ABSTRACT

SHAH, MOHIT B. End to End Communication Architecture and Technology Performance Evaluation: Ethernet and WiFi for Substation Automation Networks. (Under the direction of Dr. Wenye Wang.)

The electric grid routes power flows that are constrained by the laws of physics unlike the information technology network, which routes packets of information. The latency requirements of a smart grid application depends upon priority/type of information exchanged and these messages are 'time-critical' and they demand some order of 'control action response' to stabilize an unusual event in the electric domain. Smart grid applications, such as SCADA systems that control substations, have latency requirements measured in milliseconds and the consequences of failing to deliver a control packet on time can be catastrophic. In order to achieve stability and resiliency of the existing power grid, the communication topology used to drive such smart grid applications must support a diverse set of applications each with varying network performance requirements, reliability requirements, traffic characteristics, as well as the challenges faced with supporting legacy applications and networks. Characterizing the performance requirements for various smart grid applications is critical to understand which communication technologies should be used for various applications.

With a need for an architecture that enables communication and decision making between distributed system nodes; and to successfully deliver messages within accepted latency bounds specified by IEEE 1646-2004 standard, this work aims at identifying the existing challenges and communication requirements towards developing an end to end communication topology and evaluate the capability of Ethernet and Wifi technologies in enabling the exchange of latency sensitive messages with varying priorities in substation
In this work, we present and discuss an end to end communication architecture design spread across two substation sites in a distribution domain. We have simulated this topology using open source OMNeT++ tool in order to test the performance of Ethernet and Wifi to enable exchange of 'high', 'medium' and 'low' priority messages between nodes within and external to a substation site. We present the different aspects of such an end to end system design, and use performance metrics like 'Application Latency' and 'End to End Delay' to present an in-depth analysis. The communication architecture design presented in our work models three common substation automation use cases namely 'Voltage Regulation using Capacitor Banks'; 'Voltage Regulation using Tap Changers' and 'Inter-Substation Event Monitoring Reporting'.
End to End Communication Architecture and Technology Performance Evaluation:
Ethernet and WiFi for Substation Automation Networks

by
Mohit B. Shah

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Computer Engineering

Raleigh, North Carolina
2013

APPROVED BY:

Dr. Mesut Baran
Dr. Khaled Harfoush

Dr. Wenye Wang
Chair of Advisory Committee
DEDICATION

I dedicate all the efforts made in this research work to my mom, Mrs. Jayshree Shah, my uncle, Mr. Madanlal Natali and all my loving Natalis.
BIOGRAPHY

Mohit Shah was born in August 1987 and spent his life growing up in Mumbai, India until January 2011. He received his Bachelor’s degree in Electronics and Telecommunication Engineering from K.J.Somaiya College of Engineering, Mumbai, India, in May 2009. Mohit has a deep passion for Networking, Web Designing and Web Development. He has been pursuing his hobby of Web Designing since 2007. He has been a Master’s student in the Department of Electrical and Computer Engineering at North Carolina State University since January 2011 to pursue his Master’s of Science degree in Computer Engineering. He is currently working with Extron Electronics in Raleigh, North Carolina as an Application Software Engineer with the Software Streaming team based in Raleigh.
ACKNOWLEDGEMENTS

I would like express heartfelt gratitude to my advisor Dr. Wenye Wang who has been the biggest motivating factor in my research work. She has been a great mentor and a constant source of inspiration and motivation in every aspect of this thesis work. Her immense knowledgebase about the subject and guidance to move ahead at each step has helped me to achieve my results and goals to this effect. I would thank my committee members Dr. Mesut Baran and Dr. Khaled Harfoush for being patient and supportive in all regards during this fantastic journey. Also, I’d like to thank Matt Homovich from Green Energy Corp for being patient and responsive to all my doubts and problems I went to him for in the past year or so. Finally, I would not have been able to achieve this without constant support and care from all my family members and friends in India and the United States.
# TABLE OF CONTENTS

## LIST OF TABLES

- v

## LIST OF FIGURES

- viii

### Chapter 1 Introduction

- 1.1 Smart Grid Conceptual Framework  
- 1.2 Unique Features of Intelligent Grid Systems  
- 1.3 Motivation and Objectives  
- 1.4 Related Work and Contributions
  - 1.4.1 Related Work  
  - 1.4.2 Contributions

### Chapter 2 Communication Network Requirements and Challenges

- 2.1 Design Considerations
  - 2.1.1 Communication Medium for data transport  
  - 2.1.2 TCP vs. UDP Solution  
  - 2.1.3 Communication technologies  
  - 2.1.4 Hardware/Software/Communication Specifications  
  - 2.1.5 Protocol Efficiency of DNP3 over TCP/IP
- 2.2 IEEE C37.1-2007 and IEEE 1646-2004 Overview
  - 2.2.1 Use of IEEE C37.1-2007 Standard  
  - 2.2.2 Use of IEEE 1646-2004 Standard
- 2.3 Terminologies and Definitions
- 2.4 Taxonomy of Communication Interfaces

### Chapter 3 Communication Architecture for Substation Automation

- 3.1 Three Substation Automation Use-cases
- 3.2 Design of Communication Architecture for Substation Automation Networks
- 3.3 Communication Sessions and Protocol Stacks
- 3.4 Modeling of Application Latency and End-End Delay in Substation Automation Networks
- 3.5 Simulation Scenarios
  - 3.5.1 Scenario 1: Unsolicited Reporting in Site 2
  - 3.5.2 Scenario 2: Exception Scan in Site 1
  - 3.5.3 Scenario 3: Inter-Substation Event Monitoring and Reporting

### Chapter 4 Simulation Model

- 4.1 OMNeT++ and INET

- vi
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>INET Framework</td>
<td>70</td>
</tr>
<tr>
<td>4.2</td>
<td>Simulation Model: OMNeT++</td>
<td>70</td>
</tr>
<tr>
<td>4.3</td>
<td>Simulator Application: Scenario 1</td>
<td>78</td>
</tr>
<tr>
<td>4.4</td>
<td>Simulator Application: Scenario 2</td>
<td>83</td>
</tr>
<tr>
<td>4.5</td>
<td>Protocol Software Architecture</td>
<td>88</td>
</tr>
<tr>
<td>4.6</td>
<td>General Assumptions</td>
<td>90</td>
</tr>
<tr>
<td>5.1</td>
<td>Scenario 1: Unsolicited Reporting in Site 2</td>
<td>93</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Source: M6280A Digital Capacitor Bank Controller</td>
<td>94</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Source: IVVC Integrated Volt/VAR Control Application</td>
<td>99</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Source: MasterControlCenter</td>
<td>104</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Technology Performance Analysis</td>
<td>108</td>
</tr>
<tr>
<td>5.2</td>
<td>Scenario 2: Exception Scan in Site 1</td>
<td>109</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Performance Evaluation: Ethernet Only</td>
<td>110</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Performance Evaluation: IEEE 802.11g + Ethernet</td>
<td>110</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Technology Performance Analysis</td>
<td>115</td>
</tr>
<tr>
<td>5.3</td>
<td>Scenario 3: Inter-Substation Event Monitoring</td>
<td>115</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Technology Performance Analysis</td>
<td>117</td>
</tr>
<tr>
<td>5.4</td>
<td>Summary</td>
<td>121</td>
</tr>
<tr>
<td>6.1</td>
<td>Conclusions and Future Work</td>
<td>124</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>128</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 1.1 Related Work listings by focus areas ........................................ 13
Table 2.1 IEEE 1646 Communication Timing Requirements for Substation
               Automation .................................................................................. 18
Table 2.2 Communication Technologies and Potential Applications in Smart
               Grids ............................................................................................... 20
Table 3.1 Functional Definitions of Subsystems:Site 1,2 ................................ 48
Table 3.2 Hardware and Software Specifications of IEDs and Computers ...... 51
Table 3.3 TCP Communication Sessions across Site 1 and Site 2 ............... 52
Table 4.1 One to One Network Mapping : Site 1 ....................................... 73
Table 4.2 One to One Network Mapping : Site 2 ....................................... 74
Table 4.3 Actors and associated roles:Site 1 ............................................. 76
Table 4.4 Actors and associated roles:Site 2 ............................................. 77
Table 5.1 Source of Communication : M6280A ....................................... 98
Table 5.2 Source of Communication : IVVC ........................................... 103
Table 5.3 Source of Communication : MasterControlCenter .................. 107
Table 5.4 Technology Performance : Exception Scan ................................. 114
Table 5.5 Summary of Findings : AL ...................................................... 122
Table 5.6 Summary of Findings : End to End Delay .................................. 123
LIST OF FIGURES

Figure 1.1 Smart Grid Conceptual Model[1]. ........................................ 3
Figure 1.2 Enhanced Asset Utilization[2]. ........................................ 4
Figure 2.1 The various communication layers in DNP3 stack[3]. .......... 22
Figure 2.2 Example Substation Automation Architecture without Security[4]. 26
Figure 2.3 Information Types in Substation Automation[5]. ............... 27
Figure 2.4 Complexity of Smart Grid Networks. .............................. 33
Figure 2.5 Communication network connections in Distribution domain... 35
Figure 2.6 Taxonomy of Communication Devices and Interfaces. ........ 36
Figure 3.1 Volt/VAR Regulation using Capacitor Bank Control. .......... 40
Figure 3.2 Voltage Regulation using Tap Changers. .......................... 41
Figure 3.3 Load Balancing between two transformers. ....................... 42
Figure 3.4 Communication Architecture in Substation Site 1. .............. 44
Figure 3.5 Communication Architecture in Substation Site 2. .............. 45
Figure 3.6 Load Tap Changer Subsystem:Site 1. ............................... 46
Figure 3.7 Capacitor Bank Control Subsystem:Site 2. ......................... 46
Figure 3.8 Integrated Volt/VAR Control Application Subsystem:Site 2. ... 47
Figure 3.9 SCADA Master Station Subsystem:Site 1,2. ....................... 47
Figure 3.10 DNP3 Protocol Stack : IED or Embedded Computer. ........ 53
Figure 3.11 Communication Stack : IED or Embedded Computer. ........ 54
Figure 3.12 End to End Communication Protocol Stack. ..................... 55
Figure 3.13 Delay Components : Application Latency. ....................... 57
Figure 3.14 Unsolicited Reporting Scenario in Site 2. ....................... 62
Figure 3.15 Unsolicited Reporting Sequence of Operations. ............... 63
Figure 3.16 Exception Scan Scenario in Site 1. ............................... 64
Figure 3.17 Exception Scan Sequence of Operations. ....................... 65
Figure 3.18 Inter-Substation Event Reporting between Site 1 and Site 2. 66
Figure 3.19 Inter-Substation Event Reporting Sequence of Operations. ... 67
Figure 4.1 Simulation Model of Communication Network. ................... 71
Figure 4.2 Messages Exchanged : Unsolicited Reporting Scenario. ....... 79
Figure 4.3 Scenario 1 : Client IED Simulator Application. ................ 80
Figure 4.4 Functions in Client-side IED TCP Application Code. ......... 82
Figure 4.5 Functions in Server-side TCP Application Code. ............... 83
Figure 4.6 Scenario 2 : Client IED Simulator Application. ............... 85
Figure 4.7 Functions in Client-side SCADA TCP Application Code. ...... 86
Figure 4.8 Functions in Server-side IED TCP Application Code. ......... 88
Figure 4.9 Scenario 1 : Protocol Software Architecture. ................... 90
Figure 5.1 Source = M6280A, Dest=IVVC. ................................. 95
Figure 5.2 Source = M6280A, Dest= MasterControlCenter. ............... 96
Figure 5.3 Source = IVVC, Dest=M6280A. ................................ 100
Figure 5.4 Source = IVVC, Dest=MasterControlCenter. ..................... 101
Figure 5.5 Source = MasterControlCenter, Dest=IVVC. ...................... 105
Figure 5.6 Source = MasterControlCenter, Dest=M6280A. .................. 106
Figure 5.7 Scenario 1 : Technology Performance Comparison. .............. 109
Figure 5.8 Scenario 1 : Effect of Delay Components. ....................... 110
Figure 5.9 Performance of IEEE 802.11g with TCP vs UDP. ................. 111
Figure 5.10 Ethernet 10/100Mbps, src: SCADAMasterStation, dest: M2001D. 112
Figure 5.11 Ethernet 1Gbps, src: SCADAMasterStation, dest: M2001D. .... 112
Figure 5.12 Performance of IEEE 802.11g + Ethernet 10Mbps. .............. 113
Figure 5.13 Scenario 2 : Technology Performance Comparison. ............. 116
Figure 5.14 Inter-Substation Case I : Ethernet 10Mbps with TCP. .......... 117
Figure 5.15 Inter-Substation Case II : Ethernet 100Mbps with TCP. ......... 118
Figure 5.16 Inter-Substation Case III : Ethernet 10Mbps with UDP. ......... 119
Figure 5.17 Scenario 3 : Technology Performance Comparison. ............. 120
Chapter 1

Introduction

In traditional networks, electricity is generated in central power stations and is delivered to customers via transmission and distribution networks. Electric power network of today is characterized by structural weaknesses and environmental shortcomings, particularly in relation to security of supply and climate change. Talking about enabling communications in Smart Grid systems, there are a number of challenges and issues that need to be considered beforehand. The smart grid will bring about an evolution of the power system into a highly interconnected, complex, and interactive network of power systems, telecommunications, the Internet, and electronic commerce applications. This calls for a new communication network that will account for seamless integration/interoperability of the many disparate systems and components, as well as enable the ability to manage competitive transactions resulting from competitive service offerings that emerge in the restructured utility environment. Examples of competitive transactions include settlements for demand response participation, information reporting and notification. However, the development of such an end to end communication architecture is a research challenge in itself. Such a communication architecture will be designed to enable communication
and decision making between distributed system nodes and parties. The architecture is intended to be used to develop software that can supplement the existing power distribution/market network communication infrastructure. The goals of this architecture are to allow for interoperability and flexibility to facilitate and enable information transfers to occur. Interoperability can be enabled by the use of open communication protocols.

1.1 Smart Grid Conceptual Framework

The National Institute of Standards and Technology (NIST) Smart Grid Conceptual Model provides a high-level framework for the smart grid that defines seven important domains: Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Providers.[6] It shows all the communications and energy/electricity flows connecting each domain and how they are interrelated. The NIST Smart Grid Conceptual Model helps stakeholders understand the building blocks of an end-to-end smart grid system, from Generation to (and from) Customers, and explores the interrelation between these smart grid segments.

1.2 Unique Features of Intelligent Grid Systems

In the United States, about 40% of the human caused emission of CO2 is produced in the generation of electricity[7]. If the power grid were just 5% more efficient, the resultant energy and emissions reductions would be equivalent to permanently eliminating the fuel consumption and greenhouse gas emissions from 53 million cars[8]. The following are some major factors that explain the need to modernize the conventional grid system.
Peaked Nature of Electricity Demand  Less than half of the generation capacity in the United States comes from power plants designed to run all the time to meet demand. It is estimated that capacity to meet demand during the top 100 hours in the year account for 10 to 20\% of electricity costs.[9]

Enhanced Asset Utilization  In U.S. roughly 50\% of the generation capacity is used 100\% of the time greater than 90\% of the capacity is used. Usually the most costly and inefficient generation is used during these peak periods[2]. If during the peak 400 hours DER participated to mitigate the use of this generation, then significant savings would accrue by reducing the necessary capacity by 10\% as seen in Figure 1.2.

Use of Distributed Energy Resources  Changes in technology and the resulting economics have now disrupted that traditional value chain and stimulated the adoption of distributed energy resources (DER). In addition, because of competition and deregulation, a whole new area of energy services and transactions has sprung up around the demand side of the value chain.
Human ability to innovate  Technical advancements in communications and information technology allow engineers affordable alternatives to coordinate energy resources to more effectively balance supply and demand. This technology promises higher levels of asset utilization and the flexibility required to integrate less impactful environmental energy sources such as wind and solar generation.

The following are some unique features of an intelligent grid system:

- By applying advanced information technology (IT) and combining IT with smart appliances, smart grids can enhance energy efficiency on the electricity power grid, in homes and in businesses.

- By using smart grids, transmission and distribution companies will be able to improve control over the network and can gather complex, real-time information about grid performance.

- Smart grids can enhance the reliability of electricity supply by automatically preventing outages and improving the detection of power lines overloads and faults.
• Smart grids can manage voltage within the grid and help reduce the losses that occur as electricity travels along transmission and distribution lines.

• Smart meters, (important element of smart grid) can let consumers know how much electricity they are using in their homes and offices. Smart applications can also alert them to how they can change their energy consumption during peak periods in order to save money on their electricity bills.

• Smart appliances, can also be programmed using smart grids to run on off-peak power. They can also enable heaters and air-conditioners to be remotely controlled, giving customers the ability to better manage their energy costs and help reduce the demand for electricity in peak times.

1.3 Motivation and Objectives

Our decision in choosing a study as dense and complex as modeling a communication topology and enabling technologies to drive substation automation network applications is inspired from a number of existing research challenges in developing an end to end communication architecture that will account for seamless integration/interoperability of the many disparate systems and components, as well as enable the ability to manage competitive transactions resulting from competitive service offerings that emerge in the restructured utility environment.

1. As a high level motivating factor, the electric power delivery system is almost entirely a mechanical system, with only modest use of sensors, minimal electronic communication and almost no electronic control. Even today, a power system area operator can, at best, see the condition of the power system with a 20-second delay.
In the United States, about 40 percent of the human caused emission of CO2 is produced in the generation of electricity[7]. If the power grid were just 5 percent more efficient, the resultant energy and emissions reductions would be equivalent to permanently eliminating the fuel consumption and greenhouse gas emissions from 53 million cars[10].

2. A unique communication architecture will be needed to enable communication and decision making between distributed system nodes and parties. The architecture is intended to be used to develop software that can supplement the existing power distribution/market network communication infrastructure. The communication topology must support a diverse set of applications each with varying network performance requirements, reliability requirements, and traffic characteristics, as well as the challenges faced with supporting legacy applications and networks.

3. Currently, there are a number of major obstacles and research challenges in the design of a fully functional, resilient, high availability communication network that can enable the transfer of DNP3 over TCP/IP messages within the time bounds specified by IEEE 1646-2004 timing standard[5]. The communications in the electric power domain are very different from those in the internet. The delay requirements of an application in smart grid systems depend upon the priority/type of information exchanged. The size of messages is small in the power domain but communications is more delay-sensitive than throughput-centric as in IT. Unlike IT, the messages exchanged in power domain are more ’critical’ and they demand some order of ’control action response’ to stabilize an unusual event in the power domain which requires the correct choice of communication technologies to deliver these messages within accepted latency bounds. Unlike the telecommunications
network, which routes packets of information, the electric grid routes power flows that are constrained by the laws of physics. The consequences of failing to deliver a control packet on time can be catastrophic in a power system scenario. Characterizing the performance requirements for various smart grid applications is critical to understanding which communications technologies should be used for various applications.

4. Finally, the chosen intelligent electronic devices for an application should be able to inter-operate with devices manufactured by different vendors that may be using proprietary semantics and protocol formats which calls for the need for an open source communication protocol like DNP3 and standards like IEC 61850.

With all the above listed challenges and existing problems in enabling a communication network for any given smart grid application in any domain, and to deliver the messages exchanged in such applications within the latency bounds specified by IEEE 1646-2004[5], our scope of our thesis study can be reasonably termed as 'End to End Communication Architecture and Technology Performance Evaluation of Substation Automation Communication Networks : Ethernet and WiFi'.
**Objectives:** This study aims at end to end study of a communication architecture requirements that serves as a base topology to evaluate the viability of Ethernet and Wifi technologies to drive substation automation use-cases. Such an architecture is needed to enable communication and decision making between distributed system nodes and blocks. With an effort to develop a topology and evaluate the performance of Ethernet and Wifi for substation automation networks, we aim to address and answer the following major concerns and research questions pertaining to enabling communications in smart grid systems:

**Phase I:** The first set of objectives in our work include understanding the end to end communication requirements and message delivery requirements with any substation automation application use case that we choose to evaluate. This is an important research concern and needs to be addressed because the message delivery requirements in power domain are unique. Also, the communication capabilities of embedded power devices is limited. In order to achieve this, we identify and understand the various functional blocks, types of power devices and their effect of their hardware/software specifications that will drive an application. Hence, the first phase of this work involves a detailed study of various communication components and their roles at different levels of a substation automation application functional cycle.

**Phase II:** After answering the communication network requirement concerns in phase I, it is important to address the next challenge of integrating these actors and subsystems to form a fully connected and available network. Therefore, the second phase of this study involves joining all the pieces together to formulate a system level communication block diagram. However, in order to join these pieces, we need communication interfaces
that will interact with these actors/devices and connect them to the network. Hence, this step involves identifying and developing direct and logical communication interfaces with respective bit rates that will be used to construct a fully 'functional' communication network topology. This set of communication interfaces will be used in our final simulation model for modelling the links and their associated bit rates on their output ports. They can also be used in any future work related to testing of a communication topology for any smart grid systems, to interface the various actors, devices, blocks or systems with each other.

**Phase III:** In the final phase of our work, a major objective is to study the performance of Ethernet and Wifi in combination with TCP and UDP to exchange DNP3 over TCP/IP messages with varying priorities for common substation automation use-cases. The results obtained from this phase of study will unveil answers to existing research concerns related to the viability of DNP3 over TCP/IP in substation automation networks; which combination of communication technologies and configurations can drive a substation application within latency bounds, what are the implications of using Ethernet and Wifi, TCP and UDP for substation applications and under what conditions can they be used and so on. It is worthwhile to address these issues in our work because the choice of a communication technology directly impacts the latency of the overall application under consideration. The factors affecting the latency of an application will become more diverse when the number of actors and amount of data being transferred increases. There are other factors like additional internet traffic in the path and limited computational capabilities of intermediate network device to process packets and forward them, that will affect the application latency.

Therefore, we select substation automation use-cases and model their communication
functionality in software using the end to end communication network topology presented in phase I and II. We also present a detailed result analysis and perform comparison tests using the Ethernet and Wifi technologies to study which combination and configuration provides optimum delay values for our chosen substation automation use-cases as specified by IEEE 1646-2004[5].
1.4 Related Work and Contributions

Smart Grids lately becoming a popular area of research and development, there are quite a few excellent work efforts already put in. Our work relates to communications in the transmission and distribution domains and hence we discuss some related research work relevant to our study in this section. Any work done in a smart grid research area can be categorized into either of three types namely survey, performance evaluation and simulation and finally real-world implementation.

1.4.1 Related Work

In a particular survey work presented in [11], the authors present the opportunities and challenges of a hybrid network architecture are discussed for electric system automation. More specifically, they conduct an in-depth feasibility study of how Internet based Virtual Private Networks, power line communications, satellite communications and wireless communications (wireless sensor networks, WiMAX and wireless mesh networks) can be used to leverage high speed automation in substation networks. They mention the advantages and disadvantages of using each of these technologies in the smart grid domains in detail. While talking about the possibility of using each of these technologies in the smart grid, they view the electric substation automation only from a communication networking standpoint.

In another survey based approach as shown in [12], the authors conduct a comprehensive survey on the communication architectures in the power systems, including the communication network compositions, technologies, functions, requirements, and research challenges. The authors make an attempt to summarize the current state of research efforts in the communication networks of smart grid, which have helped us in our work to
identify and understand the challenges in designing a communication network for smart grids. They have discussed the various delay components incurred as processing delay inside an Intelligent Electronic Device (IED) and also summarized the protocol stack at each network device in an end to end smart grid communication application.

In a performance evaluation study of using Wireless technology like Zigbee[13, 12] in the customer domain, the authors present an intelligent approach for proving Zigbee’s feasibility in home area networks (HAN)[14] by considering simulation of 100 resident appliances and using a smart meter as a HAN gateway. They measure the packet delivery ratio at the smart meter by varying the number of devices in a HAN.

Another important implementation work as shown in [15] employs a network performance evaluation study and conducts a unique end to end delay analysis of the Distributed Network Protocol (DNP3)[3] based messages exchanged between different power devices like a Relay IED, a Capacitor Bank Controller and a PC master. In this work, the authors establish a microsmart grid, named Green Hub, to measure the delay performance of the predominant SCADA protocol, distributed network protocol 3.0 (DNP3)[3] over the ubiquitous TCP/IP protocol suite. They conduct their experiments in using baseline delay performance tests in which they only test the performance of the application using one device of each type. They evaluate and summarize the delays incurred at to the DNP transport and data link control layers.

The above mentioned work in [15] is closely related to one of our objectives since we will also be considering the use of intelligent power devices in a substation environment like them. However, our work also considers different substation use-cases and detailed performance evaluation of different Ethernet technologies in combination with IEEE 802.1g Wifi, using TCP as well as UDP as the transport layer solution. We have adopted the physical specifications of devices mentioned in [15] for our study, due to usage
Table 1.1: Related Work listings by focus areas

<table>
<thead>
<tr>
<th>Type of Work</th>
<th>Area of focus</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey</td>
<td>Communication Requirements and Challenges</td>
<td>[16][17]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[11][13][14][18][19]</td>
</tr>
<tr>
<td>Survey</td>
<td>Feasibility of Technologies</td>
<td>[13][12]</td>
</tr>
<tr>
<td>Performance Evaluation</td>
<td>Wireless Technology Evaluation</td>
<td>[20][21]</td>
</tr>
<tr>
<td>Performance Evaluation</td>
<td>Communication Delay and Bandwidth</td>
<td>[15][22]</td>
</tr>
<tr>
<td>Implementation</td>
<td>End to End Delay and DNP3</td>
<td>[15][22]</td>
</tr>
</tbody>
</table>

of highly relevant intelligent power devices and functions in our respective experiments. In Table 1.1, we present an overview of the above mentioned and a few other related studies. According to us, our work can be accommodated into the first and second category since we conduct an end to end study of challenges and requirements to design an architecture, and further propose an end to end communication architecture design and associated simulation model.

**Organization of Chapters** The rest of the chapters in this thesis are organized as follows. Chapter 2 discusses the major factors and challenges to be considered while designing an end to end communication architecture for any smart grid related application. We also present the two important IEEE standards C37.1-2007 and 1646-2004 that provide design and timing requirement guidelines. We present general terminologies and definitions that are used in this study. Finally, we conclude this chapter with a taxonomy of required communication interfaces and schematics of communications flow across various domains of the Smart grid based on the discussion in this chapter.

In chapter 3, we introduce the proposed end to end communication architecture that we design and adopt for performing our simulation tests on and describe every aspect of
design, specifications and communication workflow of all the devices used in this diagram. We also propose the three substation automation use-cases that we simulate in the next chapter. Finally, we define the composition of a metric we use to evaluate our tests called Application Latency (AL) and End to End Delay.

In chapter 4, we introduce the proposed simulation model for the introduced end to end communication architecture described in chapter 3 and present design and operational aspects of the software application architecture that will be used to communicate between endpoints using TCP and UDP. Further we will discuss the software protocol architecture of the simulation model.

Chapter 5 presents the results, observations and performance analysis of three substation scenarios namely Unsolicited Reporting, Exception Scan and Inter-substation Event Monitoring. We discuss the implications of using Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11g Wifi with TCP and UDP in these scenarios to measure the Application Latency and end to end delay of the application under consideration. Finally, we conclude this work by presenting a summary of work and presenting various message types/technology/transport protocol/application latency range combinations in any substation automation network.

With chapter 6, we summarize all the lessons learnt from the issues addressed in this work and propose some future work that can be done with this study.
1.4.2 Contributions

With this study, we address major challenges, concerns and requirements involving the design and configuration of an end to end communication architecture that can be used to model communications in intra and inter substation automation environments.

We present a taxonomy of communication interfaces (editable) and devices that can be used to connect any communication topology endpoints designed using OMNeT++ for Smart Grid applications. These links connect two system blocks or network devices together for communicating messages using the ubiquitous TCP/IP protocol suite. Such a taxonomy of links and schematic representation of communications flow across various Smart Grid domains helps progress towards developing an end to end communication architecture from a detailed connectivity standpoint: use of Direct, Logical and Aggregated flows.

Next, our contribution to the work done in enabling communications in substation automation networks includes the development of an end to end communication topology that enables and serves three common substation automation use-cases namely Voltage Regulation using Capacitor Banks, Voltage Regulation using Tap Changers and Load Balancing between Transformers. Our topology uses system blocks and devices modeled using OMNeT++ nodes and include communication capabilities modeled within them just as real world devices like Beckwith M6280A and Beckwith M2001D Intelligent Devices are available with. All the system blocks are connected using the communication links taxonomy presented in Chapter 2.

The major challenge area in distribution substations lies with enabling technologies to drive these automation applications towards achieving message delivery within specified bounds. With a view to address this challenge, our performance evaluation tests on the
developed topology using proven technologies like Ethernet and Wifi presents minimal idea in making the correct choice of 'communication technology/transport protocol/technical specifications' combination for different priority information messages exchanged in substation automation networks. This network topology can be used to evaluate the performance of other technologies like WiMAX, Bluetooth and so on, since it is built using open-source code with OMNeT++ simulation tool.

Overall, our contribution includes the design and simulation model for an end to end communication topology for substation automation applications, a taxonomy of communication interfaces and links that can be modified and re-used for other modeling applications within or across Smart Grid domains and two simulator applications in OMNeT++ to enable the message exchange in the three substation use-cases.
Chapter 2

Communication Network

Requirements and Challenges

One of the key technology areas of the Smart Grid is integrated two-way communications, which allows for dynamic monitoring of electricity use as well as the potential for automated electricity use scheduling[2][23][10]. Many communications and networking technologies can be used to support Smart Grid applications, including traditional twisted-copper phone lines, cable lines, fiber optic cable, cellular, satellite, microwave, WiMAX, power line carrier, and broadband over power line, as well as short-range in-home technologies such as WiFi and ZigBee[13][12].

2.1  Design Considerations

In the preliminary phase of our work, we list a total of 5 major factors to be considered before designing a communication network for substation automation applications. These factors directly affect the performance of the designed topology and the application as a
Table 2.1: IEEE 1646 Communication Timing Requirements for Substation Automation

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Delay Requirement</th>
<th>Bandwidth Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>4ms</td>
<td>10Mbps - 1Gbps</td>
</tr>
<tr>
<td>Monitoring and Control</td>
<td>16ms</td>
<td>10-100kbps</td>
</tr>
<tr>
<td>Operation and Maintenance</td>
<td>1s</td>
<td>10-100kbps</td>
</tr>
</tbody>
</table>

whole. Some of these factors are recommended in the NIST report[6][1].

- Communication medium for data transport
- Use of TCP/IP vs. UDP as a transport layer solution
- Communication technologies
- Hardware/Software/Communication specifications of embedded computers
- Protocol efficiency of DNP3 over TCP/IP

2.1.1 Communication Medium for data transport

Wide Area Networks (WAN) include a hybrid mix of technologies including fiber optics, power line carrier systems, copper-wire line, and a variety of licensed and unlicensed wireless technologies.[13]. The choice of communication medium depends largely on the type of messages transferred between two applications because different priority messages are bound by specific latency requirements specified by IEEE 1646-2004 standard[5]. In our research interest, we summarize the three most important types of information exchanged in any substation automation application and their timing requirements as specified by IEEE 1646-2004 in the Table 2.1.
2.1.2 TCP vs. UDP Solution

If we adopt an all-IP philosophy in communication of messages in substation automation applications, the Smart Grid will benefit by having an open, secure network with the greatest degree of design flexibility, including redundancy and diversity, while also retaining relative simplicity. Latency is a direct function of the transmission media used (e.g. fiber optic cable, copper wire, radio signal etc.). There are, however, characteristics of the transport mechanisms supported by IP that can introduce payload latency[23][19]. Protocol related delays can occur when the Transmission Control Protocol (TCP) is used on an IP network unlike UDP that provides zero assurance for everything.

About TCP  TCP offers the highest level of packet delivery assurance, but this comes at a price. By its very nature, TCP introduces the burden of comparatively high network overhead because of its mechanism for responding to corrupted and collided packets. The degree to which resultant retransmissions impact payload latency is largely determined by the quality of the transmission media, along with loading on the communication channel[24].

About UDP  The User Datagram Protocol (UDP) is lightweight in contrast to TCPs overhead but it comes at the cost of nonassured packet delivery as there is no acknowledgement of receipt mechanism. Applications for UDP are typically written to factor in the likelihood that some packets will be lost or corrupted over the course of the session[24]. When considering the mission criticality of Smart Grid protection and control applications, three attributes are required: low latency, prioritization through QOS, and TCP.
2.1.3 Communication technologies

Unlike the internet or telecommunications network, which routes packets of information, the electric grid routes power flows that are constrained by the laws of physics. Characterizing the performance requirements for various smart grid applications is critical to understanding which communications technologies should be used for various applications. The proliferation of information technology utilizing Internet protocol (IP) transport over Ethernet has made IP the de facto standard for data transport. However, according to our study, a single communication technology cannot be used for all smart grid application scenarios. Wireless LAN or IEEE 802.11 cannot be used as a standalone solution to deliver protection information which has latency bounds of less than 4ms within substations and 8-12ms external to substations[5]. In Table 2.2, we present a list of proven and potential communication technologies and related scenarios they could possibly be deployed for.

2.1.4 Hardware/Software/Communication Specifications

Choosing an embedded computer or a workstation specifications for a substation automation application is by far the most dominant factor in profiling the end to end application delay[15]. This is because most of the embedded computers today in the power domain

---

Table 2.2: Communication Technologies and Potential Applications in Smart Grids

<table>
<thead>
<tr>
<th>Technology</th>
<th>Range of Coverage</th>
<th>Potential Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>100-200m</td>
<td>Protection, Control, Backbone</td>
</tr>
<tr>
<td>IEEE 802.11g</td>
<td>100m</td>
<td>Control, Reporting</td>
</tr>
<tr>
<td>Zigbee</td>
<td>10 - 75m</td>
<td>In-home reporting</td>
</tr>
<tr>
<td>WiMAX</td>
<td>30 miles</td>
<td>Backbone or Core network</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>5 - 30m</td>
<td>In-home reporting</td>
</tr>
</tbody>
</table>
utilize Distribution Network Protocol (DNP3) over TCP/IP for inter-device communication. The DNP3 protocol itself works in a layered manner and there is a lot of processing involved at its own transport and data link layer[3]. Detailed operation of each layer in the DNP3 protocol stack can be found in [3]. Because of this processing delay, the overall latency of the application is directly affected. Therefore, the memory of the embedded computer (RAM), the CPU speed, and the operation system platform are very important parameters to choose hardware device configuration. The cost of designing the communication network increases if you keep upgrading the hardware specifications of the power and network devices used. This in turn decreases the end to end latency of the application. Hence it is an important decision to establish a reasonable balance between the delay incurred due to the hardware limitations of the CPU and the application latency. In our work, we have modeled the intelligent electronic device specifications, their related processing delays and communication capabilities using a setup and results obtained from a real-world implementation study mentioned in [15].

2.1.5 Protocol Efficiency of DNP3 over TCP/IP

A communication protocol is considered to be efficient if it has minimum redundancy of functions in its stack and incurs minimum network protocol overhead in transferring a packet from its source to destination. In this regard, there is an immediate concern in improving the efficiency of the DNP3 protocol used to communicate messages between power devices. The DNP3 protocol has a Data Link Control layer of its own as shown in Figure 2.1 that divides the DNP3 fragments into frames of 250 bytes before passing it to the TCP/IP stack. It does error and frame control functions along with CRC check at its own Data Link layer. However, the TCP/IP protocol suite has its own Data Link Control
layer that does the same functions as the DNP3 DLC layer. Hence, there is some order of redundancy that decreases the efficiency of the overall application to some extent by incurring an additional delay due to DNP3 DLC layer on the user-space side. However, if the DNP3 transport layer functionality is combined with the TCP/IP transport layer and data link functionality combined with the TCP/IP DLC layer, it may improve the protocol and application efficiency of substation automation applications, at least for the ease of simulations.

DNP3 message packets are small in length and carry 'time critical' power information. For simulation purposes, we mimic the DNP3 layer structure by encapsulating DNP3 mes-
sage bytes in IP packets and handling their processing directly in the TCP/IP Transport and Data Link layers. This is achieved at the cost of lowering the Maximum Transmission Unit (MTU) of the path over which the DNP3 frames are passed. We adopt the lowering path MTU method to handle DNP3 protocol functionality, only for simulation purposes and do not claim it as any new implementation of DNP3 protocol stack. We assume lowering path MTU can serve our purpose to pass DNP3 messages by eliminating the DNP3 Data Link layer operation with a goal to achieve better delay results. Work has been done previously to improve the network throughput in power line networks (PLC) by lowering the path MTU in [25].

The disadvantage of having a lower MTU is that the fragmentation of IP packets at the Network layer of the TCP/IP suite may increase. However, it provides a way to improve application efficiency by shifting the DNP3 message processing functionality, previously occurring at the DNP3 DLC layer, deep into the TCP/IP protocol stack. IP layer divides the packets into smaller size if the path MTU is smaller than the Maximum Segment Size (MSS) at the transport layer. This technique works for our simulations due to the fact that the DNP3 messages are small themselves and so the number of IP fragments created to transfer the entire DNP3 message will not be too large. The protocol efficiency might come however, at the expense of increased network overhead[25][8][16].

2.2 IEEE C37.1-2007 and IEEE 1646-2004 Overview

There are a number of standard bodies, committees and commissions all over the globe today who contribute towards the development of the Smart Grid vision in some or the other aspect of survey, design, development, implementation as case may be. Some of the important standards relevant to the design of substation automation networks
Among above mentioned standards that are closely related to our field of study, we make use of the guidelines mentioned in IEEE C37.1-2007[4] for identifying, designing and building the communication blocks of our end to end substation automation network. This IEEE standard provides excellent resources and information regarding the different pieces of a communication network inside a substation, encourages a distributed processing approach as against to a centralized approach, and most importantly offers us a way to identify the different types of devices/sub-systems that interface with each other and kinds of communication interfaces we need to design to connect them in order to create our network topology. However, the design guidelines given in this standard is just a subset of many other guidelines furnished in this standard. We will use limited information from this standard and keep it restricted to design of a communication network.
Another major standard in consideration is the IEEE Standard for Communication Delivery Time Performance Requirements for Electric Power Substation Automation namely IEEE 1646-2004[5]. This standard provides a way to identify the different types of messages being exchanged between power devices inside and outside a substation. Further, it summarizes a list of information types exchanged between devices and puts an upper bound time value on delivering these messages to their respective destinations.

2.2.1 Use of IEEE C37.1-2007 Standard

The primary purpose of this standard is to provide guidance to the engineer responsible for the design and specification of SCADA and automation systems. It encourages the use of substation integration techniques to connect IEDs together using one or more communication networks. Once the substation IEDs are integrated together, it is then possible to accomplish substation automation.

In our thesis study, we have made multiple references to the substation communication diagram described by this standard shown in Figure 2.2. It provides a basis for our work to identify the various components we need to design and model our use-cases. It is an example of a substation automation system with all IEDs on a substation LAN. As IEDs are shown to have added network ports, as shown in Figure 2.2, remote and local access to IEDs can now be accomplished over the substation LAN. In Figure 2.2, the connection from the substation to the Energy Management System (EMS) and other users at engineering work stations is through a WAN. The connection from the WAN to the substation LAN is through a router and firewall. The data is stored in a data concentrator that has its own database (not shown in figure).
2.2.2 Use of IEEE 1646-2004 Standard

IEEE 1646 is a specification of communication delivery time performance requirements, other than for timesynching; it does not specify an underlying protocol nor does it specify the data model used to exchange information. End users must consider the bandwidth available for communication within an electric power substation, between substations, and between substations and other entities.

IEEE 1646 defines the following 8 information types to describe typical time delivery requirements as shown in Figure 2.3. All the results obtained and simulation model scenarios modeled in this study have this standard as reference to achieve application latency values within the upperbound specified by this standard.
2.3 Terminologies and Definitions

In this work, we have considered designing an end to end network topology for modeling substation automation use-cases. In this respect, we have referred IEEE C37.1-2007 standard design guidelines [4] to design our topology. However, before we introduce our topology in the next chapter, we will discuss a few terminologies and system definitions that we have used and referenced in the upcoming chapters. We have divided these terms and definitions into three categories based on the type of term we define. These categories are namely 'Devices', 'Networks' and 'DNP3 and related applications'.

Classification of Device Types: A list of device definitions for understanding the communication network topology in chapter 3.

1. Intelligent Electronic Device or IED: An Intelligent Electronic Device (IED) is a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers, and

<table>
<thead>
<tr>
<th>Information Types</th>
<th>Internal to Substation</th>
<th>External to Substation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Information, high-speed</td>
<td>1/4 cycle</td>
<td>8-12 ms</td>
</tr>
<tr>
<td>Monitoring and Control Information, medium-speed</td>
<td>16 ms</td>
<td>1 s</td>
</tr>
<tr>
<td>Operations and Maintenance Information, low-speed</td>
<td>1 s</td>
<td>10 s</td>
</tr>
<tr>
<td>Text Strings</td>
<td>2 s</td>
<td>10 s</td>
</tr>
<tr>
<td>Processed Data Files</td>
<td>10 s</td>
<td>30 s</td>
</tr>
<tr>
<td>Program Files</td>
<td>60 s</td>
<td>10 min</td>
</tr>
<tr>
<td>Image Files</td>
<td>10 s</td>
<td>60s</td>
</tr>
<tr>
<td>Audio and Video Data Streams</td>
<td>1 s</td>
<td>1 s</td>
</tr>
</tbody>
</table>

Figure 2.3: Information Types in Substation Automation [5].
capacitor banks. It is an embedded computer with limited RAM, limited CPU speed and runs on an Operating system such as Linux.

2. Supervisory Control and Data Acquisition System or SCADA: SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. In the physical form, this is a piece of software that runs on a laptop/computer that monitors data coming from an IED or polls the IED for data periodically.

3. Integrated Volt/VAR Controller: Integrated Volt VAR Control (IVVC) is an advanced SD function that determines the best set of control actions for all voltage regulating devices and VAR control devices to achieve a one or more specified operating objectives without violating any of the fundamental operating constraints (high/low voltage limits, load limits, etc.). An IVVC application in our work is assumed to be modeled to run on an embedded computer with limited RAM, limited CPU speed and hosted on a Linux platform. It is a server-side software application.

4. Data Concentrator or DC: A Data Concentrator converts input data from one form to another before outputting to one or more locations. Typically this function would be performed by a unit which takes a diverse assortment of discrete, analog and digital inputs to process and format them into other common digital data formats. It is an IED with varying communication and processing capabilities. A router with enhanced processing capability can also be a data concentrator as considered in this study.

5. Capacitor Bank Controller: A capacitor bank controller is a server side application
running on an IED that is monitoring the voltage on a substation bus. Whenever the voltage on a substation bus goes above or below a preset threshold value, the CB controller will either add/remove one or more capacitor banks to increase/decrease effective reactance to cancel out surges and stabilizes the voltage on the bus again. A CB controller application in our work is assumed to be modeled to run on an embedded computer with limited RAM, limited CPU speed and hosted on a Linux platform. It is a server-side software application.

6. Load Tap Changer or LTC Transformer: An LTC is a server side application running on an IED that is monitoring the position of a transformer tap on a distribution transformer. When the voltage on the substation bus goes above/below the set threshold, the LTC IED has programmed control logic to accordingly lower/raise the position of the transformer tap to reasonably lower/increase the voltage on the bus to stabilize it once again. An LTC application in our work is assumed to be modeled to run on an embedded computer with limited RAM, limited CPU speed and hosted on a Linux platform. It is a server-side software application.

7. Domain Gateway: Domain GW is in effect an IP router that may be equipped with a firewall software. This router is the default gateway router for all the network devices inside a substation to get on to a wide area network and go communicate with the outside world.

8. PC Clients: This can be any workstation or host inside or outside a substation network for data communication and file transfer. It is a client side device.

**Classification of Smart Grid Networks** A list of network type definitions for understanding the designed network topology.
1. Local Area Network (LAN): A LAN is a network normally designed for a limited geographical area, such as a utility substation or an office area. Segments may also be added to accommodate passing messages over distances exceeding the basic messaging distance inherent in the media. Serial networks can often be implemented over a LAN by embedding the serial messages in a network protocol[4]. In our work, a LAN will be modeled using an Ethernet switch with other devices.

2. Wide Area Network (WAN): A WAN provides long-distance transmission of data, voice, and image and video information over a large geographical area. WANs connect LANs together. In our work, a WAN is modeled using a mesh of routers in the internet domain. The WAN delay models the packet processing delay inside a wide area network.

3. Field Area Network (FAN): The Field Area Network is a two-tier communication network for the electric distribution grid supporting use cases such as advanced metering infrastructure (AMI)[11][29][19], distribution automation (DA)[16], distributed generation (DG), and workforce automation.

4. Process level LAN: This refers to a Ethernet connection between CT/VT merging units that provide sampled values of current and voltage to the LAN. The speeds associated with these LANS are in the range of 1 - 10Gbps.

5. Station level LAN: This refers to LAN connection between top level devices like SCADA master and other PC clients and IED all at the same level.

**Classification of DNP3 and related applications** A list of DNP3 related definitions for understanding the designed network topology.
1. Distributed Network Protocol (DNP3): DNP3 is a protocol for transmission of data from point A to point B using serial and IP communications. It has been used primarily by utilities such as the electric and water companies, but it functions well for other areas. It is the language that embedded computers (IED) understand to talk to each other. DNP3 is a non-proprietary protocol that is available to anyone by visiting the web site www.DNP3.org. DNP3 has its own application, pseudo transport and data link layer. DNP3 Link layer frames are embedded into TCP/IP packets[3].

2. Unsolicited Reporting or Report by Exception[3]: This is a mode of operating where the outstation spontaneously transmits a response without having received a specific request for the data. Not all outstations have this capability. This mode is useful when the system has many outstations and the master requires notification as soon as possible after a change occurs. Rather than waiting for a master station polling cycle to get around to it, the outstation simply transmits the change. In our work, we have modeled an unsolicited reporting use-case as one of our applications.

3. Event Driven Polls or Class Polls[3]: In DNP3, object groups, and the data points within them, can be further organized into classes. This provides an efficient method of requesting data; a simple (and small) message can be sent to request all data in a specific class (referred to as scanning for class data). There are four classes defined in DNP3.

   Class 0 represents all static (not change event data), whereas classes 1, 2, and 3, represent different priorities of change event data. For each class data response, only the class data that has changed will be returned, keeping the response messages small and efficient.
Finally, to acquire data not associated with either class 1, 2, or 3, an integrity poll, consisting of a class 0 scan, would be performed. Because of the possibly large amount of data that will be returned in a class 0 scan, it may not be terribly efficient and should be performed as least often as possible. In other words, a class 0 scan data response is largest since more number of DNP3 points will be recorded in this scan response message. In our work, we have modeled an event reporting use-case as one of our applications.

2.4 Taxonomy of Communication Interfaces

Based on the survey and literature study of requirements and challenges described in this chapter up to now, we present a high level overview of how communication data flows in a typical smart grid network in Figure 2.4. Looking at Figure 2.4, we observe the following characteristics of any communication network designed for smart grid applications:

- The Smart Grid communication network will be HUGE. That is, it will consist of network of many other networks with thousands of routers and other network devices with millions of interfacing communication links.

- In order to implement two-way communications in a smart grid or rather substation automation application, as in our case, prime importance needs to be given to the design of a network topology due to co-existence of numerous devices and connections in a mesh form.

- Physical and Logical communication links exist in any network as seen from the dark and dotted lines in Figure 2.4.
• A single application between two power IED’s may span long geographical locations. In other words, two IED’s in two remote substations will be geographically dispersed but still need to be integrated for network connectivity and data communications.

• The network topology design can be efficient and easy to understand only if we are aware of the different data flows that exist in an application. In other words, we need to be aware of what kinds of data transfers need to happen between which end points.

In lieu of the above mentioned reasons and many more, we are motivated to construct a taxonomy of communication interfaces that can be used to identify and understand the type of connections existing between any two communication endpoints in a smart grid application.
In this section, we have made a distinct classification of different types of communication links that can exist between any two actors/devices that want to communicate with each other. These links can be one of three types namely:

1. Direct Links: These are shown as dark lines. The two actors of interest are directly connected to each other.

2. Virtual or Logical Links: These are shown as dotted lines. The two actors of interest are not directly connected. They may communicate as endpoints and there will exist other network devices between them like routers, switches, other intermediate devices and so on.

3. Aggregated Links: These are shown as big and fat arrows. These arrows represent a logical pipe through which all the communication data passes between one domain and another domain. For example, all the outgoing connections from one substation can be grouped using one single arrow at the domain gateway router to represent the aggregated flow of communications from this substation to another. Aggregated flows has helped us to understand the communications flow in a more systematic manner due to reduced number of links to be considered at a high level study of an application.

For example, in Figure 2.5, the link between a data concentrator and an IED is represented as a two-way direct physical link shown in bold red, whereas a link between an IED and the WAN gateway is represented as an aggregated flow shown as a big fat pipe that is carrying many other connections from inside of the substation going outside to possibly other domains via the domain gateway.
Communications in Distribution Domain (Substation)

Figure 2.5: Communication network connections in Distribution domain.
Figure 2.6: Taxonomy of Communication Devices and Interfaces.
In the Figure 2.6, we have summarized our study of communication devices and interfaces in designing a communication network for smart grid communications. This classification is based on our discussion in this and the previous section. Finally, we present a schematic representation showing the flow of communication data between the various actors/blocks in the distribution domain in Figure 2.5. Similar diagrams can be constructed for understanding communications flow in other domains using the interface taxonomy. These interfaces are modeled in software using OMNeT++ tool and can be modified in OMNeT++[30].

This section concludes our study on the various challenges and mandatory requirements that we will come across at any time in the process of designing an end to end communication network for any application in a Smart Grid domain. In our study, we will utilize the communication architecture shown in Figures 2.2 and 2.5 as frameworks to design our substation automation network topology.
Chapter 3

Communication Architecture for Substation Automation

In this chapter, we introduce the design of an end to end communication network topology. We use this topology and model it in the chapter 4 using the open source OMNeT++ discrete simulation software[30] and the INET framework in OMNeT++.

In this phase of our work, we define three substation automation use-cases served by the designed communication architecture in the next section. These use-cases are chosen for our study because each one of them strives towards a common goal of satisfying the latency bounds on different priority messages exchanged in substation automation networks. Hence, they serve as an effective test bed for our study. These use-cases involve exchange of highly time critical ‘Protection’ messages, high priority ‘Control Action’ messages and medium to low priority ‘Administrative and State Reporting’ messages.

We discuss the functions of each subsystem used in this topology, further discuss the hardware and software specification of the devices used in our network, present the end to end communications flow for each use-case. Next, we discuss the communication protocol
stack at each device participating in the substation automation application we choose, and finally present our simulation model described in great depth in chapter 4.

The communication topology we suggest in this chapter can be applied to any of the three use-cases that follow in the next section. It is because of the very similar nature of communications flow and highly similar set of device functions in each of the three use-cases. We discuss a network topology that models communication operations for the following use-cases namely: Voltage Regulation on substation bus using Capacitor Bank Control; Voltage Regulation on substation bus using Load Tap Changer (LTC) Transformer and Load Balancing of Electric load between two transformers.

### 3.1 Three Substation Automation Use-cases

**Volt/VAR Regulation using Capacitor Bank Control**  
In capacitor bank control, the automation system optimizes the voltage and inductive load on a line or bus by connecting or disconnecting one or more capacitor banks. It prevents the imaginary part of the load from becoming too large, reducing voltage and the efficiency of the system. The banks may be widely located across the power system, or within the substation.

In distributed Volt/VAR control, one IED controls one capacitor bank on a given line, and each IED makes switching decisions individually. In centralized Volt/VAR control, each IED reports monitored values back to a Substation Computer. The Substation Computer may make switching decisions based on averages or groupings of voltages. When it decides a switch is necessary, it sends a control message to the appropriate IED, which may or may not be the device reporting the controlled measurements.

The communication network setup for the above mentioned use-case can be seen in Figure 3.1. This figure shows the connections from the deepest levels, right from the
CT/VT merging units in the switchyard back to the top level control center that is operating SCADA. The IED’s used to monitor the capacitor banks are Digital Capacitor Controller IED’s. Figure 3.1 has been modified to illustrate this scenario effectively. The original diagram can be found at the RuggedCom.com website which is a Siemens business.

**Voltage Regulation using Tap Changers** In voltage regulation, the automation system ensures a constant voltage on the substation bus by adjusting the tap of one or more transformers. A monitoring IED provides a voltage value to the Substation Computer, which has been programmed with threshold and hysteresis logic. The IED is usually monitoring the bus side of a transformer. In more complex situations, IEDs may monitor multiple voltages throughout the station and pass them all to the Substation
When the logic indicates that the bus voltage must be adjusted, the Substation Computer issues a control operation to the IED connected to the transformer tap. This will change the monitored voltage, which will be fed back through the logic. The voltage control logic typically has a pre-programmed qualification delay in the tens of seconds adjusting the tap causes wear on the equipment, so adjustments should not be made lightly. Therefore, an appropriate update time for the monitored voltage is on the order of one-half second to one second.

Because of the wear on the transformer and tap, and the impact on the rest of the system if adjusted wildly, tap raise/lower operations are typically performed with select-before-operate logic. Redundancy and reliability of the communications path is important. Figure 3.2 has been modified to illustrate this scenario effectively.
**Load Balancing between two transformers**  Load balancing is typically a distribution operation, performed between two transformers within a substation, but may also be performed in transmission systems between substations. In the distribution case, two feeders serviced by separate transformers are connected at their remote ends by a normally open switch. A pole-top IED controls the switch. Other IEDs monitor load on the line. The IEDs report the state and load of the system to a Substation Computer. The Substation Computer detects the condition when one transformer is heavily loaded and the other has excess capacity, and sends a message to the pole-top IED to close the switch. Now, instead of one line loaded at 90% and the other at 25%, both may be loaded at 50%. Figure 3.3 illustrates this power system use-case scenario condition.
3.2 Design of Communication Architecture for Substation Automation Networks

In order to model the communications network that handle and perform communications related tasks for the above mentioned three substation automation use-cases, we discuss our design of the end to end communication model shown in Figure 3.4 showing Substation Site 1 and Figure 3.5 showing Substation Site 2.

**Scenario Overview**  In this part, we briefly describe the overview of the communication system in Figures 3.4 and 3.5. In this system, there are mainly two substation sites that are located remotely, say Site 1 and Site 2. Site 1 substation houses a subsystem that models the functions of use-case 1 mentioned above in which we are monitoring voltage on a substation bus using tap changers. Site 2 hosts a subsystem that models the functions of use-case 2 mentioned above in which we monitor the total load voltage on substation bus and adjust the load by adding/ Removing one or more capacitor banks.

The two substation sites are separated by using a WAN cloud. The WAN cloud is modeled as a mesh of 10 IP routers and a packet processing delay component in each router. Site 1 has a SCADA master application that monitors the first of the two LTC IED that controls the tap position on the voltage transformer. A data concentrator aggregates all the data before communicating with the outside world using the domain gateway router. A second LTC IED is used for monitoring the voltage DNP3 points on the transformer.

Site 2 also houses a SCADA master control center station. This SCADA computer is assumed to monitor systems operating in both sites. The master SCADA also monitors the Integrated Volt/VAR application explained in the previous chapter. The IVVC
controls the digital capacitor controller which in turn is connected to capacitor banks as shown in Figure 3.1 in previous section. The second M6280A IED is shown for redundancy and for use in times of failure as redundancy is most important in designing any application as specified by NIST[6][10] in design guidelines for a communication topology.

**Functional Definition of Sub-systems used** In the communication architecture shown in Figures 3.4 and 3.5, there are a total of 4 main subsystems that communicate with each other as and when needed to stabilize the voltage conditions on the line/bus inside their respective substation sites. These 4 subsystems are namely Load Tap Changer subsystem, Capacitor Bank Control subsystem, Integrated Volt/VAR application subsys-
tem and the SCADA master control center subsystem as shown in Figures 3.6 through 3.9. Table 3.1 summarizes the activities and functions handled by various power devices and network components inside the 4 subsystems.
Figure 3.6: Load Tap Changer Subsystem: Site 1.

Figure 3.7: Capacitor Bank Control Subsystem: Site 2.
Figure 3.8: Integrated Volt/VAR Control Application Subsystem: Site 2.

Figure 3.9: SCADA Master Station Subsystem: Site 1, 2.
Table 3.1: Functional Definitions of Subsystems: Site 1,2

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTC control</td>
<td>1. Responsible for lowering/raising the tap of the transformer&lt;br&gt;2. Regulates the voltage on the substation bus in Site 1&lt;br&gt;3. IED monitors the voltage on the bus and reports a change to the SCADA master</td>
</tr>
<tr>
<td>Capacitor Bank control</td>
<td>1. Regulates the voltage levels on the substation bus and cancels reactive component in load to correct power factor&lt;br&gt;2. IED monitors the voltage on the bus and reports a change to the SCADA master in Site 2&lt;br&gt;3. Gateway router aggregates the data at the subsystem gateway</td>
</tr>
<tr>
<td>Integrated Volt/VAR control</td>
<td>1. The internal control logic is tuned to control the value of voltage on the substation bus&lt;br&gt;2. Takes control action decisions to change voltage settings on the bus by informing the digital capacitor controller IED to add/remove banks&lt;br&gt;3. Sends control action reports to main SCADA master within Site 2</td>
</tr>
<tr>
<td>SCADA master and main master</td>
<td>1. Monitors the data sent by all other subsystems including the LTC system, Capacitor Bank system and so on&lt;br&gt;2. Polls the LTC IED and Capacitor Bank IED for DNP3 data at regular intervals and also checks the health of these IEDs using Integrity polls&lt;br&gt;3. Issues control commands to configure these IEDs in times of emergency</td>
</tr>
</tbody>
</table>
Hardware, Software and Communication Specifications  In our work, we only model the communication capabilities of IEDs used in our work with those in real world. For the Digital Capacitor Bank Controller IED, we use the Beckwith M6280A Digital Capacitor Control IED device communication capabilities and model them in our simulation model. Next, we use Beckwith M2001D Load Tap Changer (LTC) IED and model its communication capabilities in our simulations. As hardware specifications for these IED’s, we have used the work in [15] and considered the specifications of similar IEDs used in this work. The hardware, software specifications and communication specifications and device features supported by our chosen IEDs are summarized in Table 3.2.

Communication Specifications of M6280A  The following communication interfaces are available with this M6280A IED in real world:

- Protocols: The standard protocols included in the M-6280 are DNP3.0 and MODBUS. The USB port uses MODBUS for local communications. The optional Ethernet Port supports DNP3.0 and MODBUS protocols simultaneously.

- Optional Ethernet Port: The optional Ethernet Port provides an RJ-45 (10/100 Base-T) or a (100 Base-Fx) Fiber Optic interface for ethernet communication to the M-6280. The protocols supported are: MODBUS over TCP, DNP3.0 over TCP and DNP3.0 over UDP.

- Optional Bluetooth: The optional Bluetooth provides wireless access to the M-6280. With Bluetooth the user is able to configure the control, read status and metering values as well as change setpoints. This feature can not be ordered with RS-232 as they share the same input to the control.
• COM2 (top), RS-232 and optional Bluetooth (user selectable if Bluetooth is installed)

• Communication Protocols include DNP 3.0, MODBUS and IEC-61850 (IEC-61850 only available with optional Ethernet port)

**Communication Specifications of M2001D**  The following communication interfaces are available with this IED:

• Ethernet Port COM3 (10/100 BaseT) is available through a RJ-45 jack or ST Fiber on the top of the control. This port supports DNP over TCP/IP, MODBUS over TCP/IP, and IEC-61850 over TCP/IP

• Local Wireless Bluetooth capability

• COM1 (top), RS-485 and Fiber Optic Port (ST and V-pin connectors available with 62.5 and 200 microfiber supported)

• COM2 (top), RS-232 and optional Bluetooth (user selectable if Bluetooth is installed)

• Communication Protocols include DNP 3.0, MODBUS and IEC-61850 (IEC-61850 only available with optional Ethernet port)

### 3.3 Communication Sessions and Protocol Stacks

This section describes all aspects of our communication architecture which establishes two-way communications between two remotely located substation sites. The substation Site 1 hosts an internal Load Tap Changer subsystem based automation scenario to
Table 3.2: Hardware and Software Specifications of IEDs and Computers

<table>
<thead>
<tr>
<th>Device</th>
<th>CPU</th>
<th>Memory</th>
<th>Kernel Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cap Bank Controller M6280A</td>
<td>ARM 200MHz</td>
<td>64MB</td>
<td>Linux 2.4.26</td>
</tr>
<tr>
<td>LTC Controller M2001D</td>
<td>ARM 500MHz</td>
<td>128MB</td>
<td>Linux 2.6.21</td>
</tr>
<tr>
<td>SCADA Control Center</td>
<td>P4 1.66GHz</td>
<td>1GB</td>
<td>Linux 2.6.32</td>
</tr>
</tbody>
</table>

protect the voltage on the substation bus. In a similar way, the substation Site 2 houses internal Digital Capacitor Bank subsystem that maintains the regulated voltage on the substation bus in Site 2. Site 1 and Site 2 are physically and logically separated from each other using a WAN cloud. The WAN cloud is modeled as a mesh of 10 IPv4 routers in this work.

**Communication Sessions** Due to a number of communication flows that exist between two or more devices to communicate with each other, we have tabulated a list of communication sessions that are maintained between endpoint devices in Table 3.3. These sessions help us to understand the source and destination devices for a particular communication data flow and to pass TCP/UDP signals between them while modeling an application running on them.

For example, in Figure 3.7, it can be seen that the M6280A IED and IVVC are two communication endpoints that are exchanging time-critical power information and hence there exists a TCP session between them as shown as the first entry in Table 3.3. Similarly, there exists another communication session between remotely located M2001D in Site 1 and Main SCADA master control center in Site 2. This session means that these two devices are connected logically and many more physical devices exist between them.
Table 3.3: TCP Communication Sessions across Site 1 and Site 2

<table>
<thead>
<tr>
<th>TCP Session</th>
<th>Source</th>
<th>Destination</th>
<th>Session housed in</th>
<th>Information Type conveyed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session 1</td>
<td>M6280A</td>
<td>IVVC</td>
<td>Site 2</td>
<td>Protection Information</td>
</tr>
<tr>
<td>Session 2</td>
<td>IVVC</td>
<td>M6280A</td>
<td>Site 2</td>
<td>Control Information</td>
</tr>
<tr>
<td>Session 3</td>
<td>IVVC</td>
<td>Main SCADA master</td>
<td>Site 2</td>
<td>Event Report</td>
</tr>
<tr>
<td>Session 4</td>
<td>Main SCADA master</td>
<td>M6280A</td>
<td>Site 2</td>
<td>Event Monitoring</td>
</tr>
<tr>
<td>Session 5</td>
<td>SCADA Master Station</td>
<td>M2001D</td>
<td>Site 1</td>
<td>Integrity Polling and Event Monitoring</td>
</tr>
<tr>
<td>Session 6</td>
<td>M2001D</td>
<td>SCADA Master Station</td>
<td>Site 1</td>
<td>Protection Information</td>
</tr>
<tr>
<td>Session 7</td>
<td>M2001D</td>
<td>Main SCADA master</td>
<td>Site 1 and 2</td>
<td>Event Report</td>
</tr>
<tr>
<td>Session 8</td>
<td>Other host (not shown)</td>
<td>Other host (not shown)</td>
<td>Site 1</td>
<td>Model additional traffic</td>
</tr>
</tbody>
</table>
**Device Protocol Stack**  The Intelligent Electronic Devices (IEDs) used in our topology mimic the communication capabilities of real world devices. In our design, we model such IED’s with communication ports as those available with Beckwith M6280A Digital Capacitor Bank Controller and Beckwith M2001 Load Tap Changer Controller. These devices are embedded computers and use a widely known device communication protocol called Distributed Network Protocol (DNP3) as explained previously in section 2.3 of chapter 2. More information about the DNP3 protocol working can be found in [13][15].

Note that in this study, we are not concerned with the internal information contents passed between one IED to another in the designed architecture. Instead, we focus on the 'End to End latency' of the application between communication endpoints to deliver time-critical information[5]. This information is passed using the DNP3 protocol information encapsulated in TCP/IP packets.

Figure 3.10 shows the DNP3 protocol stack inside any embedded computer that uses
DNP3 over TCP/IP to pass information to another computer and/or IED.

Figure 3.11 shows the communication protocol stack inside a M6280A IED. It has a combined DNP3 and TCP/IP stack. Such a stack applies to intelligent devices in the power domain like IEDs, SCADA Master and IVVC application.

In the substation Site 1, the communication protocol stack at each device that participates in a communication session to transfer information from the IED to the SCADA Master station is shown in Figure 3.12. The embedded computers that communicate important power information have a user side DNP3 stack plus an in-built TCP/IP stack, network devices like routers have only the IP stack, switches have the MAC and physical layers only. This type of classification at the protocol stack level gives an indication of a device’s functionality and communication capability.
Figure 3.12: End to End Communication Protocol Stack.
3.4 Modeling of Application Latency and End-End Delay in Substation Automation Networks

In the simulation model discussion in the next chapter with reference to the designed communication architectures shown in Figures 3.4 and 3.5, we evaluate the performance of Ethernet, Fast Ethernet, Gigabit Ethernet and Wireless technologies using TCP and UDP to measure a performance metric named Application Latency or AL of the entire substation automation application.

The metric *Application Latency* or AL is a composition of a number of different components of delays introduced at different levels of operations in the communication architecture. The various components of delay comprising the metric AL can be seen with Figure 3.13.
Figure 3.13: Delay Components: Application Latency.
**End to End Delay vs. Application Latency**  
End to End delay in substation applications is defined as the difference between the timestamp at which the necessary message is received by the Application layer of the receiving device and the timestamp at which the necessary message is first created at the Application layer of the sending device. This takes all the delay components encountered in the entire communication path from source to destination device into consideration.

If we define the delay components as follows: $T_{IED}$ is the delay incurred due to data acquisition delay, setpoints storage delay, CPU processing delay and protocol stack delay at the IED,  
$T_{prop}$ is the propagation delay at each path,  
$T_{trans}$ is the packet transmission delay at each path,  
$T_{proc}$ is the packet processing delay at each intermediate network device,  
$T_{proc-WAN}$ is the processing delay incurred in the WAN cloud of 10 routers and  
$T_{medium-access}$ is the medium access delay of the source device.

$$\text{End to End Delay} = T_{prop} + T_{trans} + T_{proc} + T_{proc-WAN} + T_{medium-access}$$ of the entire path + source(Network Protocol Delay) + dest(Network Protocol Delay)

Application Latency (AL) is defined the sum of End to End delay as defined above and additional delay components namely Data Acquisition Delay of the IED, CPU processing delay of the IED, the setpoints storage delay of the IED. These three delay components are an integral part of Application Latency and are an attribute of the hardware/software specifications of the IED under consideration and can be grouped under one delay called $T_{IED}$. This can be seen from Figure 3.13. Hence, AL is defined as, $AL = \text{End to End Delay} + T_{IED}$
Hence, finally, we represent Application Latency with the following formula:

\[ \text{AL} = T_{\text{prop}} + T_{\text{trans}} + T_{\text{proc}} + T_{\text{proc-WAN}} + T_{\text{medium-access}} + \text{source(Network Protocol Delay)} + \text{dest(Network Protocol Delay)} + T_{\text{IED}} \]

**Significance of Delay Components** Below we discuss the significance of each delay component in the end to end communication path that contribute towards the composition of Application Latency (AL) metric.

1. The data acquisition delay is the delay it takes to acquire the status of DNP3 points being monitored by an IED. It will increase with increase in number of points being polled by an IED. It will be largest in the case of an Integrity Poll response and smallest in case of an Unsolicited Report message. We have modeled it using a truncated normal random distribution in this work.

2. CPU processing delay comprises the time required to process the received information from the DNP3 points and to format the data obtained into semantics understood by the kernel before it creates the DNP3 message to be transmitted to other devices. We CPU processing delay modeled in our simulations follows a truncated normal distribution which can reasonably model the delay with these embedded computers as used in [31][32][33].

3. Setpoints storage delay comprises the delay component incurred due to storing the digital values of the DNP3 points measured in the internal memory of the IED. This component also depends on the hardware limitations of an IED.

4. Packet Processing Delay: Data is transmitted through a communication network by following the specified network protocols. Different layers of packet headers and
trailers are added, inspected, modified and removed along the transmission path taken by the packet[12].

5. Packet Transmission Delay: The current link layer mechanisms append a data integrity check field to each data frame to detect possible data errors. Every intermediate node on the packet transmission path verifies the data correctness after receiving the complete data frame and before forwarding the packet to the next relay node. Transmission delay is incurred on each link for the sending and receiving of the data frame[12].

6. Medium Access Delay: Multiple data sending nodes that share the same transmission medium, such as wireless spectrum and wireline cable, compete for the medium access in order to transmit their respective data. A packet in a node has to wait until all the other packets scheduled ahead have been cleared from the buffer[12].

3.5 Simulation Scenarios

We discuss the simulation setup, network configuration, software architecture and general assumptions in the next chapter by modeling the communication setup described in Figures 3.4 and 3.5 in OMNet++. We describe the detailed flow of communication from source to destination for each scenario. Each of the three scenarios that we simulate can be applied to any of the three substation use cases described in Section 3.1.

3.5.1 Scenario 1: Unsolicited Reporting in Site 2

In this scenario, the digital capacitor controller IED (M6280A) learns of an event of rise/fall of the voltage on the substation bus above/below a threshold from the monitored
values of the reactance on the bus. We will assume that the IED receives an emergency indication value from the connected capacitor banks.

- From this point, the M6280A IED will send an unsolicited report or an event report message to the Integrated Volt/VAR Application or IVVC indicating the need for an immediate action.

- Once the IVVC receives the unsolicited report from M6280A, it looks up its internal decision making logic and decides to take or not take an appropriate control action. This message is also referred to as an ‘control action’ message. In this case, a decision would be to add or detach a capacitor from the bus to reduce the reactance on the substation bus.

- It issues a command to add/detach a capacitor from the bus to the IED M6280A. At the same time, it also sends an ‘event control’ report to the main SCADA master control station in Site 2.

- The SCADA master finally asks for an updated ‘event monitoring’ report from the M6280A IED since its polled values may have changed after executing the ‘control action’ message received from IVVC.

The communication scenario can be seen in Figure 3.14. The sequence diagram 3.15 shows the above messages and the communication flow diagram for this scenario.

### 3.5.2 Scenario 2: Exception Scan in Site 1

The LTC IED M2001D is constantly monitoring the tap position of the transformer tap on the transformer. When the transformer is heavily loaded with load voltage on the
Substation bus exceeding a threshold value, the M2001D IED will inform of this condition to the SCADA master.

The SCADA master periodically polls the M2001D IED for either all its data (called an integrity poll) or a set of data points important for a particular application monitored by SCADA. Such a poll is called Class poll wherein it asks for Class 1, 2 and 3 event data. It may also perform an exception scan on the M2001D asking for data only if it has changed from the most recent scan. The exception scan and integrity scan are based on the exception scan rate and integrity scan rate specified by the SCADA master.

In this scenario, we have simulated the end to end delay profile for the Exception Scan or a Class poll message issued from the SCADA master to the M2001D LTC IED. The metric of interest in such a scenario is only End to End delay as against Application
Latency as defined in a previous section as this application is not a time critical application as the unsolicited reporting event (scenario 1). Also, in this case, the information exchanged between endpoints already exists at the application layer of the M2001D IED. The communication scenario can be seen in Figure 3.16. The sequence diagram 3.17 shows the above messages and the communication flow diagram for this scenario.

3.5.3 Scenario 3: Inter-Substation Event Monitoring and Reporting

The main SCADA master control station in Site 2 is the Master SCADA system for both sites as mentioned before in section 3.2.1. In such a case, any event that causes the values on the M2001D IED to change in Site 1 must be correctly reported to the
main SCADA master control station in Site 2 in a timely manner to maintain updated database. Since these two sites are remotely located, the DNP3 event reporting message will travel through a wide area network (WAN) before reaching Site 2.

- In this scenario, we assume a condition on the substation bus such that the value of voltage on the bus has exceeded a threshold value.

- This increase in voltage indicating that the transformer is heavily loaded triggers the need for a load balancing event in order to transfer some load onto the second transformer managed by the M2001D IED as explained in section 3.1.3.

- Hence, the SCADA master station issues a command to the M2001D second IED to close the load balancing switch shown in Figure 3.3.

- Now that the load is balanced between both the transformers and the second M2001D IED is in action, it needs to report its monitored point values to the
main SCADA master control station residing in Site 2.

- It creates a DNP3 unsolicited event monitoring message and sends it to Site 2 SCADA master via the domain gateway and the WAN.

- The performance metric of interest in this case will be the End to End delay from M2001D to the main SCADA master control center in Site 2.

The communication scenario can be seen in Figure 3.18 and the sequence diagram 3.19 shows the above messages and the communication flow diagram for this scenario.

In the next chapter we introduce our simulation model to model the three scenarios mentioned in sections 3.6.1 through 3.6.3 and evaluate the performance of using different communication technologies for them in combination with TCP and UDP. We also discuss the workflow of the software applications in OMNeT++ that we have modified and used
Figure 3.18: Inter-Substation Event Reporting between Site 1 and Site 2.

to model the above scenarios, the software architecture of the simulation model and finally summarize our phases of development with using OMNeT++ software[30].
Figure 3.19: Inter-Substation Event Reporting Sequence of Operations.
Chapter 4

Simulation Model

In this chapter, we introduce and present a detailed discussion of all the communication and software architecture aspects of the simulation model of the end to end communication architecture discussed in the last chapter in Figures 3.4 and 3.5. The organization of this chapter is as follows:

• Introduction and discussion of an end to end communication topology that models all the three scenarios explained in the previous chapter in sections 3.5.1 through 3.5.3.

• Discuss the workflow of the software applications that we use in our model to drive communication capabilities in these scenarios,

• Discuss the communication software architecture and end to end protocol stack used in our topology,

• Present a one to one network mapping between the nodes shown in Figures 3.4, 3.5 and the nodes we use in our simulation model and
• Present general assumptions before discussing the results and comparison analysis in the next chapter.

4.1 OMNeT++ and INET

OMNeT++[30] is an object-oriented modular discrete event network simulation framework. It has a generic architecture, so it can be (and has been) used in various problem domains:

• modeling of wired and wireless communication networks

• protocol modeling

• modeling of queueing networks

• modeling of multiprocessors and other distributed hardware systems

• validating of hardware architectures

• evaluating performance aspects of complex software systems

In general, modeling and simulation of any system where the discrete event approach is suitable, and can be conveniently mapped into entities communicating by exchanging messages. We have used the latest OMNeT++ 4.2.1 release for our simulation model.

For this study, we have built upon the existing software application programs provided by OMNeT++ and designed Network Description Files (NED files)[30] and Initialization/Configuration files (ini files)[30] for all of the scenarios and simulation runs presented in Chapter 5.
4.1.1 INET Framework

The INET Framework\cite{30} is an open-source communication networks simulation package for the OMNeT++ simulation environment. The INET Framework contains models for several wired and wireless networking protocols, including UDP, TCP, SCTP, IP, Ethernet, Serial PPP, 802.11a/b/g, OSPF, and many others.

The INET Framework builds upon OMNeT++, and uses the same concept: modules that communicate by message passing. The external interfaces of modules are described in NED files. NED files describe the parameters and gates (i.e. ports or connectors) of modules, and also the submodules and connections (i.e. netlist) of compound modules.

We use INET latest stable release 2.1.0 for modeling communication configurations between the application endpoints for the three substation automation use-cases discussed in the sections 3.6.1 to 3.6.3. We have modified the existing source code for the application layers in the INET framework to suit our needs and to simulate unsolicited reporting, class polling and inter-substation event monitoring reporting communication scenarios. Further, we model the communication interface bit rates described in section 2.5 in chapter 2 using the INET framework.

4.2 Simulation Model : OMNeT++

In this section, we introduce the simulation model corresponding to the communication architecture shown in the previous chapter in Figures 3.4 and 3.5. The model presented hereby in Figure 4.1 also shows the two remote substation sites with a WAN cloud separating the two sites.
Figure 4.1: Simulation Model of Communication Network.
One to One Network Mapping  To maintain a one to one mapping between the nodes used in the communication architecture introduced in the previous chapter and the simulation model in 4.1, we have tabulated a one-to-one mapping between the actors/devices in both the diagrams shown in 3.4, 3.5 and 4.1 in Tables 4.1 and 4.2.

For example, as seen in Table 4.1, the LTC controller IED in Figure 3.4 is represented as a simulation node named M2001D1 and M2001D2 in Figure 4.1. These both nodes represent the Load Tap Changer IED in real-world and simulation environments respectively. Similarly, as another example, the Digital Capacitor Bank Controller IED in Figure 3.5 corresponds to the simulation node named M6280A1 and M6280A2 in Figure 4.1. Such a mapping can be found in Table 4.1 and Table 4.2.
<table>
<thead>
<tr>
<th>Node in Site 1 (Figure 3.4)</th>
<th>Corresponding node in Simulation Model</th>
<th>Node Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Tap Changer Controller</td>
<td>M2001D1 and M2001D2</td>
<td>Load Tap Changer IED</td>
</tr>
<tr>
<td>Data Concentrator</td>
<td>dc</td>
<td>Router or IED with(out) extended capabilities</td>
</tr>
<tr>
<td>Internal Substation Router</td>
<td>internalSubstationRouter</td>
<td>IP router used in internal substation network</td>
</tr>
<tr>
<td>SCADA Master Station</td>
<td>SCADA Master Station</td>
<td>Master control center for Site 1</td>
</tr>
<tr>
<td>Ethernet Switch</td>
<td>StationBus</td>
<td>Substation Station LAN to connect top level devices</td>
</tr>
<tr>
<td>Integrated Volt/VAR Control</td>
<td>IVVC1</td>
<td>IVVC application for Site 1 (not used)</td>
</tr>
<tr>
<td>Load Tap Changer Transformer</td>
<td>tapChanger</td>
<td>LTC transformer used in Site 1</td>
</tr>
<tr>
<td>Additional Internet Traffic</td>
<td>internetTraffic[*] - workstation pair</td>
<td>To generate additional internet traffic</td>
</tr>
<tr>
<td>Domain Gateway Router</td>
<td>domainGateway</td>
<td>Domain or Default GW router for Site 1</td>
</tr>
<tr>
<td>Node in Site 2 (Figure 3.5)</td>
<td>Corresponding node in Simulation Model</td>
<td>Node Type</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Digital Capacitor Bank Controller</td>
<td>M6280A1 and M6280A2</td>
<td>Capacitor Bank Controller IED</td>
</tr>
<tr>
<td>Internal Substation Router</td>
<td>configRouter</td>
<td>IP router used to separate IVVC and M6280A networks</td>
</tr>
<tr>
<td>Main Master SCADA Control Center</td>
<td>MainControlCenter</td>
<td>Master control center for Site 2</td>
</tr>
<tr>
<td>Switch</td>
<td>stationbus</td>
<td>Substation Station LAN to connect top level devices</td>
</tr>
<tr>
<td>Integrated Volt/VAR Control</td>
<td>IVVC2</td>
<td>IVVC application for Site 2</td>
</tr>
<tr>
<td>Capacitor Banks</td>
<td>capBanks</td>
<td>Capacitor Banks in the switchyard used in Site 2</td>
</tr>
<tr>
<td>WAN cloud</td>
<td>wan[10]</td>
<td>Wide Area Network mesh of 10 routers</td>
</tr>
</tbody>
</table>
**Actors and Associated Roles:** In the developed communication topology shown in Figure 4.1, we have used actors/devices/network components similar to those shown in Figure 3.4 and 3.5. In this section, we summarize a complete list of these actors/devices/components utilized by our simulation model shown in Figure 4.1. We briefly mention the role of each actor/device/component used for our runs. These listings can be found in Table 4.3 and Table 4.4.

For example, M2001D IED in Site 1 functions include detecting and reporting any unusual power system voltage condition on the substation bus, back to the SCADAStation. Similarly, the main function of SCADAStation node is to monitor the M2001D and its associated DNP3 point values. It issues Exception Scan polls and Integrity polls to M2001D at regular intervals to maintain device and substation bus stability. Device roles can be understood in more detail looking at Table 4.3 and Table 4.4.
Table 4.3: Actors and associated roles: Site 1

<table>
<thead>
<tr>
<th>Actor in Simulation Model</th>
<th>Role</th>
<th>Quantity Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2001D</td>
<td>LTC Controller IED</td>
<td>2</td>
</tr>
<tr>
<td>SCADAMasterStation</td>
<td>SCADA that monitors all DNP3 applications in Site 1</td>
<td>1</td>
</tr>
<tr>
<td>dc</td>
<td>Data Concentrator node to aggregate all internal traffic and route it to domain GW</td>
<td>1</td>
</tr>
<tr>
<td>StationBus</td>
<td>Substation Station Bus to connect top level devices</td>
<td>1</td>
</tr>
<tr>
<td>internalStationBus</td>
<td>Substation Station Bus to connect IEDs and internal router</td>
<td>1</td>
</tr>
<tr>
<td>internalSubstationRouter</td>
<td>Internal IP Router to keep IEDs and top level devices on different networks and route internal traffic to data concentrator</td>
<td>1</td>
</tr>
<tr>
<td>wan[10]</td>
<td>Mesh of 10 IP routers over which the message traverses while sending from Site 1 to Site 2</td>
<td>10</td>
</tr>
</tbody>
</table>
### Table 4.4: Actors and associated roles: Site 2

<table>
<thead>
<tr>
<th>Actor in Simulation Model</th>
<th>Role</th>
<th>Quantity Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterControlCenter</td>
<td>Main SCADA Control Center managing Site 1 and 2</td>
<td>1</td>
</tr>
<tr>
<td>IVVC2</td>
<td>Integrated Volt/VAR application to control the configuration and values obtained from M6280A IED</td>
<td>1</td>
</tr>
<tr>
<td>M6280A</td>
<td>Digital Capacitor Bank Controller IED used to stabilize voltage on substation bus</td>
<td>2</td>
</tr>
<tr>
<td>stationBus</td>
<td>Substation Station LAN to connect the top level devices</td>
<td>1</td>
</tr>
<tr>
<td>configRouter</td>
<td>IP router used to keep IVVC control application and M6280A Controller IED on different networks</td>
<td>1</td>
</tr>
</tbody>
</table>
4.3 Simulator Application : Scenario 1

The unsolicited reporting scenario inside a substation network requires the capacitor bank controller IED (M6280A), the Integrated Volt/VAR Application (IVVC) and the MasterControlCenter for SCADA to communicate with each other by using a latency-centric implementation and configuration. The messages communicated by each device to the other has a unique significance and priority type as shown in Figure 4.2. In this section, we introduce two software applications we have used in our simulations for communication amongst these three communication endpoints.

When the capacitor bank controller IED learns of an unusual voltage condition on the substation bus, it sends an alarm or 'protection' message to the IVVC application informing the need for urgent control action. To mimic this alarm message, we have used two software applications, one running on M6280A and other on IVVC endpoint. The type of message exchanged in this case is a protection message as defined by IEEE 1646-2004[5].

Next, the IVVC will look up its internal control logic and stores this condition in its local database. It then decides the control action needed and issues two messages, one control action message to M6280A and another 'event control' report to the MasterControlCenter for SCADA. This requires another two communication sessions between IVVC-M6280A pair and IVVC-MasterControlCenter pair.

Finally, the MasterControlCenter issues an 'event monitoring' request message to the M6280A IED asking for its newly polled DNP3 point values. This event requires a communication session between MasterControlCenter for SCADA and M6280A.

Note that we do not focus on the internal information content of a DNP3 packet. We are only concerned with the 'size' of the DNP3 message and the various 'delay com-
ponents’ involved at various levels of application workflow as defined in section 3.6 of chapter 3. This is a communications study and hence we are also not concerned with the actual voltage/current values that trigger these unsolicited reports. We will simply assume this condition has occurred and evaluate the application latency of ‘individual’ messages exchanged between these endpoints with a goal of stabilizing the substation bus.

**Scenario 1 : Client-side Application**  An IED that wants to send an event report or a DNP3 message to another IED or application, makes use of the software application flow shown in the left half of Figure 4.3. The DNP3 application layer creates DNP3 request messages which are passed on to a transport layer. The transport layer creates DNP3 fragments worth maximum 1024B and passes them to the IP network layer. The network
layer does the necessary fragmentation if MTU is less than the Maximum Segment Size (MSS) and passes these IP fragments to the Data Link Layer. The path MTU is set to 300 bytes in order to mimic and conveniently assume each 250B data in each fragment as a DNP3 data frame. The remaining 50 bytes will be consumed by the IP and TCP header. The client or source IED is tied to the socket endpoint port 1001 and server IED on port 2001.

The functions used in this client side software application can be seen in Figure 4.4. There are a total of 5 major functions that are responsible for the generating the messages of configurable sizes; count the number of bytes transferred; model the processing delay due to hardware limitations of the devices; accept all the important socket endpoint parameters like port number, local address, destination address and so on; and finally to
record the application latency and other application specific statistics. These 5 functions are as follows:

1. `count()` - to count the number of bytes passed from the DNP3 application layer.

2. `waitUntil()` - models the CPU processing delay at the client needed to process the data sent by upper layers and to store the data, by waiting in this state: models setpoints storage and CPU processing delay of the $T_{IED}$ component.

3. `genDataBytes()` - creates an IP packet object with requested number of bytes.

4. `activity()` - sends actual data bytes to the server and again calls `waitUntil` if server is not ready to receive requests: checks if the processing is complete before instantiating the protocol stack.

5. `finish()` - records all the statistics and the Application Latency of the message transfer.

**Scenario 1: Server-side Application** Any IED that receives an event report or a DNP3 message from another IED or application makes use of the software application shown in the right half of Figure 4.3. The DNP3 DLC layer accepts the 300 bytes frames arriving from the physical medium and creates the 250 bytes frames by stripping off the IP plus TCP headers. These 250 bytes frames are re-assembled by the transport layer to create the original DNP3 fragments worth maximum 1024 bytes. These fragments are re-assembled in totality to create the original DNP3 message sent by the source IED and passed upon to the server’s application layer to re-create the ‘Unsolicited Report’ message. The server or destination IED is listening on socket endpoint port 2001.
The functions used in this server side software application can be seen in Figure 4.4. There are a total of 3 major functions that are responsible for carrying out tasks at the server. These functions are defined as follows:

1. **initialize()** - to initialize the server specifics like the port, local address and TCP threads to communicate with an endpoint.

2. **handleMessage()** - handle incoming message requests and take appropriate actions based on incoming message types as shown in Figure 4.5.

3. **finish()** - records all the statistics and the Application Latency of the message transfer.
4.4 Simulator Application : Scenario 2

In substation Site 1, the LTC controller IED M2001D is hosting an application that controls the position of the tap of the LTC transformer to prevent voltage overloading on the substation bus. It is assumed to be monitoring voltage, current and tap status related DNP3 points on the LTC transformer.

In this scenario, the SCADAMasterStation node in Site 1 polls the M2001D LTC IED to check its network connectivity and to monitor all the points and its associated values acquired by the IED. The SCADA issues 'Integrity polls' after fixed time intervals called 'Integrity Scan rate'. Also, it polls the IED for Class 1, 2 or 3 data in which it can poll for specific alarming DNP3 points that are of high interest under the virtue of the
critical application. Such a scan is called Exception Scan and the polling interval is called ‘Exception Scan rate’. We measure the End to End delay in sending a poll request message from SCADA to M2001D and response message from M2001D back to SCADA. We repeat this test scenario by evaluating the performance of different communication interfaces designed previously seen in Chapter 2, like Ethernet 10Mbps, 100Mbps, 1000Mbps, IEEE 802.11 with Ethernet. All of these technologies are tested using both TCP and then UDP.

The software application looks similar that to Figure 4.3, with some additional configurable parameters like the Integrity Scan rate, Exception Scan rate, CPU processing delay, number of requests to be sent in one session and number of sessions. The simulator application flow can be seen in Figure 4.6.

In our study, we do not focus on the internal information content of a DNP3 packet. We are only concerned with the ‘size’ of the DNP3 message and the various ‘delay components’ involved at various levels of application workflow as defined in section 3.6 of chapter 3. This is a communications study and hence we are also not concerned with the actual voltage/current values that trigger these unsolicited reports. We will simply assume this condition has occurred and evaluate the application latency of ‘individual’ messages exchanged between these endpoints with a goal of stabilizing the substation bus.

**Scenario 2 : Client-side Application** On the client (SCADAMasterStation) side, the DNP3 application layer creates requests which are passed on to combined TCP/IP transport layer. It creates DNP3 fragments of maximum size 1024 bytes each and passes them to the network layer. The network layer does the necessary fragmentation if needed and passes these IP fragments to the Data Link Layer. The path MTU is set to 300 bytes in order to mimic the transmission of one 250 bytes DNP3 frame at a time. The
remaining 50 bytes are consumed by the IP and TCP header. The client or source IED is tied to the socket endpoint port 1001. Additionally, the application offers configurable parameters like the Exception Scan rate, server processing delay, number of requests per session and number of sessions. The left half of diagram 4.6 shows the client side application workflow.

The functions used in this client side software application can be seen in Figure 4.7. There are a total of 7 major functions that are responsible for carrying out tasks at the server. These 7 functions are defined as follows:

1. initialize() - to initialize polling application start time, end time and a timeout message to handle REQUEST message send time.
2. sendRequest() - to specify the length and random distribution of the REQUEST message and to specify the REPLY message length in bytes.

3. handleTimer() - handle incoming message requests and take appropriate actions based on incoming message types as shown in Figure 4.7.

4. socketEstablished() - to determine the number of poll requests in a session.

5. socketDataArrived() - to determine the time at which next REQUEST message is scheduled to be sent on receipt of the REPLY message.

6. socketClosed() - to determine the time instance at which a new session should be
opened with M2001D.

7. socketFailure() - this function sends a re-connect request to the server upon disconnection of the session between SCADA and server.

**Scenario 2 : Server-side Application**  
SCADAMasterStation receives a DNP3 Class poll REPLY message from M2001D LTC IED. The software application that sends this REPLY message is hosted on port 2001. This application works in synchronization with the client side application that sends the REQUEST message to M2001D. Upon extracting the DNP3 message, the application infers the length of reply packet expected by SCADA and processing delay it needs to model before sending a REPLY message. It also learns of the REPLY packet length and random distribution it is to use to create the reply packet. The right half of Figure 4.6 shows the server side application workflow for the DNP3 class polling communication scenario.

The functions used in this server side software application can be seen in Figure 4.8. There are a total of 5 major functions that are responsible for carrying out tasks at the server. These 5 functions are defined as follows:

1. initialize() - to initialize the REPLY thread and to model the processing delay specified in the client application.

2. sendOrSchedule() - to send the REPLY message when timeout of processing delay time is reached.

3. handleMessage() - to handle incoming message requests and take appropriate actions based on incoming message types as shown in Figure 4.8.
4. sendBack() - to send the REPLY to SCADA in an object and to keep track of number of bytes sent.

5. finish() - to record all the statistics and the Application Latency of the message transfer.

### 4.5 Protocol Software Architecture

The two software applications described in the Sections 4.3 and 4.4 satisfy the need of designing an end to end communication system for communicating unsolicited report messages and exception scan messages between respective endpoints as described in sections 4.3 and 4.4. The communication protocol used between such embedded computers
is Distributed Network Protocol or DNP3[3]. DNP3 runs over TCP/IP protocol suite to enable communication between nodes that convey information about power. Figure 4.9 shows the protocol stack on the communication endpoints due to the overlay of software applications on embedded devices as explained in sections 4.3 and 4.4.

The left half of Figure 4.9 shows the communication protocol stack within the M6280A IED and right half shows the stack within IVVC or MasterControlCenter. A similar stack can be assumed to be existing within M2001D IED - SCADA pair as well.

1. The top three components shown in blue represent the components of delay that will be incurred due to hardware limitations of the IED and before the DNP3 thread is instantiated inside the IED. At this point, the client IED opens its port 1001 to create the message object.

2. Once the DNP3 message is created at the DNP3 application layer of length $\leq 4096$ bytes, it is passed to the kernel as a combined DNP3 and TCP transport layer request.

3. The broken DNP3 fragment is then passed to the IP Network layer for further fragmentation since we set the path MTU to 300 bytes to mimic the transfer of DNP3 frames, only for simulation purposes.

4. Finally, the Data Link Layer creates DNP3 frames of 250 bytes and sends it out on the physical network.

5. The client side application is tied to the server side application using a TCP socket (and a UDP socket when using UDP as a transport solution).

6. On the server side, the DLC reassembles all the DNP3 frames to construct the
IP fragment after checking the CRC and performing error and frame control techniques. It passes IP fragments to the network layer.

7. The IP Network layer then reassembles the IP fragments to recreate the TCP segments/DNP3 fragments of size Maximum Segment Size (MSS).

8. The combined TCP and DNP3 transport layer then reassembles the DNP3 fragments to recreate the DNP3 unsolicited or class poll message and passes it up to the DNP3 application layer.

9. Destination device decodes this message and takes appropriate control or monitoring action after storing the relevant information in its local database, if needed.

4.6 General Assumptions

We have modeled all our simulations runs in OMNeT++ under certain general assumptions while configuring them. These assumptions must be kept in mind before modeling
any other application scenario that is built upon the present application layer code. We present these assumptions before discussing the simulation runs, results and comparisons in the next chapter.

- The internet connection between every participating endpoint never goes down and has a zero downtime.

- The application latency and end to end delay values obtained in the simulation results is contingent upon the fact that the hardware device specifications were chosen and modeled from a relevant study shown in [15].

- The simulation results will hold true only for messages that are generated using a truncnormal random distribution which is a popular message distribution used in the communication world. [31][32][33]

- truncnormal message distribution[30] format looks like (double mean a, double std dev b, int rng =0) where a is the mean value of the message size in bytes in our tests, b is the standard deviation of message size in bytes and rng is the internal random number generator value used to produce random numbers.

- The nodes in the simulation model are only modeled for their communication capabilities and do not measure actual power system values from power devices. They only mimic the operations of DNP3 over TCP/IP applications.

- The message sizes chosen in our simulation model (16,128,512,1024,2048 and 4096) bytes are assumed to be realistic and related to other works done in a similar area as [15][22][12][5].
• Whenever M6280A sends a message to IVVC, it is called an 'Unsolicited Report' or 'Report by Exception' message.

• Whenever IVVC sends a message to M6280A, it is called a 'Control Action' message.

• Whenever IVVC sends a message to MasterControlCenter, it is called an 'Event Control' report/message.

• Whenever MasterControlCenter sends a message to M6280A, it is called an 'Event Monitoring REQUEST' message.

• Whenever M6280A sends a message to MasterControlCenter, it is called an 'Event Monitoring REPLY' message.
Chapter 5

Simulation Results

In this chapter, we present the simulation results from all the runs that we conducted on the end to end substation network topology shown in Figure 4.1. In our view, the results obtained from the simulations serve as a starting point or provide an idea with choosing optimum communication technologies for certain specific types of messages exchanged between applications inside and outside of a substation automation network. Further, we summarize the results by tabulating combinational packages for the type of intelligent device used, optimum communication technology and mean of AL values obtained. Finally we will conclude this thesis study by discussing future work.

5.1 Scenario 1 : Unsolicited Reporting in Site 2

This section presents the results and analysis of running the simulation model for the ‘unsolicited reporting’ scenario only in substation Site 2 as described in section 3.6.1. The developed communication topology and corresponding simulation topology can be found in Figures 3.5 and 4.1 respectively.
All the simulations for the unsolicited reporting scenario are run for DNP3 message sizes with mean 16 bytes, 128 bytes, 512 bytes, 1024 bytes, 2048 bytes and 4096 bytes. In all we run the simulation for 6 different DNP3 message sizes and the simulation was repeated for each message size for 8 times. In total, 48 simulation runs generated results to obtain a reasonable mix of application latency mean values. The results presented for each message size is the averaged results for the corresponding 8 runs for that message size.

5.1.1 Source : M6280A Digital Capacitor Bank Controller

We summarize the application latency results obtained when source of a message in Site 2 is the M6280A IED in Table 5.1. It shows the results when M6280A sends 'Protection' messages to IVVC and 'Event Monitoring Responses' to MasterControlCenter. According to IEEE 1646-2004 standard[5], the protection messages have an upperbound of 4ms and event monitoring and control messages have an upperbound of 16ms within substation and 1 second outside the substation.

The results for Application Latency values are expressed as a range with the minimum value corresponding to DNP3 message size of 16 bytes and maximum value corresponding to message size of 4096 bytes. We observed the following details while measuring the Application Latency, when M6280A sends a 'Protection' message to IVVC and an 'Event Monitoring' message to the main SCADA control center in Site 2:

Effect of Communication Technology:

- For destination = IVVC, M6280A takes around 11.2ms to 16.04ms while using Ethernet 10Mbps links and around 11ms to 11.5ms when employing Ethernet 100Mbps links.
links between them to transfer critical protection information about overloading of voltage bus.

- For destination = MasterControlCenter, M6280A takes almost similar time of around 11.2ms to 16.04ms when using Ethernet 10Mbps links.

- From the values obtained while sending to IVVC, it is clear that Ethernet 10/100 Mbps cannot be used since the required upper bound for protection messages is 4ms.

**Effect of Delay Components:** The major delay components that affect these values are the delays in the IED due to its hardware and software limitations ($T_{IED}$). Since
M6280A has a slow processor speed with 200MHz frequency, the number of instructions it can execute per second is small. Hence it takes more cycles per instruction (CPI) to process, format and finally create a DNP3 message at the application layer of the protocol stack.

The IED hardware component of delay $T_{IED}$ does not change much between using Ethernet 10Mbps and 100Mbps. The network delay component however decreases the overall application latency in case of Ethernet 100Mbps as it uses faster link speeds.

**Possible Workarounds:** For sending protection information within specified time limits, there are some workarounds that can be employed. Firstly, the hardware specifications of the IED M6280A can be upgraded. This however increases the overall cost of the IED.
on the other hand. Another solution might be to use gigabit Ethernet (1Gbps) or fiber optic cable between M6280A and IVVC to reduce the network delay to a minimum. The protocol delay (DNP3 delay) component will decrease if the functionality of the DNP3 Data link layer is moved deeper into the kernel space as simulated in our tests, thereby removing redundancy in error and frame control mechanisms carried out at DNP3 DLC and TCP DLC layers.

**Effect of DNP3 Message Size:** The test scenario is run using DNP3 message sizes with mean 16B, 128B, 512B, 1024B, 2048B and 4096B. It is found that the size of the DNP3 messages does not make a significant difference to the overall value of Application Latency (AL). This is since the major component of latency is introduced by the limited hardware memory of the IED and slow processor speed of embedded computers and the additional delay introduced at the DNP3 Data Link layers. The application latency when source device is M6280A changes only by 0.5ms between smallest and largest DNP3 fragment size used in the case when technology used is Ethernet 100Mbps. DNP3 message sizes however have a bigger effect to the AL values obtained with Ethernet 10Mbps. The range of obtained values is 11 to 16ms for DNP3 sizes of 16B to 4096B respectively.
Table 5.1: Source of Communication: M6280A

<table>
<thead>
<tr>
<th>Destination</th>
<th>Technology Used</th>
<th>Transport Protocol</th>
<th>Message Type</th>
<th>mean(AL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IVVC</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Protection, High-Speed</td>
<td>11.2 - 16.04ms</td>
</tr>
<tr>
<td>IVVC</td>
<td>Serial+Eth10M</td>
<td>TCP</td>
<td>Protection, High-Speed</td>
<td>55.82 - 6071ms</td>
</tr>
<tr>
<td>IVVC</td>
<td>Eth100M</td>
<td>TCP</td>
<td>Protection, High Speed</td>
<td>11.02 - 11.5ms</td>
</tr>
<tr>
<td>MasterControlCenter</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Event Monitoring Response, Medium Speed</td>
<td>11.2 -16.04ms</td>
</tr>
<tr>
<td>MasterControlCenter (sent with IVVC)</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Event Monitoring Response, Medium Speed</td>
<td>11.18 - 20.3ms</td>
</tr>
</tbody>
</table>
The observed results for this scenario are summarized in Table 5.1 and associated graphs are illustrated using Figures 5.1 and 5.2.

### 5.1.2 Source: IVVC Integrated Volt/VAR Control Application

In this section, we summarize the results obtained when source of a message in Site 2 is IVVC in Table 5.2. Table shows the results when IVVC sends ‘Control Action’ messages to M6280A in response to and ‘Event Control reports’ to MasterControlCenter ‘protection’ messages. The observed results for this scenario are summarized in Table 5.2 and associated graphs are illustrated using Figures 5.3 and 5.4.

The results for Application Latency values are expressed as a range with the minimum value corresponding to DNP3 message size of 16 bytes and maximum value corresponding to message size of 4096 bytes. We observed the following details while measuring the Application Latency, when IVVC sends a ‘Control Action’ message to M6280A and an ‘Event Control’ message to the main SCADA control center in Site 2:

**Effect of Communication Technology:**

- For destination = M6280A, IVVC takes around 7.63ms to 24.52ms when using Ethernet 10Mbps links and around 86ms to 6800ms when employing Serial RS-232 interfaces with 9600bps baud rate links between them to transfer critical control action information to M6280A.

- When used with IEEE 802.11g WiFi + Ethernet 10 Mbps, with TCP transport protocol, the AL range is 6.69ms to 29.54ms, whereas it comes out as 6.46ms to 11.43ms when UDP is employed as a transport layer solution.

- For destination = MasterControlCenter, IVVC takes almost similar time of around
Figure 5.3: Source = IVVC, Dest=M6280A.

6.2ms to 11.04ms when using Ethernet 10Mbps links and 6 to 6.5 ms when using Ethernet 100 Mbps links.

From the values of AL obtained while sending to M6280A, it is clear that serial RS-232 links alone cannot be used since the required upper bound for protection messages is 4ms. Also, Ethernet 10 Mbps is not a viable option for larger DNP3 fragment sizes $\geq 1024$ bytes. IEEE 802.11g Wifi can be used to transmit control action information with regards to the AL value obtained for this case. However, such a combination can be used to send medium and low priority messages since the performance of UDP will worsen in heavy load conditions.
Effect of Delay Components: IVVC performs better than M6280A in terms of overall application latency values for all combinations of technologies used. This is particularly because it has a faster CPU and higher memory than M6280A. The major delay components in these values comprise of the delay at the IED itself due to its hardware and software limitations.

The IED hardware component of delay $T_{IED}$ does not change much between using Ethernet 10Mbps and 100Mbps. The network delay component however decreases the overall
application latency in case of using Ethernet 100Mbps due to higher link speeds.

**Possible Workarounds:** For sending control information within specified time limits, the hardware specifications of the IVVC needs to be upgraded. This will increase the overall cost of the IED on the other hand. The protocol delay (DNP3 delay) component will decrease if the functionality of the DNP3 Data link layer is moved to the kernel space as simulated in our tests, thereby removing redundancy in error and frame control mechanisms carried out at DNP3 DLC and TCP DLC layers.

**Effect of DNP3 Message Sizes:** The size of the DNP message makes a significant difference to the overall value of Application Latency (AL) in the case of IVVC as against to M6280A. It is seen that the AL values for DNP3 message sizes of 4096 bytes are almost 4 times more than message sizes of 16 bytes. For example, the mean AL is 7.63 ms for 16 byte messages as against to 24.52ms for 4096 byte messages, when using Ethernet 10Mbps links. Similarly, the lower message sizes upto 1024 bytes, can be used in combination with IEEE 802.11g WiFi and Ethernet 10 Mbps with TCP or UDP to transfer ‘event control’ reports to the SCADA control center, although it can be risk taking to employ Wifi and UDP combination.
<table>
<thead>
<tr>
<th>Destination</th>
<th>Technology Used</th>
<th>Transport Protocol</th>
<th>Message Type</th>
<th>mean(AL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>M6280A</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Control Action</td>
<td>7.63 - 24.52ms</td>
</tr>
<tr>
<td>M6280A</td>
<td>Serial+Eth10M</td>
<td>TCP</td>
<td>Control Action</td>
<td>86.41 - 6796.3ms</td>
</tr>
<tr>
<td>M6280A</td>
<td>IEEE 802.11g + Eth10M</td>
<td>TCP</td>
<td>Control Action</td>
<td>6.69 - 29.54ms</td>
</tr>
<tr>
<td>M6280A</td>
<td>IEEE 802.11 + Eth10M</td>
<td>UDP</td>
<td>Control Action</td>
<td>6.46 - 11.83ms</td>
</tr>
<tr>
<td>MasterControlCenter</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Event Control Report</td>
<td>6.2 - 11.04ms</td>
</tr>
<tr>
<td>MasterControlCenter</td>
<td>Eth100M</td>
<td>TCP</td>
<td>Event Control Report</td>
<td>6.02 - 6.50ms</td>
</tr>
<tr>
<td>MasterControlCenter</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Event Control Report</td>
<td>11.26 - 20.2ms</td>
</tr>
</tbody>
</table>

(sent together with M6280A)
5.1.3 Source: MasterControlCenter

In this section, we summarize the results obtained for application latency when the source of a message in Site 2 is MasterControlCenter in Table 5.3. It shows the results when MasterControlCenter sends 'Event Monitoring REQUEST' messages to M6280A and 'Event Control REPLY' messages to IVVC. The observed results for this scenario are summarized in Table 5.3 and its corresponding graphs are illustrated using Figure 5.5 and Figure 5.6.

The results for Application Latency values are expressed as a range with the minimum value corresponding to DNP3 message size of 16 bytes and maximum value corresponding to message size of 4096 bytes. We observed the following details while measuring the Application Latency, when MasterControlCenter sends a 'Event Monitoring' REQUEST message to M6280A and an 'Event Control' RESPONSE message to the IVVC in Site 2:

**Effect of Communication Technology:**

- For destination = M6280A, SCADA takes around 1.4ms to 24.5ms when using Ethernet 10Mbps links in combination with IEEE 802.11g WiFi in with TCP transport protocol.

- It takes 7.8ms to 10.65ms while using Ethernet 10Mbps in combination with IEEE 802.11g WiFi but UDP as a transport layer solution for message sizes ranging from 16 - 4096 bytes.

- For destination = IVVC, SCADA takes 0.9ms to 5.743ms while using only Ethernet 10 Mbps links and 0.72ms to 1.2 ms while using Ethernet 100Mbps.
Effect of Delay Components: Since SCADA is a PC/laptop or a Windows based workstation, the application delay component due to its hardware specifications is minimum due to very high processor speed and larger RAM size as shown in Table 3.2. The only major component of delay when SCADA is source of communication is the overall network delay, which comprises of processing delays at intermediate network devices, congested links, packet transmission delay and propagation delay. The network protocol delay is not a major component of delay when SCADA is the source of communication since its CPU is fast enough to activate the DNP3 protocol thread and create the application layer message.
Effect of DNP3 Message Sizes: The size of the DNP3 message makes a significant difference to the overall value of Application Latency (AL) in this use-case as well. It is seen that the AL values for DNP3 message sizes of 4096 bytes are almost 25 times more than message sizes of 16 bytes. For example, the mean AL is 1.39 ms for 16 byte messages as against to 24.58ms for 4096 byte messages, when using IEEE 802.11g Wifi + Ethernet 10Mbps links with TCP as a transport protocol. Similarly, the lower message sizes upto 2048 bytes, can be used in combination with IEEE 802.11g WiFi and Ethernet 10 Mbps with TCP or UDP to transfer ‘event monitoring’ messages to M6280A IED.
Table 5.3: Source of Communication: MasterControlCenter

<table>
<thead>
<tr>
<th>Destination</th>
<th>Technology Used</th>
<th>Transport Protocol</th>
<th>Message Type</th>
<th>mean(AL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IVVC</td>
<td>Eth10M</td>
<td>TCP</td>
<td>Event Control REPLY</td>
<td>0.9 - 5.743ms</td>
</tr>
<tr>
<td>IVVC</td>
<td>Eth100M</td>
<td>TCP</td>
<td>Event Control REPLY</td>
<td>0.72 - 1.2ms</td>
</tr>
<tr>
<td>M6280A</td>
<td>IEEE 802.11g + Eth10M</td>
<td>TCP</td>
<td>Event Monitoring REQUEST</td>
<td>1.398 - 24.58ms</td>
</tr>
<tr>
<td>M6280A</td>
<td>IEEE 802.11g + Eth10M</td>
<td>UDP</td>
<td>Event Monitoring REQUEST</td>
<td>7.79 - 10.65ms</td>
</tr>
</tbody>
</table>
5.1.4 Technology Performance Analysis

In this section, we compare the performance of communication technologies and protocols used in this scenario. This section presents inter use-case analysis and provides a more clear picture of performance of communication technologies in exchanging information of varying priority levels and restricted delay bounds. Figure 5.7 shows the application latency values obtained with different combination of Ethernet and Wifi technologies in combination with TCP and UDP. Figure 5.8 explains the effect of delay components in the end to end path by showing the application latency break up in terms of delay components.

In this comparison study, we simulate the 'control action' message from IVVC to M6280A IED with different message sizes from 128, 512, 1024, 2048 and 4096 bytes. Further, we present the results while using IEEE 802.11g Wifi with TCP and IEEE 802.11g Wifi with UDP at the transport layer to deliver the control action message to M6280A. The results can be seen in Figure 5.9 with the blue line representing the trend using TCP whereas the red line showing the trend using UDP. The figure shows the mean of application latency (ms) on Y-axis versus the DNP3 fragment size (bytes) on X-axis.

**Remarks:** It can be clearly seen that UDP in combination with wireless provides a much better latency centric result than using wireless in combination with TCP. The AL values while using TCP range from 6.76ms to 29.54ms whereas the values using UDP range from 6.46ms to a maximum of 13.08ms. Thus, from these results, it can be assumed that 'real time control and monitoring' messages can be passed from IVVC to M6280A by using a combination of Ethernet 10Mbps and IEEE 802.11g Wifi links with UDP as the transport layer protocol. This is because UDP is a light weight protocol and under light load conditions, it can perform better than TCP. UDP removes the need to do frame and
error control and simply relays the packets from one link to another without providing any sort of delivery assurance. However, TCP can be used as a transport layer solution to send real time ‘monitoring and control’ messages of size \( \leq 2048 \text{ bytes} \), keeping in mind the 16ms upper bound time constraint as specified by IEEE 1646-2004[5].

### 5.2 Scenario 2 : Exception Scan in Site 1

This section summarizes the results for End to End delay obtained when SCADA MasterStation in Site 1 polls the LTC IED M2001D for either integrity poll data or class 1,2 or 3 data, also called Exception Scan. These simulations are run for a simulation time of 24 hours or 1 day (86400s). The size of REQUEST poll message follows a truncnormal distribution[31][32][33] with mean 120 bytes and standard deviation of 30 bytes. The

![Figure 5.7: Scenario 1 : Technology Performance Comparison.](image-url)
RESPONSE poll message follows a truncated normal distribution with mean 150 bytes and standard deviation of 50 bytes.

### 5.2.1 Performance Evaluation: Ethernet Only

Figures 5.10 and 5.11 show the end to end delay profile obtained when using Ethernet 10Mbps, 100Mbps and 1000Mbps links between SCADAMasterStation and M2001D for Exception Scan polls. The results and observations are summarized in Table 5.4.

### 5.2.2 Performance Evaluation: IEEE 802.11g + Ethernet

Figure 5.12 shows the performance of using IEEE 802.11g Wifi and Ethernet 10Mbps in combination with TCP or UDP for the same use-case. The trend observed with UDP
is such because it does not call for retransmissions for lost packets and does not offer any error or frame control mechanisms for packets. This is also because the channel is clear and no other traffic is flowing through it. This performance may worsen in heavy load conditions and varying message patterns at the Access Point in UDP’s case. All the obtained results are summarized using Table 5.4.
Figure 5.10: Ethernet 10/100Mbps, src: SCADAMasterStation, dest: M2001D.

Figure 5.11: Ethernet 1Gbps, src: SCADAMasterStation, dest: M2001D.
Figure 5.12: Performance of IEEE 802.11g + Ethernet 10Mbps.
Table 5.4: Technology Performance: Exception Scan

<table>
<thead>
<tr>
<th>Technology Used</th>
<th>Transport Protocol</th>
<th>mean(endtoendDelay)</th>
<th>timeavg(endtoendDelay)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 10Mbps</td>
<td>TCP</td>
<td>40ms</td>
<td>32ms</td>
</tr>
<tr>
<td>Ethernet 100Mbps</td>
<td>TCP</td>
<td>30ms</td>
<td>28ms</td>
</tr>
<tr>
<td>Ethernet 1Gbps</td>
<td>TCP</td>
<td>28ms</td>
<td>16ms</td>
</tr>
<tr>
<td>Ethernet 10Mbps + IEEE 802.11g</td>
<td>TCP</td>
<td>7.9ms</td>
<td>6.8ms</td>
</tr>
<tr>
<td>Ethernet 10Mbps + IEEE 802.11g</td>
<td>UDP</td>
<td>1.5ms</td>
<td>0.7ms</td>
</tr>
</tbody>
</table>
5.2.3 Technology Performance Analysis

- From Figure 5.13, we conclude that for the Class polling REQUEST message shown in upper half of the diagram, the lowest end to end delay is obtained in the case of using Ethernet 10Mbps and IEEE 802.11g Wifi in combination with UDP as a transport layer protocol.

- The next best performance is obtained for the same set of communication technologies but with TCP as a transport protocol and also with using Ethernet 1Gbps stand alone links.

- The highest end to end delay is obtained in the case of using Ethernet 10Mbps and Ethernet 100Mbps as stand alone solutions.

- The lowest end to end delay represents only 0.4755ms or 1% of total end to end delay relative to other technologies whereas the highest end to end delay accounts for 28.61ms or 38% relative to other solutions.

5.3 Scenario 3 : Inter-Substation Event Monitoring

In this section, we present the results of evaluating the performance of TCP and UDP with Ethernet. The communication is initiated by the LTC IED Site 1 to the main master SCADA control center in Site 2. M2001D in Site 1 say, after applying the load balancing operation wants to communicate an ’event control’ report to the SCADA center in Site 2. The results for the three scenarios can be seen in Figures 5.14, 5.15 and 5.16 respectively. It is found that UDP protocol is more faster than TCP when used in combination with Ethernet 10Mbps. Either TCP or UDP can be used to transfer medium priority messages.
Figure 5.13: Scenario 2: Technology Performance Comparison.

of this kind since the obtained values are below the upperbound value of 1000ms or 1 second external to the substation, as specified by IEEE 1646-2004[5].

From the values of application latency obtained in this scenario, it is seen that UDP can perform better than TCP because UDP is built around the goal of reducing latency. It does not offer any error or frame control services as TCP and DNP3. However, the actual values of AL will be a bit more higher than obtained here, since the do not consider the protocol delay due to DNP3 protocol in the case of using UDP. When used with TCP, DNP3 effectively operates at a combined transport layer and data link layer functionality in our simulations.
Figure 5.17 represents the application latency obtained in each of the three cases, as relative percentages with respect to each other. Such a comparison study shows that the best performance in the ‘event monitoring’ report scenario is obtained in case of Ethernet 10Mbps with UDP which accounts for only 9% of total combined AL incurred in all the three cases. The worst yet acceptable performance is obtained in the Ethernet 10Mbps and TCP case. It means that this case accounts for 46% of total combined AL in all three cases. However, the performance of UDP will worsen more if there are increased number
of flows in internet traffic in the WAN cloud. This is because there will be zero guarantee for packet ordered delivery unlike TCP and no error and frame control techniques at the transport layer.
Figure 5.16: Inter-Substation Case III: Ethernet 10Mbps with UDP.
Figure 5.17: Scenario 3: Technology Performance Comparison.
5.4 Summary

In this section, we summarize the results of this work-study by presenting results and recommended technologies for different priority type messages exchanged in smart grid applications and the ones we discussed in this thesis study. We summarize our observations in Tables 5.5 and 5.6. These results are summarized for results obtained with DNP3 mean fragment size of 2048 bytes.

It can be seen from Table 5.5 and Table 5.6 that for different types of messages exchanged within a substation communication network, there is no single communication technology and transport protocol combination that is sufficient to satisfy the timing bounds laid by IEEE 1646-2004 standard. For exchanging ‘Control Action’ messages, Ethernet 10Mbps may work best in combination with IEEE 802.11g and UDP but only under low traffic load conditions, whereas Ethernet 1Gbps may be used to perform high priority Exception Scans on an IED under the given settings in this work.
Table 5.5: Summary of Findings : AL

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Priority/Speed</th>
<th>Source Device</th>
<th>Technology</th>
<th>mean(AL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>High</td>
<td>M6280A IED</td>
<td>Eth100M/1G+TCP</td>
<td>11.28 - 11.5ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M2001D IED</td>
<td>Eth100M/1G+TCP</td>
<td>11.28 - 11.5ms</td>
</tr>
<tr>
<td>Control Action</td>
<td>High</td>
<td>IVVC</td>
<td>Eth10M+802.11g with UDP</td>
<td>6.46 - 11.83ms</td>
</tr>
<tr>
<td>Event Control Report</td>
<td>Medium</td>
<td>IVVC</td>
<td>Eth10M/100M+TCP</td>
<td>6.2 - 11.04ms</td>
</tr>
<tr>
<td>Event Monitoring REQUEST</td>
<td>Medium</td>
<td>SCADA</td>
<td>Eth10M+TCP</td>
<td>0.9 - 5.743ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IVVC</td>
<td>Eth10M+TCP</td>
<td>6.2 - 11.04ms</td>
</tr>
<tr>
<td>Event Monitoring Report</td>
<td>Medium</td>
<td>M6280A IED</td>
<td>Eth10M+TCP</td>
<td>11.2 - 16.04ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M6280A with IVVC</td>
<td>Eth10M+TCP</td>
<td>11.18 - 20.3ms</td>
</tr>
<tr>
<td>Non-real time config</td>
<td>Medium/Slow</td>
<td>IVVC</td>
<td>Serial+Eth10M with TCP</td>
<td>86.41 - 6791.31ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IVVC</td>
<td>Eth10M + TCP</td>
<td>7.63 - 24.52ms</td>
</tr>
<tr>
<td>Inter-site Event Report</td>
<td>Medium</td>
<td>M2001D</td>
<td>Eth10M+TCP</td>
<td>39.9 - 1029.7ms</td>
</tr>
</tbody>
</table>
Table 5.6: Summary of Findings: End to End Delay

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Priority/Speed</th>
<th>Potential Source Device</th>
<th>Optimum Technology</th>
<th>mean (endtoendDelay)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity Scan</td>
<td>Medium</td>
<td>SCADA</td>
<td>Eth10M+802.11g with TCP</td>
<td>6.8ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Eth10M+802.11g with UDP</td>
<td>1.5ms</td>
</tr>
<tr>
<td>Class 1 Exception</td>
<td>High</td>
<td>SCADA</td>
<td>Eth1G+TCP</td>
<td>16ms</td>
</tr>
<tr>
<td>Class 2,3 Poll</td>
<td>Medium</td>
<td>SCADA</td>
<td>Eth100M+TCP</td>
<td>28ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Eth10M+TCP</td>
<td>40ms</td>
</tr>
</tbody>
</table>
Chapter 6

Conclusions and Future Work

In summary, we have learnt a number of important lessons about enabling technologies in end to end substation automation communication networks. The communication requirements to drive a substation automation application are very diverse from those required for internet communications. Integrating the different systems in substation automation application is a major challenge at hand since power communications are not ’directly’ based on the flexible and ubiquitous TCP/IP suite, but requires unification and encapsulation of protocols like DNP3 with TCP/IP for communications among intelligent power devices. The optimum latency that can be achieved for a substation automation application is driven by many delay factors. Some of them can directly be worked upon to optimize it further, whereas some others are constrained by the limited computational capabilities of the embedded computers and their underlying protocol stack, for example DNP3.

DNP3 has its own layered approach for communicating with other IED’s. Because of the error and frame control mechanisms employed at the Data Link Control layer of the DNP3 protocol, the overall latency of the application increases significantly. This calls for
the need of a modified approach or a employ a more light-weight implementation of DNP3 to reduce the overall latency of the substation application. It challenging task to integrate the protocol stacks of DNP3 and TCP/IP in order to simulate tests to measure the performance of communication technologies in driving a substation automation application. Substation automation applications also interact with other applications from various Smart Grid domains like markets and service providers. It will be a major challenge develop a topology that can be used to effectively communicate with inter-domain intelligent power devices. This is because the communication requirements for inter-DOMAIN communication will be different than just inter-SUBSTATION communications like in our study. This will require careful consideration of many other factors like specifications of devices used in other domains, the communication links used between inter-DOMAIN systems, types of information exchanged and effect of additional internet traffic in the end to end communication path.

**Our Approach:** We use a combination of Ethernet and Wifi with TCP and UDP for our simulations. The performance metrics we considered are 'Application Latency' of the system which takes into consideration all the delay components like delay due to hardware/software limitations of the IED, network protocol delay and network transmission delay. Other metrics used to evaluate the results are End to End Delay, Loss Rate in Wifi and Jitter in Wifi. From our simulation results, it is found that better results are obtained when using UDP instead of TCP in certain scenarios since, UDP is relatively a light-weight protocol and provides better performance in certain scenarios to deliver DNP3 messages faster than TCP. However, this might not be the case in networks where the background noise and traffic profiles are significantly larger. In such cases, UDP may offer worse performance due to high number of collisions and packet loss with no guar-
antee for packet delivery. Also, it is observed that DNP3 over TCP/IP is not the best solution for exchanging 'Very High' priority protection messages that have latency bounds less than 4ms as specified by IEEE 1646-2004. We need to employ a modified approach of sending messages with a light weight power communication protocol to achieve this successfully. However, we can use Ethernet and Wifi technologies to send and receive real time monitoring and control messages between devices within and external to a substation. To exchange 'control action' messages, Ethernet 100Mbps or 1Gbps can work the best. Ethernet 10Mbps can be used in combination with IEEE 802.11g alongwith TCP or UDP for best performance in exchanging messages with latency bounds less than 16ms within the substation. Ethernet 1Gbps performs best in combination with TCP to convey Class 1 high priority exception scan messages with a peak end to end delay of 16ms. Low speed Ethernet may be used with TCP for Integrity Scan and Class 2,3 scan messages with peak end to end delay values of 28ms for Ethernet 100Mbps and 40ms for 1Gbps Ethernet.

In effect, we infer that there is no one size fits all communication topology and technology solution that may be used to enable an end to end application and deliver DNP3 over TCP/IP messages within latency bounds as specified by IEEE 1646-2004 standard. To satisfy the latency requirements for each message type, it is optimum to use a combination of technologies and communication interfaces that can provide better overall performance. The communication topology used in our work alongwith the results obtained by answering the existing challenges in developing a communication network for substation automation will provide more understanding of enabling end to end communications within a single domain of the Smart Grid. Such an understanding will supplement more information and options to enable inter-DOMAIN communications with other Smart Grid applications. The taxonomy of communication interfaces may better
help to interface an application in one domain with other applications with a different set of requirements in another Smart Grid domain. For example, integration of a substation automation application with an energy management system located at a remote site.

**Future Work:** In the future, we plan to advance with this work by using this communication topology and enabling it to evaluate the performance of other promising wireless technologies like IEEE 802.16e, Bluetooth, and find the viability of Cellular 3G and 4G LTE in substation automation networks. These wireless technologies are becoming increasingly popular in the smart grid field but need to be tested in specific substation use-cases before deployment. At the same time, it is important to conduct a cost analysis for using technologies like WiMAX and 3G since the cost of installing a WiMAX tower is huge and needs careful consideration. Along with this, we will also create communication architectures for hosting applications in other Smart Grid domains on similar lines of research and simulate the performance of Ethernet and Wifi with requirements existing in those applications. Finally, we will integrate and model the communication architectures designed in to different domains for inter-DOMAIN connectivity. Such inter-domain connectivity is necessary for inter-department and inter-process communication between different entities and subsystems that will exist across domains. Such an integrated study of architectures in two or more domains with unique and diverse set of power communication requirements will help to make real-world decisions while planning, designing and constructing real networks within and across systems in Smart Grid domains.
REFERENCES


