MASTER THESIS

INTEGRATION OF IEC 61850 MMS AND LTE TO SUPPORT REMOTE CONTROL COMMUNICATIONS IN ELECTRICITY DISTRIBUTION GRID

A.D Nguyen

Faculty of Electrical Engineering, Mathematics and Computer Science

Design and Analysis of Communication Systems (DACS) group

SUPERVISORS

Dr. ir. G. Karagiannis

Dr.ir. Geert Heijenk

Prof. dr. ir. Boudewijn Haverkort

Ir. Frans Campfens

UNIVERSITY OF TWENTE.

Abstract

This master thesis investigates on the possibility and impact of integrating the IEC 61850 Manufacturing Message Specification (MMS) protocol over the Long Term Evolution (LTE) network to support the remote control communications in electricity distribution grid. This research includes a literature study of IEC 61850 MMS protocol focusing on its requirements to support remote control communications, and simulation-based experiments to verify the performance of IEC 61850 MMS remote control communication traffic over LTE network.

Within this research, the full stack of MMS communication protocols has been designed and implemented in the NS3 LENA simulation environment together with some popular human-to-human applications (which are considered as background traffics) such as VoIP, video streaming, web browsing…etc. in order to conduct several sets of experiment with different combination of traffic. More importantly, a new LTE QoS-aware packet scheduling strategy has also been designed and implemented to differentiate and assign priority to the mission-critical remote control communication traffic.

Acknowledgement

This is the final project of my two-year Master program in University of Twente, the Netherlands. It was done under the direct supervision of Dr. Ir. G. Karagiannis from Design and Analysis of Communication Systems (DACS) group, University of Twente, and co-supervision of Ir. Frans Campfens, Senior Manager of Innovative Department, Alliander.

I would like to show my highest appreciation to my supervisor, Dr. Ir. G. Karagiannis for his enthusiastic instructions, insightful comments and feedbacks which are all significantly valuable for my research. I am also very thankful for the encouragement and inspiration from Ir. Frans Campfens who gave me plentiful support during the past eleven months. Additionally, I sincerely thank to Dr. Ir. Geert Heijenk and Prof. Dr. Ir. Boudewijn Haverkort for their comments during the starting and mid-term presentations which help me a lot to accomplish this research.

Last but definitely not least, I am very appreciated for my family, who always stays beside me and helps me overcome all the difficulties of an overseas life. Therefore, I would like to dedicate this master thesis research to my family.

Dung Nguyen

Contents

List of figures

List of tables

Acronyms

1xRTT	1 times Radio Transmission Technology
2G	Second Generation
3G	Third Generation
4G	Fourth Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorisation, Accounting
ACK	Acknowledgement
AuC	Authentication Centre
BRCB	BUFFERED-REPORT-CONTROL-BLOCK
BS	Base station
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
DER	Distributed Energy Resource
EIR	Equipment Identity Registrar
EMM	EPS Mobility Management
EPC	Evolved Packet Core
EPRI	Electric Power Research Institute
EPS	Evolved Packet System
ESM	EPS Session Management
EURANE	Enhanced UMTS Radio Access Network Extensions

E-UTRAN	Evolved-UMTS Terrestrial Radio Access Network
EVDO	Evolution Data Optimized
FACT	Flexible Alternating Current Transmission
GOOSE	Generic Object Oriented Substation Events
GRE	Generic Routing Encapsulation
GSE	Generic Substation Event
GSM	Global Systems for Mobile Communications
GSSE	Generic Substation State Event
GTP-U	GPRS Tunnelling Protocol, User Plane
HARQ	Hybrid Automatic Repeat Request
HLR	Home Location Registrar
HSS	Home Subscription Server
HV	High Voltage
IEC	International Electrotechnical Commission
IED	Intelligent Electronics Device
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Sub-system
IMT-2000	International Mobile Telecommunications-2000
IP	Internet Protocol
LD	Logical Device
LN	Logical Node
LTE	Long-term Evolution
LV	Low Voltage
M2M	Machine-to-Machine
MAC	Medium Access Control

Mcps	Megachips per second
MME	Mobility Management Entity
MSC	Mobile Switching Centre
MTC	Machine Type Communication
MV	Medium Voltage
NACK	Negative acknowledgement
NAS	Non-Access Stratum
ns-2	Network Simulator 2
ns-3	Network Simulator 3
PCF	Packet Control Function
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDSN	Packet Data Serving Node
P-GW	Packet Data Network Gateway
PHY	Physical Layer
PUAS	Power Utility Automation System
RLC	Radio Link Control
RLP	Radio Link Protocol
RNC	Radio Network Controller
RRC	Radio Resource Control
SAE	System architecture evolution
S-GW	Serving Gateway
SIP	Session Initiation Protocol

SSL	Secure Socket Layer
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
URCB	UNBUFFERED-REPORT-CONTROL-BLOCK
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Registrar

Chapter 1

Introduction

Smart Grid is considered a future-proof enhancement for the electricity network. The objective of Smart Grid is to generate, transmit and distribute electricity to the customer through the efficient, sustainable, economic and secure power systems. In order to obtain these significant advantages, Smart Grid requires many advantages technologies to enable automatic control between different intelligent systems and devices. In other words, the intelligent electrical systems and devices need to "communicate" with others to balance the electricity generation and consumption as well as to adjust the electrical working parameters so as to keep the power system safe. This cannot be done without the support of a reliable communication network which provides bidirectional communication between different Intelligent Electronics Devices (IED) and systems.

Within Smart Grid, the distribution grid which interconnects the high-voltage transmission grid, the medium-voltage renewable distributed energy resources and the customers plays a key role in Smart Grid. The higher the level of automation and control at distribution grid, the more efficiency the utilisation of electricity in Smart Grid. Currently, distribution control and automation is also an important issue in the development of Smart Grid. Therefore, this research focuses on providing a solution to support remote control and automation in electricity distribution grid.

At application level, there are many communication protocols designed to support communication between smart entities in Smart Grid. However, the large amount of different protocols raised the problem of interoperability. The International Electrotechnical Commission (IEC), as a standard organization for electrical and electronic devices, has introduced many standards to support different applications in different domains within Smart Grid. A core building block is the IEC 61850 standard, which was initially defined for internal substation automation but is now considered a promising standard to support inter-substation, control centre to substations and DERs communications.

IEC 61850 standard defines the models and services to support communications between smart entities in the electricity system at abstract application level. Therefore, these abstract models and services require to be mapped over real protocol stack that supported by a network communication system. At application level the Manufacturing Message Specification (MMS) is chosen as it provides real-time communications services and complex information models that support the mapping of IEC 61850 abstract objects. Another advantage of using MMS is that MMS provides the flexibility by supporting both TCP/IP and OSI communication profiles.

Even though, IEC 61850 MMS is potential candidate for supporting control and automation in distribution grid, there is no published work on this subject at the time this research is conducted. Inheriting the result of the internship project [63] which focused on a very new area of using IEC 61850 MMS for power control in Microgrids, we extends the research to a broader area of distribution grid. In [63] we have specified the method of using IEC 61850 information models and abstract services to perform various power control applications. Moreover, some new logical nodes which model the smart appliances and smart home controllers were also defined to support control communication between the Microgrid controller, Smart Home controllers and Smart appliance controllers. These logical nodes which can be found in [63] can be extended to use in distribution grid to support the control communications between control centre and various intelligent electrical devices.

Realizing the potential of using IEC 61850 MMS to support communications between various entities in electricity network, we propose a solution of using IEC 61850 MMS to support remote control communications in distribution grid. Moreover, due to the critical role of the distribution grid and the spread expansion in geographical area, it is required for the communication infrastructure that supports automation and control functions to be scalable, reliable and secure. With this observation, the so-call four generation (4G) Long Term Evolution (LTE) network is a very potential candidate as it provides high capacity, large coverage, reliability and security. Therefore, the main goal of this research is the integration of IEC 61850 MMS at application level and LTE network infrastructure to support remote control communications in distribution grid.

Because IEC 61850 provides great flexibility for the supporting communication network infrastructure, different communication networks can be used to support IEC 61850 communications in addition to the default-chosen Ethernet. For example, in reference [67], the authors describe the use of Wireless Local Area Network (WLAN) technology to support distribution substation applications. This solution brings the advantages of low installation cost, sufficient data rates, and easy deployment. However, it is not suitable for remote control communications in distribution grid due to the limited coverage of wifi radio. With this observation, we realize that high-speed cellular networks, especially LTE should be optimal choices. Unfortunately, at the time of writing this report, we have not yet found any published researches that provide solution of using cellular networks in general, and LTE in particular, to carry remote control communications traffic. Therefore, we determined to focus on this new researching area with the belief that it will provide an innovative solution in enabling seamless, reliable and secure communications within the future-proof Smart Grid.

This chapter presents a brief introduction about this research. The first section 1.1 describes the problem statement. Section 1.2 gives the research questions which will be answered in the next chapters. The research methodology is given in section 1.3. And finally, section 1.4 covers the structure of this report.

1.1 Problem statement

Due to the initial scope of supporting communications inside substation automation systems, IEC 61850 was defined to be mapped on Ethernet as the layer 2 communication network technology. It is because Ethernet is the dominant technology for Local area network – LAN and it brings significant advantages of high bandwidth and low latency especially with the use of optics fibres at the physical layer. Consequently, Ethernet is very appropriate for substation indoor LAN with applications that require high bandwidth e.g. measurements and time-critical functions such as protection services.

However when IEC 61850 is extended to support large-scale communication networks between substations, control centres to substations and DERs, Ethernet is no longer a good solution. The broadening emergence of DERs, the increasing amount of electric vehicles and smart meters reveals the shortcomings of Ethernet which are high set-up cost and scalability problem due to the use of cable for all connections.

Therefore, it is desired to map IEC 61850 on wide-area wireless network technologies which reduce installation cost by utilizing the existing (public) infrastructure, bringing flexibility and scalability due to the flexible wireless connections to end users and adjustable cell size in cellular networks. The so-called fourth generation Long Term Evolution (LTE) cellular network, seems to be the most potential candidate with advanced technologies to provide wireless connections in wide area, high-capacity, secure and reliable communications.

1.2 Research questions

This research aims to answer the following main research question:

How can remote control communications in electricity distributed grid be supported by using IEC 61850 MMS over LTE?

This main research question is decomposed to three sub-questions so as to step-by-step giving a complete answer for the main question. The sub-questions are:

1) What are the main requirements and challenges of integrating IEC 61850 MMS and LTE to support remote control communications in electricity distribution grid?

This question was partially answered in another literature study. Within this report, the main requirements and challenges will be included in chapter 3.

2) How can the selected challenges be solved?

This question will be answered with a proposed solution to solve the selected challenges. This question is answered in chapter 4 and 5.

3) Can the provided solution to the selected challenges satisfy the performance requirements?

Simulation-based experiments are conducted to analyse the performance of the solution to verify if it can meet the performance requirements imposed by IEC 61850. It is explained in detail in chapter 6.

1.3 Research methodology

This research uses the Waterfall research model [53] to find out the answer for the research questions above. Figure 1.1 illustrates the Waterfall model. The first step is identifying the performance requirements, which is to answer the research question 1. The research methodology used is literature study of the IEC 61850 standard and the remote control communications in distribution grid documents.

From the performance requirements, a solution will be designed to solve the existing challenges. It is the second step in the Waterfall model and the result is the answer for research question 2.

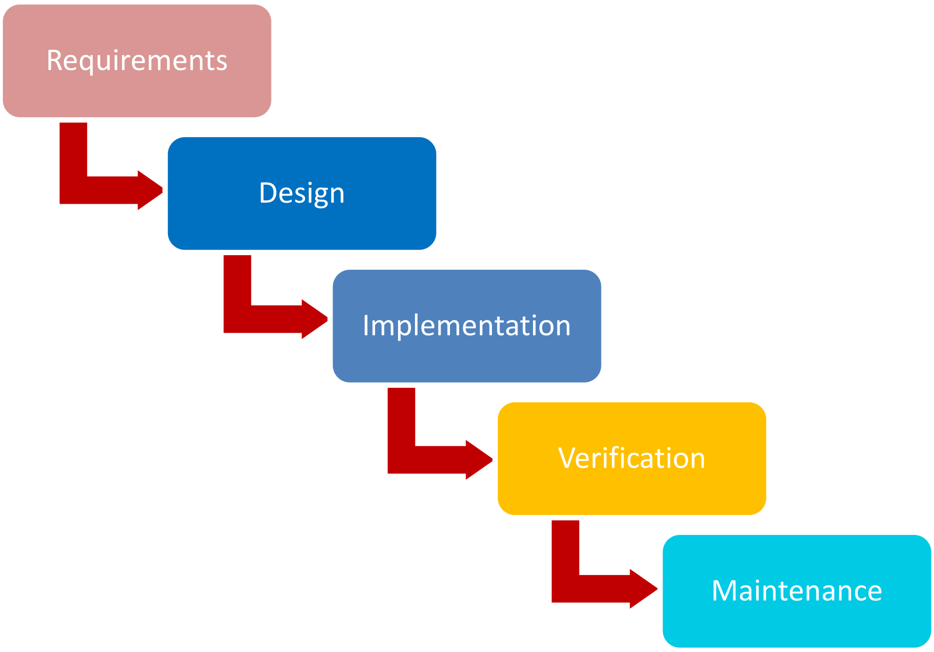


Figure 1.1 – Waterfall research model, copied from [53]

Research question 3 is answered by using the simulation experiment methodology. All the protocol and simulation models needed are designed and implemented in NS3 LENA simulation environment. Then various simulation experiments are conducted in order to verify the performance of the proposed solution and to check if it meets the requirement imposed by IEC 61850.

The solution can be improved and accomplished in the maintenance phase.

1.4 Organisation of the report

The remainder of this report is structured as follows:

Chapter 2 gives a background about Smart Grid, remote control communications in distribution grid, IEC 61850 MMS protocol and LTE network.

Chapter 3 describes the requirements of IEC 61850 and challenges of integrating IEC 61850 MMS and LTE to support remote control communication in electricity distribution grid which answer research question 1.

Chapter 4 describes the specifications and module design required for the simulation experiments. This chapter with chapter 5 answer research question 2.

Chapter 5 presents the simulation models implementation in ns-3 lena, the network topology used in the experiment.

Chapter 6 describes in detail the simulation experiments and evaluations of the simulation results. This chapter provides the answer to research question 3.

Finally there will be a conclusion and future work in chapter 7. Additional information can be found in the documentations listed in the Bibliography

Section 2.1 in chapter 2, section 4.1.1 and section 4.2.1 in chapter 4 and section chapter 5 except section 5.3 and section 5.6 in both the Master thesis reports of T.G. Pham and A.D. Nguyen are exactly the same, since they have been developed and written by both authors of these two reports. The reason of this is that the students focussed on similar research areas, which both requires the literature study of IEC 61850 as the technical background knowledge, the design and implementation of MMS communication protocol stack and LTE background traffics for the experiments.

Chapter 2

Background

This chapter describes research-related concepts and technologies including the IEC 61850 standard, MMS protocol, Smart Grid and the remote control applications in distribution grid, and finally the LTE network.

This chapter is organized as follows: Section 2.1 gives a description of IEC 61850 in general and the MMS protocol in particular. Section 2.2 describes Smart Grid concept and the remote control applications in distribution grid. Then section 2.3 explains how IEC 61850 MMS can support the remote control applications in distribution grid. Finally, section 2.4 presents the technical description of the Long Term Evolution – LTE network.

2.1 Technical description of IEC 61850 MMS

This section provides technical background of the IEC 61850 standard in general and the MMS protocol in particular.

2.1.1 Introduction to IEC 61850

2.1.1.1 Scope of IEC 61850

IEC 61850 was initially designed for communication in substation automation systems by Institute of Electrical and Electronics Engineers – IEEE/Electric Power Research Institute – EPRI Utility Communication Architecture (UCA) and the working group “Substation Control and Protection Interfaces” in the International Electrotechnical Committee (IEC) Technical Committee (TC) 57. The development of advanced and powerful microprocessors supported the possibility for building Power Utility Automation System (PUAS) [1], and consequently several intelligent electronics devices (IEDs) was created each of which support proprietary communication protocol from its manufacturer. However, the co-existing of various proprietary communication protocols led to the big challenge of interoperability, and therefore required investment for complicated and costly protocol converter when using IEDs from different vendors [11].

IEC 61850 was initialized to solve the interoperability problem by defining standard semantics, abstract communication services which can be mapped to different protocols, configuration descriptions and engineering processes [11]. From the original scope of communication within substation automation systems, IEC 61850 standard has been extended to support communication to Distributed Energy Resources (DER) and are being developed for communication to control centres and distribution automation systems domain [11].

Figure 2.1 represents the scope of the standard with updates about the possible extensions for more domains. It shows that at the moment, IEC 61850 protocols can be used to support communications inside substations and from control centres (SCADA – Supervisory Control and Data Acquisition) to the Remote Terminal Units – RTUs and DERs. The standard is going to be extended to support communications between Control centres and Power Utility substation as well as to the Medium Voltage – MV networks.

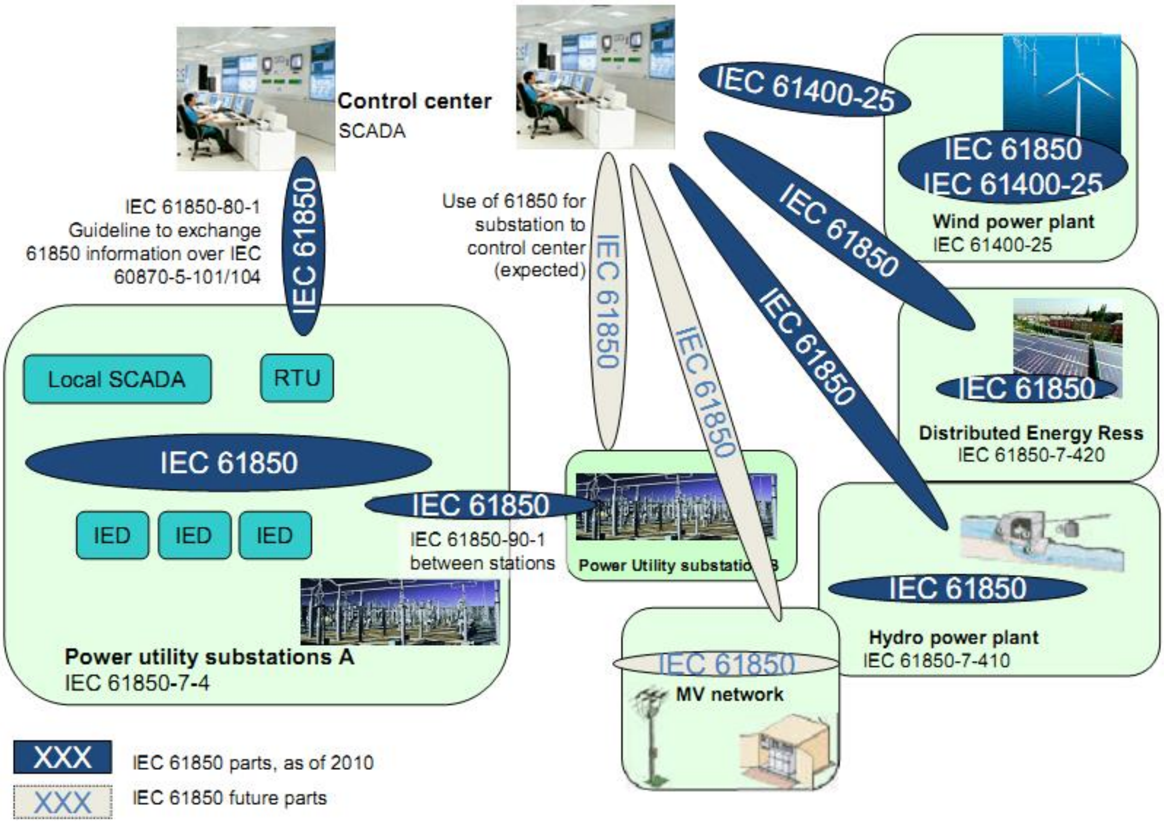


Figure 2.1 – Scope of application of IEC 61850, copied from [11]

IEC 61850 standardizes the communications inside substation automation systems by modelling the physical devices as abstract information objects and defining the abstract services to access and exchange data for power control, monitoring and protection.

2.1.1.2 IEC 61850 data modelling

IEC 61850 data modelling helps to guarantee interoperability between multi-vendor IEDs running IEC 61850 since all the data are modelled following standardized syntax and format in an object-oriented method.

There are two main levels of modelling [11]:

- The breakdown of a real device (physical device) into logical devices.
- The breakdown of logical device into logical nodes, data objects and attributes.

Logical device is the first level of breaking down the functions supported by a physical device i.e. an IED. A logical device usually represents a group of typical automation, protection or other functions [11]. The Logical Device hosts communication access point of IEDs and related communications services and provides information about the physical devices they use as host (nameplate and health) or about external devices that are controlled by the logical device (external equipment nameplate and health).

Logical nodes are the smallest entities decomposed from the application functions and are used to exchange information. It supports the free allocation of those entities on dedicated devices (IEDs). Based on its functionality, a logical node contains a list of data with dedicated data attributes which have a well-structured semantic.

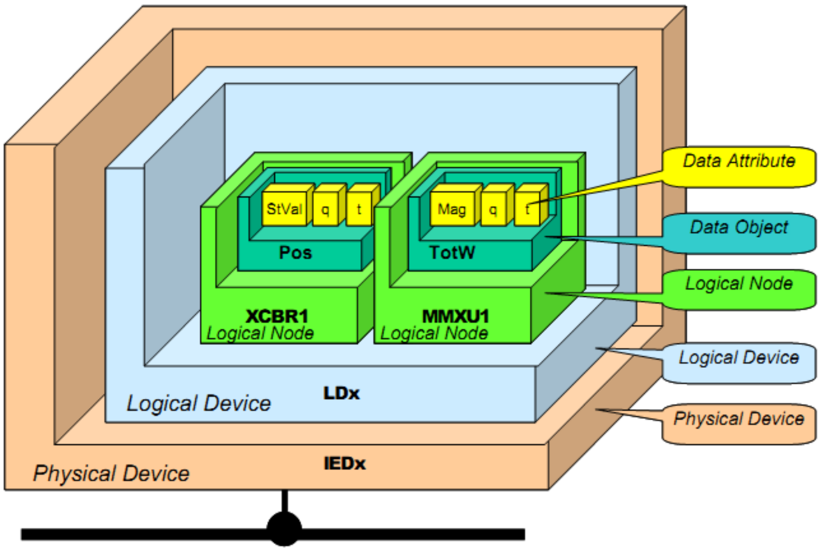


Figure 2.2 – Links between IEC 61850 parts, copied from [11]

Figure 2.2 illustrates the principle of IEC 61850 data modeling. In this case, physical device IEDx is composed of a logical device LDx in which there are two different logical nodes **XCBR** and **MMXU**. XCBR1 and MMXU1 are the instances of the logical node class XCBR and MMXU which represent the circuit breaker and the measurement unit respectively.

Each logical node is composed of many data objects. For example in this situation, logical node XCBR1 contains the data object **Pos** which represents the position of the circuit breaker. This data object consists of many data attributes among which are **StVal** attribute for setting the position of the breaker to open or close, **q** attribute stands for quality of the data and **t** stands for time of operating the function.

2.1.1.3 IEC 61850 communication services

Besides standardizing the data formats in an object-oriented manner, IEC 61850 also defines a set of abstract services for exchanging information among components of a Power Utility Automation System. These services are described in detail in part 7-2 of the standard [4]

The categories of services are as follows [11]:

- retrieving the self-description of a device,
- fast and reliable peer-to-peer exchange of status information (tripping or blocking of functions or devices),
- reporting of any set of data (data attributes), Sequence of Event SoE – cyclic and event triggered,
- logging and retrieving of any set of data (data attributes) – cyclic and event,
- substitution,
- handling and setting of parameter setting groups,
- transmission of sampled values from sensors,
- time synchronization,
- file transfer,
- control devices (operate service),
- Online configuration

The complete Abstract Communication Service Interface – ACSI services are shown in table 2.1. The description of these classes is referred to [19]

Table 2.1 – ACSI classes, copied from [19]

GenServer model GetServerDirectory **Association model** Associate Abort Release **GenLogicalDeviceClass model** GetLogicalDeviceDirectory **GenLogicalNodeClass model** GetLogicalNodeDirectory GetAllDataValues **GenDataObjectClass model** GetDataValues SetDataValues GetDataDirectory GetDataDefinition	**LOG-CONTROL-BLOCK model:** GetLCBValues SetLCBValues QueryLogByTime QueryLogAfter GetLogStatusValues **Generic substation event model – GSE** GOOSE SendGOOSEMessage GetGoReference GetGOOSEElementNumber GetGoCBValues SetGoCBValues **Transmission of sampled values model** **MULTICAST-SAMPLE-VALUE-CONTROL-BLOCK:** SendMSVMessage GetMSVCBValues

DATA-SET model GetDataSetValues SetDataSetValues CreateDataSet DeleteDataSet GetDataSetDirectory **SETTING-GROUP-CONTROL-BLOCK model** SelectActiveSG SelectEditSG SetSGValues ConfirmEditSGValues GetSGValues GetSGCBValues **REPORT-CONTROL-BLOCK and LOG-CONTROL-BLOCK model** **BUFFERED-REPORT-CONTROL-BLOCK:** Report GetBRCBValues SetBRCBValues **UNBUFFERED-REPORT-CONTROL-BLOCK:** Report GetURCBValues SetURCBValues	SetMSVCBValues **UNICAST-SAMPLE-VALUE-CONTROL-BLOCK:** SendUSVMessage GetUSVCBValues SetUSVCBValues **Control model** Select SelectWithValue Cancel Operate CommandTermination TimeActivatedOperate **Time and time synchronization** TimeSynchronization **FILE transfer model** GetFile SetFile DeleteFile GetFileAttributeValues

- **Data Set** – permit grouping of data objects and data attributes
- **Substitution** – support replacement of a process value by another value
- **Setting group control** – defines how to switch from one set of setting values to another one and how to edit setting groups
- **Report control** and **logging** – defines conditions for generating report and log. There are two classes of report control: **BUFFERED-REPORT-CONTROL-BLOCK (BRCB)** and **UNBUFFERED-REPORT-CONTROL-BLOCK (URCB)**. For **BRCB** the internal events that trigger the report will be buffered so that I will not be lost due to transport flow control constraints or loss of connection. For **URCB** internal events issues immediate sending of reports on a "best effort" basis i.e. if no association exits, or if the transport data flow is not fast enough, events may be lost.
- **Control blocks for generic substation event (GSE)** – supports a fast and reliable system-wide distribution of input or output data values; peer-to-peer exchange of IED binary status information, for example, a trip signal.
- **Control block for transmission of sampled values** – fast and cyclic transfer of samples, for example, of instrument transformers.
- **Control** – describes the services to control, for example, a device.

- **Time and time synchronization** – provides the time base for the device and system
- **File system** – defines the exchange of large data blocks such as programs.

For implementation, the abstract services could be mapped on different protocol profiles; the selection of an appropriate mapping depends on the functional and performance requirements. Figure 2.3 shows the communication stack of IEC 61850.

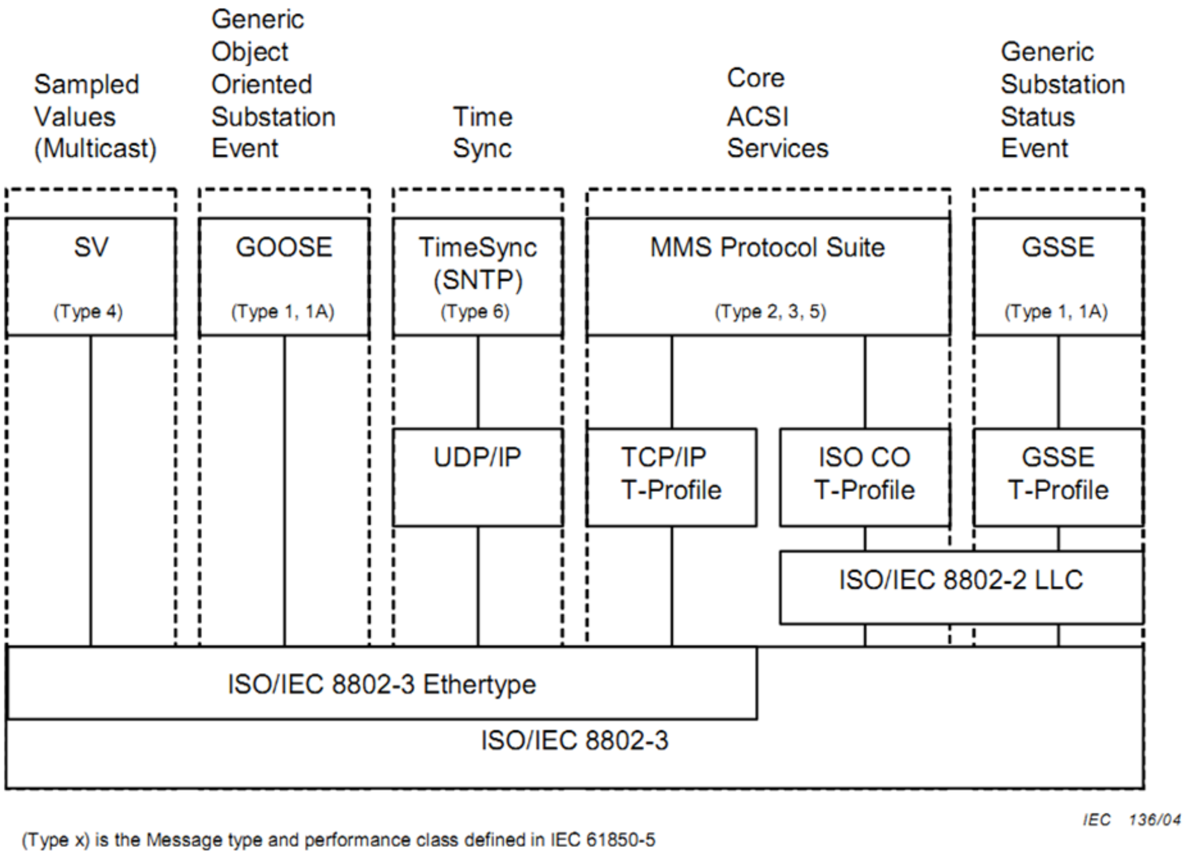


Figure 2.3 – IEC 61850 services mapping to communication profiles, copied from [16]

The Generic Object Oriented Substation Events – GOOSE is defined to support time-critical services such as protection functions and therefore directly mapped to Ethernet to reduce processing time caused by overhead of transport and network layer protocols. The raw message which contains raw measured data such as voltage and current is mapped to Sample Value (SV) which is a protocol designed to carry raw data and is also directly mapped to Ethernet to achieve time-critical performance. The Simple Network Time Protocol (SNTP) is used to support time-synchronization function.

And most importantly, the core ACSI services are mapped to the MMS protocol which supports both TCP/IP and OSI communication profiles at transport layer. The detail regarding this mapping and MMS communication profile will be describing in the next section.

For GOOSE and SV which require the underlying communication infrastructure to support fast messages with maximum transfer time of 10ms, they are defined to map directly on Ethernet to reduce overhead. Table 2.2 shows the communication profile of GOOSE/GSE

Table 2.2 – GOOSE/GSE communication profiles, copied from [16]

OSI model layer	Specification			m/o
	Name	Service specification	Protocol specification	
Application	GSE/GOOSE protocol	See Annex A		m
Presentation	Abstract Syntax	NULL		m
Session				
Transport				
Network				
Link Redundancy	Parallel Redundancy Protocol and High Availability Seamless Ring	IEC 62439-3		o
DataLink	Priority Tagging/ VLAN	IEEE 802.1Q		m
	Carrier Sense Multiple Access with collision detection (CSMA/CD).	ISO/IEC 8802-3:2001		m
Physical (option 1)	10Base-T/100Base-T	ISO/IEC 8802-3:2001		c1
	Interface connector and contact assignments for ISDN Basic Access Interface. [a]	ISO/IEC 8877:1992		
Physical (option 2)	Fibre optic transmission system 100Base-FX	ISO/IEC 8802-3:2001		c1
	Basic Optical Fibre Connector. [b]	IEC 60874-10-1, IEC 60874-10-2 and IEC 60874-10-3		

[a] This is the specification for the 10BaseT connector.

[b] This is the specification for the ST connector.

c1 It is recommended to implement at least one of the two physical interfaces. Additional or future technologies may be used.

Similar to GOOSE, SV is mapped directly to Ethernet. The transmission of sampled value is controlled by the MULTICAST-SAMPLE-VALUE-CONTROL-BLOCK – MSVCB if multicast is used; and by the UNICAST-SAMPLE-VALUE-CONTROL-BLOCK – USVCB if unicast is used. For GOOSE, only the multicast mechanism is applied (see Figure 2.4)

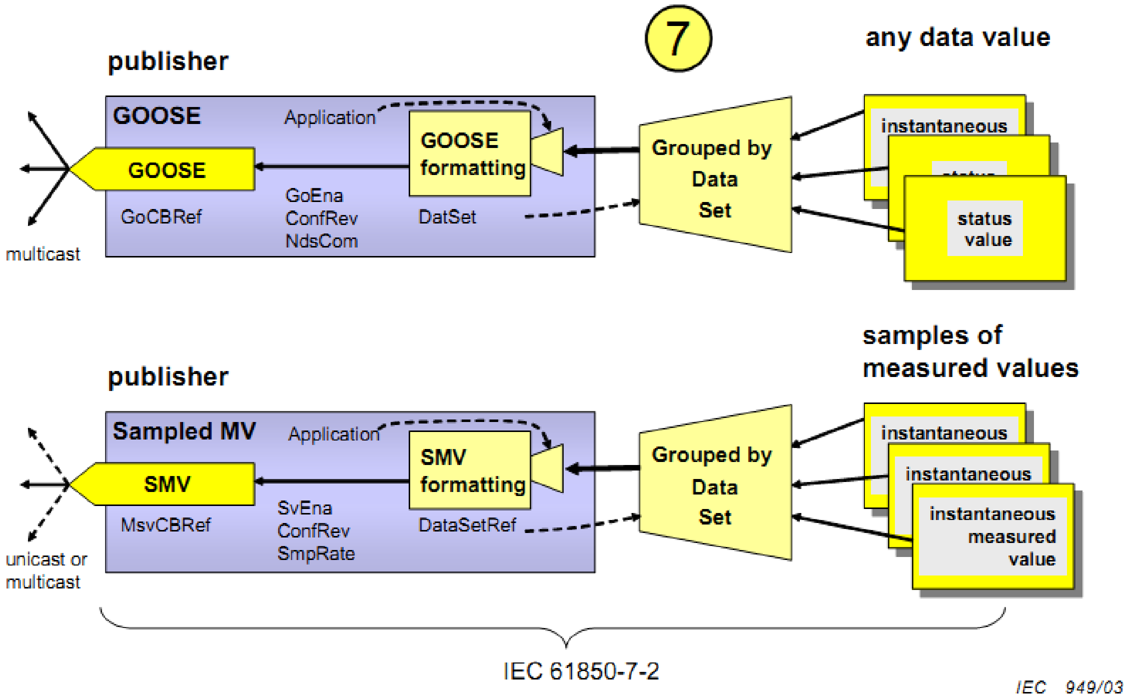


Figure 2.4 – peer-to-peer data value publishing model, copied from [4]

SV can be mapped to Ethernet with different configurations as defined in part 9-1 [20] and part 9-2 [21] of the IEC 61850 series. Part 9-1 maps the Sampled Value to a fixed link with pre-configure Data-set. Part 9-2 provides a more flexible implementation of SMV data transfer by allowing a user-configurable Data-set in which the data values of various sizes and types can be integrated together. Figure 2.5 presents the communication profile of SV

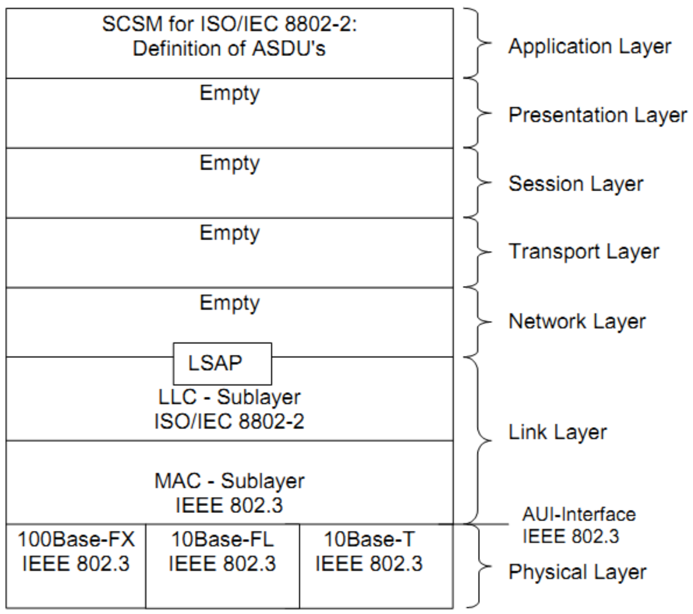


Figure 2. 5 – SV mapped to serial unidirectional multi-drop point to point link, copied from [36]

2.1.2 Manufacturing Message Specification – MMS

MMS is the international standard (International Organisation for Standardization – ISO 9506) designed to support the exchange of real-time data and supervisory control information between network devices and/or computer applications. MMS provides a generic messaging system for communications between heterogeneous industrial devices []. The specification only describes the network visible aspects of communication; therefore, it only specifies the communication between a client and a server, not the internal workings of the entities. With this strategy, MMS allows full flexibility in implementation. To provide this independence, MMS defines a complete communication mechanism between entities composed of []:

- **Objects**: A set of standard objects which must exist in every conformant device on which operations can be executed (these objects can be mapped to IEC 61850 objects).
- **Messages**: A set of standard messages exchanged between a client and a server station for the purpose of controlling these objects.
- **Encoding rules**: A set of encoding rules for these messages describes how values and parameters are mapped to bits and bytes when transmitted.
- **Protocol**: A set of protocols (rules for exchanging messages between devices).

MMS composes a model from the definition of objects, services and behaviour named the Virtual Manufacturing Device (VMD) Model. The VMD model uses an object oriented approach to represent different physical industrial (real) devices in a generic manner []. Figure 2.3 illustrates the communication between a MMS server and a MMS client. The MMS client is the one that sends the request to control the server.

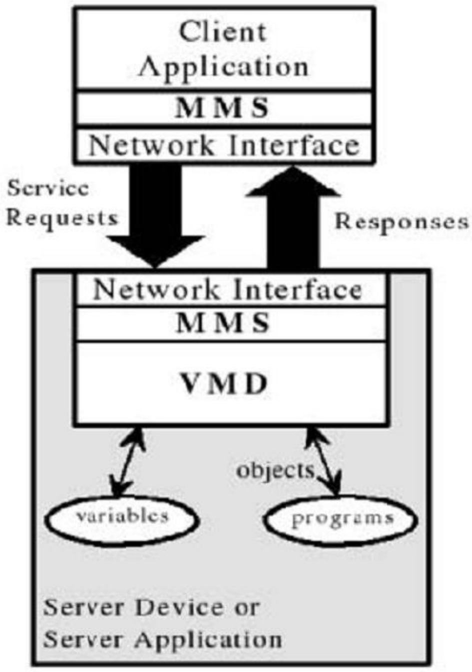


Figure 2.6 – VMD communication model between MMS client and server, copied from [54]

MMS was adopted in IEC 61850 to support the mapping of the core ACSI services. MMS can be mapped to both TCP/IP and OSI communication profiles. Table 2.2 shows the client/server Application profile (A-profile) of MMS.

Table 2. 3 – Services and protocols for client/server communication A-Profile, copied from [16]

OSI model layer	Specification			m/o
	Name	Service specification	Protocol specification	
Application	Manufacturing Message Specification	ISO 9506-1:2003	ISO 9506-2:2003	m
	Association Control Service Element	ISO/IEC 8649:1996	ISO/IEC 8650:1996	m
Presentation	Connection Oriented Presentation	ISO/IEC 8822:1994	ISO/IEC 8823-1:1994	m
	Abstract Syntax	ISO/IEC 8824-1:1999	ISO/IEC 8825-1	m
Session	Connection Oriented Session	ISO/IEC 8326:1996	ISO/IEC 8327-1:1997	m

There are two Transport profiles (T-Profile) that may be used by the client/server A-Profile: TCP/IP or OSI. The TCP/IP T-Profile is shown in Table 2.3.

Table 2. 4 – Services and protocols for client/server TCP/IP T-Profile, copied from [16]

OSI Model Layer	Specification			m/o
	Name	Service specification	Protocol specification	
Communication	Requirement for internet host	RFC 1122		m
Transport	ISO Transport on top of TCP	RFC 1006		m
	Internet Control Message Protocol (ICMP)	RFC 792		m
	Transmission Control Protocol (TCP)	RFC 793		m
Network	Internet Protocol	RFC 791		m
	An Ethernet Address Resolution Protocol (ARP)	RFC 826		m
Link Redundancy	Parallel Redundancy Protocol and High Availability Seamless Ring	IEC 62439-3		o
DataLink	Standard for the transmission of IP datagrams over Ethernet networks	RFC 894		m
	Carrier Sense Multiple Access with collision detection (CSMA/CD)	ISO/IEC 8802-3:2001		m
Physical (option 1)	10Base-T/100Base-T	ISO/IEC 8802-3:2001		c1
	Interface connector and contact assignments for ISDN Basic Access Interface. [a]	ISO/IEC 8877:1992		
Physical (option 2)	Fibre optic transmission system 100Base-FX	ISO/IEC 8802-3:2001		c1
	Basic Optical Fibre Connector. [b]	IEC 60874-10-1, IEC 60874-10-2 and IEC 60874-10-3		

[a] This is the specification for the 10BaseT connector.

[b] This is the specification for the ST connector.

c1 It is recommended to implement at least one of the two Physical interfaces. Additional or future technologies may be used.

It is recommended in IEC 61850-8-2 ed2 [16] that *an implementation that claims conformance to this standard shall implement the TCP/IP profile as a minimum.*

The OSI T-Profile is shown in table 3.16

Table 2.5 – Services and protocols for client/server OSI T-Profile, copied from [16]

OSI Model Layer	Specification			m/o
	Name	Service specification	Protocol specification	
Transport	Connection Oriented Transport	ISO/IEC 8072:1996	ISO/IEC 8073:1997	m
Network	Connectionless Network	ISO/IEC 8348:2002	ISO/IEC 8473-1:1998 ISO/IEC 8473-2:1996	m
	End System to Intermediate System (ES/IS)	ISO/IEC 9542:1988		m
Link Redundancy	Parallel Redundancy Protocol and High Availability Seamless Ring	IEC 62439-3		o
DataLink	Logical Link Control	ISO/IEC 8802-2:1998		m
	Carrier Sense Multiple Access with collision detection (CSMA/CD)	ISO/IEC 8802-3:2001		m
Physical (option 1)	10Base-T/100Base-T	ISO/IEC 8802-3:2001		c1
	Interface connector and contact assignments for ISDN Basic Access Interface. [a]	ISO/IEC 8877:1992		
Physical (option 2)	Fibre optic transmission system 100Base-FX	ISO/IEC 8802-3:2001		c1
	Basic Optical Fibre Connector. [b]	IEC 60874-10-1, IEC 60874-10-2 and IEC 60874-10-3		

[a] This is the specification for the 10BaseT connector.

[b] This is the specification for the ST connector.

c1 It is recommended to implement at least one of the two Physical interfaces. Additional or future technologies may be used.

As TCP/IP is widely implemented in current communication networks, it is preferable to choose the TCP/IP profile. In the current standardized communication profile mapping of IEC 61850 to TCP/IP, Ethernet is used as the layer 2 and 1 protocols as Ethernet is the dominant protocol for Local Area Network (LAN) which is the type of network inside SAS. The advantages of Ethernet are high bandwidth and low latency. However using Ethernet to support remote control communications in distribution grid introduces some disadvantages as described in section 1.1.

Hence this research introduces a new mapping of MMS over the wireless cellular LTE network which is also based on the TCP/IP model. The benefits of mapping MMS over LTE to support remote control communications in distribution grid will be clarified in the next chapters.

2.2 Remote control applications in electricity distribution grid

2.2.1 Introduction of Smart Grid in electricity distribution grid

2.2.1.1 Smart Grid

Traditionally, the electricity grid was built as a centralized control network with the unidirectional power flow from the massive electricity generation like hydro/thermal power plants via the transmission grids and distribution grids to the customers [1]. This centralized control network was suitable with the clear separation between customers who were almost pure consumers and the massive power plants which generated all electricity for both domestic and industrial demands.

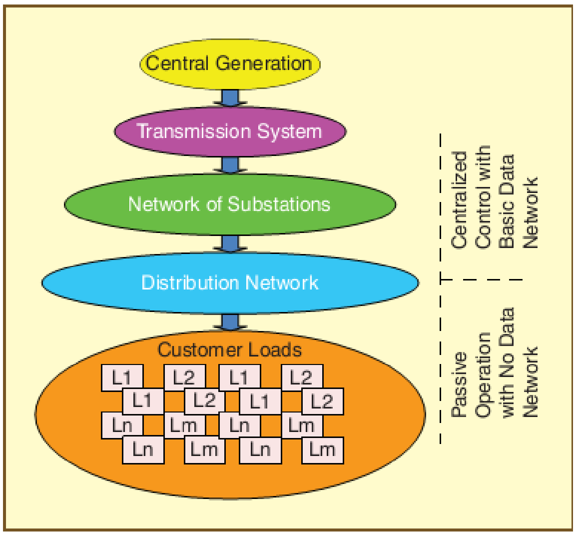


Figure 2.7 – Traditional electricity grid, copied from [2]

Figure 2.4 illustrates the architecture of a traditional centralized energy network. Electricity is only produced at the Central Generation and then will be transferred and distributed through the transmission and distribution networks to the customers. The flow of energy is one directional; therefore, the information control flow is also one way needed from the centralized control centres to the transmission/substations/distribution networks. This network architecture relied on the supply of electricity from the traditional energy resources such as gas, oil and coal.

However, the traditional energy resources such as gas, oil and coal are non-renewable. The massive electricity production has led to a global decline of gas, oil and other natural resources. The rapid development of many developing countries alongside with the population explosion led to the severe energy shortages in the late of 20th century. More importantly using these energy resources has led to seriously negative effects on human like including CO_2 pollution, global warming, climate change and etc. For example, the climate change caused more than 36 million of displacement and evacuation in 2008 according to United Nations Office for the Coordination of Humanitarian Affairs and the Internal Displace ment Monitoring Centre [3] (see figure 2.5).

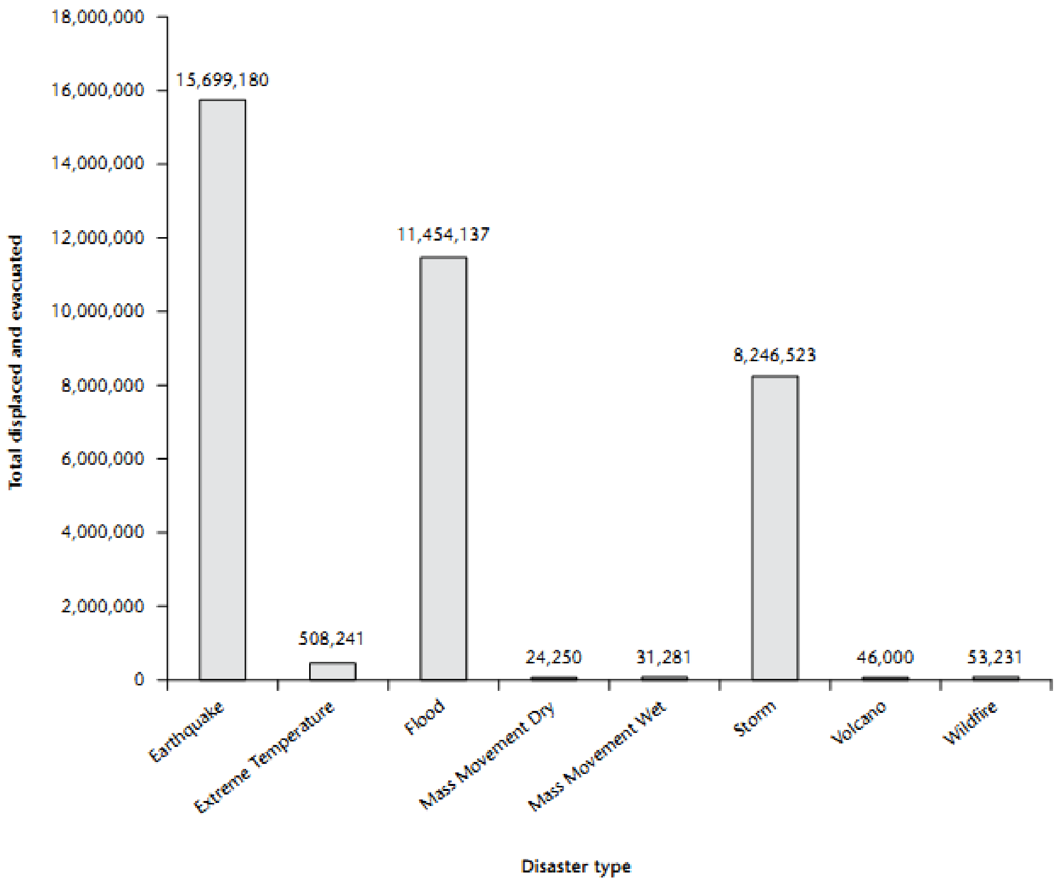


Figure 2.8 – Total displaced and evacuated in 2008 by disaster type, copied from [3]

This traditional infrastructure of electricity grid in Figure 2.4 has existed for several decades, and cannot cope with the emerging challenges nowadays. For example, the European 20-20-20 targets [4] aim to reduce Green House gas emission by 20% by 2020, and 80% by 2050, increase share of renewables in EU energy consumption to 20%, and achieve an energy-efficiency target of 20%. In order to meet these targets, more use of Distributed Energy Resources (DERs) that run on renewable energy such as solar or wind has to be integrated, which poses problems for the grid.

More electric vehicles will be used as they are environmentally friendly, but using them widely brings new challenges and also requires the evolution of the grid. These challenges together with other factors, such as the need for higher resiliency against failures, better security and protection, etc. are driving the grid towards a modernized infrastructure and bring new benefits to both utilities and customers. This modernized grid is often termed as "Smart Grid", "IntelliGrid", "GridWise", etc. [5], [6]. According to the Electric Power Research Institute's (EPRI) [7],

According to European Technology Platform Smart Grid, the definition of Smart grid is [1]:

A Smart Grid is an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies.

The key characteristic of Smart Grid is the two-way information exchange made possible by communication networks, which is the key enabler for future smart applications to be built [2]

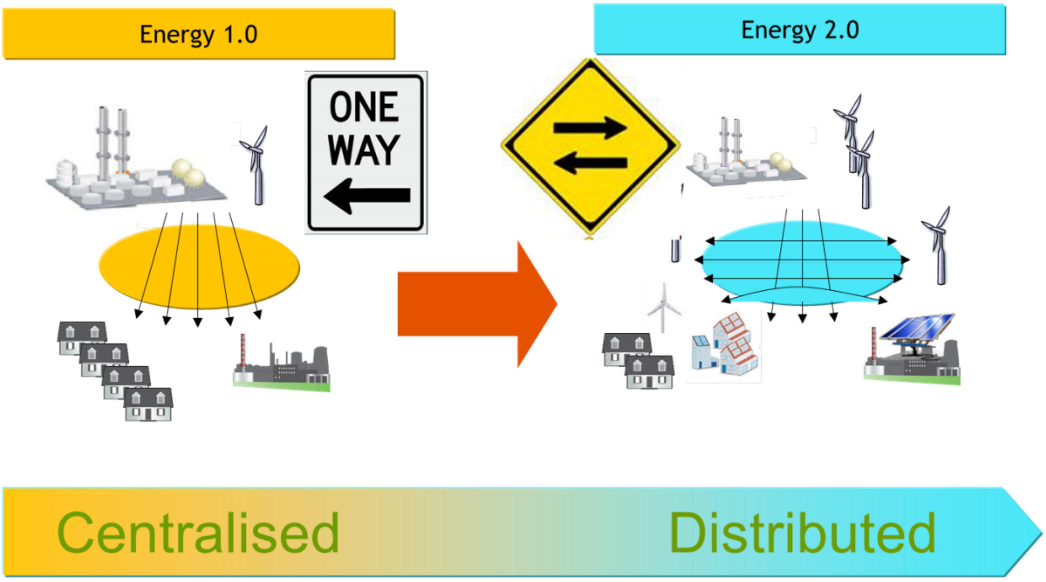


Figure 2.9 – Transformation from traditional to future electricity grid, copied from [8]

Figure 2.6 shows the evolution from the traditional centralised electricity network to the distributed-intelligent electricity network or Smart Grid. As we can see, Smart Grid requires a complex communication network to allow communications between different actors such as from power plants and DERs to customers and between DERs.

Figure 2.7 describes the architecture of the Smart Grid. It consists of the smart elements from customer / prosumer such as smart consumption which enable demand response or home automation systems, building automation systems, to bulk generation with increased use of power electronics and power grid (Transmission and Distribution) including substation automation systems, power monitoring system, energy management system, asset management system and condition monitoring, distribution automation and protection [1].

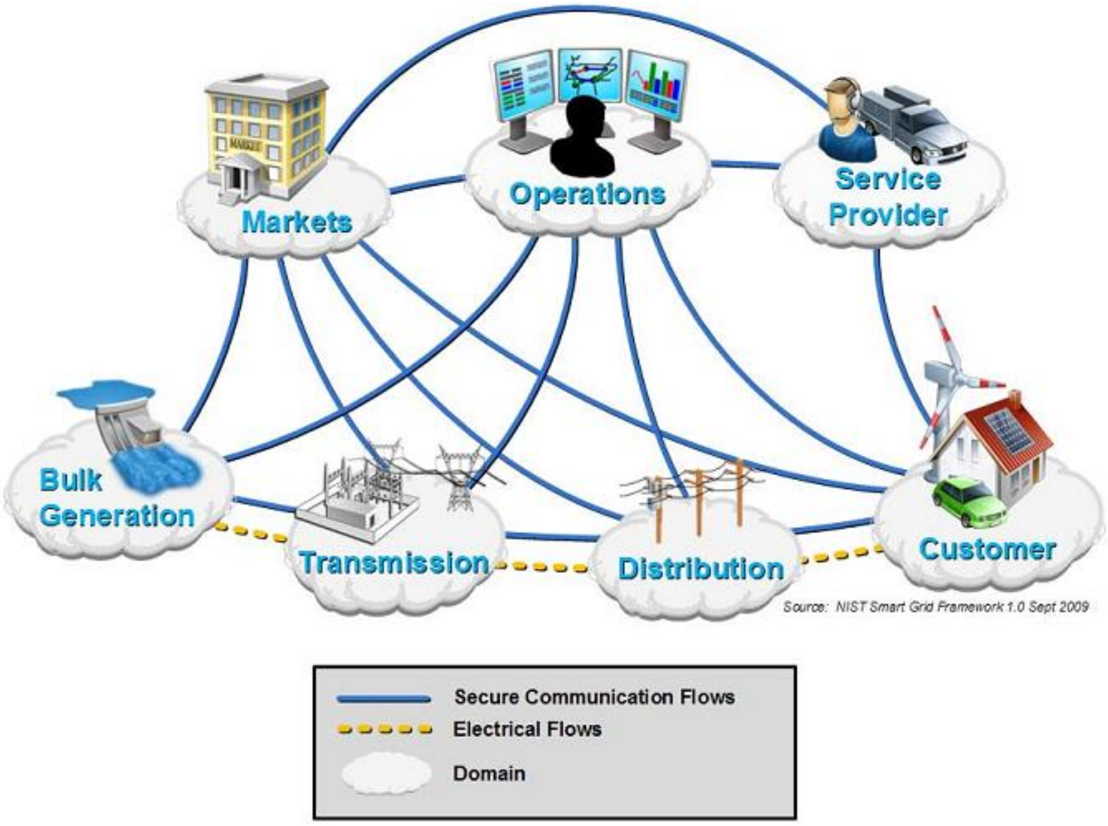


Figure 2.10 – Conceptual model of smart grid, copied from [1]

In this figure we can see there are many communication flows from the controlling parts (markets, operations and services providers) to electricity generations and loads as well as communication among controlling systems and transmission/distribution grid to bulk generation and customer. These communication flows are used to implement various functions such as power monitoring, energy management, distribution automation and functions…etc. to achieve the goal of delivering electricity sustainably, reliably, and securely from different power supplies to consumers.

2.2.1.2 Smart Grid distribution network

The distribution domain distributes the electricity to and from the end customer in the Smart Grid [9]. Therefore, the scope of distribution network as can be seen in Figure 2.6 is the transfer of electricity from the high voltage (HV) transmission grid to the customer.

The distribution network connects smart meters and all intelligent field devices, managing and controlling them through a bidirectional communication network [9]. It can be seen in figure 2.8 that the distribution network is mainly the medium voltage (MV) network, the secondary transformer substations which transform the electricity from MV to Low voltage (LV) and vice versa, and LV distribution power lines to the customers.

The distribution system is typically remotely controlled and supervised by a distribution system operator. The information will be exchanged between the Distribution Management System (DMS), which is the control centre for distribution grid, and the secondary substations and distribution energy generation resources.

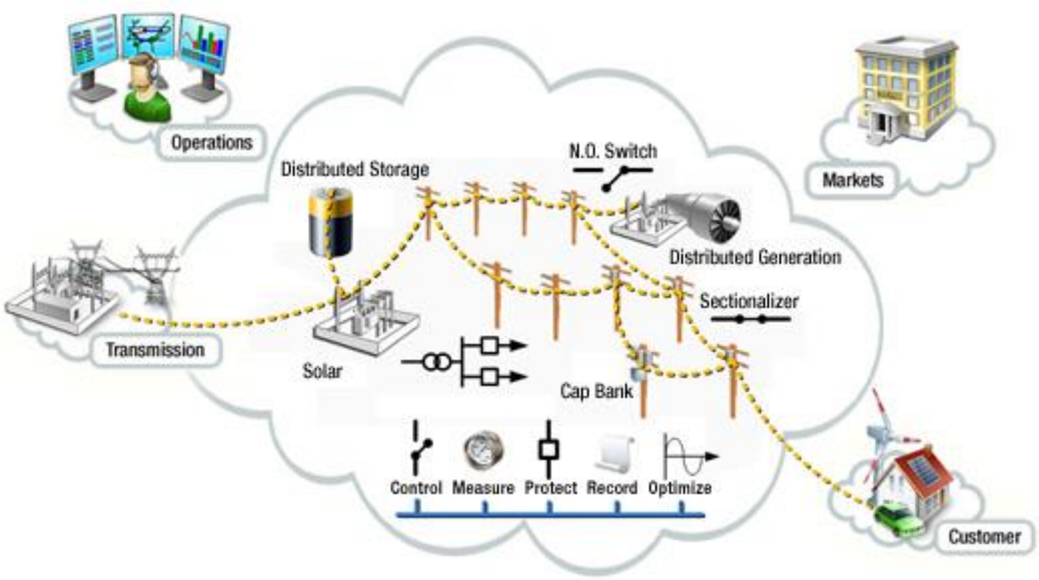


Figure 2.11 – Distribution electricity network, copied from [9]

The increasing integration of Distributed Energy Resources (DERs) such as photovoltaic systems at low-voltage level and wind generators at medium-voltage level cause voltage quality problems such as the voltage magnitude in some areas is much higher than the acceptable maximum level. Therefore, the telecontrol and supervision of secondary substations and transformer houses is crucial. The information exchanged between those components and the distribution control centre should be based on common protocols [1].

The technical committee TC 57 within IEC which is responsible for development of standards for information exchange for power system has defined the reference architecture consisting of the communication standards for power intersystem and subsystem communications as illustrated in figure 2.6.

The international standards for telecontrol communications are basically the two standardized protocol stacks [1]:

- *IEC 60870-5, Telecontrol equipment and systems*
  - IEC 60870-5-101, Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks
  - IEC 60870-5-103, Telecontrol equipment and systems - Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment

- IEC 60870-5-104, Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles

➢ *IEC 61850 Communication networks and systems for power utility automation*

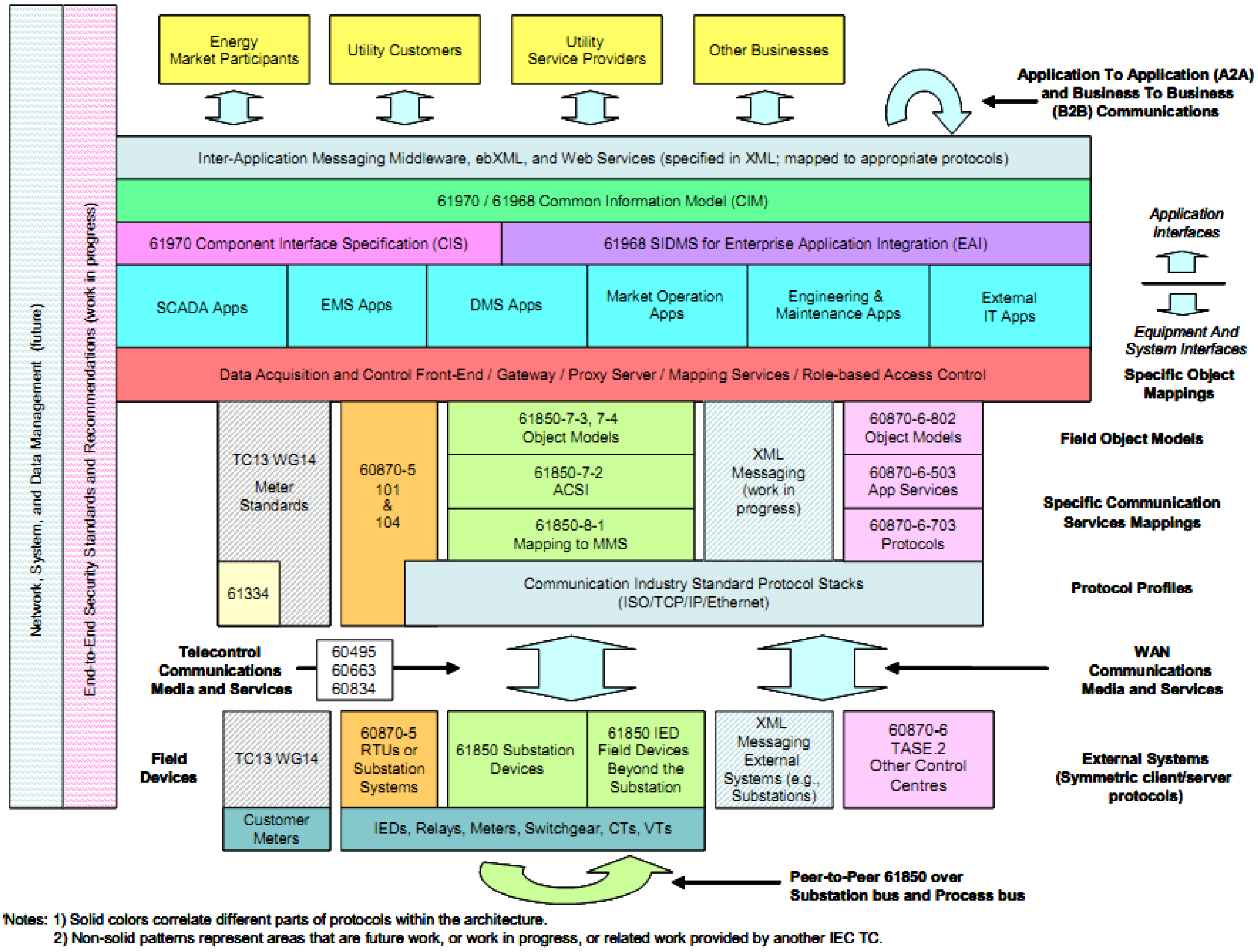


Figure 2.12 – Current TC 57 reference architecture, copied from [1]

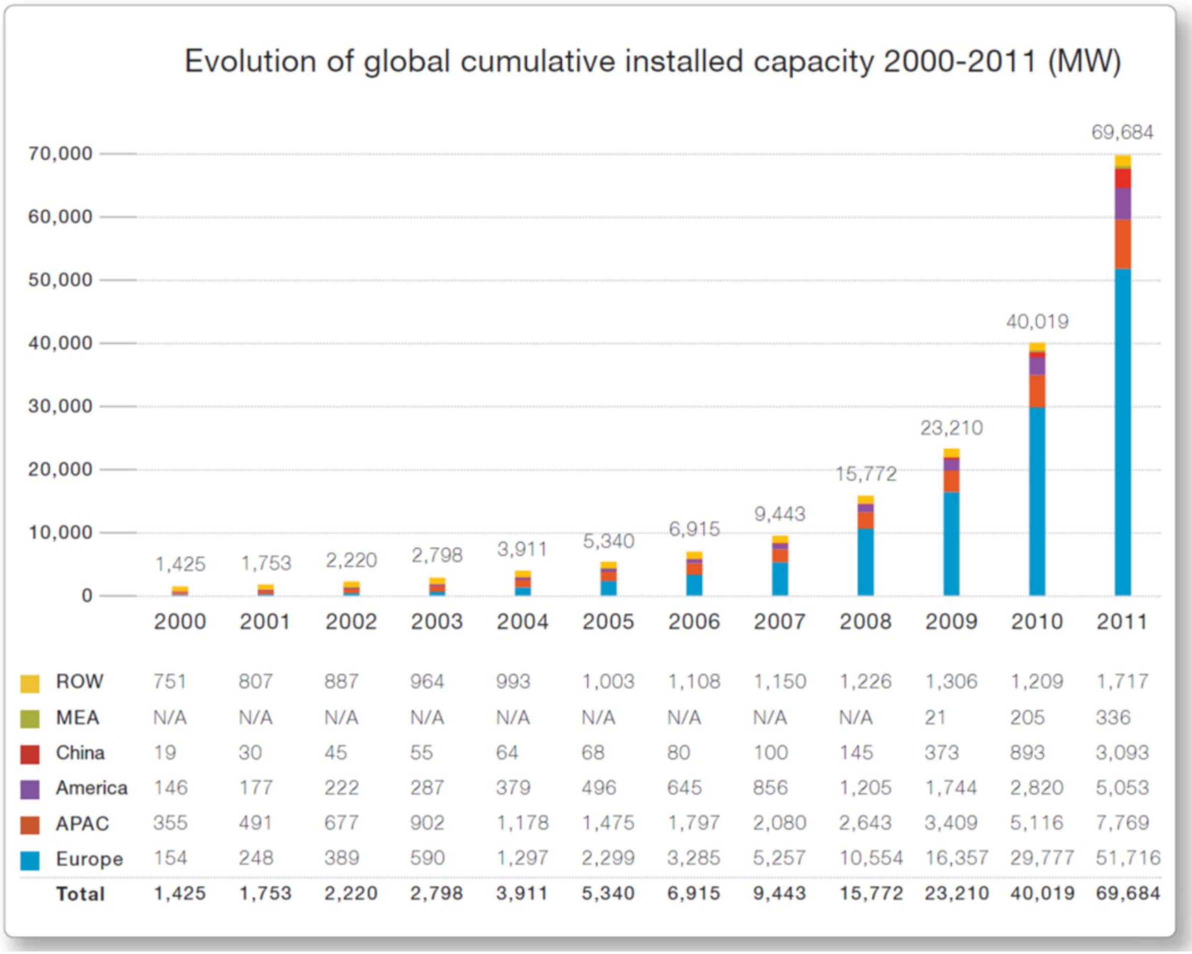
IEC 60870-5 had been defined for telecontrol in distribution automation systems before IEC 61850 was created with the initial scope of supporting communications within substation automation systems.

However, the success of IEC 61850 with object oriented architecture which allows it to provide comprehensive and accurate information models for various components in distribution systems [10], has paved the way for extensions of using IEC 61850 to support inter-substation, control centres to substations and DERs communications. Moreover, using IEC 61850 for distribution automation will eliminate the necessity of building protocol converters between substation automation systems and distribution communication networks.

A more detailed background about IEC 61850 and its capacity to be applied in distribution automation systems will be described in the next sections.

2.2.2 Remote control applications

As described in section 2.2.1, the use of DER becomes indispensible since the traditional energy resources have become more and more limited as well as they also caused many environmental problems. Figure 2.10 shows the exponential increase of PV capacity in the world and especially in Europe where renewable energy becoming more and more important.



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
ROW	751	807	887	964	993	1,003	1,108	1,150	1,226	1,306	1,209	1,717
MEA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	21	205	336
China	19	30	45	55	64	68	80	100	145	373	893	3,093
America	146	177	222	287	379	496	645	856	1,205	1,744	2,820	5,053
APAC	355	491	677	902	1,178	1,475	1,797	2,080	2,643	3,409	5,116	7,769
Europe	154	248	389	590	1,297	2,299	3,285	5,257	10,554	16,357	29,777	51,716
Total	**1,425**	**1,753**	**2,220**	**2,798**	**3,911**	**5,340**	**6,915**	**9,443**	**15,772**	**23,210**	**40,019**	**69,684**

Figure 2.13 – Evolution of the cumulative installed PV capacity, copied from [55]

The integration of DER can result in various challenges for network planning and operation. On one hand, changing power flows due to large shares of distribution generation in the low and medium voltage networks will affect the voltages, which can result in voltages violating the operational steady-state maximum and minimum voltage limits. On the other hand, the capacity of DER generation highly exceeds the load already today in some distribution networks, e.g. in Southern Germany. The ratings of the network components are not designed for these high power flows feeding back into the overlaying network. Thus overloading of cables, overhead lines and distribution transformers can be a serious problem resulting in large investments, which are necessary to strengthen the networks and to ensure security of supply [55]. Therefore, the DER-control applications are required to limit the impact of DER generation on the network components while still maximize the use of DER. Some applications are [55]:

- Demand side management, controlled generation, electrical vehicle or distributed storage devices to locally balance load and generation and to control the power exchange with the connected Medium Voltage (MV) and High Voltage (HV) networks.
- Controlling the amount of power injected by DER.
- Replacing and installation of active components to control the voltage in the distribution network. These components can be for example controllable reactive power from converters of generation sources, regulated distribution transformers, MV power electronics, booster transformers, energy storage devices, etc.

Moreover, As Smart Grid capabilities, such as smart metering, demand side management, demand response, or the integration of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system [55].

This research focuses on the real-time remote control communication between the control centres and the distributed energy generation and storage to balance the electricity generation and consumption, and to stabilize the voltage in order to ensure safety of the distribution grid.

2.3 Use of IEC 61850 over MMS to support remote control applications

2.3.1 IEC 61850 for communications in distribution electricity network

IEC 61850 is a highly dynamic standard and is still under development with new technical reports explain its new application areas. These developing technical reports focus on the use of IEC 61850 in distribution electricity network, for example, the technical report IEC 61850-90-6 is for explaining the use of IEC 61850 for distribution automation systems. Another developing technical reports are IEC 61850-90-2 for communication between substations and control centre – IEC 61850-90-2 [12], or IEC 61850-90-5 [13] for transmission of synchrophasor information which can be used for wide area monitoring and control.

In the table 2.2 provided by IEC in [1], IEC 61850 is considered a core standard which can cover all the domain of substation automation systems, distribution automation and distribution management systems, and energy storage. It proves the feasibility of using IEC 61850 to support control services in distribution electricity network.

Table 2.6 – Overview of IEC standards, copied from [1]

	HVDC/FACTS	Blackout Prevention / EMS	DMS	Distribution Automation	Substation Automation	DER	AMI	DR	Smart Home	Electric Storage	Electromobility	Relevance for Smart Grid
SOA – IEC 62357		x	x									Core
CIM – IEC 61970-301		x	x	x	x	x	x	x		x		Core
ISO/IEC 14543									x			Low
ISO/IEC 27001									x			Low
IEC 60255			x	x	x							Low
IEC 60364						x			x			Medium
IEC 60495							x		x			Low
IEC 60633	x											Low
IEC 60834		x	x		x							Low
IEC 60870-5		x	x	x	x							High
IEC 60870-6		x	x									High
IEC 60904						x		x	x			Medium
IEC/TR 61000						x	x		x	x	x	Low
IEC/TS 61085												
IEC 61140									x		x	Medium
IEC/TR 61158 / 61784					x							Medium
IEC/TR 61334							x					High
IEC 61400		x	x			x						High
IEC 61508												
IEC 61850		x	x	x	x	x	x			x	x	Core
IEC 61850-7-410		x	x	x	x	x						High
IEC 61850-7-420			x	x	x	x						High
IEC 61851									x		x	High
IEC 61869				x	x							Medium
IEC 61954	x											Low
IEC 61968			x			x	x	x				Core
IEC 61970		x	x		x							Core
IEC 61982											x	Low
IEC 62051-54 / 58-59			x			x	x	x	x	x	x	High
IEC 62056			x			x	x	x	x	x	x	High

2.3.2 IEC 61850 abstract services for control functions

As shown in section 2.2.3, IEC 61850 defines multiple abstract services class to access the data objects. For control functions in SAS, IEC 61850 provides the **Control model** with different services to change the state of internal and external process by a client [19].

The **Control model** is based on the client/service mechanism in which the client who initiated the two-party application association can send the control request and the server who accepted the association will respond to that operation control request.

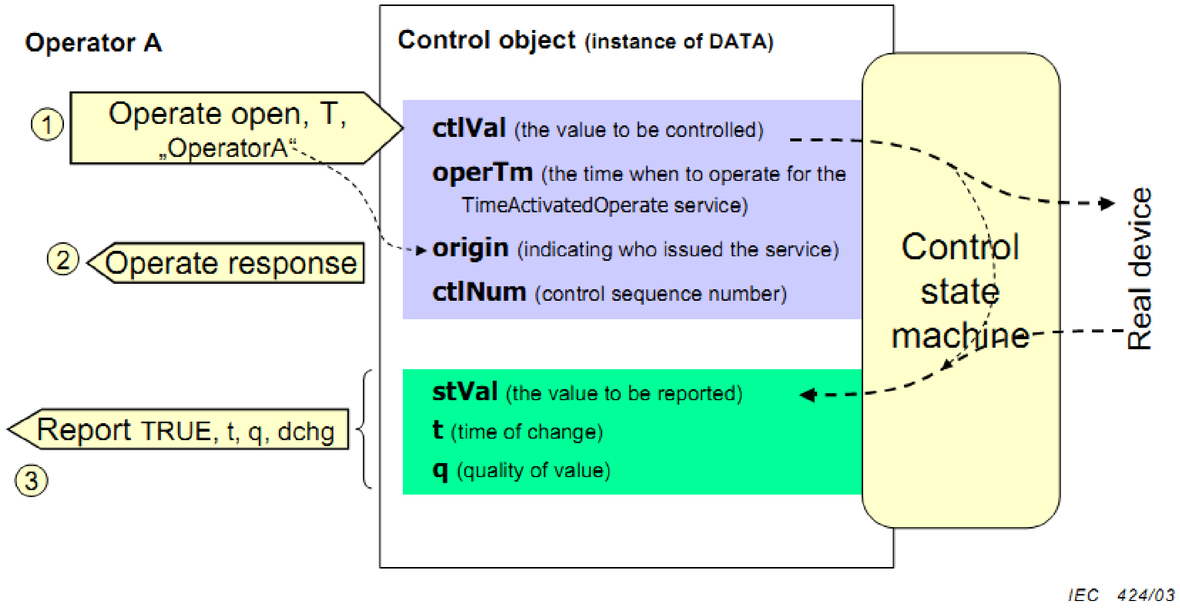


Figure 2.14 – Principle of the control model, copied from [19]

Figure 2.9 illustrates the principle of the control model. The client (Operator A) uses the control service **Operate** to control an IED. The **Operate** service parameters indicate the value to be controlled, the operate time, origin of the services and the control sequence number. The **Operate response** is generated to indicate whether or not the **Operate** service succeeded. In this example, the **report** service is used in addition to provide final result of the control operation which includes the changed value, time of change and quality of value. But the implementation of **report** service is optional [15].

2.3.3 Mapping of IEC 61850 data models and services to MMS for implementation of remote control applications

An important reason for mapping IEC 61850 to MMS is that MMS can support the complicated data models and services of IEC 61850. Theoretically, IEC 61850 data models and services can be mapped to any protocol. However, it will be very complex and cumbersome when trying to map IEC 61850 objects and services to a protocol that only provides read/write/report services for simple variables that are accessed by register numbers or index numbers [29]. It was the reason why MMS was chosen to support the complex name objects and services provided by IEC 61850.

Moreover, MMS is the only public (ISO standard) protocol that has a proven implementation track record that can easily support the complex naming and services models of IEC 61850. MMS also support the client/server two-party application association model in IEC 61850 to the MMS environment. The IEC 61850 control model can also be mapped to the existing MMS messages and objects as shown in table 2.6.

Table 2.7 – Mapping of control services, copied from [16]

ASCI service		MMS service	Variable specification	Access result
Select	Request	Read request	SBO	
	Response +	Read response	SBO	Success
	Response –	Read response	SBO = NULL	Success
SelectWithValue	Request	Write request	SBOw	
	Response +	Write response		Success
	Response –	InformationReport (ListOfVariable)	LastApplError	
		Write response		Failure
Cancel	Request	Write request	Cancel	
	Response +	Write response		Success
	Response –	InformationReport[2)] (ListOfVariable)	LastApplError	
		Write response		Failure
Operate or TimeActivatedOperate (operTm = 0)	Request	Write request	Oper	
	Response +	Write response		Success
	Response –	InformationReport[2)] (ListOfVariable)	LastApplError	
		Write response		Failure
TimeActivatedOperate (operTm != 0)	Request	Write request	Oper	
	Response +	Write response		Success
	Response –	InformationReport[2)] (ListOfVariable)	LastApplError	
		Write response		Failure
TimeActivatedOperate _Termination (operTm != 0)	Request +	InformationReport (ListOfVariable)	Oper	
	Request –	InformationReport (ListOfVariable)	LastApplError	
CommandTermination	Request +[1)]	InformationReport (ListOfVariable)	Oper	
	Request –	InformationReport (ListOfVariable)	LastApplError Oper	

1) When available, the value of operTm shall be zero(0) within the CommandTermination message.

2) Optional for control with normal security

Therefore, IEC 61850 abstract services can be fully mapped on the real MMS objects and protocol to implement the remote control communication in electricity distribution grid.

More details about the specification of MMS will be described in chapter 4.

2.4 Technical description of Long Term Evolution (LTE)

2.4.1 Overview of LTE

LTE is the fourth generation (4G) cellular communication network that was designed by a standardization organization called Third Generation Partnership Project (3GPP) and is known in full as 3GPP Long Term Evolution. LTE evolved from the well-known 3G Universal Mobile Telecommunication System (UMTS), which in turn evolved from the dominant 2G Global Systems for Mobile Communications (GSM) [24].

LTE was developed to fulfil the need of a telecommunications network that could support the huge demand for data exchange with plentiful bandwidth-consumed services. A measurement of voice and data traffic in worldwide mobile telecommunication networks done by Ericsson showed that voice was no longer the dominant service in mobile communication system but data (see figure 2.13)

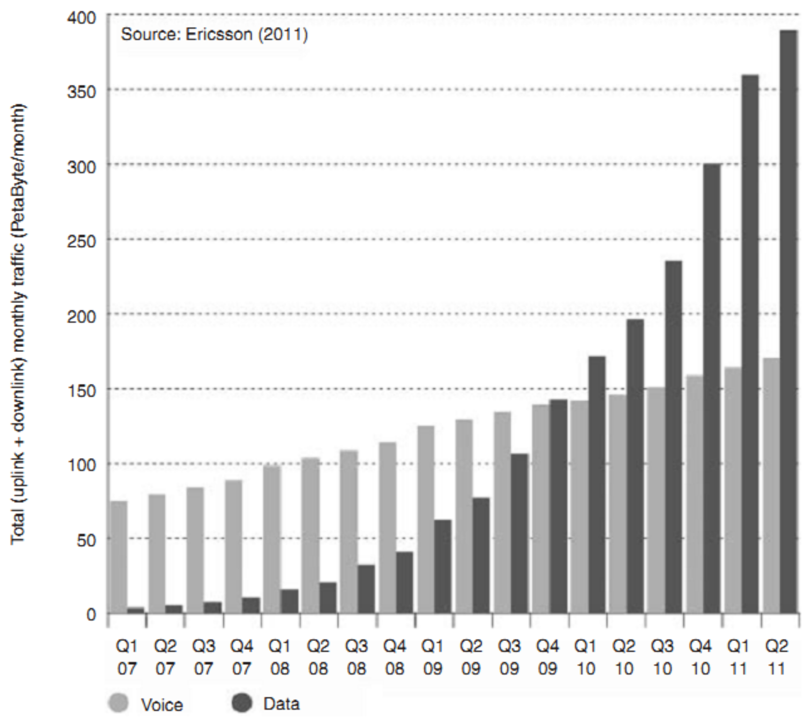


Figure 2.15 – Measurements of voice and data traffic in worldwide mobile telecommunication networks, in the period from January 2007 to July 2011, copied from [24]

In fact, LTE is not the real 4G network since LTE can only support the peak data rate of 100 Mbps in the downlink and 50 Mbps in the uplink which do not meet the requirement of ITU for 4G known as International Mobile Telecommunications IMT-Advanced which requires maximum data rate of 1Gbps. Therefore, technically LTE should be 3.9G; however, in the market LTE is still known as a representative of 4G. Figure 2.14 shows the evolution of cellular systems.

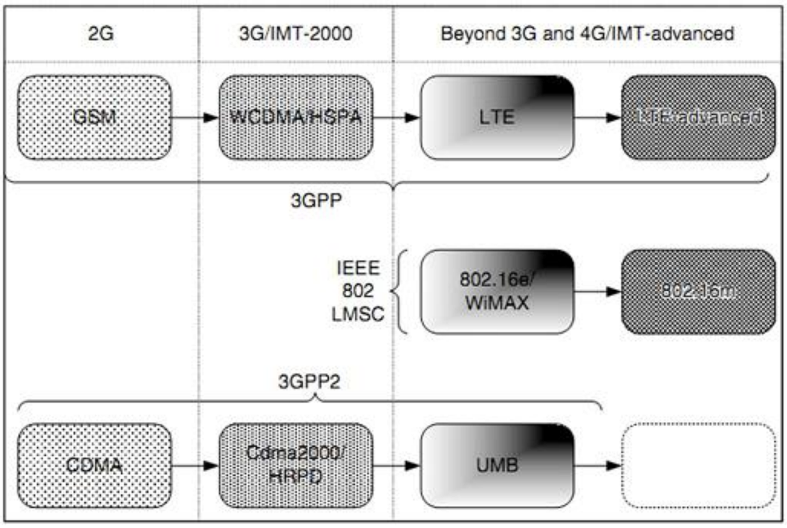


Figure 2.16 – Cellular system evolution, copied from [25]

2.4.2 LTE network architecture

Traditionally mobile communication systems (1G, 2G) were built to mainly support voice; therefore, they relied on circuit-switched technology. As the development of the Internet, mobile users desired their handsets and the communication networks to support IP-based applications. Hence, the next evolutions of mobile communication systems such as GPRS, EDGE and the 3G UMTS supported packet-switched communications. With the continuous development of mobile data applications and the huge demand for data services of the users as illustrated in figure 4.10, the evolution from the 3G UMTS to 4G LTE is carried out under the vision that future radio access network would be based on packet-switch technologies [26].

Figure 2.15 shows the evolution from the GSM and UMTS network architecture to LTE network architecture. There are evolutions in both radio access networks with new air interface (SAE – System architecture evolution) and core network that is capable to deliver both voice and data services over only packet-switched infrastructure.

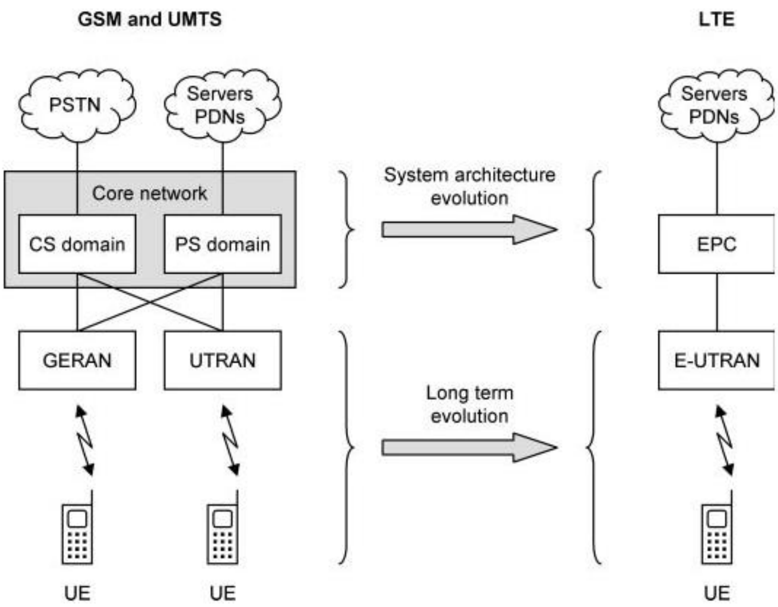


Figure 2.17 – Evolution of the system architecture from GSM and UMTS to LTE, copied from [24]

The conjunction of both SAE and LTE has introduced the Evolved Packet System (EPS) in 4G communication systems. The EPS radio access network and core network is based on a packet-switching mechanism [26].

The overall network architecture of LTE is presented in Figure 2.18

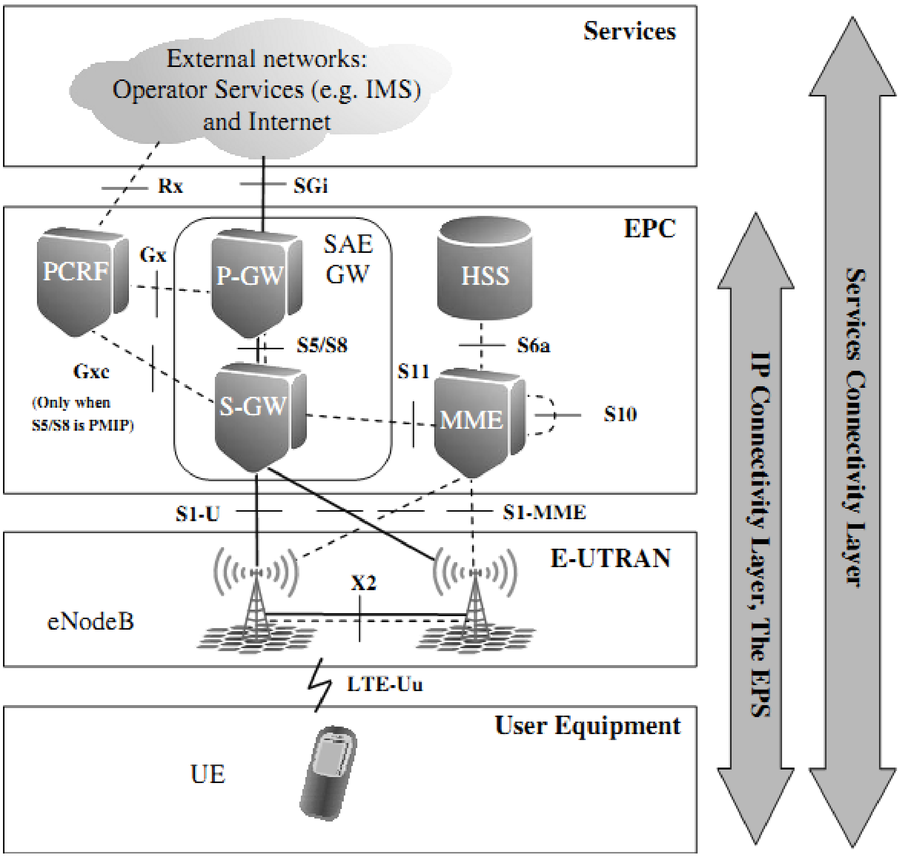


Figure 2.18 – LTE network architecture, copied from [27]

In figure 2.16 we can see the main blocks of LTE including the User Equipment – UE, the Evolved-UMTS Terrestrial Radio Access Network – E-UTRAN, the Evolved Packet Core – EPC network and the services domain.

2.4.2.1 User Equipment

Typically the user equipment is the hand held device that supports LTE to allow the user access to the voice and data services. UE contains the Universal Subscriber Identity Module (USIM) to identify and authenticate the user and to derive the security keys for protecting the radio interface transmission. UE provides the user interface to the end user so that applications such as VoIP client can be used to set up a voice call [27].

2.4.2.2 E-UTRAN

The LTE radio access network E-UTRAN consists of one or more eNodeBs, which are used to provide transmission and reception of signals over the radio interface [26]. The eNodeB inherits the functionality of both the Radio Network Controller – RNC and nodeB in UMTS Radio Access Network – RAN architecture. Basically, eNodeB implements modulation and demodulation of signals, channel coding and decoding, controlling of radio resource and mobility management. The eNodeB also acts as a layer 2 bridge between UE and EPC. The functionalities of eNodeB is depicted in Figure 2.17.

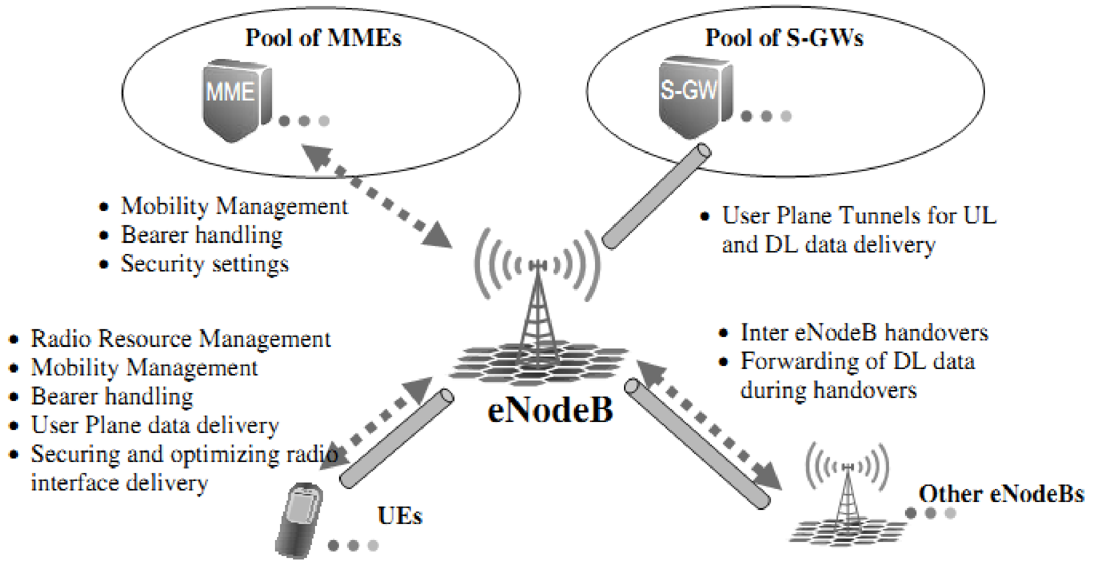


Figure 2. 19 – eNodeB connections to other logical nodes and main functions, copied from [27]

2.4.2.3 Evolved Packet Core Network – EPC

As described above, EPC consists of only single packet-switched IP domain. This architecture helps to improve both real-time and non-real-time services by facilitating the end-to-end IP connection from the UE to any terminating device or network [26]. According to 3GPP, a typical EPC consists of the following entities:

- Mobility Management Entity (MME).
- Serving Gateway (S-GW).
- Packet Data Network (PDN) Gateway (P-GW).
- Policy and Charging Rules Function (PCRF).
- Home Subscription Server (HSS).

2.4.2.3.1 Mobility Management Entity – MME

MME is considered the main controlling element which is used to process signaling and control functions between UE and EPC. Figure 2.18 shows the main functions of MME in regard to other nodes within EPC.

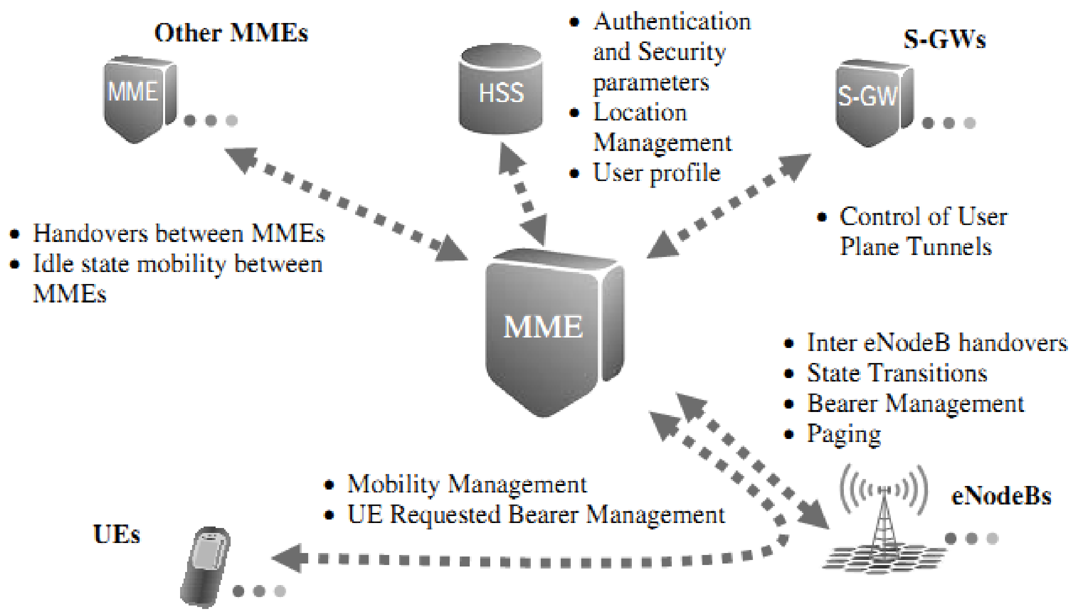


Figure 2.20 – MME connections to other logical nodes and main functions, copied from [27]

As can be seen in Figure 2.18, network resources and mobility management are the main functions of MME. Additionally, it also provide authentication and security and collect user subscription information from HSS.

2.4.2.3.2 Serving Gateway – S-GW

The main function of S-GW is to support mobility of UE when the user moves from one serving eNodeB to another, or when the UE tries to interwork with earlier 3GPP communication networks. Moreover, the S-GW is used to store user packets temporarily when the user performs inter eNodeB movements [26].

2.4.2.3.3 Packet Data Network Gateway – P-GW

The P-GW is responsible for setting up end-to-end IP based communication by providing IP addresses to the UEs and acting as a termination point for delivering user packet data.

P-GW also supports policy enforcement features and QoS parameters for each user according to agreed resource allocation and usage policy [26]. The main functions of P-GW is summarized in Figure 2.19

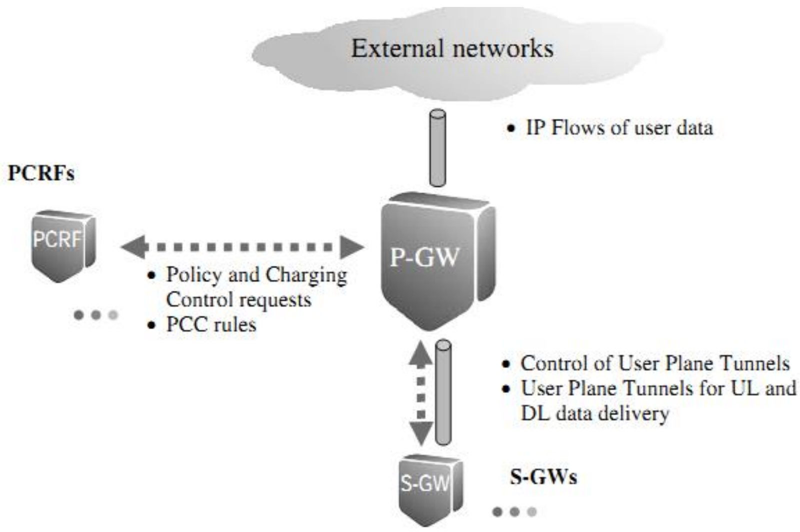


Figure 2.21 – P-GW connections to other logical nodes and main functions, copied from [27]

2.4.2.3.4 Policy and Charging Rules Function (PCRF)

The PCRF provides policy-based admission control for mobile users by determining resources access and usage limits for each user according to their user profiles [26]. The PCRF connects with IMS service through Rx interface to provide IMS access to users. The main functions of PCRF is depicted in Figure 2.20

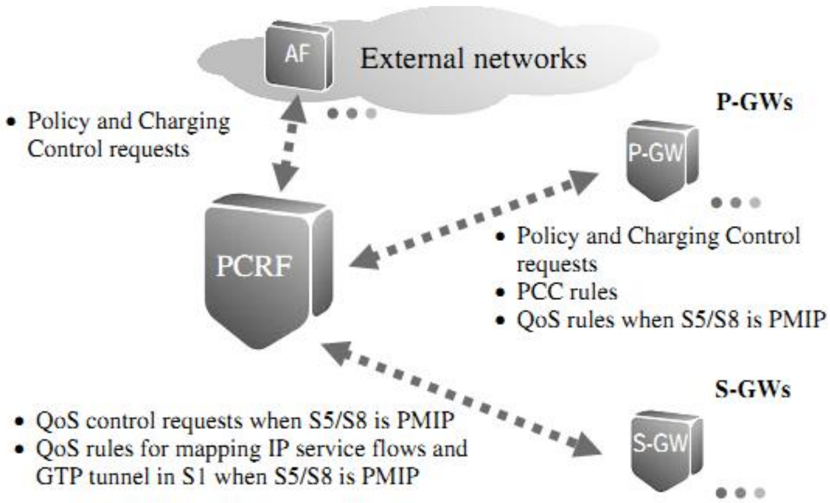


Figure 2.22 – P-GW connections to other logical nodes and main functions, copied from [27]

2.4.2.3.5 Home Subscription Server (HSS)

The HSS is typically a user profiles database which stores and updates the user subscription information and facilitates the generation of security information from user identity keys.

HSS can be considered the combination of Home Location Register (HLR) and Authentication Centre (AuC).

2.4.2.4 Service Domain

The service domain provides logical mapping of a different set of services including in the IP Multimedia Sub-system – IMS [26]. The type of services can be mainly categorized as follows;

- *IMS based operator services*: IMS is service machinery that operator may use to provide services using Session Initiation Protocol (SIP).
- *Non-IMS based operator services*: for example video streaming service provided from a streaming server.
- *Other services not provided by mobile network operator*: e.g. services provided through the Internet like web-server for web browsing services.

2.4.3 LTE protocol architecture

The protocol architecture of LTE can be divided into two main parts: the control plane which provides messages and procedures to support each interface to perform their functions, and user plane which carries the user data

2.4.3.1 Control plane

The protocol stack for the control plane between the UE and MME is depicted in Figure 2.21

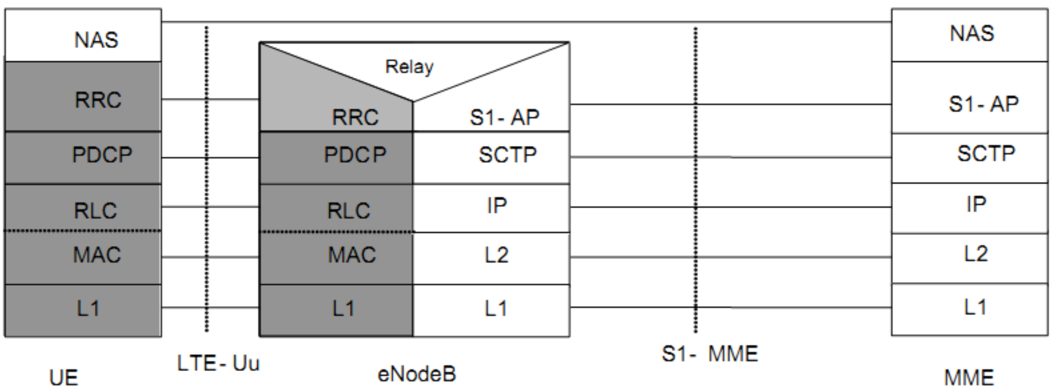


Figure 2.23 – Control plane protocol stack, copied from [28]

In Figure 2.21, the greyed region of the stack indicates the access stratum protocol. The topmost layer is Non-Access Stratum (NAS) which consists of the EPS Mobility Management (EMM) protocol and EPS Session Management (ESM) protocol. The former is responsible for handling the UE mobility within the system while the latter is used to handle the bear management between UE and MME (in addition to E-UTRAN bearer management procedures).

The radio interface protocols are [27]:

- *Radio Resource Control (RRC)*: This protocol is in control of the radio resource usage. It manages UE's signalling and data connections, and includes functions for handover.
- *Packet Data Convergence Protocol (PDCP):* The main functions of PDCP are IP header compression (UP), encryption and integrity protection (CP only).
- *Radio Link Control (RLC)*: The RLC protocol is responsible for segmenting and concatenation of the PDCP-PDUs for radio interface transmission. It also performs error correction with the Automatic Repeat Request (ARQ) method.
- *Medium Access Control (MAC):* The MAC layer is responsible for scheduling the data according to priorities, and multiplexing data to Layer 1 transport blocks. The MAC layer also provides error correction with Hybrid ARQ.
- *Physical Layer (PHY):* This is the Layer 1 of LTE-Uu radio interface that takes care of DS-CDMA Layer functions.

2.4.3.2 User plane

All IP packets for a UE is encapsulated in an EPC-specific protocol and tunnelled between the P-GW and eNodeB for transmission to the UE [28]. The user plane protocols for transmitting the user data packets are shown in figure 2.22

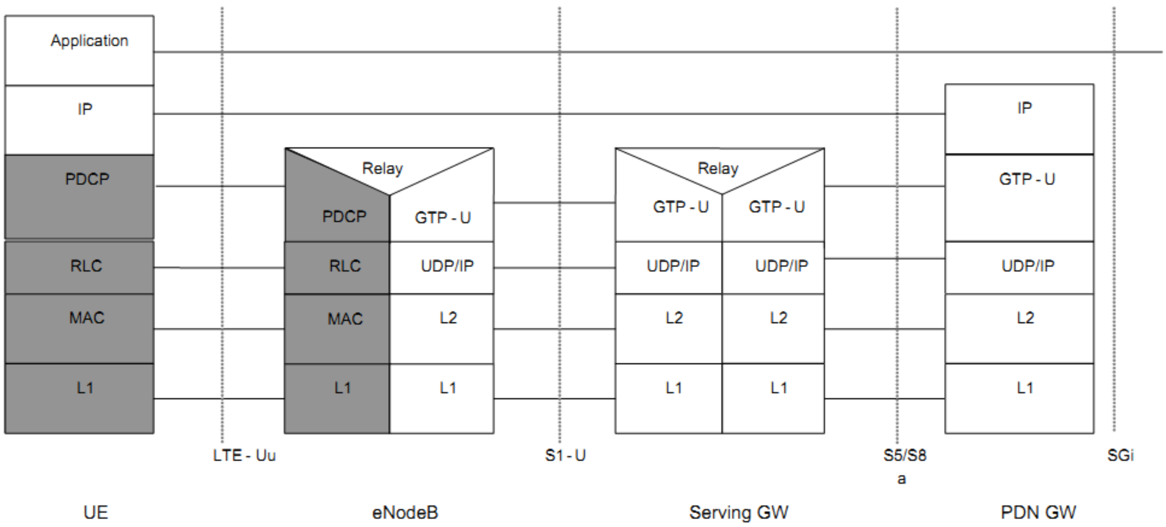


Figure 2.24 – User plane protocol stack, copied from [28]

The radio interface protocols for radio access network are the same for the control plane and were described in section 2.4.3.1.

There are two additional protocols as follows [27]:

- *GPRS Tunnelling Protocol, User Plane (GTP-U):* GTP-U is used when S5/S8 is GTP based. GTP-U forms the GTP-U tunnel that is used to send End user IP packets belonging to one EPS bearer. It is used in S1-U interface, and is used in S5/S8 if the CP uses GTP-C.
- *Generic Routing Encapsulation (GRE):* GRE is used in the S5/S8 interface in conjunction with PMIP. GRE forms an IP in IP tunnel for transporting all data belonging to one UE's connection to a particular PDN. GRE is directly on top of IP, and UDP is not used.

2.5 Summary

This chapter described the basic descriptions about IEC 61850 standard, MMS protocol, Smart Grid and the description and objectives of remote control communication in distribution grid as well as the use of IEC 61850 MMS to support those remote control applications, and finally the LTE network architecture and protocols. The objective of this chapter is to clarify the scope of this research and the technical background. It also showed that IEC 61850 is recommended beyond the original scope to support communications in distribution electricity network and IEC 61850 can be mapped over LTE network since they both based on the TCP/IP communication model. The next chapter will describe the performance requirements and challenges regarding the integration of IEC 61850 MMS and LTE to support remote control communication in distribution grid.

Chapter 3

Communication requirements and challenges

This chapter describes the communication requirements of IEC 61850 for the underlying communication technology to support control services in distribution electricity network.

IEC 61850 was created to provide interoperability inside Substation Automation System (SAS) by providing abstract definitions of the data items and services to make them independent of any underlying protocol. The abstract data and object models of IEC 61850 allow all IEDs to present data using identical structures that are directly related to their power system functions [29].

However, while the abstract models are critical to achieve a high level of interoperability, these model need to be operated over a real set protocols that are practical to implement in the power industry [29]. Therefore, one requirement for the communication protocols is the capability of supporting IEC 61850 abstract objects and services mapping. It is mentioned in this chapter as the functionality requirement.

Other type of requirement is the performance requirement of IEC 61850 for the underlying communication protocols. The performance requirements are based on the upper functions that are modelled as IEC 61850 objects and services. According to IEC 61850-5 [14]:

Communication between these devices in subsystems and between the subsystems within the overall power utility automation system fulfils a lot of requirements imposed by all the functions to be performed in power utility automation system

Since IEC 61850 provides the abstract data models and services to support supervision and control, monitoring, and protection of SAS, the requirements for these functions are different. Within the scope of this research, only the communication requirements for control services will be taken into consideration.

The basic communication requirements for SAS are defined in IEC 61850 part 5. These requirements are the basis for IEC 61850 data modelling and communication protocol mapping as stated in IEC 61850-5 [14]: *"the derived data models in subsequent parts (IEC 61850-7-x) and mappings to dedicated stacks (IEC 61850-8-x and IEC 61850-9-x) based on the communication requirements in Part 5 will not change the requirements defined in Part 5."* Therefore, this chapter is largely based on the information provided in the main part IEC 61850-5 and TR IEC 61850-90-2 – Communication between control centre and substation.

3.1 Functionality requirement

As discussed in chapter 2, IEC 61850 MMS can be mapped over a TCP/IP or OSI communication profiles. Therefore, firstly it is required for the underlying communication network to support at least one of these two communication profiles.

As MMS is an ISO communication protocol, it required to implement some adaptation protocol layers when MMS is mapped over the TCP/IP communication profiles. In fact MMS itself is not a communication protocol, as it only defines the messages that have to be transported by an unspecified network [54]. Therefore, MMS need to be supported with a communication protocol stack which includes the Association Control Service Element (ACSE, ISO 8649/8650), Abstract Syntax Notation (ASN, ISO 8822/8823), ISO 8236/8237, and RFC 1006. All these protocols must be implemented over the TCP transport layer to support all the functionalities of MMS.

To briefly say, the ACSE is an ISO application protocol which is used to establish and release Application Association (AA) between Application Entity (AE) and to determine the identity and application context of that association [54]. In case of MMS, ACSE is used to establish the client-server association between two MMS entities and to decide which one is the client that can make the request to the server. ASN is the presentation protocol which is used to transmit information between open systems using connection oriented or connectionless mode transmission at the presentation layer of the OSI 7 layer model [54]. MMS is an ISO protocol which requires the transport protocol exchanges information between peers to be in discrete units of information called transport protocol data units (TPDUs). Therefore RFC 1006 [16] describes that all TPDUs shall be encapsulated in discrete units called TPKTs. The TPKT layer is used to provide these discrete packets to the OSI Connection Oriented Transport Protocol (COTP) on top of TCP.

The detailed information about this communication stack will be describing in chapter 4. The most important point is that the underlying network infrastructure must support the mapping of IEC 61850 MMS communication protocol stack over the TCP/IP or OSI communication profiles. It is mentioned in this research as the functionality requirement of IEC 61850 MMS for the underlying communication network infrastructure.

3.2 Performance requirements

3.2.1 Transfer time

According to IEC 61850-5, the most important requirement for performance that was mentioned is transfer time. Transfer time is defined in IEC 61850-5 as follows:

The complete transfer time t is specified as complete transmission time of a message including the handling at both ends (sender, receiver).

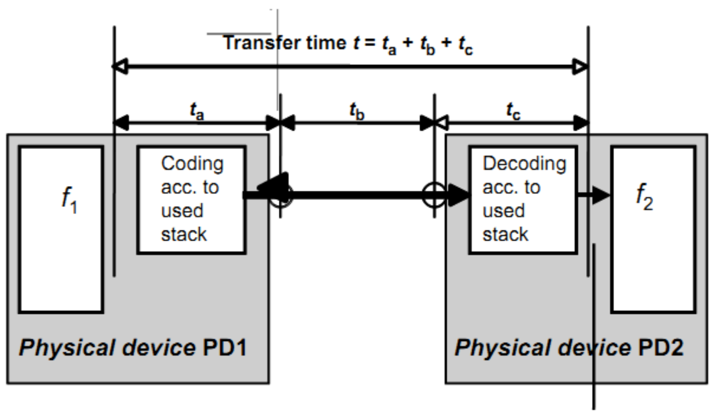


Figure 3.1 – Definition of overall transfer time t, copied from [14]

In other word, the transfer time is specified from the user or application point of view as the complete transmission of a message including the necessary coding and decoding at both ends (t_a and t_c) and the transmission time for the distance between two ends (t_b) as illustrated in Figure 3.2.

For binary signal the conventional output and input relays replace the coding and decoding. These output and input relays have response times of around 10ms [12].

If there is only a physical direct link between the control centre and substation, the time t_b is negligible referring to the speed of light. However when there are active components in the communication path, the processing time of those requirements contribute reasonably to the time t_b. If collisions or losses have to be compensated, e.g. by repetitions, also these times contribute [12].

The acceptable transfer time is varied depending on the functions and in general is categorized in 7 classes as shown in table 3.1

Table 3.1 – Performance class for control data, copied from [14]

Performamce class	Typical Transfer time [ms]	Application examples: Transfer of
TT10000	10000	Files, events, log contents
TT1000	1000	Events, alarms, status changes,
TT500	500	Operator commands
TT100	100	Slow automatic interactions
TT20	20	n/a
TT10	10	n/a
TT3	3	n/a

For communication between substation and control centre, the transfer time has to be small enough that it does not influence the operation of the function. Typical functions in the control centre are SCADA, load dispatching and power flow calculations [12].

However, since the performance classes are defined according to the requirements of the functions to be performed, the performance classes presented in table 3.5 may be overwritten by dedicated function requirements and customer specification [12].

3.2.2 Message performance requirements

The required transfer time for these types of message ranges from 3 ms for the very time-critical “trip” message, to 1000 ms for the low speed messages for control functions and even 10000 ms for control commands with access control and file transfer functions.

As the performance requirements depends on the specific applications, IEC 61850 defines 7 different message types, each has specific requirements for transfer time [12]:

- *Type 1 - Fast messages ("Protection")*: This type of message typically contains a simple binary code containing data, command or simple message, e.g. "Trip", "Close", etc. Upon receiving this message, the IED will act immediately. Those fast messages refer to time critical, protection-like functions. Performance class P1 is typical for fast messages inside the substation. Performance class P2 are for messages in between.
- *Type 1A "Trip":* the trip is the most important fast message in the substation and has the most demanding requirements.
- *Type 1B "Others"*: All other fast messages have less demanding requirements compared to the "trip".
- *Type 2 - Medium speed messages ("Automatics")*: These are messages whose originated time is important but transmission time is less critical. This type may include analogue values such as the root mean squared (r.m.s.) values calculated from type 4 messages (samples). This performance type is also applicable for messages between substations for automatic functions.
- *Type 3 - Low speed messages ("Operator")*: This type should be used for slow speed auto-control functions, transmission of event records, reading or changing set-point values and general presentation of system data. All such low speed messages refer to operator messages not time critical, referring to the slow response type of a human being (reaction time > 1 s)
- *Type 4 - Raw data messages ("Samples")*: This message type includes the output data from digitizing transducers and digital instrument transformers independent from the transducer technology (magnetic, optic, etc.). The data will consist of continuous streams of synchronized samples from each IED, interleaved with data

from other IEDs. Transfer time means for the stream of synchronized samples a constant delay resulting in a delay for the functions using the samples e.g. for protection. Therefore, this transfer time shall be so small that no negative impact on application function is experienced.

- *Type 5 - File transfer functions*: This type of message is used to transfer large files of data from disturbance recording, for information purpose, settings for IEDs, etc.
- *Command messages and file transfer with access control*: This type of message is used to transfer control orders, issued from local or remote HMI functions, where a higher degree of security is required. This type of message is based on Type 3 but with additional password and/or verification procedures.

As this research focus on the remote control communication in distribution grids with specific applications such as real-time DER generation control, voltage control, and real-time demand response, we focus on type-2 message which is designed for automatic control functions, and type-3 message which is used for slow-speed auto control functions. The performance requirements of these messages are shown in table 3.2 and table 3.3.

Table 3.2 – Transfer time requirements for medium speed messages [14]

Performance class	**Requirement description**	**Transfer time**	
		Class	**ms**
P4	The transfer time for automation functions is less demanding than protection type messages (trip, block, release, critical status change) but more demanding than operator actions.	**TT3**	≤100

Table 3.3 – Requirement for low speed messages [14]

Performance class	Requirement description	Transfer time	
		Class	**ms**
P5	The total transmission time shall be half the operator response time of = 1 s regarding event and response (bidirectional)	**TT2**	≤500
P6	The total transmission time shall be in line with the operator response time of =1 s regarding unidirectional event	**TT1**	≤1000

Depending on the control applications, the end-to-end delay requirement ranges from 100ms to 1000ms. In this research, we concentrate on the 100ms delay requirement since we consider the real-time automatic remote control functions between the control centre and the renewable energy generation, distributed energy storages, electrical vehicles…etc.

3.3 Challenges

3.3.1 Latency

Latency is the most important requirement for control communication since receiving a late control command may seriously affect the safe operation of the electricity grid.

In this research, we assume a public, shared LTE network; therefore, the amount of background traffic has a big impact on the latency of remote control communication messages. Hence, experiments will be conducted with the increase in number MMS nodes and background nodes to verify if the delay requirement is still fulfilled.

3.3.2 Quality of Service – Prioritization

Because the remote control communication is considered very critical, it should always be prioritized. In a public, shared LTE network, there are many different background traffic types; therefore, the remote control communication should be distinguished and assigned higher priority in order to guarantee its performance requirements.

It is more important in the situation when the network resources become insufficient due to the introduction of more devices and services. Within a specific limitation, the LTE network must be able to differentiate the control traffic and assign enough resource to ensure proper performance of the control traffic.

3.3.3. Reliability

The network is reliable if all the control traffics can be exchanged successfully. By using TCP, LTE provide a reliable connection-oriented transport protocol. At the lower layer, the HARQ protocol is used to retransmit the lost packet making LTE more reliable.

However, there are still the cases that can significantly reduce the reliability of LTE network such as problem with the hardware devices or power failure. These problems will corrupt the operation of the network. Hence, it is important to implement some solutions such as asset management of the LTE network devices to predict the problems, installation of power backup system and so on.

3.3.4 Security

Security is also a crucial issue since the public LTE network is considered. The network operator should implement strong security mechanisms such as encryptions and authentications to prevent attack to the control traffic.

When using the security mechanisms, it is important to consider the impact of those technologies on the performance of the control traffic since they increase the computational time which increase the end-to-end delay.

3.4 Summary

This chapter described the requirements of IEC 61850 for control communications including the functionality and performance requirements. The functionality requirement states that the underlying communication network infrastructure must support the full stack of MMS communication protocol over TCP/IP or OST communication profile. Regarding the performance requirements, the most important one is the transfer time, or in other words, the end-to-end delay. For automatic control interactions, the required delay ranges from 100ms to 1000ms depending on the control applications. The 100ms will be considered in the later experiments since the real-time remote control functions are considered. This strict delay requirement along with the QoS-prioritization, reliability and security are the main challenges. However the two later issues are out of scope of this research.

The next chapter 4 describes the specification and design of solution to solve the end-to-end delay and QoS-prioritization challenges.

Chapter 4

Specification and Design

This chapter describes of the solution of integrating IEC 61850 MMS and LTE to support remote control communications in electricity distribution. Section 4.1 introduces the architecture of the solution and describes the main functionalities of the modules. Section 4.2 provides details about the technical design of the modules mentioned in section 4.1.

4.1 Specification of the solution

As discussed in chapter 1, the goal of this research is finding a solution to support the remote control communication in Smart electricity distribution grid. After some previous researches in Smart Grid including an Internship project at Alliander, one of the largest energy distribution companies in the Netherlands and following by a Research topics conducted in University of Twente, I come up with a solution of integrating IEC 61850 MMS protocol over the LTE wireless cellular communication network to support remote control communication in distribution grid.

The overall solution consists of modelling the electricity components as IEC 61850 information objects which was partly provided by IEC 61850 standards and technical documents, and partly done in my Internship project [63], integrating IEC 61850 MMS communication stack over LTE infrastructure, and finally designing a Priority-aware MAC scheduler to give preference to control communication traffic in order to fulfil the performance requirements in network-resources-limited situations.

The architecture of the solution is shown in Figure 4.1. There are three main building blocks of the solution architecture including the MMS client and servers, the LTE network and the MAC scheduler.

To fulfil the functionality requirement specified in chapter 3, the full MMS communication protocol stack must be integrated successfully over the underlying LTE communication protocol stacks at all MMS servers which are also the LTE subscribers.

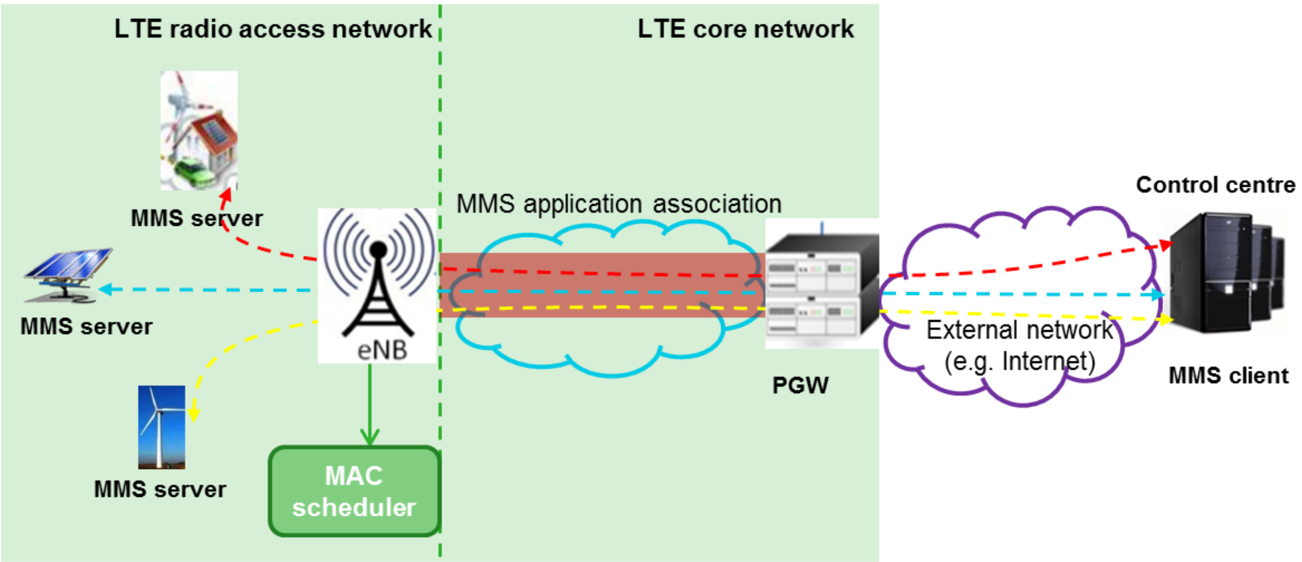


Figure 4.1 – Architecture of the solution

This is an overall architecture of an electricity and communication network system that uses IEC 61850 MMS protocol over the LTE cellular network infrastructure to enable the automatic control interaction between the control centre and different intelligent electricity systems and devices.

4.1.1 MMS client and server

The MMS client and servers are the control centre and the intelligent electricity devices to be controlled in the distribution grid respectively.

As discussed in chapter 2, there main different components in distribution grid to be controlled. In this figure, we take an example of the Distributed Energy Resources including PV panel and wind turbine, and the customer side which can be a Microgird which both generates and consumes electricity.

The MMS client is the control centre. Between the MMS client and one MMS server, there is always an application association established by the ACSE application protocol. For one application association, the MMS entity that sends an initiation-request to establish the association will be the MMS client and the other one is the MMS server. One MMS client can establish multiple application associations with different MMS servers.

After an application association has been established, the MMS client can send requests to read, write or delete information variables at the MMS servers. By this method, the MMS client can control the operating status of the MMS server. That is why the control centre is the MMS client which proactively establishes all application association to the entities that it wants to control. The MMS server, on other way, can choose to accept or reject the association-request sent by the client.

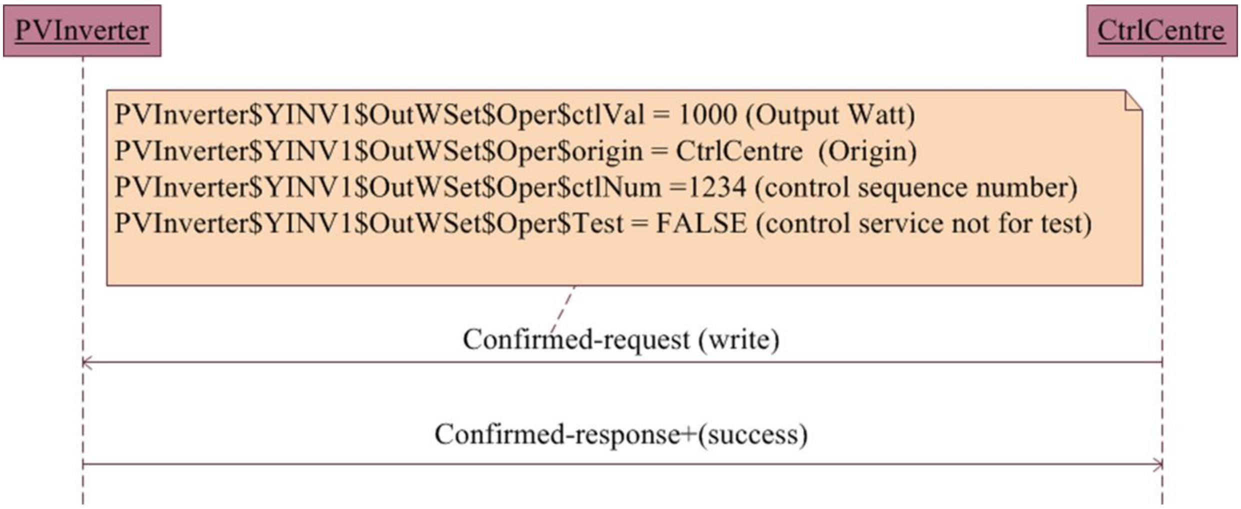


Figure 4.2 – Control centre uses IEC 61850 MMS services to control a PV panel

Figure 4.2 illustrates the message flow when a control centre uses IEC 61850 MMS services to control the power generated by a PV panel through the energy inverter module embedded in the PV panel system.

Obviously, to support IEC 61850 MMS services, the control centre and all the intelligent electrical devices have to be firstly modelled as the IEC 61850 objects. The modelling method has been described in detail in the Internship project report [63]. The models for some well-known DERs can be found in the technical report IEC 61850-7-420 of IEC [64]. Table 4.1 shows an example of a logical node that represents the control centre of a Smart home that designed during my internship project and can be found in [63]

Table 4.1 – IEC 61850 logical node for Smart home control centre, copied from [63]

ZHCM class				
Data Object Name	**Common Data Class**	**Explanation**	**T**	**M/O/C**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
Data Objects				
EEHealth	ENS	External equipment health		O
EEName	DPL	External equipment name plate		O
OpTmh	INS	Operation time		O
Status				
Oper	SPS	Operation status of the Home control and management center		M
OperMod	ENS	Operating mode Value | Explanation 1 | Autonomous 2 | Controllable		M
Settings				
MaxWh	ASG	Set-point of maximum energy consumption		O

Additionally, in order to operate over the LTE network, the MMS client and server must be installed with LTE interfaces that compliant with the implemented LTE version.

4.1.2 LTE network infrastructure

The LTE network infrastructure includes all the fundamental hardware devices and software protocols that explained in chapter 2. Particularly, it must contain the LTE radio access network which provides direct radio access to the controllable electricity devices and normal UEs and the Evolved Packet Core network as illustrated in Figure 2.16.

The LTE network infrastructure interconnects the MMS servers and client by providing LTE connections to all MMS servers via the LTE radio access network and keeping the wide-band network connection from the PGW to the control centre through an external network such as the Internet.

The brief description of LTE network infrastructure has been provided in chapter 3. In chapter 5, the detailed description of the LTE network infrastructure used for the simulation experiment will be discussed.

4.1.3 LTE MAC scheduler

The MAC layer, particularly, the MAC scheduler is the one that is in charge of assigning the resource block to the users. The MAC scheduler determines when and how many resource blocks should be assigned to a specific users based on different resource allocation algorithms. Therefore, the MAC scheduler plays a key role in the latency performance of the user.

Since the automatic control interactions requires strict latency performance, a priority-aware MAC scheduler will be designed to give higher priority to the control communication traffic in order to guarantee that this type of traffic will always have a better opportunity to access the network resources especially in case of limited network resources.

The priority-aware MAC scheduler designed in this research is an enhancement of the Round Robin scheduler and is called Priority-aware Round Robin scheduler in this research. Because in the considered research scenario, the major remote control traffic stream is from the control centre (MMS client) to the controlled nodes (MMS servers), only the downlink is considered in the research. The priority-aware feature of the Priority-aware Round Robin scheduler, therefore, is implemented in the downlink only.

The Priority-aware Round Robin MAC scheduler is developed by the author based on the Round Robin mechanism used for the traditional Round Robin MAC scheduler. If the traditional Round Robin MAC scheduler simply assigns physical resources to active users in a cyclic manner, the Priority-aware Round Robin MAC scheduler considers the priority-tag of the flow before making the scheduling decision. For LTE, 3GPP has defined some standard QCI values which reflect some sets of QoS parameters that can be assigned to traffic flows by activating the respective bearers and embedding traffic flows to those bearers. Since QCI is an 8-bits field, it can be extended to support 255 different QoS sets. Within this research, the author has defined a new set of QoS parameters for the remote control communications traffic and redefined the existing QCIs to give the remote control communication traffic the highest priority.

For scheduling physical resources, the Priority-aware Round Robin scheduler will first check all the active flows, the ones that have data to be transferred in RLC buffer. If that flow is active, then the scheduler checks the priority tag assigned to this flow. Based on the priority tag, the scheduler calculates the metrics such that the lower the priority-tag value, the higher the metrics. For example, the remote control traffics has priority-tag value equal to 1 (meaning it is the first priority traffic), it will be assigned the highest metrics calculated by the scheduler. Based on the calculated metrics, the scheduler then making the resource allocation decision on a way that the flow with the highest metric will be assigned the physical resources first.

The next section 4.2 will describe in more detail about the technical design of main entities in the solution architecture.

4.2 Technical design

This section provides the detailed technical design of the MMS communication stack and the priority-aware MAC scheduler that will be used to fulfill the requirements and overcome the challenges mentioned in chapter 3.

4.2.1 IEC 61850 MMS protocol

IEC 61850 MMS has been briefly discussed in chapter 1 and 2. In this section, the technical specifications of the protocol will be described in more details as it is necessary for the correct implementation of the IEC 61850 MMS model in the simulator.

It is important to note that MMS does not specify application-specific operations (e.g. get the smart meter data). This is covered by application-specific, in this case IEC 61850 ACSI services. MMS is also not a communication protocol; it defines messages that have to be transported by an underlying protocol [57].

The MMS architecture is based on a common client-server model. Real devices used in industrial networks often contain an MMS server allowing the device to be monitored and managed from an MMS client. As MMS does not specify how to address clients and servers, an entity containing an MMS client or server must rely on the addressing scheme of underlying protocols in the process of establishing an application association to support the

MMS environment. In practice, clients and servers are addressed by their IP address and the MMS server uses port number 102 [57].

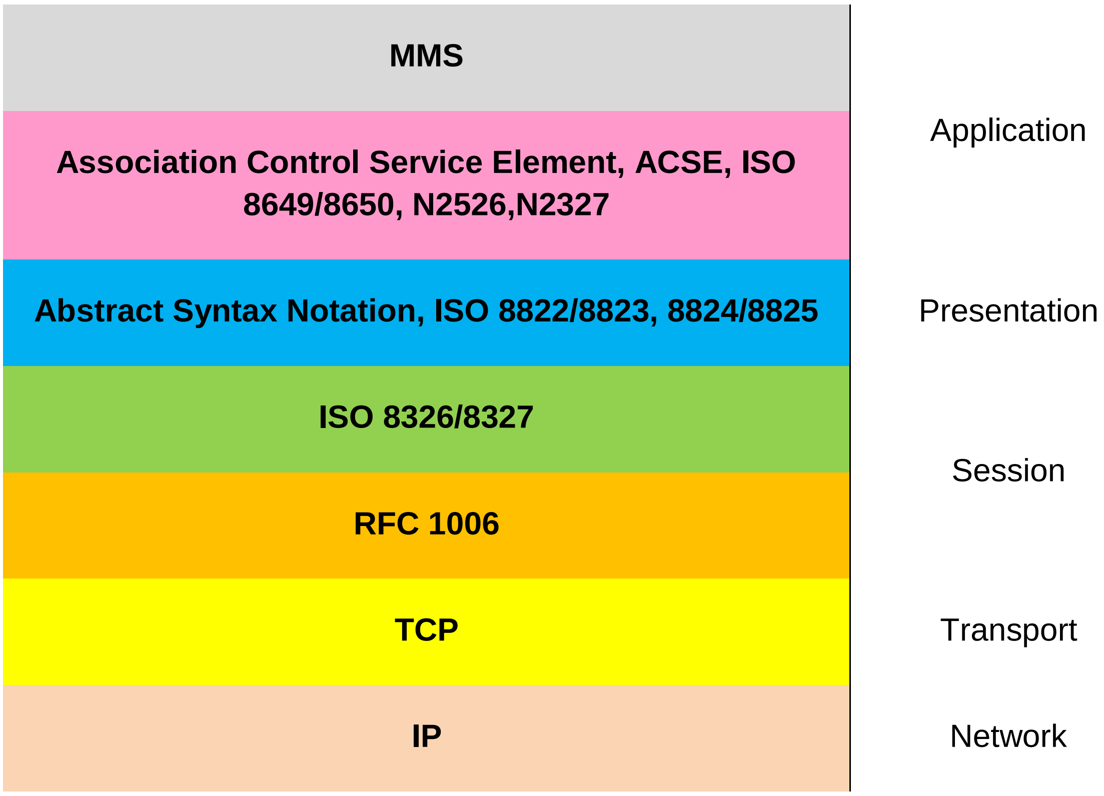


Figure 4.3 - Layer 3-7 of the current MMS communication stack, based on [57][58]

Figure 4.1 depicts layers 3 to 7 of the current MMS stack according to [57], [58].

MMS services are placed on top of the stack in the Application layer. Through the services, the MMS client can interact with the MMS server for specific functions such as reading or writing local variables. Association Control Service Element (ACSE) protocol is also situated in the Application layer and is used to establish associate and release Application Associations (AA) between the two communication parties by means of the A-ASSOCIATE and A-RELEASE services and to determine the identity and application context of that association.

The presentation layer exists to ensure that the information content of presentation data values is preserved during transfer and to add structure to the units of data that are exchanged. Presentation: ASN.1 and BER. MMS uses ASN.1 as abstract syntax notation at the presentation layer. An abstract syntax notation is the notation used in defining data structures or set of values for messages and applications. The abstract syntax notation is then encoded with a set of encoding rules before transmission [54].

The Basic Encoding Rules (BER) is one of the original sets of encoding rules specified by the ASN.1 standard. BER is a self-identifying and self-delimiting encoding scheme in which a data element is encoded using a triplet consisting of a type identifier (tag), a length description and the actual data element. The use of such a triplet for encoding is commonly referred to as a Tag-Length-Value (TLV) encoding. The use of TLV encoding allows any receiver to decode the ASN.1 information from an incomplete information stream [54].

MMS is an ISO protocol which requires the transport protocol exchanges information between peers to be in discrete units of information called transport protocol data units (TPDUs). Therefore RFC 1006 [16] describes that all TPDUs shall be encapsulated in discrete units called TPKTs. The TPKT layer is used to provide these discrete packets to the OSI Connection Oriented Transport Protocol (COTP) on top of TCP.

```
Field size:  <     8 bits    ><   8 bits    ><             16 bits            >

             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Field name:  |     vrsn      |   reserved    |          packet length        |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4.4 - TPTK header format, copied from [54]

The format of the TPTK header is depicted in figure 4.2. The format of the header is constant regardless of the type of packet. The field labelled *vrsn* is the version number which according to RFC 1006 always is three. The next field, *reserved*, is reserved for further use. The last field is the *packet length*. This field contains the length of entire packet in octets, including packet-header.

The COTP data transport PDU is described in figure 4.3.

```
                <          header           ><            body          >

Byte number       1       2           3           4       5            ... end
                +----+-----------+-----------+------------ - - - - - -------+
Field name      | LI |  T    CDT |  TPDU-NR  | User Data                    |
                |    | 1111 0000 |  and EOT  |                              |
                +----+-----------+-----------+------------ - - - - - -------+
```

Figure 4.5 - COTP PDU format

The header length in octets is indicated by a binary number in the *length indicator (LI)* field. This field has a maximum value of 254 (1111 1110). The next field is divided into two parts, first the PDU type specification (T), which describes the structure of the rest of the PDU, e.g., Data Transfer (1111) shown in the figure, Connection Request (1110), Connection Confirm (1101). The PDU type is encoded as a four bit word. The full list of codes for data types can be found in [15]. The second part is the credit part (CDT) which is always set to 0000. The third field contains the TPDU number and an end of transfer indication flag, followed by the upper layer data.

With the COTP and TPTK adaptation layers, MMS can run on TCP/IP protocol stack, making it more popular and a widely accepted standard.

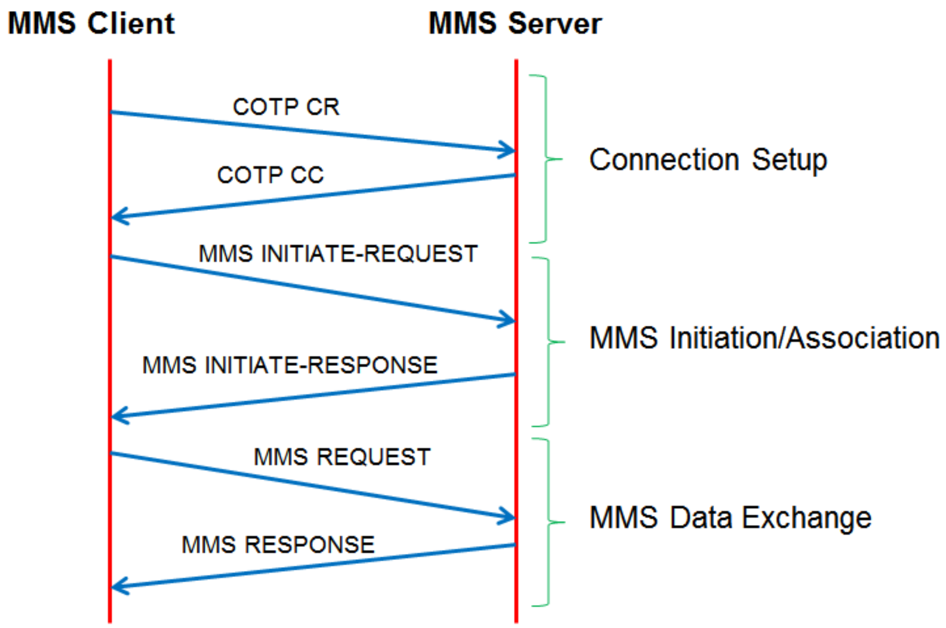


Figure 4.6 - MMS message flow in different phases between MMS client and MMS server

The message flow for the MMS data exchange is illustrated in figure 4.6. After the normal TCP three-way handshake between the MMS client and MMS server, the COTP layer establishes a connection to transport ISO protocol over TCP by means of the Connection Request message from MMS client and Connection Confirm message from MMS server. Then the MMS Initiation/Association phase begins. The MMS INITIATE-REQUEST message is mapped onto Application Association Request (AARQ) PDU of the ACSE layer, which is transported over COTP Data TPDU. The MMS server replies with the INITIATE-RESPONSE message, mapping it onto Application Association Response (AARE) PDU of the ACSE layer and is transported over COTP Data TPDU. After the MMS client receives the INITIATE-RESPONSE, the two MMS parties are associated, and can begin the MMS data exchange.

4.2.2 Priority-aware MAC scheduler

As discussed in chapter 3, the main challenges of integration IEC 61580 MMS and LTE to support remote control communication in distribution grid are latency and Quality of Service – Prioritization. And because the main control communication stream is from the control centre to the controlled devices, we mainly focus on improving the downlink latency performance.

On the downlink, LTE use the Orthogonal Frequency Division Multiple Access (OFDMA) to allow multiple users sharing the same bandwidth. The idea behind OFDMA is to split up one high data rate stream into several low data rate streams carried by a large number of subcarriers. Each subcarrier is modulated at a low symbol rate and carries one symbol of a modulation format, such as Quadrature Phase-Shift Keying (QPSK), 16-QAM (quadrature amplitude modulation) or 64-QAM for LTE. These sub-carriers are orthogonal to allow overlap in frequency domain which is very beneficial in term of bandwidth saving (see Figure 4.6)

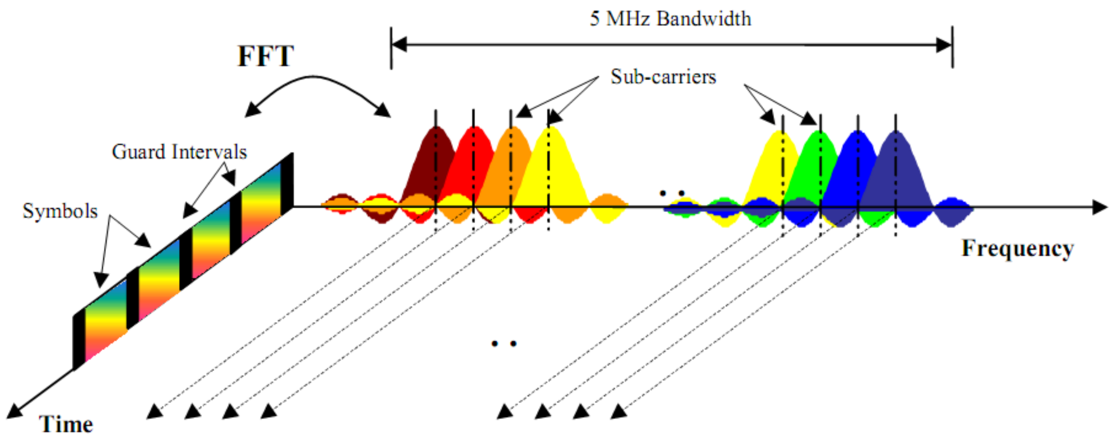


Figure 4.7 - Sub-carrier overlap in OFDMA, copied from [62]

With OFDMA, multiple users can share the same resource in both frequency and time domain. In LTE, the network resources are divided in to multiple resource blocks measured in both time and frequency domain as illustrated in figure 4.7.

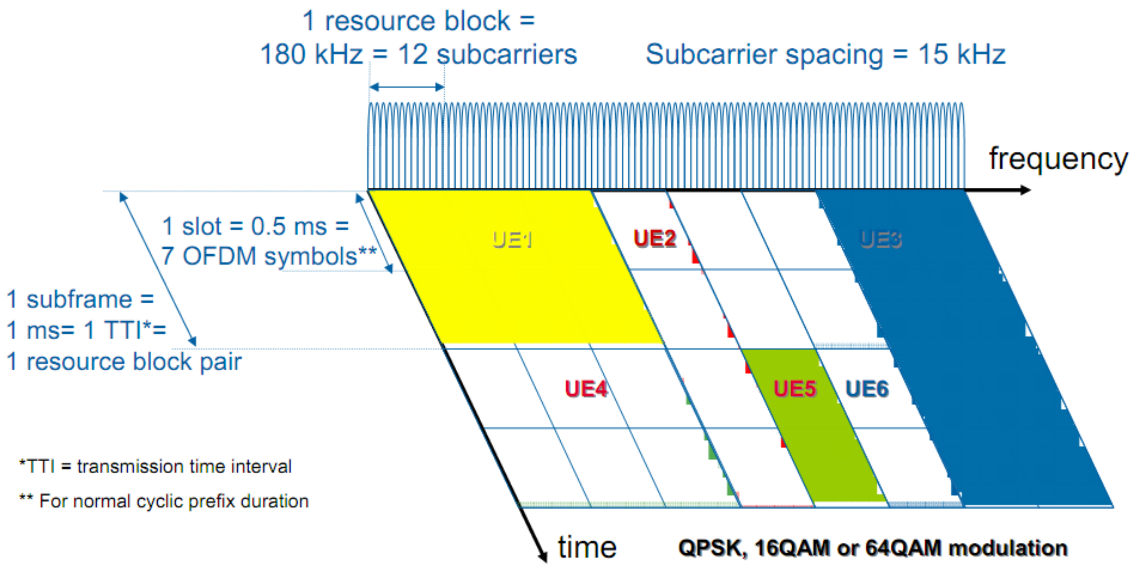


Figure 4.8 - Resource allocation for users using OFDMA, copied from [62]

The MAC layer, particularly, the MAC scheduler is the one that is in charge of assigning the resource block to the users. The MAC scheduler determines when and how many resource blocks should be assigned to a specific users based on different resource allocation algorithms. Therefore, the MAC scheduler plays a key role in the latency performance of the user.

Since this research aims to find out a solution that can provides the best guarantee of latency performance and prioritization of the control communication traffic, we should focus on the scheduling algorithm implemented in the MAC scheduler.

In general, there are four main key design factors that should be considered for designing the resource allocation mechanisms as follows [68].

- **Complexity and Scalability**: LTE packet scheduler has to take allocation decision every TTI which is 1ms. Therefore, low complexity and scalability are fundamental requirements for limiting processing time and memory usage. Using complex and exhaustive research over all possible combinations would be too expensive in term of computational cost and time [69]. Let N and R be the number of active users in the current TTI and the number of available RBs, respectively; the scheduler has to calculate $M = N * R$ metrics every TTI. This assures the scalability requirement thanks to the linear dependence on the number of resource blocks and users.
- **Spectral efficiency**: one of the main goals of the system is to achieve the effective utilization of radio resources. For example, the spectral efficiency can be achieved by always serving users that experiencing the best channel quality.
- **Fairness**: fairness is a major requirement that should be taken into account to guarantee minimum performance to also users that experiencing bad channel conditions.
- **QoS provisioning**: QoS is a major feature in all-IP architectures. QoS constraints may vary depending on the application and they are usually mapped into some parameters: minimum guaranteed bit rate, maximum delivering delay and packet loss rate (PLR).

Within the scope of this research, since the performance of remote control communications traffic should be guaranteed, QoS-provisioning is the most important factor. The LTE packet scheduler should assign higher priority to the remote control communication flows to ensure that they will somehow get served under the circumstance that the network resources are insufficient to guarantee the performance of all applications.

Figure 4.8 illustrate the generic view of the LTE MAC scheduler which takes into consideration the Downlink queue state information, channel quality information and traffic measurement for making the resource allocation decision.

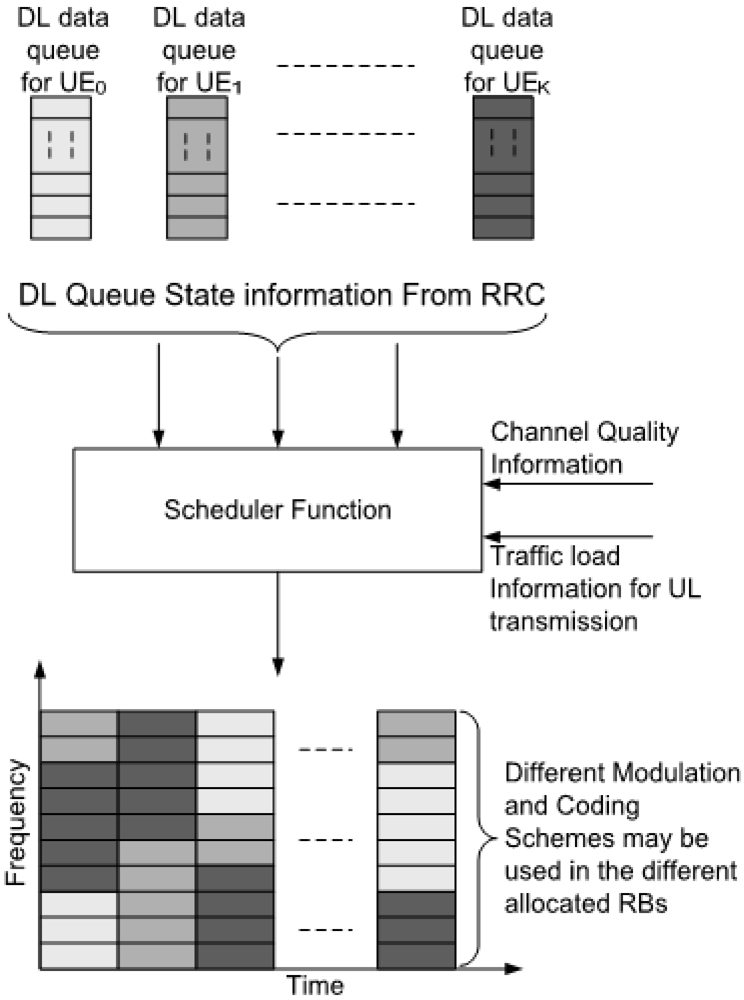


Figure 4.9 – Generic view of LTE MAC scheduler, copied from [27]

Actually, there are many different MAC scheduling algorithms which differ in them of input parameters, objectives, and service targets. These scheduling designs can be classified into five groups of strategies according to [68]: channel-unaware; channel-aware/QoS-unaware; channel-aware/QoS-aware; semi-persistent for VoIP support; and energy-aware.

For the first two groups, there are some well-known scheduling policies such as First-In-First-Out (FIFO), Round Robin (RR), Blind Equal Throughput, Resource Preemption, Weighted Fair Queuing, and Guaranteed Delay which are channel-unaware; and Maximum Throughput (MT), Proportional Fair Scheduler (PF), Throughput to Average (TTA), Joint time and frequency domain schedulers, Delay sensitivity, and Buffer-aware schedulers which are channel-ware/QoS-unaware [68]. The advantage of the channel-unaware scheduling mechanisms is the highest level of simplicity since they take into account neither channel conditions nor QoS parameters in scheduling decision. The channel-aware/QoS-unaware schedulers' advantage is mainly spectral efficiency since the channel conditions are taken into consideration.

However, because QoS is not considered by the both channel-unaware and channel-ware/QoS-unaware schedulers, it is no guarantee that the remote control communications traffic will have the better opportunities for resource allocation especially when the network resources are insufficient to ensure minimum requirements of all traffic types.

Therefore, the channel-aware/QoS-aware scheduling mechanisms should be considered. In LTE, QoS is associated with the definition of bearer and QoS Class Identifier – QCI. Bearer can be viewed as a combination of multiple QoS requirements which indicated by the QCI number. Each QCI is characterized by priority, packet delay budget and acceptable packet loss rate. The QCI label for a bearer determines how it is handled in the eNodeB. Table 4.2 summarizes the basic QCI values defined for the normal human-to-human traffic in LTE network. GBR stands for Guaranteed Bit Rate which implies that dedicated network resource will be permanently allocated when this type of bearer is established.

Table 4.2 – Standardized QoS Class Identifiers (QCIs) for LTE, copied from [60]

QCI	Resource type	Priority	Packet delay budget	Packet error loss rate	Example services
1	GBR	2	100 ms	10^{-2}	Conversational voice
2		4	150 ms	10^{-3}	Conversational video (live streaming)
3		3	50 ms	10^{-3}	Real time gaming
4		5	300 ms	10^{-6}	Non-conversational video (buffered streaming)
5	Non-GBR	1	100 ms	10^{-6}	IMS signaling
6		6	300 ms	10^{-6}	Video (buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice Video (live streaming) Interactive gaming
8		8	300 ms	10^{-6}	Video (buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9			

The QCI values were originally defined to support human-to-human communications; therefore, besides the IMS signaling, the voice traffic was associated with the highest priority. However, when integrating remote control communications which requires highest priority, we can re-define the QCI values with the highest priority assigned to this type of traffic. Since QCI is an 8-bit field, it can have 255 different values which are sufficient for the operator to specify various traffic types.

For example in table 4.3, we define a new QCI with associated QoS parameters for the remote control communication traffic with the highest priority (priority value equal to 1), delay budget of 100ms, and packet loss rate of 10^{-6}

Table 4.3 – Example of new QCI value for remote control communication traffic

QCI	Resource type	Priority	Packet delay budget	Packet loss rate	Services
1	GBR	1	100	10^{-6}	Remote control communications in distribution grid

In configuration stage, a dedicated bearer will be established and all the remote control communication over IEC 61850 MMS will be assigned into this bearer with the defined QCI value above. Based on the QCI values, the MAC scheduler can make the scheduling allocation based on the associated QoS parameters (see Figure 4.10)

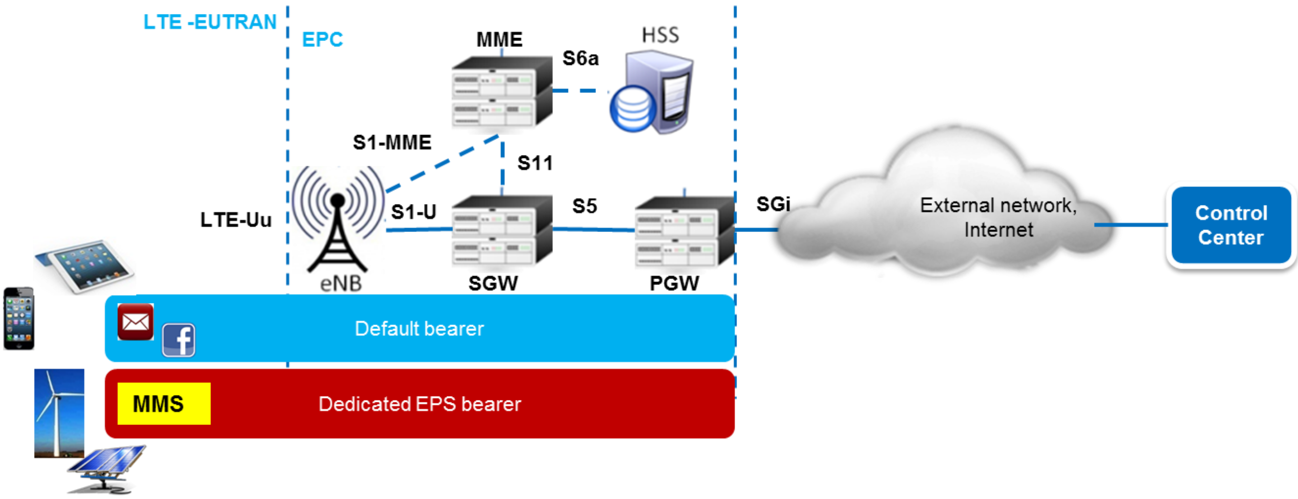


Figure 4.10 – LTE dedicated bearer for remote control communication

Depending on the scheduling algorithms, the MAC scheduler will handle the packet based on those QoS parameters such as priority, packet delay budget or packet error loss rate.

Table 4.4 summarizes the main aspects and targets of QoS-aware scheduling strategies according to reference [68]. These QoS-aware strategies use different algorithms to calculate the metrics which are used to decide which active flow will be allocated physical resources in such a way that the active flows with higher metrics will be scheduled before the ones with lower metrics.

The scheduling targets of these schedulers are basically fairness, target bit rate and bounded delay; therefore, they take the RLC head-of-line (HOL) delay and PF metric in constructing the metric calculation formulas. The objectives are to achieve the target bit rate for GBR traffic and packet delay budget. However, since these schedulers only aim to achieve the target bit rate and delay threshold for delay-sensitive applications, they do not have a mechanism to differentiate between remote control communications traffic and human-to-human communications traffic which contain all the rest such as real-time VoIP, video and best-effort traffic. As we can see in table 4.2 and table 4.3, remote control applications and voice, video streaming, interactive gaming have the same delay budget. And the delay budget for real-time gaming is even lower (50ms). In this situation, the remote control applications will not have higher priority in comparison to those human-to-human applications.

It is obvious as these schedulers are designed to ensure QoS-provisioning for one general type of traffic which is the human-to-human applications. Within our research scope, we consider two main different types of traffic: the remote control communications traffics and the human-to-human traffics with the assumption that the remote control applications are always received higher priority in comparison with human-to-human applications.

Table 4.4 – Main aspects and targets of QoS-aware scheduling strategies, based on [68]

Name	Scheduling target	Main Aspect
Priority Set Scheduler (PSS/PFsch) [70]	Fairness and target bit rate	- Joint Time Domain Packet Scheduling - TDPS and Frequency Domain Packet Scheduling - FDPS structure - PSS at TDPS to populate prioritized subset of users - PFsch at FDPS
[71]	Target bit rate	- Grouping GRB and non-GBR flows - One RB per iteration assigned to GBR users upon meeting GBR requirements - spare resources left to non-GBR
[72]	Target bit rate	- Priority-based ordering of GBR flows - All needed RBs upon meeting GBR requirement are allocated starting - from the user with the highest priority
Modified Largest Weighted Delay First (M-LWDF) [73]	Bounded delay	- LWDF scheduler for bounded delay - PF for channel awareness
Exponential - EXP/PF [74]	Bounded delay	- Exponential rule for bounded delay - PF for channel awareness
LOG rule [75]	Bounded delay	- Log rule for bounded delay - PF for channel awareness
Exponential (EXP) rule [75]	Bounded delay	- Exponential rule for bounded delay - PF for channel awareness
FLS [76]	Bounded delay	- Double-layer scheduler structure - Control law for resource preemption of real-time flows
[77]	Bounded delay and minimum guaranteed bit rate	- Cooperative game for distributing resources among different user sets - Resource allocation based on EXP rule with virtual token mechanism
Delay-prioritized scheduler - DPS [78]	Bounded delay	- Prioritization of delay-constrained flows depending on the urgency to be transmitted - All needed RBs upon meeting QoS requirement are allocated starting from the user with the highest priority
Required Activity Detection with Delay Sensitivity - RAD-DS/PFsch [79]	VoIP support	- Joint TDPS and FDPS structure - RAD-DS metric at TDPS depends on experienced delay and required QoS - PFsch at FDPS
VoIP Priority mode - VPM [80]	VoIP support	- Joint TDPS and FDPS structure - At the TDPS only VoIP flows can be scheduled in VoIP priority mode - Channel sensitive WFQ at the FDPS

Consequently, the existing channel/aware -QoS/aware scheduling algorithms summarized in survey [68] are not appropriate.

Therefore, we propose a new QoS-aware scheduling strategy: the Priority-aware Round Robin scheduler. Priority-aware or QoS-aware Round Robin scheduling strategy is based on the Round Robin mechanism with the extension of considering QoS-parameter for resource allocation. Concretely, the scheduler will calculate a metric for all active flows with the formula $m_{i,k} = \frac{c}{p_i}$ with $m_{i,k}$ is the metric for user i to be assigned resource block group k; c is a constant value; and p_i is the priority of the flow. The scheduler then compares the metric of all active users and set the maximum metric as m_{max}. If the metric of a flow is higher or equal to m_{max} then this flow will be assigned a RBG.

As we can see in table 4.2 and table 4.3, remote control communications traffics with priority = 1 will always have highest metric = c and will be assigned a RBG first. Therefore, the remote control communications traffics are always granted the best opportunities to access the network resources.

This scheduling strategy provides several advantages in term of main key design factors mentioned previously as follows.

Firstly, this scheduling strategy provides high level of simplicity since it only considers the priority-tag QoS parameter in resource allocation while these other scheduling strategies consider at least two QoS parameter in resource allocation as shown in table 4.5.

Secondly, the round robin scheduling provides the good fairness among the nodes within each prioritized group; therefore, all the devices to be controlled will receive the same opportunity for network access.

Last but not least, Priority-aware Round Robin scheduler provides a high level of QoS-provisioning since it implements a hard-priority mechanism by utilizing the priority-tag in distinguishing the remote control applications and normal human-to-human applications as well as making resource allocation decision based on the priority-tag.

Table 4.5 – Scheduling input parameters, based on [68]

Name	Requested bit rate	Instantaneous bit rate	Average data rate	Queue size	Max delay	HOL packet delay	Max packet loss rate	Past packet loss rate
Priority Set Scheduler (PSS/PFsch) [70]	X	X	X					
[71]	X	X						
[72]	X	X				X		
Modified Largest Weighted Delay First (M-LWDF) [73]		X	X		X	X		
Exponential - EXP/PF [74]		X	X		X	X		
LOG rule [75]		X	X		X	X		
Exponential (EXP) rule [75]		X	X		X	X		
FLS [76]				X	X			
[77]		X	X		X	X		
Delay-prioritized scheduler - DPS [78]		X			X	X		
Required Activity Detection with Delay Sensitivity - RAD-DS/PFsch [79]	X	X	X					
VoIP Priority mode - VPM [80]				X				X

In short, with the Priority-aware Round Robin scheduler, the MMS messages sent from the control centre to the MMS server nodes are always assigned highest priority meaning that they will be given the resources to be transferred before the traffic for other background nodes. It is very efficient in case of network resource limitation due to the increase of traffic or of users' number since the MMS traffics always have best chance to be served in comparison to other background traffic.

From the design algorithm of the Priority-aware Round Robin scheduler, it is obvious that the remote control application always have better chance to use more resources than the background traffic. It may lead to well-known problem of starvation for low priority traffics under the circumstance that the network resources are not enough and high priority flows consume too many resources. This is a drawback of Priority-aware scheduler; however, it is acceptable at least when we need to ensure the minimum performance requirements for high priority traffics. In our situation, because we assume that the remote control communications are mission-critical since they affect the safety of the electricity grid, the trade-off of starvation for low priority traffic is acceptable.

4.3 System composition

In section 4.1 we have discussed the overall architecture of the solution which is an integrated communication system with IEC 61850 MMS client and server entities interconnecting through the LTE architecture.

In section 4.2 the detailed design of the MMS communication stack and LTE MAC scheduler has been clarified to provide more insights of the proposed solution.

Figure 4.11 describes the detailed overall architecture of the solution with the communication stack used by MMS client/server and how they can be mapped over the LTE communication profile.

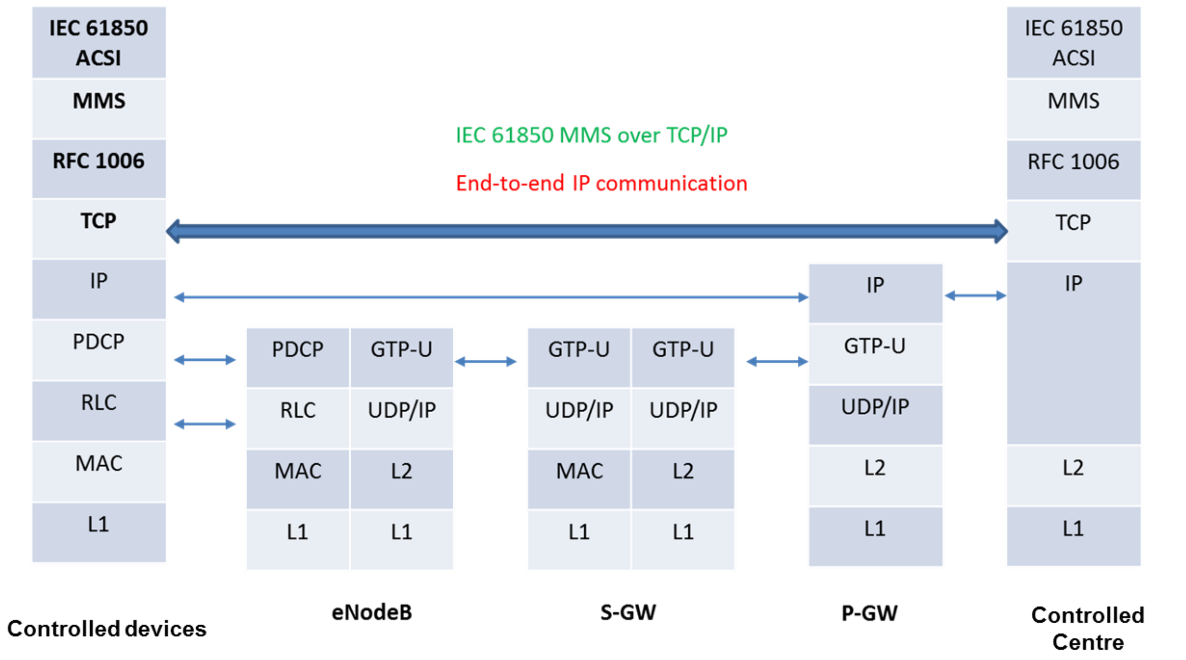


Figure 4.11 – Remote control communication system in distribution grid with the integration of 61850 MMS and LTE

The protocol layers of MMS communication stack have been described in section 4.2 as well as the communication stack of LTE has been mentioned in chapter 3. As discussed in chapter 2, the MMS communication stack supports the mapping to either TCP/IP or OSI communication profile.

Since LTE support the TCP/IP communication profiles, the MMS communication stack can be mapped over the LTE communication stack at the LTE terminals as shown in figure 4.11. These packets will then be encapsulated as LTE frames and be transmitted through the LTE radio access and core network. LTE support IP addressing scheme to allow the MMS messages to be sent to right destination.

Chapter 5

Implementation using ns3 LTE LENA simulation platform

In this chapter, the choice of NS3 LENA simulation environment is motivated, and then the implementation of the solution is discussed. The implementation of the models is based on the requirements, specifications and designs in chapter 4. This chapter partially answer question 2, and together with chapter 4 it completes the answer for the question. The implementation source codes for the MMS and background traffic modules can be found in [65] with installation guideline contained in [81]. The source codes for Priority-aware Round Robin scheduler can be found in [66] with installation guideline in Appendix.

5.1 Motivation of using NS3 LENA simulation tool

NS3 [53] is an open-source discrete-event network simulator, targeted primarily for research and educational use. NS3 is gaining more and more popularity compared to the long-established NS2. Like its predecessor NS2, NS3 relies on C++ for the implementation of the simulation models. However, NS3 no longer uses oTcl scripts to control the simulation, thus abandoning the problems which were introduced by the combination of C++ and oTcl in NS2. Instead, network simulations in NS3 can be implemented in pure C++, while parts of the simulation optionally can be realized using Python as well. One drawback of NS3 is that it is not backward compatible with NS2. Some NS2 models that are mostly written in C++ have been ported to NS3; however the oTcL-based models will not be ported as it would be equivalent to rewriting them.

The NS3 simulation core supports research on both IP and non-IP based networks. However, the large majority of its users focus on wireless/IP simulations which involve models for Wi-Fi, WiMAX, or LTE for layers 1 and 2 and a variety of static or dynamic routing protocols such as OLSR and AODV for IP-based applications.

If a simulator does not strictly comply with a real system model, it becomes really difficult comparing the results and validating the simulated model. NS3 tries to avoid excessive model approximations, so to have modules which can be efficiently reused. Like an empty computer case that needs to be filled with hardware and software, a node in NS3 needs one or more Network Interface Card (NIC) to be installed, IP protocol stack to be created and upper applications to be started.

Although NS3 is a very powerful tool, comprehending lots of features and models, most of them are not fully complete and working, and users are requested to adapt their needs to the actually implemented features, or to extend NS3 on their own.

A very good thing about open source software is the possibility to clone one project and start our own branch, modifying the code and adding features. Following this idea a new experimental, LTE-focused branch called LENA has been developed by CTTC [54]. This experimental branch is based on the developing branch on NS3, but uses a completely rewritten and enhanced model for LTE from the original one from NS3. Periodically the major release version of LENA is merged with the developing branch of NS3.

5.2 LTE model in LENA

An overview of the LTE-EPC simulation model is depicted in figure 5.1. The overall architecture of the LENA simulation model is comprised of two main components: LTE model and EPC model.

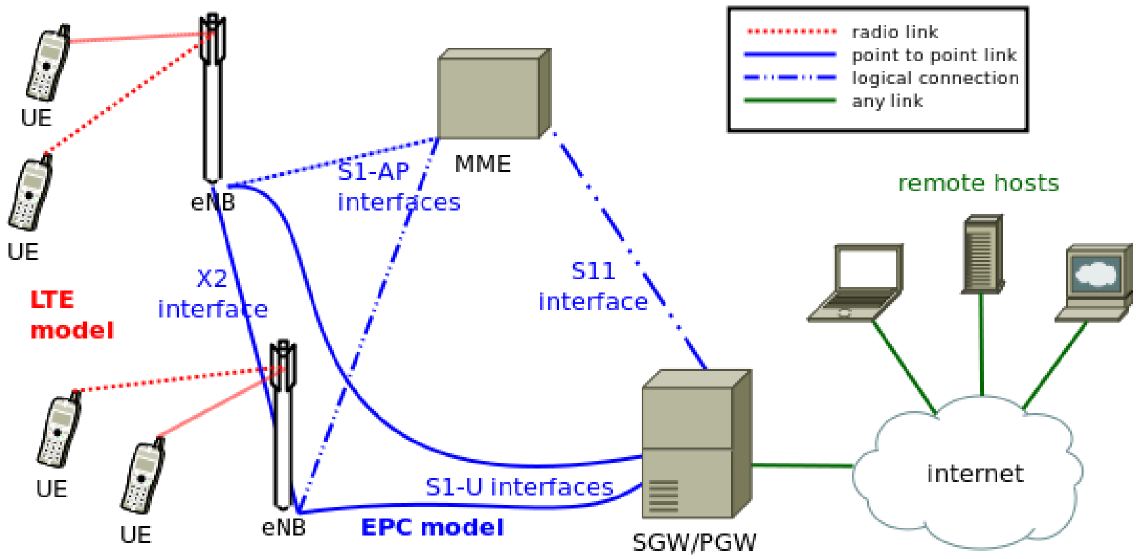


Figure 5.1 - LTE-EPC simulation model overall architecture, copied from [54]

5.2.1 LTE Model

This model includes the LTE Radio Protocol stack (RRC, PDCP, RLC, MAC, PHY). These entities reside entirely within the UE and the eNB nodes. LENA LTE model has been designed to support the evaluation of Radio Resource Management, packet scheduling, inter-cell interference co-ordination and dynamic spectrum access. To allow a correct evaluation of these aspects, LENA was modelled considering the following requirements [56]:

- At radio level, granularity of the model should be at least the one of a RB which is the fundamental unit used for resource allocation. Packet scheduling is done on a per-RB base, so an eNB can transmit only on a subset of the available RBs, possibly interfering with other eNBs transmitting on the same RBs: without a RB-fine granularity it would be impossible to accurately model inter-cell interference, nor packet scheduling. This leads to the adoption of a system level simulation approach, which evaluates resource allocation only at the granularity of call/bearer establishment..

- Simulator was intended to scale up to tens of eNBs and hundreds of UEs: this excludes the use of a link-level simulator, in which radio interfaces are modelled with a granularity up to the symbol level, and leads to huge computational complexity due to the need of implementing all the PHY layer signal processing. In fact, link-level simulators are normally limited to a single eNB and one or a few UEs.

- More than just one cell were thought to be possibly present in a simulation, and every cell had to be configurable with its own parameters, including carrier frequencies; moreover different bandwidths used by different eNBs should be allowed to overlap, thus supporting dynamic spectrum licensing; interference calculation had to be done appropriately in such a scenario.

- To be as close as possible to real-world implementations, the simulator should support the MAC Scheduler API published by the FemtoForum. This interface is expected to be used by manufacturers for the implementation of scheduling and Radio Resource Management (RRM) algorithms, so manufacturers will be able to test their equipment in a simulative scenario using the exact same algorithms that they would use in a real environment. The FemtoForum API is a logical specification only, and its implementation is left to the vendors. In LENA, the LTE simulation model has its own implementation of the API in C++.

- The simulator should be used to simulate IP packets flows, but in LTE scheduling and Radio Resource Management don't work directly with IP packets, but rather with RLC PDUs, obtained by segmentation and concatenation of IP packets done by the RLC entities; hence RLC functionalities had to be modelled very accurately.

5.2.2 EPC model

This model includes core network interfaces, protocols and entities. These entities and protocols reside within the SGW, PGW and MME nodes, and partially within the eNB nodes. SGW and PGW functionality are contained in a single SGW/PGW node, which removes the need for the S5 or S8 interfaces specified by 3GPP. On the other hand, for both the S1-U protocol stack and the LTE radio protocol stack all the protocol layers specified by 3GPP are present.

The EPC model has several design criteria:

- The only PDN supported type is IPv4;
- S-GW and P-GW functionalities are encapsulated within a single node, referred as S-GW/P-GW node;
- inter-cell mobility is not implemented, hence just a single S-GW/P-GW node is defined;
- any standard NS3 application working over TCP or UDP must work with EPC, so to be able to use EPC to simulate end-to-end performance of realistic applications;
- it is possible to define more than just one eNB, every one of which with its own backhaul connection, with different capabilities; hence data plane protocols between eNBs and S-GW/P-GW had to be modelled very accurately;
- it is possible for a single UE to use different applications with different QoS requirements, so multiple EPS bearer should be supported (and this includes the necessary TCP/UDP over IP classification made on the UE for uplink traffic and on eNB for downlink traffic);
- accurate EPC data plane modelling is the main goal, while EPC control plane was to be developed in a simplified way;
- main objective for EPC simulations is the management of active users in ECM connected mode, so all the functionalities that are relevant only for ECM idle mode (i.e. tracking area update and paging, . . .) are not modelled at all;
- The model should allow the possibility to perform an X2-based handover between two eNBs.

Figure 5.2 shows the LTE-EPC data plane protocol stack as it has been implemented in LENA.

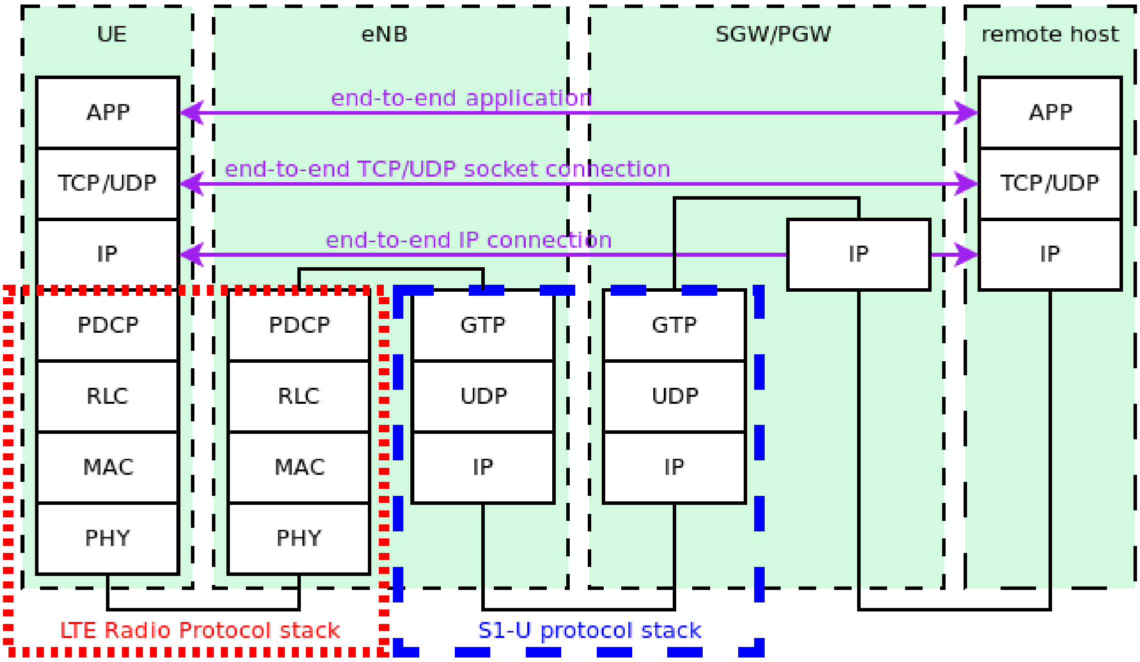


Figure 5.2 - LTE-EPC data plane protocol stack, copied from [56]

The readers are advised to refer to the Design Documentation of LENA [56] for more details about the design criteria and implementation of the LTE and EPC models in LENA.

5.3 MAC scheduler

5.3.1 Round Robin scheduler

The Round Robin (RR) scheduler divides the network resources among the active flows, i.e. those logical channels which have non-empty RLC queue. If the number of Resource Block Group (RBG) is greater than the number of active flows, all the flow can be allocated in the same sub-frame. Otherwise, if the number of active flows is greater than the number of RBGs, not all the flows can be scheduled in a given sub-frame; then, in the next sub-frame the allocation will start from the last flow that was not allocated. The Modulation and Coding Scheme (MCS) to be adopted for each user is done according to the received wideband Channel Quality Indication – CQIs.

Figure 5.3 shows how the Round Robin interfaces are used within the eNodeB. For more details, please refer to the reference [56].

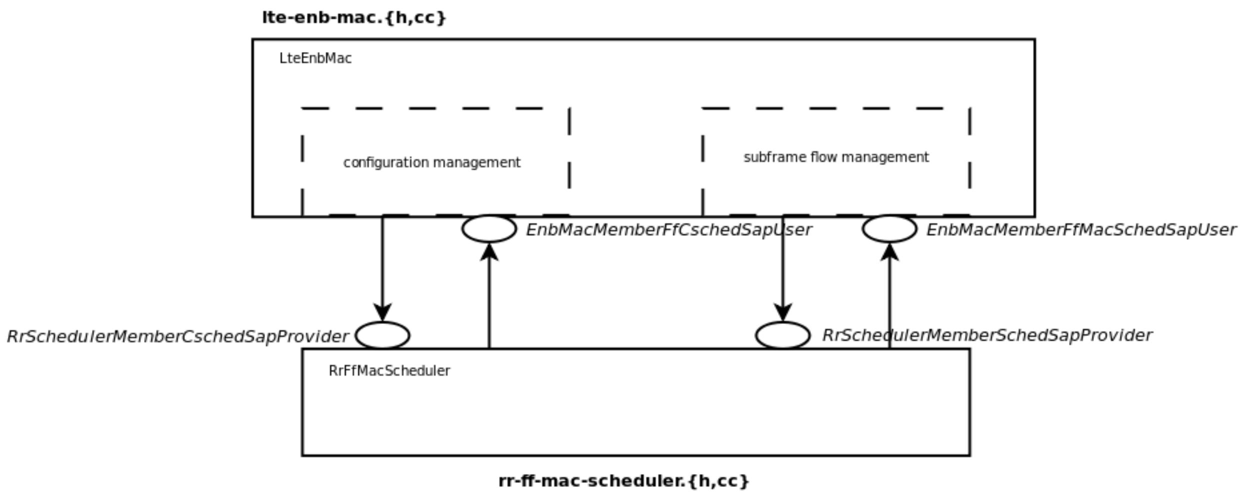


Figure 5.3 – Round robin scheduler Interface implemented in LENA, copied from [56]

There are 3 blocks involved in the MAC Scheduler interface: Control block, Sub-frame block and Scheduler block. In NS3 LENA, the specific version of the FemtoForum MAC Scheduler Interface as a set of C++ abstract classes; in particular, each primitive is translated to a C++ method of a given class [56]. The primitives in FemtoForum MAC Scheduler are grouped in two groups: the CSCHED primitives, which deal with scheduler configuration, and the SCHED primitives, which deal with the execution of the scheduler.

In figure 5.3 we can see that the User side of both the CSCHED SAP and the SCHED SAP are implemented within the eNB MAC, i.e., in the file lte-enb-mac.cc. In order to interact with the MAC of the eNB, the Round Robin scheduler implements the Provider side of the SCHED SAP and CSCHED SAP interfaces. A similar approach can be used to implement other schedulers as well [56].

5.3.2 Priority-aware Round Robin scheduler

This is an enhanced implementation of the normal Round Robin scheduler which takes the prioritization into account. A dedicated EPS bearer is established with the QoS parameters defined in table 5.1. The MMS remote control communication traffics are assigned to this dedicated bearer.

The background traffics are assigned to other bearers with respect to the standardized QoS parameters specified in table 5.1.

The Priority-aware Round Robin scheduler will assign the metrics to different active flows based on the priority tag in such a way that the flow with lowest priority value (priority = 1) will have the highest metrics. Within a sub-frame, the flows with highest metric values will be allocated the RBGs first. If in a sub-frame, the number of flows is less than the number of RBGs, the MMS flows will be allocated more RBGs since the RBGs are allocated in a cyclical manner.

Table 5.1 – New QCI values

QCI	Resource type	Priority	Packet delay budget	Packet loss rate	Services
1	GBR	1	100	10^{-6}	Remote control communications in distribution grid
2	GBR	3	100	10^{-2}	Conversational voice
3	GBR	5	150	10^{-3}	Conversational video (live streaming)
4	GBR	6	300	10^{-6}	Non-conversational video (buffered streaming)
5	GBR	4	50	10^{-3}	Real-time gaming
6	Non-GBR	2	100	10^{-6}	IMS signaling
7	Non-GBR	8	100	10^{-3}	Voice, video (live streaming), interactive gaming
8	Non-GBR	7	300	10^{-6}	Video (buffered streaming)
9	Non-GBR	9	300	10^{-6}	TCP-based (web browsing, email, ftp…)
10	Non-GBR	10	300	10^{-6}	

The Priority-based MAC scheduler inherits from the primitives in FemtoForum MAC scheduler implemented by LENA which is the `ns3::FfMacScheduler` class. The `ns3::FfMacScheduler` class provides the CSCHED primitives, which deal with scheduler configuration, and the SCHED primitives, which deal with the execution of the scheduler.

5.4 IEC 61850 MMS model

The MMS protocol stack for the MMS client and MMS server model are based on the technical specifications and design that have been described in chapter 4. The overall implementation of the modules is shown in Figure 5.4

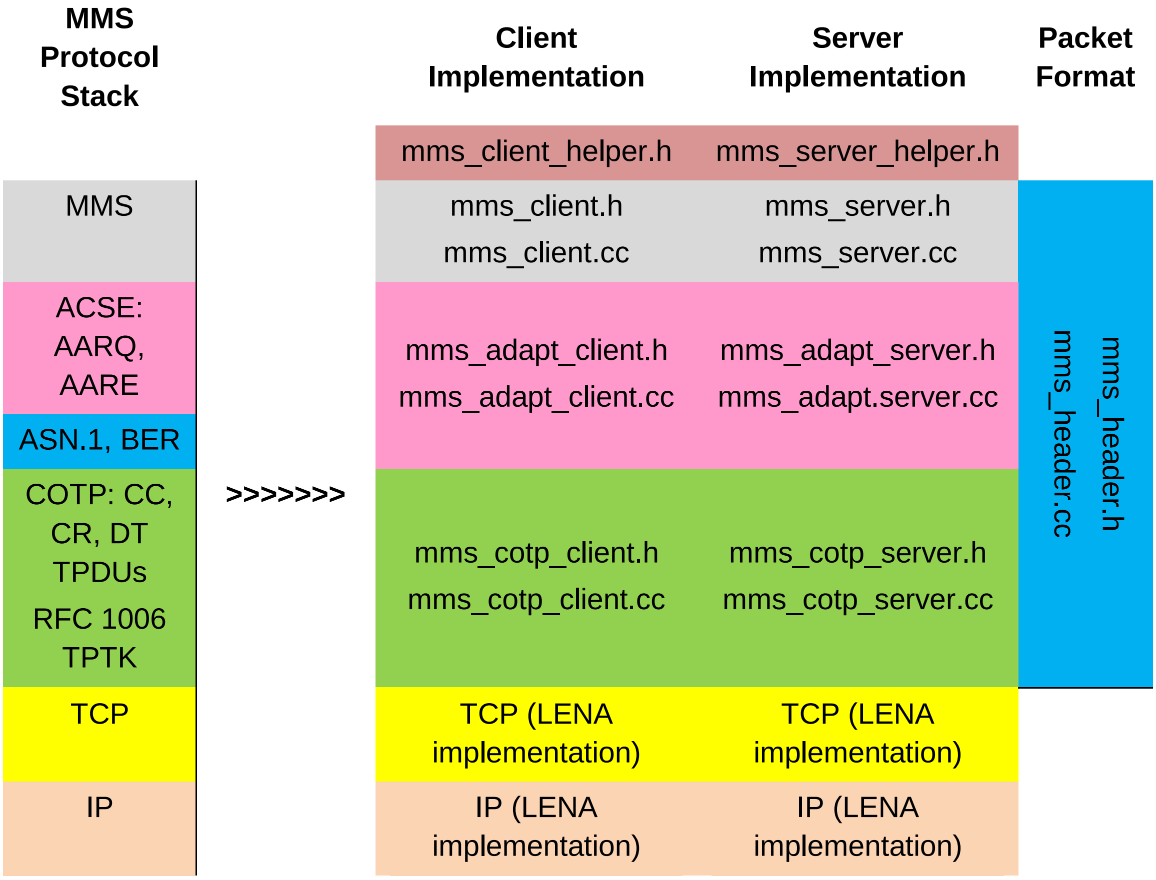


Figure 5.4 - Implementation of the MMS protocol stack for MMS client and MMS server

We reuse the existing TCP/IP stack that have been implemented in NS3 LENA and have written two different NS3 LENA applications to simulate the interaction between a MMS client and a MMS server, following the message flow in figure 4.4. The packet format for different layers is implemented in a single, common `mms_header` module that can be referenced by other module implementations.

5.4.1 mms_cotp_client module

On the client side, the `mms_cotp_client` module takes care of the COTP establishment to simulate the transport of ISO protocol on top of TCP sockets. It also provides data service for the transport of upper layer protocol.

When a client wants to setup the association with the MMS server, the `mms_cotp_client` module sends out the COTP CR (connection request) message to the server and waits for the COTP CC (connection confirm) message from the server.

When the COTP CC message is received, the `mms_cotp_client` module notifies the upper layer that the COTP connection has been established.

The `mms_cotp_client` module is also responsible for the COTP DT (data) message that carries the upper layper protocol data unit.

5.4.2 mms_adapt_client module

The `mms_adapt_client` module is used to construct the application protocol data unit (APDU) packets. Specifically, the `mms_adapt_client` module constructs the AARQ (Application Association Request) header when it receives the INITIATE-REQUEST from the MMS client which wants to associate with a MMS server.

After the PDU is constructed, it is sent to the COTP layer (the `mms_cotp_client` module) and waits for the AARE (Application Association Response) from the COTP layer which indicates the MMS server has agreed with the association.

When the AARE packet has been received, the `mms_adapt_client` module notifies the upper MMS layer to receive the INITIATE-RESPONSE packet. After the initiation is complete, the client and server can exchange the MMS data.

5.4.3 mms_client module

The `mms_client` module is responsible for the setup of the association with MMS server, and provides MMS data polling using MMS read/write services. It makes requests to the `mms_adapt_client` module to complete these tasks.

In specific, the following services are implemented:

- INITIATE-REQUEST: the `mms_client` module makes a request to the `mms_adapt_client` module to construct a PDU to simulate the INITIATE-REQUEST packet to send to the MMS server.
- INITIATE-RESPONSE: the `mms_client` module receives the notification from the lower layer (the `mms_adapt_client` module) that the MMS association is complete.
- CONFIRMED-REQUEST: the `mms_client` module makes a request to the `mms_adapt_client` module to construct an APDU to simulate the CONFIRMED-REQUEST packet (the MMS READ/WRITE service packet) to send to the MMS server.

- CONFIRMED-RESPONSE: the `mms_client` module receives the notification from the lower layer (the `mms_adapt_client` module) that the MMS data response has been received.

5.4.4 mms_cotp_server module

On the server side, the `mms_cotp_server` module takes care of the COTP establishment to simulate the transport of ISO protocol on top of TCP sockets. It also provides data service for the transport of upper layer protocol.

When the `mms_cotp_server` module receives COTP CR (connection request) message from the TCP sockets, it replies with the COTP CC (connection confirm) message.

The `mms_cotp_client` module is also responsible for the COTP DT (data) message that carries the upper layper protocol data unit.

5.4.5 mms_adapt_server module

The `mms_adapt_server` module is used to construct the application protocol data unit (APDU) packets. Specifically, the `mms_adapt_server` module notifies the MMS layer when the AARQ (Application Association Request) packet has been received. When it receives the INITIATE-RESPONSE from the MMS layer, it encapsulates the AARE header to the packet and send to the COTP layer (the `mms_cotp_server` module).

5.4.6 mms_server module

The `mms_server` module is responsible for the setup of the association with MMS server, and provides MMS data polling response using MMS read/write services. It makes requests to the `mms_adapt_server` module to complete these tasks.

In specific, the following services are implemented:

- INITIATE-REQUEST: the `mms_server` module receives the notification from the lower layer (the `mms_adapt_server` module) that the MMS association response is needed.

- INITIATE-RESPONSE: the `mms_server` module makes a request to the `mms_adapt_server` module to construct a PDU to simulate the INITIATE-RESPONSE packet to send to the MMS client.

- CONFIRMED-REQUEST: the `mms_server` module receives the notification from the lower layer (the `mms_adapt_server` module) that the MMS data request has been received and there is a client waiting for the response.

- CONFIRMED-RESPONSE: the `mms_server` module makes a request to the `mms_adapt_server` module to construct an APDU to simulate the CONFIRMED-RESPONSE packet (the MMS READ/WRITE response packet) to send to the MMS client.

5.4.7 mms_header module

The packet format for different layers is implemented in a single, common `mms_header` module. In particular, the formats for the different packet types are implemented (from lower layers to the top) in the module:

- TPTK header
- COTP CR/CC packets, COTP DT header
- AARQ/AARE header
- MMS INITIATION-REQUEST, MMS INITIATION-REPONSE, MMS CONFIRMED-REQUEST (Read service, Write service requests), MMS CONFIRMED-RESPONSE (Read service, Write service response).

We group the implementation of the packet format in a single module so that it can be reference by all the implemented modules that have been described.

5.4.8 mms_client_helper and mms_server_helper modules

Following NS3 development guidelines, some additional code have been written (the `mms_client_helper` and `mms_server_helper` modules) to simplify the described applications use. Helper s cover a key role in developing a successful NS3 applications, providing a user-friendly interface to setup applications, automatically configuring all the mandatory attributes and supplying an easy way to modify all the configurable attributes. Moreover, helpers make it possible to easily install defined applications into nodes.

5.4.9 Module ouput

The implemented MMS model can provide two different types of traces. The first option is the ASCII trace output which allows the usage of a text processing application (such as

AWK) for data analysis. The second option is the PCAP (packet capture) trace output which can be opened and analysed in a packet analyser, such as Wireshark [56]. Figure 5.4 shows the PCAP of the MMS traffic between a MMS client and a MMS server displayed in Wireshark.

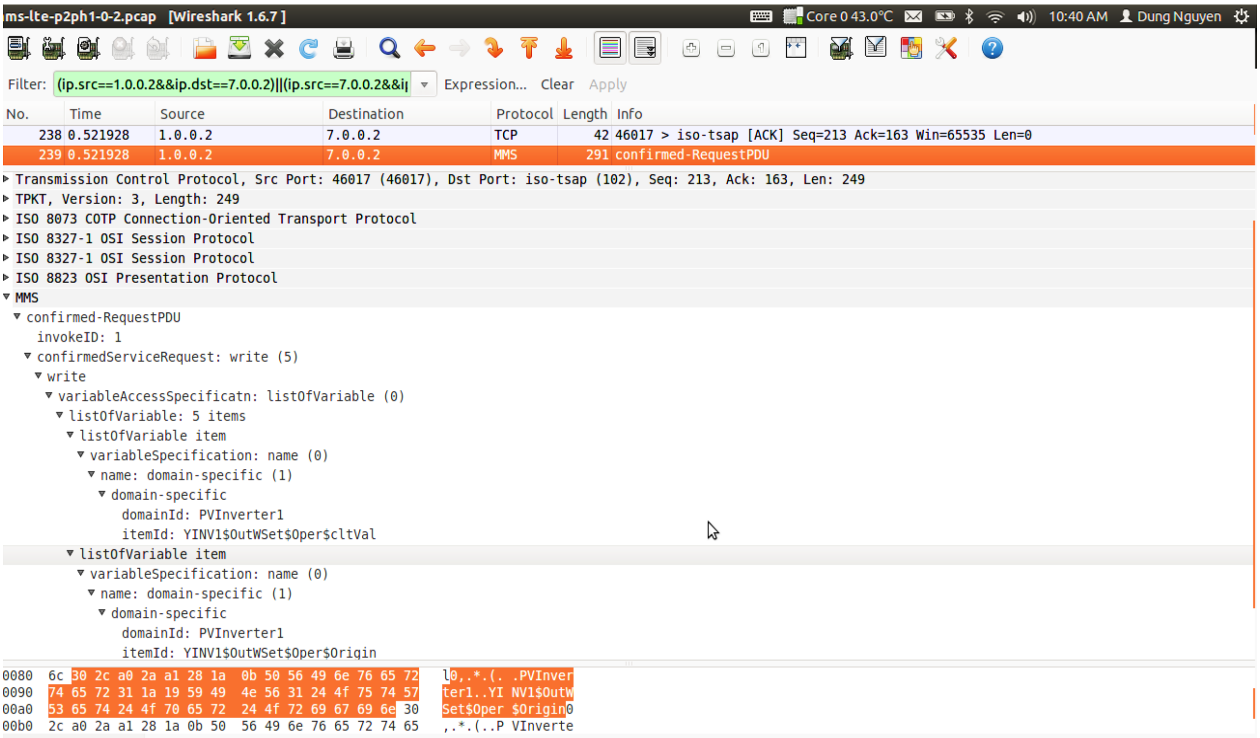


Figure 5.5 - PCAP trace output of the MMS traffic model in LENA

5.5 LTE background traffic

As one of the main goals of the research is to investigate the mutual impacts between IEC 61850 MMS traffic for smart meter communication and existing LTE services traffic, the LTE background traffic models has to be considered for the performance verification.

In this thesis, we use the traffic mix specified in [59], [60] which are given in Table 5.2

Table 5.2 – Traffic models mix

Application	Traffic category	Percentage of users
VoIP	Real-time	30%
FTP	Best effort	10%
Web browsing / HTTP	Interactive	20%
Video streaming	Streaming	20%
Gaming	Interactive real-time	20%

5.5.1 Voice-over-IP (VoIP) traffic model

A simple two-state voice activity model is considered, see figure 5.6. The probability of transitioning from state 0 (silence or inactive state) to state 1 (talking or active state) is α while the probability of staying in state 0 is (1−α). On the other hand, the probability of transitioning from state 1 to state 0 is denoted β while the probability of staying in state 1 is (1−β). The updates are made at the speech encoder frame rate R=1/T, where T is the encoder frame duration (typically 20ms).

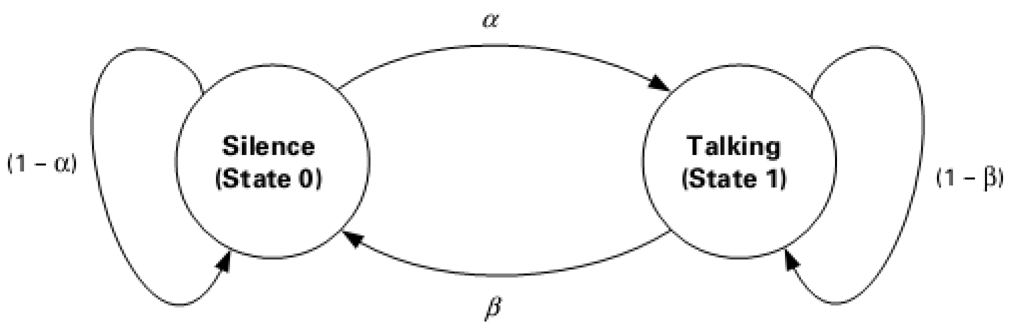


Figure 5.6 – Two-state voice activity model, copied from [60]

The voice activity factor (VAF) is the probability of being in the talking state, that is, state 1: $VAF = P_1 = \frac{\alpha}{\alpha+\beta}$

We also assume the VoIP application uses RTP AMR 12.2 Voice codec, with voice payload size of 40 bytes during talk time. A Silence Insertion Descriptor (SID) packet consisting of a total of 15 bytes is transmitted every 160ms (or equivalent of 8 voice frames) during silence periods.

5.5.2 FTP traffic model

An FTP session is a sequence of file transfers separated by reading times. The two main FTP session parameters are the size S of a file to be transferred and the reading time D, i.e. the time interval between the end of the download of the previous file and the user request for the next file. The same model applies to both downlink and uplink.

5.5.3 Web browsing HTTP traffic model

The session is divided into active and inactive periods representing web-page downloads and the intermediate reading times. A web-browser will begin serving a user's request by fetching the initial HTML page using an HTTP GET request which contains a number of the embedded objects. The session is divided into active and inactive periods representing web-page downloads and the intermediate reading times. These active and inactive periods are a result of human interaction where the packet call represents a web user's request for information and the reading time identifies the time required to digest the web-page [68].

5.5.4 Video streaming traffic model

We assume that each frame of video data arrives at a regular interval T determined by the number of frames per second. Each video frame is decomposed into a fixed number of slices, each transmitted as a single packet. The size of these packets/slices is modelled as a truncated Pareto distribution. The video encoder introduces encoding delay intervals between the packets of a frame. These intervals are also modelled by a truncated Pareto distribution. The video source rate of 64 Kbps is assumed, see [60].

5.5.5 Interactive gaming traffic model

The interactive gaming traffic model parameters for the uplink and downlink are given in [68], where an initial packet arrival time is uniformly distributed between 0 and 40ms. The packet size for both the downlink and uplink traffic is modelled using the largest extreme value distribution (also known as Fisher-Tippett distribution). The packet arrival time for the uplink is deterministic (40ms), while for the downlink it is modelled using the largest extreme value distribution [60].

5.5.6 Implementation of background traffic in NS3 LENA

The implementation of different LTE background traffic types is conducted based on the TCP/UDP implementation in NS3 LENA.

FTP traffic model has been implemented by making some extension from the built-in *BulkSendApplication* to allow file size to follow the statistical distribution mentioned in [67], [68]. This is done with the `<ns3/random-variables.h>` module of NS3 LENA which provides the implementation for generating different types of random variables (Uniform, Log-normal, Pareto, etc.).

We use the HTTP traffic model implementation described in [61], where we have also used `<ns3/random-variables.h>` module to adapt the HTTP parameters.

The same approach is used for the implementation of traffic types on top of UDP (VoIP, video, gaming). We have created a new NS3 LENA application named `gen-udp` to generate these UDP traffic types. `gen-udp` has been developed based on the *UDPClientServer* application shipped with NS3 LENA in conjunction with the mentioned random variables library. To facilitate the writing of simulation script, the syntax for defining these traffic types is made the same using the helpers `GeneralUdpClientHelper` and `GeneralUdpServerHelper`, with different parameter `type` values to distinguish between them.

5.6 Controllable electrical devices and control centre

As mentioned before, the modular design of the NS3 LENA requires different components (network interface, IP stack, application, etc.) to be installed on an existing empty node to make it a functional device. Therefore, the LTE controllable electrical devices are implemented as nodes with IP stack configured using `InternetStackHelper`. The network interface, LTE stack and IP address are configured for the node using `LteHelper` and `EpcHelper` of NS3 LENA. After that, the MMS server communication stack described in section 5.3 is installed on the node using `MmsServerHelper`.

The control centre is implemented in NS3 LENA as a node connecting to the P-GW of the LTE network through a point-to-point link. The control centre is configured with IP stack and MMS server communication stack described in section 5.3 using `MmsClientHelper`.

5.7 LTE background UEs and remote hosts

Similar to the smart meters and MDMS hosts implementations, the background UEs have LTE network interface, IP stack and LTE stack installed. After that, different applications mentioned in section 5.5 are installed on the nodes. We follow the same approach for the remote hosts of different traffic types.

Chapter 6

Experiments and Evaluation

Chapter 6 describes the simulation experiments and evaluation of the results in order to answer the research question 3 that whether the Priority-aware Round Robin scheduler can fulfill the performance and prioritization requirements for remote control communication in electricity distribution grid. This chapter is organized as follows:

Section 6.1 presents the general setup for the experiments including the network topology, the simulation parameters, and the metrics used to evaluate the performance of the network. Section 6.2 shows the simulation results with the specific analysis.

6.1 Simulation description

This section describes the simulation topology, explains the simulation parameters used for the simulation experiment and finally shows the metrics that will be used to evaluate the performance of the solution.

6.1.1 Simulation topology

The goal of the experiments is to evaluate the performance of the remote control communications while exchanging over the LTE network, and the impact of this new traffic type to the existing LTE network in two cases: with normal Round Robin MAC scheduler and with Priority-aware Round Robin scheduler.

Because the electrical devices to be controlled such as the wind turbine, PV panel are fixed, a static network topology will be considered. Because handover is a related issue, it is desired to consider a single cell topology for simplicity.

Since we also assume the background traffic generated by normal LTE subscribers in the network, the network topology includes both the controllable electrical nodes, or the MMS nodes, and other UE nodes. All the nodes are uniformly distributed in a dish-shape area with the radius of 2 km which is typical for sub-urban area.

The control centre aggregates the traffic from plentiful MMS nodes; hence, it will not be connected to the LTE network via the radio interface. Instead, the control centre maintains a high-speed point-to-point connection to the Evolve Packet Core – EPC of the LTE network. All the MMS nodes are connected to the control centre through the LTE access network and core network.

When using the Round Robin scheduler, both MMS traffics and background traffics are assigned to the default bearer. The RR scheduler will take no action regarding the QoS. Figure 6.1 shows the network topology and configuration when the RR scheduler is applied.

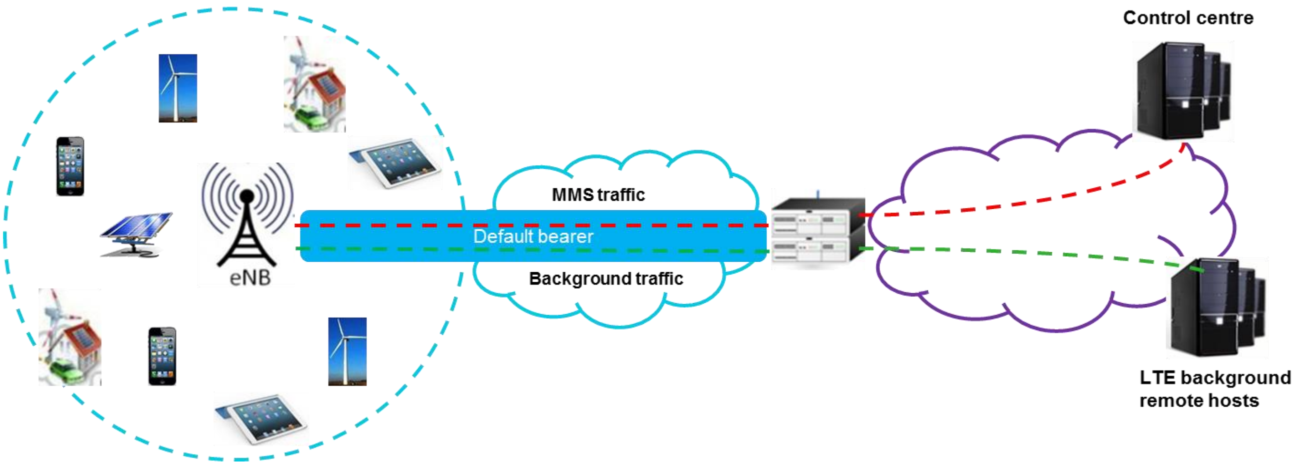


Figure 6.1 – Simulation topology and configuration when using Round Robin scheduler

When the Priority-aware Round Robin scheduler is used, different dedicated bearers are established with related QoS parameters. The Priority-aware Round Robin scheduler create the metrics for each traffic types based on the priority values following a rule that the lower the priority value (meaning higher priority), the higher the metric. And the traffic flows with highest metrics will have the first opportunities to receive the network resource. The simulation topology and network configuration when using Priority-aware Round Robin scheduler is illustrated in Figure 6.2

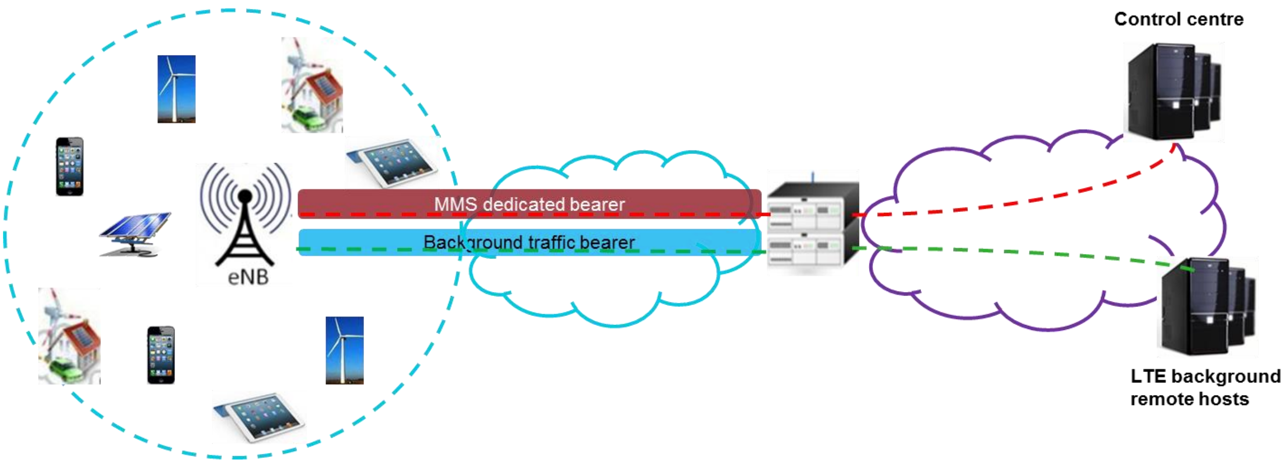


Figure 6.2 – Simulation topology and configuration when using Priority-aware Round Robin scheduler

The critical difference between figure 6.1 and figure 6.2 involves the establishment of the EPS bearers.

In figure 6.1 all types of traffic are mapped to the default bearer. It means all types of traffic will have the same QoS parameters (or no QoS parameters at all). In other words, they will be treated equally by the network. We implement this network topology with Round Robin scheduler since Round Robin scheduler does not take into account any QoS parameter in its scheduling decision. All traffic flows are treated equally by the Round Robin scheduler in a cyclic manner.

In contrast to the Round Robin scheduler, the Priority-aware Round Robin scheduler firstly considers the priority tag, which is an important QoS parameter for resource allocation. Therefore, in figure 6.2 we see there are two different bearers with different configure QoS parameters. The MMS dedicated bearer is established to map all the MMS traffic and assign high priority-tag to this traffic type. Other traffic is mapped to the other background traffic bearer with lower priority-tag. Therefore, MMS traffic with priority-tag with be considered by the Priority-aware Round Robin scheduler and gets served before other traffic types in a TTI.

In figure 6.2 we see one background traffic bearer; however, there can be multiple bearers for each background traffic type if we want to apply different priorities for the background traffic too.

6.1.2 Simulation parameters

The configuration of simulation parameters are summarized in table 6.1. All the parameters are typical for the LTE release 8 which is implemented in the ns-3 lena M5 simulation environment.

The channel bandwidth used is 5 MHz for two reasons. Firstly, it is the one of the two most popular bandwidths (with the 10MHz bandwidth) that has been implemented by the LTE network operators in reality. Secondly, an extra goal of this research is to provide a reference for Alliander, a large-scale energy distribution network, to compare with their CDMA450 network which uses the 3 MHz channel bandwidth. Therefore, the 5 MHz is more comparable to the 3 MHz bandwidth of CDMA450.

MIMO 2x2 is also applied in the network since it is the advanced technology designed to upgrade the data rate as well as the quality of LTE traffic.

The cell radius of 2km is chosen since the DERs are usually located in sub-urban area.

Table 6.1 – Simulation parameters

Parameters	Values
Uplink bandwidth	5MHz (25 RBs)
Downlink bandwidth	5MHz (25 RBs)
Uplink EARFCN	21100 band7 (2535MHz),
Downlink EARFCN	3100 band 7 (2655MHz),
CQI generation period	10ms
Transmission mode	MIMO 2x2
UE transmission power	26dBm
UE noise figure	5dB
eNB transmission power	49dBm
eNB noise figure	5dB
Cell radius	2000m (typical sub-urban case)

6.1.3 Performance metrics

In the experiments several metrics will be used for performance evaluation. These metrics are presented as follows:

6.1.3.1 Average delay

Delay is the most important metric to consider in the experiments as it relates directly to the performance requirements specified in chapter 3. There are two type of delay for the MMS traffic:

- *Initiation delay*: time from the start of the connection setup until Initiate-Response is received at the client
- *Request delay*: time from the start of the polling request until a response is received at the client

The average delay is measured at MMS layer by using the PCAP trace file generated after running the experiments.

6.1.3.2 Average throughput

The average throughput shows how much data is successfully transmitted over the LTE network. It is calculated as the total data received by the UE in the downlink over the simulation time.

The average throughput is measured as bit/s (bps).

6.1.3.2 Downlink packet loss ratio

The downlink packet loss ratio shows the reliability of the communication link. The downlink packet loss ratio is calculated using the following equations:

$$\mathrm{PLR(DL)} = \frac{packets\_sent\_by\_eNB \; - \; packets\_received\_by\_UE}{packets\_sent\_by\_eNB}$$

Downlink packet loss ratio is measured at PDCP layer by using the PDCP trace file which is a standard tracer of LENA.

6.2 Simulation experiments

The simulation experiments are conducted in ns-3 lena simulation environment with the modules designed and implemented as shown in chapter 4 and chapter 5. The main objective of the experiments is to verify the performance of the IEC 61850 MMS and LTE integration with Priority-aware Round Robin scheduler solution to support remote control communication in electricity distribution grid.

6.2.1 Experiment scenario

6.2.1.1 Traffic mix experiments

In order to evaluate the impact of integrating IEC 61850 MMS remote control communication traffic in a public LTE network, we will assume different traffic mix with the percentage of background traffic (in Kbps) over remote control traffic (in Kbps) such as 80/20, 60/40.

In each experiment with a specific traffic mix, the number of MMS nodes and background nodes will be increased but the mix is remained. Therefore, some extra experiments have to be done first, in order to find the number of background nodes and MMS nodes that combines together to create a specific traffic mix.

For the MMS traffic, we assume that the control centre sends a control request to the MMS nodes and waits for the response. If the response is positive then the control centre sends a new control request. It is applied for a real-time control algorithm in which the control centre performs real time control function to all the controllable electrical devices.

For the background traffic, it follows the mix of 5 different traffic types (VoIP, Gaming, Video, Web, and FTP) with the percentage of nodes defined in table 4.1. Due to this background traffic mix, the number of background node will start at 10 (to have integer value of the number of each type of node: 1 FTP user, 2 HTTP users, 2 gaming users, 2 video streaming users and 3 VoIP users.)

Then the number of background node will be increased by 10 to keep the integer number of each node type. The corresponding number of MMS nodes will also be increase under the condition that it will keep the traffic mix defined for each experiment. The following steps are conducted to generate the traffic mix and conduct the experiments:

- *Step 1:* set the background traffic users at the lowest 10 users, so we have 1 FTP user, 2 HTTP users, 2 gaming users, 2 video streaming users and 3 VoIP users.
- *Step 2*: set the number of electrical nodes, run the simulation and store the throughput of the background traffic and remote control communication traffic.
- *Step 3*: calculate the background traffic/remote control communication percentage mix.
    - If the mix is less than the desired value, increase the number of electrical nodes and repeat step 2.
    - If the mix is more than the desired value, decrease the number of electrical nodes and repeat step 2.
    - (We assume the mix equals to the desired value if the difference is below or equal to 5% of the desired value)
- *Step 4*: If the total traffic is lower than the maximum utilization of the scenario, increase the number of background users to 20, 30, 40, etc. and repeat step 1.

For each traffic mix experiment type, two different sets of experiment will be conducted with the Round robin and Priority-aware Round robin scheduler to compare the performances in two cases.

We assume a utilization of about 80% meaning that the operator will have 20% of the capacity for backup purpose. Besides the 80/20 traffic mix that the total traffic load will be increased until it reaches the maximum capacity of the LTE network, other traffic mix experiment will be applied the 80% utilization.

The PDCP trace files, log files and PCAP files generate after each simulation will be stored to calculate the result and draw the graphs.

6.2.1.2 Traffic overload experiment

The objective of this set of experiments is to evaluate the performance enhancement, in terms of delay and throughput, of Priority-aware Round Robin Scheduler when the total traffic load exceeds the maximum capacity of the LTE-network.

In the 80/20 traffic mix experiment, when the total traffic mix reach the maximum capacity of the LTE network we will keep increasing the total traffic load by keeping the number of MMS nodes while increasing the number of background nodes.

This experiment makes sense for the situation when the number of LTE subscribers increases due to the explosion of LTE-supported handheld devices or in special situation when the number of LTE subscribers suddenly increases in a short period of time, for example during a festival time.

6.2.2 Confidence interval

The experiment is repeated with the same traffic mix and different random seed to be able to provide reliable results.

The measured sample values from the experiment runs are used to compute the mean value of a metric with a confidence interval for this mean. The confidence interval is computed using a Student test or t-test [61]. The confidence interval is defined as:

$$(\bar{y} - \frac{t_{\frac{\alpha}{2},N-1} S}{\sqrt{N}}, \bar{y} + \frac{t_{\frac{\alpha}{2},N-1} S}{\sqrt{N}})$$

where $\bar{y}$ is the sample mean, S is the sample standard deviation, N is the sample size, is the desired significance level, and $t_{\frac{\alpha}{2},N-1}$ is the upper critical value of the (Student) t distribution with N-1 degrees of freedom.

In the experiments, a confidence interval of 95% will be used, and half the confidence interval should be less than 5% of the sample mean value.

After a batch has been performed, the traffic mix is changed and the experiment is repeated. This is done until all traffic mix scenarios have been simulated.

6.2.3 Experiment results and evaluation

The experiment results were collected by using the standard lena tracers and some generated log files for the designed and implemented traffic modules. The results are collected in text-based and pcap-based format and then are analysed to derive different graphs as shown in the coming sections.

6.2.3.1 80/20 traffic mix experiment

For this traffic mix, we start with the number of background node of 10 and find out the number of MMS nodes that generate the traffic load equal to approximately 20% of the total traffic load generated by both MMS nodes and background nodes. Then we increase the number of background node with step of 10. The number of MMS node will be increased to meet the condition that the traffic mix is always 80/20.

This traffic mix is quite reasonable because in the meantime, the number of controlled nodes in distribution grid is quite low while the number of LTE subscriber is increasing fast with the explosion of LTE-supported smart phones.

Since we only focus on the downlink from the control centre to the MMS server nodes which generates most of MMS traffic, only the results in downlink are collected and analyzed.

6.2.3.1.1 Average Throughput

Average throughput is an important metric to evaluate the performance of the network. Figure 6.3 shows the average throughput performances including the overall average throughput, background average throughput and MMS average throughput.

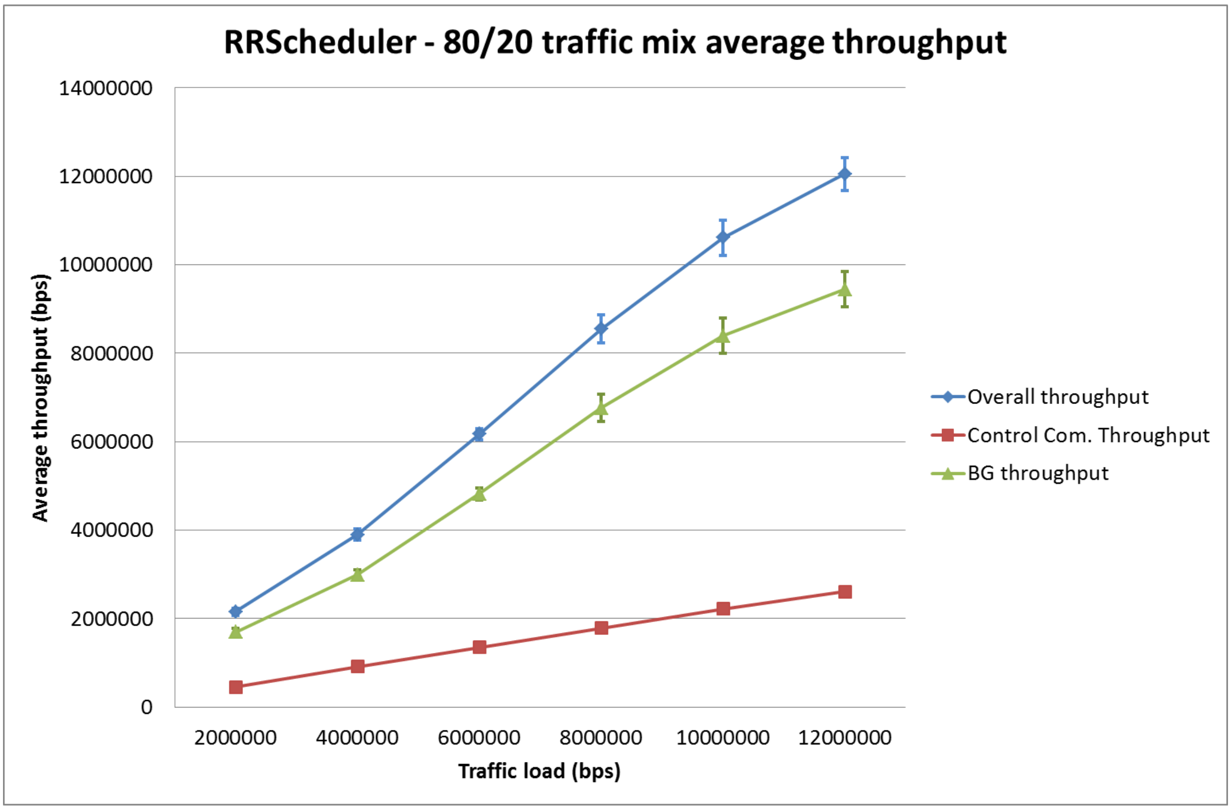


Figure 6. 3 – Average throughput performance in 80/20 traffic mix with Round Robin scheduler

As we can see from the graph, the average throughput increases when the traffic load increases and it reaches the maximum value of about 12 Mbps which is the 100% capacity of the LTE network with this specific traffic mix.

By observing the overall average throughput curve in figure 6.3 it can be seen that the values of the throughput and the associated traffic load are approximately equal. The reason of this is that when the traffic load is lower than the capacity of the communication network, nearly 100% of the exchanged packets/messages can be disseminated successfully.

The background average throughput curve and the control communication average throughput curve show that the traffic mix 80/20 was kept when the traffic load was increased.

In figure 6.4 we can see the average throughput performance when the Priority-aware Round robin scheduler was used (PrioRR). Because the traffic load did not exceed the 100% capacity of the network, all the packets should be delivered successfully; therefore, the Round robin scheduler and Priority-aware Round robin scheduler provides the same throughput performance which is shown in figure 6.4

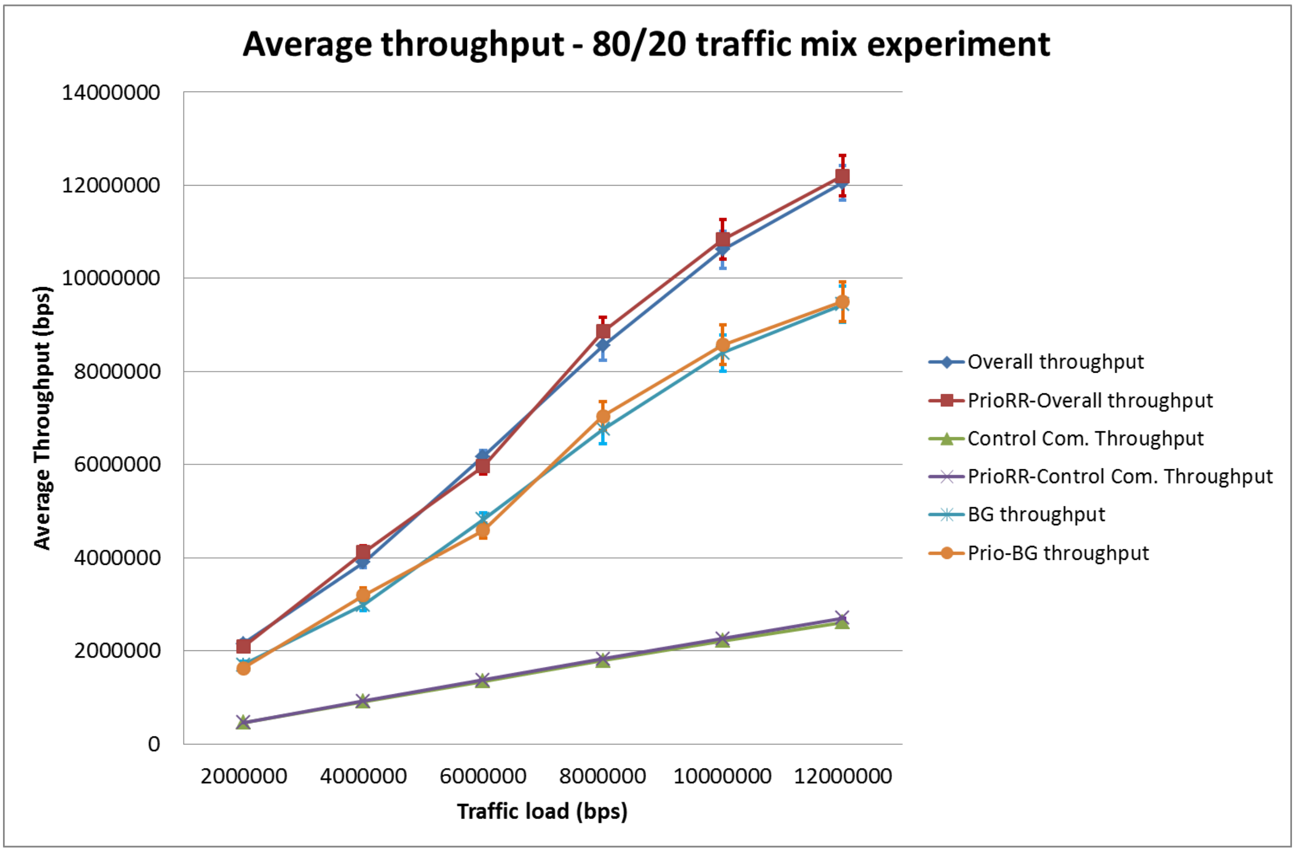


Figure 6.4 – Average throughput performance in 80/20 traffic mix experiment with both Round Robin and Priority-aware Round Robin schedulers

6.2.3.1.2 Average delay

Figure 6.5 illustrates the average delay of the remote control communication when the Round robin and Priority-aware round robin scheduler are used respectively.

Because we keep the traffic load under the network capacity, there is always enough resource for all the subscribers; therefore, the performance of Round robin and Priority-aware Round robin is approximately the same in term of delay.

In figure 6.5, there are two types of delay: the initiation delay and request delay (or Control communication delay). The initiation delay caused by the process of setting up the connection and establishing the application association between the MMS client and server. Hence, the number of messages needed to be exchanged in the initiation phase is much higher than the request-response process when the connection and association have been established successfully. That is the reason why the initiation delay is much higher than the request-response delay.

When the number of MMS nodes increase, it requires more time for all the MMS nodes to establish a LTE connection and MMS application association with the control centre. Thus the delay increases when the number of node increases.

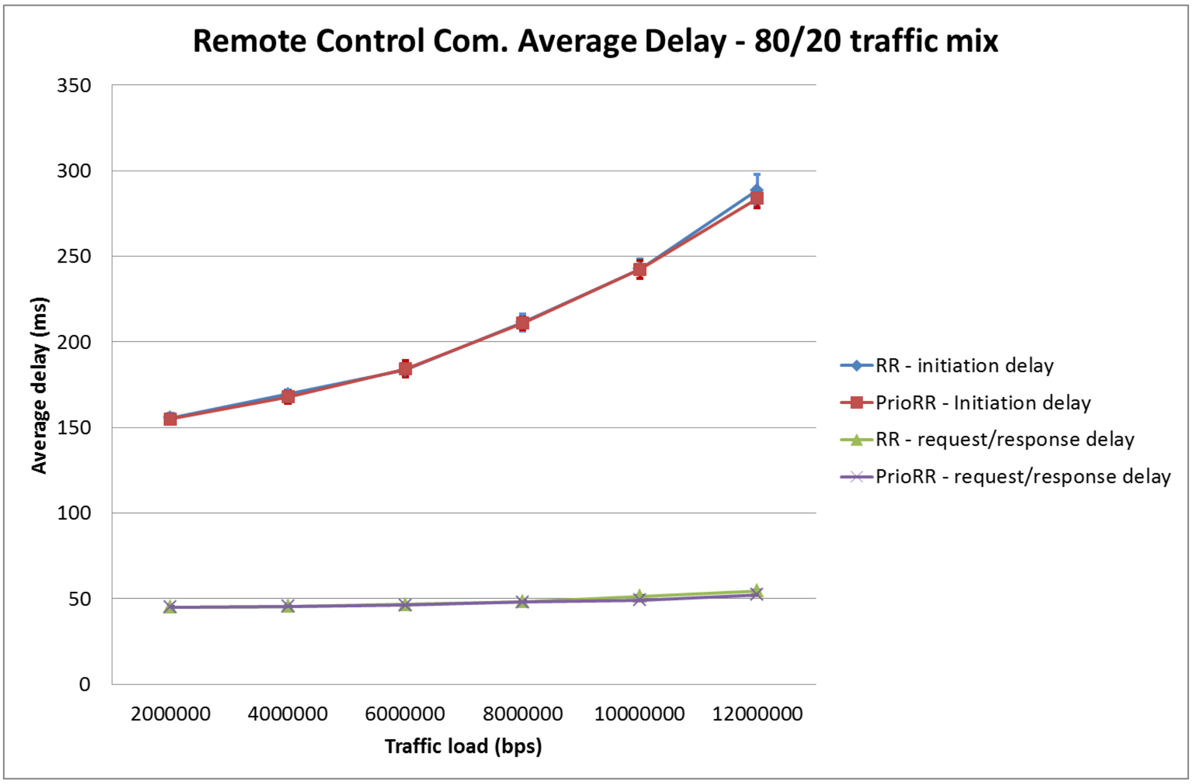


Figure 6.5 – Remote control communication average delay in 80/20 traffic mix experiment

By using the Round Robin MAC scheduling algorithm, the eNodeB schedules the access of each UE on a round robin (cyclic) fashion. Therefore, when the number of active UEs is high, each UE has to wait on getting access to the medium more than in the situation that a small number of UEs is active. Therefore, the request-response latency increases when the traffic load increases.

From the delay graph, we can see that the request-response delay performance when the traffic load does not exceed the network capacity quite fulfills the delay requirement of IEC 61850.

If we count the initiation delay, it will exceed the 100ms requirement for automatic control interaction. However, since we assume real-time control, the MMS nodes should stay connected and associated all the time.

The sum of initiation delay and request-response delay ranges from 200 ~ 350ms is still quite acceptable applying for the low-speed control functions like commands sent from the operator to change some operational parameters of the substation.

6.2.3.1.3 Packet loss ratio

Figure 6.6 illustrates the packet loss when the total traffic load increases in the 80/20 experiment.

Because the total traffic load never exceeded the LTE network capacity in this experiment, the performance of Round robin and Priority-aware Round robin scheduler in term of packet loss ratio is approximately equal.

When the traffic increases, it is easy to understand that the packet loss ratio increases because the network resource available for each node becomes less.

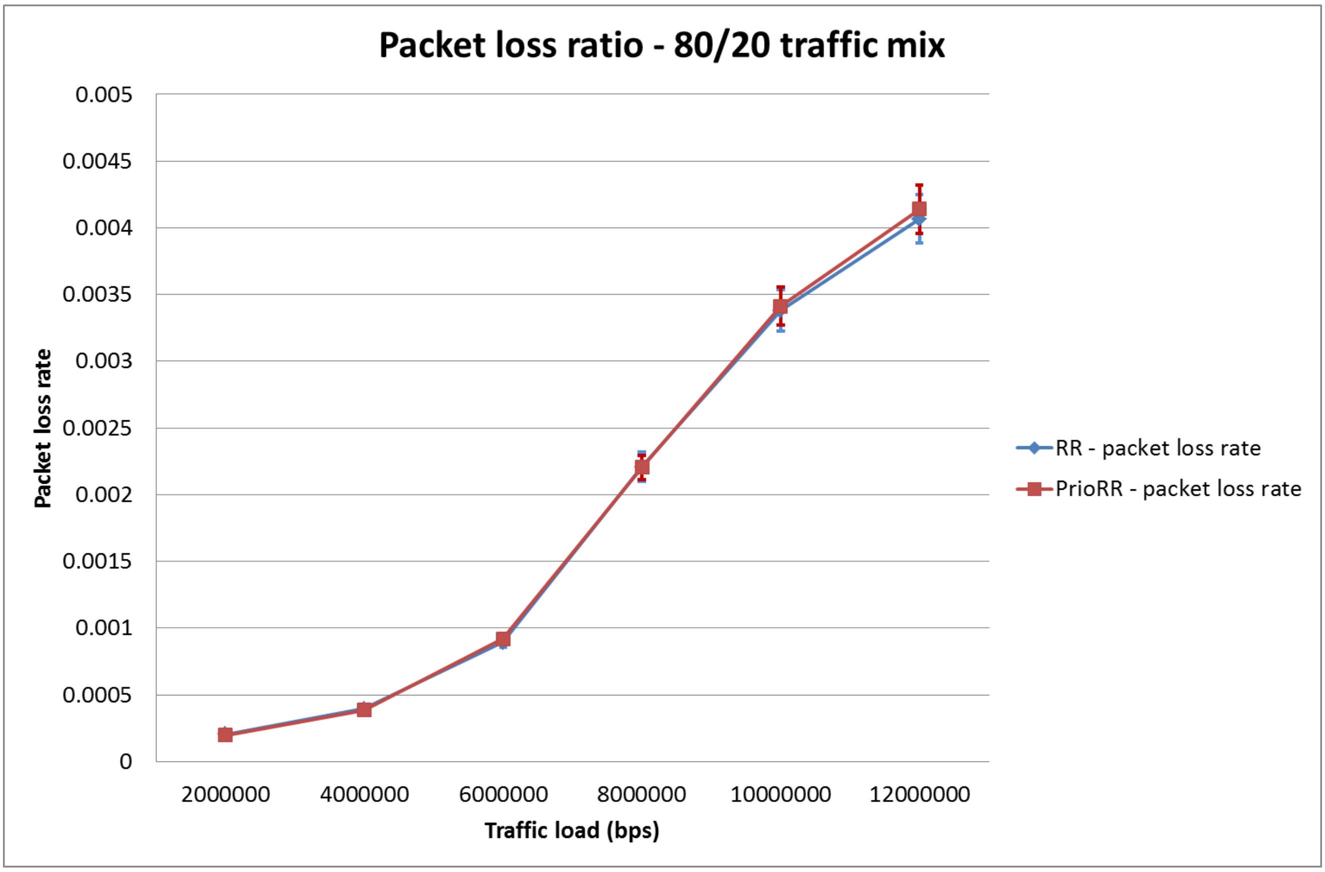


Figure 6.6 – Packet loss ratio in 80/20 traffic mix experiment

6.2.3.2 Traffic overload experiment

After finishing the 80/20 traffic mix experiment, the number of MMS nodes and background nodes that generate enough traffic to meet the network capacity was discovered. We continue increasing the number of nodes to observe how it can affect the throughput, delay and packet loss rate. The simulation results are described in the following graphs.

6.2.3.2.1 Average throughput

Figure 6.7 shows the average throughput performance of the remote control communication traffic when the traffic load was increased with the two scheduler, Round robin scheduler and Priority-aware Round robin scheduler.

Obviously, the remote control communication throughput has to decrease when the traffic load increases no matter which scheduler is used. It is because when the traffic load exceeds the network capacity and keeps increasing, the network resource available for each traffic flow becomes less and less. The chance for a message to be allocated in a RBG to be forwarded becomes less which increases the waiting time. Since the control centre will only send a new command message once receiving back a response from the controlled devices, the amount of packets generated and transmitted will be decreased leading to a decrease in throughput

However, it is also very clear that the remote control communication traffic throughput when the Priority-aware scheduler is used is always higher than when the normal Round robin scheduler is used. It is because when the Priority-aware scheduler is used, the control communication traffic is always has the best chance to be served by the network. In a sub-frame, if there are some MMS messages and some background messages ready to be transferred, the MMS messages which have highest metrics will be allocated the network resource and be forwarded first. It reduces the waiting time of the MMS messages leading to more MMS messages generated by the nodes and transferred by the LTE network.

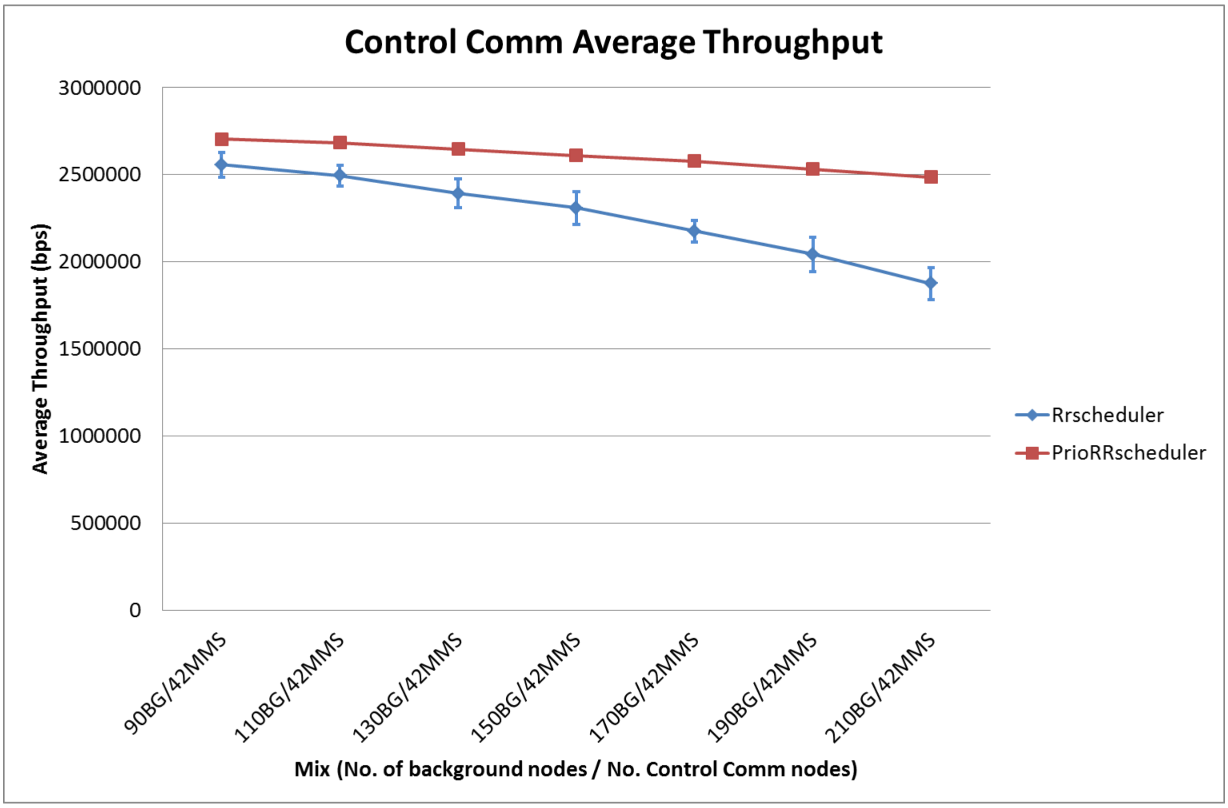


Figure 6.7 - Control communication throughput in traffic overload experiment

Because the MMS traffic is prioritized when the Priority-aware scheduler is used, the background traffic will have less chances to access the network resource. As a consequence, the throughput of the background traffic was decreased as illustrated in figure 6.8

Since the background traffic is much higher than the MMS traffic, the decrease of background traffic throughput causes a decrease in the overall throughput as shown in the graph.

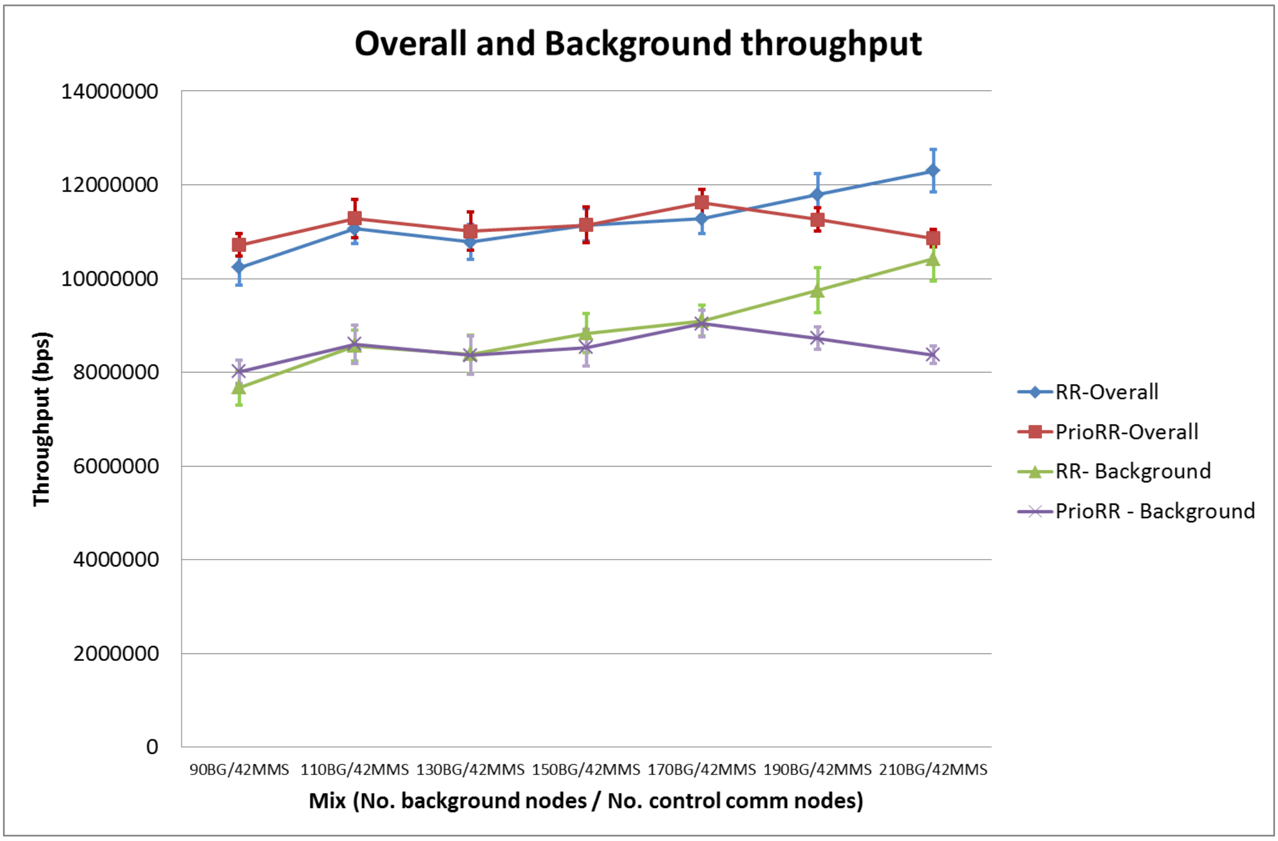


Figure 6.8 – Overall and background throughput in traffic overload experiment

For the round robin scheduler, because the MMS throughput was decreased significantly, more available resources were available and allocated to the background traffic. Therefore, the background traffic throughput increased when the traffic load increased.

6.2.3.2.2 Average delay

Figure 6.9 presents the two types of delay in a MMS-based remote control communication system: the initiation delay and request-response delay. As stated in section 6.3.2.1.2, due to the complex process of setting up the LTE connection plus establishing the client-server MMS application association, the average initiation delay is always much higher than the average request-response delay.

In this experiment, when we increases the number of background nodes, we observes that the both types of delays increase when using either Round Robin scheduler or Priority-aware

Round robin scheduler. It is due to the fact that the overall number of active nodes increases while the network resources are fixed. Consequently, all nodes suffer higher delay which is the waiting time before being served.

However, it is obvious that the delay increase much slower when the Priority-based Round Robin scheduler is used.

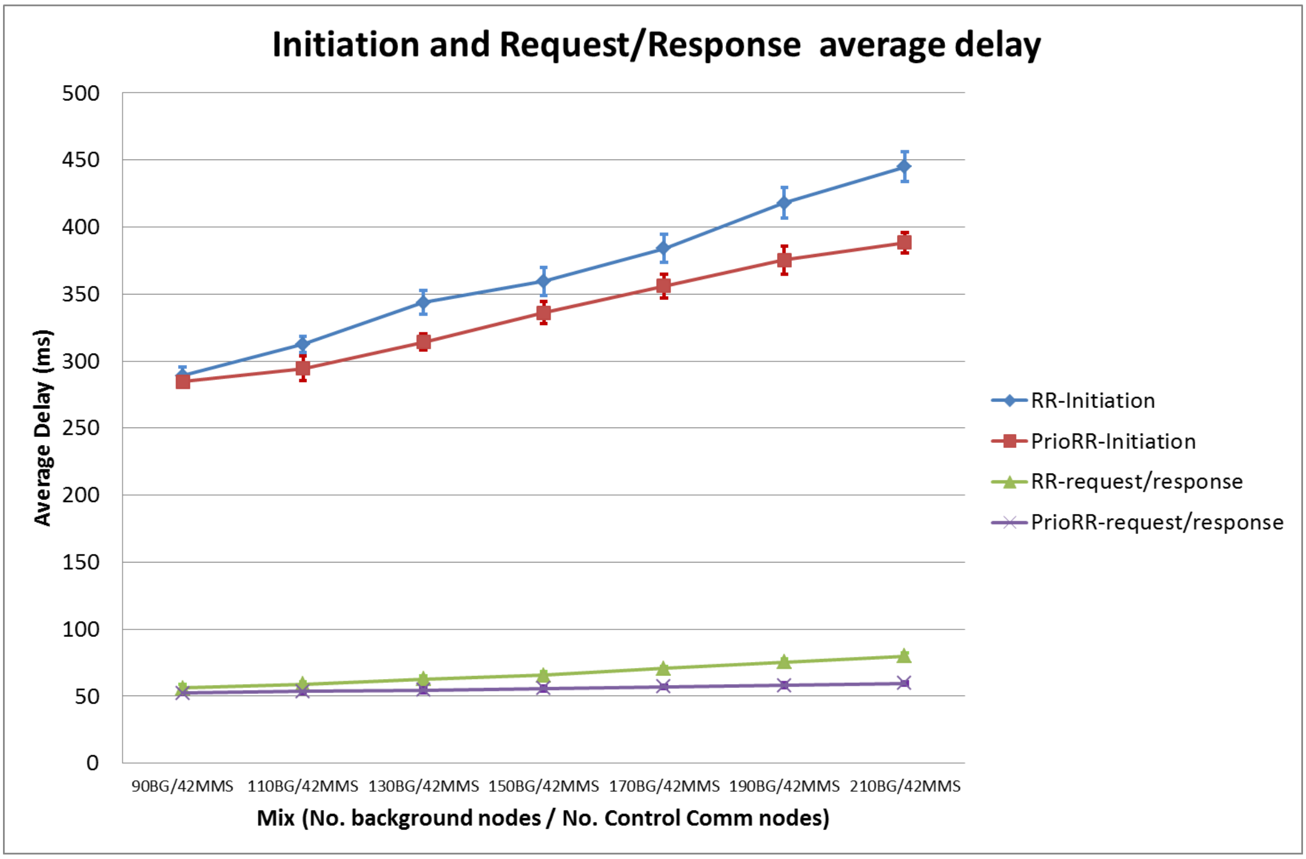


Figure 6.9 – Initiation and Request/Response average delay in traffic overload experiment

The reason is that when Priority-aware Round Robin scheduler is used with the highest metric assigned for control communication traffic, the scheduler always assigns a RBG for an active control communication traffic flow first within a TTI. Therefore, the delay caused by waiting until being scheduled decreases for the MMS traffic.

It is a very good solution when the number of background nodes increases highly but the network resources are constant. In this case, the most important traffic which is the control communication traffic always has the preference to access the network. It helps to reduce the probability that an MMS node has to suffer unaccepted latency.

6.2.3.2.3 Packet loss ratio

As we can see in figure 6.9, using Priority-aware Round Robin scheduler provides a critical benefit of decreasing the delay for control communication traffic. However, there is always a trade-off in term of packet loss ratio when the Priority-aware Round Robin scheduler is used.

Figure 6.10 illustrates the packet loss rate when the Round Robin and Priority-aware Round Robin scheduler are used.

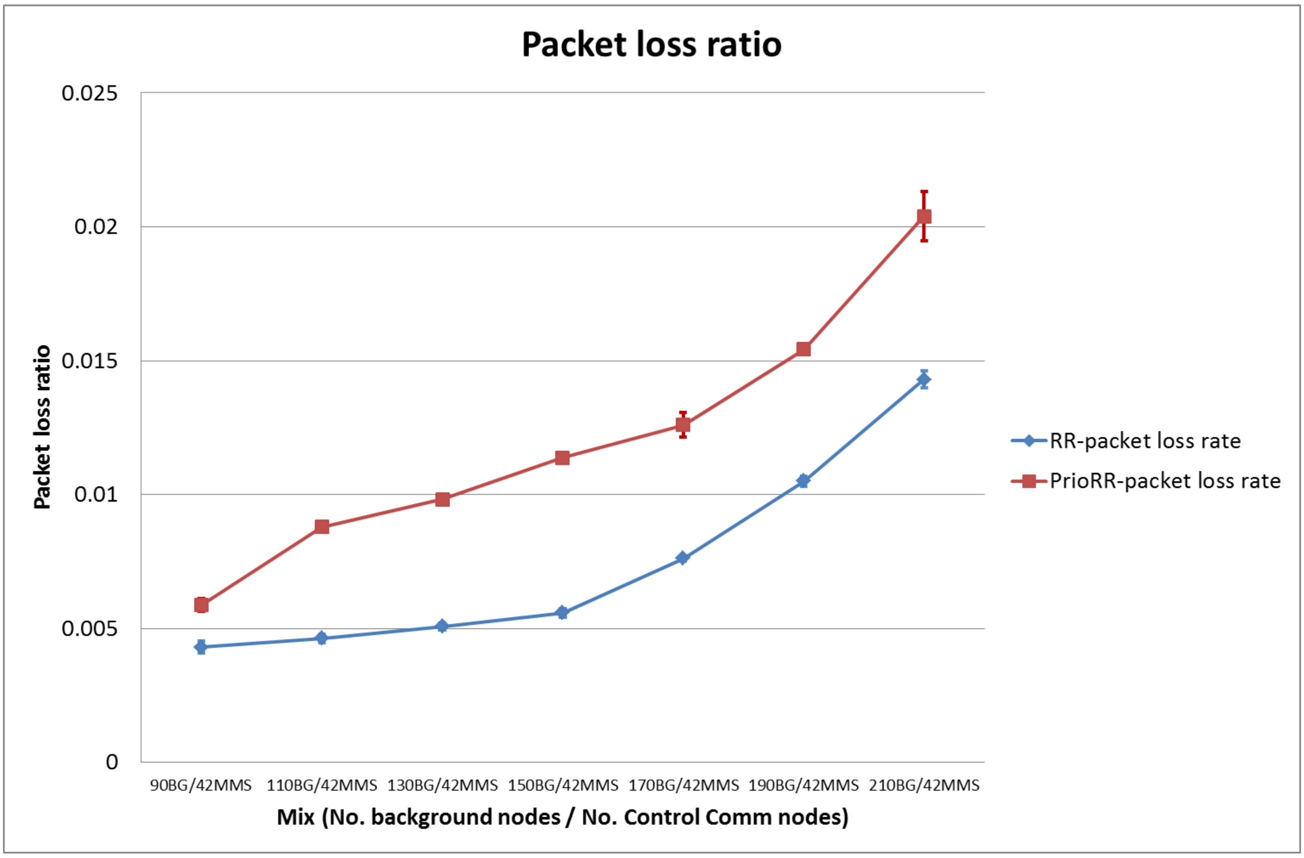


Figure 6.10 – Packet loss ratio in traffic overload experiment

As we can see in figure 6.10, the packet loss ratio for the background traffic is always higher when the Priority-aware Round Robin scheduler is used.

It can be explained that the Priority-aware Round Robin scheduler always gives higher chance to access the network resources for the control communication traffic. This algorithm, therefore, always gives less opportunity for the background nodes to access the network resources. Obviously, as a consequence, the packet loss of the background traffic will be increased and is higher than in case of normal Round Robin scheduler is implemented.

6.3.3.3 60/40 traffic mix experiment

In this experiment, the percentage of background traffic and remote control communication is always kept as 60% traffic generated by the background nodes and the rest 40% generated by MMS nodes.

In this experiment, we consider the 80% utilization as in reality; LTE network operators always prefer a safe band for some unexpected situations.

6.3.3.3.1 Average throughput

Figure 6.10 shows the average throughput performance for both MMS and background traffic. Similar to the 80/20 traffic mix experiment, we see that the throughput increases when the traffic load increases.

As the traffic load did not exceed the capacity of the network, the throughput is approximately equal to the traffic load, meaning that almost messages were delivered successfully.

Figure 6.11 – Average throughput performance in 60/40 traffic mix experiment

Because, the traffic load is under the capacity of the network, Round Robin and Priority-aware Round Robin scheduler performed almost the same. It is because the network resources available are sufficient to serve all the active nodes within the cell sector.

6.3.3.3.2 Packet loss ratio

Figure 6.12 shows the packet loss ratio in 60/40 traffic mix experiment. Similar to the 80/20 experiment, the performances of Round Robin and Priority-aware Round Robin scheduler are approximately equal.

The packet loss ratio increases when the number of nodes increases since the network resources available for each node decrease but it is still acceptably low.

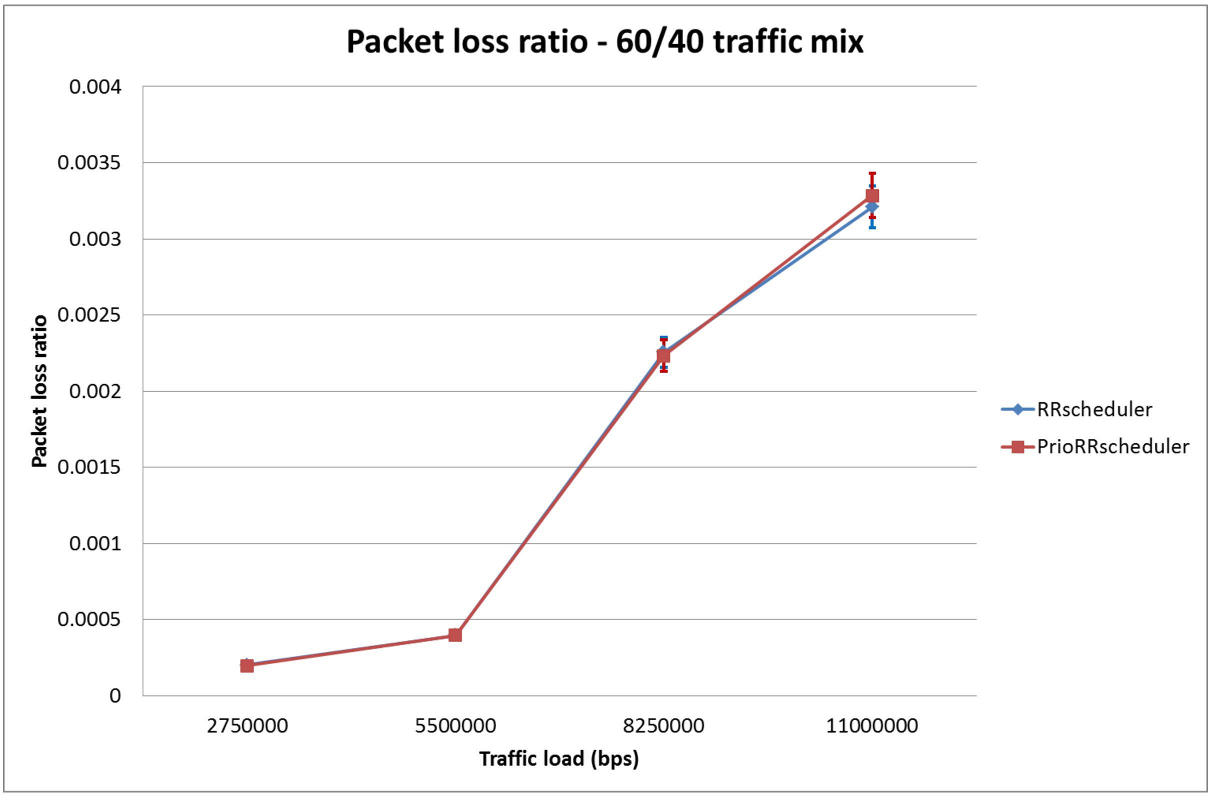


Figure 6.12 – Packet loss ratio in 60/40 traffic mix experiment

6.3.3.3.3 Average delay

Figure 6.13 illustrates the delay performance in 60/40 traffic mix experiment. Similar to the 80/20 traffic mix experiment, it is shown in the graph that the initiation delay is much higher than the request/response delay. The reason still lies in the fact that initiation is a complicated process consist of LTE connection set-up and MMS application association establishment.

In our experiment scenario, there is only one MMS client which is the control centre and many associated MMS servers which are the intelligent electrical devices to be controlled in distribution grid. Therefore, when the number of controlled nodes increases, the average time for establishing the MMS association also increases. Therefore, it is shown in figure 6.13 that the initiation delay increases significantly when the number of MMS nodes increases.

For the request/response delay, because the traffic load did not exceed the network capacity, the delay for the request/response interaction between MMS client and servers only increases slightly.

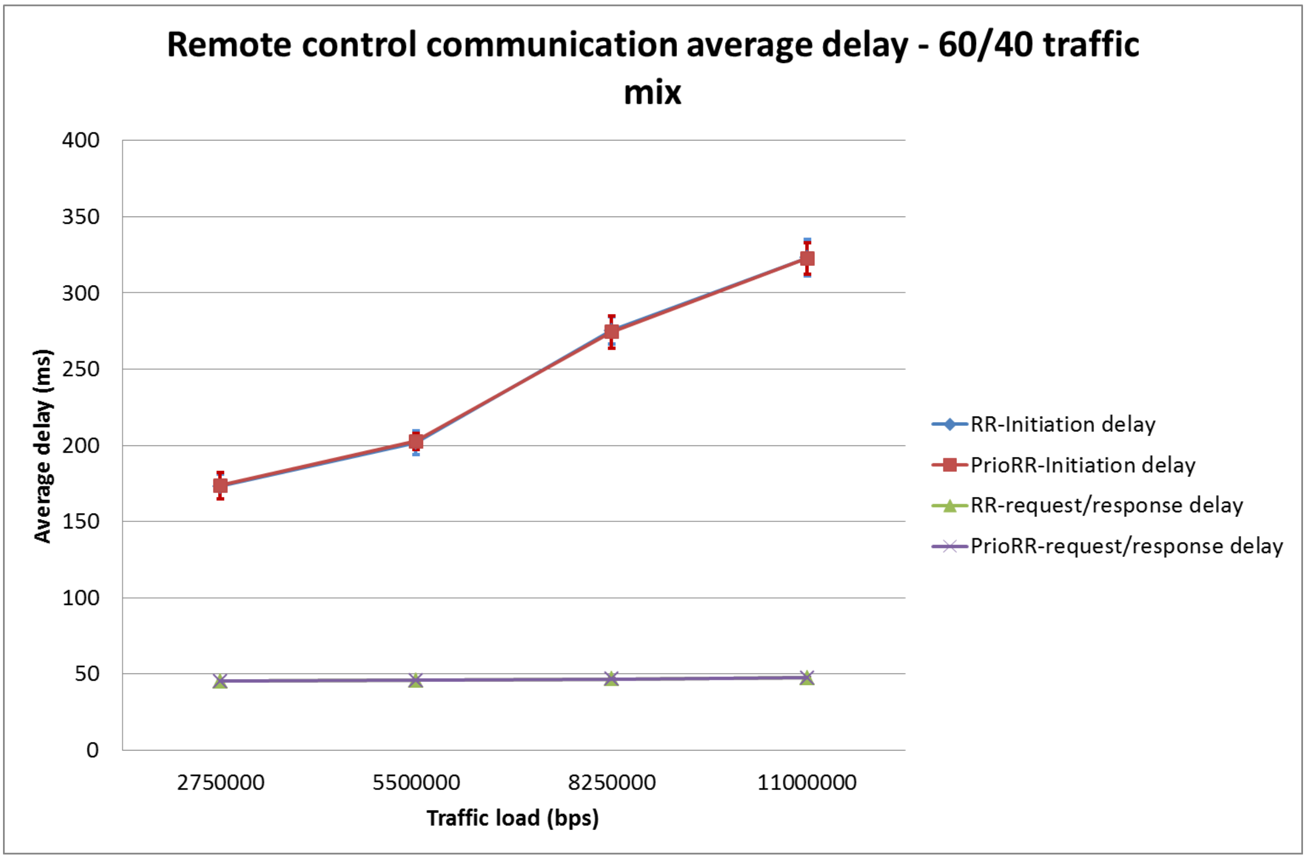


Figure 6.13 – Remote control communication traffic average delay in 60/40 traffic mix experiment

6.4 Summary

Chapter 6 describes some different sets of experiment conducted in NS3 LENA simulation environment to evaluate the performance of the proposed solution. In both 80/20 and 60/40 traffic mix, the simulation results prove that the integration of IEC 61850 MMS and LTE is not only possible but it also provides good performance in term of delay, throughput and packet loss. In both experiments, when the traffic load generated does not exceed the maximum capacity of the network, the throughput and packet loss performances are remarkable. Most importantly, the request/response delay is only about half of the delay requirement specified by IEC 61850 for the medium-speed automatic control interactions. Moreover, the result of the traffic overload experiment shows that, when the network resources become insufficient due to the increasing amount of subscribers, the Priority-aware Round Robin scheduler can provides a much better delay and throughput performance for remote control communication traffic with the trade-off of decreasing performance of other less-important background traffic.

The fact that the performance of background traffics decreases is known as the starvation problem for low-priority traffics. For Priority-aware Round Robin scheduler, the problem is serious when the number of MMS flows is (much) more than the number of background flows and the network resources are insufficient since in this case most resources will be consumed by remote control traffic. However, since we assume that remote control communications are mission-critical application such that they directly affect the efficiency, reliability and safety of the electricity network, dropping less important background traffic is an acceptable method to achieve minimum performance requirements for high priority remote control applications. As stated above, it is a trade-off when using Priority-aware Round Robin scheduler. Fortunately, the problem will not happen when the traffic load and amount of active nodes are within the system capacity. Therefore, network planning and vision are very important in designing a reliable communication network to support Smart Grid applications.

Chapter 7

Conclusion and Future work

7.1 Conclusion

Theoretically, the integration of the widely-accepted IEC 61850 MMS protocol stack and the advanced wireless cellular network LTE can be a potential solution to support the remote control communication in the distribution network of Smart Grid. Throughout this project, a combination of literature-based and simulation-based research has been conducted to answer the main research question *"How can remote control communications in electricity distributed grid be supported by using IEC 61850 MMS over LTE?"*

Following the Waterfall research model approach, a literature study had been conducted to answer for the first sub-question about the requirements and challenges for integrating IEC 61850 MMS and LTE to support remote control communications in distribution grid. The main requirements and challenges are described in chapter 3 of this report. They include the two main types of requirement which are the functionality requirement and performance requirement. The former states that the first requirement to enable this integration is the possibility to map MMS communication protocol stack over the LTE communication profile, while the latter shows that latency and prioritization are the most important performance requirements for remote control communication. Additionally, some challenges were also discovered including the quality of service, delay performance, reliability and security of the network system.

By realizing the requirements and challenges, a solution has been proposed with the architecture specification and design described in chapter 4. Since both MMS and LTE support the use of TCP/IP communication profile, the mapping of MMS over LTE to support remote control communication is feasible. In order to fulfil the latency performance requirement, especially in case of limited network resources, a Priority-aware Round Robin scheduler has been designed to allow the remote control communication traffic to have highest opportunity to access the available network resources. The detailed specification and design of the solution described in chapter 4 together with the implementation presented in chapter 5 have answered the research question 2 about how the integration of IEC 61850 MMS and LTE with priority-aware MAC scheduler can satisfy the requirements and overcome the selected challenges.

Finally, chapter 6 describes some different sets of experiment conducted in NS3 LENA simulation environment to evaluate the performance of the proposed solution. In both 80/20 and 60/40 traffic mix, the simulation results prove that the integration of IEC 61850 MMS and LTE is not only possible but also provides good performance in term of delay, throughput and packet loss. In both experiments, when the traffic load generated does not exceed the maximum capacity of the network, the throughput and packet loss performances are remarkable. Most importantly, the request/response delay is only about half of the delay requirement specified by IEC 61850 for the medium-speed automatic control interactions. Moreover, the result of the traffic overload experiment shows that, when the network resources become insufficient due to the increasing amount of subscribers, the Priority-aware Round Robin scheduler can provides a much better delay and throughput performance for remote control communication traffic with the trade-off of decreasing performance of other less-important background traffic.

Therefore, the simulation experiment and result evaluation in chapter 6 has answered for the research question 3 that the integration of IEC 61850 MMS and LTE is a feasible solution to support the remote control communication services in distribution grid, particularly when the priority-aware MAC scheduler is implemented.

In short, the research questions can be answered as the following:

1. What are the main requirements and challenges of integrating IEC 61850 MMS and LTE to support remote control communications in electricity distribution grid?

Answer: The main requirements are the functionality requirement which involve the mapping of MMS communication protocols over LTE protocol stack and performance requirement. The main and selected challenges to work on are Quality of Service and strict delay requirement.

2. How can the selected challenges be solved?

Answer: These challenges can be solved by designing and implementing MMS communication protocol stack and LTE protocol interfaces on the intelligent electrical devices so that they can communicate with the control centre via the LTE network. In addition, a Priority-aware Round Robin scheduler was also designed and implemented to give the control communication traffic high preference in accessing the network resources; therefore, reducing the delay when the available resources are insufficient.

3. *Can the provided solution to the selected challenges satisfy the requirements?*

By analysing the simulation experiments' results, we can conclude that provided solution satisfies all the main requirements and selected challenges.

Another conclusion is that IEC 61850 MMS should be mapped successfully on any wireless technologies that support TCP/IP communication profile. It is also mentioned in IEC 61850 standard as the flexibility advantage of IEC 61850 [11]. Depending on the specific functions and requirements, the electricity network operator can choose to implement IEC 61850 MMS over other wireless technologies like wifi, WiMax or CDMA2000 and so on.

7.2 Future work

For future work, firstly more experiments should be done to verify the performance of IEC 61850 MMS over LTE when different types of background traffic mix are used. It is also beneficial to change the LTE configuration parameter such as the channel bandwidth, cell size or using more than one cells to verify the performance of the solution.

Moreover, as Smart Grid is a very broad area with plentiful applications, the integration of IEC 61850 and LTE can be investigated more to support other applications in not only distribution grids. When multiple applications are based on IEC 61850 MMS and LTE, it is also important to investigate on the impact of each application to other type of MMS traffic and the performance of each application in the system.

One more feasible research direction is to investigate on the integration of IEC 61850 MMS over other wireless network infrastructure such as Wifi, Wimax, UMTS, and CDMA2000 to support different types of control functions such as Smart Home control or Microgrid control applications.

References

[1]. SMB Smart Grid Strategic Group (SG3), "IEC Smart Grid Standardization Roadmap", Edition 1.0, June 2010.

[2]. The path of Smart Grid, IEEE

[3]. United Nations Office for the Coordination of Humanitarian Affairs and the Internal Di splacement Monitoring Centre, "Monitoring disaster displacement in the context of climate change", 2008

[4]. THE EU 20/20/2020 targets: An overview of the EMF22 assessment

[5]. EPRI's IntelliGridSM initiative, [Online]. Available: http://intelligrid.epri.com

[6]. GridWise Architecture Council, [Online]. Available: http://www.gridwiseac.org

[7]. EPRI Smart Grid Resource Center [Online]. Available: http://smartgrid.epri.com/

[8]. Frans Campfens, "the Role of the DNO in Smart Grid Cyber Security", *European Smart Grid Cyber Security and Privacy*, Amsterdam November, 2011.

[9]. IEEE Smart Grid [Online]. Available: http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model#distribution

[10]. Salman Mohagheghi, Jean-Charles Tournier, James Stoupis, Laurent Guise, Thierry Coste, "Applications of IEC 61850 in Distribution Automation", *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*, March 2011.

[11]. IEC 61850-1 TR Ed.2, "Communication networks and systems for power utility automation – Part 1: Introduction and Overview", 2012.

[12]. Draft IEC TR 61850-90-2, "Use of IEC 61850 for the communication between substations and control centres", 21/09/2012.

[13]. IEC 61850-90-5 TR Ed.1, "Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118", 12/08/2011.

[14]. IEC 61850-5, "Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models", 2012.

[15]. Draft IEC TR 61850-90-2 – Use of IEC 61850 for the communication between substations and control centres, 21/9/2012.

[16]. IEC 61850-8-1 Ed.2, "Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) – Mapping to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3", 2009.

[17]. CDMA Development Group – CDG website [Online]. Available: http://www.cdg.org/technology/cdma450.asp

[18]. M.R Karim, M. Sarraf, "W-CDMA and CDMA2000 for 3G Mobile Networks", McGraw-Hill, 2002.

[19]. IEC 61850-7-2 Ed.2, "Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)", 2008.

[20]. Javier Juárez, Carlos Rodríguez-Morcillo, José Antonio Rodríguez-Mondéjar, "Simulation of IEC 61850-based substations under OMNeT++", *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques*, 2012.
[21]. Draft IEC 61850-90-4 TR Ed1, "Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines for substations", 2012.
[22]. Jyn-cheng Chen, Tao Zhang, "IP-based next-generation wireless networks", John Wiley & Sons, Inc, 2004.
[23]. Christopher Cox, "An Introduction to LTE, LTE-Advanced, SAE and 4G Mobile Communications", John Wiley & Son, Inc, 2012.
[24]. Heikki Karanen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, Valtteri Niemi, "UMTS Networks Architecture, Mobility and Services", John Wiley & Sons, Ltd, England, 2001
[25]. Ebrabim M. Al-Dhari, Husam M. Nasher, Mohammed A. Al-khalaqi, Mohsen Y. Ba alawi, "Upgrading from 3G to 4G: UMTS to LTE", 2011.
[26]. Harri Holma and Antti Toskala, "LTE for UMTS OFDMA and SC-FDMA Based Radio Access", John Wiley & Son, 2009.
[27]. Stefania Sesia, Issam Toufik, Matthew Baker, "LTE – The UMTS Long Term Evolution: From Theory to Practice", John Wiley & Son, Ltd, 2009.
[28]. R. E. Mackiewicz, "Overview of IEC 61850 and Benefits", Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES, 2006.
[29]. IEC 62351-4 Committee Draft version 1, "Data and Communications Security – Profiles including MMS", April 2005.
[30]. Anna Larmo, Magnus Lindström, Michael Meyer, Ghyslain Pelletier, Johan Torsner, Henning Wiemann, Ericsson Res., Plano, TX, "The LTE-Link Layer Design", *Communication Magazine IEEE*, 2009
[31]. Pierre Lescuyer, Thierry Lucidarme – Acatel Lucent "Evolved Packet System (EPS), the LTE and SAE evolution of 3G UMTS", John Wiley & Son, 2008.
[32]. Feuerhahn, S.; Zillgith, M.; Wittwer, C.; Wietfeld, C., "Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications," *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on* , vol., no., pp.410,415, 17-20 Oct. 2011
[33]. IEC 61850-9-2 Ed.2, "Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3", 2009
[34]. 3GPP2 S.R0141-0, "Study for Machine-to-Machine (M2M) communication for CDMA2000 network", December 2010.
[35]. 3GPP TR 23.888, "System improvements for Machine-Type Communications (MTC) (Release 11)"
[36]. 3GPP TS 22.368, "Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 12)"
[37]. 3GPP TR 37.868, "Study on RAN Improvements for Machine-type Communications; (Release 11)"
[38]. http://otcl-tclcl.sourceforge.net/otcl/

[39]. http://www.isi.edu/nsnam/nam/index.html
[40]. http://www.isi.edu/nsnam/xgraph/index.html
[41]. http://www.gnuplot.info/
[42]. http://www.lrc.ic.unicamp.br/wimax_ns2/
[43]. http://eurane.ti-wmc.nl/eurane/
[44]. P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu and A. Shami, "Evaluation of Communication Technologies for IEC 61850 based Distribution Automation System with Distributed Energy Re-sources," in Power & Energy Society General Meeting, 2009. PES '09. IEEE, pp. 1-8, 26-30 July 2009.
[45]. I. Ali and M. S. Thomas, "Substation Communication Networks Architecture," in Power System Technology and IEEE Power India Conference, 2008. POWERCON 2008. Joint International Conference on, pp. 1-8, 12-15 Oct. 2008.
[46]. Y. Liang and R. H. Campbell, "Understanding and Simulating the IEC 61850 Standard," 2008. [Online]. Available: https://www.ideals.illinois.edu/handle/2142/11457
[47]. Palak Parikh, "Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations", PhD Thesis. [Online]. Available: http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1931&context=etd
[48]. http://www.nsnam.org/
[49]. http://iptechwiki.cttc.es/LTE-EPC_Network_Simulator_%28LENA%29
[50]. http://www.nsnam.org/docs/models/ns-3-model-library.pdf
[51]. Konka, J.W.; Arthur, C.M.; Garcia, F.J.; Atkinson, R.C., "Traffic generation of IEC 61850 sampled values," *Smart Grid Modeling and Simulation (SGMS), 2011 IEEE First International Workshop on* , vol., no., pp.43,48, 17-17 Oct. 2011
[52]. http://www.wireshark.org/
[53]. http://en.wikipedia.org/wiki/Waterfall_model
[54]. Jan Tore Sorensen, Martin Gilje Jaatun, "A description of the Manufacturing Message Specification (MMS)", SINTEF, 2007.
[55]. CIRED, Working Group on Smart Grid, "Smart Grid on the distribution level – Hype or Vision", 2013.
[56]. LENA M5 design documentation. Available online: http://lena.cttc.es/manual/lte-design.html#description-of-the-components
[57]. Prof. Dr. H. Kirrmann, ABB Research Center, Baden, Switzerland, "MMS - Manufacturing Message Specifications". [Online]. Available: http://lamspeople.epfl.ch/kirrmann/Slides/AI_420_MMS.ppt
[58]. "Industrial automation systems, Manufacturing Message Specification. Part 1," ISO 9506-1:2003(E) ISO 2003.
[59]. NGMN Alliance, "NGMN Radio Access Performance Evaluation Methodology"

[60]. Farooq Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge: Cambridge UP, 2009. Print.

[61]. “NIST/SEMATECH e-Handbook of Statistical Method,” National Institute of Standards and Technology, July 2006. [Online]. Available: http://www.itl.nist.gov/div898/handbook/eda/section3/eda352.htm

[62]. Rohde & Schwarz, “LTE technology and LTE test; a desk-side chat”, April 2009.

[63]. A.D.Nguyen, “Use of IEC 61850 for Low Voltage Microgird Power Control”, *Internship project at Alliander*, the Netherlands, 2013.

[64]. IEC 61850-7-420 Final Draft International Standard (FDIS), “Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources logical nodes”, 2008.

[65]. https://github.com/tgpham/iec61850-mms-traffic-generator-for-ns3/tree/master/mms

[66]. https://github.com/anhdung0111/myrepository/blob/master/priority-aware-scheduler.rar

[67]. Parikh, P.P.; Sidhu, T.S.; Shami, A., "A Comprehensive Investigation of Wireless LAN for IEC 61850–Based Smart Distribution Substation Applications," *Industrial Informatics, IEEE Transactions on* , vol.9, no.3, pp.1466,1476, Aug. 2013

[68]. Capozzi, Piro, Grieco, Boggia & Camarda: Downlink Packet Scheduling in LTE Cellular Networks, In: IEEE Communications Surveys & Tutorials, Early Access Article, IEEE Xplore, 2012, pp. 1 - 8.

[69]. R. Kwan, C. Leung, and J. Zhang, “Multiuser scheduling on the downlink of an LTE cellular system,” Research Lett. Commun., pp. 3:1–3:4, Jan. 2008.

[70]. G. Monghal, K. I. Pedersen, I. Z. Kovacs, and P. E. Mogensen, “QoS oriented time and frequency domain packet schedulers for the UTRAN long term evolution”, *in Proc. IEEE Veh. Tech. Conf.*, VTC-Spring, Marina Bay, Singapore, May 2008.

[71]. Y. Zaki, T. Weerawardane, C. Gorg, and A. Timm-Giel, “Multi-QoS-Aware Fair Scheduling for LTE,” *in Proc. IEEE Veh. Tech. Conf.*, VTC-Spring, May 2011, pp. 1 –5

[72]. D. Skoutas and A. Rouskas, “Scheduling with QoS provisioning in Mobile Broadband Wireless Systems,” *in Proc. IEEE European Wireless Conf.*, EW, Apr. 2010, pp. 422 – 428

[73]. H. Ramli, R. Basukala, K. Sandrasegaran, and R. Patachaianand, “Per-formance of well-known packet scheduling algorithms in the downlink 3GPP LTE system,” *in Proc. IEEE Malaysia International Conf. on Comm.*, MICC, Kuala Lumpur, Malaysia, 2009, pp. 815 –820.

[74]. R. Basukala, H. Mohd Ramli, and K. Sandrasegaran, “Performance analysis of EXP/PF and M-LWDF in downlink 3GPP LTE system,” *in Proc. Asian Himalayas International Conf. on Internet*, AH-ICI, Kathmundu, Nepal, Nov. 2009, pp. 1 –5.

[75]. B. Sadiq, R. Madan, and A. Sampath, “Downlink scheduling for multiclass traffic in LTE,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 9–9, 2009.

[76]. G. Piro, L. Grieco, G. Boggia, R. Fortuna, and P. Camarda, “Two-level Downlink Scheduling for Real-Time Multimedia Services in LTE Networks,” *in IEEE Trans. Multimedia*, vol. 13, no. 5, Oct. 2011, pp.1052 –1065.

[77]. M. Iturralde, A. Wei, and A. Beylot, “Resource Allocation for Real Time Services Using Cooperative Game Theory and a Virtual Token Mechanism in LTE Networks,” in Proc. IEEE Personal Indoor Mobile Radio Commun., PIMRC, Sydney, Australia, Jan. 2012.
[78]. K. Sandrasegaran, H. A. Mohd Ramli, and R. Basukala, “Delay-prioritized scheduling DPS for real time traffic in 3gpp lte system,”in Proc. IEEE Wireless Commun. and Net. Conf., WCNC, Apr. 2010, pp. 1 –6
[79]. G. Monghal, D. Laselva, P. Michaelsen, and J. Wigard, “Dynamic Packet Scheduling for Traffic Mixes of Best Effort and VoIP Users in E-UTRAN Downlink,” in Proc. IEEE Veh. Tech. Conf., VTC-Spring, Marina Bay, Singapore, May 2010, pp. 1 –5.
[80]. S. Choi, K. Jun, Y. Shin, S. Kang, and B. Choi, “MAC Scheduling Scheme for VoIP Traffic Service in 3G LTE,” in Proc. IEEE Veh. Tech. Conf., VTC-Fall, Baltimore, MD, USA, Oct. 2007.
[81]. T.G.Pham, “Integration of IEC 61850 MMS and LTE to support smart metering communications”, Master thesis, University of Twente, 2013.

APPENDIX

A. Background traffic specification

The traffic model outlined below are used by most standardization bodies according to [59]

A.1 Voice traffic

Voice traffic specification is summarized in Table A.1

Table A.1 – Voice traffic specification

Parameter	Value
Voice codec	RTP AMR 12.2, Source rate 12.2 Kb/s
Encoder frame length	20 ms
Voice activity factor (VAF)	50% $\alpha = \beta = 0.01$
SID payload	SID packet every 160 ms during silence 15 bytes (5 bytes + header)
Protocol overhead with header compression	10 bit + padding (RTP pre-header) 4 byte (RTP/UDP/IP) 2 byte (RLC/security)16 bits (CRC)
Total voice payload on air interface	40 bytes

A.2 FTP traffic

The two main FTP session parameters are: the size S of a file to be transferred; reading time D, i.e. the time interval between end of download of previous file and the user request for next file

Table A.2 – FTP traffic specification

Parameter	Statistical characterization
File size S	Truncated lognormal distribution mean = 2 Mbytes, standard deviation = 0.722 Mbytes, maximum size = 5 Mbytes (before truncation) PDF: $f_x = \frac{1}{\sqrt{2\pi}\sigma x} e^{\frac{-(\ln x - \mu)^2}{2\sigma^2}} \quad x > 0 \quad \sigma = 0.35, \mu = 14.45$
Reading time D	Exponential distribution with mean = 180 seconds PDF: $f_x = \lambda e^{-\lambda x} \quad x \geq 0 \quad \lambda = 0.006$

A3. HTTP traffic

The main parameters to characterize web-browsing are: the main size of an object S_M; the size of an embedded object in a page S_E; the number of embedded objects N_D; reading time D; parsing time for the min page T_P

Table A.3 – HTTP traffic specification

Parameter	Statistical characterization
Main object size S_M	Truncated lognormal distribution, mean = 10710 bytes, standard deviation = 25032 bytes, minimum = 100 bytes, maximum = 2 Mbytes (before truncation) PDF: $f_x = \frac{1}{\sqrt{2\pi}\sigma x} e^{\frac{-(\ln x - \mu)^2}{2\sigma^2}}$ $x > 0 \sigma = 1.37, \mu = 8.37$
Embedded object size S_E	Truncated lognormal distribution, mean = 7758 bytes, standard deviation = 126168 bytes, minimum = 50 bytes, maximum = 2 Mbytes (before truncation) PDF: $f_x = \frac{1}{\sqrt{2\pi}\sigma x} e^{\frac{-(\ln x - \mu)^2}{2\sigma^2}}$ $x > 0 \quad \sigma = 2.36, \mu = 6.17$
Number of embedded objects per page N_D	Truncated Pareto distribution, mean = 5.64, maximum = 53 (before truncation) PDF: $f_x = \frac{\alpha_k^\alpha}{\alpha + 1}, k \leq x < m \quad f_x = \left(\frac{k}{m}\right)^\alpha, x = m$ $\alpha = 1.1, \quad k = 2, \quad m = 55$ Note: subtract k from the generated random value to obtain N_D
Reading time D	Exponential distribution with a mean = 30 seconds PDF: $f_x = \lambda e^{-\lambda x} \quad x \geq 0 \quad \lambda = 0.033$
Parsing time T_p	Exponential distribution with mean = 0.13 seconds PDF: $f_x = \lambda e^{-\lambda x} \quad x \geq 0 \quad \lambda = 7.69$

A4. Video streaming

Each frame of video data arrives at a regular interval T determined by the number frames per second. Each frame is decomposed into a fixed number of slices, each transmitted as a single packet. The size of these packets/slices is modelled to have a truncated Pareto distribution. The video encoder introduces encoding delay intervals between the packets of a frame. These intervals are modelled by a truncated Pareto distribution. The following distributions assume a source video rate of 64 kbps.

Table A.4 – Video streaming traffic specification

Parameter	Statistical characterization
Inter-arrival time between the beginning of each frame	Deterministic at 100 ms (10 frames per second)
Number of packets (slices) in a frame	Deterministic, 8 packets per frame
Packet (slice) size	Truncated Pareto distribution, mean = 10 Bytes, maximum = 250 bytes (before truncation) PDF: $f_x = \frac{\alpha_k^\alpha}{\alpha+1}, k \le x < m \quad f_x = \left(\frac{k}{m}\right)^\alpha, x = m$ $\alpha = 1.2, k = 20$ bytes, $m = ??$
Inter-arrival time between packets (slices) in a frame	Truncated Pareto distribution, mean = $m = 6$ ms, maximum =12.5 ms (before truncation) PDF: $f_x = \frac{\alpha_k^\alpha}{\alpha+1}, k \le x < m \quad f_x = \left(\frac{k}{m}\right)^\alpha, x = m$ $\alpha = 1.2, k = 2.5$ ms, $m = ??$

A.5 Interactive real-time services: Gaming

The specification of Gaming traffic is summarized in table A.5

Table A.5 – Gaming traffic specification

Parameter	Statistical characterization
Initial packet arrival	Uniform distribution $f_x = \frac{1}{b-a} \quad a \le x \le b \quad a = 0 \quad b = 40$ ms
Packet arrival	Deterministic, 40 ms
Packet size	Largest extreme value distribution (also known as Fisher–Tippett distribution) $f_x = \frac{1}{b} e^{-\frac{x-a}{b}} e^{-e^{-\frac{x-a}{b}}} \qquad a = 45$ bytes $\quad b = 5.7$

B. Priority-aware Round Robin scheduler installation and usage guide

The priority-aware Round Robin scheduler is developed and implemented in ns-3 LENA simulation environment. The author has made some modifications to the source codes of LENA. In order to use the Priority-aware Round Robin scheduler, it is required to download the modified version of ns-3 simulator.

B.1 Download the module

Step 1: download the *priority-aware-scheduler.rar* file from [66].

Step 2: install *priority-aware-scheduler.rar* by downloading the file, extract and add them to your *ns-3-dev/src/lte/model* folder (replacing the existing files) and build again by using *./waf*

B.2 Priority-aware Round Robin scheduler

The scheduler modules are at `pf-ff-mac-scheduler.cc` and `pf-ff-mac-scheduler.h`

Originally the `pf-ff-mac-schedueler.cc` and `pf-ff-mac-scheduler.h` modules are the implementation of the Proportional Fair MAC scheduler. However, it was modified to perform as the Priority-aware Round Robin scheduler. Some modifications can be found at functions `PfFfMacScheduler::DoCschedLcConfigReq` which is for configuring the logical links and updating the priority-tag of each flow.

"uint8_t prioUlDl = params.m_logicalChannelConfigList.at(i).m_prio;

flowStatsDl.priority = prioUlDl;"

The most important modifications were made can be found at `PfFfMacScheduler::DoSchedDlTriggerReq` from line 976

As specified in section 4.2.2, a new QoS group needed to be established for remote control communications traffic. The modifications can be found at *eps-bearer.cc* and *eps-bearer.h*

```
bool
EpsBearer::IsGbr () const
{
  // 3GPP 23.203 Section 6.1.7.2
  switch (qci)
    {
    case GBR_CONV_VOICE:
    case GBR_CONV_VIDEO:
    case GBR_GAMING:
    case GBR_NON_CONV_VIDEO:
    case GBR_MTC_TIME_CRITICAL_FIRST:
    case GBR_MTC_TIME_CRITICAL_SECOND:
    case GBR_MTC_TIME_NON_CRITICAL:
      return true;
    case NGBR_IMS:
    case NGBR_VIDEO_TCP_OPERATOR:
    case NGBR_VOICE_VIDEO_GAMING:
    case NGBR_VIDEO_TCP_PREMIUM:
    case NGBR_VIDEO_TCP_DEFAULT:
      return false;
    default:
      NS_FATAL_ERROR ("unknown QCI value " << qci);
      return false;
    }
}

uint8_t
EpsBearer::GetPriority () const
```

```
{
  // 3GPP 23.203 Section 6.1.7.2
  switch (qci)
    {
    case GBR_CONV_VOICE:
      return 5;
    case GBR_CONV_VIDEO:
      return 7;
    case GBR_GAMING:
      return 6;
    case GBR_NON_CONV_VIDEO:
      return 8;
    case NGBR_IMS:
      return 4;
    case NGBR_VIDEO_TCP_OPERATOR:
      return 9;
    case NGBR_VOICE_VIDEO_GAMING:
      return 10;
    case NGBR_VIDEO_TCP_PREMIUM:
      return 11;
    case NGBR_VIDEO_TCP_DEFAULT:
      return 12;
    case GBR_MTC_TIME_CRITICAL_FIRST:
      return 1;
    case GBR_MTC_TIME_CRITICAL_SECOND:
      return 2;
    case GBR_MTC_TIME_NON_CRITICAL:
      return 3;
    default:
      NS_FATAL_ERROR ("unknown QCI value " << qci);
      return 0;
    }
}

uint16_t
EpsBearer::GetPacketDelayBudgetMs () const
{
  // 3GPP 23.203 Section 6.1.7.2
  switch (qci)
    {
    case GBR_CONV_VOICE:
      return 100;
    case GBR_CONV_VIDEO:
      return 150;
    case GBR_GAMING:
      return 50;
    case GBR_NON_CONV_VIDEO:
      return 300;
    case NGBR_IMS:
      return 100;
```

```
    case NGBR_VIDEO_TCP_OPERATOR:
      return 300;
    case NGBR_VOICE_VIDEO_GAMING:
      return 100;
    case NGBR_VIDEO_TCP_PREMIUM:
      return 300;
    case NGBR_VIDEO_TCP_DEFAULT:
      return 300;
    case GBR_MTC_TIME_CRITICAL_FIRST:
      return 20;
    case GBR_MTC_TIME_CRITICAL_SECOND:
      return 50;
    case GBR_MTC_TIME_NON_CRITICAL:
      return 1000;
    default:
      NS_FATAL_ERROR ("unknown QCI value " << qci);
      return 0;
    }
}

double
EpsBearer::GetPacketErrorLossRate () const
{
  // 3GPP 23.203 Section 6.1.7.2
  switch (qci)
    {
    case GBR_CONV_VOICE:
      return 1.0e-2;
    case GBR_CONV_VIDEO:
      return 1.0e-3;
    case GBR_GAMING:
      return 1.0e-3;
    case GBR_NON_CONV_VIDEO:
      return 1.0e-6;
    case NGBR_IMS:
      return 1.0e-6;
    case NGBR_VIDEO_TCP_OPERATOR:
      return 1.0e-6;
    case NGBR_VOICE_VIDEO_GAMING:
      return 1.0e-3;
    case NGBR_VIDEO_TCP_PREMIUM:
      return 1.0e-6;
    case NGBR_VIDEO_TCP_DEFAULT:
      return 1.0e-6;
    case GBR_MTC_TIME_CRITICAL_FIRST:
      return 1.0e-6;
    case GBR_MTC_TIME_CRITICAL_SECOND:
      return 1.0e-6;
    case GBR_MTC_TIME_NON_CRITICAL:
      return 1.0e-6;
```

```
  default:
    NS_FATAL_ERROR ("unknown QCI value " << qci);
    return 0;
  }
}
```

As we can see in the code, there are three different new groups of QoS parameters defined which are MTC_TIME_CRITICAL_FIRST, MTC_TIME_CRITICAL_SECOND, and MTC_TIME_NON_CRITICAL. Within this research, we only use the first one for the remote control communication traffic; however, the others are necessary when more energy-related control applications are implemented with different QoS requirements. Since QCI is a 8-bit field, more QoS groups can be defined following this method.

B.3 Using the Priority-aware Round Robin MAC scheduler

Firstly, the user needs to enable the scheduler

```
lteHelper->SetSchedulerType("ns3::PfFfMacScheduler");
```

Secondly, it is required to establish a dedicated bearer for remote control communication and define the associate QCI for this dedicated bearer as the MTC_TIME_CRITICAL_FIRST

```
for (uint32_t u = 0; u < lteMmsUeContainer.GetN(); u++)
        {
        enum EpsBearer::Qci q1 = EpsBearer::GBR_MTC_TIME_CRITICAL_FIRST; // 
define Qci type --> priority = 1
                GbrQosInformation qos1;
                EpsBearer bearer1 (q1, qos1);
                Ptr<EpcTft> tft1 = Create<EpcTft> ();
                EpcTft::PacketFilter ulpf1;
//              ulpf1.remotePortStart = 102;
//              ulpf1.remotePortEnd = 102;
//              ulpf1.remoteAddress = "1.0.0.2";
//              ulpf1.remoteMask = "255.0.0.0";
//              ulpf1.direction = EpcTft::DOWNLINK;
                tft1->Add(ulpf1);
                 lteHelper->ActivateDedicatedEpsBearer (lteMmsUeDevice.Get(u), bearer1, 
tft1);
        }
```

For background traffic, it is possible to establish multiple dedicated bearers for different background applications following the same method as above.