Performance Evaluation of Non-commercial LTE Network For Smart Grid Application

Modification of IEC 61850-90-5 Protocol stack and its Testing over Non-commercial LTE

RAJENDRA BOGATI
Modification of IEC 61850-90-5 Protocol stack and its Testing over Non-commercial LTE

Modification of IEC 61850-90-5 Protocol stack and its Testing over Non-commercial LTE

Rajendra Bogati
August 2017

The thesis work was carried out in coordination
ABB Corporate Research Centre
Vasteras, Sweden

Examiner: Professor Dr. Ahmed Hemani
School of ICT
KTH Royal Institute of Technology

Supervisor: Dimitrios Stathis
School of ICT
KTH Royal Institute of Technology

Dr. Gargi Bag
Senior Scientist
ABB Corporate Research Centre
Acknowledgement

The dissertation describes the master thesis project conducted in cooperation with ABB at ABB Corporate Research in Västerås, Sweden.

First and foremost, I express my humble gratitude to the Almighty for the strength he has given me throughout my life.

I would like to thank Mr. Linus Eriksson who was a part of this project and who has contributed to the success of this project. I would also like to thank ABB Corporate Research for giving me the opportunity to work on this project. Many thanks to my supervisor Dr. Gargi Bag, Scientist, ABB Corporate Research Centre for all her help, guidance, support and feedback throughout the project. Many thanks to Mr. Linus Thrybom and Mr. Morgan E. Johansson for providing useful documents and giving the right direction to solve the problem. Special thanks to my colleague Deep, Monika, Camila, Huang, Mattias, Hamze, Sayed and all other thesis workers at ABB Corporate Research Centre for their wonderful company and kind help to solve problem that came across while working on my thesis and stay at Västerås.

Many thanks to my examiner Prof. Dr. Ahmed Hemani, Department of Electronic Systems, KTH Royal Institute of Technology for all the support and feedback whenever I need it. I am particularly grateful to Dimitrios Stathis for his valuable feedback and suggestion on writing the report.

I am always thankful to my family for their everlasting love and support. Special thanks to all my friends who supported and inspired me when I need them. I won’t accomplish this without their kind support.

Rajendra Bogati
Stockholm
August 2017
Abstract

The introduction of smart grid technology has changed the way traditional power grid network function. It made the grid structure more dynamic by enhancing electrical usage management capability. Also, it has increased the scope to enhance communication infrastructure in a smart grid structure. The current smart grid solution is based on IEC 61850 architecture where the exchange of information between the electrical utilities is over the fast Ethernet LAN connection. This communication mechanism is fast, efficient but lacks scalability, flexibility and less susceptible to failure. Also, earlier technical paper from IEC 61850 standard was for communication within a substation.

Wide Area Monitoring Protection and Control implementation which utilizes coherent real time synchrophasor information would play a vital role in realizing the utility physical status. IEC 61850-90-5, a new technical report from International Electrotechnical Commission provides the mechanism to transmit and receive the synchrophasor information using the advance IP protocol over a wireless communication infrastructure for WAMPAC application. IEC 61850-90-5 provide a way to exchange routable synchrophasor information over public IP network such as LTE, WiMax, WLAN, etc. Out of all the available wireless solution, LTE provides high flexibility, distance coverage, data rate with low latency and hence can play an important role in replacing the existing communication structure in a smart grid.

The thesis work evaluates the performance and applicability of LTE for smart grid communication. An IEC 61850-90-5 communication model utilizing UDP/IP protocol to transmit and receive data over the LTE network was developed from the open source project. The modified model was used to benchmark the performance of LTE. Different communication metrics such as reliability, availability, latency, and throughput was evaluated to benchmark the performance of LTE for time critical smart grid application. The metrics were measured for different packet sizes and transmission rates combination.

The result shares some interesting findings on the readiness of LTE for smart grid solution. It is concluded that cellular network can play an important role in realizing communication infrastructure in a smart grid application.
Contents

Abstract i
List of Figures v
List of Tables vii
Abbreviations ix

1 Introduction 1
  1.1 Motivation .................................................. 1
  1.2 Scope of thesis .............................................. 2
  1.3 Related Work .............................................. 2
    1.3.1 Performance of LTE for Smart Grid Application .......... 2
    1.3.2 Performance Evaluation of Smart Grid Communications via Network Simulation Version 3 .......... 3
    1.3.3 Performance Evaluation of Cellular Communication System for Machine-to-Machine Smart Grid Application .......... 3
    1.3.4 Work Related to Routable GOOSE and SV Transmission .......... 4
  1.4 Thesis outline ............................................ 4

2 Background 5
  2.1 Electric Power System ....................................... 5
  2.2 Smart Grid Technology ....................................... 7
    2.2.1 Architecture of Smart Grid ................................ 7
    2.2.2 Technology requirement for Smart Grids ..................... 8
  2.3 Substation Automation System .................................. 8
    2.3.1 Communication in SAS ..................................... 10
  2.4 IEC 61850 .................................................. 10
    2.4.1 IEC61850 Series Outline .................................. 11
    2.4.2 IEC 61850 Data Modeling ................................... 13
    2.4.3 IEC 61850 Service and Data Mapping to Communication Protocols .......... 14
    2.4.4 Generic Object Oriented Substation Event ................. 15
    2.4.5 Sample Value ........................................... 16
  2.5 Synchrophasor Technology ..................................... 16
  2.6 TR IEC 61850-90-5 ........................................ 17
    2.6.1 Data Modeling in IEC 61850-90-5 ........................... 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.2</td>
<td>Communication Scheme</td>
<td>19</td>
</tr>
<tr>
<td>2.6.3</td>
<td>IEC 61850-90-5 services</td>
<td>21</td>
</tr>
<tr>
<td>2.6.4</td>
<td>Routed-Sample Value Profile Mapping</td>
<td>22</td>
</tr>
<tr>
<td>2.6.4.1</td>
<td>Route-SV A-Profile</td>
<td>22</td>
</tr>
<tr>
<td>2.6.4.2</td>
<td>Route-SV T-Profile</td>
<td>28</td>
</tr>
<tr>
<td>3</td>
<td>Wireless Communication Performance Metrics</td>
<td>31</td>
</tr>
<tr>
<td>3.1</td>
<td>Wireless Communication</td>
<td>31</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Long Term Evolution</td>
<td>31</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Communication Requirement in IEC 61850-90-5</td>
<td>32</td>
</tr>
<tr>
<td>3.1.2.1</td>
<td>Network Throughput</td>
<td>32</td>
</tr>
<tr>
<td>3.1.2.2</td>
<td>Latency or Transfer time</td>
<td>33</td>
</tr>
<tr>
<td>3.1.2.3</td>
<td>Reliability</td>
<td>34</td>
</tr>
<tr>
<td>3.1.2.4</td>
<td>Availability</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>Implementation and Testing</td>
<td>37</td>
</tr>
<tr>
<td>4.1</td>
<td>Design and Implementation of IEC 61850-90-5 Protocol Stack</td>
<td>37</td>
</tr>
<tr>
<td>4.1.1</td>
<td>IEC 61850-90-5 Standalone Application Control flow</td>
<td>38</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Synchrophasor Data Encoding in R-SV packet</td>
<td>40</td>
</tr>
<tr>
<td>4.1.3</td>
<td>IEC 61850 Timestamping</td>
<td>41</td>
</tr>
<tr>
<td>4.2</td>
<td>Test Methodology</td>
<td>42</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Setup Overview</td>
<td>42</td>
</tr>
<tr>
<td>4.2.1.1</td>
<td>Environmental Setup</td>
<td>42</td>
</tr>
<tr>
<td>4.2.1.2</td>
<td>Time Synchronization Setup</td>
<td>43</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Test Model</td>
<td>43</td>
</tr>
<tr>
<td>4.2.2.1</td>
<td>Control Flow</td>
<td>43</td>
</tr>
<tr>
<td>4.2.2.2</td>
<td>Configuration File</td>
<td>45</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Test Cases</td>
<td>46</td>
</tr>
<tr>
<td>4.2.3.1</td>
<td>Test Case To Measure Throughput</td>
<td>46</td>
</tr>
<tr>
<td>4.2.3.2</td>
<td>Test Case To Measure Latency</td>
<td>46</td>
</tr>
<tr>
<td>4.2.3.3</td>
<td>Test Case To Measure Reliability</td>
<td>47</td>
</tr>
<tr>
<td>4.2.3.4</td>
<td>Test Case To Measure Availability</td>
<td>47</td>
</tr>
<tr>
<td>4.2.4</td>
<td>Data Analysis and Extraction</td>
<td>48</td>
</tr>
<tr>
<td>5</td>
<td>Result and Analysis</td>
<td>49</td>
</tr>
<tr>
<td>5.1</td>
<td>Result</td>
<td>49</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Throughput</td>
<td>49</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Latency</td>
<td>49</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Reliability</td>
<td>51</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Availability</td>
<td>52</td>
</tr>
<tr>
<td>6</td>
<td>Conclusion and Future Work</td>
<td>55</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>60</td>
</tr>
</tbody>
</table>
List of Figures

2.1 Conventional Electric Power Grid System Structure .......................... 5
2.2 Conventional Unidirectional Electric Power Grid System Architecture ... 6
2.3 Smart Grid Conceptual Model .................................................... 7
2.4 IEC 61850 based substation automation system ............................. 9
2.5 IEC 61850 based Data Model .................................................. 14
2.6 IEC 61850 standard mapping to OSI Stack .................................. 15
2.7 Mapping of Synchrophasor Information in 90-5 ............................... 18
2.8 PMU data Modeling ................................................................... 20
2.9 service mapping in IEC61850-90-5 ............................................. 21
2.10 IEC 61850-90-5 Routed-Sample Value (R-SV) OSI Model ............... 23
2.11 General Byte Ordering of IEC 61850-90-5 Session Protocol ............. 23
2.12 IEC 61850-90-5 A-Profile ....................................................... 25
2.13 Basic Encoding Rule ............................................................... 26
2.14 ASN.1 BER Encoded Sample Value data format ............................ 27
2.15 IEC 61850-90-5 T-Profile ....................................................... 29
3.1 Transfer time for WMAPAC application ....................................... 34
4.1 Control Flow in Protocol Stack .................................................. 39
4.2 R-SV packet captured in Wireshark ............................................ 40
4.3 Synchrophasor data representation captured in Wireshark ............... 41
4.4 Environmental setup ................................................................ 42
4.5 Time Synchronization setup ....................................................... 44
4.6 Test Model Control flow ............................................................ 44
4.7 Sample Configuration File ......................................................... 45
5.1 Throughput graph of different transmission intervals against different packet sizes . 50
5.2 latency for different transmission interval and packet size ................ 50
5.3 Cumulative Distribution Frequency of latency ................................ 51
5.4 Reliability for SV over a period of 60 seconds ............................... 52
5.5 Availability of the LTE network in 24 hours ................................. 53
List of Tables

2.1 IEC 61850 series Outline ................................................. 12
2.2 New Added Series of IEC 61850 ........................................ 13
2.3 Different Security Option in 90-5 ..................................... 19
2.4 IEEE C37.118.2 Command Frame Equivalent in IEC 61850-90-5 .... 22
4.1 Time Quality Definition .................................................. 42
Abbreviations

2G  Second Generation.
3G  Third Generation.
3GPP  3rd Generation Partnership Project (3GPP).
4G  Fourth Generation.
5G  Fifth Generation.
A-Profile  Application Profile.
ABB  ASEA Brown Boveri.
AC  Alternating Current.
ACSI  Abstract Communication Service Interface.
AES  Advanced Encryption Standard.
AMI  Advanced Metering Infrastructure.
APDU  Application Protocol Data Unit.
BER  Basic Encoding Rule.
CDC  Common Data Class.
CDF  Cumulative Distribution Function.
CT  Current Transformer.
DC  Direct Current.
DCU  Data Concentrator Unit.
DER  Distributed Energy Resource.
DG  Distributed Generation.
EPC  Evolved Packer Core.
**FACTS** Flexible AC Transmission Systems.

**GDOI** Group Domain of Interpretation.

**GOOSE** Generic Object Oriented Substation Event.

**GSE** Generic Substation Event.

**GSM** Global System for Mobile Communications.

**GSSE** Generic Substation State Event.

**HMAC** Hashed Message Authentication Code.

**HMI** Human Machine Interaction.

**IDE** Integrated Development Environment.

**IEC** International Electrotechnical Commission.

**IED** Intelligent Electronic Device.

**IGMPv3** Internet Group Management Protocol version 3.

**IP** Internet Protocol.

**KDC** Key Distribution Center.

**LAN** Local Area Network.

**LTE** Long Term Evolution.

**LTE-SAE** Long Term Evolution -System Architecture Evolution.

**M2M** Machine-to-Machine.

**MIMO** Multiple-Input Multiple-Output.

**MMS** Manufacturing Message Specification.

**MPLS** Multi Protocol Label Switching.

**MU** Merging Unit.

**OFDM** Orthogonal Frequency Division Multiplexing.

**OSI** Open Source Interconnect.

**PDC** Phasor Data Concentrators.

**PLC** Power Line Communication.

**PMU** Phasor Measurement Unit.

**pps** packet per second.
**PT** Power Transformer.

**R-GoCB** Routed- Goose Control Block.

**R-GOOSE** Routed- Generic Object Oriented Substation Event.

**R-MSVCB** Routed Multicast Sample Value Control Block.

**R-SV** Routed- Sample Value.

**RFC** request For Comment.

**ROCOF** Rate Of Change Of Frequency.

**RTT** Round-Trip-Time.

**SAS** Substation Automation System.

**SC-FDMA** Single Carrier Frequency Division Multiple Access.

**SCADA** Supervisory Control And Data Acquisition.

**SCL** Substation Configuration Language.

**SCMS** Specific Communication Service Mapping.

**SDH** Synchronous Digital Hierarchy.

**SISCO** System Integration Specialist Com-pany.

**SONET** Synchronous Optical Networking.

**SPDU** Session Protocol Data Unit.

**SV** Sampled Value.

**SVCB** Sampled Value Control Block.

**T-Profile** Transport Profile.

**TCP** Transmission Control Protocol.

**TLV** Tag Length Value.

**TSDU** Transport Session Data Unit.

**UCA** Utility Communication Architecture.

**UDP** User Datagram Protocol.

**UMTS** Universal Mobile Telecommunications System.

**UTC** Coordinated Universal Time.

**WAMPAC** Wide Area Monitoring Protection and Control.

**WLAN** Wireless LAN.
1 | Introduction

Electrical power network has transformed rapidly over the past few decades. The introduction of smart technology has revolutionized the conventional power grid structure from uni-directional power flow to bi-directional power flow system and made the grid structure more distributed, dynamic and even more complex. This has increased the need for robust communication system between different smart grid equipment for control, monitoring, and protection application.

Wide Area Monitoring Protection and Control application can be realized through synchrophasor information exchange. IEEE C37.118 standard provides the way to measure and exchange synchrophasor information [1], [2]. But it suffers the interoperability and security issues. On the other hand, IEC 61850 provides a standard solution for interoperability and security issue. IEC 61850 is the first series of the standard which basically describes the way of exchanging IEC related information within a substation. It cannot be used for inter-substation communication. Hence, a new technical report was required that helps in exchanging synchrophasor information based on IEC 61850 standard.

Technical report IEC 61850-90-5 is prepared by International Electrotechnical Commission technical committee 57 and provides the way to exchange the synchrophasor information between different smart grid equipment and outside a substation in IEC 61850 context [3]. It makes use of Internet Protocol protocol to transmit/receive synchrophasor data between two devices using public IP networks such as 4G and 5G.

1.1 Motivation

There have been several electrical disturbance event over the past few years and from the study, it was realized that synchrophasor information can be useful in preventing such great electrical blackout [4]. The efficient communication system is required to exchange this useful synchrophasor information within and outside the substation. The existing communication system lacks the flexibility and redundancy in case of electrical failure. Cellular technology like Long Term Evolution and 5G has evolved and matured a lot over the past few years and can be a suitable solution to strengthen the communication infrastructure in a smart grid operation.

IEC 61850-90-5 propose to use the advanced Internet Protocol along with multicast and enhanced security feature mentioned in IEC 62351 to create a routable synchrophasor traffic that can be exchanged using any wireless communication. WAMPAC application has to meet the communication requirement of availability. For the choice of wireless communication to be used for WAMPAC application, have to meet requirements related to latency, reliability and availability.
of the different applications in power grids. While the severity of the requirements varies from application to application, there will be additional requirements related to redundancy, time synchronization, security and coverage.

LTE is a high speed all IP wireless communication system used for mobile communication. LTE offers high bandwidth, enhanced security, high reliability, and low latency for time-critical traffic. It can be a potential solution to replace the existing smart grid communication infrastructure.

1.2 Scope of thesis

The scope of the work was to study the applicability of LTE in smart grid communication for time critical application. Synchrophasor data were created, mapped into Routed- Sample Value profile and transmitted in LTE infrastructure. Overall the thesis was divided into two major task.

The first task includes the development of complete IEC 61850-90-5 protocol stack. This work includes the creation of synchrophasor data, encapsulating the data into UDP/IP protocol and forming a R-SV profile data. In addition to that, different counters and functions were implemented to facilitate the measurement of important communication parameters.

The second part includes identifying the important communication metrics to benchmark the communication system applicability. Four different parameter latency, reliability, throughput, and availability were identified and was measured. A test and measurement framework was created during the course of the thesis work to analyze the performance of 90-5 protocol in an LTE environment.

In order to finish the thesis work in provided time, the work was mainly focused on implementing the synchrophasor data as IEC 61850-90-5 services. The security aspect of the data was not considered and is being left for future work. The performance result for both Routed- Sample Value and Routed- Generic Object Oriented Substation Event shows almost similar result and since R-SV are used for transmitting stream of synchrophasor information, the report only includes the result from R-SV calculation.

The non-commercial LTE network used for the thesis work is called as LTE-evolution. It was provided by an external project partner and hence the architecture of LTE network is not described in this report.

1.3 Related Work

The innovation in wireless and cellular communication has gained the interest of researcher to understand its applicability in smart grid application. Many researchers has worked in utilizing wireless communication for smart grid automation application that is explained in the following subsection.

1.3.1 Performance of LTE for Smart Grid Application

The author in [5] has investigated the performance of LTE in combination with IEC 61850 and MMS for smart grid automation application like Advanced Metering Infrastructure and remote communication application. Two set one for each application i.e. remote monitoring and smart
metering was studied. The simulation was verified to check the latency and priority requirement satisfaction in both the application.

The remote communication model was MMS client-server based that uses LTE for communication infrastructure. Additionally, MAC scheduling was used to prioritize the IEC packet. Two MAC scheduling mechanisms are supported; Round Robin (RR) and Priority-aware Round Robin (PrioRR). The smart metering application smart meter entity and MDMS Host entity. And also, only the RR MAC scheduler was used for the experiment.

The work was simulated using network simulator-3 (ns-3) tool. Various communication parameter like reliability, throughput, and latency was calculated to evaluate LTE performance for automation application. The result shows LTE satisfy the performance requirement for both the application. The simulation results indicated that LTE can be integrated with IEC 61850 MMS to satisfy the performance requirements on smart metering and remote control communication services in smart grid distribution networks.

1.3.2 Performance Evaluation of Smart Grid Communications via Network Simulation Version 3

In [6], the author has evaluated the performance Zigbee, Wi-Fi and LTE for smart grid communication between Data Concentrator Unit and Advance Metering Infrastructure (AMI). The investigation of smart grid communication between Data Concentrator Units (DCU)s and Advanced Metering Infrastructure (AMI) separates the simulation results into two sections. Firstly, the maximum distance for data transmission between DCU and AMI devices is compared to three wireless technologies. Secondly, the performance of ZigBee in different smart grid situations.

The authors describe smart grid technologies and communication frameworks such as DLMS/-COSEM which is a protocol that can be utilized as an interface to gather power consumption data between DCUs and AMIs. One of the interesting result presented in the paper was the coverage distance of all three communication protocol. LTE has 4 times better coverage distance than the other two wireless protocol (Wi-Fi and Zigbee).

1.3.3 Performance Evaluation of Cellular Communication System for Machine-to-Machine Smart Grid Application

The author in [7] has simulated the performance of GSM (2G), UMTS (3G) and LTE (4G) for Machine-to-Machine communication in smart grid application. The M2M communication setup used for the experiment make use of internet and cellular network for smart grid communication. The utilities in home make use of internet while the utilities far ahead uses the public internet to transmit and receive the packets.

The experiment measures different performance metrics like data rates, RTT and jitter to check the suitability of cellular communication for M2M smart grid communication. The paper concludes that LTE has the least latency of 70 ms which can be used for less demanding smart grid application.
1.3.4 Work Related to Routable GOOSE and SV Transmission

Other studies on LTE performance for smart grid application is mentioned in [8]. In this measurement, GOOSE and SV packet were encapsulated in IP packet using a specialize router. RTT was measured in the research work. The research work shows the RTT is less than 100 ms which could be useful for less time critical smart grid application.

The work in [9] shows the exchange of synchrophasor information between PMU. The work was implemented in a specialized library Khorjin which is used to receive and parse synchrophasor data from IEEE C37.118.2 based PMU/Phasor Data Concentrators, map it to the IEC 61850 data model and further transmit it as Routed- GOOSE (R-GOOSE) or Routed-Sample Value (R-SV) services.

The previous work in LTE as a smart grid communication solution shows LTE could play a vital role in smart grid communication extension. Most of the LTE performance related work is suitable for less time demanding application. Mapping of IP routable packet directly over the LTE network helps in reducing the latency and thereby increasing the scalability and reliability of the networking infrastructure. The performance evaluation of routable smart grid packet such as synchrophasor data over non-commercial LTE has never been done before. The main work of the thesis work is to benchmark LTE performance for directly mapped synchrophasor information based in IEC 61850-90-5 protocol.

1.4 Thesis outline

Chapter 2, provides the comprehensive background to understand the key concept explained in this thesis work. This chapter provides a short explanation about smart grid architecture, substation automation system, IEC 61850 and IEC 61850-90-5 protocol.

Chapter 3, defines and explains the different performance metrics used to benchmark wireless communication system are introduced and explained in this chapter.

Chapter 4, describes design, implementation and testing method of IEC 61850-90-5 in the targeted platform in combination with LTE network is explained.

Chapter 5, presents the result of the thesis work.

Chapter 6, discusses the finding of the work and the future work to enhance the performance.
This chapter presents background study on electric power system, smart grid technology and Substation Automation System. In addition to that it includes a detailed study of IEC 61850 standard and IEC 61850-90-5 standard.

2.1 Electric Power System

The electrical power industry has limited or no capacity to store the generated electricity [10]. Hence the generated power needs to be transported from the remote generation station to the end consumers. The electrical power industry deploys an electrical power system to transfer the generated powers. An electrical power system consists of electrical machines, lines, and way to transfer the power over a longer distance. It is also referred to as electrical grid or a power network [11].

The electric grid is a network of interconnected electrical equipment deployed to supply, transfer and use electrical power. An electrical grid is a complex system and is broadly divided into three major sub-systems as shown in the Figure 2.1:

- Generation subsystem
- Transmission subsystem
- Distribution subsystem
The generation subsystem consists of generators and steps up transformers. The generator is a 3-phase Alternating Current (AC) generator that generates the power and the step-up transformer converts power to high voltages. This high voltage power is fed on the transmission subsystem and transmitted over a long distance till the load center. At the load center, the voltage is stepped down and fed to the distribution system that distributes the electrical power to nearby residence and industries [13].

Challenges of Electric Power System

The consumption of electricity is steadily increasing over the past few years. EIA recently released International Energy Outlook 2013 project estimates the consumption of electricity would increase 56% by 2040 [14]. The present electrical structure has not been changed for over 100 years and is not suited to meet the need of 21st century [15]. It lacks automated analysis, high responsive mechanical switches, real-time analysis tools, etc [16].

Also the introduction of Distributed Generation which provides the flexibility to add renewable energy source at distribution level makes the grid structure more complex. The introduction of energy storage equipment at the different level in power grid makes it more and more dynamic. The market-driven requirement has increased the need for control and protection application for grid automation.

The introduction of SCADA [17] system which is an automated control and enhanced communication system helped to address some of its challenges. It provides the flexibility to monitor the behavior to track any major electrical disturbances in the grid network. It also ensures proper operation and security of the generation and the transmission system. But the distribution or the feeder network is still passive with little or limited control as shown in the Figure 2.2. This has been the major threat to the current grid structure and it requires an immediate attention. The next generation of power system, so called as Smart Grid helps in solving this problem and has revolutionized the way the electric power system has been realized in the past [16].

![Figure 2.2: Conventional Unidirectional Electric Power Grid System Architecture](image)

Page 6
2.2 Smart Grid Technology

The smart grid is a next-generation electric power grid structure that offers higher efficiency, better reliability and more secured energy transfer. It combines the energy generated from both renewable and alternative energy sources, using an automated control and modern communications technologies [19].

There is no single definition of smart grid technology. The European Technology Platform defines in [20] the Smart Grid as

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

2.2.1 Architecture of Smart Grid

Smart grid does not have a single architecture and most of the literature uses the NIST conceptual model architecture as defined in [21]. It divides the smart grids into seven major domains as: Customers, Markets, Service Providers, Operations, Bulk Generation, Transmission and Distribution. Each domain communicates securely with each other as shown by the solid lines in figure 2.3.

![Smart Grid Conceptual Model](image)

*Figure 2.3: Smart Grid Conceptual Model [21]*

Each domain has its own actors and applications. An actor is a device, system or a program...
that takes a decision of what information needs to be exchange to perform a particular application. While, applications are the task performed by one or more actor in a domain. To enable Smart Grid functionality, an actor in one domain particularly interact with an actor from the other domain.

The conceptual model is a high-level perspective of the smart grid. It is just a way to understand the operation of smart grid but does not provide any information on smart grid implementation.

2.2.2 Technology requirement for Smart Grids

To fulfill the requirements of smart grid, in [22] following technologies are introduced to be developed and implemented:

1. Information and Communication Technologies that include
   - The communication technologies like
     - 802 series like Ethernet LAN, Wireless LAN, WiMAX, etc.
     - Mobile Communication like 3G, LTE, etc.
     - Multi Protocol Label Switching
     - Power Line Communication
   - The information exchange technologies like
     - Standard for smart metering
     - Modbus
     - DNP3
     - IEC 61850

2. Sensing, measurement, control and automation technologies that include
   - Intelligent Electronic Device for advanced protection, measurement and event recording
   - Phasor Measurement Unit (PMU) and Wide Area Monitoring, Protection and Control (WAMPAC) for higher security
   - Integrated sensors, measurements, control and automation systems and information and communication technologies
   - Measuring technology like Synchrophasor

3. Power electronics and energy storage technologies that includes
   - High Voltage DC (HVDC) transmission and back-to-back schemes and Flexible AC Transmission Systems for long distance transport and integration of energy source
   - Different power electronic interfaces and power electronic supporting devices to provide efficient connection of renewable energy sources and energy storage devices

2.3 Substation Automation System

The electrical substation is a subsidiary station in an electric grid that is used for controlling, monitoring and protection of the power equipment [23]. According to [24] [25], an electrical substation is divided into 4 different types as:
1. **Switchyard substation** which is at the generating substation and connects the generator sub-system to the utility grid.

2. **Customer substation** that connects the power to different business application.

3. **System substation** that transforms the power across the network grid.

4. **Distribution substation** that transfers power from the transmission system to the distribution system of an area.

The substation is an important element of the modern power grid network [23]. It connects many systems. To ensure uninterrupted and smooth operation of the power network, different substation needs to share basic variable information like Bus voltages and frequencies, line loading, transformer loading, power factor, real and reactive power flow, temperature, etc. between each other. A Substation Automation System (SAS) process the information collected from different power equipments and perform the action accordingly. It controls, monitor and protect all devices in a substation [26].

The Substation Automation System connects and integrates the number of devices into a functional array for monitoring, controlling, and configuring the substation. Modern SAS structure has 3 basic level as shown in the figure 2.4:

![Image](image.png)

**Figure 2.4:** IEC 61850 based Substation Automation System Architecture [18]

The station level includes Human Machine Interaction , Station Computer, etc. and are located in a shielded control room. The bay level is the middle layer is located close to the switchgear. Bay level includes different protection and control IEDs (intelligent electrical devices). The equipments in between these 2 layers are often referred to as secondary equipment. Process level is the last level that interface the SAS and the switchgear. Switchyard equipment (also primary equipment) such as CTs/Power Transformers, remote I/O, actuators, merging units, etc. are included in this level [23] [26].
2.3.1 Communication in SAS

Communication plays a critical role in implementing an end-to-end and two-way open communication grid infrastructure in a real-time system such as power network [27]. Over 50 different communication protocols like DNP3, LON, EthernetIP, OPC-DA, etc have been used in the past and present. The Communication standard is based on communication architecture in an SA system. It defines the way of encoding, decoding and sharing the electrical parameters between the control centers, IEDs and other communication equipment. The communication standard usually consists of a data link protocol, physical layer protocol with one or more application layer protocol running on top of TCP/IP.

The selection of communication protocol is based on the bandwidth, reliability and latency requirement of the link. The author in paper [23] categories these communication protocols in 3 broad categories:

- Proprietary/vendor specification, e.g. UCA and DNP3, etc.
- National standard, e.g. IEEE 1613, etc.
- International standard, e.g. IEC 60870-5-101/104, IEC 60870-6-TASE.2, IEC 61850, etc

Most of these technologies were vendor specific and have low bandwidth, limited network devices applicability, serial interface, etc. Also, the communication model has limited to station and bay level communication as in case of DNP3 and IEC 60870-5-104 protocol. These protocols are not suited for corporate communication technology and are not able to expand the network reachability.

To address these issue, IEC introduced the IEC 61850 standard which is high-speed ethernet based standard. It is used for communication between all three level in all modern SA system as shown in figure 2.4. It defines two communication bus namely station and process bus for exchange of information. Station bus provides the communication link between station and bay level. Process bus exchanges the time-critical information between the bay and process level [23].

2.4 IEC 61850

IEC 61850 is a communication networks and systems standard for power utility automation. It is developed by IEC Technical Committee 57 Working Groups 10 [28]. IEC 61850 is based on the work by Utility Communication Architecture 2.0. It defines vendor independent communication standard for uninterrupted operation of different types IEDs that includes the breaker/switch IED, Merging Unit IED, and protection & control (P & C) IED [29]. The main aim of the standard was to create an international standard for communication within a substation. The main feature of this standards are:

- It defines a common naming conventional called as data model for easy information management in a substation.
- It provides Abstract Communication Service Interface that makes its application and database unchanged when communication and media changes.
- It standardize a Substation Configuration Language to describe the data model and configuration of IEDs from different vendors.
- It provides TCP/IP based communication model over an Ethernet.
- It defines two communication network bus (process and station bus) to minimize the hard-wiring within a substation.

### 2.4.1 IEC61850 Series Outline

The standard is divided into 10 parts as shown in the table 2.1.

<table>
<thead>
<tr>
<th>Series</th>
<th>Title</th>
<th>Edition</th>
<th>Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61850-1</td>
<td>Part 1: Communication networks and systems in substations - Introduction and overview</td>
<td>1</td>
<td>28-Apr-03</td>
</tr>
<tr>
<td>IEC 61850-2</td>
<td>Communication networks and systems in substations - Part 2: Glossary</td>
<td>1</td>
<td>07-Aug-08</td>
</tr>
<tr>
<td>IEC 61850-3</td>
<td>Communication networks and systems in substations - Part 3: General requirements</td>
<td>2</td>
<td>12-Dec-13</td>
</tr>
<tr>
<td>IEC 61850-4</td>
<td>Communication networks and systems in substations - Part 4: System and project management</td>
<td>2</td>
<td>11-Apr-11</td>
</tr>
<tr>
<td>IEC 61850-5</td>
<td>Communication networks and systems in substations - Part 5: Communication requirements for functions and device models</td>
<td>2</td>
<td>30-Jan-13</td>
</tr>
<tr>
<td>IEC 61850-6</td>
<td>Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs</td>
<td>2</td>
<td>17-Dec-09</td>
</tr>
<tr>
<td>IEC 61850-7</td>
<td>Communication networks and systems in substations - Basic communication structure principles and models</td>
<td>2</td>
<td>15-Jul-11</td>
</tr>
<tr>
<td>IEC 61850-7-1</td>
<td>Communication networks and systems in substations - Basic communication structure principles and models</td>
<td>2</td>
<td>24-Aug-10</td>
</tr>
<tr>
<td>IEC 61850-7-2</td>
<td>Abstract Communication Service Interface (ACSI)</td>
<td>2</td>
<td>16-Dec-10</td>
</tr>
<tr>
<td>IEC 61850-7-3</td>
<td>Common Data Classes</td>
<td>2</td>
<td>31-Mar-10</td>
</tr>
<tr>
<td>IEC 61850-7-4</td>
<td>Compatible Logical Node classes and data 2.0 classes</td>
<td>2</td>
<td>30-Oct-12</td>
</tr>
<tr>
<td>IEC 61850-7-10</td>
<td>Hydroelectric power plants - Communication 2.0 for monitoring and control</td>
<td>2</td>
<td>10-Mar-09</td>
</tr>
<tr>
<td>IEC 61850-7-420</td>
<td>Distributed energy logical nodes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>IEC 61850-8</td>
<td>Communication networks and systems in substations - Specific Communication Service Mapping (SCSM) Mapping to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3</td>
<td>2</td>
<td>17-Jun-11</td>
</tr>
<tr>
<td>IEC 61850-9</td>
<td>Communication networks and systems in substations - Specific Communication Service Mapping (SCSM)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 2.1: IEC 61850 series Outline

The first part of the IEC 61850 standard provides an introduction and a general overview of all 10 complete standards [28]. Part 3,4 and 5 describes the key communication requirements of IEC 61850 to be used within a substation. These requirements include identification of data & service model and underlying application, data link, network, transport and physical layer to meet the overall communication requirement [27].

Part 6 of the standard gives an overview of System Configuration Language (SCL). SCL is an XML based language used to configure the communication related parameter of different IEDs in a substation [30].

The data modeling aspect of IEC 61850 is defined in part 7 of the standard. IEC 61850 has an abstract object-oriented modeling structure which follows the hierarchy defined in part 7-2 [31] of the standard. The method to create the abstract data object and to map it to abstract services is defined in this standard. The abstraction of data object referred to as logical nodes is defined in part 7-4 [32]. All the data objects are further constructed using the common block called as Common Data Class. Part 7-3 [33] defines all the CDC. To extend its application to non substation automation, further standard in parts 7-410, 7-420 and 7-510 are defined.

Part 8-1 [34] defines the way of mapping abstract services and data to a real protocol such as Manufacturing Message Specification. Part 9-2 [35] defines Specific Communication Service Mapping for the transmission of sampled values between sensors and IEDs. The last part 10 defines the testing method to verify its conformance with various protocol defined in the document.

The first publication of the standard was released in 2003. The initial scope of the publication was communication within the substation. However, after the release, the applicability of IEC 61850 for nonsubstation related application was realized and was extended to other domains such as Distributed Energy Resource, Hydroelectric power plant, etc. This results in renaming the new standards as “Communication networks and systems for power utility automation” instead of “Communication networks and systems in substations” used in first editions.

The IEC standard is continuously updated. Few new standard is in the process of reviewing and editing before they are officially published. The new standard added after the first release are listed as the technical report in table 2.2.
Table 2.2: New Added Series of IEC 61850

Part 90-5, newly added standard in IEC series is used for wide-area transmission of synchrophasor information according to IEEE C37.118 for Wide-Area Monitoring, Protection and Controlling (WAMPAC) application [3]. The information is transmitted over a public network like cellular communication and is explained further in section 4.1.2.

### 2.4.2 IEC 61850 Data Modeling

The data from the devices are mapped into an abstract object-oriented data model following the modeling method defined in part 7 of the standard. The model follows a hierarchy and is application independent. It is divided into the various logic block called as devices, nodes, data class, and data.

- **Physical Device**
  Physical layer is the first layer in an IEC 61850 data model which include an intelligent device such as Intelligent Electronic Device (IED). It is connected to a network and is identified by its network address. Each physical device contains one or more logical node like breaker/control.

- **Logical Device**
  Logical device (LD) in [31] is defined as “entity that represents a set of typical substation functions”. The set of substation function includes performing power network function like measurement or protection. Every LD consists of one or more Logical Nodes (LN).

- **Logical Node**
  LN is the basic building block of the IEC data model. It is defined in [31] as “an entity that
represents a specific substation function. Each LN consists of one or more data elements. Part 7-4 categorize the 92 different logical nodes into 13 different main groups which represent the typical substation function. The naming convention of the LN is standardized and should always starts with the group it belongs to. For e.g. The LN “MMXU” starts with group indicator ’M’ which represents this LN is used for metering and measuring function.

- Data Class
  Each data element belongs to one of the CDC defined in part 7-3 of the standard. Each CDC follows a standardized naming conventional and defines the data type for that logical node. Additionally, it contains several individual attributes categorized based on their Functional Constraints (FC).
  For e.g. The LN XCBR includes “PoS” (Switch Position) as one of its data object from the simple CDC type DPC (Controllable Double Point).

- Data Attributes
  The data attributes represent the contains the actual data in binary form to be shared with other logical devices. For e.g. The ’PoS’ data class of DPC simple CDC has \(stVal, q\) and \(t\) as the data attributes.

![Figure 2.5: IEC 61850 based Data Model](image)

2.4.3 IEC 61850 Service and Data Mapping to Communication Protocols

The IEC 61850 built based on the Open Source Interconnect 7 layer model. The data services and application related to SA system is mapped to the top layer (application layer) of the OSI protocol stack as shown in the figure 2.6. This ensures the no change in the upper layer protocol with the development of lower underlying layer with the communication standard.
The Abstract Communication Service Interface (ACSI) defined in part 7-2 of the standard is a physical device that provides abstract communication services such as connection, variable access, unsolicited data transfer, device control and file transfer services, independent of the actual communication stack and profiles used [36]. These communication services must be mapped to a real protocol such as Manufacturing Message Specification (MMS) in an SA system. IEC 61850 defines a Specific Communication Service Mapping (SCSM) to map ACSI models onto real protocols. SCSM is a set of standardized rule that provides the concrete mapping of ACSI services and objects onto a particular communication protocol stack [37] as shown in the figure 2.6. Part 8-1 and 9-2 defines SCSM mapping of GOOSE and SV respectively.

2.4.4 Generic Object Oriented Substation Event

The IEC 61850 defines two different class of communication model to be used for communication within the Substation Automation System (SAS) namely:

- Client/server communication model used for reporting and remote switching application
- peer-peer communication model for Generic Substation Event and SV services

The GSE provides fast and reliable communication model for the exchange of input and output data values. It make use of publisher/subscriber model to distribute the generic substation event information among various physical device using multicast and broadcast services. Part 7-2 of IEC 61850 defines two classes of control messages.

1. Generic Object Oriented Substation Event message format that are used for the exchange of a wide range of possible common data organized by a data-set
2. Generic Substation State Event message format that are used to convey state change information in bit pairs
The IEC 61850 GOOSE/GSSE replaces the hard-wired binary signaling with ethernet bases station bus. All of the hard-wiring needed for status signals can be replaced by a single Ethernet connection between IEDs. The transfer to control message like a trip or a break status can using GOOSE/GSE message is really fast and is typically in the range of 3-10ms.

2.4.5 Sample Value

Sample Value (SV) is used for the transmission of the synchronized stream of current and voltage value. It is transmitted over Ethernet providing fast and cyclic exchange of measured current and voltage values replacing the traditional analog wiring. Special attention is required to choose the sample rate for the transmission of SV in a time-controlled way. This is required to minimize the combined jitter of sampling and transmission. For e.g. the Busbar voltage used to trigger protection relays is measured at 4000 samples/s and transmitted cyclically at 1 kHz [38].

It is also based on a publisher/subscriber mechanism. There are two model defined in IEC 61850-7-2 to exchange SV between the publisher and one or more subscriber:

1. Multicast-application-association
2. Two-party-application-association

2.5 Synchrophasor Technology

Synchronized phasor measurement of voltage and current plays an important role in the smooth functioning of the todays smart grid structure. Phasor measurement, when measured simultaneously and synchronized with a precise timing clock, is called as synchrophasor measurement.

A Sinusoidal wave is used to represent a signal in power system analysis and is represented using the Equation 2.1

\[ X = X_m \sin(\omega t + \phi) \] (2.1)

It is represented in phasor form by Equation 2.2

\[ x(t) = (\frac{X_m}{\sqrt{2}})e^{j\phi} = (\frac{X_m}{\sqrt{2}})(\sin \phi + j \cos \phi) = X_r + jX_i \] (2.2)

where \( \frac{X_m}{\sqrt{2}} \) represents the amplitude of phasor in root mean square (RMS) value and r and j are the real and imaginary part in a rectangular co-ordinate system. The value X in Equation 2.2 represents the synchrophasor representation of the signal x(t) in Equation 2.1 and \( \phi \) is the instantaneous phase angle relative to a cosine function at the nominal system frequency synchronized to UTC time.

Phasor Measurement Unit is used to measure the synchrophasor values. Modern PMU are capable of measuring the frequency and Rate Of Change Of Frequency which given by Equation 2.3 and Equation 2.4 respectively.

\[ x(t) = X_m \cos[\Psi(t)] \] (2.3)
\[ ROCOF(t) = \frac{df(t)}{dt} \] (2.4)

where,

\[ f(t) = \frac{1}{2\pi} \frac{d\Psi(t)}{dt} \]

The IEEE first standardized the synchrophasor measurement as IEEE 1344 standard and was reaffirmed in 2001. Later in 2005, to deal with the PMU measurement issue, IEEE released a complete new revised standard in the name IEEE C37.118-2005 – IEEE Standard for Synchrophasor Measurements for Power Systems. The specification includes the standard to measure, quantify, test and certify the accuracy of the transmitted data used for real-time data communication [39]. The standard didn’t have the complete list of factors a PMU can detect in a power system. Hence, it was split into two parts in 2011:

1. **C37.118-1**
   This standard deals with phasor estimation and measurement system. It defines the method to measure Synchrophasors, Frequency, and Rate of change of frequency (ROCOF) in all operating condition [1].

2. **C37.118-2**
   This standard deals with the real-time exchange of synchrophasor measurement between different entities in a power system. It defines different data types and message type. In addition, it also introduced two classifications of PMU, M - measurement & P - protection [2].

### 2.6 TR IEC 61850-90-5

Synchrophasor measurement and calculation done by PMU are useful in estimating the condition of the electrical power network and preventing big electrical disturbances. The measurement and transmission method of this useful synchrophasor information is defined in IEEE C37.118.1 and IEEE C37.118.2 respectively. IEEE C37.118 has certain limitation which are

- Security concerning the transmission of synchrophasor information is not well defined in the standard
- The dataset naming in the standard is not standardized and hence the inter-operability between the devices from different vendors is the biggest drawback of the IEEE C37.118 standard
- The dataset configuration tool defined in the standard is vendor specific.
- No mechanism is defined in the standard to transmit the same message to more client in a multicast domain.
IEC 61850 helps in filling the gap observed in C37.118 with system independent, better security and standardized data modeling and configuration approach. Hence a completely new communication mechanism has to be proposed to transmit the synchrophasor measurement in compliance with IEC 61850 standard. IEC in 2012 released a new technical report in the name of "Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118" to solve this problem. TR IEC 61850-90-5 specifies the communication mechanism for the exchange of time synchronized power measurement over wide area networks based on the IEC 61850 format [3]. It defines the synchrophasor data exchange mechanism between:

- Phasor Measurement Units (PMU)s
- Phasor Data Concentrators (PDC)s
- Between control center applications
- Wide Area Monitoring, Protection, and Control (WAMPAC)

The IEC 61850-90-5 standard also provides a way to route the IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sample Value packets. These packets can be used to transport synchrophasor information as well as general IEC 61850 data. Internet Protocol along with Transmission Control Protocol (TCP) or User Datagram Protocol is used to transport the synchrophasor information as shown in the Figure 2.7. Hence the message format are called as Routed- Generic Object Oriented Substation Event and Routed- Sample Value.

![Figure 2.7: Mapping of Synchrophasor Information in 90-5](image)

IEC 61850-90-5 provides enhanced security for IP packet using the Secured Hash Algorithm-2 (SHA-2) algorithm for message integrity and Advanced Encryption Standard for encryption. Encryption is optional. Both asymmetric and symmetric key pair is used for hashing function. The key management system based on RFC 3547 - Group Domain of Interpretation is implemented to exchange the hash key to both publisher and subscriber. The different security option available in IEC 61850-90-5 is shown in the Table 2.3.

In the table 2.3 Message Authentication Code (MAC) -None is provided for testing.

### 2.6.1 Data Modeling in IEC 61850-90-5

To model a system in IEC 61850, both client and server shall be modeled as logical nodes on some IEDs. A PMU in IEC 61850-90-5 is a logical device which has one or more logical nodes depending on its use for the particular application. Classical logical node and its data objects defined in part 7 of IEC 61850 as well as some new logical nodes and data objects are used to model IEEE C37.118.2 PMU in 90-5 compliance. For e.g. one or more instances of classical logical node MMXU is used.
<table>
<thead>
<tr>
<th>HMAC algorithm</th>
<th>Number of bits</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>MAC-None</td>
</tr>
<tr>
<td>SHA-256</td>
<td>80</td>
<td>HMAC-SHA256-80</td>
</tr>
<tr>
<td>SHA-256</td>
<td>128</td>
<td>HMAC-SHA256-128</td>
</tr>
<tr>
<td>SHA-256</td>
<td>256</td>
<td>HMAC-SHA256-256</td>
</tr>
<tr>
<td>AES-GMAC</td>
<td>64</td>
<td>AES-GMAC-64</td>
</tr>
<tr>
<td>AES-GMAC</td>
<td>128</td>
<td>AES-GMAC-128</td>
</tr>
</tbody>
</table>

Table 2.3: Different Security Option in 90-5

for publishing phase currents and voltage value and one or more instances of classical logical node MSQI is used for publishing sequence current and voltage value.

IEEE C37.118.2 PMU is capable of measuring synchrophasor, frequency, and ROCOF value. Hence a new data object HzRte is added to MMXU logical node to exchange the ROCOF value. In addition to that information regarding the status of PMU is transmitted using the common data class named “PhyHealth” in an instance of LPHD Logical Node as shown in the Figure 2.8

2.6.2 Communication Scheme

IEC61850-90-5 shall be used as the primary protocol for synchrophasor data exchange for WAMPAC (Wide Area Monitoring, Protection, and Control) application. The synchrophasor measurement and calculation can be exchanged within and outside the substation using SV while additional event status data can be communicated using the GOOSE or reporting considering the time criticality of the situation. The information can be exchanged using any of the two communication scheme defined in [3]

- **Direct connection with Tunelling**
  In this communication scheme, SV and GOOSE message are tunnelled across the high speed connection like Synchronous Optical Networking or Synchronous Digital Hierarchy.

- **The Gateway Approach**
  In this communication scheme SV and GOOSE message are communicated in an IP public network.

The use of communication scheme for synchrophasor data exchange depends on the applications they serve. The first option is a good option for shorter distance communication and hence the second one is preferred over it which serves for both long and short distance communication. In this approach, messages are encapsulated in an IP based protocol which can transverse to a longer distance and multiple stages of networking equipment. The enhance mapping of SV and GOOSE to support the gateway approach is shown in the Figure 2.9
Figure 2.8: PMU data Modeling
As can be seen in Figure 2.9, the synchrophasor data is encapsulated in IP based protocol using UDP as transport layer protocol. Since it uses the IP network, the data can be multicasted using some IP multicast protocol like Internet Group Management Protocol version 3. The SV and GOOSE data are transmitted as a routable data and hence in 90-5, they are called as Routed-SV (R-SV) and Routed-GOOSE (R-GOOSE).

### 2.6.3 IEC 61850-90-5 services

Section 6 of IEEE C37.118.2 define four different messaging frame for communicating synchrophasor information which are:

- Header frame
- Configuration frame
- Command frame
- Data frame

These frame are translated as services in 90-5. The functionality of command frame is implemented in 90-5 using the two control block namely Routed Multicast Sample Value Control Block and Routed- GOOSE Control Block and is explained in the Table 2.4.

All the configuration in IEC 61850 is configured through the SCL file and there is no need for an extra configuration frame. The data frame in C37.118.2 is used to transfer the synchrophasor information and is defined by the following four different services in IEC 61850-90-5:

- Routed Sampled Value service
- Routed GOOSE service
- Tunneled GOOSE or Sampled Value service
- Management service
### Table 2.4: IEEE C37.118.2 Command Frame Equivalent in IEC 61850-90-5

<table>
<thead>
<tr>
<th>Command</th>
<th>Definition C37.118.2</th>
<th>Equivalent IEC 61850 service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Turn off transmission of frames</td>
<td>Disable SVCB (set SvEna in SVCB to False)</td>
</tr>
<tr>
<td>2</td>
<td>Turn on transmission of frames</td>
<td>Enable SVCB (set SvEna in SVCB to True)</td>
</tr>
<tr>
<td>3</td>
<td>Send header</td>
<td>Read information for FC “DC” and read SvCB (</td>
</tr>
<tr>
<td>4</td>
<td>Send CFG-1 information</td>
<td>Obtain data model of PMU related function</td>
</tr>
<tr>
<td>5</td>
<td>Send CFG-2 information</td>
<td>Read actual measurements from data model (MMXU, etc.)</td>
</tr>
<tr>
<td>8</td>
<td>Extended frame</td>
<td>Out-of-scope</td>
</tr>
</tbody>
</table>

Among the 4 different data service, only R-SV services were implemented and tested in the public network. The implementation includes the function to exchange the R-GOOSE services as well but the communication performance of that services was not considered due to resource limitation and was kept as a future work.

### 2.6.4 Routed-Sample Value Profile Mapping

R-SV is used for the exchange of synchrophasor information. R-SV service is based on IEC 61850-9-2 standard in addition to the new session layer over the protocol stack as seen in the Figure 2.10.

As can be seen from the Figure 2.10, the 7-layer OSI model is divided into Application Profile and Transport Profile. The upper 3 layer of OSI model is called as A-profile and the bottom 4 layer falls under T-profile. The A-profile and T-profile of R-SV are explained in the following section.

#### 2.6.4.1 Route-SV A-Profile

The A-Profile is used to transport R-SV APDUs, as defined in IEC 61850-9-2 over an IP based network in a secure manner. In order to transfer synchrophasor information, the notation of absolute time and quality for each dataset in introduced in R-SV control block (R-MSVCB). Also, a new session layer is introduced in IEC 61850-90-5 to support the transmission in an IP network.

**Session Layer**

The packets generated from session layer are called as Session Protocol Data Unit and are fed to the transport layer as Transport Session Data Unit. The general construction of IEC 61850-90-5 SPDU is shown in Figure 2.11.

As can be seen in the Figure 2.11, each SPDU starts with a single-byte Session Identifier (SI) that identifies the APDU type, for e.g. for R-SV, the value is set to be 0xA2 in hexadecimal. The single-byte SI is followed by a Length Identifier (LI) that indicates the total length of Application Protocol Data Unit. The LI is followed by a common header whose value is set to zero (0x80 in hexadecimal).

The R-SV session layer is divided into following 3 subsection as shown in the Figure 2.12:
Figure 2.10: IEC 61850-90-5 Routed-Sample Value (R-SV) OSI Model

Figure 2.11: General Byte Ordering of IEC 61850-90-5 Session Protocol [3]
1. Header
2. User data
3. Signature

The header has the following sequence of information:

- **SPDU Length**
  It is a 4-byte unsigned integer that represents the total length of the SPDU. The maximum value of SPDU length is 65,517 octets.

- **SPDU Number**
  It is a 4-byte unsigned integer to detect duplicate or out-of-order packet delivery. Its value range from 0 to 4,294,967,295. It is maintained by a sender on a destination basic and is incremented whenever a packet is sent to the destination address. When the maximum value is reached, the value is reset to zero.

- **Version**
  It is a 2-byte unsigned integer that represents the protocol version number as specified by the standard. The value specified in the standard is 1.

- **TimeofCurrentKey**
  It is a 4-byte unsigned integer that represent the SecondsSinceEpoch value. SecondSinceEpoch shall be the interval in seconds counted continuously since the epoch 1970-01-01 00:00:00 Coordinated Universal Time. The value shall not be adjusted for leap seconds.

- **TimetoNextKey**
  It is a 2-byte signed integer that represents the number of minutes remaining to use the new key.

- **SecurityAlgorithms**
  It is a 2-byte field representing the encryption and HMAC algorithm type used. The most significant byte is used to indicate the type of encryption while the least significant byte indicated the type of the HMAC used in the packet.

- **Key ID**
  The 4-byte number is used as a reference to the key that is in use. This value is assigned by KDC.

The user data consists of two length and payload field:

- **Length**
  The length is a 4-byte unsigned integer. The maximum size of the length is based on the SPDU length and its value cannot be larger than the

  SPDU Length – 14 – Signature Size

- **Payload**
  The payload payload starts with the common payload attributes:

  - **Payload type**
    This attribute is used to identify the type of PDU. The hexadecimal values for R-SV data type is 0x82.
Figure 2.12: IEC 61850-90-5 A-Profile [9]
- **Simulation**
  It is a single byte boolean attribute to indicate if the payload is sent for test or not.

- **APPID**
  It is a 2-byte value as defined in 61850-90-2.

- **APDU Length**
  It is a 2-byte unsigned integer used to indicate the total length of Application PDU (APDU).

- **R-SV APDU**
  The payload length is followed with R-SV APDU explained in the next section.

The signature field starts with 1-byte tag and its hexadecimal value is 0x85. The tag is followed by 1-byte length field that indicated the total length of HMAC value. The final octet contains the final HMAC value as calculated by the algorithm mentioned in the security algorithm field.

**R-SV ASDU**

The SV ASDU is explained in detail in IEC 61850-9-2 and is called as savPdu. The savPdu is encoded based on ASN.1 Basic Encoding Rule (BER).

**ASN.1 Basic Encoding Rule**

Abstract Syntax Notation One (ASN.1) is a notation used to describe the message that can be transmitted and received in a network [40]. It is divided into two part:

- The first part specifies the syntax for describing the content of a message in data type and content sequence format. It is defined in ISO 8824/ITU X.208 standard.

- The second part specifies the basic encoding rules for encoding each data item in a message. The encoding standard is defined in ISO 8824/ITU X.209 standard.

There are set of encoding rules defined in ISO 8824/ITU X.209 and sample Value is encoded based on Basic Encoding Rule (BER). BER encodes abstract information into a concrete data stream. The principle of BER standard is to encode each message in a TLV triplet structure, where T represents Tag, L represents Length and V represents Value as shown in the Figure 2.13.

![Figure 2.13: Basic Encoding Rule](image)

- **Tag**
  The tag is a 1-byte information that indicate the type of message encoded.
• **Length**
The length is 1-byte in length which represent the length of data in Value field.

• **Value**
The value contains the actual data. The value can contain several other data coded in form of other TLVs as can be seen in the Figure 2.13.

The sample value starts with a tag 0x60 hexadecimal value followed by the length of the total PDU as can be seen in the Figure 2.14. The length is followed by the sequence of following attributes:

![ASN.1 BER Encoded Sample Value data format](image)

Figure 2.14: ASN.1 BER Encoded Sample Value data format

- **noASDU**
  It indicates the number of Sample Value ASDU contains in an SV packet. The tag associated with this attribute is 0x80.

- **Security**
  The security field is optional and is associated with a tag 0x81.

- **Sequence of ASDUs**
  All ASDUs concatenated in a SV packet are associated with a tag 0x60. The tag is followed by the length. The value field of this attribute has the series of ASDU data as can be seen in the Figure 2.14. Each ASDU has the series of the following data:

  - **svID (Sample Value Identifier)**
    It is a visible string of maximum 129 octets that indicates unique identification of the sampled value. It is associated with a 0x80 tag.
- **datset**
  The DatSet attribute specify the reference of the data-set of the transmitted MSVCB message. The Tag associated with datSet is set to 0x81.

- **smpCnt**
  The smpCnt attribute is a 2-byte unsigned integer containing the sample count value which will be incremented every time a new sample value is taken. The tag associated with this attribute is 0x82.

- **ConfRev (Configuration Revision)**
  The ConfRev attribute is a 4-byte unsigned integer containing counts of the number of times the configuration with regard to the SVCB (Sample Value Control Block) has been changed. The counter shall be incremented when the configuration changes. The Tag associated with ConfRev is set to 0x83.

- **refrTm**
  The refrTm is an 8-byte optional field that indicates the TIMESTAMP of the refresh time of the SV Buffer. It is associated with 0x84 tag.

- **smpSynch**
  It is a boolean value which indicates if the SV is synchronized by a clock signal or not. It is associated with a tag of 0x85.

- **SmpRate**
  It is a 2-byte unsigned integer containing the sample rate value. The Tag associated with SmpRate is set to 0x86.

- **Sample**
  The sample attribute starts with 0x87 tag and its value contains the member of data set that is to be transmitted.

### 2.6.4.2 Routed-SV T-Profile

The T-profile used for the transmission of SV packet is specified in IEC 61850-9-2. To transport the Routed-SV in a public network, UDP/IP protocol is used as shown in the Figure 2.15.
Figure 2.15: IEC 61850-90-5 T-Profile [9]
3 | Wireless Communication Performance Metrics

This chapter provides an introduction to wireless communication, communication requirement for IEC 61850-90-5 application and a detailed explanation of parameter used to benchmark LTE system for the 90-5 application.

3.1 Wireless Communication

Wireless communication has transformed rapidly over the years. The technological innovation from the first generation (1G) to fourth generation (4G) has increased bandwidth, coverage, and capacity of wireless communication significantly while reducing the latency to few milliseconds [41]. The technological advancement has widened its application. At present wireless communication is used to transfer data in almost all major industries that include medical, transport, university, military, etc. The standardization of WLAN, LTE, and Wi-Max technologies has increased its dominance in an industrial application during the past 10 years [42].

3.1.1 Long Term Evolution

LTE is a high-speed wireless communication system and is the evolution of GSM/WCDMA core network. LTE is a 4G communication technology standardized by 3rd Generation Partnership Project (3GPP) in release 8. To support high-speed data connectivity and mobility, it uses Orthogonal Frequency Division Multiplexing as its radio access technology for downlink traffic and Single Carrier Frequency Division Multiple Access for uplink traffic. LTE features advanced antenna technologies such as Multiple-Input Multiple-Output.

LTE is an all IP packet-switched based network and offers low latency both in user and control plane. The architecture is based on Long Term Evolution -System Architecture Evolution with new Evolved Packer Core as its core network. The new EPC network is optimized for better network performance, cost-efficiency and facilitate the uptake of mass-market multimedia traffic [43].

LTE technology is continuously evolving to improve network performance, flexibility and reduce latency. LTE-Advanced which features fast switching for direct device-device communication in case of emergency, carrier aggregation to increase the data transmission rate are some of the key innovation in the current LTE world. The data throughput with LTE-Advanced is theoretically around 1 Gbps in downlink and 500 Mbps in Uplink [44]. This key development has always fascinated researcher to utilize LTE for the different application.
3.1.2 Communication Requirement in IEC 61850-90-5

Wireless communication provides the high level of flexibility and scalability with low deployment cost compared to other fast data rate technologies like Optical communication. For wireless communication to be acceptable in smart grid automation, it has to fulfill the critical requirements related to latency, reliability, availability and data rates of different power grid application. The severity of the requirement varies from application to application and there could be an additional requirement related to redundancy, time synchronization, security, and coverage.

There are several long and short-range wireless technologies available but LTE can play a key role in replacing the currently deployed communication technologies in the smart grid. LTE provides high data rate, low latency, high availability and enhanced security. LTE also features different Quality-of-service (QoS) based on application criticality that can be useful in reducing the transfer time in smart grid application.

The Communication requirement in smart grid application is application dependent and varies from one application to another. This requirement includes transmission rate, delay in measurement and transmission of data, reliability at which the packets are delivered and the availability of the network for transmission. These parameters are critical in benchmarking the performance of a protocol in a public wireless infrastructure. LTE is an all IP-network which guarantees high reliability, high data throughput and low latency, and following parameter are measured to benchmark its applicability for the transmission of synchrophasor information:

- Network Throughput
- Latency or Transfer time
- Reliability or packet delivery ratio
- Availability

The time-critical application considered in the thesis work requires latency below 30ms, a reliability of 99.99%, 100-200 pps transmission rate and less failure rate.

3.1.2.1 Network Throughput

Network throughput in a communication network is the measure of the rate of successfully delivered message over the communication channel. In other words, it is a measure of the number of packets successfully transmitted per second in a given networking infrastructure. Throughput is usually measured in bits per second, and sometimes in data packet per second [45].

The throughput in a given network is given by Equation 3.1.

\[
\text{Throughput} = \frac{\text{Total number of packet successfully delivered}}{\text{Total time interval}}
\] (3.1)

Network throughput is the measure of amount of information or message can be processed by a system in the given time interval. Throughput helps in measuring the system efficiency and sometime is useful in calculating the channel utilization. Throughput is affected by many factor like load in a given system, interface due to other signal, radio resource allocation, etc.
In smart grid automation application, huge amount of data has to be processed in a minimal time and hence the throughput should be significantly higher. Non-commercial LTE offers high bandwidth to transmit data from multiple users or device. This parameter is measured during the thesis work to understand channel utilization of the given non-commercial LTE infrastructure. Also, it helps in measuring the rate at which the data is processed.

### 3.1.2.2 Latency or Transfer time

Latency is the total time a packet takes to get from source to destination. Latency is an important parameter in understanding the total delay a packet may suffer when traversing through the various networking equipment. Latency involves transmission, processing and propagation delay. These delays in a network effects the performance in a communication system [46].

Delay in a network can be measured either as one-way delay (message transmission time from source to destination) or as Round-Trip-Time delay (transmission time from source to destination and back to the source). Smart grid automation application desires low latency which ranged from 5 to 100 ms depending on the application its serves while time critical application requires latency mostly below 30ms [47]. LTE provides low latency to high critical message and can serve a key communication enabler in smart grid application.

In general, latency is given by the Equation 3.2 provided both the receiving and transmitting node synchronized to same time source.

\[
\text{Latency} = T_{rx} - T_{tx} \tag{3.2}
\]

where,

- \( T_{rx} \) = Time at which the packet is received at the receiving node
- \( T_{tx} \) = Time at which the packet is sent by the transmitting node

IEC 61850-5 defines latency as the transfer time which is defined as the complete transmission time of a data packet including the processing time at both sender and receiver end. The time begins from the moment sender puts the application data content on top of its transmission stack (coding and sending) till the moment receiver extracts the data from its transmission stack (receiving and decoding). Furthermore, IEC 61850-5 defines six message types depending on its usage. These message types are:

- Type 1 - Fast messages
- Type 2 - Medium speed messages
- Type 3 - Low speed messages
- Type 4 - Raw Speed messages
- Type 5 - File Transfer functions
- Type 6 - Command messages and file transfer with access control

Synchrophasor information is the continuous stream of voltage and current measured at a clock signal. These message type falls under Type 4 - Raw speed message. These message needs to have
a constant delay and its transfer time or transmission delay falls in the range of 10-30ms.

IEC 61850-90-5 is used for WAMPAC application where the synchrophasor information has to shared between different substation as shown in the Figure 3.1.

![Figure 3.1: Transfer time for WMAPAC application [48]](image)

The transfer time in this case is given by the equation 3.3:

\[ \text{TransferTime} = t_a + t_{b1} + t_{a1} + t_{b0} + t_{c2} + t_{b2} + t_c \]  

(3.3)

### 3.1.2.3 Reliability

Reliability is the probability of success or the probability that the system will perform its intended function under specified design limits [49]. It is measured based on a total number of packet successfully delivered against the total number of packets transmitted. Theoretically, it is the measure of the rate of success. Reliability is an important communication parameter to understand the dependability of a given system. Reliability is mostly affected by the loss of the packet in a network. Packet loss in a network could be because of numerous reason which includes congestion in a network, no network availability, network failure, etc.

In general, reliability is measured in percentage and is given by the Equation 3.4

\[ \text{Reliability} = \frac{\text{Total no. of Received Packet for some T time}}{\text{Total no. of Transmitted Packet during the same time}} \times 100\% \]  

(3.4)

Reliability helps in analyzing the networking condition. This is very useful information in analyzing the applicability of a given communication infrastructure for a given system. Time-critical application requires highly reliable system. Higher reliability is desirable for proper and efficient operation of time-critical application. Missing of information can affect the system performance.
to predict electrical disturbance. In smart grid automation system, an IED requires around 200 packets per second to interpolate the system condition and predict if there is any fault in the transmission system.

In smart grid automation, the devices exchange message or information continuously and are very sensitive to loss of information. The reliability requirement for smart grid application is 99.99% which means the system can tolerate only 1 packet loss in every 10000 packet it sends. Communication network reliability is only measured during the thesis work.

### 3.1.2.4 Availability

Availability is the probabilistic measurement to check if a system is operational at a certain point in time [50]. Availability depends on two factors:

- Failure rate of the elements
- Repair rate of the elements

The former can be improved through better elements quality, condition monitoring, and redundancy while the latter depends on the maintenance strategy of the operator [48].

During normal operation, the devices exchange message continuously for a longer period of time and availability calculation of communication network is important to understand the failure rate and up time of the entire networking system. If we define the status function \( X(t) = 1 \) for any time \( t > 0 \), then the availability at a given time ‘t’ of the communication system is given by Equation 3.5 [50].

\[
Availability(t) = Pr[X(t) = 1]
\]  

Availability measurement of a system is the measurement of reliability at a given point of time. Reliability is dependent on availability. Hence to have a better reliability in a system, the network should availability all time. This, in turn means the network should have a very low failure rate and in case of failure, the network should have an efficient redundant implementation.

During the thesis work, availability parameter was used to measure the robustness of the communication network. It is also useful in measuring the device failure rate of a network and also the level of redundant implementation in case of failure. LTE network is highly susceptible to devise failure and is always deployed with a redundant path to compensate for the failure. This parameter was used to measure the robustness of LTE network and find its suitability for synchrophasor information transmission application.
4 | Implementation And Testing

As mentioned in Chapter 1, the work is divided into two major tasks: Design & Implementation of IEC 61850-90-5 protocol stack, and testing its performance over the non-commercial LTE network.

The first section covers the design and implementation of IEC 61850-90-5 protocol stack on the targeted machine. It includes the contribution done to develop the complete 90-5 protocol stack. The information contained in encoded synchrophasor message is explained in detail in this subsection. Also, it gives an introduction to timestamping type used to timestamp the data.

The later section presents the test setup, test control flow, and test cases. Different test cases used to measure availability, reliability, throughput, and latency are explained in detail in this chapter.

4.1 Design and Implementation of IEC 61850-90-5 Protocol Stack

The protocol stack was designed to exchange synchrophasor data between two machines based on a client-server model. The packets were encoded and transmitted in a UDP/IP network at the server side. The transmitted data was received, decoded and analyzed at the client side. The development work also includes the addition of a function to keep track of transmission information, to facilitate the measurement of key communication parameter mentioned in section 3.1.2.

The 90-5 protocol stack was started from an open source code from site [51]. The open source code was started by System Integration Specialist Company and is the platform where many developers have collaborated and contributed to the development of 90-5 protocol stack. The open source code was provided by ABB and is licensed under the Apache License, Version 2.0. It has the basic interface and function definition to transmit the data between the machines.

The protocol stack source code was written in C language. C language because it is very powerful, rich in the library and most importantly has less processing delay than any other high-level language. The development was performed in Microsoft Visual Studio IDE in windows platform. Microsoft Visual Studio was used because it has some useful inbuilt function to measure the HMAC and time that were used for the development of protocol stack. Also, it has an easy method to translate the source code to a standalone application.

The final output of the development was a standalone application that accepts the configuration file (explained in 4.2.2.2) as an input from the directory mentioned in the source code and
generates an output which is a statistics file that contains required transmission information like transmitted, received, missing packets, etc.

The original source code was modified as per the project requirement and the major changes implemented in the code is illustrated below:

- The origin source code supports the encoding and decoding of R-SV information, but the data field was empty. The data to be send was analyzed and encoded in the data field of R-SV. Also, the decoded of encoded data was included on the client side. It is explained in details with an example in sub-subsection 4.1.2.

- Synchrophasor data needs to be timestamped while encoding. The original source code includes second accuracy time-stamping function. But for the measurement of latency parameter, time resolution up to few microsecond was required. For microsecond time resolution, windows inbuilt function was implemented in the original source code. The time-stamping with microsecond resolution was implemented as per IEC 61850 format which is explained in details in sub-subsection 4.1.3.

- The original source code supports encoding and decoding of R-SV information. Hence to extend the study for R-GOOSE information, R-GOOSE encoding and decoding functions were defined in the original source code.

- The major aim of the project was to measure the important communication metrics defined in subsection 3.1.2. Periodic update of packet size and transmission interval was required for in-depth analysis and measurement of the communication metrics. To facilitate the dynamic update of packet size and transmission interval, changes were done in the configuration file. The original source code was also changed accordingly to accept the changes.

- The output of the program is a statistics file which logs the data transmission information like transmitted, received, missing packets, etc. Major changes were done on the source code to track the transmission logs and extra counter were added in the original source code to facilitate the measurement of key communication parameters.

- Minor changes were done in the original source code to suit the implementation of the project on the targeted platform (windows). Some key functions and header were added in the project file.

4.1.1 IEC 61850-90-5 Standalone Application Control flow

The control flow of 90-5 application follows the following steps and is shown in Figure 4.1.

- The application starts by initializing internal storage for keys and payloads, KDC and IP interface stack.

- Encoding of Synchrophasor data and preparation of R-SV packet.

- The prepared R-SV is then transmitted to the receiver/client IP address over the UDP port specified in the source code. The destination UDP port used during the course of work was 102.

- The receiver/client at the other end continuously searches for the packet on the same UDP port and from server IP address. The client on reception of information checks for the security information and then decodes it.
Figure 4.1: Control Flow in Protocol Stack

- Transmitter
  - Initialise all the stack
  - Encoding of synchrophasor data
  - Encapsulating in Sample Value
  - Transmitting over UDP/IP Network

- Receiver
  - Initialise all the stack
  - Check for synchrophasor data in specified port number
    - Yes
      - Decode the data
    - No

LTE Network
4.1.2 Synchrophasor Data Encoding in R-SV packet

As explained in sub-subsection 2.6.4, the R-SV ASDUs are encoded in ASN.1 BER encoding format. Wireshark capture of the R-SV ASDUs is shown in Figure 4.2.

As can be seen in Figure 4.2, each field is encoded as Tag Length Value triplet. The samples field starts with a tag of 0x87 in hexadecimal followed by its length (0x3C in hexadecimal as shown in Figure 4.3). The value of the samples field includes the synchrophasor value and the capture of samples field and explanation can be seen in Figure 4.3.

As can be seen in Figure 4.3, all three phasor information is packed into a single R-SV ASDU and each synchrophasor value is represented as:

- A 2-byte integer number to represent the phase number
- The angle and magnitude of phasor information is 5 octets long each and is represented in floating point number representation
- The time-stamping is 8 octets long and is represented in IEC 61850 format

It should be noted that R-SV data set is not encoded in ASN.1 BER format. There is no tag and length associated with synchrophasor value. They are directly represented in their normal format. This is the main difference between the data-set representation in R-GOOSE and R-SV.
4.1.3 IEC 61850 Timestamping

The timestamp shall represent the UTC time since the epoch of midnight of 1970-01-01. Section 6.1.2.9 of IEC 61850-7-2 defines the timestamp type. This timestamp type is used to timestamp the synchrophasor data. The timestamp type consist of following three attributes:

- **SecondSinceEpoch**
  It is a 4-byte unsigned integer and shall represent the count of a number of seconds elapsed since epoch 1970-01-01 00:00:00 UTC.

- **FractionOfSecond**
  It is a 3-byte unsigned integer and shall represent the fraction of a second when the value of the TimeStamp has been determined. The resolution of time can be calculated using the Equation 4.1:

\[
Resolution = \sum_{i=0}^{23} b_i \times 2^{-(i+1)} s
\]  

(4.1)

where i represent the number of bits used to represent FractionOfSecond attribute. When all 3 bytes are used, the resolution is 60 nanosecond.

- **TimeQuality**
  the TimeQuality is a single byte long packed list that provide information about the time source quality. Its definition is shown in Table 4.1.
<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClockFailure</td>
<td>BOOLEAN</td>
<td></td>
</tr>
<tr>
<td>ClockNotSynchronized</td>
<td>BOOLEAN</td>
<td></td>
</tr>
<tr>
<td>TimeAccuracy</td>
<td>CODED ENUM</td>
<td>Number of significant bits in the FractionOfSecond: Minimum time interval shall be: $2^{-n}$</td>
</tr>
</tbody>
</table>

Table 4.1: Time Quality Definition

![Environmental setup](image)

Figure 4.4: Environmental setup

4.2 Test Methodology

The modified IEC 61850-90-5 protocol stack was used to test and benchmark its performance over a non-commercial LTE network. R-SV packets were exchanged between the machines and key communication parameter explained in sub-subsection 3.1.2 were measured to study the applicability of LTE for smart grid application.

4.2.1 Setup Overview

4.2.1.1 Environmental Setup

The standalone IEC 61850-90-5 application was run on two different machines that emulate two different IEDs. Both the machines were connected directly via Ethernet to two separate 4G LTE modems that had 100 Mbit/s downlink and 50 Mbit/s uplink capacity. The 4G LTE modem connects to base-station via air-interface. A Virtual Private Network (VPN) tunneling was used through the public network to connect the base station to the core network. The core network is located around 90 km from the base station (BS).

When a packet is transmitted, it returns back to another machine after traverse through core network shown in Figure 4.4.
Machine and LTE Modem Configuration

- Both machines were configured to have static IP in order to avoid change of IP addresses. Dynamic Host Configuration Protocol (DHCP) could be used but would require more configuration changes during the test runs.

- The machines were connected to different modems which were on different Local Area Networks (LAN)s and thus no direct communication could be reachable between the machines. Hence port forwarding functionality was enabled in both the LTE modem.

- To synchronize both the machine to the same time server, one machine was configured as NTP time server and other as NTP client.

4.2.1.2 Time Synchronization Setup

Synchrophasor data is the complex angle and magnitude value timestamped with the same timing source. Hence the machine used for synchrophasor data exchange has to be synced to the same timing source. Network Time Protocol (NTP) was used as a time synchronization protocol during the experiment. NTP is a time synchronization protocol used to synchronize network time between the machines. It is a client-server based model and utilizes UDP port number 123 for an exchange of time synchronization information between the machines.

Meinberg NTP packages were used to install NTP services and associated service in both the machines. Meinberg NTP packages because it is an open source binary file available freely on the internet and is easy to configure [52]. Time synchronization between the machines running IEC 61850-90-5 application is shown in Figure 4.5.

As can be seen in Figure 4.5, Machine 1 is synchronized to NTP server from the public Internet and machine 2 is synchronized to machine 1. The NTP package on machine 1 is synchronized to a highly accurate stratum 1 network time server like 0.se.pool.ntp.org. The NTP package in machine 2 is configured to get the time from machine 1 by embedding its IP address as a server address. This makes sure that both machines have the same time.

To increase the accuracy of the test, the offset and drift of both machines were measured using a command line application before the start of every test. This drift/offset was then used to compensate the latency calculations.

4.2.2 Test Model

In order to evaluate and benchmark the performance of non-commercial LTE, machines were configured based on client-server model. A point-to-point communication model was used to finish the work on time but the design process has the useful function and interfaces definition to support multicast communication.

4.2.2.1 Control Flow

The test model control flow is shown in Figure 4.6. Before the start of the application, key parameter like packet size, transmission interval, logging interval, etc. needs to set in the application. These were set using the configuration file explained in the next section.
Figure 4.5: Time synchronization setup

Figure 4.6: Test Model Control Flow
The application running on both the machine loads the configuration and start exchanging R-SV based on the configuration file feed to it. The application produces a statistics file as an output. The statistics file is a log file that has important transmission parameters used to measure the communication metrics. The results from both the statistics files were compared and the final compared result was plotted using MATLAB.

Additionally, packet sniffing tool like Wireshark was run on both the machine before the start of the program to capture all the packets received and transmitted from its interface. Wireshark with IEC 61850-90-5 extension provided with the open source project was used during the test. Wireshark was used to inspect the proper delivery of packets.

### 4.2.2.2 Configuration File

For the calculation of key communication metrics, the configuration file was used. It helps in dynamic and static updating of the application parameter. The sample configuration file is shown in Figure 4.7.

Some of the key parameter is explained below:

- **InterfaceID** – It is the Globally Unique IDentifier (GUID) of the interface used to transmit/receive data. During the experiment, the machine emulating an IED was directly connected to LTE modem via Ethernet. Hence, this parameter was fixed for the whole experiment.

- **SMVIP4Pub** – It was used to set the destination IP address on the application. Both the machines were communicating with port forwarding feature enabled in the LTE modem. Hence this parameter was filled with the IP address of the LTE modem connected to another machine.

- **StatResetMinute** – The value set for this parameter represents the time in minutes to reset the statistics file.

- **LogIntMin** – The value set for this parameter represent the time interval in minutes to populate the transmission information in the statistics file.
• **TransIntMsec** – The value set for this parameter represent the rate of transmission of data. For e.g., if it is set to 5 meaning application will transmit packet every 5 ms counting in total of 200 packets per second.

• **Ulong** – This parameter was used to dynamically update the packet size. The packet size was calculated using the Equation 4.2

\[
\text{Packet Size (in bytes)} = 289 + Ulong \times 8
\]  
(4.2)

### 4.2.3 Test Cases

A general test plan template was formed to test the transmission performance of R-SV over a non-commercial LTE infrastructure. Different test cases were derived to test different communication metrics introduced in 3.1.2. The test plan was based on the different behavior of packet size and the transmission interval. Each test case was run for different trials to get the closest expected measurement results.

During the test, parameters such as packet size (Ulong), transmission interval (TransIntMsec), logging interval (LogIntMin) and reset interval (StatResetMinute) were modulated as per the test requirements or test cases. StatResetMinute and LogIntMin parameter in configuration file was also dynamically update to facilitate the capture of correct information in the statistics file. All these parameters were updated using bat scripting.

#### 4.2.3.1 Test Case To Measure Throughput

Throughput test was conducted to measure the number of packets transmitted from source to destination every second. The test was further extended to study the effect of transmission throughput for different packet size and transmission interval combination. The throughput test plan is explained below:

• Ten different packet size ranging from 500 to 2400 bytes were considered for this test.

• Five different transmission interval ranging from 40 to 200 pps (packets per sec) was considered during the course of this test

• Each test combination was run for 3 trials and for a minute duration

The throughput Equation 3.1, was used to measure the throughput result.

#### 4.2.3.2 Test Case To Measure Latency

The latency test was conducted to check the transfer time of R-SV in a non-commercial LTE network. The latency test plan is explained below:

• Five different packet size ranging from 500 to 1500 bytes were considered for this test.

• Five different transmission interval ranging from 40 to 200 pps (packets per sec) was considered during the course of this test

• Each test combination was run for 3 trials and for 1-minute duration.
The latency Equation 3.2, was modified to measure the latency result and is shown by Equation 4.3:

$$Latency = (T_s - \Delta_s)(T_d - \Delta_d)$$  \hspace{1cm} (4.3)

where,
- $T_s$ and $T_d$ are the times where the packets are transmitted and received on the source and destination machines respectively
- $\Delta_s$ and $\Delta_d$ are the offset from the NTP server for the source and destination machine respectively

### 4.2.3.3 Test Case To Measure Reliability

The reliability test was carried to check the delivery rate of R-SV packet over a non-commercial LTE network. The reliability test plan is explained below:

- Only one packet size i.e. 537 bytes was considered for the test.
- The transmission interval was fixed to 2 msec i.e. 500 packet transmission every second.
- The LogIntMin was set to its lowest value i.e. 17 msec.
- Each test combination was run for 5 trials and for a duration of 1 minute

The reliability Equation 3.4, was modified to measure the reliability result and modified reliability equation is shown in Equation 4.4:

$$Reliability = \sum_{t=0}^{60000} \frac{R_x}{R_x + M_x}$$  \hspace{1cm} (4.4)

where,
- $R_x$ = Total number of received packet on the given machine
- $M_x$ = Total number of packet not received on the same machine
- $t$ = time interval in ms

### 4.2.3.4 Test Case To Measure Availability

Availability test was executed to check the readiness of the non-commercial LTE network. The availability test plan is explained below:

- Packet size 1237 bytes was considered for the test.
- The transmission interval was fixed to 1000 ms to limit the transmission of the packet to one per second.
- The LogIntMin was set to 5 to capture the transmission interval every 5 min.
- The test was run for longer duration of 24 hours and only 1 trail was run in total
The availability Equation 3.5, was modified to measure the availability result and the modified equation is shown in Equation 4.5:

\[
\text{Availability} = \frac{R_x}{R_x + M_x}
\]  

(4.5)

where,

\(R_x\) = Total number of received packet on the given machine for every 15-minute interval
\(M_x\) = Total number of packet not received on the same machine for every 15-minute interval

### 4.2.4 Data Analysis and Extraction

The size of the raw data from the test is approximately 45 Gigabyte. The raw data consists of Wireshark captures, time offset files and statistic files that were generated during the test runs. This result was used for plotting the graph results.

To extract the useful information, different bat script was written and was run. Bat script because the test was conducted in windows machine. Basically, two different bat scripts were created for data collection.

- Script to collect data for the availability measurements
- Script to collect data for latency, throughput and reliability measurements
5 | Result And Analysis

The following chapter presents the performance evaluation result of IEC 61850-90-5 protocol stack over a non-commercial LTE network. It includes the plot result for the different communication metrics throughput, reliability, latency, and availability measured during the course of thesis work.

5.1 Result

The measured result for availability, latency, throughput, and reliability was plotted in MATLAB program using Matlab scripts. MATLAB because it has rich in-built plot function to realize the result and also it has diverse file format to save the plot result. Based on the extracted information different MATLAB scripts were created to read the extracted file and plot accordingly.

5.1.1 Throughput

The throughput metrics was measured to analyze the rate at which the packets are being transmitted and received. It was tested for different packet size against the different transmission interval. The test was conducted for several trials and the final result was measured based on all the results average. The throughput plot for R-SV transmission is shown in Figure 5.1.

An interesting finding of the test was the decrease in overall throughput when the packet size is increased beyond 950 bytes which can be seen in Figure 5.1. The observed behavior was common for all the transmission interval and is more prominent when the number of packets transmitted every second is more i.e for transmission interval 5 and 10 ms. The throughput drop observed ranges from 15% for lower transmission interval 5ms to 5% for higher transmission interval of 25 ms.

The potential reason for this throughput drop may be due to the resource limitation in the core network or an issue with the network scheduler. Another potential reason may be due to packet segmentation i.e. splitting of larger packets. Splitting of larger packet into two increases the overhead, thereby reducing the throughput.

5.1.2 Latency

The latency metrics was the measure to understand the delay imposed on the packet by the non-commercial LTE network while traversing from source to destination. Figure 5.2 shows the average latency for different packet sizes and transmission intervals. This to examine if packets with less size traverse the network faster than bigger packets. The average latency observed was around 22 ms.
Figure 5.1: Throughput graph of different transmission intervals against different packet sizes

Figure 5.2: latency for different transmission interval and packet size
The average latency increases slightly with packet size. For e.g. For transmission interval of 10 ms, the average latency for 537 bytes the latency is around 17 ms and for packet size 1369 bytes is around 22 ms as can be seen in the latency graph. This trend is not uniform which is an unexpected behavior. Hence CDF was calculated for the latency test to analyze the trend. Figure 5.3 shows the Cumulative Distribution Function i.e. occurrence of a certain latency for different transmission intervals. CDF was measured by grouping the latency value of packet size and all its trial into a single transmission interval.

The CDF graph shows maximum latency observed was around 45 ms. The CDF characteristics of Transmission interval 10ms and 25ms shows a different behavior than other 3 transmission interval. On analyzing the results, it was found transmission interval 10ms and 25ms has larger standard deviation.

A potential reason for larger deviation may be due to software limitation as the protocol stack was emulated in a personal computer which was running other application as well. Other reason could be congestion in the network and public internet access in LTE network.

5.1.3 Reliability

The reliability plot is presented in Figure 5.4. Reliability was measured to understand the efficiency at which the packets are received and drop in a non-commercial LTE network. Network was expected to be highly reliable and the expected average reliability was around 99.99%.

Figure 5.4 shows measured reliability decreases with the time interval. During the start, the
application takes some time to stabilize which results in the huge dip in the graph. As the time progress, the reliability tends to stabilize for some time and once again packet drop is observed in the network. These packet drop results in decreasing the overall reliability to 99.7% even after stabilizing which is less from the expected result. This drop in reliability would affect the performance and is highly undesirable.

On analyzing the Wireshark, it was found that the packets that were dropped not were received on the receiving interface. So, the packet is dropped while traversing the network. The potential reason may be the public internet, congestion or network unavailability.

5.1.4 Availability

Figure 5.5 shows the availability plot of LTE network for a duration of 24 hours. One R-SV packet per second was continuously exchanged between the machine and the plot was taken for every 5 min interval reading.

As can be seen in Figure 5.5, the network availability of the non-commercial 4G LTE drops below 94% between 9:00 AM and 1:00 PM. The drop in network availability was due to an occurrence of more packet drop during that time interval and is shown in the graph by a huge dip.

the potential reason for this behavior could be due to congestion in the public network or may the core network infrastructure is used somewhere else. On discussing with the network provider, it was found out that the network was not dedicated for the test.
**Figure 5.5:** Availability of the LTE network in 24 hours
6 Conclusion and Future Work

Technical Report IEC 61850-90-5 provides a way to exchange routable GOOSE and SV message in a public IP network such as Long Term Evolution and 5G. LTE has evolved significantly over the past few years and could play an important role to be the suitable solution for wireless communication in a smart grid infrastructure. The thesis work evaluates the performance of non-commercial LTE for smart grid applications such as Wide Area Monitoring Protection and Control.

An IEC 61850-90-5 model with new session layer and data packed in Routed- Sample Value format as defined in the technical report was developed during the thesis work. The modified R-SV packets representing the synchrophasor information was exchanged between two machines that emulate a virtual Intelligent Electronic Device over a non-commercial LTE environment. Communication metrics such as throughput, reliability, availability, and latency were considered to benchmark the performance of non-commercial LTE. Different test cases were formulated to measure and calculate these metrics.

The routable GOOSE and SV packet proposed in the technical report will be key in utilizing wireless communication for smart grid application. LTE provides flexibility and scalability with low deployment cost. LTE in combination with IEC 61850-90-5 can play a major role in replacing the existing wired communication model in a smart grid. Also, it would play a major role in Machine-to-Machine communication.

The test presented in the report is to analyze the readiness of IEC 61850-90-5 protocol and its applicability in combination with non-commercial LTE. It can be concluded from the obtained result that LTE would be a suitable solution for wireless communication for most of the smart grid application. But there is still some major optimization to be implemented in LTE network along with QoS priority to support its complete usage in applications with stringent requirements on communication network performance.

The network throughput test was conducted to understand the effect of packet size and transmission rate combination in data transmission rate. The result shows the gradual decrease in transmission speed when is increased beyond 950 Bytes for lower transmission interval. The transmission frequency drop observed was around 15% for lower transmission interval of 2ms (i.e. 200 packets transmitted per second).

The highest latency observed was around 45ms which could affect the performance. The availability and reliability result was crucial to analyze the LTE network stability. The overall result shows poor network performance during the 9:00 AM and 1:00 PM time. The poor availability has also resulted in lower reliability. The overall reliability observed was 99.7% which is below than the expected reliability of 99.99%. This can be improved by using a dedicated network.
The innovation in cellular communication has gained the interest of many researchers to use it for the different application. Utilization of cellular communication for smart grid application would be key in coming days. The existing non-commercial LTE could give better performance and result for time demanding smart grid application when provided with the dedicated connection and enhance QoS for smart grid packets. Additional with the trend moving from 4G to 5G, cellular communication would have a great impact in strengthening the backbone of smart grid communication.

Future Work

The main work of the thesis work was to study the usability of LTE for time-critical smart grid application. To define LTE applicability, various communication metrics such as throughput, reliability, latency, and availability was considered. Another aspect such as security was not considered due to time restriction and is kept for future.

A comprehensive analysis of IEC 61850-90-5 standard was done. The complete implementation was beyond the scope of the project and hence only packet structuring, data integrity check and UDP/IP transmission were covered in the development process. Security and enhancing the reliability of the sent packet was kept for future work.

The test cases run to evaluate the performance of non-commercial LTE were limited due to time restriction. More test trial can be run to get more accurate result. Also, all the test except the availability test was performed during the office hour between 9 AM to 6 PM. Running the same test cases during the non-office hour would give a different result and is kept for future work.
Bibliography


