (Wi-Fi or packet channel).

When the user requests to access the network, control signals are exchanged between the user and the mobile network to establish a connection. In the proposed method the service's request is sent in the spare extension of these control signal. While in other methods and in the 3GPP standard another set of signals are exchanged between the user and the core network to transmit the data between the mobile user and the network. As a result, the time needed in the proposed method will be less than that needed by the other systems.

7.5 Comparison of the Core Network Results

The core network of the mobile network is considered as the service provider in the location-based service. However, the data provider in normal systems is a third party company, which is usually external and connected to the mobile operator via the Internet or cloud. The proposed design has introduced a new architecture for the data provider and made the mobile operator itself the data and service provider, which has two possible configurations: one GLMC or multiple GMLC. Chapter five explains the architecture in more detail.

To compare among the three different possible architecture, a network has been built as shown in Figure 7-13. PC1 considered as MSC that received the user request, the MSC (PC1) will look at the information that the user asked for in the local database that attached to the local GMLC (PC2), if the information is not there, the user request will be sent to the another database in the network which is attached to the GMLC2 (PC3 in the diagram).

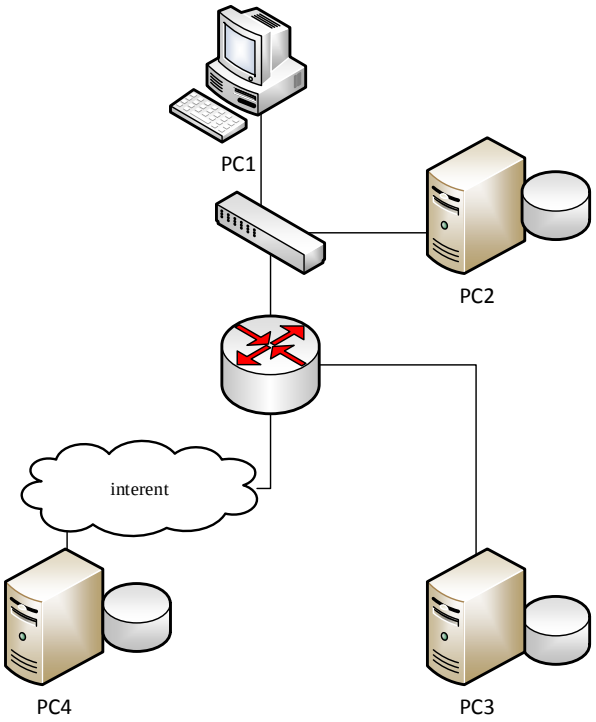


Figure 7-13 Experiment Setup

The third approach is when the user request sent to a third party company (PC4) using the internet, this method, which is used by the 3GPP standard architecture, has also been implemented.

The Matlab has been used in PC1 to send different size of user request to the different databases. First the PC1 sent the request to the local database and received the information back from PC2 and the response time has been measured and recorded. Then the next method used and the PC1 sent the request to the database that belongs to another network (PC3) and the response time has been recorded after PC1 received the information. Finally the last architecture is used and the request is sent to the database in a cloud computer PC4, the response time has been measured in PC1 as well after receiving the requested information from PC4. The size of the user request used in this experiment is vary from 5 to 58 bits.

The comparison between the response time results are shown for different architectures: the "3GPP standard" where the service provider is a third-party, "local" where a database is attached to the GMLC to act like a data provider, and "multiple GMLC" where multiple databases are attached to multiple GMLC and each acts like a data provider. Figure 7-14

shows the response time needed to send and receive the request from the mobile operator to the data provider for different data sizes.

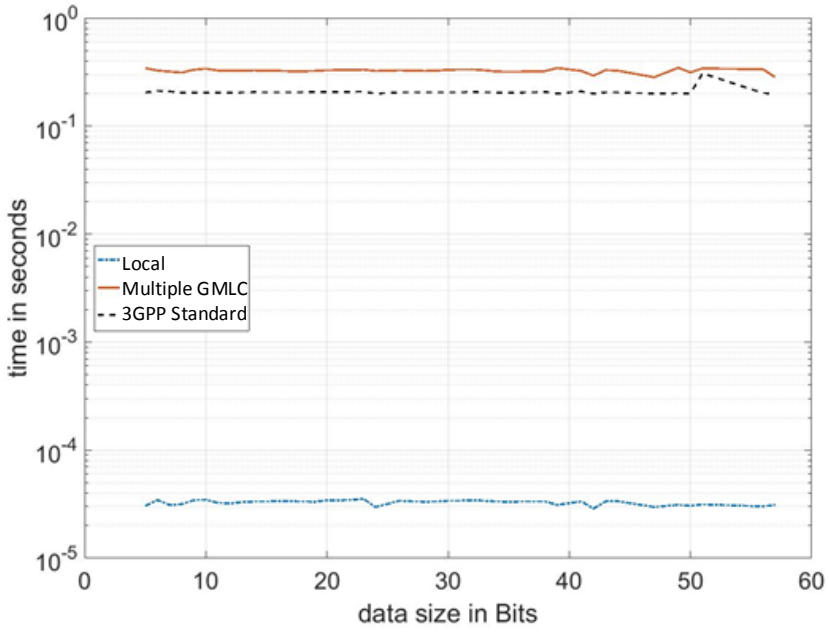


Figure 7-14 Response time with different data size

The figure shows the response time for the local database is much less than those in other architectures; that is because the time needed to send the information to a local database is faster, due to the fewer connections and interfaces. Also, the graph shows a higher time needed for the architecture using more than one GMLC. This is because of the connections being increased and also the routers and other routing devices. However, even though the time is increased from that in the one GMLC architecture, the load on one database is reduced. Figure 7-15 shows the time needed with different numbers of requests at a time.

The proposed architecture has also solved the problem of the privacy issues, as the service provider is the data provider itself. So, the user request and location information no longer need to go to a third-party data provider. To measure the user privacy, it is assumed the user asked for a specific service from the service provider who needs to know the user location. The systems that know the user location are named as coordinators, and then the information that the user asked for will be sent back from the service provider (referring to a system that knows the user information as ‘a collector’). A system that uses cloaking and anonymizers needs an additional trusted server to anonymize the user location and information, so the number of coordinators are at least two (the mobile network operator and the anonymizer)

while the number of the collectors are three; which are mobile operators, the anonymizer and the external LCS.

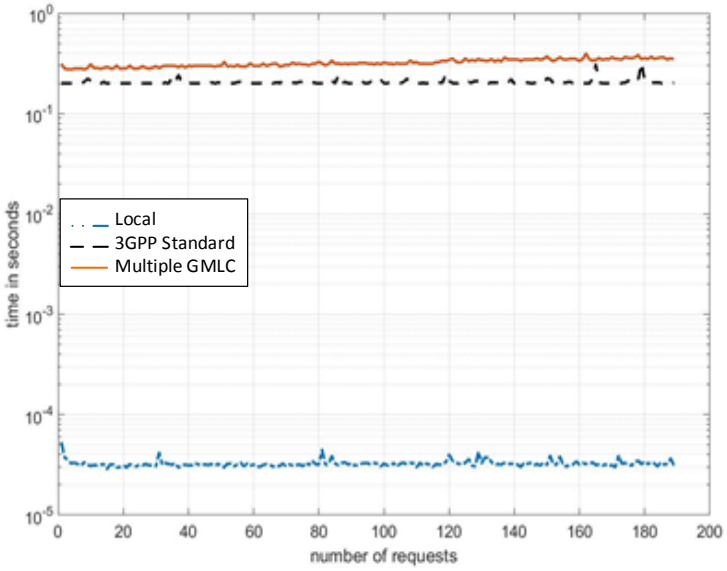


Figure 7-15 Response time with different number of requests

For a standard system where the mobile operator only sends the information to the external LCS, there is no anonymizer or middleware system, so the number of coordinators are at least two (the mobile network operator, and the external LCS) and the number of collectors is two as well (the mobile operator and LCS).

Then, in the proposed architecture, the mobile operator is the only party that knows the user information (coordinator) and can be considered as the information collector. Figure 7-16 shows a comparison of privacy in different systems where the lesser value has better privacy.

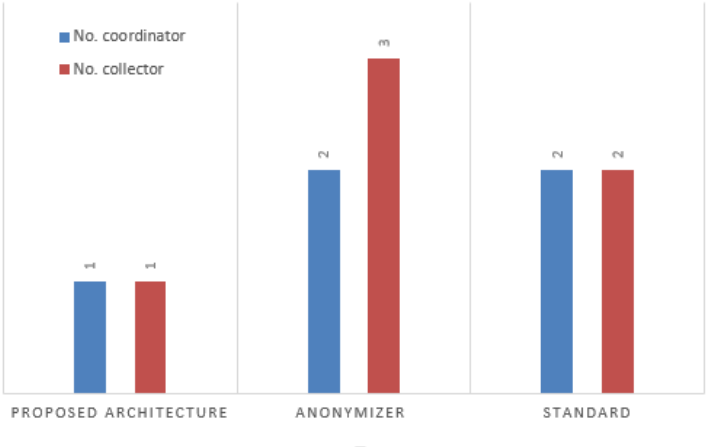


Figure 7-16 Comparison of User Privacy in Different Approaches

7.6 Summary

In this chapter, the results are shown for the transmission of the uplink and the downlink channels. Also, the comparison between the mathematical model for the proposed system and the standard is presented. Then, the differences between the mathematical model and the simulation are shown in order to validate the results. To evaluate the results, this chapter shows the differences between the proposed system and other systems for both uplink and downlink.

After that, the response time for the core network architecture is shown for different architectures, namely when the data provider is an external part, and when the data provider is the mobile operator itself, which could have two possible approaches either has one GMLC or multiple GMLC.

Finally, the different user privacy levels are shown for three types of systems: the proposed architecture, the standard architecture and the system that used an anonymizer.

In the proposed method the data will be sent in the RRC procedure RACH/FACH and no need for further steps. While in other in other system RRC procedure is used to ask for a permission to connect and establish a connection, after the RRC connection completed, the data will be sent in further steps in the data channel that means more time is needed to get the response from the data provider. However in the 3GPP standard the RACH, which is part of the RRC connection procedure, can be used to carry small amount of data, for that reason we compared the results with that in the 3GPP standard system.

Chapter Eight: Conclusion and Future Works

In this chapter the conclusion is presented, as well as possible future and extended work for the system and architecture related to the location-based services.

8.1 Conclusion

- The thesis has presented a new method to transmit the information and user request from and to the data and service provider without using the Internet. Also, it presents new architectures for the mobile operator network to improve the user privacy.
- The thesis has divided the design into three main stages, which are: uplink (for user request) and downlink (for the information sent back to the user) and the core network where the information are stored.
- The spare extension of the RACH is used for uplink and carried by the PRACH to the core network while the spare extension of FACH is used for the downlink channel and it is carried by the S-CCPCH.
- The main contribution of the thesis is to utilize the spare extension in the RACH and the FACH to communicate between the user and the LBS provider without using the Internet. It also preserves the user privacy with faster response time by using the new core network architecture.
- In the 3GPP standards, the RACH is mainly used for RRC connection establishment procedure, and the data will sent after further steps. However, in some cases it could carries small amount of data. All the results shown for the uplink in this thesis is only for the case where the RACH is used to carry the user request. Because it is the fastest method, and the results from the proposed method are compared with this method.
- The new architecture for the core network has two configurations depending on the network configuration; with one GLMC and multiple GMLC. The one GMLC design has one database attached to it to provide the contents and data to the mobile operator. On the other hand, the architecture that has more than one GMLC has multiple databases with each database attached to one GMLC. If the information that the user requested is not found in this database, the GMLC forwards the request to another GMLC.
- In both core network architectures, user privacy has a higher protection and in the first approach where the core network has only one GMLC, the response time needed to obtain the information and location is reduced. This is because the database that is

used can be considered as a local database, not a cloud database or a database on the Internet. In the second approach where the core network has more than one GMLC, the response time is equal or slightly higher compared with a system with an external third-party LCS, but using this approach will reduce the load on the single database.

- One of the achievement of this project is that the data can be sent to the core network and back again to the user successfully without using the Internet. Hence, a new connection has been established for the user to connect with the LBS service and data provider even when the user does not have the Internet enabled on his/her device, and because the spare extension has been used to transmit the data (instead of filling it with zeros) the time needed will be less to transmit the request to the core network compared with the normal system. This transmission method can be used to transmit any small amount of data up to the maximum size of the spare extension of frame structure of the control channel, which is 28 bytes for RACH and FACH. Additionally, it could be used for higher data sizes but the time needed will be increased. However, when the user sends the information or a request, this request is usually a point of interest like a hospital or hotel. So, the data size is generally less than 28 letters and also, the information sent to the user from the data provider is a coordinate, which is less than 28 characters too.
- By using the proposed methods the LBS has achieved better QoS parameters which are mentioned in chapter two: that the LBS after using the new architecture provides better response time and privacy, and because the service will be available anywhere and anytime, the new design has better reliability.
- If there are many users sending a request at the same time, the RACH uses the Slotted ALOHA methods, where when there is a collision, all the connections will be destroyed and the user is asked to retransmit with a random time [8]. So, there will be no problem for the design if there is one user asking for the service or multiple users.
- There are many possible applications that can be used in the proposed design, like emergency services, e-health system, disaster warning messages, and navigation in the rural areas or on motorways where the Internet coverage is not available.
- there are some parameters and stages left out in the mathematical model which are considered in the simulation like noise, scrambling code and channelization code.

8.2 Future Work

The location-based service system has many possible research areas, like the localization methods, way finding, communication network, architecture, QoS parameters like privacy and security and many other areas. However, as our work focuses on the communication and the core network of the LBS, the possible extended future work can be as listed below:

- Implementing the system using a real mobile network experiment and environment.
- This design can be used in any mobile network architecture but it needs to change the frame structure that is implemented. The network that is used in this thesis is the UMTS, but for extended work it can be edited to be used for LTE and LTE-A systems.
- The databases built in this thesis have a set of hotels around the city but the database could be updated in the future so it could have all the possible points of interest like hospitals, restaurants and many others.
- An application layer can be added, so the user can have access to the network from the mobile phone using the application.

References

[1] Tsai, M.H., Y.B. Lin, and H.H. Wang, *Active location reporting for emergency call in UMTS IP multimedia subsystem.* IEEE Transactions on Wireless Communications, 2009. **8**(12): p. 5837-5843.

[2] Khan, I., M. Aazam, E. Ahvar, R. Glitho, and N. Crespi. *Context-Aware Emergency Notification Service over 4G EPC Network: Concept and Design*. in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. 2015.

[3] Aal-Nouman, M., H. Takruri-Rizk, and M. Hope. *Efficient Communications for Location-Based Services Using Spare Extensions of Control Channels in Mobile Networks*. in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2016.

[4] Aal-Nouman, M., O.H. Salman, H. Takruri-Rizk, and M. Hope. *A new architecture for location-based services core network to preserve user privacy*. in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. 2017.

[5] Aloudat, A. and K. Michael, *The application of location based services in national emergency warning systems: SMS, cell broadcast services and beyond.* 2011.

[6] Steiniger, S., M. Neun, and A. Edwardes, *Foundations of location based services.* 2006.

[7] da Rocha, R.C.A., *Middleware for Location-based Services.* Laboratory for Advanced Collaboration, Pontificia Universidade Catolica do Rio de Janeiro, 2004.

[8] Schiller, J.H., *Mobile Communications*. 2003: Pearson Education M.U.A.

[9] Anisetti, M., C.A. Ardagna, V. Bellandi, E. Damiani, and S. Reale, *Map-Based Location and Tracking in Multipath Outdoor Mobile Networks.* Wireless Communications, IEEE Transactions on, 2011. **10**(3): p. 814-824.

[10] Damiani, M.L., *Third party geolocation services in LBS: privacy requirements and research issues.*

[11] 3GPP_TS23.271, *Functional stage 2 description of Location Services (LCS), Release 14 Version 14.2.0* 2017.

[12] Cole, J.M. and B.L. Murphy, *Rural hazard risk communication and public education: Strategic and tactical best practices.* International Journal of Disaster Risk Reduction, 2014. **10**: p. 292-304.

[13] Ramírez, R., *A model for rural and remote information and communication technologies: a Canadian exploration.* Telecommunications Policy, 2001. **25**(5): p. 315-330.

[14] Murphy, B.L., *Emergency management and the August 14th, 2003 blackout*. 2004: Institute for Catastrophic Loss Reduction.

[15] World Health Organization. *Global status report on road safety 2015*. 2015 [cited 2016 June]; Available from: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/.

[16] World Health Organization. *Global Status Report on Road Safety 2015, Statistical Annex*. 2015 [cited 2016 June]; Available from: http://www.who.int/violence_injury_prevention/road_safety_status/2015/Statistical_annex_GSRRS2015.pdf?ua=1.

[17] Aal-Nouman, M., H. Takruri-Rizk, and M. Hope. *Efficient message transmission method for in-vehicle emergency service*. in *2016 6th International Conference on Information Communication and Management (ICICM)*. 2016.

[18] Organization, W.H., *Global diffusion of eHealth: making universal health coverage achievable*. 2016.

[19] Arunachalan, B., J. Light, and I. Watson. *Mobile Agent Based Messaging Mechanism for Emergency Medical Data Transmission Over Cellular Networks*. in *2007 2nd International Conference on Communication Systems Software and Middleware*. 2007.

[20] Ren, Y., R. Werner, N. Pazzi, and A. Boukerche, *Monitoring patients via a secure and mobile healthcare system.* IEEE Wireless Communications, 2010. **17**(1): p. 59-65.

[21] Gallego, J.R., A. Hernandez-Solana, M. Canales, J. Lafuente, A. Valdovinos, and J. Fernandez-Navajas, *Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel.* IEEE Transactions on Information Technology in Biomedicine, 2005. **9**(1): p. 13-22.

[22] Misbahuddin, S., R. Olson, J.A. Zubairi, M. Irfan, S.M. Arif, S. Mansoor, S. Saeed, and Z. Irfan. *Client-server based transmission scheme over GSM network for MEDTOC with patient classification*. in *2012 International Conference on Collaboration Technologies and Systems (CTS)*. 2012.

[23] Tian, Z., J. Yang, and J. Zhang. *Location-based Services Applied to an Electric Wheelchair Based on the GPS and GSM Networks*. in *Intelligent Systems and Applications, 2009. ISA 2009. International Workshop* 2009.

[24] Chaklader, S., J. Alam, M. Islam, and A.S. Sabbir. *Black Box: An emergency rescue dispatch system for road vehicles for instant notification of road accidents and post crash analysis*. in *Informatics, Electronics & Vision (ICIEV), 2014 International Conference on*. 2014.

[25] Prakoso, B.M., A.R.N. Pristy, M. Arsyad, A.B. Noegroho, A. Sudarsono, and A. Zainudin. *Performance analysis of OLSR Routing for secure medical data transmission for rural areas with Delay Tolerant Network*. in *2016 International Symposium on Electronics and Smart Devices (ISESD)*. 2016.

[26] UNISDR, C., *The human cost of natural disasters: A global perspective*. 2015.

[27] Mayhorn, C.B. and A.C. McLaughlin, *Warning the world of extreme events: A global perspective on risk communication for natural and technological disaster*. Safety Science, 2014. **61**: p. 43-50.

[28] Azam, M., H.S. Kim, and S.J. Maeng, *Development of flood alert application in Mushim stream watershed Korea*. International Journal of Disaster Risk Reduction, 2017. **21**: p. 11-26.

[29] Reduction, U.O.f.D.R., *Local government powers for disaster risk reduction: A study on local-level authority and capacity for resilience*. 2017.

[30] UN, *The Sendai Framework for Disaster Risk Reduction 2015–2030*. 2015. **1516716**.

[31] Reduction, U.N.O.f.D.R., *How to Make Cities More Resilient: A Handbook for Local Government Leaders: a Contribution to the Global Campaign 2010-2015: Making Cities Resilient-My City is Getting Ready!* 2012: UNISDR.

[32] Nakamura, H., H. Umeki, and T. Kato, *Importance of communication and knowledge of disasters in community-based disaster-prevention meetings*. Safety Science, 2016.

[33] Kapucu, N., *Disaster and emergency management systems in urban areas*. Cities, 2012. **29**: p. S41-S49.

[34] Basu, M., S. Ghosh, A. Jana, S. Bandyopadhyay, and R. Singh, *Resource mapping during a natural disaster: A case study on the 2015 Nepal earthquake*. International Journal of Disaster Risk Reduction, 2017. **24**: p. 24-31.

[35] Wafi, Z.N.K., M.F.A. Malek, S.H. Alnajjar, and R.B. Ahmad. *Early warning system for Disaster management in rural area*. in *2015 International Symposium on Technology Management and Emerging Technologies (ISTMET)*. 2015.

[36] Philip, L., C. Cottrill, J. Farrington, F. Williams, and F. Ashmore, *The digital divide: Patterns, policy and scenarios for connecting the 'final few' in rural communities across Great Britain*. Journal of Rural Studies, 2017. **54**(Supplement C): p. 386-398.

[37] Song, L. and J. Shen, *Evolved cellular network planning and optimization for UMTS and LTE*. 2010: CRC Press.

[38] Auer, G., V. Giannini, C. Desset, I. Godor, P. Skillermark, M. Olsson, M.A. Imran, D. Sabella, M.J. Gonzalez, O. Blume, and A. Fehske, *How much energy is needed to run a wireless network?* IEEE Wireless Communications, 2011. **18**(5): p. 40-49.

[39] Krumm, J., *A survey of computational location privacy.* Personal and Ubiquitous Computing, 2009. **13**(6): p. 391-399.

[40] Cvrcek, D., M. Kumpost, V. Matyas, and G. Danezis. *A study on the value of location privacy*. in *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*. 2006. ACM.

[41] Poikela, M. and E. Toch. *Understanding the Valuation of Location Privacy: a Crowdsourcing-Based Approach*. in *Proceedings of the 50th Hawaii International Conference on System Sciences*. 2017.

[42] Association, U.I.R.M., *Geographic information systems: concepts, methodologies, tools, and applications*. 2012: IGI Global.

[43] Steiniger, S., M. Neun, A. Edwardes, and B. Lenz, *Foundations of LBS.* CartouCHe-Cartography for Swiss Higher Education. Obtido em, 2008. **20**: p. 2010.

[44] Filjar, R., K. Vidovi, x, P. Britvi, x, and M. Rimac. *eCall: Automatic notification of a road traffic accident*. in *MIPRO, 2011 Proceedings of the 34th International Convention*. 2011.

[45] 3GPP_TS26.267, *eCall data transfer; In-band modem solution; General description, Release 14 Version 14.0.0.* 2017.

[46] 3GPP_TS25.305, *"Stage 2 functional specification of UE positioning in UTRAN", Release 14 Version 14.0.0.* 2017.

[47] 3GPP_TS36.355, *Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP), Release 14 Version 14.2.0.* 2017.

[48] Duan, X., *Method for processing location information request initiated by a user equipment*. 2014, Google Patents.

[49] 3GPP_TS22.071, *Location Services (LCS); Service description; Stage 1, Release 14 Version 14.1.0* 2015.

[50] Küpper, A., *Architectures and Protocols for Location Services*, in *Location-Based Services*. 2005, John Wiley & Sons, Ltd. p. 271-313.

[51] Puttaswamy, K.P.N. and B.Y. Zhao, *Preserving privacy in location-based mobile social applications*, in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. 2010, ACM: Annapolis, Maryland. p. 1-6.

[52] Gabriel, G., *Privacy for Location-based Services*. Privacy for Location-based Services. 2013: Morgan & Claypool. 85.

[53] Hashem, T. and L. Kulik, *"Don't trust anyone": Privacy protection for location-based services.* Pervasive and Mobile Computing, 2011. **7**(1): p. 44-59.

[54] 3GPP_TS23.002, *Network Archituctre Release 14 Version 14.1.0* 2017.

[55] Sanchez, J. and M. Thioune, *UMTS Core Network*, in *UMTS*. 2010, ISTE. p. 61-83.

[56] Kaaranen, H., *UMTS networks: architecture, mobility and services*. 2005: John Wiley & Sons.

[57] 3GPP_TS25.435, *UTRAN Iub interface user plane protocols for Common Transport Channel data streams, Release 14 Version 14.0.0.* 2017.

[58] Toskala, A. and H. Holma, *WCDMA for UMTS : HSPA Evolution and LTE*. 2007, Chichester, England: John Wiley and Sons, Inc.

[59] 3GPP_TS25.211, *Physical channels and mapping of transport channels onto physical channels (FDD), Release 14 Version 14.0.0* 2017.

[60] Sanchez, J. and M. Thioune, *UTRA/FDD Transmission Chain*, in *UMTS*. 2010, ISTE. p. 227-270.

[61] 3GPP_TR25.212, *Multiplexing and channel coding (FDD), Release 14 Version 14.0.0* 2017.

[62] Walke, B., R. Seidenberg, and M.P. Althoff, *UMTS, The Fundamentals*. 2003: WILEY.

[63] Xiong, F., *Digital Modulation Techniques*. Artech House Telecommunications Library. 2006, Boston, MA: Artech House.

[64] 3GPP_TS25.331, *Radio Resource Control (RRC) Protocol specification, Release 14 Version 14.3.0.* 2017.

[65] 3GPP_TR25.931, *UTRAN functions, examples on signalling procedures, Release 14 Version 14.0.0* 2017.

[66] 3GPP_25.410, *UTRAN Iu interface: General aspects and principles, Release 14, Version 14.0.0.* 2017.

[67] 3GPP_TS25.414, *UTRAN Iu interface data transport and transport signalling, Release 14 Version 14.0.0.* 2017.

[68] Karlander, B., S. Nádas, S. Rácz, and J. Reinius, *AAL2 switching in the WCDMA radio access network.* Ericsson Review, 2002. **79**(3): p. 114-123.

[69] Union, I.T., *ITU-T I.361 "Overall network aspects and functions – Protocol layer requirements, B-ISDN ATM layer specification".* 1999.

[70] McLoughlin, M. and J. O'Neil, *Adapting voice for ATM networks: An AAL2 tutorial.* General DataComm, Inc. document, 1997.

[71] Sherif, M.R., A. Elnashar, M.A. El-saidny, and M.R. Sherif, *Voice Evolution in 4G Networks*, in *Design, Deployment and Performance of 4G-LTE Networks*. 2014, John Wiley & Sons, Ltd. p. 445-506.

[72] 3GPP_TS32.401, *GPRS enhancement for E-UTRAN access, Version 12.10.0, Release 12.* 2015.

[73] 3GPP_TS23.272, *Circuit Swirched fallback in Evolved Packet System; Stage 2, Version 12.6.0 Release 12.* 2015.

[74] Cambridge, A.T.L. *The Active Badge System.* [cited 2017 May 2017]; Available from: http://www.cl.cam.ac.uk/research/dtg/attarchive/ab.html.

[75] Silventoinen, M.I. and T. Rantalainen. *Mobile station emergency locating in GSM*. in *1996 IEEE International Conference on Personal Wireless Communications Proceedings and Exhibition. Future Access*. 1996.

[76] 3GPP_TR22.967, *Transferring of emergency call data, Release 14 Version 14.0.0.* 2017.

[77] Forum, e., *Clarification Paper - EG. 2 , High level requirements for a eCall in-vehicle system, Supplier perspective, Version 1 .0* 2006.

[78] Forum, e., *European Memorandum of Understanding for Realisation of Interoperable In-Vehicle eCall.* 2004.

[79] Sukaphat, S., *An implementation of location-based service system with cell identifier for detecting lost mobile.* Procedia Computer Science, 2011. **3**(0): p. 949-953.

[80] Hasemann, J.M., *Method and system for using Location-Based Services for mobile terminals*. 2012, Google Patents.

[81] Panahi, M.S., P. Woods, and H. Thwaites. *Designing and developing a location-based mobile tourism application by using cloud-based platform*. in *Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on*. 2013.

[82] Fogue, M., P. Garrido, F.J. Martinez, J.C. Cano, C.T. Calafate, P. Manzoni, and M. Sanchez. *Prototyping an automatic notification scheme for traffic accidents in vehicular networks*. in *Wireless Days, 2011 IFIP*. 2011.

[83] Dhas, B.C. and P.P.E. Winston. *Efficient vehicular communication using random access channels in UMTS based network*. in *2014 International Conference on Electronics and Communication Systems (ICECS)*. 2014.

[84] Hongsheng, Z., W. Guoyu, L. Mingying, W. Daicheng, and X. Peng. *Emergency warning and bidirectional communication via Digital Audio Broadcast*. in *2017 IEEE International Conference on Consumer Electronics (ICCE)*. 2017.

[85] Singh, Piplani, Shinde, and Karthik. *mKRISHI fisheries: a case study on early warning system (EWS) for disaster communication and management*. in *2016 IEEE International Symposium on Technology and Society (ISTAS)*. 2016.

[86] Chen, Z., C. Fang, and R. Deng. *Research and application of Jinggangshan geological disaster prevention system based on wireless sensor network system*. in *2015 23rd International Conference on Geoinformatics*. 2015.

[87] Erdelj, M., M. Król, and E. Natalizio, *Wireless Sensor Networks and Multi-UAV systems for natural disaster management.* Computer Networks, 2017. **124**: p. 72-86.

[88] Erd, M., F. Schaeffer, M. Kostic, and L.M. Reindl, *Event monitoring in emergency scenarios using energy efficient wireless sensor nodes for the disaster information management.* International Journal of Disaster Risk Reduction, 2016. **16**: p. 33-42.

[89] Solmaz, G. and D. Turgut, *Modeling pedestrian mobility in disaster areas.* Pervasive and Mobile Computing, 2017. **40**: p. 104-122.

[90] Landwehr, P.M., W. Wei, M. Kowalchuck, and K.M. Carley, *Using tweets to support disaster planning, warning and response.* Safety Science, 2016. **90**: p. 33-47.

[91] Carley, K.M., M. Malik, P.M. Landwehr, J. Pfeffer, and M. Kowalchuck, *Crowd sourcing disaster management: The complex nature of Twitter usage in Padang Indonesia.* Safety Science, 2016. **90**: p. 48-61.

[92] Huang, H., T. Gong, N. Ye, R. Wang, and Y. Dou, *Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System.* IEEE Transactions on Industrial Informatics, 2017. **13**(3): p. 1227-1237.

[93] Rehunathan, D., S. Bhatti, O. Chandran, and H. Pan. *vNurse: Using virtualisation on mobile phones for remote health monitoring*. in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*. 2011.

[94] Brahmi, H.I., S. Djahel, and J. Murphy. *Improving emergency messages transmission delay in road monitoring based WSNs*. in *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*. 2013.

[95] Shahbazi, A., A.H. Rezaie, A. Sayadiyan, and S. Mosayyebpour, *Data Transmission over GSM Adaptive Multi Rate Voice Channel Using Speech-Like Symbols.* 2010 International Conference on Signal Acquisition and Processing: Icsap 2010, Proceedings, 2010: p. 63-67.

[96] LaDue, C.K., V.V. Sapozhnykov, and K.S. Fienberg, *A Data Modem for GSM Voice Channel.* Vehicular Technology, IEEE Transactions on, 2008. **57**(4): p. 2205-2218.

[97] Ali, B.T., G. Baudoin, and O. Venard. *Data transmission over mobile voice channel based on M-FSK modulation*. in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*. 2013.

[98] Ghosh, R., B. Chatterjee, D. Dey, and S. Chakravorti, *Low-complexity leakage current acquisition system for transmission line insulators employing GSM voice channel.* Electronics Letters, 2015. **51**(19): p. 1538-1540.

[99] Peric, M., P. Milicevic, Z. Banjac, and B.M. Todorovic. *An experiment with real-time data transmission over global scale mobile voice channel*. in *Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2015 12th International Conference on*. 2015.

[100] Colbert, M. *A diary study of rendezvousing: implications for position-aware computing and communications for the general public*. in *Proceedings of the 2001 International ACM SIGGROUP Conference on Supporting Group Work*. 2001. ACM.

[101] Danezis, G., S. Lewis, and R.J. Anderson. *How much is location privacy worth?* in *WEIS*. 2005. Citeseer.

[102] Iachello, G., I. Smith, S. Consolvo, G.D. Abowd, J. Hughes, J. Howard, F. Potter, J. Scott, T. Sohn, and J. Hightower. *Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service*. in *International Conference on Ubiquitous Computing*. 2005. Springer.

[103] Barkhuus, L. and A.K. Dey. *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*. in *Interact*. 2003. Citeseer.

[104] Lin, J., M. Benisch, N. Sadeh, J. Niu, J. Hong, B. Lu, and S. Guo, *A comparative study of location-sharing privacy preferences in the United States and China.* Personal and Ubiquitous Computing, 2013. **17**(4): p. 697-711.

[105] Puttaswamy, K.P., S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel, and B.Y. Zhao, *Preserving location privacy in geosocial applications.* IEEE Transactions on Mobile Computing, 2014. **13**(1): p. 159-173.

[106] Peng, T., Q. Liu, and G. Wang, *Enhanced Location Privacy Preserving Scheme in Location-Based Services.* IEEE Systems Journal, 2017. **11**(1): p. 219-230.

[107] Schlegel, R., C. Chow, Q. Huang, and D. Wong, *User-Defined Privacy Grid System for Continuous Location-Based Services.* IEEE Transactions on Mobile Computing, 2015(99).

[108] Dewri, R. and R. Thurimella, *Exploiting service similarity for privacy in location-based search queries.* IEEE Transactions on parallel and distributed systems, 2014. **25**(2): p. 374-383.

[109] Gong, Z., G.-Z. Sun, and X. Xie. *Protecting privacy in location-based services using k-anonymity without cloaked region*. in *Mobile Data Management (MDM), 2010 Eleventh International Conference on*. 2010. IEEE.

[110] Gan, J., H. Xu, M. Xu, K. Tian, Y. Zheng, and Y. Zhang, *Study on Personalized Location Privacy Protection Algorithms for Continuous Queries in LBS*, in *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings*, G. Wang, et al., Editors. 2016, Springer International Publishing: Cham. p. 98-108.

[111] Lee, H., B.-S. Oh, H.-i. Kim, and J. Chang, *Grid-based cloaking area creation scheme supporting continuous location-based services*, in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. 2012, ACM: Trento, Italy. p. 537-543.

[112] Ardagna, C.A., M. Cremonini, S.D.C. di Vimercati, and P. Samarati, *An obfuscation-based approach for protecting location privacy.* IEEE Transactions on Dependable and Secure Computing, 2011. **8**(1): p. 13-27.

[113] Niu, B., X. Zhu, H. Chi, and H. Li, *Pseudo-Location Updating System for privacy-preserving location-based services.* China Communications, 2013. **10**(9): p. 1-12.

[114] Myungah, K. and C. Myungwhan. *Anonymization scheme using non-trusted agent for location based services*. in *2017 International Conference on Information Networking (ICOIN)*. 2017.

[115] Tang, D., G. Jian, H. Weijia, and M. Xiao. *A novel secure forwarding scheme for Location Based Service*. in *2017 International Conference on Computing, Networking and Communications (ICNC)*. 2017.

[116] Freudiger, J., R. Shokri, and J.-P. Hubaux, *Evaluating the Privacy Risk of Location-Based Services*, in *Financial Cryptography and Data Security*, G. Danezis, Editor. 2012, Springer Berlin Heidelberg. p. 31-46.

[117] Ahson, S. and M. Ilyas, *Location-based services handbook : applications, technologies, and security*. 2011, Boca Raton, Fla.: CRC ; London : Taylor & Francis

[118] Springer, A. and R. Weigel, *UMTS :The Physical Layer of the Universal Mobile Telecommunications System*. 2002: Springer Berlin Heidelberg.

[119] 3GPP_TS25.425, *UTRAN Iur interface user plane protocols for Common Transport Channel data streams, Release 14 Version 14.0.0.* 2017.

[120] Patil, B., *IP in wireless Networks*. 2003: Prentice Hall Professional.

[121] Naveh, T., *Mobile backhaul: Fiber vs. microwave.* Ceragon White Paper, 2009. **1**: p. 1-11.

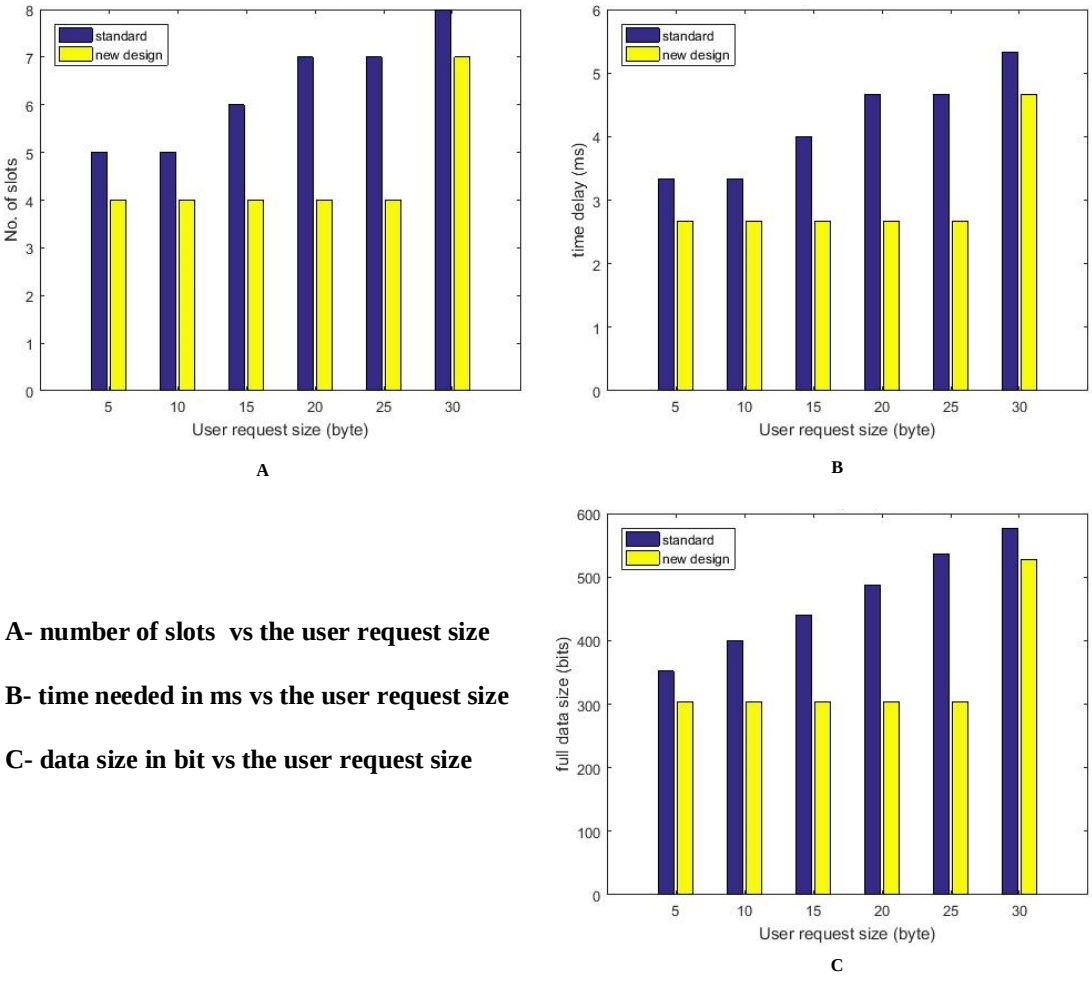
[122] Bhadra, D.R., C.A. Joshi, P.R. Soni, N.P. Vyas, and R.H. Jhaveri. *Packet loss probability in wireless networks: A survey*. in *Communications and Signal Processing (ICCSP), 2015 International Conference on*. 2015. IEEE.

Appendix A: Mathematical Results

In this appendix the results gotten from the mathematical model are shown with different spreading factors, for the uplink the SF= 32, 64,128, and 256 are shown, and the results for the spreading factors SF=4, 8,16,32,64, and 128 are shown in this appendix

Uplink

In this section, the comparison between the results gotten from the uplink equations have been shown. The spreading factor can take different values vary from 32 to 256, which are namely (32, 64, 128, and 256).

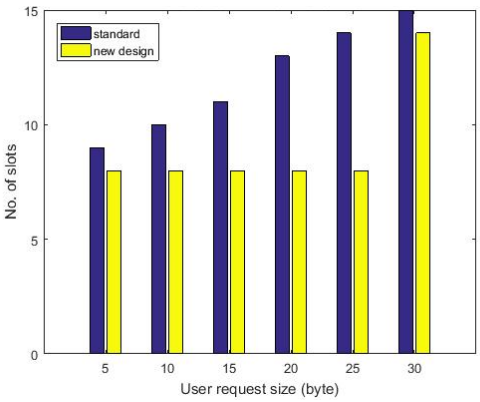


A- number of slots vs the user request size

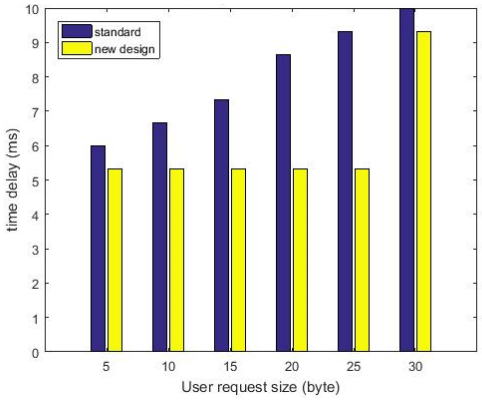
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure A-1 Mathematical Uplink Result for SF=32

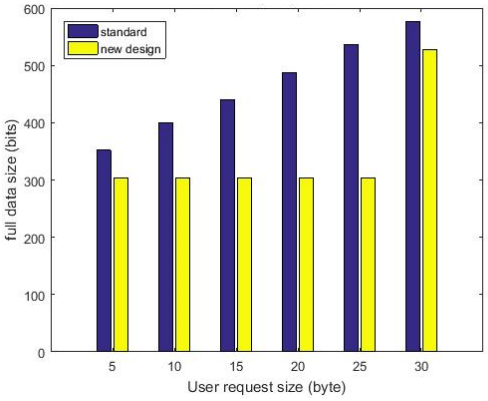


A



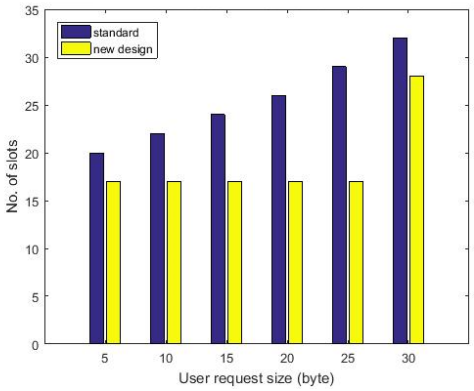
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

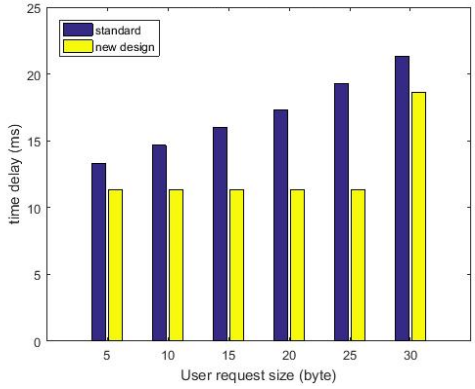


C

Figure A-2 Mathematical Uplink Result for SF SF=64

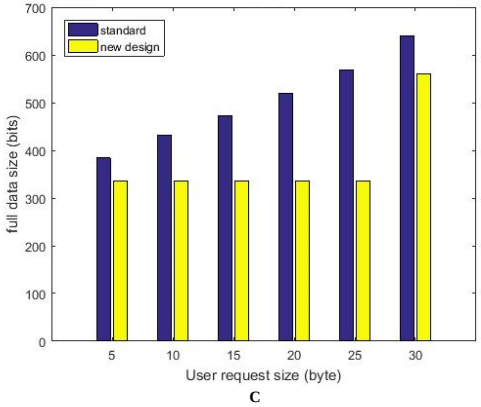


A



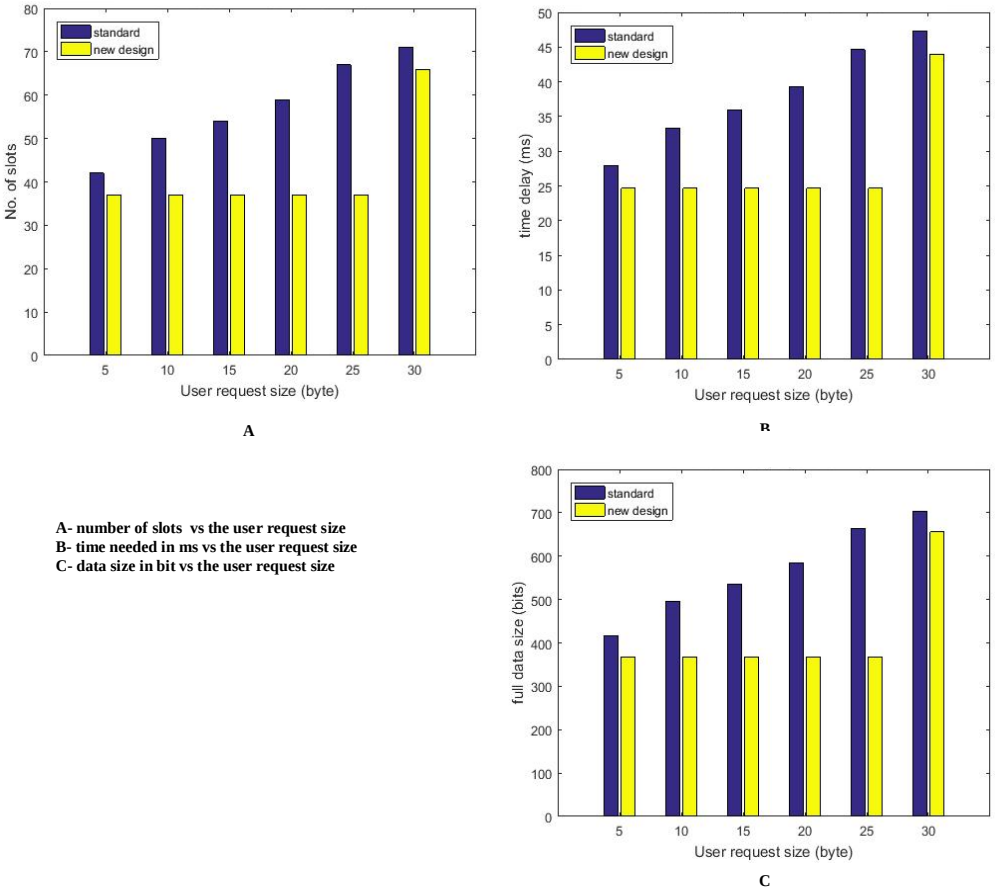
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size



C

Figure A-3 Mathematical Uplink Result for SF=128

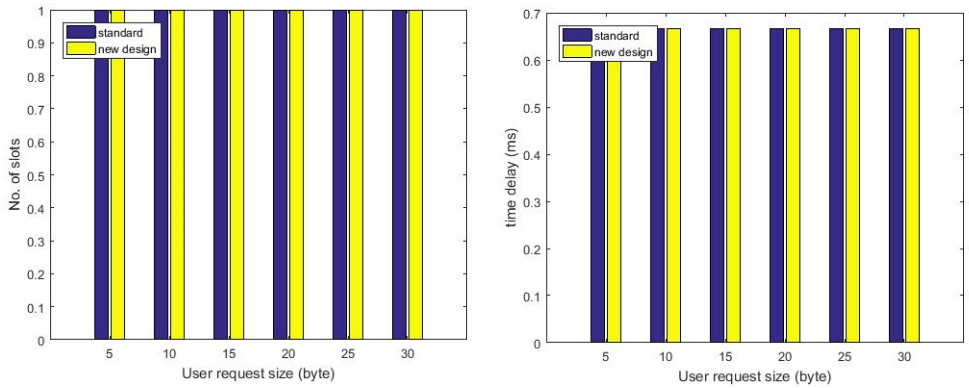


A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

Figure A-4 Mathematical Uplink Result for SF=256

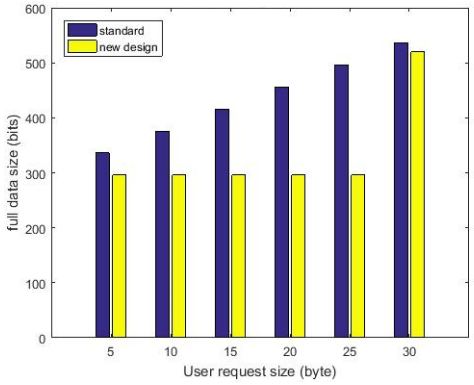
Downlink

The downlink mathematical results of a comparison between the standard model and the system design is illustrated in this section. The downlink has many options for the spreading factors, which is started from 4 till 256



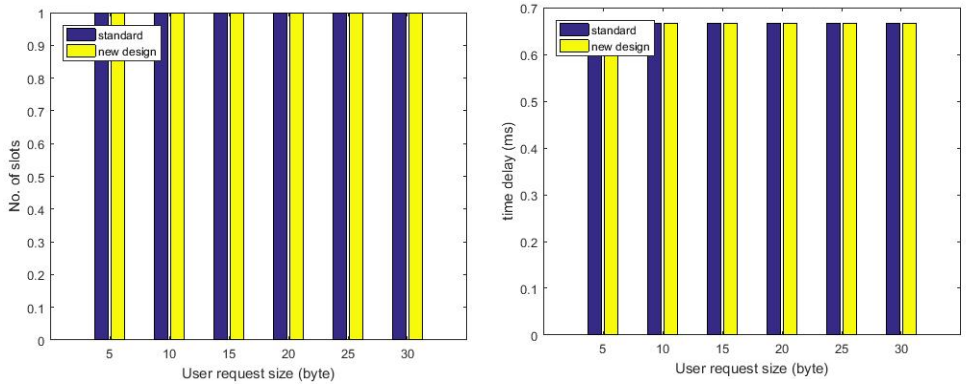
A B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size



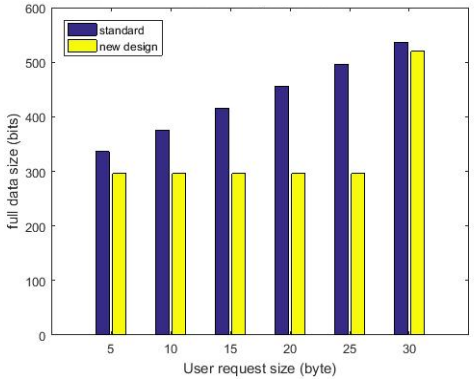
C

Figure A-5 Mathematical Downlink Results for SF=4



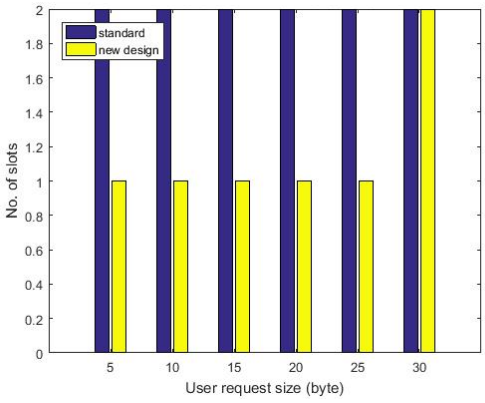
A B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

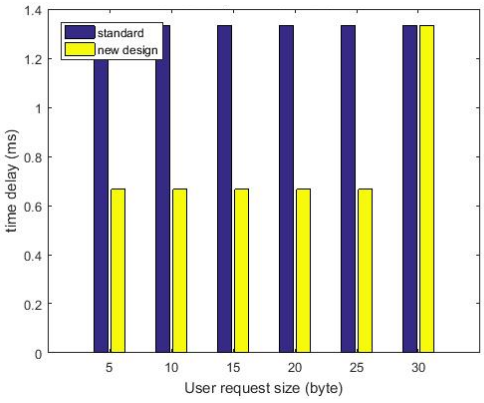


C

Figure A-6 Mathematical Downlink Results for SF=8

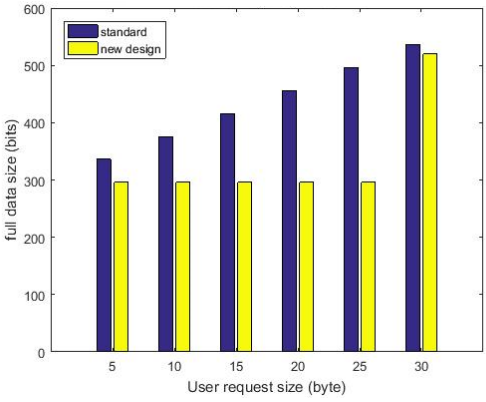


A



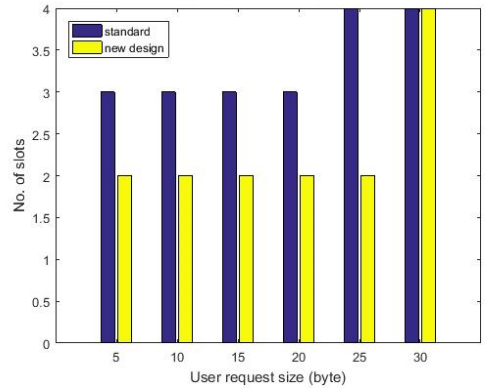
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

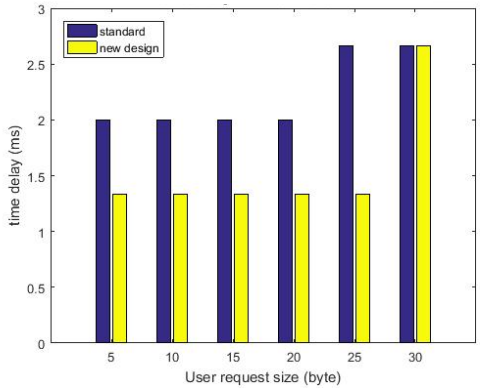


C

Figure A-7 Mathematical Downlink Results for SF=16

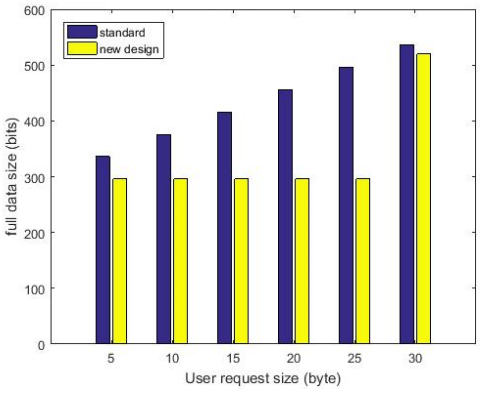


A



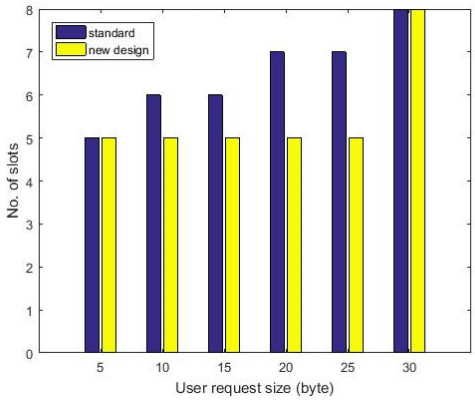
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

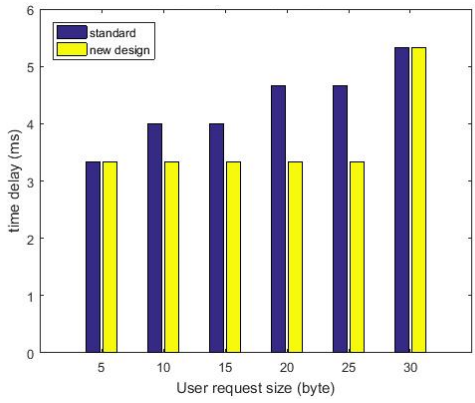


C

Figure A-8 Mathematical Downlink Results for SF=32

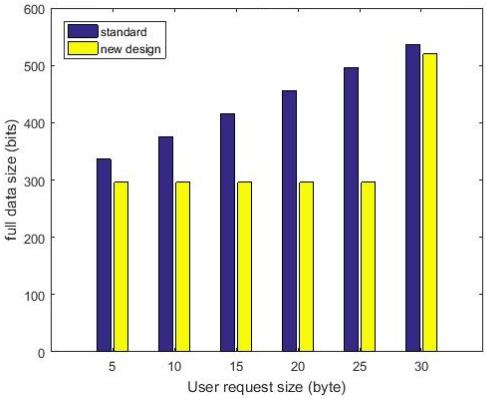


A



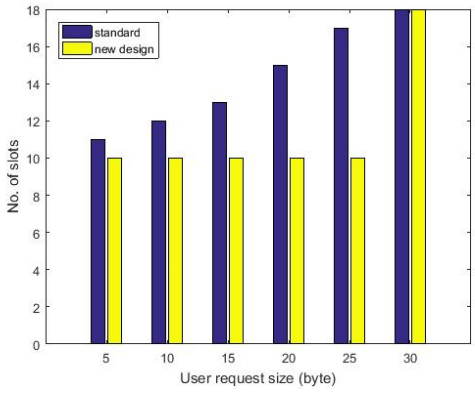
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

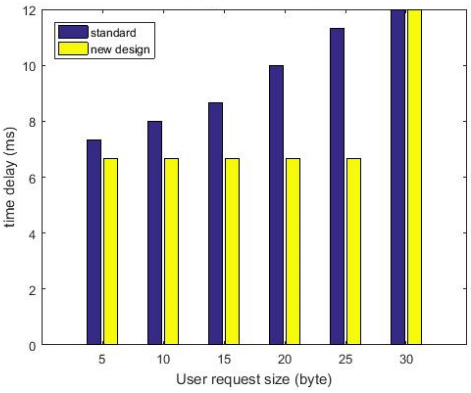


C

Figure A-9 Mathematical Downlink Results for SF=64

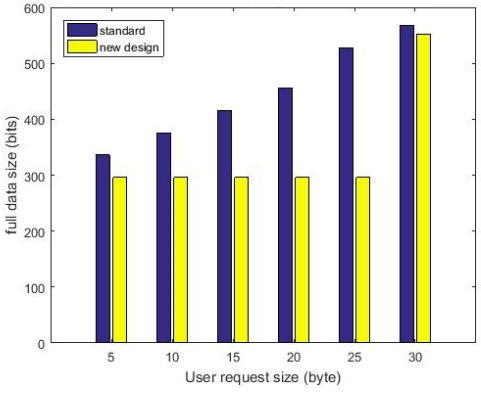


A



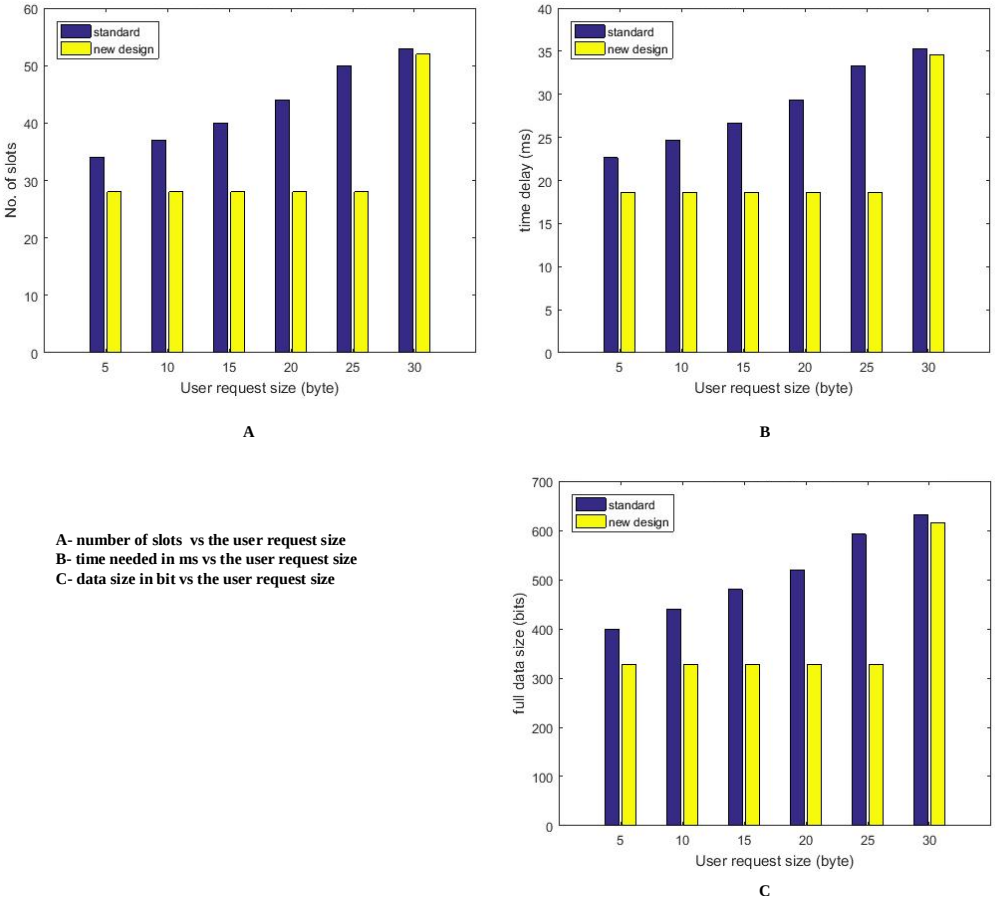
B

A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size



C

Figure A-10 Mathematical Downlink Results for SF=128



A- number of slots vs the user request size
B- time needed in ms vs the user request size
C- data size in bit vs the user request size

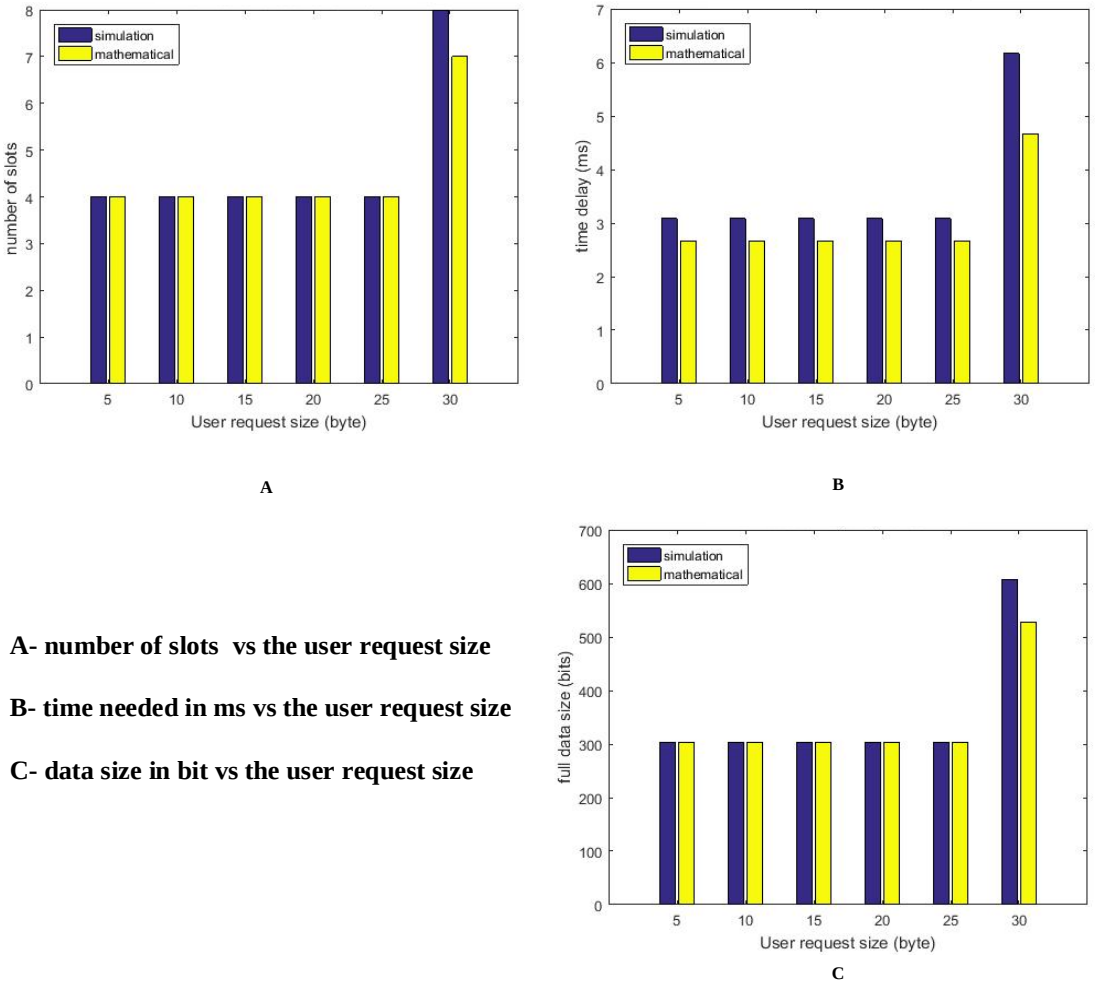
Figure A-11 Mathematical Downlink Results for SF=256

Appendix B: Simulation Results

The simulation results are shown in this section to show the differences and compare between the simulation results and the mathematical model in order to validate the simulation results. The results can be divided into uplink result and downlink results.

Uplink

The simulation result gotten from the uplink channel using the RACH is compared with the mathematical model to validate the simulation results. As mentioned earlier in this chapter, the uplink can take different spreading factors which are 32, 64, 128 and 256.

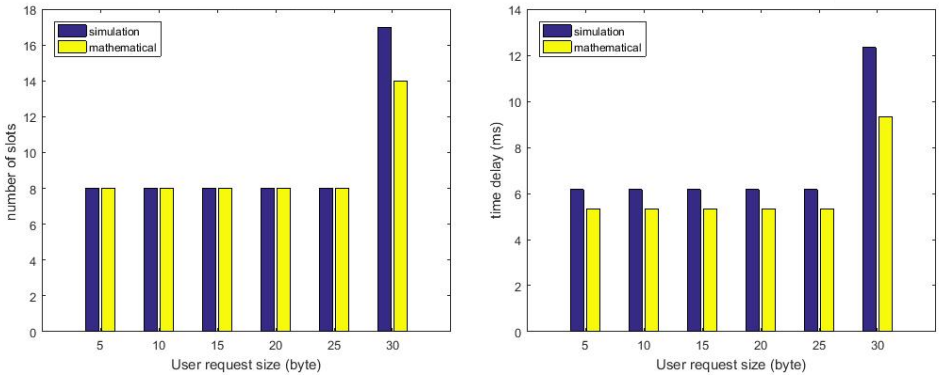


A- number of slots vs the user request size

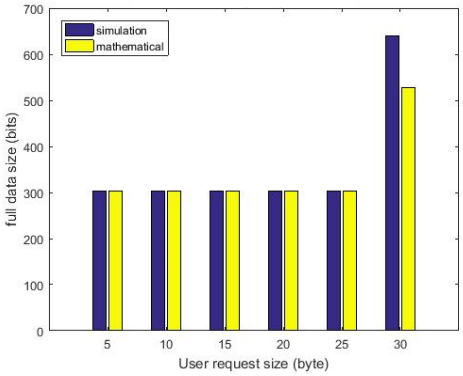
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure B-1 Comparison Between The Mathematical Results and Simulation Result for Uplink with SF= 32



A B



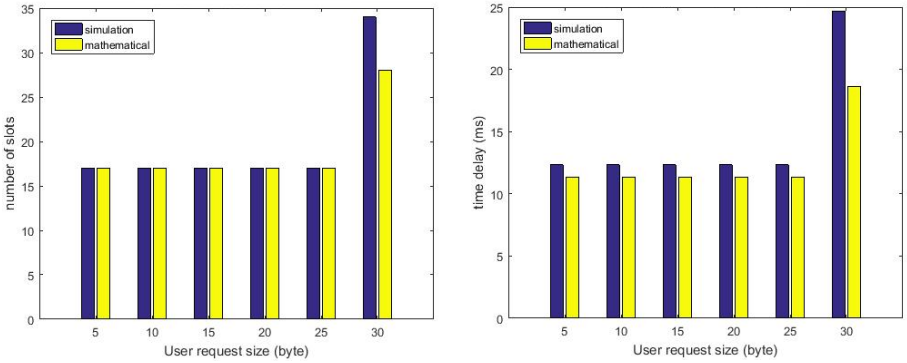
C

A- number of slots vs the user request size

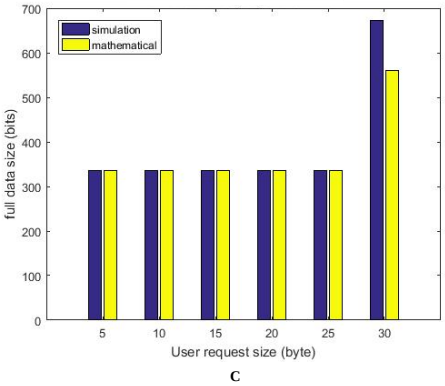
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure B-2 Comparison Between The Mathematical Results and Simulation Result for Uplink with SF=64



A B



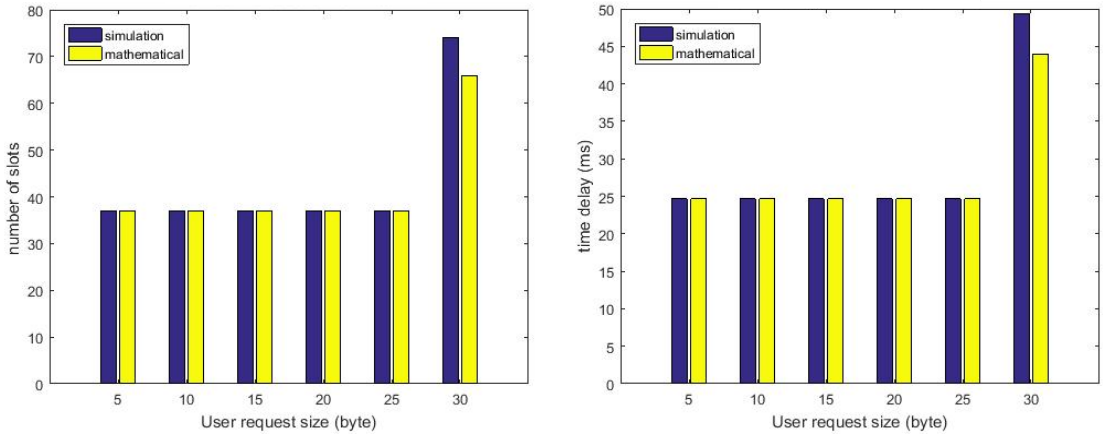
C

A- number of slots vs the user request size

B- time needed in ms vs the user request size

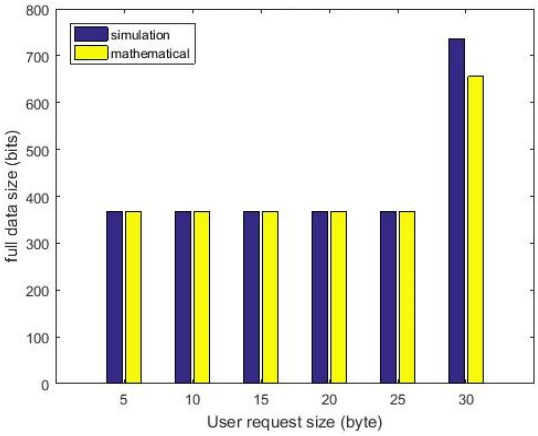
C- data size in bit vs the user request size

Figure B-3 Comparison Between The Mathematical Results and Simulation Result for Uplink with SF= 128



A

B



C

A- number of slots vs the user request size

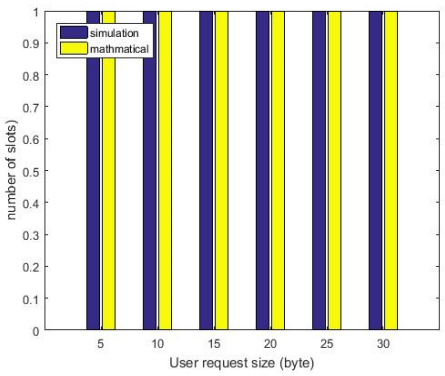
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

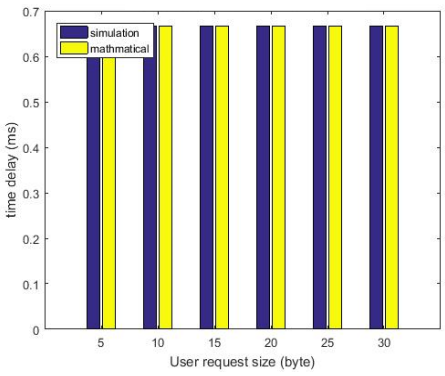
Figure B-4 Comparison Between The Mathematical Results and Simulation Result for Uplink with SF= 256

Downlink

A comparison between the simulation result gotten from the downlink channel using the FACH and mathematical model is shown in this section to validate the downlink simulation results. The downlink channel can take different spreading factors which are 4, 8, 16, 32, 64, 128 and 256, all these possible spreading factors are considered in the results to validate the downlink channel results as shown.



A

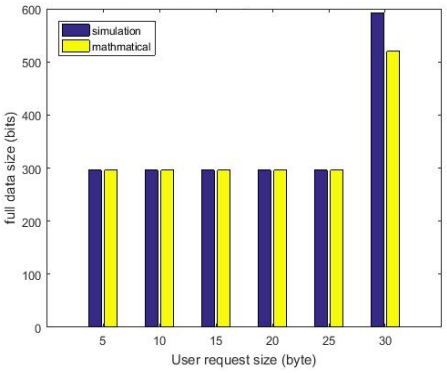


B

A- number of slots vs the user request size

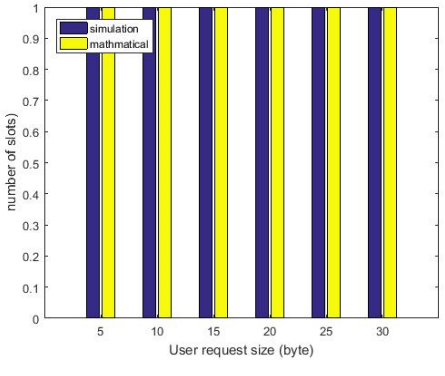
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

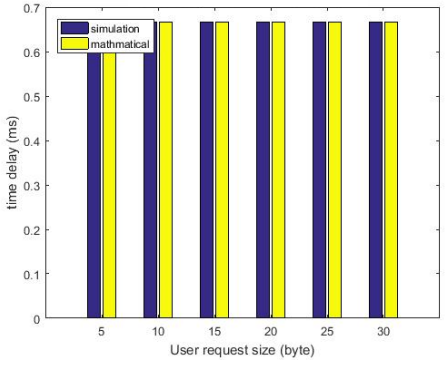


C

Figure B-5 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=4



A

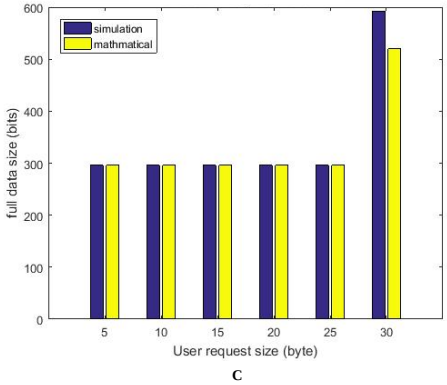


B

A- number of slots vs the user request size

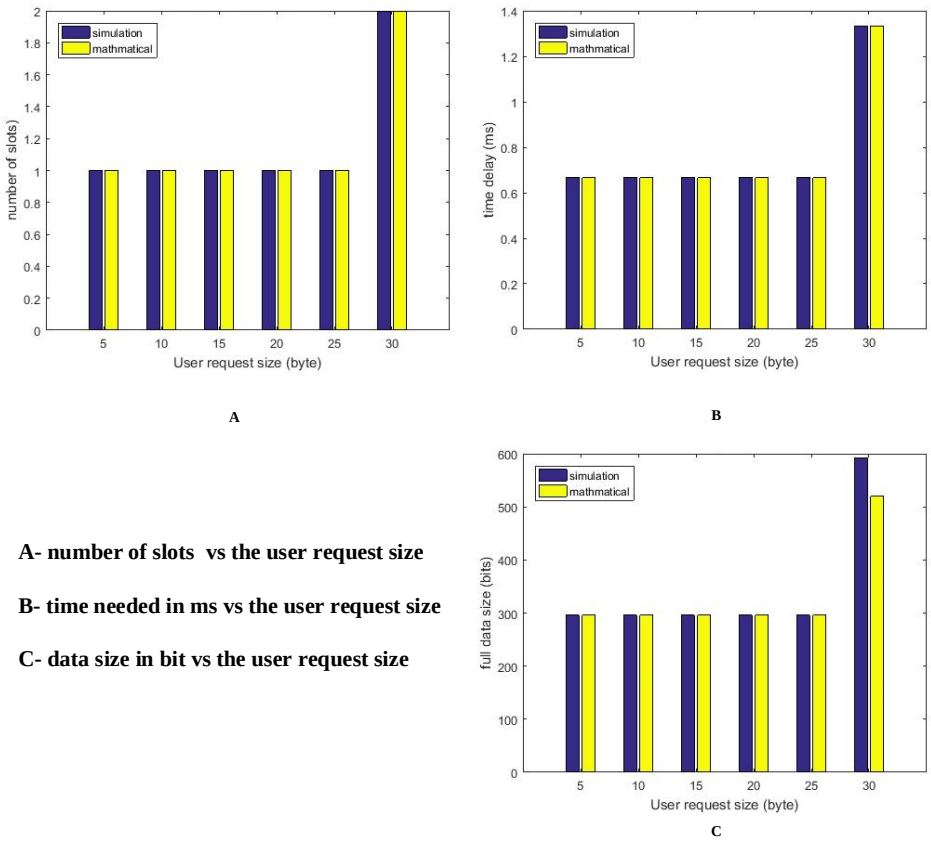
B- time needed in ms vs the user request size

C- data size in bit vs the user request size



C

Figure B-6 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=8

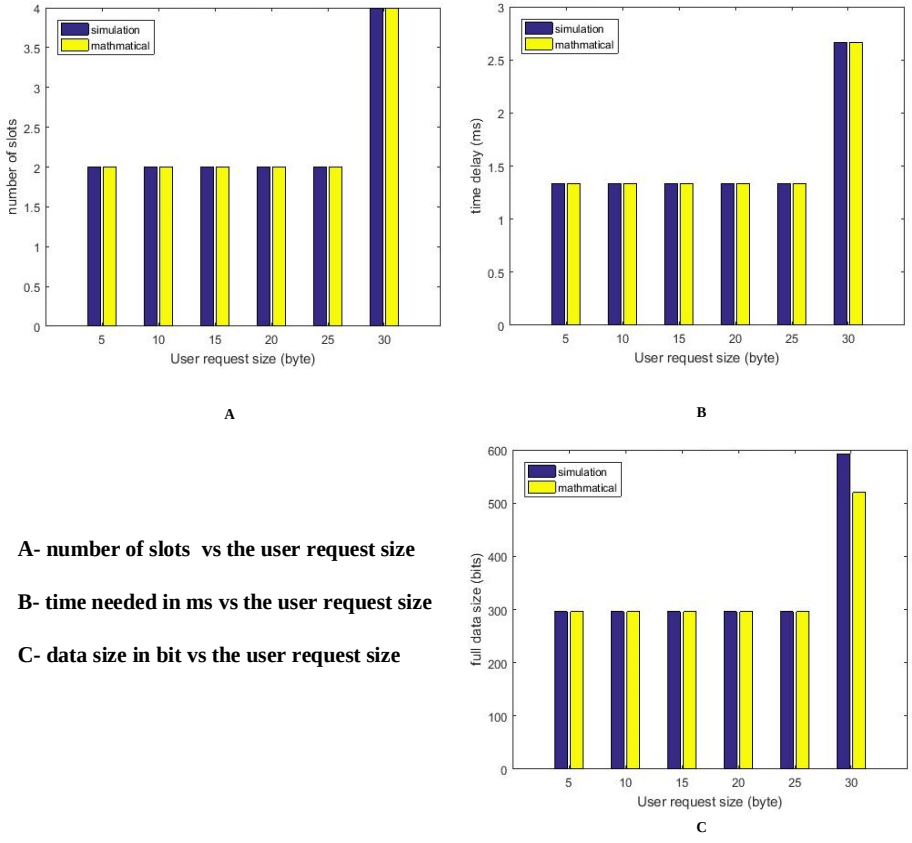


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure B-7 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=16

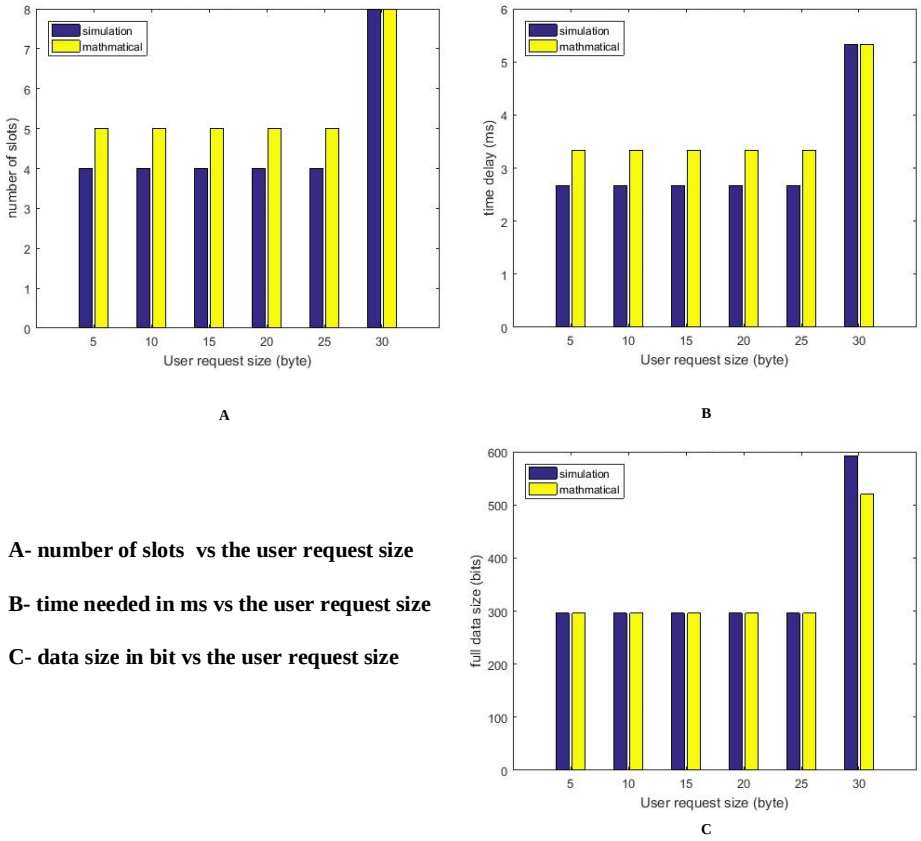


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure B-8 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=32

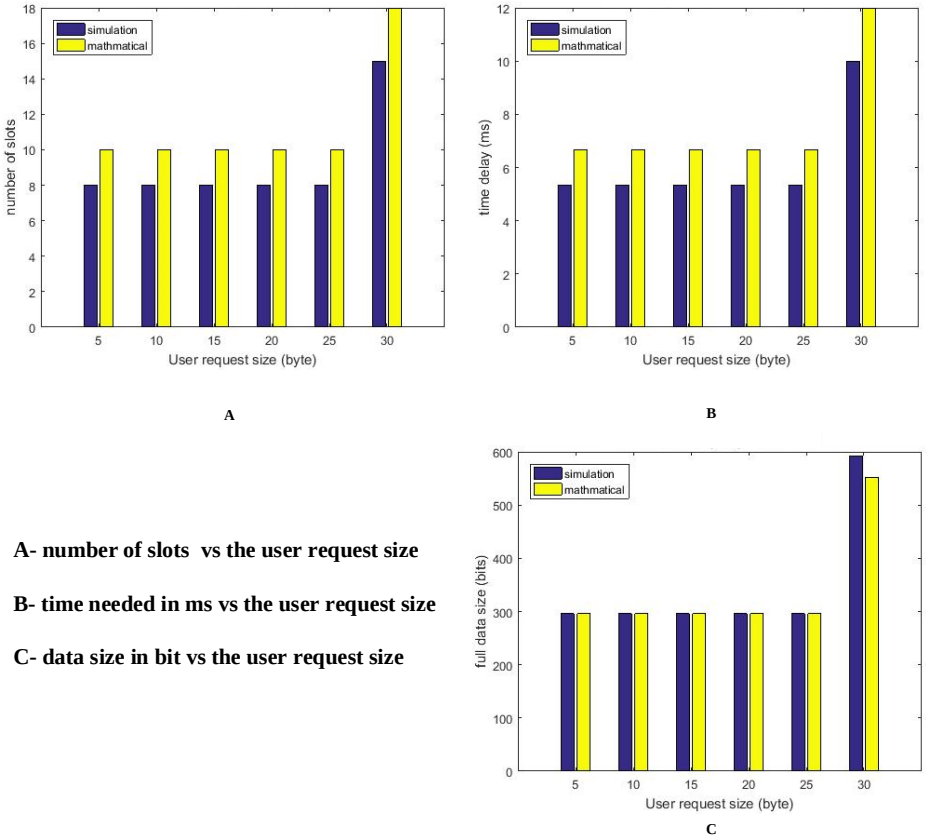


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure B-9 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=64



A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

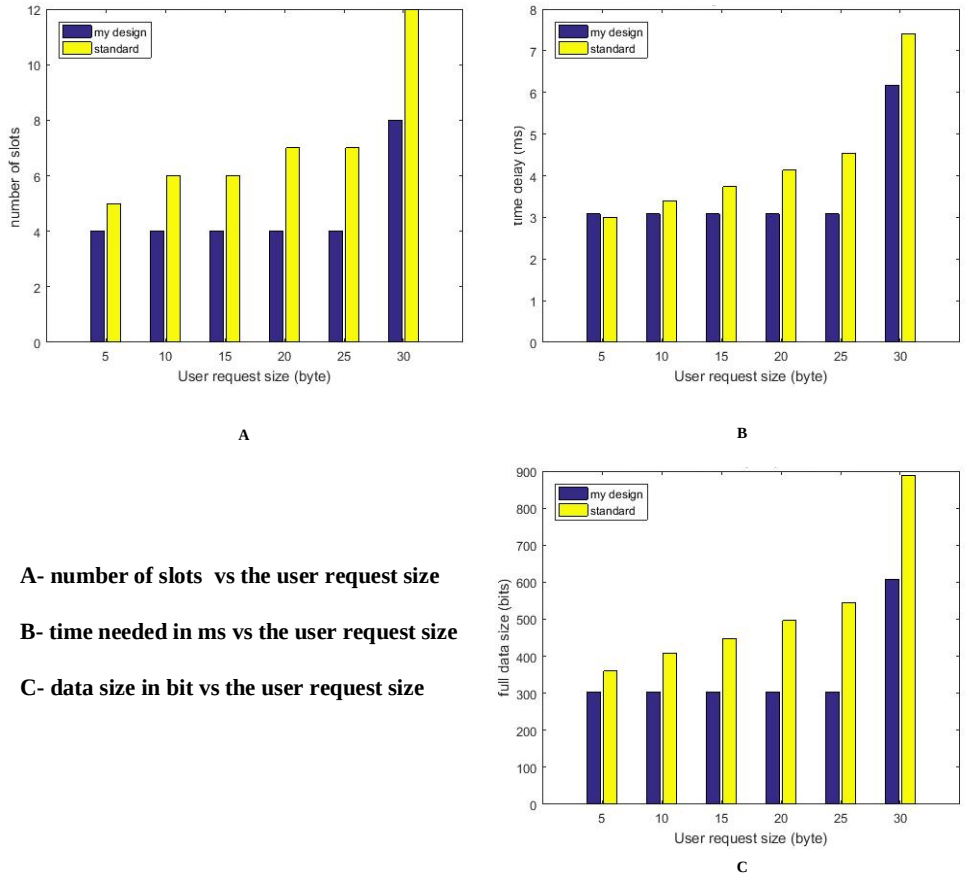
Figure B-10 Comparison Between The Mathematical Results and Simulation Result for Downlink with SF=128

Appendix C: Result Evaluation

This section compares between the results from the proposed design and the results from the other system. The standard system design is taken to be compared with as it is the nearest one to the proposed system design

Uplink

the results shows the evaluation results between the proposed system with the standard system, where the new system design proposed to send the user request using the spare extension of the RACH I the uplink, while the standard sends the spare extension as zeros and use another field in the frame structure to send the user information

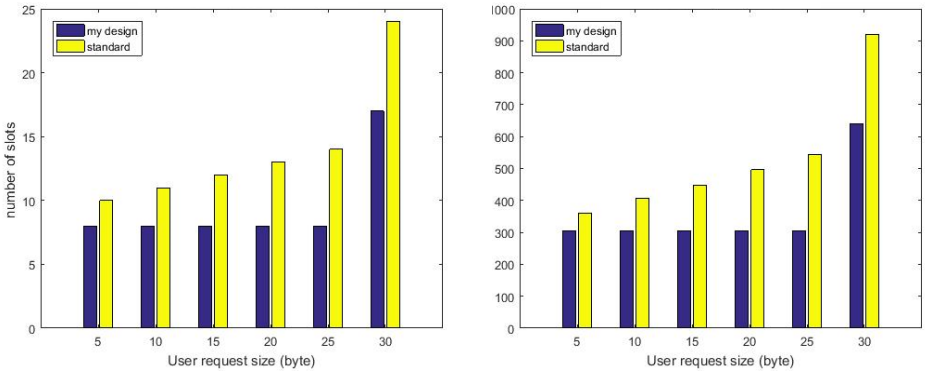


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure C-1 Comparison Between Simulation Results of The Standard and The New Design for Uplink SF= 32



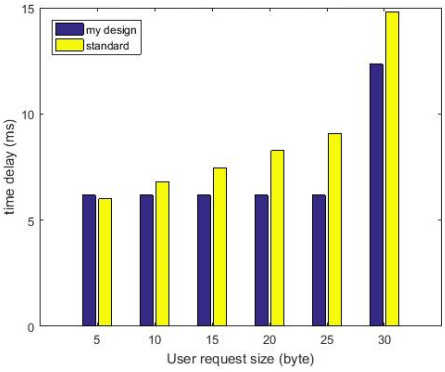
A

B

A- number of slots vs the user request size

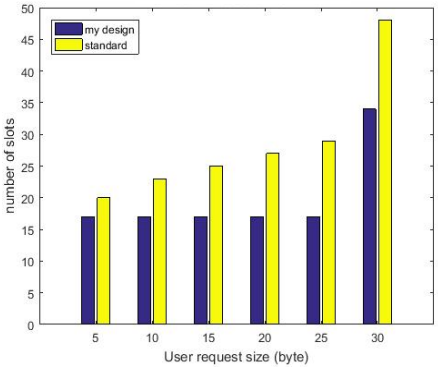
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

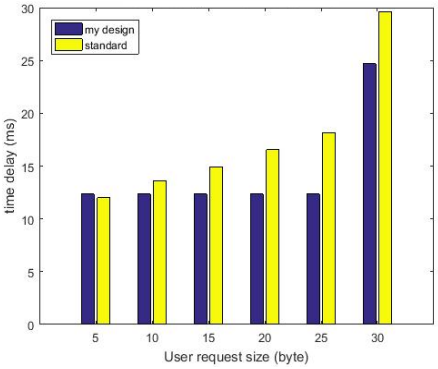


C

Figure C-2 Comparison Between Simulation Results of The Standard and The New Design for Uplink SF= 64



A

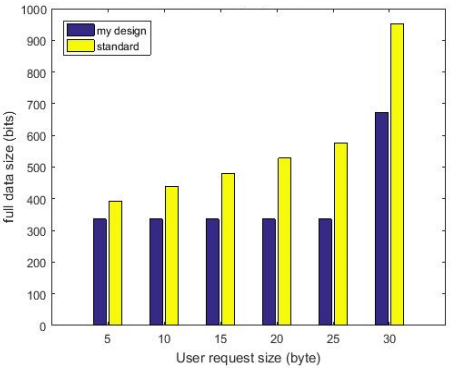


B

A- number of slots vs the user request size

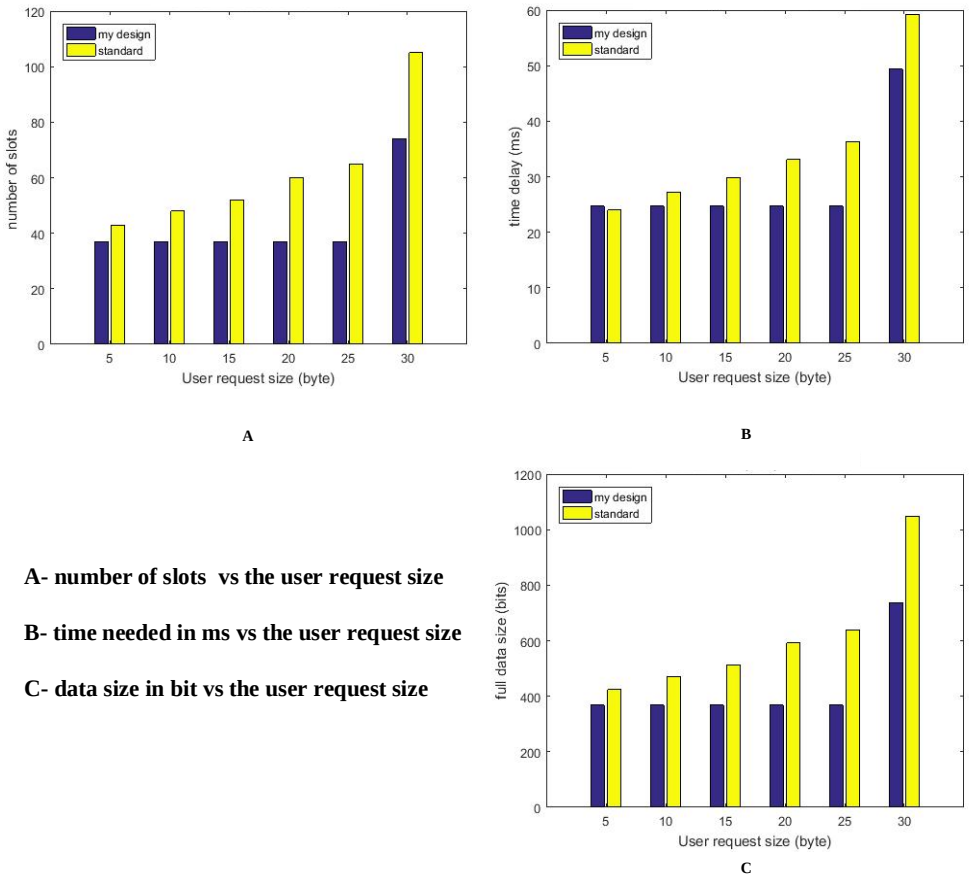
B- time needed in ms vs the user request size

C- data size in bit vs the user request size



C

Figure C-3 Comparison Between Results of The Standard and The New Design for Uplink SF= 128



A- number of slots vs the user request size

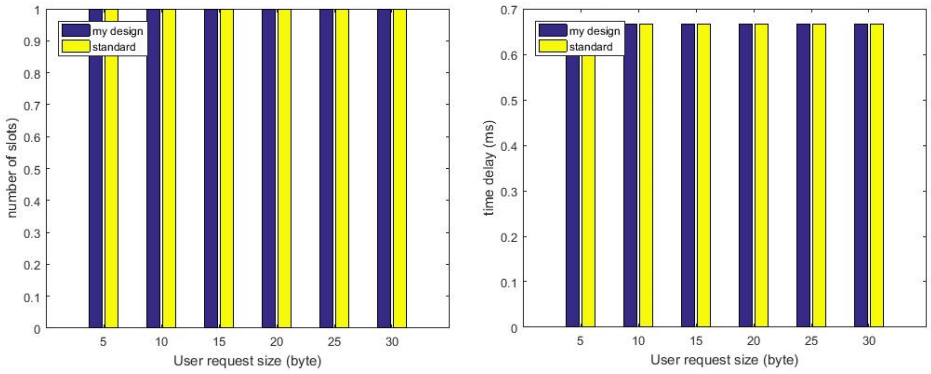
B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure C-4 Comparison Between Results of The Standard and The New Design for Uplink SF= 256

Downlink

A comparison between the simulation result gotten from the proposed system downlink channel using the FACH and the simulation result of the standard to evaluate our system is shown in this section.

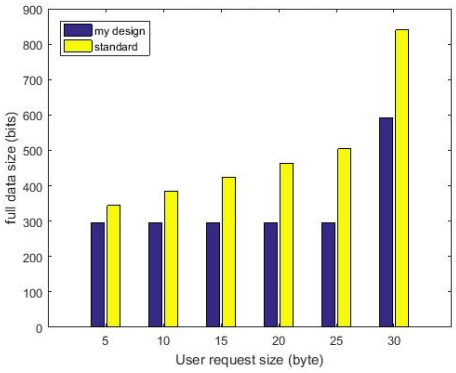


A B

A- number of slots vs the user request size

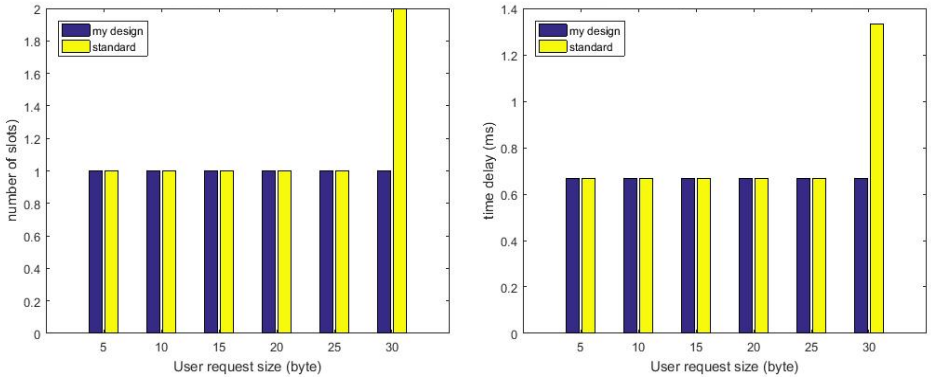
B- time needed in ms vs the user request size

C- data size in bit vs the user request size



C

Figure C-5 Comparison Between Results of The Standard and The New Design for Downlink SF= 4

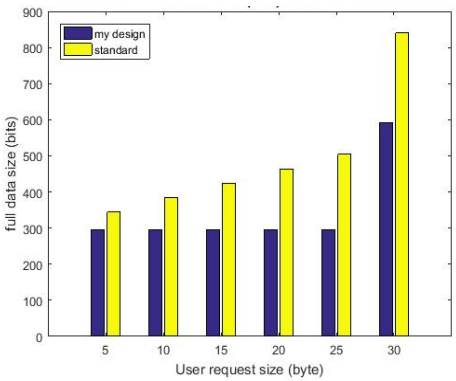


A B

A- number of slots vs the user request size

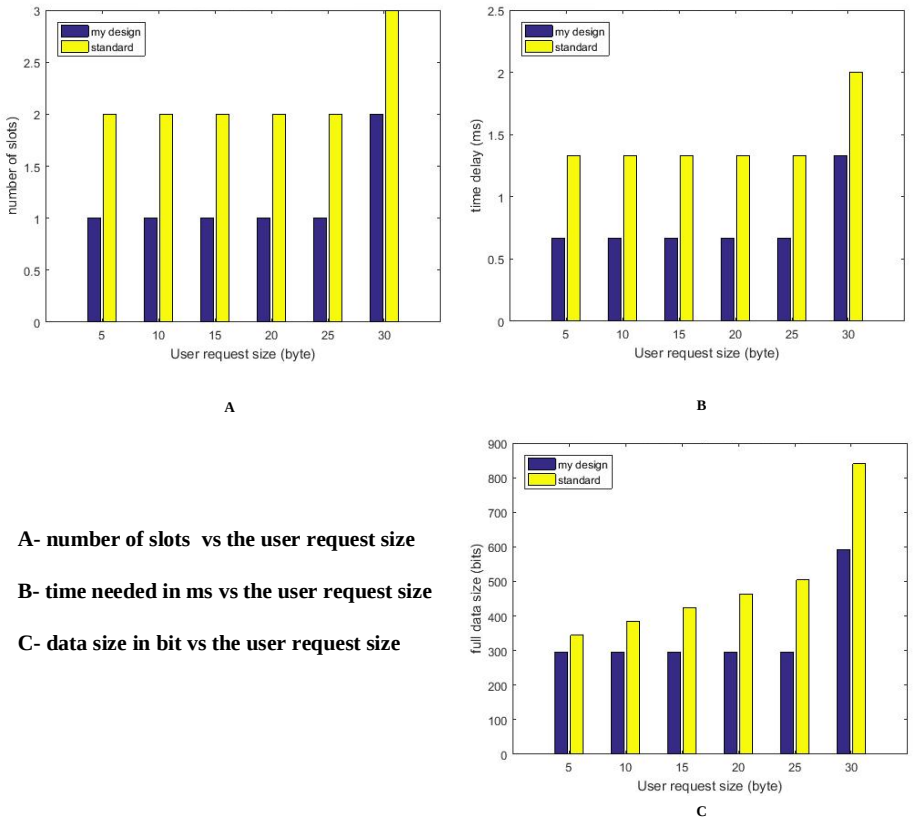
B- time needed in ms vs the user request size

C- data size in bit vs the user request size



C

Figure C-6 Comparison Between Results of The Standard and The New Design for Downlink SF= 8

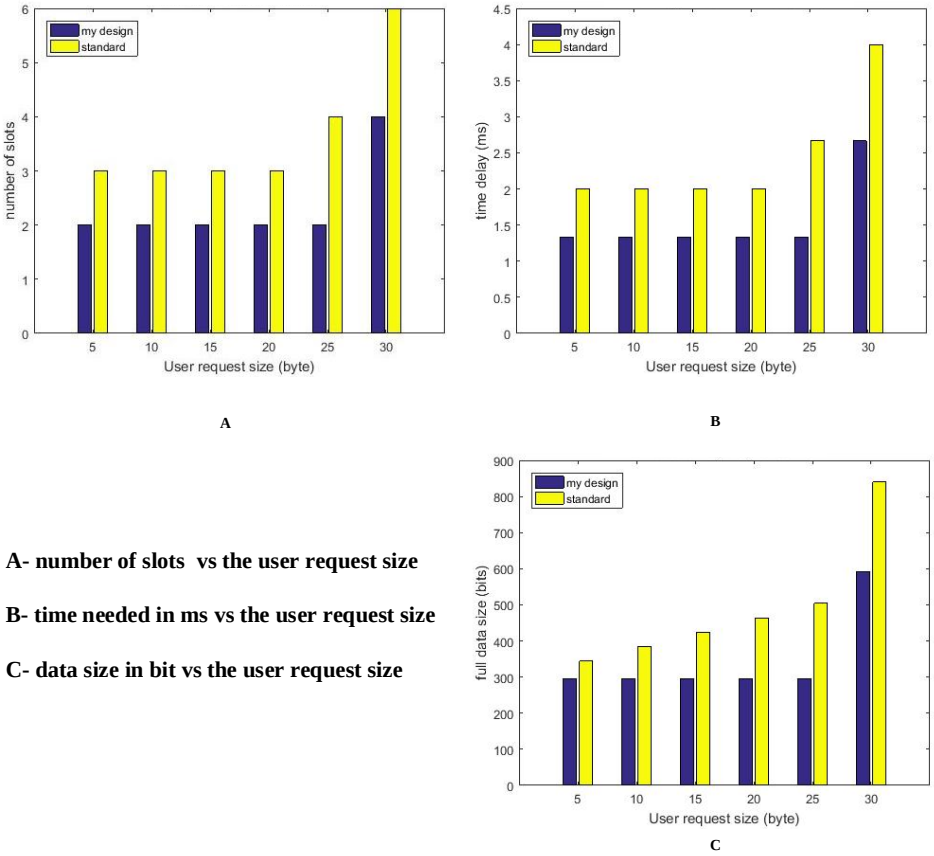


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure C-7 Comparison Between Results of The Standard and The New Design for Downlink SF= 16

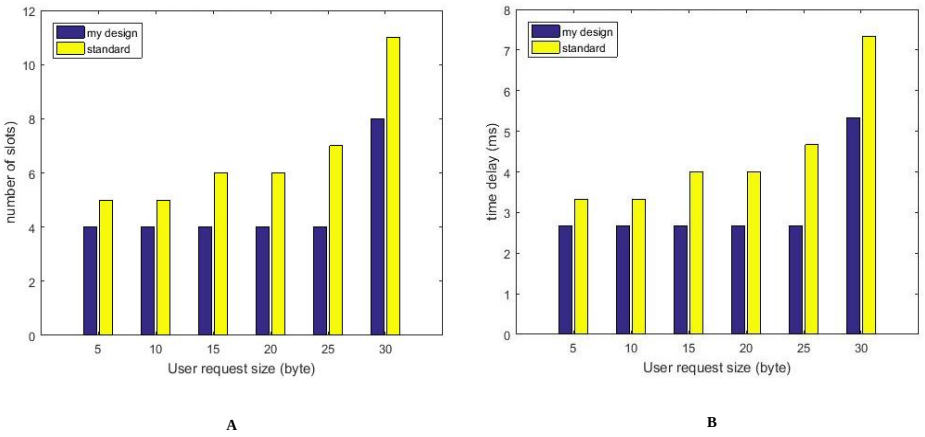


A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

Figure C-8 Comparison Between Results of The Standard and The New Design for Downlink SF= 32



A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

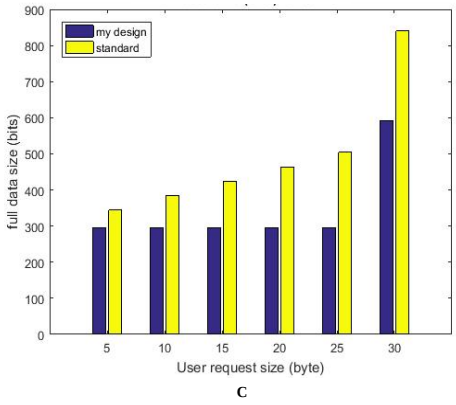
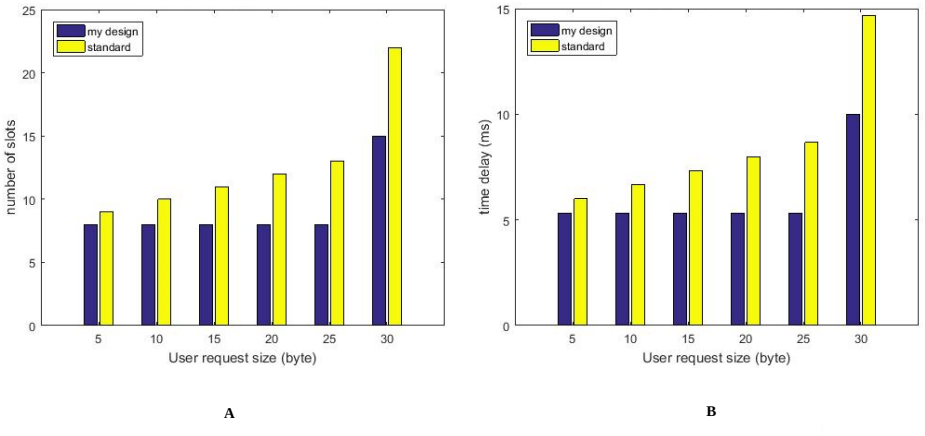


Figure C-9 Comparison Between Results of The Standard and The New Design for Downlink SF= 64



A- number of slots vs the user request size

B- time needed in ms vs the user request size

C- data size in bit vs the user request size

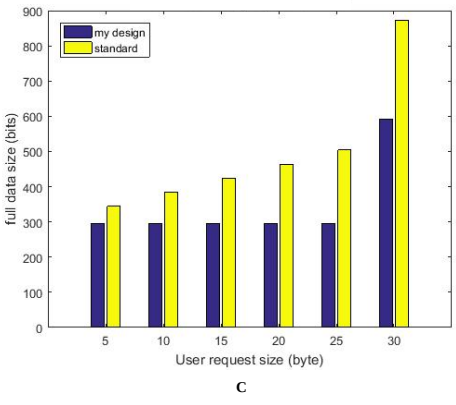


Figure C-10 Comparison Between Results of The Standard and The New Design for Downlink SF= 128