UNIVERSITY OF TWENTE.

Master Thesis

University of Twente
Faculty of Electrical Engineering, Mathematics and
Computer Science (EEMCS)
Design and Analysis of Communication Systems (DACS)

Integration of IEC 61850 MMS and LTE to support smart metering communications

Giang T. Pham

August 2013

Supervisors:
Dr. ir. Georgios Karagiannis
Dr. ir. Geert Heijenk
Prof. dr. ir. Boudewijn Haverkort
Ir. Frans Campfens

Abstract

Smart Grid is the term used for next generation power grid which aims to minimize environmental impact, enhance markets, improve reliability and service, and reduce costs and improve efficiency. In order to achieve these goals, Smart Grid relies on a two-way information exchange infrastructure made possible by communication networks. The initial step will be the deployment of the two-way smart metering communication between the smart meters and the control centre, which can be seen as the key enabler for future Smart Grid applications to be built.

IEC 61850 is the international standard protocol defined to ensure interoperability within Substation Automation System (SAS) by standardizing the abstract data models and services to support SAS communications. As the scope of the protocol is extended beyond substation boundary, it has the potential to be used for smart metering communication.

IEC 61850 services for metering are mapped on the Manufacturing Message Specification (MMS). MMS is the OSI protocol than can run over TCP/IP or OSI networks to support IEC 61850 services. Currently the MMS uses Ethernet as the layer 2 protocol. However, when applying to the smart metering infrastructure, it is not favourable to run Ethernet because of its physical limitations (e.g., wired technology) and high installation costs. Long Term Evolution (LTE), a fourth-generation (4G) cellular standard, seems to be more suitable with its advanced technologies to provide high-capacity, low-latency, secure and reliable data-packet switched network.

The objective of this research is to integrate IEC 61850 MMS and LTE to support communications between smart meters and the central meter data management system. The research includes a literature study of IEC 61850 MMS protocol, focusing on its requirements to support smart metering communication, and simulation-based performance evaluation of IEC 61850 MMS smart metering traffic over LTE network.

Acknowledgments

During the work of this thesis, I have received the assistance of many people whose contributions I gratefully acknowledge.

First, I am heartily thankful to my advisor, Dr. ir. Georgios Karagiannis, whose encouragement, guidance and support from the initial to the final stage enabled me to develop an understanding of the subject. I would like to thank Dr.ir. Geert Heijenk and Prof. dr. ir. Boudewijn Haverkort for their support during the thesis development. The value and contribution of this thesis have increased a lot with their comments. I would also like to express my thankfulness to Ir. Frans Campfens, who has provided me great support and inputs during my internship period at Alliander and during the work of this thesis.

I would like to thank the EEMCS members who have supported me with the practical experiments in this thesis.

Finally, I would like to show my gratitude to the University of Twente for bringing me here, a wonderful place for learning and development.

Giang Pham

Table of Contents

List of Abbreviations

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AMI	Advanced Metering Infrastructure
AuC	Authentication Centre
BPLC	Broadband Power Line Communications
BSAP	Base Station Application Part
BSC	Base Station Controller
BSMAP	Base Station Management Application Part
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CIS	Consumer Information System
CN	Core Network
COSEM	COmpanion Specification for Energy Metering
DER	Distributed energy resources
DLMS	Distribution Line Message Specification
DTAP	Direct Transfer Application Part
EPC	Evolved Packet Core Network
EPRI	Electric Power Research Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EV	Electric vehicles
EV-DO	Evolution Data Optimized
GOOSE	Generic Object Oriented Substation Event
HAN	Home Area Network
HLR	Home Location Register
HSS	Home Subscription Server
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
LD	Logical Device

LN	Logical Node
LTE	Long Term Evolution
MDMS	Meter Data Management System
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MS	Mobile Station
MSC	Mobile Switching Centre
NAS	Non-Access Stratum
NPLC	Narrow-band Power Line Communications
OFDMA	Orthogonal Frequency Division Multiple Access
OMS	Outage Management System
PAPR	Peak-to-Average Power Ratio
PCF	Packet Control Function
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDSN	Packet Data Serving Node
P-GW	Packet Gateway
PICOM	Piece of Information for Communication
PLC	Power Line Communications
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
RAN	Radio Access Network
RLC	Radio Link Control
SC-FDMA	Single Carrier Frequency Division Multiple Access
S-GW	Serving Gateway
SV	Sampled Value
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
VLAN	Virtual Local Area Network
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide interoperability for Microwave Access

List of Figures

List of Tables

Chapter 1

Introduction

The current power grid is evolving toward a modernized grid, often termed Smart Grid, which promises to efficiently deliver sustainable, economic and secure electricity supplies. In order to realize this objective, Smart Grid requires bidirectional communication between different components within the grid such as power plants, substations and control centres. Smart metering is the first application that utilizes the bidirectional communication channel to provide reliability, robustness and efficiency to the Smart Grid, and more importantly, lays a foundation for future applications to be built.

The International Electrotechnical Commission (IEC) has introduced IEC 61850 standard to solve the interoperability among different Intelligent Electronic Devices (IEDs) from different manufacturers within a substation automation domain. An IED is the microprocessor based device that performs several protective, control, and similar functions. The main idea of IEC 61850 to break down the functions of IEDs into core functions called Logical Nodes (LNs). Several logical nodes can be grouped into a Logical Device (LD) which provides communication access point of IEDs. By standardizing the common information model for each LN and the associated services, IEC 61850 provides the interoperability among IEDs of different manufacturers in substation automation systems.

IEC 61850 has been extended outside the scope of substation automation systems to cover distributed energy resources (DERs), electric vehicles (EVs), and the communication to control centre. Therefore it can potentially be applied to support metering services within distribution network, starting with the support for Advanced Metering Infrastructure (AMI).

4G Long Term Evolution (LTE) is the latest cellular technology defined by 3rd Generation Partnership Project (3GPP) and is a promising choice as the WAN technology to support IEC 61850 as the application protocol.

1.1 Problem statement and motivation

IEC 61850 services for metering are mapped on the Manufacturing Message Specification (MMS). MMS is the OSI protocol than can run over TCP/IP or OSI networks to support IEC 61850 services. Currently the MMS uses Ethernet, a popular Local Area Network (LAN) protocol, as the underlying communication network technology. However, the high setup cost and non-flexible nature of Ethernet may introduce difficulties for applying IEC 61850 MMS in energy distribution networks. It is therefore preferable to use IEC 61850 MMS on top of another Wide Area Network (WAN) technology to realize the communication between smart meters and data centre in AMI.

4G Long Term Evolution (LTE) is the latest cellular technology defined by 3rd Generation Partnership Project (3GPP) and is a promising choice as the WAN technology to support IEC 61850 as the application protocol. By having this integration, we combine the advantages of both technologies for the deployment of AMI, as IEC 61850 has been used widely within the power grid to ensure interoperability while LTE provides a wide geographical coverage, low delay, and high bandwidth.

Therefore, this networking solution for AMI makes smart metering communication possible, even in a real-time manner. By collecting meter data in real-time, utilities can correctly predict the load profile, perform load forecasting, support real-time pricing and demand response, etc.

Another advantage of using this approach is that the utilities can offload the deployment, operation and maintenance to a mobile operator by using public networks, significantly reducing costs and save implementation time thanks to outsourcing one of the most complex tasks in deploying an AMI project.

The important question is to investigate whether this solution can meet the performance requirements imposed by the real-time smart meter collection application, given a huge number of meters to be served in a large area. Another aspect to look at is the mutual influence of smart meter traffic and existing LTE traffic within a public cellular network. Therefore, this research can provide major contributions to both power utilities and mobile operators in the deployment of an AMI project.

To the best of our knowledge, there has been no previous work that specifies how IEC 61850 MMS can be used for smart metering within the AMI. There are a number of logical nodes defined in IEC 61850 that represent different functions of an IED within the substation domain, however there is no specification on how the logical nodes can

be used for smart metering applications. In addition, there has been no work that discusses how the IEC 61850 used for smart metering can be integrated with LTE. The work proposed in this assignment is innovative, since it specifies, designs, implements and evaluates a solution on integrating the IEC 61850 MMS used for smart metering application.

1.2 Research questions

The objective of this research is to integrate IEC 61850 MMS and LTE to support communications between smart meters and the central meter data management system. Therefore, the main research question is:

How can smart metering communication be supported by using IEC 61850 MMS over LTE?

In order to answer this main question, several research questions are defined:

1- What are the main requirements and challenges of integrating IEC 61850 MMS and LTE for smart metering communication?

The first step is to identify the requirements imposed by IEC 61850 MMS for metering services. The challenges of the integration of IEC 61850 MMS and LTE are also pointed out by answering this question.

2- How can the selected challenges be solved?

An answer for this question will clarify how the identified challenges in question 1 are solved.

3- Can the provided solutions to the selected challenges satisfy the performance requirements?

Using the provided solutions by answering question 2, the performance of the integration of IEC 61850 MMS and LTE is evaluated to see if it meets the requirements that have been defined in question 1.

1.3 Research methodology

The questions 1 is answered using literature study. The answers to the research questions 2 and 3 are provided by using the Waterfall research method. In particular, the

solutions to the selected challenges will be specified, designed, implemented and evaluated with the NS3 LENA [69] simulation environment.

1.4 Structure of the report

This report is structured as follows: Chapter 2 gives some background information on Smart Grid, distribution network and supporting communication technologies, IEC 61850 standard and its application in smart metering. A brief overview on LTE architecture will also be described in this chapter. Chapter 3 discusses the performance requirements for the underlying communication technologies to support smart meter communication. In this chapter, the challenges that need to be solved are also identified. The answer to question 1 is delivered in chapter 3. Chapter 4 and 5 answer question 2, where the specifications and design of the provided solution is presented in chapter 4, while the actual implementation and verification of the developed solution models are included in chapter 5. Chapter 6 presents the experiments and performance evaluation of the solution, which answer question 3. First, the simulation environment and descriptions of the experiments and performance metrics are described. In the simulation, different scenarios are defined based on the goal of this assignment. After that, the simulation results are collected and analysed. Finally, chapter 7 provides some conclusion of the assignment and future works.

Some parts 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. Specifically, the technical specifications of IEC 61850 in chapter 2 and the IEC 61850 message types and performance are identical. The design of IEC 61850 MMS model in chapter 4 and the IEC 61850 MMS model and LTE background traffic implementation in chapter 5 are also developed jointly by the authors, and the text used to describe these parts are exactly the same. The reason for this is that the students focussed on similar research areas, which both requires the background study, design and implementation of the simulation models for the experiments.

Chapter 2

Background

The chapter gives some background information on Smart Grid and the need to have a robust communication network for the Advanced Metering Infrastructure. The IEC 61850 standard and its application in smart metering are described in this chapter, followed by an overview of Long Term Evolution (LTE) technology.

2.1 Smart Grid

Many believe that there is a need for the current power grid to undergo a profound change to evolve into a more modern grid. The existing power grid relies on some central massive power plant to generate electricity, and distribute it to the places where it is consumed (Figure 2.1).

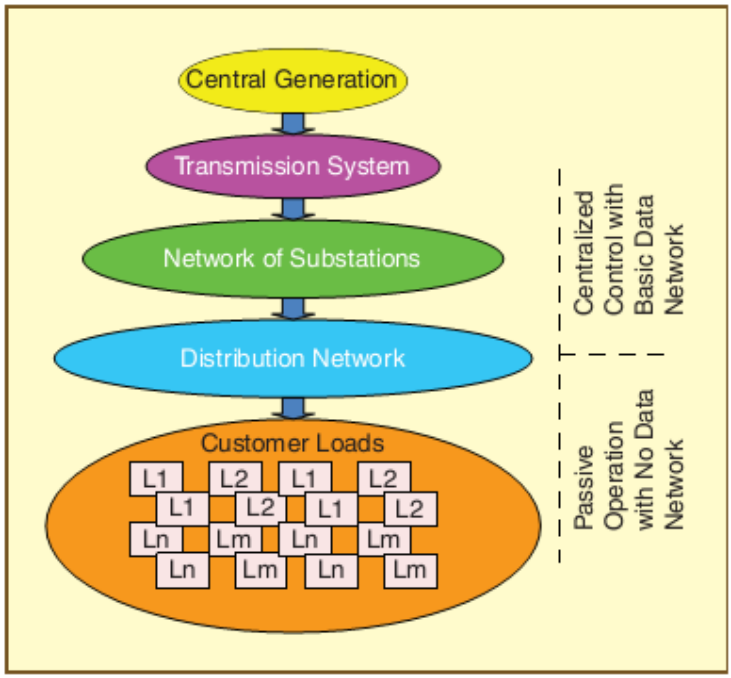


Figure 2.1 - Traditional power grid architecture, copied from [5]

This infrastructure has existed for several decades, and cannot cope with the emerging challenges nowadays. For example, the European 20-20-20 targets [2] 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 DERs that run on renewable energy such as solar or wind has to be integrated, which poses problems for the grid.

More EVs will be used as they are environmentally friendly, but using them widely will bring 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. [1], [3]. According to the Electric Power Research Institute (EPRI) [4], "a Smart Grid is one that incorporates information and communications technology into every aspect of electricity generation, delivery and consumption in order to minimize environmental impact, enhance markets, improve reliability and service, and reduce costs and improve efficiency." [4]

2.2 Advanced Metering Infrastructure

2.2.1 The need for Advanced Metering Infrastructure in Smart Grid

In order to achieve the goals mentioned, Smart Grid has to rely on a two-way information exchange infrastructure made possible by communication networks. The initial step will be the deployment of the two-way Advanced Metering Infrastructure (AMI), which is the key enabler for future smart applications to be built [5].

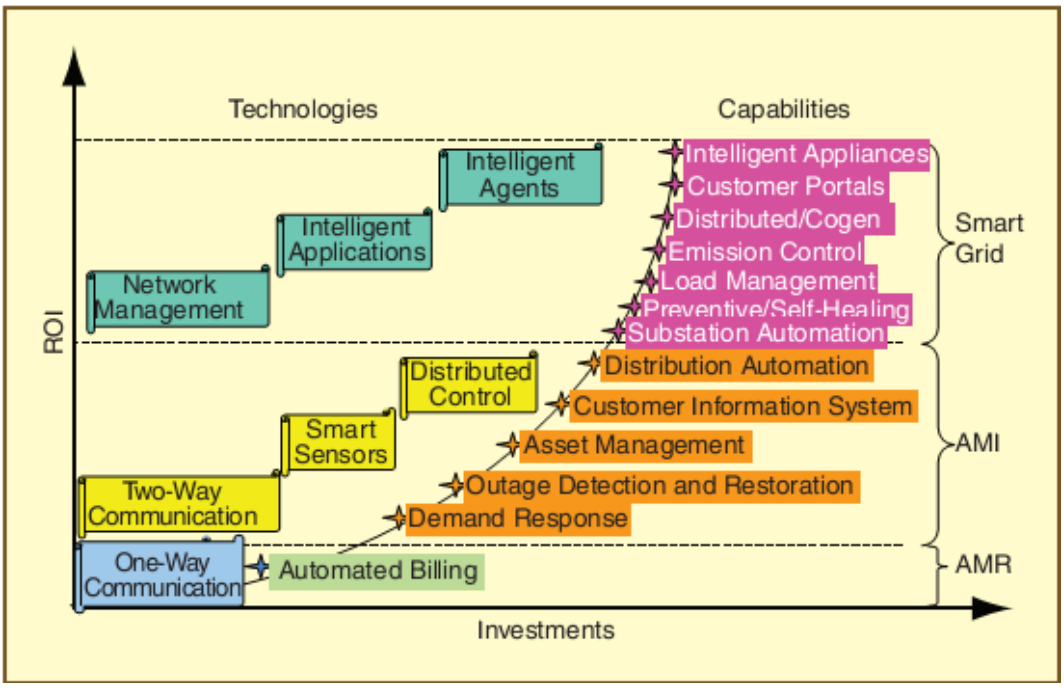


Figure 2.2 - The evolution of the smart grid, copied from [5]

In fact, communication networks have been in existence for several decades along with the power grid for monitoring and protection control, but the network architecture has not changed much since the first day [6]. Power utilities still do not have much insight into distribution network, where nearly 90% of all power problems come from [5]. Communication networks will provide more information about the grid which can help utilities to ensure higher availability and quality of the power they offer to the customers.

Having robust communication infrastructure will also facilitate high penetration of DERs into the current grid. Traditionally, power flows one way from major generators via transmission lines to the distribution network. However, more DERs, mostly based on renewable resources such as wind and solar, are being integrated to the grid and injecting power directly into the distribution network. This requires communication networks to inform operating centre of the DER status to take remedial actions in case of an outage, e.g. making sure DERs are offline to prevent damage to the equipment and ensure the human safety [7].

The use of electric vehicles (EV) is encouraged as it helps reducing fuel consumption and pollutant emissions. Nevertheless, the emergence of electric vehicles introduces further demands on the grid for charging cars, and brings challenges like the case of

DERs. Communications are needed to control the normal operation of the charging of the EVs. [7].

In short, communication networks play a vital role in the development of the current grid towards a modernized, smarter one, which will improve service reliability and quantity to customers, increase productivity and utilization for utilities, and facilitate renewable energy resources.

Utility companies are moving towards advanced metering infrastructure (AMI) with the widespread roll-out of smart meters, which features two-way communication that does not only allow utilities to perform automated readout functions of meters like its predecessor Automatic Meter Reading (AMR), but also allows the control of smart meters [5], [8].

Through AMI, utilities can perform demand response, dynamic tariffs and impose load management [5]. The concept of smart grid clearly does not stop with the deployment of smart meters. The communication network used for AMI will be utilized for further applications (Figure 2.2). The implementation of an AMI will be the beginning of the steps towards the Smart Grid vision.

2.2.2 AMI architecture

AMI is a fully configured infrastructure that includes Home Area Network (HAN), smart meters, communication networks from smart meters to local data concentrators, back-haul communication networks to corporate data centres, meter data management systems (MDMS), and data integration into existing and new software application platforms [9]. Figure 2.3 describes the overview architecture of AMI.

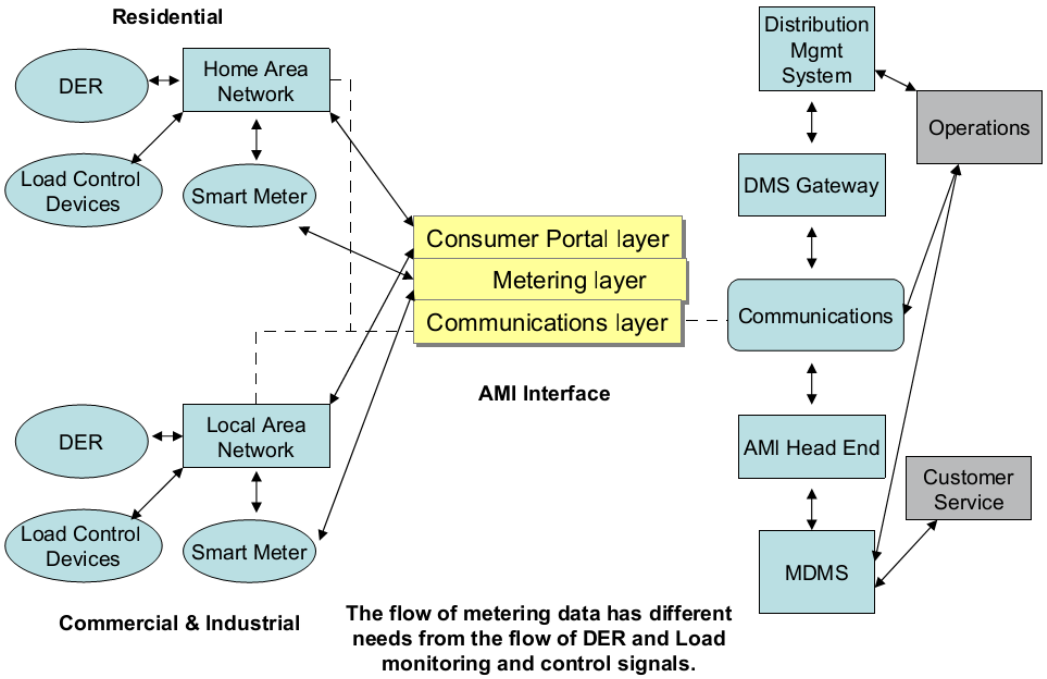


Figure 2.3 - AMI overview, copied from [9]

AMI systems can bring benefits to both users and service providers, as they can: [10]

- Give users feedback on their energy consumption and costs, hence promote economical usage.
- Support dynamic pricing, thereby shift the resource usage from times of high demand to times of low demand.
- Create an infrastructure for future smart grid applications.

There are a number of components that are used in an AMI system [9]:

- Smart Meter: an electronic meter that functions as an intelligent end-point for AMI. It can perform many more functions than a conventional meter, such as:
    - Time-based pricing
    - Consumption data for consumer and utility
    - Remote on/off operations
    - Load limiting, or demand response
    - Communications with intelligent devices within HAN

- Home Area Networks (HAN): a communication system for conveying real time price, load cost and control of load within customer's property. The energy management functions may include:
    - In-home display for showing energy consumption
    - Local control actions
    - Response to price signals
- Communication infrastructure: supports bi-directional and continuous interaction between the utility, the consumer and controllable electrical load. Several protocols and communication media can be employed. The communication infrastructure will be described in more details in the next section.
- Meter Data Management System (MDMS): A MDMS is a database with analytical tools that enable interaction with other information systems (see Operational Gateways below) such as Consumer Information System (CIS), billing systems, Outage Management System (OMS), etc. One of the primary functions of an MDMS is to perform validation, editing and estimation (VEE) on the AMI data to ensure that despite disruptions in the communications network or at customer premises, the data flowing to the systems described above is complete and accurate.
- Operational Gateways: interfaces with many system-side applications to support transmission and distribution in the grid.

2.2.3 Communication technologies for AMI

Several standards can be used for communications in AMI. The standards and the related OSI placement are depicted in Figure 2.4 and are described in details in [8]. We study some of the standards in terms of its openness, OSI layer position and its intended use and functionalities.

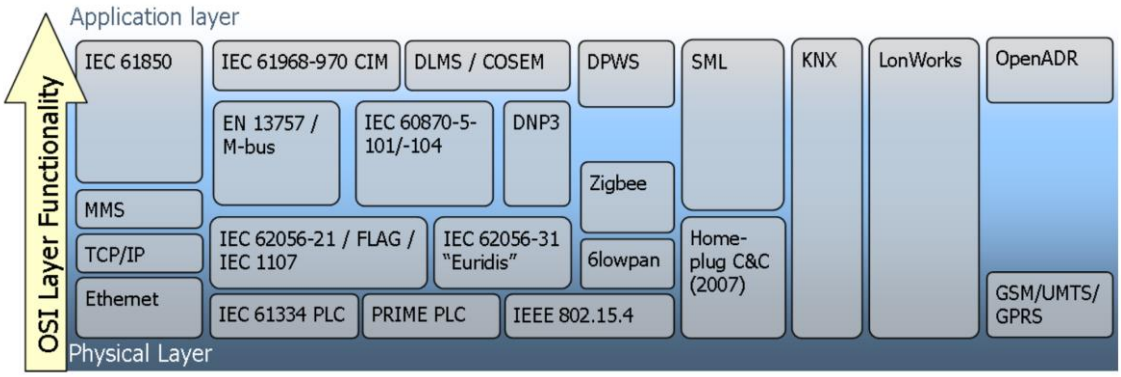


Figure 2.4 - Available standards for smart metering communications, copied from [8]

2.2.3.1 IEC 62056-21

The IEC 62056-21 standard, referred to as "Flag" or IEC 1107 [71], describes software protocols and hardware suitable for data exchange with utility meters. At the hardware side, an optical interface and a 3 two-wire system are described. On top of this, asynchronous half-duplex ASCII-based RS232 data transfer is used. IEC 62056 supports different operating modes, labelled from A to D, which differ in baud rate, directionality and security. IEC 62056-21 is one of the first meter data exchange standards and is widely used today. However it does not use a data model or uniform memory mapping, which requires manufacturer specific information and limits interchangeability.

2.2.3.2 Smart Message Language (SML)

SML [72] is a communication protocol for data acquisition and parameterization whose main purpose is to have a simple structure that is usable in low-power embedded devices. On the application layer defines a file and document structure to carry data between the measuring point and a collection centre. SML provides two options for the presentation layer: readable XML encoding or more efficient SML binary coding.

In typical metering applications SML messages will then be transported using TCP/UDP over IP networks. SML only defines a message structure. The data model or a standard functions list or interface classes are the task for companion specifications, which is still under development.

2.2.3.3 EN 13757 / M-Bus EN 13757 (Meter bus)

M-Bus [73] is a European standard for the remote interaction with utility meters and various sensors and actuators. Part 2 of the standard describes physical and link layers, while part 3 describes the application layer [74]. M-Bus is also usable for other types of consumption meters. The M-Bus interface is made for communication on two wire, making it very cost effective. A radio variant of M-Bus (Wireless M-Bus) is also specified in EN 13757-4 [75].

2.2.3.4 DLMS/COSEM or IEC 62056

DLMS (Device Language Message specification) (integrated in IEC 62056) [76] is a generalized concept for abstract modelling of communication entities. COSEM (Companion Specification for Energy Metering) sets the rules, based on existing standards, for data exchange with energy meters. DLMS/COSEM defines an object model to view the functionality of the smart meter via interfaces, methods to turn data objects into a series of bytes, and transport the information between the smart meters and data concentrator or centre system. DLMS/COSEM is based on a client/server structure in which the data collection system acts as a client requesting data from the servers (pull operation). Future additions will provide push operation (server to client). DLMS/COSEM can be used over TCP, UDP, HDLC, Meter-Bus, GPRS and different narrow band PLC protocols.

2.2.3.5 IEC 61850

IEC 61850 protocol suite [14] was designed as an effort to solve interoperability between different IEDs from different vendors within substation automation systems. The same approach can be applied to AMI where a large number of smart meters from different vendors are used. Based on the flexibility of the standard, IEC 61850 can be used to cover smart metering application. Using IEC 61850 in metering infrastructure has an advantage that it can be used for other smart grid applications besides smart metering [10]. As an open standard, mature and extensible protocol with success in the substation domain, IEC 61850 will be likely to follow through in the utilities sector. More details of IEC 61850 will be described in section 2.3.

2.3 IEC 61850

2.3.1 Overview

IEC 61850 protocol suite [14] was designed to as an effort to solve interoperability between different IEDs from different vendors within substation automation systems. The standardization approach of IEC 61850 series as mentioned in IEC 61850-1 is to blend the strength of three methods [14]:

- *Functional decomposition:* is used to understand the logical relationship between components of a distributed function which is decomposed and represented as Logical Nodes (LNs)
- *Data flow modelling:* is used to understand the communication interfaces that must support the exchange of information between distributed functional components and the functional performance requirements.
- *Information modelling:* is used to define the abstract syntax and semantics of the information exchanged

The main idea of IEC 61850 is to break down a physical device into logical devices, each of which will be further broken down into Logical Nodes, data objects and data attributes [14].

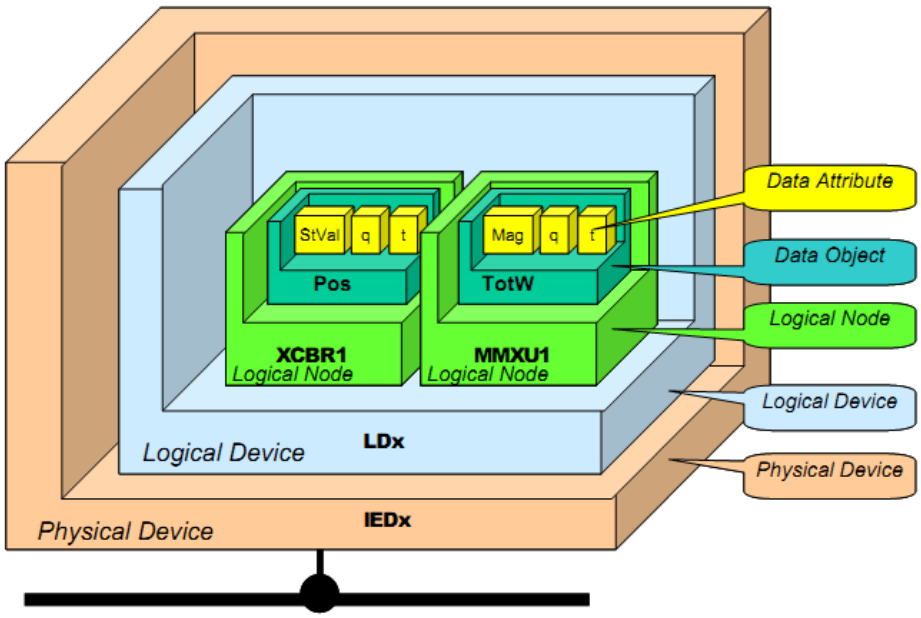


Figure 2.5 - IEC 61850 data modelling, copied from [14]

The Logical Device hosts communication access point of IEDs and related communication services and is hosted by a single IED. However, there's no rule on how to arrange Logical Devices into a physical device which brings a great flexibility to the user.

Logical Nodes are the smallest entities which are derived from the application functions. Logical nodes are the building blocks of the standard since they represent the smallest functions of the device.

For example, Figure 2.5 shows a physical device (IED) which contains one Logical Device. The device has two functions: a circuit breaker (represented by the Logical Node XCBR), and measurement functions (represented by the Logical Node MMXU). The Logical Nodes have their corresponding data objects which contain data attributes with associated values.

In short, IEC 61850 decomposes and standardizes the functions as Logical Nodes, classifies the communication interfaces between different functional levels, and models the information exchange in term of data objects, data attributes and abstract communication services.

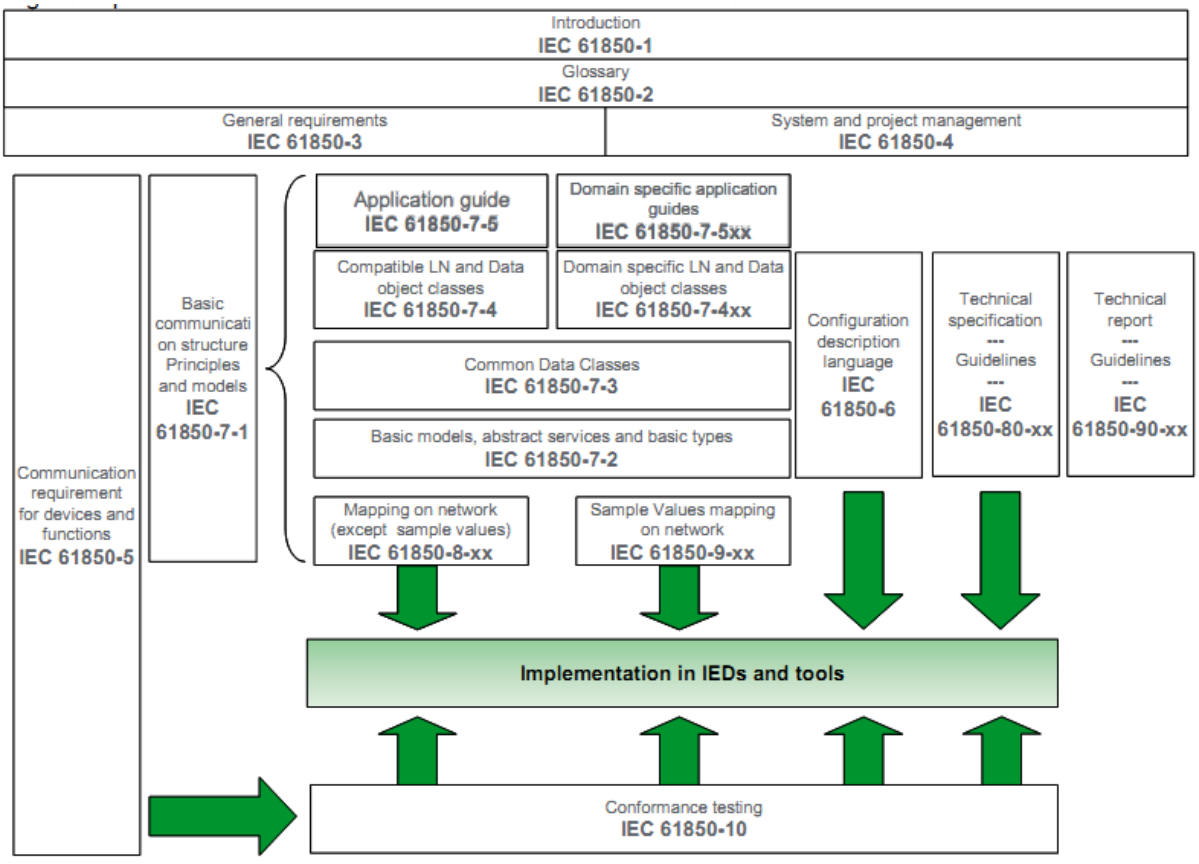


Figure 2.6 - Links between IEC 61850 parts, copied from [14]

IEC 61850 consists of different parts which define different aspects of IEC 61850 (Figure 2.6). These parts convey from general information such as the introduction and overview in part 1, the glossary in part 2, the general requirements in part 3, system and project management in part 4 to the communication requirements and specifications in part 5, part 6 and part 7-1 to 7-4.

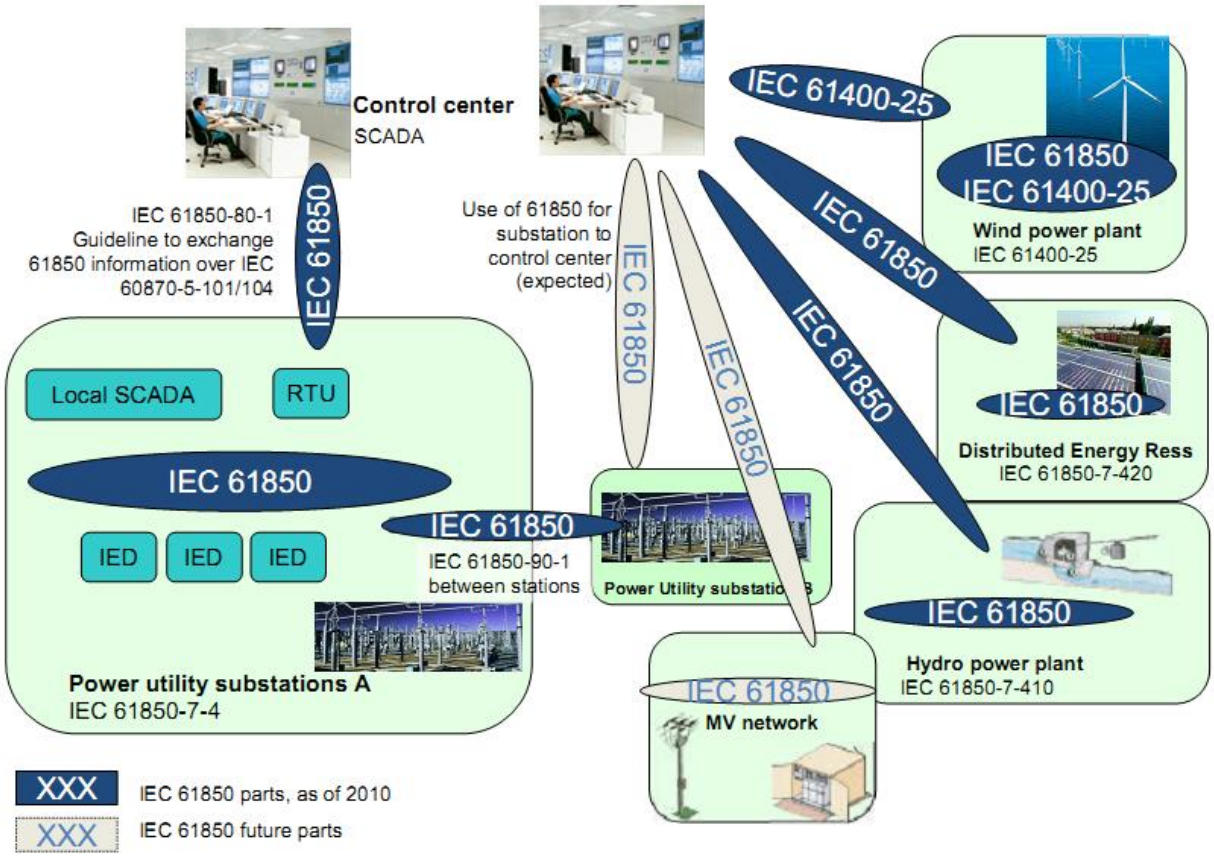


Figure 2.7 - Application scope of IEC 61850, copied from [14]

From the original scope within substation automation systems, IEC 61850 has been extended to define information models for power plants, DERs, and many more areas in the future (Figure 2.7).

What makes the flexibility of IEC 61850 is the split between the communication and application. By specifying a set of abstract services and objects, IEC 61850 allows the user to design different applications without relying on the specific protocols (Figure 2.8). As a consequence, the data models defined in IEC 61850 can be used on the diversity of communication solutions.

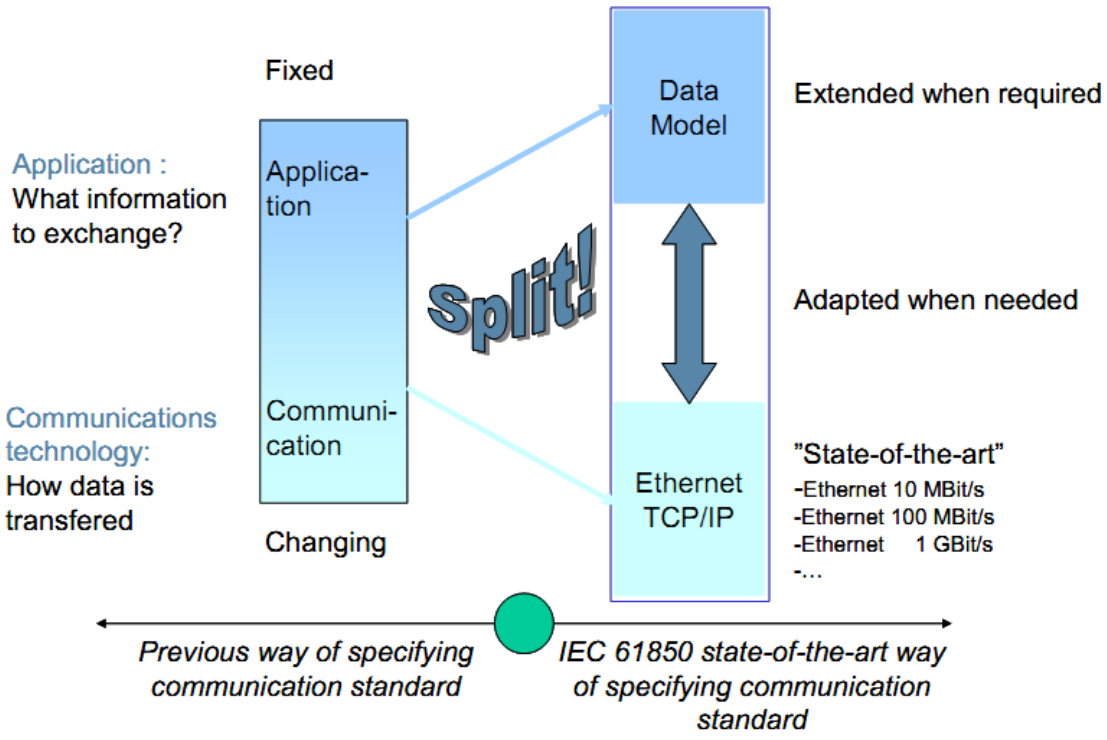


Figure 2.8 - The split between application and communication of IEC 61850, copied from [14]

Due to this split, the models and services have to be mapped to specific protocols to support different functional requirements for protection, control, supervision and monitoring. Parts 8-1 [17], 9-1 [60], 9-2 [61] of the standard define the specific communication service mapping (SCSM) to different communication technology, e.g. Ethernet, TCP/IP, etc.

Besides standardizing the data format 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. The complete Abstract Communication Service Interface (ACSI) services can be found in the Appendix. These services are described in details in part 7-2 of the standard [59].

2.3.2 IEC 61850 communication stack

The communication services mapping of IEC 61850 has to meet several communication requirements defined in IEC 61850-5. As a consequence, the different message types which belong to different performance classes are mapped to different communication

protocols in order to support the respective requirement for specific message types. These message types will be described in more details in chapter 3.

The IEC 61850 communication services mapping is depicted in Figure 2.9. The message types which have similar performance requirements are grouped together and mapped to the same protocol. For example the type 1 and 1A messages are very time critical so that they are mapped to Generic Object Oriented Substation Events – GOOSE and directly mapped to Ethernet to reduce processing time caused by overhead of transport and network layer protocols. The raw message type 4 is mapped to Sampled Value (SV) which is a protocol designed to carry raw data and is also directly mapped to Ethernet to achieve time-critical performance.

Type 6 message represents the message used for time synchronization and is mapped to the Simple Network Time Protocol (SNTP).

Message type 2, 3 and 5 which can be used to support core IEC 61850 services are mapped to the Manufacturing Message Specification (MMS).

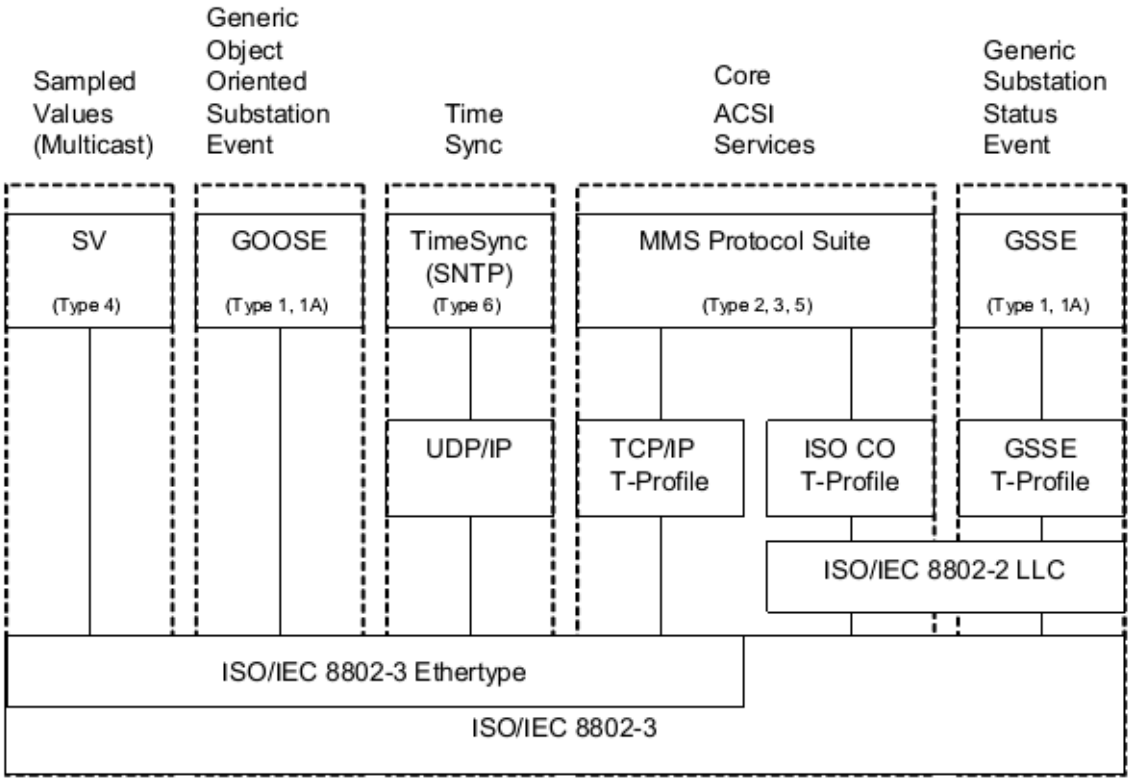


Figure 2.9 - Overview of functionality and profiles, copied from [17]

2.3.3 GOOSE services communication profile

The Generic Object Oriented Substation Events – GOOSE provides fast and reliable system-wide distribution of data, based on a publisher-subscriber mechanism (Generic Substation Event – GSE management). GOOSE is one of the two control classes within the GSE control model (the other is Generic Substation State Events – GSSE).

GOOSE uses Data-set to group the data to be published. The use of Data-set allows grouping many different data and data attributes. Table 2.1 shows the application profile (A-profile) of GSE/GOOSE services:

Table 2.1: Service and protocols for GSE management and GOOSE communication A-profile, copied from [17]

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				

Instead of mapping to the TCP/IP profile like MMS, GOOSE is mapped directly to Ethernet. The transport profile (T-profile) for GSE/GOOSE can be found in Table 2.2. This gives the advantage of improved performance for real-time messages by shortening the Ethernet frame (no upper layer protocol overhead) and reducing the processing time. This type of mapping also utilizes the use of priority tag value within the Ethernet frame to separate time critical and high priority traffic from lower priority traffic. It is shown in [18] that Ethernet with VLAN and Priority Tagging meet the communication requirements for the 4ms latency of Type 1 messages within the substation.

GOOSE provides an efficient method of simultaneously delivery of the same generic substation event information to more than one physical device through the use of multicast services. GOOSE messages contain information that allows the receiving device to know that a status has changed and the time of the last status change [17]. GOOSE sending is triggered by the server by issuing **SendGOOSEmessage** service. The event that causes the server to invoke a **SendGOOSEmessage** service is a local application issue as defined in IEC 61850-7-2 [59], such as detecting a fault by a protection relay.

Table 2.2: GOOSE/GSE T-profile, copied from [17]

OSI model layer	Specification			m/o
	Name	Service specification	Protocol specification	
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.

2.3.4 Sampled Value (SV)

Sampled Value is the protocol for transmission of digitized analogue measurement from sensors (temperature, current transformer, voltage transformer).

Sampled value messages are exchanged in a peer-to-peer publisher/subscriber mechanism like GOOSE messages. However GOOSE uses the multicast model while SMV can be unicast or multicast. Figure 2.10 sketches the comparison between GOOSE and SMV communication models.

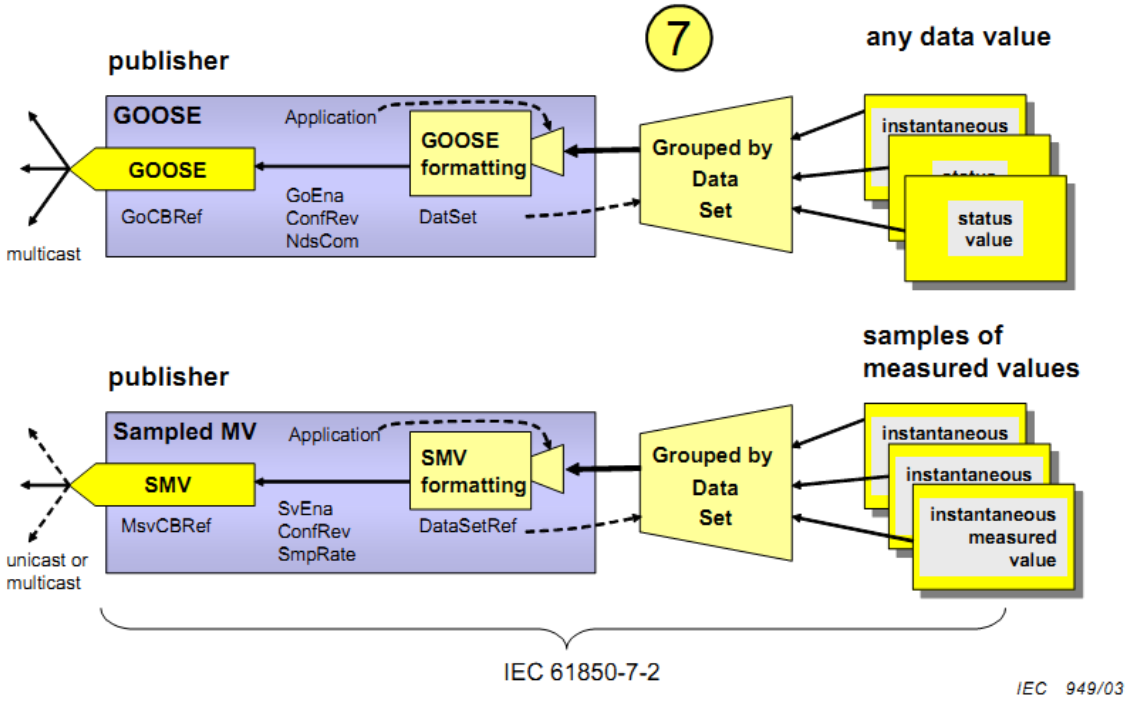


Figure 2.10 - GOOSE and SV peer-to-peer data value publishing model, copied from [59]

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.

The transmission rate of the sampled value can be altered by configuring the Data Attribute **SmpMod** which specifies the definition of units of samples i.e. unit of samples per nominal period, samples per second or seconds per sample; and the **SmpRate** which specifies the sample rate with the definition of units of sample defined by **SmpMod**.

Basically SMV can be mapped to Ethernet with different configuration as defined in part 9-1 [60] and part 9-2 [61] of the IEC 61850 series.

Part 9-1 maps the Sampled Value to a fixed link with pre-configure Data-set. Figure 2.11 presents the communication profile defined in part 9-1.

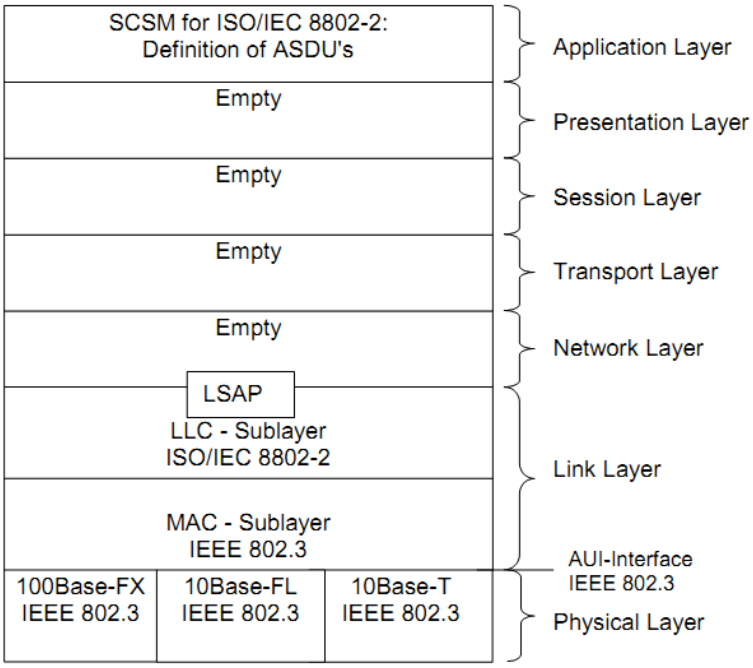


Figure 2.11 - Sampled value mapped to serial unidirectional multi-drop point to point link, copied from [60]

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.

One disadvantage of this direct mapping of GOOSE and SV on Ethernet is that they are not routable in case the communication outside the substation is needed. There are also applications that require the transmission of GOOSE and SV over WAN, e.g. teleprotection between substations, transmitting synchrophasors. There have been some guidelines in [19] that allow the transmission of GOOSE and SV over WAN by using L2 tunnelling or gateway/proxy approaches [19].

2.3.5 Generic Substation State Events – GSSE

This control model is similar to GOOSE. However, the GSSE only supports a fixed structure of status data to be published; meanwhile the data for the GOOSE message is configurable by applying data sets referencing any data [59].

2.3.6 Time Sync

The time synchronization model must provide accurate time to all IEDs in a power utility system for data time stamping with various ranges of accuracy, e.g. millisecond range for reporting, logging and control and microsecond range for sample values [59].

Time synchronization protocol used by IEC 61850 to provide synchronization between IEDs is Simple Network Time Protocol – SNTP. Table 2.3 shows the application profile of the Time Sync service.

Table 2.3: Time Sync A-Profile, copied from [17]

OSI model layer	Specification			m/o
	Name	**Service specification**	**Protocol specification**	
Application	Simple Network Time Protocol	RFC 2030		m
Presentation				
Session				

The transport layer uses the Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) over IP and Ethernet.

2.3.7 Manufacturing Message Specification (MMS)

Manufacturing Message Specification (MMS) [64] is an international standard (ISO 9506) supporting the transfer of real time process data and supervisory control information between networked devices and/or computer applications. MMS defines the following [65]:

- A set of standard objects which must exist in every device, on which operations like read, write, event signalling etc. can be executed. Virtual manufacturing device (VMD) is the main object and all other objects like variables, domains, journals, files etc. comes under VMD.
- A set of standard messages exchanged between a client and a server stations for the purpose of monitoring and/or controlling these objects.

- A set of encoding rules for mapping these messages to bits and bytes when transmitted.

In IEC 61850, MMS supports the mapping of the core ACSI services. In fact, 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. The core ACSI services are mapped to MMS services, then MMS can be mapped to either the TCP/IP or OSI protocol stack [17].

MMS services and protocol are specified to operate over full OSI and TCP compliant communication profiles to support the exchange of real-time data indications, control operations, report notification [17]. The services and protocol of the Application profile (A-Profile) client/server are shown in Table 2.4.

Table 2.4 - Services and protocols for client/server communication A-Profile, copied from [17]

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 2.5, while the OSI T-Profile can be found in Table 2.6.

Table 2.5 - 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.

Table 2.6 - 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. 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.

2.4 Long Term Evolution (LTE)

2.4.1 Overview

Long Term Evolution (LTE) [77] is a fourth generation technology which is standardized in the Release 8 specifications by the 3rd Generation Partnership Project (3GPP). It is capable of providing high data rates as well as support high speed mobility. It has a completely packet switched core network architecture unlike its predecessor Universal Mobile Telecommunications System (UMTS) which is capable

of supporting both the Circuit Switched (CS) as well as Packet Switched (PS) core networks. Compared to CDMA or UMTS, LTE uses new access schemes on the air interface: Orthogonal Frequency Division Multiple Access (OFDMA) in the downlink and Single Carrier Frequency Division Multiple Access (SC-FDMA) in the uplink, which brings further flexibility in user scheduling as well as power efficiency [28]. LTE also features low latency in both the control plane and user plane, which creates new opportunities for real-time application such as video surveillance, distance learning or telemedicine.

In the Smart Grid context, the success and rapid roll-out of LTE in many countries have lead to an increased interest to use this technology for different application domains, including smart metering, distribution automation, fault location, etc. within distribution networks. The rest of this chapter will describe the technologies used in LTE and its network architecture, and will also focus on how LTE can be used to support metering services with IEC 61850 as the application protocol.

2.4.2 Orthogonal Frequency Division Multiple Access (OFDMA)

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 [26]. The aggregation of these many low-rate subcarriers provides a high overall data rate. The subcarriers are orthogonal, that is, the peak of a subcarrier lines up with the zero-crossings of other subcarriers; therefore, no interference occurs between them [26]. This characteristic allows the subcarriers to overlap in the frequency domain, thus saves the bandwidth (Figure 2.12).

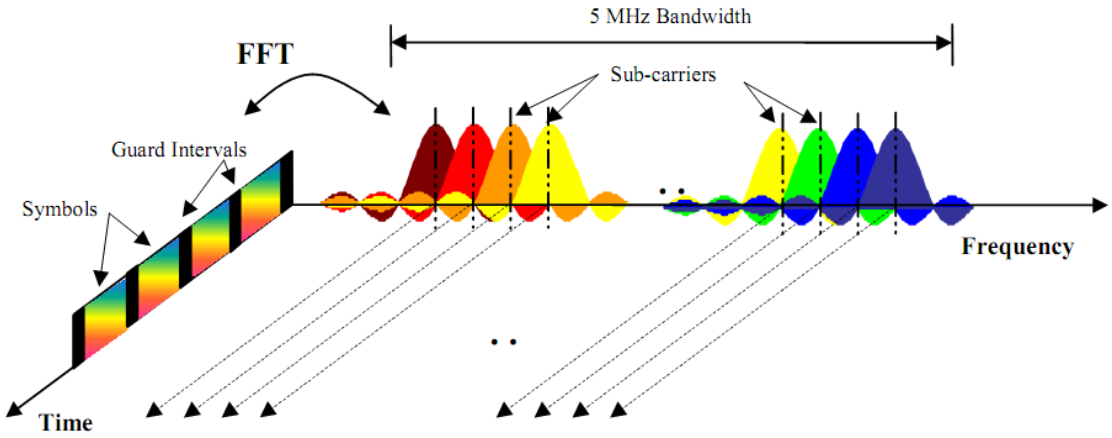


Figure 2.12 - Sub-carrier overlap in OFDMA, copied from [27]

OFDMA allows multiple UEs to share the same bandwidth, as can be seen in Figure 2.13. This is done by assigning a subset of sub-carriers to different UEs allowing multiple low data rate streams to different UEs at the same time [27].

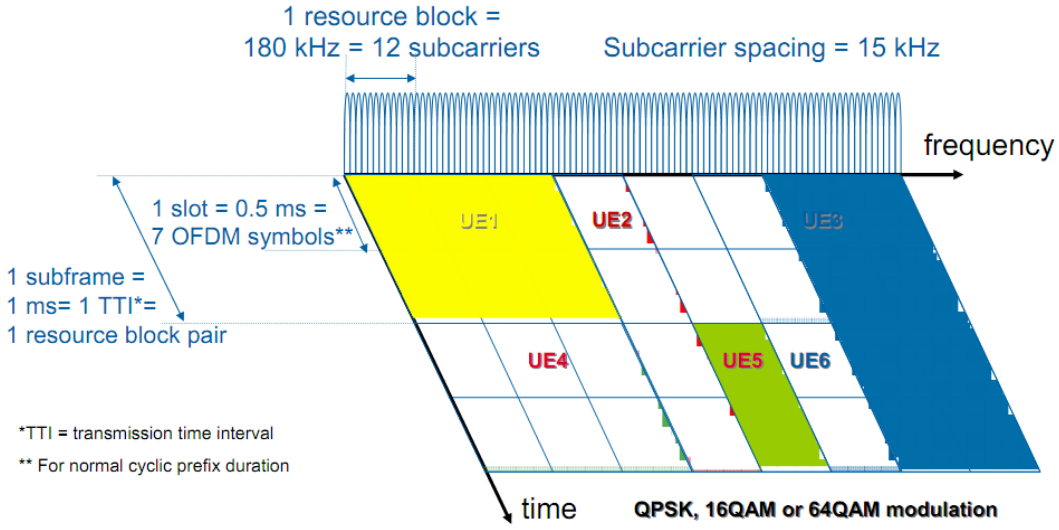


Figure 2.13 - Resource allocation for users using OFDMA, copied from [27]

2.4.3 Single Carrier Frequency Division Multiple Access (SC-FDMA)

For the uplink, SC-FDMA is used instead of OFDMA [26]. One characteristic of OFDMA is the high Peak-to-Average Power Ratio (PAPR), which is the major concern at the UE because it relates to the power amplifier efficiency. The low PAPR is critical

in the UE since it improves power-amplifier efficiency, reduces terminal power consumption and cost, and increases coverage [26].

SC-FDMA uses orthogonal sub carriers to transmit information symbols; however, they transmit the sub carriers sequentially and not in parallel in contrast to OFDMA signals. Relative to OFDMA, this arrangement reduces considerably the envelope fluctuations in the transmitted waveform. SC-FDMA combines the low PAPR characteristic of single-carrier transmission systems with the flexible frequency allocation and multipath resistance offered by OFDMA [26].

2.4.4 Multiple Input Multiple Output (MIMO)

LTE targets a very high performance in system capacity, coverage, and data rates. In order to achieve this, LTE employs multi-antenna techniques besides the modulation scheme and access methods that have been discussed [26].

Multiple Input Multiple Output (MIMO) is one of the most popular advanced multi-antenna techniques. In a Multiple Input Multiple Output (MIMO) system both sides of the communication link has multiple receiving and transmitting antennas. Each antenna uses the same time-frequency space. When a data stream is transmitted it can be divided between the multiple antennas to increase the transfer rate of the stream. MIMO can also be used to allow multiple UEs transmitting and receiving simultaneously [28]. In LTE, the basic configuration are considered to be two receiving and two transmitting antennas per cell on the eNB while there are two receiving and one transmitting antennas per UE. Support for up to 4x4 (4 receiving, 4 transmitting) antennas is also considered [26].

2.4.5 LTE network architecture

The architecture of an LTE network is depicted in Figure 2.14. LTE has a flat all-IP architecture which is divided into four main high level domains: User Equipment (UE), Evolved UTRAN (E-UTRAN), Evolved Packet Core Network (EPC), and the Services domain [28].

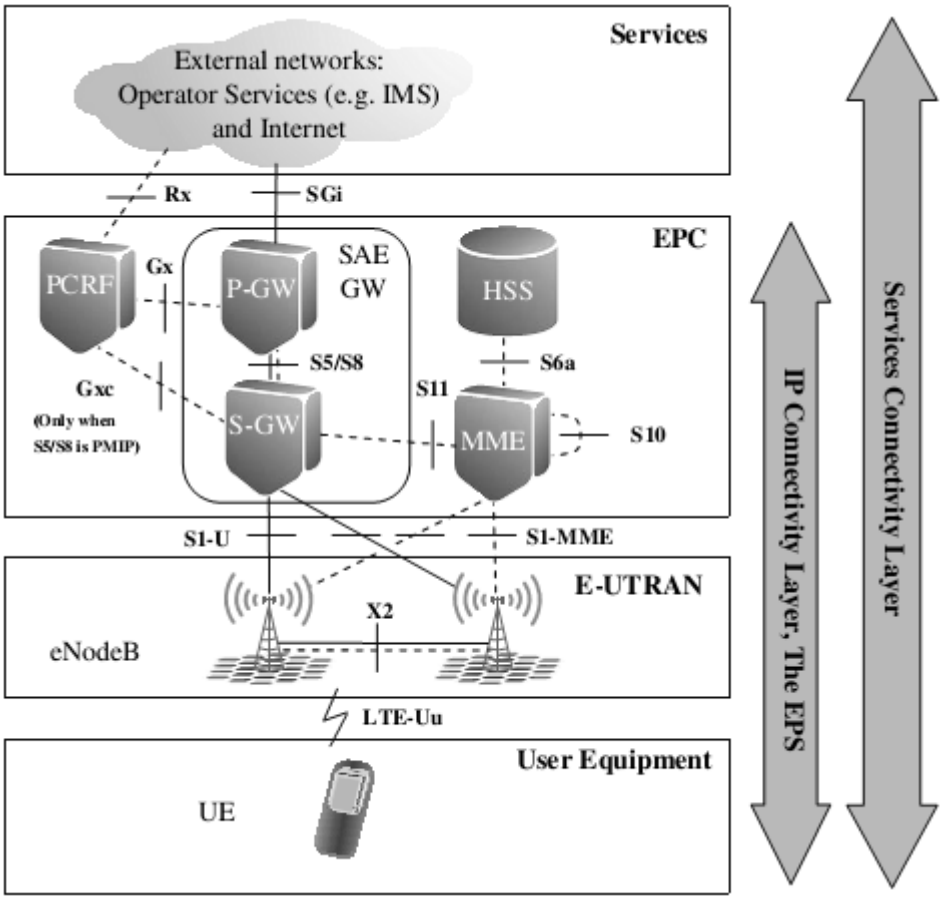


Figure 2.14 - LTE network architecture, copied from [28]

2.4.5.1 User Equipment (UE)

UE is the device that the end user uses for communication. The UE contains the Universal Subscriber Identity Module (USIM), which is used to identify and authenticate the user and to derive 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 [78].

2.4.5.2 E-UTRAN Node B (eNodeB)

E-UTRAN in LTE architecture consists of a single entity, called the eNodeB (eNB). The eNB includes all those algorithms that are located in Radio Network Controller (RNC) in 3GPP Release 6 architecture. By having only one entity in the radio access

network, LTE simplifies network architecture and reduces the latency of all radio interface operations [28].

2.4.5.3 Mobility Management Entity (MME)

The MME is the key control node for the LTE access network. It only operates only in the CP and is not involved in the UP data. The main functionalities of MME include [28]:

- Authentication and Security
- Mobility Management
- Managing Subscription Profile and Service Connectivity

2.4.5.4 Serving Gateway (S-GW)

The high level function of S-GW is UP tunnel management and switching. The S-GW is part of the network infrastructure maintained centrally in operation premises [28].

2.4.5.5 Packet Data Network Gateway (P-GW)

Packet Data Network Gateway (P-GW, also often abbreviated as PDN-GW) is the edge router between the EPS and external packet data networks. It is the highest level mobility anchor in the system, and usually it acts as the IP point of attachment for the UE. It also performs traffic gating and filtering functions as required by the service in question, which is known as Policy and Charging Enforcement Function (PCEF) [28].

2.4.5.6 Policy and Charging Rules Function (PCRF)

PCRF is the network element that is responsible for Policy and Charging Control (PCC). It makes decisions on how to handle the services in terms of QoS, and provides information to the PCEF located in the P-GW. PCRF is a server usually located with other CN elements in operator switching centres [28].

2.4.5.7 Home Subscription Server (HSS)

The HSS (Home Subscriber Server) is the concatenation of the HLR (Home Location Register) and the AuC (Authentication Centre). The HLR part of the HSS is in charge of storing and updating when necessary the database containing all the user subscription information. The AuC part of the HSS is in charge of generating security information from user identity keys. This security information is provided to the HLR and further communicated to other entities in the network [28].

2.4.6 Interface protocols

The interface protocols can be categorized into two main groupings: the control plane protocols and the user plane protocols. The former is responsible for controlling the connections between the UE and the network and the radio access bearers, while the latter carries user data through the access stratum [28].

2.4.6.1 Control Plane protocols

The control plane protocol function is to control the radio access bearers and the connection between the UE and the network, i.e., signalling between E-UTRAN and EPC. Figure 2.15 shows the CP protocols related to a UE's connection to a PDN [28].

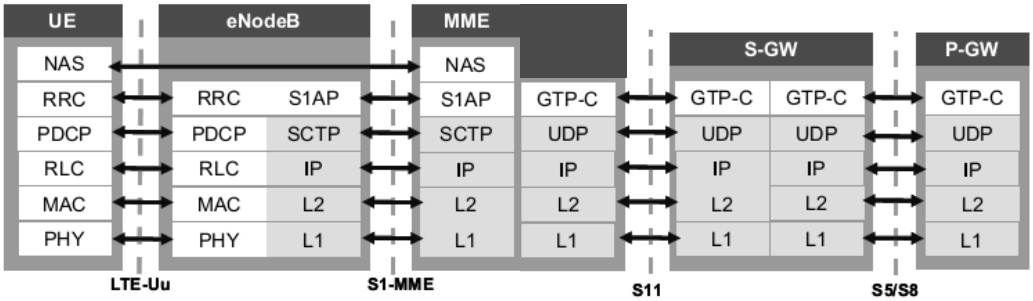


Figure 2.15 - LTE control plane protocols, based on [28]

The topmost layer between the UE and the MME is the Non-Access Stratum (NAS). Main functions of the protocols that are part of the NAS are the support of mobility of

the user equipment (UE) and the support of session management procedures to establish and maintain IP connectivity between the UE and a P-GW.

The radio interface protocols are [28]:

- 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

The S1 interface connects the E-UTRAN to the EPC, and involves the S1 Application Protocol (S1AP), Stream Control Transmission Protocol (SCTP) and Internet Protocol (IP) signalling transport. S1AP handles the UE's CP and UP connections between the E-UTRAN and EPC, including participating in the handover when EPC is involved. SCTP provides the reliable transport and in-order delivery. SCTP is used on top of IP, which allows different data link and physical layer technologies (L2 and L1) [28].

In the EPC, the S11 and S5/S8 interfaces involve the use of GPRS Tunnelling Protocol, Control Plane (GTP-C) on top of Unit Data Protocol (UDP). GTP-C manages the UP connections in the EPC including signalling the QoS and other parameters. In the S5/S8 interface it also manages the GTP-U tunnels and performs the mobility management functions within the EPC (e.g. switching UP tunnels of UE during handover) [28].

2.4.6.2 User Plane protocols

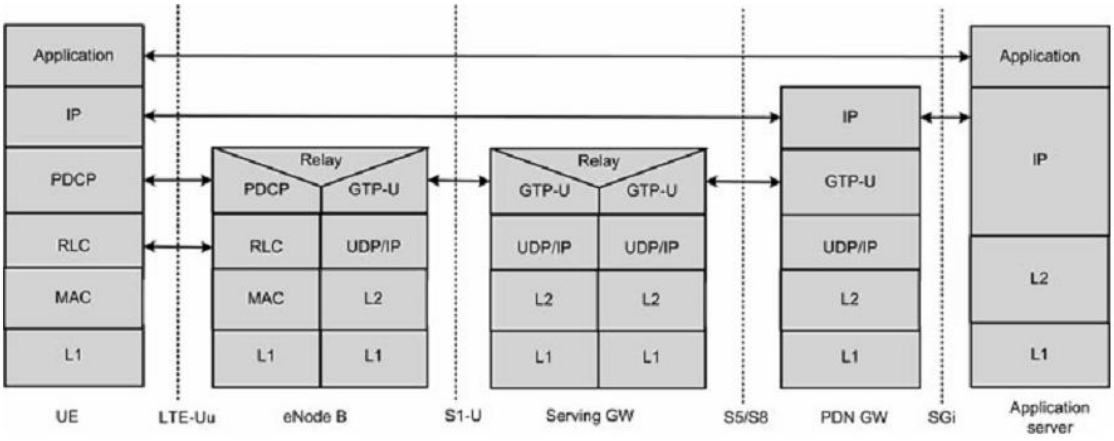


Figure 2.16 - LTE end-to-end user plane protocols, copied from [29]

Figure 2.16 shows the end-to-end user plane protocols on different interfaces between a UE and an Application server. The MME is not involved in the user plane communication. A GPRS Tunnelling Protocol, Control Plane (GTP-U) tunnel is established from the eNB to the P-GW in the EPC to carry user data. The P-GW provides the UE with IP access, so the communication on the Application layer is established between the UE and the Application server [29].

2.4.7 Connection setup in LTE

The goal of setting up the connection (or "attaching") to the network is to obtain the IP address for the UE to communicate with the outside world.

The attach procedure is shown in Figure 2.17 and can be described step-by-step as follows [30]:

- Steps (1) - (4): The mobile terminal (or User Equipment - UE) sends an attach request message to the MME, which performs user authentication based on subscriber's information from to establish a bearer.
- Steps (5) - (11): Based on the APN received from the UE, the MME selects the S-GW and P-GW to be used as destinations when establishing a bearer in accordance with the Domain Name System (DNS), and sends a create session request message to the selected S-GW. The S-GW then performs Establish

bearer processing with respect to the P-GW specified in the create session request message. The P-GW gets information on what charging needs to be applied from the PCRF, and also performs connection processing with a PDN. On completing bearer setup between the S-GW and P-GW, the S-GW sends to the MME information about propagation conditions for the eNodeB. The MME sends this propagation information received from the S-GW to the eNodeB as an initial context setup request, which includes an attach accept message for the UE. The eNodeB now establishes a radio bearer with the UE and sends it the attach accept message, and then receives an RRC connection reconfiguration complete message from the UE and passes propagation information for the S-GW to the MME.

- Steps (12) - (15): On receiving an attach complete message from the UE, the MME sends the propagation information received from the eNodeB to the S-GW. Finally, based on the propagation information so received, the S-GW completes the establishment of a bearer between the eNodeB and S-GW. This completes the establishment of a bearer for the user plane data path UE -eNodeB - S-GW - P-GW.

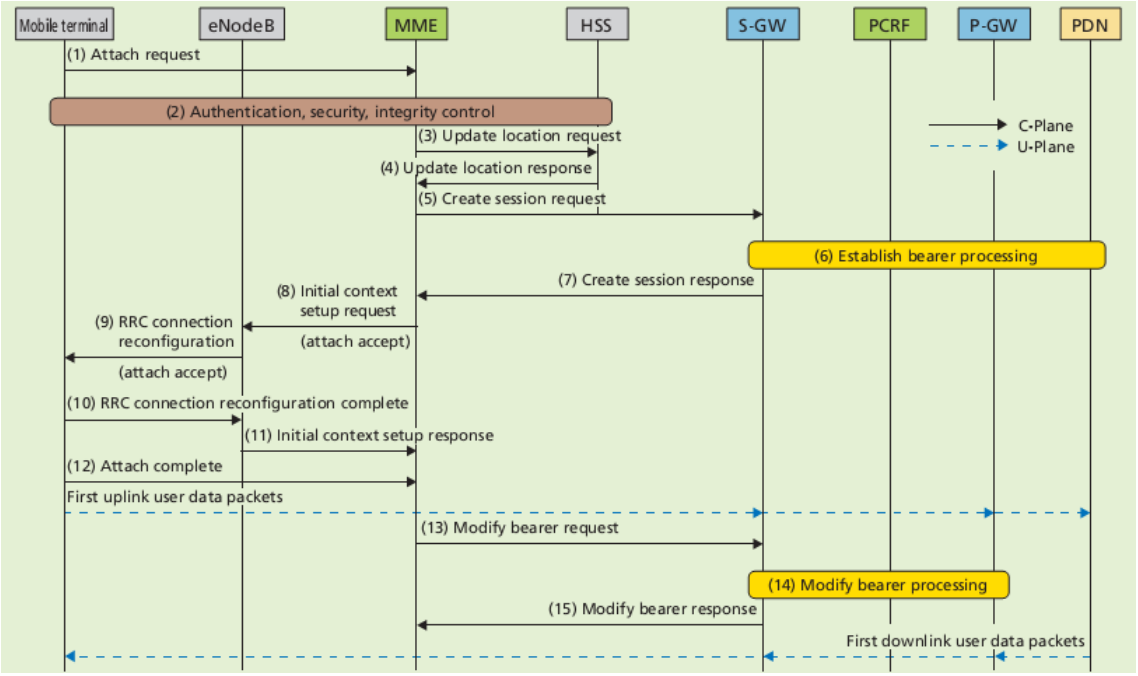


Figure 2.17 - Connection setup in LTE, copied from [30]

2.4.8 LTE Machine Type Communication (MTC) architecture

3GPP has provided some optimization for LTE to improve LTE performance for Machine Type Communication (MTC) or Machine-to-machine (M2M) traffic. These optimizations are discussed in several technical reports on the improvements for M2M communication / MTC in LTE Release 10, 11 and 12. [33], [34], [35]. Figure 2.18 shows an 3GPP architectural reference model for MTC, where a UE used for MTC connecting to the 3GPP network (UTRAN, E-UTRAN, GERAN, I-WLAN, etc.) via the Um/Uu/LTE-Uu interface. Several new entities and reference point protocols have been defined in the control plane to support the transport of M2M traffic, e.g. the MTC signalling protocol (MTCsp), MTC Interworking Function (MTC-IWF), etc. More information about the architecture can be found in [33]

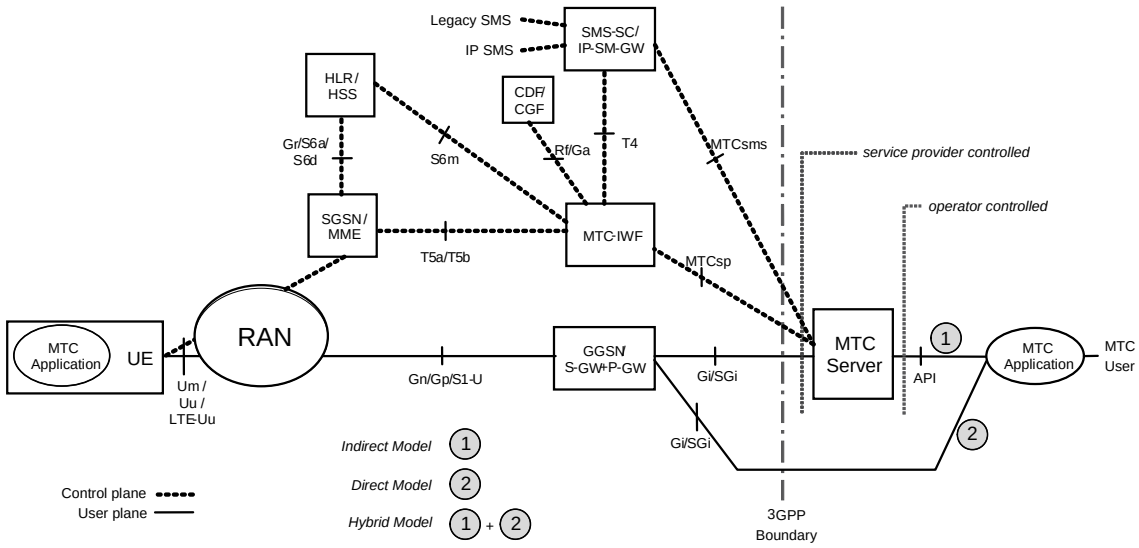


Figure 2.18 - 3GPP architecture for MTC, copied from [33]

M2M is recognized as a key segment in future packet networks. Initial 3GPP efforts have focused on the ability to differentiate machine-type devices to allow the operator to selectively handle such devices in overload situations.

Low priority indicator has been added to the relevant UE-network procedures and overload and Congestion control is done on both core network and radio access network based on this indicator.

In summary, 3GPP Release 10, RAN has the ability to configure MTC devices as (access) delay tolerant UEs. This "delay tolerant" indication is sent by low-priority access UEs to E-UTRAN at RRC setup. The "extended wait timer" (up to 30min) indication is sent by the RAN to low-priority access UEs for the UEs to wait for the admission. To mitigate the overload in the CN, new signalling has been introduced in the E-UTRAN. The CN can indicate "overload" to the E-UTRAN to limit Delay Tolerant traffic, and the E-UTRAN can reject/release "delay tolerant" connections with the "extended wait timer".

Chapter 3

Requirements and Challenges

The core of this chapter is about identifying the requirements of IEC 61850 for the underlying communication technologies especially to support the metering infrastructure.

The basic communication requirements for SAS are described in IEC 61850 part 5 [16]. Based on these requirements, the specific IEC 61850 data modelling in subsequent parts (IEC 61850-7-x) and mappings to dedicated stacks (IEC 61850-8-x and IEC 61850-9-x) are defined.

Since we are looking into the requirements of IEC 61850 for communication protocols, the different data models that are used to support different functions are outside the scope of this chapter. They can be found in details in the IEC 61850-7-x parts. In this chapter we will be focusing on the communication performance requirements as well as the specific IEC 61850 service mappings on different protocols.

Also in this chapter, we will discuss several challenges of supporting smart metering communication with the integration of IEC 61850 and LTE.

3.1 IEC 61850 performance requirements

3.1.1 IEC 61850 logical interfaces

In order to specify the requirements for the communication of smart metering in distribution network, we first have to define different scopes of the systems (within substation, between substations and between substation and control centre) as they have different requirements for the communication network. Figure 3.1 illustrates the interfaces belonging to different levels [15]:

- IF1: protection-data exchange between bay and station level.
- IF2: protection-data exchange between bay level and remote protection
- IF3: data exchange within bay level.

- IF4: CT and VT instantaneous data exchange (especially samples) between process and bay level.
- IF5: control-data exchange between process and bay level.
- IF6: control-data exchange between bay and station level.
- IF7: data exchange between substation (level) and a remote engineer's workplace.
- IF8: direct data exchange between the bays especially for fast functions such as interlocking.
- IF9: data exchange within station level.
- IF10: remote control-data exchange between substation (devices) and a remote network control centre.
- IF11: the control-data exchange between different substations

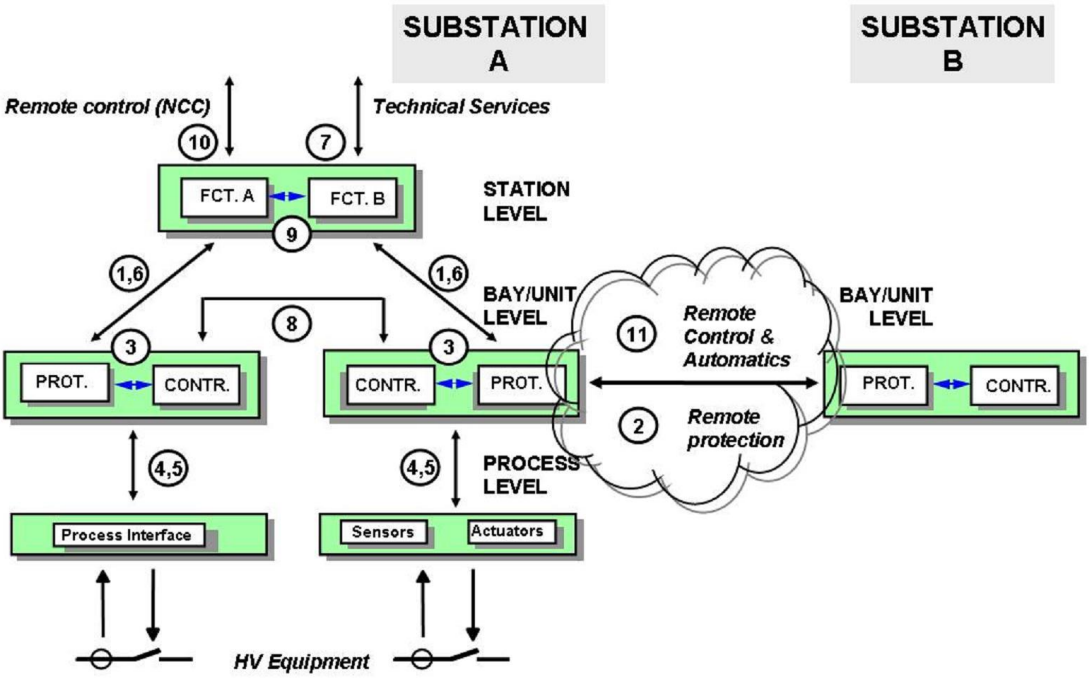


Figure 3.1 - IEC 61850 logical interfaces, copied from [16]

These logical interfaces have different requirements because of the different scope within the system. Several classes with different transfer time requirements are defined in section 3.1.2, and they will be applied on these logical interfaces.

Among all the interfaces mentioned, only IF10 is applicable to the interface between the smart meters to the meter data centre over a WAN connection in distribution electricity network. Therefore, in the next sections, even though we will look at the requirements for different kinds of message exchanged through all of these interfaces, for the purpose of investigating communication between smart meters and control centre we will focus on the requirements that are related to IF10.

3.1.2 Message performance requirements

The transfer time is specified as complete transmission time of a message including the handling at both ends (sender and receiver) [20]. The transfer time requirements are given by the needs of the application functions, and are shown in Table 3.1.

Table 3.1 - Classes for transfer times

Transfer time class	Transfer time [ms]	Application examples: Transfer of
TT0	>1 000	Files, events, log contents
TT1	1 000	Events, alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases, status changes
TT6	3	Trips, blockings

As the performance requirements depends on the specific applications, IEC 61850 defines 7 different message types, each has specific requirements for transfer time, and is mapped to a specific transfer time class specified in Table 3.1:

- *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.

The details on the performance requirements for other IEC 61850 message types can be found in the Appendix B. It can be concluded from the requirements of different message types that the communication between substation and the control centre (IF10) is considered as non time-critical and can be supported by message types 3, 5 and 6.

This is also applicable to the communication between smart meters and the control centre if IEC 61850 is extended to cover this area. These message types have similar performance requirements which are shown in Table 3.2.

Table 3.2 - Performance requirements for message type 3

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P5	The total transmission time shall be half the operator response time of = 1 s regarding event and response (bidirectional)	**TT2**	≤500	1, 3, 4, 5, 6, 7, 8, 9, 10
P6	The total transmission time shall be in line with the operator response time of =1 s regarding unidirectional event	**TT1**	≤1000	1, 3, 4, 5, 6, 7, 8, 9, 10

These message types that can be used to support control services through interface IF10 between control centre and substation are mapped to the Manufacturing Message Specification (MMS) protocol. Therefore, it is important to see whether the integration of MMS and LTE is capable of meeting this performance requirement of IEC 61850.

3.2 Functional requirements of the AMI components

The requirements for the components of the system are formulated based on the specific goal of supporting real-time smart metering communication with the IEC 61850 MMS protocol and LTE cellular network.

3.2.1 Smart meters

The smart meters are the end point in an AMI network. The smart meter must have the energy measurement functions and will be polled by the utilities to get the meter value. Therefore, a communication module is needed for the smart meter to connect to the utilities meter data management system.

3.2.2 Meter data aggregator/concentrator

In some designs of AMI network, a number of smart meters can be aggregated by a device called data aggregator/concentrator. For example, this approach is common for the design with PLC smart meters, as one limitation of PLC is that it requires hopping/relaying of the PLC signal around transformers; otherwise the signal is scrambled by this element in the grid [11]. Therefore, the data concentrator has to support communication with the connected smart meters, and must have LTE communication module to connect to the LTE network.

3.2.3 LTE network

One essential component in the proposed AMI approach is the LTE network. In addition to the existing non-energy-related traffic, such as voice, video, FTP, etc., the LTE network has to support the transport of the smart metering traffic between the smart meters and MDMS.

3.2.4 MDMS

In order to communicate with the smart meter, the host in the MDMS must have the connection to the LTE network. The MDMS has to be able to connect to the smart meters and retrieve the meter data from the smart meters. As real-time meter data collection is assumed, the MDMS host has to support fast polling of the smart meters and poll many smart meters at the same time.

3.3 Challenges

The integration of IEC 61850 MMS and LTE contributes many advantages to the AMI Communication Network solution. However, there are challenge questions in planning, designing and deploying this AMI solution, from the perspectives of both power utilities and mobile operators.

3.3.1 Scalability

It is expected that over 200 million smart meters will be deployed in Europe between 2011 and 2020 [32], which will have a massive demand for the network. The large number of smart meters also affects the performance of the systems. In theory, LTE is capable of meeting the performance requirements of IEC 61850 for metering services, but we do not know how the performance is affected by a large number of end devices like the case of smart meters.

In this research, we will investigate the number of smart meters that can be supported in a number of experiment sets in different network situations and how the performance varies in these network scenarios.

3.3.2 Latency

It is preferable to collect meter data in real-time, because utilities can correctly predict the load profile, perform load forecasting, dynamic balancing between generation and consumption, support real-time pricing and demand response, etc. In general, with the meter data collected in real-time, the stability and intelligence of the grid are greatly improved. The challenge is whether this solution can meet the performance requirements imposed by the real-time smart meter collection application, given a huge number of meters to be served in a large area.

In this research, we assume a public, shared LTE network; therefore, the amount of background traffic has a big impact on the latency of the smart metering traffic. Experiments will be conducted with the increase in number smart meters and LTE background nodes to verify if the latency requirement is satisfied.

3.3.3 Quality of service (QoS)

Since a shared, public LTE network is considered, another important aspect to look at is the mutual impacts of smart meter traffic and other traffic. It is important to maintain QoS in smart metering systems where data has to be made accessible for authorized entities in a timely manner. This is of great importance if smart meter data is sent on the same network with other crucial data for the operation of the grid, such as load control or distributed generation commands. Considering IEC 61850 is used for both smart meters and other applications such as distributed automations, the data for these

different applications must be classified based on their priority and the access control mechanisms of the cellular network has to support the differentiation of application data.

3.3.4 Security

As an smart metering system makes possible a two-way communication between smart meters and utility's centre system, a number of security concerns have been raised.

Customers do not want the information about their energy usage to be exposed to unauthorized parties. Therefore, this information must be kept confidential. If the AMI has an interface with HAN, the customers want to have the control over which information they share, e.g. whether it is permissible for the utility to control the appliances.

In addition, the AMI has to ensure that the smart meters data is kept intact on transmission and to prevent the unauthorized commands from being transmitted through AMI to smart meters. This requirement is more important if a wireless network is in use, where data may float over the air and is easily accessible.

Security is a crucial challenge, especially in the public LTE network. Security mechanisms such as encryptions and authentications should be taken into consideration. However, when these security mechanisms are in use, it is important to consider their impact on the performance of the smart metering traffic since the overhead (packet size/ computation time) is increased which may affect the end-to-end delay of the traffic.

In the later chapters of the report, the challenges of scalability and real-time latency requirements of the smart metering will be investigated, while the quality of service and security are not yet considered and will be left open for future research.

Chapter 4

Specifications and design of the solution

In this chapter, the overall architecture of the proposed solution is discussed. After that, specifications of the integration of IEC 61850 MMS and LTE to support smart metering communication will be presented in section 4.1. The design for the models of the solution can be found in section 4.2, and the system composition of the designed components is included in section 4.3. The answer to research question 2 is partially given in this chapter.

The overall architecture of the solution is described. Based on this architecture, we will look at the technical specifications and design of the components that are used in the proposed solution. The solution of using LTE and IEC 61850 MMS protocol for smart metering within distribution network is depicted in Figure 4.1.

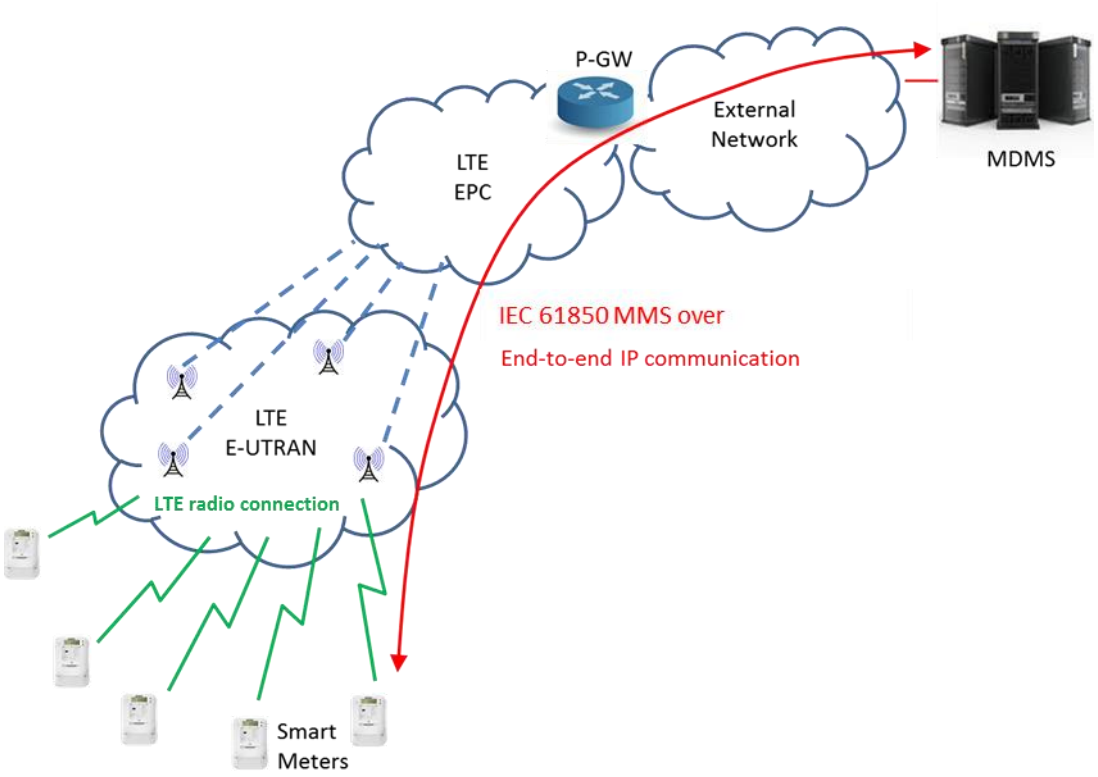


Figure 4.1 - Smart metering system using IEC 61850 MMS and LTE

It should be noted that the LTE MTC architecture described in section 2.4.8 is not used in the proposed solution. The reason for this is the MTC architecture requires some additional components and changes in the LTE architecture that are often not available for the majority of mobile network operators. Moreover, we look forward to a solution that can be used to compare with the AMI based on CDMA450 [21] of Alliander, a large energy distribution network operator in the Netherlands. To the best of our knowledge, CDMA450 technology does not support MTC. Lastly, the MTC solution is not available in any of the simulators that we can find, and it is not possible for us to implement MTC in time for the experiment phase. Therefore, we have decided to use the LTE architecture without MTC.

It is shown in Figure 4.1 that the AMI system has several components that are interconnected to each other: smart meters, meter data concentrator/aggregator, LTE network, and the meter data management system (MDMS). A more detailed description of these components can be found in section 4.2 and section 4.3.

Each smart meter/data concentrator has a LTE communication module which allows it to connect to LTE network. The geographical area is divided into cells, each under control of one eNodeB which provides radio communication resources to the smart meters/data concentrator. IEC 61850 application protocol can be used between the smart meter and the MDMS on top of TCP/IP to support MMS client/server communication model.

4.1 Technical specifications

In this section, based on the requirements that have been discussed in chapter 3, the technical specifications for different components in the proposed AMI architecture are specified, which provide inputs for the design and implementation phases. This is also an important step in order to implement the required models (see chapter 5) for the performance evaluation of the solution which will be given in chapter 6.

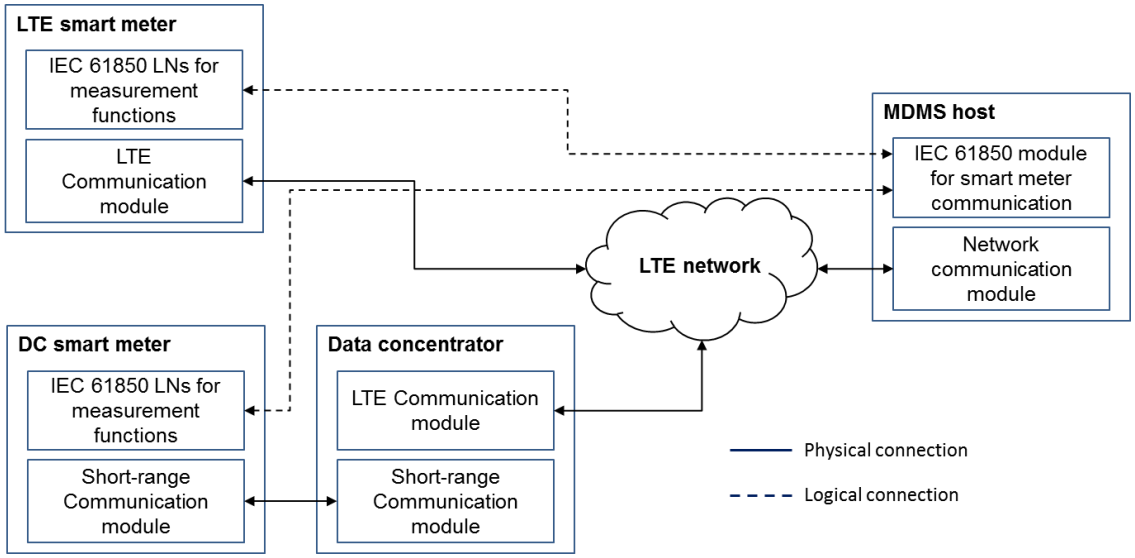


Figure 4.2 - Specification of the solution

The AMI components that are used for the smart metering solution and how they are interconnected are depicted in Figure 4.2. The specifications are derived from the functional requirements in section 3.2.

4.1.1 Smart meters specifications

The smart meter must support IEC 61850 MMS protocol to communicate with the remote host situated in the MDMS at the utilities premises, which also runs IEC 61850. Using the IEC 61850 MMS protocol stack, the smart meter must support:

- The response message to establish COTP connection with the client.
- The response message to establish MMS Application Association with the MMS client after the client has sent an association request.
- The MMS (read/write) service response message to reply to the MMS client's request with the meter data value.

If the smart meters are stand-alone (not placed behind data concentrator), the smart meters must have LTE communication module to connect directly to the LTE network.

If the smart meter is placed behind the data concentrator, a short-range communication module (e.g. WiFi, ZigBee, PLC, etc.) has to be present in the smart meter to allow it to connect to the data concentrator.

These specifications are based on the requirements specified in section 3.2.1.

4.1.2 Meter data concentrator

Based on the requirements in section 3.2.2, for the specifications of the meter data concentrator in our system, we assume a data concentrator connects to a number of smart meter using some short-range protocols and the traffic from these smart meters are relayed by the data concentrator to the MDMS. Therefore, the data concentrator has to support communication with the connected smart meters, and must have LTE communication module to connect to the LTE network.

In reality, the data concentrator has the aggregation function of the collected smart meter data. It communicates with the short-range smart meter through protocols like ZigBee, PLC and stores the meter data. It also communicates with the MDMS via a longer range communication technology (such as WiMAX, cellular, etc.) to transfer the meter data. However, in our design, this aggregator function is not specified and designed. We assume that a data concentrator is an UE within the LTE network that has routing capability and only relays traffic from the locally connected interface to the LTE network and vice versa.

4.1.3 LTE network

The specifications to the LTE network are discussed in section 2.4, and it meets the requirements presented in section 3.2.3. The LTE E-UTRAN has to support the radio connection to the LTE smart meter and Data concentrator. The LTE EPC is connected to the MDMS host to allow end-to-end connection between the smart meters and the MDMS host.

The brief description of LTE network infrastructure has been provided in chapter 2. In chapter 5, the detailed description of the LTE network infrastructure used for the simulation experiment will be discussed.

4.1.4 MDMS host

Section 3.2.4 discusses the requirements for the MDMS host and it derives the specifications for the MDMS host in this section.

The MDMS has the IEC 61850 MMS communication stack to communicate with the smart meter. As the MMS client, the MDMS host has to support:

- The request message to establish COTP connection with the MMS server
- The request message to establish MMS Application Association with the MMS server after the COTP connection has been established.
- The MMS (read/write) service request message to poll the smart meter (MMS server) in order to retrieve the meter data value.
- As real-time meter data collection is assumed, the MDMS host has to support fast polling of the smart meters and poll many smart meters at the same time.

In order to communicate with the smart meter, the host in the MDMS must have the connection to the LTE network (through the network communication module to connect to the P-GW), which will route the traffic between the smart meters and the MDMS host.

4.2 Design of the solution

In this section, the design of the components that are used in the solution is presented. The design is derived from technical specifications in section 4.1.

4.2.1 Design of the IEC 61850 MMS model

The MMS traffic model is designed and implemented based on the technical specifications of the IEC 61850 MMS specifications for the smart meters (see section 4.1.1) and the MDMS host (see section 4.1.2).

Specifically, based on the specifications, the OSI layers 4-7 of the MMS traffic model will be implemented on top of the existing TCP/IP stack:

- *Application layer:* the Application Association Request (AARQ) and Application Association Response (AARE)
- *Presentation:* the ASN.1 notation and BER
- *Session:* Connection Oriented Transport Protocol (COTP) with Connection Request (CR), Connection Confirm (CC), and Data (DT) TPDUs on top of RFC 1006 Transport Packet (TPKT)
- *Transport layer:* TCP, on top of standard IP stack.

IEC 61850 MMS has been briefly discussed in chapter 1 and 2. In this section, 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 [63].

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 [63].

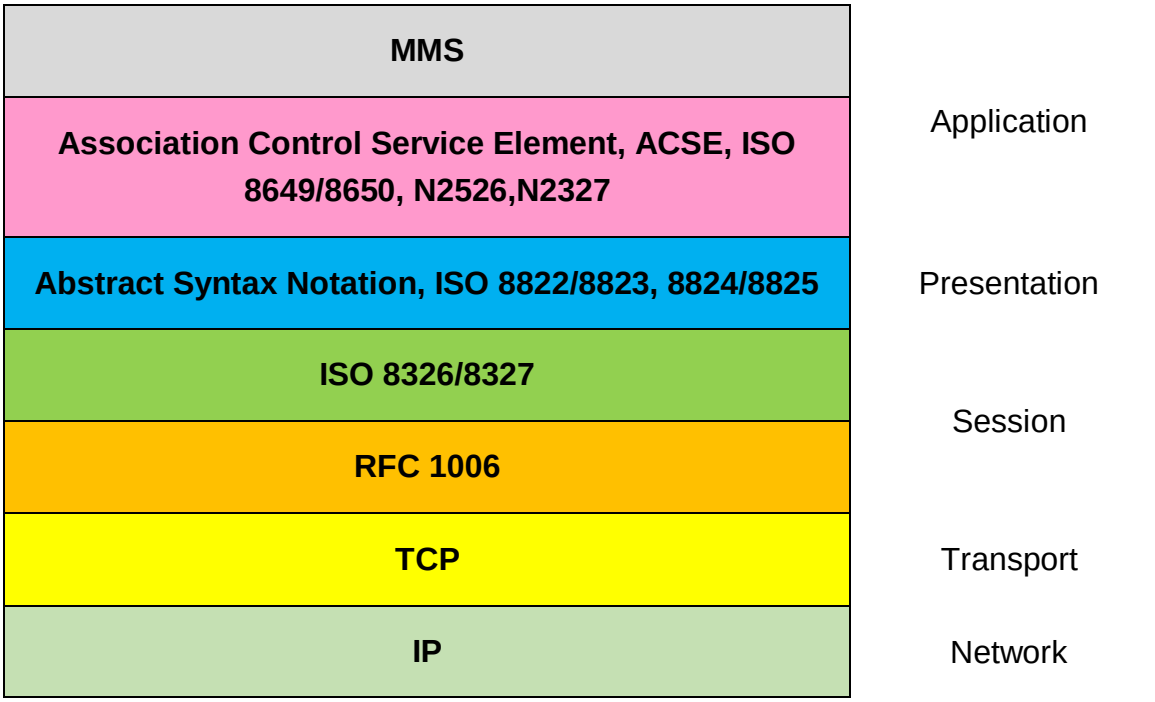


Figure 4.3 - Layer 3-7 of the current MMS communication stack, based on [63][65]

Figure 4.3 depicts layers 3 to 7 of the current MMS stack according to [63], [65].

4.2.1.1 Application layer

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.

4.2.1.2 Presentation layer: ASN.1 and BER

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. 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 [64].

The Basic Encoding Rules (BER) is one of the original sets of encoding rules specified by the ASN.1 standard. BER is an 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 [64].

4.2.1.3 Session layer

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.

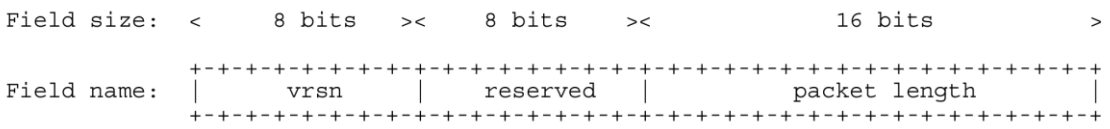


Figure 4.4 - TPTK header format, copied from [64]

The format of the TPTK header is depicted in Figure 4.4. 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 4.5.

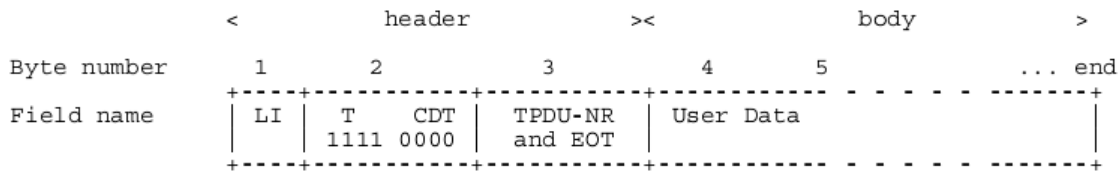


Figure 4.5 - COTP PDU format

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.

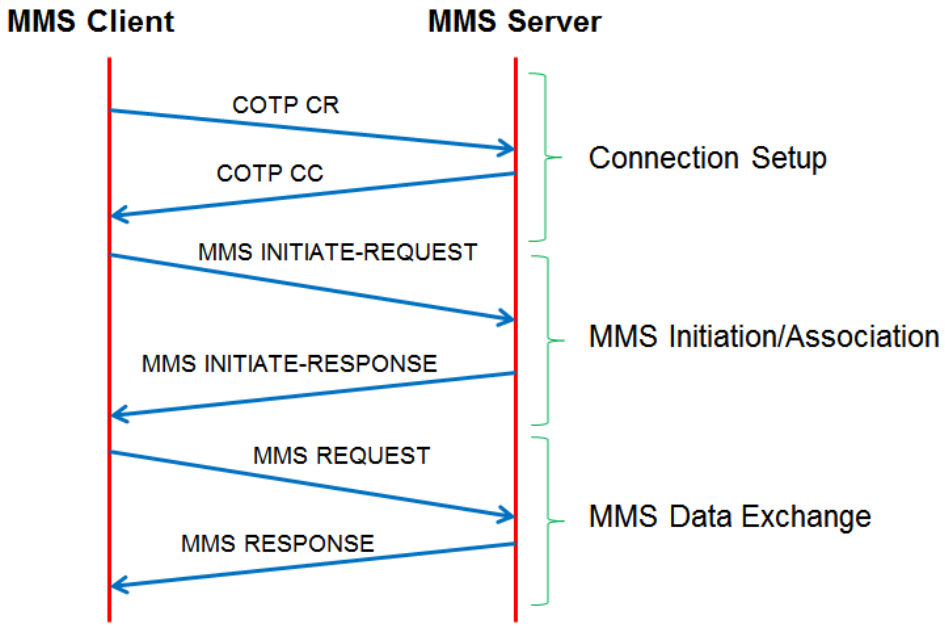


Figure 4.6 - MMS message flow in different phases between MMS client and MMS server

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 Smart meter model

There are currently no standardized IEC 61850 models for smart meters. The scope of IEC 61850 has been made broader, but not yet covered this endpoint in AMI. Based on IEC 61850-7-4, we assume that the smart meter is an IED that has a specific measurement function represented by IEC 61850 logical node MMXN (Non phase related Measurement). This LN shall be used for calculation of currents, voltages, powers and impedances in a single-phase system. The main use is for operative applications. The data objects contained in this Logical node is depicted in Table 4.1.

The smart meter will have the MMS protocol stack (see section 4.2.1) and acts as a MMS server to receive the polling request and respond with meter data value.

Based on the specifications in section 4.1.1, in addition to the IEC 61850 module, the smart meter is designed with a communication module that allows it to connect to the LTE network (in the LTE smart meter case) or the data concentrator (in case the smart meter is placed behind a data concentrator). The implementation of this communication protocol is up to the simulation environment whether the type of communication is supported.

Table 4.1 - MMXN Logical Node

MMXN class				
Data Object Name	**Common Data Class**	**Explanation**	**T**	**M/O/C**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2 clause 19		
Data Objects				
Measured Values				
Amp	MV	Current I not allocated to a phase		O
Vol	MV	Voltage V not allocated to a phase		O
Watt	MV	Power (P) not allocated to a phase		O
VolAmpr	MV	Reactive Power (Q) not allocated to a phase		O
VolAmp	MV	Apparent Power (S) not allocated to a phase		O
PwrFact	MV	Power Factor not allocated to a phase		O
Imp	CMV	Impedance		O
Hz	MV	Frequency		O

4.2.3 Data concentrator model

Based on the specifications given in section 4.1.2, the data concentrator is designed to have two communication modules. The first one is the short-range communication module to allow the data concentrator to connect to the local smart meters. The second one is the LTE communication module, which allows the data concentrator to connect to the LTE network. The data concentrator can be viewed as a relay node (router) between the short-range communication network and LTE network.

4.2.4 MDMS host

The protocol stack that is designed in section 4.2.1 will be used for the MDMS host model, where the MDMS acts as a MMS client that will initiate a connection, setup the Application Association, and do periodic polling of the smart meters.

The specifications of the MDMS in section 4.1.2 also require the connection from the MDMS host to the LTE network (through the network communication module to connect to the P-GW) as the MDMS host is situated in the utilities' data centre which is modelled as an external network connected to the LTE EPC. Therefore, in addition to the IEC 61850 module, the MDMS host has a network communication module to connect to the P-GW of the LTE EPC network

Chapter 5

Implementation using NS3 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 all the modules described in this section can be found in [79], and the guideline to use the modules is included in the Appendix.

5.1 Choice of the NS3 LENA simulation environment

In order to use to most appropriate simulation environment for the implementation of the solution, we have investigated some of the most popular simulators, such as NS2 [38], OMNeT++ [45], OPNET [47], and NS3 [53].

NS2 [38] is an open-source discrete event simulator which provides support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. It is one the most popular network simulators used by researchers. However, LTE is not supported in NS2, and there have been no IEC 61850 models developed in NS2.

OMNeT++ [45] is a open source, discrete event simulator tool written in C++. OMNET++ is a general-purpose simulator capable of simulating any system composed of devices interacting with each other. OMNeT++ supports wireless and mobile simulations within OMNeT++. OMNet++ is for academic and educational use. OMNeT++ is a feature-rich and powerful simulation tool. An IEC 61850 model is available in OMNeT++, which is described in [46]. The authors presented the integration of IEC 61850 communication stack into OMNeT++ that allows the sending of GOOSE, SV and MMS. Unfortunately, like NS2, LTE is not supported in OMNeT++.

OPNET [47] offer a large number of different tools supporting modelling and simulation of networks in various technologies. IEC 61850 models are not included in OPNET. Several research investigations, such as [49], [50], [51], [52], looked into the simulation modelling of IEC 61850 communication services in OPNET to model the substation communication network and analyse the network's dynamic performance (i.e., packet delay characteristics of time-critical services). The authors mostly focus on the modelling of the GOOSE and SV within substation communication network. For MMS client/server model, the authors of [49] use the standard TCP/IP stack in OPNET to evaluate the performance of metered/measured value communication. However, the models developed by the authors are not made available for public use. Also, OPNET is a commercial simulator. An academic version is available with limited features, however we did not have sufficient time to obtain the license and study the simulation environment.

The choice of using NS3 LENA is made, because it is the only open-source packet-level simulator in our investigation that supports LTE (Release 8). Regarding the IEC 61850 models for ns-3, [55] presents a traffic generation of IEC 61850 SV. Based on the structure of the SV in the standard, the authors developed a model of the SV traffic generator, captured the packet traces and saved in PCAP file for verification using Wireshark network protocol analyser [56]. Even though IEC 61850 MMS is not available in NS3 LENA, we can use the existing communication stack to develop our own models.

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 to 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 ore 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, which will be described in section 5.2.1 and 5.2.2 respectively.

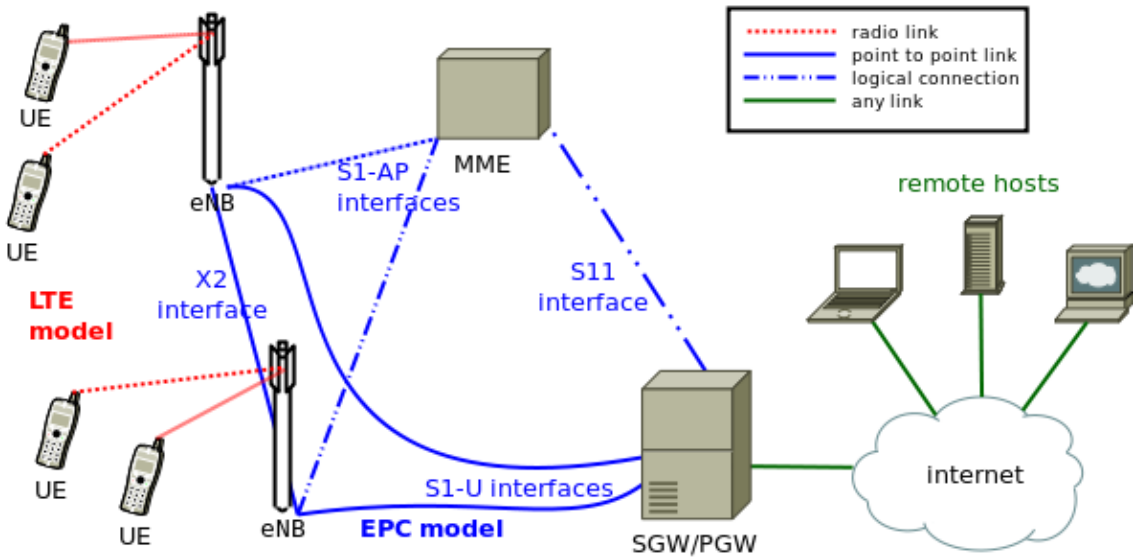


Figure 5.1 - LTE-EPC simulation model overall architecture, copied from [54]

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 [69]:

- 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 [69]:

- 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.

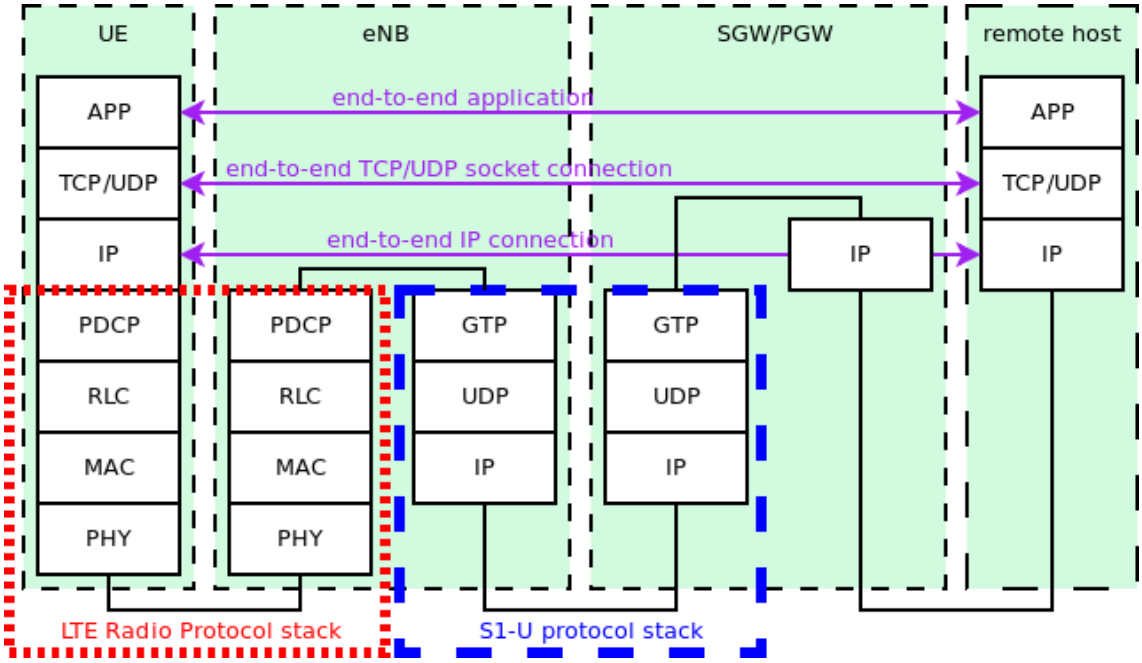


Figure 5.2 - LTE-EPC data plane protocol stack, copied from [69]

5.2.3 MAC

5.2.3.1 Round Robin Scheduler

The Round Robin (RR) scheduling is a non-aware scheduling scheme that allocates the shared resources (time/RBs) for the users in a cyclic manner, without taking the instantaneous channel conditions into account. Therefore, it offers great fairness among the users in radio resource assignment, but may negatively affect the performance [69].

The RR scheduler is the simplest scheduler: it simply divides available resources among the active flows, i.e. those logical channels which a have a non-empty RLC queue; if the number of available RBGs is greater than or equal to the number of active flows, then all flows can be allocated in the same subframe; otherwise not every flow can be scheduled in the given subframe, and then allocation decisions for next subframe will have to start from the last flow that was not served in the previous TTI [69].

The principal advantage of Round Robin scheduling is the guaranty of fairness for all users. Furthermore Round Robin is easy to implemented, that is the reason why it is usually used by many systems. Since Round Robin ignores the channel quality information, it usually results in lower user and overall network throughput levels.

In this research, we use the existing RR implementation of LENA for the performance evaluation in chapter 6.

5.2.3.2 Resource Allocation Model

In LTE, scheduler is in charge of creating (Downlink Control Indicator) DCIs, specific data structures used to inform attached UEs about eNB resource allocation. These messages are sent from eNB's PHY every subframe, and for the downlink direction contain, among the others, information about the Modulation and Coding Scheme (MCS) that will be used, the MAC TB size, the allocation bitmap describing in which RB a given UE will receive data transmitted for him.

Each RB is assigned to the same user in downlink direction for a given subframe. Allocation bitmap is coded using Allocation Type 0 (see [25]), grouping RBs in RBGs of different sizes according to a function of the transmission bandwidth configuration in use. There are cases in which the number of available RBs (e.g. 25 in 5 MHz bandwidth configurations) is not dividable by group size (e.g. 2), hence not all RBs are usable.

Uplink DCI format is slightly different, since only adjacent RBs can be used because of SC-FDMA modulation, thus all RBs can be allocated regardless to the bandwidth configuration.

5.2.4 PHY

The DCI messages discussed in section 5.2.3.2 are carried in the Physical Downlink Control Channel (PDCCH), which occupies up to three OFDM symbols (or four if the system bandwidth is 1.4 MHz) at the start of the subframe [24].

Given that PDCCH can only occupy up to three or four OFDM symbols in a subframe, a limited number of DCI messages can be transmitted per subframe, which may become a bottleneck, especially in the case improved spectral efficiency of the data channels may need to be supported by higher capacity on the control channels, or frequent transmissions of small amounts of data causing higher loading on the control channels than applications with large data packets, for which LTE was primarily designed to support. If the PDCCH is full, the eNB cannot send any more data until the next TTI, even if there are enough PRBs to hold the data. Similarly, the eNB itself may be limited by how many scheduling decisions it can make in a TTI before it has to send what it has and move on to the next TTI.

This signalling overload challenge has been studied in [23], and the several enhancements have been proposed in the LTE MTC architecture in [33] and the Enhanced PDCCH [24].

In LENA, the transmission of the control frame of a fixed duration of 3/14 of milliseconds spanning in the whole available bandwidth, since the scheduler does not estimate the size of the control region. Therefore, the maximum users that can be supported in LENA is limited, by both the PRB and TTI limits (the PDSCH channel), and the PDCCH and scheduling limits.

The LENA implementation of the CQI generation follows guidelines specified by FemtoForum and includes periodic wideband CQIs (one single values summarizing the whole channel per-ceived by the UE) and inband CQIs as well (a set of values, one for each RB in use, representing a way more detailed view of the channel from the UE standing point). PHY interference model is based on famous and well-known Gaussian model in which power of interfering signals (in linear units) are summed up to deter-mine the overall interference power

The readers are advised to refer to the Design Documentation of LENA [69] for more details about the design criteria and implementation of the LTE and EPC models in LENA.

5.3 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 5.3.

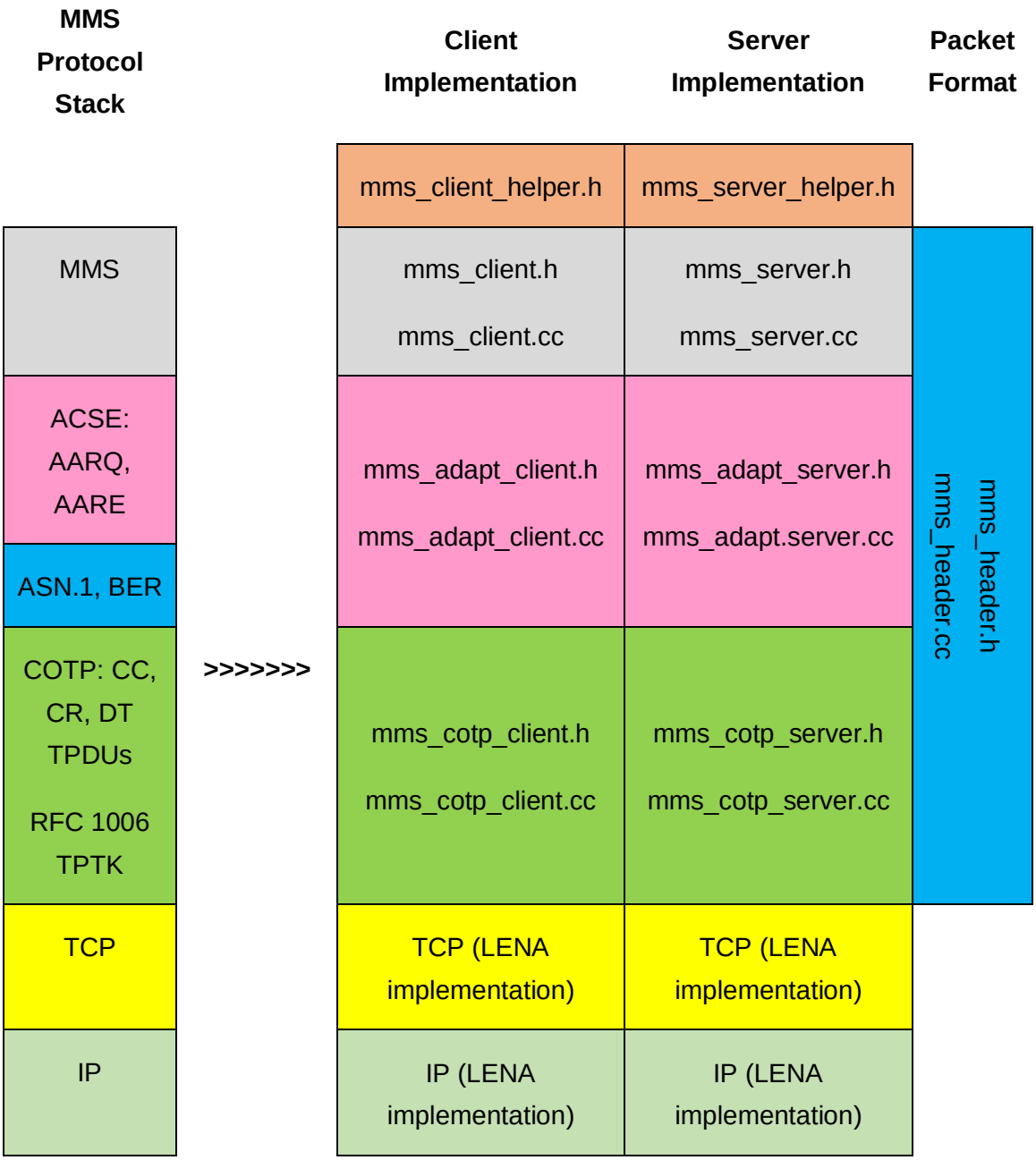


Figure 5.3 - Implementation of the MMS protocol stack for MMS client and MMS server

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 4.6. There are a number of modules that have been developed for each of these two applications.

The set of modules on the client side is implemented based on the design given in section 4.2.1 and 4.2.4 (MDMS host). On the server side, the implementation of the modules is based on the design presented in section 4.2.1 and 4.2.2 (smart meter model).

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.3.4 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.

5.3.5 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).

5.3.6 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.

5.3.7 mms_header module

The packet format for different layers is implemented in a single, common `mms_header` module based on the design in section 4.2.1. 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.

5.3.8 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.

5.3.9 Module output

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.

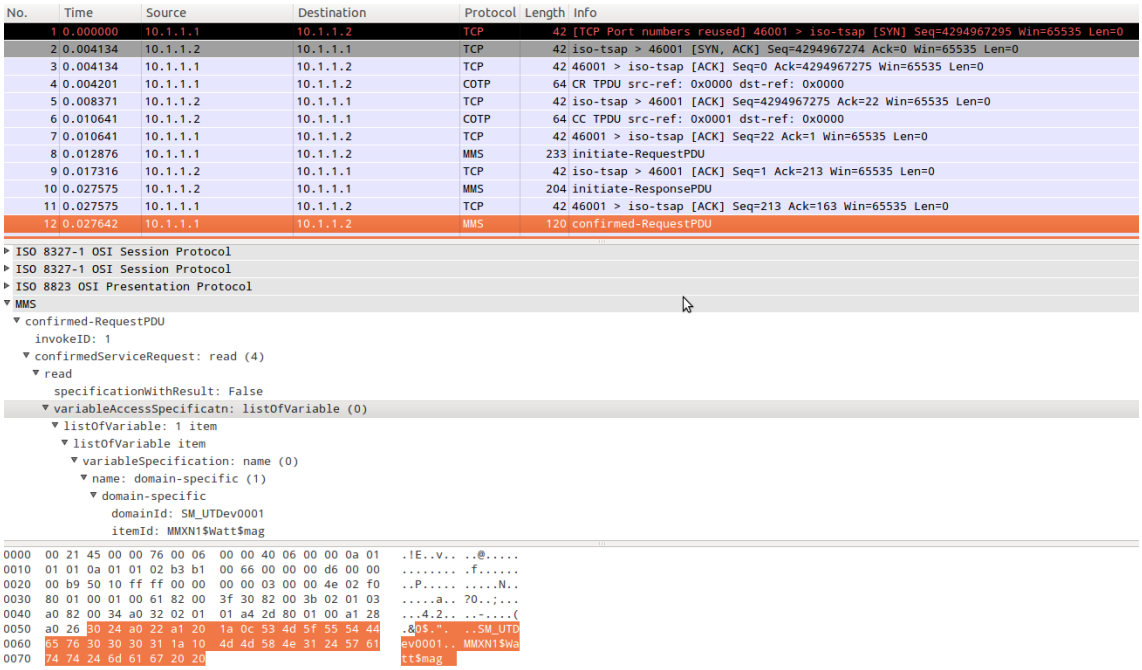


Figure 5.4 - PCAP trace output of the MMS traffic model in LENA

5.4 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 [67], [68] which are given in Table 4.2. The details about the traffic model parameters and their related statistical characteristics are listed in Appendix of this report.

Table 4.2 - 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%

5.4.1 Description of the traffic models

5.4.1.1 Voice-over-IP (VoIP) traffic model

A simple two-state voice activity model is considered, see Figure 5.5. 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).

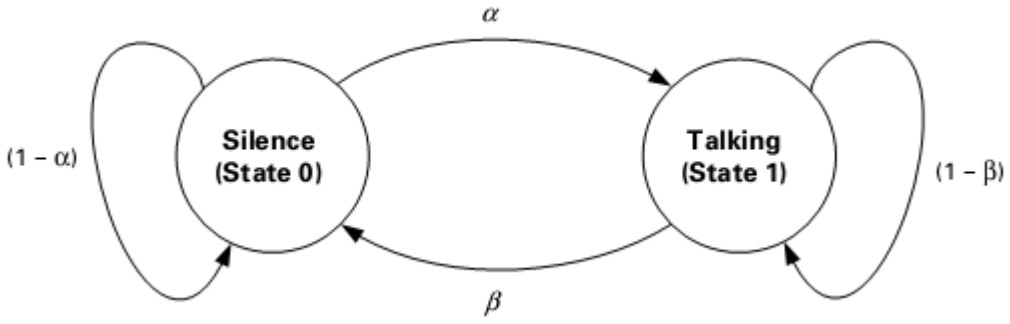


Figure 5.5 - Two-state voice activity model, copied from [68]

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.

5.4.1.2 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.

5.4.1.3 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].

5.4.1.4 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 [68].

5.4.1.5 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 [68].

The design of LTE background traffic follows the same approach, in which the traffic generator is placed on top of the existing TCP/UDP over IP stack. The characteristics of the LTE background traffic has to follow the specified statistical distribution.

5.4.2 Implementation of the LTE background traffic

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 [70], 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.

5.5 Smart meters, data concentrators and MDMS hosts

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 smart meter is implemented as a node 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 use of the helper modules make it easy to define different layers of the communication stack installed on a node (see Figure 5.6)

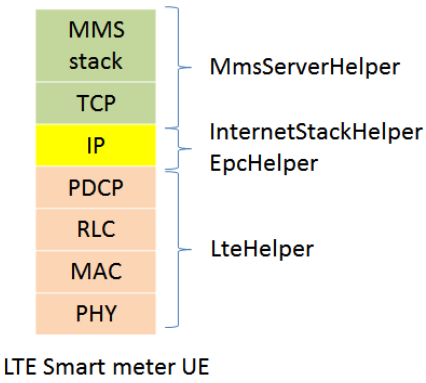


Figure 5.6 - Implementation of the LTE smart meter

A smart meter that works behind a data concentrator has similar implementation, but without LTE stack (see Figure 5.7). Instead, we create a point-to-point link between the smart meter and a data concentrator using `PointToPointHelper`. The LTE stack is installed on the data concentrator that allows it to connect to the LTE network to relay (route) the traffic of the smart meters from the point-to-point link to the MDMS host. As routing capability has to be implemented for the relaying to work, we use static routing with `Ipv4StaticRoutingHelper` module.

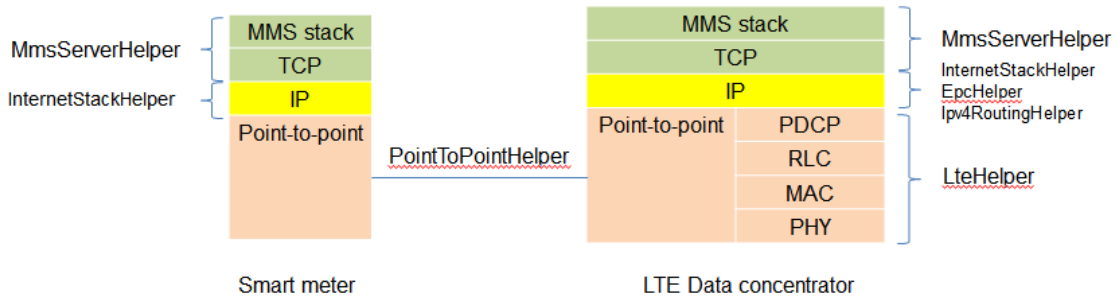


Figure 5.7 - Implementation of the local smart meter and LTE data concentrator

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

5.6 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

The answer to question 3 is given in this chapter. The solution of the integration between IEC 61850 and LTE to support smart metering will be evaluated to determine its performance under a mixed traffic network environments. The chapter consists of the following:

Section 6.1 describes the experiments that are used for the performance evaluation of the solution. In Section 6.2 provides the data collection and results after the experiments are run. Finally some analysis about the experiment results is provided in section 6.3.

6.1. Description of the experiment scenarios

This section provides some description of the experiments scenarios to be conducted for the evaluation of the proposed solution, including the simulation topology, simulation parameters, different performance metrics and the simulation scenarios.

6.1.1 Simulation topology

In the experiments we are going to investigate the performance of the IEC 61850 MMS and LTE solution and the impacts of the smart meter traffic on the existing LTE traffic and vice versa. In order to achieve this goal, we use a single cell topology as shown in Figure 6.1. In the real world, the locations of the smart meters are fixed; hence we are dealing with fixed wireless communication and will not consider handovers between different eNodeBs in this case.

The LTE UEs, including the LTE smart meters (SM), LTE data concentrator (DC) and LTE background users, are uniformly distributed around the eNodeB in a disc with radius R. We assume 20% of the total smart meters are LTE smart meters, while the rest (80%) are placed behind data concentrators with up to 100 smart meters per DC. These are realistic numbers based on the AMI implementation of Alliander.

The implemented modules on the server side (see Figure 5.3) are installed on the smart meter nodes, while the modules on the client side are installed on the MDMS host which allows the smart meters communicate with the MDMS host situated at the utilities head-end. For the smart meter traffic, we assume the case of real time meter data collection, where the MDMS host polls each smart meter every second to get the measurement data objects in MMS MMXN logical node: Volt, Watt, Amp, Hz, Power factor, etc. (see Table 4.1).

The background traffic is also generated between the LTE users and the remote hosts for different types of traffic.

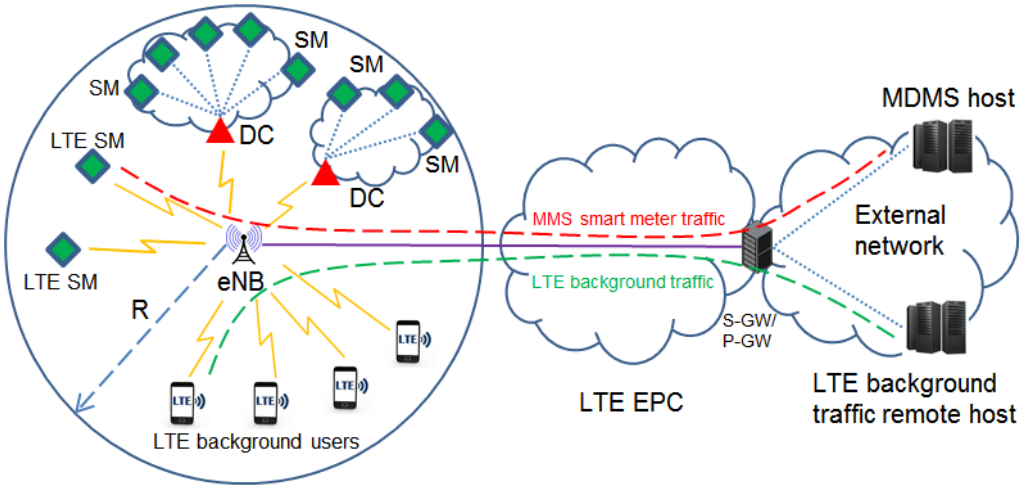


Figure 6.1 - Simulation topology

6.1.2 Simulation parameters

The simulation environment we use is NS3 LENA M5, which implements LTE release 8 features [69]. The main LTE eNodeB parameters in LENA are summarized in Table 6.1. The channel bandwidth 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, another goal of this research is to provide a reference for Alliander 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 antenna technology designed to enhance the data rate as well as the quality of LTE traffic.

The cell radius of 800m is chosen as the majority of smart meters are placed in the urban area.

Table 6.1 - Main LTE eNodeB parameters in LENA

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	800m (typical 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 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 eNB in the UL and received by the UE in the downlink over the simulation time.

6.1.3.2 Packet loss ratio

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

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

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

The number of packets is calculated below the TCP layer.

6.1.3.3 Delay

Delay is an important metric to consider in the experiments as it relates directly to the performance requirements specified in chapter 3. We will look at the average delay for the MMS smart meter traffic as well as for the time-critical background traffic such as voice/video/gaming.

- MMS smart meter traffic:
    - Initiation delay: time from the start of the connection setup until Initiate-Response is received at the client (at the MMS application layer)
    - Request delay: time from the start of the polling request until a response is received at the client (at the MMS application layer)
- Time-critical background traffic (voice/video/gaming):
    - One-way delay: time from the moment the packet is sent at one host until it is received at the other host (at the application layer).

6.1.3.4 Jitter

Jitter, or variation of the delay, is important because it has an impact on the buffering requirements for all downstream network and devices, and extreme jitter can lead to performance degradation because of buffer overflow or underflow. It is measured by the absolute difference of the delay (calculated in the between 2 successive received packets. In the simulation, we will look at the average jitter for the voice traffic.

6.1.4 Simulation scenarios

The number of LTE background traffic users and smart meters will be varied to define different scenarios. The implemented background traffic models in chapter 5 are used in this section following the traffic mix as in Table 4.2.

We define several simulation scenarios which are characterized by the different mix percentage of the background traffic and smart meter traffic: 80/20, 60/40, and the special case 0/100. These types of mix allow us to investigate the mutual impacts of smart meter traffic and background traffic in different network situations. The special case 0/100 refers to the private AMI network, where a dedicated LTE network is used for the smart metering communication.

As the number of LTE background user in the simulator has to be integers, the following steps are needed to generate the required traffic mix:

- *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 smart meters, run the simulation and store the throughput of the background traffic and smart meter traffic.
- *Step 3*: calculate the background traffic/smart meter percentage mix.
    - If the mix is less than the desired value, increase the number of smart meters and repeat step 2.
    - If the mix is more than the desired value, decrease the number of smart meters 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.

6.2 Experiment data collection and confidence interval

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

NS3 has several built-in traces that allow us to measure the performance metrics. Specifically, we use the DlPdcpTracer.txt file trace for the downlink. In the trace file, the number of packet sent by the eNodeB (TXPdus) and received by the UEs (RXPdus), the numbers of bytes sent by the eNodeB (TXBytes) and received by the UEs (RXBytes) are listed, which is enough to calculate traffic load and traffic throughput based on the equations given in section 6.1.3.

On the uplink, due to the bug of redundant PDU issue, we use the UlRlcTracer.txt instead, which also gives us the same parameters to calculate the traffic load and throughput.

To measure the delay of the MMS traffic and background traffic, in our implementation of the traffic models, we attach the timestamp and packet ID for each sent packet. Upon receiving the packet, the receiver deducts the timestamp value from the time the packet is received to calculate the one-way delay. The jitter for voice traffic is calculated based on the delay values of successive packets.

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 [70]. The confidence interval is defined as:

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

where $\bar{\gamma}$ 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.

6.3 Simulation results and analysis

This section presents the simulation results and analysis for the conducted experiments.

6.3.1 80/20 downlink traffic mix scenario

This traffic mix is a typical case since the traffic generated by a single smart meter node is very little. Additionally, the traffic generated by popular LTE applications such as video streaming, web browsing…etc. are much higher than the traffic from a single smart meter.

The simulation results for both downlink and uplink are collected and analysed to evaluate the impact of integrating smart metering traffic to an existing LTE network.

The measurements are performed by following the steps mentioned in section 6.1.4. We start from the lowest traffic load (10 background nodes and the corresponding number of smart meters that make up the desired 80/20 traffic mix). After that, we increase the load and go up to the point where the throughput starts decreasing when the load is further increased.

The number of background nodes and smart meters to meet the desired 80/20 percentage traffic mix is shown in Table 6.2.

Table 6.2 - Number of background nodes and smart meters in the 80/20 traffic mix

Number of background nodes	Number of smart meters	Total traffic load (kbps)
10	38	2169.325
20	76	4408.442
30	114	6316.864
40	152	8277.077
50	160	10188.463
60	220	12099.850

6.3.1.1 Throughput

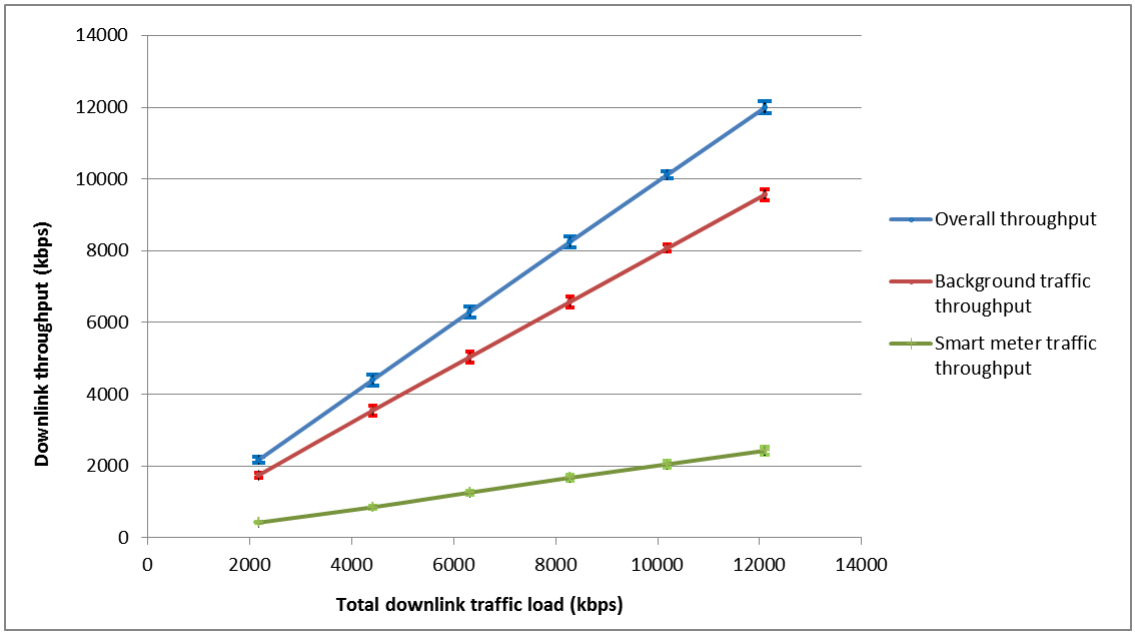
Figure 6.2 shows the overall throughput for both the downlink and uplink which consists of the smart meter traffic throughput and background throughput when the percentage of traffic load generated by the background applications is 80% and by smart metering application is 20%. As shown in all three lines of the graph, the throughput increases almost linearly when the traffic load increases and reaches the maximum capacity of around 12 Mbps. If we compare the value of the overall throughput and the corresponding traffic load, we can see that the two values are approximately equal. The reason for this is that when the traffic load is less than the network capacity, nearly 100 percentages of the generated messages will be disseminated successfully to the destination. Thus, the throughput keeps increasing when the more packets are added to the network.

Similarly to the downlink throughput performance, the uplink throughput increases when the total traffic loads increases. Since the traffic load did not exceed the network capacity, the traffic load and throughput are the nearly same indicating that almost packets were exchanged successfully.

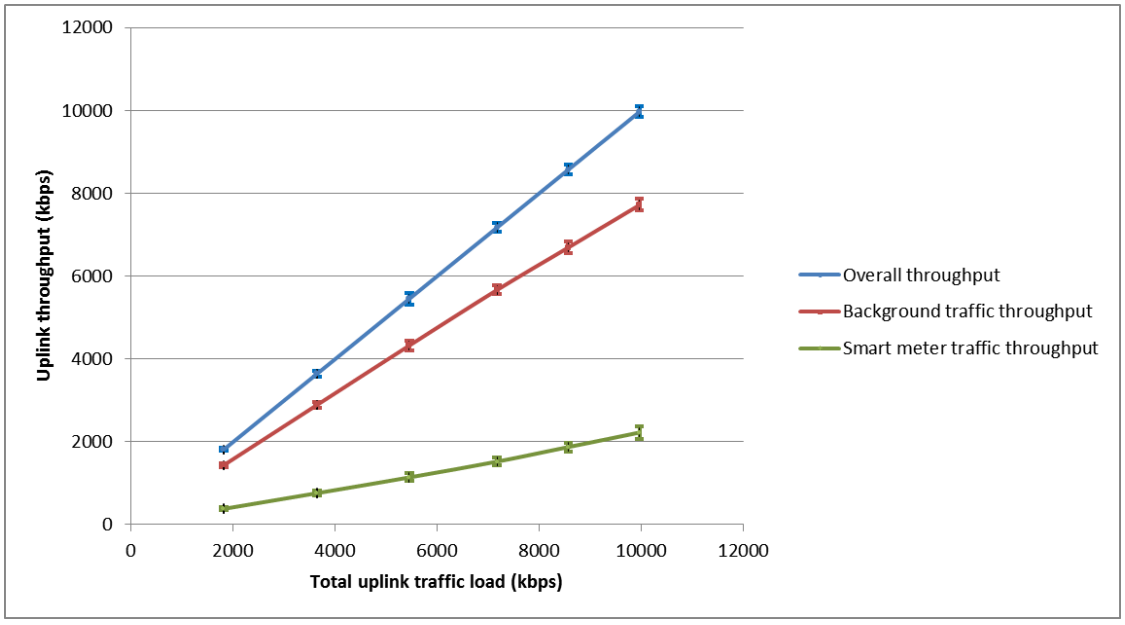
The throughput in uplink is lower than in downlink because the traffic generated by the background nodes in uplink is lower than in downlink (see chapter 5).

We also see that the traffic mix for the downlink and uplink are slightly different. This is due to different traffic characteristics generated in the downlink and uplink, such as packet size, packet arrival rate, etc. When the background applications/smart metering

traffic mix is fixed at 80%/20% in the downlink, the traffic mix is almost fixed at 79%/21%.



(a)



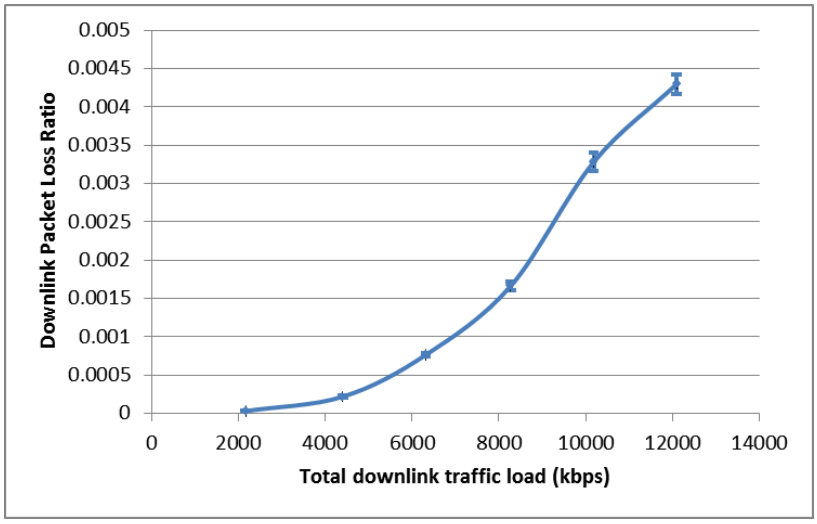
(b)

Figure 6.2 – Throughput performance in 80/20 traffic mix experiment for the downlink (a) and uplink (b)

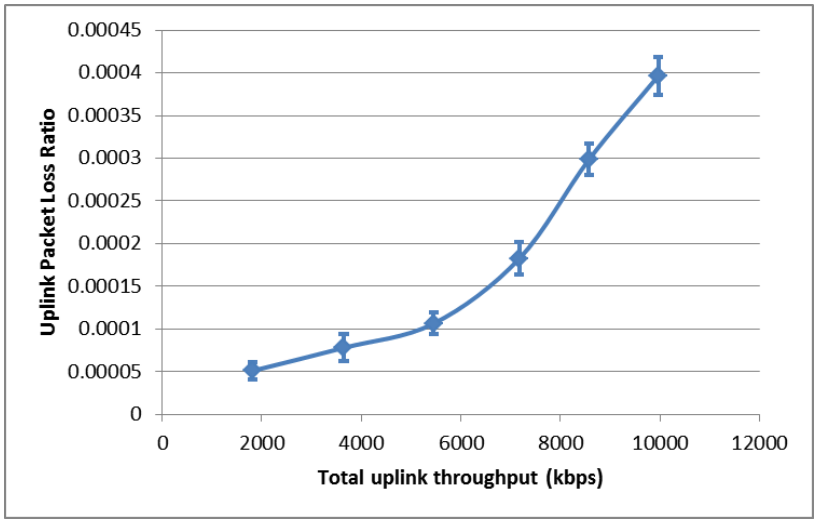
6.3.1.2 Packet loss ratio

Figure 6.3 shows the packet loss ratio when the traffic load does not exceed the maximum capacity of the network. Therefore, the packet loss ratio is quite low (10^{-5} ~ 10^{-4}) when the traffic load is less than half of the network capacity and is still acceptable when the traffic load approach the maximum capacity.

The packet loss ratio curve shows that more packets were lost when the traffic load increased since the more the traffic, the less the amount of network resources available for each node. Consequently, the packet loss ratio will increase.



(a)



(b)

Figure 6.3 – Downlink packet loss ratio in 80/20 traffic mix experiment for the downlink (a) and uplink (b)

6.3.1.3 MMS Delay

The delay performances of the smart meter initiation process and smart meter polling process are illustrated in Figure 6.4.

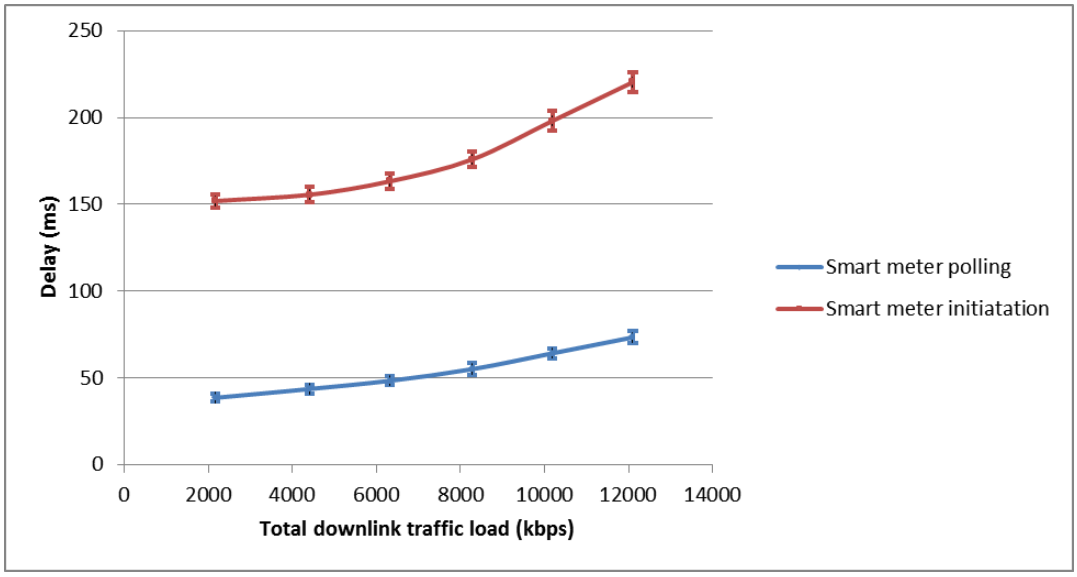


Figure 6.4 – MMS delay in 80/20 traffic mix experiment

The first observation that can be derived from the delay curves in Figure 6.4 is both initiation and polling delay increase when the total traffic load increases. The reason is because when the total traffic load increases, the network resources available for one traffic flow decrease since the total network resources are fixed.

The second comment is that the delay for the initiation process is much higher than the polling delay. The explanation is simple when looking at the MMS message flows (see Figure 4.6) because in the initiation process more MMS messages are needed to be exchanged to firstly set up the connection (COTP messages) and secondly establish the application association between the MMS client and server (initiate-request and initiate-response messages).

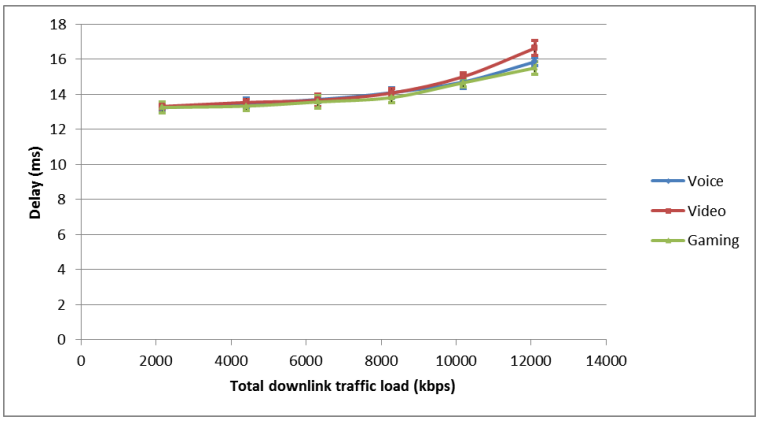
Another important conclusion is that comparing with the delay requirement specified in chapter 3, the delay performance of smart metering traffic over LTE network is very satisfactory when the total traffic load is under the network capacity.

6.3.1.4 Background traffic delay

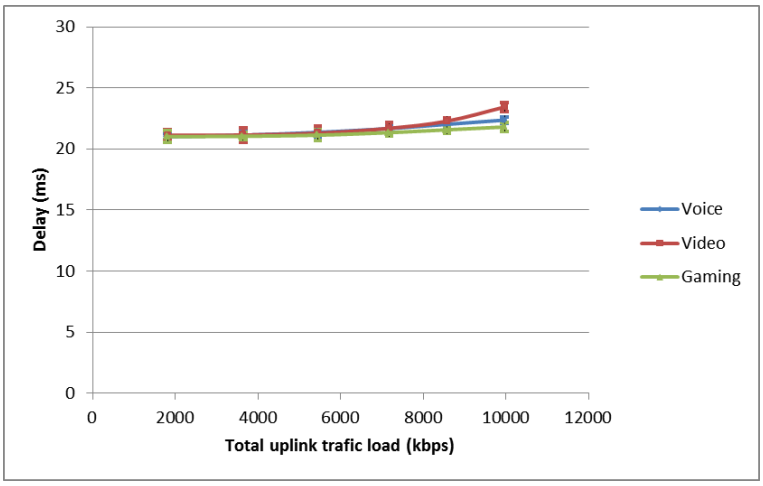
The background traffic delay is shown in Figure 6.5. Since the network always operates within its capacity and the data rates of the background traffics are not high, the delays are relatively small.

Similar to the smart metering traffic, the delay of all background traffics increase when the traffic load increases. Because video streaming application has the highest packet rate, it suffers higher delay especially when the traffic load increases.

Another observation is that the delay in the downlink is slightly less than the delay in the uplink. This can be due to the random access time in the uplink or the slower processing in the eNB for the uplink packets.



(a)

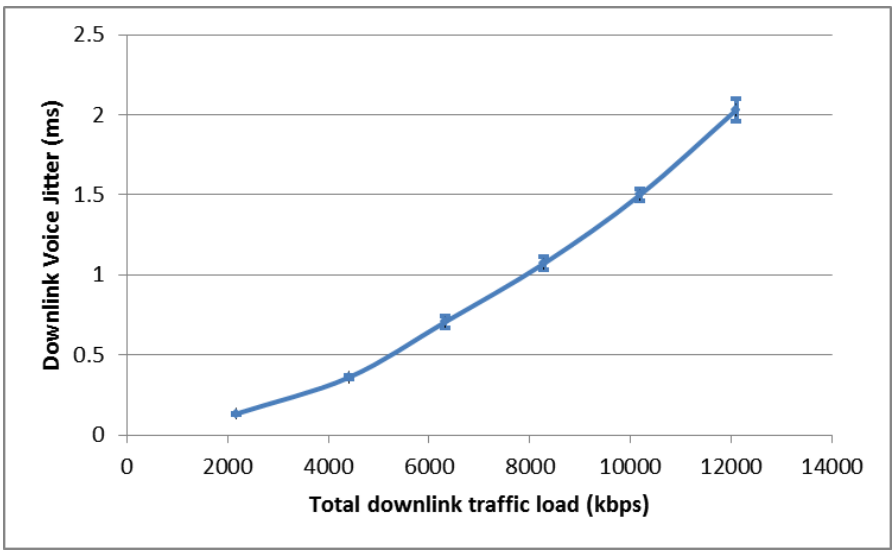


(b)

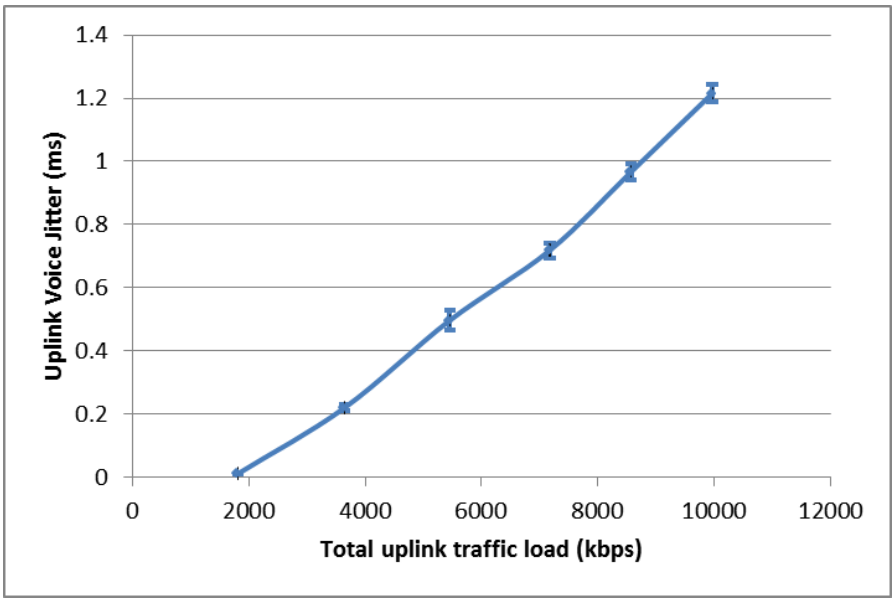
Figure 6.5 –Background traffic delay in 80/20 traffic mix experiment in the downlink (a) and uplink (b)

6.3.1.5 Voice jitter

Figure 6.6 shows the downlink and uplink voice jitter when the total traffic load increases to reach the capacity of the network. Because when the traffic load increases, the chance for the voice traffic to be assigned a RBG becomes less. It leads to the case when some messages have to wait for a longer period before get delivered resulting in an increasing jitter.



(a)



(b)

Figure 6.6 – Voice jitter in 80/20 traffic mix experiment in the downlink (a) and uplink (b)

6.3.2 60/40 downlink traffic mix scenario

In this experiment, the percentage of background traffic and smart metering traffic is always kept as 60% traffic generated by the background nodes and the rest 40% generated by smart meters.

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

The number of background nodes and the corresponding number of smart meters to achieve the 60/40 percentage mix is given in Table 6.3.

Table 6.3 - Number of background nodes and smart meters in the 60/40 traffic mix

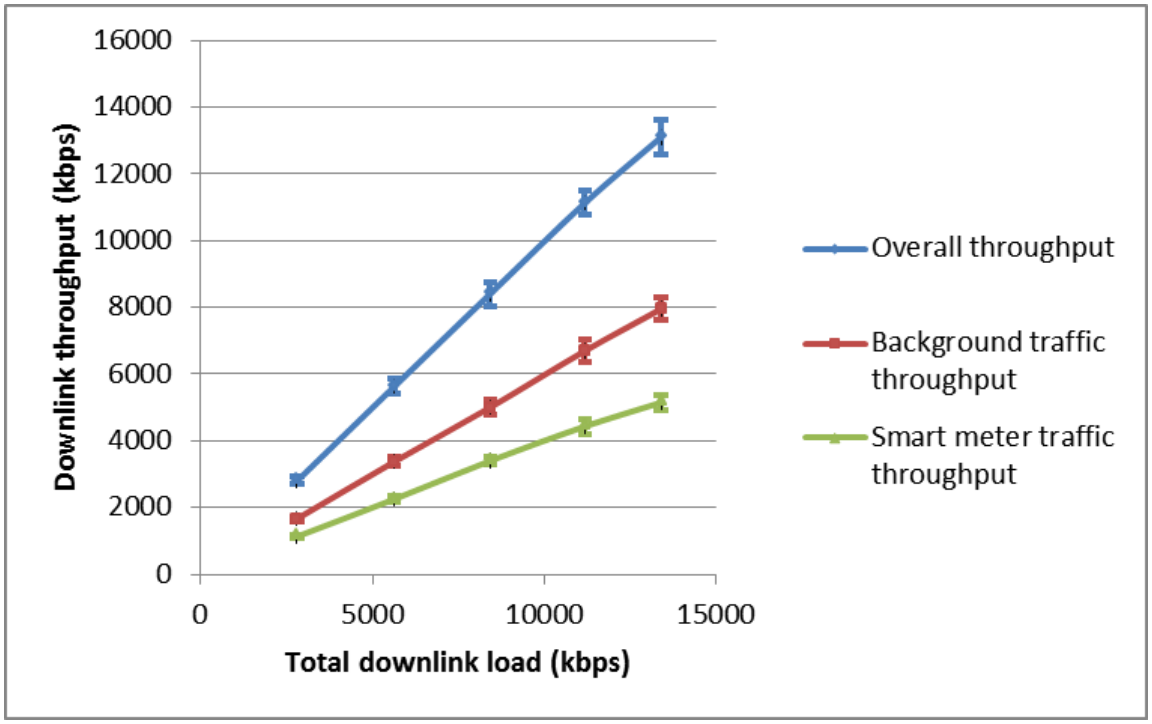
Number of background nodes	Number of smart meters	Total traffic load (kbps)
10	100	2802.670
20	202	5636.251
30	307	8417.335
40	400	11180.450
50	500	13404.009

6.3.2.1 Throughput

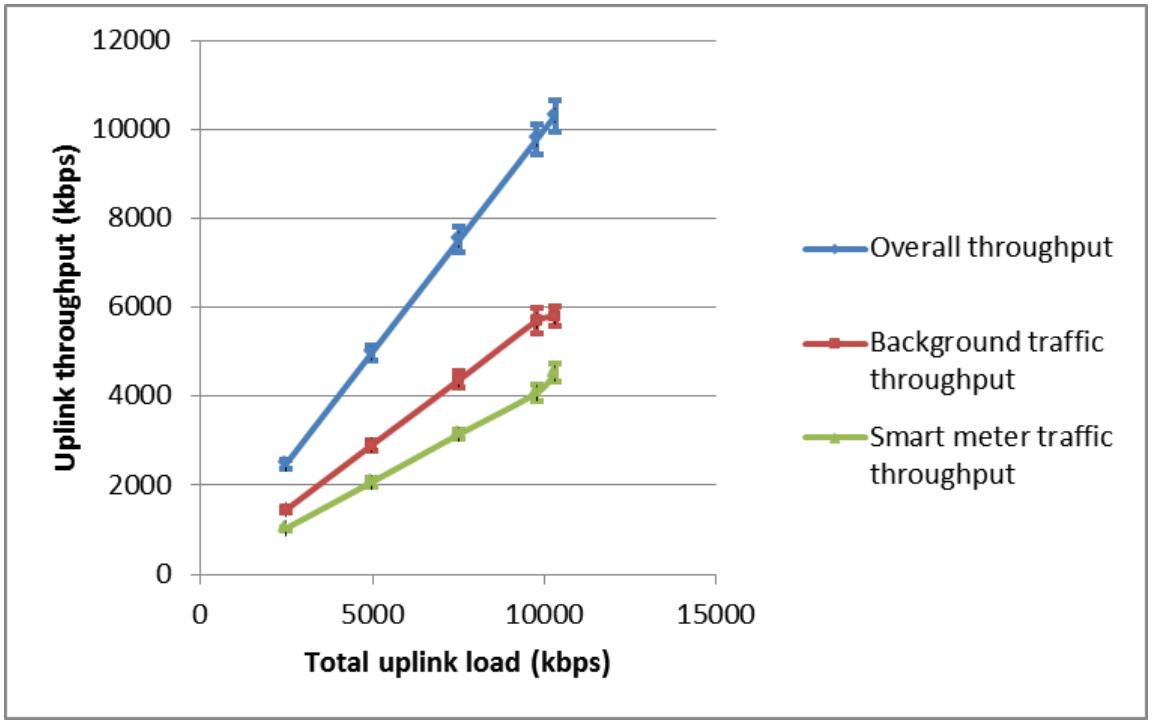
Figure 6.7 shows the average throughput performance for both smart meter and background traffic. Similar to the 80/20 traffic mix experiment, we see that the throughput increases when the traffic load increases.

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.

We also notice that the throughput for the background traffic load is approximately the same as in the case of 80/20 mix in section 6.3.1.1. Due to the higher smart meter traffic over background traffic mix (60/40), the overall throughput in this case is higher due to more smart meter traffic is present.



(a)

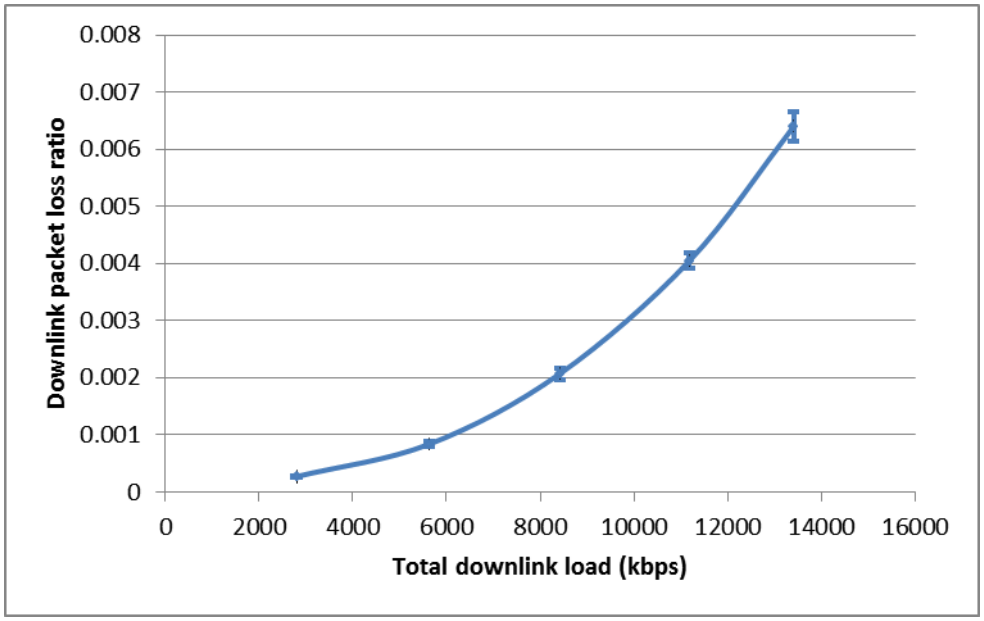


(b)

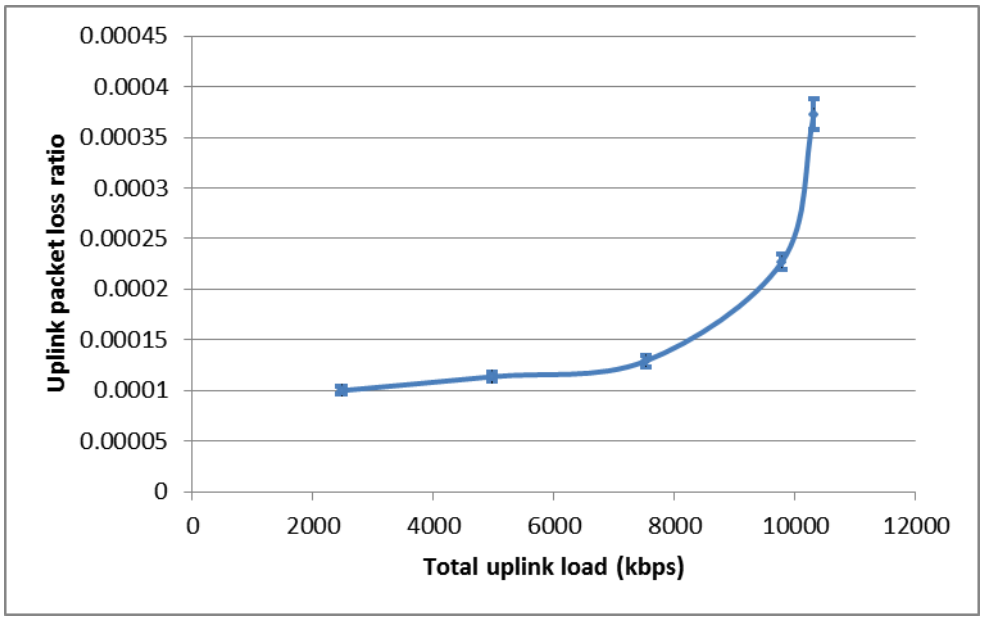
Figure 6.7 – Average throughput performance in 60/40 traffic mix experiment for the downlink (a) and uplink (b)

6.3.2.2 Packet loss ratio

Figure 6.8 shows the packet loss ratio in 60/40 traffic mix experiment. 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.



(a)



(b)

Figure 6.8 – Packet loss ratio in 60/40 traffic mix experiment for the downlink (a) and uplink (b)

6.3.2.3 MMS delay

The delay performances of the smart meter initiation process and smart meter polling process in the 60/40 traffic mix experiment are illustrated in Figure 6.9.

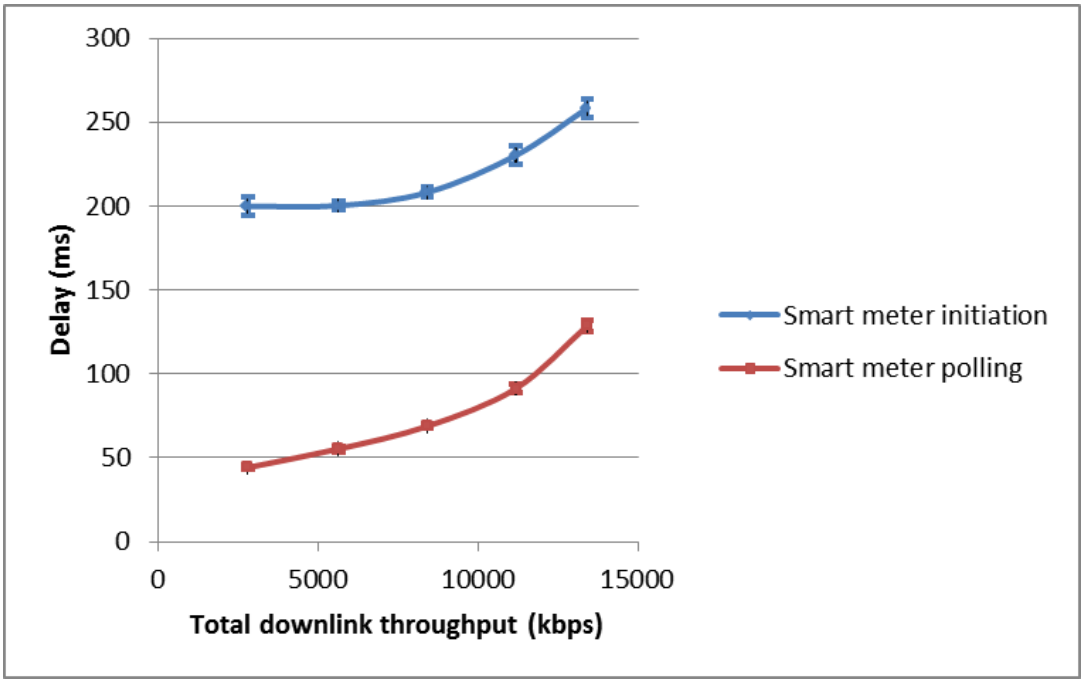


Figure 6.9 – MMS delay in 60/40 traffic mix experiment

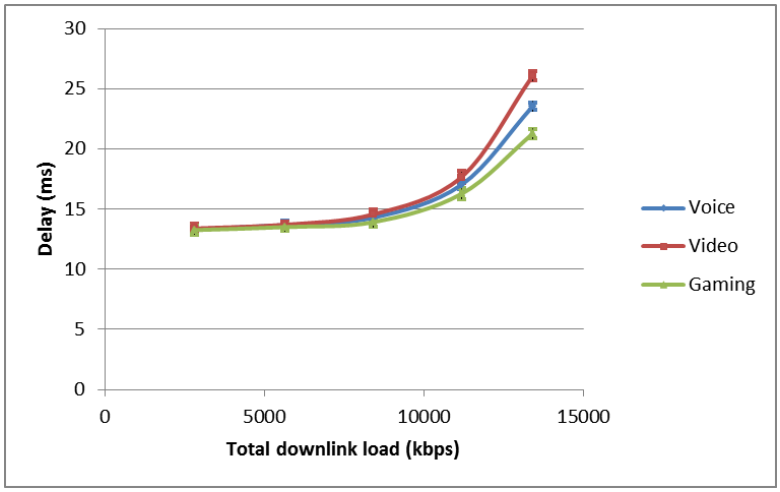
It can be seen in Figure 6.9 that similar to the 80/20 traffic mix scenario, when the traffic load increases, the smart meter initiation delay and polling delay also increase. It is due to the less available resource in both the downlink and uplink and there is a large number of packets in the queue waiting to be scheduled.

It can also be derived from Figure 6.9 that the polling request/response delay is almost the same as in the 80/20 case when the number of nodes is small (10 background nodes), but the polling delay increases more quickly when the traffic load is further increased. On the other hand, the initiation delay is consistently larger than in the 80/20 case by ~50ms, because there are more smart meters trying to access the LTE network, and also the time it takes for the MMS client to initiate with the smart meters is longer.

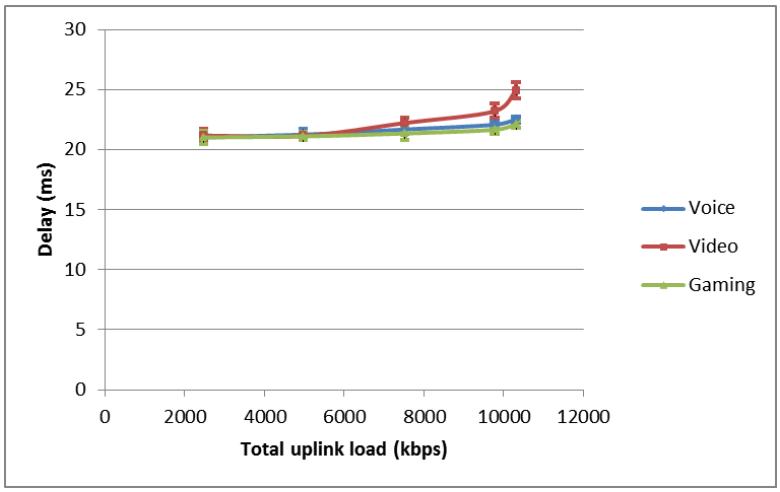
The delay shown in Figure 6.9 is still very low when compared to the IEC 61850 performance requirements of the smart meter communication (1 second).

6.3.2.4 Background traffic delay

The delay performances of the smart meter initiation process and smart meter polling process in the 60/40 traffic mix experiment are illustrated in Figure 6.10.



(a)



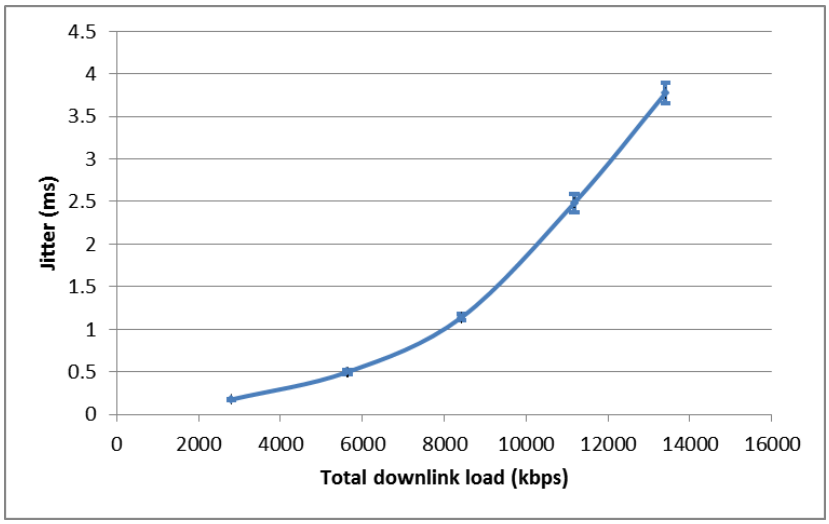
(b)

Figure 6.10 – Background traffic delay in 60/40 traffic mix experiment for the downlink (a) and uplink (b)

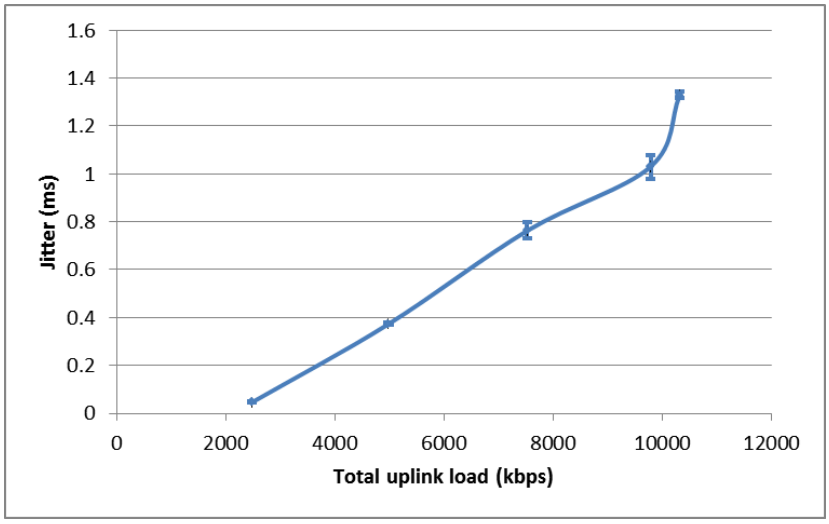
It can be seen in Figure 6.10, that the delay for the background traffic in this scenario is similar to the 80/20 case. For the downlink, the delay in the 60/40 and 80/20 case is the same ~13ms with 10 background nodes. However, in the 60/40 traffic mix scenario, the delay increases much more quickly when the load increases. At 50 background nodes, the delay in the 60/40 case is ~25ms, while in the 80/20 it is ~16ms. The reason for this is given the same number of background nodes; the total number of UEs in the 60/40 case is higher. The uplink exhibits the same behaviour for the 80/20 and 60/40 cases.

6.3.2.5 Voice jitter

Figure 6.11 shows the downlink and uplink voice jitter in the 60/40 traffic mix scenario. The figure presents the same behaviour as the voice jitter in the 80/20 case that the voice jitter increases when the load increases. For the downlink, when the traffic load is less than 10 Mbps, the voice jitter of the two cases is approximately equal. However, when the load is further increases, the voice jitter in the downlink for the 60/40 case is higher (4ms) than in the 80/20 case (2ms). The same observation holds for the voice jitter in the uplink.



(a)



(b)

Figure 6.11 – Voice jitter in 60/40 traffic mix scenario in the downlink (a) and uplink (b)

6.3.3 0/100 traffic mix scenario

In this scenario, we investigate the case where no background traffic is present. The scenario refers to the case where a dedicated network is used to support only the smart meter traffic.

To conduct the experiment, we keep increasing the numbers of smart meters, starting from 100, until the maximum number of UEs that can be supported by LENA in one single cell is reached.

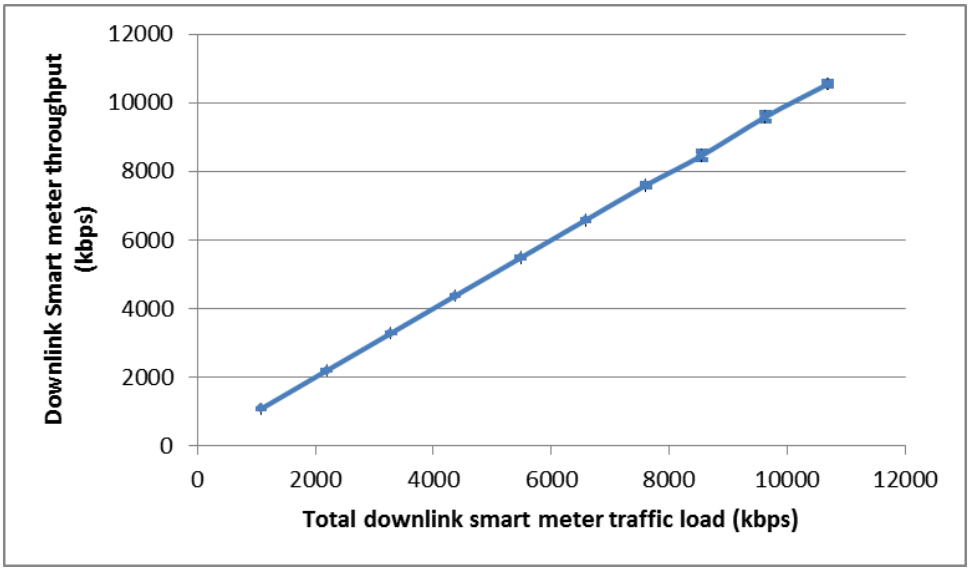
6.3.3.1 Throughput

Figure 6.12 shows average throughput performance for smart meter traffic when the traffic load increases.

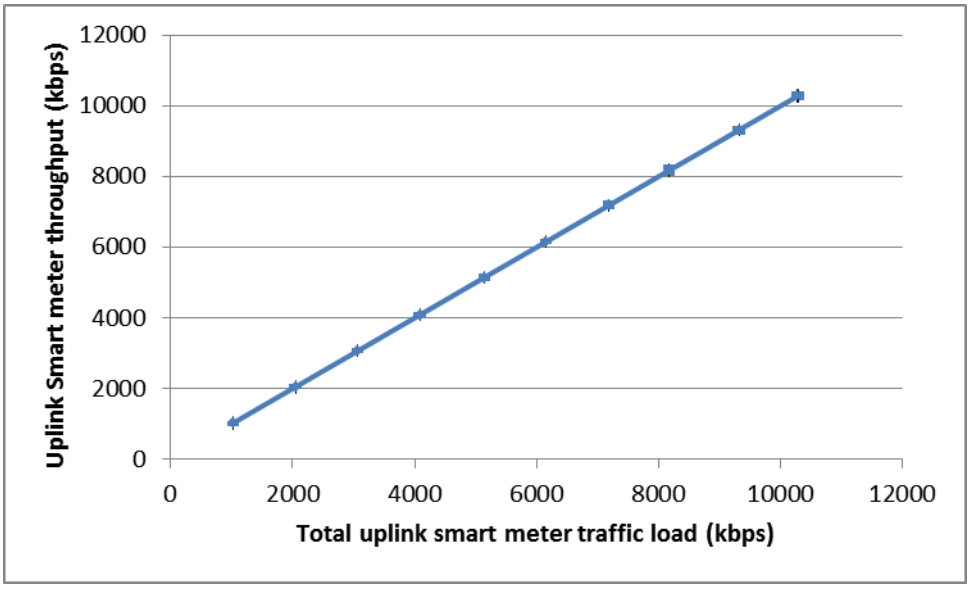
As the traffic load did not exceed the capacity of the network, the throughput is approximately equal to the traffic load, meaning that almost messages were delivered successfully.

6.3.2.2 Packet loss ratio

Figure 6.13 shows the packet loss ratio in the 0/100 traffic mix experiment. The packet loss ratio increases when the number of nodes increases since the network resources available for each node. It should be noted that since the IEC 61850 uses TCP as the transport protocol, it ensures the packet delivery to the destination. Therefore, the packet loss in the network will result in the retransmission of the TCP, which in turn affects the latency of the polling request/response.

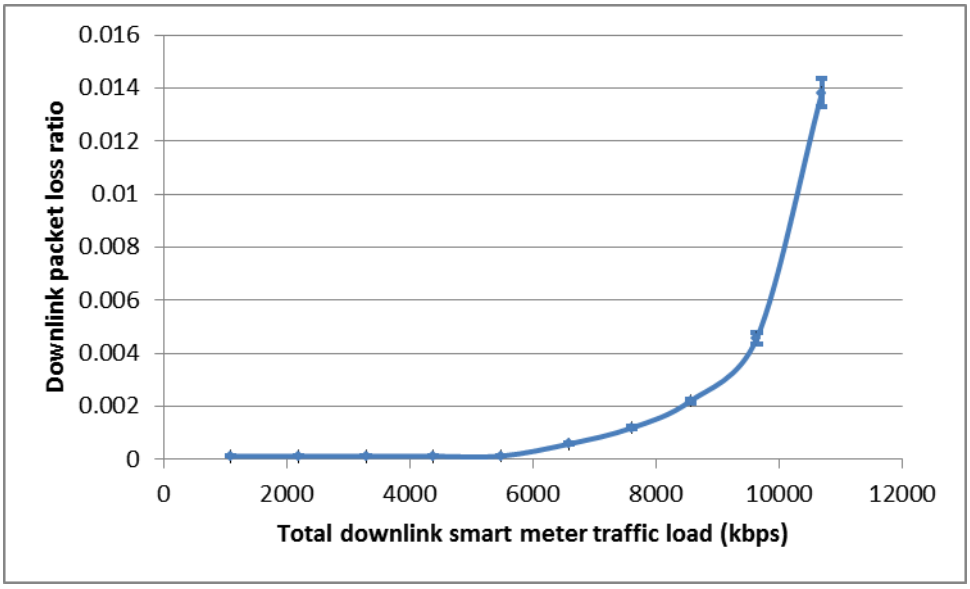


(a)

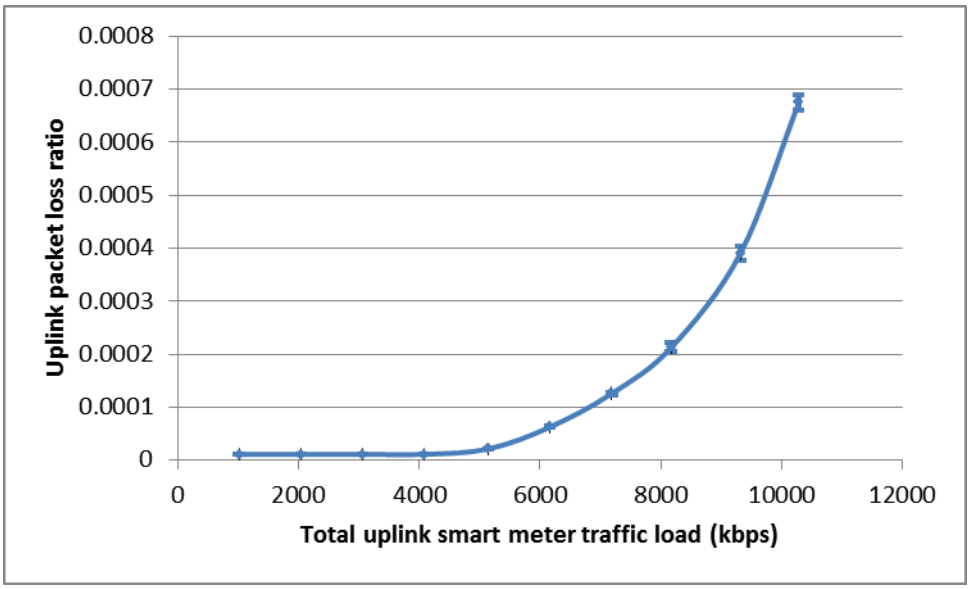


(b)

Figure 6.12 – Average smart meter throughput performance in 0/100 traffic mix experiment for the downlink (a) and uplink (b)



(a)



(b)

Figure 6.13 – Packet loss ratio in 0/100 traffic mix experiment for the downlink (a) and uplink (b)

6.3.2.3 MMS delay

The delay performances of the smart meter initiation process and smart meter polling process in the 60/40 traffic mix experiment are illustrated in Figure 6.14.

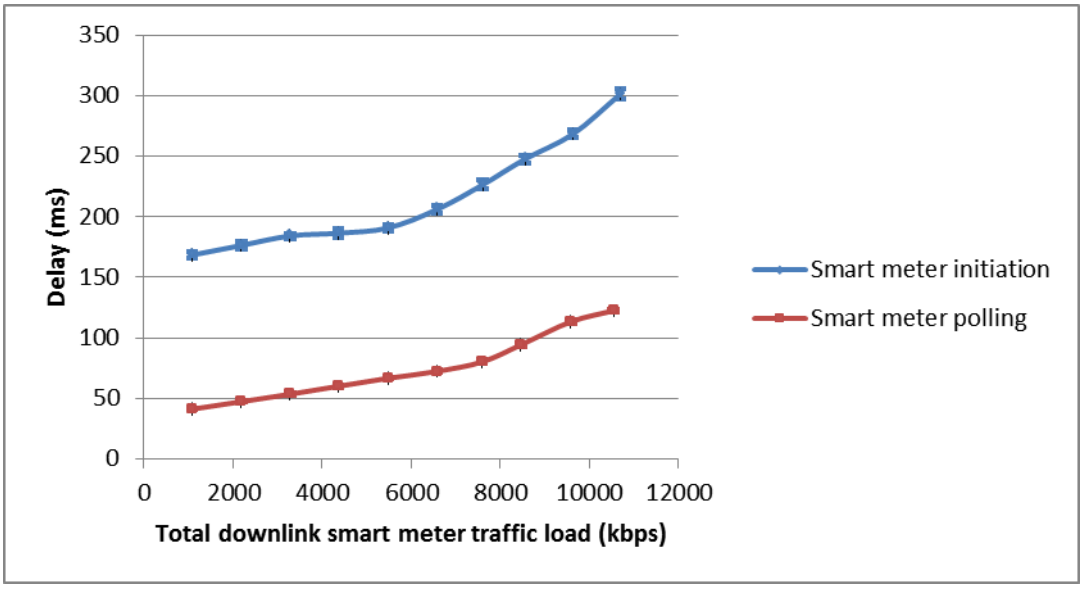


Figure 6.14 – MMS delay in 0/100 traffic mix experiment

It can be seen in Figure 6.14 that similar to the previous 80/20 and 60/40 traffic mix scenarios, when the traffic load increases, the smart meter initiation delay and polling delay also increase. It is due to the less available resource in both the downlink and uplink and there is a large number of packets in the queue waiting to be scheduled. Another cause of the increasing delay is the increasing number of packet loss in both the uplink and the downlink, which requires more retransmission of the TCP traffic, hence higher delay.

However, the delay shown in Figure 6.14 is still about ten times less than the maximum delay required by the smart metering communication, even when the number of smart meters is increased to 1000.

6.4 Chapter summary

In this chapter, the performance evaluation of the proposed AMI solution is carried out. Some different sets of experiment conducted in NS3 LENA simulation environment to evaluate the performance of the proposed solution are discussed. In all of the simulation scenarios, 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 these set of 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 approximately ten times less than the delay requirement specified by IEC 61850 for the smart meter traffic which suggests real-time meter data collection of 1 second polling interval is possible.

The scalability issue is also evaluated throughout the experiments. The increasing number of smart meters and background nodes brings the degradation in the performance. However, the simulation results show that when the load is less than the maximum capacity, the IEC 61850 and LTE still meet the performance requirements of the smart meter communication.

Chapter 7

Conclusion and future work

This chapter discusses the conclusions and the future work. First the research questions are answered. Then the overall conclusions are given and discussed. Finally some recommendations for future work are presented.

7.1 Conclusions

IEC 61850 is an extensible protocol to support a growing demand in different domains. The flexibility of IEC 61850 allows the same data model to be used on different underlying communication protocol, which ensures interoperability within the communicating entities in Smart Grid. On the other hand, LTE is the latest cellular technology that promises many performance enhancements that will meet the need for the growing demanding applications.

In this report we have presented an evaluation of the integration between IEC 61850 MMS and LTE to support smart metering communication. A combination of literature study and simulation-based evaluation has been conducted to answer the main research question "How can smart metering communication be supported by using IEC 61850 MMS over LTE?"

Several sub-questions have been defined in section 1.2, and the answers are given as the following:

1) What are the main requirements and challenges of integrating IEC 61850 MMS and LTE for smart metering communication?

Answer: We have conducted a literature study to answer the first sub-question about the requirements and challenges for integrating IEC 61850 MMS and LTE to support smart metering communication. The main requirements and challenges are described in chapter 3 of this report, which can be divided into two main types of requirement: 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. The smart meter acts as a MMS

server that receives the polling request from the MDMS host which is a MMS client. The latter shows that scalability and delay for real-time meter data collection are the most important performance requirements for remote control communication. Additionally, some challenges were also discovered including the quality of service, and security of the network system.

2) How can the selected challenges be solved?

Answer: 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. The answers to the selected challenges are given by using simulation-based evaluation with the detailed specification and design of the solution described in chapter 4 together with the implementation presented in chapter 5.

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

Answer: 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 set of 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 ten times less than the delay requirement specified by IEC 61850 for the smart meter traffic which suggests real-time meter data collection of 1 second polling interval is possible.

The scalability issue is also evaluated throughout the experiments. The increasing number of smart meters and background nodes brings the degradation in the performance. However, the simulation results show that when the load is less than the maximum capacity, the IEC 61850 and LTE still meet the performance requirements of the smart meter communication.

7.2 Future work

For future work, 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.

IEC 61850 MMS can be mapped 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.

LTE MTC architecture described in section 2.4.8 can be useful to be used, as it brings many enhancements to the performance especially when the number of nodes is huge. As long as there is a simulator that can support LTE MTC, the experiments should be done to evaluate its performance.

We can also investigate a hybrid AMI architecture which combines LTE with a short range wireless technology (such as WiFi, ZigBee, etc.) to see if it can be a more scalable solution. In our research, we only assume a simple point-to-point link between the local smart meter and data concentrator. However, when the short-range wireless technologies are put in place, they might bring additional challenges such as energy efficiency, security, etc. that need to be solved in the short-range communication area.

References

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

[2] Christoph Böhringer, Thomas F. Rutherford, Richard S.J. Tol, "THE EU 20/20/2020 targets: An overview of the EMF22 assessment", 2009

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

[4] EPRI Smart Grid Resource Centre, [Online]. Available: http://smartgrid.epri.com/

[5] Hassan Farhangi, "The path of the Smart Grid", IEEE power & energy magazine, 2010

[6] Ericsson, "Smart-grid communications: enabling next-generation energy networks", EBR #1, 2012

[7] Michael James Martin, "Designing a Broadband Network for a Smart Grid Solution: Challenges and Remedies", [Online]. Available: http://www.generatinginsights.com/whitepaper/designing-a-broadband-network-for-a-smart-grid-solution-challenges-and-remedies.html

[8] Klaas De Craemer, Geert Deconinck, "Analysis of State-of-the-art Smart Metering Communication Standards", [Online]. Available: https://lirias.kuleuven.be/bitstream/123456789/265822/1/Smar

[9] Office of Electricity Delivery and Energy Reliability, "Advanced Metering Infrastructure ", February 2008.

[10] 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

[11] Communications requirements of Smart Grid technologies. [Online]. Available:

http://www.smartgrid.gov/sites/default/files/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf

[12] Ye Yan; Yi Qian; Sharif, H.; Tipper, D., "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," *Communications Surveys & Tutorials, IEEE* , vol.15, no.1, pp.5,20, First Quarter 2013

[13] Parikh, P.P.; Kanabar, M.G.; Sidhu, T.S., "Opportunities and challenges of wireless communication technologies for smart grid applications," *Power and Energy Society General Meeting, 2010 IEEE* , vol., no., pp.1,7, 25-29 July 2010

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

[15] Nian Liu; Jinshan Chen; Hong Luo; Wenxia Liu, "A Preliminary Communication Model of Smart Meter Based on IEC 61850," *Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific* , vol., no., pp.1,4, 25-28 March 2011

[16] IEC 61850-5: Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models

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

[18] Sidhu, T.; Kanabar, M.; Parikh, P., "Configuration and performance testing of IEC 61850 GOOSE," *Advanced Power System Automation and Protection (APAP), 2011 International Conference on* , vol.2, no., pp.1384,1389, 16-20 Oct. 2011

[19] IEC 61850-90-1: Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations

[20] 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

[21] CDG, "CMDA 450 technology". [Online]. Available: http://www.cdg.org/technology/cdma450.asp

[22] Siemens Energy Sector, "Communication Network Solutions for Smart Grids", Power Engineering Guide. [Online]. Available:

http://www.energy.siemens.com/fi/pool/hq/energy-topics/power%20engineering%20guide/PEG_70_KAP_08.pdf

[23] Puttonen, J.; Puupponen, H.-H.; Aho, K.; Henttonen, T.; Moisio, M., "Impact of Control Channel Limitations on the LTE VoIP Capacity," *Networks (ICN), 2010 Ninth International Conference on* , vol., no., pp.77,82, 11-16 April 2010

[24] Sigen Ye; Shin Horng Wong; Worrall, C., "Enhanced physical downlink control channel in LTE advanced Release 11," *Communications Magazine, IEEE* , vol.51, no.2, pp.82,89, February 2013

[25] 3GPP, Technical specification 36.213, evolved universal terrestrial radio access (e-utra); physical layer procedures, 2012.

[26] Agilent Technologies, *LTE And The Evolution To 4G Wireless: Design And Measurement Challenges*, Agilent, 2009

[27] Rohde & Schwarz, "LTE technology and LTE test; a desk-side chat", April 2009.

[28] Harri Holma and Antti Toskala, *LTE for UMTS: OFDMA and SC-FDMA Based Radio Access*, Wiley, 2009

[29] Tara Ali-Yahiya, *Understanding LTE and its Performance*, Springer, 2011

[30] Core Network (EPC) for LTE, Report, Docomo

[31] Olivier Pauzet, Cellular Communications and the Future of Smart Metering, Sierra Wireless Inc., 2010

[32] Smart Meters in Europe. [Online]. Available: http://www.pikeresearch.com/research/smart-meters-in-europe

[33] 3GPP TR 23.888, "System improvements for Machine-Type Communications (MTC) (Release 11)"

[34] 3GPP TS 22.368, "Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 12)"

[35] 3GPP TR 37.868, "Study on RAN Improvements for Machine-type Communications; (Release 11)"

[36] 3GPP2 S.R0146-0, Machine-to-Machine Communication System Requirements, May 2011

[37] 3GPP2 S.R0141-0, "Study for Machine-to-Machine (M2M) Communication for cdma2000 Networks", December 2010

[38] The Network Simulator - NS2 http://www.isi.edu/nsnam/ns/

[39] http://otcl-tclcl.sourceforge.net/otcl/

[40] http://www.isi.edu/nsnam/nam/index.html

[41] http://www.isi.edu/nsnam/xgraph/index.html

[42] http://www.gnuplot.info/

[43] http://www.lrc.ic.unicamp.br/wimax_ns2/

[44] http://eurane.ti-wmc.nl/eurane/

[45] http://www.omnetpp.org/

[46] 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

[47] http://www.opnet.com/

[48] T. S. Sidhu and Y. Yin, "Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems," in IEEE Transactions on Power Delivery, vol. 22, pp. 1482-1489, July 2007.

[49] 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.

[50] 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.

[51] Y. Liang and R. H. Campbell, "Understanding and Simulating the IEC 61850 Standard," 2008. [Online]. Available: https://www.ideals.illinois.edu/handle/2142/11457

[52] 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

[53] http://www.nsnam.org/

[54] http://iptechwiki.cttc.es/LTE-EPC_Network_Simulator_%28LENA%29

[55] 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

[56] http://www.wireshark.org/

[57] http://klub.com.pl/numbat/

[58] http://www.nsnam.org/docs/models/NS3-model-library.pdf

[59] 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.

[60] IEC 61850-90-1 Ed 1.0, “Communication Networks and Systems in Substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Serial Unidirectional Multidrop Point to Point Link”, 2001

[61] 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

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

[63] 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

[64] Jan Tore Sørensen, Martin Gilje Jaatun, "A Description of the Manufacturing Message Specification (MMS)". [Online]. Available: http://sislab.no/MMS_Notat.pdf

[65] "Industrial automation systems, Manufacturing Message Specification. Part 1," ISO 9506-1:2003(E) ISO 2003.

[66] A. M. McKenzie, "ISO Transport Protocol specification ISO DP 8073", 1984

[67] NGMN Alliance, “NGMN Radio Access Performance Evaluation Methodology”

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

[69] LENA Design Documentation. [Online]. Available: http://lena.cttc.es/manual/lte-design.htm

[70] “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

[71] The Flag Protocol. [Online]. Available: www.theflagprotocol.com

[72] M. Wisy, “SML, Smart Message Language v1.03,” Nov. 2008.

[73] European Committee for Standardization (CEN) Std, "EN 13757 Communication systems for remote reading of meters"

[74] "Meter Bus: EN13757-2 and EN13757-3". [Online]. Available: www.m-bus.com/

[75] "Wireless M-Bus Documentation". [Online]. Available: http://www.stzedn.de/wireless-m-bus-stack.html?file=tl_files/products/wmbus_stack/wireless_m_bus_internet.pdf

[76] International Electrotechnical Commission Std, "IEC 62056 Electricity metering - Data exchange for meter reading, tariff and load control".

[77] Heikki Karanen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, Valtteri Niemi, "UMTS Networks Architecture, Mobility and Services", John Wiley & Sons, Ltd, England, 2001

[78] Stefania Sesia, Issam Toufik, Matthew Baker, "LTE – The UMTS Long Term Evolution: From Theory to Practice", John Wiley & Son, Ltd, 2009.

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

Appendix A

IEC 61850 services and message performance requirements

A.1 IEC 61850 ACSI

The IEC 61850 abstract services are summarized in Table A.1.

Table A.1: ACSI classes, copied from [59]

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

A.2 IEC 61850 message performance requirements

Table A.2 – A.8 provide the descriptions and performance requirement of all IEC 61850 message types.

Table A.2 – Requirements for message type 1A

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P1	The total transmission time shall be below the order of a quarter of a cycle (5 ms for 50 Hz, 4 ms for 60 Hz).	**TT6**	≤3	3, 5, 8
P2	The total transmission time shall be in the order of half a cycle (10 ms for 50 Hz, 8 ms for 60 Hz).	**TT5**	≤10	2, 3, 11

Table A.3 – Requirements for message type 1B

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P3	The total transmission time shall be the order of one cycle (20 ms for 50 Hz, 17 ms for 60 Hz).	**TT4**	20	2, 3, 8, 11

Table A.4 – Requirements for message type 2

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		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	2, 3, 8, 9, 11

Table A.5 – Requirements for message type 3

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P5	The total transmission time shall be half the operator response time of = 1 s regarding event and response (bidirectional)	**TT2**	≤500	1, 3, 4, 5, 6, 7, 8, 9, 10
P6	The total transmission time shall be in line with the operator response time of =1 s regarding unidirectional event	**TT1**	≤1000	1, 3, 4, 5, 6, 7, 8, 9, 10

Table A.6 – Requirements for message type 4

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P7 (equiv. to P1)	Delay acceptable for protection functions using these samples	**TT6**	≤3	4, 8
P8 (equiv. to P2)	Delay acceptable for other functions using these samples	**TT5**	≤10	2, 4, 8

Table A.7 – Requirements for message type 5

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P9	Transfer times for files are not critical. Typically, files with process data are used either for post-mortem analysis or for off-line statistics. Files with configuration data require a careful installation and check process. Therefore, no quick operator action of about 1 s is requested. Therefore, 10 000 ms fit very well the file transfer requirements.	**TT0**	≤10000	1, 4, 5, 6, 7, 10

Table A.8 – Requirements for message type 6

Performance class	Requirement description	Transfer time		Typical for interfaces in Figure 3.1
		Class	ms	
P10 (equiv. to P5)	Type 3.P5 message with access control: The total transmission time shall be half the operator response time of =1 s regarding event and response (bidirectional)	**TT2**	≤500	1, 3, 4, 5, 6, 7, 8, 9, 10
P11 (equiv. to P6)	Type 3.P6 message with access control: The total transmission time shall be in line with the operator response time of =1 s regarding unidirectional event	**TT1**	≤1000	1, 3, 4, 5, 6, 7, 8, 9, 10
P12 (equiv. to P9)	Type 5 message with access control: Transfer times for files are not critical. Typically, the time requirements are in the order of the operator response time (= 1 s) or of archives for post-mortem analysis (>>1 s).	**TT0**	≤10000	1, 4, 5, 6, 7, 10

Appendix B

Background traffic specification

Table B.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

Table B.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: $f_x = \lambda e^{-\lambda x} \quad x \geq 0 \quad \lambda = 0.006$

Table B.3 - HTTP/Web 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: $f_x = \frac{1}{\sqrt{2\pi}\sigma x} e^{\frac{-(\ln x - \mu)^2}{2\sigma^2}} \quad x > 0 \sigma = 1.37, \mu = 8.37$
Embedded object size S_E	Truncated lognormal distribution, mean = 7758 bytes, standard deviation = 126168 bytes, minimum = 50 bytes, maximum = 2 Mbytes (before truncation) PDF: $f_x = \frac{1}{\sqrt{2\pi}\sigma x} e^{\frac{-(\ln x - \mu)^2}{2\sigma^2}} \quad x > 0 \quad \sigma = 2.36, \mu = 6.17$
Number of embedded objects per page N_D	Truncated Pareto distribution, mean = 5.64, maximum = 53 (before truncation) PDF: $f_x = \frac{\alpha_k^\alpha}{\alpha + 1}, k \le x < m \quad f_x = \left(\frac{k}{m}\right)^\alpha, x = m$ $\alpha = 1.1, \quad k = 2, \quad m = 55$ Note: subtract k from the generated random value to obtain N_D
Reading time D	Exponential distribution with a mean = 30 seconds PDF: $f_x = \lambda e^{-\lambda x} \quad x \ge 0 \quad \lambda = 0.033$
Parsing time T_p	Exponential distribution with mean = 0.13 seconds PDF: $f_x = \lambda e^{-\lambda x} \quad x \ge 0 \quad \lambda = 7.69$

Table B.4 - Video 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, $m = ??$

Table B.5 - Uplink gaming traffic specification

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

Table B.6 - Uplink gaming traffic specification

Parameter	Statistical characterization
Initial packet arrival	Uniform distribution $f_x = \frac{1}{b-a} \quad a \le x \le b \quad a = 0 \quad b = 40\,\text{ms}$
Packet arrival	Largest Extreme Value Distribution (also known as Fisher–Tippett distribution) PDF: $f_x = \frac{1}{b} e^{-\frac{x-a}{b}} e^{-e^{-\frac{x-a}{b}}} \qquad a = 55\,\text{ms}, \quad b = 6$
Packet size	Largest extreme value distribution (also known as Fisher–Tippett distribution) PDF: $f_x = \frac{1}{b} e^{-\frac{x-a}{b}} e^{-e^{-\frac{x-a}{b}}} \qquad a = 120\,\text{bytes}, \quad b = 36$

Appendix C

IEC 618850 MMS and LTE background traffic module for NS3 manual

C.1 Installation

C.1.1 Install NS-3

The NS3 installation instruction is available at

http://www.nsnam.org/wiki/index.php/Installation

C.1.2 Install the IEC 61850 MMS module in NS3

The source code of IEC 61850 MMS module is available at the web address:

https://github.com/tgpham/mms

Change directory to the source code directory of NS3: `cd <NS3_path>/src`

Clone a copy of the IEC 61850 MMS repository:

```
git clone https://github.com/tgpham/mms.git
```

To compile the IEC 61850 MMS module, change the directory to the NS3: `cd <NS3_path>`, and run the following command in the shell: `./waf`

Waf will start compiling the new module.

C.1.3 Install the LTE background traffic module in NS3

The source codes for the LTE UDP background traffic is available at:

https://github.com/tgpham/gen-udp.git

Change directory to the source code directory of NS3: `cd <NS3_path>/src`

Clone a copy of the IEC 61850 MMS repository: `git clone https://github.com/tgpham/gen-udp.git`

To compile the IEC 61850 LTE background traffic module, change the directory to the NS3: `cd <NS3_path>`, and run the following command in the shell: `./waf`

Waf will start compiling the new module.

* Note: If there is a problem with the build, the following adjustments need to be made in the `wscript` file in the modules:

Change from `headers = bld.new_task_gen(features=['ns3header'])`

to `headers = bld (features=['ns3header'])`

(remove `.new_task_gen`, as for WAF 1.7 and above it will cause errors)

C.2 Using IEC 61850 MMS module in NS3

An example of using IEC 61850 MMS module is included in the `<NS3_path>/src/mms/examples/mmsp2p.cc` script.

The module support several log components that will be printed out to the screen during simulation run-time, and they can be enabled by:

```
LogComponentEnable ("MmsClient", LOG_LEVEL_INFO);
LogComponentEnable ("MmsServer", LOG_LEVEL_INFO);
LogComponentEnable ("MmsAdaptClient", LOG_LEVEL_INFO);
LogComponentEnable ("MmsAdaptServer", LOG_LEVEL_INFO);
LogComponentEnable ("CotpClient", LOG_LEVEL_INFO);
LogComponentEnable ("CotpServer", LOG_LEVEL_INFO);
```

The module can be used like any other NS3 applications, and can be installed on a NS3 node with different underlying protocol (i.e. point-to-point, CSMA, WiFi, LTE, etc.). In this example, we assume a point-to-point link exists between 2 NS3 nodes:

```
// Nodes
NodeContainer clientNodes;
clientNodes.Create (1);
NodeContainer serverNodes;
serverNodes.Create (1);

// Communication Interface
PointToPointHelper pointToPoint;
pointToPoint.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));

// NetDevices
NetDeviceContainer devices;
devices = pointToPoint.Install (clientNodes.Get (0), serverNodes.Get
(0));
```

To enable IEC 61850 MMS protocol on the node, the IP stack first has to be installed, and the IP addresses have to be assigned for the nodes using the Helper.

```
// Internet Stack
InternetStackHelper stack;
stack.Install (clientNodes.Get (0));
stack.Install (serverNodes.Get (0));

Ipv4AddressHelper address;
address.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer clientInterfaces = address.Assign (devices.Get
(0));
Ipv4InterfaceContainer serverInterfaces = address.Assign (devices.Get
(1));
```

The packet trace (PCAP output) can be turned on to allow verifying/analysing the communication on the link:

```
pointToPoint.EnablePcapAll("mms-p2p-");
```

The MMS server and client are defined using the `MmsServerHelper` and `MmsClientHelper`. These helpers facilitate the usage of the IEC 61850 MMS module in the simulation script. First the user has to specify the interfaces that the MMS server listens on, create an `ApplicationContainer` on the NS3 server node, and specify the application start and stop time.

```
// MMS Application

MmsServerHelper mmsServer (serverInterfaces);

ApplicationContainer serverApps = mmsServer.Install (serverNodes.Get
(0));
serverApps.Start (Seconds (1.0));
serverApps.Stop (Seconds (20.0));
```

Similarly for the client side, the user has to specify the interfaces that the MMS client uses to connect to the server and the server `ApplicationContainer`:

```
MmsClientHelper mmsClient (serverApps, clientInterfaces, MilliSeconds
(0), type, mode, false);

ApplicationContainer clientApps = mmsClient.Install (clientNodes.Get
(0));
clientApps.Start (Seconds (2.0));
clientApps.Stop (Seconds (20.0));
```

C.3 Using LTE background traffic module in NS3

An example of using IEC 61850 MMS module is included in the `<NS3_path>/src/gen-udp/examples/lte-BgNodes.cc` script. Every section in the source code is commented to help the user with the usage of the code.

Some of the key points in using the module are listed as follows.

The LTE UE nodes are created based on the traffic mix specified in [68]:

```
// Create Voice UEs (30% of the nodes)
NodeContainer lteVoiceUeContainer;
lteVoiceUeContainer.Create((float)0.3*numberOfBgNodes);

// Create Video UEs (20% of the nodes)
NodeContainer lteVideoUeContainer;
lteVideoUeContainer.Create((float)0.2*numberOfBgNodes);

// Create Gaming UEs (20% of the nodes)
NodeContainer lteGamingUeContainer;
lteGamingUeContainer.Create((float)0.2*numberOfBgNodes);

// Create HTTP UEs (20% of the nodes)
NodeContainer lteHttpUeContainer;
lteHttpUeContainer.Create((float)0.2*numberOfBgNodes);

// Create FTP UEs (the rest)
NodeContainer lteFtpUeContainer;
lteFtpUeContainer.Create(numberOfBgNodes-lteVoiceUeContainer.GetN()
-lteVideoUeContainer.GetN()
-lteGamingUeContainer.GetN()
-lteHttpUeContainer.GetN());
```

The remote hosts are created to allow each type of traffic to be transfered:

```
// Create Voice Remote host to send/receive Voice traffic to/from
Voice UEs
NodeContainer lteVoiceRemoteContainer;
lteVoiceRemoteContainer.Create(1);

// Create Video Remote host to send/receive Video traffic to/from
Video UEs
NodeContainer lteVideoRemoteContainer;
lteVideoRemoteContainer.Create(1);

// Create Gaming Remote host to send/receive Gaming traffic to/from
Gaming UEs
NodeContainer lteGamingRemoteContainer;
lteGamingRemoteContainer.Create(1);

// Create FTP Remote host to send/receive FTP traffic to/from FTP UEs
NodeContainer lteFtpRemoteContainer;
lteFtpRemoteContainer.Create(1);
```

```
// Create a number of HTTP Server, one for each UEs (currently server
does not support multiple clients)
NodeContainer lteHttpRemoteContainer;
lteHttpRemoteContainer.Create(lteHttpUeContainer.GetN());
```

In order to work with LTE, several steps need to be followed. These steps are based on the tutorial of the LTE in NS3 LENA, and details can be found in the source code.

- Create the PGW
- Create Point to Point connections between P-GW and all remote hosts
- Assign the IPv4 addresses to the Remote hosts
- Install needed routing information from remote hosts to UEs
- Create the eNB and Install Mobility Model for the eNB and UEs
- Install LTE Devices to the nodes
- Install the IP stack on the UEs
- Define IPv4 interfaces on UEs
- Set default gateways for UEs

The LTE background traffic server and client are defined using the `GeneralUdpServerHelper` and `GeneralUdpClientHelper`. There is also an additional parameter to specify the exact traffic type (Video=0, Gaming uplink=1, Gaming downlink=2, VoIP=3), and it must be declared when adding ApplicationContainer to the node. For example, the following part of the script creates uplink and downlink video traffic

```
// ------------------------------------------------------------------
// Video Application, both UL and DL

// UPLINK (from UEs)
//
// Create one Video applications on remote host.
//
uint16_t lteVideoRemotePort = 5000;
GeneralUdpServerHelper lteVideoRemoteServer (lteVideoRemotePort, 0);
ApplicationContainer lteVideoUeApp = lteVideoRemoteServer.Install
(lteVideoRemoteNode);
lteVideoUeApp.Start (Seconds (0.0));
lteVideoUeApp.Stop (Seconds (1000.0));

//
// Create one Video application to send UDP datagrams from UE nodes to
// Remote Video host.
//
GeneralUdpClientHelper VideoClientUe (lteVideoRemoteAddress,
lteVideoRemotePort, 0); //0 = video; 1 = Video uplink
lteVideoUeApp = VideoClientUe.Install (lteVideoUeContainer);
lteVideoUeApp.Start (Seconds (0.1));
lteVideoUeApp.Stop (Seconds (100.0));

// DOWNLINK (to UEs)
```

```
//
// Create Video applications on UE nodes.
//
uint16_t lteVideoUePort = 5000;
GeneralUdpServerHelper lteVideoUeServer (lteVideoUePort, 0);
ApplicationContainer lteVideoRemoteApp = lteVideoUeServer.Install
(lteVideoUeContainer);
lteVideoRemoteApp.Start (Seconds (0.0));
lteVideoRemoteApp.Stop (Seconds (1000.0));

//
// Create one Video application to send UDP datagrams from Remote Host
to
// VoIP UEs.
//
for (uint32_t i = 0; i < lteVideoUeInterface.GetN(); i++)
{
GeneralUdpClientHelper VideoClientRemote
(lteVideoUeInterface.GetAddress(i), lteVideoUePort, 0); //0 = video; 1
= Video uplink
lteVideoRemoteApp = VideoClientRemote.Install (lteVideoRemoteNode);
lteVideoRemoteApp.Start (Seconds (0.1));
lteVideoRemoteApp.Stop (Seconds (100.0));
}
```