SECURITY ISSUES IN DISTRIBUTED ENERGY RESOURCES (DER) IN SMART GRID

Mruga Vyas
B.E., Dhramsinh Desai University, India, 2007

PROJECT

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in
COMPUTER SCIENCE

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

SPRING
2011
SECURITY ISSUES IN DISTRIBUTED ENERGY RESOURCES (DER) IN SMART GRID

A Project

by

Mruga Vyas

Approved by:

__________________________________, Committee Chair
Isaac Ghansah, Ph.D.

__________________________________, Second Reader
Ted Krovetz, Ph.D.

____________________________
Date
Student: Mruga Vyas

I certify that this student has met the requirements for format contained in the University format manual, and that this project is suitable for shelving in the Library and credit is to be awarded for the Project.

__________________________, Graduate Coordinator       ________________

Nikrouz Faroughi, Ph.D.                                                         Date

Department of Computer Science
Abstract

of

SECURITY ISSUES IN DISTRIBUTED ENERGY RESOURCES (DER) IN SMART GRID

by

Mruga Vyas

One of the main goals of smart grid is to create a de-centralized and consumer controlled power system which can increase efficiency, reliability and reduce cost for energy. One of the ways to achieve this goal is to introduce Distributed Energy Resources (DER) into the smart grid. DER devices are small scale power generation units which can provide energy according to the consumer demand. DER systems are interconnected with many other systems in the smart grid. The major systems interconnected with DER system are micro grids, distribution system and synchrophasor system. This project discusses security issues, counter measures, and research issues in DER and systems interconnected with it. It covers proper data handling practices for maintaining confidentiality, integrity, availability, and accountability. In conclusion, this project helps to evaluate security and possible best practices for energy efficient solutions associated with systems interconnected with DER.

_______________________, Committee Chair
Isaac Ghansah, Ph.D.

_______________________
Date
DEDICATION

This project is dedicated to my beloved parents Kaushik Vyas and Purvi Vyas for their never-ending sacrifice, love and support and understanding.
ACKNOWLEDGMENTS

I would like to extend my gratitude to my project advisor Dr. Isaac Ghansah, Professor, Computer Science and Engineering for guiding me throughout this project and helping me in completing this project successfully. I am also thankful to Dr. Ted Krovetz, Professor, Computer Science and Engineering, for reviewing my report. I am grateful to Dr. Nikrouz Faroughi, Graduate Coordinator, Department of Computer Science, for reviewing my report and providing valuable feedbacks. In addition, I would like to thank The Department of Computer Science at California State University for extending this opportunity for me to pursue this program and guiding me all the way to become a successful student.

Lastly, I would like to thank my parents Kaushik Vyas and Purvi Vyas for providing me the moral support and encouragement throughout my life.
TABLE OF CONTENTS

Dedication........................................................................................................................................... v
Acknowledgments................................................................................................................................. vi
List of Tables.......................................................................................................................................... x
List of Figures.......................................................................................................................................... xi
List of Abbreviations.............................................................................................................................. xiii

Chapter

1. INTRODUCTION................................................................................................................................. 1
   1.1 Introduction to Smart Grid............................................................................................................ 1
   1.2 Introduction to Distributed Energy Resources (DER)................................................................. 4
   1.3 Systems Interconnected with DER............................................................................................. 6
       1.3.1 Micro Grid System and DER.......................................................................................... 7
       1.3.2 Distribution System and DER......................................................................................... 8
       1.3.3 Synchrophasor System and DER.................................................................................... 9
   1.4 Goal of the Project.......................................................................................................................... 9

2. MICRO GRID SYSTEM SECURITY ISSUES AND SECURITY MEASURES........................................... 11
   2.1 Introduction to Micro Grid System .............................................................................................. 11
   2.2 IDAPS – An Intelligent Micro Grid........................................................................................... 13
       2.2.1 Supply-Driven-Demand Approach.................................................................................. 15
       2.2.2 IDAPS Agent-based Framework...................................................................................... 16
   2.3 Security Issues in IDAPS............................................................................................................. 18
       2.3.1 Security Concerns in IDAPS ......................................................................................... 18
2.3.2 Cyber Threats in IDAPS ................................................................. 22

2.4 IDAPS Security Measures .................................................................. 23
2.4.1 Security Requirements for IDAPS .................................................. 23
2.4.2 Security Measures for IDAPS ....................................................... 24
2.4.2.1 Web Service Security .............................................................. 24

3. DISTRIBUTION SYSTEM SECURITY ISSUES AND SECURITY MEASURES ...... 32
3.1 Introduction to Distribution System ................................................... 32
3.2 Distribution Automation System (DAS) .............................................. 35
3.2.1 Communication Technologies Used in DAS .................................. 37
3.3 Security Issues in DAS ...................................................................... 38
3.3.1 Security Requirements of DAS ..................................................... 39
3.3.2 Cyber Threats in the DAS ............................................................. 42
3.3.3 Security Goals ............................................................................ 44
3.4 DAS Security Measures ..................................................................... 45
3.4.1 Secure Information Flow ............................................................... 46
3.4.2 Access Control ............................................................................ 46
3.4.3 Account Management ................................................................. 46
3.4.4 Communication Link .................................................................. 47
3.4.5 Securing Control Operations ....................................................... 51
3.4.6 Cryptography ............................................................................. 53

4. SYNCHROPHASOR SYSTEM SECURITY ISSUES AND SECURITY MEASURES ................................................................. 58
4.1 Introduction to Synchrophasor System .............................................. 58
4.2 Security Issues in Synchrophasor System .......................................... 62
4.2.1 Security Requirements in Synchrophasor System

4.2.2 Cyber Threats in Synchrophasor System

4.3 Synchrophasor System Security Measures

4.3.1 Substation Security Measure

4.3.2 Information Security

4.3.3 Security Concerns and its Solutions

5. RESEARCH ISSUES

5.1 Overview

5.2 Authorization and Authentication for IDAPS

5.3 Security Issue in Log Information

5.4 Traffic Analysis

5.5 Enhancing the Security of Serial Communication

5.6 Roles to be Defined in Control Center

5.7 Authentication and Authorization of User at Field Substations

5.8 Timing Information Dependency

5.9 Software Patches Update

6. CONCLUSIONS

6.1 Summary

6.2 Strengths and Weaknesses

6.3 Future Works

References
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2-1</td>
<td>Possible Attacks and Impacts on Multi Agent Interface</td>
<td>19</td>
</tr>
<tr>
<td>Table 3-1</td>
<td>Correlation of Security Requirements and Threats</td>
<td>44</td>
</tr>
<tr>
<td>Table 4-1</td>
<td>Security Concerns and its Solutions</td>
<td>74</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1:</td>
<td>Conceptual Smart Grid Architecture</td>
<td>2</td>
</tr>
<tr>
<td>Figure 1-2:</td>
<td>Types of Distributed Energy Resources</td>
<td>5</td>
</tr>
<tr>
<td>Figure 1-3:</td>
<td>Future DER Vision</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2-1:</td>
<td>Micro Grid Framework</td>
<td>12</td>
</tr>
<tr>
<td>Figure 2-2:</td>
<td>IDAPS Framework</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2-3:</td>
<td>Multi Agent Frameworks in an IDAPS</td>
<td>16</td>
</tr>
<tr>
<td>Figure 2-4:</td>
<td>IDAPS Agent Interaction</td>
<td>18</td>
</tr>
<tr>
<td>Figure 2-5:</td>
<td>Shared Key (Symmetric) Encryption</td>
<td>26</td>
</tr>
<tr>
<td>Figure 2-6:</td>
<td>Public Key (Asymmetric) Encryption</td>
<td>26</td>
</tr>
<tr>
<td>Figure 2-7:</td>
<td>Hybrid Encryption</td>
<td>27</td>
</tr>
<tr>
<td>Figure 2-8:</td>
<td>Digital Signature</td>
<td>29</td>
</tr>
<tr>
<td>Figure 3-1:</td>
<td>Distribution Domain in Smart Grid</td>
<td>33</td>
</tr>
<tr>
<td>Figure 3-2:</td>
<td>Categories of Benefits Used to Justify Automation in Distribution System</td>
<td>34</td>
</tr>
<tr>
<td>Figure 3-3:</td>
<td>Schematic Diagram of Distribution Automation System (DAS)</td>
<td>37</td>
</tr>
<tr>
<td>Figure 3-4:</td>
<td>CHAP Authentications</td>
<td>48</td>
</tr>
<tr>
<td>Figure 3-5:</td>
<td>TLS Handshake with Server and Client Side Certificate – MITM Attack</td>
<td>50</td>
</tr>
<tr>
<td>Figure 3-6:</td>
<td>Challenge Response Mode</td>
<td>52</td>
</tr>
<tr>
<td>Figure 3-7:</td>
<td>Aggressive Mode</td>
<td>53</td>
</tr>
<tr>
<td>Figure 3-8:</td>
<td>Symmetric Key Encryption with MAC</td>
<td>55</td>
</tr>
<tr>
<td>Figure 3-9:</td>
<td>X.509 Certificate Issued by CA</td>
<td>57</td>
</tr>
<tr>
<td>Figure 4-1:</td>
<td>Basic Synchrophasor Architecture</td>
<td>59</td>
</tr>
</tbody>
</table>
Figure 4-2: Typical Synchrophasor System Components and its Data Flow ................. 60
Figure 4-3: Example of Phasor Measurement .......................................................... 62
Figure 4-4: Multilayer Architecture ........................................................................ 68
Figure 4-5: Example of Firewalls in Security Architecture ...................................... 69
Figure 4-6: Example of VPN Working with Firewall .............................................. 70
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DER</td>
<td>Distributed Energy Resources</td>
</tr>
<tr>
<td>IDAPS</td>
<td>Intelligent Distributed Autonomous Power System</td>
</tr>
<tr>
<td>DAS</td>
<td>Distribution Automation System</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>DR</td>
<td>Demand Response</td>
</tr>
<tr>
<td>OpenADR</td>
<td>Open Automated Demand Response</td>
</tr>
<tr>
<td>UA</td>
<td>User Agent</td>
</tr>
<tr>
<td>DA</td>
<td>Device Agent</td>
</tr>
<tr>
<td>CA</td>
<td>Control Agent</td>
</tr>
<tr>
<td>AA</td>
<td>Aggregation Agent</td>
</tr>
<tr>
<td>DBA</td>
<td>Database Agent</td>
</tr>
<tr>
<td>DERA</td>
<td>Distributed Energy Resources Agent</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
<tr>
<td>UDDI</td>
<td>Universal Description, Discovery and Integration</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>FTU</td>
<td>Feeder Terminal Unit</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>DTU</td>
<td>Distribution Terminal Unit</td>
</tr>
<tr>
<td>TTU</td>
<td>Transformer Terminal Unit</td>
</tr>
<tr>
<td>AMI</td>
<td>Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>DCC</td>
<td>Data Control Center</td>
</tr>
<tr>
<td>OMS</td>
<td>Outage Management System</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>LMS</td>
<td>Load Management System</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>CIS</td>
<td>Customer Information System</td>
</tr>
<tr>
<td>DA</td>
<td>Distribution Automation</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>DNP3</td>
<td>Distributed Network Protocol</td>
</tr>
<tr>
<td>ASDU</td>
<td>Application Service Data Unit</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
</tbody>
</table>
Chapter 1
INTRODUCTION

1.1 Introduction to Smart Grid

The current power infrastructure has been serving United States for a very long time. Although, the current power system has a lot of advantages, it is now coming to its limitations. It may still provide adequate electricity, but as the time goes on the risk that is associated with using an old infrastructure also increases accordingly [1]. The goal of smart grid is to develop an infrastructure which is more decentralized and consumer controlled network as compared to the current power infrastructure which is centralized and producer controlled network. Due to the constant increase in energy demand the need for smart grid has also increased. Consumer controlled infrastructure of the smart grid will allow the consumers to manage and control their energy usage in more efficient ways. Changes in the infrastructure of current power network to smart grid will also change the relations between the different stakeholders such as utilities, energy service providers, consumers, technology and many others [1].

A smart grid infrastructure consists of interconnected systems with two-way flow of energy and information between the points of power generation and points of power consumption. Smart grid was mainly developed with the purpose of improving efficiency and reliability, improving the ability to forecast trends and events, reducing the energy cost by using other forms of renewable energies and creating energy awareness [2]. Figure 1-1 is a conceptual architecture of the smart
grid where different components such as smart appliances, sensors, storage, generators, micro grids, DER system, and central power plant are all interconnected with each other.

Figure 1-1: Conceptual Smart Grid Architecture [2]
In terms of overall vision smart grid is

1) Intelligent: It is capable of (1) working independently and can provide faster solutions than humans; (2) sensing system overloads, which can reduce or prevent the power outage by rerouting of power [1].

2) Efficient: It is capable of meeting an increasing demand of energy by consumer without the need of additional infrastructure [1].

3) Accommodating: It accepts any form of energy that is available from any fuel source such as solar, wind, coal and natural gas. Moreover it is capable of integrating any ideas and technologies for energy storage [1].

4) Motivating: It allows real-time communication between the consumers and utility, so that consumers can manage their energy usage based on their preferences and needs which are mainly related to cost and environmental concerns [1].

5) Quality Focused: It is capable of delivering the quality of power that is required for running the ever increasing digital economy, data centers and computers without any interruption [1].

6) Resilient: As smart grid infrastructure is more decentralized, it becomes more resistant to attack and natural disasters by using some of the smart grid security protocol [1].

7) “Green”: It helps in environmental improvement by using more renewable sources of energy and preventing global climatic change. [1].

Thus, the main focus is to make the grid more automated in order to provide the above functionalities. Smart grid technology allows us to overcome the challenges such as increasing
power demand, aging utility infrastructure, and environmental impact of greenhouse gases produced during electricity generation. With the smart grid technology power can be used more efficiently and the carbon content of the environment can also be reduced drastically [1]. Given the significant concern regarding the climate change, the need for renewable energy like solar and wind power is critical. The ability of smart grid to dynamically manage all the renewable energy on the grid means that more distributed energy resources (DER) can be integrated in the grid [1].

1.2 Introduction to Distributed Energy Resources (DER)

The current electrical power infrastructure has many problems such as high energy costs or low electric power reliability and quality. The solution to these problems is to use distributed energy resources (DER) in smart grid infrastructure [3]. Distributed energy resources are small, modular, energy generation unit and storage technologies which can provide electric energy according to the consumer demand. DER devices can normally produces less than 10 megawatts (MW) of power; therefore DER systems can be used by a residential user to meet their needs for energy. DER systems could also be used by utilities providing the energy to the consumer by installing it on the site along with the central power plant. DER systems are stand alone power generation units which can be used by either connecting it to the local electric power grid or by isolating it from the grid and using it as an independent power generation unit. Technologies for DER system include photovoltaic’s (PV) batteries, reciprocating engines, fuel cells, combustion turbines and gas turbines as shown in figure 1-2 [3]. There are other technologies for DER system such as wind turbines, solar panels and energy storage systems which are not shown in figure.
Because renewable energy resources are proving to be as useful and desired as the existing generation resources many utility are installing additional renewable generation sources such as solar panels and wind mills on their sites [4].

The ability to operate different segments of the smart grid, as independent generation units is increasingly becoming a reality as the number of DER devices in the grid increases. The reason for this is the demand for high availability and high quality of power. Figure 1-3 shows the future
vision of the DER system. It shows that DER devices like solar, wind, micro-turbine are also interconnected with other systems such as demand response system, controllable loads and direct load control [4].

Figure 1-3: Future DER Vision [4]

As multiple DER devices are introduced in the network, need for remote connection between them and their interconnection with the grid brings a set of vulnerabilities along with the set of vulnerabilities that belongs to different systems interconnected with the DER systems in the grid.

1.3 Systems Interconnected with DER

DER devices are connected with different systems in the smart grid. These systems include micro grid system, distribution system, and synchrophasor system. These systems such as micro grid and synchrophasor system along with DER help in providing high quality energy with increased
efficiency and reliability where consumer can produce and manage their energy usage. Distribution system helps in connecting these independent generation units with the main power grid.

1.3.1 Micro Grid System and DER

Micro grid is a small scale power supply network that can provide power to small a community. It can also be connected to the utility grid to avoid power outages. Micro grid is very similar to DER, as both can be used as standalone power generation units that can operate independently. However these days, the need for a resilient and autonomous electric power grid infrastructure which can guard itself against manmade and natural disasters is increasing. One way to assure such self-healing characteristics in an electric power system is to design for small and autonomous subsets of the larger grid. This goal can be achieved by managing the DER devices installed by the customers for their residential use, which has increased in recent years. But even if the number of customer-owned DER devices is increasing, no mechanism is developed for coordinating these devices. Practices that are in use merely focus on coordinating DER devices that belong to the same utility. A new mechanism should be developed, where different DER devices that do not belong to same utility are coordinated and managed intelligently so that they can contribute to the integrity of the critical electric power infrastructure at the distribution level [6].

Intelligent Distributed Autonomous Power System (IDAPS) is one such intelligent micro grid which is mainly used for coordinating these “customer-owned” DER devices [6]. IDAPS collects
real time information from different DER devices in the networks regarding price and availability of energy. Interconnected DER devices in the IDAPS system can also communicate with each other through a web based communication architecture using web services. Web services enable data sharing in a platform independent environment. This increase the exposure of resources which poses security issues for data and services in IDAPS system. There are many cyber security issues, threats and security requirements that are discussed further in this report along with the best practices to deal with these attacks.

1.3.2 Distribution System and DER
One of the main goals of the smart grid is to convert the current power infrastructure from centralized network to a de-centralized network. This goal can be achieved by using DER devices owned by customer for their personal use or installed by the utilities in the power grid. To interconnect these widely distributed DER devices in the network, distribution system plays an important role. Automation is introduced into the distribution system which helps in performing the task automatically in a sequence with faster operation rate, as the demand to improve efficiency and reliability of power system increases. According to the Institute of Electrical and Electronic Engineers (IEEE) automation in distribution system can be defined as “a system that enable an electric utility to monitor, coordinate, and operate distribution components in a real time mode from remote locations [44].” However, introducing automation also introduces new risks of cyber attacks, as the distribution components are operated remotely. There are many cyber security issues, threats and security requirements that are discussed further in this report along with the best practices to deal with these attacks.
1.3.3 Synchrophasor System and DER

Synchrophasor technology can be summarized as marking electrical quantities with a high-accuracy time tag in order to be able to use data from multiple sources in a coherent manner. As DER devices are widely distributed into the network, it is required that all the electrical quantities collected from different DER devices are in the same phase. Synchrophasor systems are used for synchronizing different phases of electrical quantities for proper supply and quality check. Normally, synchrophasor systems are used by the utilities for maintaining the quality of energy [9].

Electronic communication plays an important role in synchrophasor system implementations as the components are required to continuously communicate across large geographical areas. This introduces a new risk of cyber attacks as these communications can take place over non-trusted channels [9]. There are many cyber security issues, threats and security requirements that are discussed further in this report along with the best practices to deal with these attacks.

1.4 Goal of the Project

The goal of this project is to understand the interconnection of DER with other systems in the smart grid and carry out research on the current and potential security vulnerabilities in these systems. This project also covers the counter measure techniques that can be applied to combat these security issues. Research issues that still need to be explored are also discussed in this project. This report is structured as follows; Chapter 2 discusses the interconnection of micro grid system and DER along with the security issues and its counter measures. Chapter 3 discusses the
interconnection of distribution system and DER along with the security issues and its counter measures. Chapter 4 discusses the interconnection of synchrophasor system and DER along with the security issues and its counter measures. Chapter 5 discusses the research issues that still need more work, in order to provide effective security. Chapter 6 gives the summary, strength, weakness and future work.
Chapter 2

MICRO GRID SYSTEM SECURITY ISSUES AND SECURITY MEASURES

This chapter discusses the interconnection of DER with the micro grids, the security issues and security requirements for the micro grid and best practices to deal with these issues and its counter measures.

2.1 Introduction to Micro Grid System

Micro grids are small-scale and modernized versions of the centralized power system which is mainly designed to provide power for small community. Micro grids are also connected to the utility grids to prevent power outages, as excess power generated by the micro grid could be sold back to the utility. Micro grid uses various small and renewable power generating resources which makes it highly efficient and flexible. Goals such as reliability, carbon emission reduction and cost reduction can be achieved through micro grids. Figure 2-1 shows the micro grid framework. It shows that micro grids are much smaller version of the main grid which can generate, distribute, and regulate the flow of electricity to consumers. Here consumers can participate in the electricity market, but on a smaller level. Micro grids form the building blocks of the future power system [10].

The major advantage of micro grid is its ability to isolate itself from the utility grid with little or no disruption to the loads within the micro grid, during utility grid disturbance. It prevents the utility grid failure by reducing the load on the grid during peak load periods. It can also reduce the energy costs for its user by generating some or all of its electricity needs.
Intelligent micro grids has been defined by Prof. Saifur Rahman during APSCOM conference as “A part of electrical power distribution network which contains multiple DERs, multiple loads and the capability of islanding and operating separately and independently from the main power grid – macro grid [12]”. Number of users installing DER devices is increasing as the demand for energy reliability and efficiency increases. However, until now the mechanism available was only for the interconnection between DER devices that belongs to the same utility. So even though the number of customer owned DER devices is increasing, the mechanism for coordinating these DER devices is not available. So IEEE proposed a new concept for an intelligent micro grid called Intelligent Distributed Autonomous Power System (IDAPS). IDAPS is an intelligent micro grid which can organize, manage and dispatch these “customer-owned” DER devices, to maintain
the integrity of the electrical power infrastructure at distribution level. It is discussed in more detail in the next section.

2.2 IDAPS – An Intelligent Micro Grid

IDAPS is an intelligent micro grid that manages the customer owned DER devices in such a way that these energy resources can be shared in the utility grid both during normal and outage operations. The background for the building blocks of the IDAPS can be described as

1) The Micro Grids: In micro grids, DER devices are mainly used as the source of energy generation. However, it was always assumed that all those DER devices should belong to the same utility, to have communication amongst them without any conflict. So to manage these ‘customer-owned’ DER devices in micro grid, IEEE proposed a market based approach for electricity trading at local level within an IDAPS micro grid. Wholesale electricity market uses similar approach [13].

2) Electricity Market: Normal electricity market adopts a mechanism where utility sells the electricity to the consumer. Offers given by the generators are based on the energy demand that is either known or forecasted. However, micro grid is a small power generation unit where the demands can change instantly. It is very difficult to forecast the demand in advance. So IEEE proposed a new mechanism called “Supply-driven-demand management” for micro grid operations in IDAPS [13]. It is discussed further in section 2.2.1.

3) Control and Communication architecture: Control and Communication architecture is the center of any operations in power systems. In wholesale electricity market, Supervisory
Control and Data Acquisition (SCADA) systems are used for this purpose. However, automated agent technologies are used when dealing with small scale power generation unit like micro grids. However, there is a major problem with using agent based technologies. It limits the communication among various customer owned DER devices that have systems and hardware from different vendors. So to over some such obstacle web-based communication architecture is implemented, using multi agent technology and web services. It ensures the portability and interoperability among various systems using web services [13]. It is discussed further in section 2.2.2.

Based on these building blocks, framework for IDAPS is developed as shown in figure 2-2. IEEE described building blocks of IDAPS as “the building blocks of IDAPS include physical and cyber layers. The former is composed of loosely connected DER devices and loads which can communicate with one another via the latter, i.e. web-based communication overlay architecture employing multi-agent technology and web services [6].”

Figure 2-2: IDAPS Framework [6]
2.2.1 Supply-Driven-Demand Approach

In the wholesale electricity market, the generation of energy and its distribution is based on the demand-driven-supply approach. In this approach, price offers given by the generators depend on the demand of electricity. This demand is either known previously or is forecasted. On the other hand, in small scale power generation system like micro grid, the demand varies continuously. As a result, demand cannot be forecasted or known beforehand. IDAPS implements the concept of supply-driven-demand approach. Here instead of matching the supply with the demand and providing high energy price, fluctuating demand and available supply is matched at “correct” price. Thus based on the real time electricity price, customers can decide which of their suspended demands can be serviced [6].

In supply driven demand concept, IDAPS will employ a bulletin board that represents an electricity market. Here the owner of DER devices and the participants will be able to buy and sell the electricity. Here the demand for the electricity is based on the available supplies. The demand for electricity other than minimum basics is postponed until most economic DG is available locally. Thus the decision of buying the electricity depends on the real time electricity pricing information given by the suppliers in the grid. IDAPS along with real time pricing information and quantity of electricity to be sold also provides the schedule of available electricity supply which can be posted on the bulletin board in advance [6].
2.2.2 IDAPS Agent-based Framework

The components that will enable the physical and cyber layer of IDAPS framework to communicate with one another are based on the multi-agent concept that is overlaid on web service layer. An agent is a software-based entity that can respond to real-time changes in the network accordingly [6]. Figure 2-3 shows the generic architecture of the multi-agent framework in the IDAPS. Different types of agents used in the framework are

- **User Agent (UA):** User agent is responsible for connecting the user to rest of the IDAPS systems. It is also responsible for getting the real-time information and displaying all relevant information to the user.

![Figure 2-3: Multi Agent Frameworks in an IDAPS [6]](image)

<table>
<thead>
<tr>
<th>ID</th>
<th>Location</th>
<th>Type</th>
<th>Price (c/kWh)</th>
<th>Quantity (kWh)</th>
<th>Availability (time)</th>
</tr>
</thead>
</table>

**Metadata**
- DA = Device Agent
- CA = Control Agent
- UA = User Agent
- AA = Aggregation Agent
- DBA = Database Agent
- DERA = DER Agent
• DER Agent (DERA): DER agent sends the packet to the aggregation agent. This packet contains DER’s information like ID, price, availability, and quantity.

• Aggregation Agent (AA): Aggregation agent receives information from the DERA along with their bids and thus aggregates the supply into different price slots depending on the bid prices provided by DERA.

• Bulletin Board Agent: It is an agent which represents the real time information obtained from UA and AA and it offers a dynamic contact point through which they can share and retrieve bidding information.

• Database Agent (DBA): “It is responsible for collecting and storing the electricity price, demand and bidding information in database. It also provides access to the database for other agents [6]”.

• Device Agent (DA): It controls electronic devices such as switches and circuit breakers.

• Control Agent (CA): It contains software which performs tasks such as generators synchronization, loading and unloading and others [6].

Figure 2-4 summarizes the activities and interactions of IDAPS agents, as discussed above.
2.3 Security Issues in IDAPS

2.3.1 Security Concerns in IDAPS

The multi agent framework in IDAPS system uses a web-based communication infrastructure. It can exchange information and control data among different agents in the IDAPS through web services. Web service is mainly used for controlling DER operations and hosting bidding events among the members of IDAPS. Therefore, the information transmitted among the agents must be protected and prevented from any kinds of data manipulation, such as changing pricing information, bidding information, etc. The members and DER devices, participating in the market
for buying and selling the electricity should be authenticated in order to communicate with each other. Thus based on the IDAPS system discussed in previous section, we analyze the security issues on the information transmitted between different agents in the system. Table 2-1 describes the purposes and types of information transmitted among different agents, possible attacks and their overall impacts.

Table 2-1: Possible Attacks and Impacts on Multi Agent Interface

<table>
<thead>
<tr>
<th>Purpose &amp; Event</th>
<th>Information Transmitted</th>
<th>Possible Attack &amp; Overall Impact</th>
</tr>
</thead>
</table>
| To initiate, publish or update information of the event in Bulletin board based on information from UA and AA. | Date & time of the event, date & time of event issued, DER Id, and member list (account numbers). | • Confidentiality (L): Eavesdropping on this formation is not of concern since the information may not be sent regularly. The information needs to be protected from unauthorized access.  
  
  • Integrity (H): Attacker can affect the system behavior by modifying the data in the bulletin board such as, date and time of the event published, DER Id, etc. This may lead to the financial impacts on customers.  
  
  • Availability (L): Failure in communication between the UA, AA and bulletin board. |
<p>| To initiate bid request in AA | Date &amp; time of the event, date &amp; time of event issued, DER | • Confidentiality (H): Eavesdropping on this |</p>
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Information</th>
<th>Security Concerns</th>
</tr>
</thead>
</table>
| and DERA.                                                               | Ids, member list (account numbers), request for a bid issue date & time, price offered per time block.  
                                                                           | formation could result in the leaking of bidding and pricing information to the attacker. The information needs to be protected.                                                                                     |
|                                                                         | • Integrity (H): Attackers can affect the bidding program behavior by creating false bidding information.                                                                                                    |
|                                                                         | • Availability (L): Failure in communication between DER agent and aggregation agent.                                                                                                                      |
| To set accepted bids from UA to bulletin board, DERA, AA, CA, and DA.  | Member list (account numbers), accept or reject bids, quantity available during bids per time block (for verification)  
                                                                           | • Confidentiality (H): Eavesdropping on this formation could lead to the invasion of participant’s privacy.                                                                                                   |
|                                                                         | • Integrity (H): Attacker can cause instability of the grid by modifying information like member list, accepted or rejected bid.                                                                             |
|                                                                         | • Availability (L): Failure in communication amongst the agents.                                                                                     |
| To send request for bid to member through UA from AA                   | This information comes in the form of an email, phone call or page.  
                                                                           | • Integrity (L): Attacker can manually send an email, make a phone call or submit a page to the member which may respond to UA or may take wrong action in response to the bid request. |
| To notify the acceptance or rejection notification of bid to the member through | This information comes in the form of an email, phone call or page.  
                                                                           | • Integrity (L): Attacker can manually send an email, make a phone call or submit a page to the member which may respond to UA or may take wrong action in response |
To set, adjust or cancel standing bids in the bulletin board, either by member or by DERA.

| UA                                                                 | Price of the bid | • Confidentiality (M): Eavesdropping on this formation could result in the leaking of pricing information to the attacker. It can cause the leak in the electricity usage of the customer.
|                                                                    |                  | • Integrity (H): Attacker submits bids for user, causing the financial impacts on user.
|                                                                    |                  | • Availability (L): Failure in communication between UA and bulletin board.
| To send the DER information to AA                                  | DER Id, date & time of the event (shed or shift), location, type, Price, Quantity in kW/kWh, Availability (Day-Ahead or Day-Of) | • Confidentiality (H): Eavesdropping on this formation could invade the customer privacy.
|                                                                    |                  | • Integrity (H): Attackers can affect the reliability of the IDPAS system by modifying the information sent by DERA to AA. It could make AA not be able to record the actual response received from DERA. The AA may make an inappropriate response to the DERA according the false information.
|                                                                    |                  | • Availability (L): Failure in communication between DERA and AA.

Table 2-1: Possible Attacks and Impacts between Multi Agent Interface
2.3.2 Cyber Threats in IDAPS

A threat is an unauthorized attempt to access and modify the system through data communication. In IDAPS, agents communicate with each other through a web based communication channel in the network. Network can bring different kind of risk along with it. The threat can be in terms of a virus, worm or poor network architecture. Attacker can try to gain access to the resources in the system through unprotected communication channel. This section focuses on possible attacks on IDAPS system.

2.3.2.1 Access Attacks

Access attacks such as masquerading, session hijacking and repudiation can affect integrity, confidentiality and availability of the system. In access attacks, the attacker may attempt to gain access to the network and its resources. The attacker can gain unauthorized access and modify the DER information and user information. This can lead to improper actions carried out by the agents in the system. Manipulation of information can affect the financial aspect, power usage and the monitoring and controlling information.

2.3.2.2 Denial of Service Attack (DoS)

In Denial of Service attack, the attacker denies the resources to the authorized user and reduces the quality of service for a resource. The attacker can flood the disk space of DBA by sending large messages, Trojan horse, virus or worm and thus harming the system. The DOS attack can be carried out through E-mail bomb, CPU hogging and rerouting attacks. The DOS attack highly
affects the availability of services of all the agents in the IDAPS system by overloading large volumes of attack traffic.

2.4 IDAPS Security Measures

Several modes of attack can take place to tamper the IDAPS system which can range from physical attacks to remote access attacks. It is highly crucial to prevent these attacks for the proper functioning of the IDAPS system. This section addresses the security issues discussed in section 2.3. Here we analyzes security requirements, and suggest counter measures for those security issues.

2.4.1 Security Requirements for IDAPS

The following set of general security requirements is derived from the security concerns specified in Section 2.3:

- Information transmitted during communication between the agents should be protected from unauthorized access and modification.

- Communication between different agents in multi agent framework in IDAPS should be authenticated.

- Information related to the agents such as user information, pricing information, energy usage should be accessed, modified or deleted by only authorized personnel.
• The AA, Bulletin Board, DERA, UA must provide accountability for the information such as prices information, energy usage, and bids submittal information received by participants.

• Information transmitted amongst the agents must maintain confidentiality and integrity

2.4.2 Security Measures for IDAPS

In IDAPS system, a web services are used for communication to ensure the interoperability among the agents. Web Service is a web based, platform independent protocol which is capable of controlling the data in decentralized and distributed environment [14]. Security measures for confidentiality, authentication, non-repudiation and integrity among the various agents can be obtained through web service security.

2.4.2.1 Web Service Security

Web service security is used for secure communication among various agents and interfaces in IDAPS system [6]. For example an exchange of information between two agents will be done via the Simple Object Access Protocol (SOAP) where the messages will be in XML format. When SOAP messages are exchanged over the network, mutual authentication, integrity, and confidentiality are provided by HTTP. However, HTTP provides point-to-point security where as WS-Security provides end-to-end security using encryption. WS-Security signs the SOAP messages to provide non-repudiation and integrity. It also provides encryption to ensure confidentiality and integrity [16]. This section discusses how to enforce the security goals by
using some of the cryptographic tools based on Public Key Infrastructure (PKI) and X.509 certificate format with WS-Security specification.

2.4.2.1.1 Encryption

Encryption is a process of converting data into a code. An attacker can carry out traffic analysis or capture data packets within network to modify the data exchanged between the agents. So it is necessary that the data exchanges amongst the agents is not modified or lost in transaction. Encryption can be used to provide confidentiality and authentication of the data.

Encryption can be done by using the shared key (Symmetric cryptography) or public key (Asymmetric Cryptography) to provide data confidentiality. Figure 2-5 shows the use of shared key encryption (symmetric cryptography). In shared key encryption, both the sender and receiver used the same key and algorithm to encrypt and decrypt the message. Within Web services security, shared key encryption is mainly used for Secure Socket Layer (SSL) security and XML Encryption. A shortcoming for symmetric key cryptography is the key distribution as communicating entities in network need to know shared key beforehand and this increases the chances of eavesdropping. Thus, encryption proves to be costly if large numbers of nodes are present within network.

Figure 2-6 shows the use of public key encryption (Asymmetric cryptography). In public key encryption, the key used for decryption the data is different from the key used for encryption. Public key is used for encryption of data which is generated by the sender of the message. For
decryption the receiver has to use the private key [18]. Internet Protocols such as SSL and IPSec use public key cryptography to carry out authentication and to derive shared keys.

Figure 2-5: Shared Key (Symmetric) Encryption [19]

Figure 2-6: Public Key (Asymmetric) Encryption [19]
However, in the IDAPS system, the information is real-time such as Real-time pricing signal. Using public key encryption could be slow due to the size of cipher text. Another approach is the combination of both symmetric and asymmetric cryptographies. The public key can be used as a long-term key and symmetric key can be used as a short-term or one-time key. The public key is used to establish a temporary shared secret key between the communication pairs by encrypting the shared key and negotiate with the client. After the shared key is established, both communication pairs use this key to encrypt and decrypt messages [19]. Figure 2-7 shows the use of Hybrid encryption.

![Hybrid Encryption Diagram](image)

**Figure 2-7: Hybrid Encryption [19]**
2.4.2.1.2 Non-repudiation

“Non-repudiation is a service which provides the proof of the data integrity and digital origin of data.” Most common method of establishing non-repudiation is implementing digital signatures, which is discussed in next section. Typically, the private key is only known by the owner and restricted from public. Thus, using the corresponding public key can ensure that the sender is the only one who signed the message [21].

2.4.2.1.3 Digital Signatures

Encryption of message only provides data confidentiality but does not provide data integrity. Encryption does not provide protection against the unauthorized modification of message. So message authentication is required for data integrity. Digital signature is mainly used for protection against modification, impersonating and message authentication. Digital Signature Algorithm (DSA) along with RSA algorithm can be used by the receiver to make sure that message came from valid sender. DSA algorithms normally implements asymmetric cryptography where the signature is generated by using the sender’s private key and an appropriate Secure Hash Standard (SHS). Verification is done by using the corresponding public key of the sender and the same hash function. The receiver of the message can ensure that the message came from the source that it claims and the message is not modified by anyone because the only corresponding public key and the same hash function can verify the signature part and only the user that possesses the private key can digitally sign the message [23]. Figure 2-8 show the process of sending and receiving the message using Digital Signature.
2.4.2.1.4 Source Authentication Using X.509 Certificate

For authentication of SOAP message or for identification of the public key within the SOAP message, X.509 certificate is used. For source authentication, X.509 certificate is used, where the certificates are used for verifying the identity of both the server and client. The Certificates are issued by Certificate Authority (CA) and Certificate Store where all X.509 certificates are stored. The certificate includes the credentials of the sender such as identity and public key, and the digital signature of the sender, which is produced by signing the message with the private key of the CA. Client’s public key obtained from X.509 certificate, will be used by the server to validate the signature of the message after receiving it. It’s the task of the server to ensure that the X.509 certificate has not expired and the message is from valid and claimed source. X.509 certificates can be used to provide confidentiality and integrity of the message and source. Message Integrity and SOAP message Confidentiality can be provided by using XML signature along with X.509 certificate. Normally digital signature is enough to secure SOAP message. Time stamp, sequence
number or expiration date can be included into the signature part of the message or of the SOAP
header for some SOAP extension to avoid replay attack. X.509 certificate provides flexibility,
confidentiality and integrity to the messages but it also impacts the speed and complex
computation of the system.

2.4.2.1.5 Key Management
Key Management is also important security features in IDAPS systems. Along with the security
measures for message transmission and message authentication, keys used for cryptographic
purpose also needs to be protected from disclosure. A key management policy is required to
maintain confidentiality, integrity, and authentication of cryptographic keys based on
organization requirement and individual responsibilities. Roles based access controls are required
for management, maintenance, and recovery of the keys. An audit log can be maintained to have
a proper list of keys. Audit log is also maintained by another person other than system
administrator to avoid the misuse of this log which can lead to authorization violation. Public key
cryptography is one of the famous ways for secure transmission of data in communication
networks. The cryptographic keys should be stored and transferred to authorized users in a secure
manner. Different key pairs of private/public key should be used for encryption. Keys used for
encryption are short term based whereas keys for authentication and message integrity are long
term based. There is no requirement to backup the private key if it is used for authentication
purposes. However, the backup of private keys used for encryption purposes or for protecting
stored data in an organization is required. To protect the key pairs a secure place with proper
access control is required. Typically, private key should not be accessible by unauthorized parties.
The public key needs to be protected from unauthorized modification as well. To provide such protection, the public keys can be obtained from X.509 certificates, which are signed by trusted CA. Key distribution tends to be different, based on encryption algorithm and resource constraints.
Chapter 3

DISTRIBUTION SYSTEM SECURITY ISSUES AND SECURITY MEASURES

This chapter discusses the interconnection of DER with the distribution system in the smart grid, the security issues and security requirements for the Distribution system and best practices to deal with these issues and its counter measures.

3.1 Introduction to Distribution System

One of the main goals of the smart grid is to update the current power system from a centralized power generation system to a de-centralized one. Therefore, instead of using the central power plants for energy generations, different and distributed sources of energy can be used. This will allow the utilities to manage the continuous change in the energy demand in a better way. This goal can be achieved by using DER devices as one of the energy generation units. As discussed in previous chapter, DER devices are being installed by the residential user to meet their energy demands at lower cost. However, the utilities and electricity suppliers can also install these DER devices at various locations in the power grid.

Distribution system plays an important role in interconnecting all these widely distributed DER devices in the grid. Figure 3-1 shows the distribution domain in the smart grid. According to the IEEE Smart Grid, “The Distribution domain distributes the electricity to and from the end customers in the smart grid. The distribution network connects the smart meters and all intelligent field devices, managing and controlling them through a two-way wireless or wired
communications network. It may also connect to energy storage facilities and alternative distributed energy resources at the distribution level [24].

Distribution systems are normally considered as supply network providing electricity to which customers are also connected. Automation of operations in distribution system has been available for many years. However, it was only applied to some parts of the distribution system.
Automation was only available to some parts of distribution system, where large numbers of customers were affected with the loss of supply. Thus in rural areas, application of automation was not available in the distribution system, as very few customers would be affected through loss of supply [44]. In rural areas, the distribution equipments that were installed on feeders were expected to function as per the settings, with only occasional manual setting changes. For example, Capacitor bank switches might switch on or off based on local signals, such as time of day or current. However, as the advanced smart grid functionalities such as AMI and DR are being developed and the number of DER devices and PEV installed in the grid are increasing, the need for automation in all parts of distribution system also increases. Automation helps in maintaining and improving the efficiency and reliability of the distribution operations [25]. Figure 3-2 shows the survey result where, utilities were requested to categorize the reasons they used to justify the implementation of automation in distribution system.

![Figure 3-2: Categories of Benefits Used to Justify Automation in Distribution System [29]](image)
3.2 Distribution Automation System (DAS)

The word Automation means doing the particular task automatically in a sequence with faster operation rate. According to NIST a broad definition of Distribution Automation includes “Any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users [26]”. Distribution Automation System (DAS) controls the operations of substation and feeder equipments remotely. Hence, the manual procedures have been replaced by application of automation in distribution system. DAS allows the power system to operate in best optimal way, where the decision making systems and devices are receiving the accurate information in timely manner. Moreover, with the development of communication technologies, DAS has developed into a highly reliable and self healing power system that can respond to the real time events with faster and appropriate decision. The main function of DAS according to IEEE is “the remote control of switches to locate, isolate the fault and restore the service, when a fault occurs in the power distribution line [30]”. The benefits of implementing DAS into the grid are

- Improved reliability by using auto restoration scheme to reduce outage duration
- Use of data information through accurate planning and operations
- Better diagnostic analysis and fault detection
- Better component loading and management of system
- Use of system capacity in improvised way
- Improved quality of supply
- Better service reliability
• Reduction of cost interruption for industrial or commercial customers
• Better quality of supply [7]

Figure 3-3 shows the schematic diagram of the DAS. The DAS contains main components like Transformer Terminal Unit (TTU), Feeder Remote Terminal Unit (FRTU) and Distribution Terminal Unit (DTU) which are connected together through Optical fiber network in Terminal unit, Substation, Control Center (Master station) and power system.

• FRTU: It is a device that is used for monitoring current, voltage and state of switches all the time. These operations are done through automatic switch installed on the distribution line. When the trouble in the distribution line occurs, the trouble point is identified by the information that is transmitted to the Distribution Control Center (DCC). Based on this information the manipulation of switches is done for minimizing the power failure time at troubled site [28].

• TTU: It is a device that can provide real-time monitoring, fault detection, data statistics, and communication management functions.

• DTU: It is a device that can provide real-time SCADA control and monitoring and fault detection.

• Control Center: It is an integrated operation system of distribution line at DCC. It monitors and controls the various FRTU devices that are scattered on the distribution line for line operations. They are used for minimizing the power failure time at troubled sites. It acquires real time data through collecting line operation data such as voltage and current. These real time data helps in indentifying the outage area in distribution line.
Control Center system manages the operations in distribution system in most effective ways [28].

![Schematic Diagram of Distribution Automation System (DAS)](image)

**Figure 3-3: Schematic Diagram of Distribution Automation System (DAS) [27]**

### 3.2.1 Communication Technologies Used in DAS

Communication system plays an important role in DAS system. It provides the link between the customers, smart devices on the grid and system operators for their communication. The Communication System is required to communicate data from control center to various units like FRTU, TTU, and DTU and vice versa. Essentially, the communication system refers to the
communication equipment and interface needed to transfer data between DCC and different remote terminal units. Utilities install many DA functions throughout the power grid. These functions are used for different applications. Thus their requirements in communication are also different. However, no communication technology is available which meet the requirements in all the DA functions. Thus proprietary protocols were used for implementation of DA functions. The communication media can either be wired such as cable, fiber, telephone line, etc or wireless such as wireless-in-local loop, radio etc. However these communication technologies introduce new set of vulnerabilities into the system. These security issues and vulnerabilities are further discussed in the next section.

3.3 Security Issues in DAS

Automation in distribution system is mainly involved to increase reliability, efficiency and quality of the electric power system. In DAS, large number of geographically dispersed devices has been implemented in the network. These devices use various communication technologies to provide real time description of events to perform automation. However, by involving the automation into the distribution system, the possibilities of risk and threats to the system increase. For example, automation in distribution system allows the system to operate the switches and breakers through remote connection using communication technologies. These remote connections introduce new set of threats such as malfunction of system, eavesdropping, reply attack. The security requirements, security concerns and possible threats to the distribution automation system are discussed in this section [8].
3.3.1 Security Requirements of DAS.

In this section, the security requirements for the distribution automation system are discussed.

3.3.1.1 Confidentiality

The transfer of information between different components in the DAS system such as control center, FRTU, DTU, TTU must be confidential. Leak of message can lead to many threats in the DAS which will be discussed in Section 3.3.2. So the messages and information that are being transferred between different components in the system should be protected from unauthorized access by personnel and other adversaries. One of such example of the information to be secured is the transfer and exchange of secret key distribution where the secret key should be protected and secured from attackers and adversaries. It can be protected by symmetric or asymmetric key encryption algorithms [31].

3.3.1.2 Authentication

The Receivers of message and information should verify that the said message is being sent by legitimate sender and not by some attacker. Attacker can send malicious messages to FRTU or DCC which can create lots of malfunction or black out. It is one of the important requirements to maintain the security in the Distribution Automation system. The components should be authenticated on the basis of access control [31].
3.3.1.3 Integrity

Integrity is also one of the important security requirements for many applications in the distribution automation systems. The receiver of message and information should verify that the said message is not modified in any way by the adversaries. Unauthorized access and modification to any information such as load management, electrical usage and many others can lead to many attacks on the system. These attacks can lead to instability of the grid which can affect the efficiency and reliability of the distribution system [31].

3.3.1.4 Message Freshness

Message freshness means that the message that is received by the components in the system is fresh and is not the old message that is replayed by the attacker or adversaries. There are two types of freshness.

- **Weak Freshness**: It maintains ordering of the message but the delay information is not maintained in this freshness. It is mainly used in the application where the need to protect it from the reply attack is important.

- **Strong Freshness**: It not only keeps the proper ordering of the messages but also gives the information of the delay estimation. It is mainly used in the application where time synchronization is of main concern in the network [31].

3.3.1.5 Availability

Availability is also one of the important security requirements in the distribution automation system, as the services in the distribution network should be available to all the nodes and
elements all the time when required. Unavailability can lead to instability and affect the efficiency of the system. Failure to achieve information in the distribution system can lead to incorrect load control mechanisms. This can lead to threats like denial-of-service [31].

3.3.1.6 Access Control

Access control policies are mainly used to authorize the users and servers on the system to limit the unauthorized access of information transferred between the elements in the system. Access control can be implemented by authentication and authorization of the system and devices as who can log onto the system and who can control the DCC, to avoid an inside attack on the system. The utilities should carry out operations such as registration, configuration, and maintenance of the accounts of the users and employees based on the access rights assigned to them. The utility should carry out tasks such as activating, managing, reviewing, updating, disabling and deleting accounts of distribution system personnel’s from time to time to track proper access controls. Any breach to these accounts must be detected and immediately reported to the control center.

The requirements to maintain access control on the systems are

1) Authentication should be provided to all the user accounts.

2) The ability to assign feature and functions should be based on the user account.

3) Log should be maintained to observe the sequence of the events in which they occur.

4) The ability to monitor security events and make the information available to control centers [8].
3.3.2 Cyber Threats in DAS

A threat is an unauthorized attempt to access and modify the system which causes the service to be unavailable. In Distribution system communication technologies play an important role. Communication may occur either through wired network like fiber optical network or through wireless network like CDMA. Network can bring different kind of risk along with it. This section focuses on possible attacks in the DAS network.

3.3.2.1 Denial-of-Service (DoS)

One of the typical and most common attacks on the DCC server is the DoS attack. Dos attack mainly leads to the unavailability of the message or information to the FRTUs send by DCC server. Normally this attack is done by creating excessive load on the DCC server which will result in exhausting its computer resources ultimately making the resources unavailable to the server. Sometimes the attacker can send malicious and unwanted messages to the DCC server by taking over some of the legitimate nodes in the network. In case of the passive attack, attacker can cause malfunction of the system or halt their functions for some time by sending malicious information like virus to the system. Normally if these attacks are made on the server, it does not much affect the system, as it can always be rebooted. These attacks would not much affect the FRTUs, as DCC server which is mainly handled by authorized users, can handle this kind of attack in short amount of time. However, if this attack occurs on FRTUs the effect is much worse. It can mostly lead to the unwanted operations in the systems as FRTUs, installed on the remote site are mostly unattended and are directly responsible for the distribution system operations.
3.3.2.2 Eavesdropping

If the content of the message that is being exchanged between the DCC server and FRTUs is leaked to the intruder and outsider, this type of attack is known as eavesdropping. Normally the kind of information and messages that are exchanged between the FRTUs and DCC server are operating data such as voltage, current and control commands. Attacker can also collect traffic data through which the attacker can guess the information that is exchanged from the traffic data pattern. Unless the FRTUs are forced to function improperly, the knowledge of information to the intruder doesn’t affect the system much. However, it can lead to much damage if the information exchanged is of secret keys that should be known only by concerned parties.

3.3.2.3 Malfunction of System

One of the main and most important threats to the DAS system is to make the FRTUs in the system to malfunctions. There are three attacks that lead to the malfunction of FRTUs.

- To deliver false messages to the FRTUs after altering the contents of the messages that is exchanged between the DCC server and FRTUs. These false messages can control the automatic switches which, if controlled in malicious ways, can ultimately lead to power outage.

- To inject bogus messages into the communication channel. They can make the FRTUs to act in malicious way by sending them illegal message. Attacker can act as the server or can also carry out man-in-the-middle attack by intercepting the communication channel.

- Reply attack is third kind of threat that can make the FRTUs to malfunction. In this threat the attacker normally gets the information from the communication network and delivers
those same messages to the FRTUs after some time, which can lead to malfunction of FRTUs [31].

3.3.3 Security Goals

Table 3-1 shows the correlation between the security requirements discussed in Section 3.3.1 and security threats discussed in Section 3.3.2 and its degree of importance.

Table 3-1 Correlation of Security Requirements and Threats [31]

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Cyber Threats</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Confidentiality</td>
<td>Eavesdropping</td>
<td>Low (except key exchange)</td>
</tr>
<tr>
<td></td>
<td>Traffic Analysis</td>
<td>Low</td>
</tr>
<tr>
<td>Message integrity</td>
<td>Message Modification</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>False Message Injection</td>
<td>High</td>
</tr>
<tr>
<td>Message Freshness</td>
<td>Message reply</td>
<td>High</td>
</tr>
<tr>
<td>Availability</td>
<td>Denial-of-service (DoS)</td>
<td>Middle</td>
</tr>
<tr>
<td></td>
<td>Malicious code</td>
<td>Middle</td>
</tr>
<tr>
<td>Source Authentication</td>
<td>masquerade</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access</td>
<td>Middle</td>
</tr>
</tbody>
</table>
Depending on these correlation, some of the security goals has been formulated which is achieved by using the security measures that is discussed in next Section 3.4

- Receivers should be able to verify that messages they receive are from claimed senders.
- Receivers should be able to verify that messages they receive are not compromised in transit.
- Receivers should be able to verify that messages they receive are not replayed by any attacker.
- Critical contents of messages such as secret keys should be secured in transit [31].

### 3.4 DAS Security Measures

As a result of new emerging technologies in communications, along with the Internet and Telecommunication which has been integrated into the smart grid, it gives way to new era of electricity market. Due to this, the two-way communications among the users and utilities in the distribution system have been developed. Several attacks can take place on the communication links in the distribution systems which can range from physical attacks like insider attack to remote and cyber attacks. Attackers can misuse the information gained by them to increase or decrease the load on the system, to create malfunction of the devices like FRTUs. It is necessary to take security measures to avoid these attacks by existing security policies and standards available for communications in distribution systems. This section provides counter measures and potential best practices for related security issues in Distribution Automation System.
3.4.1 Secure Information Flow

Information related to the voltage/current, trouble status acquired, price information and energy usage are transmitted between DCC server and FRTUs of DAS system. The secure exchange of information between these entities is important. Authentication of entities between whom the exchange of information and message takes place is strongly required. Mutual and message authentication should be used between these entities to ensure integrity of the message. Encryption can be used for data confidentiality. Secure communication through appropriate communication protocols, such as Transport Layer Security (TLS) protocol is needed to protect network traffic.

3.4.2 Access Control

Access control is required to make sure that the resources of the distribution automation system are available only to the authorized personnel. Identification and authorization of the user, process, or component are required for granting access to the resources of the system. Identification can be done through password or an encrypted token. Role Based Access Control (RBAC) and Mandatory Access Control (MAC) for personnel within utility and its sub-systems can be used for authentication. Adding, altering, and removing access rights should be done from time to time to manage the access control list and capability list [8].

3.4.3 Account Management

The utility should maintain the security in DAS by creating, activating, maintaining, disabling and deleting the account of utility employees and third party contractors. Account management
should include identification of account types, establishment of the conditions for group membership and conditions for the access of functions or features available. Access to the function or feature in DAS is based on the account types and group membership. Modification within the account management system should be handled by the control center of the DAS [8].

3.4.4 Communication Link

Previously, most of the communication in the Distribution Automation System was based on, on-demand dial up connections. This connection was most cost effective in urban areas. Normally the dial-up connections were made secure through the use of caller-id to ensure that only authorized devices are connected and resources are available only to the authorized devices. But with emerging technologies even the dial up is becoming vulnerable to attacks such as address spoofing. So for additional security, dial-up connection sets the TCP/IP link using PPP protocol with CHAP authentication. Moreover IEC 62315 family of standards has specified the use of Transport Layer Security (TLS) to secure TCP/IP based protocol [8].

3.4.4.1 PPP Protocol with CHAP Authentication

Challenge Handshake Authentication Protocol (CHAP) is normally used for authentication of the peer by using a 3-way handshake protocol. Figure 3-4 shows the CHAP authentication. After the link is established between the server and the peer, the server sends a challenge message containing a value to the peer for verifying its identity.
Peer sends back a response message which contains a hash-value obtained from the value in the message after performing MD5 on the value. Before sending the message, server also calculates the hash-value. So when the peer sends the hash value in response message, server has something to compare the hash value with. Based on this hash value the verification of the peer is done. If the value matches, the communication is established for exchange of data, else the communication is denied. This challenge and response message is normally used to verify the
authentication. This authentication is normally used for verifying the identity of the peer and for preventing the unauthorized party to gain access to the network [32].

3.4.4.2 TLS 1.0 with Server Side and Client Side Certificate

The IEC 62351-3 standard recommends use of Transport Layer Security (TLS) for the protection of the information flow by authentication of both the party and encryption of data. TLS protocols provide a very good security between the control center and the FRTUs as it is applied to the application level. However, the use of certificate is required in TLS for authentication and TLS should also be supported at both the ends [8]. This method of authentication is very costly as it requires authentication from both server and client to establish connection between them. Moreover TLS is vulnerable to man-in-the-middle attack. Figure 3-5 shows TLS handshake along with the MITM attack.

TLS allows the refreshing of the cryptographic keys at any time by requesting the renegotiation of TLS session by either client or server. However during the renegotiation of the TLS session, concern for client authentication arises. Each time a client or server requests for renegotiation, they have to carry out the basic TLS handshake. So in order to obtain the client certificate, HTTP has to renegotiate the TLS channel. During this authentication there is a loss of continuity called “Authentication gap” which occurs because there is no cryptographic binding between the old connection and the newly established one [33]. Thus, the TLS protocol allows an attacker to carry out a number of MITM attacks due to which unauthorized data is injected into the authenticated SSL communications. This demonstrates that the existing systems which are currently
implemented using client certificates authentication are vulnerable. Server needs to disable the renegotiation in order to prevent MITM attack, until the TLS protocol is fixed. The short-term fix of this problem is to disable client-side certificates.

Figure 3-5: TLS Handshake with Server and Client Side Certificate - MITM Attack [33]
3.4.5 Securing Control Operations

Power system normally uses the DNP3 protocol for the communication of field devices with control center. However the deficiency in the security system for the DNP3 is that it always assumes that the message received or control message issued is from the legitimate control center. It never verifies the identity of the sender of the control message. This can lead to attacks such as spoofing, modification and reply attack. So to overcome this deficiency in the DNP3 protocol, two types of authentication modes can be used

- Challenge Response Mode

- Aggressive Mode

Challenge Response Mode:

The main concept of this authentication is challenging the other parties whenever they receive a critical protocol message also known as Application Service Data Unit (ASDU). Figure 3-6 shows the Challenge Response authentication mode. The challenge message send by the challenger contains pseudo-random data and a sequence number. The response message send by the responder contains a cryptographic hash (HMAC) value calculated from the challenge message, the sequence number and a shared secret key. Since both the challenger and responder share the secret key, they will both calculate the same hash value, thus authenticating the other party and the integrity of the message.
Aggressive Mode:

The steps required in the challenge mode for authentication are large in number and hence is time consuming. Another method is the aggressive method. Here along with the critical ASDU, random number is also attached and sent to the challenger for authentication. The challenger does the same process as above and authenticates itself thereby saving time. Even if there is a risk of replay attacks, it can be easily avoided if external replay protection is provided. Figure 3-7 shows the Aggressive authentication mode [8].
3.4.6 Cryptography

This section discusses the cryptographic mechanism to overcome some of the security issues related to DAS system. A successful cryptographic mechanism can be achieved through use of encryption, digital signatures and management of keys.

3.4.6.1 Encryption.

The first and most important area of cryptography to discuss is encryption. The use of encryption can be done by using the shared key (Symmetric cryptography) and public key (Asymmetric Cryptography) from the X.509 certificate in order to provide data confidentiality.
Symmetric key encryption used for authentication purposes between sender and receiver uses the same shared (private) key over the network. Symmetric cryptography can be used for those applications where asymmetric (public) key cryptography is found to be computational expensive. Figure 2-6 shows the symmetric key encryption. This encryption provides confidentiality and authentication. An authentication tag called Message Authentication Code (MAC) can be generated from the symmetric key encryption. Normally sender generates this authentication tag which is appended to the end of each message that is transmitted. Receiver can verify the sender and can also verify if the message is modified or not from this authentication tag. It is mainly used for message authentication. Figure 3-8 shows the procedure for message authentication and integrity using MAC. The Sync Code is used to verify the weak freshness of the message. The value of a new message using MAC authentication tag should be bigger than the one of an old message as the Sync Code is a non-decreasing number. Through this, whether the message was resent or not can be determined, thus making sure that no attackers replay old messages.

H: a hash function

Mₐ: Message sent by A

{Mₐ | Mᵦ}: Concatenation of message Mₐ and Mᵦ

Nₐ: a nonce generated by A

C: sync code used for verifying message freshness
This approach has an advantage that, here the whole message is not required to be encrypted which saves lots of time and computation cost. Alternative way to use MAC without encryption is using HMAC. It is a comprehensive message authentication code without encryption. It can be used in combination with other iterative cryptographic hash functions such as MD5 or SHA-1 [31].

3.4.6.2 Digital Signature
Digital signature is mainly used for protection against modification and impersonating as encryption does not provide data integrity. Digital Signature Algorithm (DSA) along with RSA
algorithm can be used by the receiver to make sure that message came from valid sender. Public key of the sender and the same hash function used for digital signature can be used by the receiver to authenticate the sender. It is mainly used for message authentication as only the corresponding public key of the sender and the same hash function can verify the signature part of the message and only user possesses the private key to sign the message. Figure 2-9 describes the process message authentication using digital signature.

3.4.6.3 Certificate Authority

For verifying the digital signature, the corresponding public key of the sender is required. Public key is used for verification of entities like person, server or device through electronic documents called Certificate. Certificate Authorities issue certificate to verify the identity of subject requesting the certificate. A public key is bounded to this issued certificate along with name of the requester. This prevents impersonation of fake public keys. The public key will only work in conjunction with the corresponding private key possessed by entity identified by the certificate. Out of the key pairs generated by the requestor, public key is used along with algorithm type and requestor’s name for CSR. . Figure 3-9 shows how X.509 certificate is obtained from CA. The issued certificate includes the credentials, such as the applicant’s public key, issuer’s name, applicant name, expiration date and the signature part; i.e. message signed by private key of the CA,. Each node in the network is required to have three keys; CA’s public key and its own pair of public - private key. The most common standard for digital certificates is X.509. CA has to revoke X.509 certificates if integrity of certificate is negotiated. The certificate revocation list
(CRL) is publicly available for the recipient of signed message to verify whether certificate has been revoked or not.

Figure 3-9: X.509 Certificate Issued by CA [35].
This chapter discusses the interconnection of DER with the synchrophasors in the smart grid, the security issues and security requirements for the synchrophasors and best practices to deal with these issues and its counter measures.

4.1 Introduction to Synchrophasor System

In chapter 2 and 3 interconnection of DER with micro grid system and distribution system are discussed. As discussed previously, DER systems play a major role in smart grid for converting the current power system into a de-centralized and consumer-controlled power system. As a result the number of these distributed generation units in the smart grid are increasing which are either owned by consume for personal use or owned by utilities. So the electricity that is generated from these different generation units may not be on the same phase. The state of the Power system, i.e. the efficiency of the power system and the quality of the energy generated is estimated by the control center from the measurements of the flow of power through power grid. In power system, electricity quantity; i.e. the amount of electricity that is passing through the power grid is measured through a device called phasors. It is assumed that all these electrical quantities are at same phase and frequencies. New techniques have been developed for all the electrical quantities that are at different phase and frequencies in the power grid. In this new technique called synchrophasors, phasor devices are synchronized at absolute time. Figure 4-1 shows the basic architecture for synchrophasor system. As name suggests synchrophasor is a method used for
real time measurement, control and analysis of absolute phase relationship between two electrical quantities from different energy generation unit at different locations on power system. These real-time measurements include the time stamp, which helps in analysis and comparison of different electrical quantities that come from different location and take different time to reach a common collection point [43].

“Synchrophasor technology can be summarized as marking power system quantities with a high-accuracy time tag in order to be able to use data from multiple sources in a coherent manner [9].” In synchrophasor systems, the device that measures the electrical quantities from all the different locations in the power grid is called phasor measurement unit (PMU). Each phasor measurements are time-stamped according to the universal time standard, so measurements taken by PMU devices at different locations can all be synchronized and time-aligned. Monitoring and analysis of these measurements allows the system to identify changes in grid conditions,
including the amount and nature of stress on the system, for better maintenance and reliability of the power grid [9].

Synchrophasor system collects, distributes and analyzes the critical data and converts it into real time information which helps in automation of grid and its operations. Transmission efficiency and utilization of energy could be improved, by using phasor data to manage the grid operations. Figure 4-2 shows the typical synchrophasor system components and its data flow.

![Figure 4-2: Typical Synchrophasor System Components and its Data Flow [9]](image)

As shown in the above figure, there are several data paths in synchrophasor systems. The first level of these data path contains PMU which is connected to the Phasor Data Concentrator (PDC). PMU measures electrical quantities from the power system. Protective relays, meters, digital fault recorders (DFRs), or other intelligent electronic devices (IEDs) can be included in the
PMU functionality. PMU devices can normally measure the grid conditions at the rate of 60 to 240 measurements per seconds in comparison to SCADA which collects the measurement at interval ranging from 2 to 15 seconds. Most systems are connected to the Global Positioning system (GPS) to have accuracy in the measurements collected from different locations across wide area systems at same instant in time. Due to this time tag, measurements can be compared directly without the need of any complex algorithms. At PDC the data is collected from different PMU devices and is sorted into different groups according to the time tag. PDC generates a concentrated packet for each time tag, which includes the values from all PMUs. After PDC receives the data, the sharing of data between the PDCs at same hierarchical level as well as at higher levels is also required [36]. PDC can also perform other functions such as calculations, logical operations, archive data, or even take control actions. Figure 4-3 shows the example of the electrical quantity measurement that was converted in same phase through synchrophasor systems. Simply put synchrophasor system collects data from different locations on the power grid which mainly includes the distributed generation units with the renewable resources and converts them into the same phase with absolute time tag using GPS.

Synchrophasors can also be used for

- Wide-area visualization
- Modal analysis
- Post-event analysis
- Power system model validation
- Wide-area synchronism check
- Loop flow analysis [9]
4.2 Security Issues in Synchrophasor System

Synchrophasor systems are still in their early developing stage for many organizations that are using the system. So they are not considered critical to the security of these power system operations. They are mainly developed to complement the existing system and infrastructure for their time and cost efficiency. So if the security is not built into the existing system understanding the critical importance of synchrophasor system soon, then there will be some security leaks which will lead to vulnerabilities for the new developing power systems. So it’s better to design the security requirements of the system keeping in mind its critical importance. In next section, the security requirements, and cyber possible threats to the synchrophasor system are discussed.
4.2.1 Security Requirements in Synchrophasor System

In this section, the security requirements for synchrophasor systems are discussed.

4.2.1.1 Confidentiality

The transfer of information between different components in the synchrophasor system such as PMU, PDU, GPS, Control center and applications must be confidential. Normally the data and information obtained from synchrophasor system is considered confidential for the sole purpose of competitive reason. So the messages and information that are being transferred between different components in the system should be protected from different adversaries and should not be read by illegitimate nodes.

4.2.1.2 Integrity

Integrity is also one of the important security requirements for the synchrophasor system. Integrity is the security requirement where the receiver has to make sure that the data it received is from a legitimate and authorized source and it is not modified in any way from its original data during the transport. Modification of data can cause the control center or the operators to take the inappropriate actions. For example, an attacker could modify the voltage angles fed into a wide-area synchronism-check system by adding pi radians to the real value. It could close the breaker while systems are out of synchronism and cause significant damage to the power system equipment. So modification of data or unauthorized access to synchrophasor data can make the system vulnerable to the attacker which can lead heavy damage to the reliability of the system [9].
4.2.1.3 Availability

Availability is a security requirement where synchrophasor data should be available to the application or corresponding entities in timely manner. An attacker normally creates situations which can lead to the unavailability of the data. Attacks like denial-of-service can cause instability of the system and can have adverse effect on the applications.

4.2.1.4 Authentication

The Receivers of message should verify that the message is being sent by legitimate sender and not by some attacker or an unauthorized replay of the data. Attacker can send malicious messages to PMU or PDC devices which can cause malfunctioning of the system. It is one of the important requirements to maintain the security of the system. A failed authentication can cause the attacker to modify the data or gain access to the PMU or PDC devices for unauthorized access to the system.

4.2.1.5 Secure Substation

One of the security requirements for the synchrophasors system is the secure substation. Attacks can take place directly on the substation which can affect the efficiency and reliability of synchrophasor system. Moreover it can also lead to the malfunction of the system. One of these concerns is the attack to substation from external cyberspace. Access points in synchrophasor system which are connected to substation as well as with other systems in the power network should be secured. These are the access points where the attack to substation is most likely to come from. One of these access points are PMU devices. PMU devices normally collects the data
for synchrophasor system, which is afterwards transmitted to other components in the system, like PDC devices. Normally the devices in the system that communicate with the external client are present within a perimeter network. A security gateway device separates the substation LAN and the perimeter network. It is important that there is no connection between these networks other than the local gateway which is developed for this particular purpose. There are some cases where the security of the synchrophasor data is at high risks [9].

1) When the phasor data flows through the unknown networks which can’t be trusted to be secure. Unidirectional Synchrophasor Streams can be used. It is discussed in Section 4.3.

2) When accessing the PMU settings remotely through an unsecured protocol like Telnet, it may possess cyber threats. Telnet transmit data in a cleat text format. This can lead to much vulnerability, as device setting and login information are exposed in the network. Secure channel like Secure Shell (SSH) should be used for remote access [9].

4.2.2 Cyber Threats in Synchrophasor System

A threat is a deliberate unauthorized attempt to access, modify, and cause the service to be unavailable. The components in the synchrophasor systems communicate with each other through a communication channel in network. This section focuses on possible attacks in the synchrophasor system.

4.2.2.1 Eavesdropping

In eavesdropping attack, the message that is being exchanges between different devices in the system is leaked to the intruder, without the consent of the system. Normally the kind of
information exchanged in the system contains data such as power measurements from power system, time tag information from GPS, etc. Attackers can also collect traffic data which indirectly lead them to guess the information that is exchanged. This attack can cause much more damage if the information exchanged is of secret keys that should be known only by concerned parties.

4.2.2.2 Modification
In modification attack, false messages are delivered to the substation or other entities in the system like PMU after altering the contents of the messages that is exchanged between the different entities in the system. These false messages can make the system unstable as it can affect the quality of the electricity delivered by the utilities due to the modified message.

4.2.2.3 Denial-of-Service (DoS)
In DOS attack, the attacker attempts to deny access to legitimate user to a particular resource, or, at the very least, reduce the quality of service of a resource. It is one of the most common threats on the synchrophasor systems. It is normally done by flooding PMU devices by sending large messages, Trojan horse, virus or worm and thus exhausting the system which ultimately leads the unavailability of the resources to the user.

4.2.2.4 Spoofing
In spoofing attack, attacker can make the system to act in malicious way by sending illegal message to the different components and devices in the system. Attacker can act as the server or
can intercept the communication channel in form of man-in-the-middle attack. This can lead to the instability or malfunction of the system depending on the wrong information sent by the attacker.

4.3 Synchrophasor System Security Measures

As a result of new emerging technologies in communications along with Internet and Telecommunication, new era of electricity market has been developed. Several attacks can take place on the communication links which can range from physical attacks like insider attack to remote and cyber attacks. Attackers can misuse the obtained information to increase or decrease the load on the system, to create malfunction of the devices like PMUs, etc. In order to discuss these security measures in more analyzed way, these security concerns and their related security measures are divided into two groups

1) Substation Security Measures
2) Information Security Measures

4.3.1 Substation Security Measures

One of the main security concerns in synchrophasor system is the attack on the substation network and cyber assets within it. One of the ways to protect the substation from external cyberspace attack is to secure the access points and limit their exposure to the outside world. The attacks to substation will most likely come from, these access points, as they are connected to substation and other entities the systems. One of the ways to limit the exposure of these access points like PMU devices to outer world is to have multi layer architecture. In this architecture
each layer will provide a new level of security to PMU devices. Figure 4-4 shows the multilayered architecture proposed for substation security.

In this multilayered architecture, the data exchanged between PMU and other entities passes through the entire protective layer in the architecture before it goes outside the perimeter network. This architecture will provide protection against the threats such as modification and spoofing [9]. As shown in the figure above, PMU devices which send the data outside the substations are in the first layer, known as security gateway device. These security gateways devices have the same properties which can fulfill the roles of Firewall and Virtual Private Network (VPN) tunneling.
Firewalls:

Firewalls are like imaginary walls that restrict the entry and exit of information i.e. incoming and outgoing of network traffic depending on the rules and policies defined by the users. White-list approach is mostly recommended for substation security, while setting the rules and policies for the firewalls. As in white list approach all the traffic and data is blocked and only data that is explicitly defined in the rules is allowed to pass. By using the white-list approach, only the necessary data which is required to be delivered to the client outside the substation is allowed to pass. Moreover gateway devices make the access points like PMU devices, which are behind these gateway devices, invisible to other entities that are outside the gateway security. It is visible to only those clients to whom the data is delivered. Figure 4-5 shows the example of firewall, as where it is normally positioned in the security architecture [9].

Figure 4-5: Example of Firewalls in Security Architecture [39]
Virtual Private Network (VPN):

A VPN network is normally developed to encrypt and secure the synchrophasor data from the other traffic in the network. The termination points of the VPN tunnel are the security gateway devices of the substation and another device that supports the same VPN protocol at the control center. Thus, synchrophasor data flow across the untrusted network in an encrypted format. Then the data is decrypted at another termination point which is then delivered to the client. So the main advantage of these VPN network is that the client, PMU or PDC devices doesn’t have to support any encryption to secure the data from attacker. Figure 4-6 shows the example of the VPN working along with firewall [9].

Figure 4-6: Example of VPN Working with Firewall [40]
In this multilayer architecture, even the PDC device can act as an additional layer to avoid the direct access of PMU. So client will receive the data from PDC instead of directly from the PMU. It will definitely minimize the need for the client to directly access the PMU settings. Example, if the IP settings of the control center changes, it is easier and sufficient to change the settings of PDC by remotely accessing it instead of changing the settings of individual PMUs.

Even with the multilayer architecture, the traffic of synchrophasor data has to pass through the untrusted network. For this security issue, unidirectional synchrophasor streams which are normally known as UDP Secure (UDP_S) can be used. UDP_S allows more simple and restrictive firewall rules because of its unidirectional characteristic. UDP datagram is the only traffic that is allowed to pass from the server to a given destination endpoint. All the other incoming and outgoing traffic is blocked by UDP_S. As server is not the one who initiates the datagram, and to initiate the datagram client does not need to know the address of the server, the client can be made invisible to the network. Moreover it is also secure against attacks like spoofing as it does not take messages like “stop “commands frames [9].

4.3.2 Information Security Measures
A cyber attack is not only limited to the attack on the substation, but also on the data that is coming out of the substation. Security requirements such as confidentiality, integrity, availability and authentication should be maintained from end-to-end in synchrophasor system for information security. All these requirements should be maintained all the way from PMU devices, substations, Wide-area network (WANs) to the end user application. As synchrophasor data are
used in power system monitoring and control, a potential attack on these data can be dangerous. In this section, the best practices for information security in the synchrophasor system are discussed [9].

4.3.2.1 Data Transmission
To ensure integrity of the message, mutual authentication should be used between substations and the clients. The information in the synchrophasor system needs to be encrypted in order to provide data confidentiality. Synchrophasor systems uses VPN to encrypt the data and send the information to the client in decrypted form and at the end point of VPN, the data are decrypted and delivered to the client.

4.3.2.2 Data Handling Practices
In synchrophasor system, data is not only exchanged between the substation and utilities but also between the substation and third party contractors. Reusing or disclosing of data by third parties could affect the working and reliability of the power system and can also affect the quality of the energy. So data transmission must be done in secured condition so that only authorized entities can access the data and only necessary information is exchanged with outside entities.

4.3.2.3 Encryption
Data in synchrophasor system is mainly transmitted through the IP networks or direct serial links. Communication link connects various substations to one another and to control centers. However, these links cannot be trusted as they may be passing through the untrusted networks. This can
lead to many threats and attacks on the synchrophasor data, if the data confidentiality and integrity is not maintained. One of the solutions to maintain data confidentiality and integrity across these untrusted networks is encryption during the link layer or IP layer.

Link Layer Encryption:
Link layer encryption takes place at the data link level between the two points of transmission in the network, where the communication link for transmission cannot be trusted. In link layer encryption the plain text data is encrypted by the source of data and is then send to the destination. Data is then decrypted at the next end point which can either be destination or another access point in the link. Data is then once again encrypted and then send to the next access point. This process is continued till the data reaches its destination. Each link can use different algorithm for encryption or can also use different key for same algorithms. Various encryption methods are available at the link layer, depending on the communication link used during the transmission. For example serial encryption device like EIA-232 can be used for serial encryption. SONET multiplexer can also be used for encryption, which provides security which is similar to end-to-end encryption security but with much greater data rates.

4.3.3 Security Concerns and its Solutions.
Table 4-1 shows the list of security concerns to the synchrophasor systems and best practices to deal with those issues in the system.
Table 4-1 Security Concerns and its Solutions

<table>
<thead>
<tr>
<th>Cyber Security Concerns and its Solutions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Concerns</td>
<td>Solutions</td>
</tr>
<tr>
<td>External attacks to PMU</td>
<td>Firewalls and VPNs</td>
</tr>
<tr>
<td>Unauthorized access to substations</td>
<td>Multilayered security architecture</td>
</tr>
<tr>
<td></td>
<td>Firewalls and VPNs</td>
</tr>
<tr>
<td></td>
<td>UDP_S</td>
</tr>
<tr>
<td></td>
<td>Disable unused ports and devices</td>
</tr>
<tr>
<td>When traffic flows through untrusted network</td>
<td>UDP_S</td>
</tr>
<tr>
<td>Spoofing</td>
<td>UDP_S</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>VPNs or Link encryption</td>
</tr>
<tr>
<td>Integrity</td>
<td>VPNs or Link encryption</td>
</tr>
<tr>
<td>Availability</td>
<td>Limited exposure of communication link</td>
</tr>
<tr>
<td></td>
<td>Real-time status and notification</td>
</tr>
<tr>
<td></td>
<td>Logic checks for data availability and validity</td>
</tr>
<tr>
<td>Denial of Service (DoS) attack</td>
<td>Firewalls</td>
</tr>
</tbody>
</table>

Table 4-1: Security Concerns and its Solutions [9]
Chapter 5
RESEARCH ISSUES

5.1 Overview

Security issues and their counter measures associated systems interconnected with DER such as Micro grid system, Distribution Automation system and Synchrophasor systems were discussed in previous chapters. These security measures and best practices help in maintaining the confidentiality, integrity and availability of the information in these systems in smart grid. However there are number of issues that require research to be carried out. Models for them need to be developed appropriately. This chapter discusses potential research and development topics relevant to these systems in smart grid.

5.2 Authorization and Authentication for IDAPS

Smart devices are integrated with the IDAPS system to receive signals back and forth between customers and IDAPS agents. These signals update the information such as electricity prices, availability of electricity, bidding information, etc. Interference with these signals by attackers can affect the IDAPS system. So authentication of these signals and devices with other devices, and entities in the smart grid is important for source and message authentication and authorization. The main aim of this research issue is to determine effective and appropriate authentication techniques for the smart devices depending on their limitations. Smart devices and systems have many limitations, which do not fulfill the requirements for smart grid such as memory, battery life, CPU computations and many more. Complex encryption algorithms and key management can be used for authentication and authorization process, but these processes
should be easy and simple so that even the customers who are non-technical person can understand how to use it. Authorization of different entities such as maintenance personnel, installers, utility operators and customers can be done through Role Based Accessed Control. Only authorized entities should be able to access the device and system. Roles should be assigned in such a way that the consumer himself cannot manipulate the incoming information from the devices. The main area of research in this topic is to define the roles and determine as which entities should perform those roles. Some of the access control policies and techniques that are already in use with current grid could be used in smart grid as well.

5.3 Security Issue in Log Information

There are people who normally manage the tasks such as administration, technical operators, and feedback operators. They are the one who manages the signals in the IDAPS system. The transmissions of these signals are maintained through agents such as DERA, AA, DBA and UA. Based on the roles of performing the operation and login session information, logs for each user’s account should be maintained. Logs are necessary to determine Role Based Access controls to view and delete information from the log. The main area of research in this topic is to determine how these logs should be maintained, how long these logs can be stored and how frequent the backups of these logs should be scheduled [41].

5.4 Traffic Analysis

Traffic analysis is the process of examining the information pattern to acquire information from the system. The data exchanged between the customers and various agents in the IDAPS system,
consists of price bidding, energy usage and customer information. This creates pronounced traffic patterns that can reveal the flow of information and location of DER devices. An attacker can determine the transfer rate of data packets as well as correlation of time between the communicating nodes through traffic analysis, even if messages are encrypted. Message length, frequency, header information and address can be used to know the identity of the source and destination of the message. This knowledge allows the attacker to predict the information and its flow. There are several ways to prevent the traffic analysis and Multiple Parents routing scheme is one such method. It allows the transfer of data to one of the multiple parents which will make the route of traffic less definite. It will confuse the attacker. Random traversal of packet or introduction of a fake path in the network can also prevent traffic analysis. However, with large number of DER devices and complex communications taking place in the system, this scheme is not ideal. To implement these methods, the DER devices would have to perform the complex cryptographic techniques to create a fake or multiple paths, which can affect the network output, ultimately affecting the system. The main area of research in this topic is to determine new techniques that could prevent traffic analysis with less complex encryption techniques.

5.5 Enhancing the Security of Serial Communication

Distribution Automation System contains a serial communication links between the Control Center and the other devices such as FRTU, DTU and TTU. Mostly DNP3 protocols are used in these communication links. DNP3 protocol normally transmits text in unencrypted format, which can be easily intercepted. The solution to avoid this is to wrap these texts into wrapping protocols like SSL/TLS, IPSEC. However, these wrapping protocols will put a load on communication
links with low band width which will bring down the speed of the system to a very large extend. The main area of research in this topic is to bring the encryption into a mechanism along with maintaining the latency and bandwidth of the system [42].

5.6 Roles to be Defined in Control Center

There are a few well defined roles in the control center. As the risk of threats and attacks in control center increases, various security schemes have been introduced into the system. Due to these schemes, more number of roles has to be defined. Responsibilities like maintaining and evaluating security mechanism involved with the system, are mainly included in these new roles. To avoid the new threats and vulnerabilities from being introduced into the system, the access control scheme for each of these roles should be defined correctly [42].

5.7 Authentication and Authorization of User at Field Substations

There are personnel working at the substation of the synchrophasor system. Authentication and authorization of these personals is an issue that requires lots of research. Access authorization to IEDs in the substation should be given only to some personnel and employees having specific roles related to those devices. However, the limitations in these setting are that system normally understands the roles of employees but is not programmed properly to limit the access of IEDs only to authorized employee. Therefore passwords are shared among multiple maintenance personnel even if the assignment of roles may be different. This fails the purpose of having roles. Moreover the password that is shared may be common among many systems, as there are so many devices deployed in a substation. Many of these devices are located at remote places and
are accessed through remote connection which takes place over slow communication line. So if authentication of user is done through remote connection, it will slow down the whole communication process. The main aim of this research is to have a mechanism which allows the access of devices in the substation to only authorize user performing particular task [42].

5.8 Timing Information Dependency
Today most of the systems in the power grid infrastructure use the real time information, which make them more dependent on the absolute time reference. It is necessary to have an absolute time reference for security protocols, which uses time stamp scheme for authentication to avoid the threat of replay action. Time reference is not only used for receiving real time information, but also used in time stamp in logs. These logs can be used to monitor and analyze the sequence of events to find and avoid any malicious activity. So it is necessary to make sure that the absolute time reference is not tampered on any devices and the provided synchronized clocks cannot be easily tampered [42].

5.9 Software Patches Update
Many devices like FRTUs, PMUs are installed in remote, distributed and isolated locations. Software updates on these devices are very difficult. It is a very lengthy process in electrical sector in which the backup systems are involved and after testing, the updates are performed and then deployed back into the system. In power sector, risk and vulnerabilities of the system are determined first. After that the patches are deployed based on their priority level. So a research is required for developing this system in more detail [42].
Chapter 6
CONCLUSIONS

6.1 Summary

The goal of this project was to understand the interconnection of DER with other systems in the smart grid and carry out research on the current and potential security vulnerabilities in those systems. This project also covered the counter measure techniques that can be applied to combat those security issues. Other systems interconnected with DER were Micro grid system, Distribution system and Synchrophasor system. All these systems are important to the DER for its proper functioning and also in fulfilling some of the goals of the smart grid.

Micro grids systems are similar to DER as they are also small and stand alone power generation units. However, micro grids are normally a part of electrical power distribution network with multiple DER devices, multiple loads along with the capability of islanding and operating independently from the grid. IDAPS is an intelligent micro grid system, which is mainly used for coordinating “customer-owned” DER devices for residential use. Distribution system is normally used for distribution of energy into the grid which connects all distributed generation units, IEDs customers, centralized generation unit, energy storage, transmission unit and market with two way flow of energy among these components. To improve the efficiency and reliability of the distribution system, automation was included in the system. Synchrophasor system is used for measuring and synchronizing absolute phase relationship between phase quantities at different
locations on power system. Synchrophasor systems are mainly used for monitoring operations of the grid through precise measurement.

There are a number of vulnerabilities that can be exploited in the IDAPS system, Distribution Automation System (DAS) and Synchrophasor system. Security issues identified in this project were securing the web services used in the IDAPS system for communication between agents. Security concerns for the existing substation infrastructure and PMU devices of synchrophasor system. Security issues in the secure communication between DCC and other remote devices in the DAS system. The vulnerabilities in these systems can lead to attacks such as modification, spoofing, reply attack and many more. The attacker can capture the message, analyze the traffic pattern, and modify parameters to cause denial of service. These security issues also affect the confidentiality, integrity, authentication, authorization and availability of data and resources in these systems.

The security measures and best practices for addressing these issues were discussed, such as use of cryptographic and non-cryptographic approach, key management, secure data transfer techniques, use of certificate and digital signature, use of firewalls and VPNs in the infrastructure and many more. Moreover as these systems consists of several components, the security measures and best practices can be used to mitigate the risks and concerns specified in this project.

The security issues and countermeasures are analyzed in this report; however, there are some areas which need further research. Bottom up approaches are required to meet these requirements. Due to varied use of communication protocols and smart devices over a massive project for smart grid, it is crucial to come up with reliable and cost effective solutions.
6.2 Strengths and Weaknesses

This project has the comprehensive list of the current and potential threats, vulnerabilities and security issues in systems connected to DER such as micro grid, distribution automation system and synchrophasor system. Various counter measures and best practices to overcome these security issues are also listed in this project. Use of real time information in IDAPS systems helps in predicting the electricity demand and usage. Use of real time information in synchrophasor systems helps in maintaining the efficiency and quality of the power system. Cost effective means which can provide counter measures against the security issues has been discussed. Cryptographic techniques including solutions through symmetric, asymmetric encryption or combinations of both have been proposed by keeping in mind the device and network constraints. The advantage of using this VPN which provides end-to-end security at the application level in synchrophasors was eliminating the complexity of the encryption, key exchange and management issues.

The weakness of the project is that the customer and owners of DER in IDAPS system can view the energy usage information through devices installed at home, but they are not able to view the real time information used by the IDAPS system. The reason for this weakness is that no mechanism has been developed which can provide real time information to customers through devices installed at home. Implementation of firewalls and electronic perimeter etc would block illegal traffic from entering the network in synchrophasor system. These are strong counter measure method which needs to be developed, implemented and tested carefully. Another protocol used for communication in distribution automation systems, is the IEC 62351. Security
issues and its counter measures for this protocol have not been discussed in this project because it is widely used in Europe and not common in North America.

6.3 Future Works

This project addressed security issues and best practices in the systems that are interconnected with DERs with a very low-level of implementation, mainly focusing on how to ensure security requirements in the information transmitted through these systems and in smart grid networks. However there are many components related to these systems and DER that are not discussed in this report, such as the Distribution Management System, Advanced Distribution Automations, and transmission systems. These systems could pose new vulnerabilities and security issues to the smart grid regarding its integration with DER systems.

Moreover many of the concepts discussed in this report are still in their experimental stage and has not yet been implemented in real system. As an example, the micro grids discussed are still a theoretical concept and has not been implemented in the real system in USA, mostly due to the safety concerns about connecting them with the utility grid.

A model for these systems should be developed, so that utilities can access these systems and can define the access control capabilities based on these models. This requires some more research as to avoid illegal access to the system.

Data mining and data processing techniques should also be developed, as large amount of data is collected in these systems. Moreover most of these data being a real-time, data center and cloud computing techniques should be used.
REFERENCES


